

# Créer des modèles de certificats AC Windows pour CUCM

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Modèle Callmanager / Tomcat / TVS](#)

[Modèle IPsec](#)

[Modèle CAPF](#)

[Générer une demande de signature de certificat](#)

[Vérifier](#)

[Dépannage](#)

## Introduction

Ce document décrit une procédure étape par étape afin de créer des modèles de certificats sur les autorités de certification Windows Server, qui sont conformes aux exigences d'extension X.509 pour chaque type de certificat Cisco Unified Communications Manager (CUCM).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM version 11.5(1) ou ultérieure
- Une connaissance de base de l'administration de Windows Server est également recommandée

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Les informations contenues dans ce document sont basées sur la version 11.5(1) ou ultérieure de CUCM.
- Microsoft Windows Server 2012 R2 avec services AC installés.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Il existe cinq types de certificats qui peuvent être signés par une autorité de certification externe :

Certificat	Utilisation	Services affectés
CallManager	Présenté lors de l'enregistrement sécurisé des périphériques, peut signer les fichiers CTL (Certificate Trust List)/ITL (Internal Trust List), utilisés pour les interactions sécurisées avec d'autres serveurs tels que les liaisons SIP (Session Initiation Protocol) sécurisées.	<ul style="list-style-type: none"> <li>·Cisco Call Manager</li> <li>·Cisco CTI Manager</li> <li>·Cisco TFTP</li> </ul>
tomcat	Présenté pour les interactions HTTPS (Secure Hypertext Transfer Protocol).	<ul style="list-style-type: none"> <li>·Cisco Tomcat</li> <li>·Authentification unique (SSO)</li> <li>·Extension Mobility</li> <li>·Répertoire d'entreprise</li> </ul>
ipsec	Utilisé pour la génération de fichiers de sauvegarde, ainsi que pour l'interaction IPsec (IP Security) avec le protocole MGCP (Media Gateway Control Protocol) ou les passerelles H323.	<ul style="list-style-type: none"> <li>·Cisco DRF Master</li> <li>·Cisco DRF Local</li> </ul>
CAPF	Utilisé pour générer des certificats LSC (Locally Significant Certificates) pour les téléphones.	<ul style="list-style-type: none"> <li>·Fonction Proxy Cisco Certificate Authority</li> </ul>
TVS	Utilisé pour créer une connexion au service de vérification de la confiance (TVS), lorsque les téléphones ne sont pas en mesure d'authentifier un certificat inconnu.	<ul style="list-style-type: none"> <li>·Service de vérification Cisco Trust</li> </ul>

Chacun de ces certificats a des exigences d'extension X.509 qui doivent être définies, sinon, vous pouvez rencontrer des comportements incorrects sur l'un des services mentionnés ci-dessus :

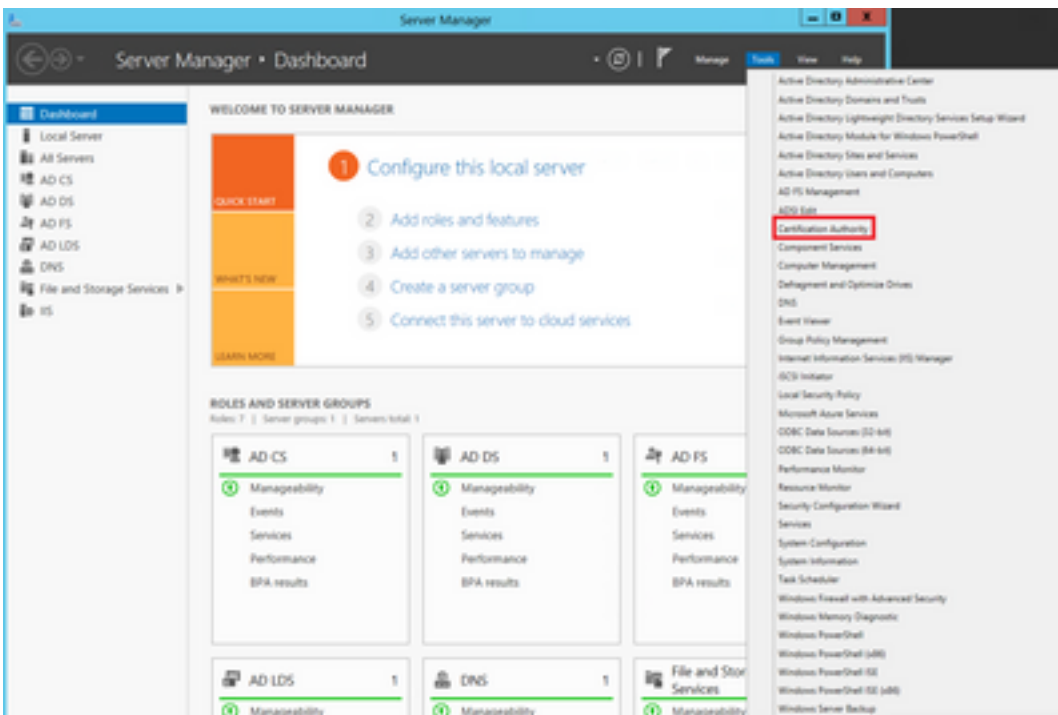
Certificat	Utilisation de la clé X.509	Utilisation de la clé étendue X.509
CallManager	<ul style="list-style-type: none"> <li>·Signature numérique</li> <li>·Chiffrement clé</li> <li>·Chiffrement des données</li> </ul>	<ul style="list-style-type: none"> <li>·Authentification du serveur Web</li> <li>·Authentification du client Web</li> </ul>
tomcat	<ul style="list-style-type: none"> <li>·Signature numérique</li> <li>·Chiffrement clé</li> <li>·Chiffrement des données</li> </ul>	<ul style="list-style-type: none"> <li>·Authentification du serveur Web</li> <li>·Authentification du client Web</li> </ul>
ipsec	<ul style="list-style-type: none"> <li>·Signature numérique</li> <li>·Chiffrement clé</li> </ul>	<ul style="list-style-type: none"> <li>·Authentification du serveur Web</li> <li>·Authentification du client Web</li> </ul>

	·Chiffrement des données	·Système final IPsec
CAPF	·Signature numérique ·Signe du certificat ·Chiffrement clé	·Authentification du serveur Web ·Authentification du client Web
TVS	·Signature numérique ·Chiffrement clé ·Chiffrement des données	·Authentification du serveur Web ·Authentification du client Web

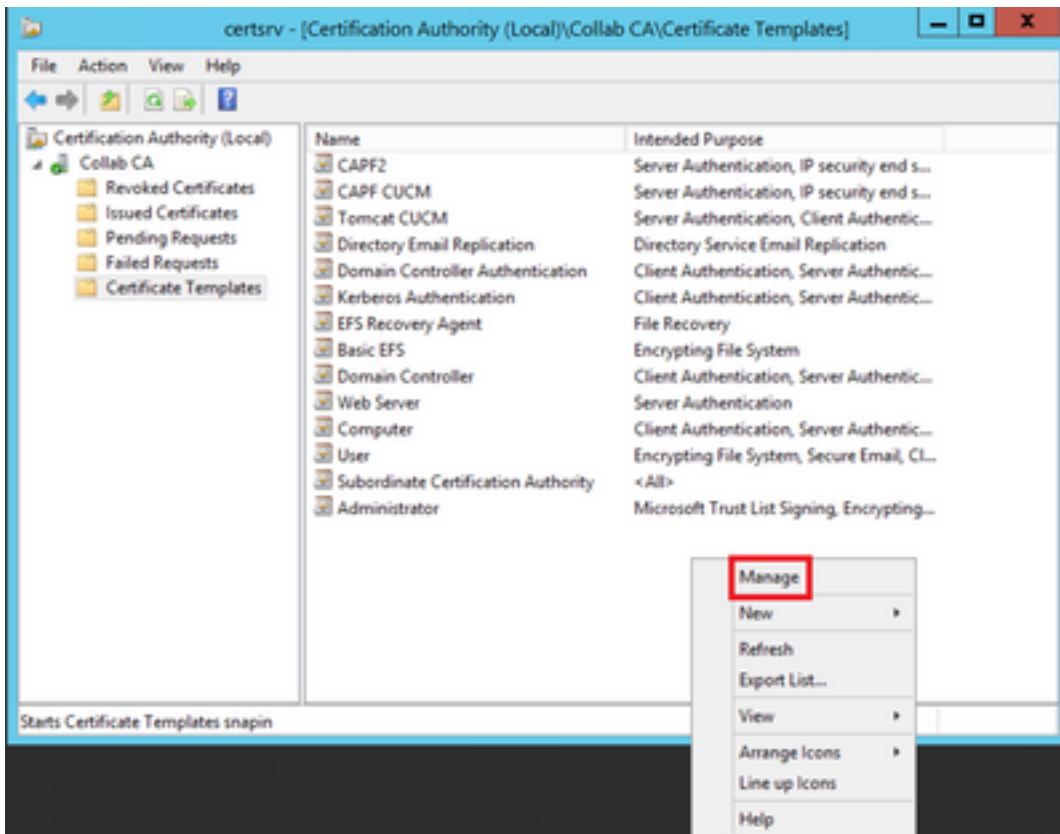
Pour plus d'informations, consultez le [Guide de sécurité de Cisco Unified Communications Manager](#)

## Configurer

Étape 1. Sur le serveur Windows, accédez à **Gestionnaire de serveur > Outils > Autorité de certification**, comme indiqué dans l'image.



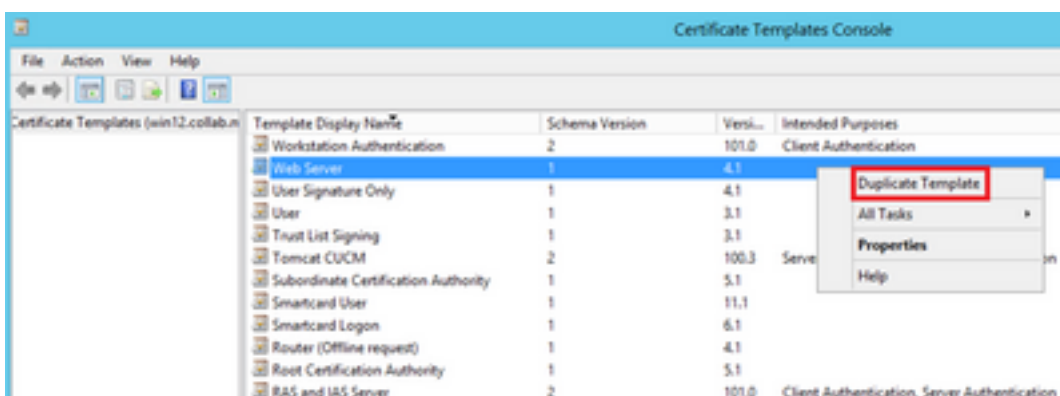
Étape 2. Sélectionnez votre autorité de certification, puis accédez à **Modèles de certificat**, cliquez avec le bouton droit sur la liste et sélectionnez **Gérer**, comme illustré dans l'image.



## Modèle Callmanager / Tomcat / TVS

Les images suivantes affichent uniquement la création du modèle CallManager, mais les mêmes étapes peuvent être suivies pour créer les modèles de certificats pour les services Tomcat et TVS. La seule différence est de s'assurer que le nom de service correspondant est utilisé pour chaque nouveau modèle à l'étape 2.

