SAFE Certificate Management Design Guide

Domain: Management

January 2023

Contents

Overview

In Cisco SAFE, the Management domain includes the management of devices and systems using centralized services for consistent policy deployment, workflow change management and the ability to keep systems patched. The Management coordinates policies, objects, and alerting.

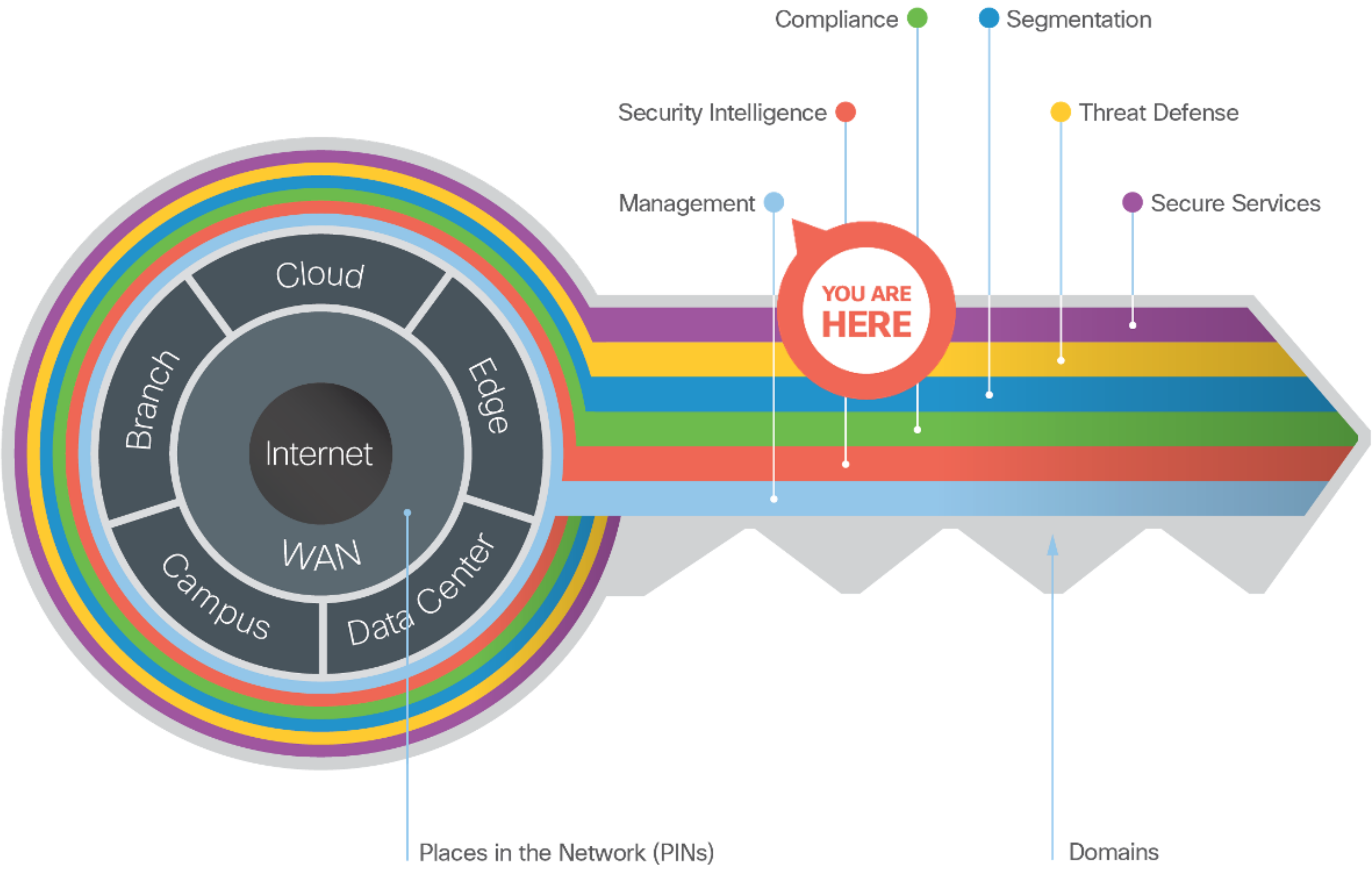


Figure 1.
SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.

SAFE simplifies security by starting with business flows, then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.

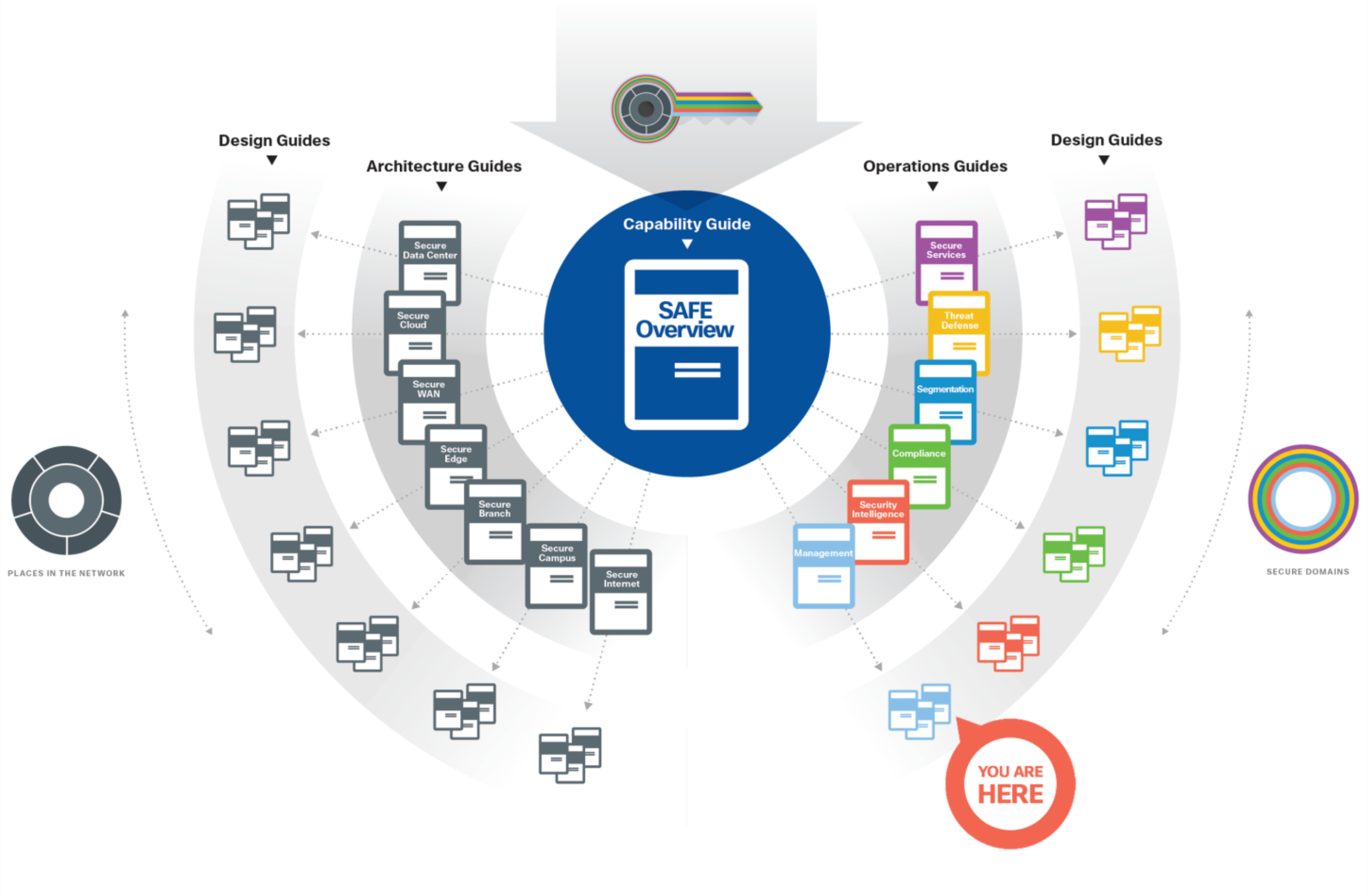


Figure 2. **SAFE Guidance Hierarchy**

This operations design guide contains instructions for certificate management required by the Zero Trust: Network and Cloud Security design guide.

This guide is focused on Active Directory (AD) as an external certificate authority (CA). The guidance is provided for configuring certificates on security components that integrate with the Platform Exchange Grid (pxGrid) provided by Identity Services Engine (ISE). Guidance is also provided on how to setup Administrator certificates.

Certificate Management

Create Externally Signed ISE Certificates for pxGrid and Admin Services

Integrating Secure Firewall with pxGrid requires that the Firewall Management Center (FMC) trust the root CA used to sign the ISE MNT server Admin certificate and the ISE pxGrid certificate.

This section will cover

- how to use ISE to generate Certificate Signing Requests (CSRs) for the pxGrid and Admin certificates
- the process of creating a template for the CSRs in AD
- the process for generating certificates from the CSRs in AD

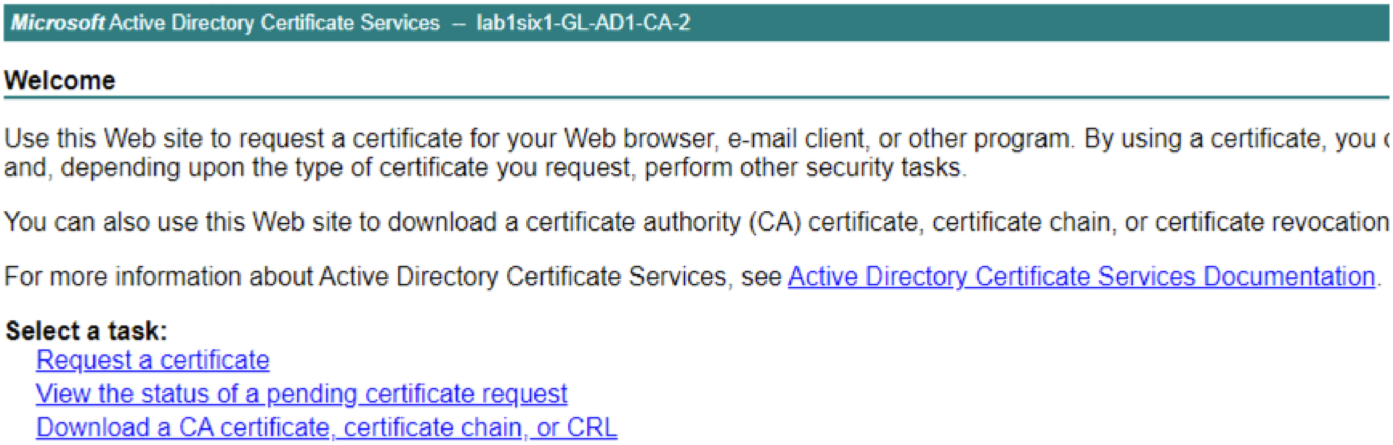
- the process for adding the CA root certificate as a trusted CA in ISE.

Active Directory Certificate Authority: Export a Root Certificate

The external CA root certificate should be trusted in ISE before importing any certificates signed by the external CA.

Step 1. To export a root certificate from an Active Directory CA, Access the CA server by appending /certsrv/ to the AD server hostname, e.g.

- **adserver.example.com**
- **adserver.example.com/certsrv/**



Microsoft Active Directory Certificate Services – lab1six1-GL-AD1-CA-2

Welcome

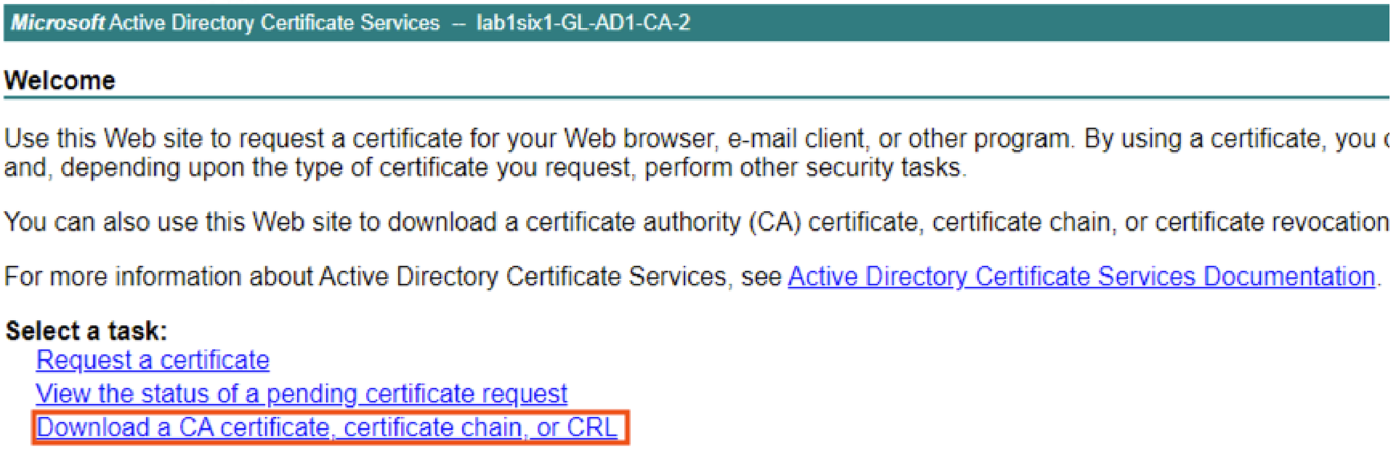
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you c and, depending upon the type of certificate you request, perform other security tasks.

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

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

Step 2. Click the Download a CA certificate, certificate chain, or CRL option.



Microsoft Active Directory Certificate Services – lab1six1-GL-AD1-CA-2

Welcome

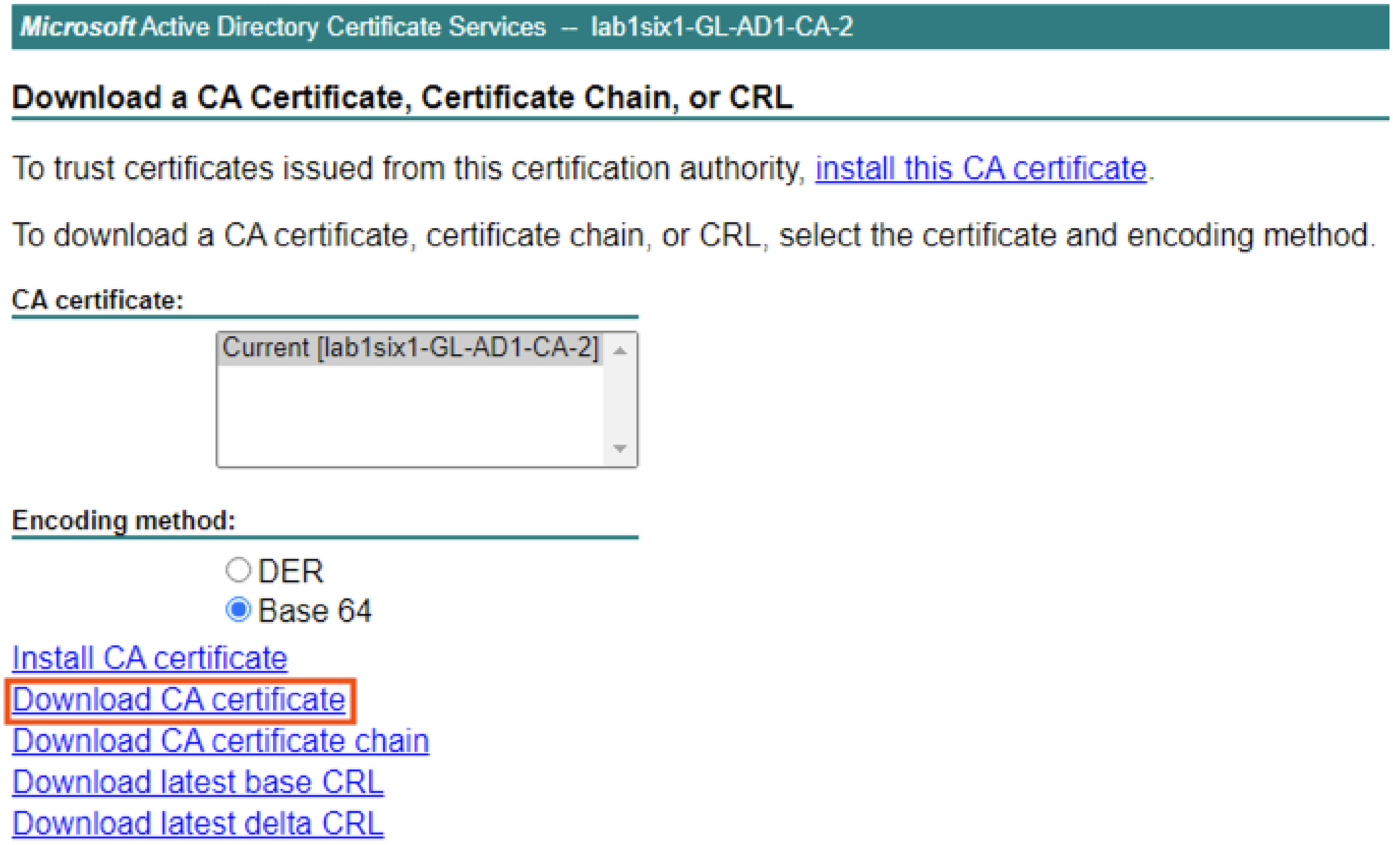
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you c and, depending upon the type of certificate you request, perform other security tasks.

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

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

Step 3. Set the encoding method if desired, then click Download CA certificate.



Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

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 [lab1six1-GL-AD1-CA-2]

Encoding method:

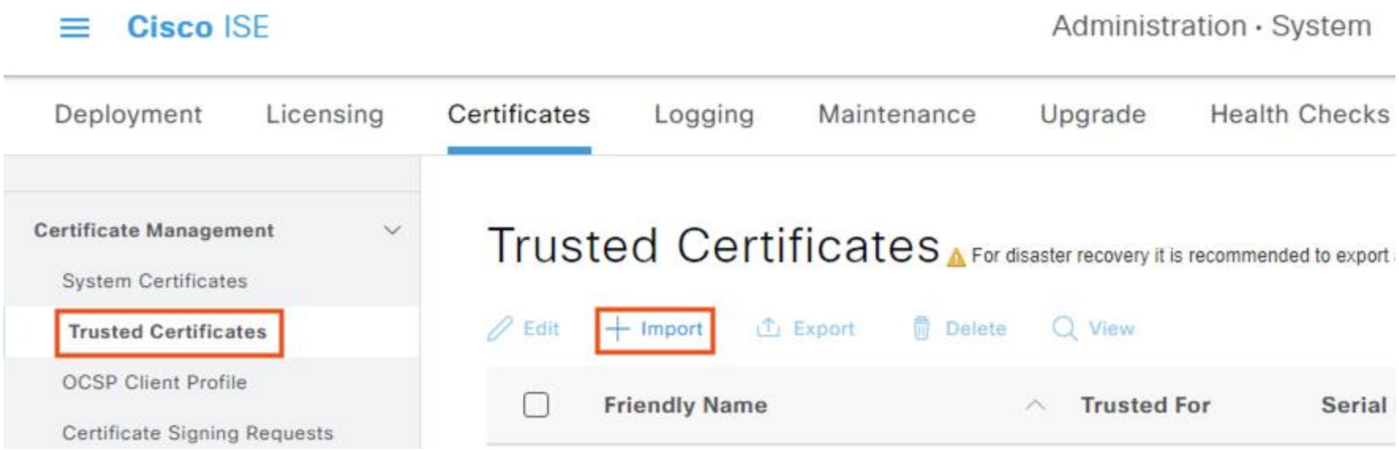
○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

ISE: Add an External Certificate to the Trusted Certificate Store

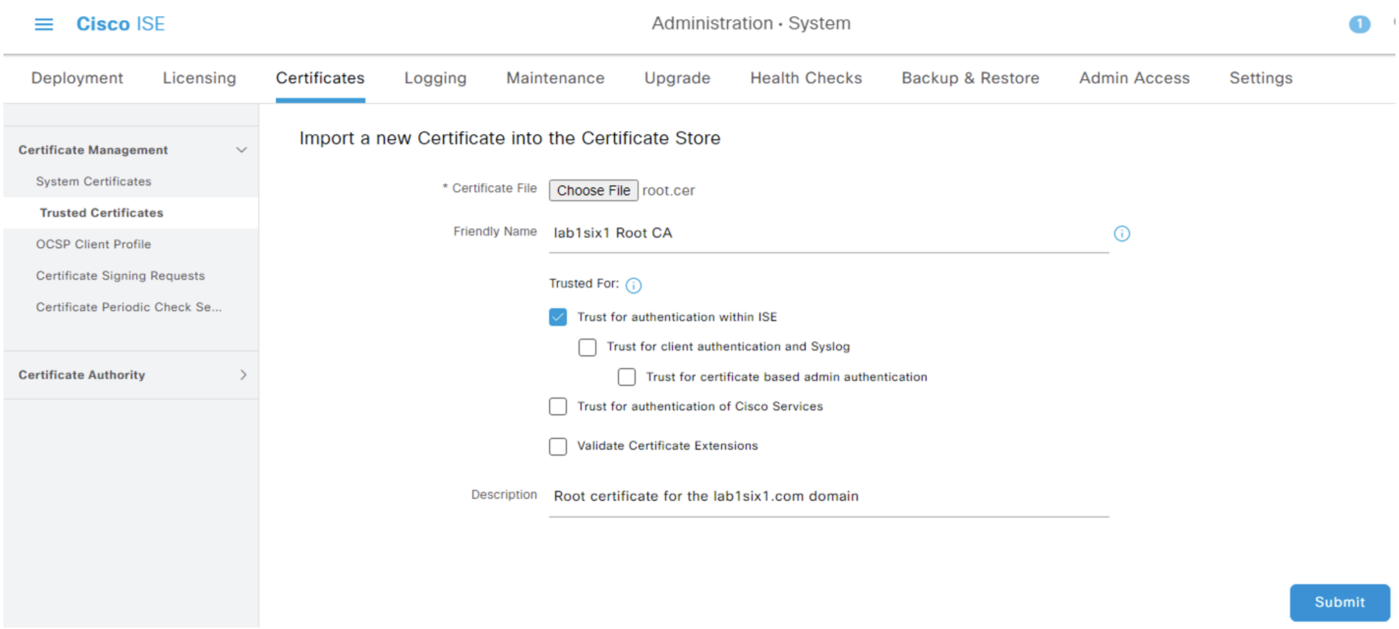
Step 1. Within ISE, click the Menu icon (☰) and navigate to Administration → System → Certificates.

Step 2. Click on Trusted Certificates, then click Import.



⚠ For disaster recovery it is recommended to export

Step 3. Select Choose File and upload the root certificate collected previously. Enter a Friendly Name, Description, and set the Trusted For fields for the certificate (this example uses the default setting for authentication within ISE, but more options can be checked). Click Submit.



