linkingvision

HTTPS certificate based on IP address

White paper

Version records

Version	Date	Describe

Content

1.0 Background Introduction **5**

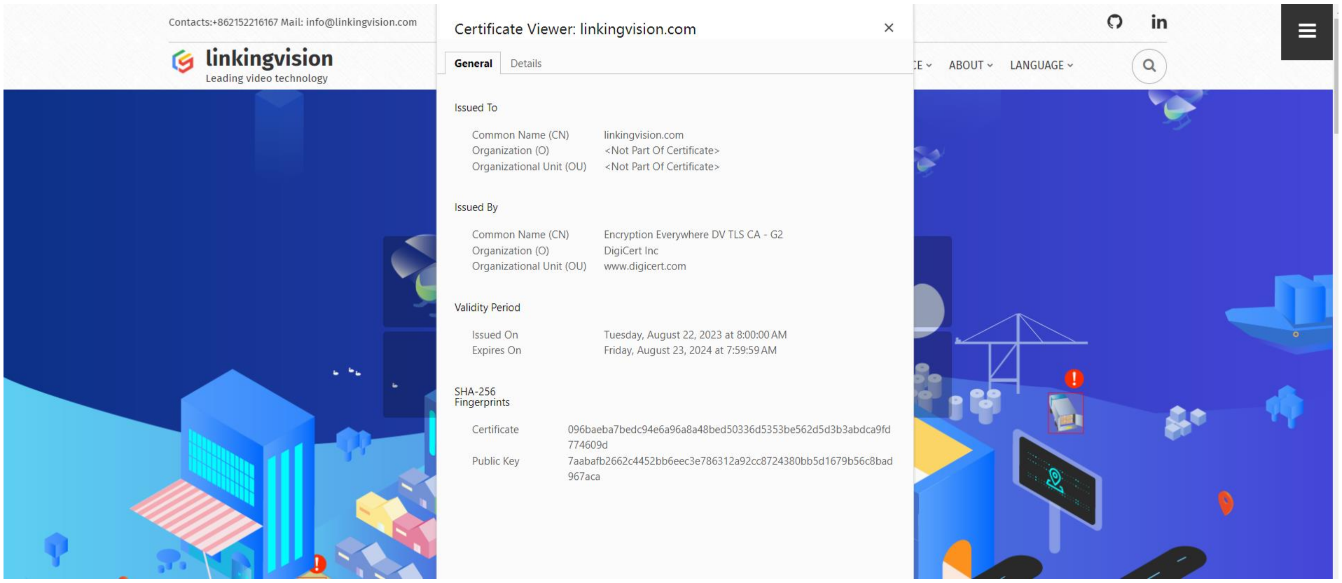
2.0 Configuration method **6**

2.1 Server configuration 7

2.2 Configuration of the machine where the browser is located 9

1.0 Background Introduction

If you want to let the browser trust a HTTPS service (hereinafter referred to as the service), the service must use a certificate that is o n the browser's trusted certificate chain. Generally, certificates need to be purchased and bound to a domain name, similar to the following image：



Certificate Viewer: linkingvision.com

General | Details

Issued To

Common Name (CN) linkingvision.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) Encryption Everywhere DV TLS CA - G2
Organization (O) DigiCert Inc
Organizational Unit (OU) www.digicert.com

Validity Period

Issued On Tuesday, August 22, 2023 at 8:00:00 AM
Expires On Friday, August 23, 2024 at 7:59:59 AM

