Konfiguration mehrerer Tunnelgruppen mit SAML auf ASA

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

SAML SP-Initiated SSO

Konfigurationen

- Cisco Secure Firewall - Secure Client aus der Galerie hinzufügen
- Azure AD-Benutzer der App zuweisen
- ASA-Konfiguration über CLI

Überprüfung

Fehlerbehebung

Zugehörige Informationen

Einleitung

In diesem Dokument wird die SAML-Authentifizierung mit Azure Identity Provider für mehrere Tunnelgruppen auf der Cisco ASA beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Adaptive Security Appliance (ASA)
- Security Assertion Markup Language (SAML)
- Secure Socket Layer (SSL)-Zertifikate
- Microsoft Azure

Verwendete Komponenten

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

- ASA 9.22(1)1

- Microsoft Azure 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

Microsoft Azure kann mehrere Anwendungen für dieselbe Entitäts-ID unterstützen. Jede Anwendung (einer anderen Tunnelgruppe zugeordnet) erfordert ein eindeutiges Zertifikat. Auf ASA können mehrere Tunnelgruppen so konfiguriert werden, dass sie aufgrund der IdP-Zertifikatfunktion andere IdP-geschützte Anwendungen (Override Identity Provider) verwenden. Mit dieser Funktion können Administratoren das primäre IdP-Zertifikat im SSO-Serverobjekt (Single Sign-On) mit einem spezifischen IdP-Zertifikat für jede Tunnelgruppe überschreiben. Diese Funktion wurde auf ASA ab Version 9.17.1 eingeführt.

SAML SP-Initiated SSO

Wenn der Endbenutzer die Anmeldung mit Zugriff auf die ASA initiiert, wird das Anmeldeverhalten wie folgt fortgesetzt:

1. Wenn der VPN-Benutzer auf eine SAML-fähige Tunnelgruppe zugreift oder diese auswählt, wird der Endbenutzer zur Authentifizierung an die SAML-IDp umgeleitet. Der Benutzer wird dazu aufgefordert, es sei denn, der Benutzer greift direkt auf die Gruppen-URL zu. In diesem Fall erfolgt die Umleitung nicht.

2. Die ASA generiert eine SAML-Authentifizierungsanforderung, die der Browser an die SAML-IDp umleitet.

3. Der IdP fordert den Endbenutzer zur Eingabe von Anmeldeinformationen auf, und der Endbenutzer meldet sich an. Die eingegebenen Anmeldeinformationen müssen der IDp-Authentifizierungskonfiguration entsprechen.

4. Die IdP-Antwort wird an den Browser zurückgesendet und an die ASA-Anmelde-URL gesendet. Die ASA verifiziert die Antwort, um die Anmeldung abzuschließen.

Konfigurationen

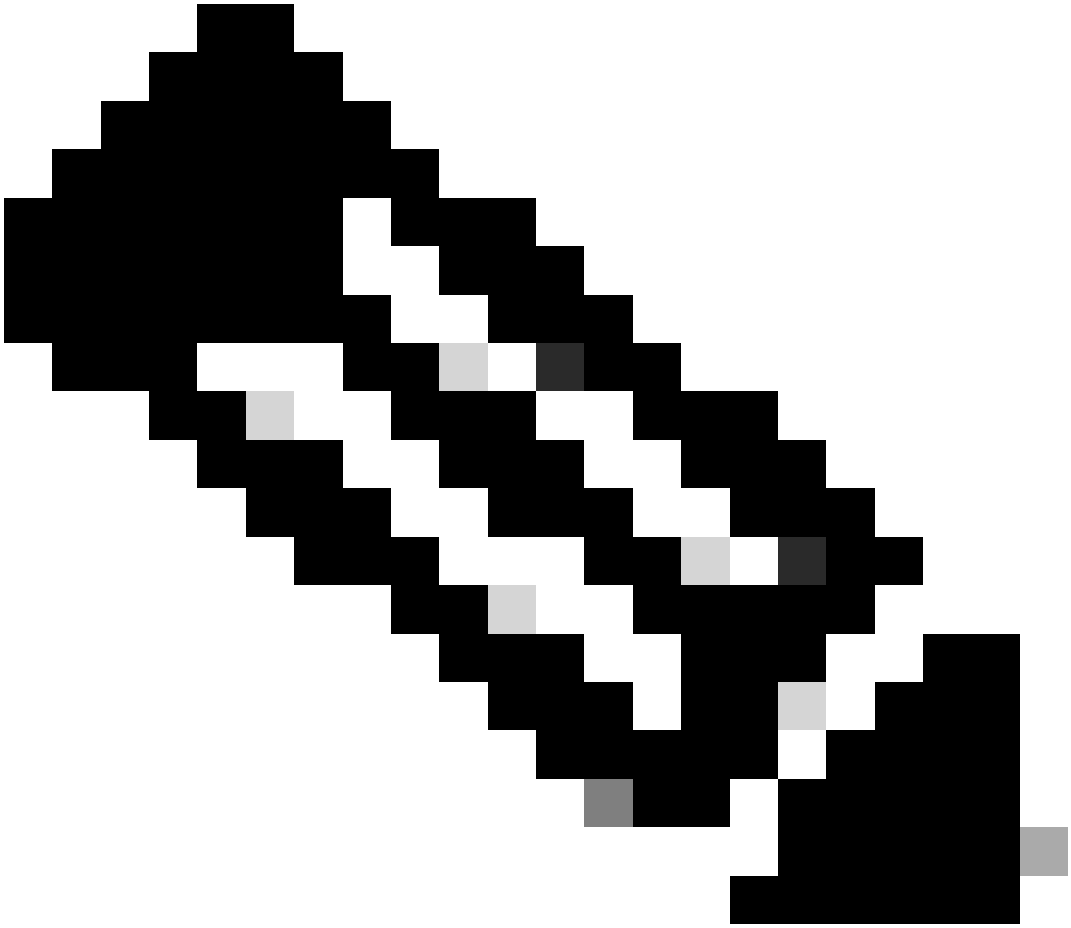
Cisco Secure Firewall - Secure Client aus der Galerie hinzufügen

In diesem Beispiel wird die Microsoft Entra SSO-Integration mit Cisco Secure Firewall - Secure Client auf Azure für zwei auf ASA konfigurierte Tunnelgruppen hinzugefügt:

- SAML1

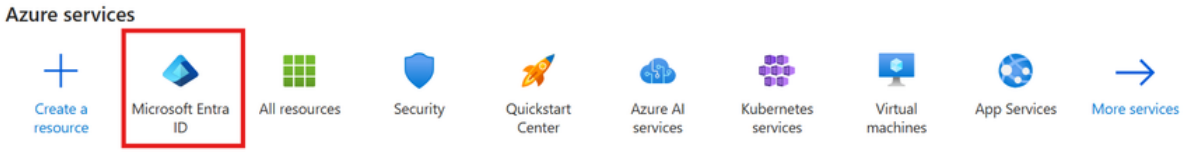
- SAML2

Um die Integration von Cisco Secure Firewall - Secure Client in Microsoft Entra ID zu konfigurieren, müssen Sie Cisco Secure Firewall - Secure Client aus der Galerie zu Ihrer Liste der verwalteten SaaS-Anwendungen hinzufügen.



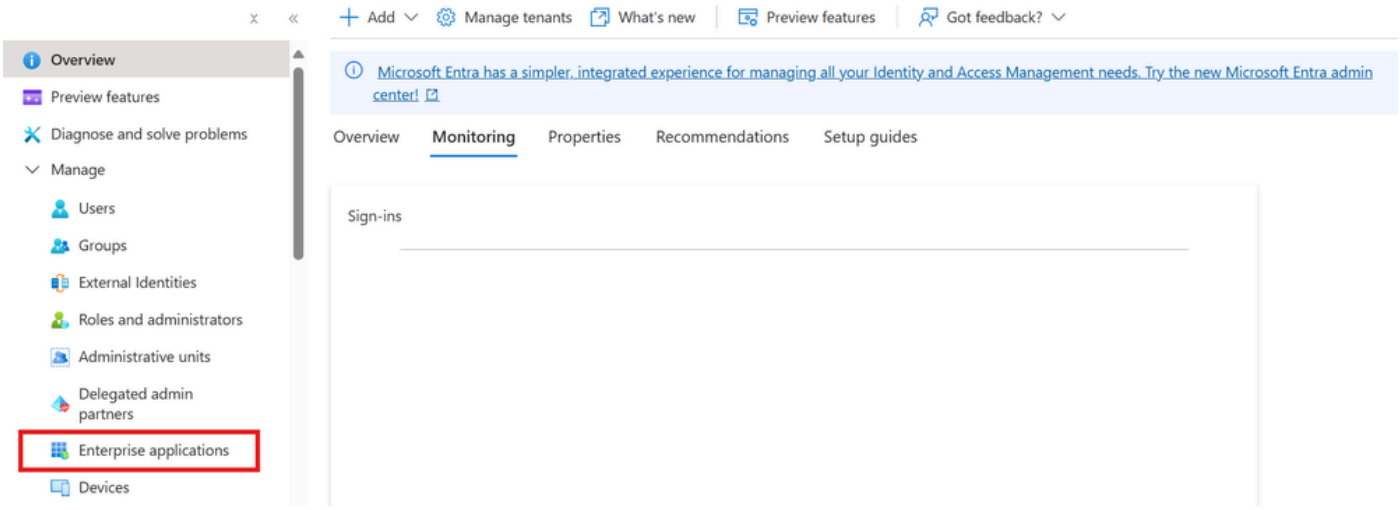
> Anmerkung: Mit diesen Schritten fügen Sie der Galerie für die erste Tunnelgruppe SAML1 Cisco Secure Firewall - Secure Client hinzu.

