

# CUCM用のWindows CA証明書テンプレートの作成

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[Callmanager/Tomcat/TVSテンプレート](#)

[IPsecテンプレート](#)

[CAPFテンプレート](#)

[証明書署名要求の生成](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、Windows Serverベースの証明機関(CA)で証明書テンプレートを作成する手順を説明します。

## 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。

- CUCM バージョン 11.5(1)
- Windows Serverの管理に関する基本的な知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 11.5(1)
- CAサービスがインストールされたMicrosoft Windows Server 2012 R2。


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

これらの証明書テンプレートは、すべてのタイプのCisco Unified Communications Manager(CUCM)証明書のX.509拡張要件に準拠しています。

外部CAによって署名できる証明書には、次の5種類があります。

証明書	利用	影響を受けるサービス
CallManager	セキュアなデバイス登録で提示され、証明書信頼リスト(CTL)/内部信頼リスト(ITL)ファイルに署名できます。このファイルは、セキュアなセッション開始プロトコル(SIP)トランクなど、他のサーバとのセキュアなインタラクションに使用されます。	<ul style="list-style-type: none"><li>・ Cisco Call Manager</li><li>・ Cisco CTI Manager</li><li>・ Cisco TFTP</li></ul>
Tomcat	Secure Hypertext Transfer Protocol(HTTPS)の相互対話に対して提示されます。	<ul style="list-style-type: none"><li>・ Cisco Tomcat</li><li>・ シングルサインオン(SSO)</li><li>・ エクステンションモビリティ</li><li>・ Corporate Directory</li></ul>
IPSec	バックアップファイルの生成、およびIP Security(IPsec)とMedia Gateway Control Protocol(MGCP)またはH323ゲートウェイとのインタラクションに使用されます。	<ul style="list-style-type: none"><li>・ Cisco DRFプライマリ</li><li>・ Cisco DRF Local</li></ul>
CAPF	電話機のローカルで有効な証明書(LSC)を生成するために使用されます。	<ul style="list-style-type: none"><li>・ Cisco Certificate Authority Proxy Function</li></ul>
TVS	電話機が不明な証明書を認証できない場合に、Trust Verification Service(TVS)への接続を作成するために使用されます。	<ul style="list-style-type: none"><li>・ Cisco Trust Verification Service</li></ul>

 注:14以降のバージョンではTomcat証明書が代わりに使用されるため、ipsec証明書はCisco DRFプライマリおよびCisco DRFローカルとは関連していません。この変更を12.5以前のバージョンに追加する予定はありません。

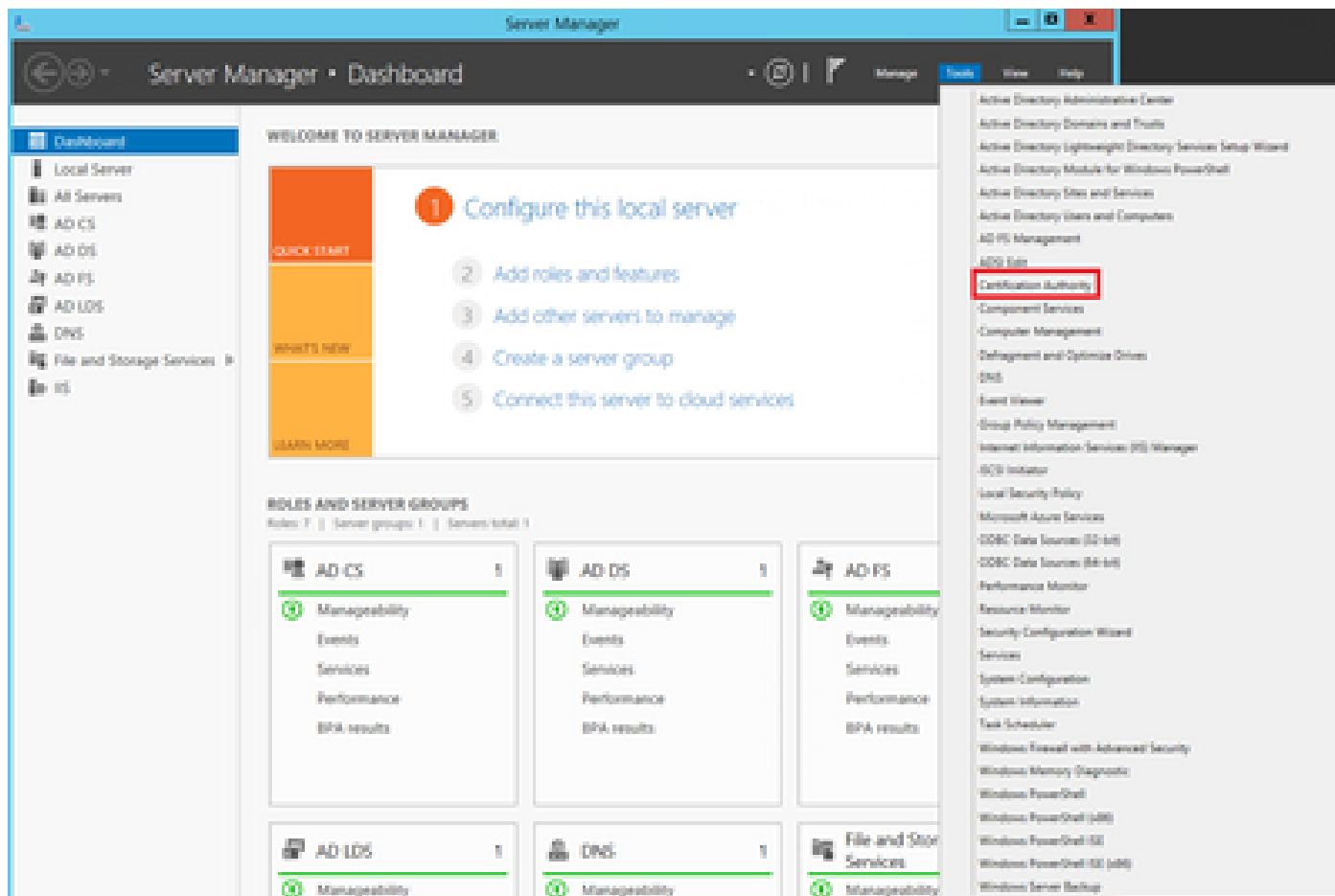
これらの証明書にはそれぞれX.509拡張要件があり、これを設定する必要があります。これを設定しないと、前述のサービスのいずれかで誤動作が発生する可能性があります。

証明書	X.509キーの使用法	X.509拡張キーの使用
CallManager	<ul style="list-style-type: none"><li>デジタル署名 ( Digital Signature )</li><li>主要な暗号化</li><li>データの暗号化</li></ul>	<ul style="list-style-type: none"><li>Webサーバ認証</li><li>Webクライアント認証</li></ul>
Tomcat	<ul style="list-style-type: none"><li>デジタル署名 ( Digital Signature )</li><li>主要な暗号化</li><li>データの暗号化</li></ul>	<ul style="list-style-type: none"><li>Webサーバ認証</li><li>Webクライアント認証</li></ul>
IPSec	<ul style="list-style-type: none"><li>デジタル署名 ( Digital Signature )</li><li>主要な暗号化</li><li>データの暗号化</li></ul>	<ul style="list-style-type: none"><li>Webサーバ認証</li><li>Webクライアント認証</li><li>IPsecエンドシステム</li></ul>
CAPF	<ul style="list-style-type: none"><li>デジタル署名 ( Digital Signature )</li><li>証明書署名</li><li>主要な暗号化</li></ul>	<ul style="list-style-type: none"><li>Webサーバ認証</li><li>Webクライアント認証</li></ul>
TVS	<ul style="list-style-type: none"><li>デジタル署名 ( Digital Signature )</li><li>主要な暗号化</li><li>データの暗号化</li></ul>	<ul style="list-style-type: none"><li>Webサーバ認証</li><li>Webクライアント認証</li></ul>