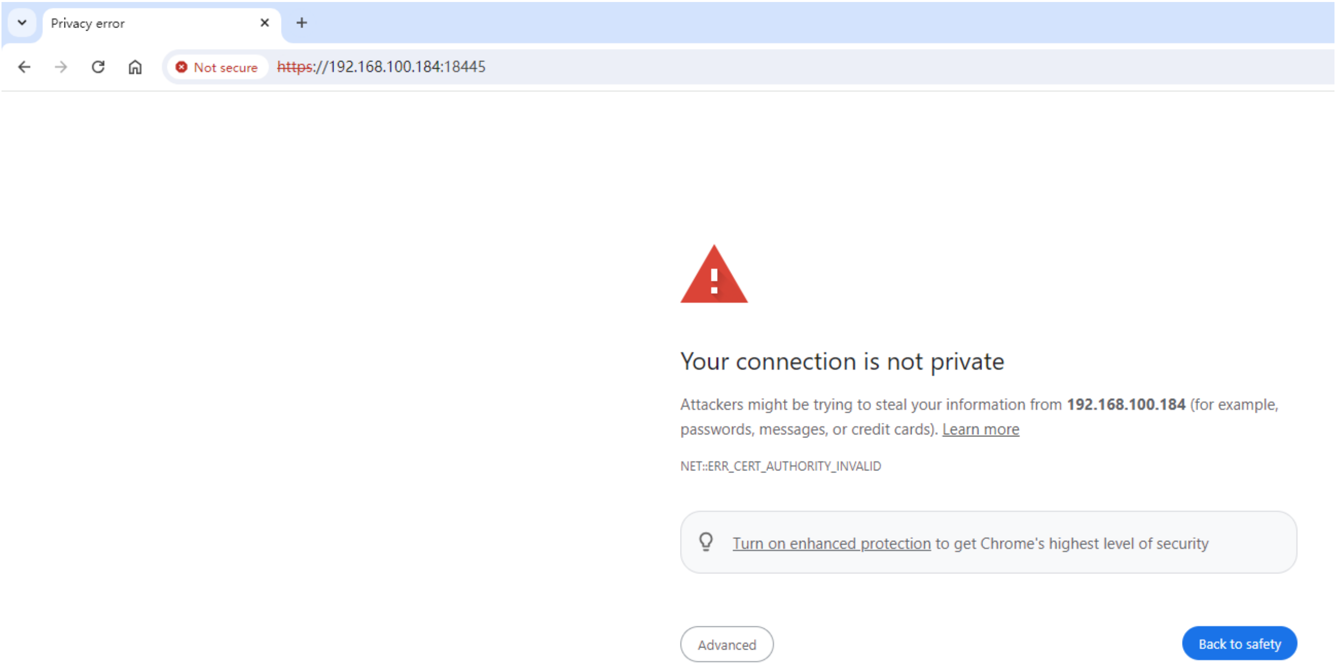
SHA-256 Fingerprints

Certificate 096baeba7bedc94e6a96a8a48bed50336d5353be562d5d3b3abdca9fd774609d
Public Key 7aabafb2662c4452bb6eec3e786312a92cc8724380bb5d1679b56c8bad967aca

But if the service is on the intranet and cannot use a domain name, can the browser trust the service based on the IP address? The answer is yes, but it requires all the computers where the browser is located to manually import the root certificate. All clients use a single root certificate, which is easier to distribute. Taking Chrome as an example, if there are multiple services, only the certificate needs to be generated on each server, and the root certificate remains unchanged.

2.0 Configuration method

If you want to access the service before configuration, you need to manually trust it, as shown in the following figure：



