

Configurazione di più profili RAVPN con autenticazione SAML in FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1: Creare un certificato autofirmato e un file PKCS#12 utilizzando OpenSSL](#)

[Passaggio 2: caricare il file PKCS#12 in Azure e FDM](#)

[Passaggio 2.1. Carica il certificato in Azure](#)

[Passaggio 2.2. Carica il certificato in FDM](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione SAML per più profili di connessione della VPN ad accesso remoto usando Azure come IdP su CSF tramite FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Certificati SSL (Secure Sockets Layer)
- OpenSSL
- RAVPN (Virtual Private Network) di accesso remoto
- Cisco Secure Firewall Device Manager (FDM)
- SAML (Security Assertion Markup Language)
- Microsoft Azure

Componenti usati

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

- OpenSSL
- Cisco Secure Firewall (CSF) versione 7.4.1
- Cisco Secure Firewall Device Manager versione 7.4.1

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

SAML, o Security Assertion Markup Language, è uno standard aperto per lo scambio di informazioni di autenticazione e autorizzazione tra parti, in particolare un provider di identità (IdP) e un provider di servizi (SP). L'utilizzo dell'autenticazione SAML per le connessioni VPN (Remote Access VPN) e diverse altre applicazioni è diventato sempre più comune grazie ai numerosi vantaggi che offre. In Firepower Management Center (FMC) è possibile configurare più profili di connessione per l'utilizzo di diverse applicazioni protette da IdP grazie all'opzione Ignora certificato provider di identità disponibile nel menu di configurazione Profilo di connessione. Questa funzionalità consente agli amministratori di sostituire il certificato IdP primario nell'oggetto server Single Sign-On (SSO) con un certificato IdP specifico per ogni profilo di connessione. Tuttavia, questa funzionalità è limitata in Firepower Device Manager (FDM) in quanto non fornisce un'opzione simile. Se è stato configurato un secondo oggetto SAML, il tentativo di connessione al primo profilo di connessione genera un errore di autenticazione e visualizza il messaggio di errore "Autenticazione non riuscita a causa di un problema durante il recupero del cookie Single Sign-On". Per ovviare a questa limitazione, è possibile creare e importare in Azure un certificato autofirmato personalizzato da utilizzare in tutte le applicazioni. In questo modo, è necessario installare un solo certificato in FDM, consentendo l'autenticazione SAML senza problemi per più applicazioni.

Configurazione

Passaggio 1: Creare un certificato autofirmato e un file PKCS#12 utilizzando OpenSSL

In questa sezione viene descritto come creare il certificato autofirmato utilizzando OpenSSL

1. Accedere a un endpoint in cui è installata la libreria OpenSSL.



Nota: in questo documento viene usato un computer Linux, quindi alcuni comandi sono specifici di un ambiente Linux. Tuttavia, i comandi OpenSSL sono gli stessi.

b. Creare un file di configurazione utilizzando il `touch`

```
.conf  
comando.
```

```
<#root>
```

```
root@host#
```

```
touch config.conf
```

c. Modificare il file con un editor di testo. Nell'esempio viene utilizzato Vim e viene eseguito il `vim`

`.conf`
comando. È possibile utilizzare qualsiasi altro editor di testo.

`<#root>`

`root@host#`

`vim config.conf`

d. Inserire le informazioni da includere nel documento autofirmato.

Assicurarsi di sostituire i valori tra `< >` con le informazioni dell'organizzazione.

```
[req]
distinguished_name = req_distinguished_name
prompt = no
```

```
[req_distinguished_name]
C =
```

ST =

L =

O =

OU =

CN =

e. L'uso di questo comando genera una nuova chiave privata RSA a 2048 bit e un certificato autofirmato utilizzando l'algoritmo SHA-256, valido per 3650 giorni, in base alla configurazione specificata nel

`.conf`

file. La chiave privata viene salvata in

`.pem`

e il certificato autofirmato viene salvato in

`.cert`

.

