Créer des modèles de certificats AC Windows pour CUCM

Table des matières

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.	·Cisco Call Manager ·Cisco CTI Manager ·Cisco TFTP
tomcat	Présenté pour les interactions HTTPS (Secure Hypertext Transfer Protocol).	·Cisco Tomcat ·Authentification unique (SSO) ·Extension Mobility ·Répertoire d'entreprise
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.	·Cisco DRF Master ·Cisco DRF Local
CAPF	Utilisé pour générer des certificats LSC (Locally Significative Certificates) pour les téléphones.	·Fonction Proxy Cisco Certificate Authority
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.	·Service de vérification Cisco Trust

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 :

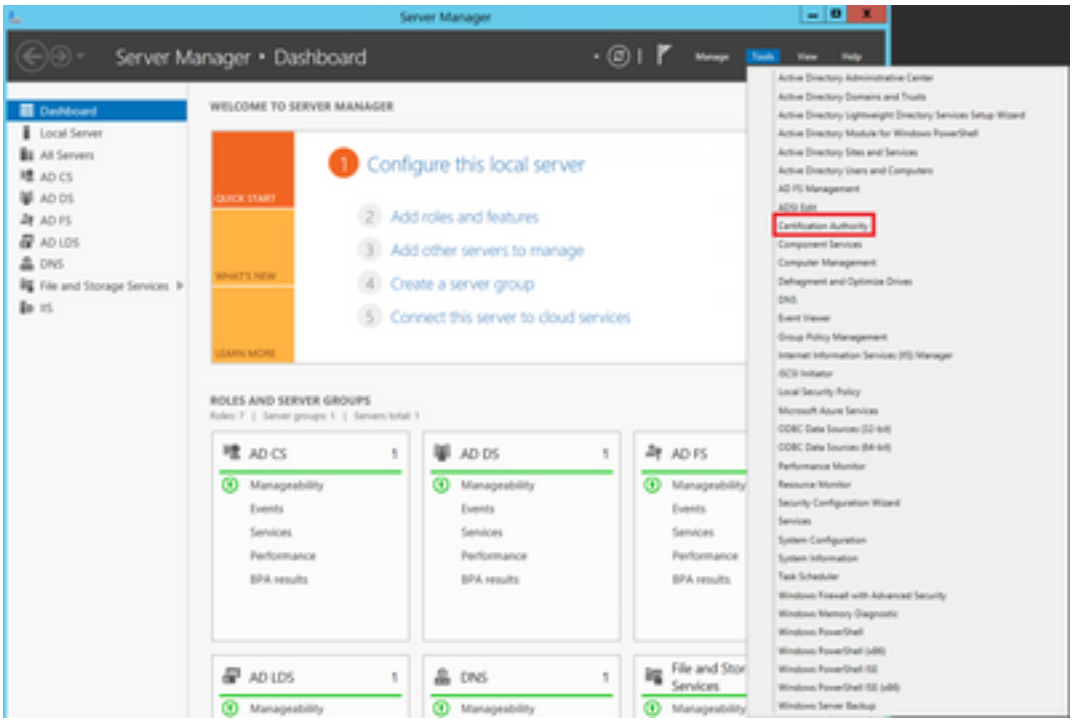
Certificat	Utilisation de la clé X.509	Utilisation de la clé étendue X.509
CallManager	·Signature numérique ·Chiffrement clé ·Chiffrement des données	·Authentification du serveur Web ·Authentification du client Web
tomcat	·Signature numérique ·Chiffrement clé ·Chiffrement des données	·Authentification du serveur Web ·Authentification du client Web
ipsec	·Signature numérique ·Chiffrement clé	·Authentification du serveur Web ·Authentification du client Web

	·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

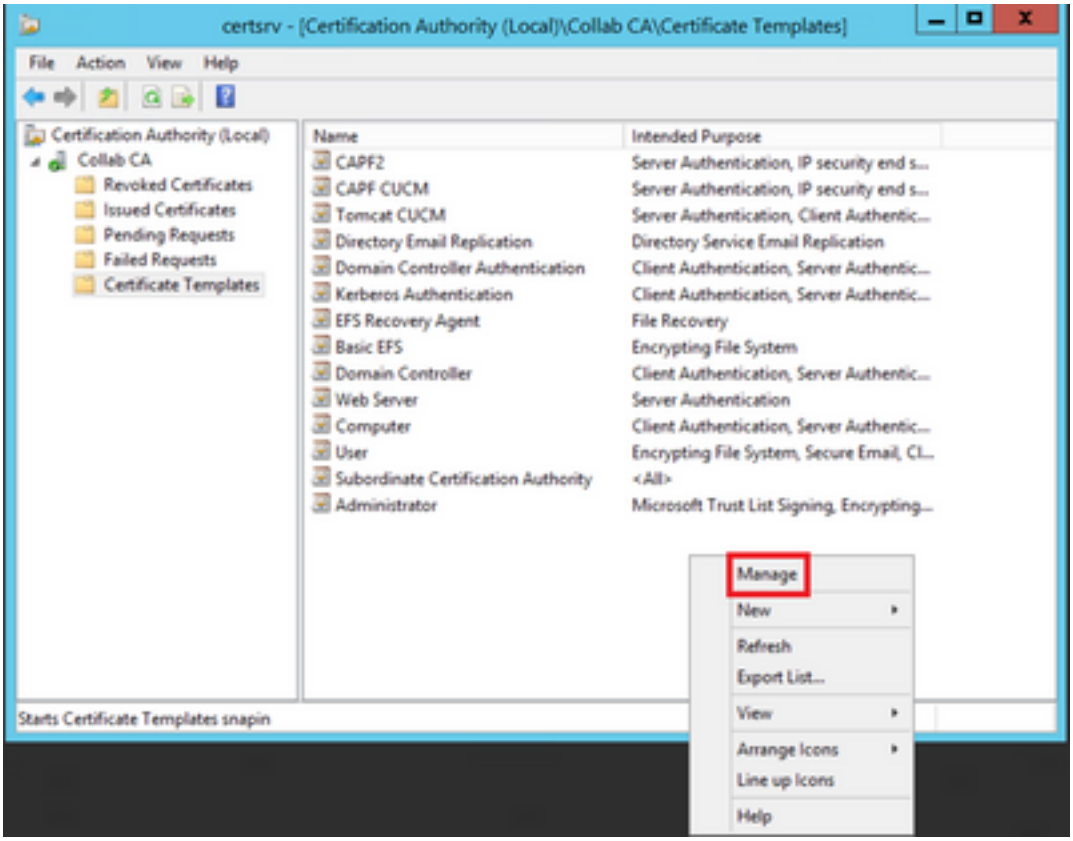
Pour plus d'informations, consultez le Guide de sécurité de Cisco Unified Communications Manager

Configurer

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



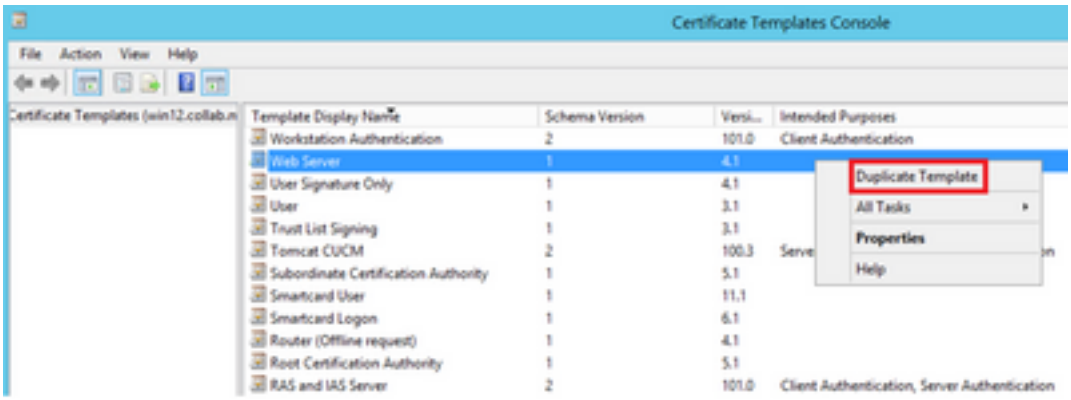
Étape 2. Sélectionnez votre autorité de certification, puis accédez à **Modèles de certificat**, cliquez avec le bouton droit sur la liste et sélectionnez **Gérer**, comme illustré dans l'image.



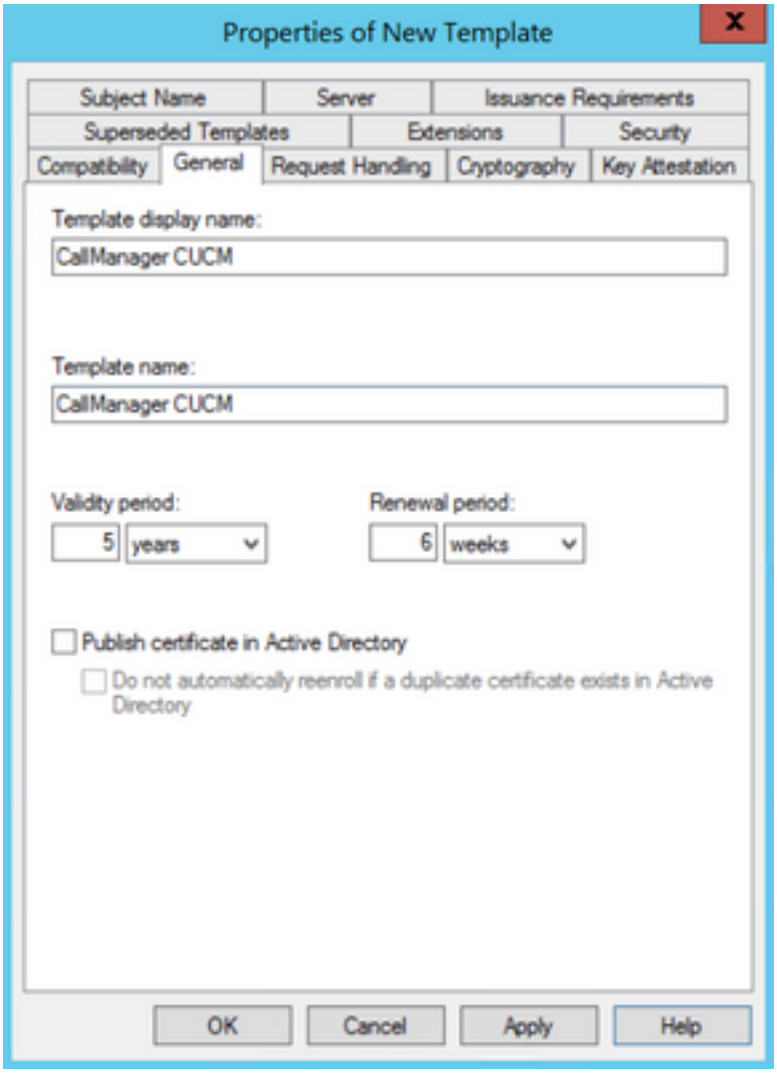
Modèle Callmanager / Tomcat / TVS

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.

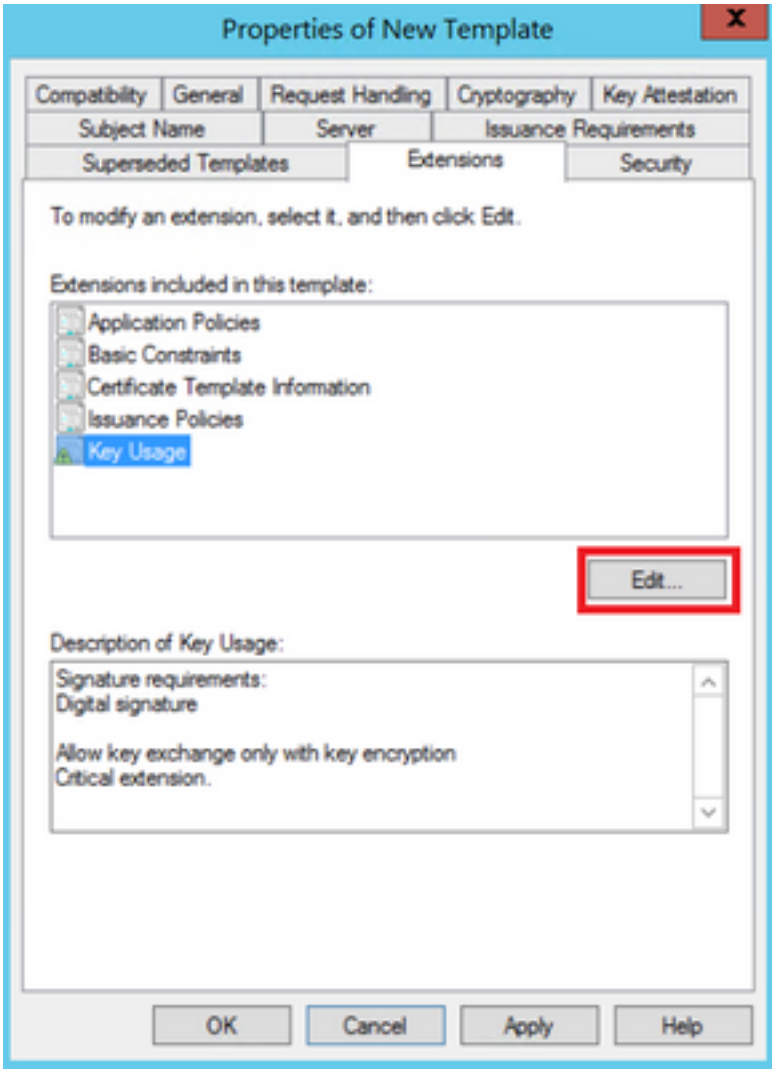
Étape 1. Recherchez le modèle **Web Server**, cliquez dessus avec le bouton droit et sélectionnez **Duplicate Template**, comme illustré dans l'image.