Import a new Certificate into the Certificate Store

* Certificate File: Choose File root.cer

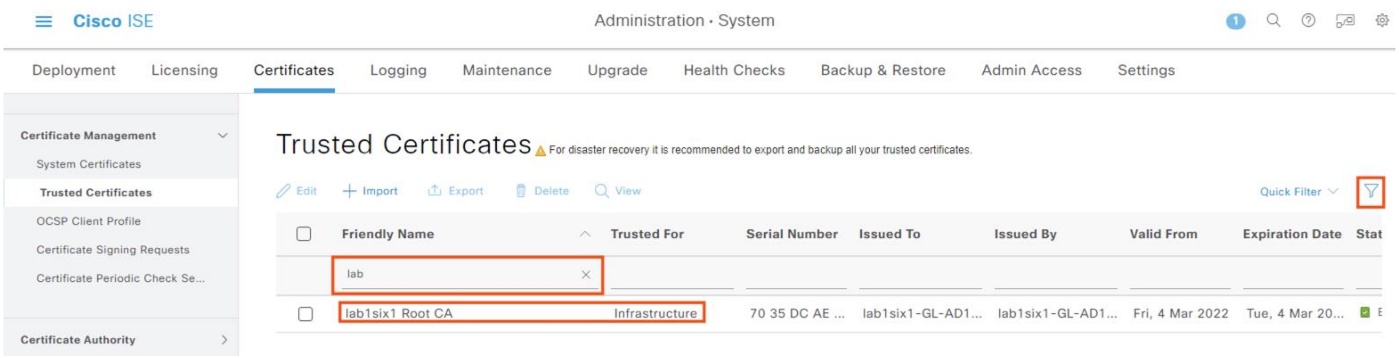
Friendly Name: lab1six1 Root CA

Trusted For:

- ☑ Trust for authentication within ISE
  - □ Trust for client authentication and Syslog
    - □ Trust for certificate based admin authentication
- □ Trust for authentication of Cisco Services
- □ Validate Certificate Extensions

Description: Root certificate for the lab1six1.com domain

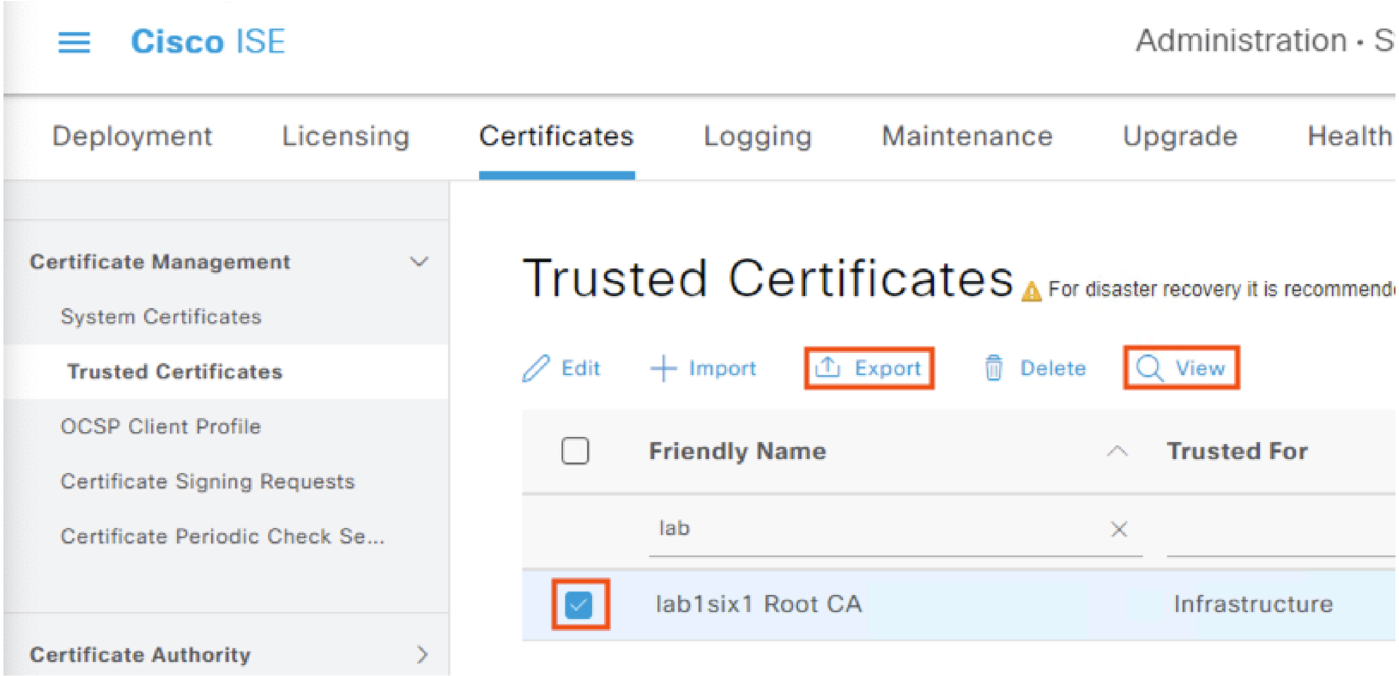
Step 4. Use the filter option to search for the friendly name and verify that the certificate has been imported.



Trusted Certificates ⚠ For disaster recovery it is recommended to export and backup all your trusted certificates.

□	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Stat
	lab							
□	lab1six1 Root CA	Infrastructure	70 35 DC AE ...	lab1six1-GL-AD1...	lab1six1-GL-AD1...	Fri, 4 Mar 2022	Tue, 4 Mar 20...	🟩 E

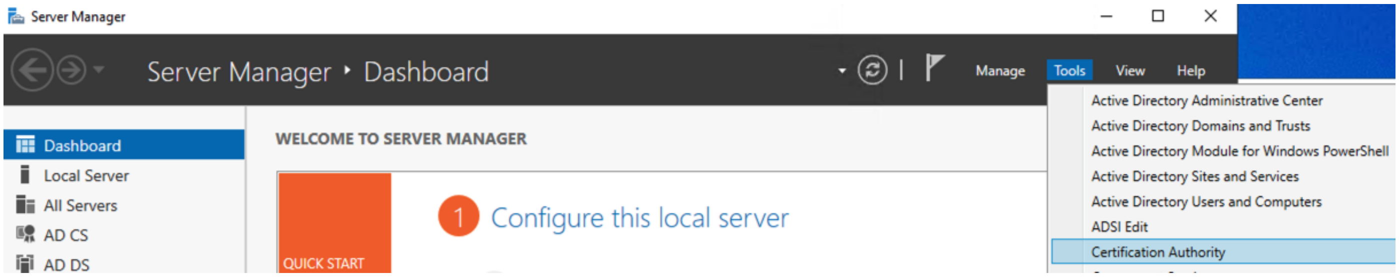
Additionally, the View and Export options can be used to check hash and certificate details for any uploaded certificate.



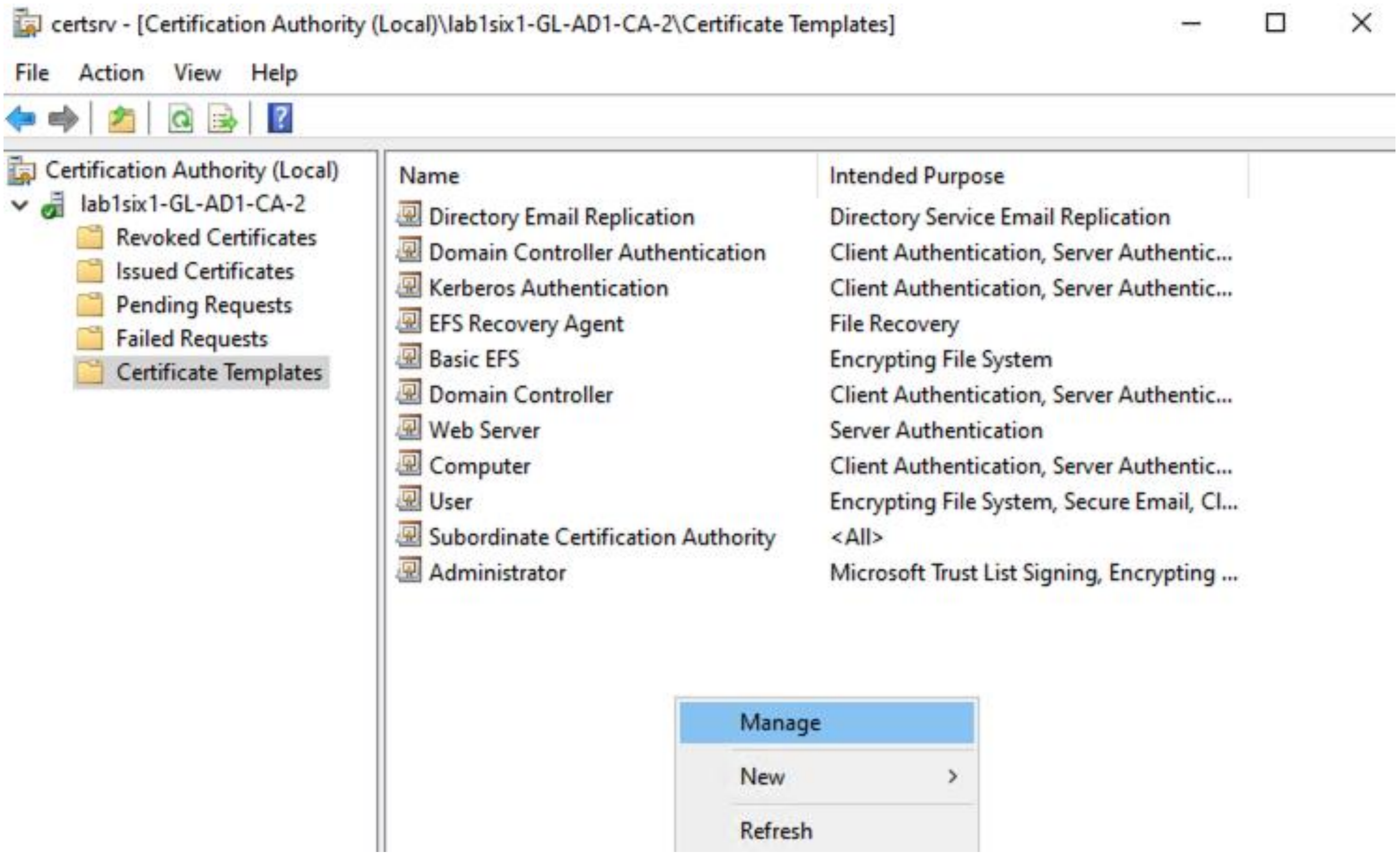
Active Directory: Create a Client and Server Authentication Template

The default ISE certificates for pxGrid and Admin are configured for both Client Authentication and Server Authentication. However, Active Directory does not have a default template to create certs with both Client and Server Authentication. This section covers how to create a CA template that will produce certificates with the Client Auth and Server Auth fields.

Step 1. Access Active Directory, open Server Manager, then select Tools → Certificate Authority.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Dashboard
Local Server
All Servers
AD CS
AD DS
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server

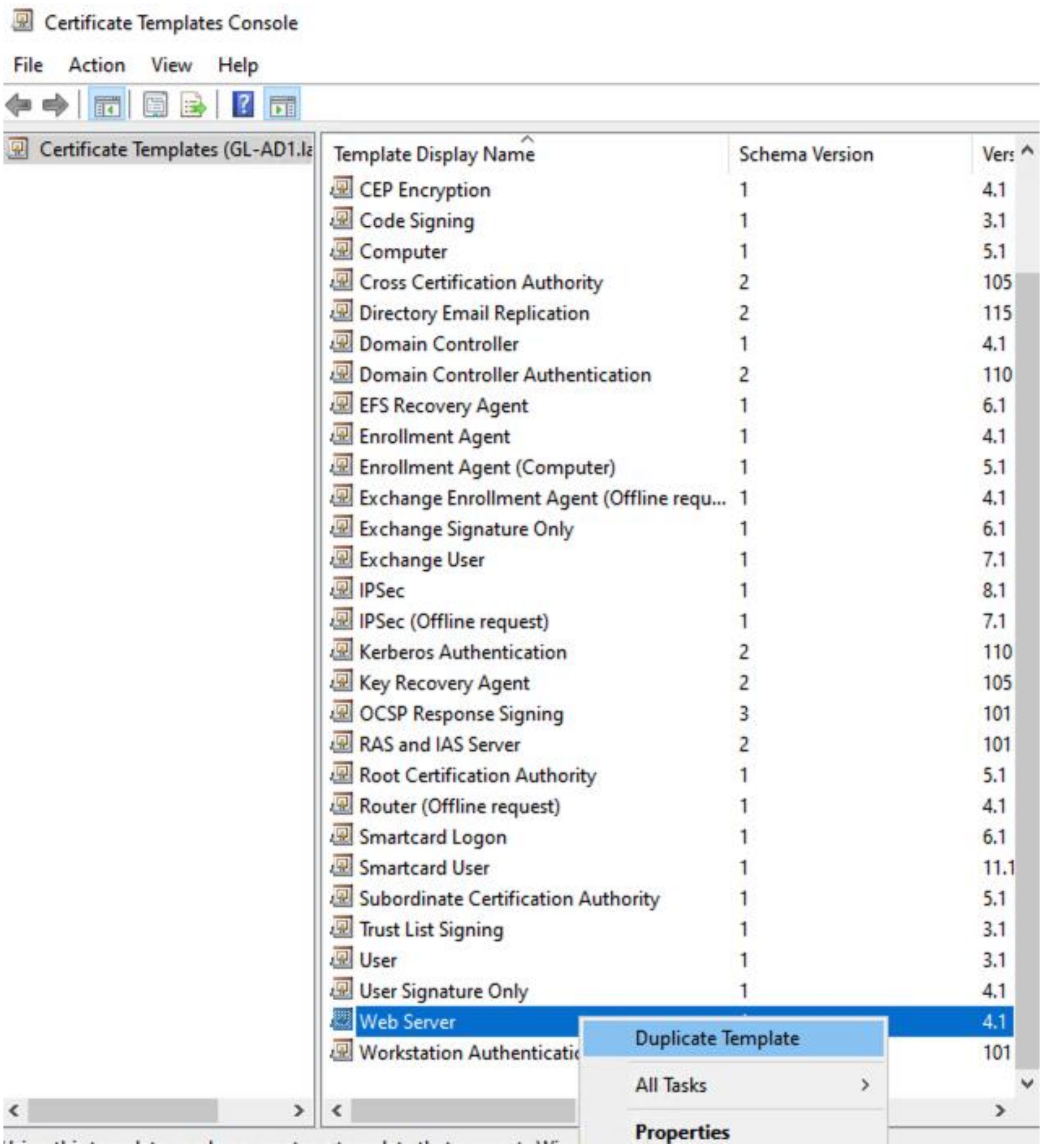
Step 2. Expand the CA server dropdown on the left menu, select Certificate Templates, right-click the empty space in the right side of the window, then select Manage.



certsrv - [Certification Authority (Local)\lab1six1-GL-AD1-CA-2\Certificate Templates]

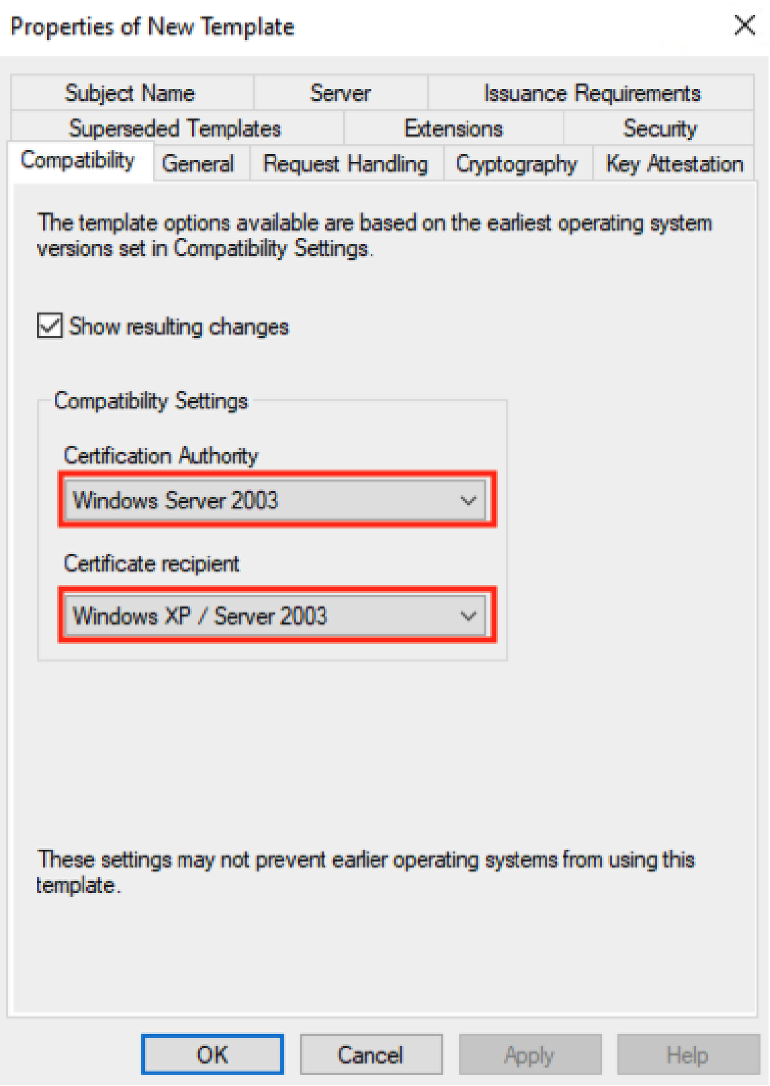
Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

Step 3. Select the Web Server template, right-click it, then click Duplicate Template.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (GL-AD1.la
Duplicate Template
All Tasks
Properties

Template Display Name	Schema Version	Vers
CEP Encryption	1	4.1
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	105
Directory Email Replication	2	115
Domain Controller	1	4.1
Domain Controller Authentication	2	110
EFS Recovery Agent	1	6.1
Enrollment Agent	1	4.1
Enrollment Agent (Computer)	1	5.1
Exchange Enrollment Agent (Offline requ...	1	4.1
Exchange Signature Only	1	6.1
Exchange User	1	7.1
IPSec	1	8.1
IPSec (Offline request)	1	7.1
Kerberos Authentication	2	110
Key Recovery Agent	2	105
OCSP Response Signing	3	101
RAS and IAS Server	2	101
Root Certification Authority	1	5.1
Router (Offline request)	1	4.1
Smartcard Logon	1	6.1
Smartcard User	1	11.1
Subordinate Certification Authority	1	5.1
Trust List Signing	1	3.1
User	1	3.1
User Signature Only	1	4.1
Web Server		4.1
Workstation Authenticati		101

Step 4. Certification Authority and Certificate Recipient can be changed if desired or left at the default of 2003 for greatest compatibility. Click Apply if changes were made.



Properties of New Template

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

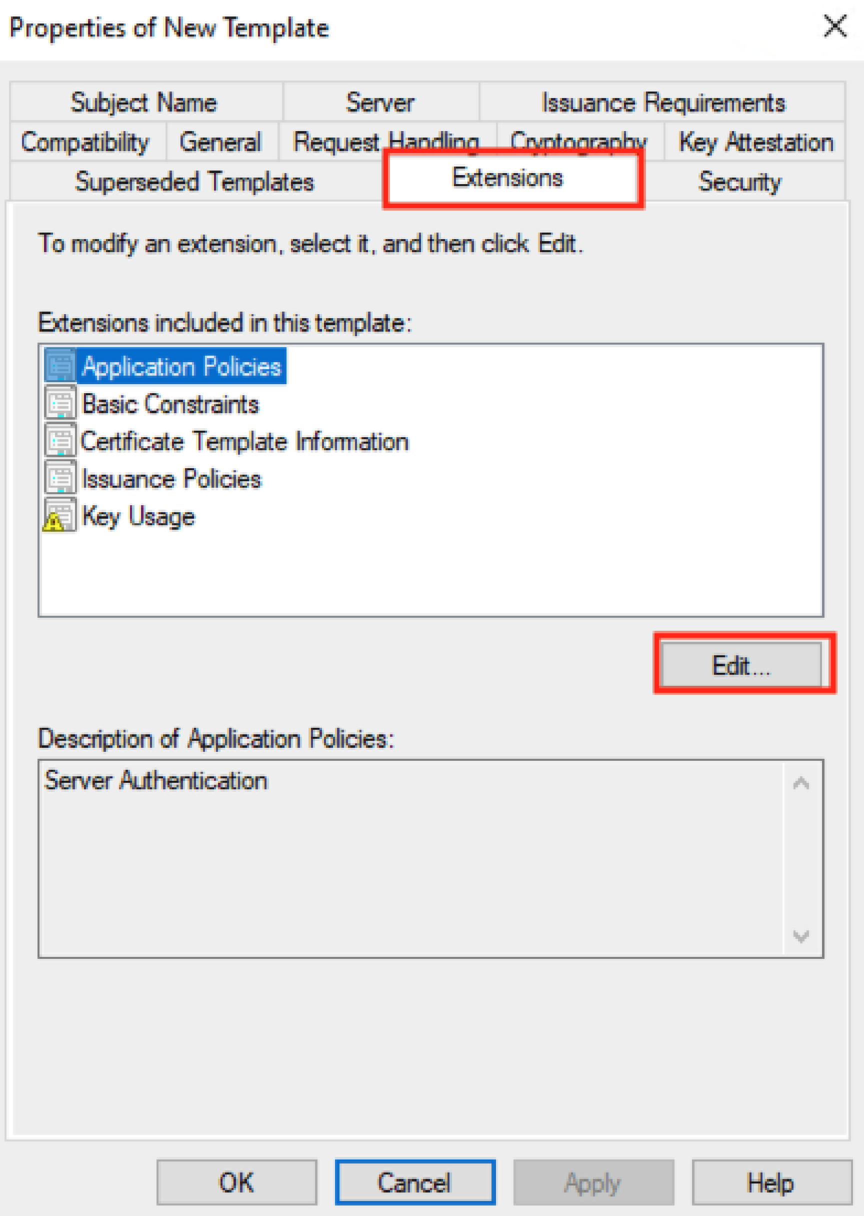
Compatibility Settings

Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

Step 5. Click on the Extensions tab, leave Application Policies selected, then click the Edit button.



Properties of New Template

To modify an extension, select it, and then click Edit.

Extensions included in this template:

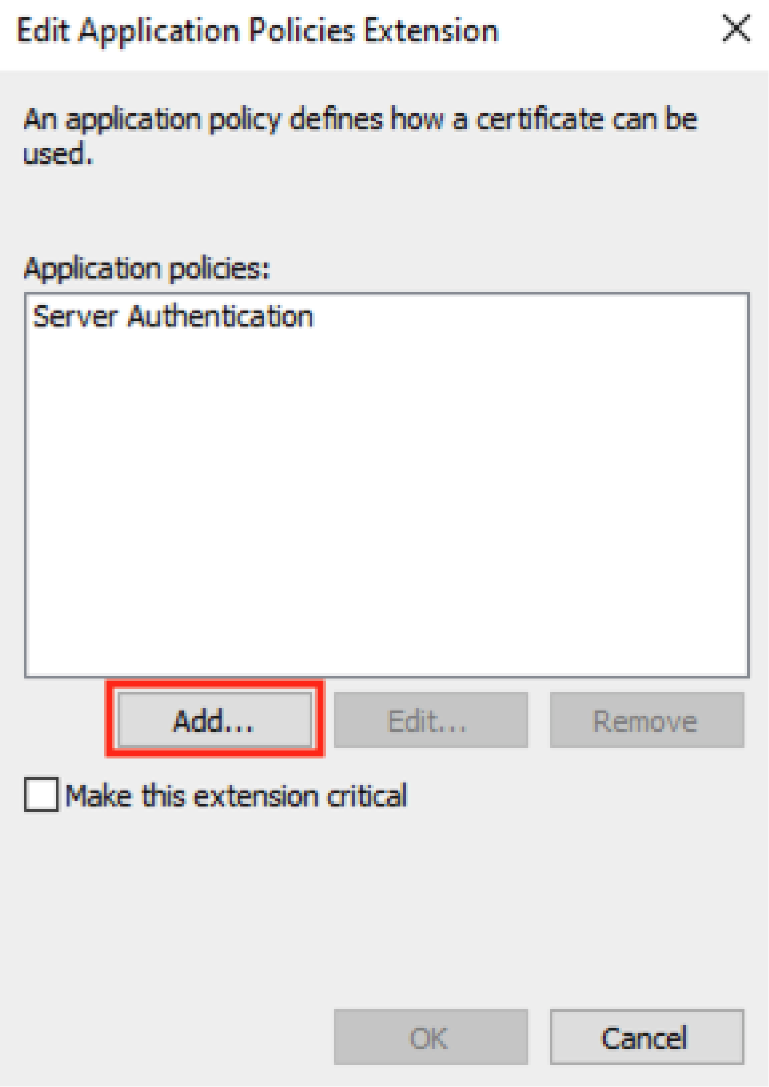
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Server Authentication

Step 6. Click the Add button.

Note: Server Authentication is added by default.



Edit Application Policies Extension

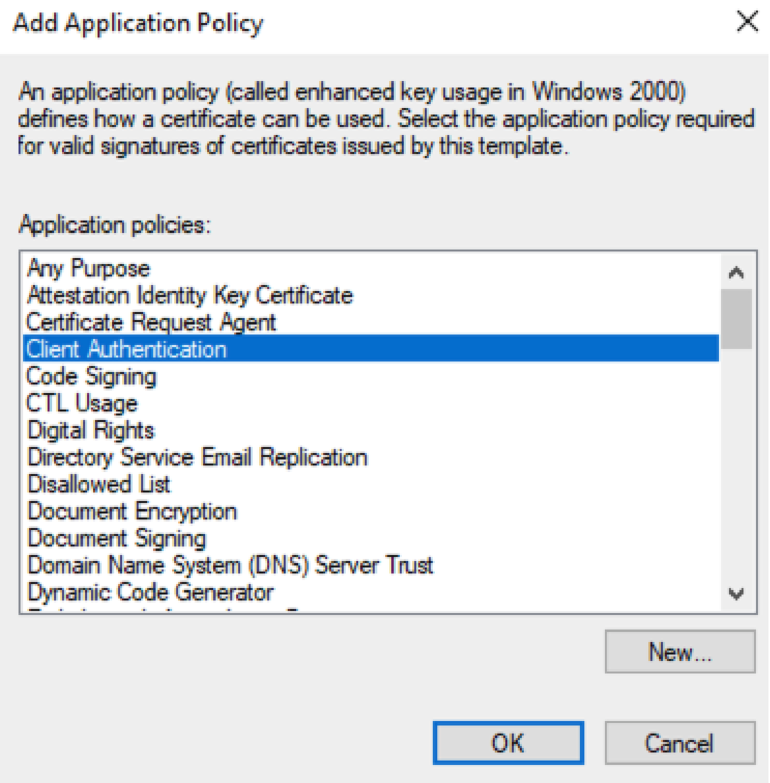
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

Step 7. Select Client Authentication and click OK.



