서명된 CA 인증서에서 새 인증서 생성

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)에서 CA(Certificate Authority)에 의해 서명된 인증서를 재생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RTMT(실시간 모니터링 도구)
- CUCM 인증서

사용되는 구성 요소

- CUCM 릴리스 10.x, 11.x 및 12.x.

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.

사전 검사 정보

> **참고:** 자체 서명 인증서 재생성에 대해서는 Certificate Regeneration Guide를 참조하십시오. CA 서명 Multi-SAN 인증서 재생성에 대해서는 Multi-SAN Certificate Regeneration Guide를 참조하십시오.

각 인증서와 해당 재생성의 영향을 이해하려면 자체 서명 재생성 가이드를 참조하십시오.

각 CSR(Certificate Signing Request) 유형에는 서로 다른 키 사용이 있으며 이는 서명된 인증서에 필요합니다. Security Guide에는 각 인증서 유형에 필요한 키 사용이 포함된 테이블이 포함되어 있습니다.

Subject Settings(Locality, State, Organization Unit 등)를 변경하려면 다음 명령을 실행합니다.

- **set web-security** orgunit orgname locality state [country] [alternatehostname]

Tomcat 인증서는 set web-security 명령을 실행합니다. Tomcat 서비스를 다시 시작하지 않는 한 새 자체 서명 인증서가 적용되지 않습니다. 이 명령에 대한 자세한 내용은 다음 가이드를 참조하십시오.

- 명령줄 참조 가이드
- Cisco 커뮤니티 단계 링크
- 비디오

인증서 구성 및 재생성

CA가 서명한 CUCM 클러스터의 단일 노드 인증서를 재생성하는 단계는 각 인증서 유형에 대해 나열됩니다. 인증서가 만료되지 않은 경우 클러스터의 모든 인증서를 다시 생성할 필요는 없습니다.

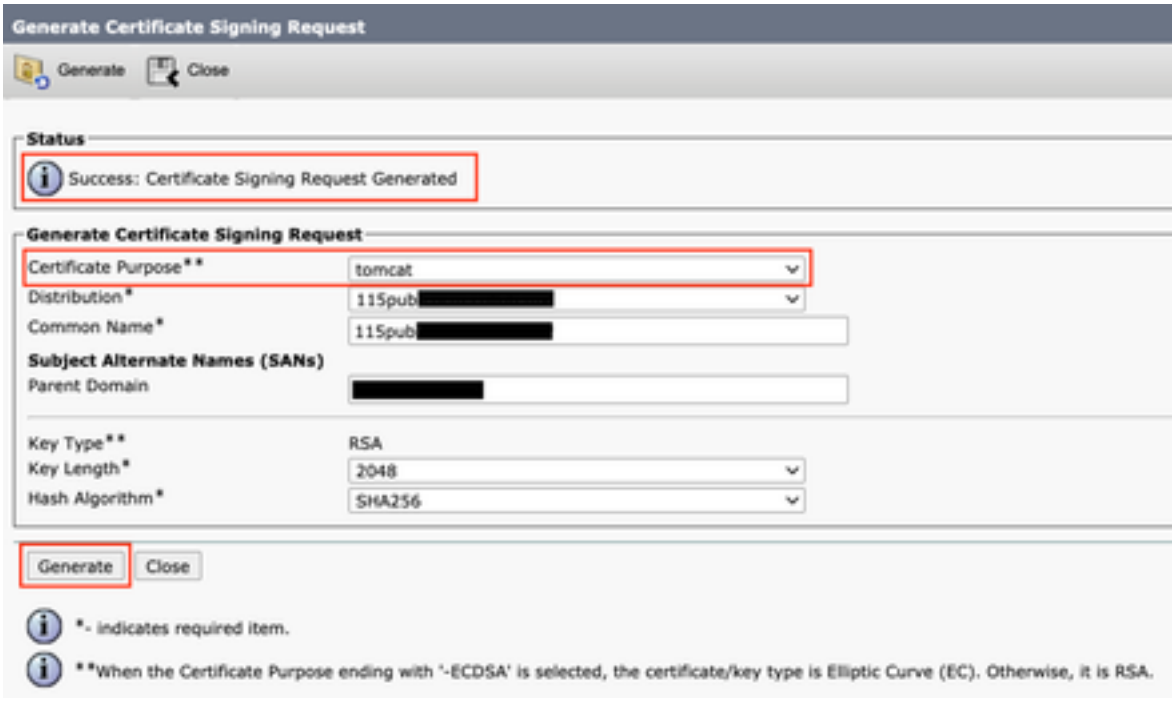
Tomcat 인증서

> **주의**: 클러스터에서 SSO가 비활성화되었는지 확인합니다(**CM Administration > System > SAML Single Sign-On**). SSO가 활성화된 경우 Tomcat 인증서 재생성 프로세스가 완료되면 비활성화한 다음 활성화해야 합니다.

클러스터의 모든 노드(CallManager 및 IM&P)에서 다음을 수행합니다.

1단계. **Cisco Unified OS Administration > Security > Certificate Management > Find** Tomcat 인증서의 만료일을 확인합니다.

2단계. Generate CSR > Certificate Purpose: tomcat. 인증서에 대해 원하는 설정을 선택한 다음 **Generate**. 성공 메시지가 나타날 때까지 기다린 후 Close.



3단계. CSR을 다운로드합니다. 클릭 Download CSR , 선택 **Certificate Purpose: tomcat**, 및 Download.

4단계. CSR을 인증 기관에 보냅니다.

5단계. Certificate Authority는 서명된 인증서 체인에 대해 둘 이상의 파일을 반환합니다. 다음 순서로 인증서를 업로드합니다.