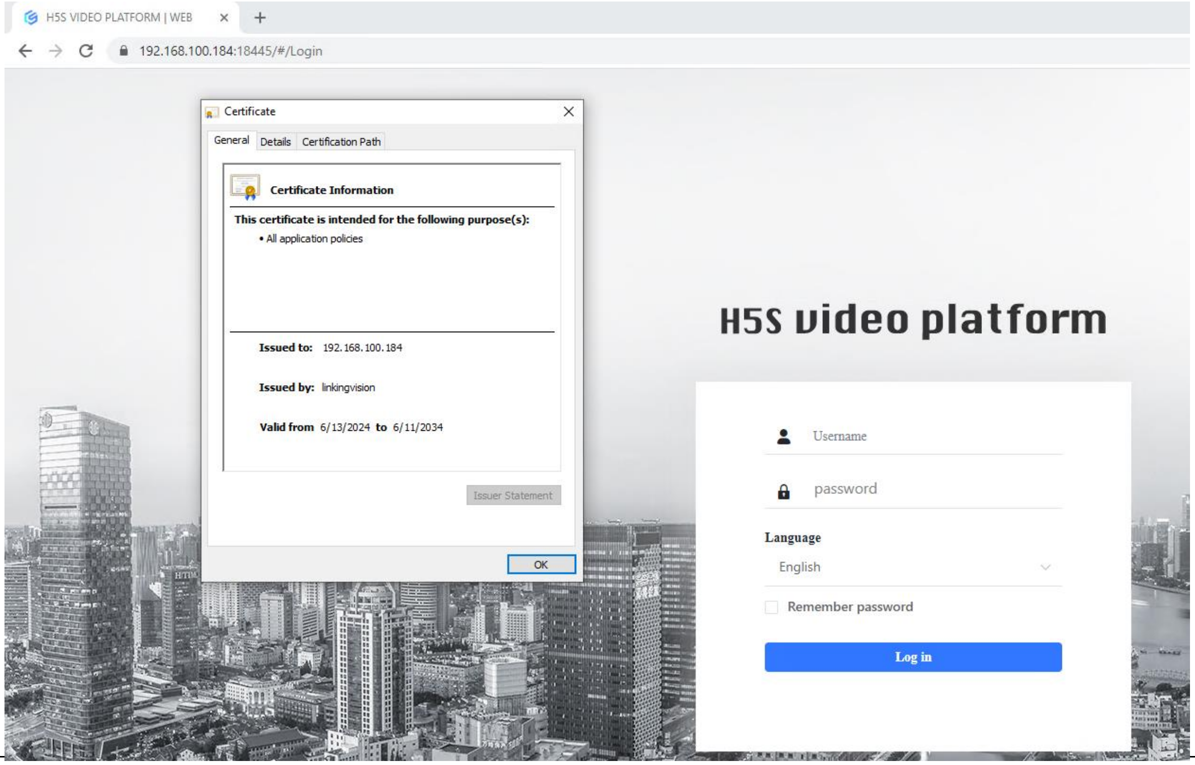
Your connection is not private

Attackers might be trying to steal your information from **192.168.100.184** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

After configuration, if you access the service, it has become a trusted service, as shown in the following figure：



Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: 192.168.100.184

Issued by: linkingvision

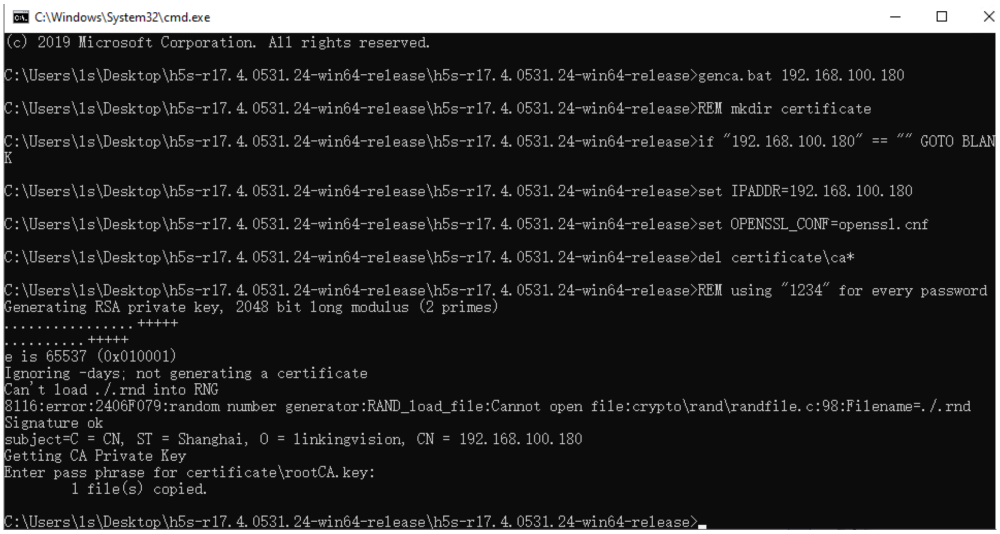
Valid from 6/13/2024 **to** 6/11/2034

2.1 Server configuration

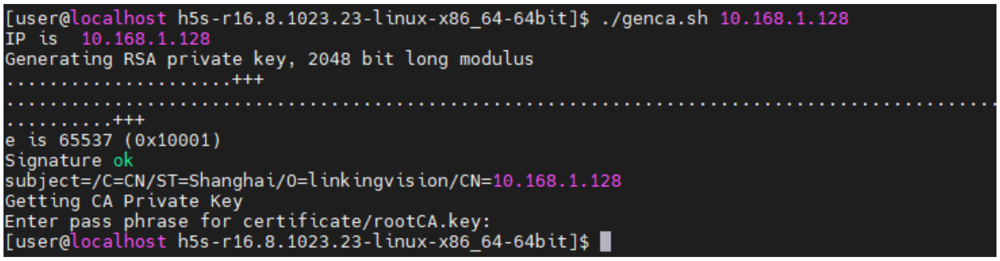
2.1.1 Generate certificate

Assuming the service IP address is 10.168.1.128, when entering the service root directory, Windows needs to open cmd.exe.

