

# Broadworks용 Webex에서 CTI 인터페이스에 대한 트러스트 업데이트

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[Trust Anchor 설정 및 갱신](#)

[프로세스 개요](#)

[Webex CA 인증서 다운로드](#)

[스플릿 인증서 체인](#)

[첫 번째 인증서\(루트 인증서\):](#)

[두 번째 인증서의 경우\(발급 인증서\):](#)

[파일 복사](#)

[트러스트 앵커 업데이트](#)

[업데이트 확인](#)

[TLS 핸드셰이크 확인](#)

[관련 정보](#)

---

## 소개

이 문서에서는 Broadworks용 Webex에서 CTI 인터페이스에 대한 트러스트 앵커를 업데이트하는 프로세스에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Control Hub 의 설정 구성에 대한 숙지
- Broadworks CLI(Command Line Interface)를 구성하고 탐색하는 방법 이해
- SSL/TLS 프로토콜 및 인증서 인증에 대한 기본 이해

### 사용되는 구성 요소

이 문서의 정보는 Broadworks R22 이상을 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

이 문서에서는 Broadworks XSP/ADP 호스트가 인터넷에 연결되어 있다고 가정합니다.

## 구성

이 절차에는 특정 인증서 파일을 다운로드하고, 분할하여, XSP의 특정 위치에 복사한 다음 이러한 인증서를 새 트러스트 앵커로 업로드하는 작업이 포함됩니다. XSP와 Webex 간의 안전하고 신뢰할 수 있는 통신을 보장하는 데 도움이 되는 중요한 작업입니다.

이 문서에서는 CTI 인터페이스용 Trust Anchor를 처음으로 설치하는 단계를 보여줍니다. 이는 업데이트를 수행해야 할 때도 마찬가지입니다. 이 설명서에서는 필요한 인증서 파일을 획득하고 개별 인증서로 분리한 다음 XSP/ADP의 새 트러스트 앵커에 업로드하는 단계를 설명합니다.

## Trust Anchor 설정 및 갱신

초기 설정 및 이후 업데이트는 동일한 프로세스입니다. 처음으로 트러스트를 추가할 때 단계를 완료하고 트러스트가 추가되었는지 확인합니다.

업데이트할 때 새 트러스트를 추가하고 새 트러스트를 설치한 후 이전 트러스트를 삭제하거나 두 트러스트를 모두 유지할 수 있습니다. W4B 서비스가 관련 인증서를 제시하여 두 트러스트 중 하나와 일치하면 기존 트러스트와 새 트러스트가 동시에 작동할 수 있습니다.

요약하자면,

- 새 Cisco 트러스트 인증서는 기존 트러스트가 만료되기 전에 언제든지 추가할 수 있습니다.
- 이전 신뢰는 새 신뢰가 추가됨과 동시에 제거할 수 있으며, 운영 팀에서 해당 접근법을 선호하는 경우 나중에 제거할 수도 있습니다.

