

Crear plantillas de certificados de CA de Windows para CUCM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Callmanager / Tomcat / Plantilla de TVS](#)

[Plantilla IPsec](#)

[Plantilla CAPE](#)

[Generar una solicitud de firma de certificado](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe un procedimiento paso a paso para crear plantillas de certificados en entidades de certificación (CA) basadas en Windows Server.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM, versión 11.5(1).
- También se recomiendan conocimientos básicos de la administración de Windows Server

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- La información de este documento se basa en CUCM versión 11.5(1).
- Microsoft Windows Server 2012 R2 con servicios de CA instalados.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.


Antecedentes

Estas plantillas de certificado cumplen los requisitos de la extensión X.509 para cada tipo de certificado de Cisco Unified Communications Manager (CUCM).

Hay cinco tipos de certificados que puede firmar una CA externa:

Certificado	Uso	Servicios afectados
CallManager	Presentado en el registro de dispositivos seguros, puede firmar archivos de lista de confianza de certificados (CTL)/lista de confianza interna (ITL), que se utilizan para interactuar de forma segura con otros servidores, como enlaces troncales de protocolo de inicio de sesión (SIP) seguros.	<ul style="list-style-type: none">· Cisco Call Manager· Cisco CTI Manager· Cisco TFTP
tomcat	Presentado para interacciones de protocolo seguro de transferencia de hipertexto (HTTPS).	<ul style="list-style-type: none">· Tomcat de Cisco· Inicio de sesión único (SSO)· Movilidad de extensiones· Corporate Directory
ipsec	Se utiliza para la generación de archivos de copia de seguridad, así como para la interacción de la seguridad IP (IPsec) con el protocolo de control de gateway de medios (MGCP) o las puertas de enlace H323.	<ul style="list-style-type: none">· Cisco DRF Master· Cisco DRF Local
CAPF	Se utiliza para generar certificados de importancia local (LSC) para teléfonos.	<ul style="list-style-type: none">· Función de proxy de Cisco Certificate Authority
TVS	Se utiliza para crear una conexión con el Servicio de verificación de	<ul style="list-style-type: none">· Servicio Cisco Trust Verification

	confianza (TVS), cuando los teléfonos no pueden autenticar un certificado desconocido.	
--	--	--

 Nota: el certificado IPsec no está relacionado con Cisco DRF Master y Cisco DRF Local, ya que en las versiones más recientes se utiliza el certificado Tomcat 14. No existe ningún plan para agregar este cambio a la versión 12.5 o anteriores.

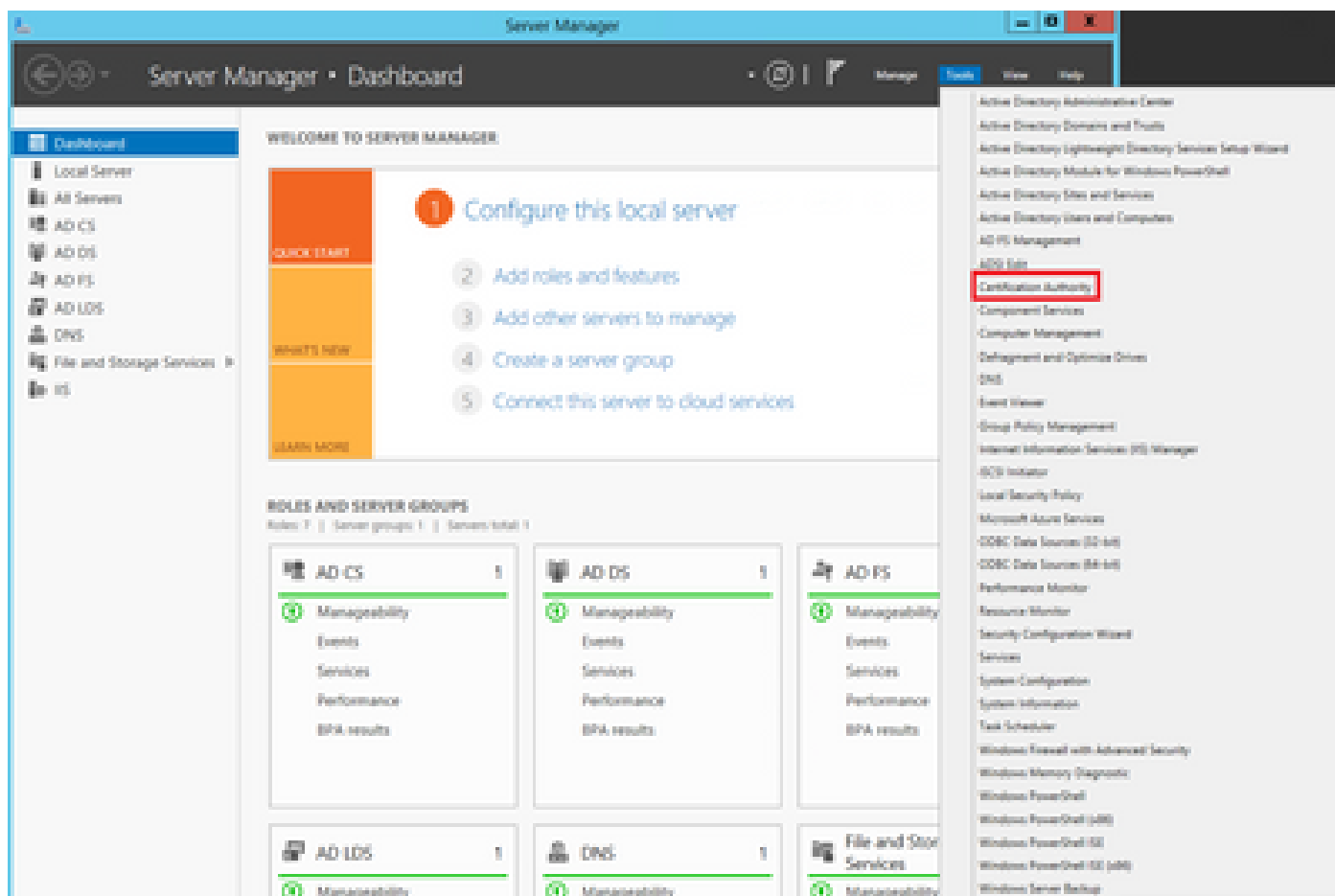
Cada uno de estos certificados tiene algunos requisitos de extensión X.509 que deben establecerse; de lo contrario, puede encontrar comportamientos incorrectos en cualquiera de los servicios mencionados:

Certificado	Uso de claves X.509	Uso de clave ampliada X.509
CallManager	<ul style="list-style-type: none"> · Firma digital · Cifrado de claves · Cifrado de datos 	<ul style="list-style-type: none"> · Autenticación de servidor web · Autenticación de cliente web
tomcat	<ul style="list-style-type: none"> · Firma digital · Cifrado de claves · Cifrado de datos 	<ul style="list-style-type: none"> · Autenticación de servidor web · Autenticación de cliente web
ipsec	<ul style="list-style-type: none"> · Firma digital · Cifrado de claves · Cifrado de datos 	<ul style="list-style-type: none"> · Autenticación de servidor web · Autenticación de cliente web · Sistema final IPsec
CAPF	<ul style="list-style-type: none"> · Firma digital · Signo de certificado · Cifrado de claves 	<ul style="list-style-type: none"> · Autenticación de servidor web · Autenticación de cliente web
TVS	<ul style="list-style-type: none"> · Firma digital · Cifrado de claves · Cifrado de datos 	<ul style="list-style-type: none"> · Autenticación de servidor web · Autenticación de cliente web

