为CUCM创建Windows CA证书模板

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[Callmanager/Tomcat/TVS模板](#)
[IPsec模板](#)
[CAPF模板](#)
[生成证书签名请求](#)
[验证](#)
[故障排除](#)

简介

本文档介绍在基于Windows Server的证书颁发机构(CA)上创建证书模板的分步过程，这些证书模板符合每种类型的Cisco Unified Communications Manager(CUCM)证书的X.509扩展要求。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM 11.5(1)版或更高版本
- 建议具备Windows Server管理基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 本文档中的信息基于CUCM 11.5(1)版或更高版本。
- 安装了CA服务的Microsoft Windows Server 2012 R2。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

有五种类型的证书可由外部CA签名：

证书	使用	受影响的服务

CallManager	在安全设备注册时提供，可以签署证书信任列表(CTL)/内部信任列表(ITL)文件，用于与其他服务器(例如安全会话发起协议(SIP)中继)的安全交互。	·Cisco Call Manager ·Cisco CTI管理器 ·Cisco Tftp
tomcat	为安全超文本传输协议(HTTPS)交互提供。	·Cisco Tomcat ·单点登录(SSO) ·分机移动 ·公司目录
ipsec	用于生成备份文件，以及与媒体网关控制协议(MGCP)或H323网关的IP安全(IPsec)交互。	·Cisco DRF Master ·Cisco DRF Local
CAPF	用于生成电话的本地重要证书(LSC)。	·Cisco 证书权限代理功能
TVS	用于在电话无法验证未知证书时创建与信任验证服务(TVS)的连接。	·思科信任验证服务

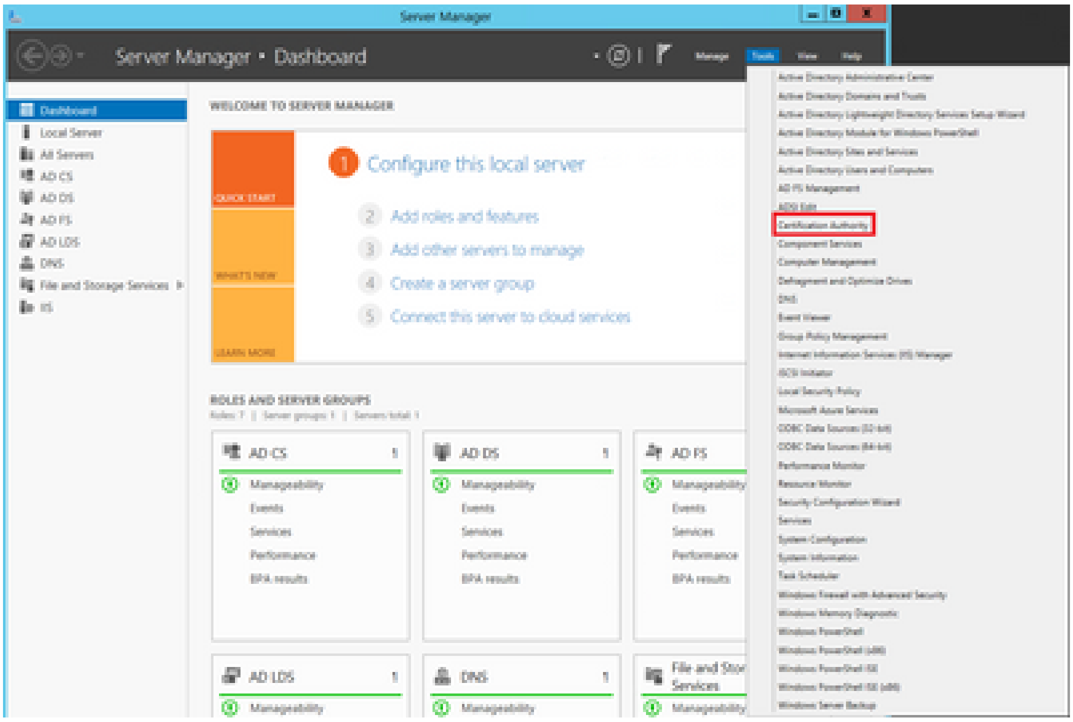
这些证书中的每一个都有一些X.509扩展要求需要设置，否则，您可能会在上述任何服务上遇到错误行为：

证书	X.509密钥用法	X.509扩展密钥用法
CallManager	·数字签名 ·密钥加密 ·数据加密	·Web服务器身份验证 ·Web客户端身份验证
tomcat	·数字签名 ·密钥加密 ·数据加密	·Web服务器身份验证 ·Web客户端身份验证
ipsec	·数字签名 ·密钥加密 ·数据加密	·Web服务器身份验证 ·Web客户端身份验证 ·IPsec终端系统
CAPF	·数字签名 ·证书签名 ·密钥加密	·Web服务器身份验证 ·Web客户端身份验证
TVS	·数字签名 ·密钥加密 ·数据加密	·Web服务器身份验证 ·Web客户端身份验证

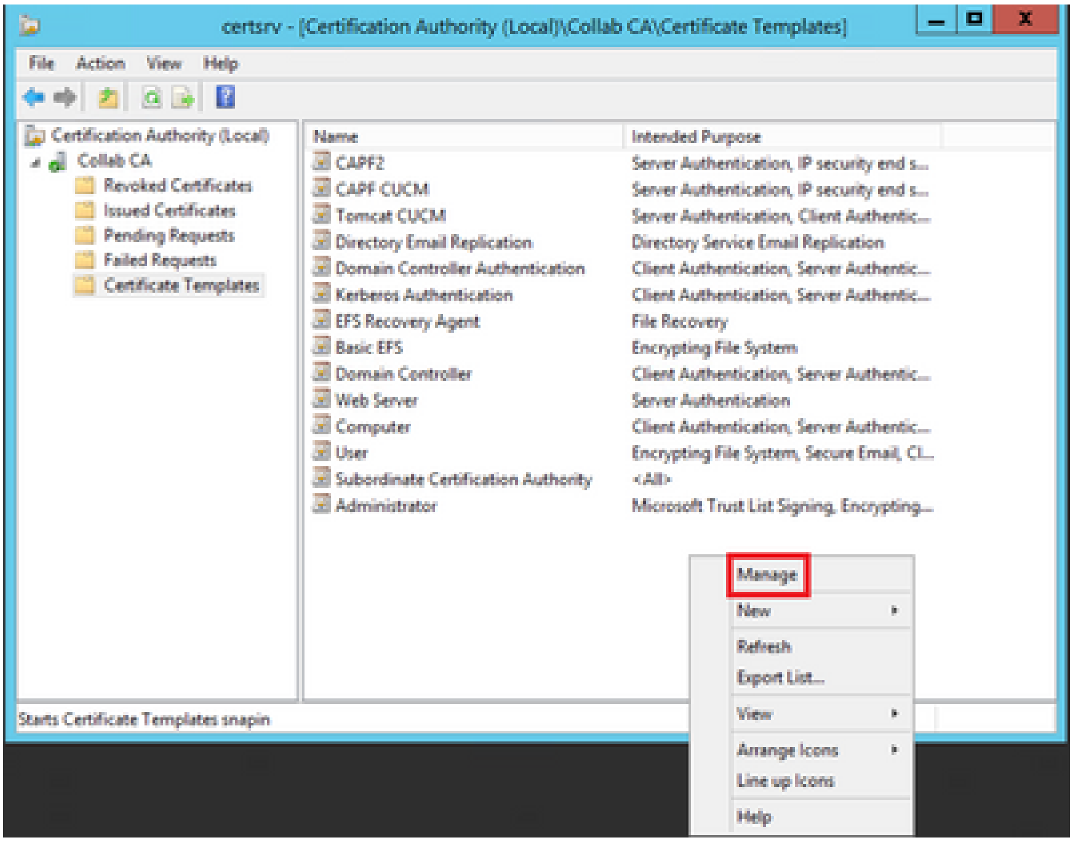
有关详细信息，请参阅思科统一通信管理器安全指南

配置

步骤1:在Windows Server上，导航到**Server Manager > Tools > Certification Authority**，如图所示。


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
Manageability
Events
Services
Performance
BPA results
AD LDS 1
DNS 1
File and Storage Services
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

第二步：选择您的CA，然后导航到**证书模板**，右键单击列表并选择**管理**，如图所示。



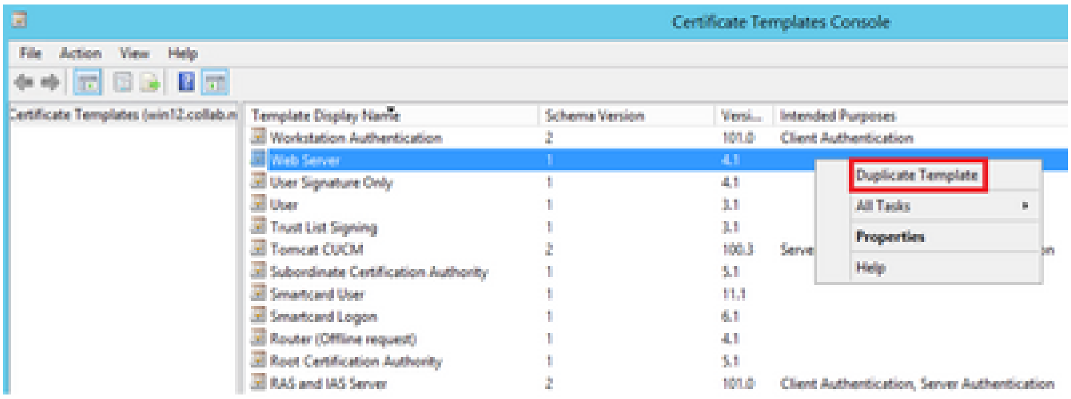
Name	Intended Purpose
CAPF2	Server Authentication, IP security end s...
CAPF CUCM	Server Authentication, IP security end s...
Tomcat CUCM	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, 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...

Starts Certificate Templates snapin

Callmanager/Tomcat/TVS模板

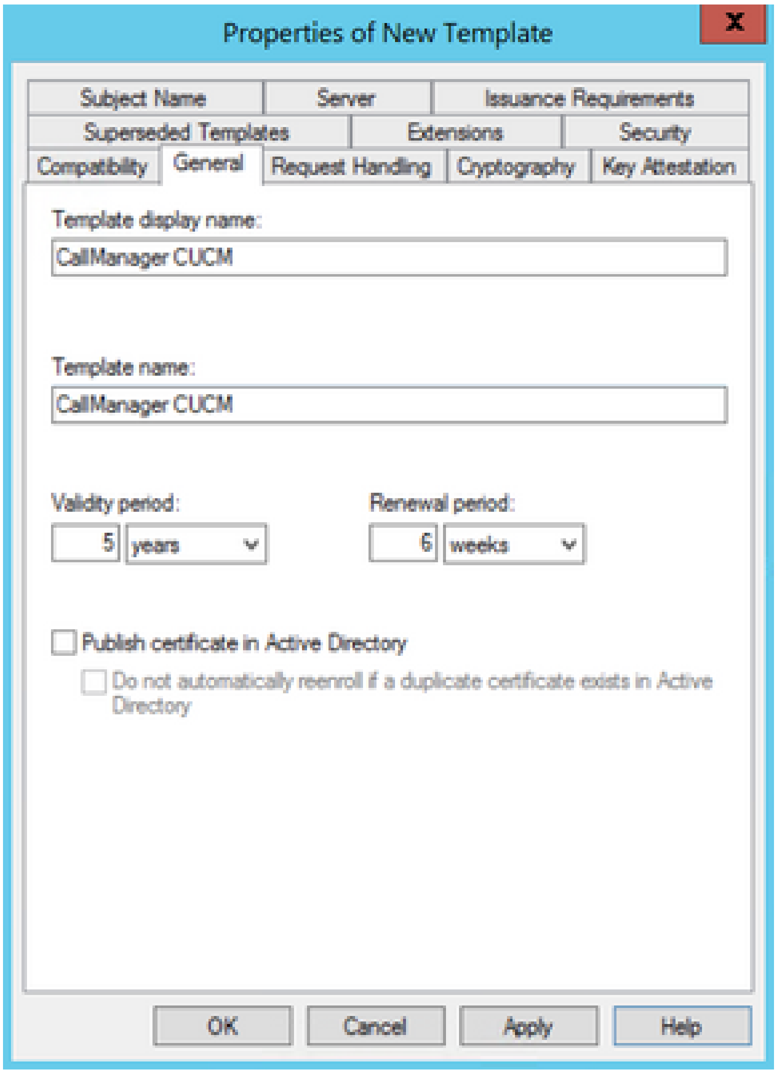
接下来的图像仅显示CallManager模板的创建；但可以按照相同的步骤为Tomcat和TVS服务创建证书模板。唯一的区别在于确保为步骤2中的每个新模板使用相应的服务名称。

步骤1:找到**Web Server**模板，右键单击该模板，然后选择**复制模板**，如图所示。


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

第二步：在General下，您可以更改证书模板的名称、显示名称、有效性等。



Template display name:
CallManager CUCM

Template name:
CallManager CUCM

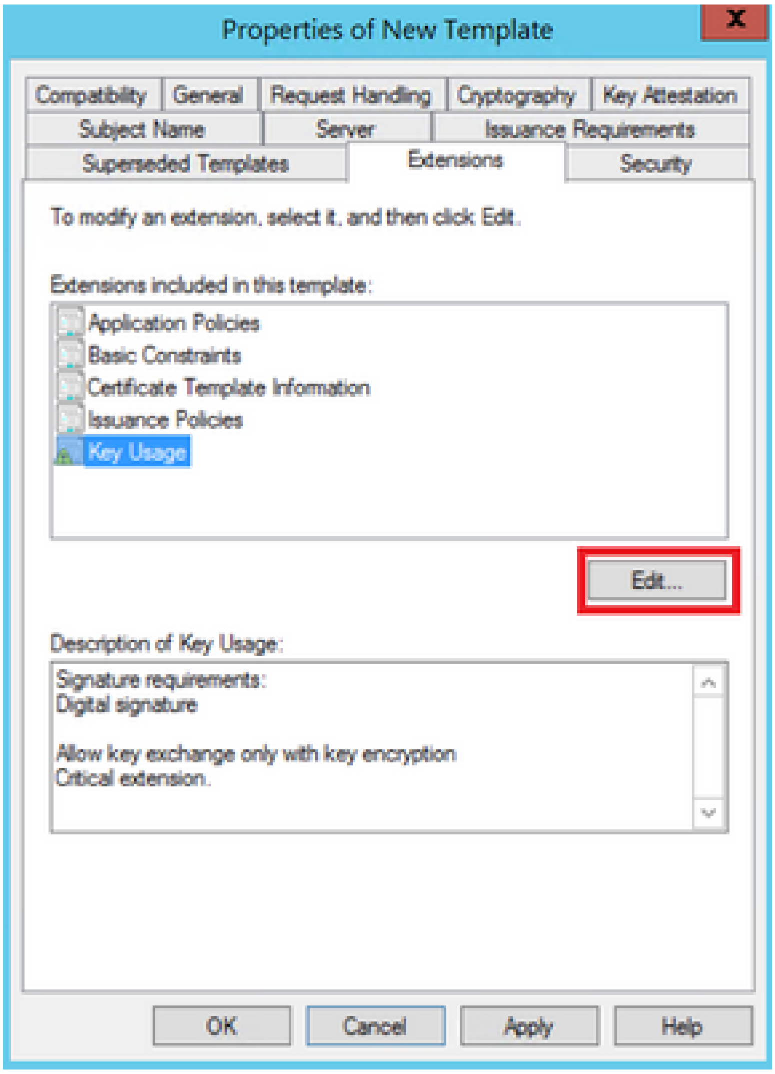
Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

