# CUCM에서 인증서 갱신과 관련된 일반적인 문제 해결

## 소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)에서 인증서를 재생성한 후 발생하는 일반적인 문제와 그 해결 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM 인증서 갱신 프로세스
- CUCM GUI 인터페이스
- Expressway 서버
- CUCM 프로세스를 통한 디바이스 등록
- 인증 기관 프록시 기능
- Cisco Unified Communications Manager 보안 설명서

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 버전 15

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.

### 비즈니스 영향

이 표에는 각 인증서 갱신이 운영에 미치는 비즈니스 영향이 표시됩니다. 정보를 주의 깊게 검토하십시오. 각 인증서의 위험 수준에 따라 몇 시간 후 또는 조용한 기간에 필요한 인증서를 갱신합니다.

Low Impact  Medium Impact.  High Impact.

| Type | Risk | Trust List | Impact | Phone Restart | Service Restart |
|---|---|---|---|---|---|
| Tomcat | | - | Web services, SSO, EM/EMCC Login | None | Tomcat |
| IPSec | | - | DRS, Ipsec Tunnels | None | DRF Master/Local |
| CAPF | | CTL + ITL | LSC must be updated, secure features | All | CAPF |
| Callmanager | | CTL + ITL | Registration, TL issues, Trunks, CTI | All | CM,CTI,TFTP |
| TVS | | ITL | Verification of TLs, CFG files, https connection | Some | TVS |
| ITLRecovery | | CTL + ITL | Signer or SAST backup for ITL/CTL | All | |

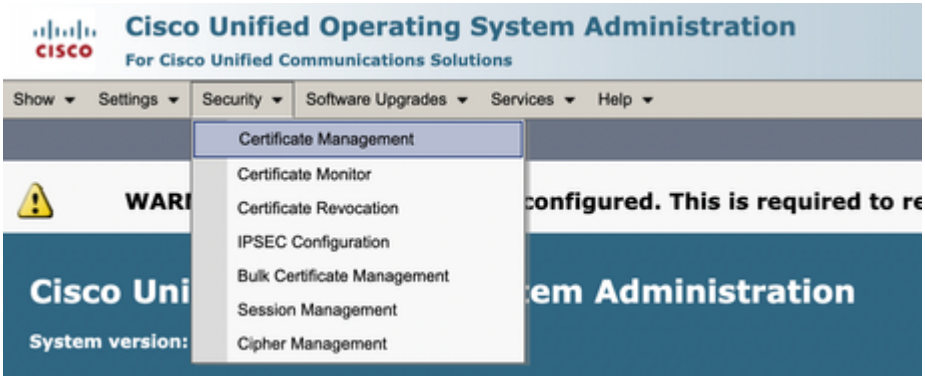
## 시나리오 1: Call Manager, TVS 및 ITL 인증서 갱신 후 전화기가 등록되지 않음

참고: 이 시나리오는 CUCM 혼합 모드 및 비보안 클러스터 하의 구축에 적용되며, 또한 자체 서명 인증서 및 CA 인증서에 적용됩니다.

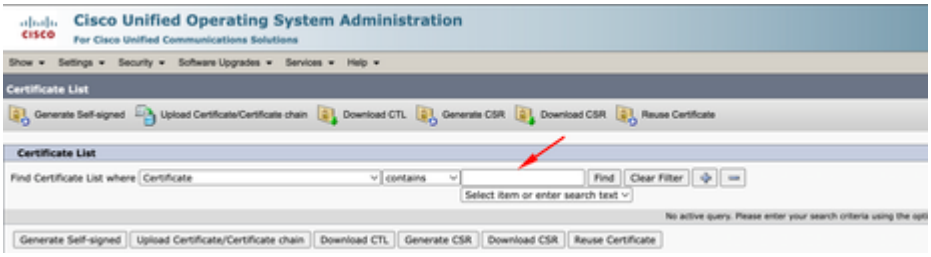
Call Manager, TVS 및 ITL 인증서가 만료되고 동시에 갱신되면 모든 전화기가 등록되지 않은 상태로 유지되어 시스템에 심각한 영향을 미치게 되며, 이는 전화기가 CUCM을 신뢰하지 않도록 트리거될 때 예상되는 동작입니다.

### 확인

1. 인증서가 Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리)에서 이미 만료되었는지 확인합니다.

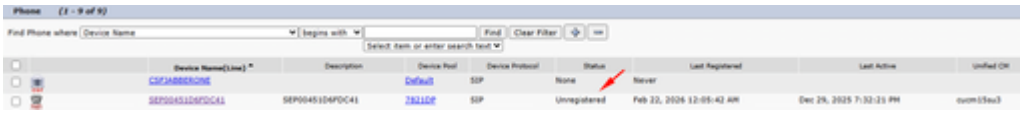



2. 페이지 상단의 필터 아래에서 Callmanager, TVS 또는 ITL로 검색하고, contains(포함) 또는 begins with options(옵션으로 시작)를 사용합니다.




3. 인증서는 만료 열 아래에 최신 상태와 확인이 표시되어야 합니다(TVS 및 ITL 인증서의 경우도 동일).

4. 인증서 갱신 후 모든 상태가 정상으로 확인되면 전화기가 등록되지 않음 상태로 표시됩니다.

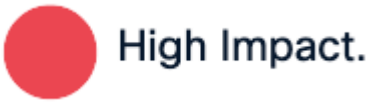


## 솔루션

이 문제를 해결하기 위한 2가지 옵션이 있습니다.

1. 전화기에서 현재 보안 설정을 지우고 전화기에서 새 인증서를 가져올 수 있도록 전화기의 공장 초기화 수행
2. 게시자 노드의 CLI에서 ITL 및 CTL 인증서를 업데이트하고 명령을 사용합니다 utils itl reset localkey(유틸리티 itl 재설정 로컬 키)입니다.
   이 단계는 등록된 전화기를 포함한 모든 전화기에 영향을 미칩니다. 이 작업은 몇 시간 후에

수행해야 합니다.



---

## 시나리오 2: Tomcat 인증서 갱신 후 단일 로그인이 작동하지 않음

---

참고: 이 시나리오는 SSO(Single Sign-On) 컨피그레이션에 클러스터 전체 또는 노드별 계약을 사용하는 구축에 적용할 수 있습니다

---

SSO(Single Sign-on)를 사용하여 CUCM 내에서 로그인하면 오류 메시지 ¨saml 응답을 처리하는 동안 오류가 발생했습니다¨ 또는 ¨saml 응답을 처리하는 동안 오류가 발생했습니다. 비밀 키를 해독하지 못했습니다¨

### 확인

1. 자체 서명된 경우 모든 노드에 유효한 tomcat 인증서가 포함되어 있는지 또는 연결된 새 multi-san tomcat 인증서가 포함되어 있는지 확인합니다.
2. 디버그 레벨에서 SSO 로그를 활성화하려면 CLI를 통해 모든 CUCM 노드에서 samltrace 레벨 디버그 설정을 사용합니다
3. CUCM에 다시 로그인하여 문제를 다시 생성하고 SSO 방법을 사용합니다.
4. 인시던트 이후 Tomcat SSO 로그를 수집하고 다음 메시지가 표시되는지 확인합니다.
    - 

