Crea modello di certificato di Windows Server per Catalyst Center

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Configurazione

Risoluzione dei problemi

Introduzione

In questo documento viene descritto come creare un modello di certificato in un server Windows che esegue lo strumento CA (Certification Authority).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Catalyst Center
- Un server Windows con il ruolo Autorità di certificazione (CA) installato e configurato
- Privilegi di amministratore sul server Windows
- Accesso alla console di gestione Autorità di certificazione
- Conoscenze base dei modelli di certificato e delle richieste di firma di certificato (CSR)

Componenti usati

Le informazioni fornite in questo documento si basano su Microsoft Windows Server 2022 Standard.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

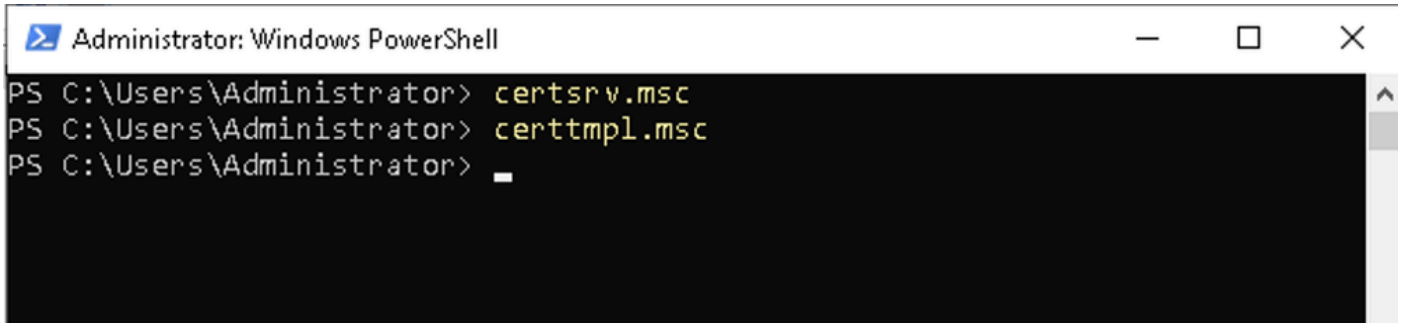
Questo modello personalizzato risolve il problema relativo alla rimozione dell'autenticazione client dagli utilizzi chiavi estesi da parte dei modelli CA predefiniti. Il modello personalizzato è in grado di firmare la richiesta di firma del certificato (CSR) generata da Catalyst Center.

Configurazione

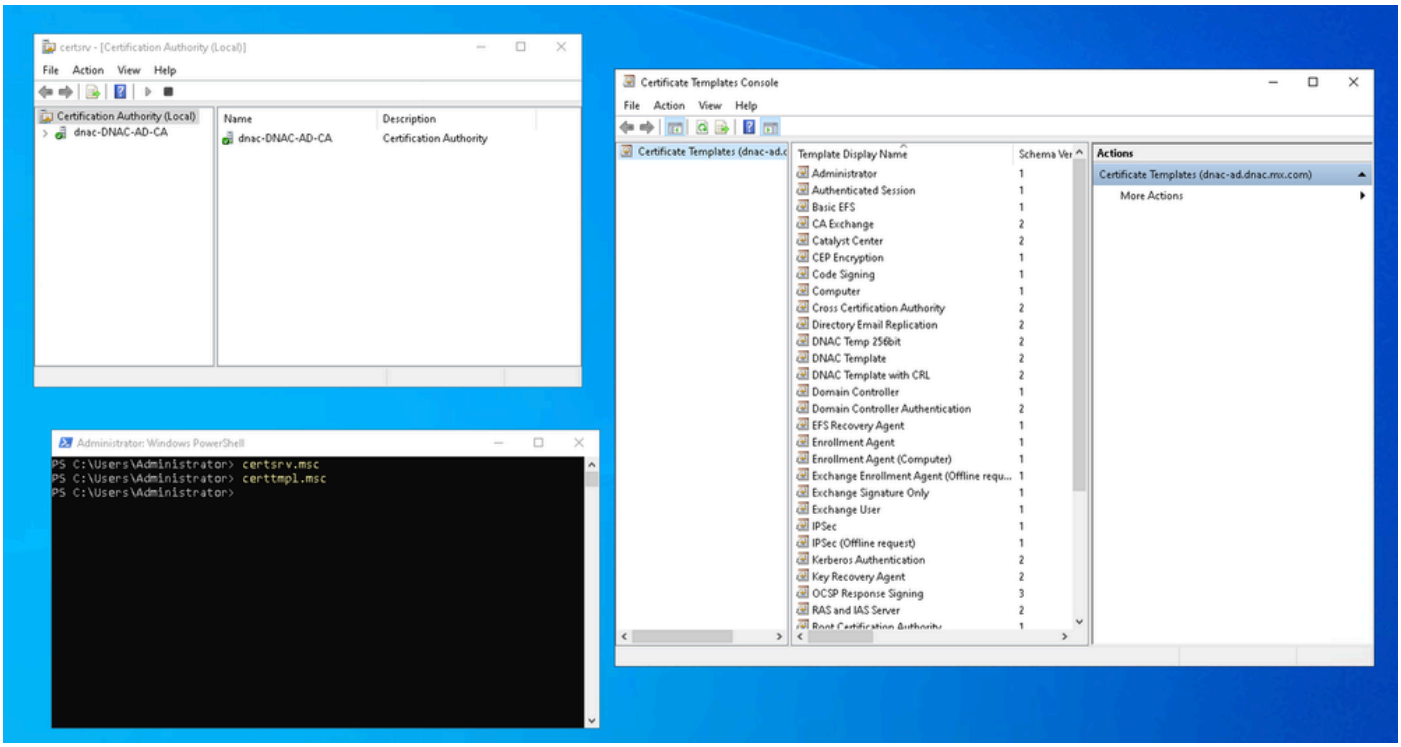
Passaggi per esaminare e configurare i modelli di certificato in Windows Server con l'Autorità di certificazione (CA).

1. Accedere al server Windows che ospita la CA tramite Desktop remoto.
2. Aprire un prompt dei comandi (CMD) o una sessione di PowerShell.
3. Avviare le console dell'autorità di certificazione e dei modelli di certificato eseguendo:

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

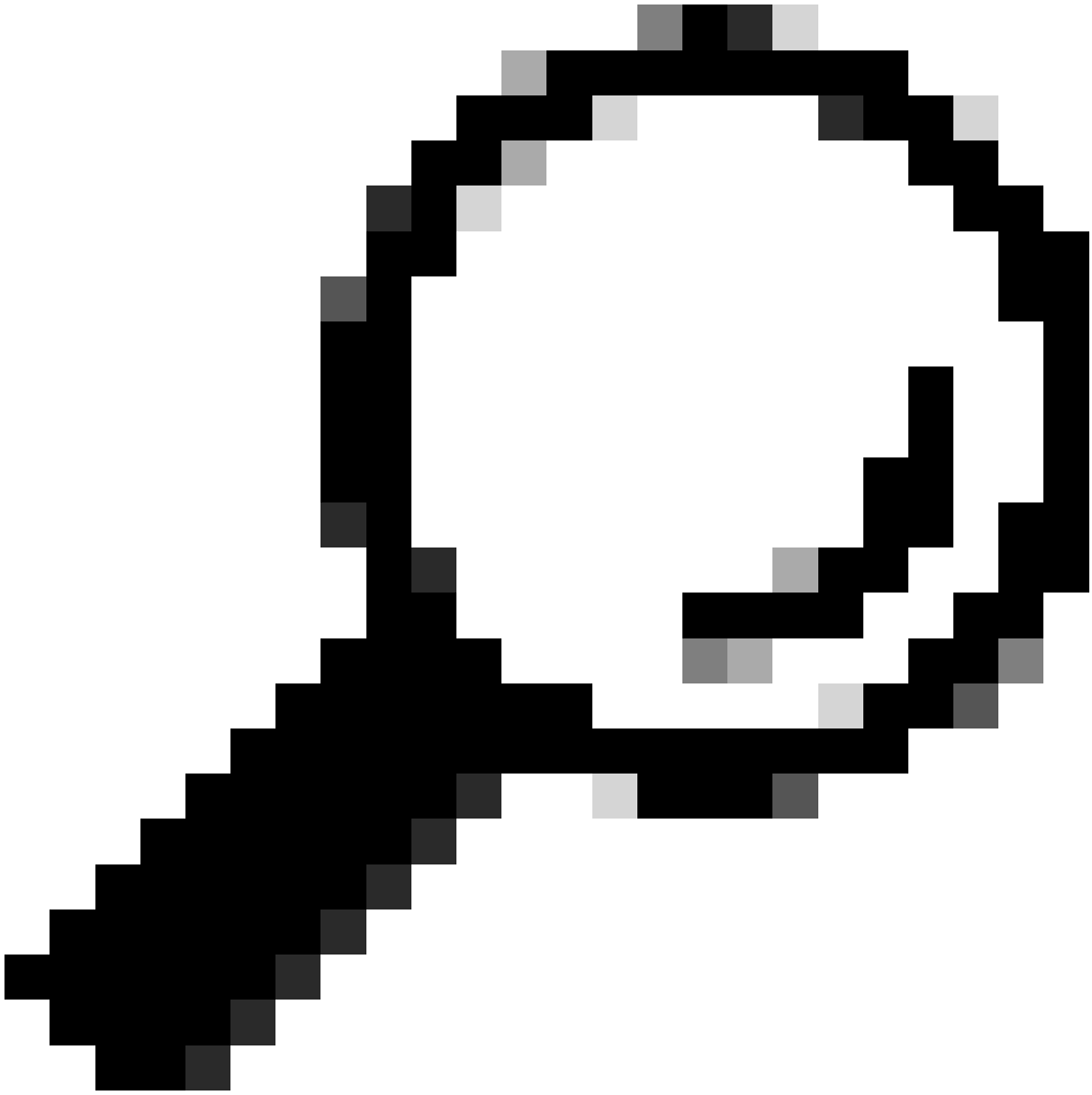


Comandi di Administration Powershell



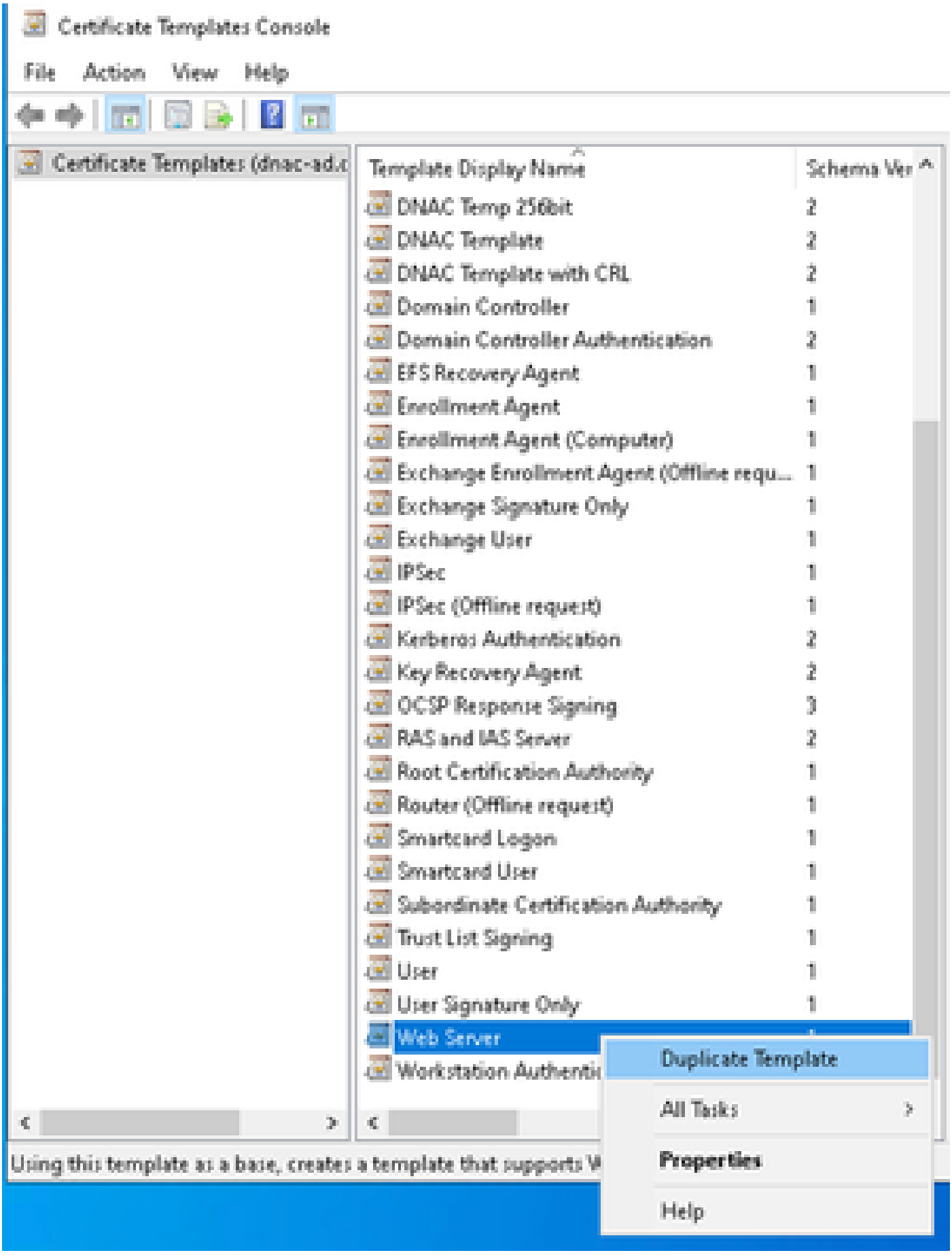
Esempio di Windows Server

4. Nella console dei modelli di certificato, individuare il modello da duplicare per creare un nuovo modello personalizzabile.