Étape 1. Recherchez le modèle **Web Server**, cliquez dessus avec le bouton droit et sélectionnez **Duplicate Template**, comme illustré dans l'image.



Étape 2. Sous **Général**, vous pouvez modifier le nom, le nom d'affichage, la validité, etc. du modèle de certificat.

Properties of New Template X

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

Template display name:

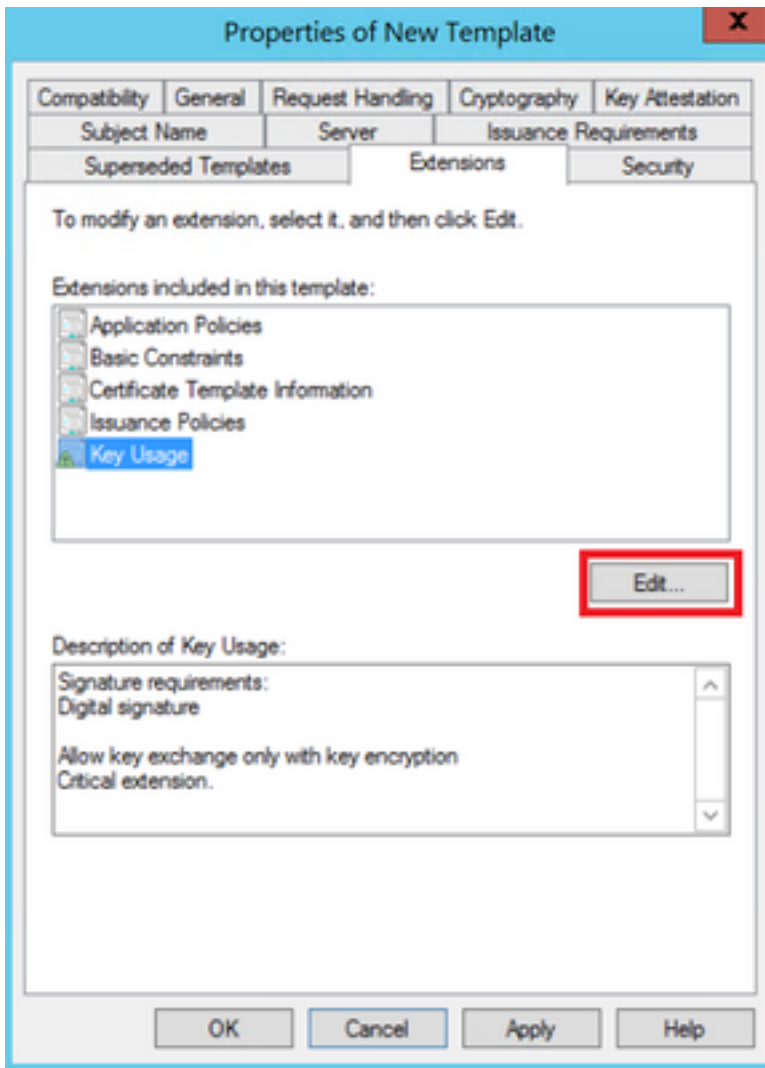
Template name:

Validity period:  years   
Renewal period:  weeks

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

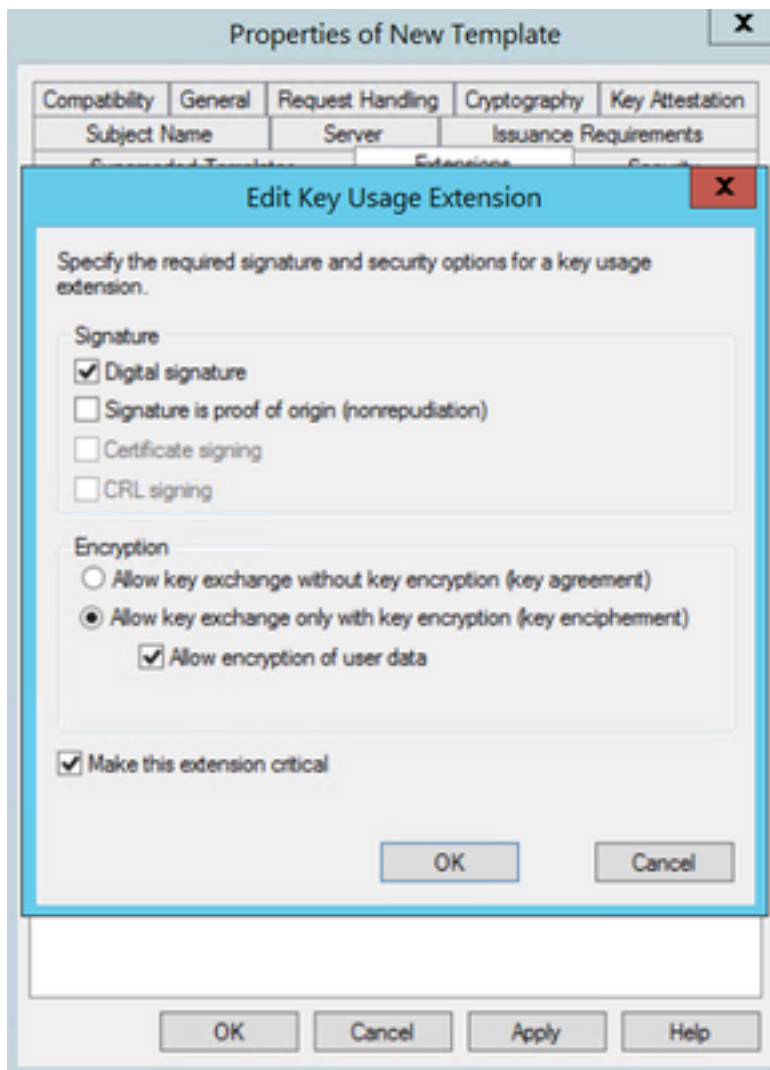
OK Cancel Apply Help

Étape 3. Accédez à **Extensions > Key Usage > Edit**, comme indiqué dans l'image.



Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

- **Signature numérique**
- **Autoriser l'échange de clés uniquement avec le chiffrement de clés (chiffrement de clés)**
- **Autoriser le chiffrement des données utilisateur**



Étape 5. Accédez à **Extensions** > **Application Politiques** > **Edit** > **Add**, comme indiqué dans l'image.