Execute genca.bat 10.168.1.128 (Linux is ./genca.sh) and refer to the following figure. Enter the password 1234：



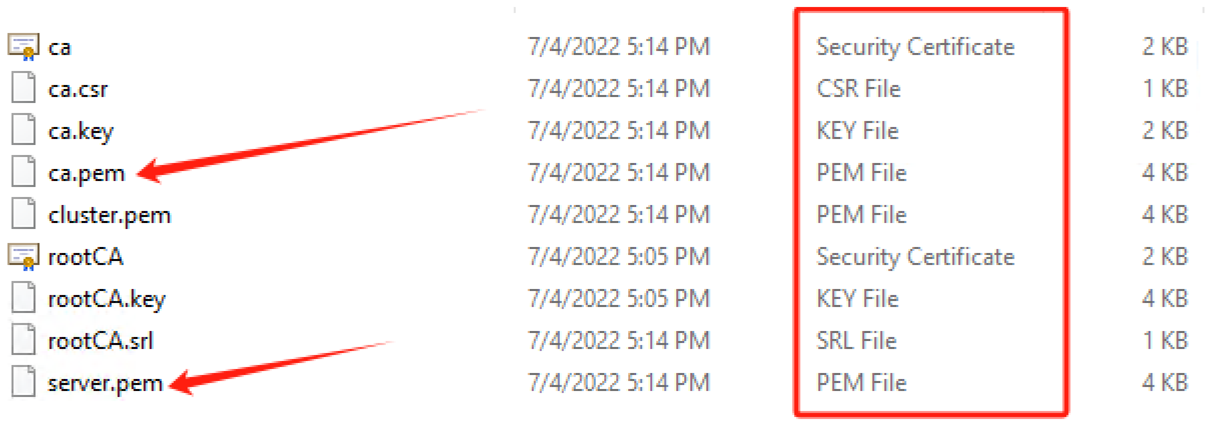
```
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>genca.bat 192.168.100.180

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>REM mkdir certificate

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>if "192.168.100.180" == "" GOTO BLAN
K

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>set IPADDR=192.168.100.180

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>set OPENSSL_CONF=openssl.cnf

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>del certificate\ca*

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>REM using "1234" for every password
Generating RSA private key, 2048 bit long modulus (2 primes)
................+++++
..........+++++
e is 65537 (0x010001)
Ignoring -days; not generating a certificate
Can't load ./.rnd into RNG
8116:error:2406F079:random number generator:RAND_load_file:Cannot open file:crypto\rand\randfile.c:98:Filename=./.rnd
Signature ok
subject=C = CN, ST = Shanghai, O = linkingvision, CN = 192.168.100.180
Getting CA Private Key
Enter pass phrase for certificate\rootCA.key:
        1 file(s) copied.

C:\Users\ls\Desktop\h5s-r17.4.0531.24-win64-release\h5s-r17.4.0531.24-win64-release>
```



```
[user@localhost h5s-r16.8.1023.23-linux-x86_64-64bit]$ ./genca.sh 10.168.1.128
IP is  10.168.1.128
Generating RSA private key, 2048 bit long modulus
.....................+++
..............................................................................................
..........+++
e is 65537 (0x10001)
Signature ok
subject=/C=CN/ST=Shanghai/O=linkingvision/CN=10.168.1.128
Getting CA Private Key
Enter pass phrase for certificate/rootCA.key:
[user@localhost h5s-r16.8.1023.23-linux-x86_64-64bit]$
```

