ADFS에 메타데이터 파일 설치

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 Microsoft ADFS(Active Directory Federation Services)에 메타데이터 파일을 설치하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ADFS
- Security Management Appliance와 SAML(Security Assertion Markup Language) 통합

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SMA 11.x.x
- SMA 12.x.x

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

배경 정보

ADFS에 메타데이터 파일을 설치하기 전에 다음 요구 사항을 해결해야 합니다.

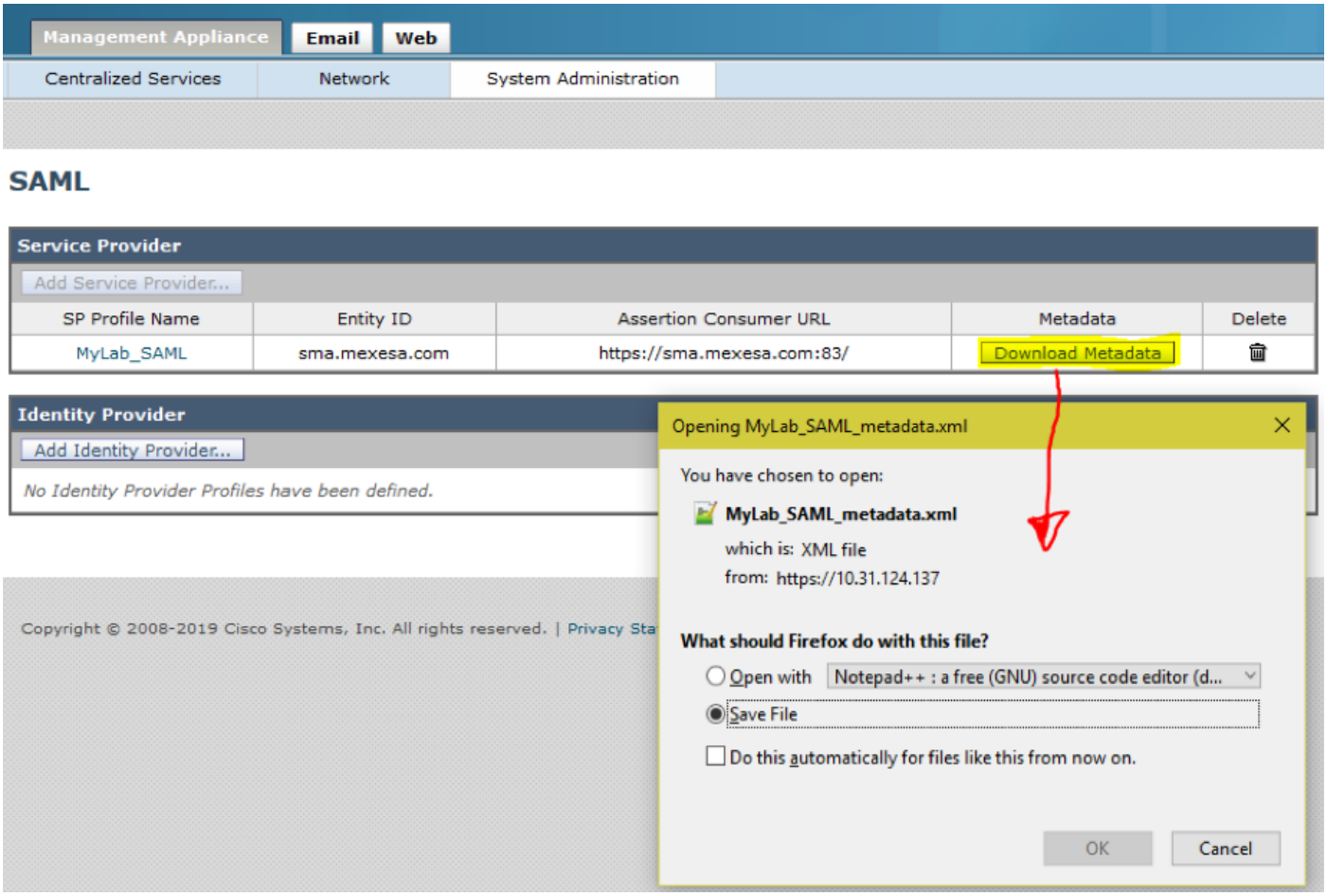
- SMA에서 활성화된 SAML
- 조직에서 사용하는 ID 공급자가 Cisco Content Security Management Appliance에서 지원되는지 확인합니다.지원되는 ID 제공자는 다음과 같습니다. Microsoft ADFS(Active Directory

