

# CallManager용 다중 SAN Tomcat 인증서 재사용 구현

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[CallManager에 Tomcat 인증서 재사용](#)

[다음을 확인합니다.](#)

---

## 소개

이 문서에서는 CUCM에서 CallManager용 Multi-SAN Tomcat 인증서를 재사용하는 방법에 대한 단계별 프로세스에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM(Cisco Unified Communications Manager)
- CUCM 인증서
- ITL(Identity Trust List)

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 릴리스 15 SU1

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

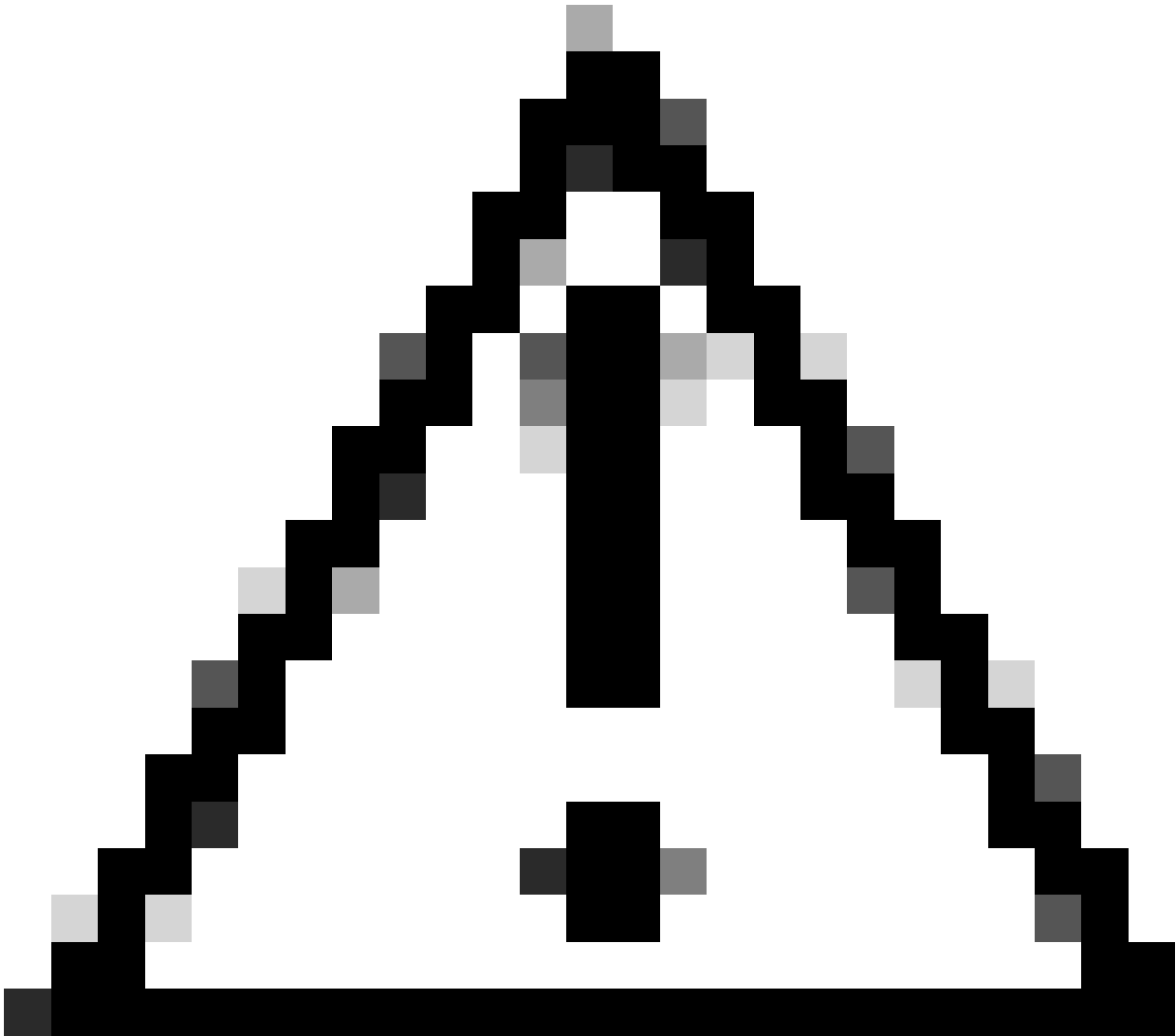
이전 버전의 CUCM에서는 전체 클러스터에 대해 서비스마다 서로 다른 인증서를 사용하여 인증서 수와 비용이 증가했습니다. 여기에는 각 ID 인증서가 있는 CUCM에서 실행되는 중요한 서비스인

Cisco Tomcat 및 Cisco CallManager가 포함됩니다.

