Konfigurieren der Gruppenrichtlinienzuweisung für SAML mithilfe der sicheren Firewall und der Microsoft Entra-ID

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Gruppenrichtlinien mithilfe der Microsoft Entra-ID für die SAML-Authentifizierung von Cisco Secure Client auf der Cisco Secure Firewall zugewiesen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Cisco Secure Client AnyConnect-VPN
- Konfiguration von Cisco Firepower Threat Defense (FTD)- oder Cisco Secure Firewall ASA-Remotezugriffs-VPN- und Single Sign-on (SSO)-Serverobjekten
- Konfiguration des Microsoft Entra ID Identity Provider (IdP)

Verwendete Komponenten

Die Informationen in diesem Leitfaden basieren auf den folgenden Hardware- und Softwareversionen:

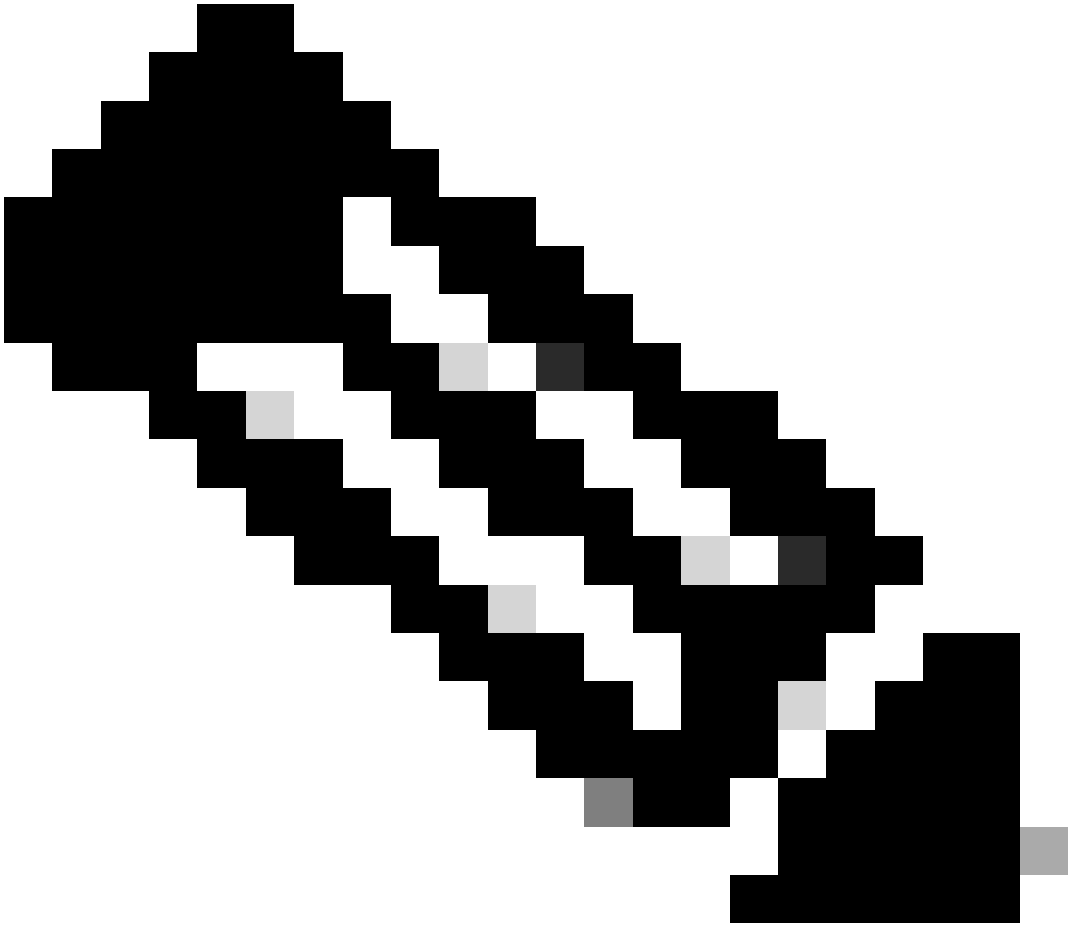
- FTD Version 7.6
- FMC Version 7.6
- MS Entra ID SAML-IDp

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 XML-basiertes Framework für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. Es wird ein Vertrauenskreis zwischen dem Benutzer, einem Dienstanbieter (SP) und einem Identitätsanbieter (IdP) erstellt, der es dem Benutzer ermöglicht, sich für mehrere Dienste einmal anzumelden. SAML kann für die Remote Access VPN-Authentifizierung für Cisco Secure Client-Verbindungen zu ASA- und FTD VPN-Headends verwendet werden, wobei ASA oder FTD der SP-Teil des Vertrauenskreises ist.

In diesem Dokument wird Microsoft Entra ID/Azure als IdP verwendet. Es ist jedoch auch möglich, Gruppenrichtlinien mit anderen IdPs zuzuweisen, da diese auf Standardattributen basieren, die in der SAML Assertion gesendet werden können.

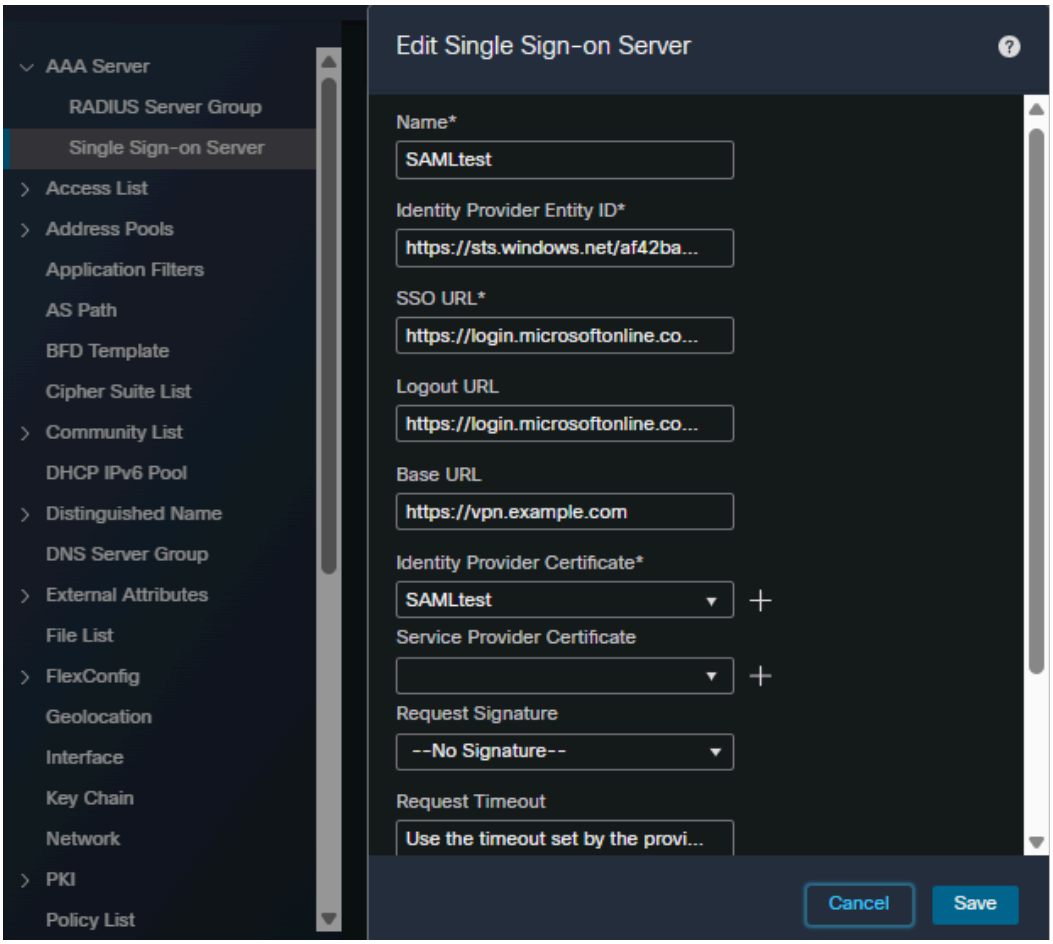


Anmerkung: Beachten Sie, dass jeder Benutzer nur zu einer Benutzergruppe mit MS Entra ID gehören darf, da mehrere SAML-Attribute, die an die ASA oder FTD gesendet werden, Probleme mit der Gruppenrichtlinienzuweisung verursachen können, wie in Cisco Bug-ID CSCwm33613 beschrieben.

