Configure AnyConnect SSO with Duo and LDAP Mapping on Secure Firewall

Contents

Introduction

This document describes a configuration example for AnyConnect Single Sign-On (SSO) with Duo and LDAP mapping for authorization on Secure Firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect Secure Mobility Client
- Cisco Secure Firepower Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)
- Fundamentals of Duo Security
- Security Assertion Markup Language (SAML)
- Configuration of Active Directory (AD) services on Microsoft Windows Server

Components Used

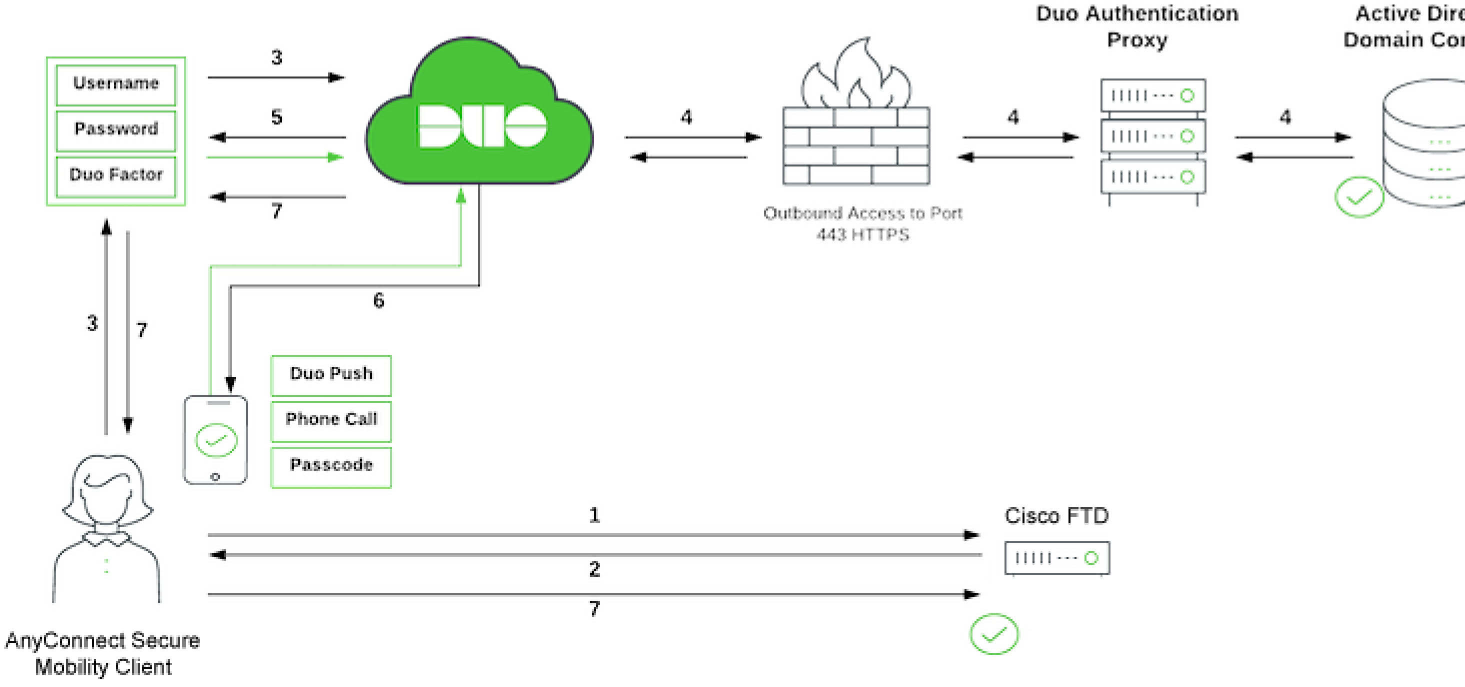
The information in this document is based on these software versions:

- Cisco Secure FMC version 7.4.0
- Cisco Secure FTD version 7.4.0
- Duo Authentication Proxy
- Anyconnect Secure Mobility Client version 4.10.06079
- Windows Server 2016, configured as an AD server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



DUO SSO Traffic Flow

Duo Traffic Flow

1. AnyConnect Client initiates a Secure Sockets Layer (SSL) Virtual Private Network (VPN) connection to Cisco Secure FTD.
2. Secure FTD redirects the embedded browser in the AnyConnect client to Duo SSO for SAML authentication.
3. AnyConnect user logs in with primary on-prem Active Directory credentials.
4. Duo SSO performs primary authentication via an on-premises Duo Authentication Proxy to on-prem Active Directory.
5. Once the primary authentication is successful, Duo SSO begins two-factor authentication (2FA).
6. AnyConnect user completes Duo 2FA.
7. Duo SSO redirects the user back to the FTD with a response message indicating success.

SAML with External LDAP

External authorization of the SAML user depends on the NameID value returned by the IdP. The Secure Firewall maps the NameID field to the username and this username can be used to query LDAP.

