보안 및 인증서

- 암호화, 1 페이지
- 음성 및 비디오 암호화, 6 페이지
- 보안 미디어에 대한 인증 방법 , 6 페이지
- PIE ASLR 지원, 7 페이지
- Federal Information Processing Standards, 7 페이지
- 공통평가기준, 8 페이지
- 보안 LDAP, 8 페이지
- 인증된 UDS 연락처 검색, 9 페이지
- 인증서, 9 페이지
- 다중 테넌트 호스팅 협업 솔루션에 대한 서버 이름 표시 지원 , 13 페이지
- 바이러스 백신 제외, 14 페이지

암호화

파일 전송 및 화면 캡처에 대한 준수 및 정책 제어

Cisco Unified Communications Manager IM and Presence 10.5(2) 이상에서 관리되는 파일 전송 옵션을 사용하여 파일 전송 및 화면 캡처를 전송하는 경우 감사 및 정책 적용을 위해 파일을 준수 서버로 보낼 수 있습니다.

준수에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스에 대한 인스턴트 메시징 준수 설명서를 참조하십시오.

파일 전송 및 화면 캡처 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager IM and Presence* 구축 및 설치 설명서를 참조하십시오.

인스턴트 메시지 암호화

Cisco Jabber는 TLS(Transport Layer Security)를 사용하여 클라이언트와 서버 사이에서 네트워크를 통해 확장 가능한 메시징 및 프레즌스 상태 프로토콜(XMPP) 트래픽을 보호합니다. Cisco Jabber는 포인트간 인스턴트 메시지를 암호화합니다.

온프레미스 암호화

다음 표에는 온프레미스 구축의 인스턴트 메시지 암호화에 대한 세부 정보가 요약되어 있습니다.

연결	프로토콜	협상 인증서	예상 암호화 알고리즘
클라이언트에서 서버로	TLS v1.2를 통한 XMPP	X.509 공개 키 인프라 인증서	AES 256비트

서버 및 클라이언트 협상

다음 서버는 X.509 PKI(공개 키 인프라) 인증서를 사용하여 Cisco Jabber와 TLS 암호화를 협상합니다.

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

서버 및 클라이언트가 TLS 암호화를 협상하면 클라이언트와 서버 모두 인스턴트 메시징 트래픽을 암호화하기 위해 세션 키를 생성하고 교환합니다.

다음 표는 Cisco Unified Communications Manager IM and Presence Service의 PKI 인증서 키 길이를 나열합니다.

버전	키 길이
Cisco Unified Communications Manager IM and Presence Service 버전 9.0.1 이상	2048비트

XMPP 암호화

Cisco Unified Communications Manager IM and Presence Service는 Cisco Jabber와 프레즌스 서버 간의 인스턴트 메시지 트래픽을 보호하기 위해 AES 알고리즘을 사용하 여 암호화된 256비트 길이 세션 키를 사용합니다.

서버 노드 간 트래픽에 대한 추가 보안이 필요한 경우 Cisco Unified Communications Manager IM and Presence Service에서 XMPP 보안 설정을 구성할 수 있습니다. 보안 설정에 대한 자세한 내용은 다음을 참조하십시오.

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence*의 보안 구성

인스턴트 메시징 로깅

규정 지침을 준수하기 위해 인스턴트 메시지를 기록하고 보관할 수 있습니다. 인스턴트 메시지를 기록하려면 외부 데이터베이스를 구성하거나 타사 컴플라이언스 서버와 통합합니다. Cisco Unified

Communications Manager IM and Presence Service는 외부 데이터베이스 또는 타사 컴플라이언스 서버에서 로그인하는 인스턴트 메시지를 암호화하지 않습니다. 기록하는 인스턴트 메시지를 보호하려면 외부 데이터베이스 또는 타사 컴플라이언스 서버를 적절하게 구성해야 합니다.

규정 준수에 대한 자세한 내용은 다음을 참조하십시오.