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

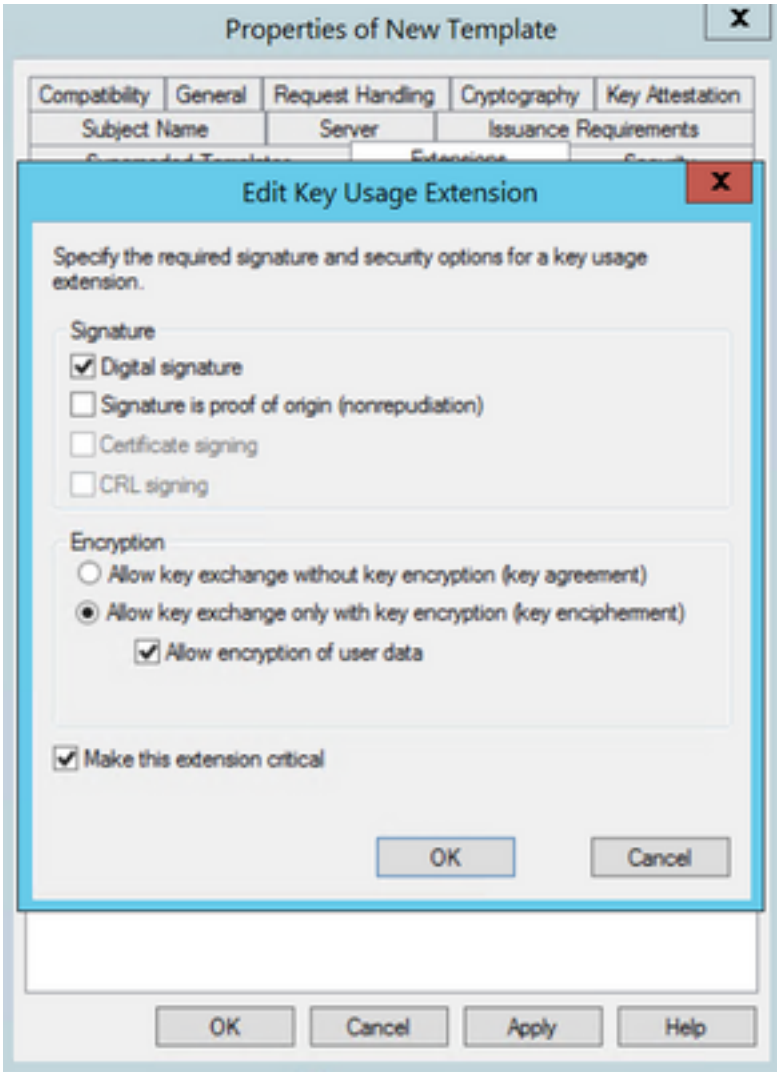


Étape 3. Accédez à **Extensions > Key Usage > Edit**, comme indiqué dans l'image.

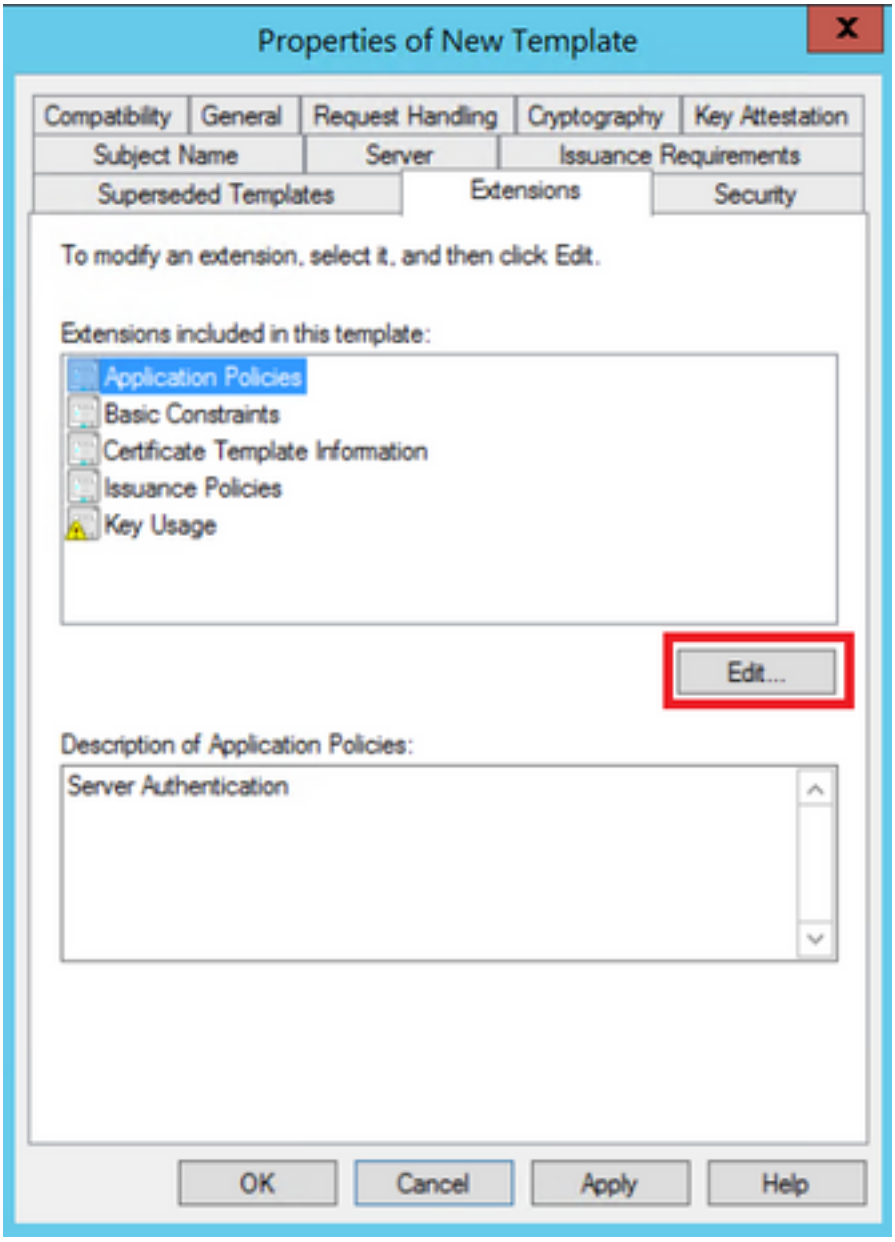


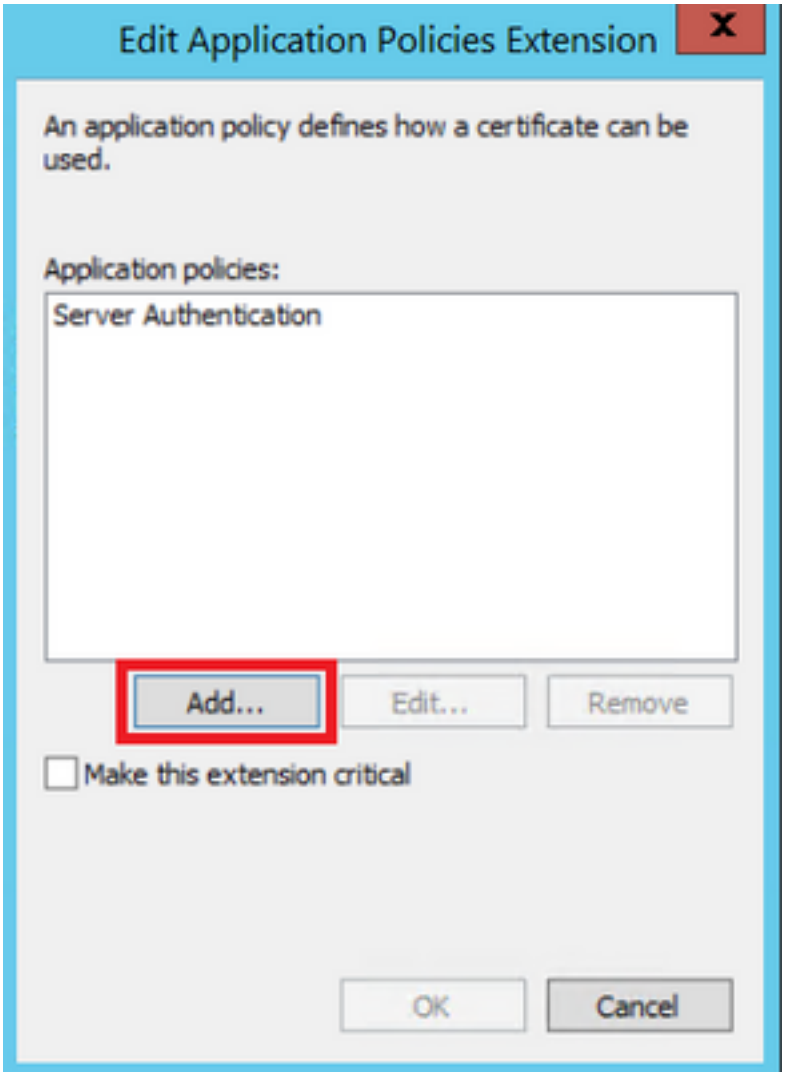
Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

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

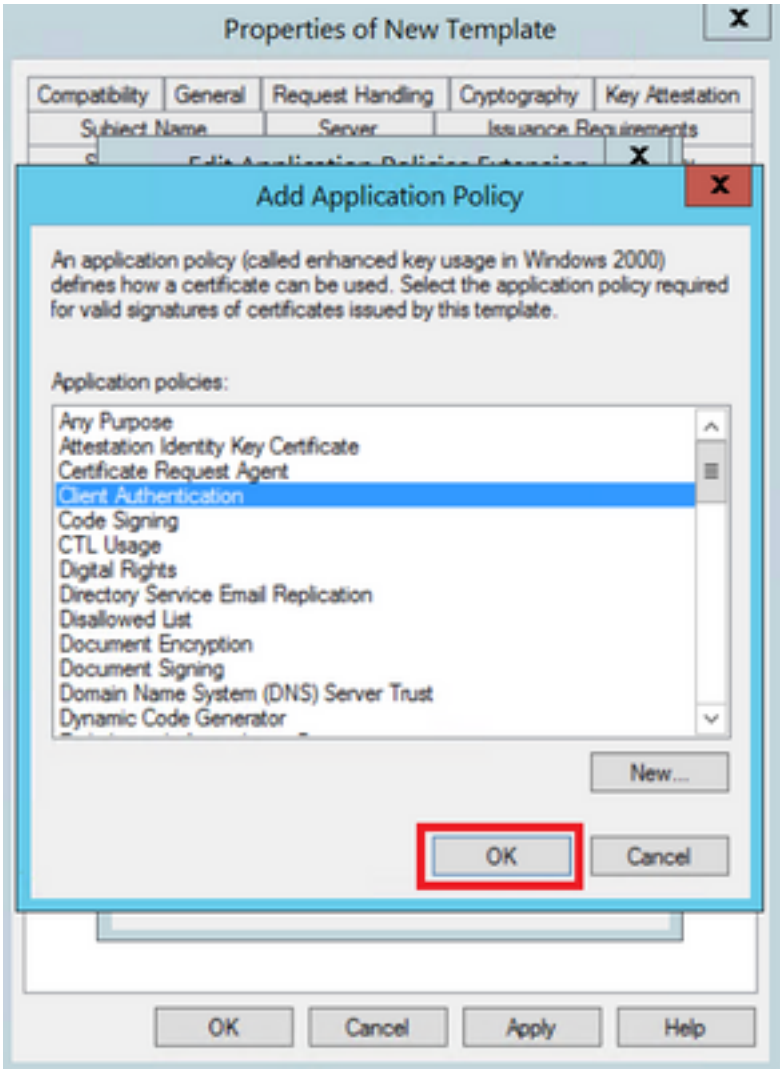


Étape 5. Accédez à **Extensions > Application Policies > Edit > Add**, comme indiqué dans l'image.