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

第三步：导航到**Extensions > Key Usage > Edit**，如图所示。



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

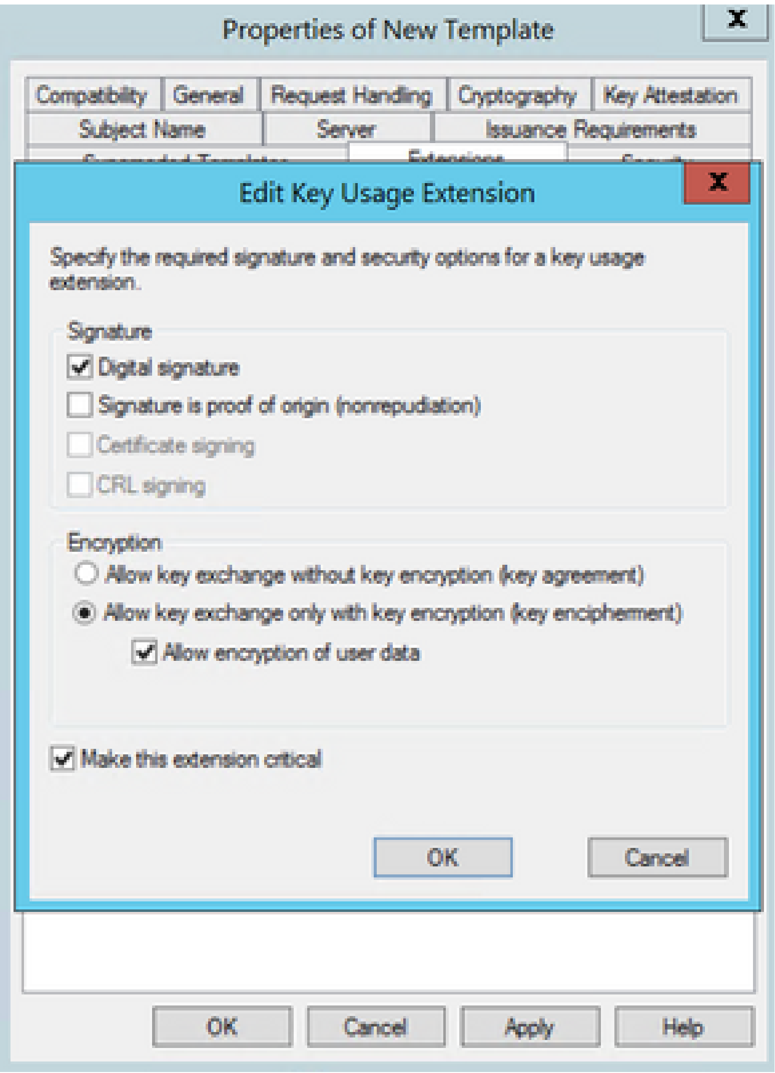
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

第四步：选择这些选项并选择OK，如图所示。

- **数字签名**
- **仅允许使用密钥加密进行密钥交换（密钥加密）**
- **允许加密用户数据**



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

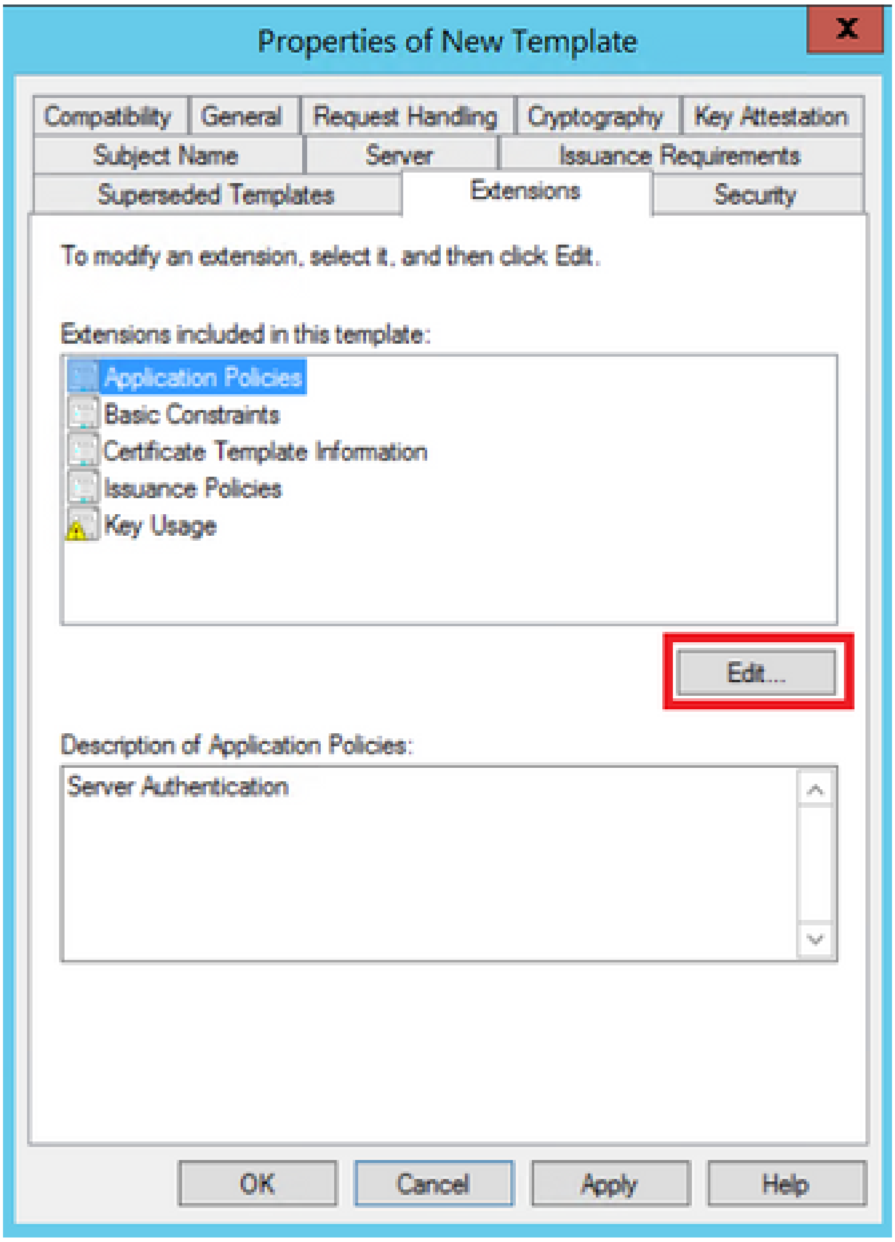
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

第五步：导航到**扩展>应用策略>编辑>添加**，如图所示。



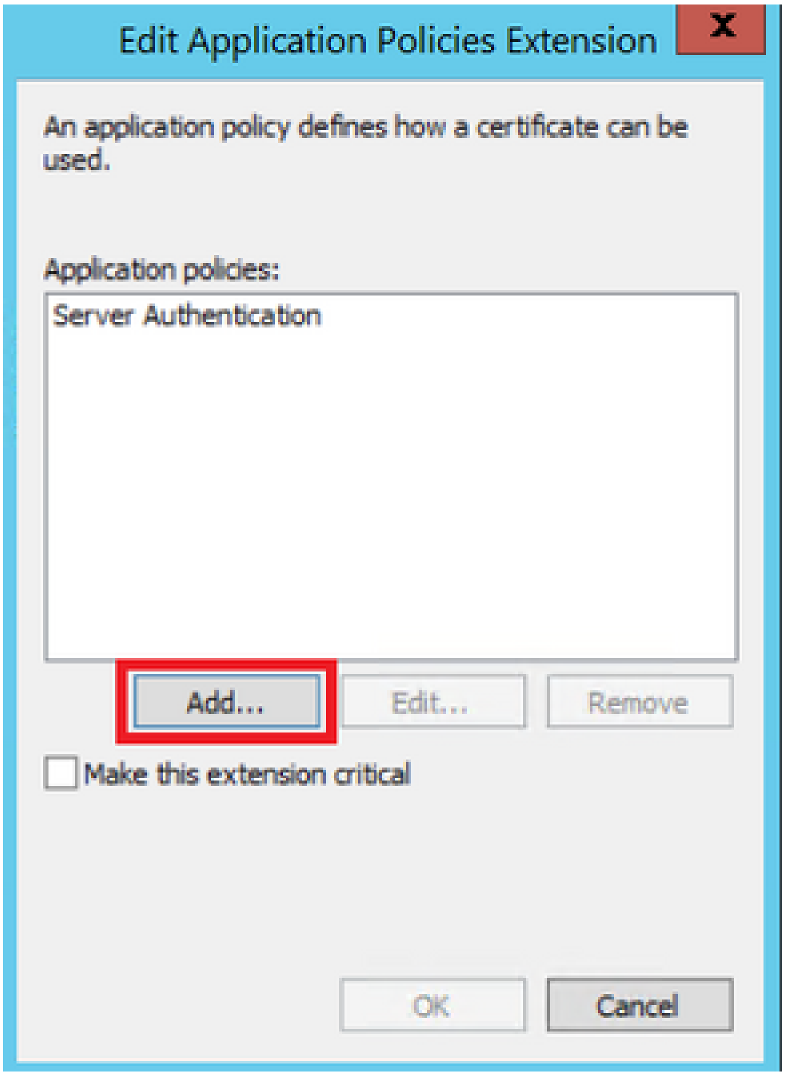
To modify an extension, select it, and then click Edit.

Extensions included in this template:

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

Description of Application Policies:

Server Authentication



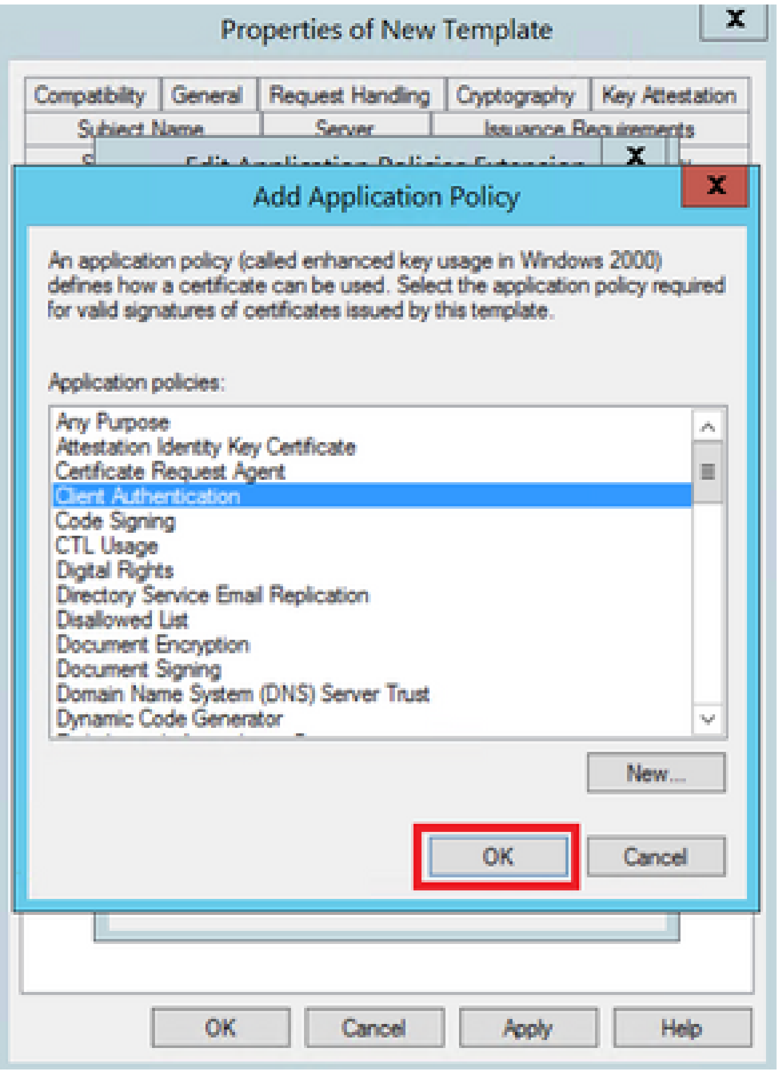
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