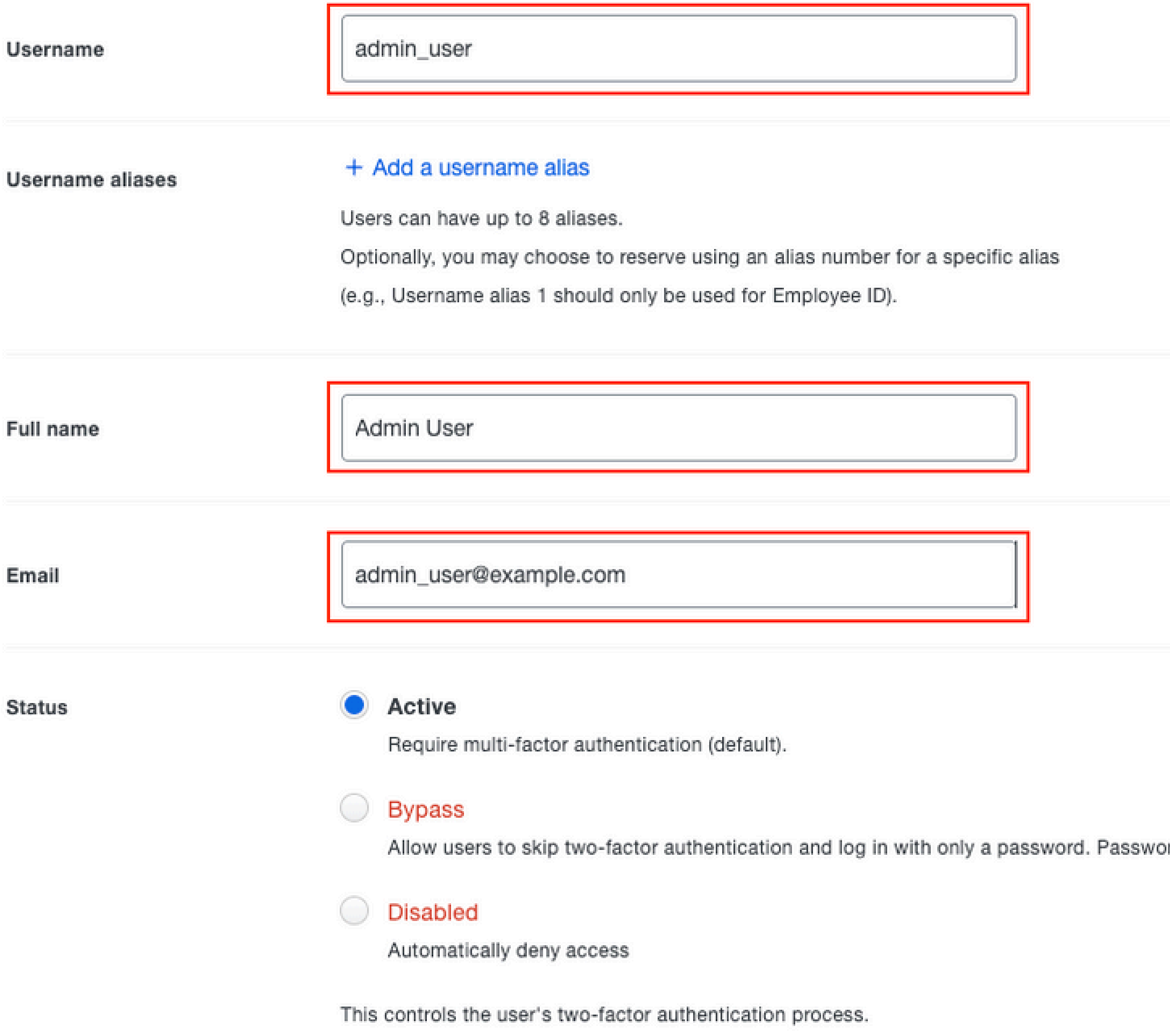
> **Note**: The configuration used in this document is to allow users that belong to an AD group to establish a Remote Access (RA) VPN connection. Connection is prohibited for users from different AD groups not defined on the map.

Configurations

Duo Admin Portal Configuration

Configure an AD or a SAML identity provider that can be used as your primary authentication source for Duo SSO.
Also, you need a Duo Authentication Proxy (recommended three authentication proxy servers for high avail

For more information, refer to Duo Single Sign-On.



Username: admin_user

Username aliases: + Add a username alias

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).

Full name: Admin User

Email: admin_user@example.com

Status:

● Active

Require multi-factor authentication (default).

○ Bypass

Allow users to skip two-factor authentication and log in with only a password. Passwo

○ Disabled

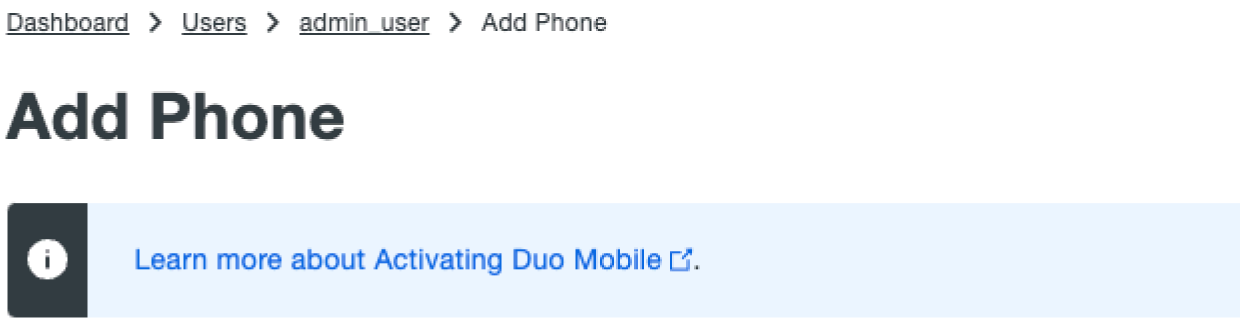
Automatically deny access

This controls the user's two-factor authentication process.

Duo User Information

> **Note**: **Username** data and **Email** data must match the information provided in the Active Directory server.

Step 6. **Add Phone** in order to add the phone number of the user. This is needed for the user to authenticate via 2FA with Duo Push.



