

# Statische IP-adrestoewijzing voor beveiligde client-VPN-gebruikers configureren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

---

## Inleiding

Dit document beschrijft hoe statische IP-adressen aan externe VPN-gebruikers kunnen worden toegewezen door gebruik te maken van een LDAP-kenmerkkaart.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Active Directory (AD)
- Lichtgewicht Directory Access Protocol (LDAP)
- Cisco Secure Firewall-bescherming tegen bedreigingen
- Cisco Secure Firewall Management Center


### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows Server 2022
- FTD versie 7.4.2
- FMC versie 7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

 **Opmerking:** De optie om een Realm voor IP-adrestoewijzing te gebruiken en LDAP attribut maps te configureren wordt ondersteund in FirePOWER versie 6.7 of hoger. Zorg ervoor dat de FirePOWER-versie 6.7 of hoger is voordat u verdergaat.

## Configureren

Stap 1. Navigeer naar Apparaten > Externe toegang en selecteer het gewenste VPN-beleid voor externe toegang. Selecteer het gewenste verbindingsprofiel. Selecteer onder het tabblad AAA een Realm voor verificatieserver en autorisatieserver.

### Edit Connection Profile ?

Connection Profile:\*

Group Policy:\*  +  
[Edit Group Policy](#)

Client Address Assignment   **AAA**   Aliases

#### Authentication

Authentication Method:

Authentication Server:   
 Fallback to LOCAL Authentication

Use secondary authentication

#### Authorization

Authorization Server:

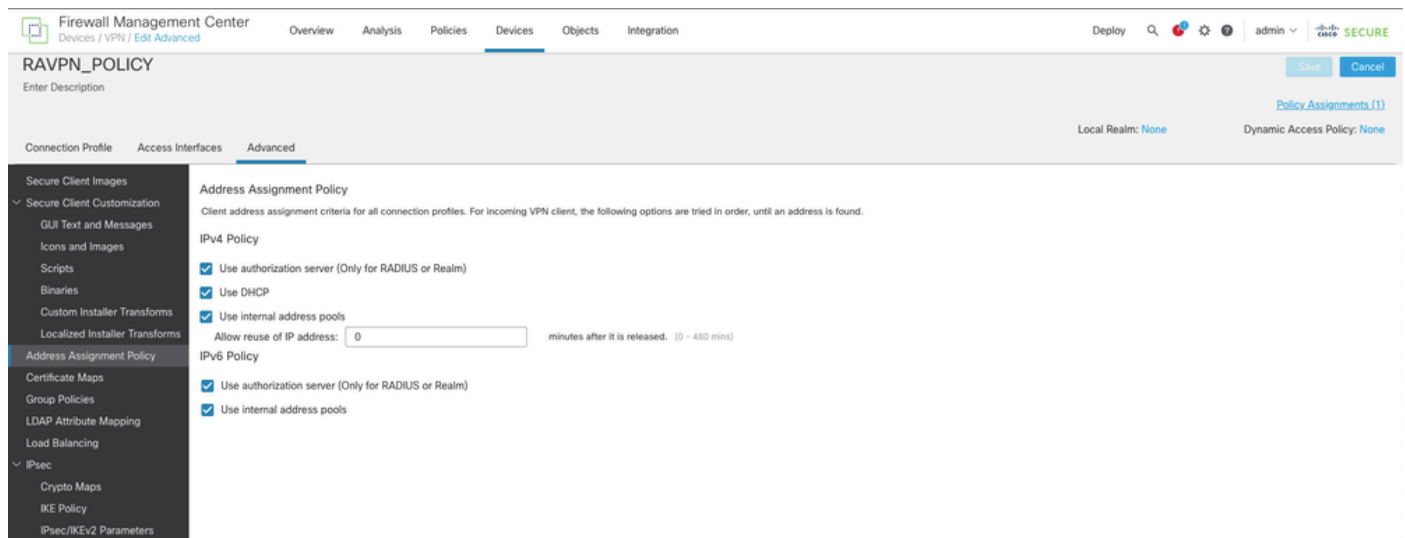
Allow connection only if user exists in authorization database  
[Configure LDAP Attribute Map](#)

