ACI 결함 코드 F3081 해결: SAML 인증서 만료

목차

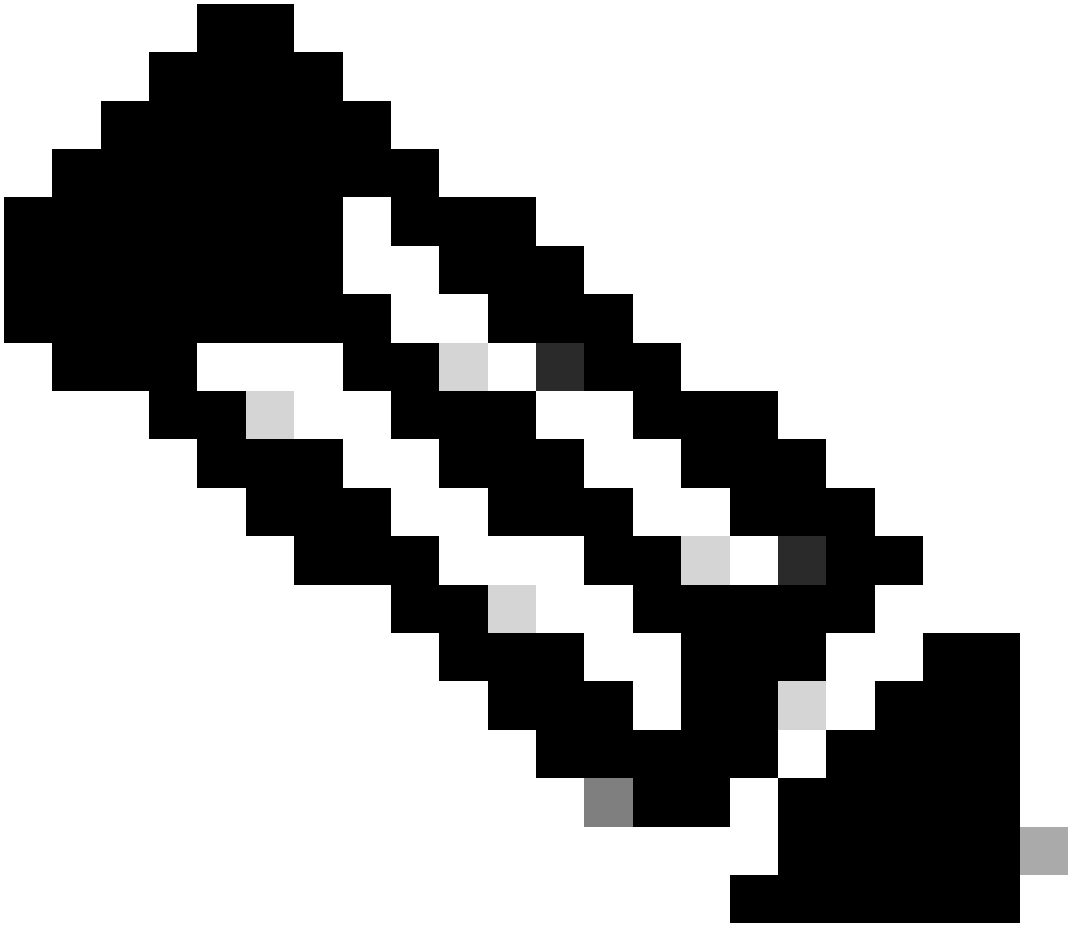
소개

이 문서에서는 ACI Fault F3081 및 해당 교정 단계에 대해 설명합니다.

배경 정보

이 결함은 APIC에서 1개월 후 SAML X.509 인증서가 만료될 때 발생합니다.

```
F3081: fltAaaSamlEncCertSamlEncCertExpiring
Severity: major
Explanation: This fault occurs when the SAML X.509 Certificate is going to expire in one month.
Recommended Action: If you see this fault, take the following actions:
Update SAML X.509 Certificate soon.
```



참고: SAML을 구현하지 않아도 동일한 상황이 발생할 수 있습니다. 그러나 SAML을 사용하지 않을 경우 시스템에 영향을 미치지 않습니다.

Intersight Connected ACI Fabric

이 결함은 사전 대응적 ACI 계약의 일부로 적극적으로 모니터링됩니다.

Intersight에 연결된 ACI 패브릭이 있는 경우 Intersight에 연결된 ACI 패브릭 내에서 이 결함의 인스턴스가 발견되었음을 알리기 위해 사용자를 대신하여 서비스 요청이 생성됩니다.

