Configurare l'assegnazione di Criteri di gruppo per SAML utilizzando Secure Firewall e Microsoft Entra ID

Sommario

Introduzione

In questo documento viene descritto come assegnare criteri di gruppo utilizzando Microsoft Entra ID per l'autenticazione SAML di Cisco Secure Client su Cisco Secure Firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Client AnyConnect VPN
- Configurazione di oggetti server VPN ad accesso remoto Cisco Firepower Threat Defense (FTD) o Cisco Secure Firewall ASA e Single Sign-On (SSO)
- Configurazione provider di identità Entra ID Microsoft (IdP)

Componenti usati

Le informazioni di questa guida si basano sulle seguenti versioni hardware e software:

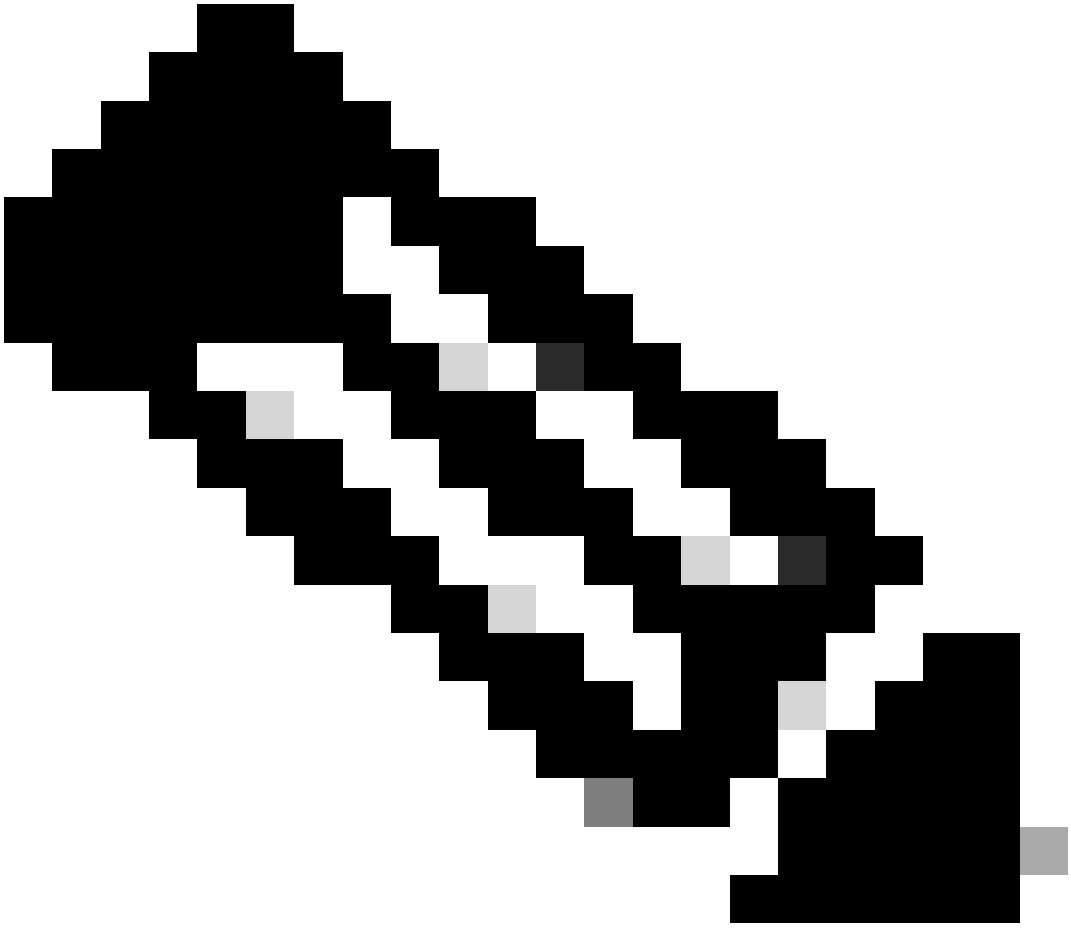
- FTD versione 7.6
- FMC versione 7.6
- ID voce SAML MS IdP

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 (Security Assertion Markup Language) è un framework basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza. Crea un cerchio di fiducia tra l'utente, un provider di servizi (SP) e un provider di identità (IdP) che consente all'utente di accedere una sola volta a più servizi. SAML può essere utilizzato per l'autenticazione VPN ad accesso remoto per le connessioni Cisco Secure Client agli headend VPN ASA e FTD, dove ASA o FTD sono la parte SP del cerchio di trust.

In questo documento Microsoft Entra ID/Azure viene usato come IdP. Tuttavia, è anche possibile assegnare criteri di gruppo utilizzando altri IdP poiché si basa su attributi standard che possono essere inviati nell'asserzione SAML.