Konfigurieren

FMC SAML-Konfiguration

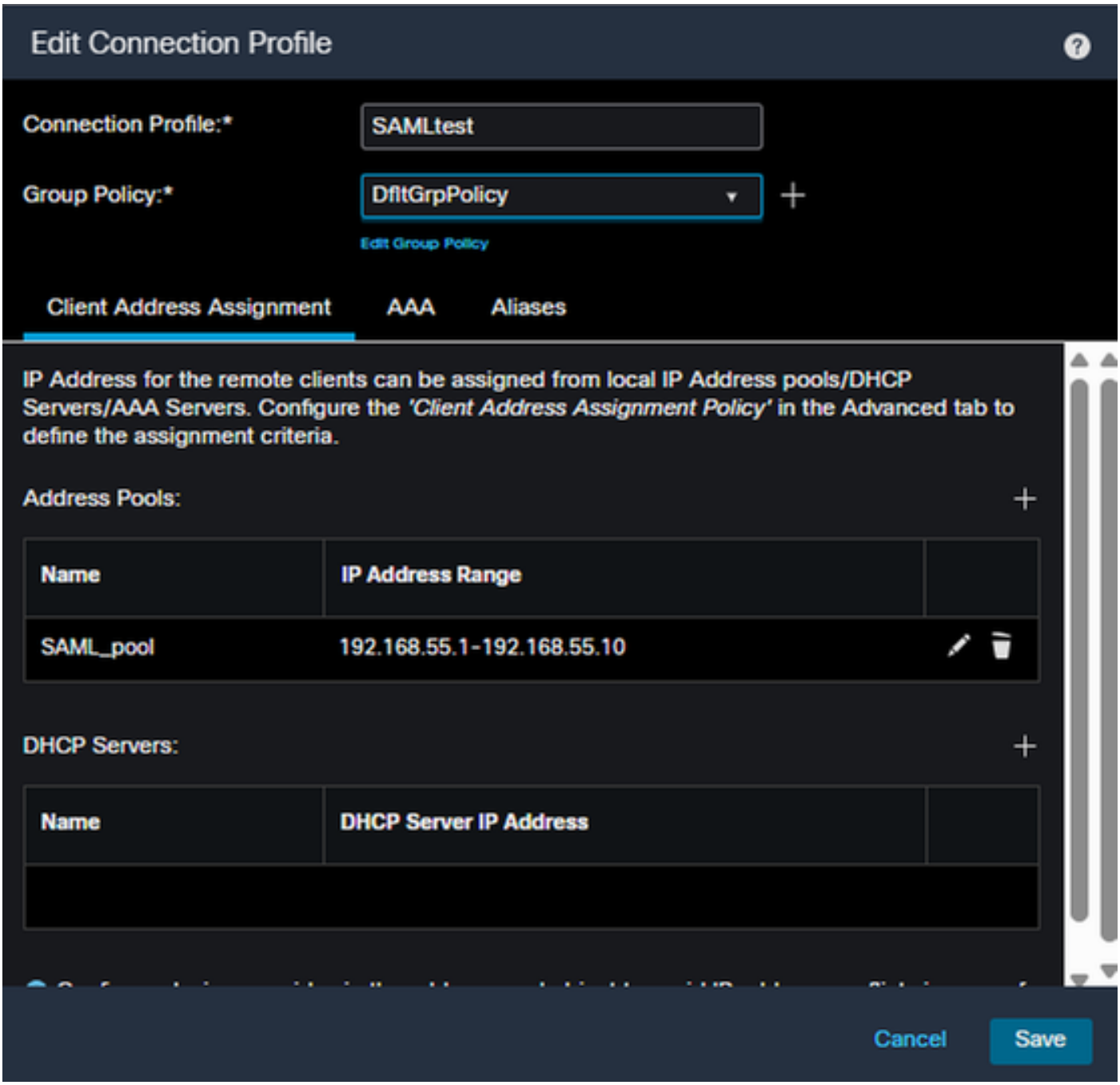
Navigieren Sie auf dem FMC zu Objects > Object Management > AAA Server > Single Sign-on Server. Die Entitäts-ID, die SSO-URL, die Abmelde-URL und das Identitätsanbieter-Zertifikat werden von der IdP abgerufen, siehe Schritt 6 im Abschnitt Microsoft Entra ID. Die Basis-URL und das Service Provider-Zertifikat sind spezifisch für den FTD, zu dem die Konfiguration hinzugefügt wird.