- 루트 CA 인증서를 tomcat-trust로 지정합니다. 탐색 **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. 인증서의 설명을 설정하고 루트 인증서 파일을 찾습니다.
- 중간 인증서를 tomcat-trust로 지정합니다(선택 사항). **탐색 Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. 인증서의 설명을 설정하고 중간 인증서 파일을 찾습니다.

  참고: 일부 CA는 중간 인증서를 제공하지 않습니다. 루트 인증서만 제공된 경우 이 단계를 생략할 수 있습니다.

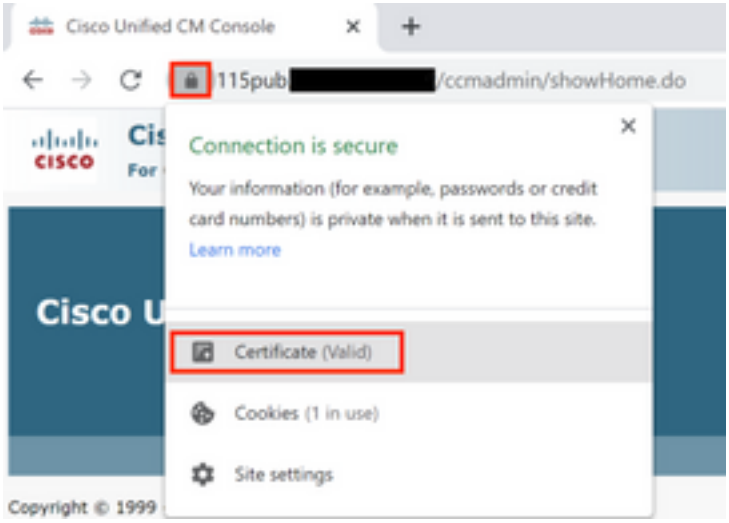
- tomcat으로 CA 서명 인증서 **탐색 Certificate Management > Upload certificate > Certificate Purpose: tomcat.** 인증서에 대한 설명을 설정하고 현재 CUCM 노드에 대한 CA 서명 인증서 파일을 찾습니다.

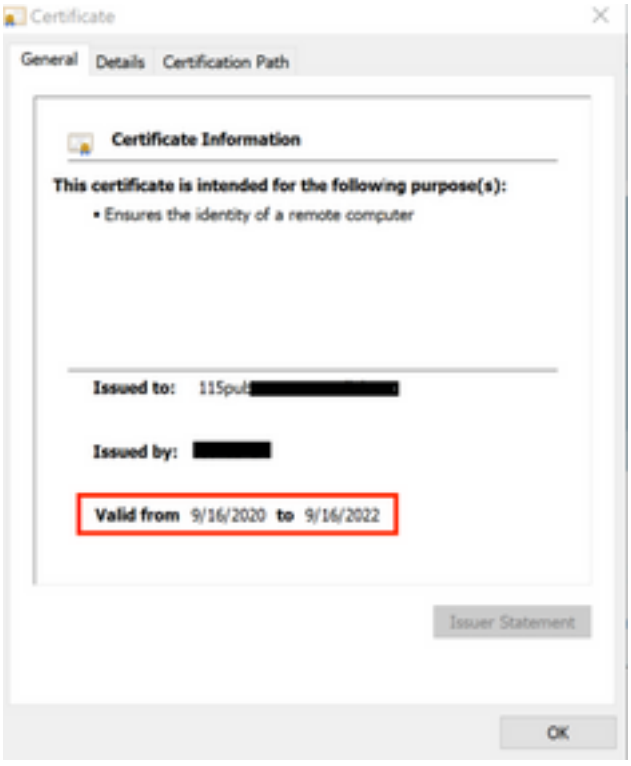
  참고: 이때 CUCM은 CSR과 업로드된 CA 서명 인증서를 비교합니다. 정보가 일치하면 CSR이 사라지고 새 CA 서명 인증서가 업로드됩니다. 인증서를 업로드한 후 오류 메시지가

표시되면 Upload Certificate Common Error Messages 섹션을 참조하십시오.

6단계. 서버에 적용된 새 인증서를 가져오려면 CLI를 통해 Cisco Tomcat 서비스를 다시 시작해야 합니다(Publisher로 시작한 다음 구독자가 한 번에 하나씩). 이 명령을 사용합니다 utils service restart Cisco Tomcat.

이제 CUCM에서 Tomcat 인증서를 사용하여 인증서의 유효성을 검사합니다. 노드의 웹 페이지로 이동하여 Site Information (잠금 아이콘) 브라우저에서 certificate 새 인증서의 날짜를 확인합니다.





CallManager 인증서

주의: CallManager 및 TVS 인증서를 동시에 재생성하지 마십시오. 이로 인해 엔드포인트에 설치된 ITL이 복구할 수 없는 불일치가 발생하므로 클러스터의 모든 엔드포인트에서 ITL을 제거해야 합니다. CallManager에 대한 전체 프로세스를 마치고 전화기가 다시 등록되면 TVS에 대한 프로세스를 시작합니다.

참고: 클러스터가 혼합 모드인지 확인하려면 **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수) > Cluster Security Mode(클러스터 보안 모드) (0 == Non-Secure; 1 == 혼합 모드)**.

클러스터의 모든 CallManager 노드에 대해 다음을 수행합니다.

1단계. Cisco Unified OS Administration > Security > Certificate Management > Find CallManager 인증서의 만료 날짜를 확인합니다.

2단계. Generate CSR > Certificate Purpose: CallManager. 인증서에 대해 원하는 설정을 선택한 다음 Generate. 성공 메시지가 나타날 때까지 기다린 후 Close.

3단계. CSR을 다운로드합니다. 클릭 **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

4단계. CSR을 Certificate Authority .

5단계. Certificate Authority는 서명된 인증서 체인에 대해 둘 이상의 파일을 반환합니다. 다음 순서로 인증서를 업로드합니다.