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence* 서비스를 위한 인스턴트 메시징 규정 준수

대칭 키 알고리즘(예: AES) 또는 공개 키 알고리즘(예: RSA)을 포함하여 암호화 수준 및 암호화 알고리즘에 대한 자세한 내용은 이 링크 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html의 차세대 암호화를 참조하십시오.

X.509 공개 키 인프라 인증서에 대한 자세한 내용은 이 링크 https://www.ietf.org/rfc/rfc2459.txt의 인터넷 *X.509* 공개 키 인프라 인증서 및 *CRL* 프로파일 문서를 참조하십시오.

클라우드 기반 암호화

다음 표에는 클라우드 기반 구축의 인스턴트 메시지 암호화에 대한 세부 정보가 요약되어 있습니다.

연결	프로토콜	협상 인증서	예상 암호화 알고리즘
클라이언트에서 서버로	TLS 내 XMPP	X.509 공개 키 인프라 인증서	AES 128비트
클라이언트-클라이언트	TLS 내 XMPP	X.509 공개 키 인프라 인증서	AES 256비트

서버 및 클라이언트 협상

다음 서버는 Webex Messenger 서비스가 있는 X.509 PKI(공개 키 인프라) 인증서를 사용하여 Cisco Jabber와 TLS 암호화를 협상합니다.

서버 및 클라이언트가 TLS 암호화를 협상하면 클라이언트와 서버 모두 인스턴트 메시징 트래픽을 암호화하기 위해 세션 키를 생성하고 교환합니다.

XMPP 암호화

Webex Messenger 서비스에서는 AES 알고리즘을 사용하여 암호화된 128비트 세션 키를 사용하여 Cisco Jabber 및 Webex Messenger 서비스 간의 인스턴트 메시지 트래픽을 보호합니다.

선택적으로 256비트 클라이언트-클라이언트 간 AES 암호화를 활성화하여 클라이언트 간의 트래픽을 보호할 수 있습니다.

인스턴트 메시징 로깅

Webex Messenger 서비스는 인스턴트 메시지를 기록할 수 있지만 이러한 인스턴트 메시지를 암호화된 형식으로 보관하지는 않습니다. 그러나 Webex Messenger 서비스는 SAE-16 및 ISO-27001 감사를 포함하여 엄격한 데이터 센터 보안을 사용하여 로그에 기록하는 인스턴트 메시지를 보호합니다.

AES 256비트 클라이언트-클라이언트 간 암호화를 활성화하면 Webex Messenger 서비스에서 인스턴트 메시지를 기록할 수 없습니다.

대칭 키 알고리즘(예: AES) 또는 공개 키 알고리즘(예: RSA)을 포함하여 암호화 수준 및 암호화 알고리즘에 대한 자세한 내용은 이 링크 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html의 차세대 암호화를 참조하십시오.

X.509 공개 키 인프라 인증서에 대한 자세한 내용은 이 링크 https://www.ietf.org/rfc/rfc2459.txt의 인터넷 *X.509* 공개 키 인프라 인증서 및 *CRL* 프로파일 문서를 참조하십시오.

클라이언트 간 암호화

기본적으로 클라이언트와 Cisco Webex Messenger 서비스 간의 인스턴트 메시징 트래픽은 안전합니다. 선택적으로 Cisco Webex 관리 도구에서 정책을 지정하여 클라이언트 간 인스턴트 메시징 트래픽을 보호할 수 있습니다.

다음 정책은 인스턴트 메시지에 대한 클라이언트 간 암호화를 지정합니다.

- **IM**에 대한 **AES** 인코딩 지원 - 전송 클라이언트는 AES 256비트 알고리즘을 사용 하여 인스턴트 메시지를 암호화합니다. 수신 클라이언트는 인스턴트 메시지의 암호를 해독합니다.
- **IM**에 대한 인코딩 지원 없음 - 클라이언트는 암호화를 지원하지 않는 다른 클라이언트와 인스턴트 메시지를 주고 받을 수 있습니다.

다음 표에서는 이러한 정책으로 설정할 수 있는 다양한 조합에 대해 설명합니다.

