ESA 및 SMA용 AD FS를 사용하여 SAML SSO 외부 인증 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

SAML에 대한 ADFS IDP 컨피그레이션 단계

신뢰 당사자 Trust 구성

- 방법 A: SP 메타데이터를 가져와 당사자 Trust 생성
- 당사자 트러스트 엔드포인트 구성(클러스터만 해당)
- 발급 변환 규칙 - 클레임
- IdP 메타데이터 다운로드 및 ESA에 업로드

다음을 확인합니다.

관련 정보

소개

이 문서에서는 Active Directory Federation Services를 Cisco ESA 및 SMA의 외부 인증을 위한 SAML ID 공급자로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서에서는 엔지니어가 볼 수 없는 서드파티 애플리케이션의 보기를 제공합니다.

- Cisco ESA(Email Security Appliance) 및 SMA(Security Management Appliance) 최신 버전용 AD FS(Active Directory Federation Services) 2012 및 2016을 사용한 SAML(Security Assertion Markup Language) 외부 인증을 위한 구성 단계.
- 특수 구축별 컨피그레이션을 포함하지 않는 기본 랩 기반 단계.
- 프로덕션 구축과 다를 수 있는 랩 환경의 작동 예

⚠ 주의: 이 절차 전에 서비스 공급자(SP) 구성을 완료합니다. 을/를 참조하십시오.

요구 사항

- Microsoft AD FS(Active Directory Federation Services) 2012 또는 2016
- Cisco ESA(Email Security Appliance) 및 SMA(Security Management Appliance) 최신 버전

사용되는 구성 요소

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.

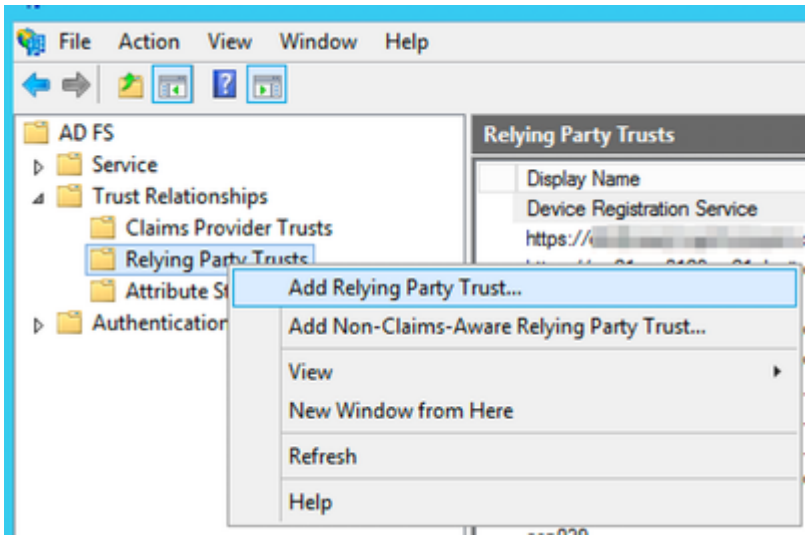
SAML에 대한 ADFS IDP 컨피그레이션 단계

신뢰 당사자 Trust 구성

AD FS에서 신뢰 당사자 트러스트를 만들려면 두 가지 옵션 중 하나를 사용합니다.

방법 A: SP 메타데이터를 가져와 당사자 Trust 생성

1. 관리 도구에서 AD FS 관리 콘솔을 엽니다.
2. AD FS 관리 콘솔에서 Trusted Relationships를 확장하고 Relying Party Trust를 마우스 오른쪽 단추로 클릭한 다음 Add Relying Party Trust를 선택합니다.



