# SAML을 사용하여 AD FS 버전 3.0으로 Umbrella 구성

## 목차



## 소개

이 문서에서는 Cisco Umbrella와 ADFS(Active Directory Federation Services) 버전 3.0 간에 SAML을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

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.

## 개요

이 문서에서는 Cisco Umbrella와 ADFS(Active Directory Federation Services) 버전 3.0 간에 SAML을 구성하는 방법에 대해 설명합니다. SAML을 ADFS와 함께 구성하는 것은 마법사에서 클릭 한 번 또는 두 번 프로세스가 아니라 ADFS를 올바르게 작동하려면 변경해야 하기 때문에 Umbrella의 다른 SAML 통합과 다릅니다.

이 문서에는 SAML과 AD FS가 함께 작동하도록 하기 위해 해야 할 세부 사항이 있습니다. 기본 단

계는 먼저 AD FS 환경과 Cisco Umbrella 간의 암호화를 비활성화한 다음 Umbrella 릴레이 파티 설정에 일부 Issuance Transform Custom Claim 규칙을 추가하는 것입니다.

기존의 작동 중인 AD FS 설정에서만 이 단계를 수행합니다. Cisco Umbrella Support는 특정 환경에서 AD FS를 구성하는 데 도움을 주거나 지원할 수 없습니다.

현재 이 지침에서는 ADFS 버전 3.0만 지원됩니다(Windows Server 2012 R2). 이전 버전(2.0 또는 2.1) 또는 이후 버전(4.0)의 ADFS가 Umbrella SAML 통합과 함께 작동할 수 있지만, 이는 테스트되거나 입증되지 않았습니다. 다른 버전의 AD FS를 보유하고 있고 Cisco 지원 및 제품 팀과 협력하여 통합하고자 하는 경우 Cisco Umbrella Support에 문의하십시오.

Umbrella 설명서에서 초기 SAML 설정의 전제 조건을 찾을 수 있습니다. ID 통합: 사전 요구 사항. 이러한 단계를 완료하면 이 문서의 ADFS 관련 지침을 계속 사용하여 컨피그레이션을 완료할 수 있습니다.

Umbrella 설명서의 단계에서는 SAML(ADFS) 메타데이터를 Umbrella에 업로드해야 한다고 설명합니다. 이 URL로 이동한 다음 XML 파일을 업로드하여 메타데이터에 액세스할 수 있습니다.

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

## 암호화 사용 안 함

1. AD FS 관리를 엽니다. Trust Relationships를 확장하고 Relying Party Trust를 선택합니다.

2. Umbrella 신뢰 당사자(또는 이름을 지정한 모든 당사자)를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.

3. 암호화 탭을 선택합니다.

4. 제거를 선택하여 암호화할 인증서를 제거합니다.

5. 확인을 선택하여 화면을 닫습니다.

