Configureer beveiligde toegang voor RA-VPNaaS postenbeoordeling met ISE

Inhoud

Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u Posture Assessment voor externe VPN-gebruikers kunt configureren met Identity Service Engine (ISE) en Secure Access.

Voorwaarden

- Gebruikersprovisioning configureren
- Cisco ISE-verbinding met beveiligde toegang via de tunnel

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Service Engine
- Beveiligde toegang
- Cisco Secure-client
- ISE-houding
- Verificatie, autorisatie en accounting

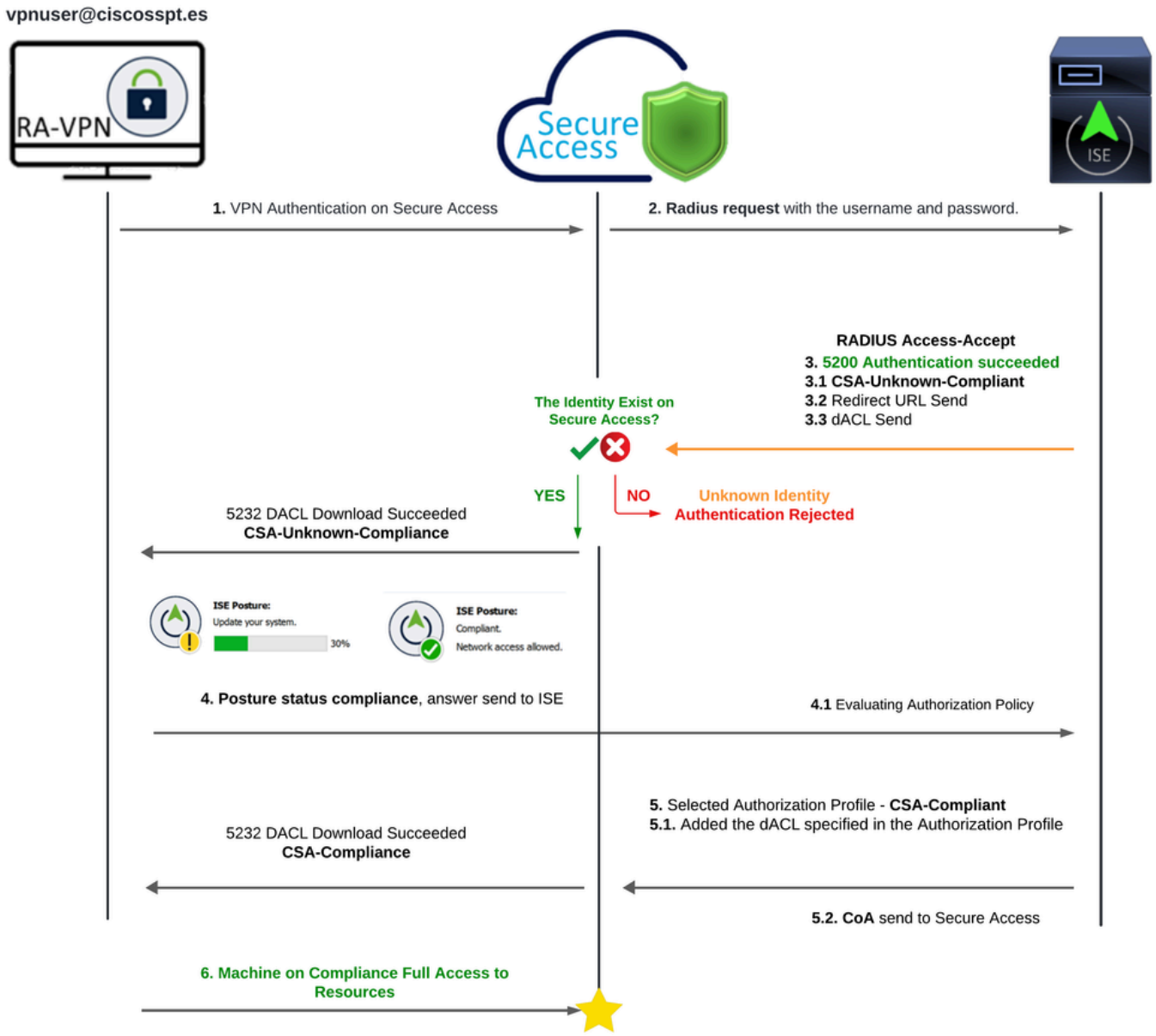
Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Identity Service Engine (ISE) versie 3.3 - patch 1
- Beveiligde toegang
- Cisco Secure Client - AnyConnect VPN-versie 5.1.2.4

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.

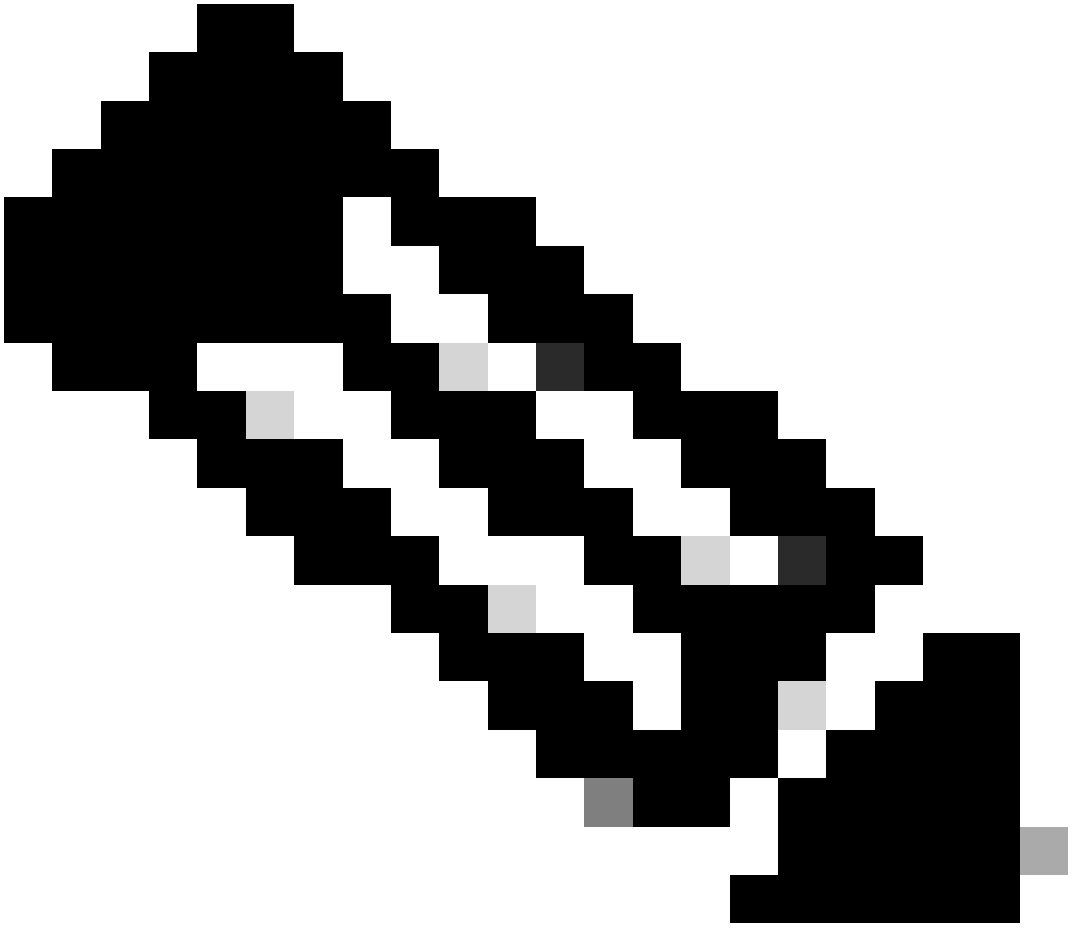
Achtergrondinformatie



Secure Access - ISE - diagram

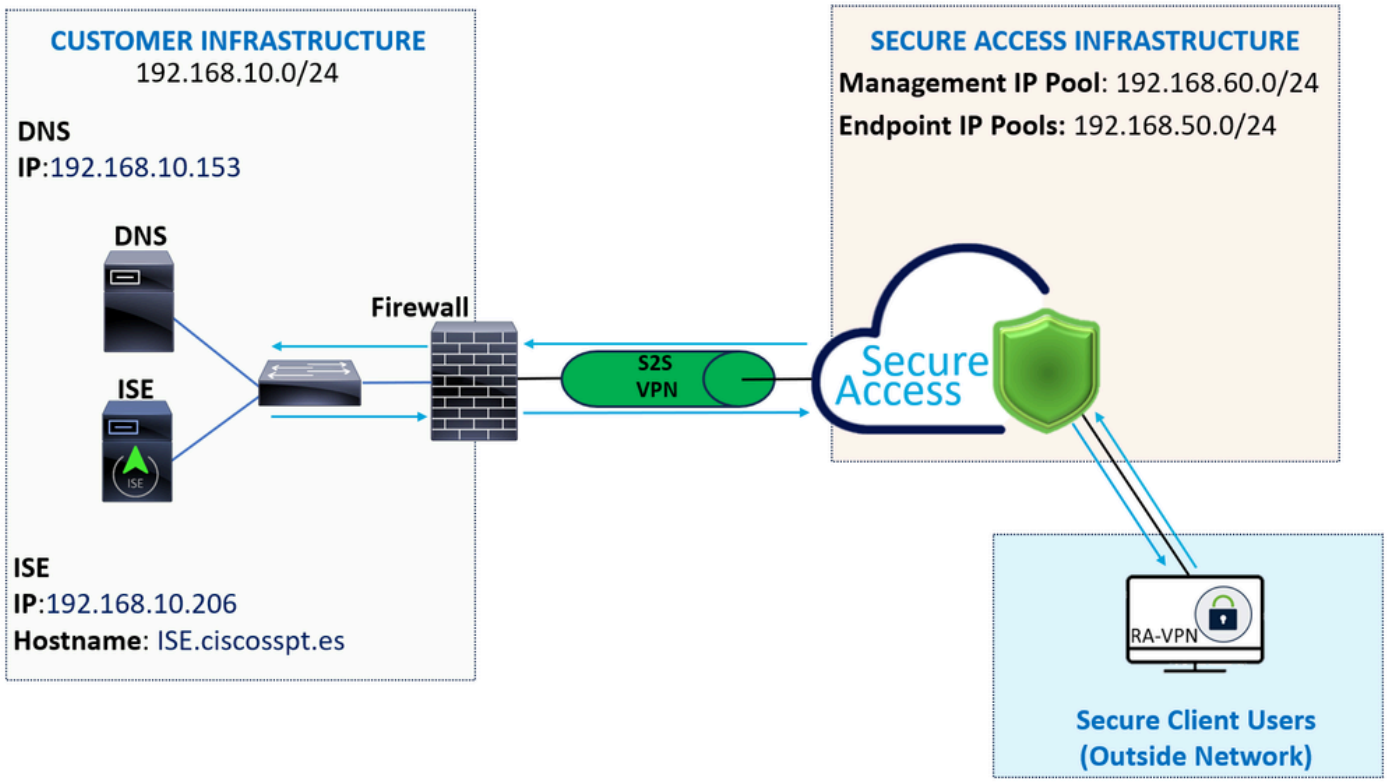
De integratie van Cisco Secure Access with Identity Services Engine (ISE) biedt een uitgebreide beveiligingsbenadering waarbij verschillende verificatieprotocollen, waaronder MS-CHAPv2, worden gebruikt om verbindingen te beveiligen. Cisco Secure Access, met zijn geavanceerde Security Service Edge (SSE)-oplossing, verbetert beveiligde connectiviteit in hypergedistribueerde omgevingen, met functies zoals VPN as a Service (VPNaaS), die met ISE-functies kunnen worden beveiligd.

Dankzij deze integratie kunnen gebruikers naadloos en veilig toegang krijgen tot elke toepassing, waar dan ook, met geoptimaliseerde prestaties en beveiliging. Het gebruik van geavanceerde functies van Cisco ISE, zoals Posture Assessment, versterkt dit beveiligingsmodel verder door de compatibiliteit van pc's met het interne gebruikersbeleid te evalueren voordat toegang wordt verleend. Dit waarborgt dat alleen apparaten die voldoen aan de beveiligingsvereisten van de organisatie toegang kunnen krijgen tot netwerkbronnen, waardoor het risico op kwetsbaarheden wordt verminderd.

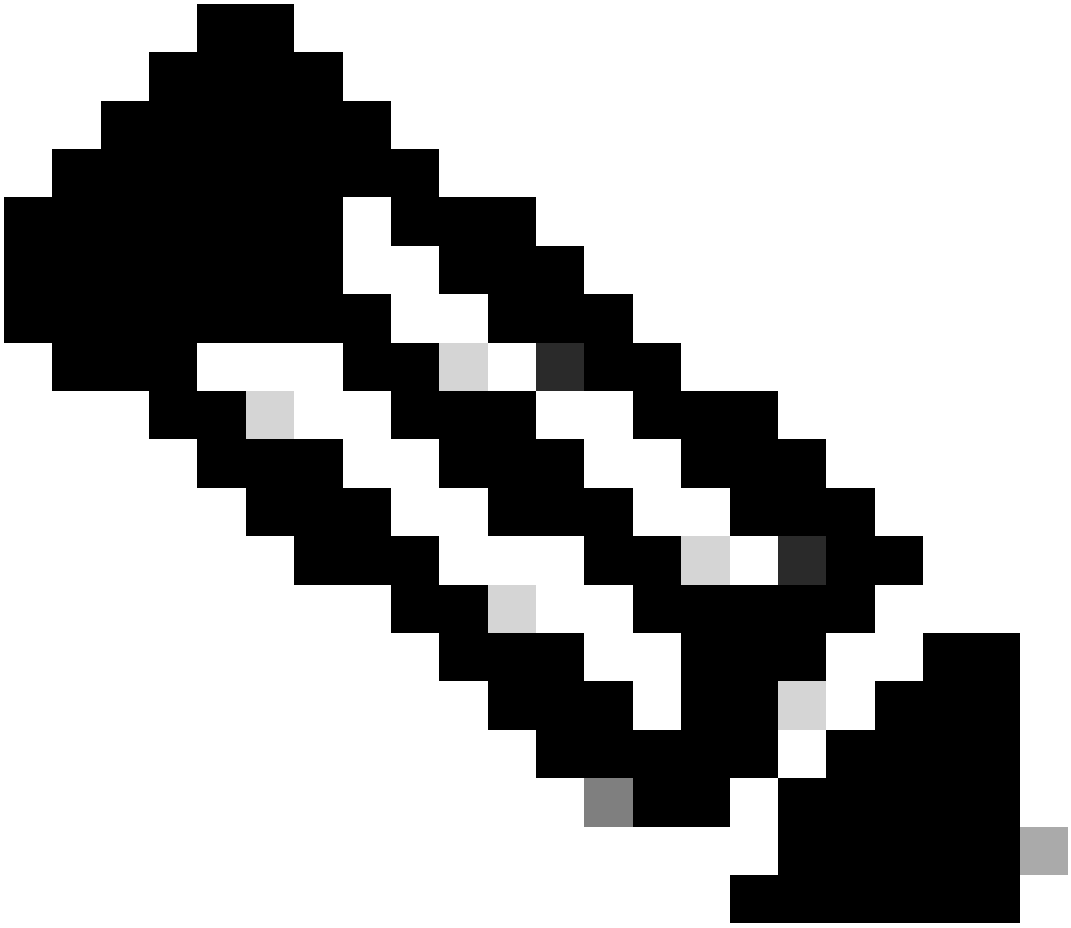


Opmerking: om de RADIUS-integratie te configureren, moet u ervoor zorgen dat u communicatie tussen beide platforms hebt.

Netwerkdiagram



Configureren



Opmerking: voordat u het configuratieproces start, moet u de eerste stappen voltooien met Secure Access en ISE-integratie.

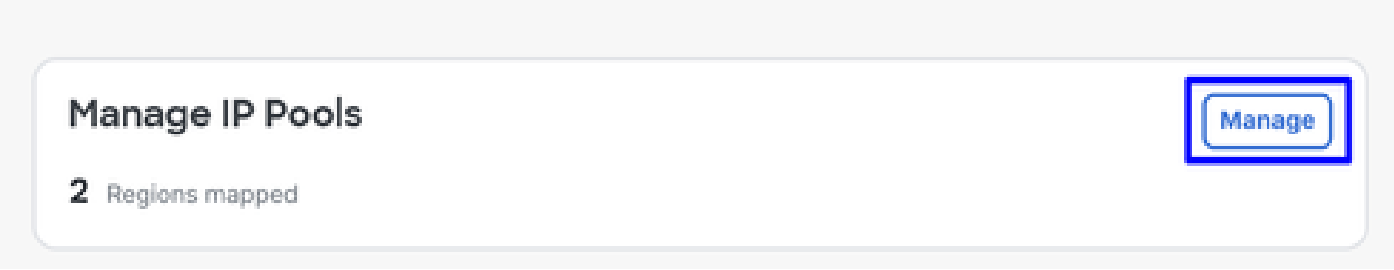
Configuratie van beveiligde toegang

Radius-groep op de IP-pools configureren

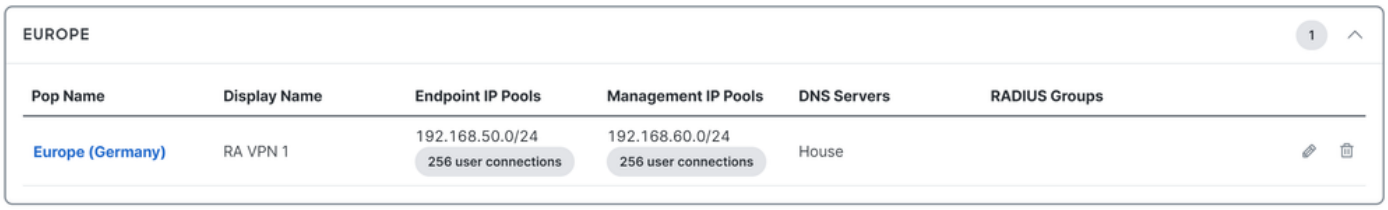
Ga verder met de volgende stappen om het VPN-profiel met behulp van Radius te configureren:

Navigeer naar uw Secure Access Dashboard.

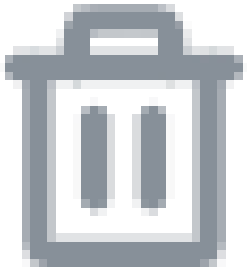
- Klik op **Connect** > **Enduser Connectivity** > **Virtual Private Network**
  - Klik onder uw Pool Configuration (**Manage IP Pools**) opManage



- Kies de **IP Pool Region** en configureer de **Radius Server**

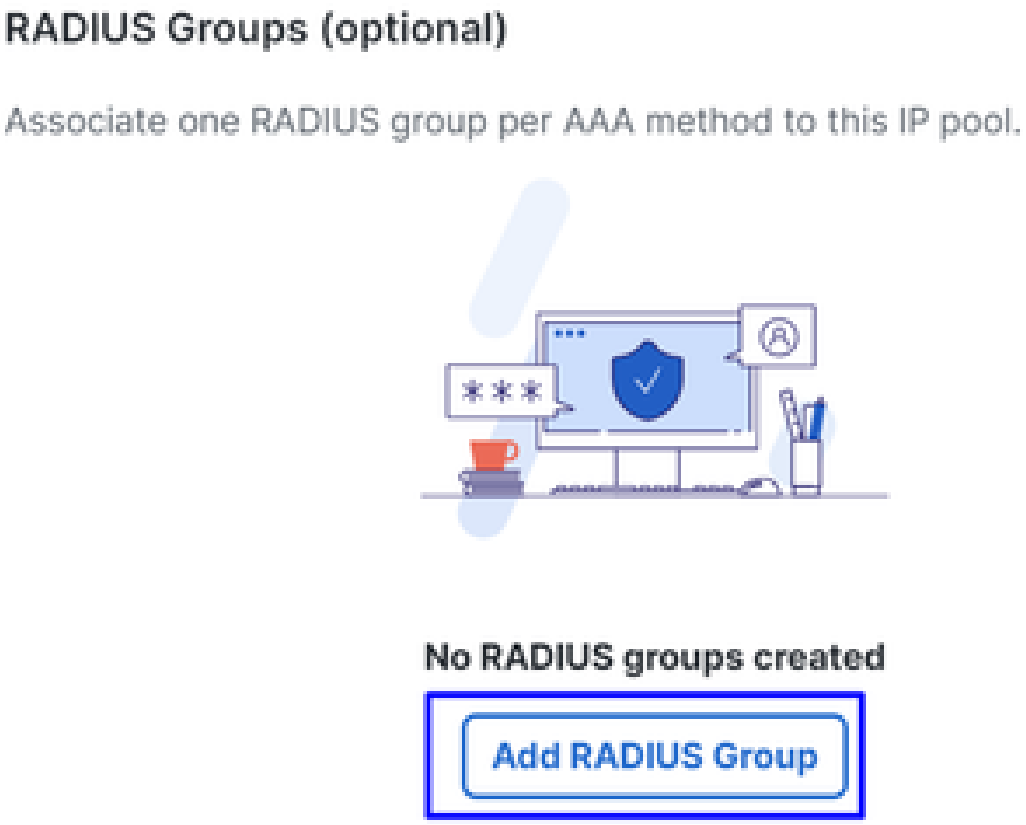


- Klik op het potlood om te bewerken



- Nu, onder de IP Pool sectie configuratie vervolgkeuzelijst onder **Radius Group (Optional)**

- Klik op de knop Add RADIUS Group



← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

Group Name: Configureer een naam voor uw ISE-integratie in Secure Access

- **AAA method**

  - **Authentication**: Vink het selectievakje aan **Authentication** en selecteer de poort, standaard, is 1812

    - In het geval dat uw verificatie vereist Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2), vinkt u het vakje aan

- **Authorization**: Vink het selectievakje aan Authorization en selecteer de poort, standaard, is 1812

  - Vink het aanvinkvakje aan **Authorization mode Only Change of Authorization (CoA) mode** en laat de postuur en wijzigingen van ISE toe

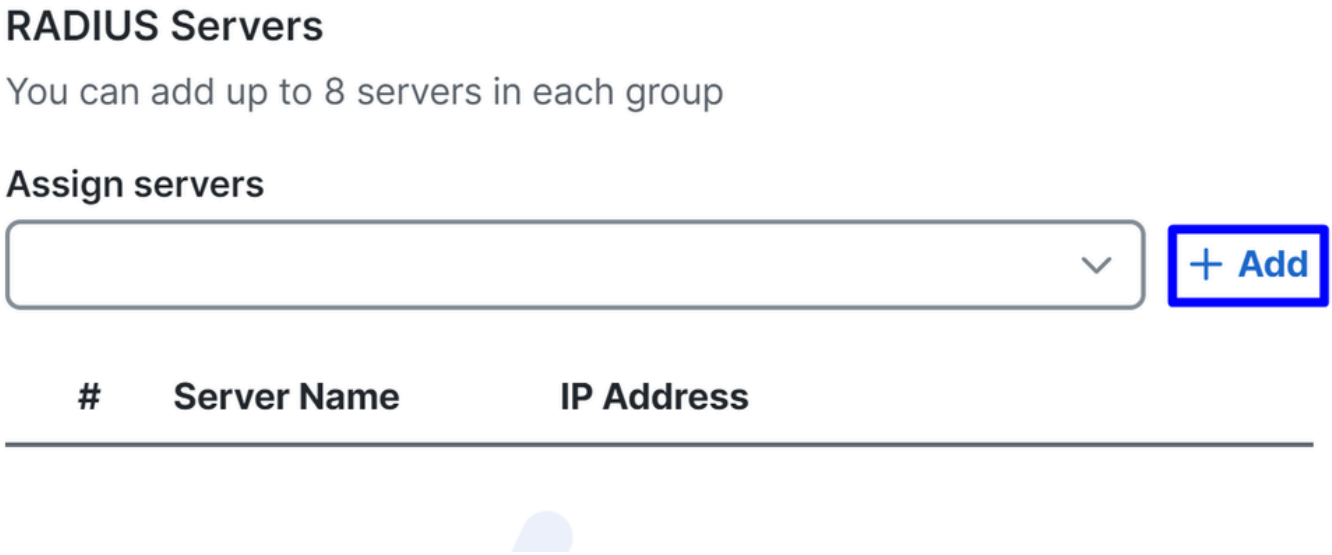
- **Accounting**: Vink het selectievakje voor autorisatie aan en selecteer de poort, standaard, is 1813

  - Kies **Single or Simultaneous** (In één modus worden de boekhoudgegevens naar slechts één server verzonden. In gelijktijdige modus, accounting gegevens naar alle servers in de groep)

    - Vink het aanvinkvakje aan **Accounting update** om de periodieke generatie van tussentijdse RADIUS-accounting-update berichten in te schakelen.

