SMA에서 SAML에 대한 "메타데이터 정보를 검색하는 동안 오류가 발생했습니다." 오류 트러블슈팅

목차

소개

이 문서에서는 SMA(Security Management Appliance)에서 SAML(Security Assertion Markup Language)에 대한 "메타데이터 정보를 검색하는 동안 오류가 발생했습니다" 오류를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AD FS(Active Directory Federation Services)
- SMA와의 SAML 통합
- OpenSSL 설치

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SMA AsyncOs 버전 11.x.x
- SMA AsyncOs 버전 12.x.x

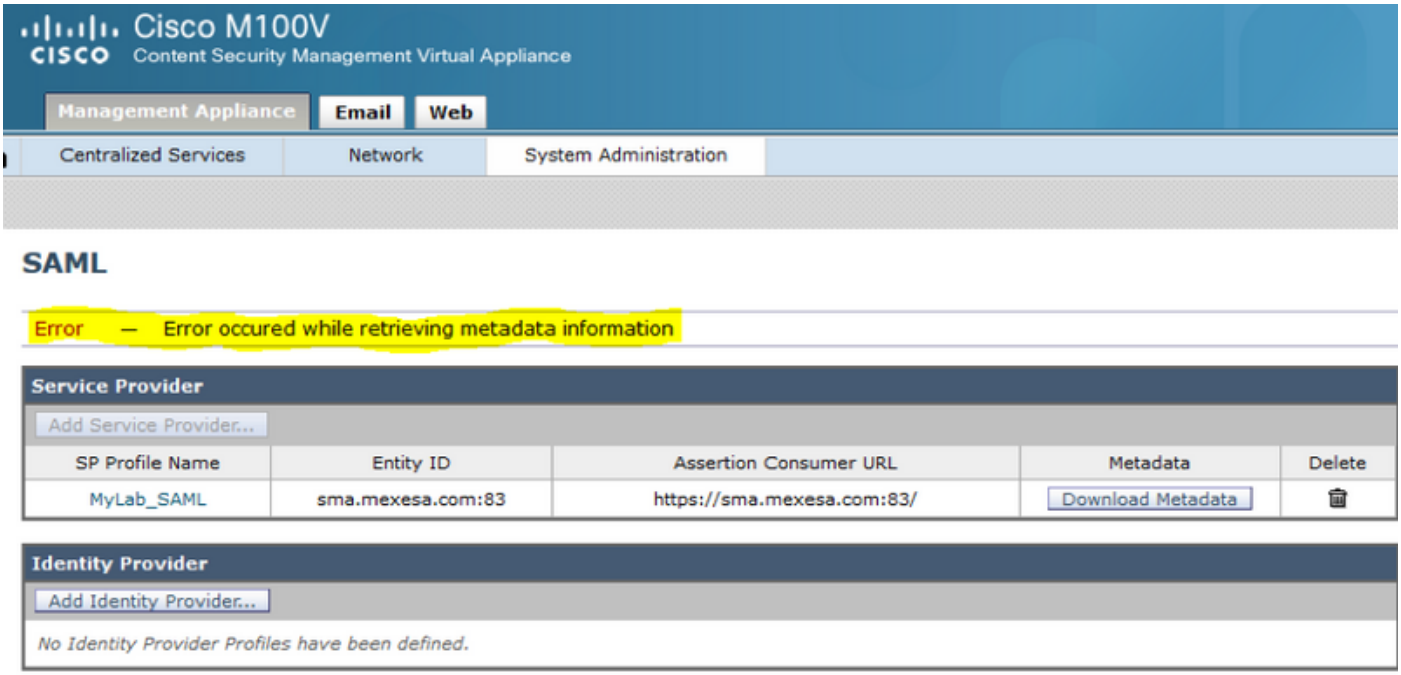
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이제 Cisco Content Security Management Appliance는 SAML 2.0 SSO(Single Sign-On)를 지원하므로 최종 사용자가 스팸 격리에 액세스하고 조직 내의 다른 SAML 2.0 SSO 지원 서비스에 액세스하는 데 사용되는 것과 동일한 자격 증명을 사용할 수 있습니다. 예를 들어 Ping Identity를 SAML IdP(ID 제공자)로 활성화하고 Rally, Salesforce 및 Dropbox에 SAML 2.0 SSO가 활성화된 계정이 있습니다. SAML 2.0 SSO를 SP(서비스 공급자)로 지원하도록 Cisco Content Security Management Appliance를 구성할 경우 최종 사용자가 한 번에 로그인하고 스팸 격리를 비롯한 모든 서비스에 액세스할 수 있습니다.

문제

SAML에 대한 메타데이터 다운로드를 선택하면 이미지에 표시된 대로 "메타데이터 정보를 검색하는 동안 오류가 발생했습니다"라는 오류가 표시됩니다.