2.1.2 Application certificate

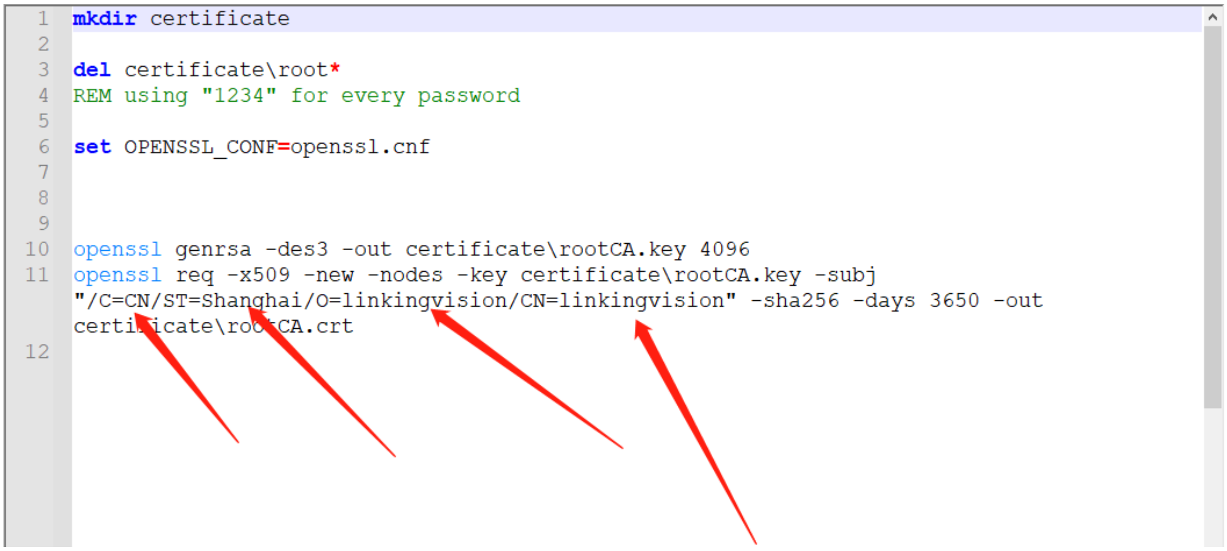
The new certificate generated in the previous step is under the certificate folder, with the file name ca.pem. The file structure is the same on Linux and Windows, as shown in the following figure：



ca	7/4/2022 5:14 PM	Security Certificate	2 KB
ca.csr	7/4/2022 5:14 PM	CSR File	1 KB
ca.key	7/4/2022 5:14 PM	KEY File	2 KB
ca.pem	7/4/2022 5:14 PM	PEM File	4 KB
cluster.pem	7/4/2022 5:14 PM	PEM File	4 KB
rootCA	7/4/2022 5:05 PM	Security Certificate	2 KB
rootCA.key	7/4/2022 5:05 PM	KEY File	4 KB
rootCA.srl	7/4/2022 5:14 PM	SRL File	1 KB
server.pem	7/4/2022 5:14 PM	PEM File	4 KB

Then delete server.pem, rename ca.pem to server.pem, and restart the service. The new certificate will be applied after the service restarts.

At the same time, copy the rootCA.crt file and distribute it to the computers where Chrome needs to access the service. The root certificate is fixed. Multiple services can be applied. If you need to modify the root certificate information, you can modify genrootca.bat (genrootca.sh) and generate a new root certificate. It is recommended that all services share a root certificate in a project, which makes it easier to distribute the root certificate. If the root certificate changes, all service certificates need to be recreated because the service certificates are issued using the root certificate.

