Unified Communication 클러스터 설정

목차

소개

이 문서에서는 CA(Certificate Authority) 서명 다중 서버 SAN 인증서를 사용하여 Unified Communication 클러스터를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM(Cisco Unified Communications Manager)
- CUCM IM and Presence 버전 10.5

이 컨피그레이션을 시도하기 전에 다음 서비스가 작동 중인지 확인하십시오.

- Cisco 플랫폼 관리 웹 서비스
- Cisco Tomcat 서비스

웹 인터페이스에서 이러한 서비스를 확인하려면 **Cisco** Unified Serviceability **Page Services(Cisco Unified 서비스 가용성 페이지 서비스) > Network Service(네트워크 서비스) > Select a server(서버 선택)로 이동합니다**. CLI에서 이를 확인하려면 utils service list **명령을** 입력합니다.

CUCM 클러스터에서 SSO가 활성화된 경우 비활성화했다가 다시 활성화해야 합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

CUCM 버전 10.5 이상에서는 이 트러스트 스토어 CSR(Certificate Signing Request)에 주체 대체 이름(SAN) 및 대체 도메인이 포함될 수 있습니다.

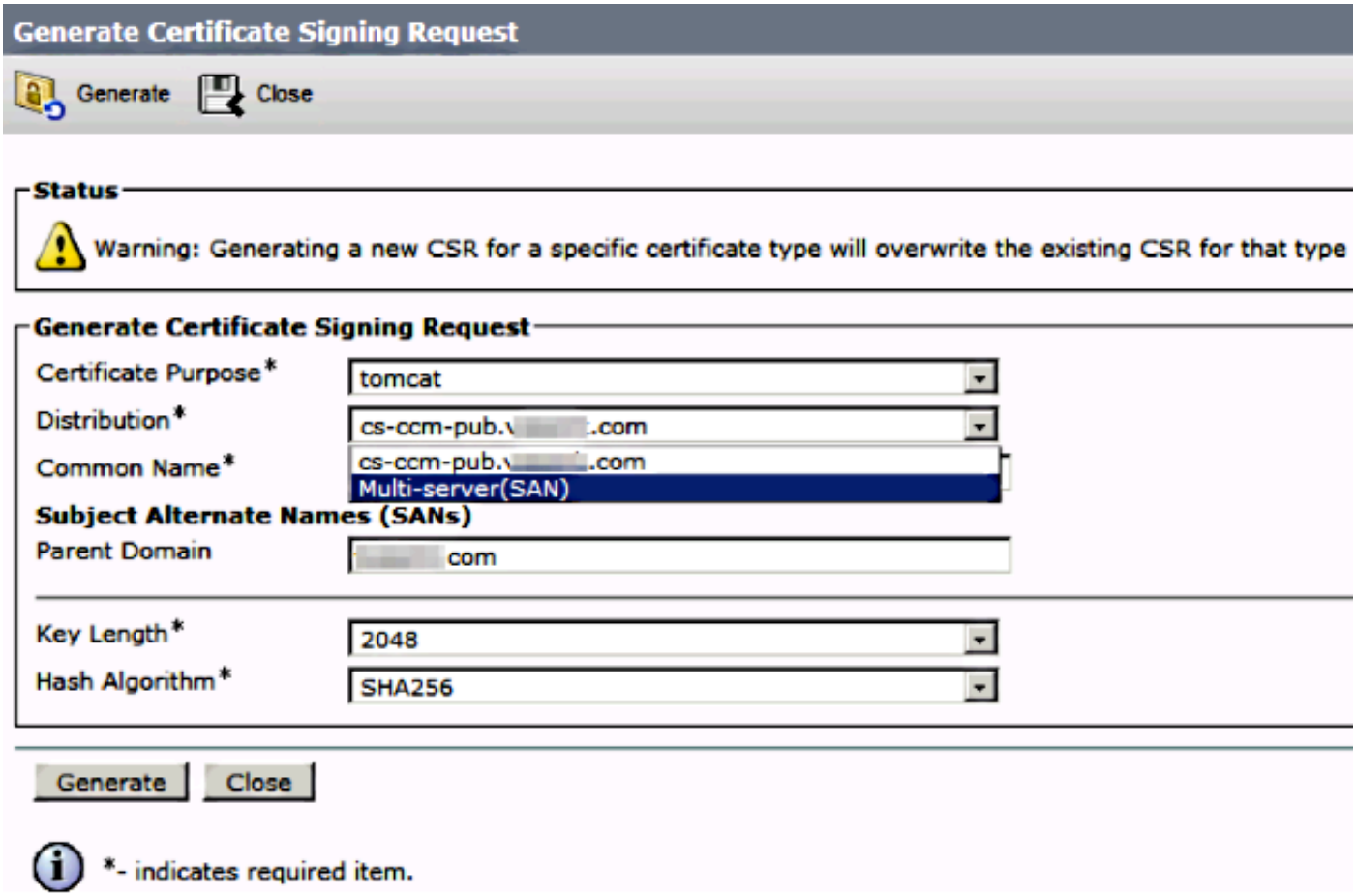
1. Tomcat - CUCM 및 IM&P
2. Cisco CallManager - CUCM 전용
3. Cisco CUP-XMPP(Unified Presence-Extensible Messaging and Presence Protocol) - IM&P 전용
4. CUP-XMPP S2S(Server-to-Server) - IM&P 전용

