



How to Create and Use Self-Signed SSL Certificates

Network security is critical to ensure data authentication, integrity, and confidentiality in today's digital age, where sensitive information is transmitted over the Internet. HTTPS (Secure HTTP) uses encryption for secure communication over a computer network. HTTPS is encrypted using Transport Layer Security (TLS), formerly Secure Sockets Layer (SSL). The protocol is still referred to as HTTP over SSL, commonly shown as **https://** in the browser address bar.

SSL/TLS relies on the use of keys and digital certificates. Keys occur in pairs (public/private) and are used for encryption/decryption. A public key is used for encryption, while the private key is used for decryption. Digital certificates are used to prove the ownership and authenticity to ensure that only authorized devices



communicate with each other. Certificates are typically issued and managed by a trusted third-party company, called a Certificate Authority (CA). Getting an SSL certificate installed for a website by a well-known CA that is trusted by all devices and browsers, such as DigiCert, Comodo, GoDaddy, Let's Encrypt, can provide access to the website seamlessly over the public Internet. These trusted CAs only provide certificates to websites which have a public IP address. They won't do this for devices on an internal network with private IP addresses.

As most of our customers use our devices on internal networks, they can create a self-signed certificate. If you don't have an IT, you can generate a self-signed certificate that will make our device trusted by your browser.

Self-signed digital certificates are created by signing the certificate with the owner's private key. They are created, issued, and signed by the company or developer who is responsible for the website/software being signed. Unlike certificates issued by a trusted CA, no external party verifies a self-signed certificate. Self-signed certificates are fast, free, and easy to issue. They are appropriate for development/testing environments, internal network websites and providing secure webpages for devices. Most devices will use a self-signed certificate because of the associated cost of getting a certificate from a well-known CA that is trusted by all browsers.

If you don't have OpenSSL on your Windows's PC, you can utilize Windows Package Manager, WinGet, a free and open-source package manager designed by Microsoft that allows users to discover, install, upgrade, remove, and configure applications on Windows 10, Windows 11, and Windows Server 2025 computers.

If you are accessing the HTTPS device from a different PC, a Security Warning message will appear. You must download the self-signed certificate and install it to your local machine's trusted certificate store.

This document explains how to add OpenSSL for Windows using WinGet and create a self-signed certificate, how to install this self-signed certificate on the device, and how to download and install the self-signed certificate on different Windows machines. Instructions are provided for commonly used browsers—Google Chrome , Microsoft Edge  and Mozilla Firefox .

I. Install OpenSSL on Windows 10/11 Computers Using WinGet

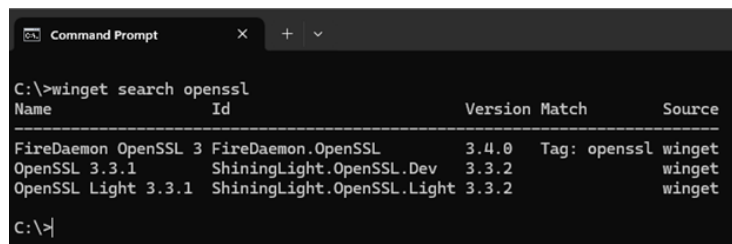
If you don't have OpenSSL on your Windows 10 or Windows 11 computer, you can utilize WinGet command line tool to install and configure the OpenSSL application. This free and open-source tool is the client interface to the Windows Package Manager service that enables users to discover, install, upgrade, remove and configure applications on Windows 10, Windows 11, and Windows Server 2025 computers.

1. Install WinGet.

Refer to: <https://learn.microsoft.com/en-us/windows/package-manager/winget/#install-winget>

2. Search for current version of OpenSSL by running the following command:

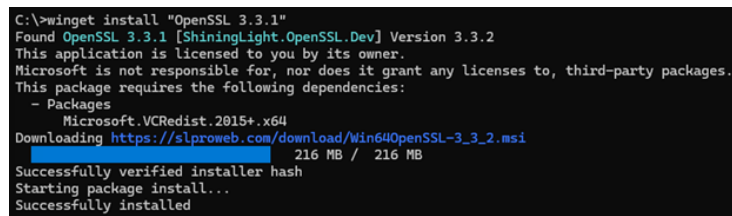
C:\>**winget search OpenSSL**



Name	Id	Version	Match	Source
FireDaemon OpenSSL 3	FireDaemon.OpenSSL	3.4.0	Tag: openssl	winget
OpenSSL 3.3.1	ShiningLight.OpenSSL.Dev	3.3.2		winget
OpenSSL Light 3.3.1	ShiningLight.OpenSSL.Light	3.3.2		winget

3. Using Winget, install OpenSSL using the full name in quotes. (Install your current version, if different than the example below.)

Example: C:\>**winget install "OpenSSL 3.3.1"**



```
C:\>winget install "OpenSSL 3.3.1"
Found OpenSSL 3.3.1 [ShiningLight.OpenSSL.Dev] Version 3.3.2
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
This package requires the following dependencies:
- Packages
  Microsoft.VCRedist.2015+.x64
Downloading https://slproweb.com/download/Win640penSSL-3_3_2.msi
216 MB / 216 MB
Successfully verified installer hash
Starting package install...
Successfully installed
```

4. To confirm OpenSSL is correctly installed and can be located, close the current terminal window, and open a new command prompt.

5. Run the following command:

C:\>**OpenSSL version -a**

NOTE: If you get an error and OpenSSL isn't installed correctly on your local machine's PATH, navigate to Settings > System > About > Advanced System Settings > Environment Variables. Then, under System variables:

- a. Click **Path** and then click **Edit**.
- b. Click **New** and paste the file path of the "openssl.exe" file.
(The common path is "C:\Program Files\OpenSSL-Win64\bin")
- c. Click **OK** to apply changes.

II. Generate Self-signed Certificate for Your Device IP

1. Create a text file containing the following minimal information and name it `openssl.cnf`

```
[ req ]
default_bits          = 4096
default_md            = sha256
prompt               = no
string_mask          = default
distinguished_name    = req_dn
x509_extensions      = x509_ext

[ req_dn ]
countryName          = US
stateOrProvinceName  = IL
organizationName     = Contemporary Controls
commonName           = BASrouterSX ←

[ x509_ext ]
subjectKeyIdentifier  = hash
authorityKeyIdentifier = keyid:always
keyUsage              = critical, digitalSignature, keyEncipherment
extendedKeyUsage      = serverAuth
subjectAltName        = IP:10.0.13.71 ←
```

Update the **commonName** to your device name and **subjectAltName** to your device IP address (BASgatewaySX and 10.0.13.71, in this example).

2. In the .cnf file, change the commonName/subjectAltName to reflect the name and IP address of the device (BASgatewaySX and **10.0.13.71**, in this example.)

