Package CCE 솔루션: 서드파티 CA 인증서를 가져오고 업로드하는 절차

목차

소개

이 문서에서는 Finesse와 Cisco CUIC(Unified Intelligence Center) 서버 간의 HTTPS 연결을 설정하기 위해 서드파티 벤더에서 생성된 CA(Certification Authority) 인증서를 가져오고 설치하는 단계에 대해 설명합니다.

Finesse와 CUIC 서버 간의 보안 통신에 HTTPS를 사용하려면 보안 인증서 설정이 필요합니다. 기본적으로 이러한 서버는 자체 서명된 인증서를 제공하며, 이는 고객이 CA 인증서를 구매하여 설치할 수 있는 경우에 사용됩니다. 이러한 CA 인증서는 VeriSign, Thawte, GeoTrust와 같은 서드파티 벤더에서 얻거나 내부에서 생성할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco PCCE(Package Contact Center Enterprise)
- CUIC
- Cisco Finesse
- CA 인증서

사용되는 구성 요소

이 문서에 사용된 정보는 PCCE 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.

절차

Finesse 및 CUIC 서버에서 HTTPS 통신용 인증서를 설정하려면 다음 단계를 수행합니다.

- CSR(Certificate Signing Request) 생성 및 다운로드
- CSR을 사용하여 CA로부터 루트, 중간(해당되는 경우) 및 애플리케이션 인증서를 얻습니다.
- 서버에 인증서 업로드

CSR 생성 및 다운로드

1. 여기에서 설명하는 단계는 CSR을 생성하고 다운로드하기 위한 것입니다. 이러한 단계는 Finesse 및 CUIC 서버에서도 동일합니다.

2. URL이 있는 Cisco Unified Communications Operating System Administration 페이지를 열고 설치 프로세스 시 생성된 운영 체제 관리자 계정으로 로그인합니다. 주 서버/플랫폼 https://hostname

