

# Crea modelli di certificato CA di Windows per CUCM

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Modello Callmanager / Tomcat / TVS](#)

[Modello IPSec](#)

[Modello CAPF](#)

[Genera una richiesta di firma del certificato](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

In questo documento viene descritta una procedura dettagliata per creare modelli di certificato in Autorità di certificazione (CA) basate su Windows Server.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM versione 11.5(1).
- È inoltre consigliabile avere una conoscenza di base dell'amministrazione di Windows Server

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Le informazioni fornite in questo documento si basano sulla versione 11.5(1) di CUCM.
- Microsoft Windows Server 2012 R2 con i servizi CA installati.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata


ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Questi modelli di certificato sono conformi ai requisiti di estensione X.509 per ogni tipo di certificato Cisco Unified Communications Manager (CUCM).

Esistono cinque tipi di certificati che possono essere firmati da una CA esterna:

Certificato	Utilizzo	Servizi interessati
CallManager	Presentato durante la registrazione sicura del dispositivo, può firmare i file CTL (Certificate Trust List)/ITL (Internal Trust List), utilizzati per interazioni protette con altri server, ad esempio i trunk SIP (Secure Session Initiation Protocol).	<ul style="list-style-type: none"> <li>· Cisco Call Manager</li> <li>· Cisco CTI Manager</li> <li>· Cisco TFTP</li> </ul>
tomcat	Presentato per le interazioni HTTPS (Secure Hypertext Transfer Protocol).	<ul style="list-style-type: none"> <li>· Cisco Tomcat</li> <li>· Single Sign-On (SSO)</li> <li>· Mobilità di estensione</li> <li>· Directory aziendale</li> </ul>
ipsec	Utilizzato per la generazione di file di backup, nonché per l'interazione di IPsec (IP Security) con i gateway Media Gateway Control Protocol (MGCP) o H323.	<ul style="list-style-type: none"> <li>· Cisco DRF Master</li> <li>· Cisco DRF locale</li> </ul>
CAPF	Utilizzato per generare certificati LSC (Locally Significant Certificates) per telefoni.	<ul style="list-style-type: none"> <li>· Funzione proxy Cisco Certificate Authority</li> </ul>
TVS	Utilizzato per creare una connessione al servizio di verifica attendibilità (TVS), quando i telefoni non sono in grado di autenticare un certificato sconosciuto.	<ul style="list-style-type: none"> <li>· Servizio di verifica attendibilità Cisco</li> </ul>

 Nota: il certificato IPsec non è correlato al master DRF Cisco e a Cisco DRF Local poiché nelle versioni più recenti viene utilizzato il certificato Tomcat. Non è prevista l'aggiunta di questa modifica alla versione 12.5 o precedenti.

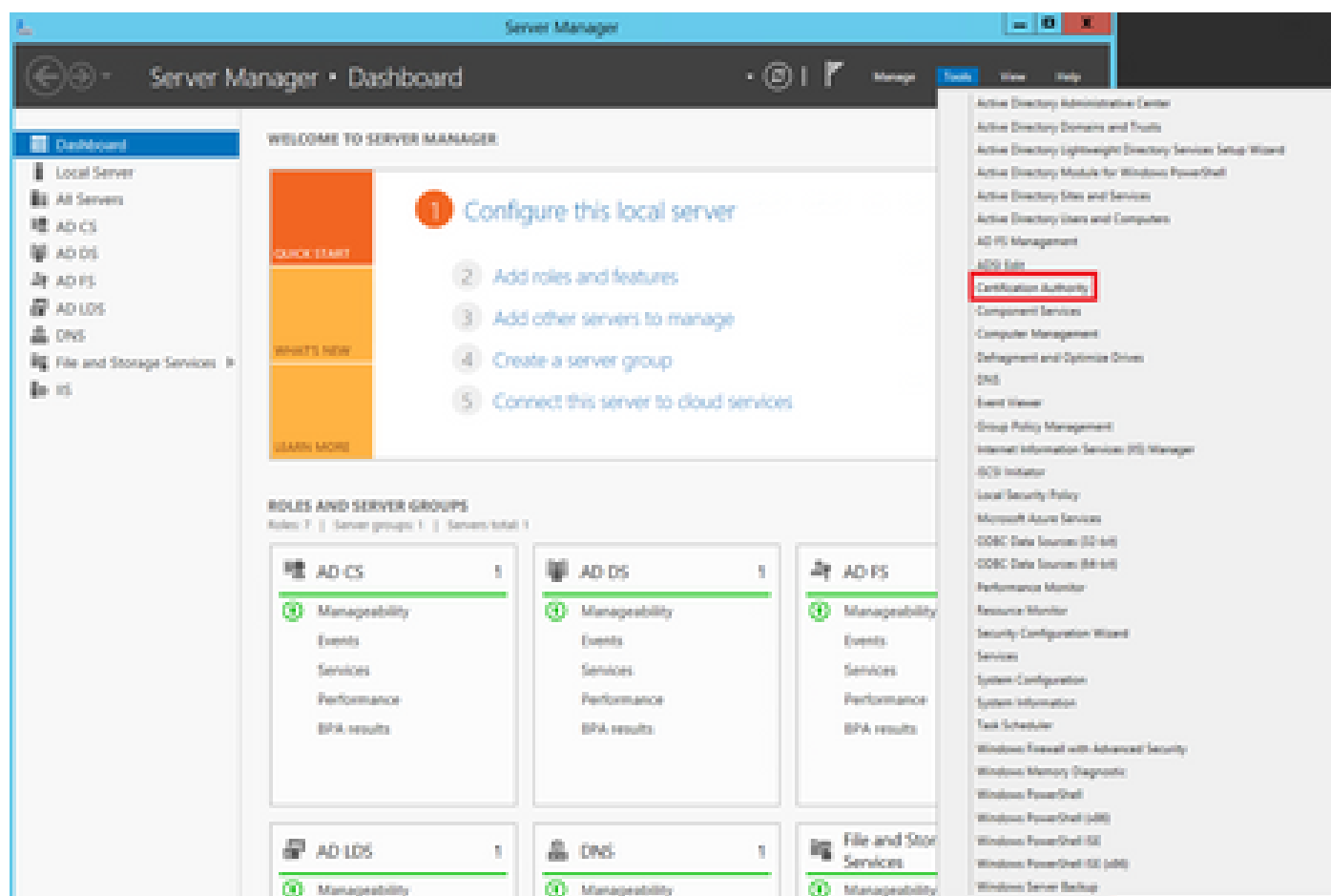
Ognuno di questi certificati ha alcuni requisiti di estensione X.509 che devono essere impostati, altrimenti si possono verificare comportamenti errati su uno qualsiasi dei suddetti servizi:

Certificato	Utilizzo chiavi X.509	Utilizzo chiavi esteso X.509
CallManager	<ul style="list-style-type: none"><li>Firma digitale</li><li>· Crittografia</li><li>· Crittografia dei dati</li></ul>	<ul style="list-style-type: none"><li>· Autenticazione server Web</li><li>· Autenticazione client Web</li></ul>
tomcat	<ul style="list-style-type: none"><li>Firma digitale</li><li>· Crittografia</li><li>· Crittografia dei dati</li></ul>	<ul style="list-style-type: none"><li>· Autenticazione server Web</li><li>· Autenticazione client Web</li></ul>
ipsec	<ul style="list-style-type: none"><li>Firma digitale</li><li>· Crittografia</li><li>· Crittografia dei dati</li></ul>	<ul style="list-style-type: none"><li>· Autenticazione server Web</li><li>· Autenticazione client Web</li><li>· Sistema terminale IPsec</li></ul>
CAPF	<ul style="list-style-type: none"><li>Firma digitale</li><li>· Firma certificato</li><li>· Crittografia</li></ul>	<ul style="list-style-type: none"><li>· Autenticazione server Web</li><li>· Autenticazione client Web</li></ul>
TVS	<ul style="list-style-type: none"><li>Firma digitale</li><li>· Crittografia</li><li>· Crittografia dei dati</li></ul>	<ul style="list-style-type: none"><li>· Autenticazione server Web</li><li>· Autenticazione client Web</li></ul>

