SWG SAML 인증에 Umbrella의 고정 메타데이터 URL 활용

목차

소개

이 문서에서는 SWG(Secure Web Gateway) SAML 인증을 위해 Umbrella의 고정 메타데이터 URL을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella SWG를 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.

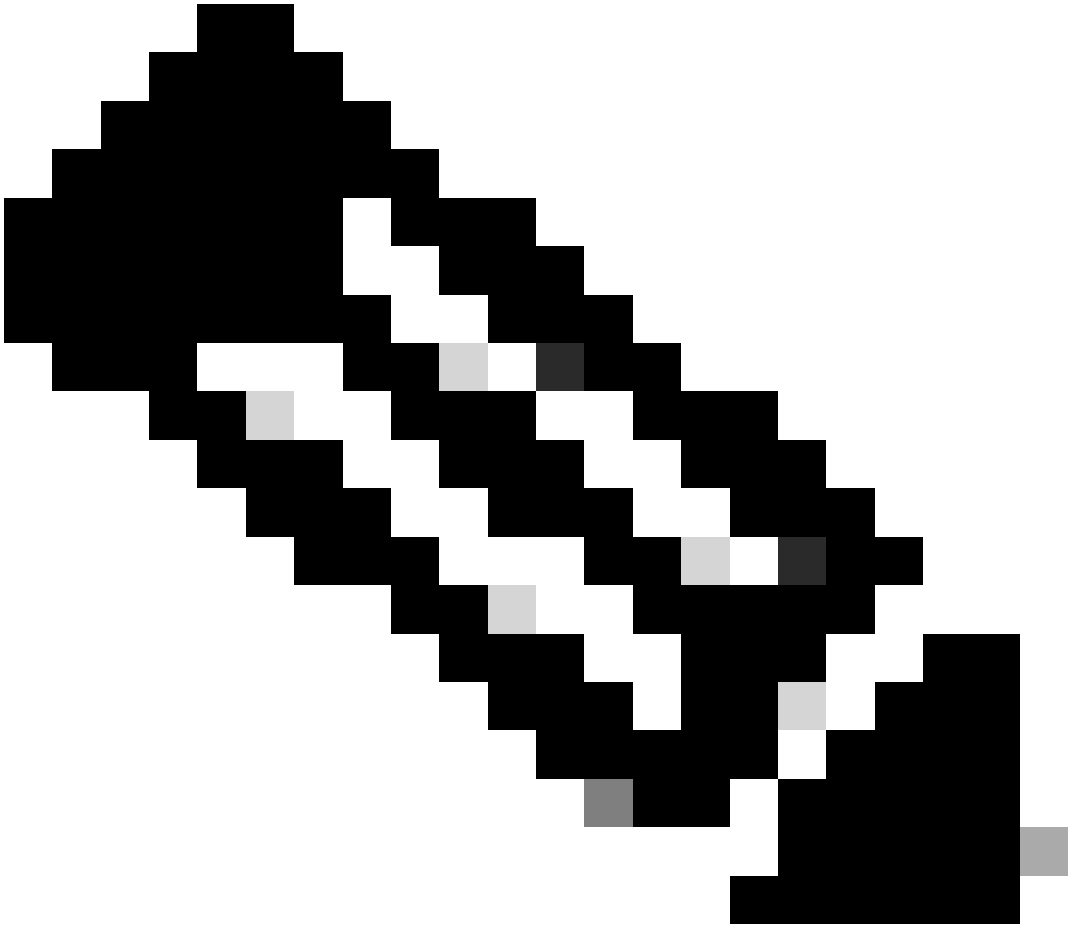
고정 메타데이터 URL

Umbrella SWG에 대한 SAML 인증을 활용할 경우 Cisco는 인증서 정보를 IdP(Identity Provider)로 가져오기 위한 두 가지 옵션을 제공합니다. 이것은 우리의 요청 서명 인증서를 확인 하는 IdP에 필요 합니다.

1. 고정 메타데이터 URL을 통한 자동 구성: https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. 새 서명 인증서의 수동 가져오기 이 작업은 인증서가 교체됨에 따라 매년 수행해야 합니다.

첫 번째 옵션은 이제 메타데이터의 URL 기반 자동 업데이트를 지원하는 IdP(ID 공급자)에 대한 기본 설정 방법입니다. 여기에는 Microsoft AD FS 및 Ping ID와 같은 인기 있는 IdP가 포함됩니다. 이 점은 IdP가 수동 개입 없이 매년 자동으로 새로운 인증서를 가져옵니다.



