Erstellen von Windows CA-Zertifikatvorlagen für CUCM

Inhalt

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.	· Cisco Call Manager · Cisco CTI Manager ·Cisco TFTP
tomcat	Präsentiert für HTTPS-Interaktionen (Secure Hypertext Transfer Protocol).	·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.	Cisco DRF Master · Cisco DRF Lokal
CAPF	Wird zum Generieren von LSC-Zertifikaten (Locally Significant Certificates) für Telefone verwendet.	· 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.	· 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:

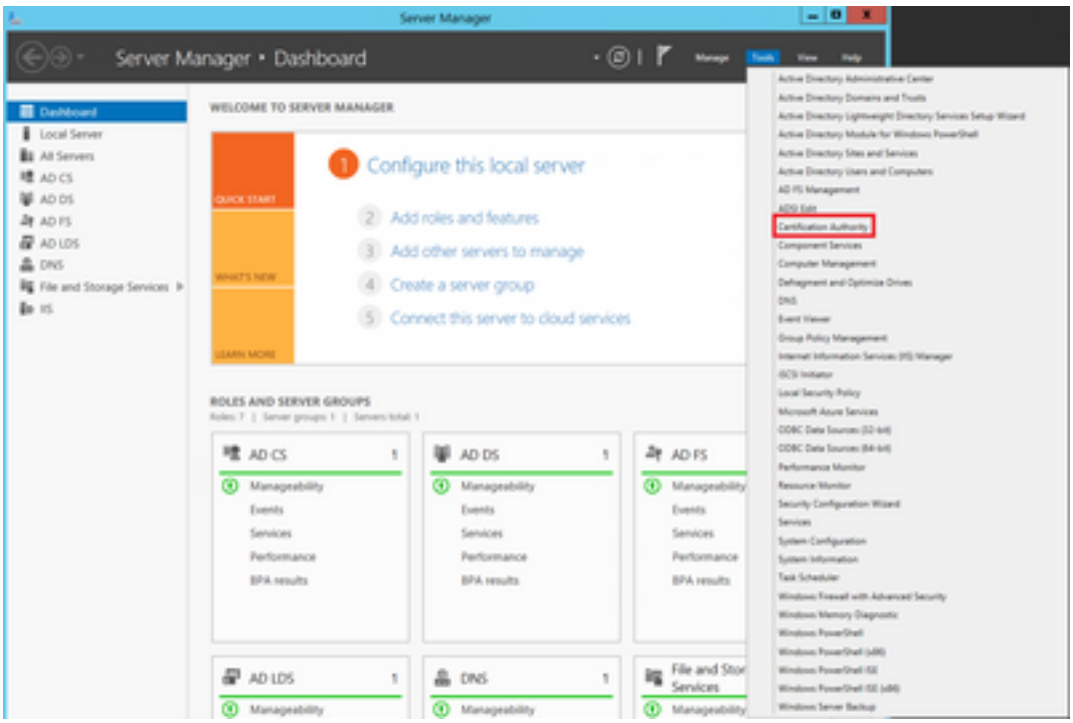
Zertifikat	X.509-Schlüsselverwendung	X.509 Extended Key-Verwendung
CallManager	· Digitale Signatur · Schlüsselverschlüsselung · Datenverschlüsselung	· Webserver-Authentifizierung · Webclient-Authentifizierung
tomcat	· Digitale Signatur · Schlüsselverschlüsselung · Datenverschlüsselun	· Webserver-Authentifizierung · Webclient-Authentifizierung

	g	
IPsec	· Digitale Signatur · Schlüsselverschlüsselung · Datenverschlüsselung	· Webserver-Authentifizierung · Webclient-Authentifizierung · IPsec-Endsystem
CAPF	· Digitale Signatur · Zertifikatzeichen · Schlüsselverschlüsselung	· Webserver-Authentifizierung · Webclient-Authentifizierung
TVS	· Digitale Signatur · Schlüsselverschlüsselung · Datenverschlüsselung	· Webserver-Authentifizierung · Webclient-Authentifizierung

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

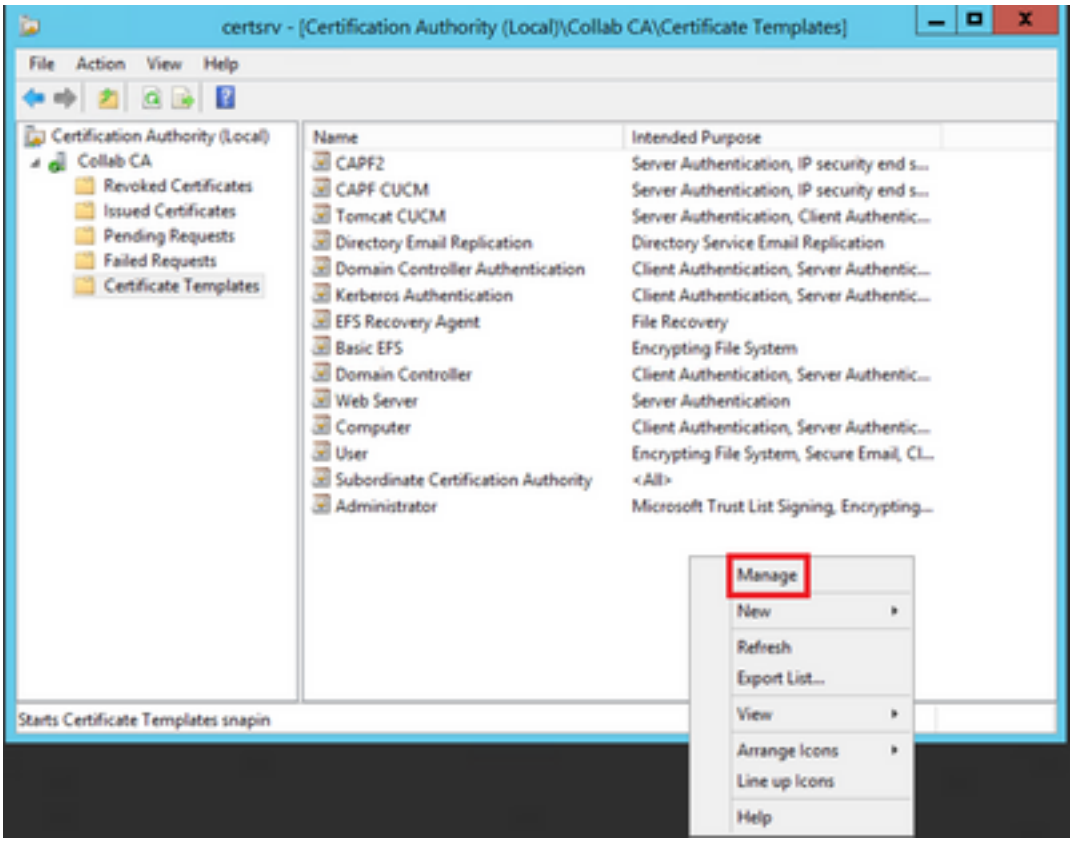
Konfigurieren

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

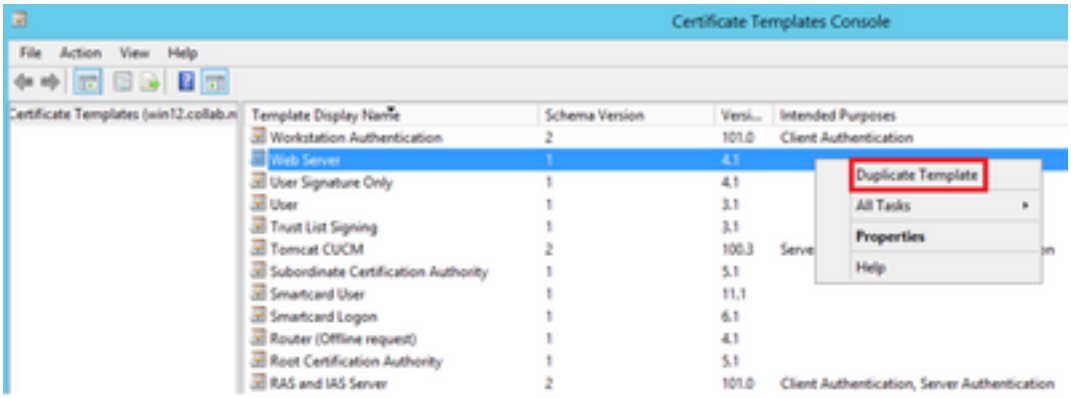
Sie mit der rechten Maustaste auf die Liste, und wählen Sie **Verwalten**, wie im Bild dargestellt.



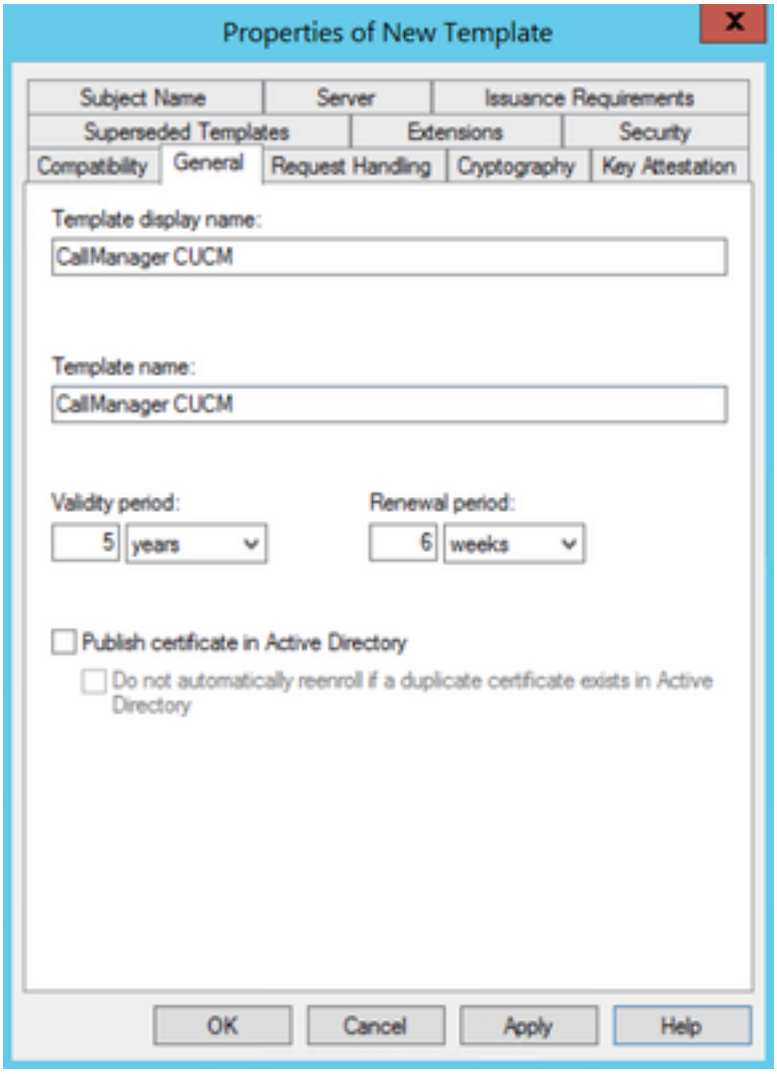
CallManager/Tomcat/TVS-Vorlage

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.

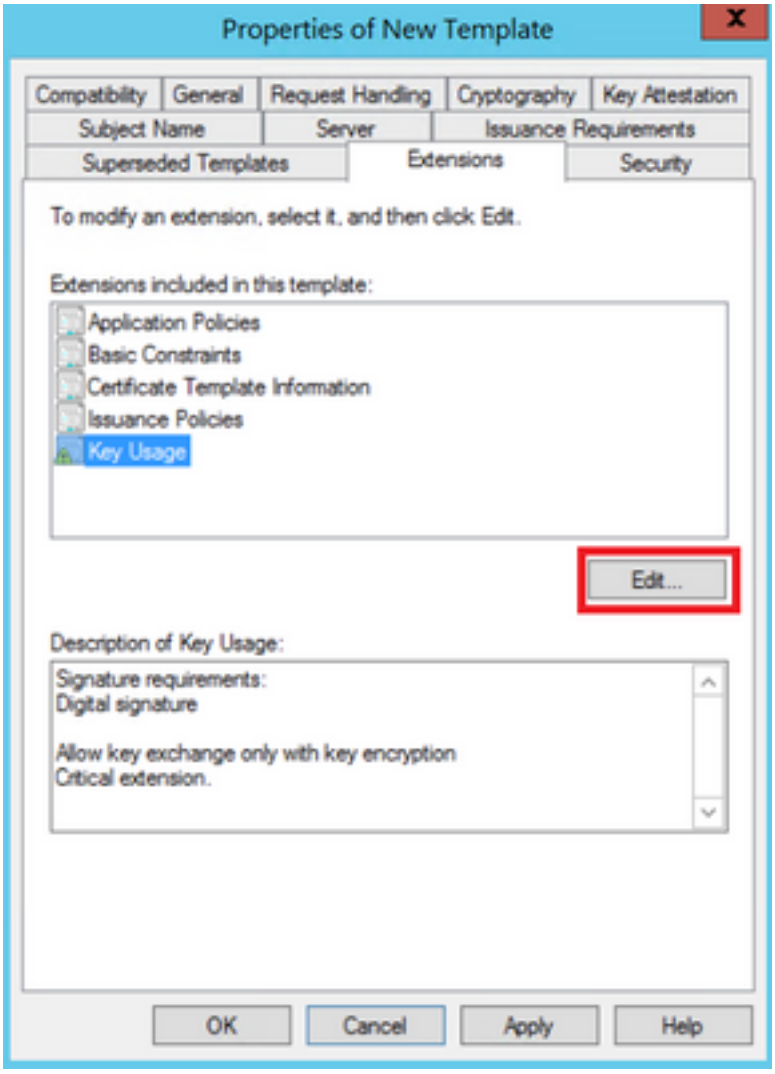
Schritt 1: Suchen Sie die **Webserver-**Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Vorlage duplizieren** aus, wie im Bild dargestellt.