Schritt 1. Melden Sie sich beim Azure-Portal an, und wählen Sie Microsoft Entra ID aus.



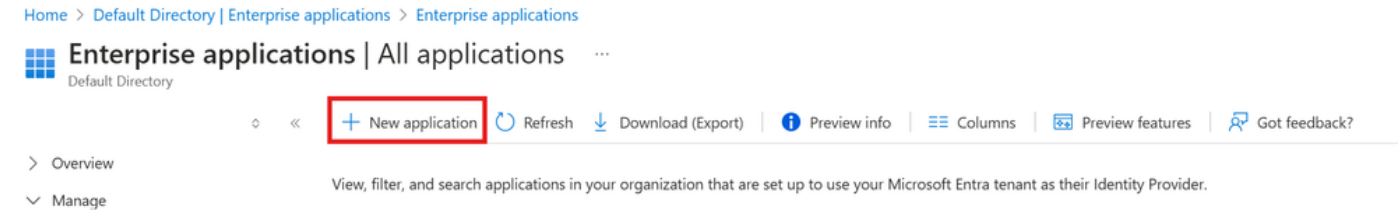
Microsoft Entra-ID

Schritt 2: Wählen Sie, wie in dieser Abbildung dargestellt, Enterprise Applications aus.



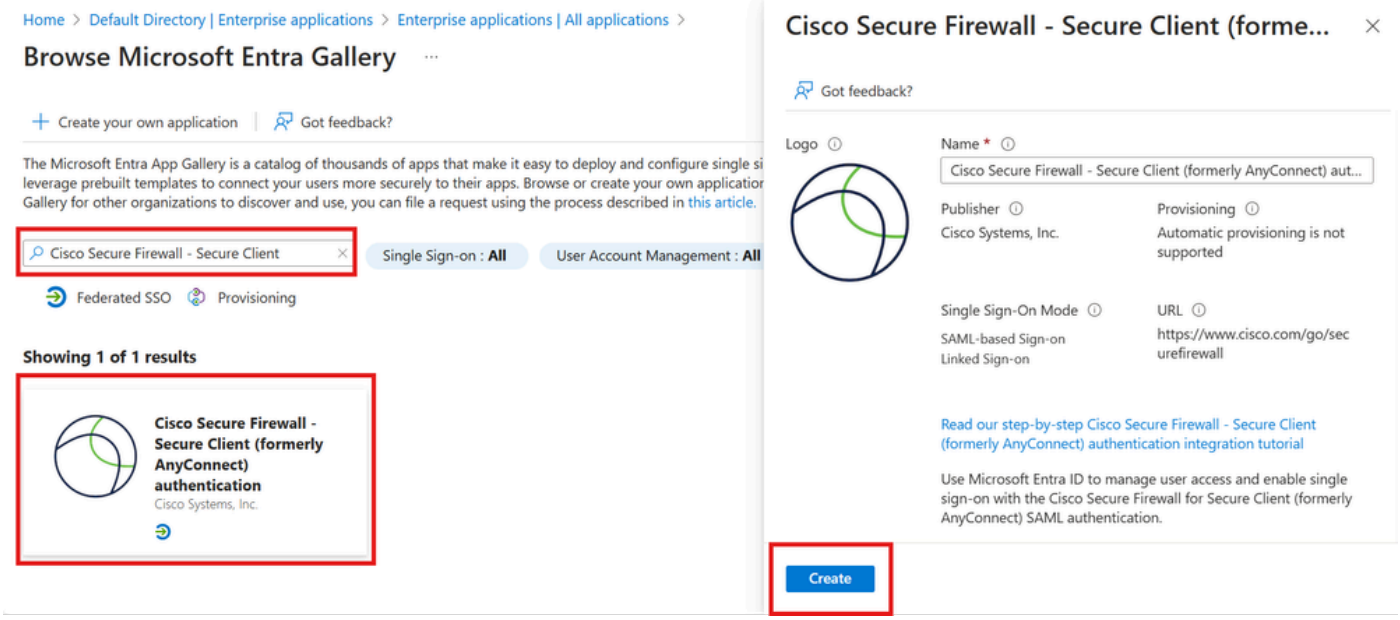
Enterprise-Anwendung

Schritt 3. Wählen Sie nun Neue Anwendung, wie in diesem Bild dargestellt.



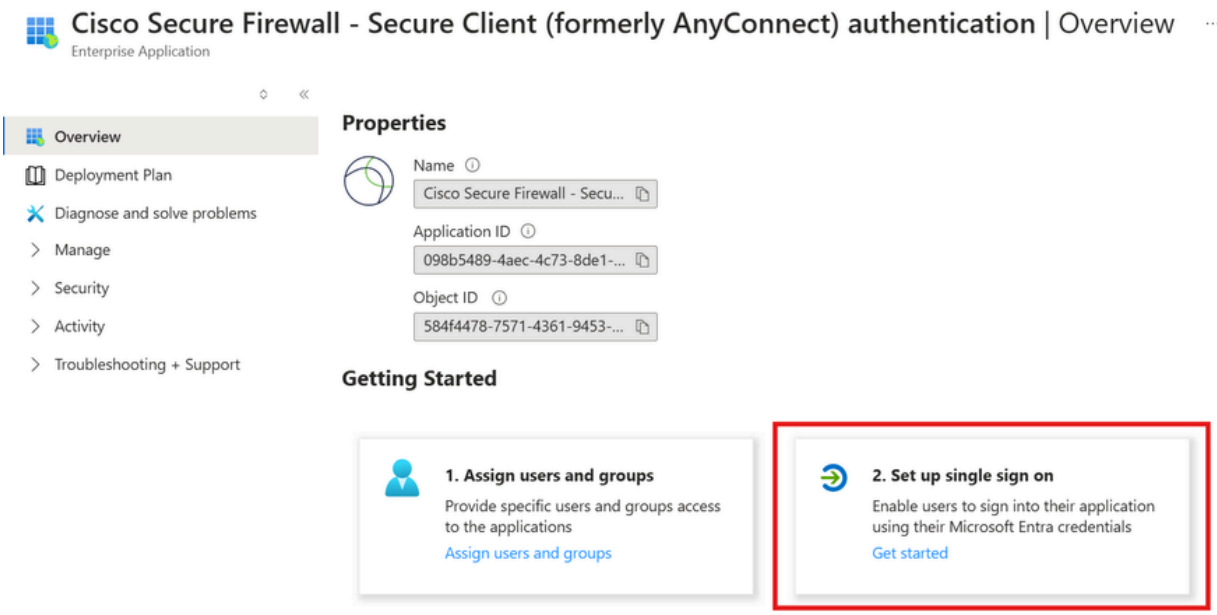
Neue Anwendung

Schritt 4. Geben Sie im Abschnitt Aus Galerie hinzufügen im Suchfeld Cisco Secure Firewall - Secure Client ein, wählen Sie Cisco Secure Firewall - Secure Client aus dem Ergebnisfenster, und fügen Sie die App hinzu.