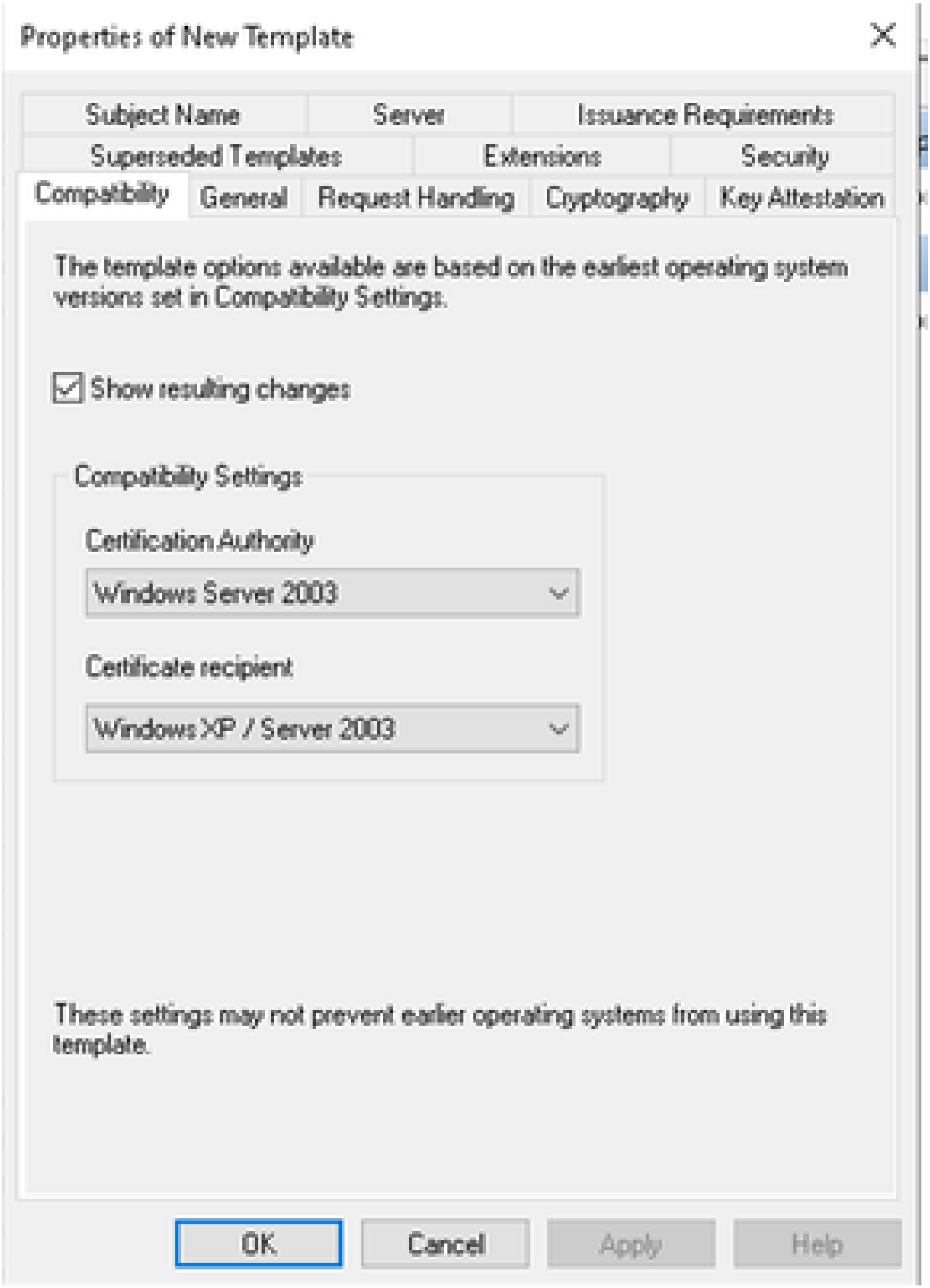
Suggerimento: Utilizzare il modello Server Web poiché include già tutti i parametri richiesti per il certificato del Centro Catalyst.

- Esempio: fare clic con il pulsante destro del mouse sul server web e selezionare duplica modello.



Duplica modello

5. È aperto un nuovo modello, modificarlo con le caratteristiche richieste.


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. Modificare il nuovo modello come segue:

6.1 Scheda Generale.

- Immettere il nome di un modello, ad esempio Modello Catalyst Center.
- Definire il periodo di validità (impostazione predefinita: 2 anni).

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

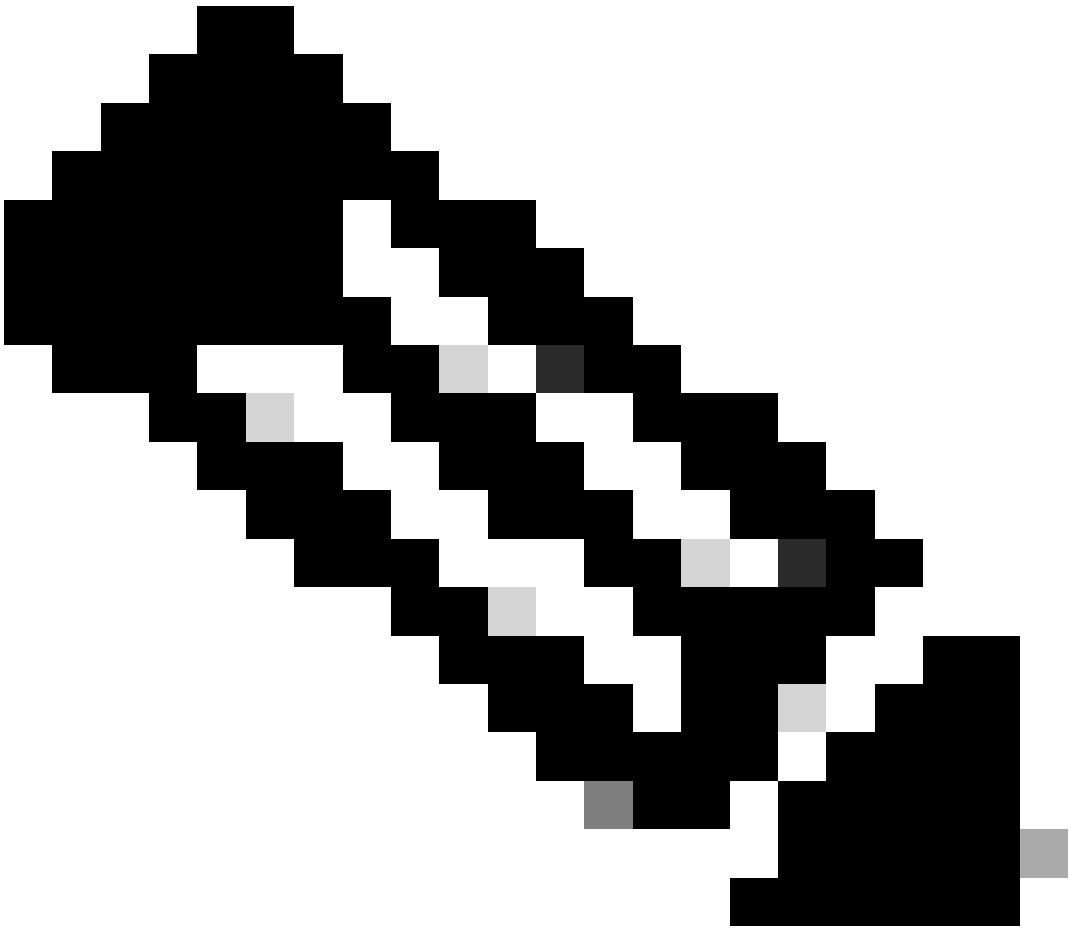
Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