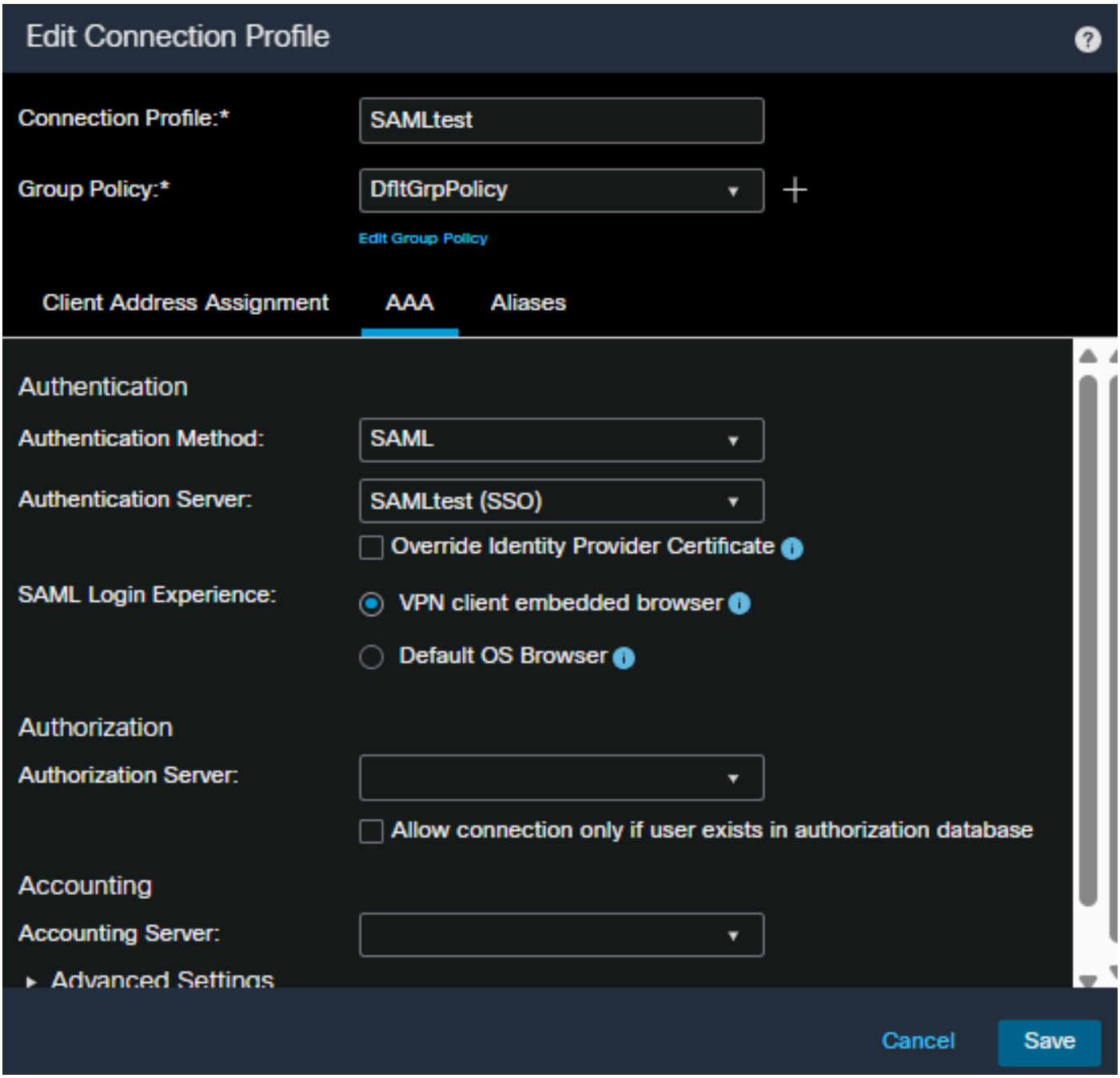
Konfiguration des FMC SSO-Objekts

Konfiguration der FMC RAVPN-Tunnelgruppe

Navigieren Sie auf dem FMC zu Devices (Geräte) > VPN (VPN) > Remote Access (Remote-Zugriff) > Connection Profile (Verbindungsprofil), und wählen Sie die VPN-Richtlinie für das von Ihnen konfigurierte FTD aus, oder erstellen Sie diese. Nach der Auswahl erstellen Sie ein Verbindungsprofil wie dieses:



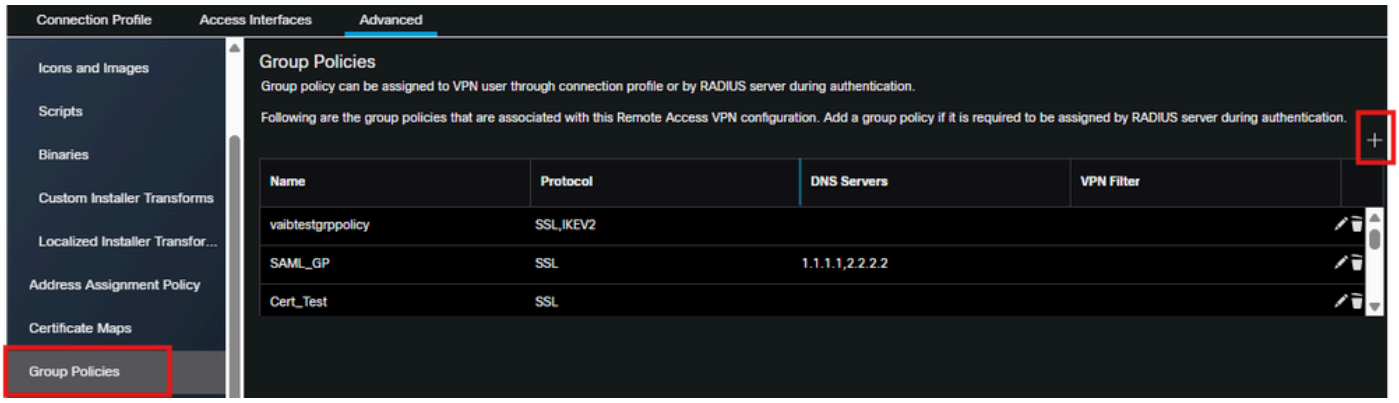
Adressenzuweisung für FMC-Verbindungsprofil



AAA-Konfiguration des FMC-Verbindungsprofils

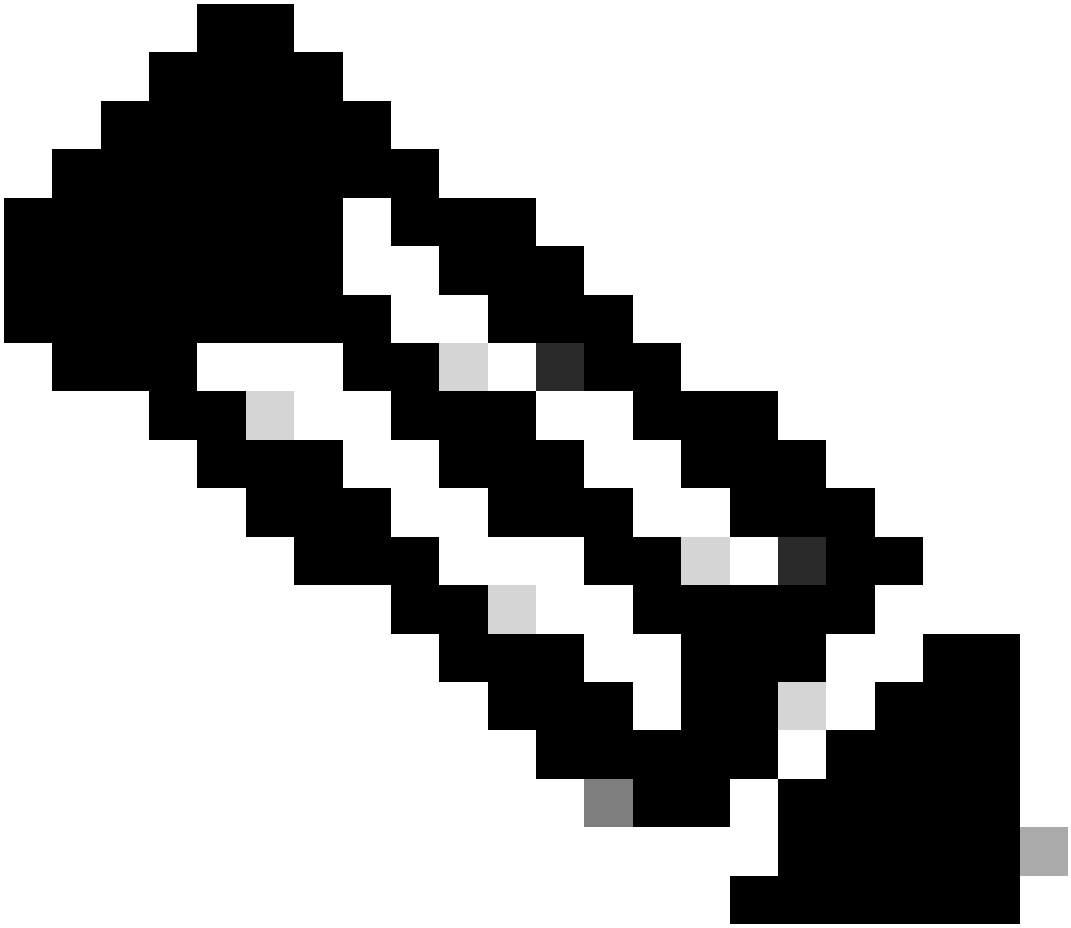
Konfiguration der FMC RAVPN-Gruppenrichtlinie

1. Sie müssen eine Gruppenrichtlinie mit den erforderlichen Optionen für jede Benutzergruppe für die Entra-ID erstellen und der RAVPN-Richtlinie für das zu konfigurierende FTD hinzufügen. Navigieren Sie dazu zu Devices > VPN > Remote Access > Advanced (Geräte > VPN > Remote-Zugriff > Erweitert), und wählen Sie Group Policies (Gruppenrichtlinien) auf der linken Seite aus. Klicken Sie dann auf das + (oben rechts), um eine Gruppenrichtlinie hinzuzufügen.

