

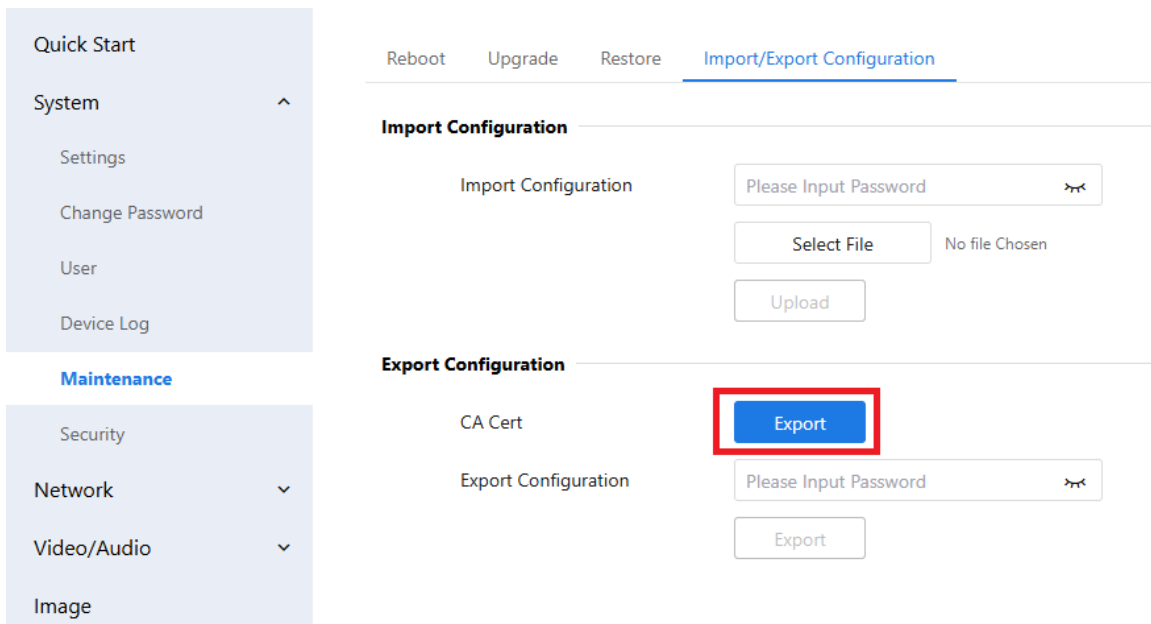
How to use secure connection in HTTPS mode

Solution 1: Use self-signed CA certificate built-in firmware

1. Download the built-in CA certificate

The firmware has a built-in CA certificate, user can download the certificate from the web page, then import the certificate to PC's system.

Go to [Setting](#) > [System](#) > [Maintenance](#) > [Import/Export Configuration](#), click on [Export](#) to export the CA certificate.



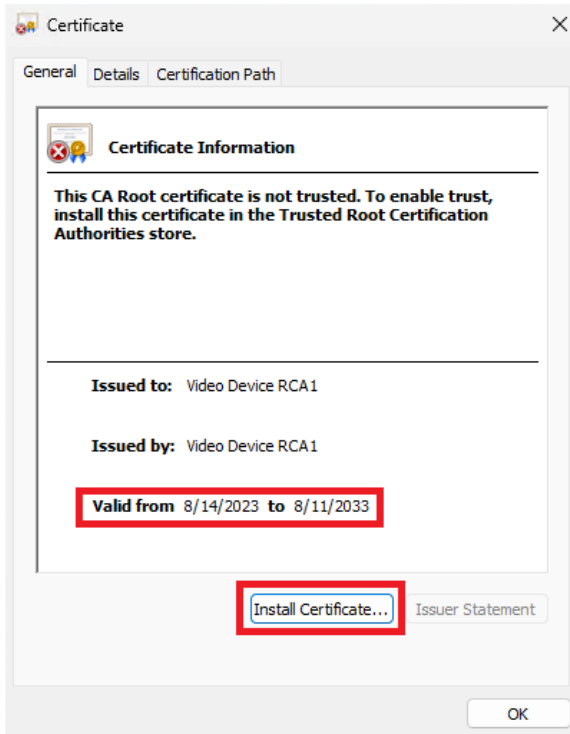
The CA certificate is named as "cacert.crt".



2. Import the CA certificate into PC's system

On Windows PC, double-click on the "cacert.crt" file to start installation. You can see the certificate valid period is 10 years, from 8/14/2023 to 8/11/2023.

Click on "Install Certificate..." to import the certificate.



Select **“Local Machine”** in the import wizard, then click on **“Next”**.

← Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

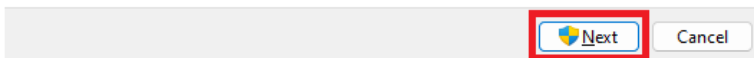
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

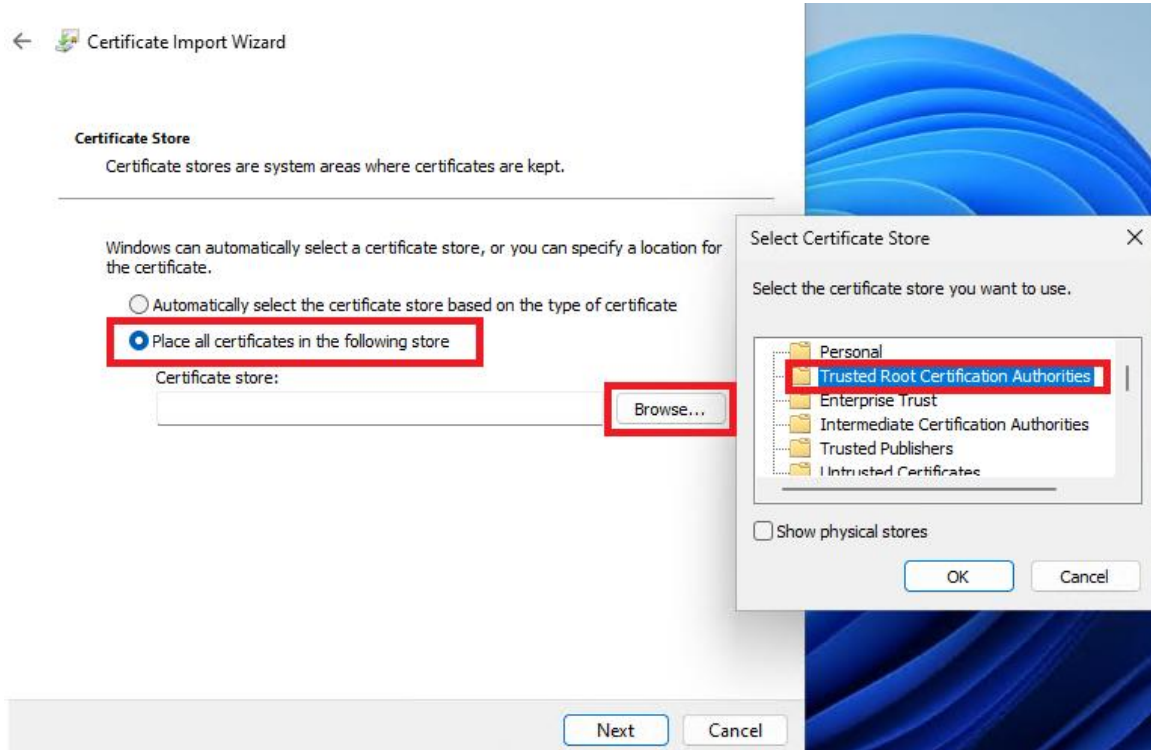
Current User

Local Machine

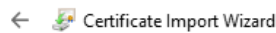
To continue, click Next.



Select **"Place all certificates in the following store"**, then click on **"Browse..."** and select **"Trusted Root Certification Authorities"**, then check on **OK** and go to **"Next"** step.



Click on **"Finish"** to finish the certificate installation.

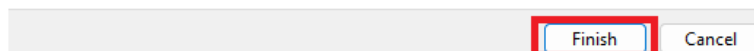


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Content
Trusted Root Certification Authorities	Certificate