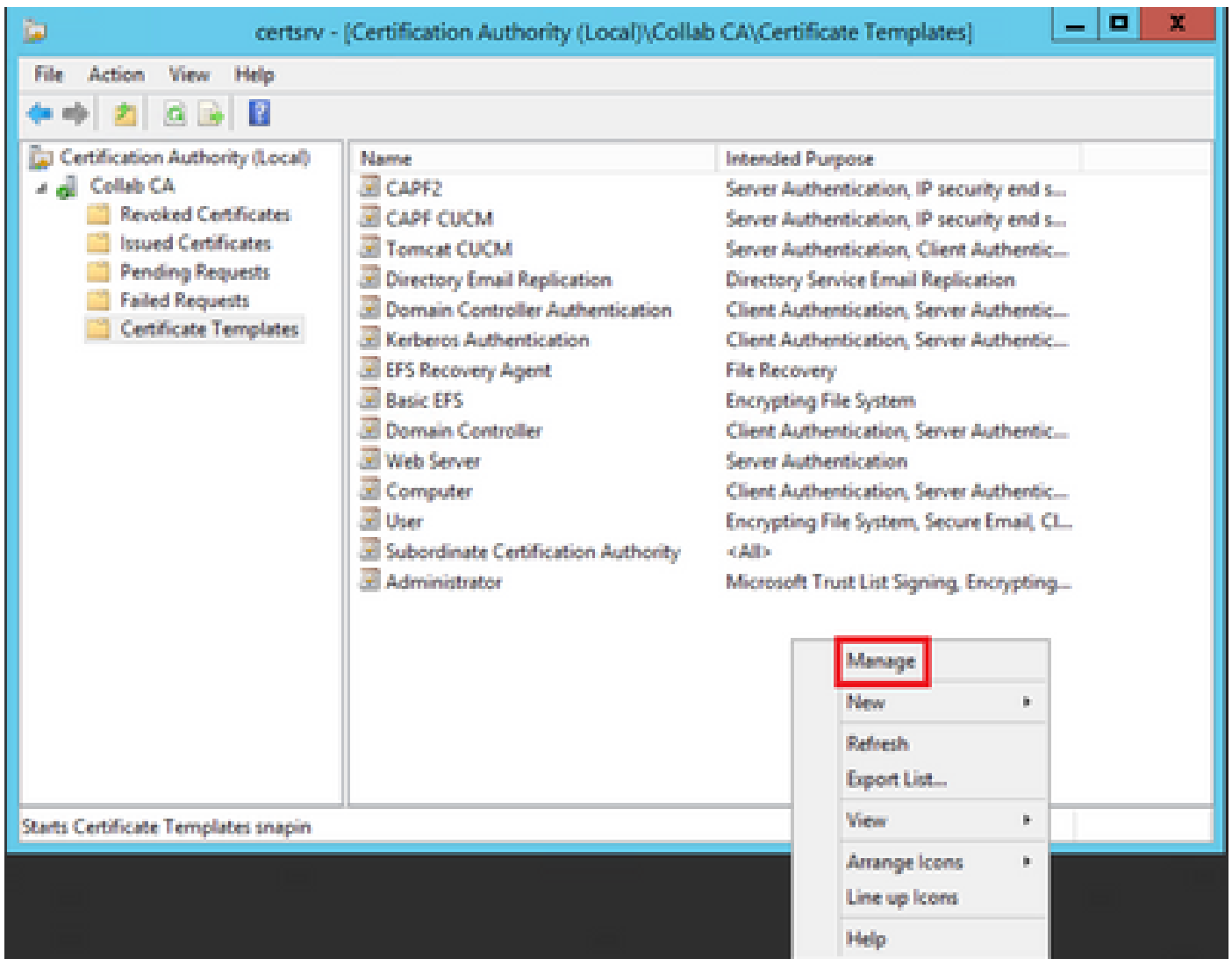
Para obtener más información, consulte la [Guía de seguridad de Cisco Unified Communications Manager](#)

Configurar

Paso 1. En Windows Server, navegue hasta Administrador del servidor > Herramientas > Entidad emisora de certificados, como se muestra en la imagen.



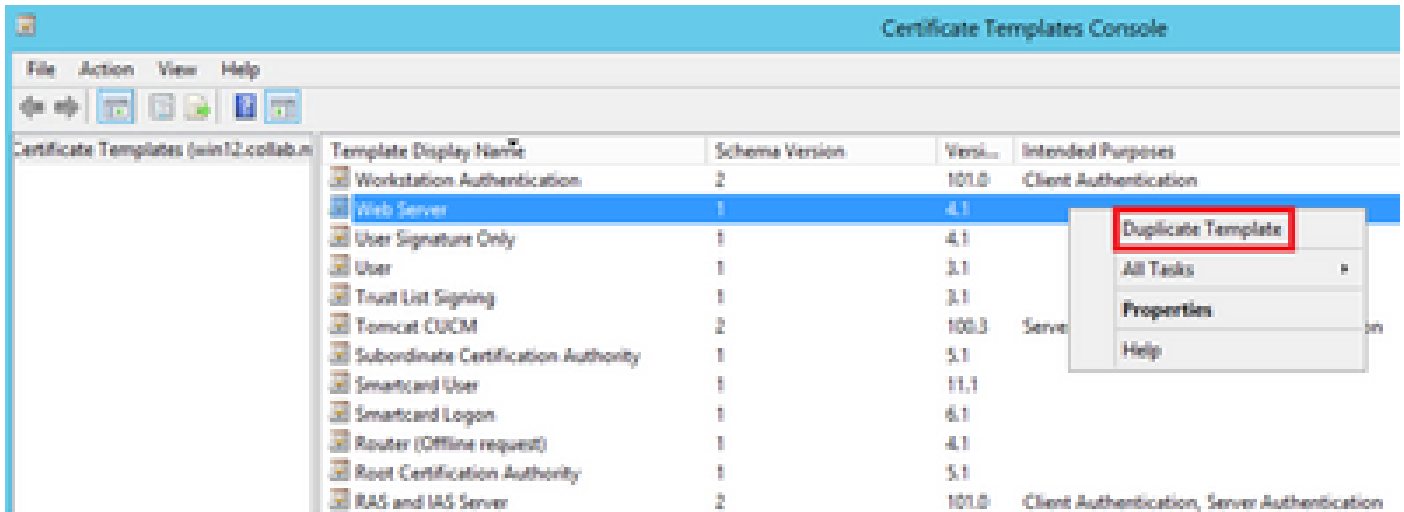
Paso 2. Seleccione su CA, navegue hasta Plantillas de certificado, haga clic con el botón derecho en la lista y seleccione Administrar, como se muestra en la imagen.



Callmanager / Tomcat / Plantilla de TVS

Las imágenes siguientes muestran solo la creación de la plantilla de CallManager; pero se pueden seguir los mismos pasos para crear las plantillas de certificado para Tomcat y los servicios de TVS. La única diferencia consiste en garantizar que se utiliza el nombre de servicio correspondiente para cada nueva plantilla en el paso 2.

Paso 1. Busque la plantilla Web Server, haga clic con el botón derecho en ella y seleccione Duplicate Template, como se muestra en la imagen.



Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.

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

Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.

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

Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Permitir el intercambio de claves sólo con el cifrado de claves (cifrado de claves)
- Permitir cifrado de datos de usuario

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

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

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.

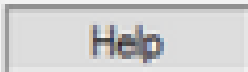
Extensions included in this template:

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



Description of Application Policies:

Server Authentication



Paso 6. Busque Client Authentication, selecciónela y seleccione OK tanto en esta ventana como en la anterior, como se muestra en la imagen.

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

Paso 7. Vuelva a la plantilla, seleccione Aplicar y, a continuación, Aceptar.