이 버전에서는 CA 서명 인증서를 얻는 것이 더 간단합니다. 각 서버 노드에서 CSR을 가져온 다음 각 CSR에 대해 CA 서명 인증서를 가져와 개별적으로 관리하려면 필요 없이 CA에서 서명하는 CSR은 하나만 필요합니다.

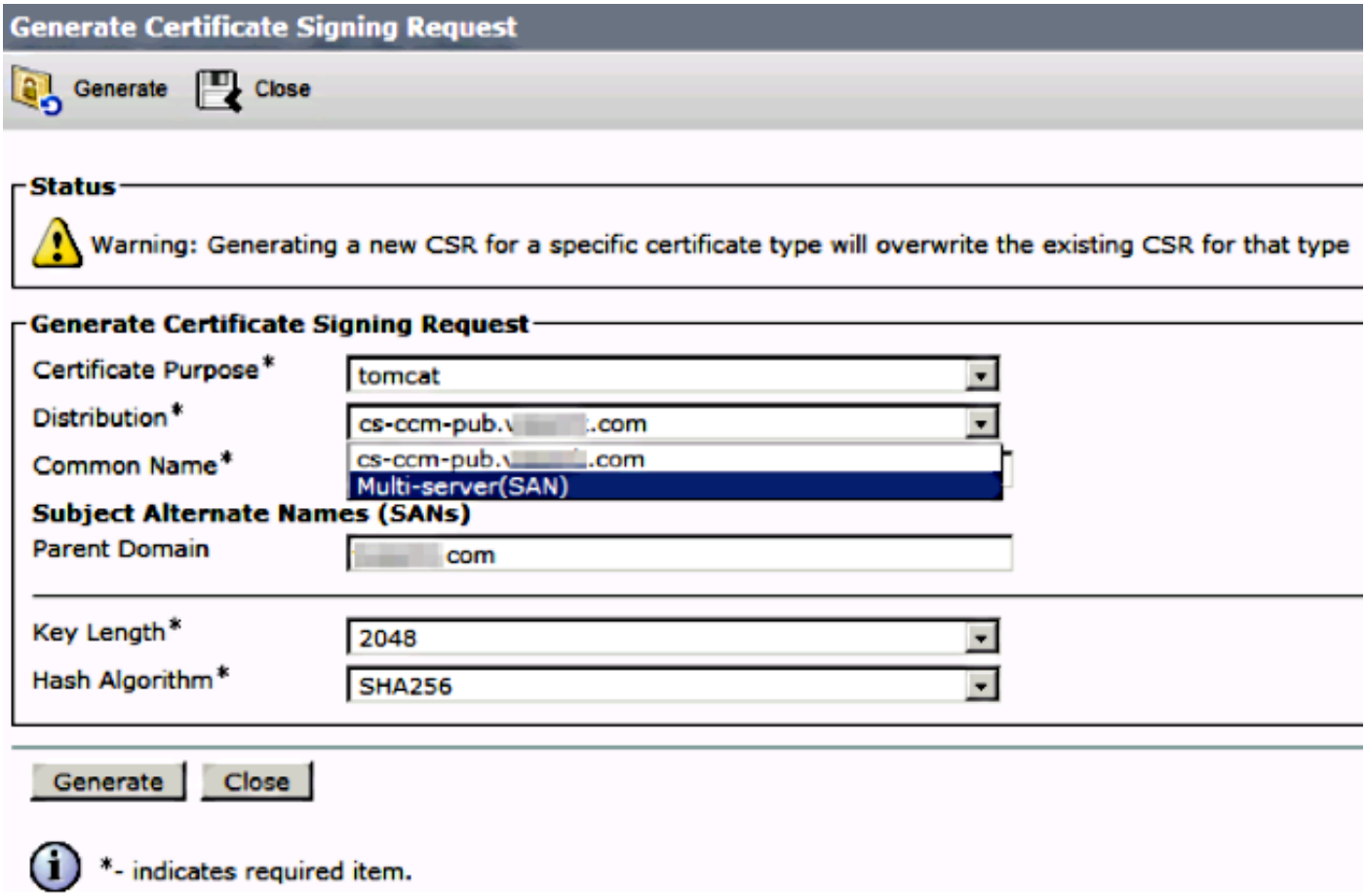
구성

1단계.

