# ESA 및 SMA 관리를 위한 SAML SSO 외부 인증 구성

## 목차



## 소개

이 문서에서는 ESA 및 SMA 시스템 관리를 위해 SAML 2.0 SSO 외부 인증을 구성하는 방법에 대해 설명합니다.

### 환경

- 제품: ESA(Email Security Appliance), SMA(Security Management Appliance)
- 적용 대상: ESA 및 SMA 시스템 관리
- 클러스터 동작: SP(서비스 공급자) 및 IdP 프로필은 시스템 레벨에서 구성됩니다. 외부 인증 매핑은 클러스터 레벨에서 구성됩니다.

## 사전 요구 사항

- ESA/SMA 웹 인터페이스에 대한 관리 액세스
- PKCS #12(PFX) 또는 PEM 형식(자체 서명 또는 CA 서명)으로 사용할 수 있는 X.509 인증서

및 개인 키
- 서드파티 IdP(Identity Provider) 애플리케이션 및 해당 SAML 메타데이터/SSO URL에 액세스

### 사전 구성 체크리스트

- 관리자가 어플라이언스에 액세스하기 위해 사용하는 관리 인터페이스 호스트 이름/FQDN을 확인합니다. ACS(Assertion Consumer Service) URL이 해당 호스트 이름과 일치하는지 확인합니다.
- 어플라이언스가 클러스터에 있는 경우 SAML 외부 인증을 활성화하기 전에 시스템 레벨에서 각 멤버에 대해 SAML을 구성할 계획입니다.
- IdP에 어플라이언스별로 별도의 애플리케이션 또는 영역이 필요한지 여부를 결정합니다.
- 필요한 인증서와 키를 사용할 수 있는지 확인합니다.
- IdP가 ESA/SMA 역할 매핑에 필요한 그룹 또는 역할 특성을 전송하는지 확인합니다.

---

주의: 이 문서는 EUQ(End User Quarantine) SAML SSO에는 적용되지 않습니다.

---

## 배경 정보

- Cisco TAC에서는 타사 IdP 컨피그레이션에 대한 기술 지원을 제공하지 않습니다. 일반적인 IdP에 대한 샘플 컨피그레이션 참조가 제공됩니다.

SSO SAML IdP

- Duo DAG(Access Gateway)는 2단계 인증을 추가하여 SAML 2.0 페더레이션을 사용하는 인기 있는 클라우드 서비스를 완성합니다.
- ADFS(Active Directory Federation Services) - ADFS 2,3,4, Azure AD(Azure Active Directory), SecureAUTH 및 PingFederate에서 테스트됨
- SAML 2.0 Single Sign-On 프레임워크 내에서 IdP가 지원하는 경우 추가 2단계 인증을 사용할 수 있습니다.
- Okta는 서비스를 지원하는 IdP를 사용한 인증을 지원합니다.

