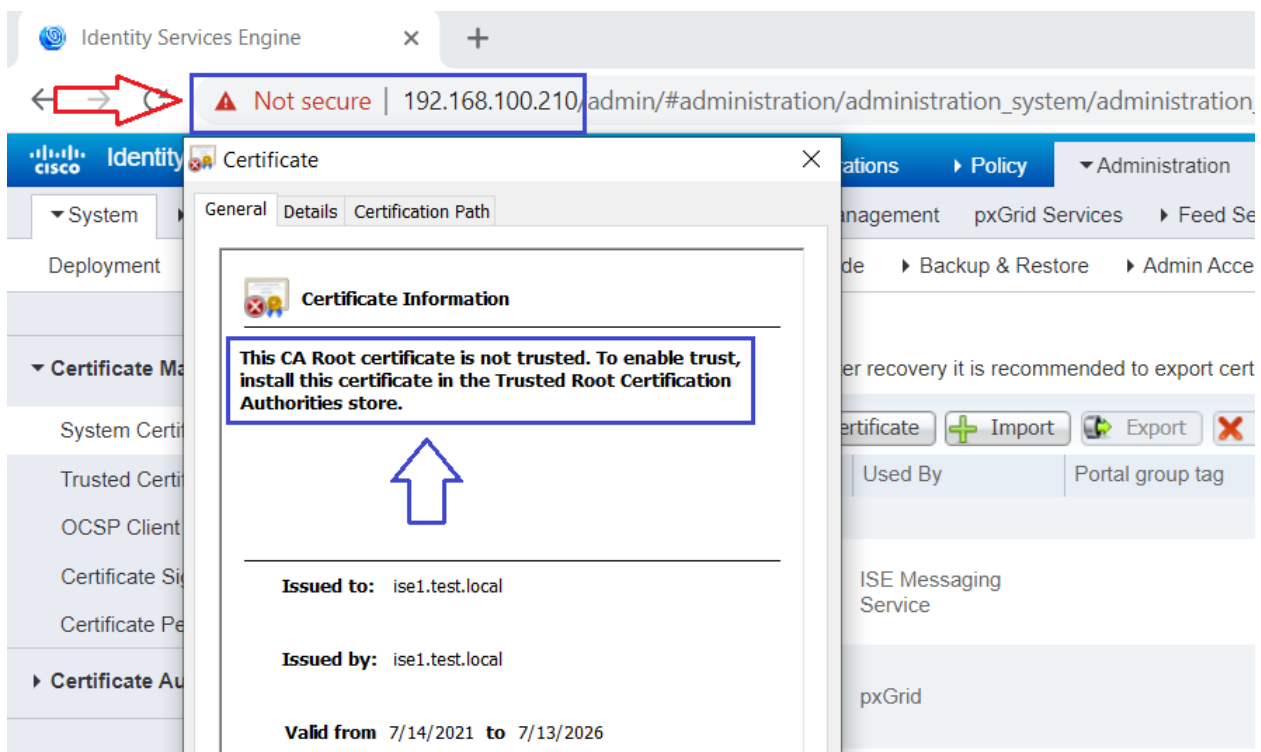
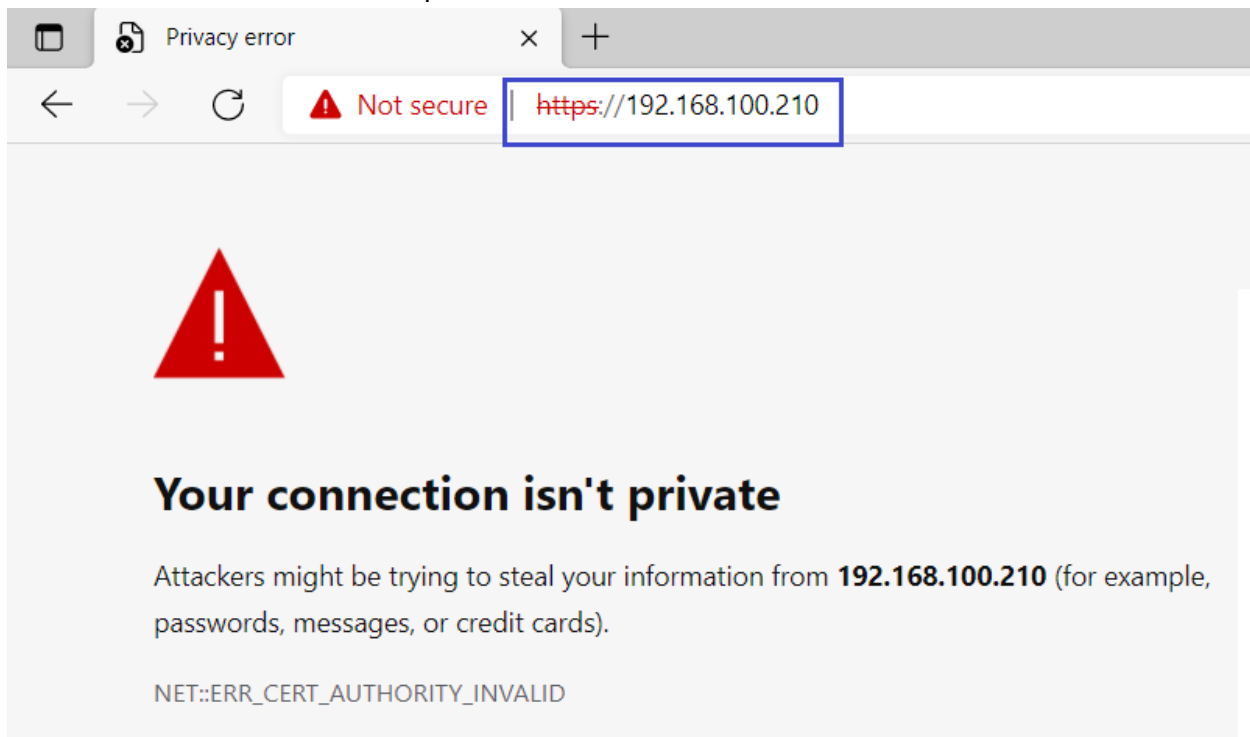


## Certificate Enrolment:

Before, certificate enrolment when you try to open Cisco ISE in browser it shows Certificate error that Your connection isn't private also in URL Not secure.



