CUCM용 Windows CA 인증서 템플릿 만들기

목차

소개

이 문서에서는 모든 유형의 Cisco Unified Communications Manager(CUCM) 인증서에 대한 X.509 확장 요구 사항을 준수하는 Windows Server 기반 CA(Certification Authority)에서 인증서 템플릿을 생성하기 위한 단계별 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM 버전 11.5(1) 이상
- Windows Server 관리에 대한 기본 지식이 필요합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서의 정보는 CUCM 버전 11.5(1) 이상을 기반으로 합니다.
- CA 서비스가 설치된 Microsoft Windows Server 2012 R2.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

외부 CA에서 서명할 수 있는 인증서는 5가지 유형입니다.

인증서	Use	영향받는 서비스
통화 관리자	보안 디바이스 등록 시 SIP(Secure Session Initiation Protocol) 트렁크와 같은 다른 서버와의 보안 상호 작용에 사용되는 CTL(Certificate Trust List)/ITL(Internal Trust List) 파일에 서명할 수 있습니다.	·Cisco Call Manager ·Cisco CTI Manager ·Cisco TFTP
수고양이	HTTPS(Secure Hypertext Transfer Protocol) 상호 작용에 대해 제공됩니다.	·Cisco Tomcat ·단일 로그인(SSO) ·내선 이동 ·회사 디렉터리
ipsec	MGCP(Media Gateway Control Protocol) 또는 H323 게이트웨이와의 IPsec(IP Security) 상호 작용뿐 아니라 백업 파일 생성에 사용됩니다.	·Cisco DRF 마스터 ·Cisco DRF 로컬
CAPF	전화기의 LSC(Locally Significant Certificates)를 생성하는 데 사용됩니다.	·Cisco Certificate Authority 프록시 기능
TV	전화기에서 알 수 없는 인증서를 인증할 수 없는 경우 TVS(Trust Verification Service)에 대한 연결을 만드는 데 사용됩니다.	·Cisco Trust Verification 서비스

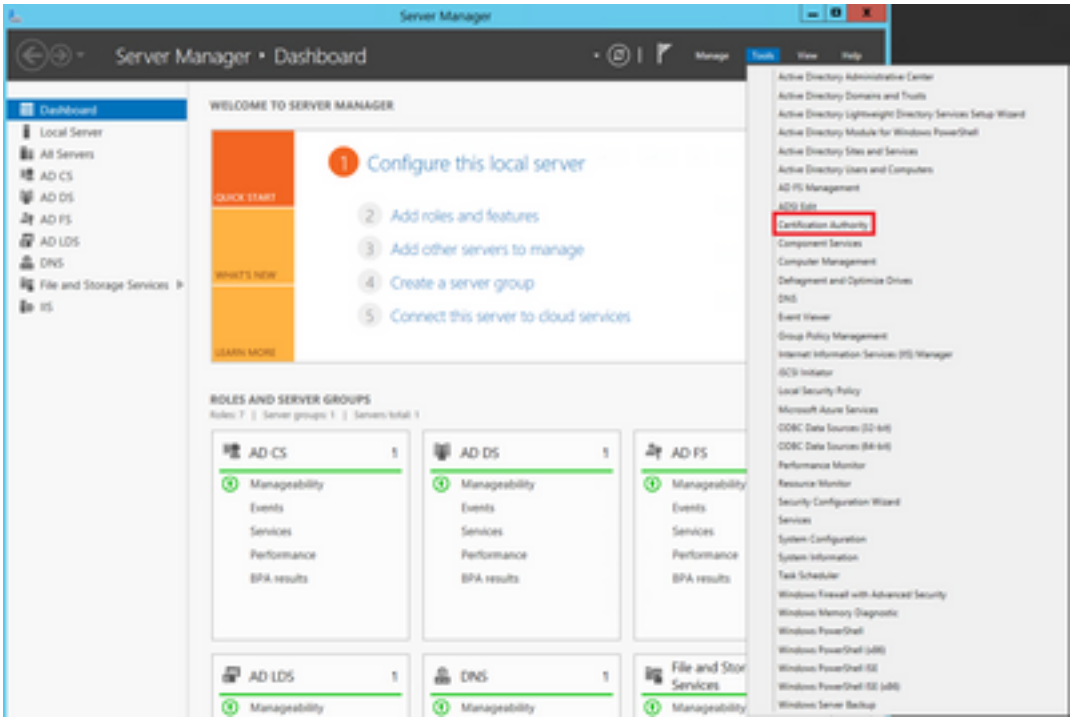
이러한 인증서에는 각각 설정해야 하는 몇 가지 X.509 확장 요구 사항이 있습니다. 그렇지 않으면 앞서 언급한 서비스 중 하나에서 잘못된 동작이 발생할 수 있습니다.

인증서	X.509 키 사용	X.509 확장 키 사용
통화 관리자	·디지털 서명 ·키 암호화 ·데이터 암호화	·웹 서버 인증 ·웹 클라이언트 인증
수고양이	·디지털 서명 ·키 암호화 ·데이터 암호화	·웹 서버 인증 ·웹 클라이언트 인증
ipsec	·디지털 서명 ·키 암호화 ·데이터 암호화	·웹 서버 인증 ·웹 클라이언트 인증 ·IPsec 엔드 시스템
CAPF	·디지털 서명 ·인증서 서명 ·키 암호화	·웹 서버 인증 ·웹 클라이언트 인증
TV	·디지털 서명 ·키 암호화 ·데이터 암호화	·웹 서버 인증 ·웹 클라이언트 인증

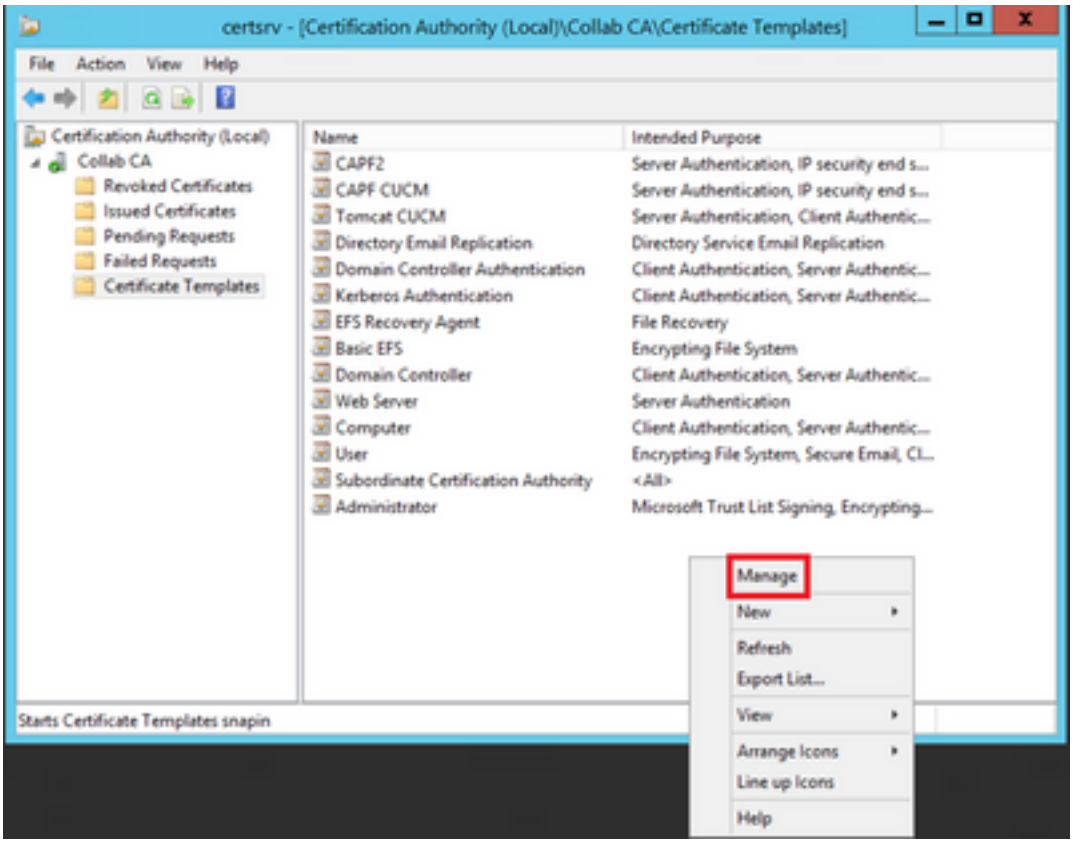
자세한 내용은 Cisco Unified Communications Manager 보안 가이드를 참조하십시오

구성

1단계. Windows Server에서 그림과 같이 **Server Manager > Tools > Certification Authority**로 이동합니다.



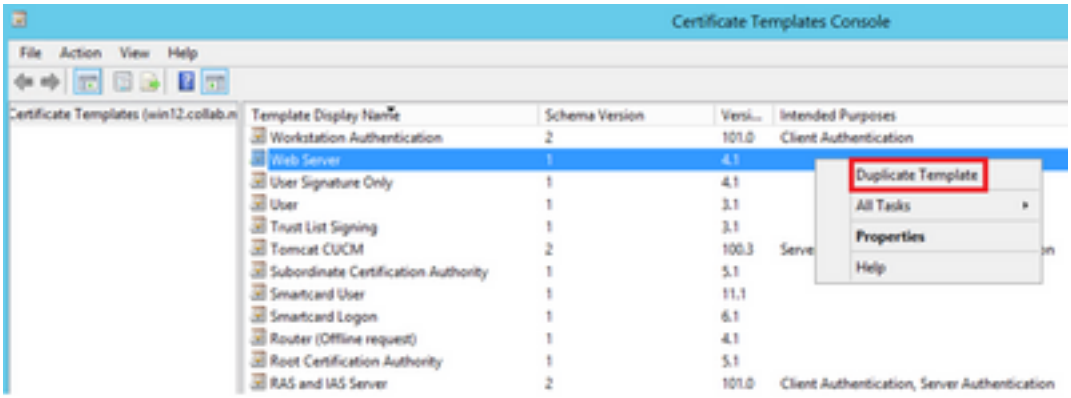
2단계. CA를 선택한 다음 **Certificate Templates(인증서 템플릿)**로 이동하여 목록을 마우스 오른쪽 버튼으로 클릭하고 Manage(**관리**)를 선택합니다(그림에 표시됨).



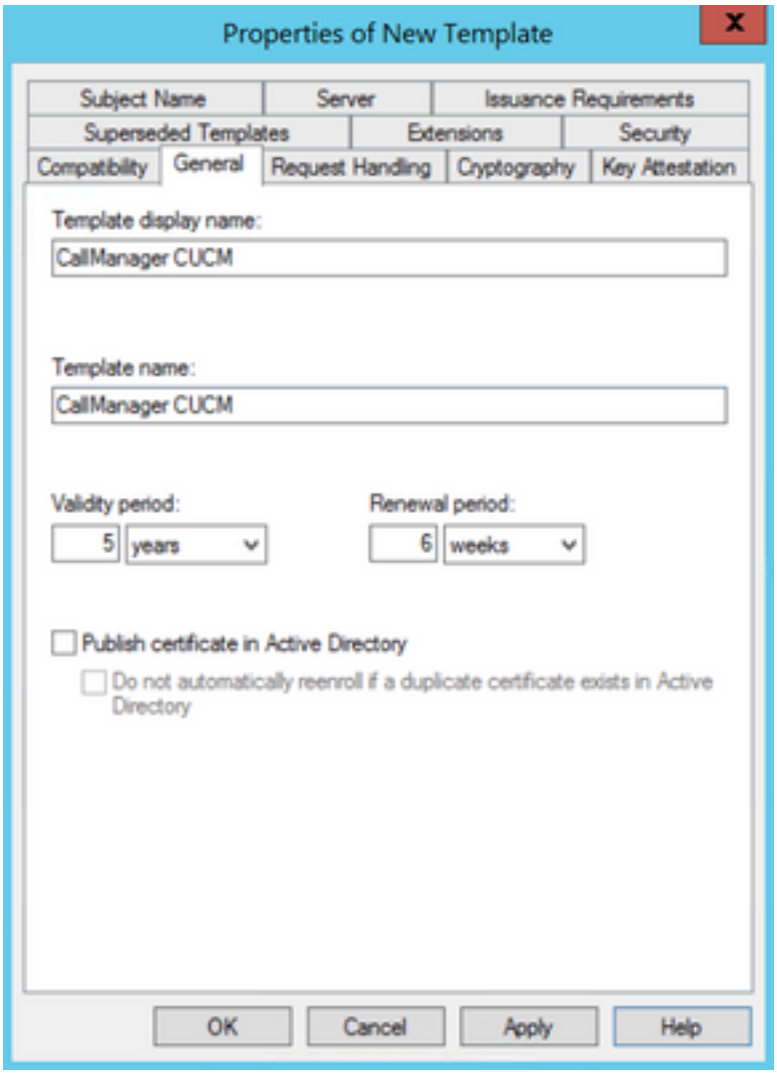
Callmanager/Tomcat/TVS 템플릿

다음 이미지는 CallManager 템플릿 생성만 표시하지만 동일한 단계를 수행하여 Tomcat 및 TVS 서비스에 대한 인증서 템플릿을 생성할 수 있습니다. 유일한 차이점은 2단계에서 각 새 템플릿에 대해 해당 서비스 이름이 사용되는지 확인하는 것입니다.

