

# Solucione el error "Error al recuperar información de metadatos" para SAML en SMA

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo resolver el error "Error al recuperar información de metadatos" para el Lenguaje de marcado de aserción de seguridad (SAML) en el Dispositivo de administración de seguridad (SMA).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ADFS (Servicios de federación de Active Directory)
- Integración de SAML con SMA
- [OpenSSL](#) instalado

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- SMA AsyncOs versión 11.x.x
- SMA AsyncOs versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

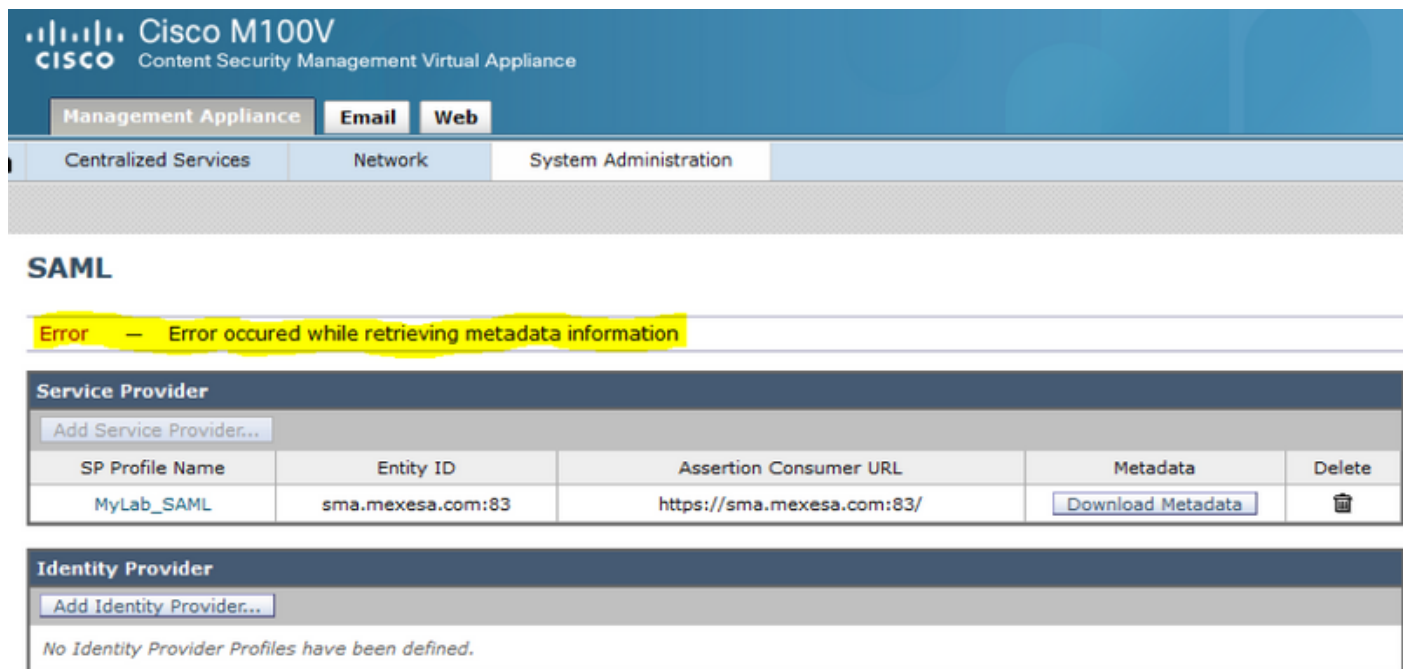
## Antecedentes

Cisco Content Security Management Appliance ahora es compatible con el inicio de sesión único


(SSO) SAML 2.0, de modo que los usuarios finales pueden acceder a Spam Quarantine y utilizar las mismas credenciales que se utilizan para acceder a otros servicios habilitados para SSO SAML 2.0 de su organización. Por ejemplo, puede habilitar la identidad de ping como su proveedor de identidad SAML (IdP) y tiene cuentas en Rally, Salesforce y Dropbox que tienen habilitado SAML 2.0 SSO. Al configurar el dispositivo Cisco Content Security Management para que admita SSO SAML 2.0 como proveedor de servicios (SP), los usuarios finales pueden iniciar sesión una vez y tener acceso a todos estos servicios, incluida Spam Quarantine.

## Problema

Al seleccionar Descargar Metadatos para SAML, se obtiene el error "Error al recuperar información de metadatos", como se muestra en la imagen:



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 section for 'Service Provider' with an 'Add Service Provider...' button. A table lists the service providers:

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com:83	https://sma.mexesa.com:83/	<a href="#">Download Metadata</a>	

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.'

## Solución

Paso 1. Cree un nuevo certificado autofirmado en el dispositivo de seguridad de correo electrónico (ESA).