NOTE: For a device that contains more than one IP: Add IP:xxx.xxx.xxx.xxx, IP:xxx.xxx.xxx.xxx, etc. , in the subjectAltName field.

```

1 [ req ]
2 default_bits = 4096
3 default_md = sha256
4 prompt = no
5 string_mask = default
6 distinguished_name = req_dn
7 x509_extensions = x509_ext
8
9 [ req_dn ]
10 countryName = US
11 stateOrProvinceName = IL
12 organizationName = Contemporary Controls
13 commonName = BASSgatewaySX
14
15 [ x509_ext ]
16 subjectKeyIdentifier = hash
17 authorityKeyIdentifier = keyid:always
18 keyUsage = critical, digitalSignature, keyEncipherment
19 extendedKeyUsage = serverAuth
20 subjectAltName = IP:10.0.13.71
21

```

3. Save the generated **openssl.cnf** file to the working directory from the command line.
4. Run the following command to build **selfsigned.key** and **selfsigned.pem** files:
C:\>openssl req -x509 -new -nodes -days 3650 -keyout selfsigned.key -out selfsigned.pem -config openssl.cnf
(Adjust the days in the above command to change the certificate validity period.)

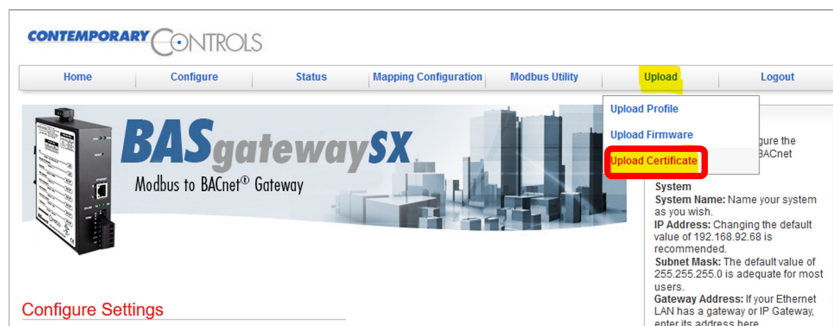
[illegible]

- Run the following command to generate a Security Certificate:
C:\>**OpenSSL x509 -in selfsigned.pem -out selfsigned.crt**

```
C:\>openssl x509 -in selfsigned.pem -out selfsigned.crt  
C:\>|
```

III. Upload Certificate to the Device using the Certificate Upload Feature

- From the device webpage **Upload** menu tab, select **Upload Certificate**.



- Select **Private Key** from the Choose Certificate drop-down menu and click **Save**.
- From the Certificate Upload section, click the **Browse** button and select the recently generated **selfsigned.key** file.
- Click **Upload**.

Certificate

Choose Certificate: Private Key

Save Cancel

Certificate Upload

Upload Certificate to Gateway Select File: Browse... selfsigned.key

Upload Cancel

- Select **Private Certificate** from the Choose Certificate drop-down menu and click **Save**.

Certificate

Choose Certificate: Private Certificate

Save Cancel

- From the Certificate Upload section, click **Browse** and select the **selfsigned.pem** file.
- Click **Upload**.
- Click **Update Certificates and Reboot**.
- Close out all open tabs of the unit and wait for it to reboot.

Certificate

Choose Certificate: Private Certificate

Save Cancel

Certificate Upload

Upload Certificate to Gateway Select File: Browse... selfsigned.pem

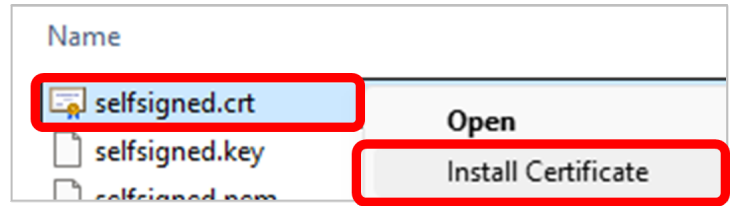
Upload Cancel

Update Certificates and Reboot

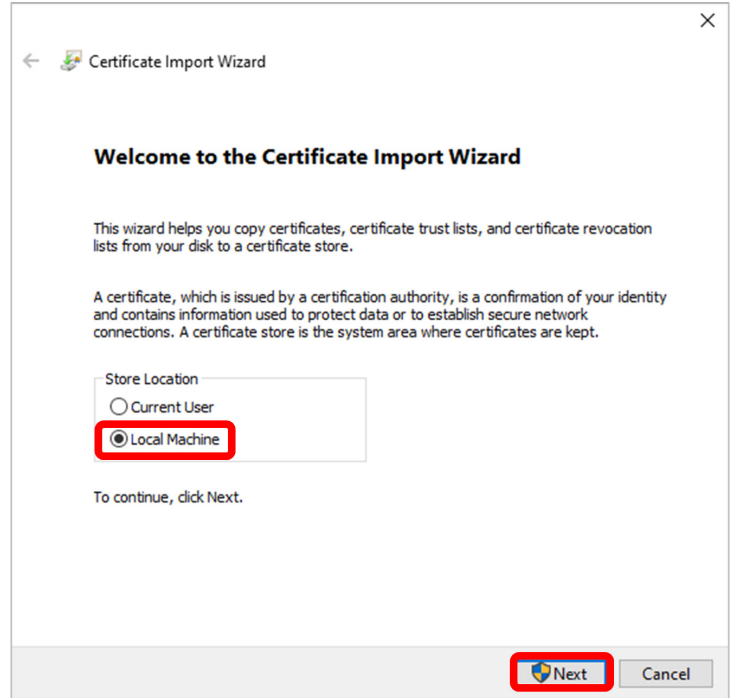
©2024 Contemporary Control Systems, Inc. All rights reserved.

IV. Install Certificate .crt Format to Trusted Root CA Folder

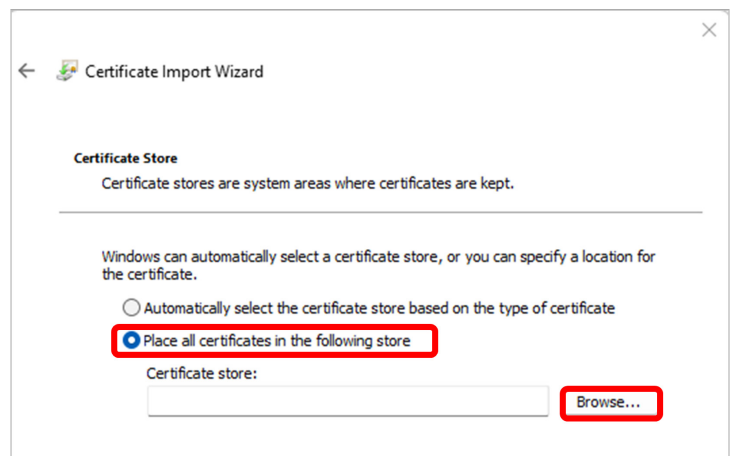
1. Right-click the selfsigned.crt file, select **Install Certificate** from the drop-down menu.
NOTE: The selfsigned.key, .pem, and .crt files should all be located in the current working directory.