第六步：搜索**Client Authentication**，选择该窗口，并在该窗口和上一个窗口中选择**OK**，如图所示。

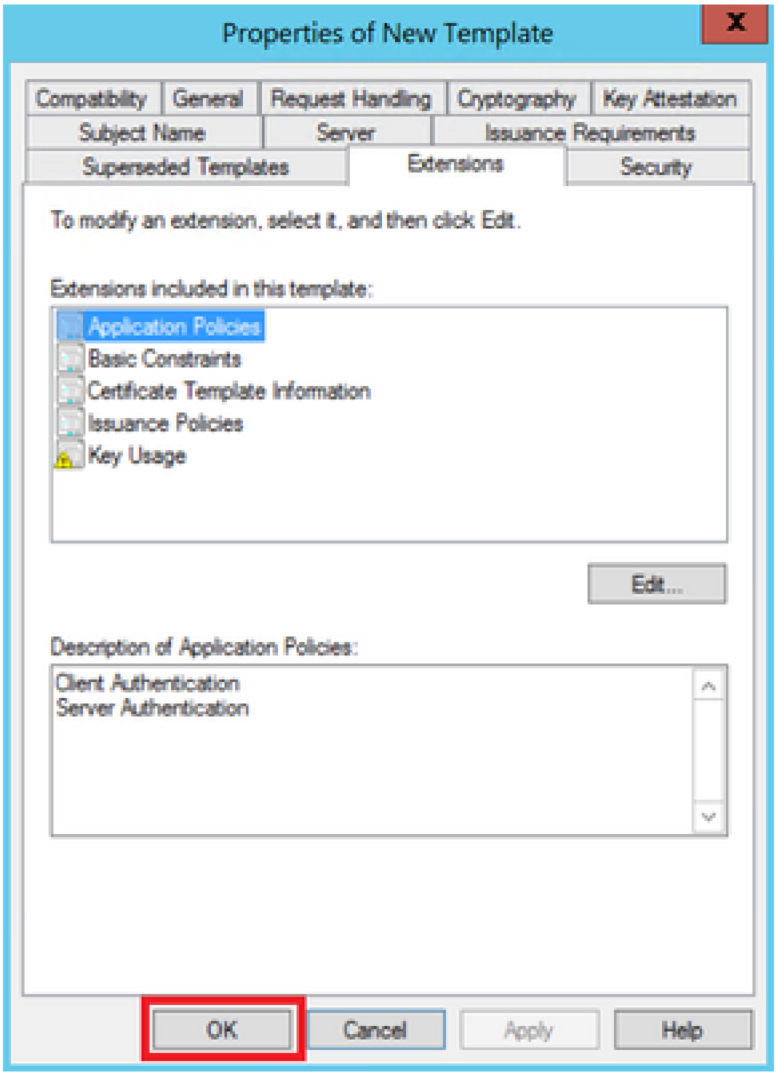


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

步骤 7.返回模板，选择Apply，然后选择OK。



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

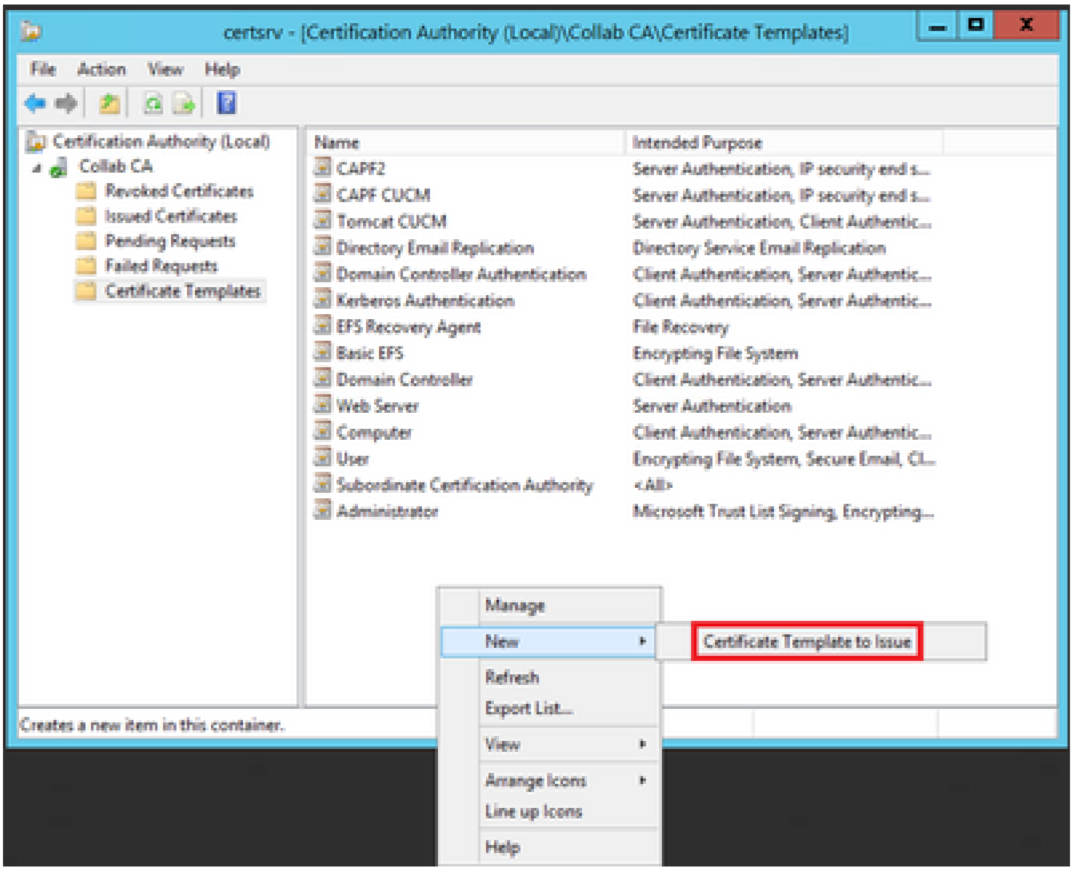
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
Server Authentication

步骤 8关闭**Certificate Template Console**窗口，然后返回第一个窗口，导航到**New > Certificate Template to Issue**，如图所示。

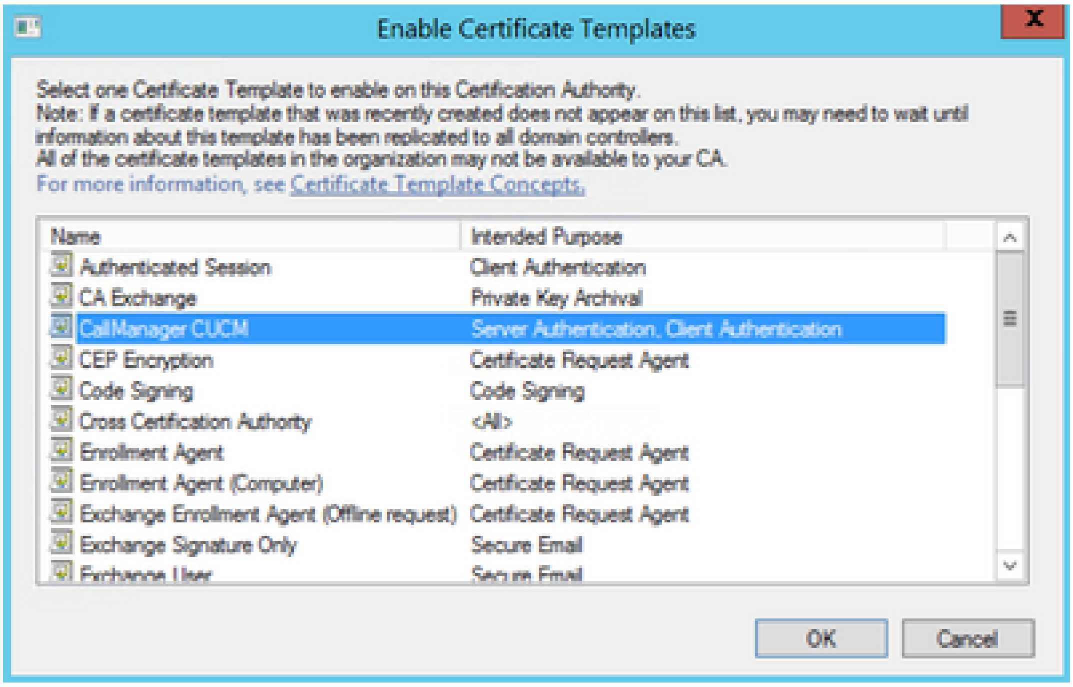


certsrv - [Certification Authority (Local)\Collab CA\Certificate Templates]

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.

步骤 9选择新的**CallManager CUCM**模板并选择**OK**，如图所示。



Enable Certificate Templates

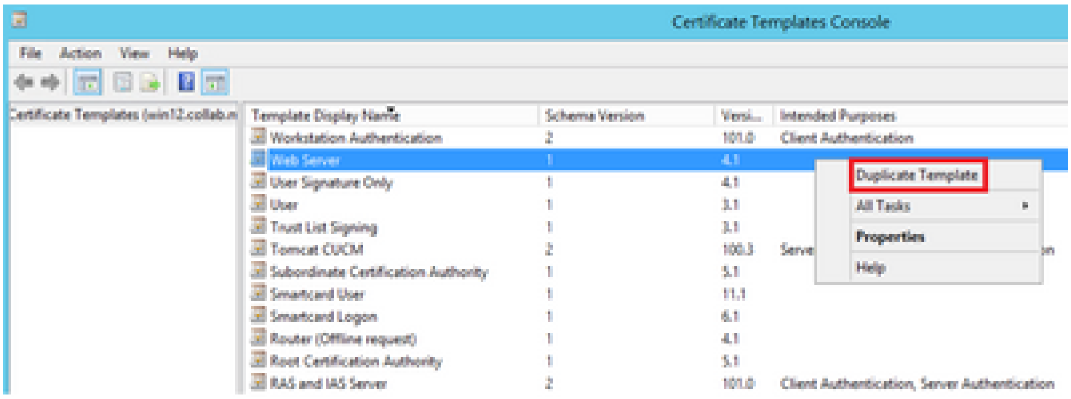
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates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