<#root>

root@host#

```
openssl req -newkey rsa:2048 -nodes -keyout
```

```
.pem -x509 -sha256 -days 3650 -config
```

```
.conf -out
```

.crt

```
root@host:~# openssl req -newkey rsa:2048 -nodes -keyout Azure_key.pem -x509 -sha256 -days 3650 -config config.conf -out Azure_SSO.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'Azure_key.pem'
-----
root@host:~#
```

f. Dopo aver creato la chiave privata e il certificato autofirmato, questi vengono esportati in un file PKCS#12, che può includere sia la chiave privata che il certificato.

<#root>

root@host#

```
openssl pkcs12 -export -inkey
```

.pem -in

.crt -name

-out

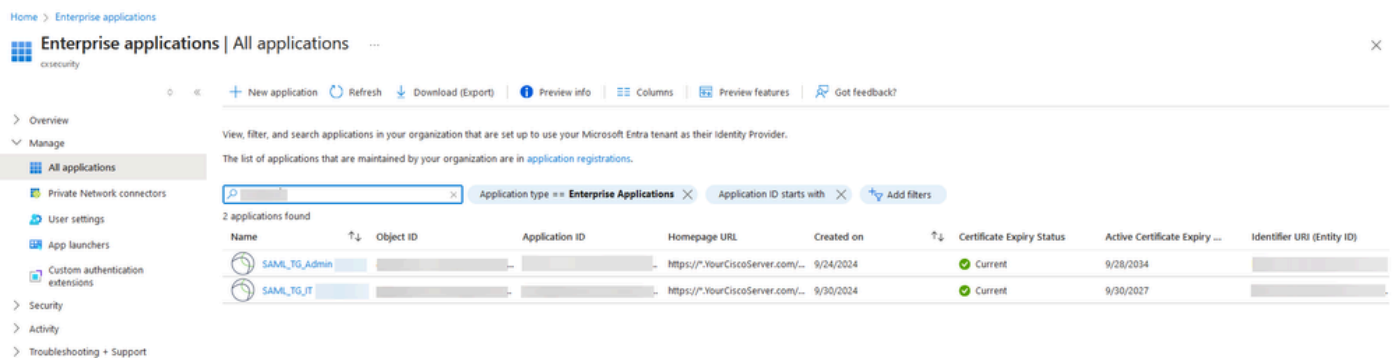
.pfx

```
root@host:~# openssl pkcs12 -export -inkey Azure_key.pem -in Azure_SSO.crt -out Azure_SSO.pfx
Enter Export Password:
Verifying - Enter Export Password:
root@host:~#
root@host:~# ls
Azure_SSO.crt Azure_SSO.pfx Azure_key.pem config.conf
```

Prendere nota della password.

Passaggio 2: caricare il file PKCS#12 in Azure e FDM

Assicurarsi di creare un'applicazione in Azure per ogni profilo di connessione che utilizza l'autenticazione SAML in FDM.



The screenshot shows the Azure Enterprise Applications management console. The page title is "Enterprise applications | All applications". The left sidebar contains navigation options: Overview, Manage, All applications (selected), Private Network connectors, User settings, App launchers, Custom authentication extensions, Security, Activity, and Troubleshooting + Support. The main content area displays a table of applications. The table has columns for Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiry Status, Active Certificate Expiry, and Identifier URI (Entity ID). Two applications are listed: SAML_TG_Admin and SAML_TG_IT, both with a status of "Current".

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry	Identifier URI (Entity ID)
SAML_TG_Admin			https://*.YourCiscoServer.com/...	9/24/2024	Current	9/28/2034	
SAML_TG_IT			https://*.YourCiscoServer.com/...	9/30/2024	Current	9/30/2027	


Dopo aver ottenuto il file PKCS#12 dal Passaggio 1: creazione di un certificato autofirmato e di un file PKCS#12 utilizzando OpenSSL, è necessario caricarlo in Azure per più applicazioni e configurarlo nella configurazione FDM SSO.

