

Probleemoplossing voor fout "Fout opgetreden tijdens ophalen metagegevens informatie" voor SAML in de SMA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de fout "Fout tijdens het ophalen van metagegevens informatie" kunt oplossen voor Security Assertion Markup Language (SAML) in de Security Management-applicatie (SMA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ADFS (Active Directory Federation Services)
- SAML-integratie met SMA
- [OpenSSL](#) geïnstalleerd

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SMA AsyncOS versie 11.x.x
- SMA AsyncOS versie 12.x.x

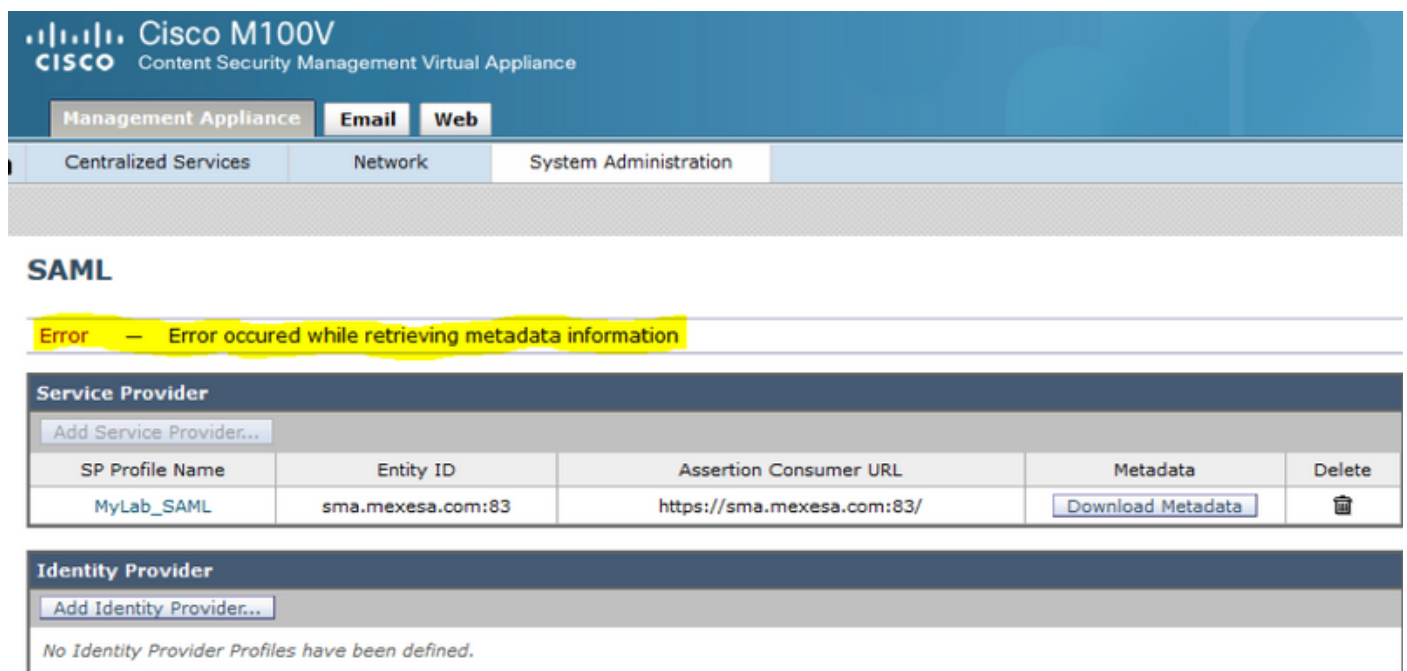
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie


Cisco Content Security Management-applicatie ondersteunt nu SAML 2.0 Single Sign-On (SSO), zodat de eindgebruikers toegang hebben tot de spamquarantaine en dezelfde referenties kunnen gebruiken die worden gebruikt voor toegang tot andere door SAML 2.0 SSO enabled-services binnen hun organisatie. U kunt bijvoorbeeld Ping Identity inschakelen als uw SAML Identity Provider (IDP) en heeft accounts op Rally, Salesforce en Dropbox die SAML 2.0 SSO ingeschakeld hebben. Wanneer u het Cisco Content Security Management-apparaat configureert om SAML 2.0 SSO als Service Provider (SP) te ondersteunen, kunnen eindgebruikers één keer inloggen en toegang hebben tot al deze services, inclusief spamquarantaine.

Probleem

Wanneer u Download Metadata voor SAML selecteert, krijgt u de fout "Fout opgetreden tijdens het ophalen van metagegevens informatie", zoals in de afbeelding:



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 occurred while retrieving metadata information'. Below the error message, there are two sections: 'Service Provider' and 'Identity Provider'. The 'Service Provider' section contains a table with one entry: 'MyLab_SAML' with Entity ID 'sma.mexesa.com:83' and Assertion Consumer URL 'https://sma.mexesa.com:83/'. A 'Download Metadata' button is visible next to this entry. The 'Identity Provider' section is currently empty, showing 'No Identity Provider Profiles have been defined.'

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

Oplossing

Stap 1. Maak een nieuw zelfondertekend certificaat op de e-mail security applicatie (ESA).

Zorg ervoor dat de algemene naam gelijk is aan de URL van de entiteit, maar zonder het poortnummer, zoals in de afbeelding:

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

Stap 2. Exporteer het nieuwe certificaat met de extensie .pfx, typ een wachtwoord en sla het op in de machine.

Stap 3. Open een Windows-terminal en voer deze opdrachten in. Typ het wachtwoord voor de vorige stap.

- Voer deze opdracht uit om de privé-sleutel te exporteren:

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

- Voer deze opdracht uit om het certificaat te exporteren:

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

Stap 4. Aan het eind van dit proces moet u twee nieuwe bestanden hebben:

certificateprivatekey.pem en **certificate.pem**. Upload beide bestanden in het serviceprovider-profiel en gebruik hetzelfde wachtwoord dat u gebruikt om het certificaat te exporteren.

Stap 5. De SMA vereist dat beide bestanden in .PEM formaat zijn om te kunnen werken, zoals in de afbeelding.

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

Stap 6. Zorg ervoor dat u het aankruisvakje **Aantekeningen** aanvinkt.

Stap 7. Verzend en leg de wijzigingen vast, u moet in staat zijn om de metagegevens te downloaden, zoals in de afbeelding.

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

Opening MyLab_SAML_metadata.xml

You have chosen to open:

MyLab_SAML_metadata.xml
which is: XML file
from: https://10.31.124.137

What should Firefox do with this file?

Open with Notepad++ : a free (GNU) source code editor (d...)

Save File

Do this automatically for files like this from now on.

OK Cancel

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 11.0 voor Cisco Content Security Management-applicaties - GD \(Algemene implementatie\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.