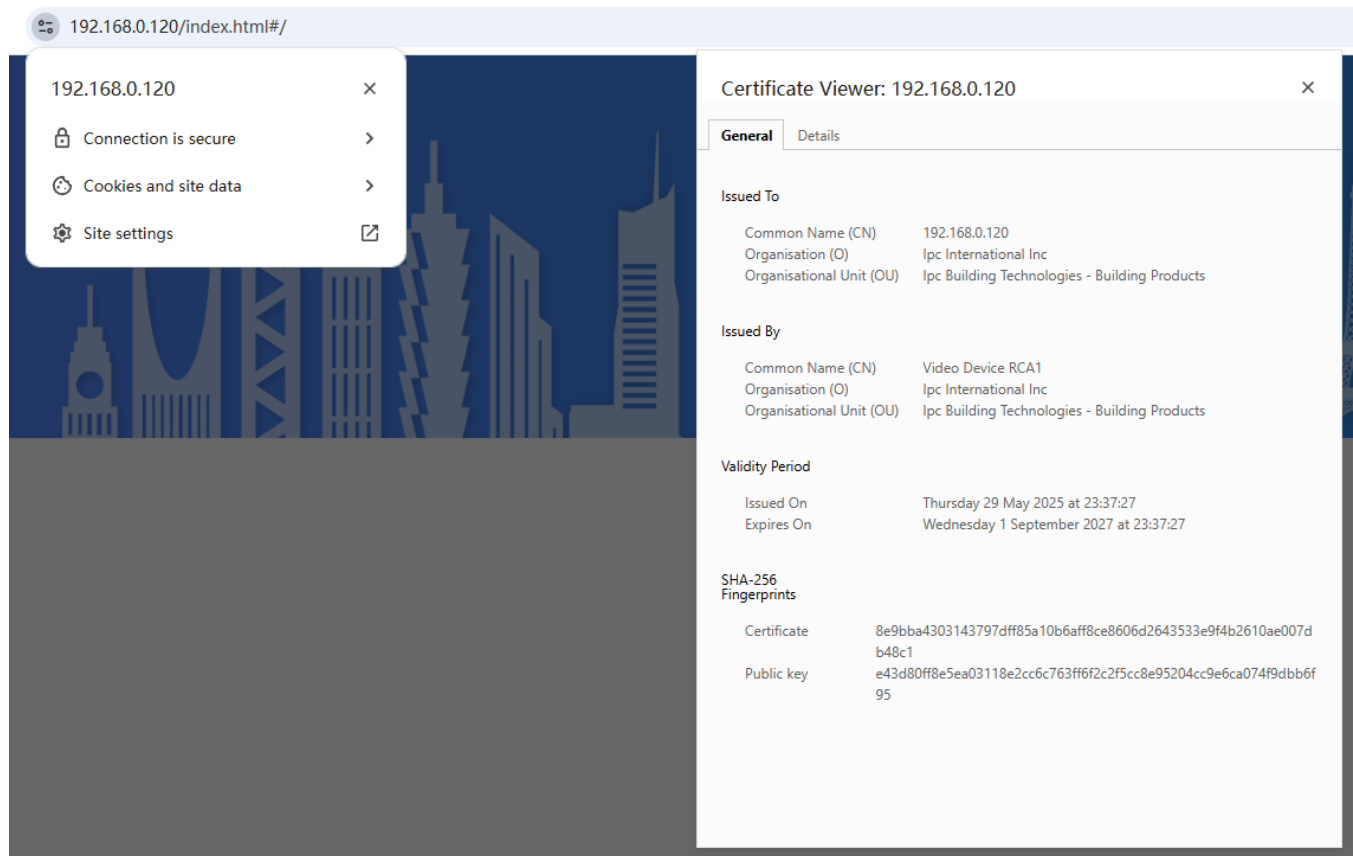


3. Check the device time

Make sure that the device time is within the certificate valid period.

4. Reboot device

If device IP is changed, then please reboot the device so the browser will show "secure" connection.



Q1: After changing the device IP, why the browser shows "Not secure" HTTPS connection?

A1: The firmware has a root CA and root CA private key. By default, every time when the device starts up, it will use the root CA and private key to generate a server certificate and server private key according to the current device IP. After changing the device IP, the server certificate IP doesn't match with device, then browser will regard it as invalid certificate, so the connection will show "Not secure". Reboot the device so that it can generate server certificate and server private key again according to the new IP, then the connection will show "secure" again.

Q2: After importing firmware built-in CA certificate into PC system, why the browser still shows "Not secure"?

A2: If you uploaded your own server certificate and server private key into the device, then it will use your certificate, since your certificate is not signed by the device built-in CA, the verification failed therefore the connection is "Not secure".

You can import the root CA which was used to generate your certificate into PC system, then the connection will be "secure".

Solution 2: Use self-signed CA certificate

1. **Create self-signed CA certificate**

Install OpenSSL on a Linux virtual machine, then use the commands in steps below to create a self-signed CA certificate.

Step 1: Generate root CA private key

Example command: `openssl genrsa -out rootCA.key 2048`

("rootCA.key" is the private key name, you can define by yourself)

Step 2: Use the root CA private key to generate root CA request.

Example Command: `openssl req -new -key rootCA.key -out rootCA.csr -subj`

`"/C=CN/ST=GD/L=SZ/O=SNL/OU=TECH/CN= ipc.security.com"`

("rootCA.csr" is root CA request file name, /C=country code, /ST=province code, /L=city code, /O=organization code, /OU=department code, /CN=Common name, it can be IP or domain or org name)

Step 3: Use root CA request and root CA private key to generate root CA.

Example command: `openssl x509 -req -days 365 -in rootCA.csr -signkey rootCA.key -out rootCA.crt` (365 means this CA's validate period is 365 days)

```
root@HannioPC:/home/hannio/HttpsTest# ls
root@HannioPC:/home/hannio/HttpsTest# openssl genrsa -out rootCA.key 2048
root@HannioPC:/home/hannio/HttpsTest#
root@HannioPC:/home/hannio/HttpsTest# openssl req -new -key rootCA.key -out rootCA.csr -subj "/C=CN/ST=GD/L=SZ/O=SNL/OU=TECH/CN=
ipc.security.com"
root@HannioPC:/home/hannio/HttpsTest#
root@HannioPC:/home/hannio/HttpsTest# openssl x509 -req -days 365 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
Certificate request self-signature ok
subject=C = CN, ST = GD, L = SZ, O = SNL, OU = TECH, CN = ipc.security.com
root@HannioPC:/home/hannio/HttpsTest#
root@HannioPC:/home/hannio/HttpsTest# ls
rootCA.crt  rootCA.csr  rootCA.key
root@HannioPC:/home/hannio/HttpsTest#
```

2. **Generate server private key and server certificate.**

Step 1: Generate server private key

Example command: `openssl genrsa -out server.key 2048`

Step 2: Use server private key to generate server certificate request.

