

Unified CCE 솔루션: 서드파티 CA 인증서 가져오기 및 업로드 절차(버전 11.x)

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. CSR\(Certificate Signing Request\)을 생성하고 다운로드합니다.](#)

[2단계. Certificate Authority에서 Root\(루트\), Intermediate\(해당하는 경우 5단계\) 및 Application certificate\(애플리케이션 인증서\)를 가져옵니다.](#)

[3단계. 서버에 인증서를 업로드합니다.](#)

[Finesse 서버](#)

[CUIC 서버\(인증서 체인에 중간 인증서가 없는 것으로 가정\)](#)

[라이브 데이터 서버](#)

[라이브 데이터 서버 인증서 종속성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 서드파티 벤더에서 생성된 CA(Certification Authority) 인증서를 가져와 설치하여 Finesse, Cisco CUIC(Unified Intelligence Center) 및 LD(Live Data) 서버 간에 HTTPS 연결을 설정하는 단계를 자세히 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCCE(Unified Contact Center Enterprise)
- Cisco LD(Live Data)
- Cisco CUIC(Unified Intelligence Center)
- Cisco Finesse
- CA 인증

사용되는 구성 요소

이 문서에 사용된 정보는 UCCE 솔루션 11.0(1) 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 단계의 잠재적 영향을 이해해야 합니다.

배경 정보

Finesse, CUIC 및 Live Data 서버 간 보안 통신에 HTTPS를 사용하려면 보안 인증서 설정이 필요합니다. 기본적으로 이러한 서버는 자체 서명 인증서를 제공하며, 이는 고객이 CA(Certificate Authority) 서명 인증서를 구매하여 설치할 수 있는 경우에 사용됩니다. 이러한 CA 인증서는 VeriSign, Thawte, GeoTrust와 같은 서드파티 벤더로부터 받거나 내부에서 생산할 수 있습니다.

구성

Finesse, CUIC 및 Live Data 서버에서 HTTPS 통신용 인증서를 설정하려면 다음 단계를 수행해야 합니다.

1. CSR(Certificate Signing Request)을 생성하고 다운로드합니다.
2. CSR을 사용하여 Certificate Authority에서 루트, 중간(해당되는 경우) 및 애플리케이션 인증서를 가져옵니다.
3. 서버에 인증서를 업로드합니다.

1단계. CSR(Certificate Signing Request)을 생성하고 다운로드합니다.

1. 여기서 CSR을 생성하고 다운로드하는 단계는 Finesse, CUIC 및 Live 데이터 서버에 대해 동일합니다.
2. 명시된 URL을 사용하여 Cisco Unified Communications Operating System Administration 페이지를 열고 설치 프로세스 중에 생성된 OS 관리자 계정으로 로그인합니다
<https://FQDN:8443/cmplatform>
3. 이미지에 표시된 대로 CSR(Certificate Signing Request)을 생성합니다.

1단계. Security(보안) > Certificate Management(인증서 관리) > Generate CSR(CSR 생성)로 이동합니다.

2단계. Certificate Purpose Name(인증서 용도 이름) 드롭다운 목록에서 tomcat을 선택합니다

3단계. 비즈니스 요구 사항에 따라 Hash Algorithm(해시 알고리즘) 및 key length(키 길이)를 선택합니다.

- 키 길이: 2048 \ 해시 알고리즘: SHA256 권장

4단계. Generate CSR(CSR 생성)을 클릭합니다.

참고: 비즈니스에서 SAN(Subject Alternate Names) 상위 도메인 필드를 도메인 이름으로 채워야 하는 경우 "[Finesse](#)에서 서드파티 [서명 인증서](#)가 있는 SAN이 문제를 일으키는 주소" [문서](#)에 문제 주소를 적어 주십시오.

4. 이미지에 표시된 대로 CSR(Certificate Signing Request)을 다운로드합니다.



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate Management

Certificate List



Generate Self-signed



Upload Certificate/Certificate chain



Generate CSR



Download CSR



1단계. Security(보안) > Certificate Management(인증서 관리) > Download CSR(CSR 다운로드)로 이동합니다.

2단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat을 선택합니다.

3단계. Download CSR(CSR 다운로드)을 클릭합니다.

참고:

참고: CSR(Certificate Authority)을 가져오려면 URL <https://FQDN:8443/cmplatform>을 사용하여 보조 서버에서 위와 같은 단계를 수행합니다

2단계. Certificate Authority에서 Root(루트), Intermediate(해당하는 경우 5단계) 및 Application certificate(애플리케이션 인증서)를 가져옵니다.