Dashboard > Users > admin_user > Add Phone

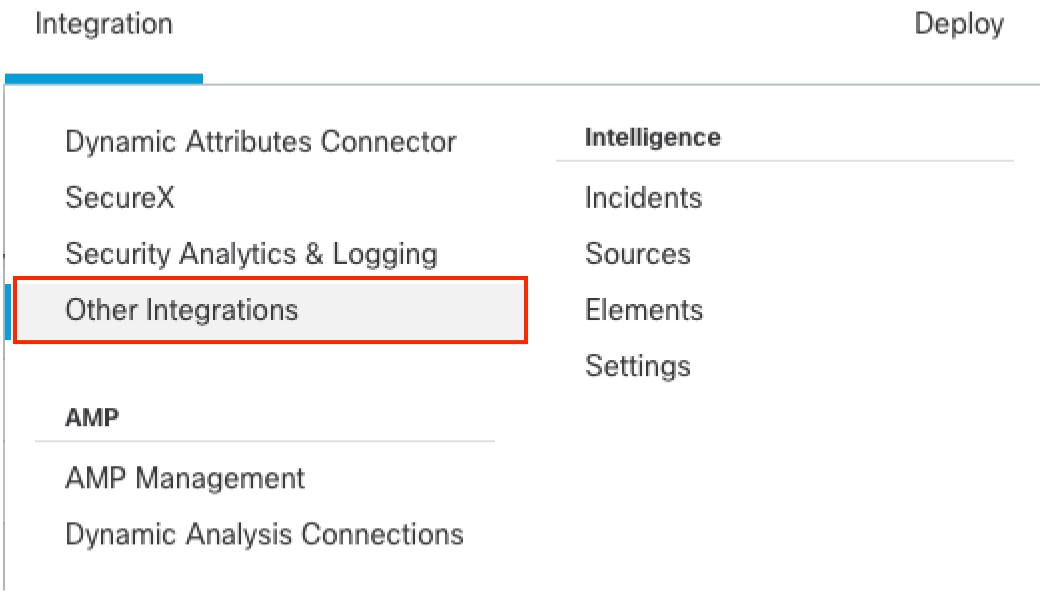
Add Phone

Learn more about Activating Duo Mobile.

is set to 300 as Duo push is sent during the authentication process and user interaction is needed. Modify the Request Timeout value according to the network design.

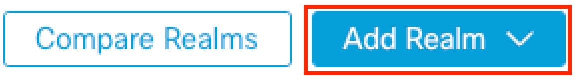
Step 3. Configure REALM/LDAP server configuration.

- Navigate to **Integration > Other Integrations**.



FMC Realm

- Click Add a new realm.

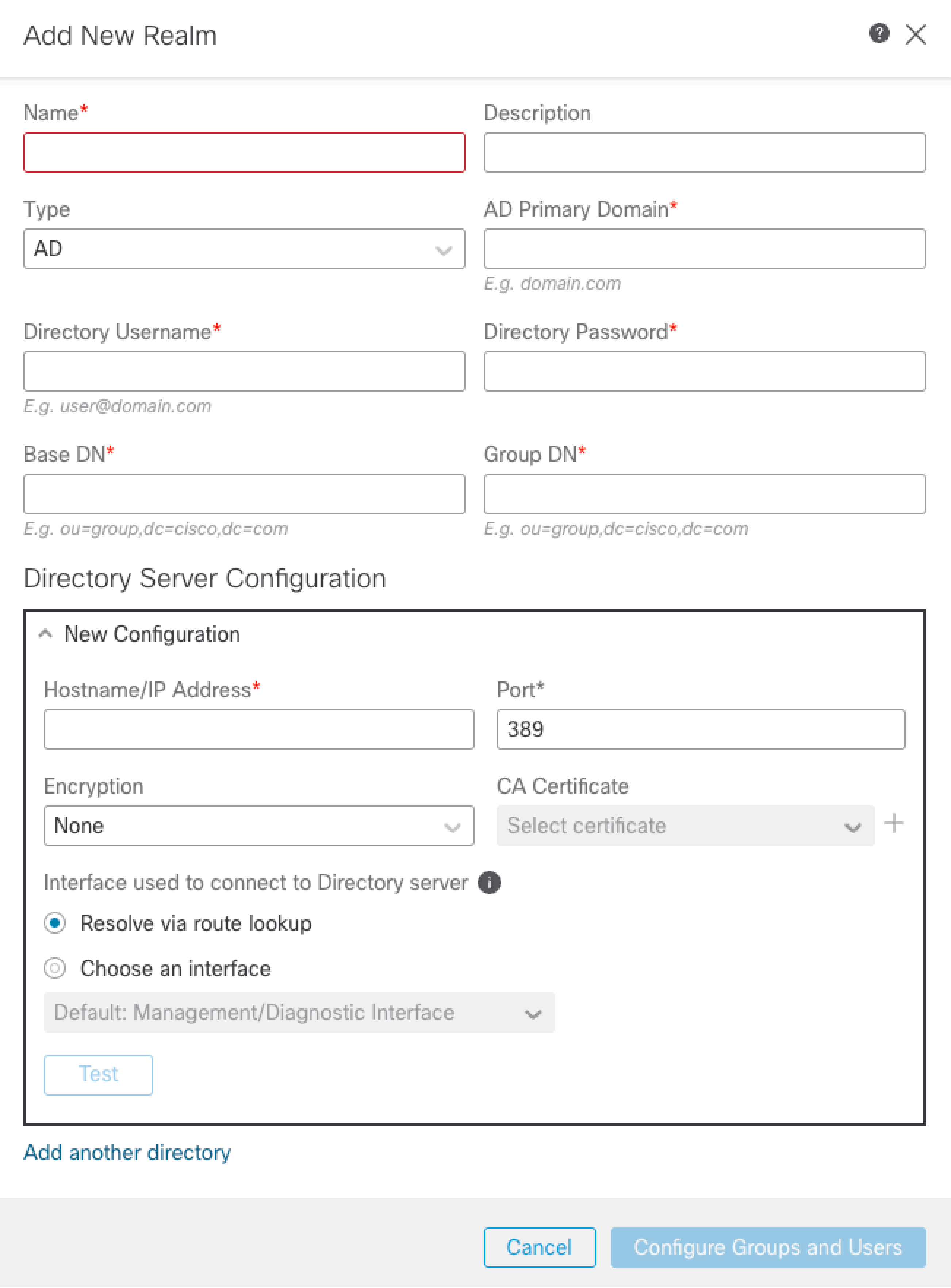


FMC Add Realm

- Provide the details of the Active Directory server and directory. Click **OK**.