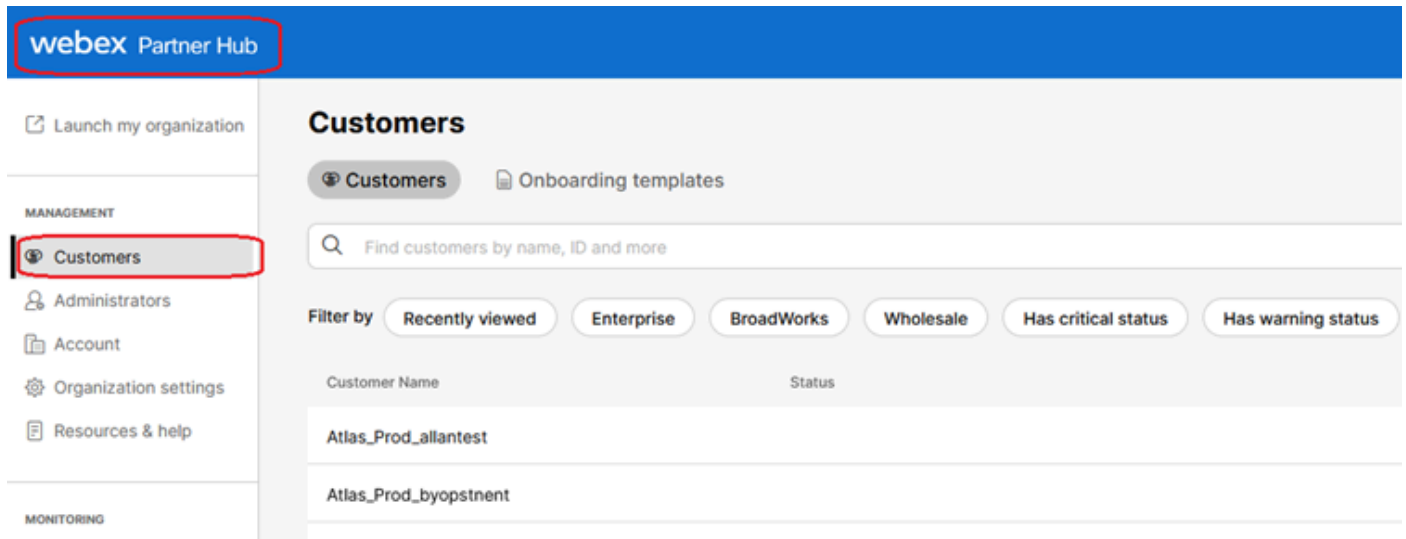
## 프로세스 개요

프로세스의 개요는 Trust Anchors에 대한 초기 설치 및 업데이트에 모두 적용됩니다.

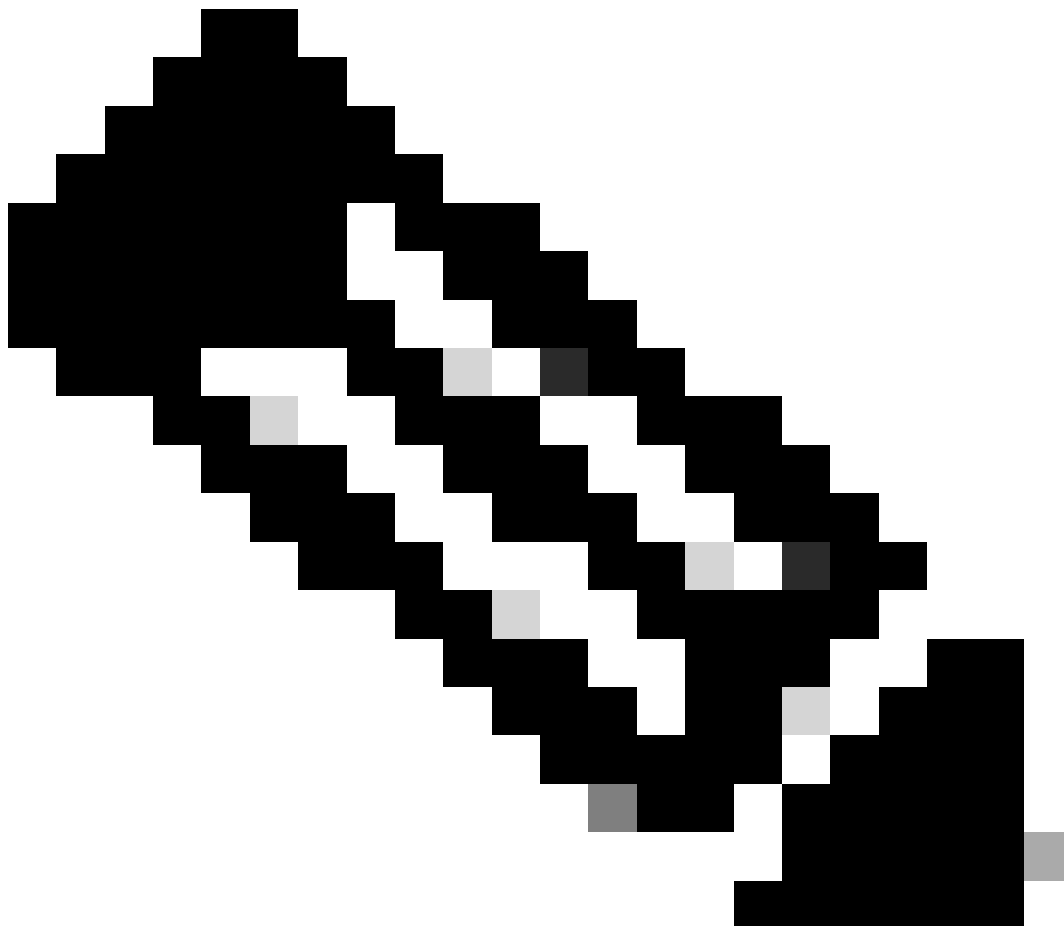
- Webex CA 인증서 다운로드: Settings(설정) > BroadWorks Calling(BroadWorks 호출) 아래의 Partner Hub에서 CombinedCertChain2023.txt 파일을 가져옵니다.
- Split Certificate Chain(인증서 체인 분할): 결합된 인증서 체인 파일을 두 개의 별도 인증서 파일(root2023.txt 및 issuing2023.txt)로 분할합니다.
- 파일 복사: 두 인증서 파일을 모두 XSP/ADP의 임시 위치로 전송합니다.
- Update Trust Anchors(트러스트 앵커 업데이트): XSP/ADP 명령줄 인터페이스 내에서 updateTrust 명령을 사용하여 인증서 파일을 새 트러스트 앵커에 업로드합니다.
- 업데이트 확인: 트러스트 앵커가 성공적으로 업데이트되었는지 확인합니다.