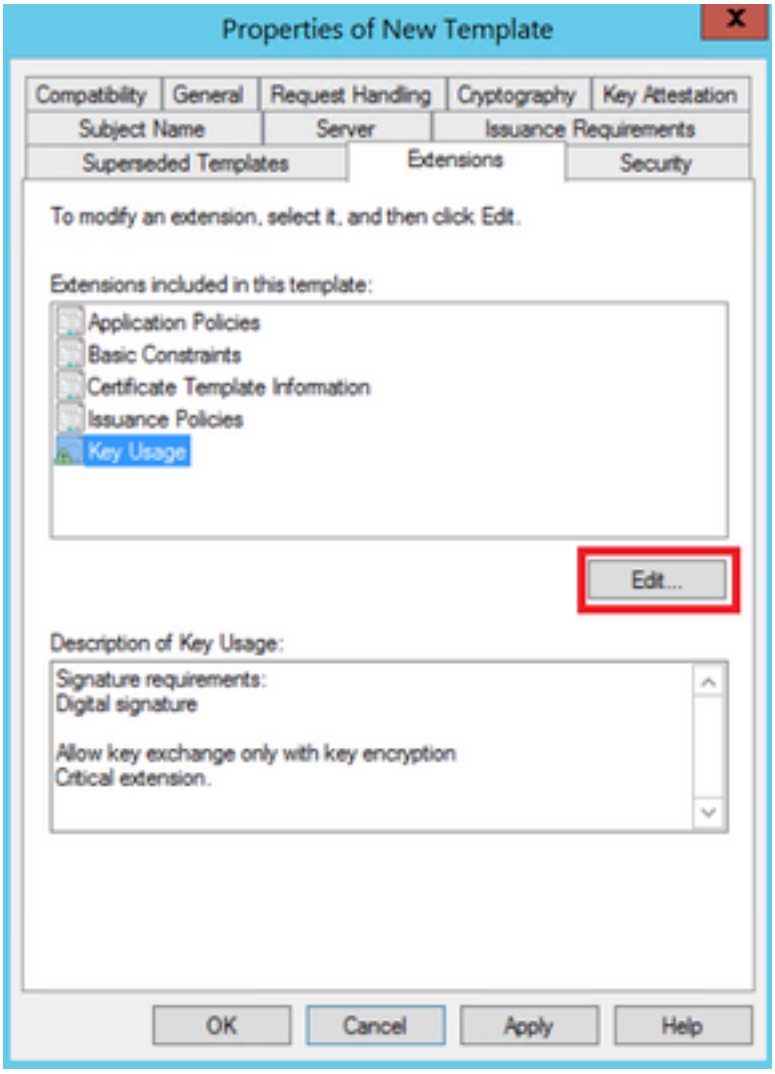
1단계. 그림과 같이 **웹 서버** 템플릿을 찾아 마우스 오른쪽 버튼으로 클릭하고 **Duplicate Template(템플릿 복제)**을 선택합니다.



2단계. **General(일반)**에서 인증서 템플릿의 이름, 표시 이름, 유효성 등을 변경할 수 있습니다.

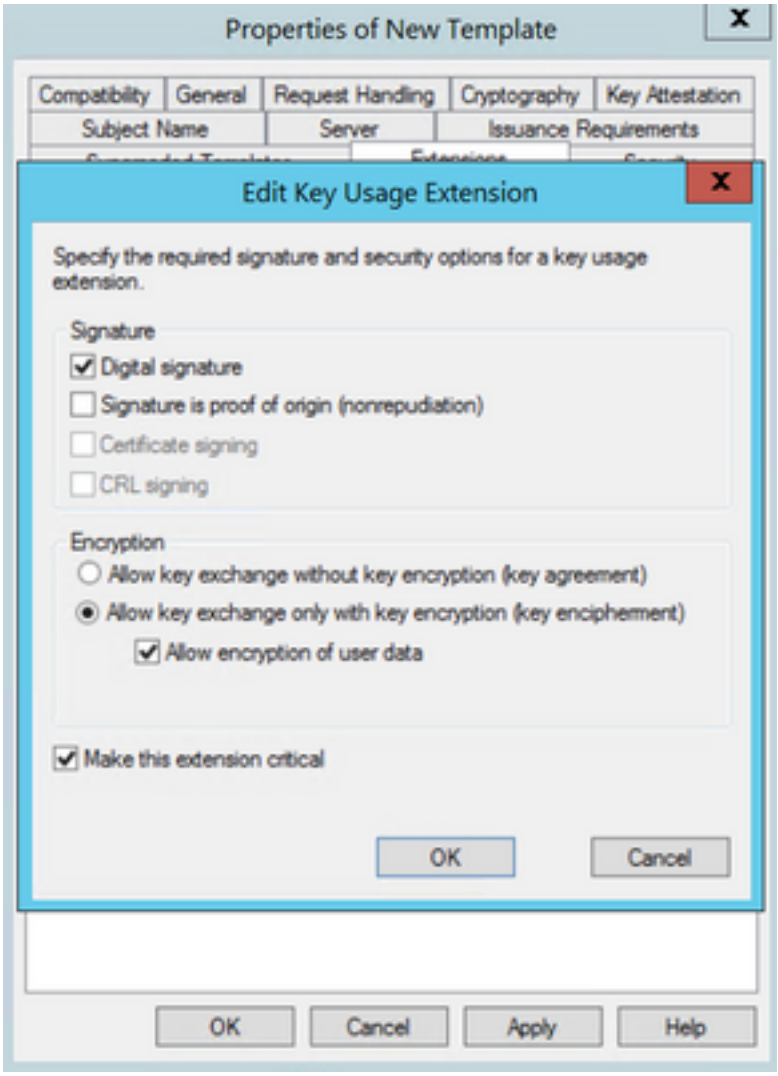


3단계. 이미지에 표시된 대로 **Extensions(확장) > Key Usage(키 사용) > Edit(편집)**로 이동합니다.

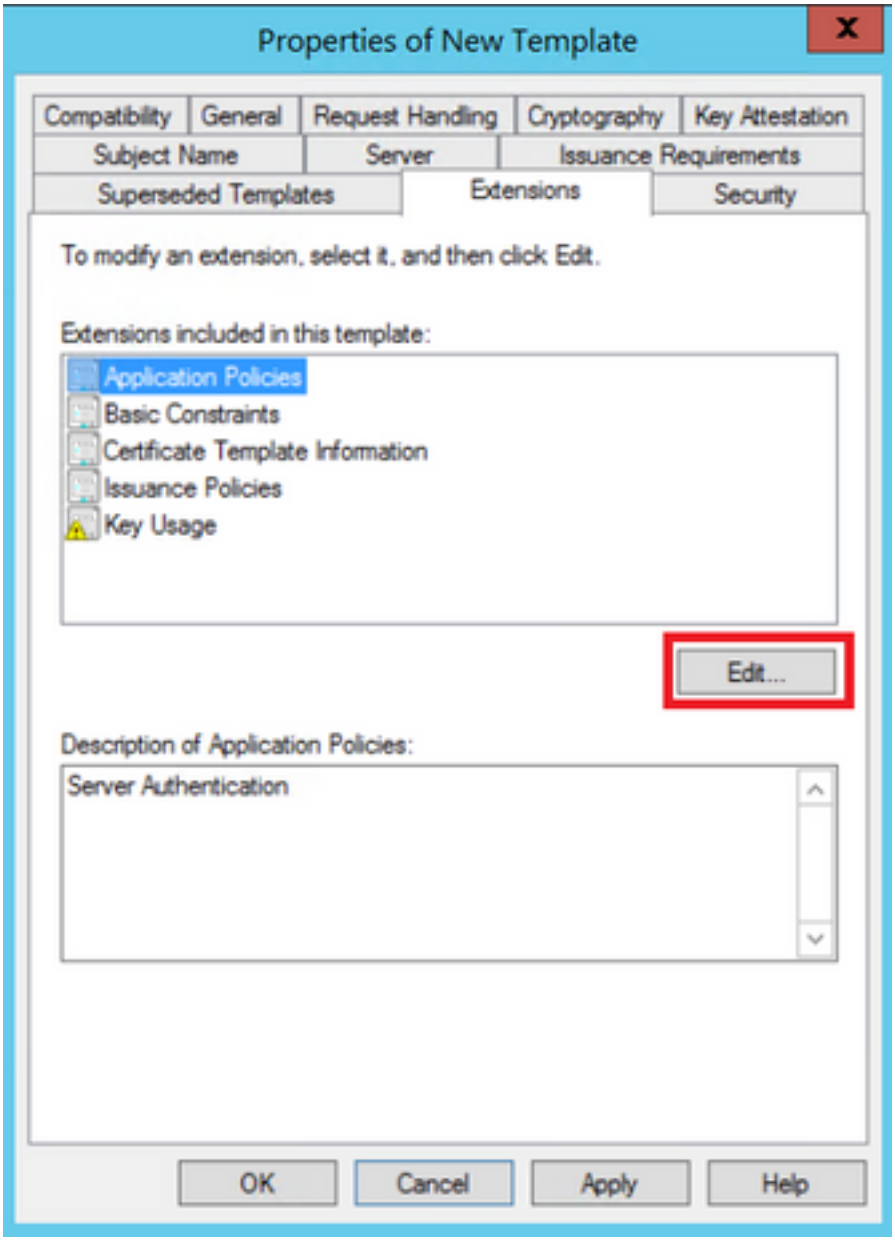


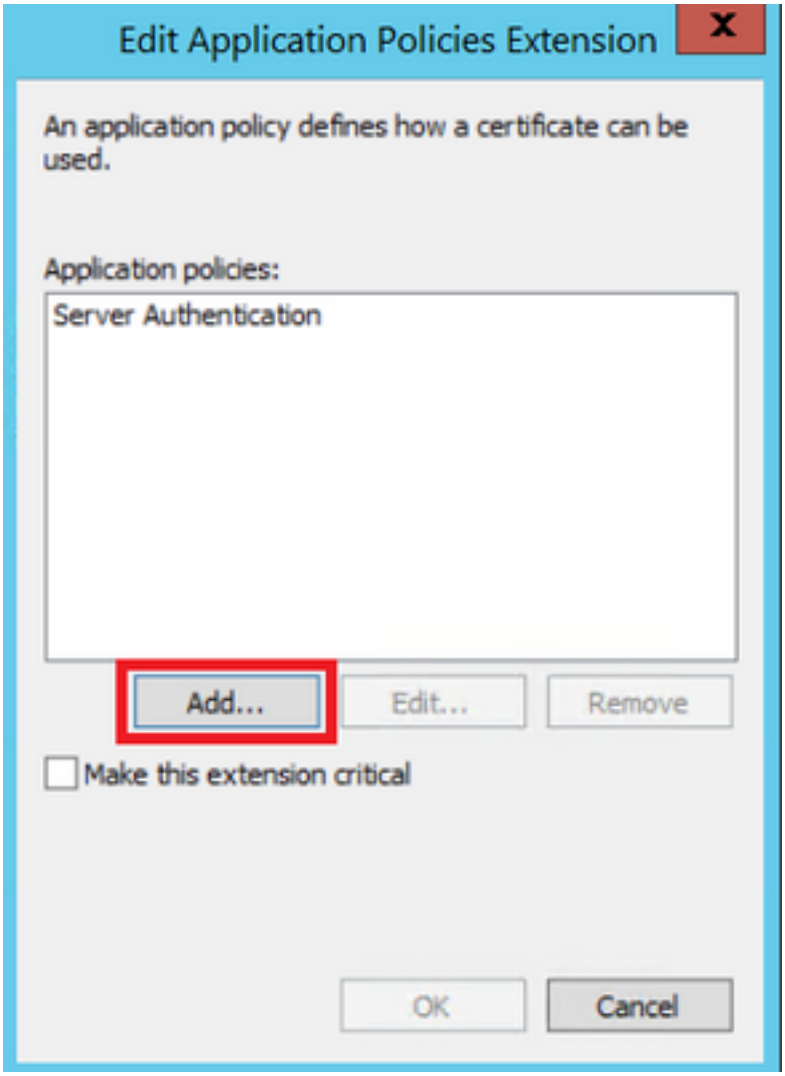
4단계. 이 옵션을 선택하고 이미지에 표시된 대로 **OK**(확인)를 선택합니다.

- **디지털 서명**
- **키 암호화(키 암호화)를 사용하는 키 교환만 허용**
- **사용자 데이터의 암호화 허용**

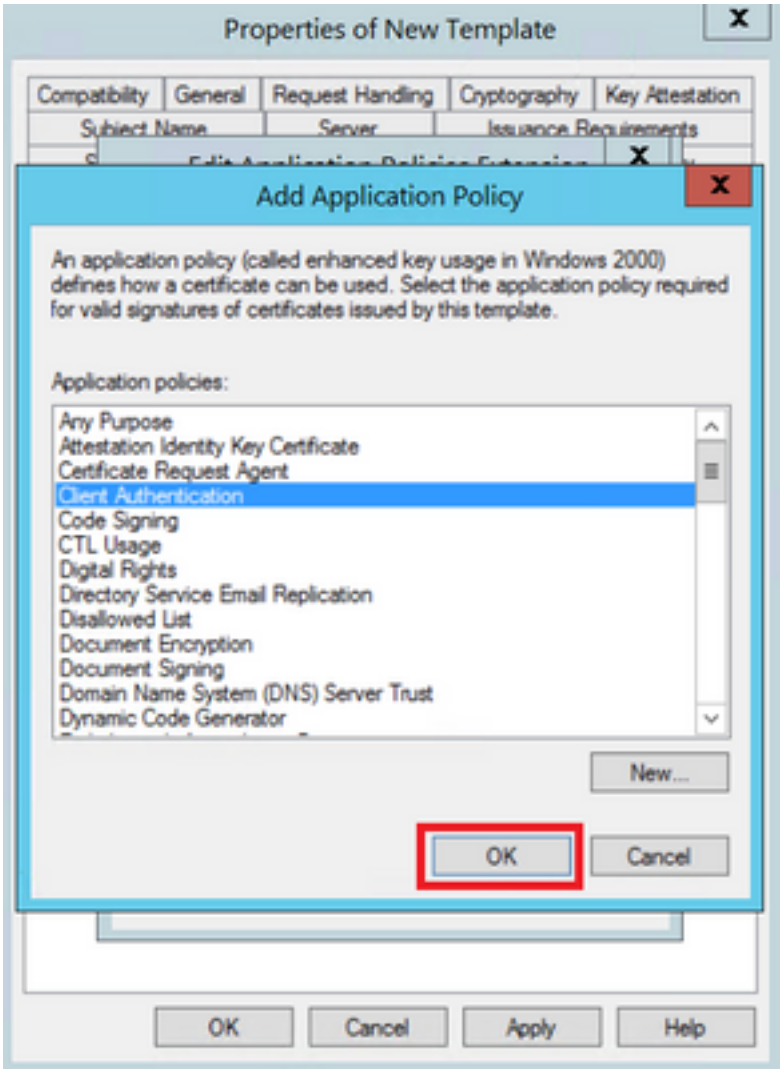


5단계. 이미지에 표시된 대로 **Extensions(확장) > Application Policies(애플리케이션 정책) > Edit(편집) > Add(추가)**로 이동합니다.