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

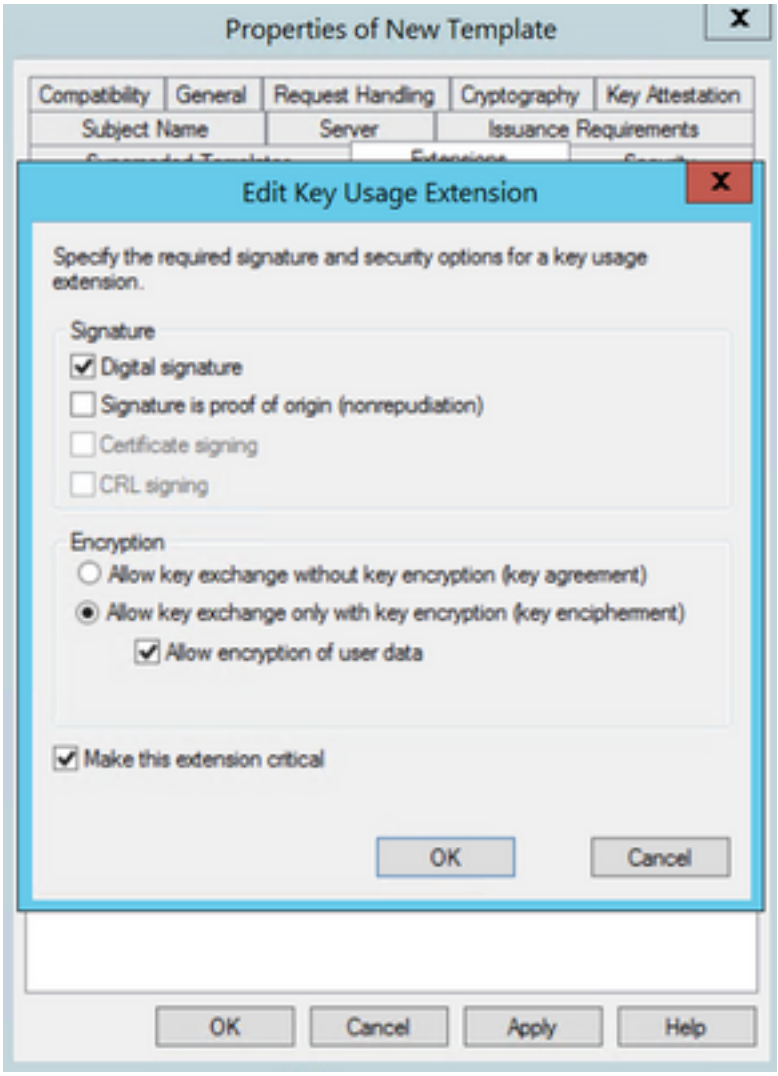


Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.

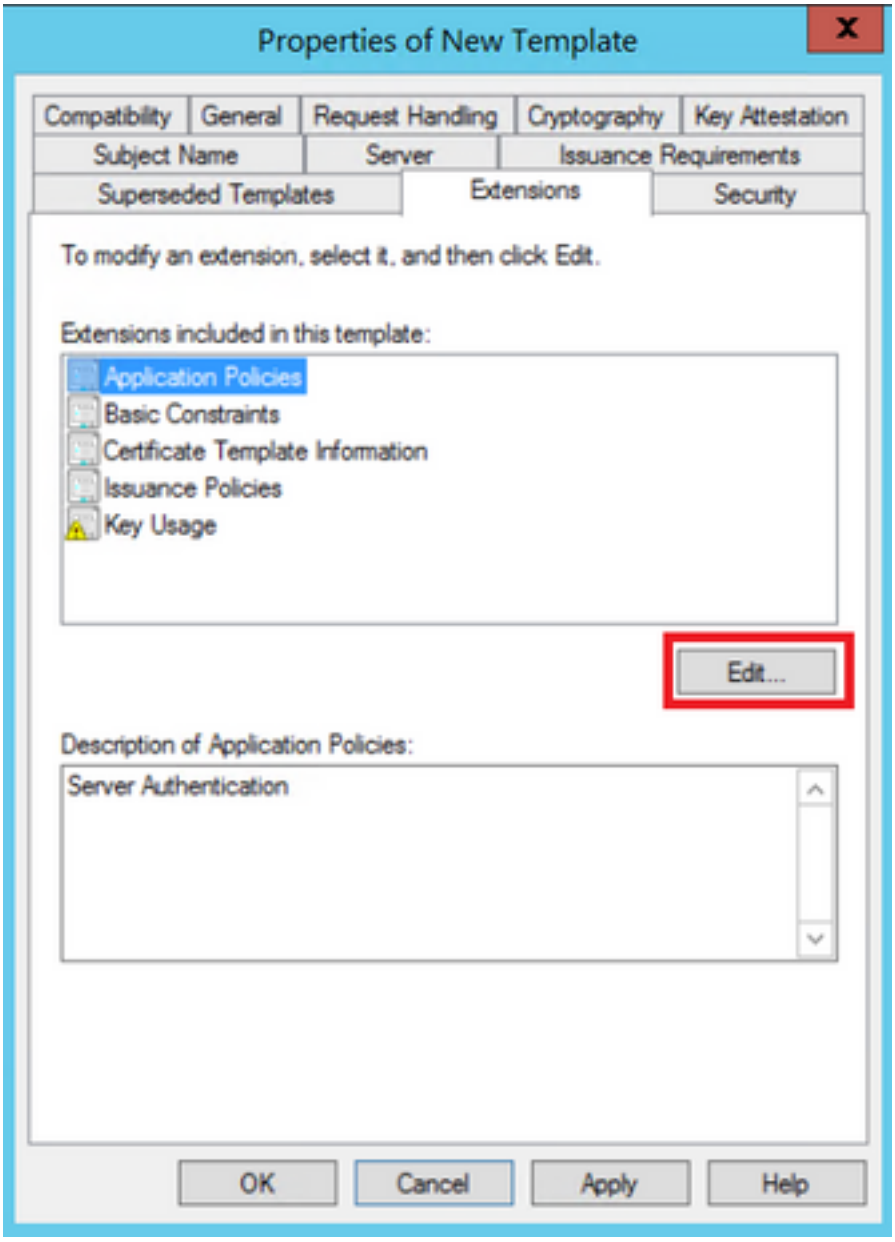


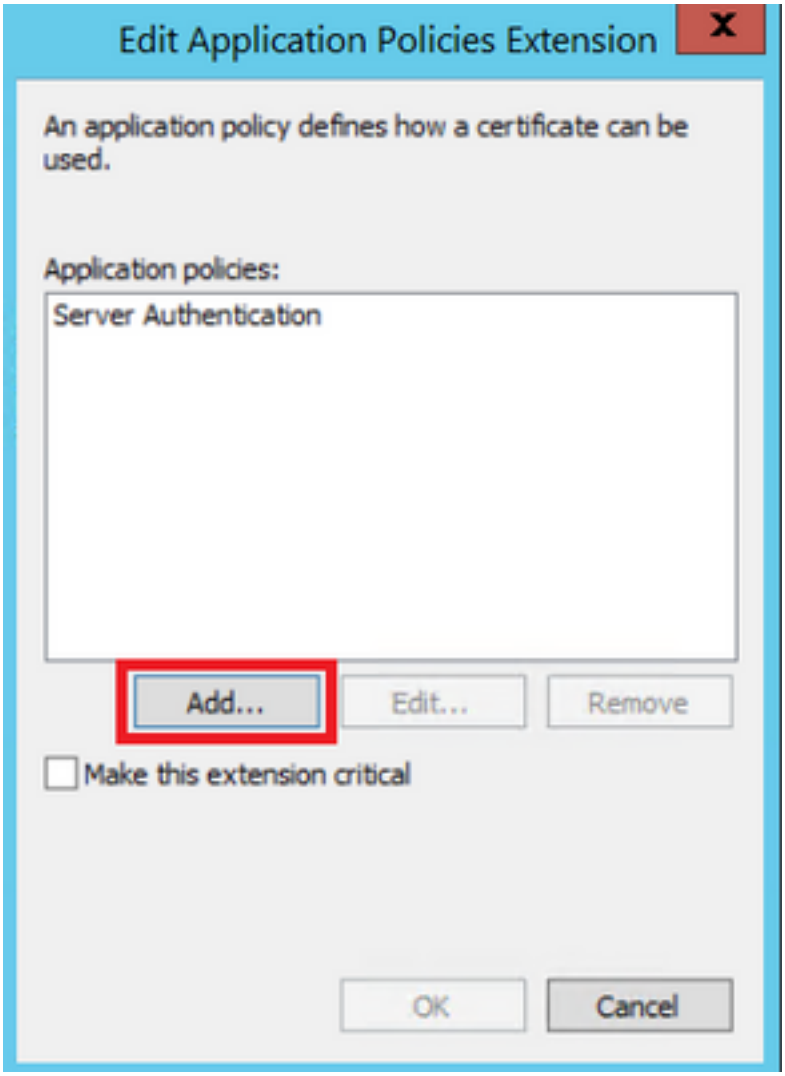
Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

