Umbrella를 NetIQ와 통합하여 SAML과 SSO 지원

목차

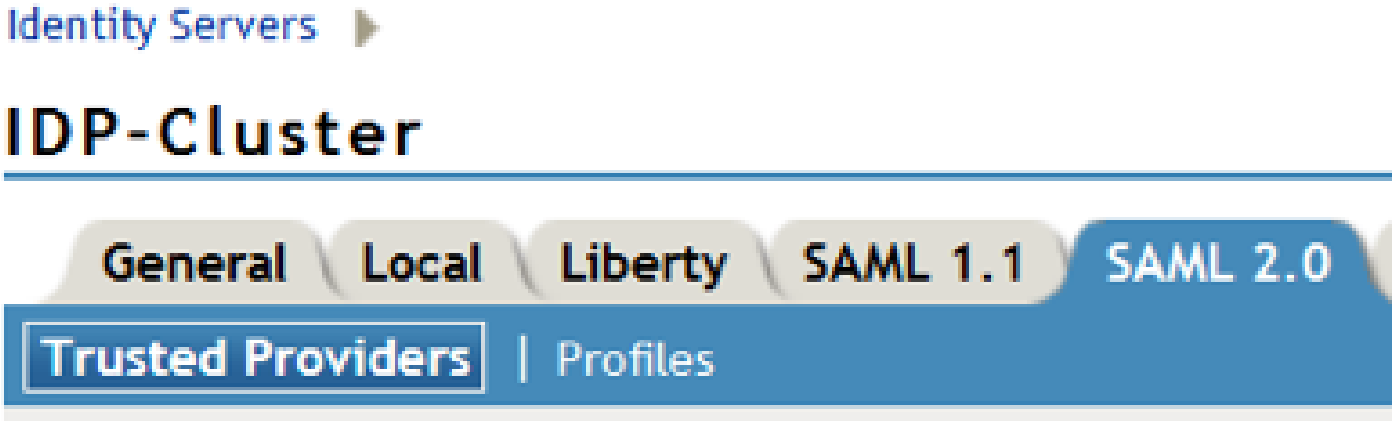
소개

이 문서에서는 Cisco Umbrella와 NetIQ for Single Sign-on(SSO)을 SAML과 통합하는 방법에 대해 설명합니다.

NetIQ용 Umbrella SAML 통합 개요

NetIQ를 사용하여 SAML을 구성하는 것은 마법사에서 클릭 한 번 또는 두 번 프로세스가 아니라 NetIQ를 올바르게 변경해야 하기 때문에 다른 SAML 통합과 다릅니다. 이 문서에서는 SAML과 NetIQ가 함께 작동하는 데 필요한 세부 수정 사항에 대해 설명합니다. 이와 같이 본 정보는 "있는 그대로" 제공되며 기존 고객과 연계하여 개발되었습니다. 이 솔루션에 대한 사용 가능한 지원은 제한적이며 Cisco Umbrella 지원에서는 여기에 제시된 일반적인 개요 외에는 지원할 수 없습니다.

SAML 통합이 Umbrella와 작동하는 방식에 대한 자세한 내용은 여기에서 검토를 참조하십시오. [Single Sign-On을 시작합니다](#).

