Configure Static IP Address Assignment for Secure Client VPN Users

Contents

Introduction

This document describes how to assign static IP addresses to Remote Access VPN users by using an LDAP attribute map.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center

Components Used

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

- Windows Server 2022
- FTD version 7.4.2
- FMC version 7.4.2

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.

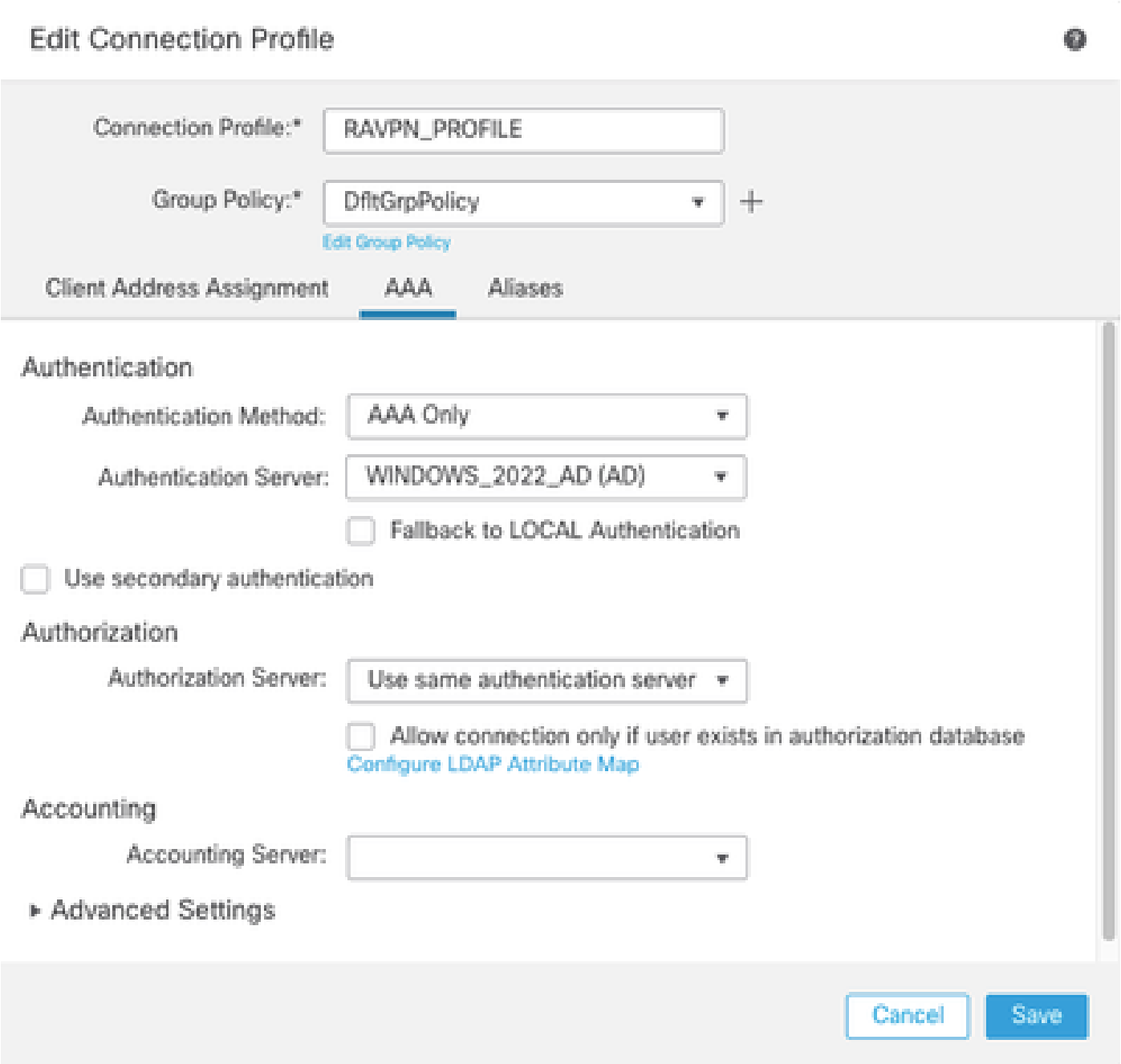
Background Information

Note: The option to use a Realm for IP address assignment and to configure LDAP attribute maps is supported in firepower version 6.7 or later. Ensure that the firepower version is 6.7 or later before you

