

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 opensource 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 O, Microsoft Edge O 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: <u>https://learn.microsoft.com/en-us/windows/package-manager/winget/#install-winget</u>
- 2. Search for current version of OpenSSL by running the following command:
 - C:\>winget search OpenSSL

Command Prompt	×						
C:\>winget search	opoperal						
Name	Id			Version	Match	ı	Source
FireDaemon OpenSSI	3 FireDa	aemon.OpenSSL		3.4.0	Tag:	openssl	winget
OpenSSL 3.3.1	Shinir	gLight.OpenSSL	Dev	3.3.2			winget
	1 Shinir	gLight.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/Win64OpenSSL-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]

[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		
organizationName	= Contemporary Controls	
commonName	= BASrouterSX	Update the commonName
[x509_ext]		to your device name and
subjectKeyldentifier	= hash	subjectAltName to your device
authorityKeyldentifier		IP address (BASgatewaySX and
keyUsage	= critical, digitalSignature, keyEncipherment	10.0.13.71, in this example).
extendedKeyUsage	= serverAuth	
subjectAltName	= IP:10.0.13.71	

 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, IP:xxx.xxx.xxx, etc., in the subjectAltName field.

📄 opei	nssl.cnf 🗵
1	[req]
2	default_bits = 4096
3	default_md = sha256
4 5	prompt = no
	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 = BASgatewaySX
14	
15	[x509_ext]
16	<pre>subjectKeyIdentifier = hash</pre>
17	authorityKeyIdentifier = keyid:always
18	<pre>keyUsage = critical, digitalSignature, keyEncipherment</pre>
19	extendedKeyUsage = serverAuth
20	<pre>subjectAltName = IP:10.0.13.71</pre>
21	

- 3. Save the generated **openssl.cnf** file to the working directory from the command line.
- 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.)

C:\>openssl reg -x509 -new -nodes -days 3660 -keyout selfsigned.key -out selfsigned.pem -config openssl.cnf
\cdots

* * * * * * * * * * * * * * * * * *
· + + + + + + + + +
· · · · · · · · · · · · · · · · · · ·
······································
+++++++++
·.+++++++++++++.
· · · · · · · · · · · · · · · · · · ·
++
· · · · · · · · · · · · · · · · · · ·
++++++++++++
· · · · · · · · · · · · · · · · · · ·
····+····
C:\>

 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

1. From the device webpage Upload menu tab, select Upload Certificate.



- 2. 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.
- 4. Click Upload.
- 5. Select **Private Certificate** from the Choose Certificate drop-down and click **Save**.
- 6. From the Certificate Upload section, click **Browse** and select the **selfsigned.pem** file.
- 7. Click Upload.
- 8. Click Update Certificates and Reboot.
- 9. Close out all open tabs of the unit and wait for it to reboot.

Certificate		
Choose Certificate: Private Key v		
	_	\square
	Save	Cancel
Certificate Upload		
Upload Certificate to Gateway Select File: Brows	e selfsigned.key	
	Upload	Cancel
Certificate		
Choose Certificate: Private Certificate V		
	Save	Cancel
Certificate		
Choose Certificate: Private Certificate v		
	Save	Cancel

Upload Certificate to Gat	eway Select File:	Browse selfsig	ned.pem
			Upload
ate Certificates and Reboot			

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

- 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**.

	selfsigned.crt	Open
	selfsigned.key	Install Certificate
← 🛓	Certificate Import Wizard	
	Welcome to the Certificate	e Import Wizard
	This wizard helps you copy certificates, ce lists from your disk to a certificate store.	rtificate trust lists, and certificate revocation
	A certificate, which is issued by a certifica and contains information used to protect connections. A certificate store is the sys	
	Store Location	
	O Current User	
	Local Machine	
	Local Machine To continue, dick Next.	
		Next Canc
÷ §		Next Canc
	To continue, dick Next.	∳ Next Canc
	To continue, dick Next.	
	To continue, dick Next. Certificate Import Wizard Certificate Store Certificate stores are system areas whe	
	To continue, click Next. Certificate Import Wizard Certificate Store Certificate stores are system areas whe Windows can automatically select a cert the certificate.	re certificates are kept. ificate store, or you can specify a location for e store based on the type of certificate

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

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



5. Click Next.

	\times
🗧 🛃 Certificate Import Wizard	
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location the certificate.	for
\bigcirc Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Browse	
Next	Cancel

6. Click Finish.

÷ 🦻	Certificate Import Wizard		×
	Completing the Certifi	cate Import Wizard	
	The certificate will be imported after	you dick Finish.	
	You have specified the following set	tings:	
		Trusted Root Certification Authorities Certificate	
		Finish Cancel	
Certifi	cate Import Wizard	×	
ĺ	The import was success	sful.	
		r l	

- 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 (2), Microsoft Edge (2) and Mozilla Firefox (2).