## Root CA:

Navigate to AD Certificate Services Web Enrollment page <https://192.168.100.230/certsrv> to download the CA certificate. click on **Download a CA certificate, certificate chain, or CRL** link:

Microsoft Active Directory Certificate Services – test-SRV-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#) 

On the next page, choose radio button for **Base 64** and click on **Download CA certificate** link. This will download the CA certificate locally to your Computer.

← → ↻ ⚠ Not secure | 192.168.100.230/certsrv/certcarc.asp

Microsoft Active Directory Certificate Services – test-SRV-CA

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).


To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

#### CA certificate:

Current [test-SRV-CA] ▲  
▼

#### Encoding method:

☐ DER

☒ Base 64 

[Install CA certificate](#)

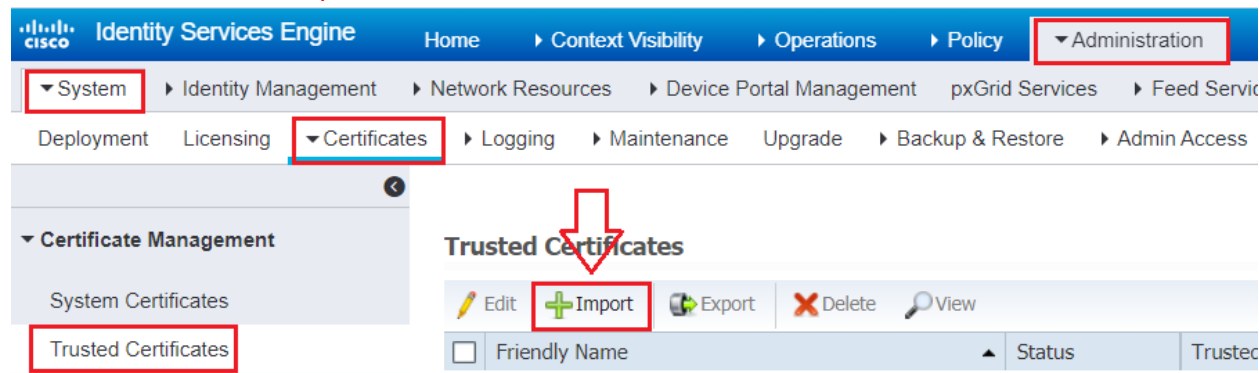
[Download CA certificate](#) 

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Go back to Cisco ISE and navigate to **Administration -> System -> Certificates -> Trusted Certificates** and click **Import**.



On next page, upload CA certificate that you just download. Give friendly name & description. Check the boxes next to:

**Trust for authentication within ISE:**

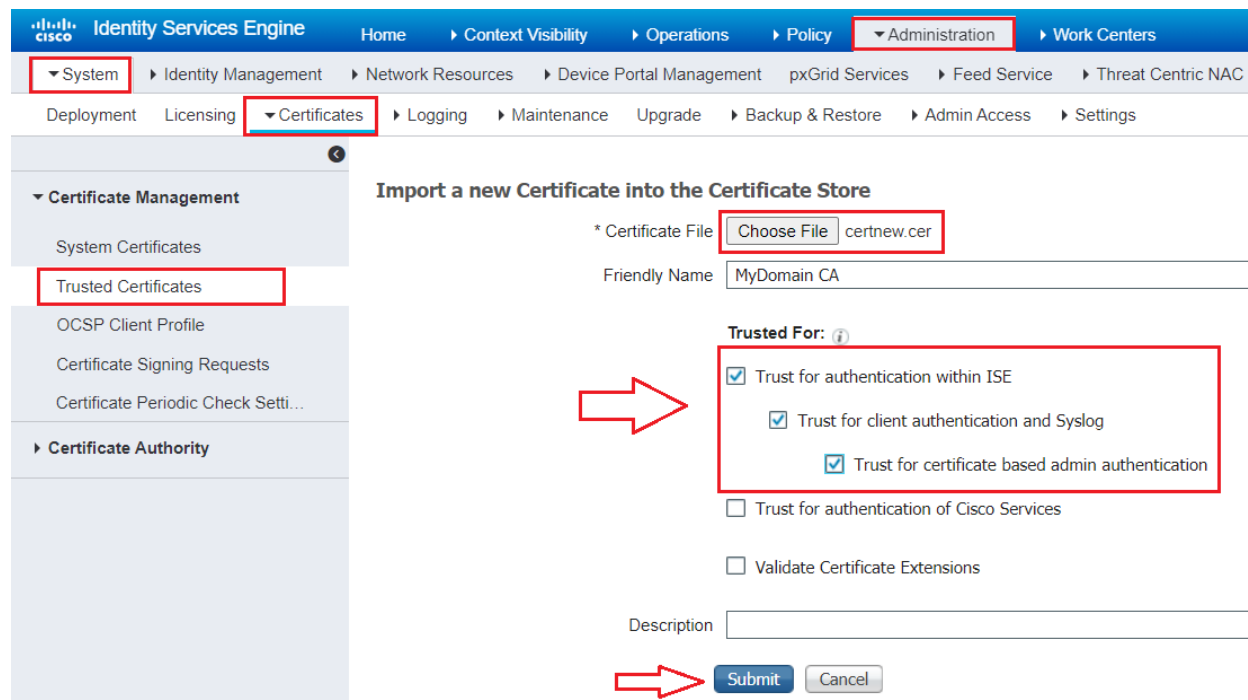
This will all you to add new ISE nodes as long as they have the same trusted CA certificate loaded to their Trusted Certificate store.