Example command: `openssl req -new -key server.key -out server.csr -subj "/C=CN/ST=GD/L=SZ/O=SNL/OU=TECH/CN=192.168.1.120" -addext "subjectAltName=IP:192.168.1.120"`

(The server certificate will be uploaded the device side, the `subjectAltName` should be device IP or domain, or both, for example: `"subjectAltName=DNS:ipc.support.com,IP:192.168.1.120"`)

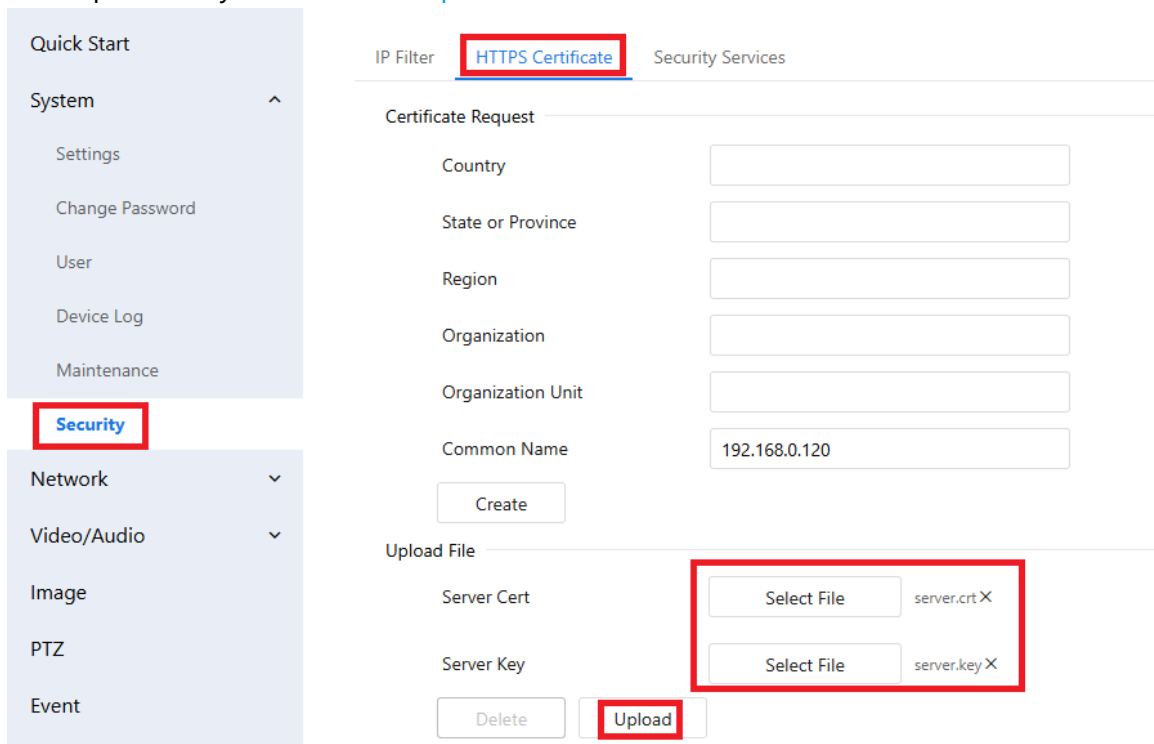
Step 3: Use root CA, root CA private key, server certificate request to generate server certificate.

Example command: `openssl x509 -req -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -sha256 -extfile <(echo "subjectAltName=IP:192.168.1.120")`

```
root@HannioPC:/home/hannio/HttpsTest# openssl genrsa -out server.key 2048
root@HannioPC:/home/hannio/HttpsTest# openssl req -new -key server.key -out server.csr -subj "/C=CN/ST=GD/L=SZ/O=SNL/OU=TECH/CN=192.168.1.120" -addext "subjectAltName=IP:192.168.1.120"
root@HannioPC:/home/hannio/HttpsTest# openssl x509 -req -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -sha256 -extfile <(echo "subjectAltName=IP:192.168.1.120")
Certificate request self-signature ok
subject=C = CN, ST = GD, L = SZ, O = SNL, OU = TECH, CN = 192.168.1.120
root@HannioPC:/home/hannio/HttpsTest# ls
rootCA.crt rootCA.csr rootCA.key rootCA.srl server.crt server.csr server.key
root@HannioPC:/home/hannio/HttpsTest#
```

3. Upload server certificate and server private key into device

Go to [Setting](#) -> [System](#) -> [Security](#) -> [HTTPS Certificate](#). Select your server certificate and server private key, then click on [Upload](#).