게시자의 OS(운영 체제) 관리에 로그인하고 **Security(보안) > Certificate Management(인증서 관리) > Generate CSR(CSR 생성)로 이동합니다**.

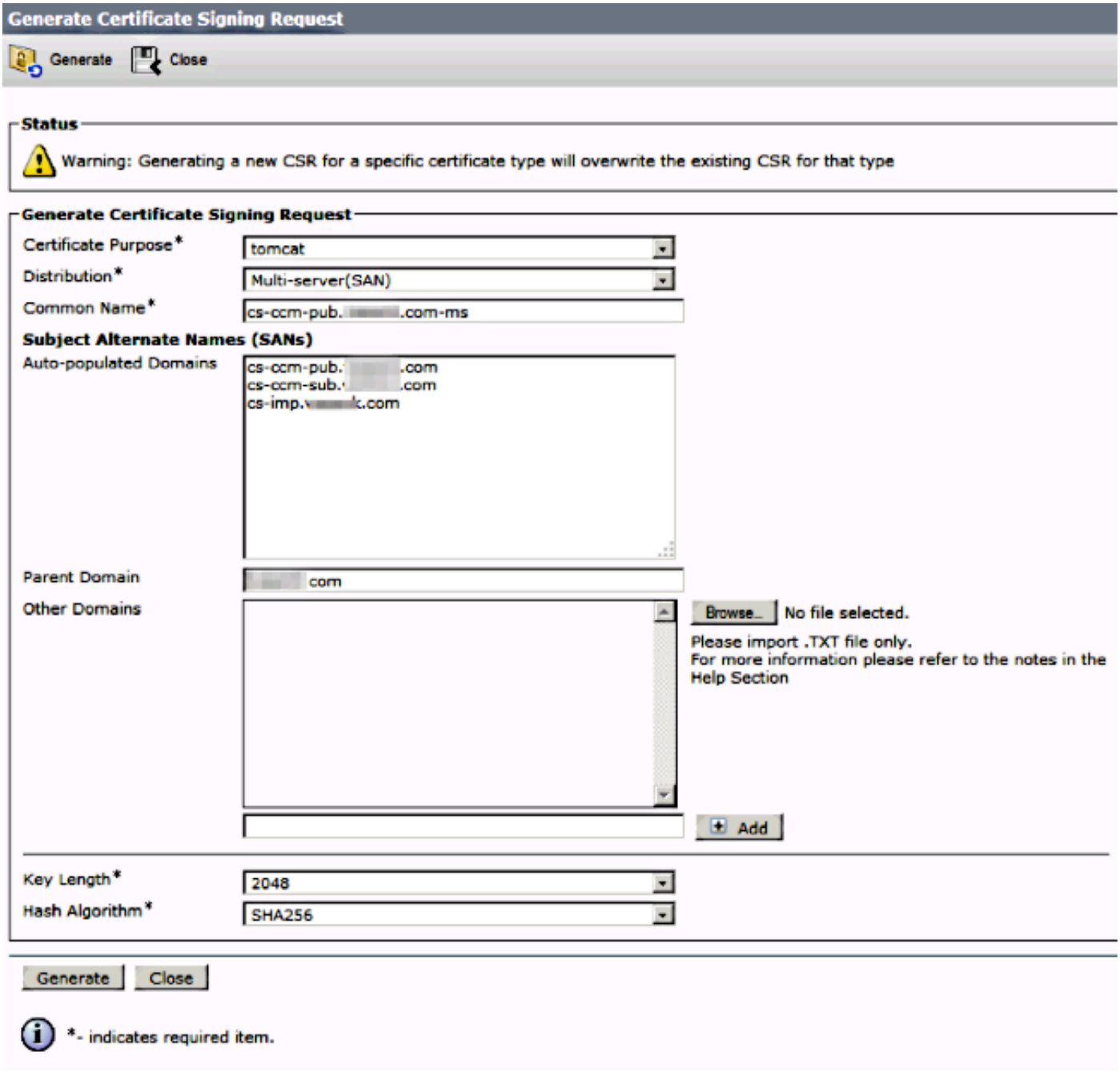


2단계.
Distribution에서 **Multi-Server SAN**을 선택합니다.



