

Beheben Sie den Fehler "Fehler beim Abrufen von Metadateninformationen" für SAML in der SMA.

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Fehler "Fehler beim Abrufen von Metadateninformationen" für Security Assertion Markup Language (SAML) in der Security Management Appliance (SMA) beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ADFS (Active Directory-Verbunddienste)
- SAML-Integration mit SMA
- [OpenSSL](#) installiert

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- SMA AsyncOS Version 11.x.x
- SMA AsyncOs Version 12.x.x

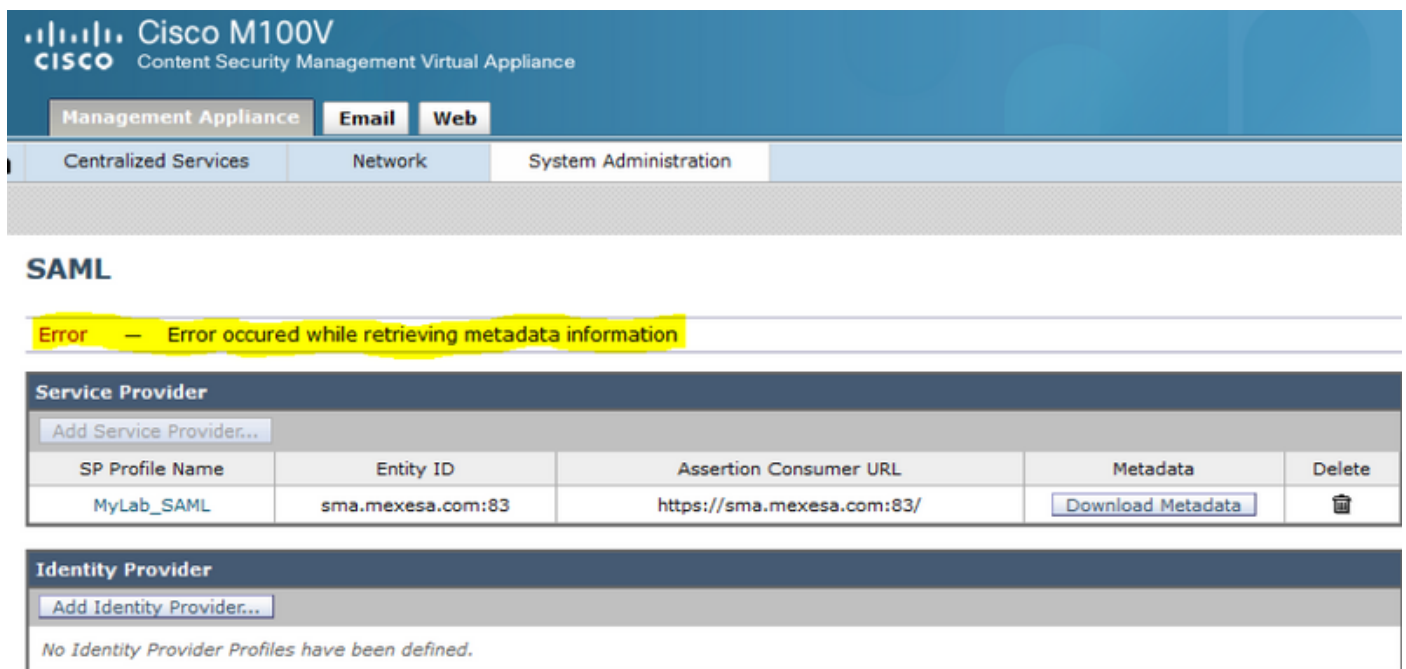
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen


Die Cisco Content Security Management Appliance unterstützt jetzt SAML 2.0 Single Sign-On (SSO), sodass die Endbenutzer auf die Spam-Quarantäne zugreifen und dieselben Anmeldeinformationen verwenden können, die auch für den Zugriff auf andere SAML 2.0 SSO-fähige Dienste innerhalb ihrer Organisation verwendet werden. Sie aktivieren beispielsweise Ping Identity als SAML Identity Provider (IdP) und verfügen über Konten bei Rally, Salesforce und Dropbox, auf denen SAML 2.0 SSO aktiviert ist. Wenn Sie die Cisco Content Security Management Appliance so konfigurieren, dass sie SAML 2.0 SSO als Service Provider (SP) unterstützt, können sich Endbenutzer einmal anmelden und haben Zugriff auf all diese Services, einschließlich Spam Quarantine.