Waarschuwing: zowel de Authentication als de **Authorization** methoden moeten, indien geselecteerd, dezelfde poort gebruiken.

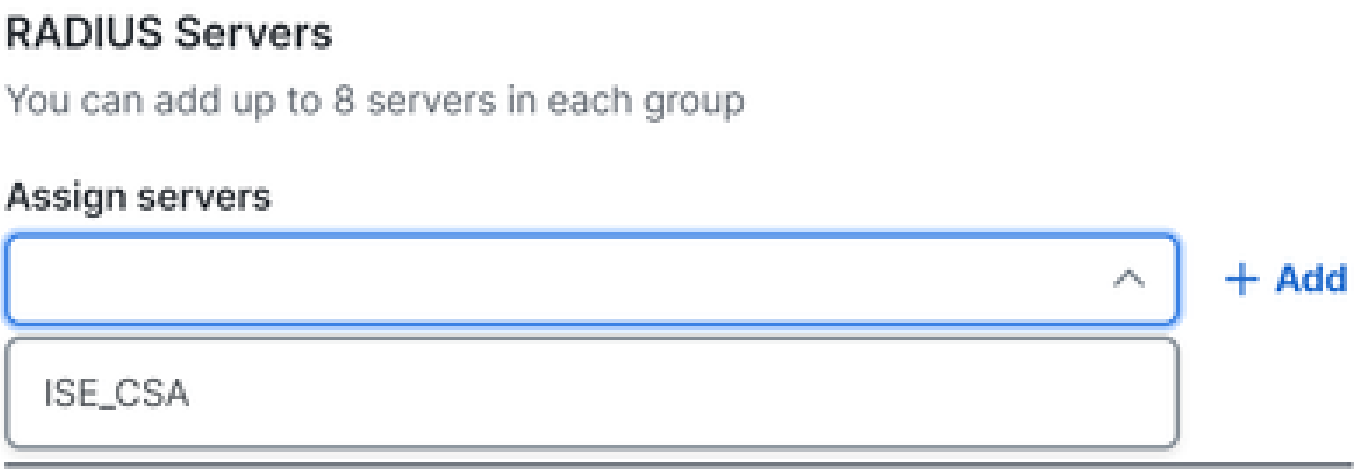
- Daarna moet u de **RADIUS Servers** (ISE) configureren die wordt gebruikt om via AAA te verifiëren in het vak **RADIUS Servers**:
- Klik op + Add



- Configureer vervolgens de volgende opties:

- Server Name: Configureer een naam om uw ISE-server te identificeren.
- **IP Address**: Configureer het IP-adres van uw Cisco ISE-apparaat dat bereikbaar is via beveiligde toegang
- **Secret Key**: Configureer uw RADIUS geheime sleutel
- **Password**: Configureer uw RADIUS-wachtwoord

- Klik op **Save** en wijs uw Radius Server toe onder de optie onder Assign Server en selecteer uw ISE-server:



- Klik **Save** nogmaals om alle uitgevoerde configuratie op te slaan

← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

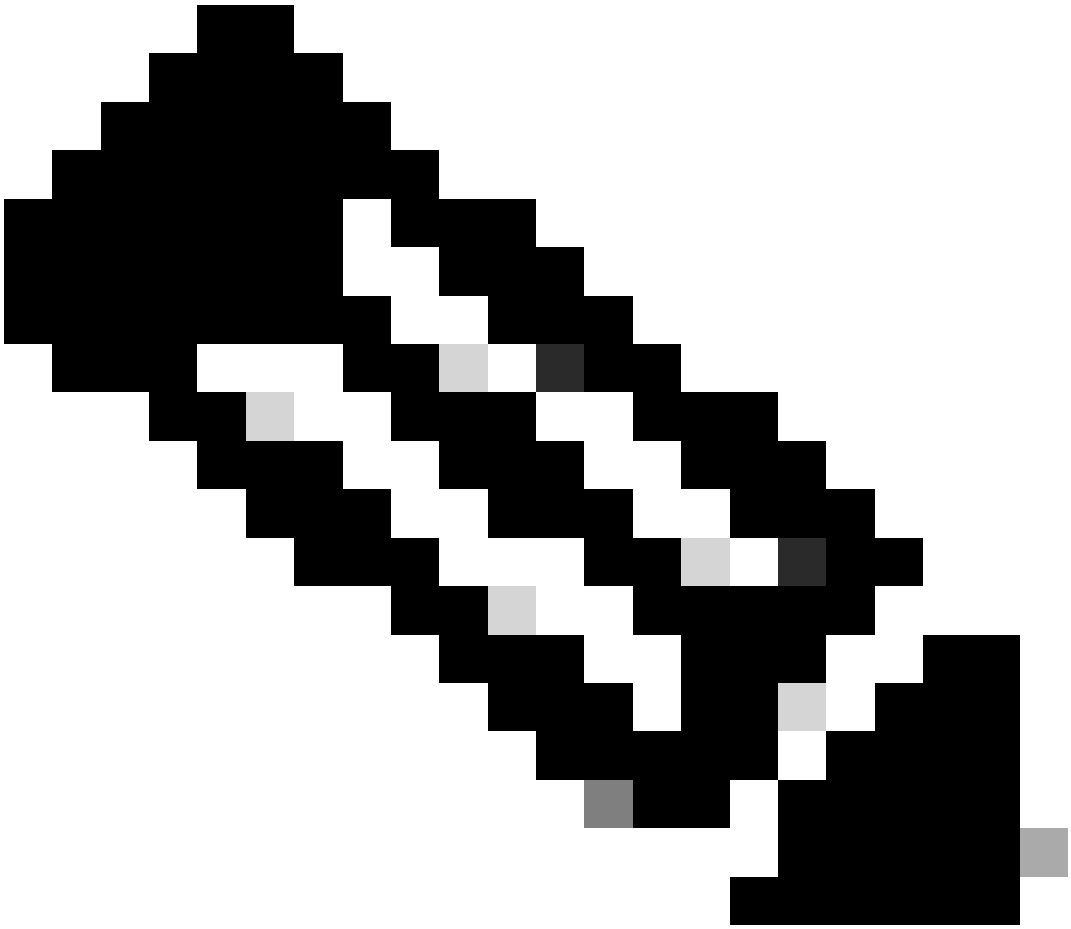
+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**: Kies **Radius**

- **Map authentication groups to regions**: Kies de regio's en kies uw **Radius Groups**

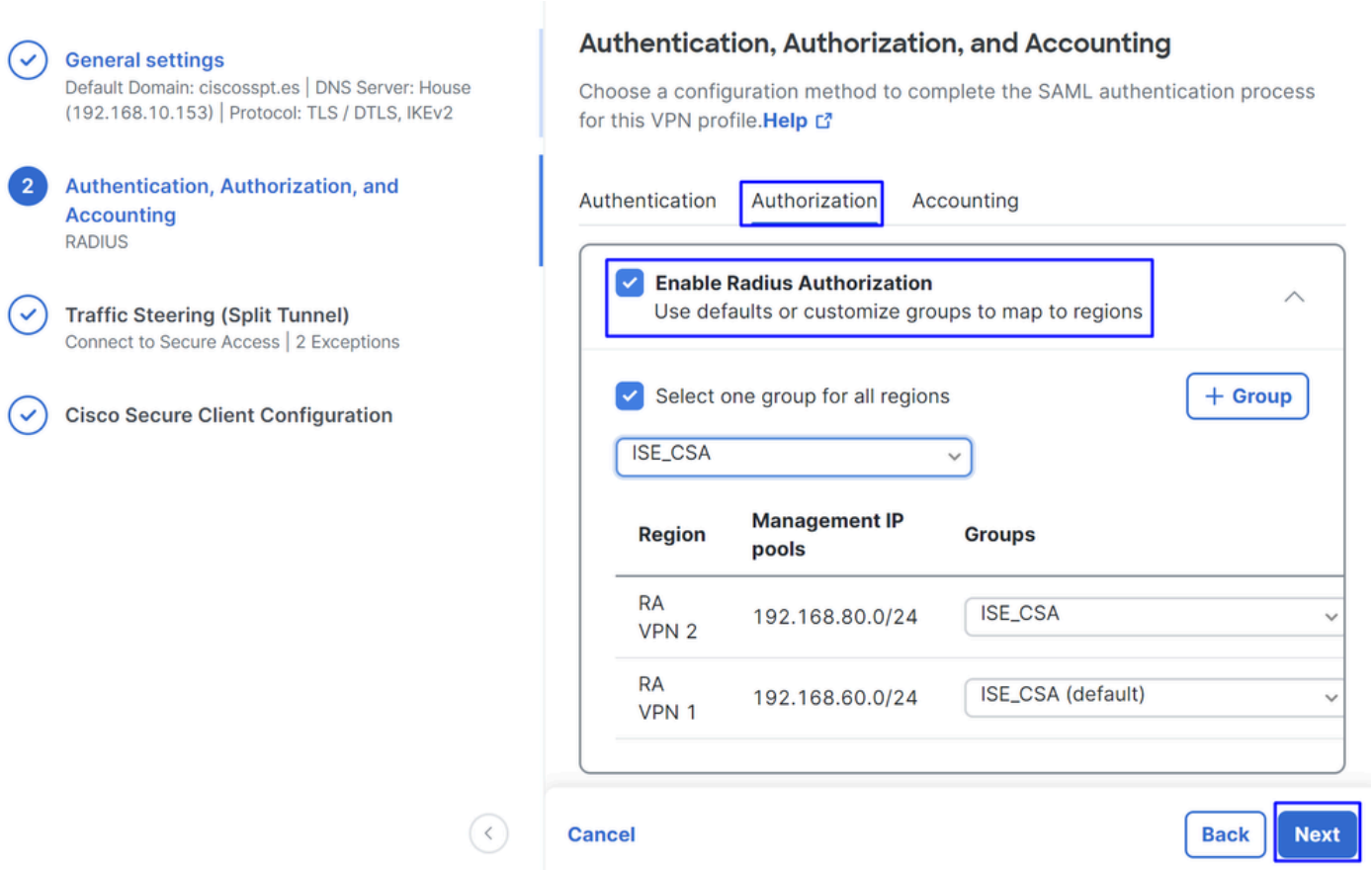
- Klik op de knop **Next**



Opmerking: als u meerdere gebieden hebt, moet u alle gebieden aanvinken en de radiusgroepen selecteren. Als u dat niet doet, is uw **Next** knop grijs.

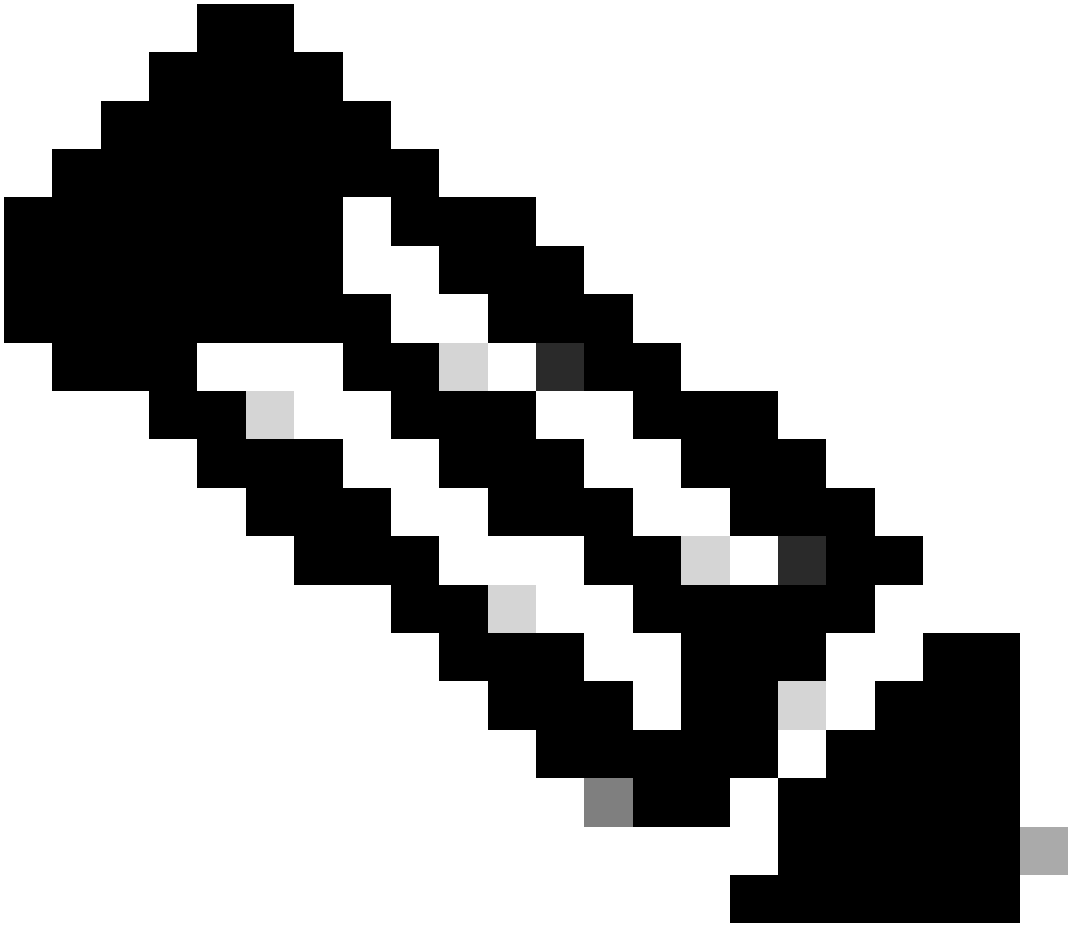
Nadat u alle verificatieonderdelen hebt geconfigureerd, gaat u verder met de autorisatie.

Authorization



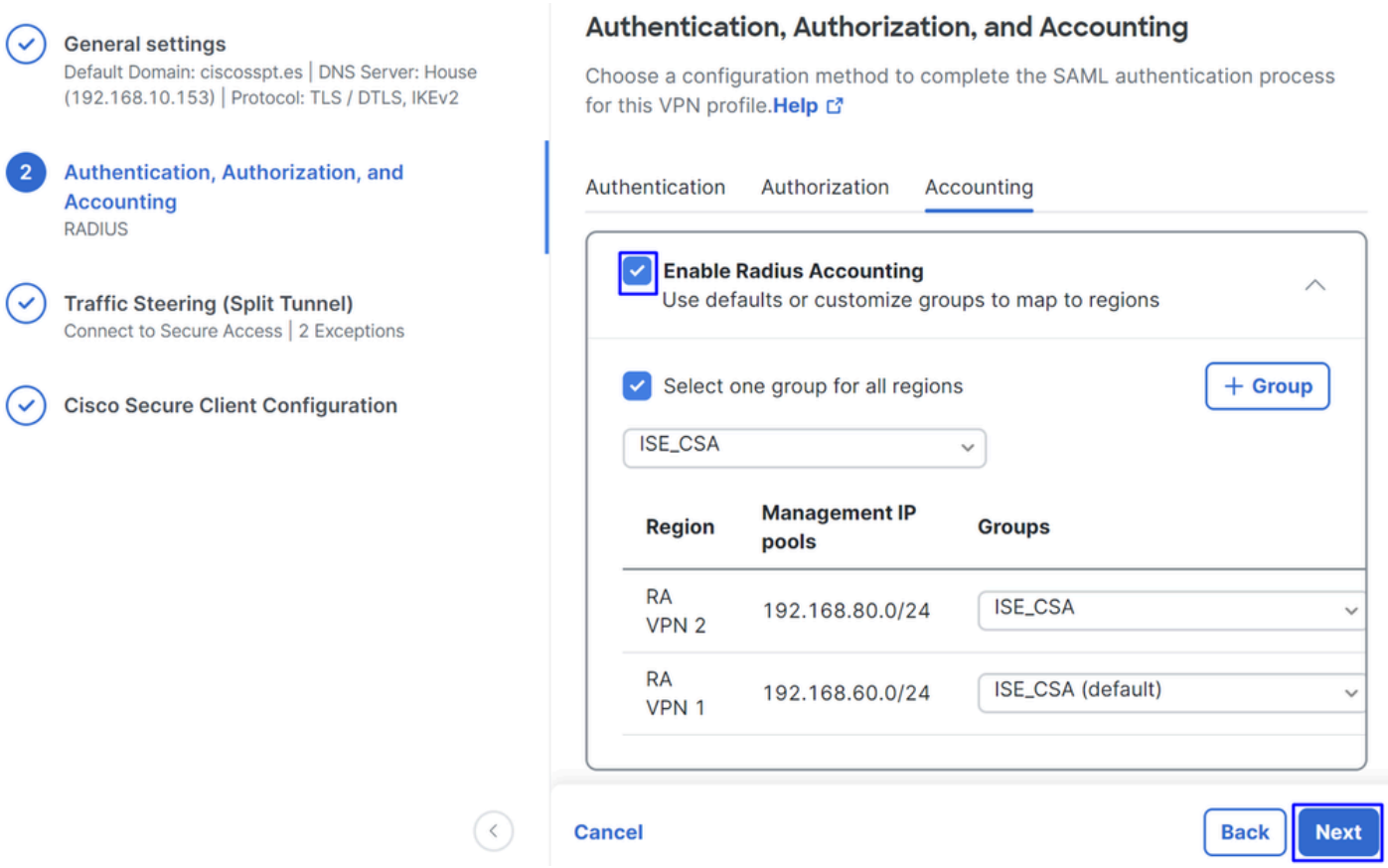
- **Authorization**
    - **Enable Radius Authorization**: vink het aanvinkvakje aan om de straalautorisatie in te schakelen
    - **Selecteer één groep voor alle regio's**: vink het selectievakje aan om één specifieke radiusserver te gebruiken voor alle Remote Access - Virtual Private Network (RA-VPN)-pools, of definieer het voor elke pool afzonderlijk
- Klik op de knop **Next**

Nadat u alle **Authorization** onderdeel hebt geconfigureerd, gaat u verder met het **Accounting**onderdeel.



Opmerking: als u deze functie niet inschakelt, kan postuur niet **Radio Authorization**werken.

Accounting



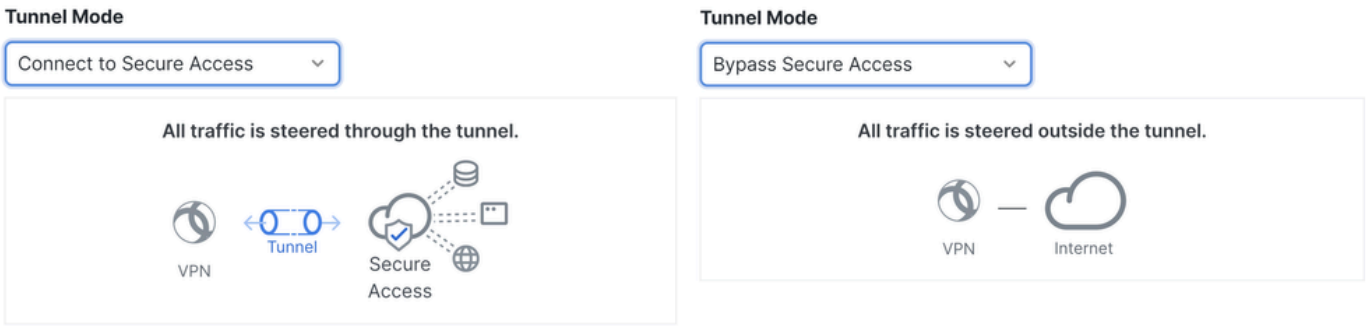
- **Accounting**
    - **Map Authorization groups to regions**: Kies de regio's en kies uw **Radius Groups**

- Klik op de knop **Next**

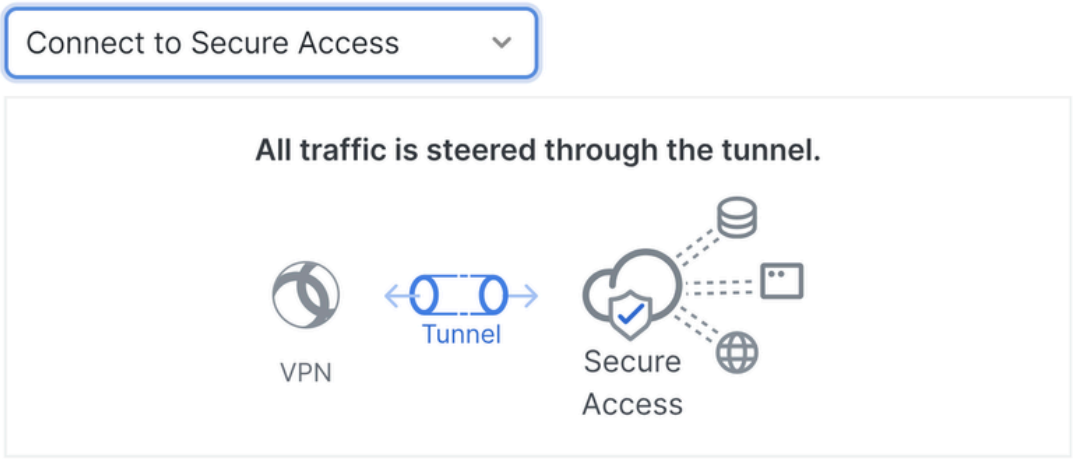
After you have done configured the Authentication, Authorization and Accounting gaat u alstublieft verder metTraffic Steering.

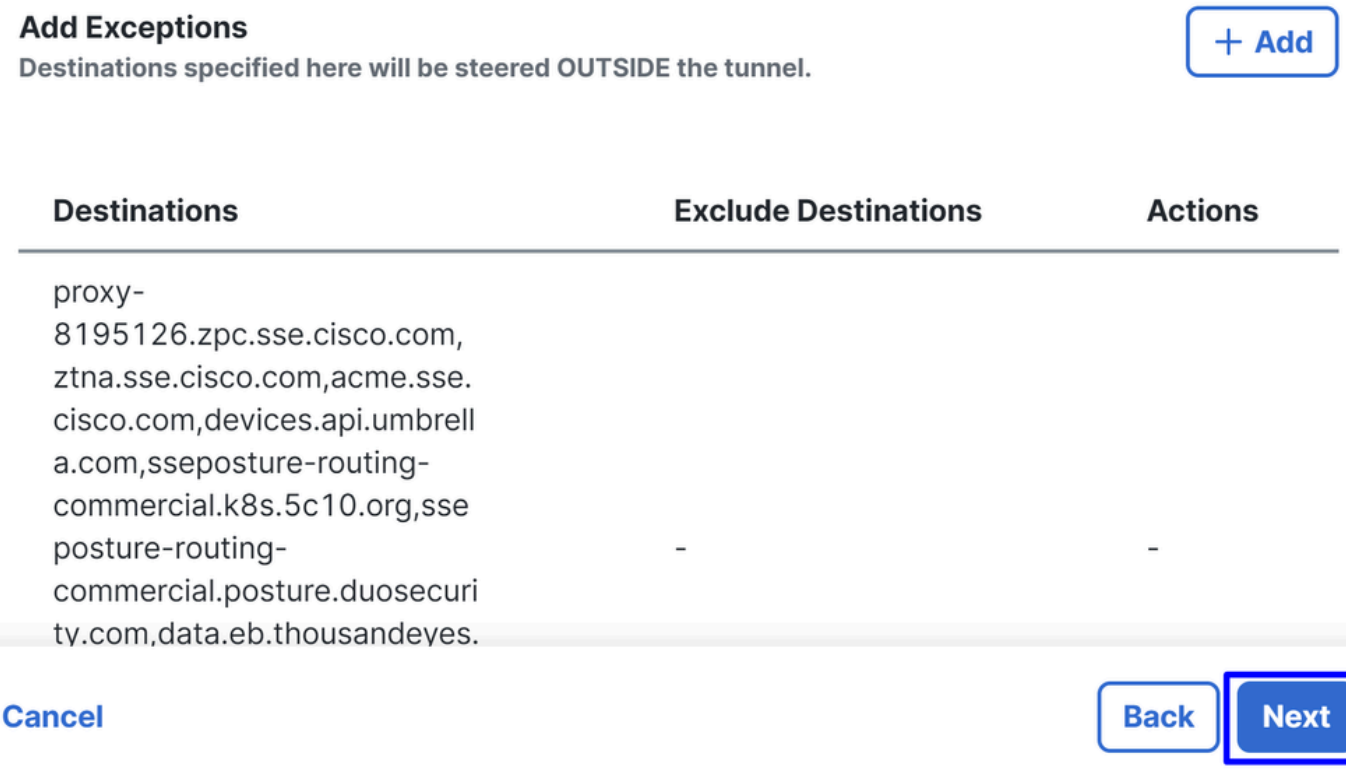
Besturing van verkeer

Onder traffic shaping moet u het type communicatie configureren via Secure Access.