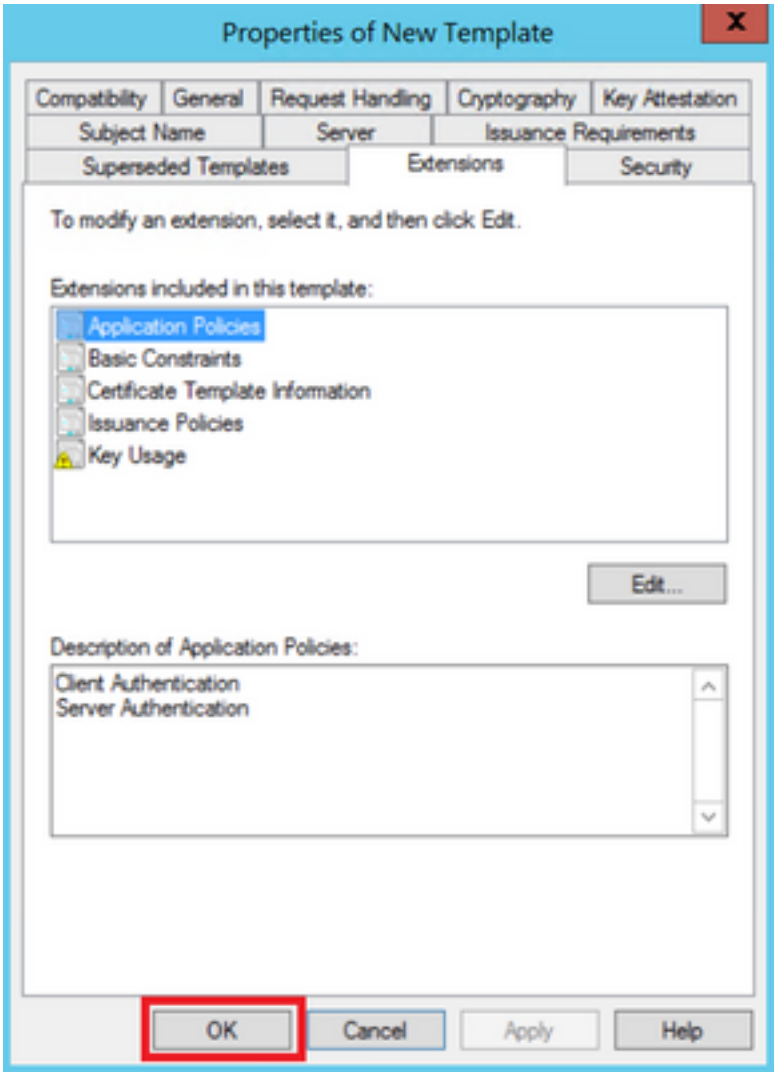

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



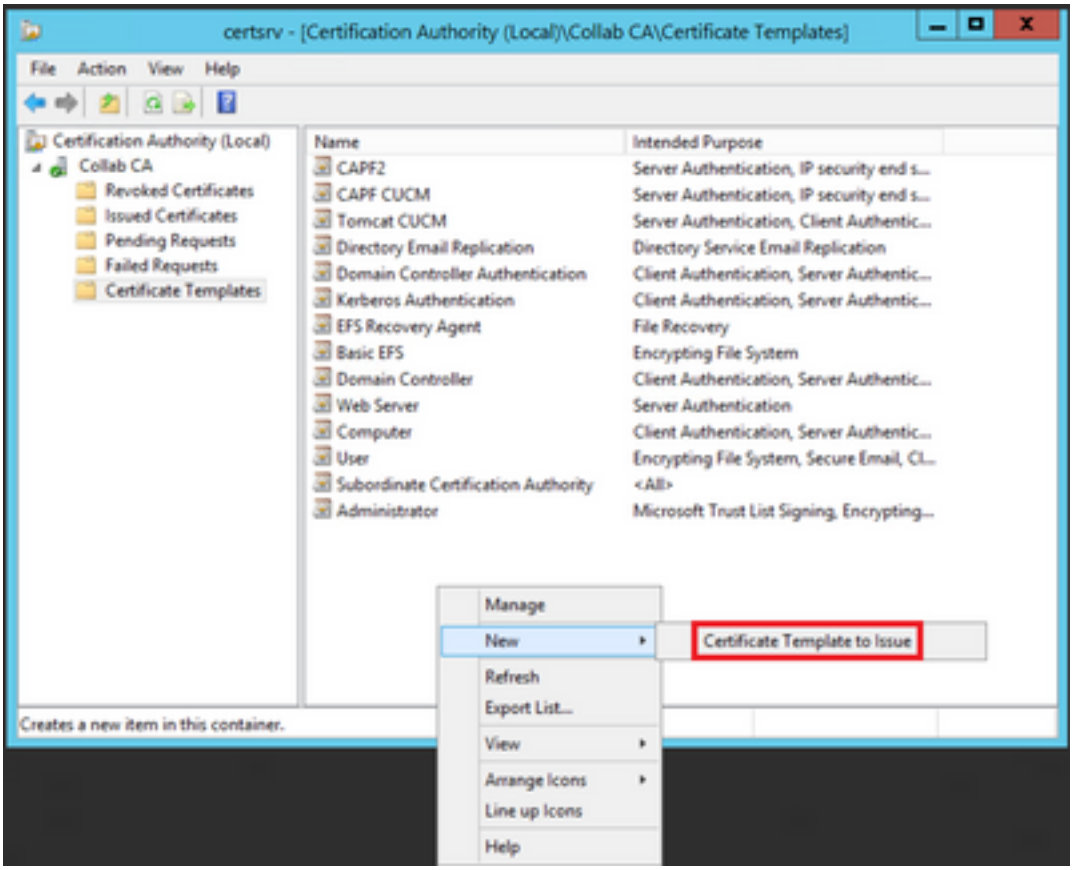
Étape 6. Recherchez **Client Authentication,** sélectionnez-le et sélectionnez **OK** sur cette fenêtre et la précédente, comme illustré dans l'image.



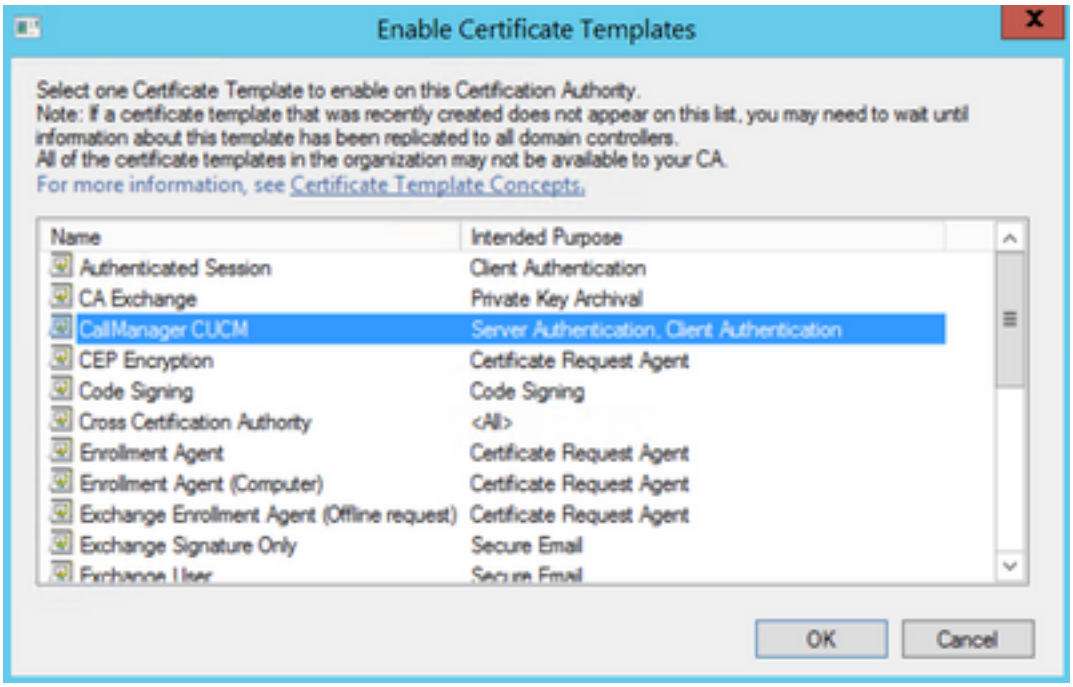
Étape 7. Retournez sur le modèle, sélectionnez **Apply**, puis **OK.**



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.



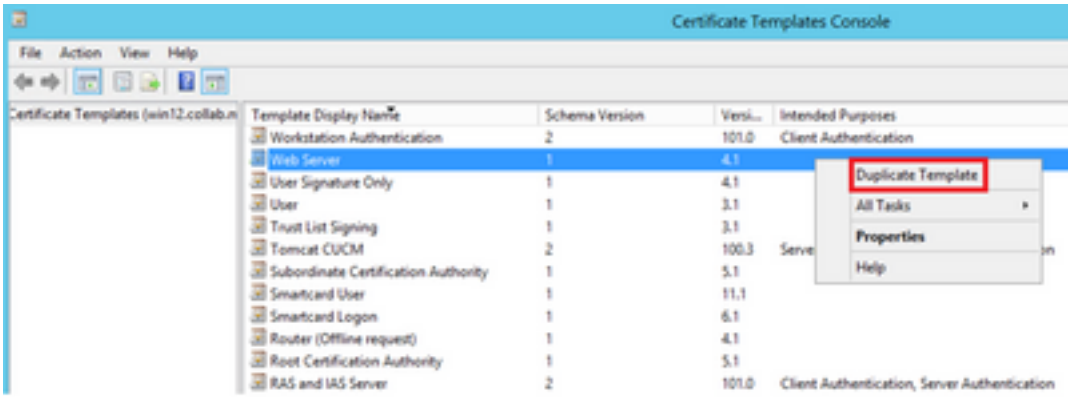
Étape 9. Sélectionnez le nouveau modèle **CallManager CUCM** et cliquez sur **OK**, comme illustré dans l'image.



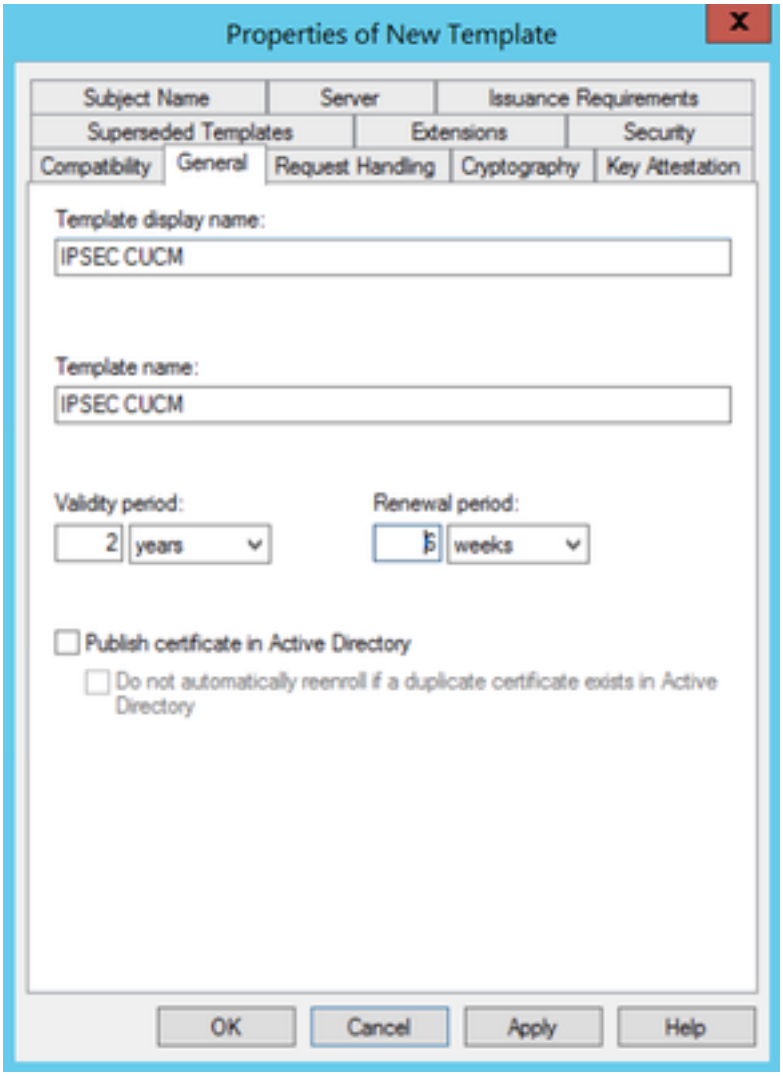
Étape 10. Répétez toutes les étapes précédentes pour créer des modèles de certificats pour les services Tomcat et TVS, le cas échéant.