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

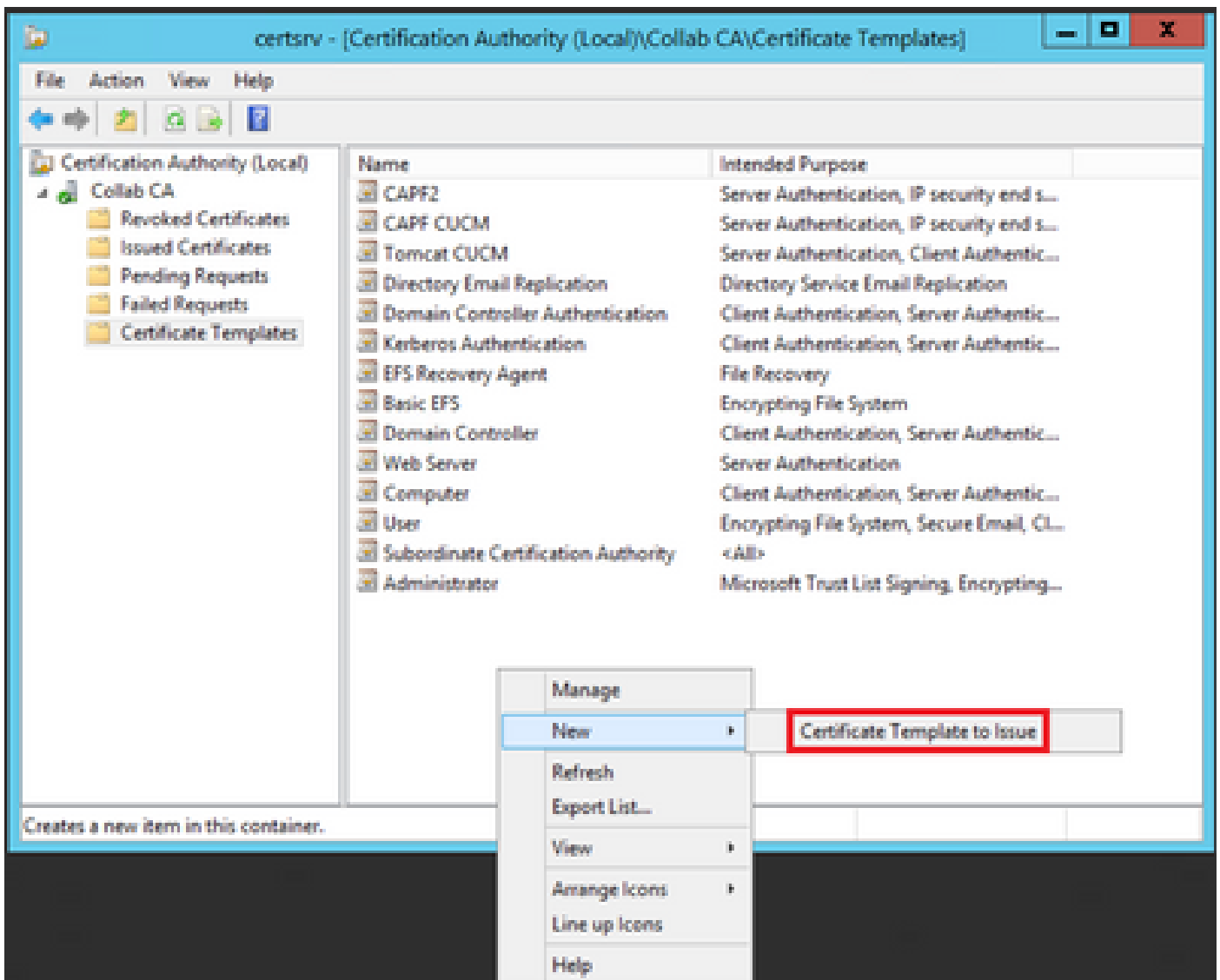
OK

Cancel

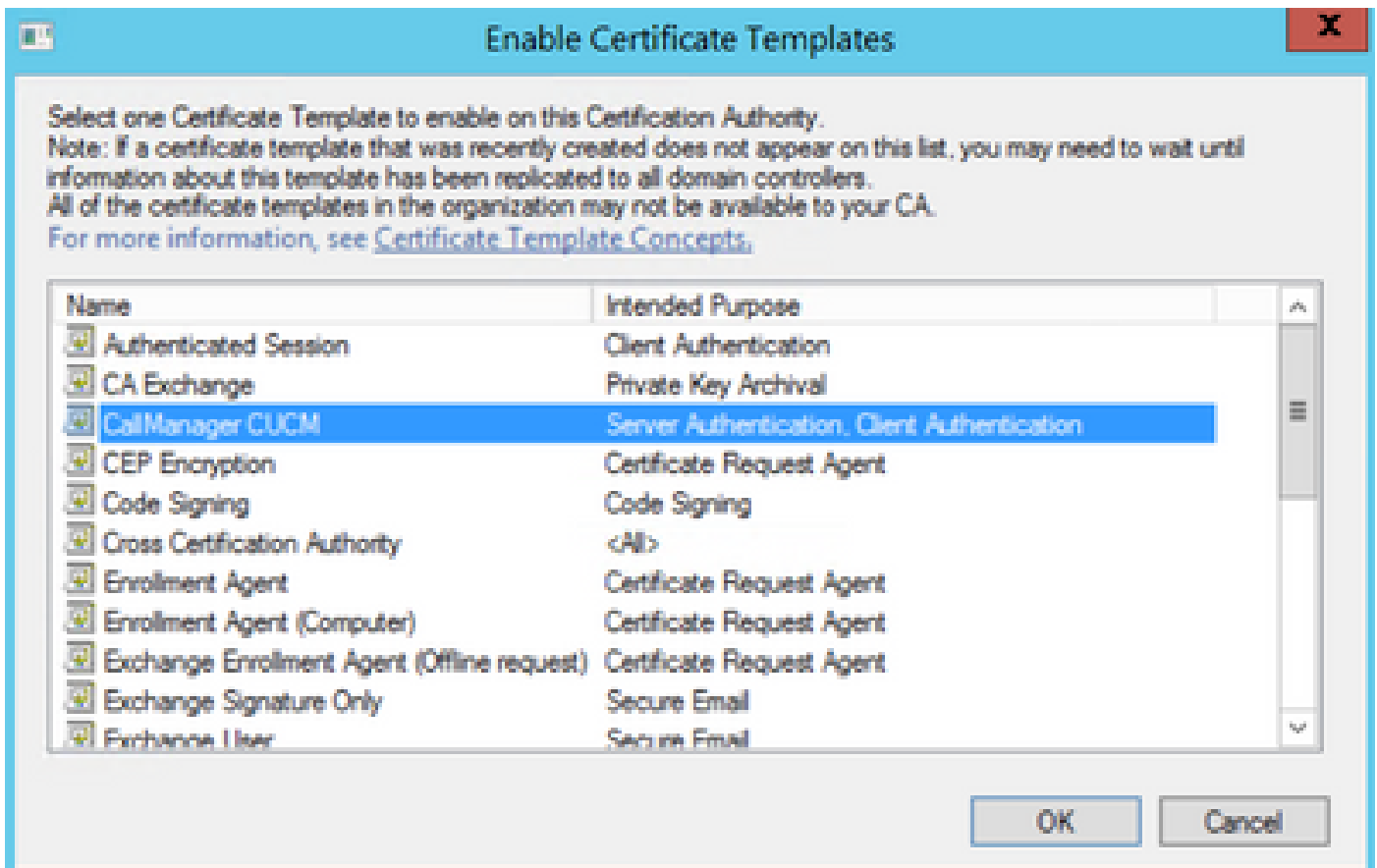
Apply

Help

Paso 8. Cierre la ventana Consola de Plantilla de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.



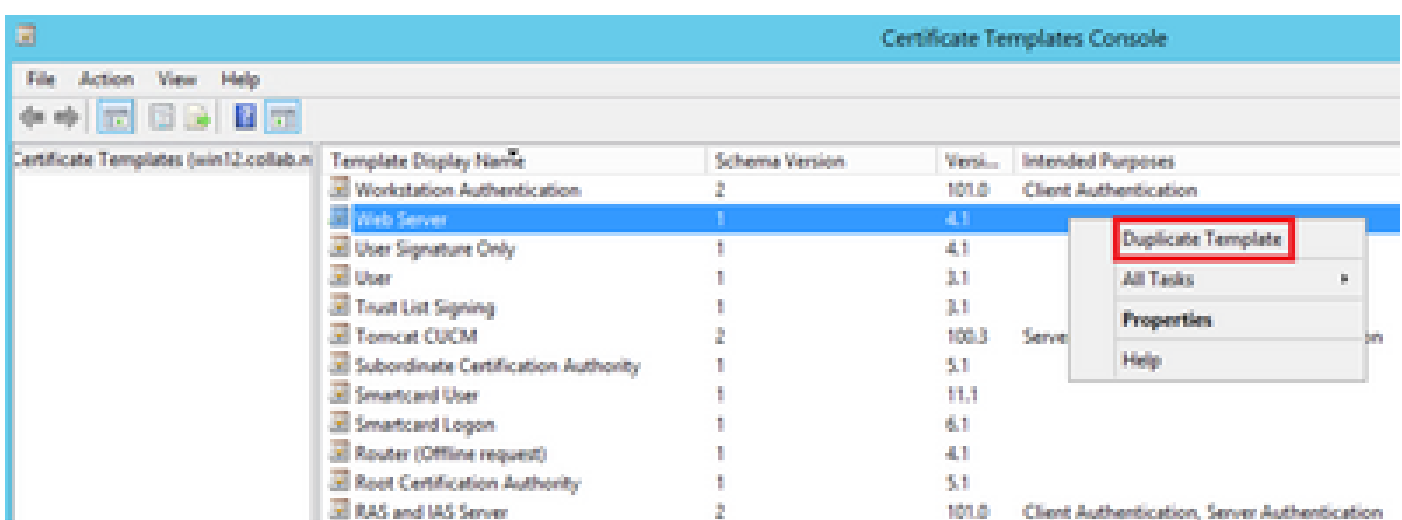
Paso 9. Seleccione la nueva plantilla de CallManager CUCM y seleccione OK, como se muestra en la imagen.



Paso 10. Repita todos los pasos anteriores para crear plantillas de certificado para los servicios Tomcat y TVS según sea necesario.

Plantilla IPsec

Paso 1. Busque la plantilla Web Server, haga clic con el botón derecho en ella y seleccione Duplicate Template, como se muestra en la imagen.



Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.

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

Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.

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 Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption

Critical extension.

