Catalyst Center用のWindows Server証明書テンプレートの作成

内容

はじめに

このドキュメントでは、認証局(CA)ツールを実行するWindows Serverで証明書テンプレートを作成する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalystセンター
- 認証局(CA)の役割がインストールされ、設定されているWindows Server。
- Windows Serverでの管理者権限
- Certification Authority Management Consoleへのアクセス
- 証明書テンプレートおよび証明書署名要求(CSR)に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、Microsoft Windows Server 2022 Standardに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このカスタムテンプレートを使用すると、デフォルトのCAテンプレートによって拡張キーの使用

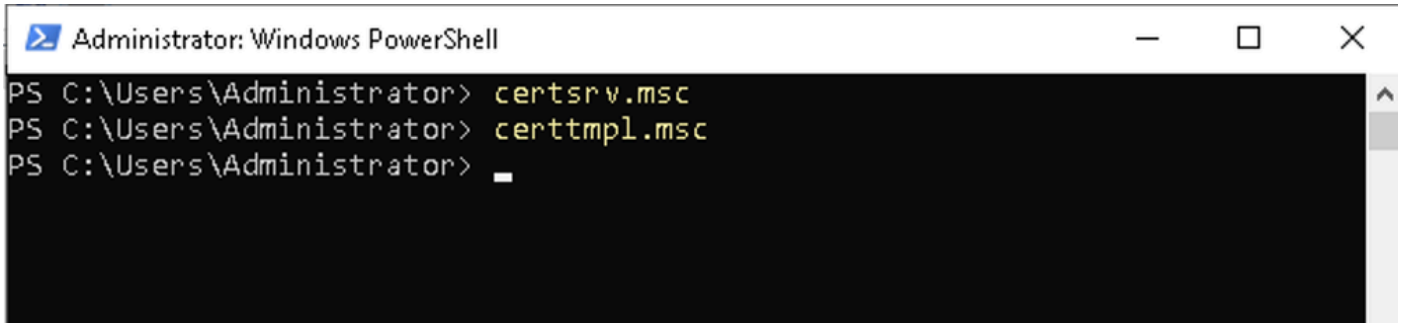
からクライアント認証が削除される問題が解決します。カスタムテンプレートは、Catalyst Centerによって生成された証明書署名要求(CSR)に署名できます。

設定

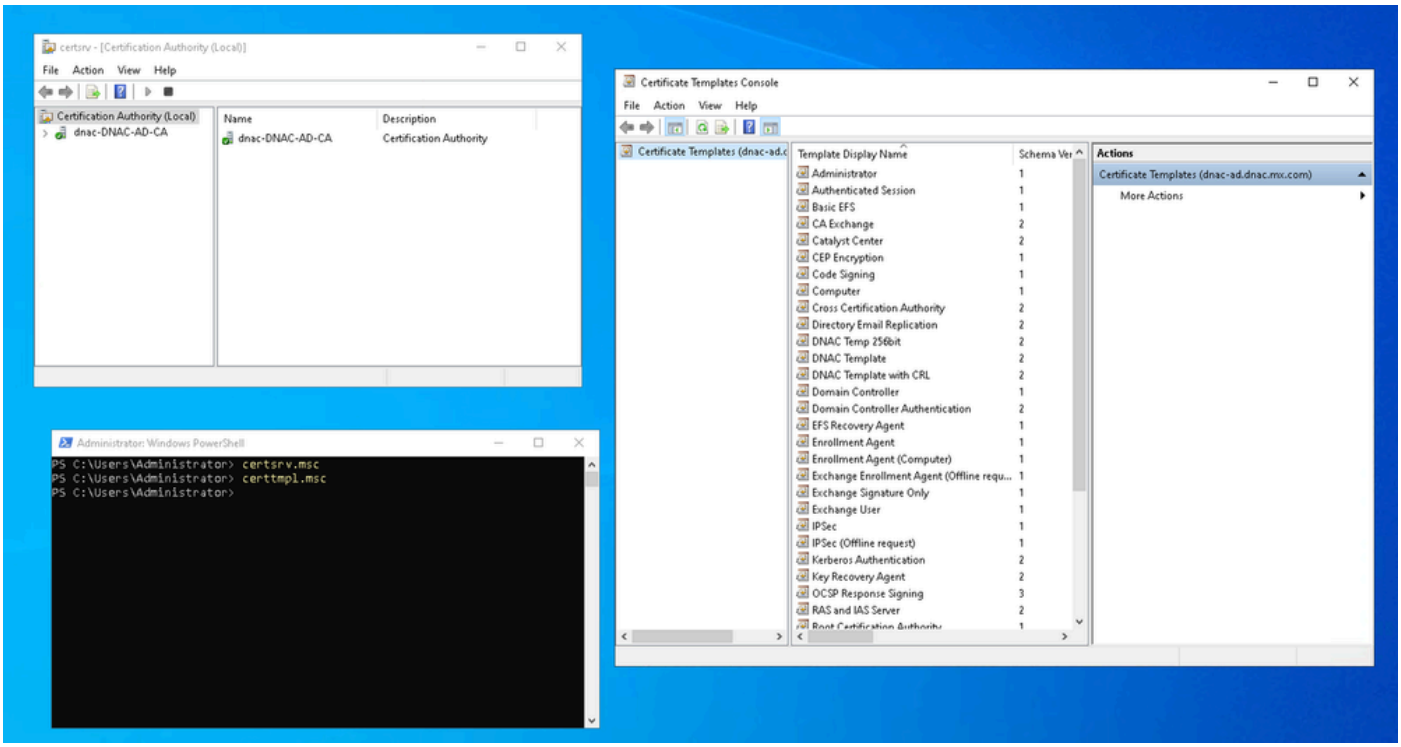
Certification Authority（CA；認証局）を使用して、Windows Serverで証明書テンプレートを確認および設定する手順。

1. リモートデスクトップを使用して、CAをホストしているWindows Serverにログインします。
2. コマンドプロンプト(CMD)またはpowerShellセッションを開きます。
3. 次のコマンドを実行して、認証局と証明書テンプレートのコンソールを起動します。

