

Erstellen von Windows CA-Zertifikatvorlagen für CUCM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[CallManager/Tomcat/TVS-Vorlage](#)

[IPsec-Vorlage](#)

[CAPF-Vorlage](#)

[Generieren einer Zertifikatsignierungsanforderung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt eine schrittweise Vorgehensweise zum Erstellen von Zertifikatvorlagen auf Windows Server-basierten Zertifizierungsstellen, die die X.509-Erweiterungsanforderungen für jeden Typ eines Cisco Unified Communications Manager (CUCM)-Zertifikats erfüllen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CUCM-Version 11.5(1) oder höher
- Grundkenntnisse der Windows Server-Administration werden ebenfalls empfohlen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Die Informationen in diesem Dokument basieren auf CUCM-Version 11.5(1) oder höher.
- Microsoft Windows Server 2012 R2 mit installierten Zertifizierungsstellendiensten.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Es gibt fünf Zertifikatstypen, die von einer externen Zertifizierungsstelle signiert werden können:

Zertifikat	Nutzung	Betroffene Services
CallManager	Wird bei der Registrierung sicherer Geräte angezeigt und kann CTL- (Certificate Trust List)/ITL-Dateien (Internal Trust List) signieren, die für sichere Interaktionen mit anderen Servern, z. B. sicheren SIP-Trunks (Session Initiation Protocol), verwendet werden.	<ul style="list-style-type: none"> · Cisco Call Manager · Cisco CTI Manager · Cisco TFTP
tomcat	Präsentiert für HTTPS-Interaktionen (Secure Hypertext Transfer Protocol).	<ul style="list-style-type: none"> · Cisco Tomcat · Single Sign-On (SSO) · Anschlussmobilität · Firmenverzeichnis
IPsec	Verwendet für die Erstellung von Sicherungsdateien sowie für die IP Security (IPsec)-Interaktion mit MGCP- (Media Gateway Control Protocol) oder H323-Gateways.	<ul style="list-style-type: none"> · Cisco DRF Master · Cisco DRF Lokal
CAPF	Wird zum Generieren von LSC-Zertifikaten (Locally Significant Certificates) für Telefone verwendet.	<ul style="list-style-type: none"> · Cisco Certificate Authority Proxy-Funktion
TVS	Wird verwendet, um eine Verbindung mit dem Trust Verification Service (TVS) herzustellen, wenn die Telefone ein unbekanntes Zertifikat nicht authentifizieren können.	<ul style="list-style-type: none"> · Cisco Trust Verification Service

Für jedes dieser Zertifikate müssen einige X.509-Erweiterungsanforderungen festgelegt werden. Andernfalls können Sie bei den oben genannten Services auf Fehlverhalten stoßen:

Zertifikat	X.509-Schlüsselverwendung	X.509 Extended Key-Verwendung
CallManager	<ul style="list-style-type: none"> · Digitale Signatur · Schlüsselschlüsselverwendung · Datenverschlüsselung 	<ul style="list-style-type: none"> · Webserver-Authentifizierung · Webclient-Authentifizierung
tomcat	<ul style="list-style-type: none"> · Digitale Signatur · Schlüsselschlüsselverwendung · Datenverschlüsselung 	<ul style="list-style-type: none"> · Webserver-Authentifizierung · Webclient-Authentifizierung

g

- Digitale Signatur

.

IPsec

- Schlüsselschlüsselung
- Webserver-Authentifizierung
- Webclient-Authentifizierung
- IPsec-Endsystem

Datenverschlüsselung

g

- Digitale Signatur
- Zertifikatzeichen

CAPF

- Webserver-Authentifizierung
- Webclient-Authentifizierung

Schlüsselschlüsselung

- Digitale Signatur

.

TVS

- Schlüsselschlüsselung
- Webserver-Authentifizierung
- Webclient-Authentifizierung

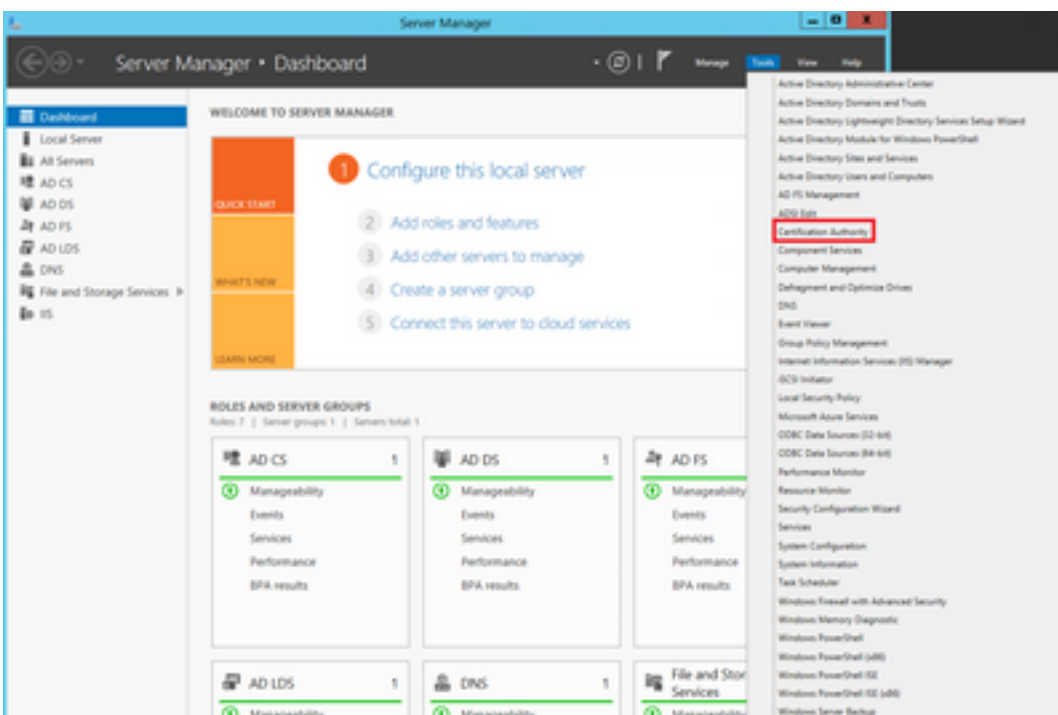
Datenverschlüsselung

g

Weitere Informationen finden Sie im [Sicherheitsleitfaden für Cisco Unified Communications Manager](#).

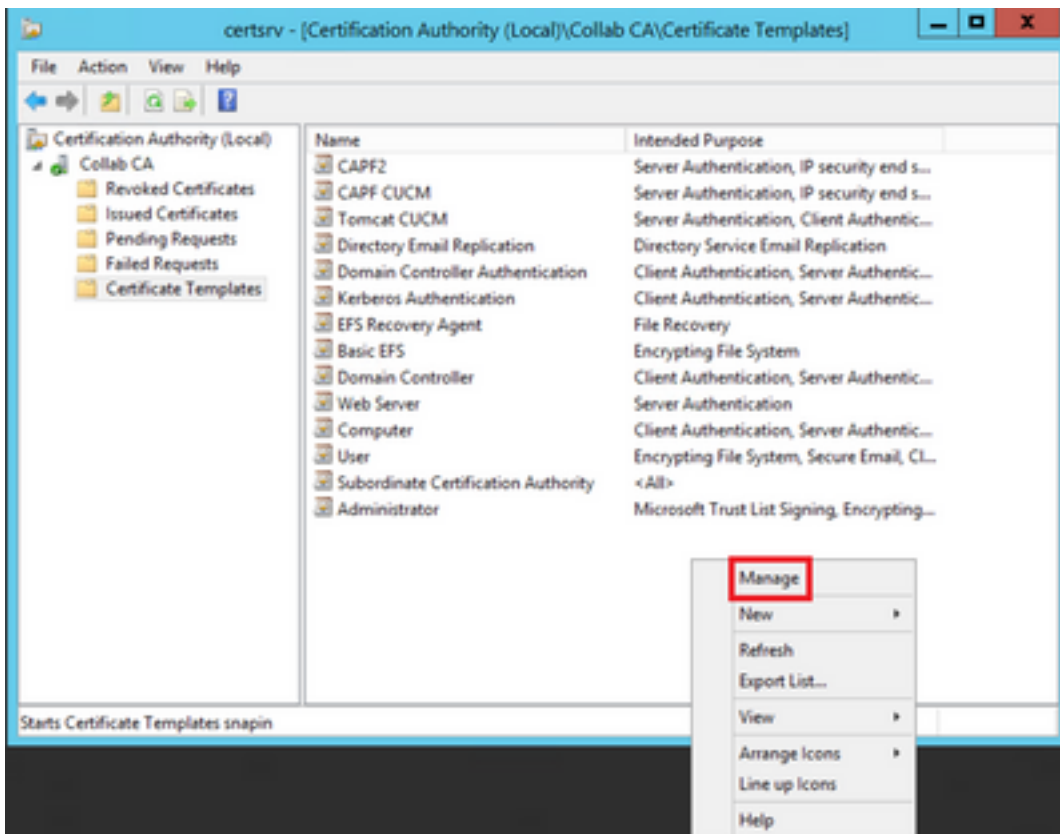
Konfigurieren

Schritt 1: Navigieren Sie auf dem Windows Server zu **Server Manager > Tools > Certification Authority**, wie im Bild dargestellt.



Schritt 2: Wählen Sie Ihre Zertifizierungsstelle aus, navigieren Sie zu **Zertifikatvorlagen**, klicken

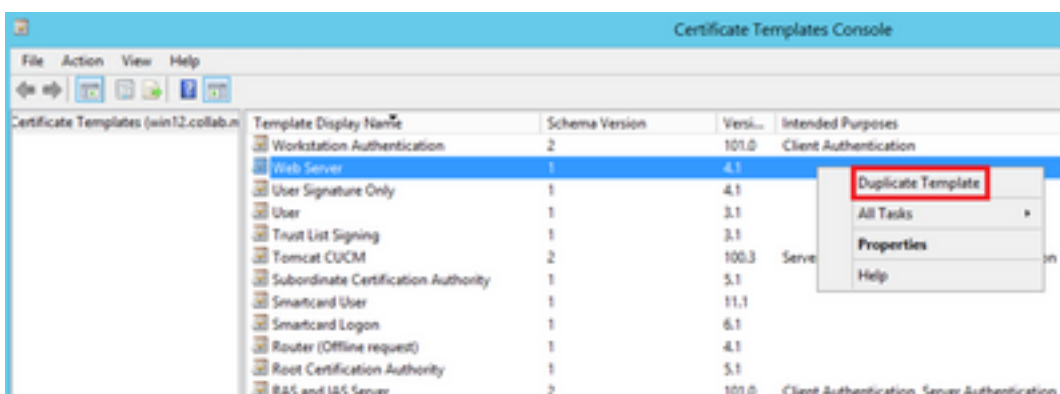
Sie mit der rechten Maustaste auf die Liste, und wählen Sie **Verwalten**, wie im Bild dargestellt.