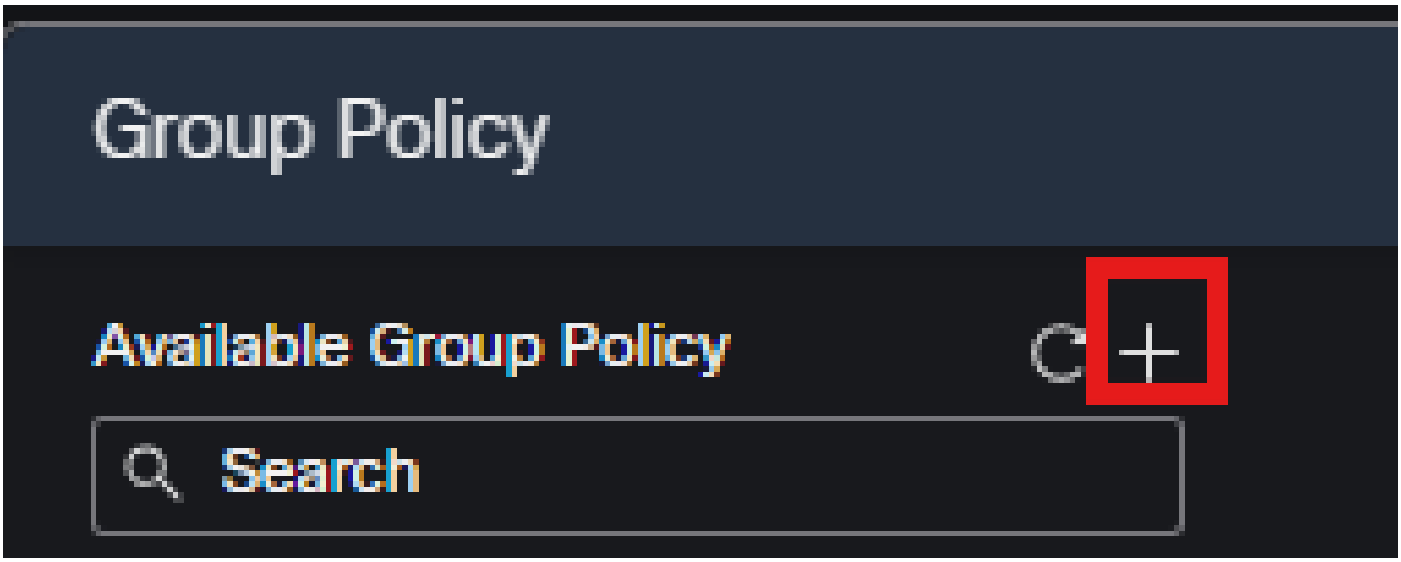


FMC-Richtlinie zum Hinzufügen von Gruppen

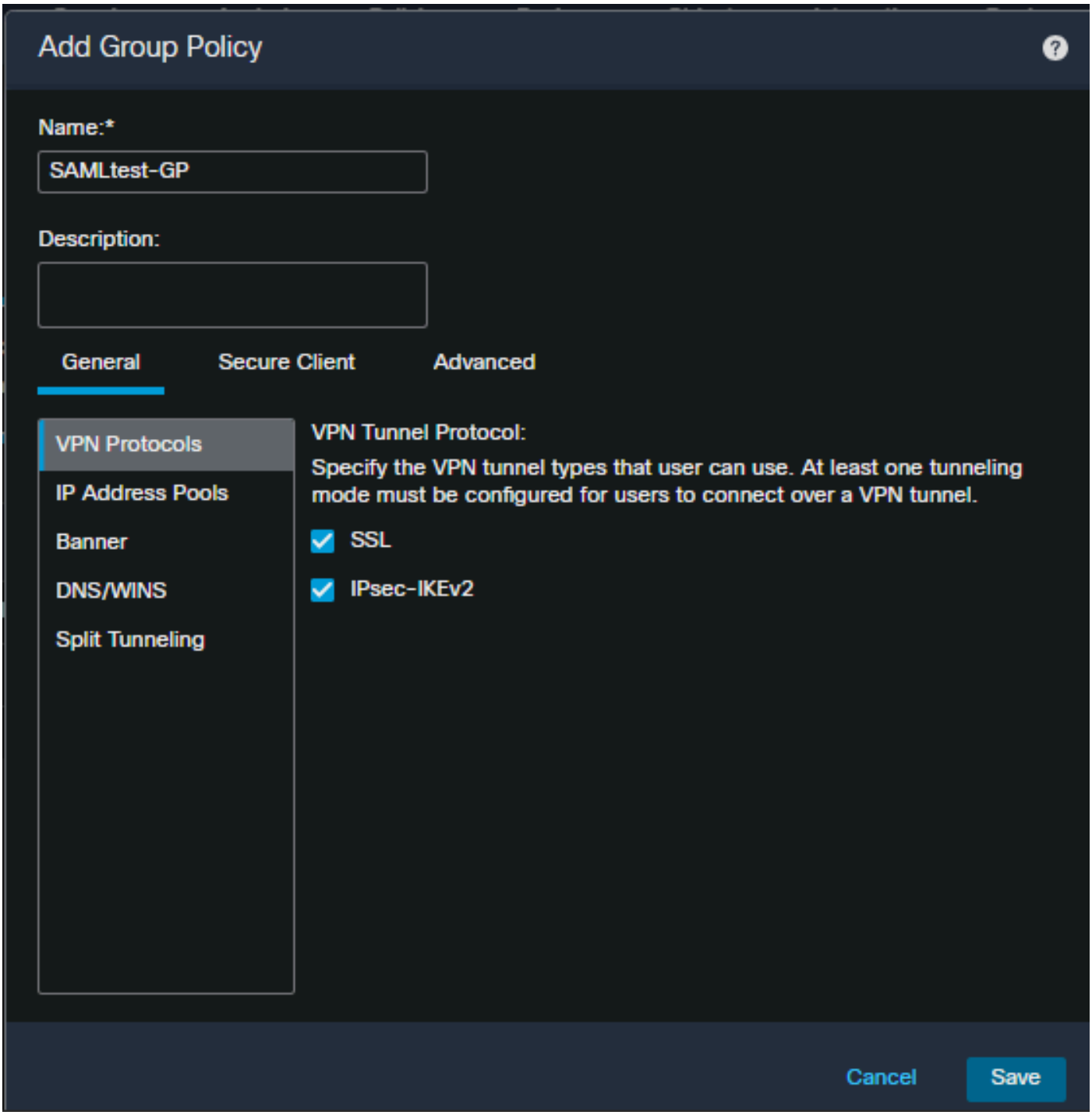
2. Klicken Sie im Popup-Fenster auf das +, um den Dialog zum Erstellen einer neuen Gruppenrichtlinie zu öffnen. Geben Sie die erforderlichen Optionen ein, und speichern Sie.



