

UCS Central에 대한 서드파티 인증서 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[신뢰 지점 만들기](#)

[키링 및 CSR 생성](#)

[키링 적용](#)

[검증](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco UCS Central(Unified Computing System Central Software)에서 서드파티 인증서를 구성하는 모범 사례를 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco UCS Central
- CA(인증 기관)
- OpenSSL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

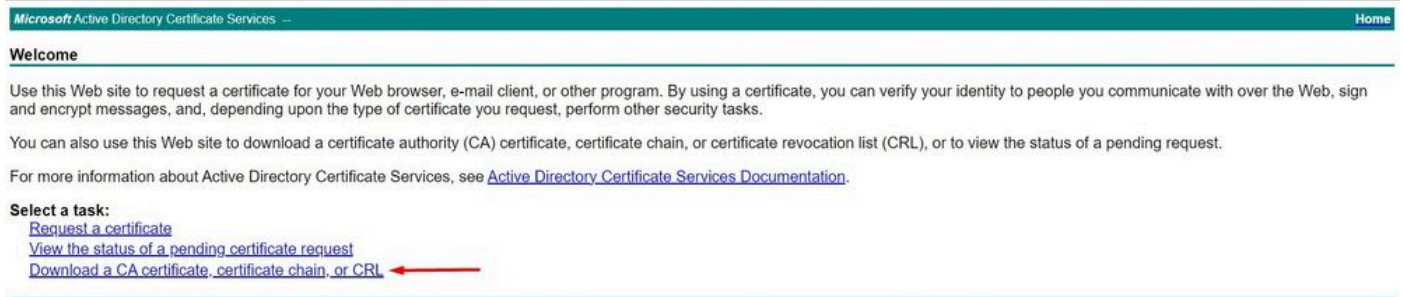
- UCS Central 2.0(1q)
- Microsoft Active Directory 인증서 서비스
- Windows 11 Pro N
- OpenSSL 3.1.0

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.

구성

인증 기관에서 인증서 체인을 다운로드합니다.

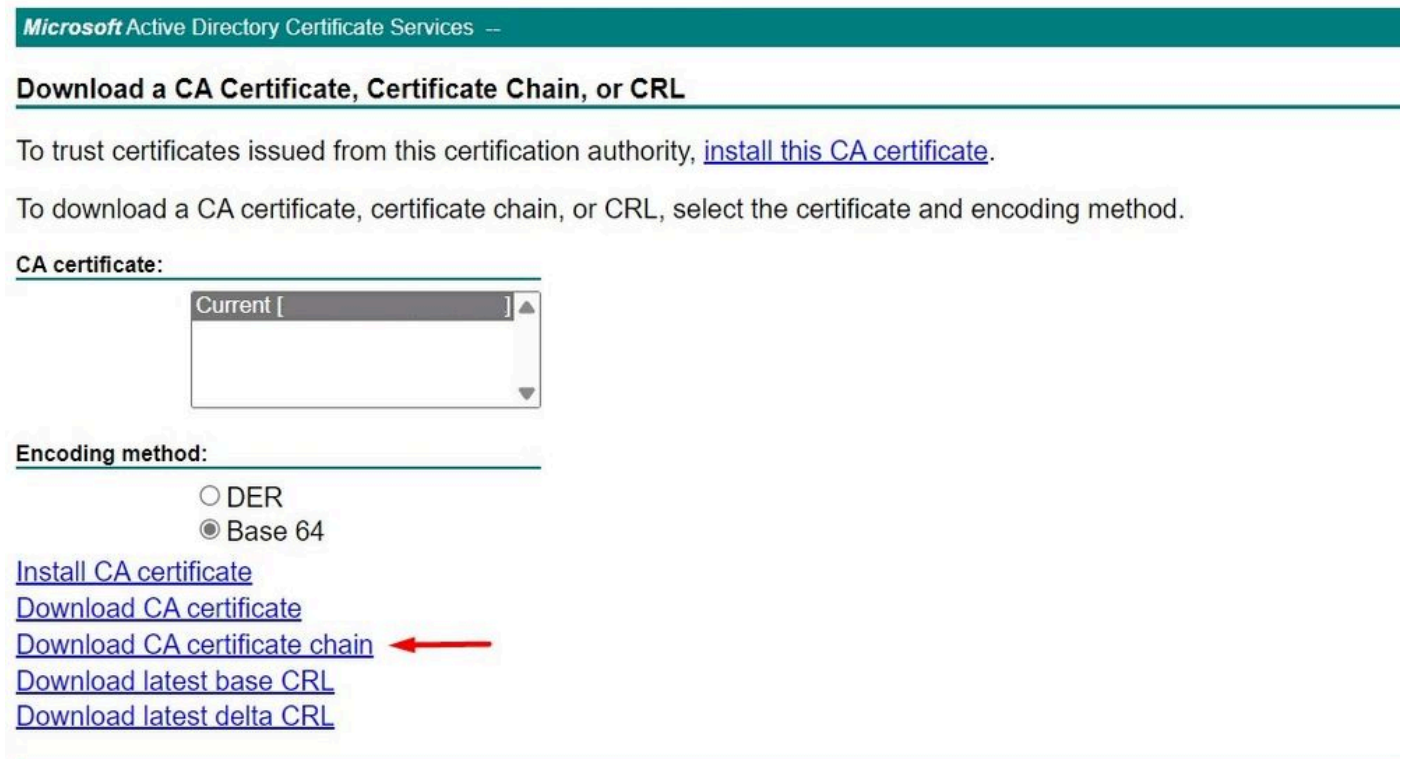
1. CA(Certificate Authority)에서 인증서 체인을 다운로드합니다.