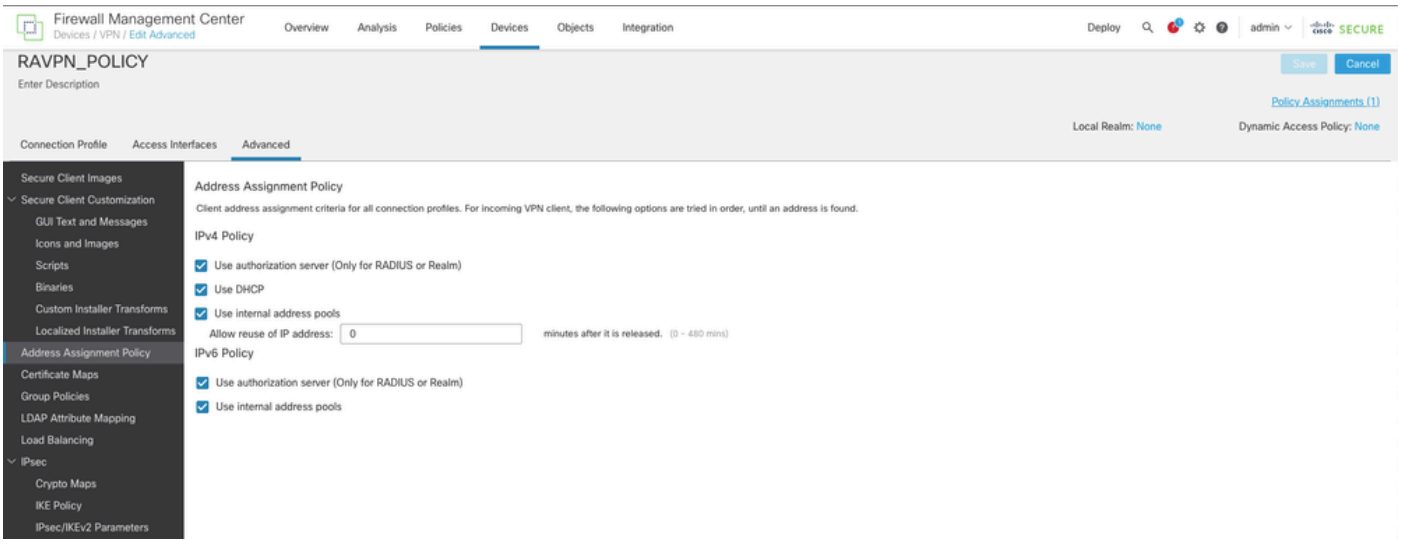
proceed.