### ESA/SMA를 서비스 공급자로 구성

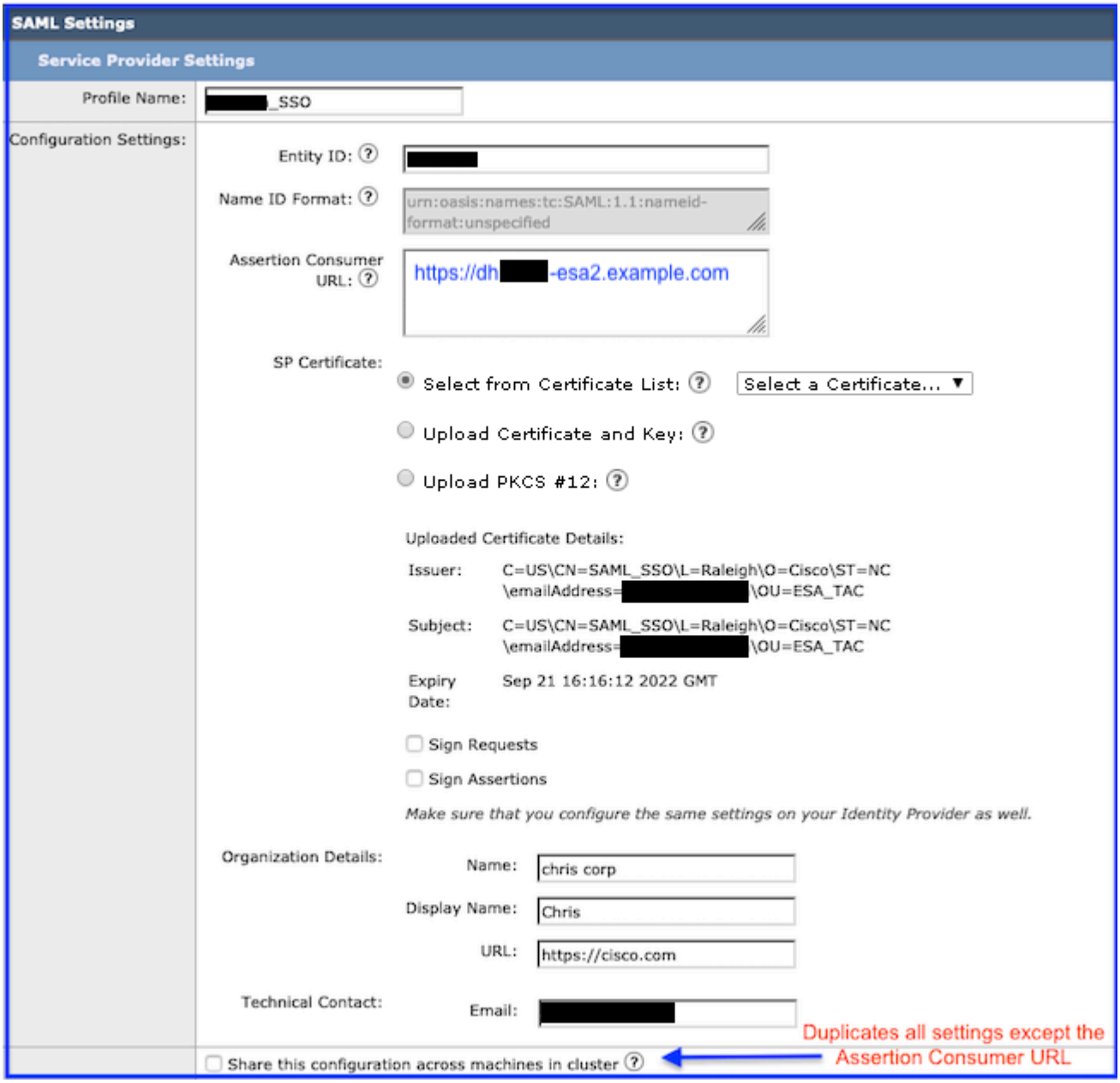
System Administration(시스템 관리) > SAML > (Machine Level) > Add Service Provider(서비스 공

급자 추가)로 이동합니다.

참고: SAML을 활성화하려면 클러스터의 모든 멤버에 대해 시스템 레벨 컨피그레이션이 필요합니다.