The screenshot shows the 'Welcome' page of the Microsoft Active Directory Certificate Services website. The page includes a header with the site name and a 'Home' link. Below the header, there is a 'Welcome' section followed by instructions on how to use the site to request a certificate or download a CA certificate, certificate chain, or CRL. A 'Select a task:' section contains three links: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'. A red arrow points to the third link.

CA에서 인증서 체인 다운로드

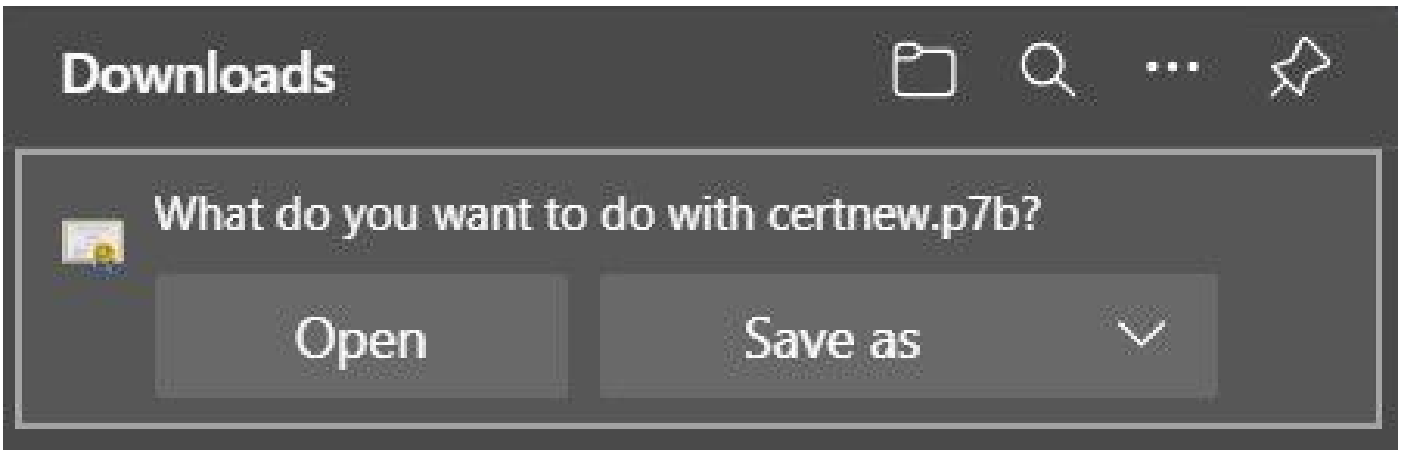
2. 인코딩을 Base 64로 설정하고 CA 인증서 체인을 다운로드합니다.



The screenshot shows the 'Download a CA Certificate, Certificate Chain, or CRL' page. It includes a header with the site name and a 'Home' link. Below the header, there is a 'Download a CA Certificate, Certificate Chain, or CRL' section followed by instructions on how to trust certificates issued from this certification authority and how to download a CA certificate, certificate chain, or CRL. A 'CA certificate:' section contains a dropdown menu with 'Current' selected. Below this, there is an 'Encoding method:' section with two radio buttons: 'DER' and 'Base 64'. The 'Base 64' radio button is selected. Below the encoding method section, there are five links: 'Install CA certificate', 'Download CA certificate', 'Download CA certificate chain', 'Download latest base CRL', and 'Download latest delta CRL'. A red arrow points to the 'Download CA certificate chain' link.

인코딩을 Base 64로 설정하고 CA 인증서 체인을 다운로드합니다

3. CA 인증서 체인은 PB7 형식입니다.




인증서가 PB7 형식입니다.

4. OpenSSL 툴을 사용하여 인증서를 PEM 형식으로 변환해야 합니다. Open SSL이 Windows에 설치되어 있는지 확인하려면 `openssl version` 명령을 사용합니다.

```
C:\Program Files\OpenSSL-Win64\bin>openssl version
OpenSSL 3.1.0 14 Mar 2023 (Library: OpenSSL 3.1.0 14 Mar 2023)
```

OpenSSL이 설치되어 있는지 확인

 참고: OpenSSL 설치 는 이 문서의 범위를 벗어납니다.

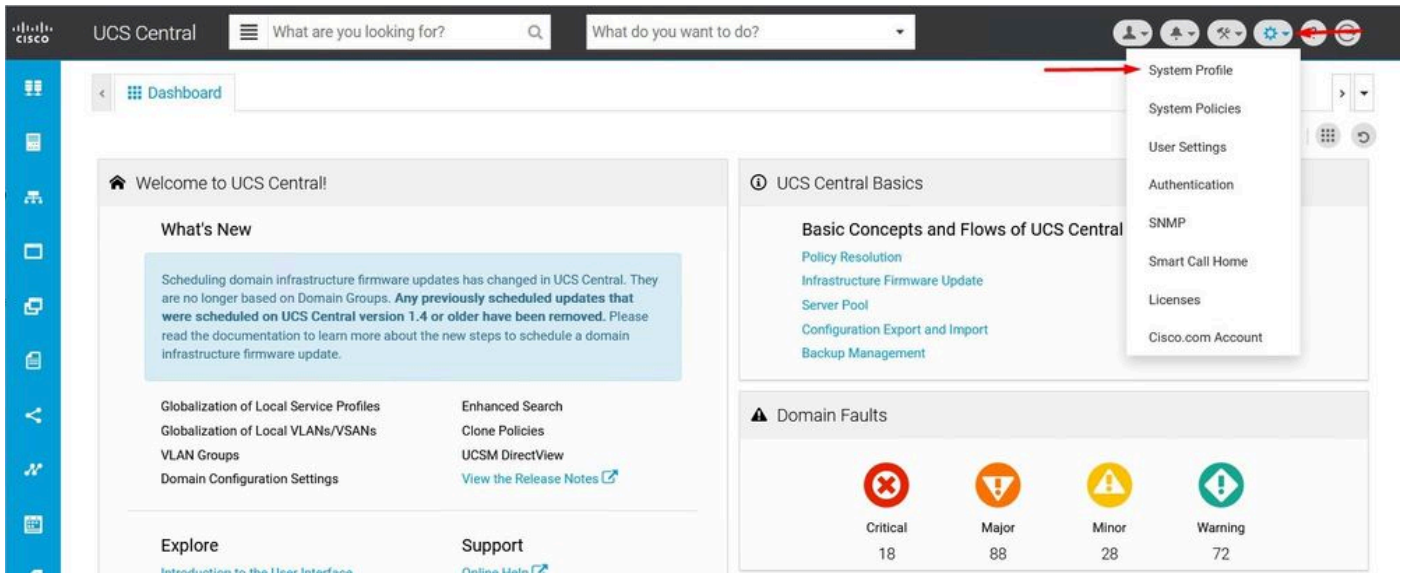
5. OpenSSL이 설치된 경우 `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` 명령을 실행하여 변환을 수행합니다. 인증서가 저장된 경로를 사용해야 합니다.