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

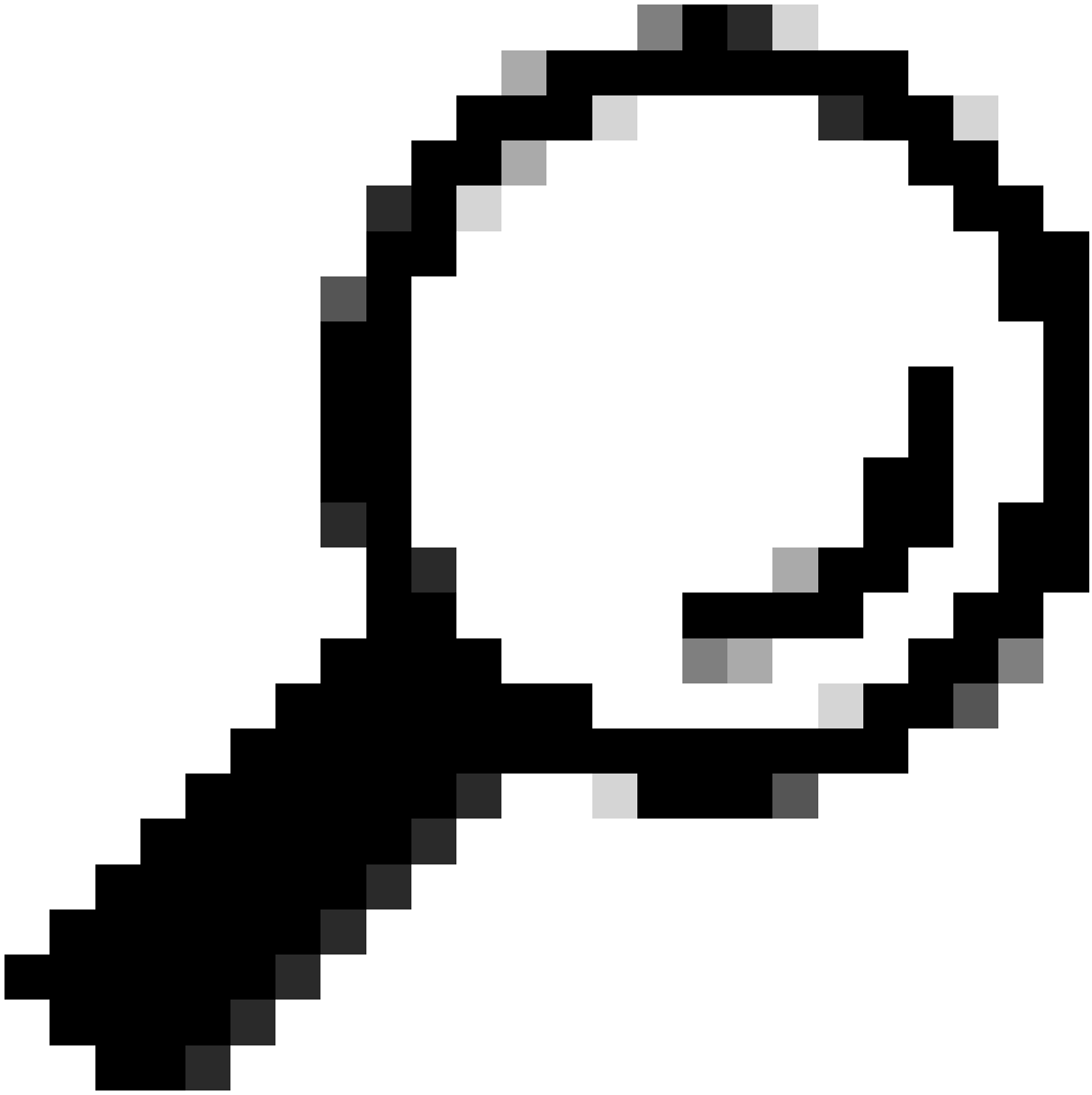


管理Powershellコマンド



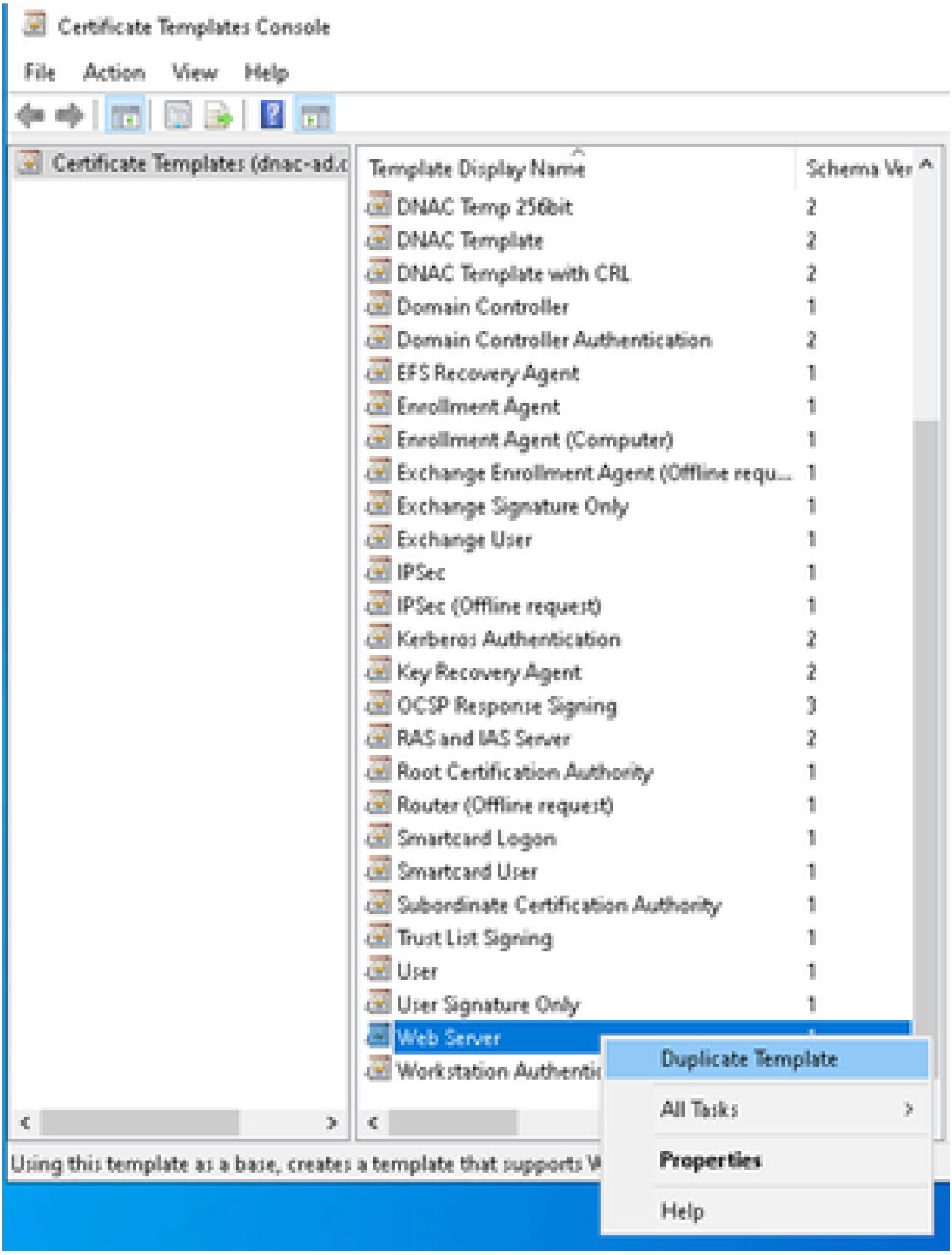
Windows Serverの例

4. Certificate Template Consoleで、クローニングしてカスタマイズ可能な新しいテンプレートを作成するテンプレートを見つけます。



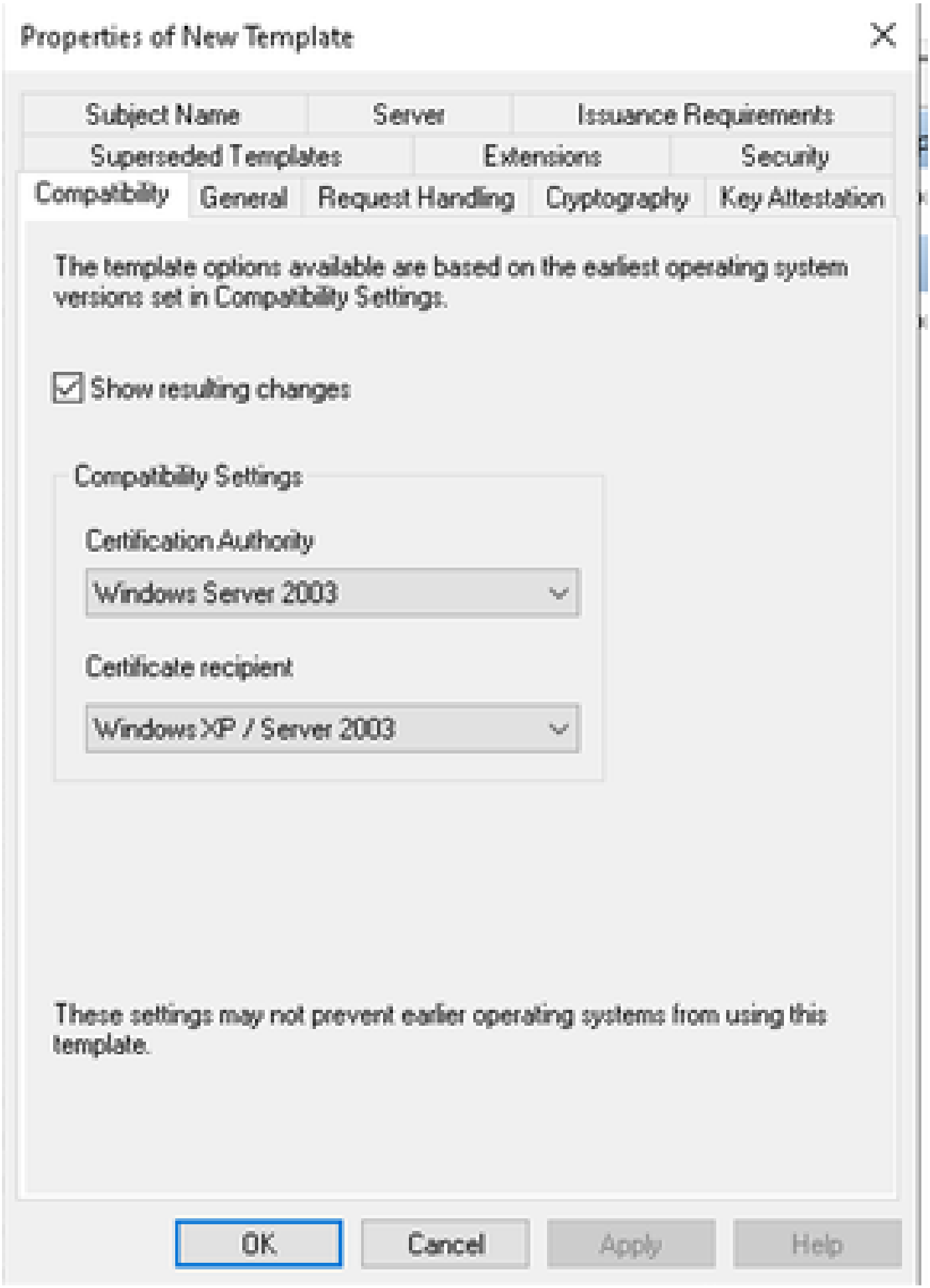
ヒント:WebサーバテンプレートにはCatalyst Center証明書に必要なパラメータがすべて含まれているため、このテンプレートを使用してください。