정책 조합	클라이언트 간 암호화	원격 클라이언트가 **AES** 암호화를 지원하는 경우	원격 클라이언트가 **AES** 암호화를 지원하지 않는 경우
IM에 대한 **AES** 인코딩 지원 = 거짓 **IM**에 대한 인코딩 지원 안 함 = 참	아니요	Cisco Jabber 암호화되지 않은 인스턴트 메시지를 전송합니다. Cisco Jabber 키 교환을 협상하지 않습니다. 그 결과, 다른 클라이언트는 Cisco Jabber 암호화된 인스턴트 메시지를 전송하지 않습니다.	Cisco Jabber 암호화되지 않은 인스턴트 메시지를 보내고 받습니다.
IM에 대한 **AES** 인코딩 지원 = 참 **IM**에 대한 인코딩 지원 안 함 = 참	예	Cisco Jabber 암호화된 인스턴트 메시지를 보내고 받습니다. Cisco Jabber 인스턴트 메시지가 암호화되었음을 나타내는 아이콘을 표시합니다.	Cisco Jabber 암호화된 인스턴트 메시지를 전송합니다. Cisco Jabber 암호화되지 않은 인스턴트 메시지를 수신합니다.

정책 조합	클라이언트 간 암호화	원격 클라이언트가 **AES** 암호화를 지원하는 경우	원격 클라이언트가 **AES** 암호화를 지원하지 않는 경우
IM에 대한 **AES** 인코딩 지원 = 참 **IM**에 대한 인코딩 지원 안 함 = 거짓	예	Cisco Jabber 암호화된 인스턴트 메시지를 보내고 받습니다. Cisco Jabber 인스턴트 메시지가 암호화되었음을 나타내는 아이콘을 표시합니다.	Cisco Jabber 원격 클라이언트로 인스턴트 메시지를 보내거나 받지 않습니다. Cisco Jabber 사용자가 원격 클라이언트로 인스턴트 메시지를 보내려고 할 때 오류 메시지를 표시합니다.

참고 Cisco Jabber에서는 그룹 채팅을 통한 클라이언트 간 암호화를 지원하지 않습니다.Cisco Jabber는 포인트 간 채팅에 대해서만 클라이언트 간 암호화를 사용합니다.

암호화 및 Cisco Webex 정책에 대한 자세한 내용은 Cisco Webex 설명서의 암호화 수준 정보를 참조하십시오.

암호화 아이콘

클라이언트가 암호화 수준을 표시하기 위해 표시하는 아이콘을 검토합니다.

클라이언트와 서버 간 암호화 잠금 아이콘

온프레미스 및 클라우드 기반 구축에서 Cisco Jabber는 클라이언트가 서버에 암호를 제공하라는 것을 나타내는 다음 아이콘을 표시합니다.

클라이언트 간 암호화 잠금 아이콘

클라우드 기반 구축에서 Cisco Jabber는 클라이언트가 서버에 암호를 제공하라는 것을 나타내는 다음 아이콘을 표시합니다.

로컬 채팅 기록

참가자가 채팅 창을 닫은 후 참가자가 로그아웃할 때까지 채팅 기록이 유지됩니다. 참가자가 채팅 창을 닫은 후 채팅 기록을 유지하지 않으려면 Disable_IM_History 매개 변수를 true로 설정합니다. 이 매개 변수는 IM 전용 사용자를 제외한 모든 클라이언트에서 사용할 수 있습니다.

Mac용 Cisco Jabber의 온프레미스 구축의 경우 Mac용 Cisco Jabber의 채팅 환경설정 창에서 채팅 아카이브를 다음 위치에 저장**:** 옵션을 선택하는 경우 채팅 기록은 Mac 파일 시스템에 로컬로 저장되며 스포트라이트를 사용하여 검색할 수 있습니다.

Cisco Jabber는 로컬 채팅 기록이 활성화되어 있을 때 보관된 인스턴트 메시지를 암호화하지 않습니다.

