RNA VPN configureren met LDAP-verificatie en -autorisatie voor FTD

Inhoud

Inleiding

Dit document beschrijft hoe u Remote Access VPN kunt configureren met LDAP AA op een Firepower Threat Defence (FTD) die wordt beheerd door een Firepower Management Center.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van werken met Remote Access VPN (RA VPN).
- Ga op de hoogte van navigatie via het Firepower Management Center (FMC).
- Configuratie van Lichtgewicht Directory Access Protocol (LDAP)-services op Microsoft Windows Server.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Firepower Management Center versie 7.3.0
- Cisco Firepower Threat Defense versie 7.3.0
- Microsoft Windows Server 2016, geconfigureerd als LDAP-server

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

Dit document beschrijft de configuratie van Remote Access VPN (RA VPN) met LDAP-verificatie (Lichtgewicht Directory Access Protocol) en autorisatie op een Firepower Threat Defence (FTD) die wordt beheerd door een Firepower Management Center (FMC).

LDAP is een open, leverancier-neutraal, industrie-standaardtoepassingsprotocol om tot de gedistribueerde indexinformatiediensten toegang te hebben en te handhaven.

Een LDAP attributenkaart vergelijkt attributen die in de Active Directory (AD) of LDAP server bestaan met de attributennamen van Cisco. Vervolgens kan het FTD-apparaat, wanneer de AD- of LDAP-server de verificatiereacties op het FTD-apparaat retourneert tijdens een instelling voor externe VPN-verbindingen, de informatie gebruiken om aan te passen hoe de AnyConnect-client de verbinding voltooit.

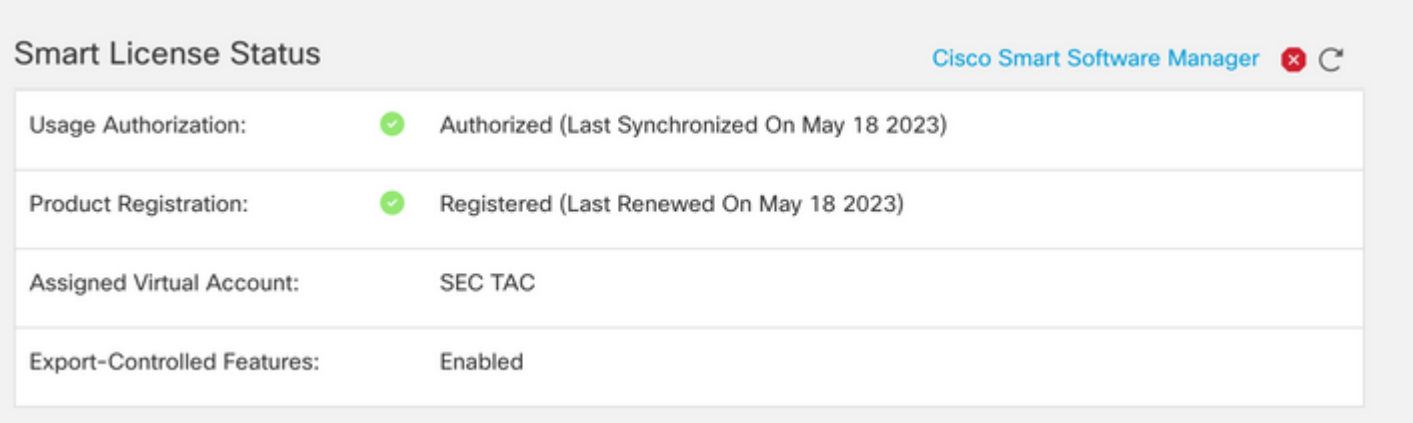
RA VPN met LDAP-verificatie is ondersteund op het VCC sinds versie 6.2.1 en LDAP-autorisatie voorafgaand aan FMC versie 6.7.0 werd geadviseerd via FlexConfig om LDAP Attribute Map te configureren en deze te koppelen aan de Real Server. Deze optie, met versie 6.7.0, is nu geïntegreerd met de RA VPN-configuratiewizard op het VCC en vereist geen gebruik meer van FlexConfig.

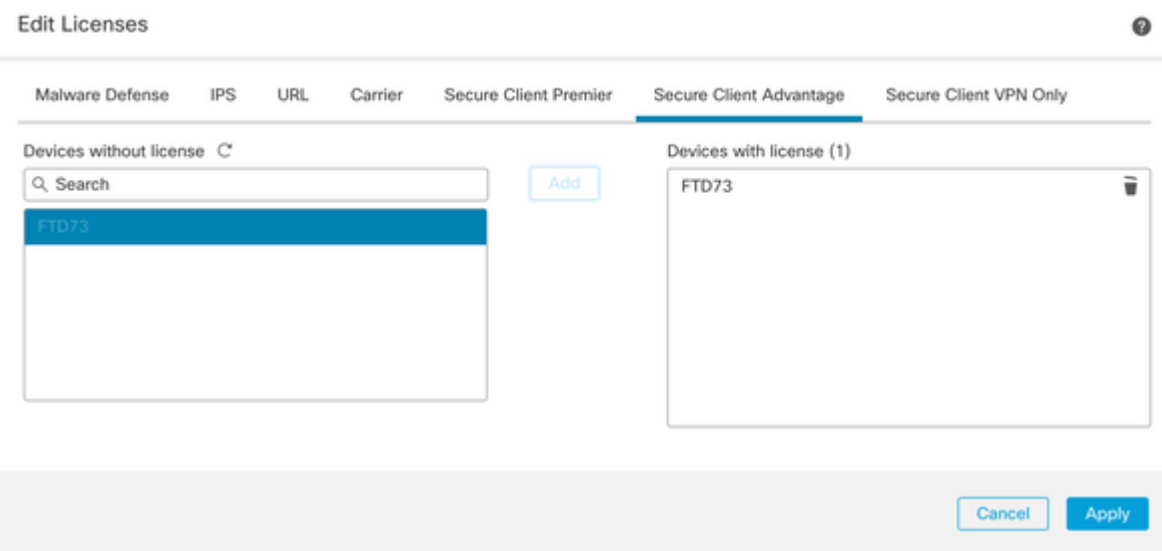
> **NB:** Voor deze functie moet het VCC versie 6.7.0 hebben; het beheerde VCC kan op elke versie hoger zijn dan 6.3.0.

