Windows Server-Zertifikatvorlage für Catalyst Center erstellen

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Konfigurieren

Fehlerbehebung

Einleitung

In diesem Dokument werden die Schritte zum Erstellen einer Zertifikatvorlage auf einem Windows-Server mit dem CA-Tool (Certificate Authority) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Center
- Ein Windows-Server mit installierter und konfigurierter Zertifizierungsstellenrolle (Certification Authority, CA)
- Administratorrechte auf dem Windows Server
- Zugriff auf die Verwaltungskonsole der Zertifizierungsstelle
- Grundkenntnisse von Zertifikatvorlagen und Zertifikatsanforderungen (Certificate Signing Requests, CSR)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Microsoft Windows Server 2022 Standard.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

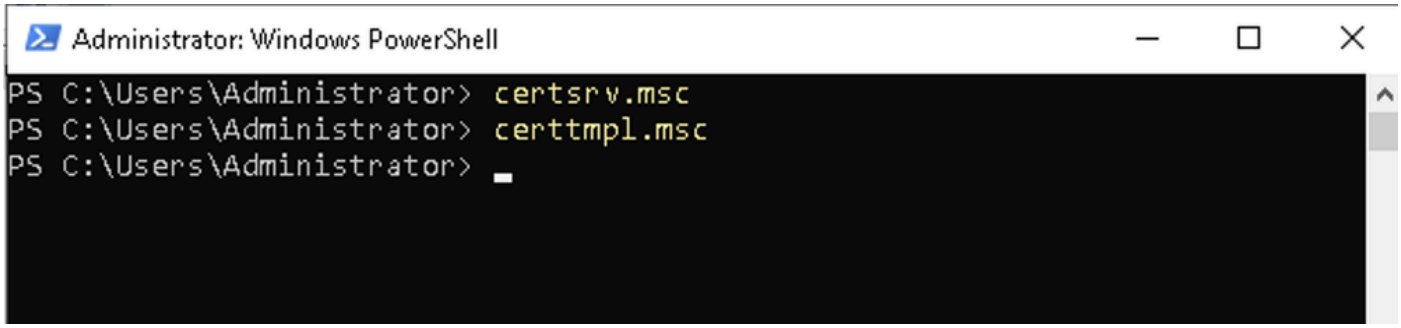
Diese benutzerdefinierte Vorlage löst das Problem, dass die Standard-CA-Vorlagen die Client-Authentifizierung von den erweiterten Schlüsselverwendungen entfernen. Die benutzerdefinierte Vorlage kann die von Catalyst Center generierte CSR-Anforderung (Certificate Signing Request) signieren.

Konfigurieren

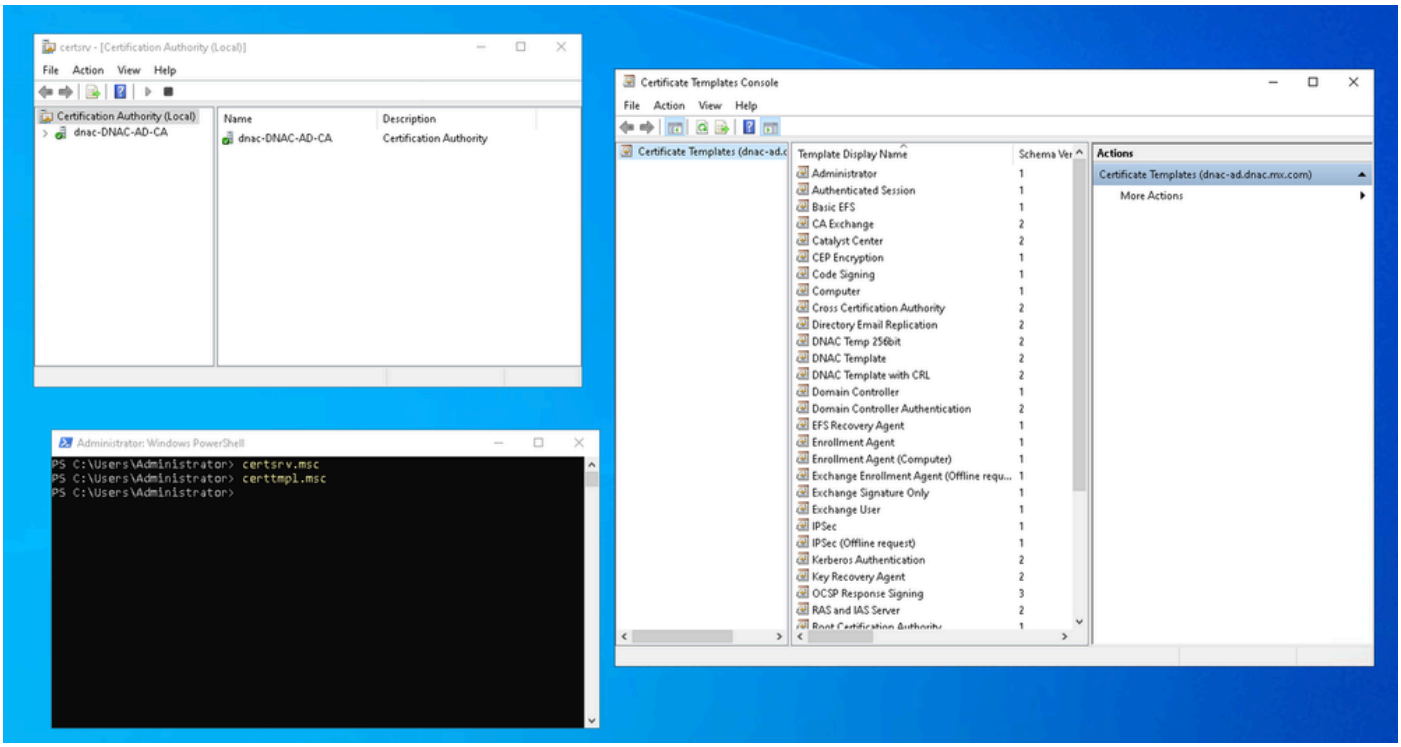
Schritte zum Überprüfen und Konfigurieren von Zertifikatvorlagen auf Windows Server mit der Zertifizierungsstelle (Certification Authority, CA)

1. Melden Sie sich bei dem Windows-Server an, der die Zertifizierungsstelle hostet, und verwenden Sie Remotedesktop.
2. Öffnen Sie eine Eingabeaufforderung (CMD) oder eine PowerShell-Sitzung.
3. Starten Sie die Konsolen der Zertifizierungsstelle und Zertifikatvorlage, indem Sie Folgendes ausführen:

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

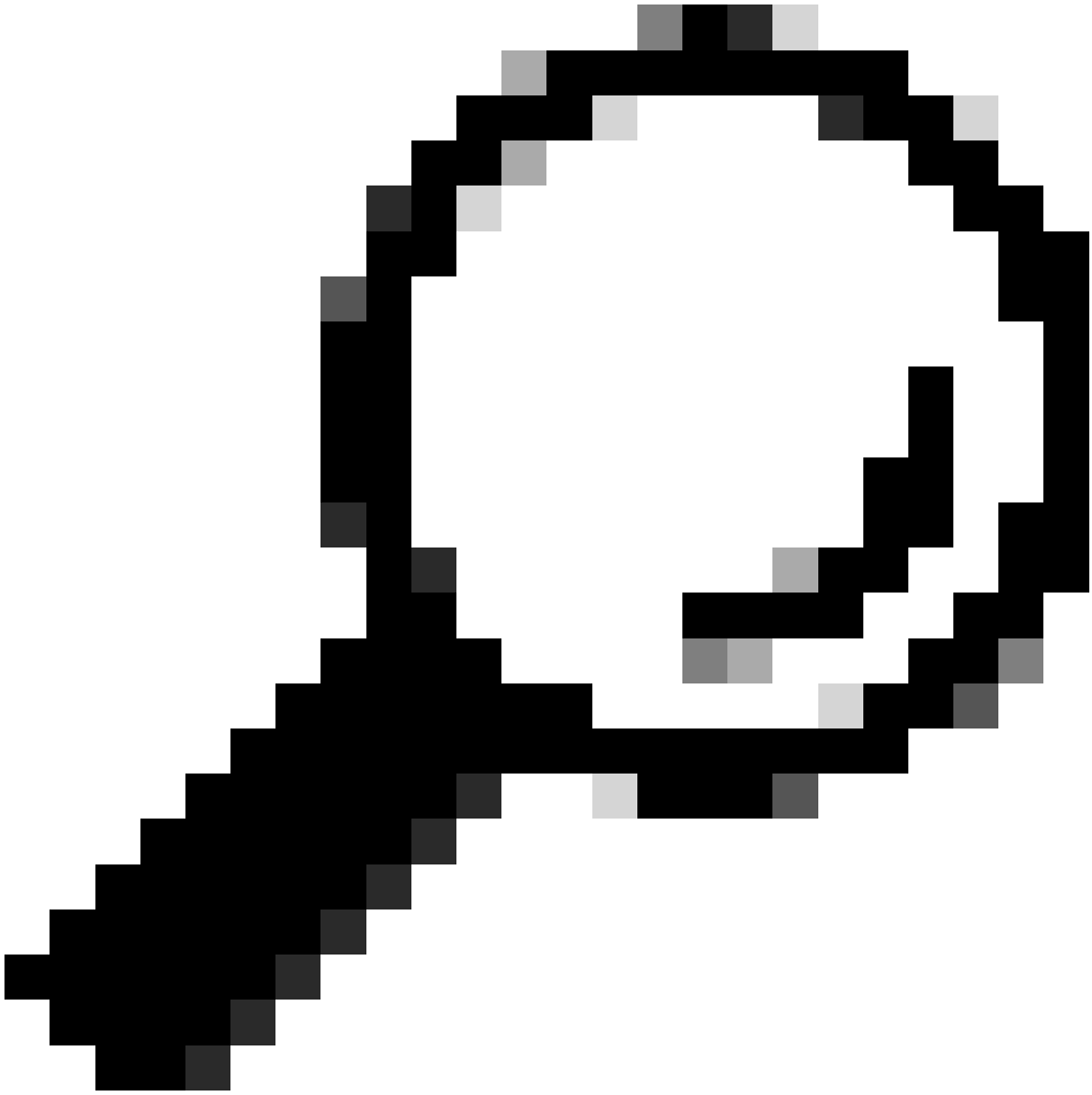


PowerShell-Administrationsbefehle



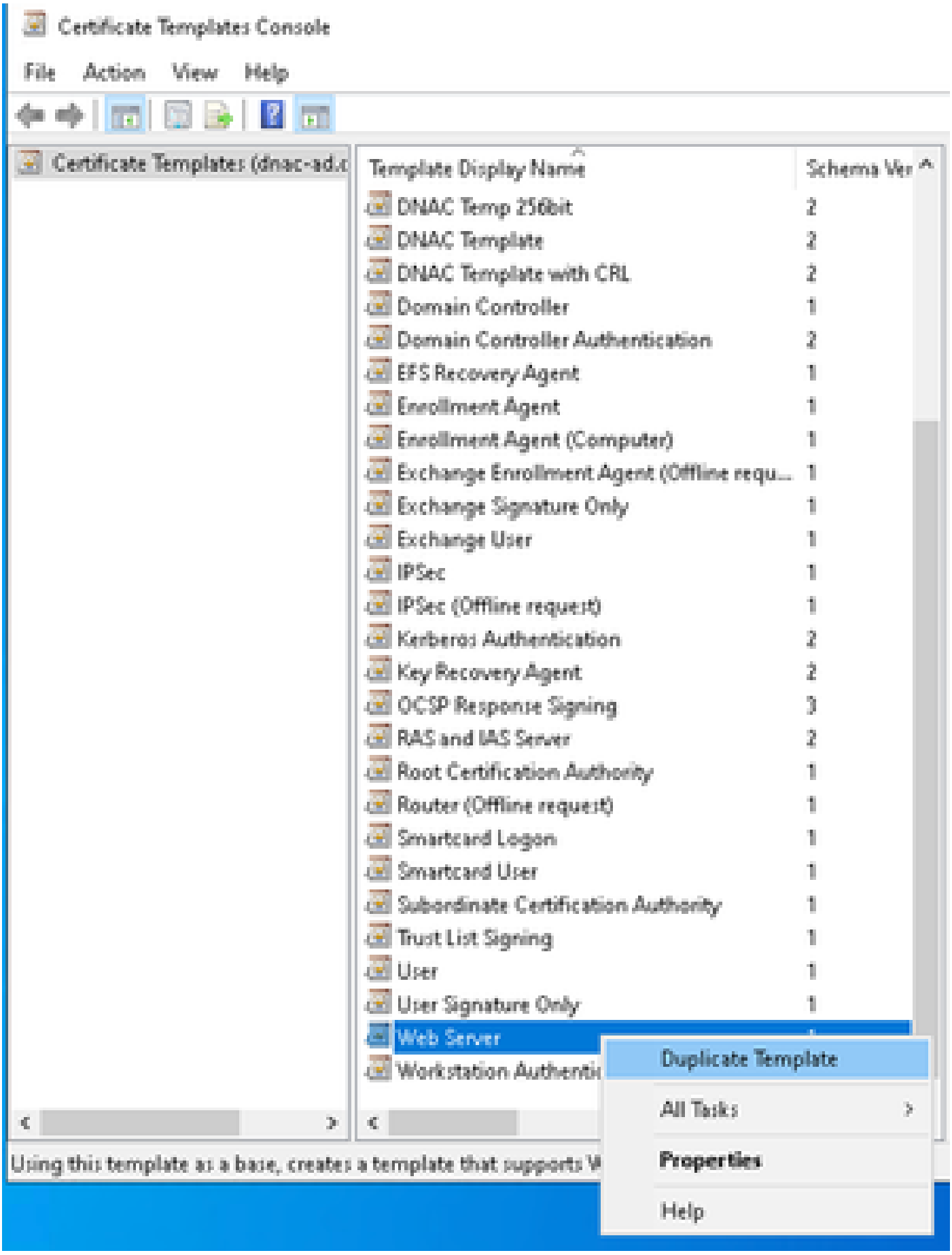
Beispiel für Windows Server

4. Suchen Sie in der Zertifikatvorlagenkonsole die Vorlage, die geklont werden soll, um eine neue anpassbare Vorlage zu erstellen.