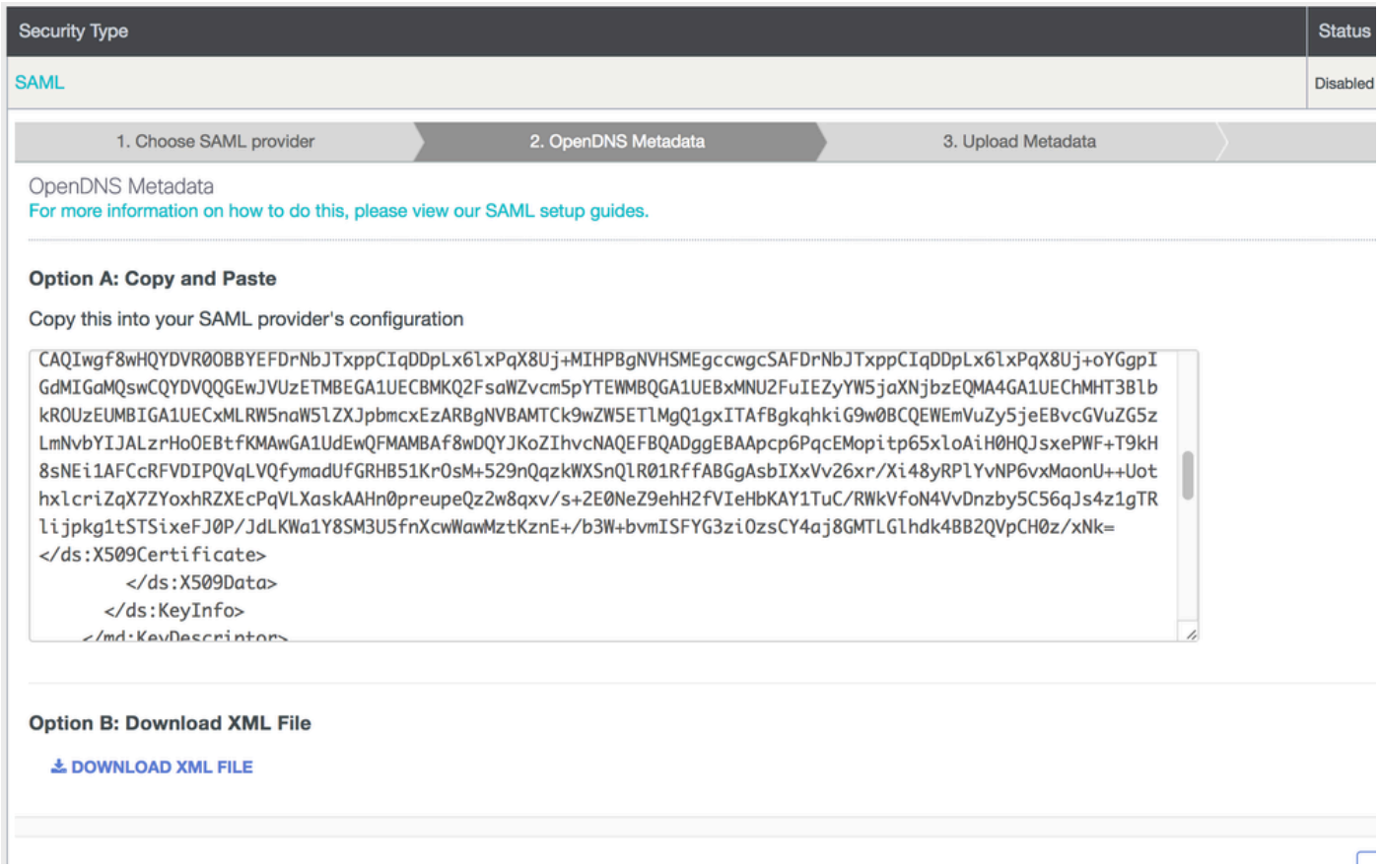


115000348788

사전 요구 사항

다음과 같이 초기 SAML 설정을 통과하는 단계를 찾을 수 있습니다. ID 통합: 사전 요구 사항. Cisco Umbrella 메타데이터 다운로드가 포함된 단계를 완료하면 이 NetIQ 관련 지침을 계속 사용하여 컨피그레이션을 완료할 수 있습니다.

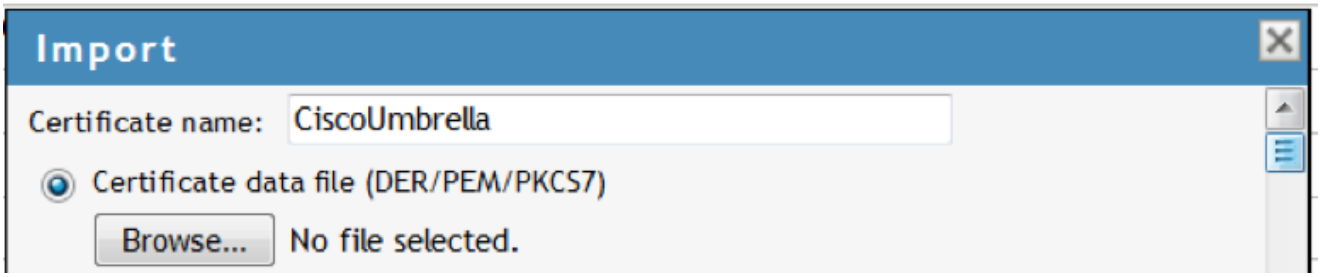
메타데이터는 Cisco Umbrella SAML 설정 마법사(Settings(설정) > Authentication(인증) > SAML)에서 찾을 수 있습니다.