참고: 많은 IDP는 SAML 요청 서명의 검증을 수행하지 않으므로 이러한 단계가 필요하지 않습니다. 확실하지 않은 경우 ID 공급자 공급업체에 문의하여 확인하십시오.

요구 사항

메타데이터 URL에 액세스하기 위한 요건

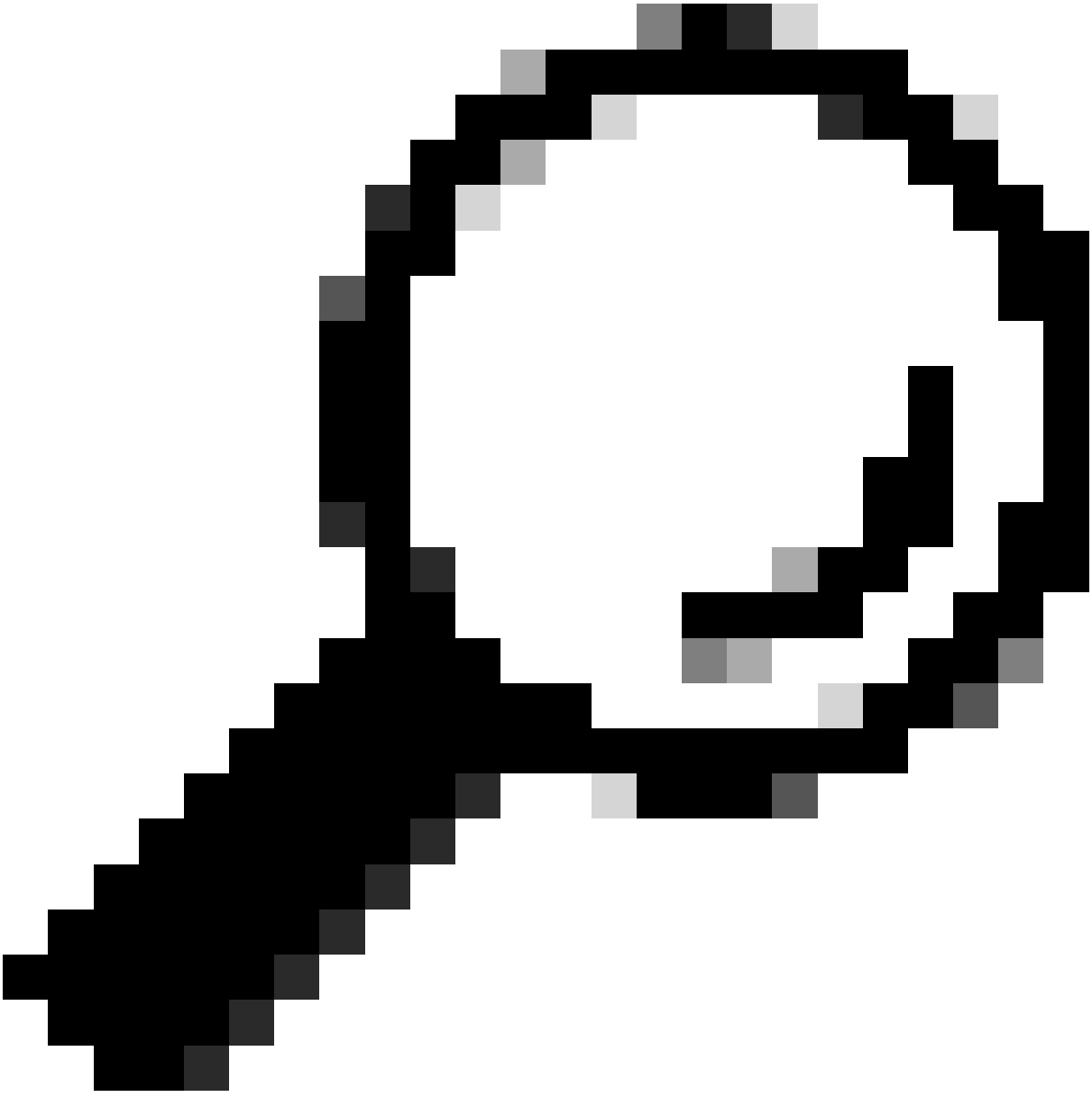
- URL(예: ADFS, Ping)에서 서비스 공급자 메타데이터의 자동 업데이트를 지원하는 IdP
- IdP 플랫폼이 메타데이터 URL 및 연결된 인증 기관 URL에 액세스할 수 있어야 합니다.
- IdP 플랫폼에서도 인증서 자체의 인증 기관 URL에 액세스할 수 있어야 합니다
- IdP 플랫폼이 메타데이터 URL에 안전하게 연결하려면 TLS 1.2를 지원해야 합니다. IDP 응용 프로그램에서 .NET Framework 4.6.1 또는 이전 버전을 사용하는 경우 Microsoft 설명서에 따

라 추가 구성이 필요할 수 있습니다.