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs7 -print_certs -in C://Users/ /Desktop/certnew.p7b -out C://Users/ /Desktop/certnew.pem
```

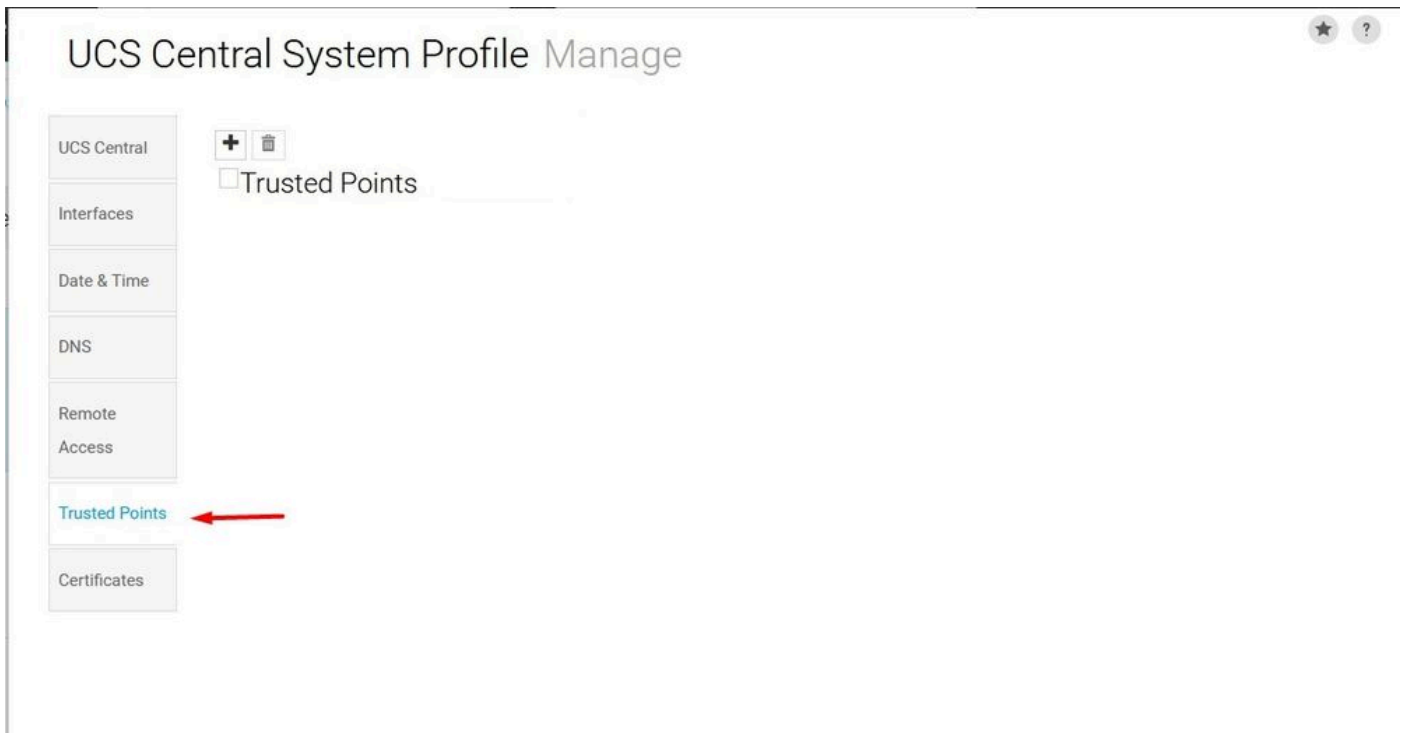
P7B 인증서를 PEM 형식으로 변환

신뢰 지점 만들기

1. 시스템 구성 아이콘 > 시스템 프로파일 > 신뢰 지점을 클릭합니다.



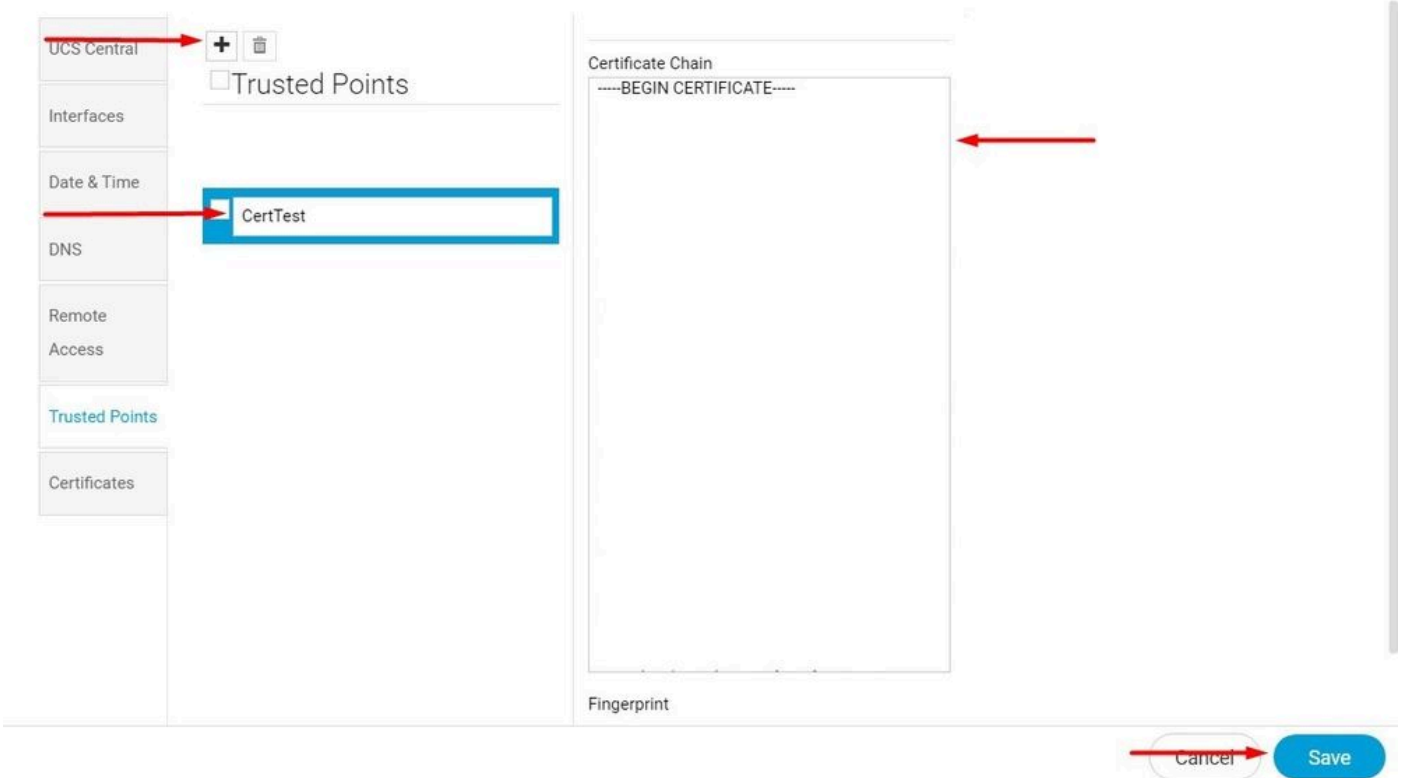
UCS Central 시스템



프로필 UCS Central 신뢰 지점

2. +(더하기) 아이콘을 클릭하여 새 신뢰 지점을 추가합니다. PEM 인증서의 내용에 이름을 쓰고 붙여넣습니다. Save(저장)를 클릭하여 변경 사항을 적용합니다.

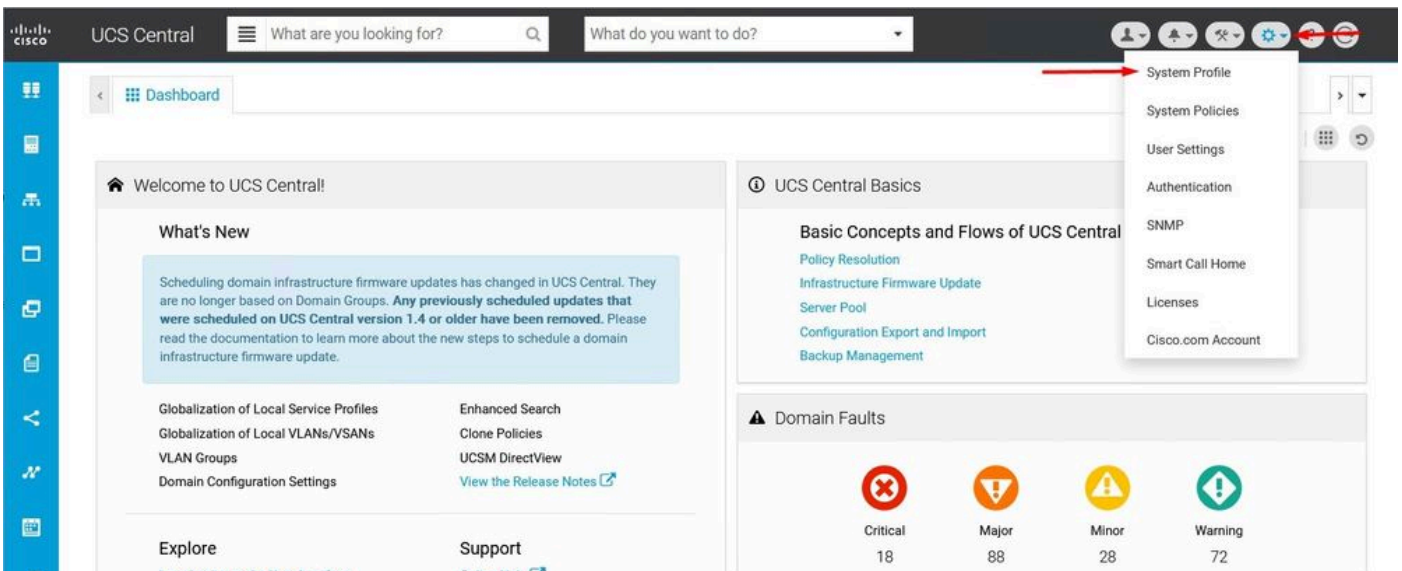
UCS Central System Profile Manage



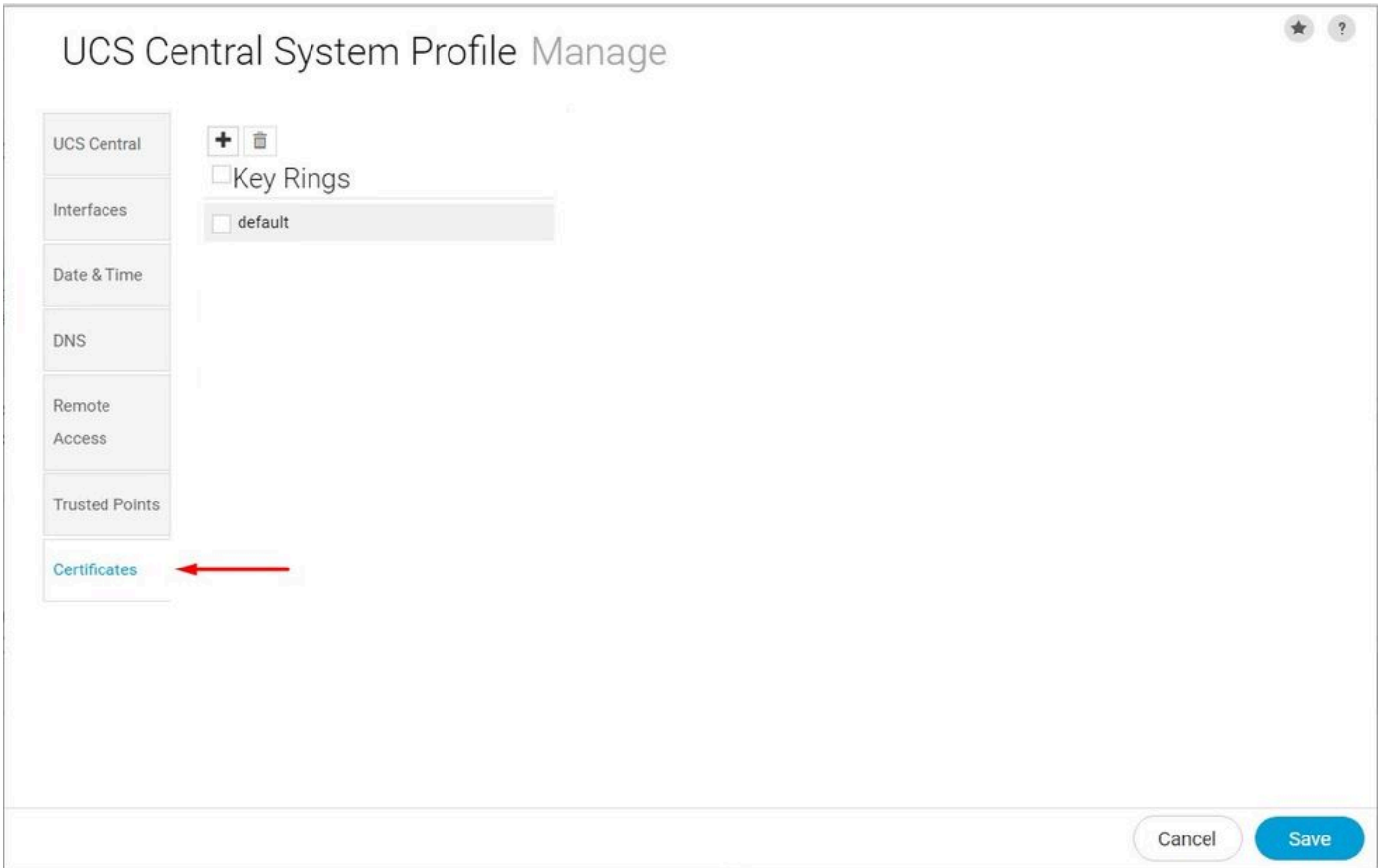
인증서 체인 복사

키링 및 CSR 생성

1. 시스템 구성 아이콘 > 시스템 프로파일 > 인증서를 클릭합니다.



UCS Central 시스템



프로파일 UCS Central 인증서

2. 더하기 아이콘을 클릭하여 새 키 링을 추가합니다. 이름을 쓰고 모듈러스를 기본값으로 유지하고 (또는 필요한 경우 수정) 이전에 생성한 신뢰 지점을 선택합니다. 이러한 매개변수를 설정한 후 Certificate Request(인증서 요청)로 이동합니다.

UCS Central System Profile Manage



UCS Central

- Interfaces
- Date & Time
- DNS
