Resuelva problemas el " del error; El error ocurrió mientras que extraía el information" de los meta datos; para SAML en el S A

Contenido

Introducción

Este documento describe cómo resolver problemas el error “error ocurrió mientras que extrae la información de los meta datos” para el lenguaje de marcado de la aserción de la Seguridad (SAML) en el dispositivo de la Administración de seguridad (S A).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- ADFS (servicios de la federación del Active Directory)
- SAML integración con el S A
- OpenSSL instalado

Componentes Utilizados

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

- Versión 11.x.x S A AsyncOs
- Versión 12.x.x S A AsyncOs

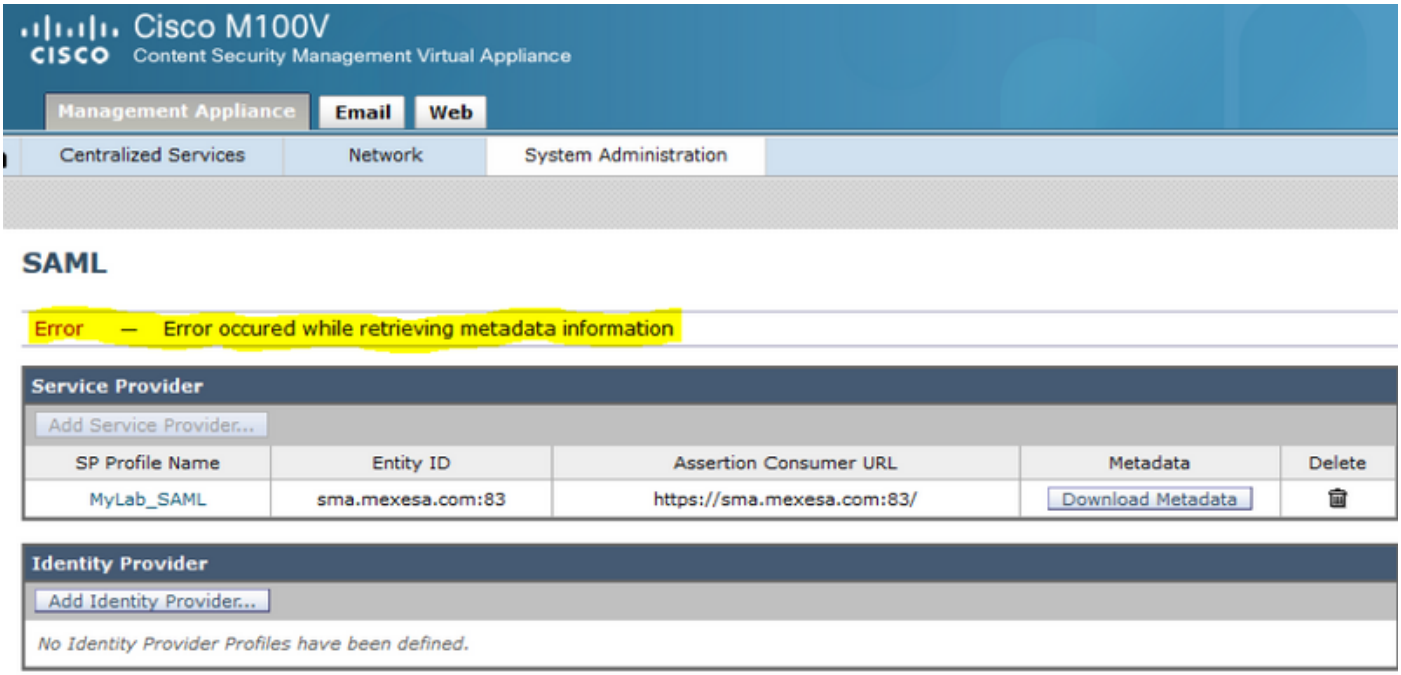
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco contenta la Administración de seguridad que el dispositivo ahora soporta SAML 2.0 solos Muestra-en (SSO) de modo que los usuarios finales puedan acceder la cuarentena del Spam y utilizar las mismas credenciales que se utilizan para acceder el otro SAML 2.0 servicios habilitados SSO dentro de su organización. Por ejemplo, usted habilitan la identidad del ping como su proveedor de la identidad de SAML (IdP) y tienen cuentas en la reunión, Salesforce, y el Dropbox que hacen SAML 2.0 SSO habilitar. Cuando usted configura el dispositivo de la Administración de seguridad del contenido de Cisco para soportar SAML 2.0 SSO como proveedor de servicio (SP), los usuarios finales pueden ingresar una vez y tener acceso a todos estos servicios incluyendo la cuarentena del Spam.