OK Cancel Apply Help

Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Permitir el intercambio de claves sólo con el cifrado de claves (cifrado de claves)
- Permitir cifrado de datos de usuario

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

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

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

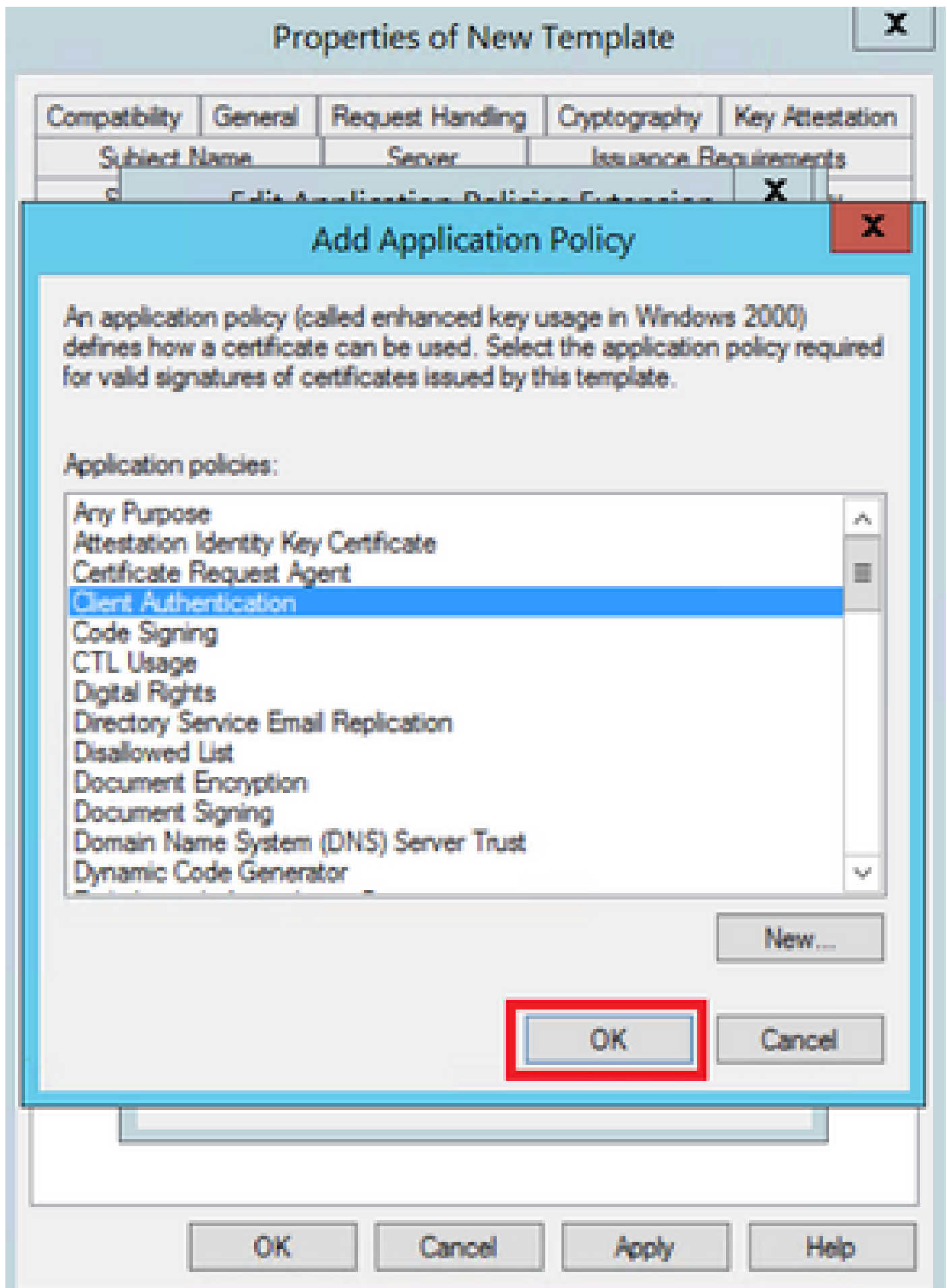
OK

Cancel

Apply

Help

Paso 6. Busque Client Authentication, selecciónela y luego OK, como se muestra en la imagen.



Paso 7. Seleccione Add nuevamente, busque IP security end system, selecciónelo y luego seleccione OK en esta ventana y en la anterior.

Properties of New Template



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

- 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

Paso 8. De nuevo en la plantilla, seleccione Apply y luego OK, como se muestra en la imagen.