Licentievereisten

Vereist AnyConnect Apex, AnyConnect Plus of AnyConnect VPN Only-licentie met exportgestuurde functionaliteit.

Als u de licentie wilt controleren, navigeer dan naar **System > Licenses > Smart Licenses.**



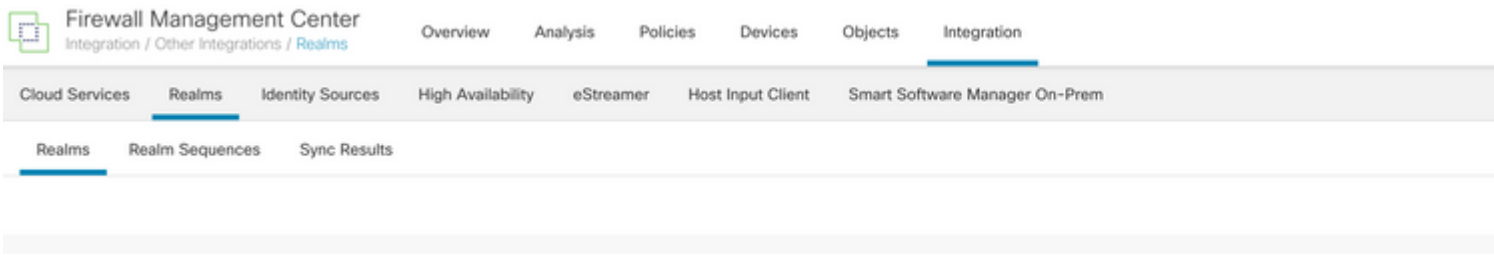


Configuratiestappen op FMC

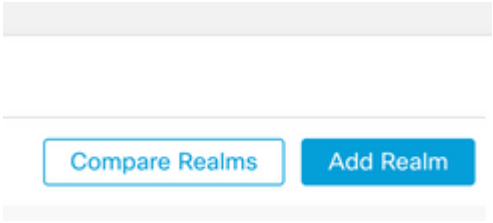
Configuratie van REALM/LDAP-server

> **Opmerking:** de genoemde stappen zijn alleen vereist als het gaat om de configuratie van een nieuwe REALM / LDAP-server. Als u een vooraf ingestelde server hebt, die kan worden gebruikt voor verificatie in RA VPN, navigeer dan naar RA VPN Configuration.

Stap 1. Naar navigeren System > Other Integrations > Realms, zoals in deze afbeelding wordt getoond.



Stap 2. Zoals in de afbeelding, klikt u op **Add a new realm.**



Stap 3. Geef de details van de AD-server en de directory. Klik OK.

Voor deze demonstratie:

Naam: LDAP

Type: AD

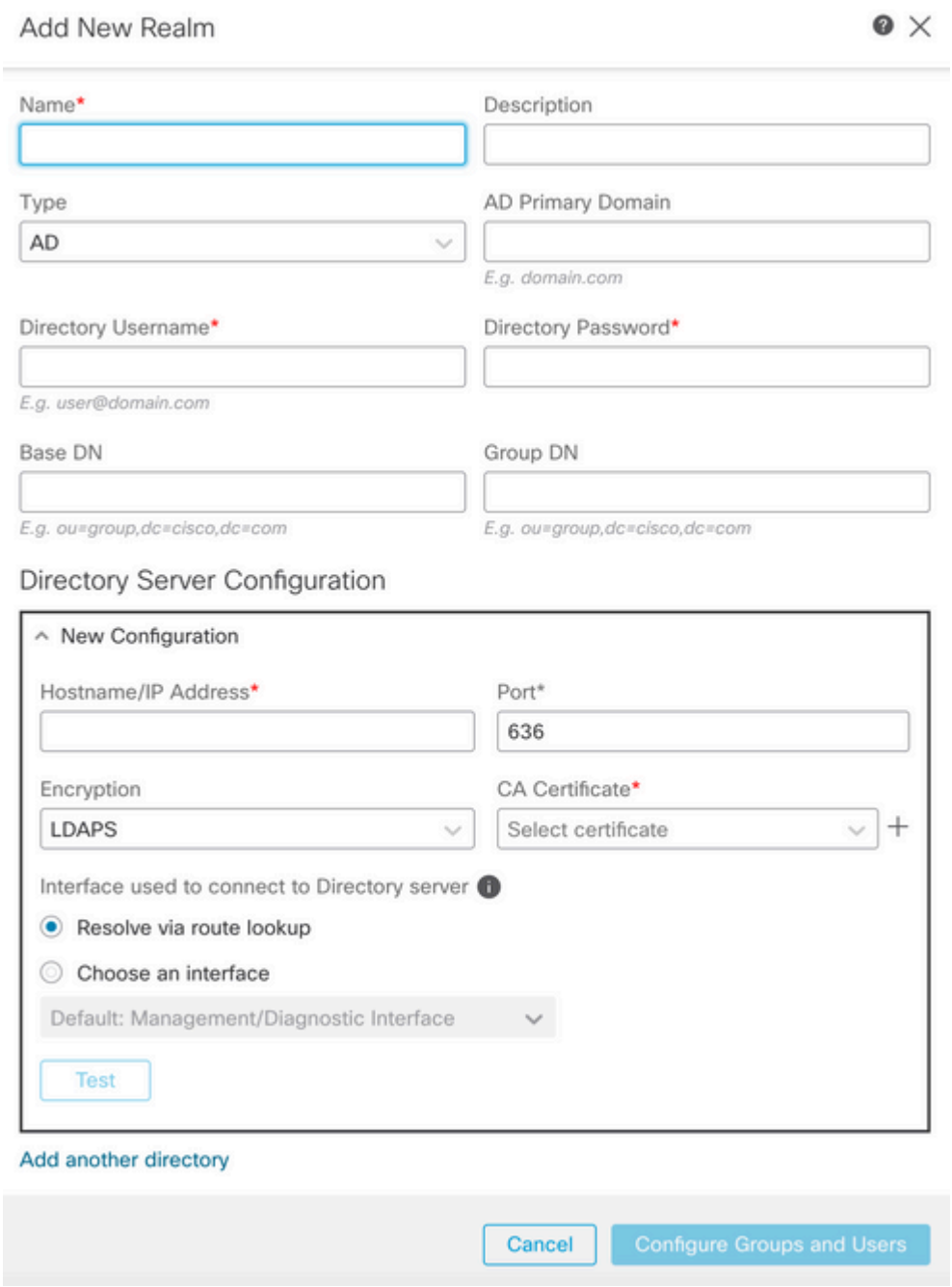
AD Primair domein: test.com

Gebruikersnaam voor map: CN=Administrator, CN=users, DC=test, DC=com

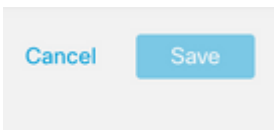
Directory Wachtwoord: <Hidden>

Base-DN: DC=test, DC=com

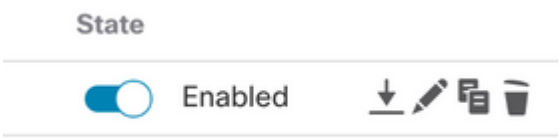
Groep DN: DC=test, DC=com



Stap 4. Klik Save om de wijzigingen in domein/map op te slaan, zoals in deze afbeelding wordt getoond.



Stap 5. Schakel de State om de status van de server te wijzigen in Ingeschakeld, zoals in deze afbeelding wordt weergegeven.

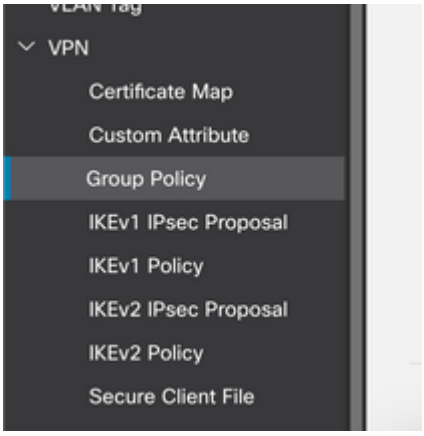


RA VPN-configuratie

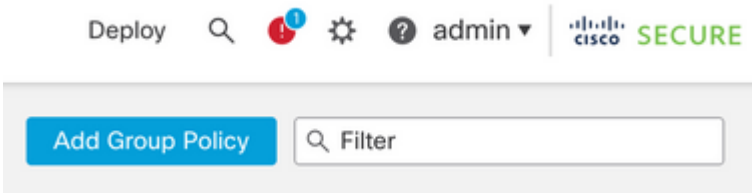
Deze stappen zijn nodig om het groepsbeleid te configureren, dat is toegewezen aan geautoriseerde VPN-gebruikers. Als het groepsbeleid al is gedefinieerd, gaat u naar Stap 5.

Stap 1. Naar navigeren Objects > Object Management.

Stap 2: Ga in het linkerdeelvenster naar VPN > Group Policy.



Stap 3: Klik op **Add Group Policy**.



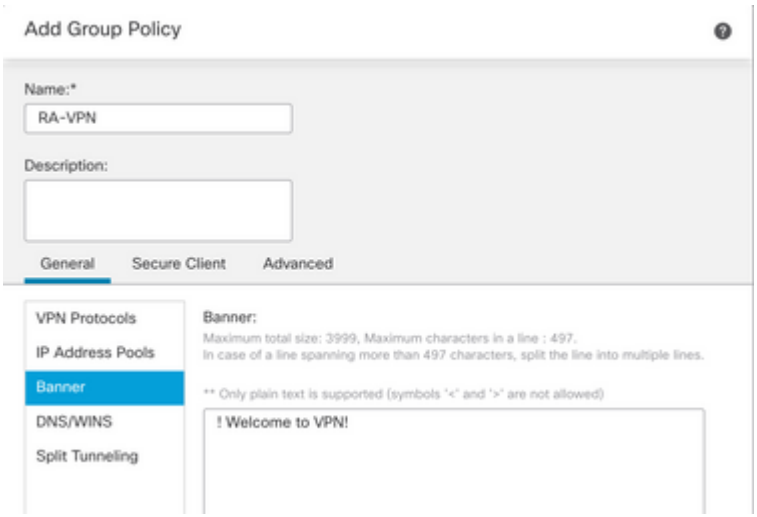
Stap 4: Verstrek de waarden van het Beleid van de Groep.

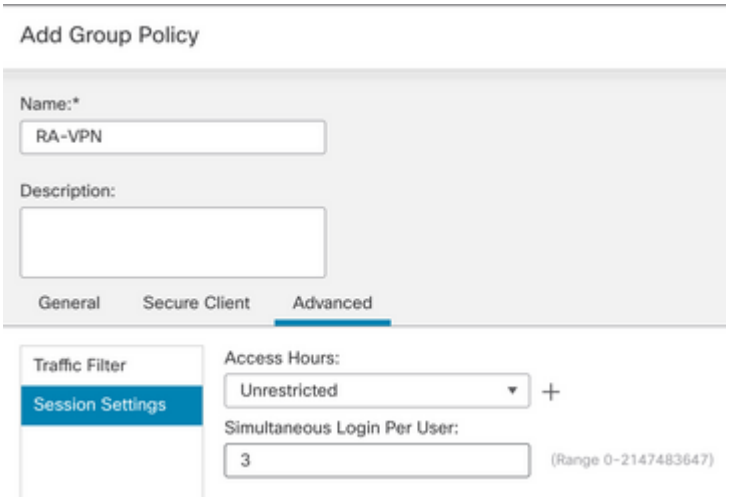
Voor deze demonstratie:

Naam: RA-VPN

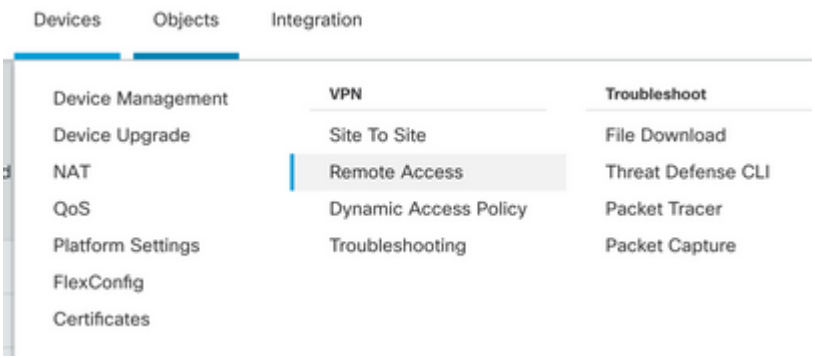
Banier: ! Welkom bij VPN!