- Remote Access
- Trusted Points
- Certificates

Key Rings

- default
- KeyRingTest**

Basic | Certificate Request

Modulus: mod2048

Trusted Point: CertTest

Certificate Status: Valid

Certificate Chain

Cancel Save

새 키 링 만들기

3. 필요한 값을 입력하여 인증서를 요청하고 저장을 클릭합니다.

UCS Central System Profile Manage



UCS Central

- Interfaces
- Date & Time
- DNS
- Remote Access
- Trusted Points
- Certificates

Key Rings

- default
- KeyRingTest**

Basic | Certificate Request

DNS

Locality

State

Country

Organization Name

Organization Unit Name

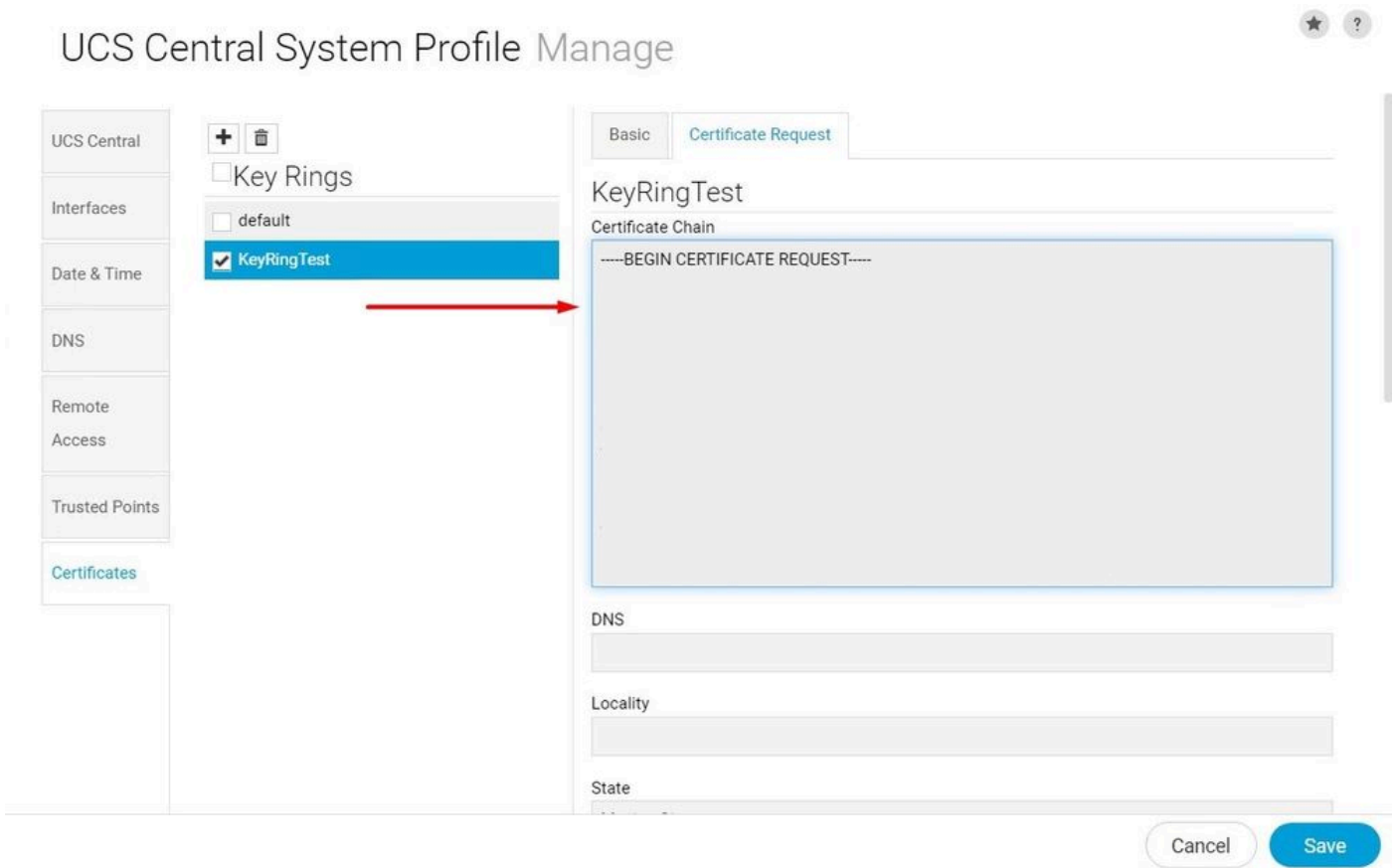
Email

Subject

Cancel Save

인증서를 생성하려면 세부 정보를 입력합니다.

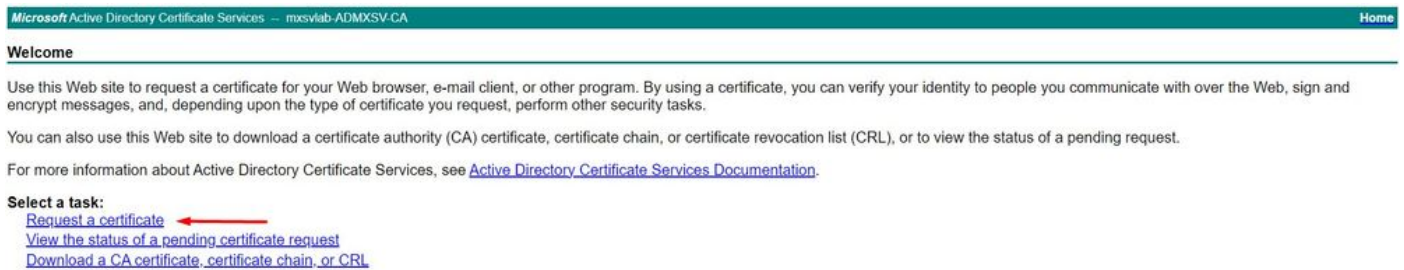
4. 생성된 키 링으로 돌아가서 생성된 인증서를 복사합니다.



The screenshot shows the 'UCS Central System Profile Manage' interface. On the left, a sidebar lists various system settings: UCS Central, Interfaces, Date & Time, DNS, Remote Access, Trusted