- 例：webサーバを右クリックし、duplicate templateを選択します。



テンプレートの複製

5. 新しいテンプレートが開いている場合は、必要な特性で変更します。


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. 新しいテンプレートを次のように変更します。

6.1 [全般]タブ

- テンプレート名（Catalyst Center Templateなど）を入力します。
- 有効期間を定義します（デフォルト：2年）。

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

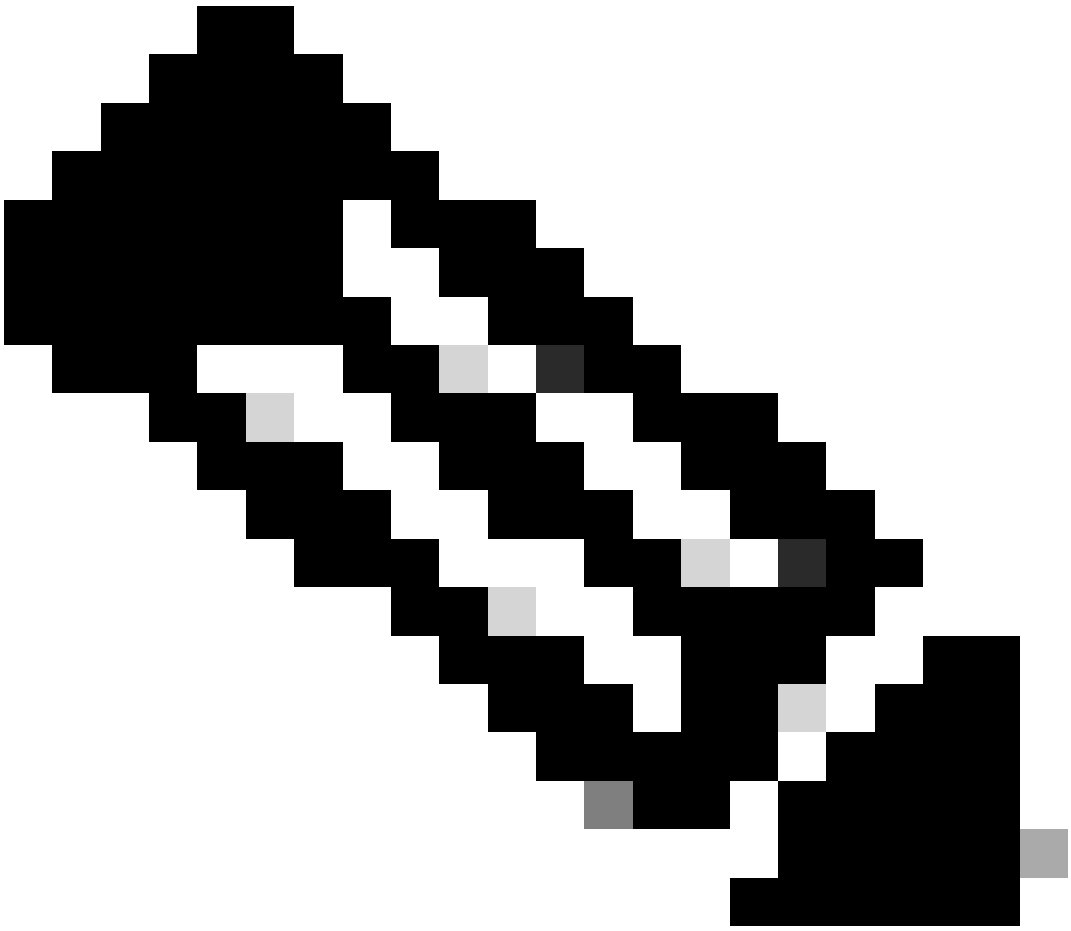
Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