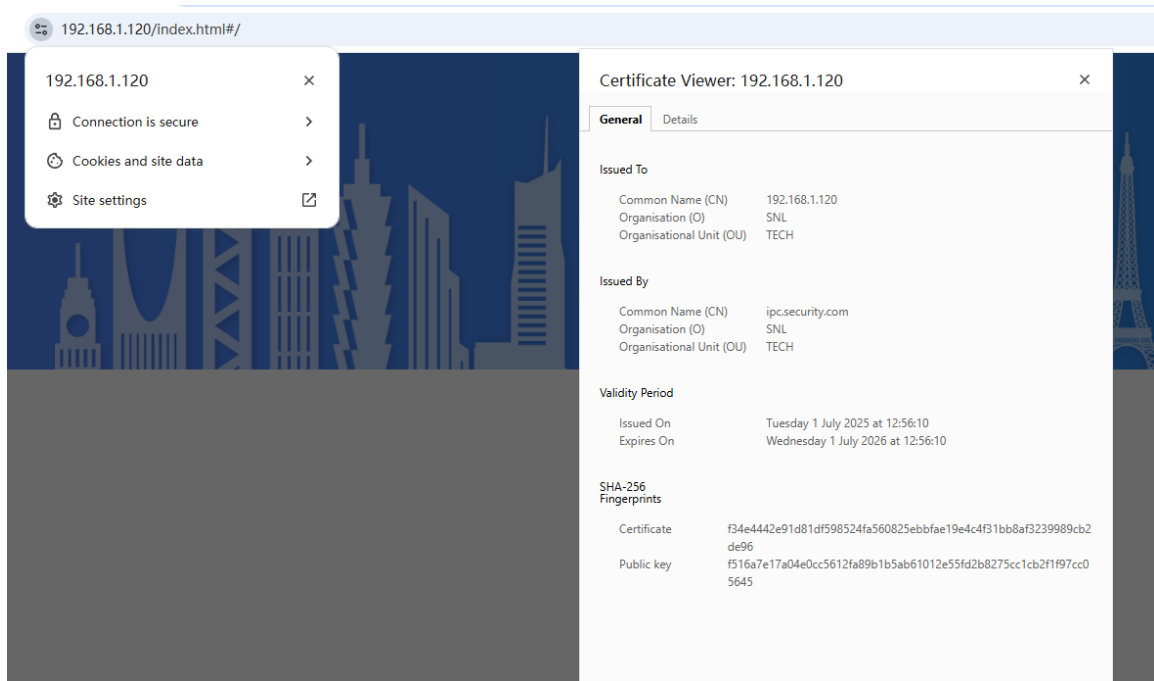


4. Import the self-signed CA certificate into PC's system

Refer to [Import the CA certificate into PC's system] in Solution 1 to import the self-signed CA certificate.

5. Change device IP and synchronize device time

The device IP should be aligned with the IP address inside the certificate. If not, please change your device IP. The device time should be within the server certificate valid period. If not, please change your device time.



Solution 3: Use public CA certificate

There are lots of public Certificate Authorities, like DigiCert, Sectigo, GlobalSign, etc. Those public Certificate Authorities are trusted by the popular operation systems and browsers, so they will embed their root CA certificates.

If a server is using a server certificate signed by the public Certificate Authority, then root CA doesn't need to be manually imported into system.

1. Input the certificate request information and then click on [Create](#) to generate certificate request. (The Common Name should be the device IP address/domain)

The screenshot shows the 'IP Camera' web interface. The top navigation bar includes 'Live View', 'Playback', 'IVS', and 'Setting'. The left sidebar contains 'Quick Start', 'System' (with sub-items: Settings, Change Password, User, Device Log, Maintenance), 'Security' (with sub-items: Network, Video/Audio, Image, PTZ, Event), and 'Maintenance'. The main content area is titled 'HTTPS Certificate' and contains a 'Certificate Request' form. The form fields are: Country (CN), State or Province (GD), Region (SZ), Organization (SNL), Organization Unit (TECH), and Common Name (MyCamera). A red box highlights the 'Create' button below the form. Below the form is an 'Upload File' section with 'Server Cert' and 'Server Key' fields, each with a 'Select File' button and 'No file Chosen' text. At the bottom of the 'Upload File' section are 'Delete' and 'Upload' buttons.

- Click on **Export** to download the certificate request file. The file is named as "certreq.pem" by default.

IP Filter **HTTPS Certificate** Security Services

Certificate Request

Country	<input type="text" value="CN"/>
State or Province	<input type="text" value="GD"/>
Region	<input type="text" value="SZ"/>
Organization	<input type="text" value="SNL"/>
Organization Unit	<input type="text" value="TECH"/>
Common Name	<input type="text" value="MyCamera"/>