- 루트 CA 인증서를 CallManager-trust로 지정합니다. 탐색 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. 인증서의 설명을 설정하고 루트 인증서 파일을 찾습니다.
- 중간 인증서를 CallManager-trust로 지정합니다(선택 사항). 탐색 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. 인증서의 설명을 설정하고 중간 인증서 파일을 찾습니다.

참고: 일부 CA는 중간 인증서를 제공하지 않습니다. 루트 인증서만 제공된 경우 이 단계를 생략할 수 있습니다.

- CallManager로 CA 서명 인증서 탐색 Certificate Management > Upload certificate > Certificate Purpose: CallManager. 인증서의 설명을 설정하고 현재 CUCM 노드에 대한 CA 서명 인증서 파일을 찾습니다.

  참고: 이때 CUCM은 CSR과 업로드된 CA 서명 인증서를 비교합니다. 정보가 일치하면 CSR이 사라지고 새 CA 서명 인증서가 업로드됩니다. 인증서를 업로드한 후 오류 메시지가 표시되면 Upload Certificate **Common Error Messages 섹션을** 참조하십시오.

6단계. 클러스터가 혼합 모드인 경우 서비스를 다시 시작하기 전에 CTL을 업데이트합니다. 토큰 또는 토큰리스. 클러스터가 비보안 모드에 있는 경우 이 단계를 건너뛰고 서비스 재시작을 진행합니다.

7단계. 서버에 적용된 새 인증서를 가져오려면 필요한 서비스를 다시 시작해야 합니다(서비스가 실행되고 활성화된 경우에만). 다음으로 이동합니다.

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

8단계. 모든 전화기를 재설정합니다.

- 탐색 Cisco Unified CM Administration > System > Enterprise Parameters > Reset. You are about to

reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가 포함된 팝업 창이 나타납니다. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? 선택 OK 다음을 클릭합니다. Reset .

참고: RTMT를 통해 디바이스 등록을 모니터링합니다. 모든 전화기가 다시 등록되면 다음 인증서 유형으로 진행할 수 있습니다.

IPSec 인증서

주의: IPSec 인증서가 다시 생성되면 백업 또는 복원 작업이 활성화되지 않아야 합니다.

클러스터의 모든 노드(CallManager 및 IM&P):

1단계. Cisco Unified OS Administration > Security > Certificate Management > Find ipsec 인증서의 만료일을 확인합니다.

2단계. Generate CSR(CSR **생성) > Certificate Purpose(인증서 용도)를 클릭합니다. ipsec.** 인증서에 대해 원하는 설정을 선택한 다음 Generate(**생성**)를 클릭합니다. 성공 메시지가 나타날 때까지 기다린 다음 닫기를 **클릭합니다**.

3단계. CSR을 다운로드합니다. Download CSR(**CSR 다운로드)을 클릭합니다**. Certificate Purpose ipsec(인증서 용도 ipsec)을 선택하고 Download(**다운로드)**를 **클릭합니다**.

4단계. CSR을 인증 기관에 보냅니다.

5단계. Certificate Authority는 서명된 인증서 체인에 대해 둘 이상의 파일을 반환합니다. 다음 순서로 인증서를 업로드합니다.

- 루트 CA 인증서를 ipsec-trust로 지정합니다. **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **ipsec-trust입니다.** 인증서의 설명을 설정하고 루트 인증서 파일을 찾습니다.
- 중간 인증서를 ipsec-trust로 지정합니다(선택 사항). **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **tomcat-trust**. 인증서의 설명을 설정하고 중간 인증서 파일을 찾습니다.

  참고: 일부 CA는 중간 인증서를 제공하지 않습니다. 루트 인증서만 제공된 경우 이 단계를 생략할 수 있습니다.

  - CA 서명 인증서를 ipsec으로 사용합니다. **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **ipsec**. 인증서의 설명을 설정하고 현재 CUCM 노드에 대한 CA 서명 인증서 파일을 찾습니다.

  참고: 이때 CUCM은 CSR과 업로드된 CA 서명 인증서를 비교합니다. 정보가 일치하면 CSR이 사라지고 새 CA 서명 인증서가 업로드됩니다. 인증서를 업로드한 후 오류 메시지가 표시되면 인증서 **공통 오류 메시지 업로드< /strong> 섹션을 참조하십시오.**

6단계. 서버에 적용된 새 인증서를 가져오려면 필요한 서비스를 다시 시작해야 합니다(서비스가 실행되고 활성화된 경우에만). 다음으로 이동합니다.

- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center -**

Network Services(제어 센터 - 네트워크 서비스) > Cisco DRF Master(게시자)
- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스) > Cisco DRF Local(게시자 및 가입자)

CAPF 인증서

참고: 클러스터가 혼합 모드인지 확인하려면 **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수) > Cluster Security Mode(클러스터 보안 모드)(0 == Non-Secure; 1 == 혼합 모드)**.

참고: CAPF 서비스는 Publisher에서만 실행되며, 이는 사용되는 유일한 인증서입니다. CA에서 서명한 가입자 노드는 사용되지 않으므로 가져올 필요가 없습니다. 인증서가 가입자에서 만료 된 경우 만료 된 인증서의 경고를 방지 하려면, 자체 서명 가입자 CAPF 인증서를 다시 생성 할 수 있습니다. 자세한 내용은 CAPF Certificate as Self-Signed를 참조하십시오.

게시자:

1단계. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find and verify the** expiration date of the CAPF certificate(CAPF 인증서 찾기 및 만료 날짜)로 이동합니다.

2단계. Generate CSR(CSR **생성) > Certificate Purpose(인증서 용도)를 클릭합니다. 캡프** 인증서에 대해 원하는 설정을 선택한 다음 Generate를 **클릭합니다**. 성공 메시지가 나타날 때까지 기다린 후 닫기를 **클릭합니다**.