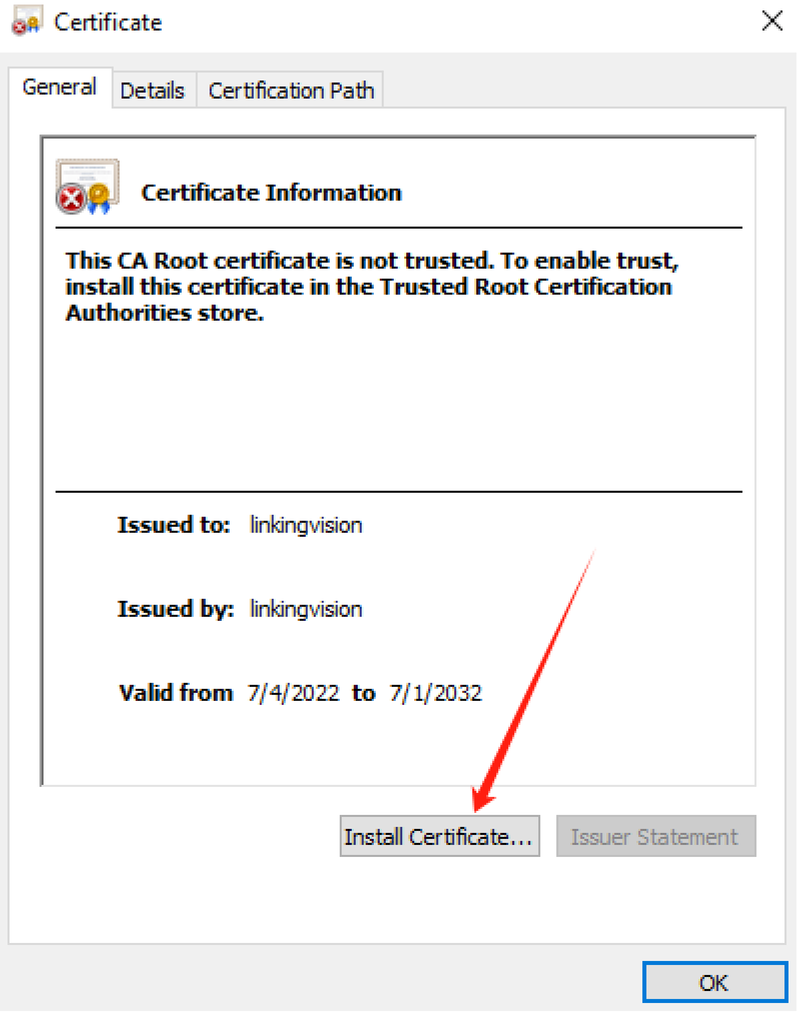


```
mkdir certificate

del certificate\root*
REM using "1234" for every password

set OPENSSL_CONF=openssl.cnf



openssl genrsa -des3 -out certificate\rootCA.key 4096
openssl req -x509 -new -nodes -key certificate\rootCA.key -subj "/C=CN/ST=Shanghai/O=linkingvision/CN=linkingvision" -sha256 -days 3650 -out certificate\rootCA.crt

```

2.2 Configuration of the machine where the browser is located

2.2.1 Import root certificate

Double-click rootCA.crt copied from the service to open it, and follow the screenshot below:



Certificate

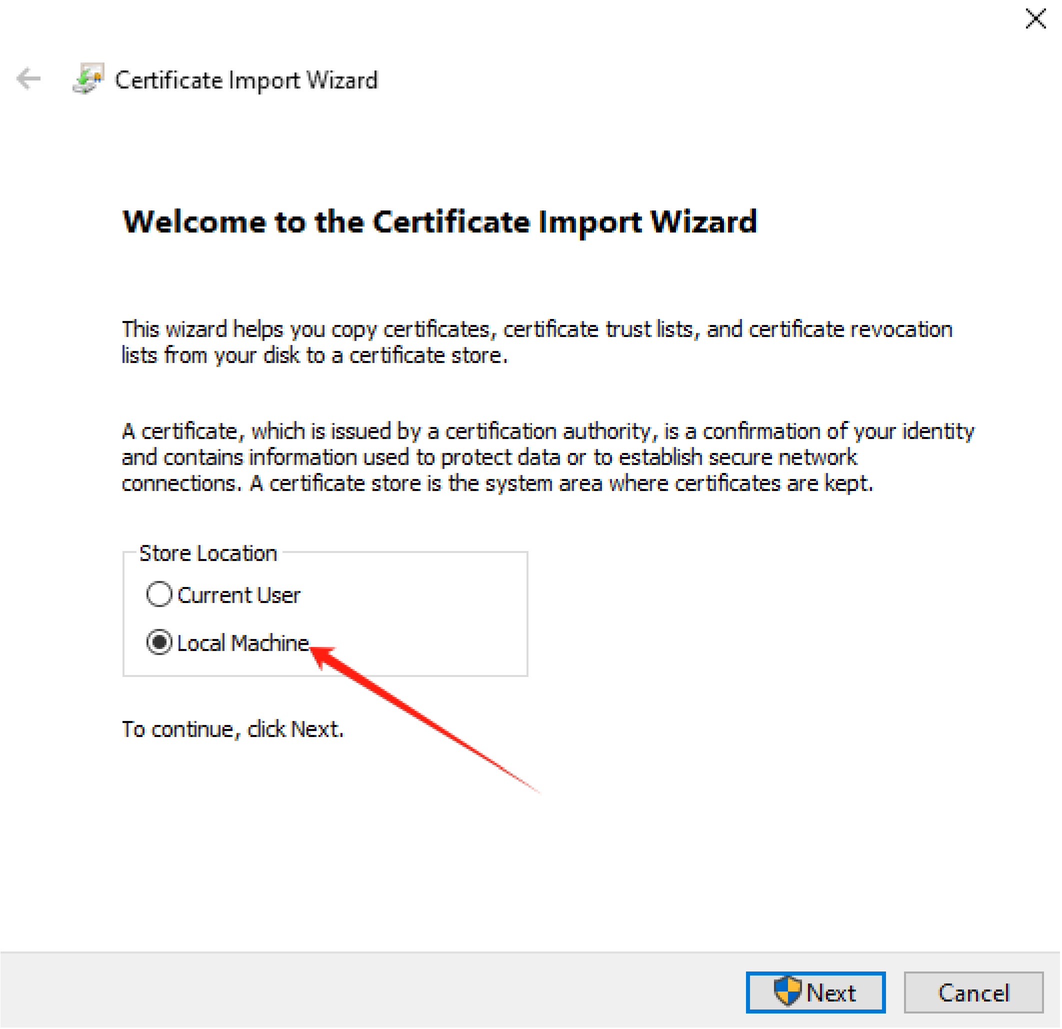
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: linkingvision