## 새 발급 변환 클레임 규칙 추가

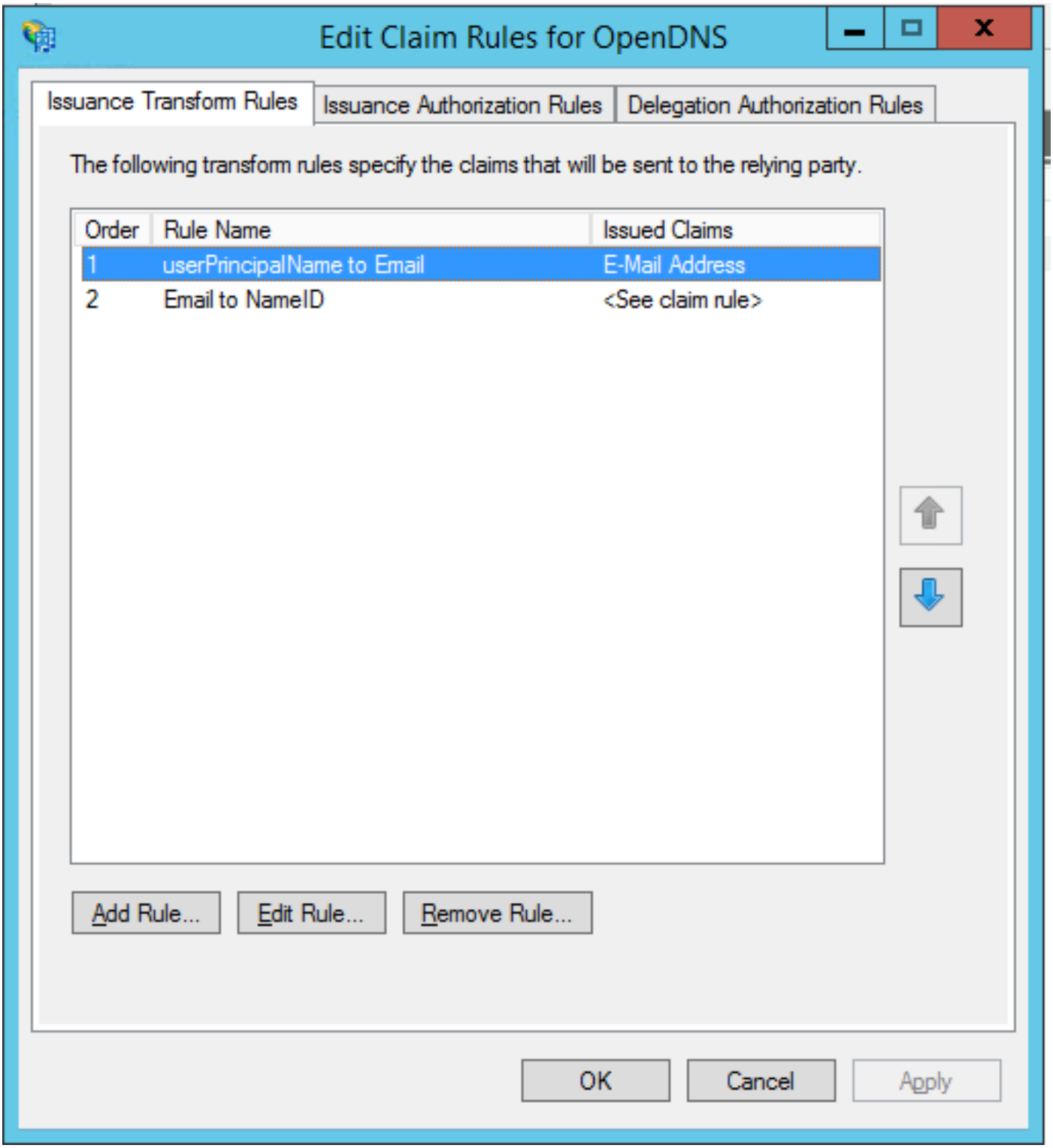
1. AD FS 관리를 엽니다. Trust Relationships(신뢰 관계)를 확장하고 Relaying Party Trust를 선택합니다.