Configure

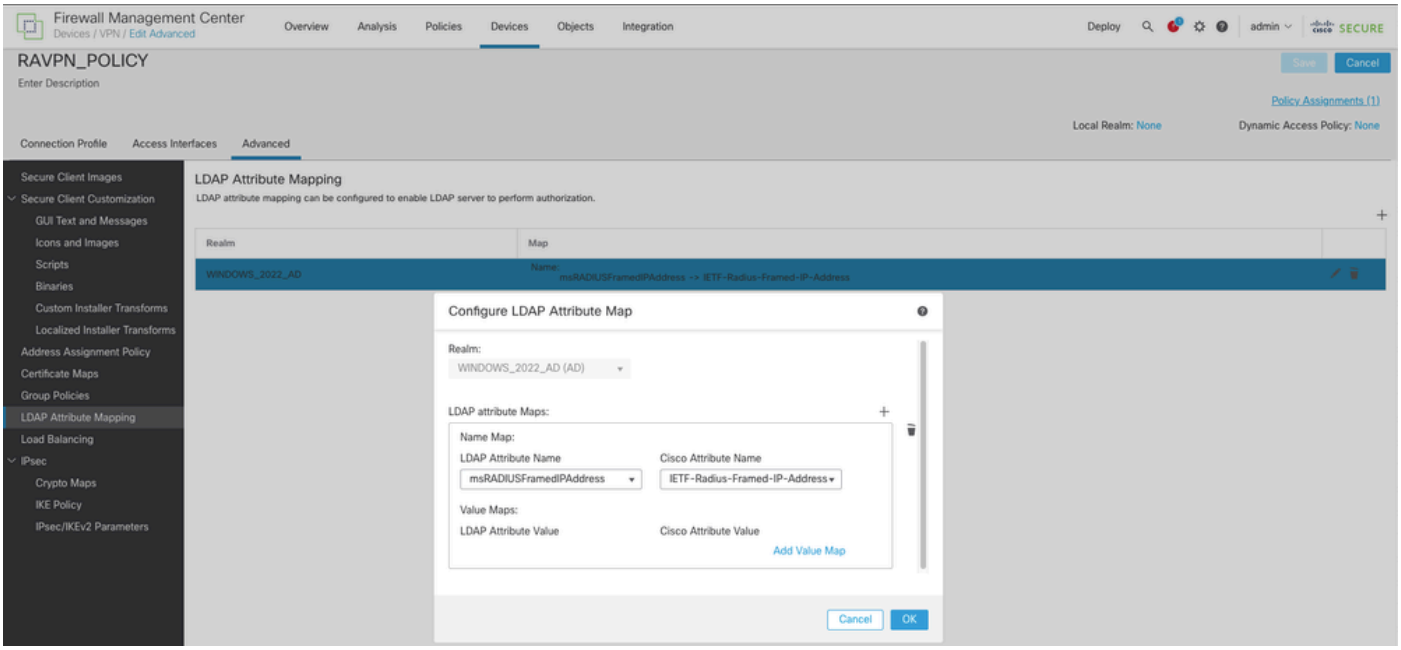
Step 1. Navigate to **Devices** > **Remote Access** and select the desired **Remote Access VPN Policy**. Select the desired **Connection Profile**. Under the **AAA** tab, select a Realm for **Authentication Server** and **Authorization Server**.



