Crear plantilla de certificado de Windows Server para Catalyst Center

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

Troubleshoot

Introducción

Este documento describe los pasos para crear una plantilla de certificado en un servidor Windows que ejecute la herramienta Entidad de certificación (CA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Catalyst Center
- Un Windows Server con el rol Entidad de certificación (CA) instalado y configurado
- Privilegios de administrador en Windows Server
- Acceso a la consola de administración de entidades emisoras de certificados
- Conocimiento básico de las plantillas de certificados y las solicitudes de firma de certificados (CSR)

Componentes Utilizados

La información de este documento se basa en Microsoft Windows Server 2022 Standard.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

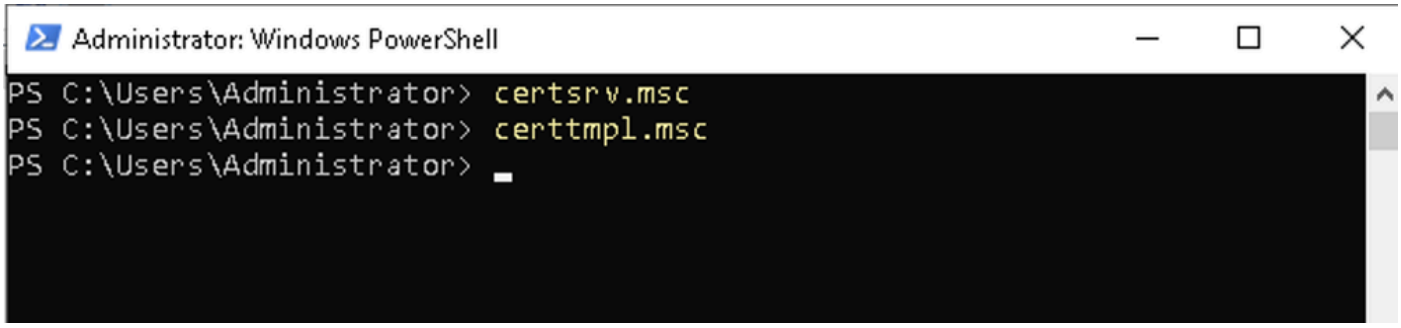
Esta plantilla personalizada resuelve el problema de que las plantillas de CA predeterminadas quitan la autenticación de cliente de los usos de clave extendida. La plantilla personalizada puede firmar la solicitud de firma de certificado (CSR) generada por Catalyst Center.

Configurar

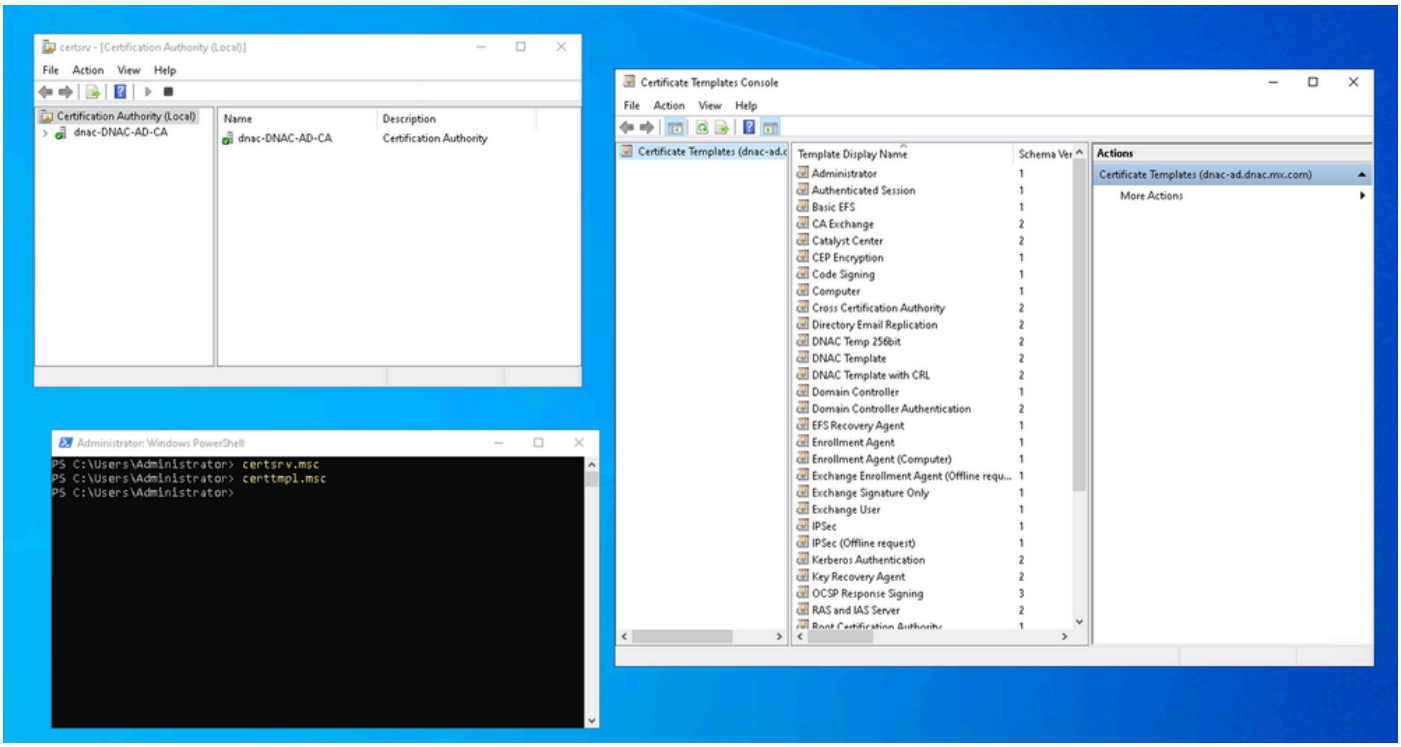
Pasos para revisar y configurar plantillas de certificados en Windows Server con la entidad emisora de certificados (CA).

1. Inicie sesión en Windows Server que aloja la CA mediante Escritorio remoto.
2. Abra una sesión de símbolo del sistema (CMD) o de PowerShell.
3. Inicie las consolas Certificate Authority y Certificate Template ejecutando:

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

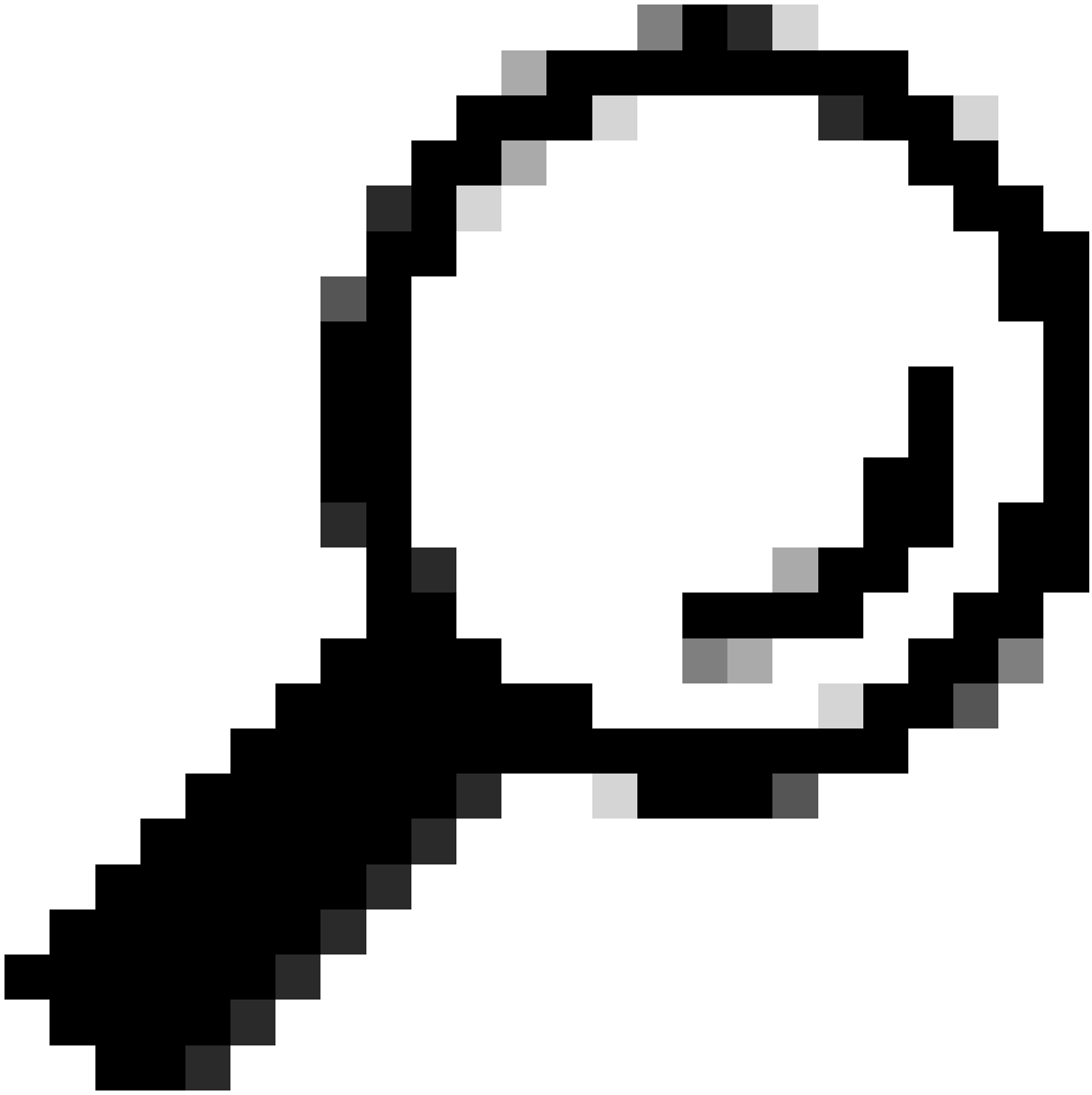


Administración Comandos de Powershell



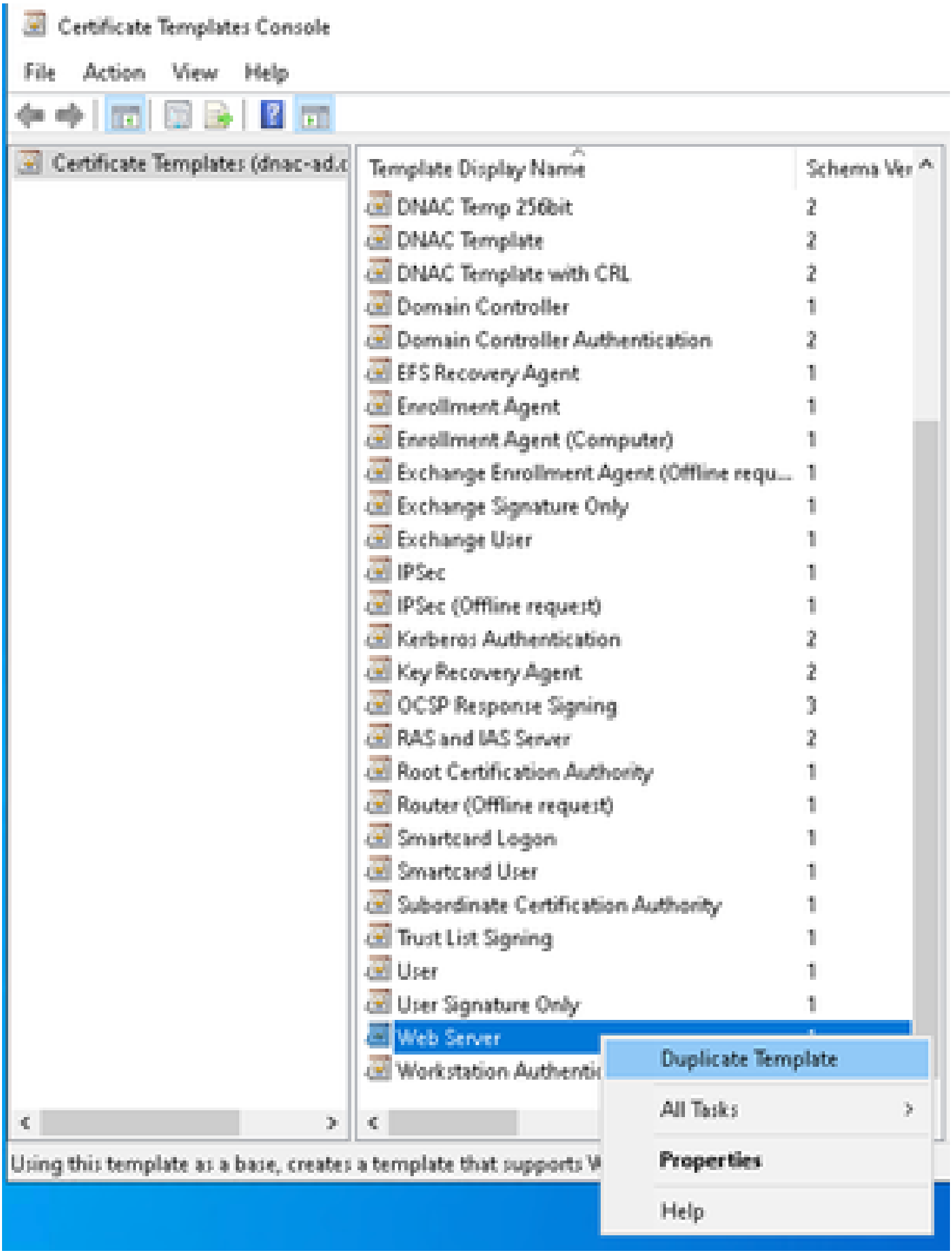
Ejemplo de Windows Server

4. En la Consola de Plantilla de Certificados, localice la plantilla que desea clonar para crear una nueva plantilla personalizable.



