SWG SAML에서 Umbrella 인증서 갱신 후 UPN 구성되지 않음 오류 트러블슈팅

목차

소개

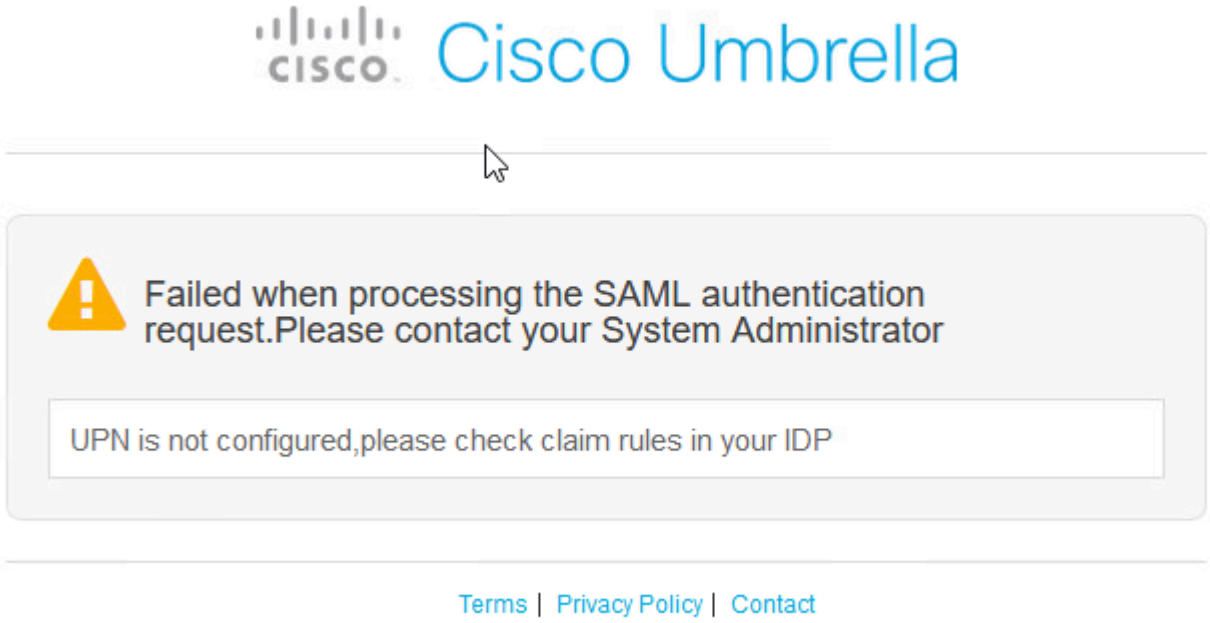
이 문서에서는 Umbrella SAML 서명 인증서를 갱신한 후 "UPN not configured" 오류를 해결하는 방법을 설명합니다.

개요

"UPN not configured"는 여러 가지 이유로 발생할 수 있는 일반적인 오류입니다. 한 가지 가능한 원인은 매년 갱신되는 Umbrella SAML 서명 인증서의 만료와 관련이 있습니다. 인증서 만료에 대한 최신 정보는 공지 포털을 참조하십시오.

Umbrella 인증서가 만료되고 사용자가 조치를 취하지 않은 경우 사용자는 다음과 같은 잠재적인 오류와 함께 인터넷 액세스로부터 차단됩니다.

- SWG를 통해 웹을 탐색할 때 Umbrella 브랜드 "UPN Not Configured" 오류 발생
- ID 제공자가 제공한 다른 오류



이 문서에서는 오류를 유발하는 두 가지 시나리오에 대해 설명합니다.

- 시나리오 1 - 새 Umbrella 인증서를 가져온 후 오류 발생
- 시나리오 2 - Umbrella 인증서 만료 후 오류

영향

SWG에 대한 새 사용자 로그온이 실패하여 인터넷 액세스가 차단됩니다. 이는 모든 사용자에게 반드시 적용되는 것은 아니지만 다음과 같은 경우에 트리거됩니다.

- 사용자의 세션이 재인증 설정(예: daily)으로 인해 만료됩니다.
- 새 사용자가 로그온합니다
- 사용자가 브라우저 캐시를 지우거나 새 브라우저를 사용합니다.

시나리오 1 - 새 Umbrella 인증서를 가져온 후 오류 발생

변경 후 바로 오류가 발생하는 경우(예: Umbrella의 인증서 갱신 준비) 인증서 가져오기에서 오류가 발생했을 가능성이 높습니다.

현재 및 새 Umbrella 인증서를 모두 가져와야 합니다.

인증서 갱신 준비 Umbrella는 새 인증서를 사용할 수 있도록 하지만 만료 시간까지 서명에 새 인증서가 사용되지 않습니다. 따라서 IdP 컨피그레이션에는 Service Provider/Relying Party 컨피그레이션에 나열된 두 개의 인증서가 있어야 합니다. 이 문제를 해결하려면 메타데이터에서 다시 구성하십시오.

- 현재 인증서 - 만료 예정일 포함

- Future Certificate(향후 인증서) - 다음 해에 유효합니다.

특성 클레임 맵이 올바른지 확인합니다.

서비스 공급자/신뢰 당사자를 다시 구성한 경우, IdP가 SAML 응답을 검증하는 데 필요한 특성을 보내는지 확인하기 위해 추가 컨피그레이션을 변경해야 합니다. 이는 클레임 맵을 다시 만들어야 하는 Microsoft AD FS에서 일반적으로 사용됩니다.

시나리오 2 - Umbrella 인증서 만료 후 오류

Umbrella 인증서가 만료되고 IdP가 변경되지 않은 후에 오류가 발생하는 경우

새 인증서를 ID 공급자로 가져왔는지 확인합니다.