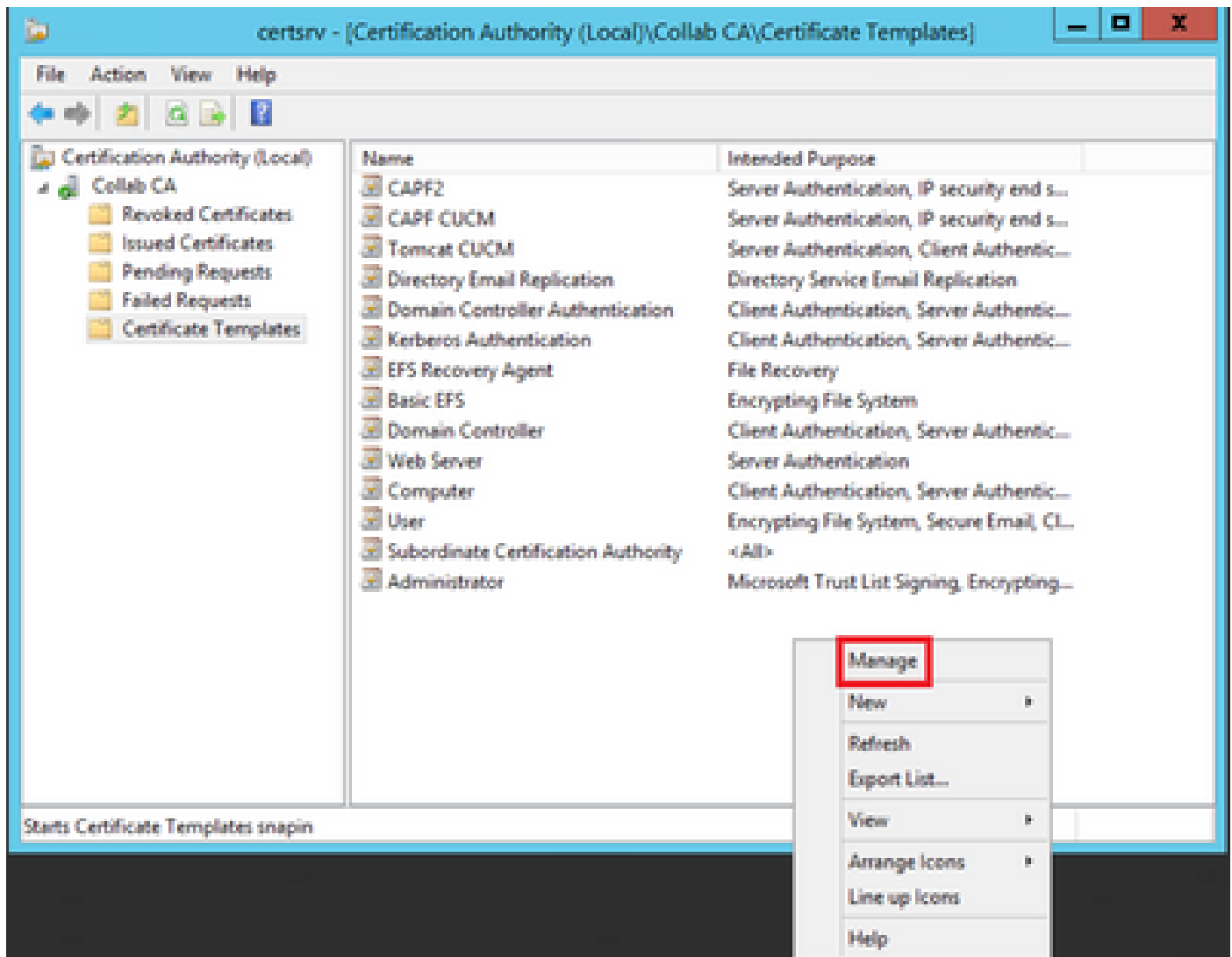
Per ulteriori informazioni, fare riferimento alla [Guida alla sicurezza per Cisco Unified Communications Manager](#)

## Configurazione

Passaggio 1. In Windows Server, selezionare Server Manager > Strumenti > Autorità di certificazione, come mostrato nell'immagine.



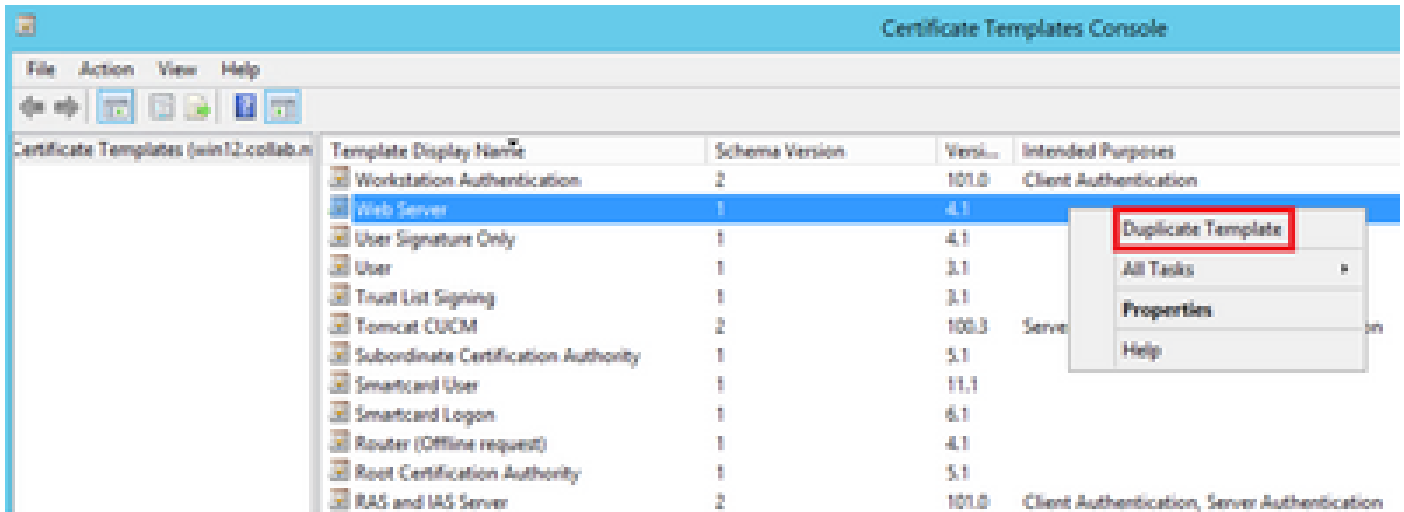
Passaggio 2. Selezionare la CA, passare a Modelli di certificato, fare clic con il pulsante destro del mouse sull'elenco e selezionare Gestisci, come mostrato nell'immagine.



