Windows CA-certificaatsjablonen voor CUCM maken

Inhoud

Inleiding

Dit document beschrijft een stapsgewijze procedure voor het maken van certificaatsjablonen op Windows Server-gebaseerde certificeringsinstanties (CA), die compatibel zijn met X.509-uitbreidingsvereisten voor elk type Cisco Unified Communications Manager (CUCM)-certificaat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM versie 11.5(1) of hoger
- Basiskennis van het Windows Server-beheer wordt ook aanbevolen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- De informatie in dit document is gebaseerd op CUCM versie 11.5(1) of hoger.
- Microsoft Windows Server 2012 R2 met CA-services geïnstalleerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Er zijn vijf soorten certificaten die door een externe CA kunnen worden ondertekend:

Certificaat	Gebruik	Betrokken services
CallManager	Bij beveiligde apparaatregistratie kunt u CTL-bestanden (Certificate Trust List)/ITL-bestanden (Internal Trust List) ondertekenen, die worden gebruikt voor beveiligde interacties met andere servers zoals Secure Session Initiation Protocol (SIP)-trunks.	·Cisco Call Manager ·Cisco CTI Manager ·Cisco TFTP
kater	Aangeboden voor Secure Hypertext Transfer Protocol (HTTPS)-interacties.	·Cisco Tomcat ·Single Sign-On (SSO) ·Uitbreidingsmobiliteit ·Corporate Directory
ipsec	Wordt gebruikt voor het genereren van back-upbestanden, evenals interactie met IPsec (IPsec) en Media Gateway Control Protocol (MGCP) of H323-gateways.	·Cisco DRF-master ·Lokale Cisco DRF
CAPF	Gebruikt om Locally Significant Certificates (LSC) voor telefoons te genereren.	·Functie van Cisco-certificeringsinstantie
TV's	Gebruikt om een verbinding te maken met de Trust Verification Service (TVS), wanneer de telefoons niet in staat zijn om een onbekend certificaat te verifiëren.	·Cisco Trust Verification Service

Elk van deze certificaten heeft een aantal X.509-uitbreidingsvereisten die moeten worden ingesteld, anders kunt u op een van de bovengenoemde diensten fouten tegenkomen:

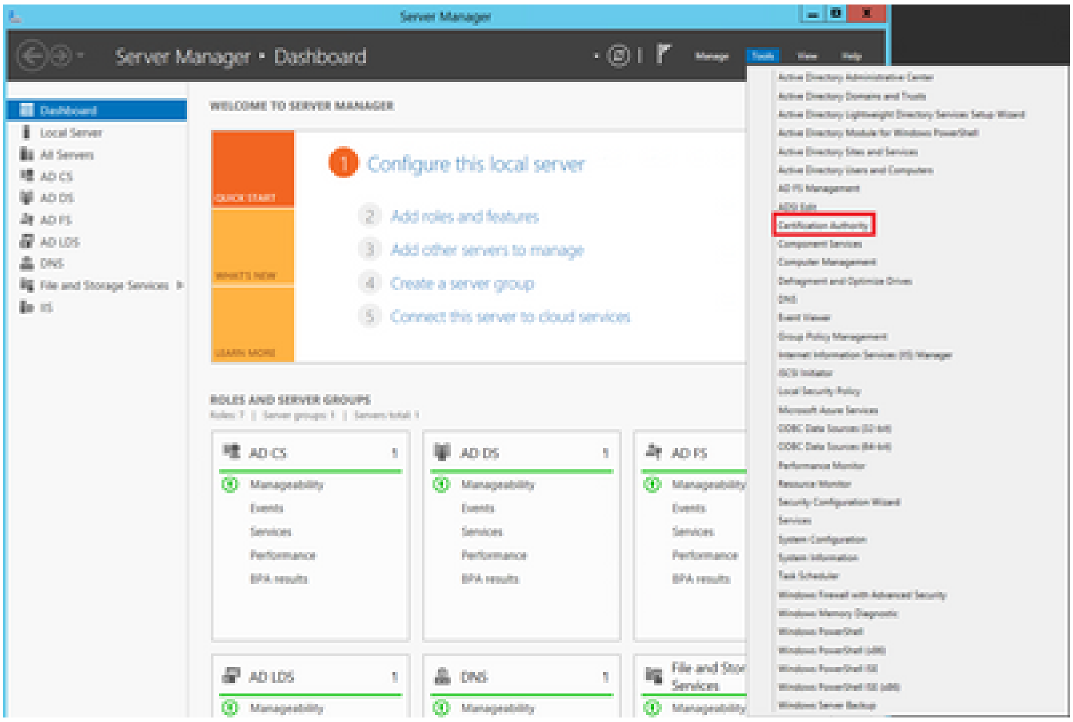
Certificaat	X.509-toetsgebruik	Uitgebreid sleutelgebruik van X.509
CallManager	·Digitale handtekening ·Key Encipherment ·Gegevensversleuteling	·Webserververificatie ·Web clientverificatie
kater	·Digitale handtekening ·Key Encipherment ·Gegevensversleuteling	·Webserververificatie ·Web clientverificatie
ipsec	·Digitale handtekening ·Key Encipherment ·Gegevensversleuteling	·Webserververificatie ·Web clientverificatie ·IPsec-eindsysteem
CAPF	·Digitale handtekening	·Webserververificatie ·Web clientverificatie

	·Certificaatteken ·Key Encipherment	
TV's	·Digitale handtekening ·Key Encipherment ·Gegevensversleuteling	·Webserververificatie ·Web clientverificatie

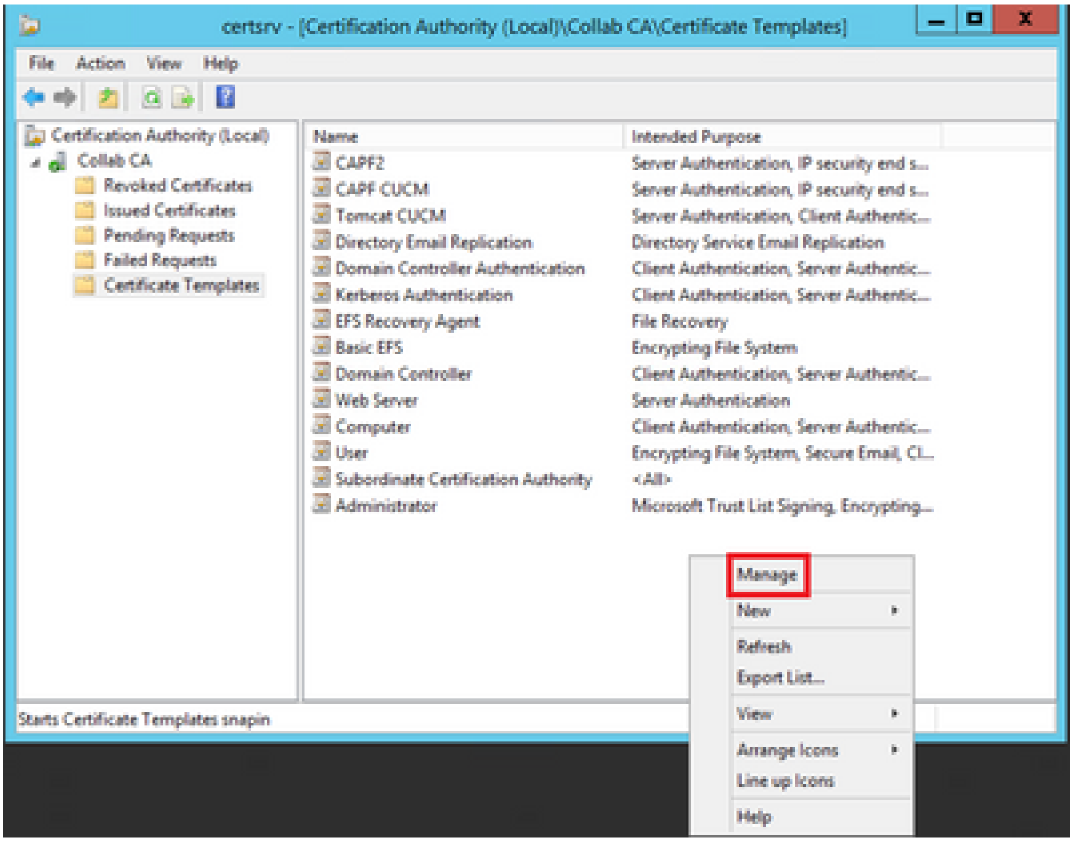
Raadpleeg de Security Guide voor Cisco Unified Communications Manager voor meer informatie

Configureren

Stap 1. Navigeer op de Windows Server naar **Server Manager > Gereedschappen > Certificeringsinstantie**, zoals in de afbeelding.


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

Stap 2. Selecteer uw CA, navigeer vervolgens naar **certificaatsjablonen**, klik met de rechtermuisknop op de lijst en selecteer **Beheer**, zoals in de afbeelding.

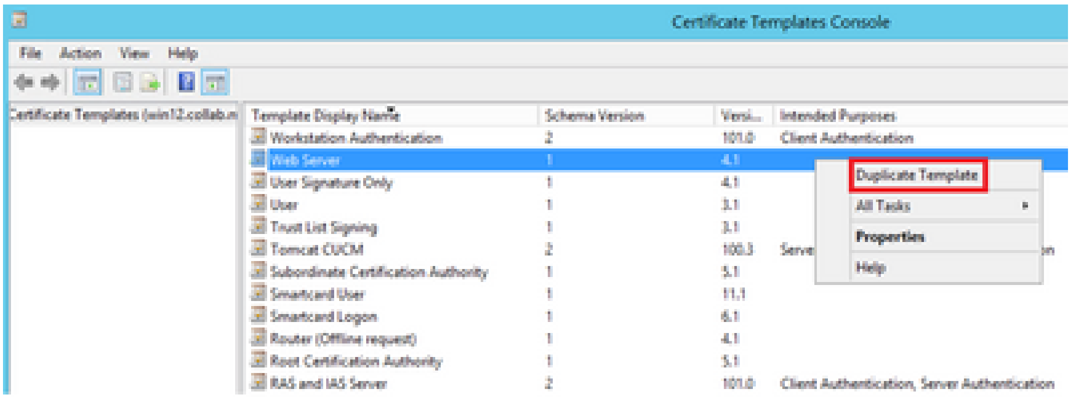


Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication,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

Callmanager / Tomcat / TVS Template

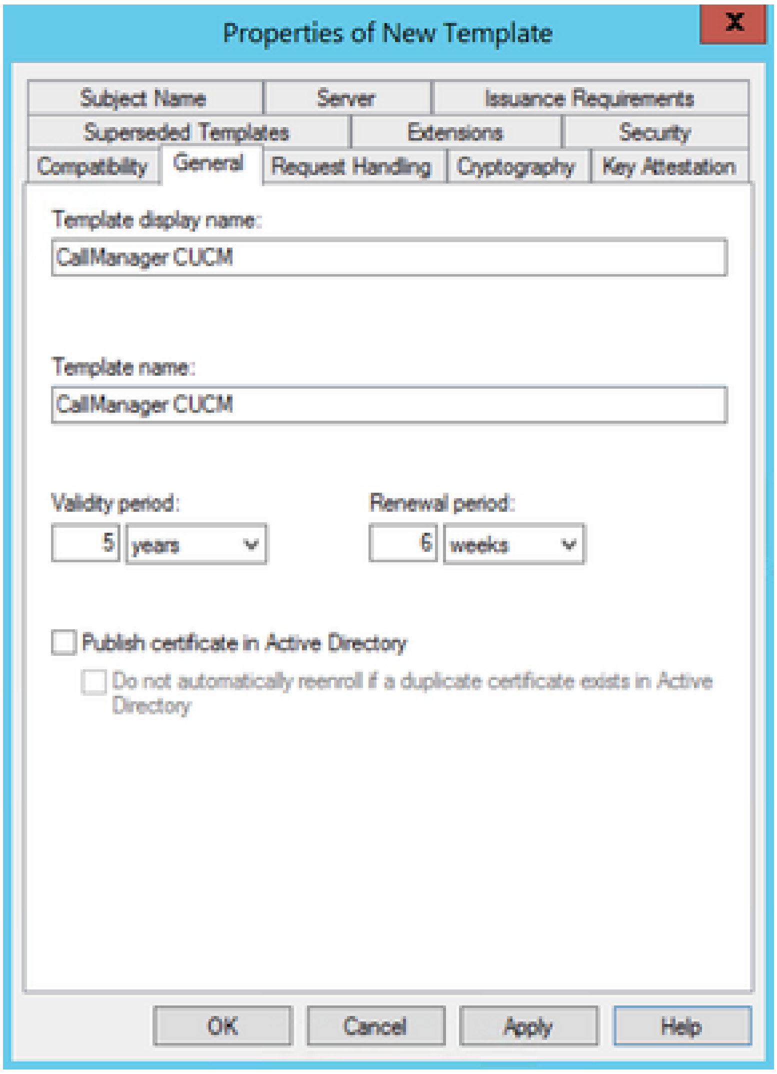
De volgende afbeeldingen tonen alleen de creatie van de CallManager-sjabloon; maar dezelfde stappen kunnen worden gevolgd om de certificaat-sjablonen voor de Tomcat en de TVS-services te maken. Het enige verschil is dat de respectievelijke servicenaam voor elke nieuwe sjabloon in stap 2 moet worden gebruikt.

Stap 1. Vind de **Web Server** sjabloon, klik met de rechtermuisknop op het en selecteer **Duplicate Template**, zoals in de afbeelding.


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

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

Stap 2. Onder **Algemeen**, kunt u de naam van het certificaatmalplaatje, de vertoningsnaam, geldigheid, enz. veranderen.



Template display name:
CallManager CUCM

Template name:
CallManager CUCM

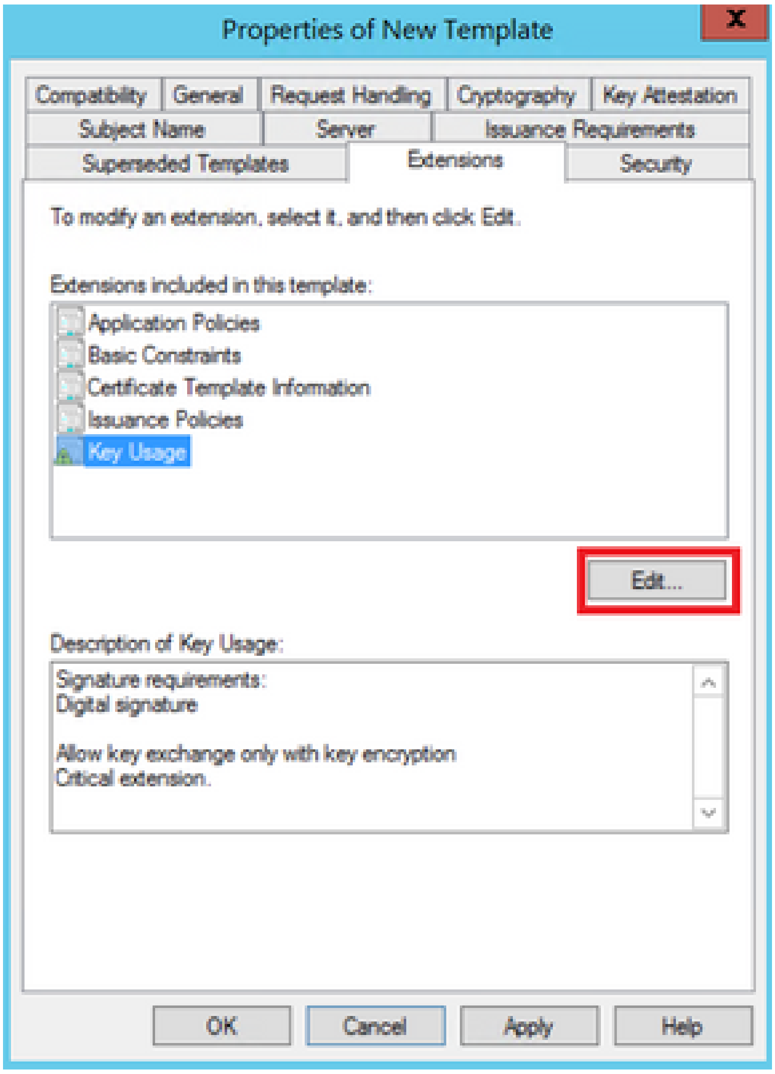
Validity period:
5 years

Renewal period:
6 weeks

□ Publish certificate in Active Directory

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

Stap 3. Navigeer naar **Uitbreidingen > Hoofdgebruik > Bewerken**, zoals in de afbeelding wordt getoond.