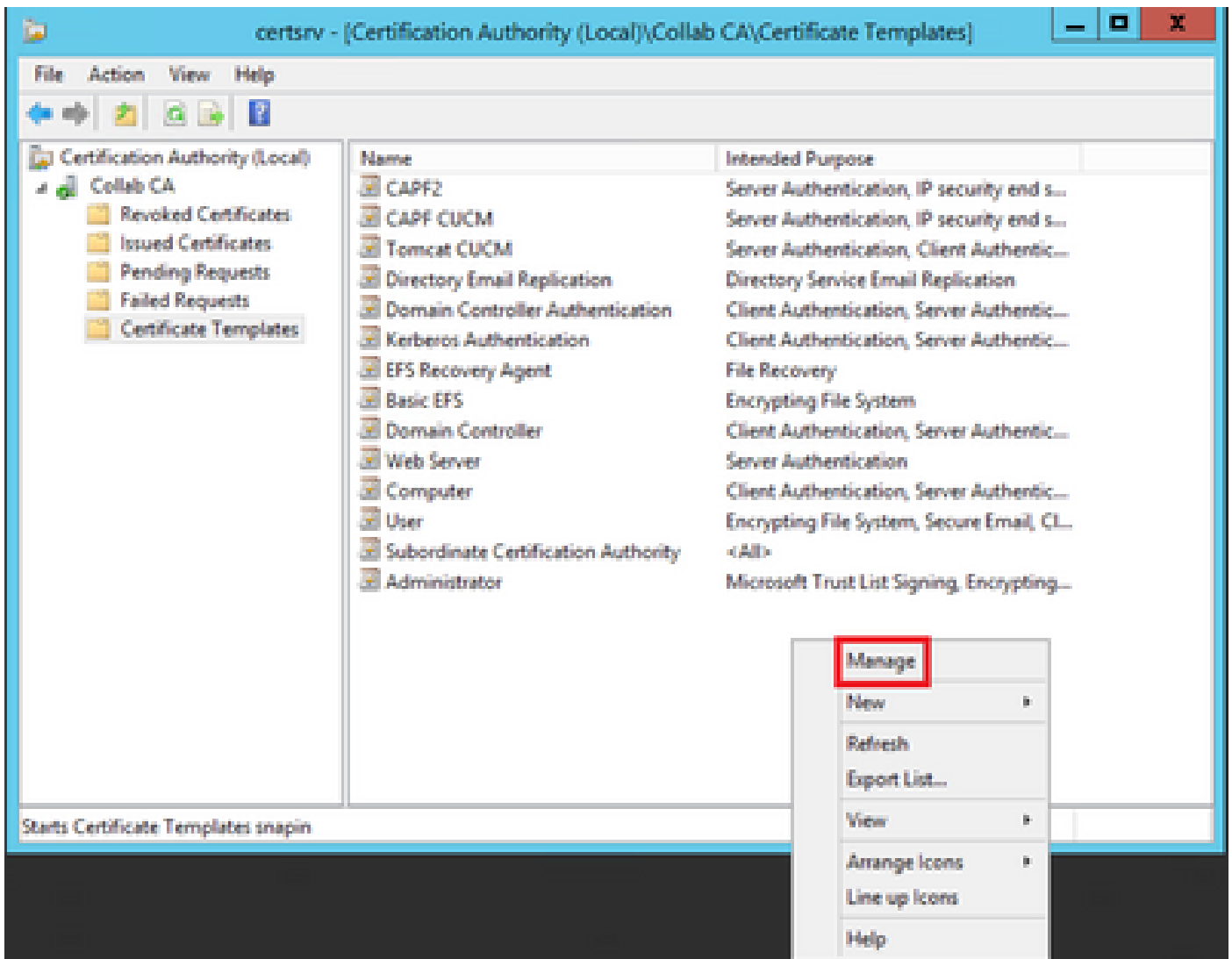
詳細については、『[Security Guide for Cisco Unified Communications Manager](#)』を参照してください。

## 設定

ステップ 1：図に示すように、Windows ServerでServer Manager > Tools > Certification Authorityの順に移動します。



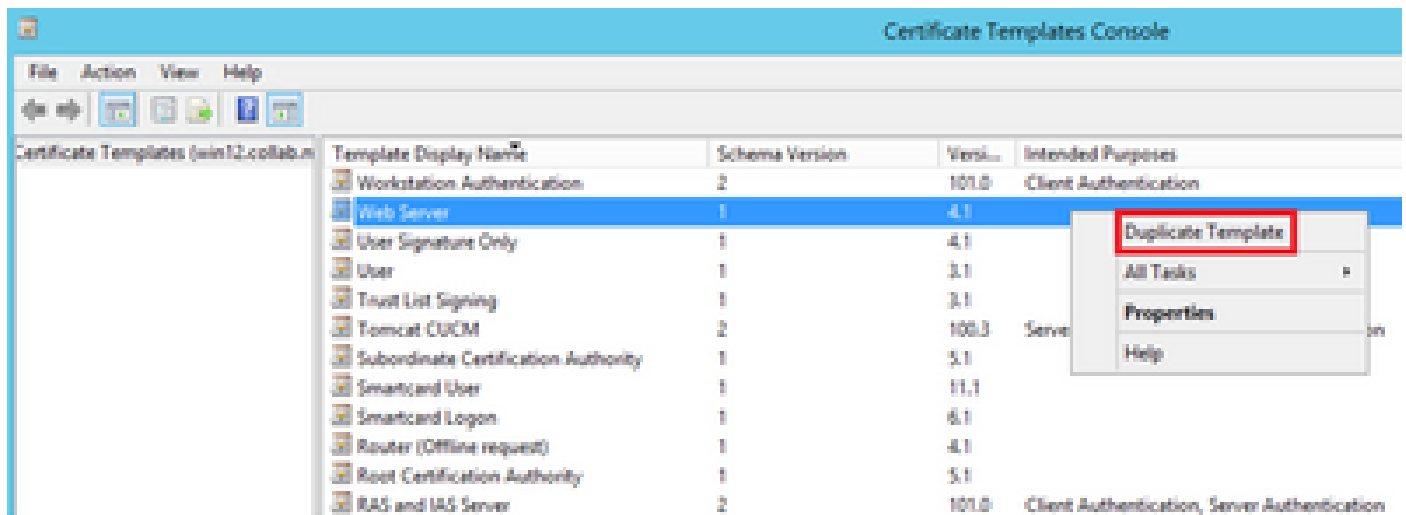
ステップ 2：次の図に示すように、CAを選択し、Certificate Templatesに移動して、リストを右クリックし、Manageを選択します。



## Callmanager/Tomcat/TVSテンプレート

次の図は、CallManagerテンプレートの作成のみを示しています。同じ手順で、TomcatおよびTVSサービスの証明書テンプレートを作成できます。唯一の違いは、手順2で新しいテンプレートごとに各サービス名が使用されるようにすることです。

ステップ 1 : Web Serverテンプレートを見つけ、右クリックして、図に示すようにDuplicate Templateを選択します。



ステップ 2 : Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数を変更できます。

## Properties of New Template



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

Template display name:

Template name:

Validity period:

 years 

Renewal period:

 weeks 

Publish certificate in Active Directory

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

ステップ 3 : 図に示すように、Extensions > Key Usage > Editの順に移動します。



# Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
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 Key Usage:

Signature requirements:  
Digital signature

Allow key exchange only with key encryption

Critical extension.

OK Cancel Apply Help

ステップ 4 : 次の図に示すように、これらのオプションを選択してOKを選択します。

- デジタル署名 ( Digital Signature )
- キーの暗号化 ( キーの暗号化 ) でのみキー交換を許可する
- ユーザーデータの暗号化を許可する

## Properties of New Template



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

### Edit Key Usage Extension



Specify the required signature and security options for a key usage extension.

#### Signature

- Digital signature
- Signature is proof of origin (nonrepudiation)
- Certificate signing
- CRL signing

#### Encryption

- Allow key exchange without key encryption (key agreement)
- Allow key exchange only with key encryption (key encipherment)
  - Allow encryption of user data

- Make this extension critical

OK

Cancel

OK

Cancel

Apply

Help

ステップ 5 : 図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

# Properties of New Template



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

To modify an extension, select it, and then click Edit.

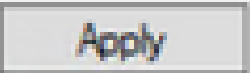
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage



Description of Application Policies:

Server Authentication



手順 6 : Client Authenticationを検索して選択し、次の図に示すように、このウィンドウと前のウィンドウの両方でOKを選択します。

## Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name	Server	Issuance Requirements		
...	Edit Application Policies Extension	X		

### 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

OK

Cancel

Apply

Help

手順 7 : テンプレートに戻り、Applyを選択してからOKを選択します。



## Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
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:

- Client Authentication
- Server Authentication

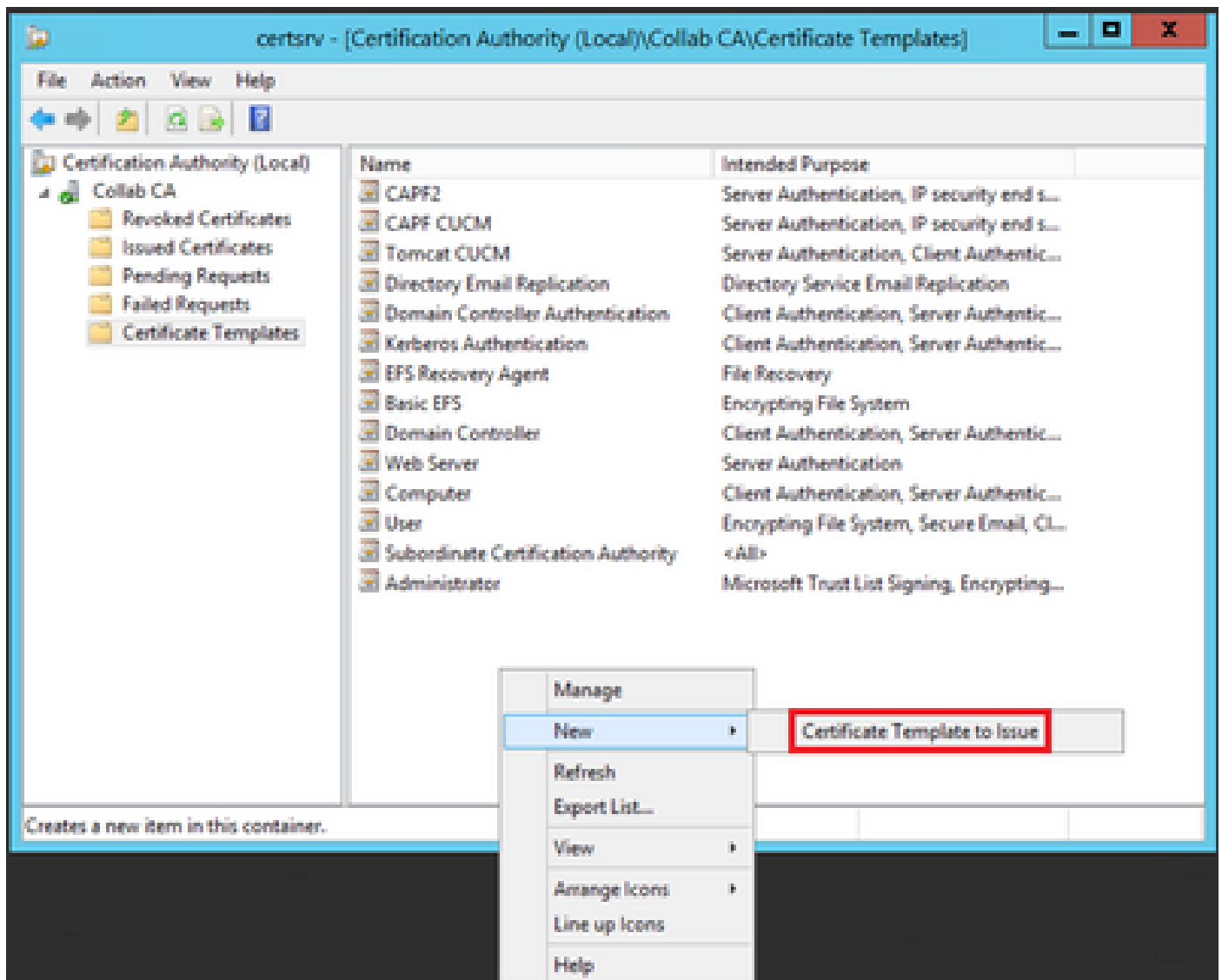
OK

Cancel

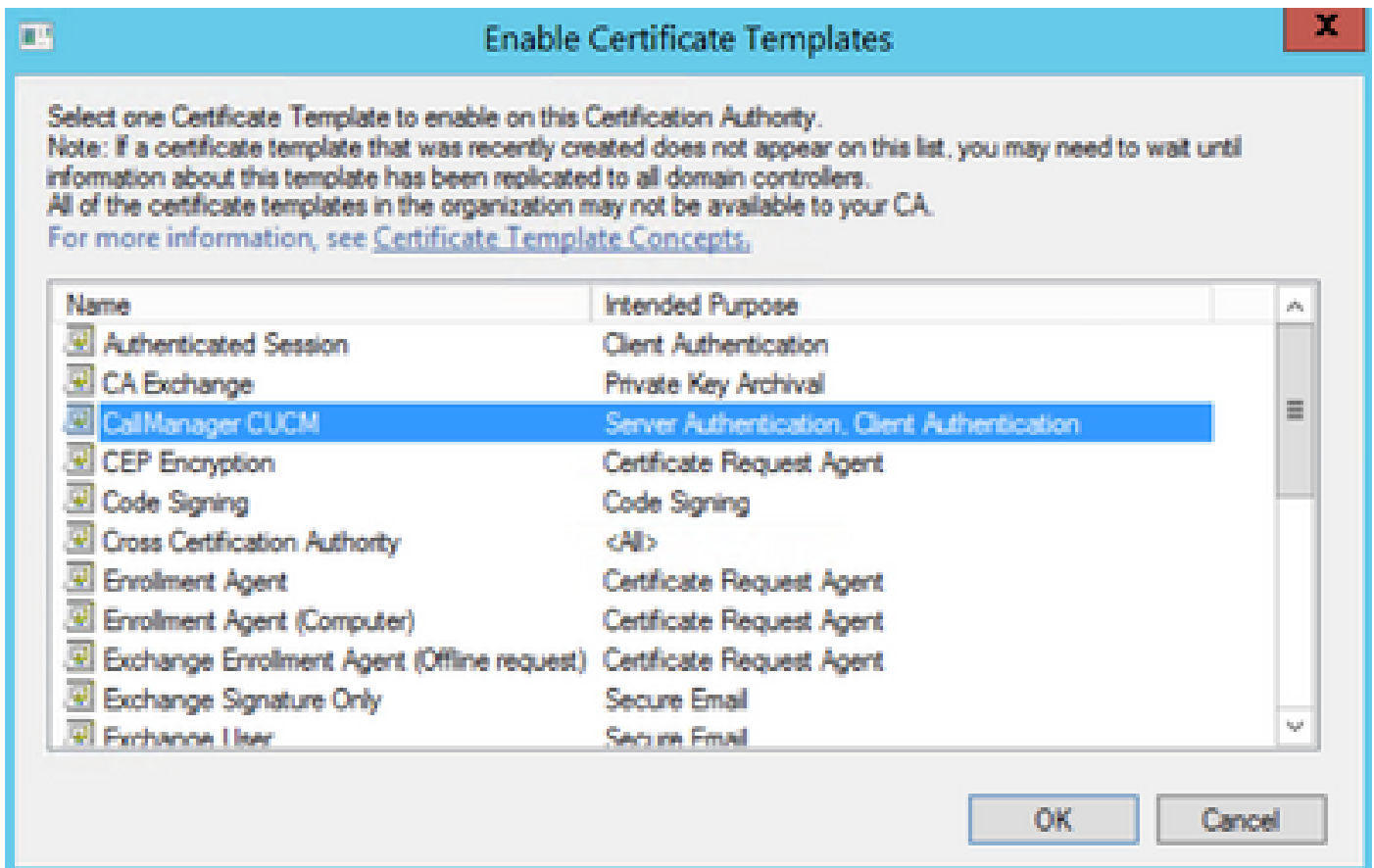
Apply

Help

ステップ 8 : Certificate Template Console ウィンドウを閉じ、最初のウィンドウに戻り、図に示すように New > Certificate Template to Issue の順に移動します。



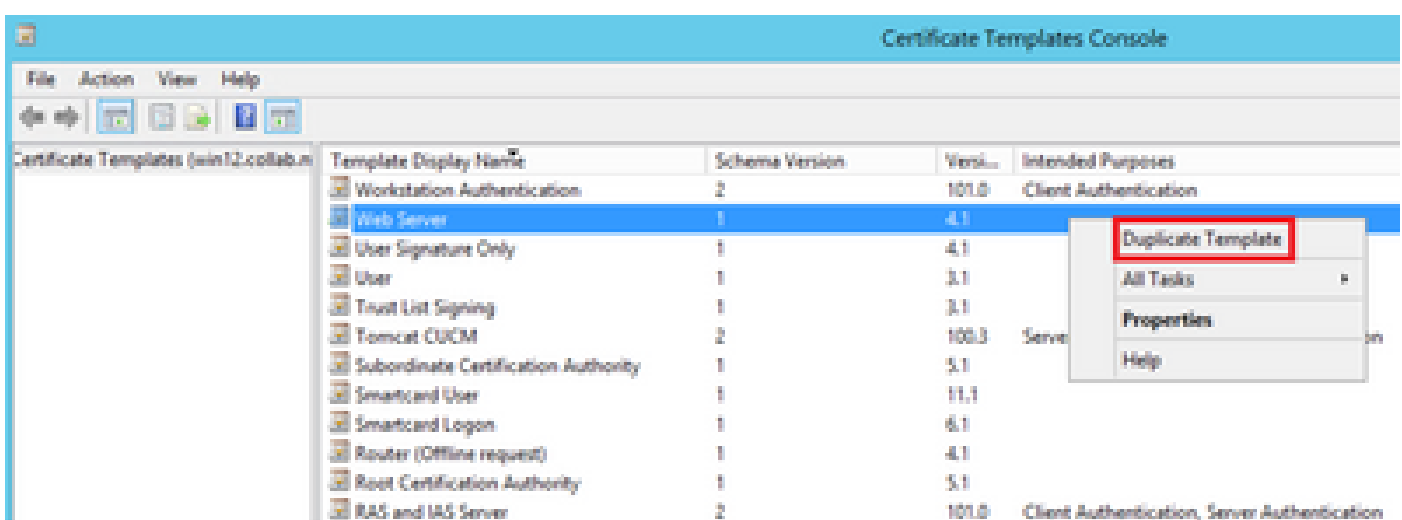
ステップ 9 : 図に示すように、新しい CallManager CUCM テンプレートを選択し、OK を選択します。



ステップ 10 : 必要に応じて、前述のすべての手順を繰り返して、TomcatおよびTVSサービスの証明書テンプレートを作成します。

## IPsecテンプレート

ステップ 1 : Web Serverテンプレートを見つけ、右クリックして、図に示すようにDuplicate Templateを選択します。



ステップ 2 : Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数を変更できます。

## Properties of New Template



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

Template display name:

Template name:

Validity period:

Renewal period:

Publish certificate in Active Directory

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

ステップ 3 : 図に示すように、Extensions > Key Usage > Editの順に移動します。

# Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
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 Key Usage:

Signature requirements:  
Digital signature

Allow key exchange only with key encryption

Critical extension.