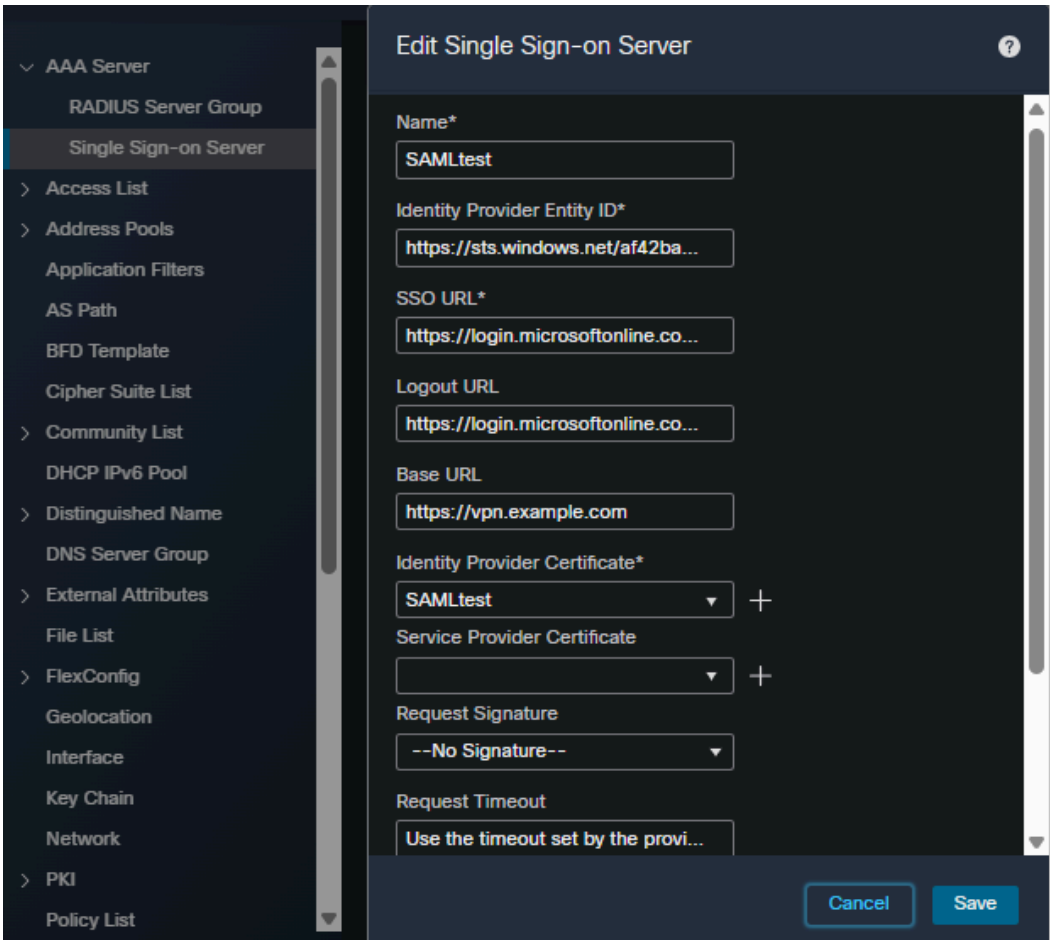


Nota: Tenere presente che ogni utente deve appartenere a un solo gruppo di utenti con ID Entra MS, in quanto più attributi SAML inviati all'ASA o all'FTD possono causare problemi con l'assegnazione dei criteri di gruppo, come descritto in ID bug Cisco CSCwm33613

Configurazione

Configurazione SAML FMC

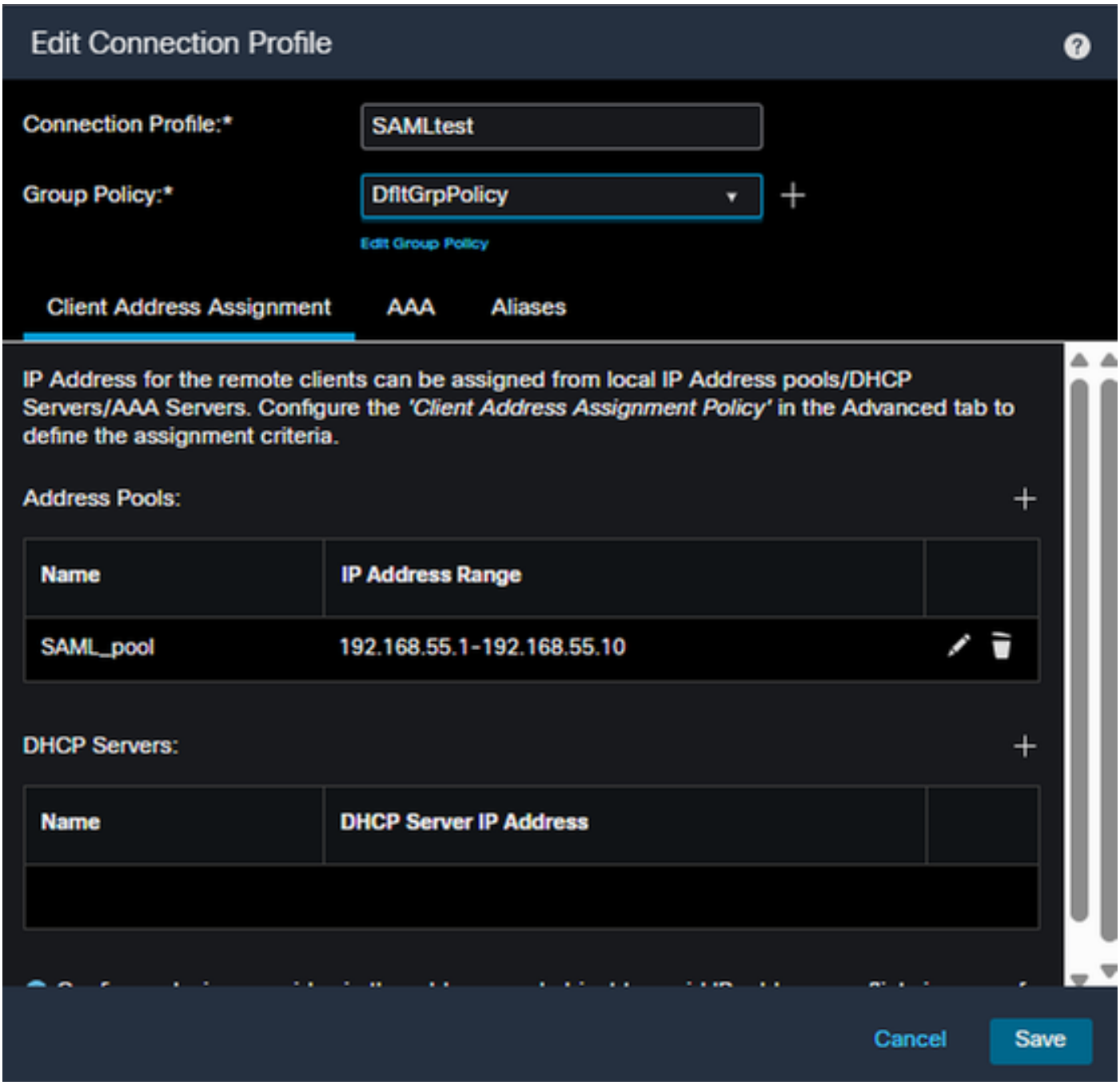
Nel FMC, selezionare Oggetti > Gestione oggetti > Server AAA > Server Single Sign-On. L'ID entità, l'URL SSO, l'URL di disconnessione e il certificato del provider di identità sono ottenuti dal provider di identità. Vedere il passaggio 6 nella sezione Microsoft Entra ID. L'URL di base e il certificato del provider di servizi sono specifici dell'FTD a cui viene aggiunta la configurazione.