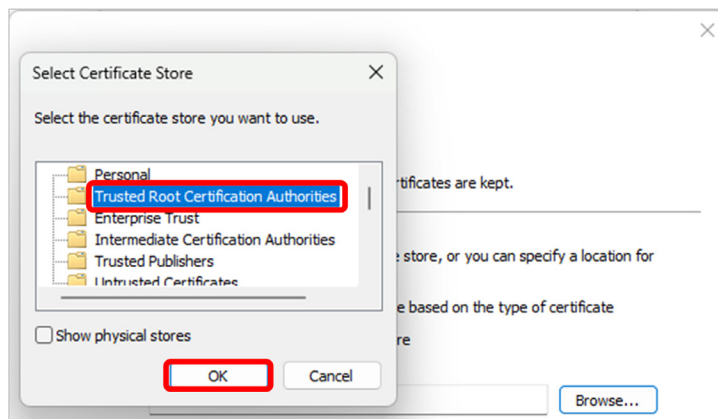
2. From the Certificate Import Wizard, select **Local Machine**. Then, click **Next**.



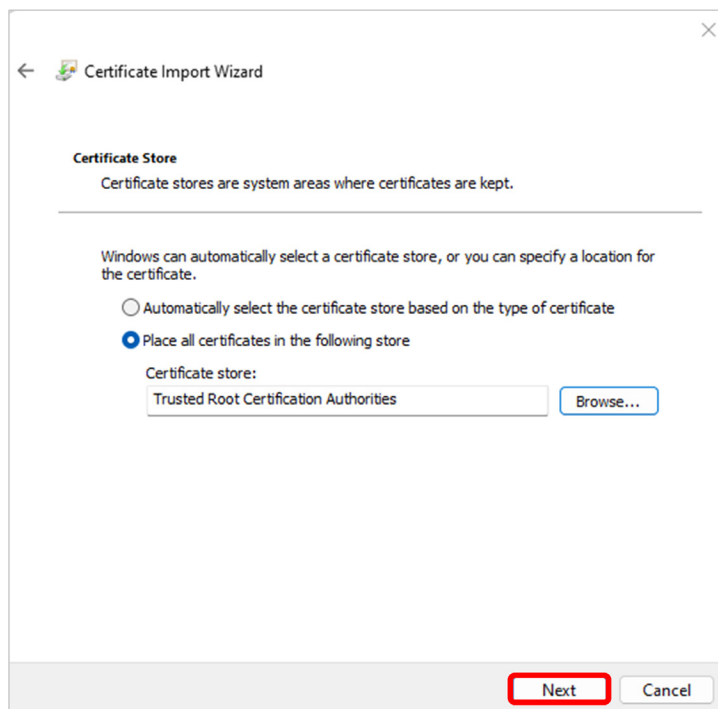
3. Select **Place all certificates in the following store**, then click **Browse...**



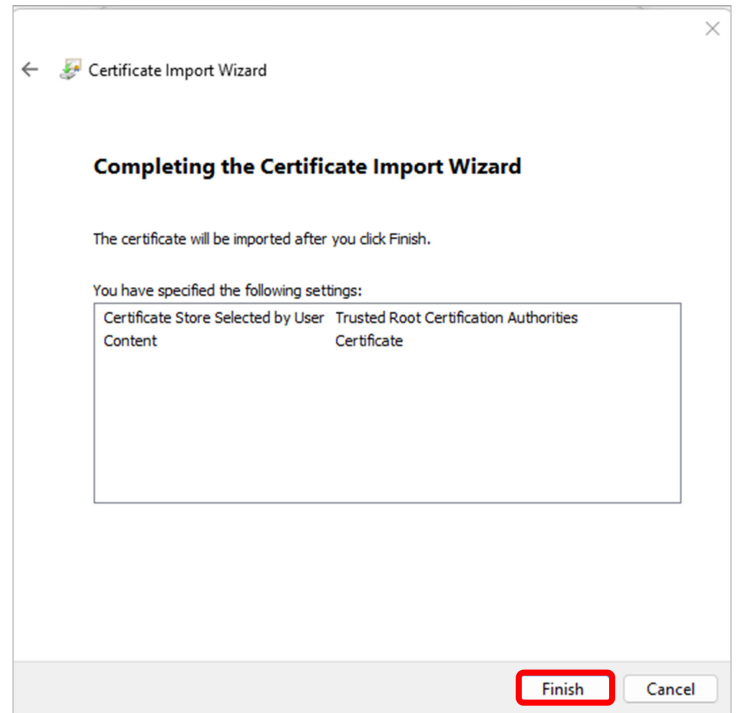
- From the Select Certificate Store pop-up, select **Trusted Root Certificate Authorities**, and then click **OK**.



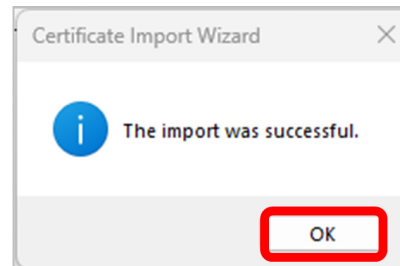
- Click **Next**.



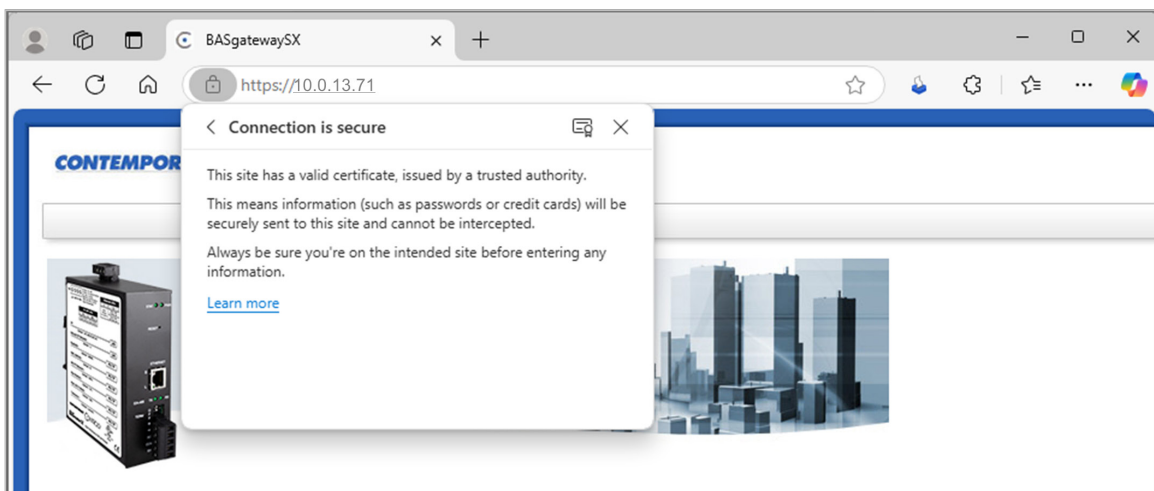
6. Click **Finish**.