**Trust for client authentication and Syslog:**

You would check this box if you want to use this certificate to authenticate endpoints that connect to ISE using EAP and/or trust a Secure Syslog server

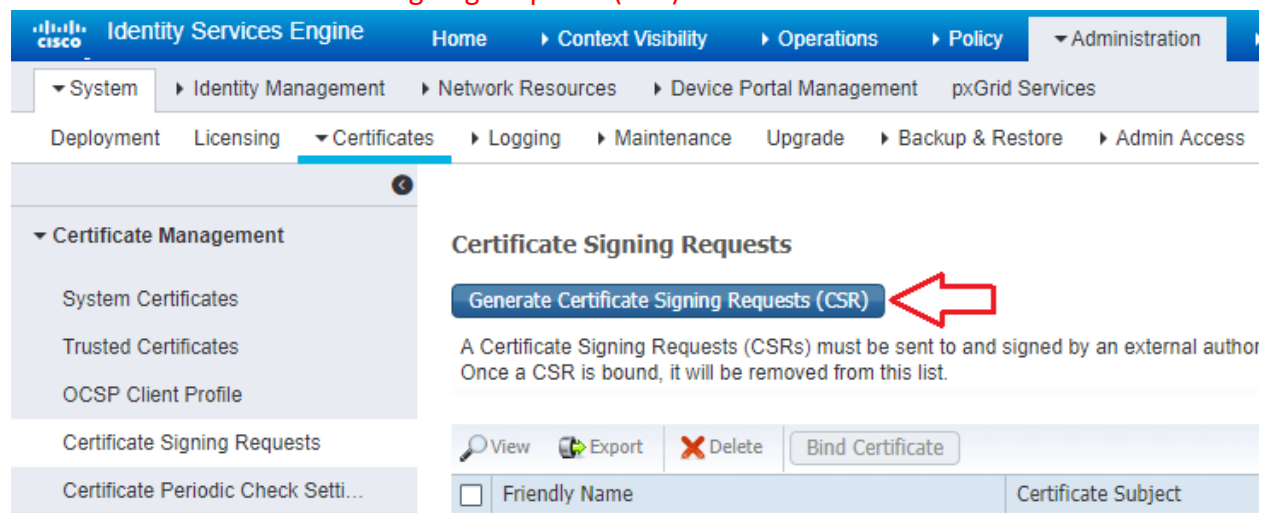
**Trust for authentication of Cisco Services:**

You only need to check this if you want this certificate to be trusted for external Cisco services such as a feed service.

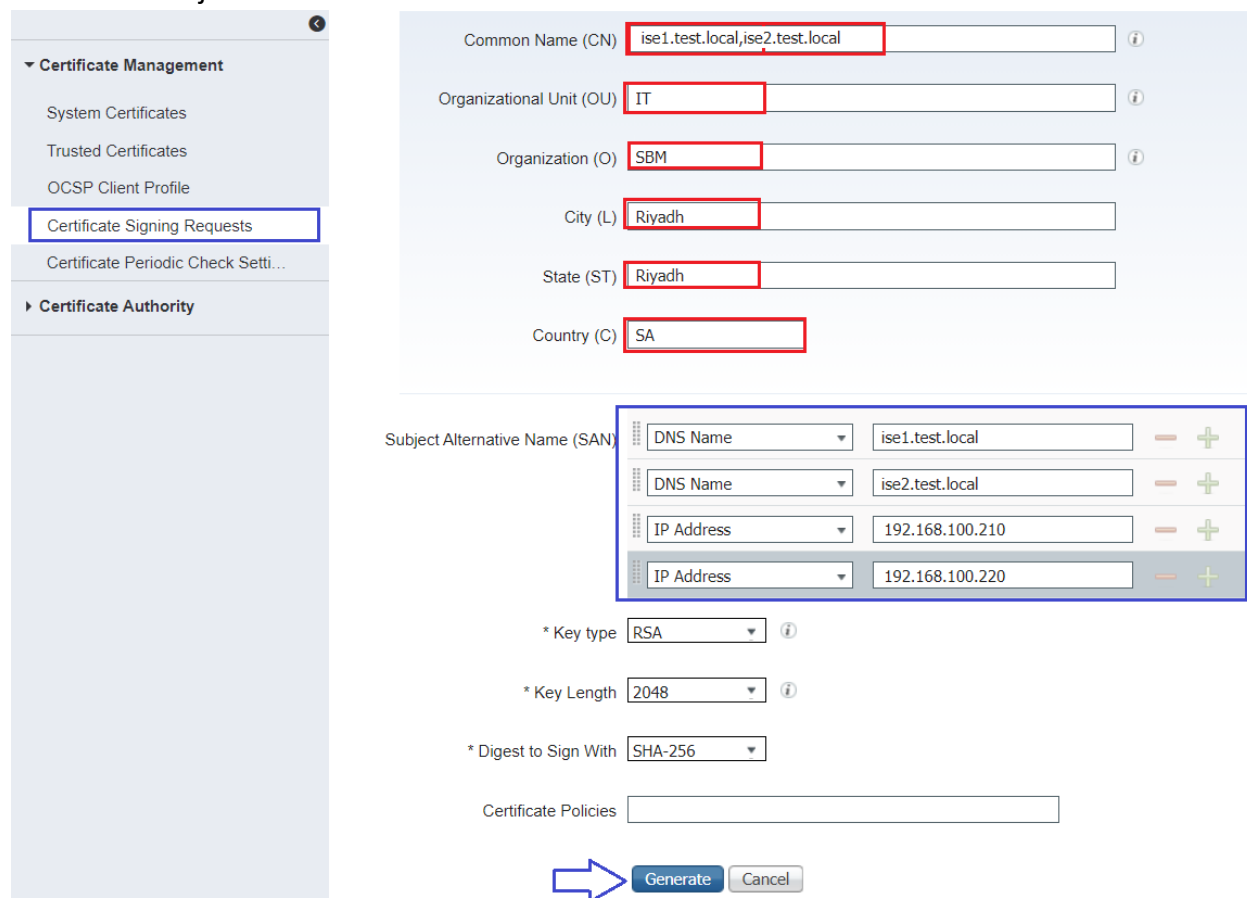


## Generating Certificate Signing Request:

Issue the CSR by going to **Administration>System>Certificates>Certificate Signing Requests** and click on **Generate Certificate Signing Requests (CSR)**.



