

CUCM 14에서 CallManager에 대한 Tomcat 인증서 재사용 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1. Tomcat 인증서를 다중 SAN으로 설정](#)

[자체 서명](#)

[CA 서명](#)

[2. CallManager에 Tomcat 인증서 재사용](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 서버에서 CallManager용 Multi-SAN Tomcat 인증서를 재사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM 인증서
- RTMT(실시간 모니터링 도구)
- ITL(Identity Trust List)

사용되는 구성 요소

이 문서의 정보는 CUCM 14.0.1.13900-155를 기반으로 합니다.

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

CUCM의 두 가지 주요 서비스는 Tomcat과 CallManager입니다. 이전 버전에서는 전체 클러스터에 대해 서비스마다 다른 인증서가 필요했습니다. CUCM 버전 14에서는 CallManager 서비스를 위해 Multi-SAN Tomcat 인증서도 재사용할 수 있는 새로운 기능이 추가되었습니다. 이 기능을 사용하면 다음과 같은 이점이 있습니다.

- CA 서명 인증서의 한 클러스터에 대해 CA(Public Certificate Authority)에서 서명 한 두 인증서를 얻는 비용을 줄입니다.
- 이 기능은 ITL 파일의 크기를 줄여 오버헤드를 줄입니다.

● 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	

구성



주의: Tomcat 인증서를 업로드하기 전에 SSO(Single Sign-On)가 비활성화되어 있는지 확인합니다. 활성화된 경우 Tomcat 인증서 재생성 프로세스가 완료되면 SSO를 비활성화했다가 다시 활성화해야 합니다.

1. Tomcat 인증서를 다중 SAN으로 설정



Low Impact

CUCM 14에서 Tomcat Multi-SAN 인증서는 자체 서명 또는 CA 서명 가능합니다. Tomcat 인증서가 이미 Multi-SAN인 경우 이 섹션을 건너뜁니다.

자체 서명

1단계. 에 로그인하고 Publisher > Operating System (OS) Administration > Security > Certificate Management > Generate Self-Signed 이동합니다.

2단계. Certificate Purpose: tomcat > Distribution: Multi-Server SAN 선택합니다. SAN 도메인 및 상위 도메인이 자동으로 채워집니다.

Generate New Self-signed Certificate

Generate Close

Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 14pub.

Subject Alternate Names (SANs)

Auto-populated Domains

14pub.

14sub.

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Validity Period (in years)* 5

Generate Close

*- indicates required item.

**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Generate Self-Signed Multi-SAN Tomcat Certificate(자체 서명 다중 SAN Tomcat 인증서 생성) 화면

3단계. 을 Generate 클릭하고 모든 노드가 메시지 아래에 나열되어 있는지 Certificate upload operation successful 확인합니다. 을 클릭합니다.Close

Generate New Self-signed Certificate

Generate Close

Status

Certificate upload operation successful for the nodes 14sub., 14pub.

Restart Cisco Tomcat Service for the nodes 14sub., 14pub. using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

자체 서명된 Multi-SAN Tomcat 성공 메시지 생성

4단계. Tomcat 서비스를 다시 시작하고 클러스터의 모든 노드에 대한 CLI 세션을 연 다음 명령을 utils service restart Cisco Tomcat 실행합니다.

5단계. 로 이동하여 Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services를 재시작하고 를 Cisco DRF Master ServiceCisco DRF Local Service 시작합니다.

6단계. 각각 Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services 탐색하고 재시작합니다Cisco DRF Local Service.

CA 서명

1단계. 에 로그인하고 Publisher > Operating System (OS) Administration로 Security > Certificate Management > Generate CSR 이동합니다.


2단계. Certificate Purpose: tomcat > Distribution: Multi-Server SAN 선택합니다. SAN 도메인 및 상위 도메인이 자동으로 채워집니다.

Generate Certificate Signing Request

Generate

Close

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**tomcat

Distribution*Multi-server(SAN)

Common Name*14pub-ms.

Include OU in CSR☐

Subject Alternate Names (SANs)

Auto-populated Domains

14pub.
14sub.

Parent Domain

Other Domains

Choose File

No file chosen
Please import .TXT file only.

Add


Key Type**RSA


Key Length*2048

Hash Algorithm*SHA256

Generate

Close

 *- indicates required item.

 **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Tomcat Certificate용 Multi-SAN CSR 생성 화면

3단계. 을 Generate 클릭하고 메시지 아래에 모든 노드가 나열되어 있는지 CSR export operation successful 확인합니다. 을 클릭합니다.Close

Generate Certificate Signing Request

Generate Close

Status

- Success: Certificate Signing Request Generated
- CSR export operation successful on the nodes **[14sub., 14pub.]**.

Generate Multi-SAN CSR Tomcat Successful Message(다중 SAN CSR Tomcat 생성 성공 메시지)

4단계. 을 클릭합니다Download CSR > Certificate Purpose: tomcat > Download.

Download Certificate Signing Request

Download CSR Close

Status

! Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

i *- indicates required item.

Tomcat CSR 다운로드 화면

5단계. 서명을 위해 CSR을 CA에 보냅니다.

6단계. CA 신뢰 체인을 업로드하려면 탐색합니다Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. 인증서의 설명을 설정하고 신뢰 체인 파일을 탐색합니다.

7단계. CA 서명 인증서를 업로드하고 로Certificate Management > Upload certificate > Certificate Purpose: tomcat이동합니다. 인증서의 설명을 설정하고 CA 서명 인증서 파일을 찾습니다.

8단계. Tomcat 서비스를 다시 시작하고 클러스터의 모든 노드에 대한 CLI 세션을 연 다음 명령을 utils service restart Cisco Tomcat실행합니다.