- 페이지 하단의 Share this configuration across machines in the cluster(클러스터에 있는 시스템 간에 이 컨피그레이션 공유) 옵션을 선택한 경우 다음 조건이 적용됩니다.
  - 모든 필드는 Assertion Consumer URL을 제외한 클러스터 멤버에 복제됩니다.
  - Assertion Consumer URL은 관리 인터페이스의 호스트 이름을 ACS로 자동 채웁니다.
  - 대체 호스트 이름을 사용하여 호스트에 액세스하는 환경에서는 각 호스트에 대해 수동 컨피그레이션이 필요합니다(예: CES 호스팅 어플라이언스).
  - 프로필 이름: ESA 또는 SMA 인터페이스에서 SP 인스턴스의 레이블을 지정하는 데 사용되는 이름입니다.
  - 엔터티 ID: IdP에서 볼 때 SP 인스턴스에 사용되는 이름입니다. 이 이름은 IdP에서 SP를 나타내는 데 사용하는 레이블입니다. ESA_SP 또는 ESA_SSO와 같은 모든 이름을 사용할 수 있습니다.
  - 이름 ID 형식: 구성할 수 없는 필드.
  - Assertion Consumer URL 또는 Assertion Consumer Service(ACS): IdP가 이 ESA/SMA 호스트와 통신하는 데 사용하는 URL입니다.
  - SP 인증서:
    - 형식: PFX/PKCS12 또는 PEM 형식의 X.509 공용/사설 인증서
    - 옵션 1: 인증서 목록에서 선택: Network(네트워크) > Certificates(인증서)의 ESA에 이미 생성된 인증서 중에서 선택합니다.
    - 옵션 2: 인증서 및 키 업로드: PEM 형식의 인증서와 키를 업로드합니다.
    - 옵션 3: PKCS #12 업로드: PKCS #12 파일을 업로드합니다.
    - 선택 사항: SAML Single Sign-On용 ESA/SMA에 자체 서명 인증서를 생성합니다.
    - 필요한 경우 개인 키를 암호로 보호합니다.

참고: PEM 형식의 인증서를 사용하는 경우 각 인증서와 개인 키를 별도의 파일에 보관합니다.




서비스 공급자 설정 페이지

서비스 공급자 설정 페이지

- 서명 요청: IdP로 전송된 ESA/SMA SAML 통신에 서명하는 옵션입니다.
- 어설션 서명: ESA/SMA에 전송된 어설션에 IdP가 서명하도록 요구하는 옵션입니다.
- 조직 세부사항: 적절한 회사 데이터로 채울 수 있습니다.
- 설정을 유지하기 위해 변경 내용을 제출하고 커밋합니다.
- SAML 구성 페이지에서 SP 메타데이터를 다운로드합니다.

## ESA/SMA 어플라이언스와 작동하도록 IdP(Identity Provider)를 구성합니다

참고: 일부 IdP에는 각 ESA에 대해 별도의 애플리케이션 또는 영역이 필요합니다(예: DUO)

이러한 링크는 게시 시점에 여러 IdP에 대한 샘플 컨피그레이션을 제공합니다.
Cisco TAC는 타사 제품에 대한 기술 지원을 제공하지 않습니다. 이러한 예는 참조로 제공됩니다.