Certificate will be used for **Multi-use** in the drop-down. Check the box next to your ISE node and fill out the subject information then click on **Generate**.



Click **Export** on the pop-up that comes up. This will download the CSR request to your local Computer system.

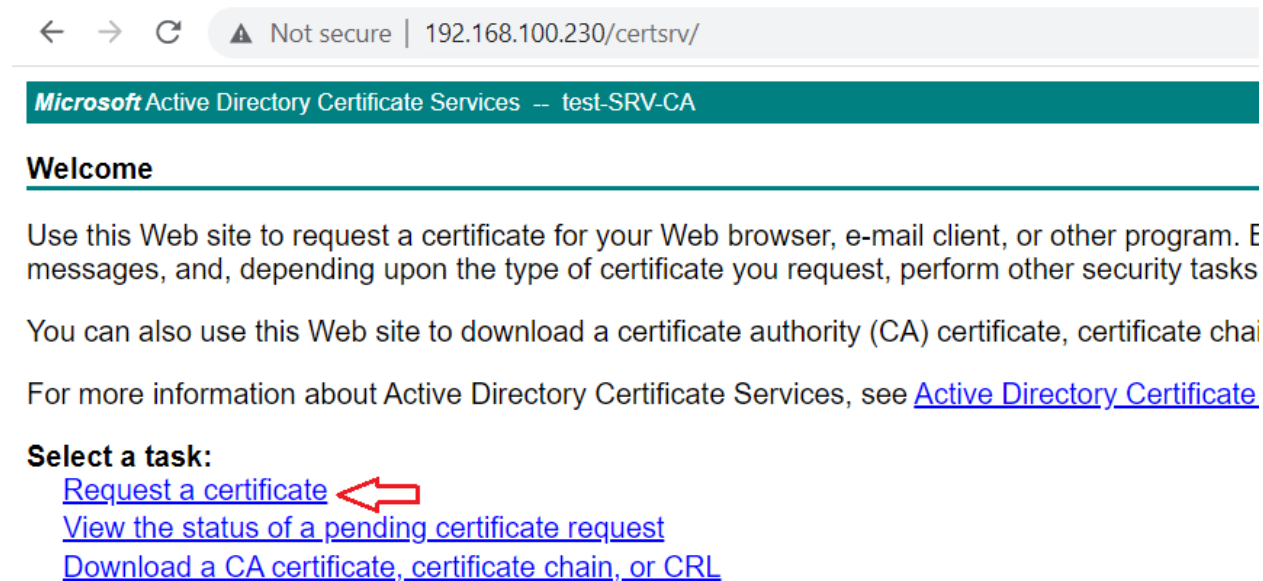
The screenshot shows a web-based CSR generation form. The form fields are: Common Name (CN) with value 'ise1.test.local,ise2.test.local'; Organizational Unit (OU) with value 'IT'; Organization (O) with value 'SBM'; City (L) with value 'Riyadh'; State (ST) with value 'Riyadh'; Country (C) with value 'SA'. Below these are fields for Subject Alternative Name (SAN) with options for DNS Name, DNS Name, and IP Address. A white pop-up window is overlaid on the form, displaying the message: 'Successfully generated CSR(s) ✓', 'Certificate Signing request(s) generated:', 'ise1#Multi-Use', and 'Click Export to download CSR(s) or OK to return to list of CSR(s) screen'. At the bottom of the pop-up are 'Export' and 'OK' buttons. A red arrow points to the 'Export' button.

Open the CSR that you just downloaded in Notepad or Notepad ++.

