CUCM PHONE 인증서용 Q.A(LSC/MIC)

목차

소개
Phone Certificates의 일반적인 용도는 무엇입니까?
설치/업그레이드, 삭제 또는 문제 해결을 위한 CAPF와 전화 간
TLS(Transport Layer Security) 연결을 위한 CallManager와 전화 간
802.1x 인증을 위한 전화 및 인증 서버 간
VPN용 Phone과 Cisco ASA(Adaptive Security Appliance) 간 인증서 기반 인증
LSC 및 MIC가 있는 경우 연결에 대해 LSC 또는 MIC를 명시적으로 선택할 수 있는 방법이 있습니까?
새 클러스터로 이동할 때 보안 프로필이 있는 LSC가 설치된 전화기가 등록되지 않은 이유는 무엇입니까?
Authenticated(인증) 또는 Encrypted secured(암호화된 보안) 프로파일을 사용하여 등록하려면 전화기에 LSC가 설치되어 있어야 합니까?
LSC를 설치/업그레이드/삭제하려면 각 디바이스 보안 프로필의 디바이스 보안 모드를 인증 또는 암호화해야 합니까?
전화기에 LSC를 설치하려면 클러스터가 혼합 모드에 있어야 합니까?
전화기에서 사용하는 LSC에 문제가 있는지 신속하게 테스트하는 방법
문제 해결을 위해 전화 인증서를 가져오는 방법
CallManager와의 TLS 연결을 설정하는 데 전화기의 LSC 또는 MIC를 사용하는 경우 패킷 캡처에서 확인하는 방법
CAPF(Certification Authority Proxy Function) 정보에서 인증 모드의 중요성은 무엇입니까?CUCM과 Phone 간의 TLS 연결이 중요합니까?
CAPF 인증서를 다시 생성한 후 전화기에 대해 고려할 기본 LSC 작업은 무엇입니까?
CallManager와의 TLS 연결
CAPF-Trust를 통한 LSC 작업
802.1x 인증을 위한 전화 및 인증 서버 간
ASA와 전화 간
관련 정보

소개

이 문서에서는 Cisco CUCM(Unified Communications Manager) 전화 인증서에 대한 몇 가지 질문과 답변을 다룹니다. 전화기 인증서를 간단히 볼 수 있습니다.

제조업체 설치 인증서(MIC):

이름에서 알 수 있듯이 전화기는 MIC와 함께 사전 설치되며 관리자가 삭제하거나 수정할 수 없습니다.CA(Certificate Authority) 인증서 CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA 및 Cisco Manufacturing CA SHA2는 MIC를 신뢰하기 위해 CUCM에 미리 설치되어 있습니다. MIC CA를 다시 생성함으로써 유효성 만료 후 MIC를 사용할 수 없습니다.

LSC(Locally Significant Certificate):

LSC는 Cisco Unified Communications Manager CAPF(Certificate Authority Proxy Function) 개인

키에 의해 서명된 Cisco IP 전화의 공개 키를 보유합니다.기본적으로 전화기에 설치되지 않습니다.관리자는 LSC를 완벽하게 제어할 수 있습니다.CAPF CA 인증서를 다시 생성하면 필요할 때마다 전화기에 새 LSC를 발급할 수 있습니다.

Phone Certificates의 일반적인 용도는 무엇입니까?

다음은 전화기 인증서에 대한 일반적인 사용 방법입니다.

설치/업그레이드, 삭제 또는 문제 해결을 위한 CAPF와 전화 간

전화기에서 인증서를 설치/업그레이드, 삭제 또는 트러블슈팅하기 위해 CAPF와의 연결을 설정합니다.Phone Certificate(전화기 인증서)는 기존 인증서(LSC에 우선 순위) 또는 기존 인증서(MIC에 우선 순위)로 설정된 CAPF(Certification Authority Proxy Function) 정보 아래의 인증 모드에서 CAPF와의 연결을 설정하는 데 사용됩니다.

기존 인증서별(LSC에 우선): 전화기는 LSC를 사용하여 CAPF로 인증합니다.LSC가 설치되지 않은 경우 MIC를 사용합니다.사용된 인증서에 문제가 있는 경우 "잘못된 LSC"라는 이유로 인해 설치가 실패합니다.예를 들어 LSC에 대해 서명된 CA는 CAPF Trust에서 사용할 수 없습니다.다른 인증서 방법을 사용하여 인증 모드를 업데이트하거나 그러한 실패 사례의 경우 null 문자열로 업데이트합니다.

기존 인증서별(MIC에 우선):전화기는 MIC를 사용하여 CAPF를 인증합니다.

TLS(Transport Layer Security) 연결을 위한 CallManager와 전화 간

전화기는 LSC 또는 MIC를 사용하여 CallManager와의 TLS 연결을 설정합니다.CallManager는 CallManager-trust를 확인하여 전화기에서 제공한 인증서를 검증합니다.각 CAPF 인증서는 LSC용 CallManager-trust 및 MIC용 Cisco Manufacture CA에서 사용할 수 있어야 합니다.