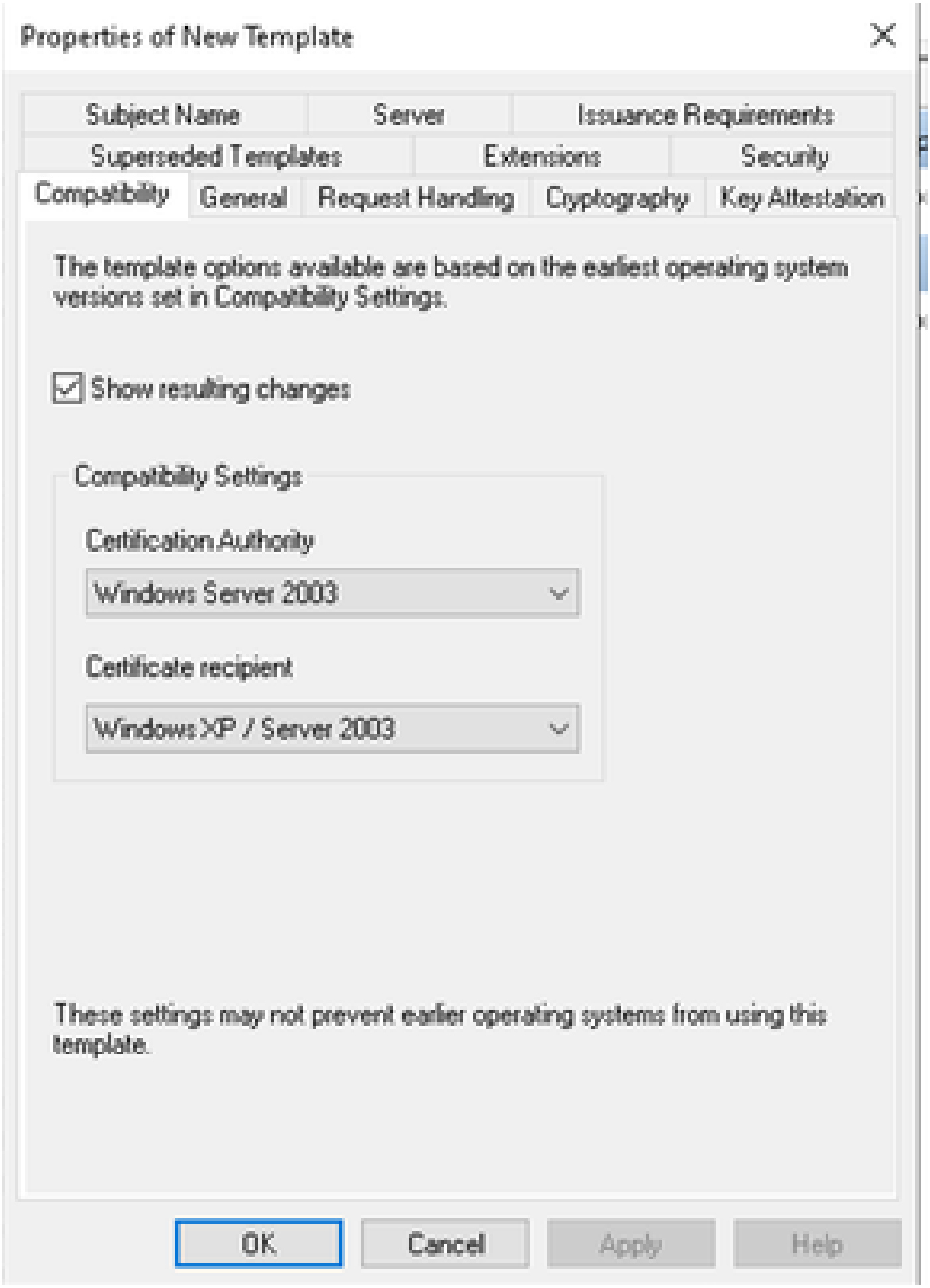
Consejo: Utilice la plantilla de servidor web, ya que ya incluye todos los parámetros necesarios para el certificado de Catalyst Center.

- Ejemplo: haga clic con el botón derecho en el servidor web y seleccione plantilla duplicada.



Duplicar plantilla

5. Una nueva plantilla está abierta, modifíquela con las características requeridas.


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. Modifique la nueva plantilla de la siguiente manera:

6.1 Ficha General.

- Introduzca un nombre de plantilla (por ejemplo, Plantilla de Catalyst Center).
- Defina el período de validez (valor predeterminado: 2 años).

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

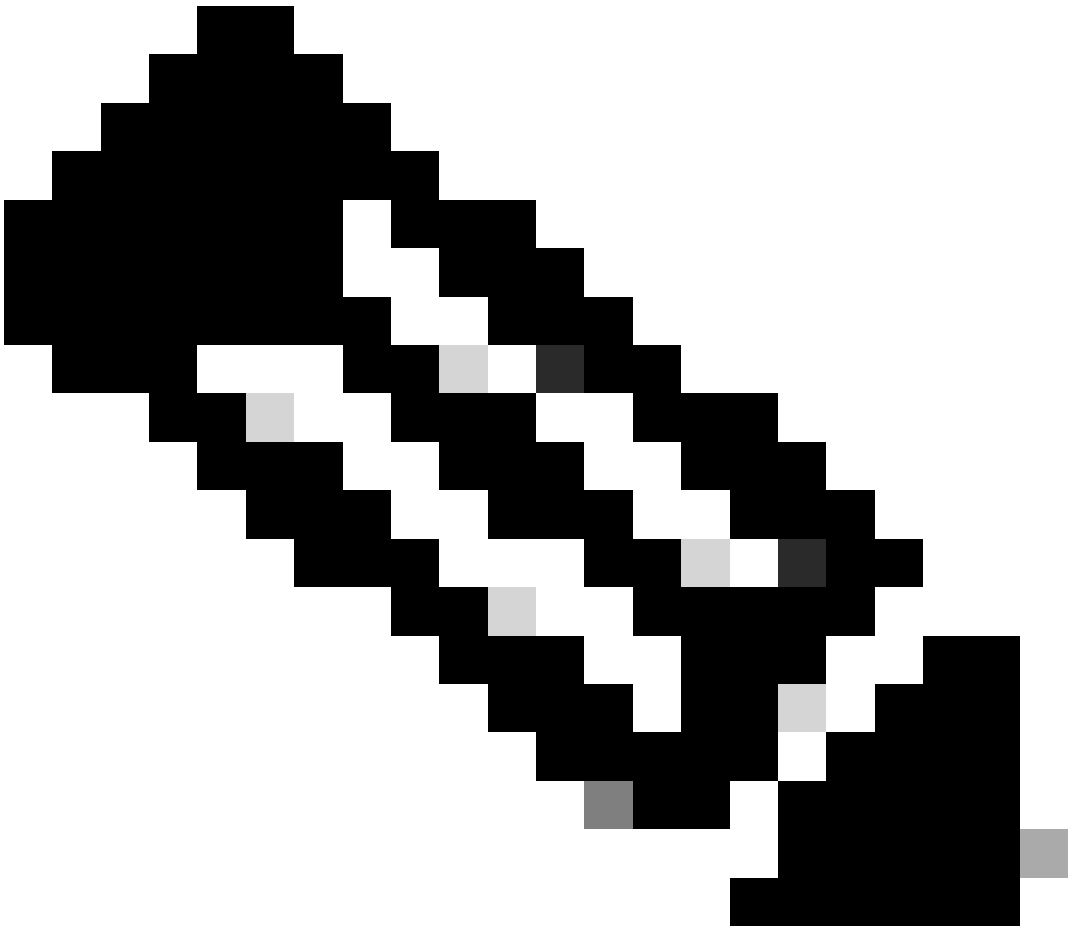
Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