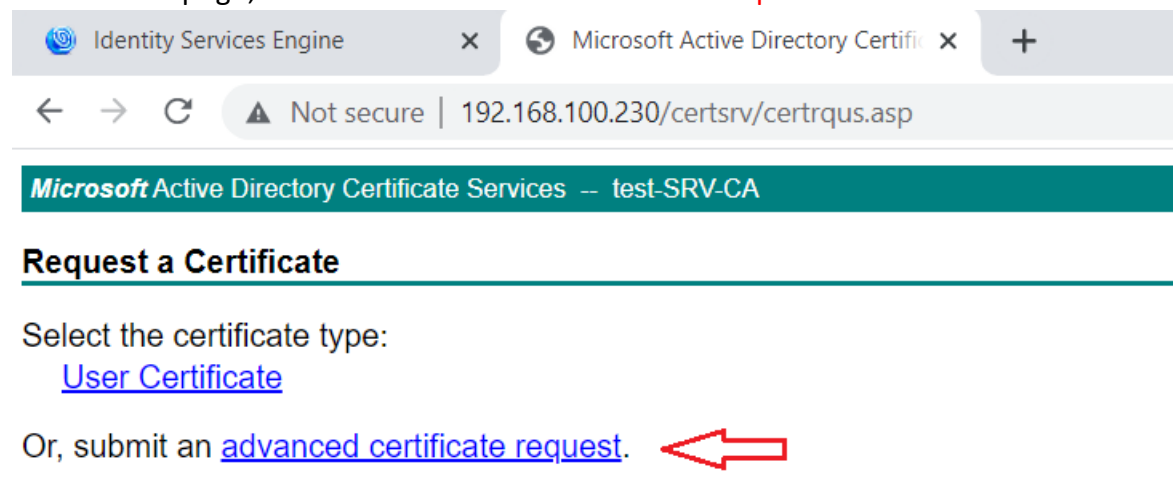
The screenshot shows a Notepad window with the file name 'ise1MultiUse.pem'. The text content is a Base64-encoded CSR request, starting with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. The middle section contains a long string of Base64 characters.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDZTCCAk0CAQAwDEoMCMYGA1UEAxMfaXNlMS50ZXN0LmxvY2FsLGlzZTIudGVz
dC5sb2NhbmDELMakGA1UECzMCSVQxDDAKBgNVBAoTAlNCTTEPMA0GA1UEBxMGUml5
YWRoMQ8wDQYDVQQIEWZSaXlhZGxhZGxhZGxhZGxhZGxhZGxhZGxhZGxhZGxhZGxh
AQEFAAOCAQ8AMIIBCgKCAQEAMd1yj2do9Y7/dg2xTWgUbs3dKliR6KZ4+uqVht7
3qFtICVbOwyphXZj3Ilu7+xkahecAId7w0GJV5PKW6HTr8k5HDFQPC55NnFuDkU
2OEfc182fcDewCYQ1LNx7FO7DhGH7oRUbLymi7ygViJtTIVhRwfnfyQN3DdIgnIM
+dr/Dew4msURDAPa9VV63x1UNnoQggDK321AYUN1rdigbpCj/juApL/RpDOG8xwp
5WXbb6mBHOLDhAlQ1LPeGDbOC9sS4EFqTKAqlqV1AwXNo+cfe4GoElODEsb6YyUw
Bmbxe5XOVY4NgF1mFhGv6Azq/vvYykRd+hJarNiwIPKZjQIDAQABOIGrMIGoBgkq
hkiG9w0BCQ4xgzowgzcwNwYDVR0RBDAwLoIPaXNlMS50ZXN0LmxvY2FsLGlzZTIu
LnRlc3QubG9jYWyHBMC0ZKNHBMCoZNwwCwYDVR0PBAQDAGXgMB0GA1UdDgQWBbTa
OaPuXmtLDTJVv++VYBiQr9gHCTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
AwIwEQYJYIZIAyB4QgEBBAQDAGZAMA0GCSqGSIs3DQEBChUAA4IBAQ79RHe2Pgp
FoMRxIyalk0U5HKH4kKfNasnB9pirb7glCpG+cwatZ6jMEGhNb0IzlkMmD4OxCnd
17JzkdLULt5br2L1Lk30wlziNiCIDCaUyWrPH3eZ84KdLo0FJG+8ILRhWBFRAtJV
msJGR4h6Q57Jvflmr+55DDnJW0+keFrSePfl5ONNFdlzXq5OFpHeUgr3tCz5Uh6S
YLPgYiV9/Z72qnipIsqcrfuY/5gFLD07ibIEtTFVpsnmbas6Y8D1viu9zaSsRDou
R3De5njsY26T60x4Fdr6+aljiCwhk0gjFyy+V8za/kBmoev/4rE8+KqQfrCjht6H
IUksLsE2jYha
-----END CERTIFICATE REQUEST-----
```

Now, go to your Microsoft AD CA Web Enrollment first page. Click on the **Request a certificate** link.



On the next page, click on the **advanced certificate request** link.



Paste the contents of your **CSR to the Base-64-encoded certificate request** box. Select the appropriate Certificate Template. In my case it's Web Server. Click **Submit**.

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
17JzkDLU1T5br2L1Lk30wlziNiCIDCaUyWrPH3e.  
msJGR4h6Q57Jvf1mr+55DDnJW0+keFrSePf150NI  
YLPgYiV9/Z72qnipIsqcrfuY/5gF1D07ibIEtTF  
R3De5njSY26T60x4Fdr6+aljiCwhk0gjFyy+V8z  
IUksLsE2jYha  
-----END CERTIFICATE REQUEST-----
```



### Certificate Template:

Web Server

### Additional Attributes:

Attributes:

Submit >




Select the **Base 64 encoded** radio button and click **Download certificate**



Not secure | 192.168.100.230/certsrv/certfnsh.asp

## Certificate Issued

The certificate you requested was issued to you.

 ☐ DER encoded or ☒ Base 64 encoded

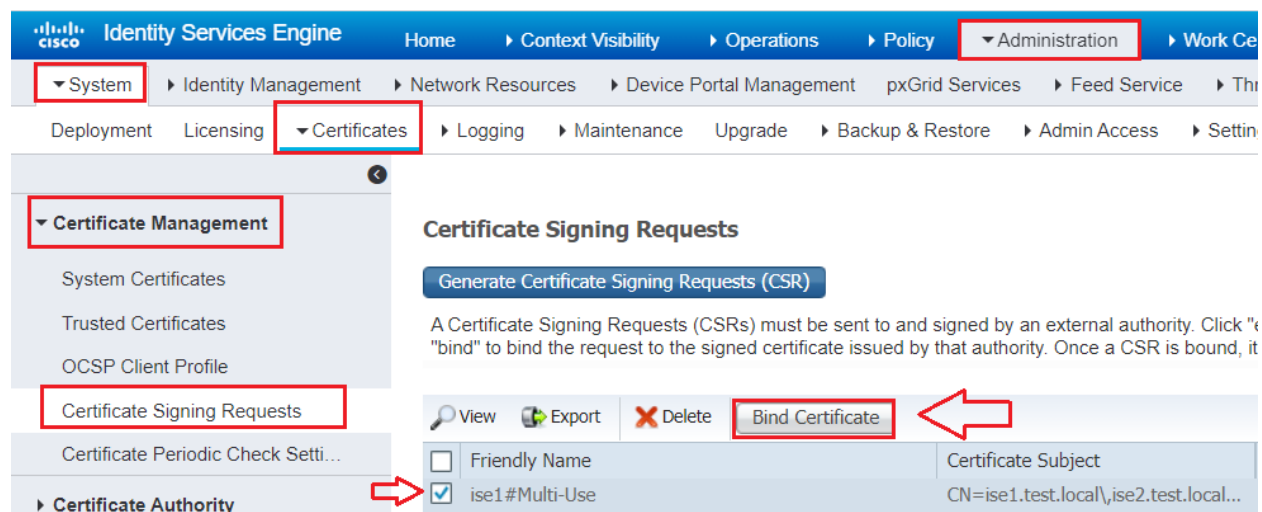


[Download certificate](#)