## 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

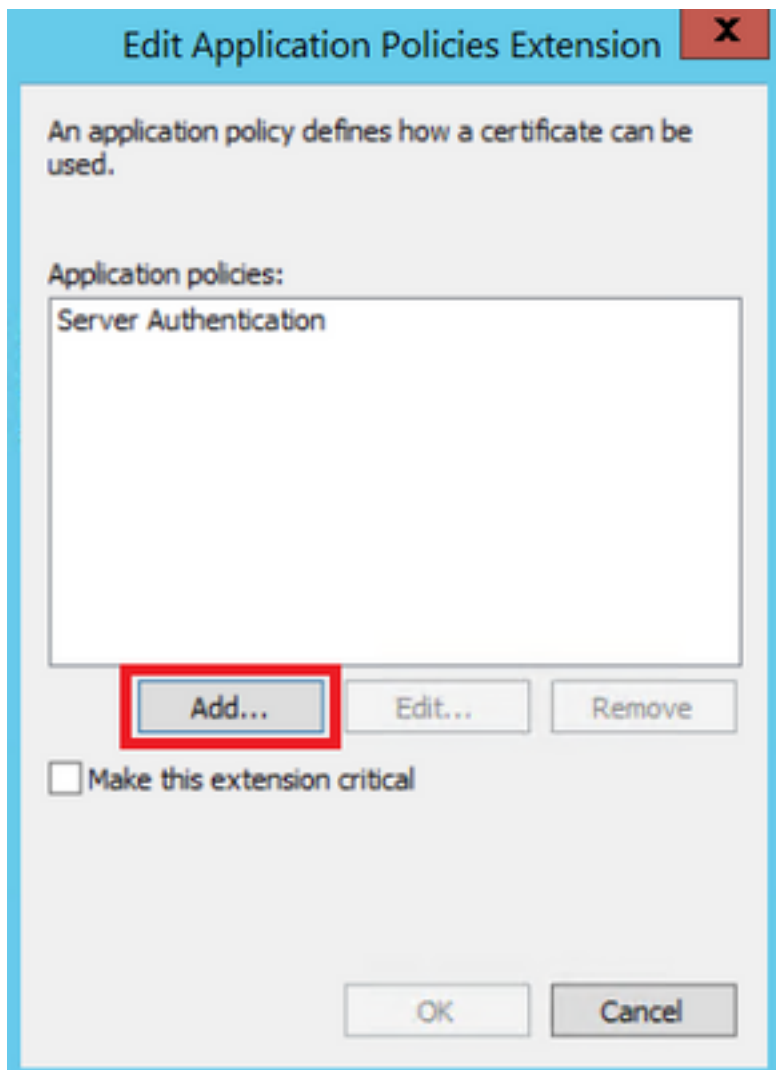
OK

Cancel

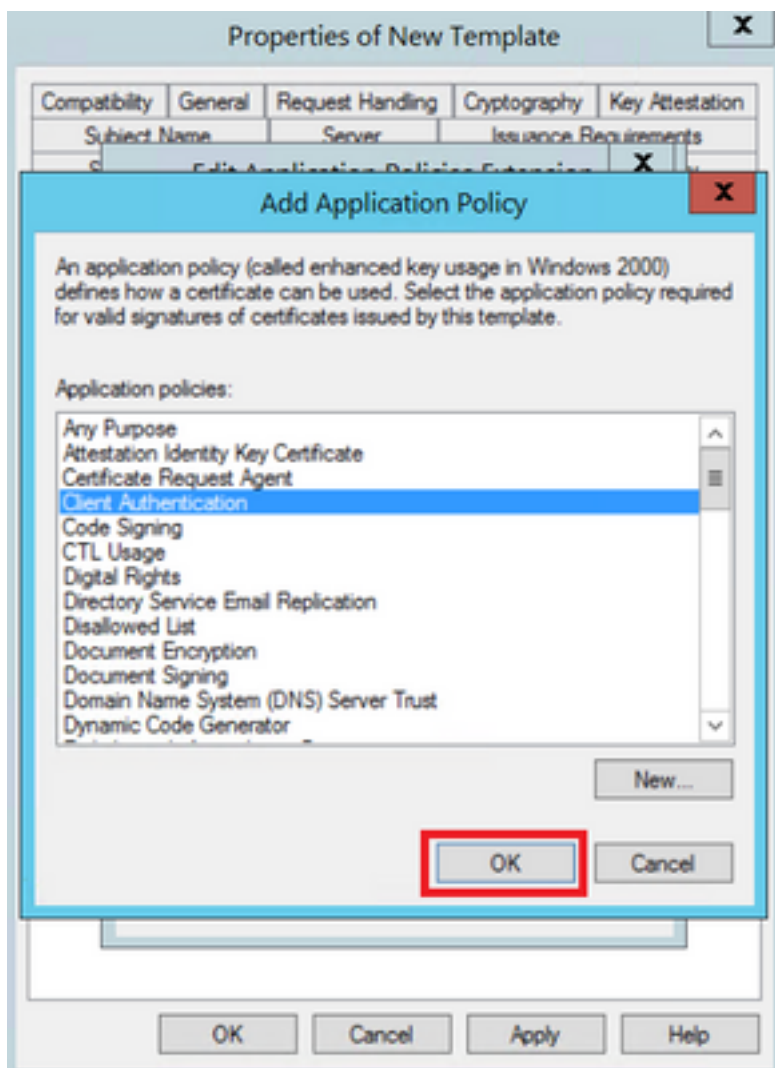
Apply

Help

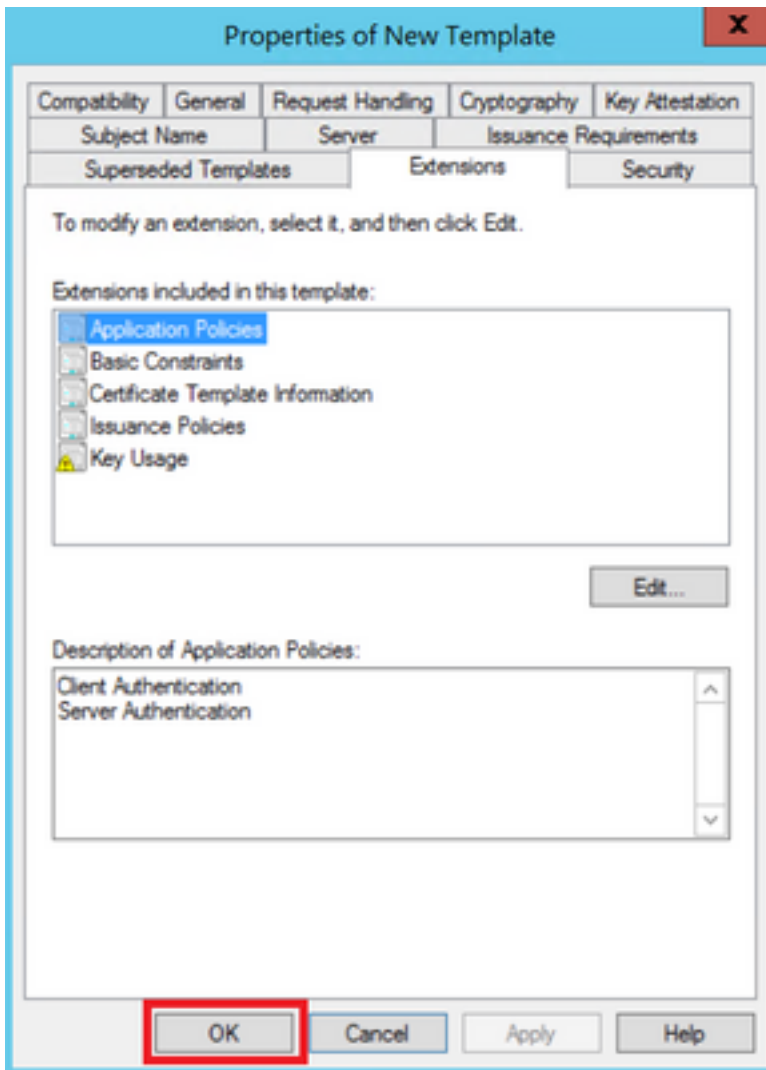




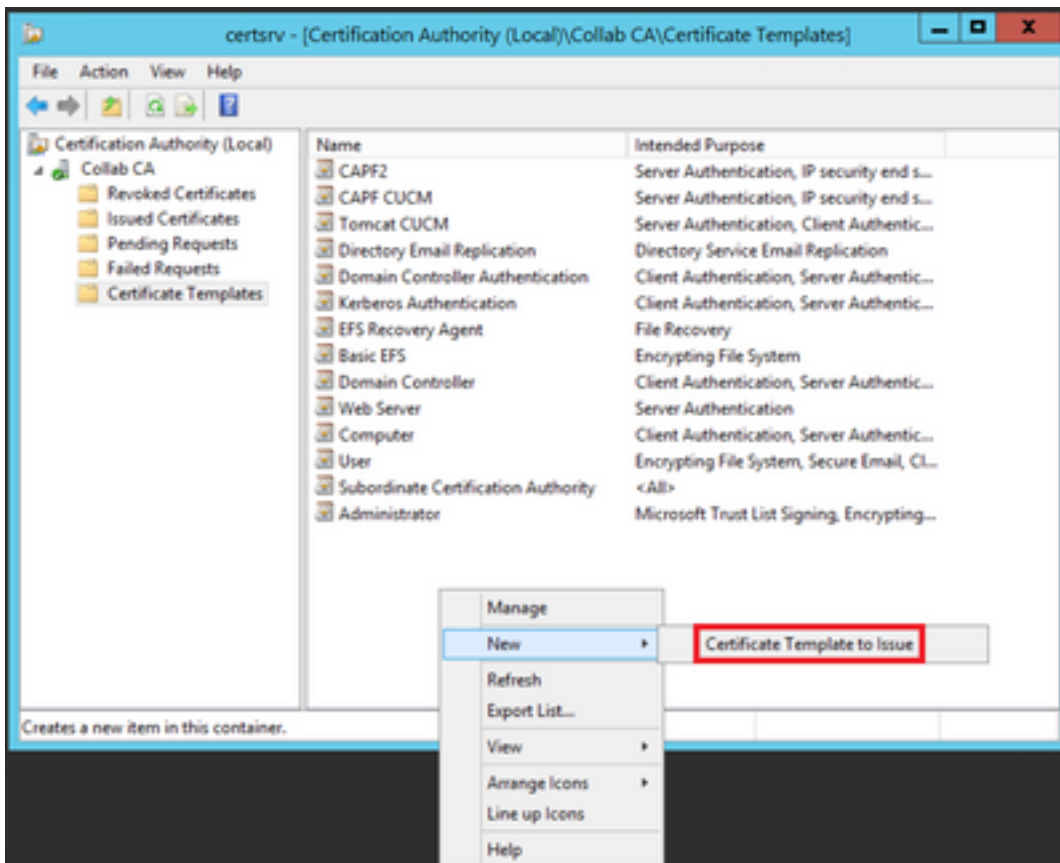
Étape 6. Recherchez **Client Authentication**, sélectionnez-le et sélectionnez **OK** sur cette fenêtre et la précédente, comme illustré dans l'image.



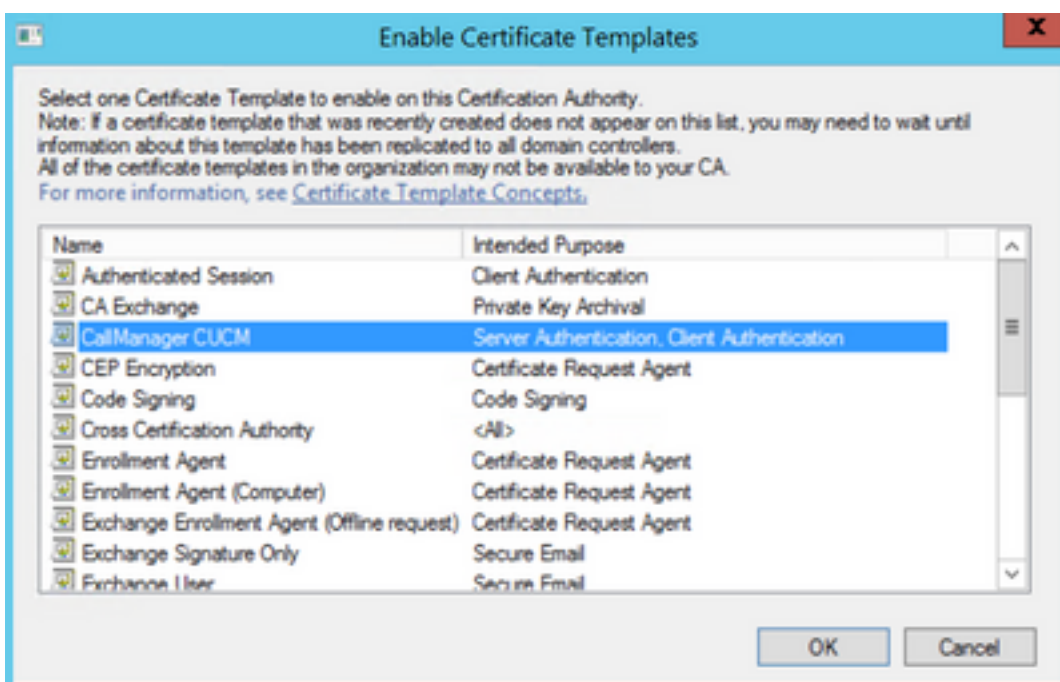
Étape 7. Retournez sur le modèle, sélectionnez **Apply**, puis **OK**.



Étape 8. Fermez la fenêtre **Certificate Template Console** et, de retour dans la toute première fenêtre, accédez à **New > Certificate Template to Issue**, comme indiqué dans l'image.



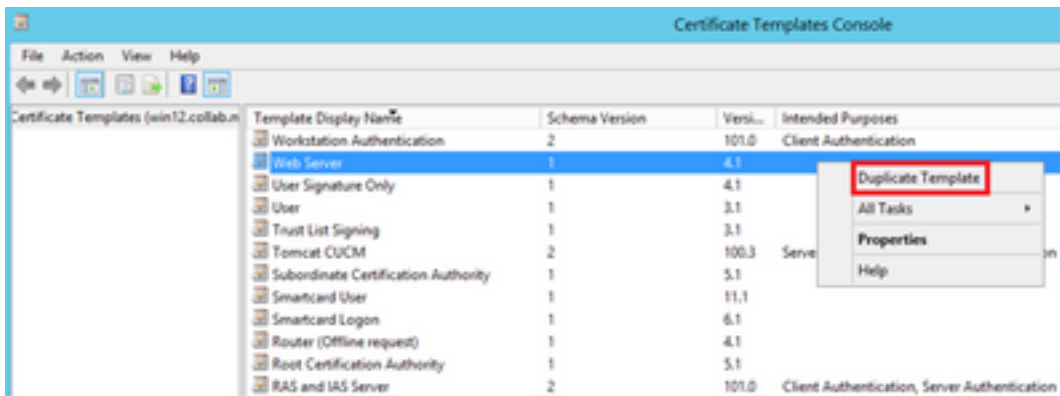
Étape 9. Sélectionnez le nouveau modèle **CallManager CUCM** et cliquez sur **OK**, comme illustré dans l'image.