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authenticatio
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
              at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...
```

### 솔루션

Tomcat 인증서 갱신 후 CUCM 메타데이터를 내보내고 ID 공급자 서버로 가져와 이 통신에 사용할 새 tomcat 인증서가 있는지 확인합니다.

SSO 구축을 활성화하여 tomcat을 갱신하는 절차:

---

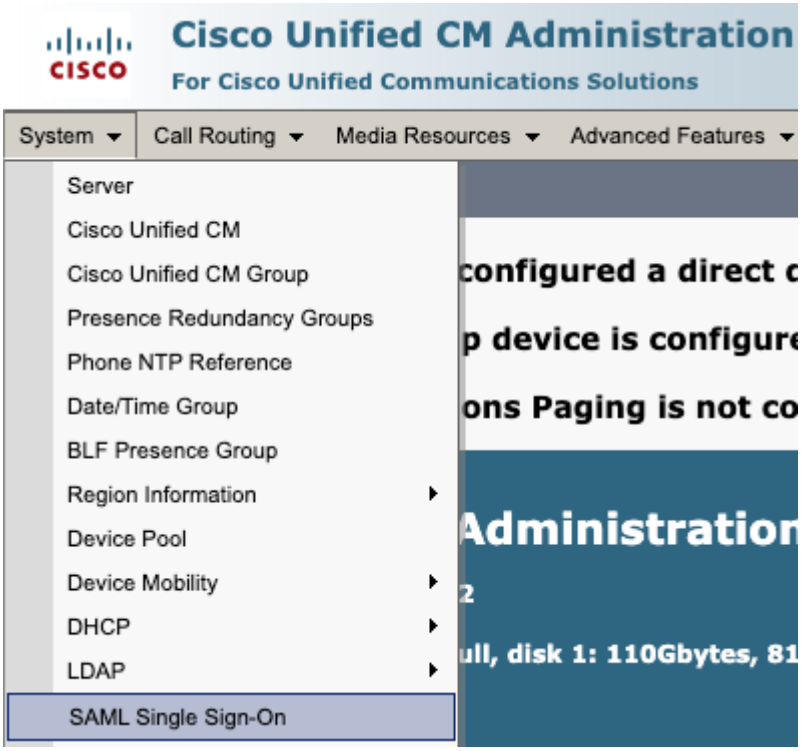
⚠ 주의: TAC(Technical Assistance Center)에서는 Tomcat 인증서 갱신 후 문제가 발생하지 않도록 다음 단계를 권장하며, 이 절차를 몇 시간 후에 수행하도록 권장합니다.

---

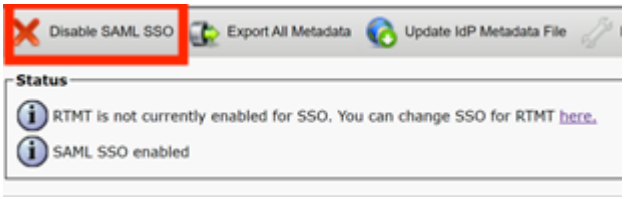
Low Impact

1. 모든 CUCM 노드에서 SSO 비활성화


- CM 관리 > 시스템 > SAML Single Sign-on에 액세스



- Disable SAML SSO(SAML SSO 비활성화)를 선택합니다

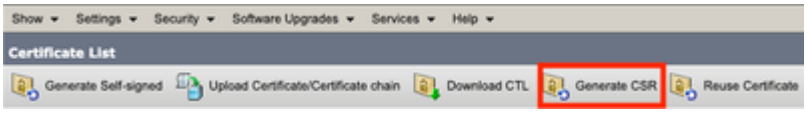



- 이 프로세스는 노드별 계약을 사용하는 경우 GUI를 통해 나머지 모든 노드에서 수행해야 합니다.

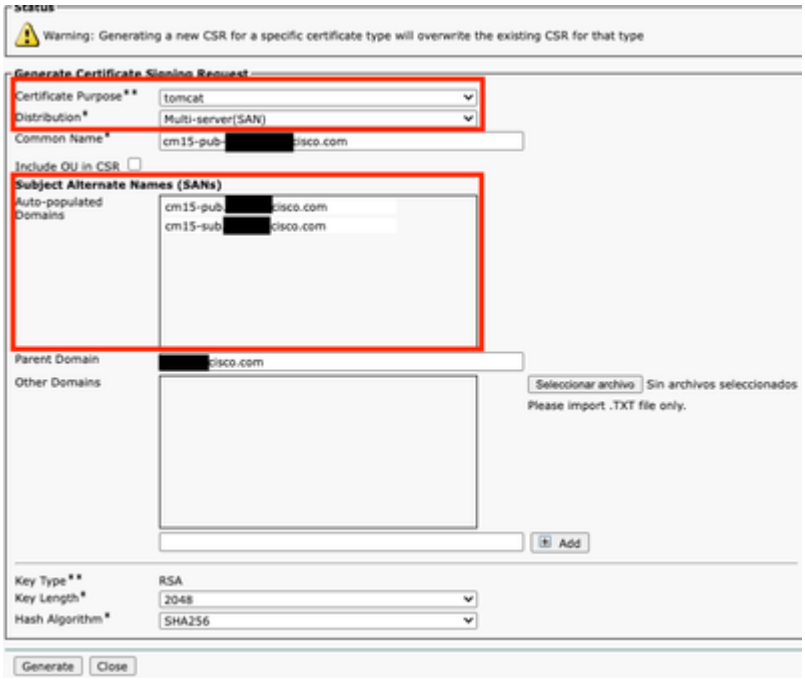
2. CUCM 클러스터에서 Tomcat 인증서 갱신


CUCM 클러스터에서 Tomcat 다중 SAN 인증서를 갱신하는 전반적인 절차:

- OS administration(OS 관리) > Security(보안) > Certificate management(인증서 관리)로 이동합니다.
- Generate CSR(CSR 생성)을 선택합니다.




- Certificate Porpuse에서 Tomcat을 선택합니다.
- Distribution에서 Multi-SAN을 선택합니다.
- 클러스터의 모든 노드가 Auto-populated Domains(자동 입력 도메인) 아래에 나열되어 있는지 확인합니다.




- Generate를 선택합니다. 클러스터의 모든 노드에서 CSR이 생성되었는지 확인합니다.
- 생성된 CSR을 CUCM 게시자에서 다운로드하고 CA(Certificate Authority) 서버로 서명합니다 .
- OS administration(OS 관리) > Security(보안) > Certificate management(인증서 관리)로 이동합니다. Upload certificate/Certificate chain(인증서/인증서 체인 업로드)을 선택합니다.