Modèle IPsec

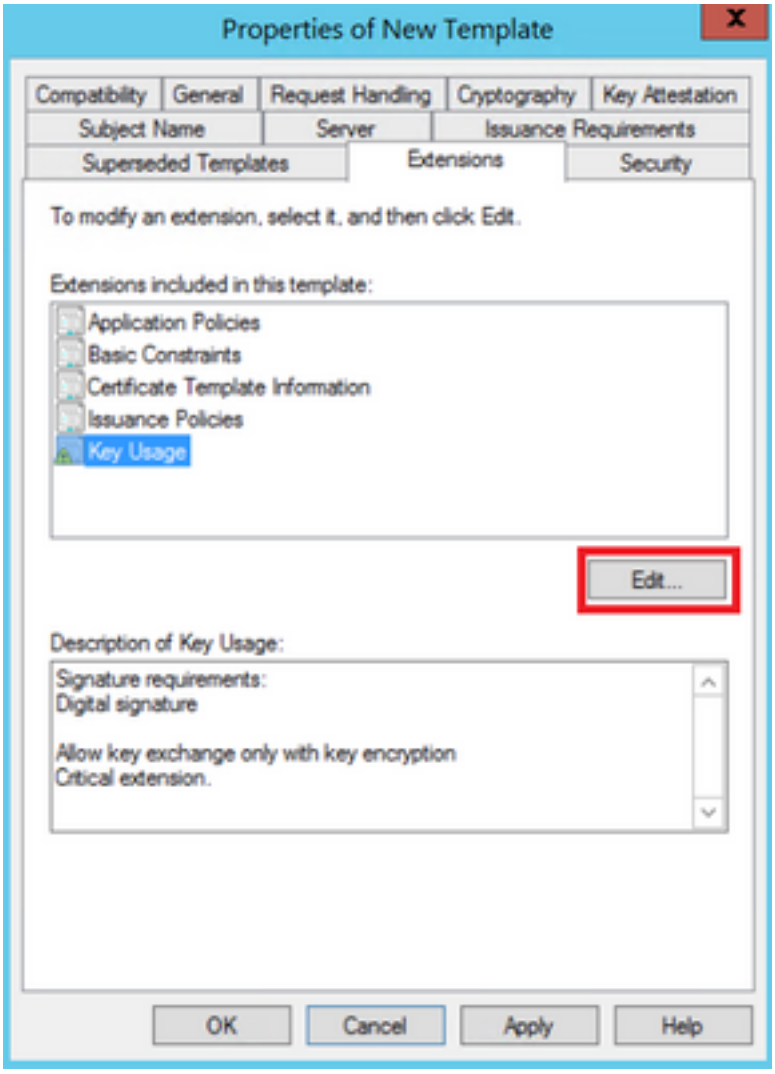
Étape 1. Recherchez le modèle **Web Server**, cliquez dessus avec le bouton droit et sélectionnez **Duplicate Template**, comme illustré dans l'image.



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

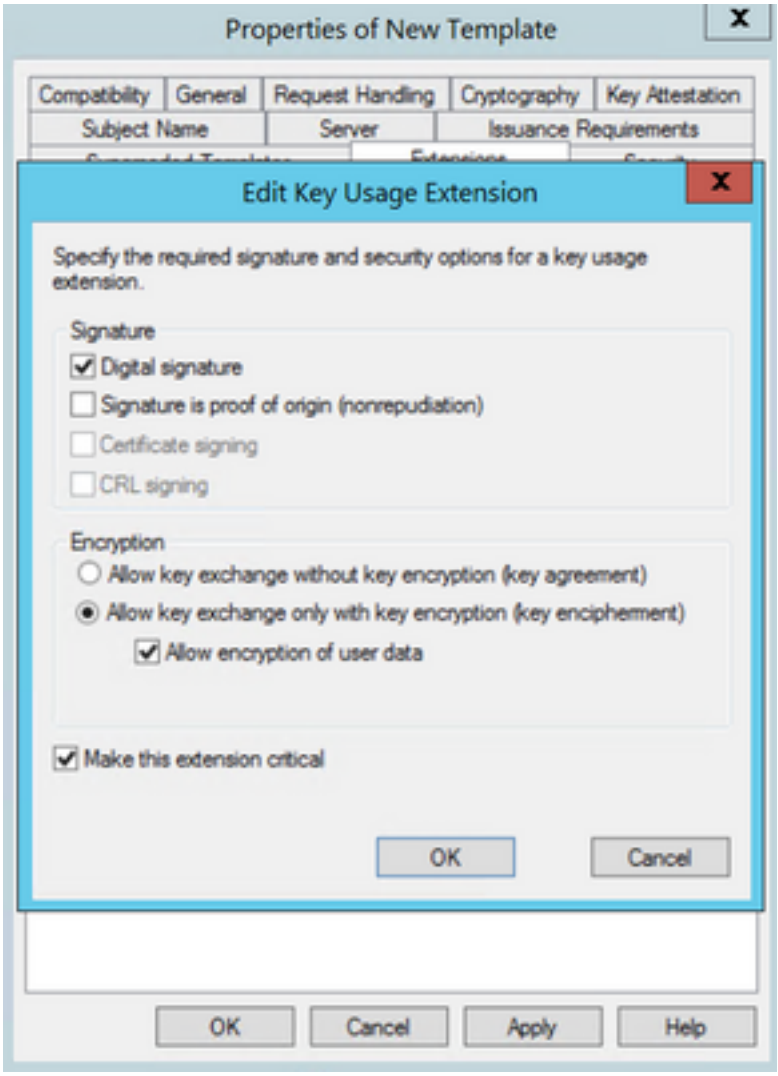


Étape 3. Accédez à **Extensions > Key Usage > Edit**, comme indiqué dans l'image.

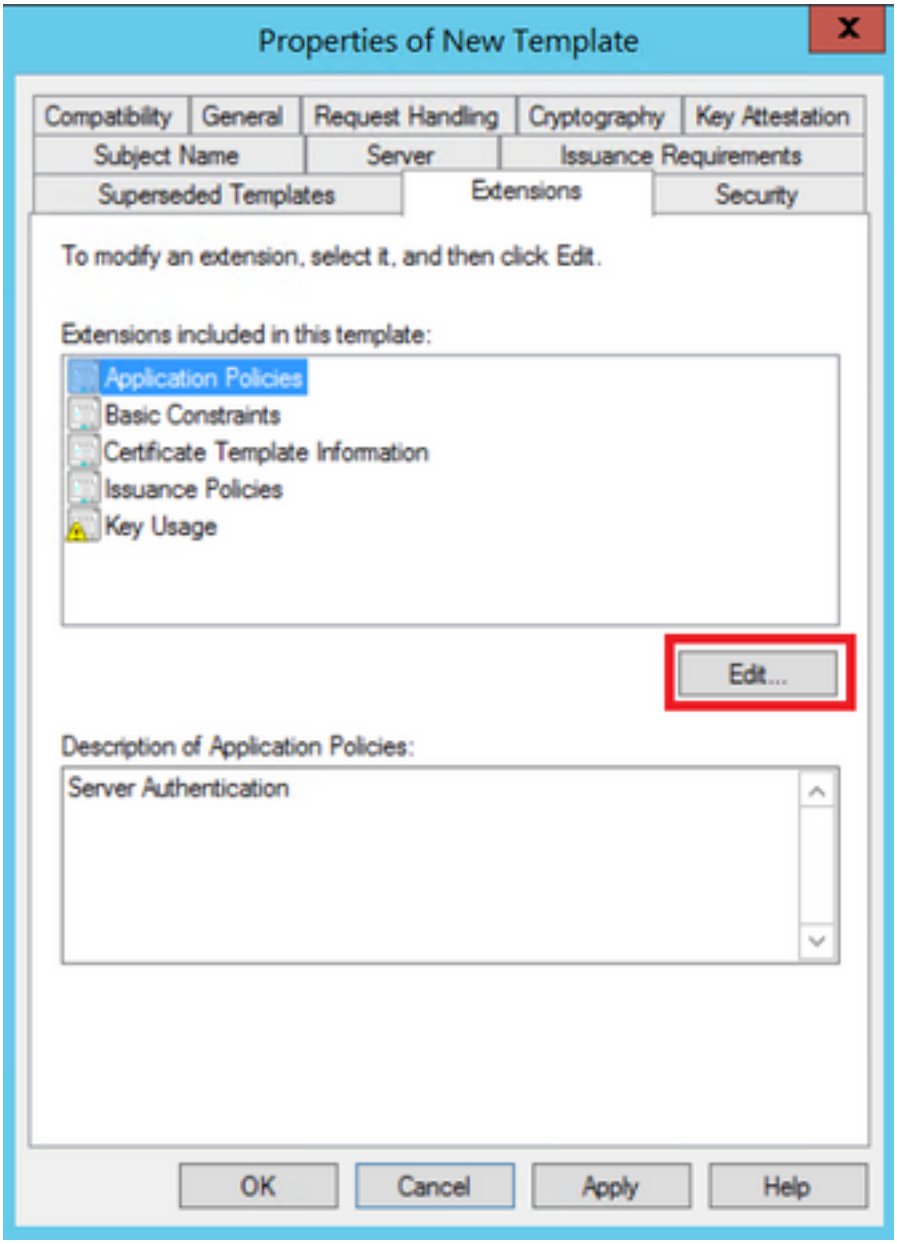


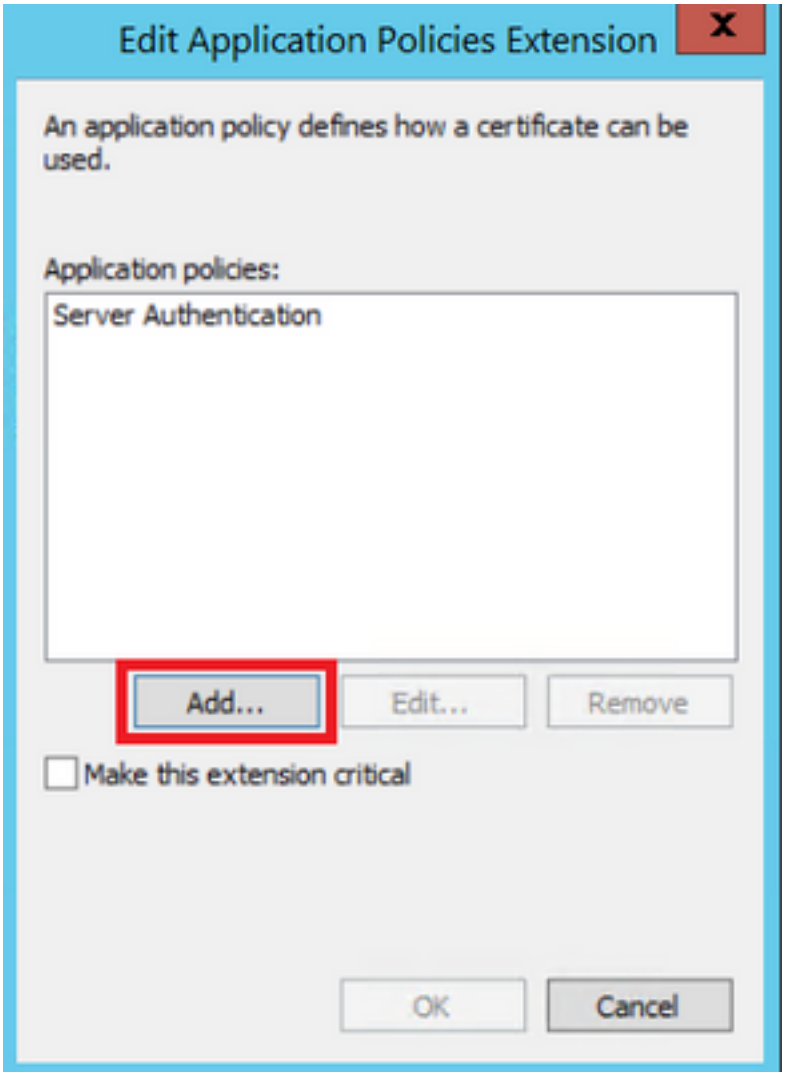
Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

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

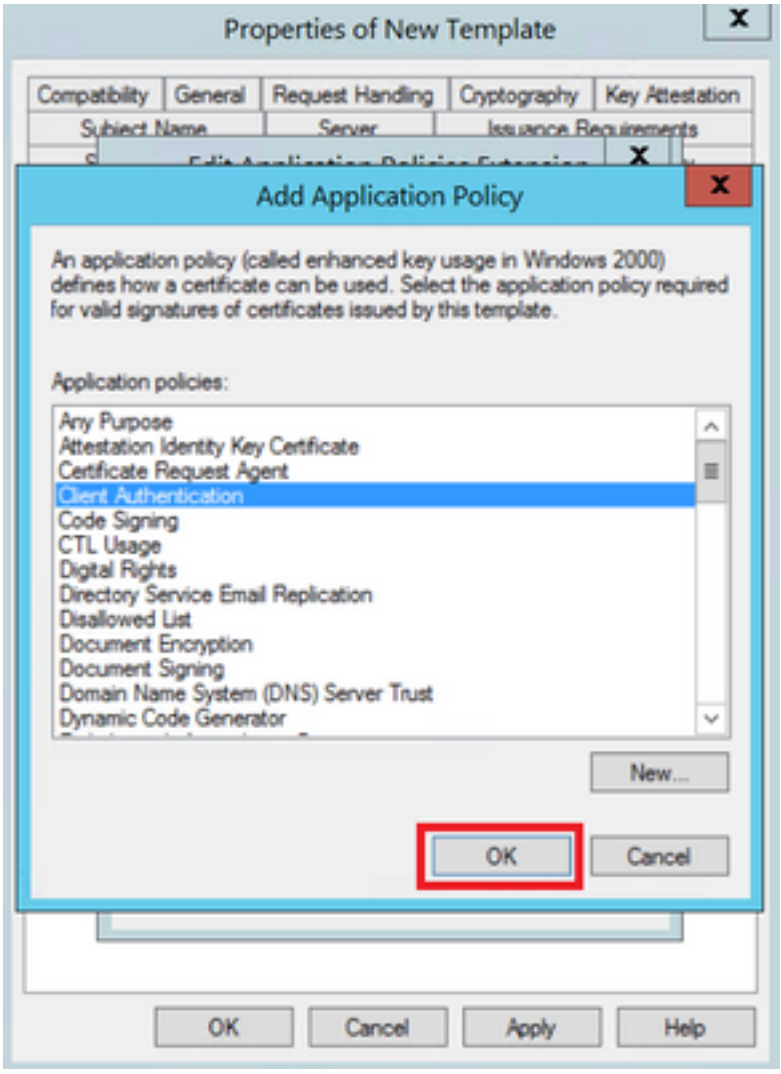


Étape 5. Accédez à **Extensions > Application Policies > Edit > Add**, comme indiqué dans l'image.