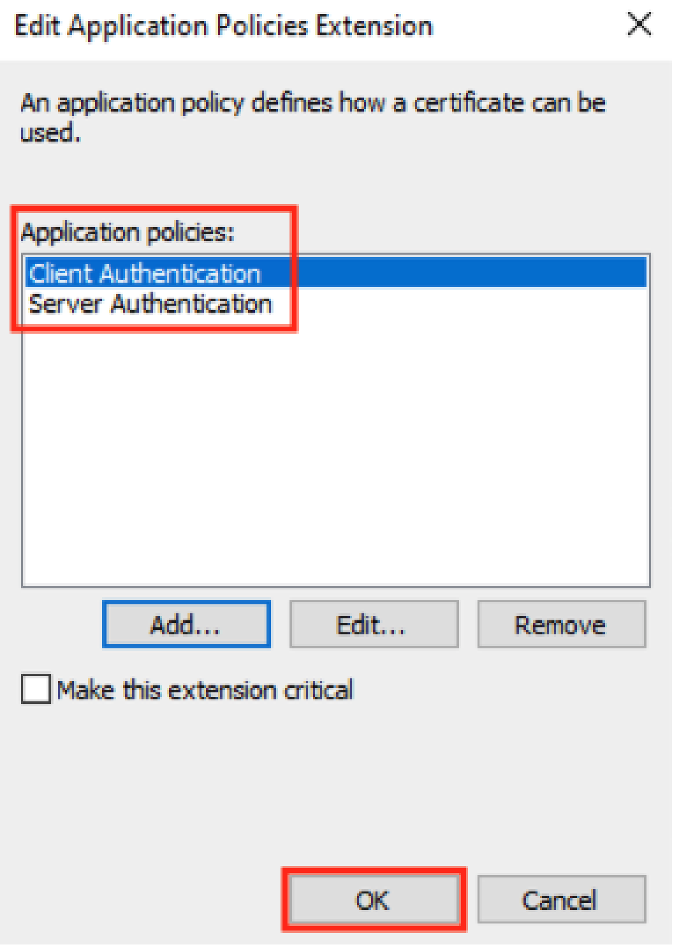
Add Application Policy

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

- Any Purpose
- Attestation Identity Key Certificate
- Certificate Request Agent
- Client Authentication
- Code Signing
- CTL Usage
- Digital Rights
- Directory Service Email Replication
- Disallowed List
- Document Encryption
- Document Signing
- Domain Name System (DNS) Server Trust
- Dynamic Code Generator

Step 8. Confirm that both Client Authentication and Server Authentication are now listed. Click OK.



Edit Application Policies Extension

An application policy defines how a certificate can be used.

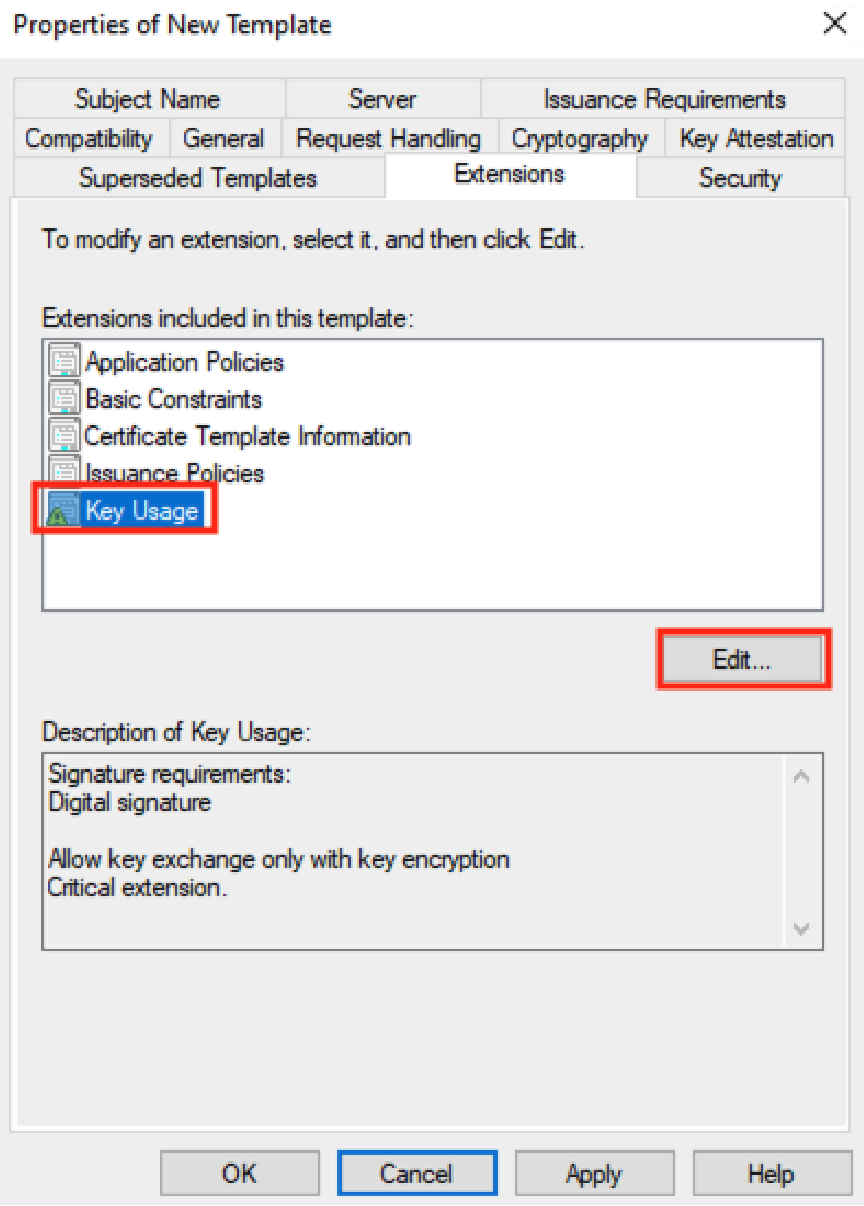
Application policies:

Client Authentication

Server Authentication

□ Make this extension critical

Step 9. Optional: while still on the Extensions tab, select Key Usage and click Edit.



To modify an extension, select it, and then click Edit.

Extensions included in this template:

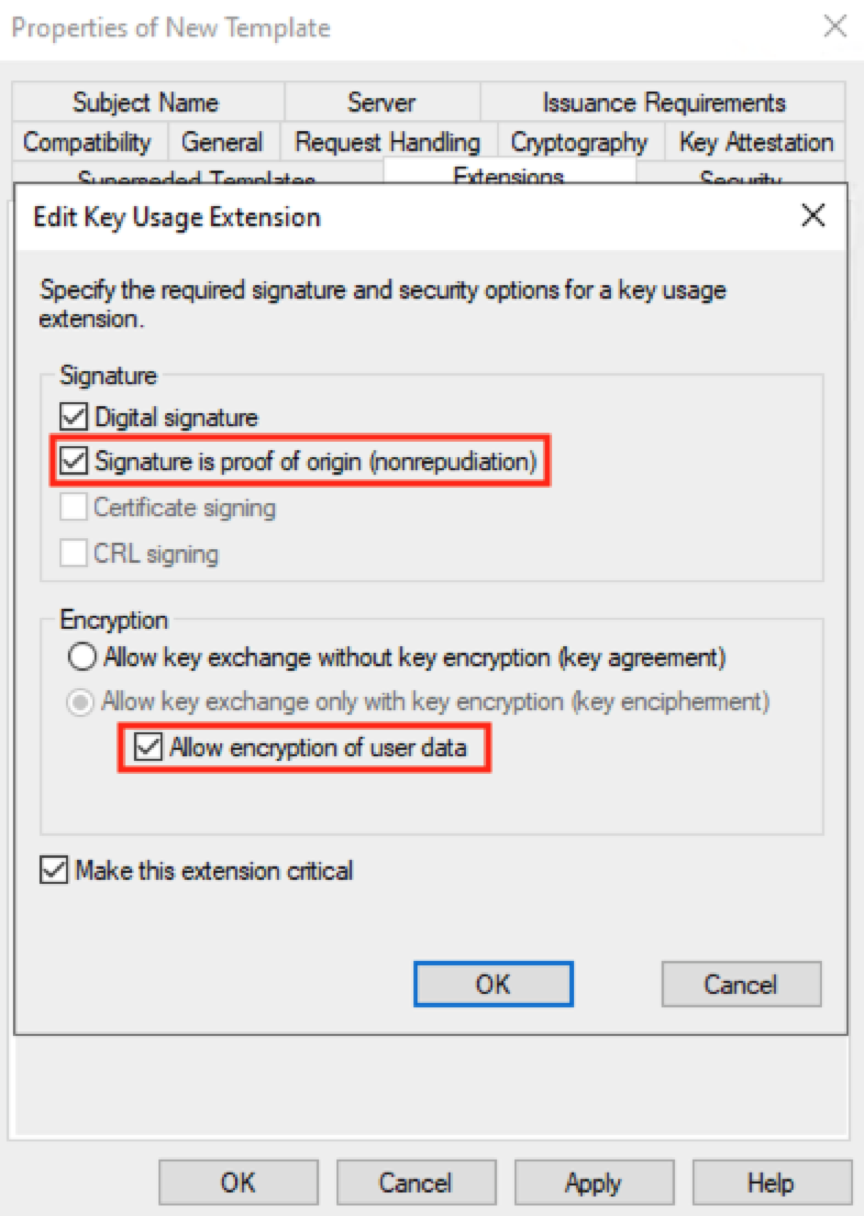
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Step 10. Enable nonrepudiation and encryption of user data. Click OK.



Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

Signature

☑ Digital signature

☑ Signature is proof of origin (nonrepudiation)

□ Certificate signing

□ CRL signing

Encryption

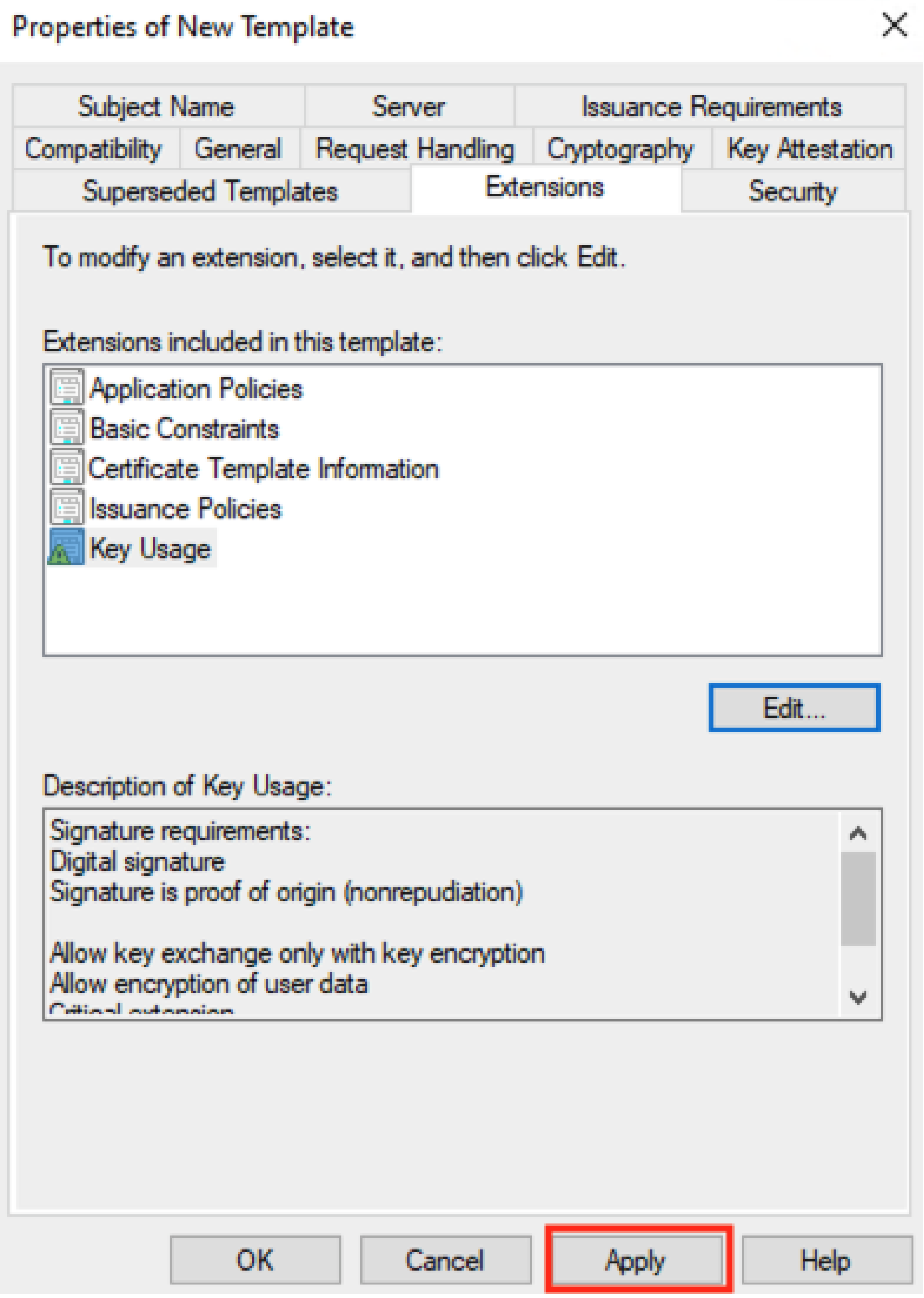
○ Allow key exchange without key encryption (key agreement)

● Allow key exchange only with key encryption (key encipherment)

☑ Allow encryption of user data

☑ Make this extension critical

Step 11. Click Apply.



To modify an extension, select it, and then click Edit.

Extensions included in this template:

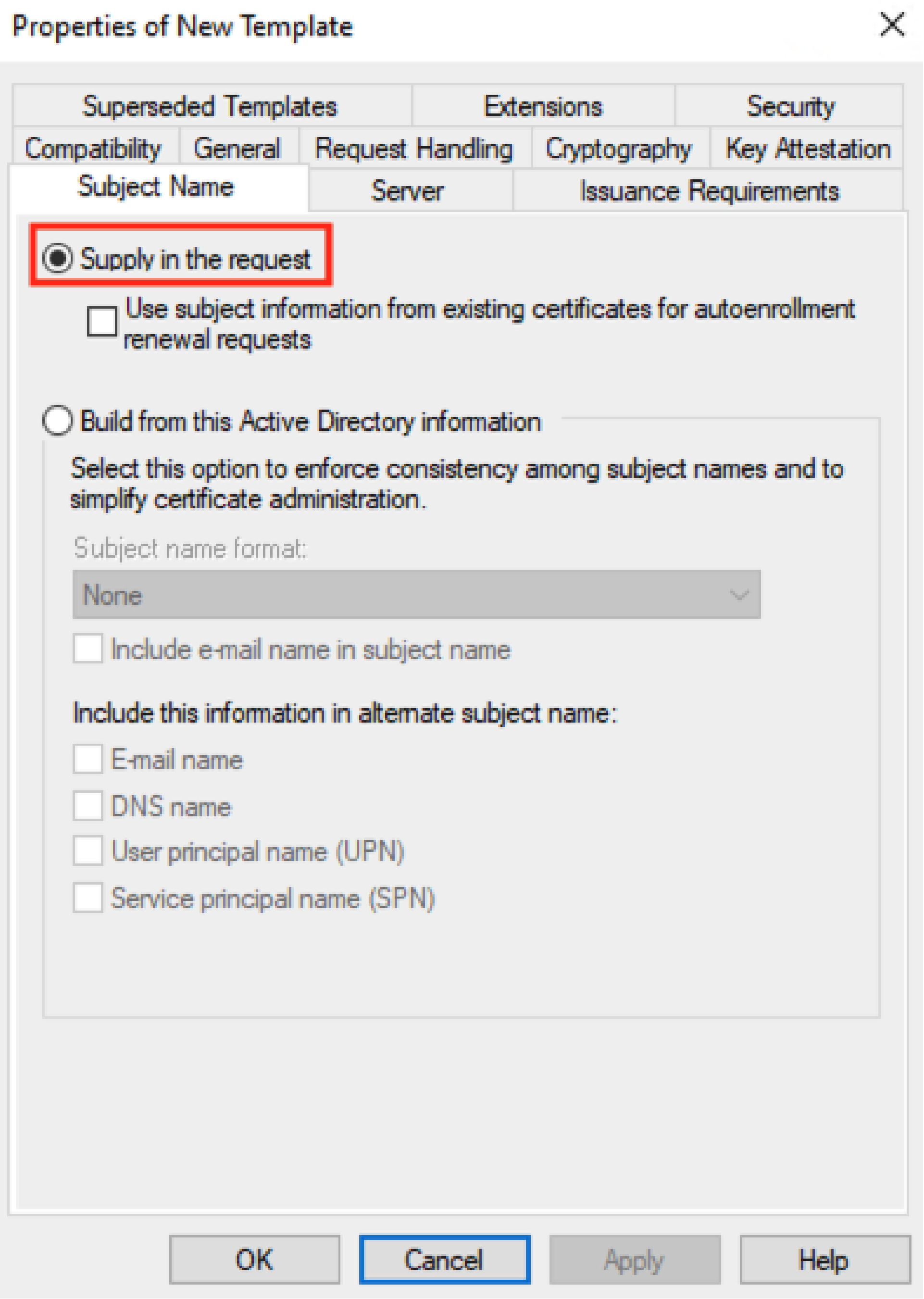
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Key Usage:

Signature requirements:
Digital signature
Signature is proof of origin (nonrepudiation)

Allow key exchange only with key encryption
Allow encryption of user data
Critical extension

Step 12. Click on the Subject Name tab and verify that ‘Supply in the request’ is selected. If it is not, select it. Click OK.



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

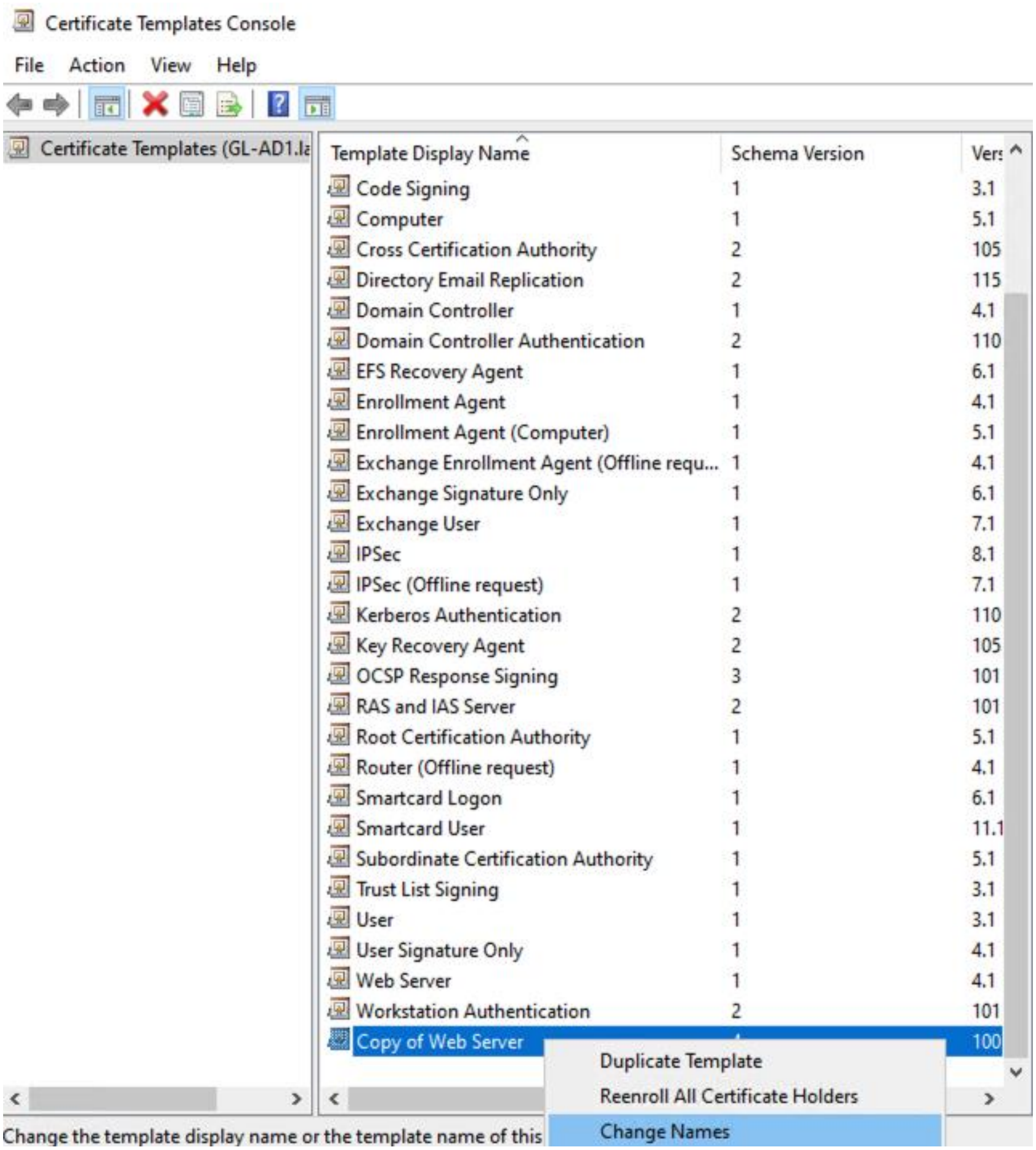
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

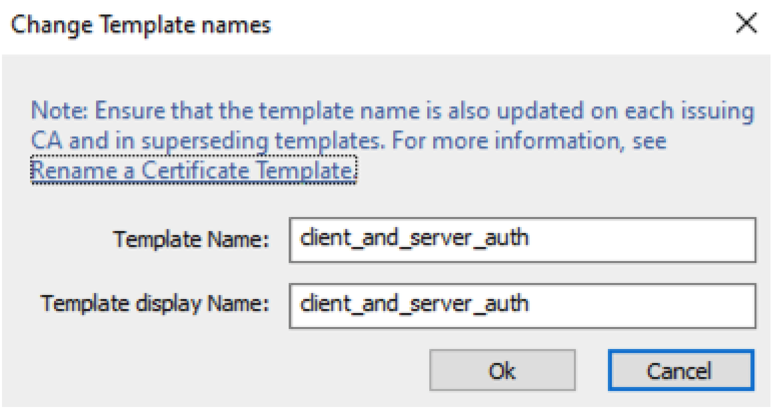
Step 13. Right click on the newly created copy and select Change Names.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (GL-AD1.la

Template Display Name	Schema Version	Vers
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	105
Directory Email Replication	2	115
Domain Controller	1	4.1
Domain Controller Authentication	2	110
EFS Recovery Agent	1	6.1
Enrollment Agent	1	4.1
Enrollment Agent (Computer)	1	5.1
Exchange Enrollment Agent (Offline requ...	1	4.1
Exchange Signature Only	1	6.1
Exchange User	1	7.1
IPSec	1	8.1
IPSec (Offline request)	1	7.1
Kerberos Authentication	2	110
Key Recovery Agent	2	105
OCSP Response Signing	3	101
RAS and IAS Server	2	101
Root Certification Authority	1	5.1
Router (Offline request)	1	4.1
Smartcard Logon	1	6.1
Smartcard User	1	11.1
Subordinate Certification Authority	1	5.1
Trust List Signing	1	3.1
User	1	3.1
User Signature Only	1	4.1
Web Server	1	4.1
Workstation Authentication	2	101
Copy of Web Server		100

Change the template display name or the template name of this

Step 14. Set a name, then click OK.