솔루션

1단계. ESA(Email Security Appliance)에서 새 자체 서명 인증서를 생성합니다.

이미지에 표시된 대로 CN이 엔티티 ID URL과 동일하지만 포트 번호가 없는지 확인합니다.

2단계. 확장명이 .pfx인 새 인증서를 내보내고 암호를 입력한 다음 컴퓨터에 저장합니다.

3단계. Windows 터미널을 열고 이 명령을 입력한 다음 이전 단계의 암호를 입력합니다.

- 다음 명령을 실행하여 개인 키를 내보냅니다.

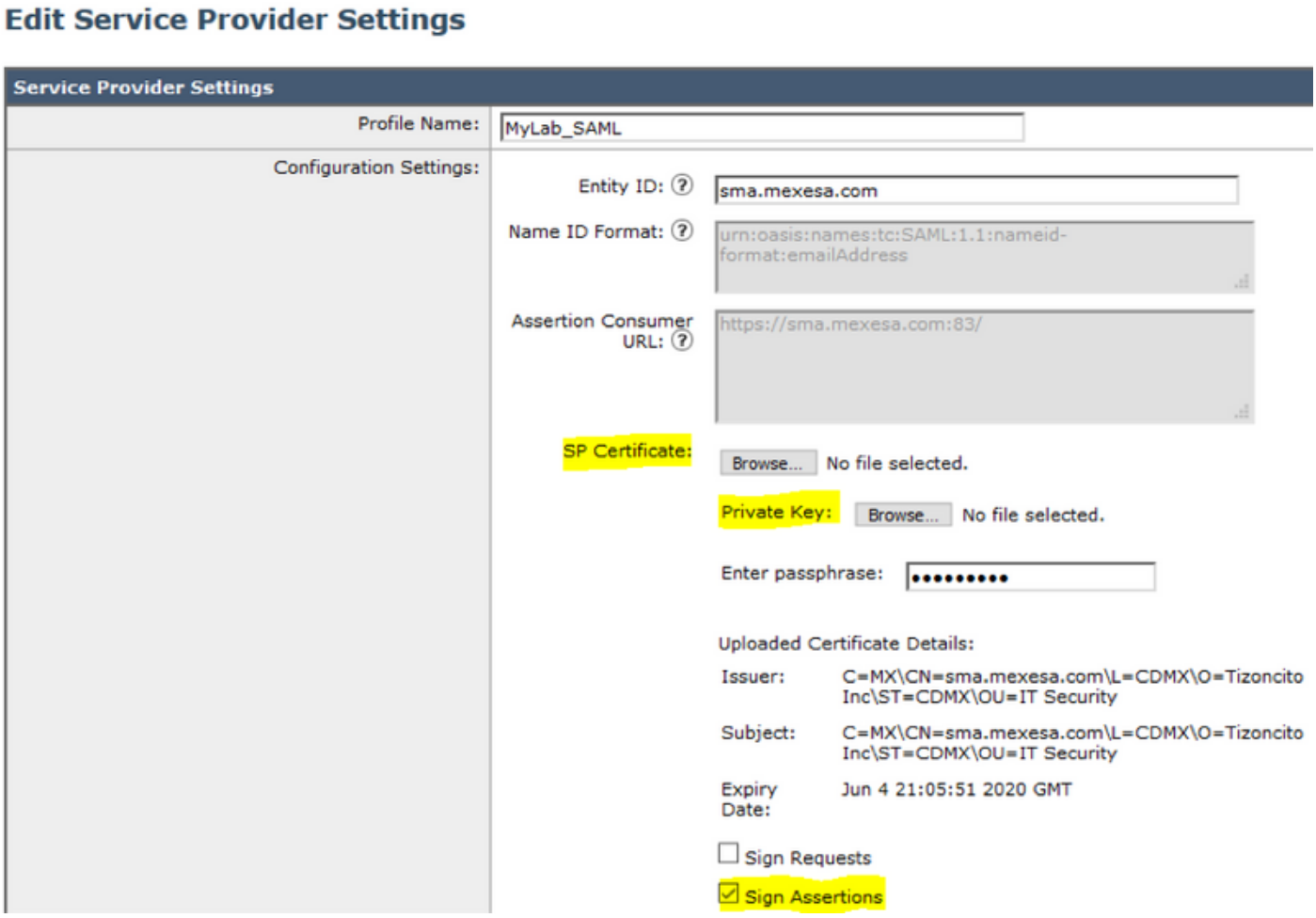
```
openssl pkcs12 -in created_certificate.pfx -nocerts -out certificateprivatekey.pem -nodes
```

- 다음 명령을 실행하여 인증서를 내보냅니다.

```
openssl pkcs12 -in created_certificate.pfx -nokeys -out certificate.pem
```