- CA 인증서를 Tomcat-trust로 업로드합니다.
- 6단계를 반복한 다음 Tomcat 서명 인증서를 Tomcat으로 업로드합니다.
- 완료하고 모든 노드에 새 tomcat 인증서가 적용되었는지 확인한 후 클러스터의 모든 노드에서 CLI를 통해 Tomcat 서비스를 재시작합니다. 이 명령 utils service restart Cisco Tomcat.

자세한 내용은 다음 설명서를 참조하십시오.

- Tomcat 자체 서명 인증서 다시 생성
- Tomcat CA 서명 인증서를 다시 생성합니다.

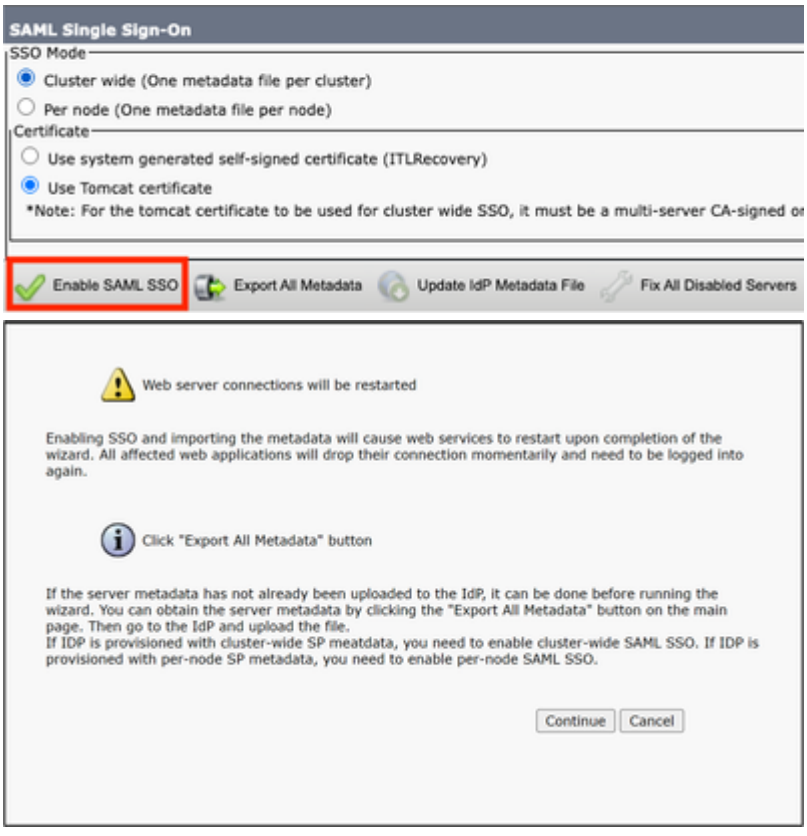
3. SP(서비스 공급자) 메타데이터 내보내기


- CM administration(CM 관리) > System(시스템) > Single Sign-On(단일 로그인)으로 이동합니다.
- SSO 옵션을 구성한 다음(이 경우 SSO 모드에서 클러스터 전체를 사용하고 인증서에서 tomcat 인증서 사용을 예로 구성함) 모든 메타데이터 내보내기를 선택합니다

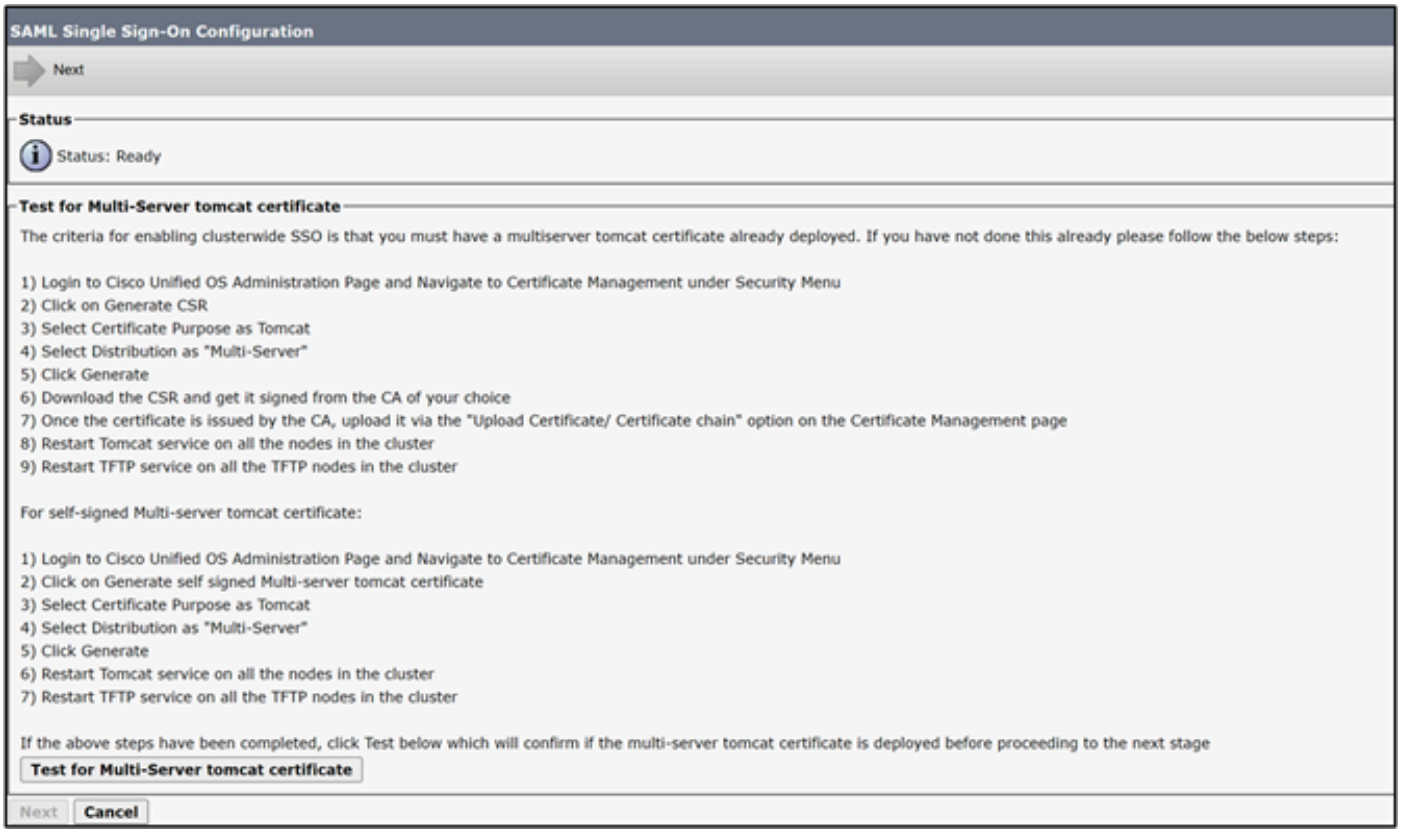

- SP 메타데이터를 IdP(Identity Provider) 서버로 가져옵니다. 자세한 내용은 ID 공급자에 SAML SSO 구성을 참조하십시오

4. CUCM 클러스터에서 SSO 활성화

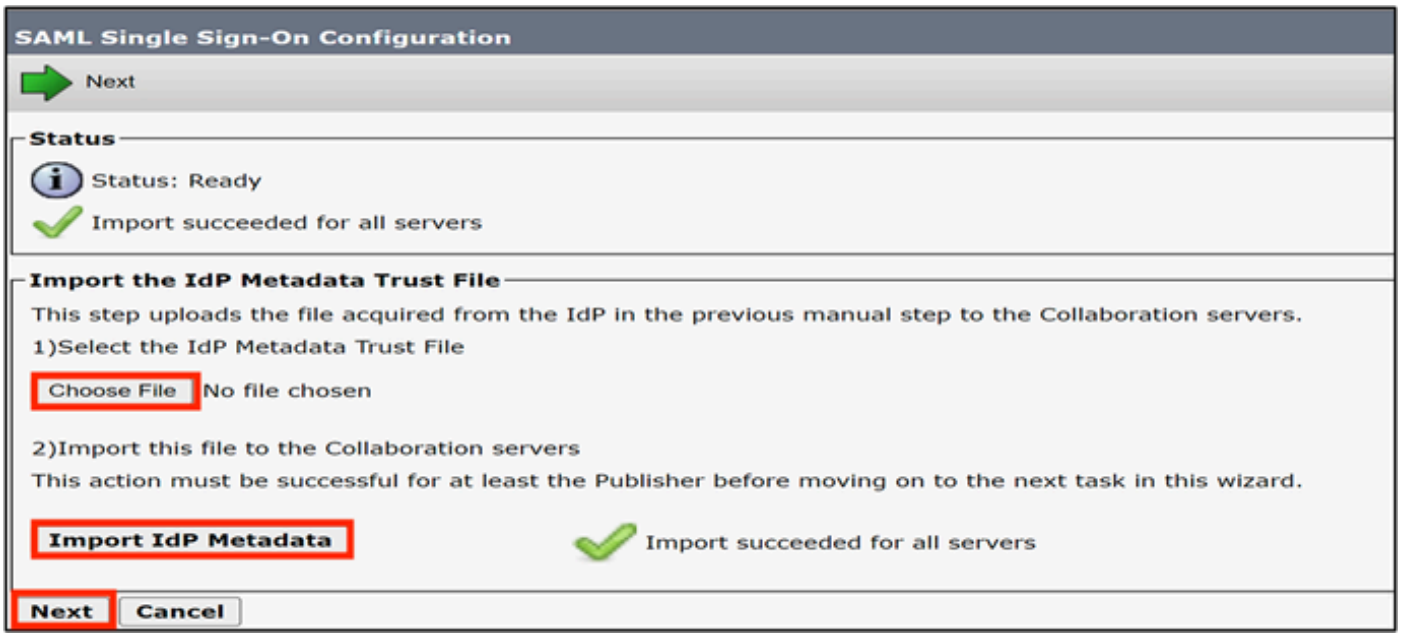

- CM administration(CM 관리) > System(시스템) > Single Sign-On(단일 로그인)으로 이동합니다.
- CUCM 메타데이터를 내보내는 동안 동일한 SSO 옵션을 선택한 상태에서 Enable SAML SSO(SAML SSO 활성화)를 선택하고 Continue(계속)를 선택합니다.



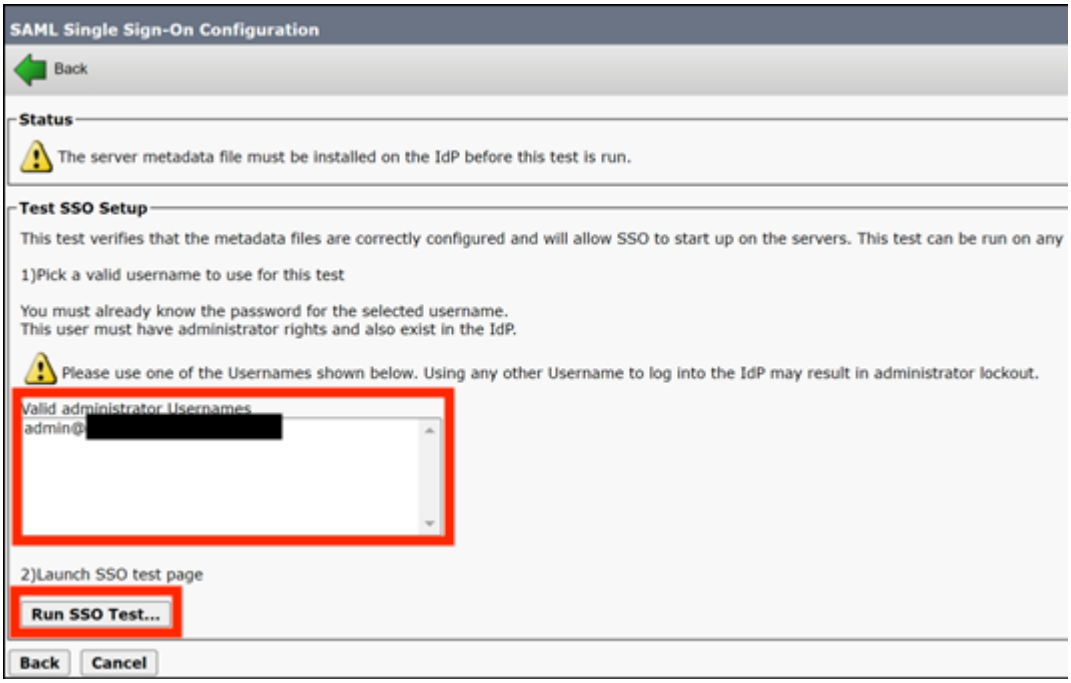
- 클러스터 전체에 적용되는 경우 이 단계를 사용하여 모든 노드에서 다중 SAN 인증서를 확인할 수 있습니다. Test for multi-server tomcat certificate(다중 서버 tomcat 인증서 테스트)를 선택합니다. 완료되면 다음을 선택합니다.

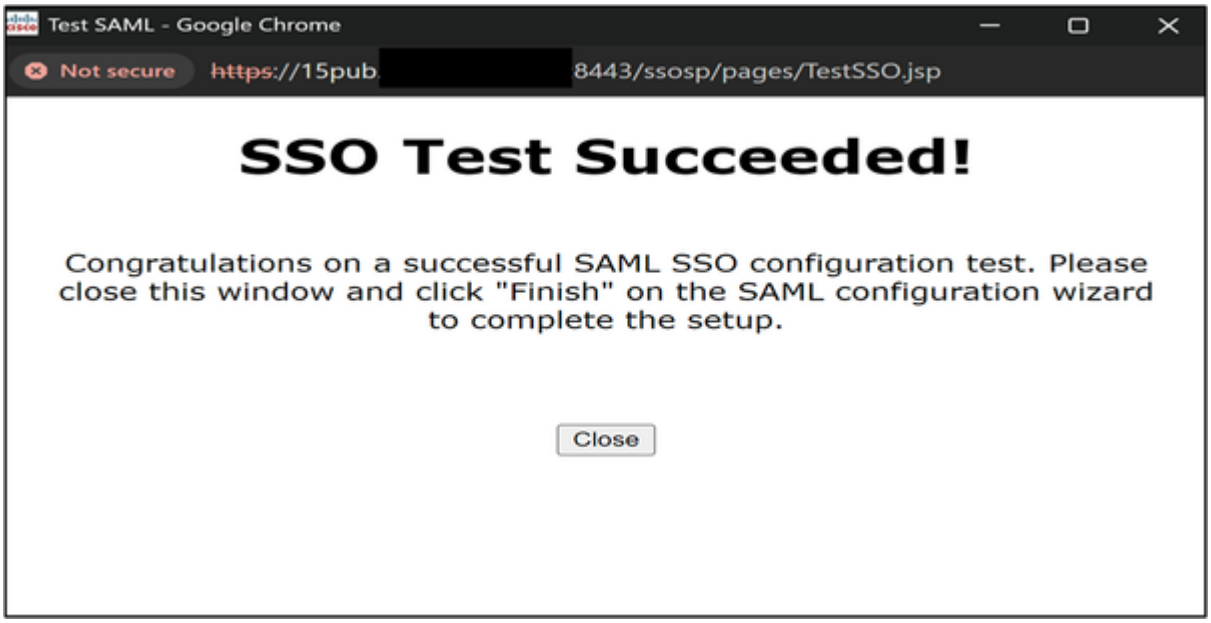



- IdP 메타데이터를 업로드하고 Import IdP Metadata(IdP 메타데이터 가져오기)를 선택한 후 완료되면 Next(다음)를 선택합니다.



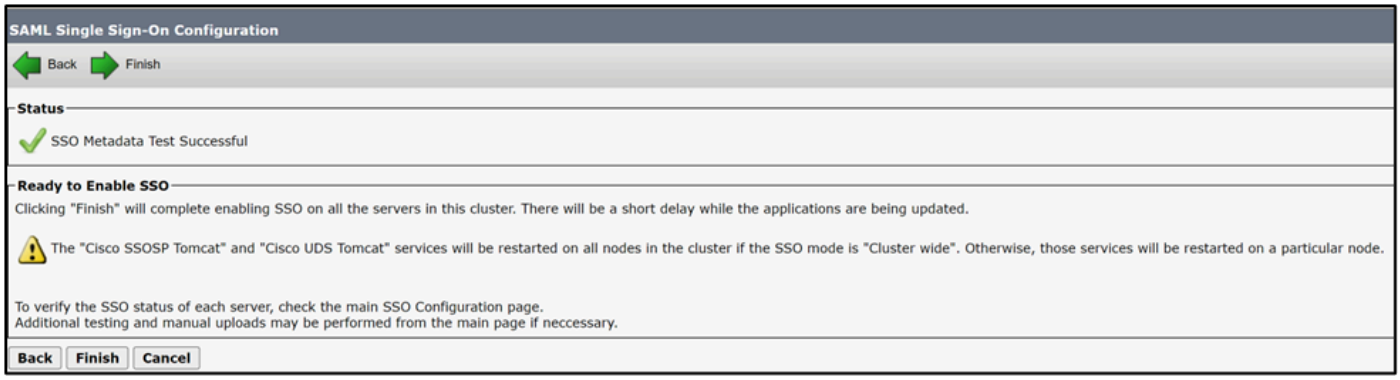