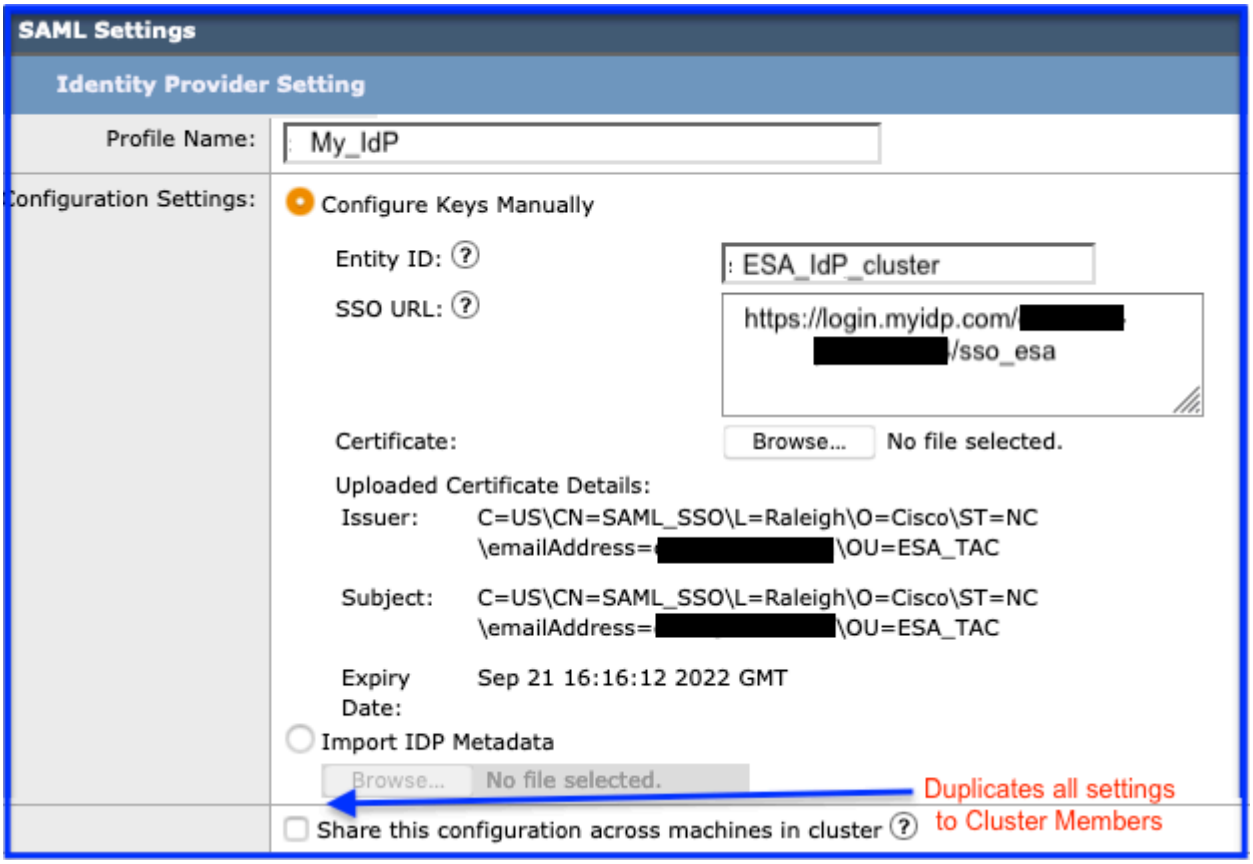
## ESA/SMA에서 IDP 설정 구성

1. 시스템 관리 > SAML로 이동합니다.

2. ID 제공자 추가를 선택합니다.

- 두 가지 옵션을 사용할 수 있습니다.
- IdP 메타데이터 가져오기
- 수동으로 키 구성:
  - 엔터티 ID: IdP를 식별하는 데 사용되는 모든 값 가능
  - SSO URL: SP에서 SAML 인증 요청을 보내는 URL
  - 개인 키 및 공용 인증서를 별도의 파일로 업로드

3. 클러스터의 모든 ESA에서 컨피그레이션을 복제하려면 클러스터의 여러 시스템에서 이 컨피그레이션을 공유합니다.