OK Cancel Apply Help

ステップ 4 : 次の図に示すように、これらのオプションを選択してOKを選択します。

- デジタル署名 ( Digital Signature )
- キーの暗号化 ( キーの暗号化 ) でのみキー交換を許可する
- ユーザーデータの暗号化を許可する

## Properties of New Template



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

### Edit Key Usage Extension



Specify the required signature and security options for a key usage extension.

#### Signature

- Digital signature
- Signature is proof of origin (nonrepudiation)
- Certificate signing
- CRL signing

#### Encryption

- Allow key exchange without key encryption (key agreement)
- Allow key exchange only with key encryption (key encipherment)
  - Allow encryption of user data

Make this extension critical

OK

Cancel

OK

Cancel

Apply

Help



ステップ 5 : 図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

## Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
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

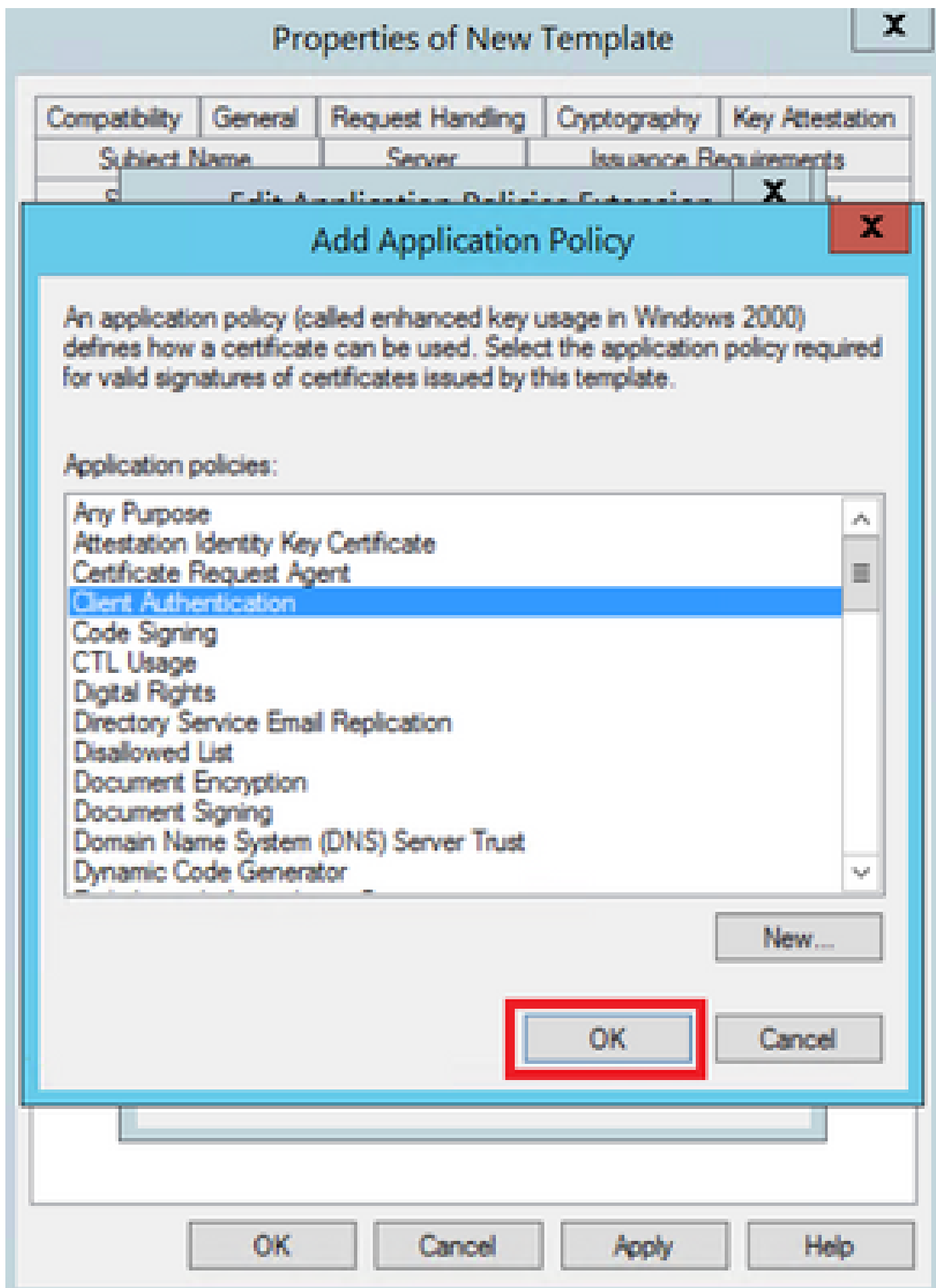
OK

Cancel

Apply

Help

手順 6 : Client Authenticationを検索して選択し、図に示すようにOKをクリックします。



手順 7 : 再度Addを選択し、IP security end systemを検索して選択し、これと前のウィンドウの両方でOKを選択します。

## Properties of New Template



Subject Name		Server		Issuance Requirements	
Compatibility	General	Request Handling	Controversy	Key Attestation	
					X
Edit Application Policies Extension					

### 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:

- Early Launch Antimalware Driver
- Embedded Windows System Component Verification
- Encrypting File System
- Endorsement Key Certificate
- File Recovery
- HAL Extension
- IP security end system**
- IP security IKE intermediate
- IP security tunnel termination
- IP security user
- KDC Authentication
- Kernel Mode Code Signing
- Key Pack Licenses

New...