데스크톱 클라이언트의 경우, 아카이브 저장을 통한 채팅 기록에 대한 액세스를 다음 디렉터리로 제한할 수 있습니다.

- Windows, `%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`
- Mac: `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`.

모바일 클라이언트의 경우 채팅 기록 파일에 액세스할 수 없습니다.

음성 및 비디오 암호화

선택적으로 모든 장치에 대 한 보안 전화기 기능을 설정할 수 있습니다. 보안 전화기 기능은 보안 SIP 신호 처리, 보안 미디어 스트림 및 암호화된 장치 구성 파일을 제공합니다.

사용자에 대한 보안 전화기 기능을 활성화한 경우, Cisco Unified Communications Manager에 대한 장치 연결은 안전합니다. 그러나 다른 장치를 사용한 통화는 두 장치에 모두 보안 연결이 있는 경우에만 안전합니다.

보안 미디어에 대한 인증 방법

SIP oAuth를 사용하여 토큰 기반 인증에서 보안 미디어를 활성화합니다. 온프레미스, 클라우드 및 Jabber의 하이브리드 구축의 보안 인증에 대한 CAPF 등록 대신 SIP oAuth를 설정할 수 있습니다.

SIP oAuth

Cisco Unified Communications Manager 설정에서 한 번 수행합니다. 이는 RTP 미디어를 포함하여 SIP 트래픽이 안전하다는 것을 확인합니다.

CAPF 등록

CAPF 등록 활성화에 대한 워크플로는 다음과 같습니다.

- Jabber 장치 만들기 및 구성
- 인증 문자열
- 전화기 보안 프로파일 구성

PIE ASLR 지원

Android, iPhone 및 iPad용 Cisco Jabber는 PIE ASLR(Position Independent Executable Address Space Layout Randomization)을 지원합니다.

Federal Information Processing Standards

FIPS(Federal Information Processing Standard) 140은 암호화 모듈에 대한 보안 요건을 지정하는 미국 정부 표준입니다. 이러한 암호화 모듈에는 승인된 보안 기능을 구현하고 암호화 경계 내에 포함되는 하드웨어, 소프트웨어 및 펌웨어 집합이 포함됩니다.

FIPS를 사용하려면 클라이언트 내에서 사용되는 모든 암호화, 키 교환, 디지털 서명 및 해시 및 난수 생성 기능이 암호화 모듈 보안에 대한 FIPS 140.2 요구 사항을 준수해야 합니다.

FIPS 모드는 클라이언트가 인증서를 더 엄격하게 관리합니다. 서비스에 대한 인증서가 만료되고 해당 자격 증명을 다시 입력하지 않은 경우 FIPS 모드 사용자에게 클라이언트의 인증서 오류가 표시될 수 있습니다. 허브 창에 FIPS 아이콘을 표시하여 클라이언트가 FIPS 모드에서 실행 중임을 나타냅니다.

Windows용 **Cisco Jabber**에 대해 **FIPS** 활성화

Windows용 Cisco Jabber는 FIPS를 활성화하는 두 가지 방법을 지원합니다.

- 운영 체제 활성화됨 - Windows 운영 체제가 FIPS 모드에 있습니다.
- Cisco Jabber 부트스트랩 설정 - FIPS_MODE 설치 관리자 스위치를 구성합니다. Cisco Jabber는 FIPS가 활성화되어 있지 않은 운영 체제의 FIPS 모드에 있을 수 있습니다. 이 시나리오에서는 비 Windows API를 사용한 연결만 FIPS 모드입니다.

표 ***1: FIPS***에 대한 ***Windows***용 ***Cisco Jabber*** 설정

플랫폼 모드	부트스트랩 설정	**Cisco Jabber** 클라이언트 설정
FIPS 활성화	FIPS 활성화	FIPS 활성화 - 부트스트랩 설정입니다.
FIPS 활성화	FIPS 비활성화됨	FIPS 비활성화 - 부트스트랩 설정입니다.
FIPS 활성화	설정 없음	FIPS 활성화 - 플랫폼 설정입니다.
FIPS 비활성화됨	FIPS 활성화	FIPS 활성화 - 부트스트랩 설정입니다.
FIPS 비활성화됨	FIPS 비활성화됨	FIPS 비활성화 - 부트스트랩 설정입니다.
FIPS 비활성화됨	설정 없음	FIPS 비활성화 - 플랫폼 설정입니다.