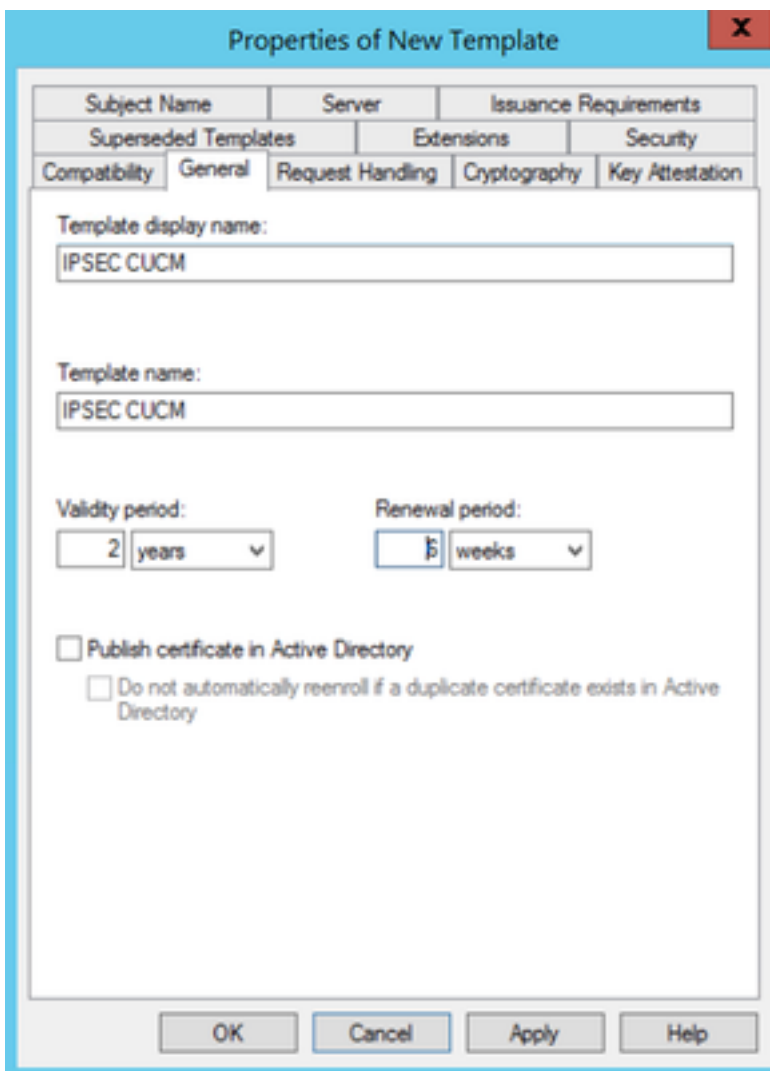
Étape 10. Répétez toutes les étapes précédentes pour créer des modèles de certificats pour les services Tomcat et TVS, le cas échéant.

## Modèle IPsec

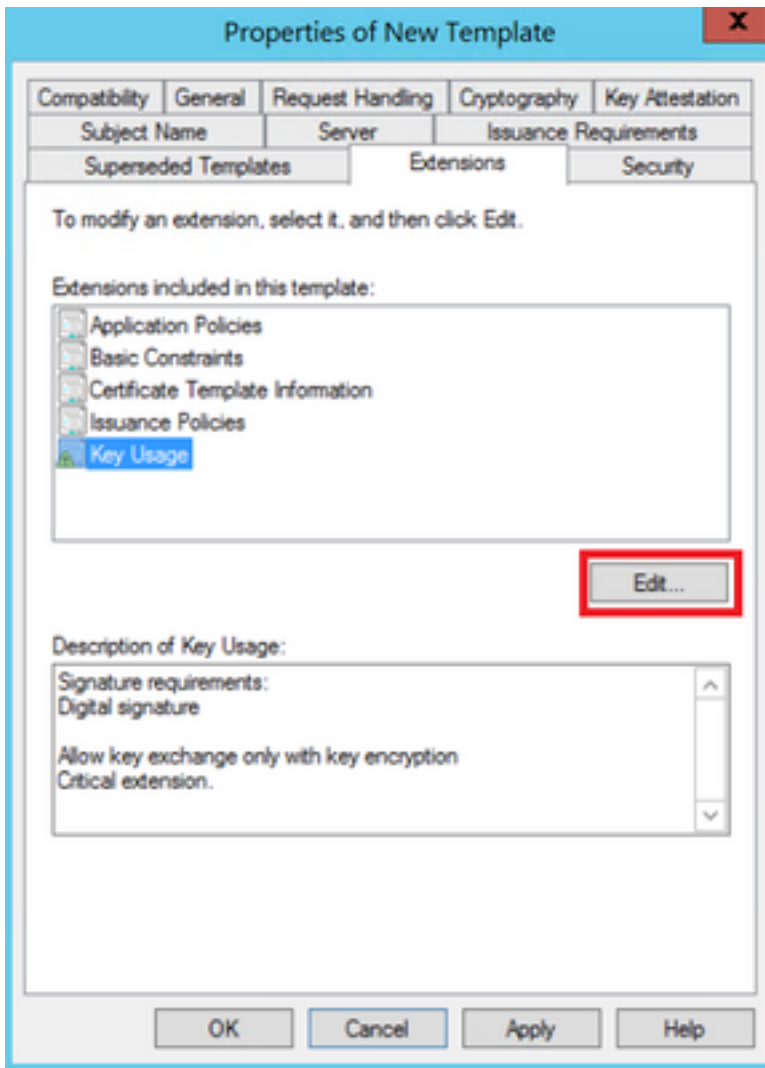
Étape 1. Recherchez le modèle **Web Server**, cliquez dessus avec le bouton droit et sélectionnez **Duplicate Template**, comme illustré dans l'image.



Étape 2. Sous **Général**, vous pouvez modifier le nom, le nom d'affichage, la validité, etc. du modèle de certificat.

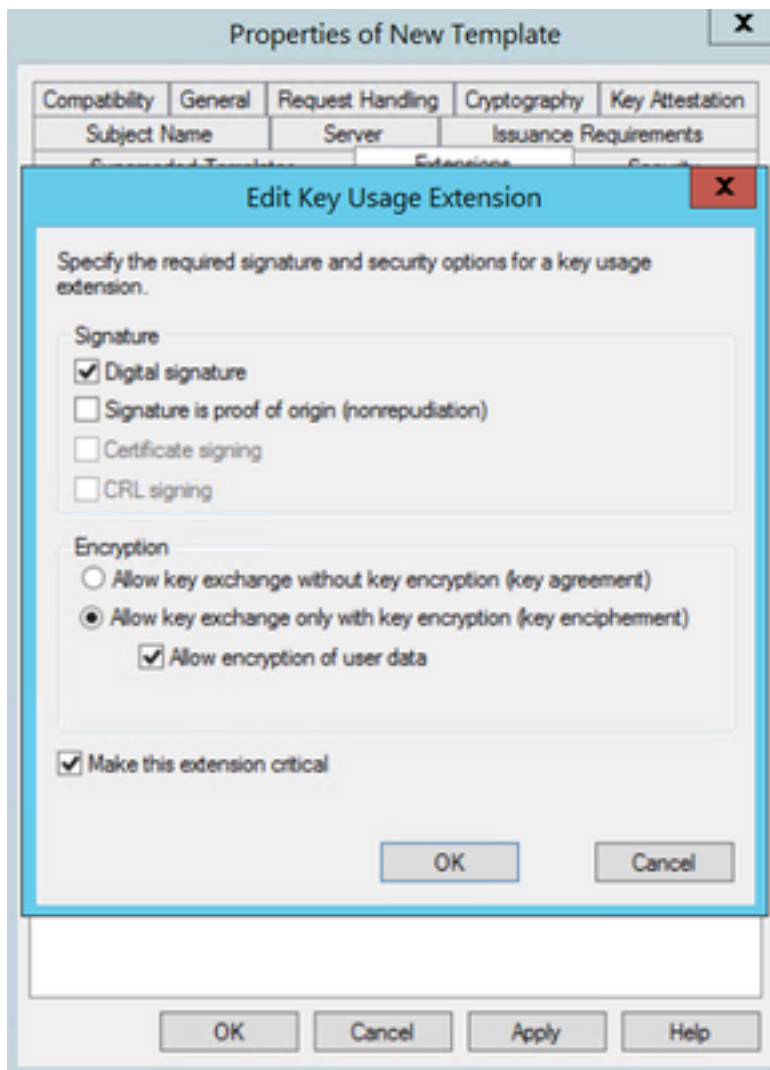


Étape 3. Accédez à **Extensions > Key Usage > Edit**, comme indiqué dans l'image.



Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

- **Signature numérique**
- **Autoriser l'échange de clés uniquement avec le chiffrement de clés (chiffrement de clés)**
- **Autoriser le chiffrement des données utilisateur**



Étape 5. Accédez à **Extensions** > **Application Politiques** > **Edit** > **Add**, comme indiqué dans l'image.