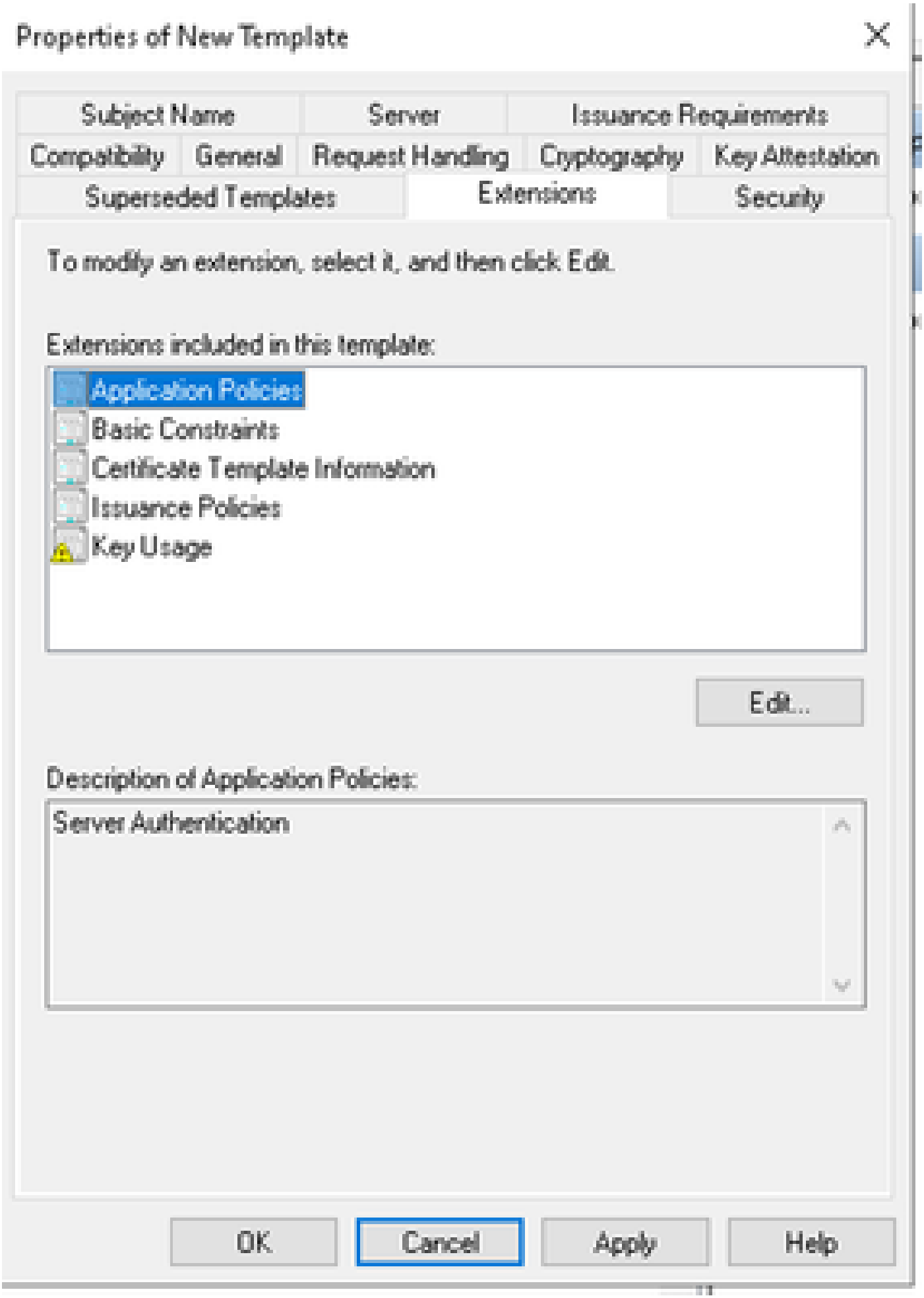
Nome modello

6.2 Scheda Estensioni.

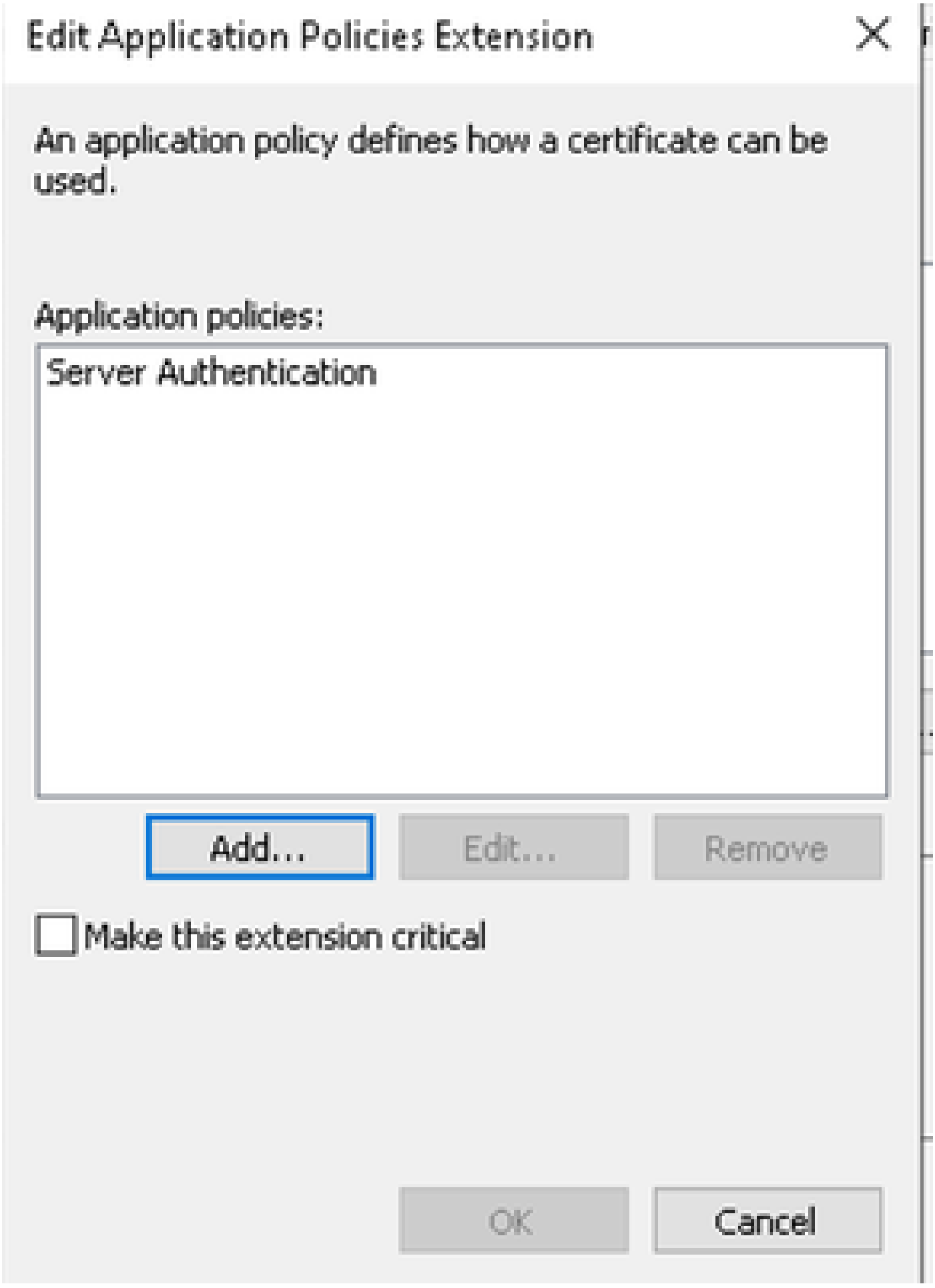
- Passare ai criteri di applicazione e fare clic su Modifica.