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

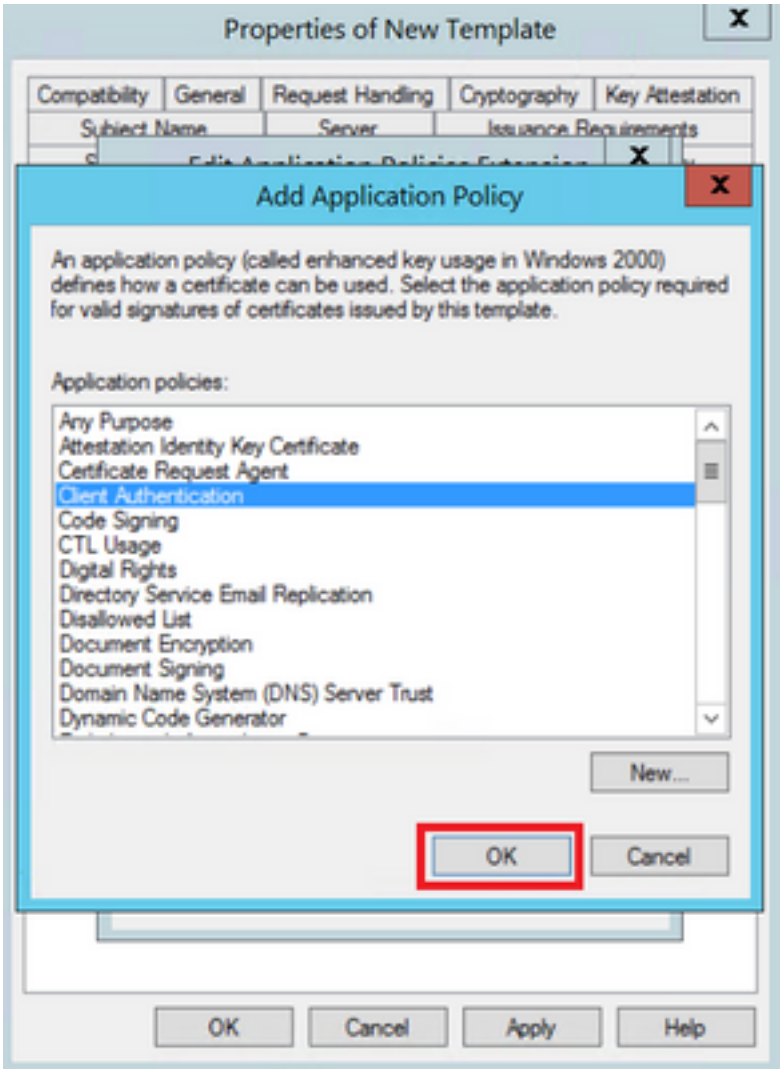


Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

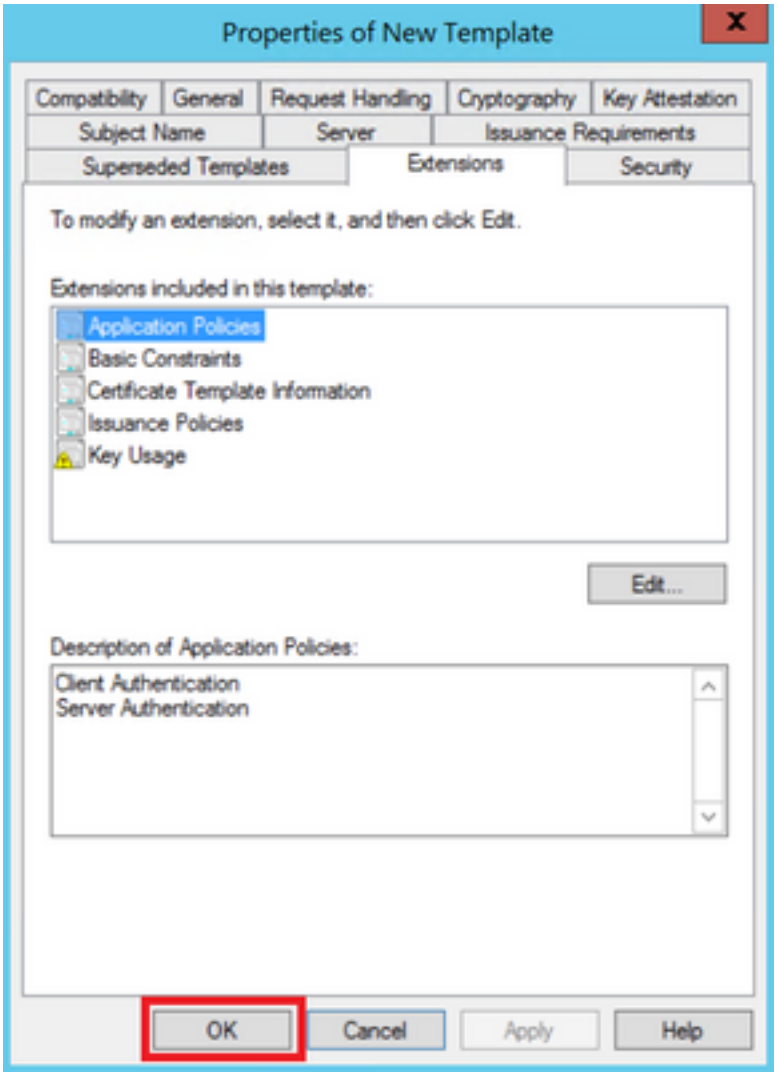

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



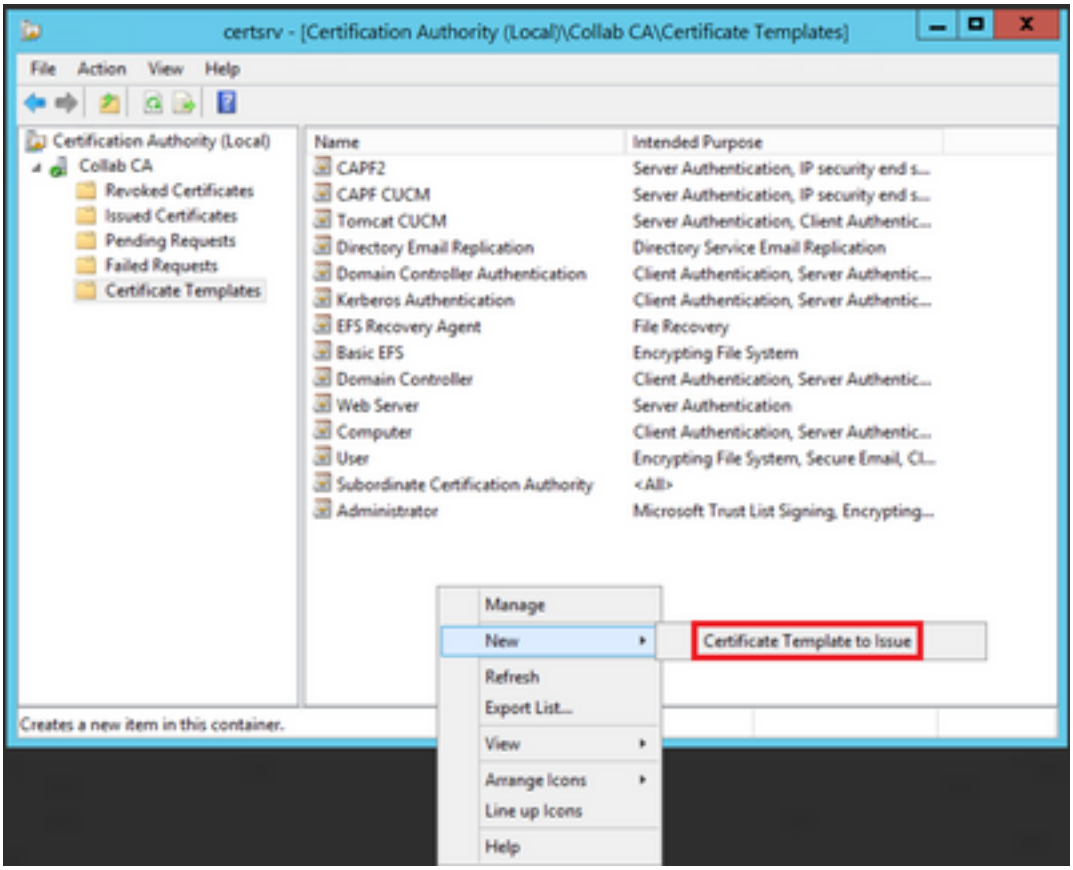
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und wählen Sie **OK** für dieses und das vorherige Fenster aus, wie im Bild gezeigt.



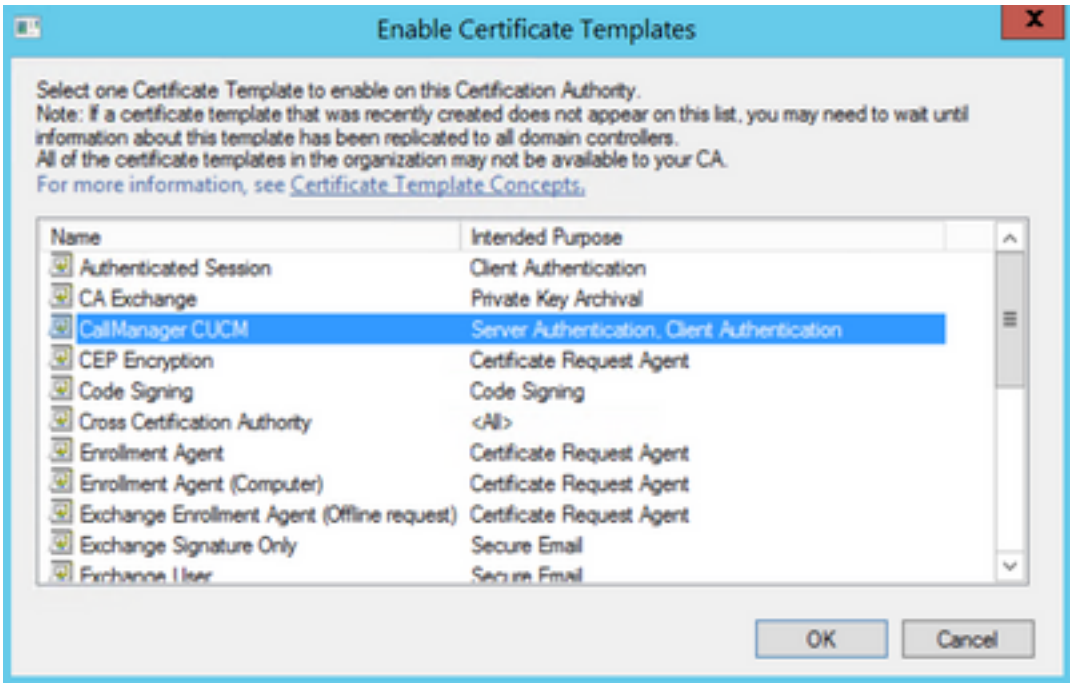
Schritt 7. Wählen Sie auf der Vorlage die Option **Übernehmen** und dann **OK aus.**



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



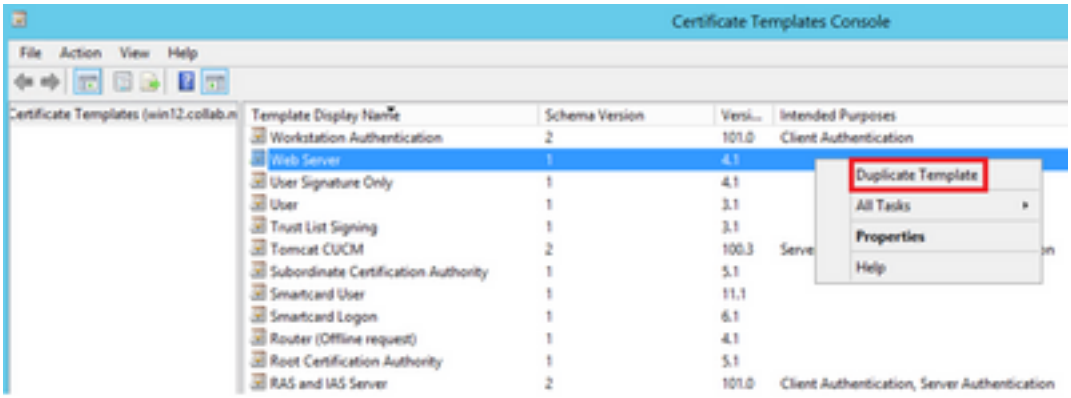
Schritt 9. Wählen Sie die neue **CallManager-CUCM-**Vorlage aus, und wählen Sie **OK** aus, wie im Bild gezeigt.



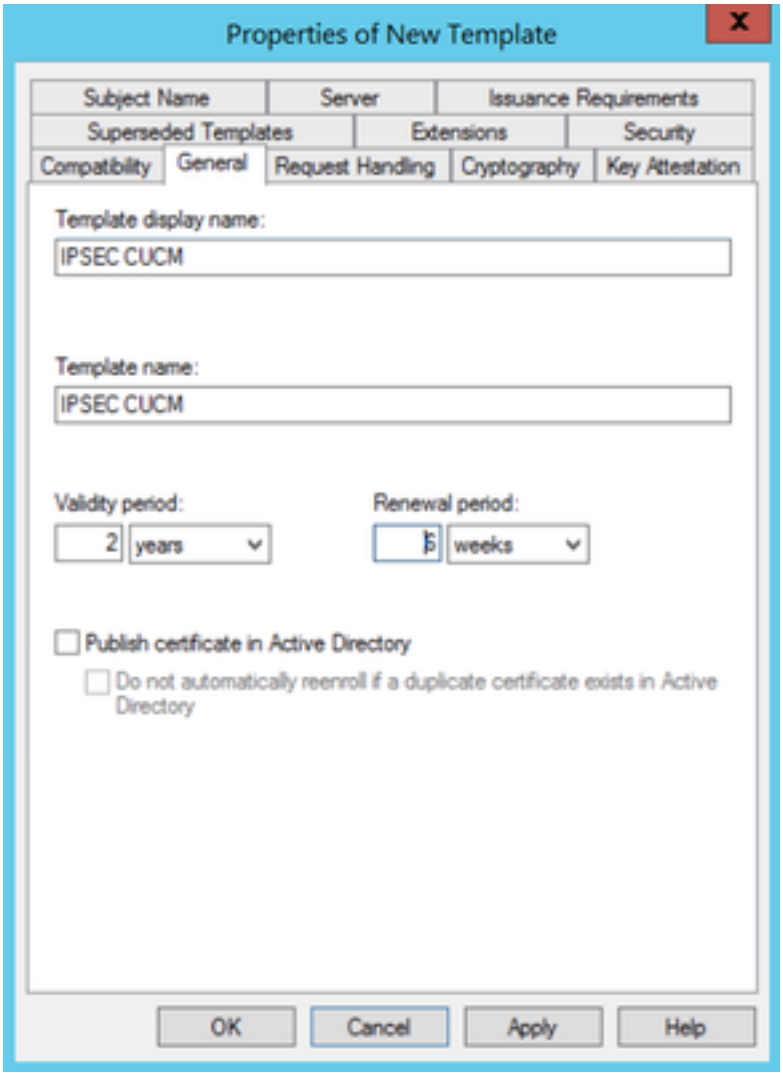
Schritt 10. Wiederholen Sie alle vorherigen Schritte, um nach Bedarf Zertifikatvorlagen für die Tomcat- und TVS-Dienste zu erstellen.