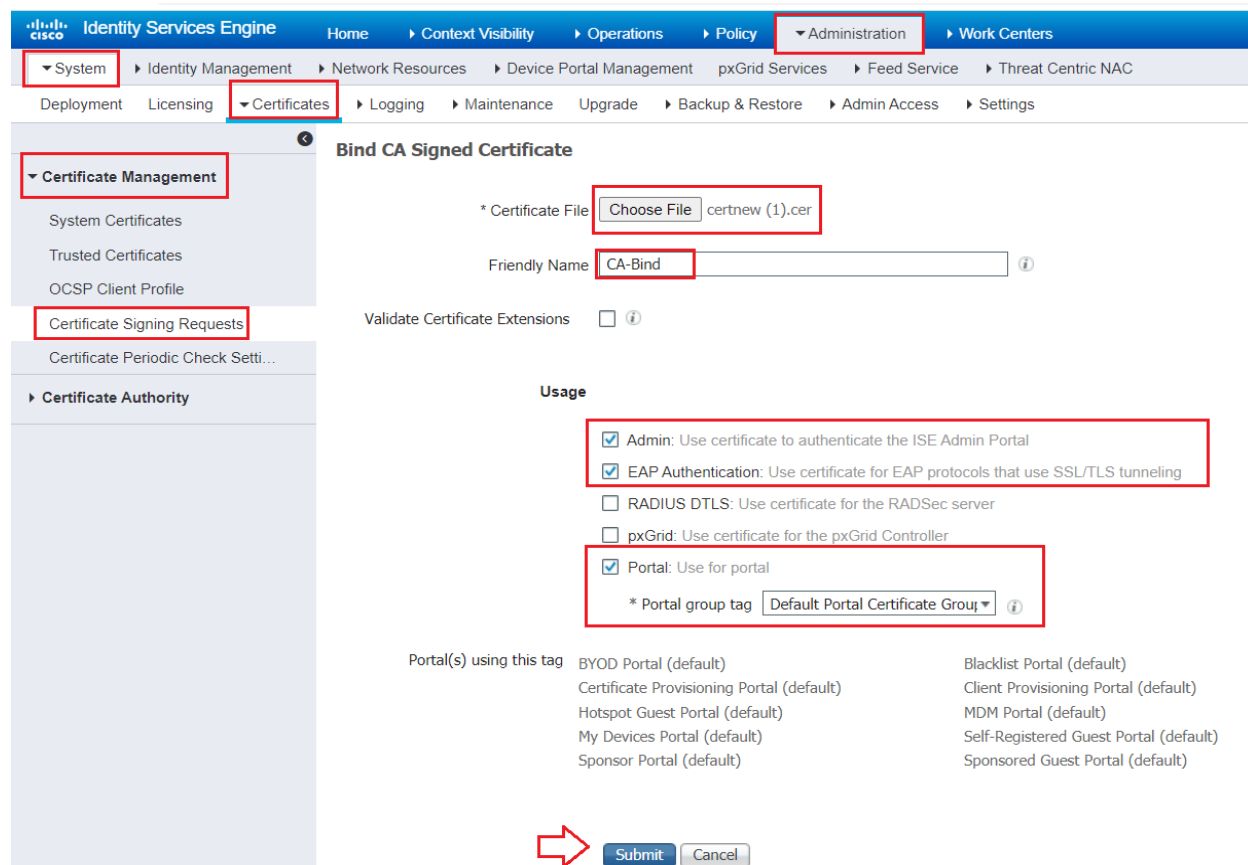
[Download certificate chain](#)

## Binding a CA-Signed Certificate:

Go back to Cisco ISE and navigate to **Administration -> System -> Certificates -> Certificate Management -> Certificate Signing Requests** and check the box next to the CSR you created earlier and click Bind Certificate.

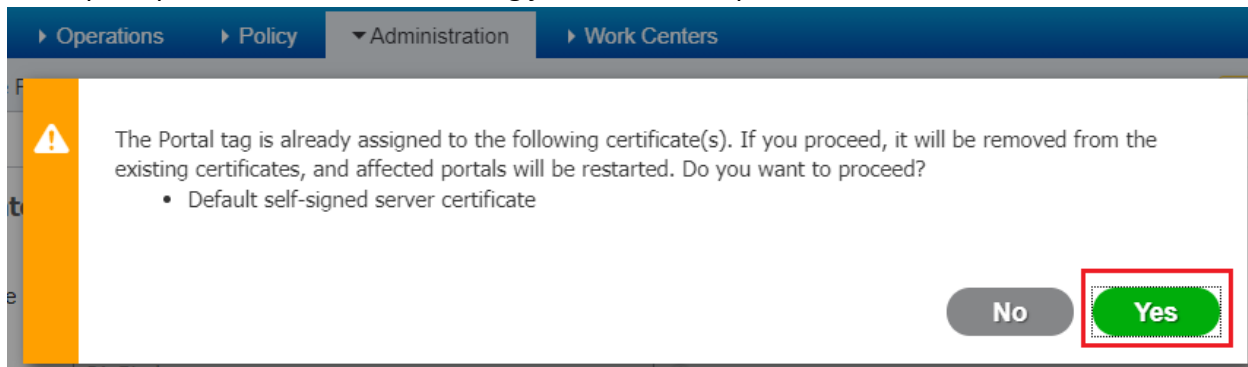


Choose the certificate you downloaded, enter a friendly name, and select the services you plan to use this cert for under Usage.

