

# Create Windows Server Certificate Template for Catalyst Center

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Troubleshoot](#)

---

## Introduction

This document describes the steps to create a certificate template on a Windows Server running the Certificate Authority (CA) tool.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst Center
- A Windows Server with the Certification Authority (CA) role installed and configured
- Administrator privileges on the Windows Server
- Access to the Certification Authority Management Console
- Basic knowledge of certificate templates and Certificate Signing Requests (CSR)

### Components Used

The information in this document is based on Microsoft Windows Server 2022 Standard.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

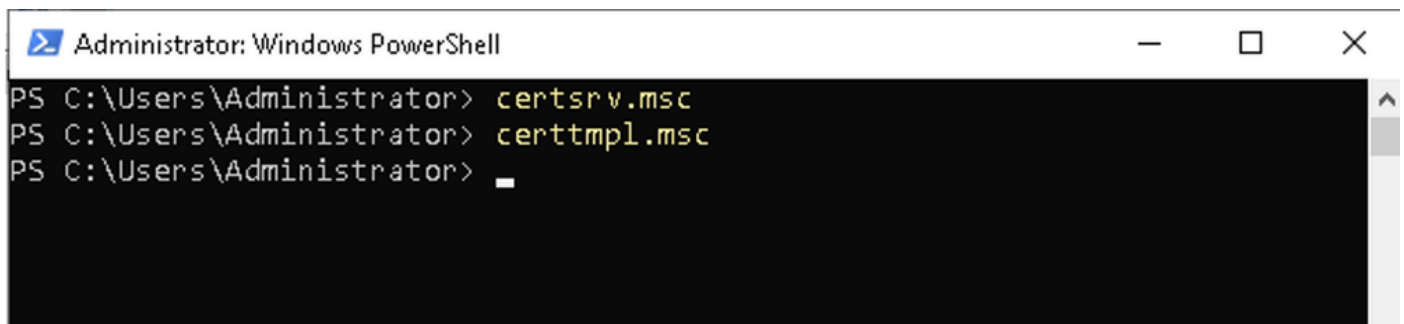
This custom template solves the issue where the default CA templates remove the Client Authentication from Extended Key Usages. The custom template is able to sign the Certificate Signing Request (CSR) generated by Catalyst Center.

## Configure

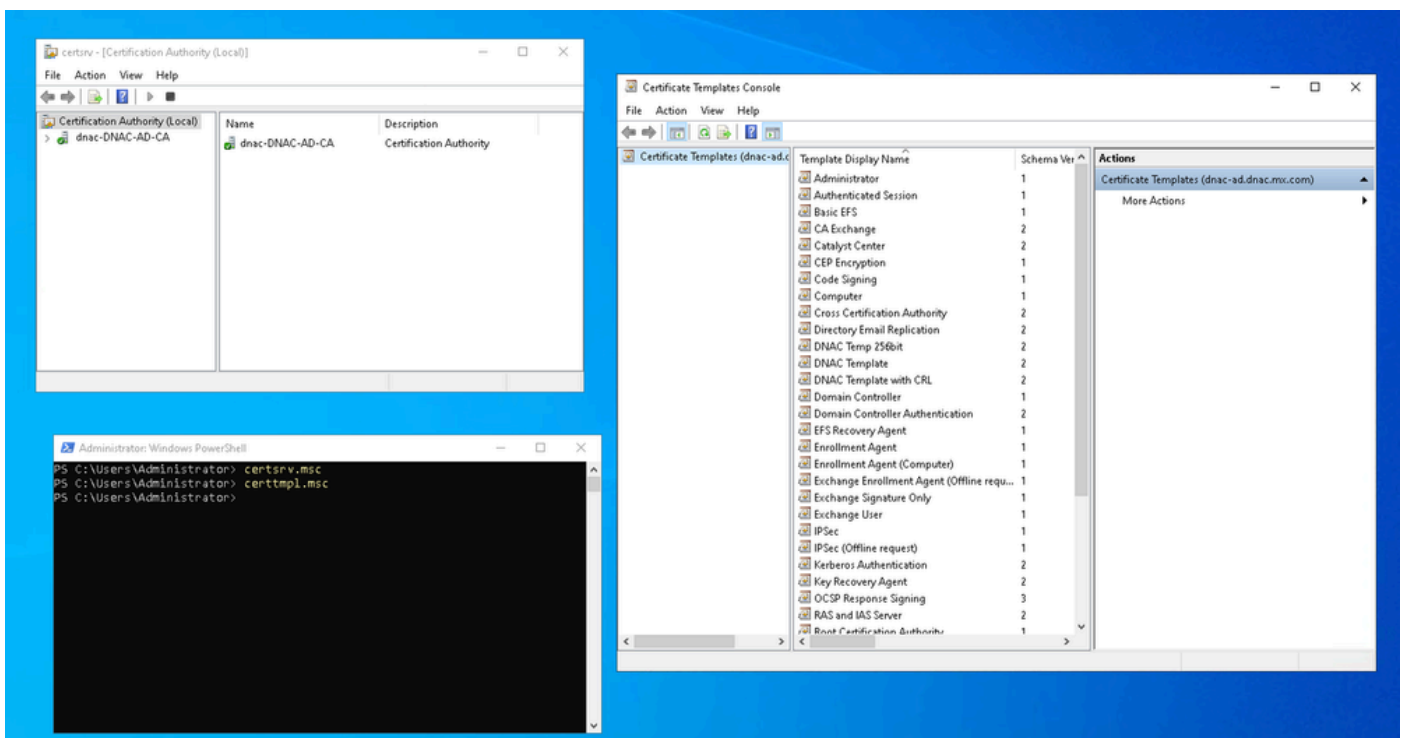
Steps to review and configure Certificate Templates on Windows Server with the Certification Authority (CA).

