Criar modelos de certificado de CA do Windows para CUCM

Contents

Introduction

Este documento descreve um procedimento passo a passo para criar modelos de certificado em Autoridades de Certificação (CA) baseadas em Windows Server, que são compatíveis com os requisitos de extensão X.509 para cada tipo de certificado do Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM versão 11.5(1) ou posterior
- O conhecimento básico da administração do Windows Server também é recomendado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- As informações neste documento são baseadas no CUCM versão 11.5(1) ou posterior.
- Microsoft Windows Server 2012 R2 com serviços de autoridade de certificação instalados.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Há cinco tipos de certificados que podem ser assinados por uma CA externa:

Certificado	Uso	Serviços afetados
CallManager	Apresentado no registro de dispositivo seguro, pode assinar arquivos CTL (Certificate Trust List)/ITL (Internal Trust List), usados para interações seguras com outros servidores, como troncos SIP (Session Initiation Protocol) seguros.	·Cisco Call Manager ·Cisco CTI Manager ·Cisco TFTP
tomcat	Apresentado para interações do protocolo HTTPS.	·Cisco Tomcat ·SSO (Single Sign-On, login único) ·Mobilidade de ramal ·Corporate Directory
ipsec	Usado para geração de arquivos de backup, bem como para interação de segurança IP (IPsec) com gateways MGCP (Media Gateway Control Protocol) ou H323.	·Cisco DRF Master ·Cisco DRF Local
CAPF	Usado para gerar LSC (Locally Significant Certificates) para telefones.	·Função de proxy da Cisco Certificate Authority
TVS	Usado para criar uma conexão com o TVS (Trust Verification Service), quando os telefones não podem autenticar um certificado desconhecido.	·Serviço de verificação de confiança da Cisco

Cada um desses certificados tem alguns requisitos de extensão X.509 que precisam ser definidos, caso contrário, você pode encontrar comportamentos incorretos em qualquer um dos serviços mencionados acima:

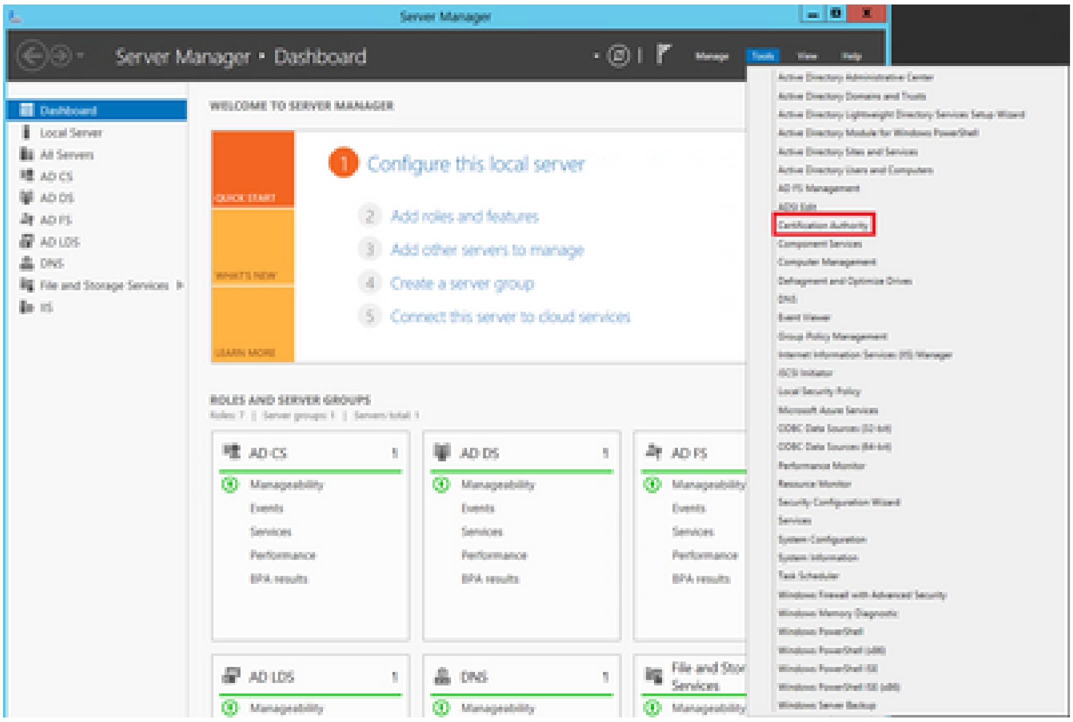
Certificado	Uso de chave X.509	Uso Estendido de Chave X.509
CallManager	·Assinatura digital ·Codificação de chaves ·Codificação de dados	·Autenticação de servidor da Web ·Autenticação de cliente Web
tomcat	·Assinatura digital ·Codificação de chaves ·Codificação de dados	·Autenticação de servidor da Web ·Autenticação de cliente Web
ipsec	·Assinatura digital ·Codificação de chaves ·Codificação de dados	·Autenticação de servidor da Web ·Autenticação de cliente Web ·Sistema final IPsec

CAPF	·Assinatura digital ·Assinatura de certificado ·Codificação de chaves	·Autenticação de servidor da Web ·Autenticação de cliente Web
TVS	·Assinatura digital ·Codificação de chaves ·Codificação de dados	·Autenticação de servidor da Web ·Autenticação de cliente Web

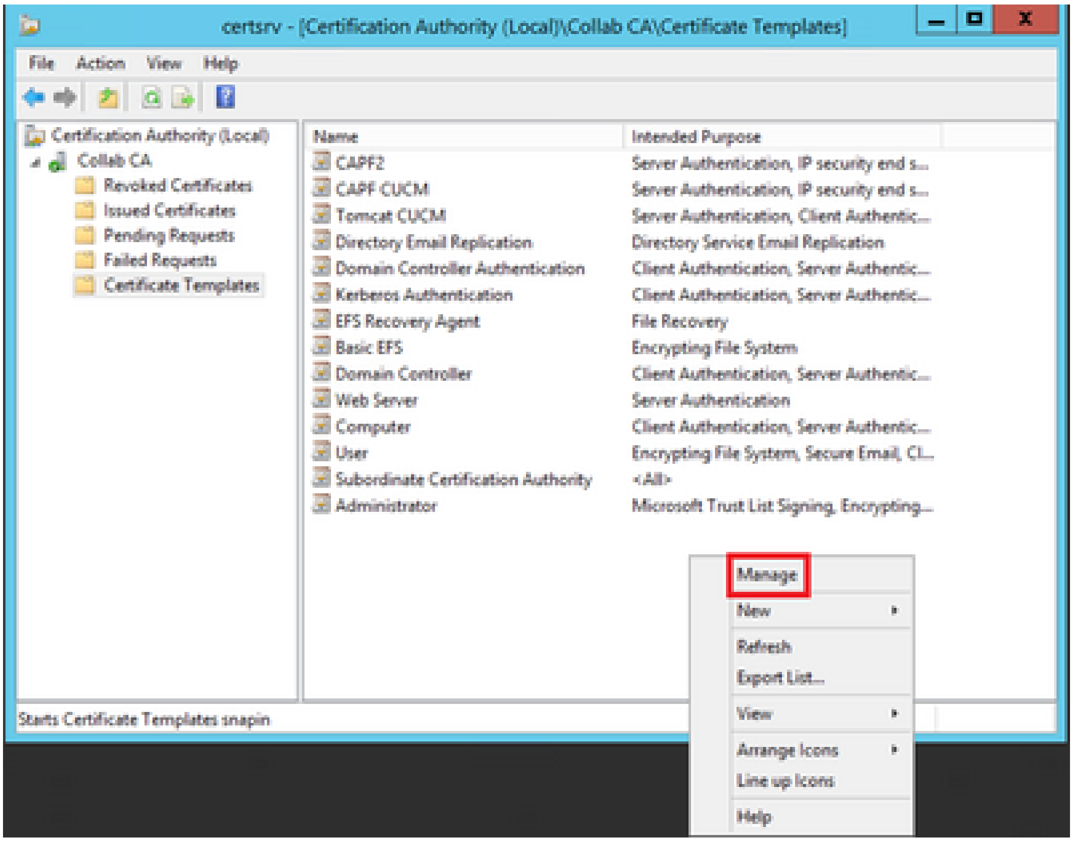
Para obter mais informações, consulte o Guia de segurança do Cisco Unified Communications Manager

Configurar

Etapa 1. No Windows Server, navegue para **Server Manager > Tools > Certification Authority**, conforme mostrado na imagem.


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
AD FS
AD LDS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
AD FS
Manageability
Events
Services
Performance
BPA results
AD LDS 1
DNS 1
File and Storage Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

Etapa 2. Selecione sua CA, navegue até **Modelos de certificado**, clique com o botão direito do mouse na lista e selecione **Gerenciar**, como mostrado na imagem.

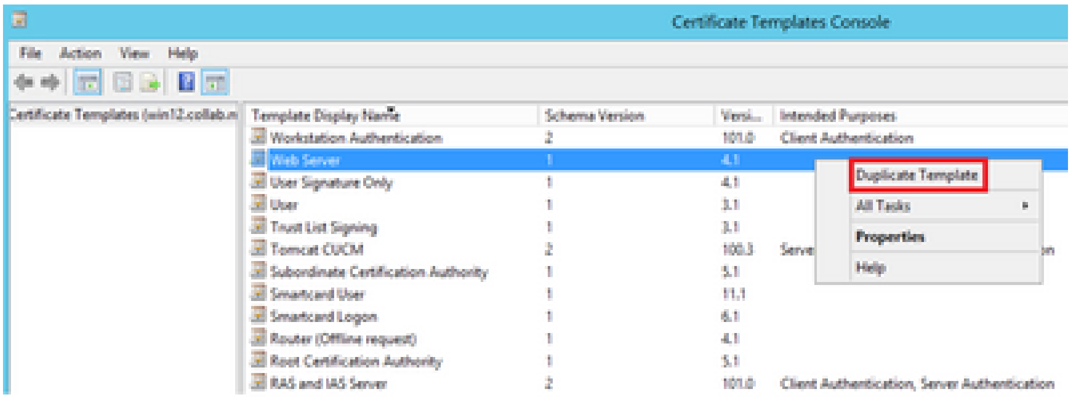


Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Modelo do Callmanager / Tomcat / TVS

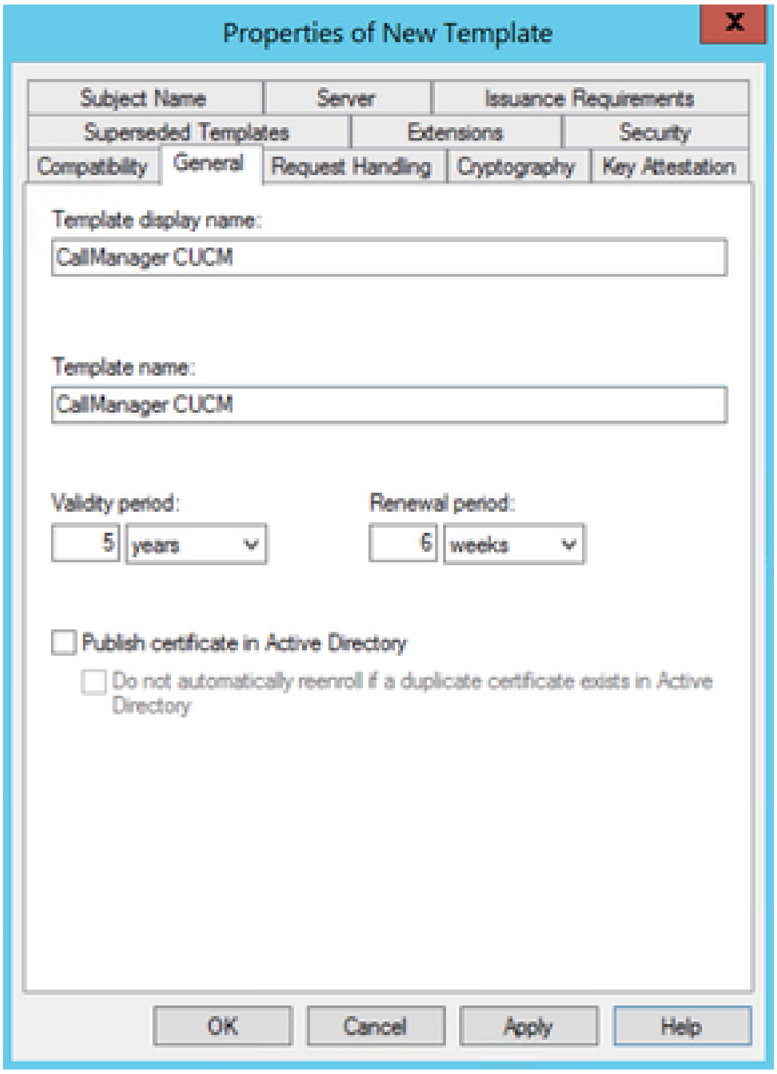
As imagens a seguir exibem apenas a criação do modelo do CallManager; mas as mesmas etapas podem ser seguidas para criar os modelos de certificado para os serviços Tomcat e TVS. A única diferença é garantir que o nome do serviço respectivo seja usado para cada novo modelo na etapa 2.

Etapa 1. Localize o modelo **Servidor Web**, clique nele com o botão direito do mouse e selecione **Modelo Duplicado**, como mostrado na imagem.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (win12.collab.n
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Schema Version	Versi...	Intended Purposes
Workstation Authentication	2	101.0	Client Authentication
Web Server	1	4.1	
User Signature Only	1	4.1	
User	1	3.1	
Trust List Signing	1	3.1	
Tomcat CUCM	2	100.3	Serve
Subordinate Certification Authority	1	5.1	
Smartcard User	1	11.1	
Smartcard Logon	1	6.1	
Router (Offline request)	1	4.1	
Root Certification Authority	1	5.1	
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication

Etapa 2. Em **Geral**, você pode alterar o nome, o nome de exibição, a validade, etc. do modelo de certificado.