115001332488

메타데이터 및 Cisco Umbrella 인증서 가져오기

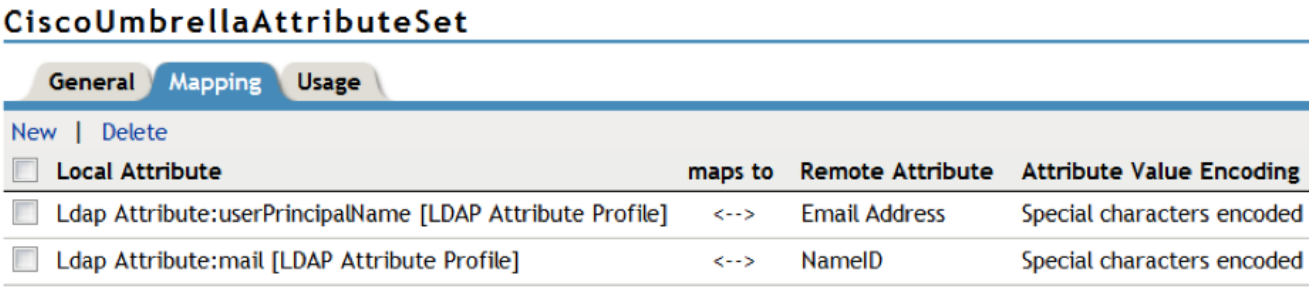
1. 텍스트 편집기에서 Cisco Umbrella 메타데이터(사전 요구 사항에 다운로드됨)를 열고 X509 인증서를 추출합니다. 인증서는 ds:X509Certificate로 시작하고 /ds:X509Certificate로 끝납니다. 맨 처음부터 끝까지 복사하기만 하면 됩니다.
2. 이 새 파일을 CiscoUmbrella.cer로 저장합니다.
3. x509 인증서를 PKCS7/PEM으로 변환합니다. 이에 대한 방법은 다양하지만 이 명령은 다음을 수행합니다. **openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM**
4. NetIQ에서 Trusted Roots 아래에서 NAM을 시작합니다.
5. New(새로 만들기) > Browse(찾아보기)를 선택하고 CiscoUmbrella.pem을 가져옵니다.



115000349367

특성 그룹 생성

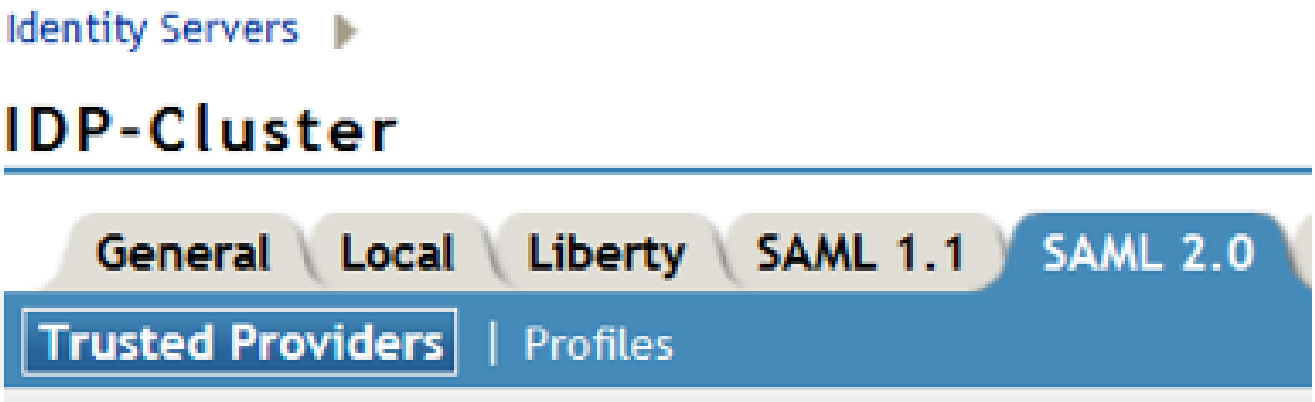
1. Identity Servers(ID 서버) > NetIQ NAM으로 이동합니다.
2. Attribute Sets를 클릭합니다.
3. New(새로 만들기)를 선택하고 LDAP 특성을 매핑합니다.