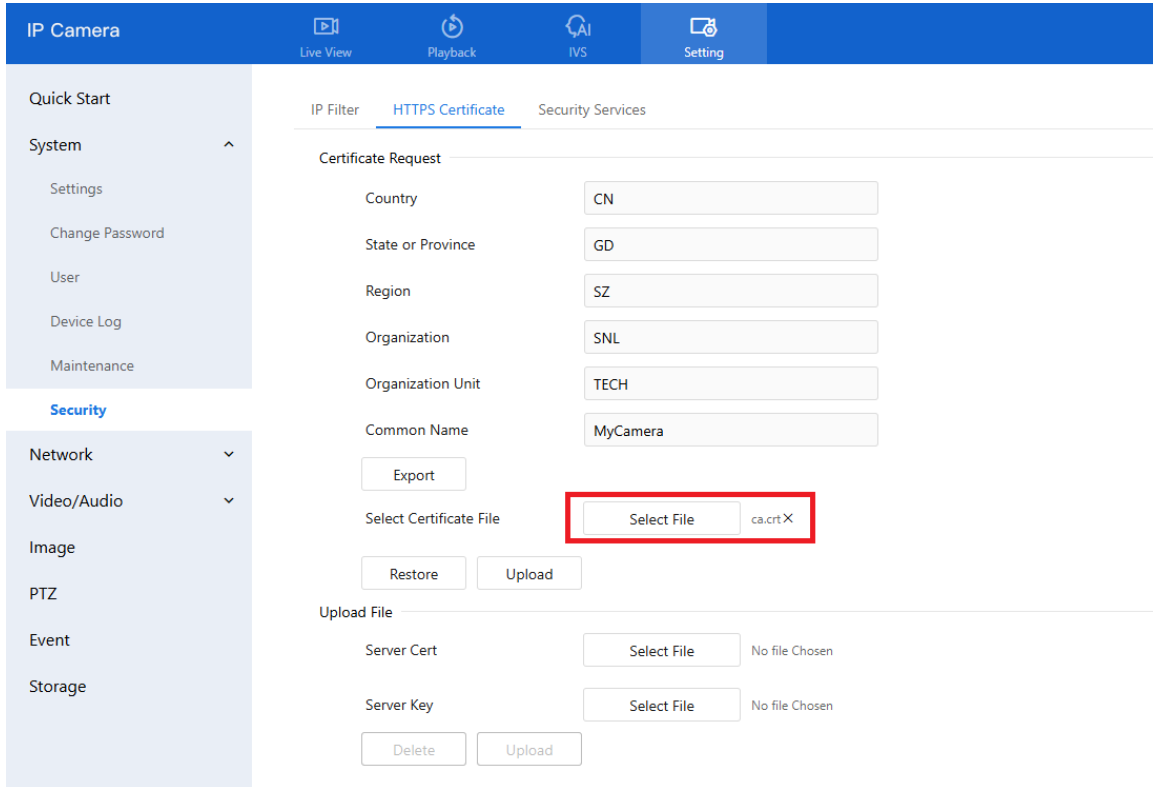
Export

Select Certificate File No file Chosen

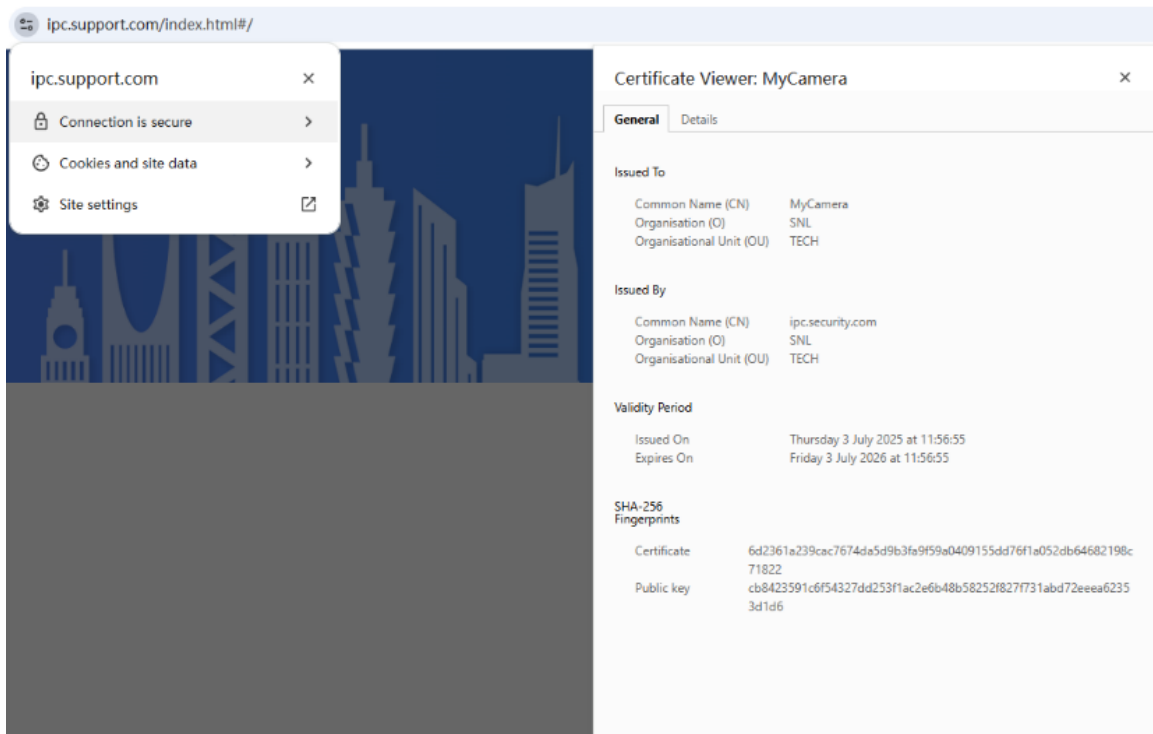
- Send the certificate request file "certreq.pem" to a public Certificate Authority to generate/sign a server certificate.