빠른 시작 - 결함 해결

1. SAML X.509 인증서 만료 상태를 확인합니다. 만료 또는 만료 결함이 표시되면 F3081이 발생합니다.

2. 인증서 발급자가 Cisco 또는 타사인지 확인합니다.

3. 발급자가 Cisco인 경우 SAML 암호화 키 쌍을 다시 생성합니다.

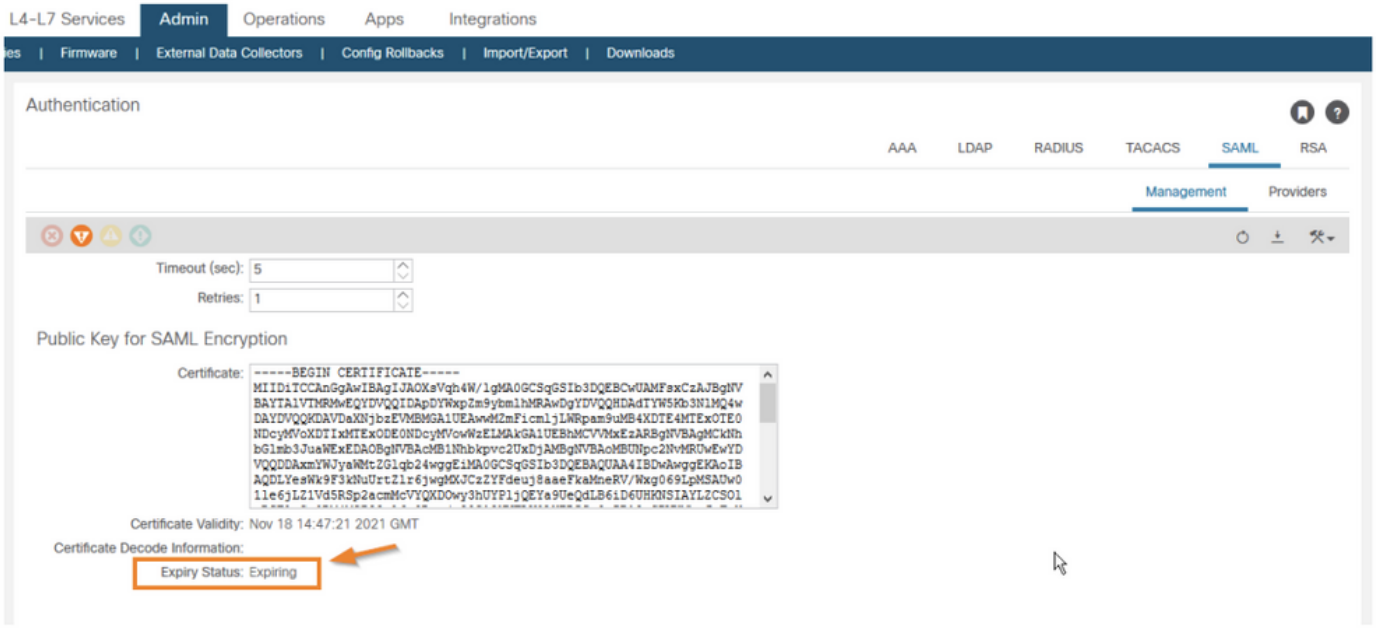
결함 해결을 위한 세부 단계

SAML X.509 인증서 만료 상태 확인

APIC GUI를 통해

1. 로 Admin > AAA > Authentication > SAML > Management 이동합니다.