Gelijktijdige aanmelding per gebruiker: 3 (standaard)

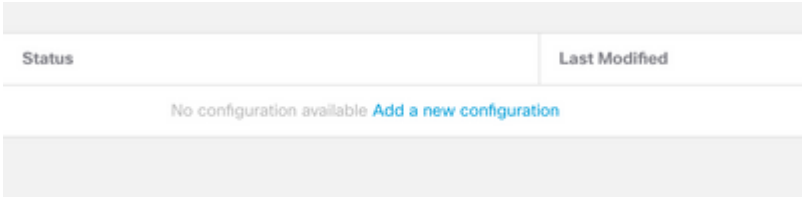




Stap 5. Naar navigeren Devices > VPN > Remote Access.



Stap 6. Klik **Add a new configuration.**



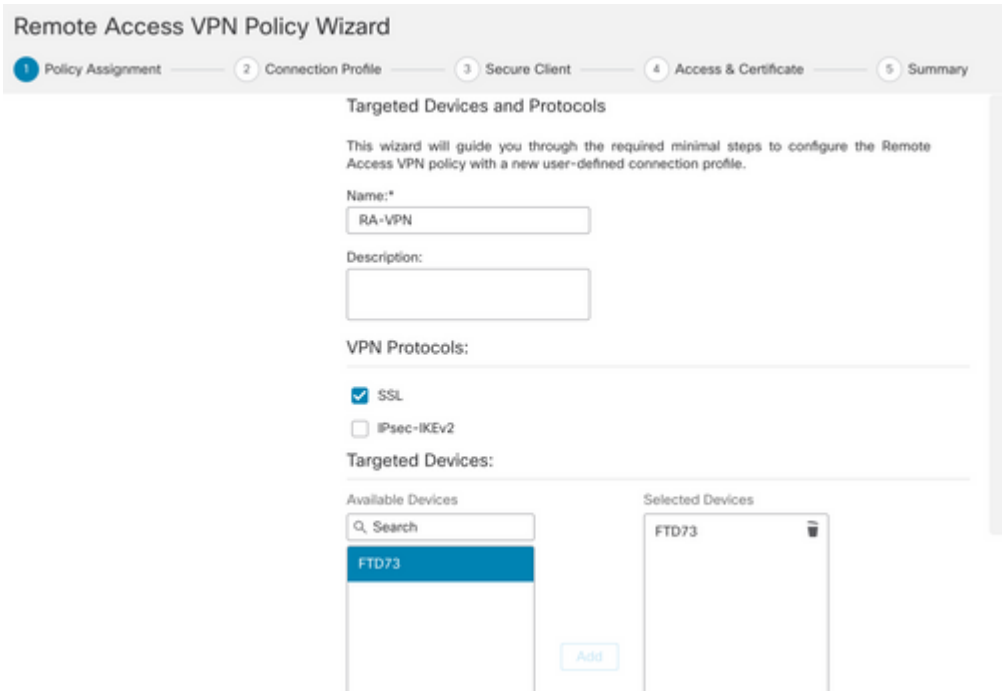
Stap 7. Een Name voor het RA VPN-beleid. Kiezen **VPN Protocols** en kiezen **Targeted Devices.** Klik **Next.**

Voor deze demonstratie:

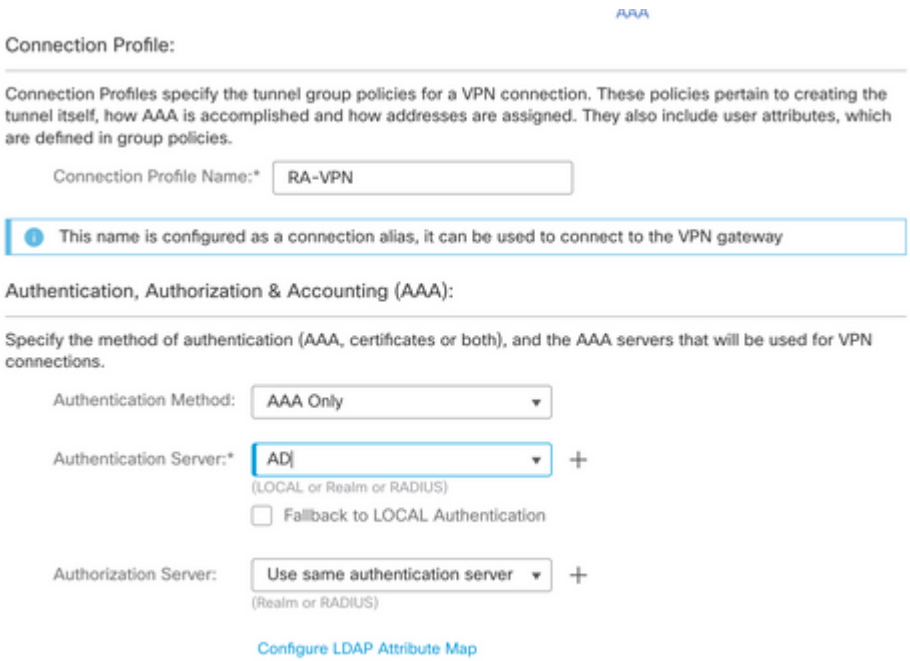
Naam: RA-VPN

VPN-protocollen: SSL

Gerichte apparaten: FTD



Stap 8. Voor de Authentication Method, kiezen **AAA Only**. Kies de REALM / LDAP server voor de Authentication Server. Klik **Configure LDAP Attribute Map** (om LDAP-autorisatie te configureren).