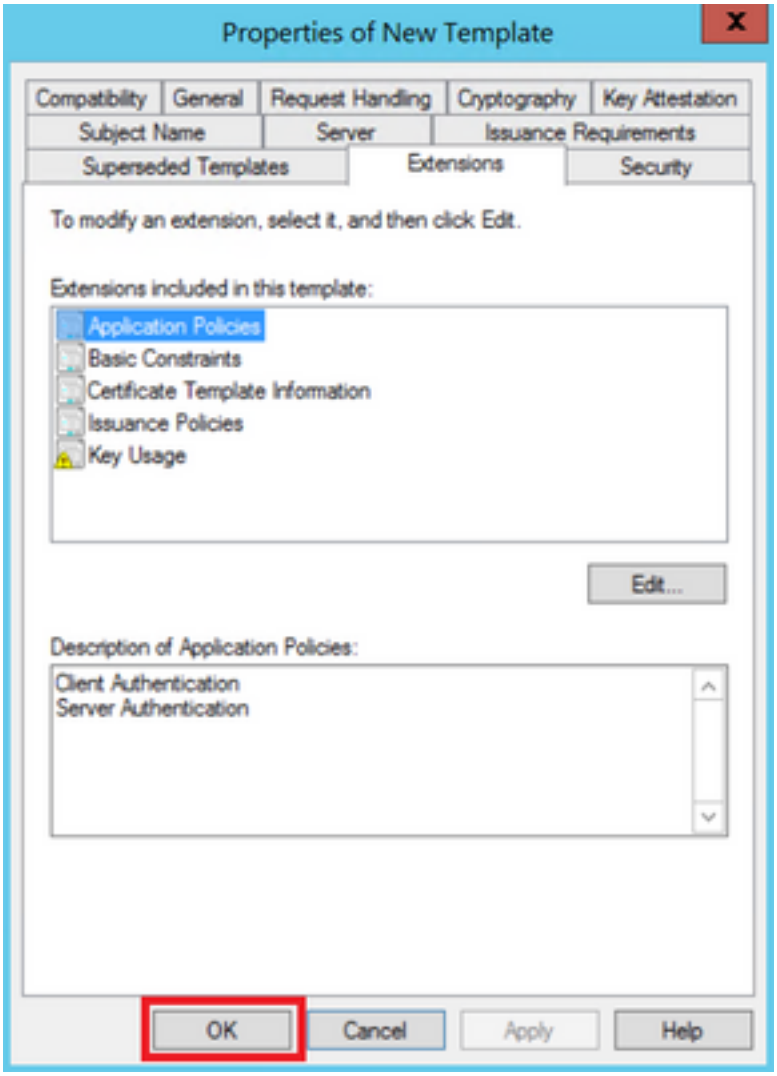

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



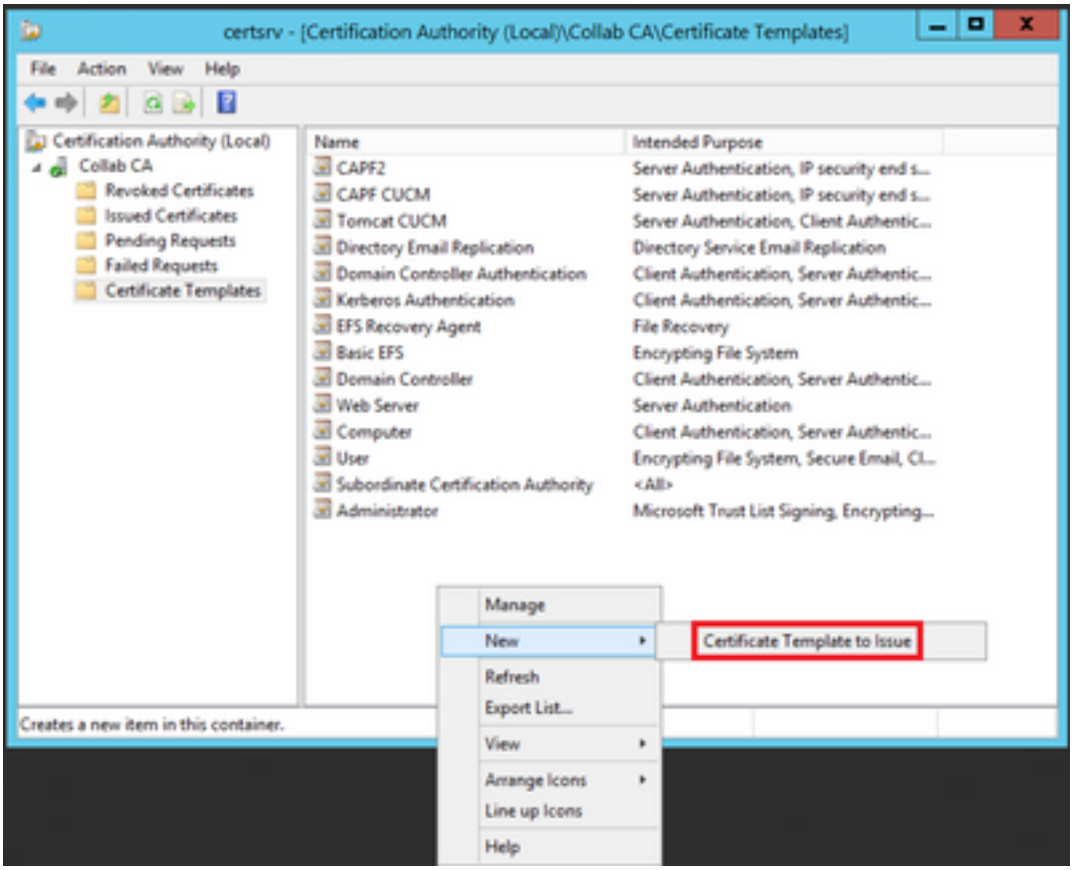
6단계. 이미지에 표시된 대로 **클라이언트 인증**을 검색하고 선택한 다음 이 창과 이전 창에서 모두 확인을 **선택합니다**.



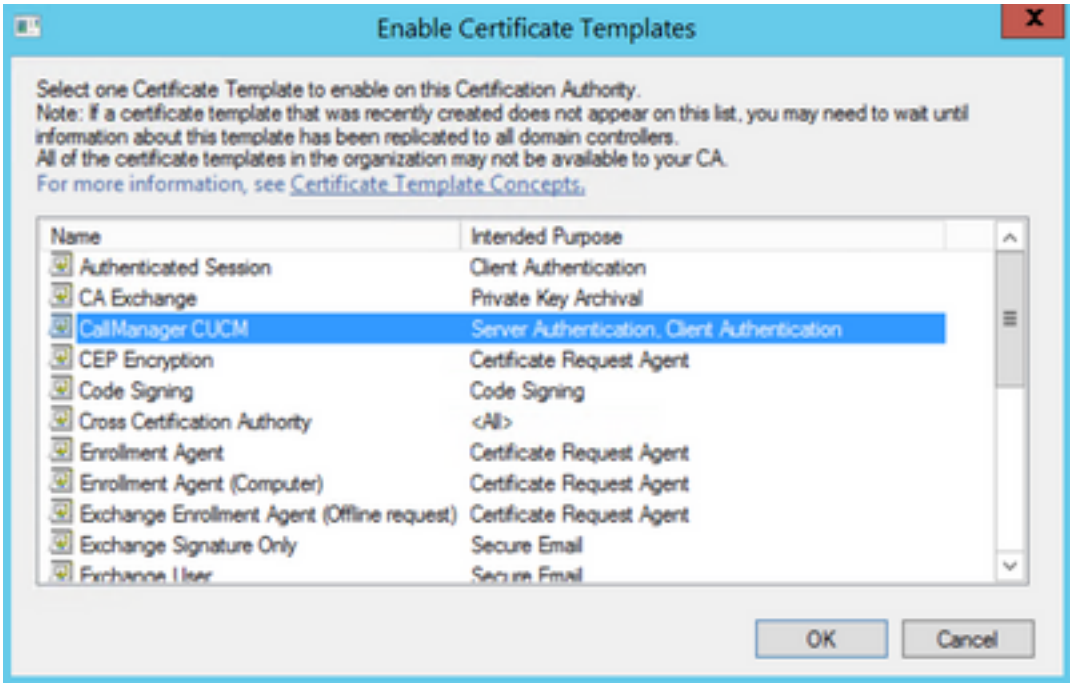
7단계. 템플릿으로 돌아가서 Apply(적용)와 **OK(확인)**를 차례로 선택합니다.



8단계. Certificate **Template Console(인증서 템플릿 콘솔)** 창을 닫고 맨 첫 번째 창으로 돌아와서 이미지에 표시된 대로 **New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)**로 이동합니다.



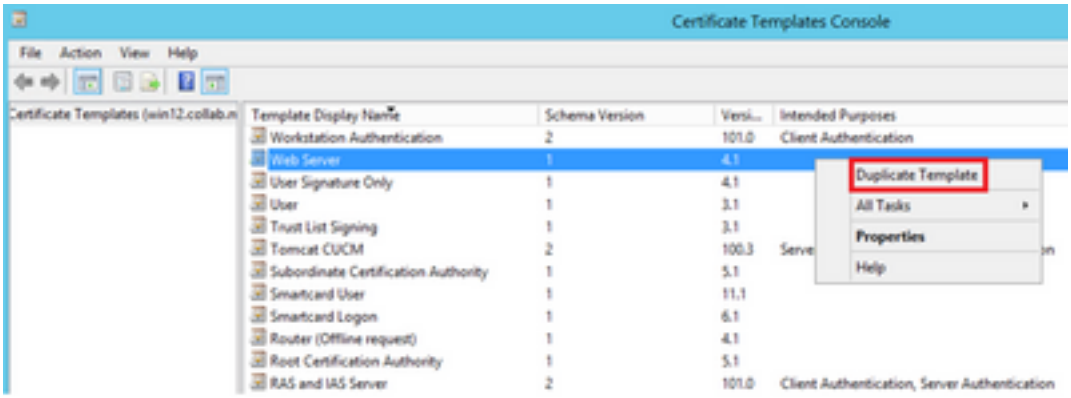
9단계. 새 CallManager **CUCM 템플릿**을 선택하고 이미지와 같이 **OK**(확인)를 선택합니다.



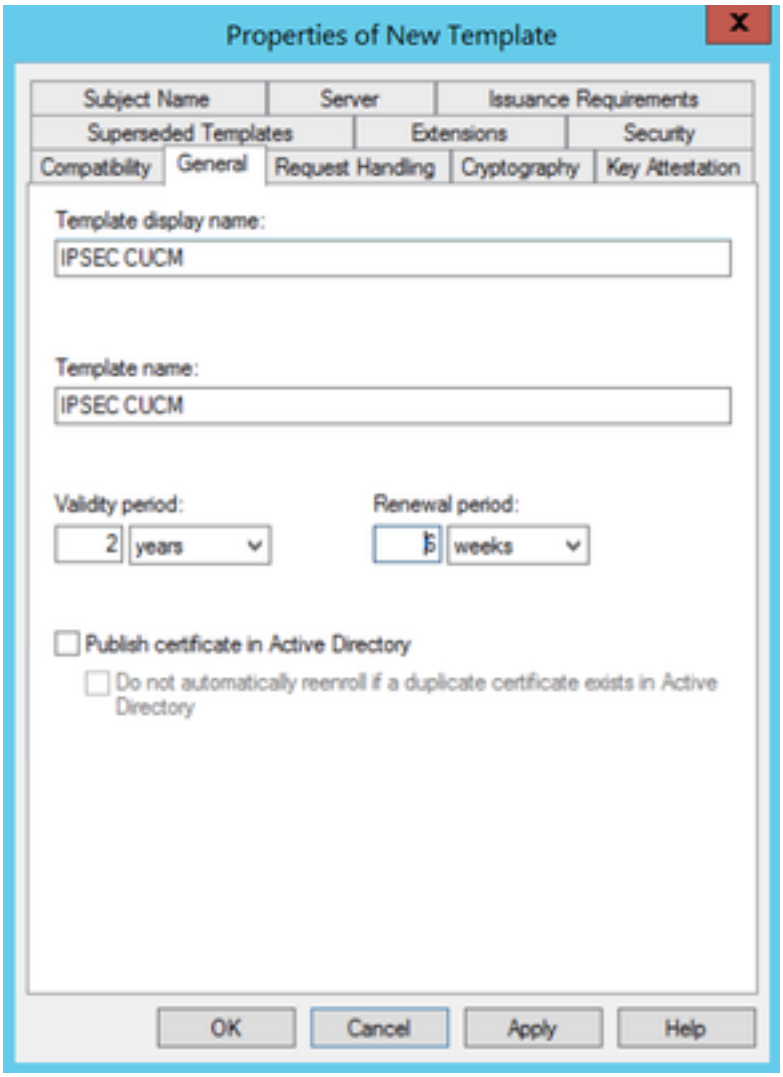
10단계. 이전 단계를 모두 반복하여 필요에 따라 Tomcat 및 TVS 서비스에 대한 인증서 템플릿을 생성합니다.