Points, and Certificates. Under 'Certificates', there are two options: 'Key Rings' (unchecked) and 'KeyRingTest' (checked). A red arrow points from the 'KeyRingTest' option to the main content area. The main content area has two tabs: 'Basic' and 'Certificate Request'. The 'Certificate Request' tab is active, showing a 'Certificate Chain' section with a text area containing '-----BEGIN CERTIFICATE REQUEST-----'. Below this are input fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.

생성된 인증서 복사


5. CA로 이동하여 인증서를 요청합니다.



The screenshot shows the Microsoft Active Directory Certificate Services website. The header includes 'Microsoft Active Directory Certificate Services - mxslab-ADMXSV-CA' and a 'Home' link. Below the header is a 'Welcome' section with the following text: 'Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).' Below this is a 'Select a task:' section with three links: 'Request a certificate' (with a red arrow pointing to it), 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

CA에서 인증서 요청

6. UCS Central에서 생성된 인증서를 붙여넣고 CA에서 웹 서버 및 클라이언트 템플릿을 선택합니다. 인증서를 생성하려면 Submit(제출)을 클릭합니다.

 **참고:** Cisco UCS Central에서 인증서 요청을 생성할 때 결과 인증서에 SSL 클라이언트 및 서버 인증 키 사용이 포함되어 있는지 확인하십시오. Microsoft Windows Enterprise CA를 사용하는 경우 컴퓨터 템플릿을 활용하거나, 컴퓨터 템플릿을 사용할 수 없는 경우 두 가지 키 사용이 모두 포함된 다른 적절한 템플릿을 활용하십시오.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

-----END CERTIFICATE REQUEST-----

Certificate Template:

Web Server and Client

Additional Attributes:

Attributes:

Submit >

생성된 키 링에 사용할 인증서 생성

7. openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem 명령을 사용하여 새 인증서를 PEM으로 변환합니다.

8. PEM 인증서의 내용을 복사하고 생성된 키 링으로 이동하여 내용을 붙여넣습니다. 생성한 신뢰 지점을 선택하고 컨피그레이션을 저장합니다.

UCS Central System Profile Manage

UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+ -