IPsec-Vorlage

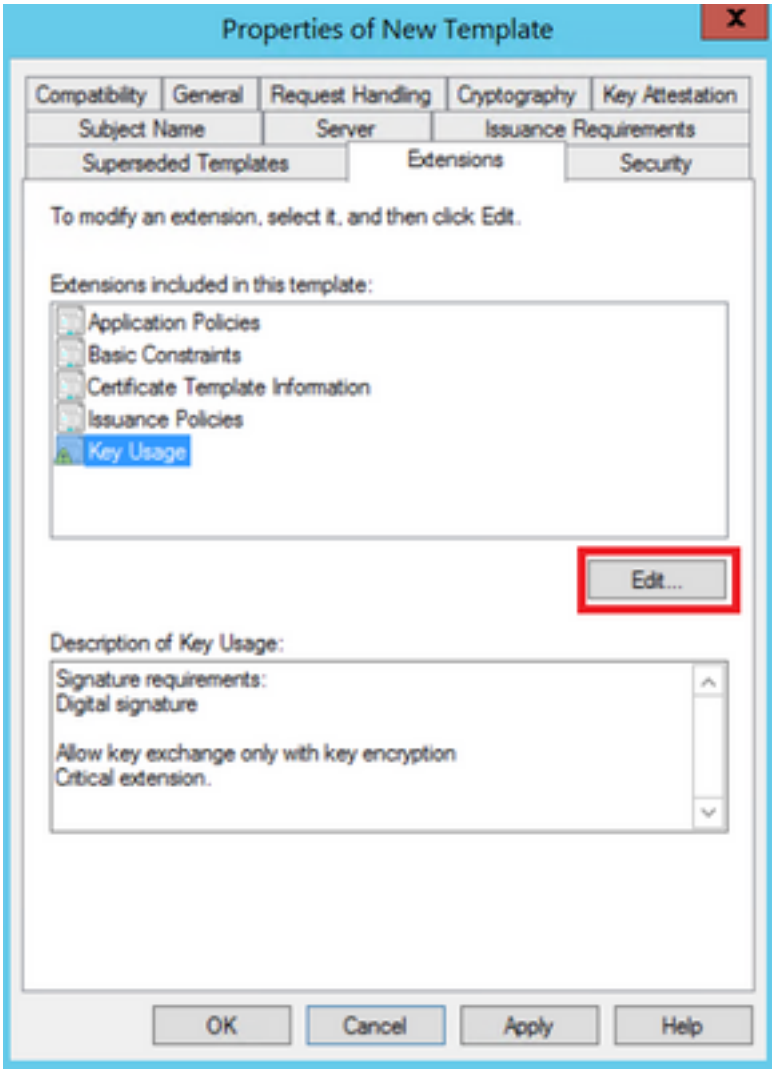
Schritt 1: Suchen Sie die **Webserver**-Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Vorlage duplizieren** aus, wie im Bild dargestellt.



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

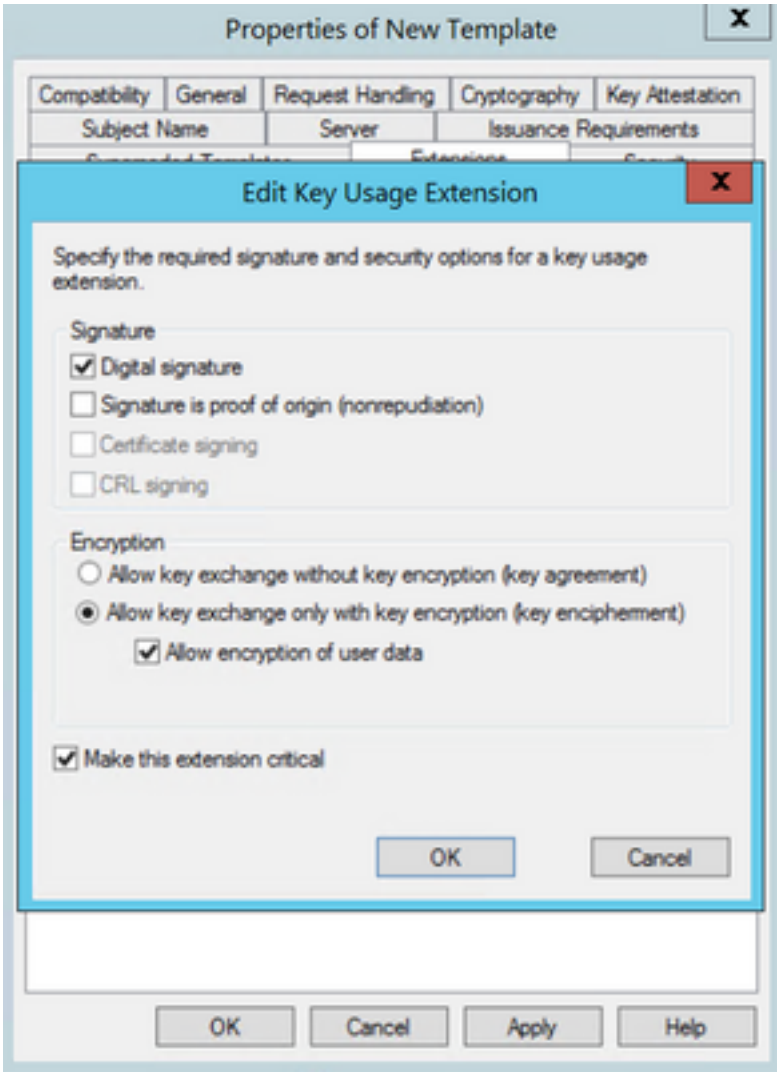


Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.

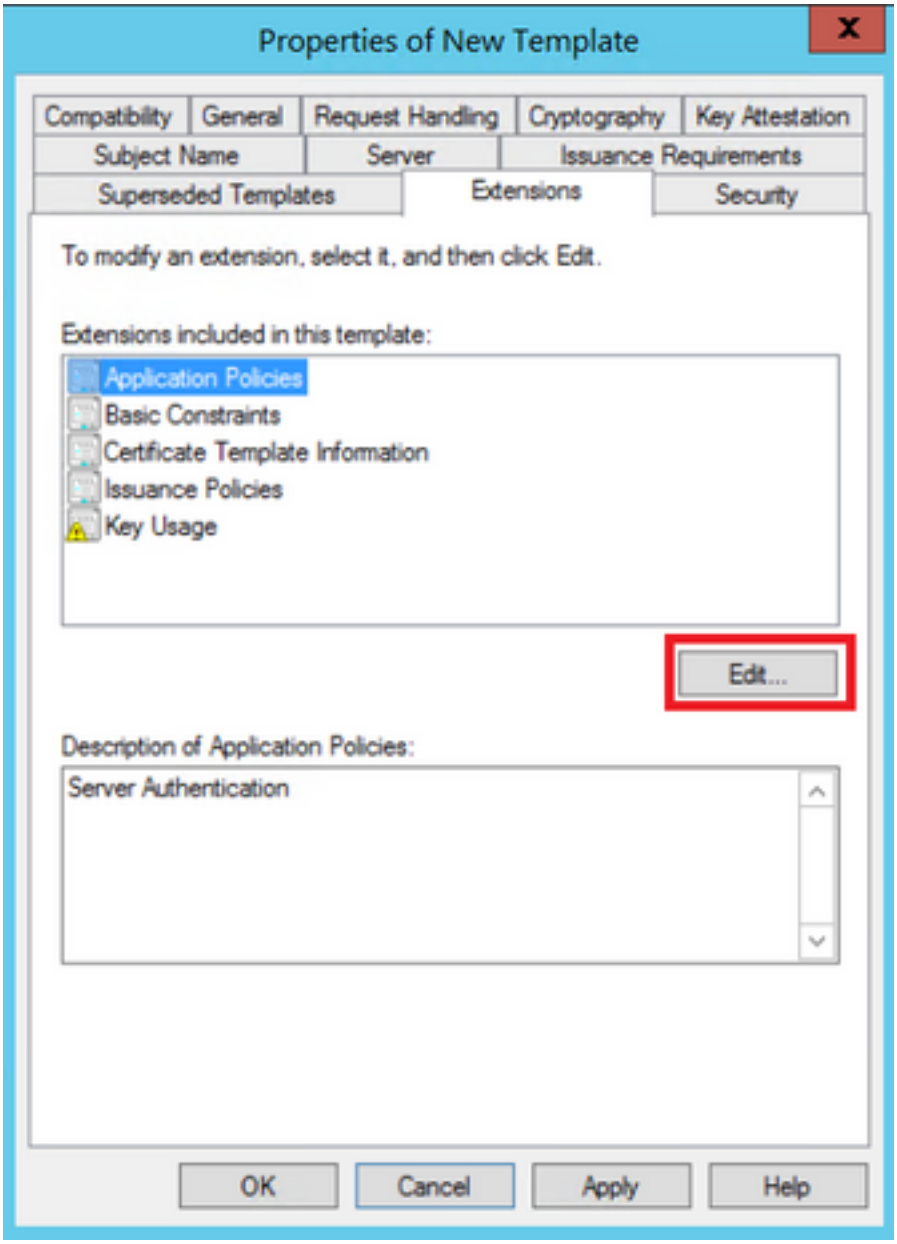


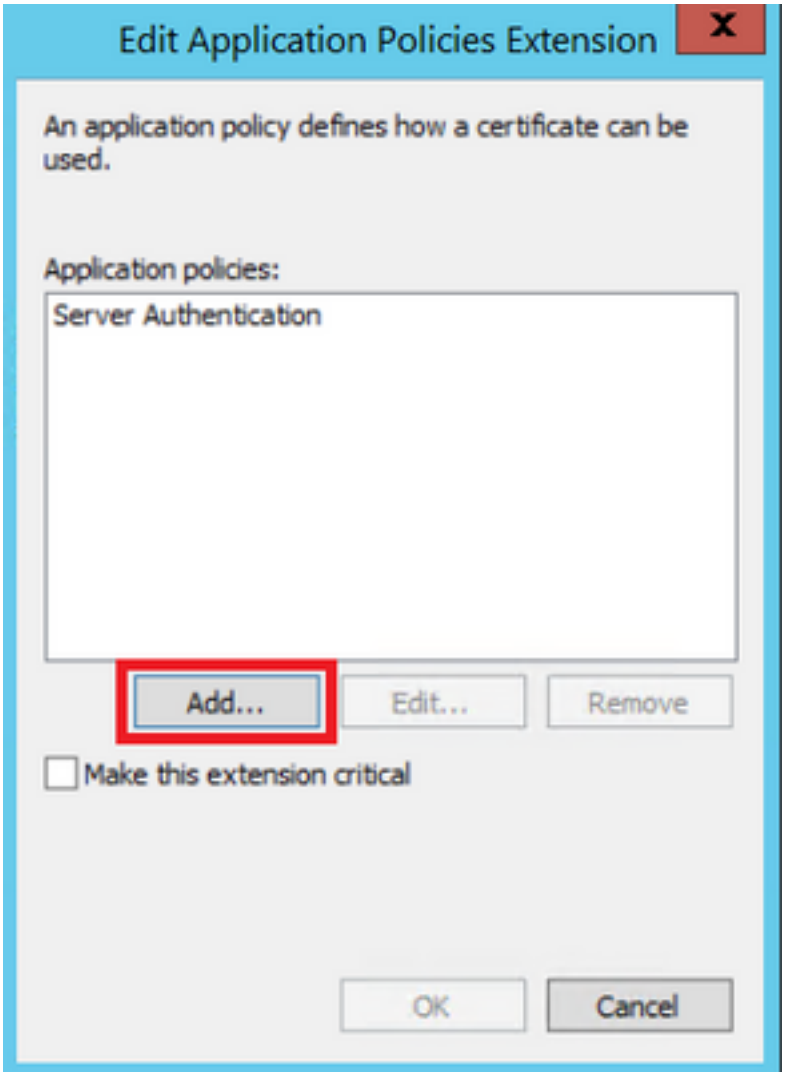
Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