1. VeriSign, Thawte, GeoTrust 등과 같은 타사 인증 기관에 기본 및 보조 서버 CSR(Certificate Signing Request) 정보를 제공합니다.
2. 인증 기관에서는 기본 및 보조 서버에 대해 다음 인증서 체인을 수신해야 합니다.
 - Finesse 서버: 루트, 중간(선택 사항) 및 애플리케이션 인증서
 - CUIC 서버: 루트, 중간(선택 사항) 및 애플리케이션 인증서
 - 라이브 데이터 서버: 루트, 중간(선택 사항) 및 애플리케이션 인증서

3단계. 서버에 인증서를 업로드합니다.

이 섹션에서는 Finesse, CUIC 및 Live 데이터 서버에서 인증서 체인을 올바르게 업로드하는 방법에 대해 설명합니다.

Finesse 서버

The screenshot shows a web-based dialog box titled "Upload Certificate/Certificate chain". At the top, there are "Upload" and "Close" buttons. Below this is a "Status" section with an information icon and a warning message: "Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster". The main content area is titled "Upload Certificate/Certificate chain" and contains a dropdown menu for "Certificate Purpose" with "tomcat-trust" selected. Below this is a text field for "Description(friendly name)". The "Upload File" section includes a "Browse..." button and the text "No file selected.". At the bottom of the dialog are "Upload" and "Close" buttons.

1. 다음 단계를 통해 기본 Finesse 서버에 루트 인증서를 업로드합니다.

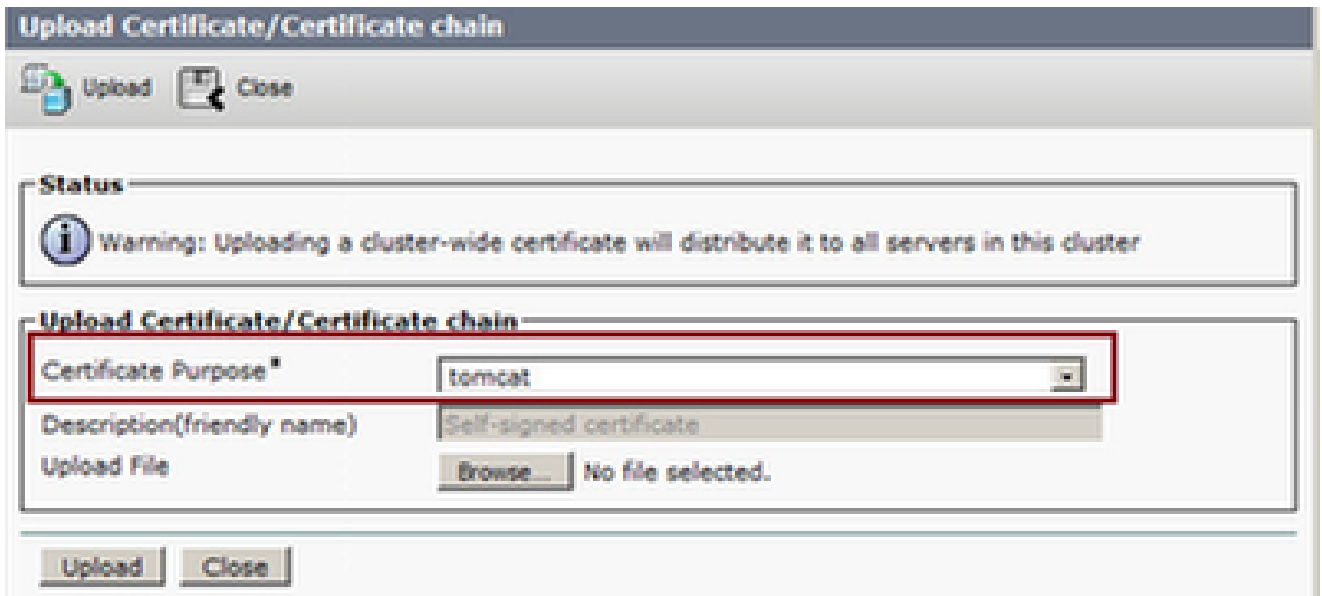
- 1단계. 기본 서버 Cisco Unified Communications 운영 체제 관리 페이지에서 Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)
- 2단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat-trust를 선택합니다.
- 3단계. Upload File(파일 업로드) 필드에서 browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.
- 4단계. 파일 업로드를 클릭합니다.

2. 다음 단계를 통해 기본 Finesse 서버에 중간 인증서를 업로드합니다.

- 1단계. 중간 인증서를 업로드하는 단계는 1단계에 나와 있는 루트 인증서와 같습니다.
- 2단계. 기본 서버 Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지에서 Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.
- 3단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat-trust를 선택합니다.
- 4단계. Upload File(파일 업로드) 필드에서 browse(찾아보기)를 클릭하고 Intermediate certificate file(중간 인증서 파일)을 찾습니다.
- 5단계. Upload를 클릭합니다.