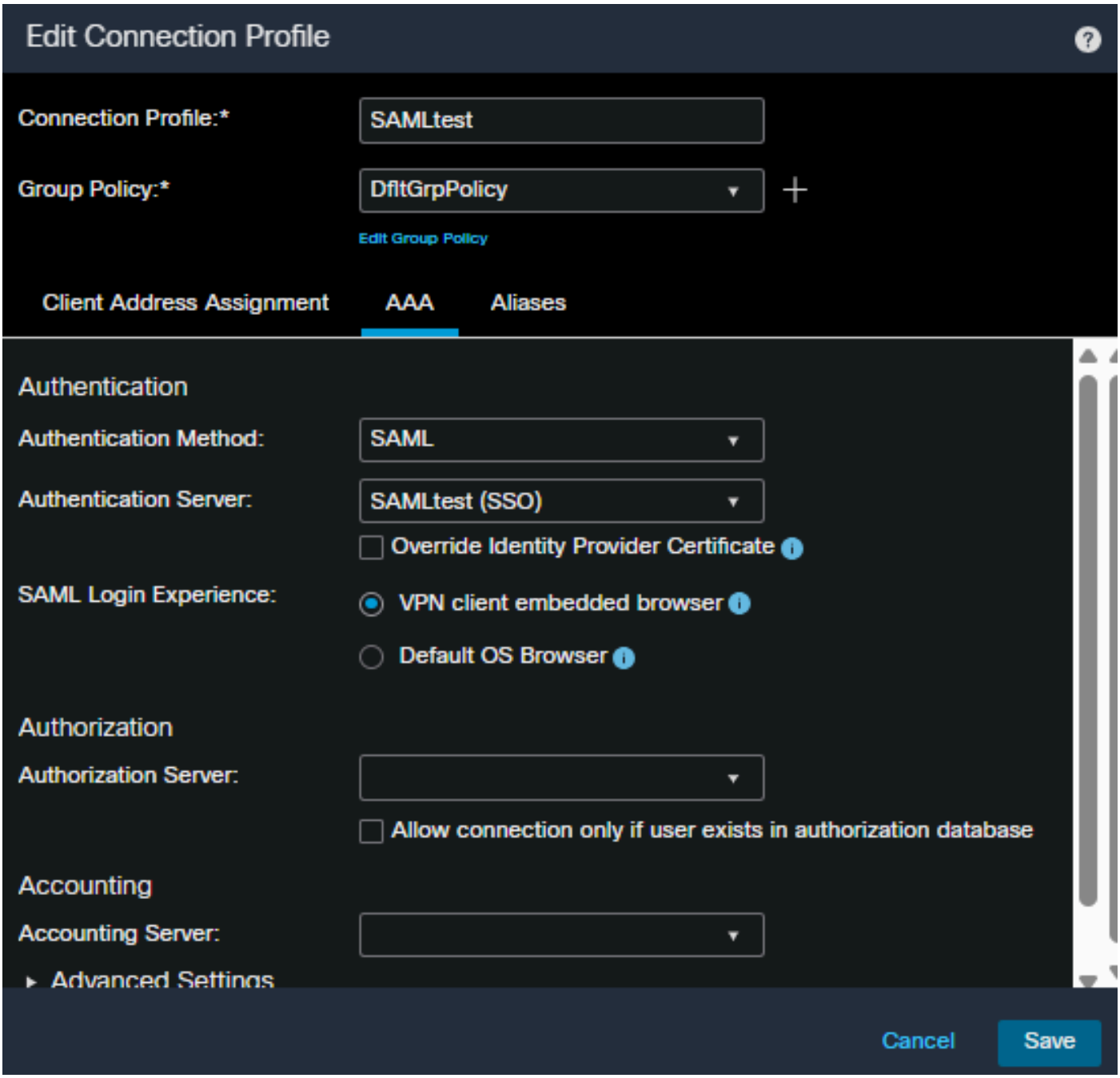
Configurazione oggetto SSO FMC

Configurazione gruppo tunnel RAVPN FMC

Nel FMC, selezionare Devices > VPN > Remote Access > Connection Profile (Dispositivi > Accesso remoto > Profilo di connessione), quindi selezionare o creare il criterio VPN per il FTD che si sta configurando. Una volta selezionata l'opzione, creare un profilo di connessione simile al seguente:



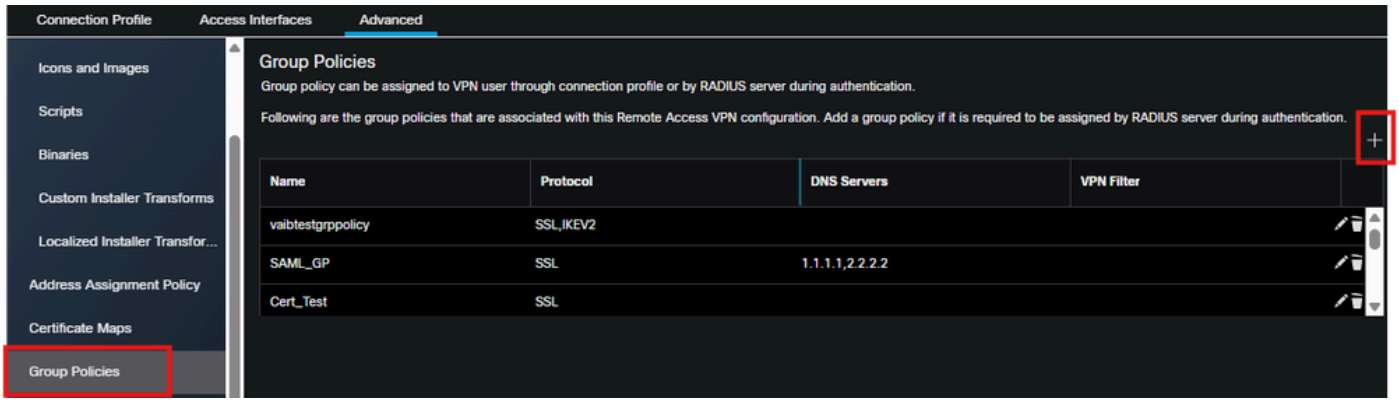
Assegnazione dell'indirizzo del profilo di connessione FMC