## 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

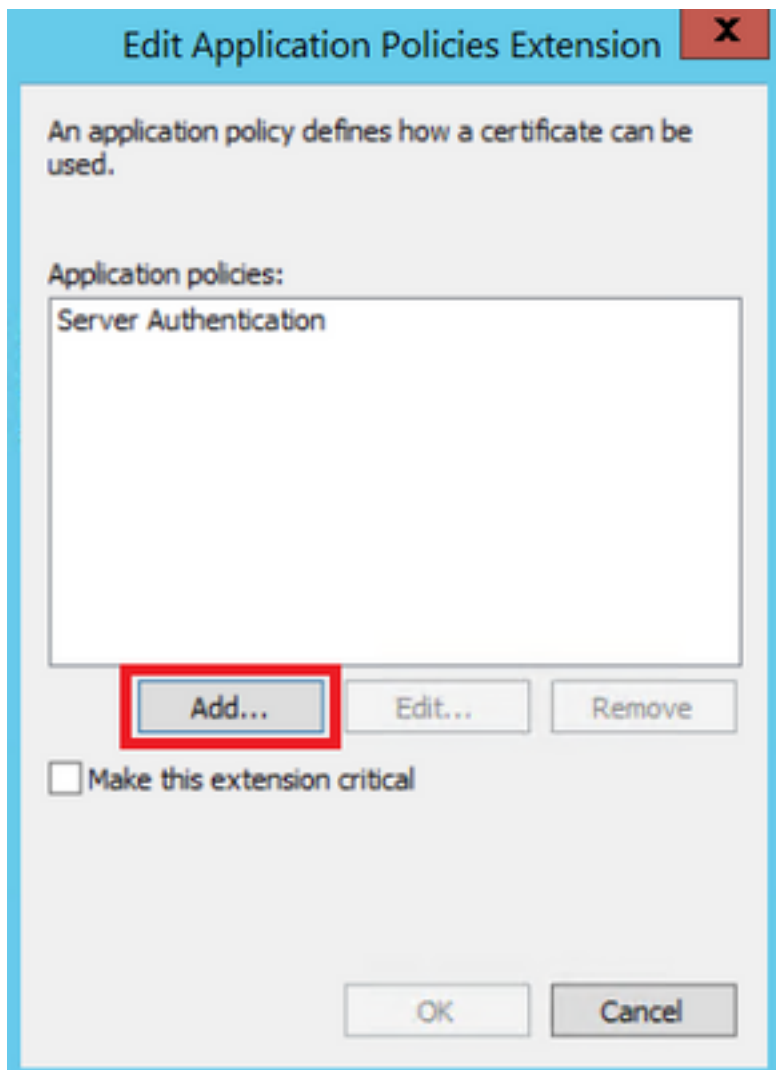
OK

Cancel

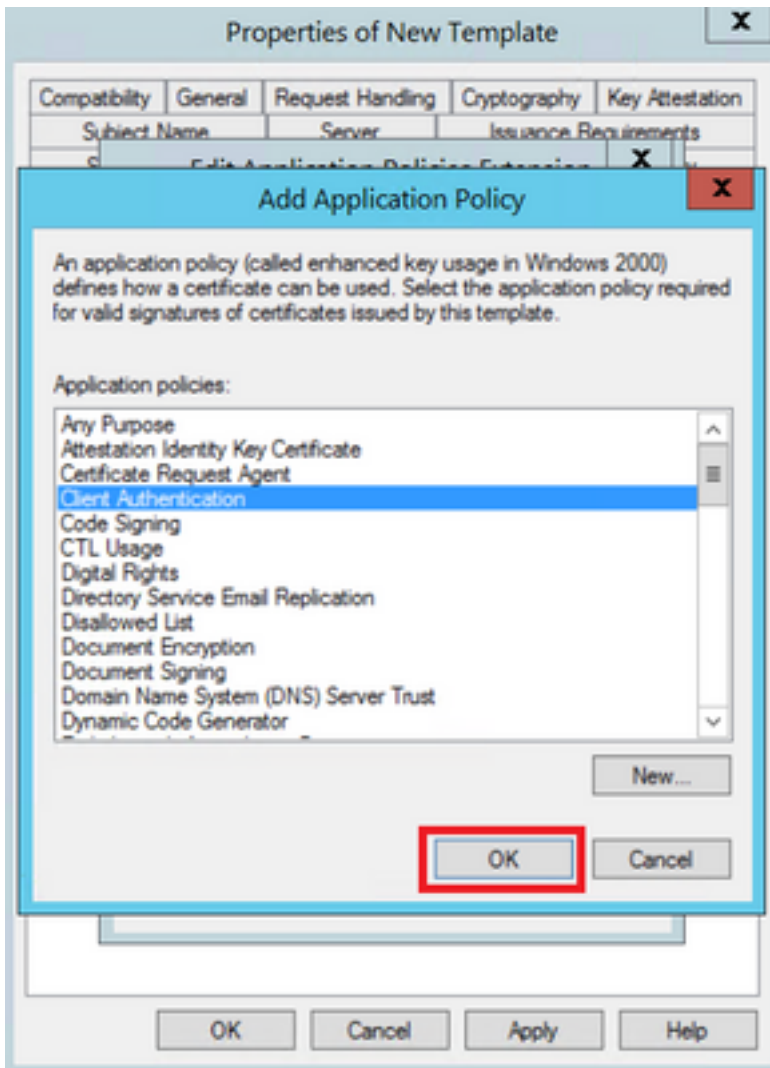
Apply

Help

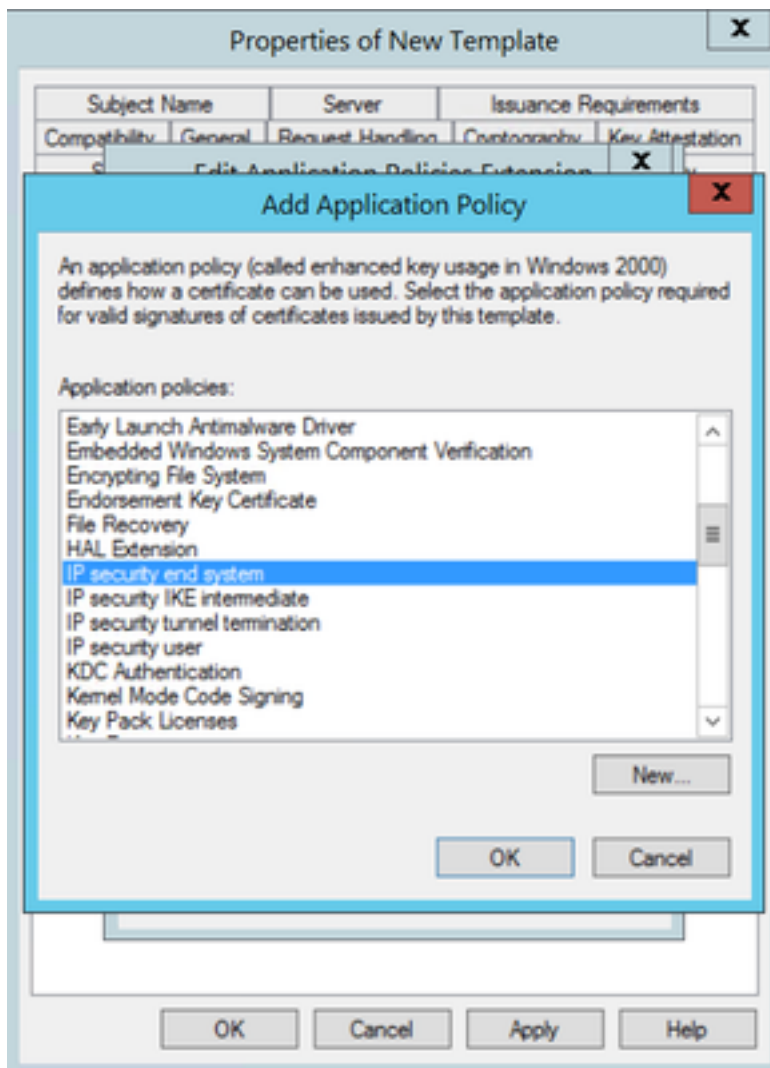




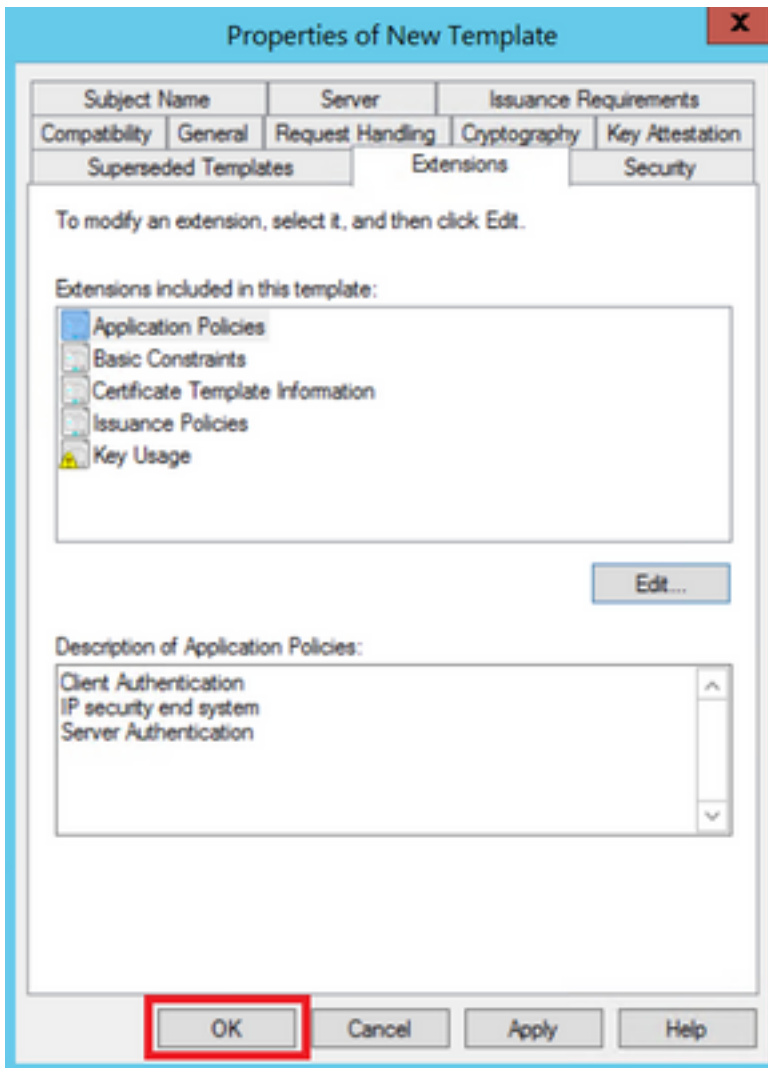
Étape 6. Recherchez **Client Authentication**, sélectionnez-le, puis **OK**, comme indiqué dans l'image.



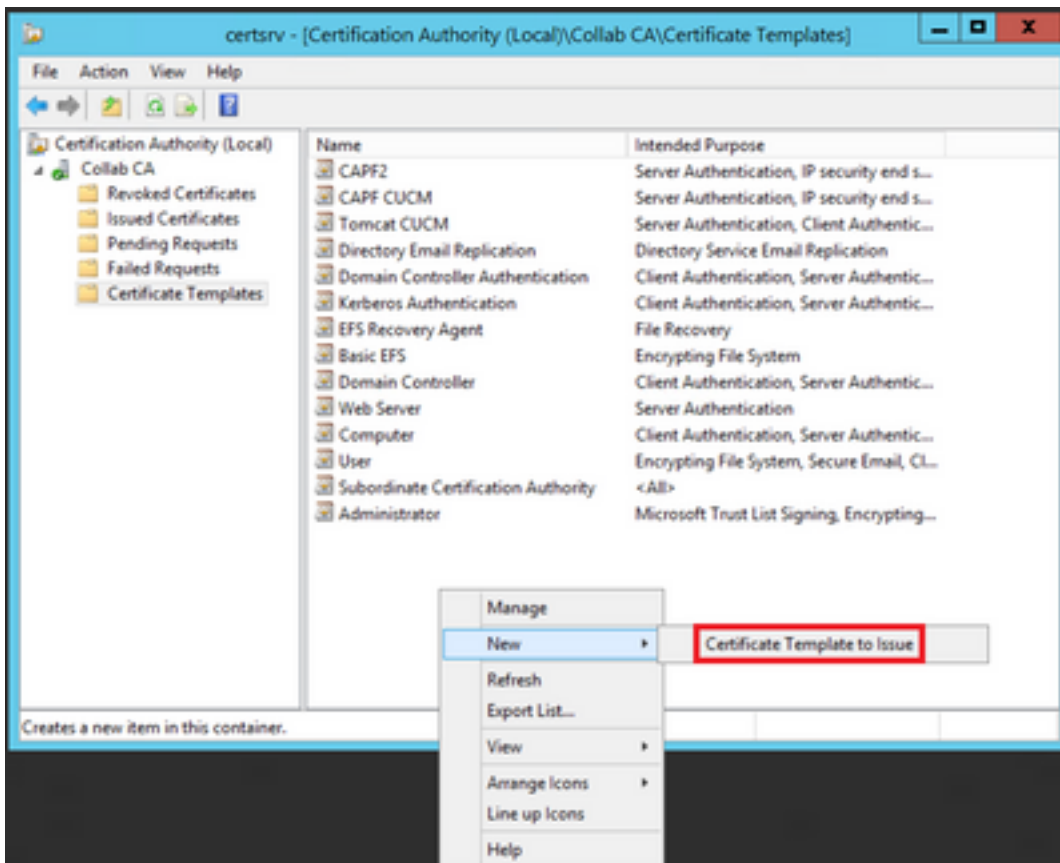
Étape 7. Sélectionnez **Add à nouveau**, recherchez **IP security end system**, sélectionnez-le, puis sélectionnez **OK** sur ce et sur la fenêtre précédente ainsi.