1. Log in to the **Windows Server** hosting the CA using Remote Desktop.
2. Open a **command prompt (CMD)** or **powerShell** session.
3. Launch the **certificate authority** and **certificate template** consoles by running:

```
certsrv.msc  
certtmpl.msc
```

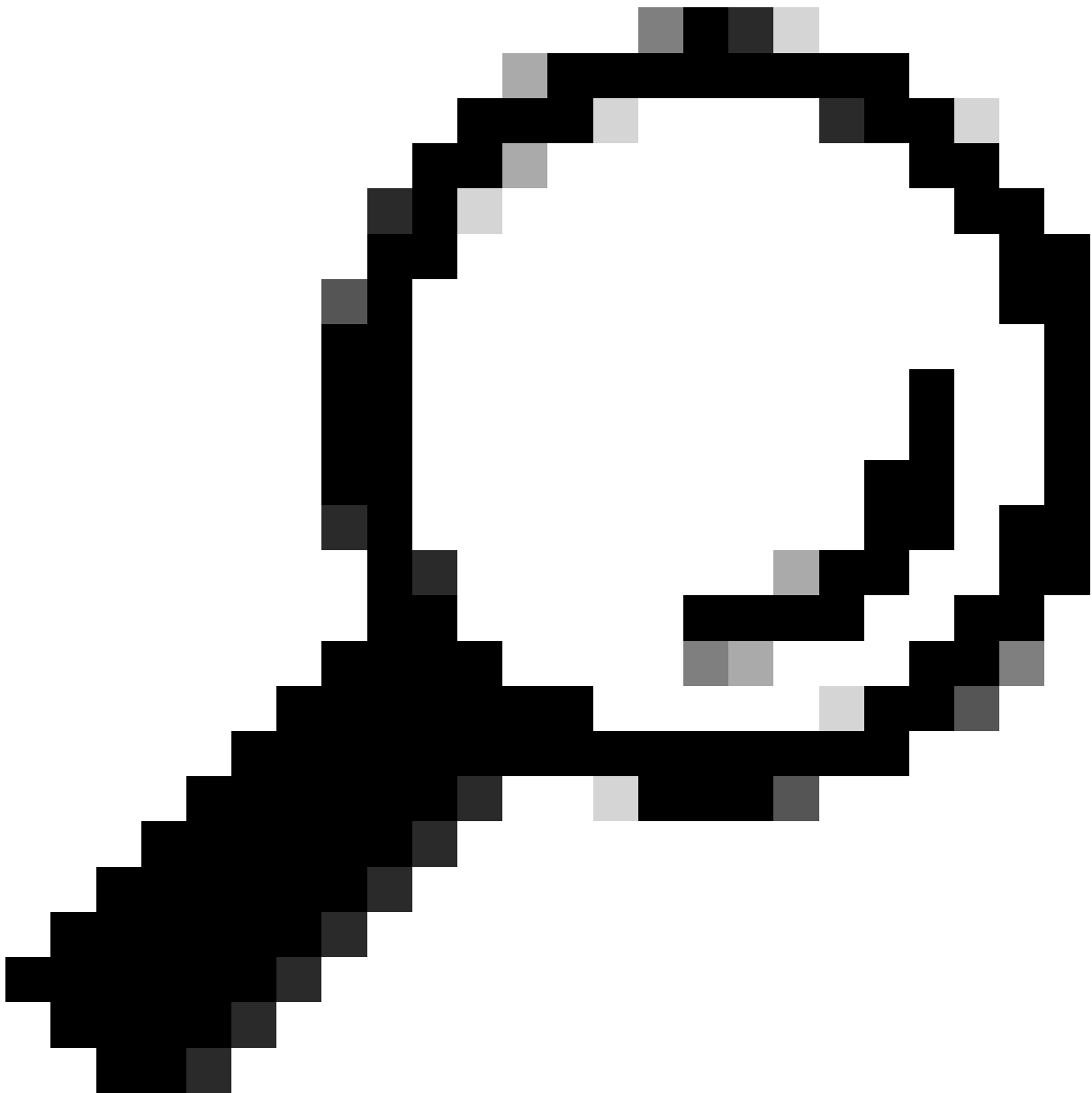


*Administration Powershell Commands*