신뢰 당사자 Trust 추가

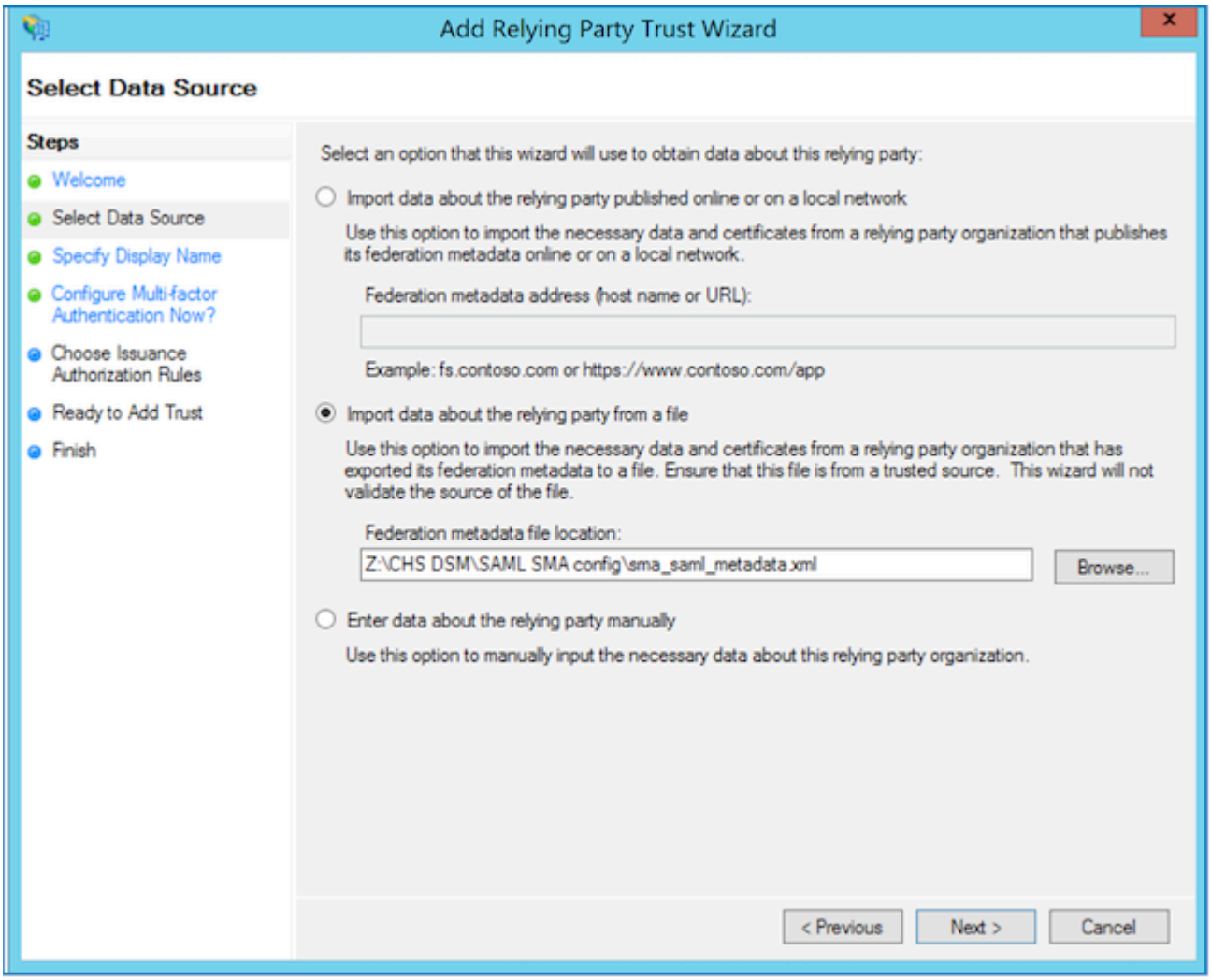
팁: Microsoft 신뢰 당사자 트러스트

다음 두 가지 옵션 중 하나를 사용하여 계속 진행합니다.

- 옵션 A: 파일에서 당사자 데이터를 가져옵니다. ESA 또는 SMA SP(서비스 공급자) metadata.xml 파일을 업로드합니다.
- 옵션 B: 신뢰 당사자에 대한 데이터를 수동으로 입력합니다. 이 옵션은 수동 컨피그레이션을 안내합니다.

옵션 A: 파일에서 당사자 데이터를 가져옵니다. ESA 또는 SMA SP(서비스 공급자) metadata.xml 파일을 업로드합니다.

1. 파일에서 신뢰 당사자에 대한 데이터를 가져오는 옵션을 선택하고 다음을 선택합니다.