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

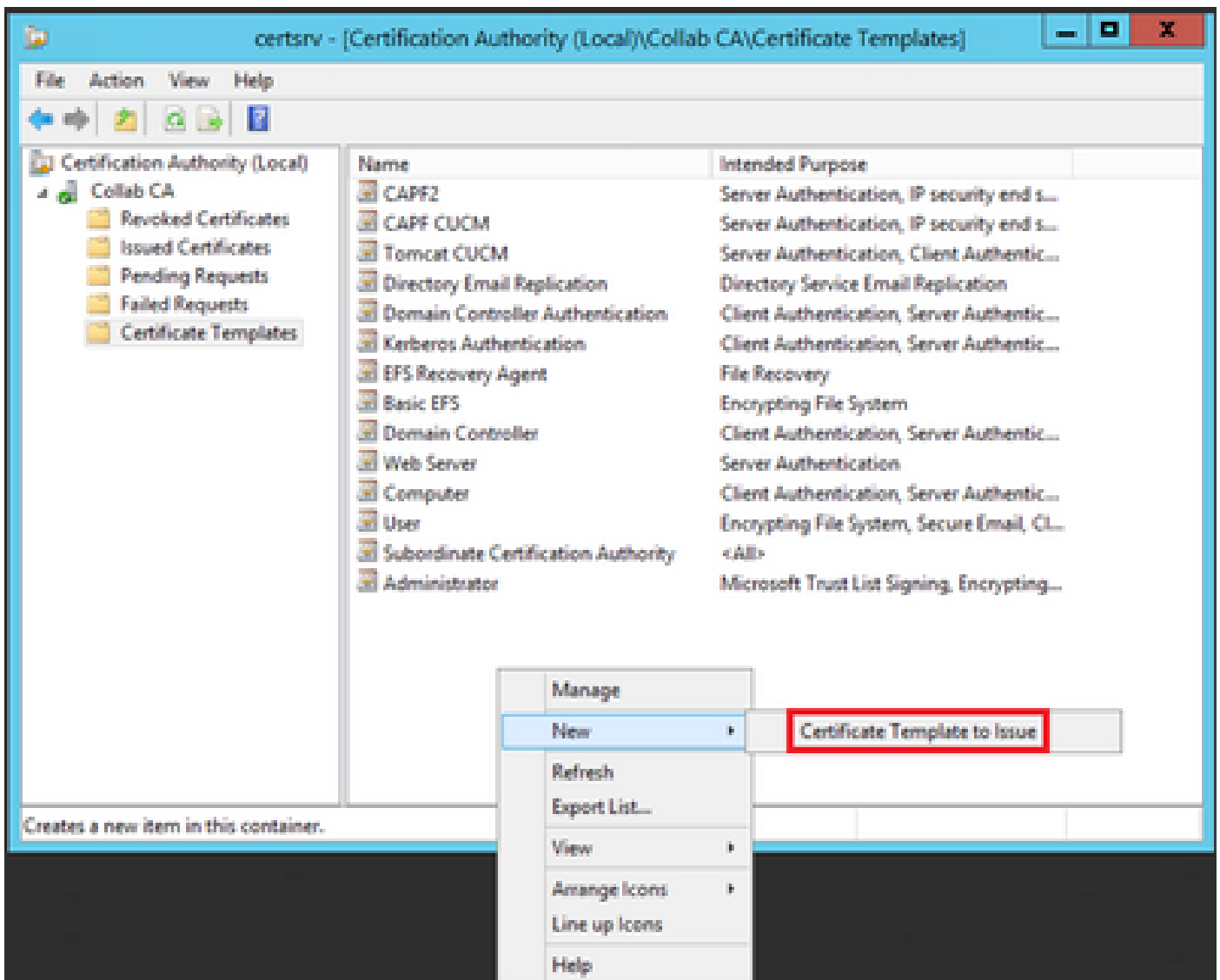
OK

Cancel

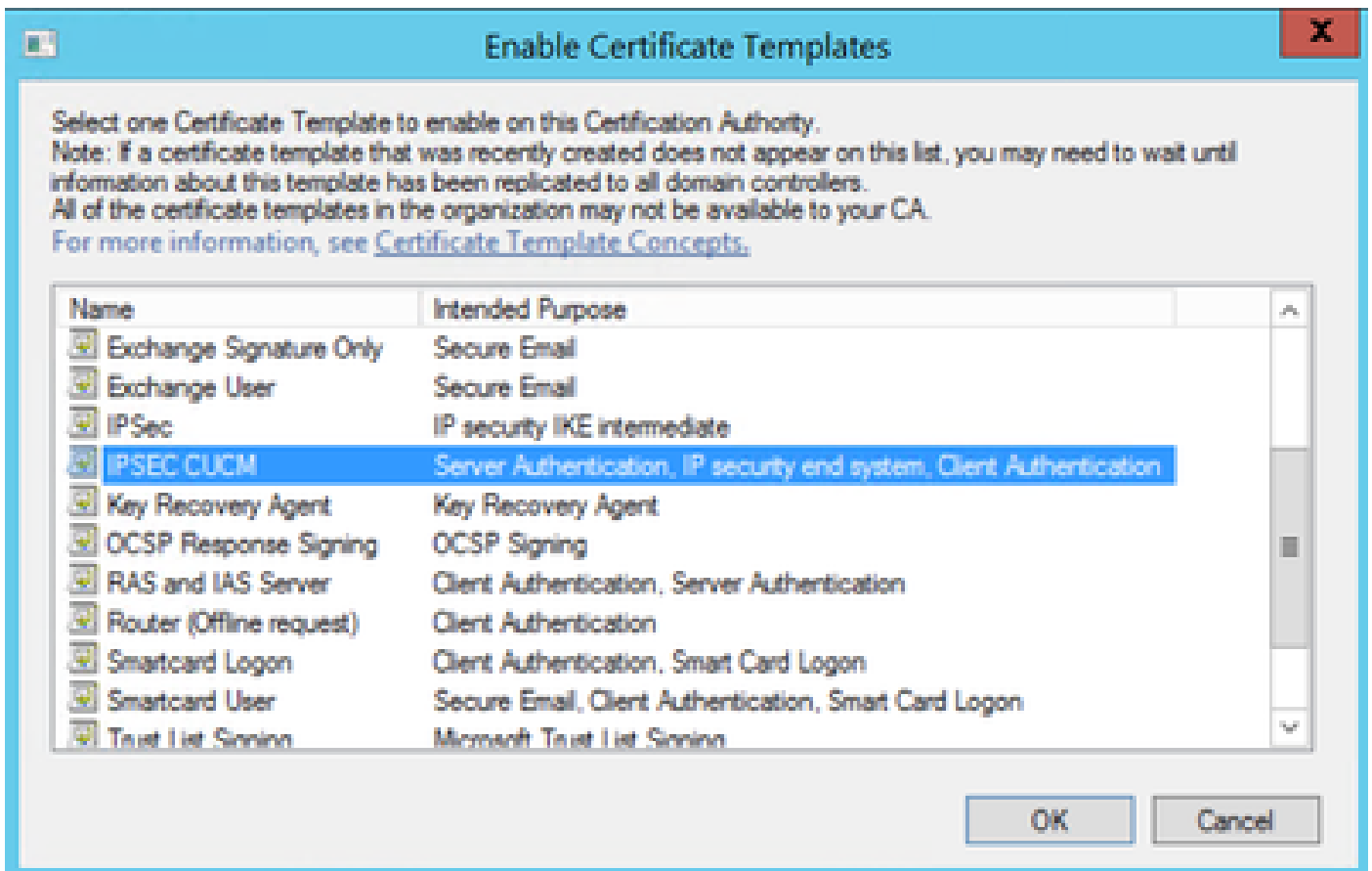
Apply

Help

Paso 9. Cierre la ventana de la Consola de Plantillas de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.

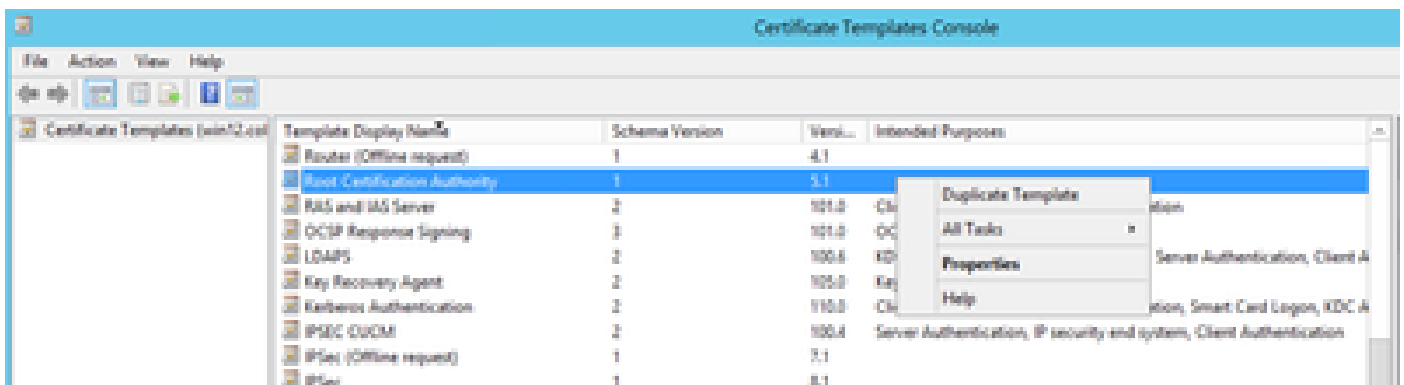


Paso 10. Seleccione la nueva plantilla IPSEC CUCM y seleccione en Aceptar, como se muestra en la imagen.