2. SAML X.509 인증서 만료 상태를 확인합니다. Expiring 인증서가 한 달 내에 만료됨을 의미합니다.



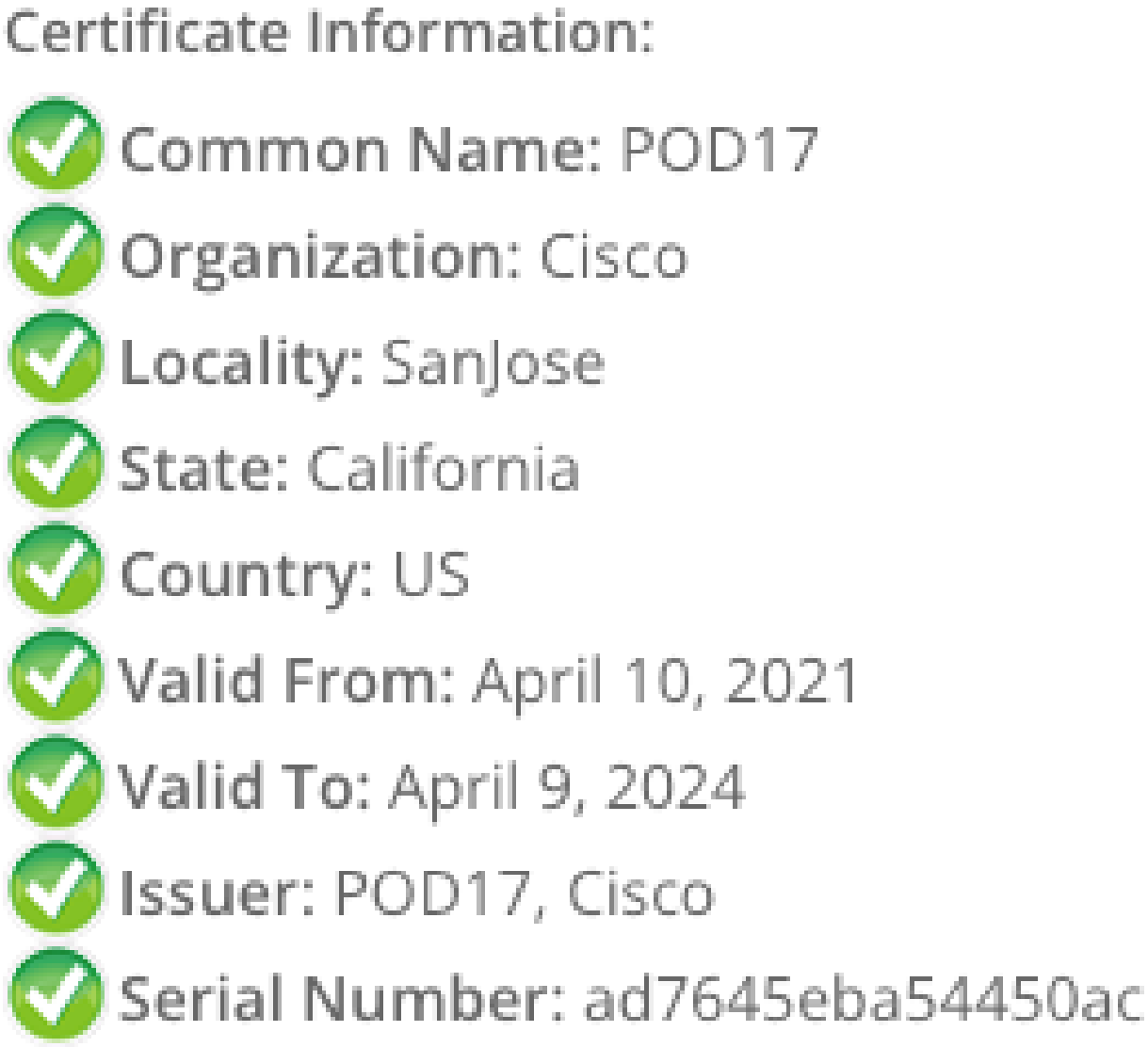
SAML X.509 인증서 재생성 및 갱신

이 결함을 해결하려면 인증서를 다시 생성 및 갱신하고 만료 날짜를 연장하여 오류를 지울 수 있습니다.

SAML X.509 인증서를 다시 생성해도 아무런 영향이 없습니다.

계속하기 전에 인증서의 CA(Certificate Authority) 발급자가 Cisco인지 또는 서드파티 엔터티인지 다시 확인하십시오.

APIC에서 인증서 내용을 가져오려면 모든 X.509 디코더의 인증서를 디코딩하여 인증서 매개변수를 가져옵니다.