7. If successful, a pop-up window should read, "The import was successful." Click, **OK**.



8. Clear your cache, then open the unit's IP address in a web browser and confirm the connection is secure.



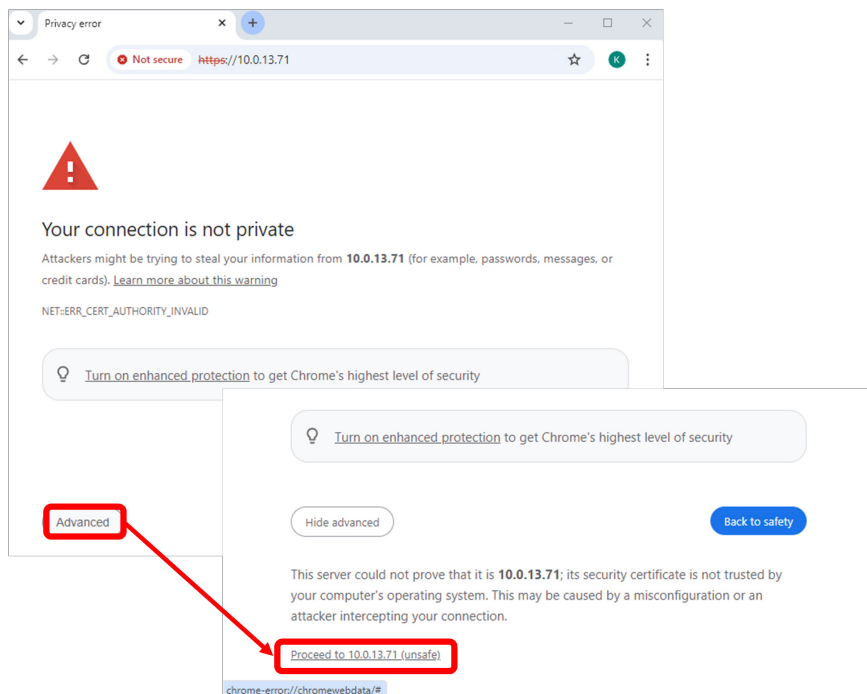
V. Accessing the Device From Additional PCs

If you are accessing the device from a different PC, you must download the self-signed certificate and install it to your local machine's trusted certificate store. The self-signed certificate can be downloaded via the browser. Instructions are provided for commonly used browsers—Google Chrome , Microsoft Edge  and Mozilla Firefox .

Download Certificates Using Google Chrome

1. Launch the device webpage in Google Chrome .

- a. Enter the **IP address** for the Contemporary Controls device (10.0.13.71 in this example.)
- b. From the Warning screen:
 - Click **Advanced**.
 - Click **Proceed to [IP address] (unsafe)**. IP is 10.0.13.71 in this example.



2. The device webpage will launch.

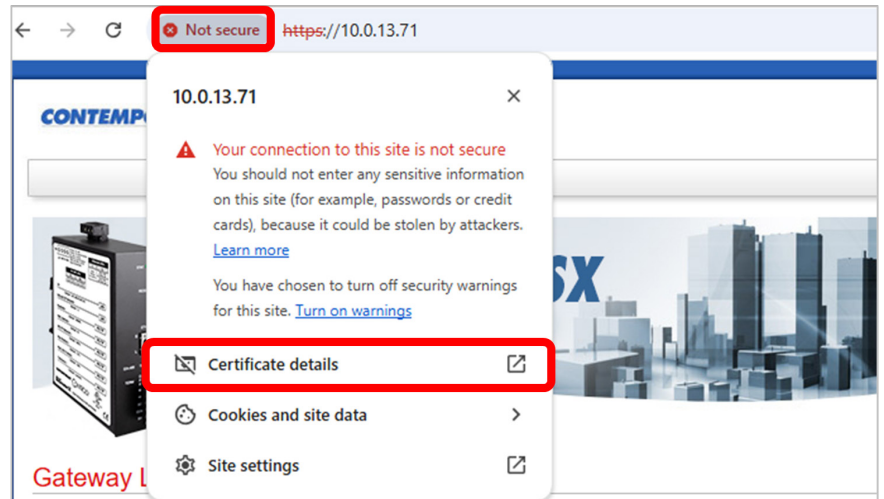
NOTE: For GSA-compliant devices, a GSA WARNING will appear.

Click **I Agree** to continue.

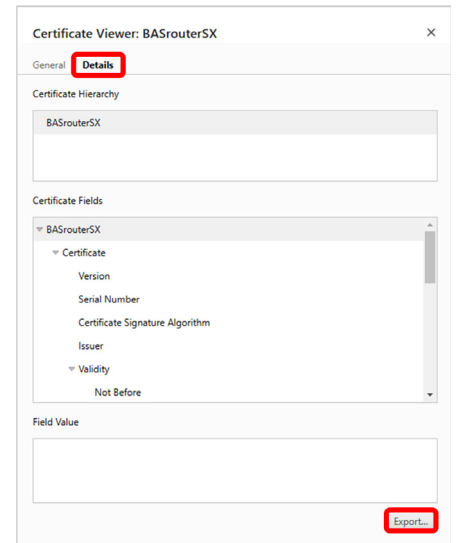


Application Note – Self Signed SSL Certificates

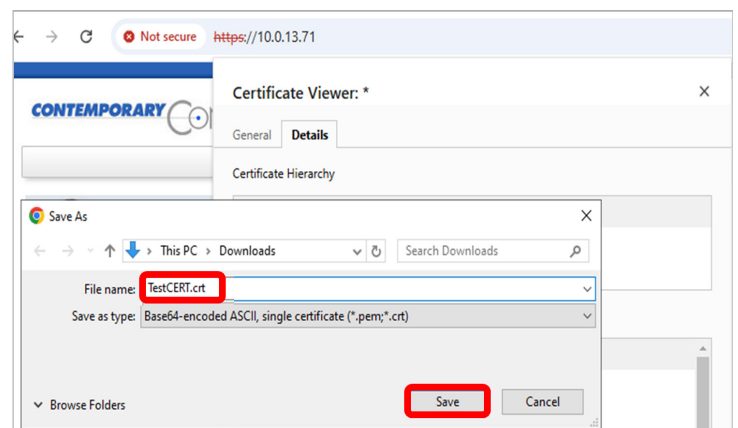
3. Download certificate to your local computer in .crt format.
 - a. Click **Not secure** in the URL and select **Certificate details** from the drop-down menu.