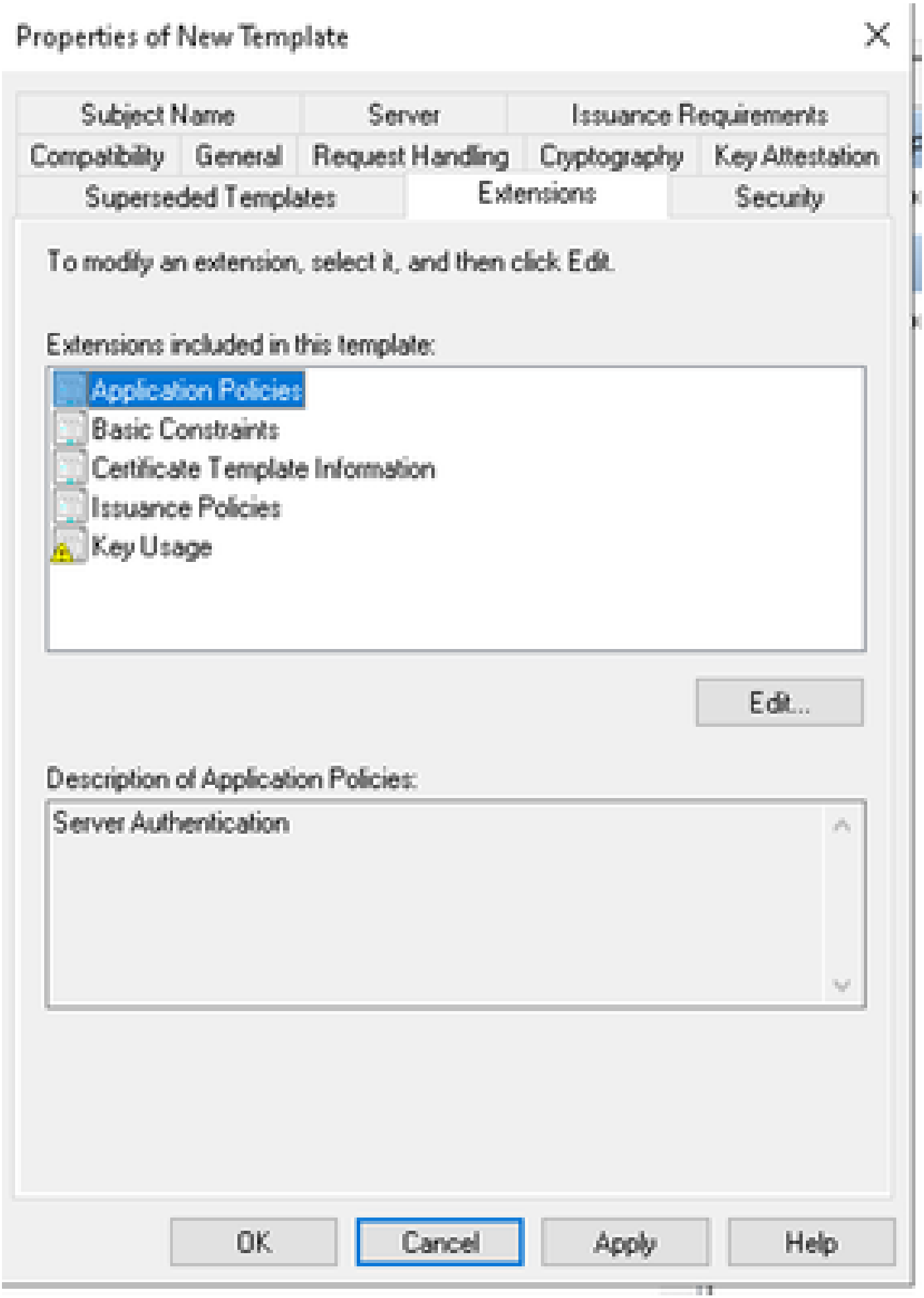
Nombre de plantilla

6.2 Ficha Extensiones.

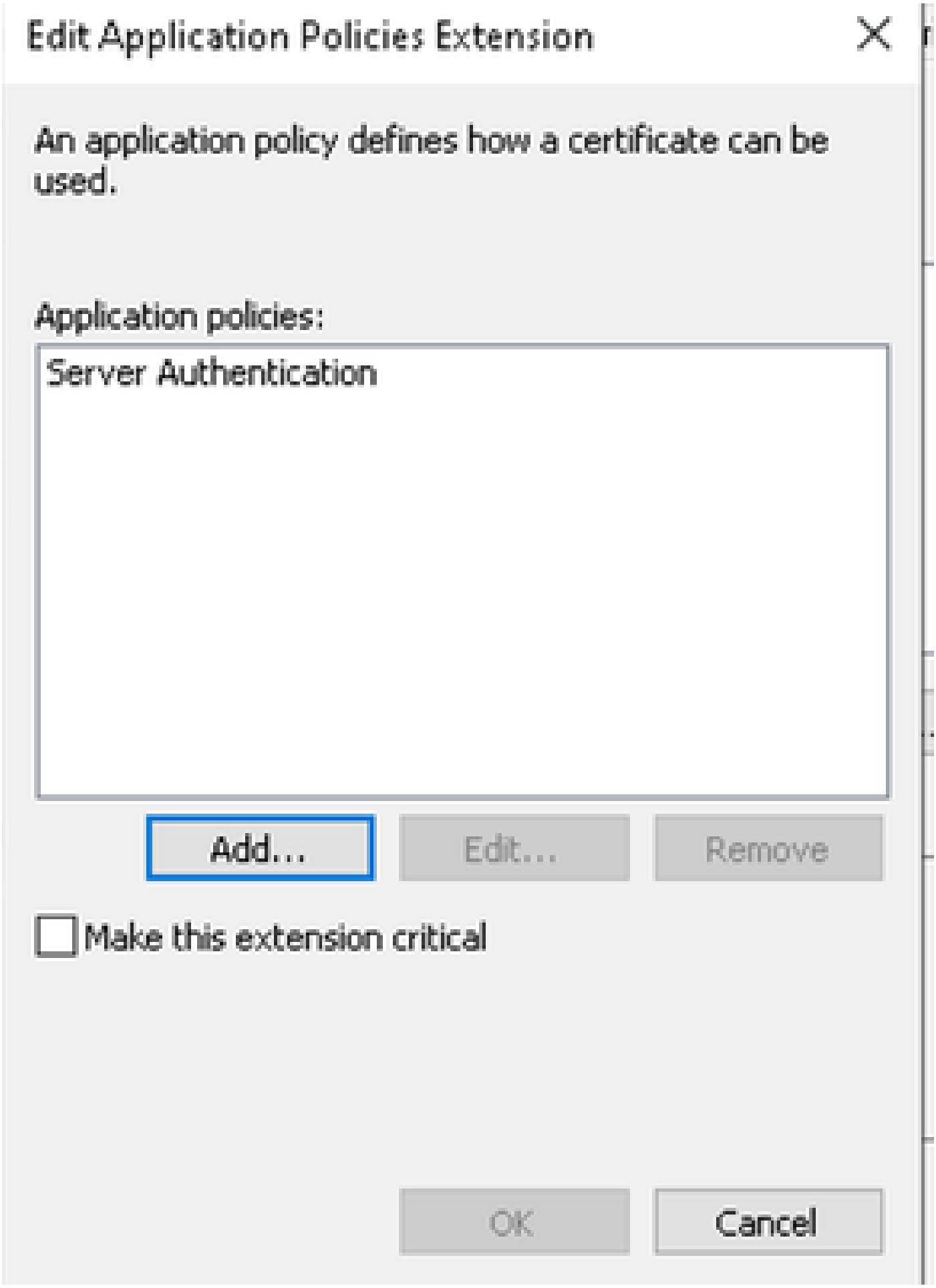
- Desplácese hasta directivas de aplicación y haga clic en editar.