CUCM 버전 14부터 CallManager 서비스를 위해 Multi-SAN Tomcat 인증서를 재사용하는 새로운 기능이 추가되었습니다.

이 기능을 사용하면 CA에서 하나의 인증서를 얻어 여러 애플리케이션에서 사용할 수 있다는 이점이 있습니다. 이를 통해 비용을 최적화하고 관리를 줄이며 ITL 파일의 크기를 줄여 오버헤드를 줄일 수 있습니다.

---



주의: 재사용 컨피그레이션을 계속 진행하기 전에 Tomcat 인증서가 다중 서버 SAN 인증서인지 확인합니다. Tomcat Multi-SAN 인증서는 자체 서명 또는 CA 서명 가능합니다.

---

## 구성

CallManager에 Tomcat 인증서 재사용



경고: 계속하기 전에 클러스터가 혼합 모드 또는 비보안 모드인지 확인하십시오.

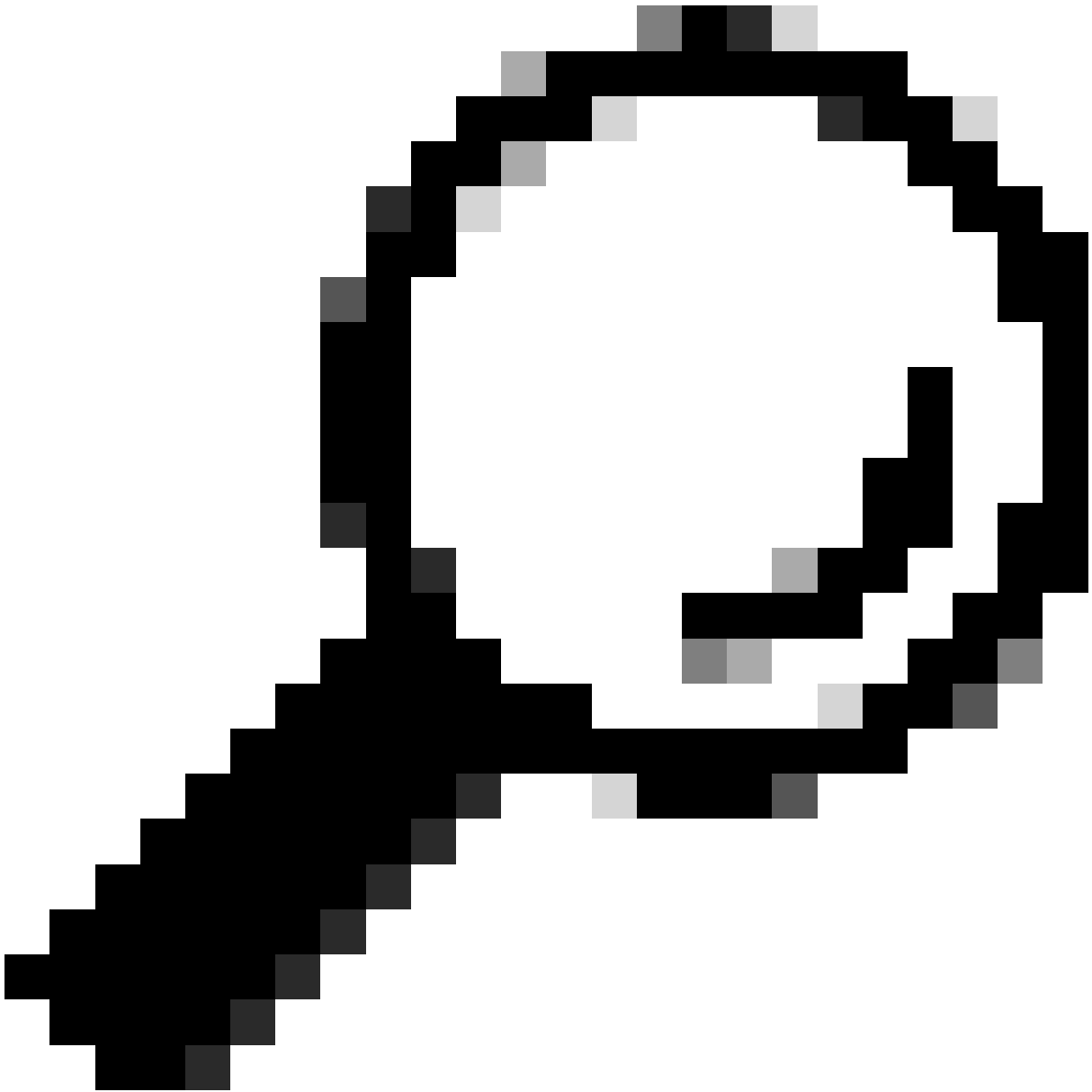
---

1단계. Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)로 이동합니다.

Security Parameters(보안 매개변수) 섹션을 확인하고 클러스터 보안 모드가 0 또는 1로 설정되어 있는지 확인합니다. 값이 0이면 클러스터는 비보안 모드에 있습니다. 1이면 클러스터가 혼합 모드이며 서비스를 재시작하기 전에 CTL 파일을 업데이트해야 합니다.

2단계. CUCM 게시자로 이동한 다음 Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리)로 이동합니다.

3단계. Multi-SAN Tomcat CA 인증서 체인을 CallManager Trust 저장소에 업로드합니다.



팁: Tomcat에 대해 셀프 서명된 다중 서버 SAN 인증서를 사용하는 경우 이 단계를 건너뛸 수 있습니다.

---

인증서를 다시 사용하기 전에 tomcat ID 인증서에 서명한 CA 인증서 체인을 CallManager 신뢰 저장소에 수동으로 업로드해야 합니다.

tomcat 인증서 체인을 CallManager 트러스트에 업로드할 때 이러한 서비스를 재시작합니다.

- CallManager: Cisco HAProxy 서비스
- CallManager-ECDSA: Cisco CallManager 서비스 및 Cisco HAProxy 서비스

4단계. Reuse Certificate(인증서 재사용)를 클릭합니다. Use Tomcat Certificates For Other Services 페이지가 나타납니다.

## Use Tomcat Certificate For Other Services



Finish



Close

### Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

### Source

Choose Tomcat Type\*