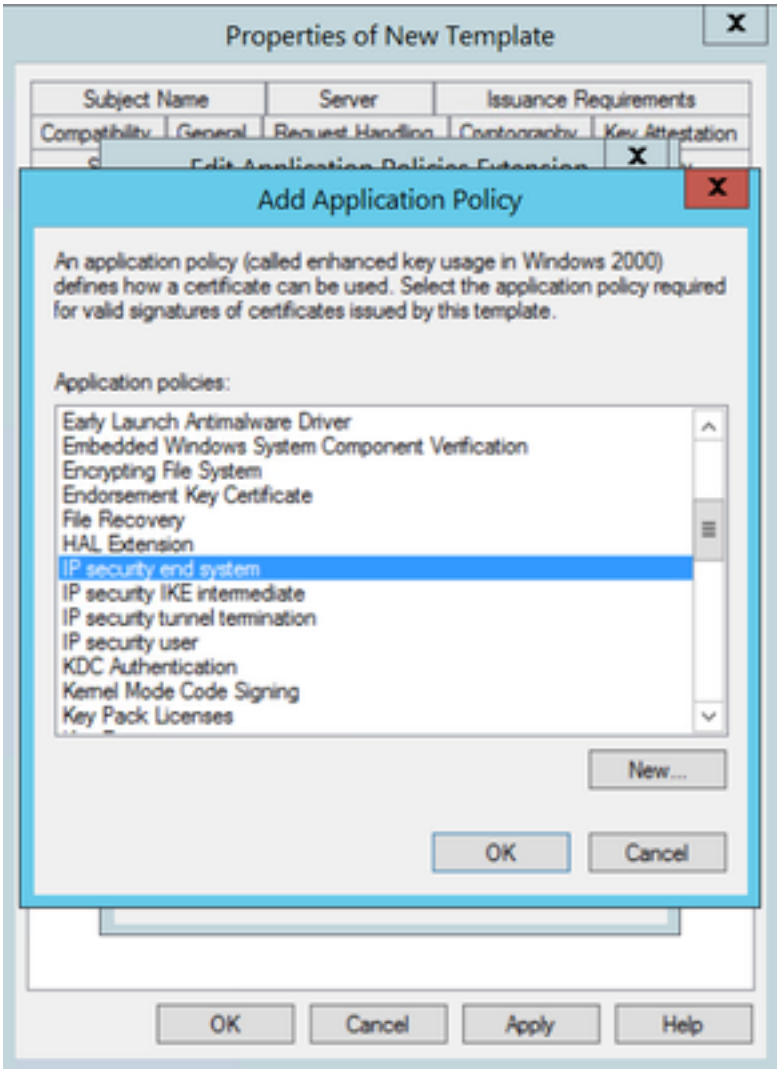

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



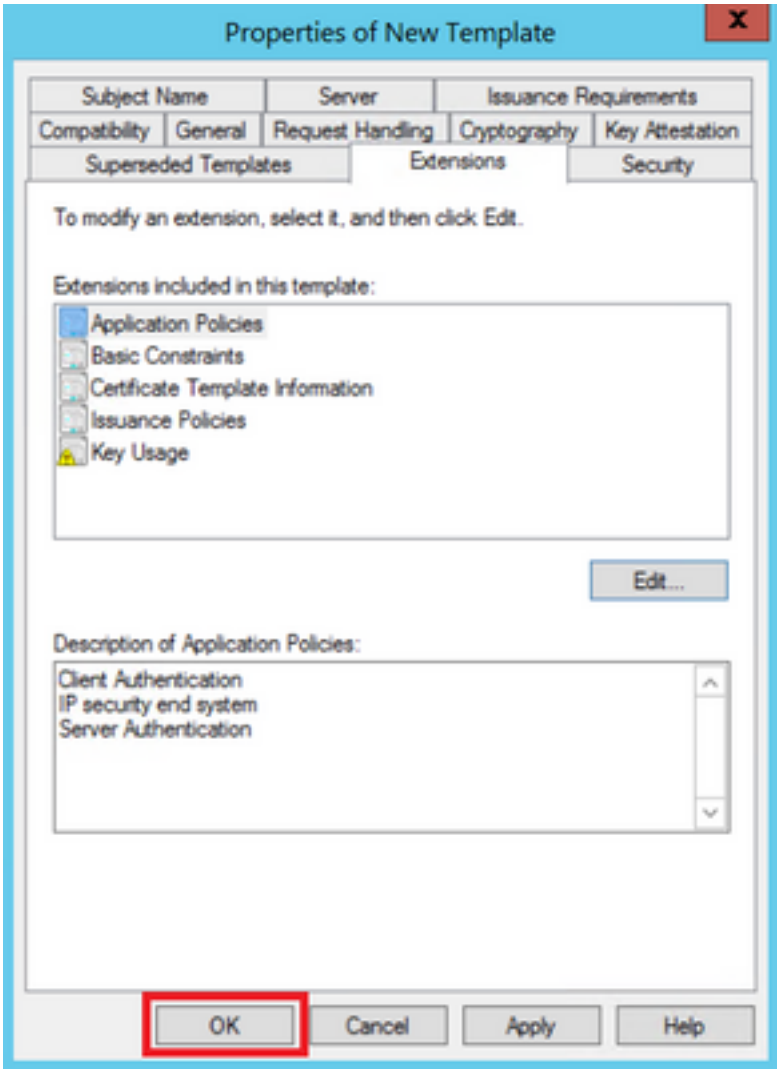
Étape 6. Recherchez **Client Authentication,** sélectionnez-le, puis **OK**, comme indiqué dans l'image.



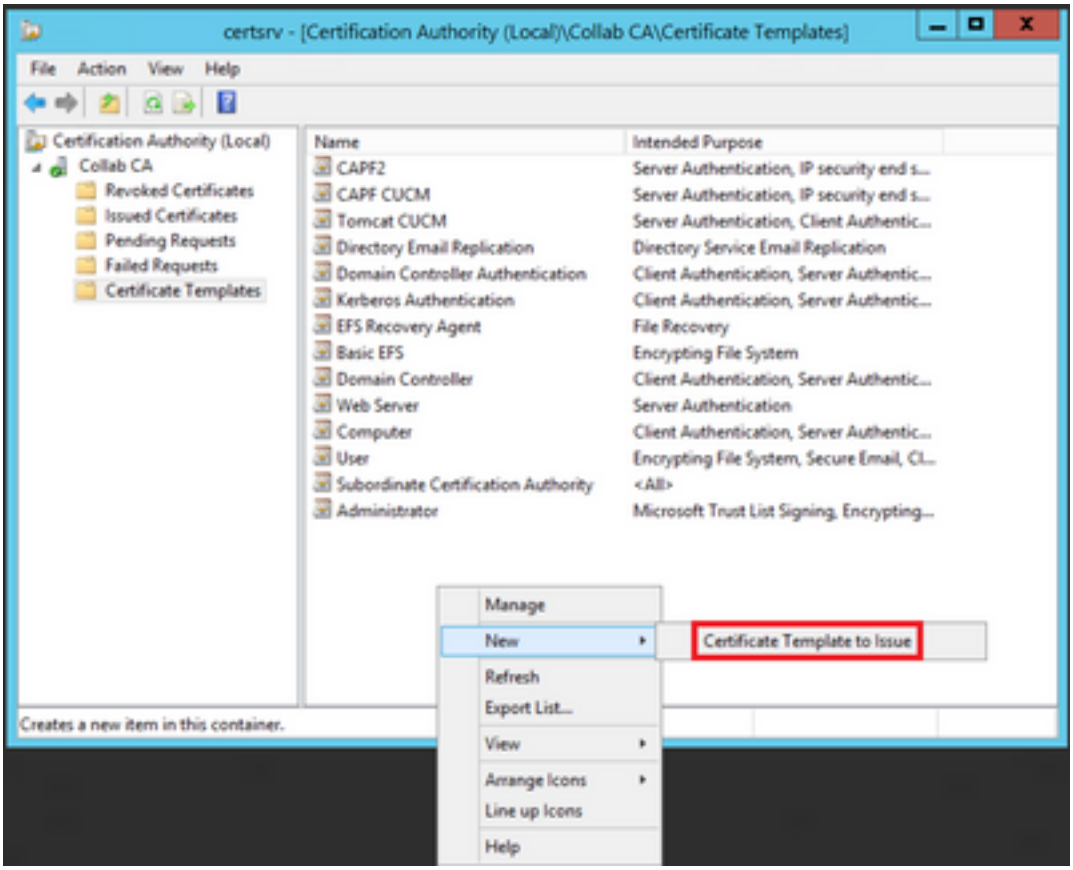
Étape 7. Sélectionnez **Add** à nouveau, recherchez **IP security end system**, sélectionnez-le, puis sélectionnez **OK** sur ce et sur la fenêtre précédente ainsi.



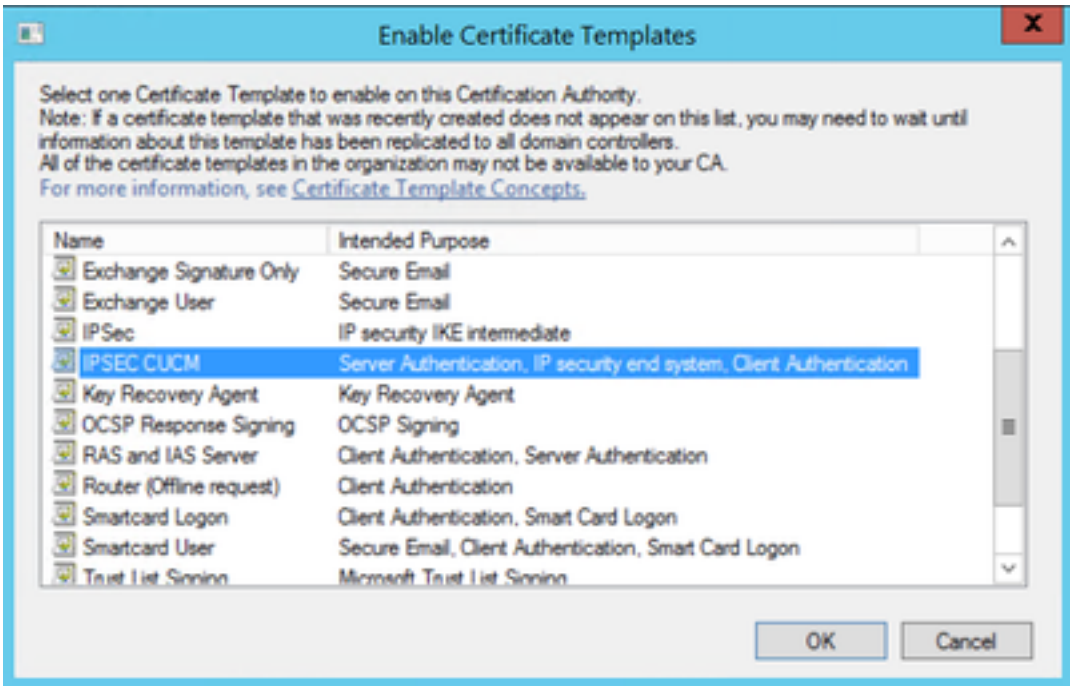
Étape 8. De retour sur le modèle, sélectionnez **Apply** puis **OK**, comme indiqué dans l'image.



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.

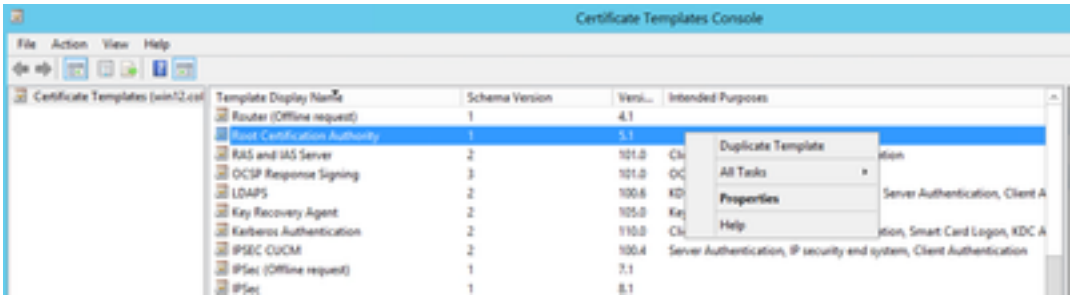


Étape 10. Sélectionnez le nouveau modèle **IPSEC CUCM** et cliquez sur **OK**, comme illustré dans l'image.