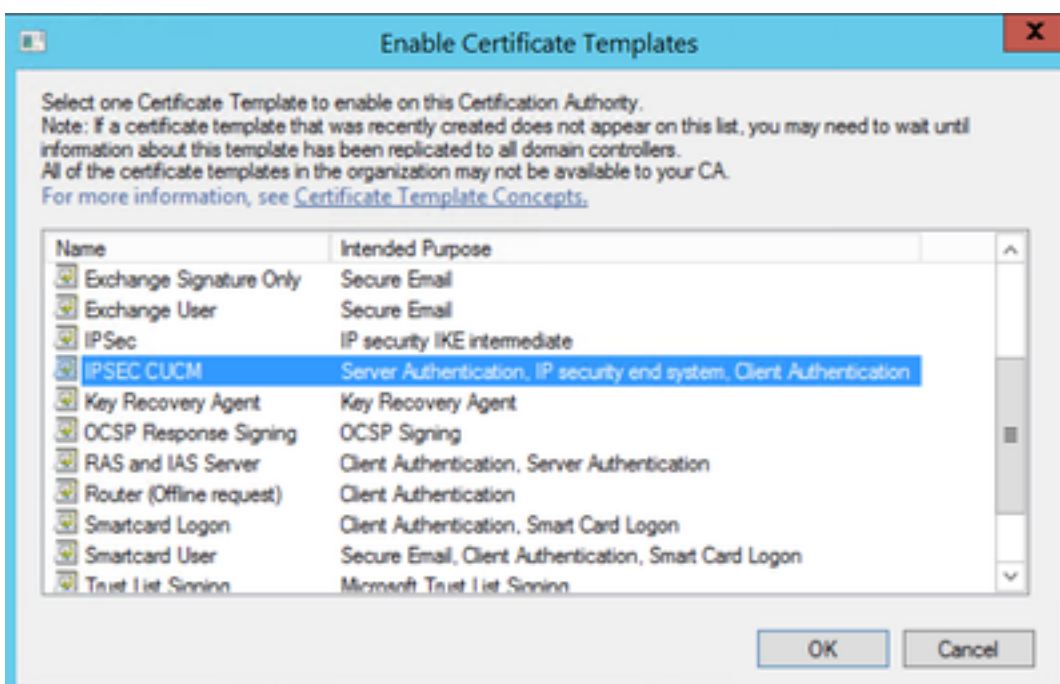
Étape 8. De retour sur le modèle, sélectionnez **Apply** puis **OK**, comme indiqué dans l'image.



Étape 9. Fermez la fenêtre **Certificate Templates Console** et, de retour dans la toute première fenêtre, accédez à **New > Certificate Template to Issue**, comme illustré dans l'image.

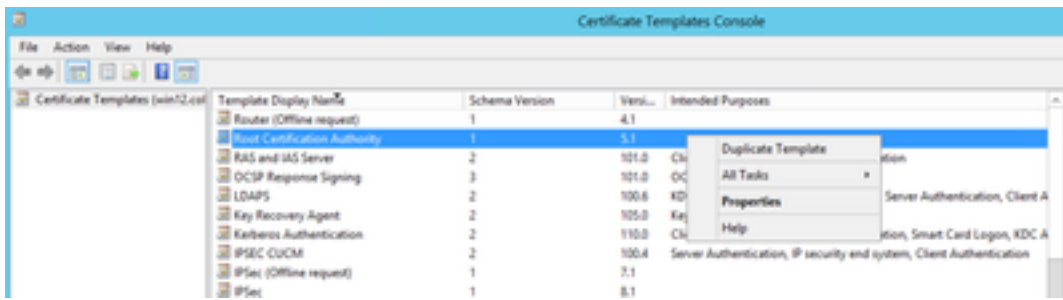


Étape 10. Sélectionnez le nouveau modèle **IPSEC CUCM** et cliquez sur **OK**, comme illustré dans l'image.

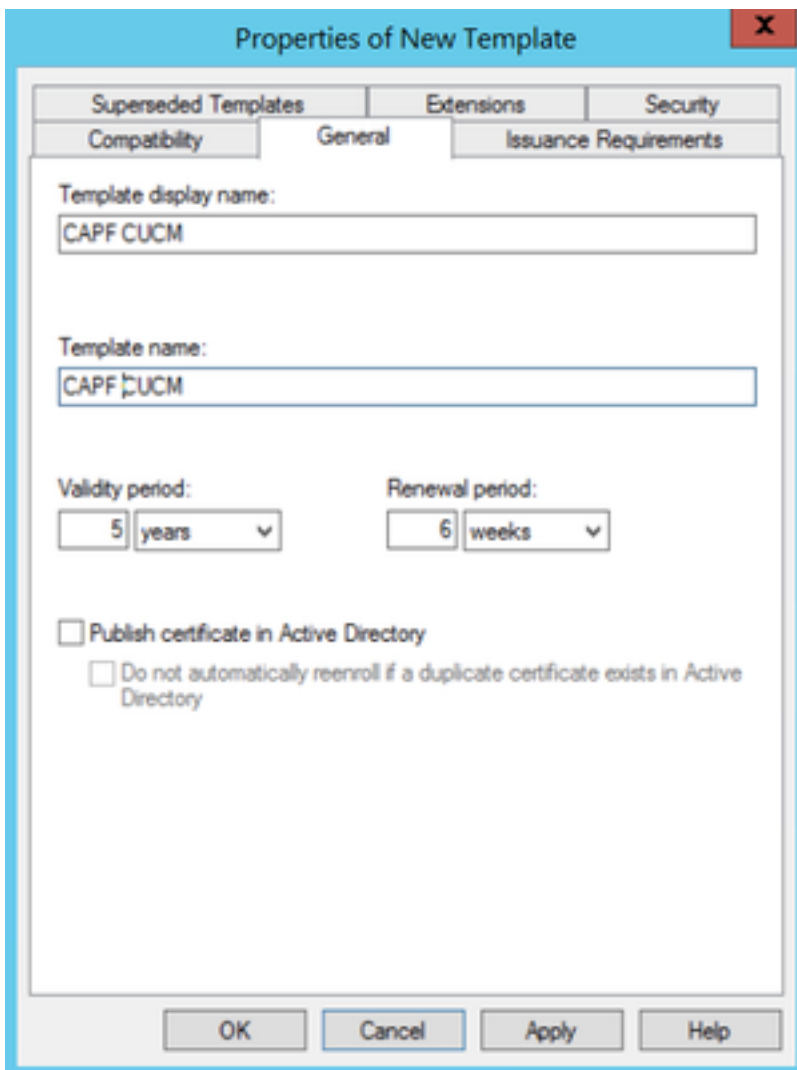


## Modèle CAPF

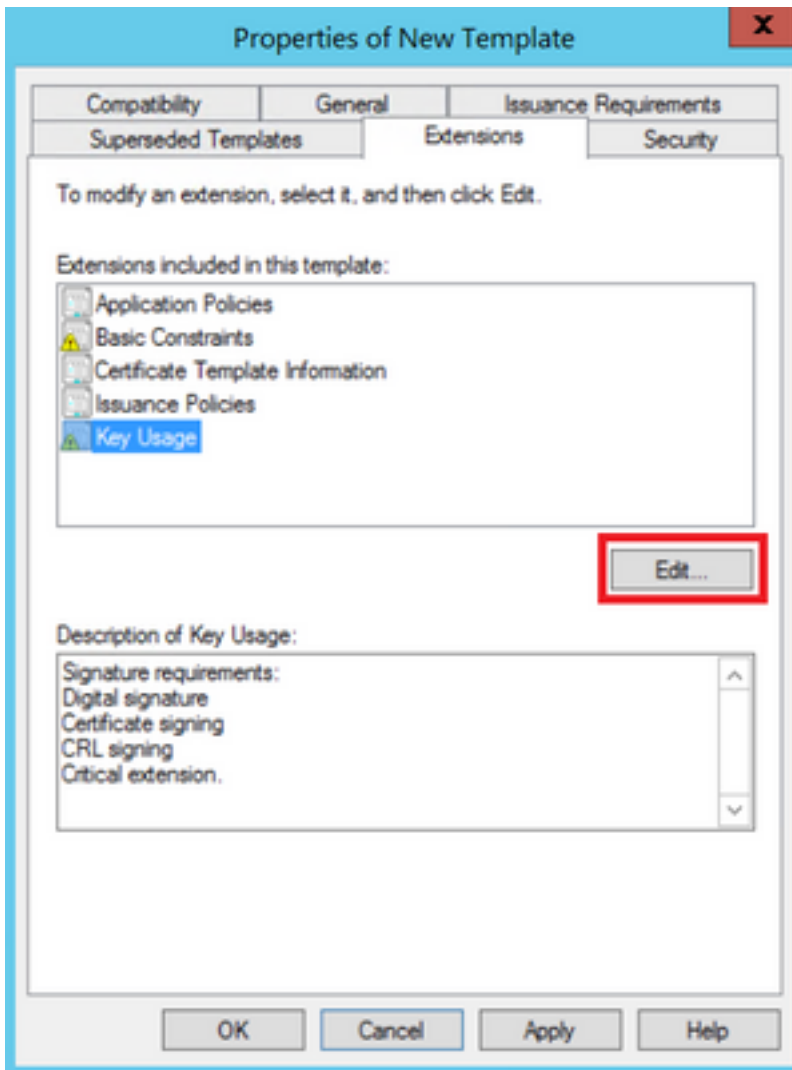
Étape 1. Recherchez le modèle **Root CA** et cliquez dessus avec le bouton droit. Sélectionnez ensuite **Duplicate Template**, comme indiqué dans l'image.



Étape 2. Sous **Général**, vous pouvez modifier le nom, le nom d'affichage, la validité, etc. du modèle de certificat.

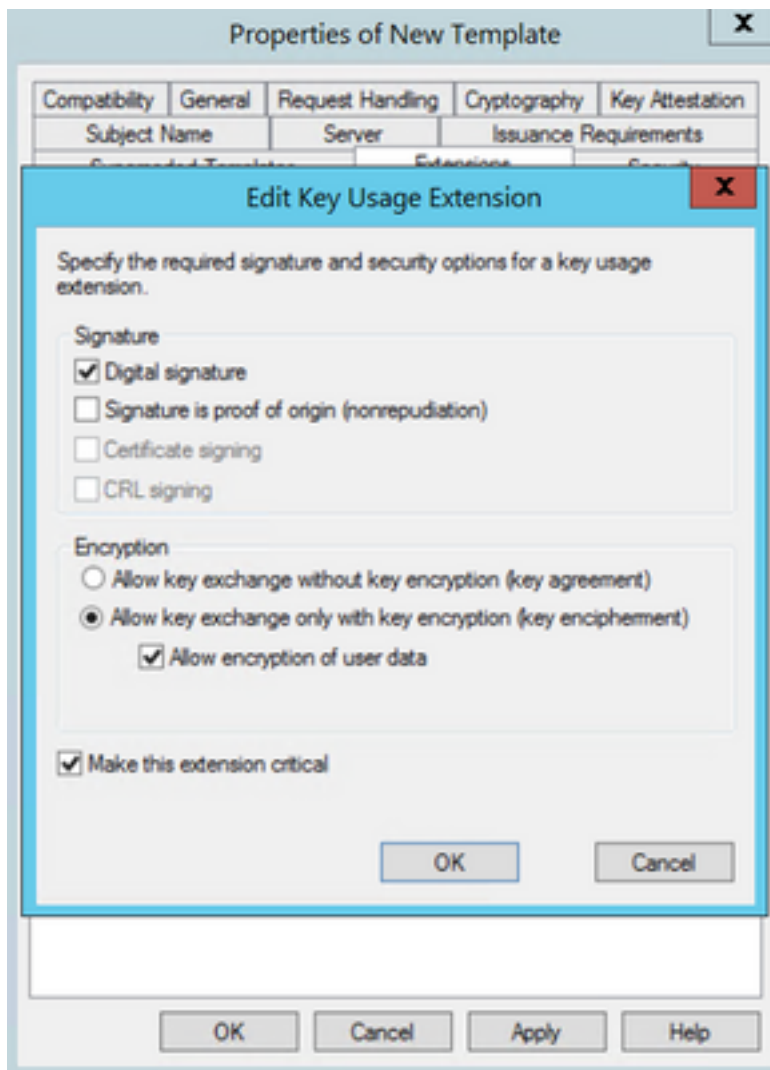


Étape 3. Accédez à **Extensions > Key Usage > Edit**, comme indiqué dans l'image.



Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

- **Signature numérique**
- **Signature de certificat**
- **signature CRL**



Étape 5. Accédez à **Extensions** > **Application Politiques** > **Edit** > **Add**, comme indiqué dans l'image.



## 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:

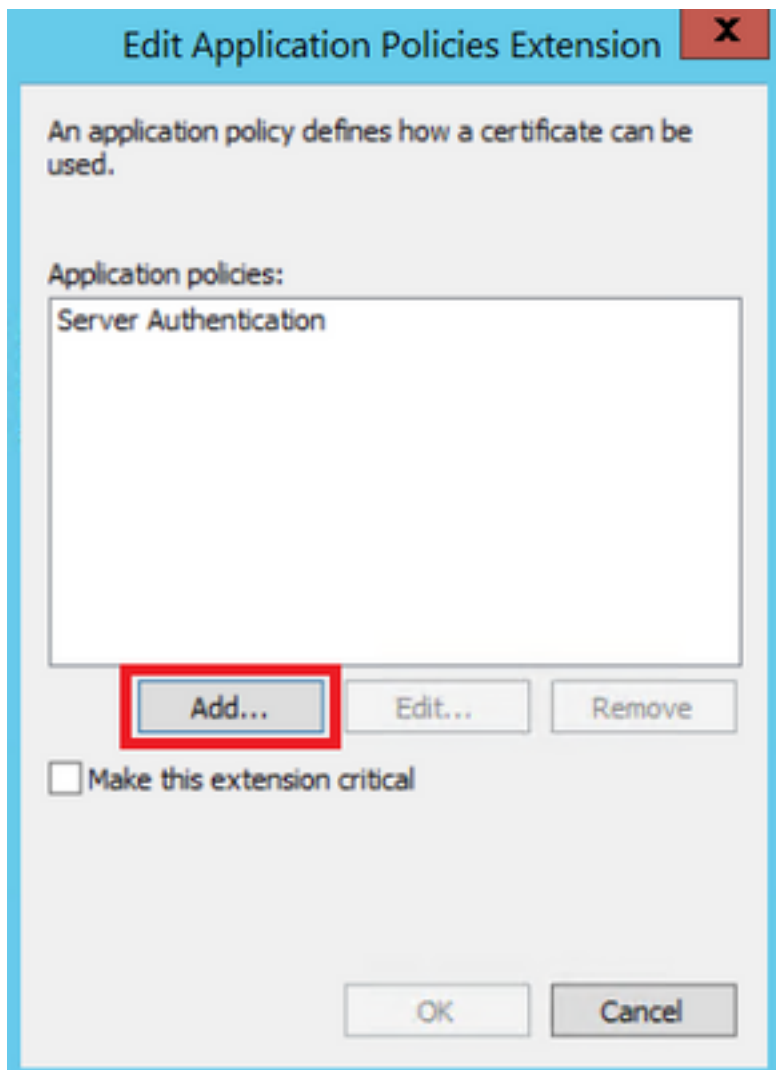
Server Authentication

OK

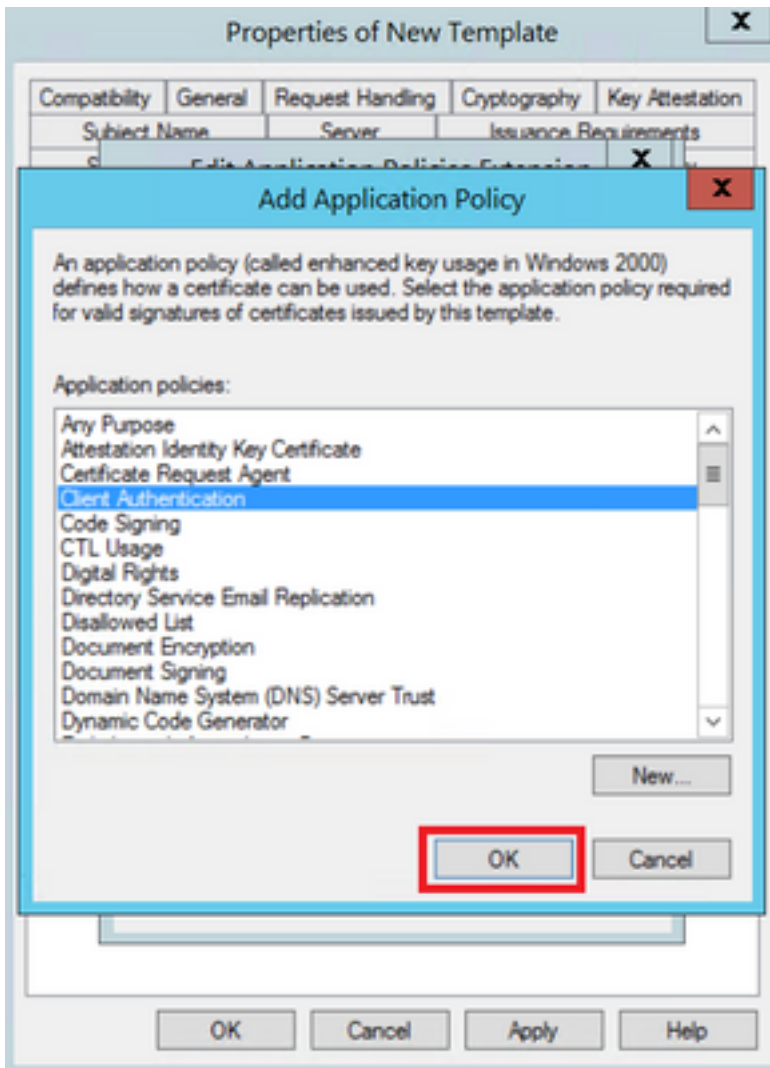
Cancel

Apply

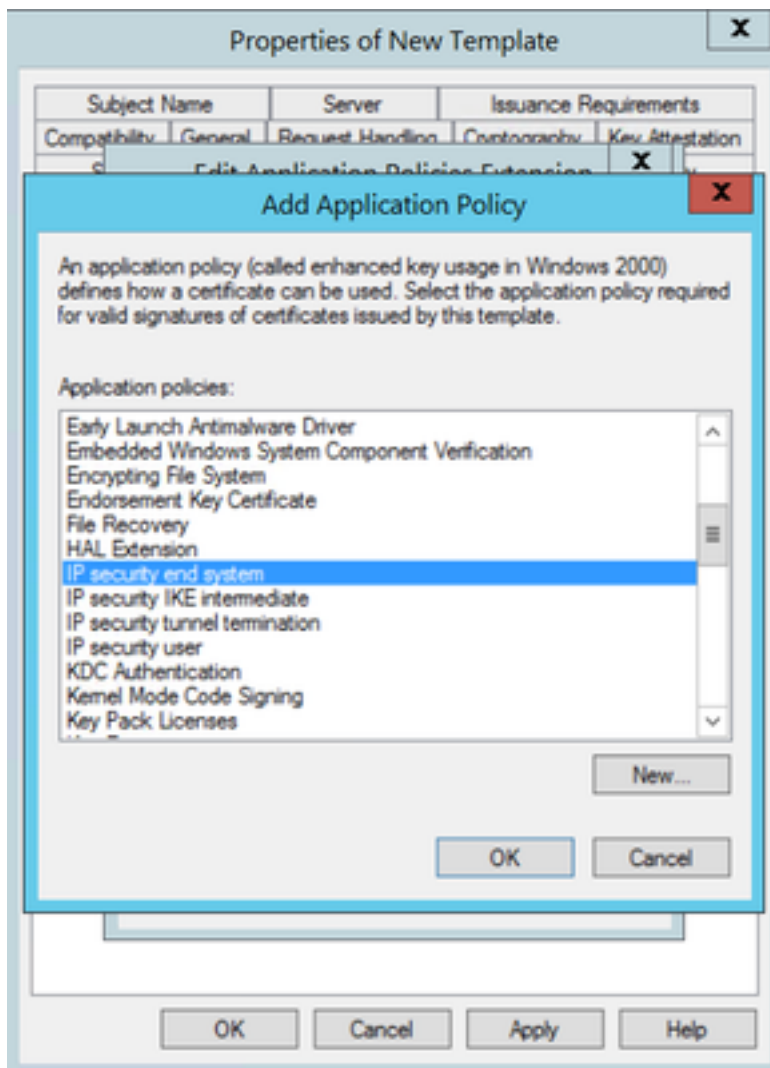
Help



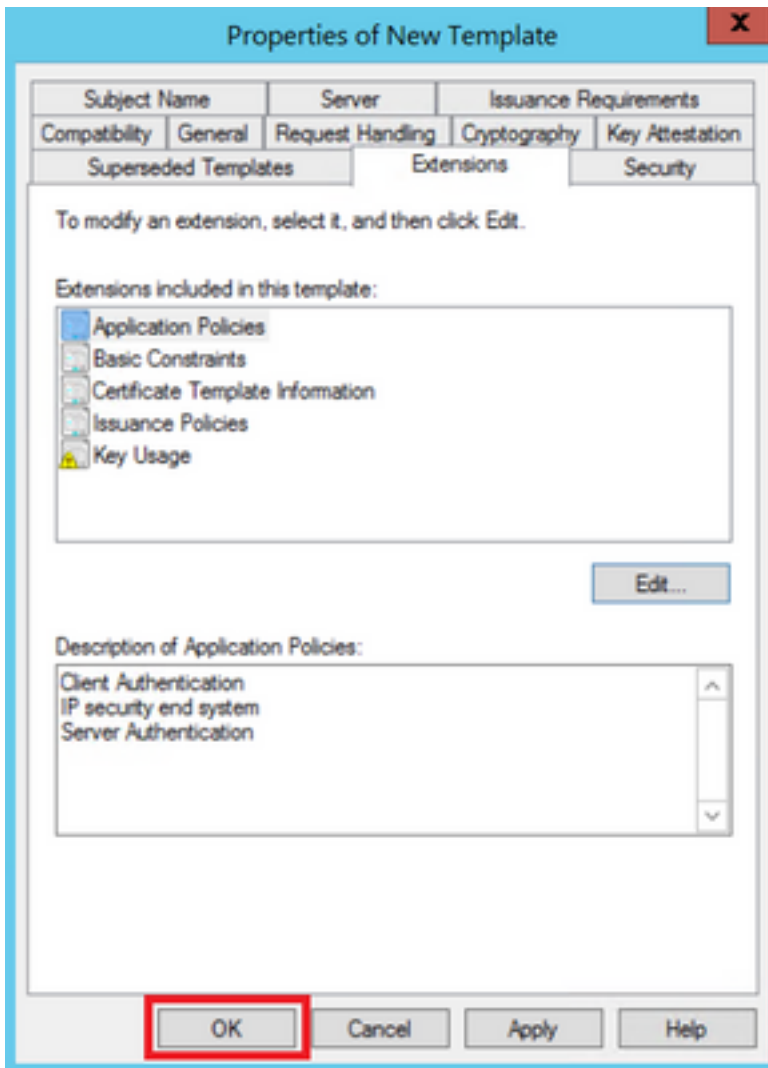
Étape 6. Recherchez **Client Authentication**, sélectionnez-le, puis sélectionnez **OK**, comme indiqué dans l'image.



