

# Risoluzione dei problemi relativi all'errore "Errore durante il recupero delle informazioni sui metadati" per SAML in SMA

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come risolvere l'errore "Errore durante il recupero delle informazioni sui metadati" per il linguaggio SAML (Security Assertion Markup Language) in Security Management Appliance (SMA).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ADFS (Active Directory Federation Services)
- Integrazione SAML con SMA
- [OpenSSL](#) installato

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SMA AsyncOs versione 11.x.x
- SMA AsyncOs versione 12.x.x

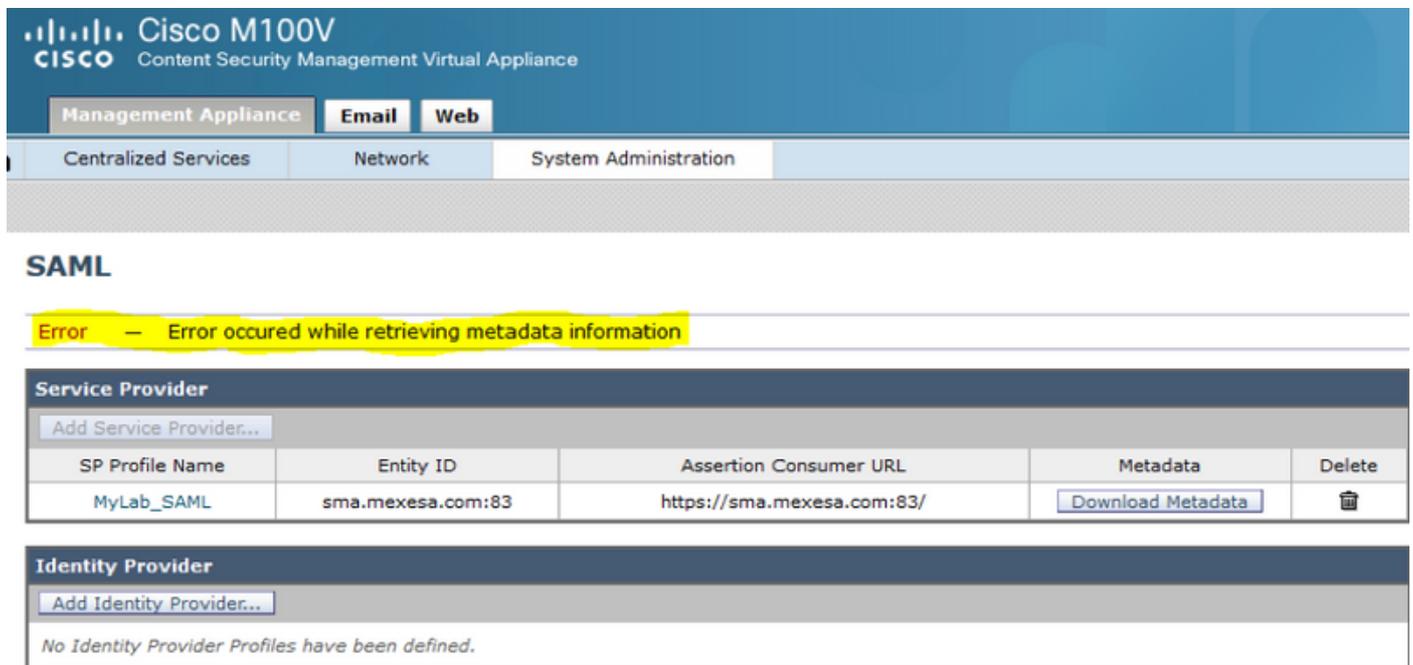
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Cisco Content Security Management Appliance supporta ora il Single Sign-On (SSO) SAML 2.0 in modo che gli utenti finali possano accedere alla quarantena della posta indesiderata e utilizzare le stesse credenziali utilizzate per accedere ad altri servizi SAML 2.0 SSO all'interno dell'organizzazione. Ad esempio, si abilita Ping Identity come provider di identità SAML (IdP) e si dispone di account su Rally, Salesforce e Dropbox con SSO SAML 2.0 abilitato. Quando si configura l'appliance Cisco Content Security Management per il supporto di SAML 2.0 SSO come provider di servizi (SP), gli utenti finali possono accedere una sola volta a tutti questi servizi, inclusa la quarantena della posta indesiderata.

# Problema

Quando si seleziona Scarica metadati per SAML viene visualizzato l'errore "Errore durante il recupero delle informazioni sui metadati", come mostrato nell'immagine:



# Soluzione

Passaggio 1. Creare un nuovo certificato autofirmato in Email Security Appliance (ESA).

Assicurarsi che il nome comune sia uguale all'URL dell'ID entità, ma senza il numero di porta, come mostrato nell'immagine:

## 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

Passaggio 2. Esportare il nuovo certificato con estensione .pfx, digitare una passphrase e salvarlo nel computer.

Passaggio 3. Aprire un terminale Windows e immettere questi comandi, fornire la passphrase indicata nel passaggio precedente.

- Eseguire questo comando per esportare la chiave privata:

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

- Eseguire questo comando per esportare il certificato:

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

Passaggio 4. Al termine di questo processo, è necessario disporre di due nuovi file: **certificateprivatekey.pem** e **certificate.pem**. Caricare entrambi i file nel profilo del provider di servizi e utilizzare la stessa passphrase utilizzata per esportare il certificato.

Passaggio 5. L'SMA richiede che entrambi i file siano in formato .PEM per funzionare, come mostrato nell'immagine.

## 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**

Passaggio 6. Assicurarsi di selezionare la casella di controllo **Firma asserzioni**.

Passaggio 7. Inviare e confermare le modifiche, è necessario essere in grado di scaricare i metadati, come mostrato nell'immagine.

## SAML

**Service Provider**

Add Service Provider...

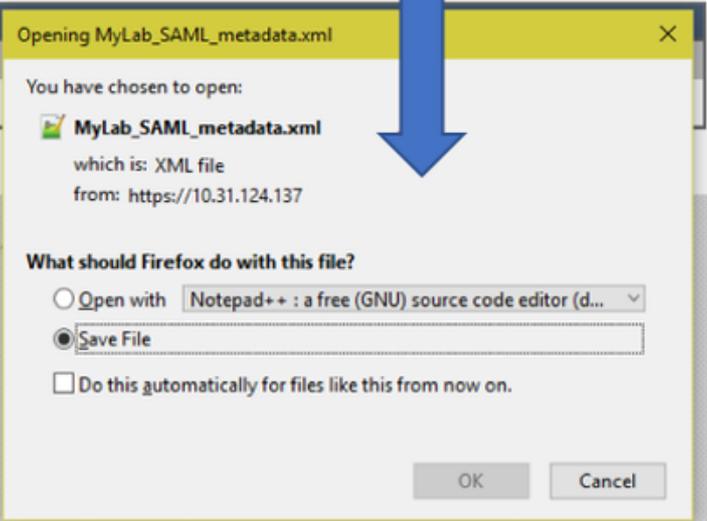
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

**Identity Provider**

Add Identity Provider...

No Identity Provider Profiles have been defined.

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



## Informazioni correlate

- [Guida per l'utente di AsyncOS 11.0 per Cisco Content Security Management Appliance - GD \(General Deployment\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).