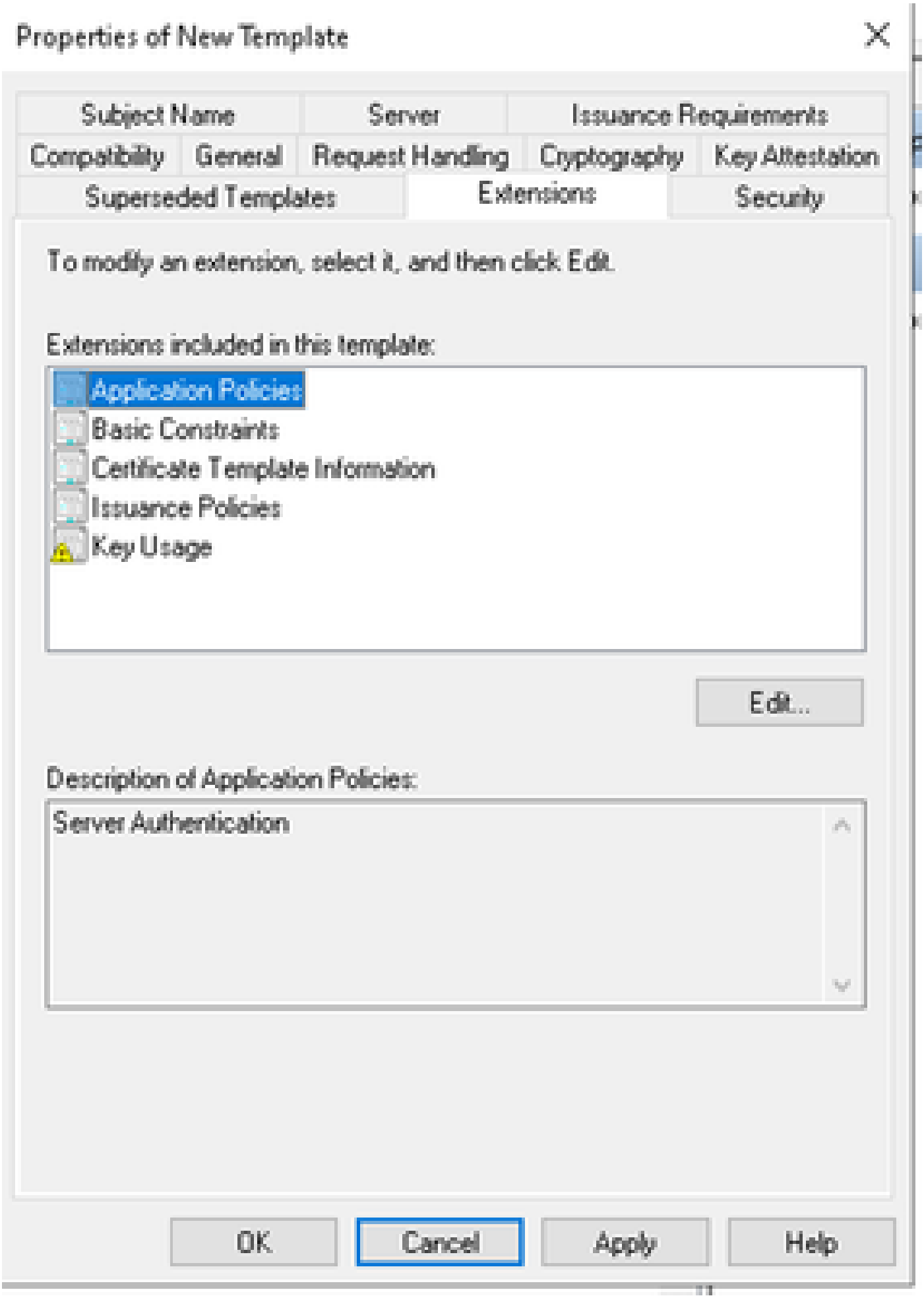
テンプレート名

6.2 Extensionsタブ

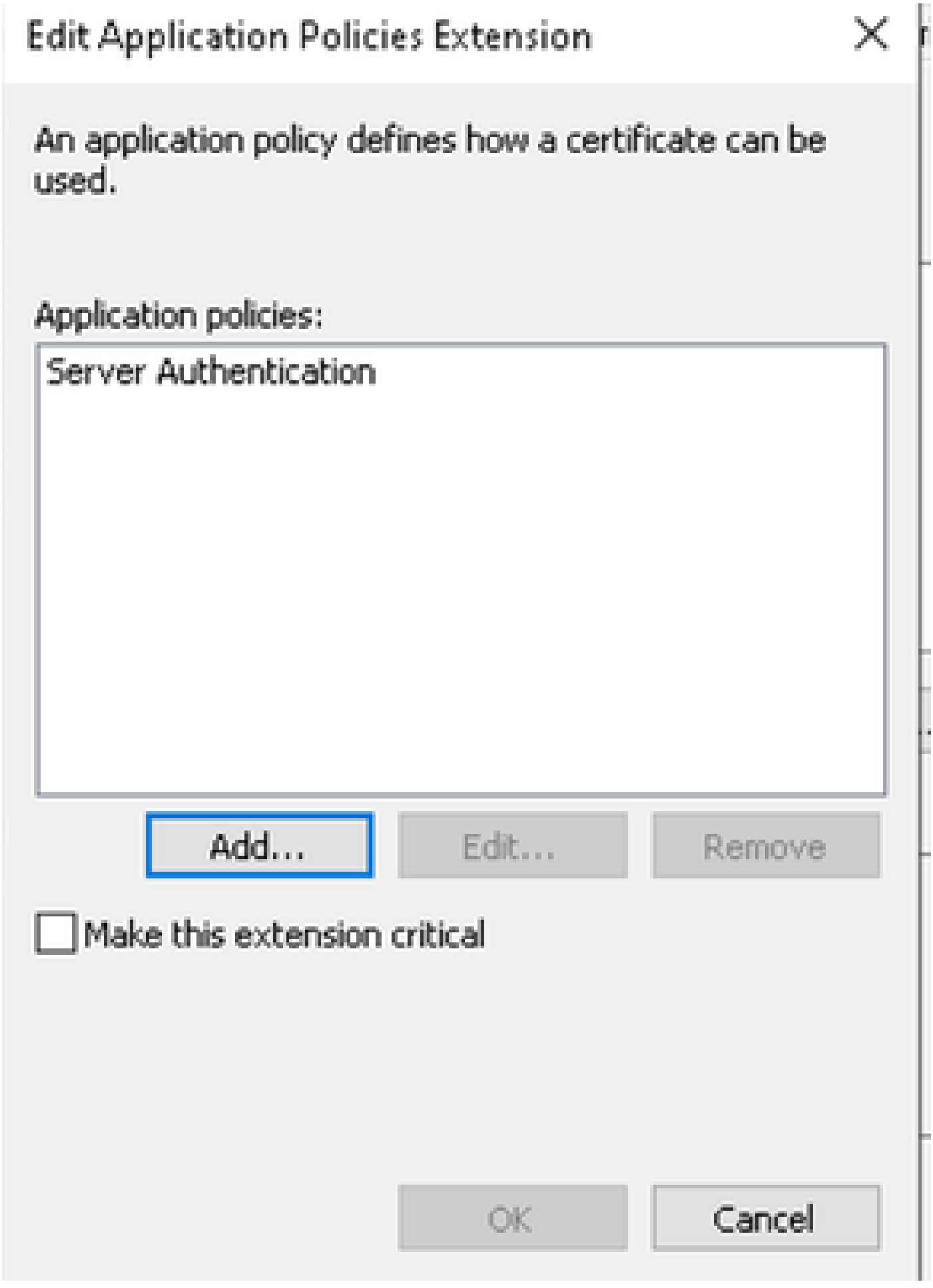
- application policiesに移動し、editをクリックします。