For the purpose of this demonstration:

- Name: ActiveDirectory_SSO
- Type: AD
- AD Primary Domain: example.com
- Directory Username: administrator@example.com
- Directory Password: <Hidden>
- Base DN: DC=example, DC=com
- Group DN: DC=example, DC=com



Add New Realm

Name*

Description

Type: AD

AD Primary Domain*
E.g. domain.com

Directory Username*
E.g. user@domain.com

Directory Password*

Base DN*
E.g. ou=group,dc=cisco,dc=com

Group DN*
E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

New Configuration

Hostname/IP Address*

Port*: 389

Encryption: None

CA Certificate: Select certificate

Interface used to connect to Directory server

● Resolve via route lookup

○ Choose an interface

Default: Management/Diagnostic Interface

FMC Realm Information

Note: LDAPS (LDAP over SSL) can be used. The port must be changed from 389 to 636.

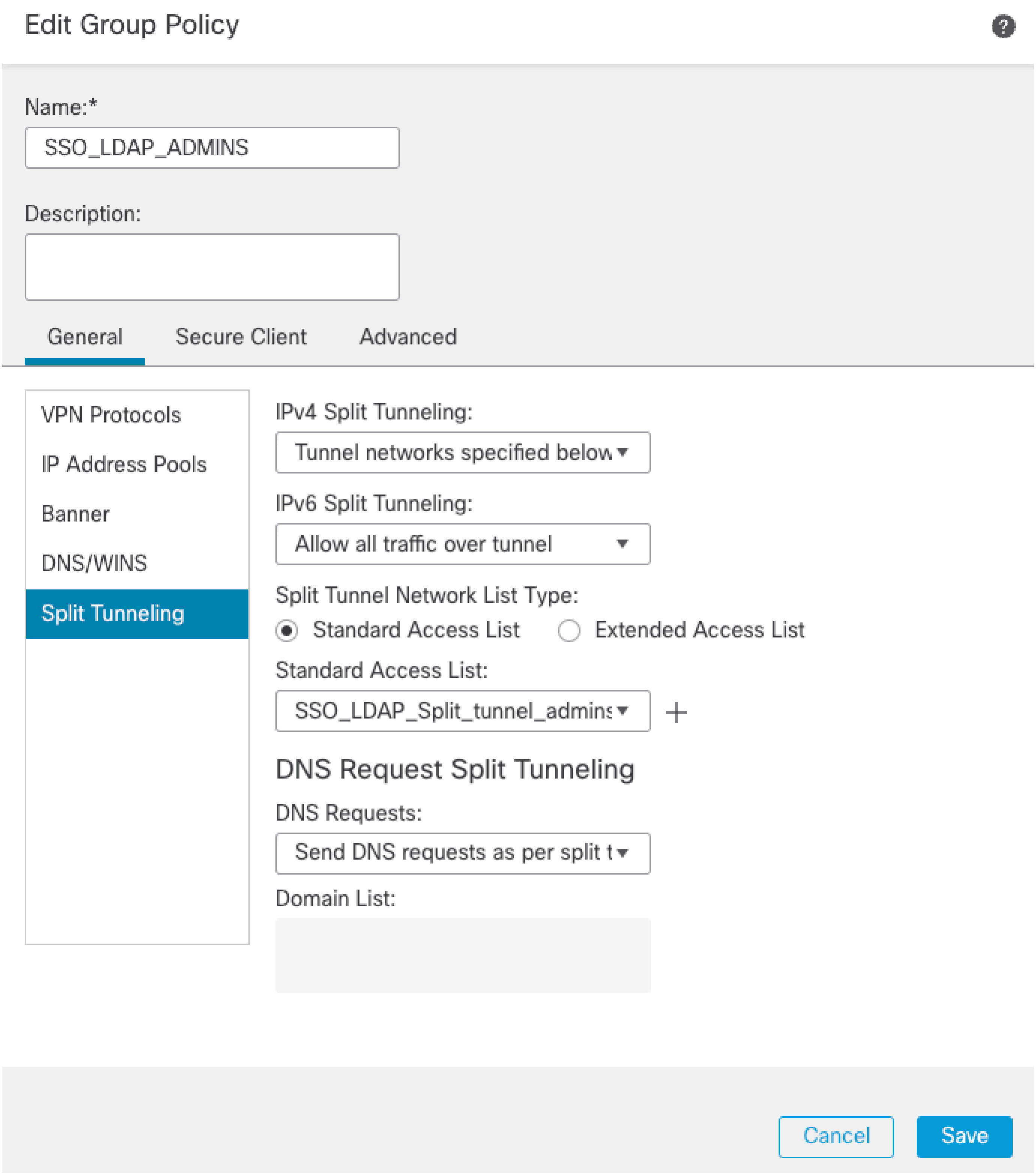
Note: AD server must have user data that has been uploaded to Duo.

Step 4. Create Group Policies as needed.

- Navigate to Objects > Object Management > VPN > Group Policy.
- ClickAdd Group Policy .
- Create Group Policy with its respective parameters.

For the purpose of this demonstration, three Group Policies have been configured:

1. SSO_LDAP_ADMINS Group Policy is the group for users that belong to the AnyConnect Admins group.



Edit Group Policy

Name:*

SSO_LDAP_ADMINS

Description:

IPv4 Split Tunneling:

Tunnel networks specified below

IPv6 Split Tunneling:

Allow all traffic over tunnel

Split Tunnel Network List Type:

● Standard Access List ○ Extended Access List

Standard Access List:

SSO_LDAP_Split_tunnel_admins

DNS Request Split Tunneling

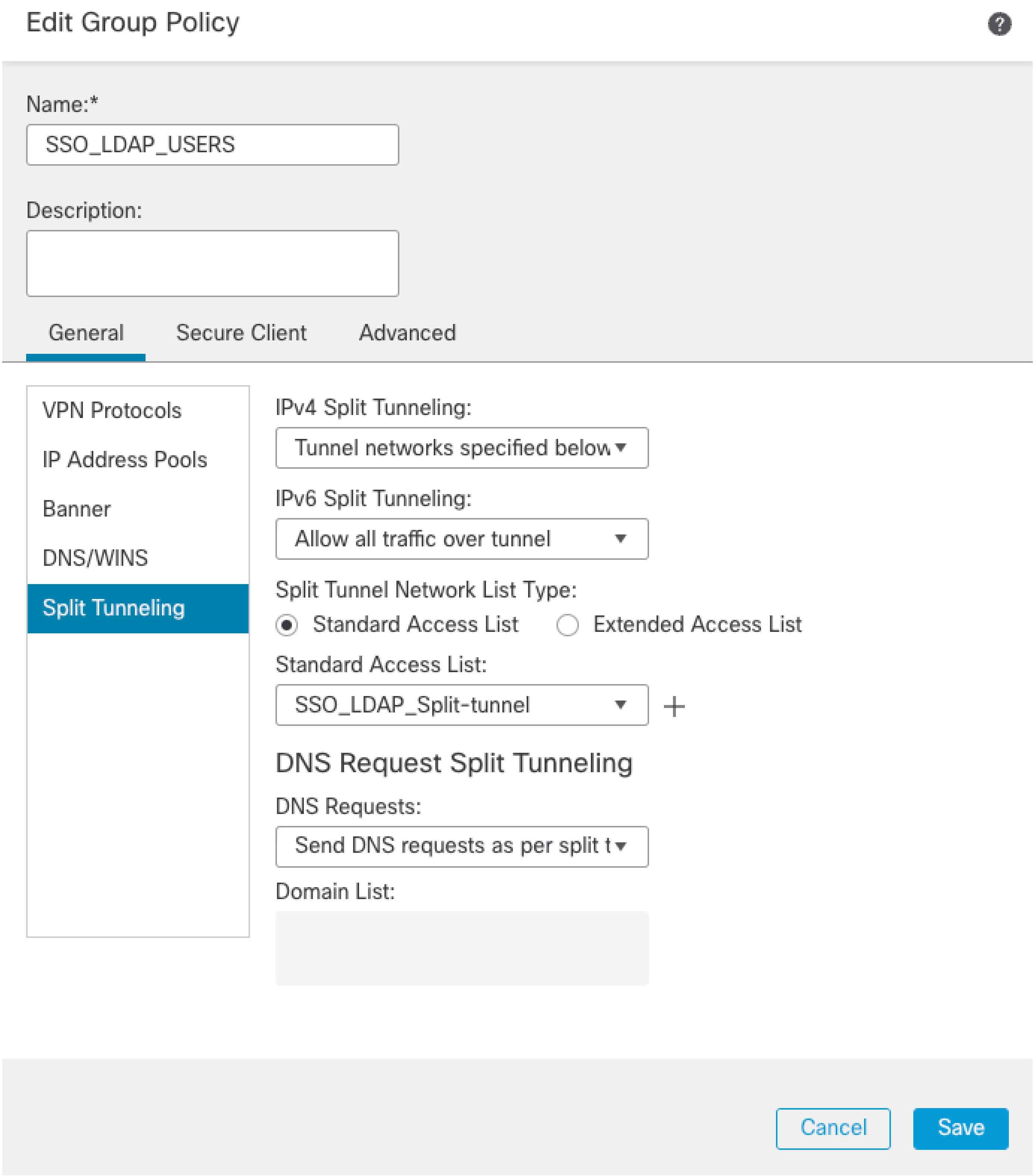
DNS Requests:

Send DNS requests as per split t

Domain List:

Group Policy 1

2. SSO_LDAP_USERS Group Policy is the group for users that belong to the AnyConnect Users group.



Edit Group Policy

Name:* SSO_LDAP_USERS

Description:

IPv4 Split Tunneling: Tunnel networks specified below

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

Standard Access List: SSO_LDAP_Split-tunnel

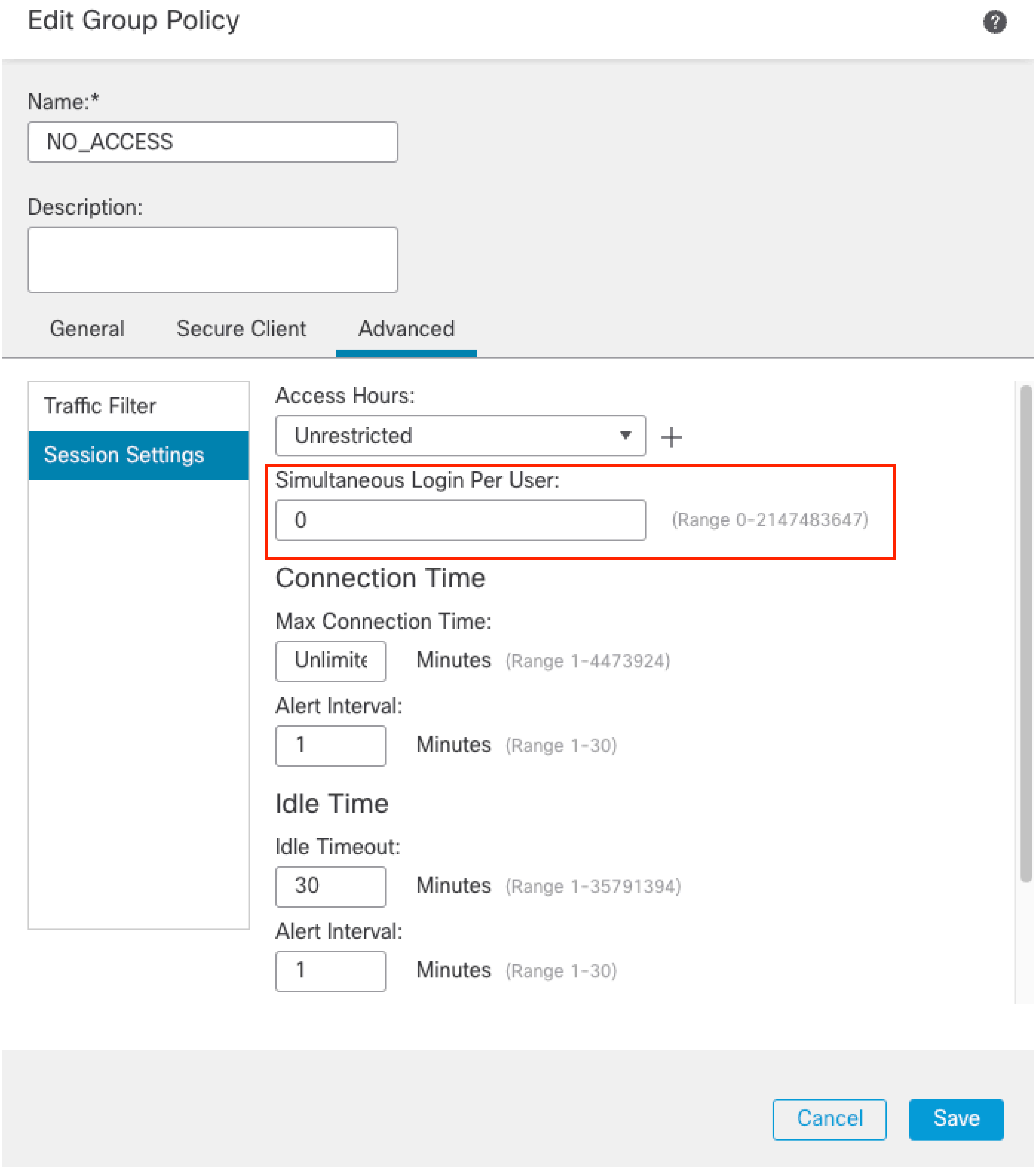
DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split t

