Konfigurieren der SAML-Authentifizierung für mehrere RAVPN-Verbindungsprofile auf FTD

Inhalt

Einleitung

In diesem Dokument wird die SAML-Authentifizierung mit dem Azure-Identitätsanbieter für mehrere Verbindungsprofile auf dem von FMC verwalteten Cisco FTD beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Sichere Client-Konfiguration auf Next-Generation Firewall (NGFW), verwaltet vom FirePOWER Management Center (FMC)
- SAML- und metatada.xml-Werte

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firepower Threat Defense (FTD) Version 7.4.0
- FMC Version 7.4.0
- Azure Microsoft Entra ID mit SAML 2.0

- Cisco Secure Client 5.1.7.80

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

Mit dieser Konfiguration kann FTD sichere Client-Benutzer mithilfe von zwei verschiedenen SAML-Anwendungen auf Azure IDP authentifizieren, wobei ein einziges SAML-Objekt auf FMC konfiguriert ist.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate ...	Active Ce...	Identifier URI (Entity I...
FTD-SAML-1	44988e73-c06f-4008-be74...	0cff60a9-271f-4976-9848-...	https://*.YourCiscoServer....	25/11/2024	Current	25/11/2027	https://
FTD-SAML-2	dbe20be6-5440-4951-863...	2400bc8b-21b7-4f29-85c4...	https://*.YourCiscoServer....	25/11/2024	Current	27/11/2027	https://

In einer Microsoft Azure-Umgebung können mehrere Anwendungen dieselbe Objektkennung verwenden. Jede Anwendung, die in der Regel einer anderen Tunnelgruppe zugeordnet ist, benötigt ein eindeutiges Zertifikat, das die Konfiguration mehrerer Zertifikate innerhalb der IdP-Konfiguration der FTD-Seite unter einem einzelnen SAML-IdP-Objekt erfordert. Cisco FTD unterstützt jedoch nicht die Konfiguration mehrerer Zertifikate unter einem SAML IdP-Objekt, wie in Cisco Bug-ID CSCvi29084 beschrieben.

Um diese Einschränkung zu überwinden, hat Cisco die IdP-Zertifikatüberschreibungsfunktion eingeführt, die in FTD-Version 7.1.0 und ASA-Version 9.17.1 verfügbar ist. Diese Erweiterung bietet eine dauerhafte Lösung für das Problem und ergänzt die im Fehlerbericht beschriebenen Problemumgehungen.

Konfigurationen

In diesem Abschnitt wird der Prozess für die Konfiguration der SAML-Authentifizierung mit Azure als Identitätsanbieter (IdP) für mehrere Verbindungsprofile in Cisco Firepower Threat Defense (FTD) beschrieben, die vom FirePOWER Management Center (FMC) verwaltet werden. Die IdP-Zertifikatüberschreibungsfunktion wird verwendet, um dies effektiv einzurichten.

Konfigurationsübersicht:

Auf Cisco FTD sind zwei Verbindungsprofile zu konfigurieren:

- FTD-SAML-1
- FTD-SAML-2

In diesem Konfigurationsbeispiel wird die VPN-Gateway-URL (Cisco Secure Client FQDN) auf nigarapa2.cisco.com festgelegt.