Configurazione AAA profilo connessione FMC

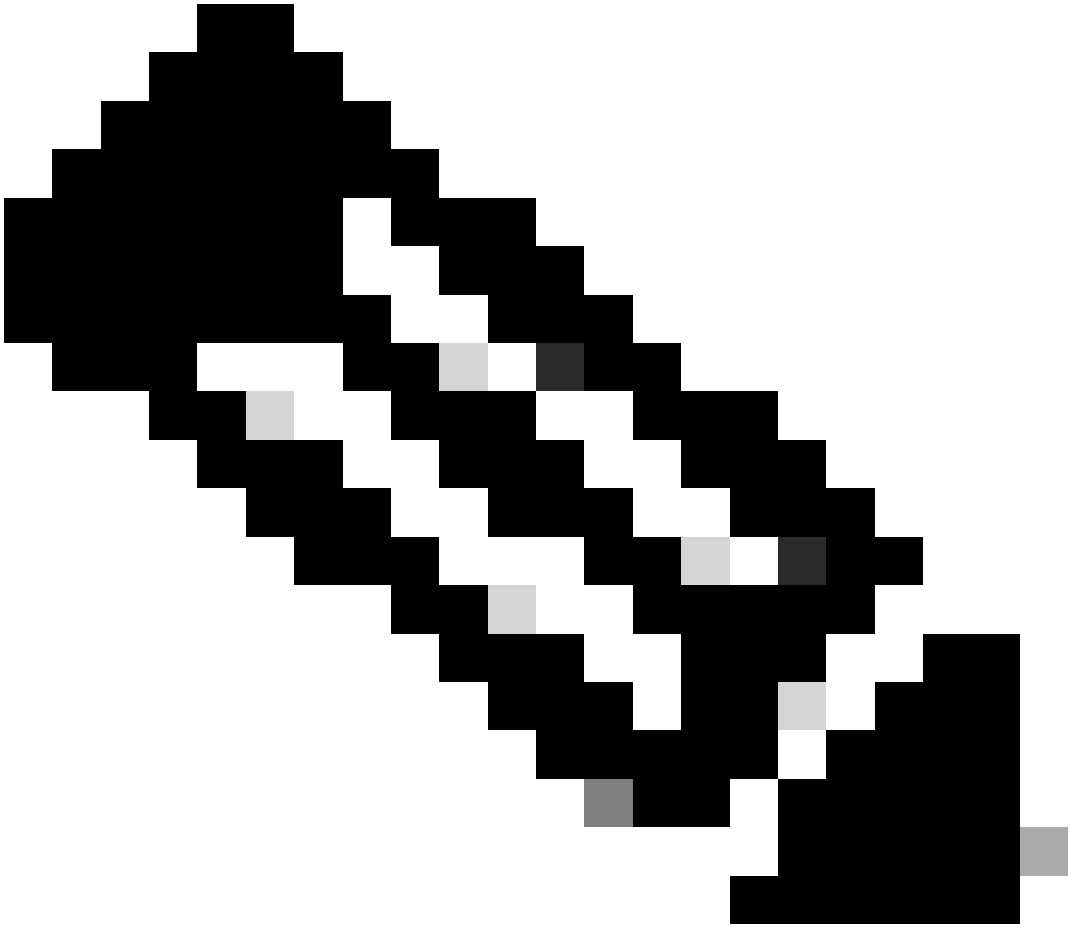
Configurazione di Criteri di gruppo RAVPN FMC

1. È necessario creare un criterio di gruppo con le opzioni necessarie per ogni gruppo di utenti su Entra ID e aggiungerlo al criterio RAVPN per l'FTD da configurare. A tale scopo, passare a Dispositivi > VPN > Accesso remoto > Avanzate e selezionare Criteri di gruppo dal lato sinistro, quindi fare clic sul segno + in alto a destra per aggiungere un criterio di gruppo.