## Webex CA 인증서 다운로드

1. 파트너 허브에 로그인합니다.



Webex 파트너 허브



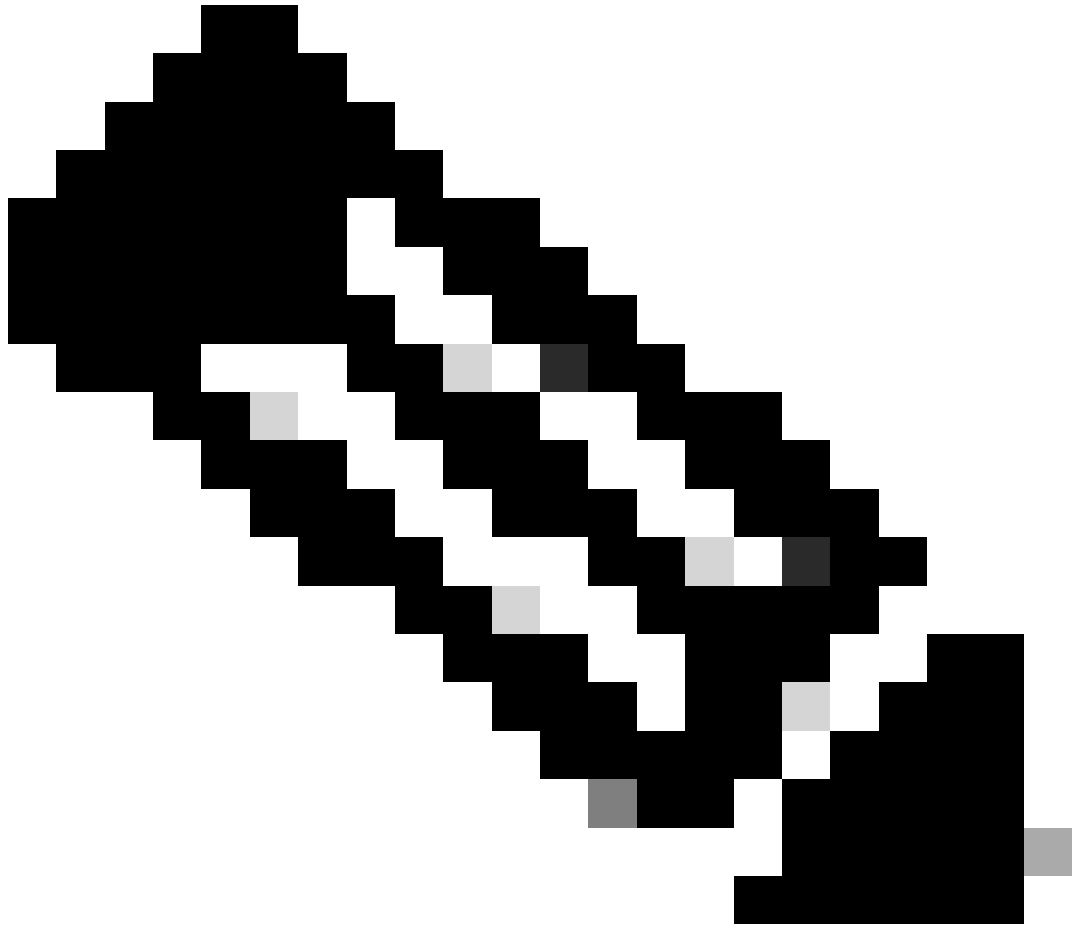
참고: Partner Hub는 Control Hub와 다릅니다. Partner Hub의 왼쪽 창에 Customers(고객

)가 있고 제목 창에 Partner Hub(파트너 허브)가 있습니다.