Konfigurieren

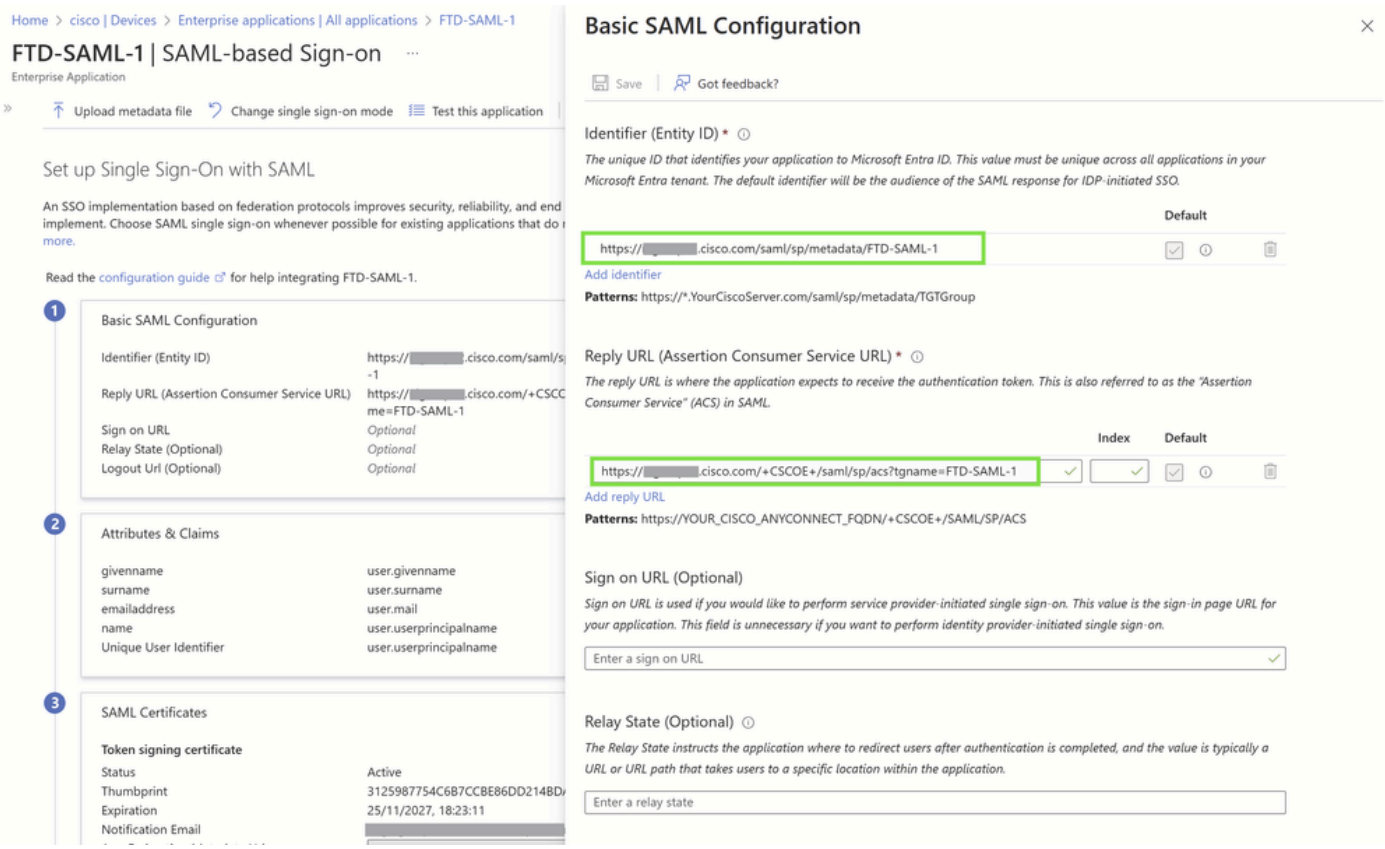
Konfiguration auf Azure IdP

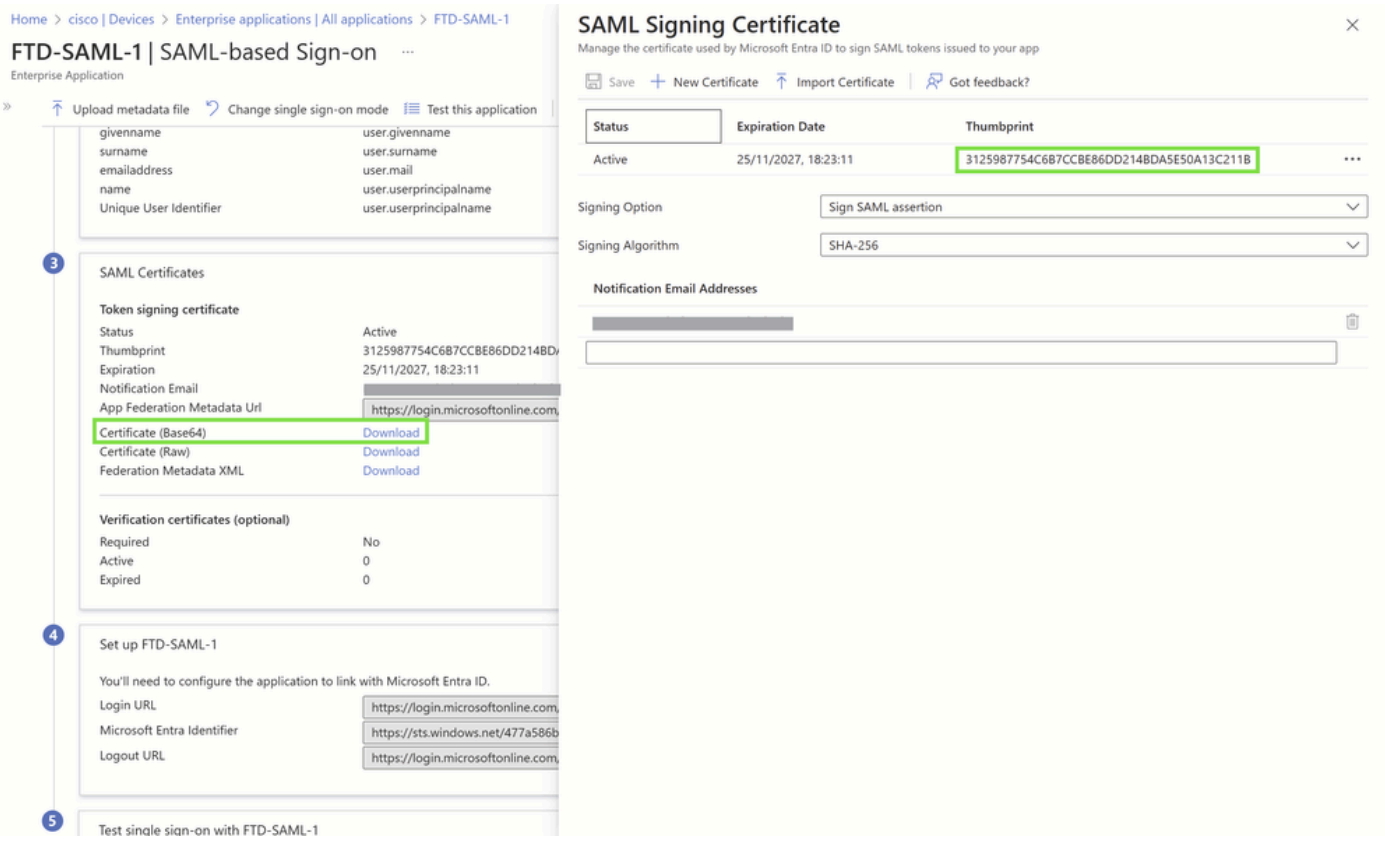
Um die SAML-Unternehmensanwendungen für den Cisco Secure Client effektiv zu konfigurieren, stellen Sie sicher, dass alle Parameter für jede Tunnelgruppe richtig eingestellt sind. Gehen Sie dazu wie folgt vor:

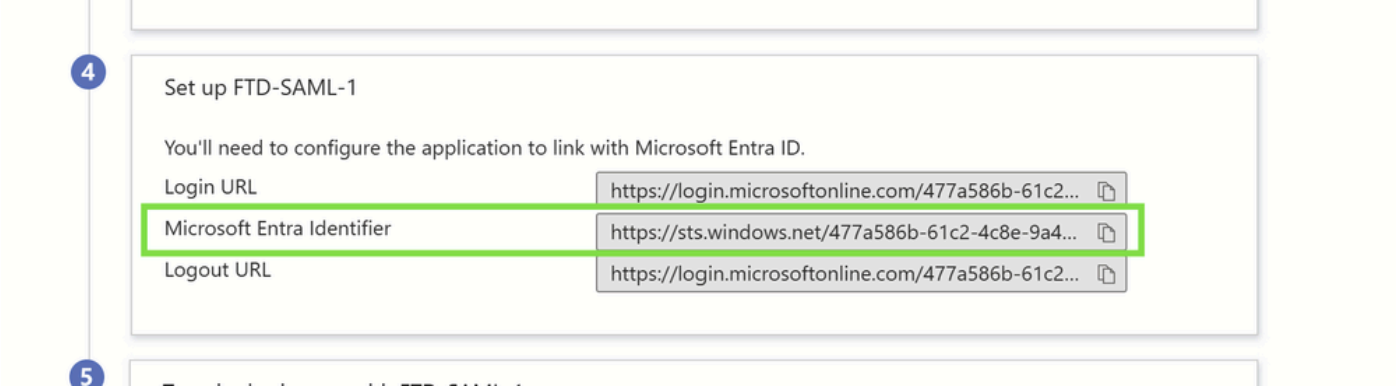
- Zugriff auf SAML Enterprise-Anwendungen:
  - Navigieren Sie zur Administrationskonsole Ihres SAML-Anbieters, in der Ihre Unternehmensanwendungen aufgeführt sind.
- Wählen Sie die entsprechende SAML-Anwendung aus:
  - Identifizieren Sie die SAML-Anwendungen, die den Cisco Secure Client-Tunnelgruppen entsprechen, die Sie konfigurieren möchten, und wählen Sie diese aus.
- Identifikator (Element-ID) konfigurieren:
  - Legen Sie den Bezeichner (Element-ID) für jede Anwendung fest. Dies muss die Basis-URL sein, d. h. Ihr vollqualifizierter Domänenname (FQDN) für den Cisco Secure Client.
- Legen Sie die Antwort-URL (Assertion Consumer Service-URL) fest:
  - Konfigurieren Sie die Antwort-URL (Assertion Consumer Service-URL) mit der richtigen Basis-URL. Stellen Sie sicher, dass sie mit dem FQDN des Cisco Secure Client übereinstimmt.
  - Hängen Sie den Namen des Verbindungsprofils oder der Tunnelgruppe an die Basis-URL an, um die Spezifität sicherzustellen.
- Konfiguration überprüfen:
  - Überprüfen Sie, ob alle URLs und Parameter korrekt eingegeben wurden und den jeweiligen Tunnelgruppen entsprechen.
  - Speichern Sie die Änderungen, und führen Sie nach Möglichkeit eine Testauthentifizierung durch, um sicherzustellen, dass die Konfiguration wie erwartet funktioniert.

Weitere Informationen finden Sie in der Cisco Dokumentation unter "Add Cisco Secure Client from the Microsoft App Gallery" (Cisco Secure Client aus der Microsoft-Anwendungsgalerie hinzufügen): Konfigurieren von ASA Secure Client VPN mit Microsoft Azure MFA über SAML