- b. Select the **Details** tab and click **Export** to save the certificate locally on the computer.

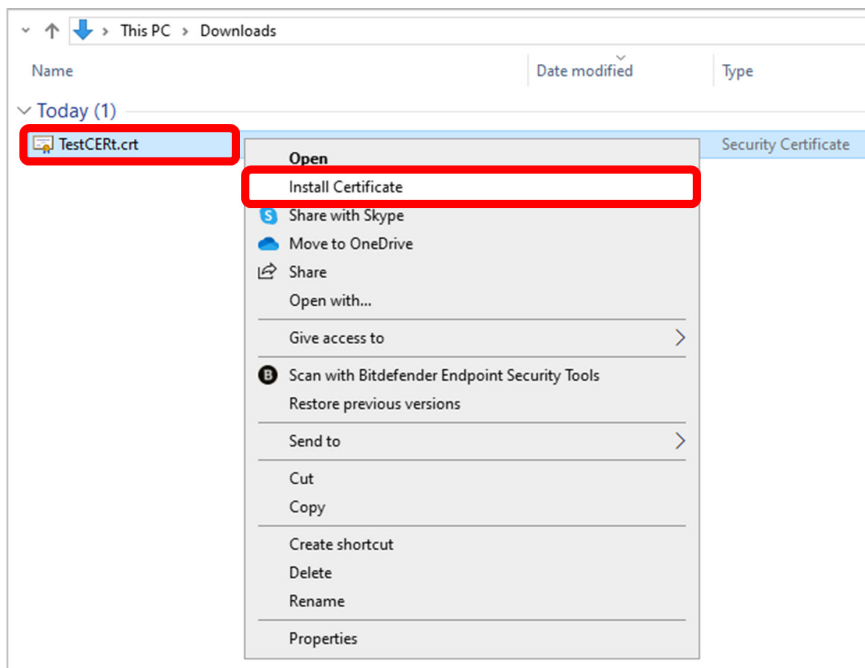


- c. Name the certificate, then click **Save**.



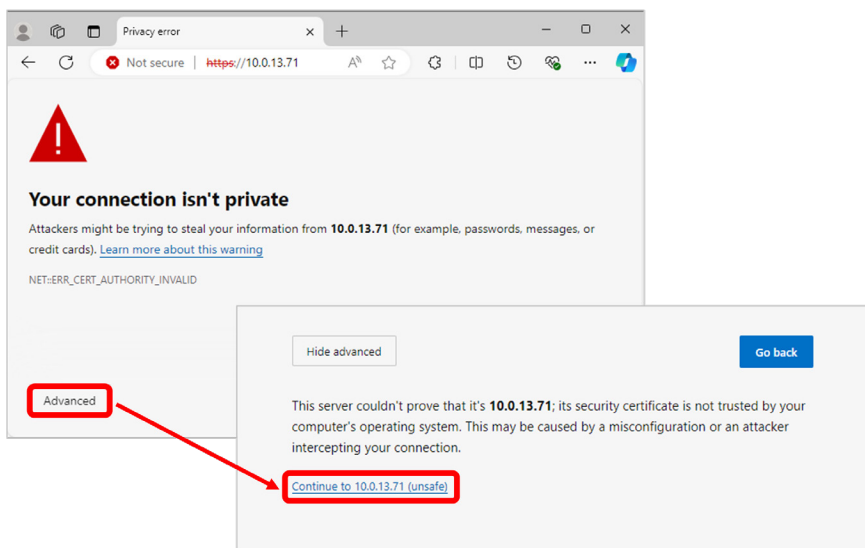
- d. Select the certificate in the Downloads folder. Right-click, then select **Install Certificate** from the drop-down menu.

4. Follow the instructions described in [Section IV: Install Certificate .crt Format to Trusted Root CA folder](#)



Download Certificates Using Microsoft Edge

1. Launch the device webpage and advance through the Security Warning.
 - a. Enter the **IP address** for the Contemporary Controls device, (10.0.13.71 in this example.)
 - b. From the Warning screen:
 - Click **Advanced**.
 - Click **Continue to [IP address] (unsafe)**.



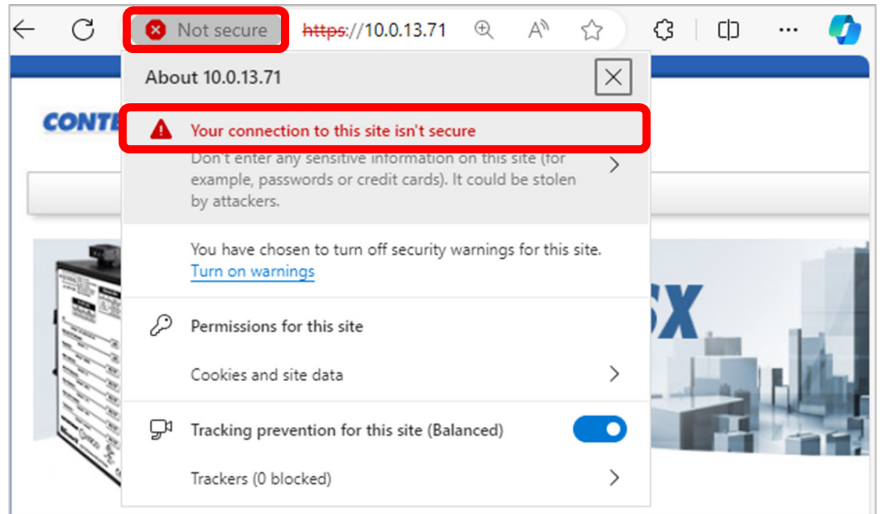
2. The device webpage will launch.

NOTE: For GSA-compliant devices, a GSA WARNING will appear.

Click **I Agree** to continue.