참고: Tomcat-trust 저장소가 기본 서버와 보조 서버 간에 복제되므로 루트 또는 중간 인증서를 보조 finesse 서버에 업로드할 필요가 없습니다.

3. 이미지에 표시된 대로 기본 Finesse 서버 애플리케이션 인증서를 업로드합니다.



The screenshot shows a web interface for uploading a certificate. The title is "Upload Certificate/Certificate chain". There are "Upload" and "Close" buttons at the top left. A status message with an information icon says: "Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster". Below this, the main form has a "Certificate Purpose" dropdown menu with "tomcat" selected, which is highlighted by a red rectangle. The "Description(friendly name)" field contains "Self-signed certificate". The "Upload File" section has a "Browse..." button and the text "No file selected.". At the bottom, there are "Upload" and "Close" buttons.

1단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat을 선택합니다.

2단계. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 애플리케이션 인증서 파일을 찾습니다.

3단계. 파일을 업로드하려면 Upload(업로드)를 클릭합니다.

4. 보조 Finesse 서버 애플리케이션 인증서를 업로드합니다.

이 단계에서 자체 애플리케이션 인증서에 대해 보조 서버에서 3단계에서 언급한 것과 동일한 프로세스를 수행합니다.

5. 이제 서버를 다시 시작할 수 있습니다.

기본 및 보조 Finesse 서버에서 CLI에 액세스하고 `utils system restart` 명령을 입력하여 서버를 다시 시작합니다.

CUIC 서버(인증서 체인에 중간 인증서가 없는 것으로 가정)

1. 기본 CUIC 서버에 루트 인증서 업로드

1단계. 기본 서버 Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지에서 Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드

)으로 이동합니다.

2단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat-trust를 선택합니다.

3단계. Upload File(파일 업로드) 필드에서 browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

4단계. 파일 업로드를 클릭합니다.

참고: tomcat-trust 저장소가 기본 서버와 보조 서버 간에 복제되므로 루트 인증서를 보조 CUIC 서버에 업로드할 필요가 없습니다.

2. 기본 CUIC 서버 애플리케이션 인증서를 업로드합니다.

1단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat을 선택합니다.

2단계. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 애플리케이션 인증서 파일을 찾습니다.

3단계. 파일 업로드를 클릭합니다.

3. 보조 CUIC 서버 애플리케이션 인증서를 업로드합니다.

자체 애플리케이션 인증서에 대해 보조 서버에서 (2)단계에서 설명한 것과 동일한 프로세스를 따릅니다

4. 서버 다시 시작

기본 및 보조 CUIC 서버에서 CLI에 액세스하고 "utils system restart" 명령을 입력하여 서버를 재시작합니다.

참고: CA 기관이 중간 인증서를 포함하는 인증서 체인을 제공하는 경우 Finesse Servers 섹션에 설명된 단계를 CUIC 서버에도 적용할 수 있습니다.

라이브 데이터 서버

1. Live-Data 서버에서 인증서를 업로드하는 단계는 인증서 체인에 따라 Finesse 또는 CUIC 서버와 동일합니다.

2. 기본 Live-Data 서버에 루트 인증서 업로드

1단계. 기본 서버 Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지에서 Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.

2단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat-trust를 선택합니다.

3단계. Upload File(파일 업로드) 필드에서 browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

4단계. Upload를 클릭합니다.

3. 주 Live-Data 서버에 중간 인증서를 업로드합니다.

- 1단계. 중간 인증서를 업로드하는 단계는 1단계에 나와 있는 루트 인증서와 같습니다.
- 2단계. 기본 서버 Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지에서 Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.
- 3단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat-trust를 선택합니다.
- 4단계. Upload File(파일 업로드) 필드에서 browse(찾아보기)를 클릭하고 Intermediate certificate(중간 인증서) 파일을 찾습니다.
- 5단계. Upload를 클릭합니다.

참고: Tomcat-trust 저장소가 기본 서버와 보조 서버 간에 복제되므로 루트 또는 중간 인증서를 보조 Live-Data 서버에 업로드할 필요가 없습니다.

4. 주 Live-Data 서버 응용 프로그램 인증서 업로드.

- 1단계. Certificate Name(인증서 이름) 드롭다운 목록에서 tomcat을 선택합니다.
- 2단계. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 애플리케이션 인증서 파일을 찾습니다.
- 3단계. Upload를 클릭합니다.

5. 보조 Live-Data 서버 응용 프로그램 인증서를 업로드합니다.