Template display name: CallManager CUCM

Template name: CallManager CUCM

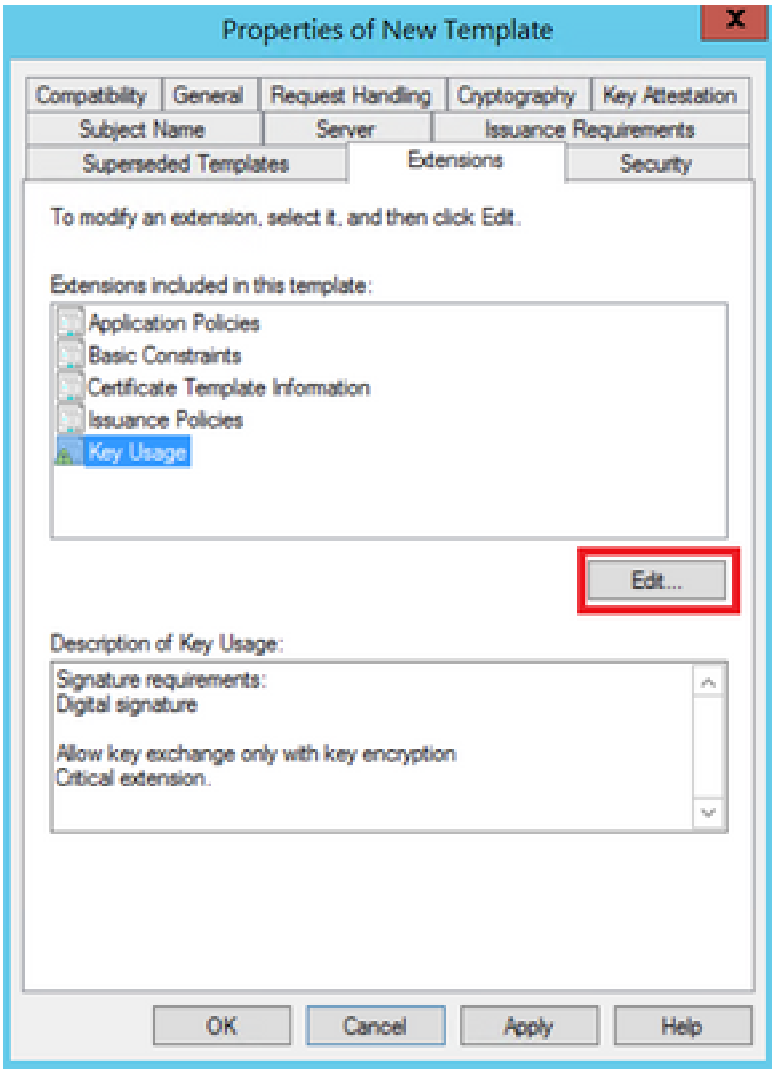
Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

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

Etapa 3. Navegue até **Extensions > Key Usage > Edit**, conforme mostrado na imagem.



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

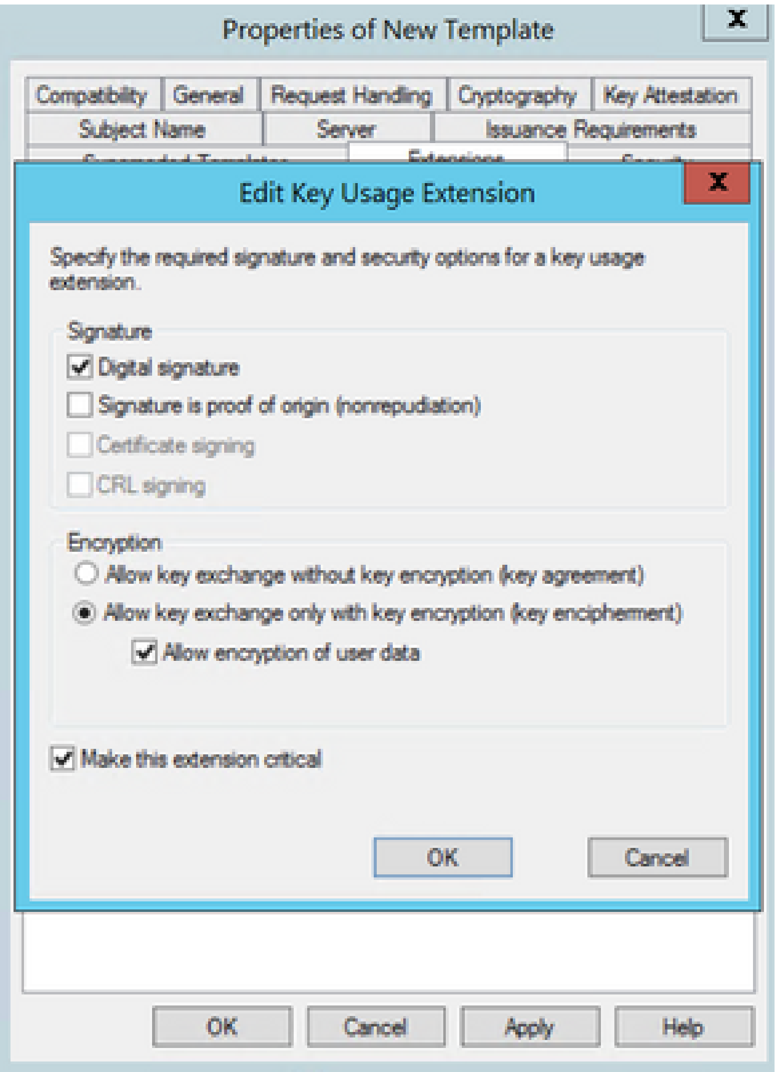
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Etapa 4. Selecione essas opções e selecione **OK**, como mostrado na imagem.

- **Assinatura digital**
- **Permitir troca de chaves somente com criptografia de chave (codificação de chave)**
- **Permitir criptografia de dados do usuário**



Properties of New Template

Compatibility | General | Request Handling | Cryptography | Key Attestation

Subject Name | Server | Issuance Requirements

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

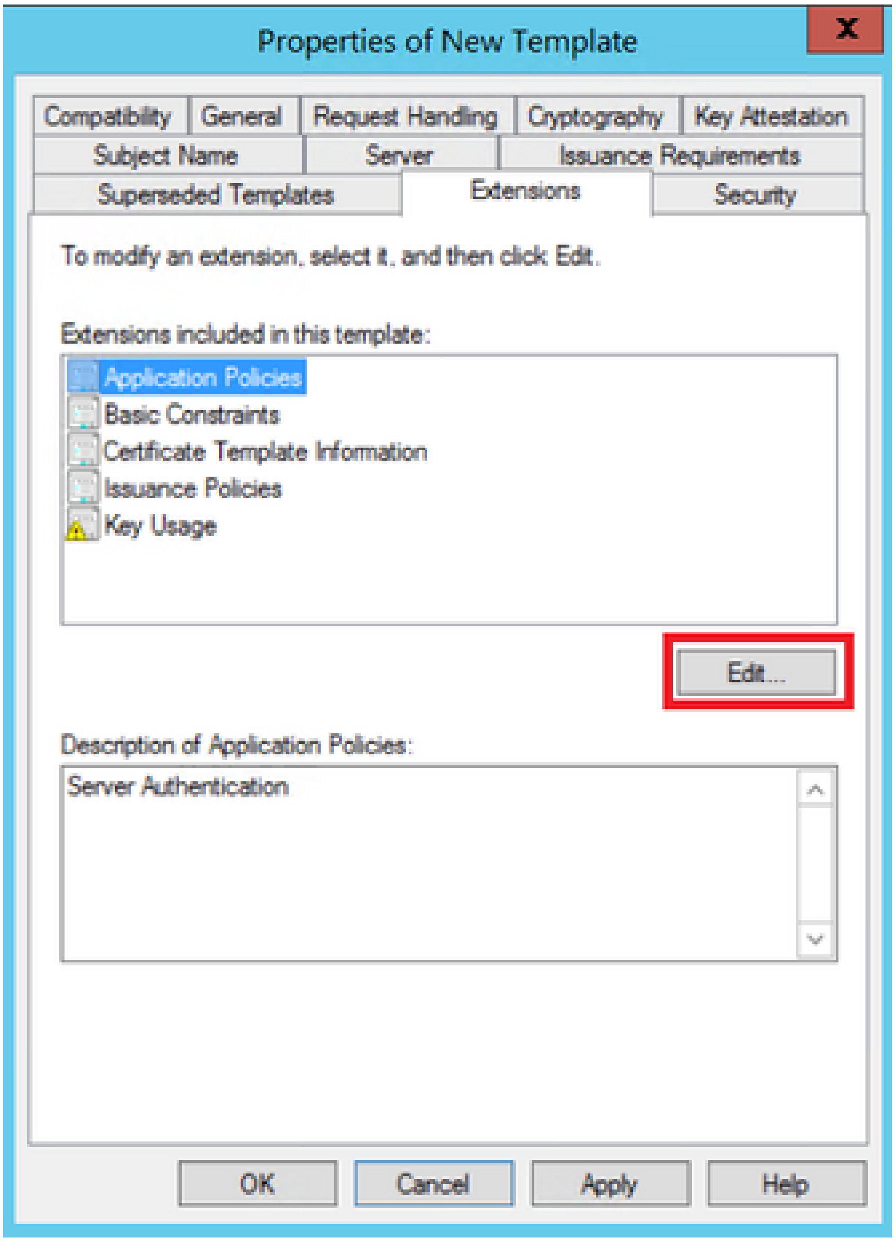
○ Allow key exchange without key encryption (key agreement)

● Allow key exchange only with key encryption (key encipherment)

☑ Allow encryption of user data

☑ Make this extension critical

Etapa 5. Navegue para **Extensões > Políticas de aplicativo > Editar > Adicionar**, como mostrado na imagem.



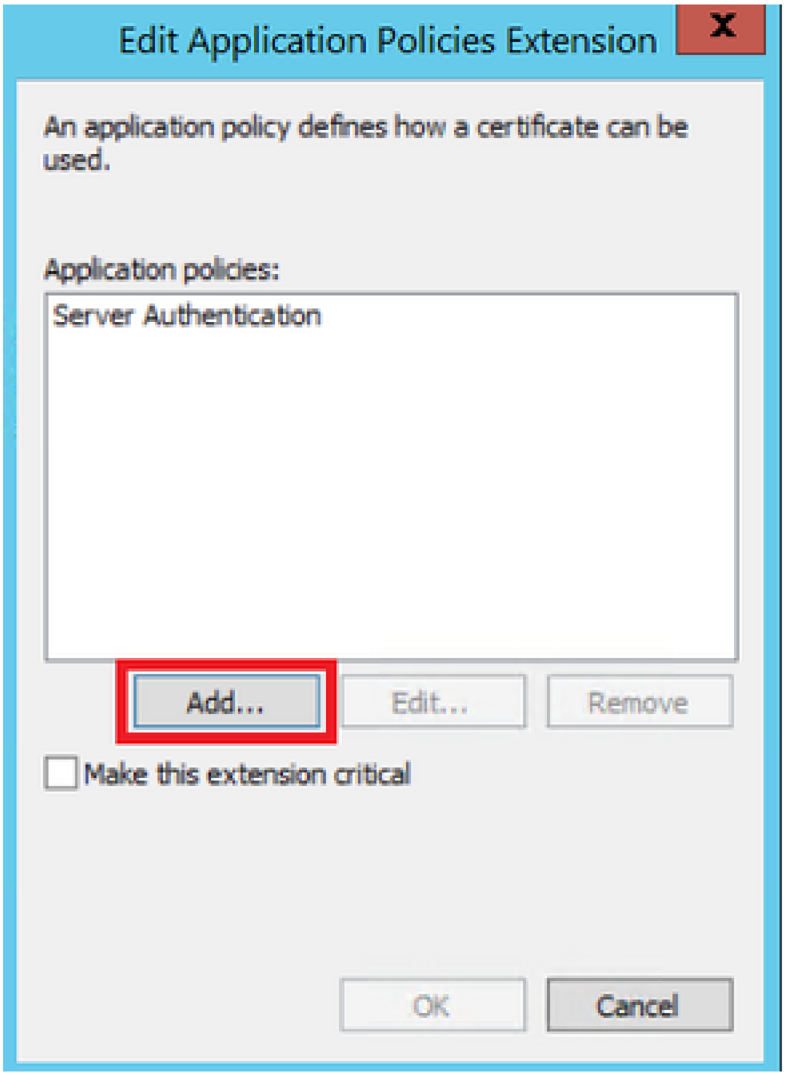
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



Edit Application Policies Extension

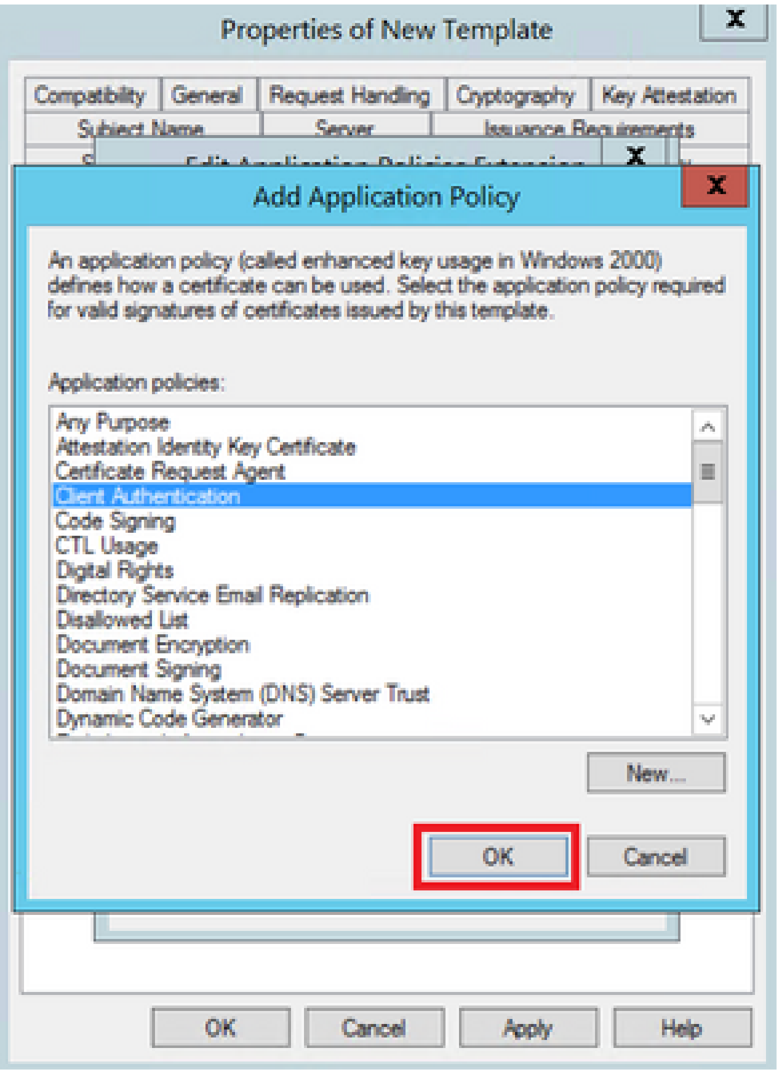
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

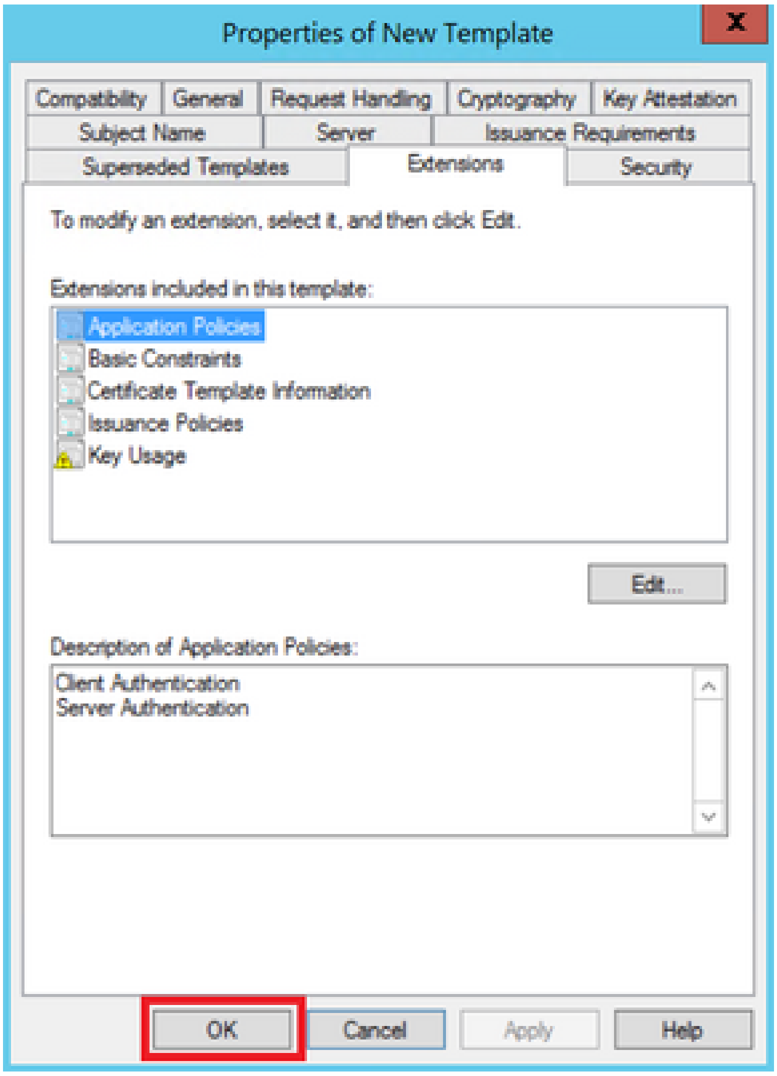
□ Make this extension critical

Etapa 6. Pesquise a **autenticação do cliente,** selecione-a e selecione **OK** nesta janela e na anterior, conforme mostrado na imagem.