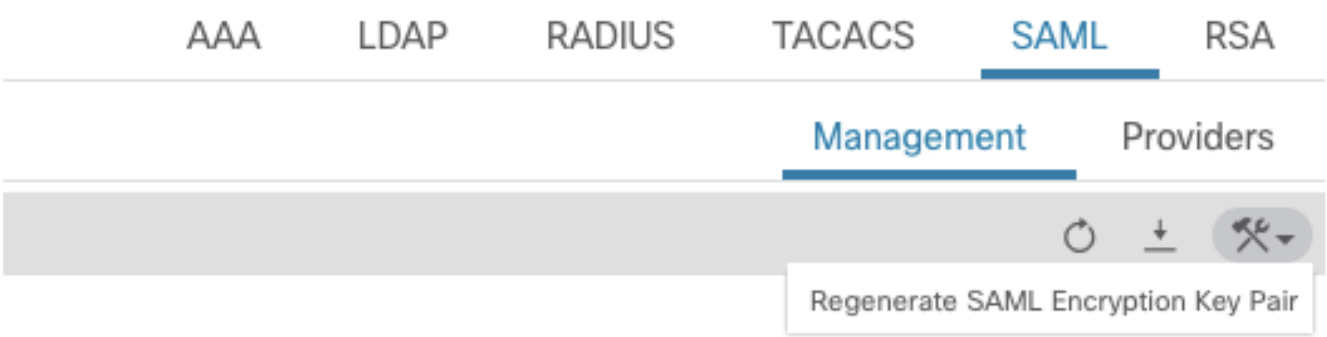


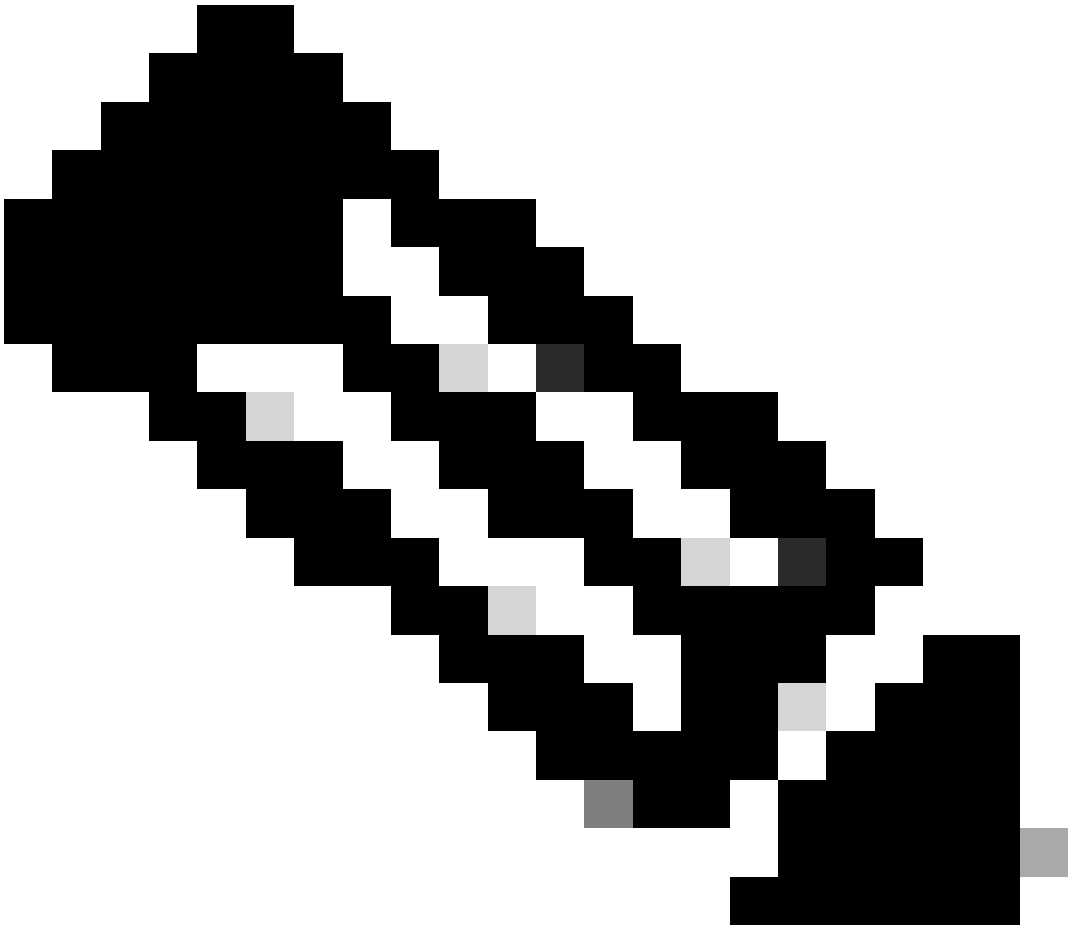
서드파티 CA에서 인증서를 발급한 경우 CA에 문의하여 SAML X.509 인증서를 갱신하십시오.

그러나 인증서 발급자가 Cisco인 경우 다음 단계를 진행할 수 있습니다.

APIC GUI 사용

1. 로 Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair 이동합니다.