802.1x 인증을 위한 전화 및 인증 서버 간

CAPF/제조 CA 인증서는 Cisco ACS(Secure Access Control Server) 또는 ISE(Identity Services Engine)와 같은 인증 서버에 업로드됩니다. 인증 서버는 업로드된 인증서를 사용하여 인증서가 있으면 전화기를 인증합니다(LSC 또는 MIC).

VPN용 Phone과 Cisco ASA(Adaptive Security Appliance) 간 인증서 기반 인증

CAPF/Manufacture CA 인증서는 ASA에 업로드되며, 전화기에 LIC/MIC가 있으면 ASA는 이를 신뢰하는지 확인하여 검증합니다.

LSC 및 MIC가 있는 경우 연결에 대해 LSC 또는 MIC를 명시적으로 선택할 수 있는 방법이 있습니까?

연결에 대해 LSC인지 MIC인지를 선택할 수 있는 옵션이 없습니다.LSC가 설치된 경우 전화기에서 LSC를 사용합니다. LSC가 설치되지 않은 경우 전화기에서 MIC를 사용합니다.

LSC가 없는 경우 콘솔 항목:

보안:-PXY_NO_LSC:[SCCP]에 대한 LSC가 없습니다. MIC를 시도합니다.

LSC가 있는 경우 콘솔 항목:

보안:-PXY_CERT_CIPHER:[SCCP], [TLSv1], 인증서 [LSC]

CAPF와 전화 설치/업그레이드, 삭제 또는 문제 해결 간에만 LSC 또는 MIC를 선택할 수 있습니다.

새 클러스터로 이동할 때 보안 프로필이 있는 LSC가 설치된 전화기가 등록되지 않은 이유는 무엇입니까?

이는 OLD Cluster에서 이미 LSC가 있는 전화기에 대해 발생할 수 있습니다.MIC와 LSC가 모두 있는 경우 LSC를 사용하여 TLS 연결을 설정합니다.새 CUCM에 CallManager-trust에 이 LSC에 대한 CA가 없으므로 TLS를 설정할 수 없습니다.

콘솔 로그는 TLS를 설정하는 데 사용되는 인증서를 표시합니다.아래 항목은 LSC가 사용된 것을 보여줍니다.

3469 NOT 00:01:31.935298 SECD:-PXY_CERT_CIPHER:[SCCP], [TLSv1], 인증서 [LSC], 암호 [AES256-SHA:AES128-SHA]

콘솔 로그에서 실패한 케이스에 대해 "알 수 없는 CA"가 있는 SSL3_Alert:-

3486 오류 00:01:31.938954초:-STATE_SSL3_ALERT:SSL3 경고 [읽기]:[치명적]:[알 수 없는 CA

이 문제를 해결하는 방법 중 하나는 비보안 프로필을 사용하여 전화기를 등록한 다음 기존 LSC를 삭제하는 것입니다.새 클러스터에서 LSC를 설치한 다음 보안 프로필을 사용하여 전화기를 등록합니다.또한 LSC를 설치하지 않고 보안 프로필이 있는 전화기를 MIC를 사용하여 등록할 수 있습니다
.

Authenticated(인증) 또는 Encrypted secured(암호화된 보안) 프로파일을 사용하여 등록하려면 전화기에 LSC가 설치되어 있어야 합니까?

아니요. LSC가 설치되지 않은 경우 전화기는 MIC를 사용하여 CUCM에 대한 TLS 연결을 설정합니다.

4878 경고 15:47:34.756063초:-PXY_NO_LSC:[SCCP]에 대한 LSC가 없습니다. MIC를 시도합니다
.

LSC를 설치/업그레이드/삭제하려면 각 디바이스 보안 프로필의 디바이스 보안 모드를 인증 또는 암호화해야 합니까?

필수 사항은 아닙니다. Device Security Mode(디바이스 보안 모드)의 경우 기본 표준 Non-Secure Profile(비보안 프로파일)을 사용하여 수행할 수 있습니다.

전화기에 LSC를 설치하려면 클러스터가 혼합 모드에 있어야 합니까?

필수 사항은 아닙니다.클러스터 보안 모드가 비보안 모드인 경우에도 LSC 설치/삭제를 수행할 수 있습니다.

전화기에서 사용하는 LSC에 문제가 있는지 신속하게 테스트하는 방법

전화기 관리 페이지로 이동하여 전화기 중 하나에서 LSC를 삭제합니다.이렇게 하면 전화기가 MIC를 사용하도록 설정됩니다.MIC가 모두 정상인 경우 LSC로 트러블슈팅을 진행합니다.

문제 해결을 위해 전화 인증서를 가져오는 방법

Device/Phone(디바이스/전화기)에서 Certificate Operation(인증서 작업)을 Troubleshoot(문제 해결)로 설정합니다.저장 후 구성 적용을 누릅니다. Certificate Operation Status(인증서 작업 상태)가 Troubleshoot Success(**성공 문제 해결)를** 볼 때까지 **기다립니다**.RTMT(**Real** Time Monitoring Tool)에서 Cisco Certificate Authority Proxy Function Logs를 수집합니다. 전화기의 인증서가 포함되어 있습니다.