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.

Passo 7. De volta ao modelo, selecione **Aplicar** e, em seguida, **OK.**



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.

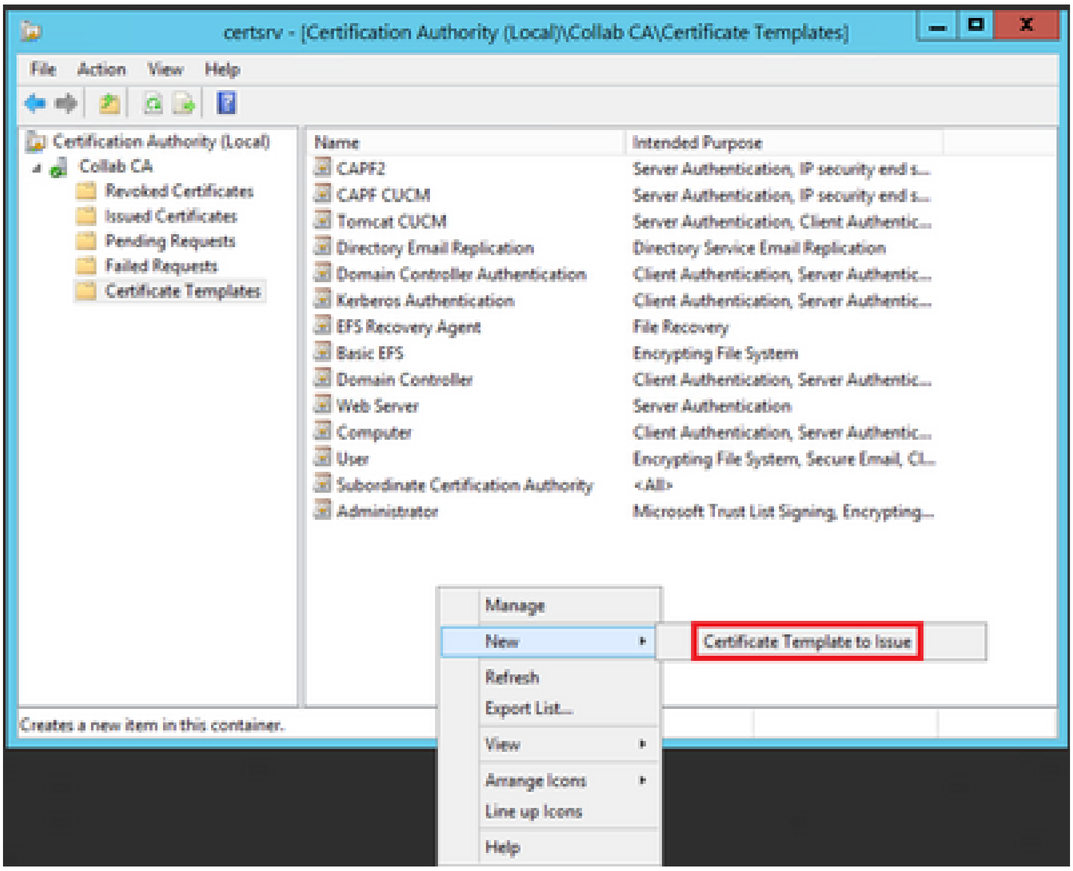
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
Server Authentication

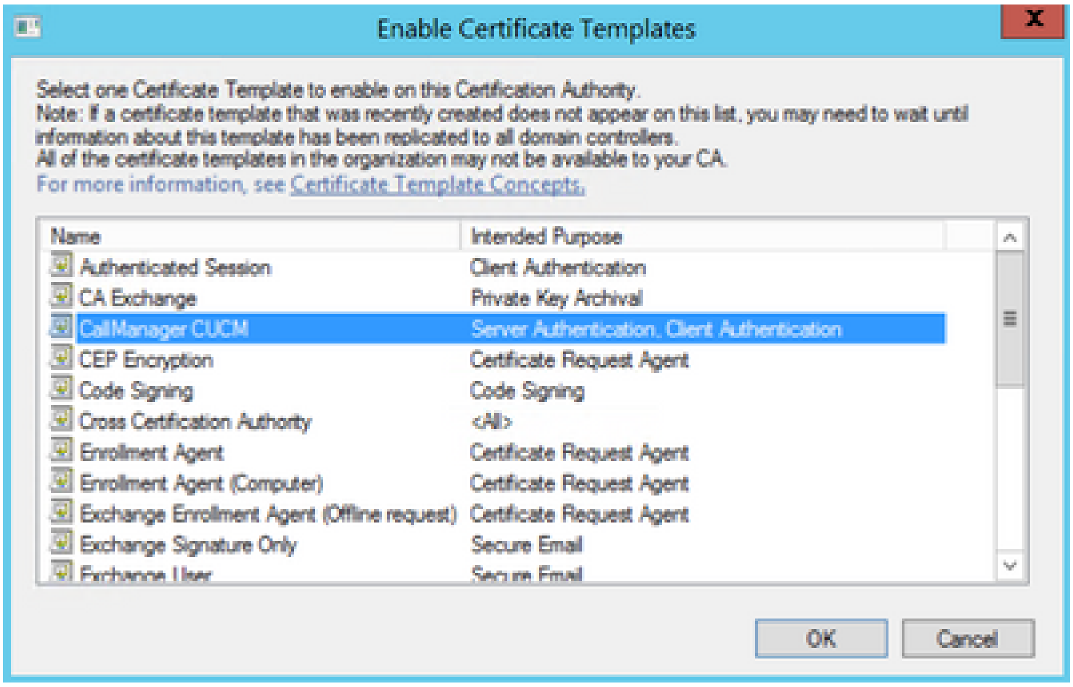
Etapa 8. Feche a janela **Console do modelo de certificado** e, na primeira janela, navegue para **Novo > Modelo de certificado a ser emitido**, como mostrado na imagem.



Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Creates a new item in this container.

Etapa 9. Selecione o novo modelo **CallManager CUCM** e selecione **OK**, como mostrado na imagem.



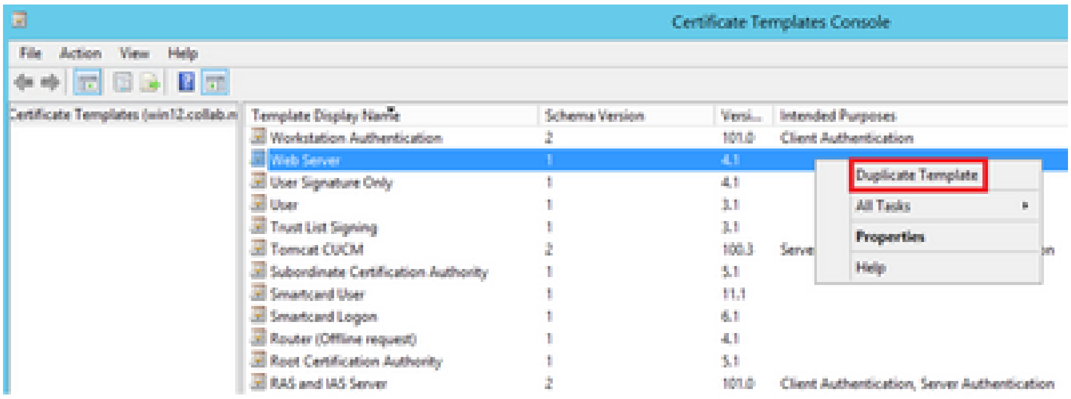
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CallManager CUCM	Server Authentication, Client Authentication
CEP Encryption	Certificate Request Agent
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email

Etapa 10. Repita todas as etapas anteriores para criar modelos de certificado para os serviços Tomcat e TVS, conforme necessário.

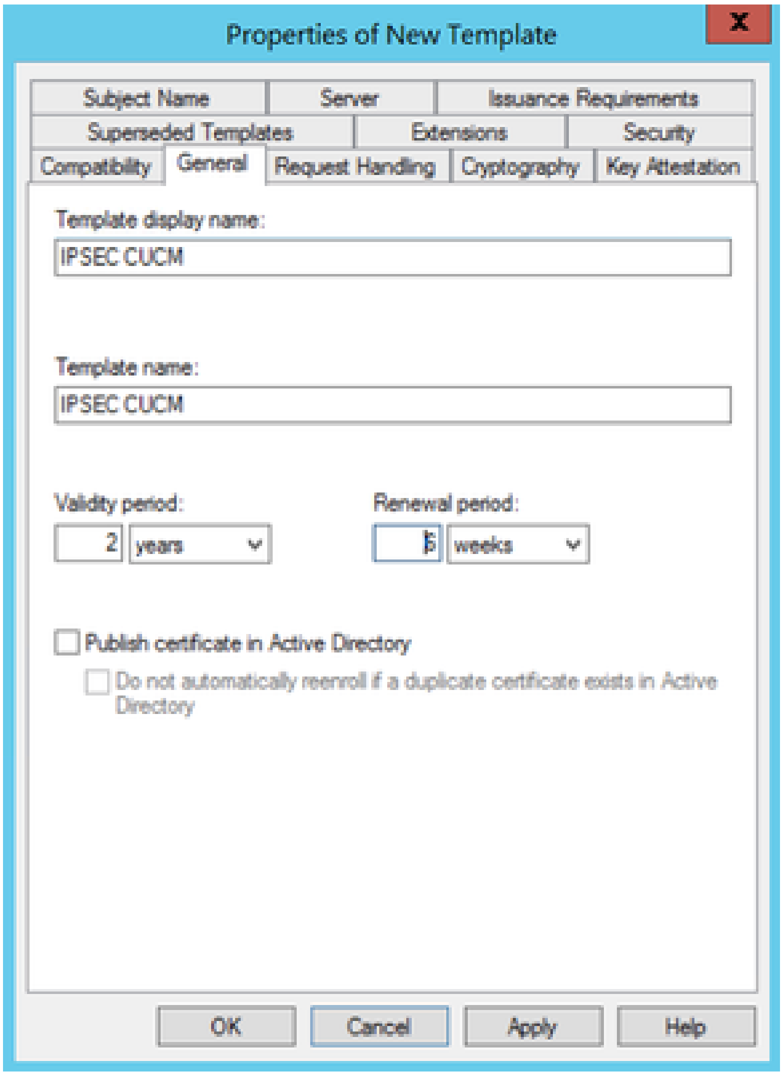
Modelo de IPsec

Etapa 1. Localize o modelo **Servidor Web**, clique nele com o botão direito do mouse e selecione **Modelo Duplicado**, como mostrado na imagem.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (win12.collab.n
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Schema Version	Versi...	Intended Purposes
Workstation Authentication	2	101.0	Client Authentication
Web Server	1	4.1	
User Signature Only	1	4.1	
User	1	3.1	
Trust List Signing	1	3.1	
Tomcat CUCM	2	100.3	Serve
Subordinate Certification Authority	1	5.1	
Smartcard User	1	11.1	
Smartcard Logon	1	6.1	
Router (Offline request)	1	4.1	
Root Certification Authority	1	5.1	
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication

Etapa 2. Em **Geral**, você pode alterar o nome, o nome de exibição, a validade, etc. do modelo de certificado.



Template display name: IPSEC CUCM

Template name: IPSEC CUCM

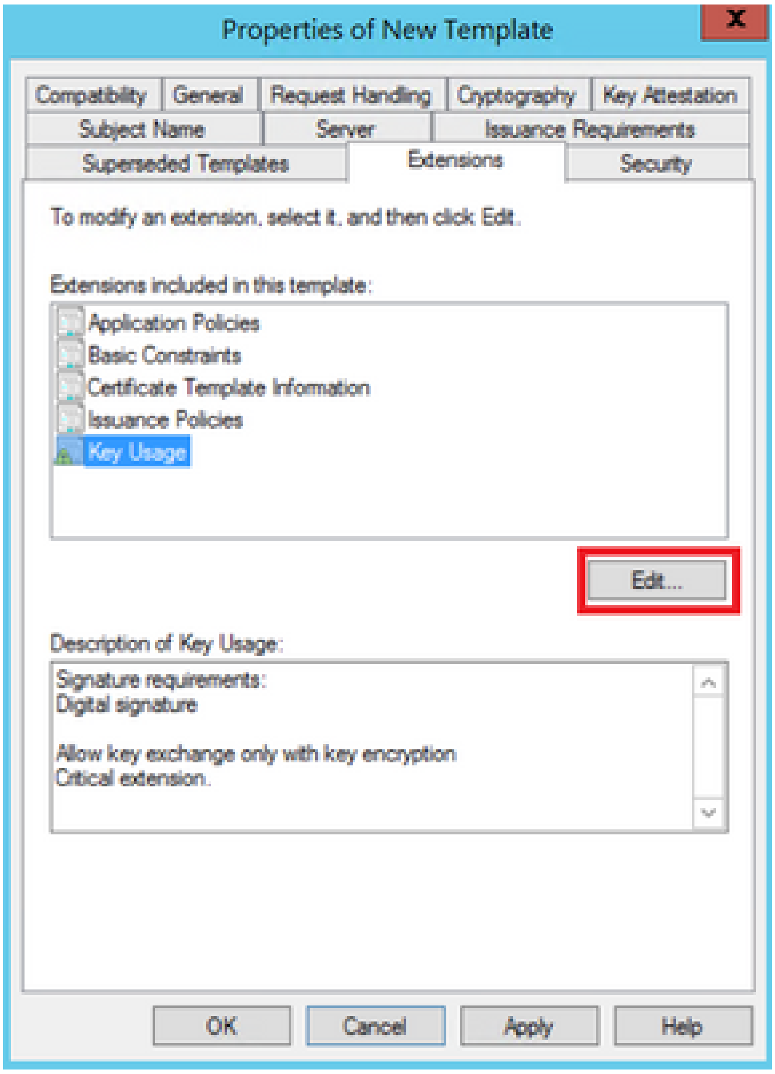
Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

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

Etapa 3. Navegue até **Extensions > Key Usage > Edit**, conforme mostrado na imagem.