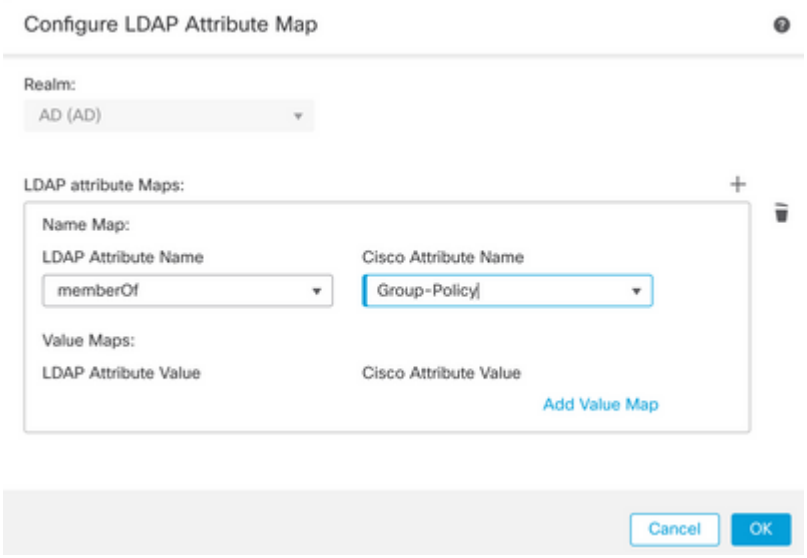


Stap 9. Geef de LDAP Attribute Name en de Cisco Attribute Name. Klik **Add Value Map**.

Voor deze demonstratie:

Naam van LDAP-kenmerk: memberOfI

Cisco-naam van kenmerk: groepsbeleid

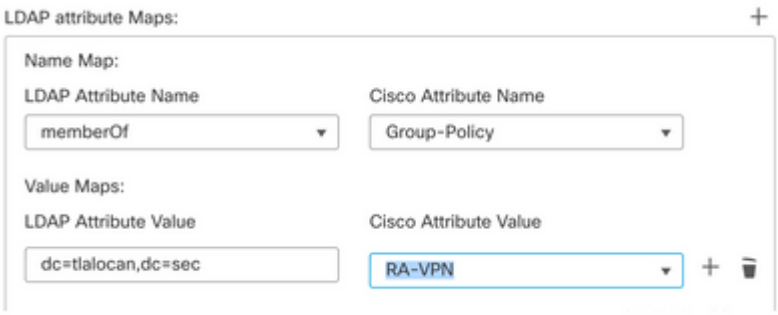


Stap 10. Geef de LDAP Attribute Value en de Cisco Attribute Value. Klik **OK**.

Voor deze demonstratie:

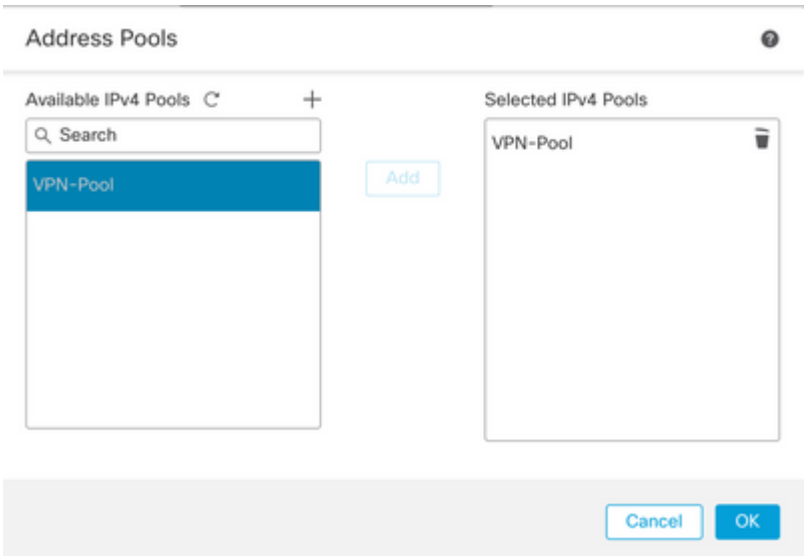
LDAP Attribute Value: DC=tlalocan,DC=sec

Cisco Attribute Value: RA-VPN



Opmerking: Je kunt meer Waardekaarten toevoegen volgens de vereiste.

Stap 11. Voeg het Address Pool voor de lokale adrestoewijzing. Klik **OK**.



Stap 12. Geef de **Connection Profile Name** en de Group-Policy. Klik Next.

Voor deze demonstratie:

Naam verbindingsprofiel: RA-VPN

Verificatiemethode: alleen AAA

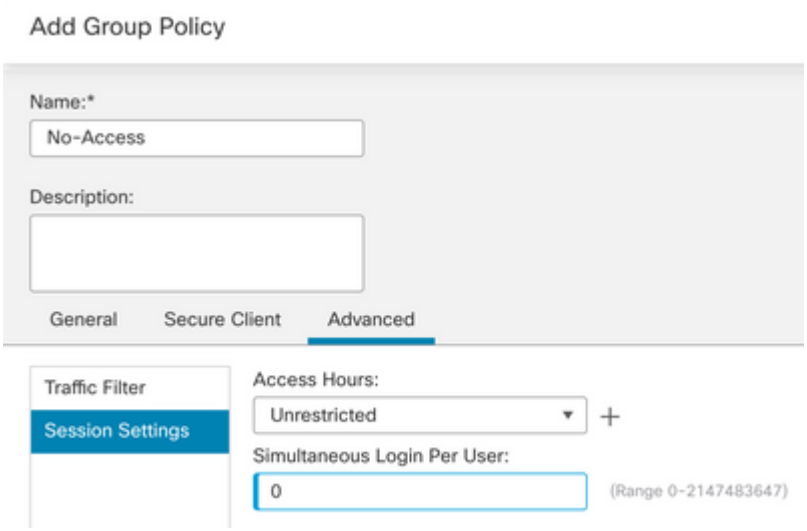
Verificatieserver: LDAP

IPv4-adresgroep: VPN-pool

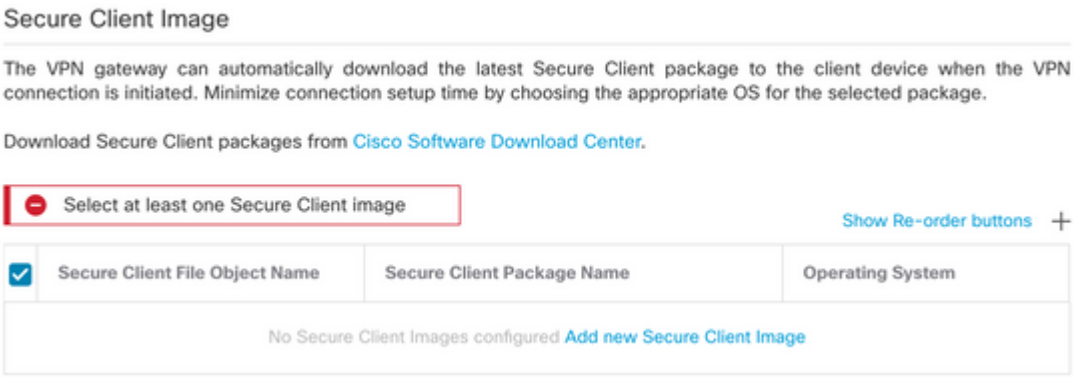
Groepsbeleid: geen toegang

> **Opmerking:** de **verificatiemethode**, **verificatieserver** en de IPV4-adresgroep zijn in de vorige stappen geconfigureerd.