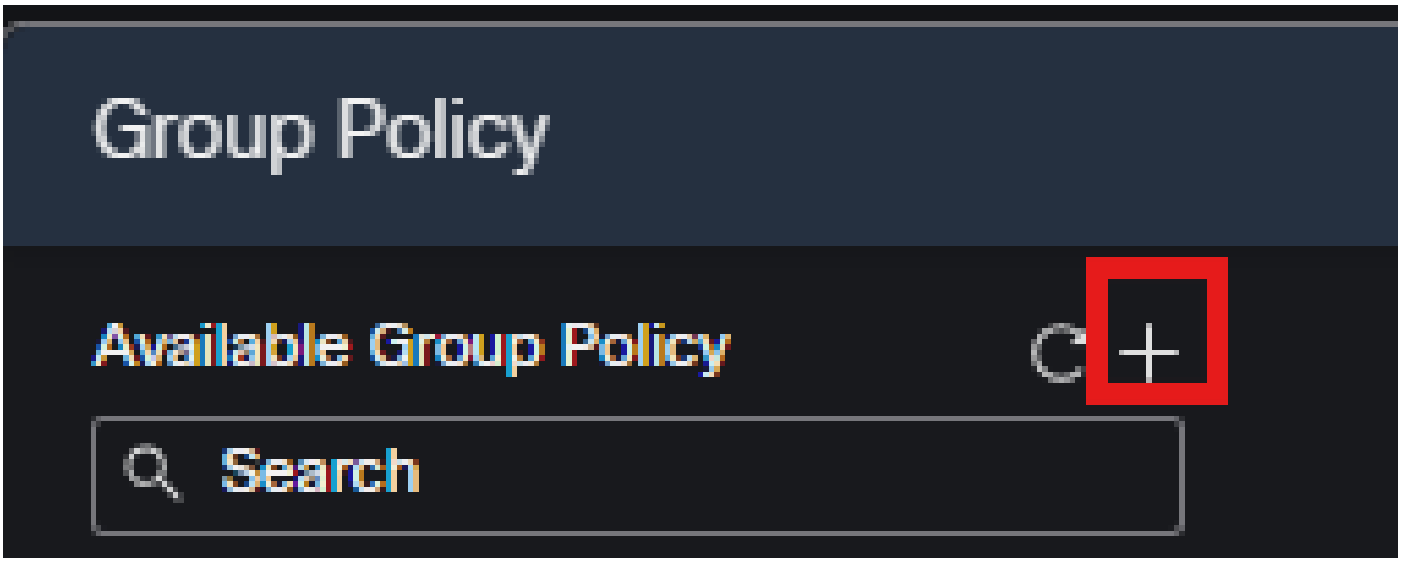


FMC: aggiungi criteri di gruppo

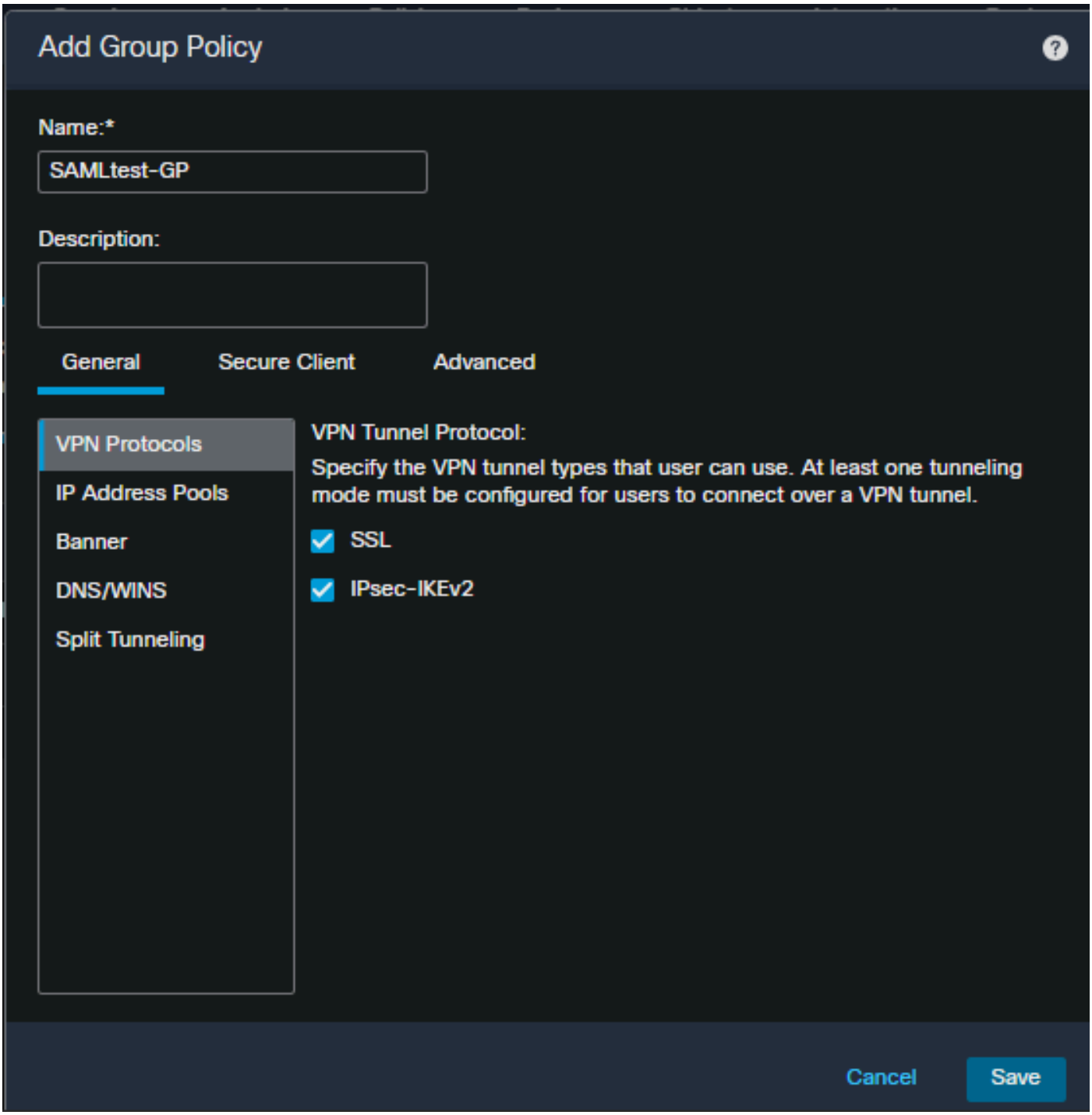
2. Fare clic sul segno + nel popup per visualizzare la finestra di dialogo e creare un nuovo criterio di gruppo. Specificate le opzioni richieste e salvate.