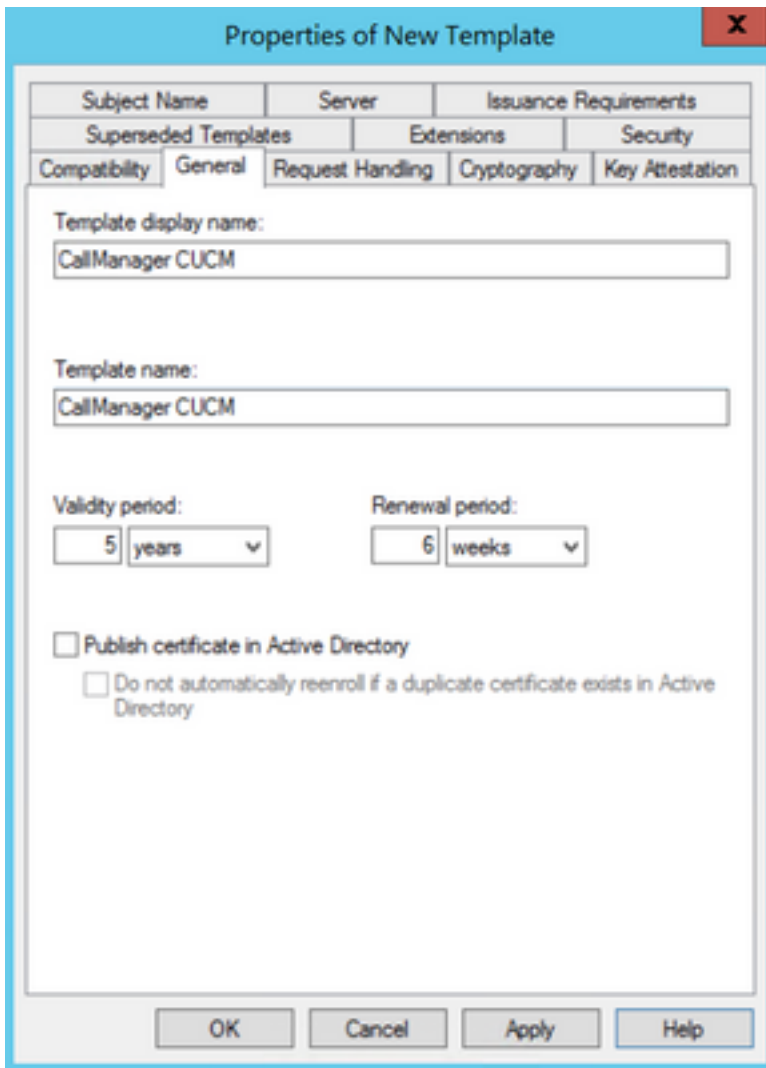
CallManager/Tomcat/TVS-Vorlage

Die nächsten Bilder zeigen nur die Erstellung der CallManager-Vorlage. Die gleichen Schritte können jedoch auch ausgeführt werden, um die Zertifikatvorlagen für die Tomcat- und TVS-Dienste zu erstellen. Der einzige Unterschied besteht darin, dass in Schritt 2 für jede neue Vorlage der entsprechende Servicename verwendet wird.

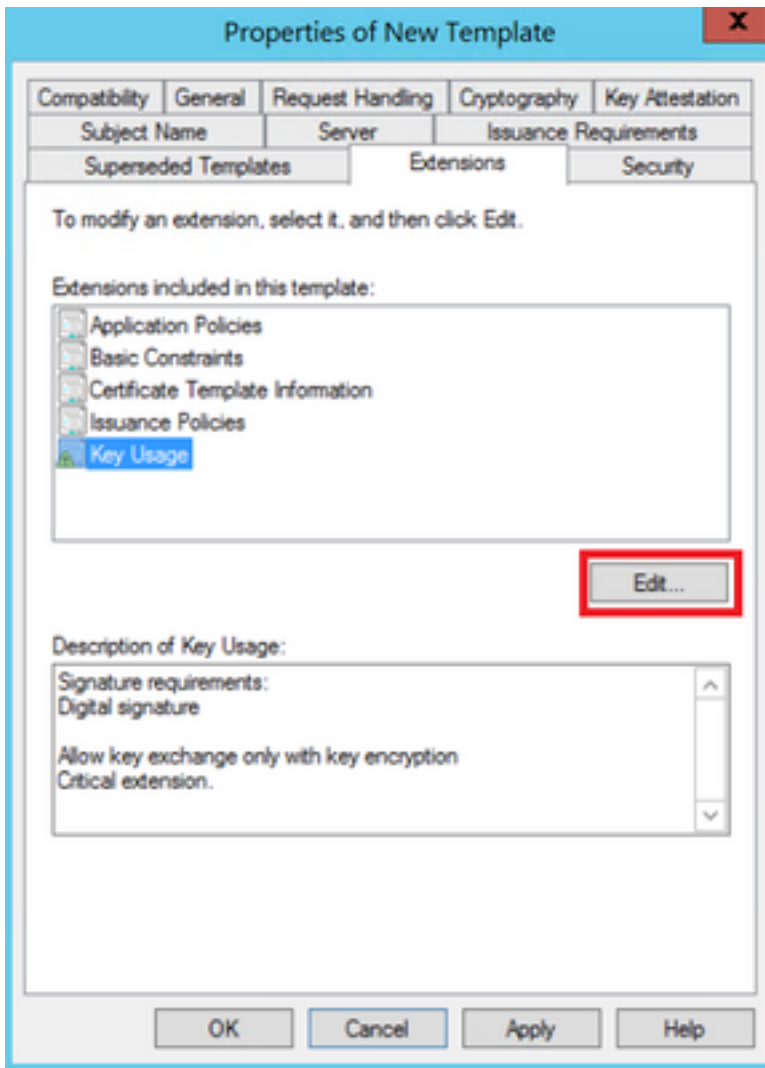
Schritt 1: Suchen Sie die **Webserver**-Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Vorlage duplizieren** aus, wie im Bild dargestellt.



Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

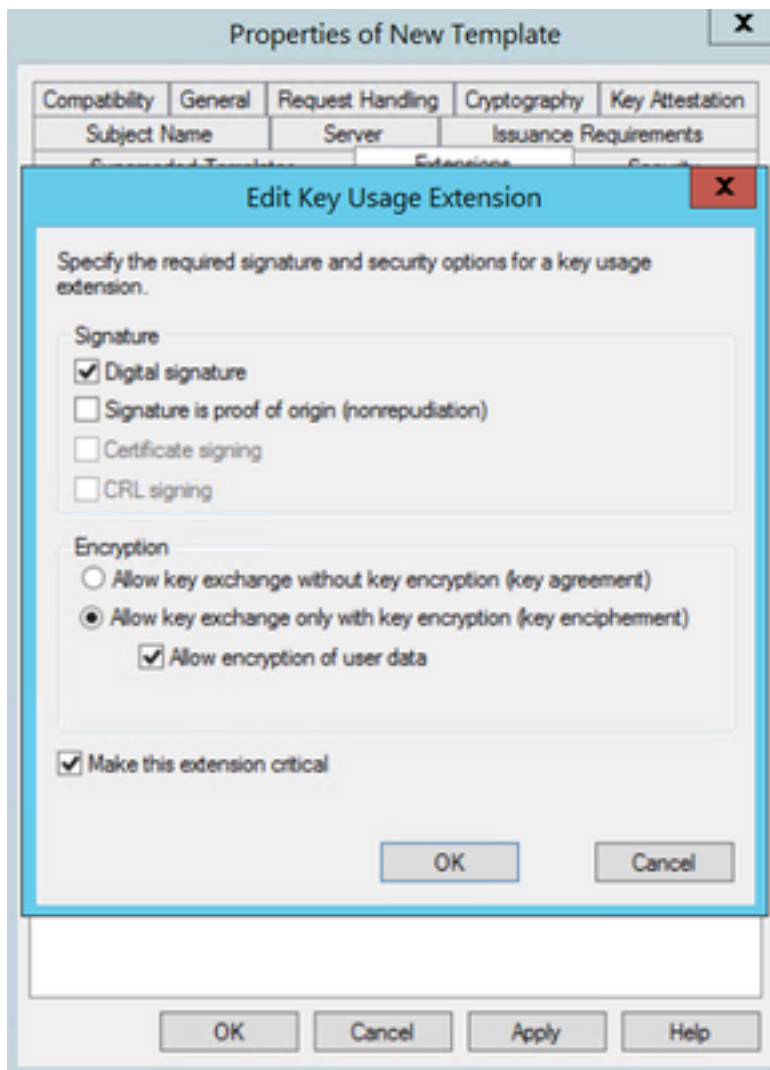


Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselerwendung > Bearbeiten**, wie im Bild dargestellt.



Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

- **Digitale Signatur**
- **Schlüsselaustausch nur mit Schlüsselverschlüsselung zulassen (Schlüsselverschlüsselung)**
- **Verschlüsselung von Benutzerdaten zulassen**



Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

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:

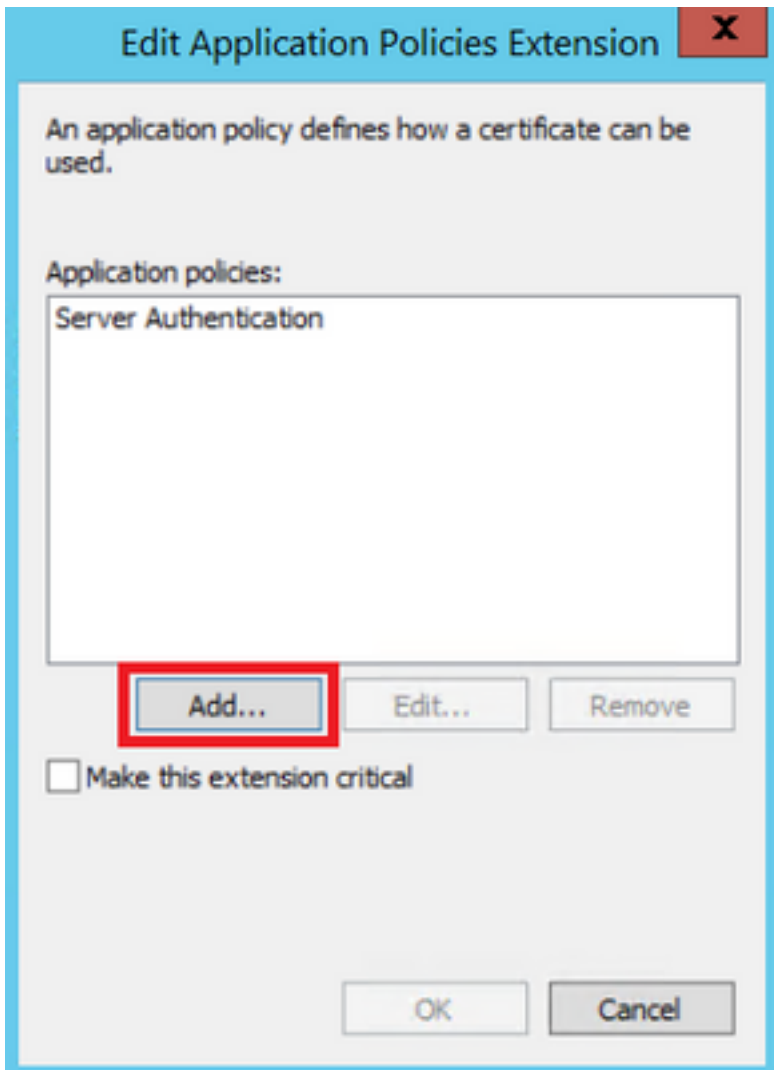
Server Authentication

OK

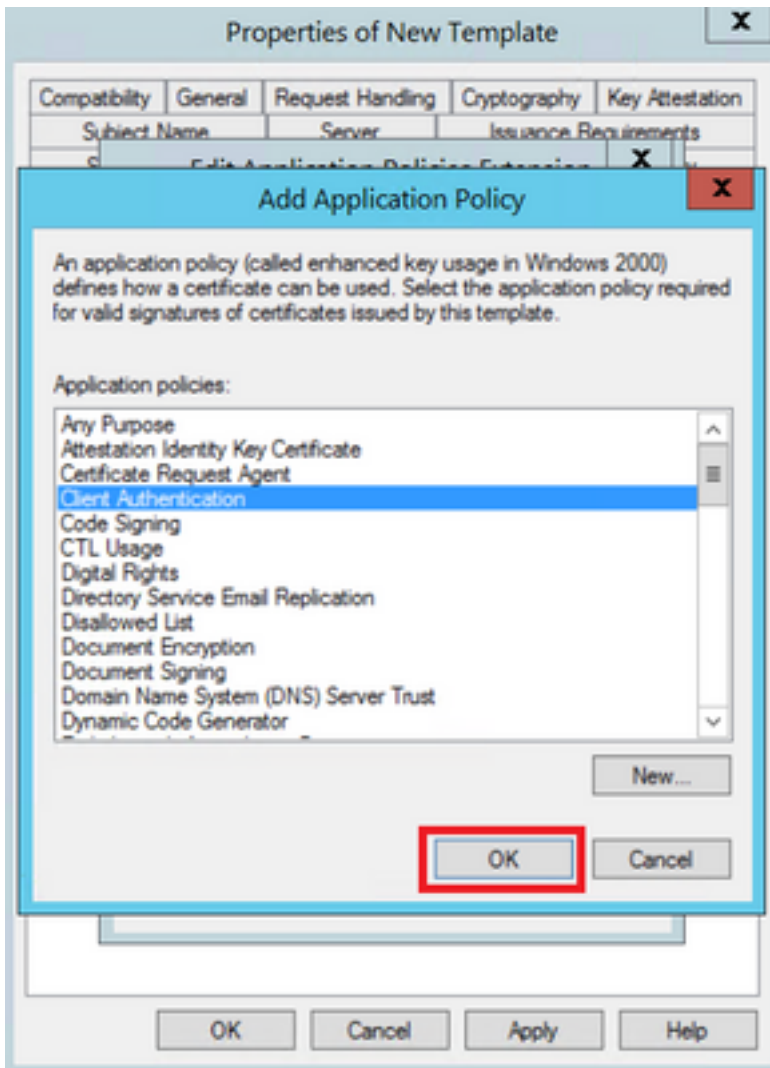
Cancel

Apply

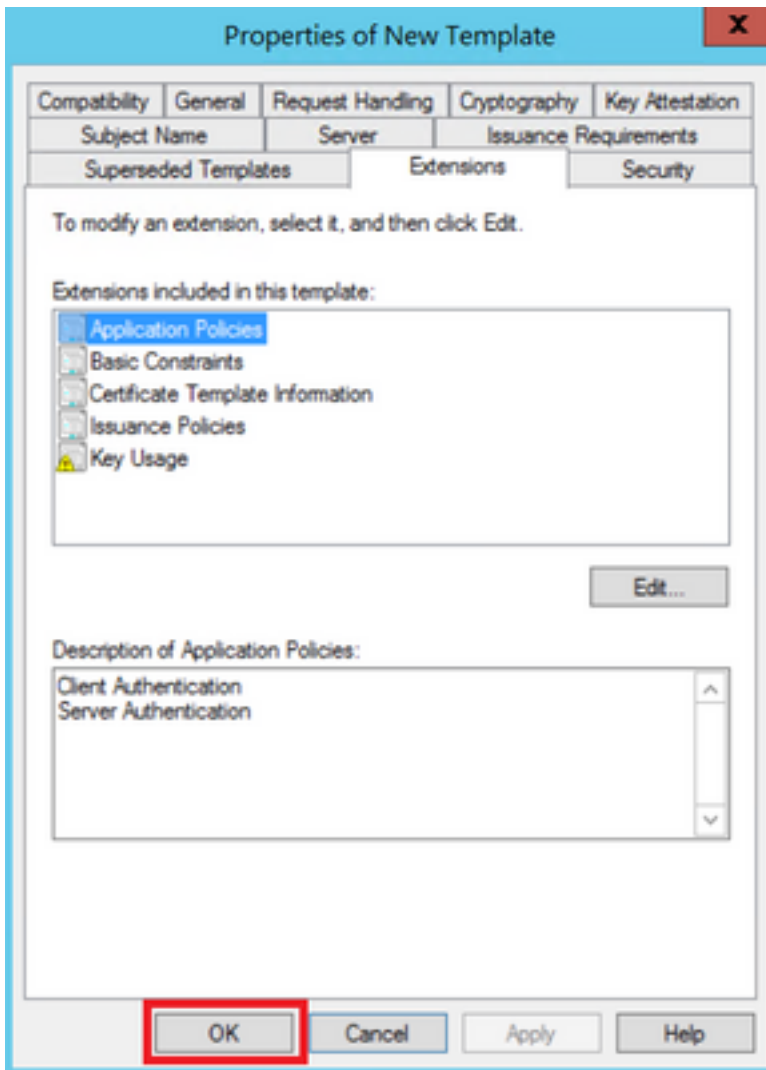
Help



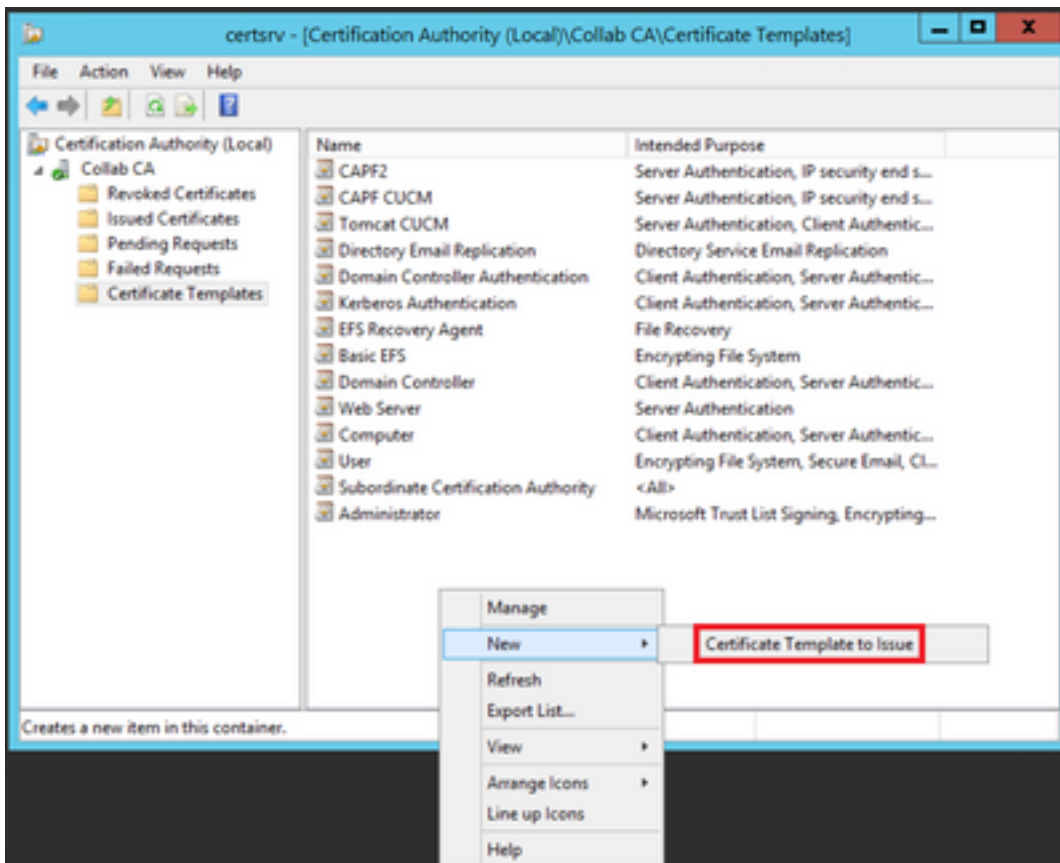
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und wählen Sie **OK** für dieses und das vorherige Fenster aus, wie im Bild gezeigt.



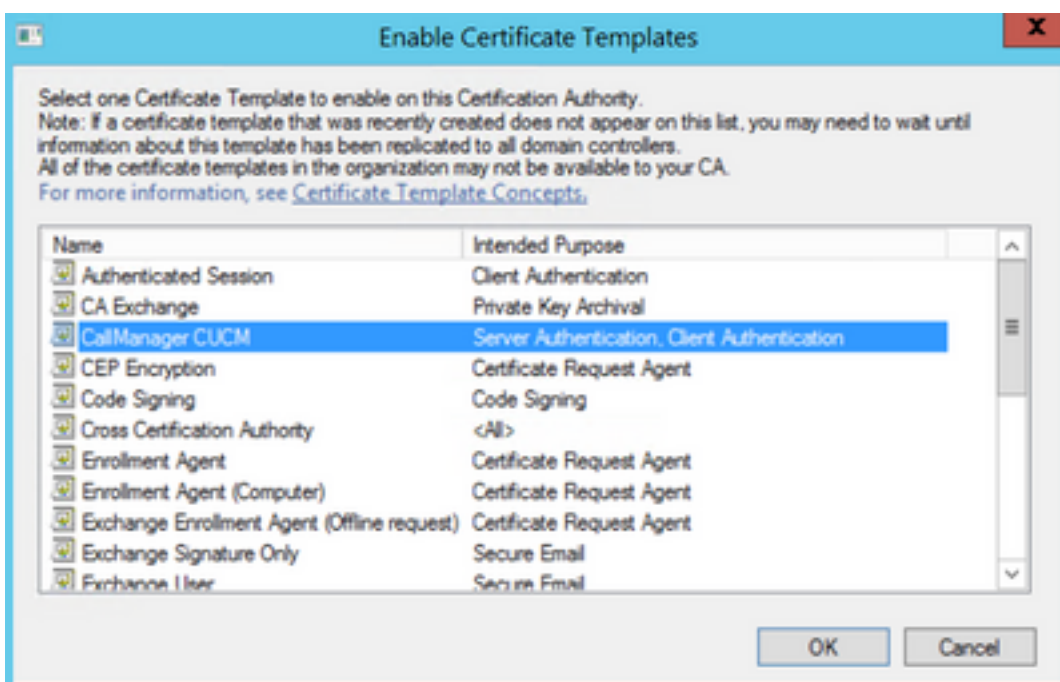
Schritt 7. Wählen Sie auf der Vorlage die Option **Übernehmen** und dann **OK** aus.



Schritt 8: Schließen Sie das Fenster **Zertifikatvorlagenkonsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.



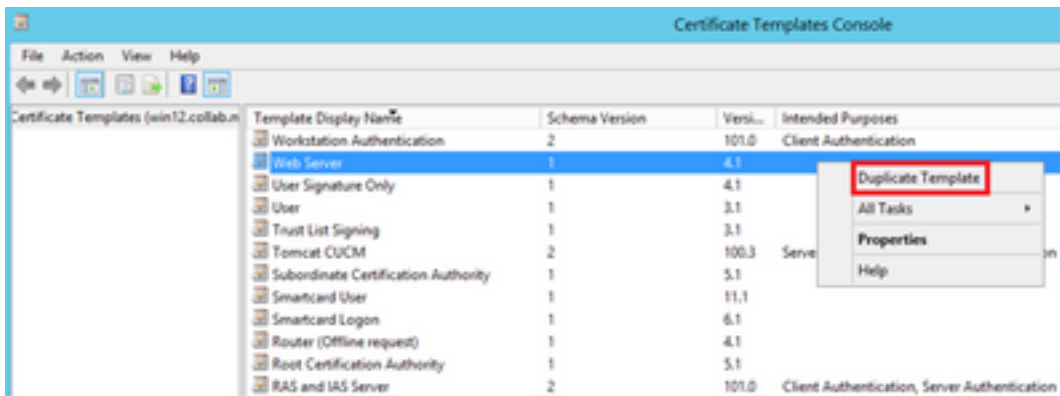
Schritt 9. Wählen Sie die neue **CallManager-CUCM**-Vorlage aus, und wählen Sie **OK** aus, wie im Bild gezeigt.