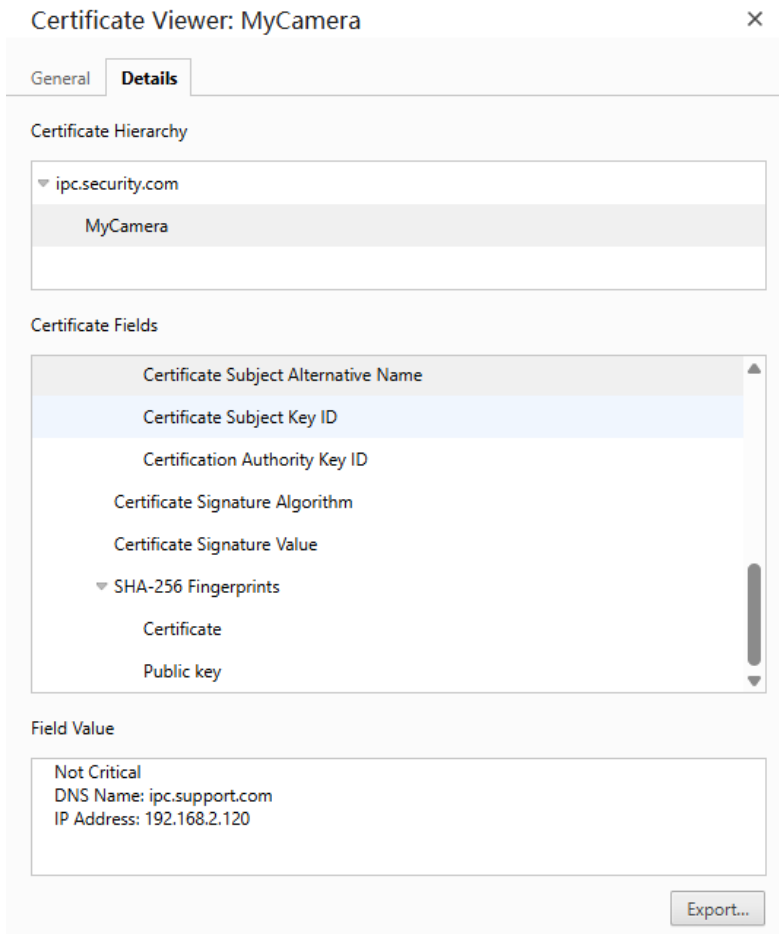
Note: When Certificate Authority sign the server certificate, the server certificate must contain subjectAltName (for example: "subjectAltName=DNS:ipc.support.com,IP:192.168.2.120") and the IP/Domain must be the same with device IP/Domain.

4. Select the server certificate signed by public Certificate Authority, then click on "Upload" to upload it to device.



5. Re-open the browser and access device via HTTPS, the connection will show "secure".





Q3: *Certificate Authority provides server certificate according to my CSR (certificate request file), can I upload the same certificate file to other devices?*

A3: No. The server certificate is generated through a CSR, and the CSR is generated through the server private key. When you create CSR (certreq.pem) on device, it will create a private key first. Each time the device will create a different private key and store inside, so your server certificate and devices private key is a pair.

If you restore the device, the previous private key will be deleted from it, next time the device will generate a new private key, therefore the old server certificate generated through the old CSR will not be valid any more.

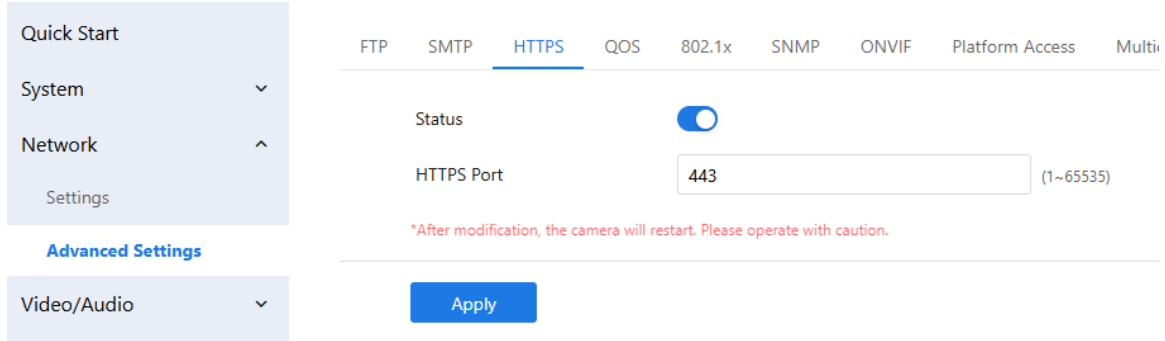
Q4: *How to upload Certificate Authority's certificate to different devices?*

A4: If you want to apply for server certificate from Certificate Authority and upload the same certificate into different devices, then Don't use device to create CSR, but create CSR and save the private key by yourself, or you can ask Certificate Authority to create both server certificate and server private key for you, then upload both files into the device.