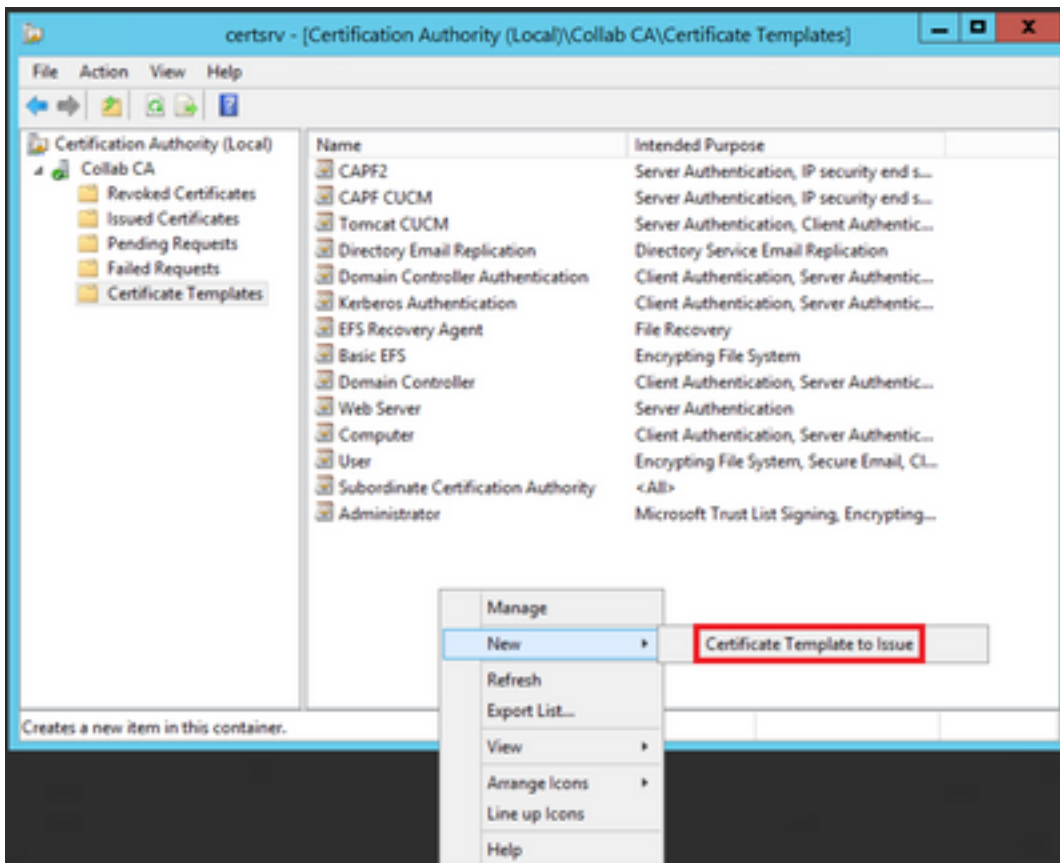
Étape 7. Sélectionnez **Add à nouveau**, recherchez **IP security end system**, sélectionnez-le, puis cliquez sur OK dans cette fenêtre et dans la fenêtre précédente également, comme illustré dans l'image.



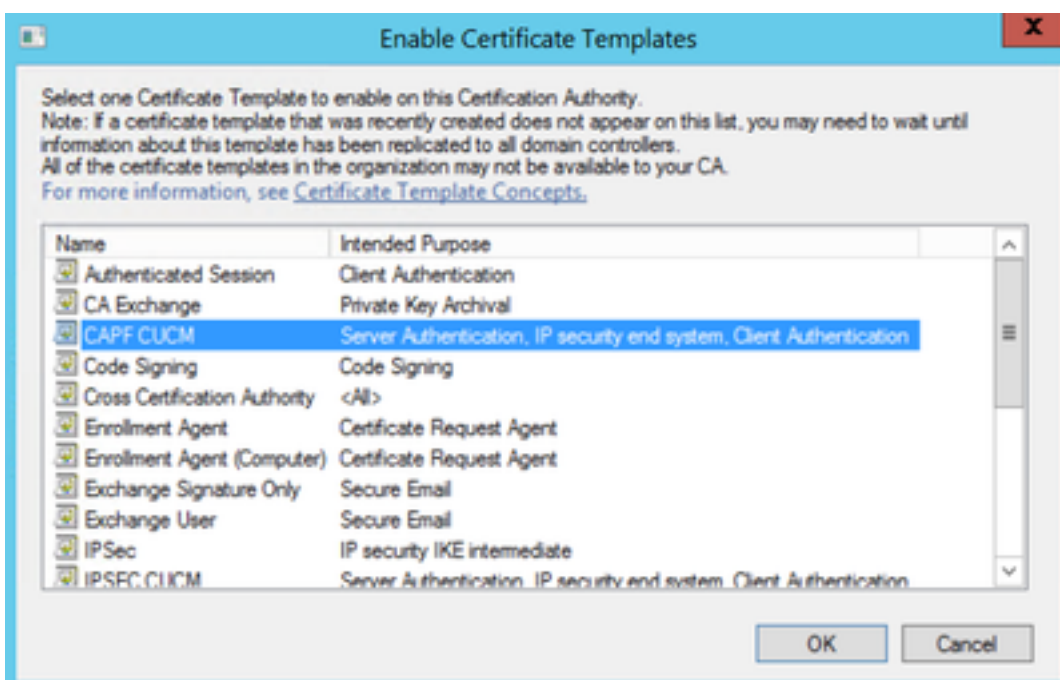
Étape 8. De retour sur le modèle, sélectionnez **Apply** puis **OK**, comme indiqué dans l'image.



Étape 9. Fermez la fenêtre **Certificate Templates Console** et, de retour dans la toute première fenêtre, accédez à **New > Certificate Template to Issue**, comme illustré dans l'image.



Étape 10. Sélectionnez le nouveau modèle **CAPF CUCM** et cliquez sur **OK**, comme illustré dans l'image.



## Générer une demande de signature de certificat

Utilisez cet exemple afin de générer un certificat CallManager avec l'utilisation des modèles nouvellement créés. La même procédure peut être utilisée pour n'importe quel type de certificat. Il vous suffit de sélectionner les types de certificat et de modèle en conséquence :

Étape 1. Sur CUCM, accédez à **OS Administration > Security > Certificate Management > Generate CSR**.

Étape 2. Sélectionnez ces options et sélectionnez **Generate**, comme indiqué dans l'image.

- Objectif du certificat : **CallManager**
- Distribution : **<il peut s'agir d'un seul serveur ou de plusieurs réseaux SAN>**

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

Étape 3. Un message de confirmation est généré, comme illustré dans l'image.

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].

Étape 4. Dans la liste des certificats, recherchez l'entrée avec le type **CSR Only** et sélectionnez-la, comme indiqué dans l'image.

Certificate List

Generate Self signed Upload Certificate/Certificate chain Generate CSR Download CSR

Status

16 records found

Certificate List (11 - 50 of 56) Rows per Page 50

Find Certificate List where Certificate begins with Find Clear Filter

Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
auth	auth2_admin	Self-signed	RSA	115PUB.maucabal.lab	AUTH2_admin	01/27/2018	Self-signed certificate generated by system
CallManager	115PUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(SAN)			
CallManager	115PUB.maucabal.lab	Self-signed	RSA	115PUB.maucabal.lab	115PUB.maucabal.lab	05/30/2023	Self-signed certificate generated by system
CallManager-ECDSA	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	03/04/2023	Self-signed certificate generated by system
CallManager-trust	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	03/04/2023	Trust Certificate

Étape 5. Dans la fenêtre contextuelle, sélectionnez **Download CSR**, et enregistrez le fichier sur votre ordinateur.

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

Delete Download CSR

**Status**  
 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
cab144fd5f1538efe514fd8207d3dde43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
Requested Extensions [
  
```

Delete Download CSR

Étape 6. Dans votre navigateur, accédez à cette URL et entrez vos informations d'identification d'administrateur de contrôleur de domaine : <https://<votreWindowsServerIP>/certsrv/>.

Étape 7. Naviguez jusqu'à **Request a certificate > advanced certificate request**, comme indiqué dans l'image.

Microsoft Active Directory Certificate Services — Collab CA Home

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

---

Microsoft Active Directory Certificate Services — Collab CA Home

**Request a Certificate**

Select the certificate type:

- [User Certificate](#)

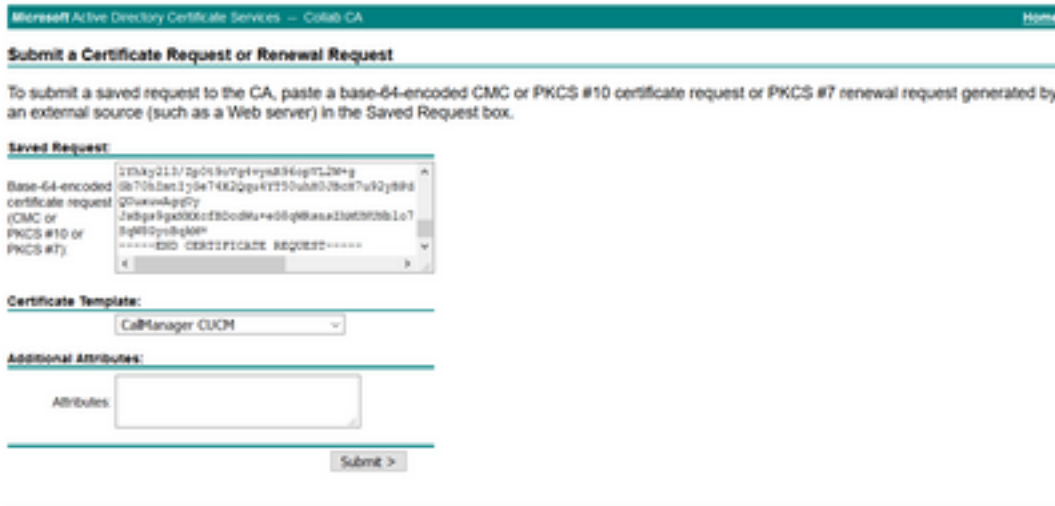
Or, submit an [advanced certificate request](#).

Étape 8. Ouvrez le fichier CSR et copiez tout son contenu :





Étape 9. Collez le CSR dans le champ de demande de certificat codé en base 64. Sous **Modèle de certificat**, sélectionnez le modèle correct et sélectionnez **Envoyer**, comme illustré dans l'image.



Étape 10. Enfin, sélectionnez **Base 64 encoded** et **Download certificate chain**, le fichier généré peut maintenant être téléchargé dans CUCM.



## Vérier

La procédure de vérification fait en fait partie du processus de configuration.

## Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.