예: Microsoft AD FS

고정 메타데이터 URL은 Umbrella에 대한 당사자 Trust 설정을 편집하여 구성할 수 있습니다.

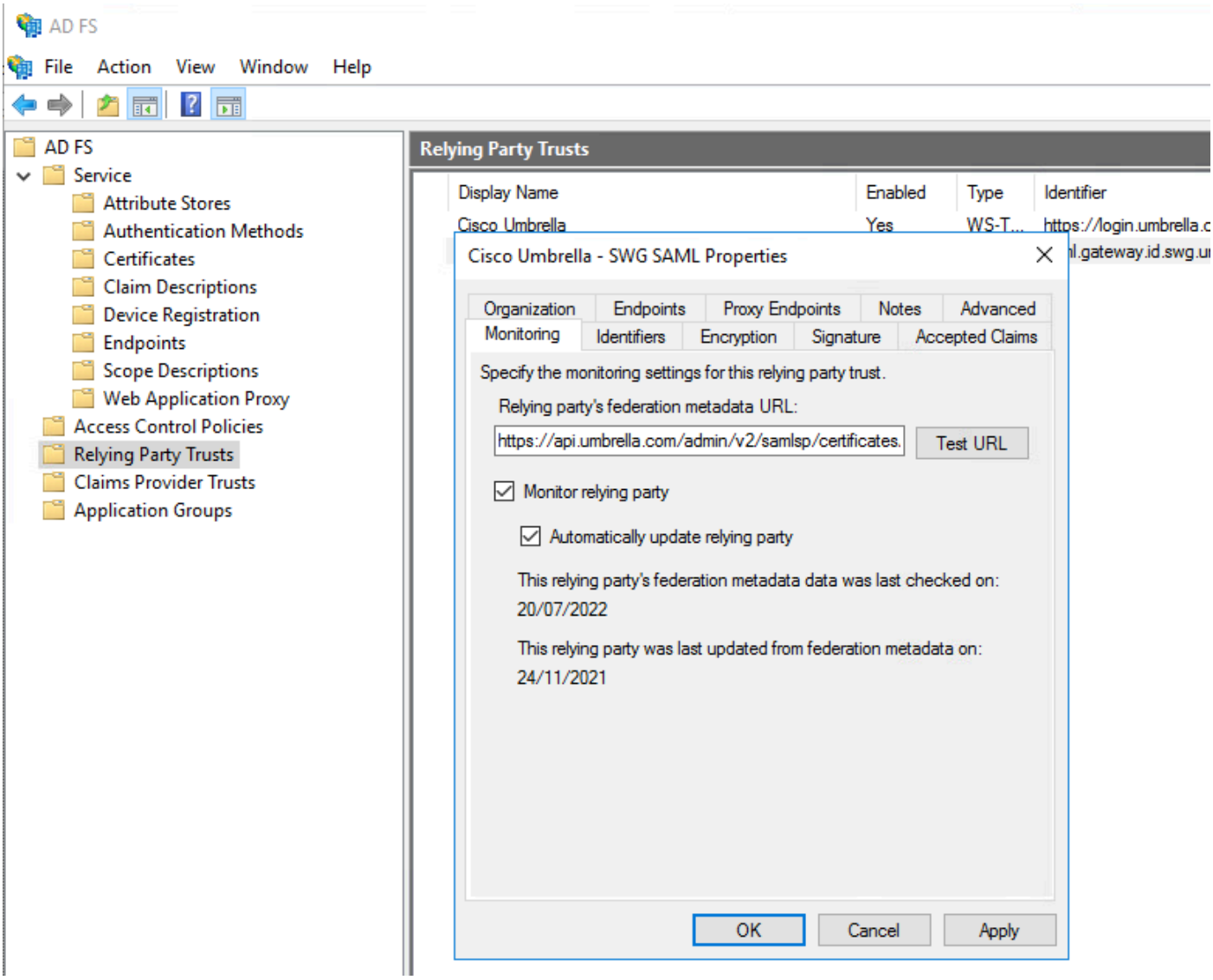
1. Monitoring(모니터링) 탭으로 이동하고 메타데이터 URL을 입력합니다.
2. Monitor Relying Party(신뢰 당사자 모니터링)를 선택하고 Automatically Update Relying Party(신뢰 당사자 자동 업데이트)를 선택합니다.