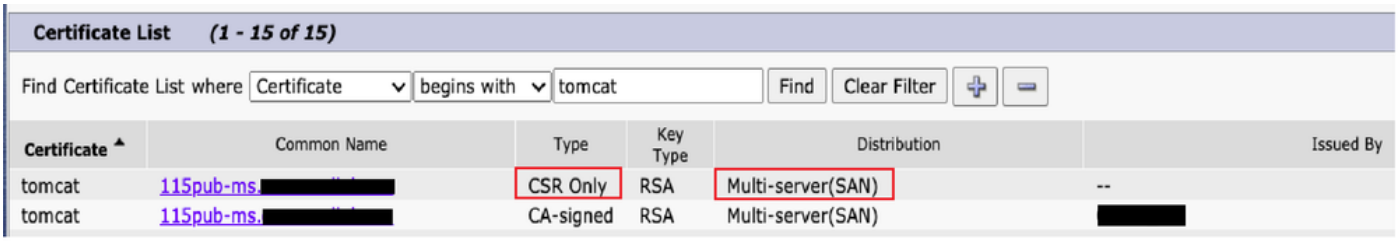
SAN 도메인 및 상위 도메인이 자동으로 채워집니다.

클러스터의 모든 노드가 Tomcat에 대해 나열되어 있는지 확인합니다. CallManager에 대한 모든 CUCM 및 IM&P 노드가 나열됩니다.



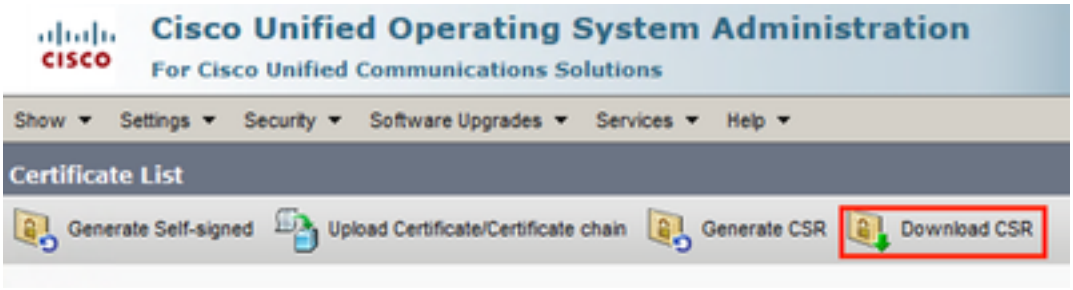
3단계.
Generate(생성)를 클릭하고 CSR이 생성되면 CSR에 나열된 모든 노드가 Successful CSR exported(성공한 CSR 내보내기) 목록에도 표시되는지 확인합니다.

Certificate Management(인증서 관리)에서 SAN 요청이 생성됩니다.



4단계.

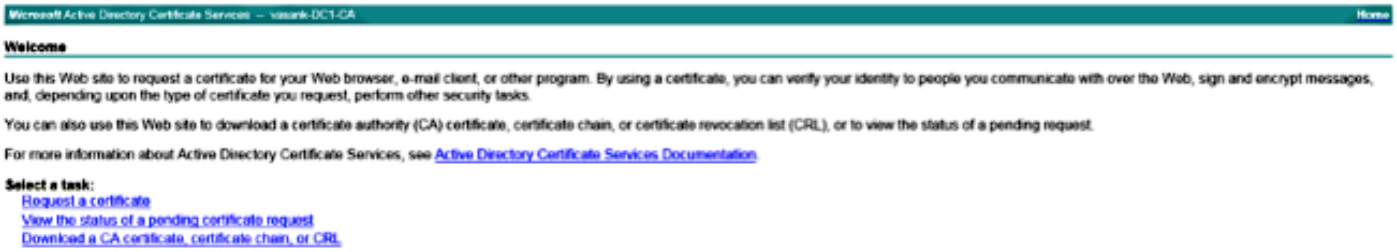
Download **CSR(CSR 다운로드)**을 클릭한 다음 인증서 용도를 선택하고 Download CSR(CSR **다운로드)을 클릭합니다**.