3단계. CSR을 다운로드합니다. Download CSR(**CSR 다운로드)을 클릭합니다**. Certificate Purpose CAPF(인증서 용도 CAPF)를 선택하고 Download(**다운로드**)를 **클릭합니다**.

4단계. CSR을 인증 기관에 보냅니다.

5단계. Certificate Authority는 서명된 인증서 체인에 대해 둘 이상의 파일을 반환합니다. 다음 순서로 인증서를 업로드합니다.

- 루트 CA 인증서를 CAPF-trust로 지정합니다. **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **CAPF-Trust입니다.** 인증서의 설명을 설정하고 루트 인증서 파일을 찾습니다.
- 중간 인증서를 CAPF-trust로 지정합니다(선택 사항). **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **CAPF-trust**. 인증서의 설명을 설정하고 중간 인증서 파일을 찾습니다.

참고: 일부 CA는 중간 인증서를 제공하지 않습니다. 루트 인증서만 제공된 경우 이 단계를 생략할 수 있습니다.

- CAPF로 CA 서명 된 인증서 **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **CAPF**. 인증서의 설명을 설정하고 현재 CUCM 노드에 대한 CA 서명 인증서 파일을 찾습니다.

참고: 이때 CUCM은 CSR과 업로드된 CA 서명 인증서를 비교합니다. 정보가 일치하면 CSR이 사라지고 새 CA 서명 인증서가 업로드됩니다. 인증서를 업로드한 후 오류 메시지가

표시되면 Upload Certificate **Common Error Messages 섹션을** 참조하십시오.

6단계. 클러스터가 혼합 모드인 경우 서비스를 다시 시작하기 전에 CTL을 업데이트합니다. 토큰 또는 토큰리스. 클러스터가 비보안 모드에 있는 경우 이 단계를 건너뛰고 서비스 재시작을 진행합니다.

7단계. 서버에 적용된 새 인증서를 가져오려면 필요한 서비스를 다시 시작해야 합니다(서비스가 실행되고 활성화된 경우에만). 다음으로 이동합니다.

- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스) > Cisco Trust Verification Service**(서비스가 실행되는 모든 노드)
- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco TFTP**(서비스가 실행되는 모든 노드)
- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco Certificate Authority Proxy Function** (Publisher)

8단계. 모든 전화기를 재설정합니다.

- **Cisco** Unified **CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수) > Reset(재설정)으로 이동합니다**. You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가 포함된 팝업 창이 나타납니다. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? **OK(확인)**를 선택한 다음 Reset(재설정)**을 클릭합니다**.

참고: RTMT를 통해 디바이스 등록을 모니터링합니다. 모든 전화기가 다시 등록되면 다음 인증서 유형으로 진행할 수 있습니다.

TVS 인증서

주의: CallManager 및 TVS 인증서를 동시에 재생성하지 마십시오. 이로 인해 엔드포인트에 설치된 ITL이 복구할 수 없는 불일치가 발생하므로 클러스터의 모든 엔드포인트에서 ITL을 제거해야 합니다. CallManager에 대한 전체 프로세스를 마치고 전화기가 다시 등록되면 TVS에 대한 프로세스를 시작합니다.

클러스터의 모든 TVS 노드에 대해 다음을 수행합니다.

1단계. **Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find and verify the** expiration date of the TVS certificate(TVS 인증서 찾기 및 만료 날짜 확인)로 이동합니다.

2단계. Generate CSR(CSR **생성) > Certificate Purpose(인증서 용도)를 클릭합니다. TV**. 인증서에 대해 원하는 설정을 선택한 다음 Generate를 **클릭합니다**. 성공 메시지가 나타날 때까지 기다린 후 닫기를 **클릭합니다**.

3단계. CSR을 다운로드합니다. Download CSR(**CSR 다운로드)을 클릭합니다**. Certificate **Purpose TVS(인증서 용도 TVS)를** 선택하고 Download(**다운로드)**를 클릭합니다.

4단계. CSR을 인증 기관에 보냅니다.

5단계. Certificate Authority는 서명된 인증서 체인에 대해 둘 이상의 파일을 반환합니다. 다음 순서로 인증서를 업로드합니다.

- 루트 CA 인증서를 TVS-trust로 지정합니다. **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **TVS 신뢰**. 인증서의 설명을 설정하고 루트 인증서 파일을 찾습니다.
- 중간 인증서를 TVS-trust로 지정합니다(선택 사항). **Certificate Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로** 이동합니다. **TVS 신뢰**. 인증서의 설명을 설정하고 중간 인증서 파일을 찾습니다.

  참고: 일부 CA는 중간 인증서를 제공하지 않습니다. 루트 인증서만 제공된 경우 이 단계를 생략할 수 있습니다.

- CA 서명 인증서를 TVS로 Certificate **Management(인증서 관리) > Upload certificate(인증서 업로드) > Certificate Purpose(인증서 용도)로 이동합니다. TV**. 인증서의 설명을 설정하고 현재 CUCM 노드에 대한 CA 서명 인증서 파일을 찾습니다.

  참고: 이때 CUCM은 CSR과 업로드된 CA 서명 인증서를 비교합니다. 정보가 일치하면 CSR이 사라지고 새 CA 서명 인증서가 업로드됩니다. 인증서를 업로드한 후 오류 메시지가 표시되면 Upload Certificate **Common Error Messages 섹션을** 참조하십시오.

6단계. 서버에 적용된 새 인증서를 가져오려면 필요한 서비스를 다시 시작해야 합니다(서비스가 실행되고 활성화된 경우에만). 다음으로 이동합니다.

- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스) > Cisco TFTP**(서비스가 실행되는 모든 노드)
- **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스) > Cisco Trust Verification Service**(서비스가 실행되는 모든 노드)

7단계. 모든 전화기를 재설정합니다.