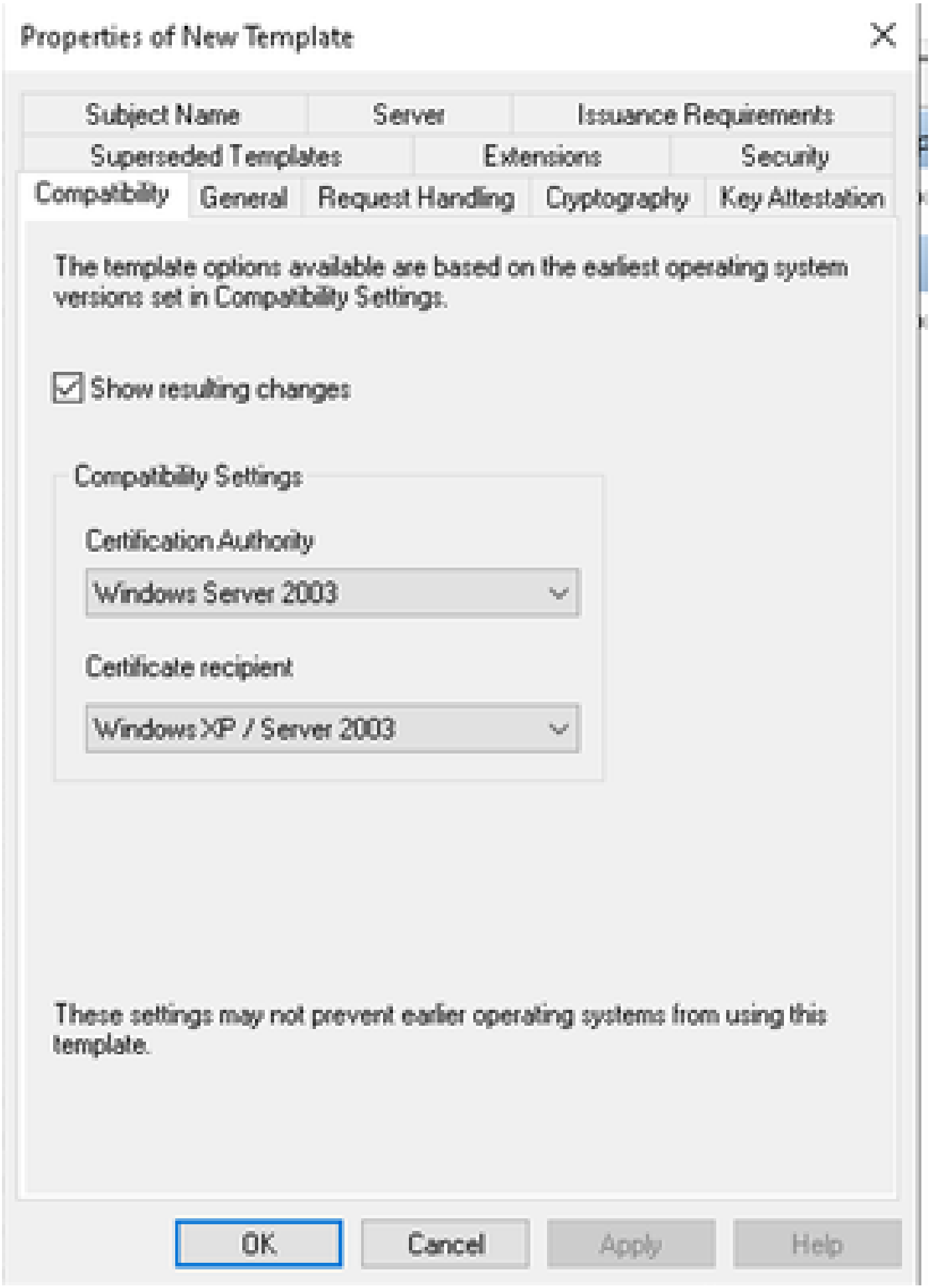
Tipp: Verwenden Sie die Webserver-Vorlage, da sie bereits alle erforderlichen Parameter für das Catalyst Center-Zertifikat enthält.

- Beispiel: Klicken Sie mit der rechten Maustaste auf den Webserver, und wählen Sie Vorlage duplizieren aus.



Vorlage kopieren

5. Eine neue Vorlage ist geöffnet, ändern Sie sie mit den erforderlichen Eigenschaften.


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. Ändern Sie die neue Vorlage wie folgt:

6.1 Registerkarte Allgemein

- Geben Sie einen Vorlagennamen ein (z. B. Catalyst Center-Vorlage).
- Definieren Sie die Gültigkeitsdauer (Standard: 2 Jahre).

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

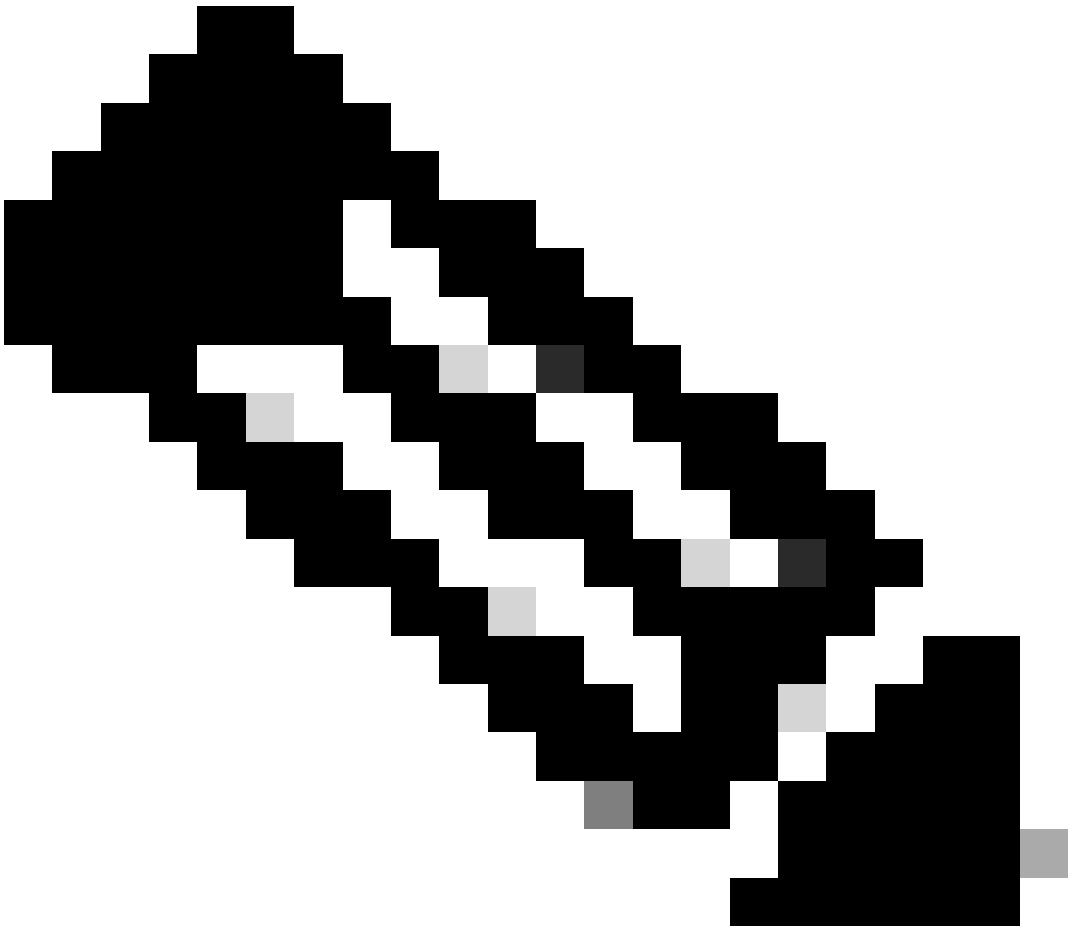
Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