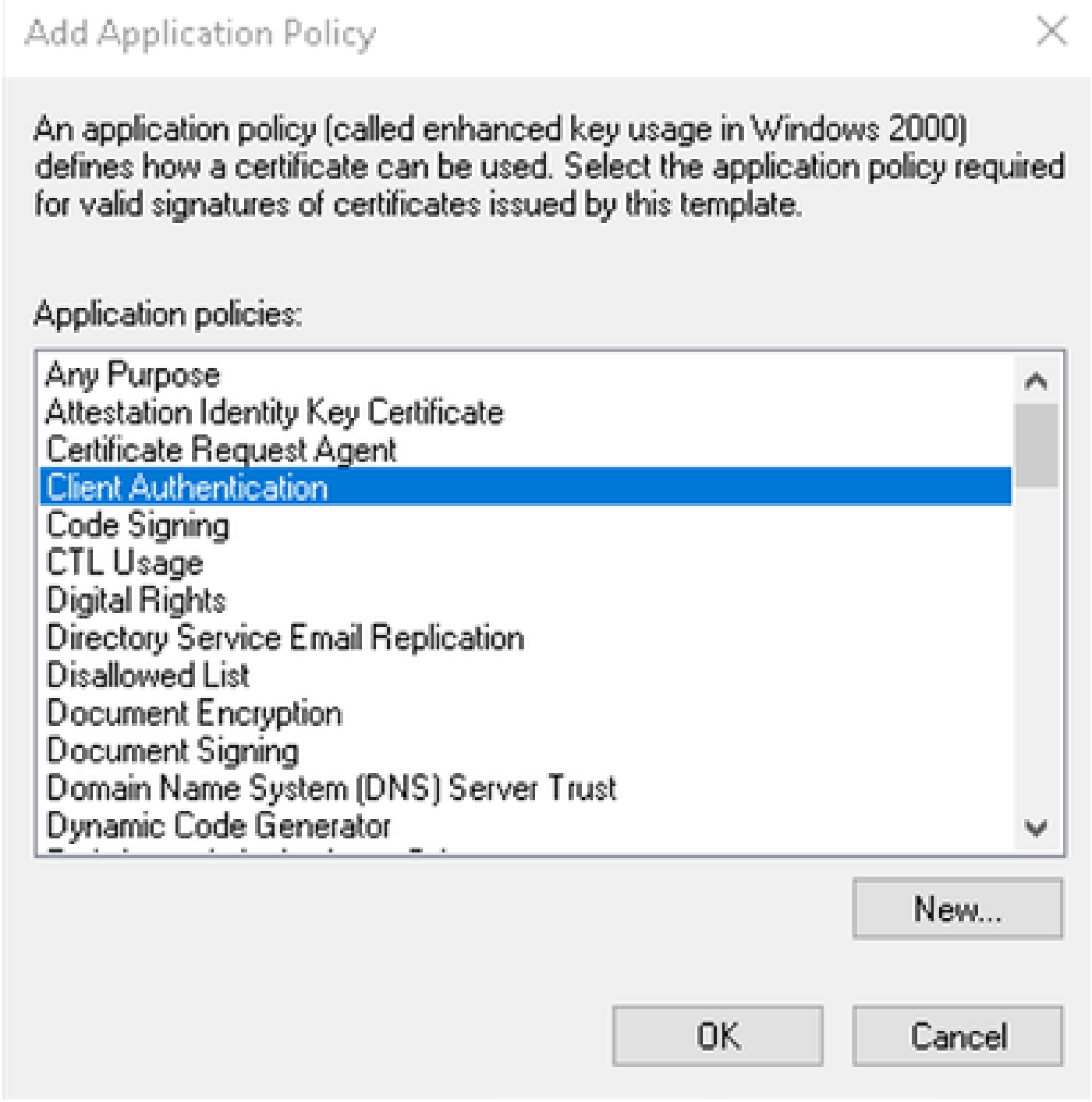
Nota: In questa scheda verificare che il modello includa le estensioni di utilizzo chiavi obbligatorie richieste dal certificato del Catalyst Center, ad esempio keyEncipherment e digitalSignature. Questi sono già presenti nel modello predefinito del server Web utilizzato come base.


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

- Fare clic su add, individuare l'autenticazione client e fare clic su ok per includerla.