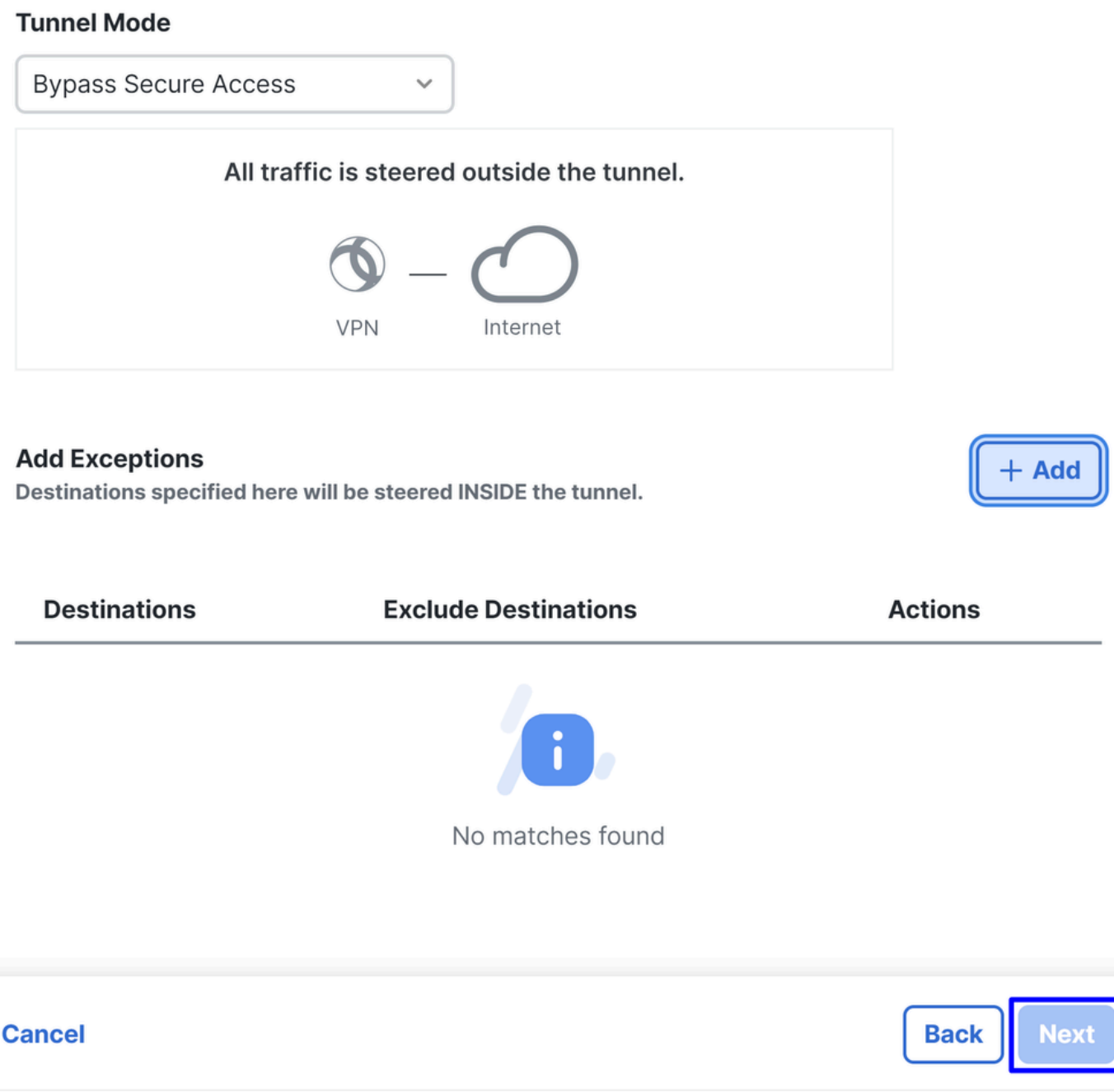
- Als u kiest, **Connect to Secure Access**gaat al uw internetverkeer door **Secure Access**

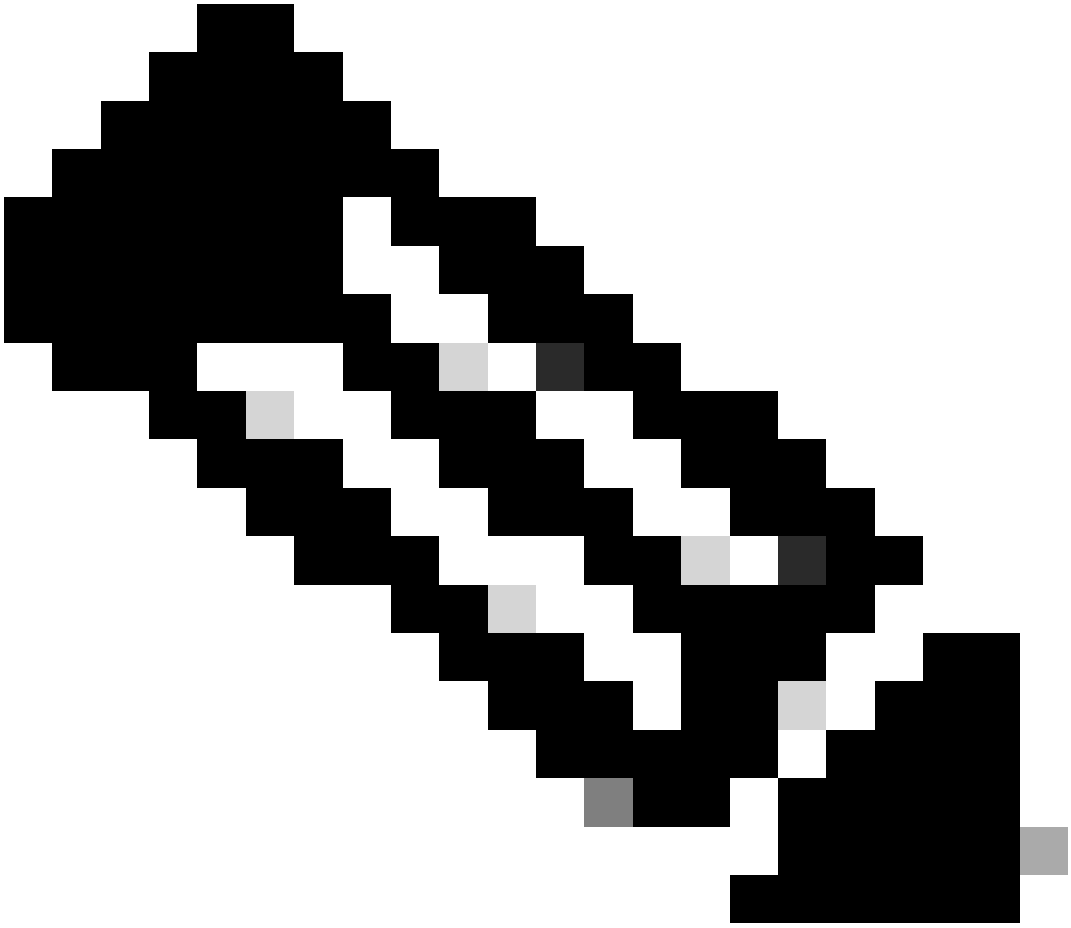




Als u uitsluitingen voor internetdomeinen of IP's wilt toevoegen, klikt u op de **+ Add** knop en vervolgens klikt u op **Next**.

- Als je besluit om te gaan **Bypass Secure Access**, gaat al je internetverkeer via je internetprovider, niet viaSecure Access (geen internetbescherming)

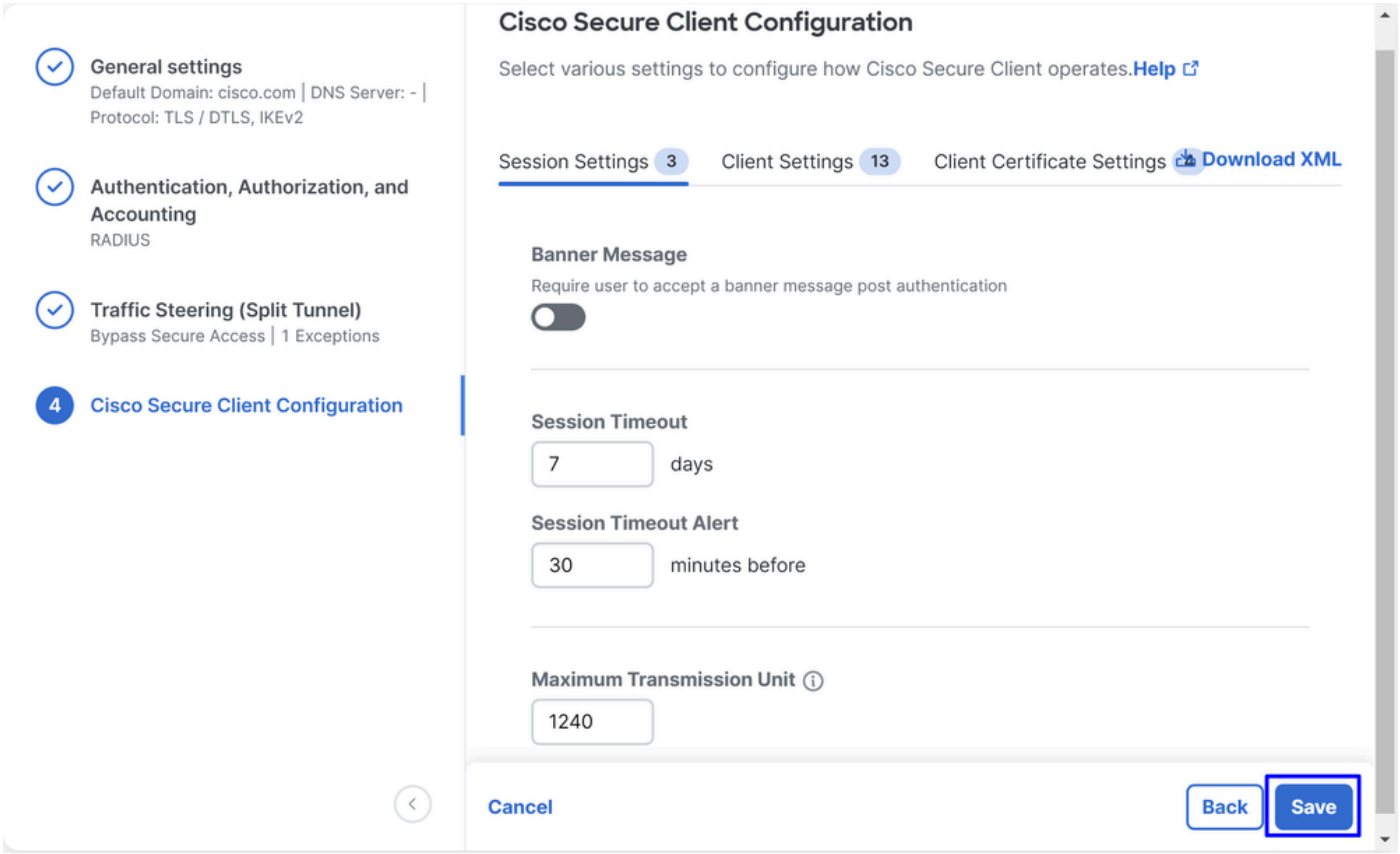




Opmerking: voeg toe **enroll.cisco.com** voor de ISE-houding wanneer u kiest **Bypass Secure Access**.

In deze stap, selecteert u alle privé netwerkmiddelen die u door VPN wilt toegang hebben tot. Klik om dit te doen **+ Add**en klik vervolgens **Next** wanneer u alle bronnen hebt toegevoegd.

Cisco Secure-clientconfiguratie



In deze stap kunt u alles standaard behouden en op klikken **Save**, maar als u uw configuratie meer wilt aanpassen, raadpleegt u de Cisco Secure Client Administrator-handleiding.

ISE-configuraties

Lijst met netwerkapparaten configureren

Om de verificatie met Cisco ISE te configureren, moet u de toegestane apparaten configureren die vragen kunnen stellen aan uw Cisco ISE:

- Naar navigeren **Administration > Network Devices**
- Klik op **+ Add**

Network Devices List > CSA

Network Devices

Name CSA

Description

IP Address * IP : 192.168.60.0 / 24

Device Profile Cisco

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret •••••••• Show

Use Second Shared Secret

Second Shared Secret Show

CoA Port 1700 Set To Default

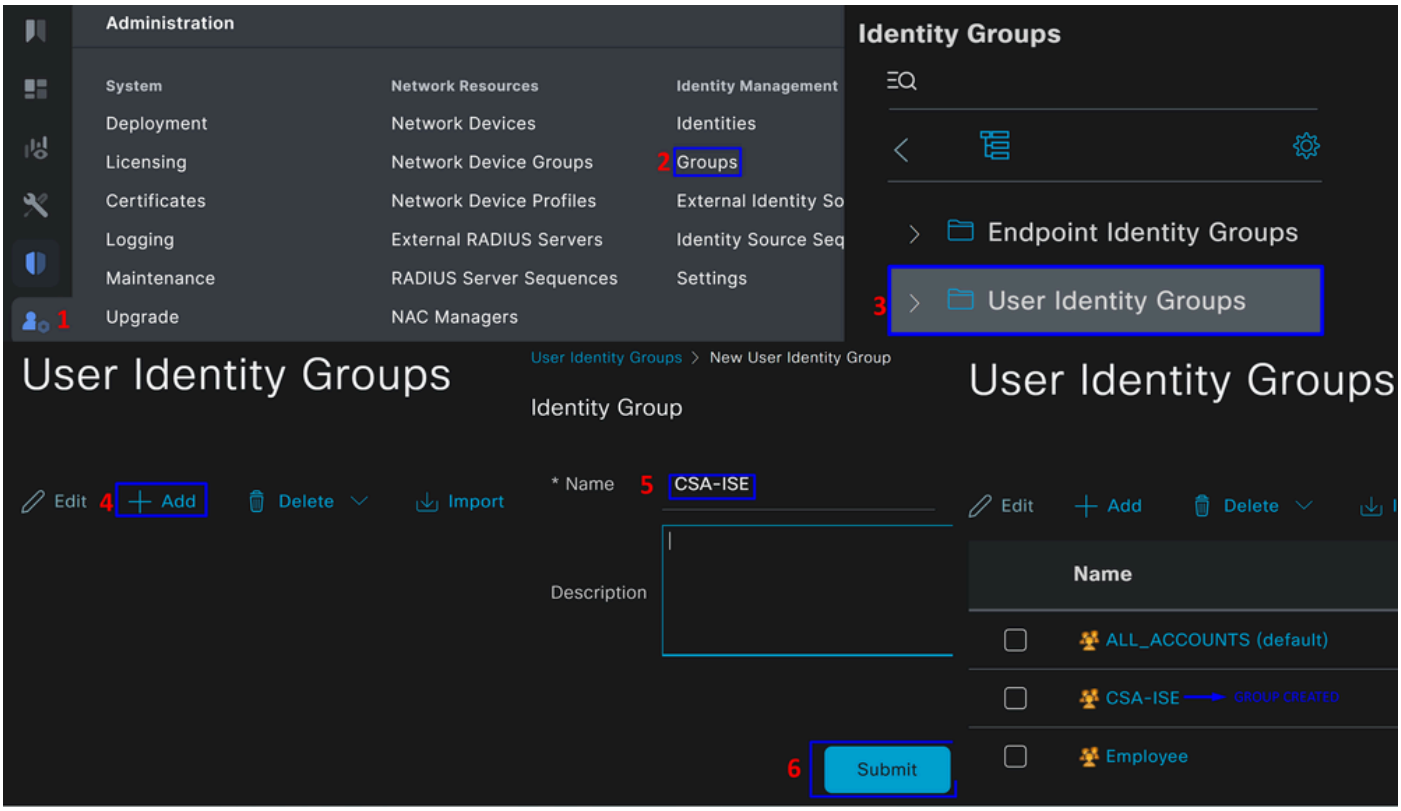
- **Name**: Gebruik een naam om beveiligde toegang te identificeren
- **IP Address**: De Management Interface stappen configureren, IP-poolregio
- **Device Profile**: Cisco kiezen
    - **Radius Authentication Settings**
        - Shared Secret: Configureer hetzelfde gedeelde geheim dat bij de stap is geconfigureerd, geheime sleutel
            - **CoA Port**: Laat het standaard; 1700 wordt ook gebruikt in Secure Access

Na die klik **Save**, om te verifiëren als de integratie correct werkt, ga te werk om een lokale gebruiker voor integratieverificatie te creëren.

Een groep configureren

Ga als volgt te werk om een groep te configureren voor gebruik met lokale gebruikers:

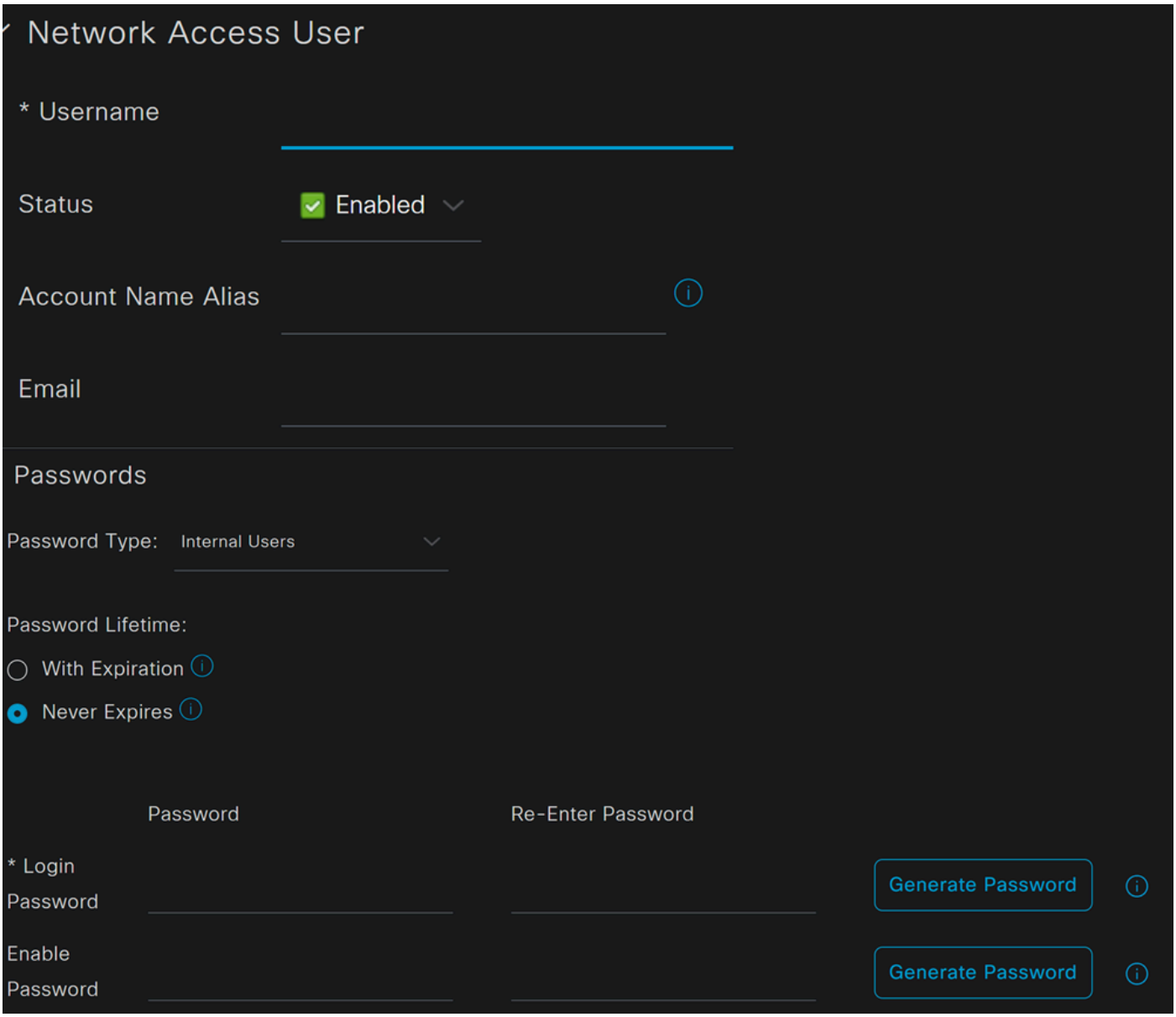
- Klik in **Administration > Groups**
- Klik op de knop **User Identity Groups**
- Klik op de knop + Add
- Maak een Namevoor de groep en klik op **Submit**

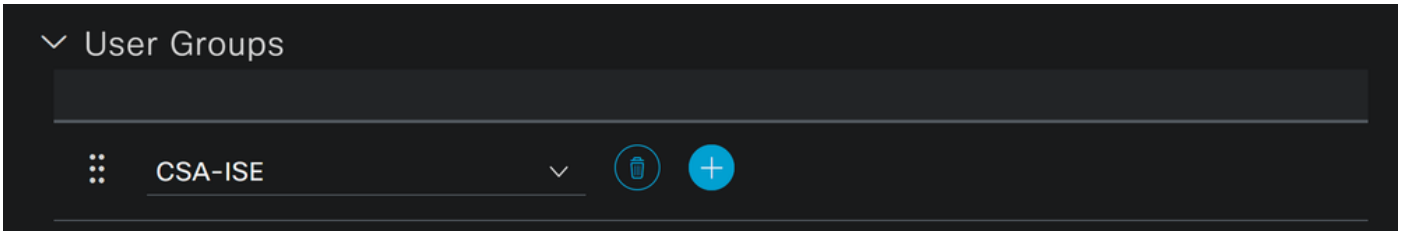


Lokale gebruiker configureren

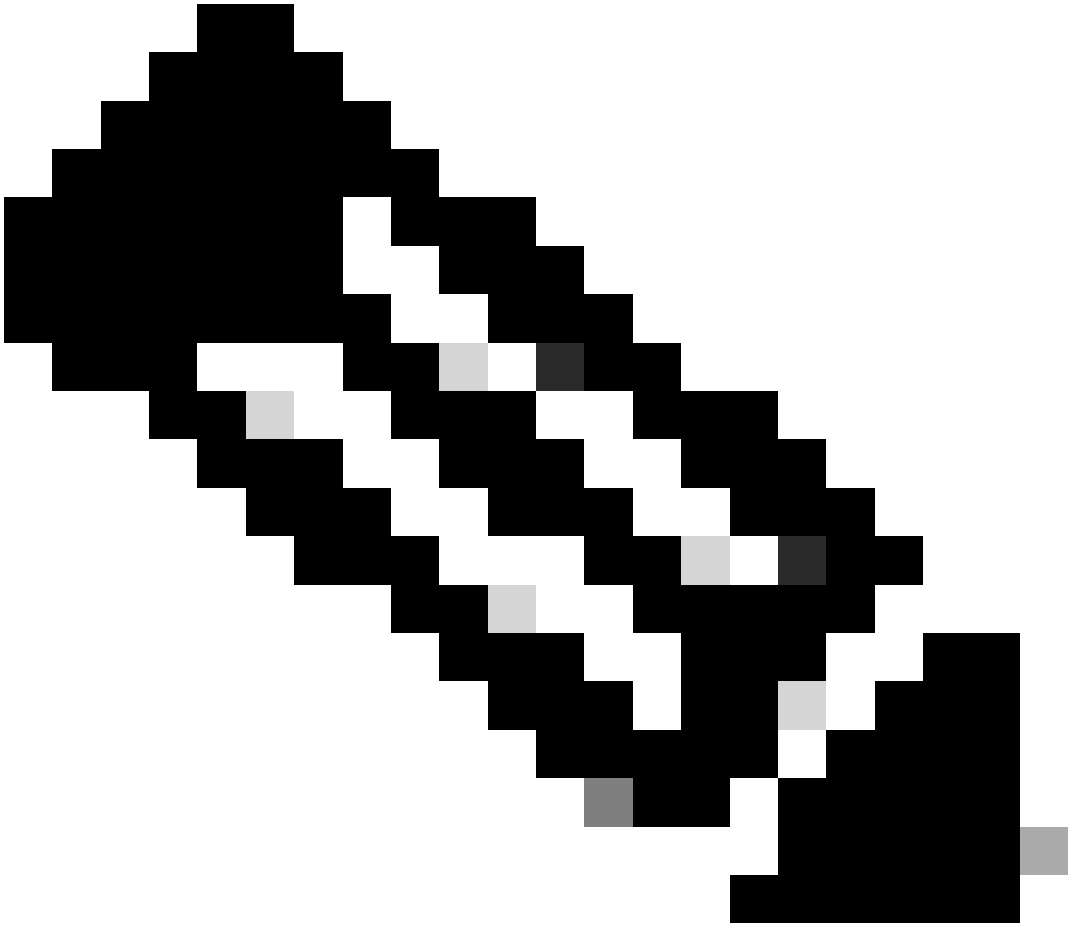
U kunt als volgt een lokale gebruiker configureren om uw integratie te verifiëren:

- Naar navigeren **Administration > Identities**
- Klik op **Add +**





- **Username**: Configureer de gebruikersnaam met een bekende UPN-voorziening in Secure Access; dit is gebaseerd op de stap, vereisten
- **Status**:Actief
- **Password Lifetime**: U kunt het configureren **With Expiration** of Never Expires, afhankelijk van u
- **Login Password**: Een wachtwoord voor de gebruiker aanmaken
- **User Groups**: Selecteer de groep die bij de stap is gemaakt en stel een groep in



Opmerking: de verificatie op basis van UPN is ingesteld om te wijzigen in toekomstige versies van Secure Access.