ESA/SMA 메타데이터 파일 가져오기

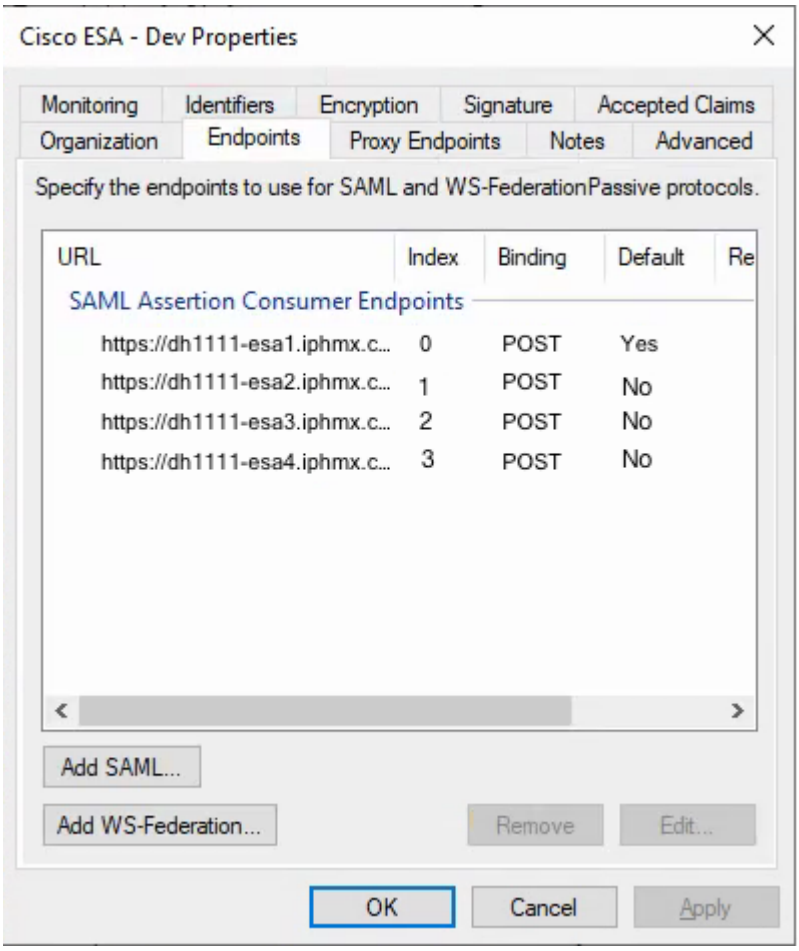
- 이 신뢰 당사자 트러스트를 식별할 표시 이름을 지정한 후 다음을 두 번 선택하십시오.

- 발급 권한 부여 규칙의 경우 Permit all users(모든 사용자 허용)를 선택한 후 Next(다음)를 선택합니다.
- Ready to Add Trust(트러스트 추가 준비) 페이지에서 기본 설정을 수락하고 Next(다음)를 선택합니다.
- 완료를 선택합니다. 이렇게 하면 Issuance Transform Rules - Claims(발급 변환 규칙 - 클레임)에서 다루는 신뢰 당사자 트러스트에 대한 Edit Claim Rules(클레임 규칙 수정) 대화 상자가 열립니다.

당사자 트러스트 속성 - 엔드포인트

클러스터에 여러 ESA가 있는 경우에만 이 단계를 수행합니다.

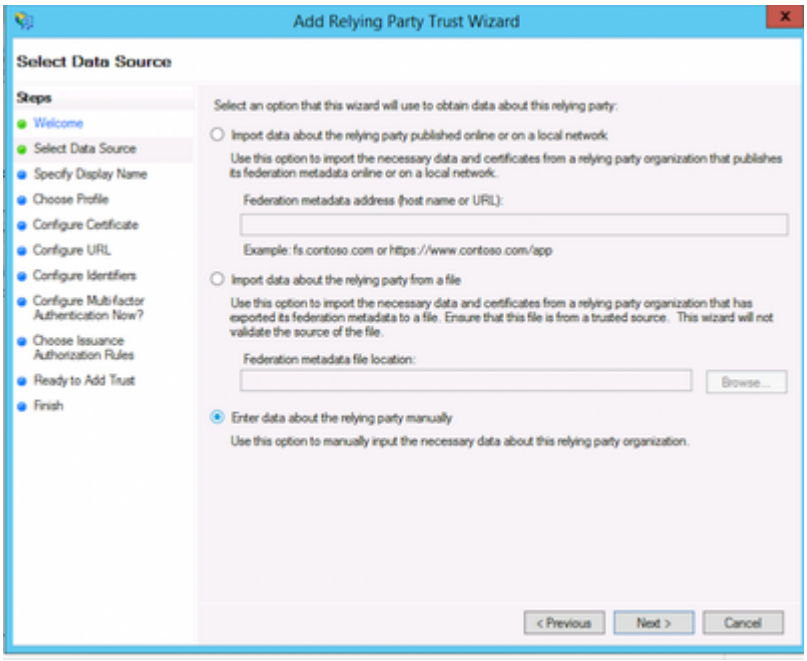
1. Relying Party Trust Properties(신뢰 당사자 트러스트 속성) > Endpoints(엔드포인트)를 엽니다.
2. 각 ESA 연결 가능 URL 주소를 추가한 다음 확인을 선택합니다.
3. 인덱스 값은 0, 즉 0, 1, 2, 3부터 계산됩니다.
4. 한 항목만 Default = Yes로 설정합니다.
5. 나머지 항목을 기본값 = 아니요로 설정합니다.