2. Organization Settings(조직 설정) > BroadWorks Calling(BroadWorks 통화)으로 이동하여 Download Webex CA(Webex CA 다운로드)를 클릭합니다.

The screenshot shows the webex Partner Hub interface. On the left sidebar, 'Organization settings' is highlighted. The main content area is titled 'Organization Settings' and has a sub-tab for 'BroadWorks Calling'. It displays various configuration options: Clusters (4 active clusters), Meeting join configuration (BYoPSTN), Call-in phone number groups (4 active groups), and Callback DNS SRV groups (4 active groups). At the bottom, under 'Partner Configuration Resources', the link 'Download Webex CA certificate (2023)' is highlighted with a red box.

인증서 다운로드 링크를 표시하는 조직 설정 페이지



참고: 최신 옵션을 선택합니다. 이 스크린샷에서는 Download Webex CA certificate(2023)가 최신 버전임을 확인할 수 있습니다

---

3. 여기에 표시된 인증서 보안상의 이유로 이미지가 난독화되었습니다.

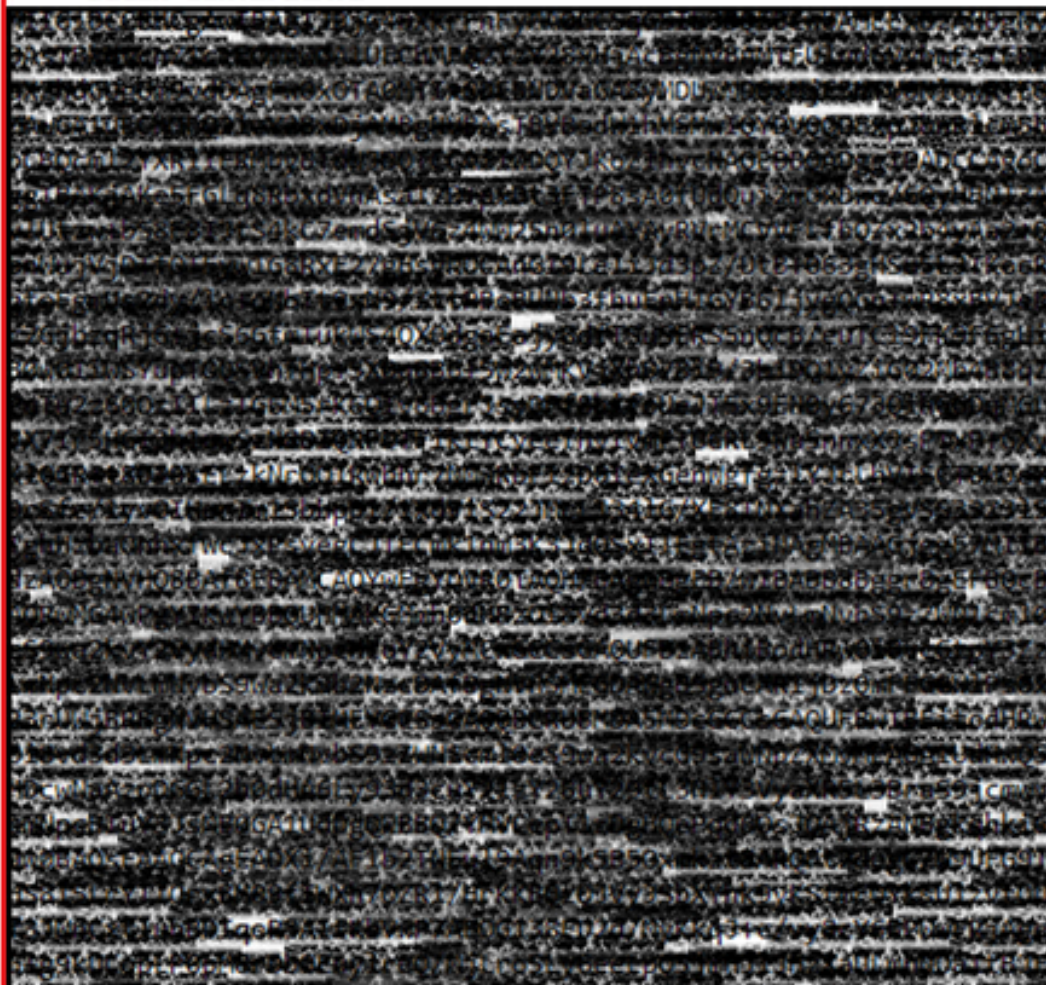
-----BEGIN CERTIFICATE-----



1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----



2

에 업로드하기 전에 파일을 분할해야 합니다. 인증서 체인을 개별 인증서로 분할하는 절차는 다음과 같습니다. 이 프로세스에서는 결합된 인증서 파일을 루트로 분리하고 인증서를 발급하는 단계를 보여줍니다.

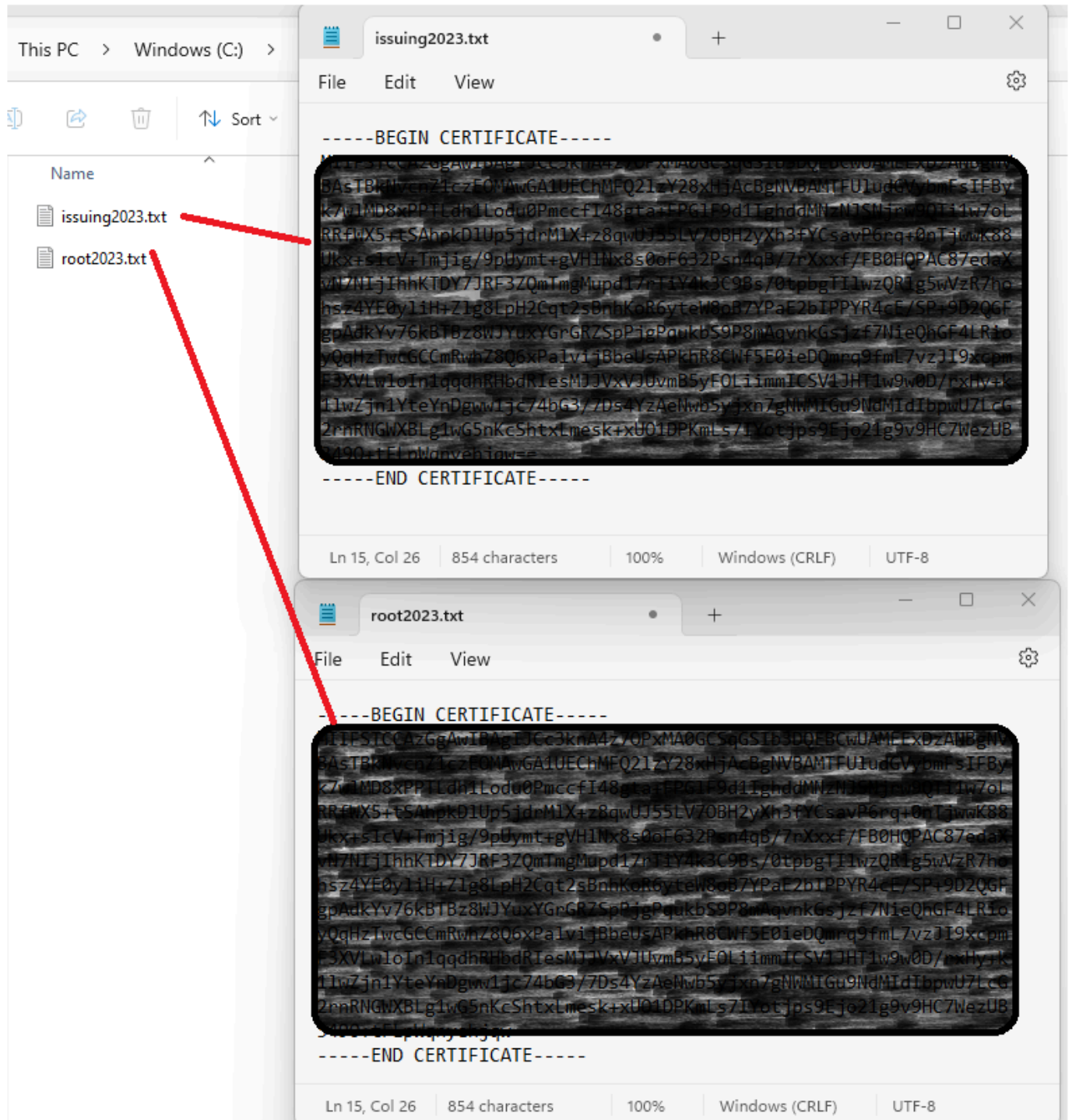
1. 결합된 인증서 파일은 2개의 개별 인증서로 분할됩니다.
  - root2023.txt
  - issuing2023.txt
2. 개별 인증서를 식별합니다.
  - 파일에는 -----BEGIN CERTIFICATE— 및 END CERTIFICATE— 마커로 구분된 여러 인증서----- 포함되어 있습니다. 각 블록은 단일 인증서를 나타냅니다.
3. 인증서 분할
  - 체인을 분할하려면 식별하는 각 인증서 블록에 대해 새 텍스트 파일을 생성해야 합니다.