- Test SSO Setup(테스트 SSO 설정)에서 Standard CCM Super Users(표준 CCM 수퍼 사용자) 그룹이 할당된 사용자를 선택하고 Run SSO Test(SSO 테스트 실행)를 선택하여 성공합니다.




4. SSO를 활성화한 후 필요한 서비스를 다시 시작합니다.


- SSO를 활성화하면 tomcat 서비스가 다시 시작됩니다.




그러나 TAC에서는 SSO 활성화 프로세스 후 모든 노드에서 Tomcat(utils service restart Cisco Tomcat) 및 UDS Tomcat(utils service restart CiscoUDSTomcat) 서비스를 수동으로 재시작하는 것이 좋습니다.

---

# 시나리오 3: 인증서 갱신 후 모빌리티 및 원격 액세스 등록 문제

Webex 앱은 Call Manager, Tomcat 및 Expressway C 인증서가 혼합 모드 구축에서 갱신된 후 MRA(Mobility and Remote Access)를 통해 CUCM에 등록할 수 없습니다.

## 확인

1. CUCM 통화 관리자 및 Tomcat 인증서는 CA 서명 인증서입니다.
2. CUCM 및 Expressway 구축은 TLS(혼합 모드)에서 실행됩니다.
3. inspect Expressway-C 로그에는 "SSL routes:ssl3_read_bytes:tlsv1 alert unknown ca"가 표시됩니다.
   <#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
 Host: expc.cisco.com:6972
 Accept: */*
 Cookie:<CONCEALED>
 User-Agent: WebEx/0.0.0.0
 TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
 Client-ip: xxx.xxx.xxx.xxx
 X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
 Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9

 |

2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for

SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

## 솔루션

신뢰 관계를 보장하기 위해 CUCM과 Expressway-C 간에 인증서를 내보내고 가져옵니다.

---

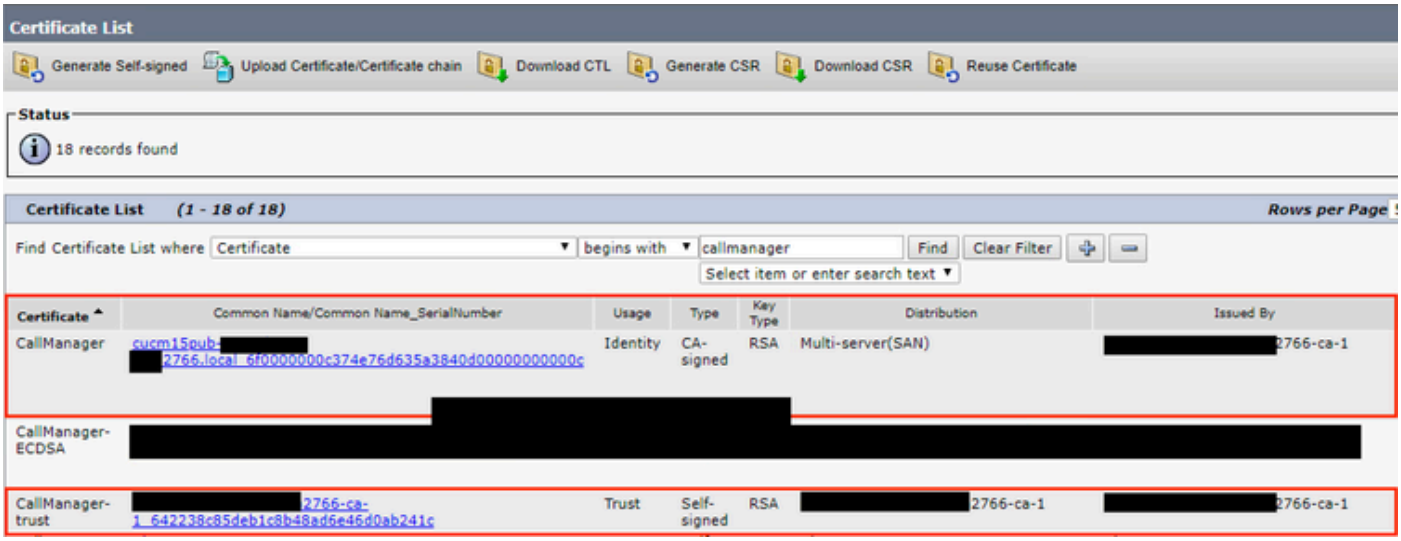
⚠ 주의: 이 절차에는 서비스를 다시 시작해야 하므로 TAC에서는 몇 시간 후에 이 작업을 수행하는 것이 좋습니다. 비즈니스 영향:

---

