Beheben von ACI-Fehlercode F3081: SAML-Zertifikat wird ablaufen

Inhalt

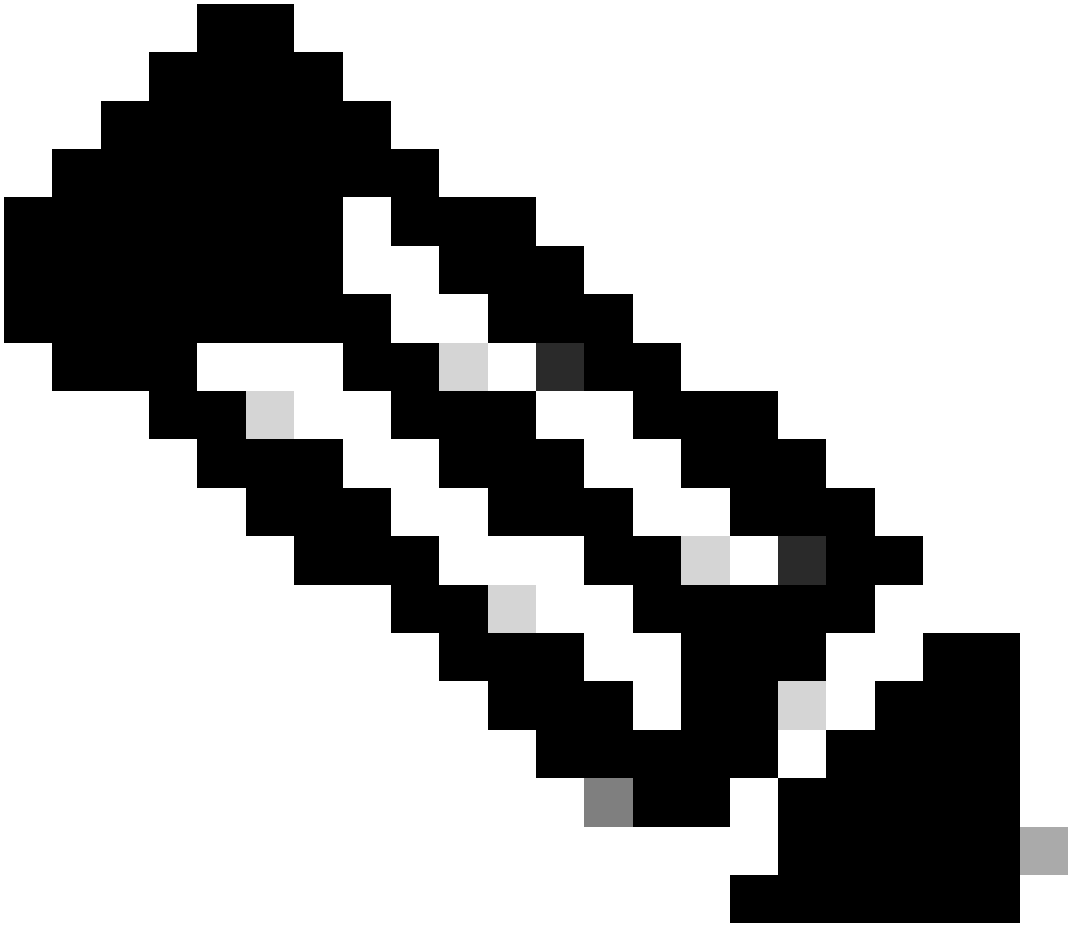
Einleitung

In diesem Dokument werden der ACI-Fehler F3081 und seine Behebungsschritte beschrieben.

Hintergrundinformationen

Dieser Fehler tritt auf, wenn ein SAML X.509-Zertifikat auf einem APIC in einem Monat abläuft.

```
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.
```



Hinweis: Dasselbe kann auch ohne SAML-Implementierung passieren. Wird jedoch SAML nicht verwendet, hat dies keine Auswirkungen auf das System.