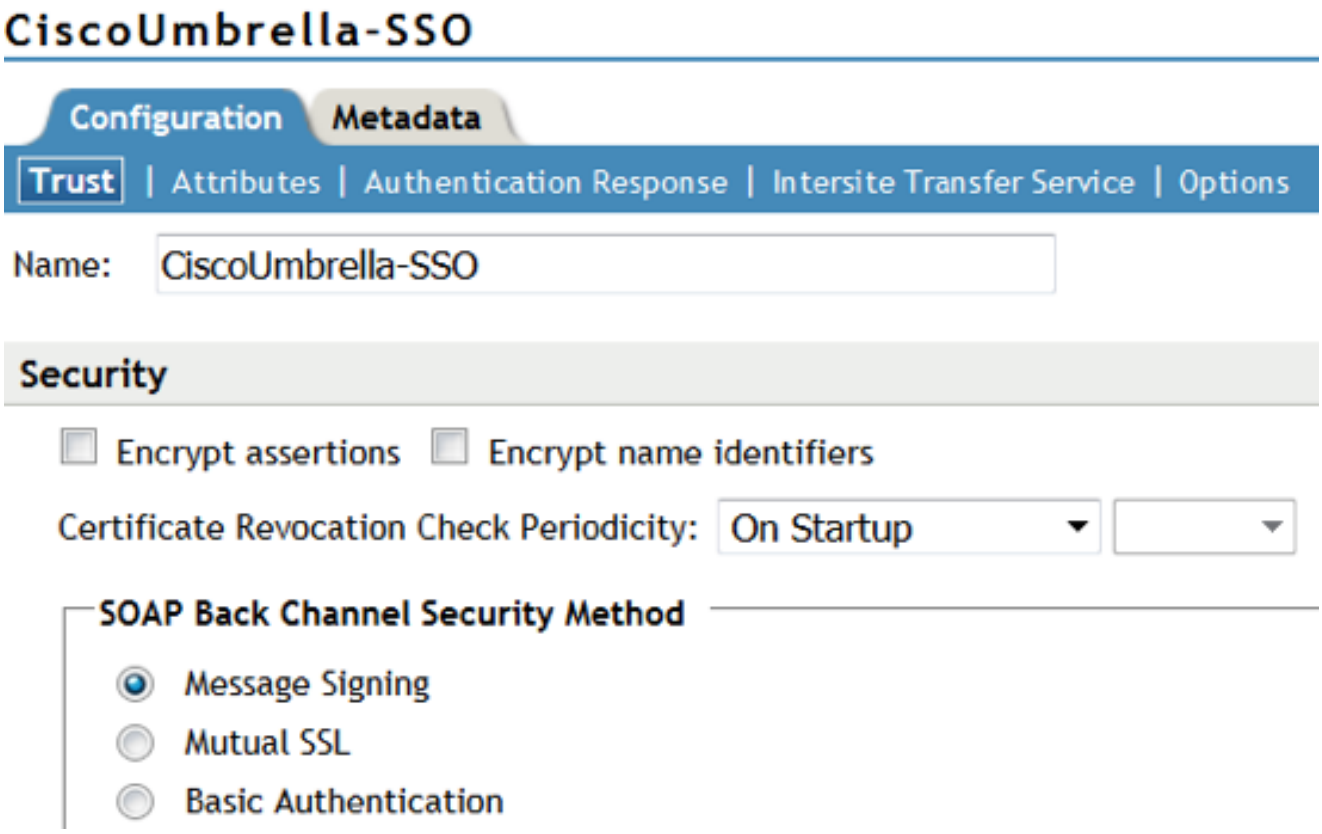
115000349567

새 트러스트 공급자 만들기

1. IDP General(IDP 일반) 탭으로 이동하여 SAML 2.0을 선택합니다.
2. Create New Trust Provider를 선택합니다.

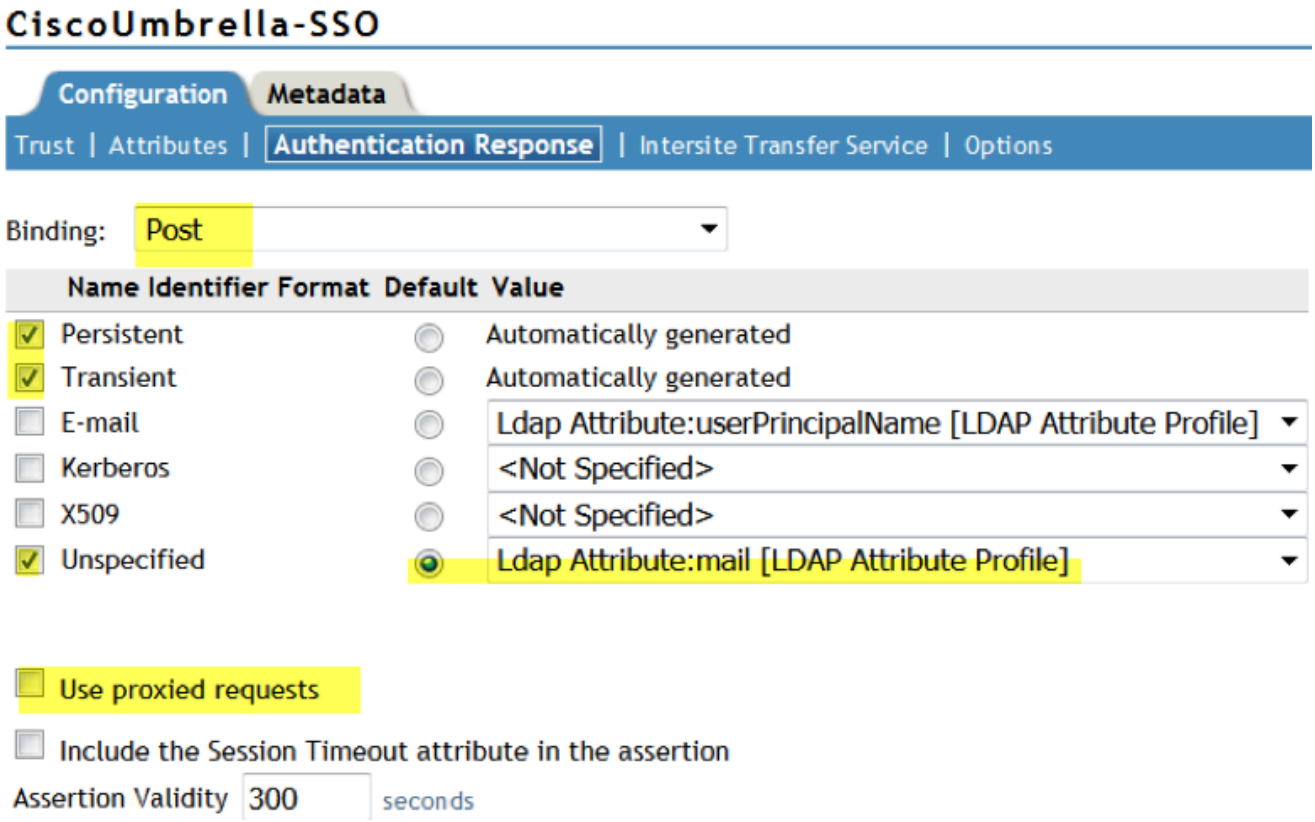


115000348788



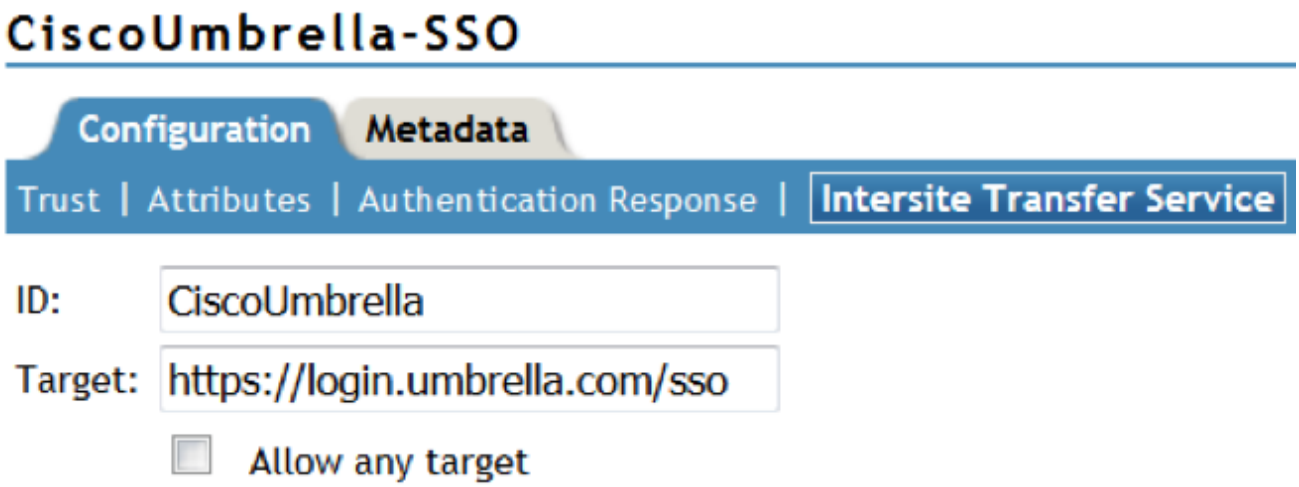