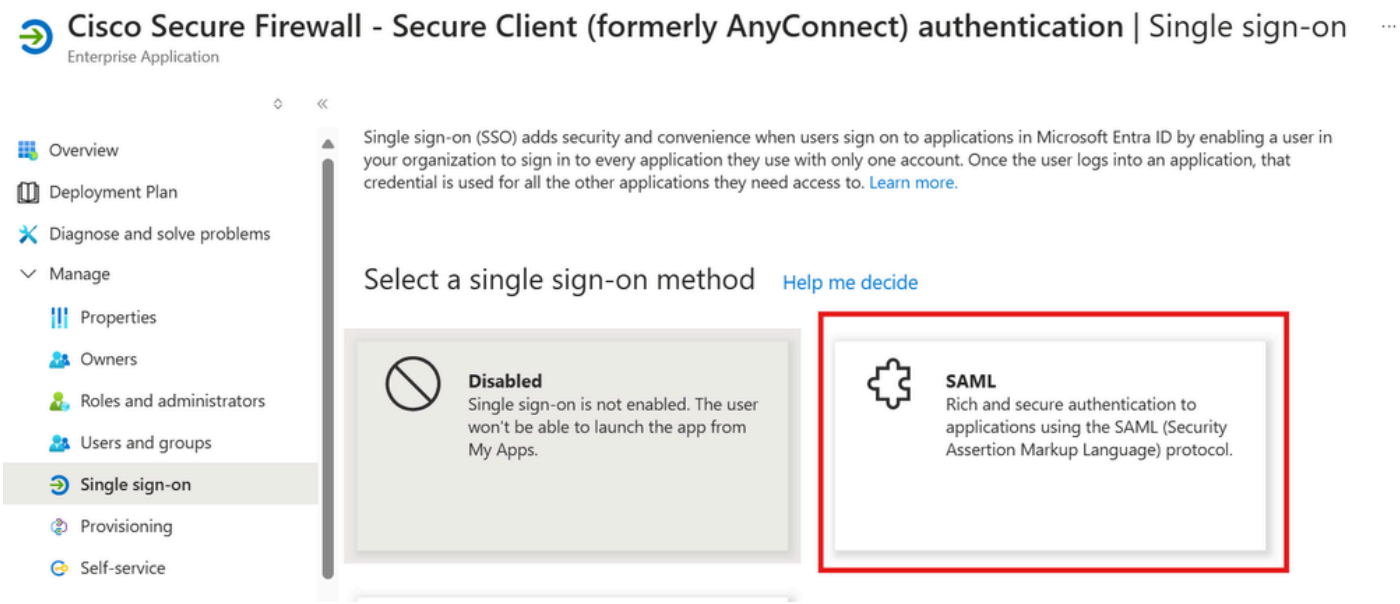
Cisco Secure Firewall - Secure Client

Schritt 5. Wählen Sie den Menüpunkt Single Sign-on (einmalige Anmeldung), wie in diesem Bild dargestellt.



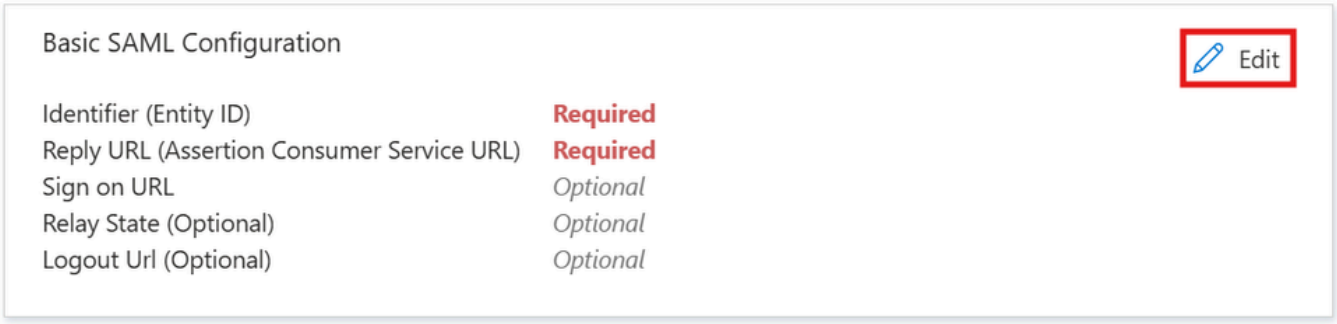
Single Sign-On einrichten

Schritt 6: Wählen Sie auf der Seite Select a single sign-on method die Option SAML aus.



SAML

Schritt 7: Klicken Sie auf der Seite Einmalige Anmeldung mit SAML einrichten auf das Bearbeiten/Öffnen-Symbol für SAML-Basiskonfiguration, um die Einstellungen zu bearbeiten.



Grundlegende Saml-Konfiguration

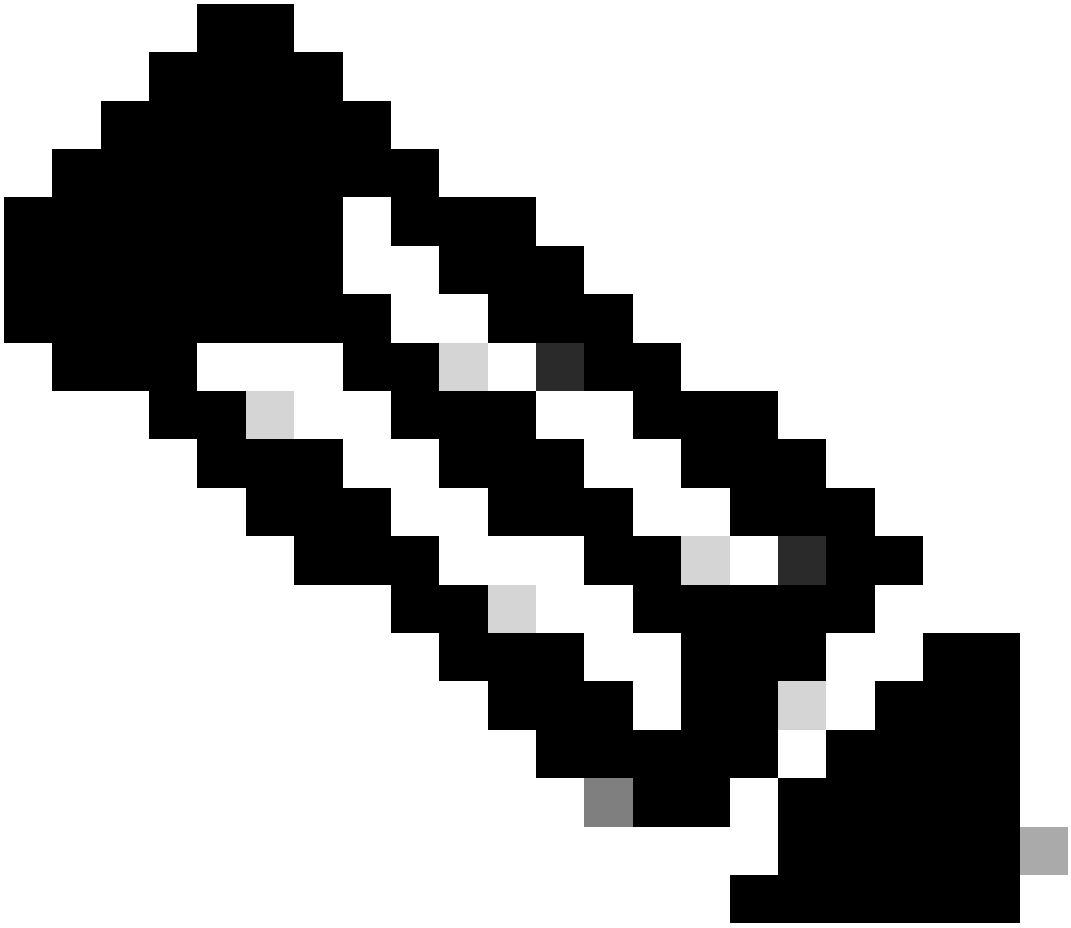
Schritt 8. Geben Sie auf der Seite Einmalige Anmeldung mit SAML einrichten die Werte für diese Felder ein:

antwort: Geben Sie im Feld Identifizierungstext eine URL nach folgendem Muster ein:

https://<VPN-URL>/saml/sp/metadaten/<Tunneling_Group_Name>

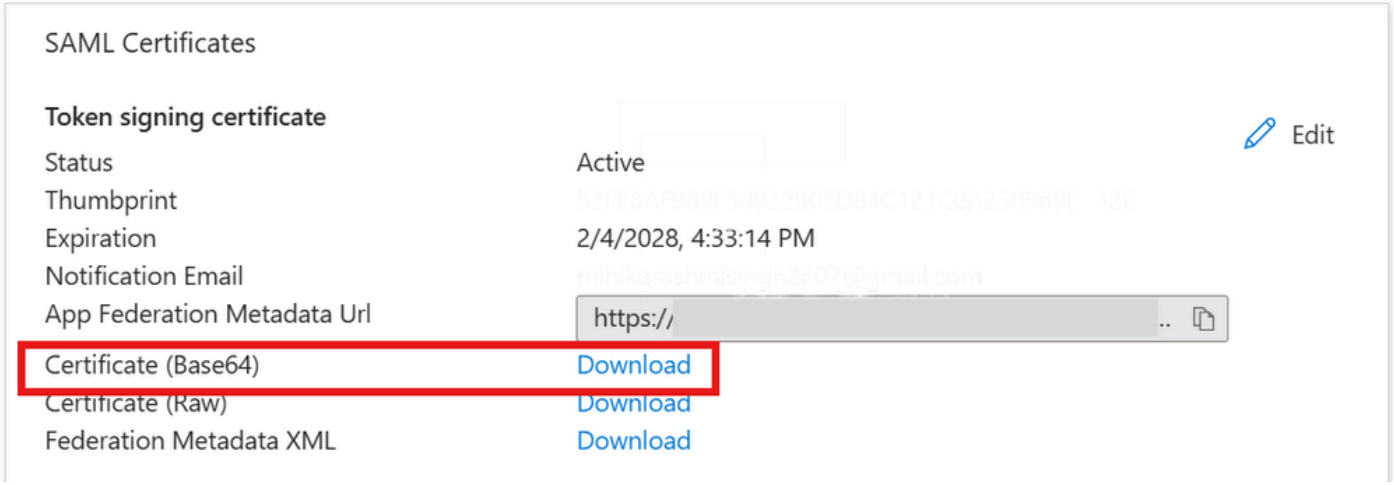
b. Geben Sie im Textfeld Antwort-URL eine URL nach folgendem Muster ein:

https://<VPN-URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>
[Tunnel_Group_Name = SAML1]