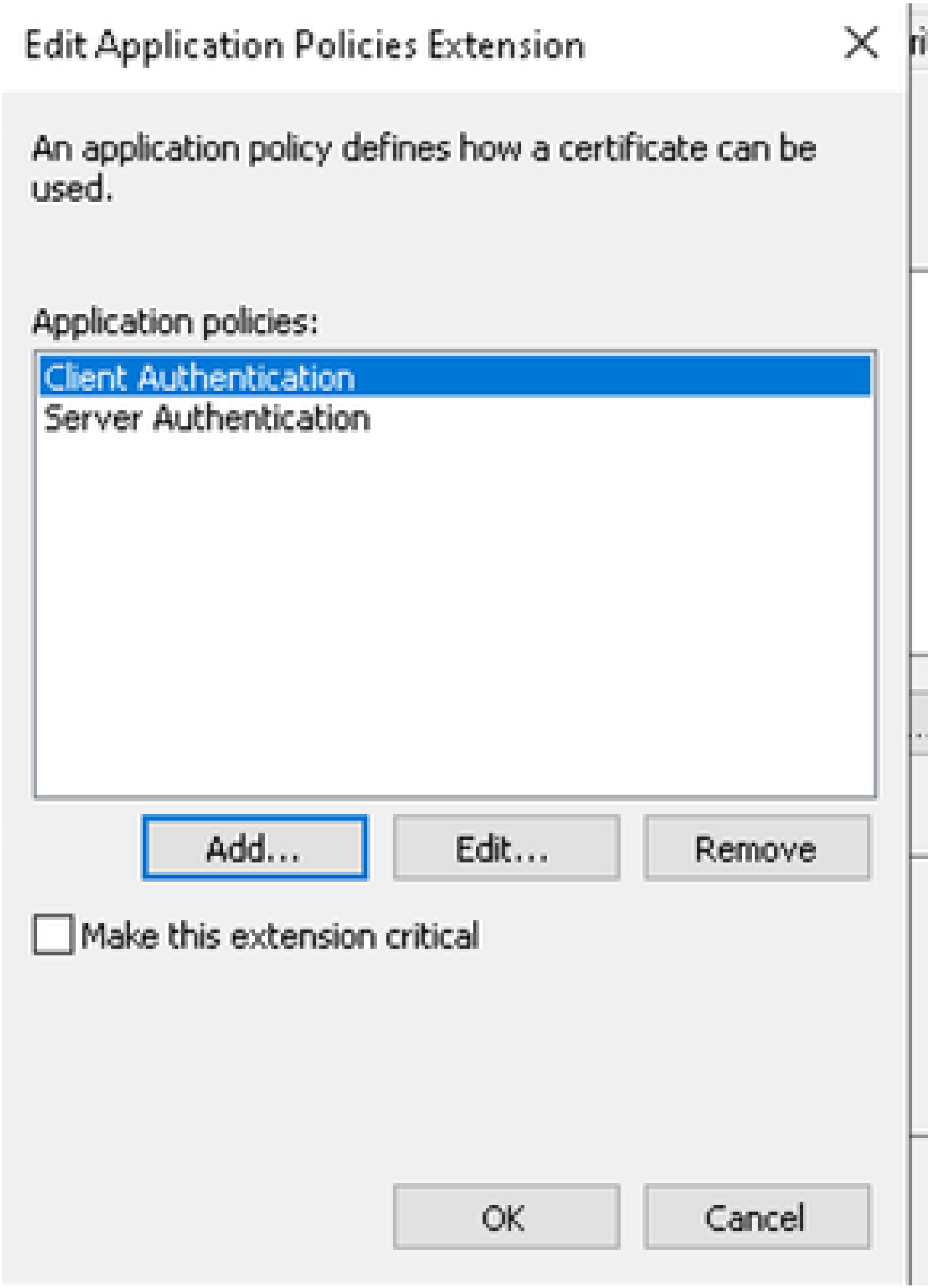


Autenticazione client



Aggiungi criterio di applicazione

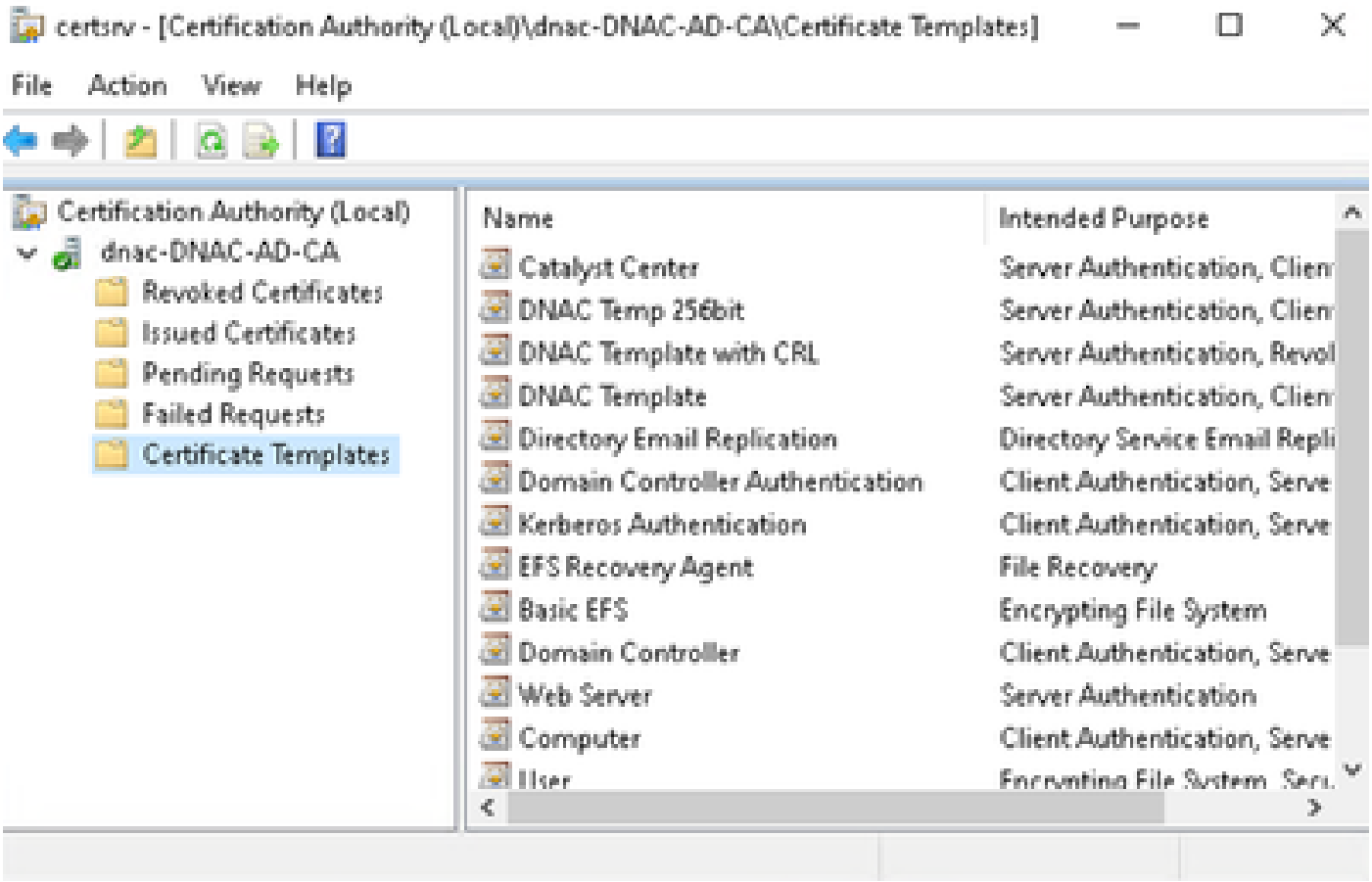
- Confermare che il modello visualizzi Autenticazione client insieme agli utilizzi predefiniti.


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

Estensione Criteri di applicazione

7. Fare clic su apply (Applica), quindi su ok.

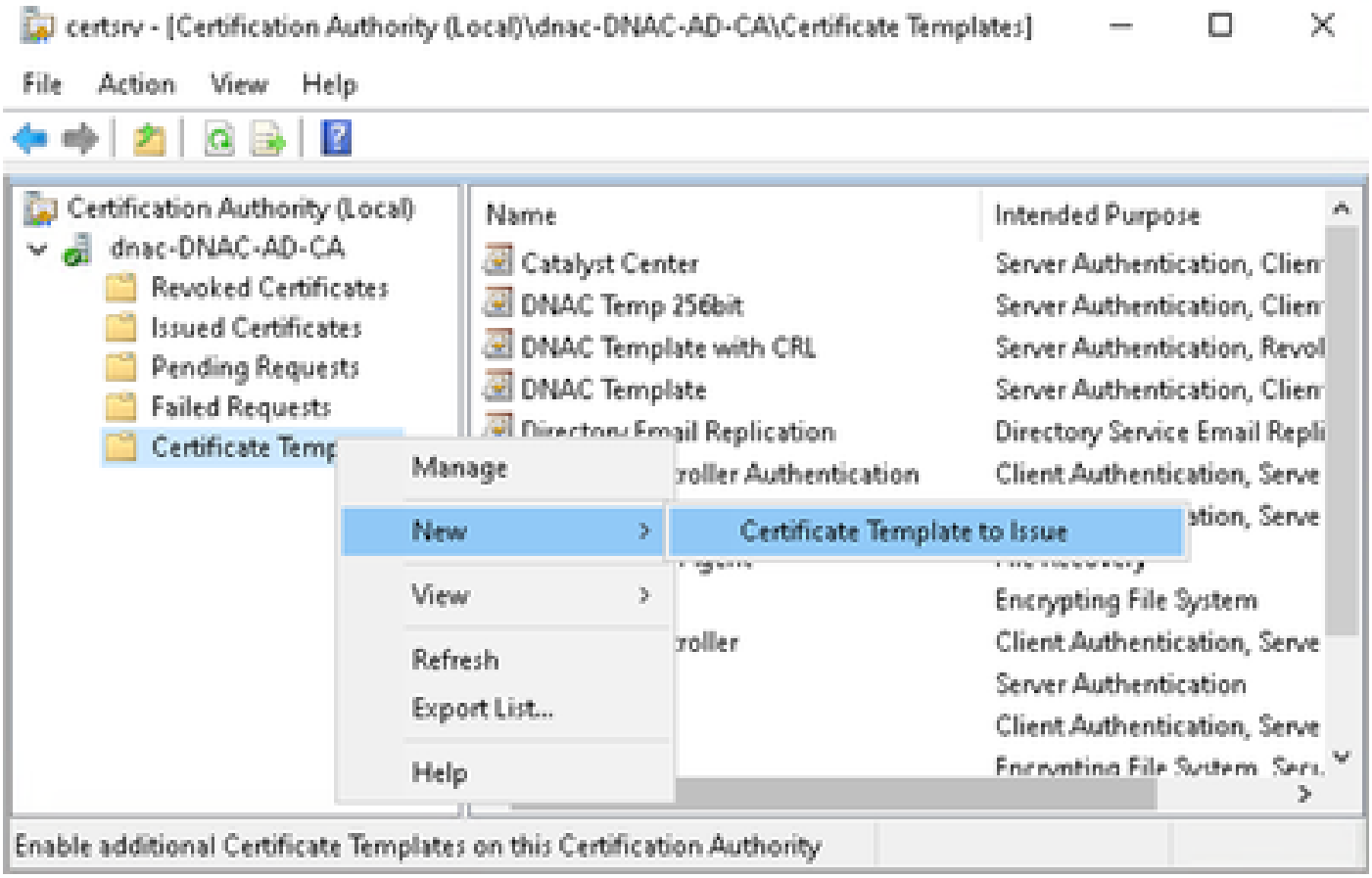
8. Nella console Autorità di certificazione, espandere la struttura CA e selezionare la cartella dei modelli di certificato.