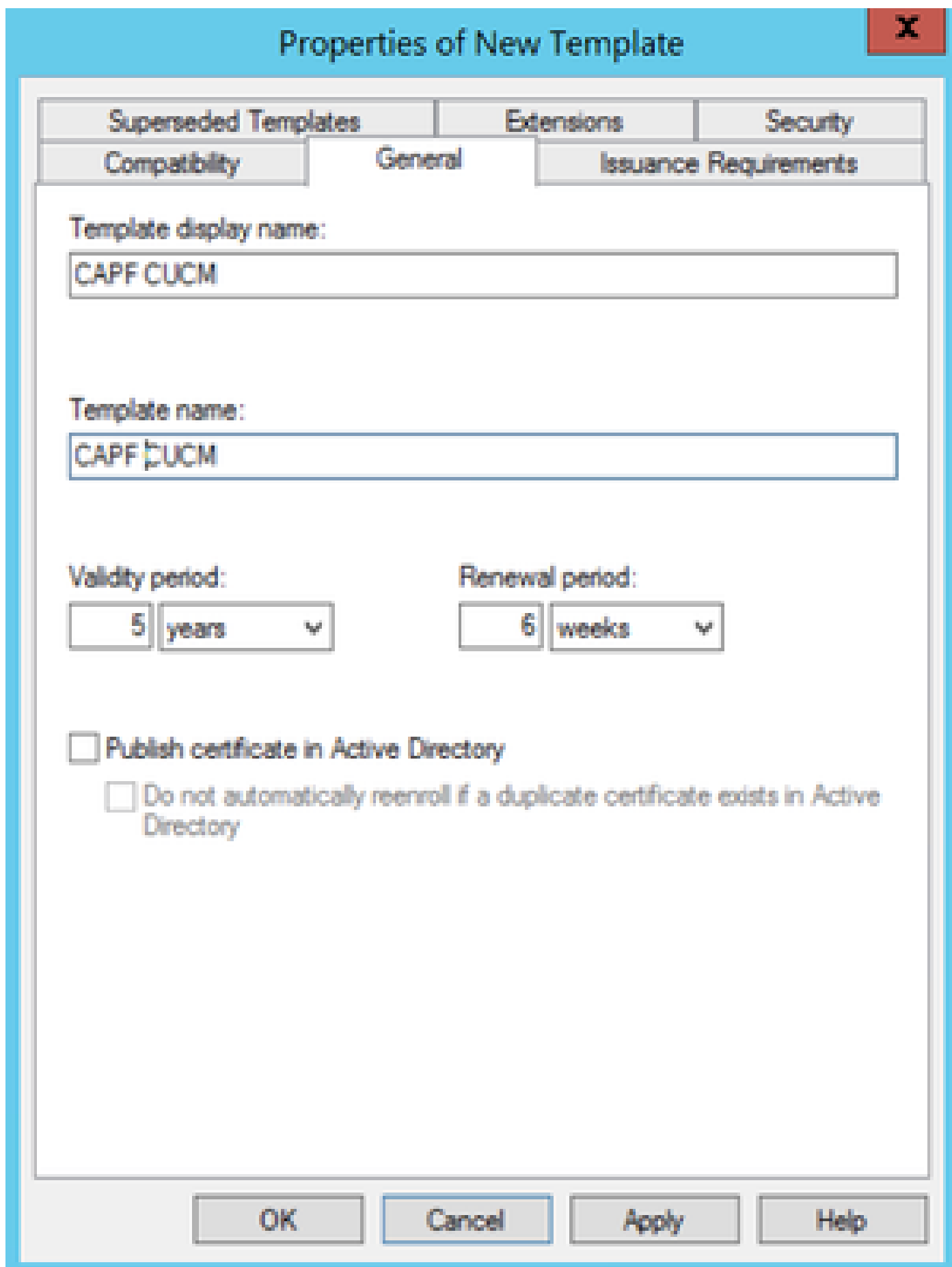


Plantilla CAPF

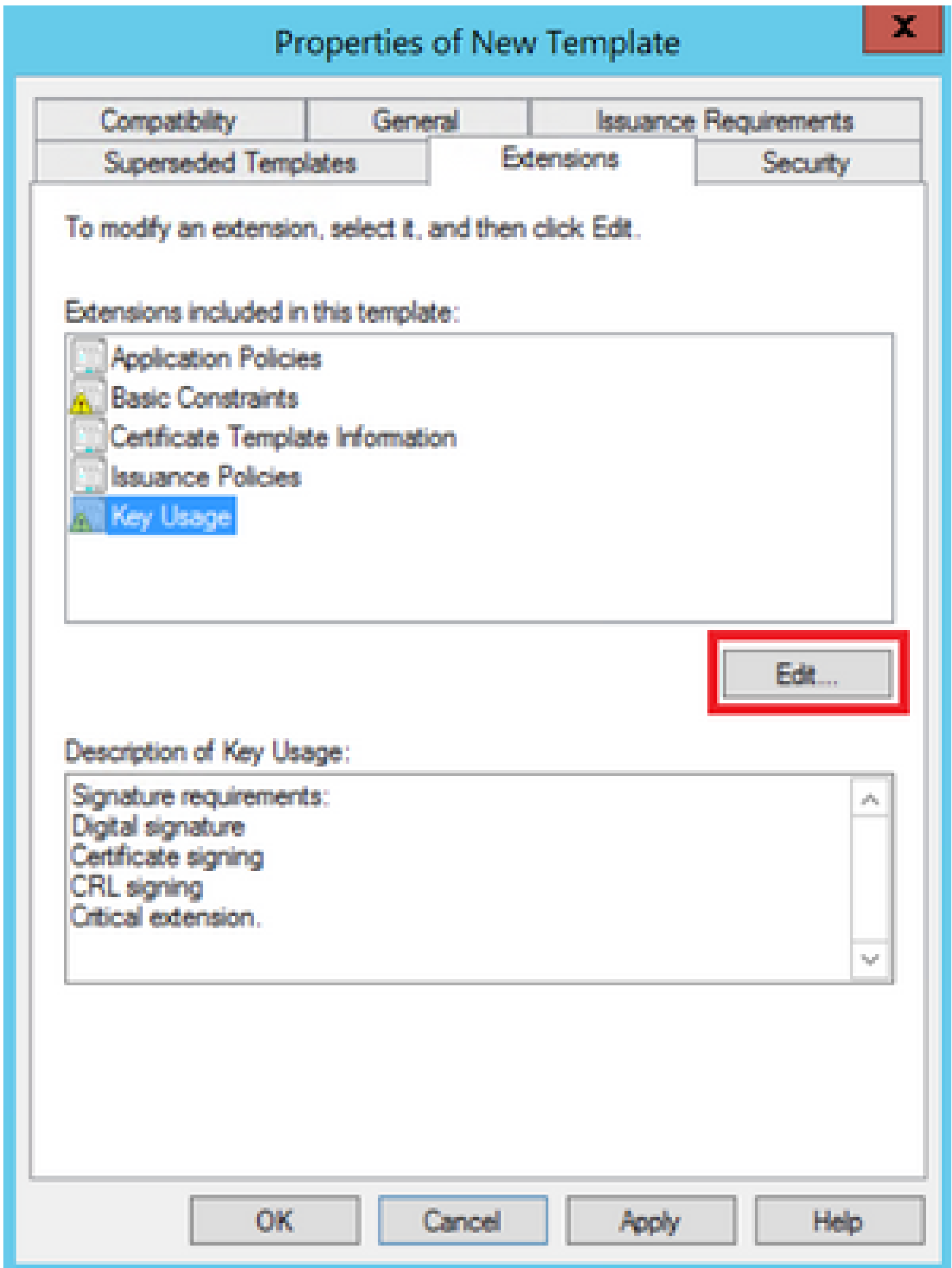
Paso 1. Busque la plantilla de CA raíz y haga clic con el botón derecho en ella. A continuación, seleccione Duplicate Template, como se muestra en la imagen.



Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.



Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.



Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Firma de certificados
- firma de CRL

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

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

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.

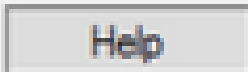
Extensions included in this template:

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



Description of Application Policies:

Server Authentication



Paso 6. Busque Client Authentication, selecciónela y luego seleccione OK, como se muestra en la imagen.

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

Paso 7. Seleccione Add nuevamente, busque IP security end system, selecciónelo y luego seleccione OK en este y en la ventana anterior también, como se muestra en la imagen.

Properties of New Template



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

- 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

Paso 8. De nuevo en la plantilla, seleccione Apply y luego OK, como se muestra en la imagen.