Name	Intended Purpose
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

步骤 10根据需要重复前面的所有步骤，为Tomcat和TVS服务创建证书模板。

IPsec模板

步骤1:找到**Web Server**模板，右键单击该模板，然后选择**复制模板**，如图所示。



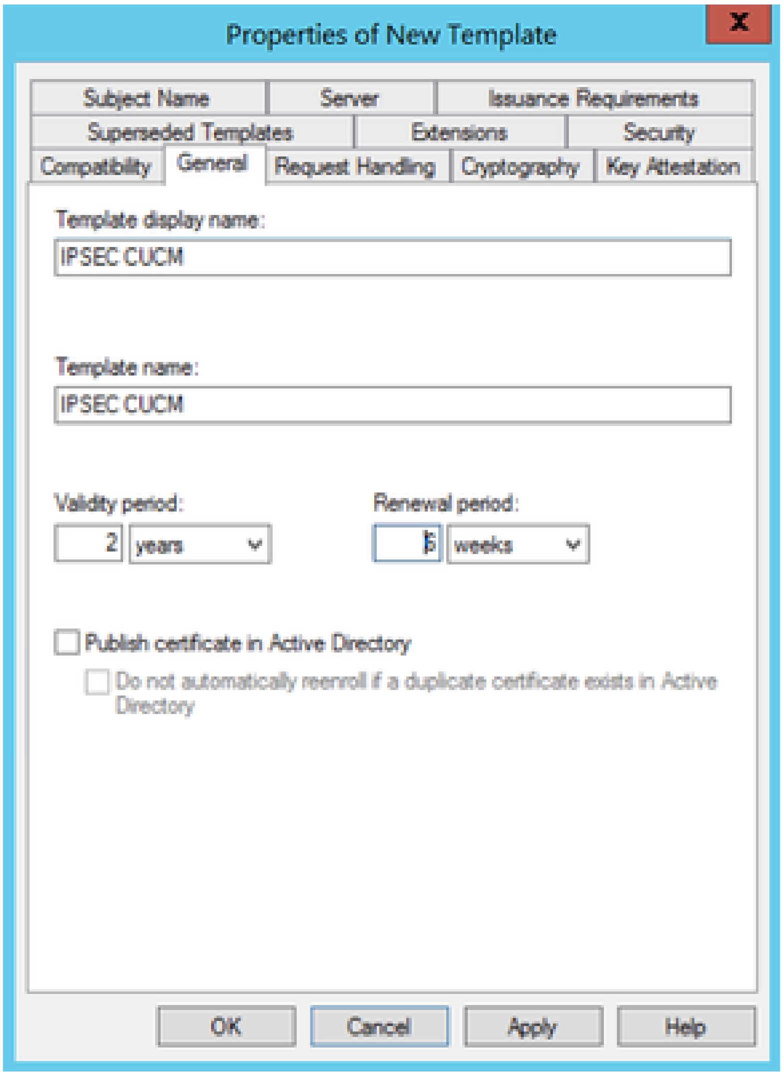
Certificate Templates Console

File Action View Help

Certificate Templates (win12.collab.n

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

第二步：在General下，您可以更改证书模板的名称、显示名称、有效性等。



Properties of New Template

Template display name: IPSEC CUCM

Template name: IPSEC CUCM

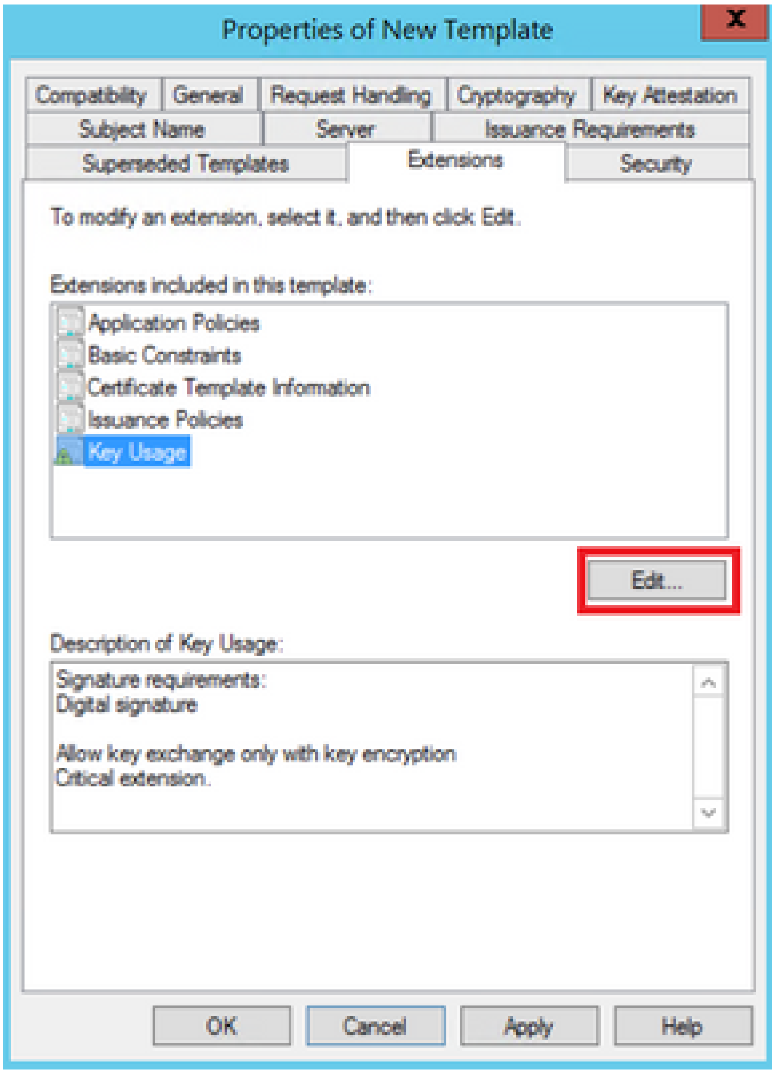
Validity period: 2 years

Renewal period: 6 weeks

☐ Publish certificate in Active Directory

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

第三步：导航到**Extensions > Key Usage > Edit**，如图所示。



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

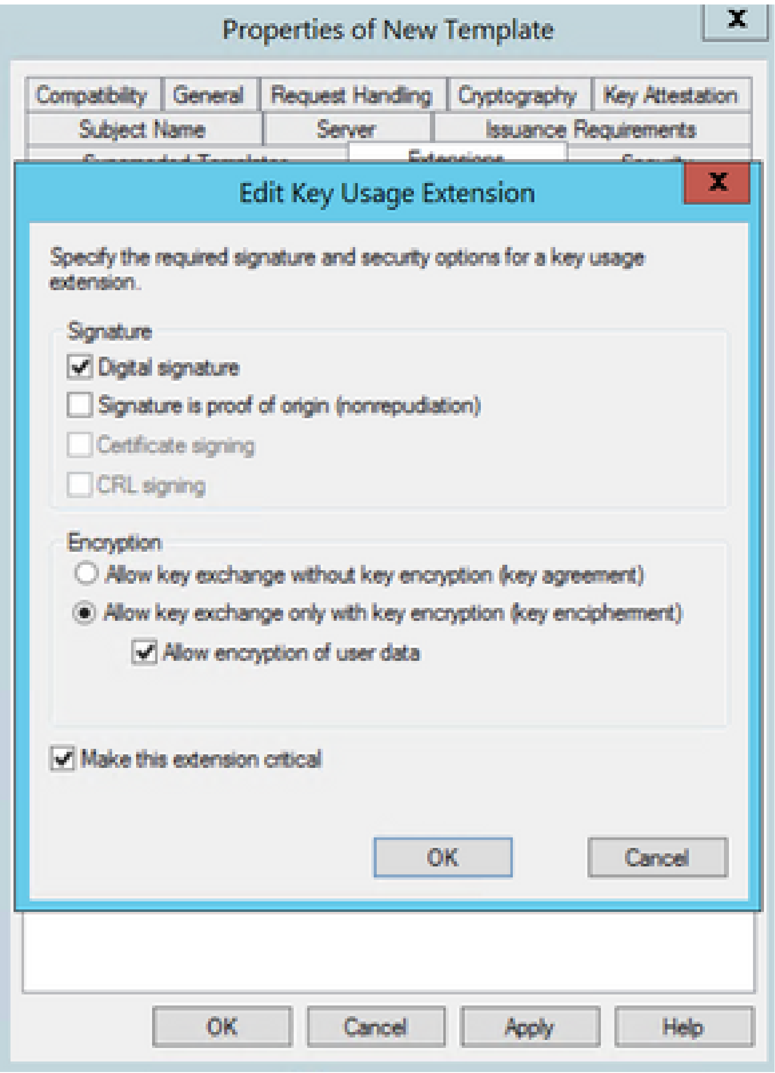
Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

第四步：选择这些选项并选择OK，如图所示。

- **数字签名**
- **仅允许使用密钥加密进行密钥交换（密钥加密）**
- **允许加密用户数据**



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

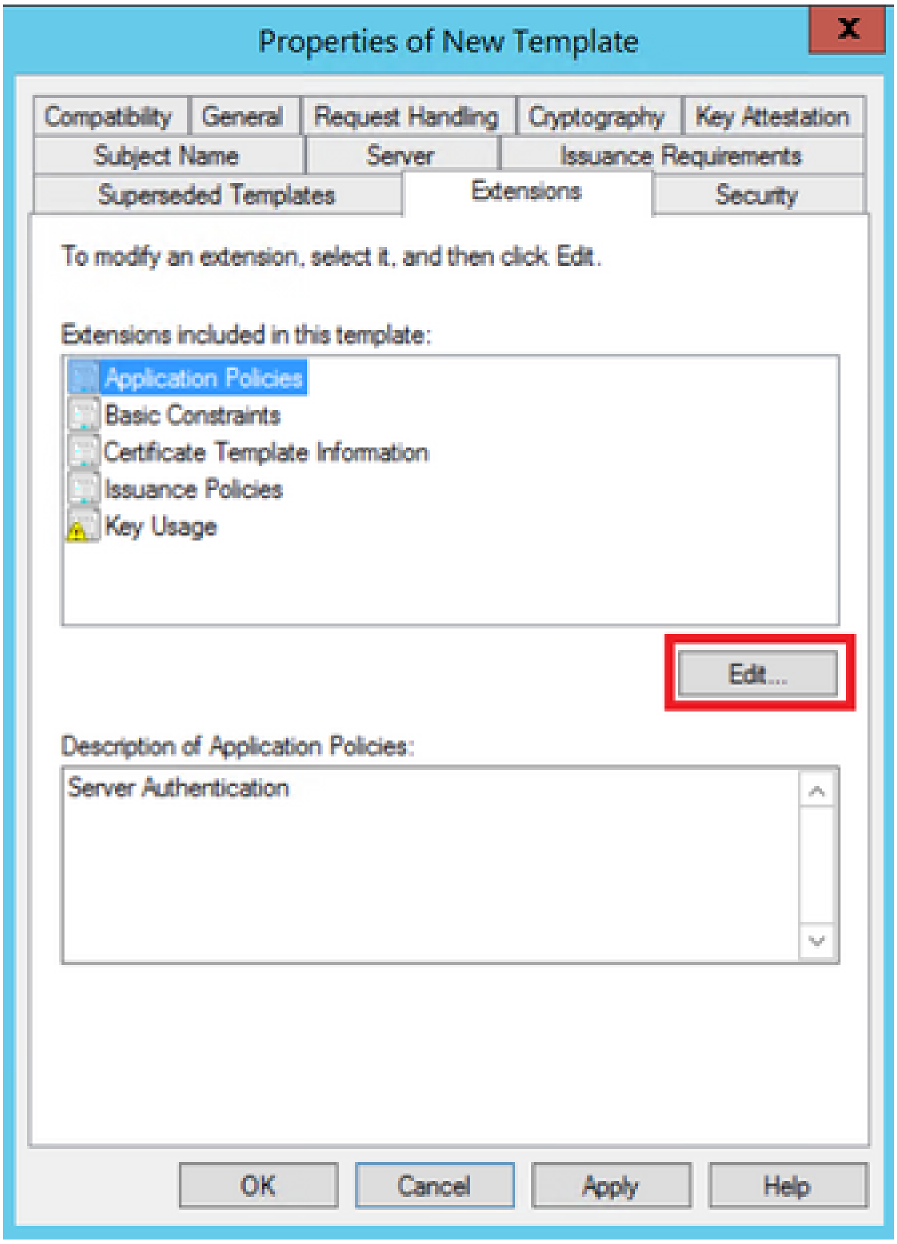
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

第五步：导航到**扩展>应用策略>编辑>添加**，如图所示。



Properties of New Template

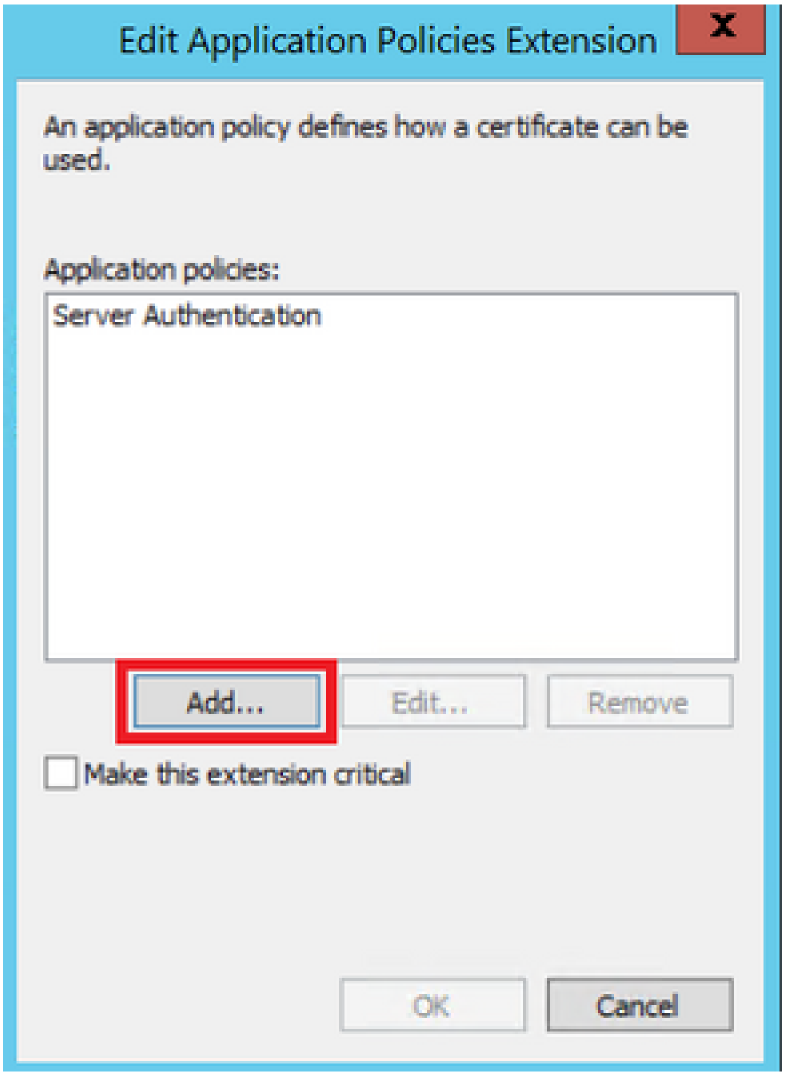
To modify an extension, select it, and then click Edit.

Extensions included in this template:

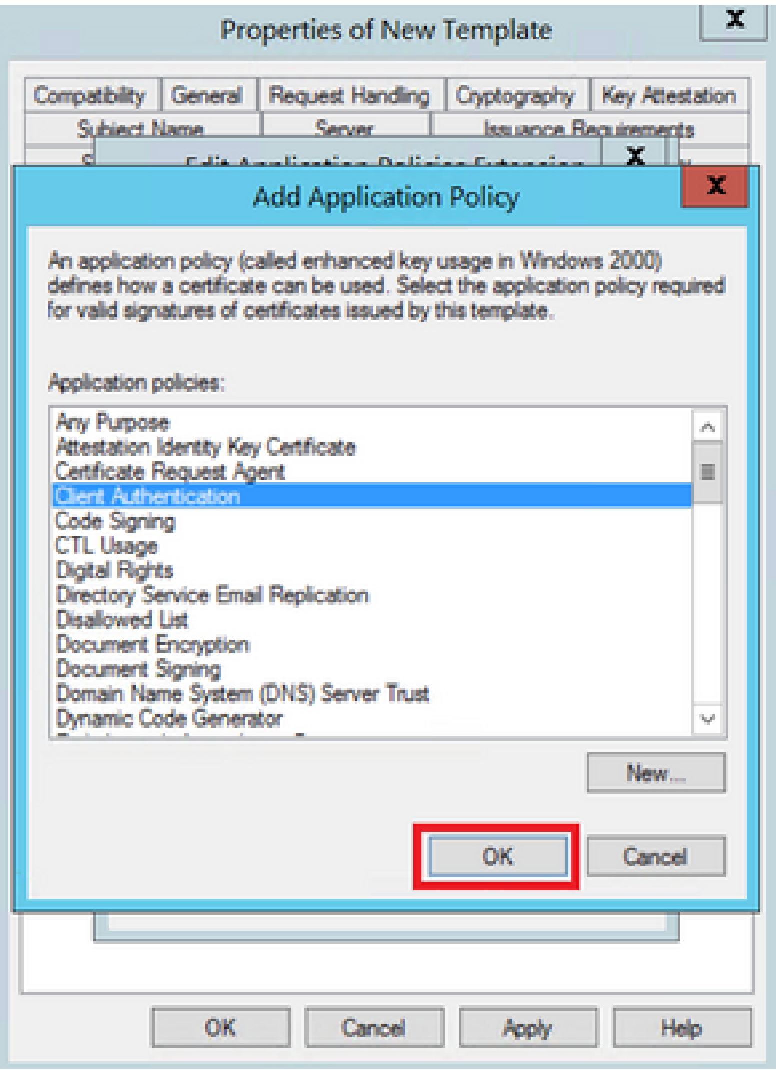
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Server Authentication


Edit Application Policies Extension
X
An application policy defines how a certificate can be used.
Application policies:
Server Authentication
Add...
Edit...
Remove
□ Make this extension critical
OK
Cancel