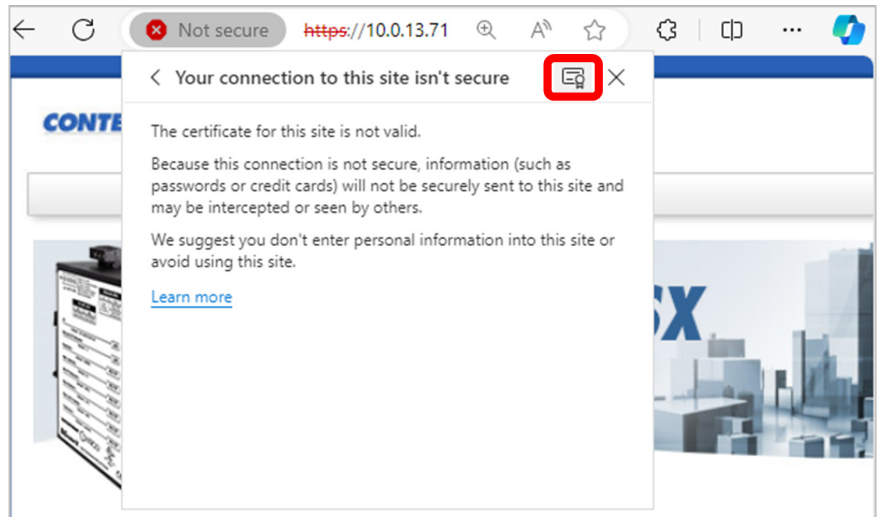


3. Download certificate to your local computer in .crt format.
 - a. Click **Not secure** in the URL and select **Your connection to this site isn't secure** from the drop-down menu.



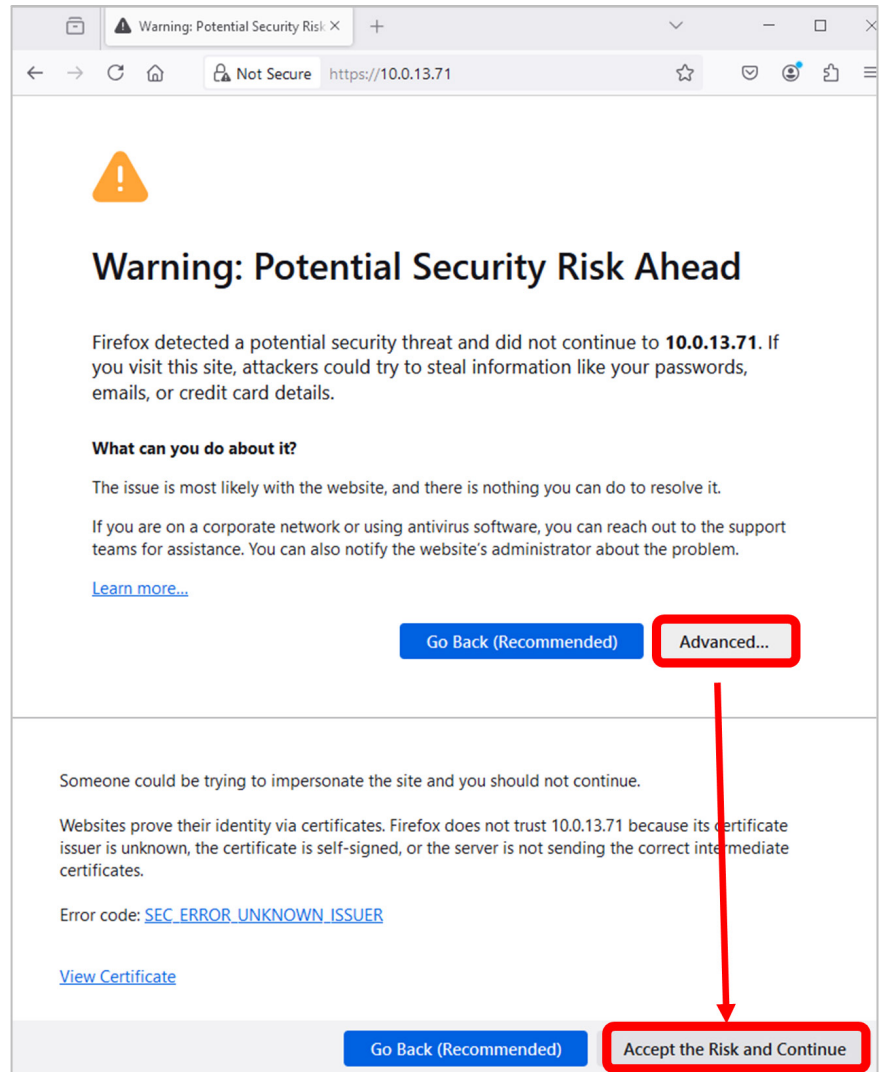
- b. Click the **certificate** icon.

4. Follow the instructions described in [Section IV: Install Certificate .crt Format to Trusted Root CA folder](#).



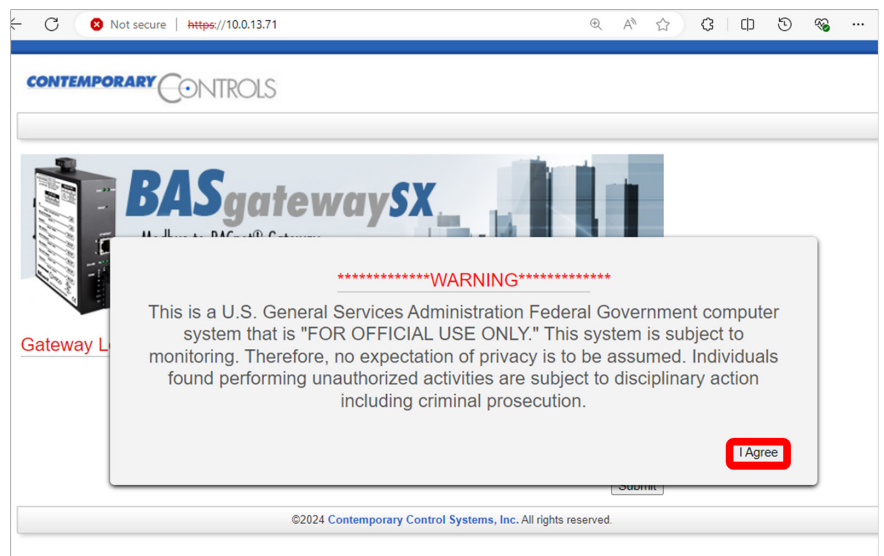
Download Certificates in Mozilla Firefox

1. Launch the device webpage and advance through the Security Warning.
 - a. Enter the **IP address** for the Contemporary Controls device, (10.0.13.71 in this example.)
 - b. From the Warning screen:
 - Click **Advanced**.
 - Click **Accept the Risk and Continue**.