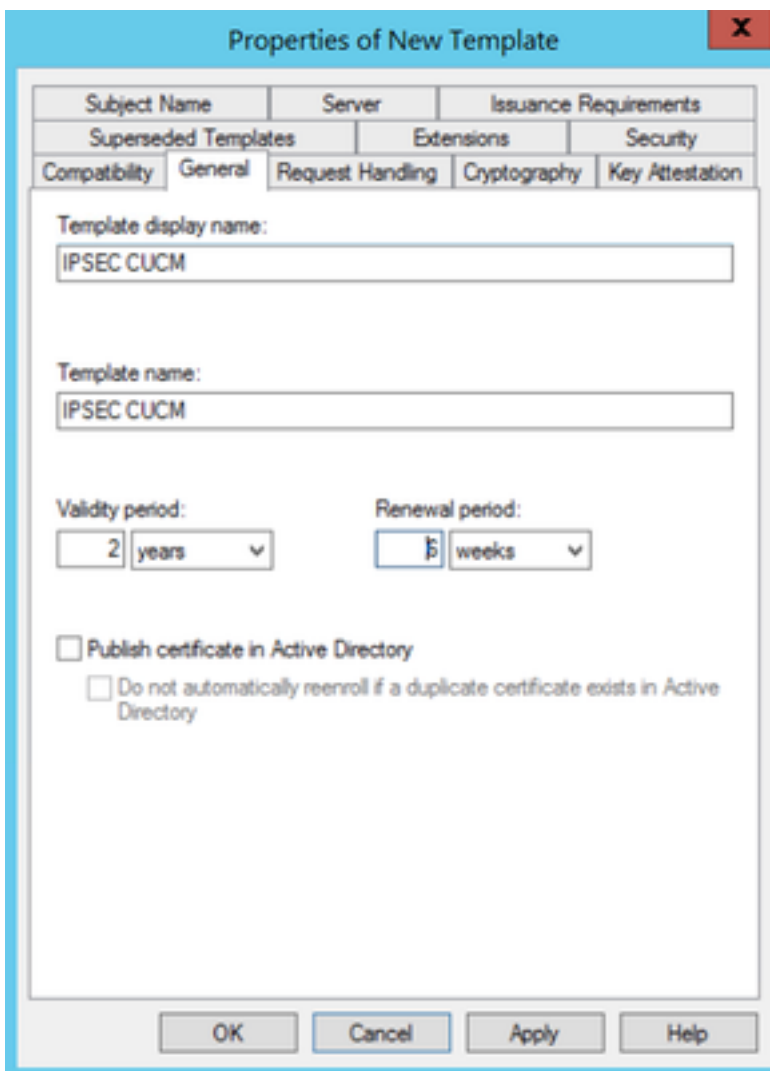
Schritt 10. Wiederholen Sie alle vorherigen Schritte, um nach Bedarf Zertifikatvorlagen für die Tomcat- und TVS-Dienste zu erstellen.

IPsec-Vorlage

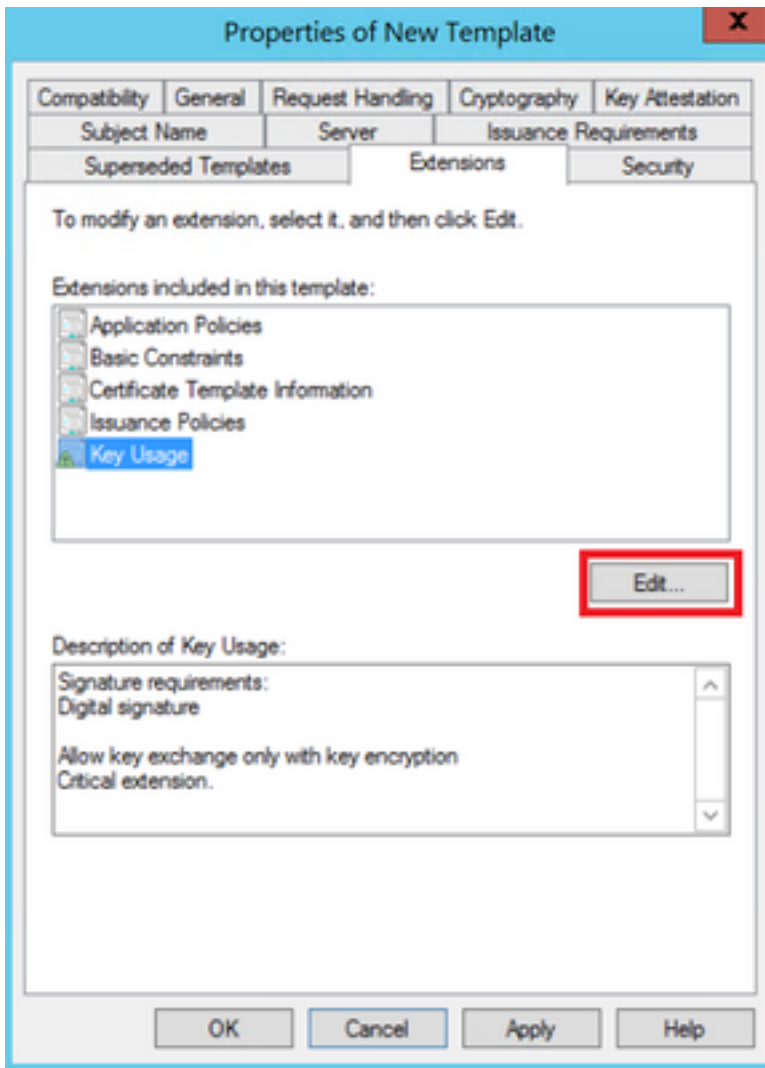
Schritt 1: Suchen Sie die **Webserver**-Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Vorlage duplizieren** aus, wie im Bild dargestellt.



Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

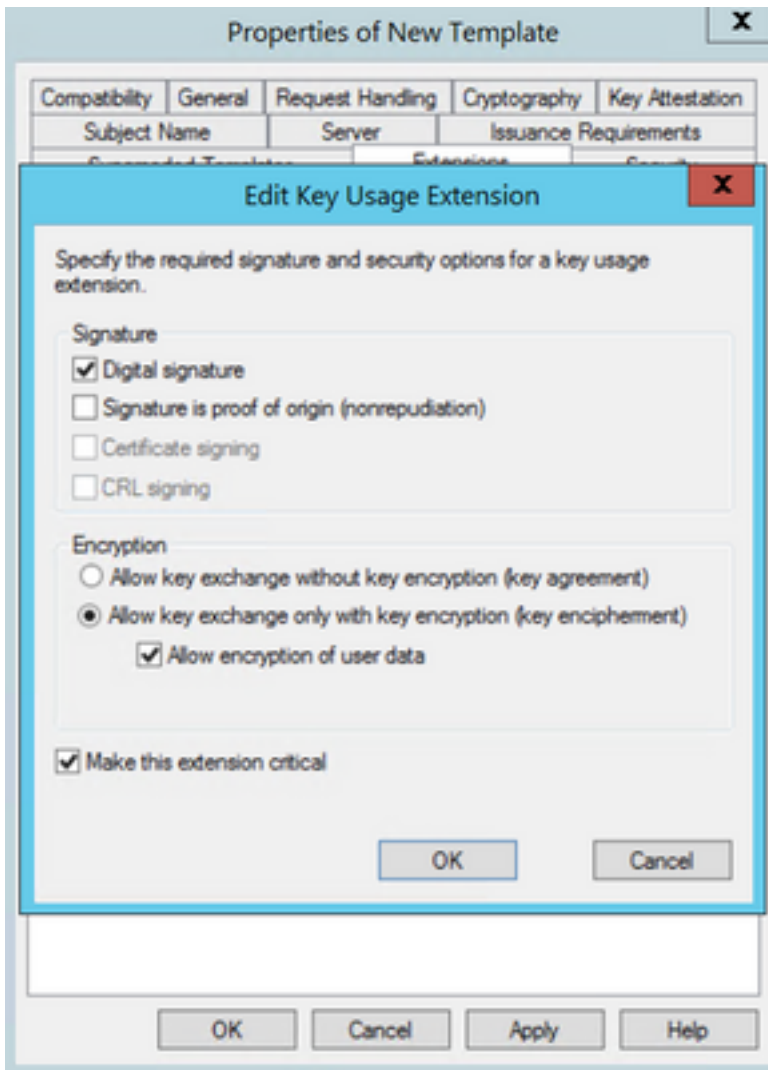


Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.



Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

- **Digitale Signatur**
- **Schlüsselaustausch nur mit Schlüsselverschlüsselung zulassen (Schlüsselverschlüsselung)**
- **Verschlüsselung von Benutzerdaten zulassen**



Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

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:

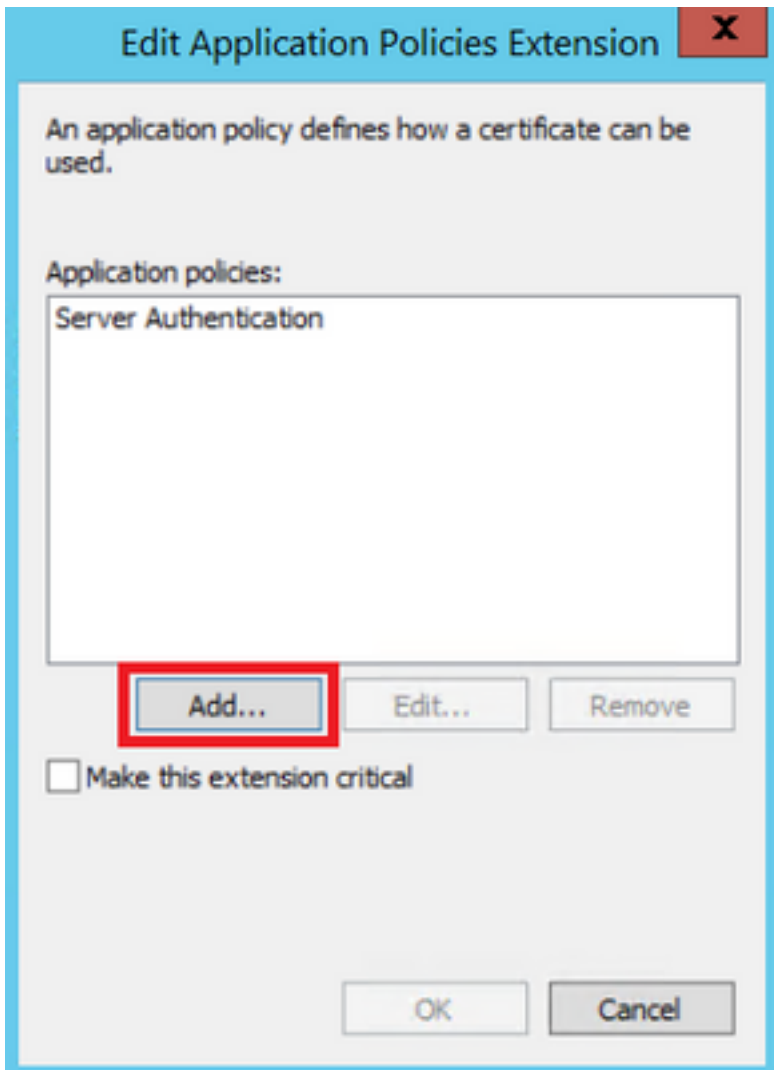
Server Authentication

OK

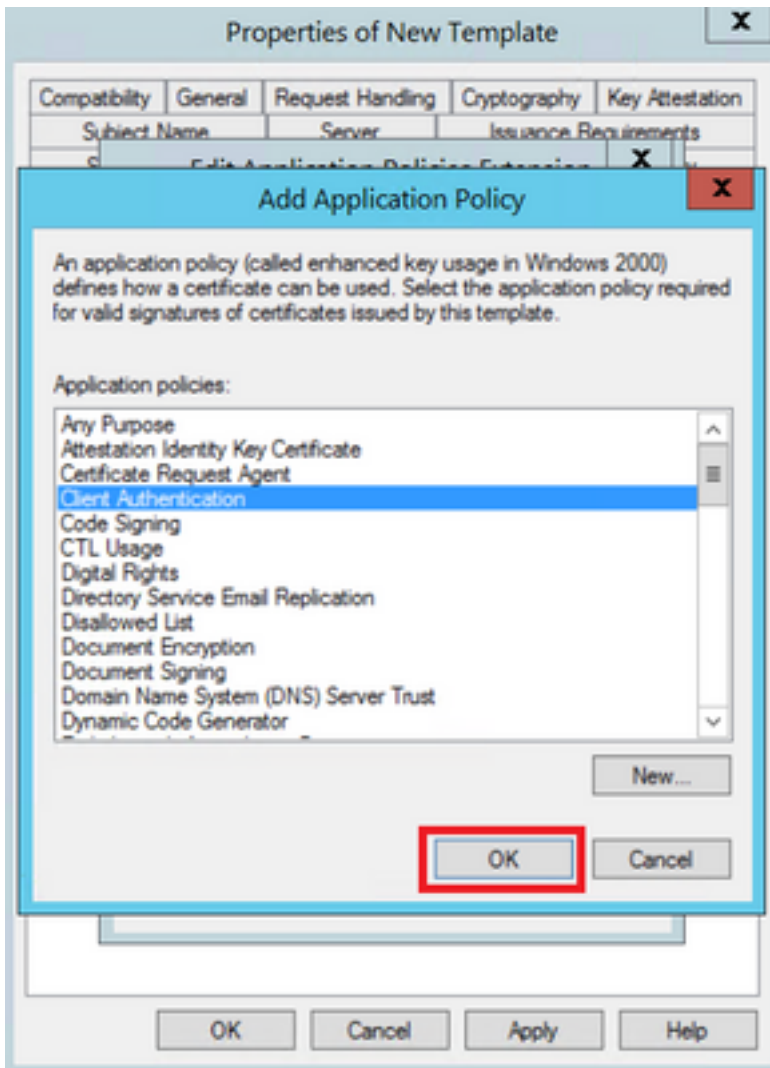
Cancel

Apply

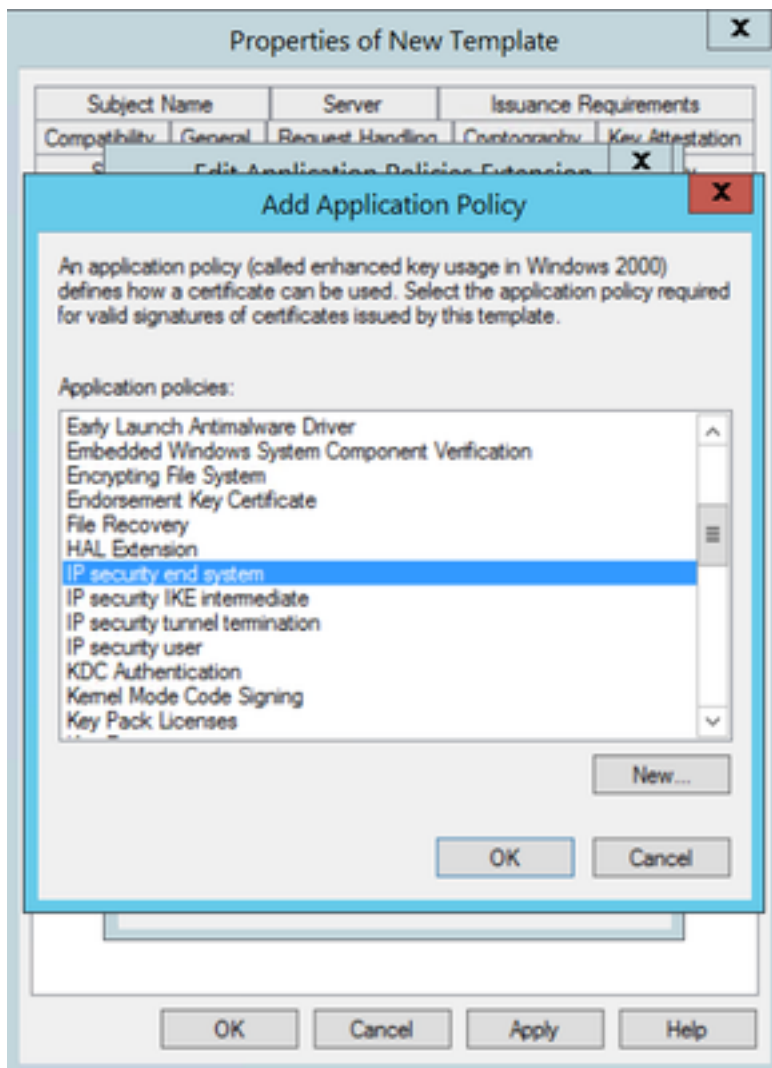
Help



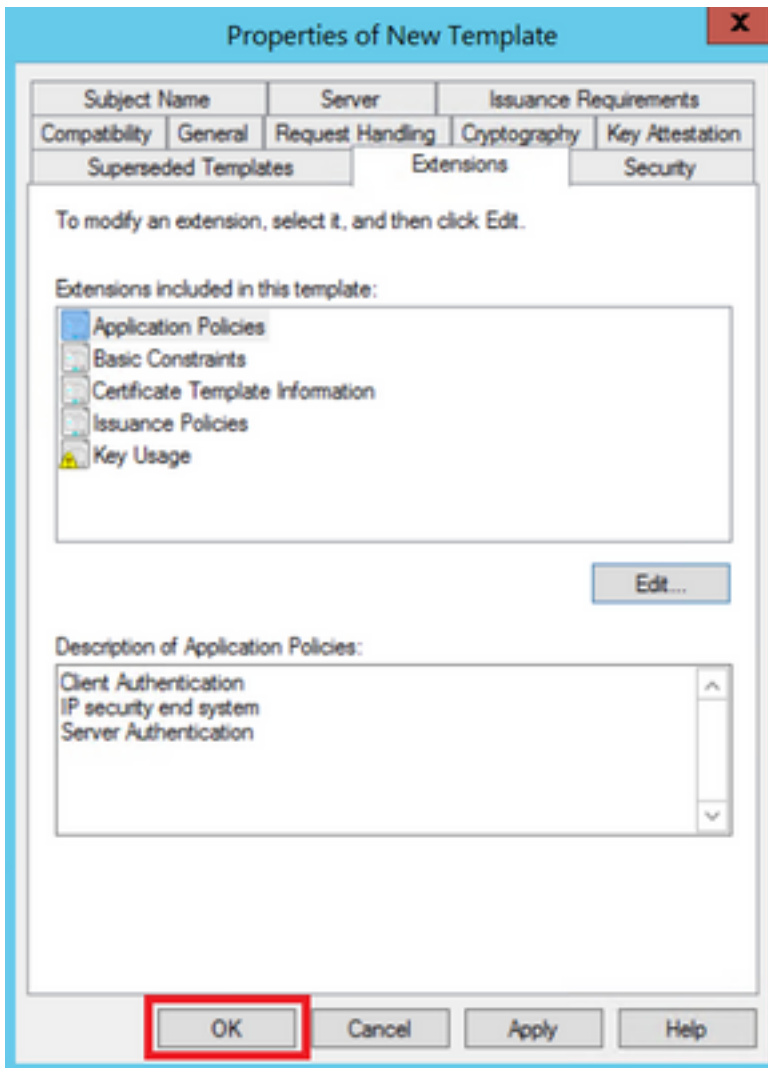
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und klicken Sie dann auf **OK**, wie im Bild gezeigt.



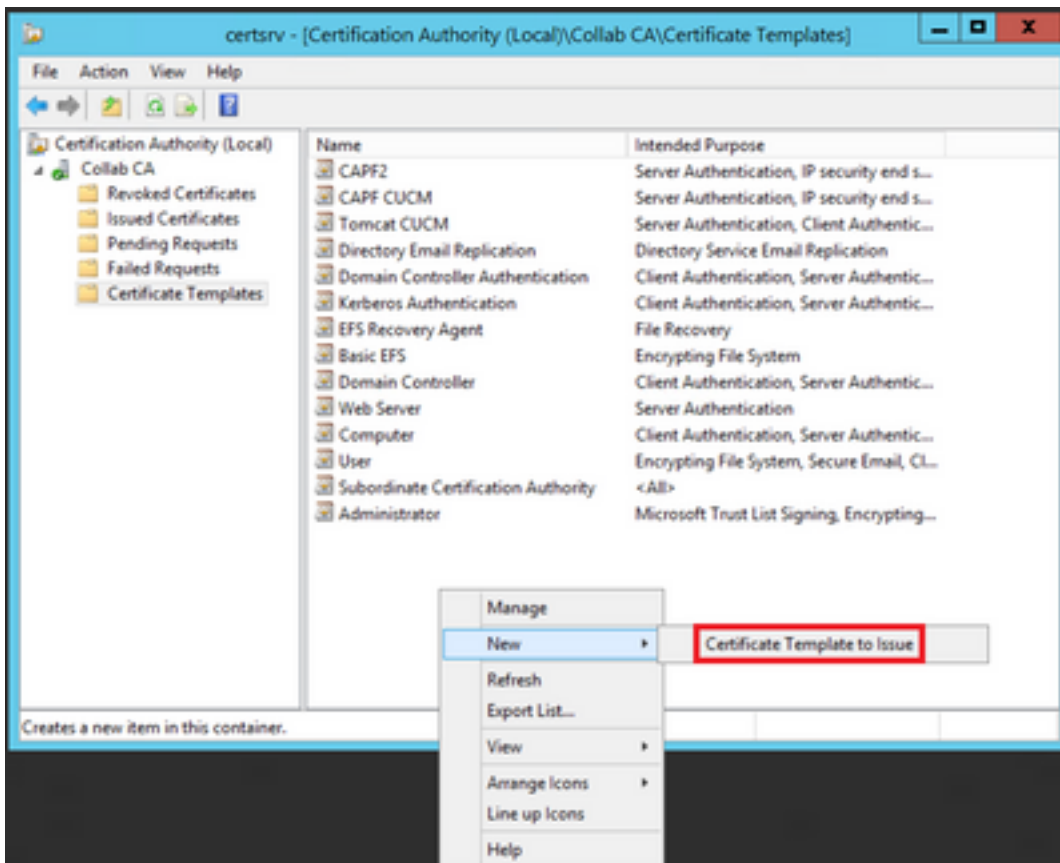
Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann in diesem und im vorherigen Fenster die Option **OK** aus.