참고 Jabber 음성 메일 서비스는 SSL 연결 중에 **https://164.62.224.15/vmrest/version with FIPS enabled** HTTPs 요청에 대해서만 TLS 버전 TLS 1.2를 허용합니다.

모바일 클라이언트용 **Cisco Jabber**에 대해 **FIPS** 활성화

모바일 클라이언트용 Cisco Jabber에 대해 FIPS를 활성화하려면 EMM(Enterprise Mobility Management)에서 FIPS_MODE 매개 변수를 TRUE로 설정합니다.

중요
- FIPS를 활성화하면 사용자가 신뢰할 수 없는 인증서를 받을 수 있는 기능이 제거됩니다. 이 경우 일부 서비스를 사용하지 못할 수 있습니다. CTL(인증서 신뢰 목록) 또는 ITL 파일은 여기에 적용되지 않습니다. 서버 인증서가 올바르게 서명되어야 합니다. 그렇지 않으면 클라이언트가 사이드 로딩을 통해 서버 인증서를 신뢰하도록 해야 합니다.
- FIPS는 TLS 1.2를 적용하므로 이전 프로토콜은 비활성화됩니다.
- 모바일 클라이언트용 Cisco Jabber는 플랫폼 모드를 지원하지 않습니다.

공통평가기준

정보 기술 보안 평가에 대한 일반 기준은 IT 제품의 보안 특성을 평가하는 데 사용되는 일련의 국제 표준을 구성합니다. 일반 기준 인증 요구 사항을 준수하는 모드에서 Cisco Jabber를 실행할 수 있습니다. 이렇게 하려면 각 클라이언트에 대해 이 기능을 활성화해야 합니다.

일반 기준으로 활성화된 환경에서 Jabber를 실행하려면 다음을 수행합니다.

- Windows용 Jabber: CC_MODE 설치 인수를 TRUE로 설정합니다.
- Android용 Jabber 및 iPhone 및 iPad용 Jabber: EMM(Enterprise Mobility Management)에서 CC_MODE 매개 변수를 TRUE로 설정합니다.
- RSA 키 길이는 2048비트 이상이어야 합니다. RSA 키 길이를 구성하려면 *Cisco Jabber 12.5* 온프레미스 구축 설명서에서 *Cisco Jabber* 장치를 만들고 구성하는 방법에 대해 읽어 보십시오.

Jabber를 Common Criteria 모드에서 실행하도록 설정하는 방법에 대 한 자세한 내용은 *Cisco Jabber 12.5* 온프레미스 구축 설명서에서 *Cisco Jabber* 애플리케이션 구축 방법을 읽어 보십시오.

보안 **LDAP**

보안 LDAP 통신은 SSL/TLS를 통한 LDAP입니다.

LDAPS는 SSL/TLS 연결을 통해 LDAP 연결을 시작합니다. 그러면 SSL 세션이 열리고 LDAP 프로토콜을 사용하기 시작합니다. 이를 위해서는 별도의 포트, 636 또는 글로벌 카탈로그 포트 3269가 필요합니다.

인증된 **UDS** 연락처 검색

Cisco Unified Communications Manager에서 UDS 연락처 검색에 대한 인증을 활성화하 고 Cisco Jabber는 연락처 검색을 위해 UDS를 인증하는 자격 증명을 제공합니다.