IPsec 템플릿

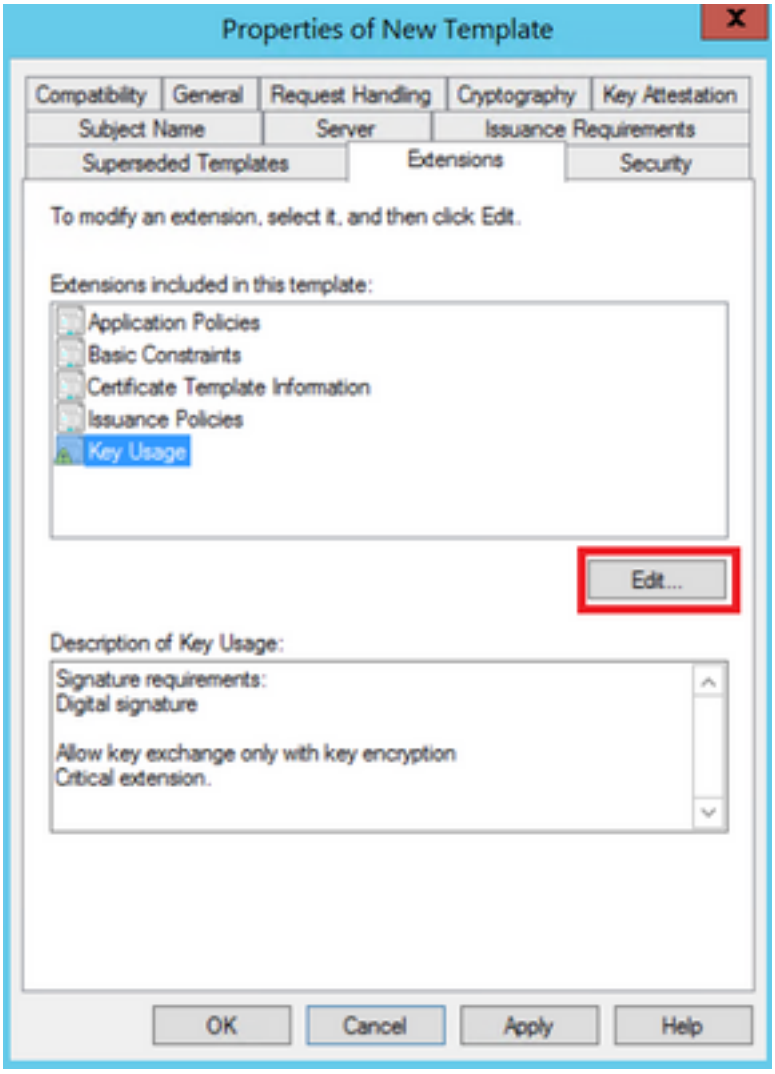
1단계. 그림과 같이 **웹 서버** 템플릿을 찾아 마우스 오른쪽 버튼으로 클릭하고 **Duplicate** Template을 선택합니다.



2단계. **General(일반)**에서 인증서 템플릿의 이름, 표시 이름, 유효성 등을 변경할 수 있습니다.

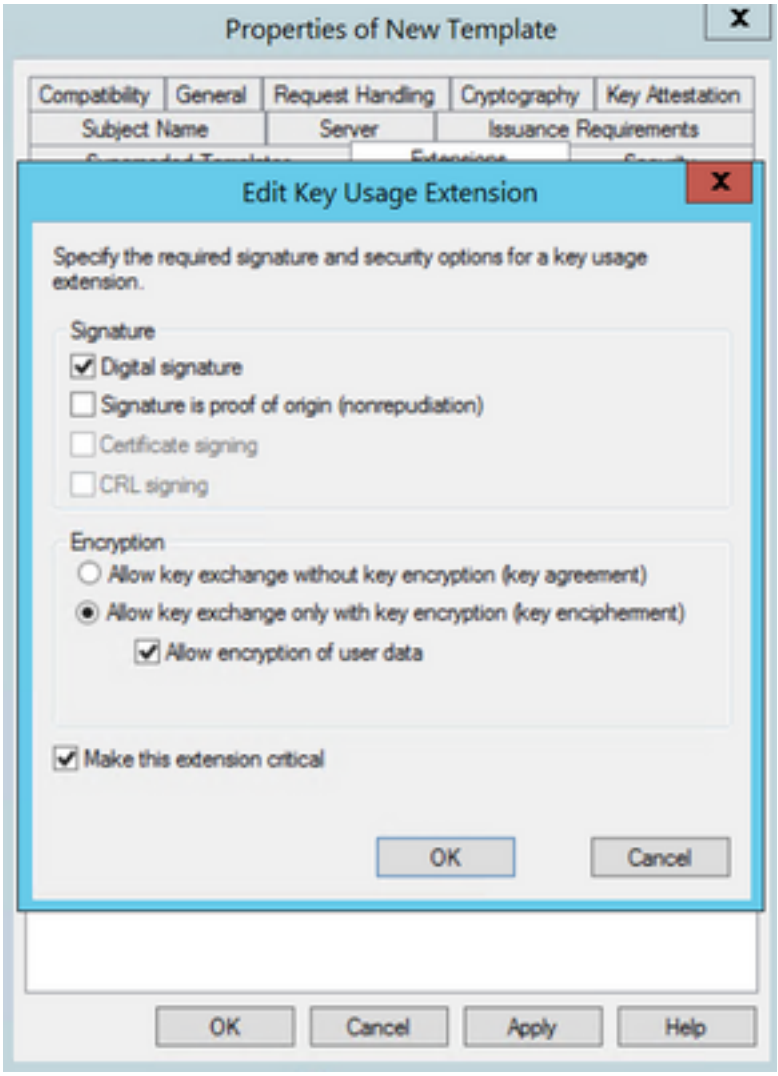


3단계. 이미지에 표시된 대로 **Extensions(확장) > Key Usage(키 사용) > Edit(편집)**로 이동합니다.

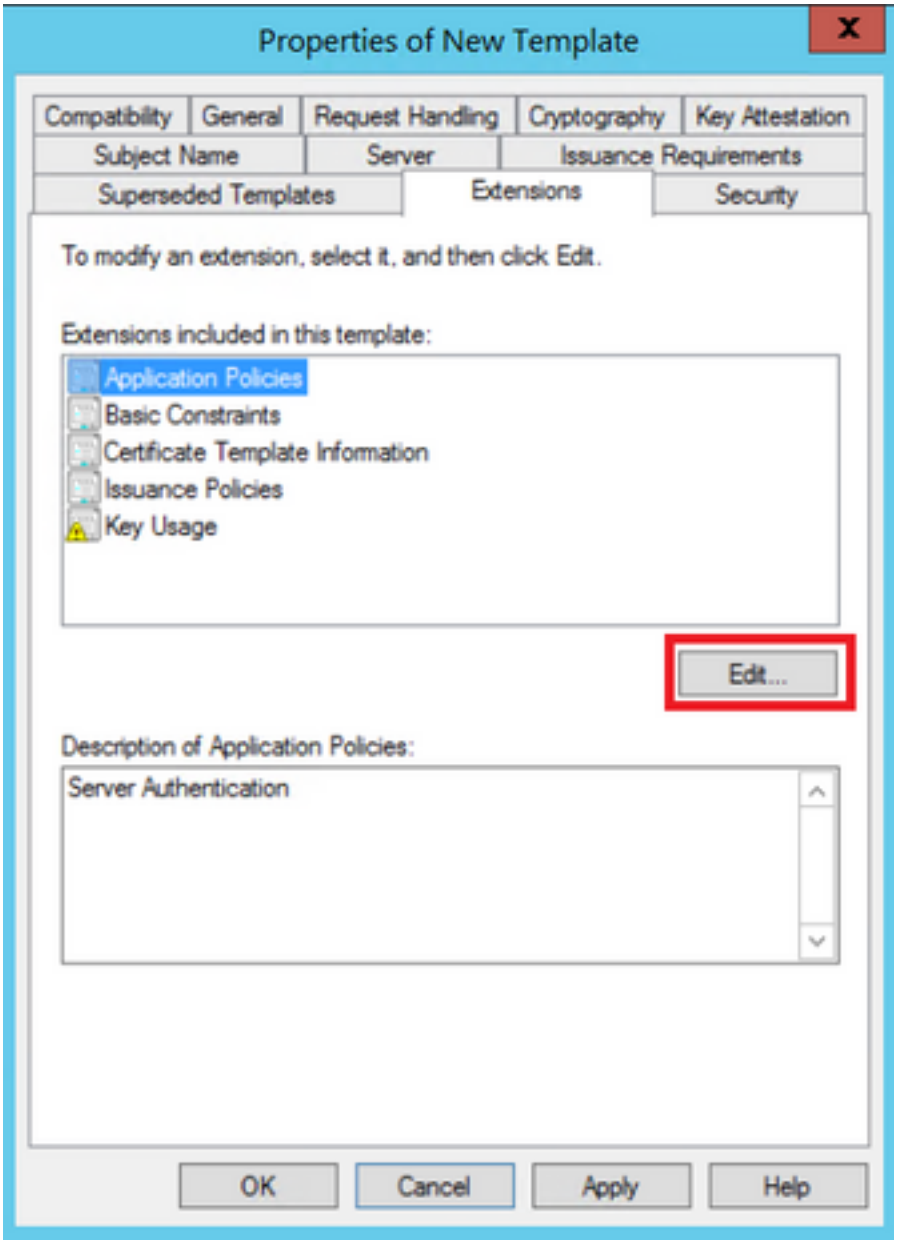


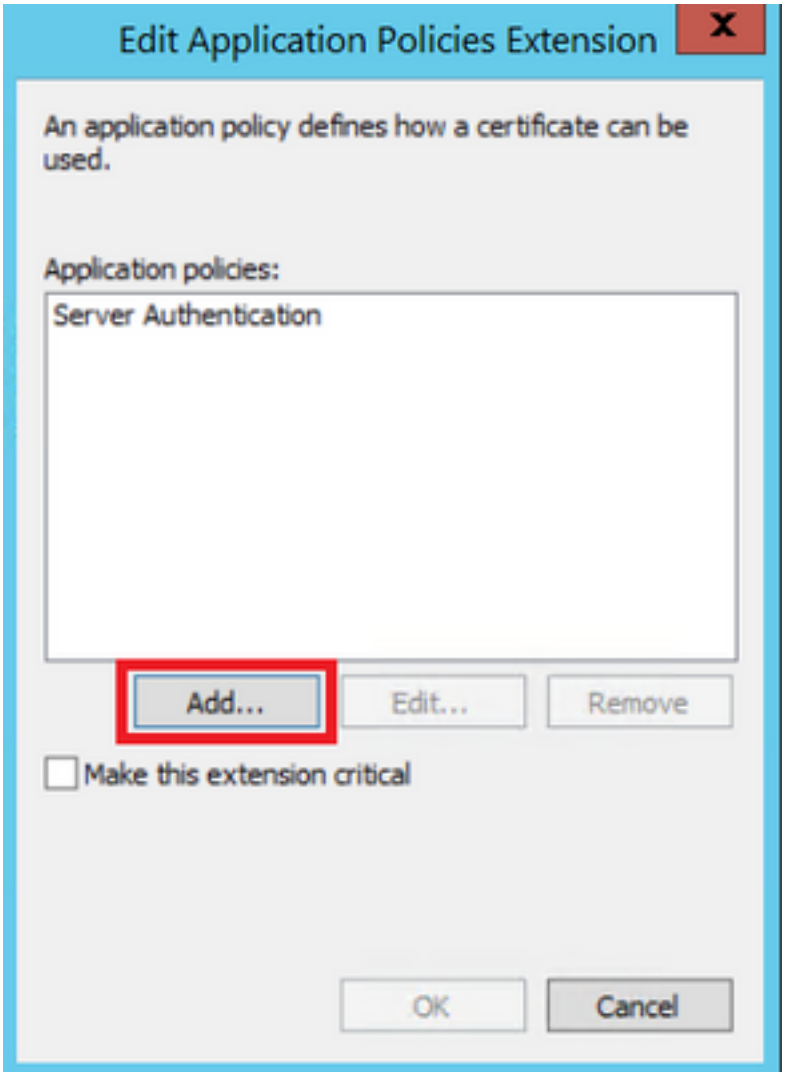
4단계. 이 옵션을 선택하고 이미지에 표시된 대로 **OK**(확인)를 선택합니다.

- **디지털 서명**
- **키 암호화(키 암호화)를 사용하는 키 교환만 허용**
- **사용자 데이터의 암호화 허용**

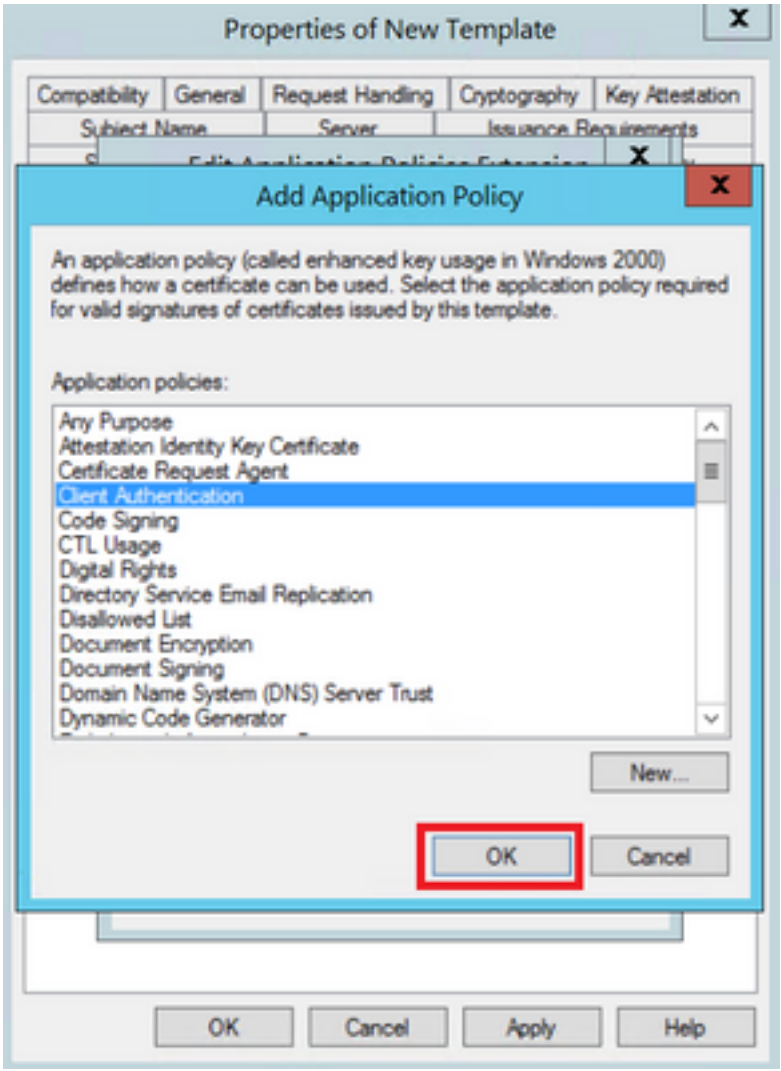


5단계. 이미지에 표시된 대로 **Extensions(확장) > Application Policies(애플리케이션 정책) > Edit(편집) > Add(추가)**로 이동합니다.