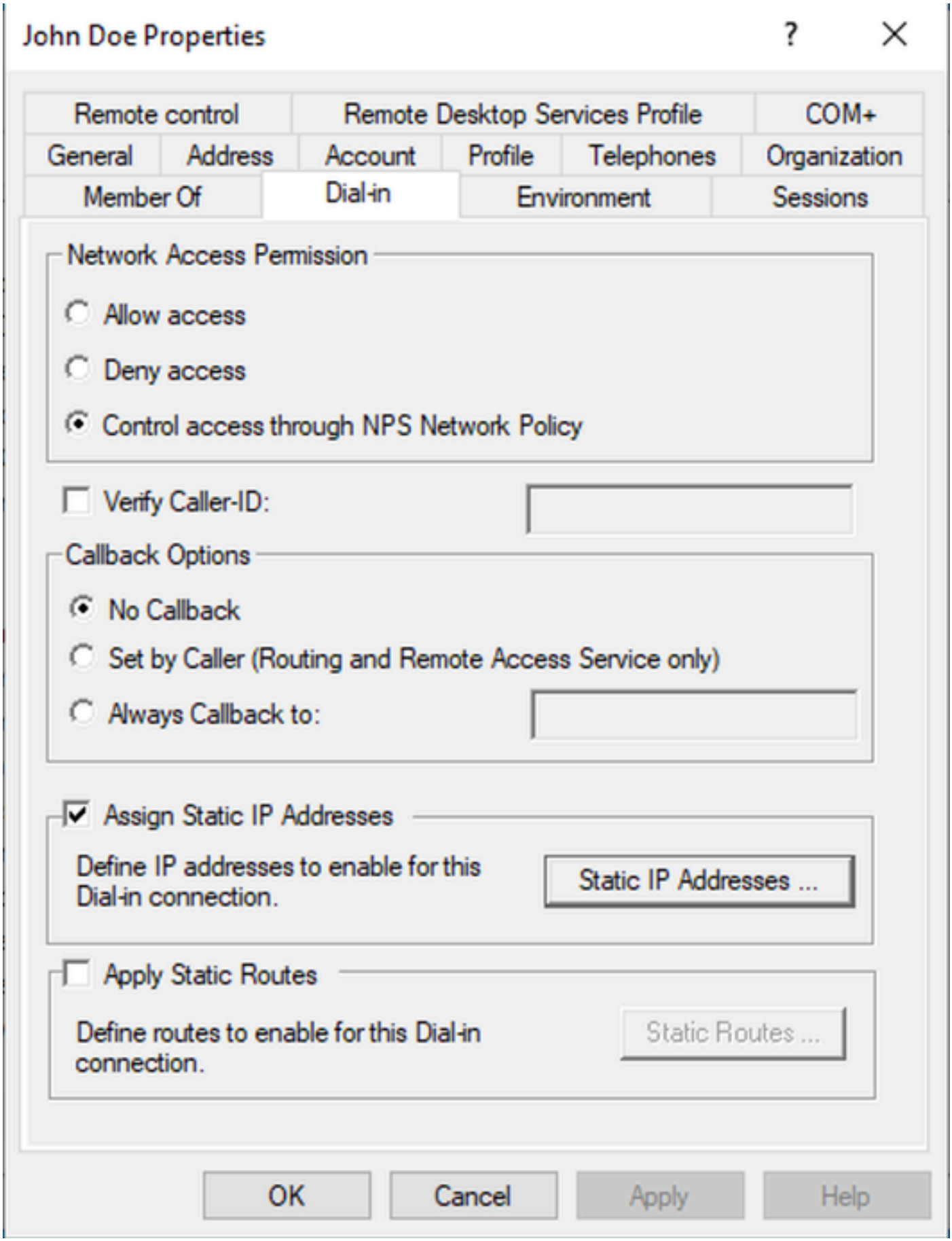
Step 2. Navigate to **Devices** > **Remote Access** and select the desired Remote Access VPN policy. Navigate to **Advanced** > **Address Assignment Policy** and ensure the option **Use authorization server (Only for RADIUS or Realm)** is enabled.