인증서

인증서 확인

인증서 확인 프로세스

운영 체제 Cisco Jabber는 서비스를 인증할 때 서버 인증서의 유효성을 확인할 때 실행됩니다. 보안 연결을 설정하는 동안에는 서비스가 Cisco Jabber에 인증서를 제공합니다. 운영 체제는 클라이언트 장치의 로컬 인증서 저장소에 있는 것과 비교하여 제시된 인증서의 유효성을 확인합니다. 인증서가 인증서 저장소에 없는 경우 인증서는 신뢰할 수 없는 것으로 간주되고 Cisco Jabber는 사용자에게 인증서를 허용하거나 거부하라는 메시지를 표시합니다.

사용자가 인증서를 수락하면 Cisco Jabber는 서비스에 연결하고 장치의 인증서 저장소나 키 체인에 인증서를 저장합니다. 사용자가 인증서를 거부하는 경우 Cisco Jabber는 서비스에 연결하지 않고 인증서가 장치의 인증서 저장소나 키 체인에 저장되지 않습니다.

인증서가 장치의 로컬 인증서 저장소에 있는 경우 인증서를 Cisco Jabber는 인증서를 신뢰합니다. Cisco Jabber는 사용자에게 인증서를 수락 또는 거절할지 묻지 않고 서비스에 연결합니다.

Cisco Jabber 조직에 구축된 항목에 따라 여러 서비스를 인증할 수 있습니다. 각 서비스에 대해 CSR(인증서 서명 요청)을 생성해야 합니다. 일부 공개 인증 기관은 FQDN(Fully Qualified Domain Name) 당 두 개 이상의 CSR을 허용하지 않습니다. 이는 각 서비스의 CSR을 별도의 공개 인증 기관에 보내야 할 수 있음을 의미합니다.

IP 주소 또는 호스트 이름 대신 각 서비스에 대한 서비스 프로파일에 FQDN을 지정했는지 확인하십시오.

서명된 인증서

인증서는 자체 서명 인증서일 수도 있고 CA(인증 기관)에서 서명한 인증서일 수도 있습니다.

- CA 서명 인증서(권장) - 장치에 인증서를 설치하고 있으므로 사용자에게 프롬프트가 표시되지 않습니다. CA 서명 인증서는 사설 CA 또는 공용 CA에서 서명할 수 있습니다. 공용 CA가 서명한 많은 인증서는 장치의 인증서 저장소 또는 키 체인에 저장됩니다. Android 7.0 이상을 사용하는 장치는 CA 서명 인증서만 인식합니다.

- 자체 서명 인증서 - 인증서를 제공하는 서비스에 의해 인증서가 서명되며, 사용자에게 인증서를 허용 또는 거부할 것인지 묻는 메시지가 항상 표시됩니다.

인증서 확인 옵션

인증서 확인을 설정하기 전에 인증서의 유효성을 확인할 방법을 결정해야 합니다.

- 온프레미스 또는 클라우드 기반 구축에 대한 인증서를 구축하는지 여부.
- 인증서에 서명하는 데 사용하는 방법.
- CA 서명 인증서를 구축하는 경우에는 공개 CA 또는 비공개 CA를 사용할지 여부.
- 인증서를 얻는 데 필요한 서비스.

온프레미스 서버에 필요한 인증서

온프레미스 서버는 다음 인증서를 제공하여 Cisco Jabber와의 보안 연결을 설정합니다.

서버	인증서
Cisco Unified Communications Manager IM and Presence Service	HTTP(Tomcat) XMPP
Cisco Unified Communications Manager	HTTP(Tomcat) 및 CallManager 인증서(보안 전화기에 대한 보안 SIP 통화 신호 처리)
Cisco Unity Connection	HTTP(Tomcat)
Webex Meetings 서버	HTTP(Tomcat)
Cisco VCS Expressway Cisco Expressway-E	서버 인증서(HTTP, XMPP 및 SIP 통화 신호 처리에 사용됨)

중요 참고 사항

- SAML(Security Assertion Markup Language) SSO(Single Sign-On) 및 IdP(ID 공급자)에는 x.509 인증서가 필요합니다.
- 인증서 서명 프로세스를 시작하기 전에 Cisco Unified Communications Manager IM and Presence Service에 대해 최근 서비스 업데이트(SU)를 적용해야 합니다.
- 필요한 인증서는 모든 서버 버전에 적용됩니다.
- 각 클러스터 노드의 경우 가입자 및 게시자는 Tomcat 서비스를 실행하고 클라이언트에 HTTP 인증서를 제공할 수 있습니다.