Problem

Wenn Sie Metadaten für SAML herunterladen wählen, erhalten Sie die Fehlermeldung "Fehler beim Abrufen von Metadateninformationen", wie im Bild gezeigt:



The screenshot shows the Cisco M100V Content Security Management Virtual Appliance interface. The top navigation bar includes 'Management Appliance', 'Email', and 'Web'. Below this, there are tabs for 'Centralized Services', 'Network', and 'System Administration'. The main content area is titled 'SAML' and displays an error message: 'Error - Error occured while retrieving metadata information'. Below the error message, there is a table for 'Service Provider' with the following data:

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com:83	https://sma.mexesa.com:83/	Download Metadata	

Below the table, there is a section for 'Identity Provider' with an 'Add Identity Provider...' button and a message: 'No Identity Provider Profiles have been defined.'

Lösung

Schritt 1: Erstellen Sie ein neues selbstsigniertes Zertifikat auf der E-Mail Security Appliance (ESA).

Stellen Sie sicher, dass der allgemeine Name mit der URL für die Element-ID übereinstimmt, jedoch ohne Portnummer, wie in der Abbildung dargestellt:

View Certificate sma.mexesa.com

Add Certificate	
Certificate Name:	MySAML_Cert
Common Name:	sma.mexesa.com
Organization:	Tizoncito Inc
Organization Unit:	IT Security
City (Locality):	CDMX
State (Province):	CDMX
Country:	MX
Signature Issued By:	Common Name (CN): sma.mexesa.com Organization (O): Tizoncito Inc Organizational Unit (OU): IT Security Issued On: Jun 5 20:52:27 2019 GMT Expires On: Jun 4 20:52:27 2020 GMT

Schritt 2: Exportieren Sie das neue Zertifikat mit der Erweiterung .pfx, geben Sie eine Passphrase ein, und speichern Sie es auf Ihrem Computer.

Schritt 3: Öffnen Sie ein Windows-Terminal, und geben Sie diese Befehle ein. Geben Sie im vorherigen Schritt die Passphrase ein.

- Führen Sie den folgenden Befehl aus, um den privaten Schlüssel zu exportieren:

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

- Führen Sie den folgenden Befehl aus, um das Zertifikat zu exportieren:

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

Schritt 4. Am Ende dieses Prozesses müssen Sie zwei neue Dateien haben:

certificateprivatekey.pem und **certificate.pem**. Laden Sie beide Dateien in das Service Provider-Profil hoch, und verwenden Sie dieselbe Passphrase, die Sie zum Exportieren des Zertifikats verwenden.

Schritt 5. Die SMA erfordert, dass beide Dateien im PEM-Format vorliegen, damit sie funktionieren, wie im Bild gezeigt.

Edit Service Provider Settings

Service Provider Settings

Profile Name:

Configuration Settings:

Entity ID:

Name ID Format:

Assertion Consumer URL:

SP Certificate: No file selected.

Private Key: No file selected.

Enter passphrase:

Uploaded Certificate Details:

Issuer: C=MX\CN=sma.mexesa.com\L=CDMX\O=Tizoncito Inc\ST=CDMX\OU=IT Security

Subject: C=MX\CN=sma.mexesa.com\L=CDMX\O=Tizoncito Inc\ST=CDMX\OU=IT Security

Expiry Date: Jun 4 21:05:51 2020 GMT

Sign Requests

Sign Assertions

Schritt 6: Aktivieren Sie das Kontrollkästchen **Assertions signieren**.