Passaggio 2.1. Carica il certificato in Azure

a. Accedere al portale di Azure, passare all'applicazione Enterprise che si desidera proteggere con l'autenticazione SAML e selezionare Single Sign-On.

b. Scorrere fino alla sezione Certificati SAML e selezionare Altre opzioni > Modifica.

SAML Certificates


Token signing certificate  Edit

Status: Active

Thumbprint: [Redacted]

Expiration: 9/28/2034, 1:05:19 PM


Notification Email: [Redacted]

App Federation Metadata Url: [https://login.microsoftonline.com/\[Redacted\]](https://login.microsoftonline.com/[Redacted]) 

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional)  Edit

Required	No
Active	0
Expired	0

c. Selezionare l'opzione Importa certificato.

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

 Save [+](#) New Certificate [↑](#) Import Certificate  Got feedback?

Status	Expiration Date	Thumbprint	
Active	8/25/2029, 7:03:32 PM	[Redacted]	...


Signing Option:

Signing Algorithm:

d. Individuare il file PKCS#12 creato in precedenza e utilizzare la password immessa al momento della creazione del file PKCS#12.

Import certificate

Upload a certificate with the private key and the pfx credentials, the type of this file should be .pfx and using RSA for the encryption algorithm

Certificate: 

PFX Password: 

Add

Cancel

e. Infine, selezionare l'opzione Rendi certificato attivo.

SAML Signing Certificate



Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save [+ New Certificate](#) [↑ Import Certificate](#) | [Got feedback?](#)

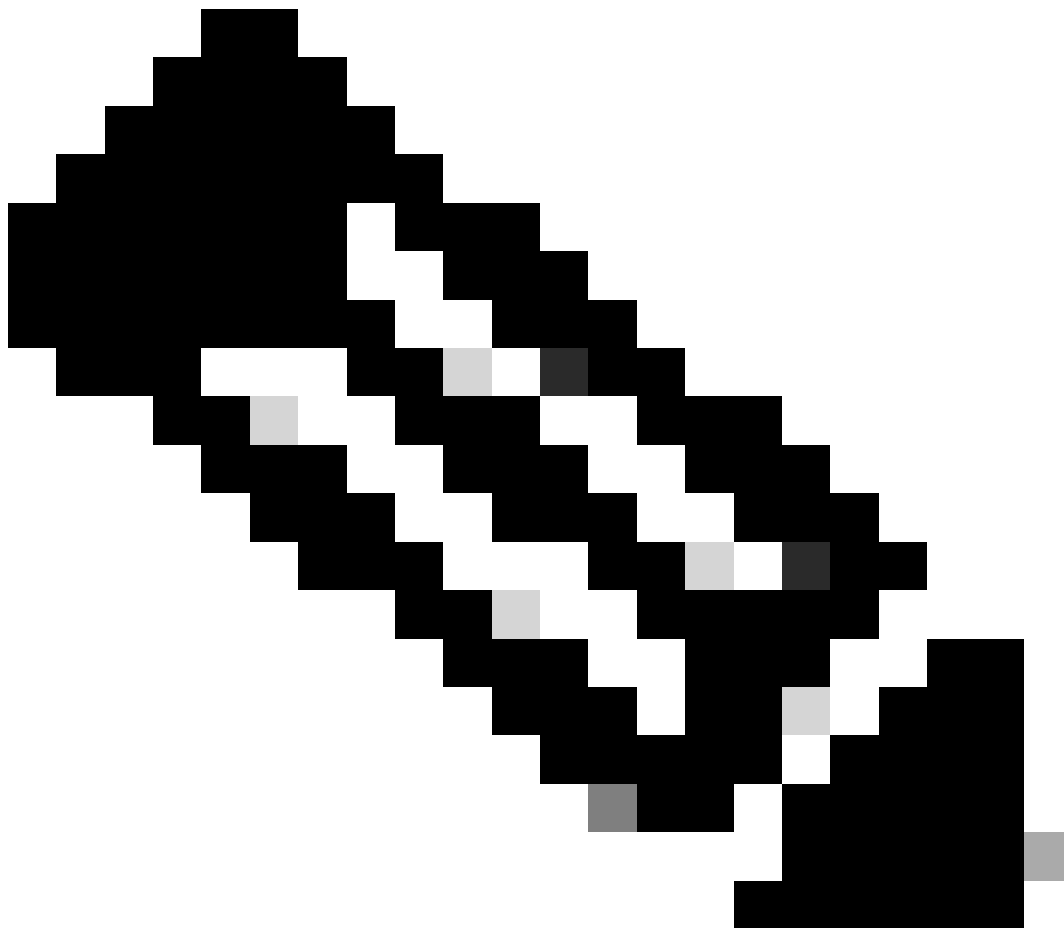
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	
Active	9/27/2027, 5:51:21 PM	[Redacted]	