당사자 트러스트 속성 - 엔드포인트

옵션 B: 신뢰 당사자에 대한 데이터를 수동으로 입력합니다. 이 옵션은 수동 컨피그레이션을 안내합니다.

1. 신뢰 당사자에 대한 데이터를 수동으로 입력을 선택합니다.

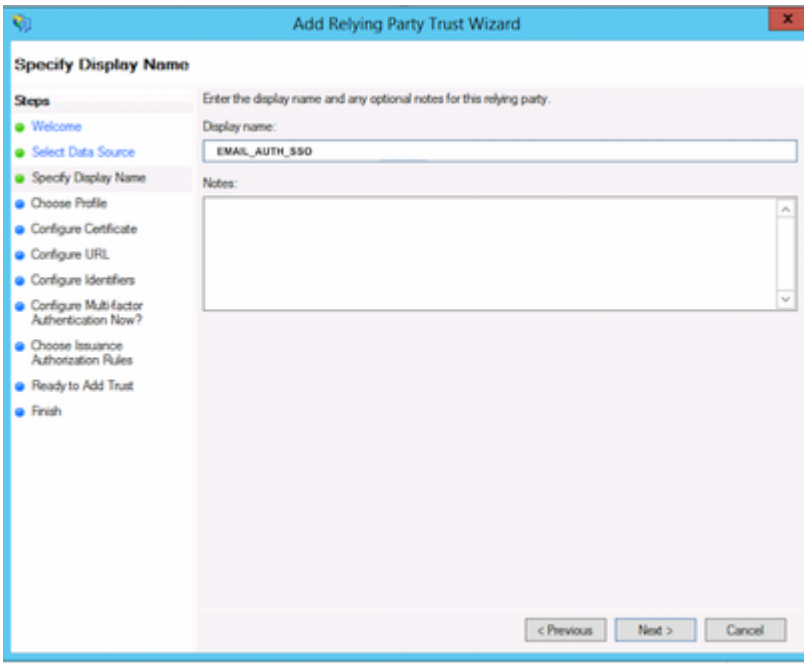


신뢰 당사자 수동 추가

팁: Display Name(표시 이름)은 ESA 또는 SMA SAML에 대한 신뢰 당사자 트러스트를 식별하기 위해 선택하는 이름입니다.

---

1. 서비스 공급자의 표시 이름(예: ESA_SP)을 입력합니다.

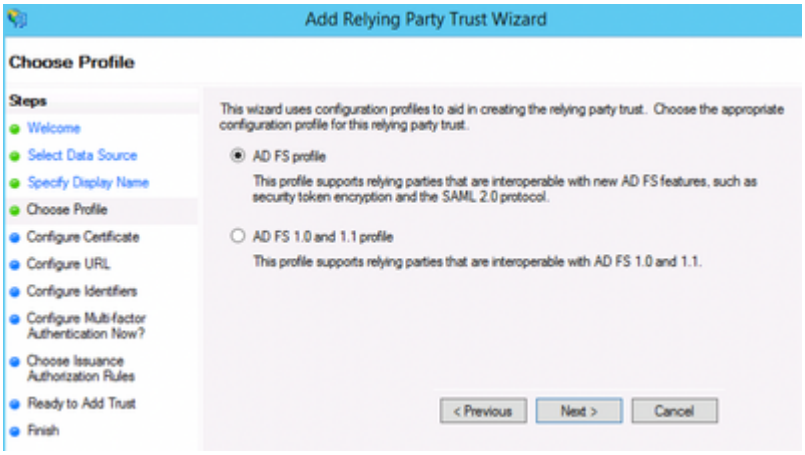


서비스 공급자 프로필의 이름 만들기

팁: [클레임 규칙 및 발급 변환 규칙의 역할]