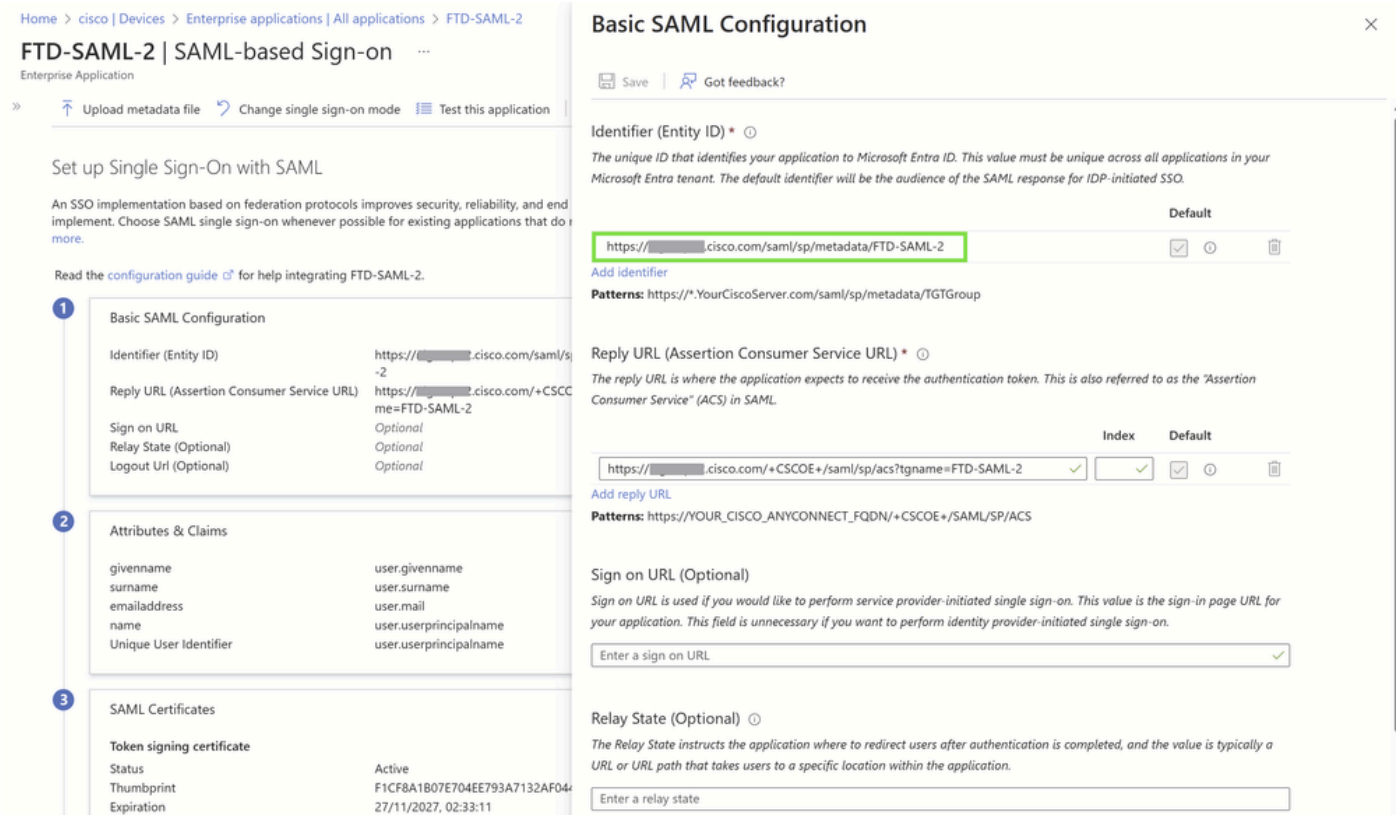
FTD-SAML-1

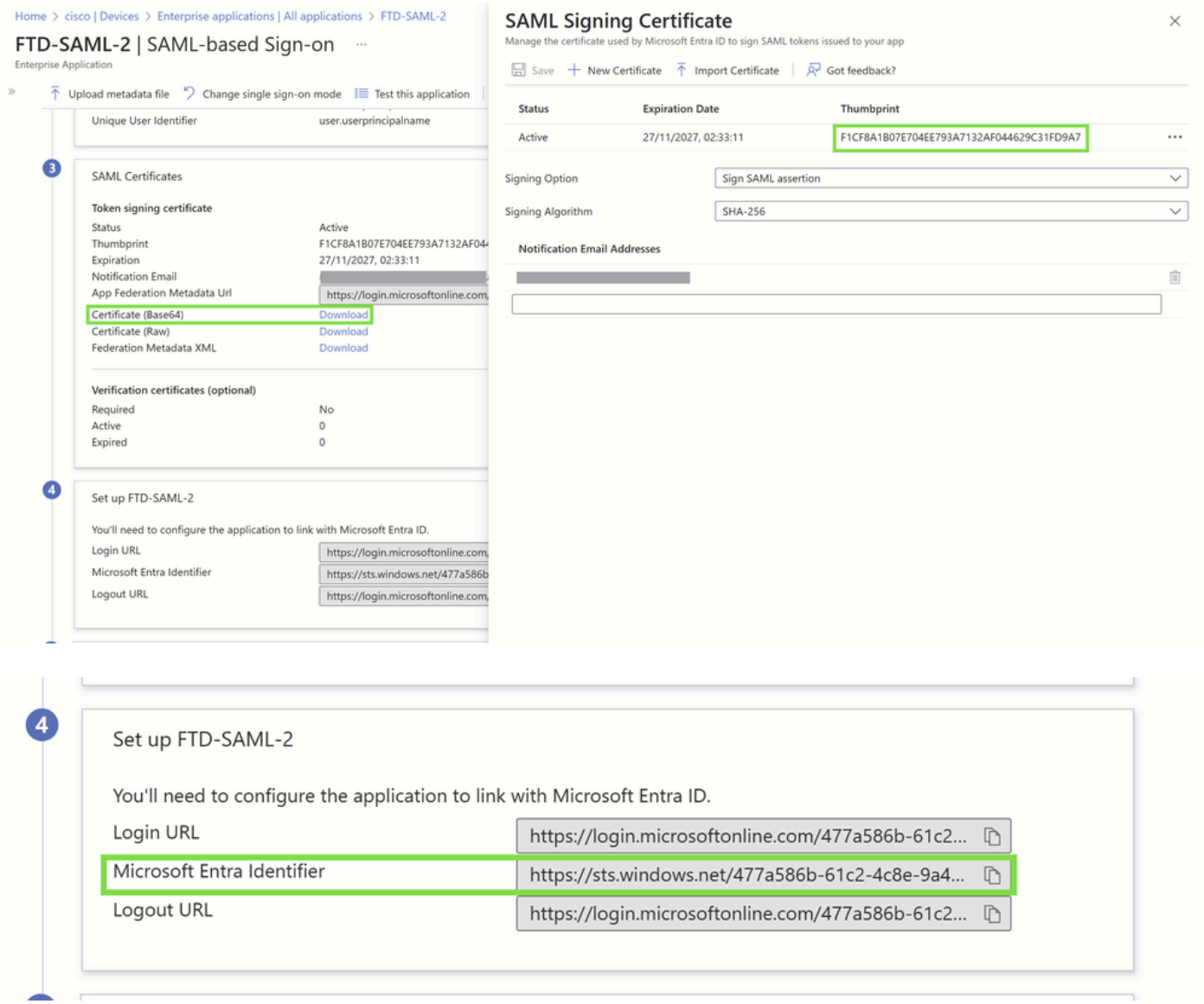

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-1.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
https://.cisco.com/saml/sp/metadata/FTD-SAML-1
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
https://.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-1
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
App Federation Metadata Url
https://login.microsoftonline.com/
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download
Verification certificates (optional)
Required
No
Active
0
Expired
0
4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/
Microsoft Entra Identifier
https://sts.windows.net/477a586b
Logout URL
https://login.microsoftonline.com/
5
Test single sign-on with FTD-SAML-1
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
25/11/2027, 18:23:11
3125987754C6B7CCBE86DD214BDA5E50A13C211B
Signing Option
Sign SAML assertion
Signing Algorithm
SHA-256
Notification Email Addresses


4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/477a586b-61c2...
Microsoft Entra Identifier
https://sts.windows.net/477a586b-61c2-4c8e-9a4...
Logout URL
https://login.microsoftonline.com/477a586b-61c2...
5

FTD-SAML-2


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-2
FTD-SAML-2 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-2.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Thumbprint
Expiration
Active
27/11/2027, 02:33:11
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
.cisco.com/saml/sp/metadata/FTD-SAML-2
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-2
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state



Stellen Sie nun sicher, dass Sie über die erforderlichen Informationen und Dateien für die Konfiguration der SAML-Authentifizierung mit Microsoft Entra als Identitätsanbieter verfügen:

Suchen Sie den Microsoft Entra Identifier:

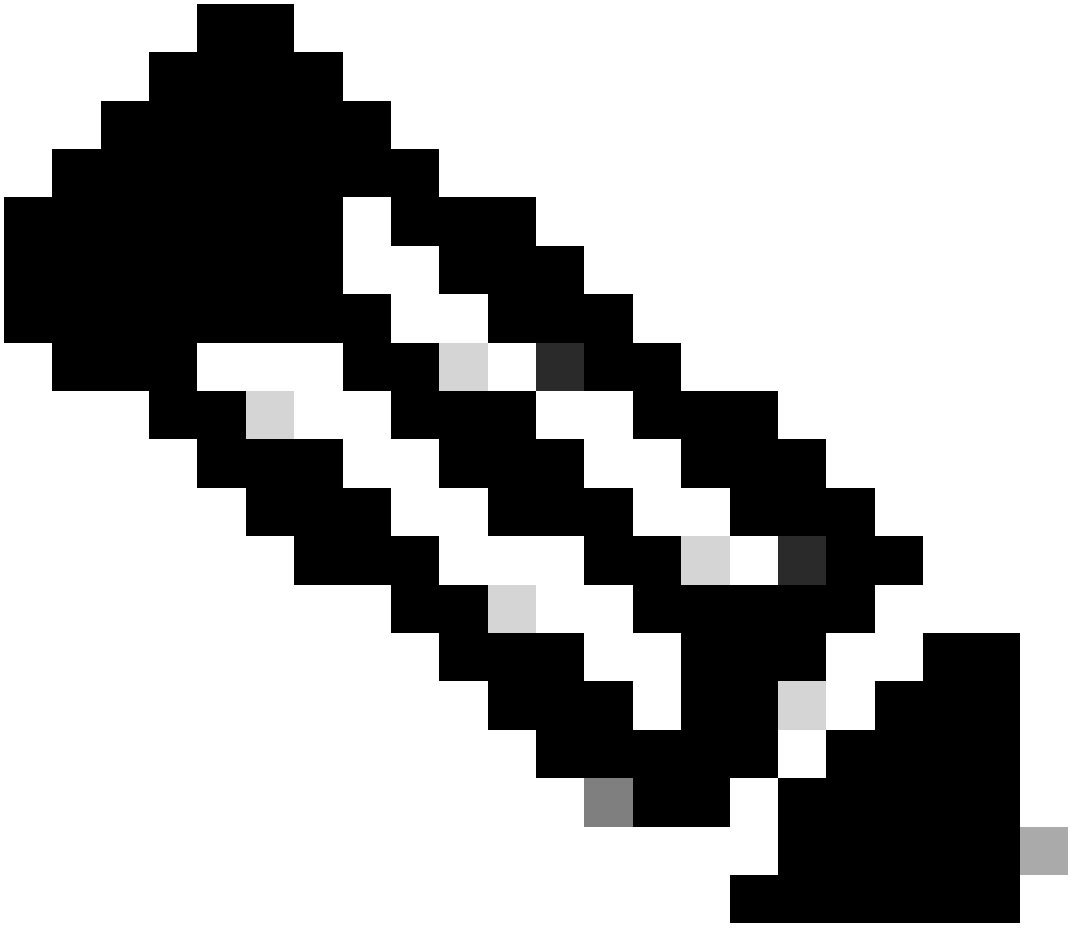
Greifen Sie auf die Einstellungen für beide SAML-Unternehmensanwendungen in Ihrem Microsoft Entra-Portal zu.

Beachten Sie den Microsoft Entra Identifier, der für beide Anwendungen konsistent bleibt und für Ihre SAML-Konfiguration von entscheidender Bedeutung ist.

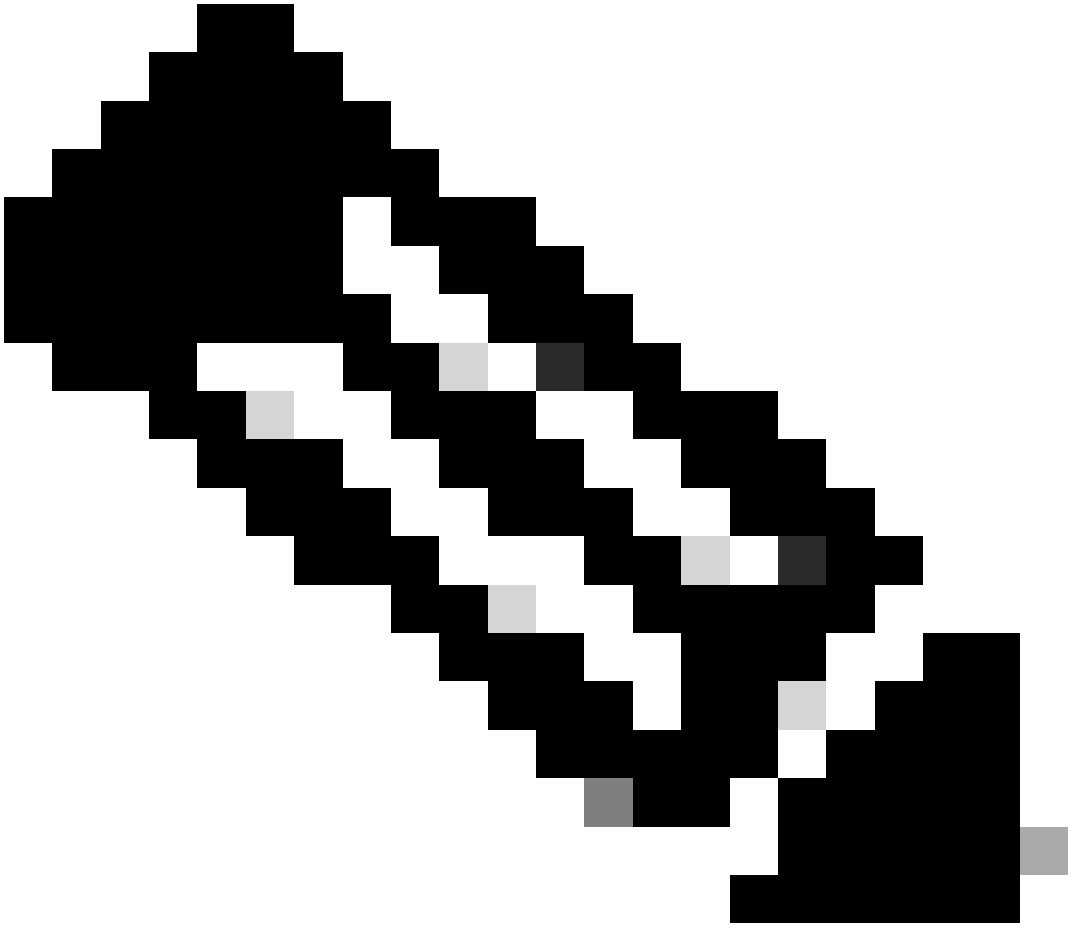
Base64 IdP-Zertifikate herunterladen:

Navigieren Sie zu jeder konfigurierten SAML-Unternehmensanwendung.

Laden Sie die entsprechenden Base64-codierten IdP-Zertifikate herunter. Diese Zertifikate sind für die Vertrauensstellung zwischen Ihrem Identitätsanbieter und Ihrem Cisco VPN-Setup unerlässlich.



Anmerkung: Alle diese für die FTD-Verbindungsprofile erforderlichen SAML-Konfigurationen können auch aus den Metadaten.xml-Dateien bezogen werden, die von Ihrem IdP für die jeweiligen Anwendungen bereitgestellt werden.



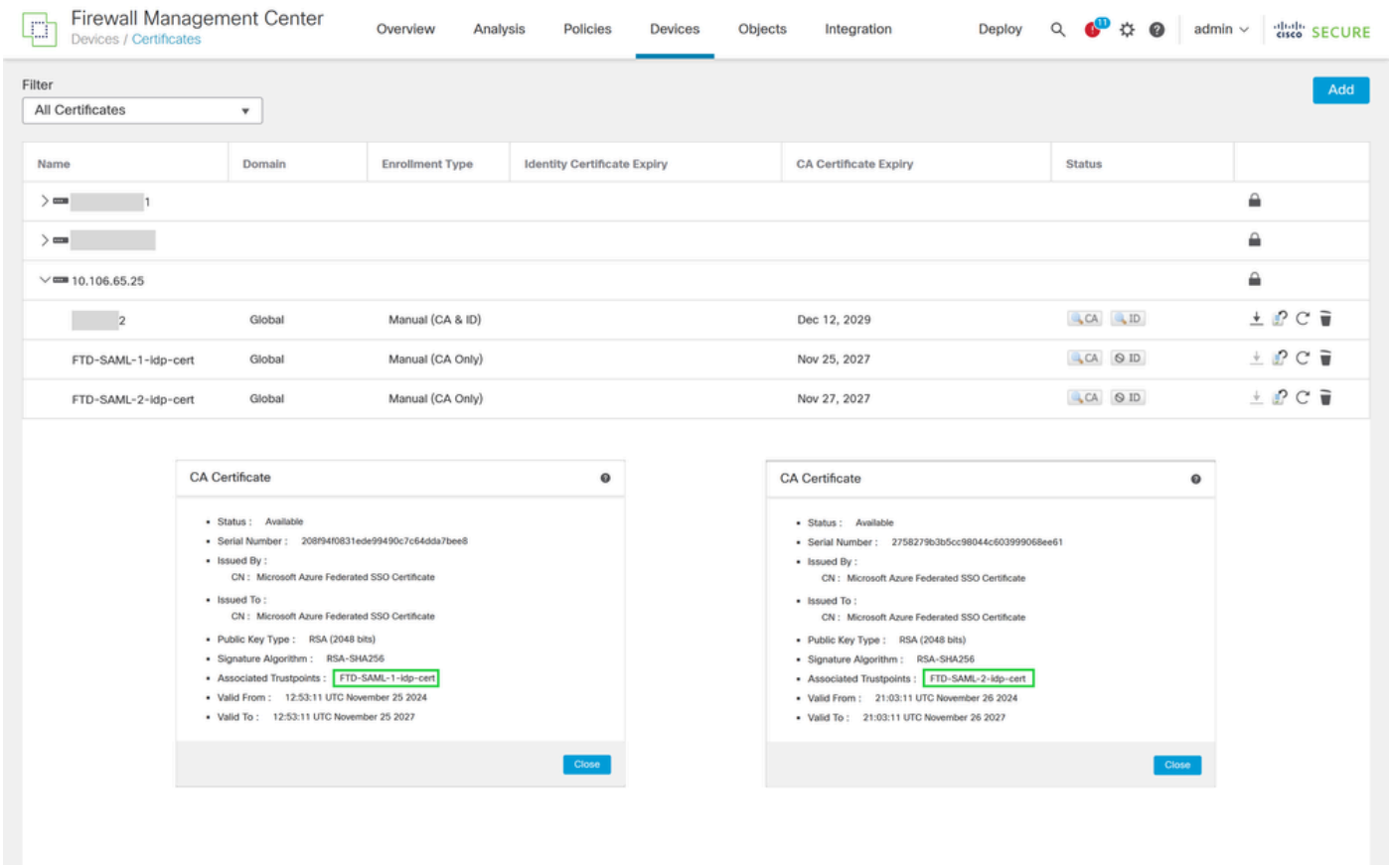
Anmerkung: Um ein benutzerdefiniertes IdP-Zertifikat zu verwenden, müssen Sie das benutzerdefinierte generierte IdP-Zertifikat sowohl in den IdP als auch in das FMC hochladen. Stellen Sie für Azure IdP sicher, dass das Zertifikat im PKCS#12-Format vorliegt. Laden Sie auf dem FMC nur das Identitätszertifikat von der IdP hoch, nicht die PKCS#12-Datei. Ausführliche Anweisungen finden Sie im Abschnitt "Laden Sie die PKCS#12-Datei auf Azure und FDM hoch" in der Cisco-Dokumentation: Konfiguration mehrerer RAVPN-Profile mit SAML-Authentifizierung auf FDM