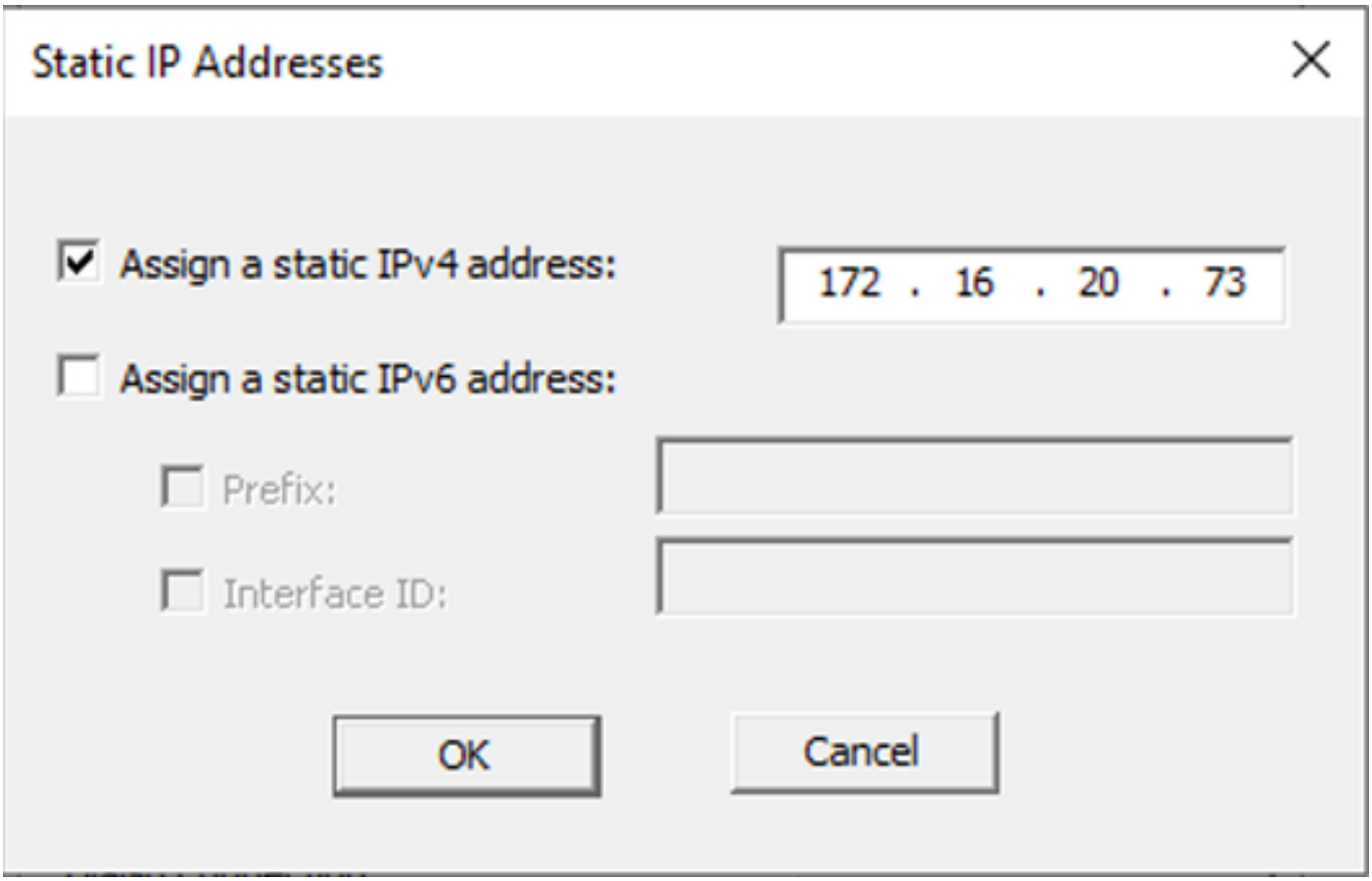
Step 3. Navigate to **Advanced > LDAP Attribute Mapping** and add a **Name Map** with **LDAP Attribute Name** set to **msRADIUSFramedIPAddress** and **Cisco Attribute Name** set to **IETF-Radius-Framed-IP-Address**.