Intersight Connected ACI Fabrics

Dieser Fehler wird im Rahmen der proaktiven ACI-Initiativen aktiv überwacht.

Wenn Sie über eine Intersight-verbundene ACI-Fabric verfügen, wird in Ihrem Namen eine Serviceanfrage generiert, um anzugeben, dass Instanzen dieses Fehlers in Ihrer Intersight-verbundenen ACI-Fabric gefunden wurden.

Schnellstart zur Fehlerbehebung

1. Validieren Sie den SAML X.509-Zertifikatsablaufstatus. Wenn der Status "Expiring" oder "Expired Fault" angezeigt wird, wird F3081 ausgelöst.

2. Überprüfen Sie, ob es sich bei dem Zertifikataussteller um Cisco oder einen Drittanbieter

handelt.

3. Wenn es sich beim Issuer um Cisco handelt, fahren Sie mit der Regenerierung des SAML Encryption Key Pair fort.

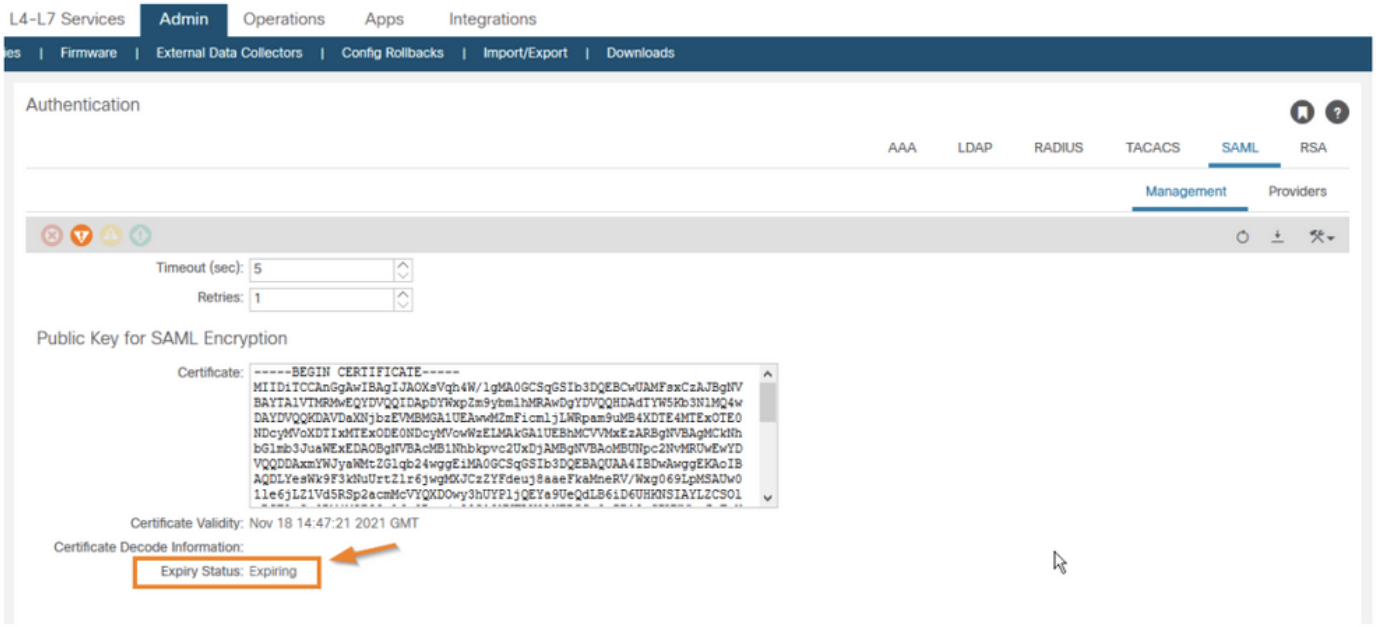
Detaillierte Schritte zur Behebung von Fehlern