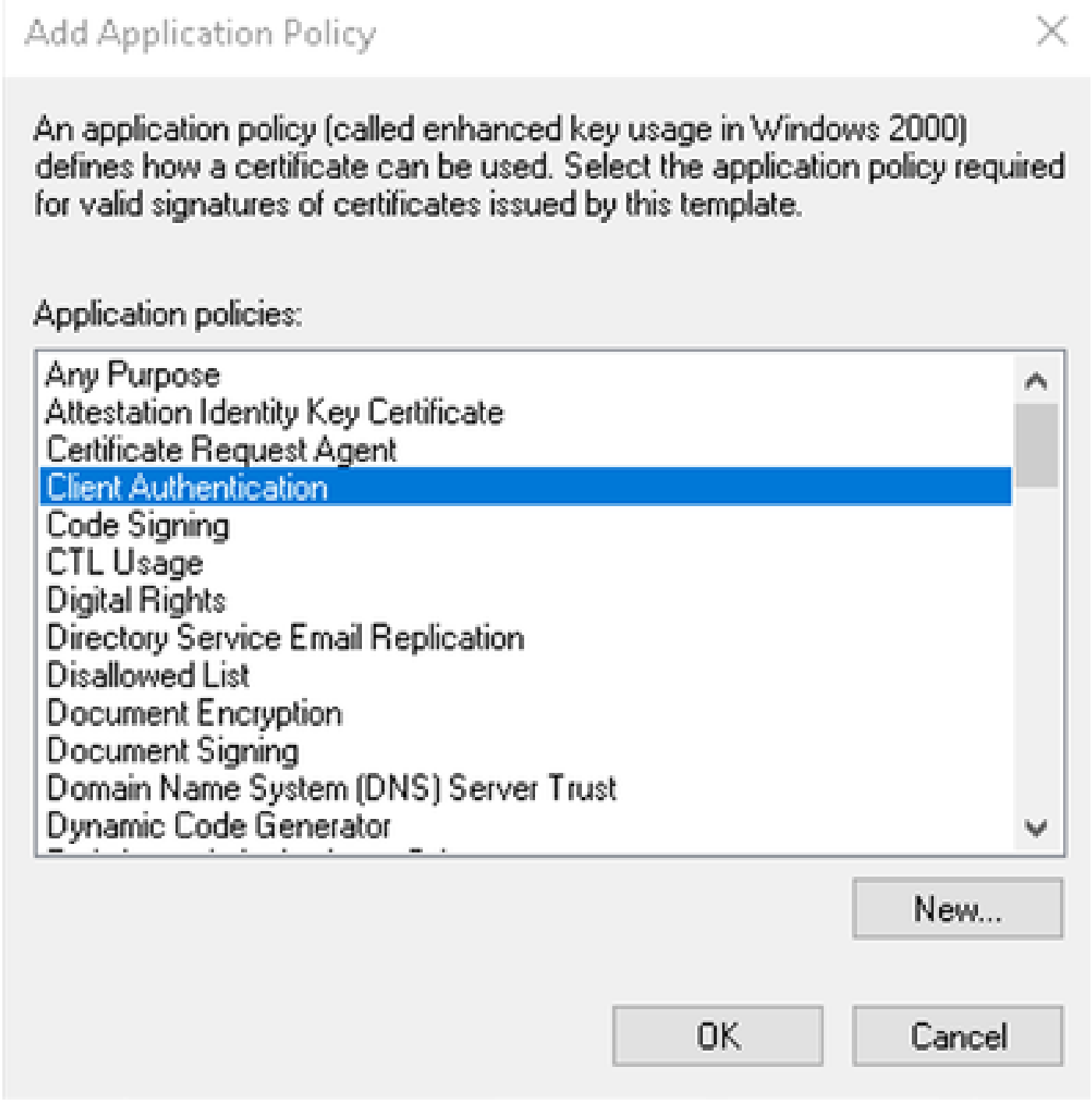
注：このタブで、テンプレートにkeyEnciphermentやdigitalSignatureなどのCatalyst Center証明書で必要とされる必須のキー使用法の拡張が含まれていることを確認します。これらは、ベースとして使用されるデフォルトのWebサーバテンプレートにすでに存在します。


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

- addをクリックし、client authenticationを見つけて、okをクリックして含めます。

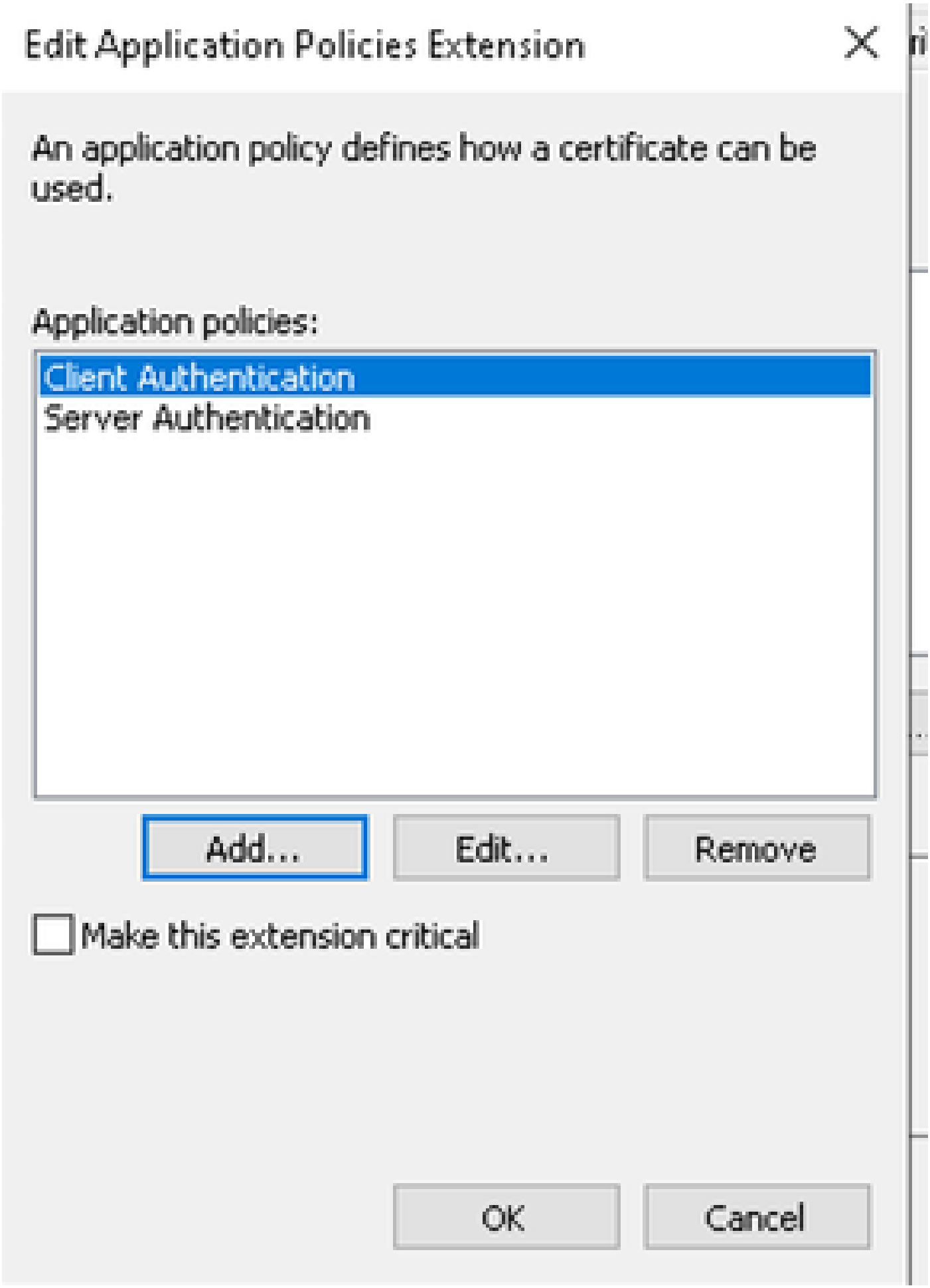

Edit Application Policies Extension
An application policy defines how a certificate can be used.
Application policies:
Server Authentication
Add...
Edit...
Remove
Make this extension critical
OK
Cancel