자체 애플리케이션 인증서에 대해 보조 서버에서 (4)에서 언급한 것과 동일한 단계를 수행합니다.

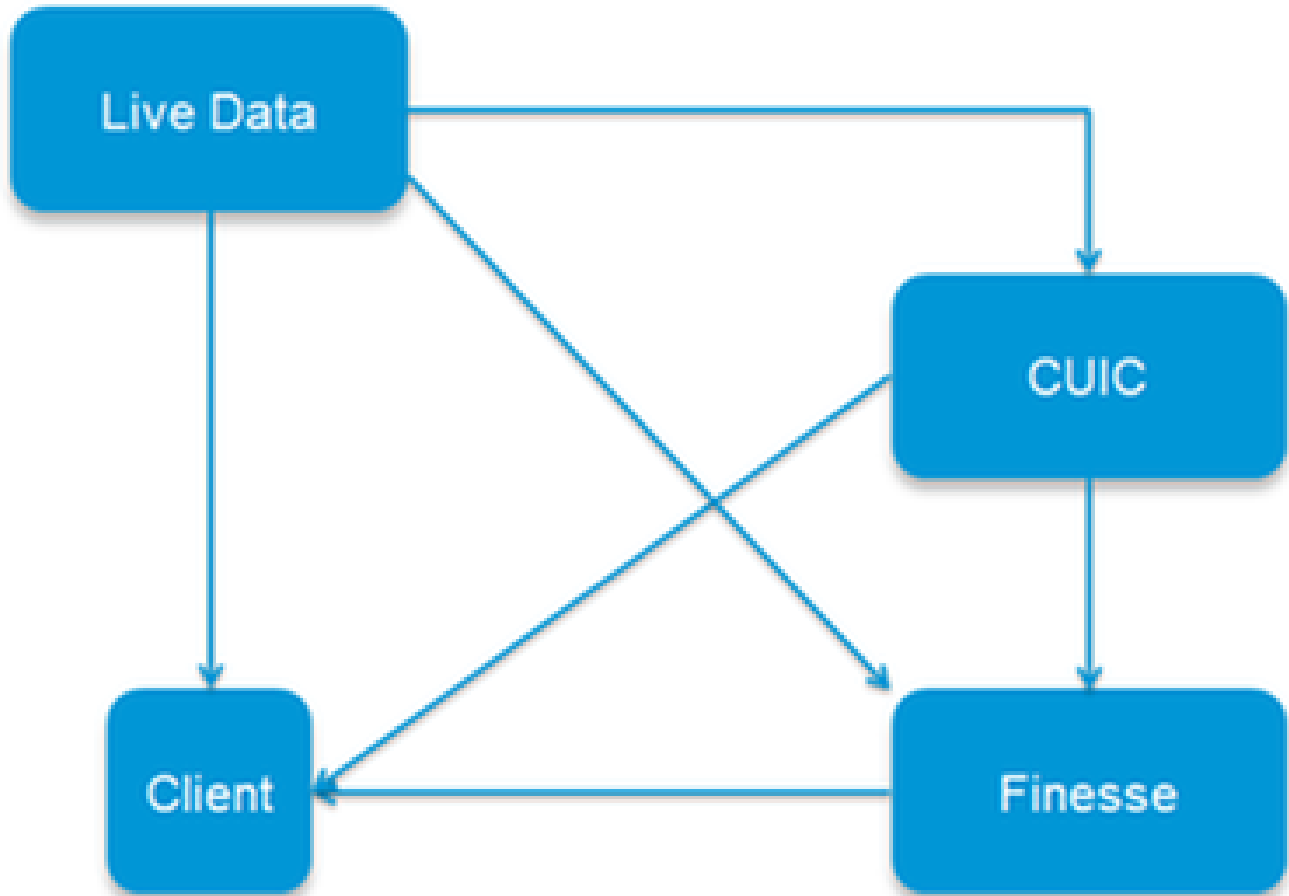
6. 서버 다시 시작

기본 및 보조 Finesse 서버에서 CLI에 액세스하고 "utils system restart" 명령을 입력하여 서버를 다시 시작합니다.

라이브 데이터 서버 인증서 종속성

라이브 데이터 서버가 CUIC 및 Finesse 서버와 상호 작용하면 그림과 같이 이러한 서버 간에 인증서 종속성이 있습니다.

Certificate Dependencies



서드파티 CA 인증서 체인과 관련하여 루트 및 중간 인증서는 조직의 모든 서버에서 동일합니다. Live 데이터 서버가 제대로 작동하려면 Finesse 및 CUIC 서버에 Tomcat-Trust 컨테이너에 루트 및 중간 인증서가 제대로 로드되어 있어야 합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

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.