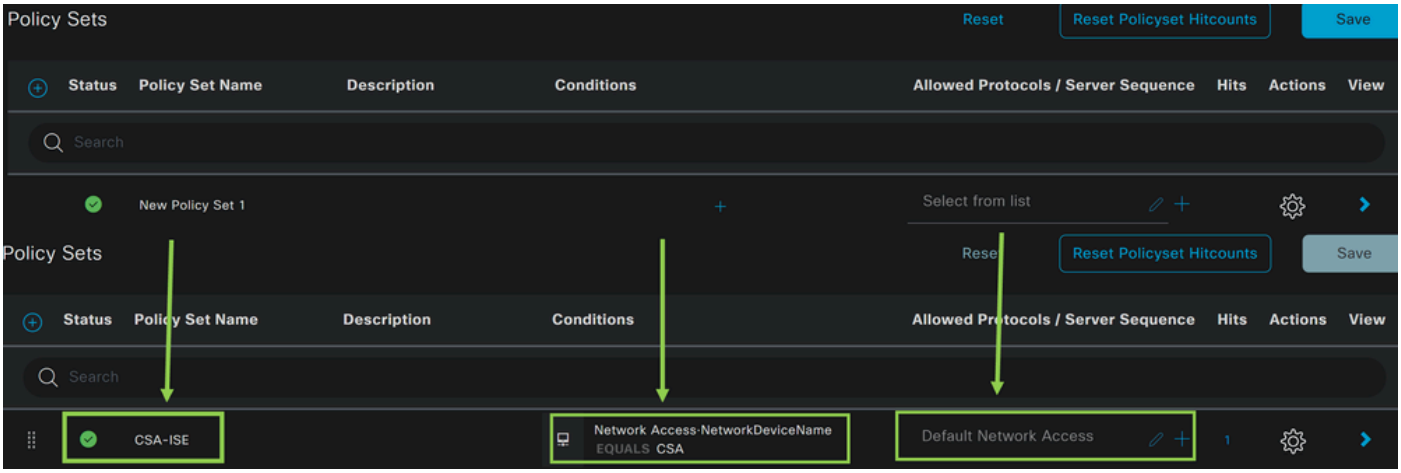
Daarna kunt u **Save** de configuratie aanpassen en doorgaan met de stap, **Configure Policy Set**.

Beleidsset configureren

Configureer onder de beleidsset de actie die ISE tijdens de verificatie en autorisatie uitvoert. Dit scenario demonstreert de gebruikscase voor het configureren van een eenvoudig beleid om toegang voor gebruikers te bieden. Ten eerste controleert ISE de oorsprong van de RADIUS-authenticaties en controleert ze of de identiteiten in de ISE-gebruikersdatabase aanwezig zijn om toegang te bieden

Om dat beleid te configureren navigeer u naar uw Cisco ISE-dashboard:

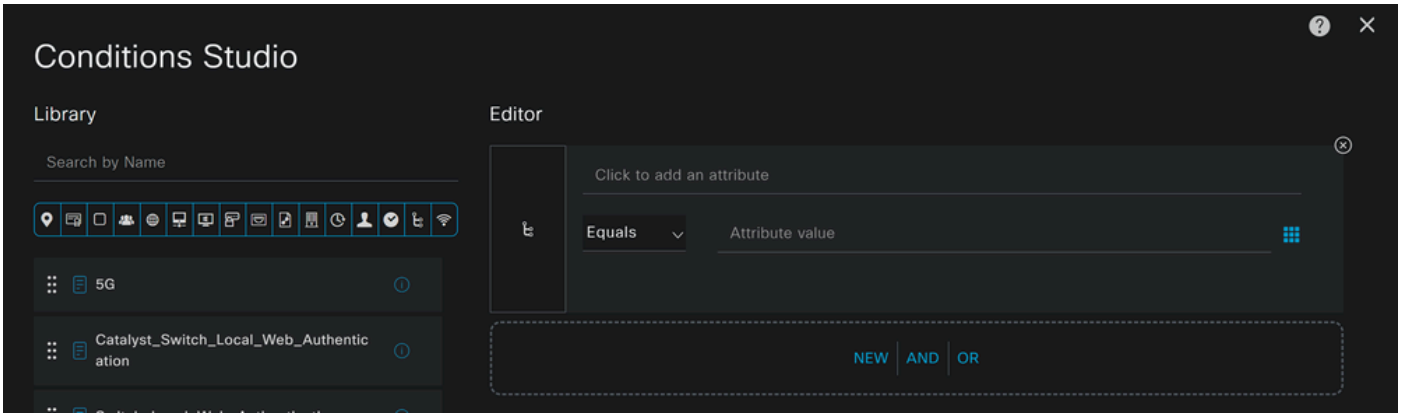
- Klik op Policy > Policy Sets
- Klik op om een nieuwe beleidsset toe + te voegen



Maak in dit geval een nieuwe beleidsset in plaats van onder de standaardset te werken. Configureer vervolgens de verificatie en autorisatie op basis van die beleidsset. Het geconfigureerde beleid maakt toegang tot het netwerkapparaat mogelijk dat is gedefinieerd in de stap Netwerkapparaten configureren om te controleren of deze verificaties afkomstig zijn van CSA Network Device List en vervolgens in het beleid als **Conditions**. En tenslotte, de toegestane protocollen, zoals **Default Network Access**.

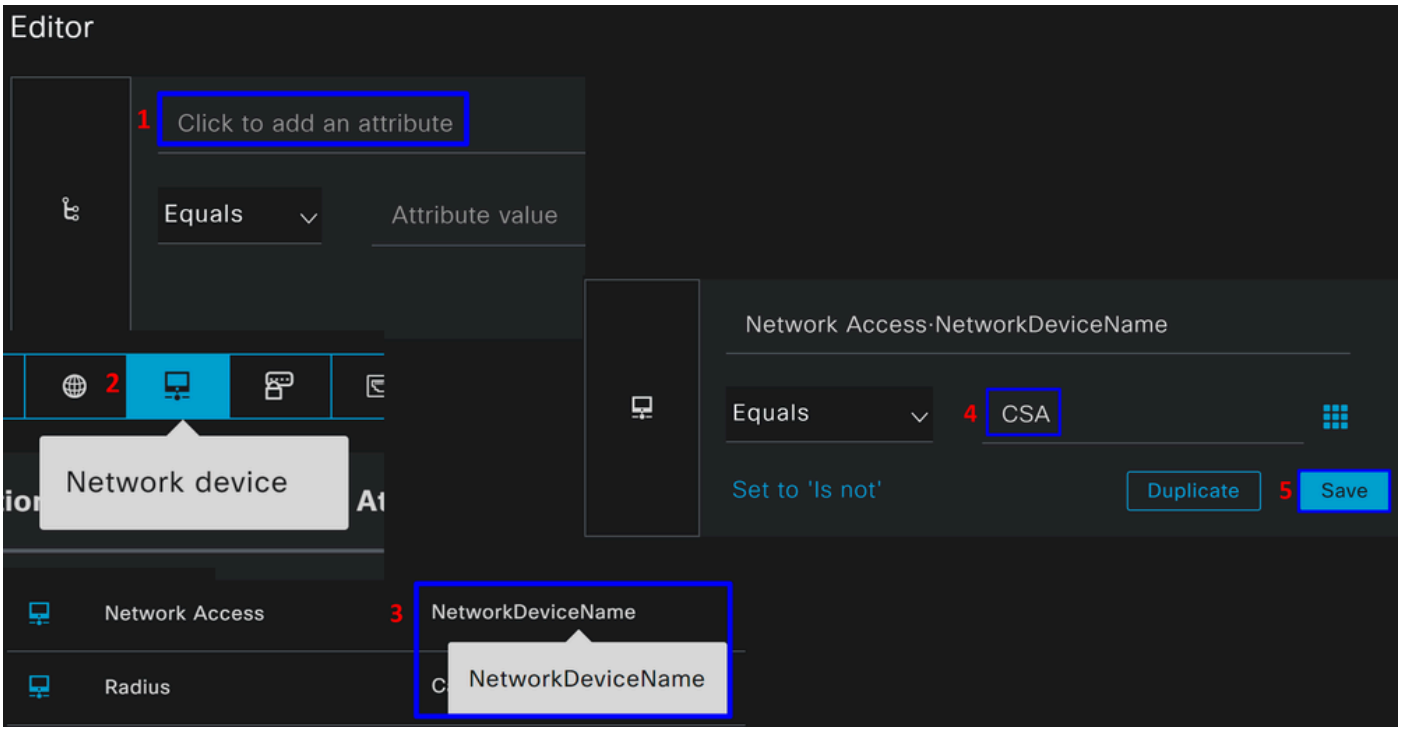
Ga verder met de volgende instructies om de instellingen te maken **condition** die overeenkomen met de beleidsset:

- Klik op +
- Onder **Condition Studio**de beschikbare informatie vallen:



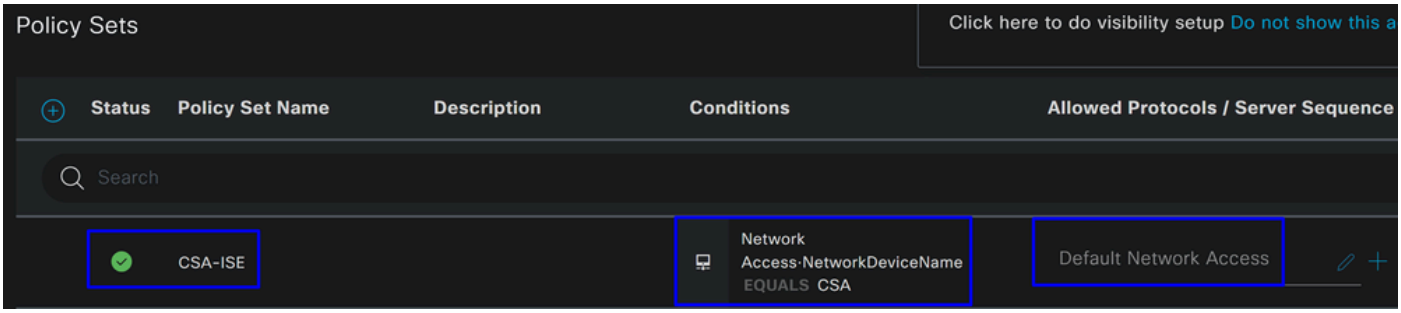
- Om de Voorwaarden te creëren, klik op Click to add an attribute
- Klik op de **Network Device** knop
- Klik onder de opties erachter op **Network Access - Network Device Name** optie
- Schrijf onder de stap **Network Device** Onder de optie Gelijk de naam van de gebruiker, Configureer de netwerkapparatenlijst

- Klik op de knop **Save**

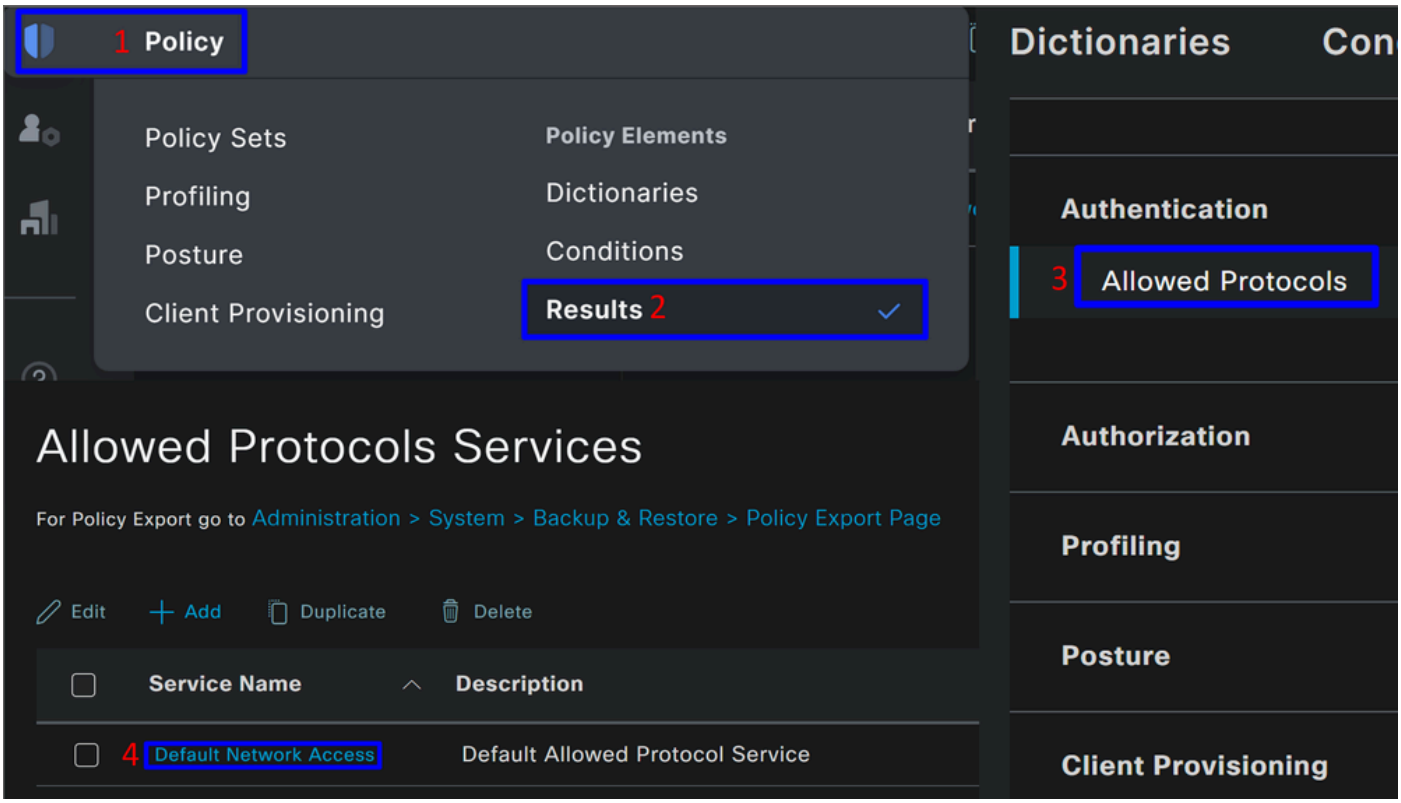


Dit beleid keurt alleen het verzoek van de bron goed CSA om door te gaan met de **Authentication** en **Authorization** installatie onder de reeks beleid **CSA-ISE**, en verifieert ook de toegestane protocollen gebaseerd op de **Default Network Access** voor de toegestane protocollen.

Het resultaat van het gedefinieerde beleid moet zijn:



- Om het **Default Network Access Protocols** toegestane te verifiëren, gaat u verder met de volgende instructies:
    - Klik opPolicy > Results
        - Klik op **Allowed Protocols**
        - Klik op **Default Network Access**

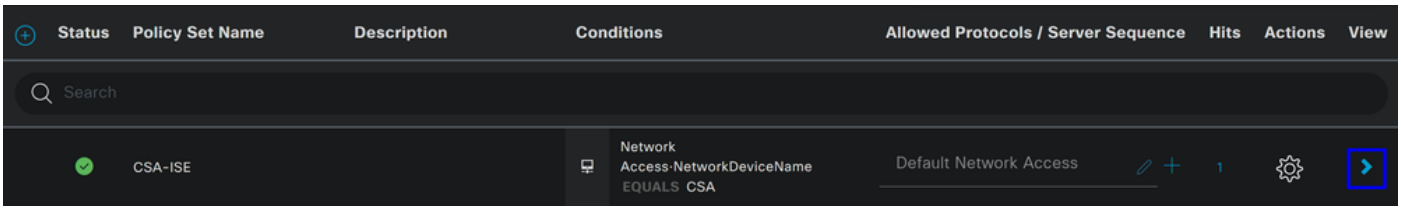


- Vervolgens ziet u alle protocollen die zijn toegestaan op **Default Network Access**

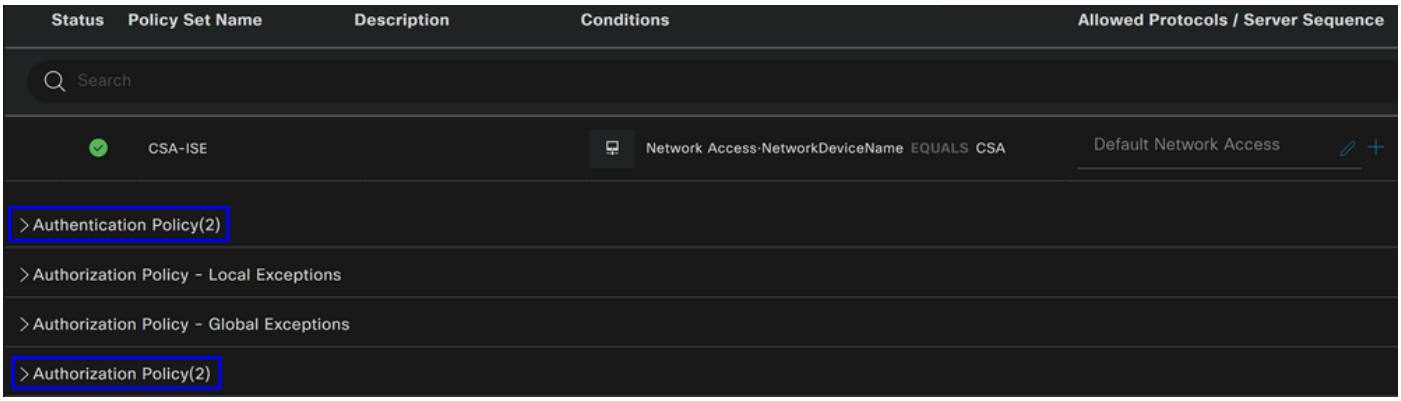
Configuratie van verificatie en autorisatie van beleidsset

Ga als volgt te werk om het Authentication en **Authorization** beleid **Policy Set**onder de map te maken:

- Klik op >



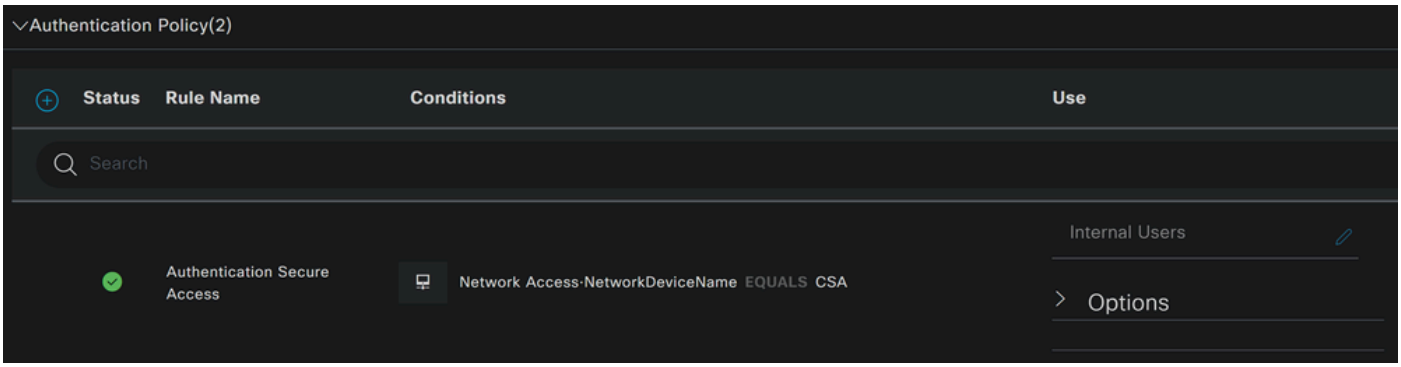
- Daarna ziet u de Authenticationinhoud en het **Authorization** beleid dat wordt weergegeven:



Verificatiebeleid

Voor het verificatiebeleid kunt u op vele manieren configureren. In dit geval ziet u een beleid voor het apparaat dat is gedefinieerd in de stap Lijst met netwerkapparaten configureren en controleert u de verificatie op basis van specifieke criteria:

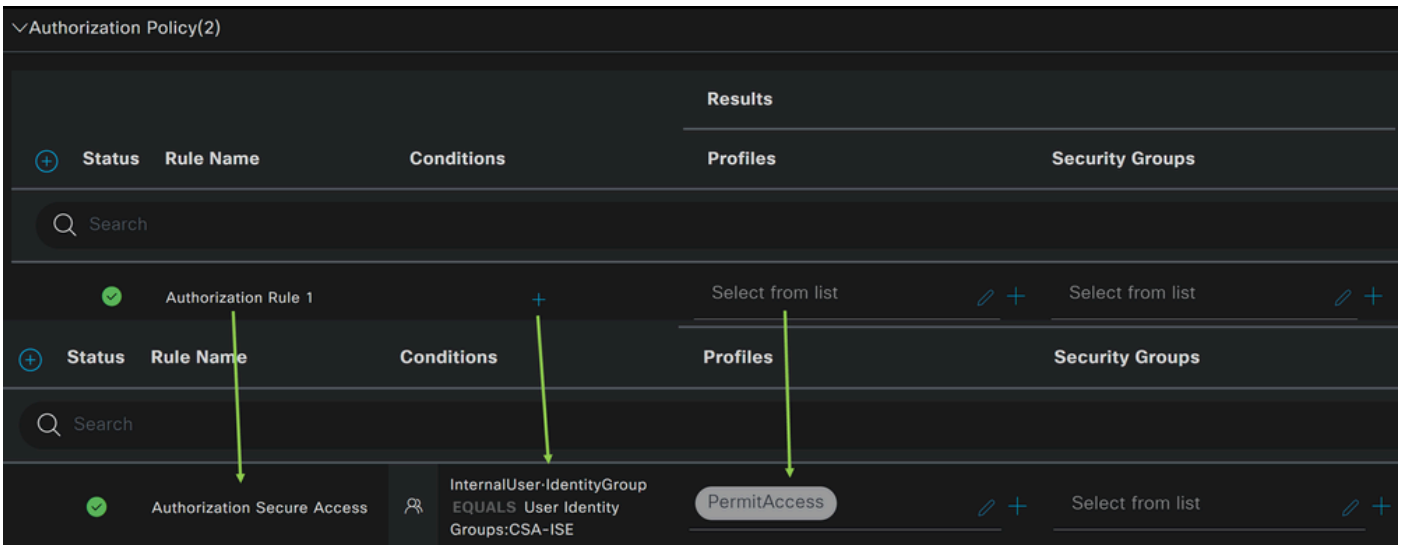
- Gebruikers die zijn geverifieerd via de computer **Network Device CSA** hebben een verificatie voltooid of geweigerd.



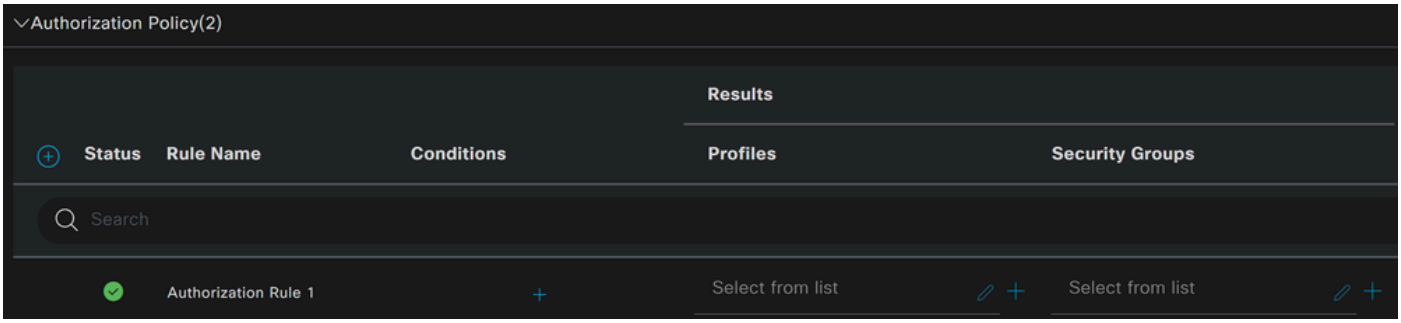
Het beleid is hetzelfde beleid dat is gedefinieerd onder de stap Reeks beleid configureren.