Domain List:

Group Policy 2

3. The NO_ACCESS Group Policy is the group for users that do not belong to any of the previous Group Policy. It has the Simultaneous Login Per User parameter must be set to 0.



Edit Group Policy

Name:* NO_ACCESS

Description:

Access Hours: Unrestricted

Simultaneous Login Per User: 0 (Range 0-2147483647)

Connection Time

Max Connection Time: Unlimite Minutes (Range 1-4473924)

Alert Interval: 1 Minutes (Range 1-30)

Idle Time

Idle Timeout: 30 Minutes (Range 1-35791394)

Alert Interval: 1 Minutes (Range 1-30)

Group Policy 3

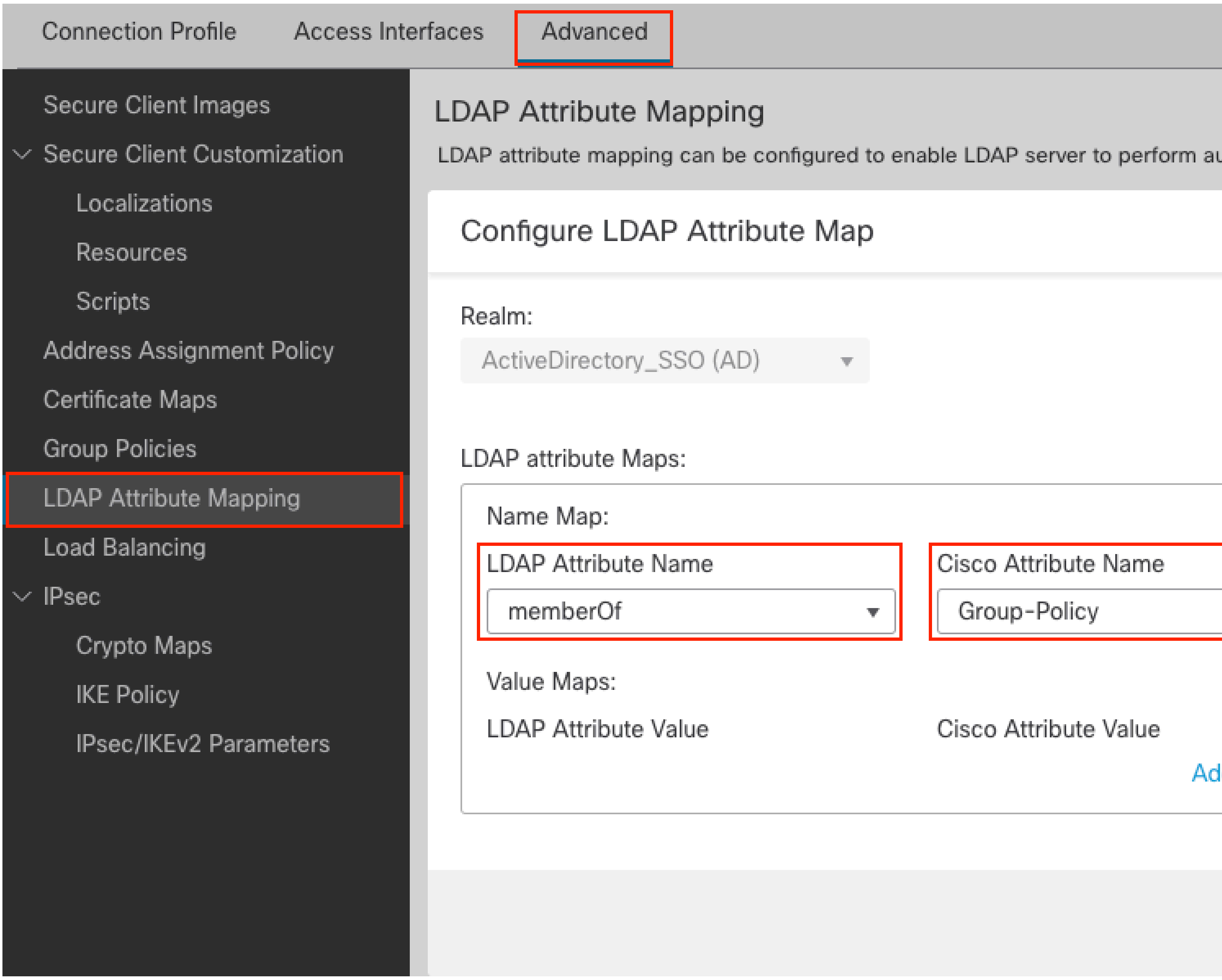
Step 5. Configure LDAP Attribute Mapping.