Anmerkung: Wenn Sie die erforderliche Gruppenrichtlinie bereits erstellt haben, können Sie diesen Schritt überspringen und mit Schritt 3 fortfahren.

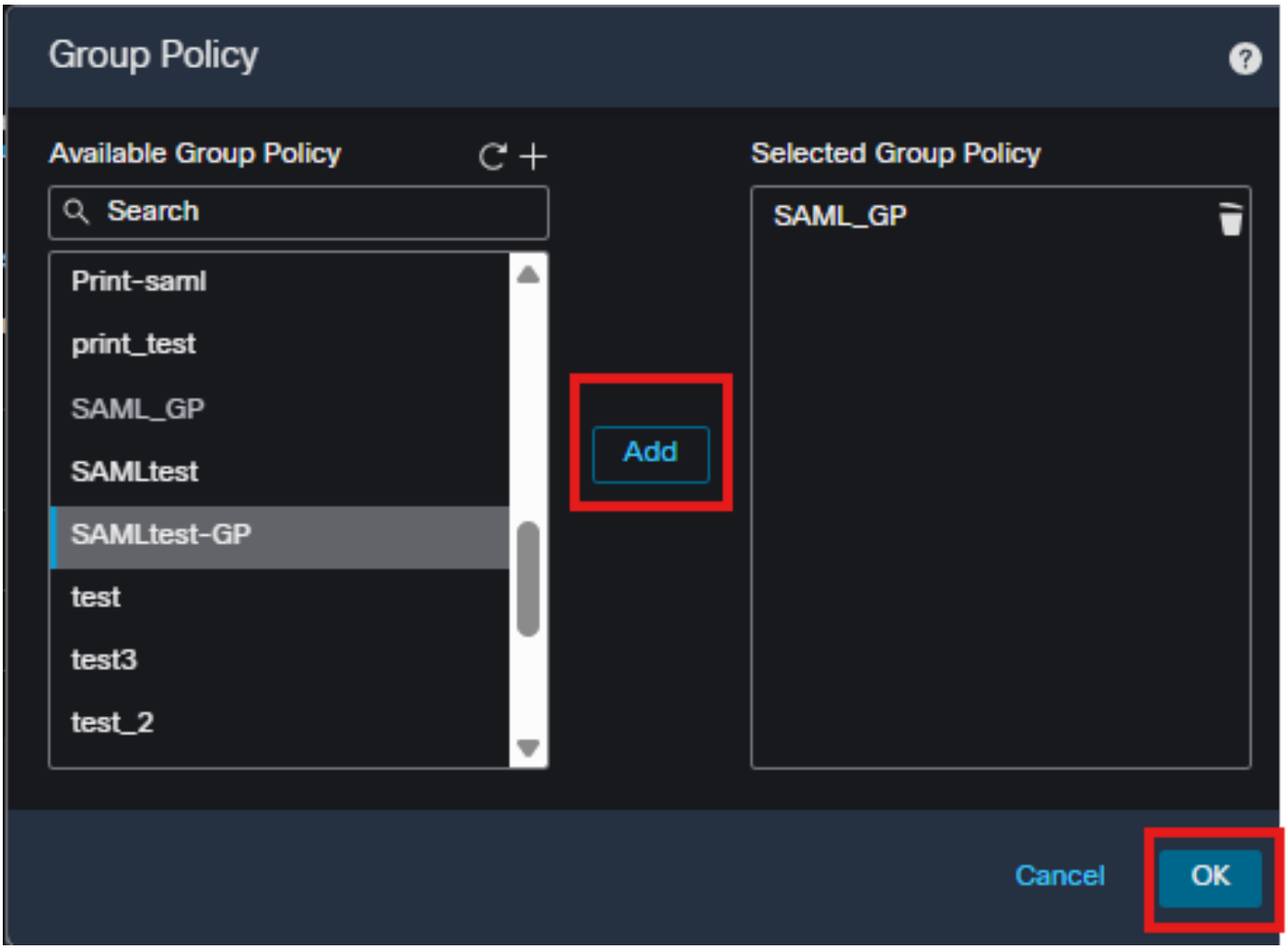


Neue Gruppenrichtlinie erstellen



Gruppenrichtlinienoptionen

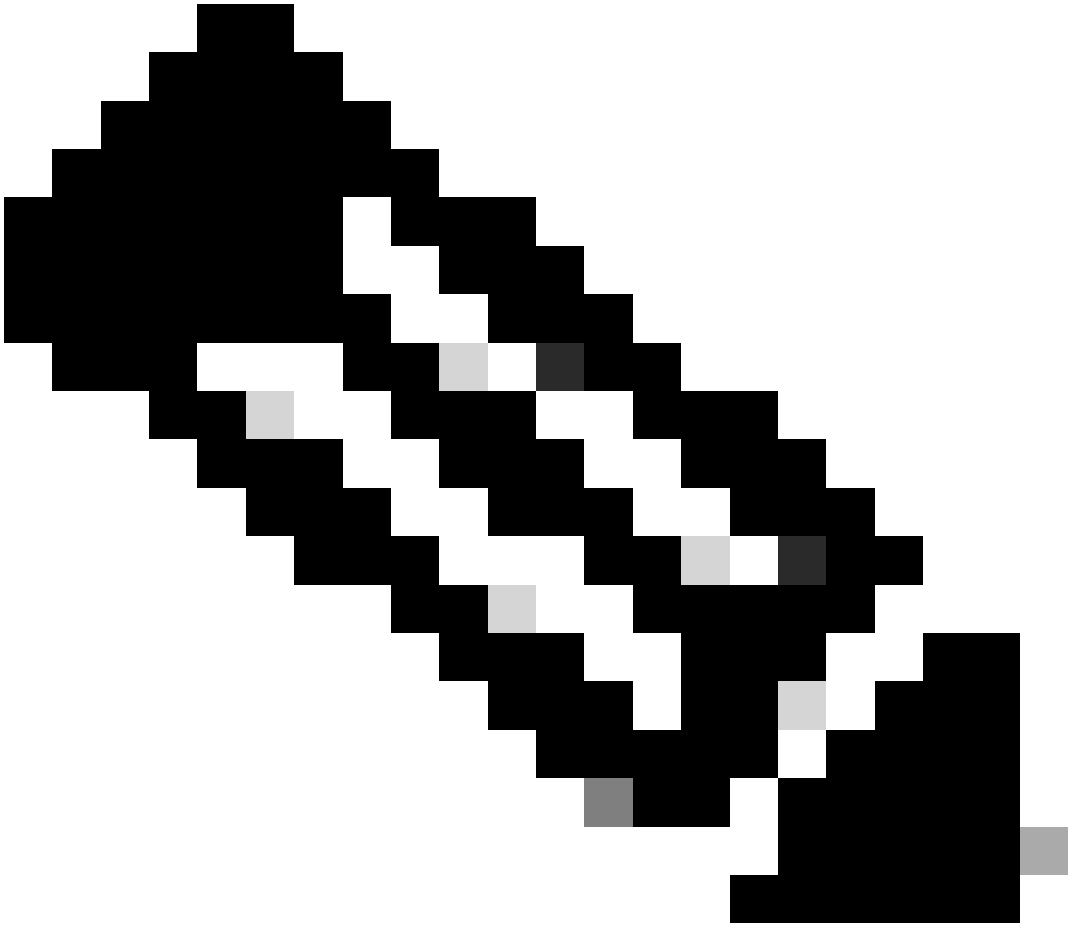
3. Wählen Sie die neu erstellte Gruppenrichtlinie in der Liste links aus, und klicken Sie auf die Schaltfläche Hinzufügen. Klicken Sie dann auf OK, um die Liste zu speichern.