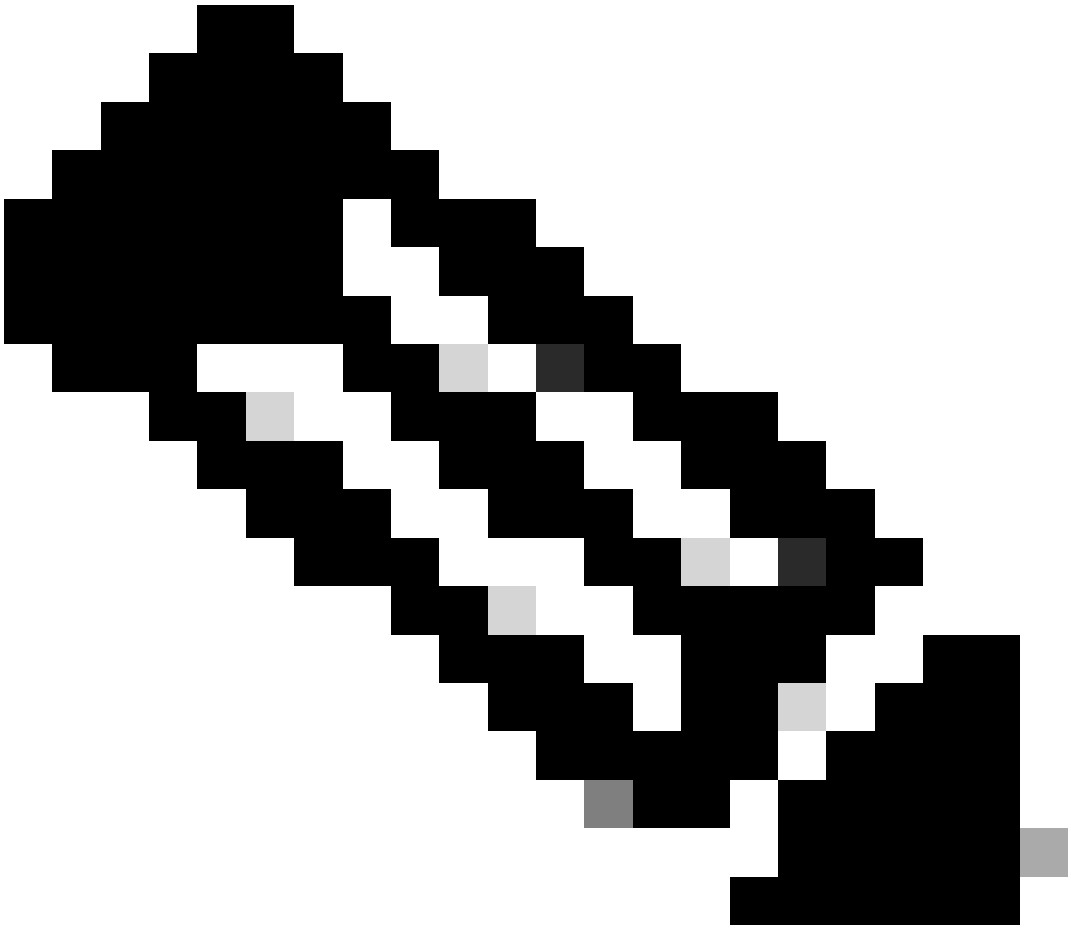


Anmerkung: Bei Tunnel_Group_Name wird die Groß-/Kleinschreibung berücksichtigt, und der Wert darf keine Punkte '' enthalten. und Schrägstrich '/'.

Schritt 9. Suchen Sie auf der Seite Einmalige Anmeldung mit SAML einrichten im Abschnitt SAML-Signaturzertifikat nach Zertifikat (Base64) und wählen Sie Herunterladen, um die Zertifikatsdatei herunterzuladen und auf Ihrem Computer zu speichern.



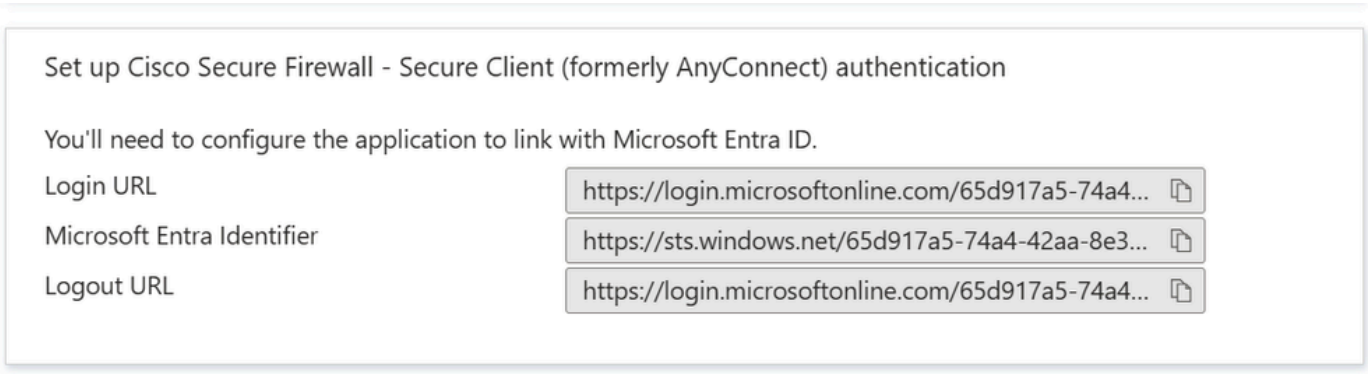
Certificate(Base64)-Download



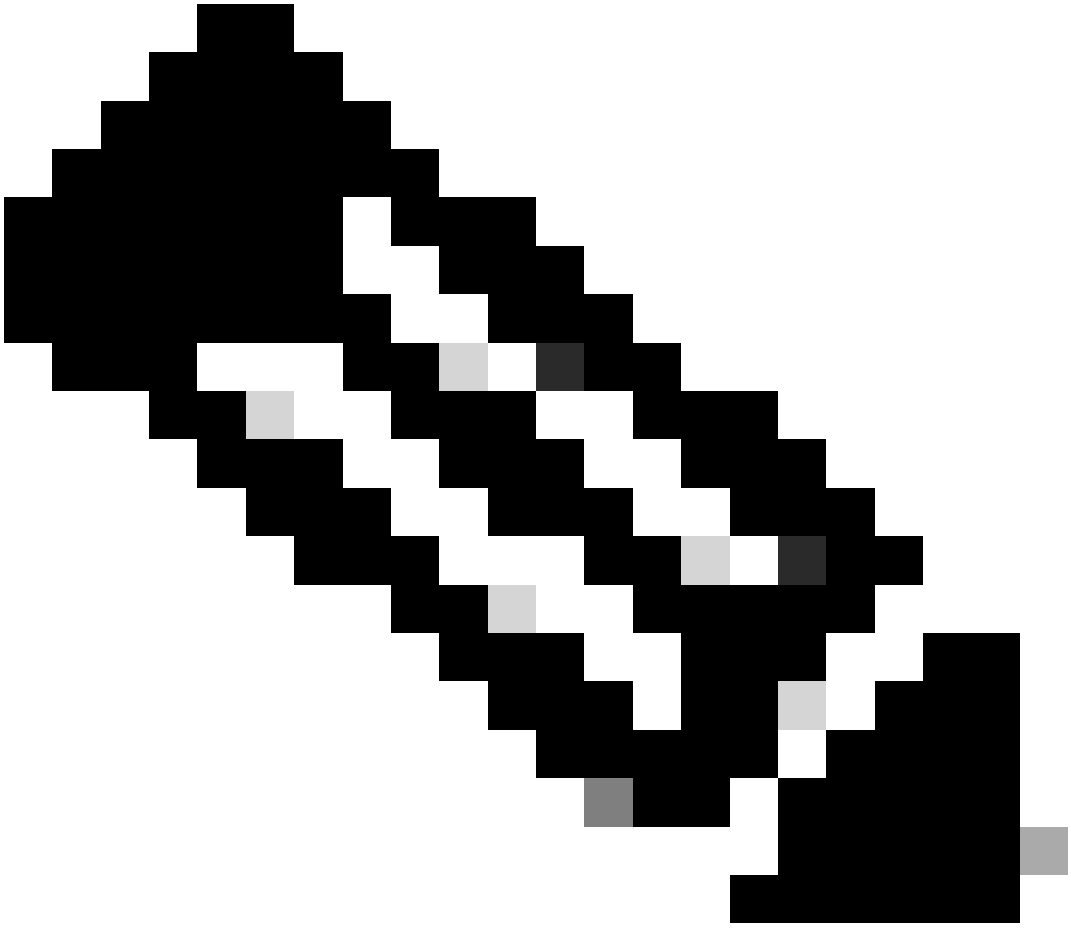
Hinweis: Dieses heruntergeladene Zertifikat wird in den ASA-Vertrauenspunkt AzureAD-AC-SAML1 importiert. Weitere Informationen finden Sie im Abschnitt zur ASA-Konfiguration.