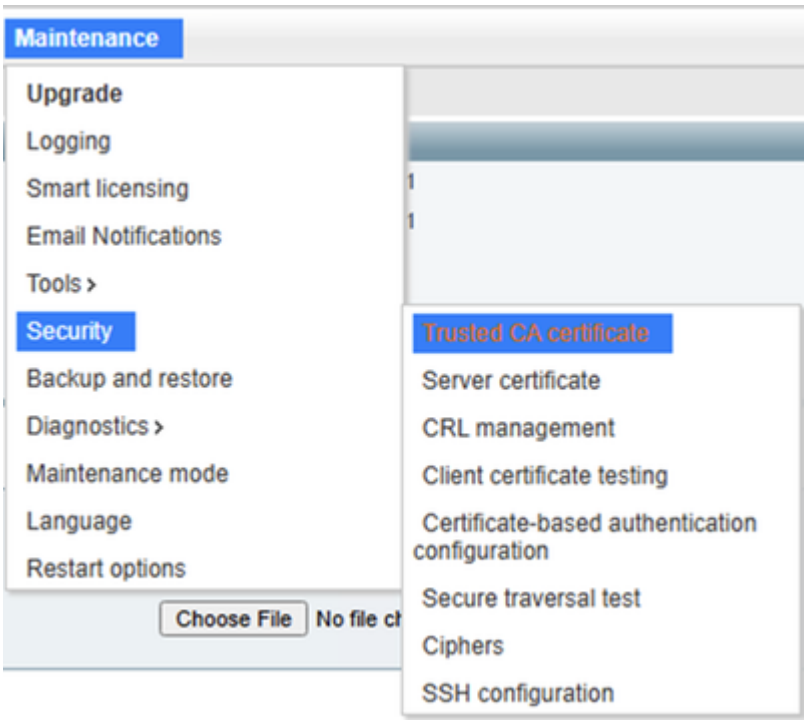
Medium Impact.

1. CA 서명 인증서를 사용하여 CUCM과 Expressway 간의 신뢰 관계를 완료하는 절차


OS administration(OS 관리) > Security(보안) > Certificate management(인증서 관리)로 이동하고 Call Manager 및 Tomcat 인증서에 서명하는 루트 CA 인증서 및 중간(있는 경우)을 다운로드합니다.



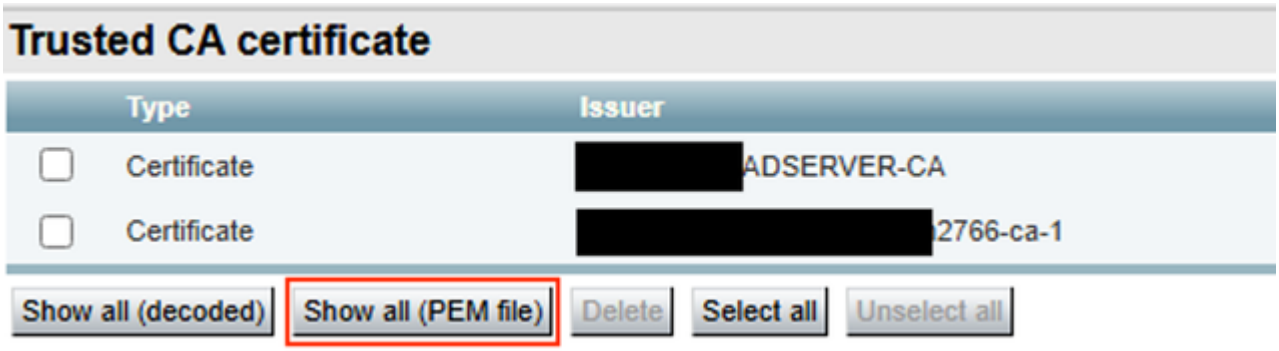

그런 다음 Expressway-C > Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동하고 Call Manager의 CA 인증서와 Tomcat 인증서를 업로드합니다.



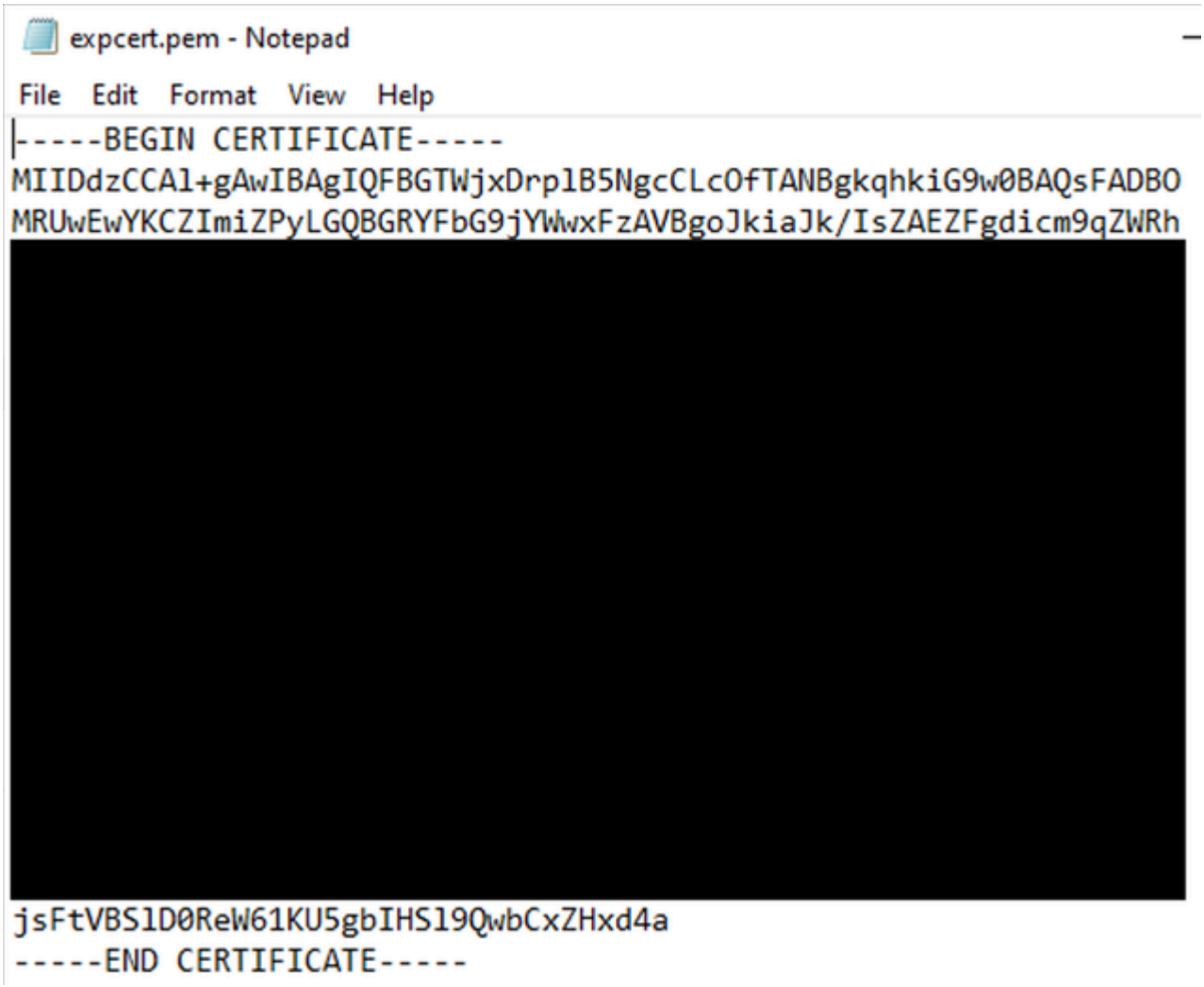



참고: Call Manager 및 Tomcat 인증서가 자체 서명된 경우, 실제 Call Manager 및 Tomcat 인증서를 다운로드하고 Expressway에 업로드합니다.

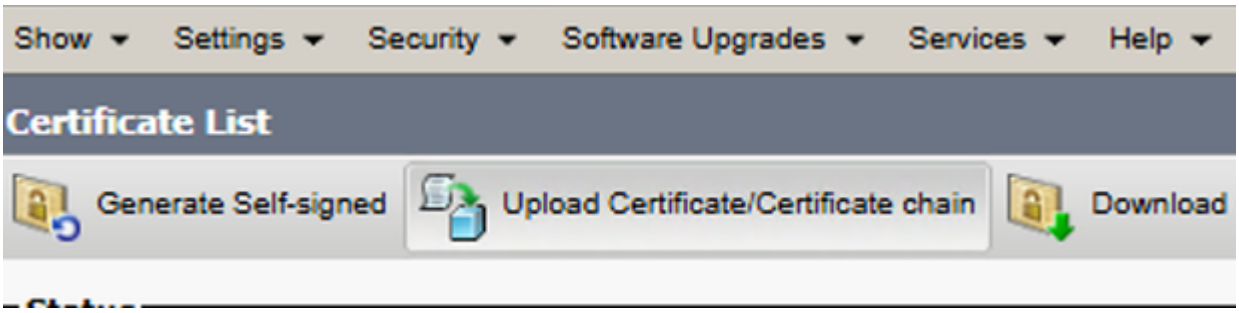

Expressway-C > Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서) > Show all (PEM file)(모두 표시(PEM 파일))로 이동합니다.

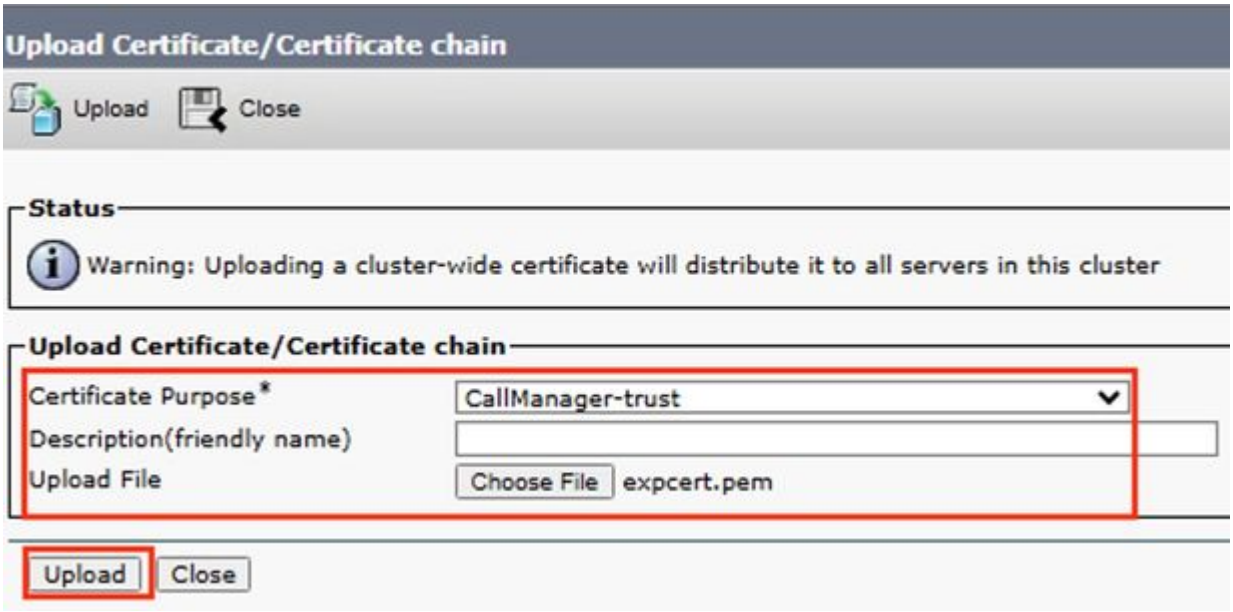



Expressway-C에 서명한 CA 인증서의 PEM 값을 복사하여 txt 파일에 저장합니다.




OS administration(OS 관리) > Security(보안) > Certificate management(인증서 관리)로 이동하고 Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드)을 선택하고 Expressway-C CA 인증서를 Tomcat-trust 및 Call Manager-trust로 업로드합니다





CUCM 클러스터에서 필요한 서비스를 다시 시작합니다.

- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동하고 Cisco CallManager 서비스를 실행하는 모든 노드에서 Cisco CallManager 서비스를 재시작합니다.
- Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동하고 Cisco TFTP 서비스를 실행하는 모든 노드에서 해당 서비스를 다시 시작합니다.