- Cisco Unified **CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수) > Reset(재설정)으로 이동합니다**. You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가 포함된 팝업 창이 나타납니다. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? **OK(확인)**를 선택한 다음 Reset(재설정)**을 클릭합니다**.

  참고: RTMT를 통해 디바이스 등록을 모니터링합니다. 모든 전화기가 다시 등록되면 다음 인증서 유형으로 진행할 수 있습니다.

업로드된 일반 인증서 오류 메시지 트러블슈팅

이 섹션에는 CA 서명 인증서가 업로드될 때 가장 일반적인 오류 메시지 중 일부가 나열됩니다.

CA 인증서를 Trust-Store에서 사용할 수 없음

이 오류는 루트 또는 중간 인증서가 CUCM에 업로드되지 않았음을 의미합니다. 서비스 인증서를 업로드하기 전에 두 인증서가 신뢰 저장소로 업로드되었는지 확인합니다.

/usr/local/platform/.security/tomcat/keys/tomcat.csr 파일이 없습니다.

이 오류는 인증서(tomcat, callmanager, ipsec, capf, tvs)에 대한 CSR이 없을 때 나타납니다. CSR이 이전에 생성되었고 인증서가 해당 CSR을 기반으로 생성되었는지 확인합니다. 유의할 점:

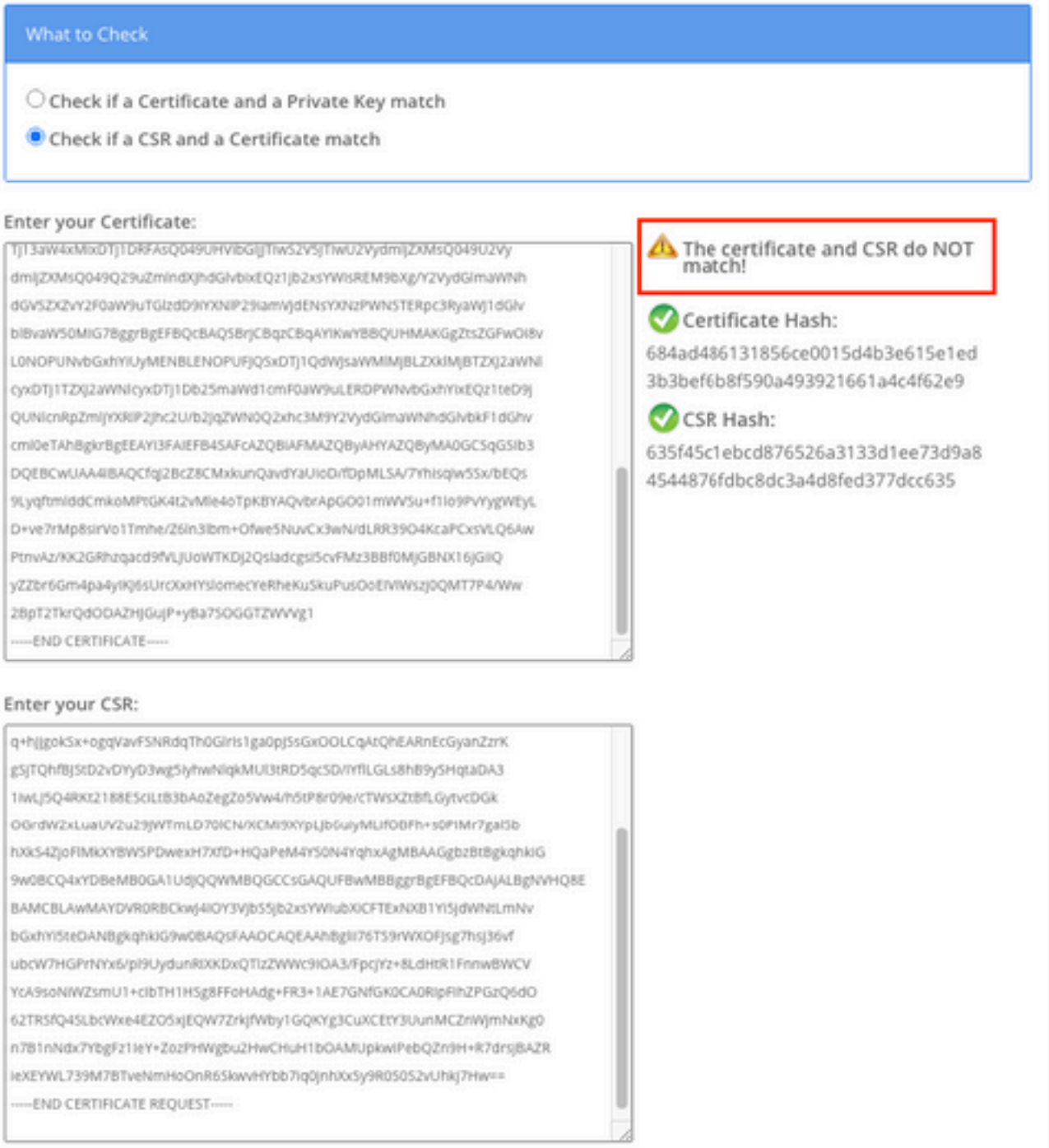
- 서버 및 인증서 유형당 1개의 CSR만 존재할 수 있습니다. 즉, 새로운 CSR이 생성되면 기존 CSR이 교체됩니다.
- 와일드카드 인증서는 CUCM에서 지원되지 않습니다.
- 새 CSR 없이 현재 사용 중인 서비스 인증서를 교체할 수 없습니다.
- 동일한 문제에 대해 또 다른 가능한 오류는 "파일 /usr/local/platform/upload/certs//tomcat.der을 업로드할 수 없습니다."입니다. 이는 CUCM 버전에 따라 다릅니다.