Schritt 10. Kopieren Sie im Abschnitt "Cisco Secure Firewall - Secure Client einrichten" die entsprechenden URL(s), basierend auf Ihren Anforderungen. Diese URL(s) werden zum Konfigurieren des SSO-Serverobjekts auf der ASA verwendet.

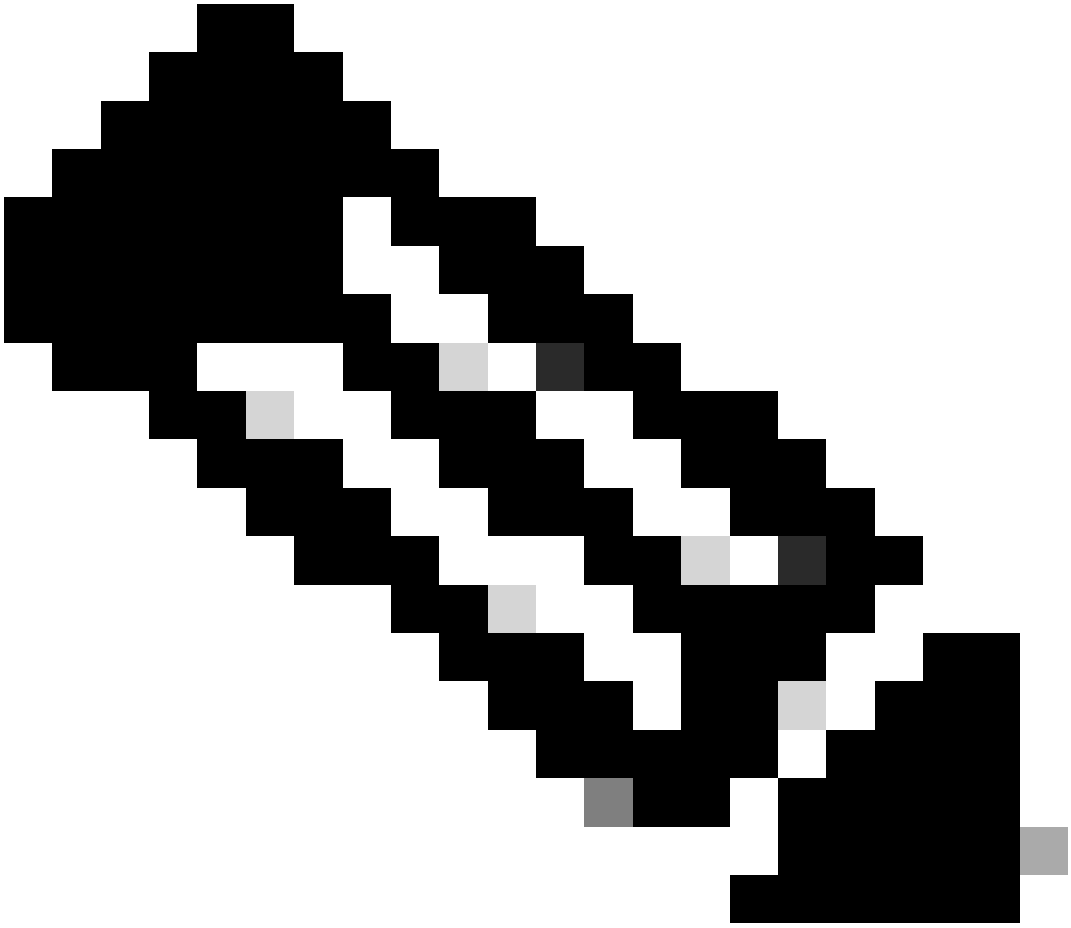
- Microsoft Entra Identifier - Dies ist der SAML-IDP in der VPN-Konfiguration.
- Login URL: Dies ist die URL-Anmeldung.
- Logout URL: Dies ist die URL-Abmeldung.



SSO-URL



Anmerkung: Wiederholen Sie die vorherigen Konfigurationsschritte, um die Cisco Secure Firewall - Secure Client-App aus der Galerie für die zweite Tunnelgruppe hinzuzufügen. Der zweite Tunnelgruppenname ist in diesem Fall SAML2.



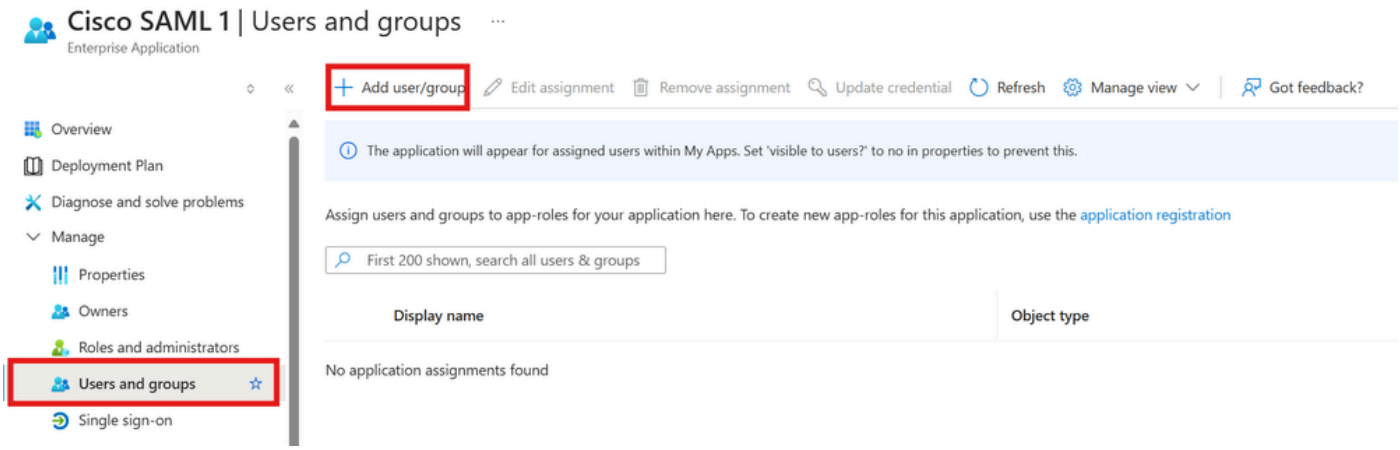
Hinweis: Beim Hinzufügen der Cisco Secure Firewall - Secure Client-App für die zweite Tunnelgruppe (SAML 2) wird das in Schritt 8. heruntergeladene azure-Zertifikat in den ASA-Vertrauenspunkt AzureAD-AC-SAML2 importiert.

Azure AD-Benutzer der App zuweisen

In diesem Abschnitt ist Test1 und Test2 aktiviert, um Azure SSO zu verwenden, wenn Sie Zugriff auf die Cisco Secure Client-App gewähren.

