

Solucionar o erro "Ocorreu um erro ao recuperar informações de metadados" para SAML no SMA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como solucionar o erro "Ocorreu um erro ao recuperar informações de metadados" para Security Assertion Markup Language (SAML) no Security Management Appliance (SMA).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ADFS (Serviços de Federação do Active Directory)
- Integração SAML com SMA
- [OpenSSL](#) instalado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- SMA AsyncOs versão 11.x.x
- SMA AsyncOs versão 12.x.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

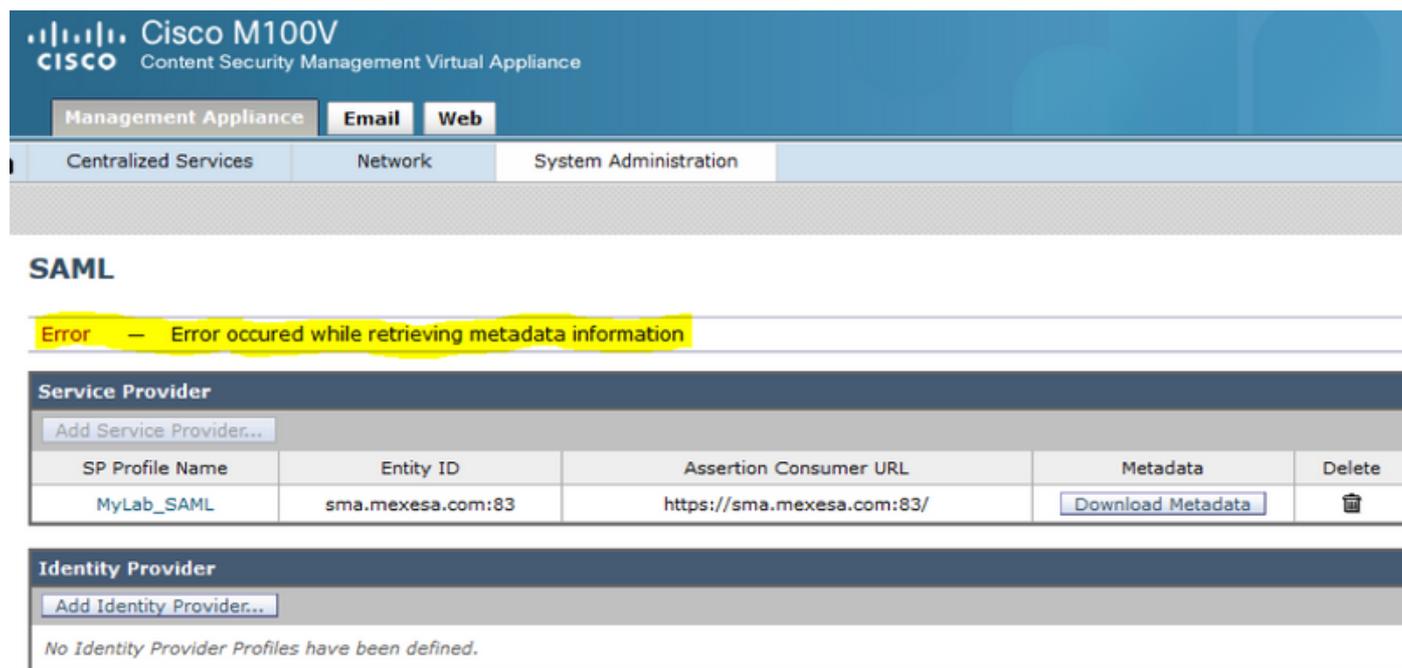
Informações de Apoio

O Cisco Content Security Management Appliance agora oferece suporte ao SSO (Single Sign-On, sign-on único) do SAML 2.0 para que os usuários finais possam acessar a Quarentena de spam e

usar as mesmas credenciais usadas para acessar outros serviços habilitados para SSO do SAML 2.0 em suas organizações. Por exemplo, você habilita a Identidade de Ping como seu provedor de identidade SAML (IdP) e tem contas no Rally, Salesforce e Dropbox que têm o SAML 2.0 SSO habilitado. Quando você configura o dispositivo Cisco Content Security Management para oferecer suporte ao SAML 2.0 SSO como um provedor de serviços (SP), os usuários finais podem se conectar uma vez e ter acesso a todos esses serviços, incluindo a Quarentena de spam.

Problema

Ao selecionar Baixar Metadados para SAML, você recebe o erro "Ocorreu um erro ao recuperar informações de metadados", como mostrado na imagem:



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 is a table of Service Providers. The table has columns for 'SP Profile Name', 'Entity ID', 'Assertion Consumer URL', 'Metadata', and 'Delete'. One service provider is listed: '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 the 'MyLab_SAML' entry. 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.'

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

Solução

Etapa 1. Crie um novo certificado autoassinado no ESA (Email Security Appliance).

Certifique-se de que o nome comum seja igual ao URL da ID da entidade, mas sem o número da porta, como mostrado na imagem:

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

Etapa 2. Exporte o novo certificado com uma extensão .pfx, digite uma senha e salve-o em sua máquina.

Etapa 3. Abra um terminal do Windows e insira esses comandos, forneça a senha na etapa anterior.

- Execute este comando para exportar a chave privada:

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

- Execute este comando para exportar o certificado:

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

Etapa 4. Ao final desse processo, você deve ter dois novos arquivos: **certificateprivatekey.pem** e **certificate.pem**. Carregue os dois arquivos no Perfil do provedor de serviços e use a mesma senha que você usa para exportar o certificado.

Etapa 5. O SMA exige que ambos os arquivos estejam no formato .PEM para que ele funcione, como mostrado na imagem.

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

Etapa 6. Certifique-se de marcar a caixa de seleção **Assinar Asserções**.

Etapa 7. Envie e confirme as alterações, você deve ser capaz de fazer download dos metadados, como mostrado na imagem.

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

Informações Relacionadas

- [Guia do usuário do AsyncOS 11.0 para dispositivos de gerenciamento de segurança de conteúdo da Cisco - GD \(General Deployment, implantação geral\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.