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

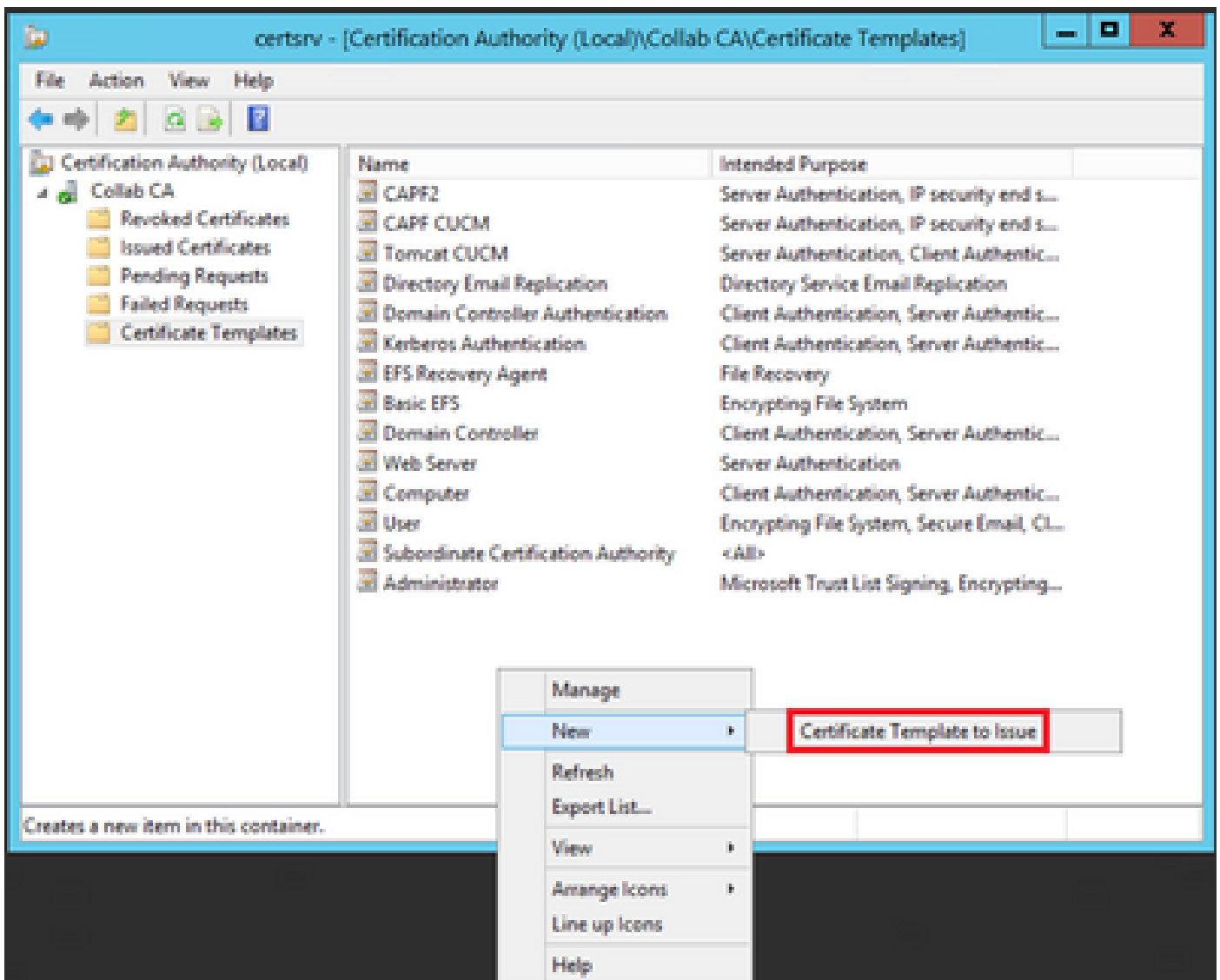
OK

Cancel

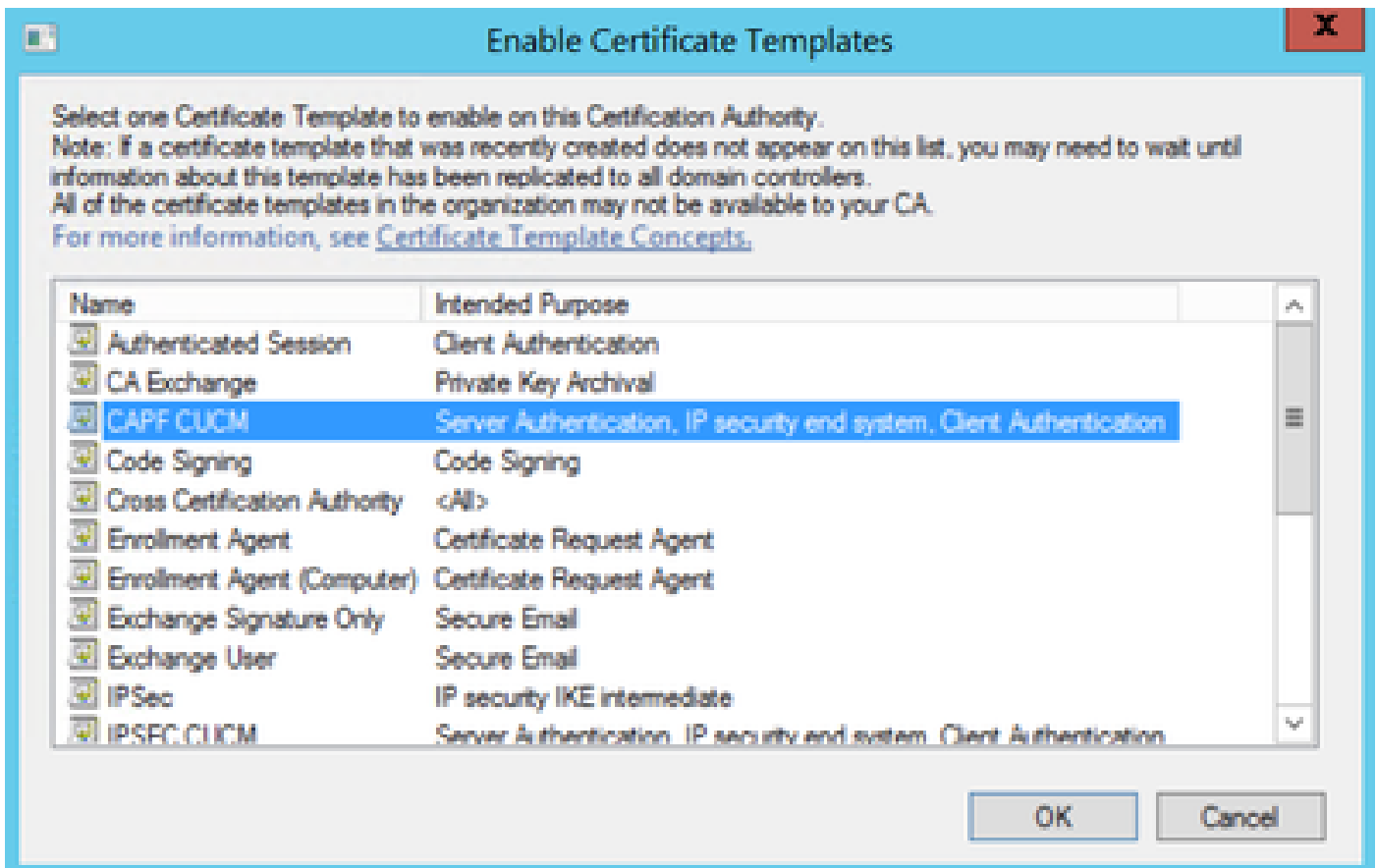
Apply

Help

Paso 9. Cierre la ventana de la Consola de Plantillas de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.



Paso 10. Seleccione la nueva plantilla CAPF CUCM y seleccione OK, como se muestra en la imagen.



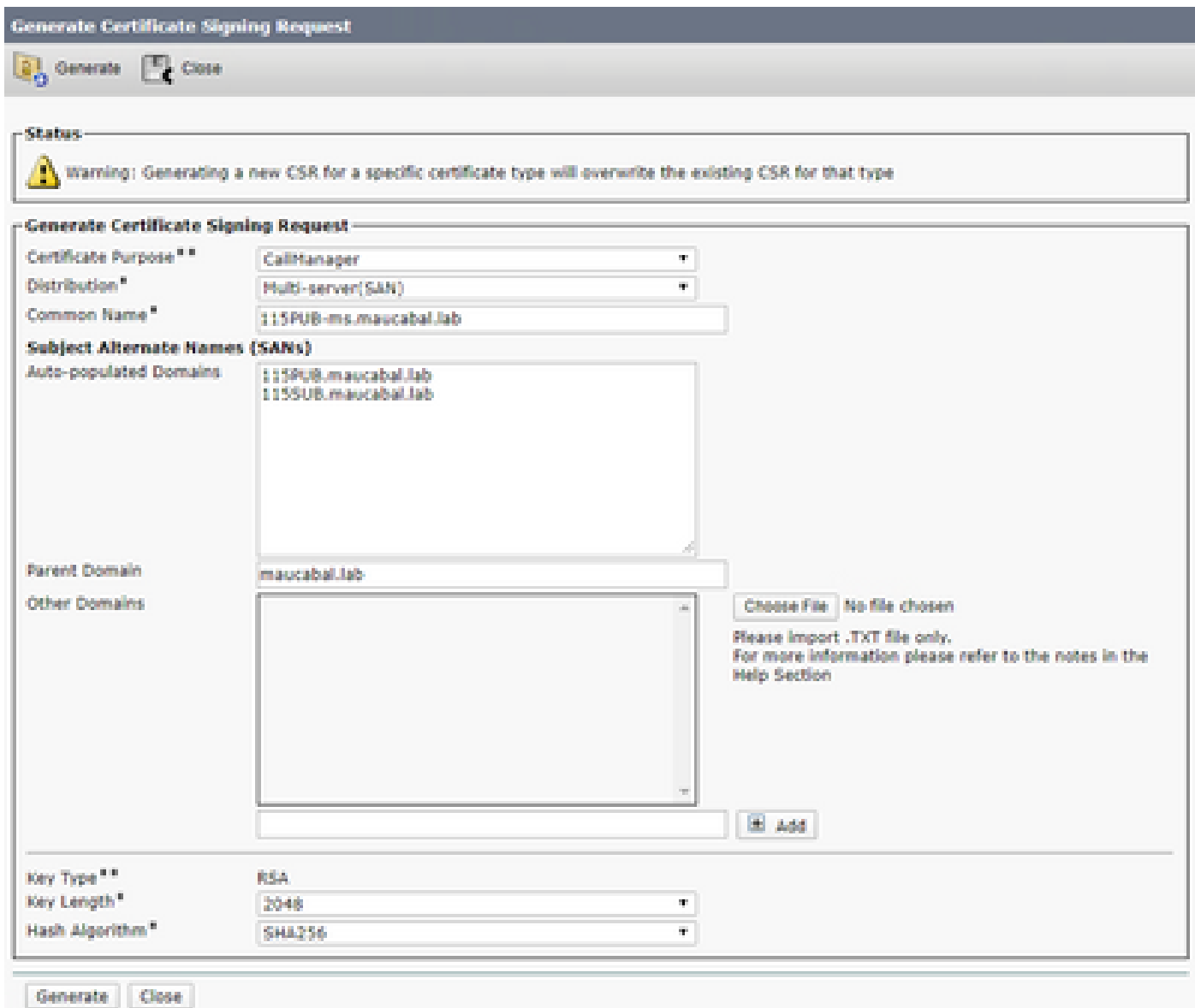
Generar una solicitud de firma de certificado

Utilice este ejemplo para generar un certificado de CallManager con el uso de las plantillas recién creadas. El mismo procedimiento se puede utilizar para cualquier tipo de certificado, solo tiene que seleccionar el certificado y los tipos de plantilla en consecuencia:

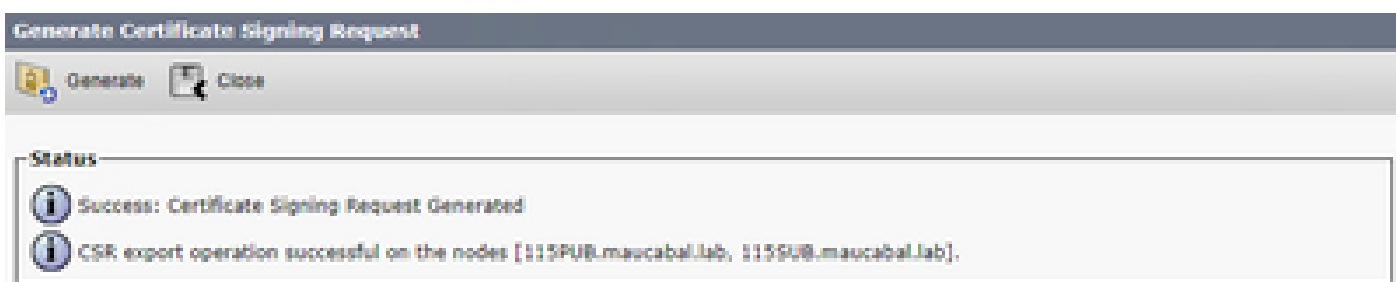
Paso 1. En CUCM, vaya a OS Administration > Security > Certificate Management > Generate CSR.

Paso 2. Seleccione estas opciones y seleccione Generate, como se muestra en la imagen.

- Propósito del certificado: CallManager
- Distribución: <Puede ser solo para un servidor o para varias SAN>



Paso 3. Se genera un mensaje de confirmación, como se muestra en la imagen.



Paso 4. En la lista de certificados, busque la entrada con el tipo CSR Only y selecciónela, como se muestra en la imagen.