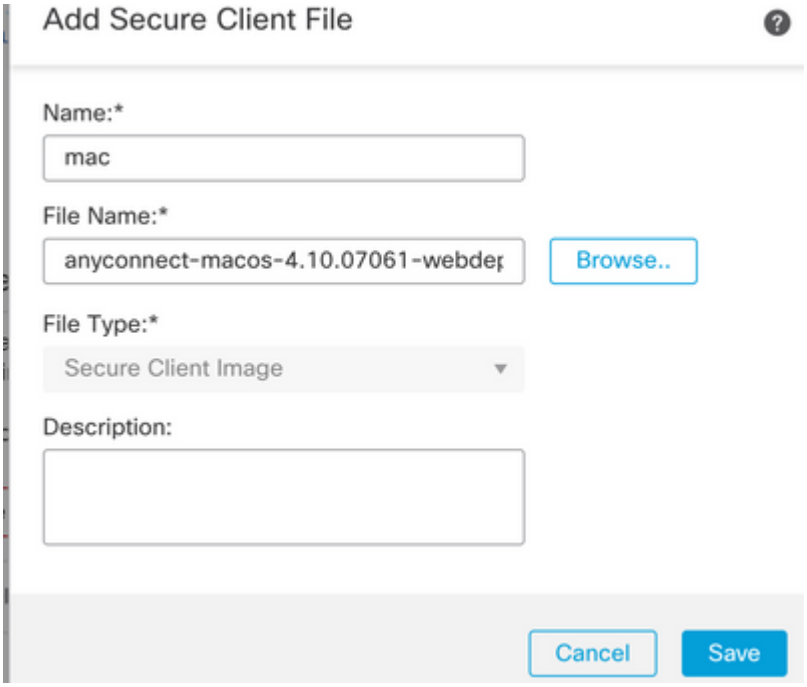
Het groepsbeleid zonder toegang heeft het volgende: Simultaneous Login Per User parameter ingesteld op 0 (om gebruikers niet in staat te stellen om in te loggen als ze het standaard geen-toegang groep-beleid ontvangen).



Stap 13. Klik Add new AnyConnect Image om een **AnyConnect Client Image** naar het FTD.



Stap 14. Een Name voor het geüploade image en blader vanuit het lokale opslagsysteem om het image te uploaden. Klik Save.



Stap 15. Klik op het aanvinkvakje naast de afbeelding om dit voor gebruik in te schakelen. Klik Next.

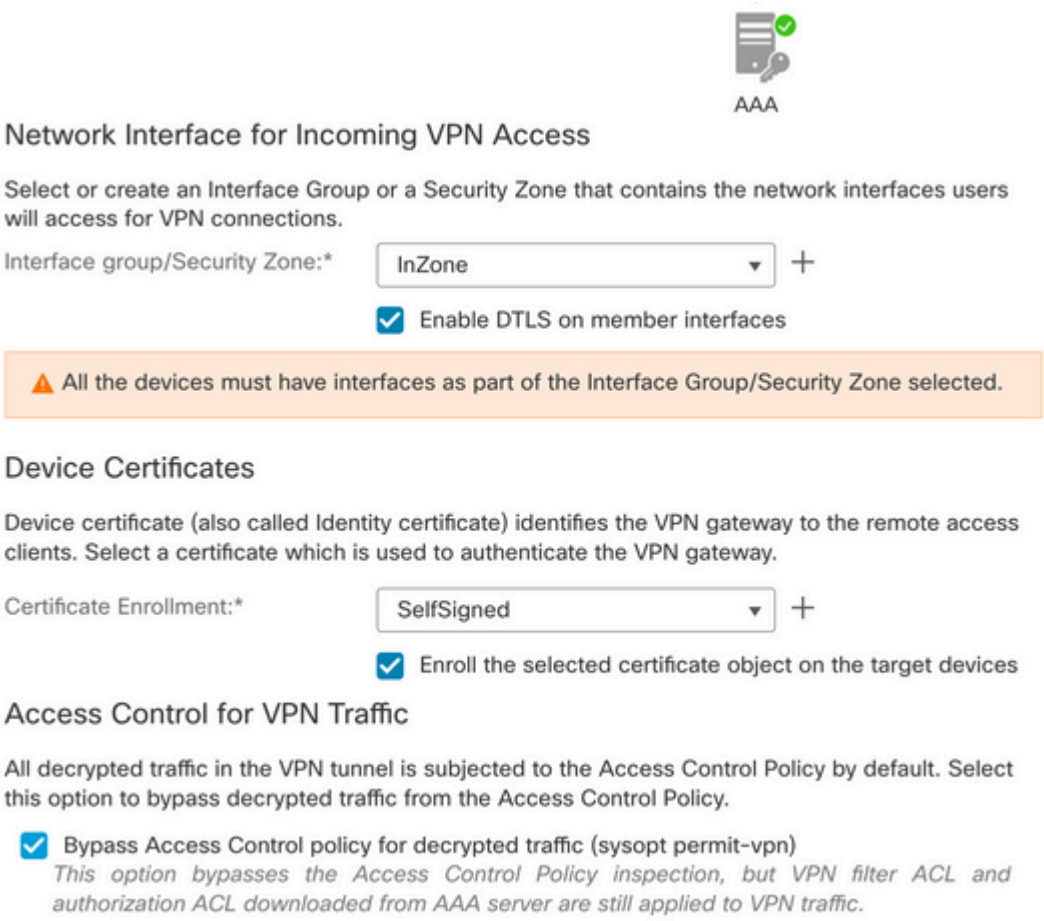
Stap 16. Kies de Interface group/Security Zone en de Device Certificate. Klik Next.