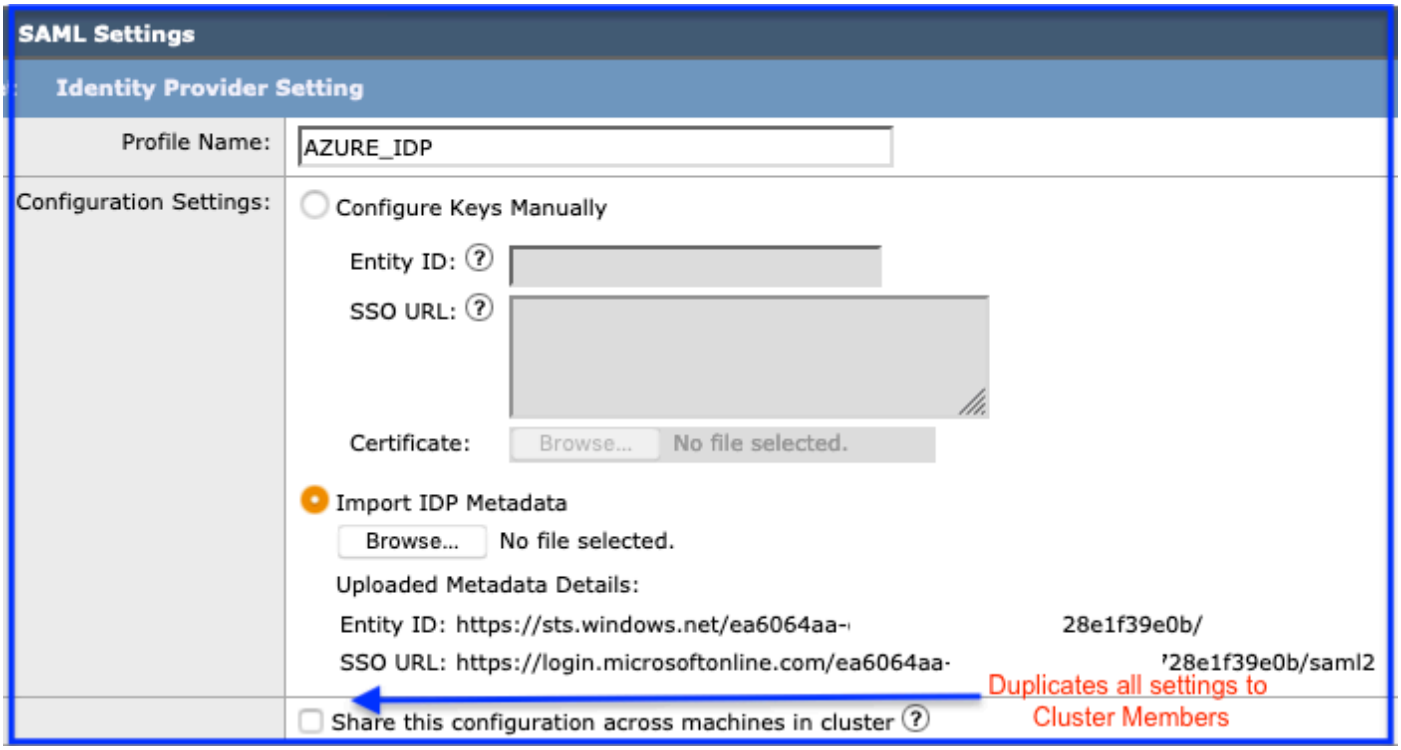



IdP 내용 수동 입력

IdP 내용 수동 입력

4. IdP에서 메타데이터 업로드

- Import IdP Metadata를 선택합니다.
- IdP에서 저장된 메타데이터 파일을 찾아 컨피그레이션을 저장합니다.
- 구축에 적용할 경우 클러스터의 여러 시스템에서 이 컨피그레이션을 공유하는 옵션을 사용할 수 있습니다.




Idp에서 메타데이터 업로드

Idp에서 메타데이터 업로드

## ESA/SMA에서 SAML을 사용하여 외부 인증 활성화

LDAP 외부 인증과 마찬가지로 SAML Single Sign-On에서는 그룹을 관리 역할에 할당하기 위한 매핑이 필요합니다.

1. System Administration > Users (Cluster Level) > External Authentication > Enable로 이동합니다.

2. 인증 유형 선택: SAML.

3. 이름맵과 대응하기 위한 속성명(선택사항): 그룹 매핑에서 검색할 속성 이름을 입력합니다.

---

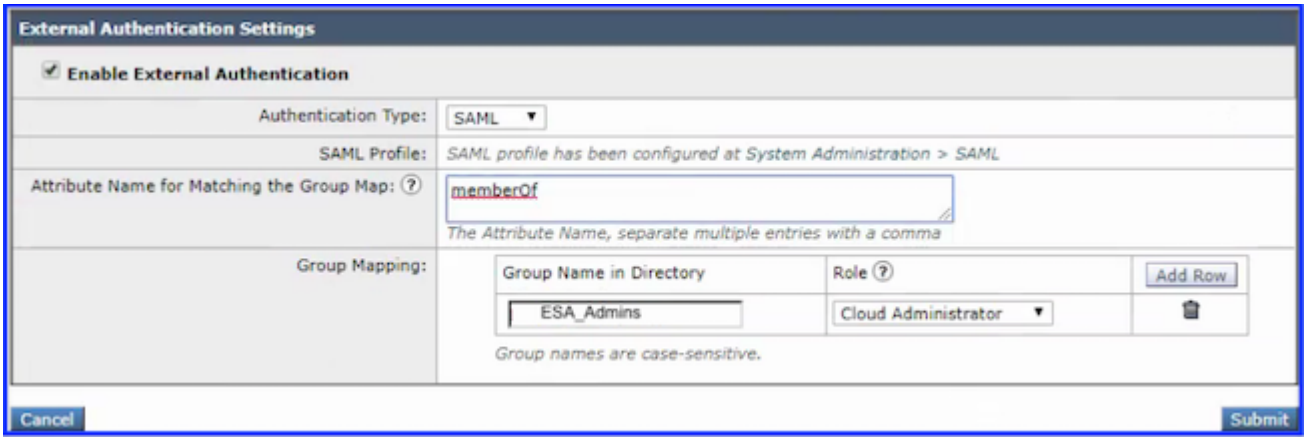
✎ 참고: 특성 이름은 ID 제공자가 SAML 응답에서 릴레이하도록 구성된 특성에 따라 달라집니다