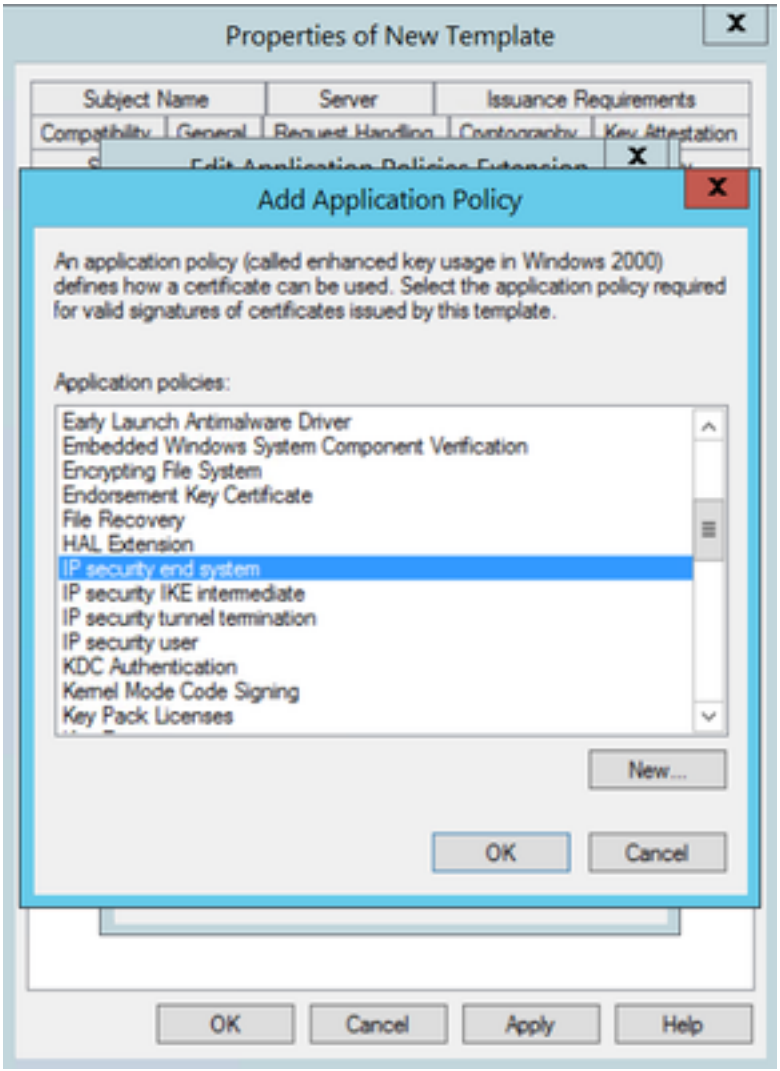

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



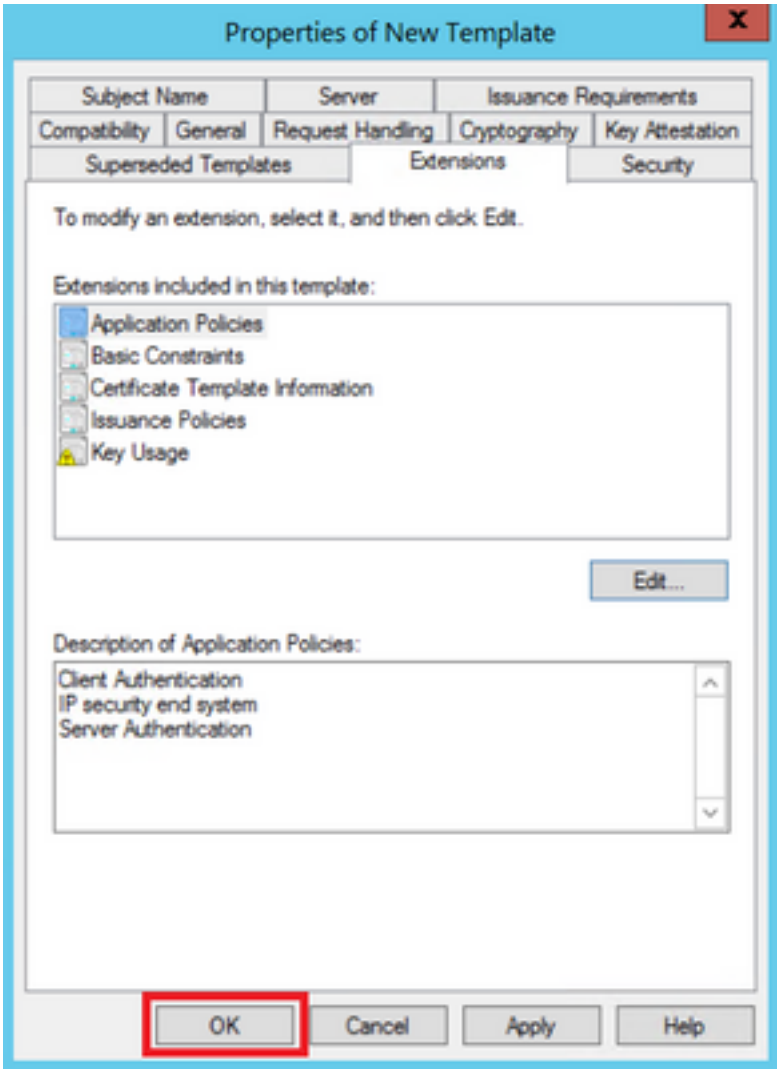
6단계. 이미지에 표시된 대로 **클라이언트 인증**을 검색하고 선택한 다음 **확인**을 누릅니다.



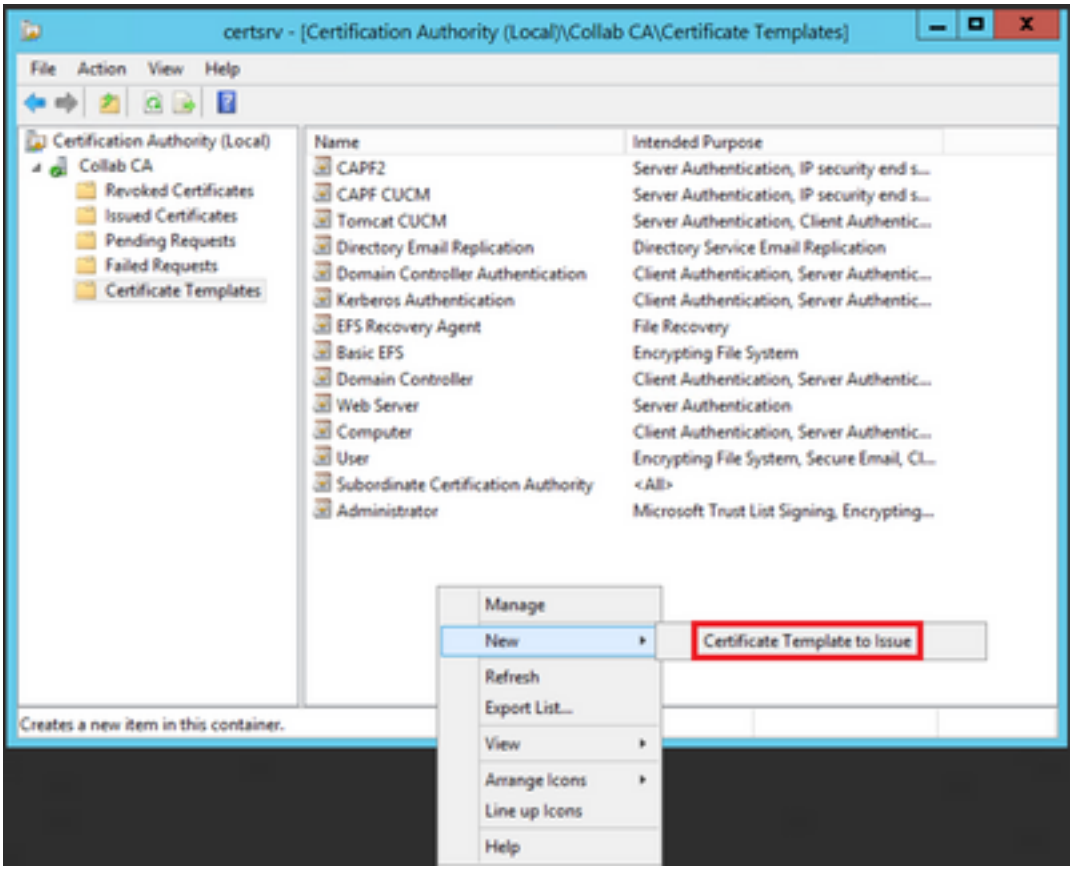
7단계. Add(**추가**)를 다시 선택하고 **IP 보안 최종 시스템**을 검색하여 선택한 다음 이 창과 이전 창에서도 **OK(확인)**를 선택합니다.



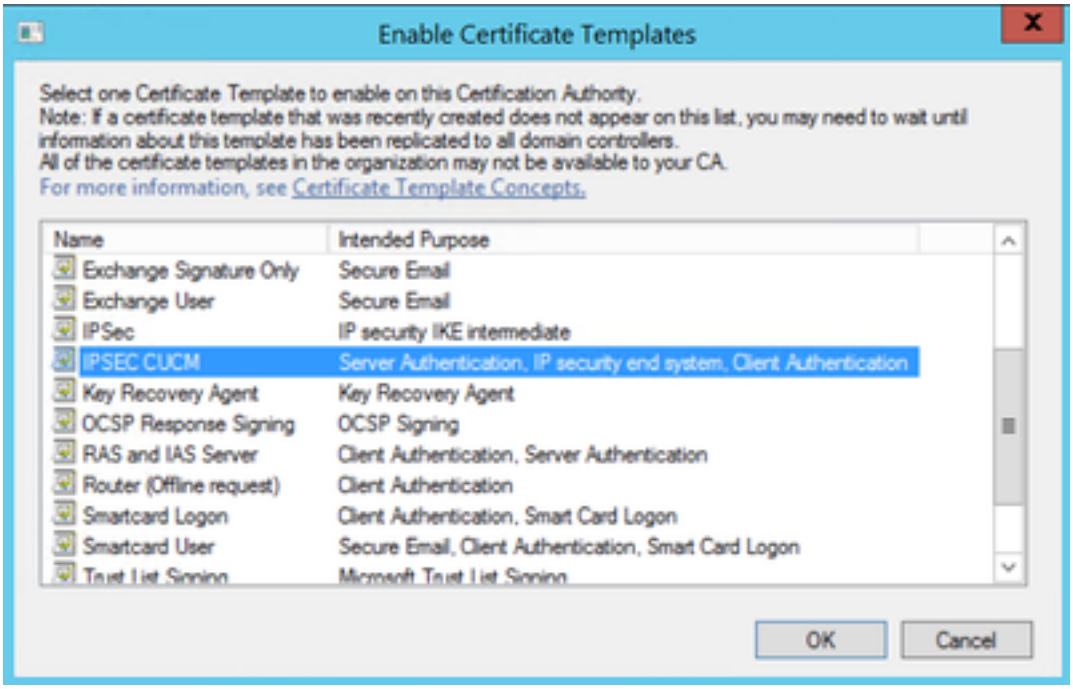
8단계. 그림과 같이 템플릿에서 **적용**, **확인** 순으로 선택합니다.



9단계. Certificate Templates **Console 창**을 닫고 맨 첫 번째 창으로 돌아와서 이미지에 표시된 대로 **New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)**로 이동합니다.

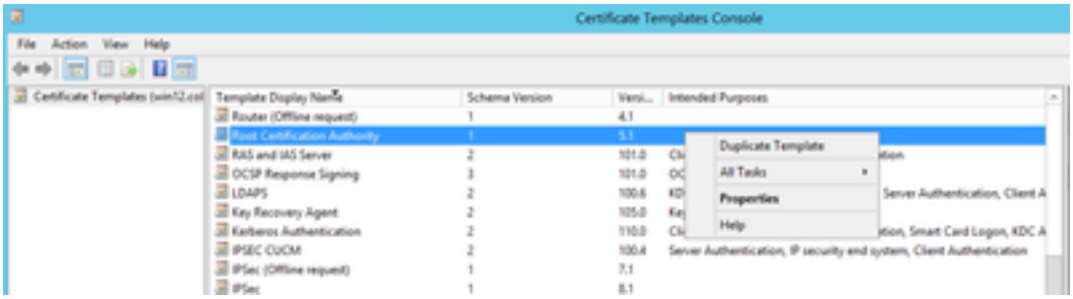


10단계. 새 IPSEC **CUCM 템플릿**을 선택하고 그림과 같이 **OK**(확인)를 선택합니다.