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

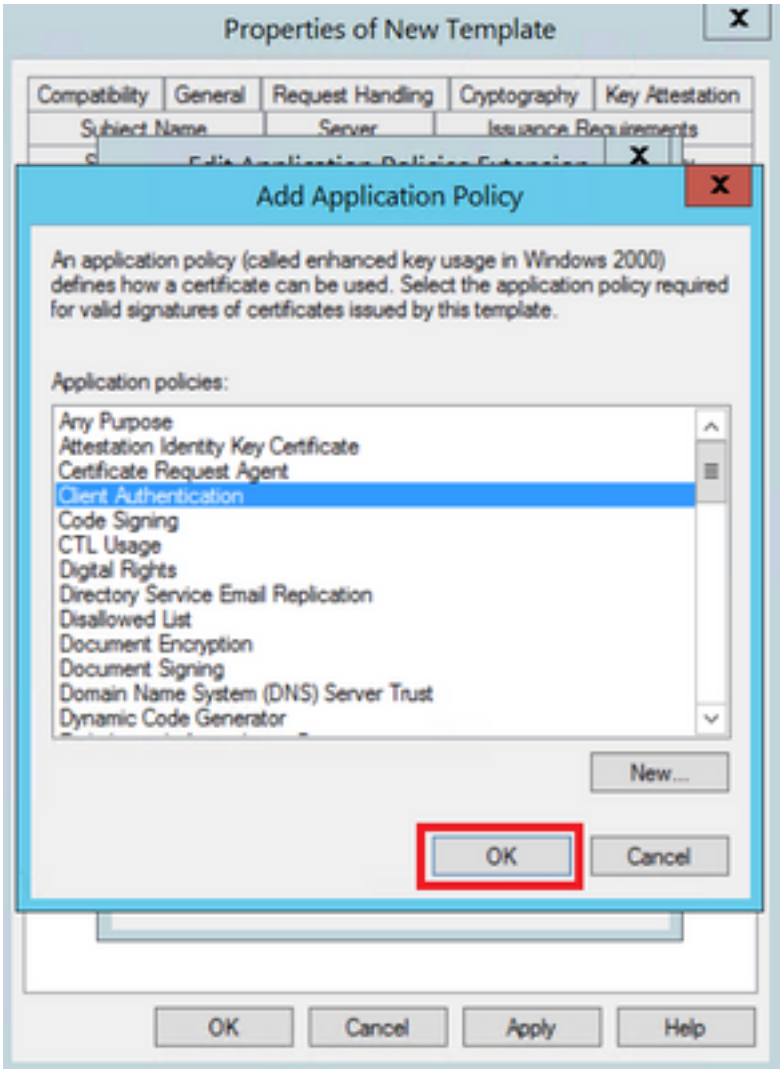


Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

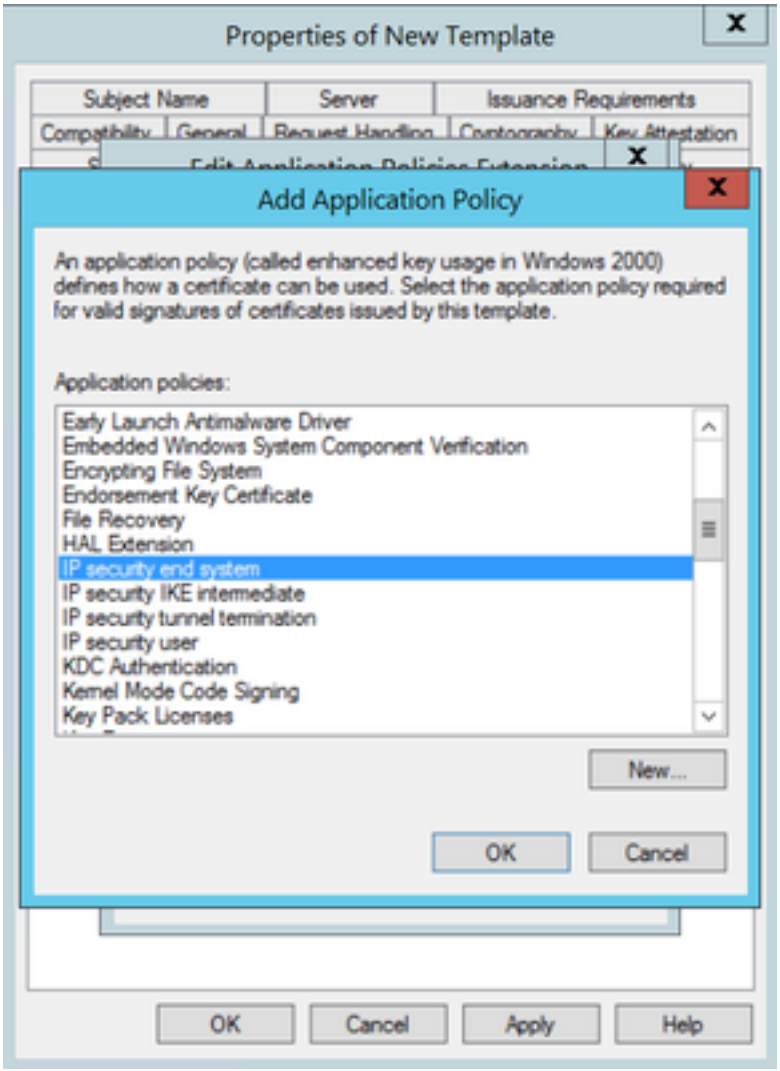

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



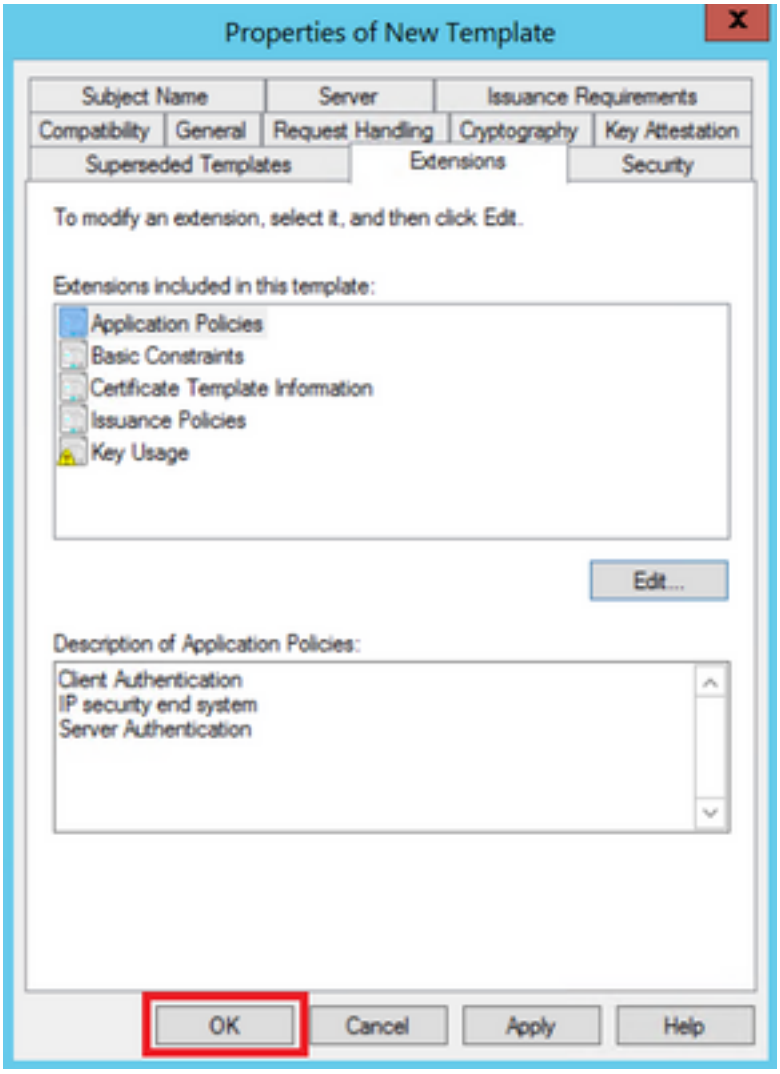
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und klicken Sie dann auf **OK**, wie im Bild gezeigt.



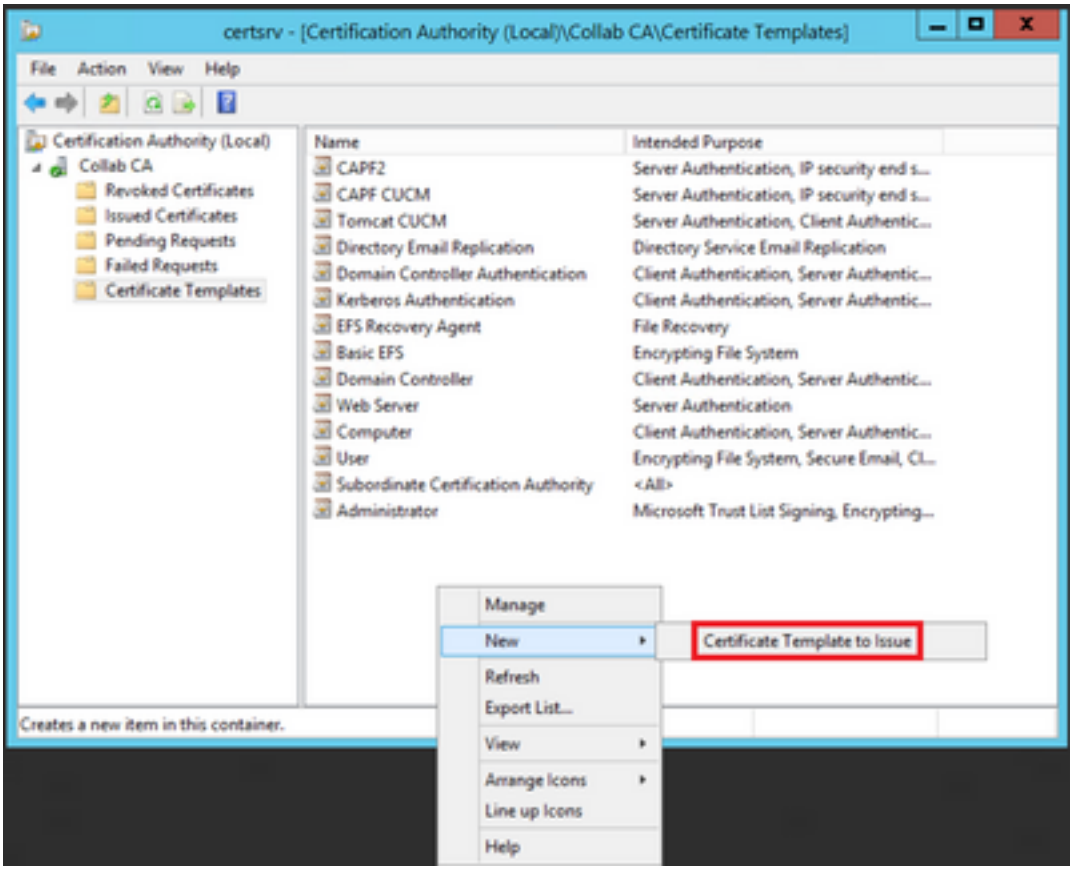
Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann in diesem und im vorherigen Fenster die Option **OK** aus.



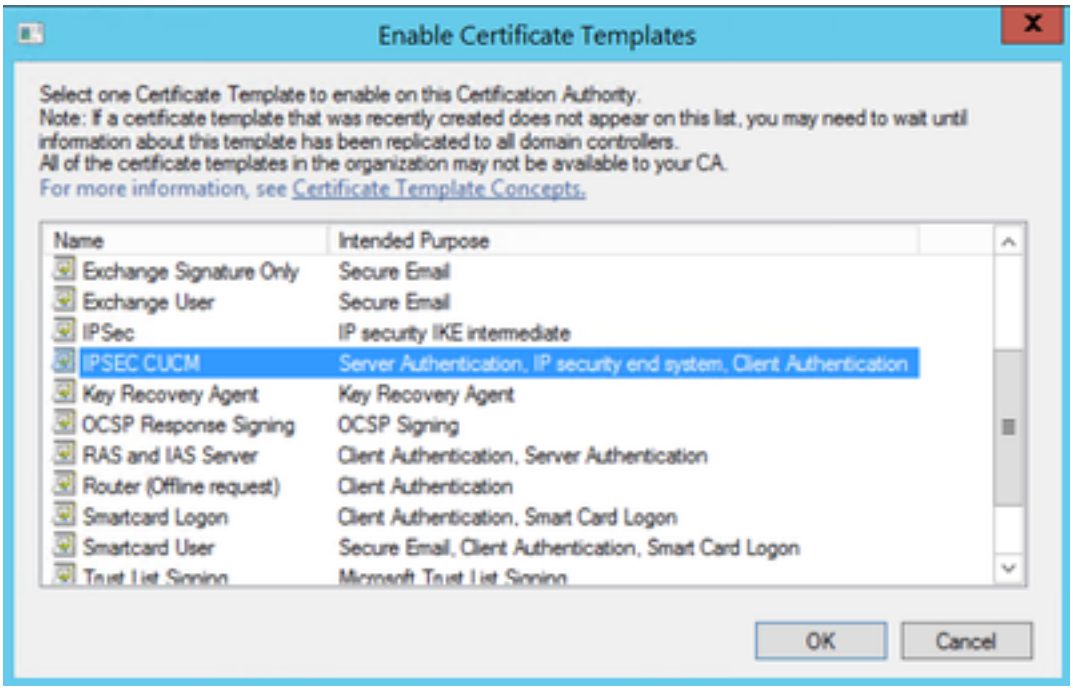
Schritt 8: Wählen Sie auf der Vorlage **Apply (Übernehmen)** und dann **OK**, wie im Bild dargestellt.



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

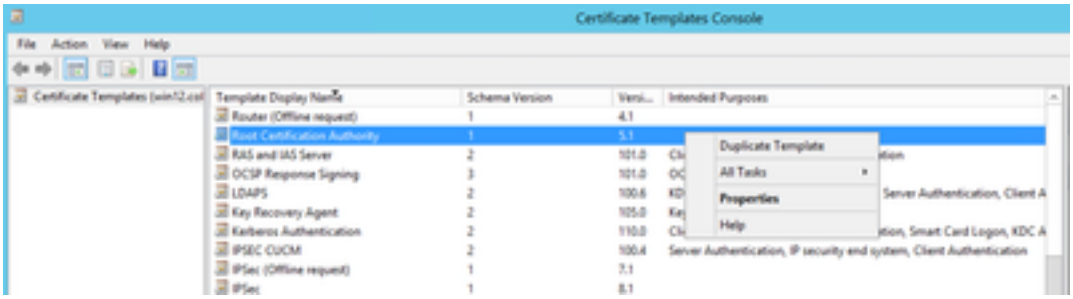


Schritt 10. Wählen Sie die neue **IPSEC-CUCM**-Vorlage aus, und wählen Sie auf **OK** aus, wie im Bild gezeigt.