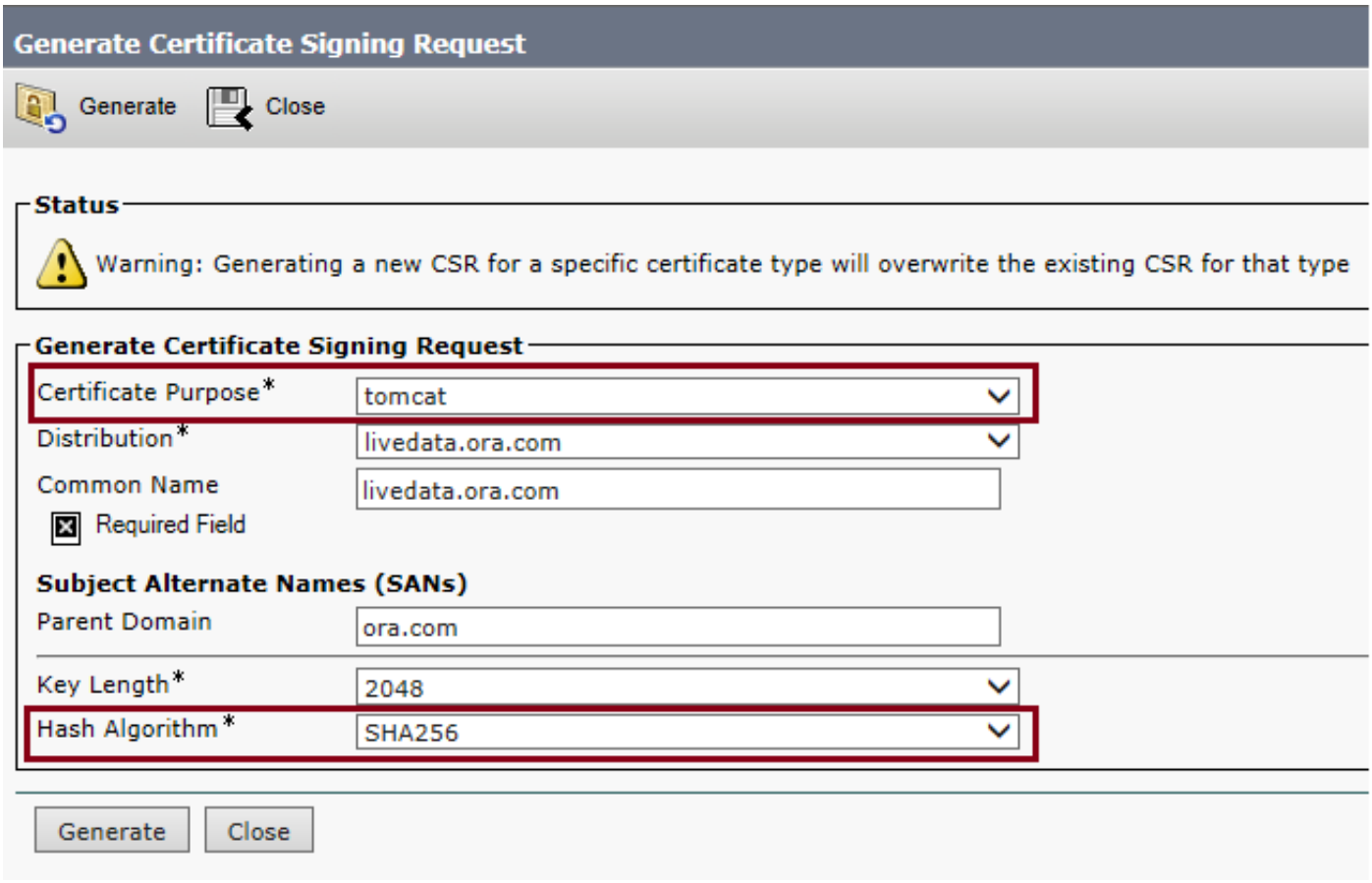
3. CSR(Certificate Signing Request) 생성

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

b. Certificate Purpose*(인증서 용도*) 드롭다운 목록에서 tomcat을 선택합니다.

c. Hash Algorithm을 SHA256으로 선택합니다.

d. 이미지에 표시된 대로 Generate(생성)를 클릭합니다.