CSR 공개 키와 인증서 공개 키가 일치하지 않습니다.

이 오류는 CA에서 제공한 인증서에 CSR 파일에서 보낸 공개 키와 다른 공개 키가 있는 경우에 나타납니다. 가능한 원인은 다음과 같습니다.

- 잘못된 인증서(다른 노드의 인증서)가 업로드됩니다.
- CA 인증서가 다른 CSR로 생성되었습니다.
- CSR이 다시 생성되었고, 서명된 인증서를 가져오는 데 사용된 기존 CSR을 교체했습니다.

CSR 및 인증서 공개 키 일치를 확인하기 위해 SSL과 같은 여러 도구가 온라인에 있습니다.



동일한 문제에 대해 또 다른 가능한 오류는 "파일 /usr/local/platform/upload/certs//tomcat.der을 업로드할 수 없습니다."입니다. 이는 CUCM 버전에 따라 다릅니다.

CSR 주체 SAN(대체 이름) 및 인증서 SAN이 일치하지 않습니다.

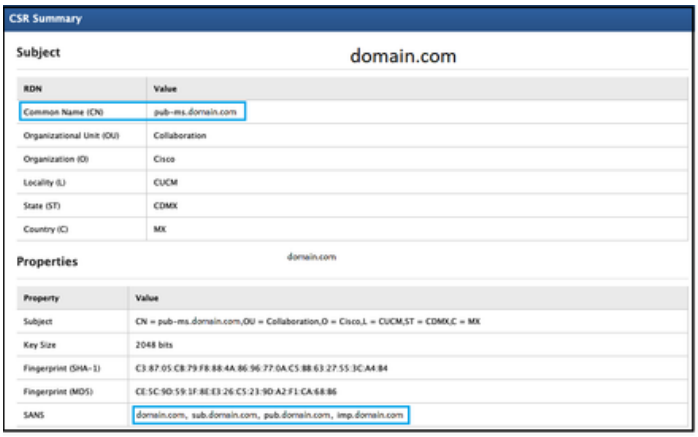
CSR과 인증서 간의 SAN이 동일해야 합니다. 그러면 허용되지 않는 도메인에 대한 인증이 방지됩니다. SAN 불일치를 확인하려면 다음 단계를 수행하십시오.

1. CSR 및 인증서를 디코딩합니다(base 64). Decoder와 같이 온라인에서 사용할 수 있는 여러 가지 디코더가 있습니다.

2. SAN 항목을 비교하고 모두 일치하는지 확인합니다. 순서는 중요하지 않지만 CSR의 모든 항목은 인증서에서 동일해야 합니다.

예를 들어, CA 서명 인증서에는 2개의 추가 SAN 항목, 즉 인증서의 CN과 추가 IP 주소가 추가됩니

다.


CSR Summary

Subject

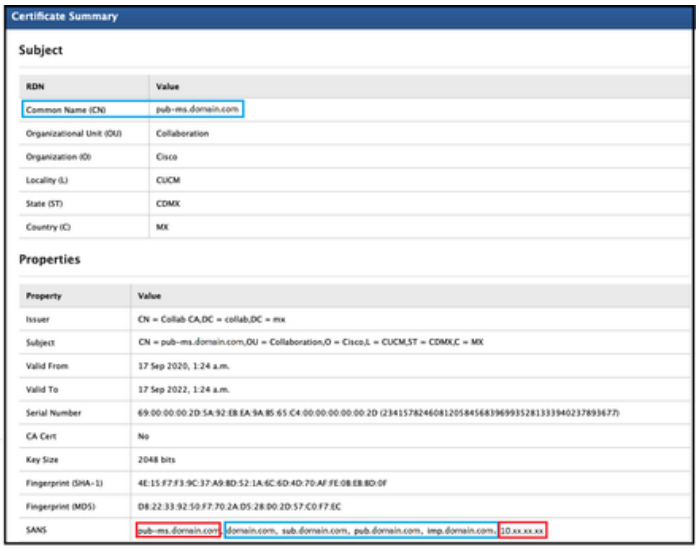
domain.com

RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX

Properties

domain.com

Property	Value
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Key Size	2048 bits
Fingerprint (SHA-1)	C3:87:05:CB:79:F8:88:4A:86:96:77:0A:C5:88:63:27:55:3C:A4:B4
Fingerprint (MD5)	CE:5C:9D:59:1F:8E:E3:26:C5:23:9D:A2:F1:CA:68:86
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com