115000349827

3. 방금 생성한 속성을 선택하고 Send with Authentication을 선택합니다. Authentication Response(인증 응답)에 대해 Post Binding(사후 바인딩), Persistent(지속), Transient(일시적), Unspecified(미지정)를 선택합니다.
4. LDAP 특성 선택: [LDAP Attribute Profile](LDAP 특성 프로필)을 메일로 보내고 기본값으로 설정합니다.



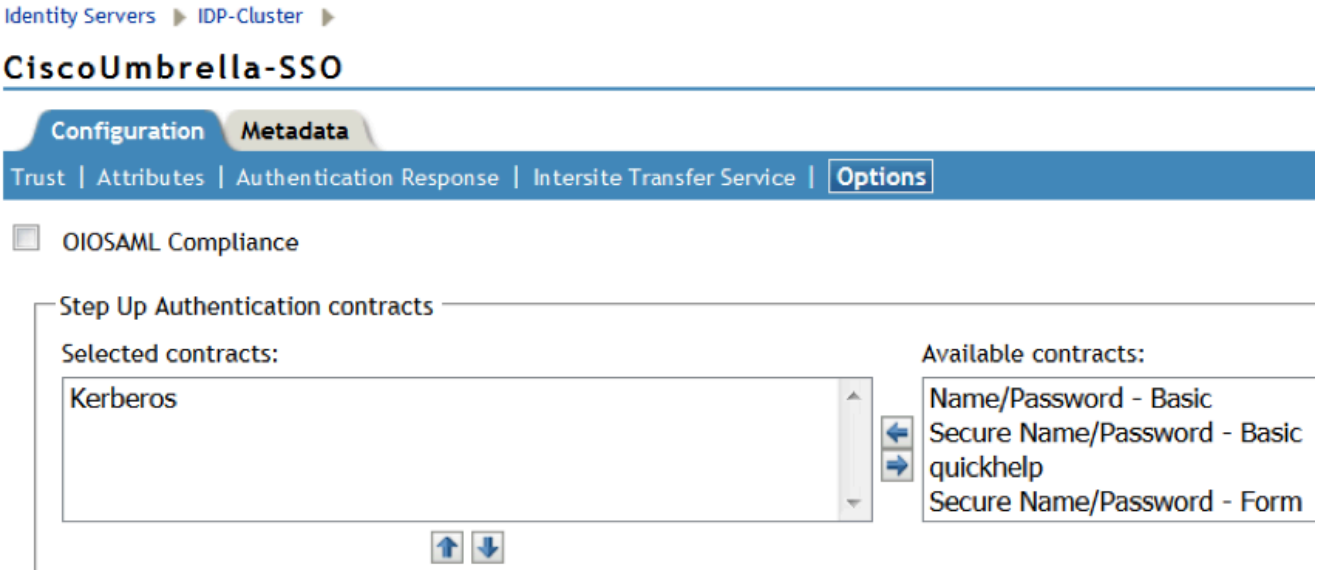
115000355688

5. Configuration(컨피그레이션) > Intersite Transfer Service(사이트 간 전송 서비스)로 이동합니다. Cisco Umbrella SAML과 같은 이름을 지정하고 Cisco Umbrella SSO 로그인 URL을 대상으로 추가합니다(https://login.umbrella.com/sso).