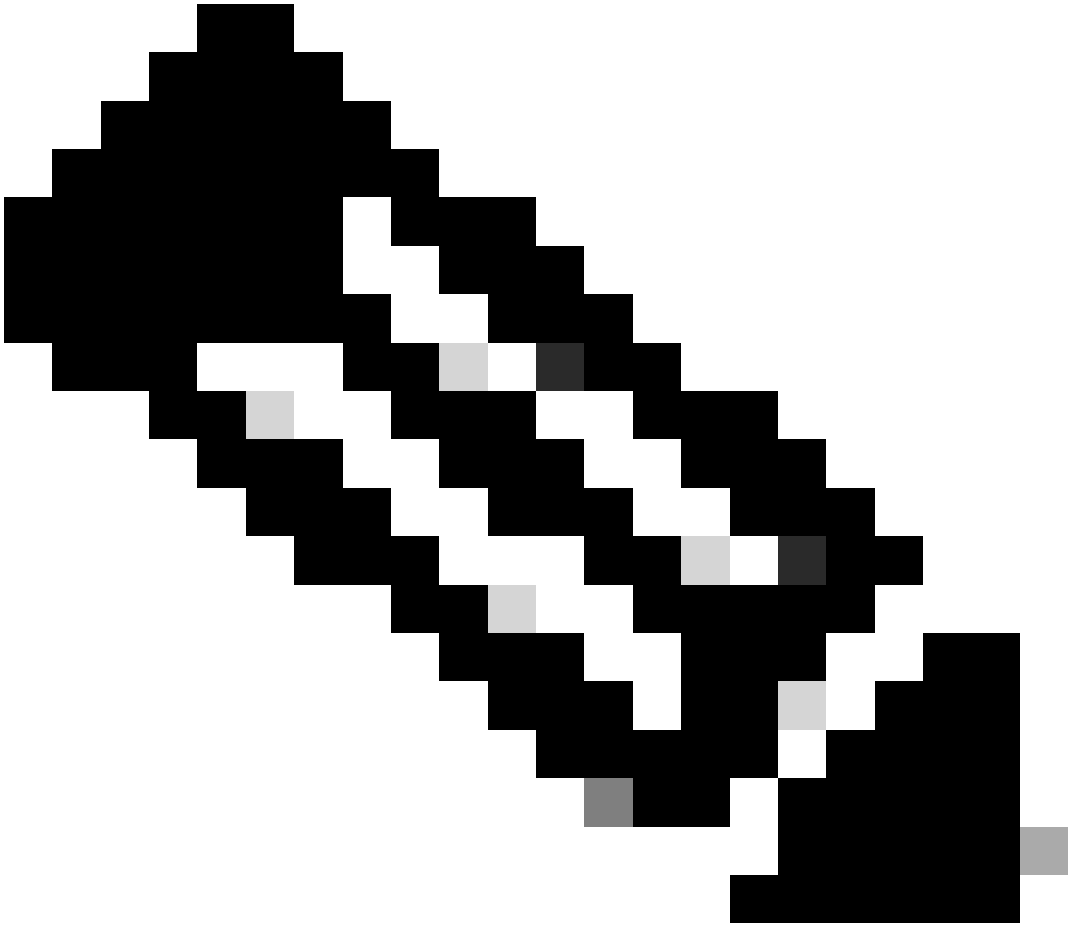
Konfiguration auf FTD über FMC

IDp-Zertifikate registrieren:

Navigieren Sie in FMC zum Abschnitt für das Zertifikatsmanagement, und registrieren Sie die heruntergeladenen Base64-codierten IdP-Zertifikate für beide SAML-Anwendungen. Diese Zertifikate sind für die Einrichtung von Vertrauen und die Aktivierung der SAML-Authentifizierung von entscheidender Bedeutung.

Ausführliche Informationen hierzu finden Sie in den ersten beiden Schritten unter "Configuration on the FTD via FMC" in der Cisco Dokumentation unter: [Konfigurieren Sie Secure Client mit SAML-Authentifizierung auf FTD Managed via FMC](#).





Anmerkung: Das Bild wurde so bearbeitet, dass beide Zertifikate gleichzeitig angezeigt werden. Es ist nicht möglich, beide Zertifikate gleichzeitig auf dem FMC zu öffnen.

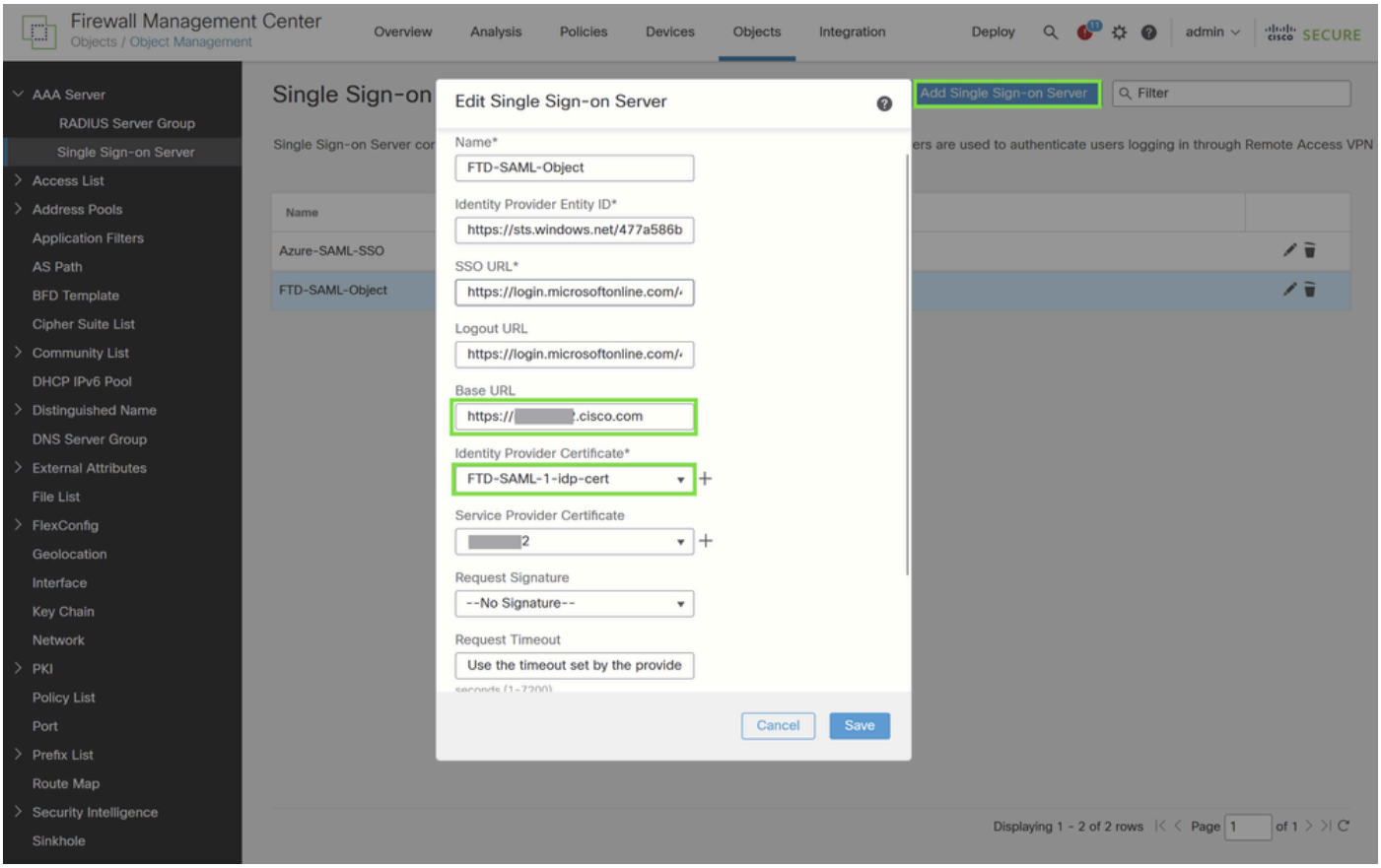
Konfigurieren der SAML-Servereinstellungen auf Cisco FTD über FMC