---

. 어플라이언스는 Group Mapping(그룹 매핑) 필드에 구성된 특성에 대해 SAML 응답에서 지정된 특성 이름의 일치 항목을 검색합니다. 이 필드가 구성되지 않은 경우 어플라이언스는 구성된 Group Mapping(그룹 매핑) 필드에 대해 SAML 응답에 있는 모든 특성을 검색합니다.

4. 사전 정의 또는 사용자 지정 사용자 역할에 따라 SAML 디렉토리에 정의된 대로 그룹 이름 속성을 입력합니다.

- Group Mapping 필드는 그룹 특성을 포함해야 합니다. Unspecified Groups 특성을 추가하여 SAML 어설션 또는 응답을 인증할 수 있습니다.




외부 인증 설정

외부 인증 설정

5. 변경사항을 제출 및 커밋합니다.

컨피그레이션이 완료되면 로그온 페이지 하단에 새 링크가 표시됩니다. ESA/SMA 로그온 페이지에는 관리자를 기업 IDP(Identity Provider)로 리디렉션하는 Use Single Sign-On 링크가 표시됩니다.

이 옵션을 선택하면 관리자가 회사 SAML 로그온 페이지로 리디렉션됩니다.


Use Single Sign-On(단일 로그인 링크 사용)은 SAML로 리디렉션됩니다.

SAML에 Single Sign-On 링크 리디렉션 사용

# 문제 해결

이 지표를 사용하여 문제가 어플라이언스 컨피그레이션과 관련되는지 또는 IdP 컨피그레이션과 관련되는지 확인합니다.

## SSO 리디렉션 링크가 로그인 페이지에 표시되지 않음("Use Single Sign-On")

System Administration(시스템 관리) > Users(사용자) > External Authentication(외부 인증) > SAML이 구성되어 있는지 확인합니다.

## "Single Sign-On Authentication Failed!(단일 로그인 인증 실패!)"가 포함된 ESA/SMA 로그인 페이지로 리디렉션 관리자에게 문의하십시오."

오류: "단일 로그인 인증에 실패했습니다. 관리자에게 문의하십시오."

- IdP에서 인증에 실패했습니다.
  - 이는 컨피그레이션이 SSO(Single Sign-On) 인증 페이지에 도달하고 자격 증명을 제출하는 지점까지 작동하고 있음을 나타냅니다.
  - 이 실패는 IdP 컨피그레이션 때문인 경우가 많으며 IdP 설정을 추가로 확인해야 합니다.

## "Authorization Failure!(권한 부여 실패!)"가 포함된 ESA/SMA 로그인 페이지로 리디렉션됩니다. 관리자에게 문의하십시오."

오류: "권한 부여 실패! 관리자에게 문의하십시오."

- 인증이 통과되었지만 ESA/SMA에서 권한 부여가 실패했습니다.
  - Users(사용자) > External Authentication(외부 인증) > SAML 내의 설정에 초점을 맞춥니다.
    - 특성 이름, 그룹 이름, 그룹 매핑.

## 관련 정보

- Cisco Email Security Appliance - 사용자 가이드
- Cisco Content Security Management Appliance - 사용 설명서
- Cisco Web Security - 사용 설명서

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.