Nota: Se sono già stati creati i Criteri di gruppo richiesti, è possibile ignorare questo passaggio e continuare con il passaggio 3

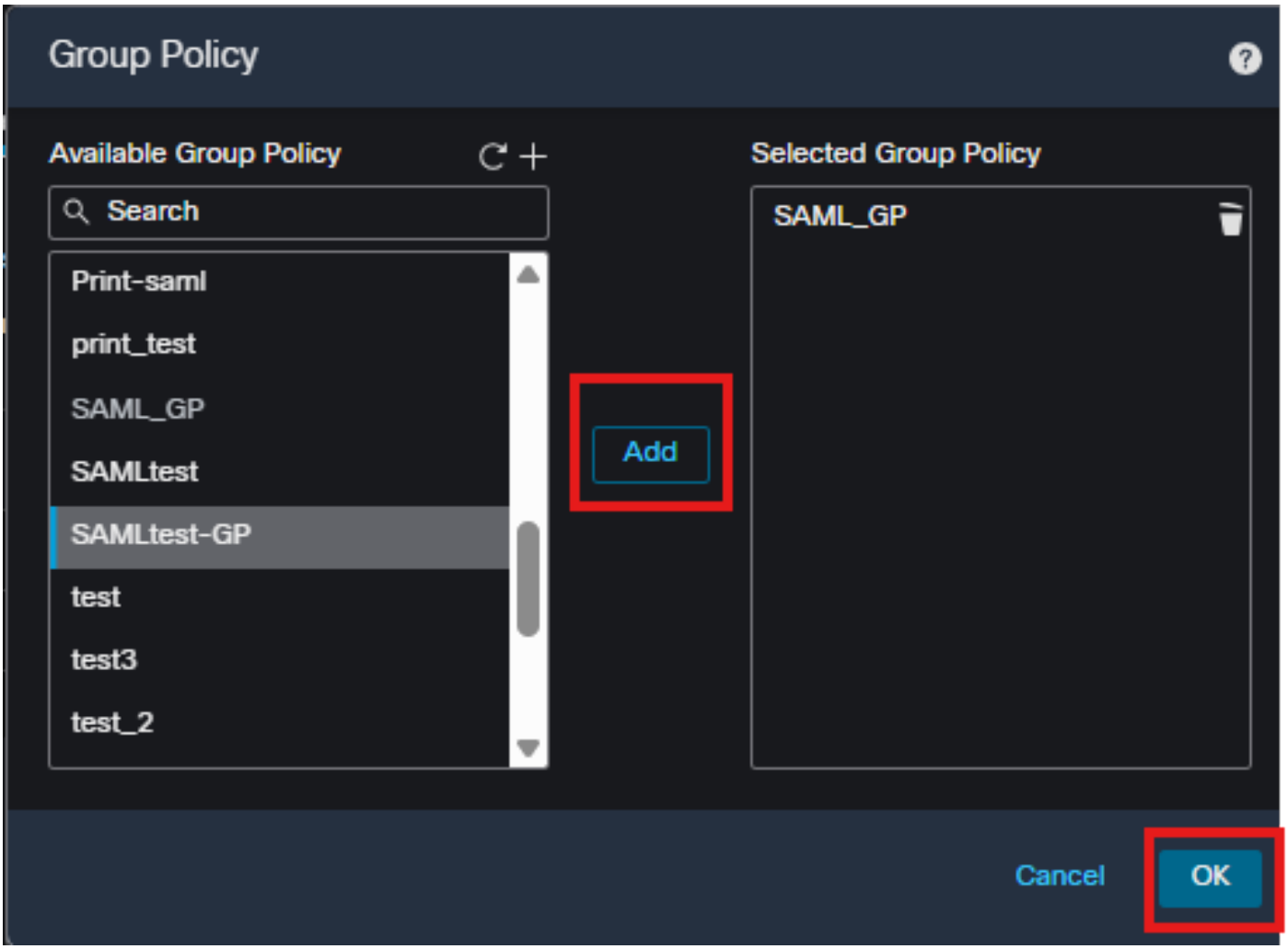


Crea nuovi Criteri di gruppo



Opzioni di Criteri di gruppo

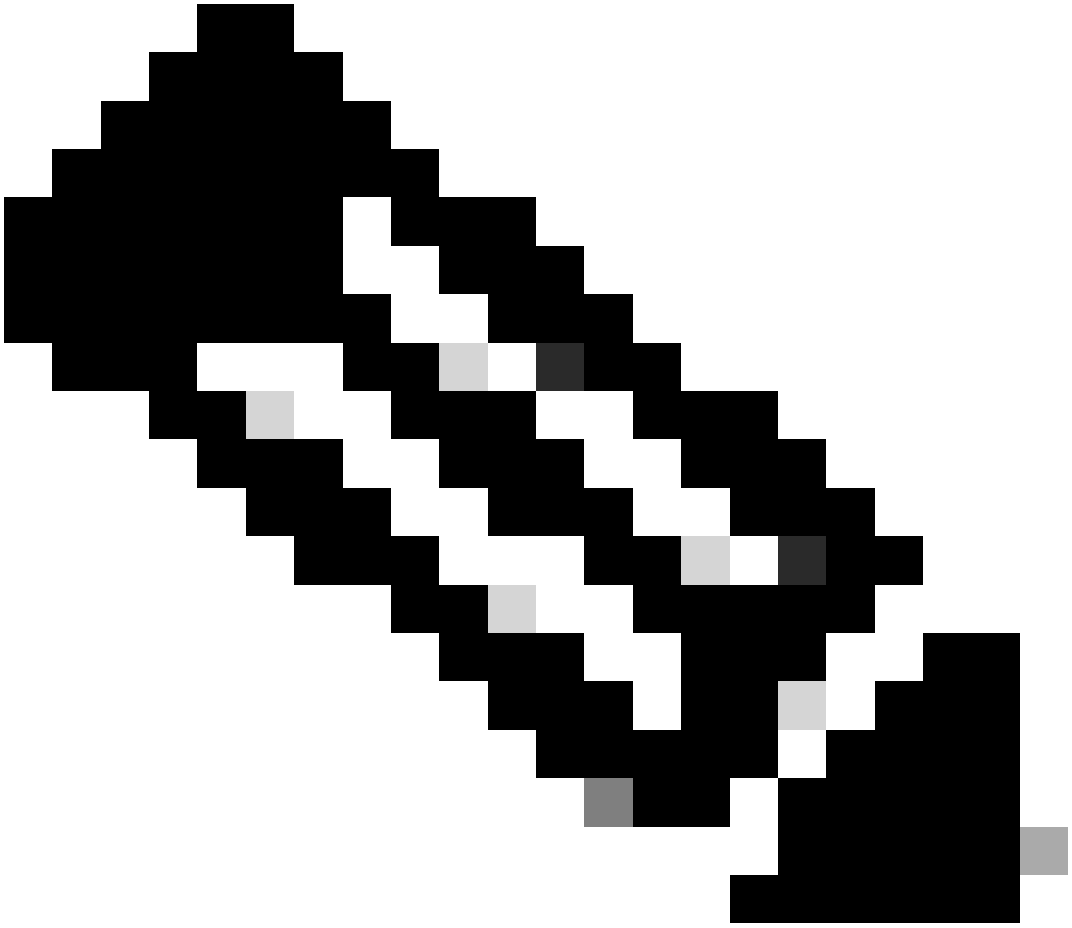
3. Selezionare il nuovo criterio di gruppo nell'elenco a sinistra e fare clic sul pulsante Aggiungi, quindi fare clic su OK per salvare l'elenco.