第六步：搜索**Client Authentication**，选择它，然后单击**OK**，如图所示。

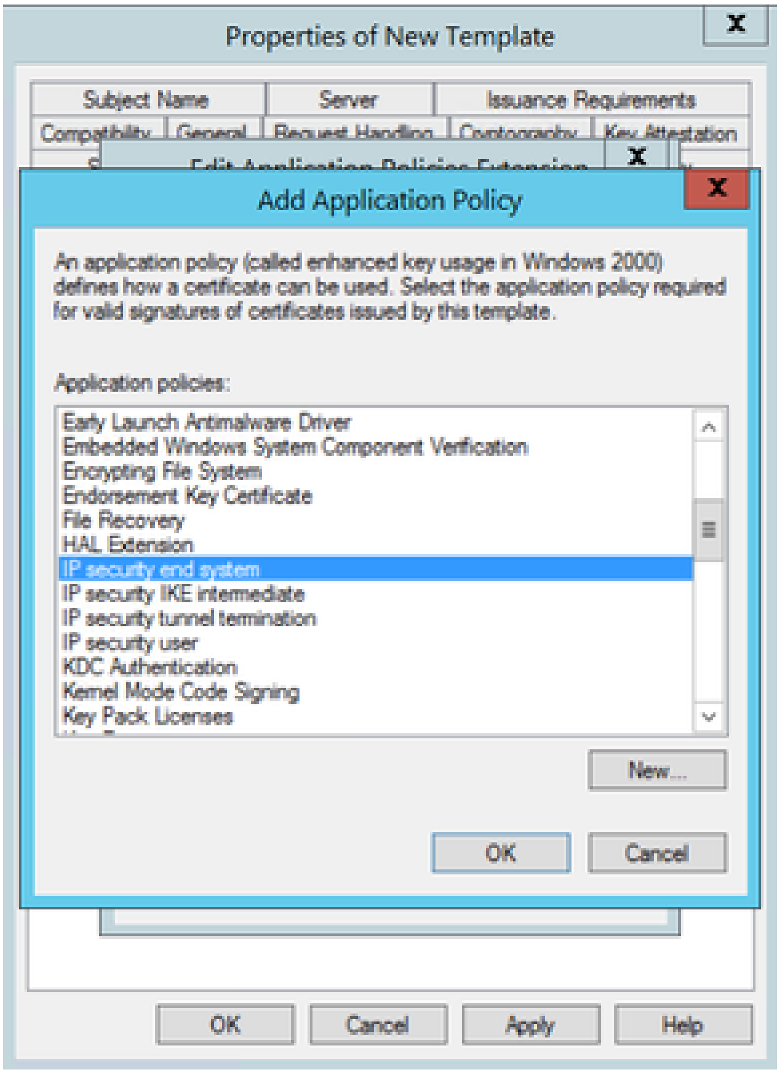


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

步骤 7.再次选择**Add**，搜索**IP安全终端系统**，选择它，然后在此窗口和上一个窗口中选择**OK**。

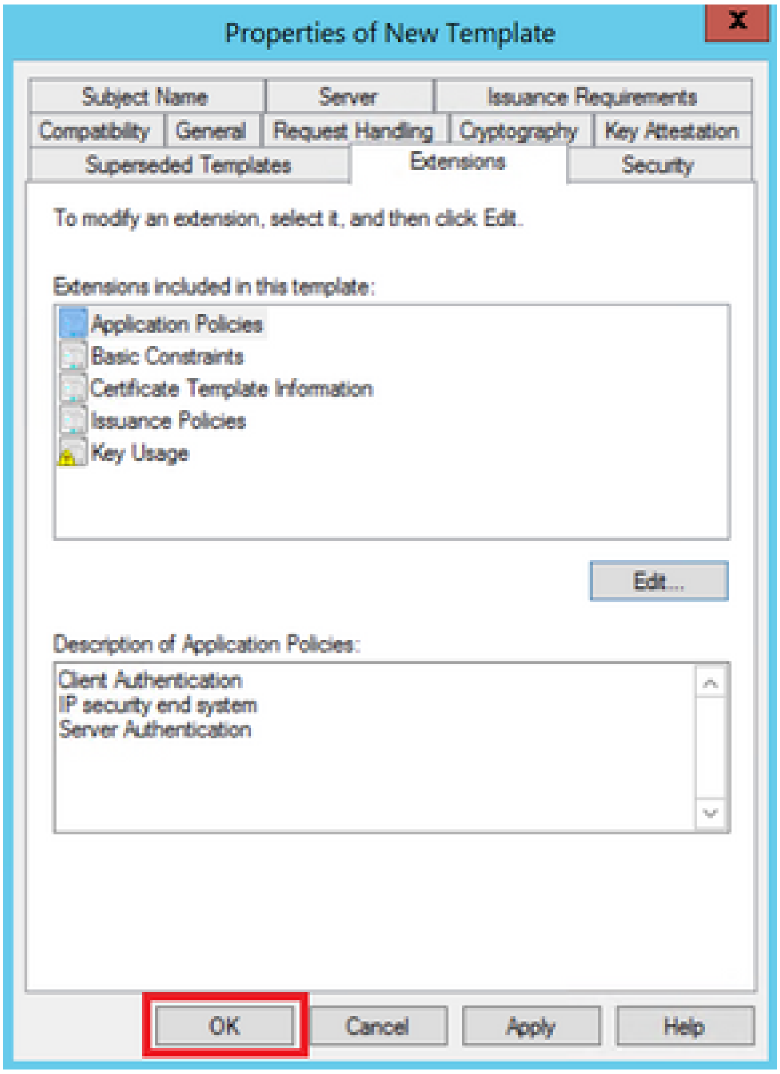


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

步骤 8返回到模板上，选择**Apply**，然后选择**OK**，如图所示。



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

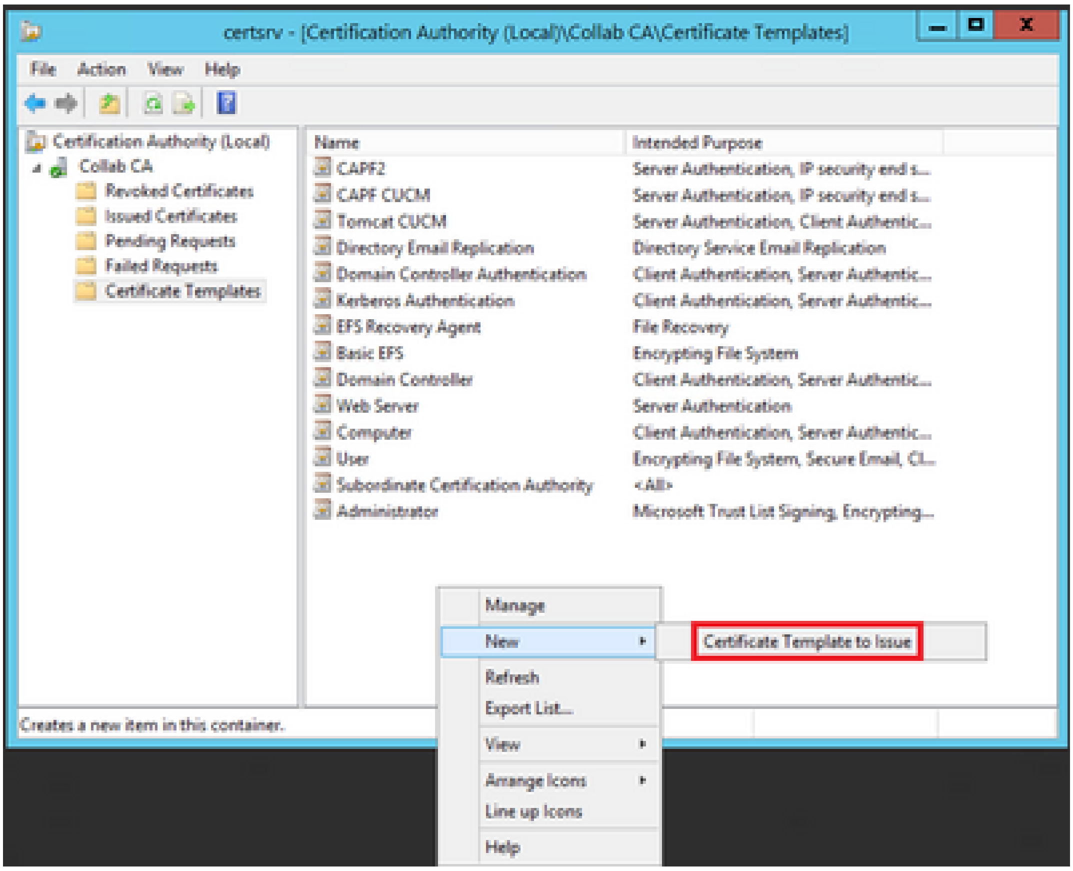
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
IP security end system
Server Authentication

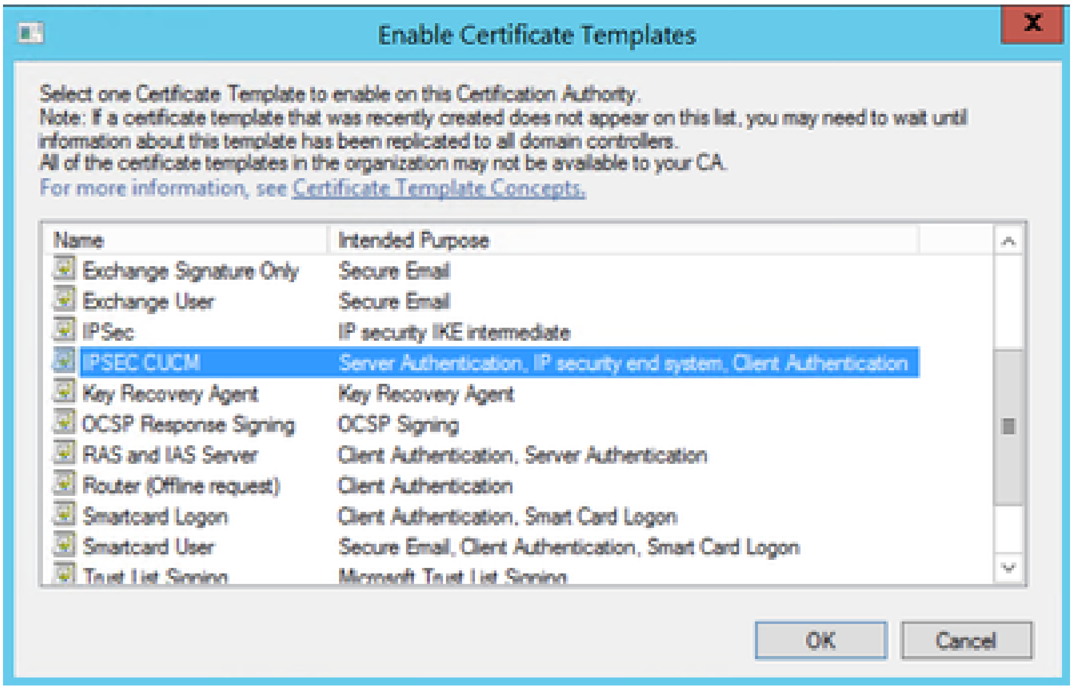
步骤 9关闭**Certificate Templates Console**窗口，然后返回第一个窗口，导航到**New > Certificate Template to Issue**，如图所示。



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.

步骤 10选择新的**IPSEC CUCM**模板，然后选择**确定**，如图所示。

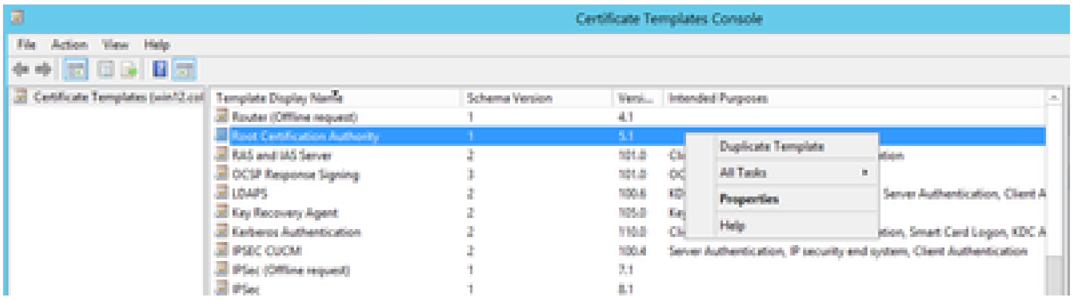


Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates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

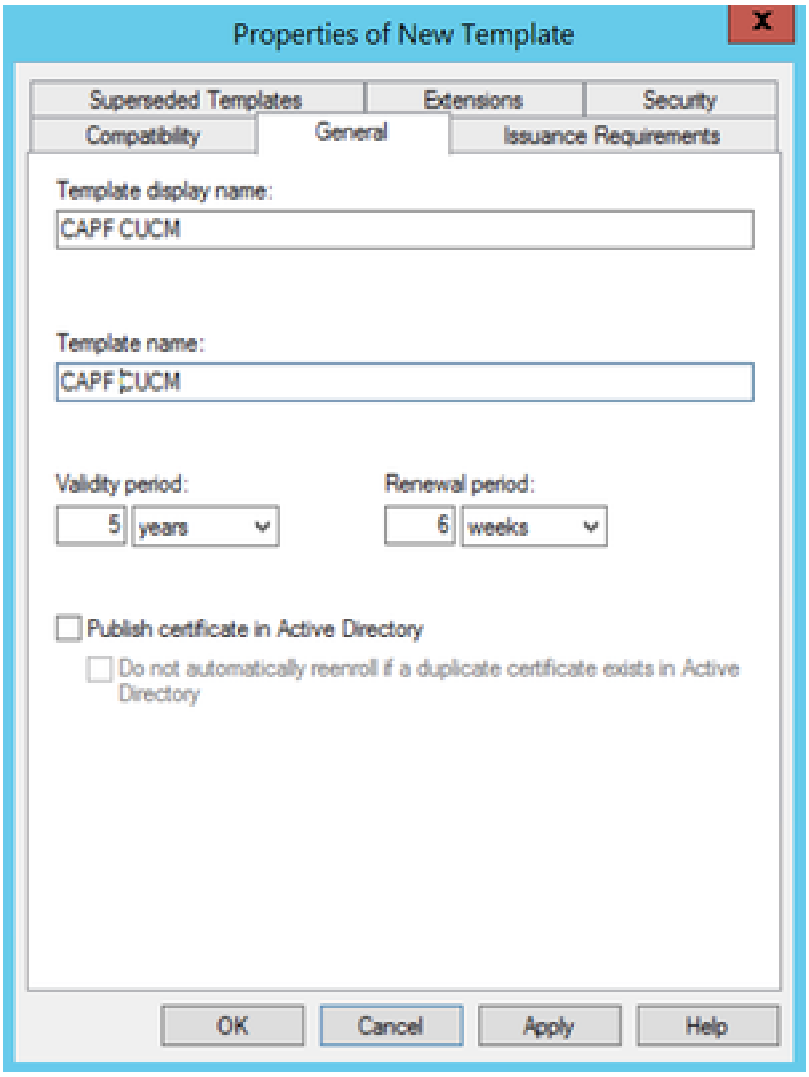
CAPF模板

步骤1:找到**根CA**模板并右键单击。然后选择**Duplicate Template**，如图所示。



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	

第二步：在General下，您可以更改证书模板的名称、显示名称、有效性等。



Template display name:
CAPF CUCM

Template name:
CAPF CUCM

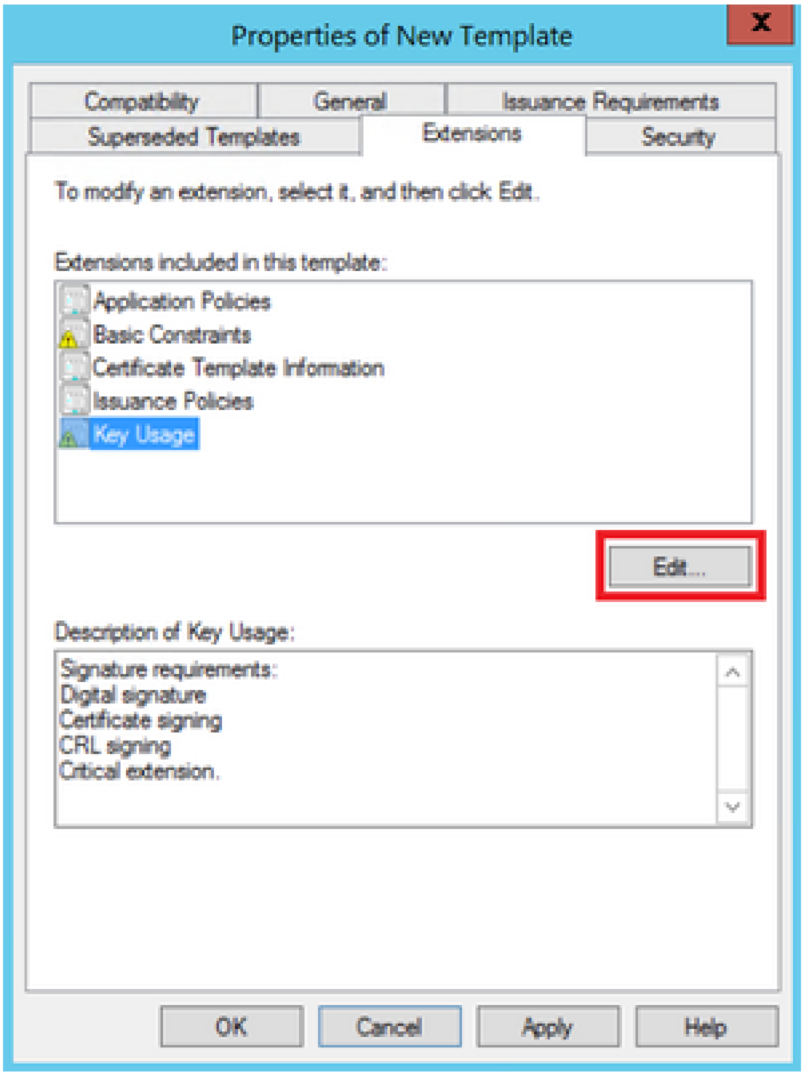
Validity period:
5 years

Renewal period:
6 weeks

□ Publish certificate in Active Directory

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

第三步：导航到Extensions > Key Usage > Edit，如图所示。



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

Extensions included in this template:

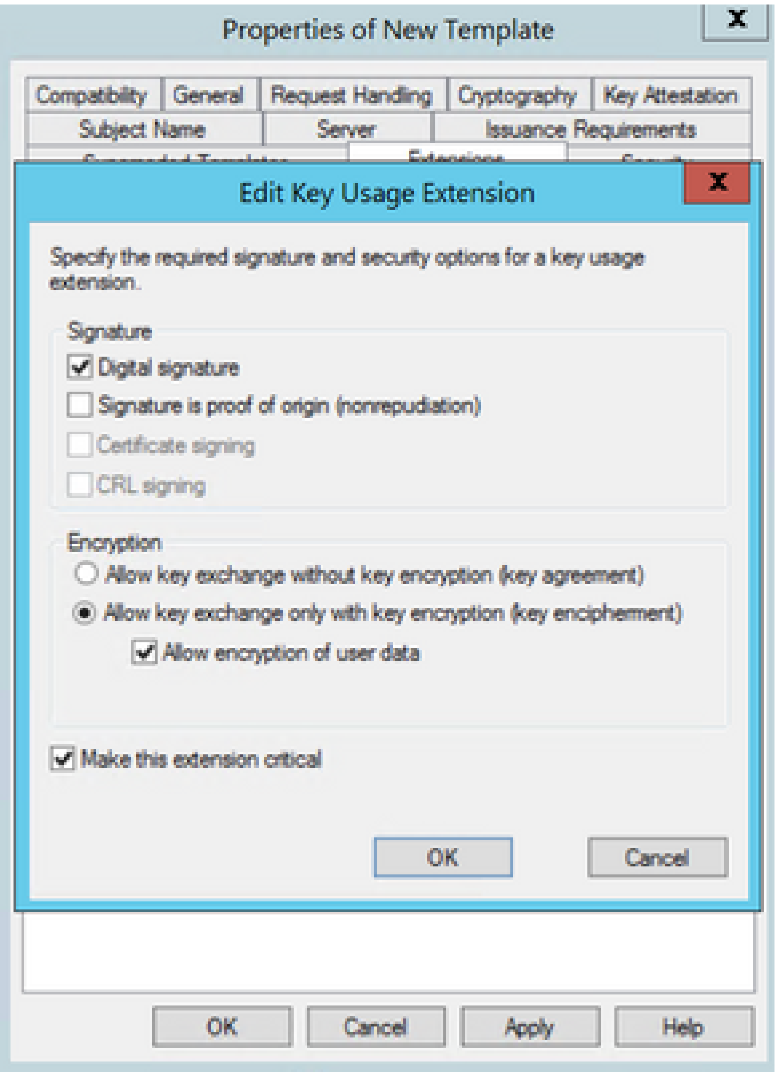
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Key Usage:

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

第四步：选择这些选项并选择OK，如图所示。

- **数字签名**
- **证书签名**
- **CRL签名**



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

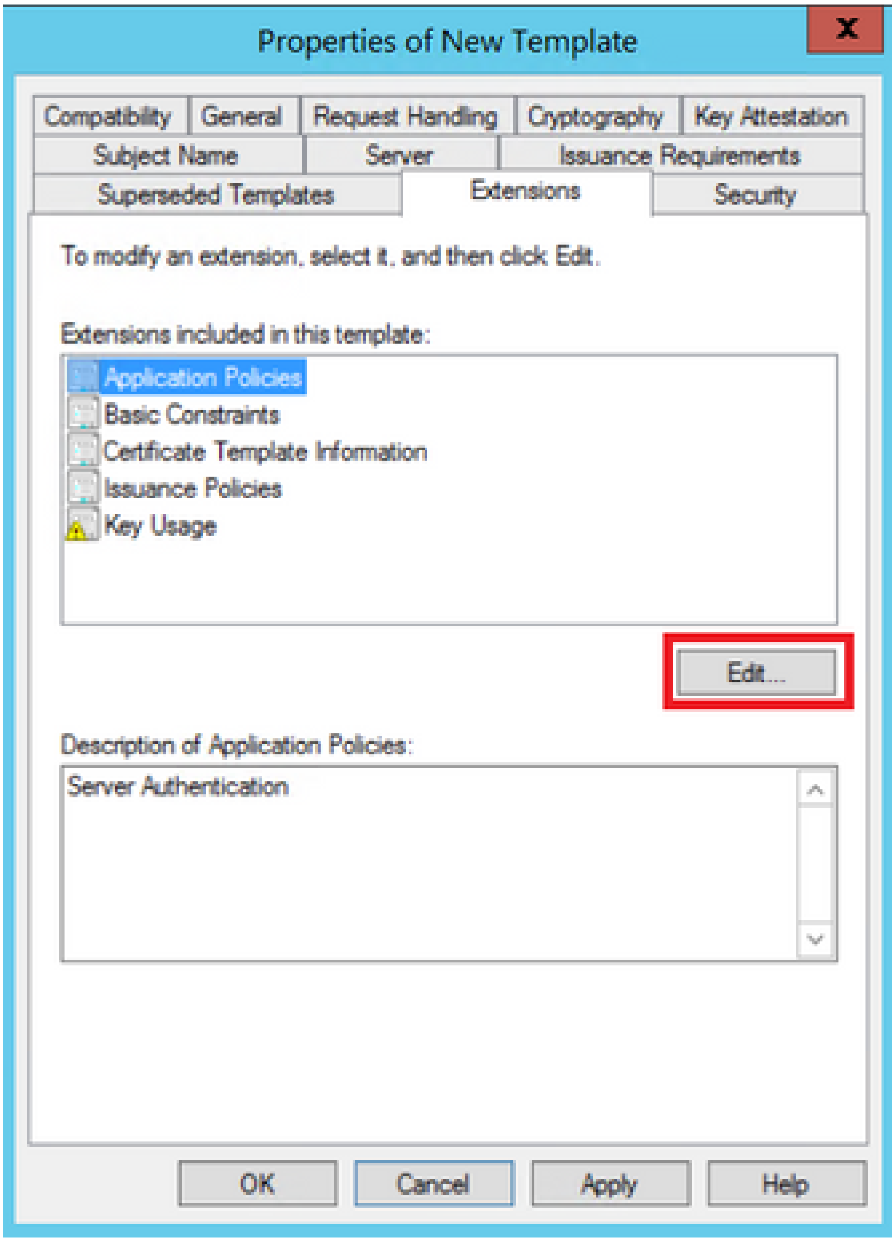
○ Allow key exchange without key encryption (key agreement)

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

☑ Allow encryption of user data

☑ Make this extension critical

第五步：导航到**扩展>应用策略>编辑>添加**，如图所示。



Properties of New Template

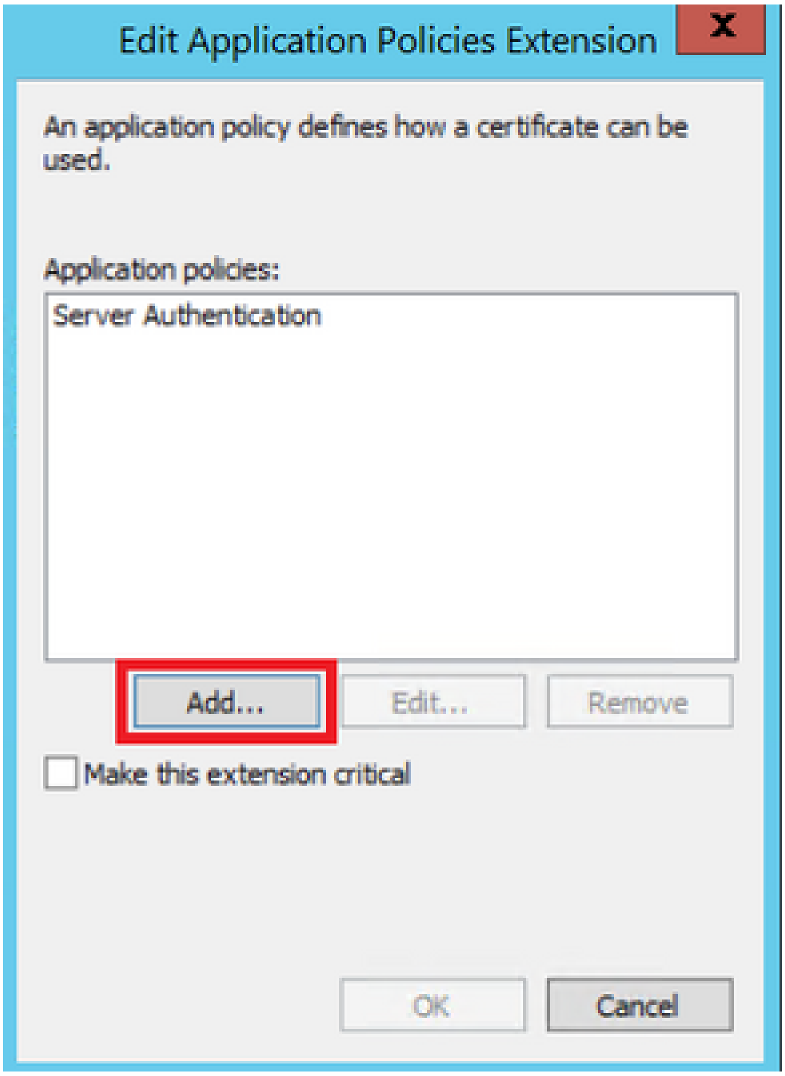
To modify an extension, select it, and then click Edit.

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

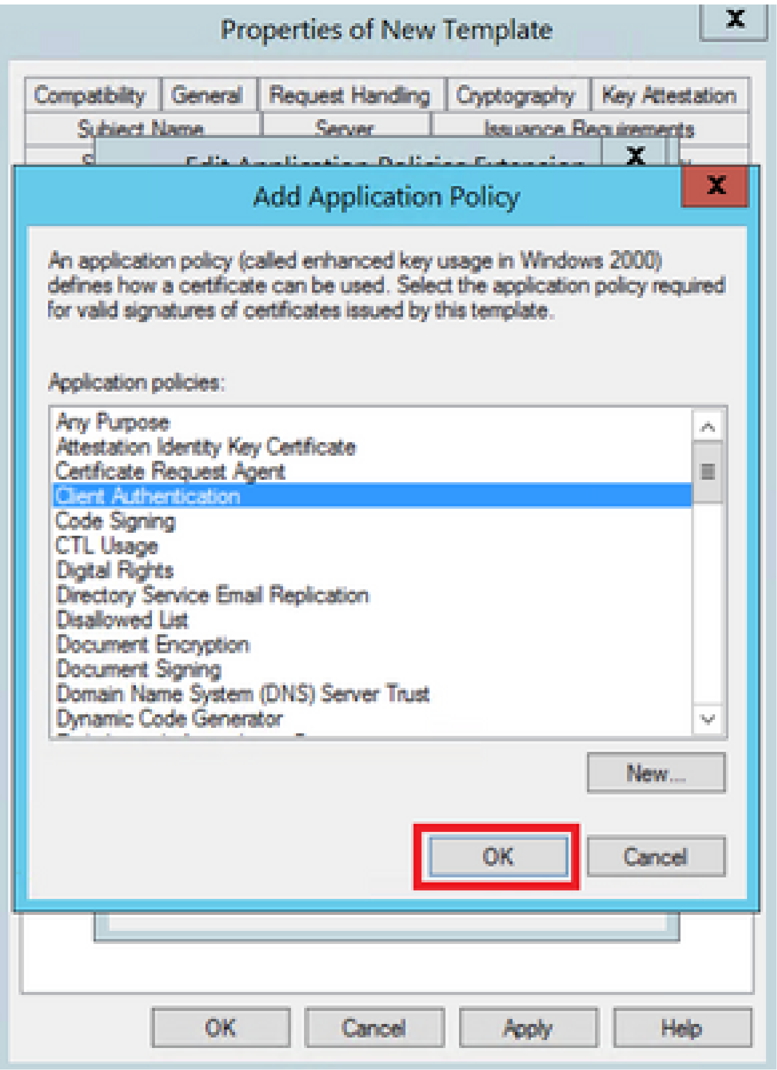
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