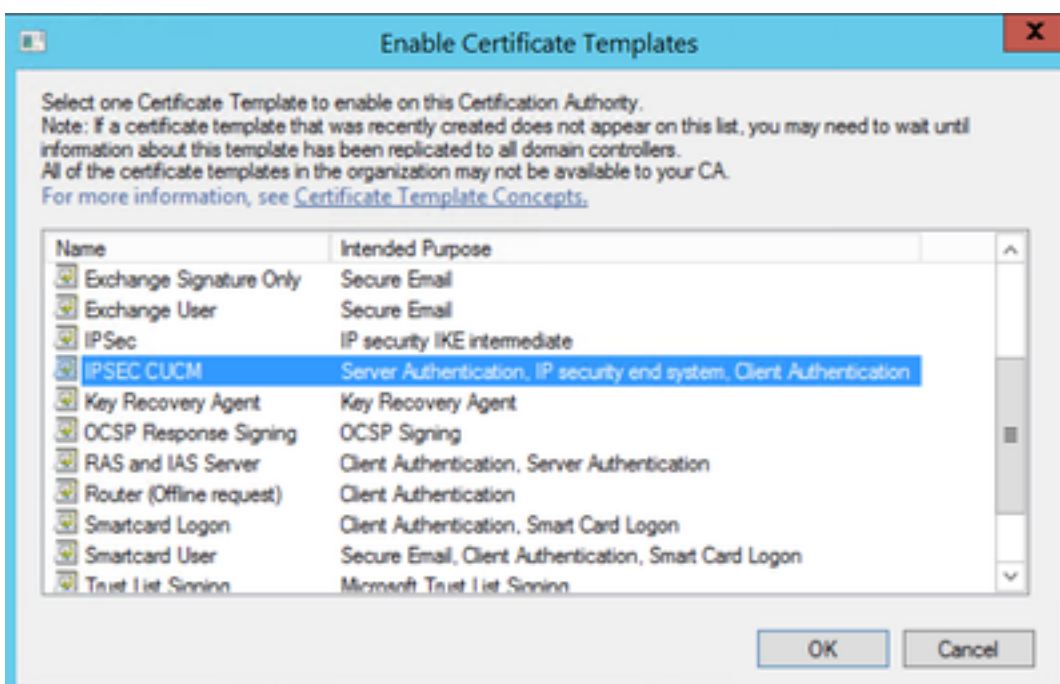
Schritt 8: Wählen Sie auf der Vorlage **Apply (Übernehmen)** und dann **OK**, wie im Bild dargestellt.



Schritt 9. Schließen Sie das Fenster **Zertifikatvorlagen-Konsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.

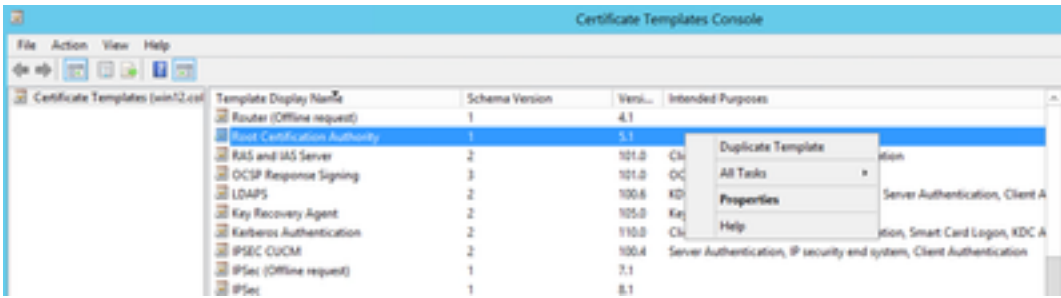


Schritt 10. Wählen Sie die neue IPSEC-CUCM-Vorlage aus, und wählen Sie auf OK aus, wie im Bild gezeigt.

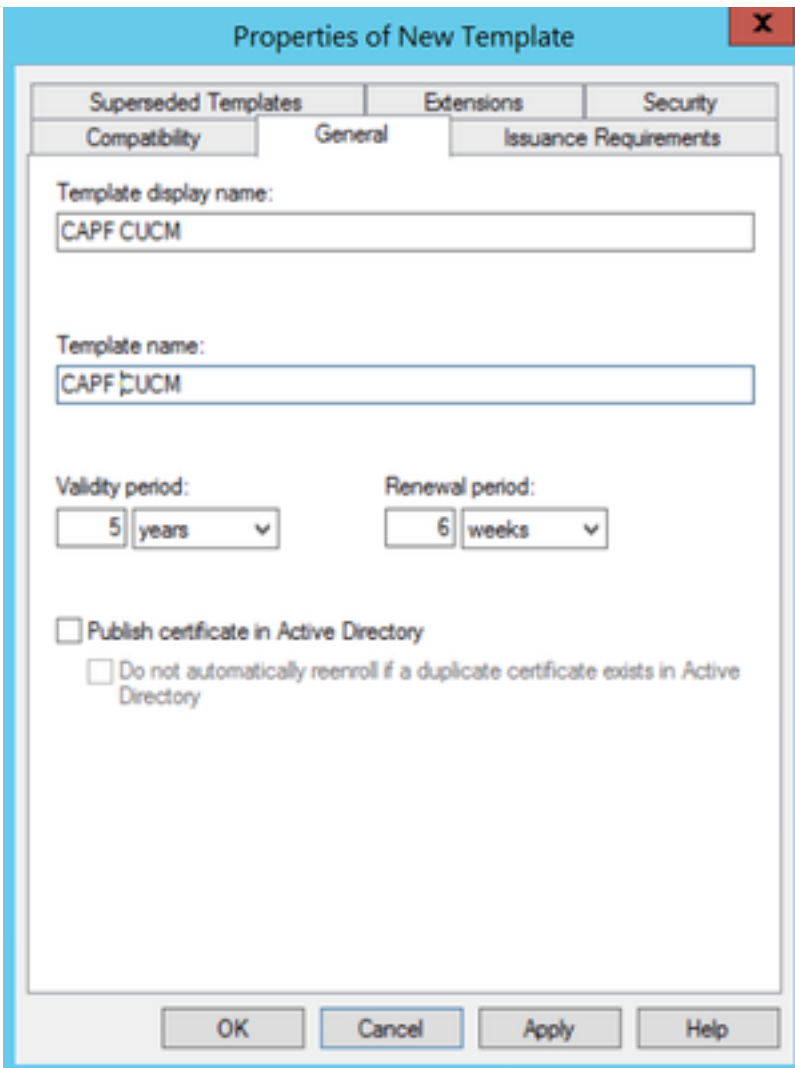


CAPF-Vorlage

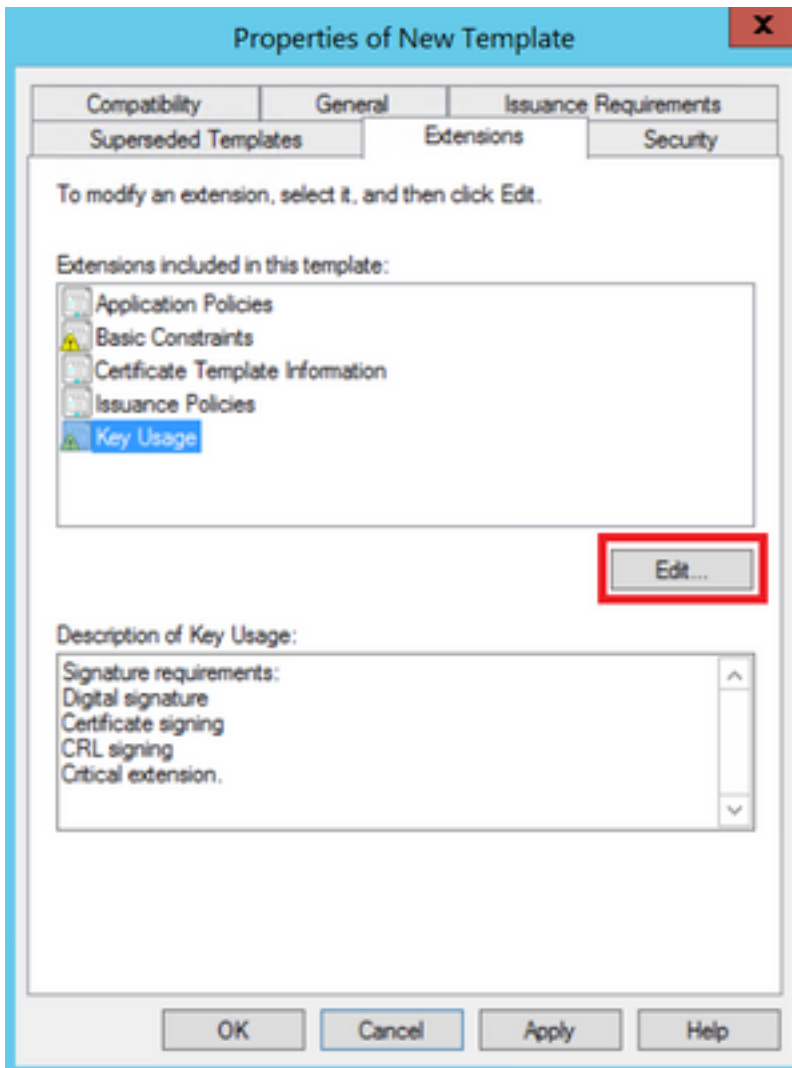
Schritt 1: Suchen Sie die Vorlage für die **Stammzertifizierungsstelle**, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie anschließend **Vorlage duplizieren**, wie im Bild dargestellt.



Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

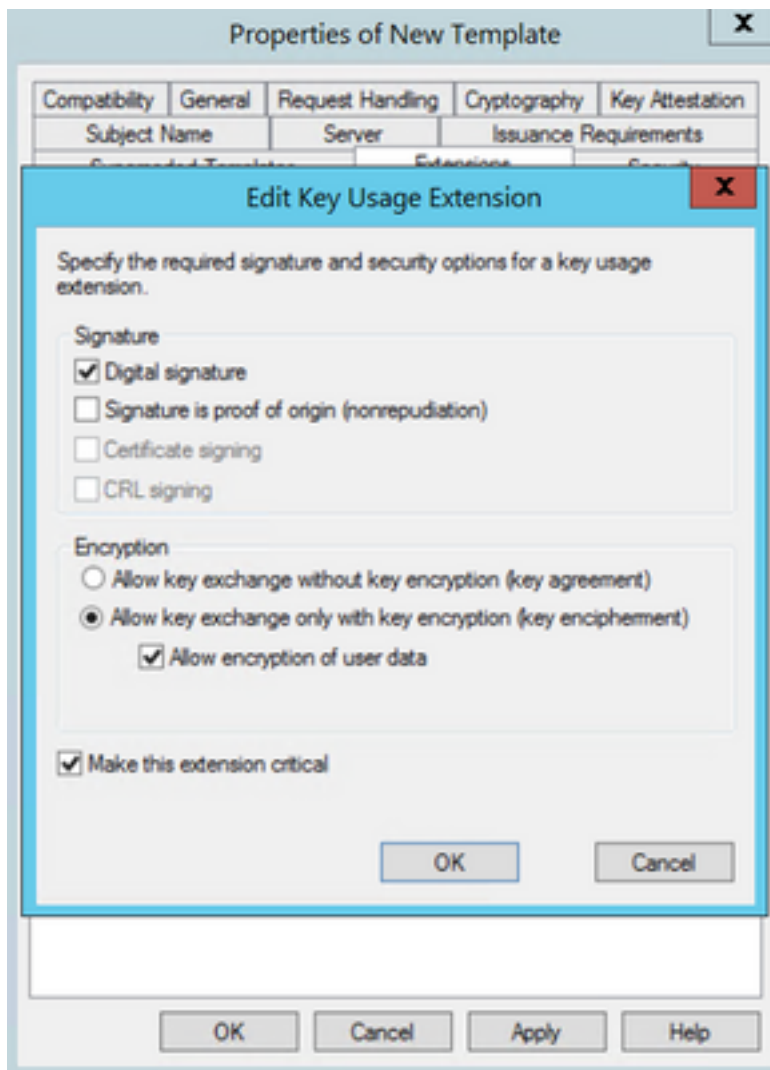


Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselerwendung > Bearbeiten**, wie im Bild dargestellt.



Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

- **Digitale Signatur**
- **Zertifikatssignatur**
- **CRL-Signierung**



Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

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:

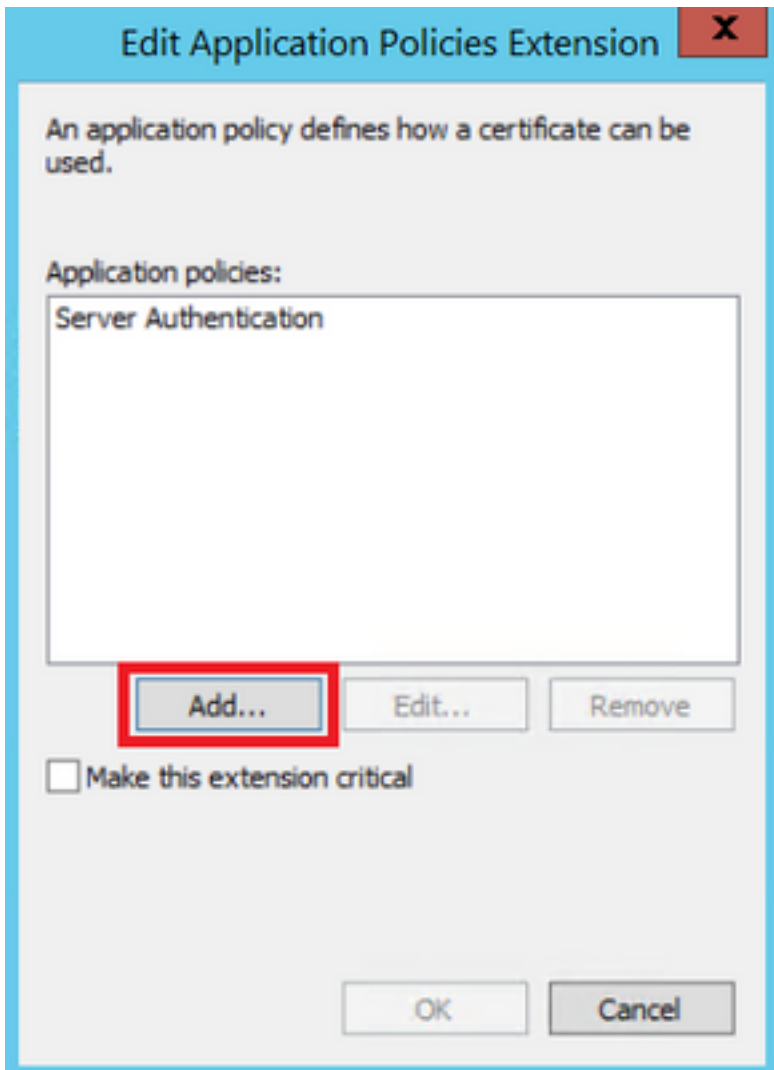
Server Authentication

OK

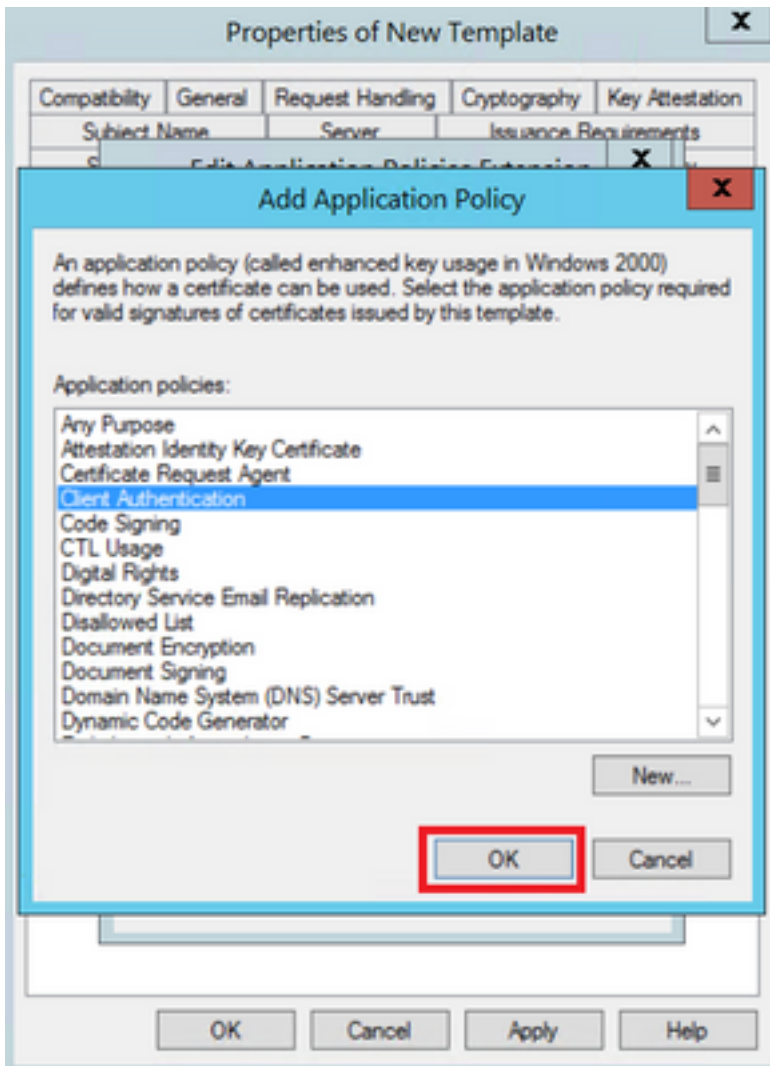
Cancel

Apply

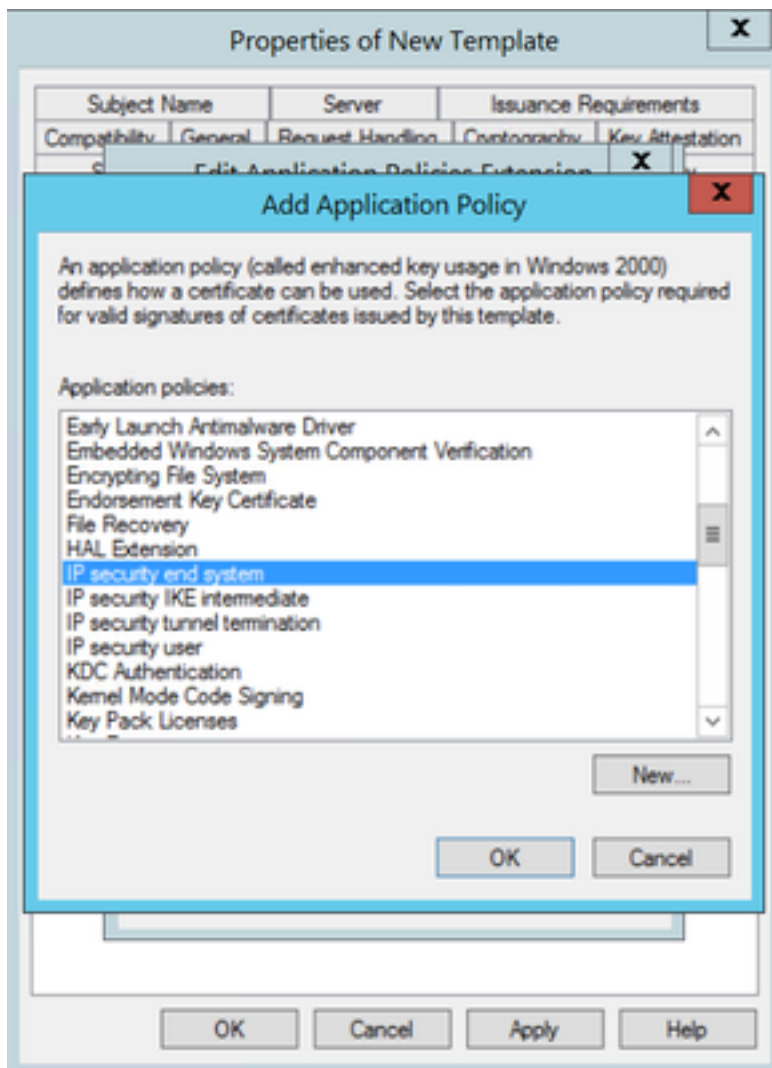
Help



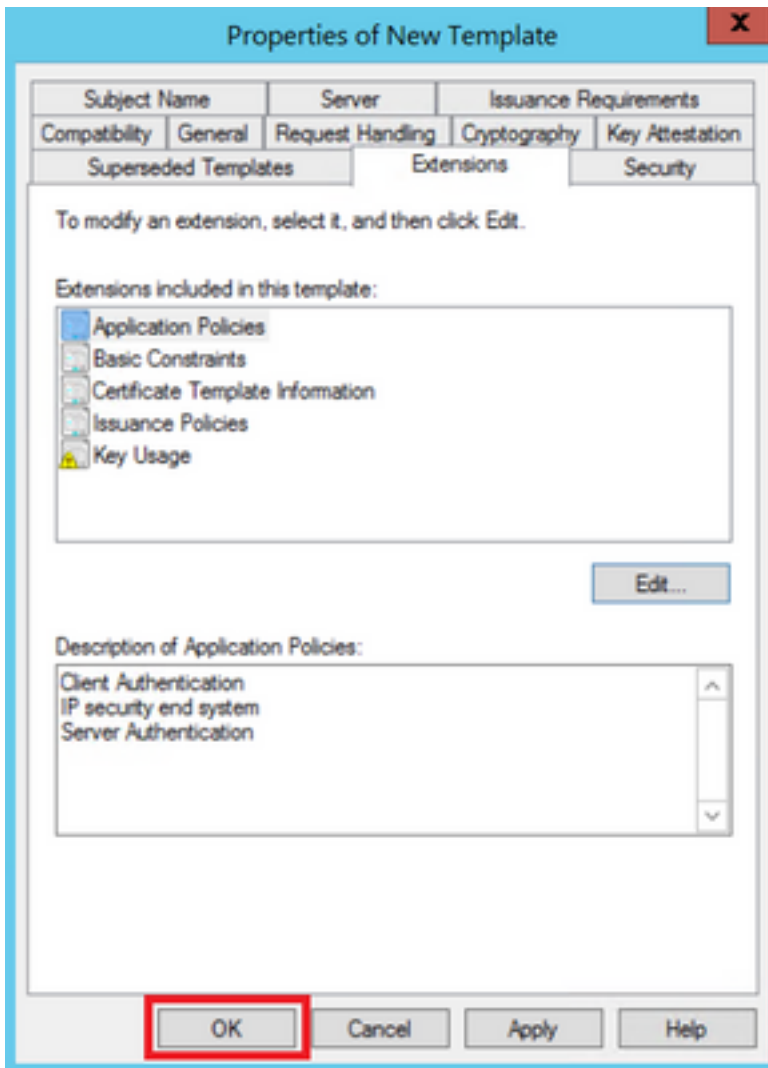
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und wählen Sie dann **OK** aus, wie im Bild gezeigt.