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

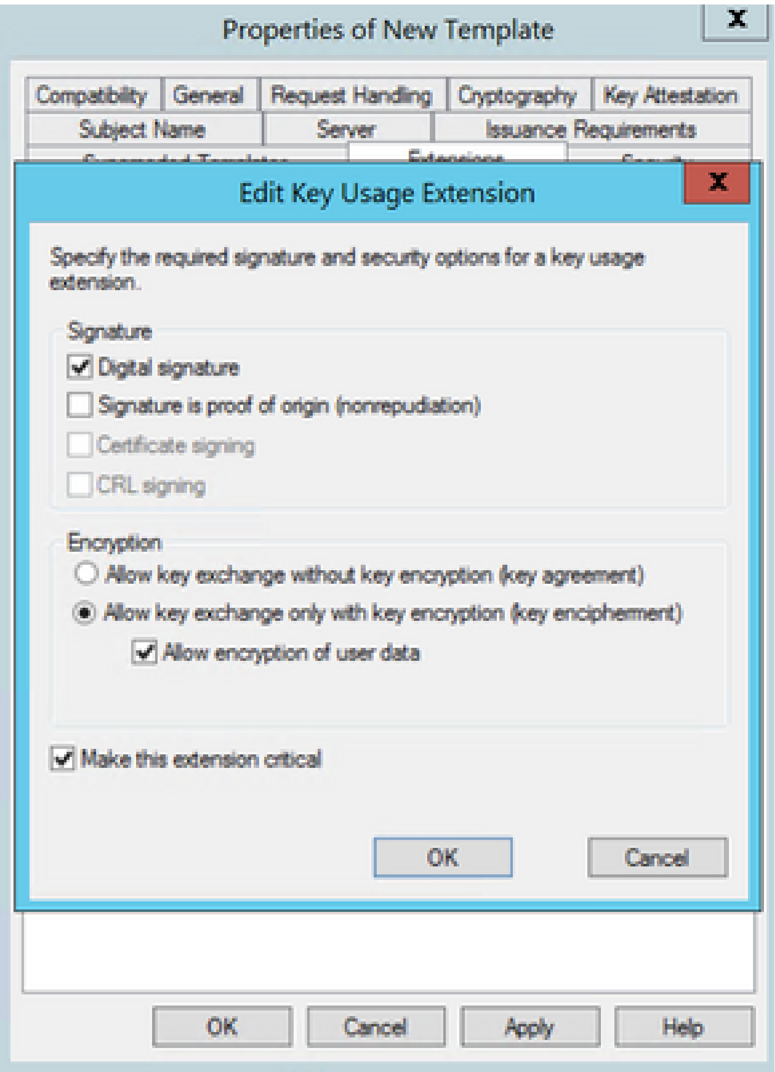
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Etapa 4. Selecione essas opções e selecione **OK**, como mostrado na imagem.

- **Assinatura digital**
- **Permitir troca de chaves somente com criptografia de chave (codificação de chave)**
- **Permitir criptografia de dados do usuário**



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

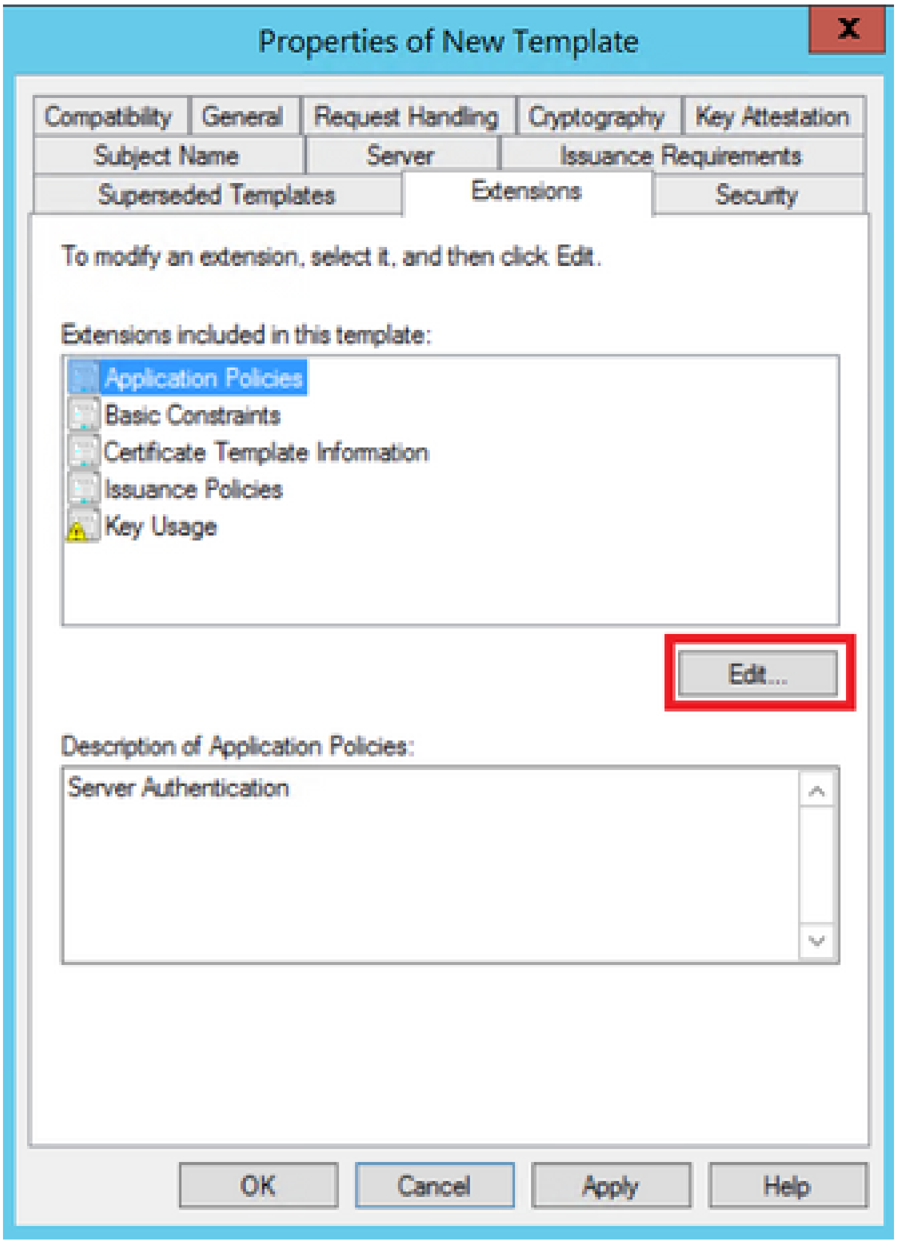
○ Allow key exchange without key encryption (key agreement)

● Allow key exchange only with key encryption (key encipherment)

☑ Allow encryption of user data

☑ Make this extension critical

Etapa 5. Navegue para **Extensões > Políticas de aplicativo > Editar > Adicionar**, como mostrado na imagem.



Properties of New Template

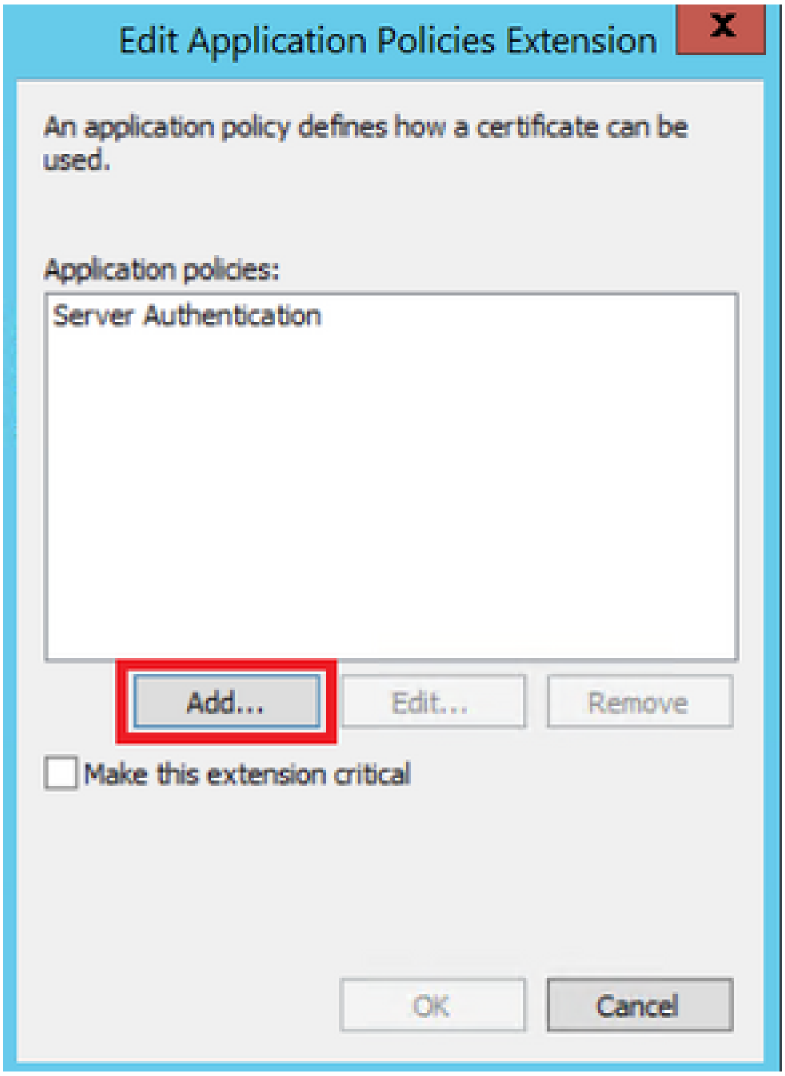
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication

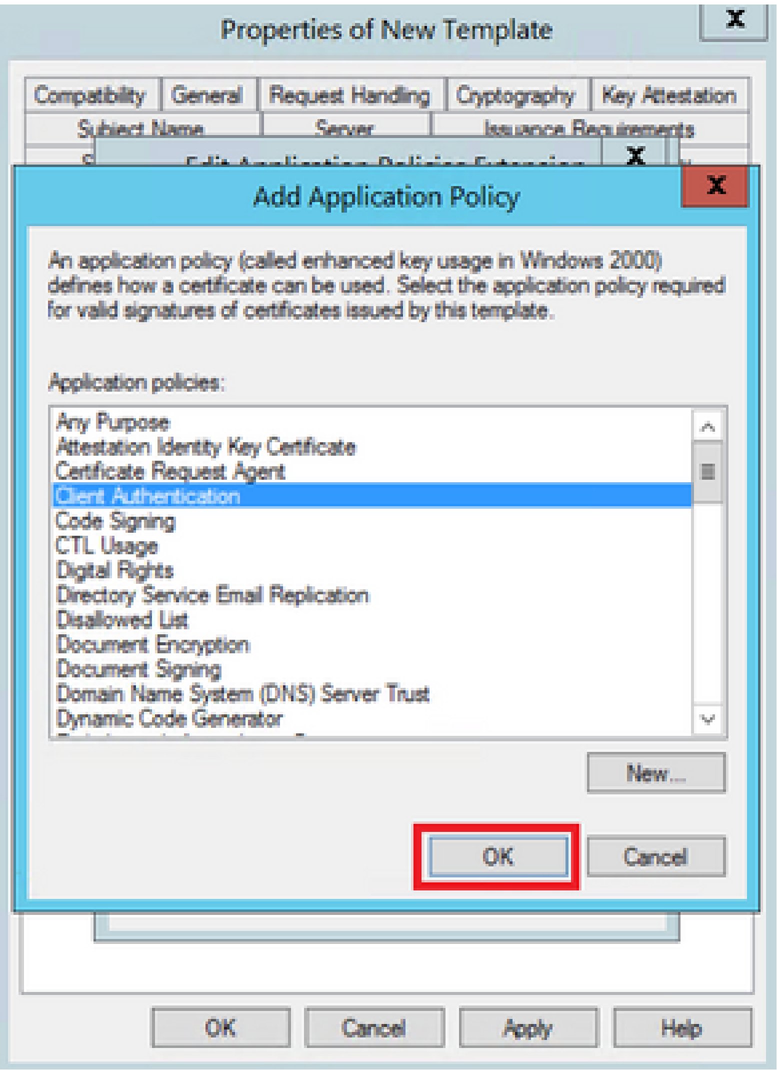


An application policy defines how a certificate can be used.

Application policies:
Server Authentication

□ Make this extension critical

Etapa 6. Procure a **autenticação do cliente,** selecione-a e, em seguida, **OK**, como mostrado na imagem.

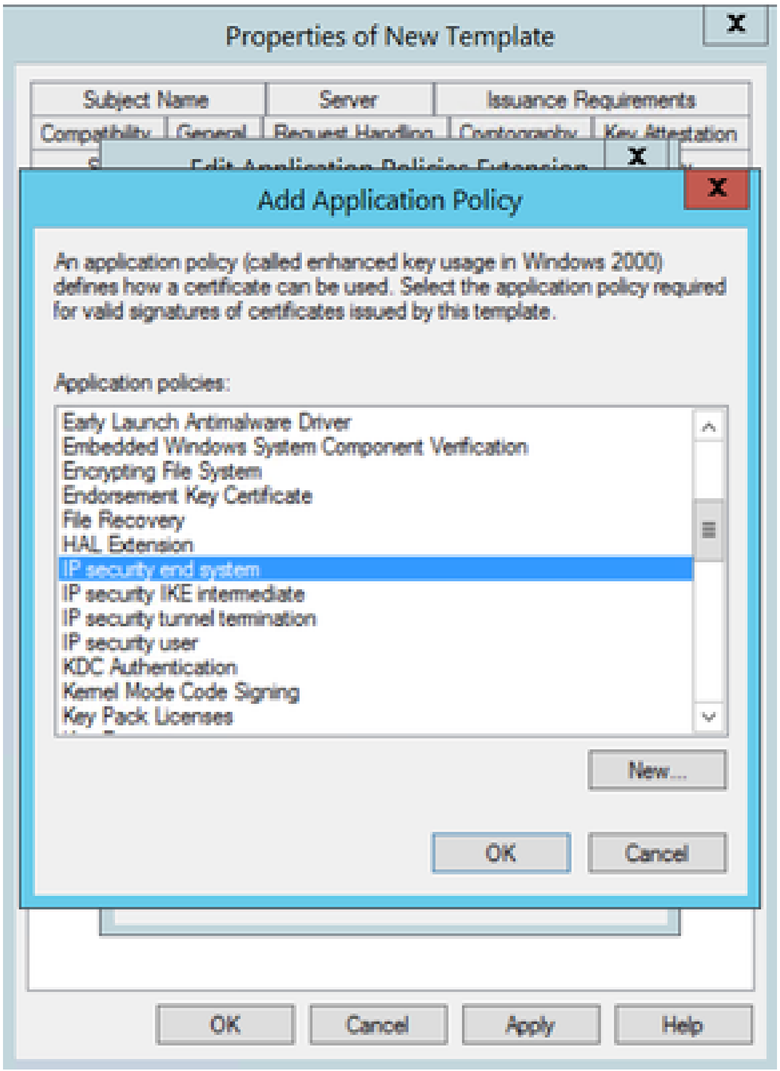


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Passo 7. Selecione **Add** novamente, procure **IP security end system**, selecione-o e selecione **OK** nesta e na janela anterior também.