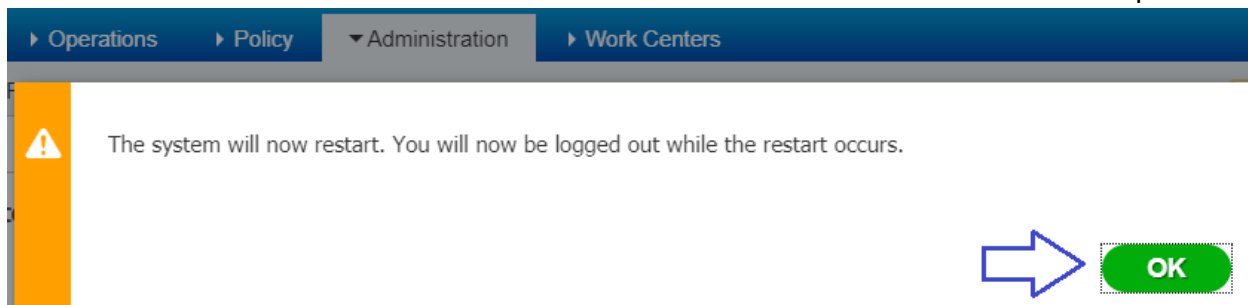




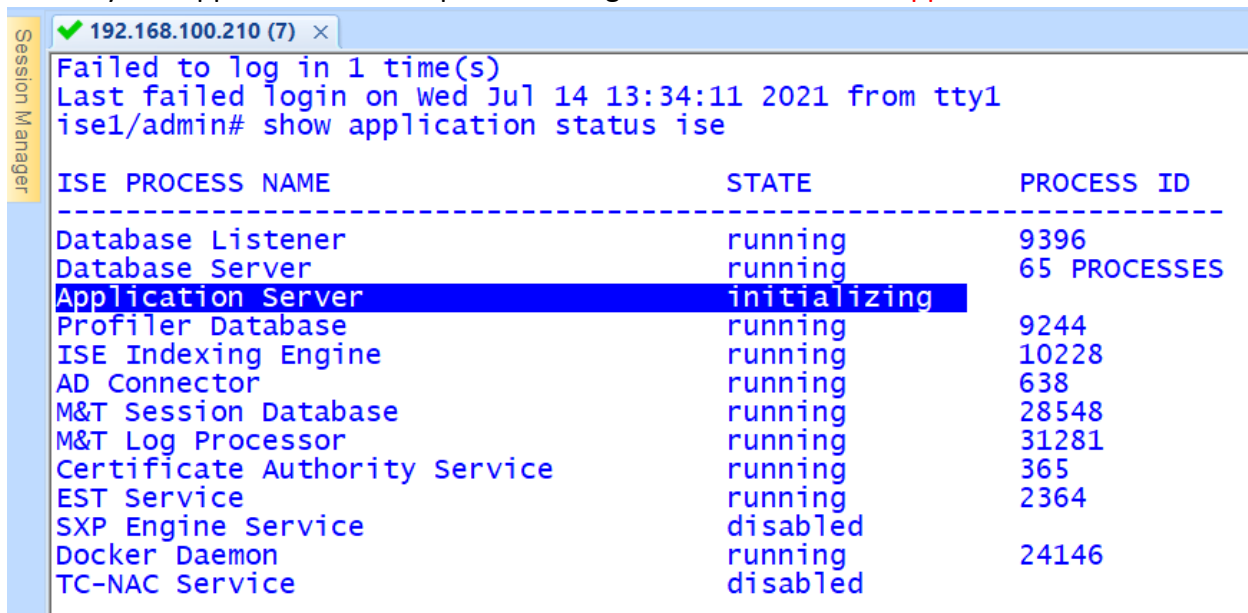
It will prompt Portal Certificate warning just click **Yes** to proceed.



ISE will restart. Because it can take a few minutes for the web interface to come back up.



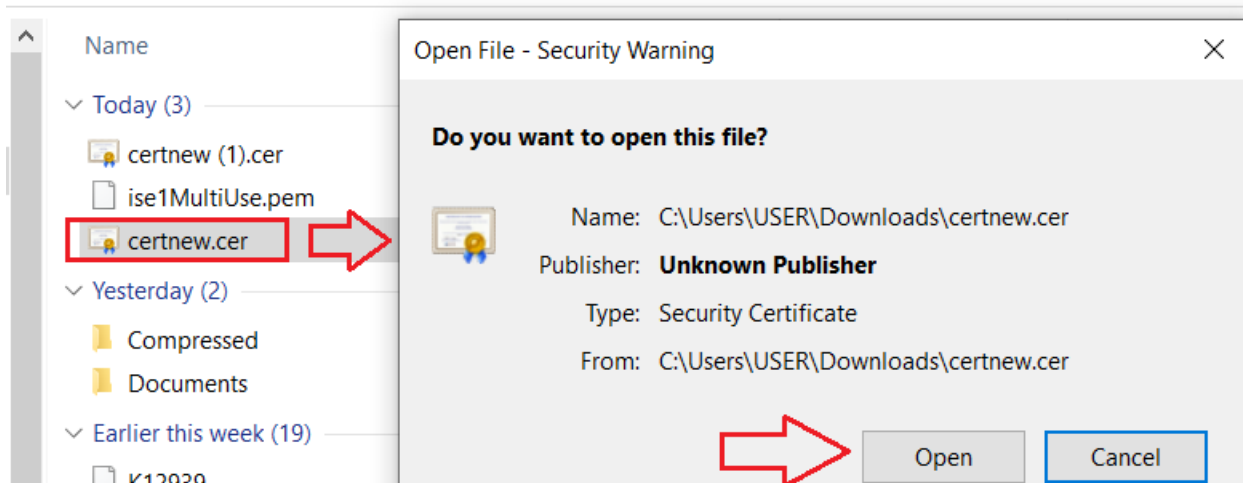
To verify the Application Server up and running use command **show application status ise**.