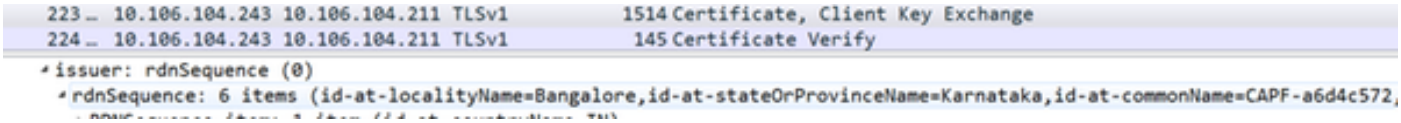
CallManager와의 TLS 연결을 설정하는 데 전화기의 LSC 또는 MIC를 사용하는 경우 패킷 캡처에서 확인하는 방법

폰 재시작을 다루는 패킷 캡처를 수집합니다.

인증서, 클라이언트 키 교환 메시지를 확인합니다.IP Phone에서 보낸 인증서를 확인합니다.

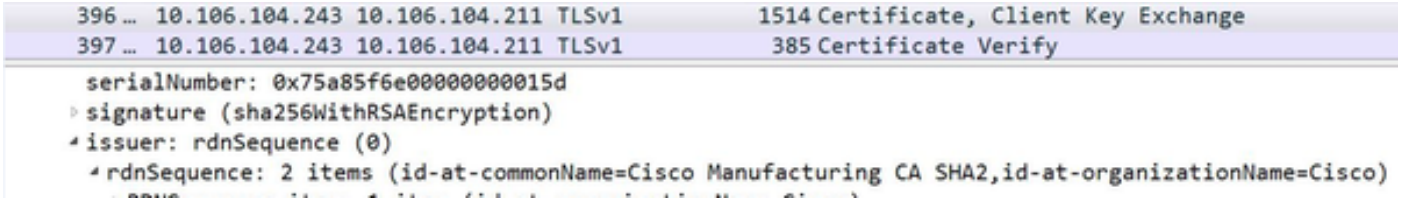
예 LSC:

LSC의 경우 발급자 필드에 CAPF CN이 표시됩니다.각 CAPF 루트가 CallManager-trust에 있어야 합니다.



MIC 예:

MIC의 경우 발급자 필드에 Cisco Manufacturing CA가 있습니다.각 루트 CA가 CallManager-trust에 있어야 합니다.



CAPF(Certification Authority Proxy Function) 정보에서 인증 모드의 중요성은 무엇입니까?CUCM과 Phone 간의 TLS 연결이 중요합니까?

설치/업그레이드/삭제 및 문제 해결 작업을 위한 전화와 CAPF 간의 인증 방법에 불과합니다 .CUCM과 Phone 간의 TLS 연결에는 아무런 의미가 없습니다.

CAPF 인증서를 다시 생성한 후 전화기에 대해 고려할 기본 LSC 작업은 무엇입니까?

이 섹션에서는 LSC를 실행하는 데 오프라인 CA가 사용되지 않는 유휴 시나리오에 대해 설명합니다.

CallManager와의 TLS 연결

CallManager-trust에서 이전 CAPF 인증서를 삭제하기 전에 전화기에 새 LSC를 설치해야 합니다 .이전 CAPF 인증서를 삭제한 다음 CallManager 서비스를 다시 시작하면 이 CAPF 인증서에서 발급한 LSC가 있는 전화기에 등록 문제가 발생합니다.

CAPF-Trust를 통한 LSC 작업

CAPF-trust에서 이전 CAPF 인증서를 삭제하기 전에 전화기에 새 LSC를 설치해야 합니다.기존 **인증서**의 인증 모드를 사용하여 설치/삭제 같은 LSC 작업**(LSC의 우선 순위)이** 실패하고 오류 이 CAPF 인증서에서 발급한 LSC가 있는 전화기의 LSC가 잘못되었습니다.

802.1x 인증을 위한 전화 및 인증 서버 간

새 CAPF 인증서가 업로드되고 전화기가 새 CAPF에서 발급한 LSC를 가져올 때까지 인증 서버에서 이전 CAPF 인증서를 삭제하지 않도록 하십시오.

ASA와 전화 간

전화기에서 새 LSC를 가져오고 새 CAPF CA 인증서를 ASA에 업로드할 때까지 ASA에서 이전 CAPF 인증서를 삭제하지 않도록 합니다.

CAPF 인증서를 재생성하려면 따라야 하는 단계는 인증서 재생성을 참조하십시오.

관련 정보

- Cisco IP Phone 인증서 및 보안 커뮤니케이션
- IP Telephony for 802.1X 설계 가이드
- Cisco Unified Communications Manager 보안 가이드