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

Extensions included in this template:

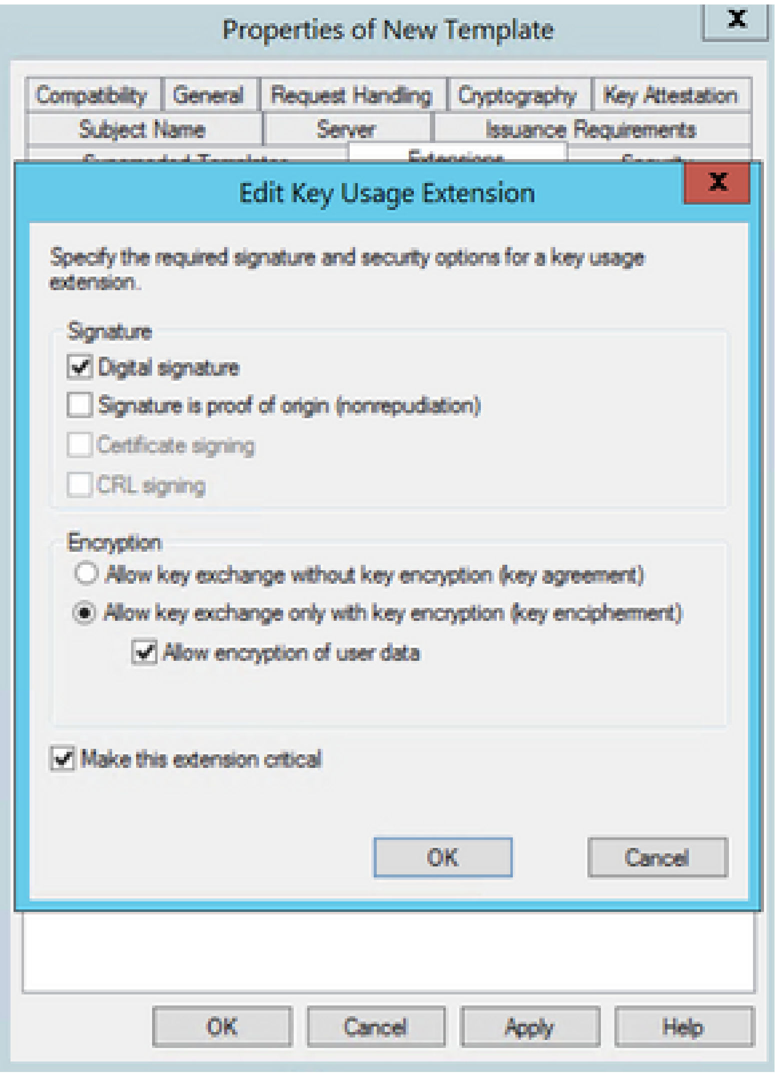
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Stap 4. Selecteer deze opties en selecteer **OK**, zoals in de afbeelding.

- **Digitale handtekening**
- **Toetsuitwisseling alleen toestaan met sleutelcodering (sleutelcodering)**
- **Versleuteling van gebruikersgegevens toestaan**



Properties of New Template

Compatibility | General | Request Handling | Cryptography | Key Attestation

Subject Name | Server | Issuance Requirements

Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

Signature

☑ Digital signature

□ Signature is proof of origin (nonrepudiation)

□ Certificate signing

□ CRL signing

Encryption

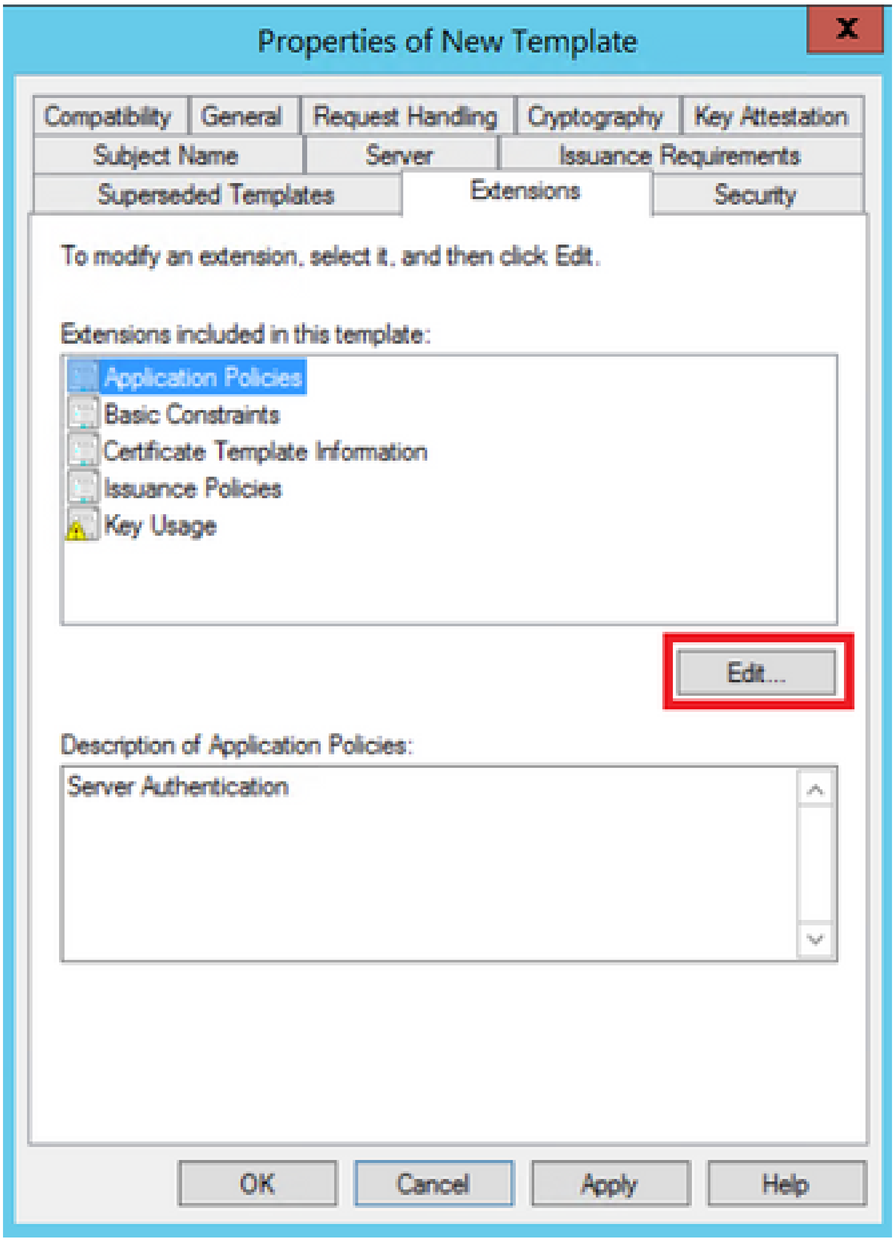
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

Stap 5. Navigeer naar **Uitbreidingen > Toepassingsbeleid > Bewerken > Toevoegen**, zoals in de afbeelding.



Properties of New Template

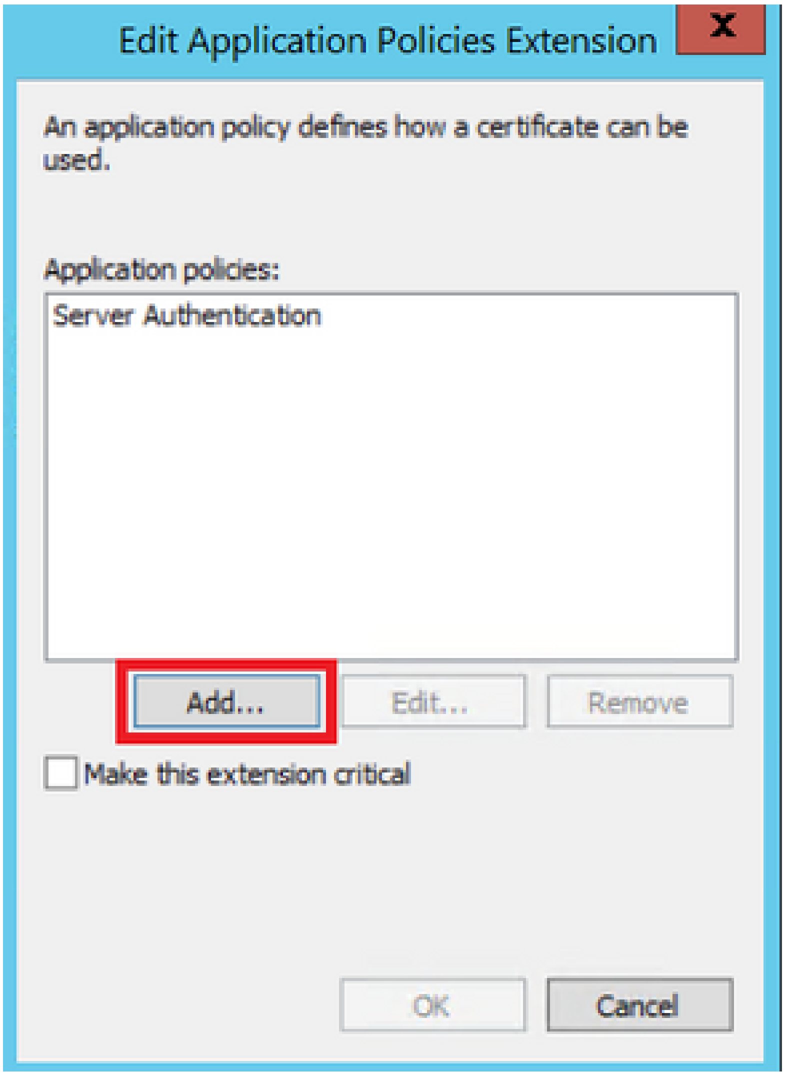
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



Edit Application Policies Extension

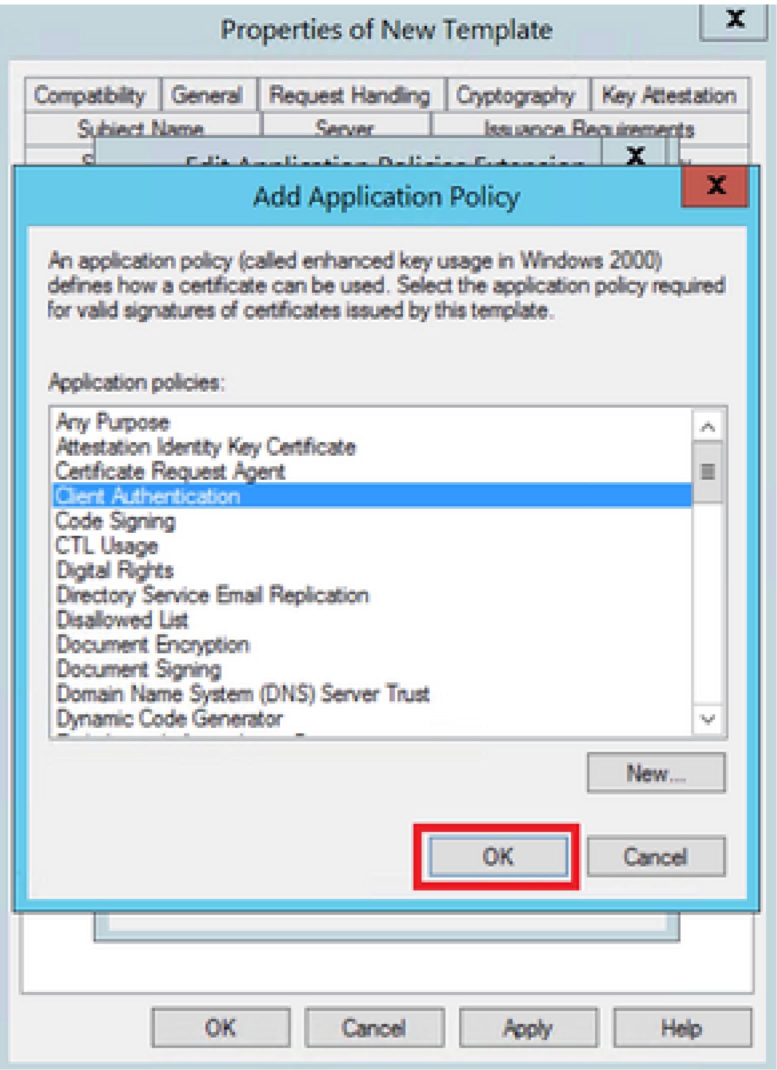
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

Stap 6. Zoek naar **clientverificatie,** selecteer deze en selecteer **OK** in zowel dit als het vorige venster, zoals wordt aangegeven in de afbeelding.