문제를 해결하려면 새 인증서를 ID 공급자로 수동으로 가져옵니다. 인증서 갱신이 가까워지면 공지 포털에서 새 인증서를 사용할 수 있습니다.

(권장) 자동 메타데이터 업데이트 구성

이제 Umbrella는 원활한 메타데이터 업데이트에 사용할 수 있는 고정 메타데이터 URL을 제공합니다. 다음 인증서 롤오버 중에 수동 작업을 방지하려면 이 방법을 구성하는 것이 좋습니다.

ID 제공자가 CRL(Certificate Revocation List) 서버 주소에 액세스할 수 있는지 확인합니다

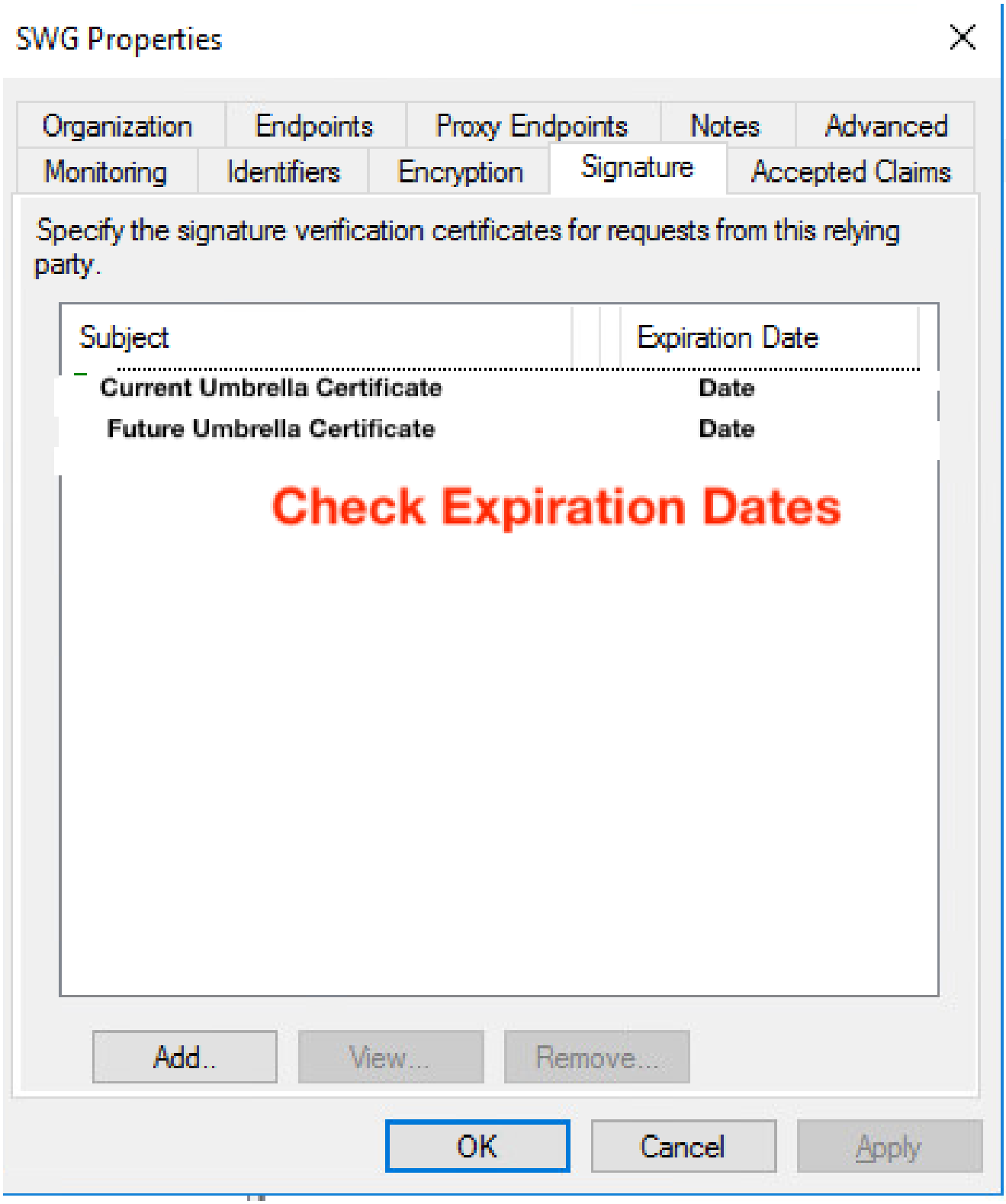
이제 Umbrella는 다른 인증 기관을 사용하므로 IdP 서버에서 다음 CRL/OCSP 주소를 사용할 수 있는지 확인합니다.

- http://validation.identrust.com
- http://commercial.ocsp.identrust.com

Microsoft AD FS - 수동 인증서 가져오기 예

Microsoft AD FS는 요청 서명의 유효성을 검사하는 것으로 알려진 자주 사용되는 IdP입니다. 인증서는 다음과 같이 업데이트할 수 있습니다.

- AD FS 관리 열기
- Relying Party Trust를 확장하고 Umbrella SWG용 RP 찾기
- ADFS에서 Relying Party(신뢰 당사자)를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 선택합니다.
- Signing(서명) 탭에서 새 인증서를 업로드합니다



인증서 만료일이 가까워지면 Cisco에서 제공하는 메타데이터에 원활한 롤오버를 준비할 수 있도록 여러 인증서가 포함됩니다. 현재 인증서가 여전히 유효한 경우 삭제하지 마십시오. Cisco는 만료 날짜/시간까지 현재 인증서를 사용하여 계속 서명합니다.

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.