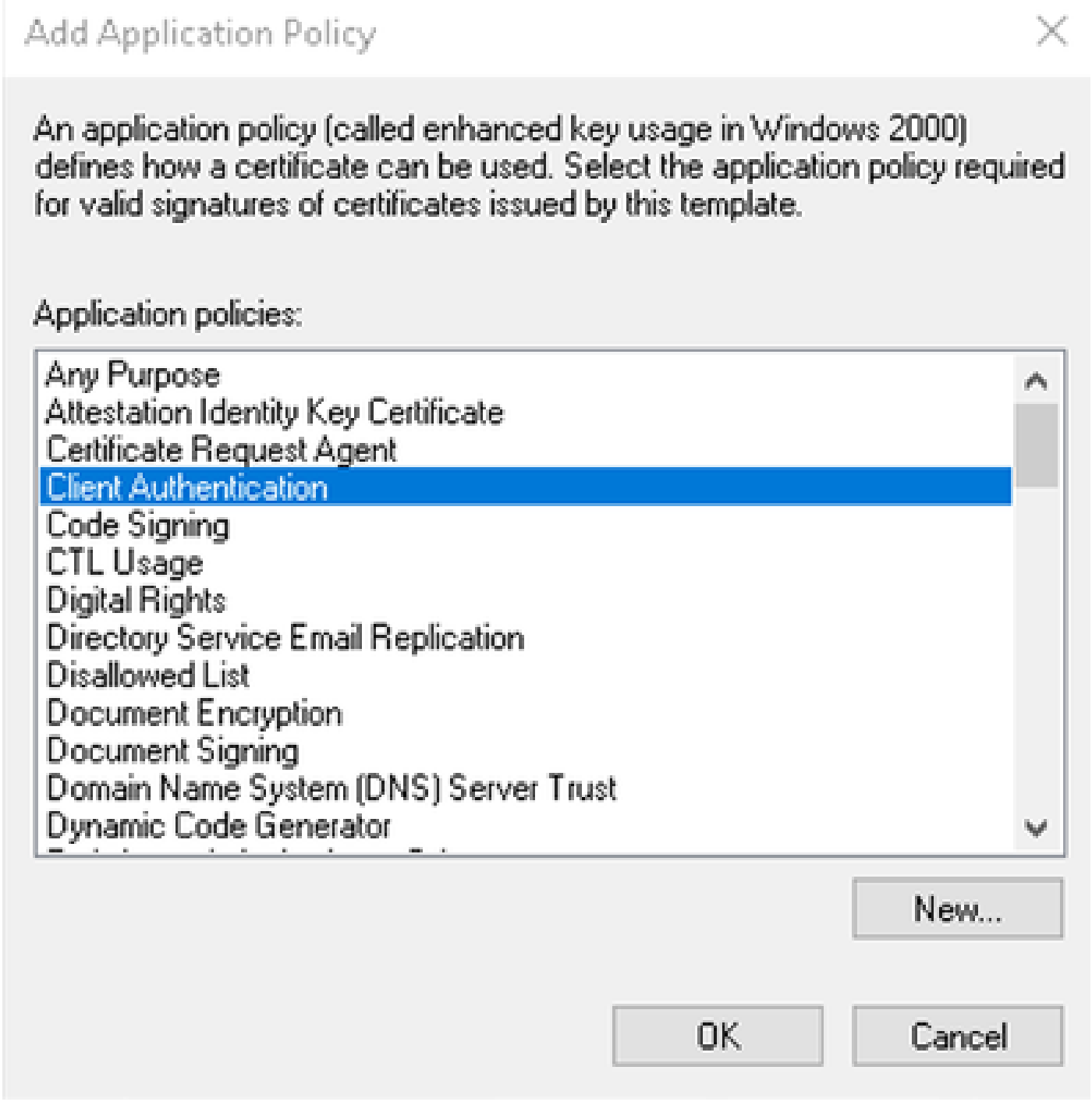
Nota: En esta ficha, confirme que la plantilla incluye las extensiones obligatorias de uso de claves requeridas por el certificado de Catalyst Center, como keyEncipherment y digitalSignature. Estos elementos ya están presentes en la plantilla de servidor Web predeterminada utilizada como base.


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

- Haga clic en add, localice client authentication y haga clic en ok para incluirlo.