OK

Cancel

OK

Cancel

Apply

Help

ステップ 8 : テンプレートに戻り、図に示すように、Applyを選択してからOKを選択します。

## 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:

- Client Authentication
- IP security end system
- Server Authentication

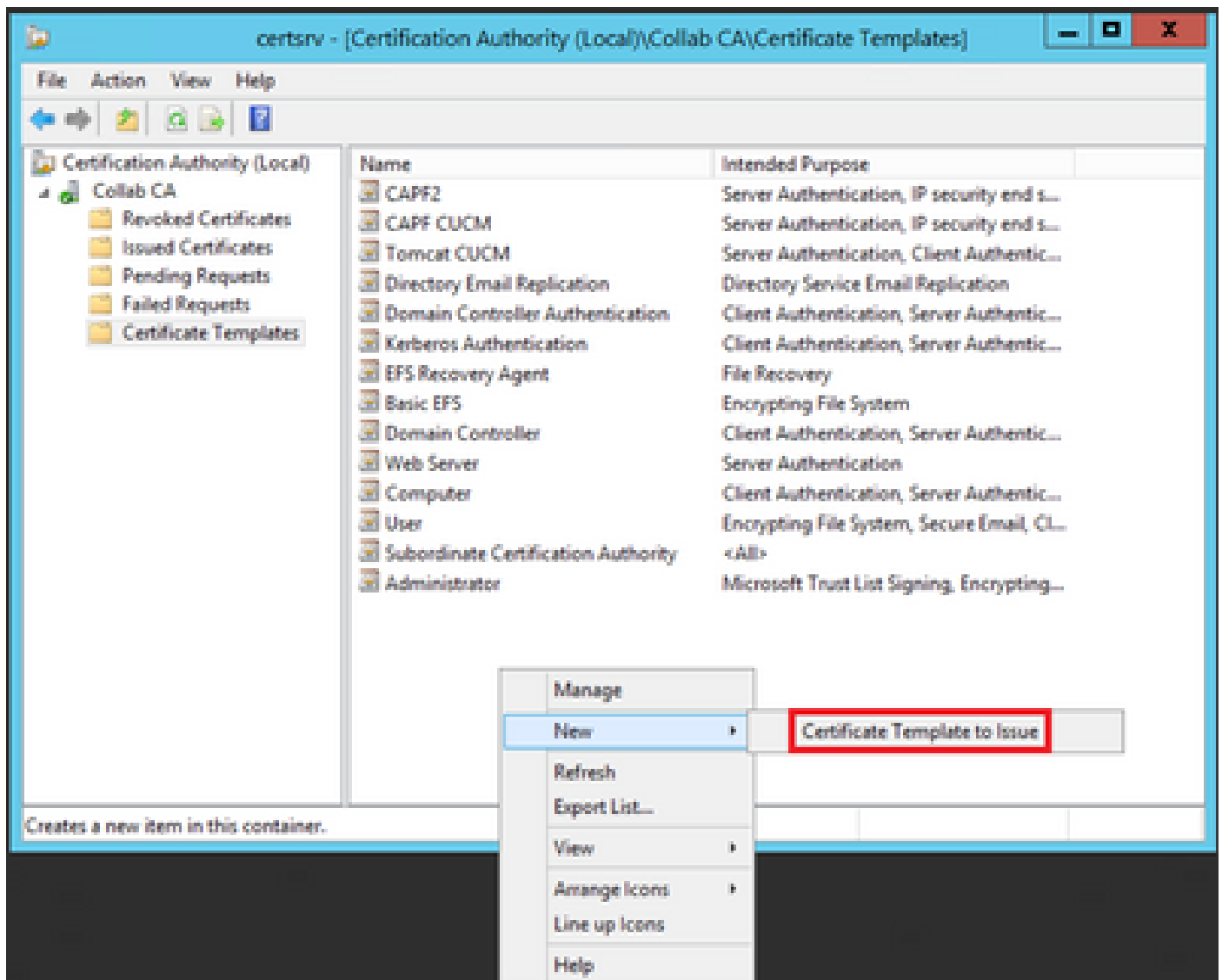
OK

Cancel

Apply

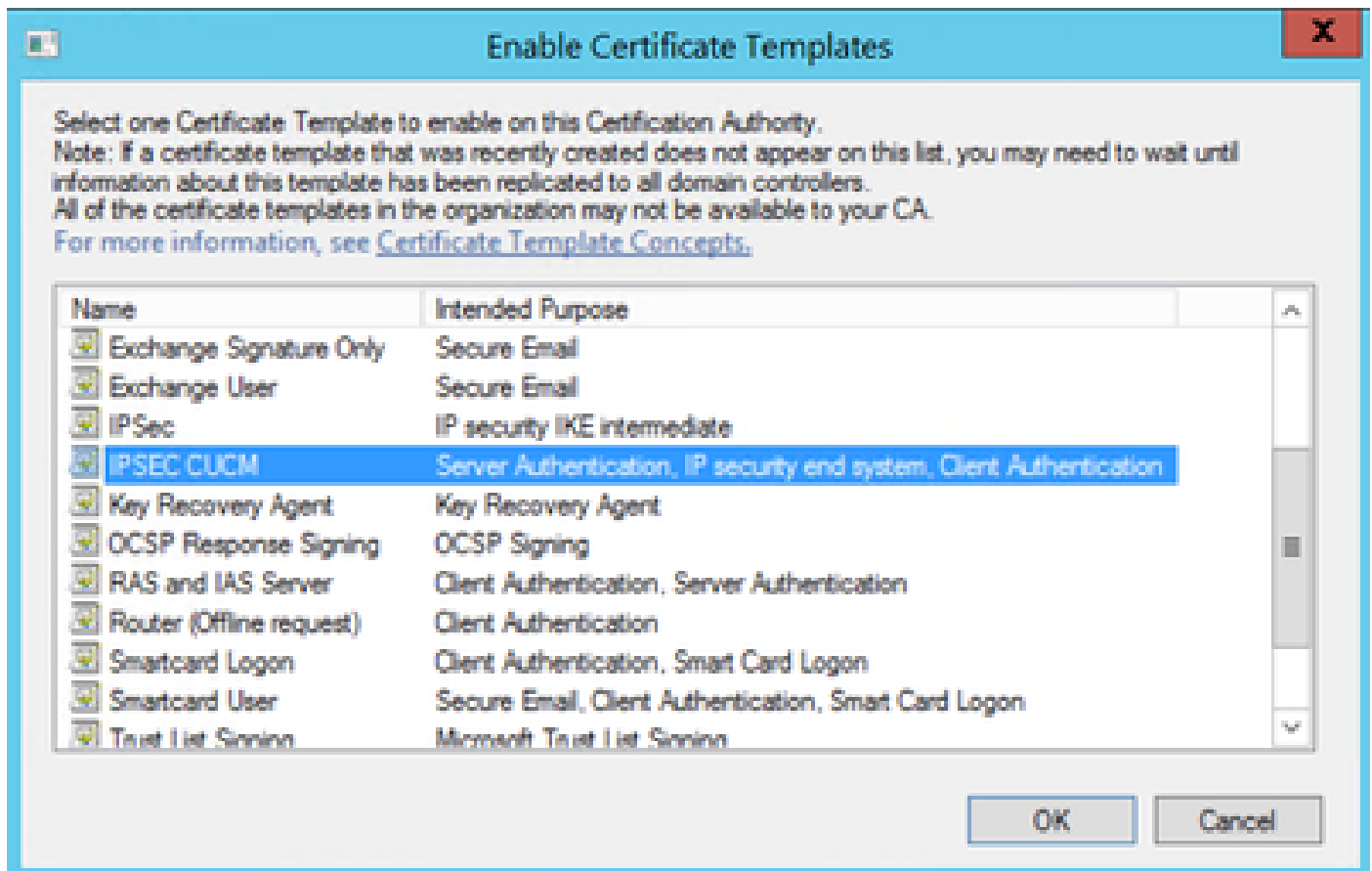
Help

ステップ 9 : Certificate Templates Console ウィンドウを閉じ、最初のウィンドウに戻り、図に示すように New > Certificate Template to Issue の順に移動します。



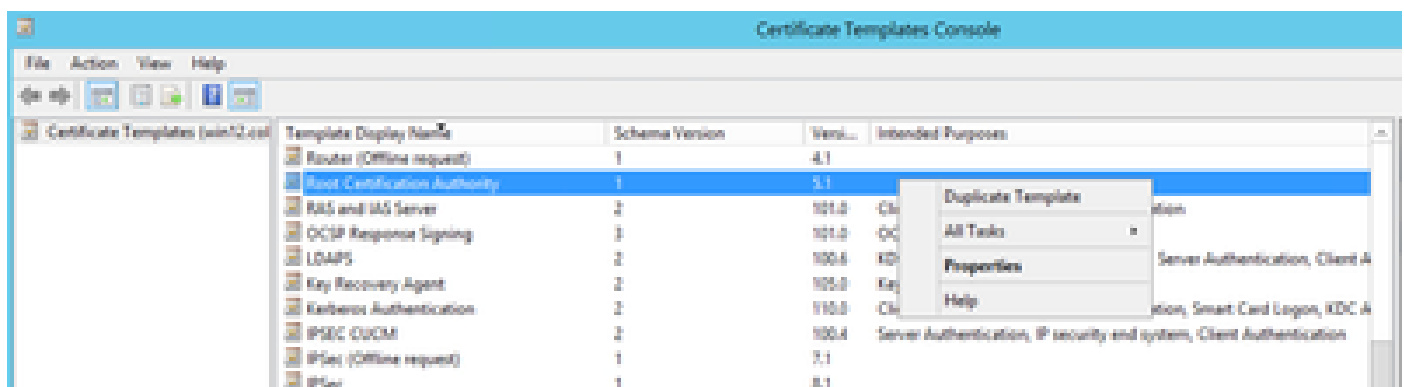
ステップ 10 : 図に示すように、新しい IPSEC CUCM テンプレートを選択し、OK を選択します。