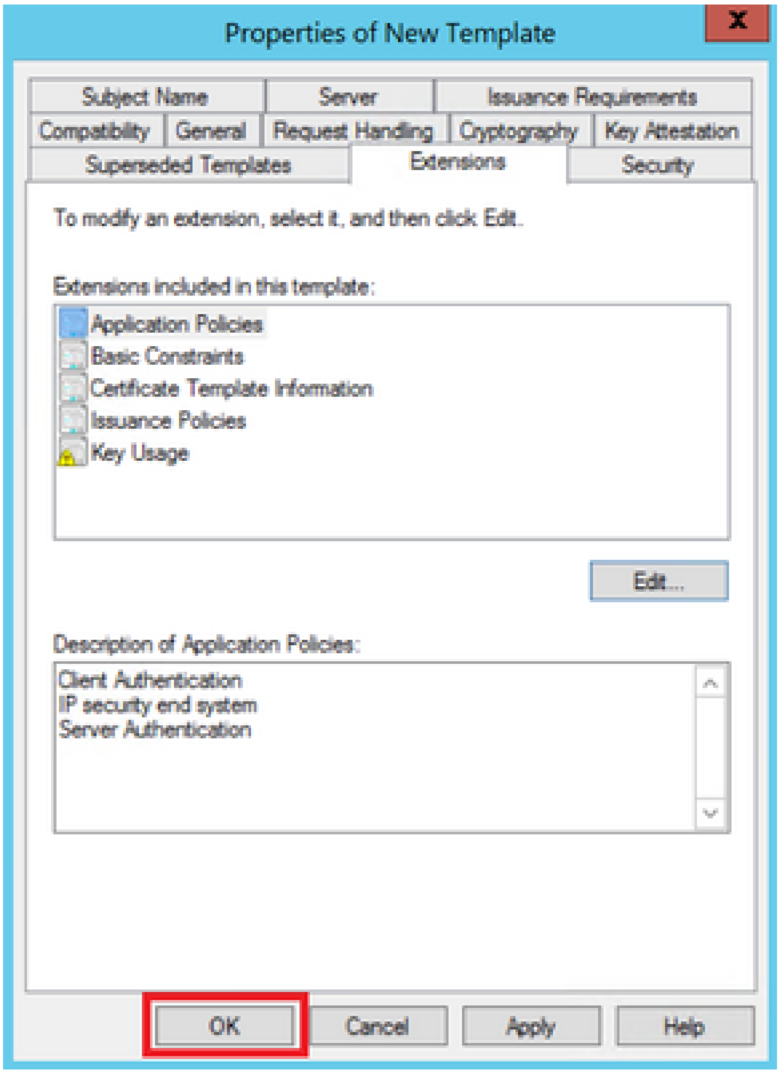


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

- Early Launch Antimalware Driver
- Embedded Windows System Component Verfication
- 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

Etapa 8. De volta ao modelo, selecione **Apply** e, em seguida, **OK**, como mostrado na imagem.



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

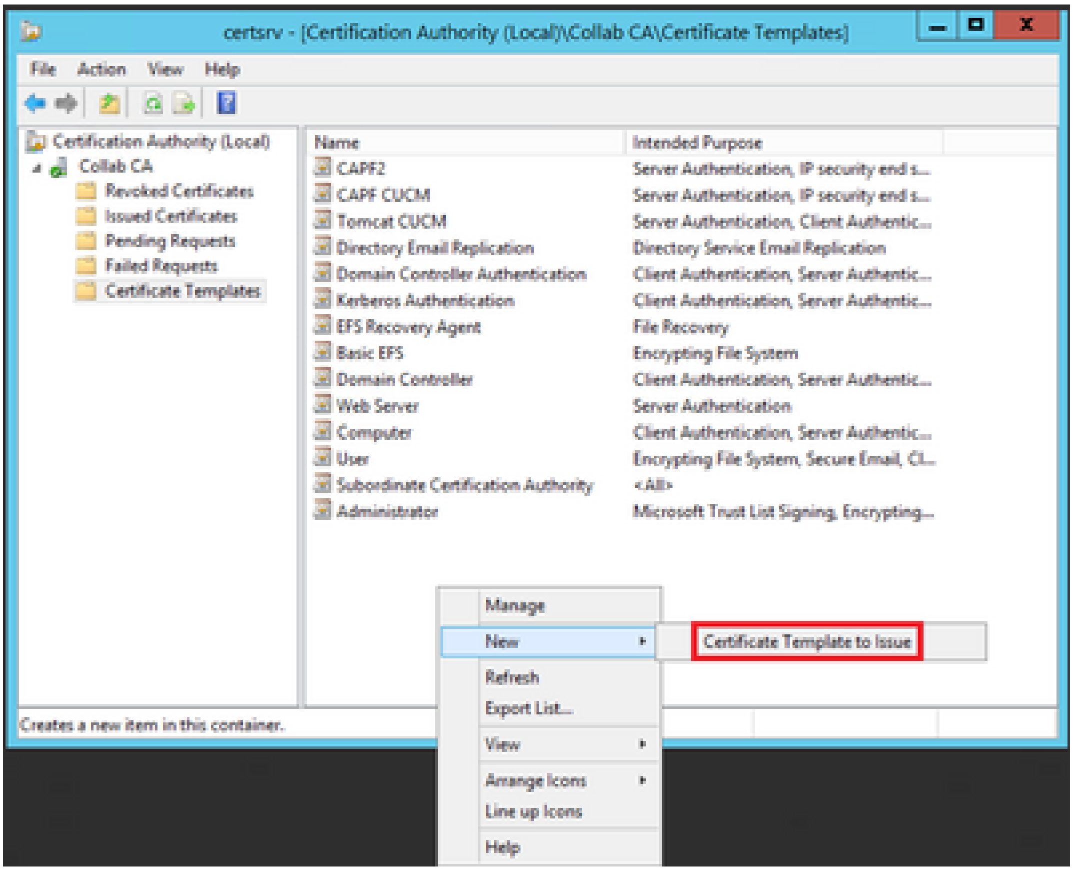
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
IP security end system
Server Authentication

Etapa 9. Feche a janela **Console de modelos de certificado** e, na primeira janela, navegue para **Novo > Modelo de certificado a ser emitido**, como mostrado na imagem.

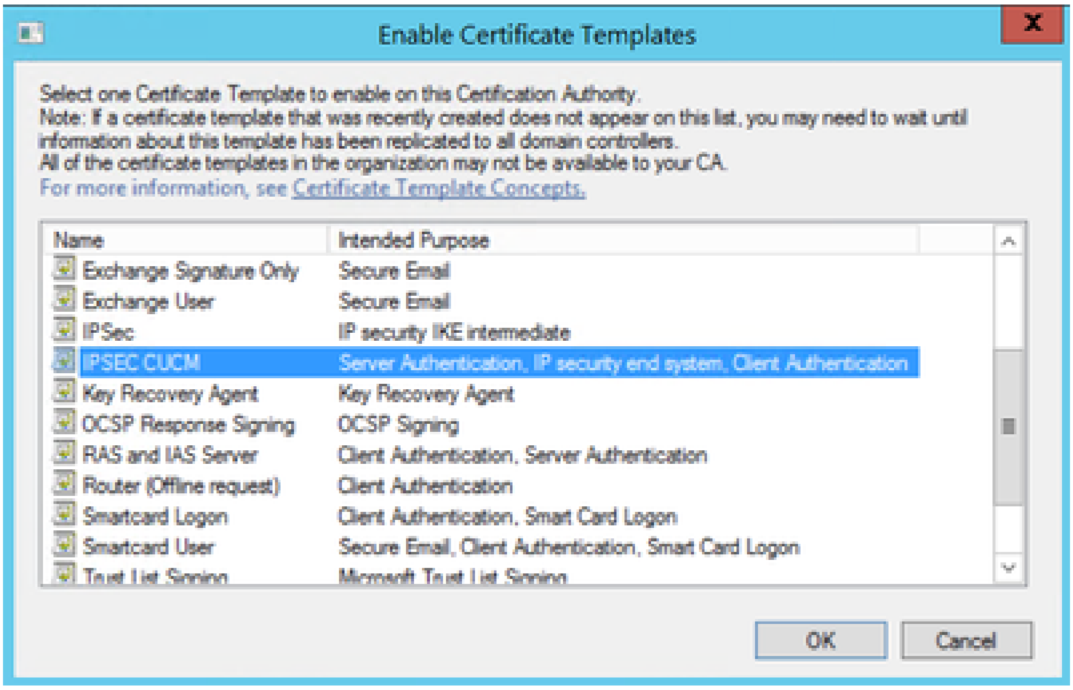


certsrv - [Certification Authority (Local)\Collab CA\Certificate Templates]

Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Creates a new item in this container.

Etapa 10. Selecione o novo modelo **IPSEC CUCM** e selecione **OK**, como mostrado na imagem.



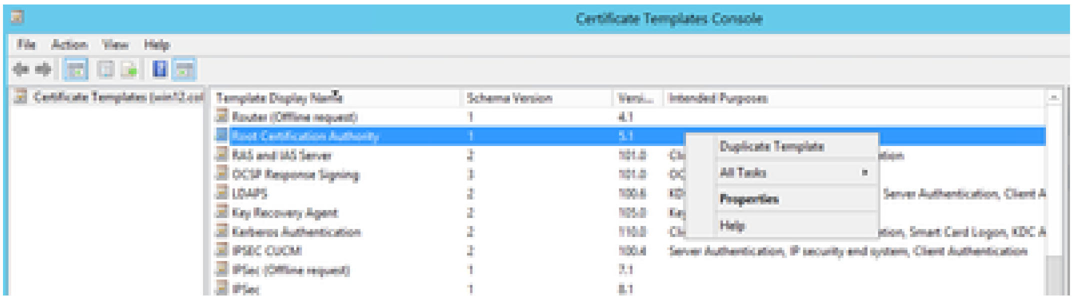
Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermediate
IPSEC CUCM	Server Authentication, IP security end system, Client Authentication
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing

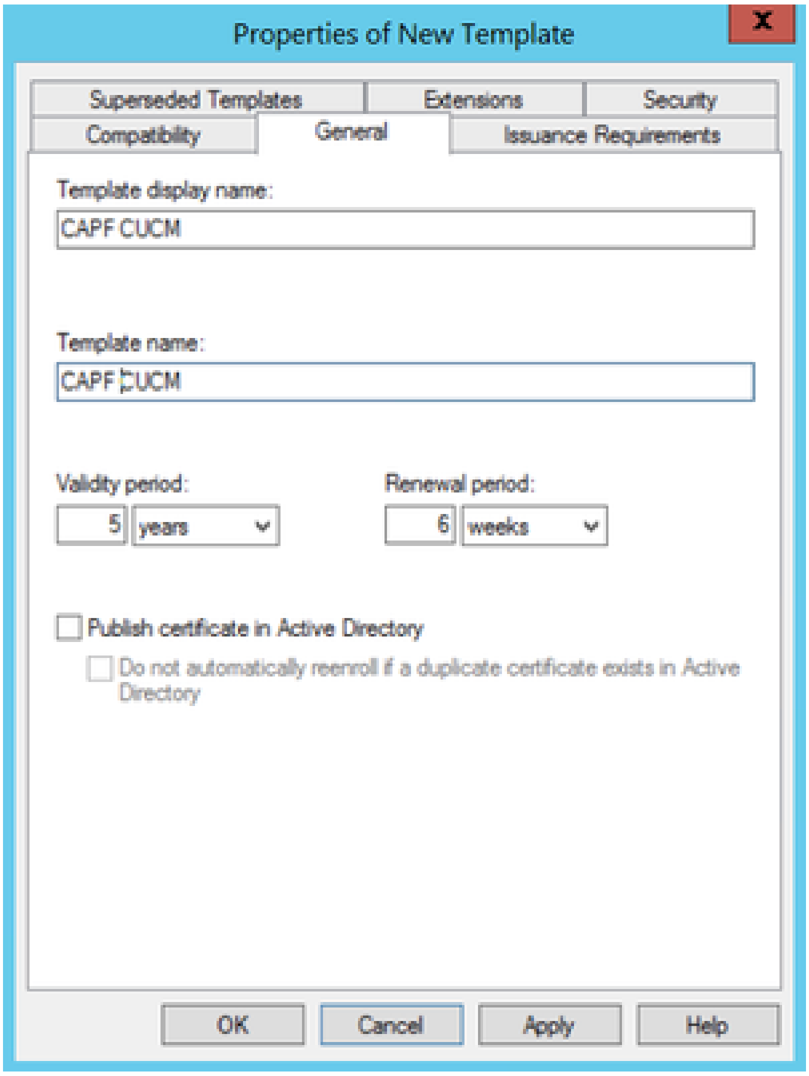
Modelo CAPF

Etapa 1. Localize o modelo **CA raiz** e clique nele com o botão direito do mouse. Em seguida, selecione **Duplicar modelo**, como mostrado na imagem.



Template Display Name	Schema Version	Versi...	Intended Purposes
Router (Offline request)	1	4.1	
Root Certification Authority	1	5.1	
RAS and IAS Server	2	101.0	Cli ... ation
OCSP Response Signing	3	101.0	OC
LDAPS	2	100.6	KD ... Server Authentication, Client A
Key Recovery Agent	2	105.0	Key
Kerberos Authentication	2	110.0	Cli ... ation, Smart Card Logon, KDC A
IPSEC CUCM	2	100.4	Server Authentication, IP security end system, Client Authentication
IPSec (Offline request)	1	7.1	
IPSec	1	8.1	

Etapa 2. Em **Geral**, você pode alterar o nome, o nome de exibição, a validade, etc. do modelo de certificado.