第六步：搜索**Client Authentication**，选择它，然后选择**OK**，如图所示。

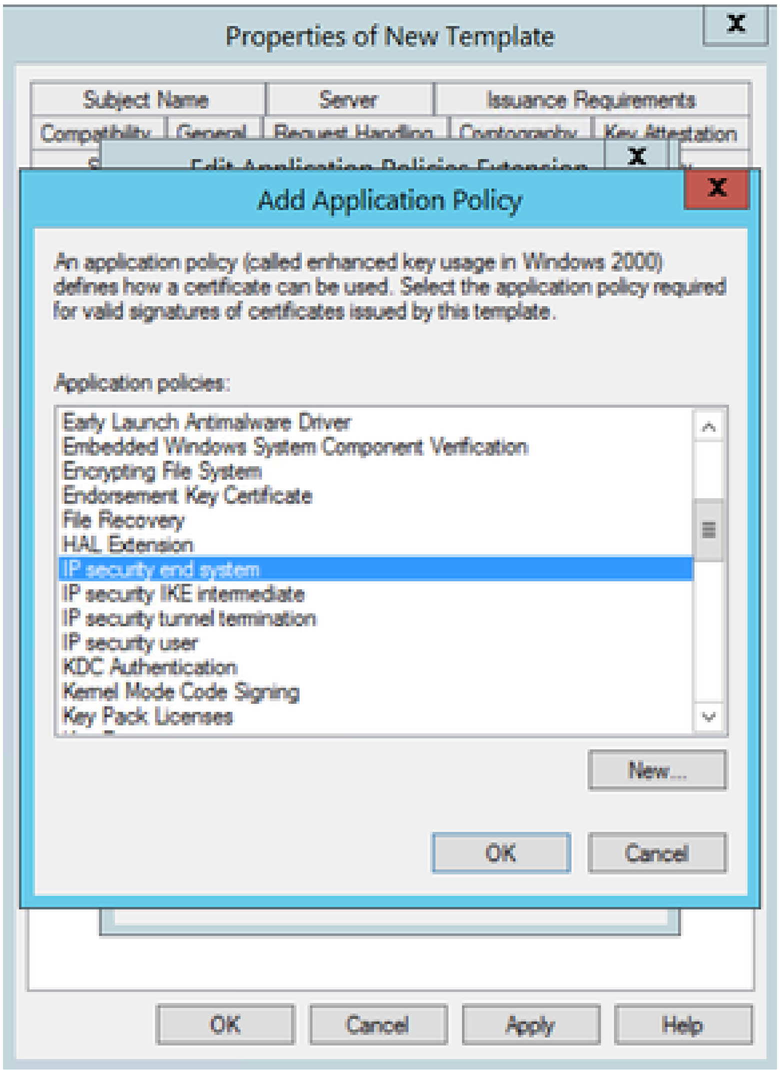


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

步骤 7.再次选择**Add**，搜索**IP安全终端系统**，选择它，然后在此窗口和上一个窗口上选择OK，如图所示。

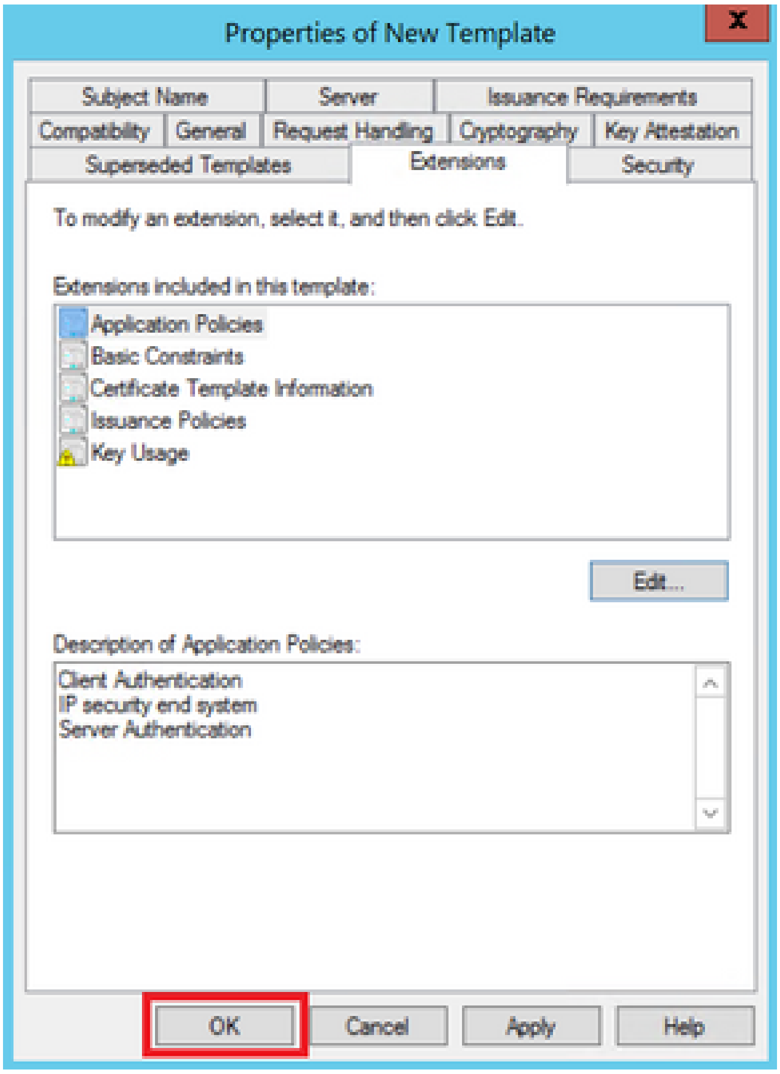


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

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

步骤 8返回到模板上，选择**Apply**，然后选择**OK**，如图所示。



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

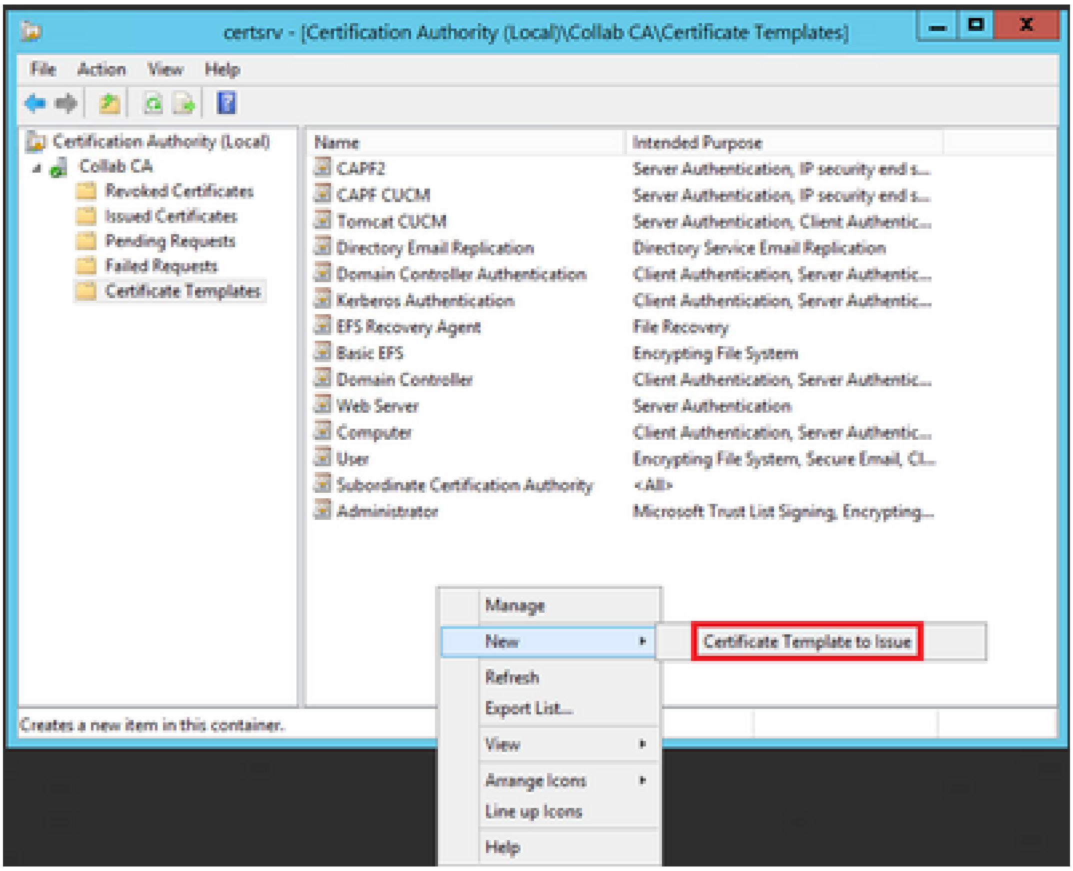
Extensions included in this template:

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

Description of Application Policies:

Client Authentication
IP security end system
Server Authentication

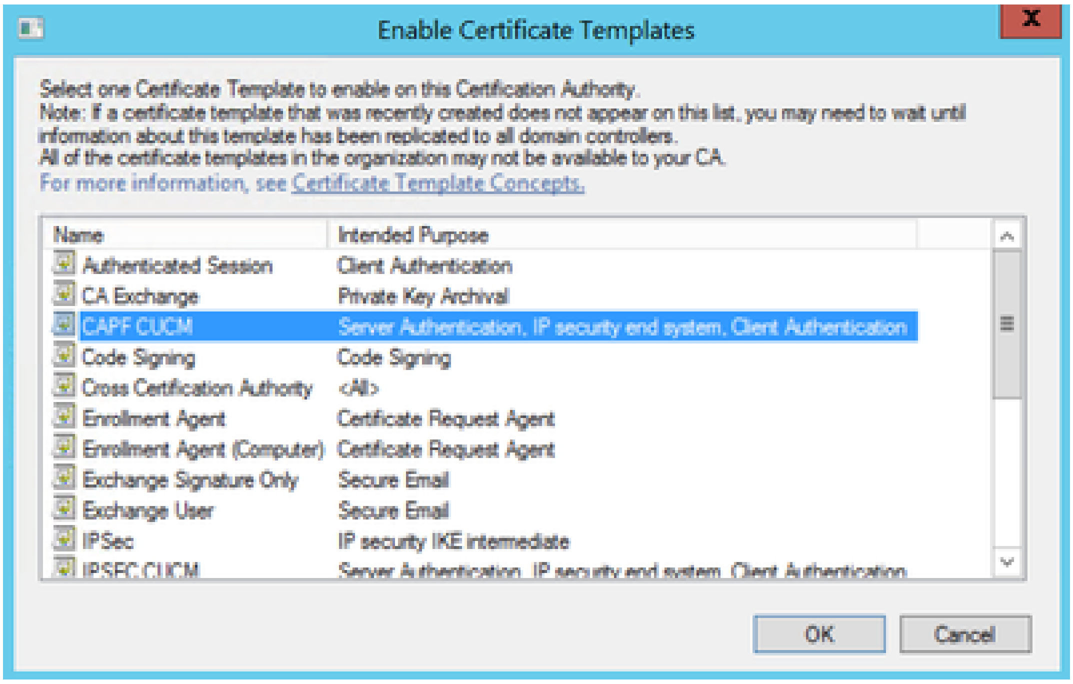
步骤 9关闭**Certificate Templates Console**窗口，然后返回第一个窗口，导航到**New > Certificate Template to Issue**，如图所示。



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.

步骤 10选择新的**CAPF CUCM模**板，然后选择**OK**，如图所示。



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

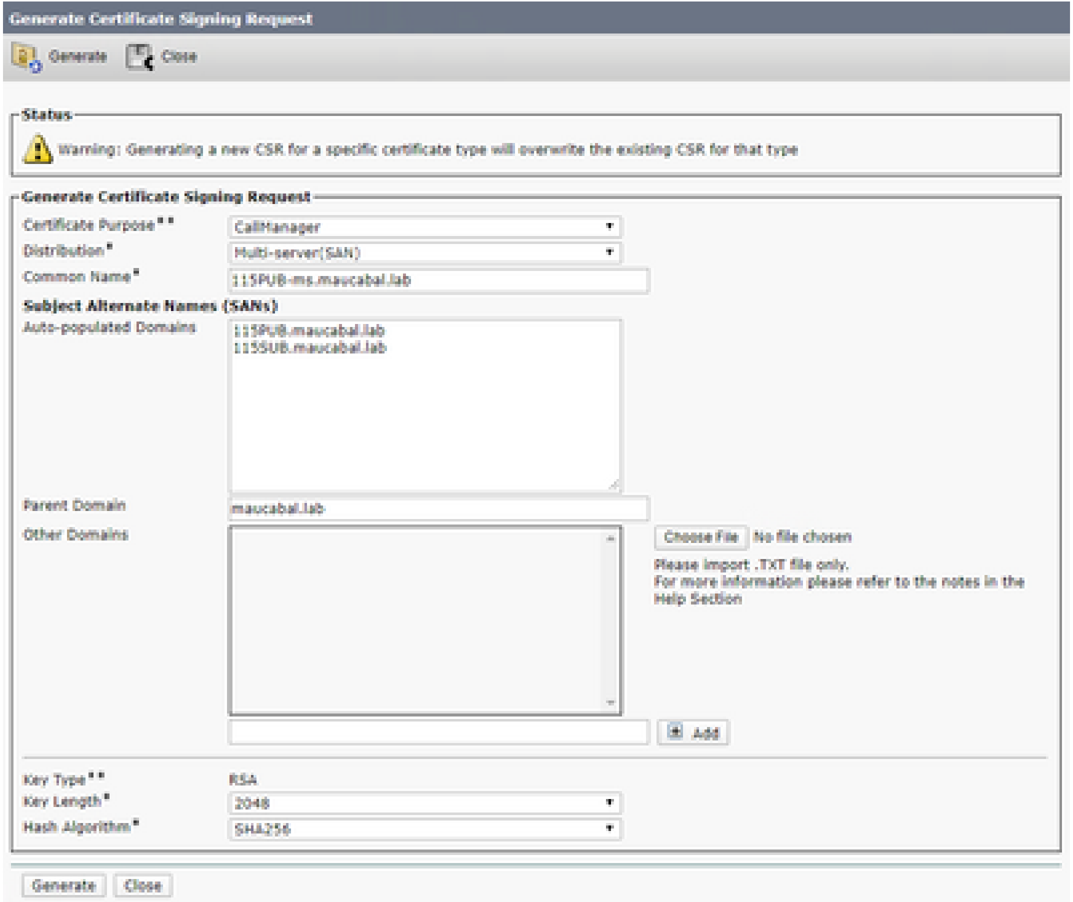
生成证书签名请求

使用此示例可使用新创建的模板生成CallManager证书。相同的步骤可用于任何证书类型，您只需相应地选择证书和模板类型：

步骤1:在CUCM上，导航到**OS Administration > Security > Certificate Management > Generate CSR**。

第二步：选择这些选项并选择**生成**，如图所示。

- 证书用途：CallManager
- 分布:**<这可以只用于一台服务器，也可以用于多SAN>**



Generate Certificate Signing Request

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

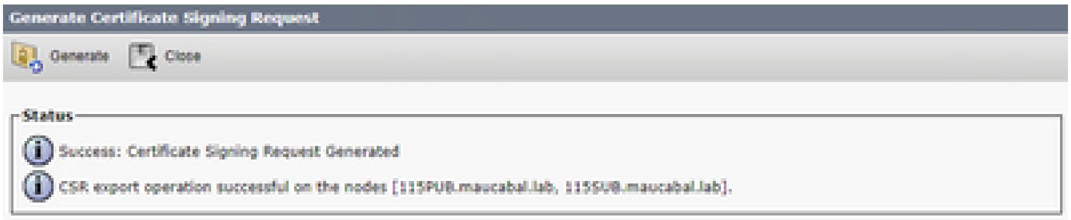
Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

