# 인증서 확인 구성


- 온프레미스 구축을 위한 인증서 구성, 1 페이지
- CA 인증서를 클라이언트에 구축, 2 페이지


# 온프레미스 구축을 위한 인증서 구성

Jabber 클라이언트가 연결하는 각 서비스에 대해 인증서가 필요합니다.

프로시저

| | 명령 또는 동작 | 목적 |
|---|---|---|
| 단계 **1** | Cisco Unified Presence 또는 Cisco Unified Communications Manager IM and Presence Service가 있는 경우, 해당 HTTP(tomcat) 및 XMPP 인증서를 다운로드하십시오. | 자세한 내용은 Cisco Unified Communications Manager의 IM and Presence 서비스 구성 및 관리에 있는 *IM and Presence* 서비스에서 보안 구성 장을 참고하십시오. |
| 단계 **2** | Cisco Unified Communications Manager 및 Cisco Unity Connection에 대한 HTTPS(tomcat) 인증서를 다운로드합니다. | 자세한 내용은 여기에 있는 *Cisco Unified Communications Manager* 보안 설명서 및 *Cisco Unified Communications* 운영 시스템 관리 설명서를 참조하십시오. |
| 단계 **3** | Webex Meetings 서버의 HTTP(tomcat)를 다운로드합니다. | 자세한 내용은 여기에 있는 *Cisco Webex Meetings* 서버 관리 설명서를 참조하십시오. |
| 단계 **4** | Remote Access를 구성하려면 Cisco VCS Expressway 및 Cisco Expressway-E 서버 인증서를 다운로드하십시오. 이 서버 인증서는 HTTP와 XMPP 모두에 사용합니다. | 자세한 내용은 Cisco VCS Expressway에서 인증서 구성을 참조하십시오. |
| 단계 **5** | CSR(Certificate Signing Request, 인증서 서명 요청)을 생성합니다. | |
| 단계 **6** | 인증서를 서비스에 업로드합니다. | 다중 서버 SAN을 사용하는 경우에는 tomcat 인증서당 클러스터당, XMPP 인증서당 클러 |

| | 명령 또는 동작 | 목적 |
|---|---|---|
| | | 스터당 각각 한 번씩만 서비스에 인증서를 업로드하면 됩니다. 다중 서버 SAN을 사용하지 않는 경우에는 모든 Cisco Unified Communications Manager 노드의 서비스에 인증서를 업로드해야 합니다. |
| 단계 7 | CA 인증서를 클라이언트에 구축, 2 페이지 | 인증서 확인을 수행할 때 인증서를 수락 또는 거부하라는 메시지를 사용자에게 표시하지 않으려면 클라이언트의 로컬 인증서 저장소에 인증서를 구축하십시오. |

# CA 인증서를 클라이언트에 구축

인증서 확인을 수행할 때 인증서를 수락 또는 거부하라는 메시지를 사용자에게 표시하지 않으려면 엔드포인트 클라이언트의 로컬 인증서 저장소에 인증서를 구축하십시오.

잘 알려진 공개 CA를 사용하는 경우, 클라이언트 인증서 저장소나 키체인에 CA 인증서가 이미 있을 수 있습니다. 그러한 경우에는 클라이언트에 CA 인증서를 구축하지 않아도 됩니다.

CA 인증서가 아직 클라이언트 인증서 저장소나 키체인에 없는 경우에는 CA 인증서를 클라이언트에 구축하십시오.

| 구축 크기가 다음과 같은 경우, | 다음을 권장합니다. |
|---|---|
| 다수의 로컬 시스템에 | 인증서 구축 도구 사용(예: 그룹 정책 또는 인증서 구축 관리 애플리케이션). |
| 더 적은 수의 로컬 시스템에 | CA 인증서를 수동으로 구축 |

# CA 인증서를 Windows용 Cisco Jabber 클라이언트에 수동으로 구축

프로시저

단계 1 Windows용 Cisco Jabber 클라이언트 시스템에서 CA 인증서를 사용할 수 있게 합니다.

단계 2 Windows 시스템에서 인증서 파일을 엽니다.

단계 3 인증서를 설치하고 다음을 선택합니다.

단계 4 다음 저장소에 모든 인증서 보관을 선택한 다음, 찾아보기를 선택합니다.

단계 5 신뢰할 수 있는 루트 인증 기관 저장소를 선택합니다.
마법사를 완료하면 인증서 가져오기가 성공하였음을 확인하는 메시지가 표시됩니다.

다음에 수행할 작업

Windows 인증서 관리자 도구를 열어 인증서가 올바른 인증서 저장소에 설치되어 있는지 확인합니다. 신뢰할 수 있는 루트 인증 기관 > 인증서로 이동합니다. CA 루트 인증서가 인증서 저장소에 나열됩니다.

# CA 인증서를 Mac용 Cisco Jabber 클라이언트에 수동으로 배포

프로시저

단계 **1** Mac용 Cisco Jabber 클라이언트 시스템에서 CA 인증서를 사용할 수 있게 합니다.

단계 **2** Mac 시스템에서 인증서 파일을 엽니다.

단계 **3** 현재 사용자만을 위한 로그인 키체인에 추가한 다음, 추가를 선택합니다.

다음에 수행할 작업

Keychain Access 도구를 열고 인증서를 선택하여 인증서가 올바른 키체인에 설치되어 있는지 확인합니다. CA 루트 인증서가 키체인에 나열됩니다.

# CA 인증서를 모바일 클라이언트에 수동으로 구축

CA 인증서를 iOS 클라이언트에 구축하려면 인증서 구축 관리 애플리케이션이 필요합니다. 사용자에게 CA 인증서를 이메일로 보내거나 사용자가 액세스할 수 있도록 웹 서버에서 인증서를 제공할 수 있습니다. 사용자는 인증서 구축 관리 도구를 사용하여 인증서를 다운로드하고 설치할 수 있습니다.

그러나 Android용 Jabber에는 인증서 관리 도구가 없으므로 다음과 같은 절차를 따라야 합니다.

프로시저

단계 **1** CA 인증서를 장치에 다운로드합니다.

단계 **2** 장치 설정 > 보안 > 장치 저장소에서 설치를 누르고 지침을 따릅니다.