- utils service restart Cisco Tomcat 명령을 사용하여 CLI를 통해 클러스터의 모든 노드에서 Tomcat 서비스를 재시작합니다.
- utils service restart Cisco HAProxy 명령을 사용하여 CLI를 통해 클러스터의 모든 노드에서 Cisco HAproxy 서비스를 재시작합니다.

---

# 시나리오 4: CA(Certificate Authority) 프록시 기능 인증서 원인 갱신

## 시나리오 4.1: 802.1x 인증 실패

CUCM 게시자에서 CAPF(Certificate Authority Proxy Function) 인증서를 다시 생성한 후에는 전화기에서 ASA를 인증하지 않습니다.

확인

1. 전화 상태 메시지에 "802.1x 인증: 실패"


2. 영향을 받는 서버의 전화 로그를 검사하고 "SSL_ERROR_WANT_READ"를 찾습니다.

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 appl
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
```

```
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

솔루션

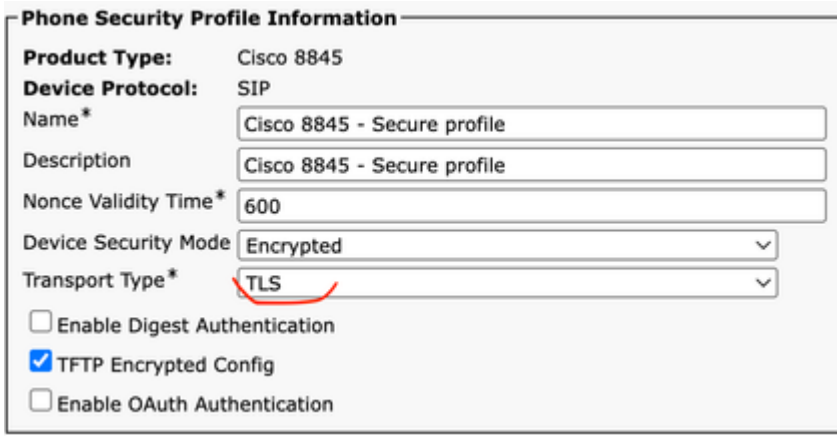
CUCM 게시자에서 CAPF 인증서를 다운로드하고 인증 서버에 업로드합니다. 802.1x를 우회하여 등록을 허용하고 영향을 받는 전화기에 LSC 인증서를 설치합니다.

## 시나리오 4.2: TLS 모드에서 보안 프로파일을 사용하는 CUCM에는 전화기가 등록되지 않습니다.

CUCM 게시자에서 CAPF 인증서를 다시 생성한 후 전화기에 "Phone is registering(전화기가 등록 중)"이 표시됩니다.

확인

1. 영향을 받는 전화기에 TLS 모드가 활성화된 보안 프로파일이 포함되어 있습니다.




2. 영향을 받는 전화기에 LSC 인증이 설치되어 있습니다.
3. CAPF 인증서가 최신 상태인지 확인합니다.


4. CUCM 게시자에 로그인하고 이전 CAPF 인증서 일련 번호를 표시하는 show ctl 명령을 사용합니다.
5. 그런 다음 전화기 보안 프로필을 비보안으로 변경합니다.

솔루션

CUCM에서 CTL 파일을 재생성하고 필요한 서비스를 재시작하여 전화기가 CAPF 파일이 있는 새 CTL 파일을 가져오도록 합니다.

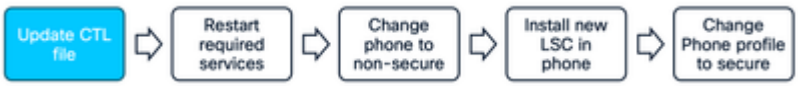
---

⚠ 주의: 이 절차에는 서비스를 다시 시작해야 하므로 TAC에서는 몇 시간 후에 이 작업을 수행하는 것이 좋습니다. 비즈니스 영향:

---

Medium Impact.

CAPF를 성공적으로 갱신하기 위한 절차.