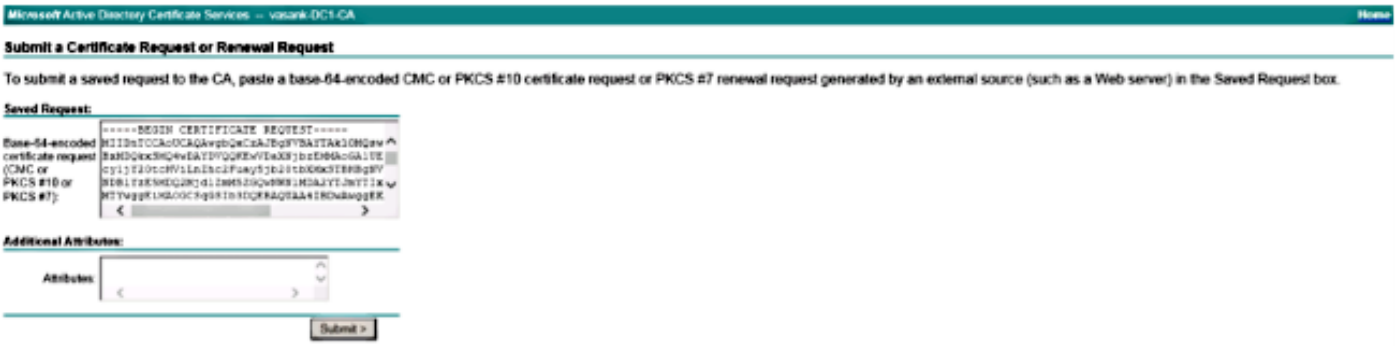
로컬 CA 또는 VeriSign과 같은 외부 CA를 사용하여 CSR(이전 단계에서 다운로드한 파일)에 서명을 받을 수 있습니다.

이 예에서는 Microsoft Windows Server 기반 CA의 컨피그레이션 단계를 보여줍니다. 다른 CA 또는 외부 CA를 사용하는 경우 5단계로 이동합니다.

https://<windowsserveripaddress>/certsrv/에 로그인합니다.
Request **a Certificate(인증서 요청) > Advanced Certificate Request(고급 인증서 요청)를 선택합니다.**
CSR 파일의 내용을 Base-64 인코딩 인증서 요청 필드에 복사하고 Submit(제출)을 **클릭합니다**.



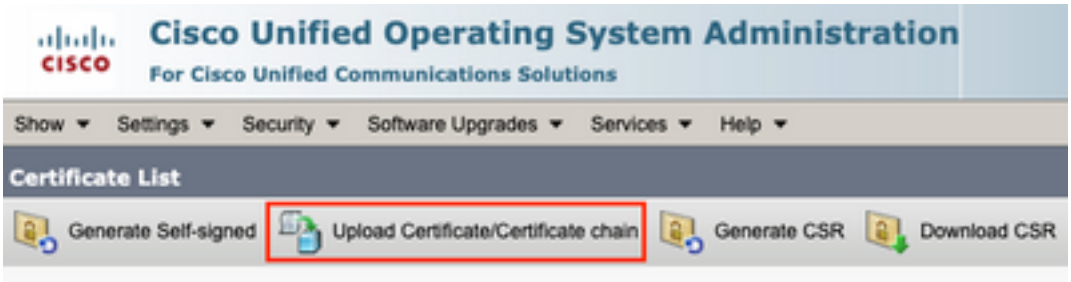
여기에 표시된 대로 CSR 요청을 제출합니다.