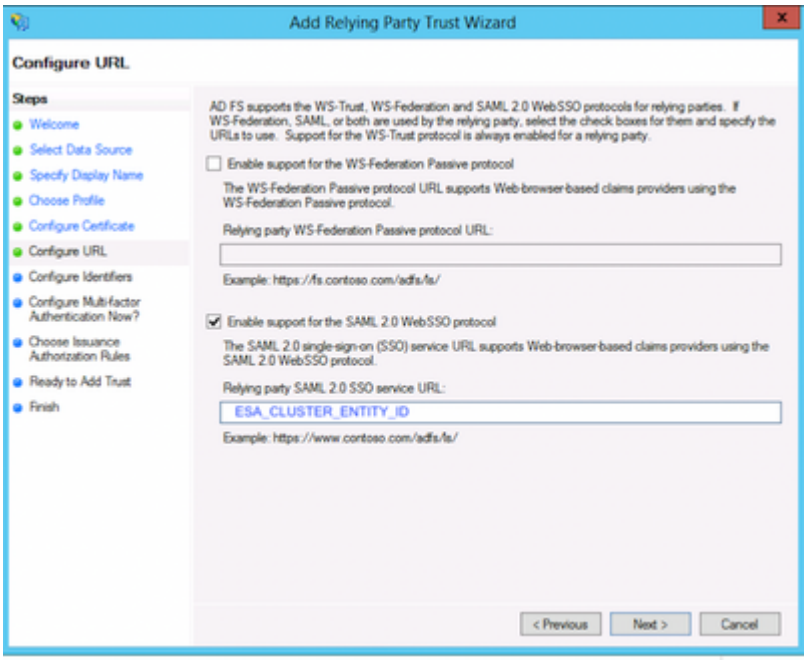
---

1. 프로파일 옵션 AD FS 프로파일을 선택합니다.



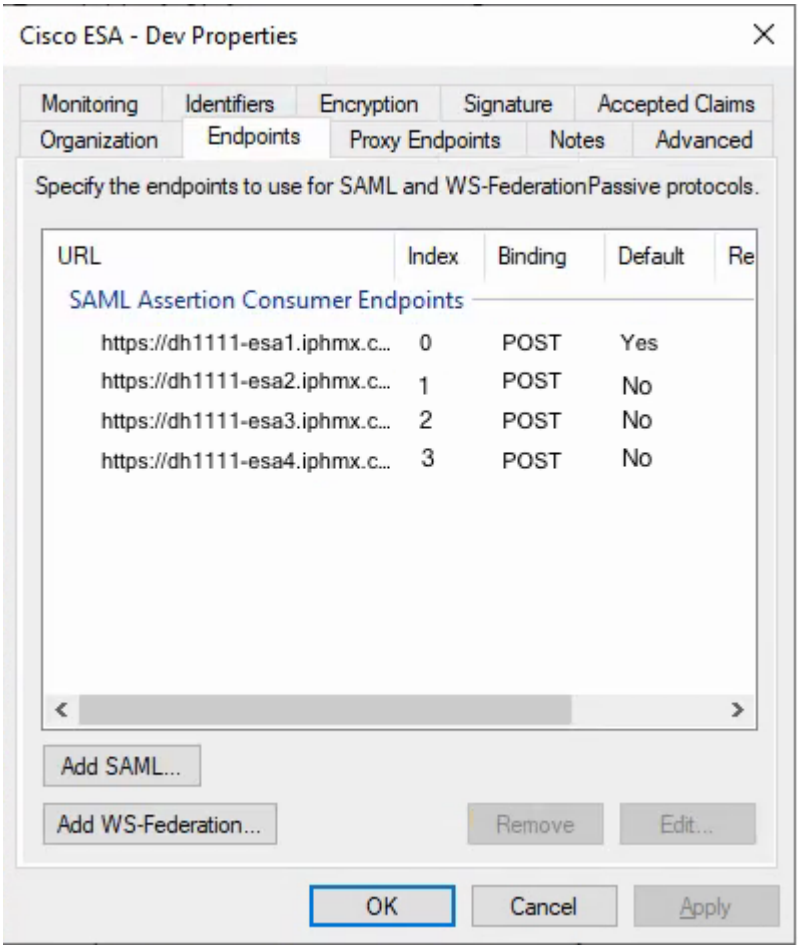
SAML 2.0 활용을 위한 AD FS 프로파일 옵션

1. ESA SP(서비스 공급자) 컨피그레이션에서 공용 인증서를 로드합니다.
2. Configure URL(URL 구성)에서 Enable support for the SAML 2.0 single-sign-on (SSO)(SAML 2.0 SSO(단일 로그인)에 대한 지원 활성화)을 선택합니다.
3. SP 프로필 Entity ID 값으로 당사자 SAML 2.0 SSO 서비스 URL을 입력합니다.



발급 권한 부여 규칙 - 모든 사용자 허용

1. 발급 권한 부여 규칙의 경우 Permit all users to access this relying party(모든 사용자가 이 신뢰 당사자에 액세스하도록 허용)를 선택합니다.