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.



 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 **Certificate details** from the drop-down menu.



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

Certificate Viewer: BASrouterSX	
General Details	
Certificate Hierarchy	
BASrouterSX	
Certificate Fields	
Version	
Serial Number	
Certificate Signature Algorithm	
Issuer	
∀ Validity	
Not Before	
Field Value	
	Expor

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

	Certificate Viewer: *	×
Save As	Certificate Hierarchy	
← → ✓ ↑ ↓ → This PC → File name: TestCERT.crt	×	
Save as type: Base64-encode	ed ASCII, single certificate (*,pem;*.crt) V	*



- 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 C.

- 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.



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 the **Security Warning** icon in the URL and select **Connection not secure** from the drop-down menu.
 - b. Select More Information.



$\leftarrow \rightarrow c$	<u>ن</u>	08	https:	//10.0.13.7	I				
			<	Connec	tion security	y for 10.	0.13.71		
CONTEM	PORAR	and .	A You	are not secur	ely connec	ted to t	his site.		
			You have	added a secu	rity exceptio	on for tł	nis site.		
-					<u>R</u> emove Exe	ception			
		BA	More info	ormation					
ڬ Page Info —	https://10.0	.13.71/					_		×
General M	dedia <u>P</u> er	t ö missions	<u>S</u> ecurity						
Website Identity Website: 10.0.13.71 Owner: This website does not supply ownership information. Verified by: Contemporary Controls									
Privacy & Histo Have I visited th		prior to tod	av?		No				
Is this website storing information on my computer? No <u>Clear Cookies and</u>						and Site	Data		
Have I saved any passwords for this website? No View Saved Password						ords			
Technical Detai Connection End The page you a Encryption mak is therefore unl	crypted (TLS re viewing v kes it difficu	vas encrypt It for unaut	ted before l thorized pe	peing transmit	ted over the formation to	raveling		ompute Hel	

c. Click View Certificate.

d. Click the **PEM cert** link to download the "pem" file.

۲	Firefox	about:ce	rtificate?cert=MIIGKTCCBBGgAwIBAg 50%	
C	Certificate			
			*	
		Subject Name		
		Country		
	State/Province			
	-		Downers Grove	
			Contemporary Controls R&D	
	Organizational Unit Common Name		*	
		Email Address	info@ccontrols.com	
		Issuer Name		
		Country	US	
		State/Province		
		Locality	Downers Grove	
			Contemporary Controls	
	Organizational Unit			
	c	Common Name	•	
		Email Address	info@ccontrols.com	
		Validity		
		Not Before	Thu, 12 May 2022 00:10:51 GMT	
		Not After	Wed, 19 May 2032 00:10:51 GMT	
	Sub	ject Alt Names		
		DNS Name	*.pcbook.com	
		DNS Name		
		IP Address	0.0.0	
	i	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:09:52:67:	
		Miscellaneous		
		Serial Number	38:55:D8:15:DD:5D:56:9C:D9:C0:35:54:A5:83:AA:02:6F:41:81:44	
	Signa	ture Algorithm	SHA-256 with RSA Encryption	
	Signature Algorithm Version			
		Download	<u>PEM (cert) PEM (chain)</u>	
		Fingerprints		
		SHA-256	027F-A5-34-35-99-15-DB-15-4C-F5-EE-19-EF-06-A2-CC-DB-08-01-EC-2F-6E-66-6	
		SHA-250 SHA-1		
		anadi	and any second department of the second process of the second second second second second second second second	

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

← → × ↑ 🕹 > This PC > Downloads						
Documents	^	Name				
🕂 Downloads		∽ Today (1)				
Music		📮 pem.crt				
		E _R) pem.crt				
📑 Videos						
🏪 Windows (C:)	¥					

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 <u>Section IV:</u> <u>Install Certificate .crt Format to Trusted Root CA</u> <u>folder</u>.



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 <u>Section IV: Install</u> <u>Certificate .crt Format to Trusted Root CA folder</u>.



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

AN-SSLCERTO-AA0 February, 2025