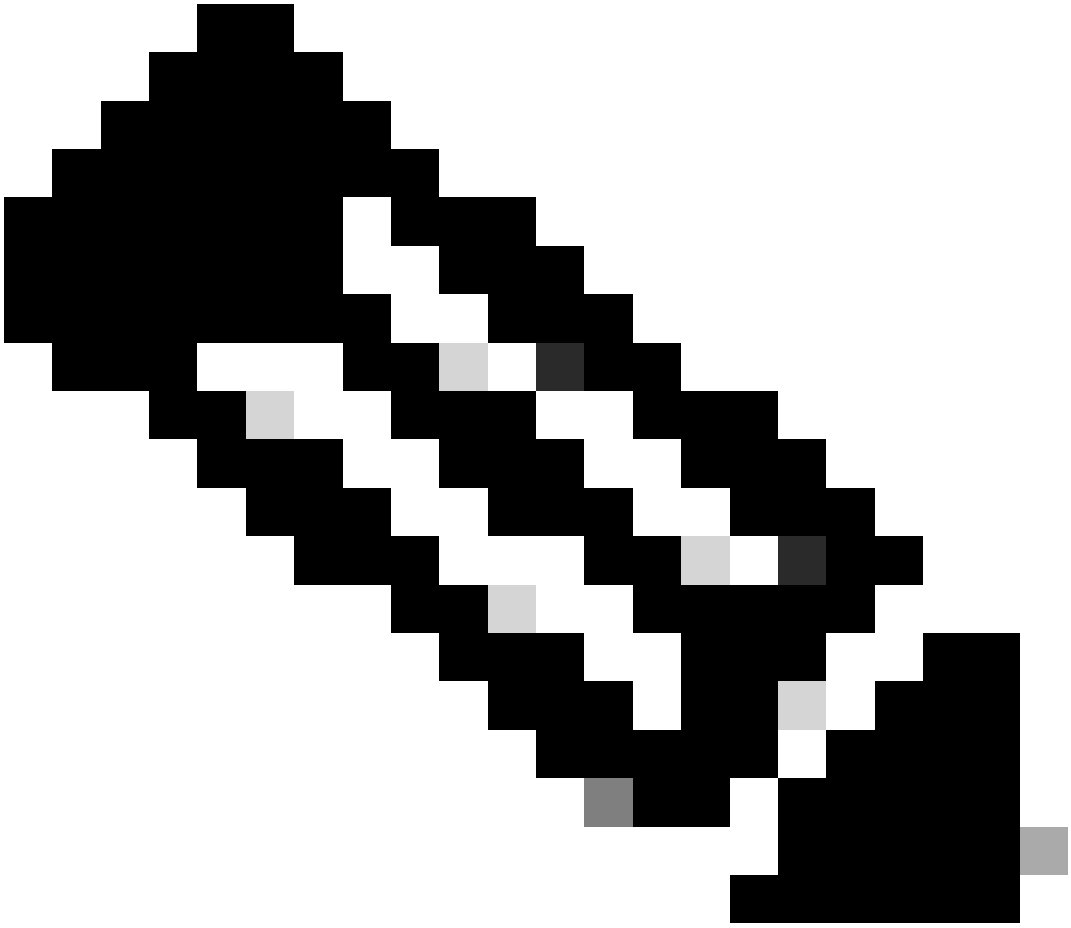
Um die SAML-Servereinstellungen auf Ihrem Cisco Firepower Threat Defense (FTD) mit dem Firepower Management Center (FMC) zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu Konfiguration des Single Sign-on-Servers:
    - Navigieren Sie zu Objekte > Objektverwaltung > AAA-Server > Single Sign-on-Server.
    - Klicken Sie auf Single Sign-on Server hinzufügen, um die Konfiguration eines neuen Servers zu beginnen.

2. Konfigurieren der SAML-Servereinstellungen:
    - Verwenden Sie die Parameter, die aus Ihren SAML-Unternehmensanwendungen oder aus der Metadaten.xml-Datei, die von Ihrem Identity Provider (IdP) heruntergeladen wurde, gesammelt wurden, und geben Sie die erforderlichen SAML-Werte im Formular New Single Sign-on Server (Neuer Single Sign-on Server) ein.

- Zu den wichtigsten zu konfigurierenden Parametern gehören:
  - SAML-Anbieter-Element-ID: entityID aus metadaten.xml
  - SSO-URL: SingleSignOnService aus metadaten.xml.
  - Abmelde-URL: SingleLogoutService aus metadaten.xml.
  - BASE-URL: FQDN Ihres FTD SSL ID Zertifikats.
  - Zertifikat des Identitätsanbieters: IDp-Signaturzertifikat.
    - Fügen Sie im Abschnitt Identity Provider Certificate (Identitätsanbieter-Zertifikat) eines der registrierten IdP-Zertifikate an.
    - Für diesen Anwendungsfall verwenden wir das IdP-Zertifikat der Anwendung FTD-SAML-1.
  - Dienstanbieterzertifikat: FTD-Signaturzertifikat.