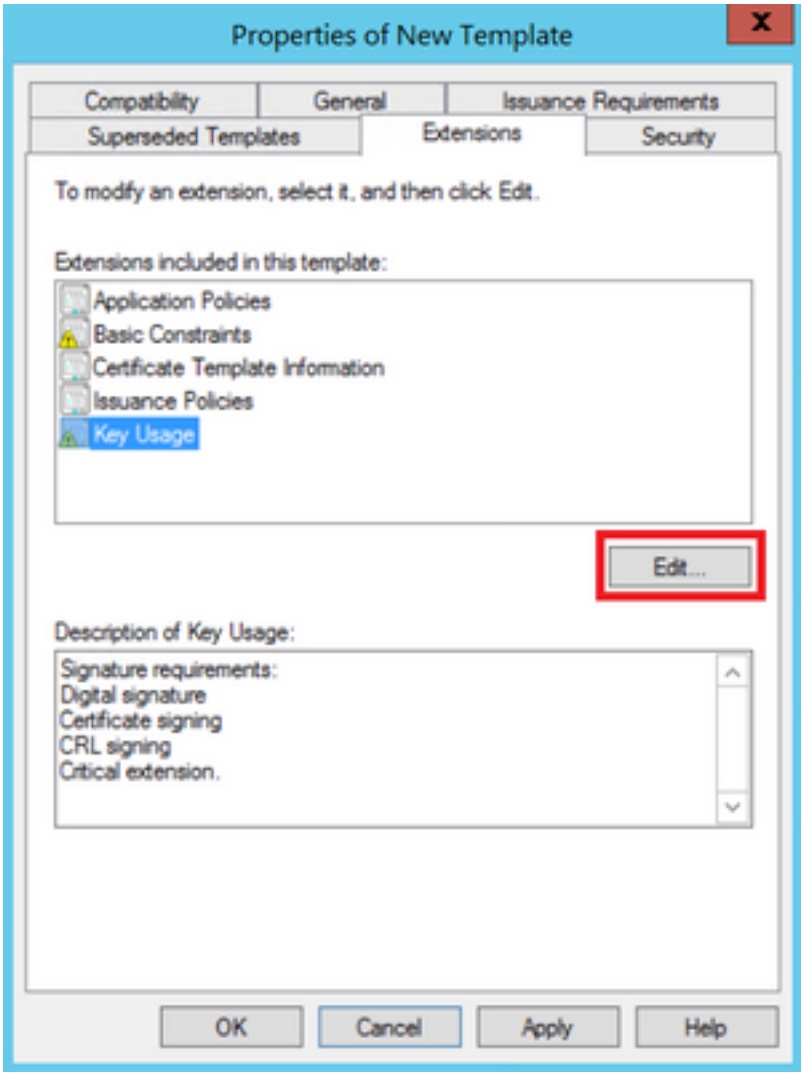
Modèle CAPF

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



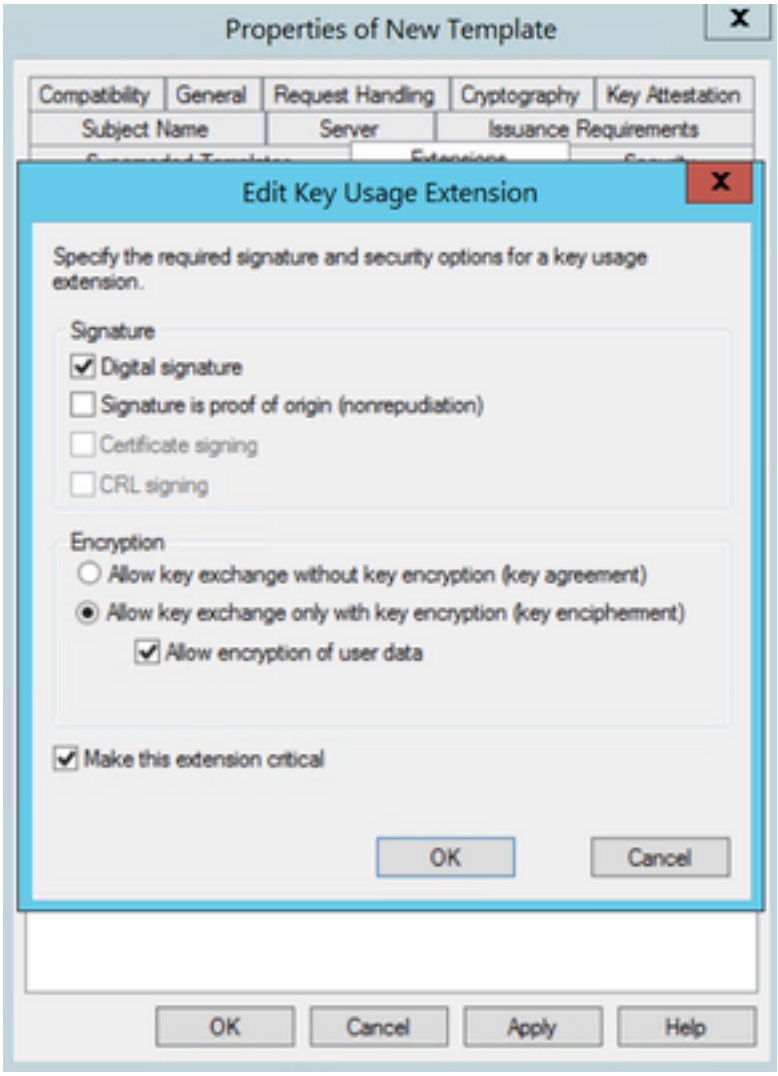
Étape 2. Sous **Général**, vous pouvez modifier le nom, le nom d'affichage, la validité, etc. du modèle de certificat.

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

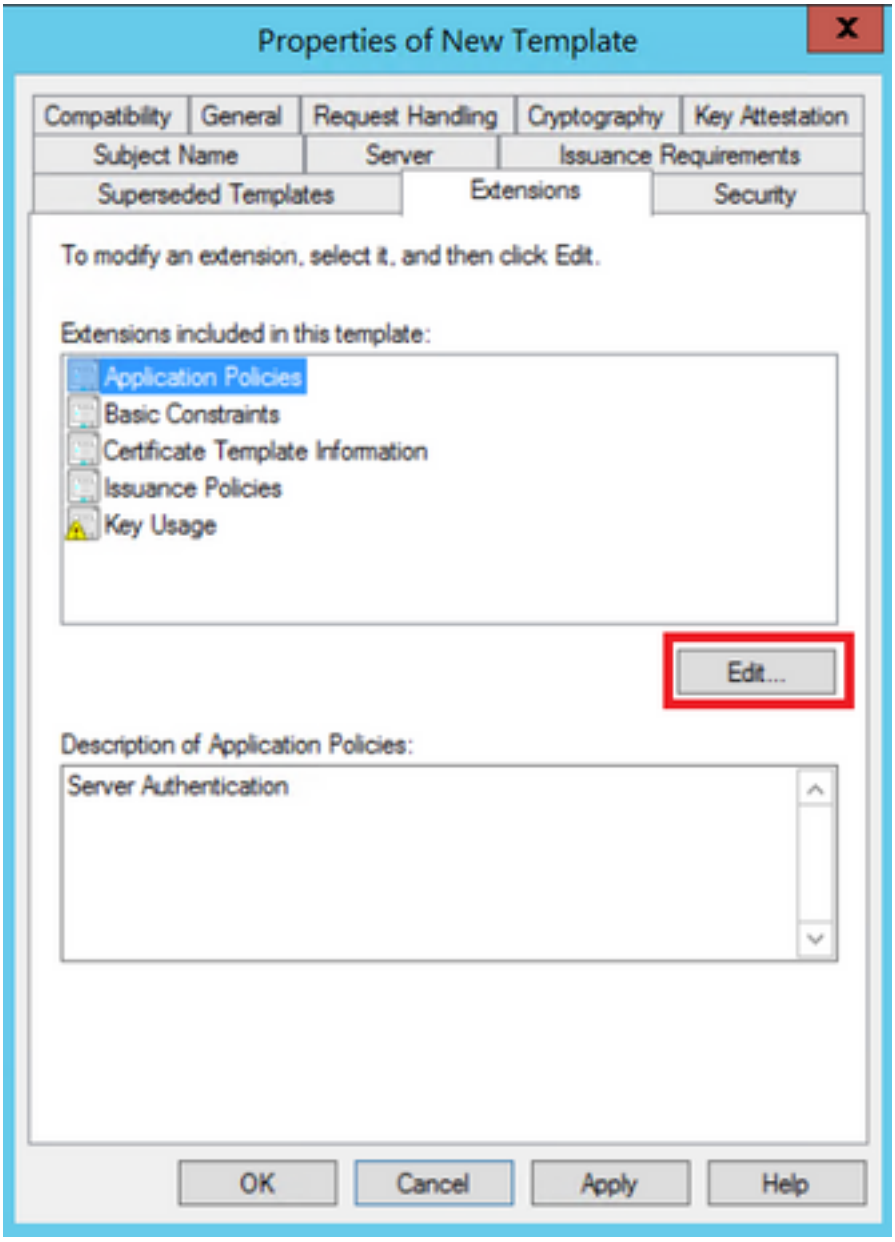


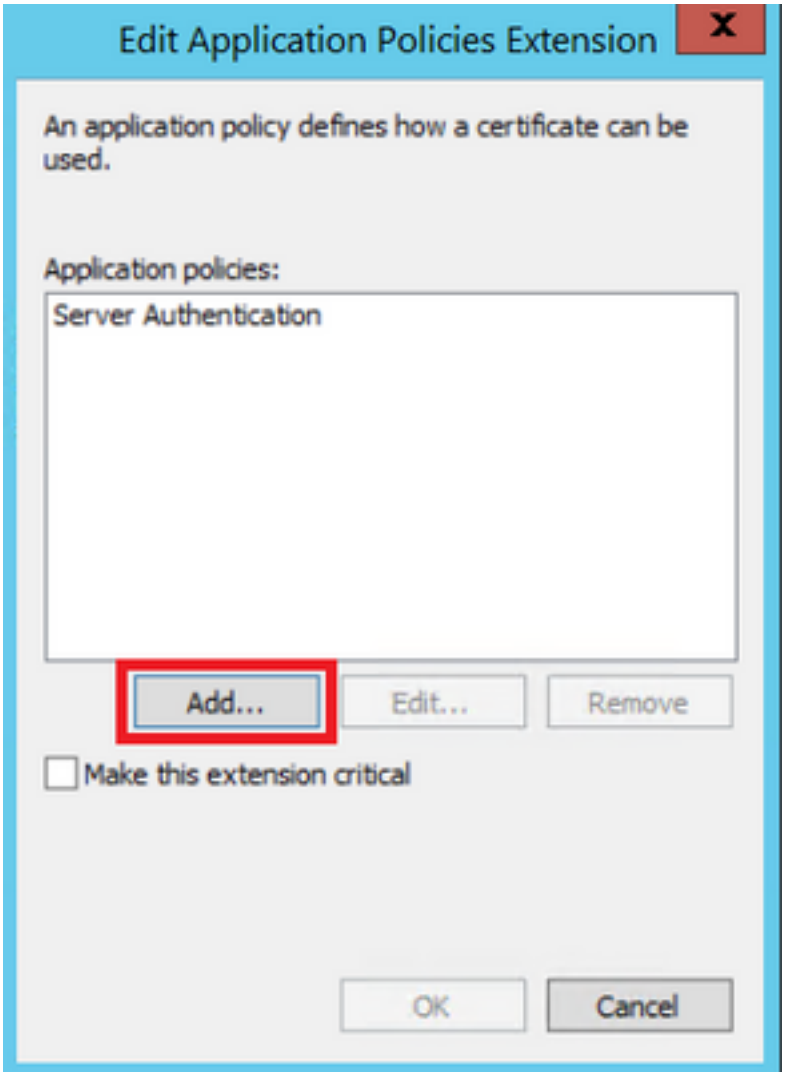
Étape 4. Sélectionnez ces options et cliquez sur **OK**, comme illustré dans l'image.