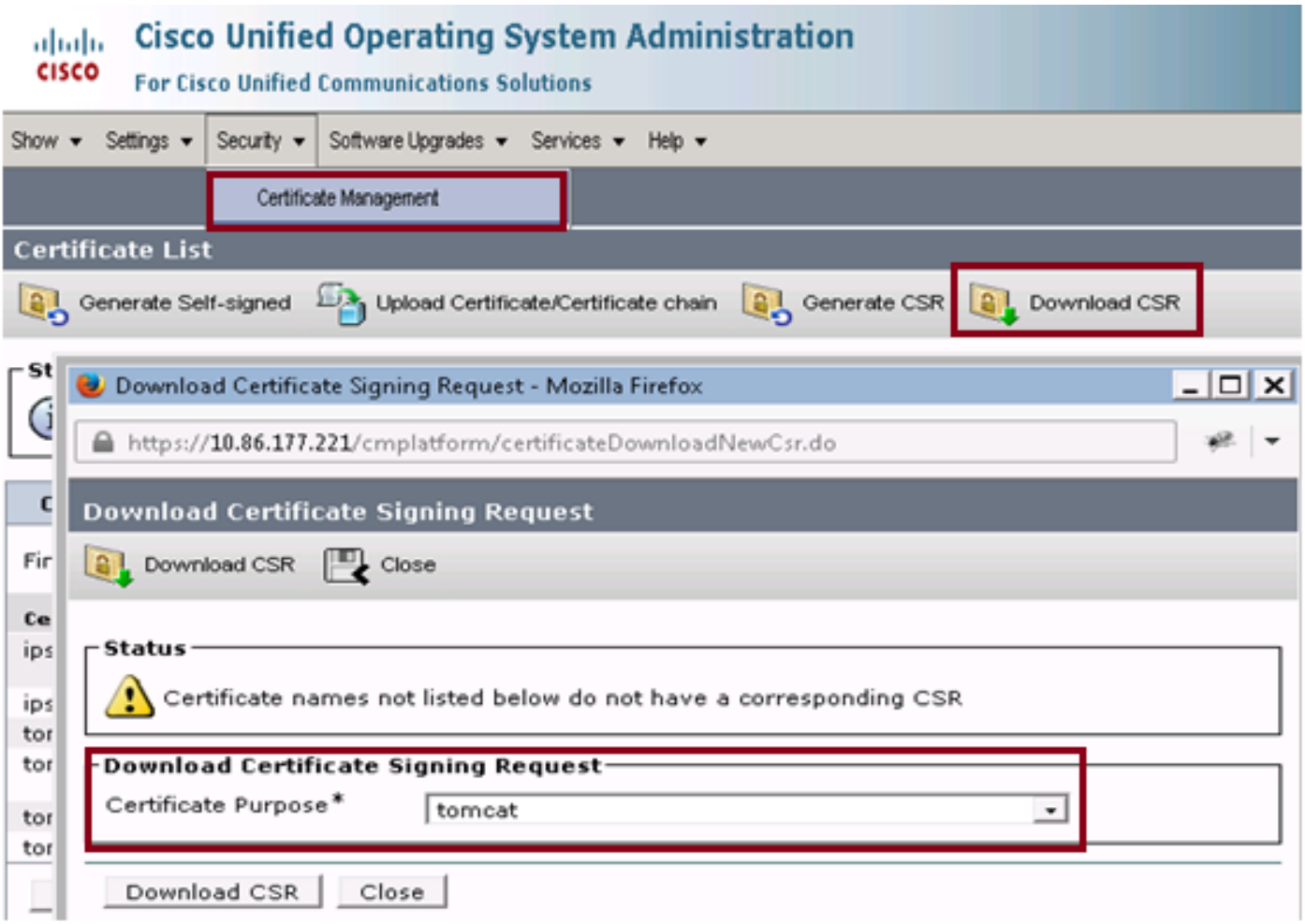


4. CSR 다운로드

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

b. Certificate Purpose*(인증서 용도*) 드롭다운 목록에서 tomcat을 선택합니다.

c. 이미지에 표시된 대로 Download CSR(CSR 다운로드)을 클릭합니다.



참고: CA용 CSR을 가져오려면 보조 서버/cmplatform의 URL https://hostname을 사용하여 보조 서버에서 다음 단계를 수행합니다.

CA에서 루트, 중간(해당되는 경우) 및 애플리케이션 인증서 얻기

1. VeriSign, Thawte, GeoTrust 등과 같은 타사 CA에 기본 및 보조 서버의 CSR 정보를 제공합니다.

2. CA에서 다음과 같은 기본 및 보조 서버에 대한 인증서 체인을 수신해야 합니다.

- Finesse 서버: 루트, 중간 및 애플리케이션 인증서
- CUIC 서버: 루트 및 애플리케이션 인증서

서버에 인증서 업로드

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

Finesse 서버

1. 기본 Finesse 서버 루트 인증서 업로드:

a. 기본 서버의 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.

b. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

2. 기본 Finesse 서버 중간 인증서 업로드:

a. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

b. 루트 인증서 필드에 이전 단계에서 업로드된 루트 인증서의 이름을 입력합니다. 루트/공용 인증서를 설치할 때 생성되는 .pem 파일입니다.

이 파일을 보려면 Certificate Management(인증서 관리) > Find(찾기)로 이동합니다. 인증서 목록에서 .pem 파일 이름이 tomcat-trust에 대해 나열됩니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 중간 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

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

---

3. 주 Finesse 서버 애플리케이션 인증서 업로드:

a. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat을 선택합니다.

b. Root Certificate(루트 인증서) 필드에 이전 단계에서 업로드된 중간 인증서의 이름을 입력합니다. .pem 확장명(예: TEST-SSL-CA.pem)을 포함합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 애플리케이션 인증서 파일을 찾아봅니다.

d. 파일 업로드를 클릭합니다.