Issued by: linkingvision

Valid from 7/4/2022 **to** 7/1/2032



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.

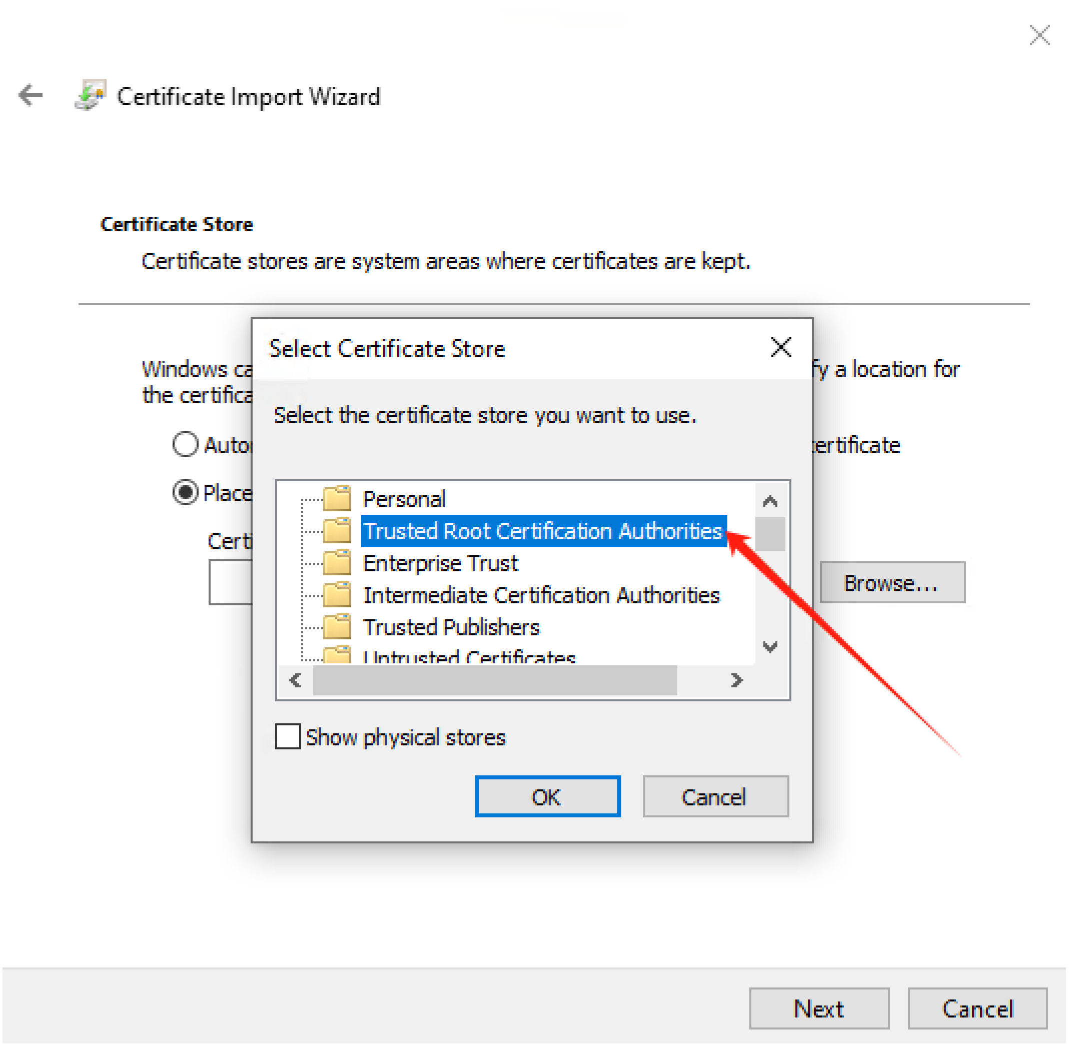
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