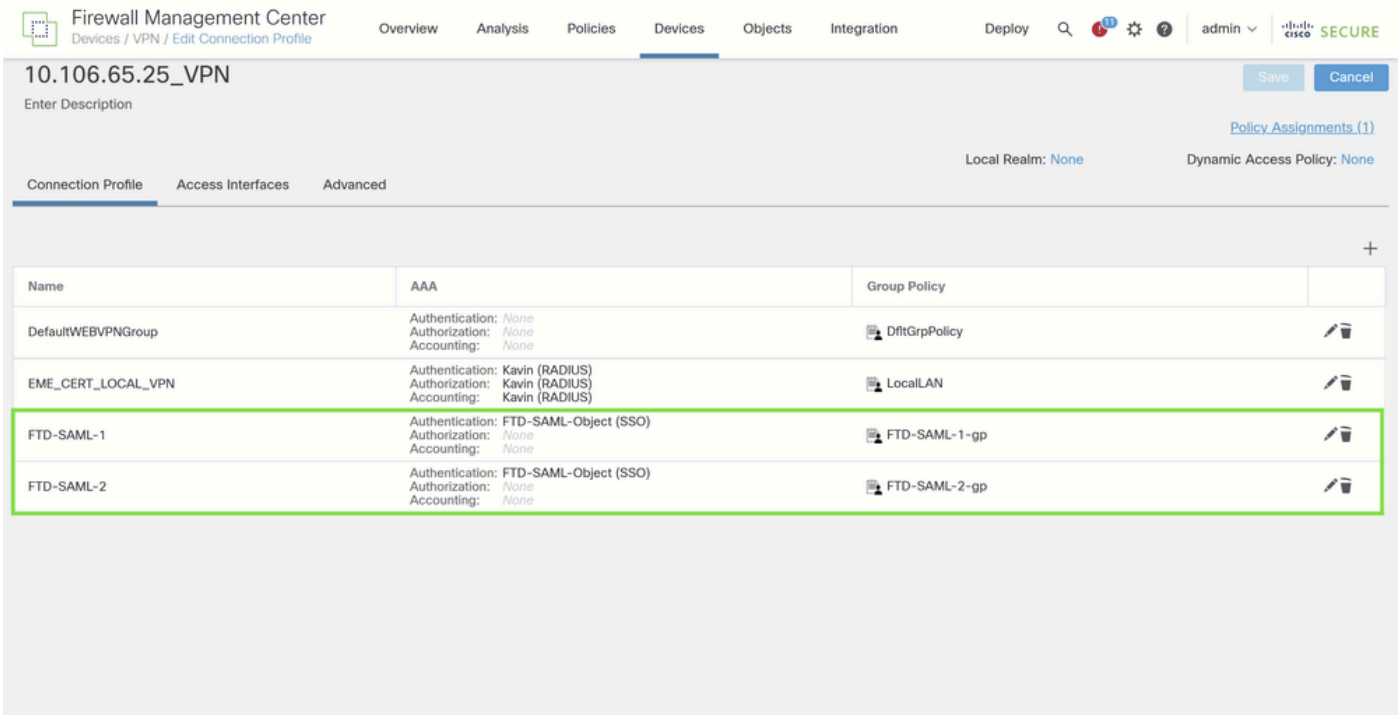




Anmerkung: In der aktuellen Konfiguration kann nur das Identity Provider-Zertifikat aus dem SAML-Objekt in den Verbindungsprofileinstellungen überschrieben werden. Leider können Funktionen wie "Request IdP re-authentication on login" und "Enable IdP only access on internal network" nicht für jedes Verbindungsprofil einzeln aktiviert oder deaktiviert werden.

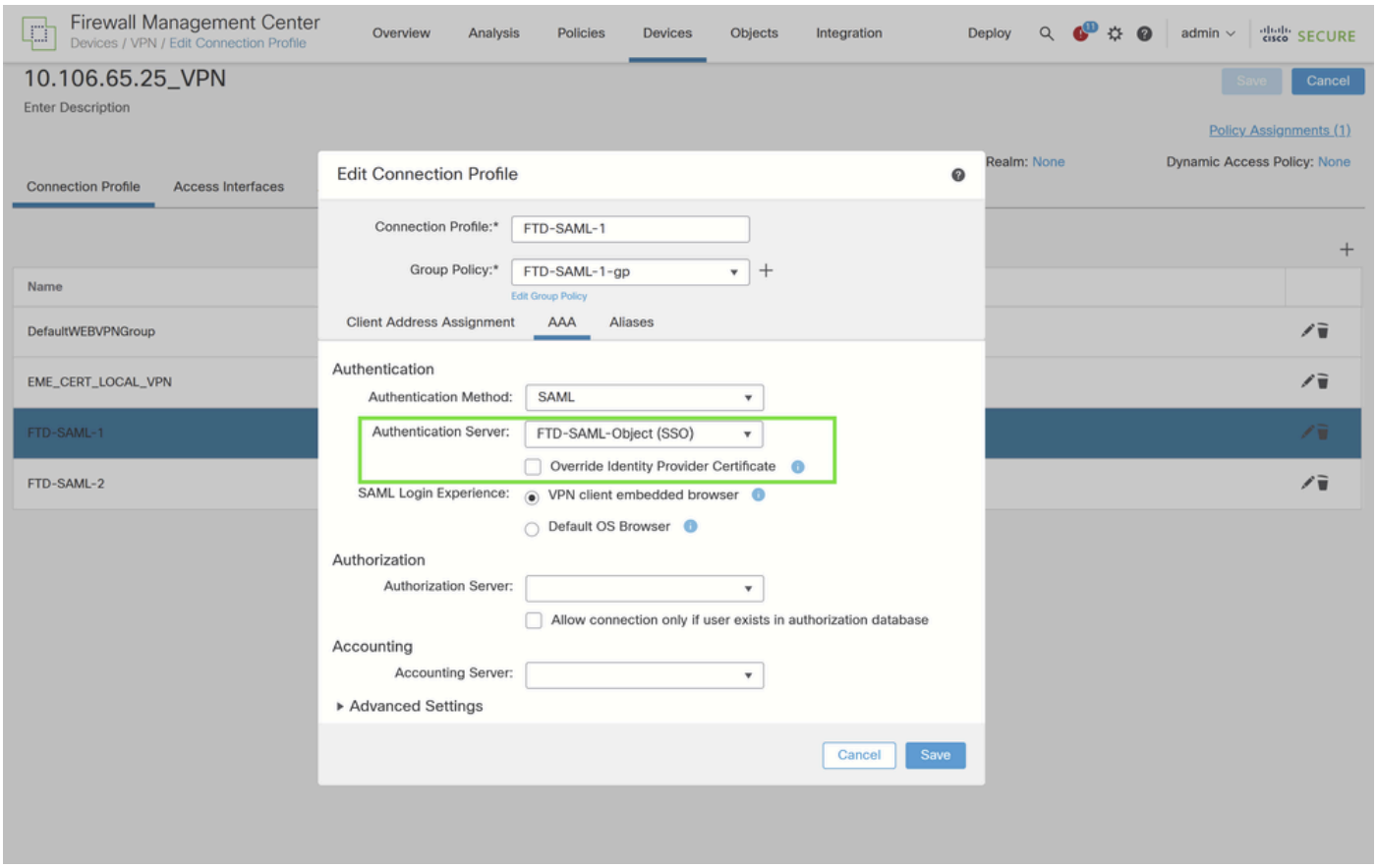
Konfigurieren von Verbindungsprofilen auf Cisco FTD über FMC

Um die Einrichtung der SAML-Authentifizierung abzuschließen, müssen Sie die Verbindungsprofile mit den entsprechenden Parametern konfigurieren und die AAA-Authentifizierung mithilfe des zuvor konfigurierten SAML-Servers auf SAML festlegen. Weitere Informationen finden Sie im fünften Schritt unter "Configuration on the FTD via FMC" in der Cisco Dokumentation: Konfigurieren Sie Secure Client mit SAML-Authentifizierung auf FTD Managed via FMC.



Auszug aus der AAA-Konfiguration für das erste Verbindungsprofil

Nachfolgend finden Sie eine Übersicht der AAA-Konfigurationseinstellungen für das erste Verbindungsprofil:



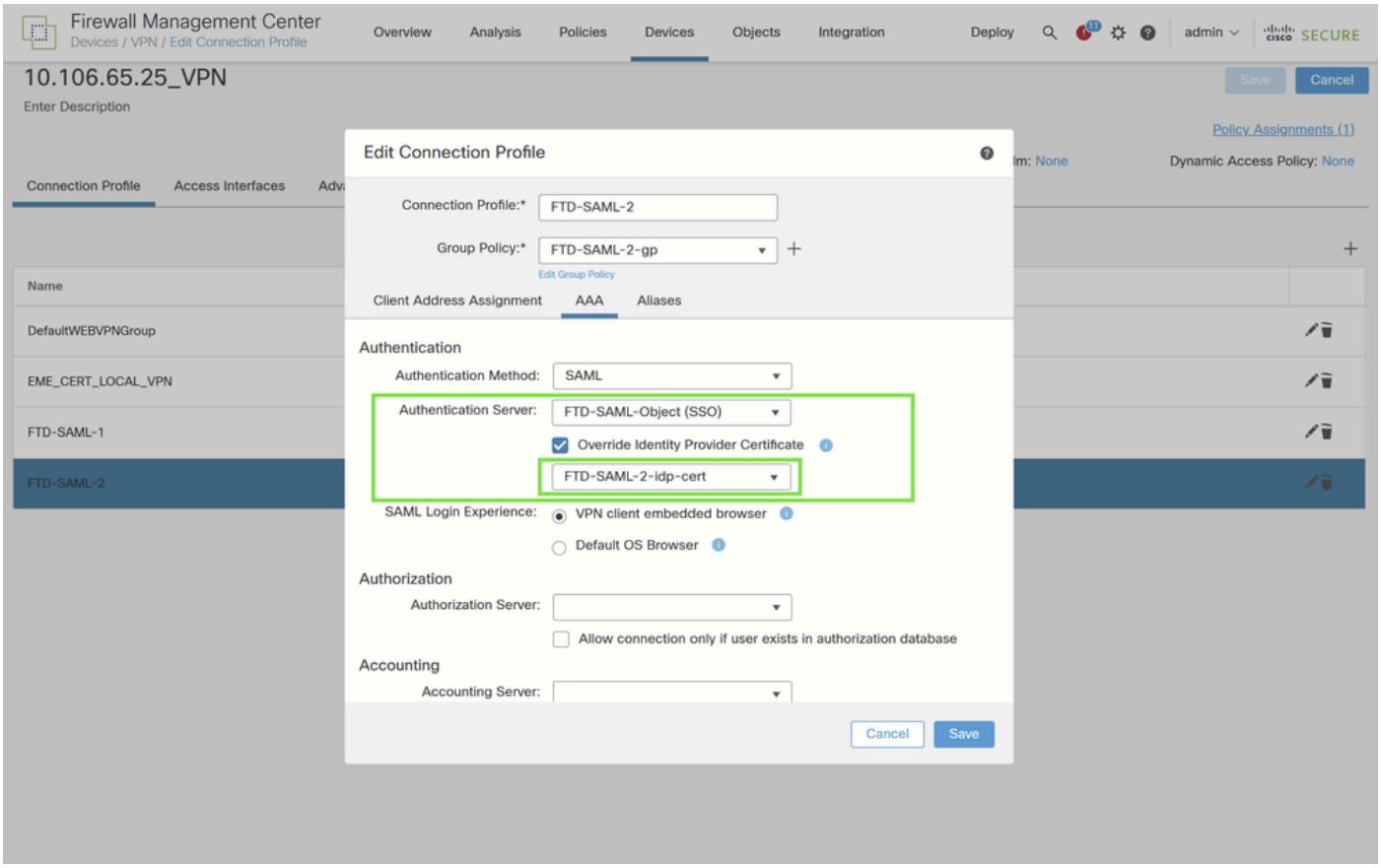
Konfigurieren der IDp-Zertifikatübersteuerung für das zweite Verbindungsprofil in Cisco FTD