クライアント認証



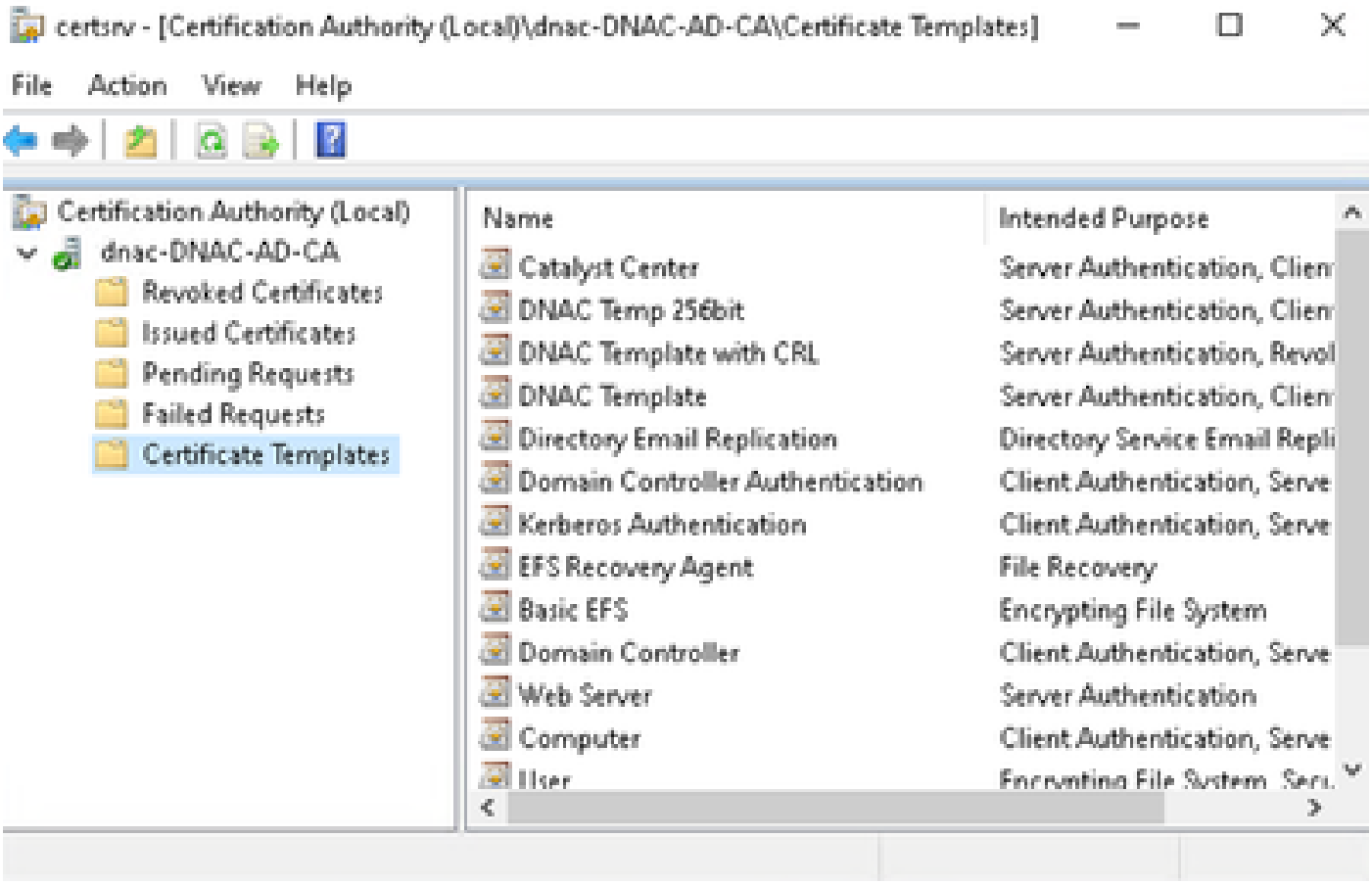
アプリケーションポリシーの追加

- テンプレートに、デフォルトの使用状況とともにクライアント認証が表示されていることを確認します。


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. applyをクリックし、次にokをクリックします。

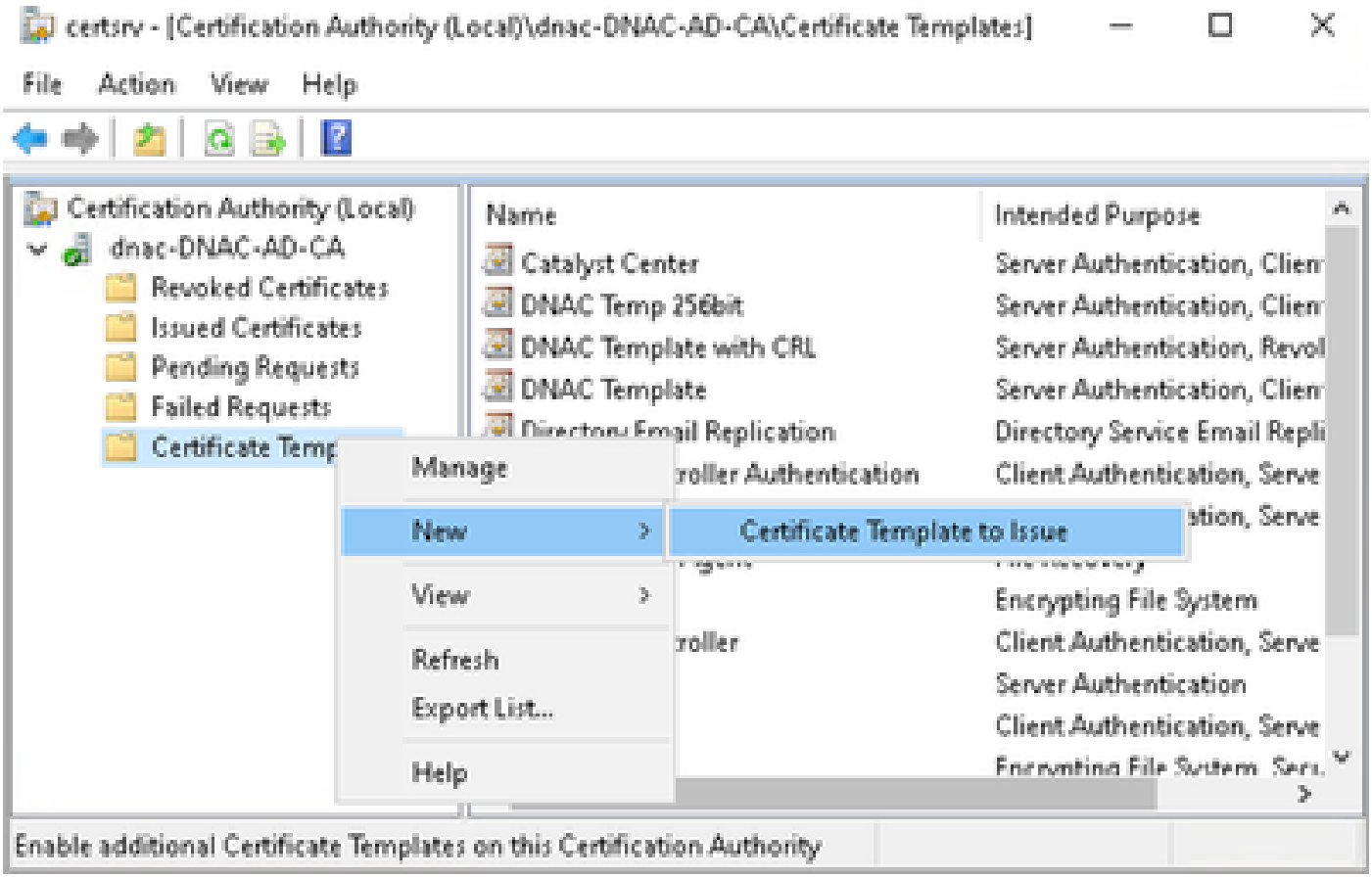
8. Certificate Authorityコンソールで、CAツリーを展開し、certificate templatesフォルダを選択します。