Asegúrese de que el nombre común sea el mismo que la URL de ID de entidad, pero sin el número de puerto, como se muestra en la imagen:

## 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

Paso 2. Exporte el nuevo certificado con la extensión .pfx, escriba una frase de contraseña y guárdelo en el equipo.

Paso 3. Abra un terminal de Windows e ingrese estos comandos, proporcione la frase de contraseña en el paso anterior.

- Ejecute el comando this para exportar la clave privada:

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

- Ejecute este comando para exportar el certificado:

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

Paso 4. Al final de este proceso, debe tener dos archivos nuevos: **certificateprivatekey.pem** y **certificate.pem**. Cargue ambos archivos en el perfil del proveedor de servicios y utilice la misma frase de contraseña que utiliza para exportar el certificado.

Paso 5. El SMA requiere que ambos archivos estén en formato .PEM para que funcionen, como se muestra en la imagen.

## 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**

Paso 6. Asegúrese de seleccionar la casilla de verificación **Firmar aserciones**.

Paso 7. Envíe y confirme los cambios, debe poder descargar los metadatos, como se muestra en la imagen.

## SAML

**Service Provider**

Add Service Provider...

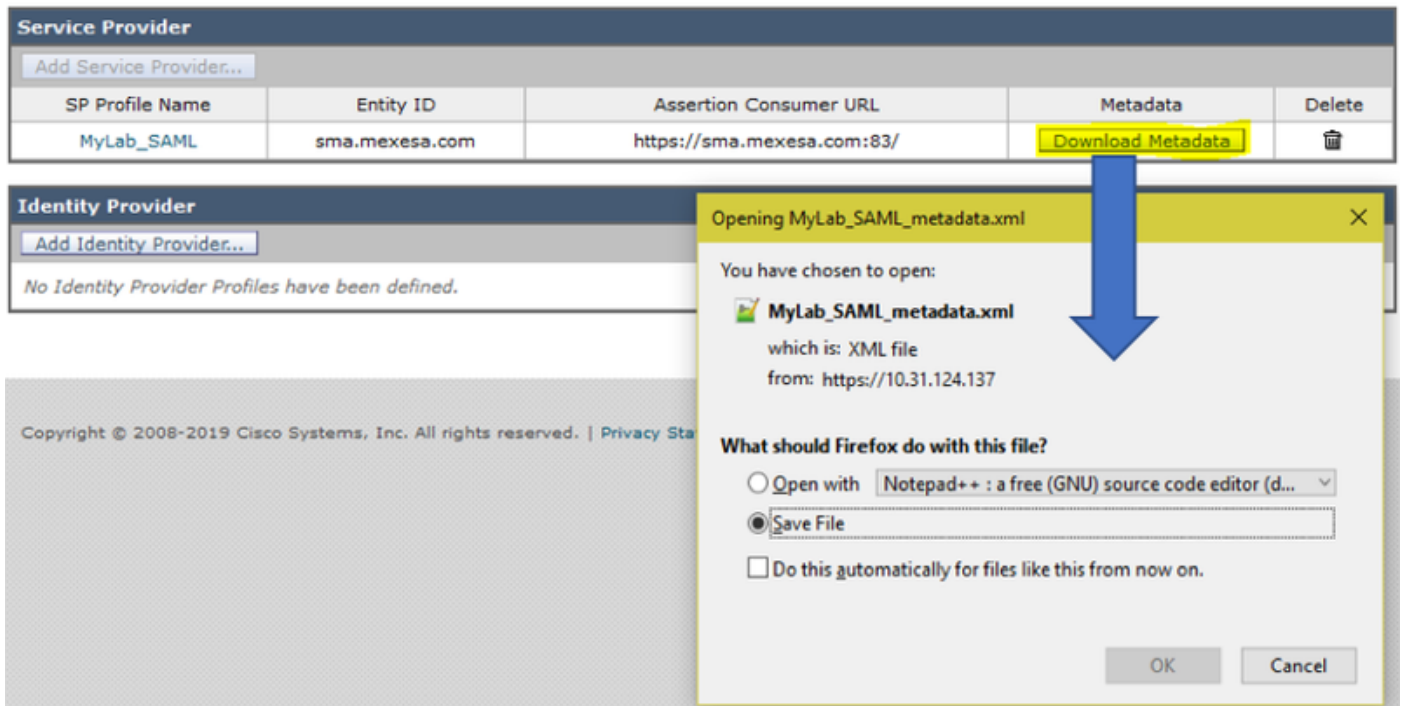
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

**Identity Provider**

Add Identity Provider...

No Identity Provider Profiles have been defined.

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



## Información Relacionada

- [Guía del usuario de AsyncOS 11.0 para los dispositivos de administración de seguridad de contenido de Cisco - GD \(implementación general\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).