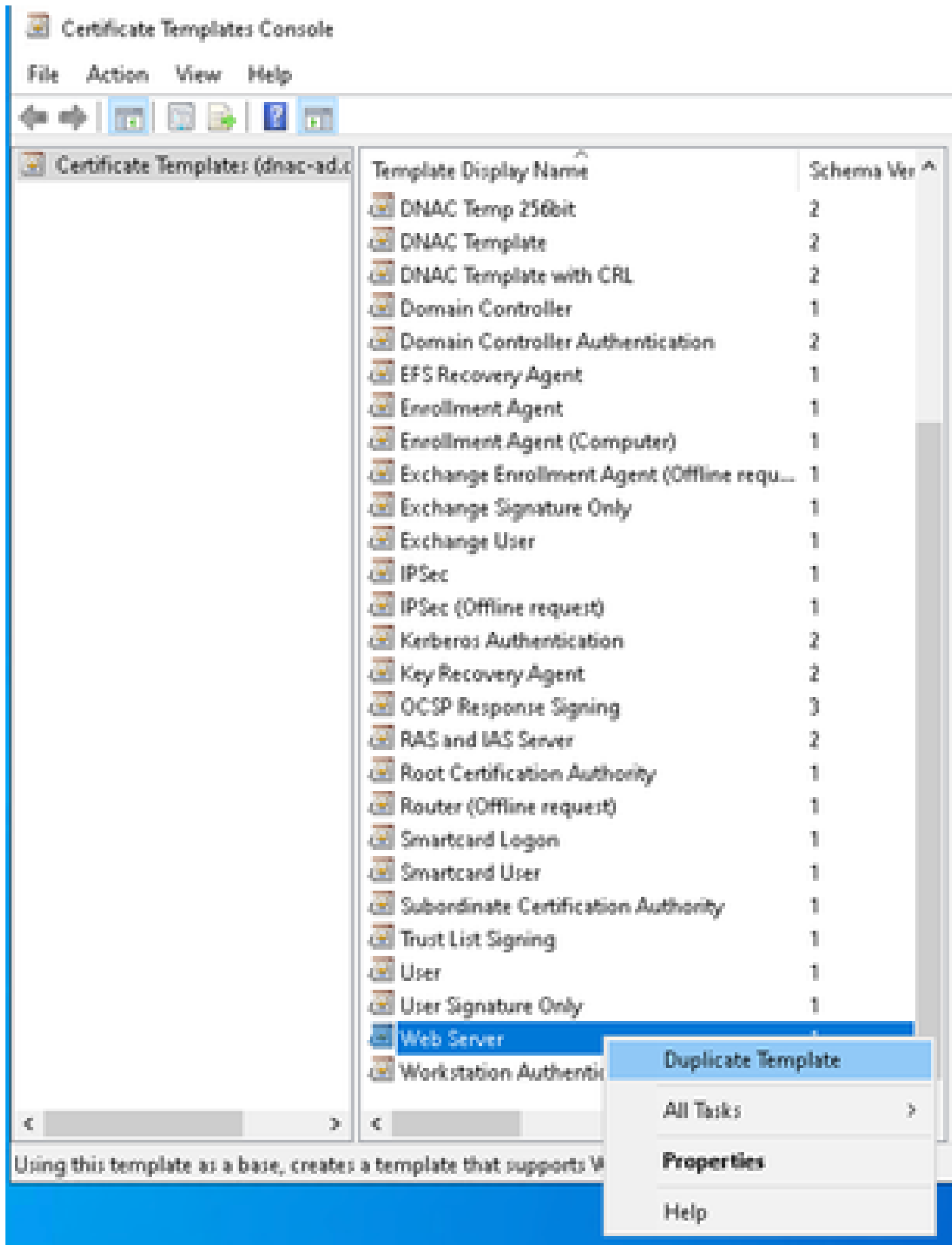
*Windows Server Example*

4. In the Certificate Template Console, locate the **template** to be cloned to create a new customizable template.



**Tip:** Use the Web Server template since it already includes all the required parameters for the Catalyst Center certificate.