4. 보조 Finesse 서버 루트 및 중간 인증서를 업로드합니다.

a. 인증서에 대한 보조 서버의 1단계와 2단계에서 설명한 것과 동일한 단계를 수행합니다.

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

---

5. 보조 Finesse 서버 애플리케이션 인증서 업로드:

a. 3단계에서 설명한 것과 동일한 단계를 따릅니다. 보조 서버에서는 자체 인증서를 사용합니다.

6. 서버를 다시 시작합니다.

a. 기본 및 보조 Finesse 서버에서 CLI에 액세스하고 utils system restart 명령을 실행하여 서버를 다시 시작합니다.

CUIC 서버

1. CUIC 기본 서버 루트(공용) 인증서를 업로드합니다.

a. 기본 서버의 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.

b. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

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

---

2. CUIC 주 서버 애플리케이션(주) 인증서를 업로드합니다.

a. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat을 선택합니다.

b. Root Certificate(루트 인증서) 필드에 이전 단계에서 업로드된 루트 인증서의 이름을 입력합니다.

루트/공용 인증서를 설치할 때 생성되는 .pem 파일입니다. 이 파일을 보려면 인증서 관리 > 찾기로 이동합니다.

인증서 목록에서 .pem 파일 이름이 tomcat-trust에 대해 나열됩니다. .pem 확장명을 포함합니다(예: TEST-SSL-CA.pem).

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

d. 파일 업로드를 클릭합니다.

3. CUIC 보조 서버 루트(공용) 인증서를 업로드합니다.

a. 보조 CUIC 서버에서 루트 인증서에 대해 1단계에서 설명한 것과 동일한 단계를 수행합니다.

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

---

4. CUIC 보조 서버 애플리케이션(기본) 인증서를 업로드합니다.

a. 2단계에서 설명한 것과 동일한 프로세스를 따릅니다. 보조 서버에서 자체 인증서를 찾습니다.

5. 서버를 다시 시작합니다.

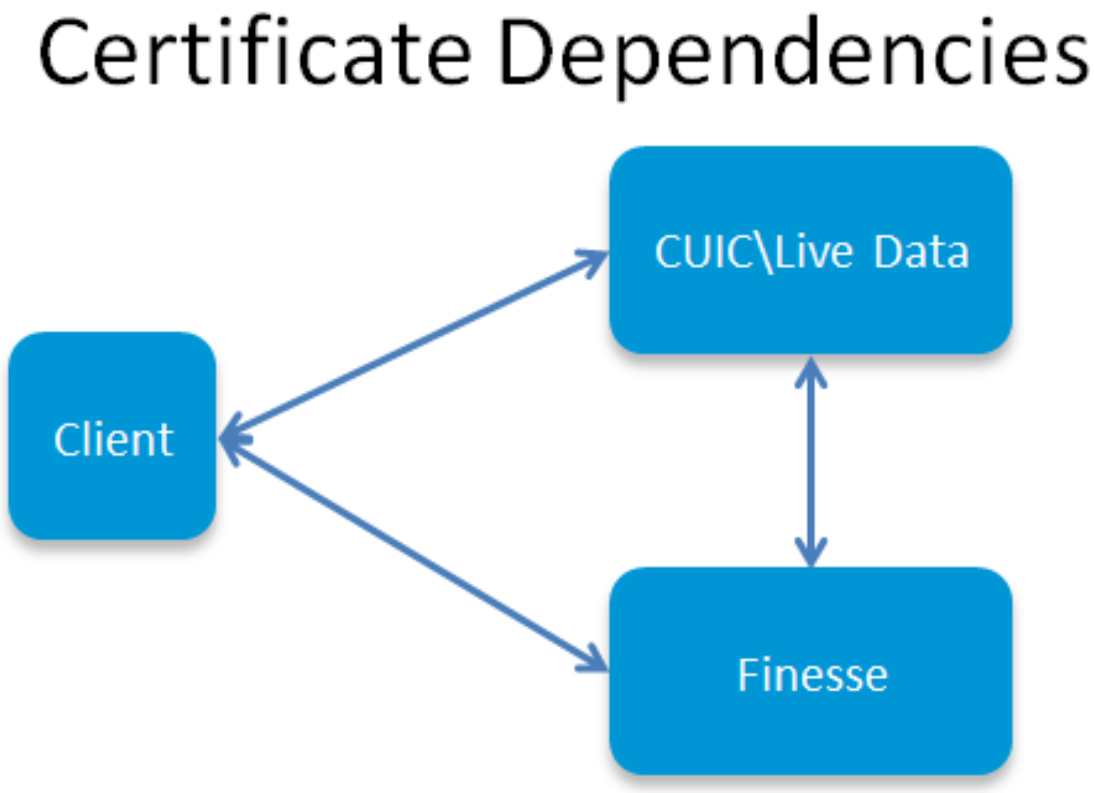
a. 기본 및 보조 CUIC 서버에서 CLI에 액세스하고 utils system restart 명령을 실행하여 서버를 재시작합니다.