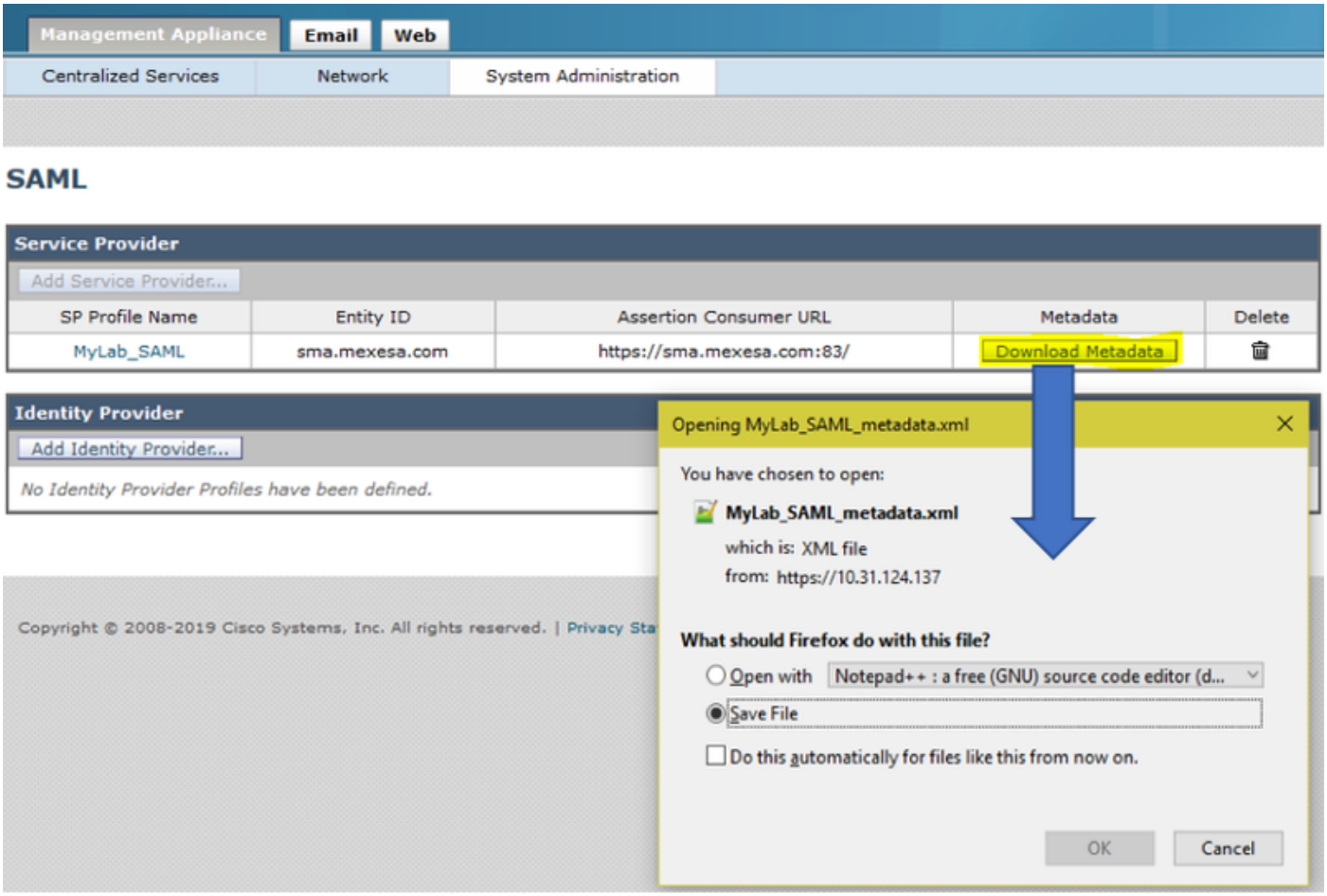
4단계. 이 프로세스가 끝나면 다음 두 개의 새 파일이 있어야 합니다. **certificateprivatekey.pem** 및 **certificate.pem**. 서비스 공급자 프로필의 두 파일을 모두 업로드하고 인증서를 내보내는 데 사용하는 것과 동일한 암호를 사용합니다.

5단계. SMA에서 두 파일이 모두 .PEM 형식이어야 작동합니다(그림에 나와 있음).



6단계. Sign Assertions(어설션 서명) **확인란을** 선택합니다.

7단계. 변경 사항을 제출하고 커밋합니다. 이미지에 표시된 대로 메타데이터를 다운로드할 수 있어야 합니다.



관련 정보

- AsyncOS 11.0 for Cisco Content Security Management Appliance 사용 설명서 - GD(일반 배포)
- 기술 지원 및 문서 – Cisco Systems

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.