

Konfiguration mehrerer RAVPN-Profile mit SAML-Authentifizierung auf FDM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Erstellen eines selbstsignierten Zertifikats und einer PKCS#12-Datei mit OpenSSL](#)

[Schritt 2: Laden Sie die PKCS#12-Datei auf Azure und FDM hoch.](#)

[Schritt 2.1: Zertifikat in Azure hochladen](#)

[Schritt 2.2: Zertifikat in FDM hochladen](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die SAML-Authentifizierung für mehrere Verbindungsprofile des RAS-VPN mithilfe von Azure als IdP auf CSF über FDM konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Secure Socket Layer (SSL)-Zertifikate
- OpenSSL
- Remote Access Virtual Private Network (RAVPN)
- Cisco Secure Firewall Device Manager (FDM)
- Security Assertion Markup Language (SAML)
- Microsoft Azure

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SAML (Security Assertion Markup Language) ist ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen Parteien, insbesondere zwischen einem Identity Provider (IdP) und einem Service Provider (SP). Die Verwendung der SAML-Authentifizierung für RAVPN-Verbindungen (Remote Access VPN) und verschiedene andere Anwendungen wird aufgrund der zahlreichen Vorteile immer beliebter. Im FirePOWER Management Center (FMC) können mehrere Verbindungsprofile so konfiguriert werden, dass sie verschiedene IDp-geschützte Anwendungen verwenden, da die Option Identitätsanbieter-Zertifikat überschreiben im Konfigurationsmenü Verbindungsprofil verfügbar ist. Mit dieser Funktion können Administratoren das primäre IdP-Zertifikat im Single Sign-On (SSO)-Serverobjekt mit einem spezifischen IdP-Zertifikat für jedes Verbindungsprofil überschreiben. Diese Funktionalität ist jedoch auf den FirePOWER-Gerätemanager (FDM) beschränkt, da sie keine ähnliche Option bietet. Wenn ein zweites SAML-Objekt konfiguriert ist, führt der Versuch, eine Verbindung mit dem ersten Verbindungsprofil herzustellen, zu einem Authentifizierungsfehler, und es wird die Fehlermeldung angezeigt: "Authentifizierung fehlgeschlagen aufgrund eines Problems beim Abrufen des Einmal-Anmelde-Cookies." Um diese Einschränkung zu umgehen, kann ein benutzerdefiniertes selbstsigniertes Zertifikat erstellt und in Azure zur Verwendung in allen Anwendungen importiert werden. Auf diese Weise muss nur ein Zertifikat im FDM installiert werden, wodurch eine nahtlose SAML-Authentifizierung für mehrere Anwendungen ermöglicht wird.

Konfigurieren

Schritt 1: Erstellen eines selbstsignierten Zertifikats und einer PKCS#12-Datei mit OpenSSL

In diesem Abschnitt wird beschrieben, wie Sie das selbstsignierte Zertifikat mithilfe von OpenSSL erstellen.

1. Melden Sie sich bei einem Endpunkt an, auf dem die OpenSSL-Bibliothek installiert ist.



Hinweis: In diesem Dokument wird ein Linux-System verwendet, sodass einige Befehle speziell für eine Linux-Umgebung gelten. Die OpenSSL-Befehle sind jedoch identisch.

b. Erstellen Sie eine Konfigurationsdatei mit dem `touch`

`.conf`
Befehl.

`<#root>`

`root@host#`

`touch config.conf`

c. Bearbeiten Sie die Datei mit einem Texteditor. In diesem Beispiel wird Vim verwendet, und der `vim`

.conf

Befehl wird ausgeführt. Sie können jeden anderen Texteditor verwenden.

<#root>

root@host#

vim config.conf

d. Geben Sie die Informationen ein, die in das Selbstsignierte aufgenommen werden sollen.

Ersetzen Sie die Werte zwischen < > durch die Informationen Ihrer Organisation.

[req]

distinguished_name = req_distinguished_name

prompt = no

[req_distinguished_name]

C =

ST =

L =

O =

OU =

CN =

e. Mit diesem Befehl werden ein neuer privater 2048-Bit-RSA-Schlüssel und ein selbstsigniertes Zertifikat mit dem SHA-256-Algorithmus generiert, der 3650 Tage lang gültig ist und auf der in der

.conf

Datei angegebenen Konfiguration basiert. Der private Schlüssel wird in gespeichert

.pem

und das selbstsignierte Zertifikat 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. Nach dem Erstellen des privaten Schlüssels und des selbstsignierten Zertifikats werden diese in eine PKCS#12-Datei exportiert. Dabei handelt es sich um ein Format, das sowohl den privaten Schlüssel als auch das Zertifikat enthalten kann.