Key Rings

default

KeyRingTest

Basic Certificate Request

KeyRingTest

Modulus

mod2048

Trusted Point

CertTest

Certificate Status

Empty Cert

Certificate Chain

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

Cancel Save

키 링에서 요청한 인증서를 붙여넣습니다.

키 링 적용

1. System Profile(시스템 프로파일) > Remote Access(원격 액세스) > Keyring(키링)으로 이동하고, 생성된 키 링을 선택한 후 Save(저장)를 클릭합니다. UCS Central에서 현재 세션을 닫습니다.

UCS Central System Profile Manage



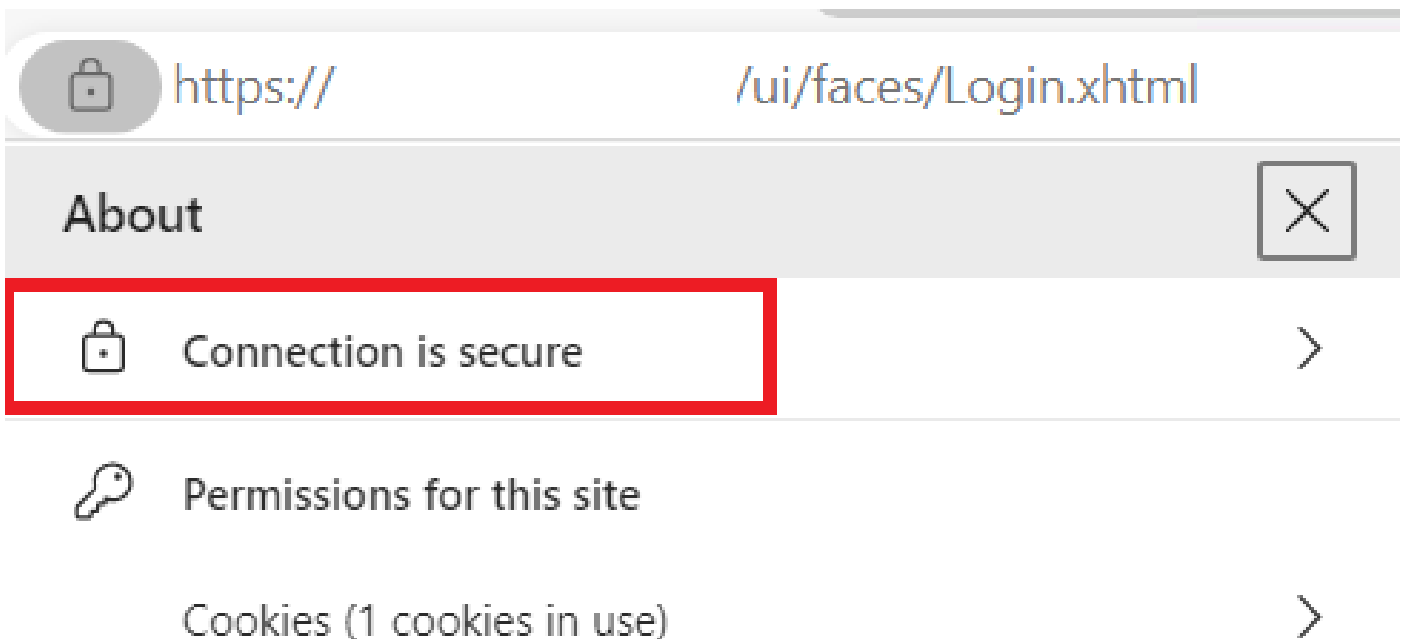
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Cancel Save

생성된 키 링 선택

검증

1. UCS Central에 액세스할 수 있을 때까지 기다렸다가 https:// 옆의 잠금을 클릭합니다. 사이트가 안전합니다.



UCS Central은

문제 해결

생성된 인증서에 SSL 클라이언트 및 서버 인증 키 사용이 포함되는지 확인합니다.

CA에 요청한 인증서에 SSL 클라이언트 및 서버 인증 키가 포함되지 않은 경우 "Invalid certificate(유효하지 않은 인증서)"라는 오류가 사용됩니다. 이 인증서를 TLS 서버 인증에 사용할 수 없습니다. "key usage extensions 확인"이 나타납니다.