2. Umbrella 릴레이 상대방(또는 이름을 지정한 항목)을 마우스 오른쪽 버튼으로 클릭하고 청구 규칙 편집을 선택합니다.

3. Issuance Transform Rules(발급 변환 규칙)에서 Add Rule(규칙 추가)을 선택합니다.

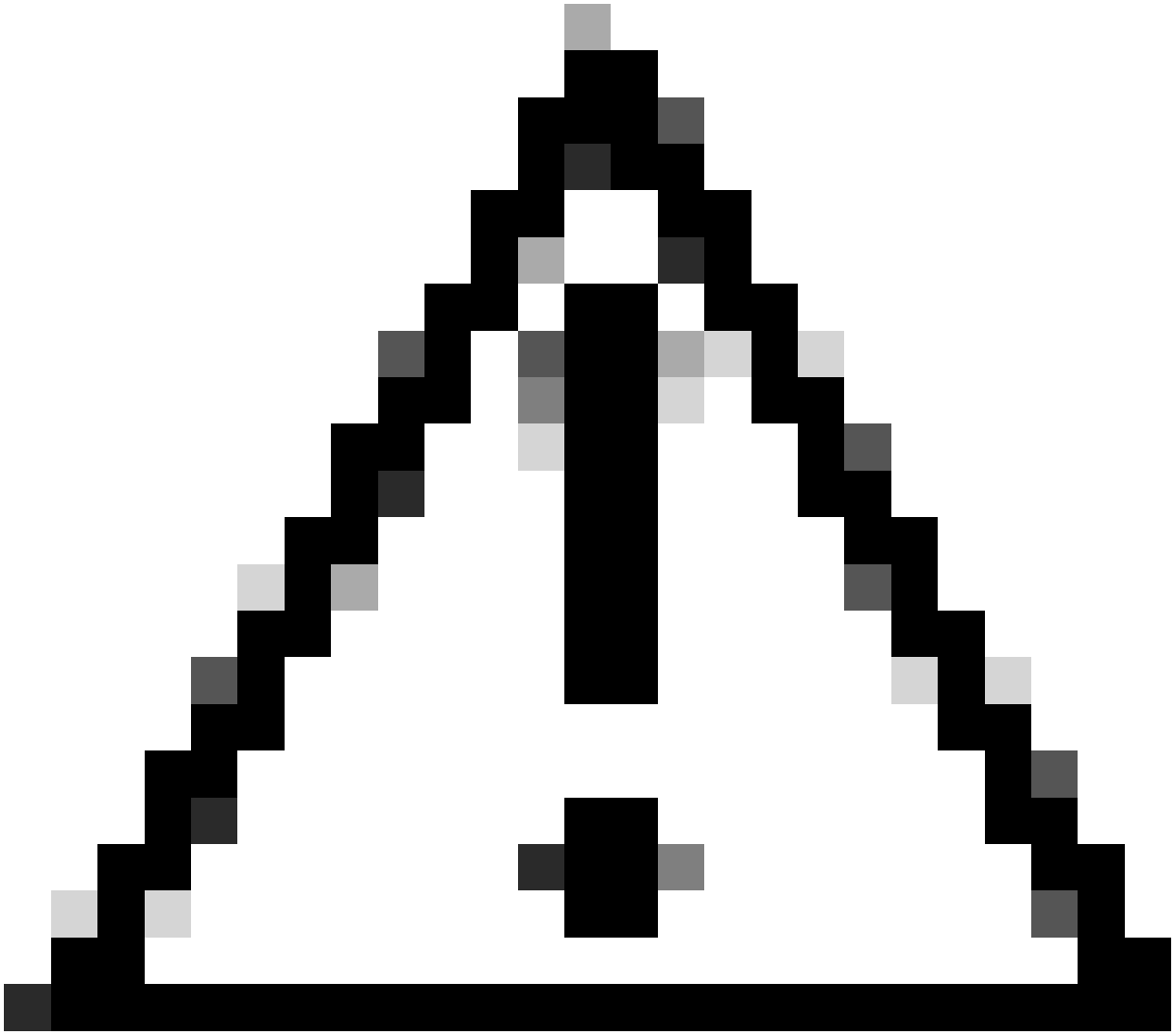
4. 사용자 지정 규칙을 사용하여 청구 전송을 선택합니다.

추가할 수 있는 규칙 목록은 이 스크린샷을 참조하십시오.




이러한 규칙을 각각 추가하면 통합이 시작될 수 있습니다.

## 변환 규칙



주의: 이러한 규칙은 Umbrella의 AD FS 랩 환경 및 몇몇 고객 프로덕션 환경에서 테스트되고 작동했습니다. 환경에 맞게 수정하십시오.

---

이메일 주소에 대한 사용자 계정 이름

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

NameID로 이메일 보내기

```
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");
```

# 부록: 'mail' 특성으로 로그인

기본적으로 AD FS는 UPN(User Principal Name)을 사용하여 사용자를 인증합니다. 사용자의 전자 메일 주소(Umbrella 계정 이름)가 UPN과 일치하지 않으면 추가 단계가 필요합니다. 다음 기술 자료 문서를 참조하십시오. 이메일 주소로 로그인을 허용하도록 Cisco Umbrella Dashboard에서 AD FS를 구성하려면 어떻게 해야 합니까?

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.