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

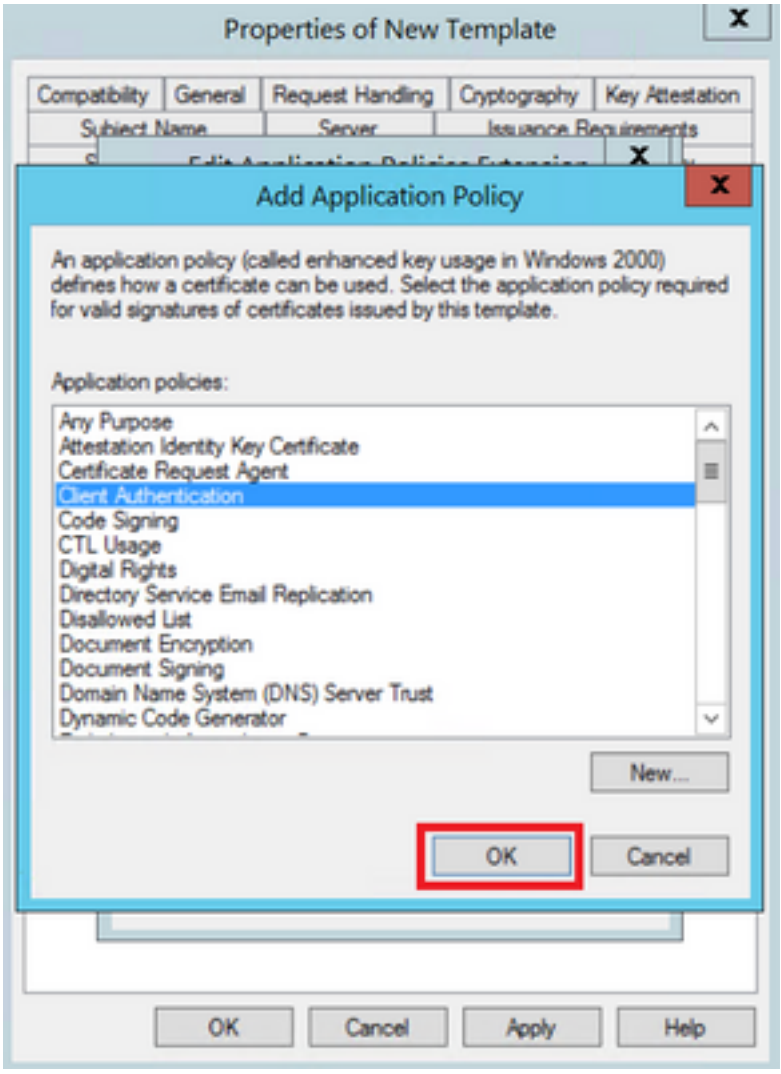


Étape 5. Accédez à **Extensions > Application Policies > Edit > Add**, comme indiqué dans l'image.

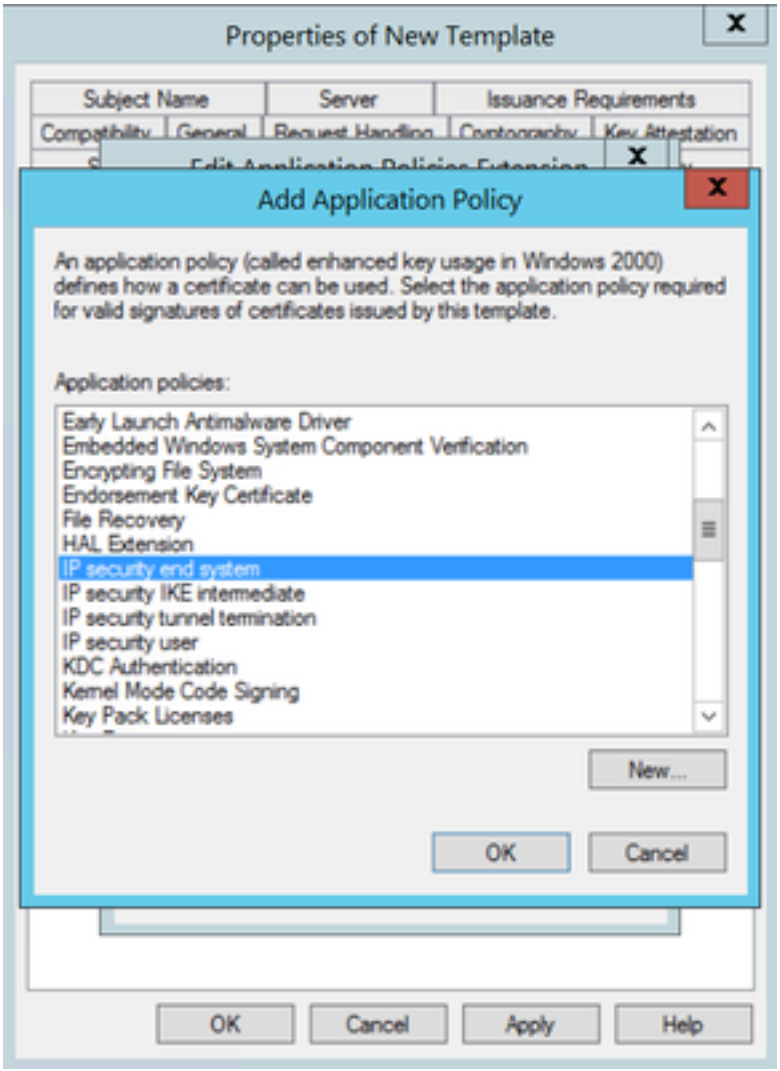

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



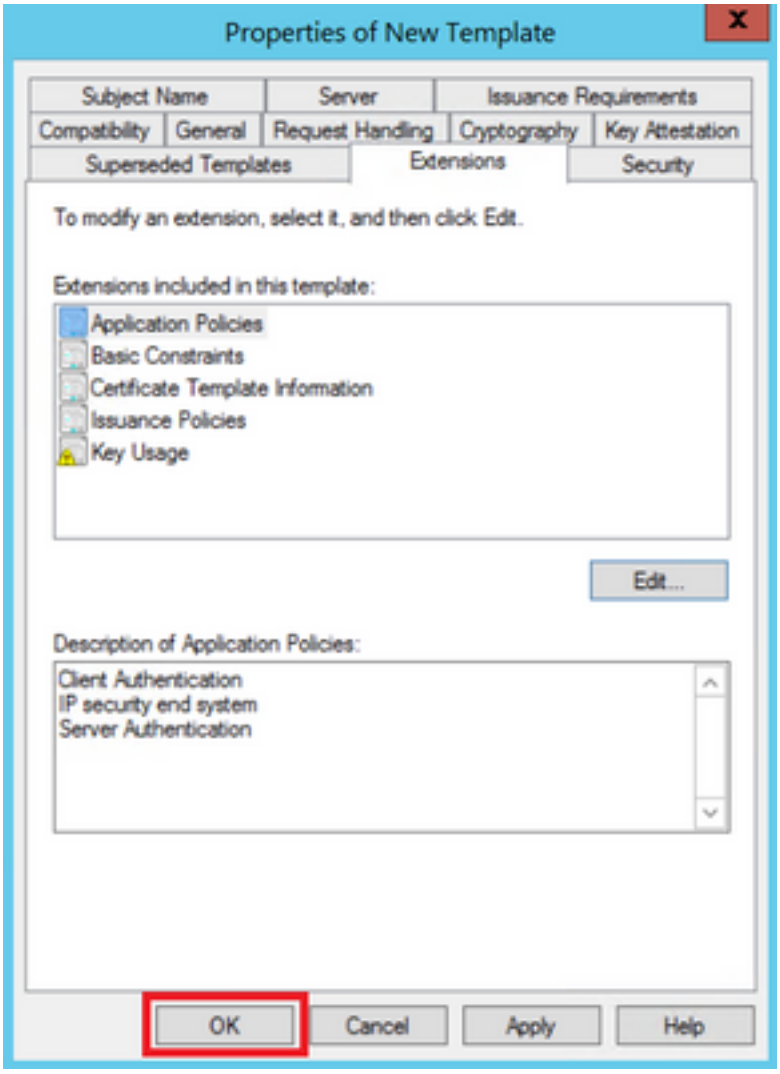
Étape 6. Recherchez **Client Authentication,** sélectionnez-le, puis sélectionnez **OK**, comme indiqué dans l'image.



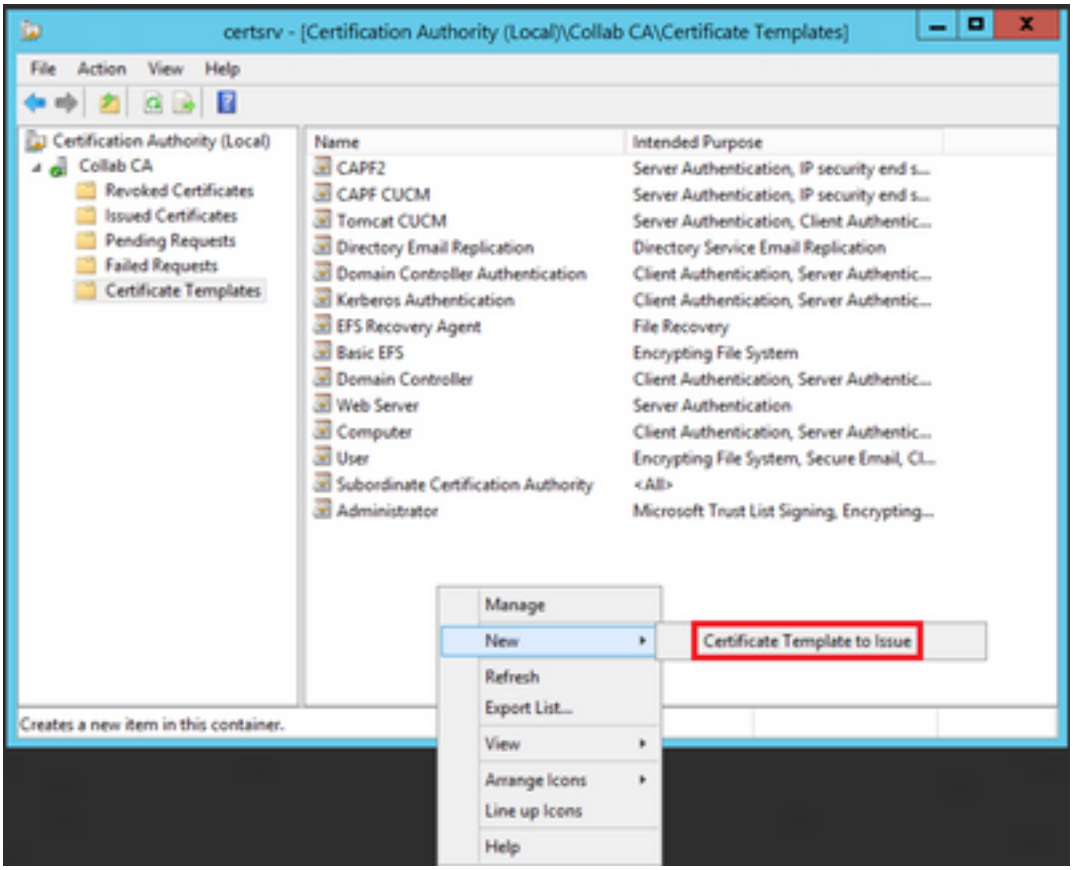
Étape 7. Sélectionnez **Add** à nouveau, recherchez **IP security end system**, sélectionnez-le, puis cliquez sur OK dans cette fenêtre et dans la fenêtre précédente également, comme illustré dans l'image.



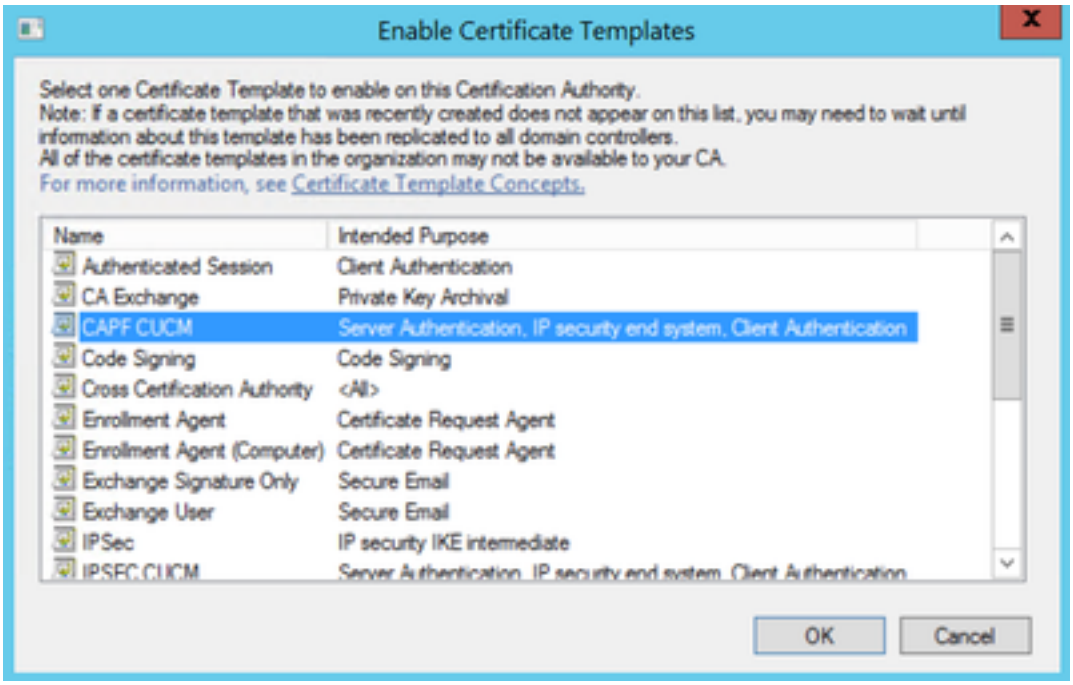
Étape 8. De retour sur le modèle, sélectionnez **Apply** puis **OK**, comme indiqué dans l'image.



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.