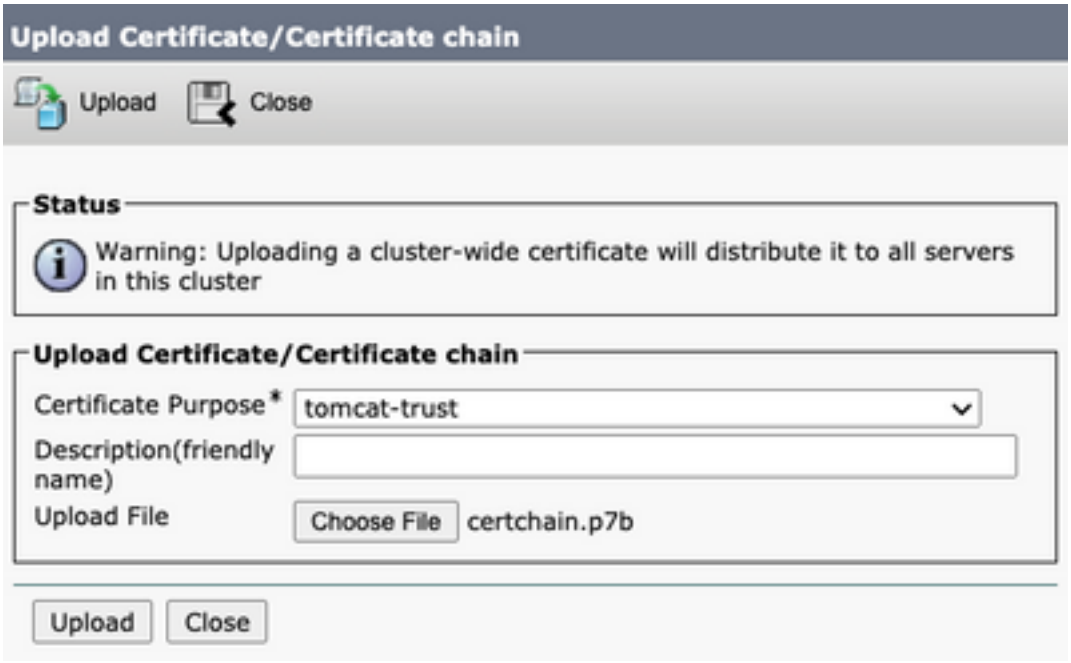


5단계.

> **참고**: Tomcat 인증서를 업로드하기 전에 SSO가 비활성화되어 있는지 확인합니다. 활성화된 경우 모든 Tomcat 인증서 재생성 프로세스가 완료되면 SSO를 비활성화했다가 다시 활성화해야 합니다.

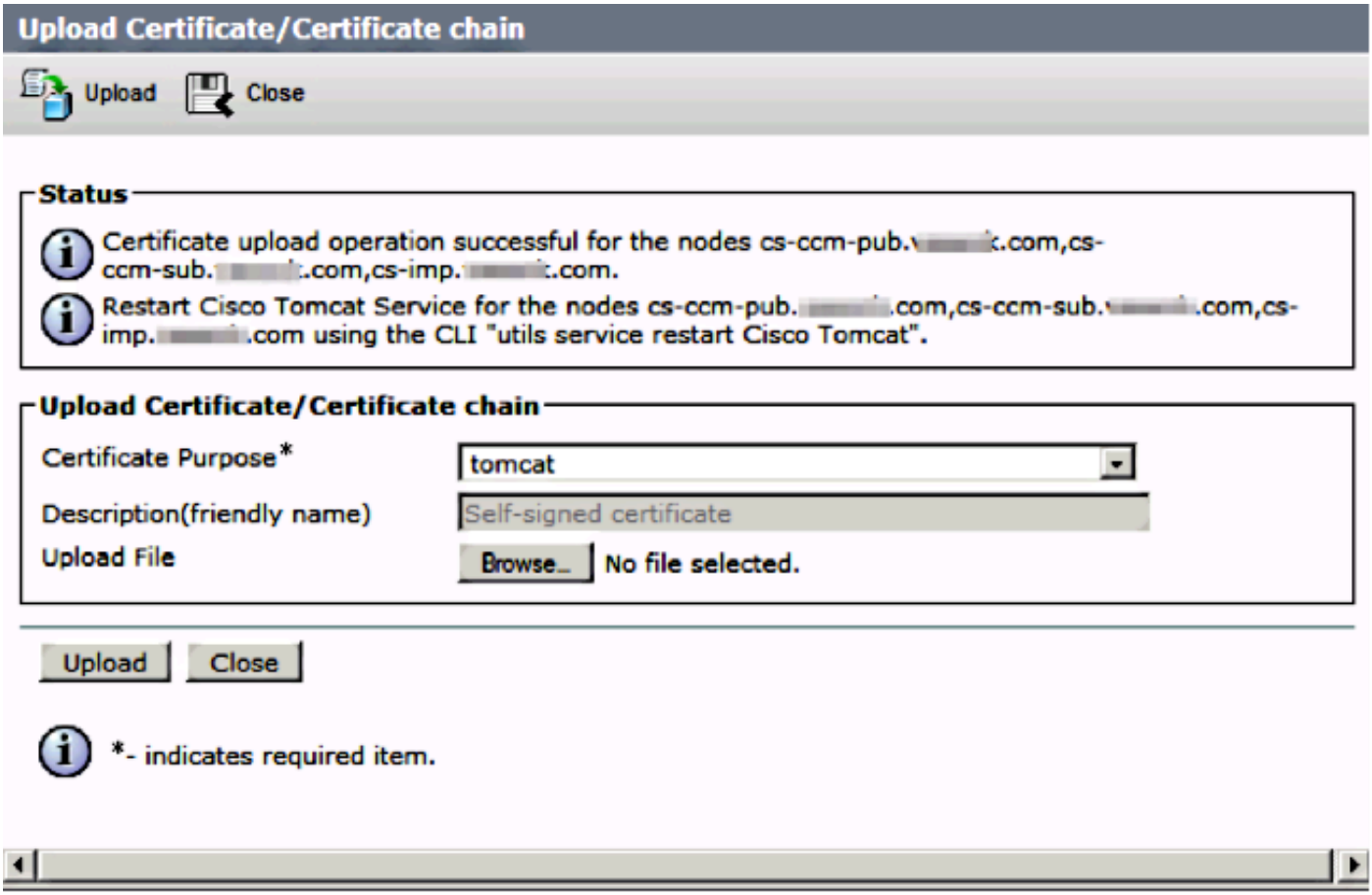
서명된 인증서를 사용하여 CA 인증서를 tomcat-trust로 업로드합니다. 먼저 루트 인증서를 선택한 다음 중간 인증서가 있는 경우 이를 선택합니다.