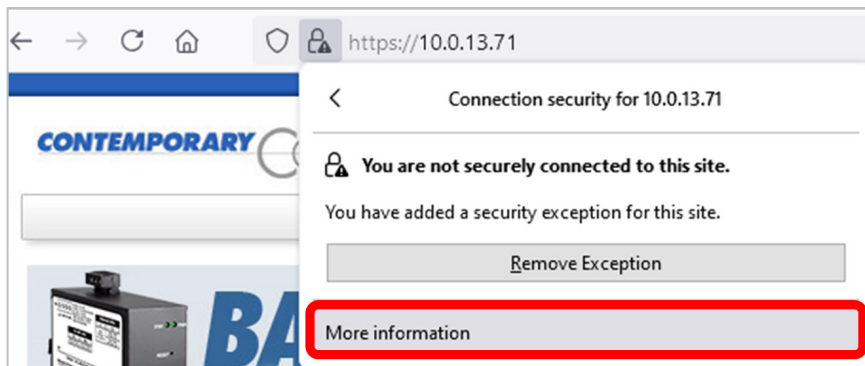
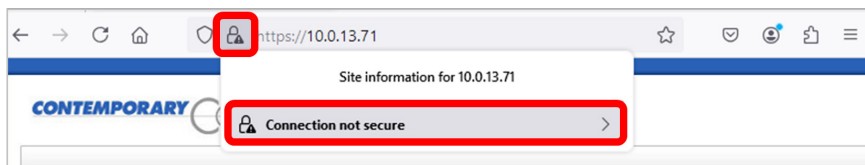
2. The device webpage will launch.

NOTE: For GSA-compliant devices, a GSA WARNING will appear.
Click **I Agree** to continue.

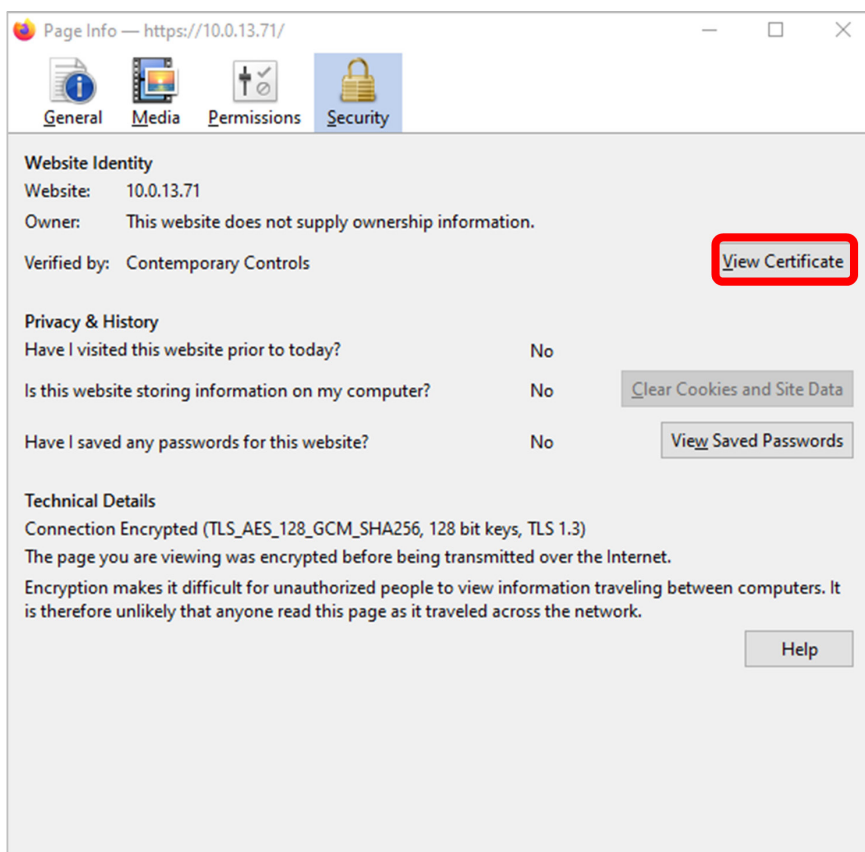


Application Note – Self Signed SSL Certificates

3. Download certificate to your local computer in .crt format.
 - a. Click the **Security Warning** icon in the URL and select **Connection not secure** from the drop-down menu.
 - b. Select **More Information**.



- c. Click **View Certificate**.



- d. Click the **PEM cert** link to download the “pem” file.

Firefox about:certificate?cert=MIIGKTCCBBGgAwIBAg 50%

Certificate

Subject Name	
Country	US
State/Province	Illinois
Locality	Downers Grove
Organization	Contemporary Controls
Organizational Unit	R&D
Common Name	*
Email Address	info@cccontrols.com

Issuer Name	
Country	US
State/Province	Illinois
Locality	Downers Grove
Organization	Contemporary Controls
Organizational Unit	R&D
Common Name	*
Email Address	info@cccontrols.com

Validity	
Not Before	Thu, 12 May 2022 00:10:51 GMT
Not After	Wed, 19 May 2032 00:10:51 GMT

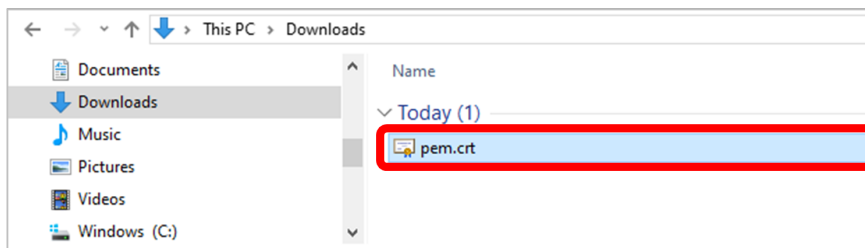
Subject Alt Names	
DNS Name	*.pcbook.com
DNS Name	*.pcbook.org
IP Address	0.0.0.0

Public Key Info	
Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	BC:EE:0D:77:CE:96:CE:21:11:9A:9A:88:25:47:2C:E0:E7:4D:6F:CB:9F:09:52:87:...

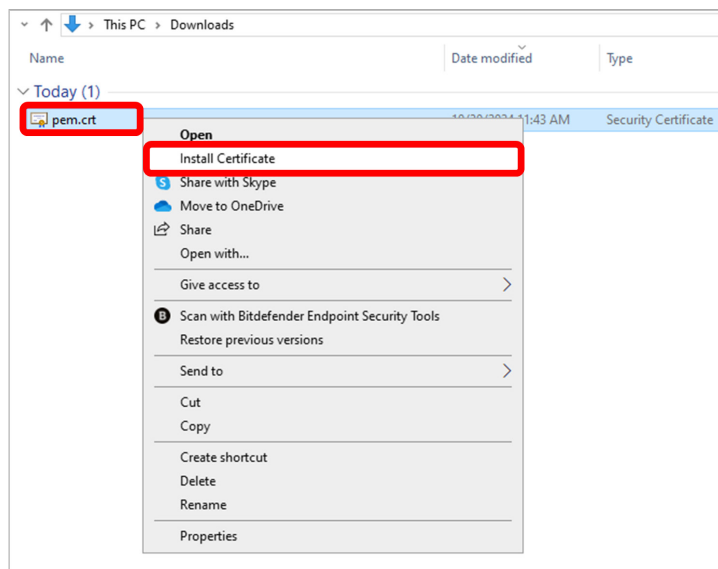
Miscellaneous	
Serial Number	38:5E:DB:1E:DD:ED:56:9C:D9:C0:35:E4:A5:83:AA:02:6F:41:B1:44
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints	
SHA-256	02:7E:AS:34:35:99:15:D8:15:4C:F5:EE:19:EF:06:A2:CC:D8:08:01:EC:2F:6E:66:6...
SHA-1	0D:4F:C2:1C:DF:58:9A:85:64:32:07:62:13:C7:7A:3F:57:99:E9:45