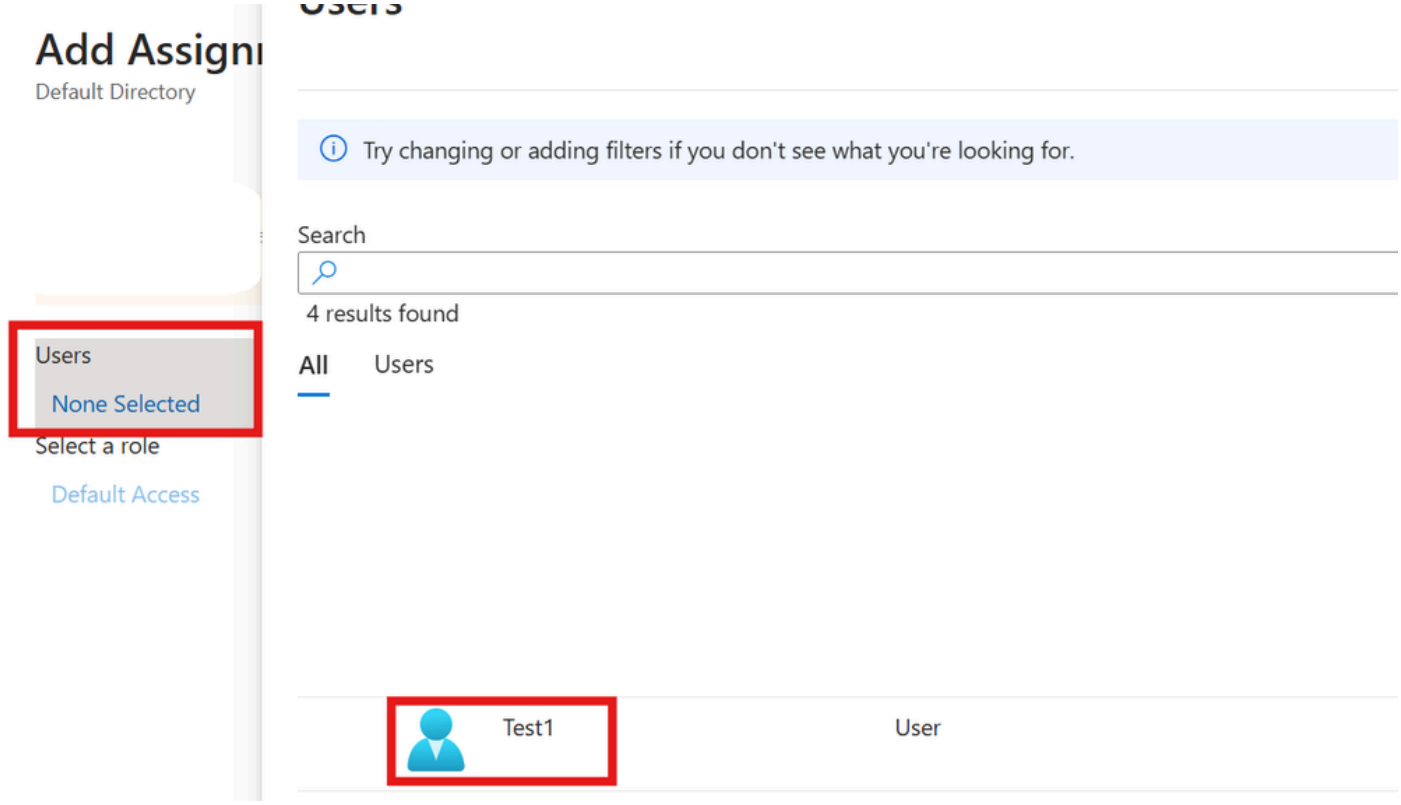
Für die erste IDp-Anwendung:

Schritt 1: Wählen Sie auf der ersten Übersichtsseite der IdP-Anwendung Benutzer und Gruppen und dann Benutzer hinzufügen aus.



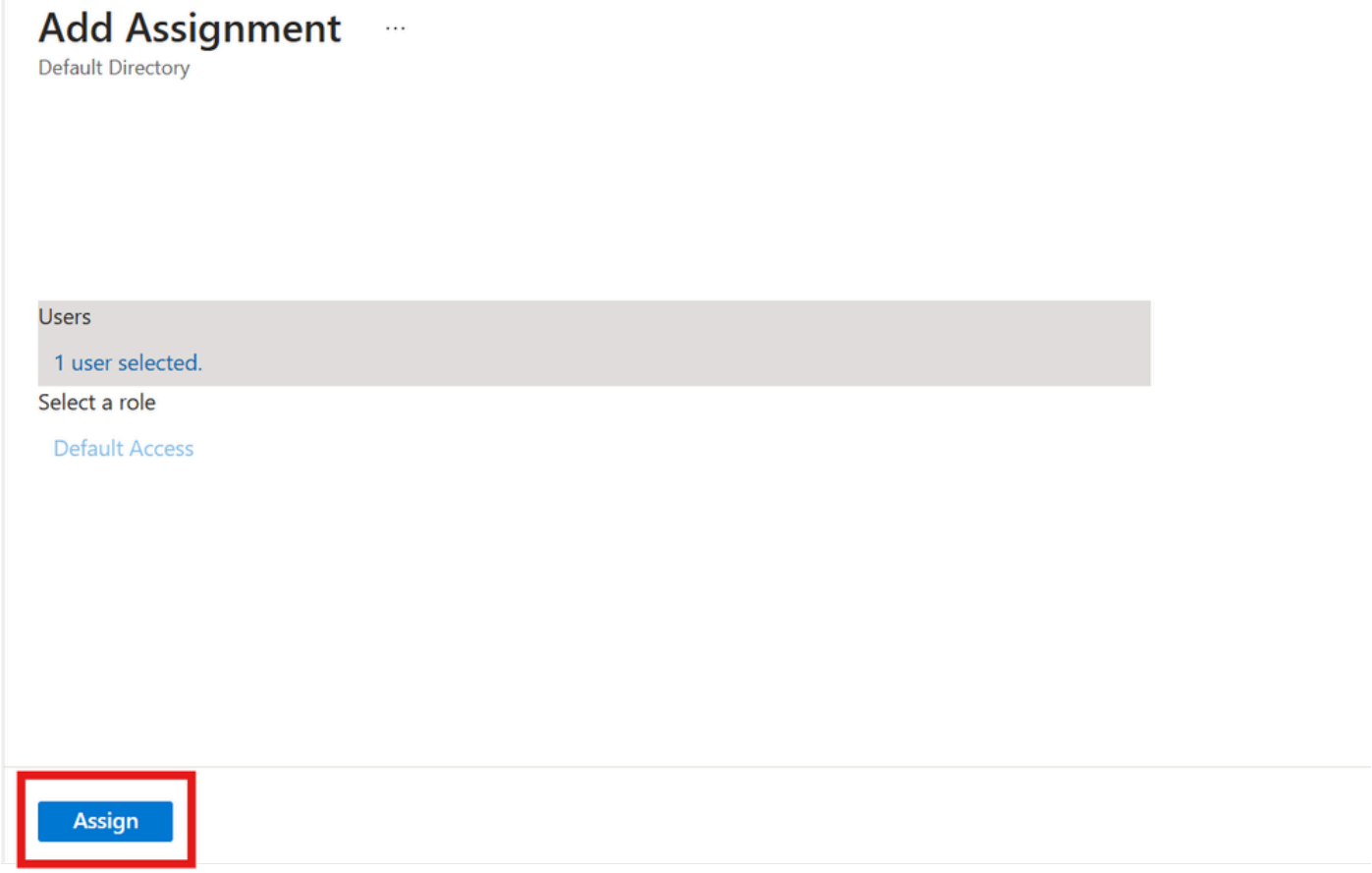
Benutzer und Gruppen

Schritt 2: Wählen Sie im Dialogfeld "Zuweisung hinzufügen" Benutzer oder Gruppen.