Federation Services) 2.0Ping ID PingFederate 7.2Cisco Web Security Appliance 9.1

- 어플라이언스와 ID 공급자 간의 통신을 보호하는 데 필요한 다음 인증서를 가져옵니다.어플라이언스가 SAML 인증 요청에 서명하도록 하거나 ID 제공자가 SAML 어설션을 암호화하도록 하려면 신뢰할 수 있는 CA(Certificate Authority) 및 관련 개인 키에서 자체 서명 인증서 또는 인증서를 가져옵니다.ID 공급자가 SAML 어설션에 서명하도록 하려면 ID 공급자의 인증서를 가져옵니다.어플라이언스는 이 인증서를 사용하여 서명된 SAML 어설션을 확인합니다.

구성

1단계. SMA로 이동하여 이미지에 표시된 대로 **System Administration(시스템 관리) > SAML > Download Metadata(메타데이터 다운로드)**를 선택합니다.



2단계. 고객이 ADFS 메타데이터 파일을 업로드하면 ID 제공자 프로파일이 자동으로 채워집니다.Microsoft에는 기본 URL이 있습니다.**https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

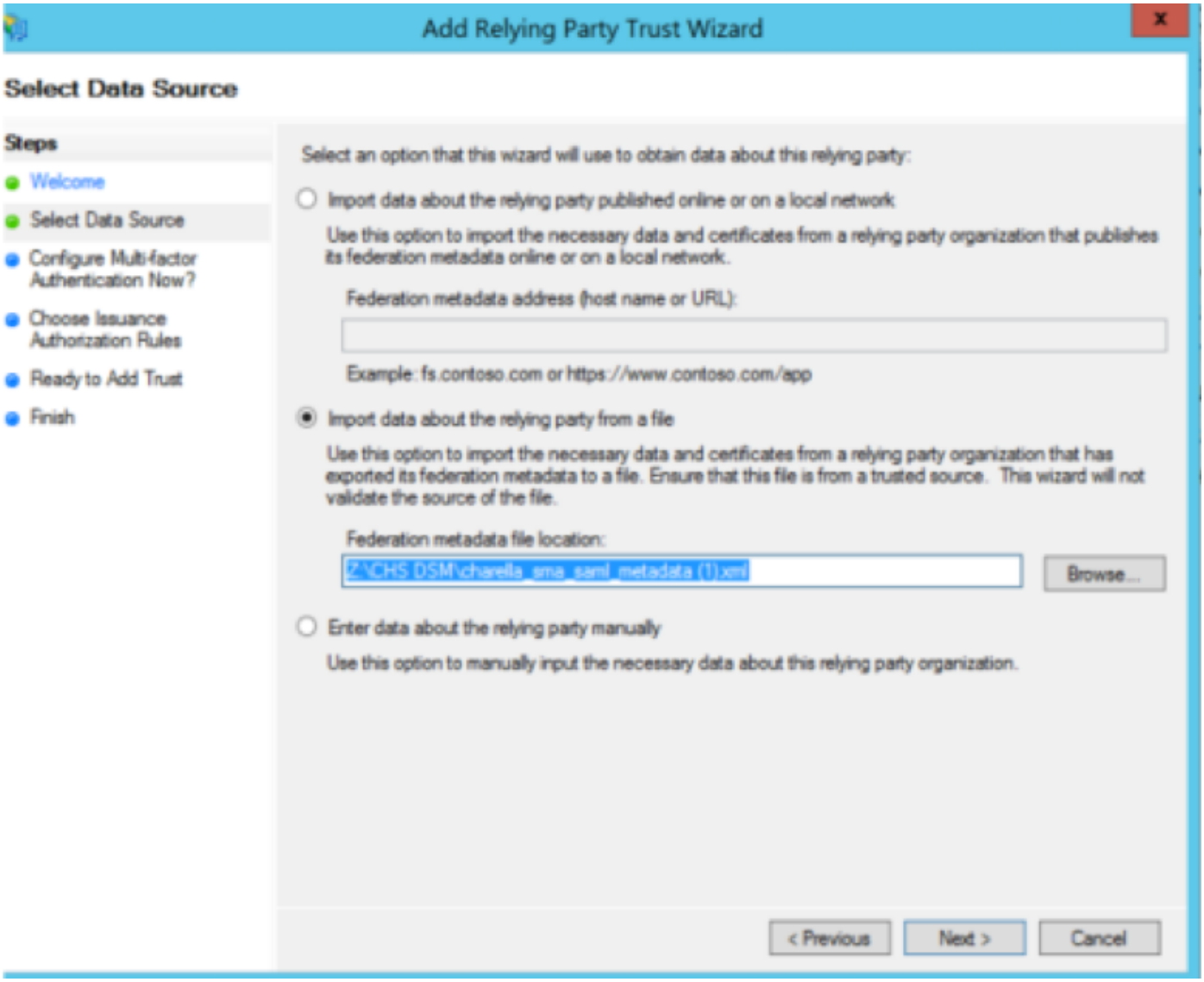
3단계. 두 프로파일 모두 설정되면 버그 CSCvh30183.과 같이 SP 프로필 메타데이터를 편집해야 합니다.메타데이터 파일은 이미지에 표시된 것처럼 보입니다.