- 
- Example: right-click the **web server** and select **duplicate template**.



*Duplicate Template*

5. A new template is open, modify it with the **required characteristics**.

## Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

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.

OK

Cancel

Apply

Help

6. Modify the new template as follows:

6.1 General Tab.

- Enter a **template name** (for example, Catalyst Center Template).
- Define the validity period (default: 2 years).

Properties of New Template



Subject Name

Server

Issuance Requirements

Superseded Templates

Extensions

Security

Compatibility

General

Request Handling

Cryptography

Key Attestation

Template display name:

Catalyst Center Template

Template name:

CatalystCenterTemplate

Validity period:

2

years



Renewal period:

6

weeks

☐ Publish certificate in Active Directory☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK

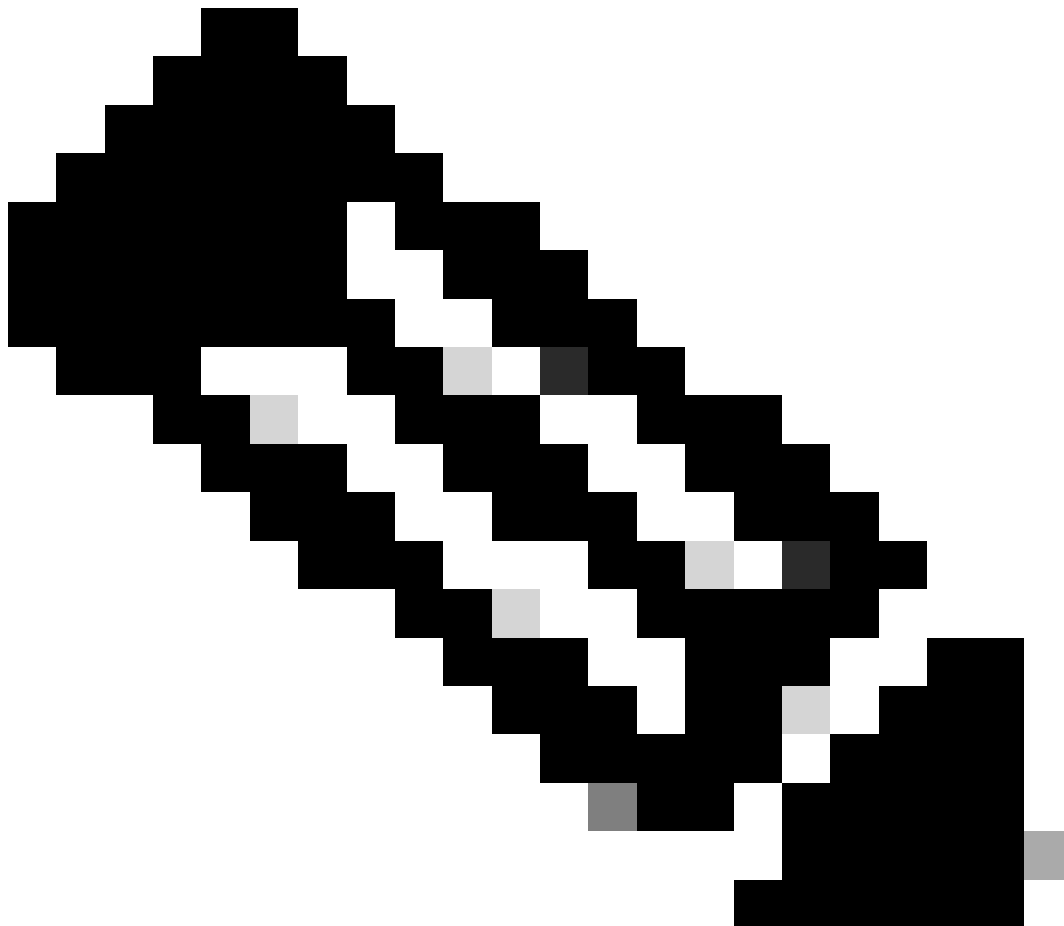
Cancel

Apply

Help

## 6.2 Extensions Tab.

- Navigate to **application policies** and click **edit**.
- 



**Note:** In this tab, confirm that the template includes the mandatory Key Usage extensions required by the Catalyst Center certificate, such as keyEncipherment and digitalSignature. These are already present in the default Web Server template used as the base.