6단계.

이제 CUCM 서명 인증서를 Tomcat으로 업로드하고 클러스터의 모든 노드가 그림과 같이 "인증서 업로드 작업 성공"에 나열되어 있는지 확인합니다.



다중 서버 SAN은 그림과 같이 Certificate Management(인증서 관리)에 나열됩니다.

ipsec-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY_cs-ccm-pub.[redacted].com	ITLRECOVERY_cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Certificate Signed by [redacted]-DC1-CA
tomcat-trust	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.[redacted].com	Self-signed	dc1-ccm-pub.[redacted].com	dc1-ccm-pub.[redacted].com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-sub.[redacted].com	Self-signed	dc1-ccm-sub.[redacted].com	dc1-ccm-sub.[redacted].com	04/18/2019	Trust Certificate
tomcat-trust	[redacted]-DC1-CA	Self-signed	[redacted]-DC1-CA	[redacted]-DC1-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

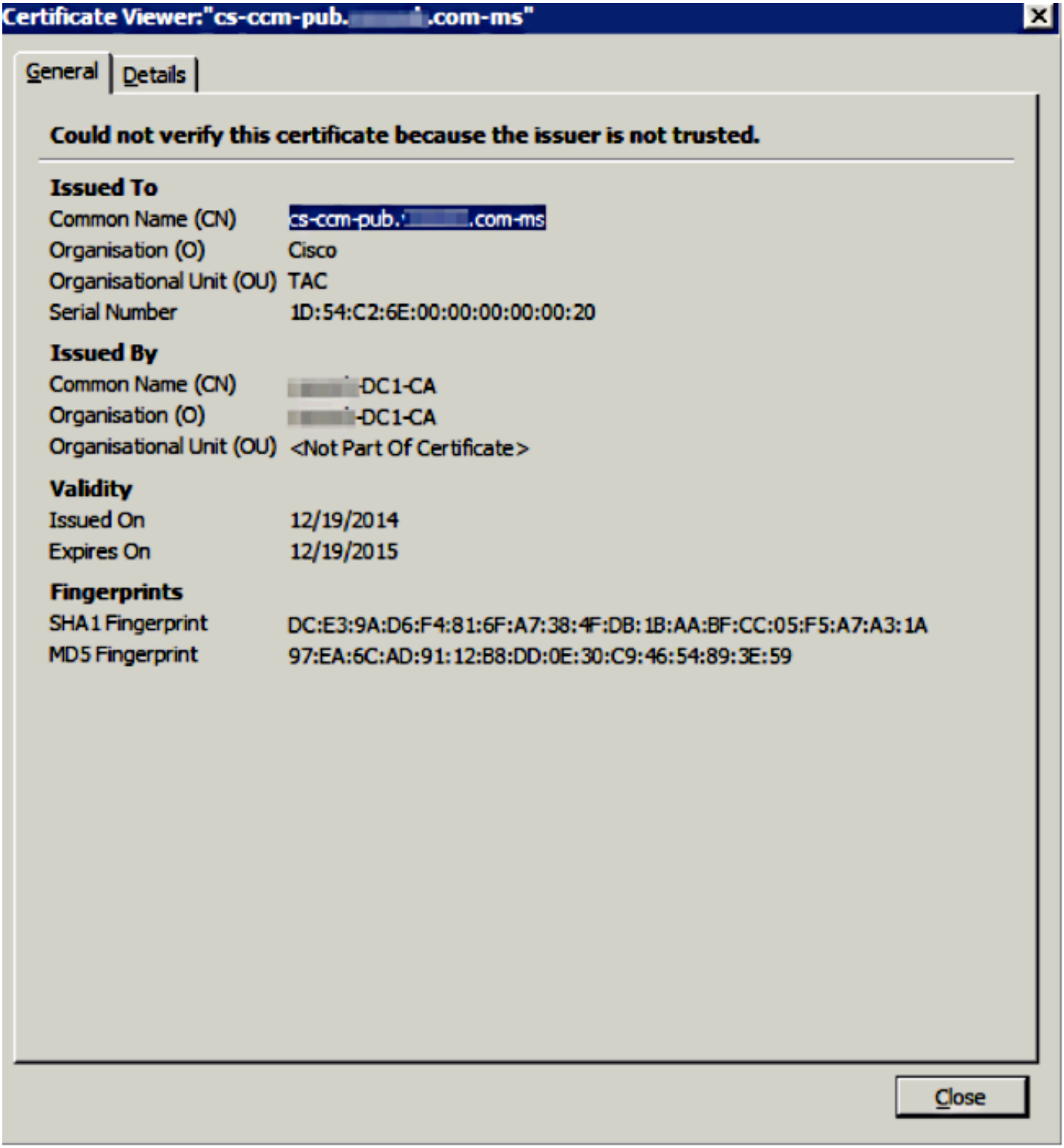
7단계.