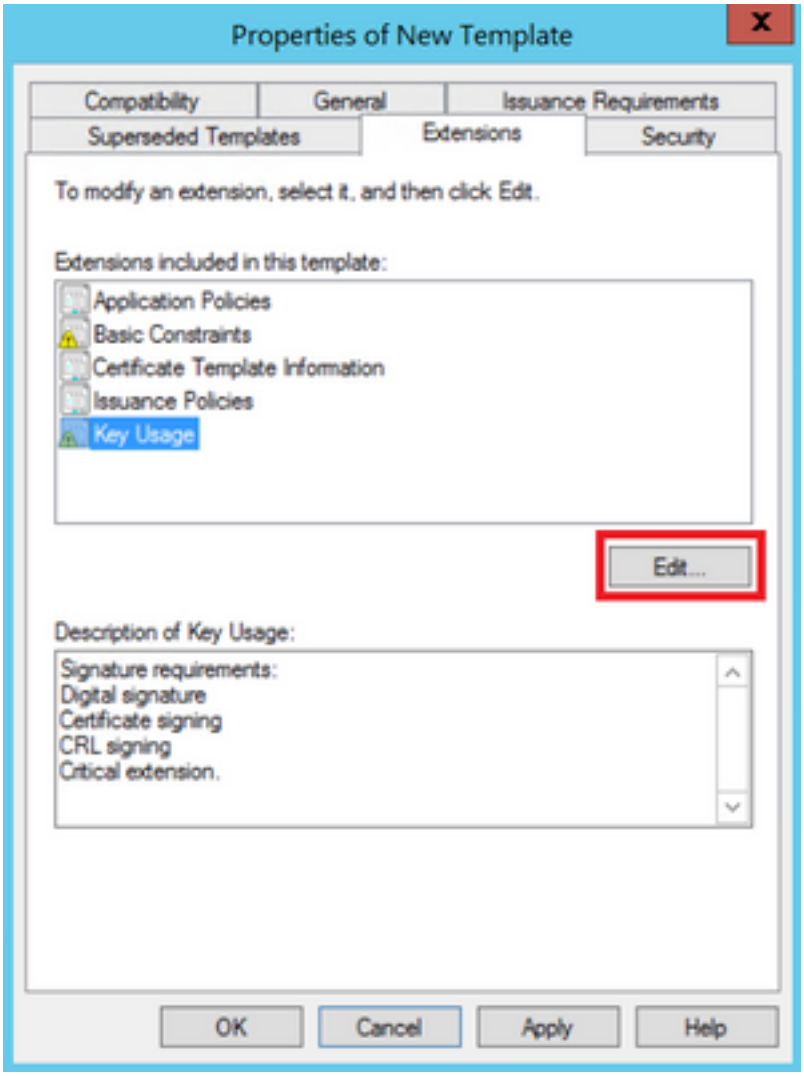
CAPF-Vorlage

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.



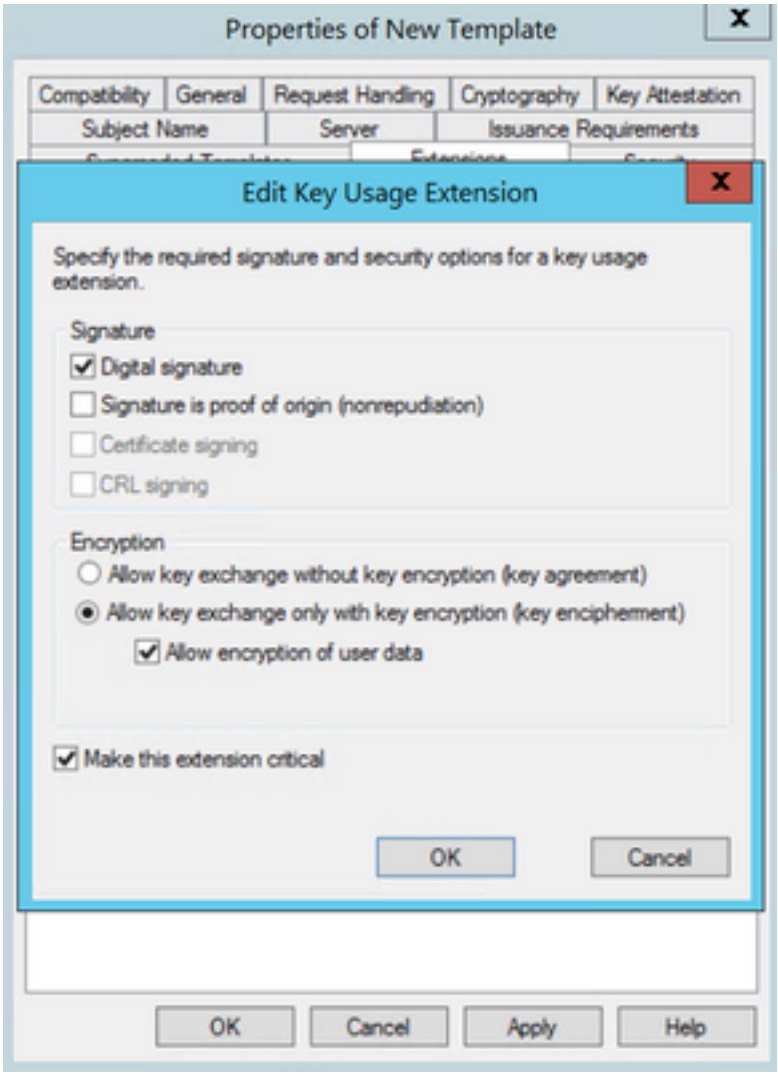
Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

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

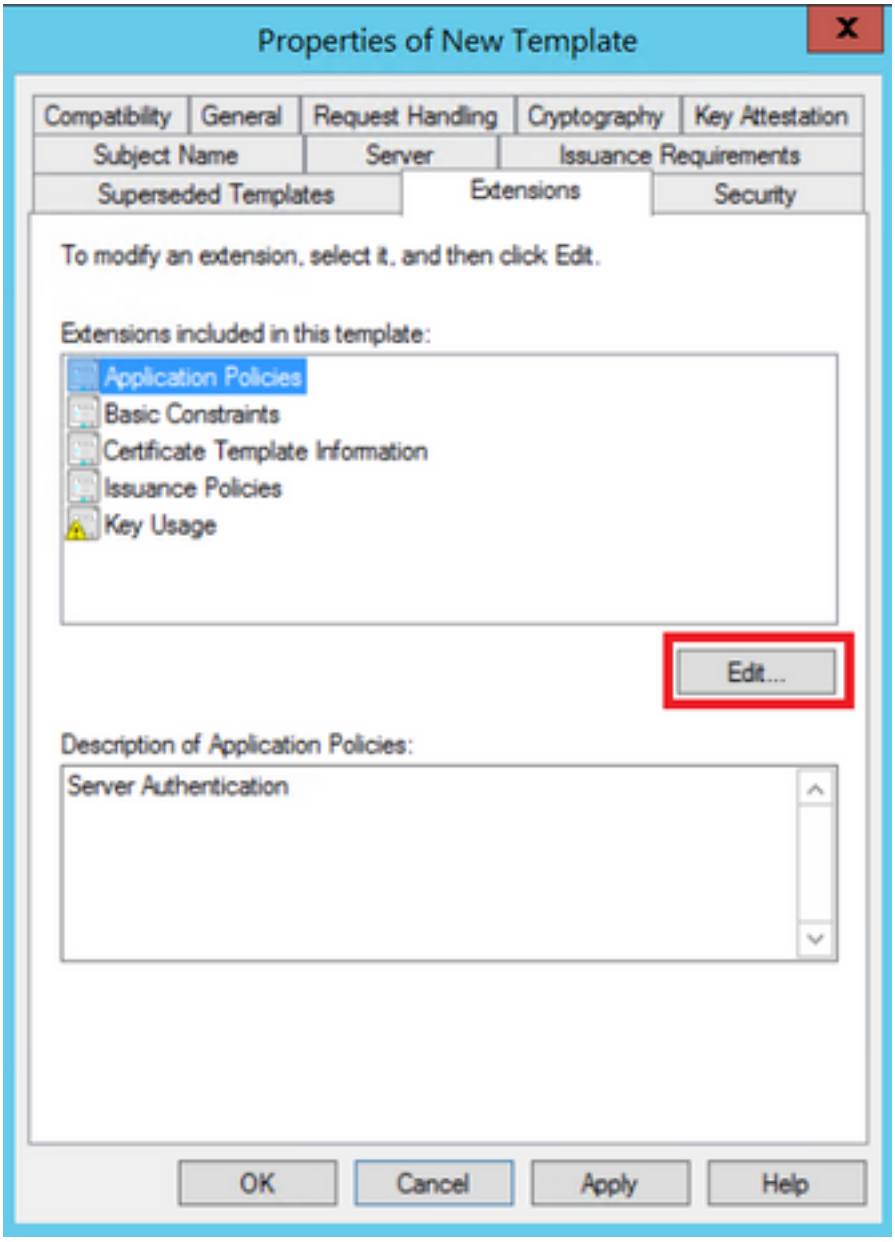


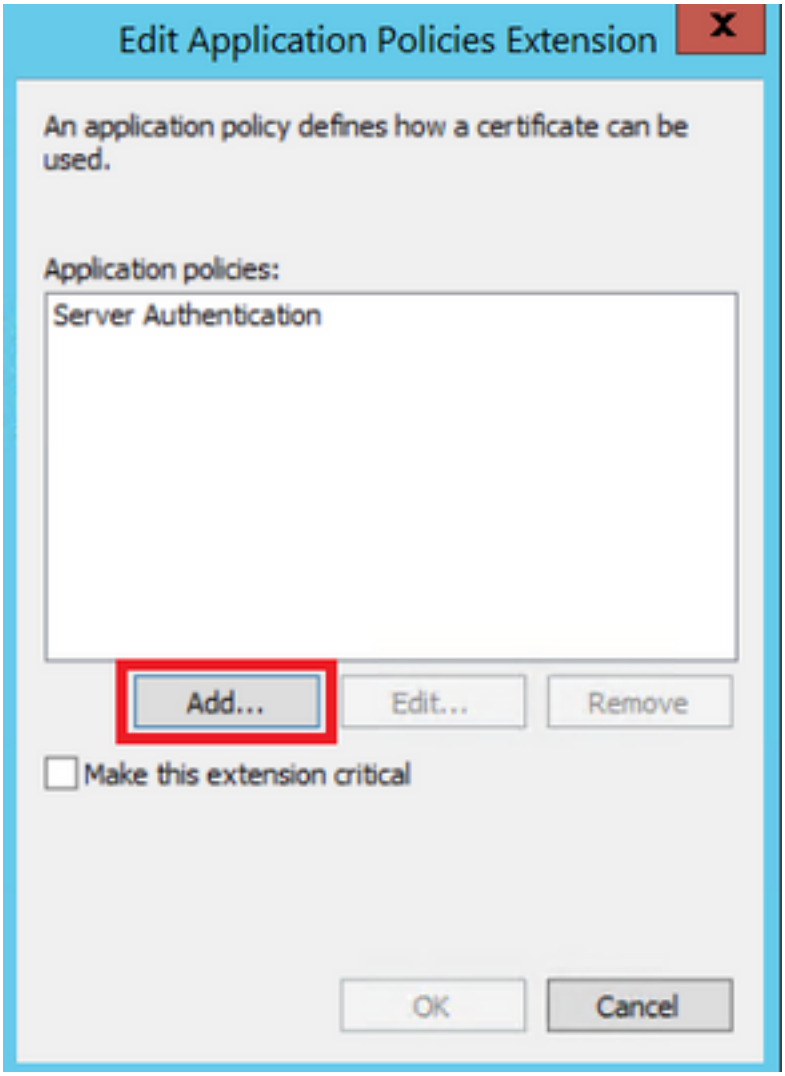
Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie **OK**, wie im Bild dargestellt.