---

## Properties of New Template



Subject Name

Server

Issuance Requirements

Compatibility

General

Request Handling

Cryptography

Key Attestation






Superseded Templates

Extensions

Security

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

**Edit...**

Description of Application Policies:

Server Authentication

OK

Cancel

Apply

Help

- Click **add**, locate **client authentication**, and click **ok** to include it.

## Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Server Authentication

Add...

Edit...

Remove

☐ Make this extension critical

OK

Cancel

## 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

New...

OK

Cancel

*Add Application Policy*

- Confirm the template shows Client Authentication along with the default usages.

## Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication  
Server Authentication

Add...

Edit...

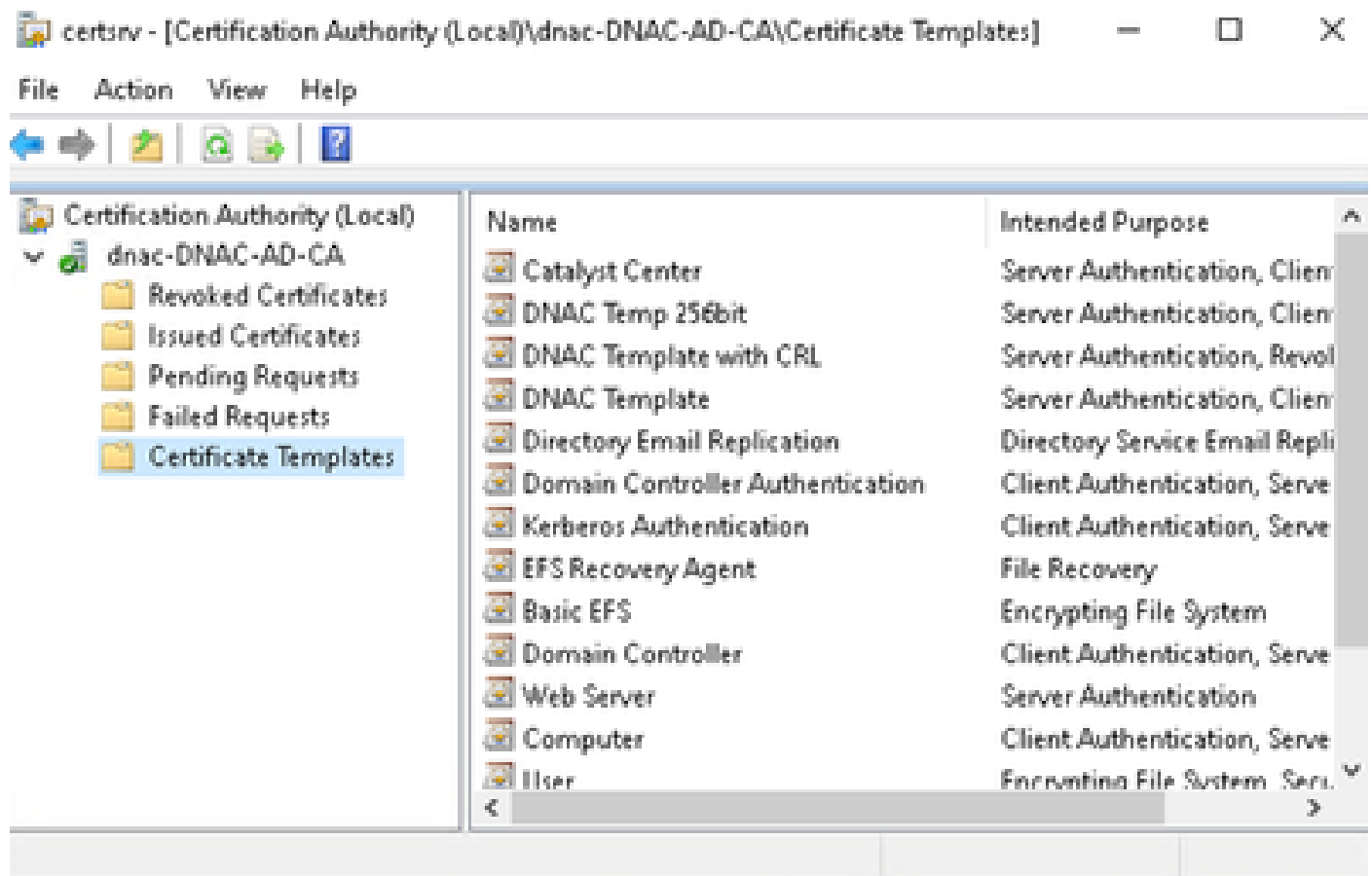
Remove

☐ Make this extension critical

OK

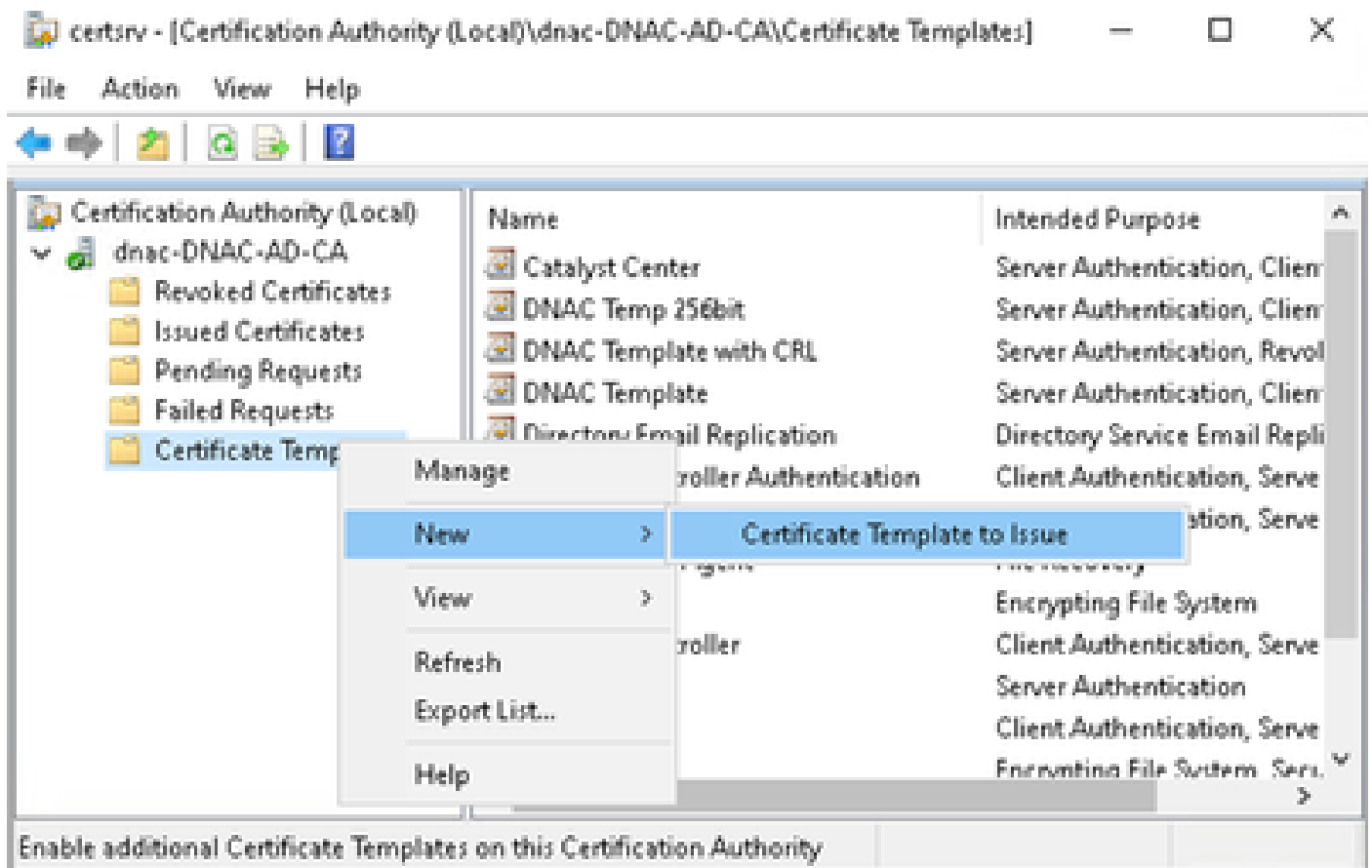
Cancel

7. Click **apply** and then **ok**.
8. In the Certificate Authority console, expand the **CA tree** and select the **certificate templates** folder.