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="sma.mexesa.com">
  <SPSSODescriptor
      AuthnRequestsSigned="false"  WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>Bag Attributes
    localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
    friendlyName: sma.mexesa.com
subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
-----BEGIN CERTIFICATE-----
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm1leGVzYS5jb20xDTALBgNVBAcMBENE
TVgxFjAUBgNVBAoMDVRpem9uY2l0byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B
cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb
emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79
+ZIjQkekyCAM5N0Of1ZRrJ9oGD5qoYlZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7
7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq
ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
PO1jBG5MZuWE
-----END CERTIFICATE-----
          </ds:X509Certificate>
        </ds:X509Data>
```

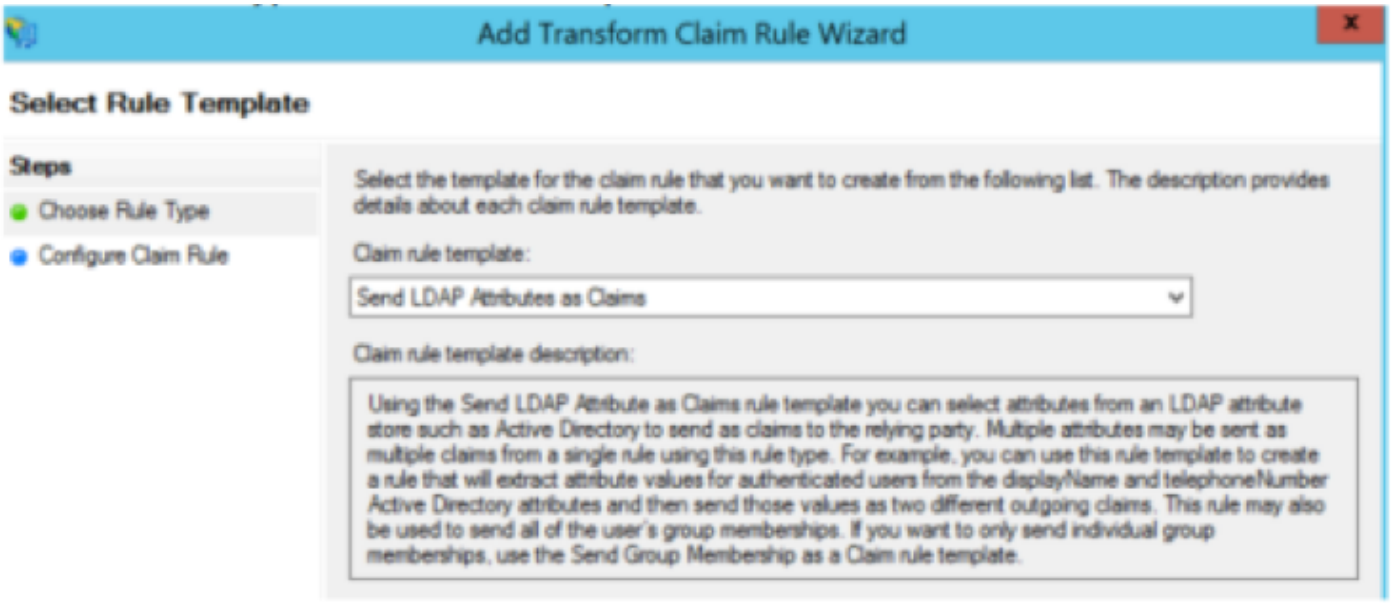
4단계. 강조 표시된 정보를 제거합니다. 마지막 메타데이터 파일은 이미지에 표시된 대로 있어야 합니다.

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="sma.mexesa.com">
  <SPSSODescriptor
      AuthnRequestsSigned="false"  WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm1leGVzYS5jb20xDTALBgNVBAcMBENE
TVgxFjAUBgNVBAoMDVRpem9uY2l0byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B
cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb
emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79
+ZIjQkekyCAM5N0Of1ZRrJ9oGD5qoYlZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7
7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq
ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
PO1jBG5MZuWE
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

5단계. ADFS로 이동하고 이미지에 표시된 대로 ADFS **Tools > AD FS Management > Add Relying Party Trust(ADFS 툴 > AD FS 관리 > 신뢰 당사자 신뢰 추가)**에서 편집된 메타데이터 파일을 가져옵니다.



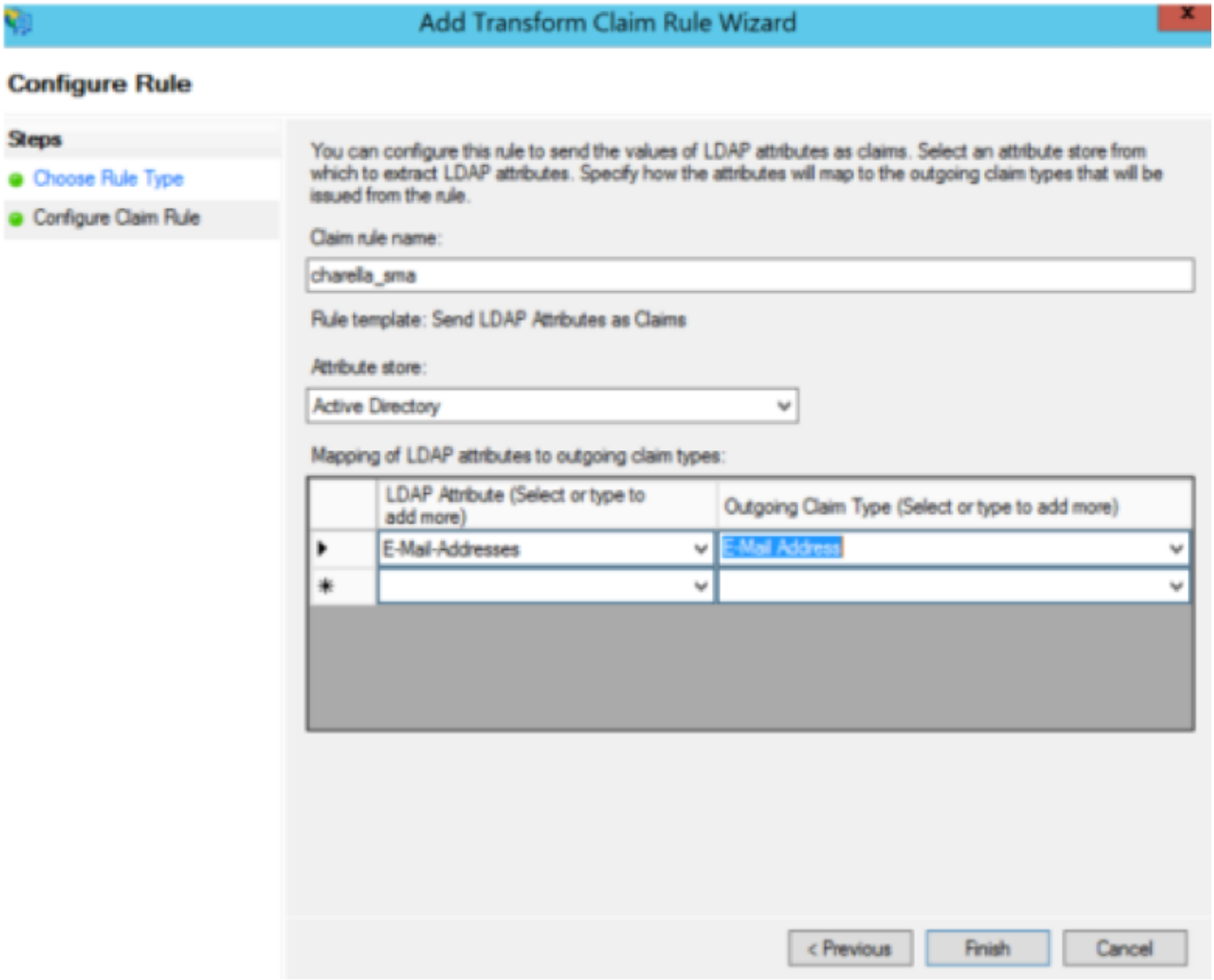
6단계. 메타데이터 파일을 성공적으로 가져온 후 새로 생성된 신뢰 당사자 트러스트에 대한 클레임 규칙을 구성하고 이미지에 표시된 대로 **클레임 규칙 템플릿 > LDAP 특성 전송**을 선택합니다.