#### Accounting

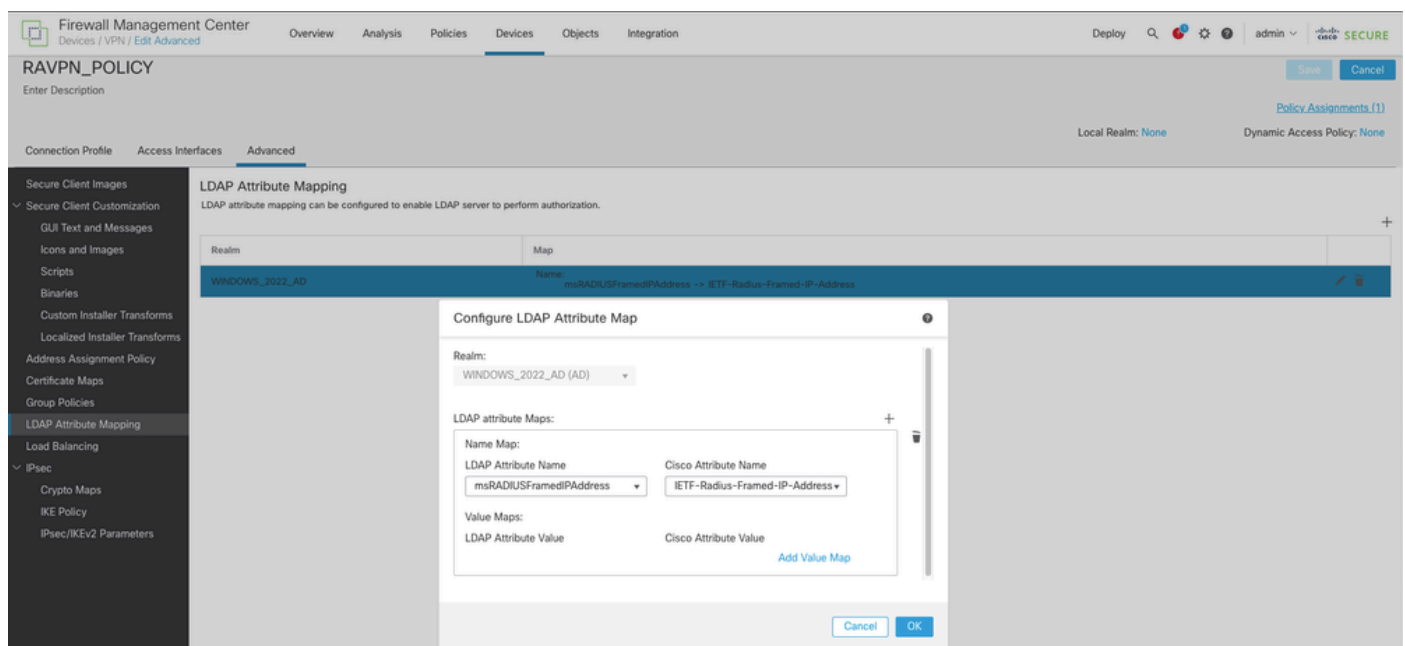
Accounting Server:

▶ Advanced Settings

Stap 2. Navigeer naar Apparaten > Externe toegang en selecteer het gewenste Remote Access VPN-beleid. Navigeer naar Advanced > Address Assignment Policy en controleer of de optie Use autorisatieserver (Alleen voor RADIUS of Real) is ingeschakeld.



Stap 3. Navigeer naar Geavanceerd > Toewijzing van LDAP-kenmerken en voeg een Naamkaart toe waarvan de naam van LDAP-kenmerken is ingesteld op msRADIUSFramedIPAddress en de naam van Cisco-kenmerken is ingesteld op IETF-Radius-Framed-IP-Address.



Stap 4. Open Server Manager op uw Windows AD-server en navigeer naar Tools > Active Directory-gebruikers en computers. Klik met de rechtermuisknop op een gebruiker, selecteer Eigenschappen > Inbellen en controleer het vakje Statische IP-adressen toewijzen.

# John Doe Properties



Remote control

Remote Desktop Services Profile

COM+

General

Address

Account

Profile

Telephones

Organization

Member Of

Dial-in

Environment

Sessions

Network Access Permission

- Allow access
- Deny access
- Control access through NPS Network Policy

Verify Caller-ID:

Callback Options

- No Callback
- Set by Caller (Routing and Remote Access Service only)
- Always Callback to:

Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

Static IP Addresses ...

Apply Static Routes

Define routes to enable for this Dial-in connection.

Static Routes ...