SAML X.509-Zertifikatablaufstatus validieren

Über die APIC-GUI

1. Navigieren Sie zu Admin > AAA > Authentication > SAML > Management.

2. SAML X.509-Zertifikatsablaufstatus validieren. bedeutet,Expiring dass das Zertifikat innerhalb eines Monats abläuft.



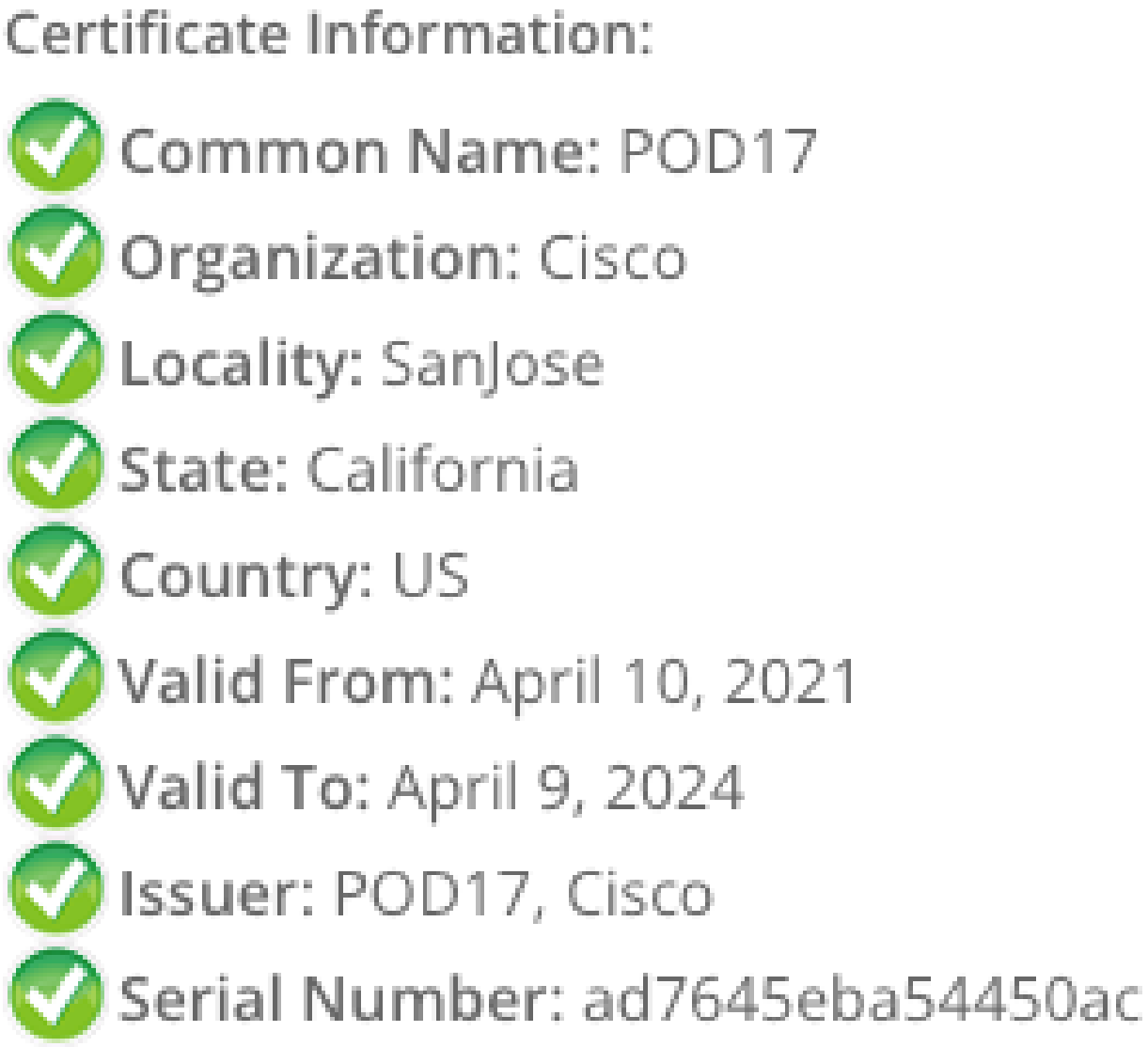
SAML X.509-Zertifikat erneuern und verlängern

Um diesen Fehler zu beheben, können Sie das Zertifikat generieren und erneuern sowie das Ablaufdatum verlängern.