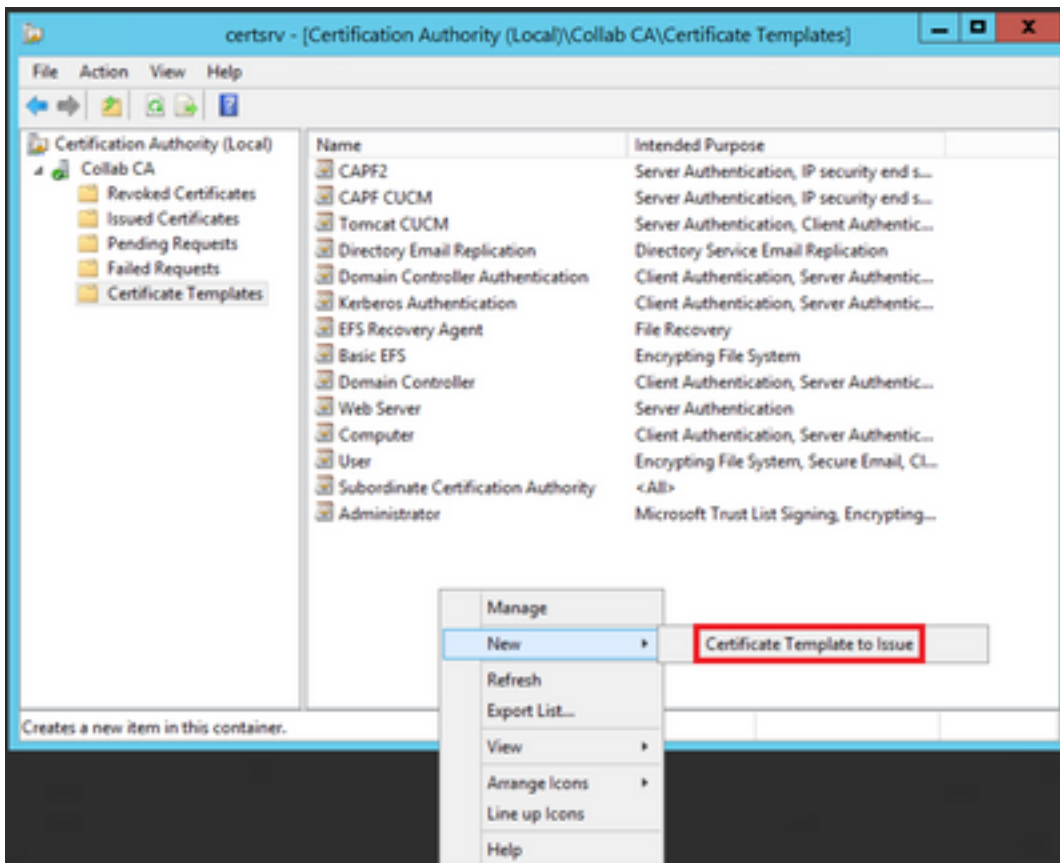
Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann OK für dieses und das vorherige Fenster aus, wie im Bild gezeigt.



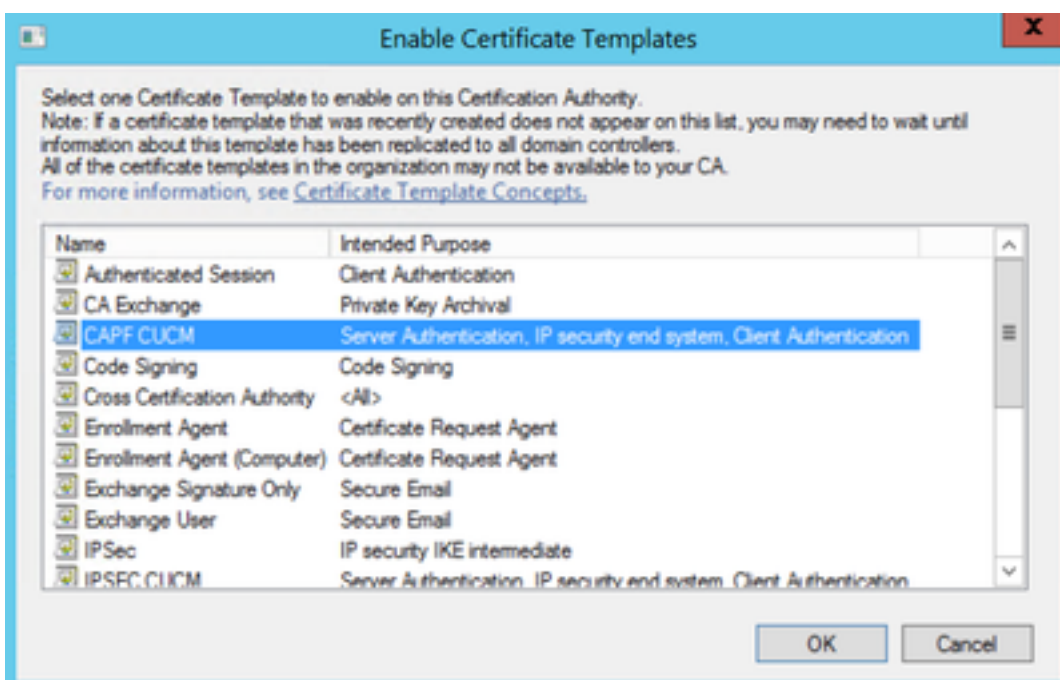
Schritt 8: Wählen Sie auf der Vorlage **Apply (Übernehmen)** und dann **OK**, wie im Bild dargestellt.



Schritt 9. Schließen Sie das Fenster **Zertifikatvorlagen-Konsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.



Schritt 10. Wählen Sie die neue **CAPF CUCM**-Vorlage aus, und wählen Sie **OK**, wie im Bild dargestellt.



Generieren einer Zertifikatsignierungsanforderung

Verwenden Sie dieses Beispiel, um unter Verwendung der neu erstellten Vorlagen ein CallManager-Zertifikat zu generieren. Das gleiche Verfahren kann für jeden Zertifikatstyp verwendet werden. Sie müssen nur das Zertifikat und die Vorlagentypen entsprechend auswählen:

Schritt 1: Navigieren Sie auf CUCM zu **OS Administration > Security > Certificate Management >**

Generate CSR (Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung > CSR erstellen).

Schritt 2: Wählen Sie diese Optionen aus, und wählen Sie **Generate (Erstellen)** aus, wie im Bild dargestellt.

- Zertifikatzweck: **CallManager**
- Distribution: **<Dies kann entweder nur für einen Server oder mehrere SANs sein>**

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

Schritt 3: Es wird eine Bestätigungsmeldung generiert, wie im Bild dargestellt.

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].

Schritt 4: Suchen Sie in der Zertifikatliste nach dem Eintrag mit dem Typ **CSR Only**, und wählen Sie ihn aus, wie im Bild dargestellt.

Certificate List

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

Status

36 records found

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

Find Certificate List where Certificate begins with Find Clear Filter

Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
auth	AUTHZ_admin	Self-signed	RSA	115PUB.maucabal.lab	AUTHZ_admin	01/27/2018	Self-signed certificate generated by system
CallManager	115PUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(SAN)	--	--	
CallManager	115SUB.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

Schritt 5: Wählen Sie im Popup-Fenster die Option **CSR herunterladen**, und speichern Sie die Datei auf Ihrem Computer.

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

Delete Download CSR

Status
Status: Ready

Certificate Settings

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

Certificate File Data

```
PKCS10 Request: [  
Version: 0  
Subject: CN=115PUB-ms.maucabal.lab, OU=clisco, O=clisco, L=clisco, ST=clisco, C=MX  
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)  
Key value:  
3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d  
cab144fd5f1538efe514fd8207d3dde43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34  
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2  
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b  
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c  
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164  
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c  
6b25a37e84cd0203010001  
Attributes: [  
Requested Extensions [  
]
```

Delete Download CSR

Schritt 6: Navigieren Sie in Ihrem Browser zu dieser URL, und geben Sie die Administratoranmeldeinformationen für den Domänencontroller ein:
<https://<IhrWindowsServerIP>/certsrv/>.

Schritt 7. Navigieren Sie zu **Request a certificate > advanced certificate request** (Zertifikat anfordern > Erweiterte Zertifikatanforderung), wie im Bild dargestellt.

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

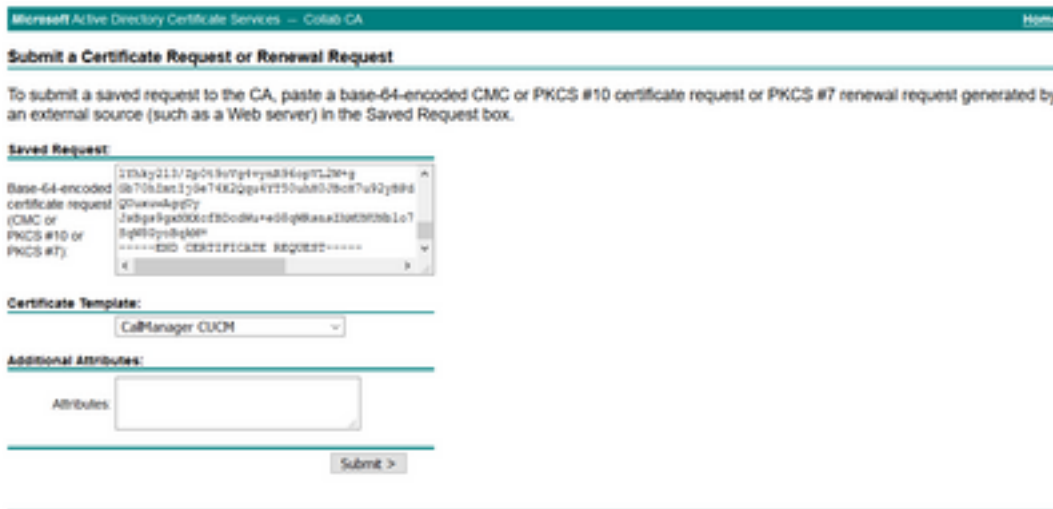
Select the certificate type:
[User Certificate](#)

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

Schritt 8: Öffnen Sie die CSR-Datei, und kopieren Sie den gesamten Inhalt:



Schritt 9. Fügen Sie den CSR in das **Base-64-kodierte Zertifikatsanforderungsfeld** ein. Wählen Sie unter **Zertifikatvorlage** die richtige Vorlage aus, und wählen Sie **Senden** aus, wie im Bild dargestellt.



Schritt 10. Wählen Sie **Base 64-codiert** und **Download certificate chain**, die generierte Datei kann jetzt in den CUCM hochgeladen werden.



Überprüfung

Das Prüfverfahren ist Teil des Konfigurationsprozesses.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.