  클러스터의 각 노드에 대해 인증서에 서명하도록 계획해야 합니다.

- 클라이언트 및 Cisco Unified Communications Manager 간 SIP 신호 처리를 보호하려면 CAPF(인증 기관 프록시 기능) 등록을 사용해야 합니다.

인증서 서명 요청 형식 및 요구 사항

일반적으로 CA(인증 기관)에는 특정 형식을 준수하기 위해 CSR(인증서 서명 요청)이 필요합니다. 예를 들어, 공개 CA는 다음과 같은 요구 사항이 있는 CSR만 받아들일 수 있습니다.

- Base64로 인코딩됩니다.
- 조직, **OU** 또는 기타 필드에 특정 문자(예: `@&!`)를 포함하지 마십시오.
- 서버의 공개 키에서 특정 비트 길이를 사용합니다.

여러 노드에서 CSR을 제출하는 경우, 공용 CA가 모든 CSR에서 일관되게 정보를 받도록 요구할 수 있습니다.

CSR에 대한 문제를 방지하려면 CSR을 제출하려는 공용 CA의 형식 요구 사항을 검토해야 합니다. 그런 다음 서버를 구성할 때 입력하는 정보가 공개 CA에 필요한 형식을 준수하는지 확인해야 합니다.

FQDN 당 인증서 하나 - 일부 공개 CA는 FQDN(Fully Qualified Domain Name) 당 하나의 인증서만 서명합니다.

예를 들어 단일 Cisco Unified Communications Manager IM and Presence Service 노드에 대한 HTTP 및 XMPP 인증서에 서명하려면 각 CSR을 서로 다른 공용 CA에 제출해야 할 수 있습니다.

해지 서버

해지 서버에 연결할 수 없는 경우 Cisco Jabber에서 Cisco Unified Communications Manager 서버에 연결할 수 없습니다. CA(인증 기관)에서 인증서를 해지하는 경우에는 Cisco Jabber에서 사용자가 해당 서버에 연결할 수 없습니다.

사용자에게 다음 결과에 대한 알림이 표시 되지 않습니다.

- 인증서에 해제 정보가 포함되어 있지 않습니다.
- 해지 서버에 연결할 수 없습니다.

인증서를 확인하려면 인증서에 해지 정보를 제공할 수 있는 연결 가능한 서버의 **CDP** 또는 **AIA** 필드에 HTTP URL이 포함되어 있어야 합니다.

CA에서 발급한 인증서를 가져올 때 인증서가 유효한지 확인하려면 다음 요구 사항 중 하나를 충족해야 합니다.

- **CRL** 구축 지점(CDP) 필드에 해지 서버의 CRL(인증서 해지 목록)에 대한 HTTP URL이 포함되어 있는지 확인합니다.
- 기관 정보 액세스(AIA) 필드에 OCSP(온라인 인증서 상태 프로토콜) 서버에 대한 HTTP URL이 포함되어 있는지 확인합니다.

인증서의 서버 ID

서명 프로세스의 일부로 CA는 인증서에 서버 ID를 지정합니다. 클라이언트가 인증서를 확인할 때 다음 사항을 확인합니다.

- 신뢰할 수 있는 기관에서 인증서를 발급했습니다.
- 인증서를 제공하는 서버의 ID가 인증서에 지정된 서버의 ID와 일치합니다.

참고 일반적으로 공개 CA에는 IP 주소가 아닌 서버 ID로서 FQDN(Fully Qualified Domain Name)이 필요합니다.

식별자 필드

클라이언트는 ID 일치를 위해 서버 인증서에서 다음 식별자 필드를 확인합니다.