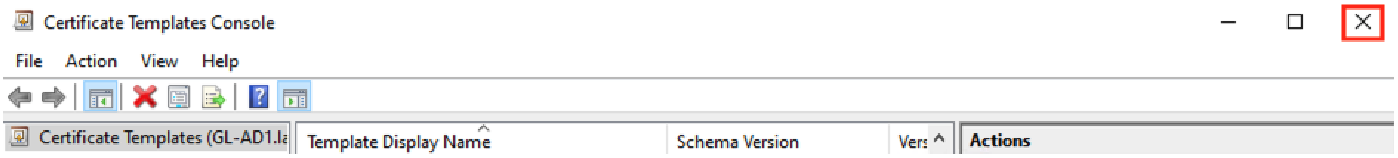


Note: Ensure that the template name is also updated on each issuing CA and in superseding templates. For more information, see Rename a Certificate Template

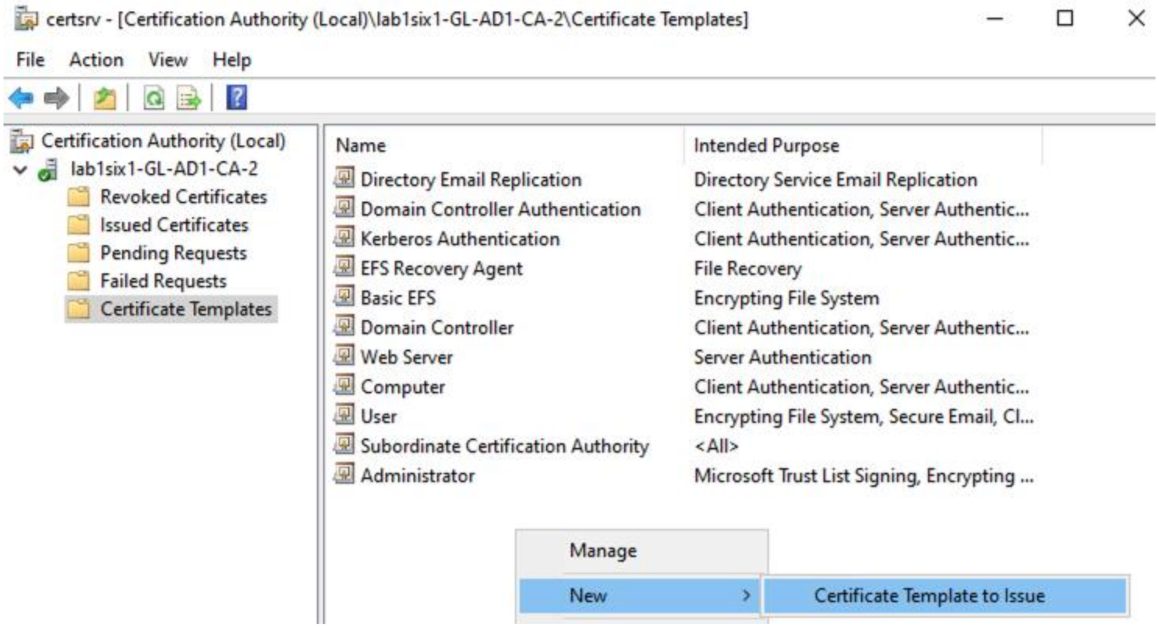
Template Name: client_and_server_auth

Template display Name: client_and_server_auth

Step 15. Close the Certificate Templates Console.

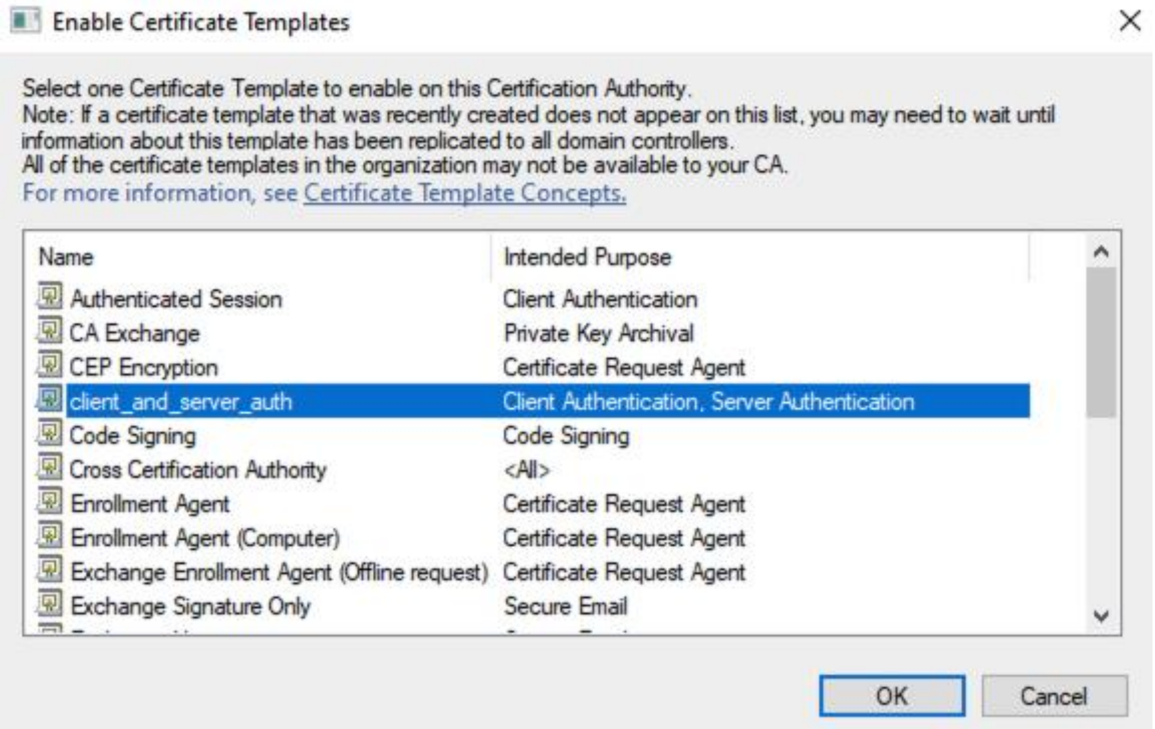


Step 16. Back on the Certificate Templates page, right-click the empty space in the right window and select New → Certificate Template to Issue.


certsrv - [Certification Authority (Local)\lab1six1-GL-AD1-CA-2\Certificate Templates]
File Action View Help
Certification Authority (Local)
lab1six1-GL-AD1-CA-2
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
Certificate Template to Issue

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

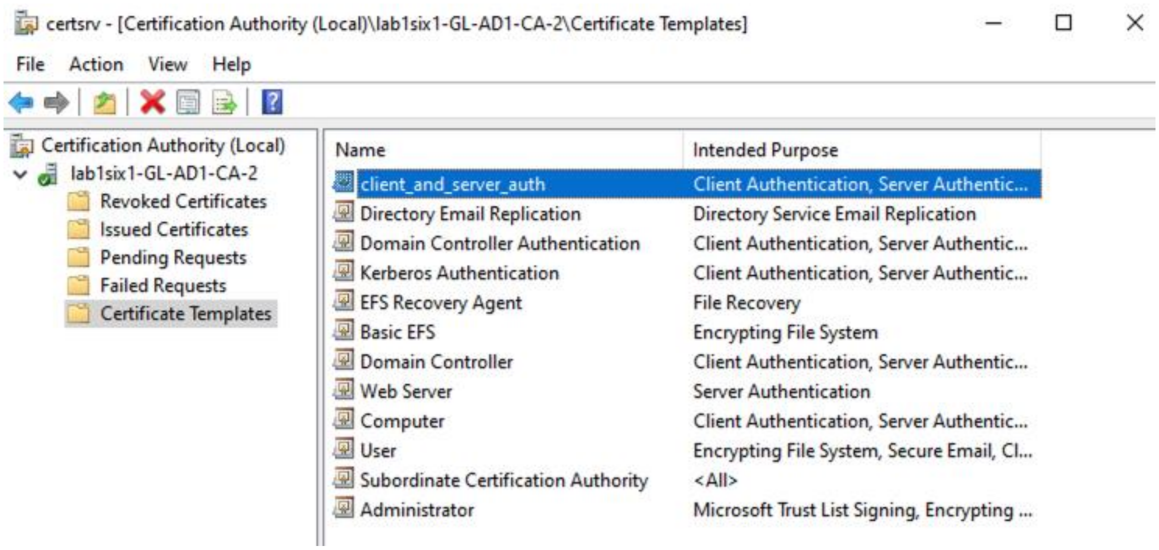
Step 17. Select the template created previously and click OK.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
client_and_server_auth	Client Authentication, Server Authentication
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email

Step 18. Verify the new template now appears in the list of Certificate Templates.

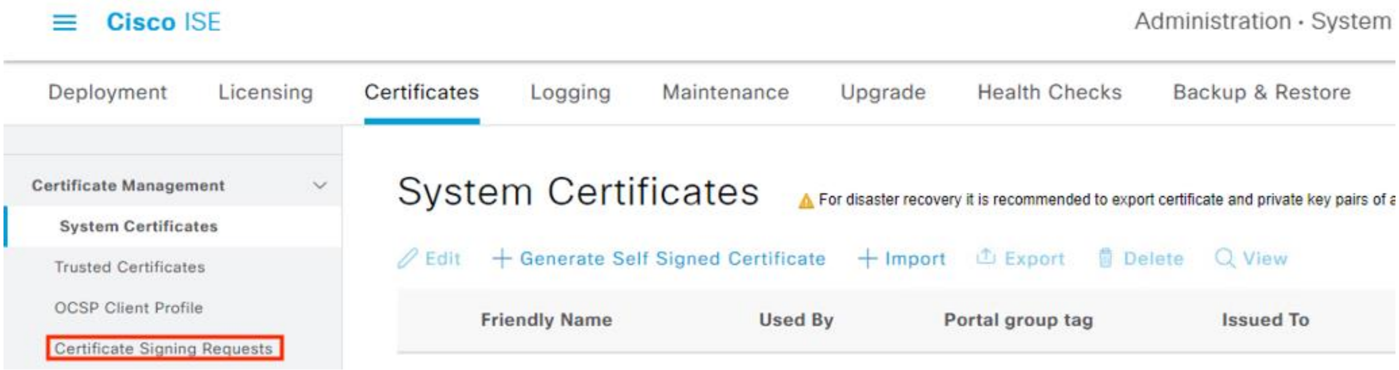


Name	Intended Purpose
client_and_server_auth	Client Authentication, Server Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

ISE: Generate Certificate Signing Request for the pxGrid Role

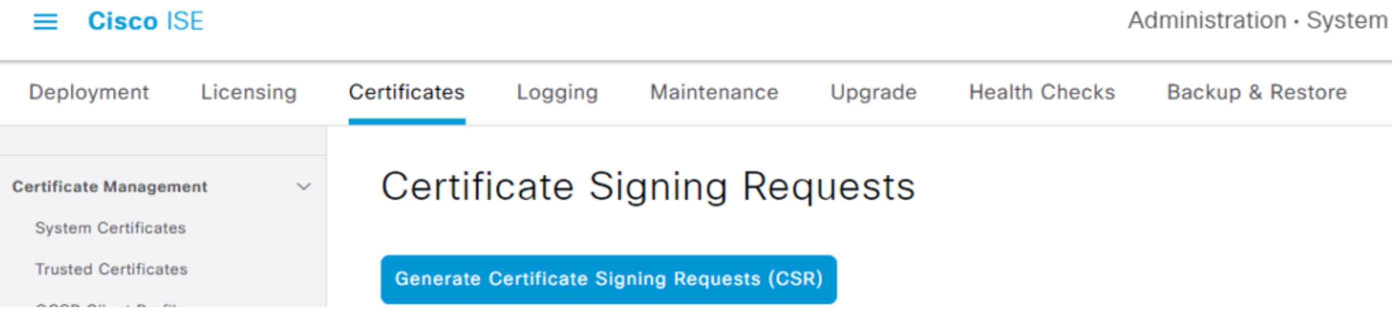
Step 1. In the Cisco ISE Graphical User Interface (GUI), click the Menu icon (≡) and choose Administration → System → Certificates.

Step 2. Click on Certificate Signing Requests in the left menu.



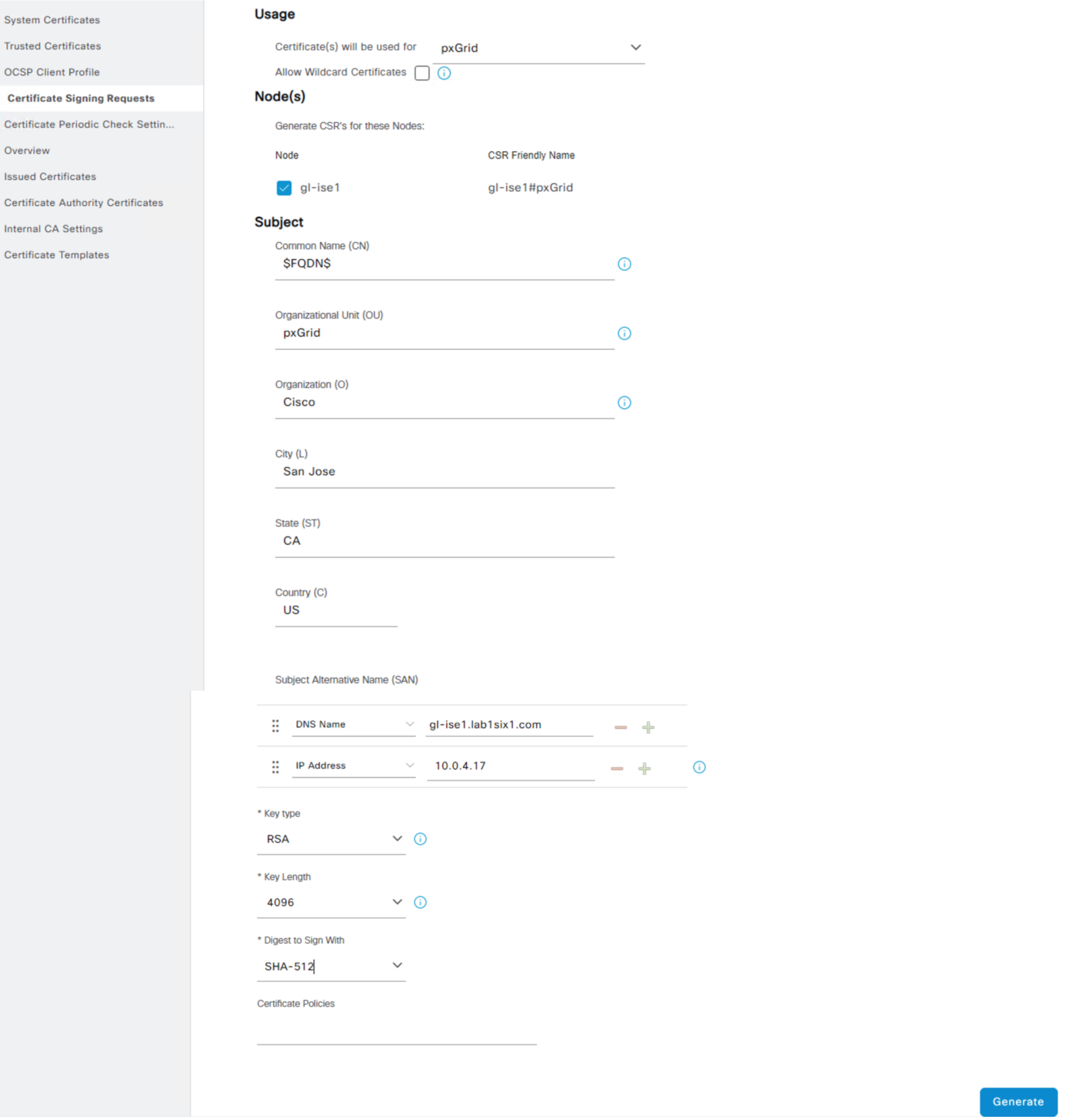
For disaster recovery it is recommended to export certificate and private key pairs of a

Step 2. Click the Generate Certificate Signing Requests button.



Step 3. Set the Certificate Usage to pxGrid, fill in Subject information, set SAN fields, and review Key Type, Length, and Digest. Click Generate when finished.

Note: ISE does not allow multiple certificates with the same Subject fields. In the example below, pxGrid is set as the OU to create a unique Subject combination.



Usage

Certificate(s) will be used for: pxGrid

Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ gl-ise1	gl-ise1#pxGrid

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU): pxGrid

Organization (O): Cisco

City (L): San Jose

State (ST): CA

Country (C): US

Subject Alternative Name (SAN)

DNS Name	gl-ise1.lab1six1.com
IP Address	10.0.4.17

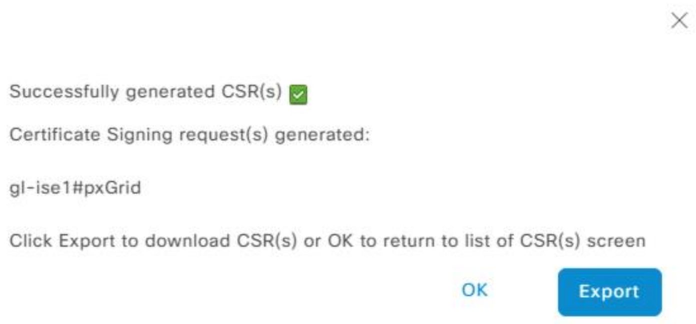
* Key type: RSA

* Key Length: 4096

* Digest to Sign With: SHA-512

Certificate Policies

Step 4. Export the CSR file.



Successfully generated CSR(s) ✓

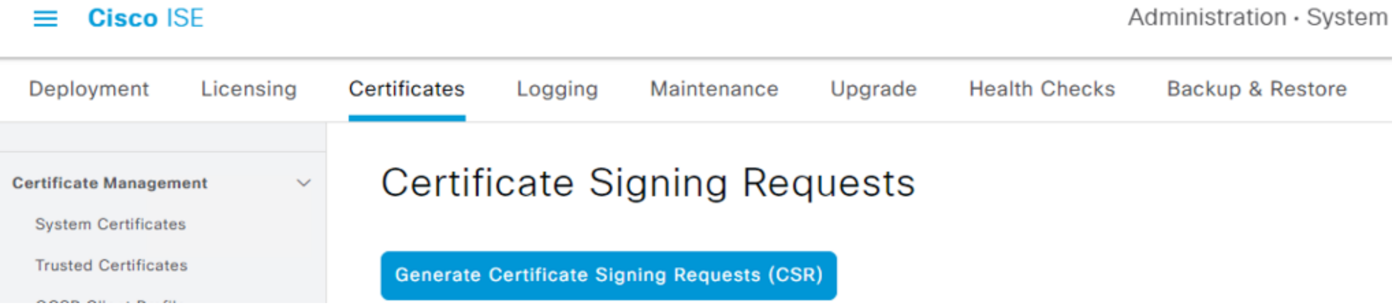
Certificate Signing request(s) generated:

gl-ise1#pxGrid

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

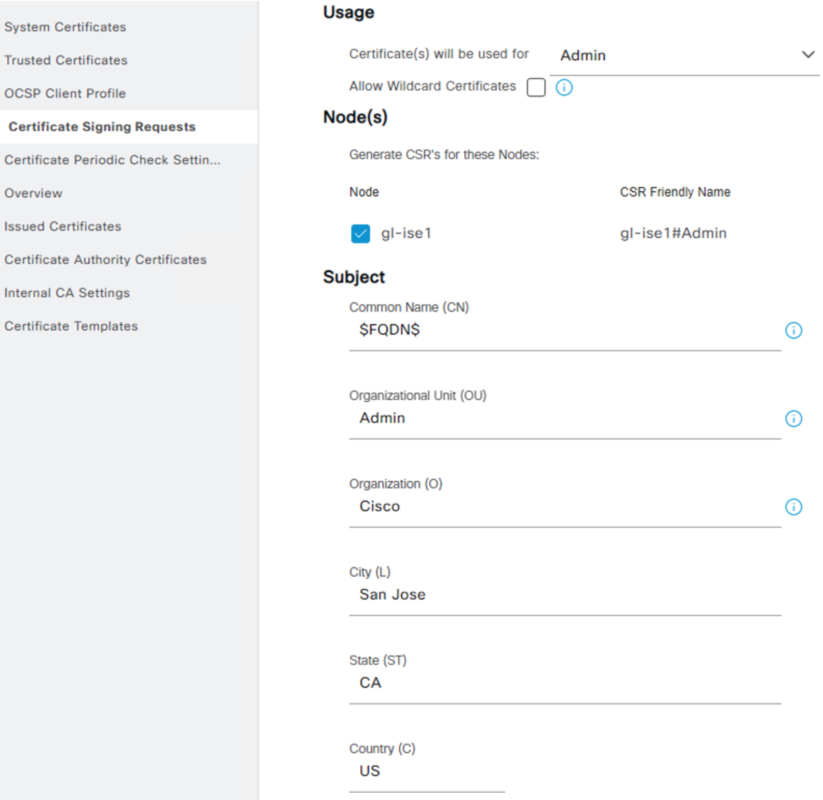
ISE: Generate Certificate Signing Request for the Admin Role

Step 1. Continuing from the prior section (Administration → System → Certificates → Certificate Signing Requests) click the Generate Certificate Signing Requests button.



Step 2. Set the Certificate Usage to pxGrid, fill in Subject information, set SAN fields, and review Key Type, Length, and Digest. Click Generate when finished.

Note: ISE does not allow multiple certificates with the same Subject fields. In the example below, Admin is set as the OU to create a unique Subject combination.



Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ gl-ise1	gl-ise1#Admin

Subject

Common Name (CN): $FQDN$

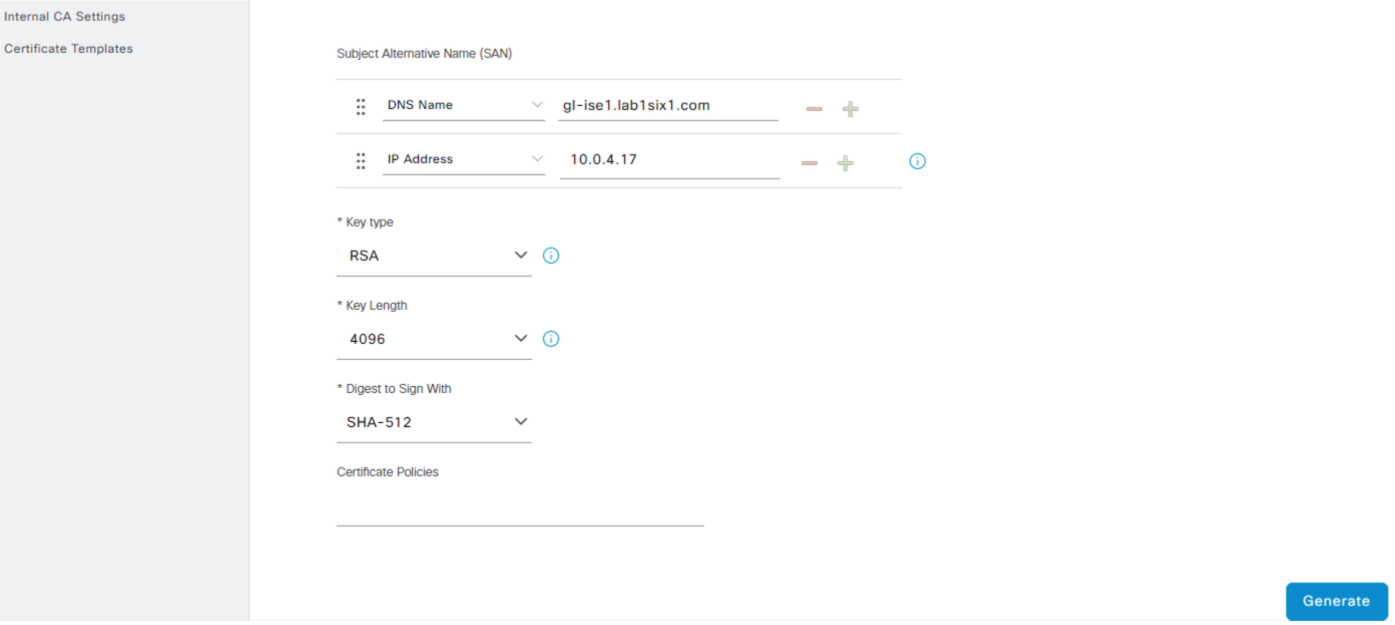
Organizational Unit (OU): Admin

Organization (O): Cisco

City (L): San Jose

State (ST): CA

Country (C): US



Subject Alternative Name (SAN)

DNS Name	gl-ise1.lab1six1.com
IP Address	10.0.4.17

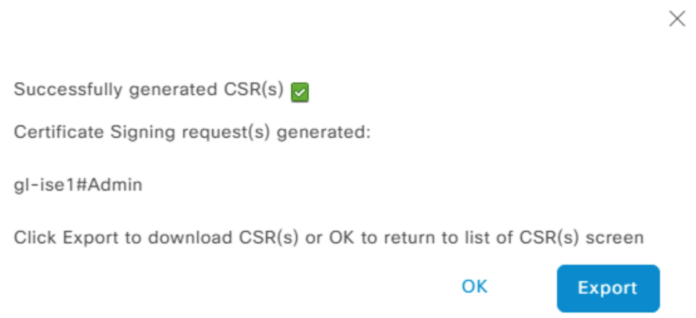
* Key type: RSA

* Key Length: 4096

* Digest to Sign With: SHA-512

Certificate Policies

Step 3. Export the file.