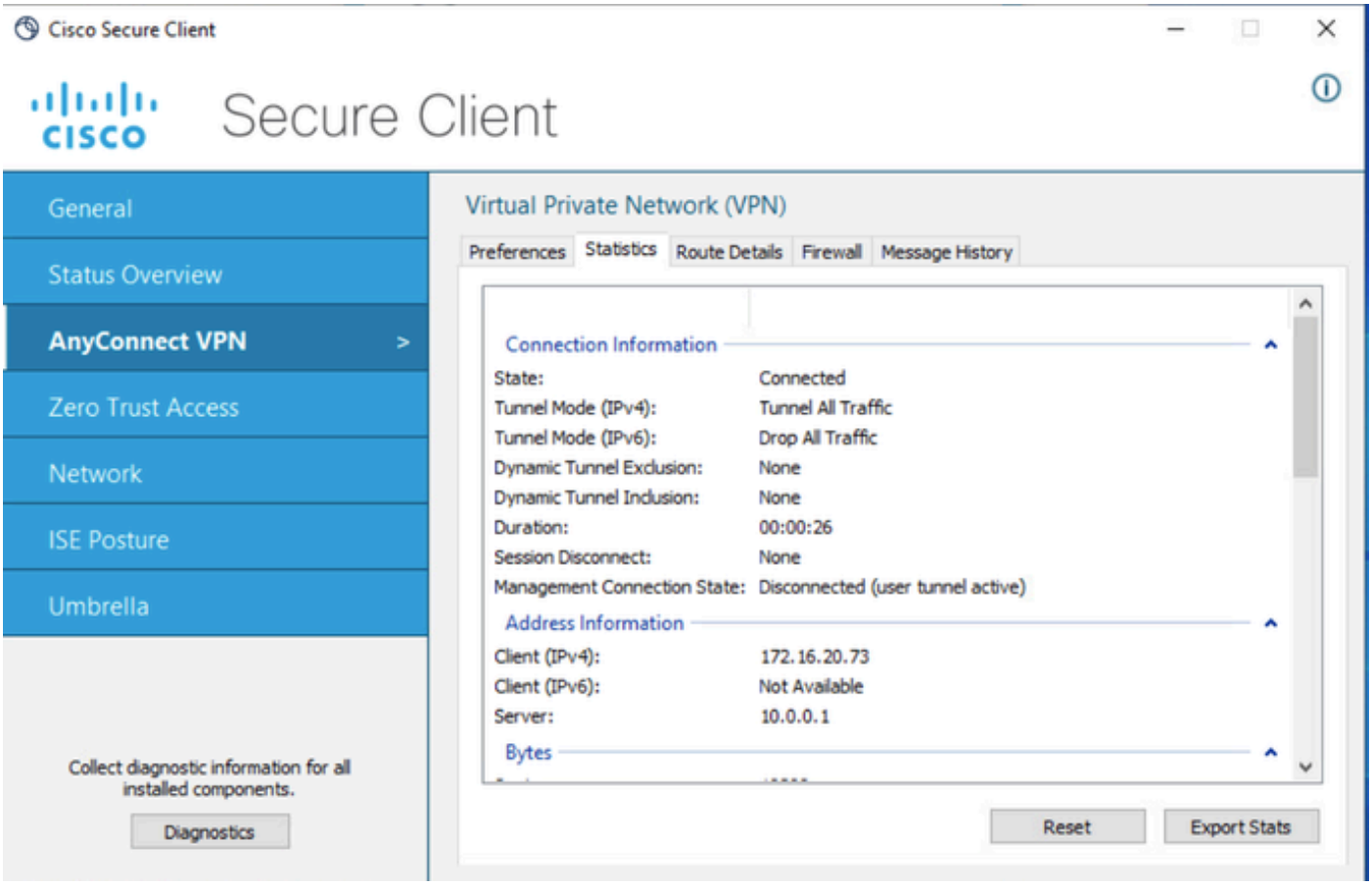
Step 4. On your Windows AD server, open **Server Manager** and navigate to **Tools > Active Directory Users and Computers**. Right-click on a **user**, select **Properties > Dial-in** and check the box named **Assign Static IP Addresses**.



Step 5. Select **Static IP Addresses** and assign a **static IP address** to the user.



Step 6. Connect to the VPN gateway and log in using the Cisco Secure Client. The user is assigned the static IP address that you configured.



Verify

Enable **debug ldap 255** and ensure that the **msRADIUSFramedIPAddress** LDAP attribute is retrieved:

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = ......fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = ............Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
```

```
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dSCorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

Troubleshoot

Debug commands:

debug webvpn 255

debug ldap

Command to validate the static IP address assigned to the desired RA VPN user:

show vpn-sessiondb anyconnect filter name <username>

<#root>

```
firepower#
```

```**show vpn-sessiondb anyconnect filter name jdoe**
```

```
Session Type: AnyConnect

Username : jdoe Index : 7
Assigned IP : 172.16.20.73 Public IP : 10.0.0.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14664 Bytes Rx : 26949
Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE
Login Time : 11:45:48 UTC Sun Sep 29 2024
Duration : 0h:38m:59s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000700066f93dec
Security Grp : none Tunnel Zone : 0
```