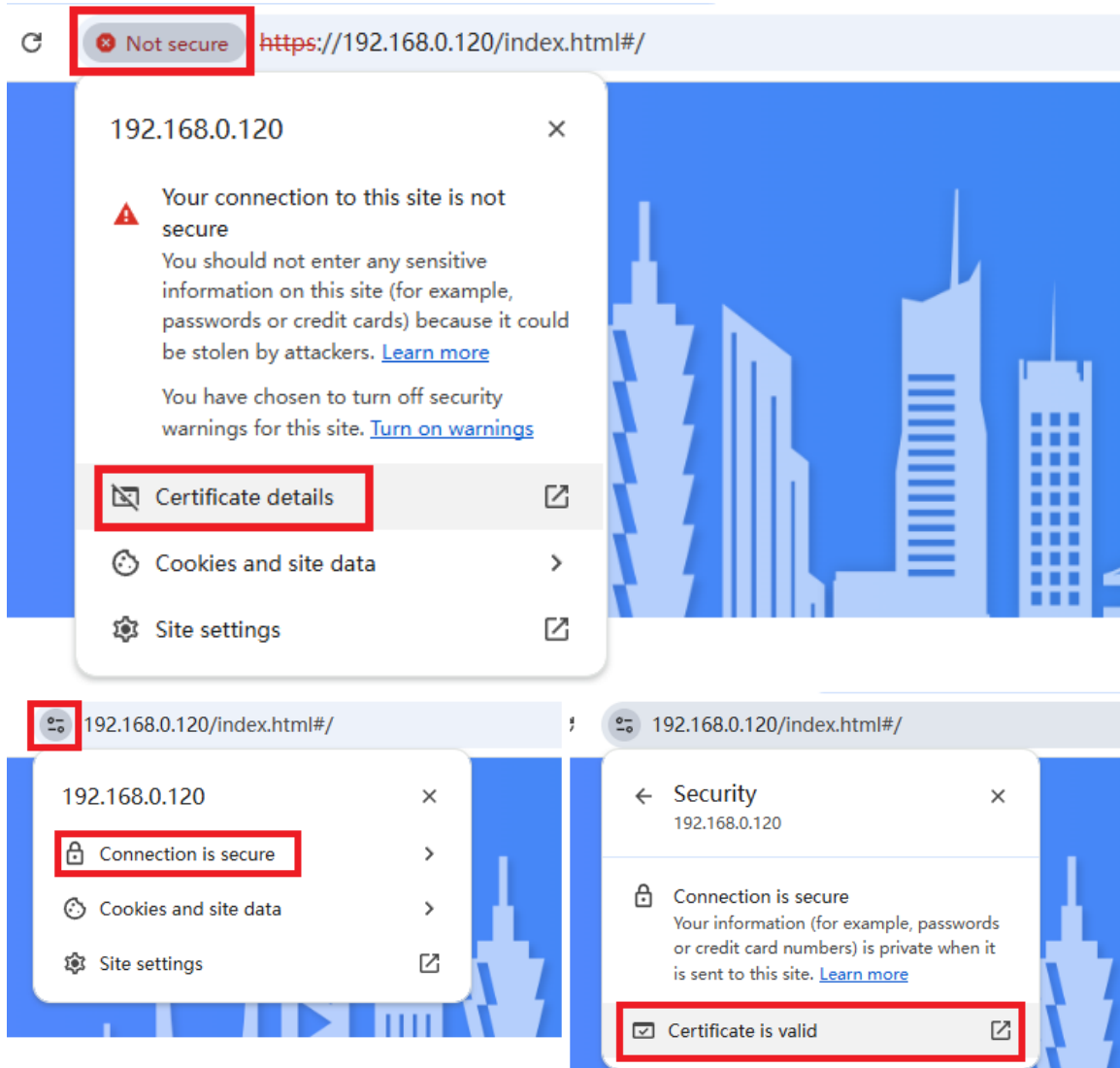
Q5: How to check the server certificate information on device?

A5: See steps below.

Step 1. Enable HTTPS mode, then access the device web page by HTTPS.



Step 2. Click on browser's "Not secure" or "Secure" icon, then click on "Certificate details" to check the current certificate details.



Step 3. Server certificate valid period can be found under "General"

Certificate Viewer: 192.168.0.120

General Details

Issued To

Common Name (CN)	192.168.0.120
Organisation (O)	Ipc International Inc
Organisational Unit (OU)	Ipc Building Technologies - Building Products

Issued By

Common Name (CN)	Video Device RCA1
Organisation (O)	Ipc International Inc
Organisational Unit (OU)	Ipc Building Technologies - Building Products

Validity Period

Issued On	Thursday 29 May 2025 at 23:33:51
Expires On	Wednesday 1 September 2027 at 23:33:51

SHA-256 Fingerprints

Certificate	c769a0b836edd032d3c9931406950aaeaa996a03125bc89406a5b042c736b203
Public key	16f1a9c9b59028455fa6aacbdbdbd09afb8c9a4c2ce53c37a9a5de6d28ced4

You can find the server/device IP assigned to this server certificate.

Note: Device IP address must align with this server certificate IP, otherwise browser will not trust this server certificate and the HTTPS connection will show "Not secure".

Certificate Viewer: 192.168.1.120

General Details

Certificate Hierarchy

- ipc.security.com
 - 192.168.1.120

Certificate Fields

- Subject
 - Subject Public Key Info
- Extensions
 - Certificate Subject Alternative Name
 - Certificate Subject Key ID
 - Certification Authority Key ID
 - Certificate Signature Algorithm
 - Certificate Signature Value

Field Value

Not Critical
IP Address: 192.168.1.120

Export...