## Modello Callmanager / Tomcat / TVS

Nelle immagini successive viene visualizzata solo la creazione del modello CallManager, ma è possibile seguire gli stessi passaggi per creare i modelli di certificato per i servizi Tomcat e TVS. L'unica differenza consiste nel garantire che il nome del servizio corrispondente venga utilizzato per ogni nuovo modello al passaggio 2.

Passaggio 1. Individuare il modello Web Server, fare clic con il pulsante destro del mouse su di esso e selezionare Duplica modello, come mostrato nell'immagine.



Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

## 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

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.



# 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

Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Consenti scambio chiave solo con crittografia (cifatura chiave)
- Consenti crittografia dei dati utente

## 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

Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.

# 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.

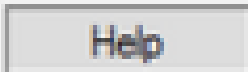
Extensions included in this template:

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



Description of Application Policies:

Server Authentication



Passaggio 6. Cercare Autenticazione client, selezionarlo e scegliere OK sia in questa finestra che in quella precedente, come mostrato nell'immagine.

## 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

Passaggio 7. Tornare al modello, selezionare Applica, quindi 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

Edit...

Description of Application Policies:

- Client Authentication
- Server Authentication

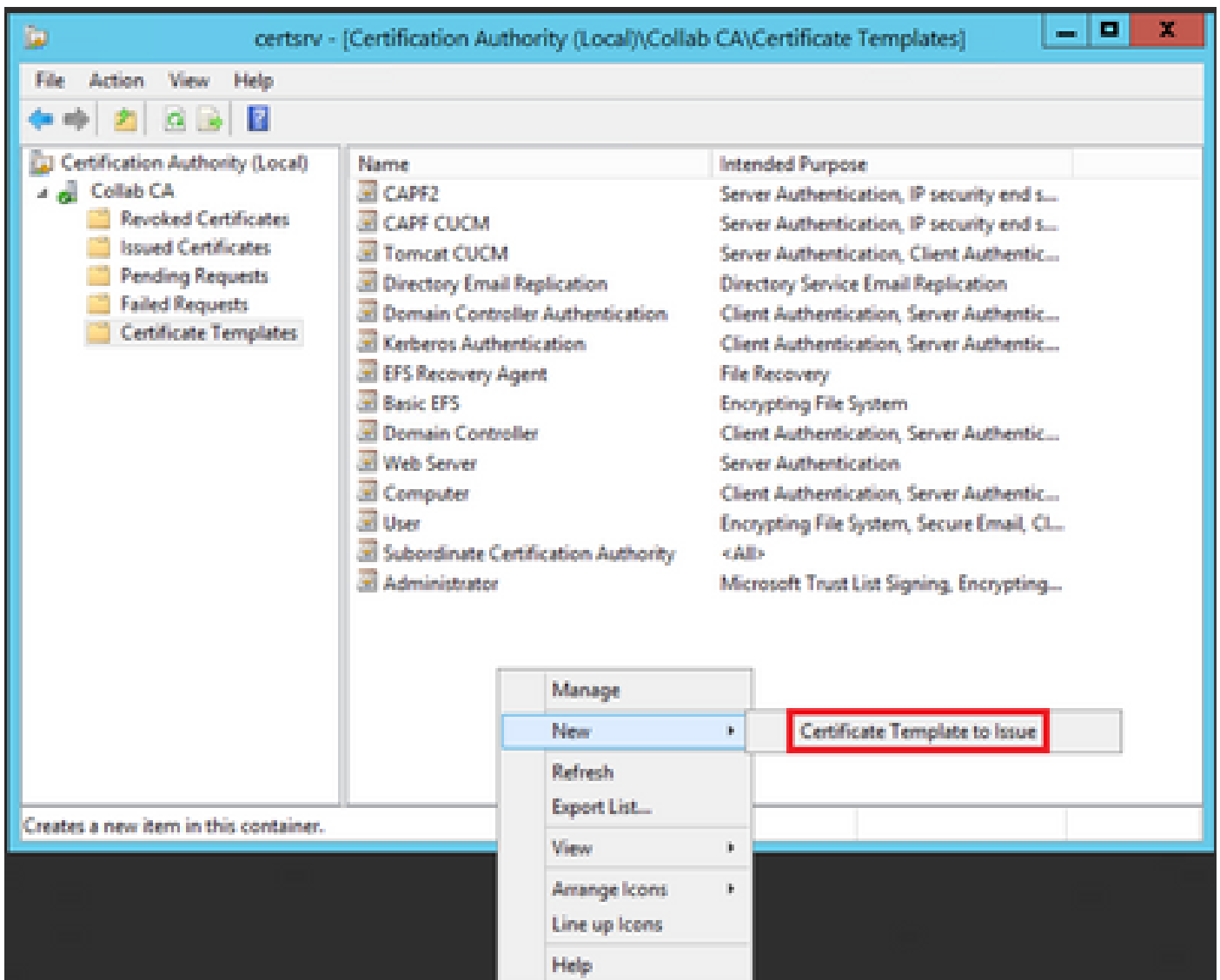