팁: AD FS가 URL에 성공적으로 연결되었는지 확인하려면 Test URL(URL 테스트) 버튼을 선택합니다.

---

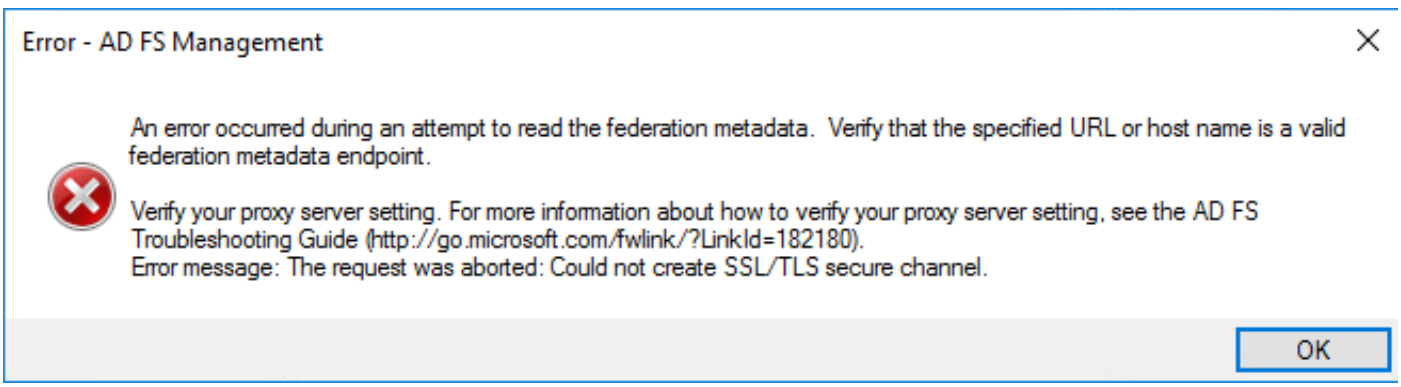
3. Apply를 선택합니다.



ADFS_RelyingPartyTrust.png

오류 트러블슈팅

오류 메시지가 표시되면 페더레이션 메타데이터를 읽는 동안 오류가 발생했습니다. 지정된 URL 또는 호스트 이름이 유효한 페더레이션 메타데이터 끝점인지 확인하십시오." URL을 테스트할 때 이는 일반적으로 강력한 암호화를 사용하고 TLS 1.2를 지원하기 위해 .NET Framework 버전을 설정하는 데 레지스트리 변경이 필요함을 나타냅니다.



ADFSmetadata_TLS_error.png

이러한 변경 사항에 대한 자세한 내용은 Microsoft 설명서의 .Net Framework 섹션에 게시됩니다.

그러나 일반적으로 이 키를 생성한 다음 ADFS Management Console을 닫았다가 다시 열어야 합니다.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

제한: 조직별 EntityID 기능

Umbrella SAML Org-Specific EntityID 기능을 사용하는 경우 URL 기반 메타데이터 업데이트 메커니즘을 사용하지 않아야 합니다. 조직별 엔터티 ID는 동일한 ID 공급자에 연결된 여러 Umbrella 조직이 있는 경우에만 적용됩니다. 이 시나리오에서는 각 IDP 컨피그레이션에 인증서를 수동으로 추가해야 합니다.

수동 인증서 가져오기(대체)

IdP가 URL 기반 업데이트를 지원하지 않는 경우 ID 공급자에게 매년 새 Umbrella 요청 서명 인증서를 수동으로 가져와야 합니다.

- 인증서는 만료일 직전에 매년 공지 포털에 제공됩니다. 알림을 위해 포털에 가입
- IdP의 서비스 공급자/신뢰 당사자 인증서 목록에 새 인증서를 추가합니다.
    - 현재 인증서를 삭제하지 마십시오. Umbrella는 만료 시까지 이전 인증서로 서명을 계속합니다.
- IdP에 서비스 공급자/신뢰 당사자 인증서를 가져올 수 있는 기능이 없는 경우 이는 SAML 요청을 검증하지 않는다는 강력한 표시이며 추가 작업이 필요하지 않습니다. IdP 공급업체에 문의하여 확인하십시오.

새 인증서를 가져온 후 "UPN is not configured" 오류가 발생하면 오류가 발생했음을 나타냅니다. 트러블슈팅은 다음 문서를 참조하십시오. SWG SAML - UPN 구성되지 않음 오류

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.