Gruppenrichtlinie hinzufügen

FTD-Metadaten

Sobald die Konfiguration im FTD bereitgestellt wurde, navigieren Sie zur FTD-CLI, und führen Sie den Befehl "show small metadates <Tunnelgruppenname>" aus, und erfassen Sie die FTD-Objektkennung und die ACS-URL.



Anmerkung: Das Zertifikat in den Metadaten wurde aus Gründen der Kürze gekürzt.

<#root>

```
FTD# show saml metadata SAMLtest
SP Metadata
-----------
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="
```

https://vpn.example.net/saml/sp/metadata/SAMLtest

```
" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="ur
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFWzCCBEOgAwIBAgITRwAAAAgZ9Nmfv5mpJQAAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV0lOQVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTBlJUUFZQTjEdMBsGA1UEAxMUcnRwdnBu
```

LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

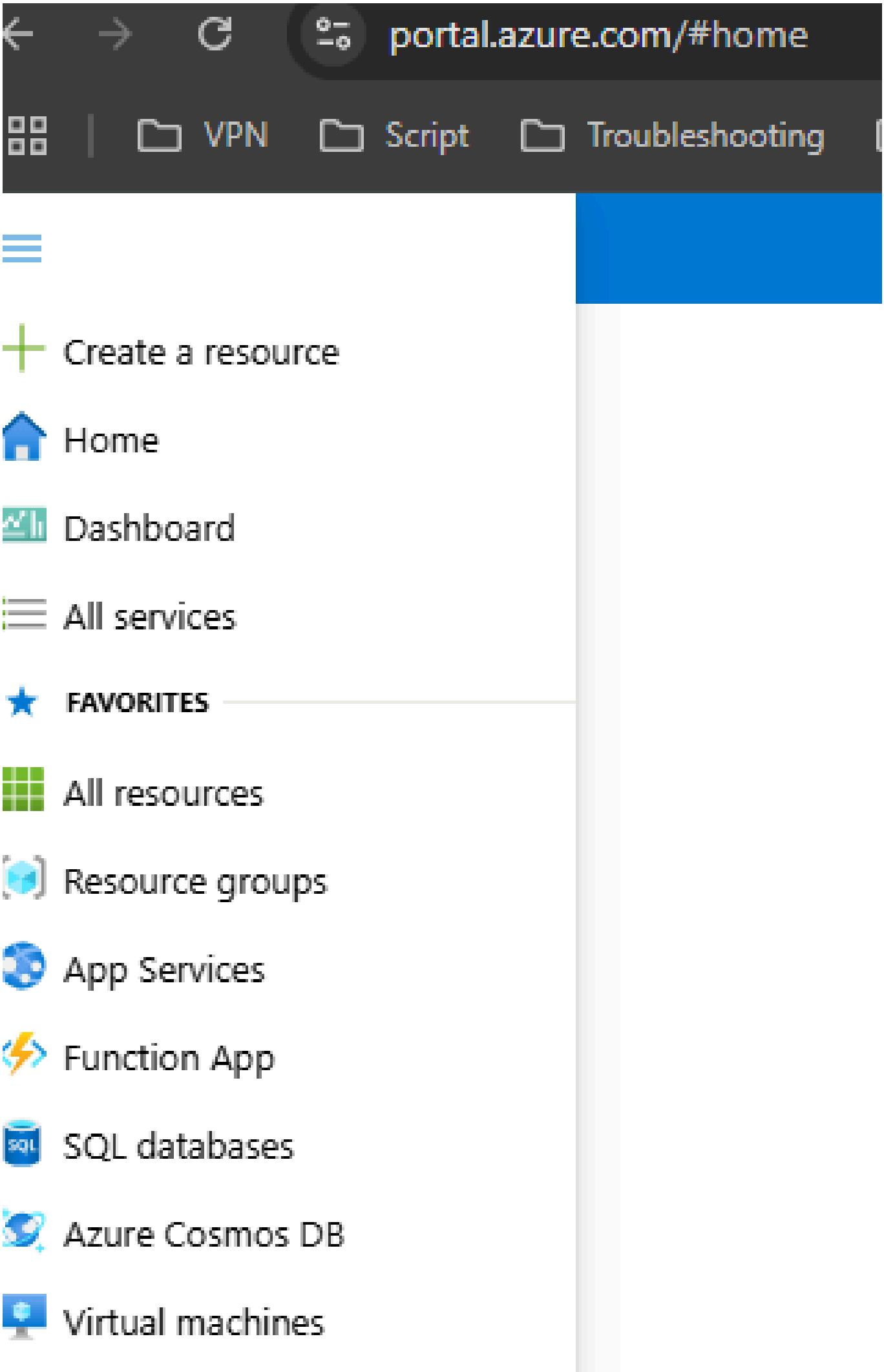
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

https://vpn.example.net/+CSCOE+/saml/sp/acs?tgname=SAMLtest

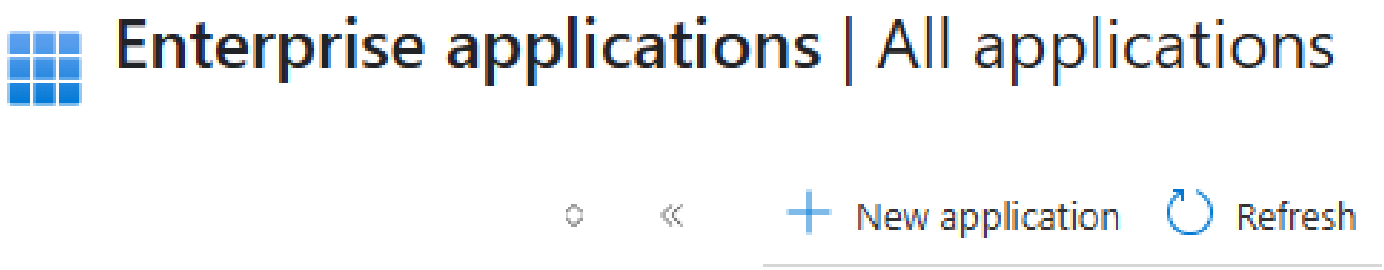
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>