Modelli di certificato struttura CA

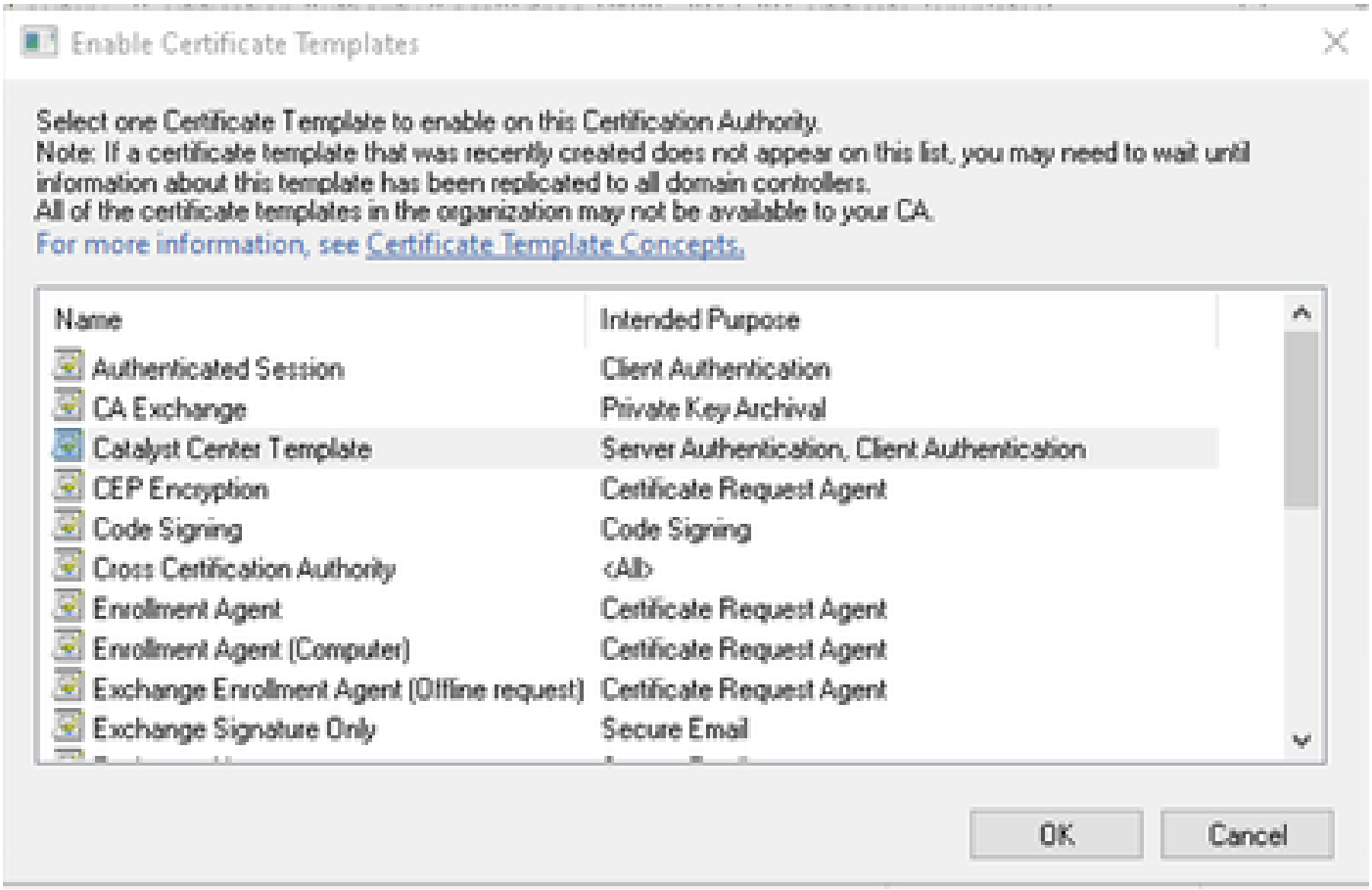
9. Fare clic con il pulsante destro del mouse sulla cartella dei modelli di certificato e selezionare:

Nuovo > Modello di certificato da rilasciare.