Voor deze demonstratie:

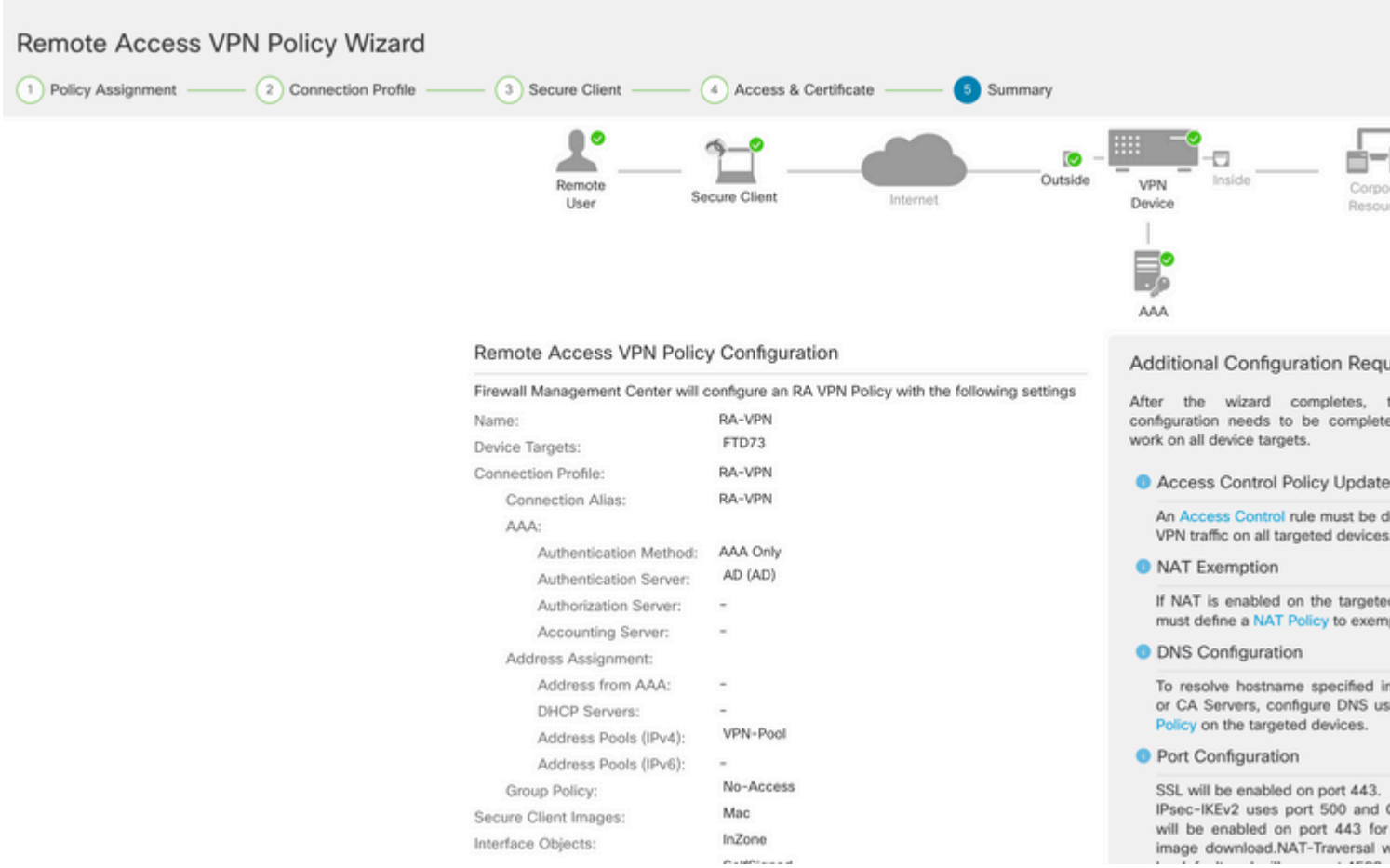
Interfacegroep/Security Zone: out-zone

Apparaatcertificaat: zelfondertekend

> **Opmerking:** u kunt ervoor kiezen de beleidsoptie Omzeilen voor toegangscontrole in te schakelen om elke toegangscontrole voor versleuteld (VPN) verkeer te omzeilen (standaard uitgeschakeld).



Stap 17. Bekijk de samenvatting van de RA VPN configuratie. Klik Finish om op te slaan, zoals in de afbeelding.



Stap 18. Naar navigeren Deploy > Deployment. Kies de FTD waarop de configuratie moet worden ingezet. Klik Deploy.

De configuratie wordt na een succesvolle implementatie naar de FTD CLI gedrukt:

<#root>

!--- LDAP Server Configuration ---!