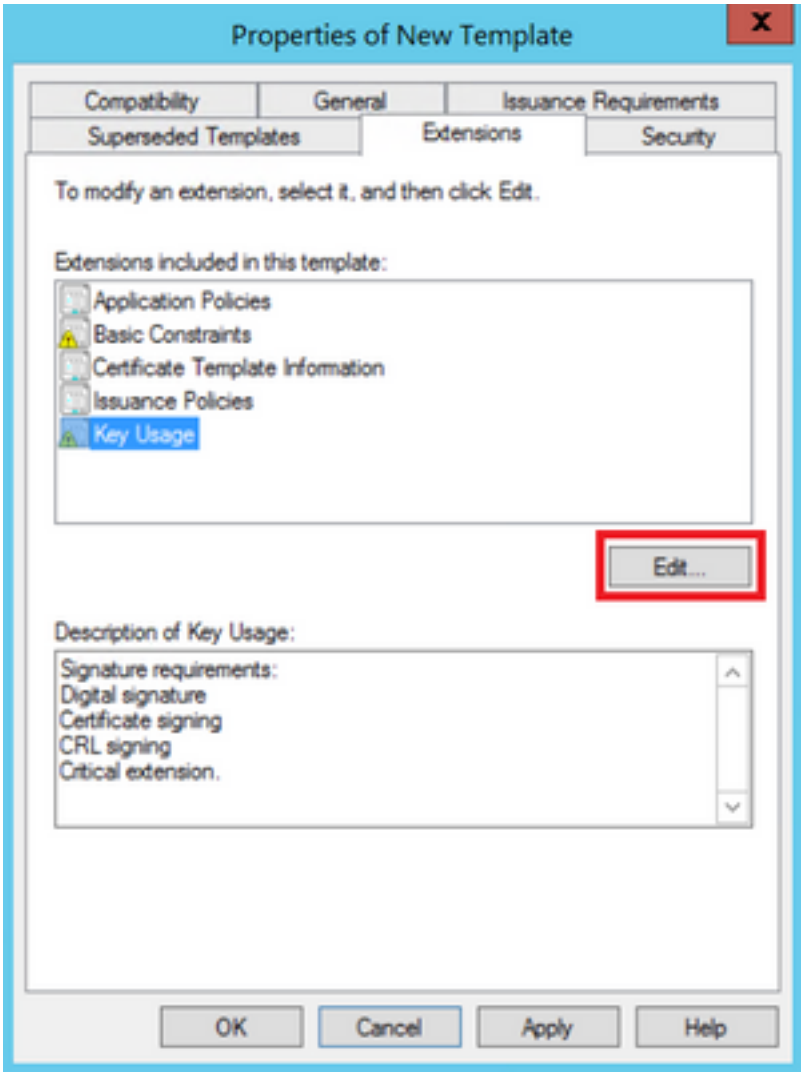
CAPF 템플릿

1단계. 루트 **CA 템플릿**을 찾아 마우스 오른쪽 버튼으로 클릭합니다. 그런 다음 **이미지**에 표시된 대로 Duplicate Template(템플릿 복제)을 선택합니다.



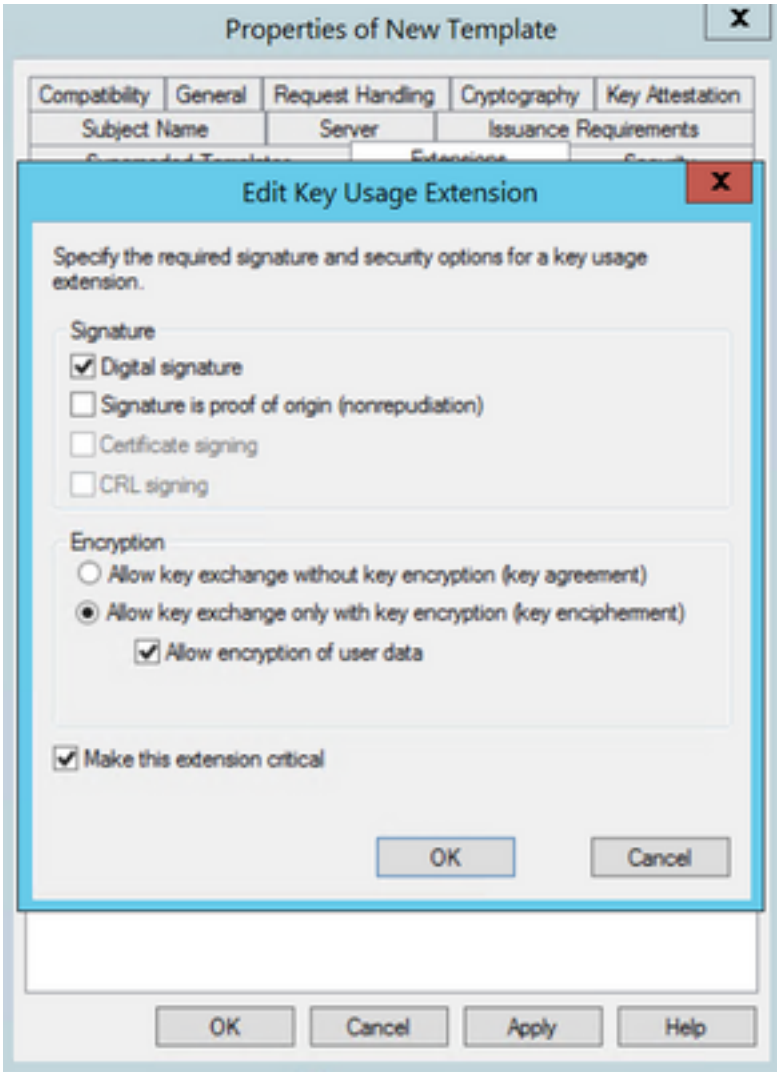
2단계. **General(일반)**에서 인증서 템플릿의 이름, 표시 이름, 유효성 등을 변경할 수 있습니다.

3단계. 이미지에 표시된 대로 **Extensions(확장) > Key Usage(키 사용) > Edit(편집)**로 이동합니다.

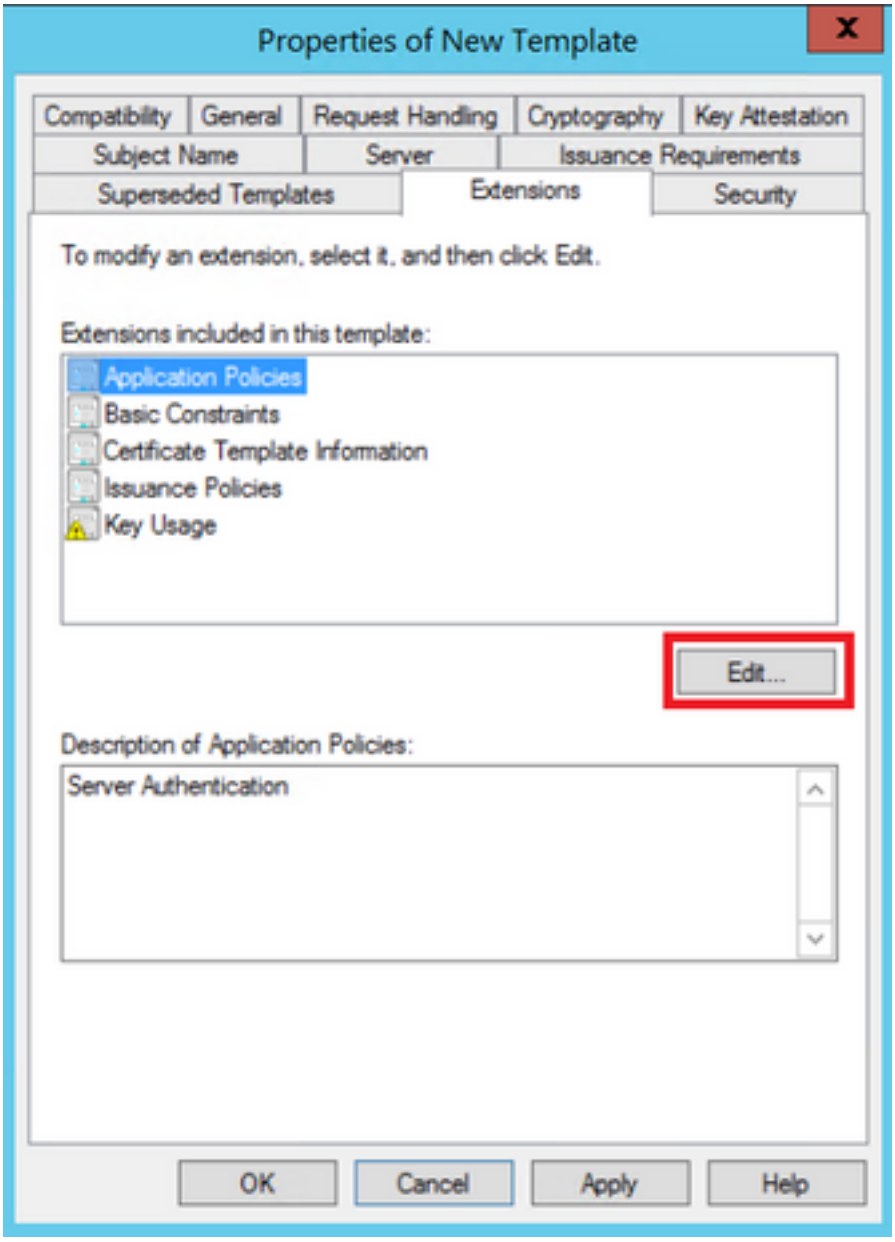


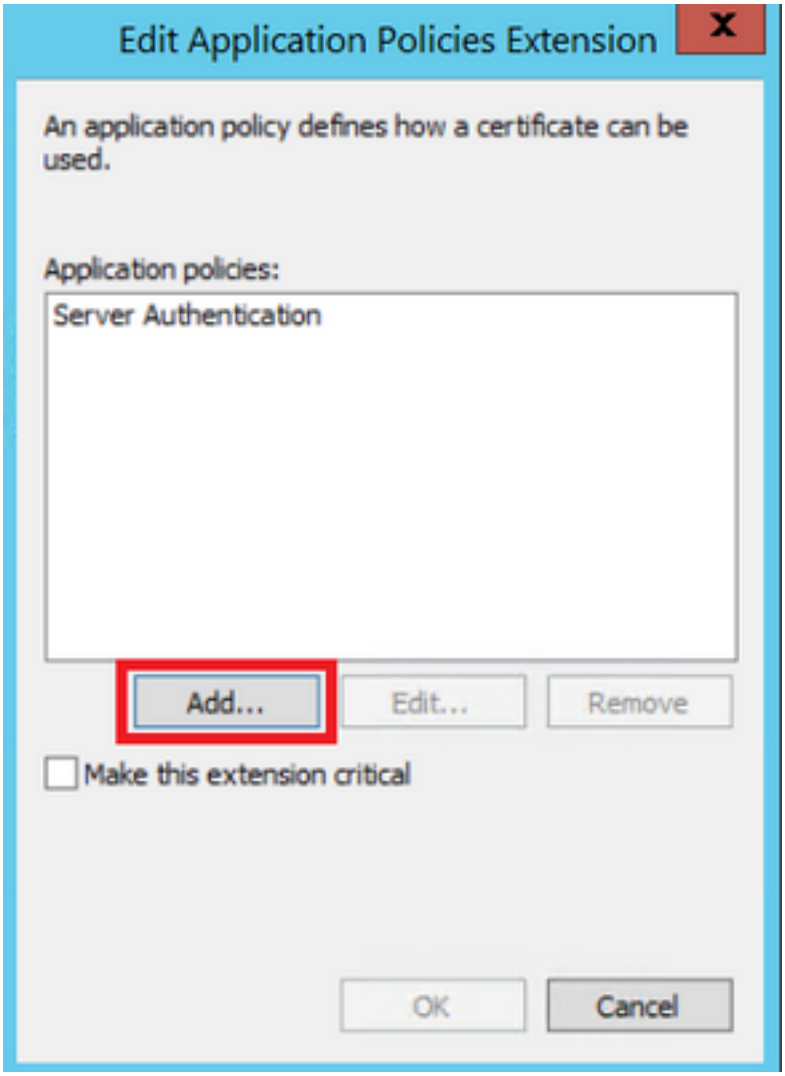
4단계. 이 옵션을 선택하고 이미지에 표시된 대로 **OK**(확인)를 선택합니다.