Template display name: CAPF CUCM

Template name: CAPF CUCM

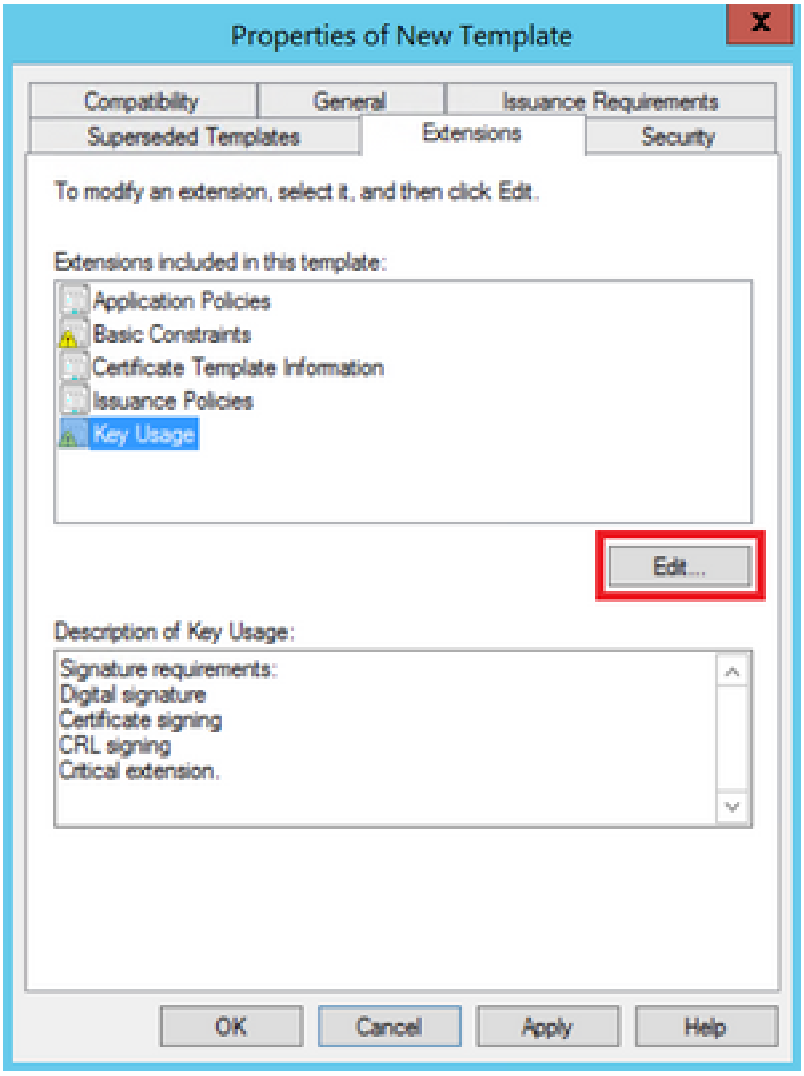
Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

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

Etapa 3. Navegue até **Extensions > Key Usage > Edit**, conforme mostrado na imagem.



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

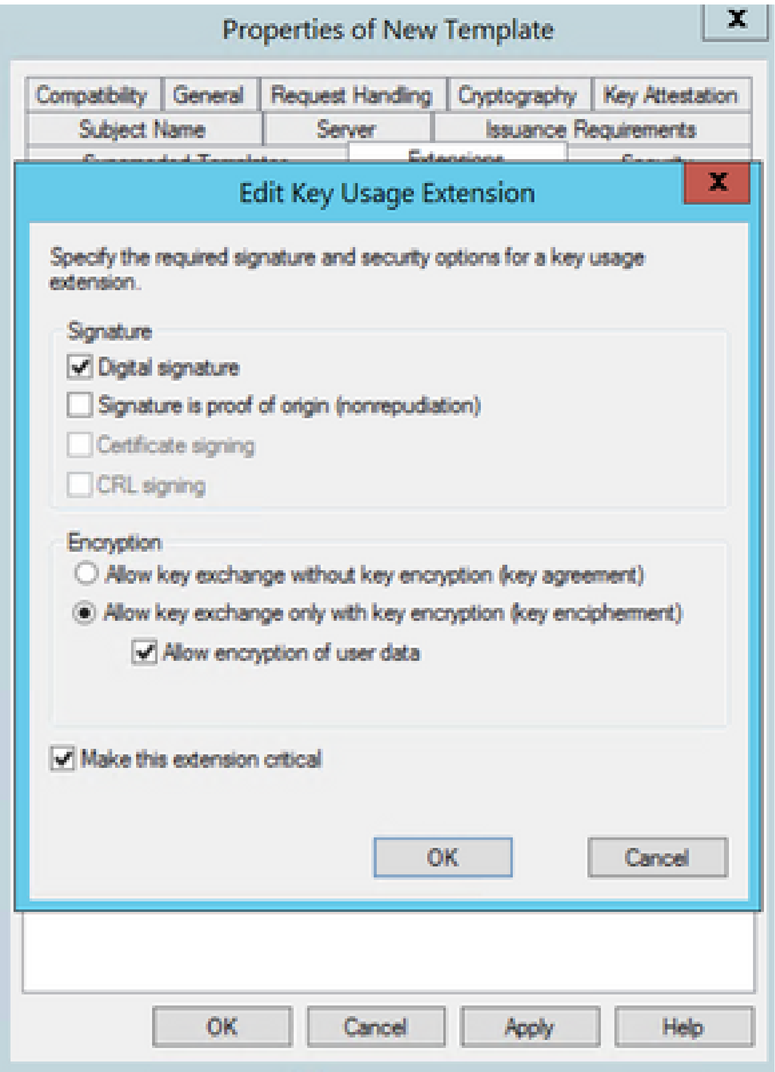
Extensions included in this template:

Description of Key Usage:

Signature requirements:
Digital signature
Certificate signing
CRL signing
Critical extension.

Etapa 4. Selecione essas opções e selecione **OK**, como mostrado na imagem.

- **Assinatura digital**
- **Assinatura de certificado**
- **Assinatura de CRL**



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

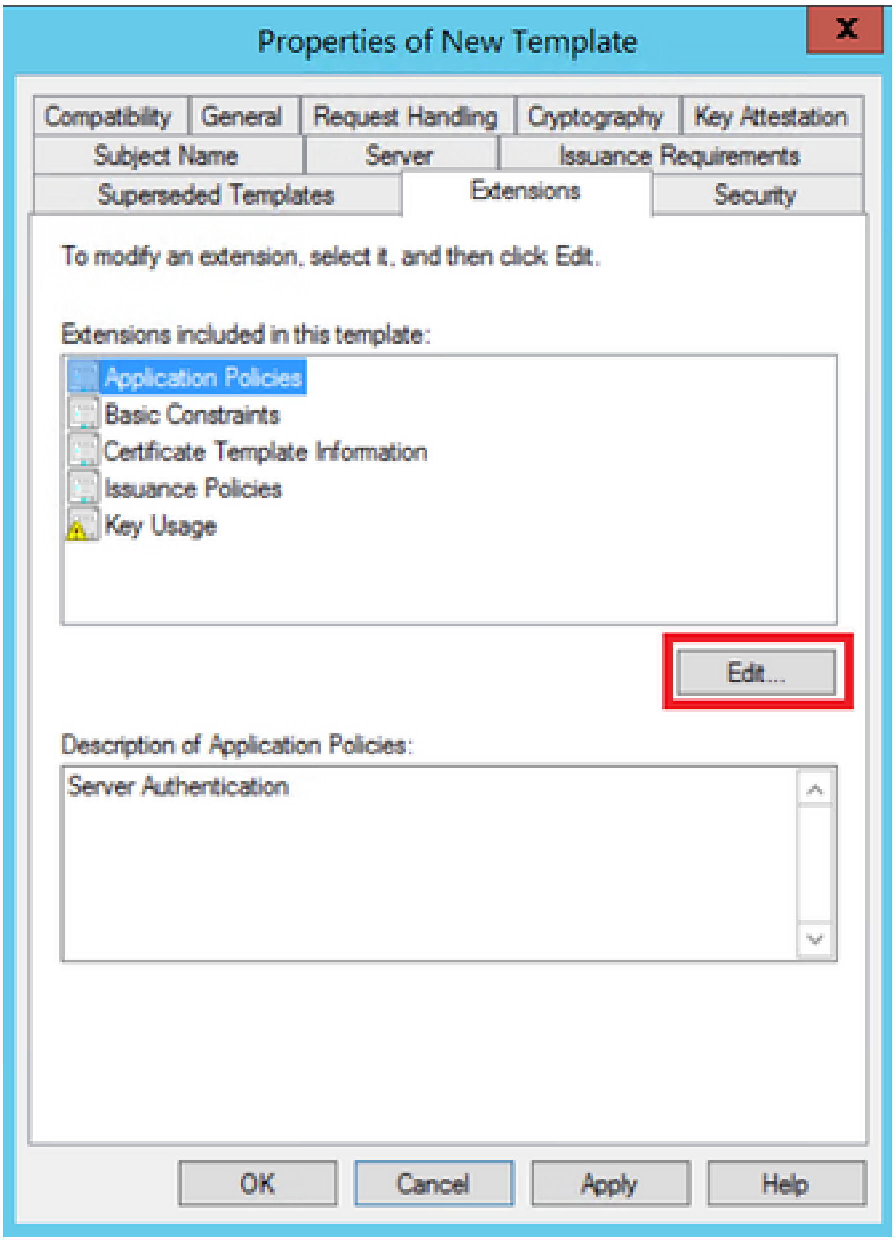
○ Allow key exchange without key encryption (key agreement)

● Allow key exchange only with key encryption (key encipherment)

☑ Allow encryption of user data

☑ Make this extension critical

Etapa 5. Navegue para **Extensões > Políticas de aplicativo > Editar > Adicionar**, como mostrado na imagem.



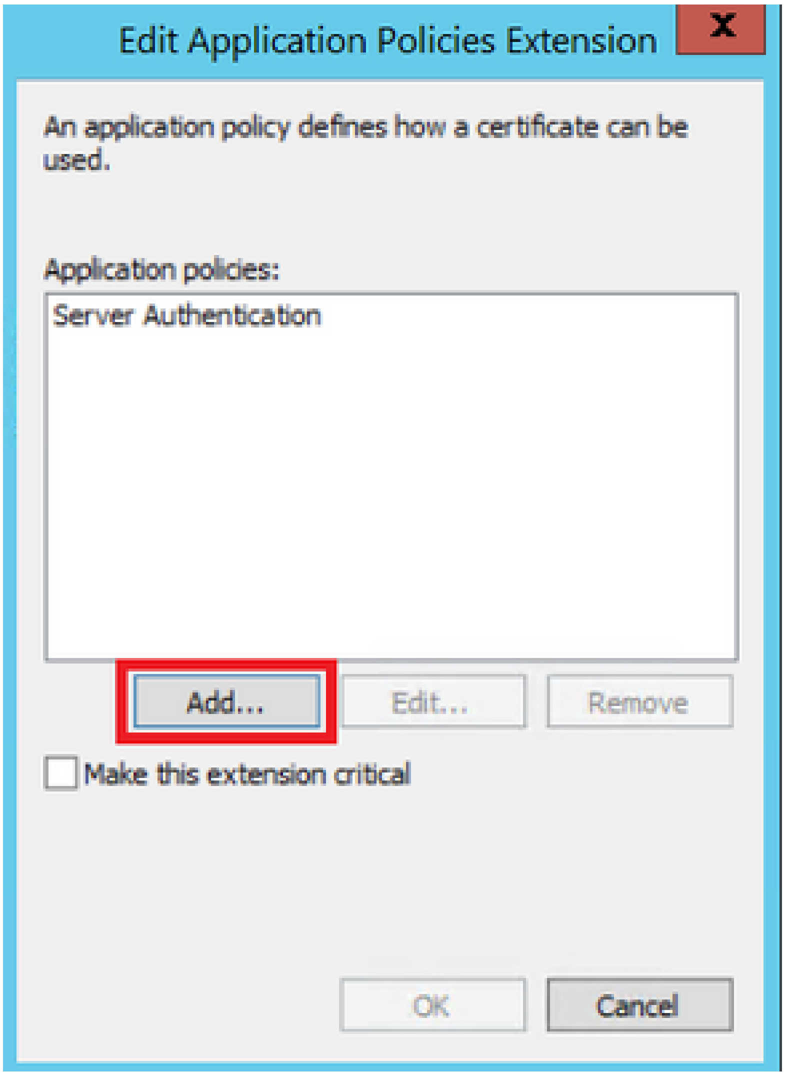
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



Edit Application Policies Extension

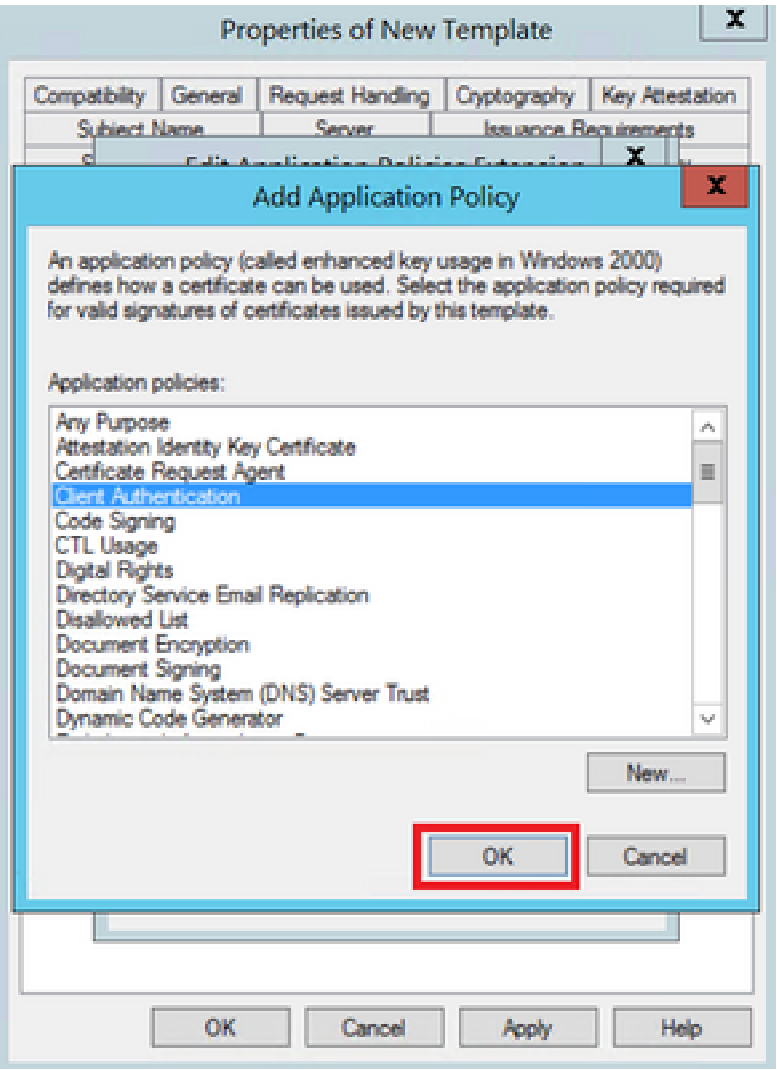
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

Etapa 6. Procure a **autenticação do cliente,** selecione-a e, em seguida, **OK**, como mostrado na imagem.