Vergunningsbeleid

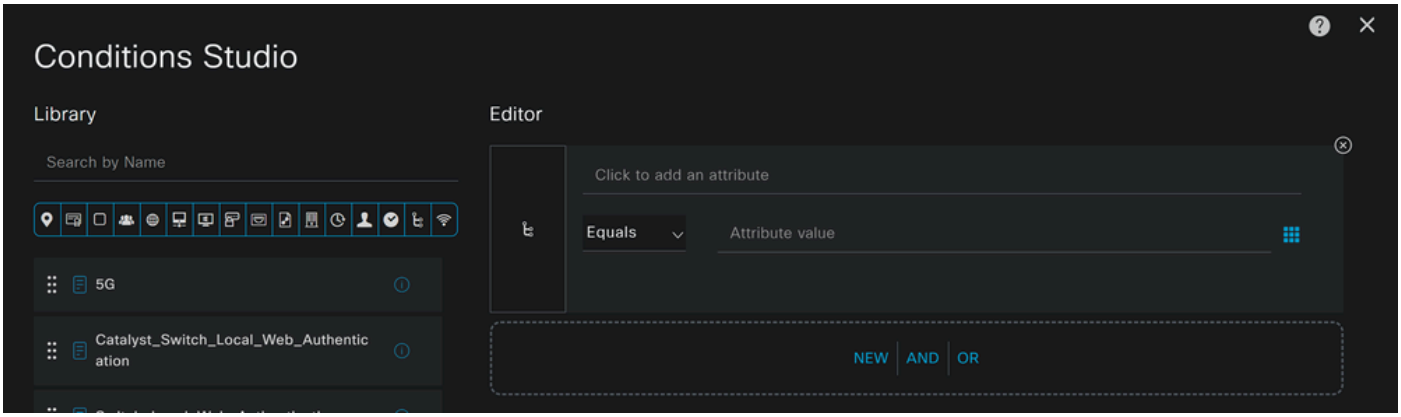
U kunt het autorisatiebeleid op vele manieren configureren. In dit geval, autoriseer alleen de gebruikers in de groep die gedefinieerd is in de stap Een groep configureren.Zie het volgende voorbeeld om uw autorisatiebeleid te configureren:



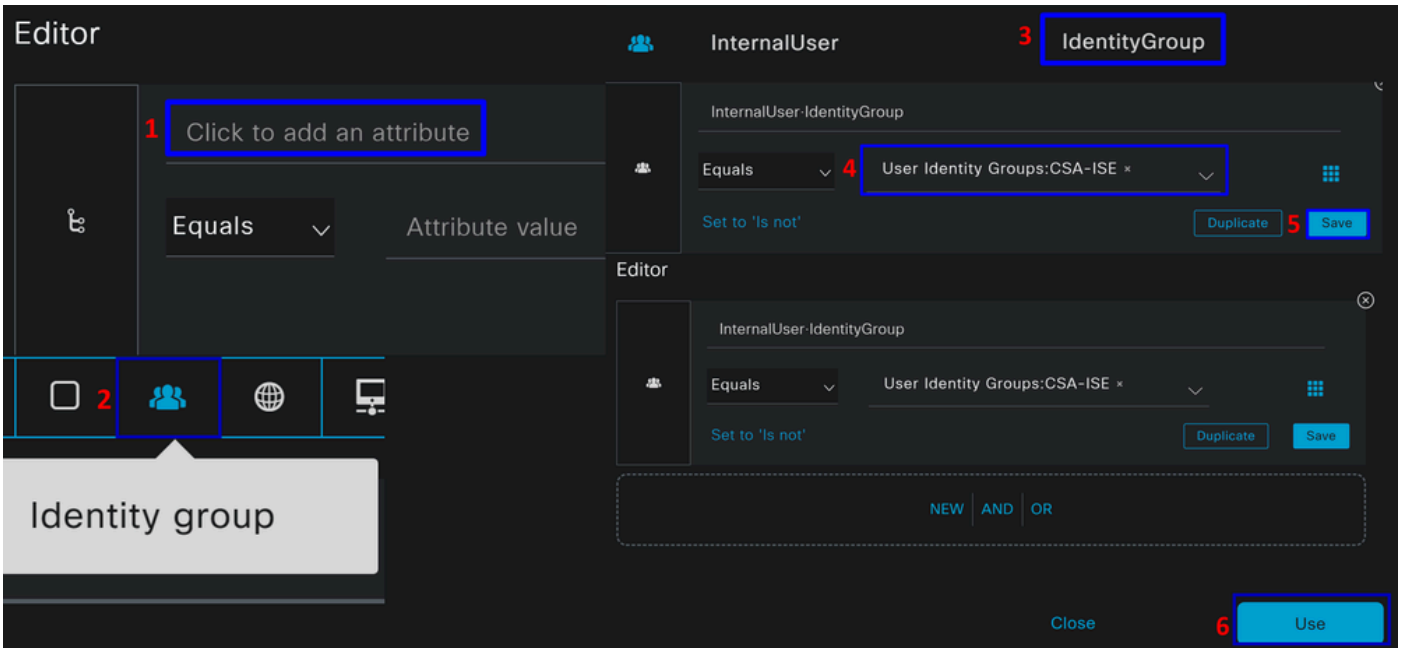
- Klik op **Authorization Policy**
- Klik op om het beleid voor autorisatie als volgt + te definiëren:



- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt, kunt u het autorisatiebeleid gemakkelijk herkennen
- Klik op het **Condition**veld +
- Onder **Condition Studio**, vindt u de informatie:

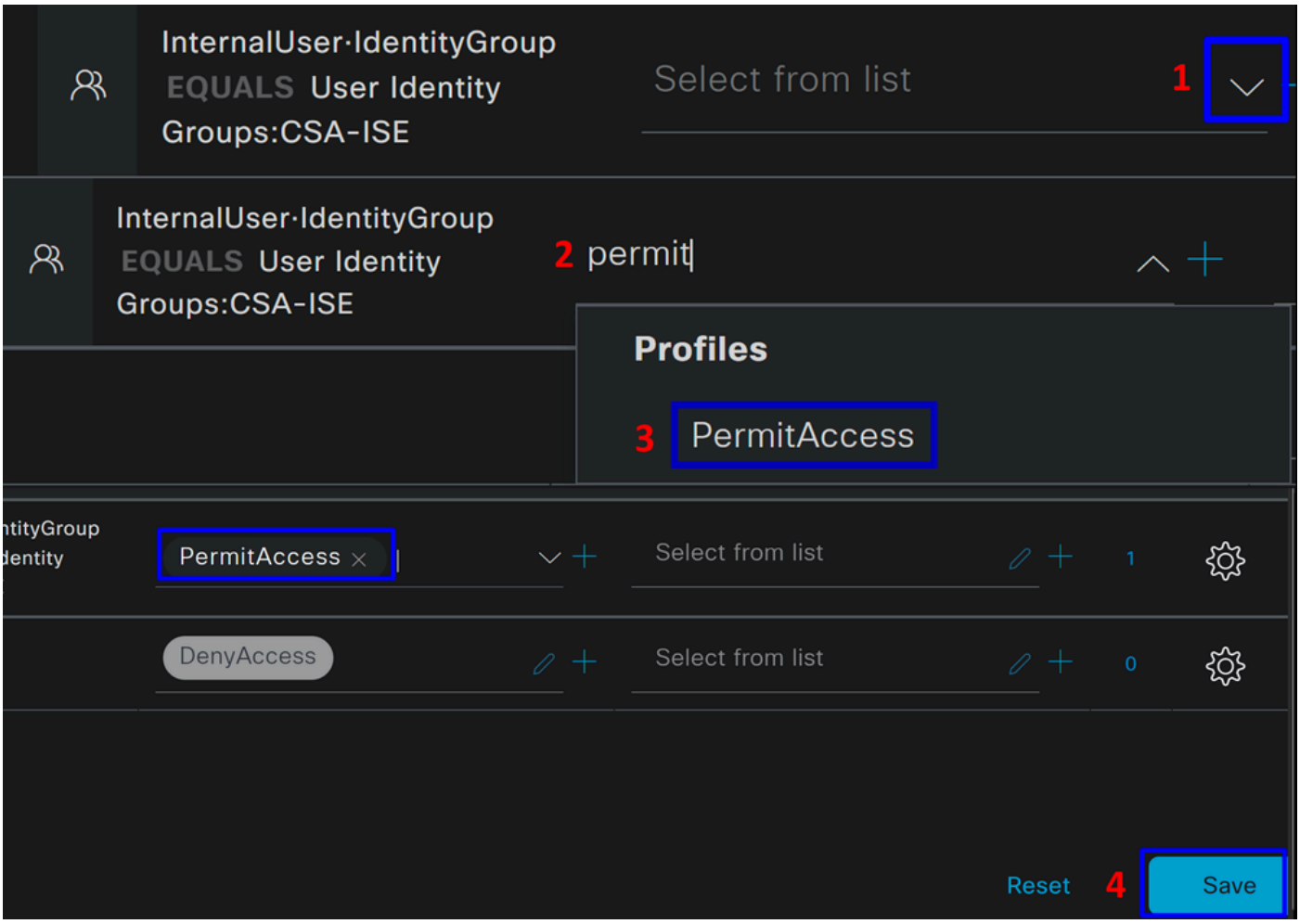


- Om de Voorwaarden te creëren, klik op Click to add an attribute
- Klik op de **Identity Group** knop
- Klik onder de achterliggende opties op **Interne Gebruiker - IdentityGroup** optie
- Gebruik onder de **Equals** optie de vervolgkeuzelijst om de **Group** goedgekeurde verificatiestap in de stap te vinden, een groep configureren
- Klik op de knop **Save**
- Klik op de knop **Use**



Daarna moet u de **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Klik onder het **Authorization Policy**kopje op de vervolgkeuzelijst **Profiles**
- Vergunning zoeken
- Kiezen **PermitAccess**
- Klik op de knop Save



Daarna hebt u uw **Authentication Authorization** beleid bepaald. Verifiëren om te verifiëren of de gebruiker verbinding maakt zonder een probleem en of u de logbestanden op Secure Access en ISE kunt zien.

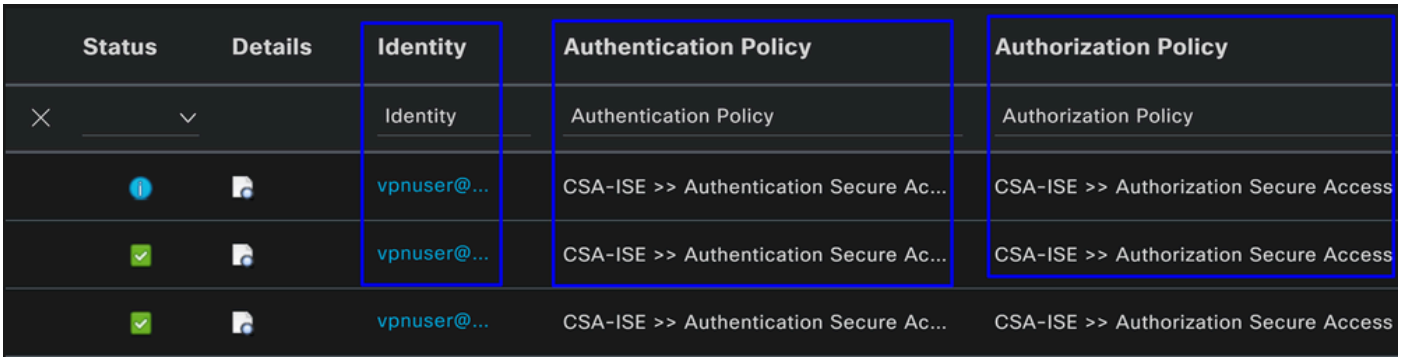
Als u verbinding wilt maken met VPN, kunt u het profiel gebruiken dat op Secure Access is gemaakt en verbinding maken via Secure Client met het ISE-profiel.

- **Hoe wordt het logbestand weergegeven in Secure Access als de verificatie wordt goedgekeurd?**
  - Naar het Secure Access Dashboard navigeren
  - Klik op **Monitor > Remote Access Log**

28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
vpn user (vpnuser@ciscosspt.es)	Connected		192.168.50.2	151.248.21.152	ISE_CSA

- **Hoe wordt het logbestand weergegeven in ISE als de verificatie wordt goedgekeurd?**
    - Naar het **Cisco ISE Dashboard**
        - Klik op **Operations > Live Logs**



Lokale of actieve mapgebruikers van RADIUS configureren

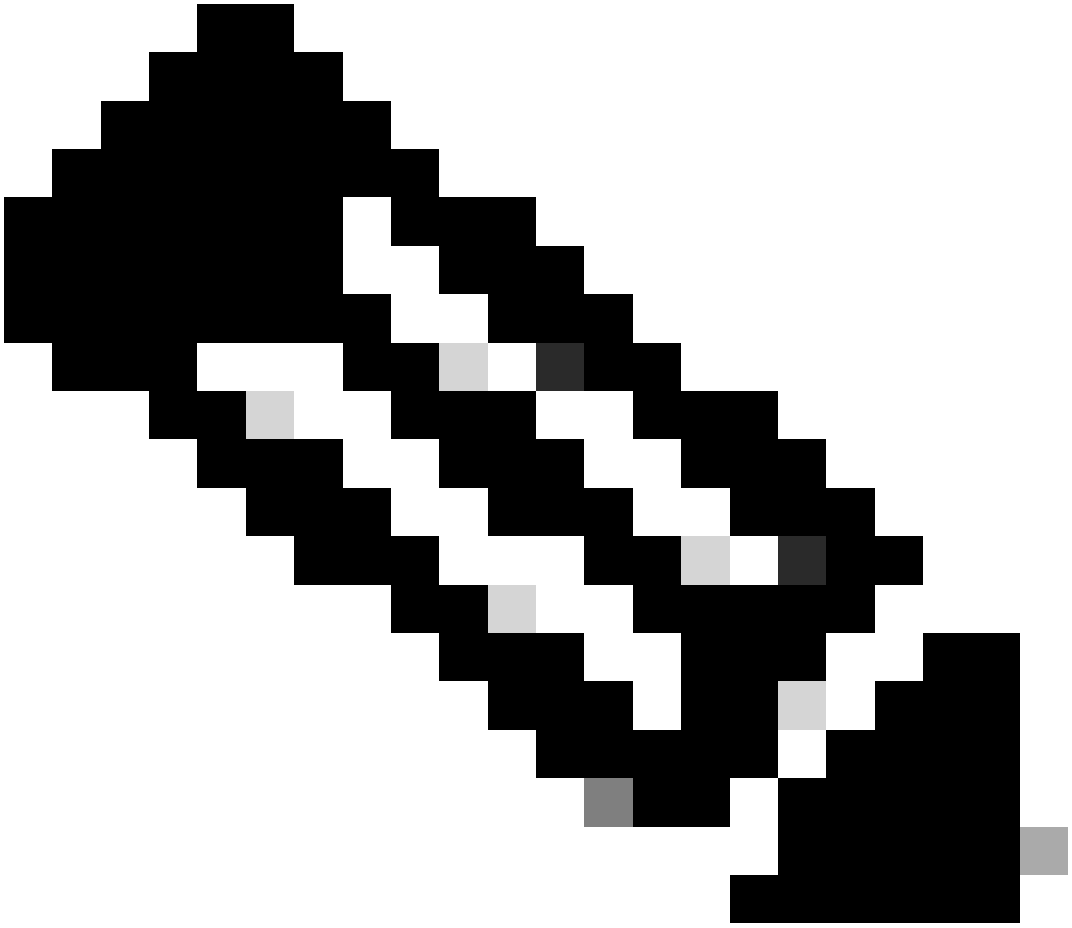
ISE-houding configureren

In dit scenario, creeer de configuratie om endpointnaleving te verifiëren alvorens toegang tot interne middelen te verlenen of te ontkennen.

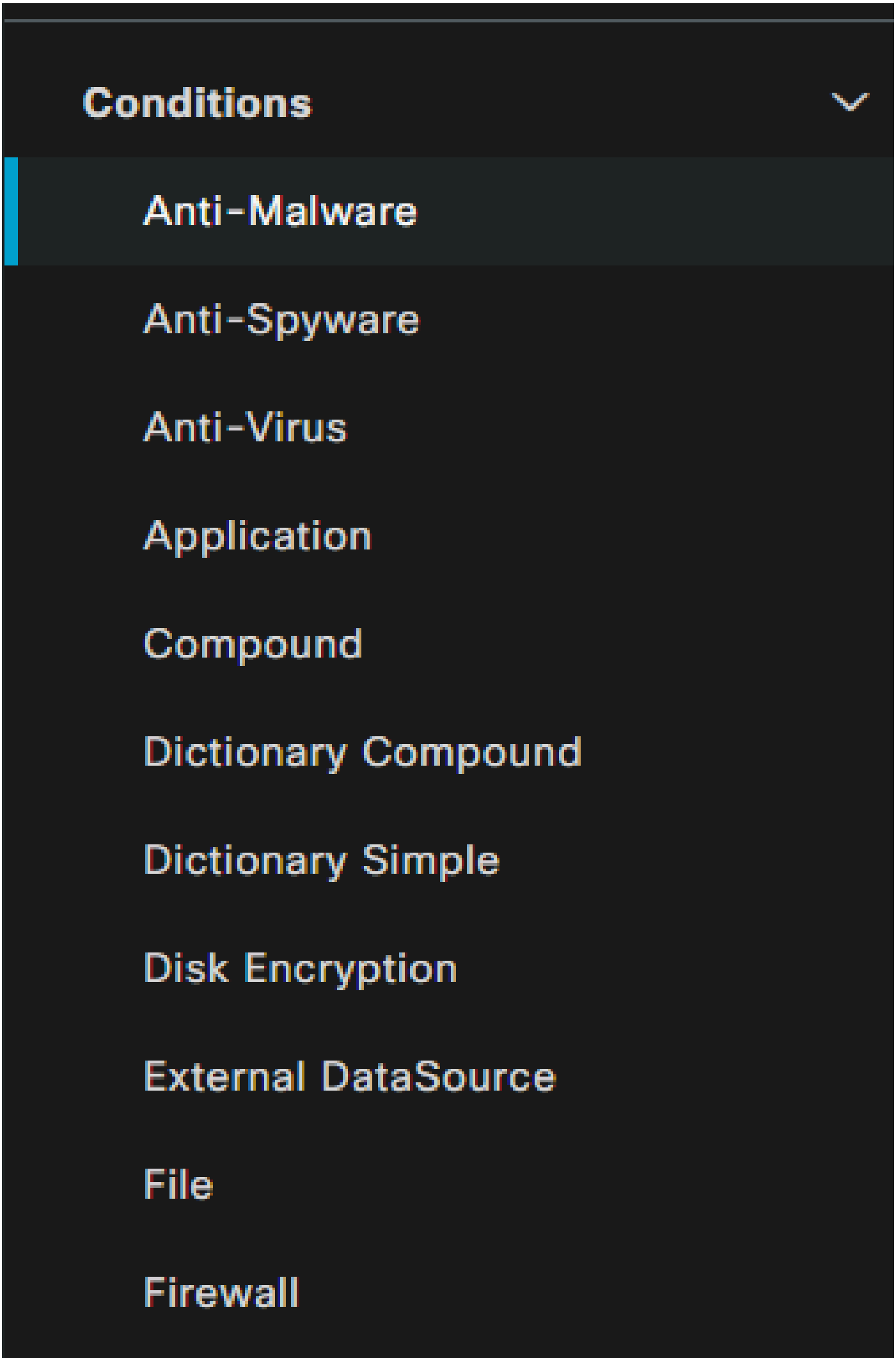
Ga verder naar de volgende stappen om het beeld te configureren:

Posteringvoorwaarden configureren

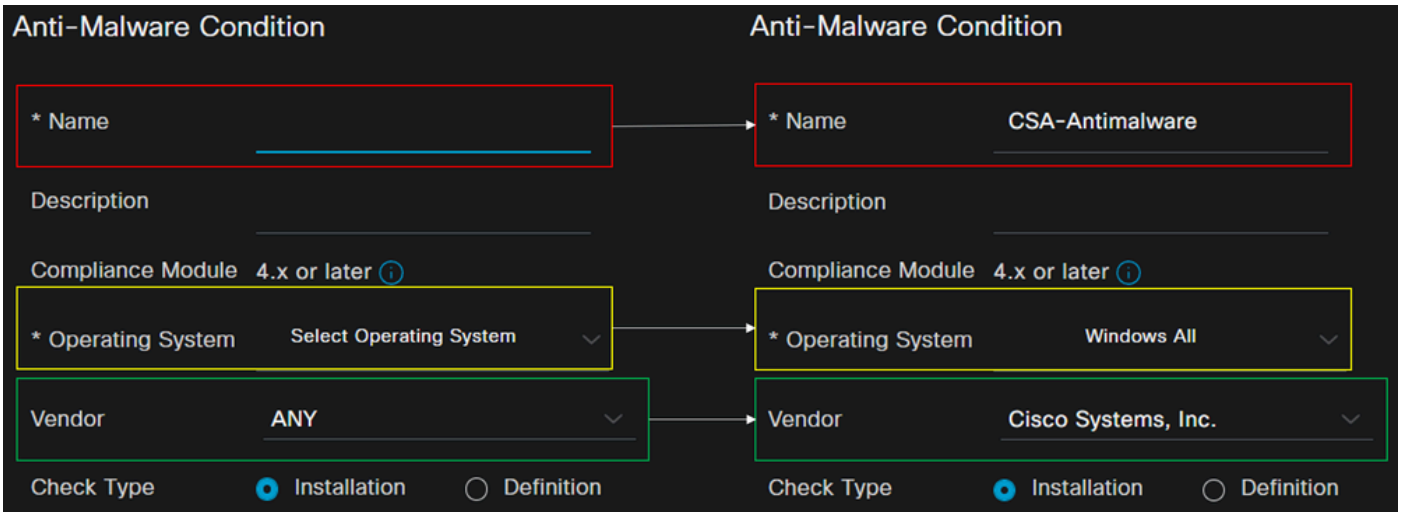
- Naar uw ISE-dashboard navigeren
- Klik op **Work Center > Policy Elements > Conditions**
- Klik op **Anti-Malware**



Opmerking: Daar vindt u veel opties om de positie van uw apparaten te verifiëren en de juiste beoordeling te maken op basis van uw interne beleid.

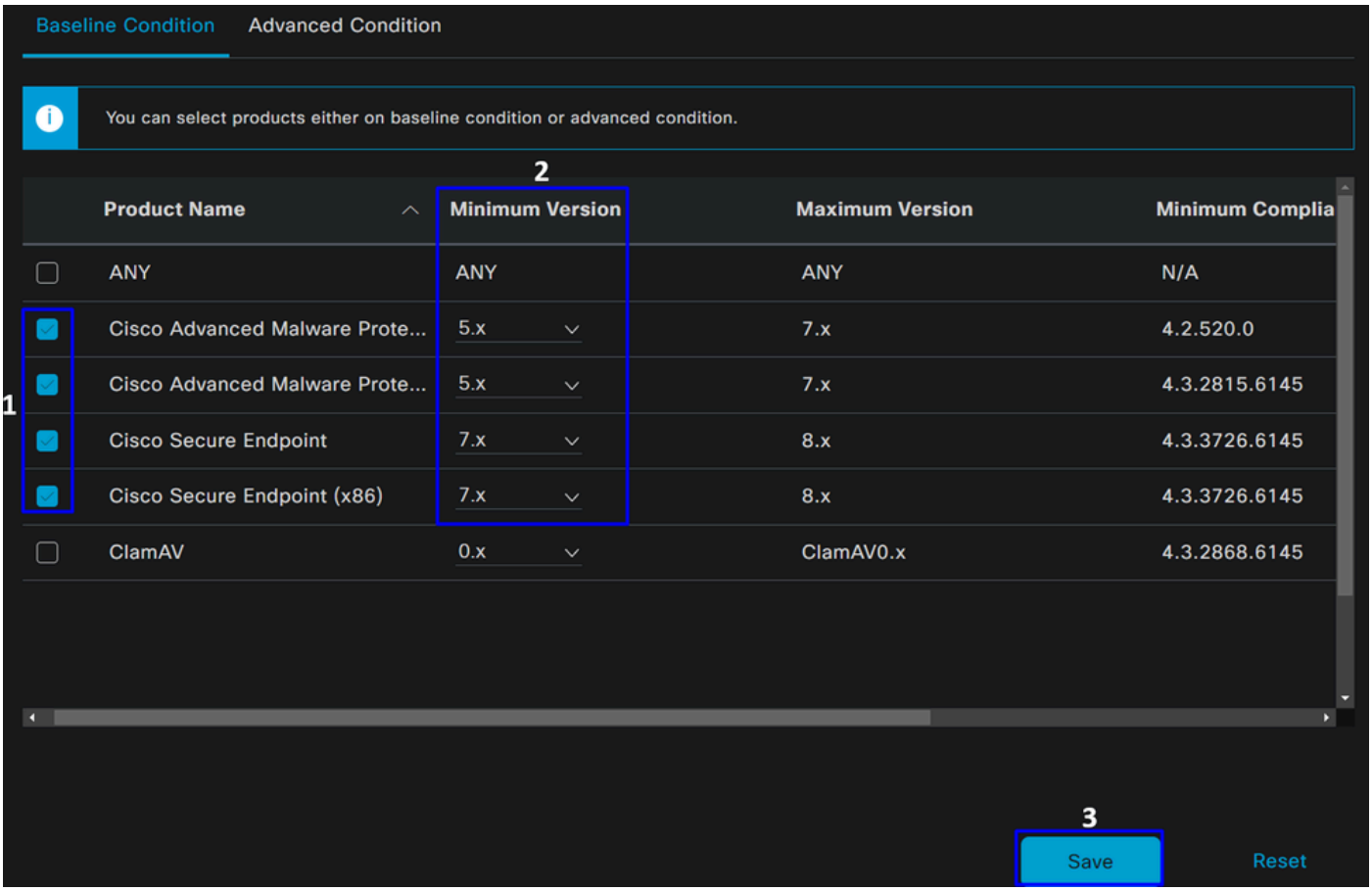

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

Anti-Malware Condition om de antivirus installatie op het systeem te detecteren; u kunt ook de versie van het besturingssysteem kiezen indien nodig.