OK

Cancel

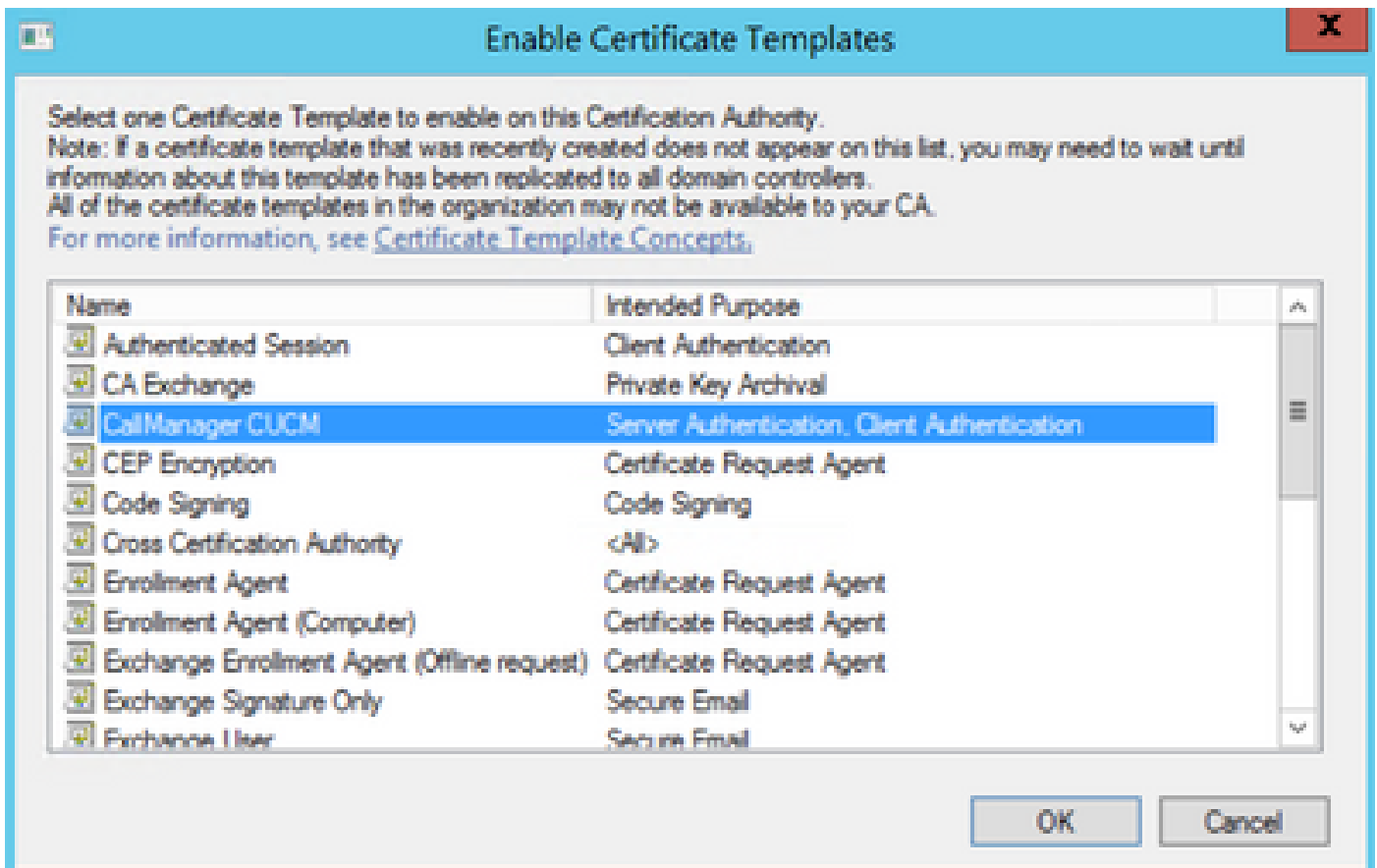
Apply

Help

Passaggio 8. Chiudere la finestra Console modello certificato e tornare alla prima finestra, selezionare Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.



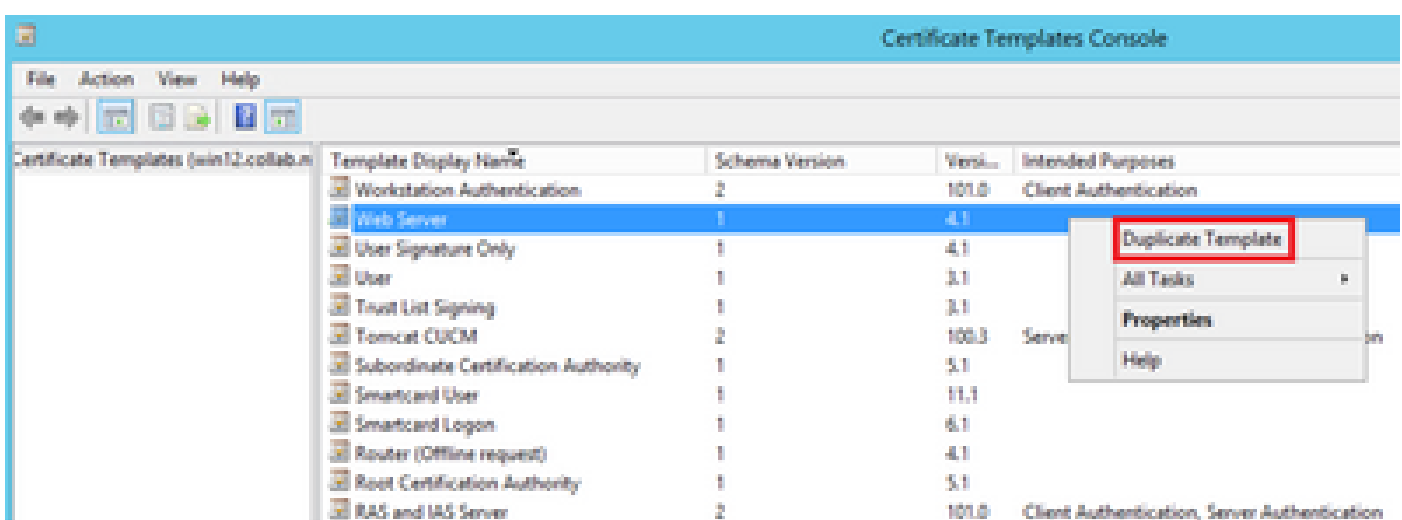
Passaggio 9. Selezionare il nuovo modello CallManager CUCM e scegliere OK, come mostrato nell'immagine.



Passaggio 10. Ripetere tutti i passaggi precedenti per creare modelli di certificato per i servizi Tomcat e TVS in base alle esigenze.

## Modello IPsec

Passaggio 1. Individuare il modello Web Server, fare clic con il pulsante destro del mouse su di esso e selezionare Duplica modello, come mostrato nell'immagine.



Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

## 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

OK Cancel Apply Help

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.

# 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

Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Consenti scambio chiave solo con crittografia (cifatura chiave)
- Consenti crittografia dei dati utente

## 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



Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.






## 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

Passaggio 6. Cercare Autenticazione client, selezionarla e quindi OK, come mostrato nell'immagine.

## 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

Passaggio 7. Selezionare di nuovo Add, cercare IP security end system, selezionarlo, quindi selezionare OK anche in questo caso e nella finestra precedente.

## 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

Passaggio 8. Tornare al modello, selezionare Apply (Applica), quindi OK, come mostrato nell'immagine.