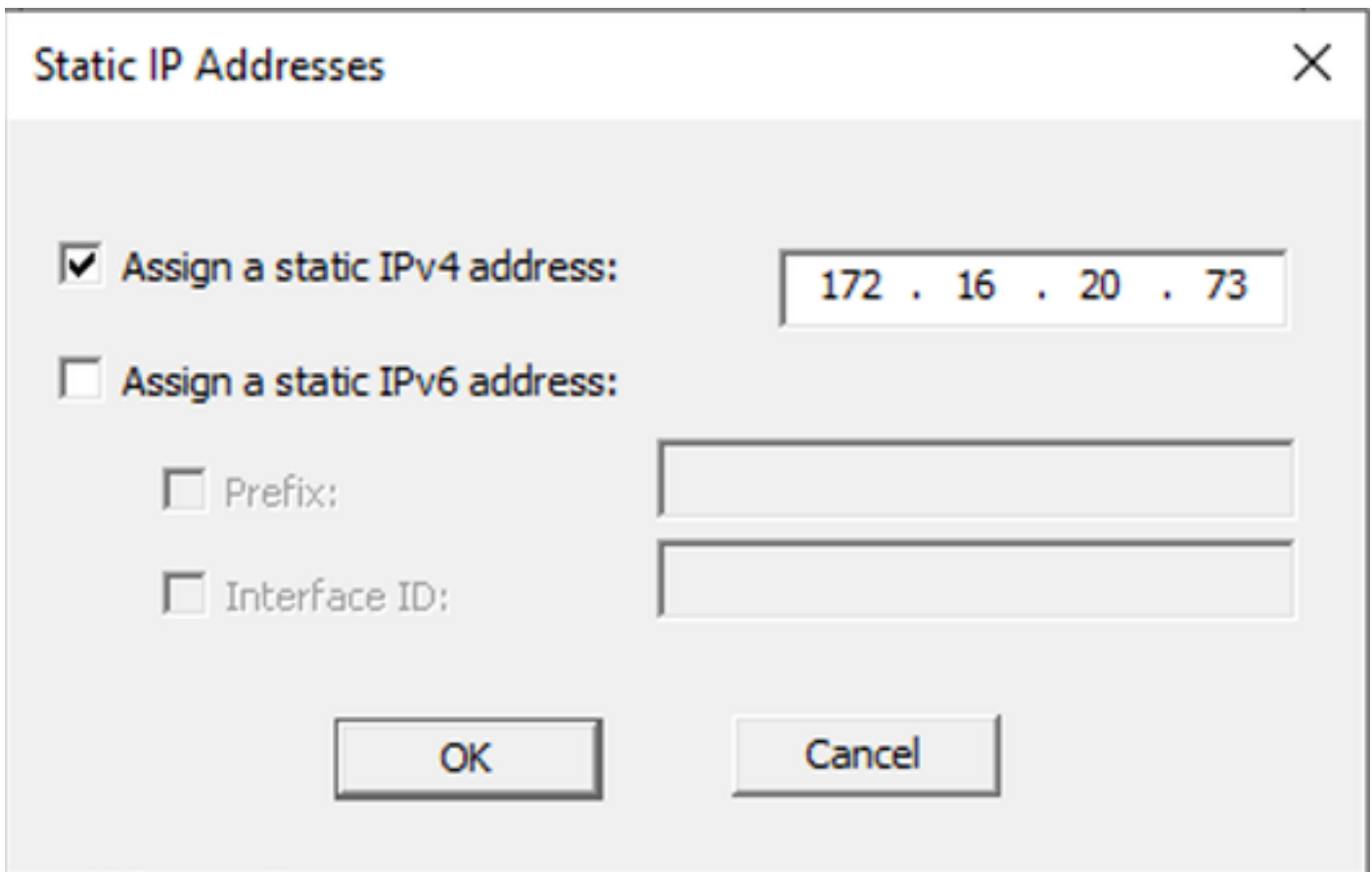
OK

Cancel

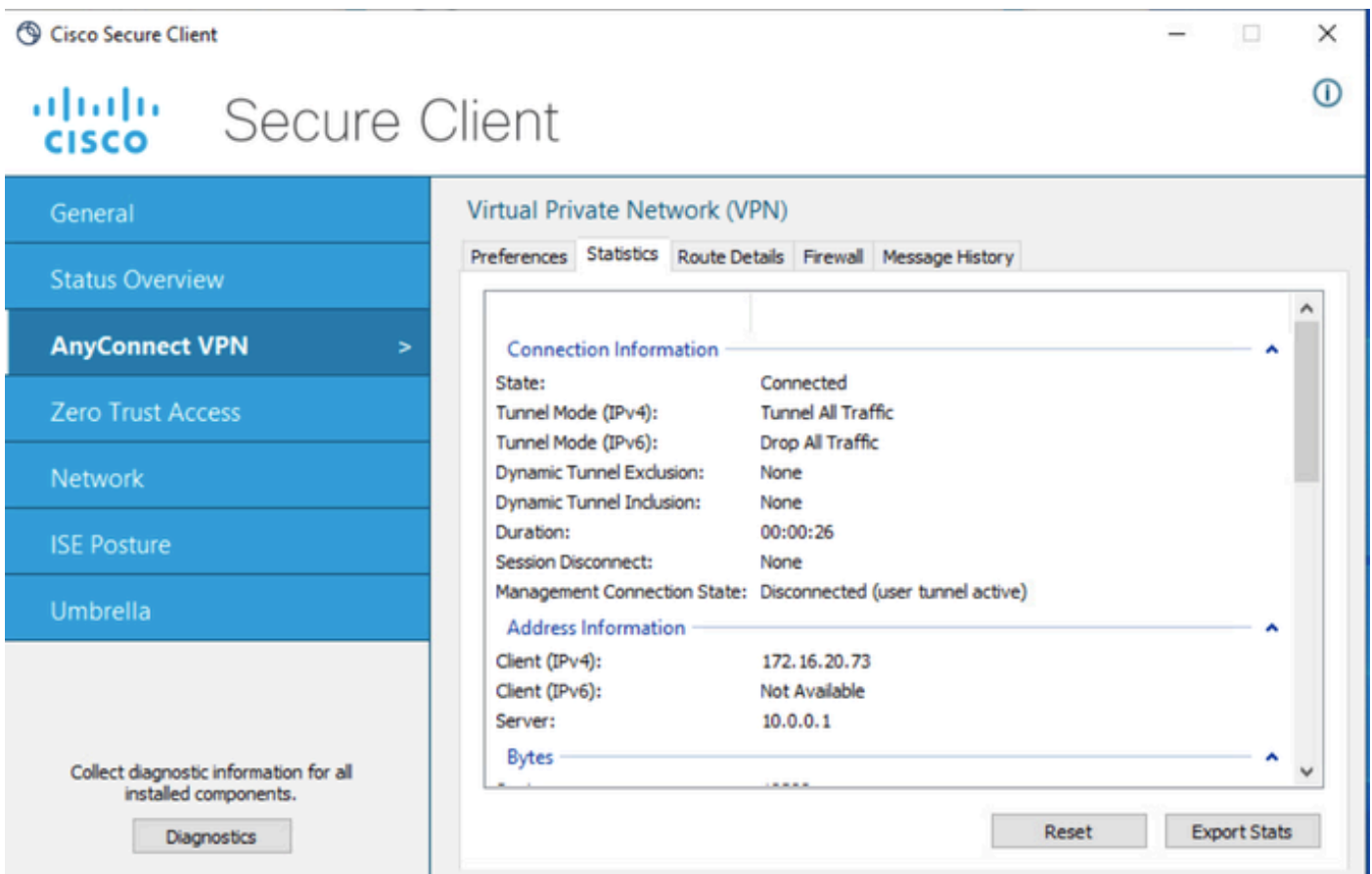
Apply

Help

Stap 5. Selecteer Statische IP-adressen en wijs een statisch IP-adres aan de gebruiker toe.



Stap 6. Maak verbinding met de VPN-gateway en log-in met de Cisco Secure-client. De gebruiker krijgt het statische IP-adres toegewezen dat u hebt geconfigureerd.



# Verifiëren

Schakel debug ldap 255 in en controleer of het kenmerk msRADIUSFramedIPAddress LDAP wordt opgehaald:

```
[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
```

## Problemen oplossen

Opdrachten voor debugging:

debug webvpn 255

debug ladder

Opdracht om het statische IP-adres te valideren dat is toegewezen aan de gewenste RA VPN-gebruiker:

toon vpn-sessiondb om het even welke verbindingfilternaam <gebruikersnaam>

```
<#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
```

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.