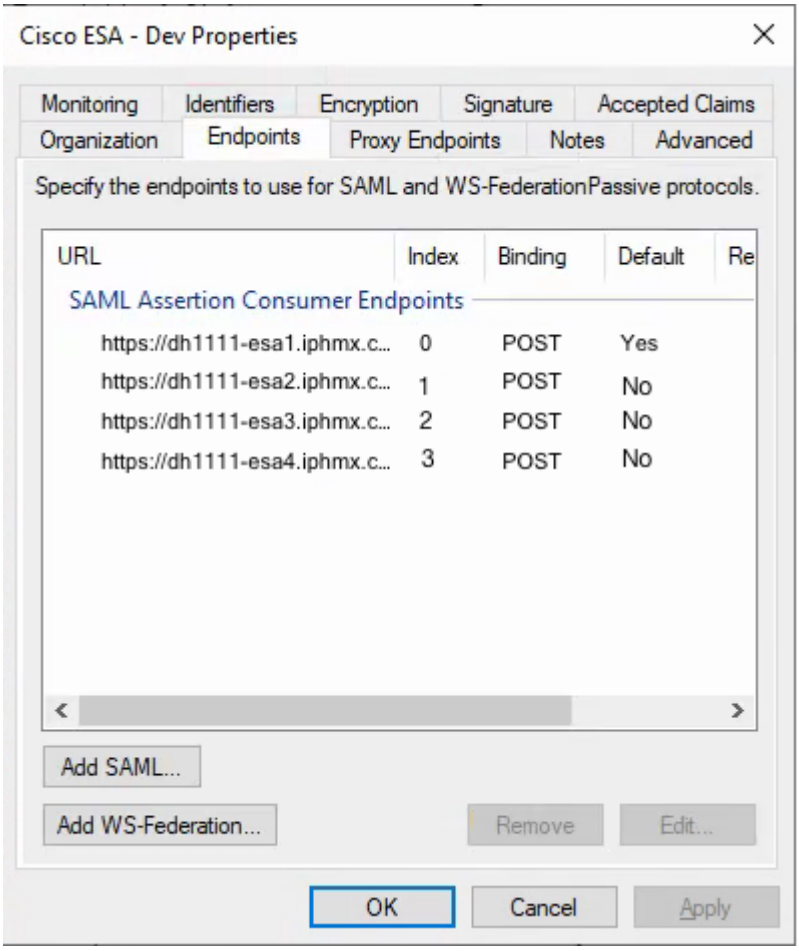
발급 권한 부여 규칙 선택

1. 다음을 선택하여 완료 페이지로 이동합니다.

당사자 트러스트 엔드포인트 구성(클러스터만 해당)

클러스터에 여러 ESA가 있는 경우에만 이 단계를 수행합니다.

1. Relying Party Trust Properties(신뢰 당사자 트러스트 속성) > Endpoints(엔드포인트)를 엽니다.
2. 각 ESA 연결 가능 URL 주소를 추가한 다음 OK(확인)를 클릭합니다.
3. 0, 1, 2, 3과 같이 0부터 시작하는 엔드포인트 인덱스 값을 설정합니다.
4. 하나의 엔드포인트만 Default = Yes로 설정합니다. 나머지 엔드포인트를 Default = No로 설정합니다.

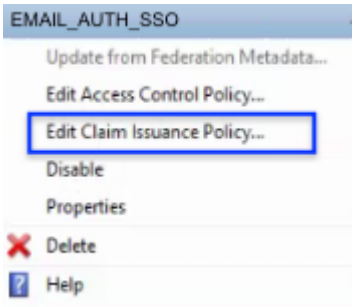


발급 권한 부여 규칙 - 모든 사용자 허용

- Finish(마침) 단계에서는 Issuance Transform Rules(발급 변환 규칙)에서 다루는 신뢰 당사자 트러스트에 대한 Edit Claim Rules(클레임 규칙 수정) 대화 상자를 시작합니다.