<#root>

root@host#

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

.pem -in

.crt -name

-out

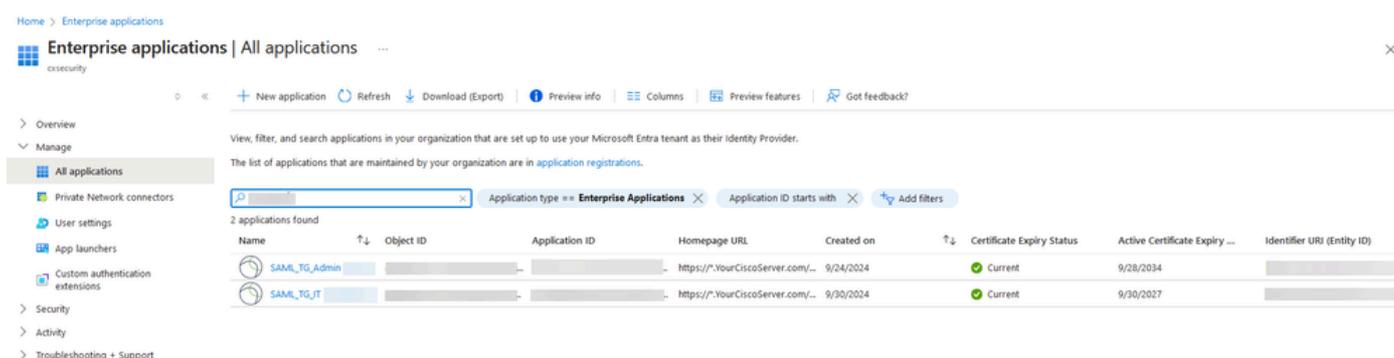
.pfx

```
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
```

Notieren Sie sich das Kennwort.

Schritt 2: Laden Sie die PKCS#12-Datei auf Azure und FDM hoch.

Stellen Sie sicher, dass auf Azure für jedes Verbindungsprofil, das die SAML-Authentifizierung auf dem FDM verwendet, eine Anwendung erstellt wird.



The screenshot shows the Azure Enterprise Applications management console. The page title is "Enterprise applications | All applications". The main content area displays a table of applications with the following columns: Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiry Status, Active Certificate Expiry, and Identifier URI (Entity ID). Two applications are listed:

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	

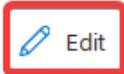
Sobald Sie die PKCS#12-Datei aus Schritt 1: Erstellen eines selbstsignierten Zertifikats und eine PKCS#12-Datei mit OpenSSL haben, muss sie für mehrere Anwendungen nach Azure hochgeladen und in der FDM SSO-Konfiguration konfiguriert werden.

Schritt 2.1: Zertifikat in Azure hochladen

a. Melden Sie sich bei Ihrem Azure-Portal an, navigieren Sie zu der Enterprise-Anwendung, die Sie mit SAML-Authentifizierung schützen möchten, und wählen Sie Single Sign-On aus.

b. Blättern Sie nach unten zum Abschnitt SAML-Zertifikate, und wählen Sie Mehr Optionen > Bearbeiten aus.

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/> 

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional)  Edit

Required: No

Active: 0

Expired: 0

c. Wählen Sie jetzt die Option Zertifikat importieren.

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. Suchen Sie die zuvor erstellte PKCS#12-Datei, und verwenden Sie das Kennwort, das Sie beim Erstellen der PKCS#12-Datei eingegeben haben.

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: 

e. Wählen Sie abschließend die Option Zertifikat aktivieren aus.

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



Hinweis: Führen Sie Schritt 2.1 aus: Laden Sie das Zertifikat für jede Anwendung auf Azure hoch.

Schritt 2.2: Zertifikat in FDM hochladen

a. Navigieren Sie zu **Objects > Certificates > Click Add Trusted CA certificate.**

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 Us... ▼

Identity Provider Certificate

Azure_SSO (Validation Usage: ... ▼

Request Signature

None ▼

Request Timeout

Range: 1 - 7200 (sec)

d. Legen Sie das SAML-Objekt für die verschiedenen Verbindungsprofile fest, die SAML als Authentifizierungsmethode verwenden und für die die Anwendung in Azure erstellt wurde. Bereitstellen der Änderungen

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



Überprüfung

Führen Sie die `show running-config` Befehle `webvpn` und `show running-config tunnel-group` aus, um die Konfiguration zu überprüfen und sicherzustellen, dass dieselbe IDP-URL für die verschiedenen Verbindungsprofile konfiguriert ist.

```
<#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:/anyconnprofs/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#
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.