- Navigate to Devices > VPN > Remote Access.
- Choose the current Remote Access VPN configuration.
- Navigate to **Advanced > LDAP Attribute Mapping**.
- Click the plus + sign and add a new LDAP Attribute Mapping .

- Provide the LDAP Attribute Name and the Cisco Attribute Name. Click Add Value Map.

For the purpose of this demonstration, LDAP attribute map configuration:

- LDAP Attribute Name: memberOf
- Cisco Attribute Name: Group-Policy



LDAP Attribute Mapping

LDAP attribute mapping can be configured to enable LDAP server to perform au

Configure LDAP Attribute Map

Realm: ActiveDirectory_SSO (AD)

LDAP attribute Maps:

Name Map:

LDAP Attribute Name: memberOf

Cisco Attribute Name: Group-Policy

Value Maps:

LDAP Attribute Value

Cisco Attribute Value

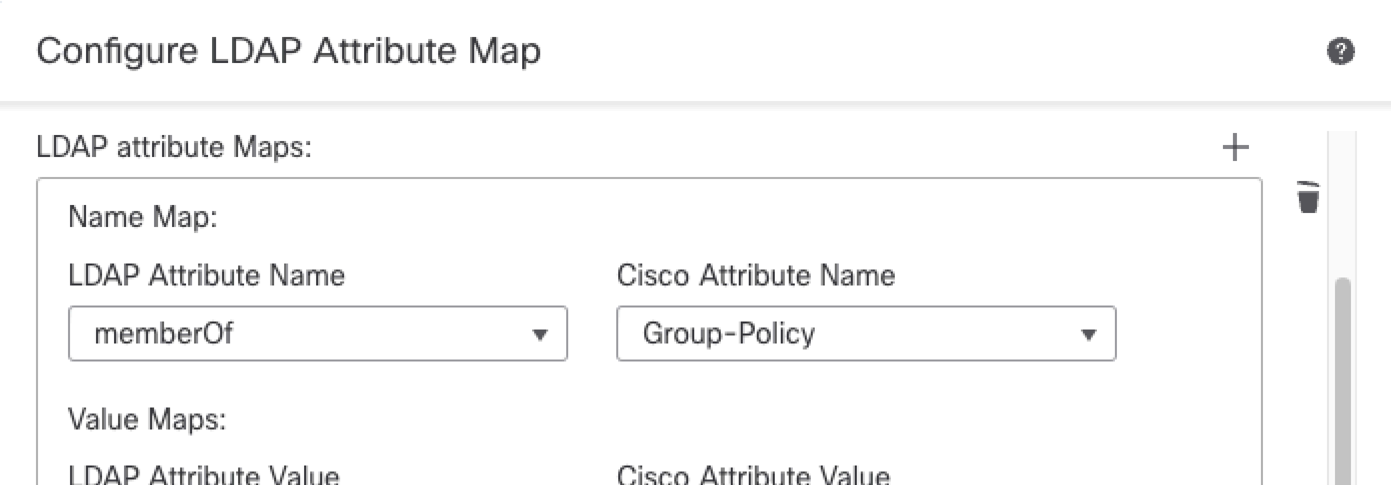
LDAP Attribute Map

- Provide the LDAP Attribute Value and the Cisco Attribute Value. Click **OK** .

For the purpose of this demonstration:

LDAP Attribute Value: CN=AnyConnect Admins, CN=Users, DC=example, DC=com
Cisco Attribute Value: SSO_LDAP_ADMINS

LDAP Attribute Value: CN=AnyConnect Users, CN=Users, DC=example, DC=com
Cisco Attribute Value: SSO_LDAP_USERS



Configure LDAP Attribute Map

LDAP attribute Maps:

Name Map:

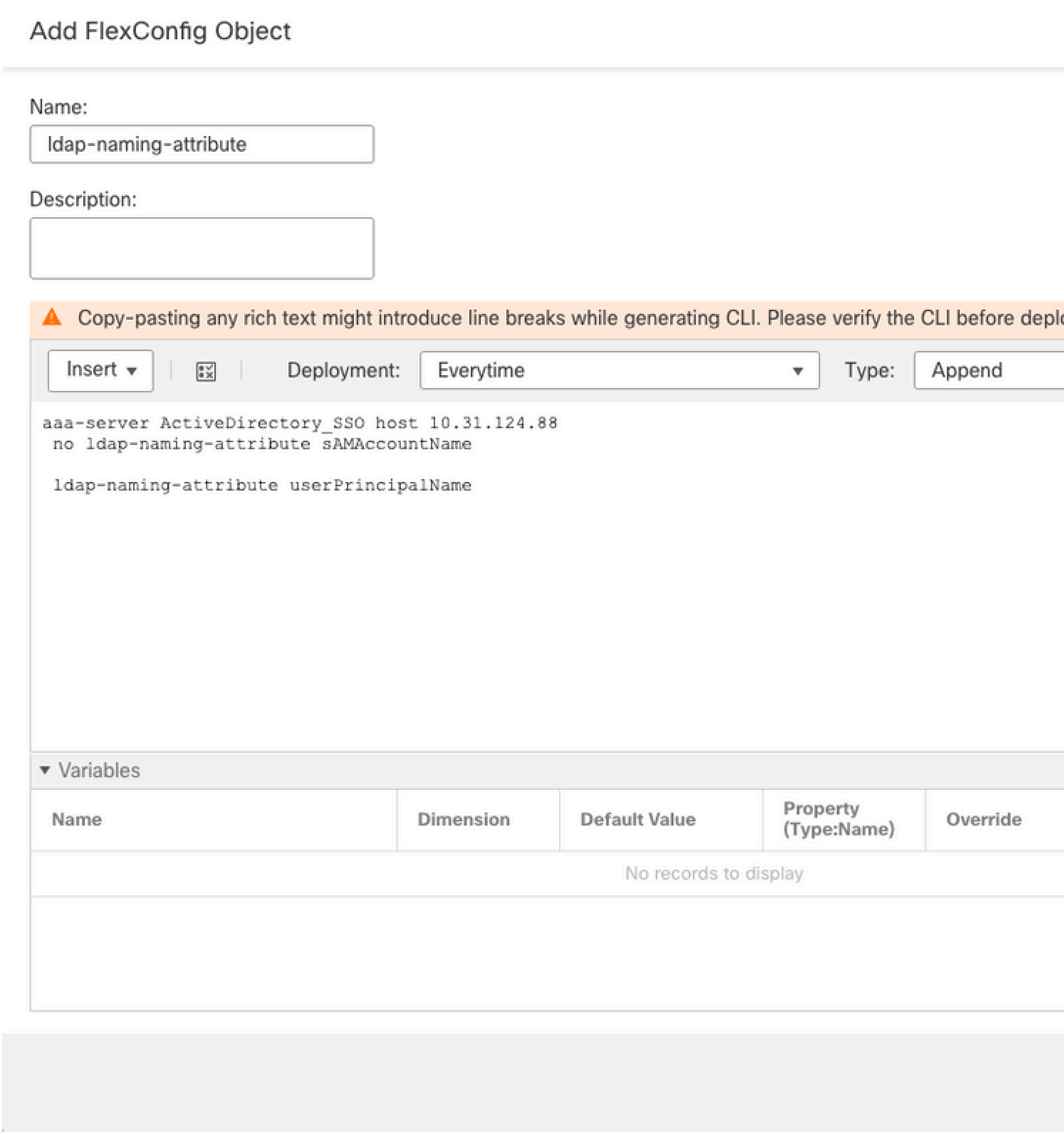
LDAP Attribute Name: memberOf

Cisco Attribute Name: Group-Policy

Value Maps:

LDAP Attribute Value

Cisco Attribute Value



Add FlexConfig Object

Name: ldap-naming-attribute

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before depl

Deployment: Everytime

Type: Append

```
aaa-server ActiveDirectory_SSO host 10.31.124.88
 no ldap-naming-attribute sAMAccountName

 ldap-naming-attribute userPrincipalName
```

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Add FlexConfig Object

- Click **Save**.

Step 8. Navigate to Deploy > Deployment and choose the proper FTD in order to apply the configuration.

Verify

From LDAP debug snippet debug ldap 255, it can be observed that there is a match on the LDAP Attribute Map for **Admin User**:

```
[26] LDAP Search:
```

Tunnel Group : SSO_AD_Split-tunnel Login Time : 19:37:28 UTC Thu Jul 20 2023 Duration : 0h:01m:33s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a1f7c490000600064b98cf8 Security Grp : none Tunnel Zone : 0. From LDAP debug snippet debug ldap 255, it can be observed that there is a match on the LDAP Attribute Map for **Test User**:

<#root>

```
[29] LDAP Search:
       Base DN = [DC=example,DC=com]
       Filter  = [

userPrincipalName=test_user@example.com

]
        Scope   = [SUBTREE]
<snipped>
[29]

memberOf: value = CN=AnyConnect Users,CN=Users,DC=example,DC=com

[29]

mapped to Group-Policy: value = SSO_LDAP_USERS

[29]

mapped to LDAP-Class: value = SSO_LDAP_USERS
```

Issue the show vpn-sessiondb anyconnect command in order to ensure that the user is in the correct group.

<#root>

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     :

test_user@example.com

Index        : 6
Public IP    : XX.XX.XX.XX
Protocol     : AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none
Hashing      : AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 0
Group Policy :

 SSO_LDAP_USERS

        Tunnel Group : SSO_AD_Split-tunnel
Login Time   : 19:37:28 UTC Thu Jul 20 2023
Duration     : 0h:08m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a1f7c490000600064b98cf8
Security Grp : none                   Tunnel Zone  : 0
```

From LDAP debug snippet debug ldap 255, it can be observed that there is no match on the LDAP Attribute Map for NOACCESS User and with debug webvpn that NO_ACCESS Group Policy is chosen, therefore, the user is unable to authenticate.

```
<#root>

[32] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter  = [

userPrincipalName=noaccess_user@example.com

]
        Scope   = [SUBTREE]
<snipped>
User Policy Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
tunnel policy attributes:
  1     Filter-Id(11)      8    ""
  2     Session-Timeout(27)      4    0
  3     Idle-Timeout(28)      4    30
  4     Simultaneous-Logins(4098)      4    0
  5     Primary-DNS(4101)      4    IP: 0.0.0.0
  6     Secondary-DNS(4102)      4    IP: 0.0.0.0
  7     Primary-WINS(4103)      4    IP: 0.0.0.0
  8     Secondary-WINS(4104)      4    IP: 0.0.0.0
  9     Tunnelling-Protocol(4107)      4    96
 10     Banner(4111)      0    0x000014e304401888   ** Unresolved Attribute **
 11     Group-Policy(4121)      9

 "NO_ACCESS"
```

Troubleshoot

Most SAML troubleshooting involves a misconfiguration which can be found by checking the SAML configuration or debugs:

- debug webvpn saml 255
- debug webvpn 255
- debug webvpn anyconnect 255
- debug webvpn session 255
- debug webvpn request 255

For LDAP mapping authorization issues the useful debugs are:

- debug aaa common 255
- debug ldap 255

Related information

- For additional assistance, please contact TAC. A valid support contract is required:Cisco Worldwide Support Contacts
- You can also visit the Cisco VPN Communityhere.

- Cisco Technical Support & Downloads