To continue, click Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows ca… …fy a location for the certifica…

○ Auto… …ertificate

● Place…

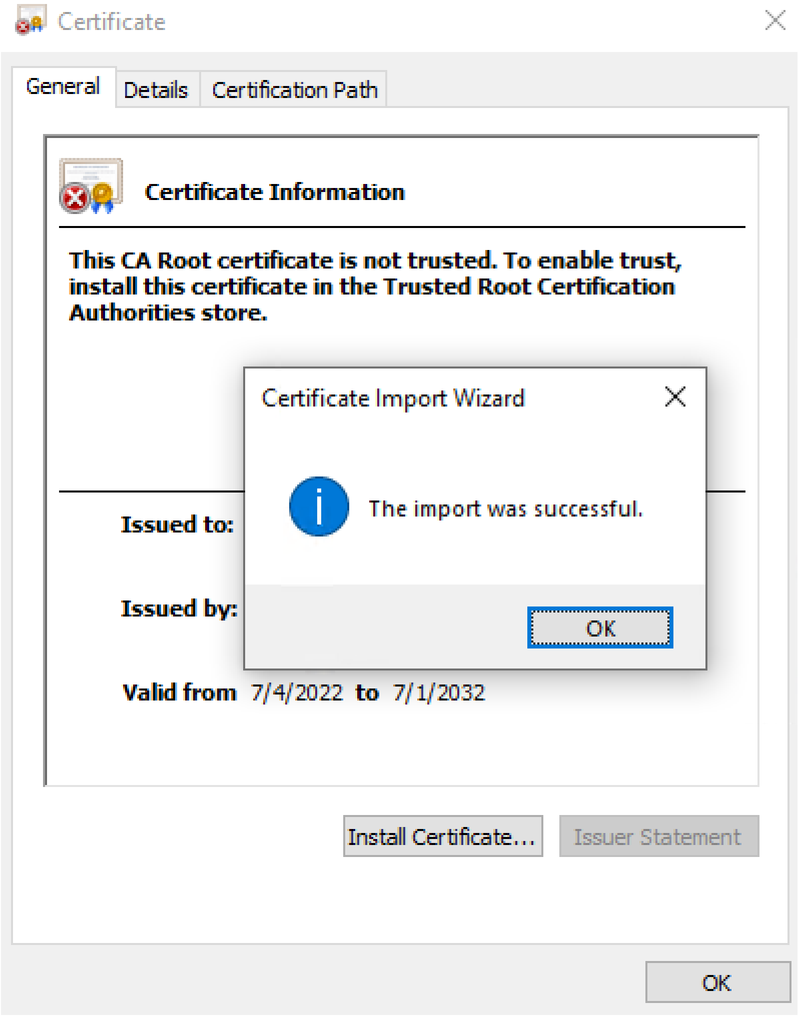
Certi…

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores



Certificate

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Certificate Import Wizard

The import was successful.

Valid from 7/4/2022 to 7/1/2032

Finally, it is displayed that the import is successful, and the service has become a trusted service after the import is successful.