Certificate Summary

Subject

RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX

Properties

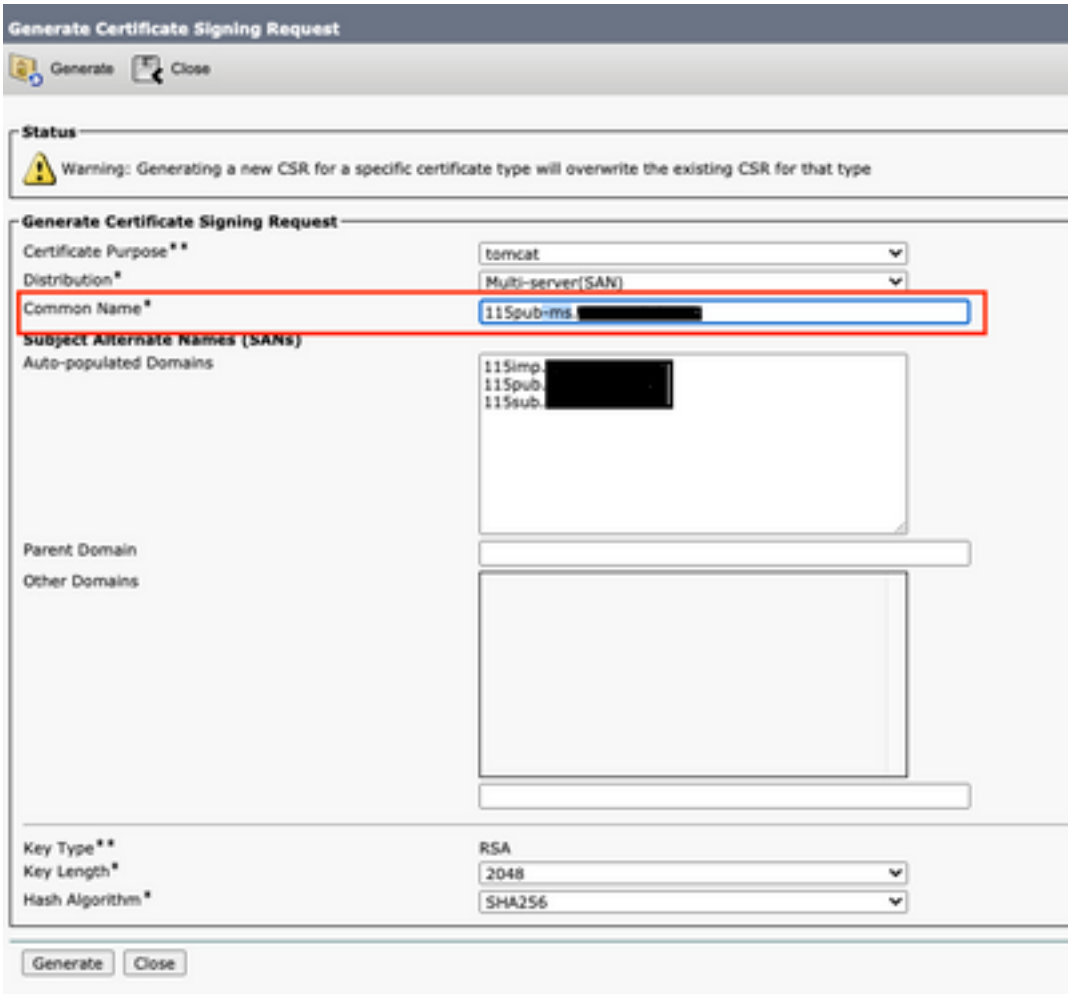
Property	Value
Issuer	CN = Collab CA,DC = collab,DC = mx
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Valid From	17 Sep 2020, 1:24 a.m.
Valid To	17 Sep 2022, 1:24 a.m.
Serial Number	69:00:00:00:2D:5A:92:EB:EA:9A:B5:65:C4:00:00:00:00:00:2D (234157824608120584568396993528133394023789367?)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	4E:15:F7:F3:9C:37:A9:BD:52:1A:6C:6D:4D:70:AF:FE:0B:EB:BD:0F
Fingerprint (MD5)	D8:22:33:92:50:F7:70:2A:D5:28:00:2D:57:C0:F7:EC
SANS	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx

3. SAN이 일치하지 않는 경우 이를 해결하기 위한 두 가지 옵션이 있습니다.

1. CA 관리자에게 CSR로 전송되는 것과 동일한 SAN 항목이 있는 인증서를 발급하도록 요청합니다.
2. CA의 요구 사항과 일치하는 CSR을 CUCM에 생성합니다.

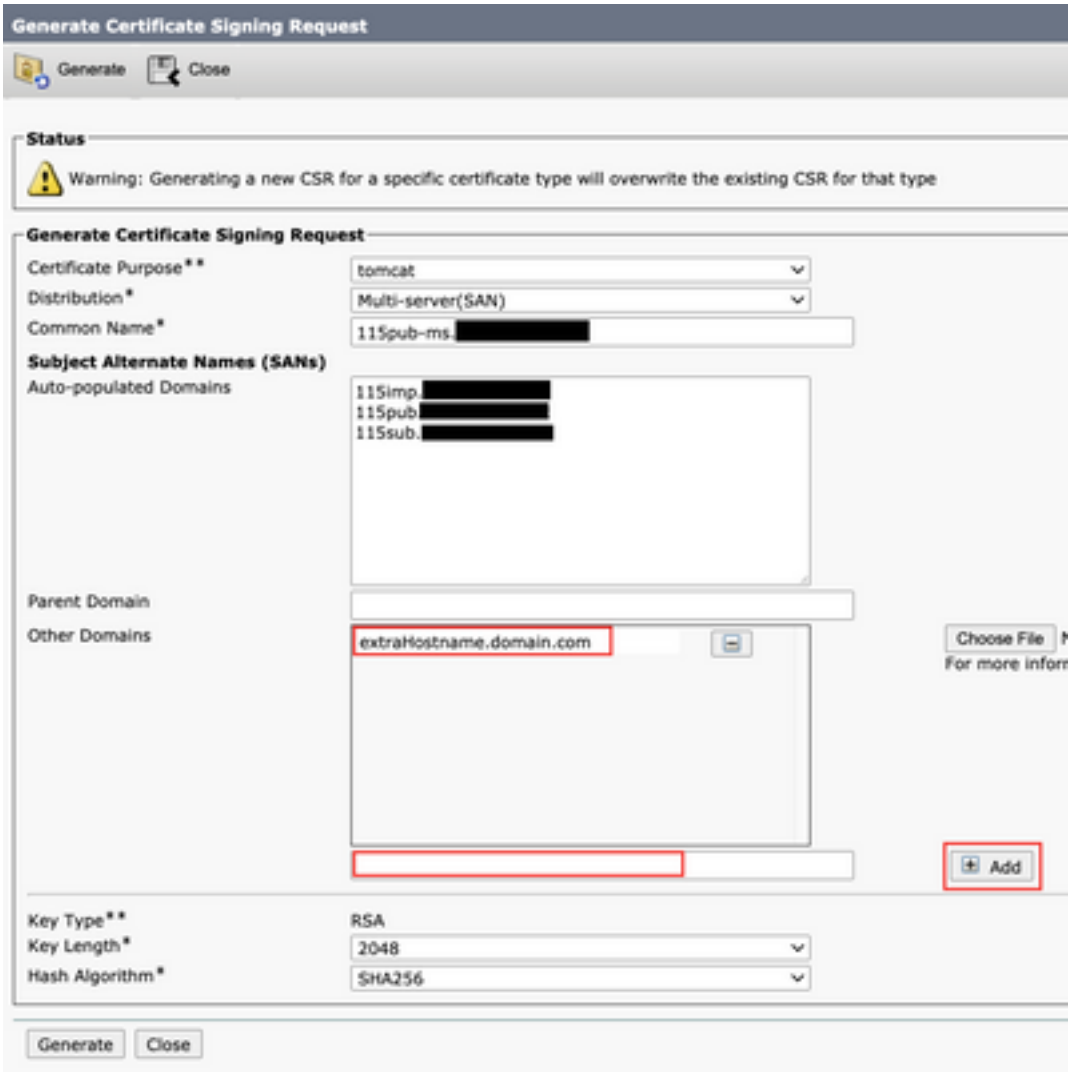
CUCM에서 생성한 CSR을 수정하려면 다음을 수행합니다.