첫 번째 인증서(루트 인증서):

- -----BEGIN CERTIFICATE(시작 인증서) 및 END CERTIFICATE(종료 인증서) 줄을 포함하여 첫 번째 텍스트 블록----- 선택합니다.
- 선택한 텍스트를 복사합니다.
- 새 텍스트 파일을 열고 복사한 텍스트를 이 파일에 붙여넣습니다.
- 새 파일을 root2023.txt로 저장합니다.

두 번째 인증서의 경우(발급 인증서):

- 원래의 결합된 인증서 체인 파일로 돌아갑니다.
- 두 번째 텍스트 블록(체인의 다음 인증서)을 선택합니다. 여기에는 -----BEGIN CERTIFICATE— 및 -----END CERTIFICATE—행이 포함됩니다.
- 선택한 텍스트를 복사하여 새 텍스트 파일에 붙여 넣고 파일을 issuing2023.txt로 저장하는 프로세스를 반복합니다



수정된 분할 인증서



---

참고: 각 새 파일에 인증서가 하나만 있고 BEGIN 및 END 마커가 올바르게 포함되어 있는지 확인하는 것이 좋습니다.

---

## 파일 복사

root2023.txt 및 issuing2023.txt를 모두 XSP/ADP의 임시 디렉토리(예: /var/broadworks/tmp/)에 복사합니다. WinSCP 또는 기타 유사한 애플리케이션을 사용하여 이 작업을 수행할 수 있습니다.

```
bwadmin@tac-ucaas.cisco.com$ ls -l /var/broadworks/tmp/  
-rwxrwxrwx 1 bwadmin bwadmin 2324 Jul 21 2023 issuing2023.txt  
-rwxrwxrwx 1 bwadmin bwadmin 1894 Jul 21 2023 root2023.txt
```

## 트러스트 앵커 업데이트

새 트러스트 앵커를 설정하기 위해 인증서 파일을 업로드합니다. CTI XSP/ADP BWCLI 내에서 다음 명령을 실행합니다.

```
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> updateTrust webexclientroot2023  
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> updateTrust webexclientissuing
```

---

참고: 각 별칭은 고유해야 합니다. 예를 들어 webexclientroot2023 및 webexclientissuing2023은 트러스트 앵커의 샘플 별칭 역할을 합니다. 각 별칭이 고유하도록 사용자 지정 별칭을 자유롭게 생성할 수 있습니다.

---

## 업데이트 확인

이 명령을 실행하여 앵커가 업데이트되었는지 확인합니다

```
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> get  
Alias Owner Issuer
```

```
=====
```

webexclientissuing2023	Internal	Private	TLS SubCA	Internal	Private	Root
webexclientroot2023	Internal	Private	Root	Internal	Private	Root[self-signed]

CTI 인터페이스가 최신 인증서로 업데이트되었습니다.

# TLS 핸드셰이크 확인

SSL 핸드셰이크를 보려면 FieldDebug 심각도에서 Tomcat TLS 로그를 활성화해야 합니다.

```
ADP_CLI/Applications/WebContainer/Tomcat/Logging/InputChannels> get
Name Enabled Severity
=====
TLS true FieldDebug
```

TLS 디버깅은 ADP 2022.10 이상에서만 가능합니다. [Cisco BroadWorks Log Cryptographic Connection Setup and Teardown](#)을 참조하십시오.

## 관련 정보

- [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.