Signing Option:

Signing Algorithm:

Notification Email Addresses:

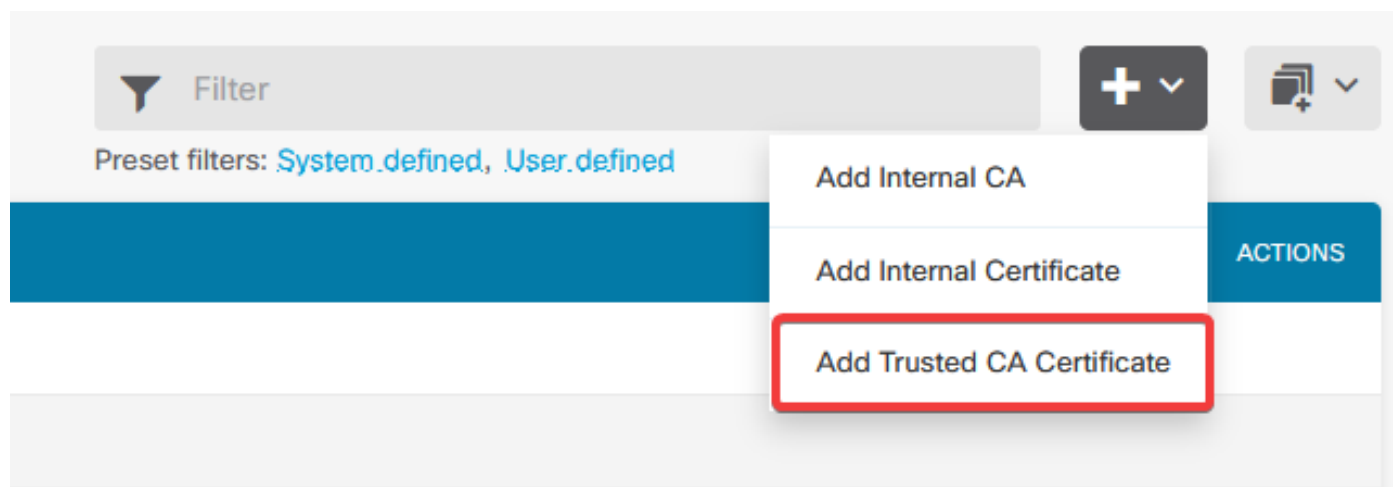
- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate



Nota: eseguire il passaggio 2.1: Caricare il certificato in Azure per ogni applicazione.

Passaggio 2.2. Carica il certificato in FDM

a. Passare a **Objects > Certificates > Click Add Trusted CA certificate.**



b. Inserire il nome del trust point desiderato e caricare solo il certificato di identità dall'IdP (non il file PKCS#12), quindi controllare la **Skip CA Certificate Check** tabella.