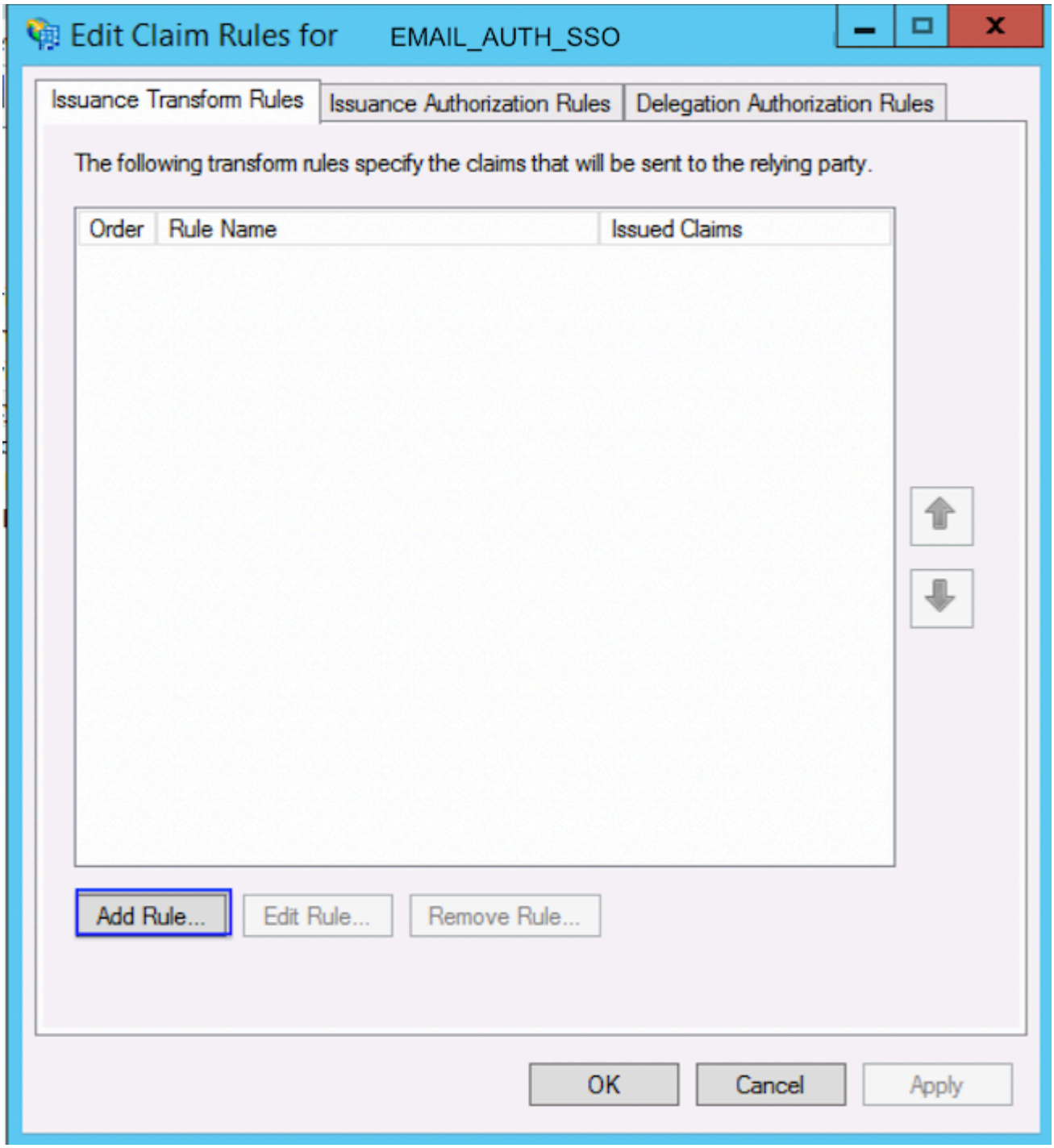
발급 변환 규칙 - 클레임

- Edit Claims Issuance Policy(클레임 발급 정책 수정)를 선택합니다.



클레임 발급 정책 편집

- Add Rule을 선택합니다.