9단계. 로 이동하여Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services를 다시 시작하고 을 Cisco DRF Master Service다시 시작합니다Cisco DRF Local Service.

10단계. 각각을 탐색하고Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services재시작합니다Cisco DRF Local Service.

2. CallManager에 Tomcat 인증서 재사용



주의: CUCM 14의 경우 새로운 엔터프라이즈 매개변수 Phone Interaction on Certificate Update가 도입됩니다. 이 필드를 사용하여 TVS, CAPF 또는 TFTP(CallManager/ITLRecovery) 인증서 중 하나가 업데이트될 때 필요에 따라 수동으로 또는 자동으로 전화기를 재설정할 수 있습니다. 이 매개변수는 기본적으로 `reset the phones automatically` 설정됩니다. 인증서를 다시 생성, 삭제 및 업데이트한 후 적절한 서비스가 다시 시작되었는지 확인합니다.

일반적인 CallManager 인증서를 다시 생성하려면 서비스를 다시 시작해야 합니다. [Unified Communications Manager에서 인증서 재생성을 선택합니다.](#)

1단계. CUCM 게시자로 이동한 다음 `Cisco Unified OS Administration > Security > Certificate Management` 이동합니다.

2단계. `을` 클릭합니다 `Reuse Certificate`.

3단계. choose **Tomcat type** 드롭다운 목록에서 `을` 선택합니다 `tomcat`.

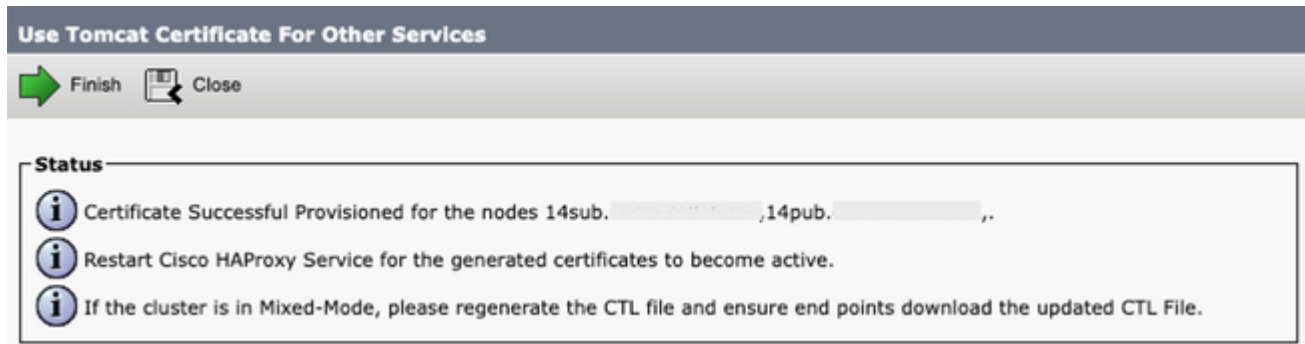
4단계. 창에서 `Replace Certificate for the following purpose` 체크박스를 `CallManager` 선택합니다.

다른 서비스에 Tomcat 인증서 재사용 화면



참고: 인증서 유형으로 Tomcat을 선택하면 CallManager가 대체용으로 활성화됩니다. 인증서 유형으로 tomcat-ECDSA를 선택하면 CallManager-ECDSA가 대체용으로 활성화됩니다

5단계. CallManager 인증서를 Tomcat Multi-SAN 인증서로 교체하려면 클릭Finish합니다.



Tomcat 인증서 재사용 성공 메시지

6단계. Cisco HAProxy 서비스를 다시 시작하고 클러스터의 모든 노드에 대한 CLI 세션을 연 다음 명령을 `utils service restart Cisco HAProxy` 실행합니다.



참고: Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode 클러스터가 혼합 모드에 있는지 확인하려면 (0 == Non-Secure; 1 == 혼합 모드).

7단계. 클러스터가 혼합 모드인 경우 게시자 노드에 대한 CLI 세션을 열고 명령을 실행한 다음 CTL 파일 업데이트가 적용되도록 클러스터의 모든 폰을 `utils ctl update CTLFile` 재설정합니다.

다음을 확인합니다.

1단계. CUCM 게시자로 이동한 다음 로 Cisco Unified OS Administration > Security > Certificate Management 이동합니다.

2단계. 필터링 기준 Find Certificate List where: Usage > begins with: identity 및 Find 을 클릭합니다.

3단계. CallManager 및 Tomcat 인증서는 동일한 값으로 끝나야 Common Name_Serial Number 합니다.

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	14pub. 45cdf84f42748393f6acdf739c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager
CallManager-ECDSA	14pub-EC 56a32bfe3062996d5c3851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
CAPF	CAPF-02a10666 6f44af5c5cdf753d5ff1538c3879b044	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system
IPsec	14pub. 6f44af5c5cdf753d5ff1538c3879b044	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY 14pub. 7270299ea3d929d99ce9bee38720c89e	Identity	Self-signed	RSA	14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
Tomcat	14pub. 45cdf84f42748393f6acdf739c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat
tomcat-ECDSA	14pub-EC 5ea1f2fedf9f6183cdf629a4a0d0447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
TVS	14pub. 7d8022f6eb2885c3406b77cb4126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system



참고: SU4 이후부터는 인증서 재사용이 활성화된 상태에서 Call Manager 인증서가 GUI에 표시되지 않지만, 두 인증서는 모두 SU2 및 SU3에 표시됩니다.

관련 정보

- [Cisco Unified Communications Manager 보안 설명서 14](#)
- [Cisco 기술 지원 및 다운로드](#)

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.