- **Name**: Gebruik een naam om de anti-malware voorwaarde te herkennen
- **Operating System**: Kies het besturingssysteem dat u onder de voorwaarde wilt plaatsen
- **Vendor**: Kies een leverancier of een willekeurige
- **Check Type**: U kunt controleren of de agent is geïnstalleerd of dat de definitie van die optie correct is.

- Bijvoorbeeld **Products for Selected Vendor**, u configureren wat u wilt verifiëren over de antimalware op het apparaat.

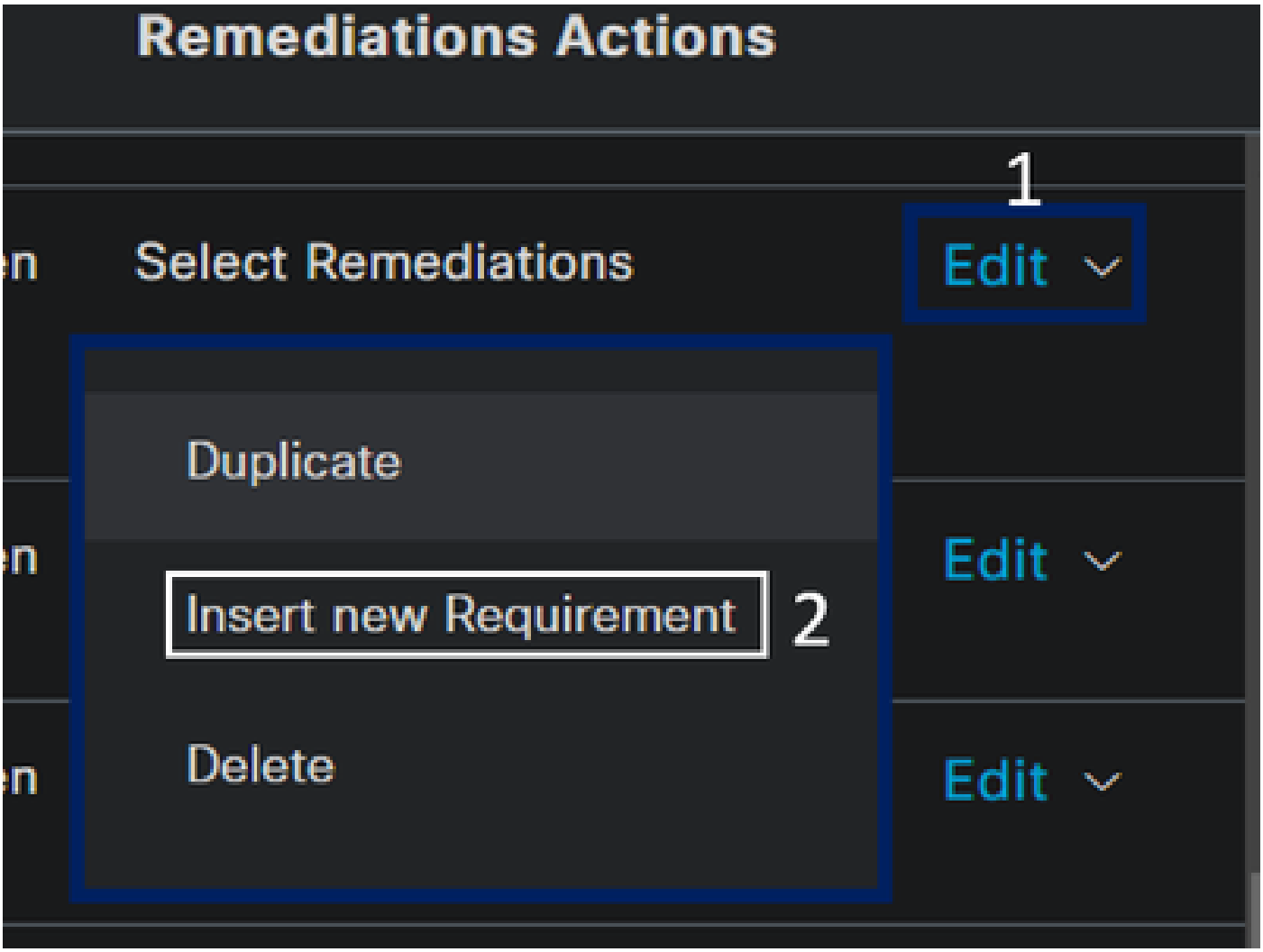


- Vink het aanvinkvakje aan voor de voorwaarden die u wilt evalueren
- Configureer de minimumversie om te verifiëren
- Klik op Opslaan om door te gaan met de volgende stap

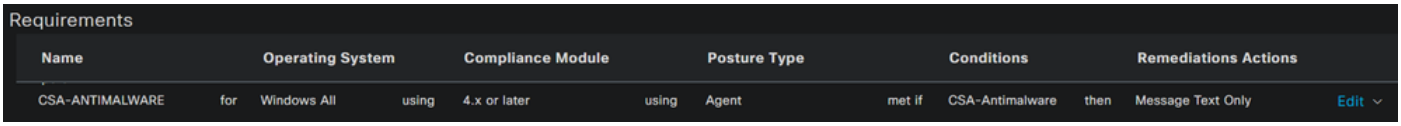
Zodra u het configureert, kunt u doorgaan met de stap, **Configure Posture Requirements**.

Houdingsvereisten configureren

- Naar uw ISE-dashboard navigeren
- Klik op **Work Center > Policy Elements > Requeriments**
- Klik op een **Edit** van de vereisten en klik op **Insert new Requirement**



- Onder de nieuwe vereiste moet u de volgende parameters configureren:

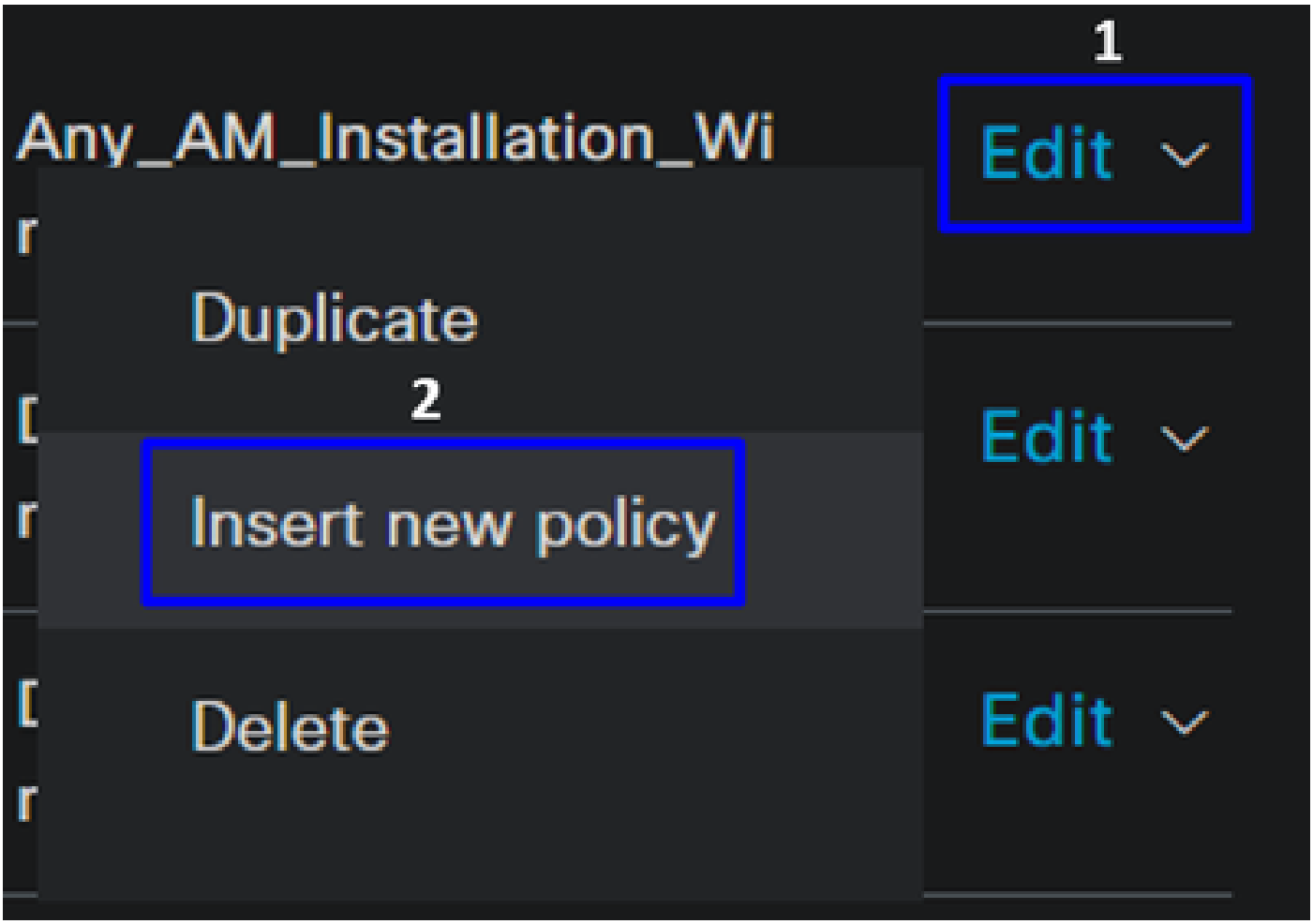


- **Name**: Stel een naam in om de antimalwarevereiste te herkennen
- **Operating System**: Kies het besturingssysteem dat u kiest onder de conditiestap, Besturingssysteem
- **Compliance Module**: U moet ervoor zorgen om dezelfde compliance module te selecteren die u onder de conditiestap heeft, Anti-Malware Condition
- **Posture Type**: Agent kiezen
- **Conditions**: Kies de voorwaarde of voorwaarden die u onder de stap hebt gecreëerd, stel voorwaarden configureren
- **Remediations Actions**: Kies **Message Text Only** voor dit voorbeeld, of als u een andere remediërende actie hebt, gebruik het
- Klik op de knop **Save**

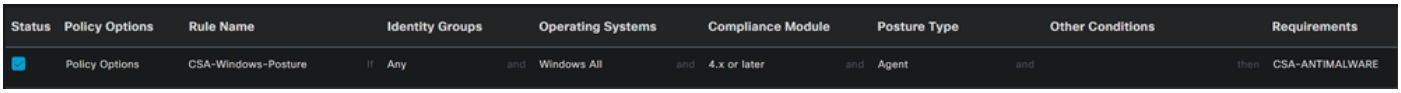
Zodra u het vormt, kunt u met de stap te werk gaan, **Configure Posture Policy**

Posturebeleid configureren

- Naar uw ISE-dashboard navigeren
- Klik op **Work Center > Posture Policy**
- Klik op een **Edit** van de beleidsregels en klik op **Insert new Policy**



- Configureer onder het nieuwe beleid de volgende parameters:



- **Status**: Vink het selectievakje aan om het beleid in te schakelen
- **Rule Name**: Configureer een naam om het geconfigureerde beleid te herkennen
- **Identity Groups**: Kies de identiteiten die u wilt evalueren

- **Operating Systems**: Kies het besturingssysteem op basis van de conditie en de vereiste die voor is geconfigureerd
- **Compliance Module**: Kies de compliance module op basis van de conditie en de vereiste die daarvoor is geconfigureerd
- Posture Type: Agent kiezen
- **Requeriments**: Kies de vereisten die bij de stap zijn ingesteld, stel vereisten
- Klik op de knop **Save**

Clientprovisioning configureren

Om de gebruikers van de module van ISE te voorzien, vorm de cliëntlevering om de machines met de module van de houding van ISE uit te rusten. Hiermee kunt u de houding van de machines verifiëren nadat de agent is geïnstalleerd. Om met dit proces door te gaan, volgt u de volgende stappen:

Navigeer naar uw ISE Dashboard.

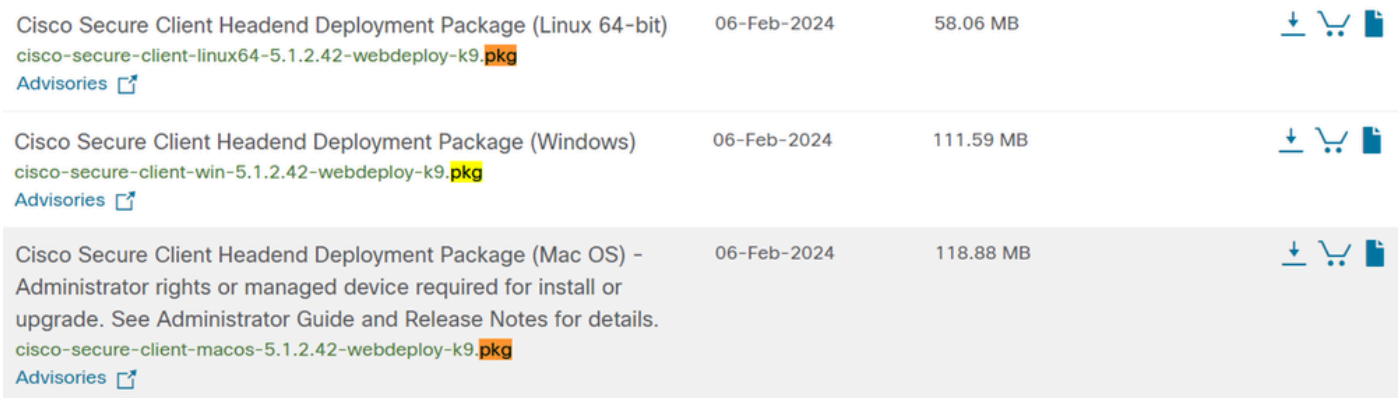
- Klik op **Work Center > Client Provisioning**
- Kiezen **Resources**

Er zijn drie dingen die u moet configureren onder client provisioning:

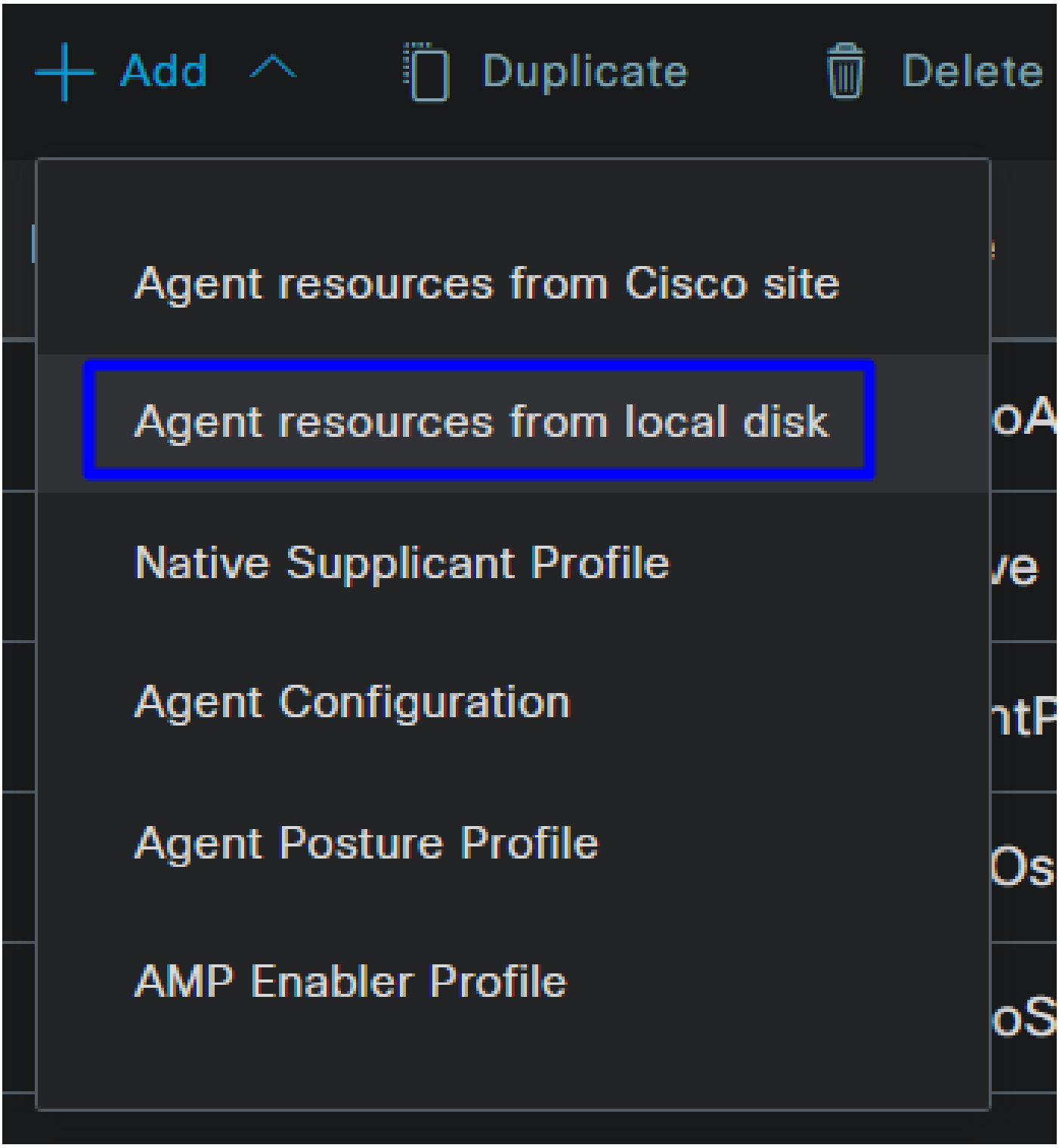
Te configureren bronnen	Beschrijving
1. **Agent Resources**	Secure Client-webprovisioningpakket
2. **Compliance Module**	Cisco ISE-nalevingsmodule
3. **Agent Profile**	Beheer van het provisioningprofiel.
3. **Agent Configuration**	Definieer welke modules zijn voorzien door het provisioningportal op te zetten met behulp van het Agent-profiel en de Agent-bronnen.

Step 1 Downloaden en uploaden van Agent-bronnen

- Als u een nieuwe agent-resource wilt toevoegen, navigeert u naar het Cisco Download Portal en downloadt u het web-implementatiepakket; het web-implementatiebestand moet een .pkg-indeling hebben.