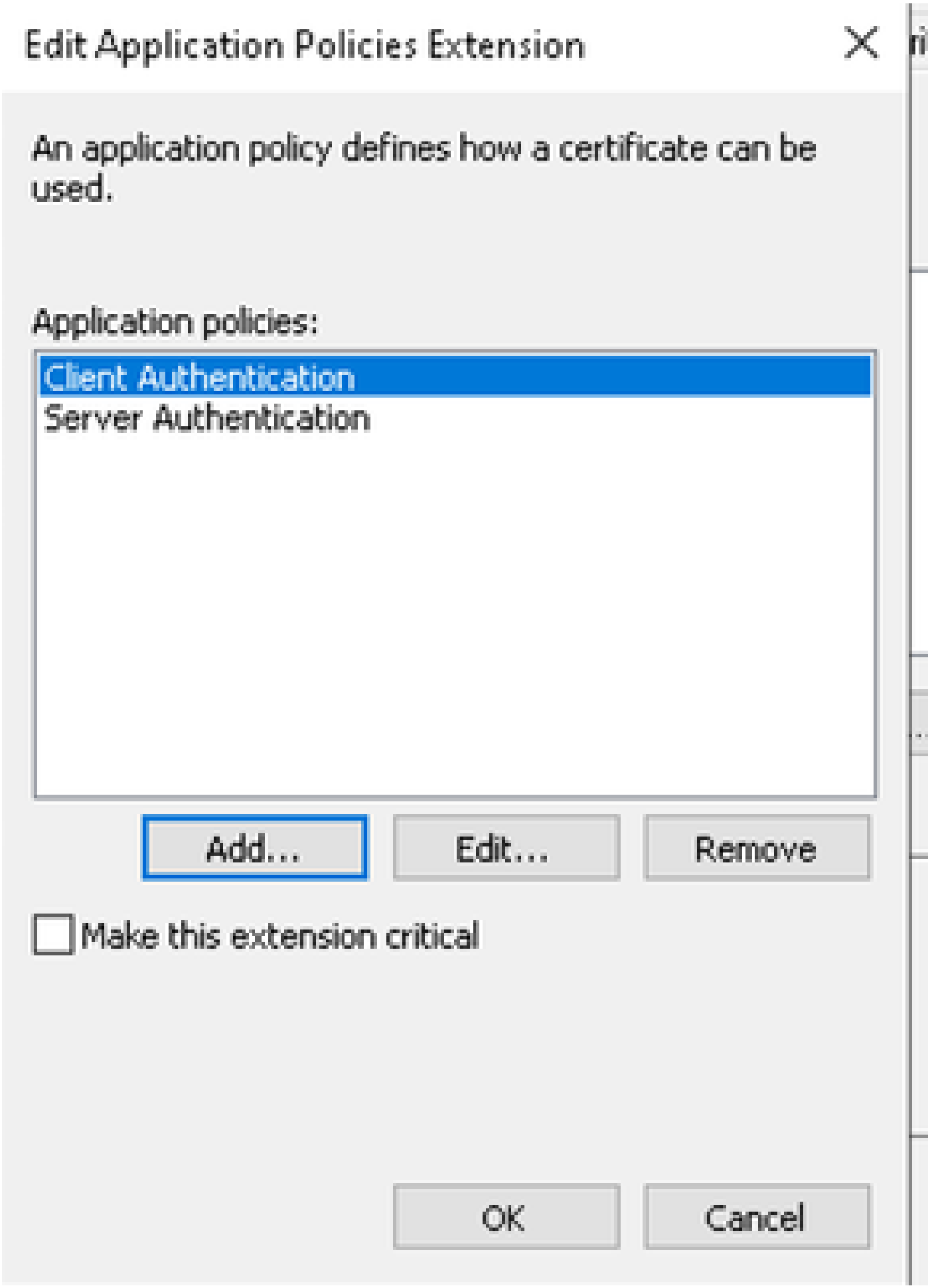


Autenticación del cliente



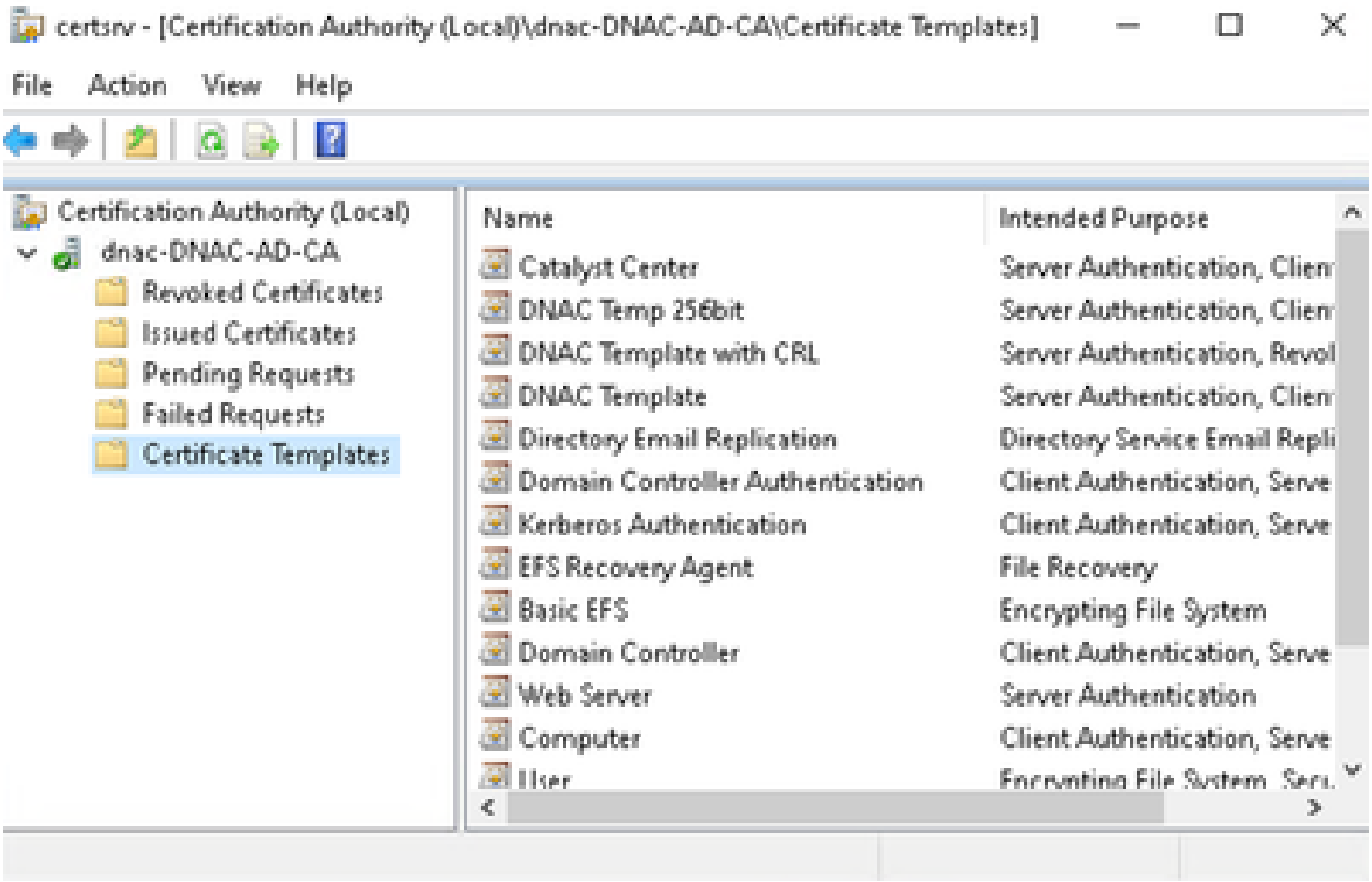
Agregar política de aplicación

- Confirme que la plantilla muestre Autenticación del cliente junto con los usos predeterminados.


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. Haga clic en aplicar y luego en aceptar.

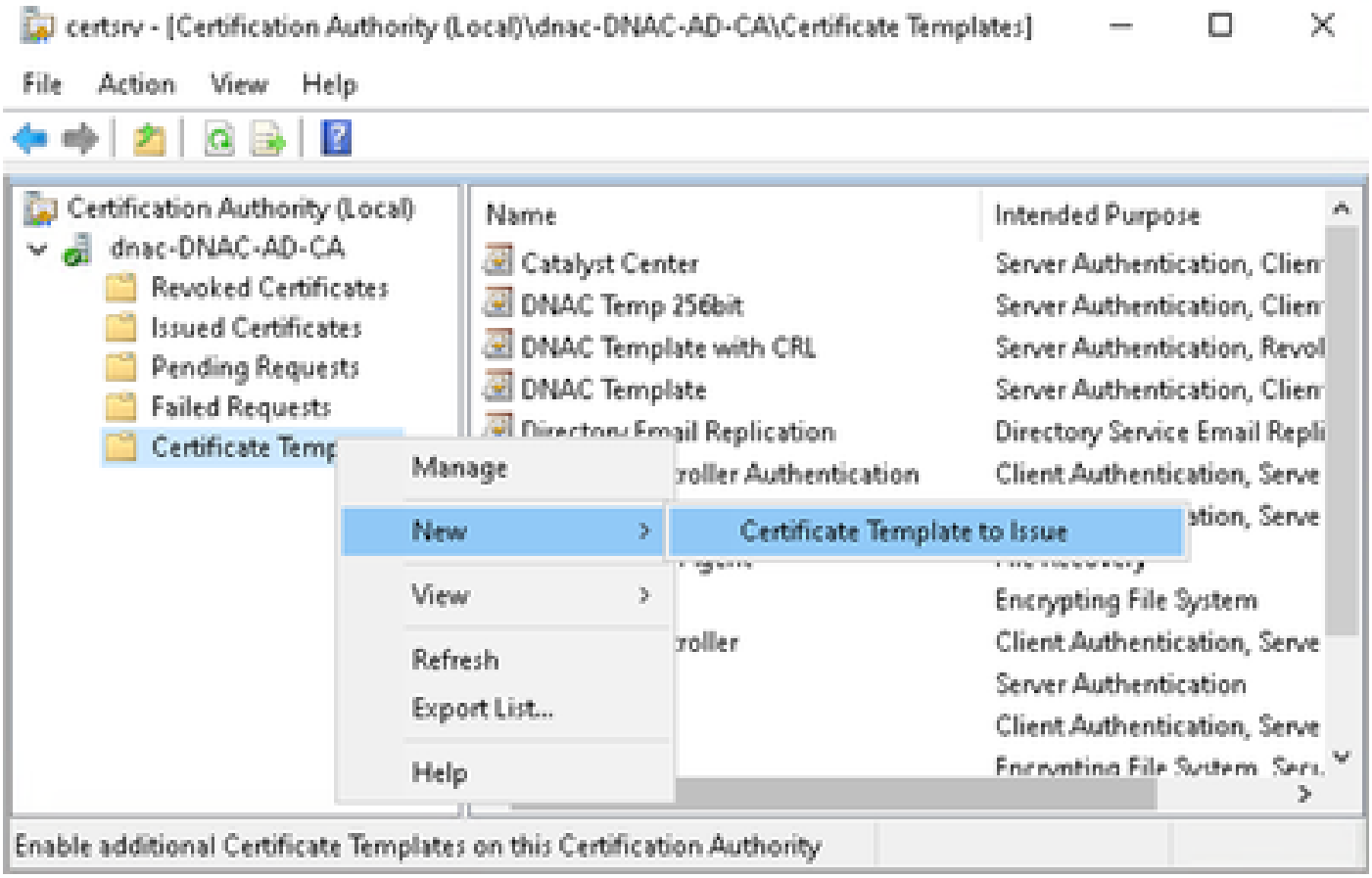
8. En la consola Certificate Authority, expanda el árbol CA y seleccione la carpeta certificate templates.