## 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

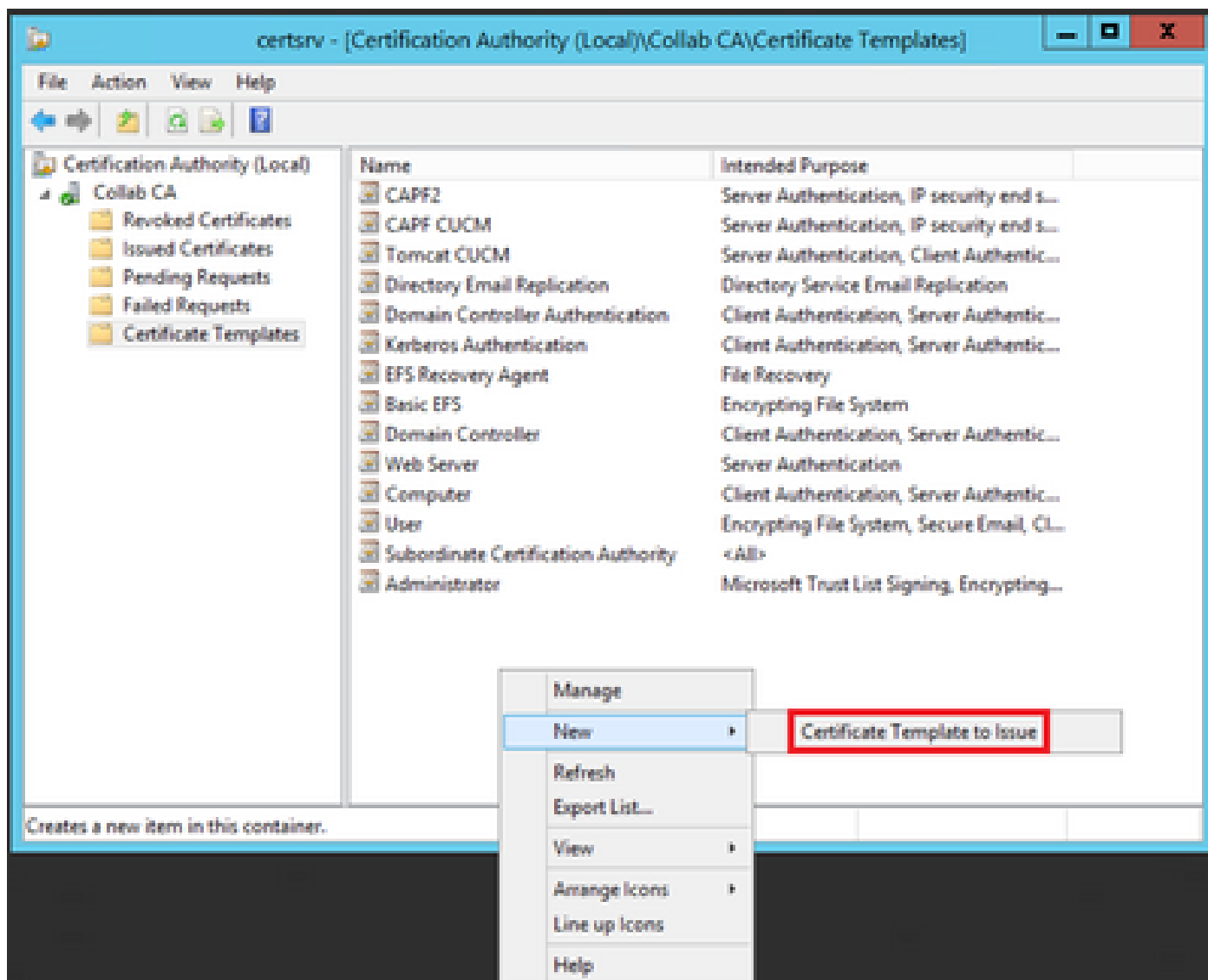
Cancel

Apply

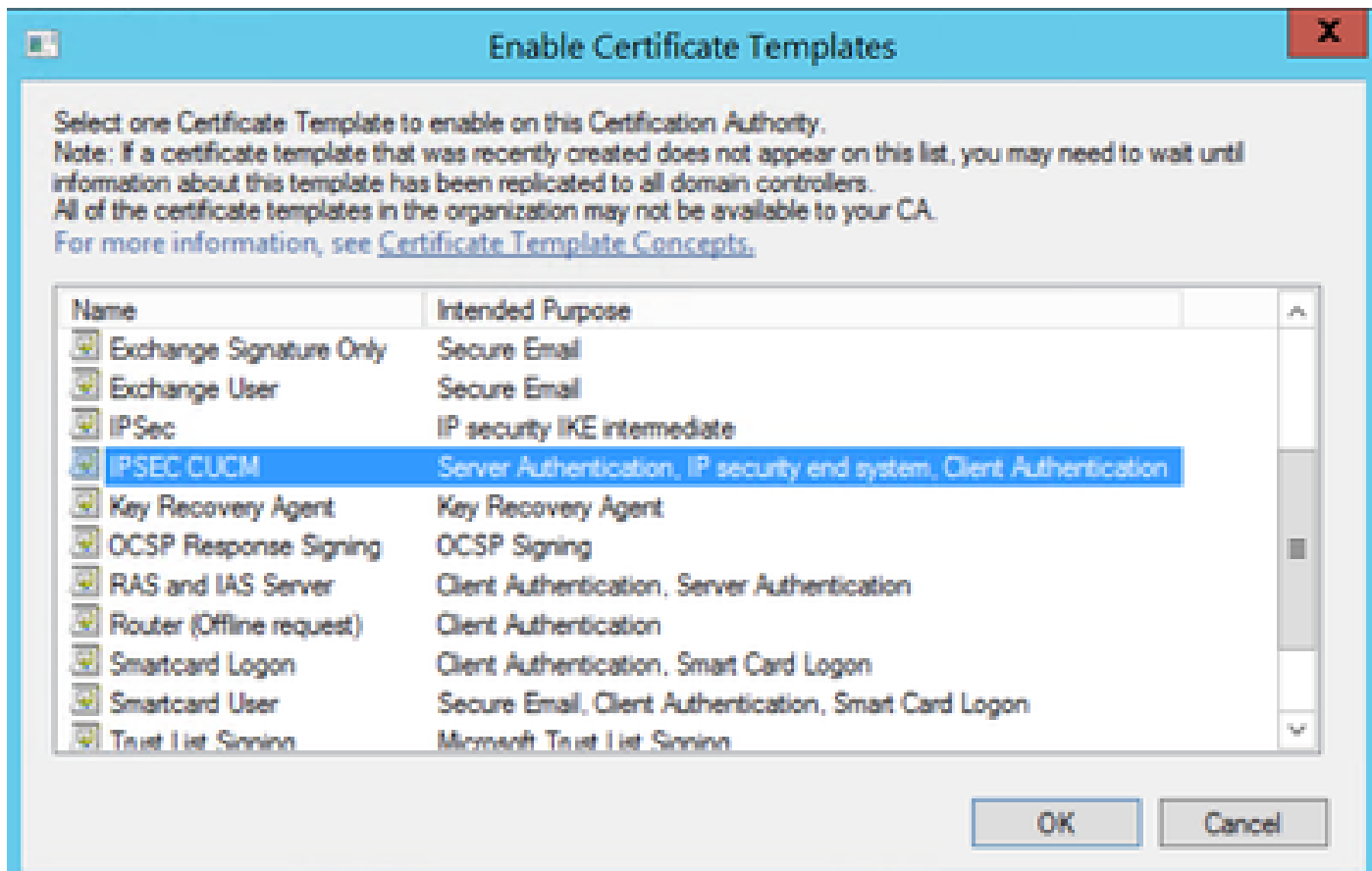
Help



Passaggio 9. Chiudere la finestra della console Modelli di certificato e tornare alla prima finestra, passare a Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.

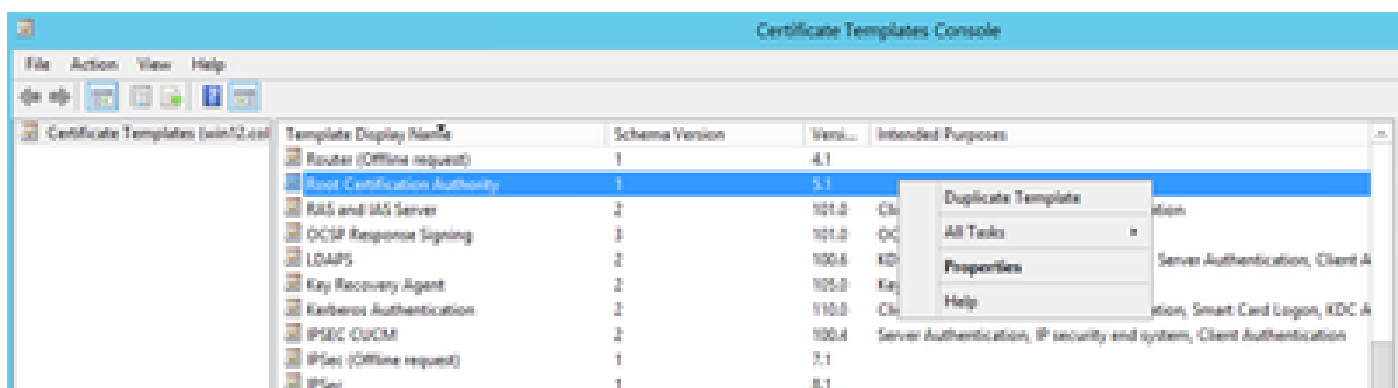


Passaggio 10. Selezionare il nuovo modello IPSEC CUCM e scegliere OK, come mostrato nell'immagine.



## Modello CAPF

Passaggio 1. Individuare il modello Root CA (CA radice) e fare clic con il pulsante destro del mouse su di esso. Quindi selezionate **Duplica modello (Duplicate Template)**, come mostrato nell'immagine.



Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

## Properties of New Template



Superseded Templates

Extensions

Security

Compatibility

General

Issuance Requirements

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

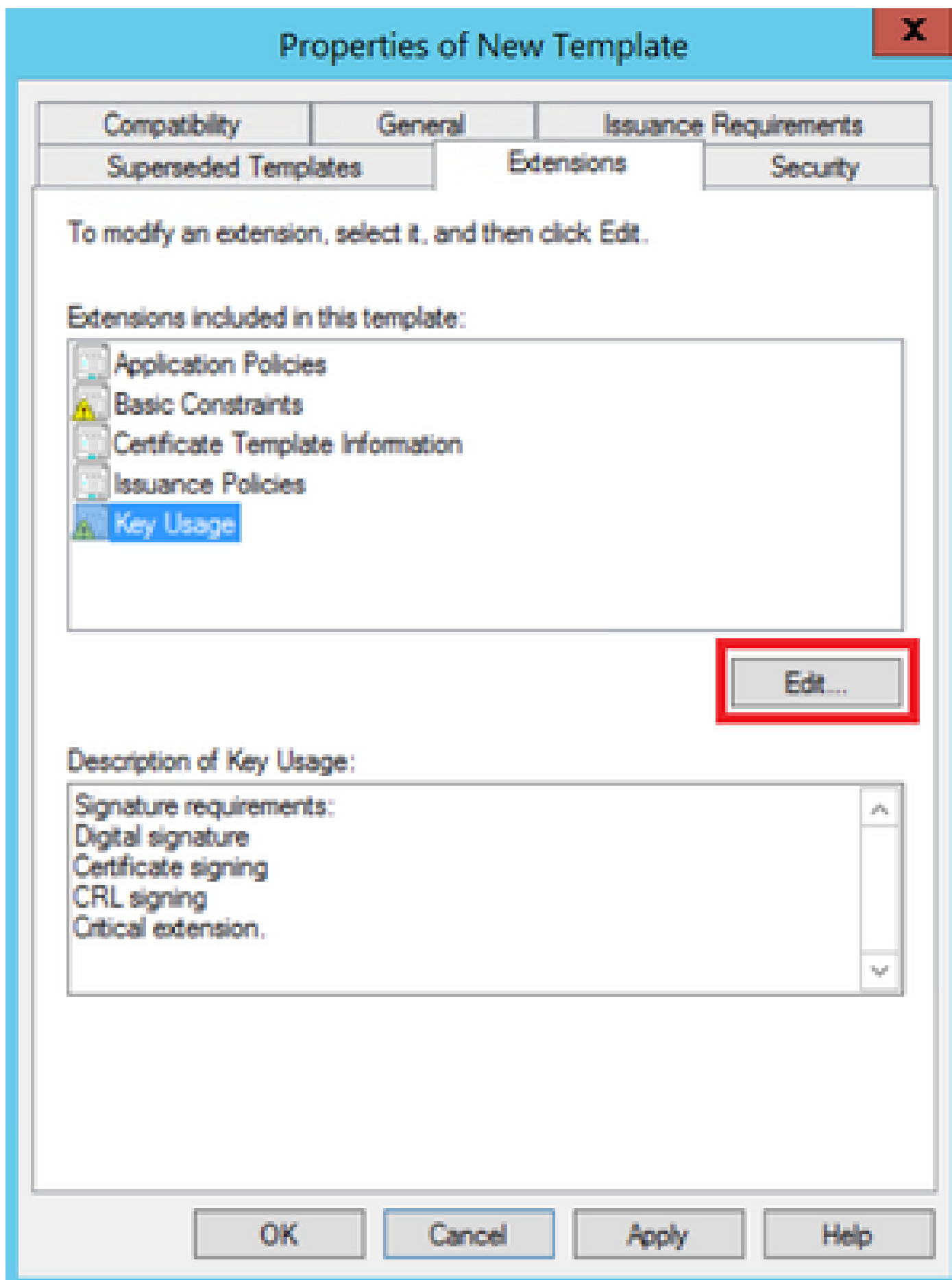
OK

Cancel

Apply

Help

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.



Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Firma certificato
- Firma 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

Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.

# 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



Passaggio 6. Cercare Autenticazione client, selezionarla e quindi scegliere OK, come mostrato nell'immagine.

## 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

Passaggio 7. Selezionare di nuovo Add, cercare IP security end system, selezionarlo, quindi selezionare OK anche su questo e sulla finestra precedente, come mostrato nell'immagine.

## 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

Passaggio 8. Tornare al modello, selezionare Apply (Applica), quindi OK, come mostrato nell'immagine.