Das Regenerieren des SAML X.509-Zertifikats hat keine Auswirkungen.

Überprüfen Sie vor dem Fortfahren nochmals, ob es sich bei der Zertifizierungsstelle (Certificate Authority, CA), von der das Zertifikat ausgestellt wird, um Cisco oder eine Drittpartei handelt.

Um den Zertifikatsinhalt vom APIC zu erhalten, dekodieren Sie das Zertifikat in einem beliebigen X.509-Decoder, um die Zertifikatparameter zu erhalten:

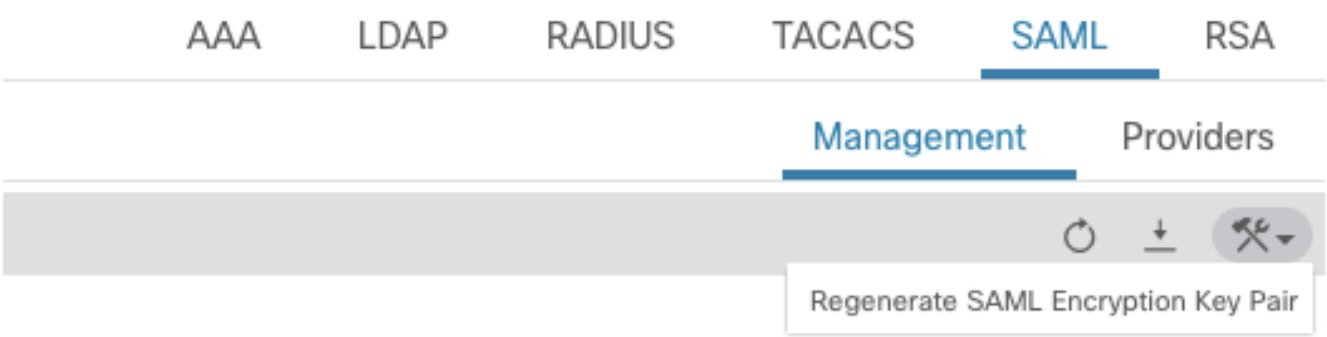


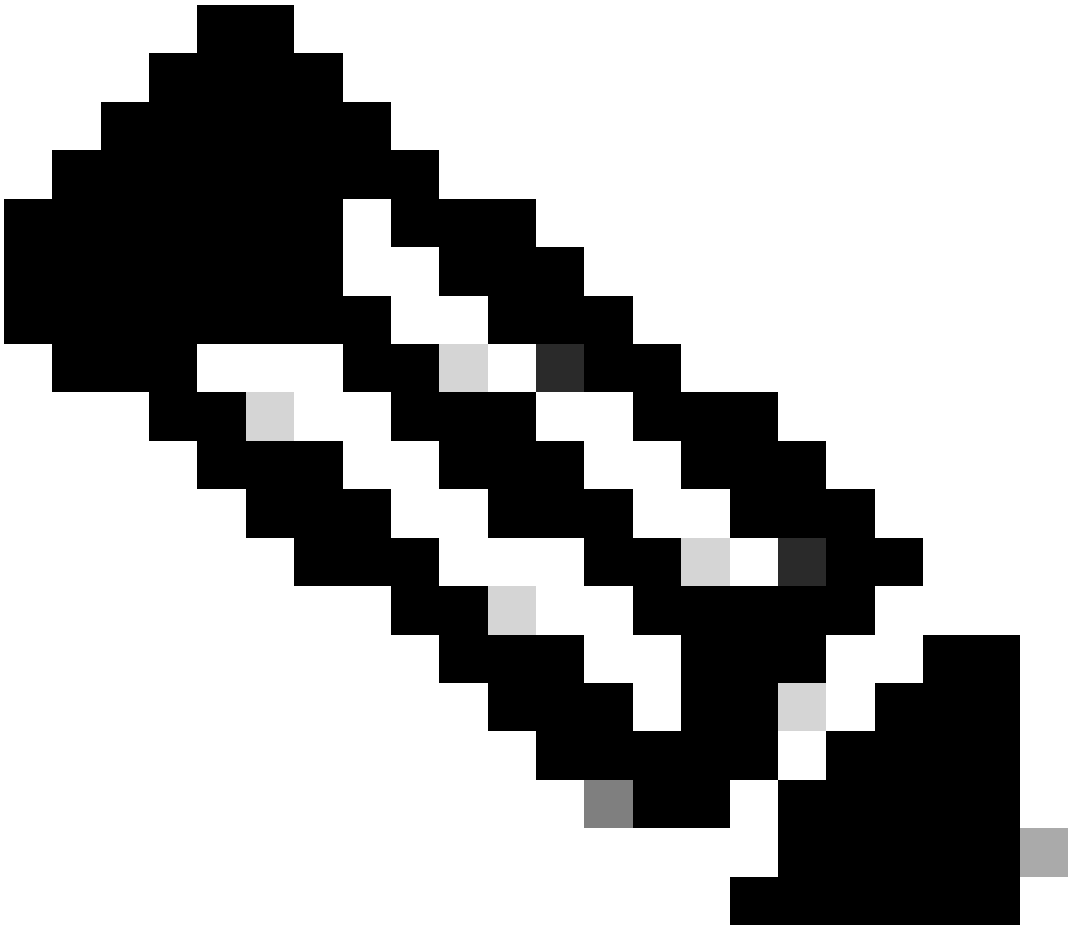
Wenn das Zertifikat von einer Zertifizierungsstelle eines Drittanbieters ausgestellt wurde, wenden Sie sich an die Zertifizierungsstelle, um Ihr SAML X.509-Zertifikat zu erneuern.

Wenn das Zertifikat jedoch von Cisco ausgestellt wird, können Sie mit diesen Schritten fortfahren.