Invalid certificate: This certificate cannot be used for TLS server authentication, check key usage extensions.

TLS 서버 권한 부여 키에 대한 오류

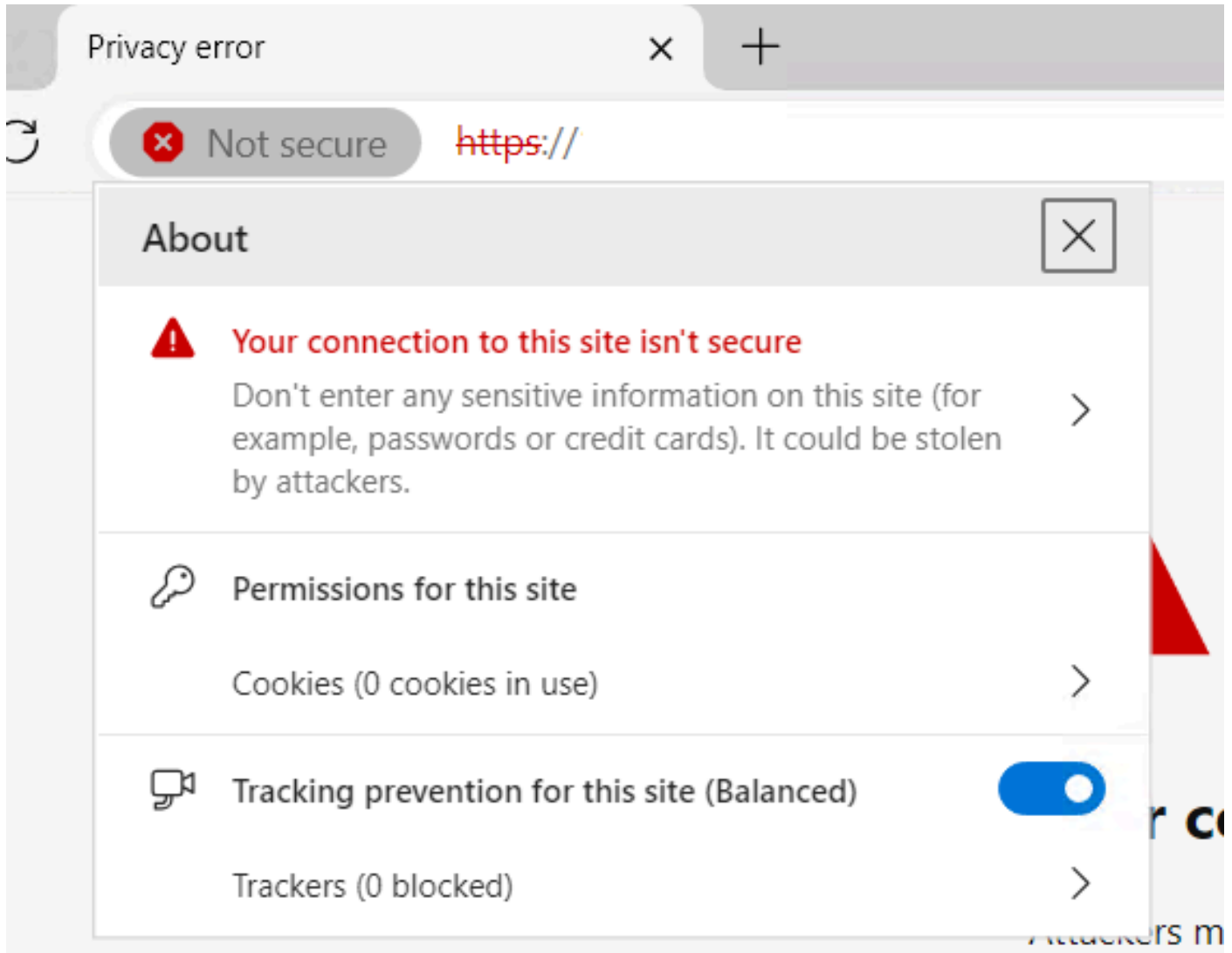
CA에서 선택한 템플릿에서 만든 PEM 형식의 인증서에 올바른 서버 인증 키 사용이 있는지 확인하려면 `openssl x509 -in <my_cert>.pem -text -noout` 명령을 사용할 수 있습니다. Extended Key Usage(확장 키 사용) 섹션 아래에 웹 서버 인증 및 웹 클라이언트 인증이 있어야 합니다.

```
21:75
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Alternative Name: critical
        DNS:
    X509v3 Subject Key Identifier:
    X509v3 Authority Key Identifier:
    X509v3 CRL Distribution Points:
        Full Name:
    Authority Information Access:
```

요청된 인증서의 웹 서버 및 웹 클라이언트 권한 부여 키

UCS Central은 여전히 안전하지 않은 사이트로 플래그 지정되어 있습니다.

서드파티 인증서를 구성한 후에도 여전히 브라우저에 연결이 플래그됩니다.



UCS Central은 여전히 안전하지 않은 사이트입니다.

인증서가 올바르게 적용되고 있는지 확인하려면 디바이스에서 인증 기관을 신뢰하는지 확인하십시오.

관련 정보

- [Cisco UCS Central 관리 가이드, 릴리스 2.0](#)
- [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.