Problema

Cuando usted selecciona los meta datos de la descarga para SAML usted consigue el error “error ocurrió mientras que extrae la información de los meta datos”, tal y como se muestra en de la imagen:



Solución

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

Asegúrese que el Common Name sea lo mismo que la entidad ID URL, pero sin el número del puerto, tal y como se muestra en de la imagen:

Paso 2. Exporte el nuevo certificado con una extensión del .pfx, teclee adentro un passphrase, y sálvelo en su máquina.

Paso 3. Abra un Terminal de Windows y entre estos comandos, proporcione el passphrase en el paso anterior.

- Funcione con el este comando de exportar la clave privada:

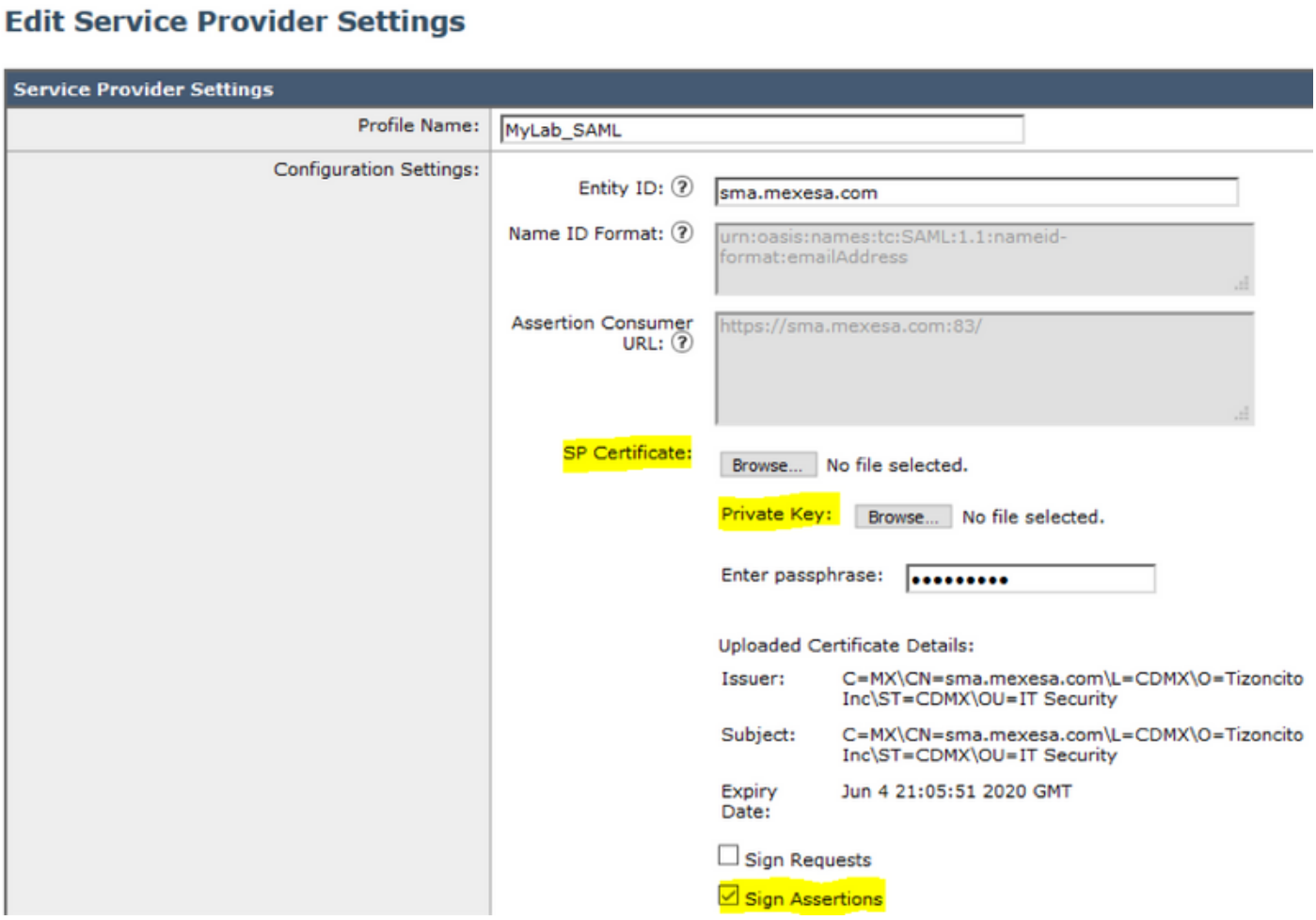
```
openssl pkcs12 -in created_certificate.pfx -nocerts -out certificateprivatekey.pem -nodes
```

- Funcione con este comando de exportar el certificado:

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

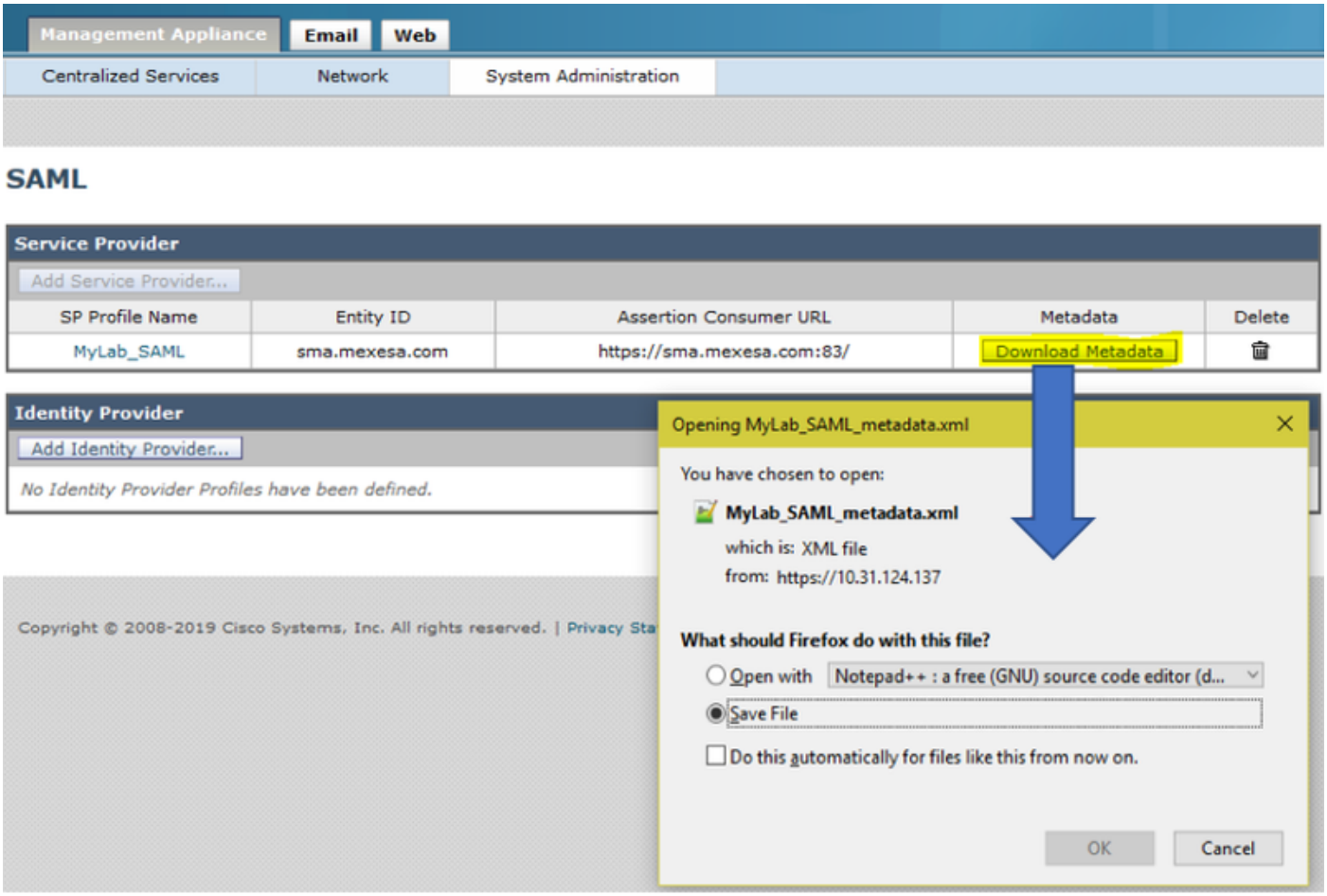
Paso 4. En el final de este proceso, usted debe tener dos nuevos archivos: **certificateprivatekey.pem y** certificate.pem**. Cargue** ambos archivos en el perfil del proveedor de servicio y utilice el mismo passphrase que usted utiliza para exportar el certificado.

Paso 5. El S A requiere ambos archivos estar en el formato del .PEM para que trabaje, tal y como se muestra en de la imagen.



Paso 6. Asegúrese que usted seleccione el checkbox de las **aserciones de la muestra**.

Paso 7. Someta y confíe los cambios, usted debe poder descargar los meta datos, tal y como se muestra en de la imagen.



Información Relacionada

- [Guía del usuario para AsyncOS 11.0 para los dispositivos de la Administración de seguridad del contenido de Cisco - GD (General Deployment)]
- [Soporte Técnico y Documentación - Cisco Systems]