Successfully generated CSR(s) ✓

Certificate Signing request(s) generated:

gl-ise1#Admin

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

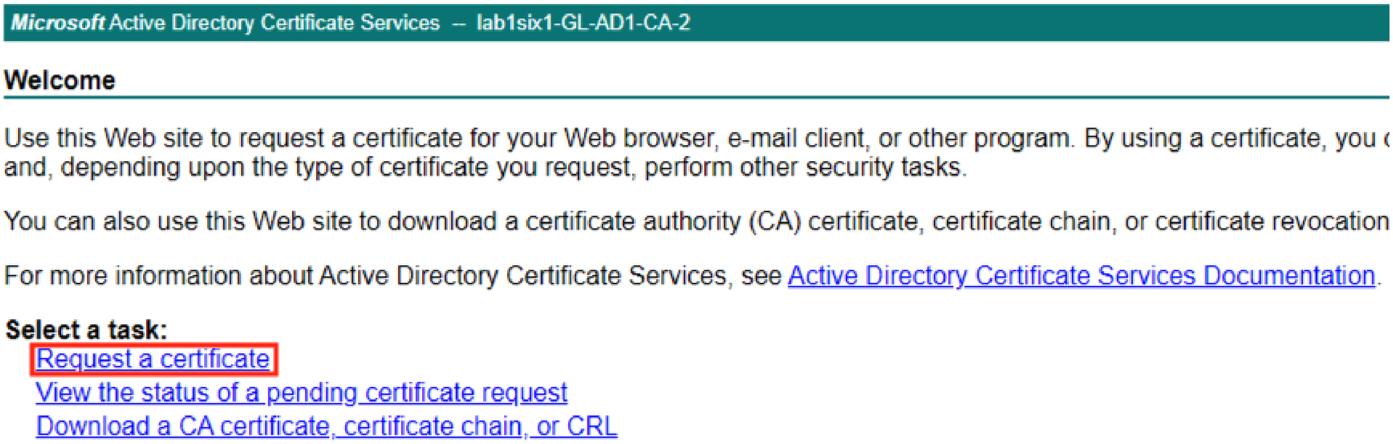
Active Directory: Create Certificates from Certificate Signing Requests

Before starting this section, generate CSRs using the steps in the prior section (or other methods such as OpenSSL, if preferred).

Step 1. Access the CA server by appending /certsrv/ to the AD server hostname, e.g.

- **adserver.example.com**
- **adserver.example.com/certsrv/**

Step 2. From the CA server, click the Request a certificate link.



Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

Welcome

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

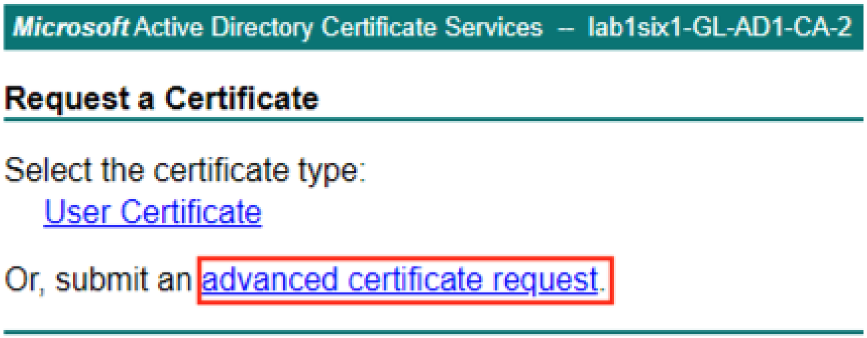
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation

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

Step 3. Select the advanced certificate request option.



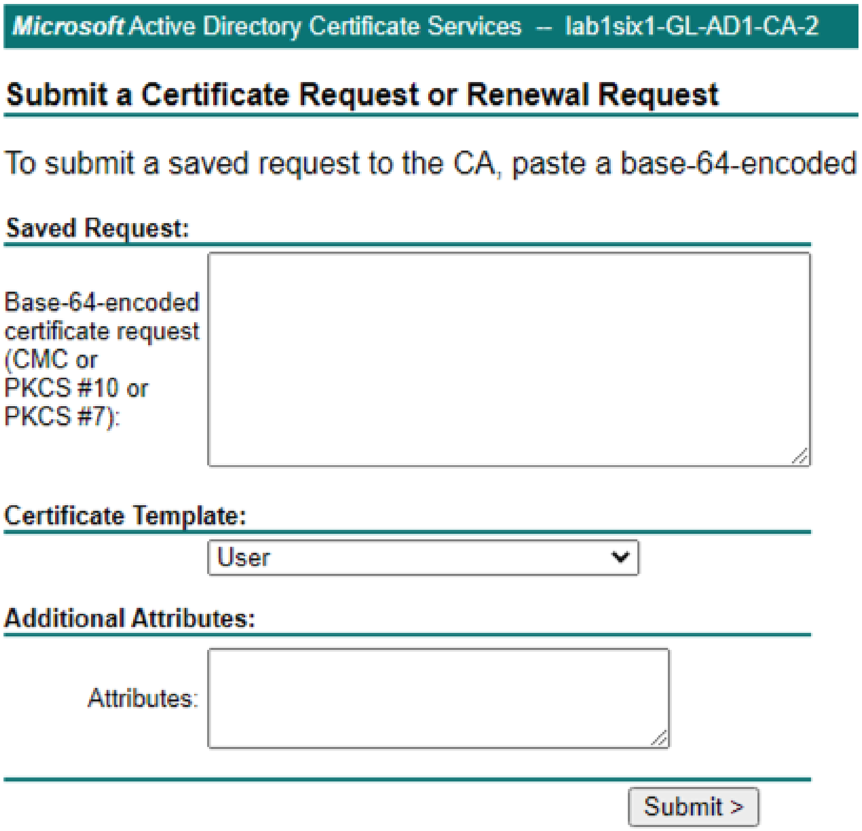
Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

The advanced certificate request page prompts for entry of a CSR in text format.



Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded

Saved Request:

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

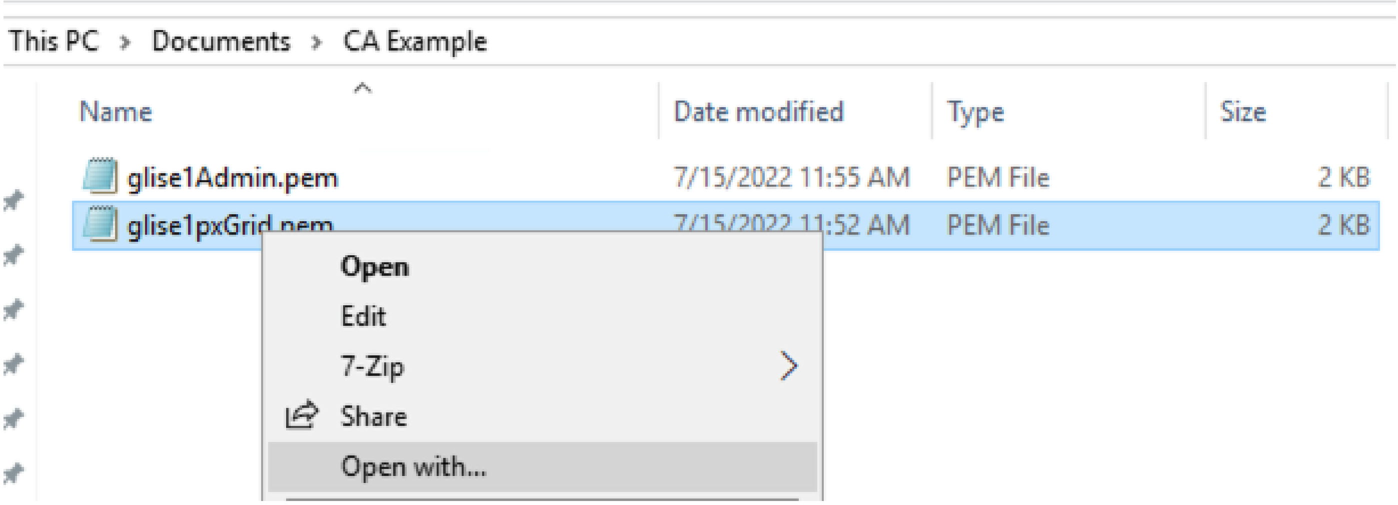
Certificate Template:

User

Additional Attributes:

Attributes:

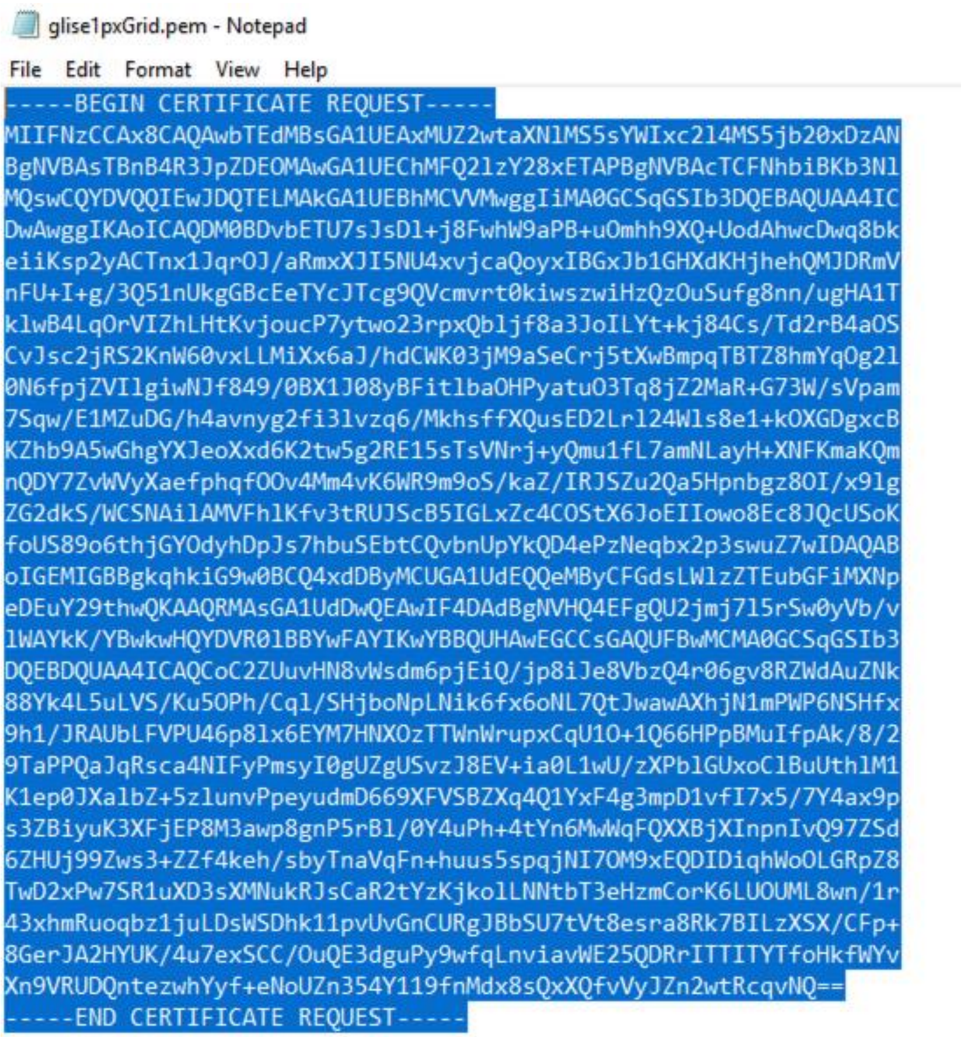
Step 4. Locate the CSR file to upload and open with a text editor (right-click the CSR file and select 'Open with...' if the CSR is not associated with a text editor by default).



This PC > Documents > CA Example

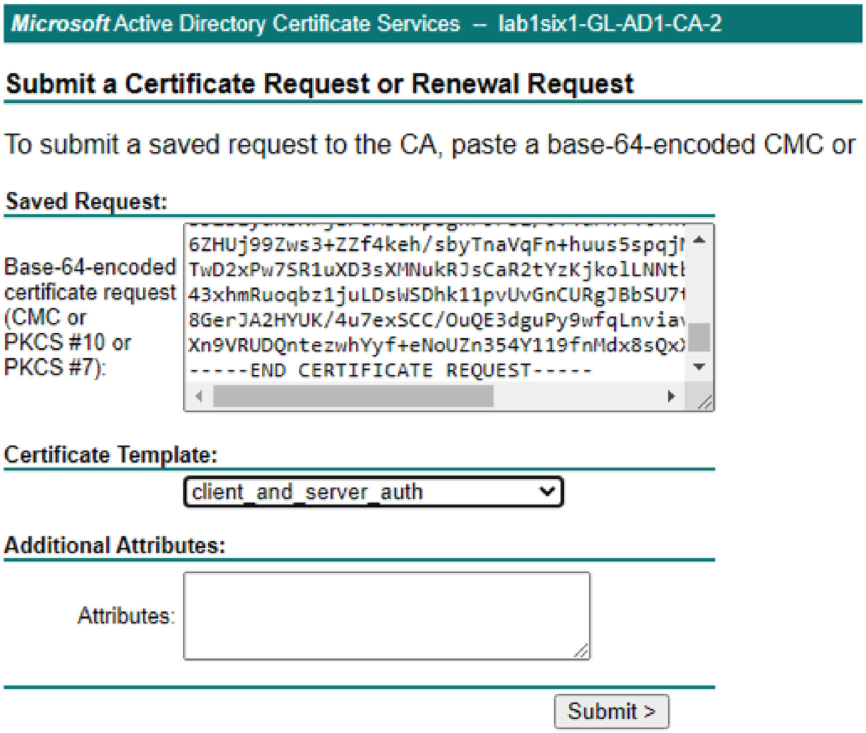
Name	Date modified	Type	Size
glise1Admin.pem	7/15/2022 11:55 AM	PEM File	2 KB
glise1pxGrid.pem	7/15/2022 11:52 AM	PEM File	2 KB

Step 5. Copy the entire block of text starting with the BEGIN line and ending with the END line.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIFNzCCAx8CAQAwbTEdMBsGA1UEAxMUZ2wtaXNlMS5sYWIxc2l4MS5jb20xDzAN
BgNVBAsTBnB4R3JpZDEOMAwGA1UEChMFQ2lzY28xETAPBgNVBAcTCFNhbiBKb3Nl
MQswCQYDVQQIEwJDQTELMAkGA1UEBhMCVVMwggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQDM0BDvbETU7sJsDl+j8FwhW9aPB+uOmhh9XQ+UodAhwcDwq8bk
eiiKsp2yACTnx1JqrOJ/aRmxXJI5NU4xvjcaQoyxIBGxJb1GHXdKHjhehQMJDRmV
nFU+I+g/3Q51nUkgGBcEeTYcJTcg9QVcmvrt0kiwszwiHzQzOuSufg8nn/ugHA1T
klwB4LqOrVIZhLHtKvjoucP7ytwo23rpxQbljf8a3JoILYt+kj84Cs/Td2rB4aOS
CvJsc2jRS2KnW60vxLLMiXx6aJ/hdCWK03jM9aSeCrj5tXwBmpqTBTZ8hmYqOg2l
0N6fpjZVIlgiwNJf849/0BX1J08yBFitlbaOHPyatuO3Tq8jZ2MaR+G73W/sVpam
7Sqw/E1MZuDG/h4avnyg2fi3lvzq6/MkhsffXQusED2Lrl24Wls8e1+kOXGDgxcB
KZhb9A5wGhgYXJeoXxd6K2tw5g2RE15sTsVNrj+yQmu1fL7amNLayH+XNFKmaKQm
nQDY7ZvWVyXaefphqfOOv4Mm4vK6WR9m9oS/kaZ/IRJSZu2Qa5Hpnbgz8OI/x9lg
ZG2dkS/WCSNAilAMVFhlKfv3tRUJScB5IGLxZc4COStX6JoEIIowo8Ec8JQcUSoK
foUS89o6thjGYOdyhDpJs7hbuSEbtCQvbnUpYkQD4ePzNeqbx2p3swuZ7wIDAQAB
oIGEMIGBBgkqhkiG9w0BCQ4xdDByMCUGA1UdEQQeMByCFGdsLWlzZTEubGFiMXNp
eDEuY29thwQKAAQRMAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw0yVb/v
lWAYkK/YBwkwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA0GCSqGSIb3
DQEBDQUAA4ICAQCoC2ZUuvHN8vWsdm6pjEiQ/jp8iJe8VbzQ4r06gv8RZWdAuZNk
88Yk4L5uLVS/Ku5OPh/Cql/SHjboNpLNik6fx6oNL7QtJwawAXhjN1mPWP6NSHfx
9h1/JRAUbLFVPU46p8lx6EYM7HNXOzTTWnWrupxCqU1O+1Q66HPpBMuIfpAk/8/2
9TaPPQaJqRsca4NIFyPmsyI0gUZgUSvzJ8EV+ia0L1wU/zXPblGUxoClBuUthlM1
K1ep0JXalbZ+5zlunvPpeyudmD669XFVSBZXq4Q1YxF4g3mpD1vfI7x5/7Y4ax9p
s3ZBiyuK3XFjEP8M3awp8gnP5rBl/0Y4uPh+4tYn6MwWqFQXXBjXInpnIvQ97ZSd
6ZHUj99Zws3+ZZf4keh/sbyTnaVqFn+huus5spqjNI7OM9xEQDIDiqhWoOLGRpZ8
TwD2xPw7SR1uXD3sXMNukRJsCaR2tYzKjkolLNNtbT3eHzmCorK6LUOUML8wn/1r
43xhmRuoqbz1juLDsWSDhk11pvUvGnCURgJBbSU7tVt8esra8Rk7BILzXSX/CFp+
8GerJA2HYUK/4u7exSCC/OuQE3dguPy9wfqLnviavWE25QDRrITTITYTfoHkfWYv
Xn9VRUDQntezwhYyf+eNoUZn354Y119fnMdx8sQxXQfvVyJZn2wtRcqvNQ==
-----END CERTIFICATE REQUEST-----
```

Step 6. Return to the CA server and paste the copied text into the Request field. Set the Certificate Template to the one configured in the prior Create a Client and Server Authentication Template section. Click Submit.



Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or

Saved Request:

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