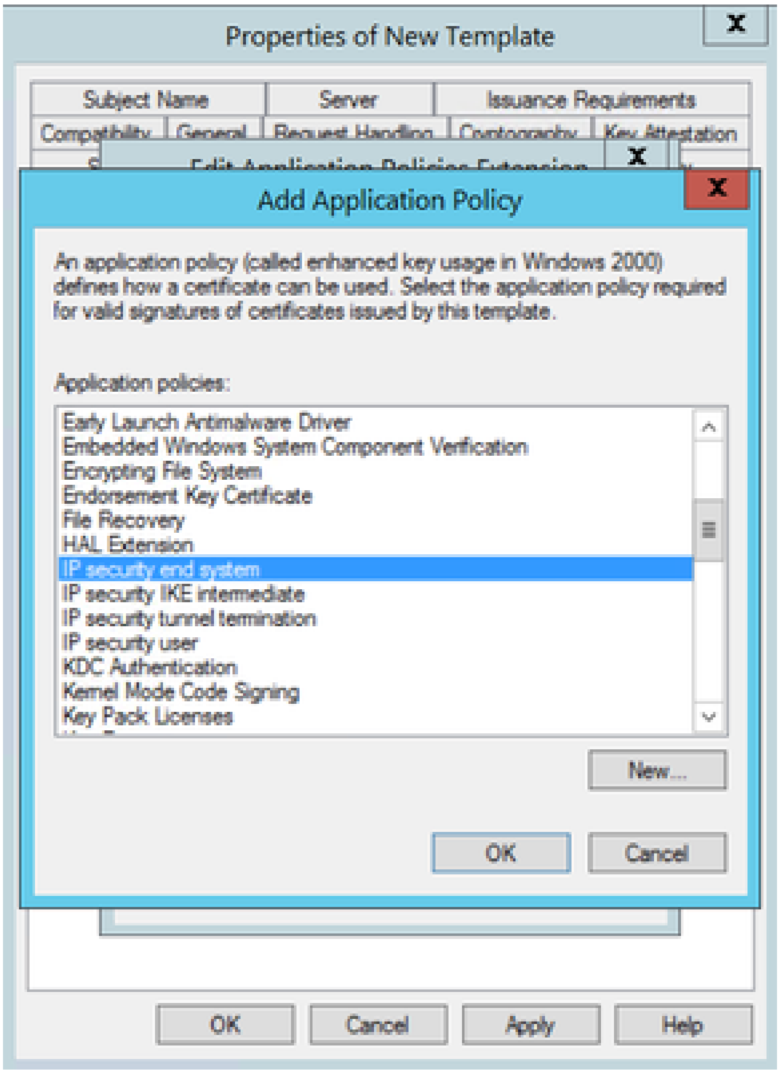


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Passo 7. Selecione **Add** novamente, procure **IP security end system**, selecione-o e depois selecione OK nesta e na janela anterior também, como mostrado na imagem.

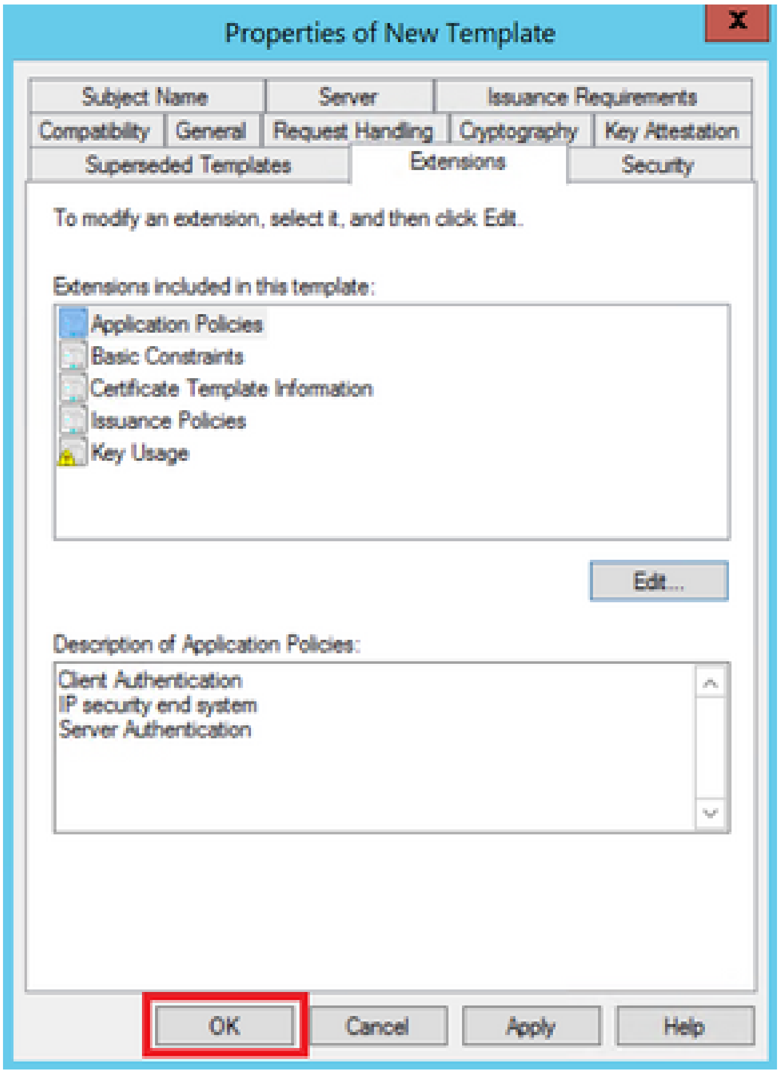


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Etapa 8. De volta ao modelo, selecione **Apply** e, em seguida, **OK**, como mostrado na imagem.



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

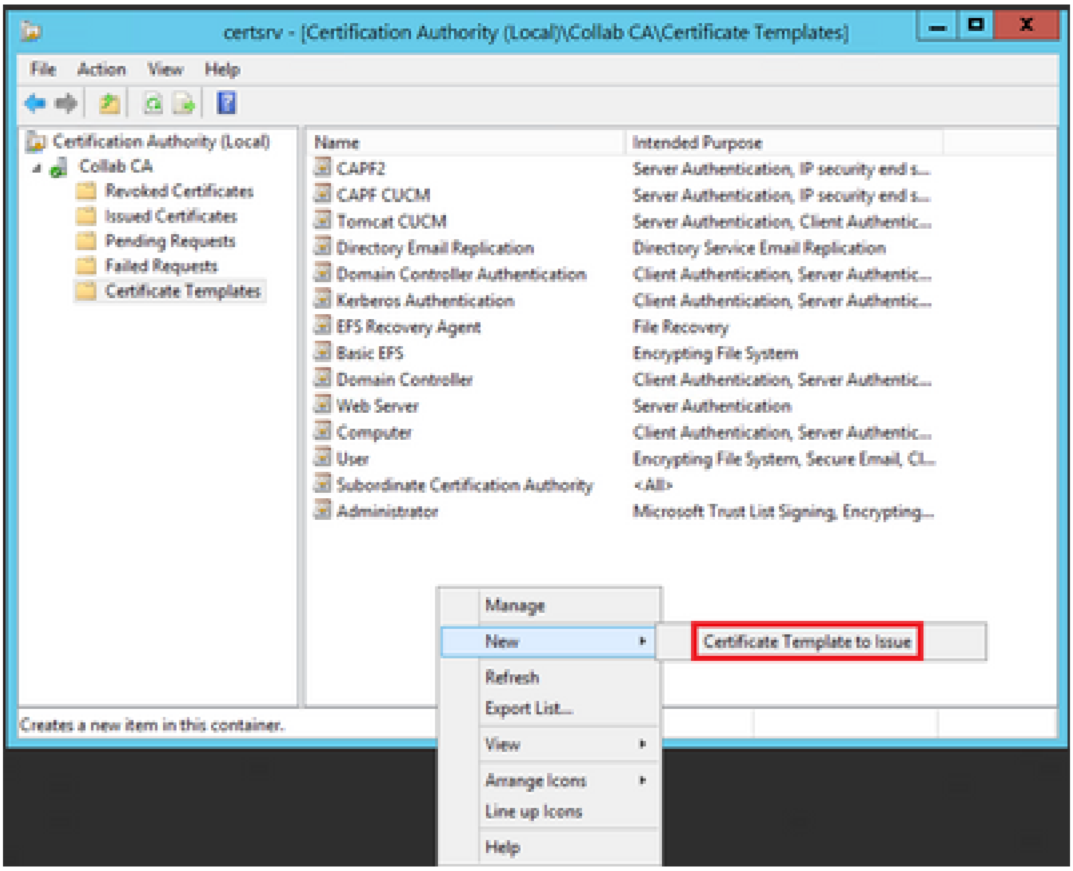
Extensions included in this template:

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

Description of Application Policies:

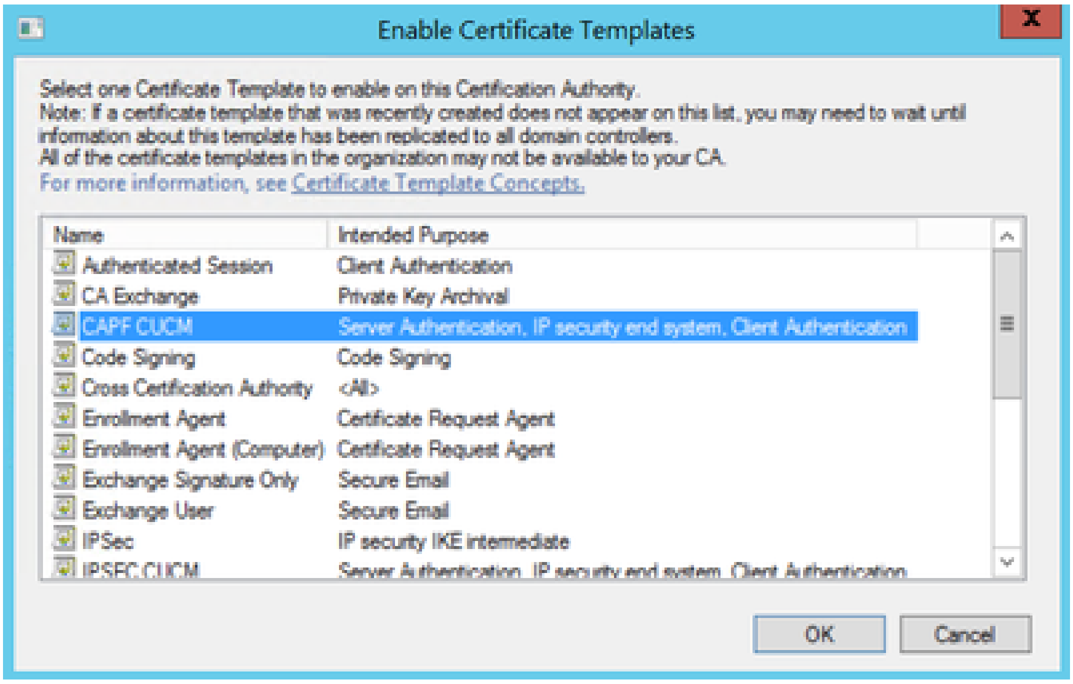
Client Authentication
IP security end system
Server Authentication

Etapa 9. Feche a janela **Console de modelos de certificado** e, na primeira janela, navegue para **Novo > Modelo de certificado a ser emitido**, como mostrado na imagem.



Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Etapa 10. Selecione o novo modelo **CAPF CUCM** e selecione **OK**, como mostrado na imagem.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CAPF CUCM	Server Authentication, IP security end system, Client Authentication
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermediate
IPSEC CUCM	Server Authentication, IP security end system, Client Authentication

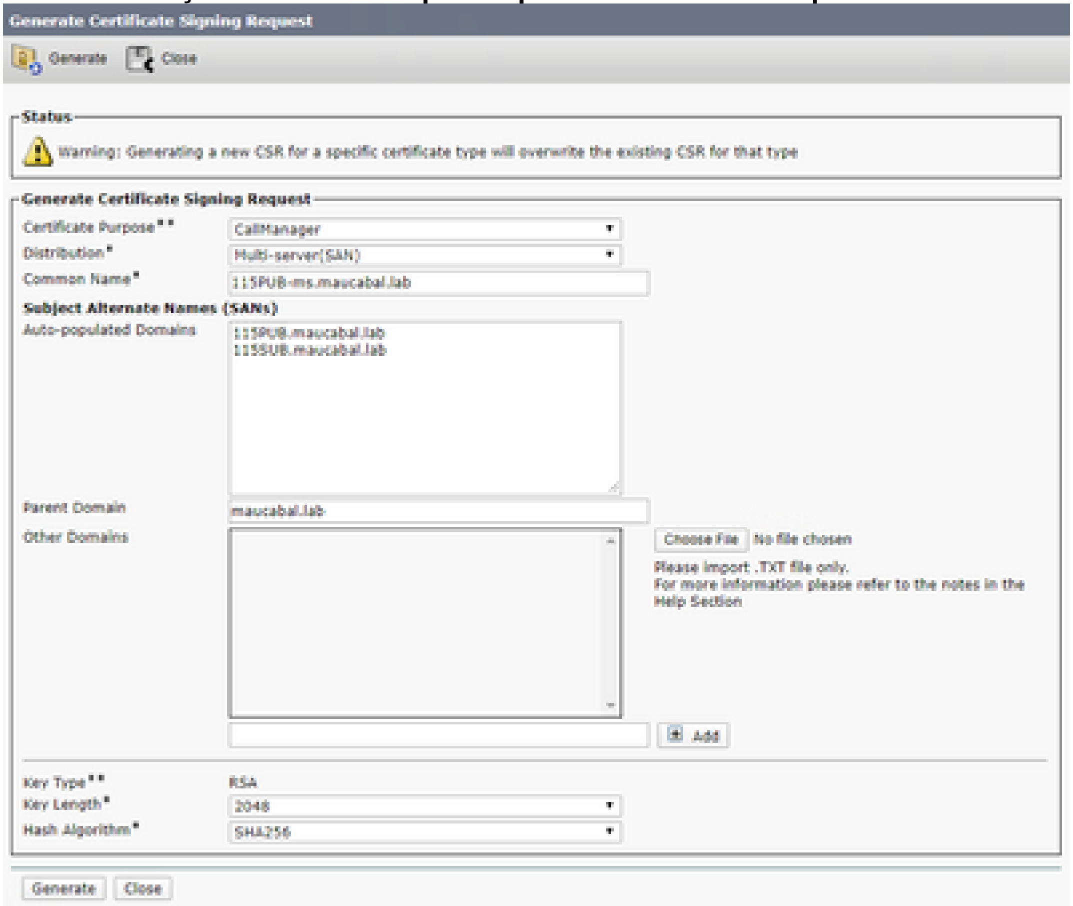
Gerar uma Solicitação de Assinatura de Certificado

Use este exemplo para gerar um certificado do CallManager com o uso dos modelos recém-criados. O mesmo procedimento pode ser usado para qualquer tipo de certificado. Você só precisa selecionar o certificado e os tipos de modelo de acordo:

Etapa 1. No CUCM, navegue para **OS Administration > Security > Certificate Management > Generate CSR**.

Etapa 2. Selecione essas opções e selecione **Gerar**, como mostrado na imagem.

- Finalidade do certificado: **CallManager**
- Distribuição: **<Pode ser apenas para um servidor ou para várias SANs>**



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)

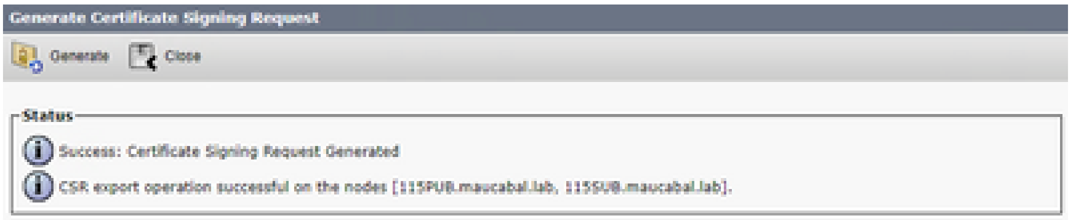
Auto-populated Domains	115PUB.maucabal.lab 115SUB.maucabal.lab
Parent Domain	maucabal.lab
Other Domains	

Choose File No file chosen

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

Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256

Etapa 3. Uma mensagem de confirmação é gerada, como mostrado na imagem.