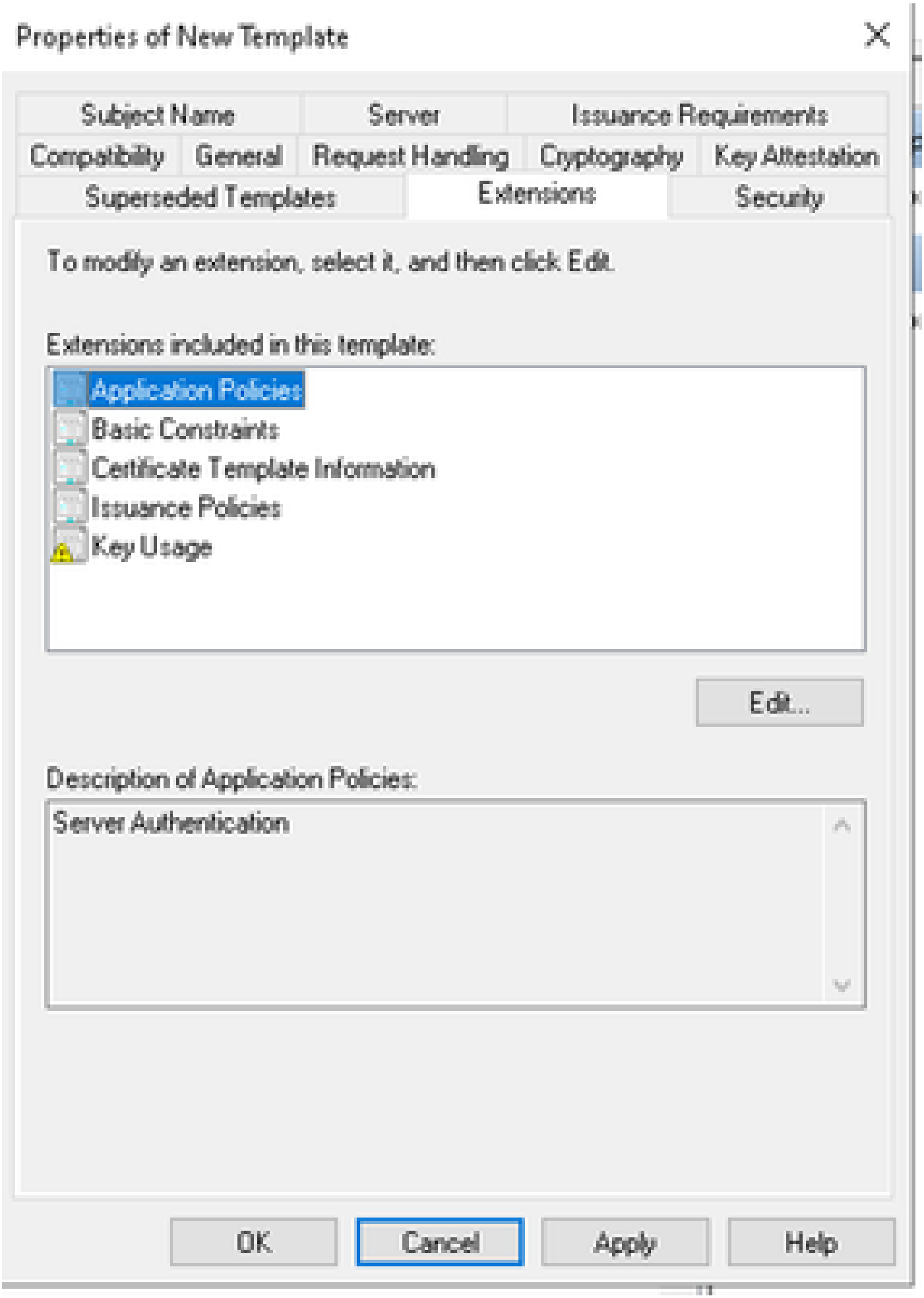
Vorlagenname

6.2 Registerkarte Erweiterungen.

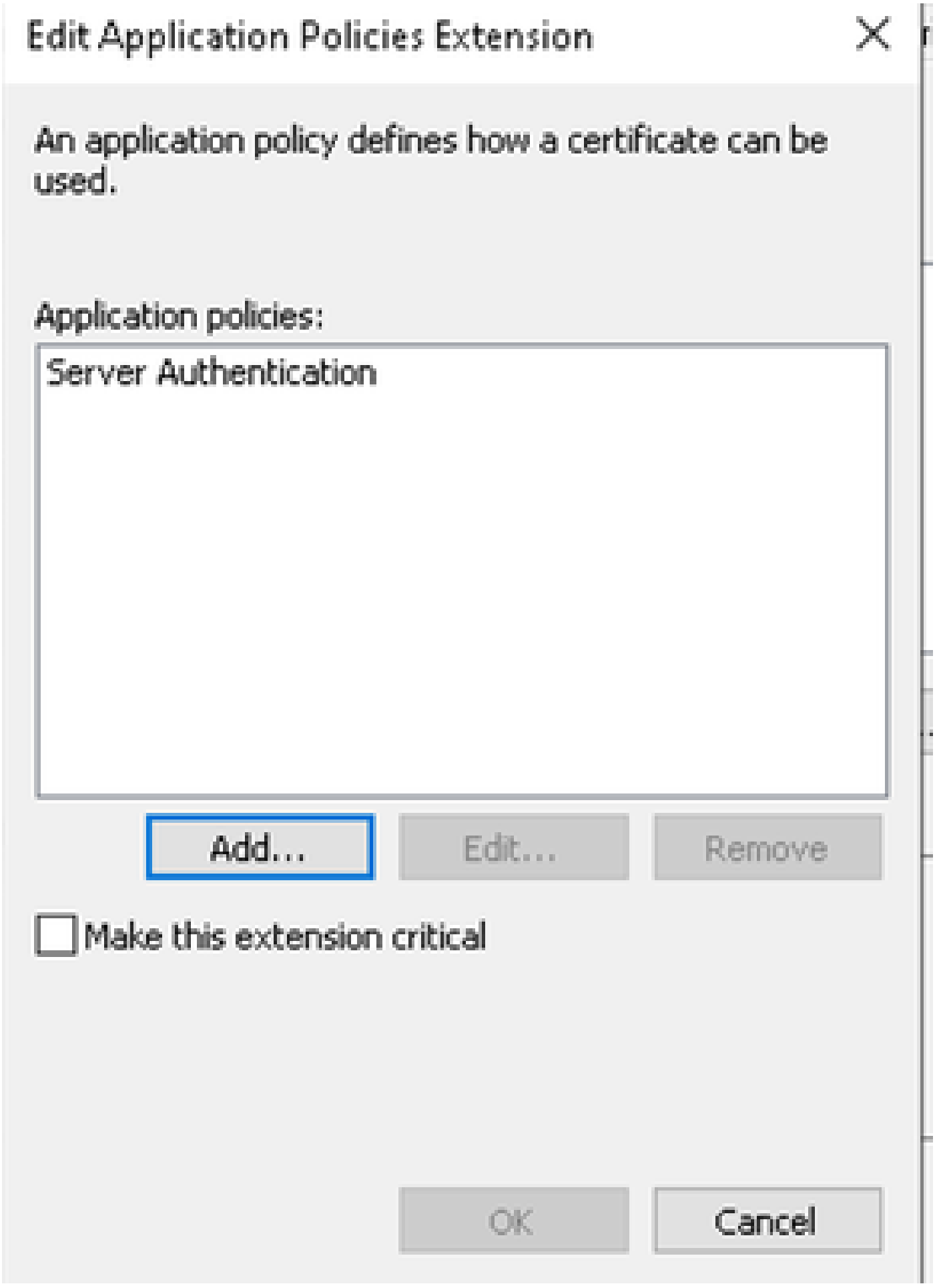
- Navigieren Sie zu Anwendungsrichtlinien, und klicken Sie auf Bearbeiten.