ldap attribute-map LDAP

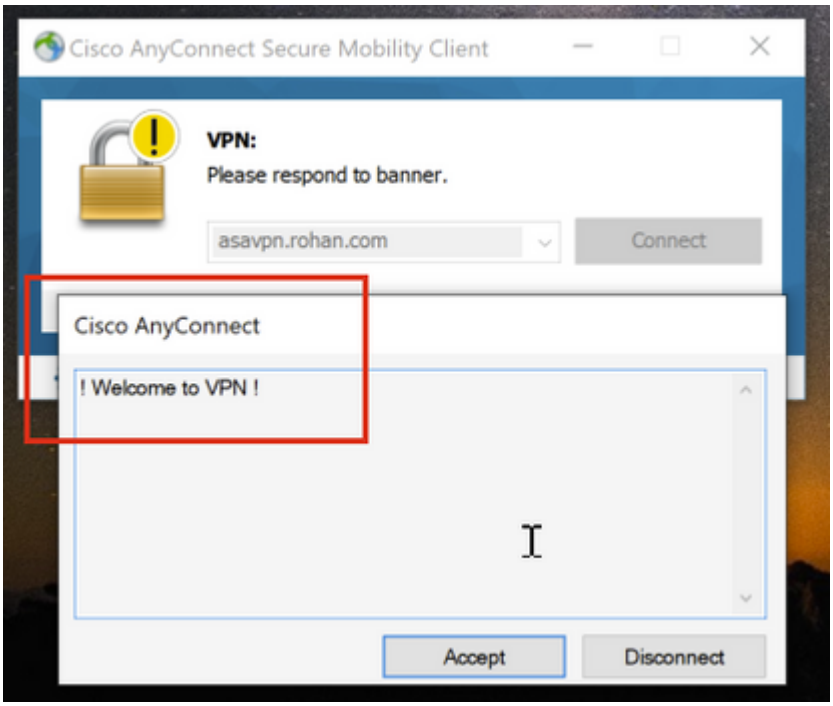
```
 map-name memberOf Group-Policy
 map-value memberOf DC=tlalocan,DC=sec RA-VPN

aaa-server LDAP protocol ldap
 max-failed-attempts 4
 realm-id 2
aaa-server LDAP host 10.106.56.137
 server-port 389
 ldap-base-dn DC=tlalocan,DC=sec
 ldap-group-base-dn DC=tlalocan,DC=sec
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=Users,DC=test,DC=com
 server-type microsoft
```

```
 ldap-attribute-map LDAP



!--- RA VPN Configuration ---!



webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-win-4.10.07061-webdeploy-k9.pkg 1 regex "Mac"
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable

ssl trust-point Self-Signed

group-policy No-Access internal

group-policy No-Access attributes



 vpn-simultaneous-logins 0


 vpn-idle-timeout 30

 !--- Output Omitted ---!

 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list none

group-policy RA-VPN internal

group-policy RA-VPN attributes



banner value ! Welcome to VPN !



 vpn-simultaneous-logins 3


 vpn-idle-timeout 30

 !--- Output Omitted ---!

 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list non

ip local pool VPN-Pool 10.72.1.1-10.72.1.150 mask 255.255.255.0

tunnel-group RA-VPN type remote-access

tunnel-group RA-VPN general-attributes


address-pool VPN-Pool
```

```
authentication-server-group LDAP
default-group-policy No-Access

tunnel-group RA-VPN webvpn-attributes
group-alias RA-VPN enable
```

Verifiëren

Meld u op de AnyConnect-client aan met de geldige VPN-gebruikersgroep Credentials en u krijgt het juiste groepsbeleid toegewezen door de LDAP-kenmerkkaart:

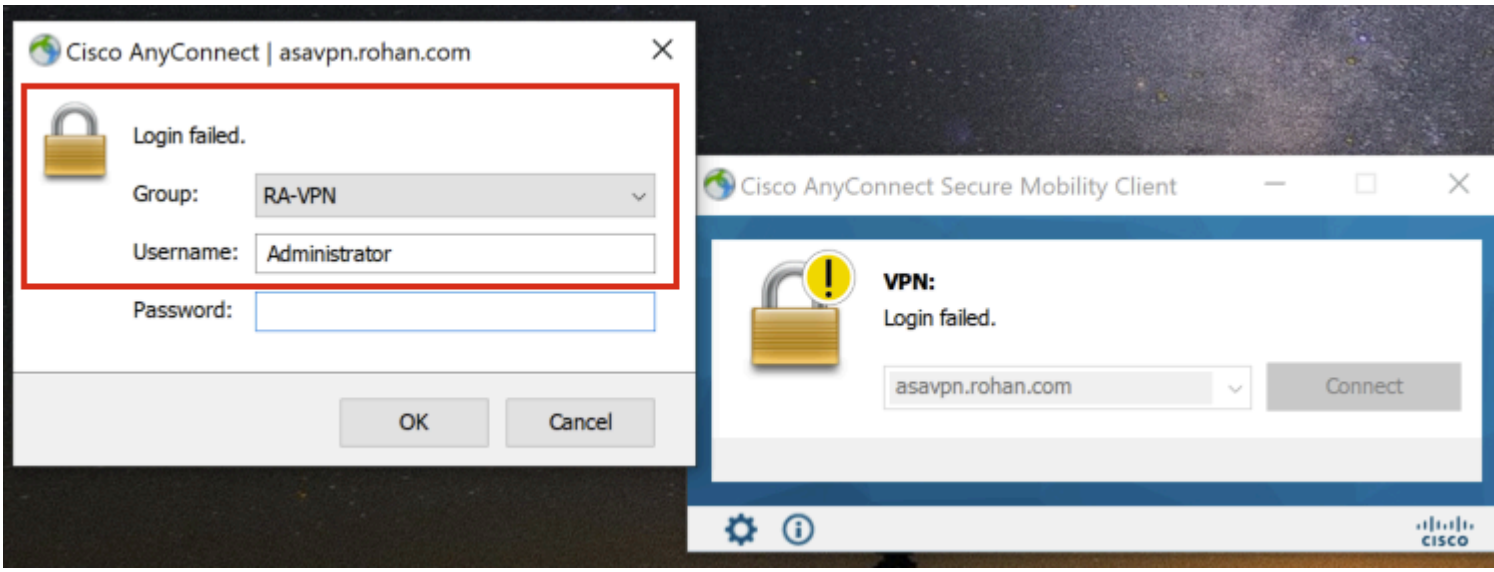


Van het LDAP Debug Snippet (debug ldap 255) kunt u zien dat er een match is op de LDAP Attribute Map:

<#root>

```
Authentication successful for test to 10.106.56.137

memberOf: value = DC=tlalocan,DC=sec

mapped to Group-Policy: value = RA-VPN

        mapped to LDAP-Class: value = RA-VPN
```

Meld u aan bij de AnyConnect-client met een ongeldige VPN-gebruikersgroep Credentials en u krijgt het groepsbeleid Geen toegang.



<#root>

```
%FTD-6-113004: AAA user authentication Successful : server = 10.106.56.137 : user = Administrator
```

%FTD-6-113009: AAA retrieved default group policy (No-Access) for user = Administrator

```
%FTD-6-113013: AAA unable to complete the request Error : reason =
```

Simultaneous logins exceeded for user : user = Administrator

Van LDAP Debug Snippet (debug ldap 255), kunt u zien dat er geen match is op de LDAP Attribute Map:

<#root>

Authentication successful for Administrator to 10.106.56.137

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
memberOf: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
        mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
        mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
```

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.