참고: 인증서 예외 경고를 방지하려면 FQDN(정규화된 도메인 이름)을 사용하여 서버에 액세스해야 합니다.

인증서 종속성

Finesse 에이전트와 수퍼바이저는 보고용으로 CUIC 가젯을 활용하므로, 이러한 서버의 루트 인증서도 여기에 언급된 순서대로 업로드해야 이러한 서버 간의 HTTPS 통신을 위한 인증서 종속성을 유지할 수 있습니다.

- Finesse 주 서버에 CUIC 서버 루트 인증서 업로드
- CUIC 기본 서버에 Finesse 루트\중간 인증서 업로드



Finesse 주 서버에 CUIC 서버 루트 인증서 업로드

1. 기본 Finesse 서버에서 URL이 있는 Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지를 열고 설치 프로세스 시 생성된 OS 관리자 계정으로 로그인합니다.

https://hostname: 기본 Finesse 서버/cmplatform

2. 기본 CUIC 루트 인증서를 업로드합니다.

a. Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.

b. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

3. 보조 CUIC 루트 인증서 업로드

a. Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.

b. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

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

---

4. 기본 및 보조 Finesse 서버에서 CLI에 액세스하고 utils system restart 명령을 실행하여 서버를 재시작합니다.

CUIC 기본 서버에 Finesse 루트/중간 인증서 업로드

1. 기본 CUIC 서버에서 URL이 포함된 Cisco Unified Communications Operating System Administration 페이지를 열고 설치 프로세스 시 생성된 OS 관리자 계정으로 로그인합니다.

기본 CUIC 서버/cmplatform의 https://hostname

2. 기본 Finesse 루트 인증서 업로드:

a. Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드)로 이동합니다.

b. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 루트 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

3. 기본 Finesse 중간 인증서 업로드:

a. Certificate Purpose(인증서 용도) 드롭다운 목록에서 tomcat-trust를 선택합니다.

b. 루트 인증서 필드에 이전 단계에서 업로드된 루트 인증서의 이름을 입력합니다.

c. Upload File(파일 업로드) 필드에서 Browse(찾아보기)를 클릭하고 중간 인증서 파일을 찾습니다.

d. 파일 업로드를 클릭합니다.

4. 기본 Live Data 서버의 보조 Finesse 루트\중간 인증서에 대해 2단계와 3단계를 동일하게 수행합니다.

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

---

5. 기본 및 보조 CUIC 서버에서 CLI에 액세스하고 utils system restart 명령을 실행하여 서버를 재시작합니다.

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.