## CAPFテンプレート

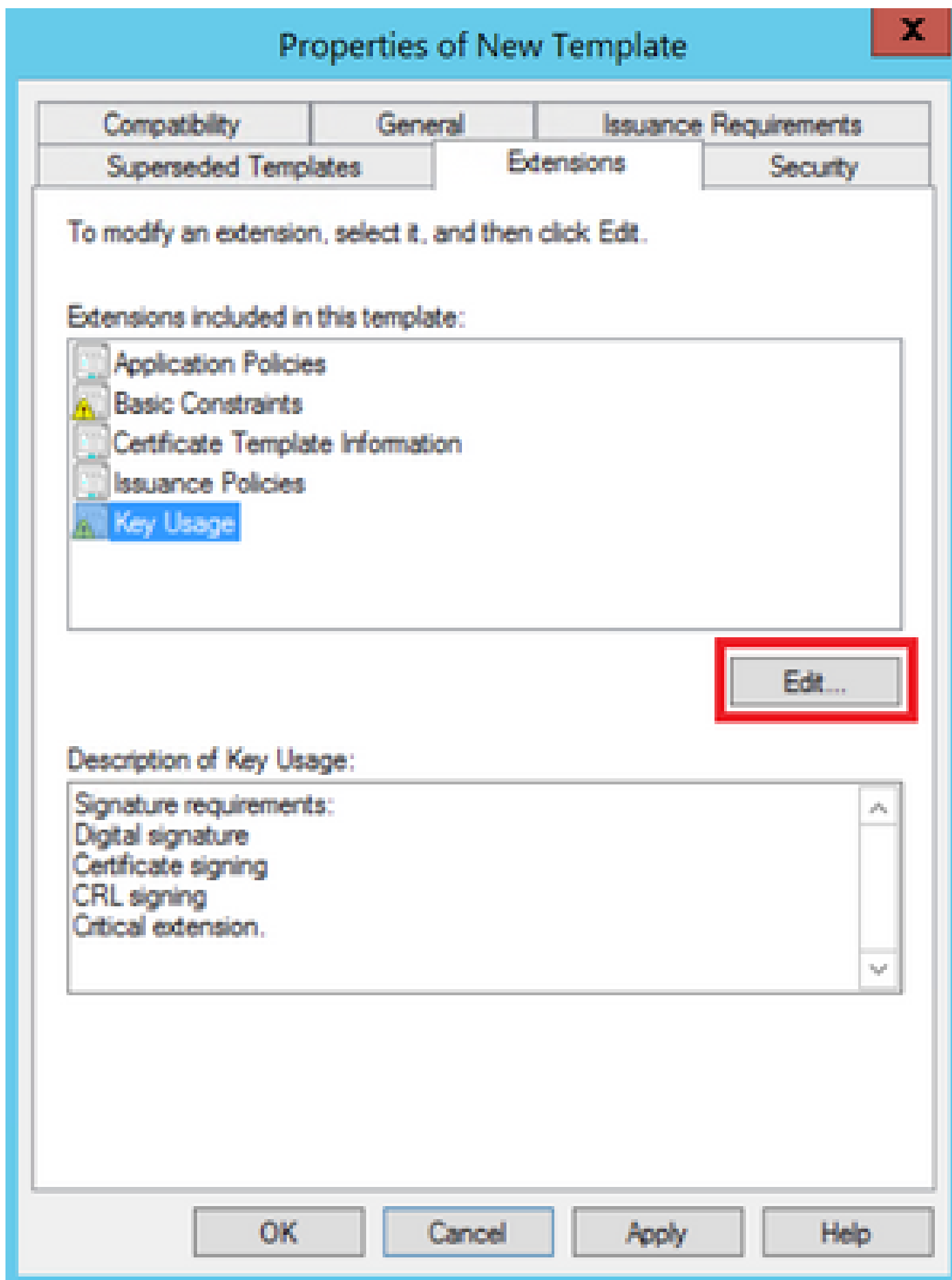
ステップ 1：ルートCAテンプレートを見つけて右クリックします。次に、図に示すように、Duplicate Templateを選択します。



ステップ 2：Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数を変更できます。



ステップ 3 : 図に示すように、Extensions > Key Usage > Editの順に移動します。



ステップ 4 : 次の図に示すように、これらのオプションを選択してOKを選択します。

- デジタル署名 ( Digital Signature )
- 証明書の署名
- CRL署名

## Properties of New Template



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

### Edit Key Usage Extension



Specify the required signature and security options for a key usage extension.

#### Signature

- Digital signature
- Signature is proof of origin (nonrepudiation)
- Certificate signing
- CRL signing

#### Encryption

- Allow key exchange without key encryption (key agreement)
- Allow key exchange only with key encryption (key encipherment)
  - Allow encryption of user data

Make this extension critical

OK

Cancel

OK

Cancel

Apply

Help

ステップ 5 : 図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

# Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
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

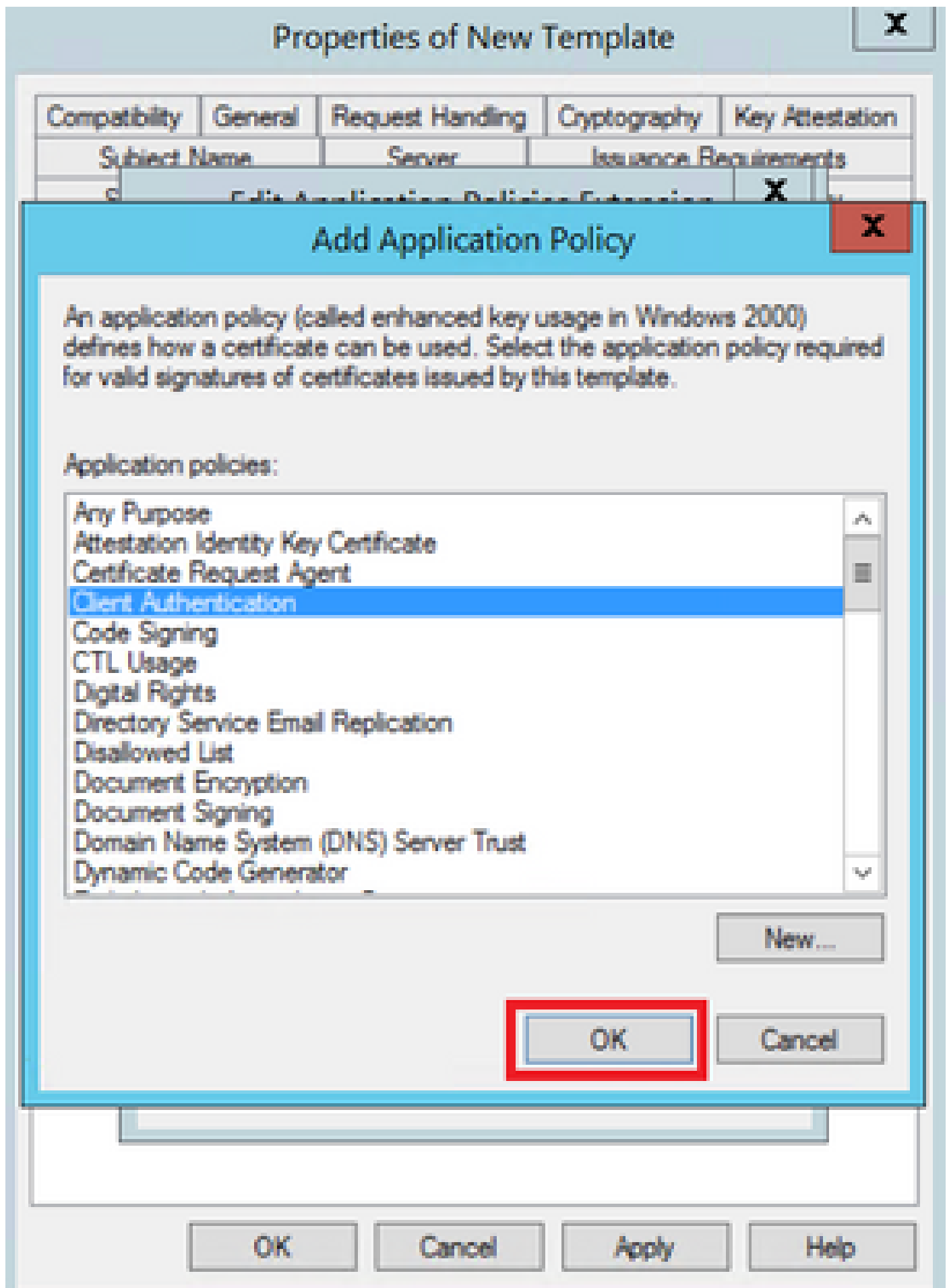
OK

Cancel

Apply

Help

手順 6 : Client Authenticationを検索して選択し、図に示すようにOKを選択します。





手順 7 : 再度Addを選択し、IP security end systemを検索して選択し、次に図に示すようにこのウィンドウと前のウィンドウでOKを選択します。

## Properties of New Template



Subject Name		Server		Issuance Requirements	
Compatibility	General	Request Handling	Controversy	Key Attestation	
					X
Edit Application Policies Extension					

### 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:

- Early Launch Antimalware Driver
- Embedded Windows System Component Verification
- Encrypting File System
- Endorsement Key Certificate
- File Recovery
- HAL Extension
- IP security end system**
- IP security IKE intermediate
- IP security tunnel termination
- IP security user
- KDC Authentication
- Kernel Mode Code Signing
- Key Pack Licenses

New...