utils service restart **Cisco** Tomcat 명령을 사용하여 CLI를 통해 SAN 목록의 모든 노드(첫 번째 게시자 및 가입자)에서 **Tomcat 서비스를 재시작합니다**.

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

다음을 확인합니다.

새 인증서가 사용되는지 확인하려면 http://<fqdnofccm>:8443/ccmadmin에 로그인합니다.



CallManager 다중 서버 SAN 인증서

CallManager 인증서에 대해서도 유사한 절차를 따를 수 있습니다. 이 경우 자동으로 채워진 도메인은 CallManager 노드뿐입니다. Cisco CallManager 서비스가 실행되고 있지 않으면 SAN 목록에 유지하거나 제거하도록 선택할 수 있습니다.

> **경고**: 이 프로세스는 전화 등록 및 통화 처리에 영향을 미칩니다. CUCM/TVS/ITL/CAPF 인증서를 사용하는 모든 작업에 대해 유지 보수 기간을 예약해야 합니다.

CUCM에 대한 CA 서명 SAN 인증서 전에 다음을 확인합니다.

- IP Phone에서 TVS(Trust Verification Service)를 신뢰할 수 있습니다. 전화기에서 HTTPS 서비스에 액세스하여 이를 확인할 수 있습니다. 예를 들어 회사 디렉터리 액세스가 작동하는 경우 전화기가 TVS 서비스를 신뢰한다는 의미입니다.
- 클러스터가 비보안 모드 또는 혼합 모드인지 확인합니다.

혼합 모드 클러스터인지 확인하려면 **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수) > Cluster Security Mode(클러스터 보안 모드)(0==비보안, 1== 혼합 모드)**.

> **경고**: 서비스를 다시 시작하기 전에 혼합 모드 클러스터에 있는 경우 CTL은 Token 또는 Tokenless로 업데이트해야 합니다.

CA에서 발급한 인증서를 설치한 후 다음 서비스 목록을 활성화된 노드에서 다시 시작해야 합니다.

- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco TFTP
- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco CallManager
- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco CTIManager
- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스) > Cisco Trust Verification Service

문제 해결

이러한 로그는 Cisco Technical Assistance Center에서 멀티서버 SAN CSR 생성 및 CA 서명 인증서 업로드와 관련된 문제를 식별하는 데 도움이 됩니다.

- Cisco Unified OS Platform API
- Cisco Tomcat
- IPT 플랫폼 CertMgr 로그
- 인증서 갱신 프로세스

알려진 주의 사항

·Cisco 버그 ID CSCur97909 - 멀티서버 인증서를 업로드해도 DB의 자체 서명 인증서가 삭제되지 않음
·Cisco 버그 ID CSCus47235 - CSR용 SAN에 CUCM 10.5.2 CN 중복 없음
·Cisco 버그 ID CSCup28852 - 다중 서버 인증서 사용 시 인증서 업데이트로 인해 7분마다 폰 재설정

기존 다중 서버 인증서가 있는 경우 다음 시나리오에서 다시 생성하는 것이 좋습니다.

- 호스트 이름 또는 도메인 변경 호스트 이름 또는 도메인 변경이 수행되면 인증서가 자동으로 자체 서명된 인증서로 다시 생성됩니다. CA 서명 된 로 변경 하려면 이전 단계를 따라야 합니다.
- 클러스터에 새 노드가 추가된 경우 새 노드를 포함하도록 새 CSR을 생성해야 합니다.
- 가입자가 복원되고 백업이 사용되지 않은 경우 노드에는 새 자체 서명 인증서가 있을 수 있습니다. 가입자를 포함하려면 전체 클러스터에 대한 새 CSR이 필요할 수 있습니다. (개선 요청이 있음Cisco 버그 ID CSCuv75957 을(를) 클릭하여 이 기능을 추가합니다.

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.