## 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

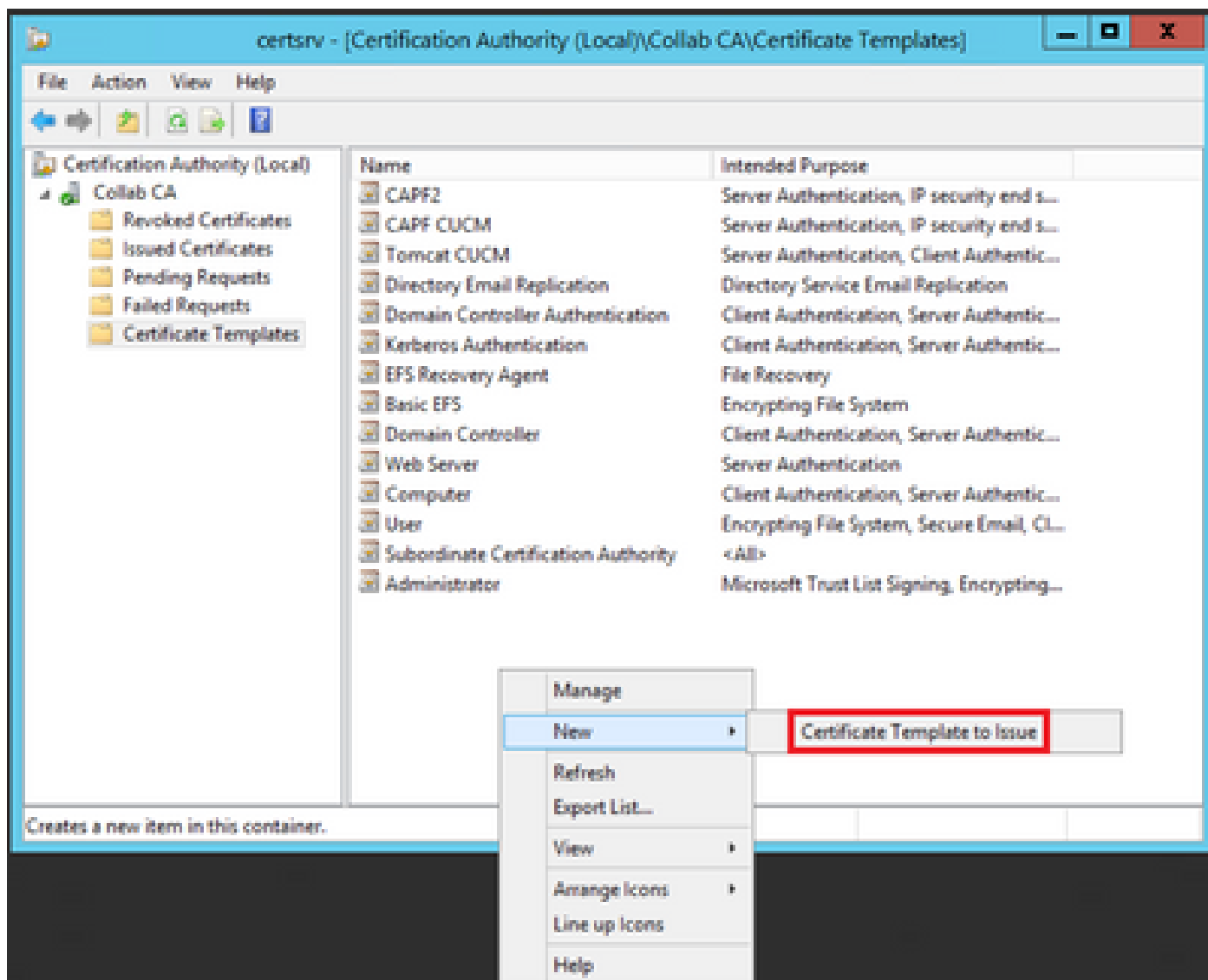
OK

Cancel

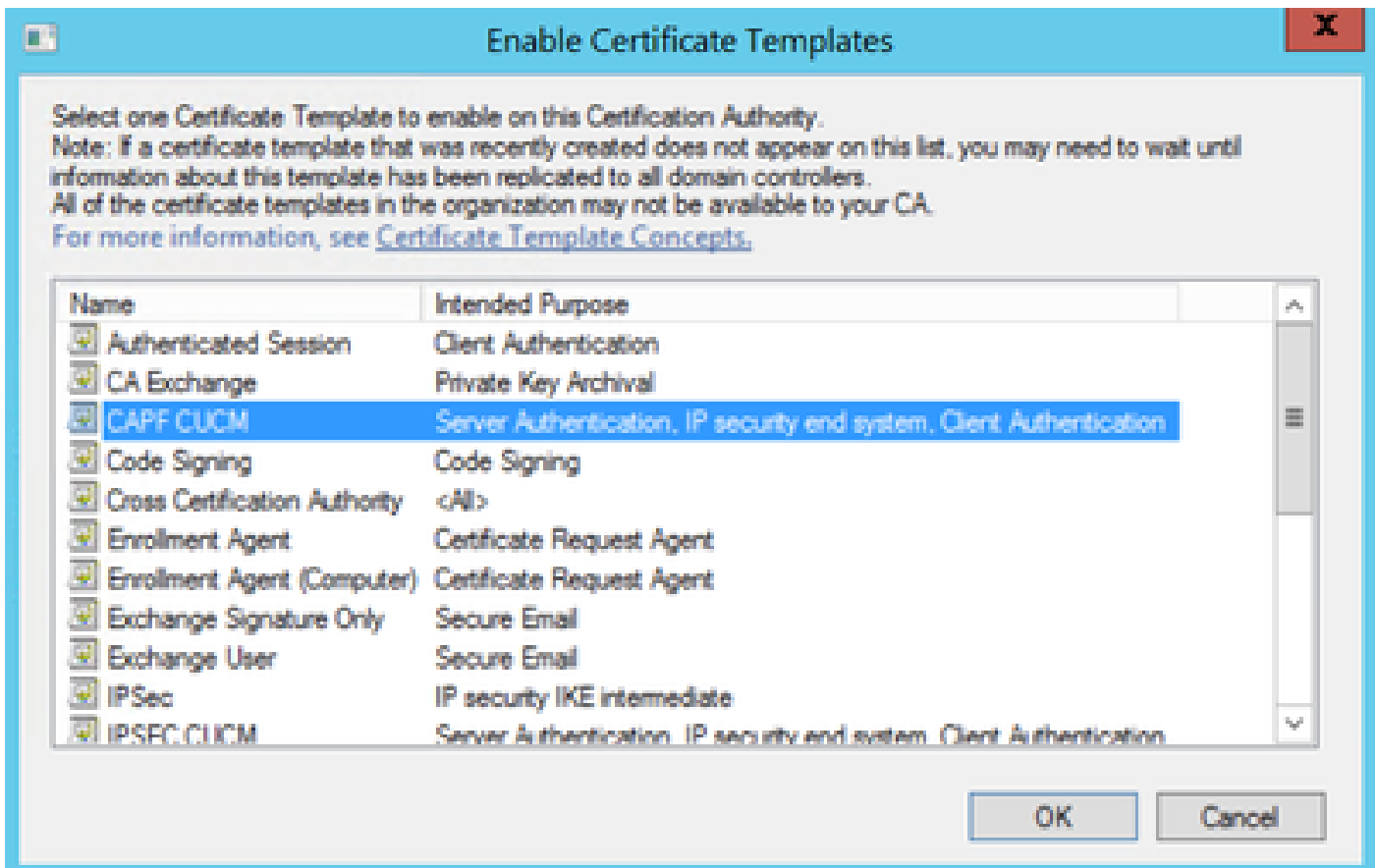
Apply

Help

Passaggio 9. Chiudere la finestra della console Modelli di certificato e tornare alla prima finestra, passare a Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.



Passaggio 10. Selezionate il nuovo modello CAPF CUCM e OK, come mostrato nell'immagine.



## Genera una richiesta di firma del certificato

Utilizzare questo esempio per generare un certificato CallManager con l'utilizzo dei nuovi modelli creati. La stessa procedura può essere utilizzata per qualsiasi tipo di certificato. È sufficiente selezionare il certificato e i tipi di modello di conseguenza:

Passaggio 1. In CUCM, selezionare Amministrazione sistema operativo > Protezione > Gestione certificati > Genera CSR.

Passaggio 2. Selezionate queste opzioni e selezionate Genera (Generate), come mostrato nell'immagine.


- Scopo certificato: CallManager
- Distribuzione: <può trattarsi di un solo server o di più 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

Passaggio 3. Viene generato un messaggio di conferma, come mostrato nell'immagine.

**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].

Passaggio 4. Nell'elenco dei certificati cercare la voce con il tipo Solo CSR e selezionarla, come mostrato nell'immagine.

**Certificate List**

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

Status

16 records found

Certificate List (1 - 50 of 56)   Rows per Page 10

Find Certificate List where Certificate begins with Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
auth	auth_admin	Self-signed	RSA	11SPUB.maucabal.lab	auth_admin	01/27/2018	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	01/30/2013	Self-signed certificate generated by system
CallManager-ECDSA	11SPUB-EC.maucabal.lab	Self-signed	EC	11SPUB.maucabal.lab	11SPUB-EC.maucabal.lab	01/04/2013	Self-signed certificate generated by system
CallManager-trust	11SPUB-EC.maucabal.lab	Self-signed	EC	11SPUB.maucabal.lab	11SPUB-EC.maucabal.lab	01/04/2013	Trust Certificate

Passaggio 5. Nella finestra pop-up, selezionare Download CSR, quindi salvare il file sul computer.