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

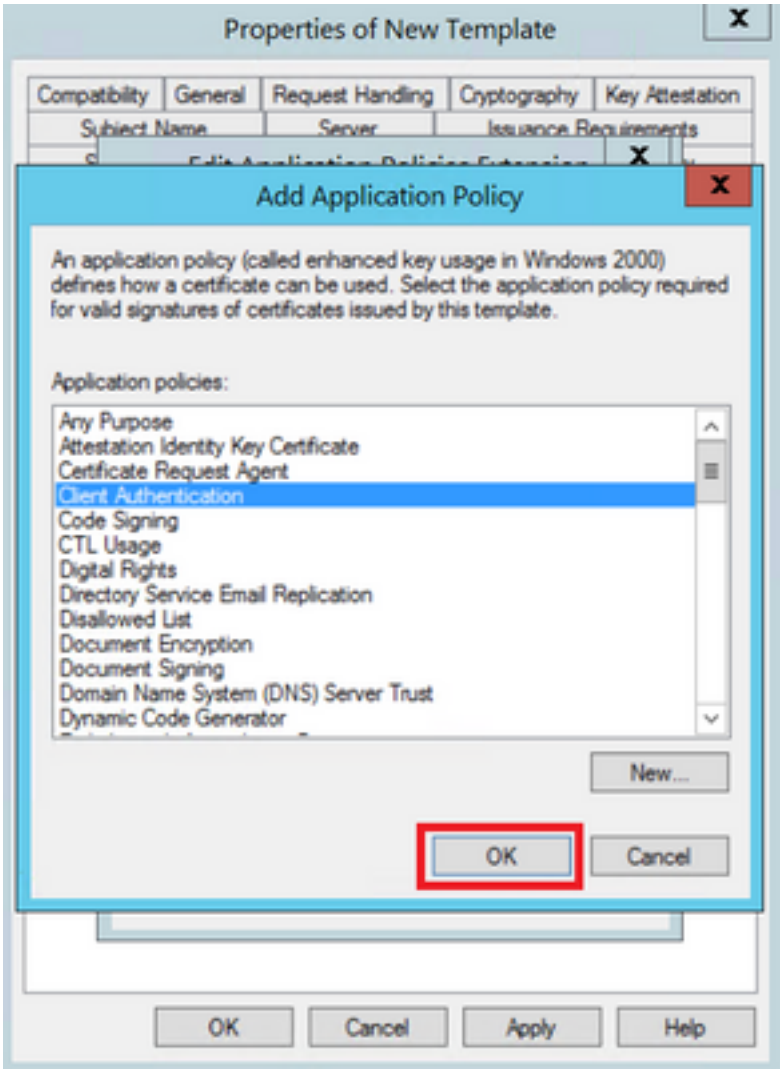


Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

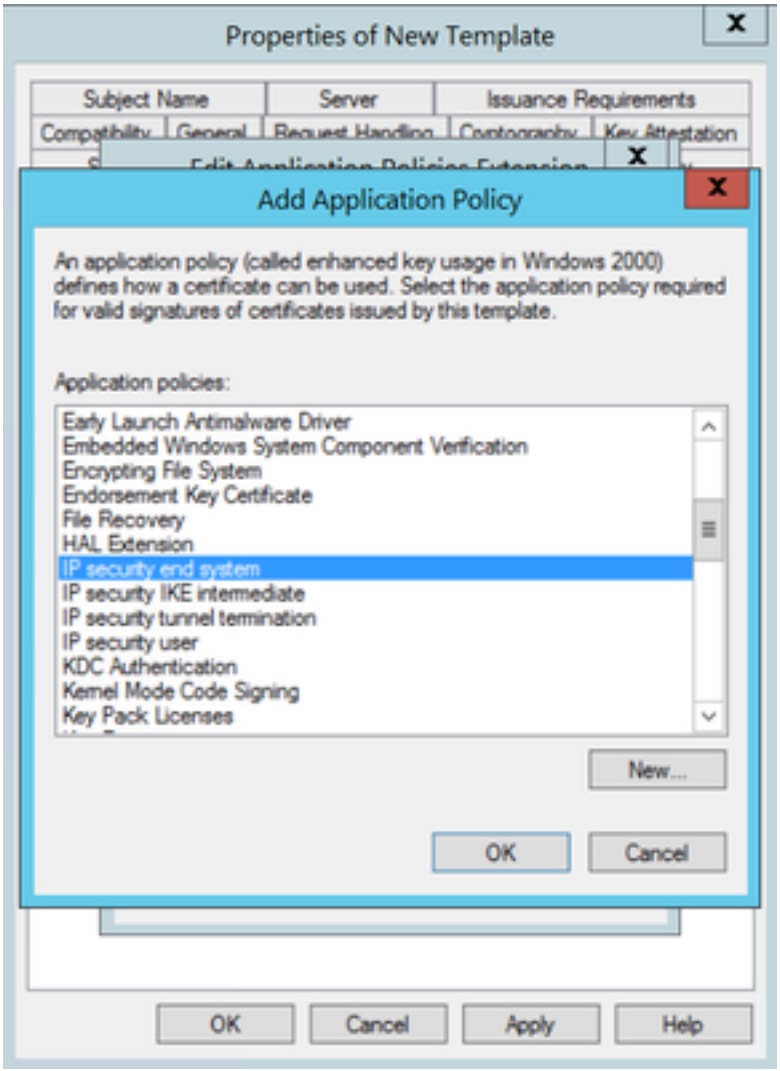

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



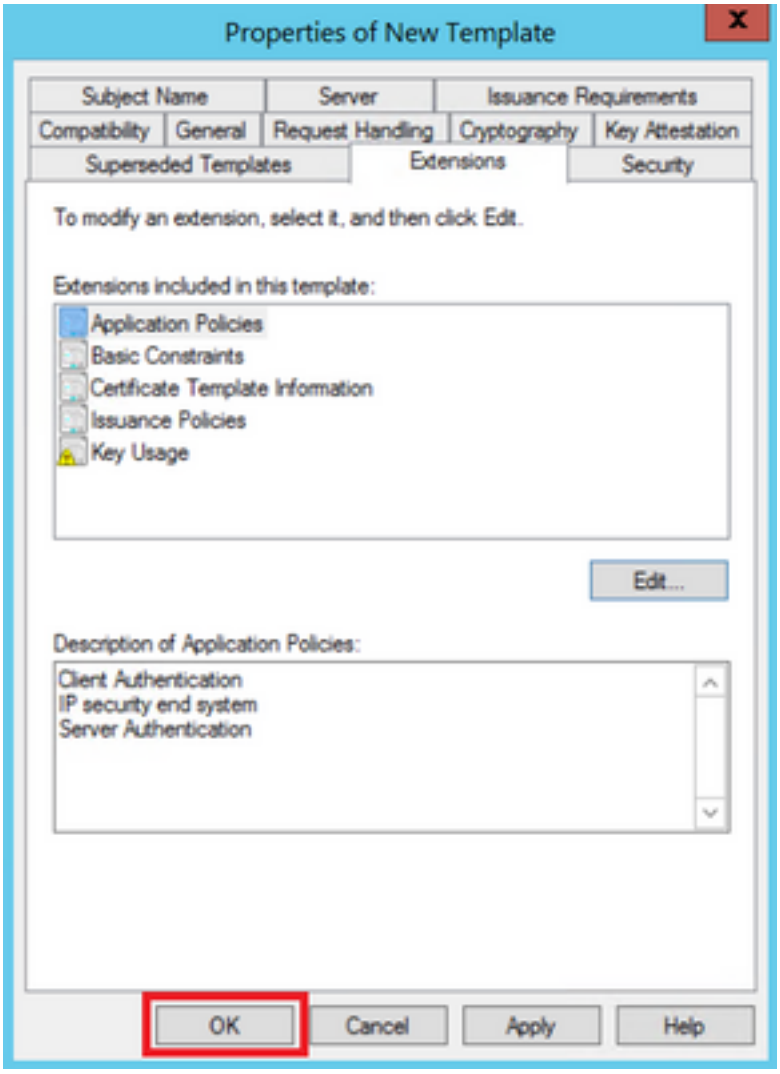
Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung)**, wählen Sie sie aus, und wählen Sie dann **OK** aus, wie im Bild gezeigt.



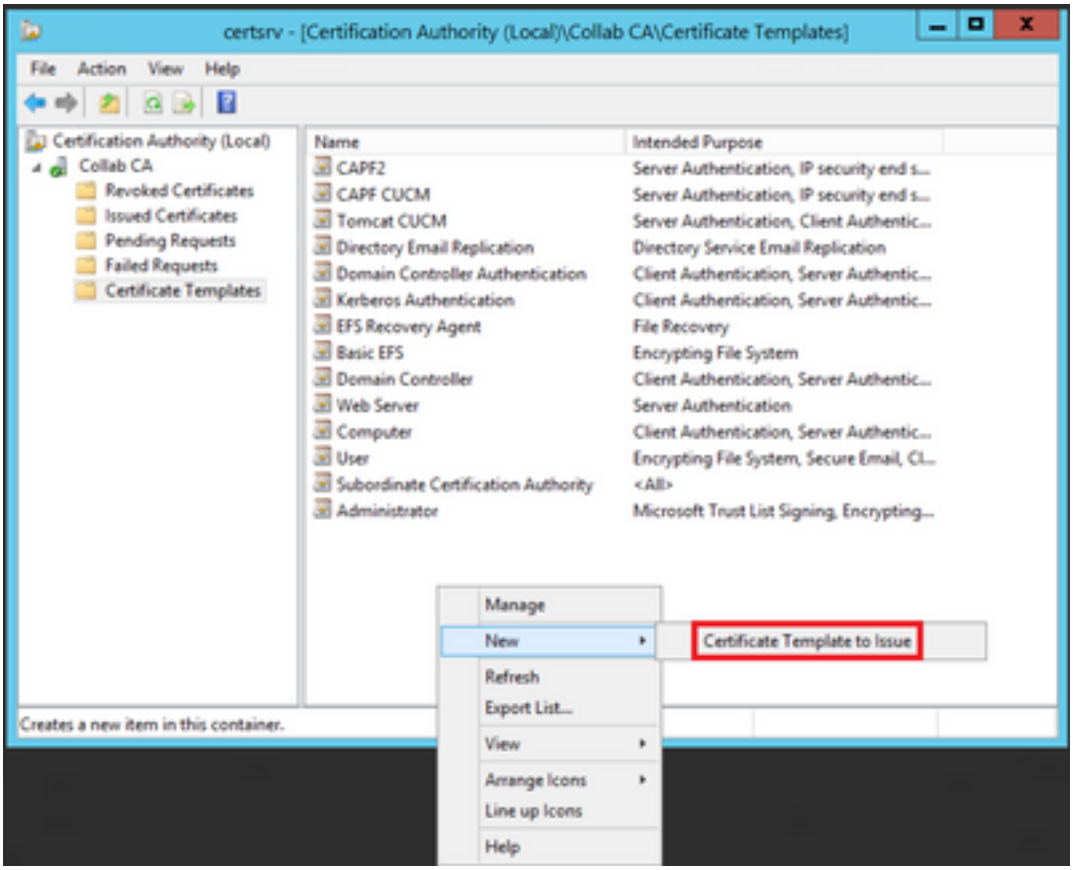
Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann OK für dieses und das vorherige Fenster aus, wie im Bild gezeigt.



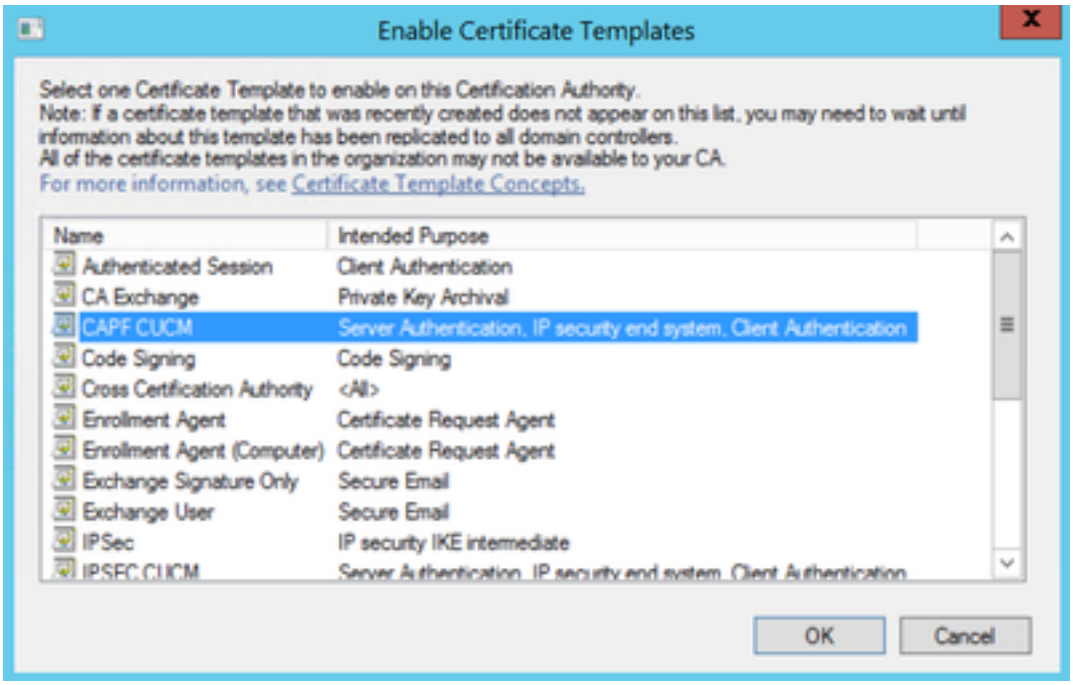
Schritt 8: Wählen Sie auf der Vorlage **Apply (Übernehmen)** und dann **OK**, wie im Bild dargestellt.