- **디지털 서명**
- **인증서 서명**
- **CRL 서명**

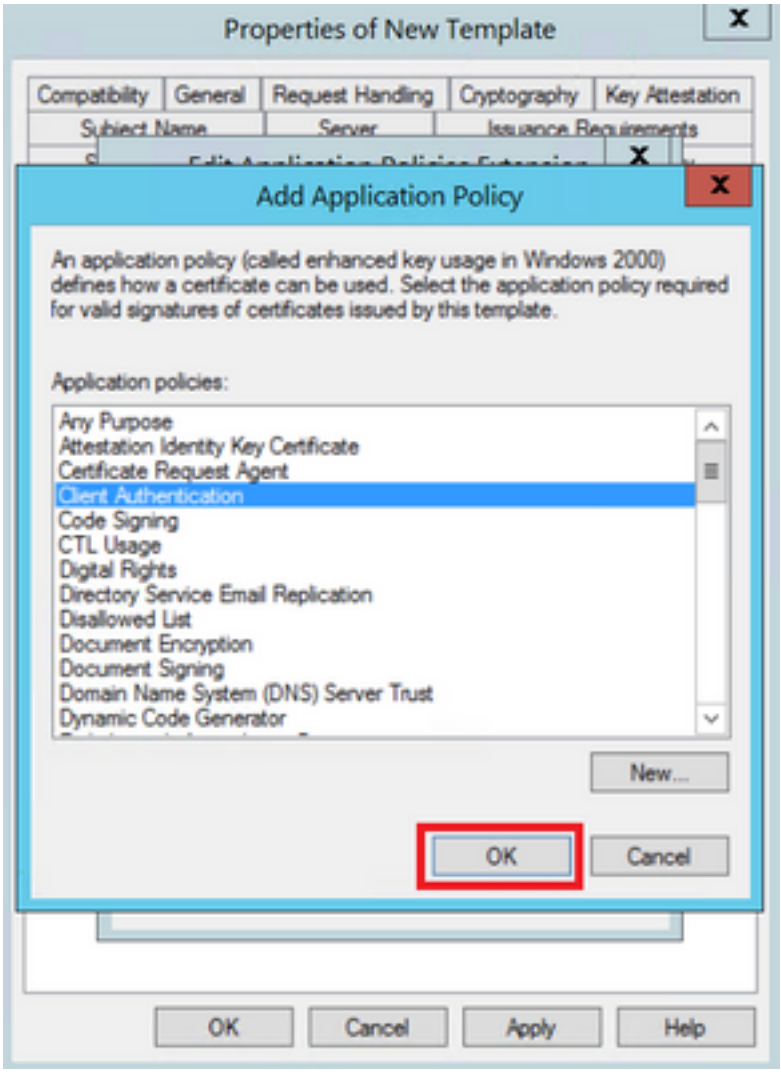


5단계. 이미지에 표시된 대로 **Extensions(확장) > Application Policies(애플리케이션 정책) > Edit(편집) > Add(추가)**로 이동합니다.

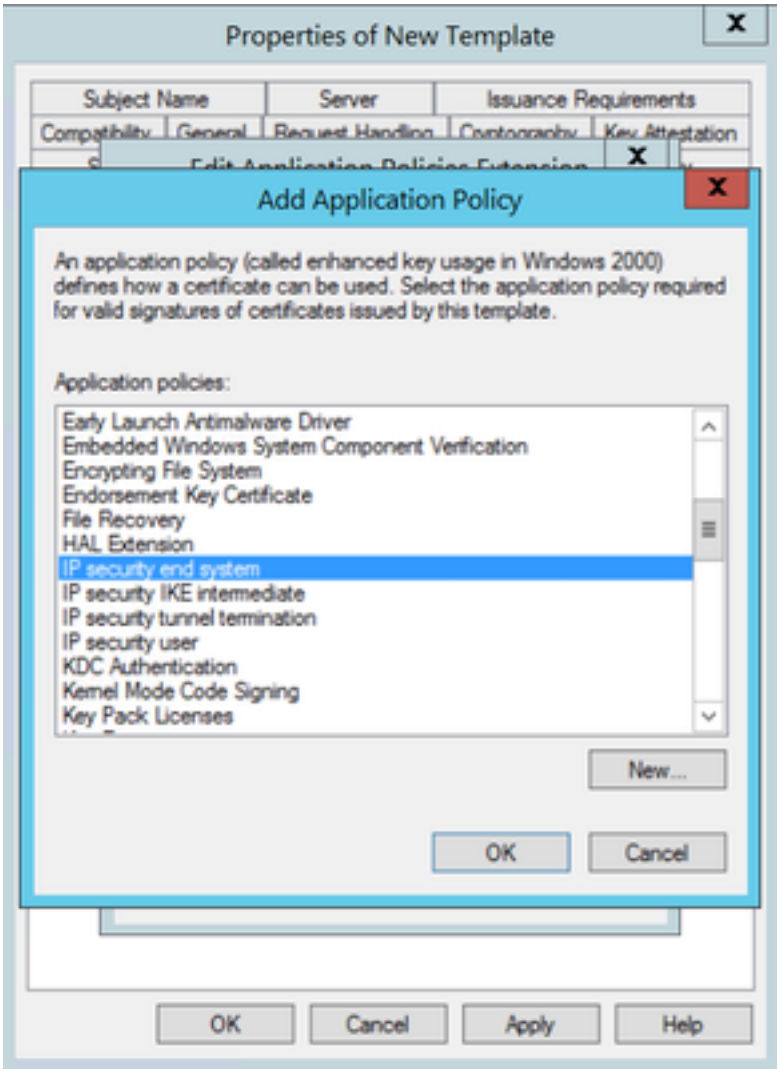

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints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



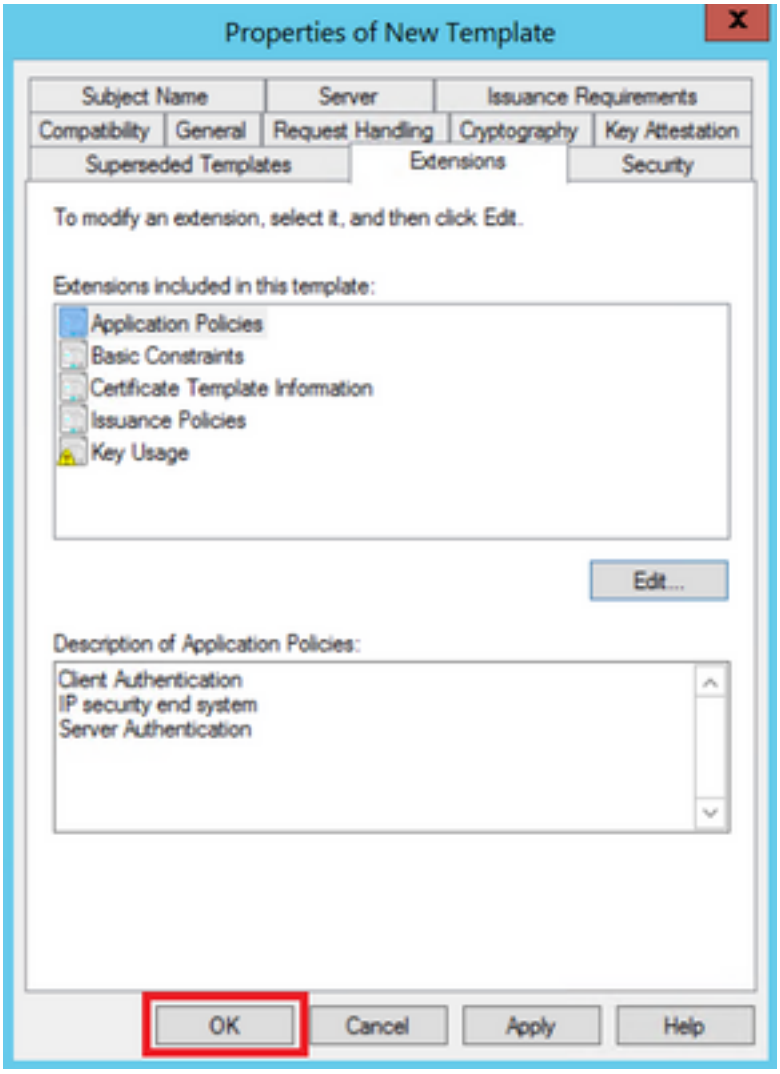
6단계. 이미지에 표시된 대로 **클라이언트 인증**을 검색하여 선택한 다음 **확인**을 선택합니다.



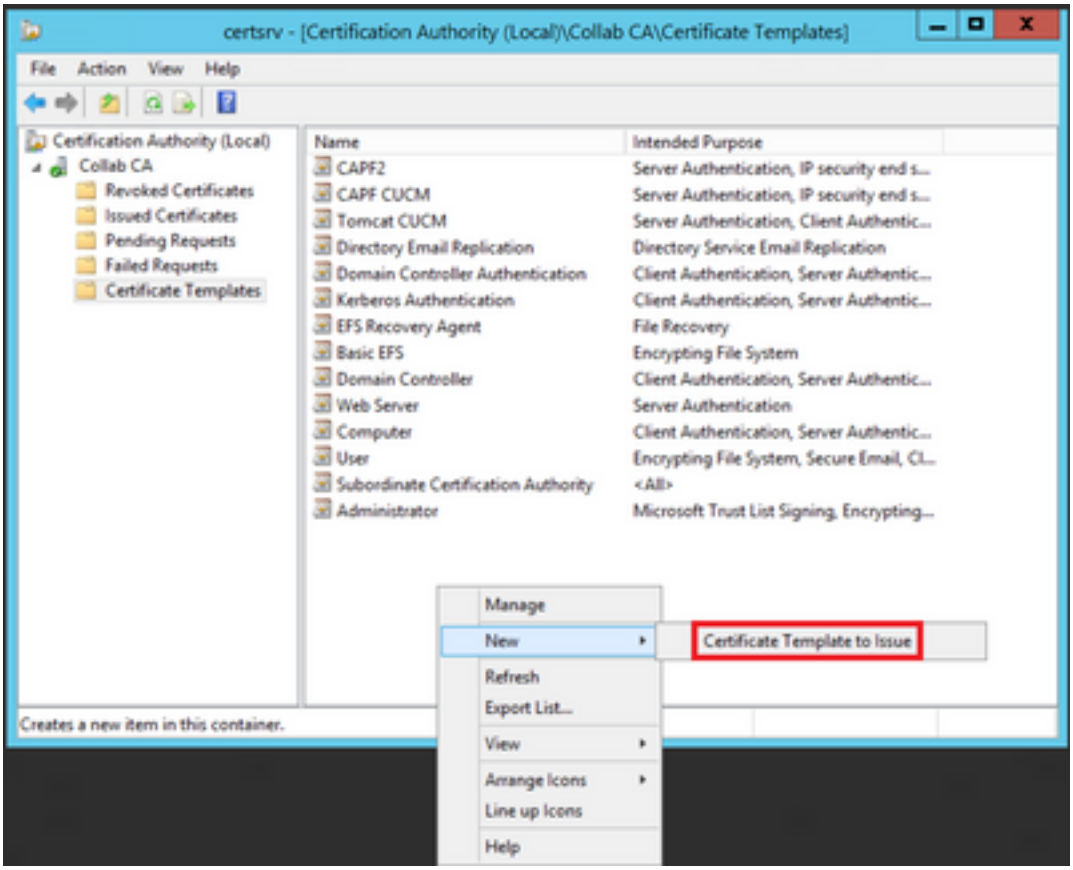
7단계. 이미지와 같이 **Add**(추가)를 다시 선택하고 **IP Security End System(IP 보안 최종 시스템)**을 검색하여 선택한 다음 이 창과 이전 창에서도 OK(확인)를 선택합니다.



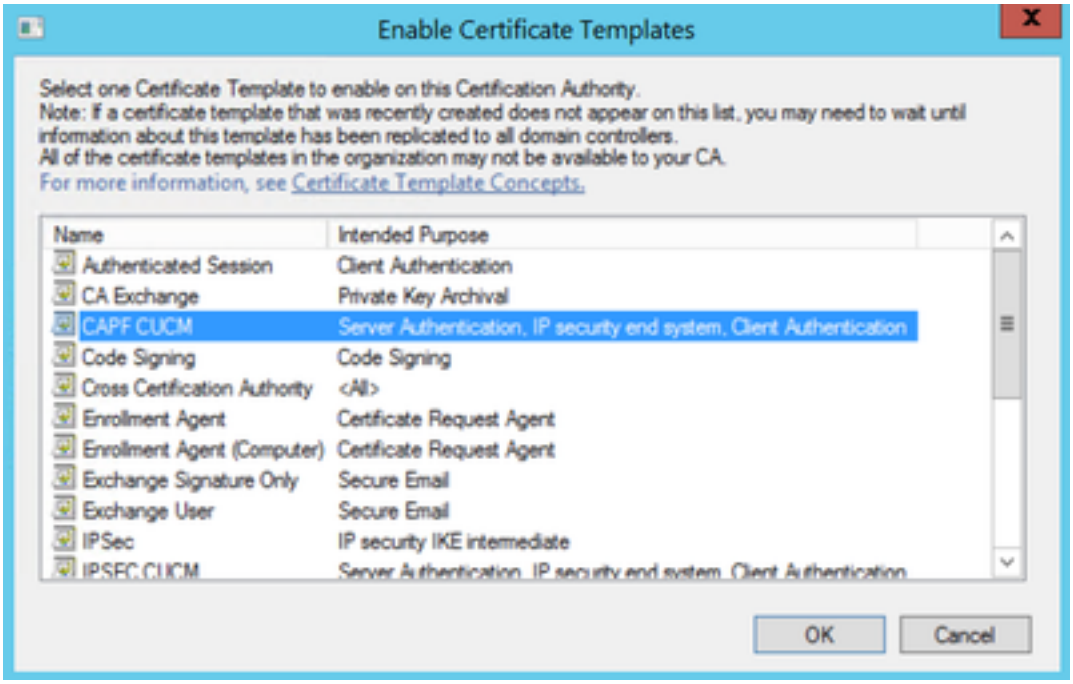
8단계. 그림과 같이 템플릿에서 **적용**, **확인** 순으로 선택합니다.



9단계. Certificate Templates **Console 창**을 닫고 맨 첫 번째 창으로 돌아와서 이미지에 표시된 대로 **New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)**로 이동합니다.



10단계. 새 CAPF CUCM **템플릿**을 선택하고 그림과 같이 **OK**(확인)를 선택합니다.