OK

Cancel

OK

Cancel

Apply

Help

ステップ 8 : テンプレートに戻り、図に示すように、Applyを選択してからOKを選択します。

## 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:

- Client Authentication
- IP security end system
- Server Authentication

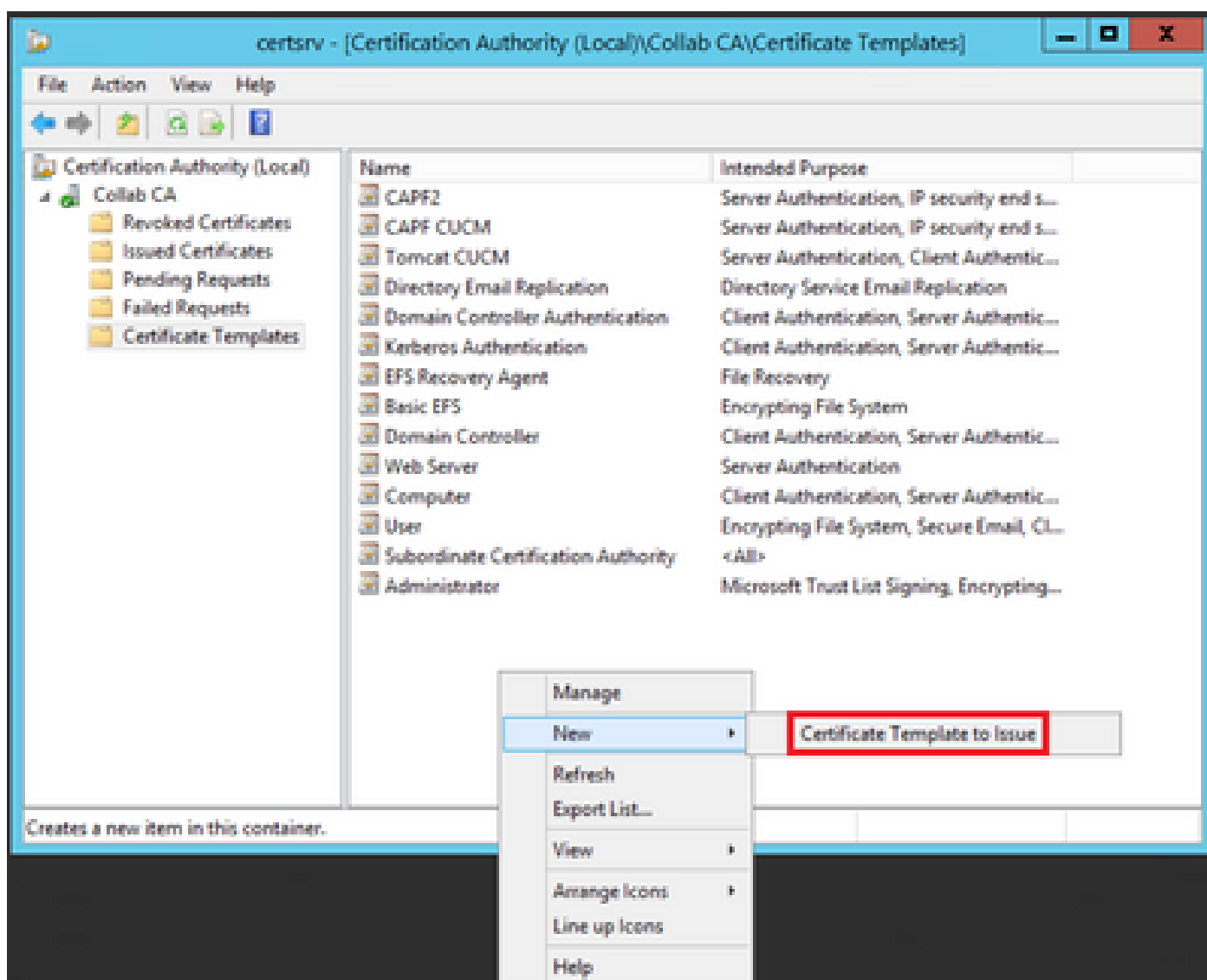
OK

Cancel

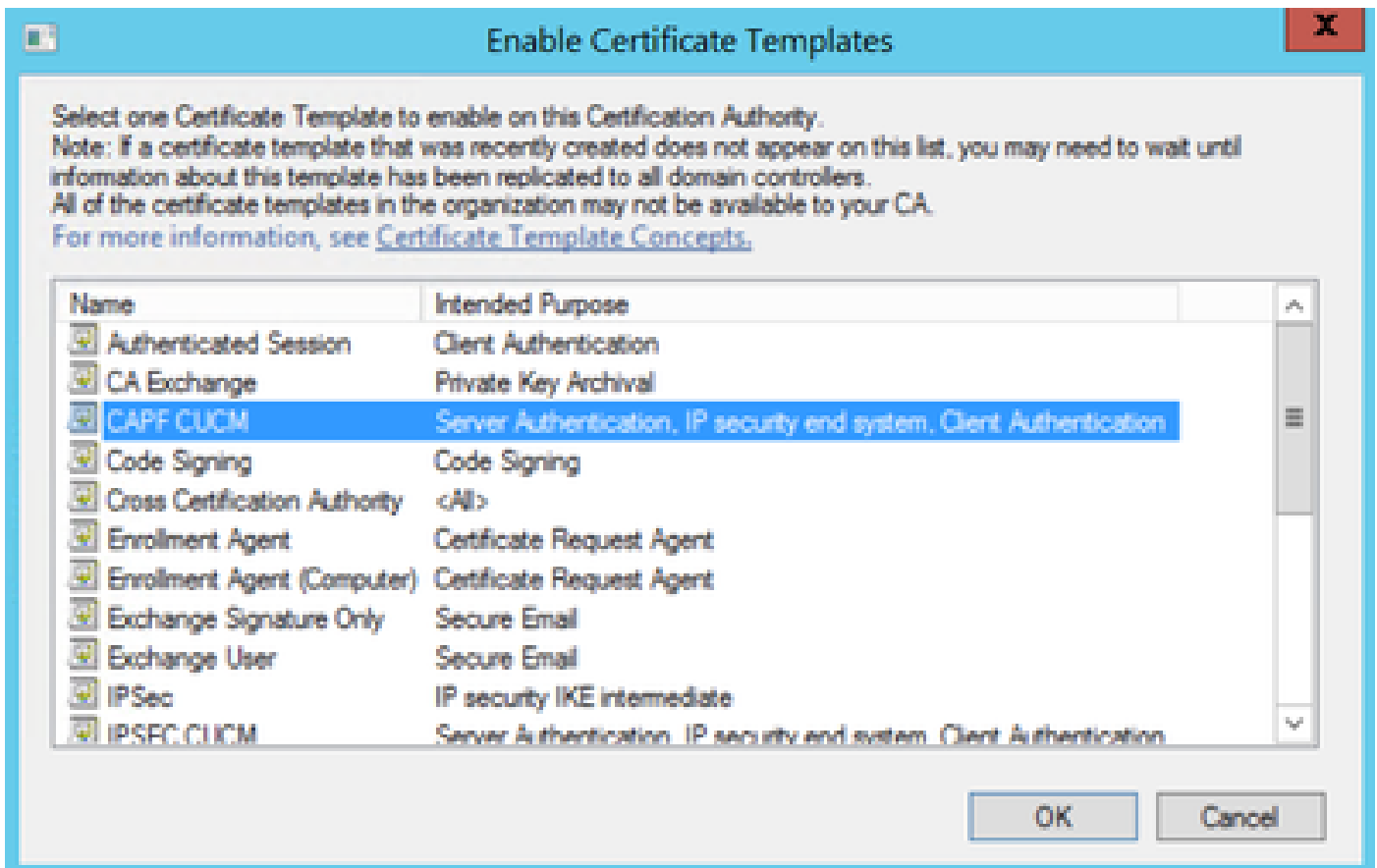
Apply

Help

ステップ 9 : Certificate Templates Console ウィンドウを閉じ、最初のウィンドウに戻り、図に示すように New > Certificate Template to Issue の順に移動します。



ステップ 10 : 図に示すように、新しいCAPF CUCMテンプレートを選択し、OKを選択します。



## 証明書署名要求の生成

新しく作成したテンプレートを使用してCallManager証明書を生成するには、次の例を使用します。同じ手順を任意の証明書タイプに使用できます。証明書とテンプレートのタイプを選択するだけです。

ステップ 1 : CUCMで、OS Administration > Security > Certificate Management > Generate CSRの順に移動します。


ステップ 2 : 次の図に示すように、これらのオプションを選択し、Generateを選択します。

- 証明書の目的 : CallManager
- ディストリビューション : <1台のサーバまたはマルチSAN用のいずれか>

Generate Certificate Signing Request

Generate Close

**Status**

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

**Generate Certificate Signing Request**

Certificate Purpose \*\* CallManager

Distribution \* Multi-server(SAN)

Common Name \* 115PUB-ms.maucabal.lab

**Subject Alternate Names (SANs)**

Auto-populated Domains

- 115PUB.maucabal.lab
- 115SUB.maucabal.lab

Parent Domain maucabal.lab

Other Domains

Choose File No file chosen

Please import .TXT file only.  
For more information please refer to the notes in the Help Section

Add

Key Type \*\* RSA

Key Length \* 2048

Hash Algorithm \* SHA256



Generate Close

ステップ 3 : 次の図に示すように、確認メッセージが生成されます。

Generate Certificate Signing Request

Generate Close

**Status**

-  Success: Certificate Signing Request Generated
-  CSR export operation successful on the nodes [115PUB.maucabal.lab, 115SUB.maucabal.lab].