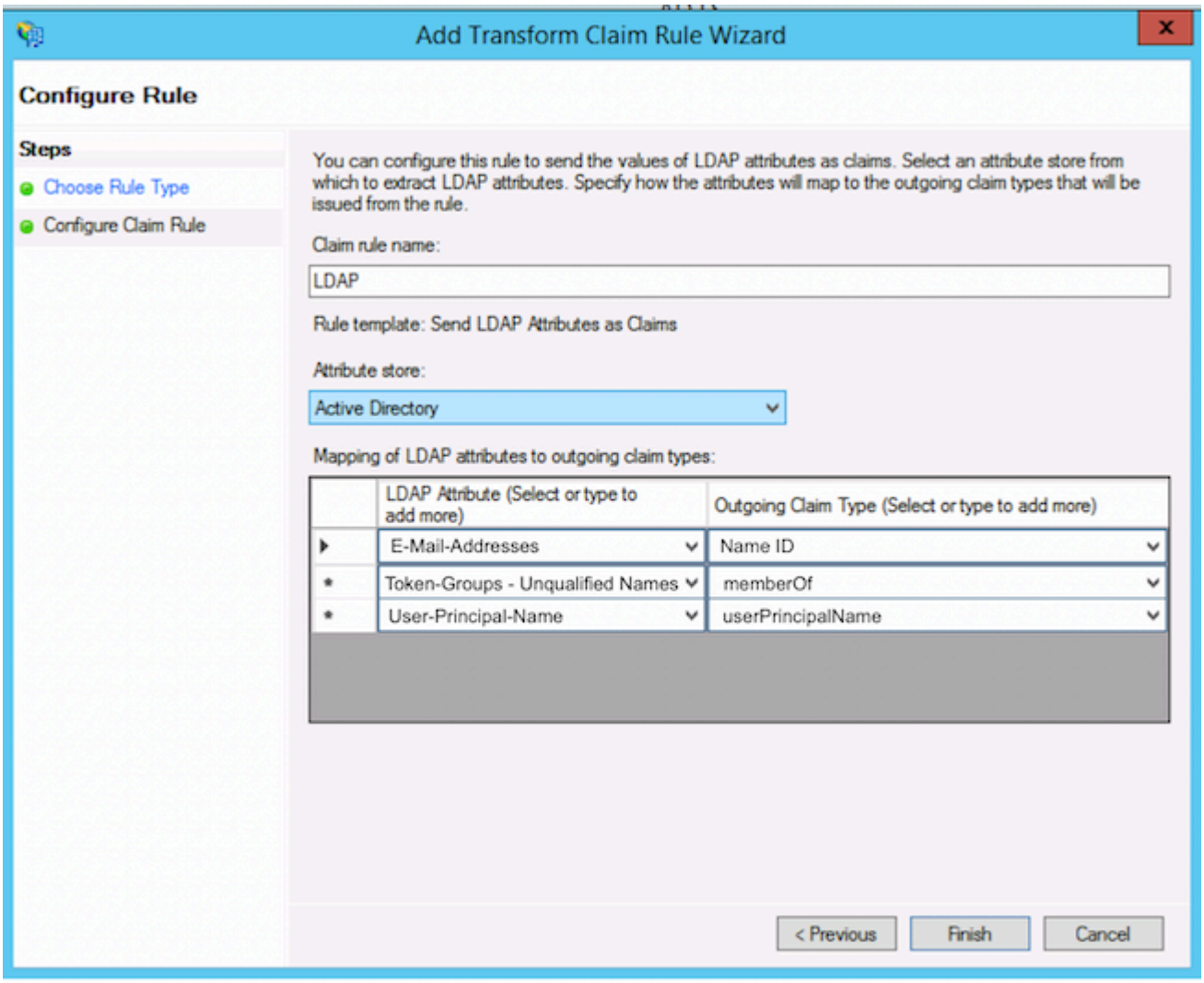


발급 변환 규칙 추가

여기에 표시된 값은 ESA가 외부 인증 설정에서 그룹 이름을 채울 수 있도록 하는 공통 값입니다.

팁: 매핑의 값은 관리자 환경 설정에 따라 달라질 수 있습니다.

팁: 나열된 샘플에서 발신 클레임 유형 memberOf 및 userPrincipalName을 수동으로 입력합니다. 드롭다운 목록에서 Name ID를 선택합니다.



클레임 규칙 변환

- 완료를 선택합니다.

IdP 메타데이터 다운로드 및 ESA에 업로드

신뢰 당사자 신뢰 및 클레임 규칙 컨피그레이션을 완료한 후 IdP(ID 공급자) 메타데이터를 내보내고 ESA에 업로드합니다.

⚠ 주의: AD FS 서비스를 다시 시작하면 활성 인증 세션이 중단될 수 있습니다. 필요한 경우 유지 관리 기간 중에 이 단계를 수행합니다.

- 필요한 경우 AD FS 서비스를 다시 시작합니다.
- 다음 명령을 실행합니다.

```
net stop adfssrv
net start adfssrv
```

- 다음 URL에서 메타데이터 파일을 다운로드합니다.

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- 완료하고 ESA 클러스터로 돌아갑니다.

다음을 확인합니다.

1. ESA 또는 SMA에서 IdP 메타데이터 가져오기가 성공적으로 완료되었는지 확인합니다.
2. SAML SSO(단일 로그인)를 사용하여 관리 로그인을 테스트합니다.
3. 예상되는 그룹 클레임을 받았는지, 그리고 역할 매핑이 외부 인증 컨피그레이션에서 예상대로 채워졌는지 확인합니다.

관련 정보

-

- Cisco Email Security Appliance – 엔드 유저 가이드
- Cisco Content Security Management Appliance - 최종 사용자 가이드

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.