aggiungi criteri di gruppo

Metadati FTD

Una volta distribuita la configurazione nell'FTD, passare alla CLI dell'FTD ed eseguire il comando "show saml metadata <nome gruppo tunnel>" e raccogliere l'ID entità FTD e l'URL ACS.



Nota: Il certificato nei metadati è stato troncato per brevità.

<#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
```

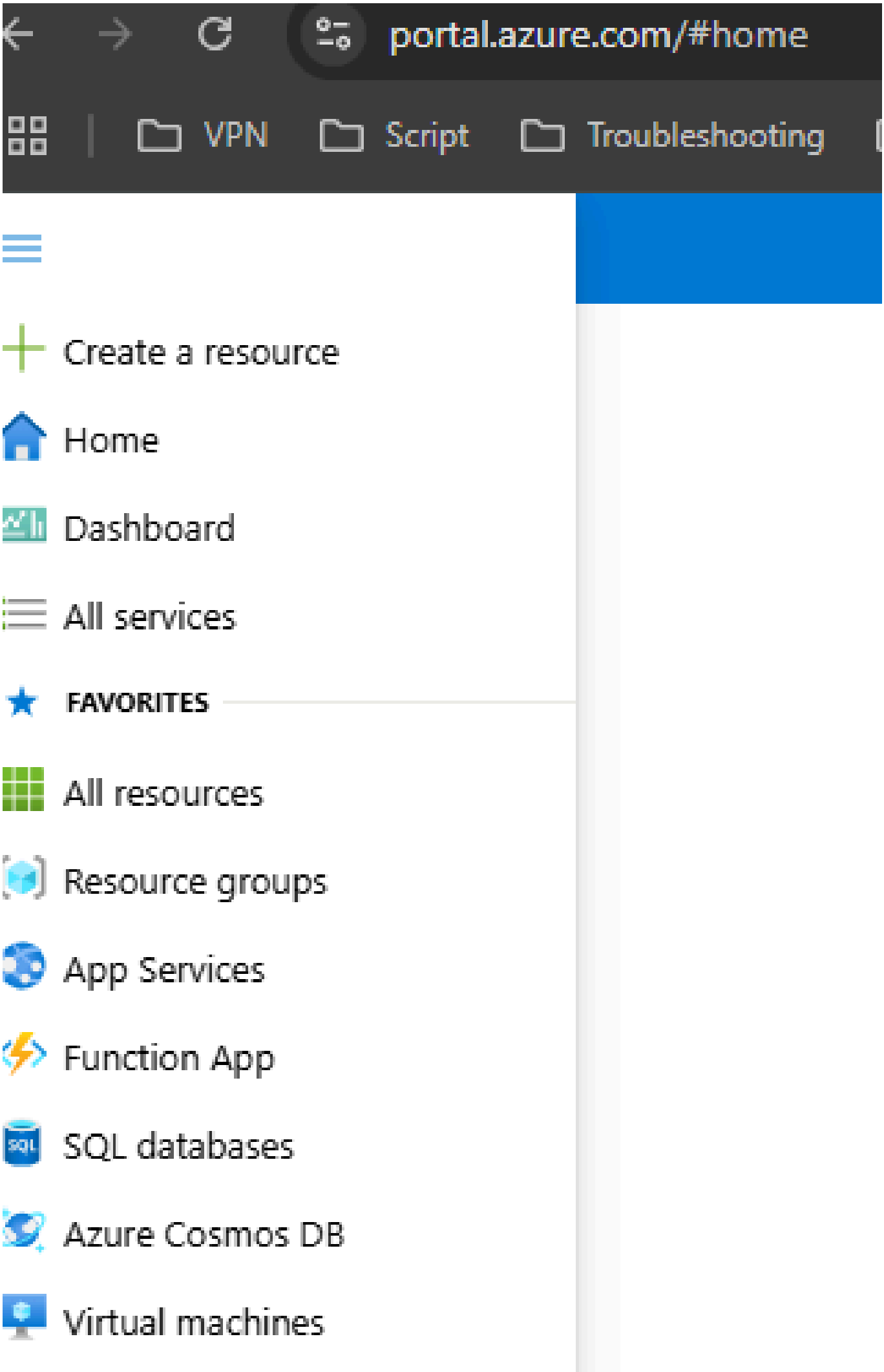
```
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</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