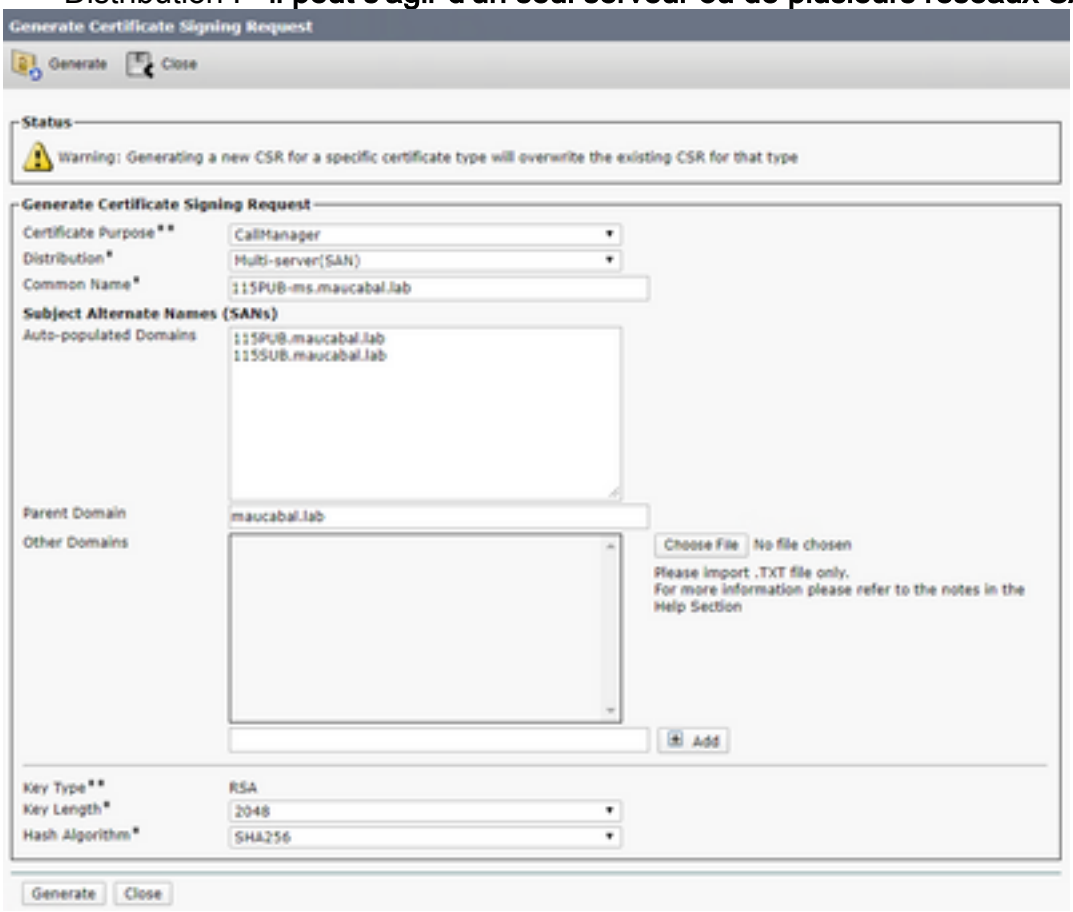
Générer une demande de signature de certificat

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**.

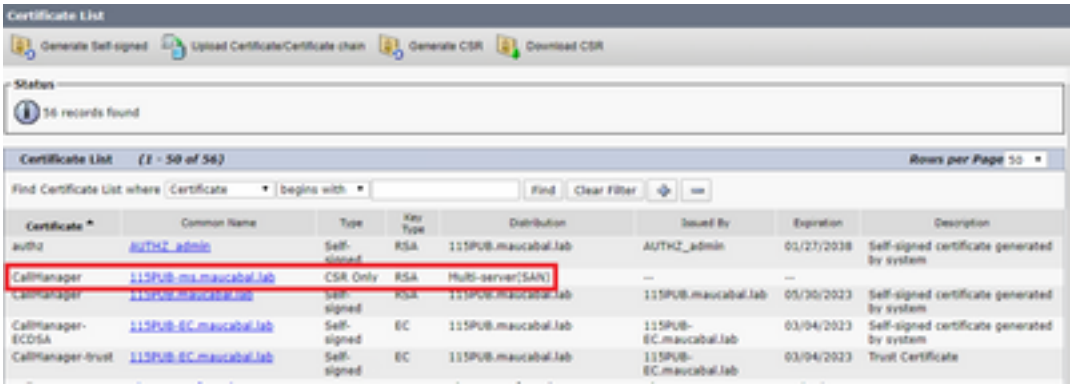
Étape 2. Sélectionnez ces options et sélectionnez **Generate**, comme indiqué dans l'image.

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

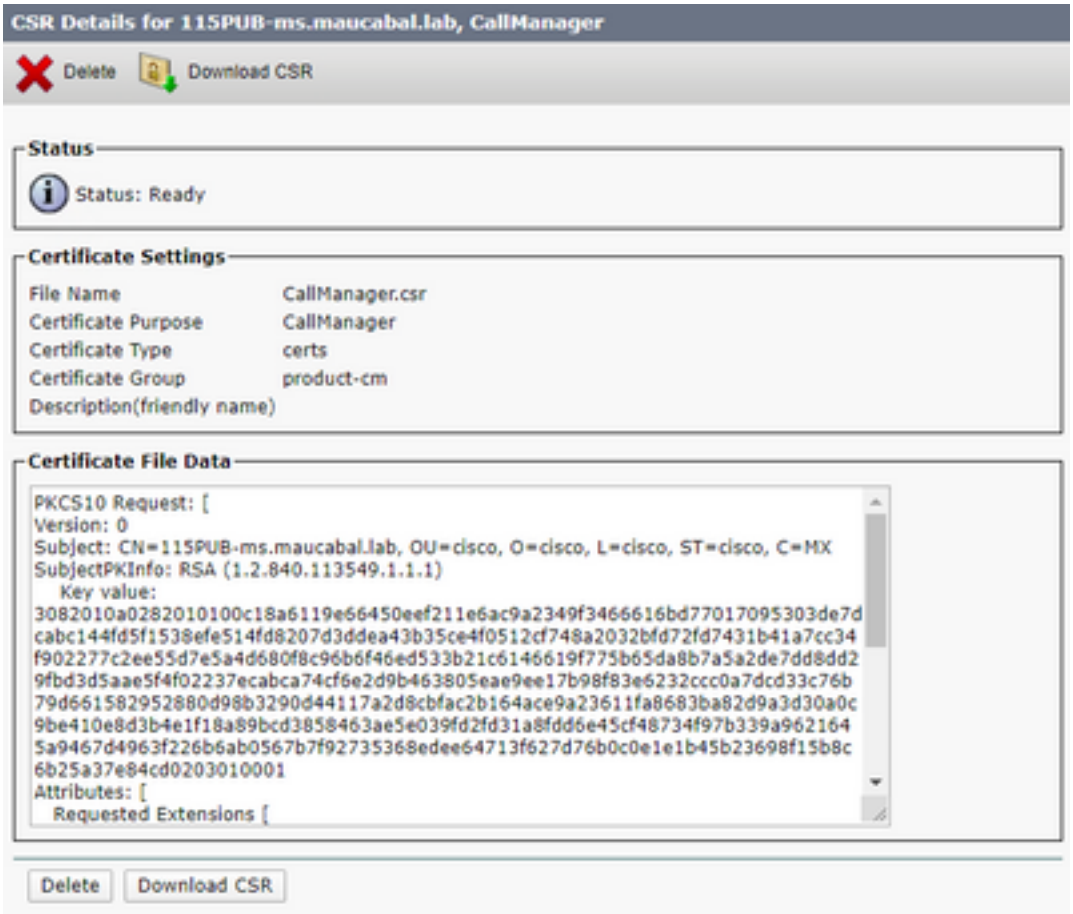


Étape 3. Un message de confirmation est généré, comme illustré dans l'image.

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

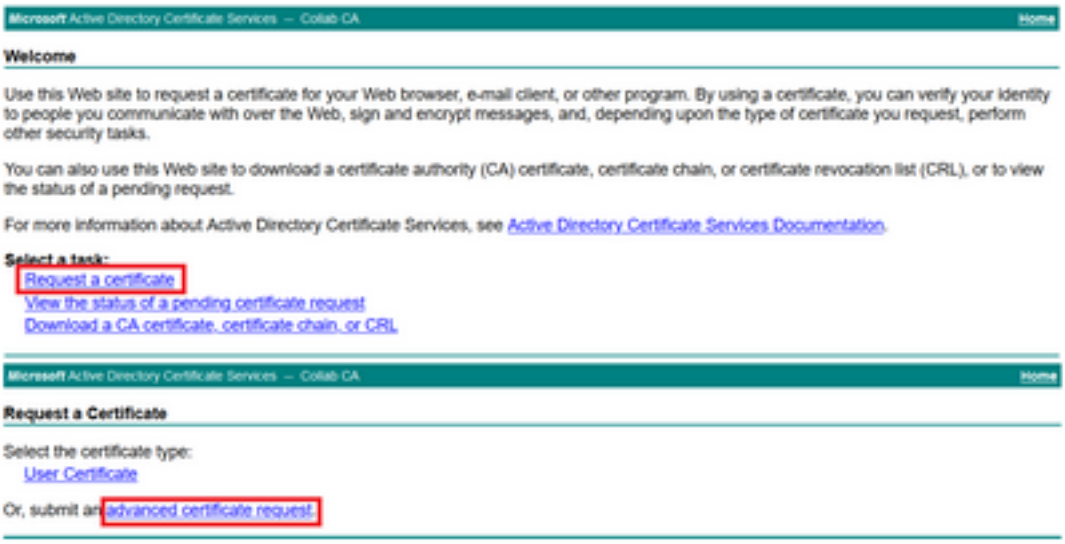


Étape 5. Dans la fenêtre contextuelle, sélectionnez **Download CSR**, et enregistrez le fichier sur votre ordinateur.

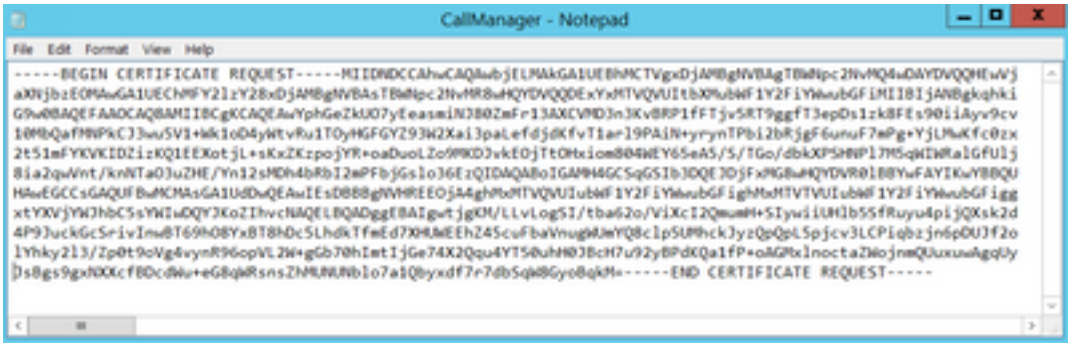


Étape 6. Dans votre navigateur, accédez à cette URL et entrez vos informations d'identification d'administrateur de contrôleur de domaine : **https://<votreWindowsServerIP>/certsrv/.**

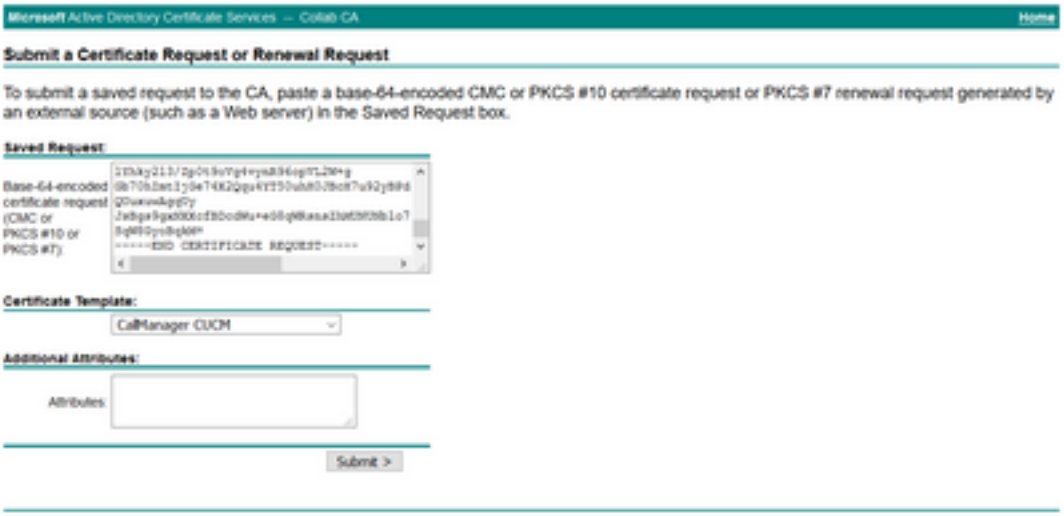
Étape 7. Naviguez jusqu'à **Request a certificate > advanced certificate request**, comme indiqué dans l'image.



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.

Vérifier

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.