CAツリー証明書テンプレート

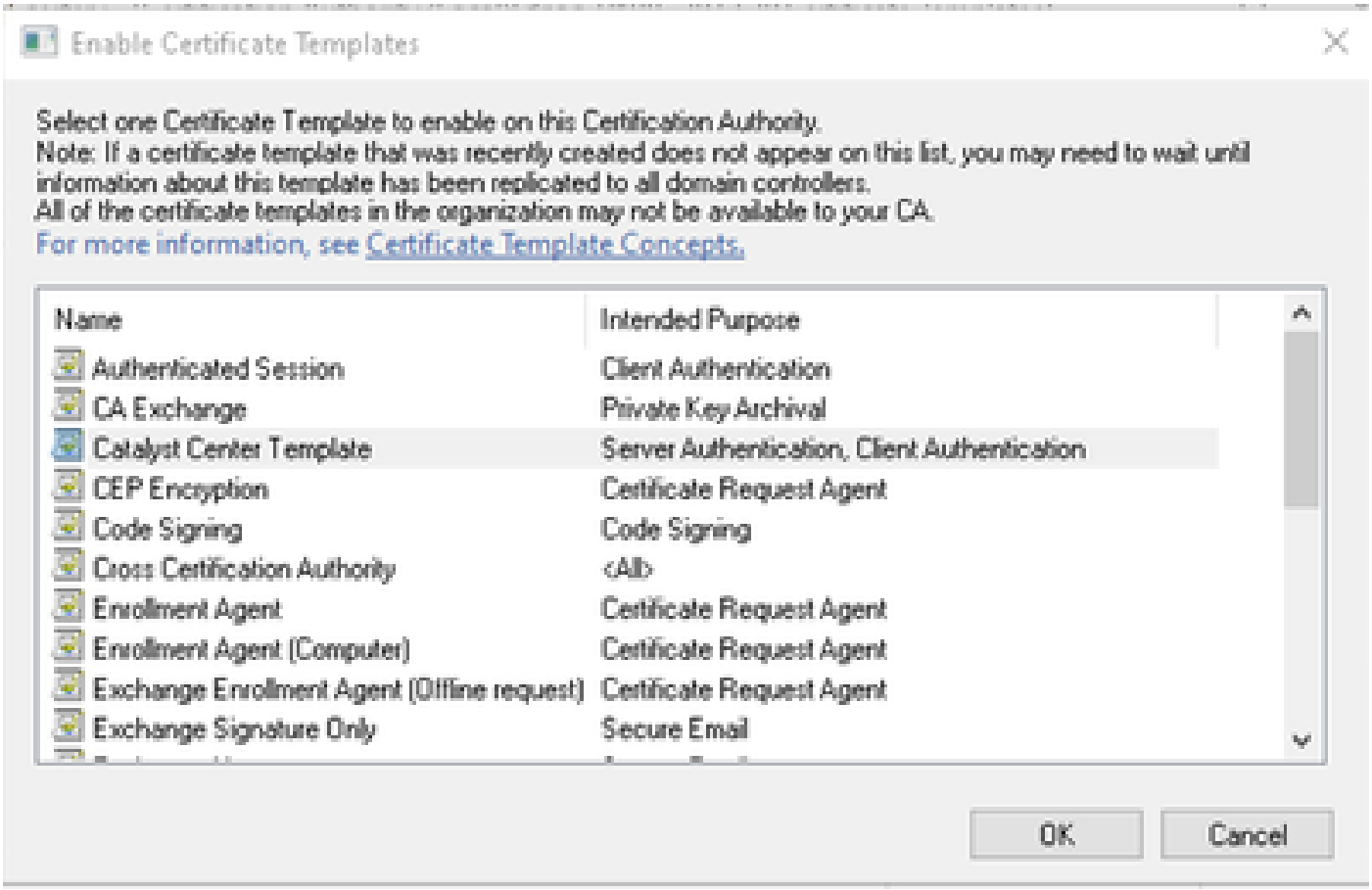
9. certificate templatesフォルダを右クリックし、次のいずれかを選択します。

[新規作成] > [発行する証明書テンプレート].