tomcat



### Replace Certificate for the following purpose



CallManager



CallManager-ECDSA

Finish

Close

5단계. Tomcat 유형 드롭다운 목록에서 Tomcat 또는 Tomcat-ECDSA를 선택합니다.



6단계. Replace Certificate for the following purpose 창에서 이전 단계에서 선택한 인증서에 따라 CallManager 또는 CallManager-ECDSA 확인란을 선택합니다.






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

7단계. Finish(마침)를 클릭하여 CallManager 인증서를 tomcat 다중 서버 SAN 인증서로 교체합니다.

**Use Tomcat Certificate For Other Services**

 Finish  Close

**Status**

-  Certificate Successful Provisioned for the nodes cucmpub15. , cucmsub15. .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

8단계. CLI를 통해 `utils service restart Cisco HAProxy` 명령을 실행하여 클러스터의 모든 노드에서 Cisco HAProxy 서비스를 재시작합니다.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin: █
```

9단계. 클러스터가 혼합 모드인 경우 CUCM 게시자의 CLI를 통해 `utils ctl update CTLFile` 명령을 실행하여 CTL 파일을 업데이트하고 전화기를 재설정하여 새 CTL 파일을 가져옵니다.

다음을 확인합니다.

---

참고: CallManager 인증서는 인증서를 재사용할 때 GUI에 표시되지 않습니다.

---

CLI에서 명령을 실행하여 CallManager가 Tomcat 인증서를 재사용하는지 확인할 수 있습니다.

- 인증서 목록 고유 표시

```
admin:show cert list own
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
ITLRecovery/ITLRecovery.pem:
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager
TVS/TVS.pem: Self-signed certificate generated by system

admin:█
```



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.