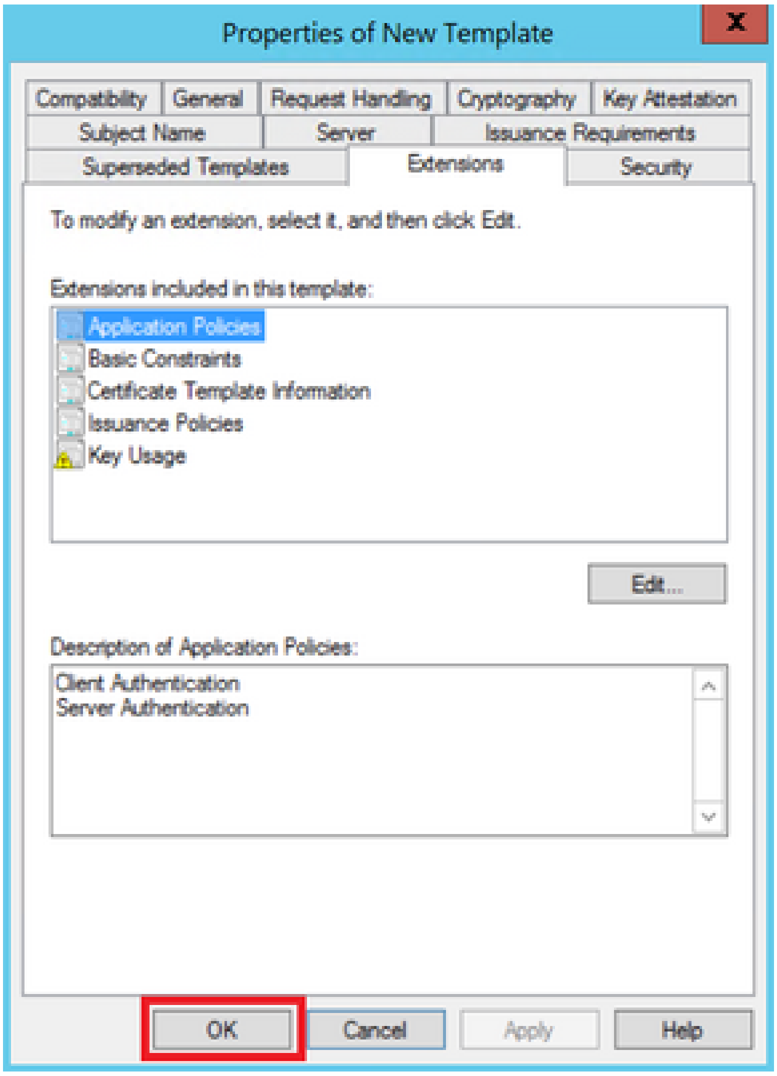
Properties of New Template
Compatibility | General | Request Handling | Cryptography | Key Attestation
Subject Name | Server | Issuance Requirements
Edit Application Policies Extension
Add Application Policy

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

Stap 7. Terug op de sjabloon selecteert u **Toepassen** en vervolgens **OK.**



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

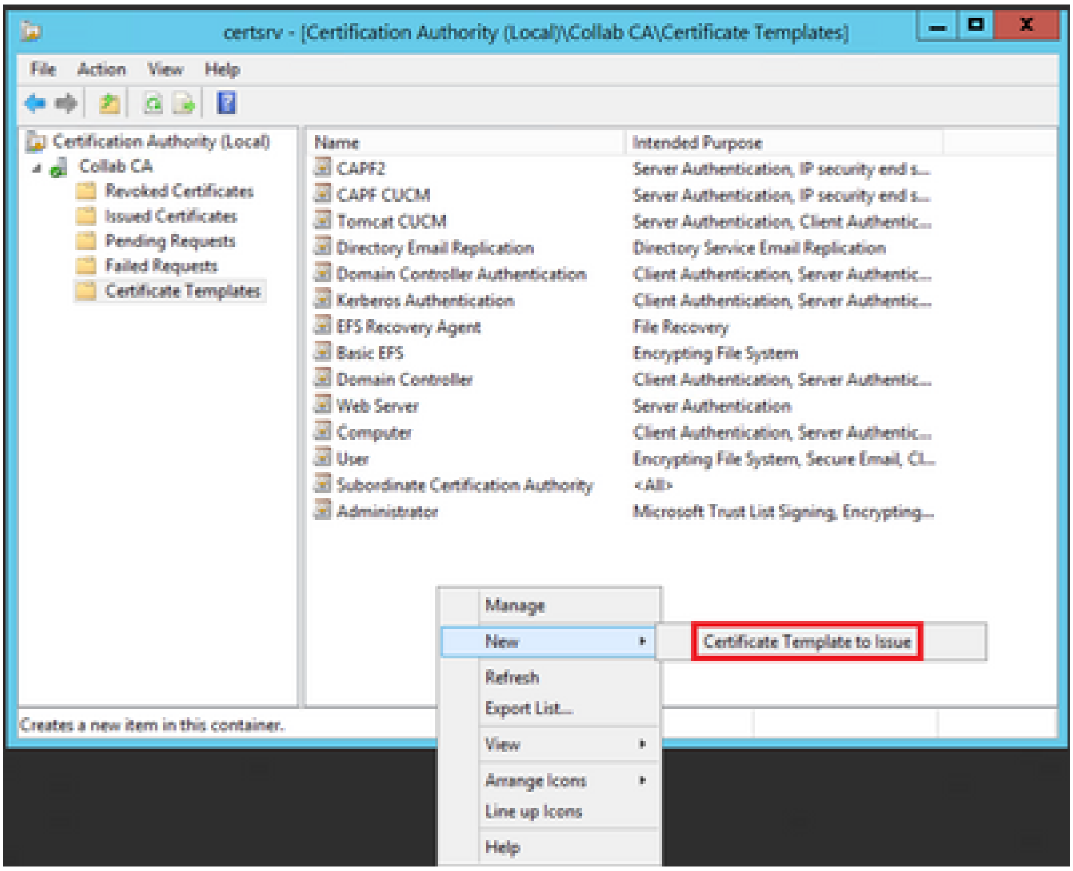
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
Server Authentication

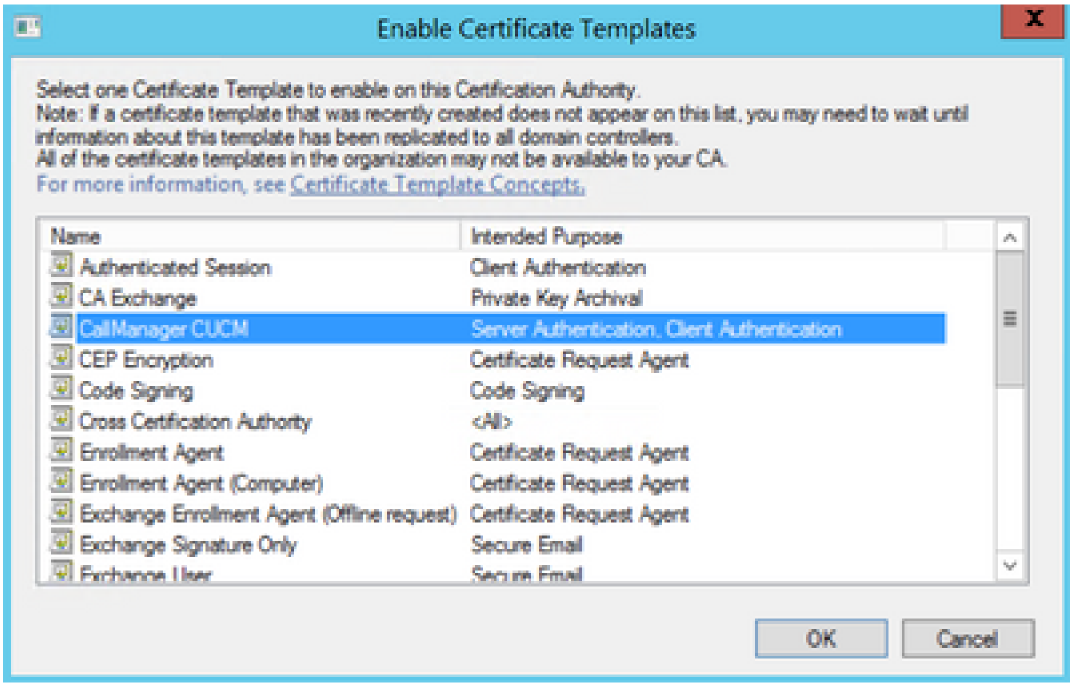
Stap 8. Sluit het venster **Certificaatsjabloon console** en navigeer in het allereerste venster naar **Nieuw > Certificaatsjabloon voor uitgifte**, zoals in de afbeelding.



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

Creates a new item in this container.

Stap 9. Selecteer de nieuwe **CallManager CUCM-**sjabloon en selecteer **OK**, zoals in de afbeelding.



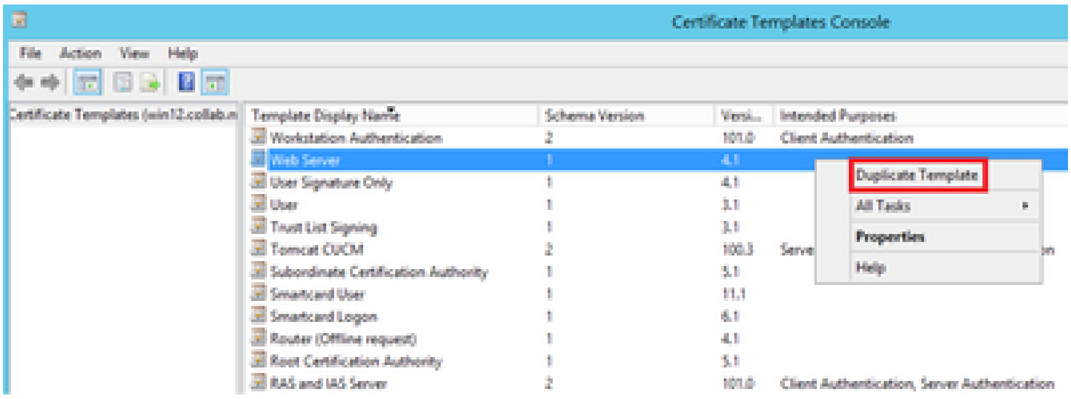
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates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

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

Stap 10. Herhaal alle vorige stappen om certificaatsjablonen te maken voor de Tomcat- en TVS-services zoals nodig.

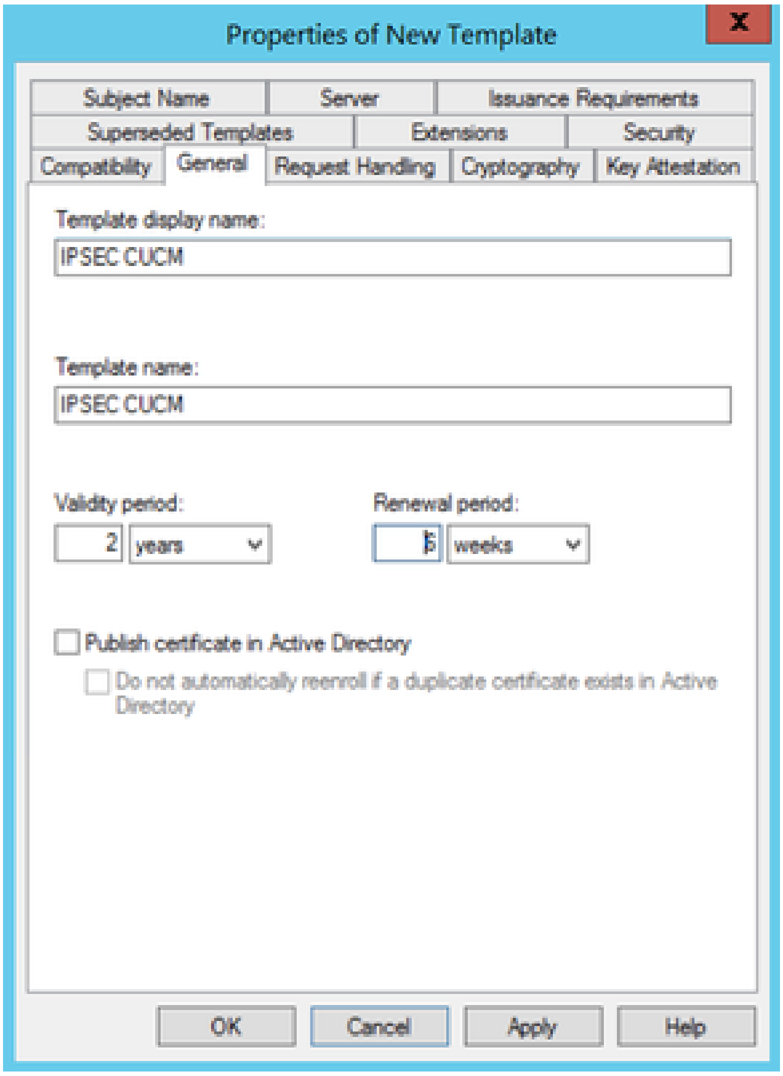
IPsec-sjabloon

Stap 1. Vind de **Web Server** sjabloon, klik met de rechtermuisknop op het en selecteer **Duplicate Template**, zoals in de afbeelding.


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

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

Stap 2. Onder **Algemeen**, kunt u de naam van het certificaatmalplaatje, de vertoningsnaam, geldigheid, enz. veranderen.



Template display name: IPSEC CUCM

Template name: IPSEC CUCM

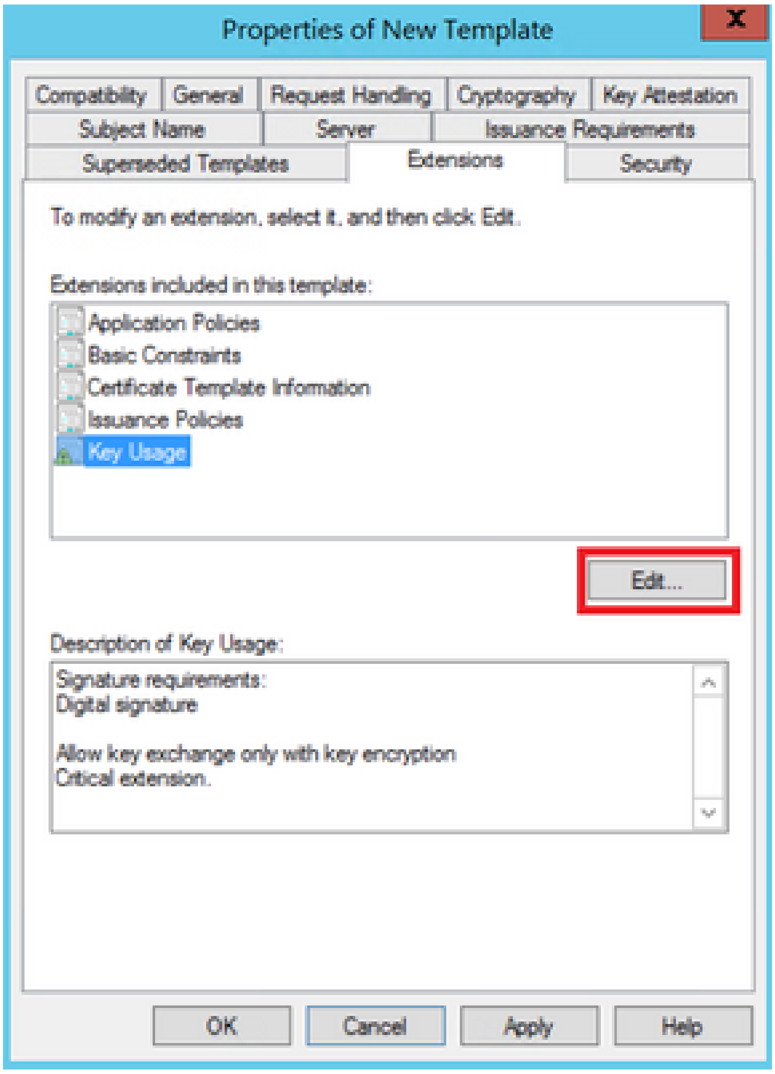
Validity period: 2 years

Renewal period: 6 weeks

☐ Publish certificate in Active Directory

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

Stap 3. Navigeer naar **Uitbreidingen > Hoofdgebruik > Bewerken**, zoals in de afbeelding wordt getoond.