発行する新しい証明書テンプレート

10. 新しいウィンドウで、新しく作成したテンプレート（たとえば、Catalyst Center Template）を選択し、okをクリックします。

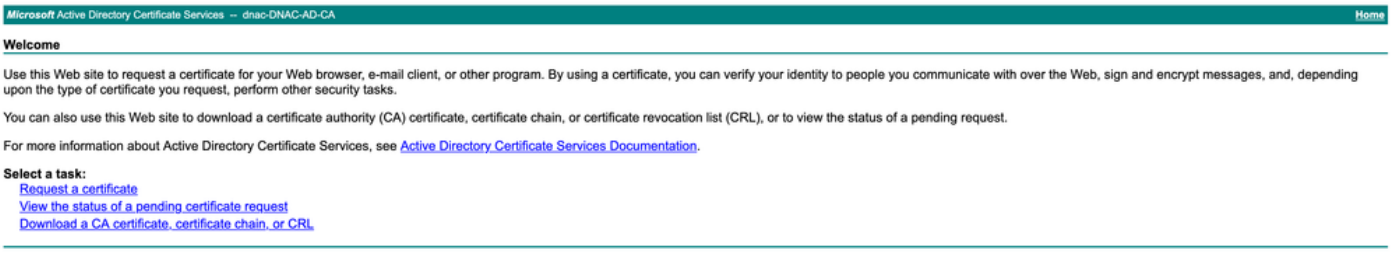


Catalyst Centerテンプレート

11. これで、テンプレートがCAのCertificate Templatesリストの下に表示されます。

12. ブラウザを開き、次の場所に移動します。

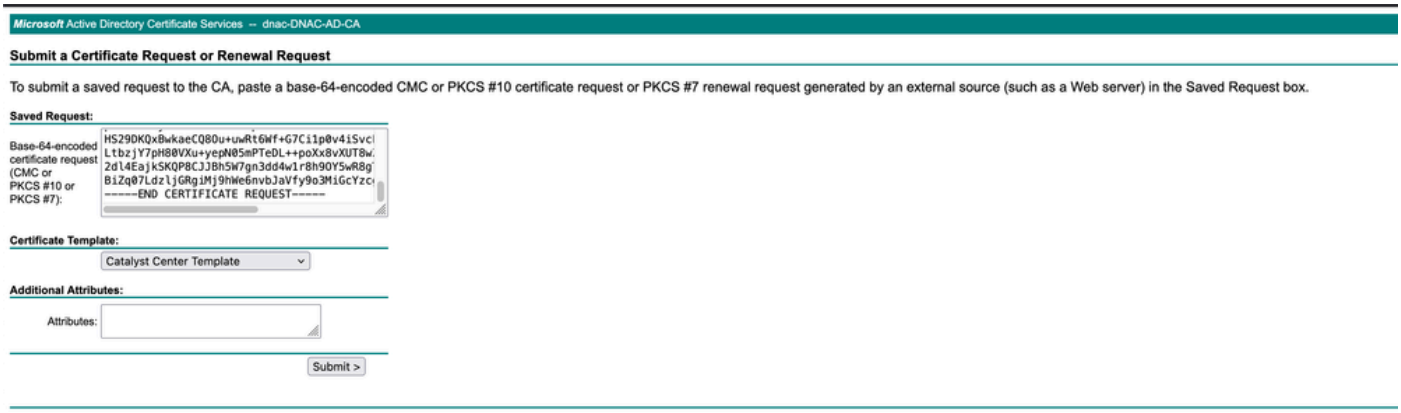
```
http://localhost/certsrv/
```



ログインページhttp://localhost/certsrv/

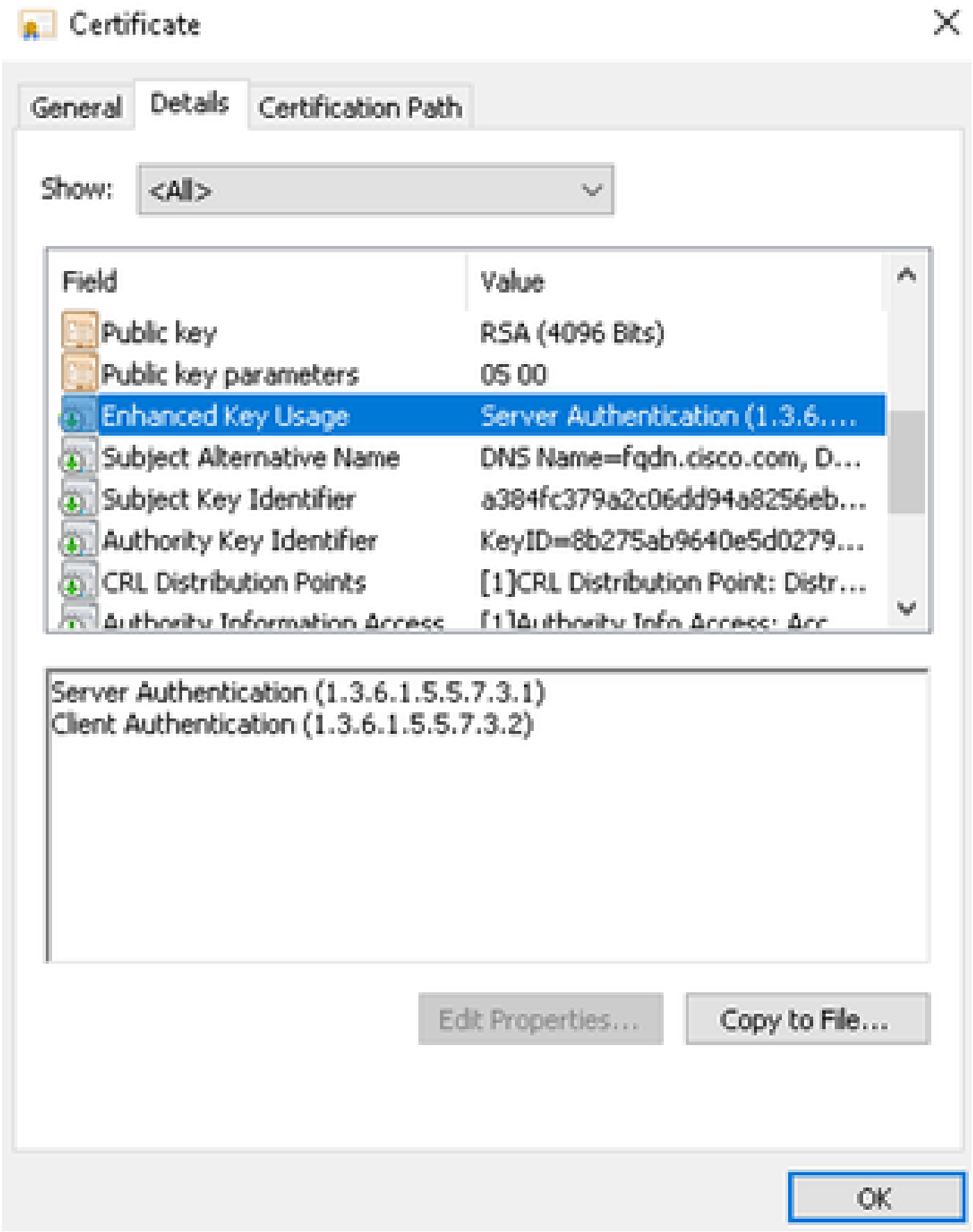
13. request a certificate、advanced certificate requestの順に選択し、新しいテンプレートが使用可能であることを確認します。

14. このページで、CSRを送信し、新しく作成したテンプレートを選択して署名付き証明書を生成します。



証明書の要求

13.証明書は、例に示すように、正しい拡張子で生成されます。



証明書の例

トラブルシュート

CSRの署名中にエラーが発生した場合は、Windowsサーバログで詳細を確認してください。

エラー:

エラーのトラブルシューティング

1. 次のコマンドを実行して、イベントビューアを開きます。

```
eventvwr.msc
```

2. [イベントビューア] > [Windowsログ] > [アプリケーション] に移動します。

3. 次の条件を満たすイベントをフィルタまたは検索します。

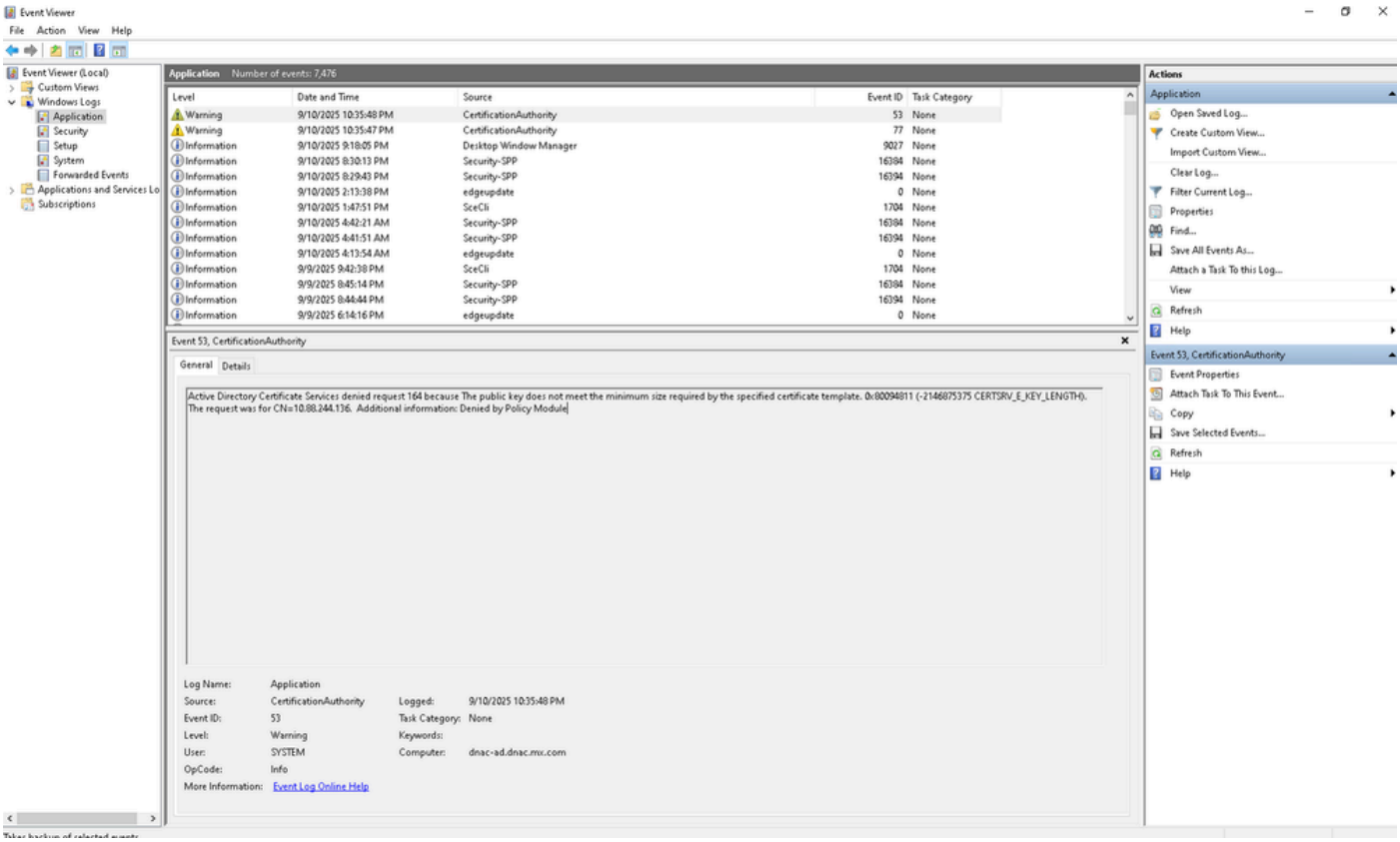
    1. 送信元 = 認証局

    2. Event ID = 53、54、55、またはsimilar (これらは、要求が発行されたか、拒否されたか、または保留中であることを示します) 。

    3. イベントメッセージには、拒否の理由に関する詳細 (該当する場合) が含まれます。

4. Findオプション(Application > Find...を右クリック)を使用して、次の条件で検索します。

- 証明書SRV
- 要求ID(既知の場合、164など)



Windows Serverログのトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。