- e. From your Downloads folder, rename the pem file to **pem.crt**

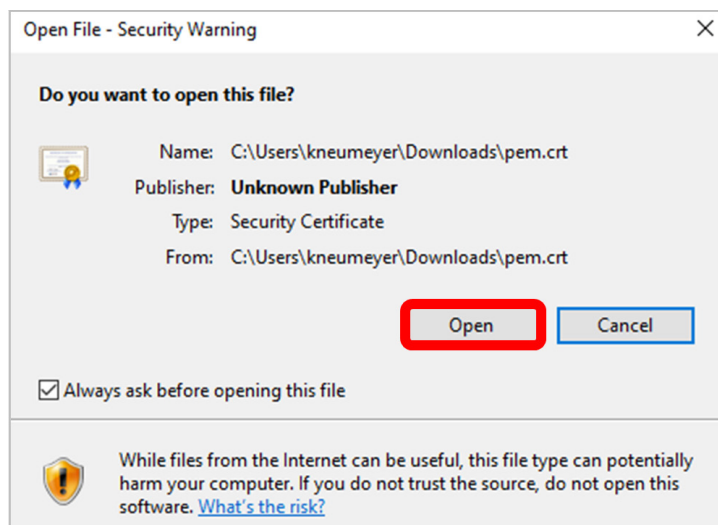


- f. Select the certificate. Right-click, then select **Install Certificate** from the drop-down menu.



- g. Click **Open** on the pop-up screen to allow installation.

4. Follow the instructions described in [Section IV: Install Certificate .crt Format to Trusted Root CA folder](#).

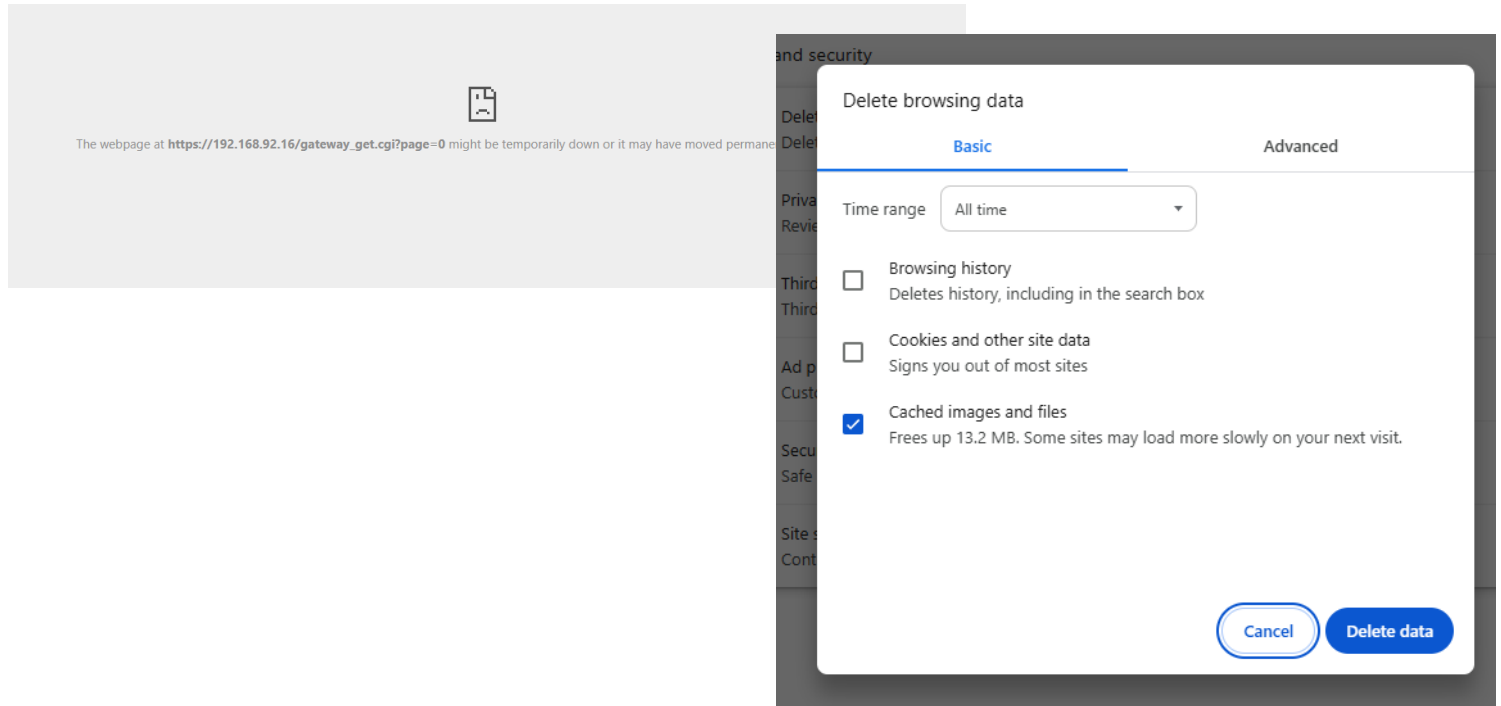


VI. Appendix: IP Resetting on your Device

Your self-signed certificate can be overwritten if you reset the device on a PC that has a previously established self-signed certificate.

For example, say the device's self-signed certificate is Installed at IP 10.0.13.71 and trusted by your PC via the Trusted Root CA folder. When you reset your device (by pressing the device's reset button), the device returns to the default IP (e.g., 192.168.92.16), and your new self-signed certificate at IP 10.0.13.71 is not recognized.

Clear your cache and device's webpage will be accessible, and follow the instructions described in [Section IV: Install Certificate .crt Format to Trusted Root CA folder](#).



United States
Contemporary Control
Systems, Inc.

Tel: +1 630 963 7070
Fax: +1 630 963 0109

info@ccontrols.com

China
Contemporary Controls
(Suzhou) Co. Ltd

Tel: +86 512 68095866
Fax: +86 512 68093760

info@ccontrols.com.cn

United Kingdom
Contemporary Controls Ltd

Tel: +44 (0)24 7641 3786
Fax: +44 (0)24 7641 3923

ccl.info@ccontrols.com

Germany
Contemporary Controls GmbH

Tel: +49 341 520359 0
Fax: +49 341 520359 16

ccg.info@ccontrols.com

www.ccontrols.com