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

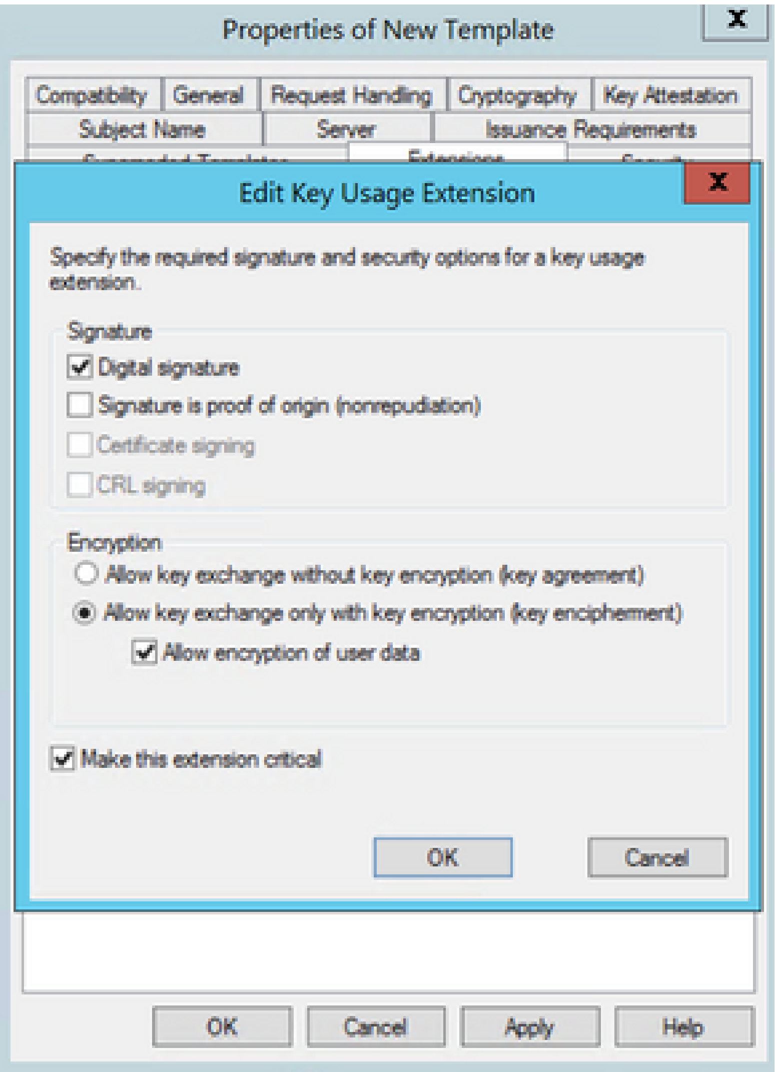
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Stap 4. Selecteer deze opties en selecteer **OK**, zoals in de afbeelding.

- **Digitale handtekening**
- **Toetsuitwisseling alleen toestaan met sleutelcodering (sleutelcodering)**
- **Versleuteling van gebruikersgegevens toestaan**



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

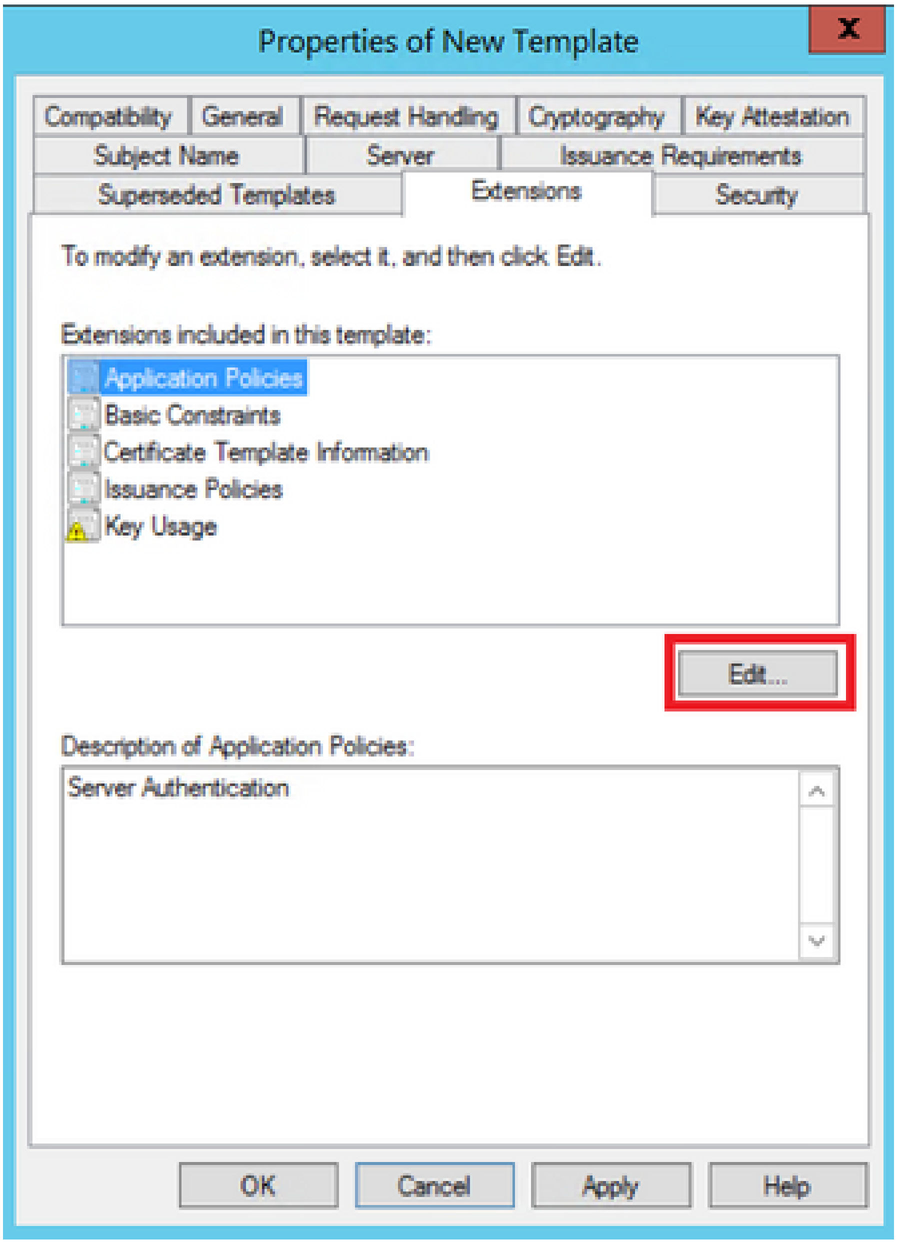
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

Stap 5. Navigeer naar **Uitbreidingen > Toepassingsbeleid > Bewerken > Toevoegen**, zoals in de afbeelding.



Properties of New Template

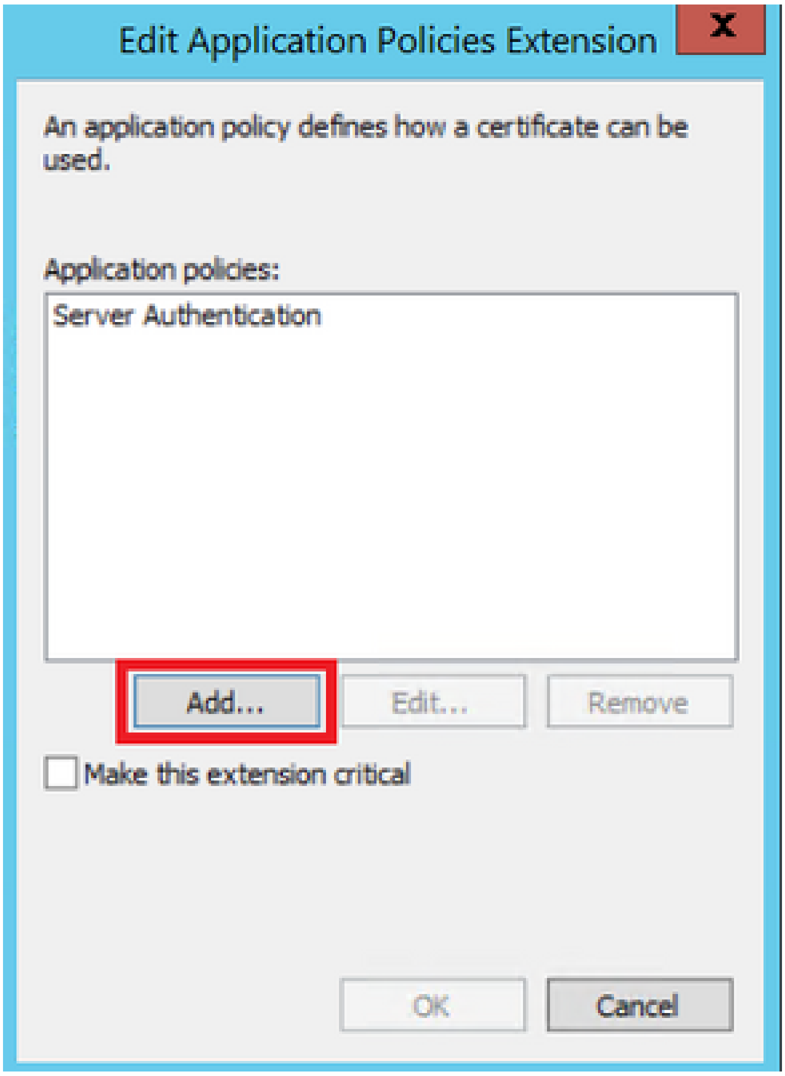
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



Edit Application Policies Extension

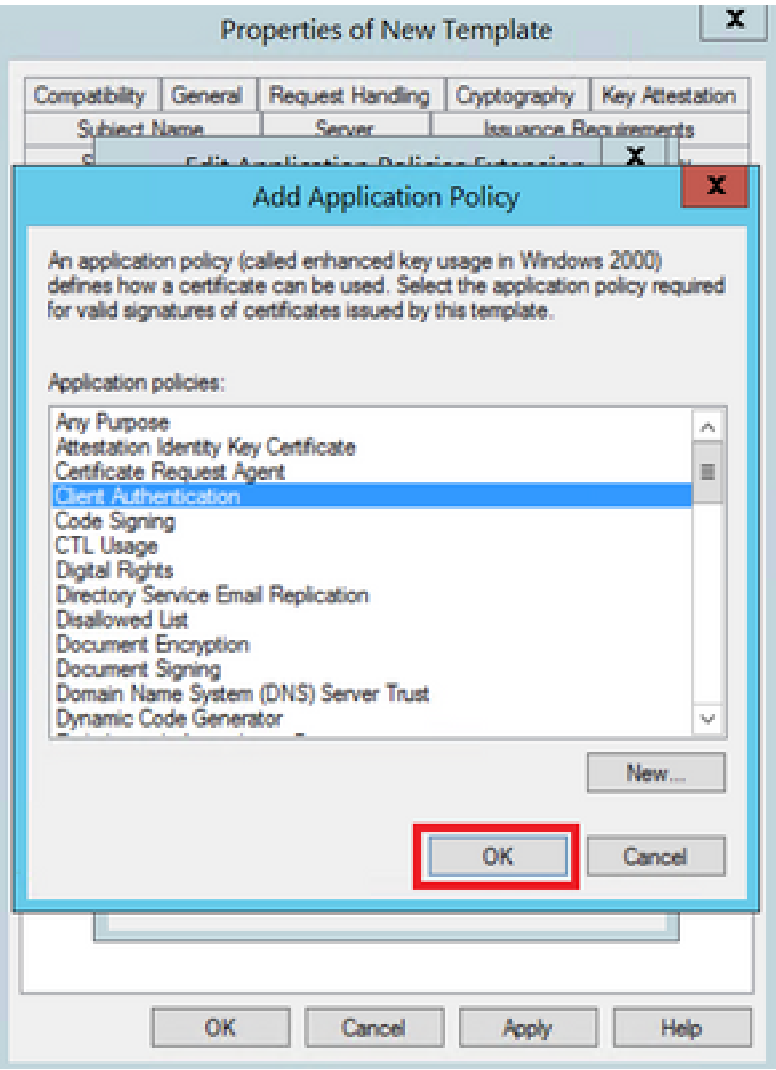
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

Stap 6. Zoek naar **Clientverificatie,** selecteer deze en **klik** op **OK**, zoals in de afbeelding.

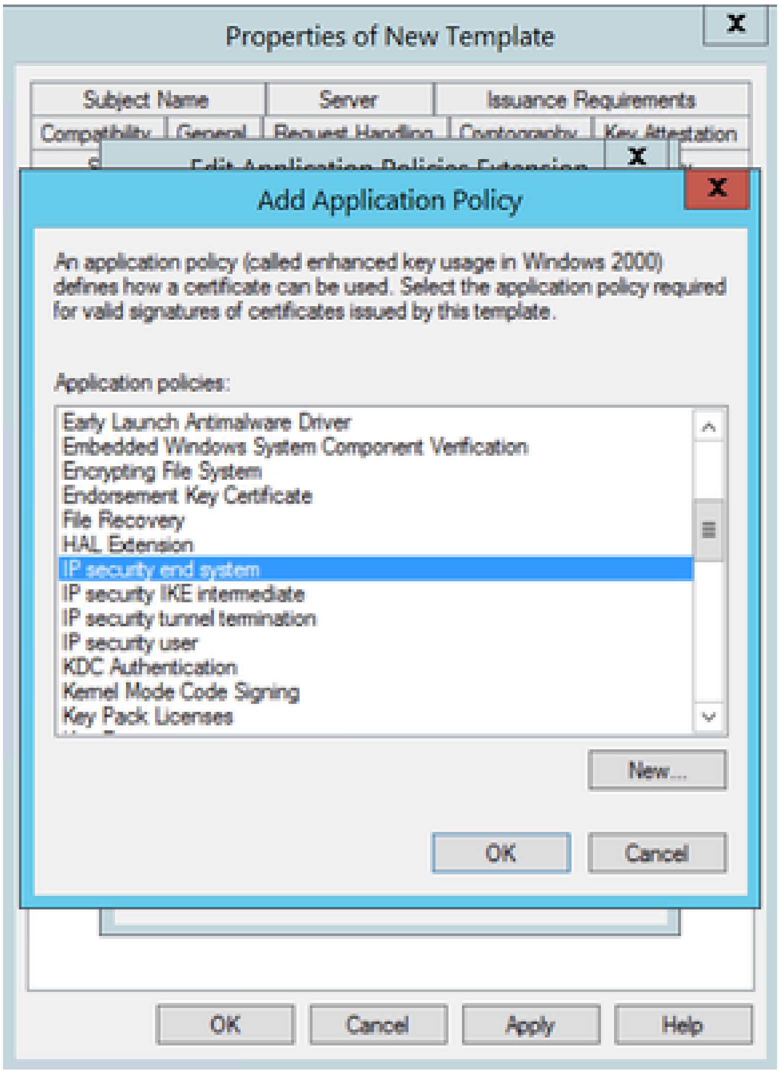


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Stap 7. Selecteer **Add** again, zoek naar **IP security eindsysteem**, selecteer het en selecteer vervolgens **OK** op dit en op het vorige venster.