ステップ 4 : 証明書リストで、CSR Onlyタイプのエントリを探し、図に示すように選択します。

Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
auth	AuthZ_admin	Self-signed	RSA	115PUB.maucabal.lab	AuthZ_admin	01/27/2018	Self-signed certificate generated by system
CallManager	115PUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(SAN)	--	--	--
CallManager	115PUB-ms.maucabal.lab	Self-signed	RSA	115PUB.maucabal.lab	115PUB.maucabal.lab	01/30/2013	Self-signed certificate generated by system
CallManager-ECDSA	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	01/04/2013	Self-signed certificate generated by system
CallManager-trust	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	01/04/2013	Trust Certificate

ステップ 5 : ポップアップウィンドウでDownload CSRを選択し、コンピュータにファイルを保存します。

### CSR Details for 115PUB-ms.maucabal.lab, CallManager

✖ Delete
  Download CSR

**Status**

i Status: Ready

**Certificate Settings**

File Name	CallManager.csr
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	

**Certificate File Data**

```

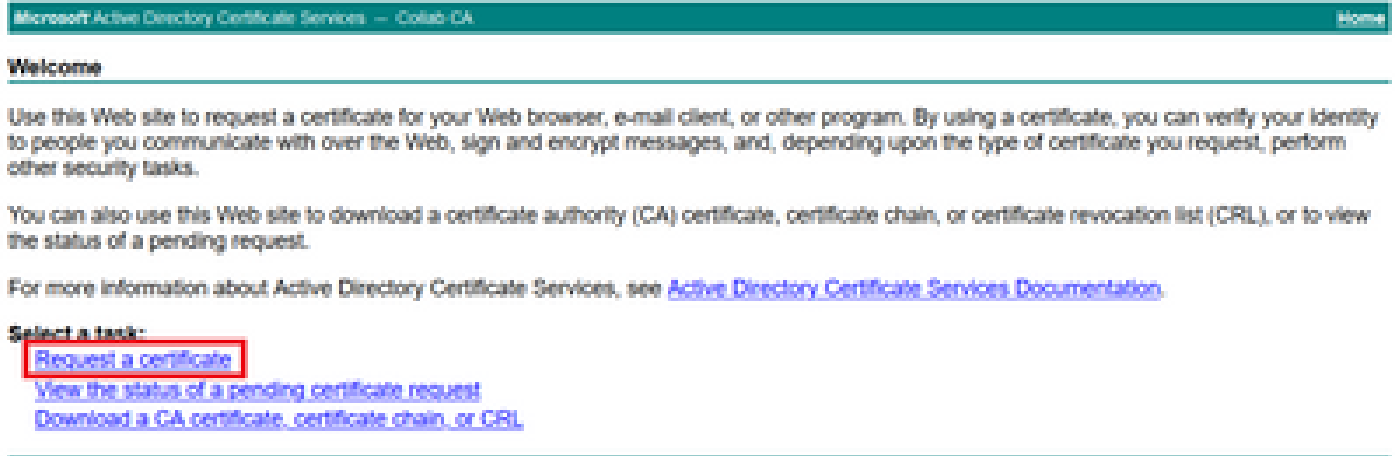
PKCS10 Request: [
Version: 0
Subject: CN=115PUB-ms.maucabal.lab, OU=disco, O=disco, L=disco, ST=disco, C=MX
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)
  Key value:
3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d
cabcb144fd5f1538efe514fd8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4fo2237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
  Requested Extensions [
          
```

Delete
Download CSR

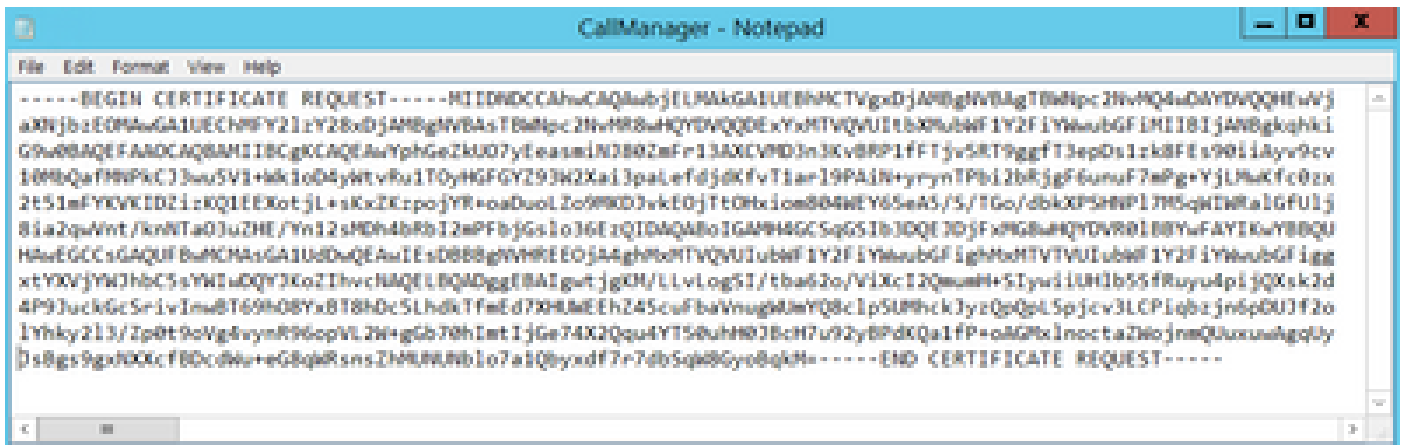
手順 6 : ブラウザでURLに移動し、ドメインコントローラ管理者のクレデンシャル (https://<yourWindowsServerIP>/certsrv/)を入力します。



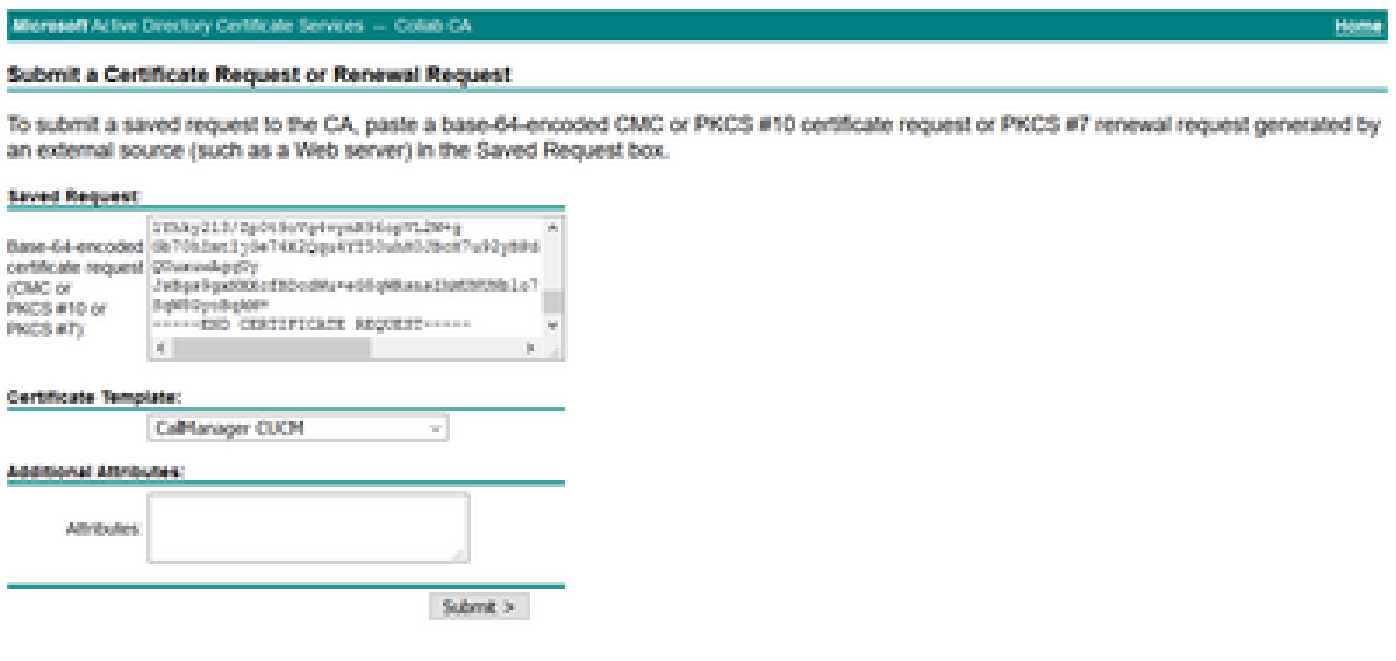
手順 7 : 図に示すように、Request a certificate > advanced certificate requestの順に移動します。



ステップ 8 : CSRファイルを開き、すべての内容をコピーします。



ステップ 9 : Base-64-encoded certificate requestフィールドにCSRを貼り付けます。図に示すように、Certificate Templateで正しいテンプレートを選択し、Submitを選択します。



ステップ 10 : 最後に、Base 64 encodedとDownload certificate chainを選択します。これで、生成されたファイルをCUCMにアップロードできます。

### Certificate issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

---

## 確認

検証手順は、実際には設定プロセスの一部です。

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 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。