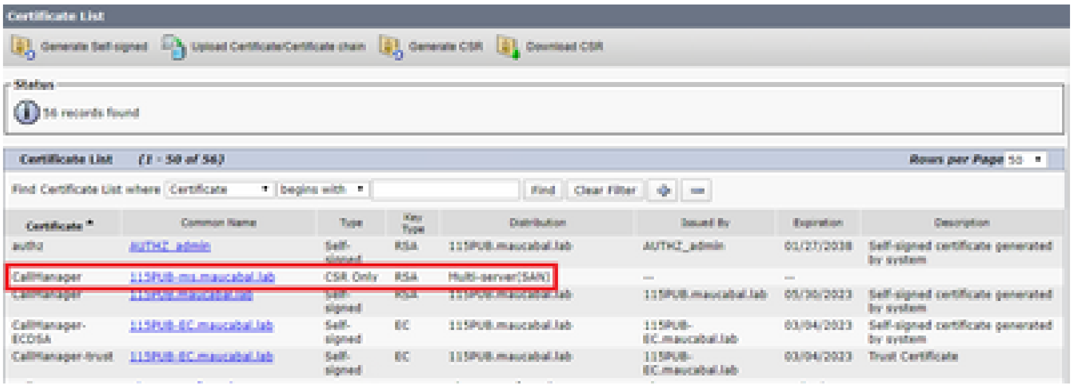


Status

Success: Certificate Signing Request Generated

CSR export operation successful on the nodes [115PUB.maucabal.lab, 115SUB.maucabal.lab].

Etapa 4. Na lista de certificados, procure a entrada com o tipo **CSR Only** e selecione-a, como mostrado na imagem.



Status

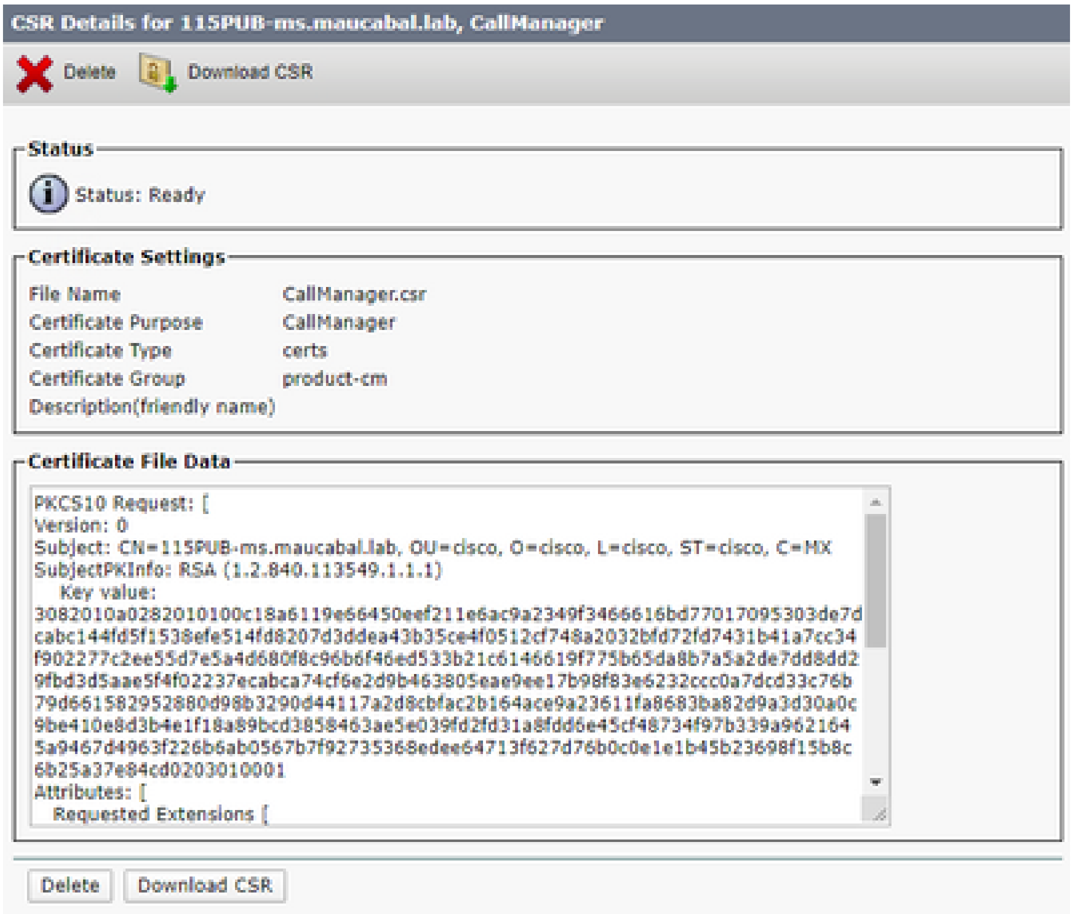
56 records found

Certificate List (1 - 50 of 56) Rows per Page 50

Find Certificate List where Certificate begins with

Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_admin	Self-signed	RSA	115PUB.maucabal.lab	AUTHZ_admin	01/27/2038	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

Etapa 5. Na janela pop-up, selecione **Download CSR** e salve o arquivo no computador.



Status

Status: Ready

Certificate Settings

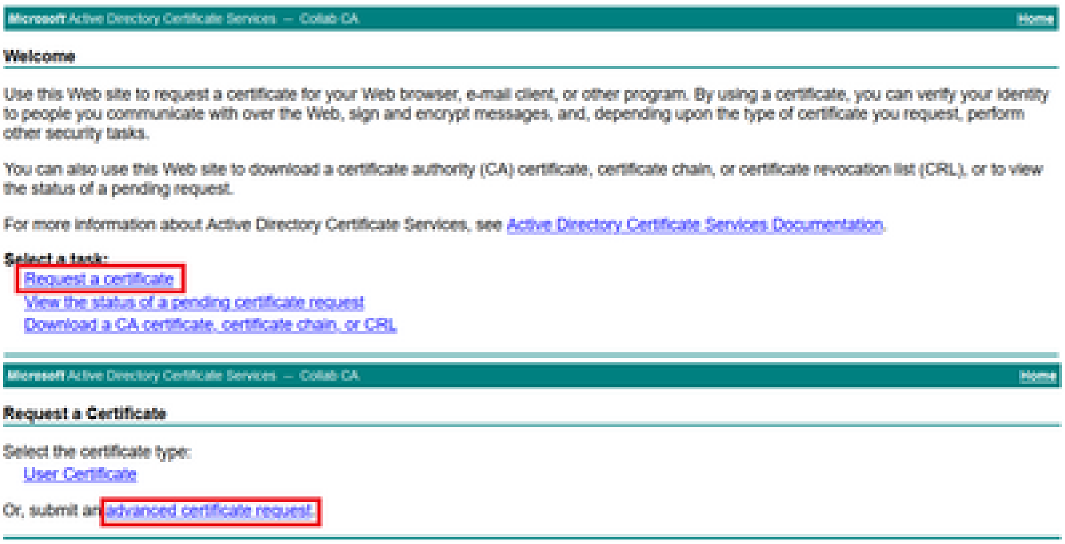
File Name	CallManager.csr
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	

Certificate File Data

```
PKCS10 Request: [
Version: 0
Subject: CN=115PUB-ms.maucabal.lab, OU=cisco, O=cisco, L=cisco, ST=cisco, C=MX
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d
cabc144fd5f1538efe514fd8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d6615829528800d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
  Requested Extensions [
```

Etapa 6. No navegador, navegue até este URL e insira as credenciais de administrador do controlador de domínio: **https://<yourWindowsServerIP>/certsrv/.**

Passo 7. Navegue para **Solicitar um certificado > solicitação de certificado avançado**, como mostrado na imagem.



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

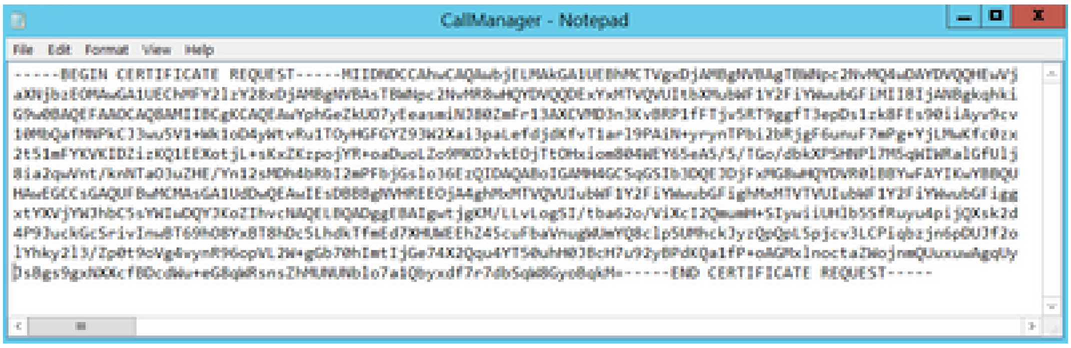
Microsoft Active Directory Certificate Services -- Collab CA
Home

Request a Certificate

Select the certificate type:
User Certificate

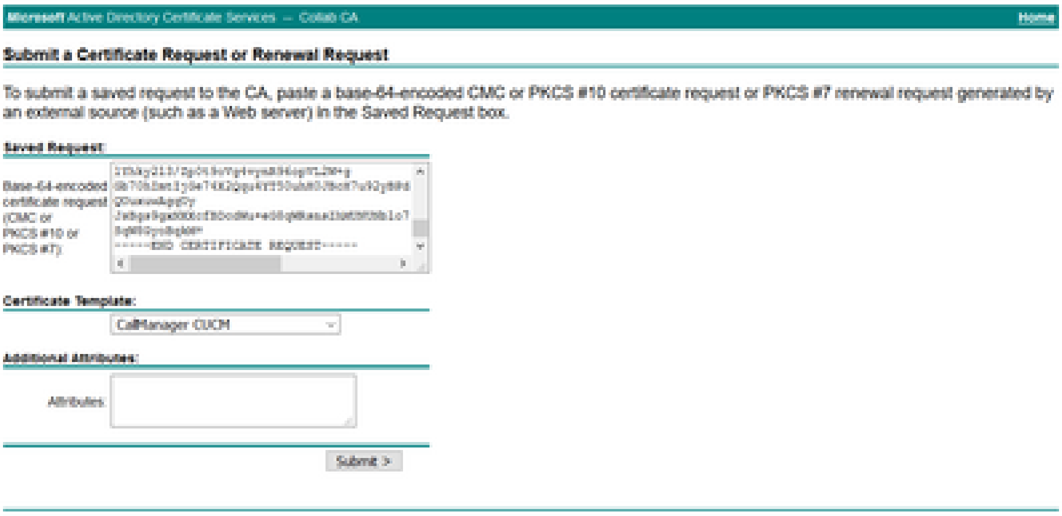
Or, submit an advanced certificate request.

Etapa 8. Abra o arquivo CSR e copie todo o seu conteúdo:



```
-----BEGIN CERTIFICATE REQUEST-----MIIDNDCCAhwCAQAwbjELMAkGA1UEBhMCTVgxDjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVj
aXNjbzEOMAwGA1UEChMFY2lzY28xDjAMBgNVBAsTBWNpc2NvMR8wHQYDVQQDExYxMTVQVUItbXMubWF1Y2FiYWwubGFiMIIBIjANBgkqhki
G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYphGeZkUO7yEeasmiN3B0ZmFr13AXCVMD3n3KvBRP1fFTjv5RT9ggfT3epDs1zk8FEs90iiAyv9cv
10MbQafMNPkCJ3wu5V1+Wk1oD4yWtvRu1TOyHGFGYZ93W2Xai3paLefdjdKfvT1arl9PAiN+yrynTPbi2bRjgF6unuF7mPg+YjLMwKfc0zx
2t51mFYKVKIDZizKQ1EEXotjL+sKxZKzpojYR+oaDuoLZo9MKDJvkEOjTtOHxiom804WEY65eA5/5/TGo/dbkXP5HNP17M5qWIWRalGfUlj
8ia2quWnt/knNTaO3uZHE/Yn12sMDh4bRbI2mPFbjGslo36EzQIDAQABoIGAMH4GCSqGSIb3DQEJDjFxMG8wHQYDVR0lBBYwFAYIKwYBBQU
HAwEGCCsGAQUFBwMCMAsGA1UdDwQEAwIEsDBBBgNVHREEOjA4ghMxMTVQVUIubWF1Y2FiYWwubGFighMxMTVTVUIubWF1Y2FiYWwubGFigg
xtYXVjYWJhbC5sYWIwDQYJKoZIhvcNAQELBQADggEBAIgwtjgKM/LLvLogSI/tba62o/ViXcI2QmumM+SIywiiUMIb5SfRuyu4pijQXsk2d
4P9JuckGcSrivIm+BT69h0BYxBT8hDc5LhdkTfmEd7XHUWEEhZ45cuFbaVnugWUmYQ8clp5UMhckJyzQpQpL5pjcv3LCPiqbzjn6pDUJf2o
lYhky2l3/Zp0t9oVg4vynR96opVL2W+gGb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPdKQa1fP+oAGMxlnoctaZWojnmQUuxuwAgqUy
Ds8gs9gxNXKcfBDcdWu+eG8qWRsnsZhMUNUNblo7a1QbyxdfTr7dbSqWBGyoBqkM=-----END CERTIFICATE REQUEST-----
```

Etapa 9. Cole o CSR no campo de **solicitação de certificado codificado na Base 64**. Em **Modelo de certificado**, selecione o modelo correto e selecione **Enviar**, como mostrado na imagem.



Microsoft Active Directory Certificate Services -- Collab CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
lYhky2l3/Zp0t9oVg4vynR96opVL2W+g
Gb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPd
QOa1fP+oAGMxlnoctaZWojnmQUuxuwAgqUy
Ds8gs9gxNXKcfBDcdWu+eG8qWRsnsZhMUNUNblo7
BqkM=
-----END CERTIFICATE REQUEST-----
```

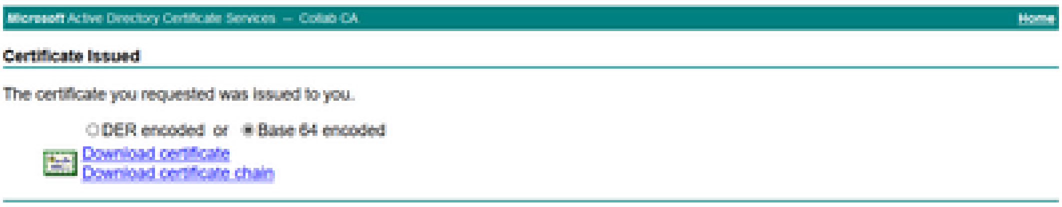
Certificate Template:

CallManager CUCM

Additional Attributes:

Attributes:

Etapa 10. Por fim, selecione **Base 64 encoded** e **Download certificate chain**, o arquivo gerado agora pode ser carregado no CUCM.



Microsoft Active Directory Certificate Services -- Collab CA
Home

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Verificar

O procedimento de verificação é, na verdade, parte do processo de configuração.

Troubleshoot

No momento, não há informações específicas de solução de problemas disponíveis para essa configuração.