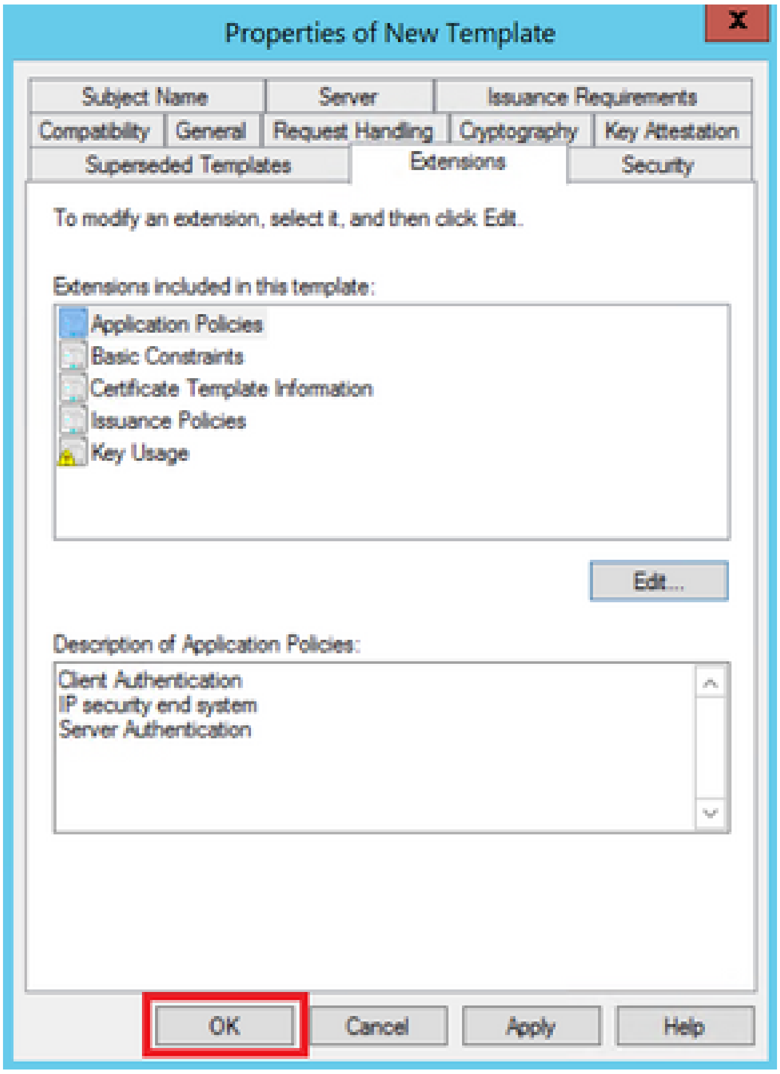


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Stap 8. Terug op de sjabloon selecteert u **Toepassen** en vervolgens **OK**, zoals in de afbeelding.



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

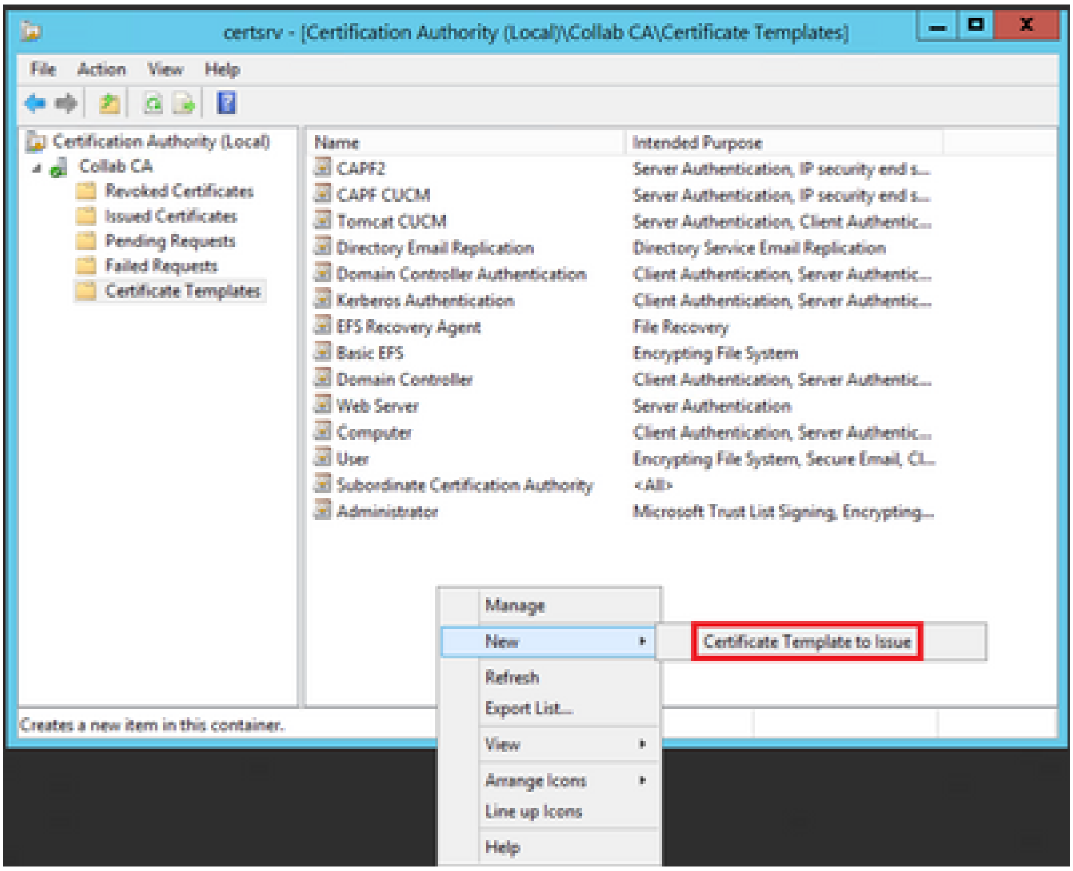
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
IP security end system
Server Authentication

Stap 9. Sluit het venster **Certificaatsjablonen console** en ga terug in het allereerste venster, navigeer naar **Nieuw > Certificaatsjabloon om uit te geven**, zoals in de afbeelding.

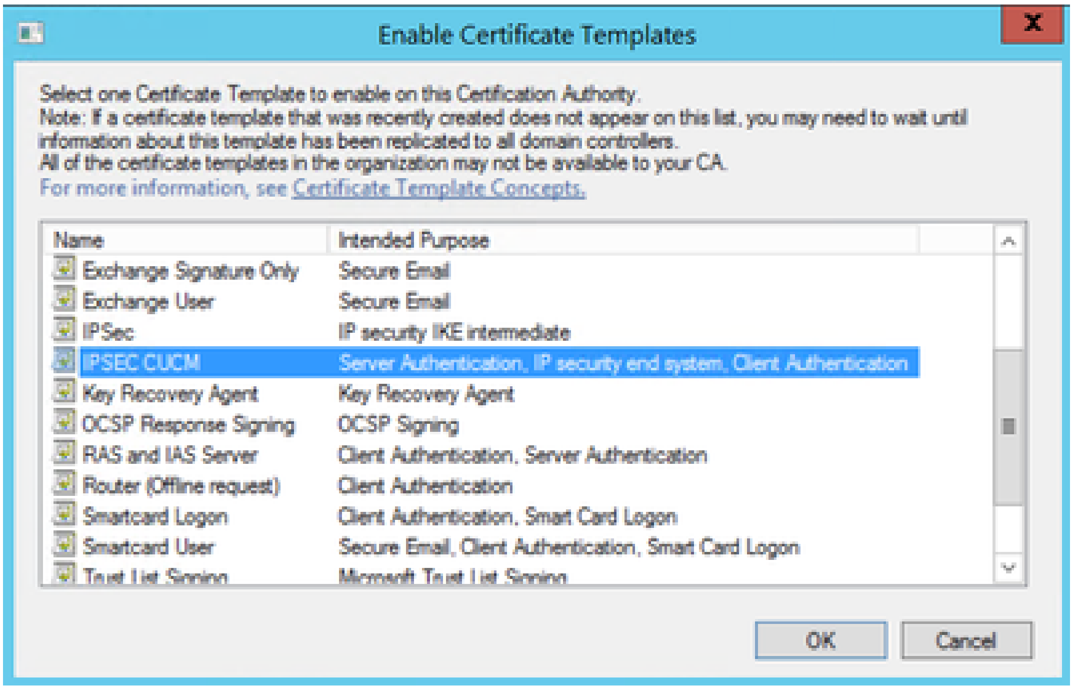


certsrv - [Certification Authority (Local)\Collab CA\Certificate Templates]

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

Creates a new item in this container.

Stap 10. Selecteer de nieuwe **IPSEC CUCM-**sjabloon en selecteer op **OK**, zoals in de afbeelding.



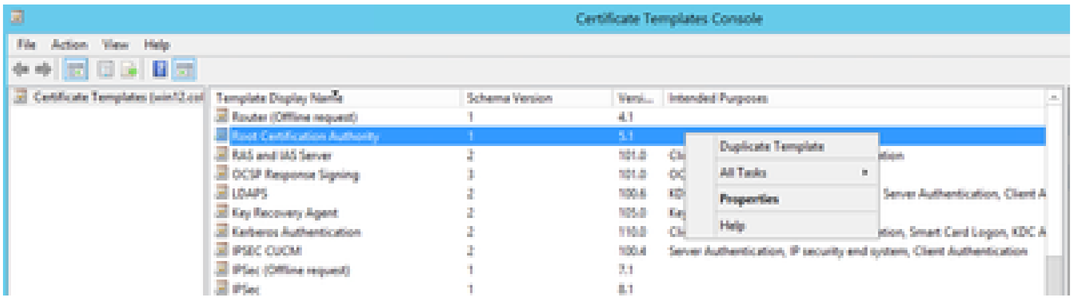
Enable Certificate Templates

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

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

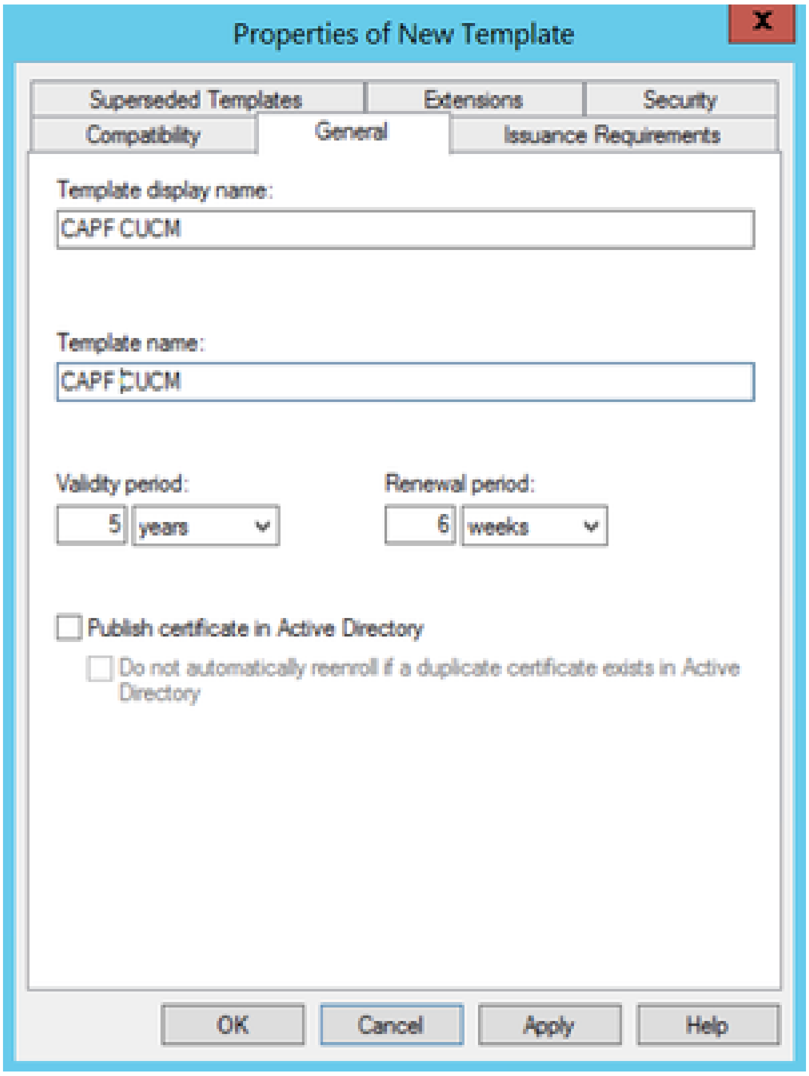
CAPF-sjabloon

Stap 1. Zoek de **Root CA-**sjabloon en klik er met de rechtermuisknop op. Selecteer vervolgens **Sjabloon dupliceren**, zoals in de afbeelding.


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

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

Stap 2. Onder **Algemeen**, kunt u de naam van het certificaatmalplaatje, de vertoningsnaam, geldigheid, enz. veranderen.



Template display name: CAPF CUCM

Template name: CAPF CUCM

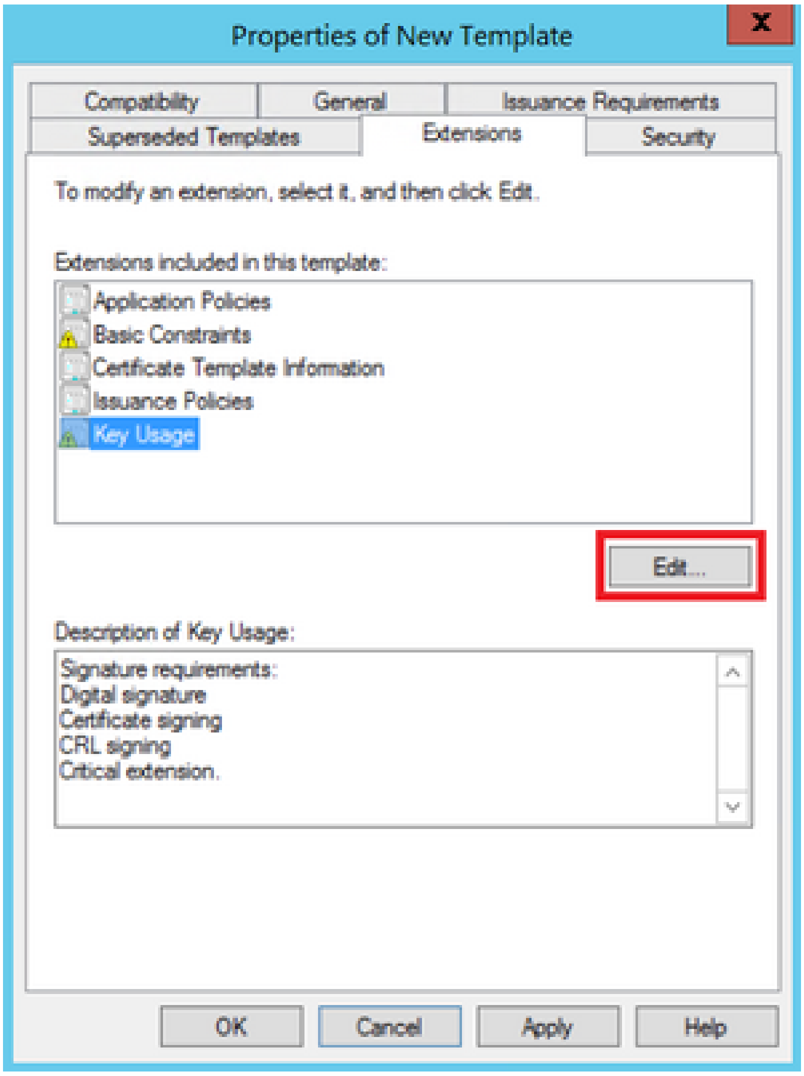
Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

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

Stap 3. Navigeer naar **Uitbreidingen > Hoofdgebruik > Bewerken**, zoals in de afbeelding wordt getoond.