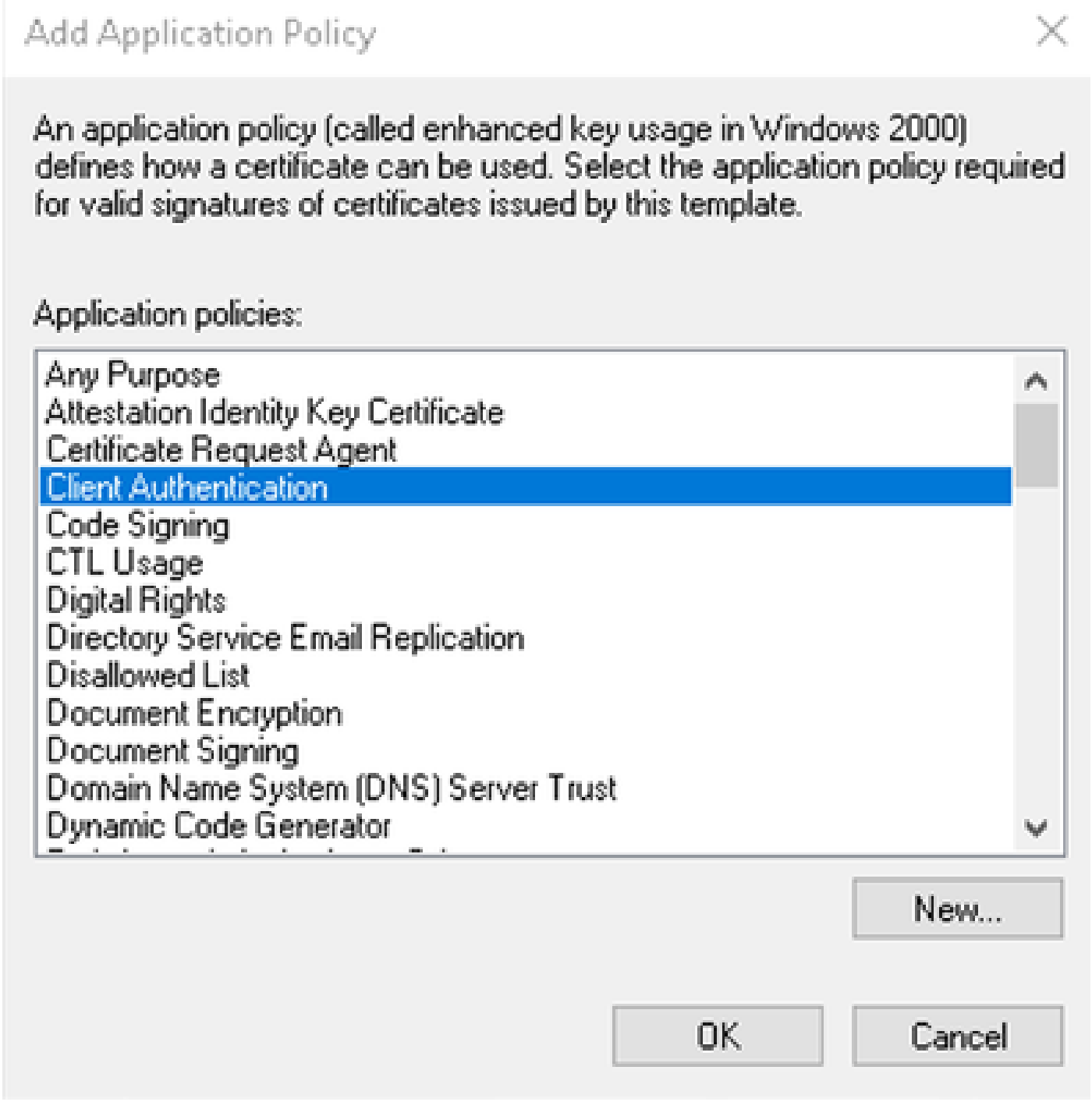
Anmerkung: Vergewissern Sie sich auf dieser Registerkarte, dass die Vorlage die obligatorischen Erweiterungen für die Schlüsselverwendung enthält, die für das Catalyst Center-Zertifikat erforderlich sind, z. B. keyEncipherment und digitalSignature. Diese sind bereits in der als Basis verwendeten Webserver-Standardvorlage vorhanden.


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

- Klicken Sie auf Hinzufügen, suchen Sie nach Client-Authentifizierung, und klicken Sie auf OK, um sie einzuschließen.