```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

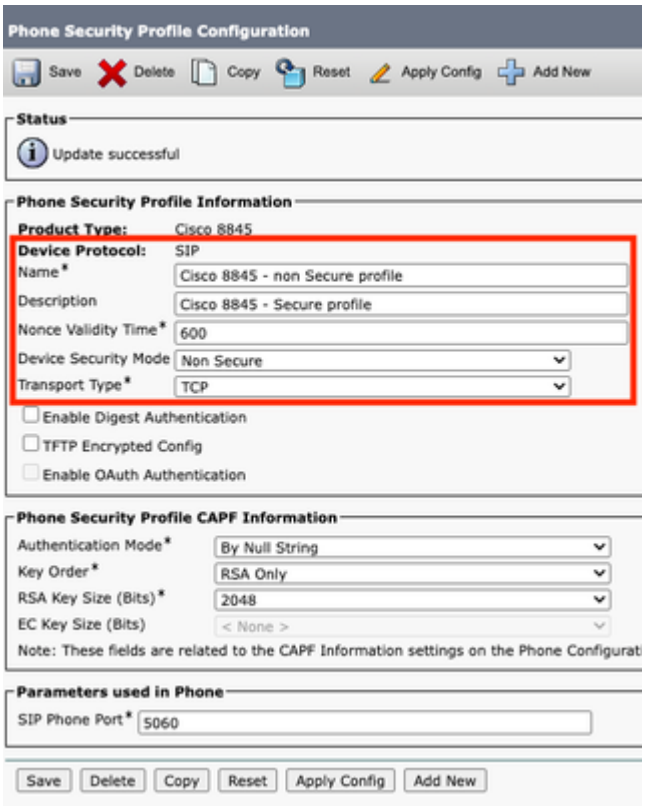
CAPF 재생성 후 CTL 파일을 업데이트합니다. 게시자의 CLI에 로그인하고 utils ctl update CTLFile 명령을 입력합니다.