```
6ZHUj99Zws3+ZZf4keh/sbyTnaVqFn+huus5spqj
TwD2xPw7SR1uXD3sXMNukRJsCaR2tYzKjkolLNNt
43xhmRuoqbz1juLDsWSDhk11pvUvGnCURgJBbSU7
8GerJA2HYUK/4u7exSCC/OuQE3dguPy9wfqLnvia
Xn9VRUDQntezwhYyf+eNoUZn354Y119fnMdx8sQx
-----END CERTIFICATE REQUEST-----
```

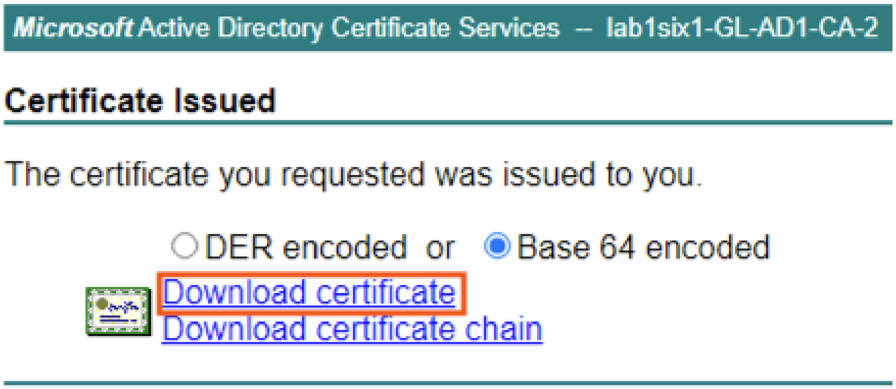
Certificate Template:

client_and_server_auth

Additional Attributes:

Attributes:

Step 7. Select Base 64 encoded and click either the Download certificate or Download certificate chain option. It is recommended to rename the file to denote the certificate type (in this case, the Admin certificate). This example uses the ‘Download certificate’ option for simplicity, as AD generates the certificate in .cer format, which can be imported directly into ISE. The chain option generates the certificate in .p7b format, which requires conversion to an ISE compatible format via OpenSSL.



Microsoft Active Directory Certificate Services -- lab1six1-GL-AD1-CA-2

Certificate Issued

The certificate you requested was issued to you.

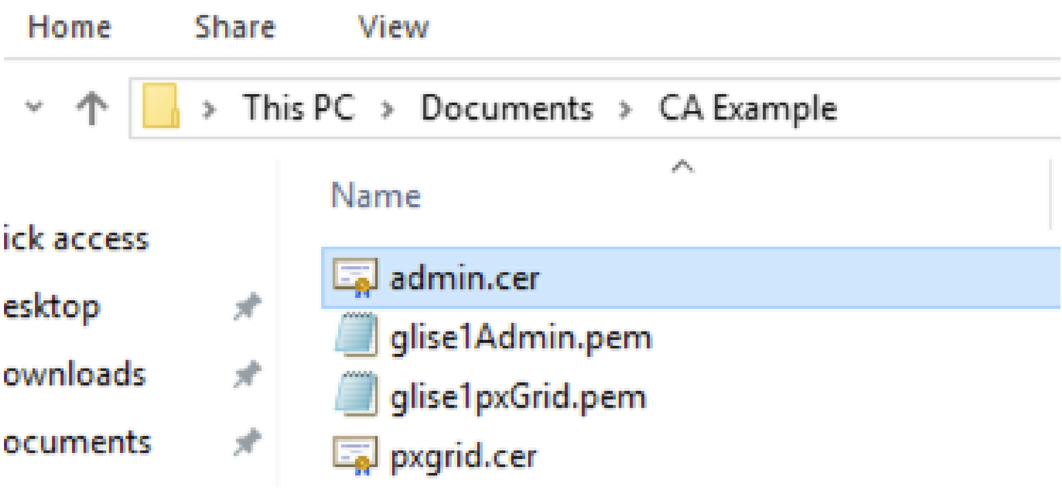
○ DER encoded or ● Base 64 encoded

Step 8. Repeat the above steps to generate the pxGrid certificate, which also uses the client_and_server_auth template.

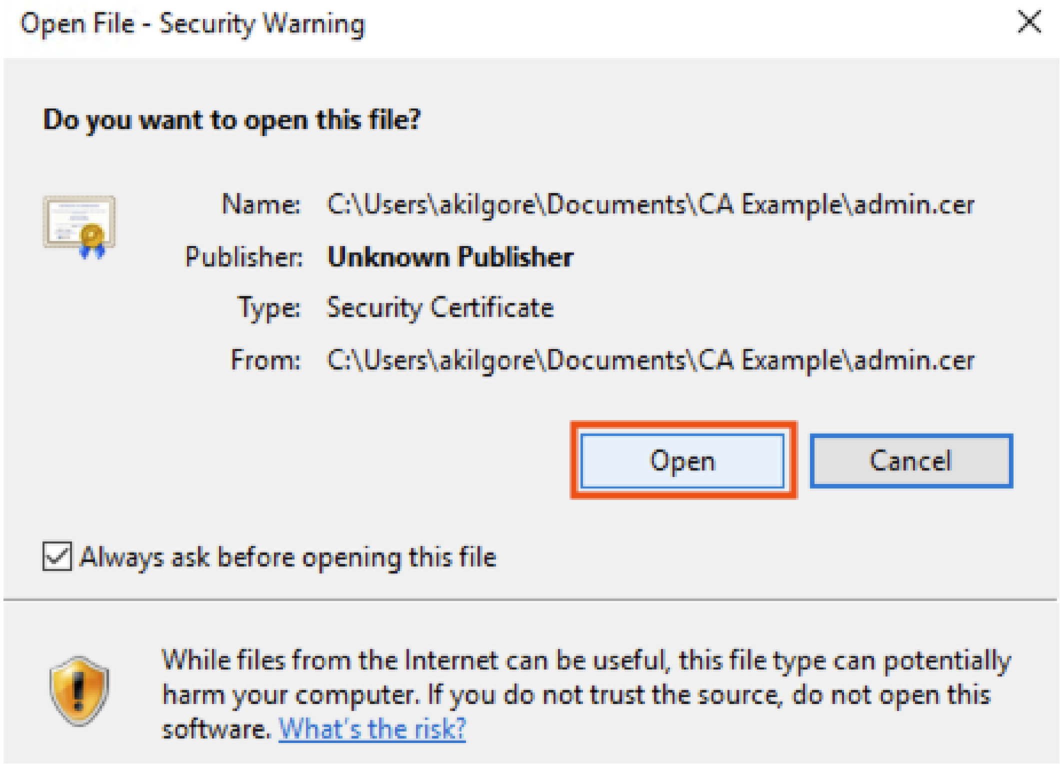
Windows: Verify Certificate Details

Step 1. Double click the newly created certificate to open it.

Note: Only the .cer format will open using this method; the .p7b format created from the chain option will not.



Step 2. If a Security Warning prompt appears, click Open.



Open File - Security Warning

Do you want to open this file?

Name: C:\Users\akilgore\Documents\CA Example\admin.cer

Publisher: **Unknown Publisher**

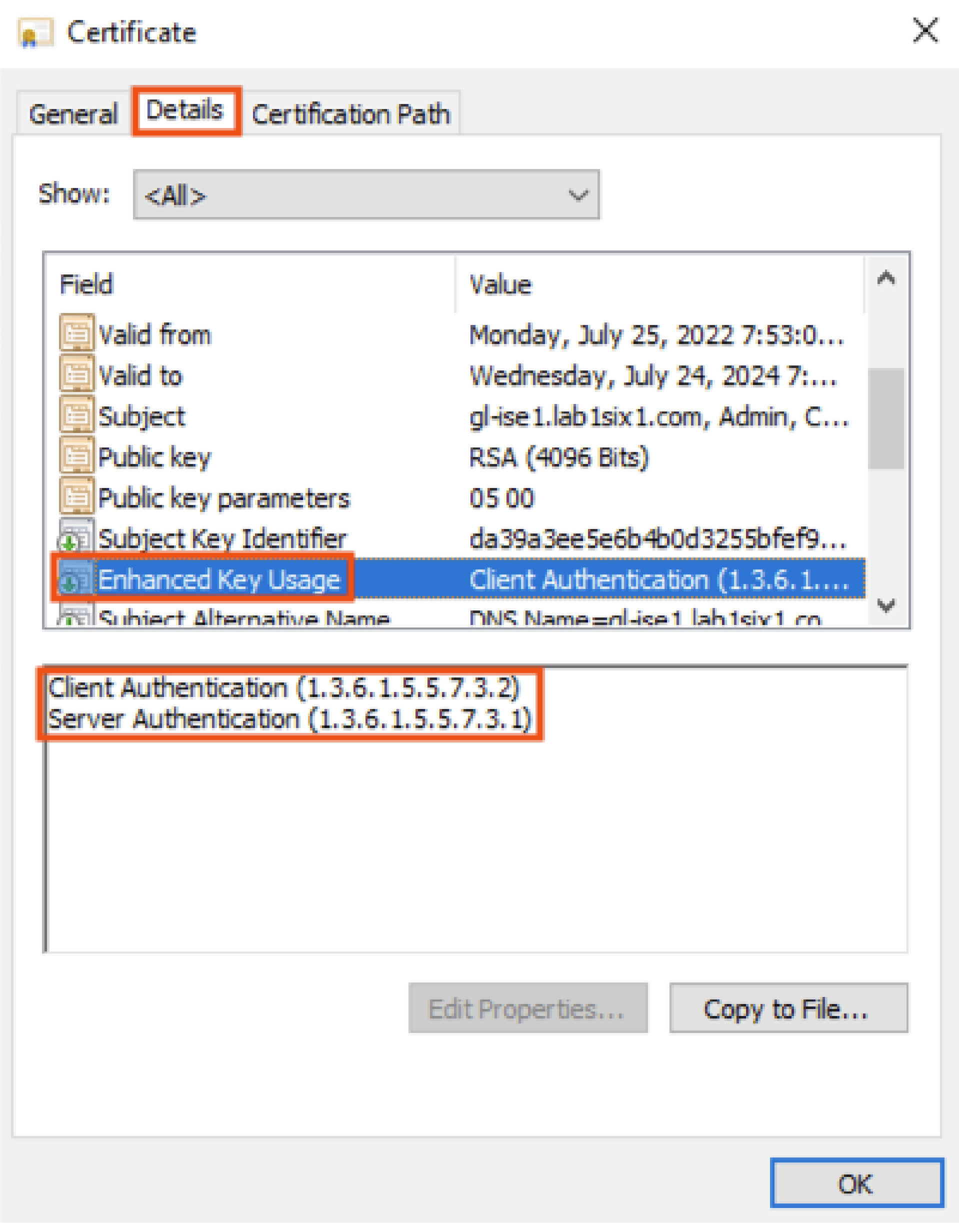
Type: Security Certificate

From: C:\Users\akilgore\Documents\CA Example\admin.cer

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Step 3. Click the Details tab and select Enhanced Key Usage. Verify that both Client Authentication and Server Authentication are available. Click OK to close.



Field	Value
Valid from	Monday, July 25, 2022 7:53:0...
Valid to	Wednesday, July 24, 2024 7:...
Subject	gl-ise1.lab1six1.com, Admin, C...
Public key	RSA (4096 Bits)
Public key parameters	05 00
Subject Key Identifier	da39a3ee5e6b4b0d3255bfef9...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Subject Alternative Name	DNS Name=gl-ise1.lab1six1.co

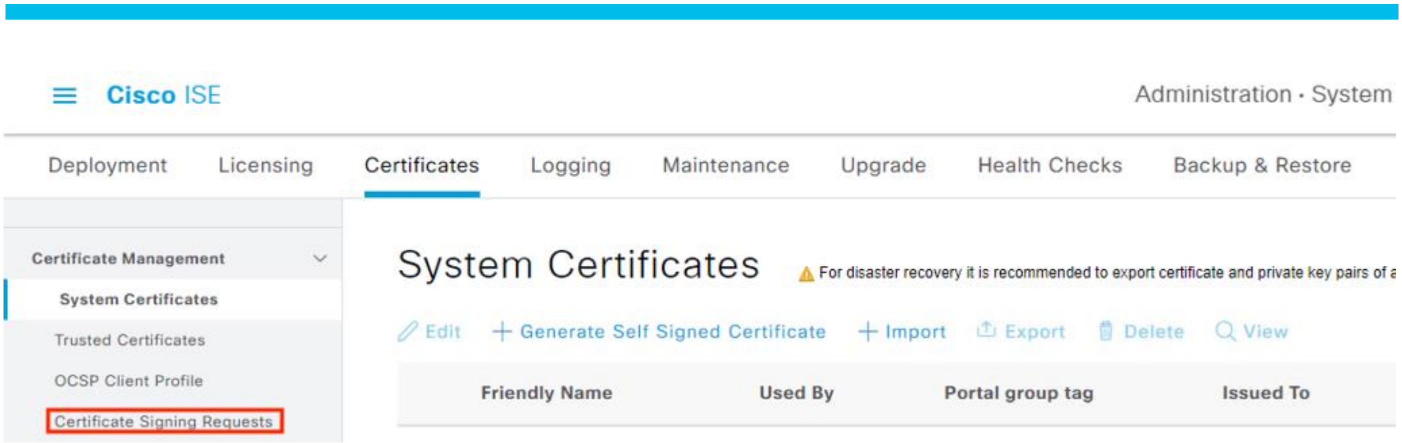
Client Authentication (1.3.6.1.5.5.7.3.2)
Server Authentication (1.3.6.1.5.5.7.3.1)

ISE: Bind Certificates to CSR Requests and Assign Certs to Roles

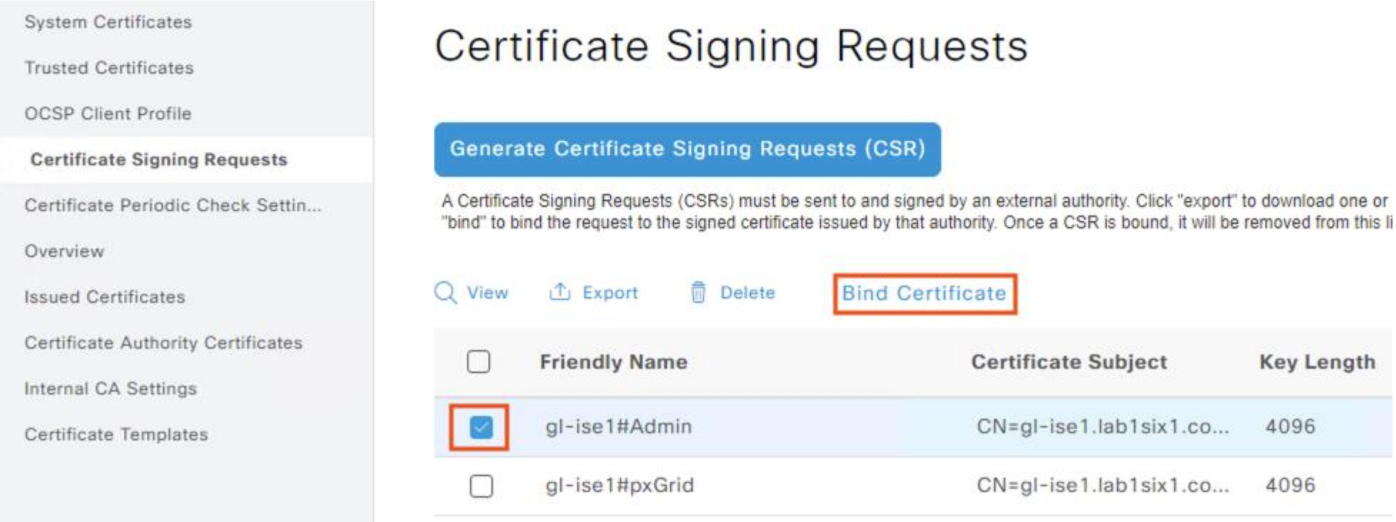
Before starting, note that changing the Admin certificate will cause the application server to restart.

Step 1. Click the Menu icon (☰) and navigate to Administration → System → Certificates.

Step 2. Click on Certificate Signing Requests.



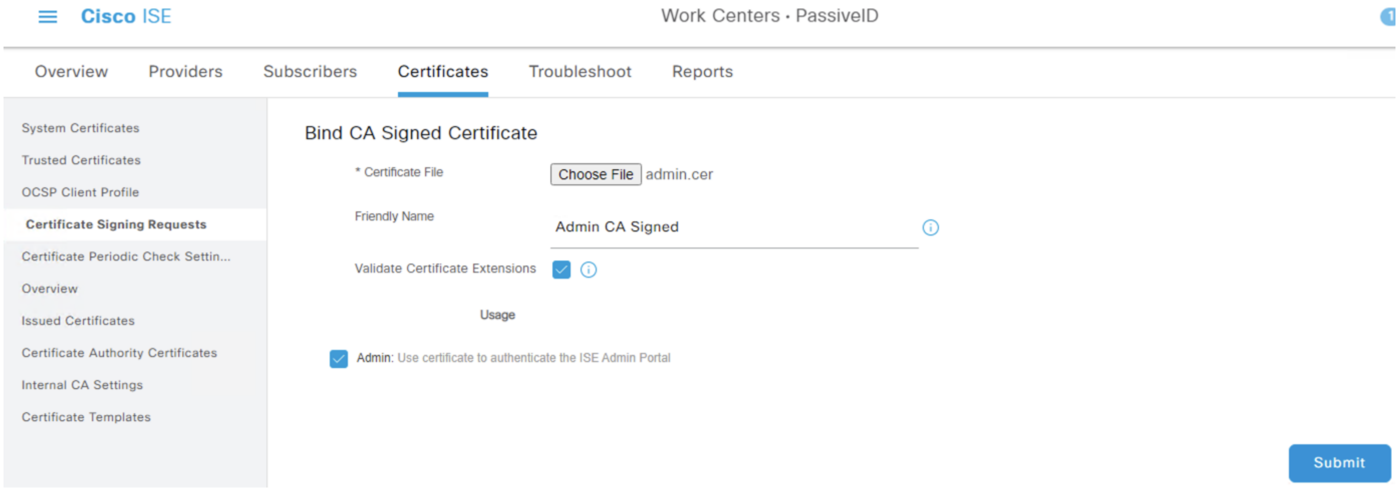
Step 3. Locate the CSRs created in the Generate Certificate Signing Requests step. Check the box next to the Admin entry, then click Bind Certificate (the bind action will bind the generated certificate to the private key ISE created when the CSR was made).


System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settin...
Overview
Issued Certificates
Certificate Authority Certificates
Internal CA Settings
Certificate Templates
Certificate Signing Requests
Generate Certificate Signing Requests (CSR)
View
Export
Delete
Bind Certificate

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this li

□	Friendly Name	Certificate Subject	Key Length
☑	gl-ise1#Admin	CN=gl-ise1.lab1six1.co...	4096
□	gl-ise1#pxGrid	CN=gl-ise1.lab1six1.co...	4096

Step 4. Click the Choose File button and upload the Admin Certificate created in the Create Certificates from CSRs step. Enter a Friendly Name for the certificate and check the Validate Certificate Extensions box. Click Submit.



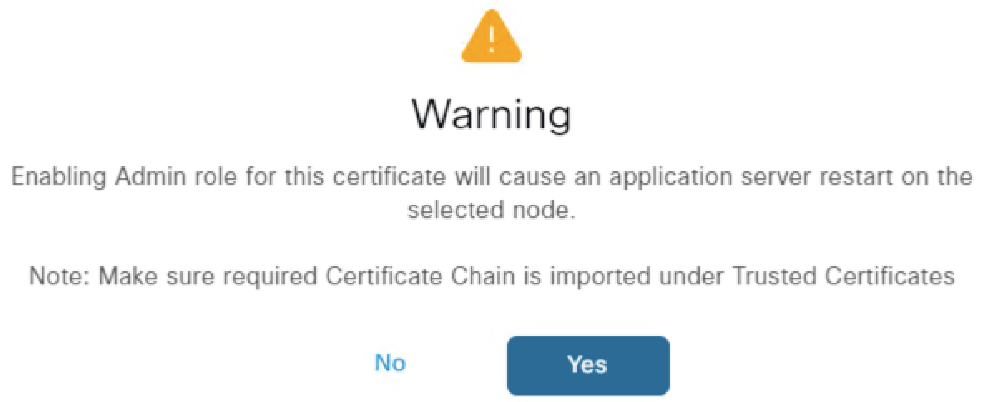
* Certificate File: Choose File admin.cer

Friendly Name: Admin CA Signed

Validate Certificate Extensions ☑

☑ Admin: Use certificate to authenticate the ISE Admin Portal

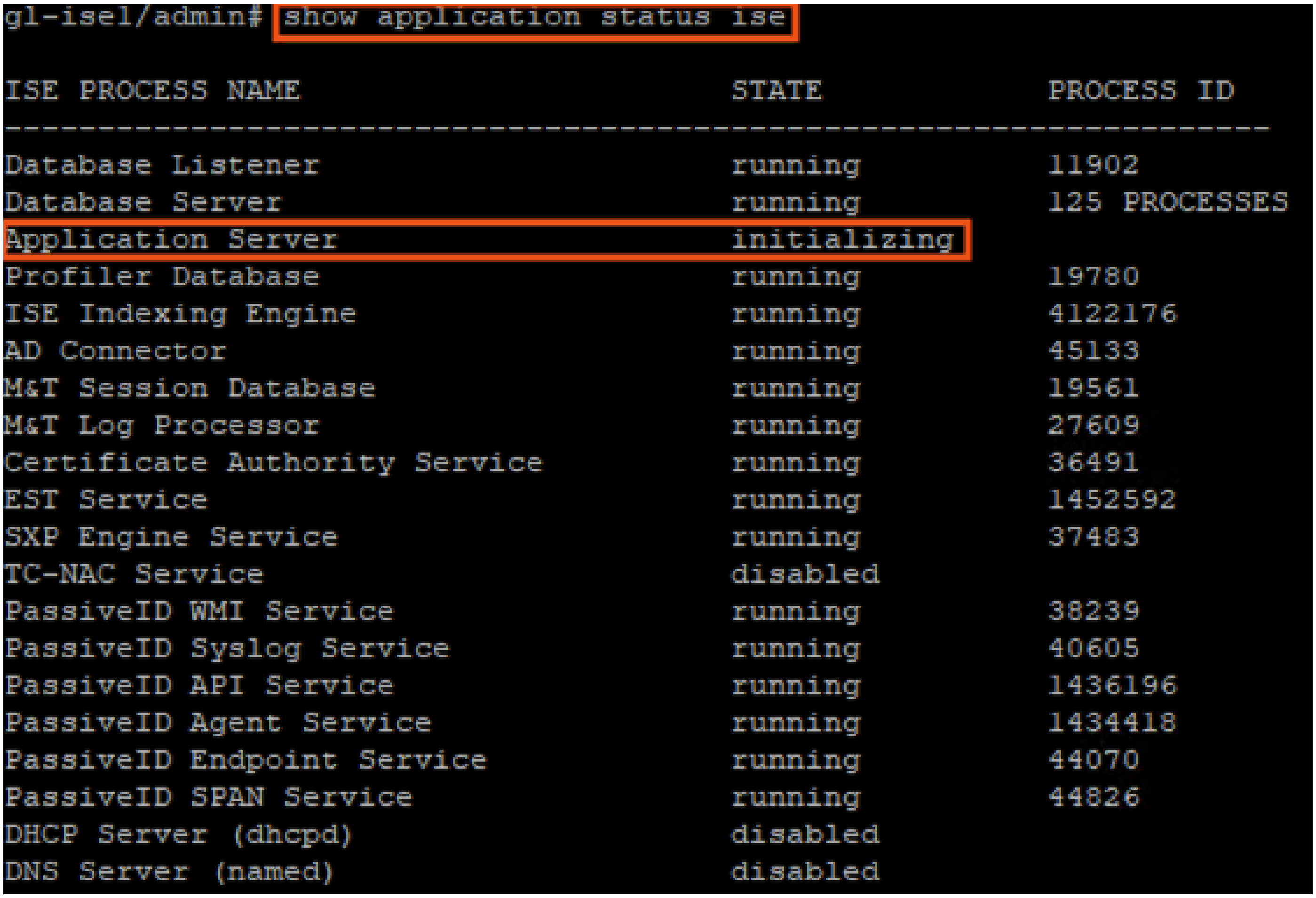
Step 5. An alert will appear stating that changing the Admin certificate will restart the application server. If a service outage is currently acceptable for the node, select Yes. If not, click No and reschedule for a change window.


Warning

Enabling Admin role for this certificate will cause an application server restart on the selected node.

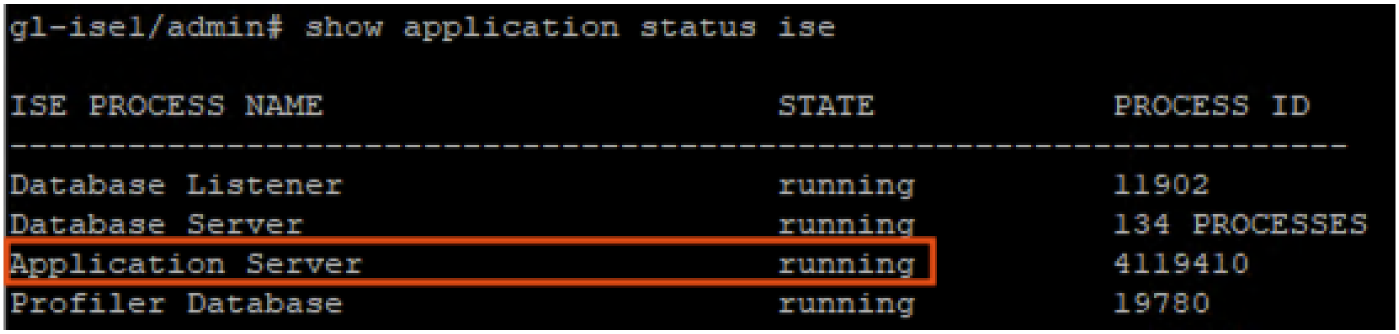
Note: Make sure required Certificate Chain is imported under Trusted Certificates

Step 6. To verify when the Application Server is up, access the ISE node Command Line Interface (CLI) and run the command ‘show application status ise’. The screenshot below shows output for the Application Server in an Initializing state.



```
gl-ise1/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          11902
Database Server                        running          125 PROCESSES
Application Server                     initializing
Profiler Database                      running          19780
ISE Indexing Engine                    running          4122176
AD Connector                           running          45133
M&T Session Database                   running          19561
M&T Log Processor                      running          27609
Certificate Authority Service          running          36491
EST Service                            running          1452592
SXP Engine Service                     running          37483
TC-NAC Service                         disabled
PassiveID WMI Service                  running          38239
PassiveID Syslog Service               running          40605
PassiveID API Service                  running          1436196
PassiveID Agent Service                running          1434418
PassiveID Endpoint Service             running          44070
PassiveID SPAN Service                 running          44826
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
```

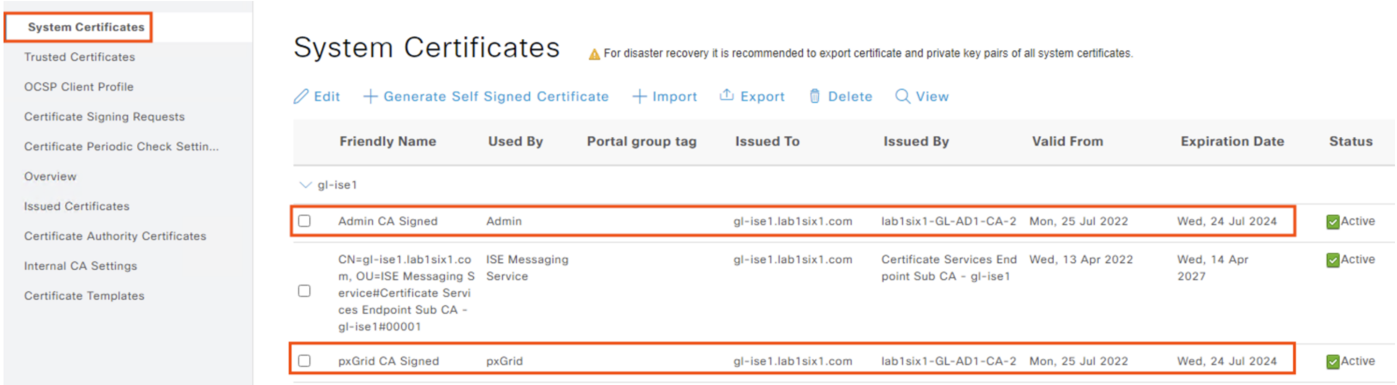
Once the Application Server has fully restarted, the State will change to running.