Um sicherzustellen, dass das richtige Identity Provider (IdP)-Zertifikat für das zweite Verbindungsprofil verwendet wird, aktivieren Sie das Überschreiben des IdP-Zertifikats, indem Sie

die folgenden Schritte ausführen:

Suchen Sie in den Einstellungen für das Verbindungsprofil nach der Option "Identitätsanbieter-Zertifikat überschreiben", und aktivieren Sie sie, damit ein anderes als das für den SAML-Server konfigurierte IdP-Zertifikat verwendet werden kann.

Wählen Sie aus der Liste der registrierten IdP-Zertifikate das Zertifikat aus, das speziell für die Anwendung FTD-SAML-2 registriert wurde. Durch diese Auswahl wird sichergestellt, dass bei einer Authentifizierungsanforderung für dieses Verbindungsprofil das richtige IdP-Zertifikat verwendet wird.



Bereitstellung der Konfiguration

Navigieren Sie**Deploy** > **Deployment**zu, und wählen Sie das FTD aus, das die VPN-Änderungen für die SAML-Authentifizierung übernehmen soll.

Überprüfung

Konfiguration in der FTD-Befehlszeile

<#root>

```
firepower# sh run 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
    Secure Client image disk0:/csm/Secure Client-win-4.10.08025-webdeploy.pkg 1 regex "Windows"
    Secure Client enable


 saml idp https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


        url sign-in https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        url sign-out https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        base-url https://nigarapa2.cisco.com


        trustpoint idp FTD-SAML-1-idp-cert


        trustpoint sp nigarapa2


        no signature


        force re-authentication


    tunnel-group-list enable
    cache
        disable
    error-recovery disable
firepower#
```

<#root>

```
firepower# sh run tunnel-group FTD-SAML-1
tunnel-group FTD-SAML-1 type remote-access
tunnel-group FTD-SAML-1 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-1-gp
tunnel-group FTD-SAML-1 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-1 enable


saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/
```

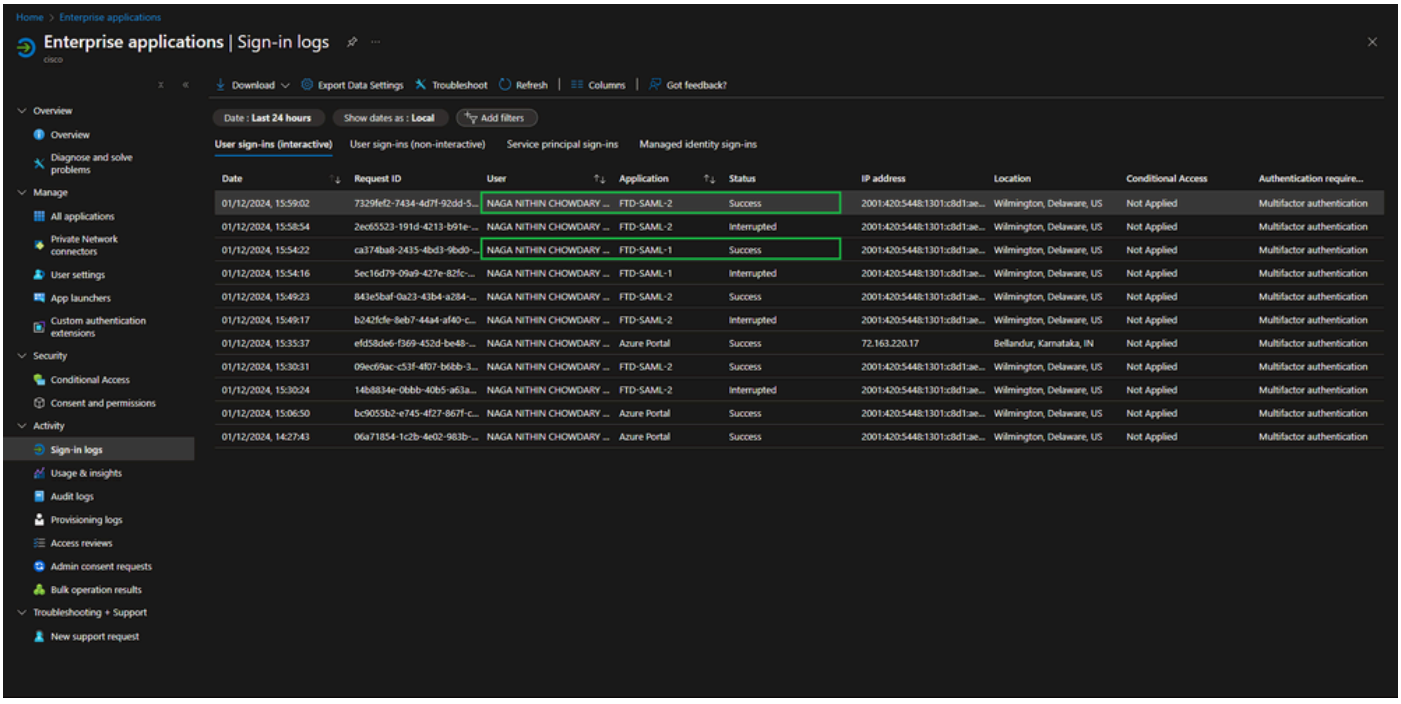
```
firepower#
```

<#root>

```
firepower# sh run tunnel-group FTD-SAML-2
tunnel-group FTD-SAML-2 type remote-access
tunnel-group FTD-SAML-2 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable
    saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/
    saml idp-trustpoint FTD-SAML-2-idp-cert
firepower#
```

Anmelde-Protokolle von Azure Central Identifier

Greifen Sie unter der Enterprise-Anwendung auf den Abschnitt Anmelde-Logs zu. Suchen Sie nach Authentifizierungsanforderungen, die sich auf die spezifischen Verbindungsprofile beziehen, z. B. FTD-SAML-1 und FTD-SAML-2. Überprüfen Sie, ob die Benutzer sich erfolgreich über die SAML-Anwendungen authentifizieren, die den einzelnen Verbindungsprofilen zugeordnet sind.



Anmeldeprotokolle auf Azure IdP

Fehlerbehebung

1. Sie können die Fehlerbehebung mit DART über den Secure Client-Benutzer-PC durchführen.
2. Um ein SAML-Authentifizierungsproblem zu beheben, verwenden Sie den folgenden Debugger:

   <#root>

   ```
   firepower#
    debug webvpn saml 255
   ```

3. Überprüfen Sie die Konfiguration des sicheren Clients wie oben beschrieben. kann dieser Befehl verwendet werden, um das Zertifikat zu überprüfen.

   <#root>

   ```
   firepower#
    show crypto ca certificate
   ```

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.