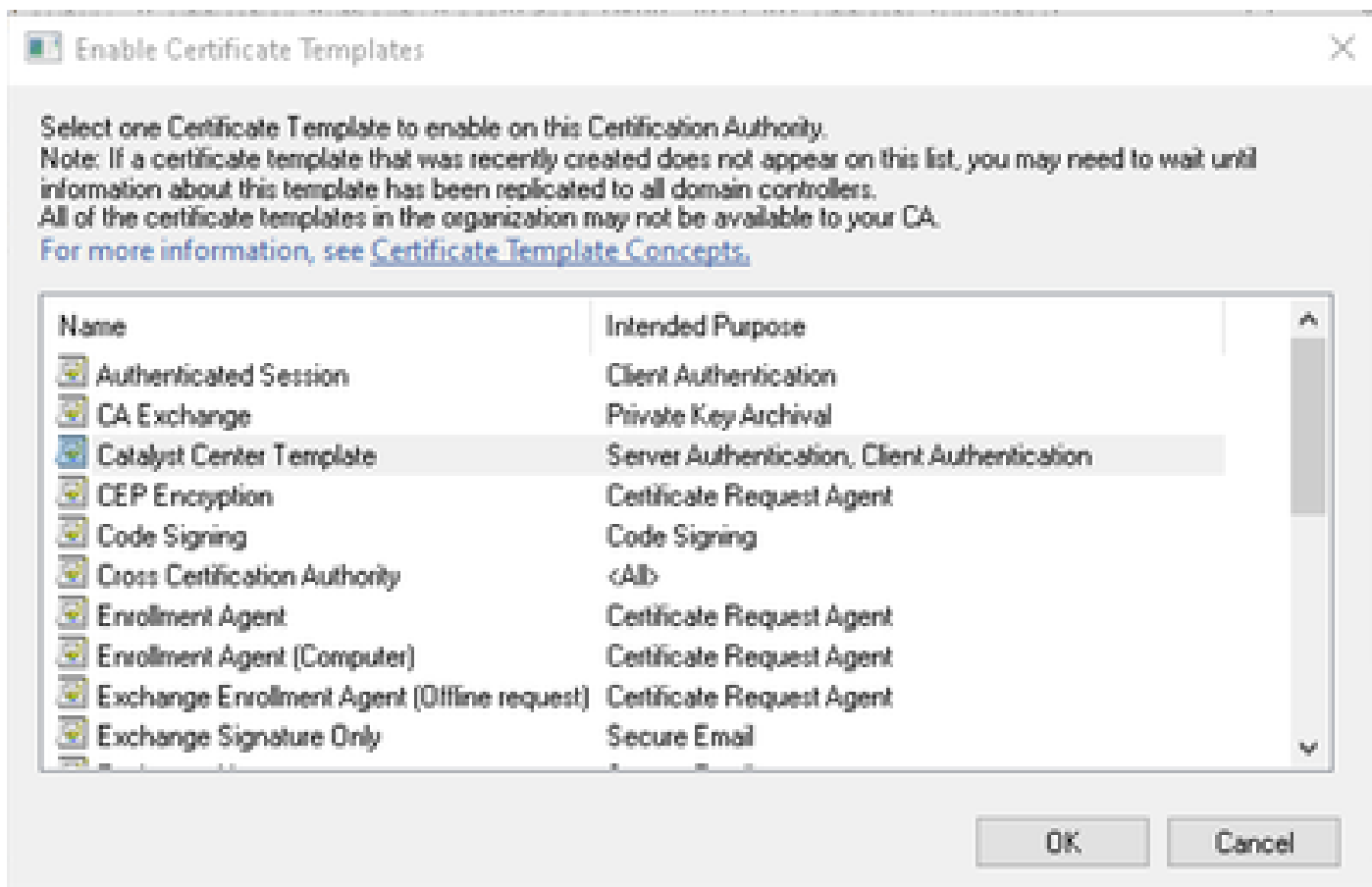
CA Tree Certificate Templates

9. Right-click the **certificate templates** folder and select:  
**New > Certificate Template to Issue**.



*New Certificate Template to Issue*

10. In the new window, select the **newly created template** (for example, Catalyst Center Template) and click **ok**.

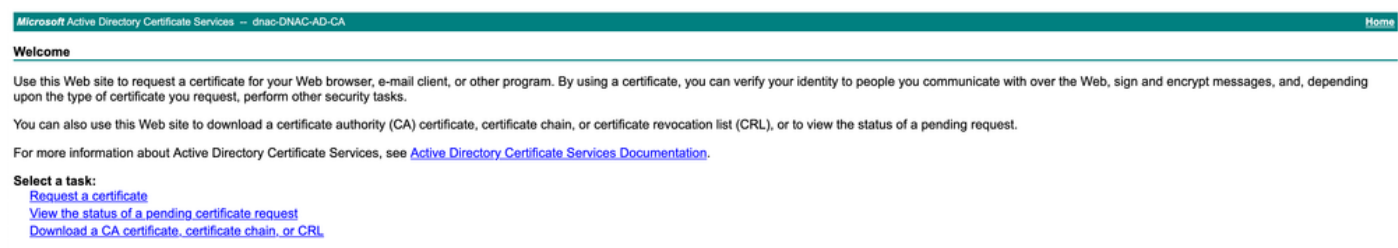


*Catalyst Center Template*

11. The template now appears under the Certificate Templates list in the CA.

12. Open a **browser** and navigate to:

<http://localhost/certsrv/>



*Log In Page <http://localhost/certsrv/>*

13. Select **request a certificate**, then **advanced certificate request**, to verify that the new template is available.

14. On this page, submit the **CSR** and select the **newly created template** to generate the signed certificate.

**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 or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

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

```
HS29DKQx8wkaeC080u+uwRt6Wf+G7Ci1p0v415vc|
LtbzjY7pH80VXu+yePN85mPTeDL++poXx8vXUT8w|
2d14EajkSKQP8CJJh5W7gn3dd4w1r8h90Y5wR8g|
B1Zq07Ldz1jGRgJMj9hWe6nvnvJaVfy9o3M1GcYzc|
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

Catalyst Center Template

**Additional Attributes:**

Attributes:

Submit >

*Request a Certificate*

13. The certificate is generated with the correct extensions, as shown in the example.



## Certificate



General

Details

Certification Path

Show:

<All>



Field	Value
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative Name	DNS Name=fqdn.cisco.com, D...
Subject Key Identifier	a384fc379a2c06dd94a8256eb...
Authority Key Identifier	KeyID=8b275ab9640e5d0279...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...

Server Authentication (1.3.6.1.5.5.7.3.1)

Client Authentication (1.3.6.1.5.5.7.3.2)

Edit Properties...

Copy to File...

OK

Certificate Example

## Troubleshoot

If you encounter errors while signing the CSR, review the Windows Server logs for more details:

Error:



#### *Troubleshoot Error*

1. Open the **event viewer** by running:

`eventvwr.msc`

2. Navigate to **Event Viewer > Windows Logs > Application**.