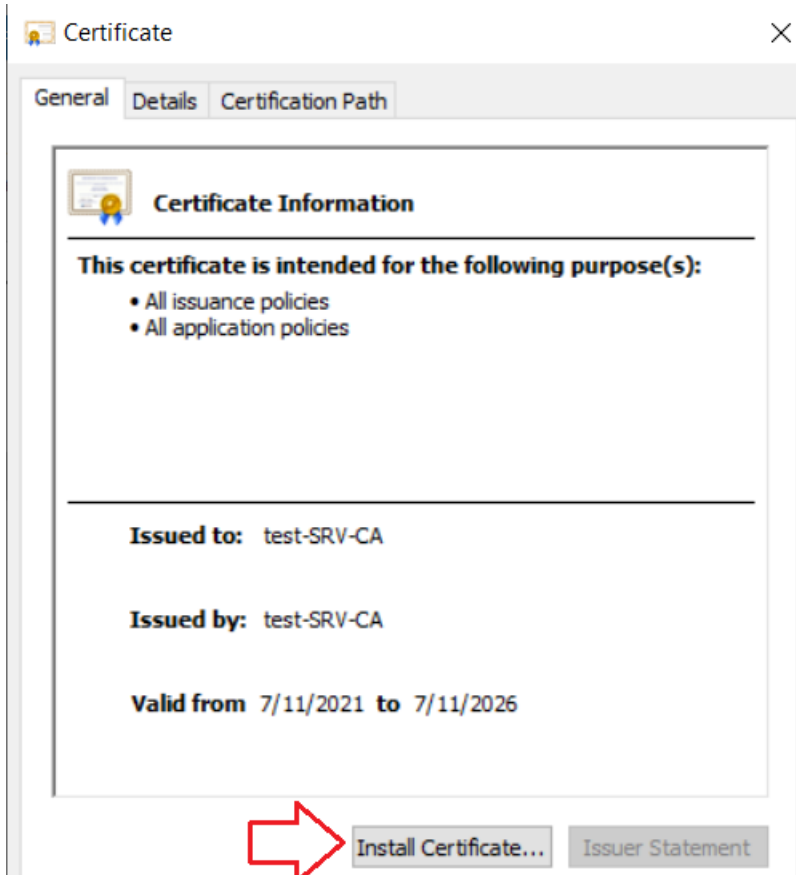
## Install Certificate in Client PC:

Double click on **certificate**, it will open Security Warning Click **Open**.

This PC > Downloads



it will start new Certificate installation wizard, click **Install Certificate** to continue.



Choose Store Location **Local Machine** and click Next to continue.

### 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 Certificate Store, place all certificates in the following store, **Trusted Root Certification Authorities** click **Next**.

#### Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

## Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

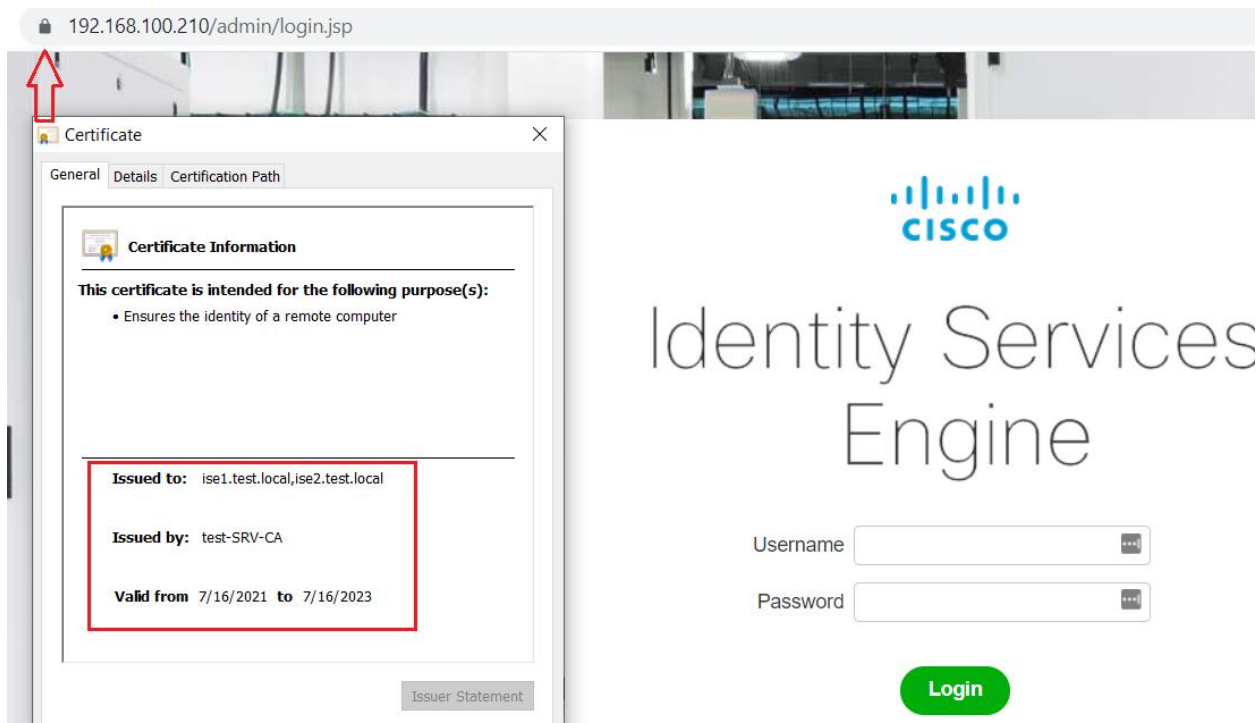
You have specified the following settings:

<b>Certificate Store Selected by User</b>	Trusted Root Certification Authorities
Content	Certificate

Finish

Cancel

192.168.100.210/admin/login.jsp



The image shows the Cisco Identity Services Engine (ISE) login page. A red arrow points to the top-left corner of the browser window. A 'Certificate' dialog box is open, displaying the following information:

- Certificate Information**
- This certificate is intended for the following purpose(s):
  - Ensures the identity of a remote computer
- Issued to:** ise1.test.local, ise2.test.local
- Issued by:** test-SRV-CA
- Valid from:** 7/16/2021 to 7/16/2023
- Issuer Statement

The background shows the Cisco Identity Services Engine login page with the Cisco logo, the text 'Identity Services Engine', and input fields for 'Username' and 'Password', followed by a green 'Login' button.