7단계. 클레임 규칙 이름의 이름을 지정하고 Attribute **Store > Active Directory**를 선택합니다.

8단계. 이미지에 표시된 대로 LDAP 특성을 매핑합니다.

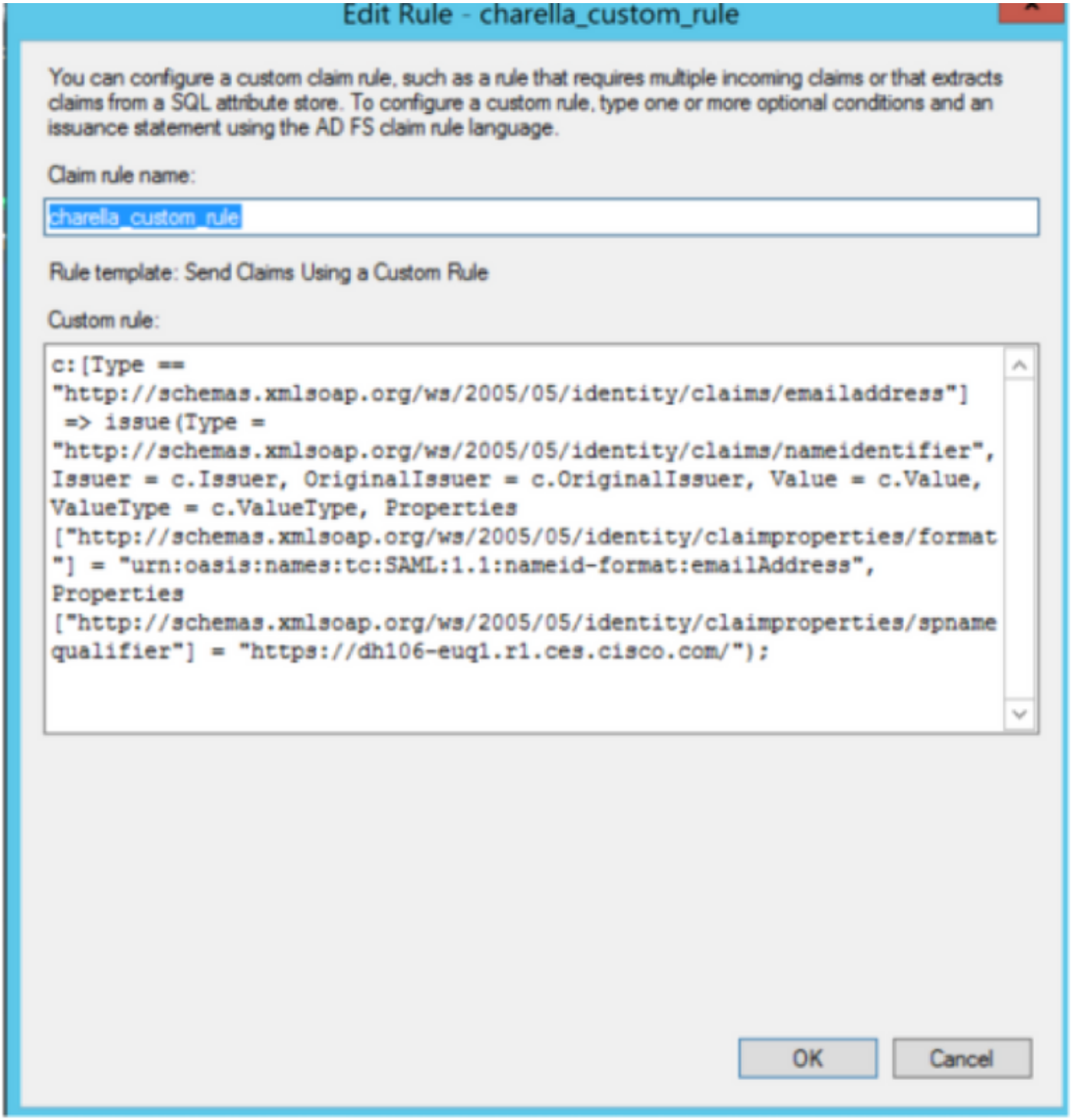
- LDAP 특성 > 이메일 주소
- 발송 청구 유형 > 이메일 주소



9단계. 이미지에 표시된 대로 이 정보로 새 사용자 지정 클레임 규칙을 만듭니다.

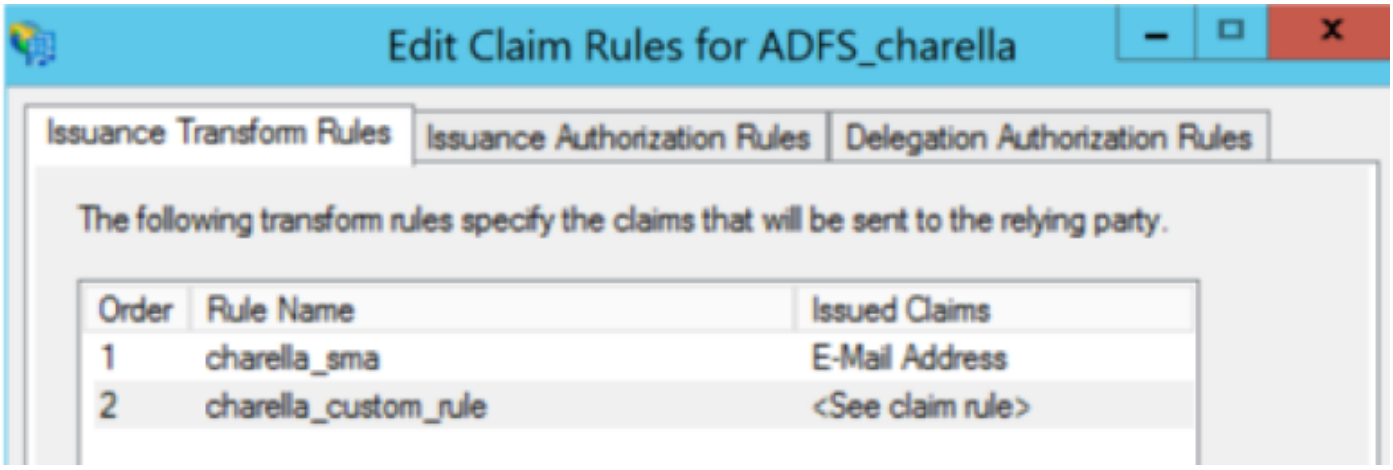
사용자 지정 클레임 규칙에 추가해야 하는 사용자 지정 규칙입니다.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "https://<smahostname>:83");
```



- 강조 표시된 URL을 SMA 호스트 이름 및 포트로 수정합니다(CES 환경에 있는 경우 포트는 필요하지 않지만 euq1.<allocation>.iphmx.com을 가리켜야 함).

10단계. 청구 규칙 순서가 다음과 같은지 확인합니다.이미지에 표시된 대로 LDAP 클레임 규칙 첫 번째 및 사용자 지정 클레임 규칙 두 번째.



11단계. EUQ에 로그인합니다. ADFS 호스트로 리디렉션해야 합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- CSCvh30183
- 기술 지원 및 문서 – Cisco Systems