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

Extensions included in this template:

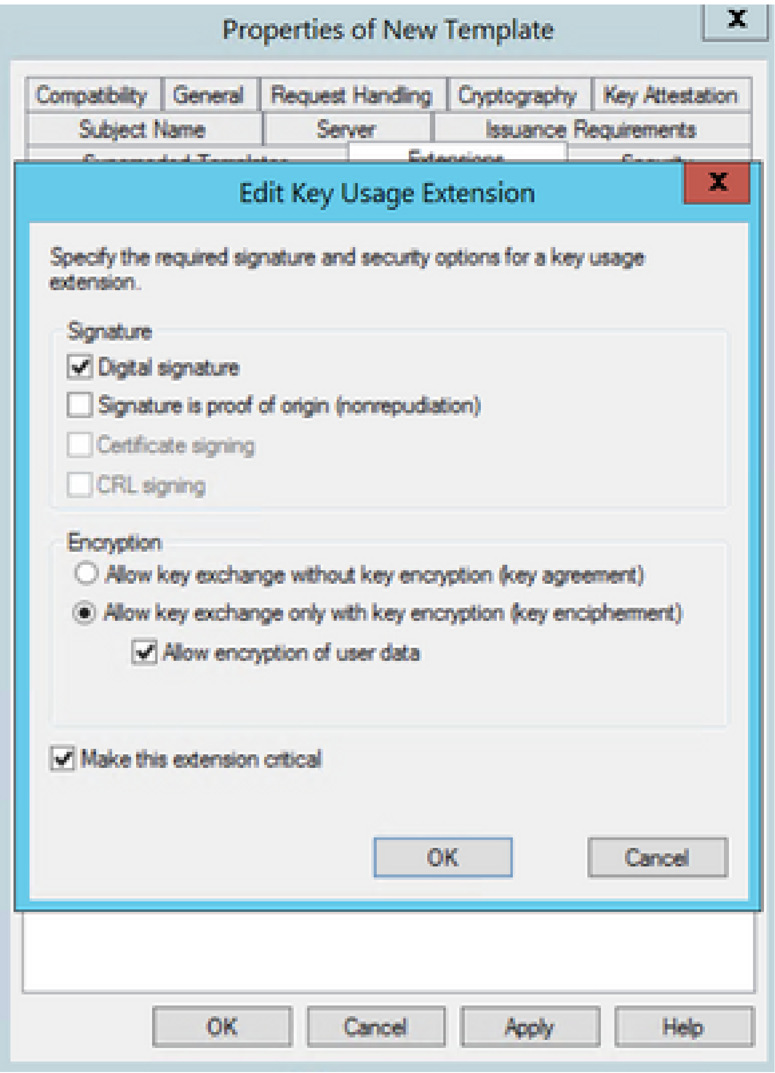
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Key Usage:

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

Stap 4. Selecteer deze opties en selecteer **OK**, zoals in de afbeelding.

- **Digitale handtekening**
- **Certificaatondertekening**
- **CRL-ondertekening**



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

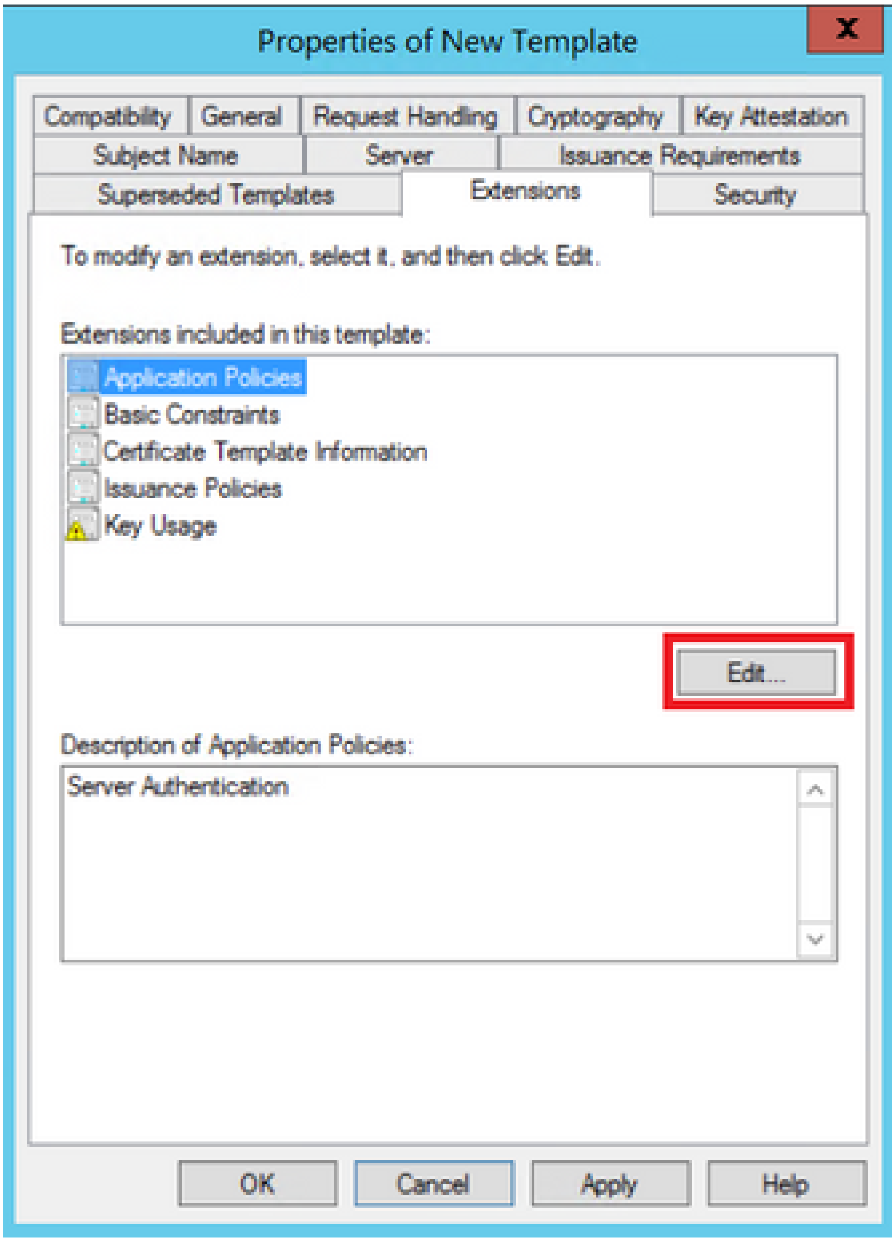
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

Stap 5. Navigeer naar **Uitbreidingen > Toepassingsbeleid > Bewerken > Toevoegen**, zoals in de afbeelding.



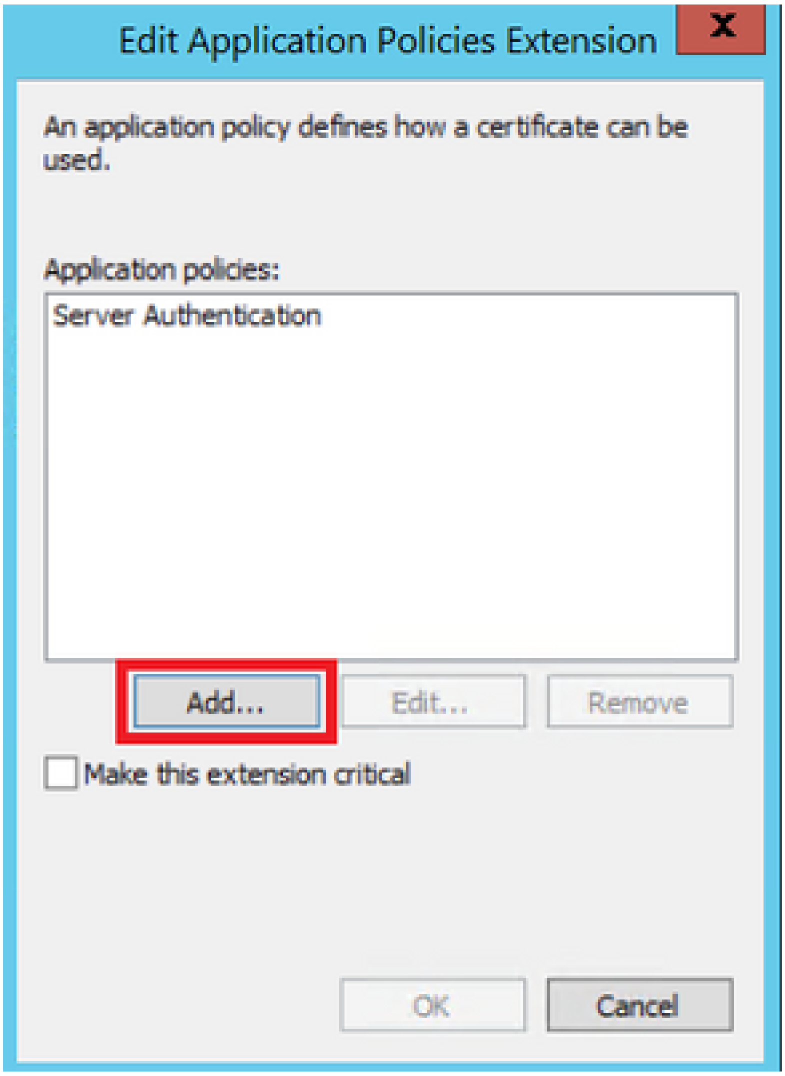
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



Edit Application Policies Extension

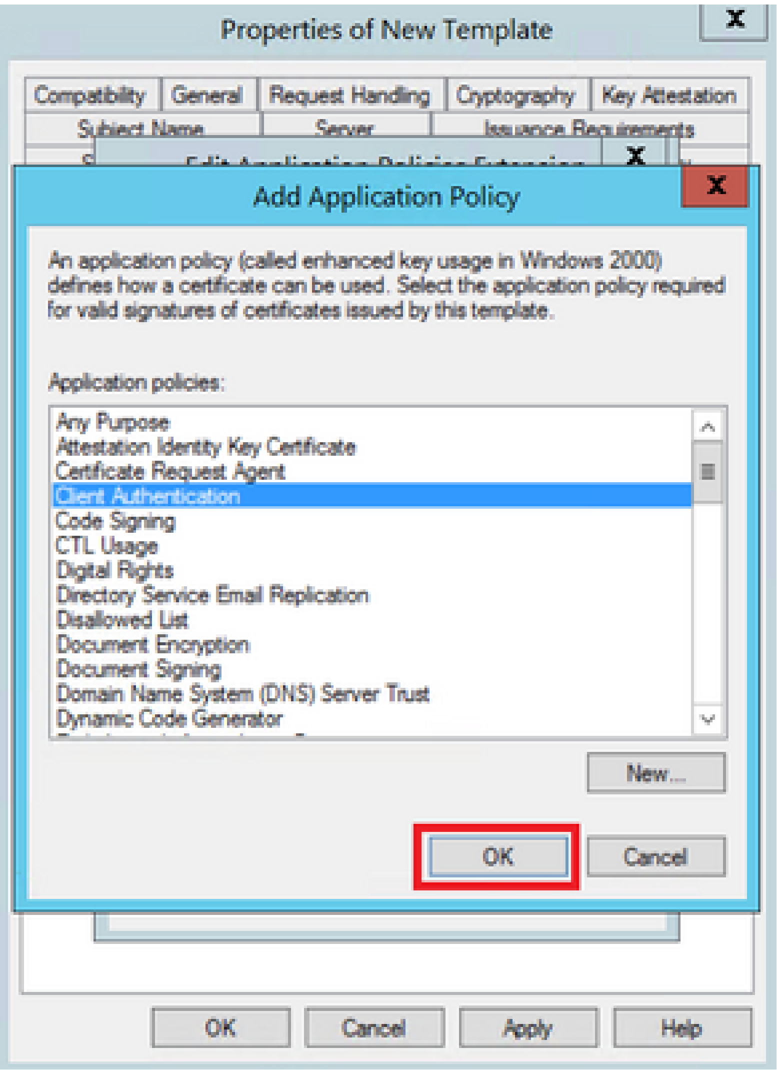
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

Stap 6. Zoek naar **clientverificatie,** selecteer deze en selecteer vervolgens **OK**, zoals in de afbeelding.



Properties of New Template

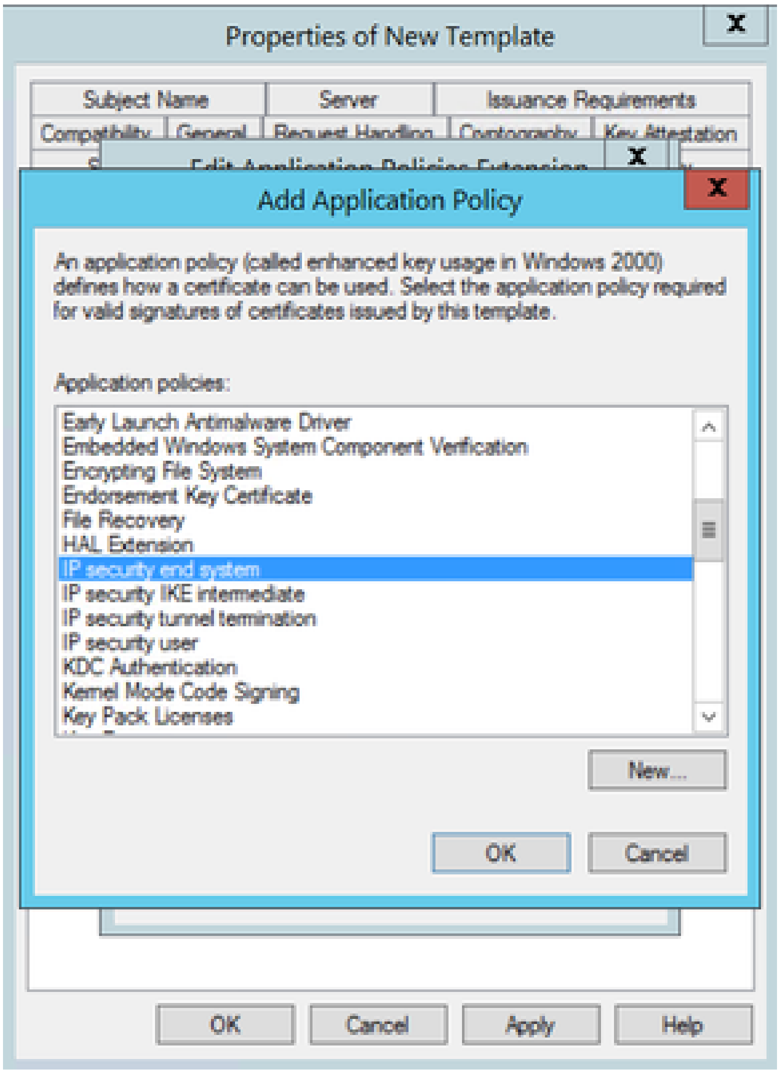
Add Application Policy

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

Stap 7. Selecteer **Add** again, zoek naar **IP security eindsysteem**, selecteer het en selecteer vervolgens OK op dit en op het vorige venster, zoals weergegeven in de afbeelding.