1. CUCM 게시자의 Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동하고 CAPF 서비스를 재시작합니다.
2. Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(Control Center - 네트워크 서비스)로 이동하고 Cisco Trust Verification Service를 실행하는 모든 노드에서 Cisco Trust Verification Service를 다시 시작합니다.
3. Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동하고 Cisco TFTP Service를 실행하는 모든 노드에서 다시 시작합니다

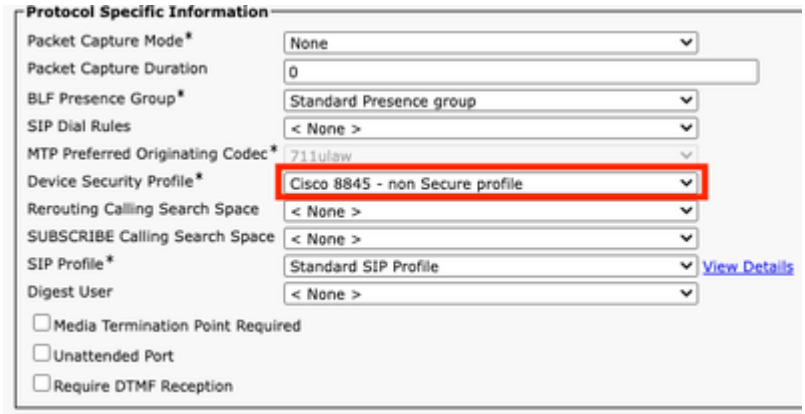
- CM administration(CM 관리) > System(시스템) > Security(보안) > Phone Security Profile(전화기 보안 프로파일)로 이동합니다.

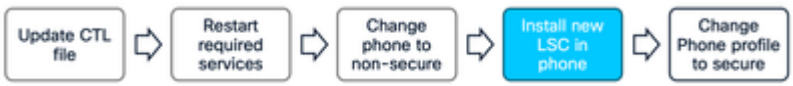

- 필요한 전화기에 할당된 현재 전화기 보안 프로필을 복사합니다.

- 이름 및 디바이스 보안 모드를 비보안으로 변경하고 컨피그레이션 저장 및 적용을 선택하여 이 변경 사항을 모든 필수 전화기에 적용합니다.



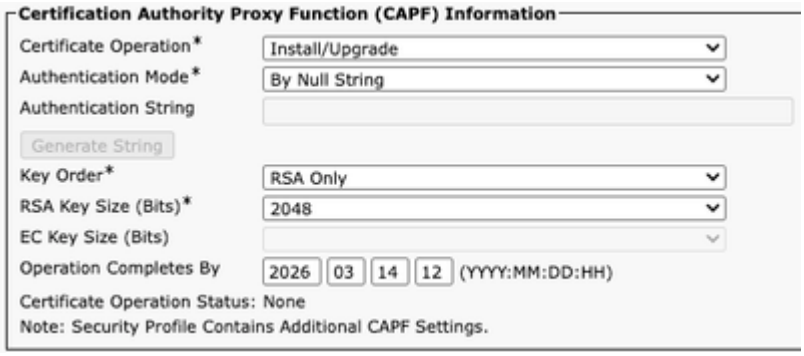

- 생성한 디바이스 보안 프로파일을 필수 전화기 컨피그레이션에 적용하고 Save and Apply Config를 선택합니다.



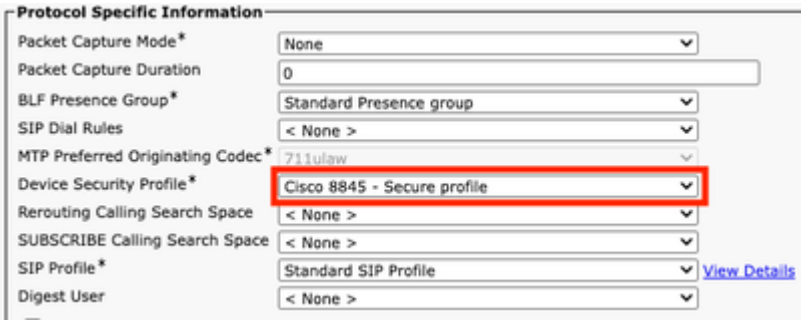

영향을 받는 전화기의 디바이스 컨피그레이션에서 CAPF 정보 섹션을 사용하여 필요한 전화기에 LSC 인증서를 설치합니다.

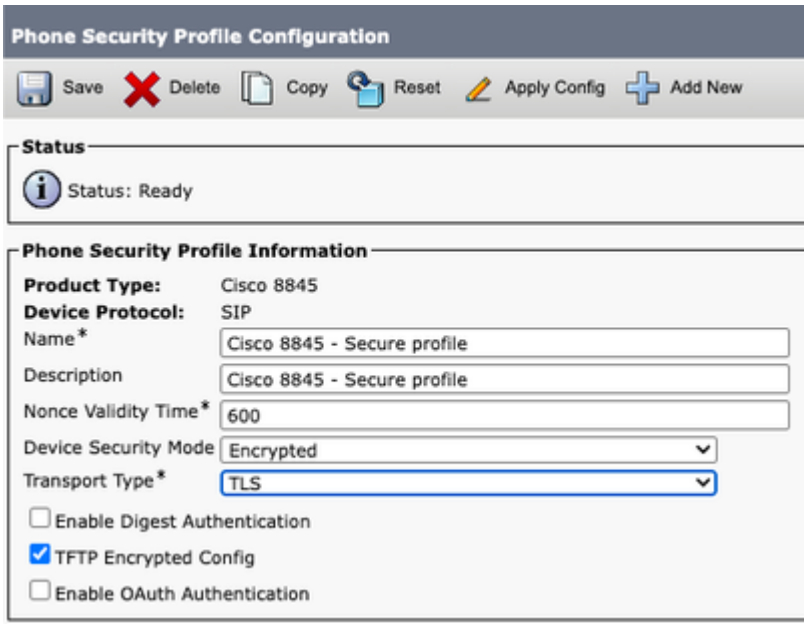
- CAPF information(CAPF 정보)에서 Install/Upgrade in Certificate Operation(인증서 작업에서 설치/업그레이드)을 선택합니다.




- Save and Apply Config를 선택합니다.
- Certificate Operation Status(인증서 작업 상태)에 Operation Completed(작업 완료됨)가 표시될 때까지 기다립니다.


Phone Configuration(전화기 컨피그레이션)의 Protocol Specific Information(프로토콜 특정 정보) 섹션에서 생성된 TLS가 활성화된 보안 프로필을 선택합니다.






## 관련 정보

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html
- https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html

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.