Über die APIC-GUI

1. Navigieren Sie zu Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair.



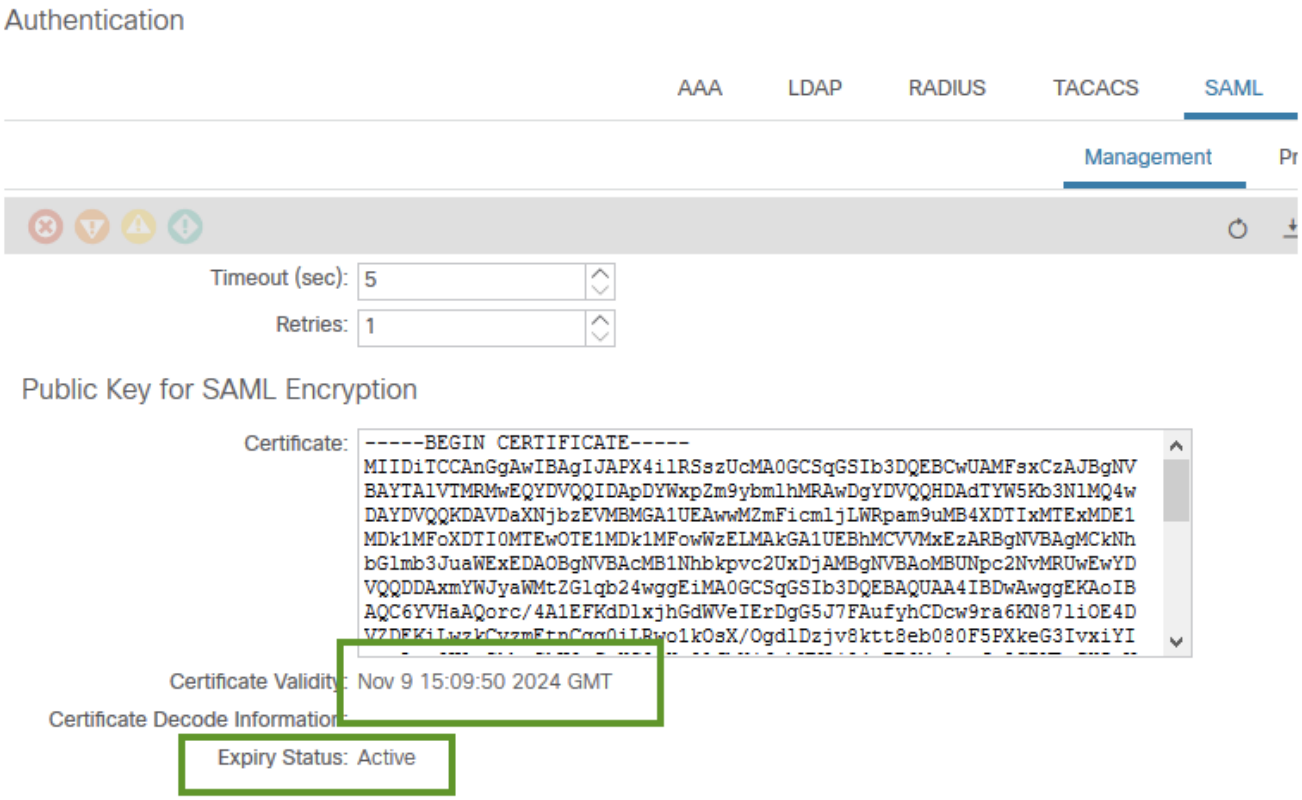


Hinweis: Durch die Verlängerung des Zertifikats wird das in der Gültigkeit des Zertifikats angegebene Ablaufdatum auf ein Datum verlängert, das drei Jahre nach dem Verlängerungsdatum liegt.

Überprüfen, ob Ablaufstatus in "Aktiv" geändert wurde

Über die APIC-GUI

1. Navigieren Sie zu Admin > AAA > Authentication > SAML > Management.



Zusätzliche Informationen

SAML ist ein XML-basiertes, offenes Standarddatenformat, mit dem Administratoren nahtlos auf eine bestimmte Gruppe von Cisco Collaboration-Anwendungen zugreifen können, nachdem sie sich bei einer dieser Anwendungen angemeldet haben. SAML beschreibt den Austausch von sicherheitsrelevanten Informationen zwischen vertrauenswürdigen Geschäftspartnern. Es handelt sich um ein Authentifizierungsprotokoll, das von Dienstanbietern zur Authentifizierung eines Benutzers verwendet wird. SAML ermöglicht den Austausch von Sicherheitsauthentifizierungsinformationen zwischen einem Identity Provider (IdP) und einem Service Provider.

SAML SSO verwendet das SAML 2.0-Protokoll, um domänenübergreifende und produktübergreifende SSO für Cisco Collaboration-Lösungen bereitzustellen. SAML 2.0 ermöglicht SSO für alle Cisco Anwendungen und ermöglicht den Verbund zwischen Cisco Anwendungen und einem IdP. SAML 2.0 ermöglicht Cisco-Administratoren den Zugriff auf sichere Web-Domänen, um Benutzerauthentifizierungs- und -autorisierungsdaten zwischen einem IdP und einem Service Provider auszutauschen, wobei hohe Sicherheitsstufen beibehalten werden. Diese Funktion bietet sichere Mechanismen für die Verwendung allgemeiner Anmeldedaten und relevanter Informationen in verschiedenen Anwendungen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.