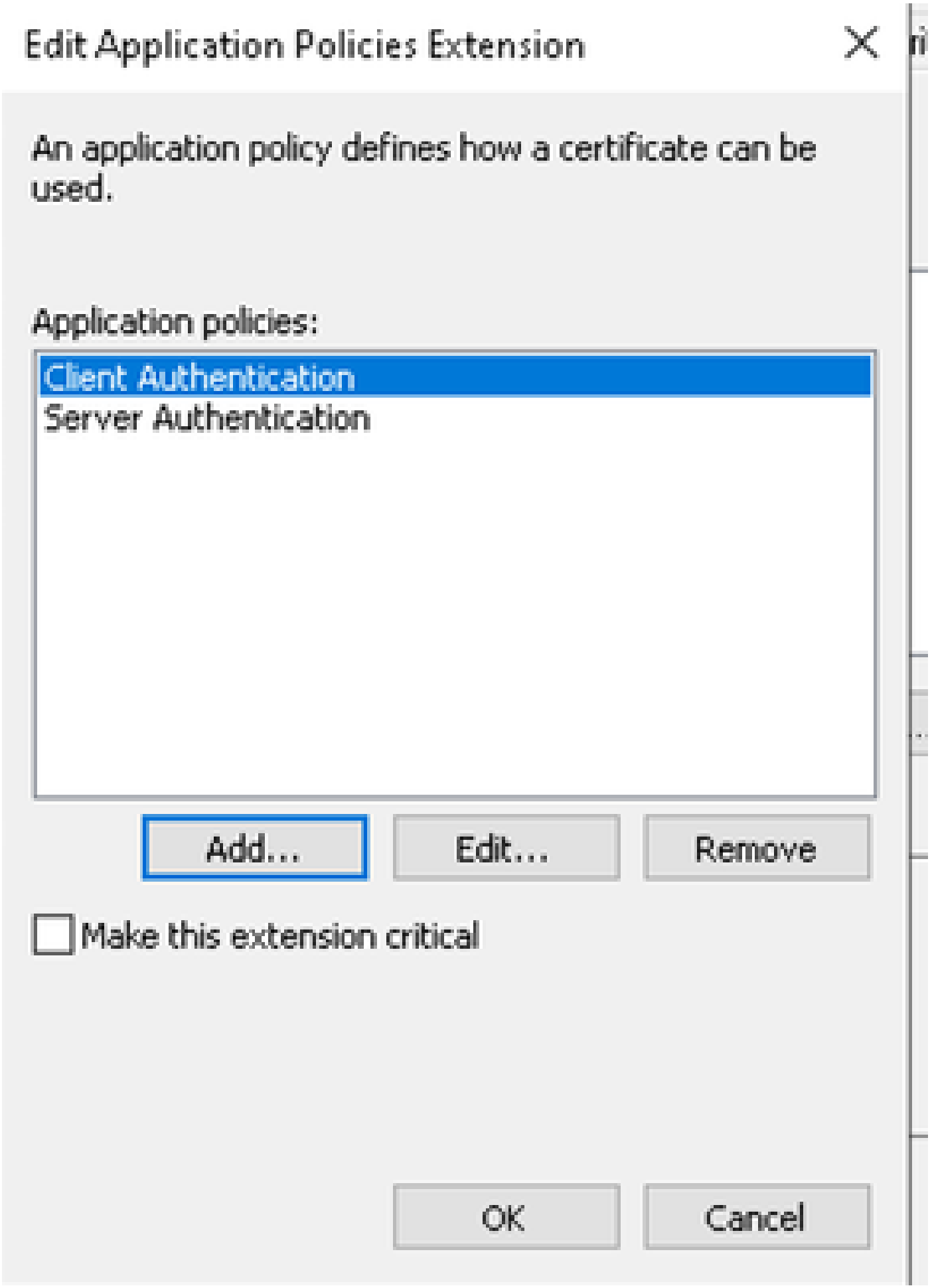


Client-Authentifizierung



Anwendungsrichtlinie hinzufügen

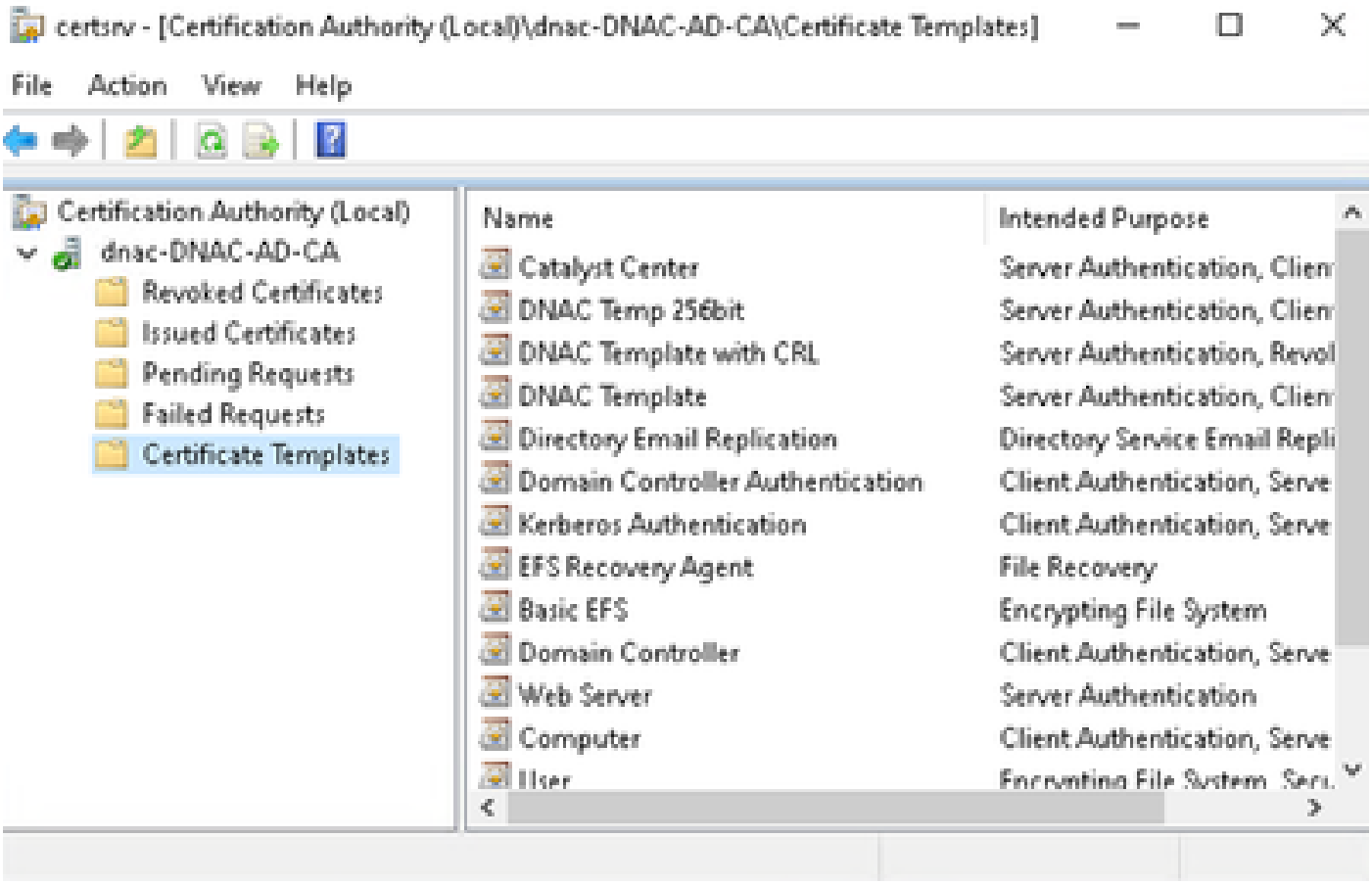
- Bestätigen Sie, dass die Vorlage Client Authentication zusammen mit den Standardverwendungen anzeigt.


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

Erweiterung für Anwendungsrichtlinien

7. Klicken Sie auf Apply und dann ok.

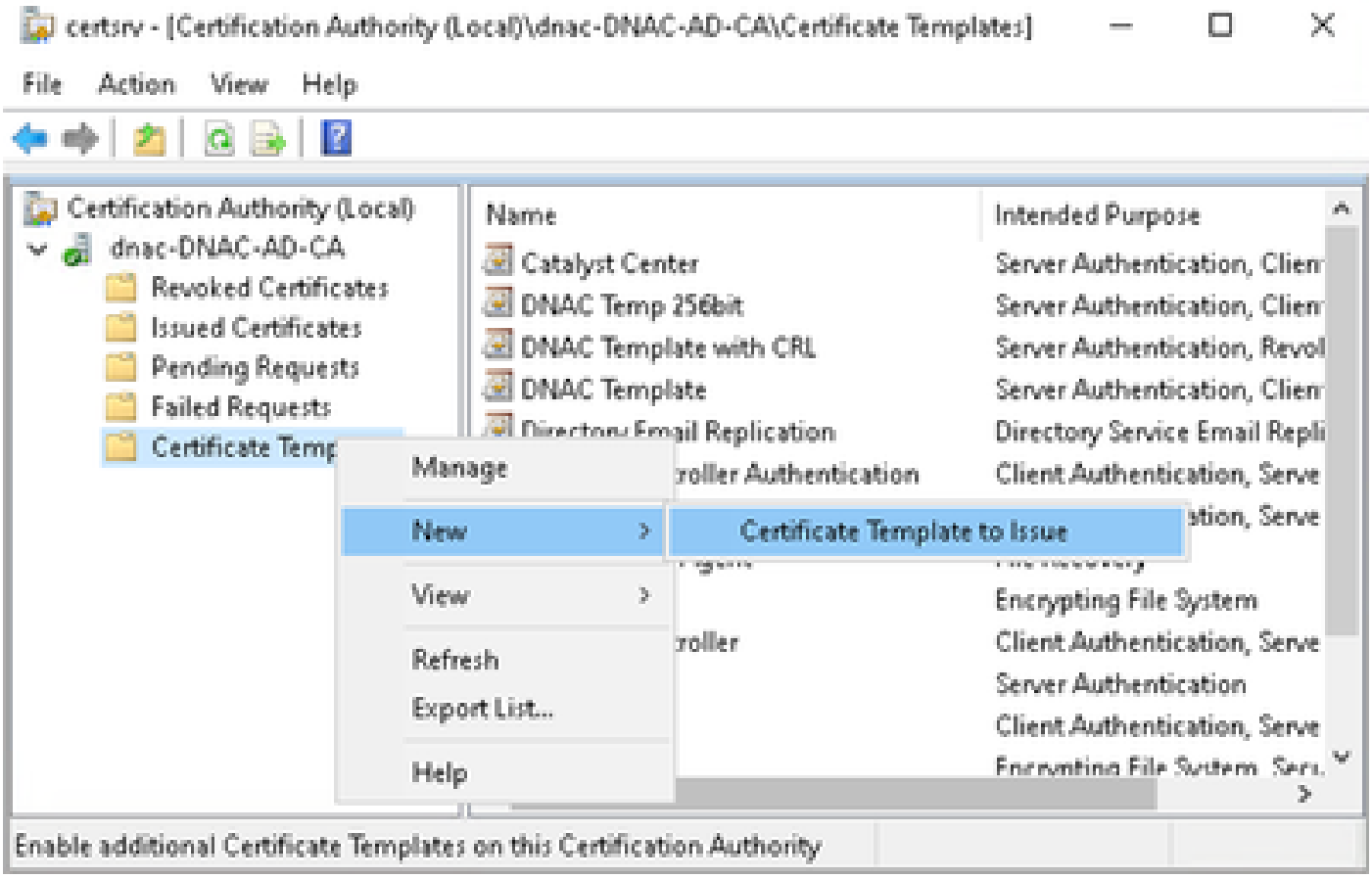
8. Erweitern Sie in der Konsole der Zertifizierungsstelle die Zertifizierungsstellenstruktur, und wählen Sie den Ordner Zertifikatvorlagen aus.