第三步：系统生成确认消息，如图所示。



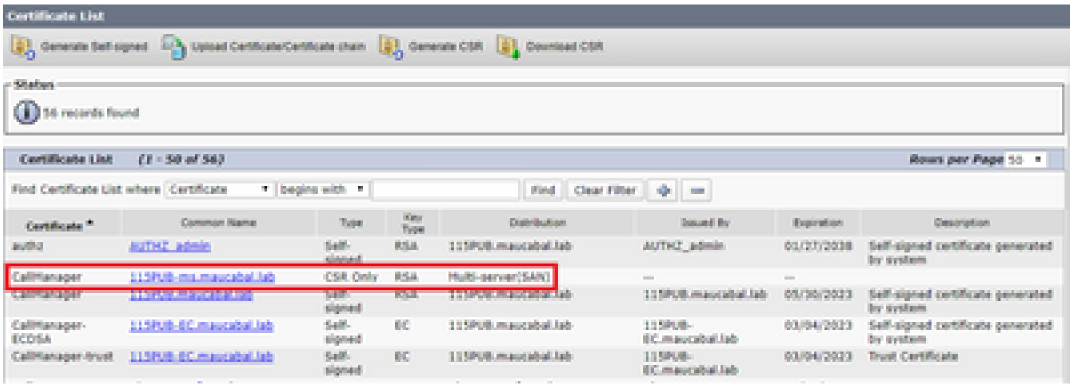
Generate Certificate Signing Request

Status

Success: Certificate Signing Request Generated

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

第四步：在证书列表中，查找类型为**CSR Only**的条目并选择它，如图所示。



Certificate List

Status

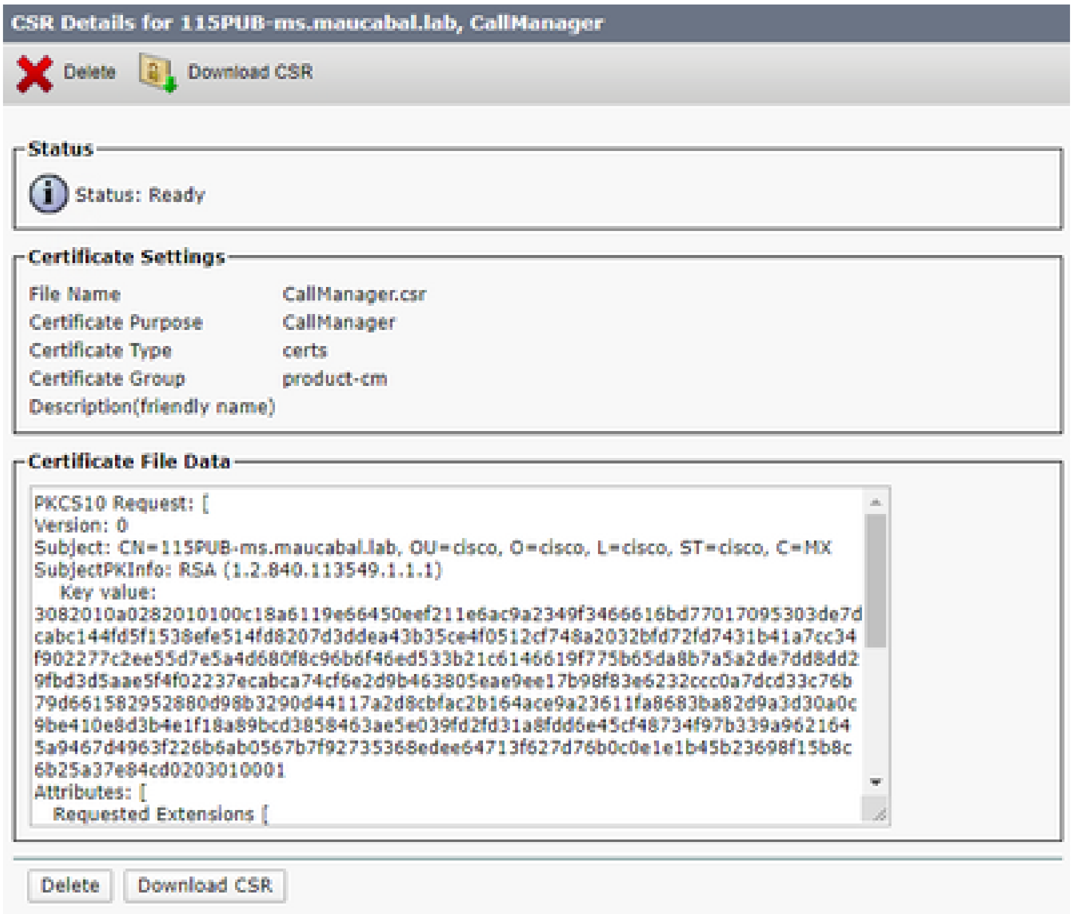
56 records found

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

第五步：在弹出窗口中，选择**下载CSR**，并将文件保存到计算机上。



Status

Status: Ready

Certificate Settings

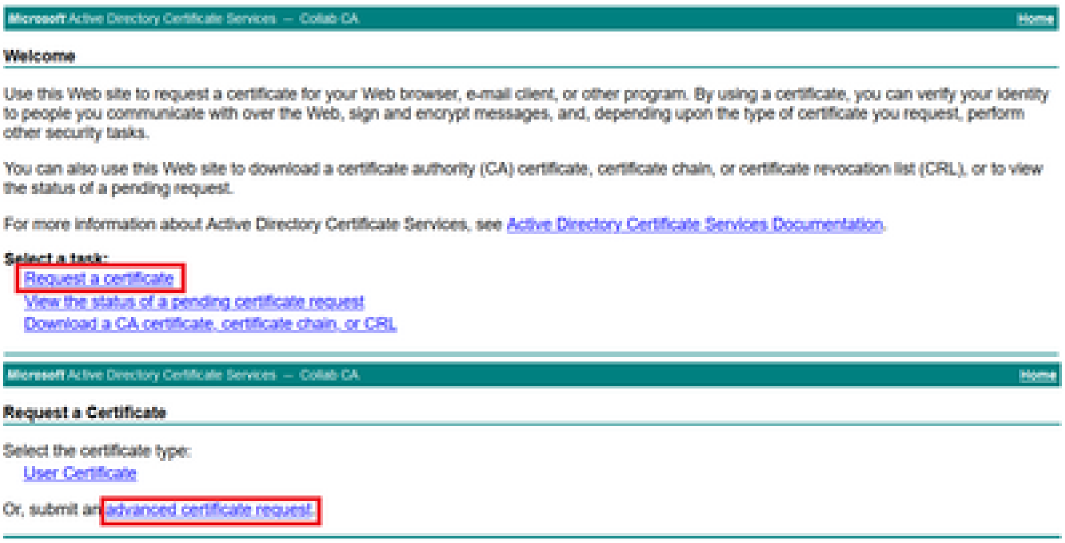
File Name	CallManager.csr
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	

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 [
```

第六步：在浏览器上，导航到此URL，然后输入域控制器管理员凭据：**https://<yourWindowsServerIP>/certsrv/。**

步骤 7.导航至**请求证书>高级证书请求**，如图所示。


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

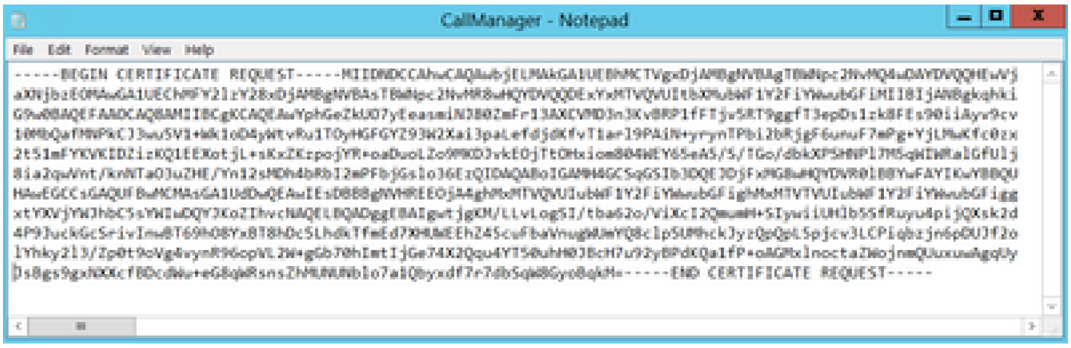
Microsoft Active Directory Certificate Services -- Collab CA
Home

Request a Certificate

Select the certificate type:
User Certificate

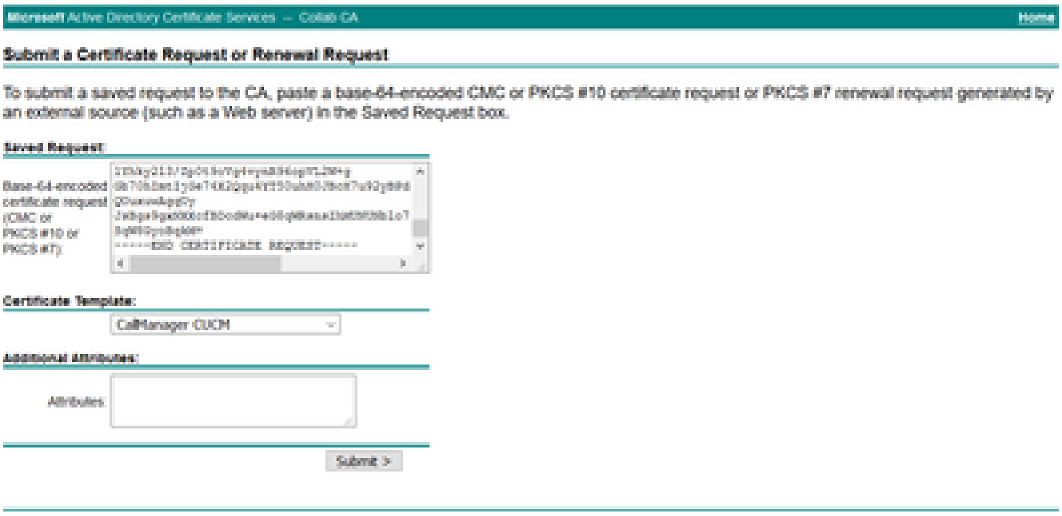
Or, submit an advanced certificate request.

步骤 8打开CSR文件并复制其所有内容：



```
-----BEGIN CERTIFICATE REQUEST-----MIIDNDCCAhwCAQAwbjELMAkGA1UEBhMCTVgxDjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVj
aXNjbzEOMAwGA1UEChMFY2lzY28xDjAMBgNVBAsTBWNpc2NvMR8wHQYDVQQDExYxMTVQVUItbXMubWF1Y2FiYWwubGFiMIIBIjANBgkqhki
G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYphGeZkUO7yEeasmiNJ80ZmFr13AXCVMD3n3KvBRP1fFTjv5RT9ggfT3epDs1zk8FEs90iiAyv9cv
10MbQafMNPkCJ3wu5V1+Wk1oD4yWtvRu1TOyHGFGYZ93W2Xai3paLefdjdKfvT1arl9PAiN+yrynTPbi2bRjgF6unuF7mPg+YjLMwKfc0zx
2t51mFYKVKIDZizKQ1EEXotjL+sKxZKzpojYR+oaDuoLZo9MKDJvkEOjTtOHxiom804WEY65eA5/5/TGo/dbkXP5HNP17M5qWIWRalGfUlj
8ia2quVnt/knNTaOJuZHE/Yn12sMDh4bRbI2mPFbjGslo36EzQIDAQABoIGAMH4GCSqGSIb3DQEJDjFxMG8wHQYDVR0lBBYwFAYIKwYBBQU
HAwEGCCsGAQUFBwMCMAsGA1UdDwQEAwIEsDBBBgNVHREEOjA4ghMxMTVQVUIubWF1Y2FiYWwubGFighMxMTVTVUIubWF1Y2FiYWwubGFigg
xtYXVjYWJhbC5sYWIwDQYJKoZIhvcNAQELBQADggEBAIgwtjgKM/LLvLogSI/tba62o/ViXcI2QmumH+SIywiiUHIb5SfRuyu4pijQXsk2d
4P9JuckGcSrivInwBT69h08YxBT8hDc5LhdkTfmEd7XHUWEEh245cuFbaVnugWJmYQ8clp5UMhckJyzQpQpL5pjcv3LCPiqbzjn6pDUJf2o
lYhky2l3/Zp0t9oVg4vynR96opVL2W+gGb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPdKQa1fP+oAGMxlnoctaZWojnmQUuxuwAgqUy
Ds8gs9gxNXKcfBDcdWu+eG8qWRsnsZhMUNUNblo7aiQbyxdf7r7dbSqW8GyoBqkM=-----END CERTIFICATE REQUEST-----
```

步骤 9将CSR粘贴到**Base-64编码的证书请求**字段中。在**证书模板**下，选择正确的模板，然后选择**提交**，如图所示。



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):

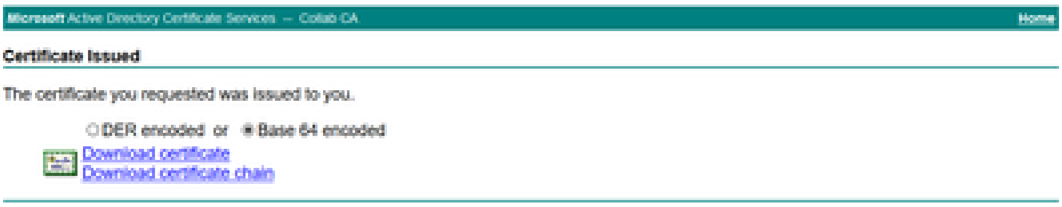
```
lYhky2l3/Zp0t9oVg4vynR96opVL2W+g
Gb70hImtIjGe74X2Qqu4YT50uhH0JBcH7u92yBPd
QUuxuwAgqUy
Ds8gs9gxNXKcfBDcdWu+eG8qWRsnsZhMUNUNblo7
8qW8GyoBqkM=
-----END CERTIFICATE REQUEST-----
```

Certificate Template: CallManager CUCM

Additional Attributes:

Attributes:

步骤 10最后，选择**Base 64 encoded**和**Download certificate chain**，现在可以将生成的文件上传到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

验证

验证过程实际上是配置过程的一部分。

故障排除

当前没有可用于此配置的特定故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。