- XMPP 인증서
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - 제목 `CN`
- HTTP 인증서
  - `SubjectAltName\dnsNames`
  - 제목 `CN`

팁 제목 `CN` 필드에는 와일드카드(*)를 가장 왼쪽에 있는 문자로 사용할 수 있습니다(예: `*.cisco.com`).

ID 불일치 방지

사용자가 IP 주소 또는 호스트 이름을 사용하여 서버에 연결을 시도하고 서버 인증서가 FQDN을 사용하여 서버를 식별하는 경우 클라이언트는 서버를 신뢰할 수 있는 것으로 식별하고 사용자에게 메시지를 표시합니다.

서버 인증서가 FQDN을 사용하는 서버를 식별하는 경우 서버의 여러 위치에서 각 서버 이름을 FQDN으로 지정하도록 계획해야 합니다. 자세한 내용은 문제 해결 기술 노트의 *ID* 불일치 방지 섹션을 참조하십시오.

다중 서버 SAN용 인증서

다중 서버 SAN을 사용하는 경우에는 tomcat 인증서당 클러스터당, XMPP 인증서당 클러스터당 각각 한 번씩만 서비스에 인증서를 업로드하면 됩니다. 다중 서버 SAN을 사용하지 않는 경우에는 모든 Cisco Unified Communications Manager 노드의 서비스에 인증서를 업로드해야 합니다.

클라우드 구축을 위한 인증서 확인

Webex Messenger및 Webex Meetings Center는 기본적으로 다음 인증서를 클라이언트에 제공합니다.

- CAS
- WAPI

참고 Webex 공공 CA(Certificate Authority)가 인증서에 서명합니다. Cisco Jabber는 이러한 인증서의 유효성을 확인하여 클라우드 기반 서비스와의 보안 연결을 설정합니다.

Cisco Jabber은(는) Webex Messenger에서 수신한 다음 XMPP 인증서를 확인합니다. 이러한 인증서가 운영체제에 포함되어 있지 않다면, 해당 인증서를 제공해야 합니다.

- VeriSign Class 3 Public Primary Certification Authority - G5 - 이 인증서는 신뢰할 수 있는 루트 인증 기관에 저장됩니다.
- VeriSign Class 3 Secure Server CA - G3 - 이 인증서는 Webex Messenger 서버 ID를 확인하며 Intermediate Certificate Authority에 저장됩니다.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority 루트 인증서

Windows용 Cisco Jabber의 루트 인증서에 관한 자세한 내용은 https://www.identrust.co.uk/certificates/trustid/install-nes36.html을(를) 참조하십시오.

Mac용 Cisco Jabber의 루트 인증서에 관한 자세한 내용은 https://support.apple.com을(를) 참조하십시오.

다중 테넌트 호스팅 협업 솔루션에 대한 서버 이름 표시 지원

Cisco Jabber는 다중 테 넌 트 호스팅 협업 솔루션을 사용 하 여 MRA (Remote Access) 구축에서 SNI (서버 이름 표시)를 지원 합니다.

Cisco Jabber는 SNI를 사용하여 도메인 정보를 Expressway로 전송합니다. Expressway는 인증서 저장소를 조회하여 도메인 정보가 포함된 인증서를 찾고 인증서를 Cisco Jabber에 반환하여 유효성을 확인합니다.

다중 테넌트 구축에 대한 자세한 내용은 Cisco Hosted Collaboration Solution, 릴리스 11.5 다중 테넌트 Expressway 구성 설명서의 도메인 인증서를 사용한 엔드포인트 서비스 검색 및 도메인 인증서를 사용한 *Jabber Service* 검색 섹션을 참조하십시오.

바이러스 백신 제외

바이러스 백신 소프트웨어를 구축하는 경우 바이러스 백신 제외 목록에 다음 폴더 위치를 포함하십시오.

- `C:\Users\<User>\AppData\Local\Cisco\Unified Communications\Jabber`
- `C:\Users\<User>\AppData\Roaming\Cisco\Unified Communications\Jabber`
- `C:\ProgramData\Cisco Systems\Cisco Jabber`