Zuweisung 1 hinzufügen

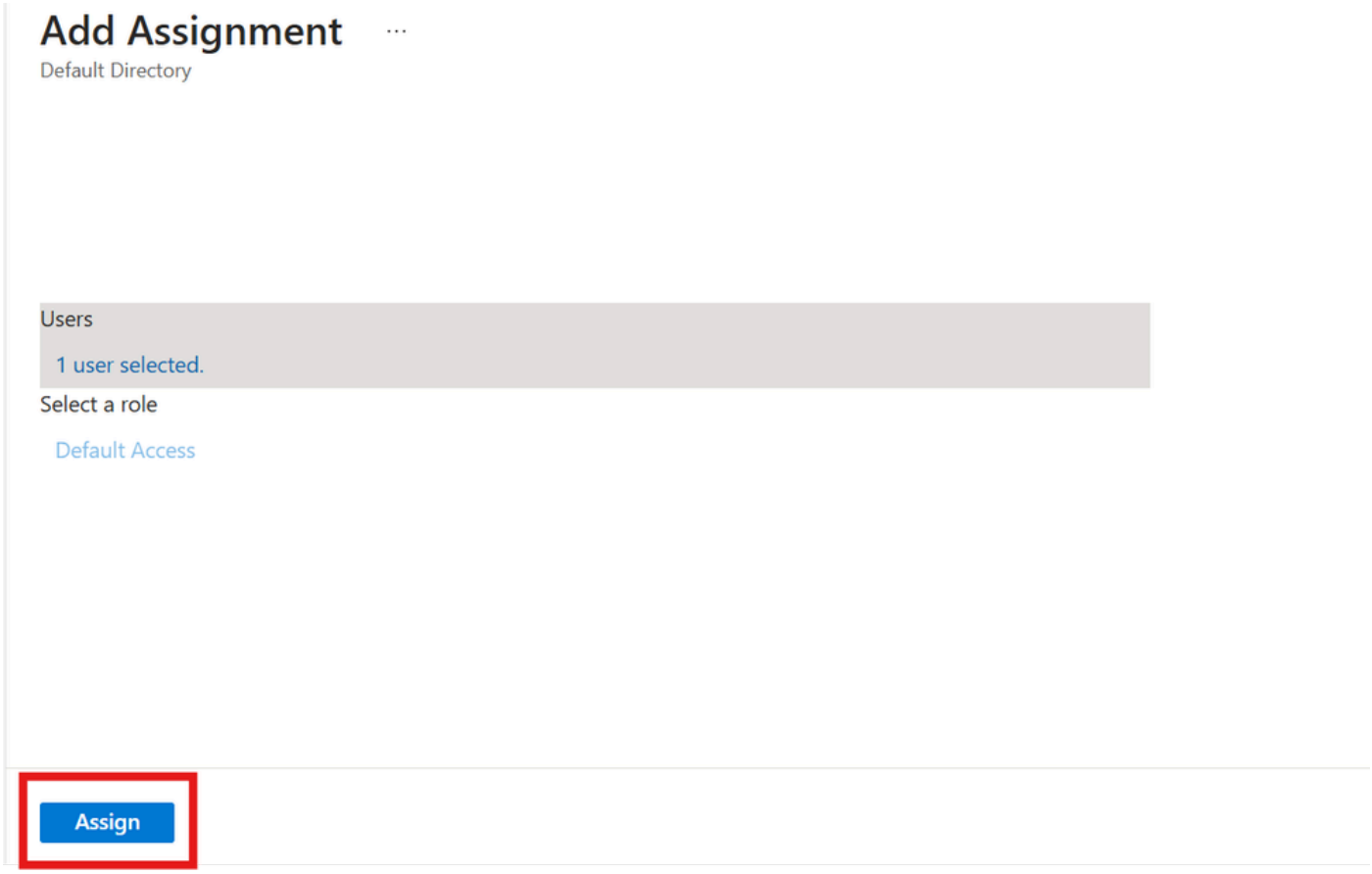
Schritt 3: Klicken Sie im Dialogfeld Zuweisung hinzufügen auf die Schaltfläche Zuweisen.



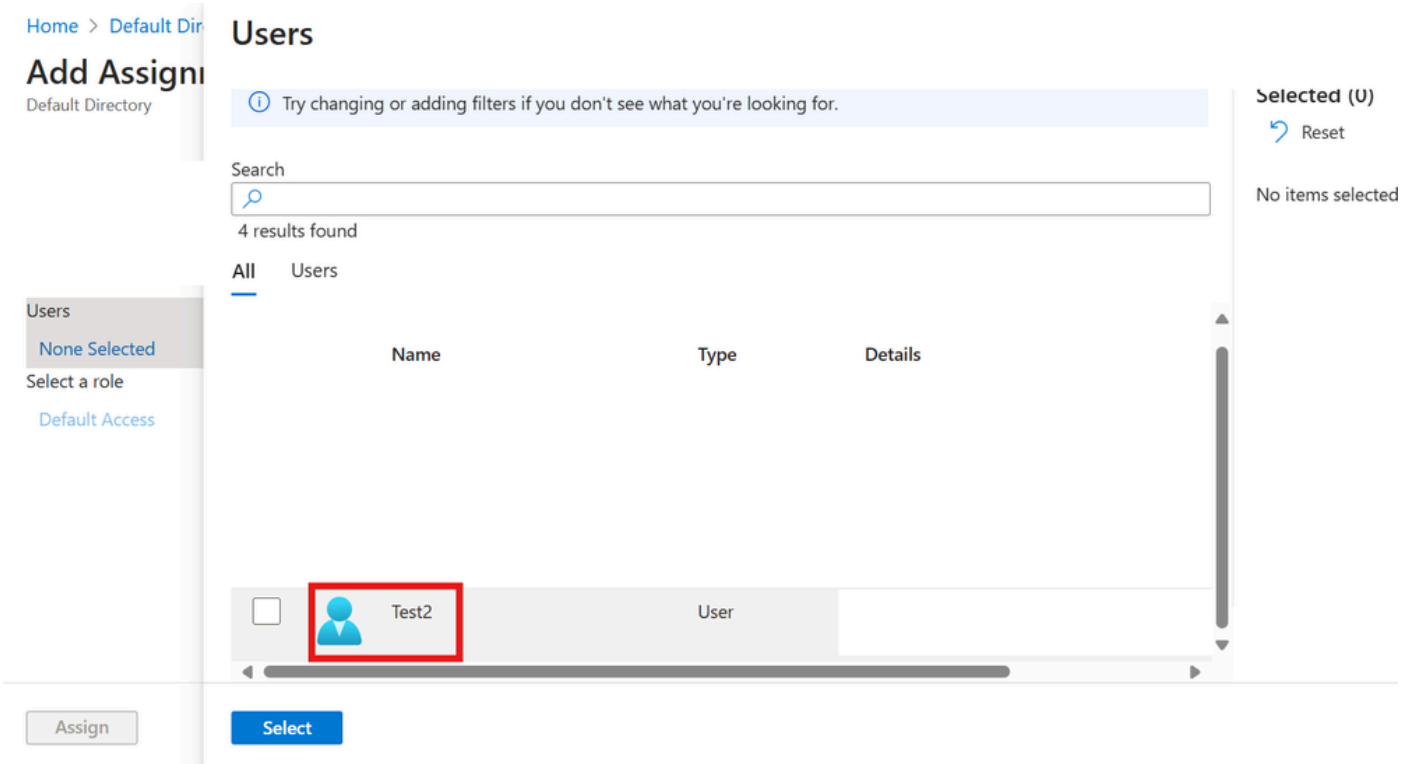
Test1-Benutzerzuweisung

Für die zweite IDp-Anwendung:

Wiederholen Sie die vorherigen Schritte für Second Idp Application, wie in diesen Bildern gezeigt.