Certificate #	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
auth	auth_admin	Self-signed	RSA	11SPUB.maucabal.lab	auth_admin	01/27/2028	Self-signed certificate generated by system
CallManager	11SPUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(SAN)	--	--	
CallManager	11SPUB.maucabal.lab	Self-signed	RSA	11SPUB.maucabal.lab	11SPUB.maucabal.lab	01/30/2023	Self-signed certificate generated by system
CallManager-ECDSA	11SPUB-EC.maucabal.lab	Self-signed	EC	11SPUB.maucabal.lab	11SPUB-EC.maucabal.lab	01/04/2023	Self-signed certificate generated by system
CallManager-trust	11SPUB-EC.maucabal.lab	Self-signed	EC	11SPUB.maucabal.lab	11SPUB-EC.maucabal.lab	01/04/2023	Trust Certificate

Paso 5. En la ventana emergente, seleccione Descargar CSR y guarde el archivo en el equipo.

CSR Details for 11SPUB-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

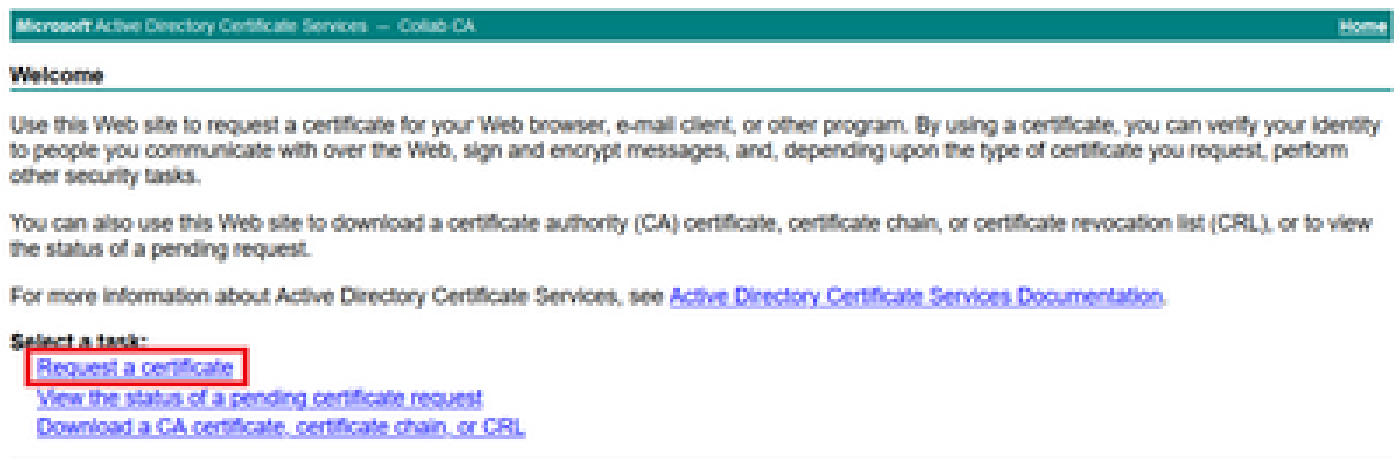
```

PKCS-10 Request: [
Version: 0
Subject: CN=11SPUB-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
cabc144fd5f1538efe514fd8207d3dde43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
Requested Extensions [
          
```

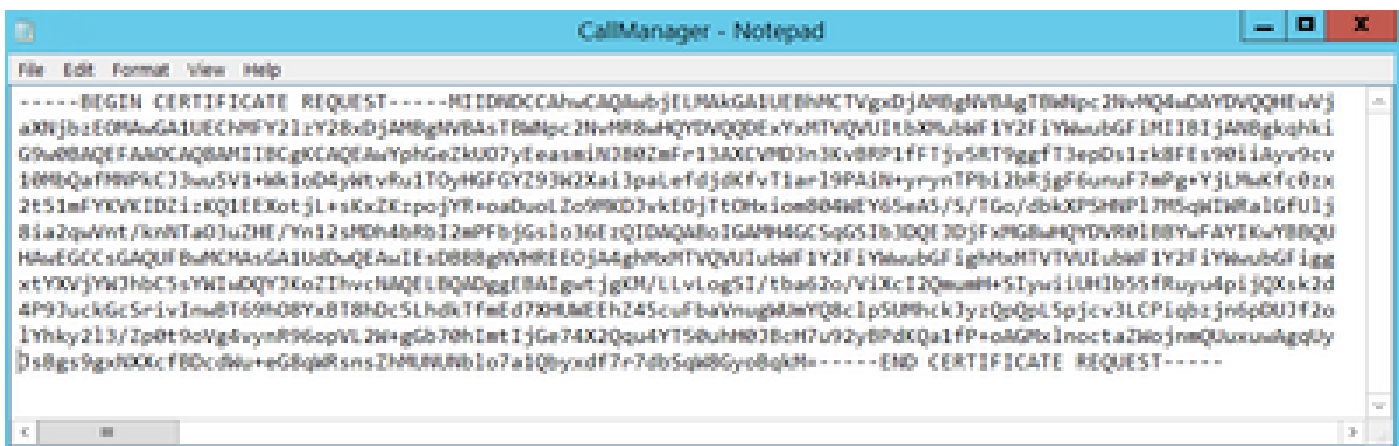
Delete
Download CSR

Paso 6. En el explorador, desplácese hasta esta dirección URL e introduzca las credenciales de administrador del controlador de dominio: <https://<yourWindowsServerIP>/certsrv/>.

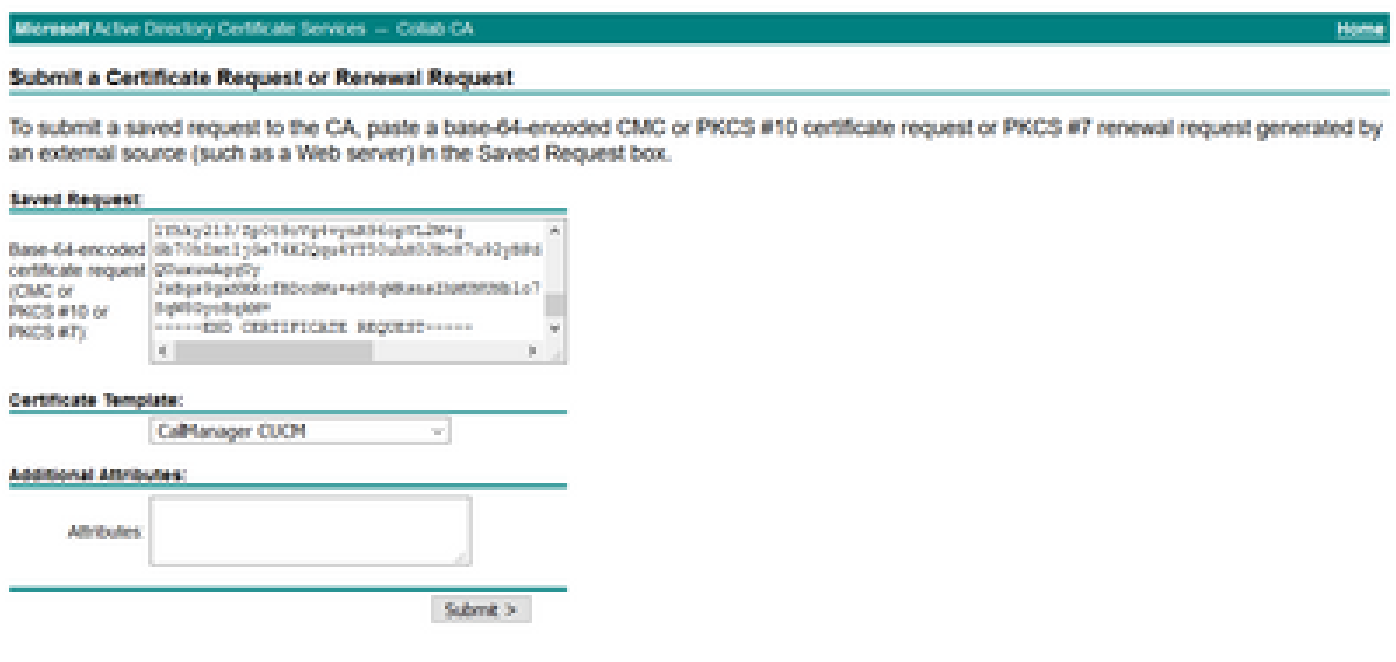
Paso 7. Navegue hasta Solicitar un certificado > Solicitud de certificado avanzada, como se muestra en la imagen.



Paso 8. Abra el archivo CSR y copie todo su contenido:



Paso 9. Pegue el CSR en el campo Solicitud de certificado codificado en Base-64. En Plantilla de certificado, seleccione la plantilla correcta y seleccione Enviar, como se muestra en la imagen.



Paso 10. Por último, seleccione Base 64 codificada y Descargar cadena de certificados; el archivo generado se puede cargar ahora en CUCM.

Certificate issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Verificación

El procedimiento de verificación es en realidad parte del proceso de configuración.

Troubleshoot

Actualmente no hay información de troubleshooting específica disponible para esta configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).