```
gl-ise1/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          11902
Database Server                        running          134 PROCESSES
Application Server                     running          4119410
Profiler Database                      running          19780
```

Step 7. Repeat the steps above to import the pxGrid certificate, which does not require a restart of the Application Server.

Step 8. Verify the uploaded certificates by clicking on the System Certificates link and confirming the Friendly Name and certificate details of the uploaded certificates.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

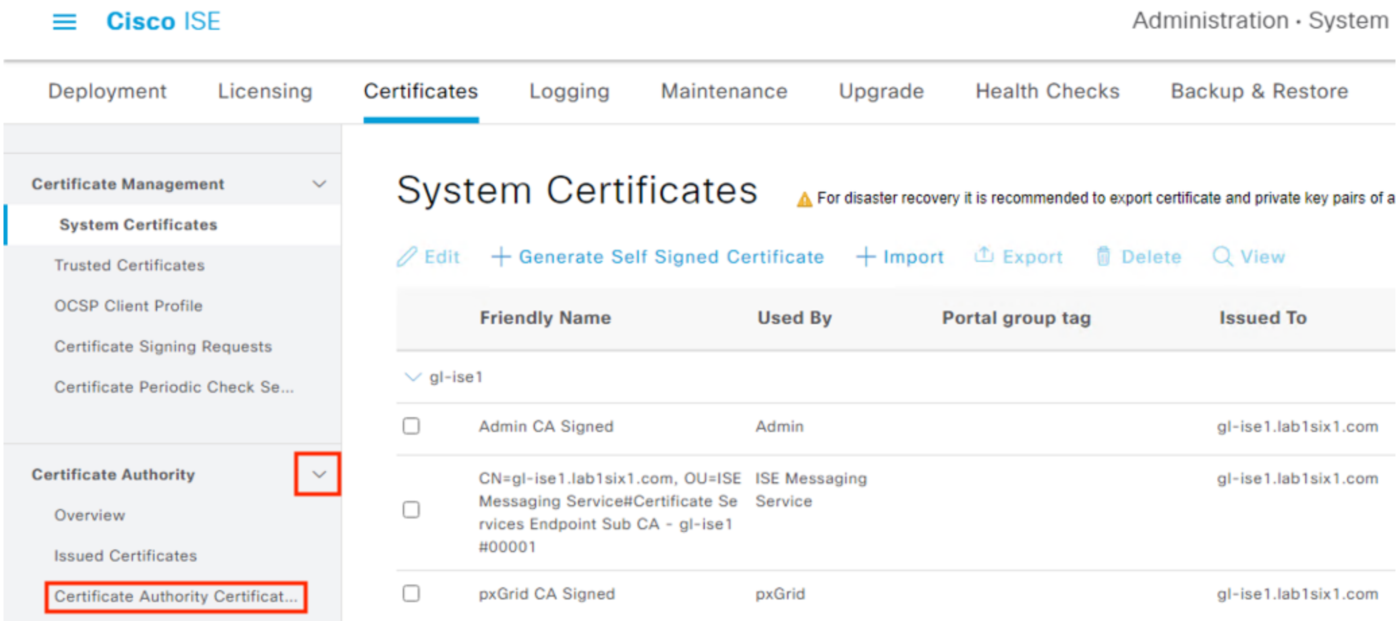
	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
gl-ise1								
□	Admin CA Signed	Admin		gl-ise1.lab1six1.com	lab1six1-GL-AD1-CA-2	Mon, 25 Jul 2022	Wed, 24 Jul 2024	✓ Active
□	CN=gl-ise1.lab1six1.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - gl-ise1#00001	ISE Messaging Service		gl-ise1.lab1six1.com	Certificate Services Endpoint Sub CA - gl-ise1	Wed, 13 Apr 2022	Wed, 14 Apr 2027	✓ Active
□	pxGrid CA Signed	pxGrid		gl-ise1.lab1six1.com	lab1six1-GL-AD1-CA-2	Mon, 25 Jul 2022	Wed, 24 Jul 2024	✓ Active

ISE: Export an ISE Root Certificate

While using an external CA is recommended, ISE does have CA capability that can be used in the absence of an outside CA. This section details how to locate and export the ISE root certificate.

Step 1. Click the Menu icon (☰) and navigate to Administration → System → Certificates.

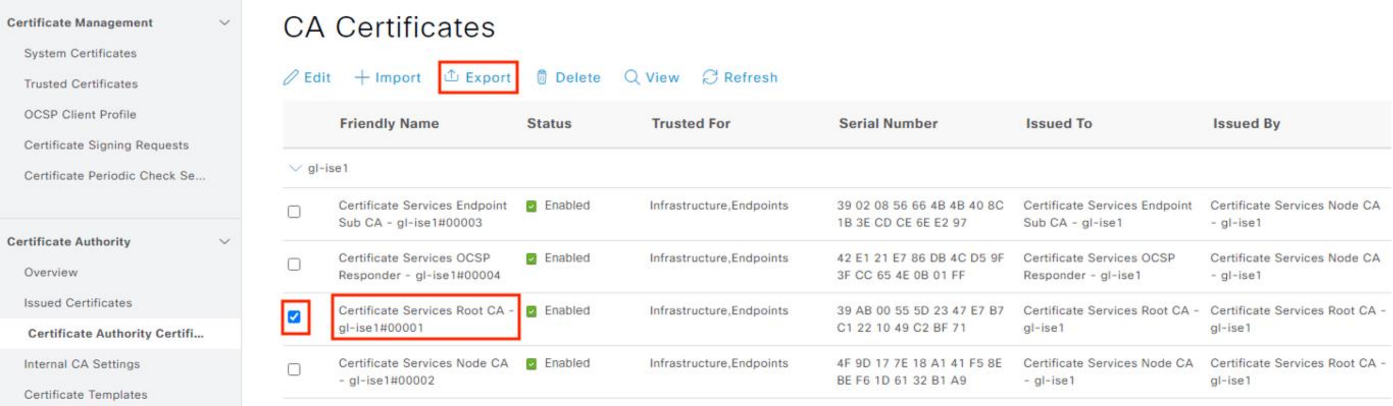
Step 2. Expand Certificate Authority, then select Certificate Authority Certificates on the left menu.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of a

	Friendly Name	Used By	Portal group tag	Issued To
gl-ise1				
□	Admin CA Signed	Admin		gl-ise1.lab1six1.com
□	CN=gl-ise1.lab1six1.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - gl-ise1 #00001	ISE Messaging Service		gl-ise1.lab1six1.com
□	pxGrid CA Signed	pxGrid		gl-ise1.lab1six1.com

Step 3. Check the box next to the Certificate Services Root CA, click Export, and download the file.



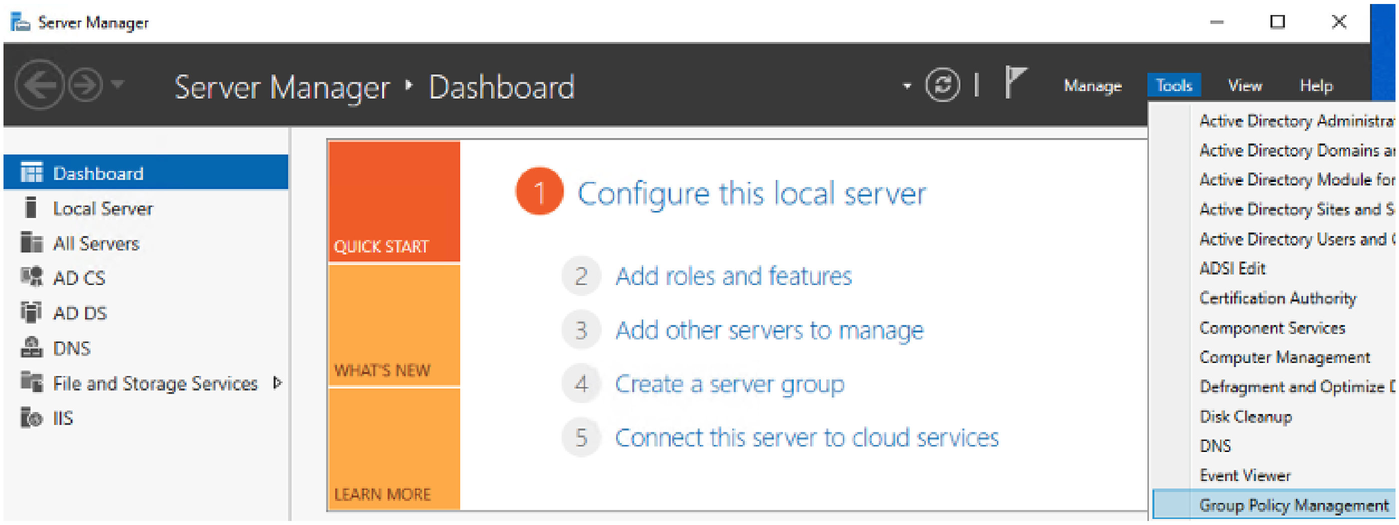
	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
gl-ise1						
□	Certificate Services Endpoint Sub CA - gl-ise1#00003	✓ Enabled	Infrastructure,Endpoints	39 02 08 56 66 4B 4B 40 8C 1B 3E CD CE 6E E2 97	Certificate Services Endpoint Sub CA - gl-ise1	Certificate Services Node CA - gl-ise1
□	Certificate Services OCSP Responder - gl-ise1#00004	✓ Enabled	Infrastructure,Endpoints	42 E1 21 E7 86 DB 4C D5 9F 3F CC 65 4E 0B 01 FF	Certificate Services OCSP Responder - gl-ise1	Certificate Services Node CA - gl-ise1
☑	Certificate Services Root CA - gl-ise1#00001	✓ Enabled	Infrastructure,Endpoints	39 AB 00 55 5D 23 47 E7 B7 C1 22 10 49 C2 BF 71	Certificate Services Root CA - gl-ise1	Certificate Services Root CA - gl-ise1
□	Certificate Services Node CA - gl-ise1#00002	✓ Enabled	Infrastructure,Endpoints	4F 9D 17 7E 18 A1 41 F5 8E BE F6 1D 61 32 B1 A9	Certificate Services Node CA - gl-ise1	Certificate Services Root CA - gl-ise1

Active Directory: Distribute Machine Certificates via Group Policy Object

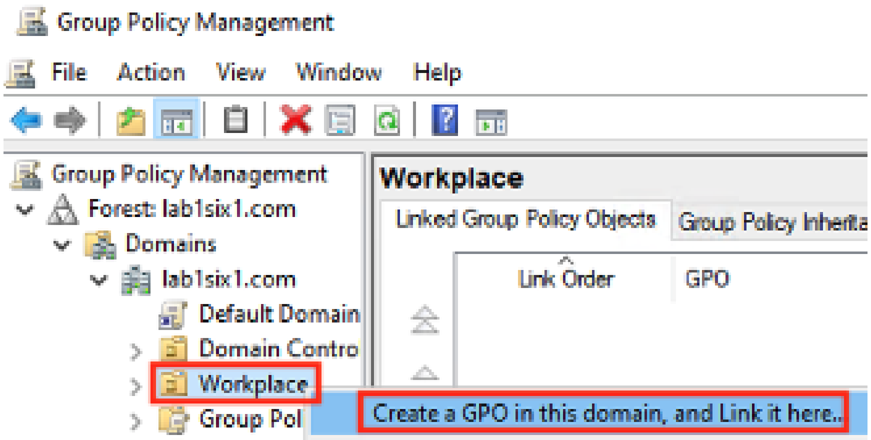
The certificates created and distributed in this step can be used for a machine authorization check in ISE. The AD Certificate Authority has a preconfigured certificate template labelled ‘Computer’ that creates certificates with client and server authentication. However, since we will only be using these certificates for client authentication, we will first create a new template that only has client auth set.

Step 1. Configure Group Policy

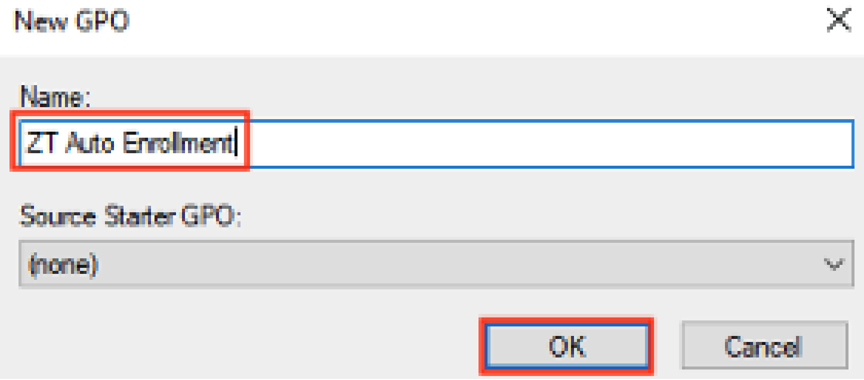
Step 2. Click on Tools → Group Policy Management.



Step 3. Right click on the target domain and click ‘Create a GPO in this domain’.



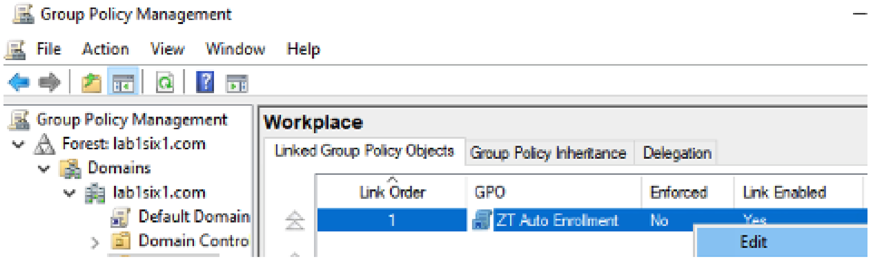
Step 4. Enter a name and click OK.



Name:
ZT Auto Enrollment

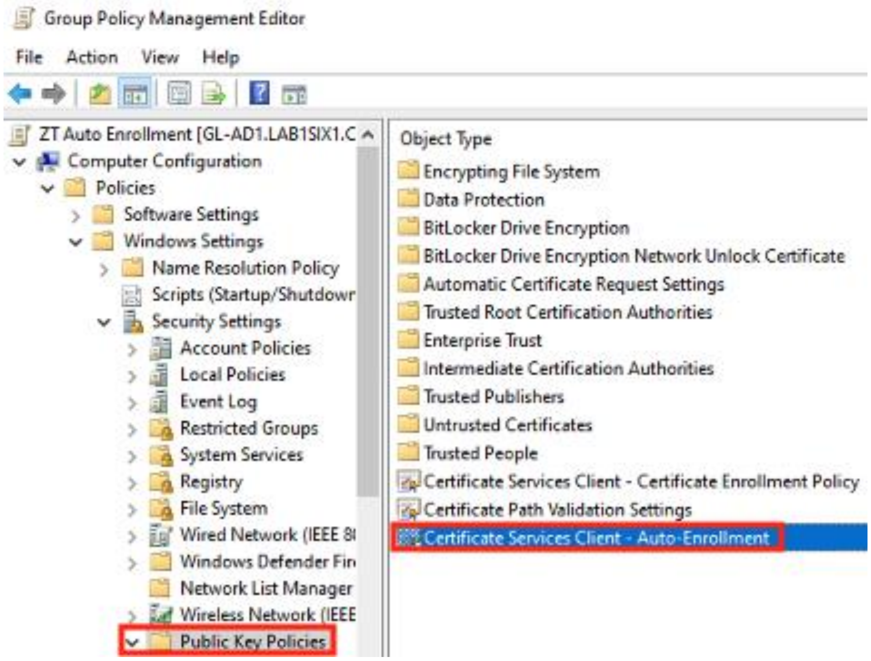
Source Starter GPO:
(none)

Step 5. Right click on the newly created GPO and click edit.

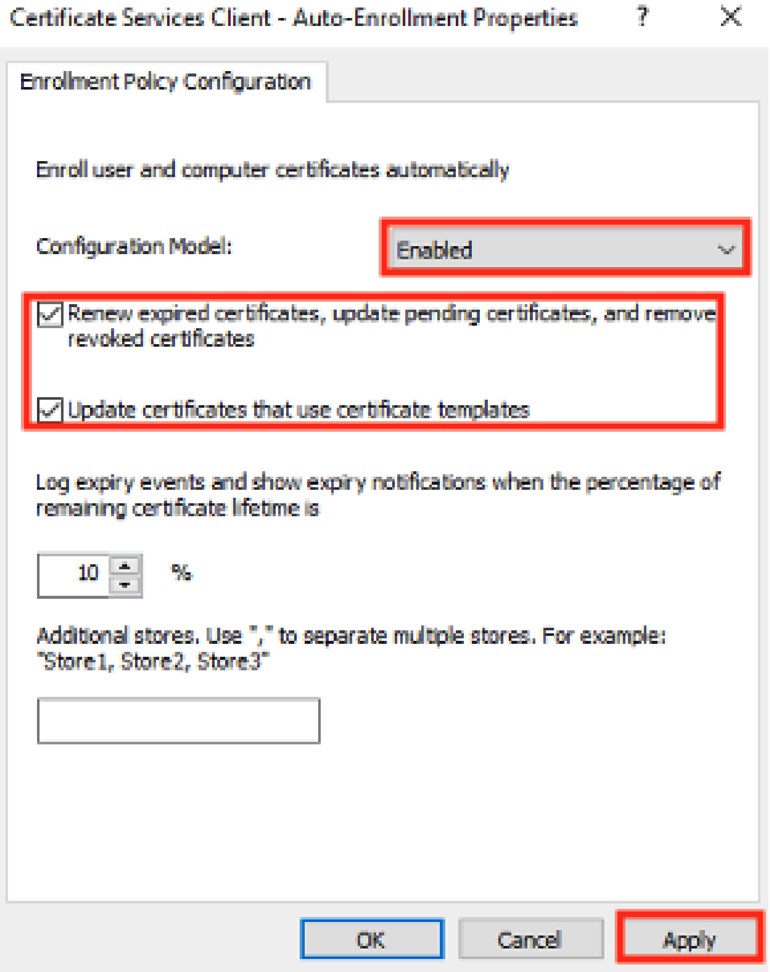


Link Order	GPO	Enforced	Link Enabled
1	ZT Auto Enrollment	No	Yes

Step 6. Expand the tree to Computer Configuration → Policies → Windows Settings → Security Settings then click Public Key Policies. Double click on Certificate Services Client – Auto-Enrollment.



Step 7. Set Configuration Model to Enabled and check the boxes to renew and update certificates. Click Apply, then click OK.


Certificate Services Client - Auto-Enrollment Properties
?
X
Enrollment Policy Configuration
OK
Cancel
Apply

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

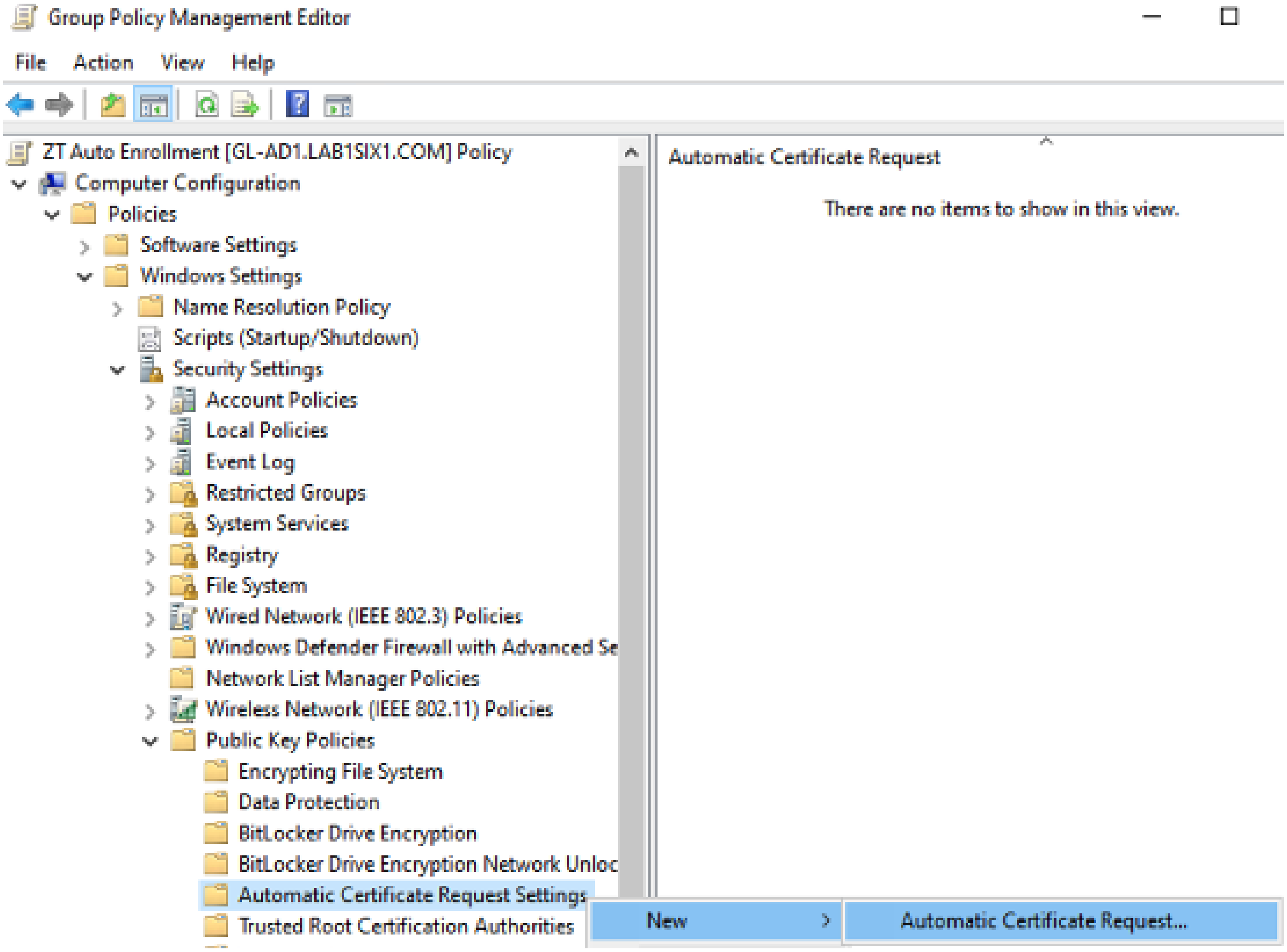
☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

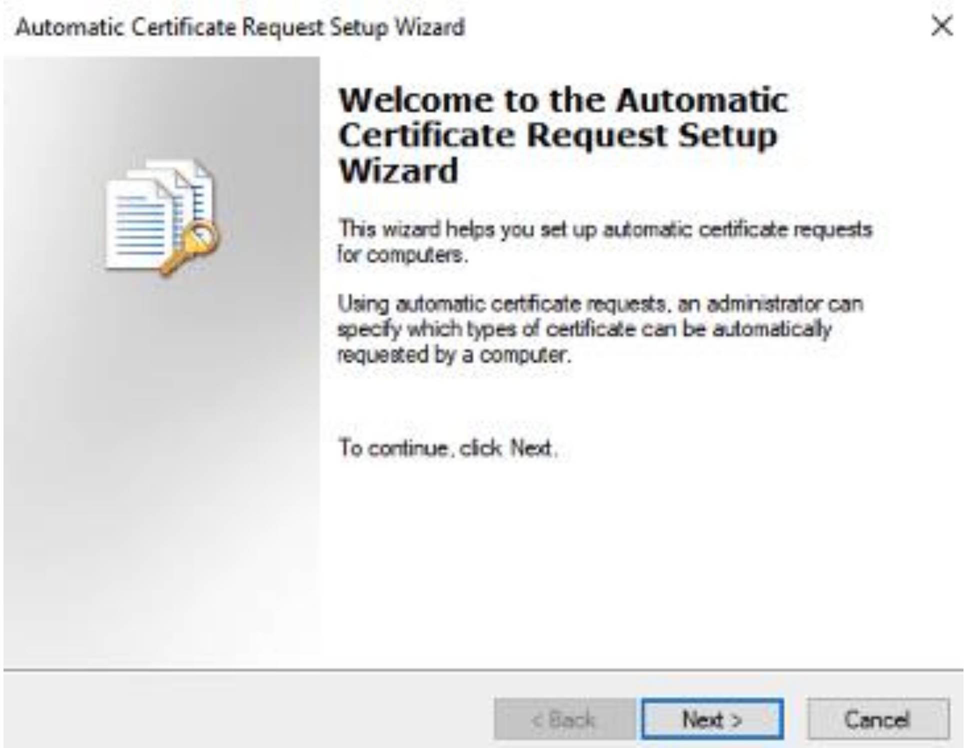
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

Step 8. Right click on Automatic Certificate Request Settings, select New, then select Automatic Certificate Request.


Group Policy Management Editor
File
Action
View
Help
ZT Auto Enrollment [GL-AD1.LAB1SIX1.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unloc
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Automatic Certificate Request
New
Automatic Certificate Request...

There are no items to show in this view.

Step 9. Click Next.


Automatic Certificate Request Setup Wizard

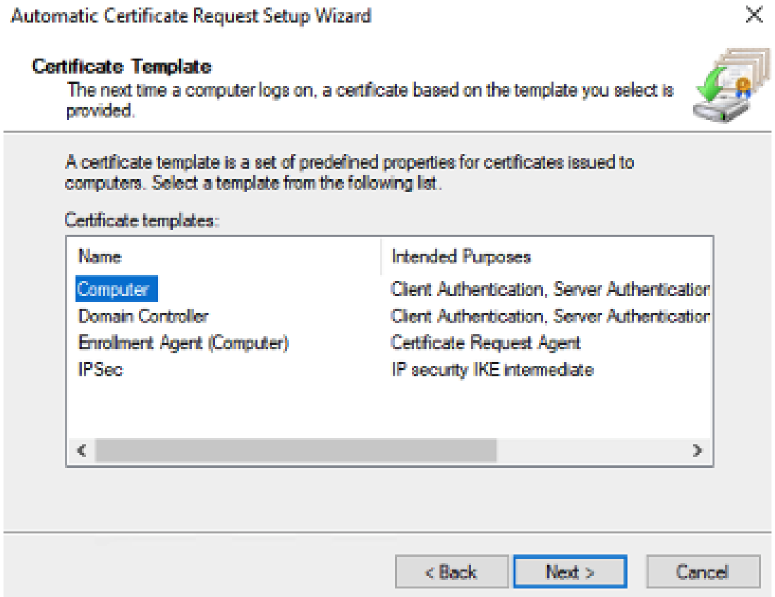
Welcome to the Automatic Certificate Request Setup Wizard

This wizard helps you set up automatic certificate requests for computers.

Using automatic certificate requests, an administrator can specify which types of certificate can be automatically requested by a computer.

To continue, click Next.

Step 10. Select the Computer template, then click Next.


Automatic Certificate Request Setup Wizard

Certificate Template

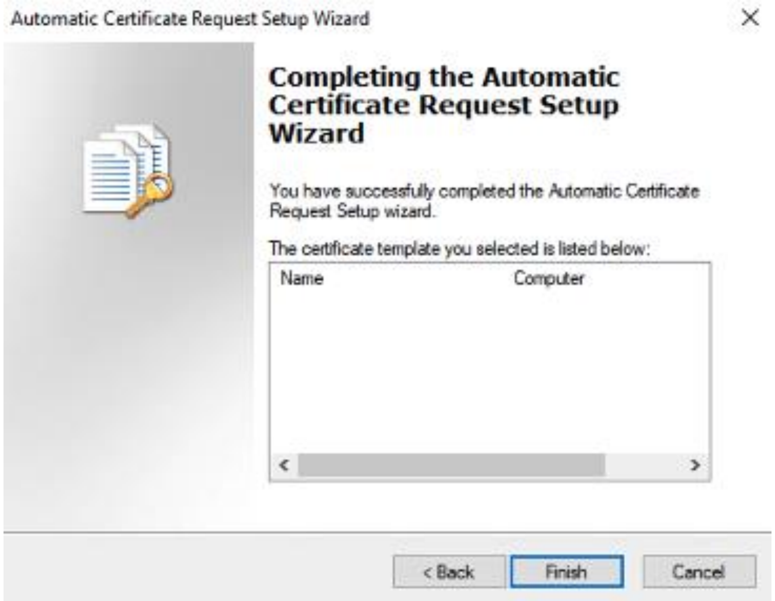
The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSec	IP security IKE intermediate

Step 11. Click Finish.



Automatic Certificate Request Setup Wizard

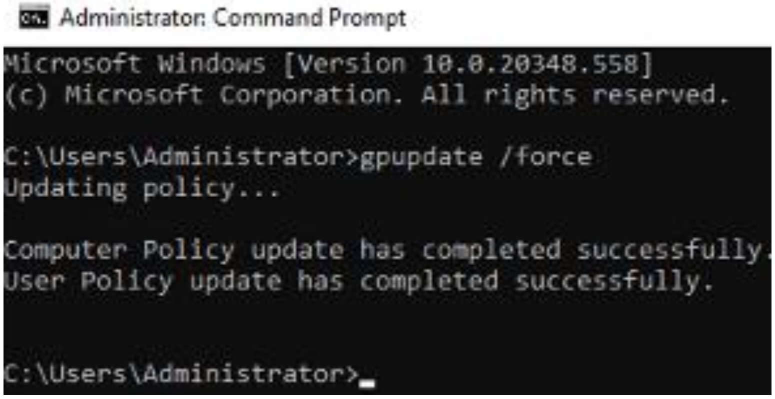
Completing the Automatic Certificate Request Setup Wizard

You have successfully completed the Automatic Certificate Request Setup wizard.

The certificate template you selected is listed below:

Name	Computer

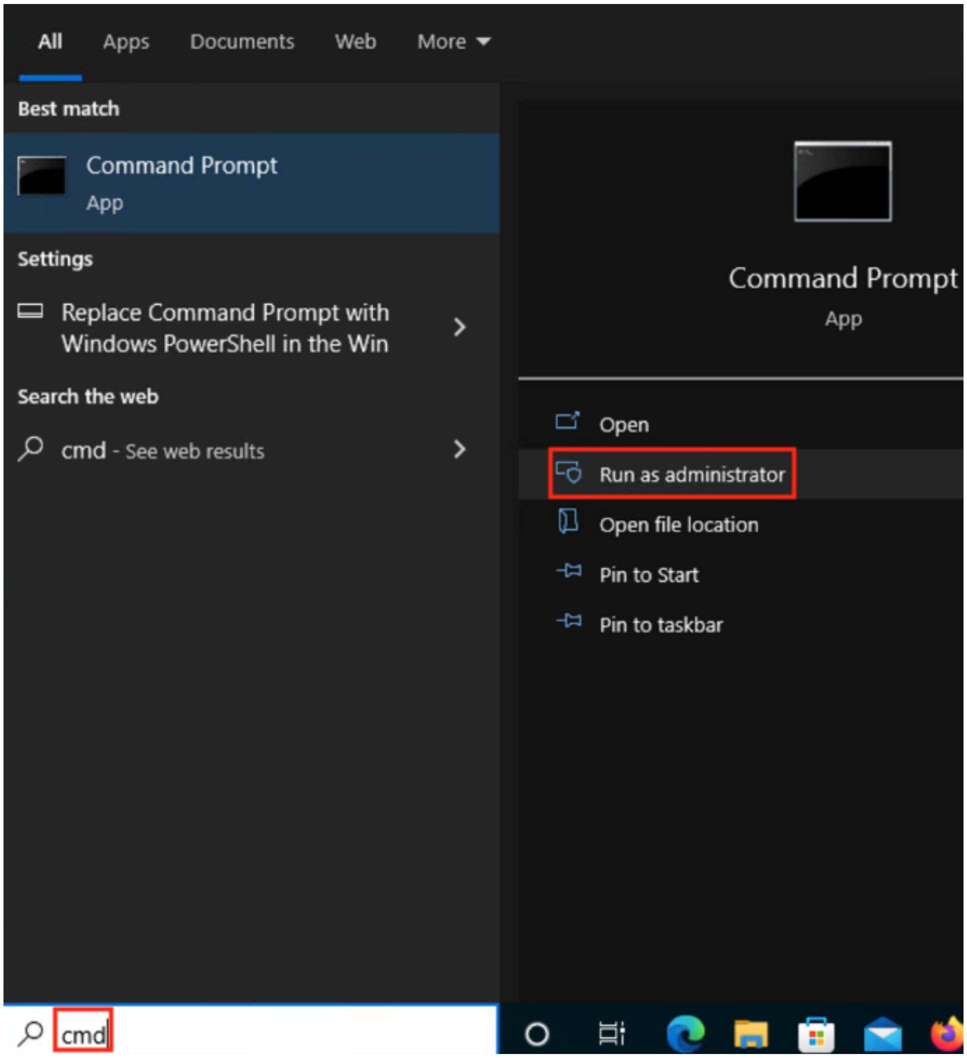
Step 12. Close the Group Policy windows. From the AD CS, launch a command line and run gpupdate /force.

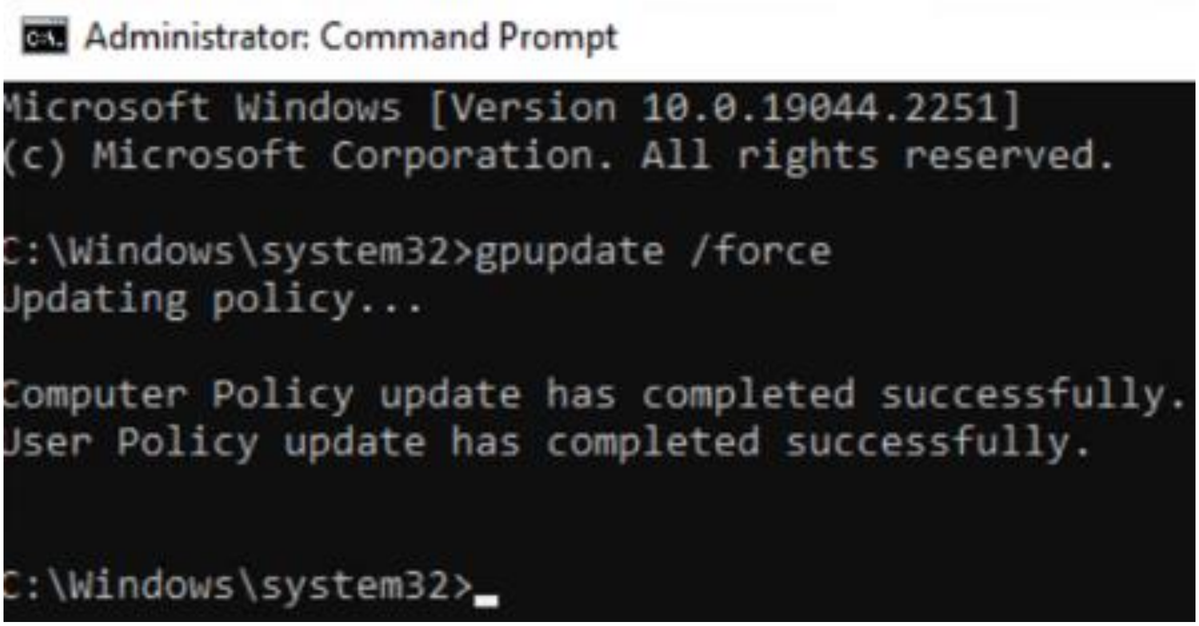


Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.558]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>_
```