1. CA가 도메인을 제거하면 도메인 없이 CUCM의 CSR을 생성할 수 있습니다. CSR을 생성하는 동안 기본적으로 채워져 있는 도메인을 제거합니다.
2. 멀티 SAN 인증서가 생성된 경우, CA에서 CN에 "-ms"를 허용하지 않습니다. "-ms"는 생성될 때 CSR에서 제거할 수 있습니다.



3. CUCM에서 자동으로 완료한 이름 외에 대체 이름을 추가하려면

   1. 다중 SAN 인증서를 사용하는 경우 FQDN을 더 추가할 수 있습니다. (IP 주소는 허용되지 않습니다.)



b. 인증서가 단일 노드인 경우 set web-security 명령을 실행합니다. 이 명령은 멀티 SAN 인증서에도 적용됩니다. (모든 종류의 도메인을 추가할 수 있으며 IP 주소도 허용됩니다.)

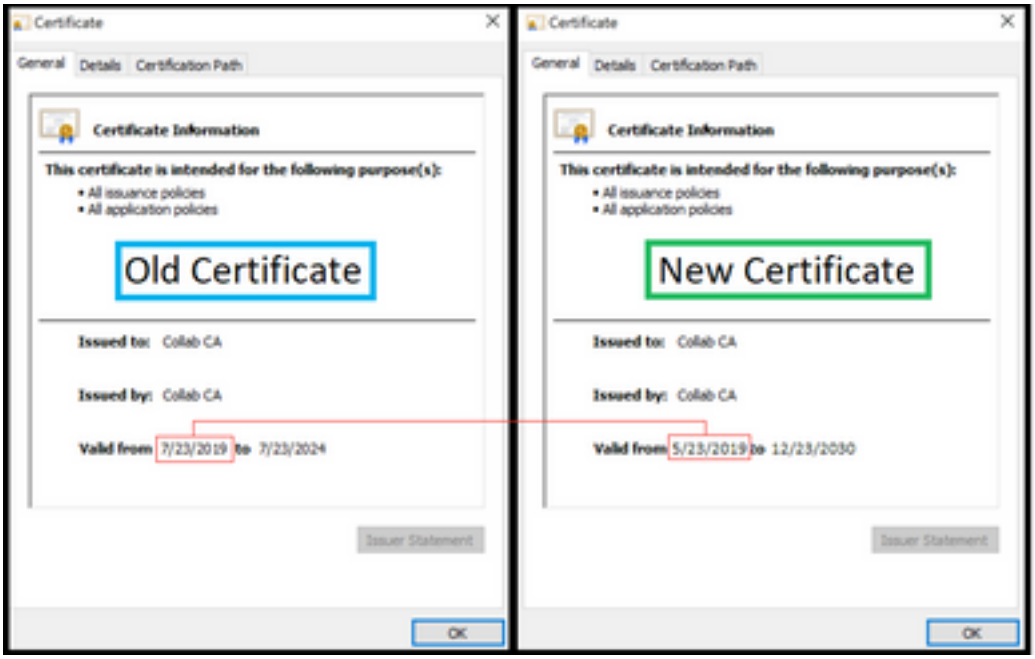
자세한 내용은 명령줄 참조 설명서를 참조하십시오.

동일한 CN의 트러스트 인증서는 교체되지 않습니다.

CUCM은 동일한 CN(Common Name) 및 인증서 유형이 동일한 하나의 인증서만 저장하도록 설계되었습니다. 즉, tomcat-trust인 인증서가 데이터베이스에 이미 있으며 동일한 CN을 가진 최신 인증서로 교체해야 하는 경우 CUCM은 기존 인증서를 제거하고 새 인증서로 교체합니다.

CUCM이 기존 인증서를 대체하지 않는 경우가 있습니다.

1. 업로드된 인증서가 만료되었습니다. CUCM에서는 만료된 인증서를 업로드할 수 없습니다.
2. 이전 인증서의 "시작" 날짜가 새 인증서의 "시작" 날짜보다 더 최근입니다. CUCM은 가장 최근의 인증서를 보관하며, 이전 "FROM" 날짜가 있으면 이전 날짜로 카탈로그화됩니다. 이 시나리오에서는 원치 않는 인증서를 삭제한 다음 새 인증서를 업로드해야 합니다.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Old Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 7/23/2019 to 7/23/2024
Issuer Statement
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
New Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 5/23/2019 to 12/23/2030
Issuer Statement
OK

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.