Microsoft Entra-ID

1. Wählen Sie im Microsoft Azure-Portal im Menü links Microsoft Entra ID aus.

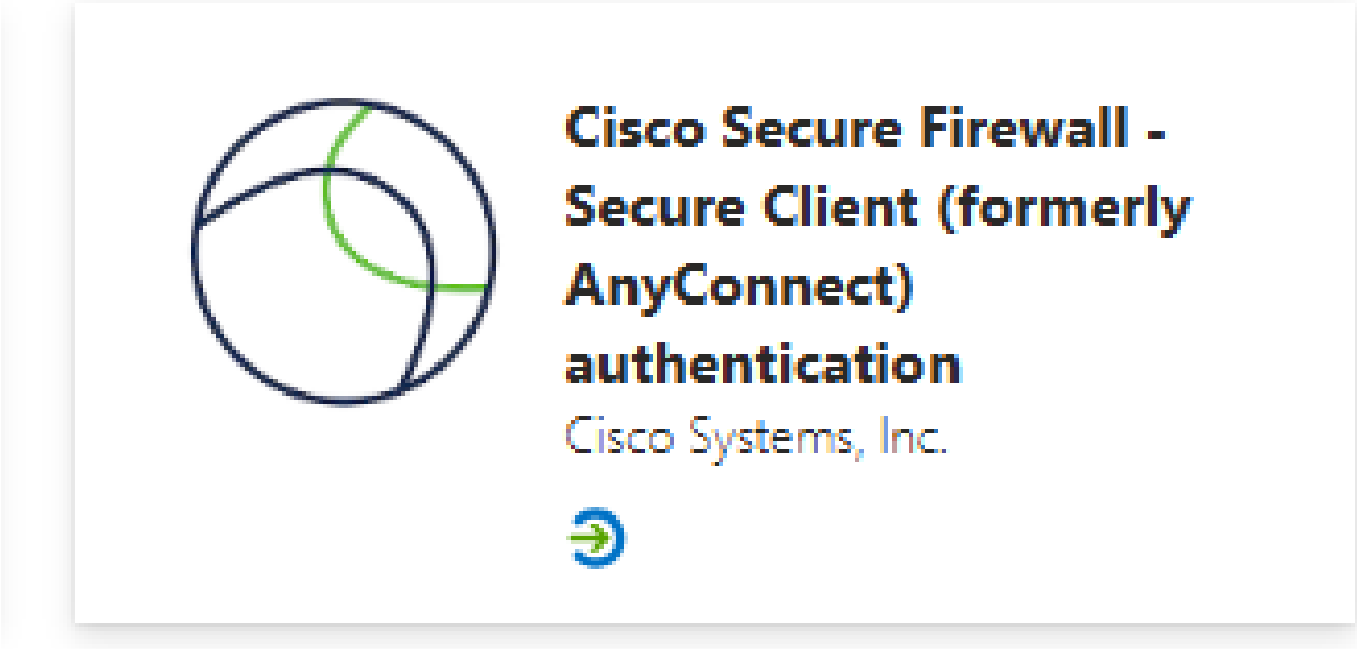

portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

Wenn bereits eine Enterprise-Anwendung für die FTD RAVPN-Konfiguration konfiguriert ist, überspringen Sie die nächsten Schritte, und fahren Sie mit Schritt 7 fort.



MS Entra ID Enterprise-Anwendung

4. Wählen Sie Cisco Secure Firewall - Secure Client (ehemals AnyConnect) Authentication unter Featured Applications aus. Geben Sie der Anwendung einen Namen, und wählen Sie Erstellen aus.



MS Entra ID Cisco Secure Firewall Secure Client (ehemals AnyConnect)-Authentifizierungsanwendung

5. Wählen Sie in der Anwendung Benutzer und Gruppen aus, und weisen Sie der Anwendung die erforderlichen Benutzer- oder Gruppennamen zu.

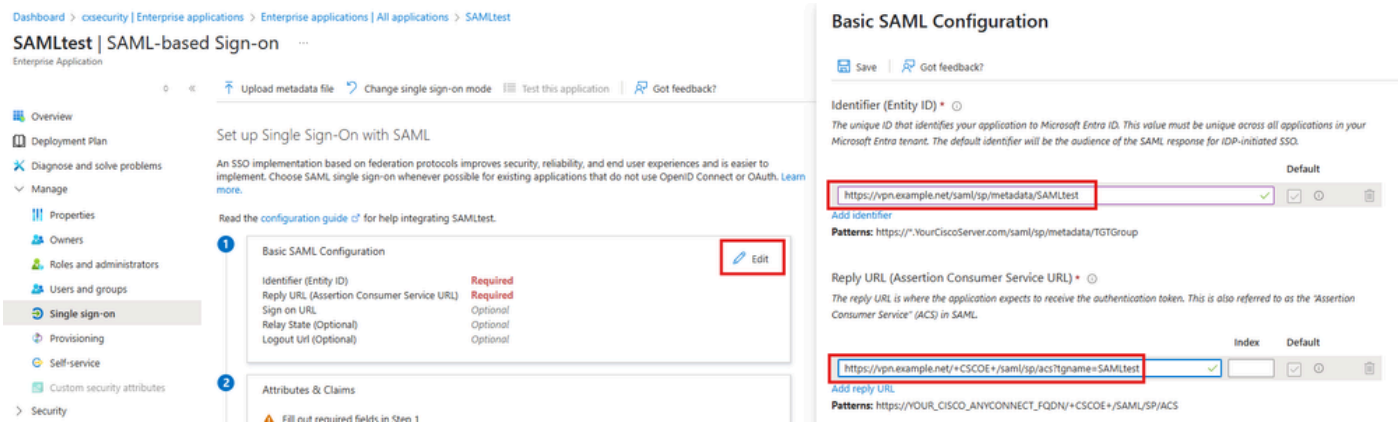
Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

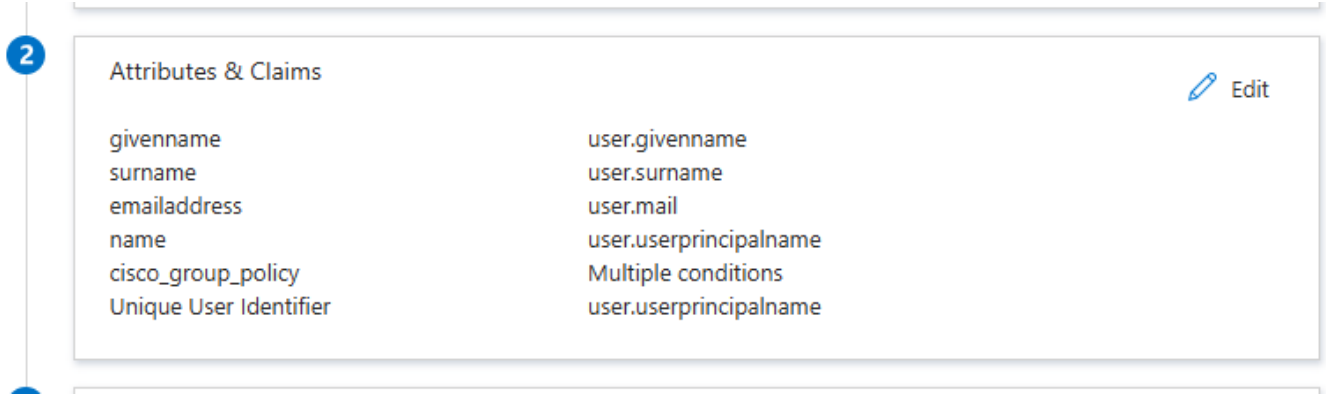
- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators

mit der aus den FTD-Metadaten abgerufenen ID (Entity ID) und Antwort (ACS)-URL, und speichern Sie sie.