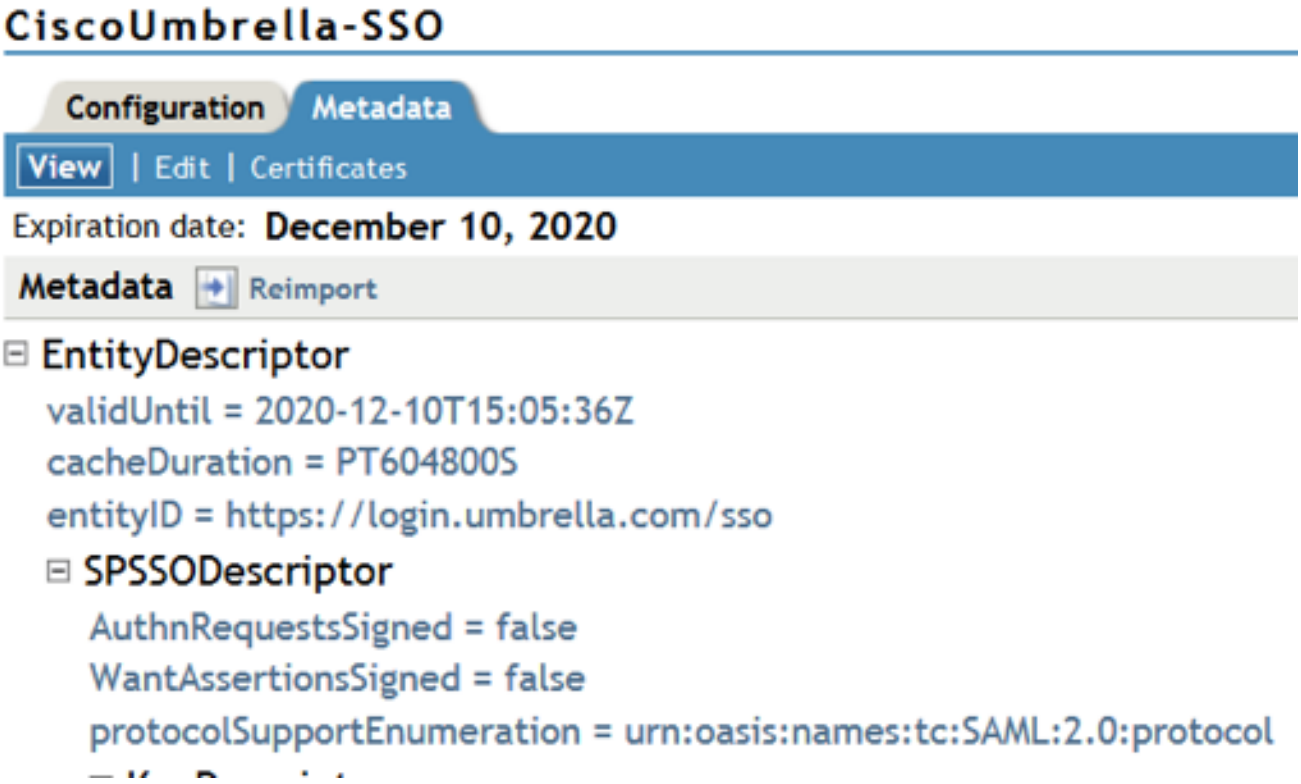
115000356827

6. Configuration(컨피그레이션) > Options(옵션)로 이동하여 Selected contracts(선택한 계약)로 Kerberos를 선택합니다.



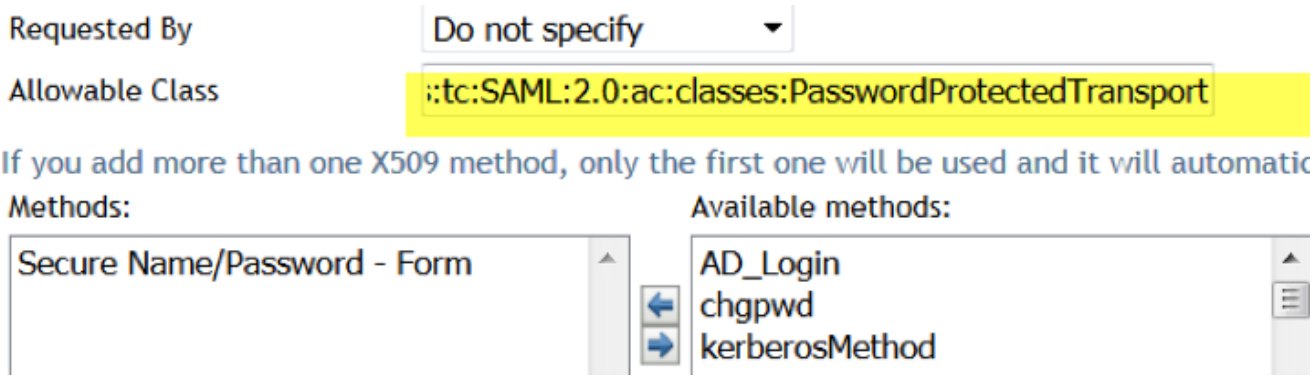
115000356068

7. Cisco Umbrella 메타데이터 파일을 엽니다. EntityDescription 필드 vailedUntil date를 2020-12-10T20:50:59Z(스크린샷과 같이)와 같은 미래 데이터로 업데이트합니다.
8. NetIQ > Metadata(메타데이터)로 돌아가 업데이트된 메타데이터 파일을 가져옵니다.



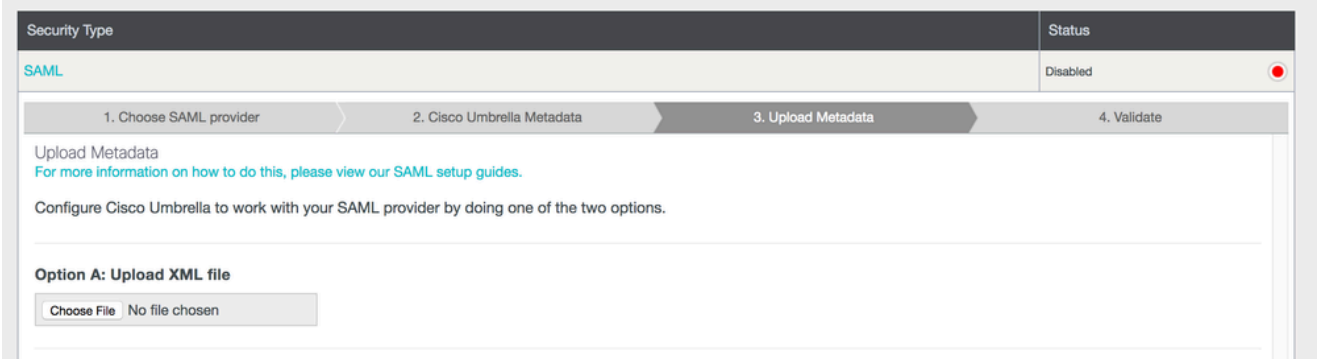
115000357147

9. 어설션에 클래스를 추가합니다. Cisco Umbrella assertion에는 **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport**
10. Local(로컬) > Contracts(계약)로 이동하여 Secure Name/Password(보안 이름/비밀번호)를 선택하고 Allowable Class(허용 클래스) 필드에 추가한 다음 위의 클래스를 추가합니다.



115000357247

11. Identity Services 및 액세스 게이트웨이를 업데이트하여 유효하고 최신 상태인지 확인한 다음 NetIQ 메타데이터를 다운로드합니다.
12. 다운로드한 메타데이터를 사용하여 Cisco Umbrella "Other" SAML 마법사를 실행합니다. 3단계에서는 메타데이터를 업로드해야 합니다.



115001186107

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.