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

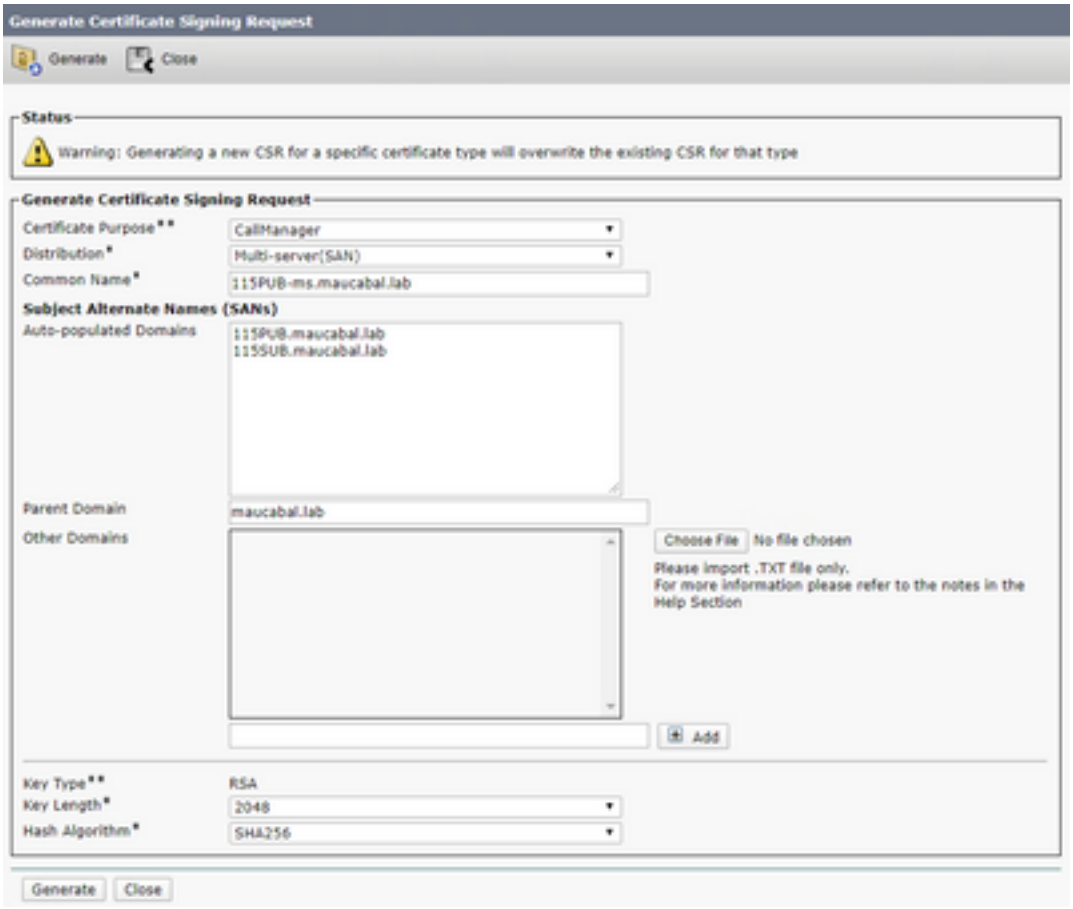
Verwenden Sie dieses Beispiel, um unter Verwendung der neu erstellten Vorlagen ein CallManager-Zertifikat zu generieren. Das gleiche Verfahren kann für jeden Zertifikatstyp verwendet werden. Sie müssen nur das Zertifikat und die Vorlagentypen entsprechend auswählen:

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

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

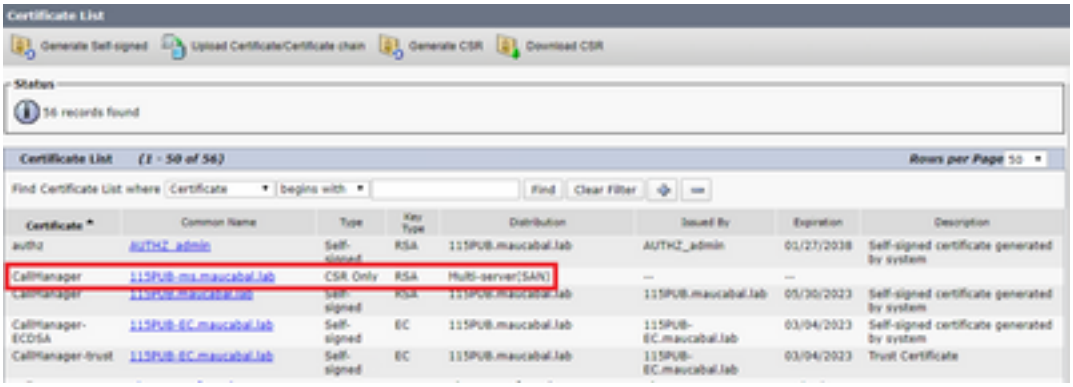
Schritt 2: Wählen Sie diese Optionen aus, und wählen Sie **Generate (Erstellen)** aus, wie im Bild dargestellt.

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

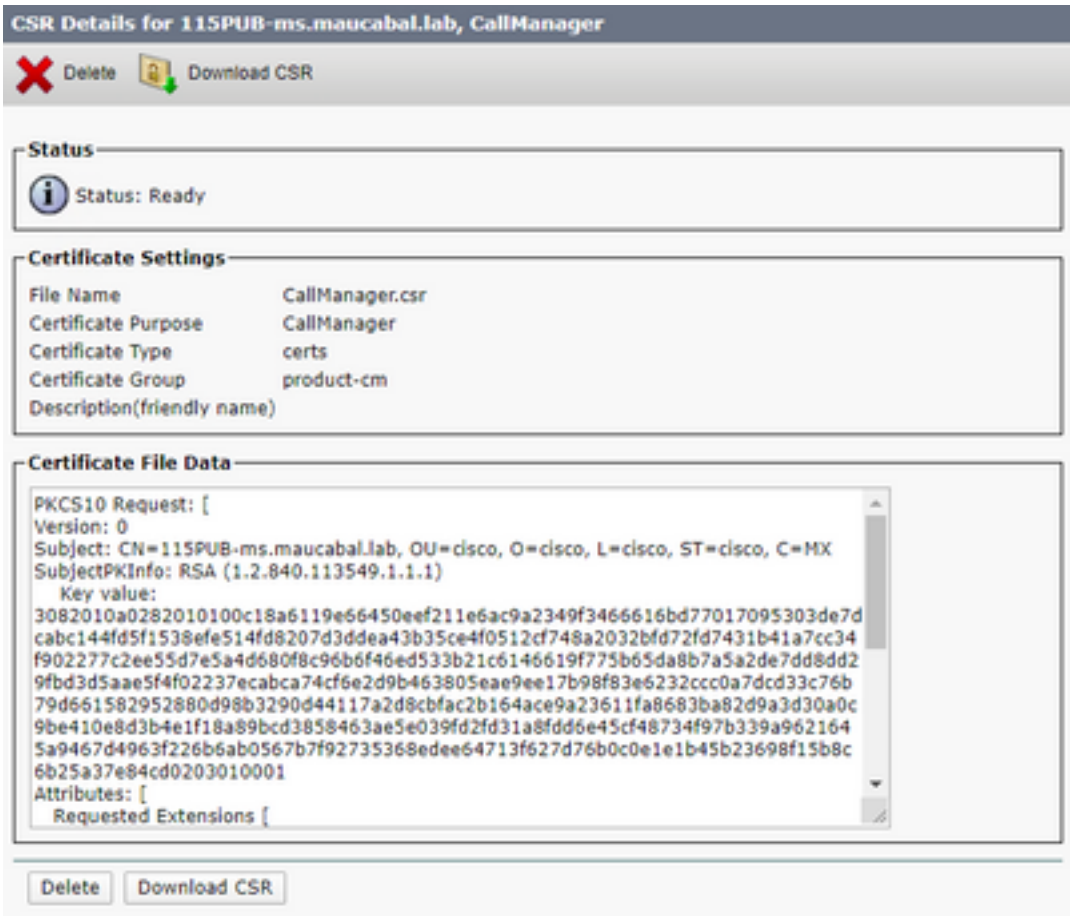


Schritt 3: Es wird eine Bestätigungsmeldung generiert, wie im Bild dargestellt.

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

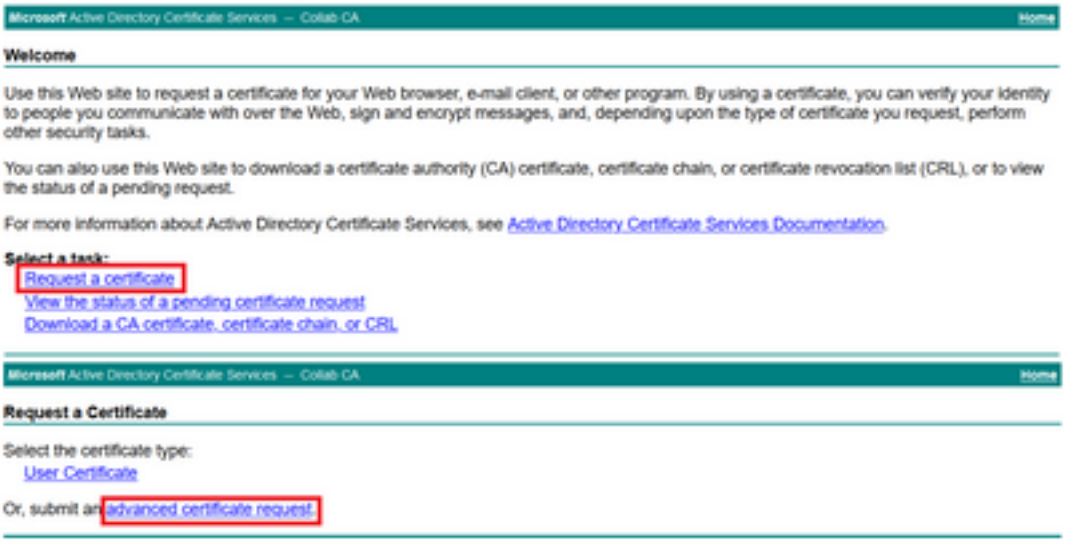


Schritt 5: Wählen Sie im Popup-Fenster die Option **CSR herunterladen**, und speichern Sie die Datei auf Ihrem Computer.

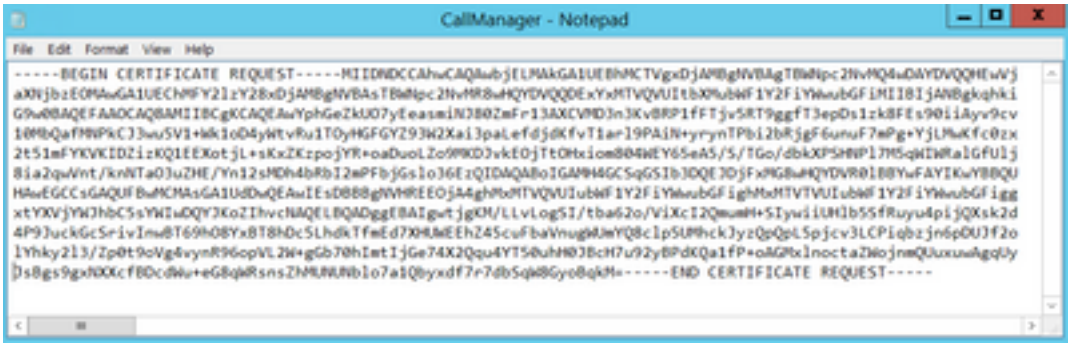


Schritt 6: Navigieren Sie in Ihrem Browser zu dieser URL, und geben Sie die Administratoranmeldeinformationen für den Domänencontroller ein: **https://<IhrWindowsServerIP>/certsrv/.**

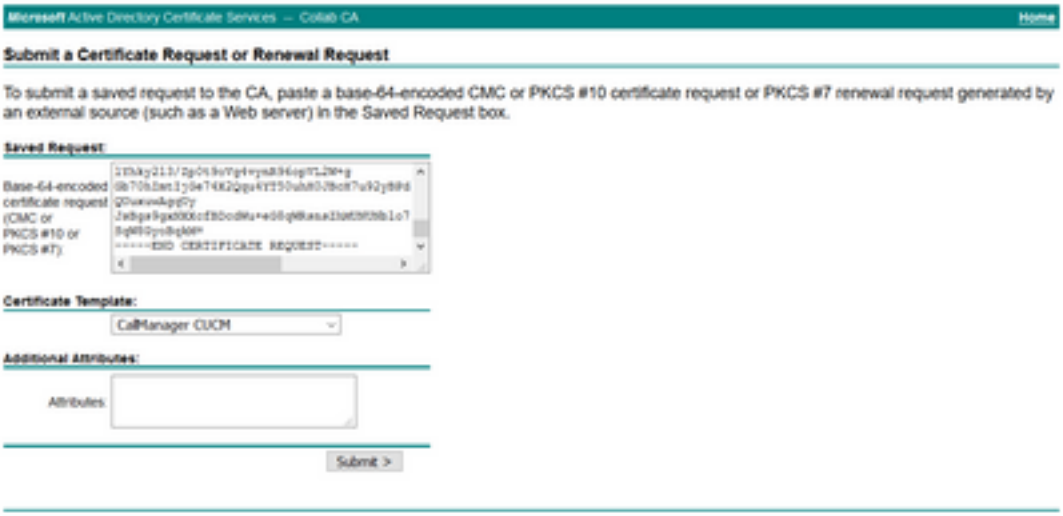
Schritt 7. Navigieren Sie zu **Request a certificate > advanced certificate request** (Zertifikat anfordern > Erweiterte Zertifikatanforderung), wie im Bild dargestellt.



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.