3. Filter or search for events where:

1. Source = CertificationAuthority
2. Event ID = 53, 54, 55, or similar (these indicate that a request was issued, denied, or is pending).
3. The event message contains details about the reason for denial (if applicable).

4. Use the Find option (right-click on **Application > Find...**) and search by:

- certsrv
- Request ID (if known, for example, 164)

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
- Forwarded Events
- Applications and Services Logs
  - Subscriptions

Level	Date and Time	Source	Event ID	Task Category
Warning	9/10/2025 10:35:48 PM	CertificationAuthority	53	None
Warning	9/10/2025 10:35:47 PM	CertificationAuthority	77	None
Information	9/10/2025 9:18:05 PM	Desktop Window Manager	9027	None
Information	9/10/2025 8:30:13 PM	Security-SPP	16394	None
Information	9/10/2025 8:29:43 PM	Security-SPP	16394	None
Information	9/10/2025 2:13:38 PM	edgeupdate	0	None
Information	9/10/2025 1:47:51 PM	SecCli	1704	None
Information	9/10/2025 4:42:21 AM	Security-SPP	16394	None
Information	9/10/2025 4:41:51 AM	Security-SPP	16394	None
Information	9/10/2025 4:13:54 AM	edgeupdate	0	None
Information	9/9/2025 9:42:38 PM	SecCli	1704	None
Information	9/9/2025 8:45:14 PM	Security-SPP	16394	None
Information	9/9/2025 8:44:44 PM	Security-SPP	16394	None
Information	9/9/2025 6:14:16 PM	edgeupdate	0	None

Event 53, CertificationAuthority

General Details

Active Directory Certificate Services denied request 164 because The public key does not meet the minimum size required by the specified certificate template. 0x00094811 (-2146875375 CERTSRV\_E\_KEY\_LENGTH). The request was for CN=10.88.244.116. Additional information: Denied by Policy Module

Log Name: Application  
Source: CertificationAuthority  
Event ID: 53  
Level: Warning  
User: SYSTEM  
OpCode: Info  
More Information: [EventLog Online Help](#)

Logged: 9/10/2025 10:35:48 PM  
Task Category: None  
Keywords:  
Computer: dnac-ad.dnac.msi.com

Actions

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 53, CertificationAuthority

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

## Troubleshoot Windows Server Logs