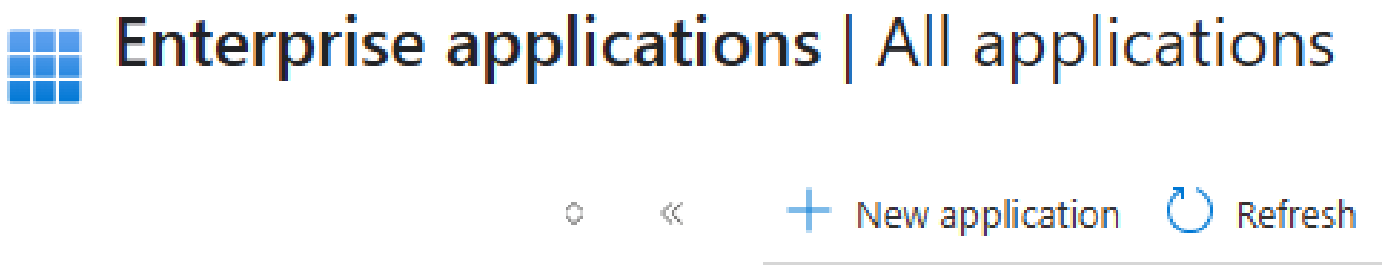
```
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

ID Entra Microsoft

1. Nel portale di Microsoft Azure, selezionare Microsoft Entra ID dal menu a sinistra.

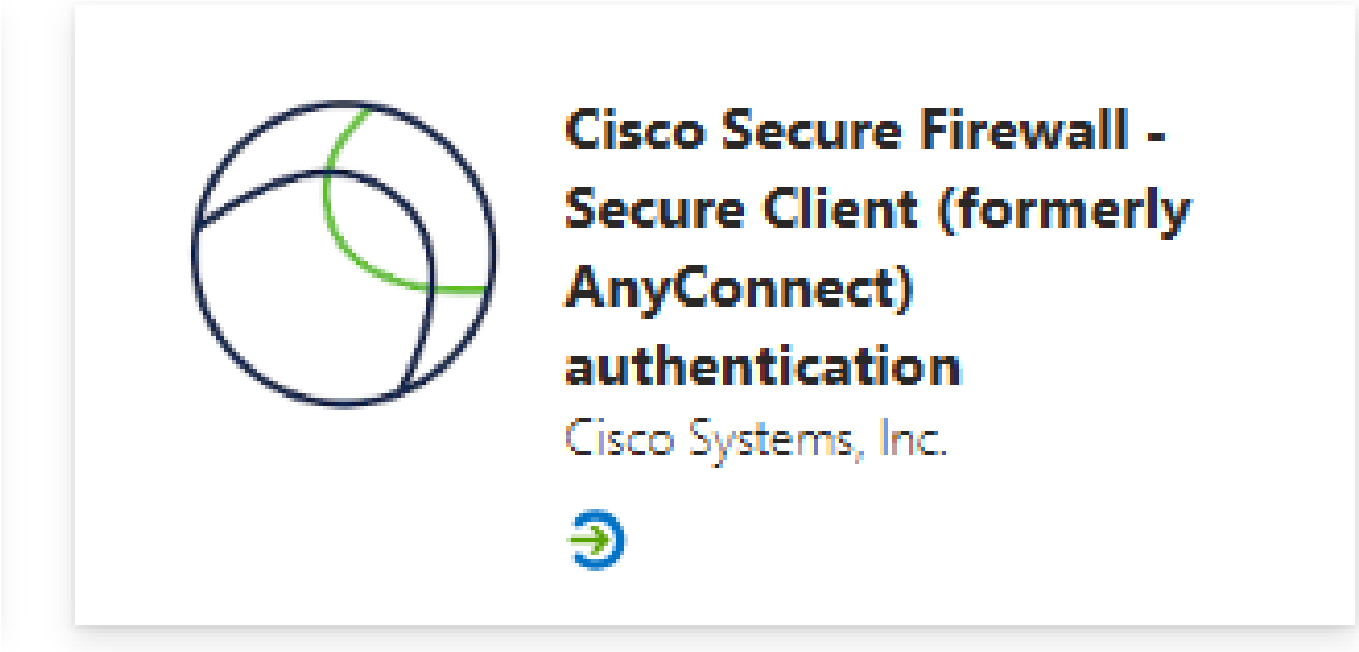

portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

Se esiste già un'applicazione enterprise configurata per la configurazione RAVPN FTD, ignorare i passaggi successivi e continuare con il passaggio 7.



Applicazione MS Entra ID Enterprise

4. Selezionare l'autenticazione Cisco Secure Firewall - Secure Client (in precedenza AnyConnect) in Applicazioni in primo piano. Assegnare un nome all'applicazione e selezionare Crea.



MS Entra ID Applicazione di autenticazione Cisco Secure Firewall Secure Client (in precedenza AnyConnect)

5. All'interno dell'applicazione, selezionare Utenti e gruppi e assegnare all'applicazione i nomi degli utenti o dei gruppi necessari.

Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

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

e recuperare l'URL di accesso, l'identificatore di accesso Microsoft e l'URL di disconnessione per la sezione Configurazione SAML FMC di questa guida.

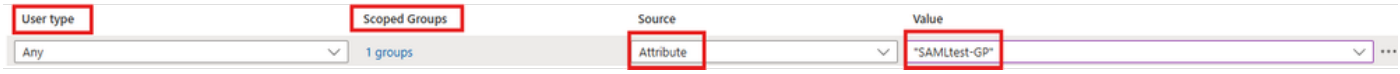
Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

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

Il nome dei criteri di gruppo personalizzati dell'FTD utilizzato in questo esempio è il criterio di gruppo denominato SAMLtest-GP creato nella sezione Configurazione Criteri di gruppo RAVPN del FMC di questa guida. Questo valore deve essere sostituito con il nome dei criteri di gruppo dell'FTD corrispondente a ogni gruppo di utenti dell'IdP.



Condizione attestazione ID entrante MS

Verifica

FTD

Per verificare i criteri di gruppo desiderati, convalidare l'output di "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
```

Per verificare che l'IdP stia inviando l'attestazione desiderata, raccogliere l'output di "debug webvpn saml 255" durante la connessione alla VPN. Analizzare l'output dell'asserzione nei debug e confrontare la sezione dell'attributo con quanto configurato nell'IdP.

<#root>

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

```
SAMLtest-GP

</AttributeValue>
</Attribute>
```

Risoluzione dei problemi

<#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
```

Informazioni correlate

Supporto tecnico Cisco e download

Guide alla configurazione dell'ASA

Guide alla configurazione di FMC/FDM

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).