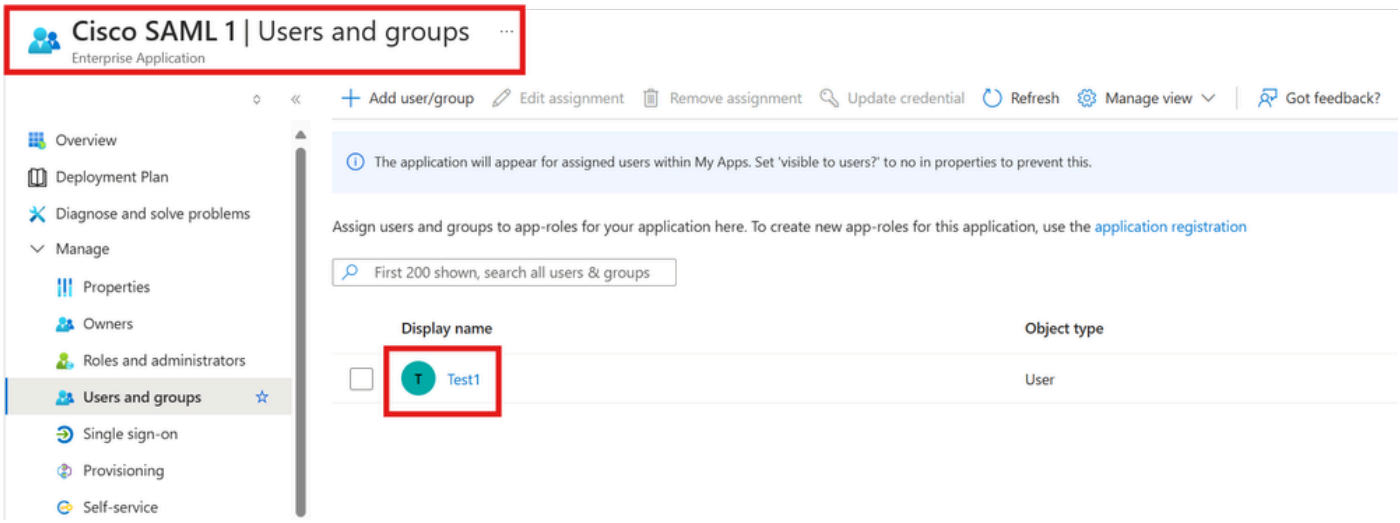


Zuweisung 2 hinzufügen



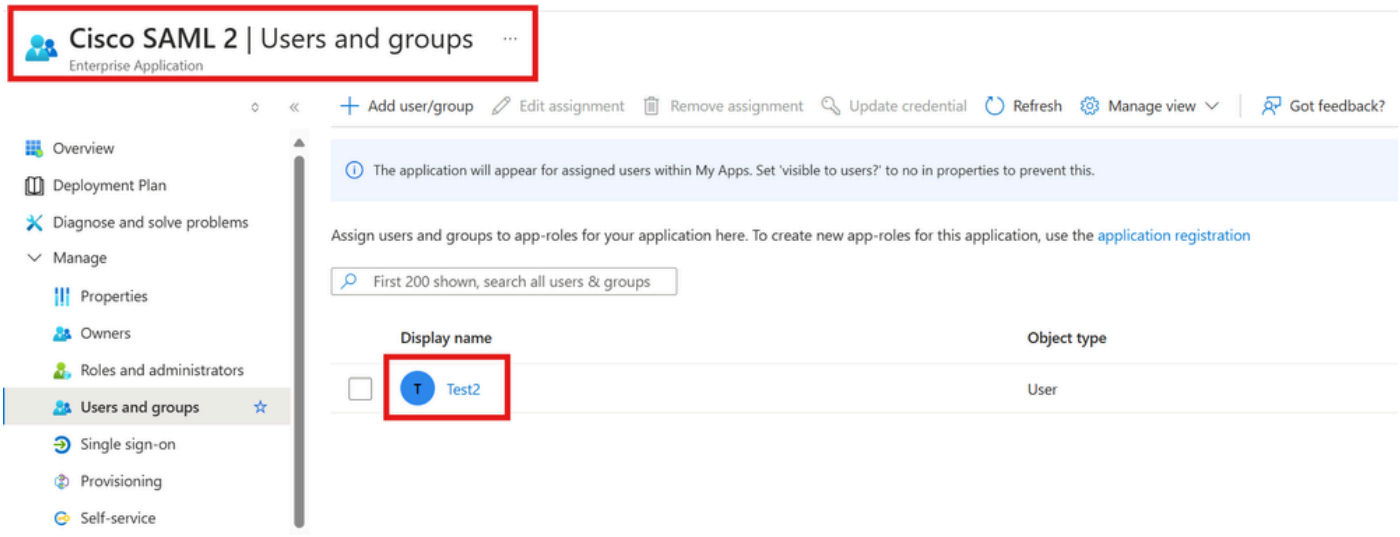
Test2-Benutzerzuweisung

Test1-Benutzerzuweisung:



Test 1: Benutzerzuweisung

Test2-Benutzerzuweisung:



Test 2: Benutzerzuweisung

ASA-Konfiguration über CLI

Schritt 1: Erstellen von Vertrauenspunkten und Importieren von SAML-Zertifikaten.

Konfigurieren Sie zwei Trustpoints, und importieren Sie die entsprechenden SAML-Zertifikate für jede Tunnelgruppe.

<#root>

```
config t

 crypto ca trustpoint
```

AzureAD-AC-SAML1

```
   revocation-check none
   no id-usage
```

```
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML1

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!

crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

Schritt 2: Konfigurieren der SAML-IDp

Verwenden Sie diese Befehle, um die SAML-IdP-Einstellungen bereitzustellen.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

Schritt 3: Anwenden der SAML-Authentifizierung auf die erste VPN-Tunnelgruppe

Konfigurieren Sie die SAML1-Tunnelgruppe mit AzureAD-AC-SAML1 IdP-Vertrauenspunkt.

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (

Schritt 4: Anwenden der SAML-Authentifizierung auf die zweite VPN-Tunnelgruppe

Konfigurieren Sie die SAML2-Tunnelgruppe mit AzureAD-AC-SAML2 IdP-Vertrauenspunkt.

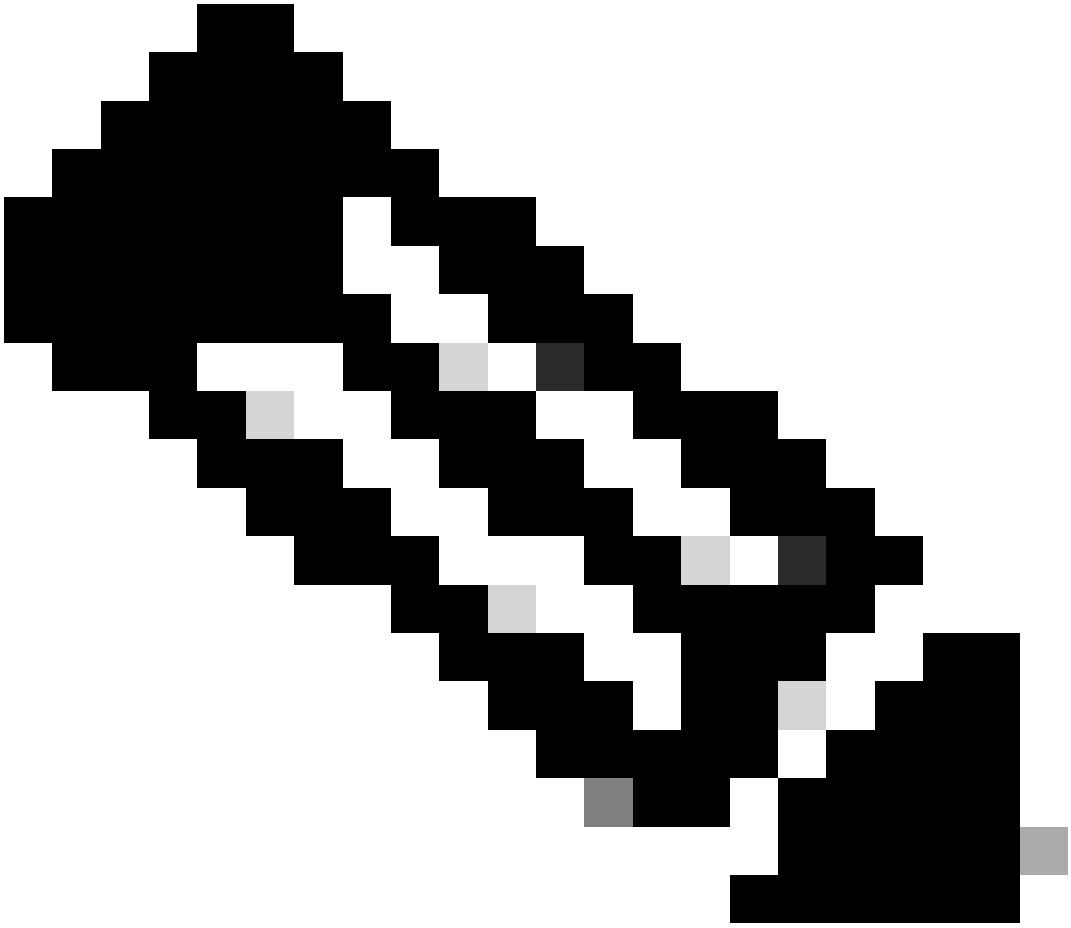
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (

Schritt 5: Speichern Sie die Konfiguration.

```
write memory
```



Anmerkung: Wenn Sie Änderungen an der IdP-Konfiguration vornehmen, müssen Sie die Konfiguration des SAML-Identitätsanbieters aus Ihrer Tunnelgruppe entfernen und erneut anwenden, damit die Änderungen wirksam werden.

Überprüfung

AnyConnect mit SAML-Authentifizierung testen.

Schritt 1: Stellen Sie eine Verbindung zu Ihrer VPN-URL her, und geben Sie die Azure AD-Details für die Anmeldung ein.

Schritt 2: (Optional) Genehmigen des Anmeldeantrags

Schritt 3.AnyConnect ist verbunden.

Fehlerbehebung

Bei den meisten SAML-Fehlerbehebungen handelt es sich um eine Fehlkonfiguration, die beim Überprüfen der SAML-Konfiguration oder beim Ausführen von Debugs festgestellt werden kann. debug webvpn saml 255 kann zur Fehlerbehebung bei den meisten Problemen verwendet werden. In Szenarien, in denen dieses Debuggen keine nützlichen Informationen liefert, können jedoch zusätzliche Debugs ausgeführt werden:

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

Zugehörige Informationen

- Konfigurieren von ASA AnyConnect-VPN mit Microsoft Azure MFA über SAML
- Technischer Support und Dokumentation für Cisco Systeme

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.