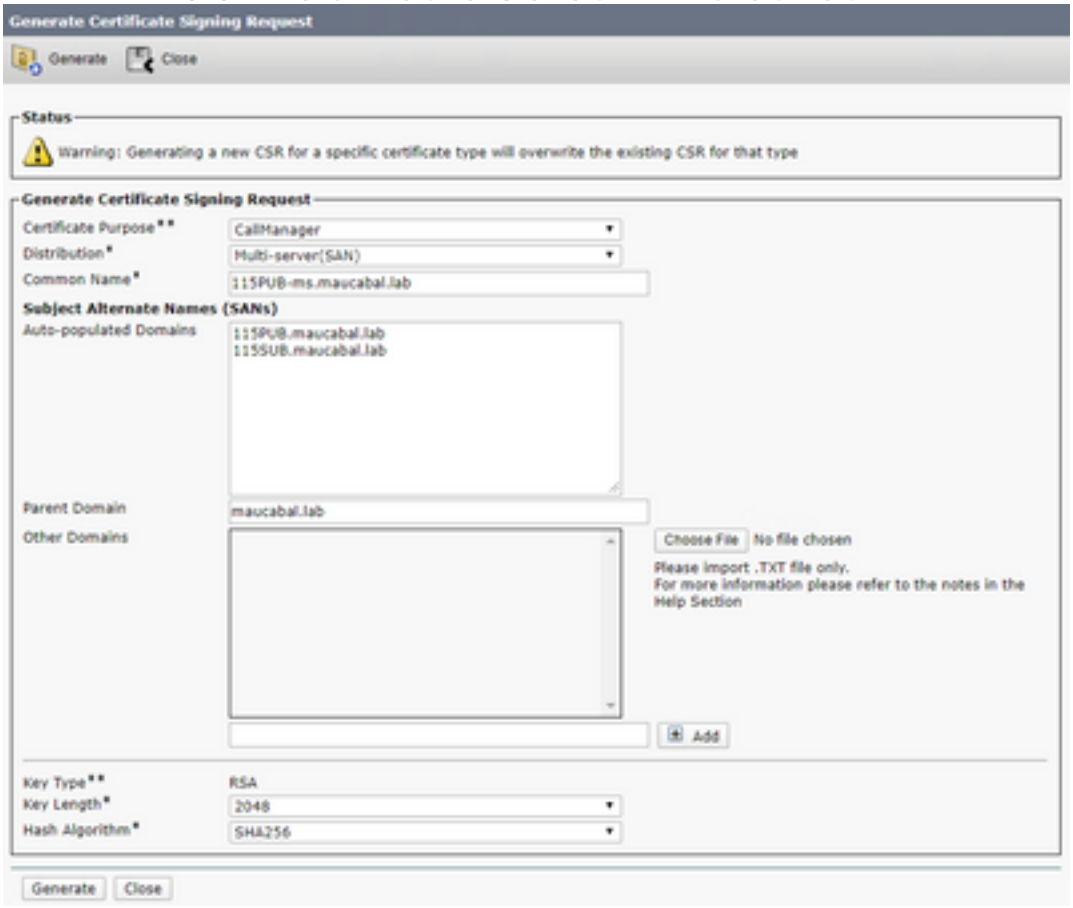
CSR(Certificate Signing Request) 생성

새로 만든 템플릿을 사용하여 CallManager 인증서를 생성하려면 다음 예를 사용하십시오. 모든 인증서 유형에 동일한 절차를 사용할 수 있습니다. 인증서 및 템플릿 유형을 적절히 선택하면 됩니다.

1단계. CUCM에서 **OS Administration(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Generate CSR(CSR 생성)로 이동합니다**.

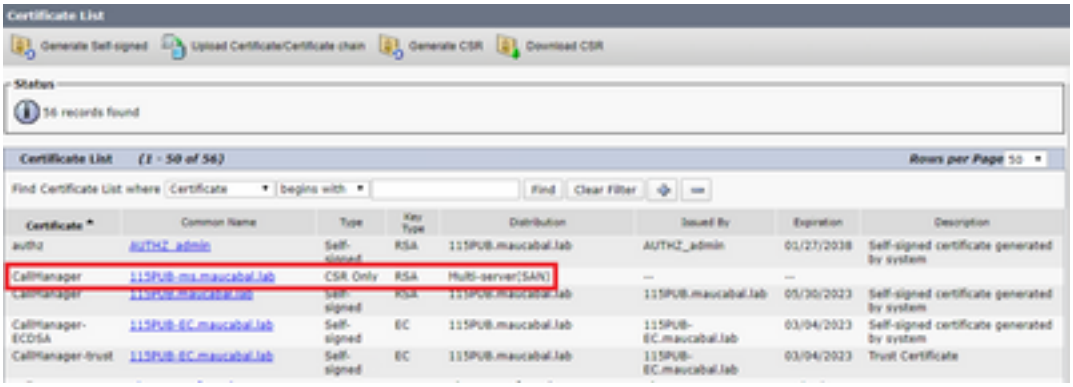
2단계. 이 옵션을 선택하고 이미지에 표시된 대로 **Generate**(생성)를 선택합니다.

- 인증서 용도: **CallManager**
- 배포: **<서버 한 대에만 사용하거나 다중 SAN에 사용 가능>**

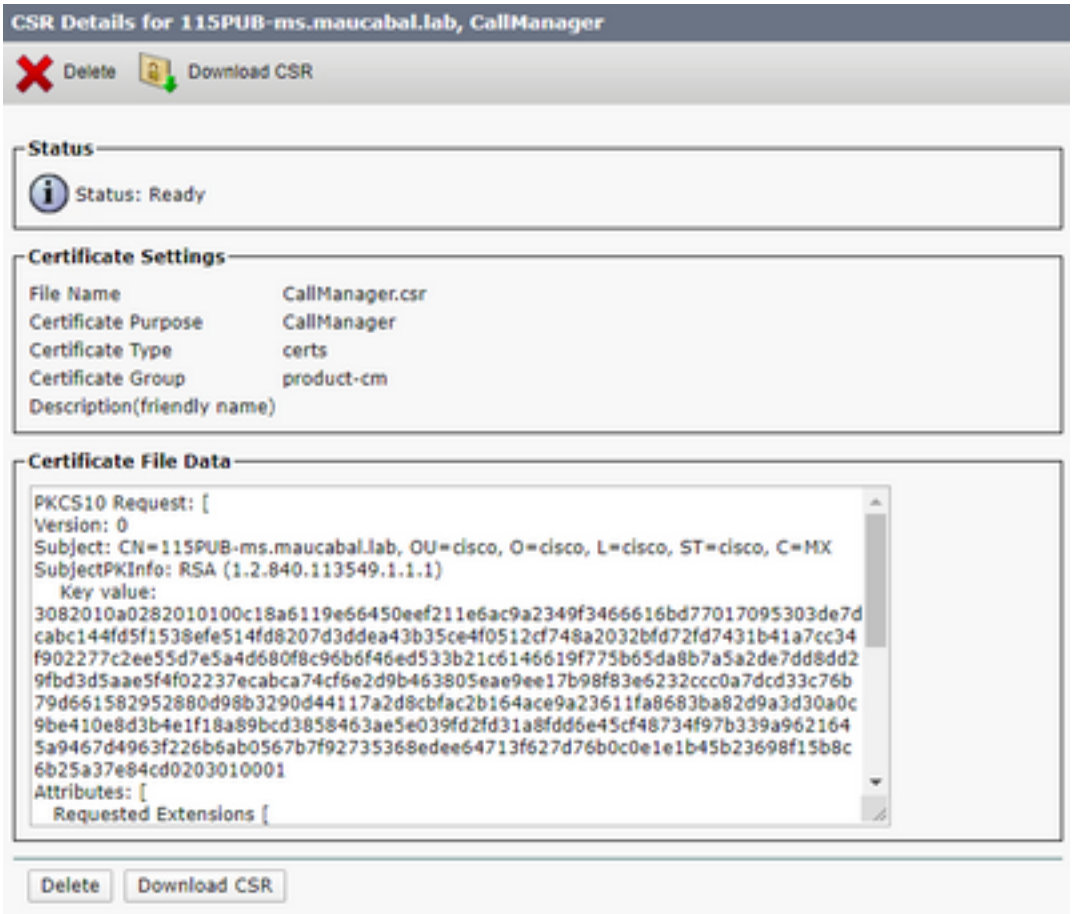


3단계. 그림과 같이 확인 메시지가 생성됩니다.

4단계. 이미지에 표시된 대로 인증서 목록에서 CSR Only **유형**의 항목을 찾아 선택합니다.

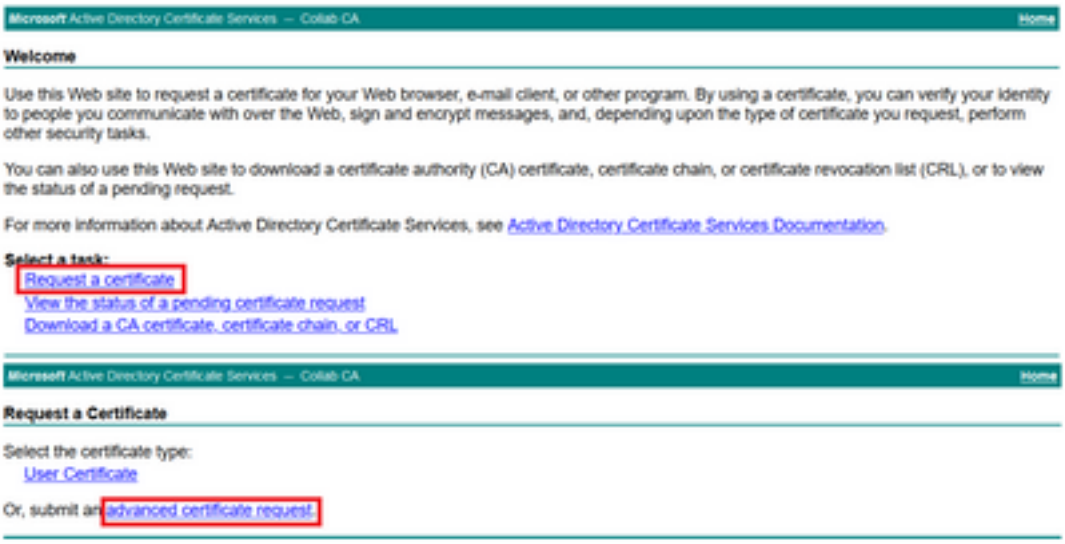


5단계. 팝업 창에서 Download CSR(CSR **다운로드**)을 선택하고 파일을 컴퓨터에 저장합니다.

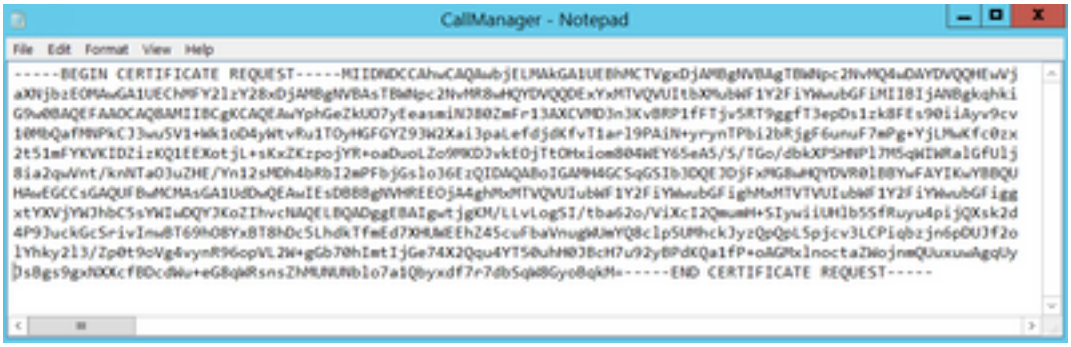


6단계. 브라우저에서 이 URL로 이동하고 도메인 컨트롤러 관리자 자격 증명을 입력합니다. https://<yourWindowsServerIP**>/certsrv/**

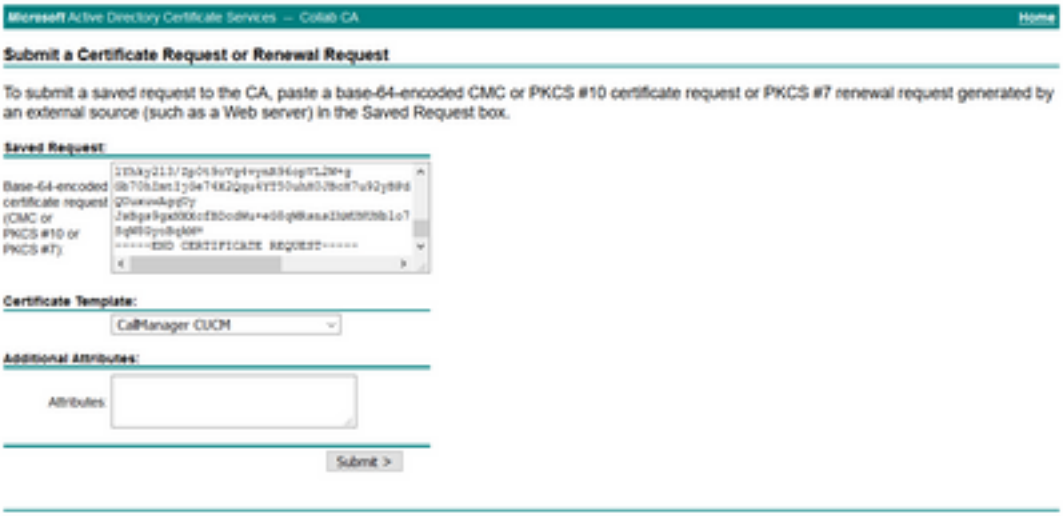
7단계. 이미지에 표시된 대로 **Request a certificate(인증서 요청) > advanced certificate** request(고급 인증서 요청)로 이동합니다.



8단계. CSR 파일을 열고 모든 내용을 복사합니다.



9단계. **Base-64**-encoded **certificate request(Base-64 인코딩 인증서 요청) 필드에 CSR을** 붙여넣습니다. Certificate **Template(인증서 템플릿)** 아래에서 올바른 템플릿을 선택하고 Submit(제출)을 선택합니다(그림과 같이).



10단계. 마지막으로, **Base 64 encoded** and **Download certificate chain(Base 64 encoded** 및 **인증서 체인 다운로드**)을 선택하면 생성된 파일을 CUCM에 업로드할 수 있습니다.

다음을 확인합니다.

확인 절차는 실제로 컨피그레이션 프로세스의 일부입니다.

문제 해결

현재 이 구성에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.