Nuovo modello di certificato da rilasciare

10. Nella nuova finestra, selezionare il nuovo modello creato (ad esempio, Catalyst Center Template) e fare clic su ok.

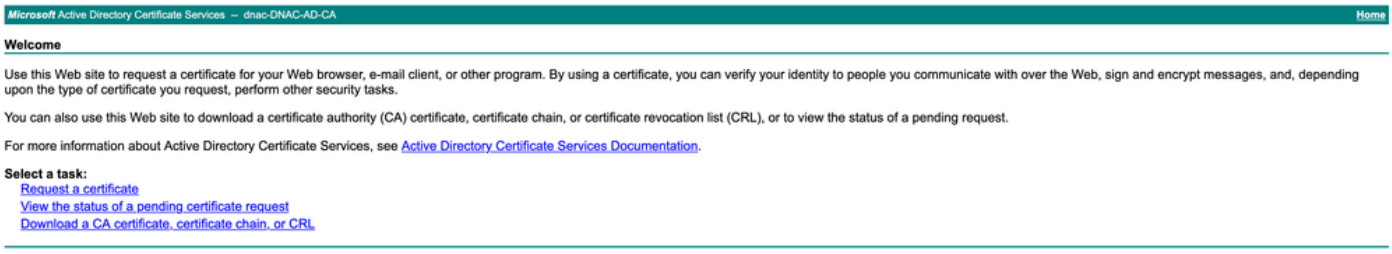


Modello Catalyst Center

11. Il modello verrà visualizzato nell'elenco Modelli di certificato della CA.

12. Aprire un browser e passare a:

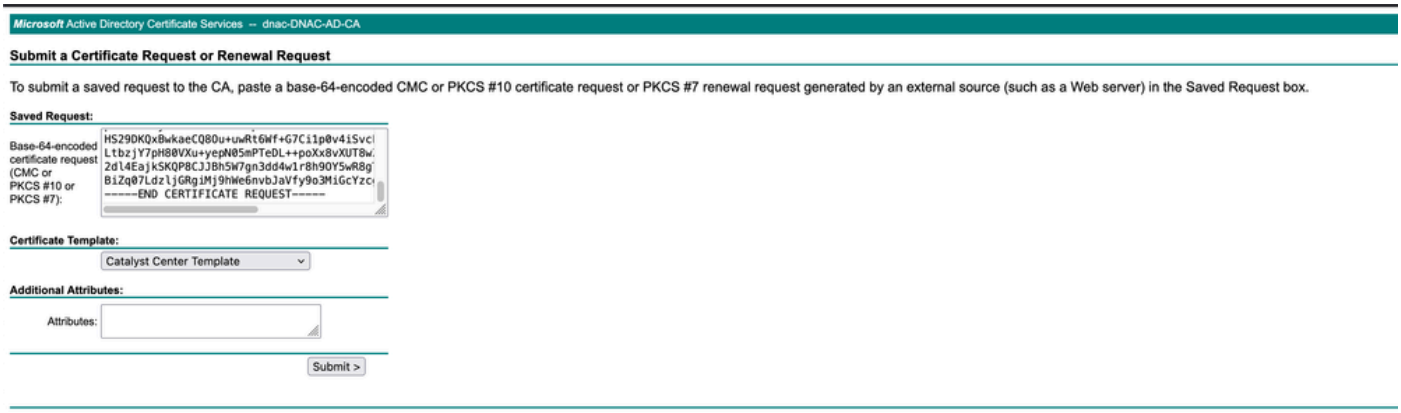
```
http://localhost/certsrv/
```



Pagina di accesso http://localhost/certsrv/

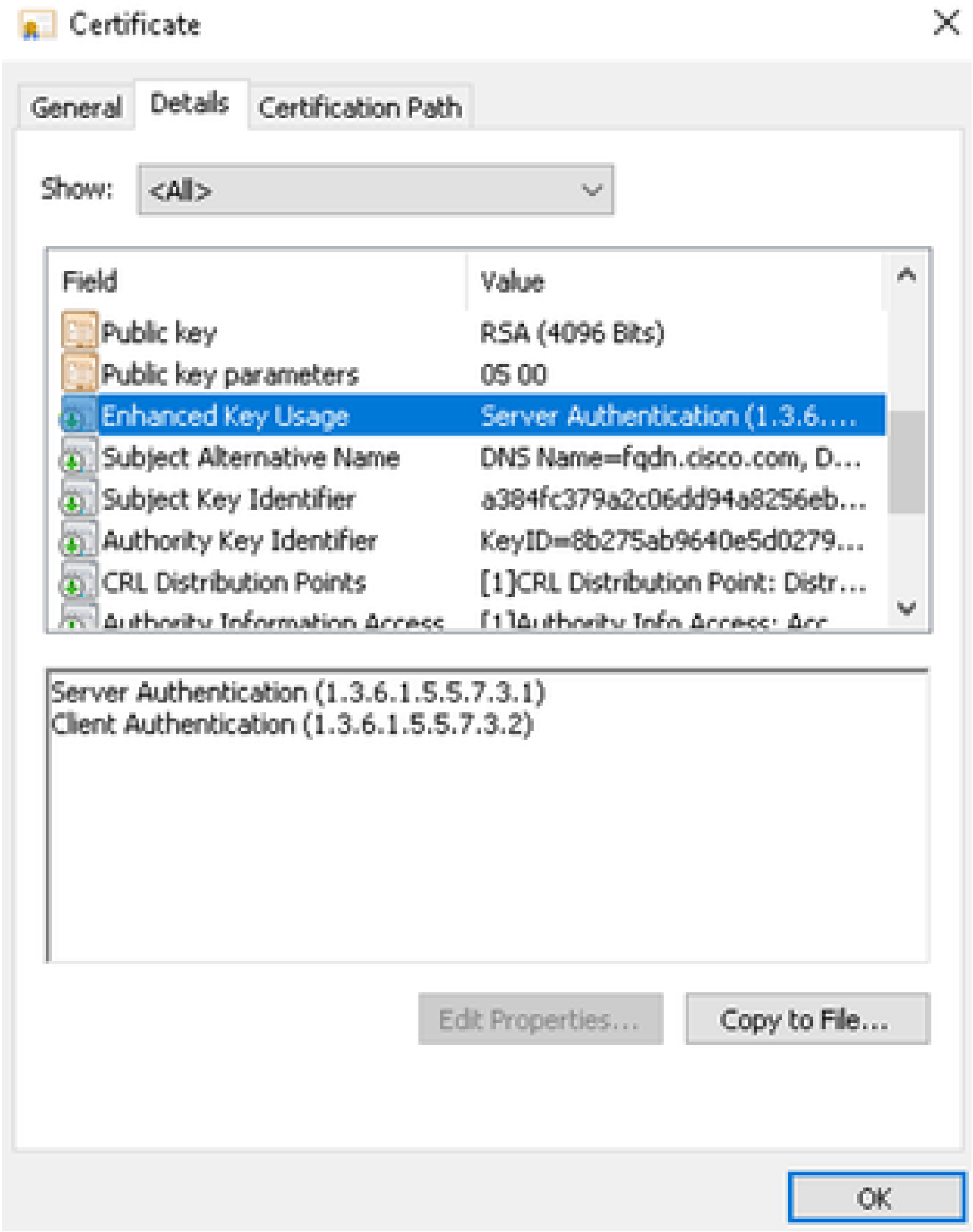
13. Selezionare Richiedi certificato, quindi Richiesta avanzata certificato, per verificare che il nuovo modello sia disponibile.

14. In questa pagina, sottomettere il CSR e selezionare il nuovo modello creato per generare il certificato firmato.



Richiedi certificato

13. Il certificato viene generato con le estensioni corrette, come mostrato nell'esempio.



Esempio di certificato

Risoluzione dei problemi

Se si verificano errori durante la firma del CSR, esaminare i registri di Windows Server per ulteriori informazioni:

Errore:

Risoluzione dei problemi

1. Aprire il Visualizzatore eventi eseguendo:

```
eventvwr.msc
```

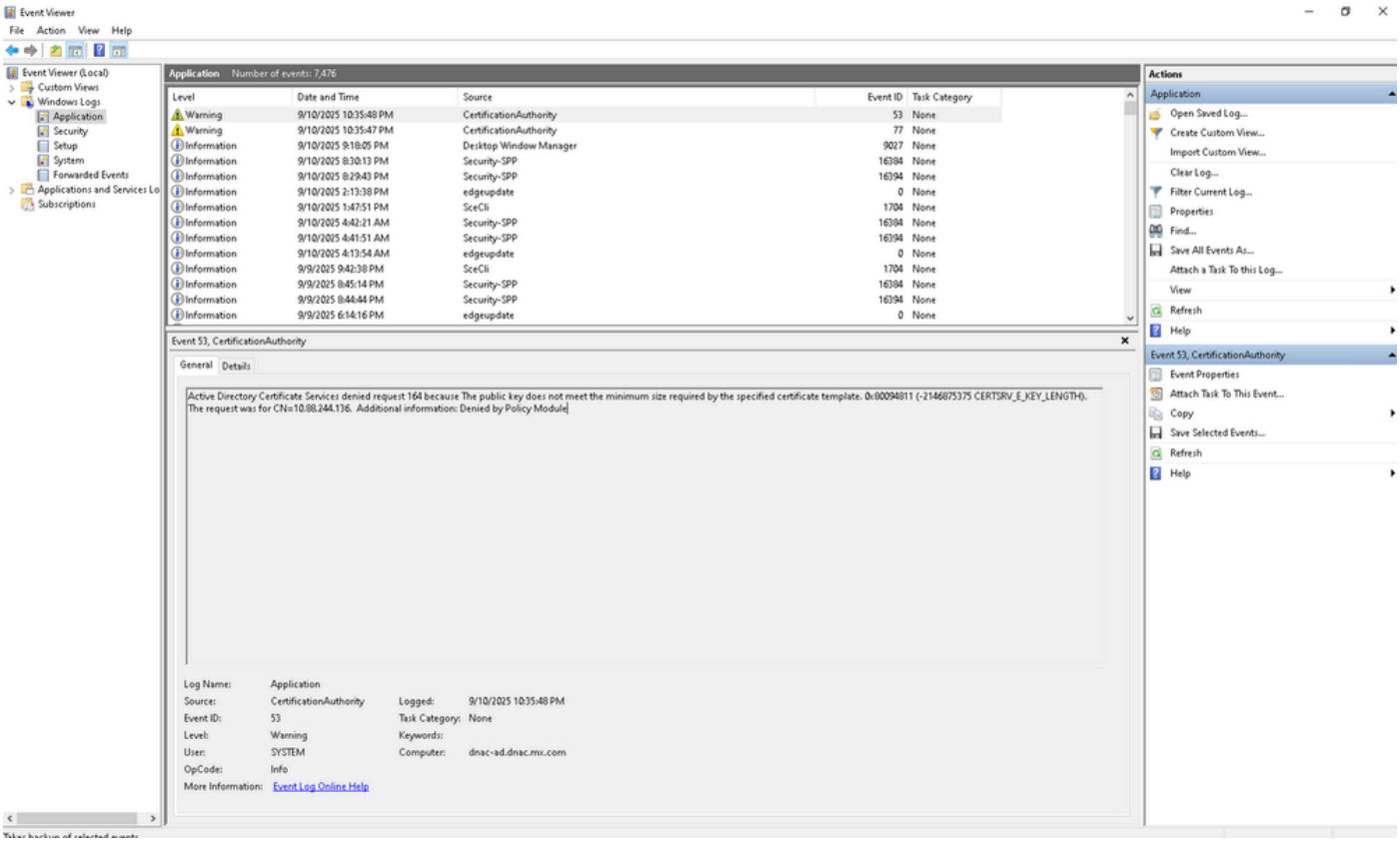
2. Passare a Visualizzatore eventi > Registri di Windows > Applicazione.

3. Filtrare o cercare eventi in cui:

    1. Origine = CertificationAuthority
    2. ID evento = 53, 54, 55 o simile (indica che una richiesta è stata emessa, negata o è in sospeso).
    3. Il messaggio dell'evento contiene informazioni dettagliate sul motivo del rifiuto (se applicabile).

4. Utilizzare l'opzione Trova (fare clic con il pulsante destro del mouse su Applicazione > Trova...) ed effettuare la ricerca in base a:

- certsrv
- ID richiesta (se noto, ad esempio, 164)



Risoluzione dei problemi relativi ai registri di Windows Server

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).