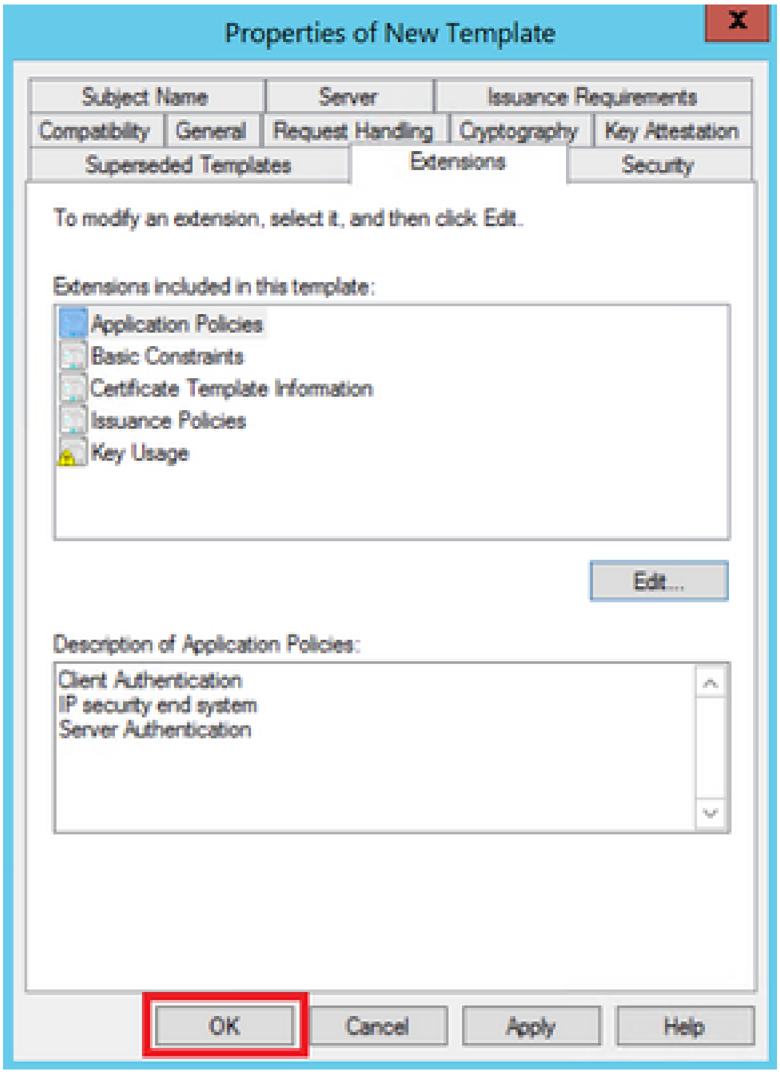


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

Stap 8. Terug op de sjabloon selecteert u **Toepassen** en vervolgens **OK**, zoals in de afbeelding.



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

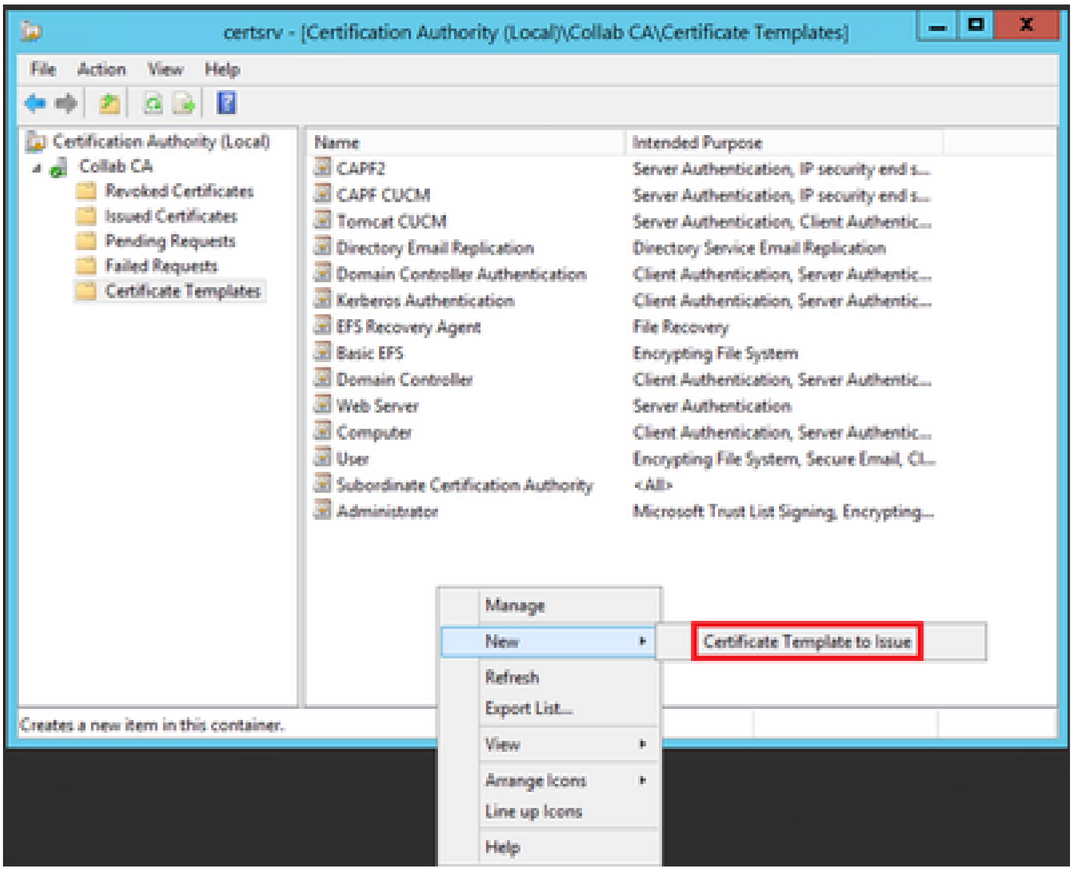
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
IP security end system
Server Authentication

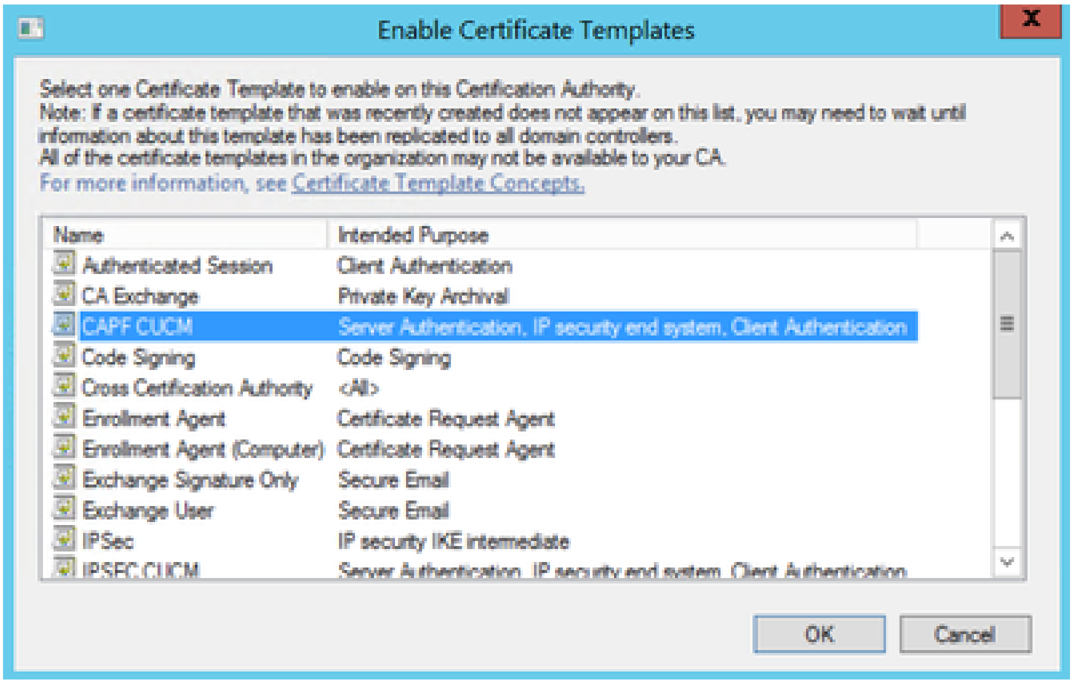
Stap 9. Sluit het venster **Certificaatsjablonen console** en ga terug in het allereerste venster, navigeer naar **Nieuw > Certificaatsjabloon om uit te geven**, zoals in de afbeelding.



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

Creates a new item in this container.

Stap 10. Selecteer de nieuwe **CAPF CUCM-**sjabloon en selecteer **OK**, zoals in de afbeelding.



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

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

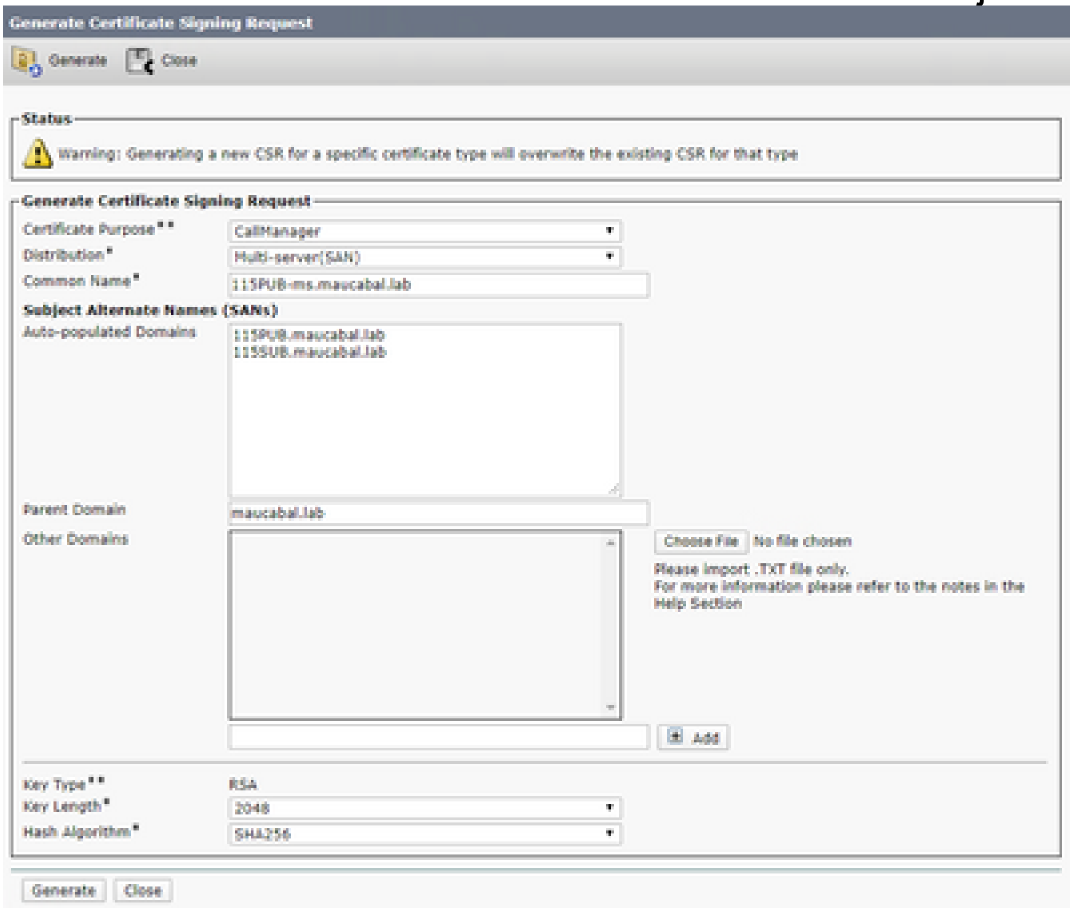
Een aanvraag voor certificaatondertekening genereren

Gebruik dit voorbeeld om een CallManager-certificaat te genereren met behulp van de nieuwe sjablonen. Dezelfde procedure kan worden gebruikt voor elk certificaat type, je hoeft alleen het certificaat en de sjabloon typen dienovereenkomstig te selecteren:

Stap 1. Op CUCM, navigeer naar **OS Administratie > Beveiliging > Certificaatbeheer > Generate CSR**.

Stap 2. Selecteer deze opties en selecteer **Generate**, zoals in de afbeelding.

- Certificaatdoel: **CallManager**
- Distributie: **<Dit kan alleen voor één server of meerdere SAN's zijn>**



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

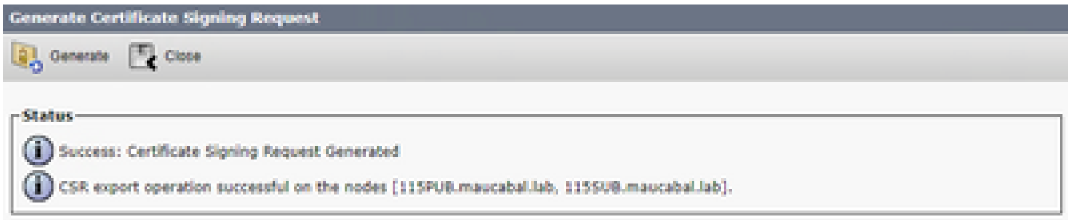
Subject Alternate Names (SANs)

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

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

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

Stap 3. Er wordt een bevestigingsbericht gegenereerd, zoals in de afbeelding wordt weergegeven.