Step 13. Access the Windows workstation that is to receive the certificate and run command line as administrator, entering the same gpupdate /force command as above.

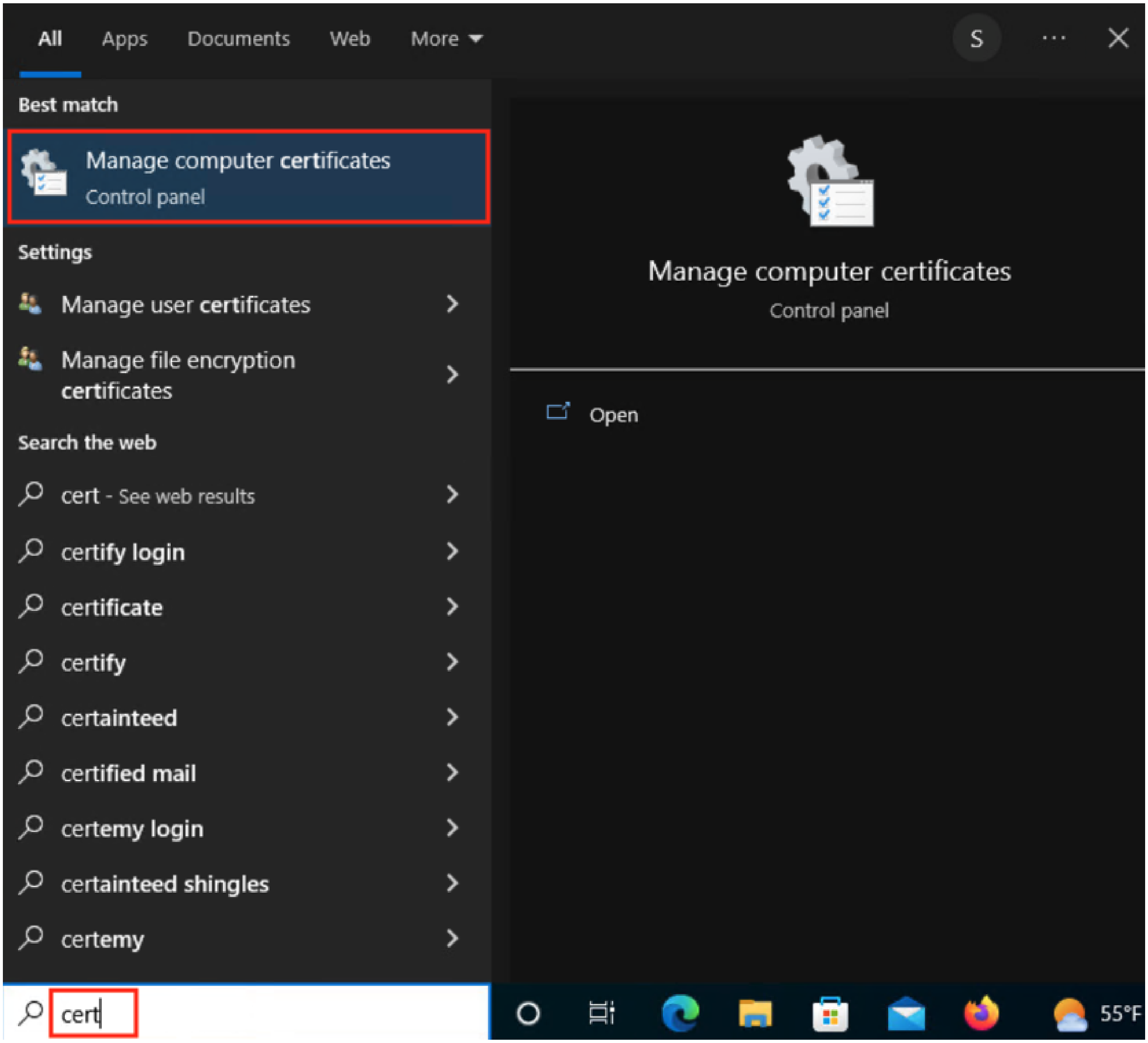




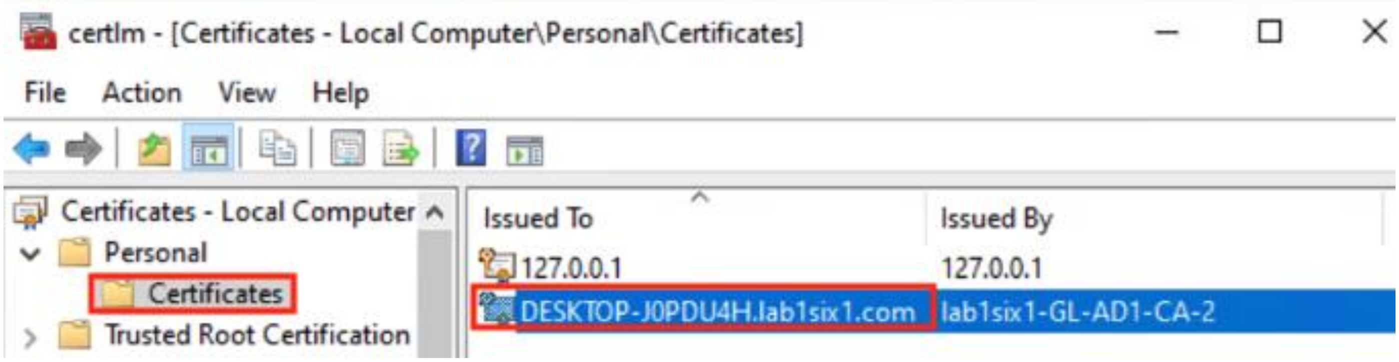
```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Windows\system32>_
```

Verify Certificate Install

Step 1. From the Windows host, type 'cert' into the search bar and select 'Manage computer certificates'.

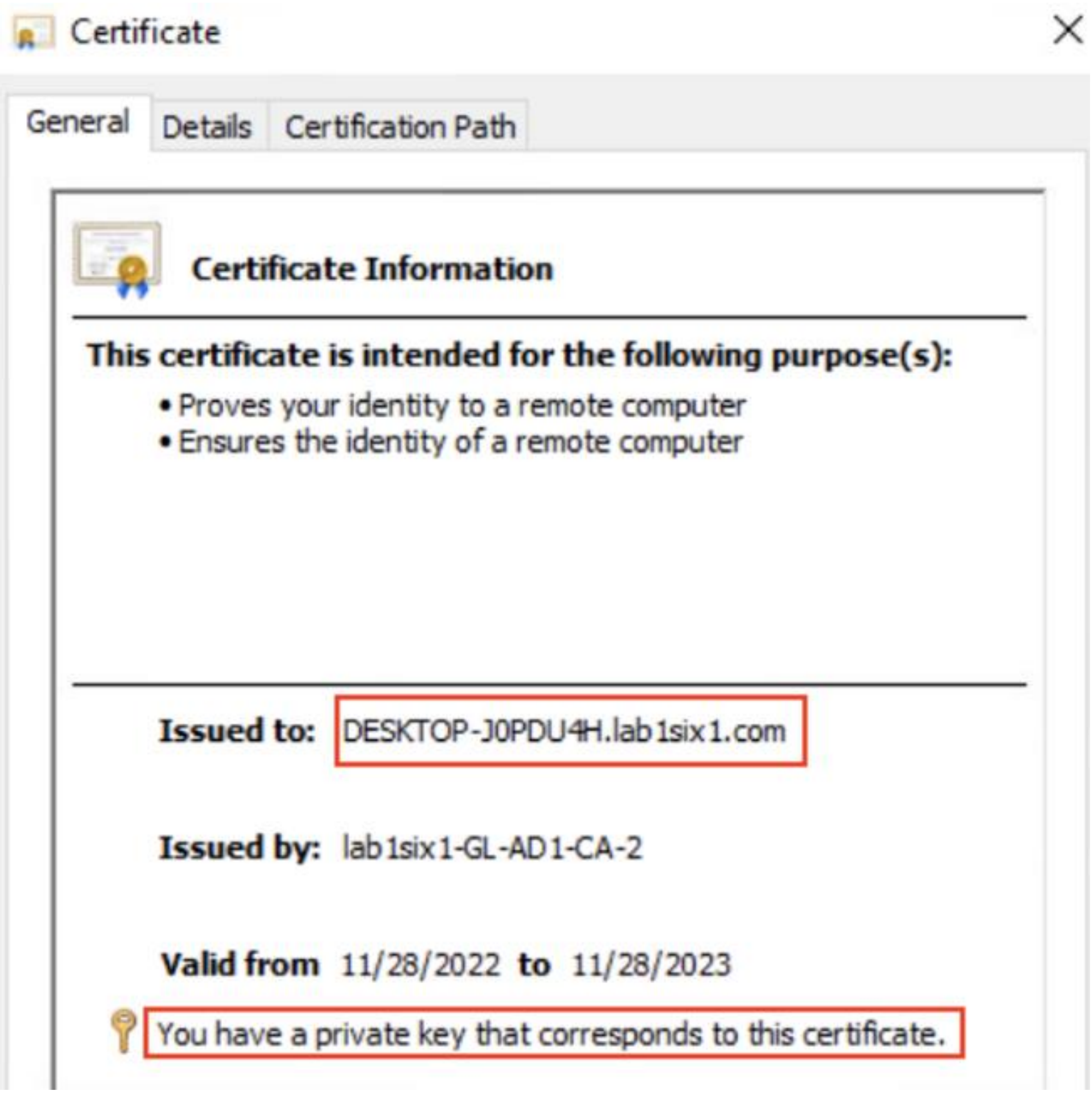


Step 2. Expand the dropdown on the Personal folder and click on Certificates. Identify the machine certificate in the right pane and double click on it.


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification

Issued To	Issued By
127.0.0.1	127.0.0.1
DESKTOP-J0PDU4H.lab1six1.com	lab1six1-GL-AD1-CA-2

Step 3. The certificate should have a name that corresponds to the device name and a local private key.



Certificate

Certificate Information

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

- Proves your identity to a remote computer
- Ensures the identity of a remote computer

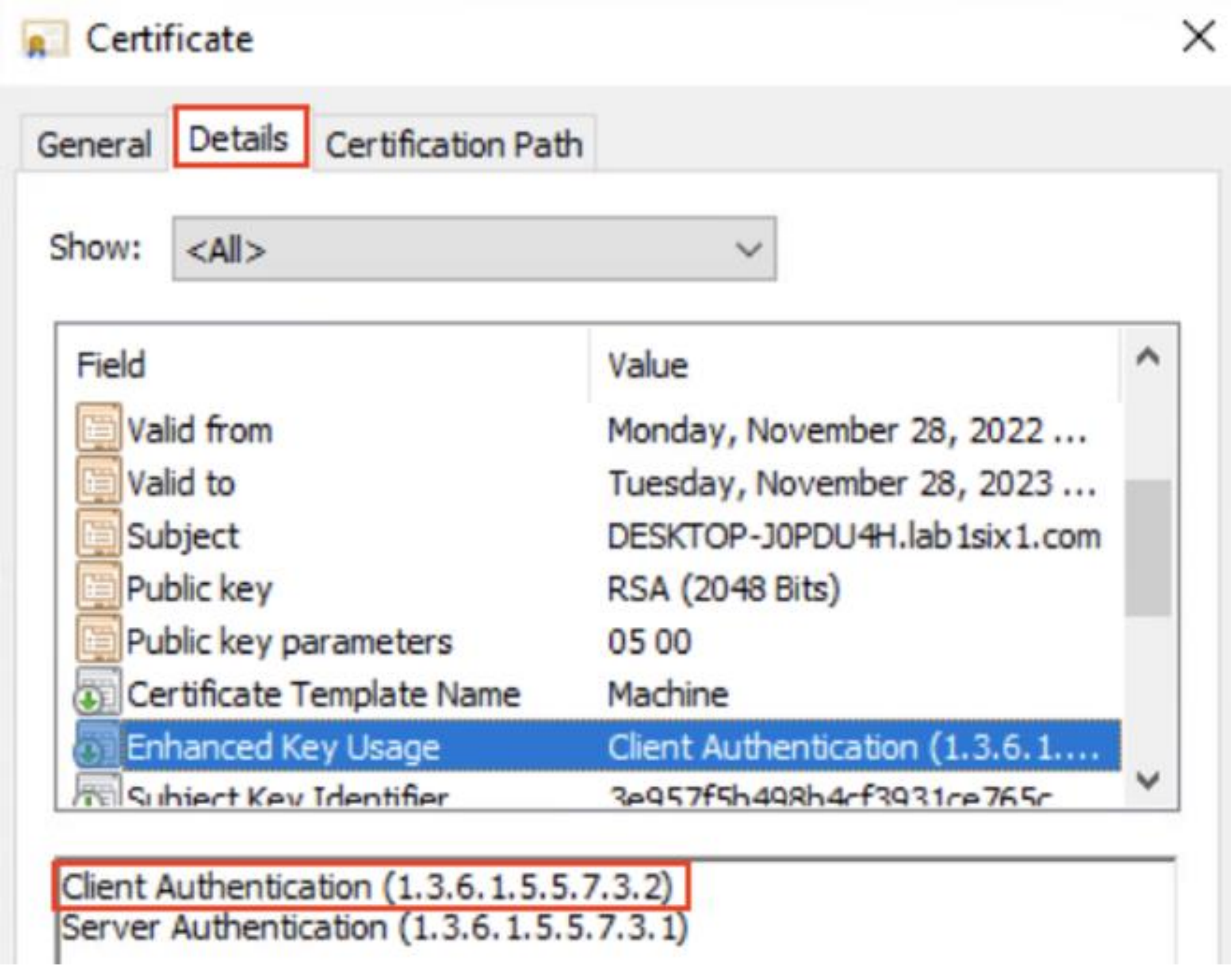
Issued to: DESKTOP-J0PDU4H.lab1six1.com

Issued by: lab1six1-GL-AD1-CA-2

Valid from 11/28/2022 to 11/28/2023

You have a private key that corresponds to this certificate.

Step 4. Click on the Details tab and scroll down to Enhanced Key Usage. Verify that the certificate has Client Authentication.



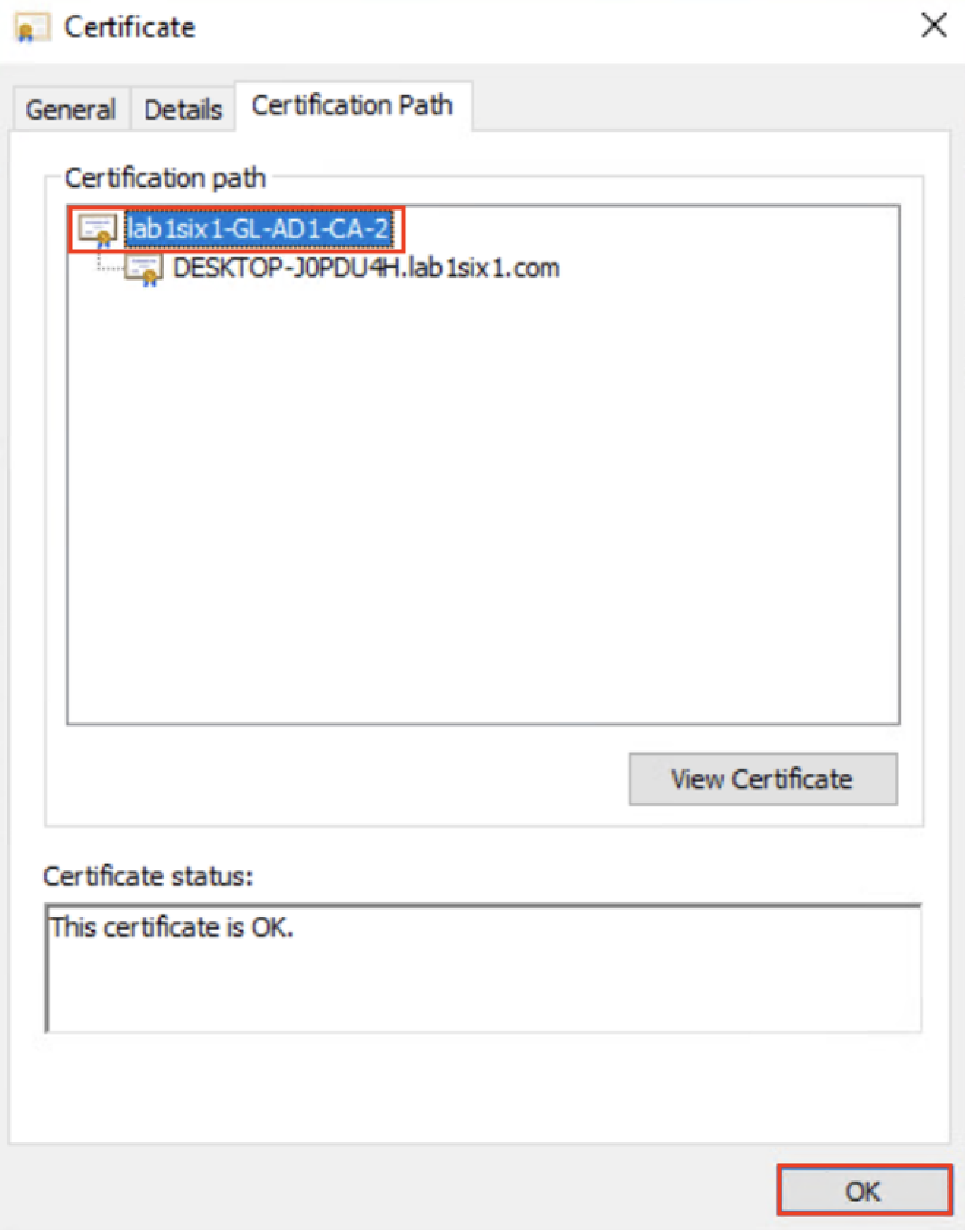
Certificate

Show: <All>

Field	Value
Valid from	Monday, November 28, 2022 ...
Valid to	Tuesday, November 28, 2023 ...
Subject	DESKTOP-J0PDU4H.lab1six1.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Name	Machine
Enhanced Key Usage	Client Authentication (1.3.6.1....
Subject Key Identifier	3e957f5b498b4cf3931ce765c

Client Authentication (1.3.6.1.5.5.7.3.2)
Server Authentication (1.3.6.1.5.5.7.3.1)

Step 5. Click on the Certification Path tab and verify the certificate chain. The root certificate and any intermediate certificates need to be trusted in ISE. Click OK.



Certificate

Certification path

- lab1six1-GL-AD1-CA-2
  - DESKTOP-J0PDU4H.lab1six1.com

Certificate status:

This certificate is OK.

Appendix

Appendix A – Acronyms Defined

Acronym	Definition
CA	Certificate Authority
CSR	Certificate Service Request
GPO	Group Policy Object
GUI	Graphical User Interface
ISE	Identity Services Engine
pxGrid	Cisco Platform Exchange Grid

Appendix B – References

- Cisco Zero Trust Architecture Guide
- Zero Trust Frameworks Guide
- Cisco Zero Trust: User and Device Security Design Guide
- Cisco SAFE
- Cisco pxGrid

Appendix C – Feedback

If you have feedback on this design guide or any of the Cisco Security design guides, please send an email to ask-security-cvd@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.