Add Trusted CA Certificate



Name

Azure_SSO

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----  
MIIC8DCCAdigAwIBAgIQGDZUgz1YHI5PirWojole+zANBgkqhkiG9w0BAQsFADA0  
MTIwMAYDVQQDEy1NaW5yb3NvZnQgQXp1cmUgRmVkdXJhdGVkIFNTTyBDZXJ0aWZp  
Y2E9ZTA0EwYwMDAEMzAwMTA0MTBzEwYwMDAEMzAwMTA0MTBzMDQyMjA0PQYw
```

Skip CA Certificate Check 

Validation Usage for Special Services

Please select



CANCEL

OK

c. Impostare il nuovo certificato nell'oggetto SAML.

Edit SAML Server



Name

AzureIDP

Description

Identity Provider (IDP) Entity ID URL

https://

Sign In URL

https://

Supported protocols: https, http

Sign Out URL

https://

Supported protocols: https, http

Service Provider Certificate

(Validation Usage: ...)

Identity Provider Certificate

Azure_SSO (Validation Usage: ...)

Request Signature

None

Request Timeout

Range: 1 - 7200 (sec)

d. Impostare l'oggetto SAML nei diversi profili di connessione che utilizzano SAML come metodo di autenticazione e per i quali l'applicazione è stata creata in Azure. Distribuire le modifiche

Device Summary

Remote Access VPN Connection Profiles

2 connection profiles

Filter



#	NAME	AAA	GROUP POLICY	ACTIONS
1	SAML_TG_Admin	Authentication: SAML Authorization: None Accounting: None	SAML_GP_Admin	
2	SAML_TG_IT	Authentication: SAML Authorization: None Accounting: None	SAML_GP_IT	

Primary Identity Source

Authentication Type

SAML



SAML Login Experience

VPN client embedded browser

Default OS browser

Primary Identity Source for User Authentication

AzureIDP



Verifica

Eseguire i comandi `show running-config webvpn` e `show running-config tunnel-group` per rivedere la configurazione e verificare che lo stesso URL IDP sia configurato sui diversi profili di connessione.

```
<#root>
```

```
firepower#
```

```
show running-config webvpn
```

```
webvpn
```

```
enable outside
```

```
http-headers
```

```
hsts-server
```

```
enable
```

```
max-age 31536000
```

```
include-sub-domains
```

```
no preload
```

```
hsts-client
```

```
enable
```

```
x-content-type-options
```

```
x-xss-protection
```

```
content-security-policy
```

```
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.10.08029-webdeploy-k9.pkg 2
```

anyconnect profiles defaultClientProfile disk0:/anyconncprofs/defaultClientProfile.xml
anyconnect enable

saml idp https://saml.lab.local/af42bac0

/

url sign-in https://login.saml.lab.local/af42bac0

/saml2

url sign-out https://login.saml.lab.local/af42bac0

/saml2

base-url https://Server.cisco.com

trustpoint idp

Azure_SSO

```
trustpoint sp FWCertificate
```

```
no signature
```

```
force re-authentication
```

```
tunnel-group-list enable
```

```
cache
```

```
disable
```

```
error-recovery disable
```

```
firepower#
```

```
<#root>
```

```
firepower#
```

```
show running-config tunnel-group
```

```
tunnel-group SAML_TG_Admin type remote-access
```

```
tunnel-group SAML_TG_Admin general-attributes
```

```
address-pool Admin_Pool
```

```
default-group-policy SAML_GP_Admin
```

```
tunnel-group SAML_TG_Admin webvpn-attributes
```

```
authentication saml
```

```
group-alias SAML_TG_Admin enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
tunnel-group SAML_TG_IT type remote-access
tunnel-group SAML_TG_IT general-attributes
  address-pool IT_Pool
  default-group-policy SAML_GP_IT
tunnel-group SAML_TG_IT webvpn-attributes
```

```
  authentication saml
```

```
group-alias SAML_TG_IT enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
firepower#
```


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).