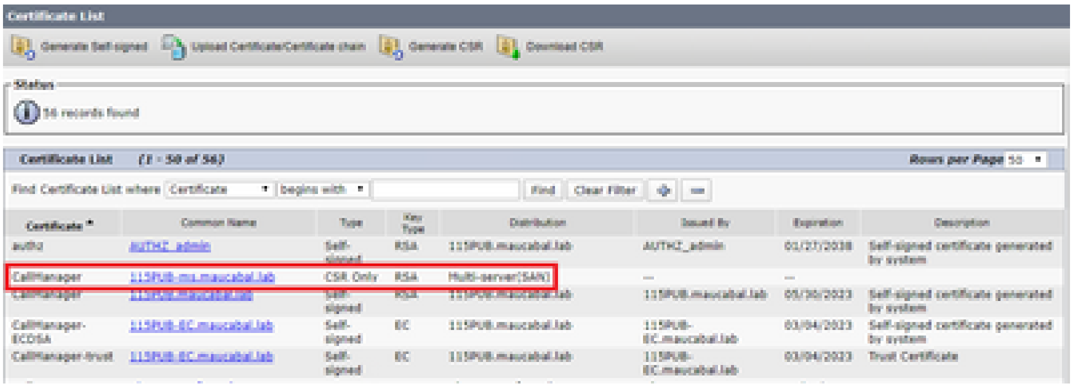


Status

ⓘ Success: Certificate Signing Request Generated

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

Stap 4. Zoek in de certificaatlijst het item met **alleen** type **CSR** en selecteer het, zoals in de afbeelding.



Status

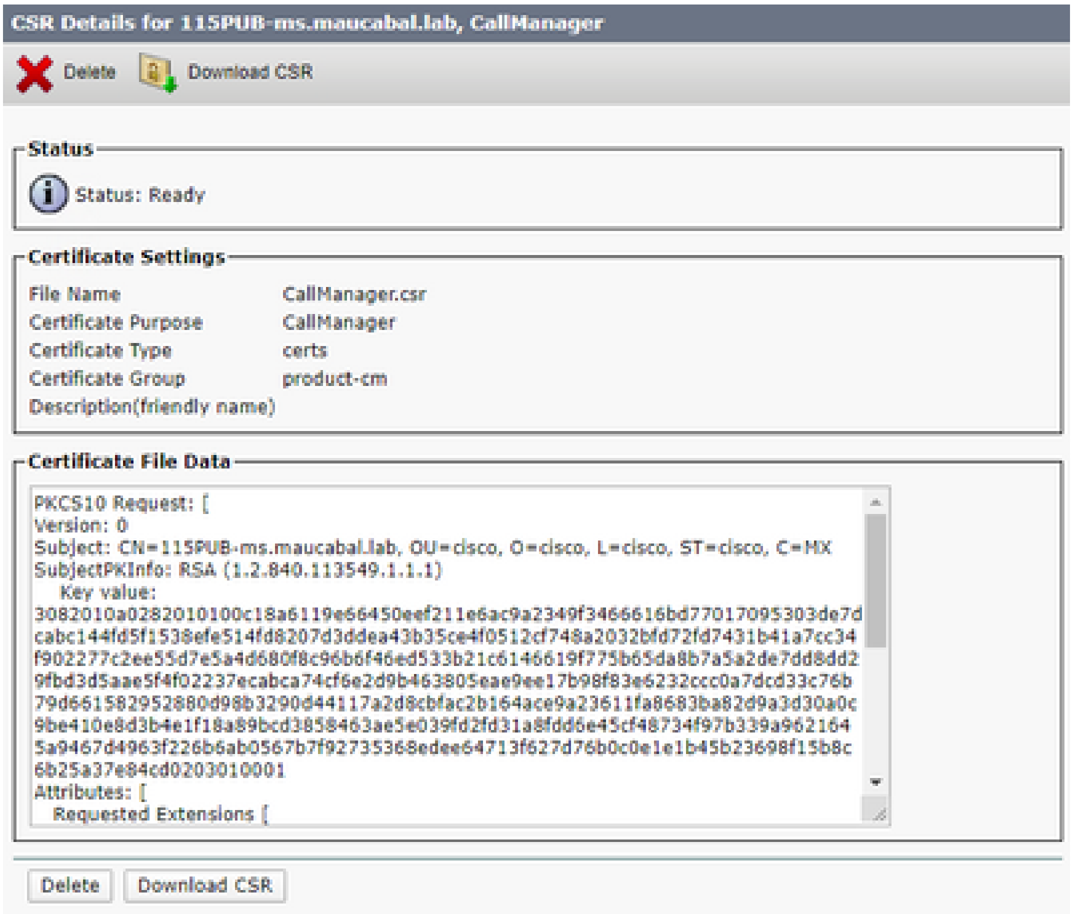
ⓘ 56 records found

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

Find Certificate List where Certificate begins with

Certificate ▲	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_admin	Self-signed	RSA	115PUB.maucabal.lab	AUTHZ_admin	01/27/2038	Self-signed certificate generated by system
CallManager	115PUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(SAN)	--	--	
CallManager	115PUB.maucabal.lab	Self-signed	RSA	115PUB.maucabal.lab	115PUB.maucabal.lab	05/30/2023	Self-signed certificate generated by system
CallManager-ECDSA	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	03/04/2023	Self-signed certificate generated by system
CallManager-trust	115PUB-EC.maucabal.lab	Self-signed	EC	115PUB.maucabal.lab	115PUB-EC.maucabal.lab	03/04/2023	Trust Certificate

Stap 5. Selecteer in het pop-upvenster **Download CSR** en sla het bestand op uw computer op.



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

Status

Status: Ready

Certificate Settings

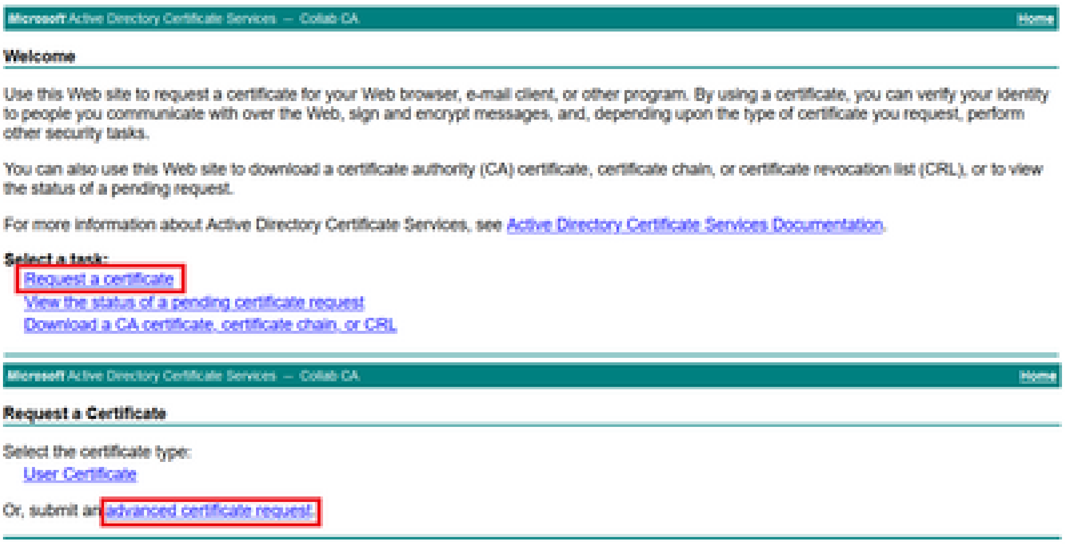
File Name	CallManager.csr
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	

Certificate File Data

```
PKCS10 Request: [
Version: 0
Subject: CN=115PUB-ms.maucabal.lab, OU=cisco, O=cisco, L=cisco, ST=cisco, C=MX
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)
   Key value:
3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d
cabc144fd5f1538efe514fd8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34
f902277c2ee55d7e5a4d680f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2
9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b
79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c
9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164
5a9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c
6b25a37e84cd0203010001
Attributes: [
  Requested Extensions [
```

Stap 6. Navigeer in uw browser naar deze URL en voer uw domeincontroller-beheerder aanmeldingsgegevens in: **https://<yourWindowsServerIP>/certsrv/.**

Stap 7. Navigeer naar **Certificaat aanvragen > Geavanceerd certificaatverzoek**, zoals in de afbeelding.



Microsoft Active Directory Certificate Services -- Collab CA

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

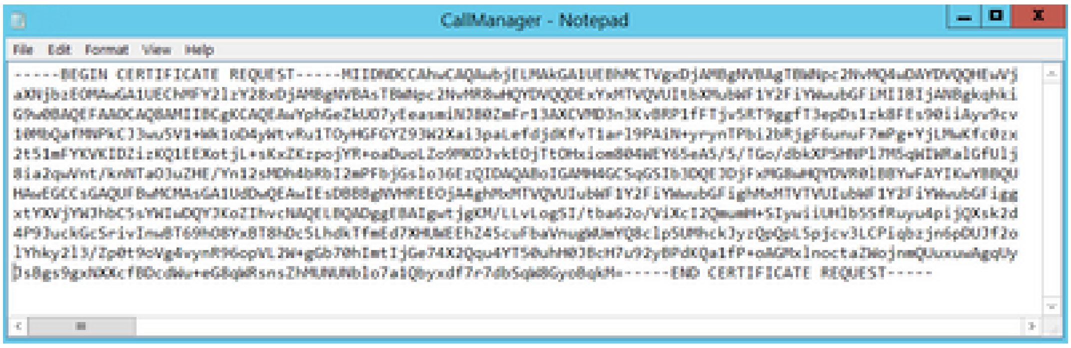
Microsoft Active Directory Certificate Services -- Collab CA

Request a Certificate

Select the certificate type:
User Certificate

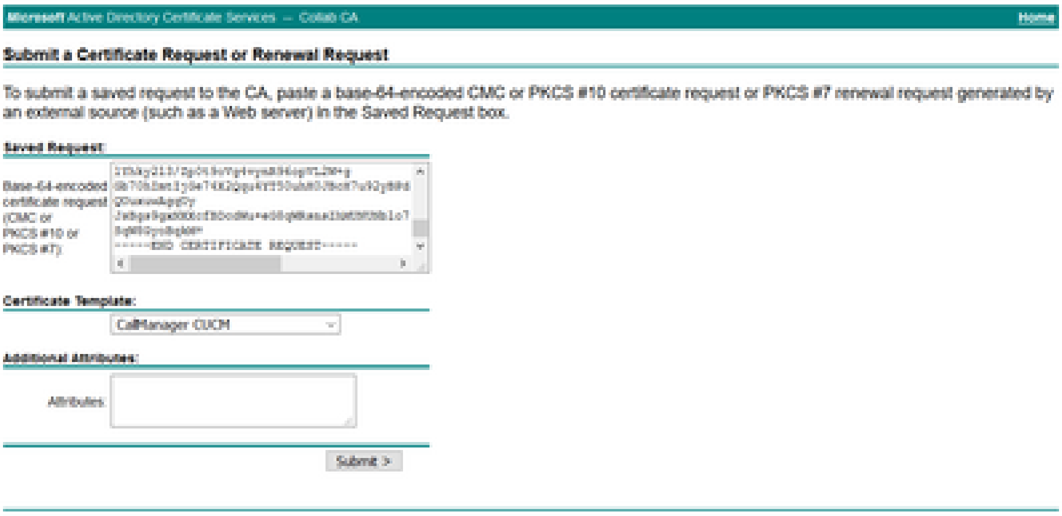
Or, submit an advanced certificate request.

Stap 8. Open het CSR-bestand en kopieer alle inhoud:



```
-----BEGIN CERTIFICATE REQUEST-----MIIDNDCCAhwCAQAwbjELMAkGA1UEBhMCTVgxDjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVj
aXNjbzEOMAwGA1UEChMFY2lzY28xDjAMBgNVBAsTBWNpc2NvMR8wHQYDVQQDExYxMTVQVUItbXMubWF1Y2FiYWwubGFiMIIBIjANBgkqhki
G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYphGeZkUO7yEeasmiN380ZmFr13AXCVMD3n3KvBRP1fFTjv5RT9ggfT3epDs1zk8FEs90iiAyv9cv
10MbQafMNPkCJ3wuSV1+Wk1oD4yWtvRu1TOyHGFGYZ93W2Xai3paLefdjdKfvT1ar19PAiN+yrynTPbi2bRjgF6unuF7mPg+YjLMwKfc0zx
2t51mFYKVKIDZizKQ1EEXotjL+sKxZKzpojYR+oaDuoLZo9MKDJvkEOjTtOHxiom804WEY65eA5/5/TGo/dbkXP5HNP17M5qWIWRalGfUlj
8ia2quWnt/knNTaO3uZHE/Yn12sMDh4bRbI2mPFbjGslo36EzQIDAQABoIGAMH4GCSqGSIb3DQEJDjFxMG8wHQYDVR0lBBYwFAYIKwYBBQU
HAwEGCCsGAQUFBwMCMAsGA1UdDwQEAwIEsDBBBgNVHREEOjA4ghMxMTVQVUIubWF1Y2FiYWwubGFighMxMTVTVUIubWF1Y2FiYWwubGFigg
xtYXVjYWJhbC5sYWIwDQYJKoZIhvcNAQELBQADggEBAIgwtjgKM/LLvLogSI/tba62o/ViXcI2QmumH+SIywiiUHIb5SfRuyu4pijQXsk2d
4P9JuckGcSrivInwBT69hO8YxBT8hDc5LhdkTfmEd7XHWWEEhZ45cuFbaVnugWUmYQ8clp5UMhckJyzQpQpL5pjcv3LCPiqbzjn6pDUJf2o
lYhky2l3/Zp0t9oVg4vynR96opVL2W+gGb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPdKQa1fP+oAGMxlnoctaZWojnmQUuxuwAgqUy
Ds8gs9gxNXXcfBDcdWu+eG8qWRsnsZhMUWUNblo7alQbyxdf7r7dbSqW8GyoBqkM=-----END CERTIFICATE REQUEST-----
```

Stap 9. Plakt de CSR op het veld **voor het certificaatverzoek met Base-64-encodering**. Selecteer onder **certificaatsjabloon** de juiste sjabloon en selecteer **Indienen**, zoals in de afbeelding.


Microsoft Active Directory Certificate Services -- Collab CA
Home

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
lYhky2l3/Zp0t9oVg4vynR96opVL2W+g
Gb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPd
QUuxuwAgqUy
Ds8gs9gxNXXcfBDcdWu+eG8qWRsnsZhMUWUNblo7
alQbyxdf7r7dbSqW8GyoBqkM=
-----END CERTIFICATE REQUEST-----
```

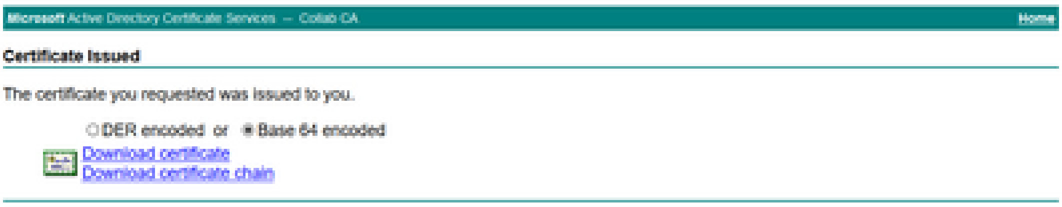
Certificate Template:

CallManager CUCM

Additional Attributes:

Attributes:

Stap 10. Tot slot selecteert u **Base 64 encoded** en **Download certificaatketen**, het gegenereerde bestand kan nu geüpload worden op de CUCM.


Microsoft Active Directory Certificate Services -- Collab CA
Home

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Verifiëren

De verificatieprocedure maakt eigenlijk deel uit van het configuratieproces.

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

Over deze vertaling