Zertifizierungsstellenbaum-Zertifikatvorlagen

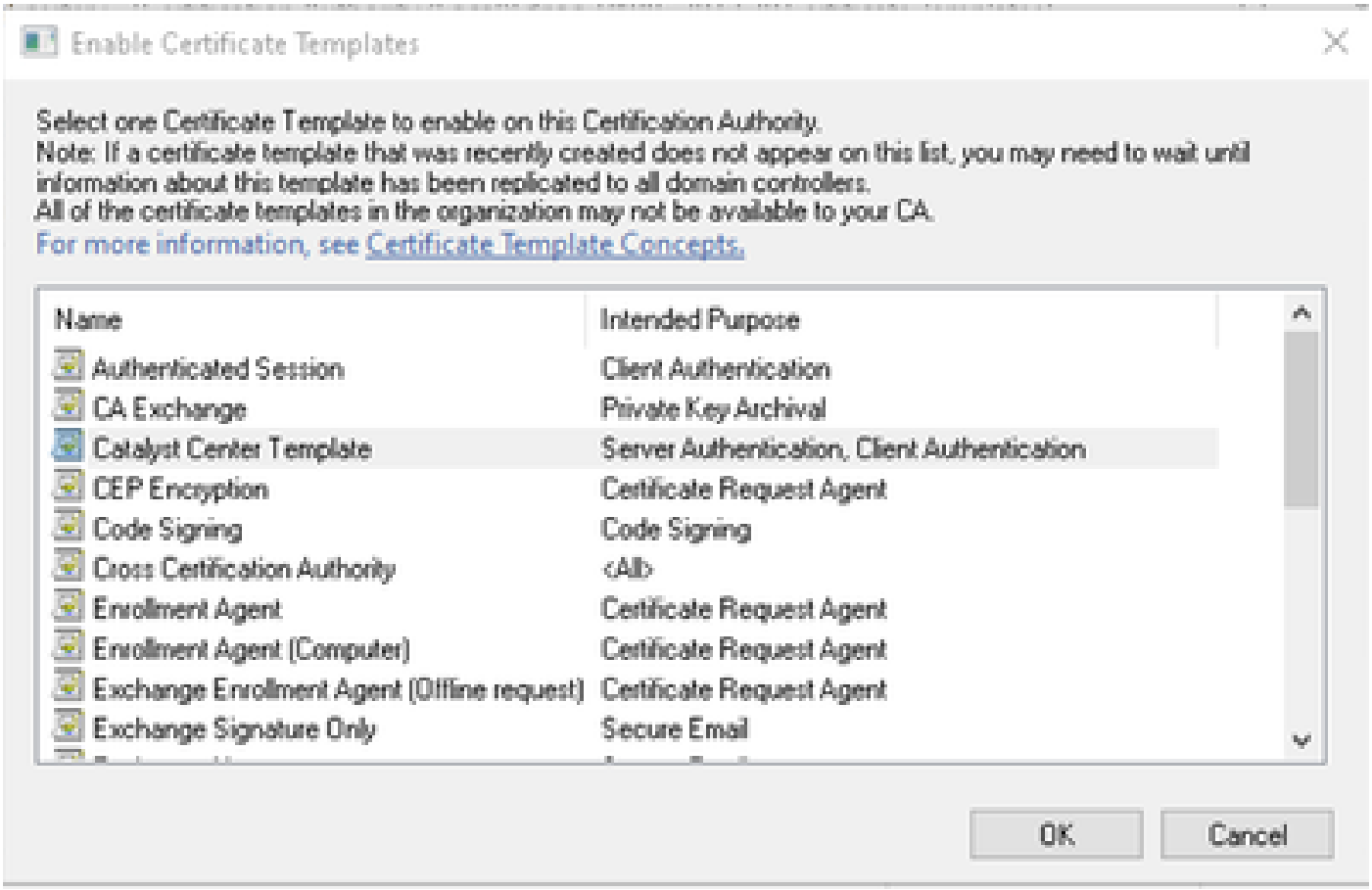
9. Klicken Sie mit der rechten Maustaste auf den Ordner Zertifikatvorlagen, und wählen Sie:

Neu > Zertifikatvorlage zur Ausgabe.



Neue auszustellende Zertifikatvorlage

10. Wählen Sie im neuen Fenster die neu erstellte Vorlage (z. B. Catalyst Center-Vorlage) aus, und klicken Sie auf OK.

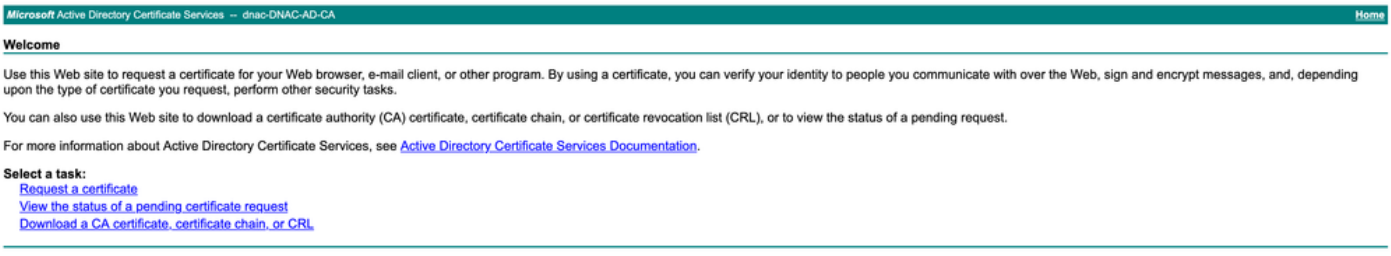


Catalyst Center-Vorlage

11. Die Vorlage wird nun in der Liste Zertifikatvorlagen der Zertifizierungsstelle angezeigt.

12. Öffnen Sie einen Browser und navigieren Sie zu:

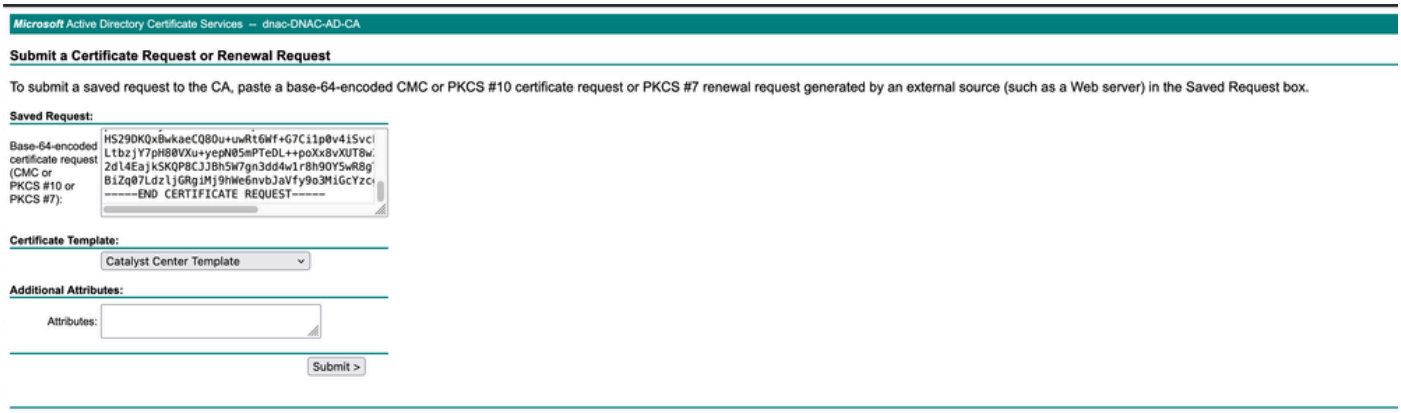
```
http://localhost/certsrv/
```



Anmeldeseite http://localhost/certsrv/

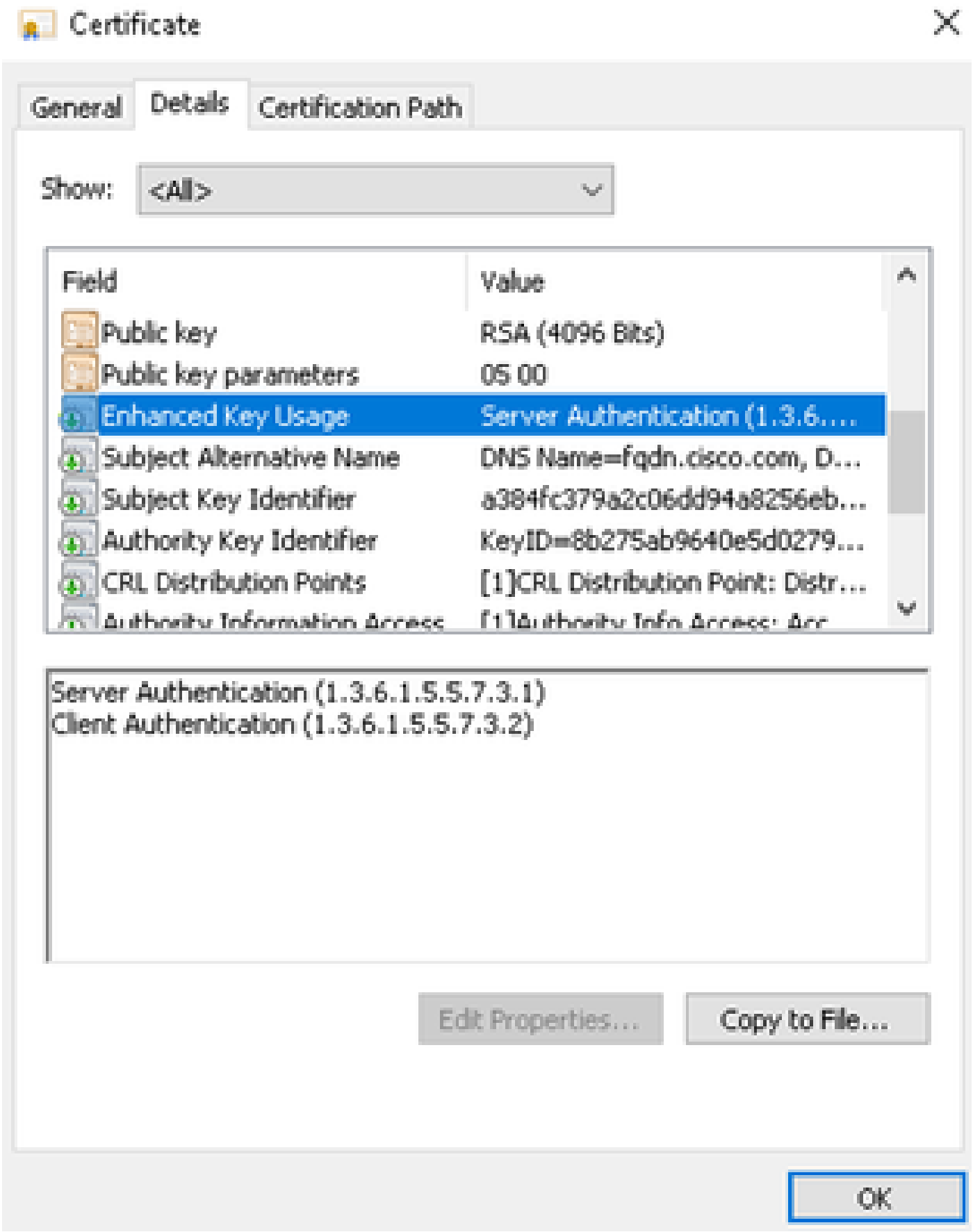
13. Wählen Sie Zertifikat anfordern und anschließend Erweiterte Zertifikatsanforderung, um zu überprüfen, ob die neue Vorlage verfügbar ist.

14. Senden Sie auf dieser Seite die CSR-Anfrage, und wählen Sie die neu erstellte Vorlage aus, um das signierte Zertifikat zu generieren.



Zertifikat anfordern

13. Das Zertifikat wird mit den richtigen Erweiterungen generiert, wie im Beispiel gezeigt.



Zertifikatbeispiel

Fehlerbehebung

Wenn beim Signieren des CSR Fehler auftreten, überprüfen Sie die Windows Server-Protokolle auf weitere Details:

Fehler:

Fehler bei Fehlerbehebung

1. Öffnen Sie die Ereignisanzeige, indem Sie Folgendes ausführen:

```
eventvwr.msc
```

2. Navigieren Sie zu Ereignisanzeige > Windows-Protokolle > Anwendung.

3. Ereignisse filtern oder suchen, bei denen:

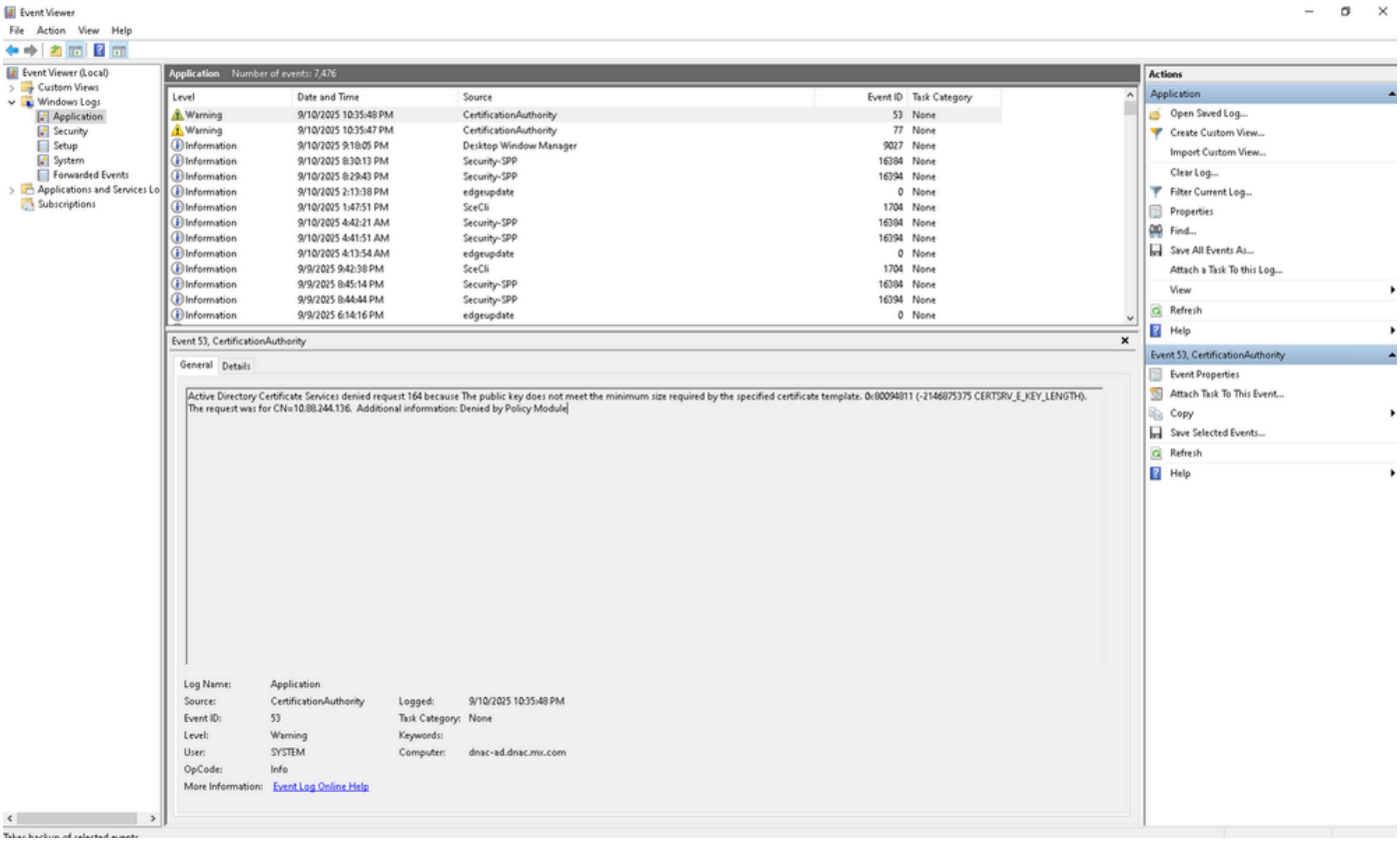
    1. Quelle = Zertifizierungsstelle

    2. Ereignis-ID = 53, 54, 55 oder Ähnliches (diese weisen darauf hin, dass eine Anforderung ausgestellt, abgelehnt oder ausstehend ist).

    3. Die Ereignismeldung enthält Details zum Grund der Ablehnung (falls zutreffend).

4. Verwenden Sie die Option Suchen (klicken Sie mit der rechten Maustaste auf Anwendung > Suchen...), und suchen Sie nach:

- certsrv
- Anforderungs-ID (falls bekannt, z. B. 164)



Fehlerbehebung bei Windows Server-Protokollen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.