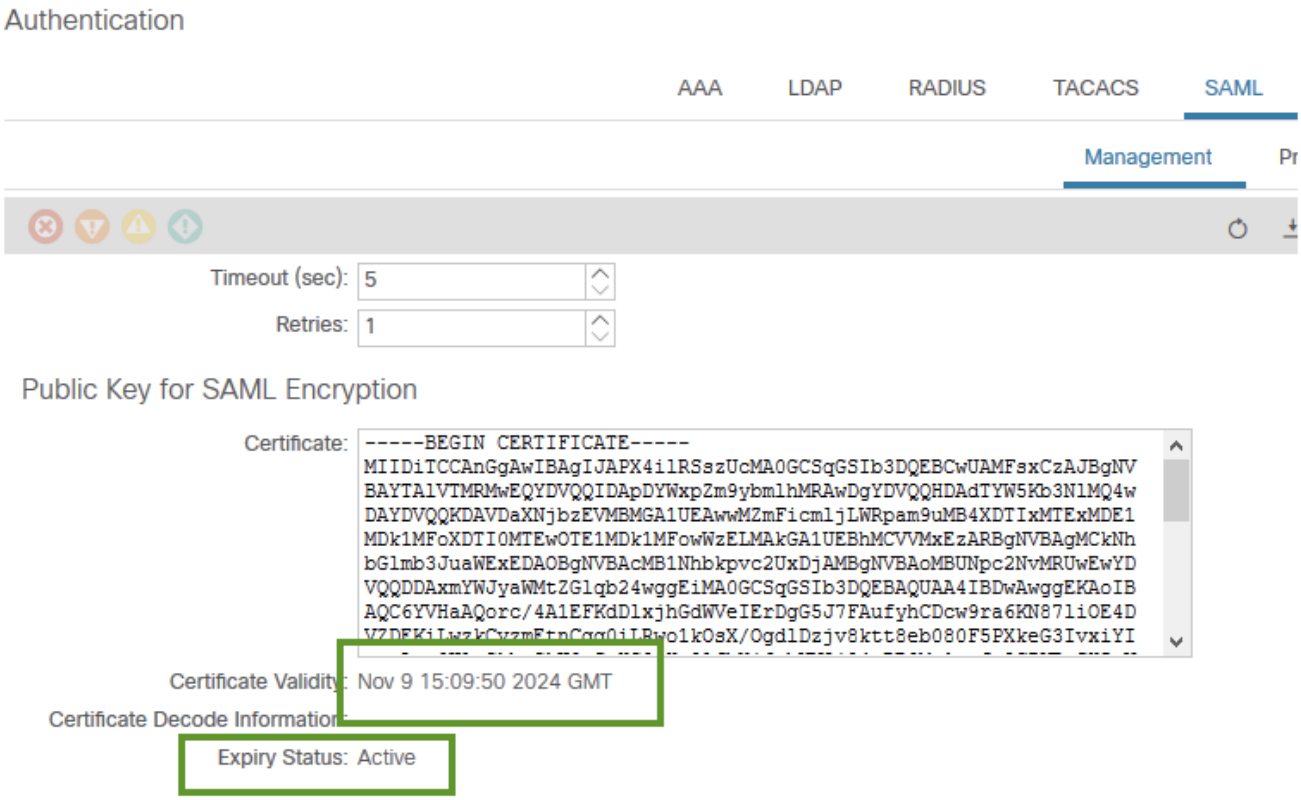


참고: 인증서를 갱신하면 Certificate Validity(인증서 유효)에 표시된 만료 날짜가 갱신 날짜로부터 3년 후로 연장됩니다.

만료 상태가 활성으로 변경되었는지 확인

APIC GUI를 통해

1. 로 Admin > AAA > Authentication > SAML > Management 이동합니다.



추가 정보

SAML은 관리자가 정의된 Cisco 협업 애플리케이션 중 하나에 로그인한 후 해당 애플리케이션에 원활하게 액세스할 수 있는 XML 기반 개방형 표준 데이터 형식입니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 서비스 공급자가 사용자를 인증하기 위해 사용하는 인증 프로토콜입니다. SAML을 사용하면 IdP(Identity Provider)와 서비스 공급자 간에 보안 인증 정보를 교환할 수 있습니다.

SAML SSO는 SAML 2.0 프로토콜을 사용하여 Cisco 협업 솔루션을 위한 교차 도메인 및 교차 제품 SSO를 제공합니다. SAML 2.0은 Cisco 애플리케이션에서 SSO를 활성화하고 Cisco 애플리케이션과 IdP 간의 페더레이션을 활성화합니다. SAML 2.0에서는 Cisco 관리 사용자가 보안 웹 도메인에 액세스할 수 있도록 하여 높은 보안 수준을 유지하면서 IdP와 서비스 공급자 간에 사용자 인증 및 권한 부여 데이터를 교환할 수 있습니다. 이 기능은 여러 애플리케이션에서 공통 자격 증명 및 관련 정보를 사용하기 위한 보안 메커니즘을 제공합니다.

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.