Plantillas de certificado de árbol de CA

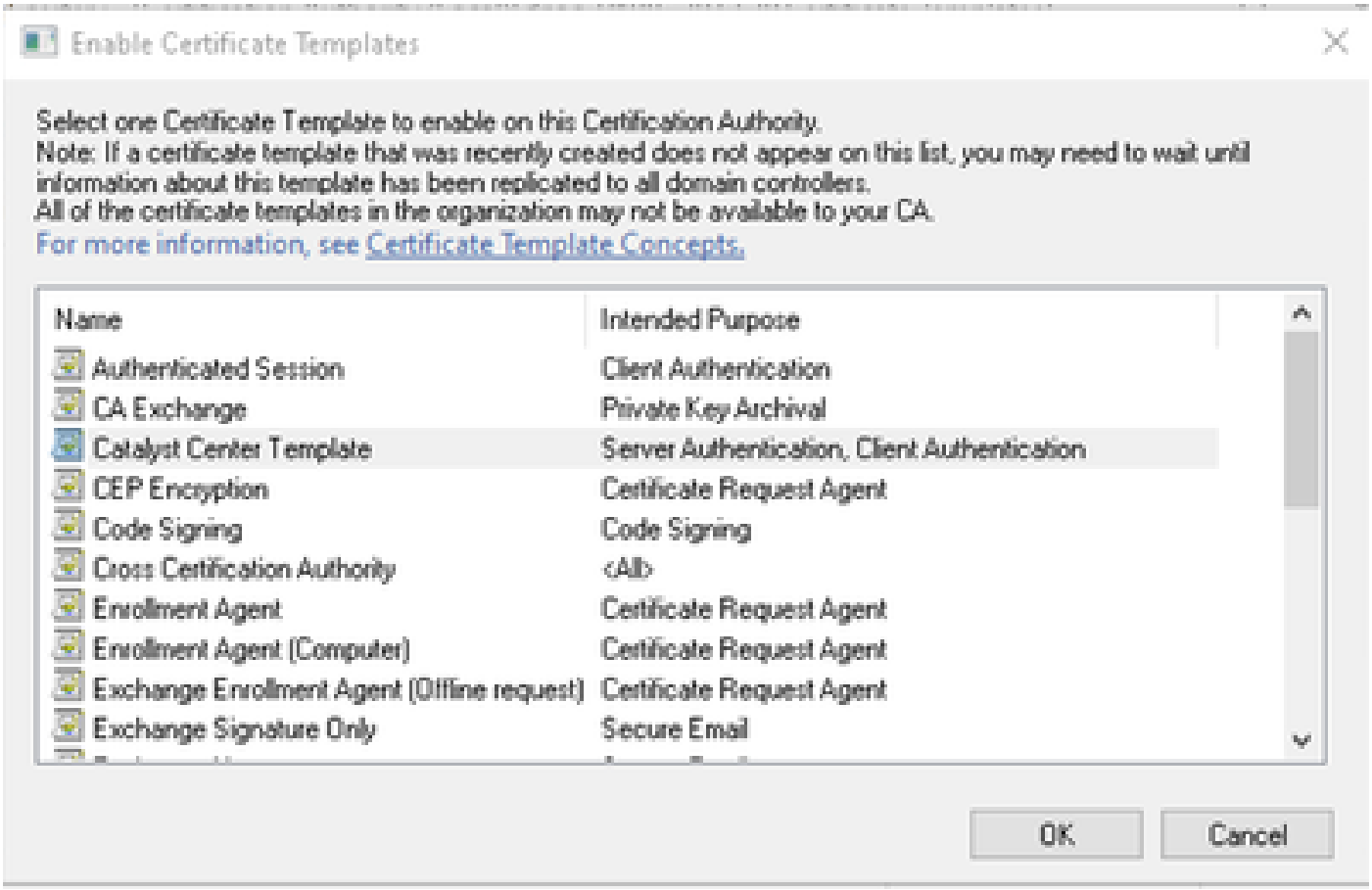
9. Haga clic con el botón derecho del ratón en la carpeta plantillas de certificado y seleccione:

Nuevo > Plantilla de certificado para emitir.



Nueva plantilla de certificado para emitir

10. En la nueva ventana, seleccione la plantilla recién creada (por ejemplo, Plantilla de Catalyst Center) y haga clic en aceptar.