**CSR Details for 11SPUB-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**

```

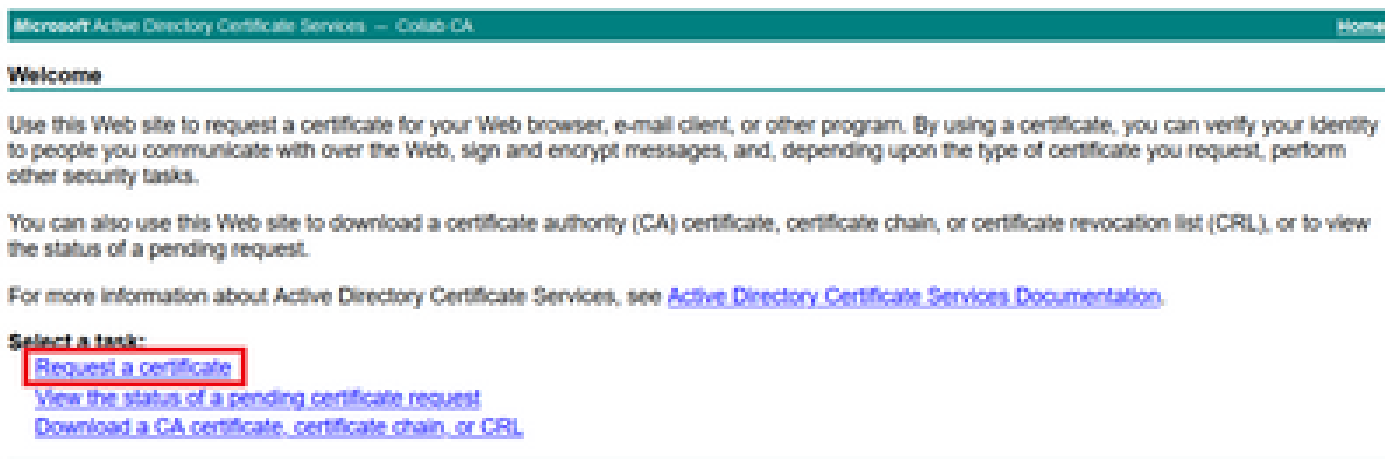
PKCS-10 Request: [
Version: 0
Subject: CN=11SPUB-ms.maucabal.lab, OU=disco, O=disco, L=disco, ST=disco, C=MX
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d
cabc144fd5f1538efe514fd8207d3dde43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
Requested Extensions [

```

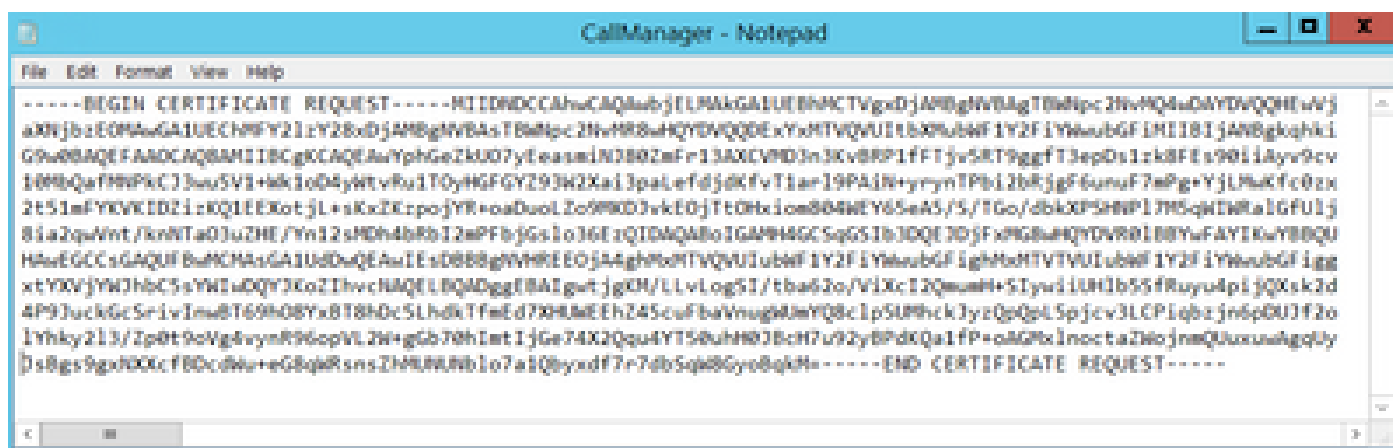
Delete   Download CSR

Passaggio 6. Nel browser passare a questo URL e immettere le credenziali dell'amministratore del controller di dominio: <https://<yourWindowsServerIP>/certsrv/>.

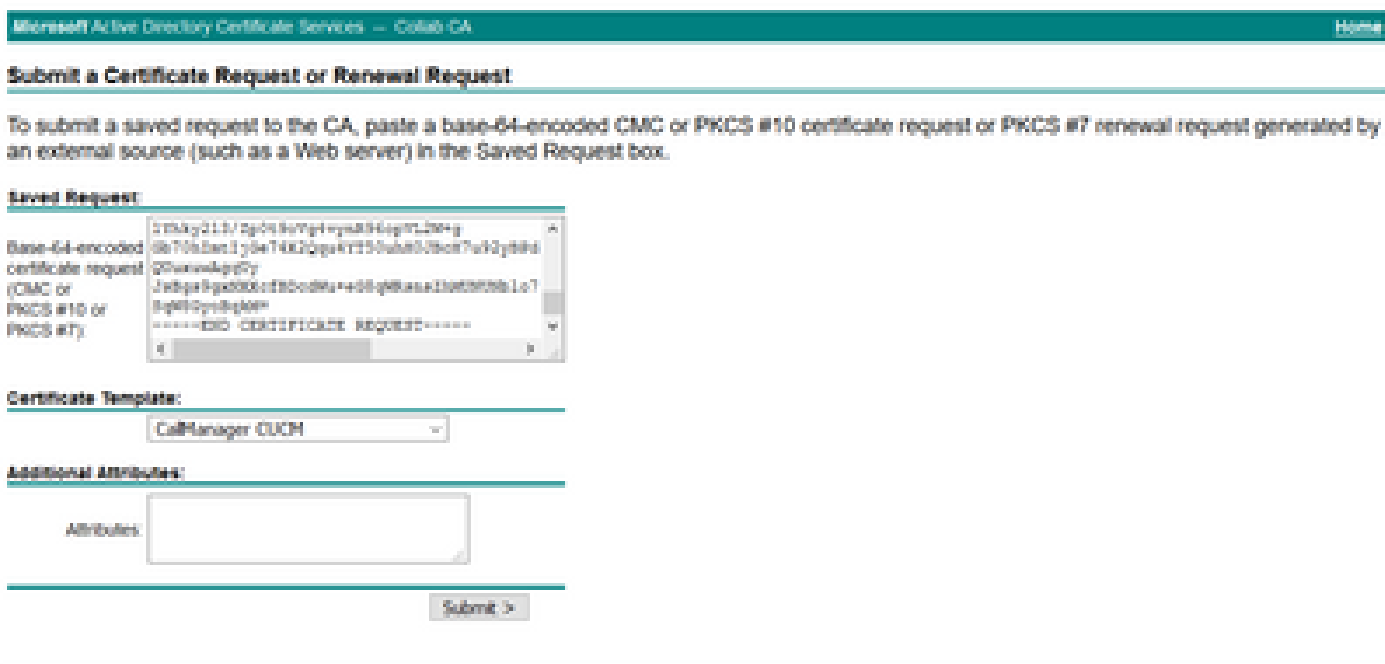
Passaggio 7. Passare a Richiedi un certificato > Richiesta avanzata di certificati, come mostrato nell'immagine.



Passaggio 8. Aprire il file CSR e copiarne il contenuto:



Passaggio 9. Incollare il CSR nel campo Richiesta certificato con codifica Base 64. In Modello di certificato selezionare il modello corretto e scegliere Invia, come illustrato nell'immagine.



Passaggio 10. Infine, selezionare Base 64 encoded (Codificato in base 64) e Download certificate chain (Scarica catena di certificati), il file generato può ora essere caricato in CUCM.

### Certificate issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

---

## Verifica

La procedura di verifica fa effettivamente parte del processo di configurazione.

## Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).