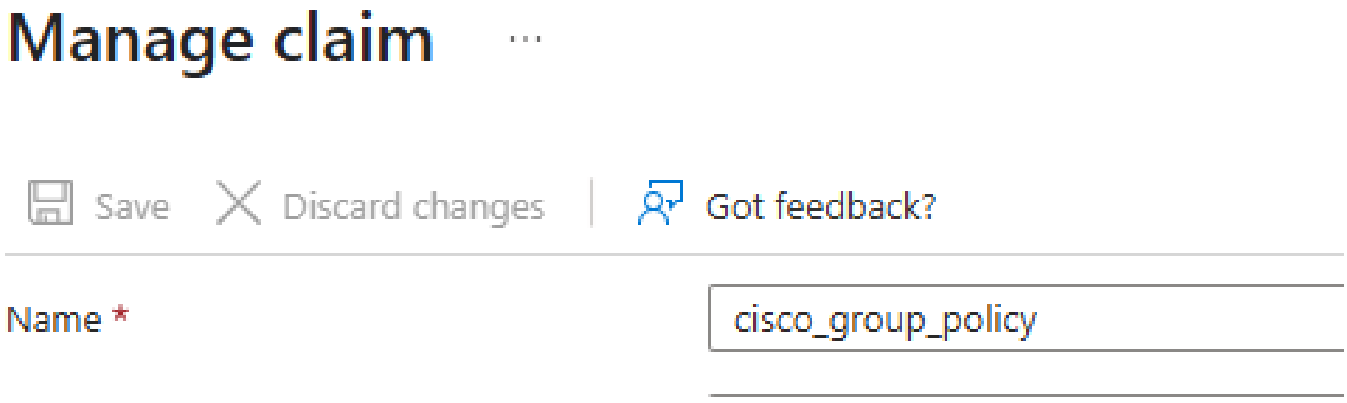
Grundlegende SAML-Konfiguration

8. Wählen Sie Bearbeiten für Attribute und Ansprüche aus, und klicken Sie auf Neuen Anspruch hinzufügen.



Attribute und Ansprüche

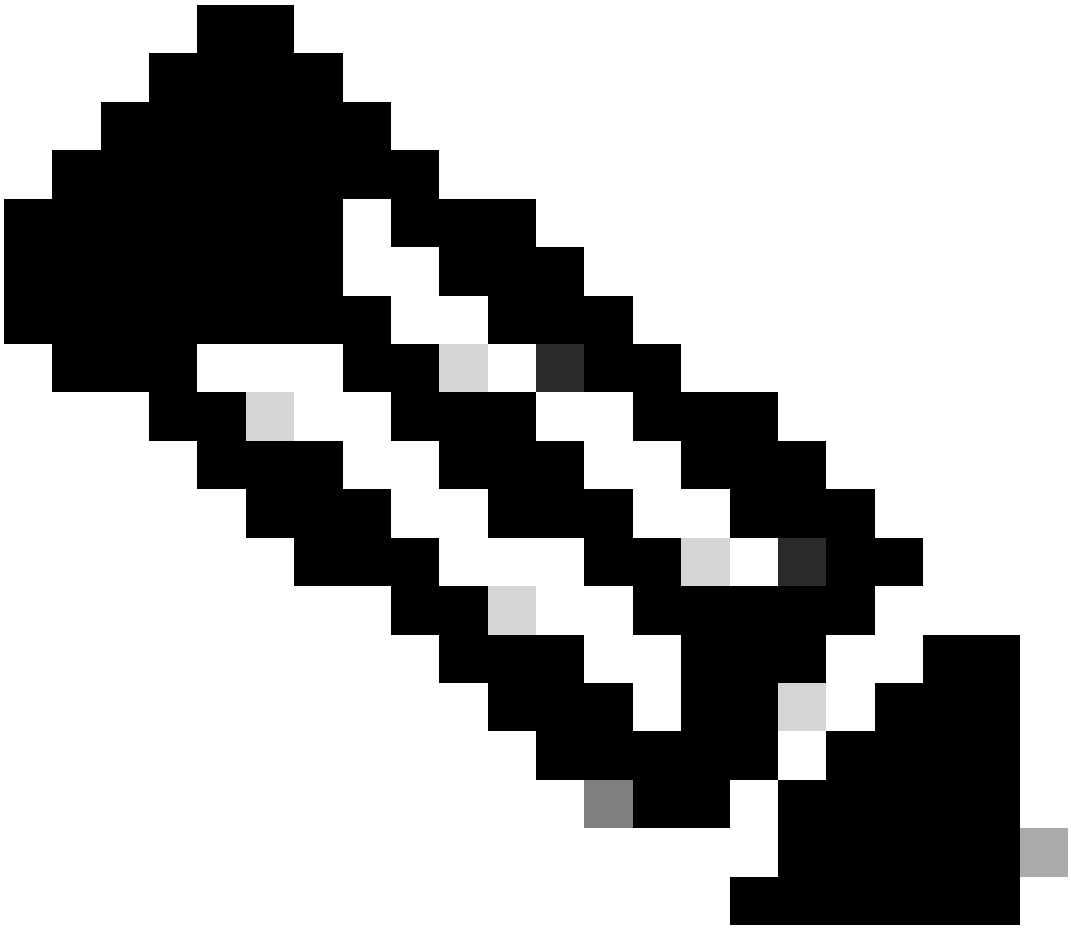
9. Der neue Anspruch muss den Namen cisco_group_policy haben.



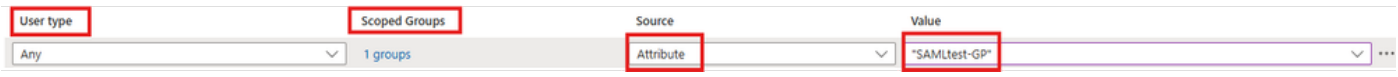
Forderung verwalten

10. Erweitern Sie den Abschnitt bezüglich der Anspruchsbedingungen. Wählen Sie den Benutzertyp und die Gruppen mit dem Gültigkeitsbereich aus, wählen Sie dann Attribute für die Quelle aus, und fügen Sie den korrekten Gruppenrichtliniennamen aus der FTD-Konfiguration im

Feld Wert hinzu, und klicken Sie auf Speichern.



Anmerkung: Der in diesem Beispiel verwendete Name der benutzerdefinierten Gruppenrichtlinie aus dem FTD ist die Gruppenrichtlinie mit dem Namen SAMLtest-GP, die im Abschnitt "Konfiguration der FMC RAVPN-Gruppenrichtlinie" dieses Leitfadens erstellt wurde. Dieser Wert muss durch den Namen der Gruppenrichtlinie aus dem FTD ersetzt werden, der jeder Benutzergruppe auf dem IdP entspricht.



MS Entra ID-Anspruchsbedingung

Überprüfung

FTD

Um die gewünschte Gruppenrichtlinie zu überprüfen, validieren Sie die Ausgabe von "show vpn-sessiondb anyconnect".

<#root>

```
FTD# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : RTPVPNtest
Index : 7110
Assigned IP : 192.168.55.3 Public IP : 10.26.162.189
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA256
Bytes Tx : 105817 Bytes Rx : 63694
Group Policy :
```

SAMLtest-GP

```
 Tunnel Group : SAMLtest
Login Time : 16:54:17 UTC Fri May 9 2025
Duration : 0h:11m:19s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : ac127ca101bc6000681e3339
Security Grp : none Tunnel Zone : 0
```

Um zu überprüfen, ob IdP den gewünschten Anspruch sendet, sammeln Sie die Ausgabe von "debug webvpn saml 255", während Sie eine Verbindung mit dem VPN herstellen. Analysieren Sie die Assertionsausgabe in den Debugs, und vergleichen Sie den Attributabschnitt mit der Konfiguration für die IdP.

<#root>

```
<Attribute Name="cisco_group_policy">
<AttributeValue>
```

SAMLtest-GP

```
</AttributeValue>
</Attribute>
```

Fehlerbehebung

<#root>

```
firepower#
```

show run webvpn

```
firepower#
show run tunnel-group

firepower#
show crypto ca certificate
firepower#
 debug webvpn saml 255
firepower#
debug webvpn 255
firepower#
debug aaa authorization
```

Zugehörige Informationen

Technischer Support und Downloads von Cisco

ASA-Konfigurationsanleitungen

FMC/FDM-Konfigurationsanleitungen

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.