Schritt 7. Senden und bestätigen Sie die Änderungen, müssen Sie in der Lage sein, die Metadaten herunterzuladen, wie im Bild gezeigt.

SAML

Service Provider

Add Service Provider...

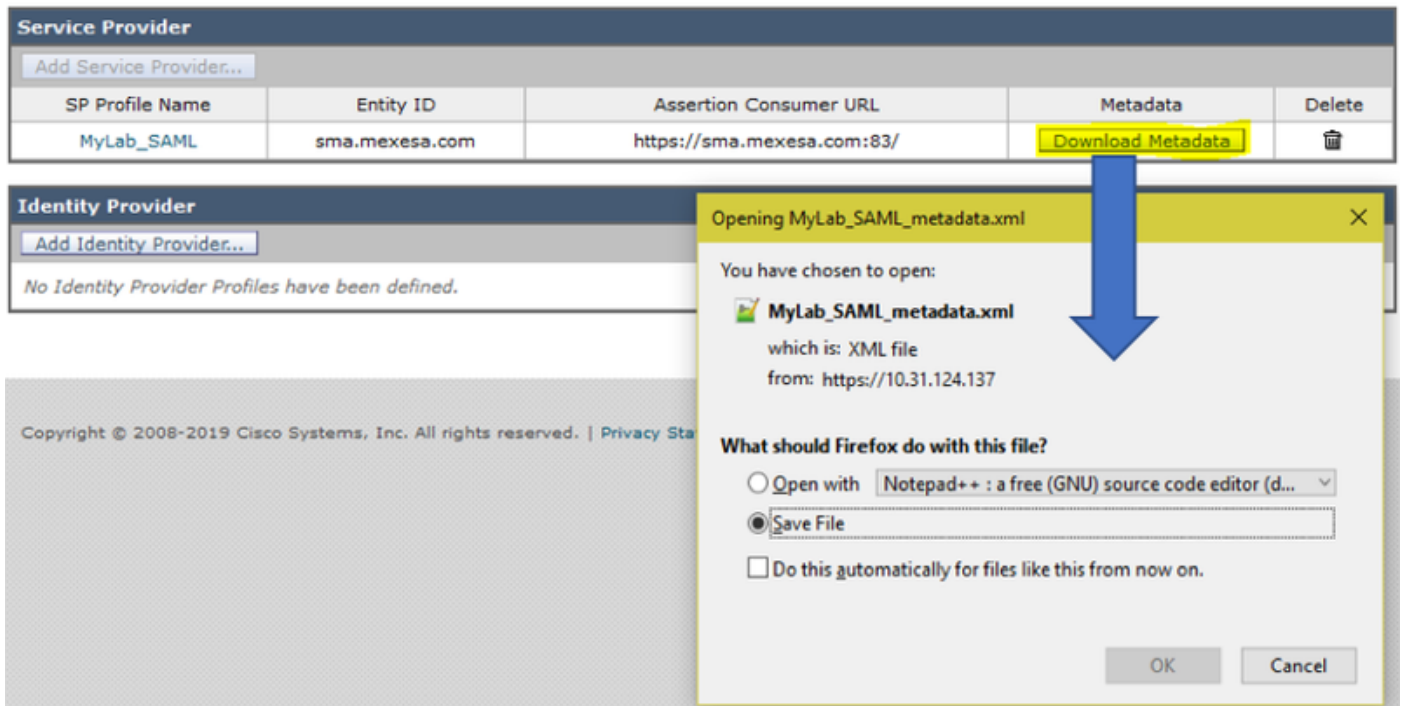
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Identity Provider

Add Identity Provider...

No Identity Provider Profiles have been defined.

Copyright © 2008-2019 Cisco Systems, Inc. All rights reserved. | Privacy Sta



Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 11.0 für Cisco Content Security Management Appliances - GD \(Allgemeine Bereitstellung\)](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

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.