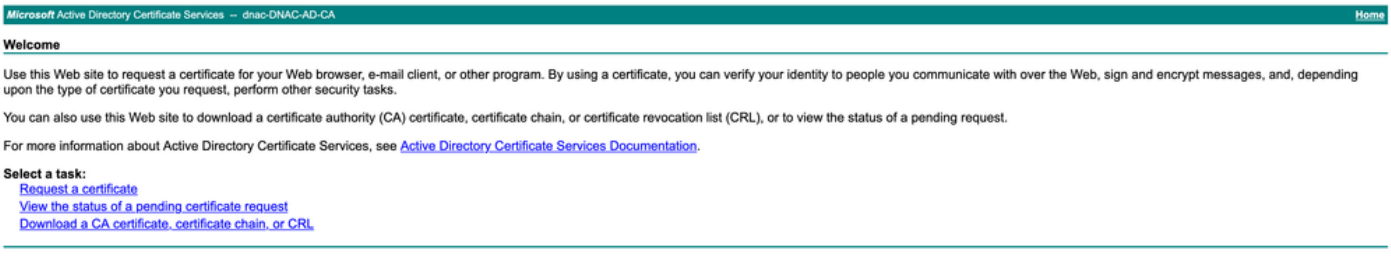


Plantilla de Catalyst Center

11. La plantilla aparece ahora en la lista Plantillas de certificado de la CA.

12. Abra un explorador y vaya a:

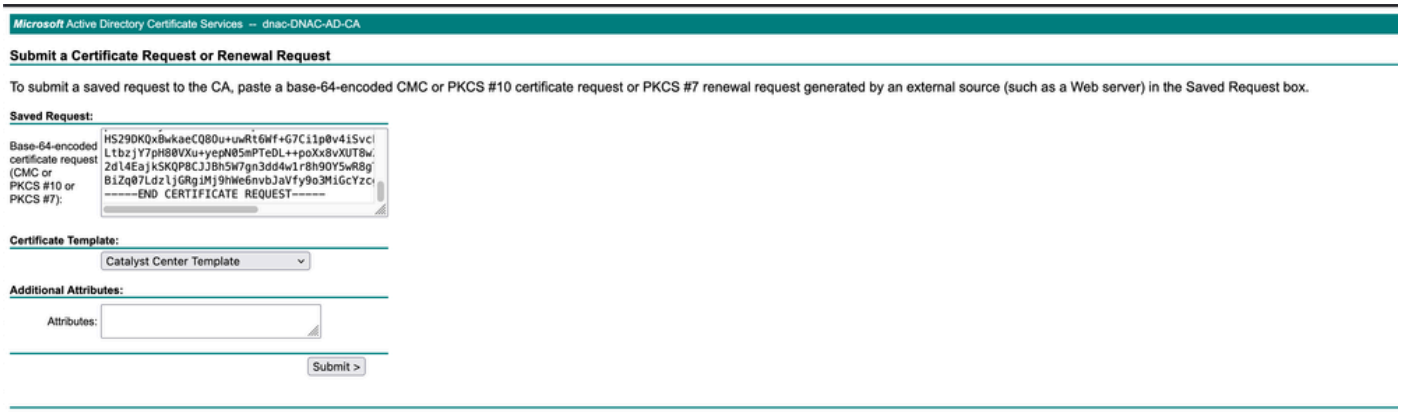
```
http://localhost/certsrv/
```



Página de inicio de sesión http://localhost/certsrv/

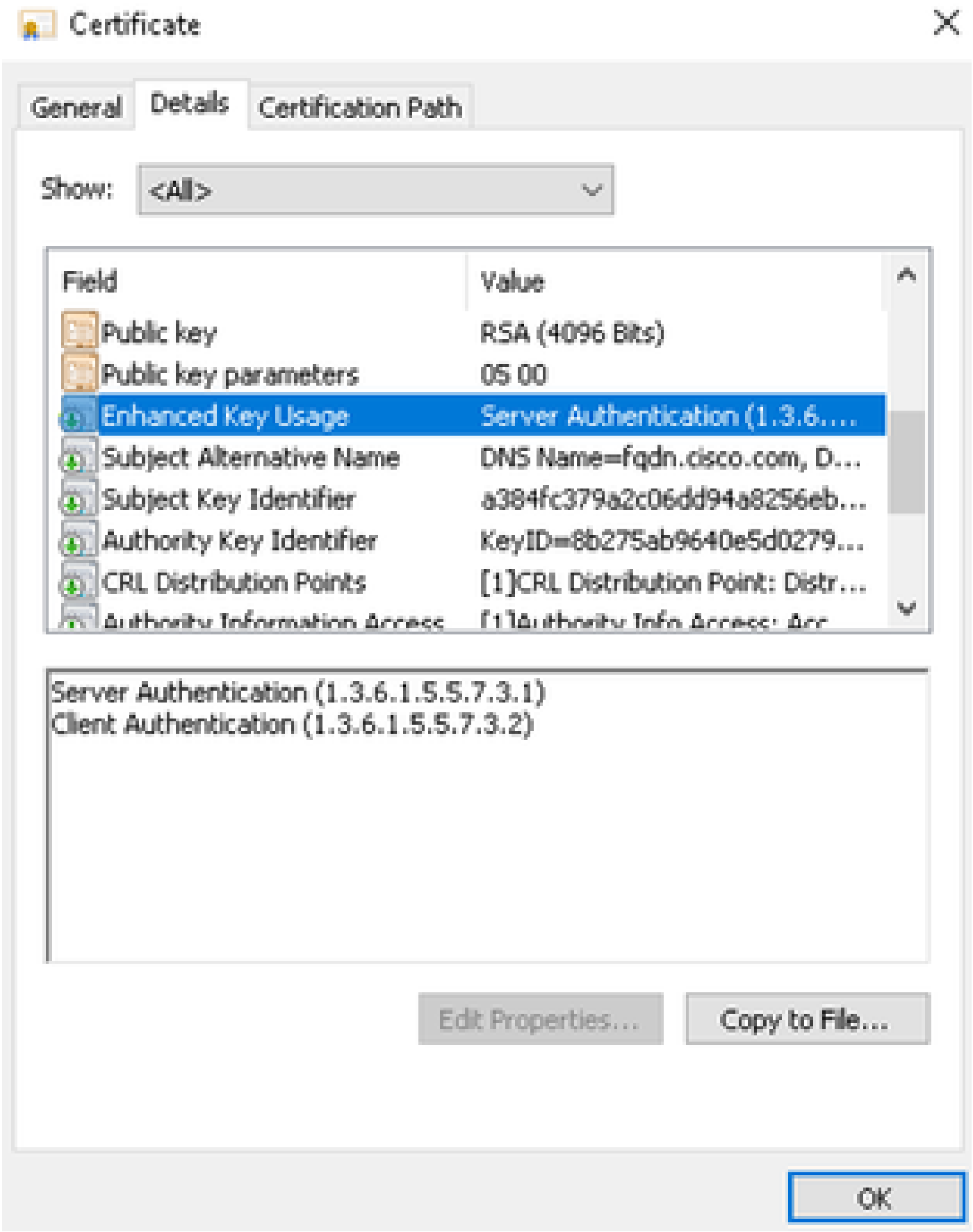
13. Seleccione solicitar un certificado y, a continuación, solicitud de certificado avanzada, para comprobar que la nueva plantilla está disponible.

14. En esta página, ejecute el CSR y seleccione la plantilla recién creada para generar el certificado firmado.



Solicitar un certificado

13. El certificado se genera con las extensiones correctas, como se muestra en el ejemplo.



Ejemplo de certificado

Troubleshoot

Si encuentra errores al firmar el CSR, revise los registros de Windows Server para obtener más detalles:

Error:

Error de Troubleshooting

1. Abra el visor de eventos ejecutando:

```
eventvwr.msc
```

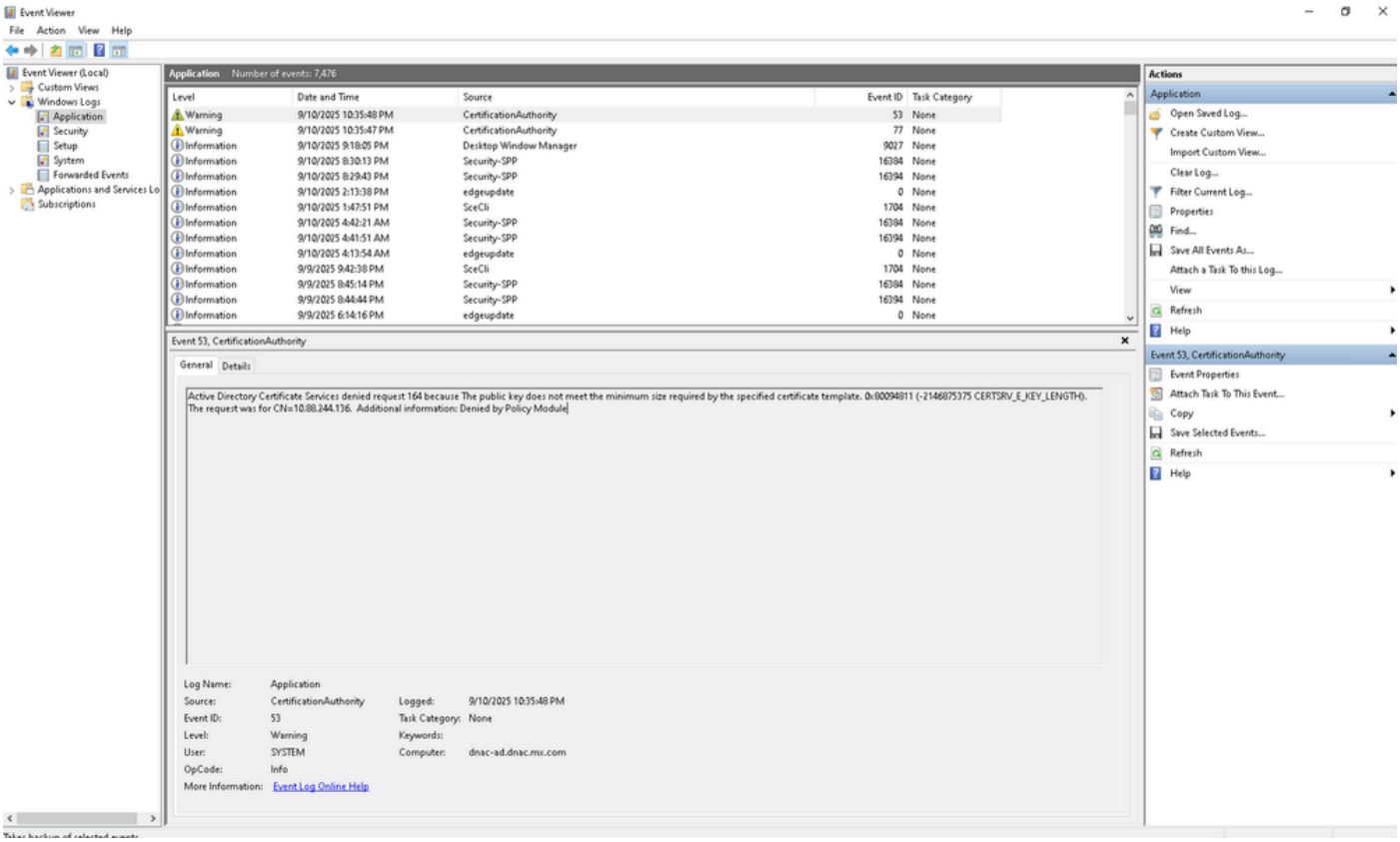
2. Vaya a Visor de eventos > Registros de Windows > Aplicación.

3. Filtre o busque eventos en los que:

    1. Origen = Entidad emisora de certificados
    2. ID de evento = 53, 54, 55 o similar (esto indica que se emitió, denegó o está pendiente una solicitud).
    3. El mensaje de evento contiene detalles sobre el motivo de la denegación (si procede).

4. Utilice la opción Find (haga clic con el botón derecho en Application > Find...) y busque por:

- certsrv
- ID de solicitud (si se conoce, por ejemplo, 164)



Solucionar problemas de registros de Windows Server

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).