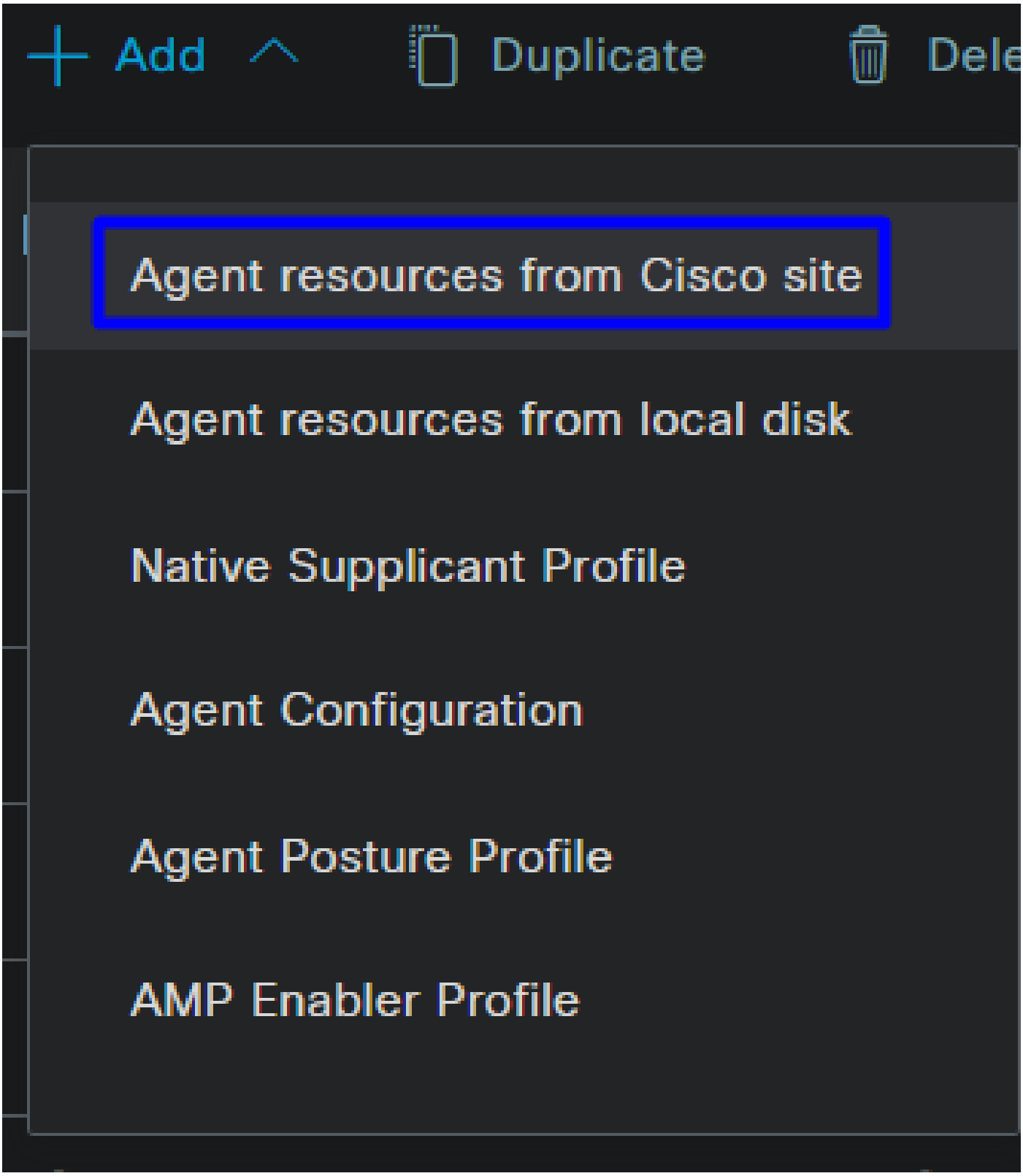


- Klik op + Add > Agent resources from local disk en upload de pakketten

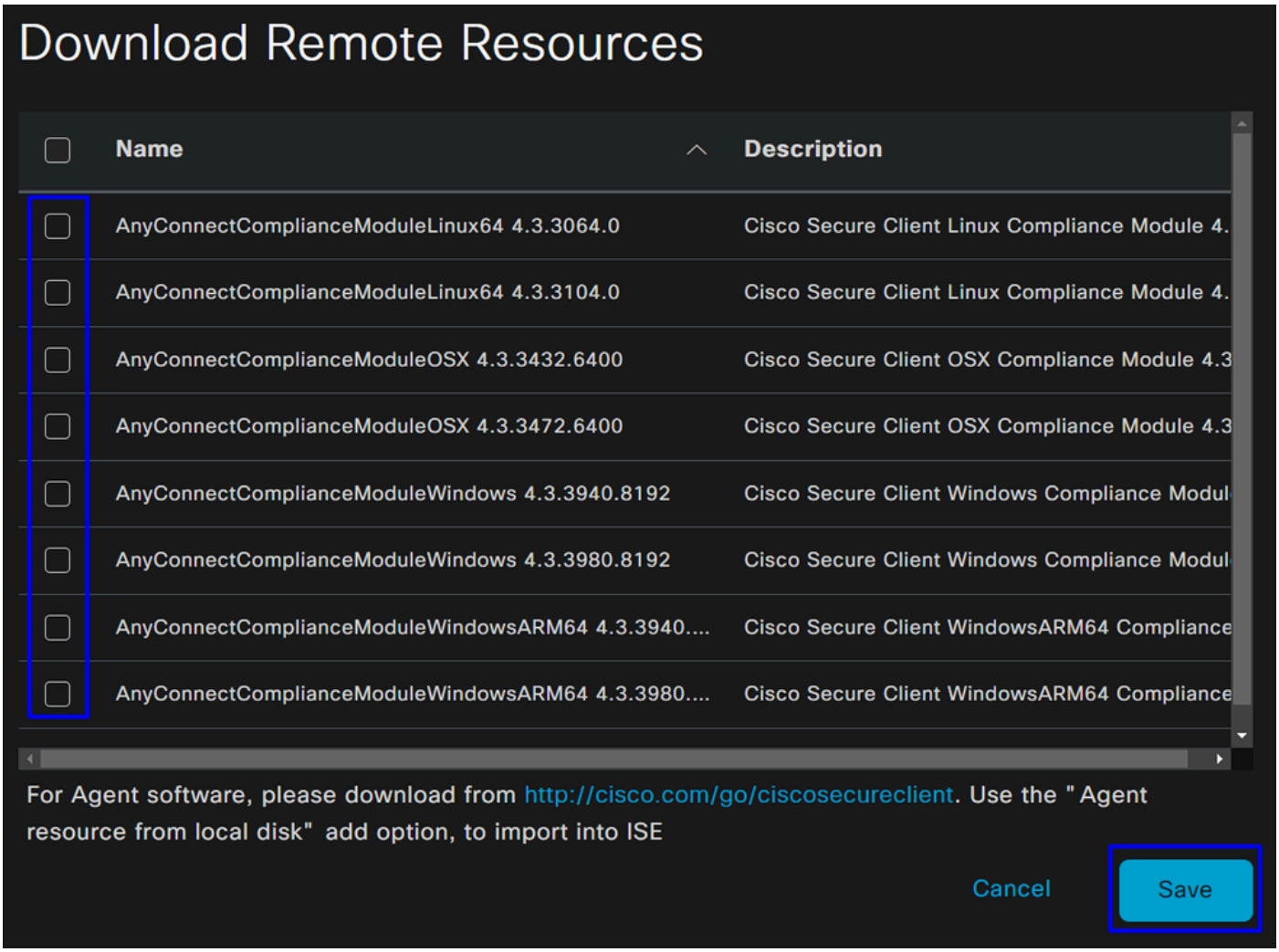


Step 2 Download de compliance module

- Klik op + Add > Agent resources from Cisco Site

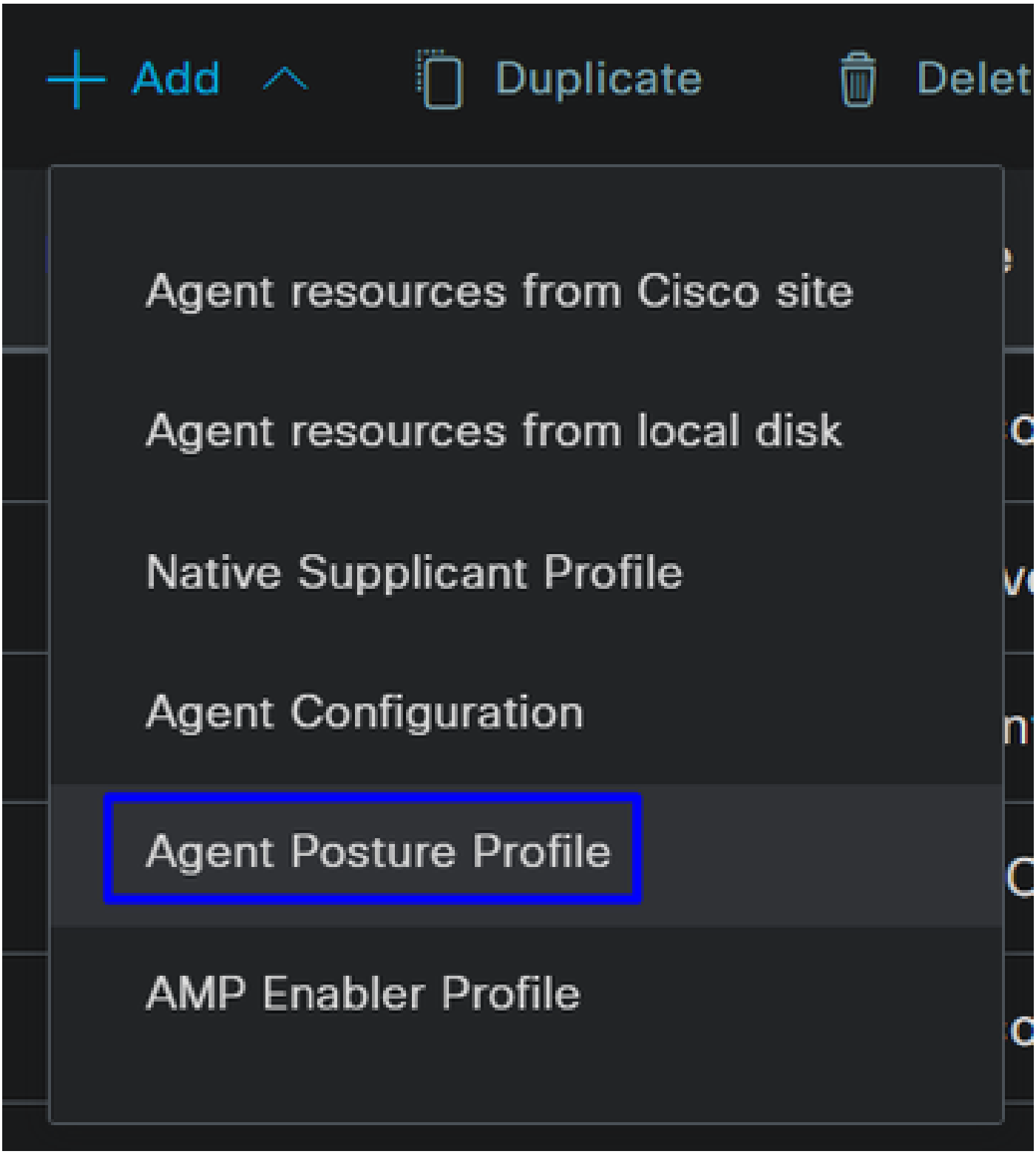


- Markeer het selectievakje voor elke compliancemodule die nodig is en klik op **Save**

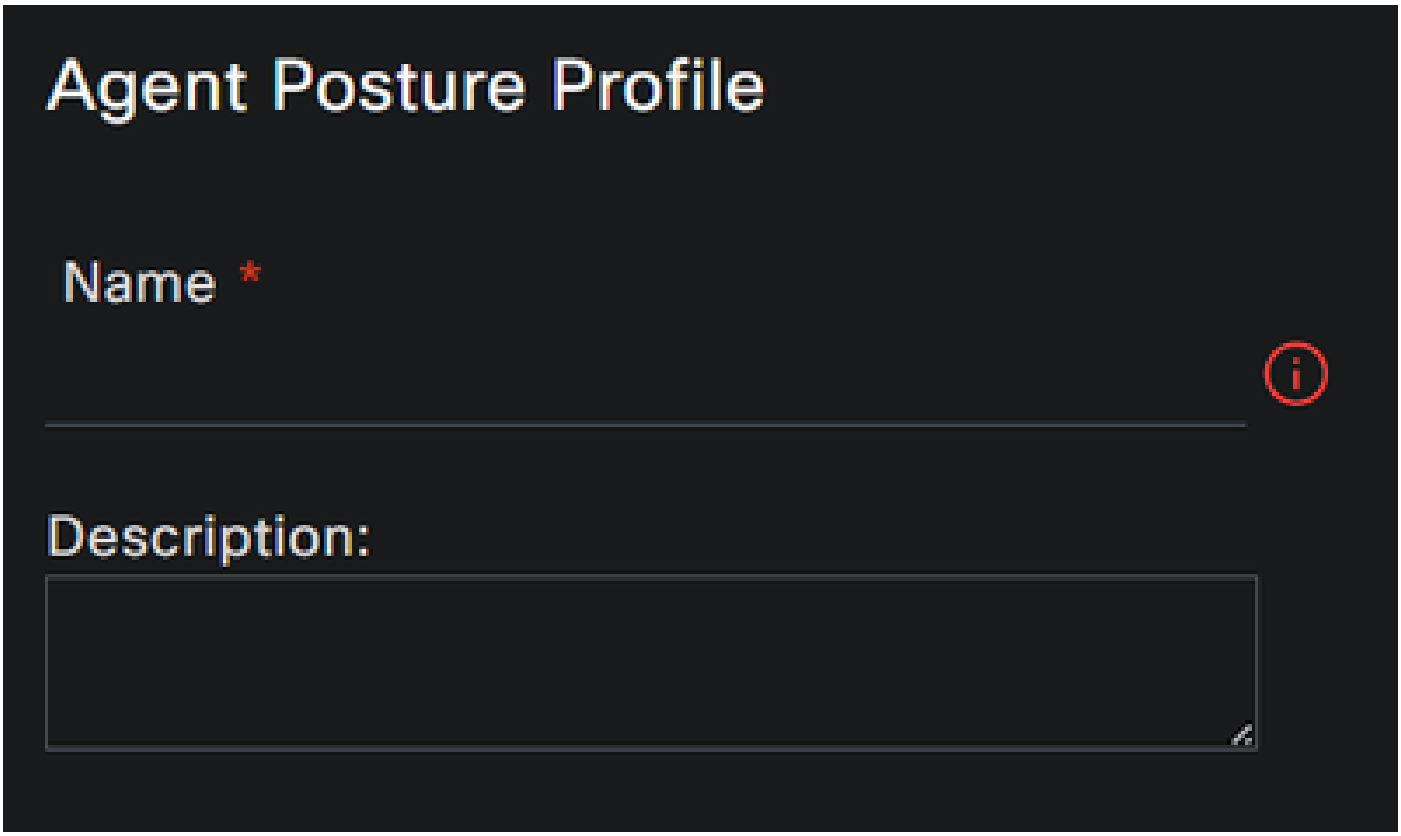


Step 3Het Agent-profiel configureren

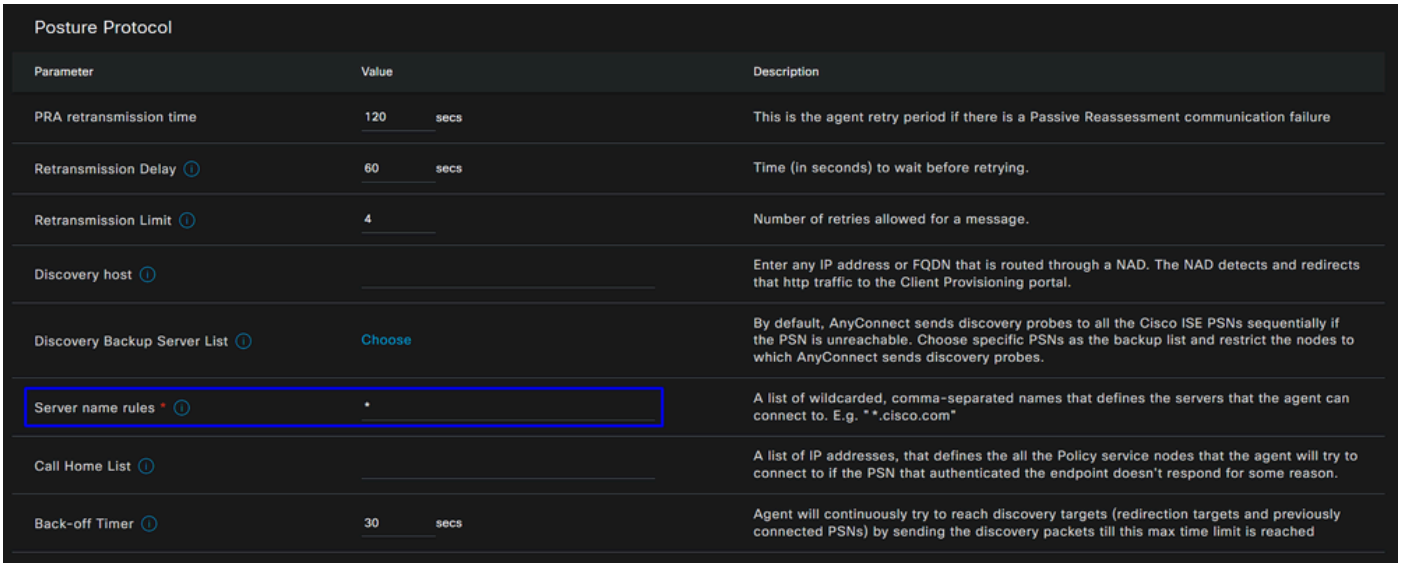
- Klik op + Add > Agent Posture Profile



- Een bestand **Name** maken voor de **Posture Profile**

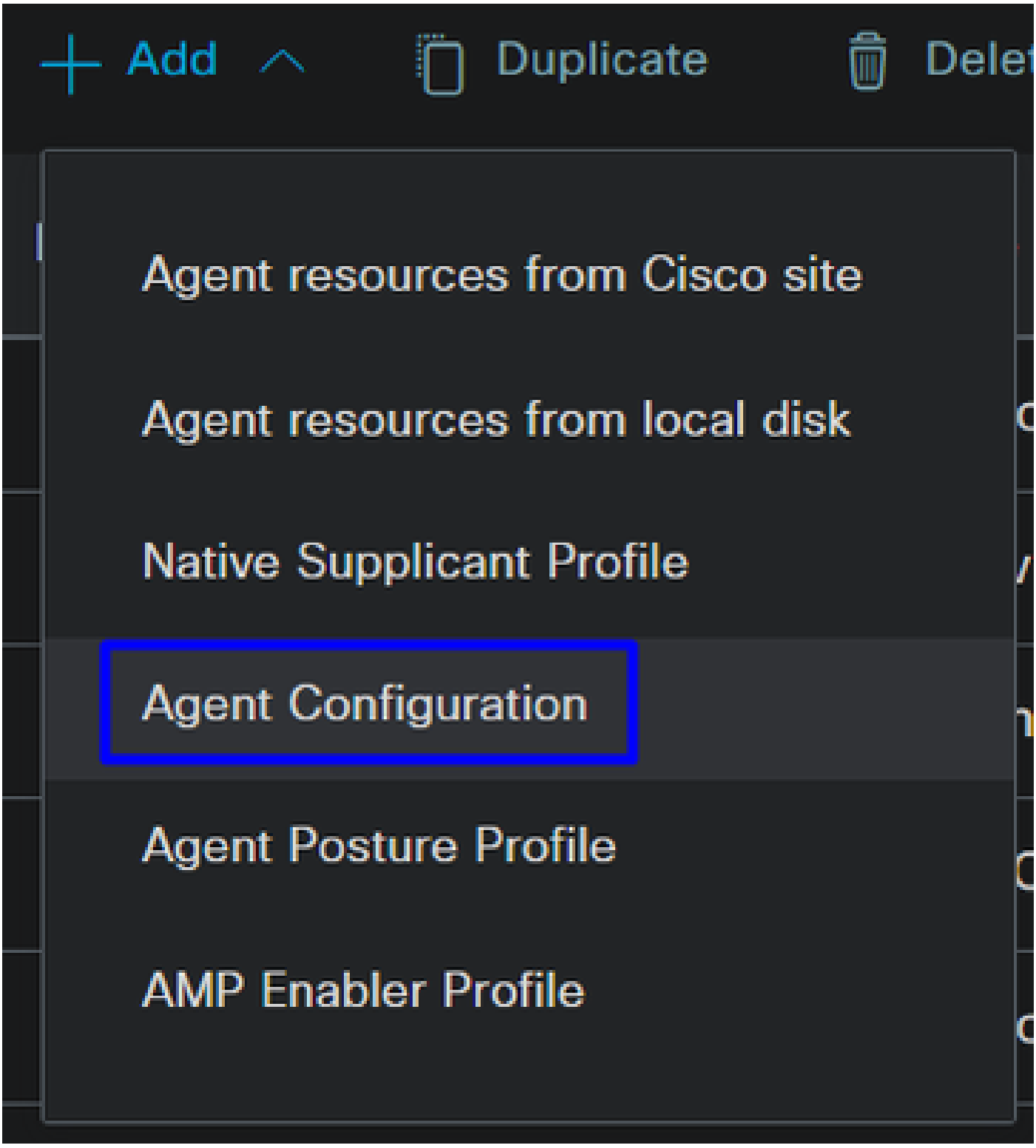


- Zet een handleiding onder Servernaamregels ***** en klik **Save** erna

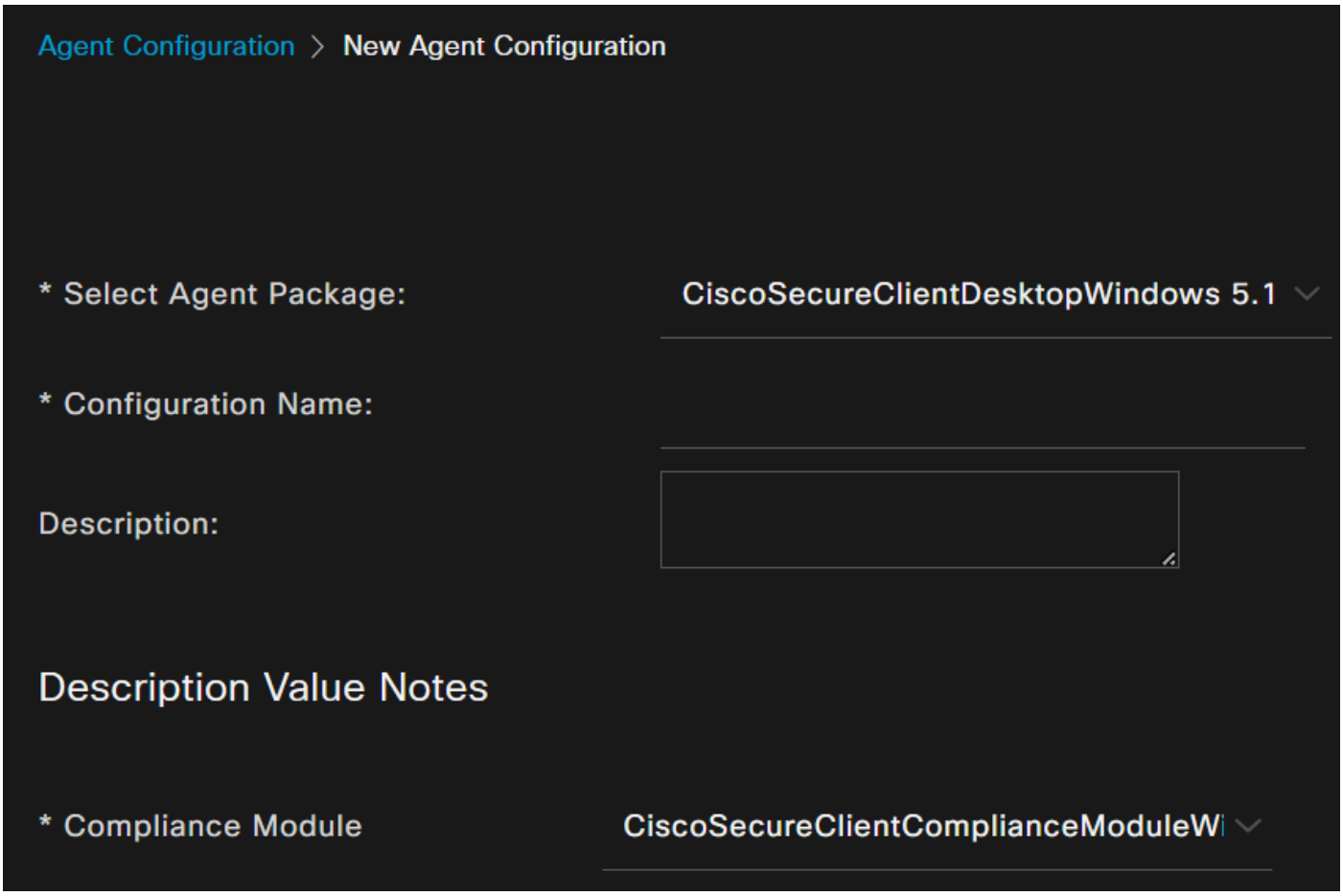


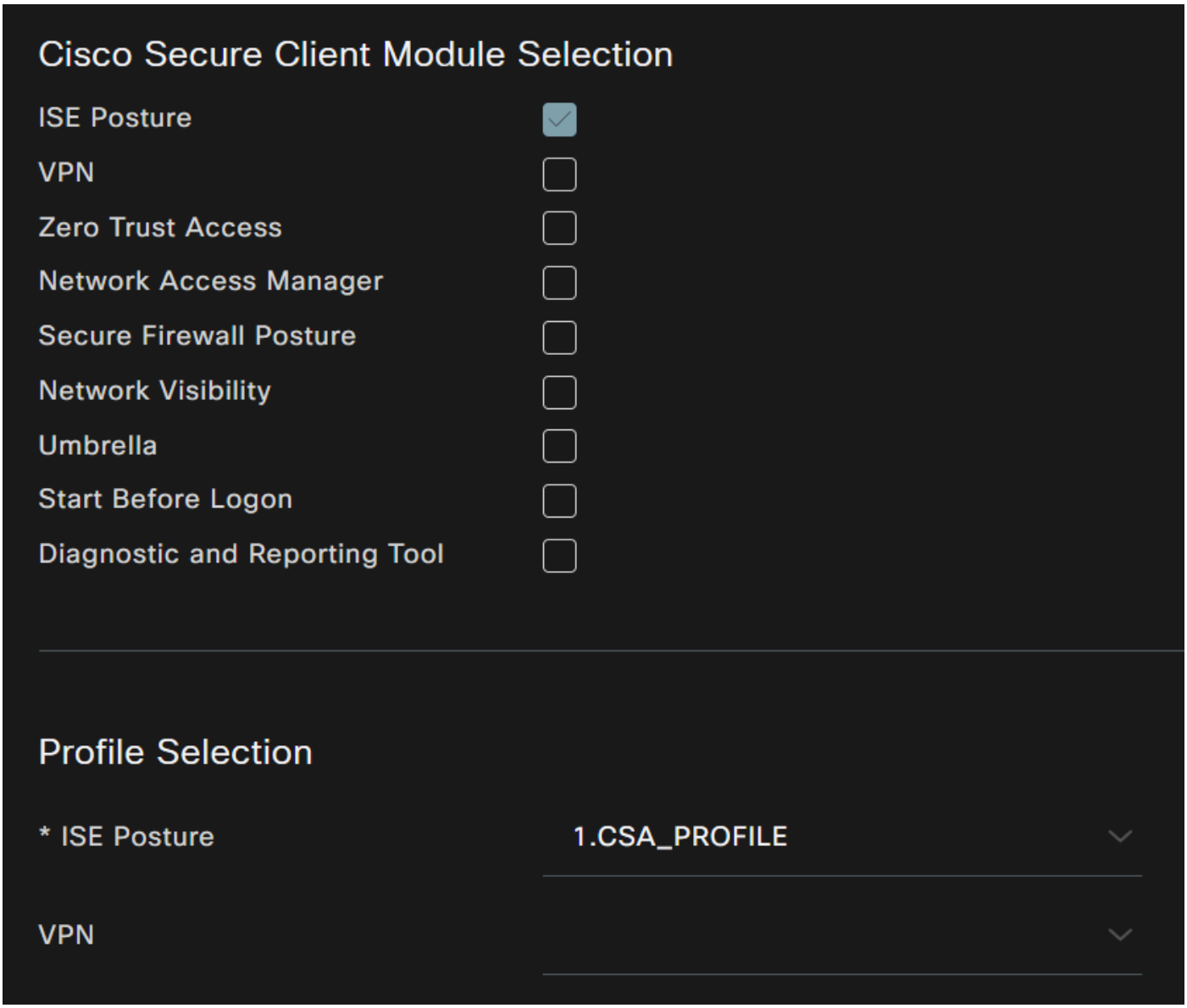
Step 4 De Agent-configuratie configureren

- Klik op + Add > Agent Configuration



- Daarna, vorm de volgende parameters:

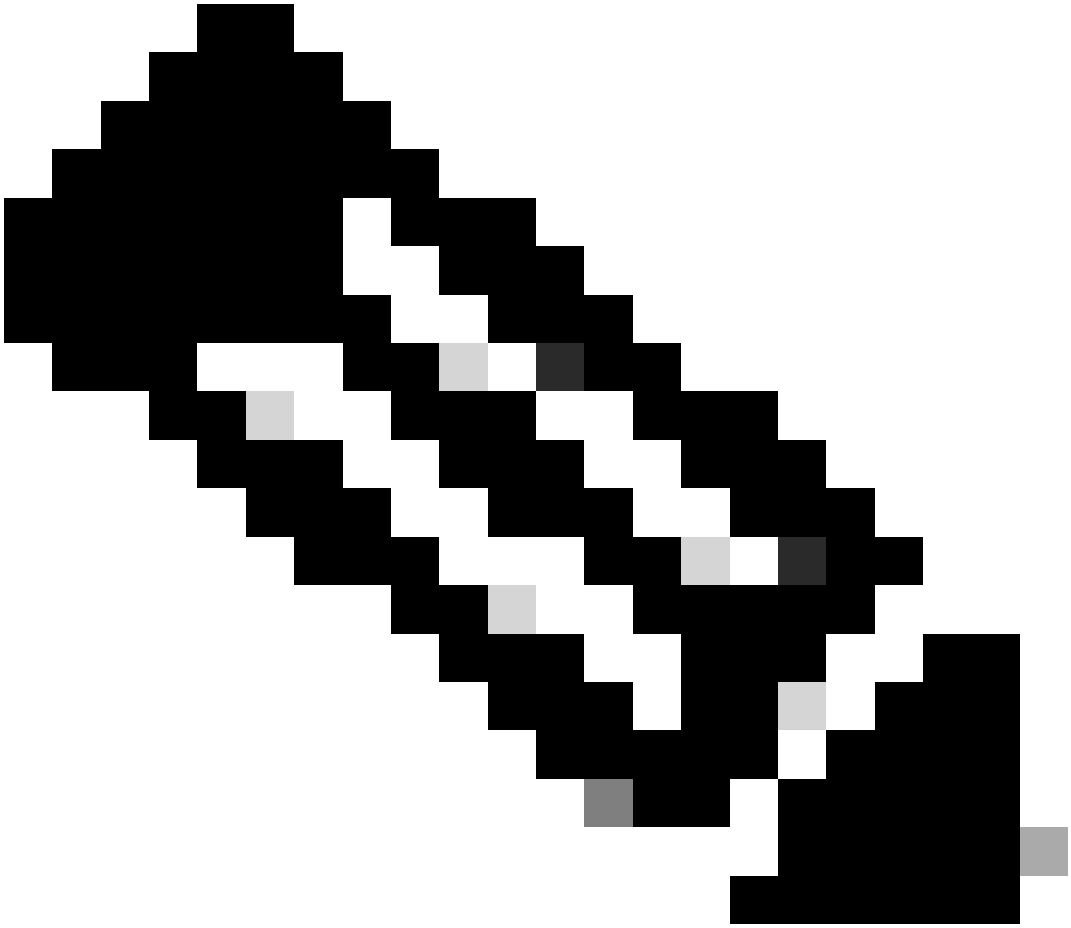

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package : Kies het pakket dat is geüpload in de Stap 1-bronnen voor downloads en uploadagents
- **Configuration Name**: Kies een naam om de **Agent Configuration**
- **Compliance Module**: Kies de Compliance Module die gedownload is op de Step2 Download de compliance module
- Cisco Secure Client Module Selection
    - **ISE Posture**: vink het vakje aan
- **Profile Selection**

- **ISE Posture**: Kies het ISE-profiel dat in stap 3 is geconfigureerd en stel het Agent-profiel in

- Klik op de knop **Save**

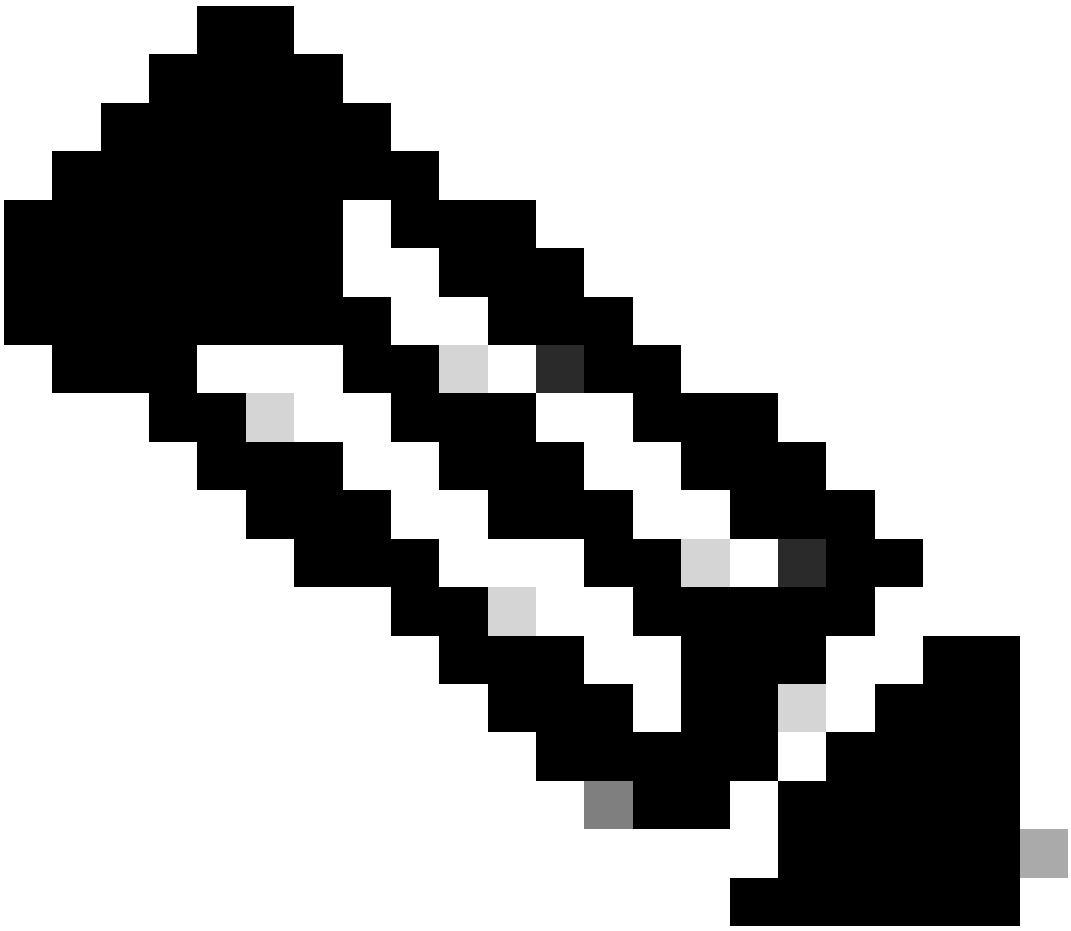


Opmerking: aanbevolen wordt dat elk besturingssysteem, Windows, Mac OS of Linux, één onafhankelijke client-configuratie heeft.

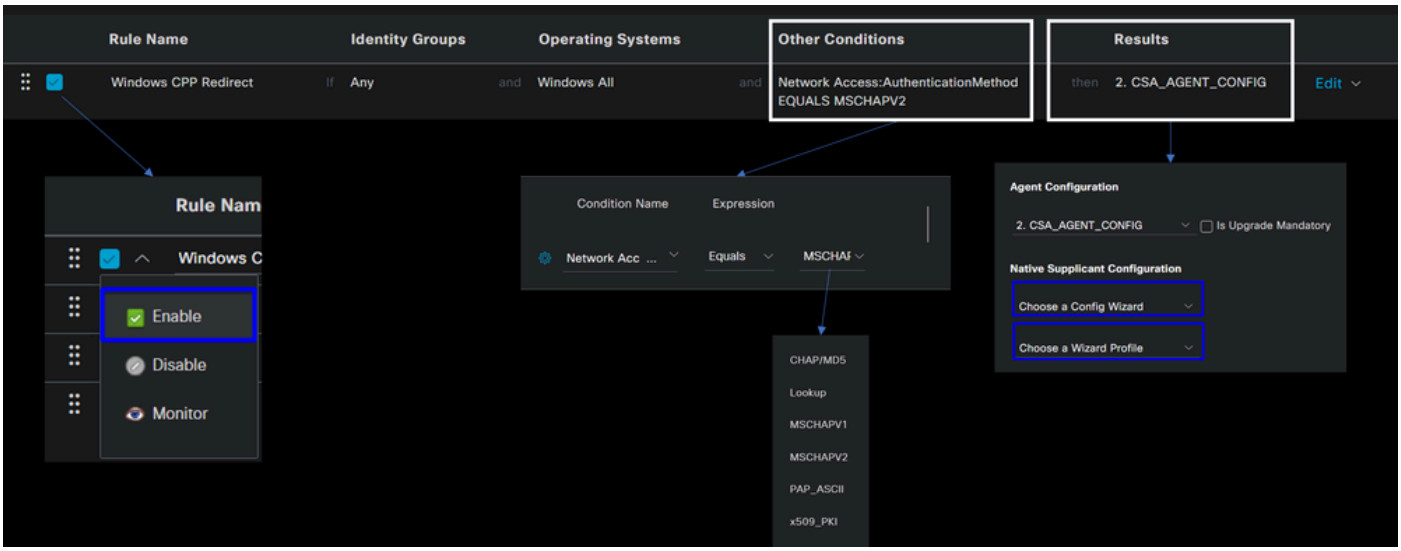
Clientprovisioningbeleid configureren

Om de levering van de houding van ISE en de modules die in de laatste stap worden gevormd toe te laten, moet u een beleid vormen om de levering te maken.

- Naar uw ISE-dashboard navigeren
- Klik op **Work Center > Client Provisioning**



Opmerking: aanbevolen wordt dat elk besturingssysteem, Windows, Mac OS of Linux, één clientconfiguratiebeleid heeft.



- **Rule Name**: Configureer de naam van het beleid op basis van het apparaattype en de selectie van de identiteitsgroep om een eenvoudige manier te hebben om elk beleid te identificeren

- **Identity Groups**: Kies de identiteiten die u wilt evalueren op het beleid

- **Operating Systems**: Kies het besturingssysteem op basis van het agent-pakket dat is geselecteerd in de stap, selecteer Agent-pakket

- **Other Condition**: Kies **Network Access** gebaseerd op de **Authentication Method**EQUALS methode die op de stap is geconfigureerd, voeg RADIUS-groep toe of u kunt deze leeg laten

- **Result**: Kies de Agent Config die in stap 4 is geconfigureerd om de Agent-configuratie te configureren

    - **Native Supplicant Configuration**: Kies Config Wizard en Wizard Profile

- Markeer het beleid als ingeschakeld als het niet wordt weergegeven zoals ingeschakeld in het aanvinkvakje.

De autorisatieprofielen maken

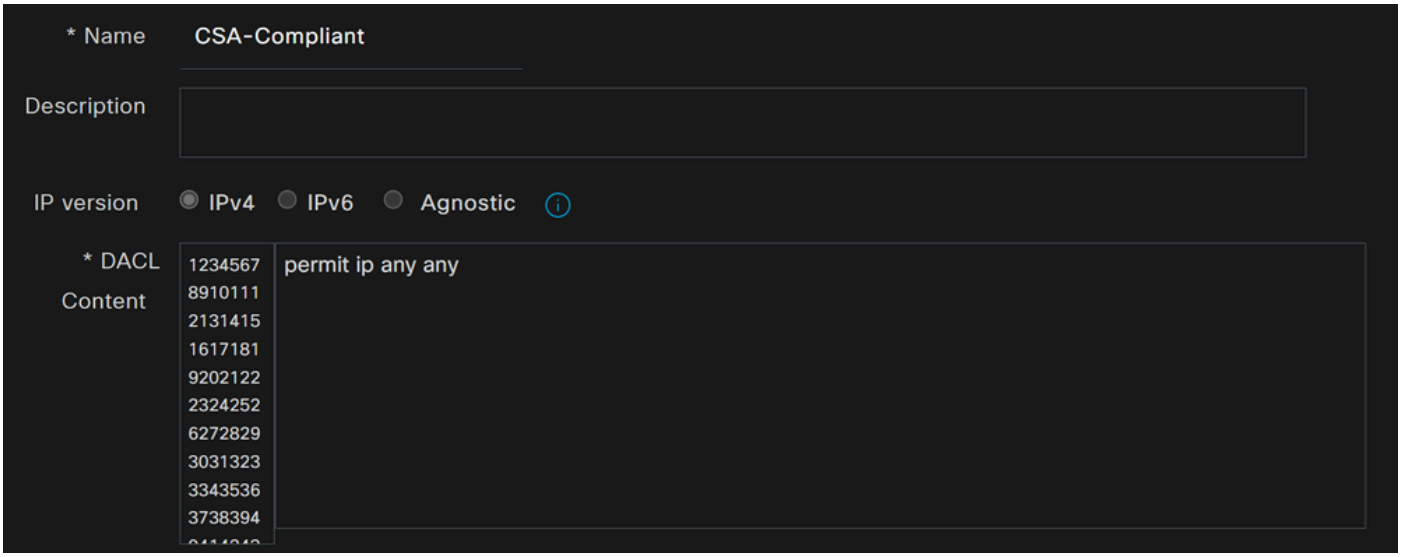
Het autorisatieprofiel beperkt de toegang tot de bronnen afhankelijk van de gebruikershouding na de verificatiekaart. De autorisatie moet worden geverifieerd om te bepalen tot welke bronnen de gebruiker toegang kan hebben op basis van de houding.

Autorisatieprofiel	Beschrijving
conform	Compatibel met gebruikers - Agent geïnstalleerd - Houding geverifieerd
Onbekend	Gebruiker niet bekend conform - Omleiden om de agent te installeren -

conform	Posture Pending te verifiëren
Toegang weigeren	Niet-conforme gebruiker - toegang weigeren

Om DACL te vormen, navigeer aan het Dashboard van ISE:

- Klik op **Work Centers > Policy Elements > Downloadable ACLs**
- Klik op **+Add**
- Maak de **Compliant DACL**



- **Name**: Voeg een naam toe die verwijst naar de DACL-conform
- **IP version**: Kies **IPv4**
- DACL Content: Maak een downloadbare toegangscontrolelijst (DACL) die toegang geeft tot alle bronnen van het netwerk

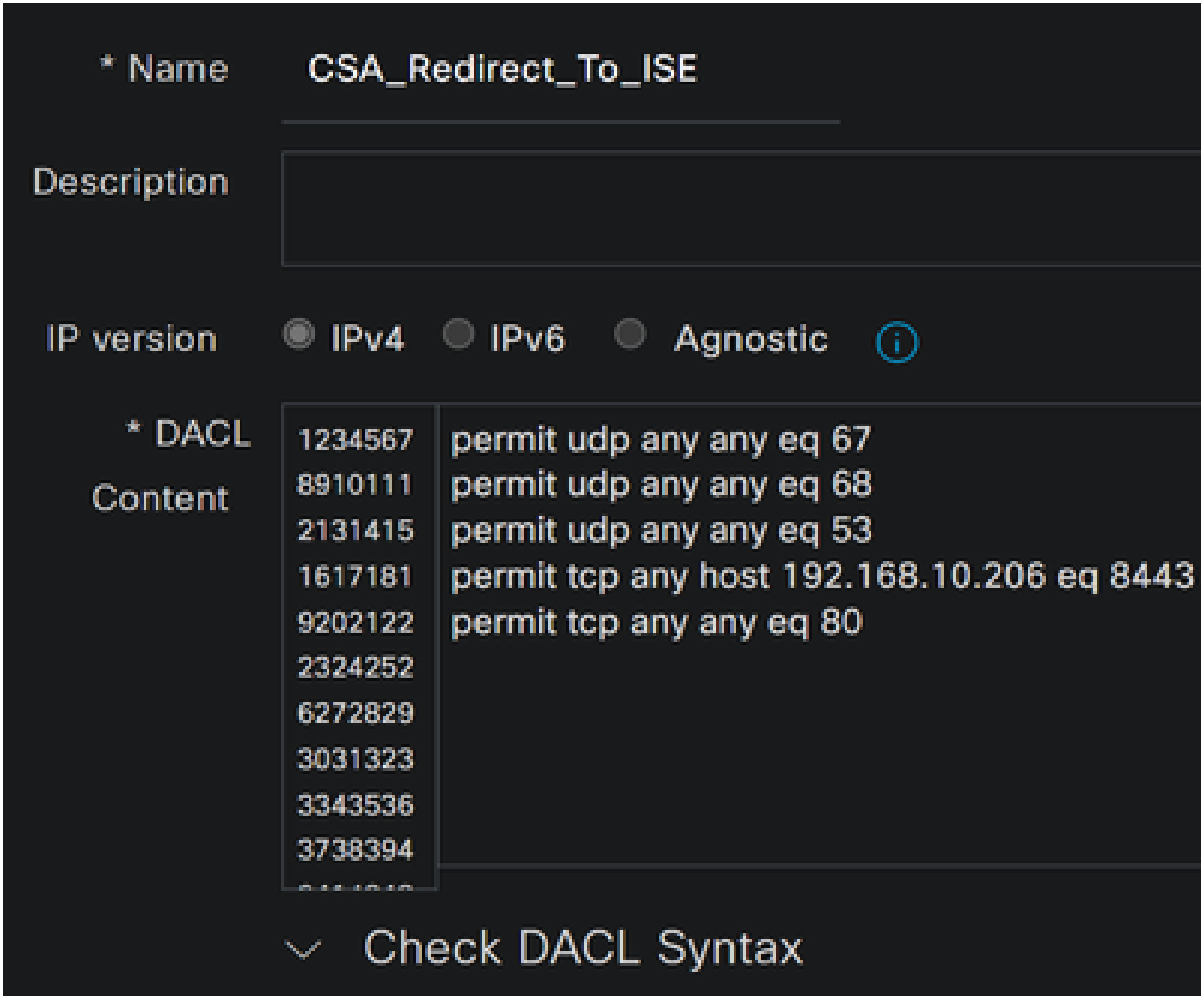
<#root>

```
permit ip any any
```

Klik **Save** en creëer de Onbekende Naleving DACL

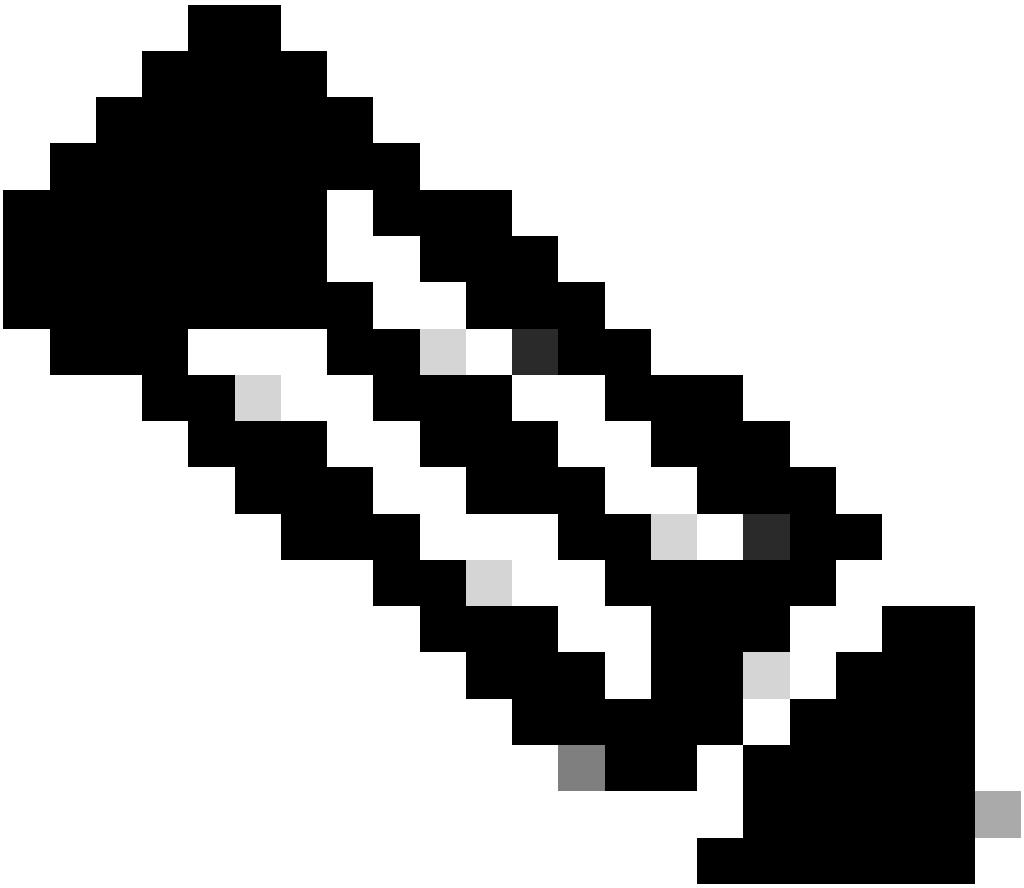
- Klik op **Work Centers > Policy Elements > Downloadable ACLs**

- Klik op **+Add**
- Maak de **Unknown Compliant DACL**



- **Name**: Voeg een naam toe die verwijst naar de DACL-onbekend-conform
- **IP version**: Kies **IPv4**
- **DACL Content**: Maak een DACL die beperkte toegang geeft tot het netwerk, DHCP, DNS, HTTP en het provisioningportal via poort 8443

```
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443
```

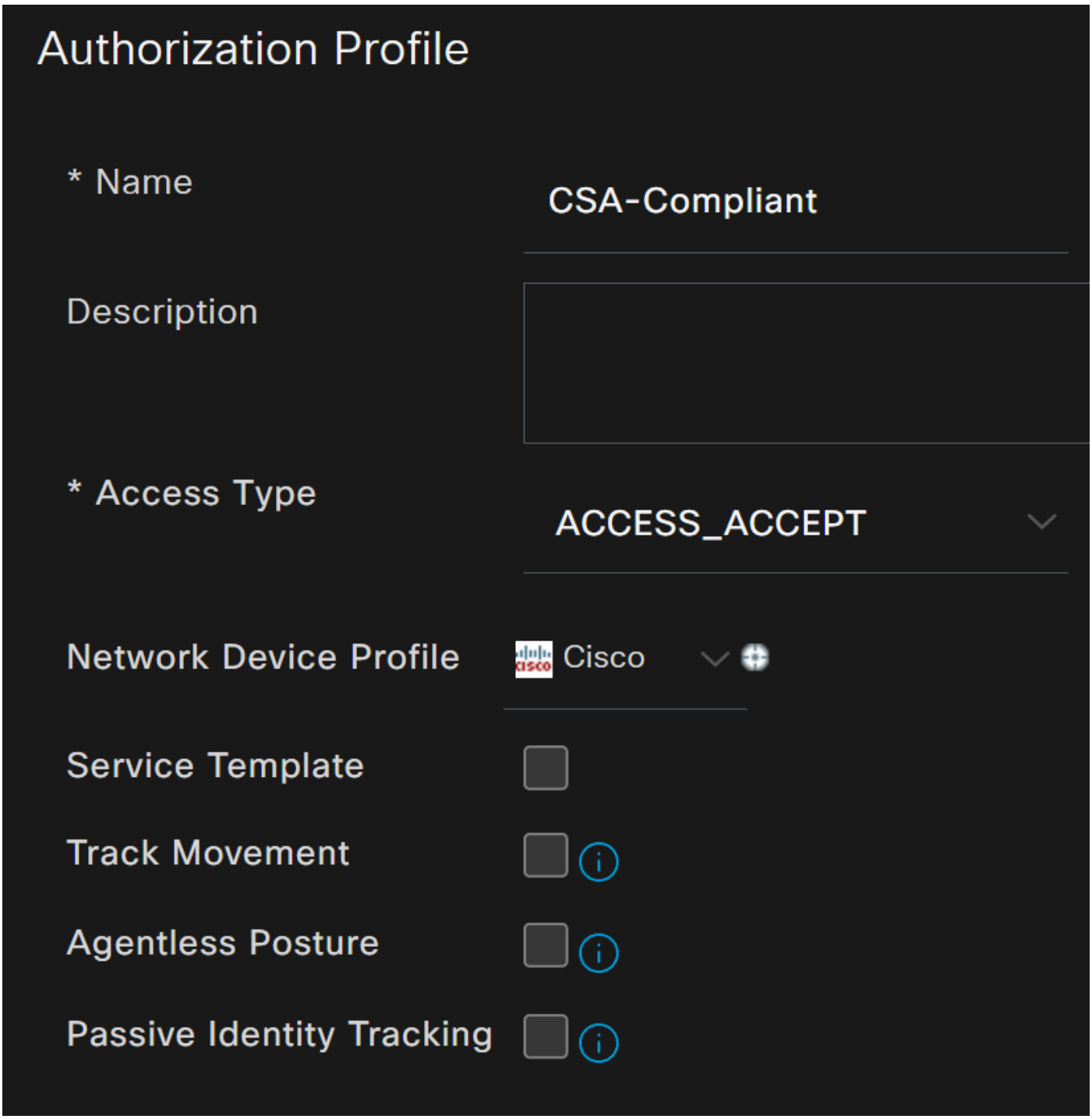


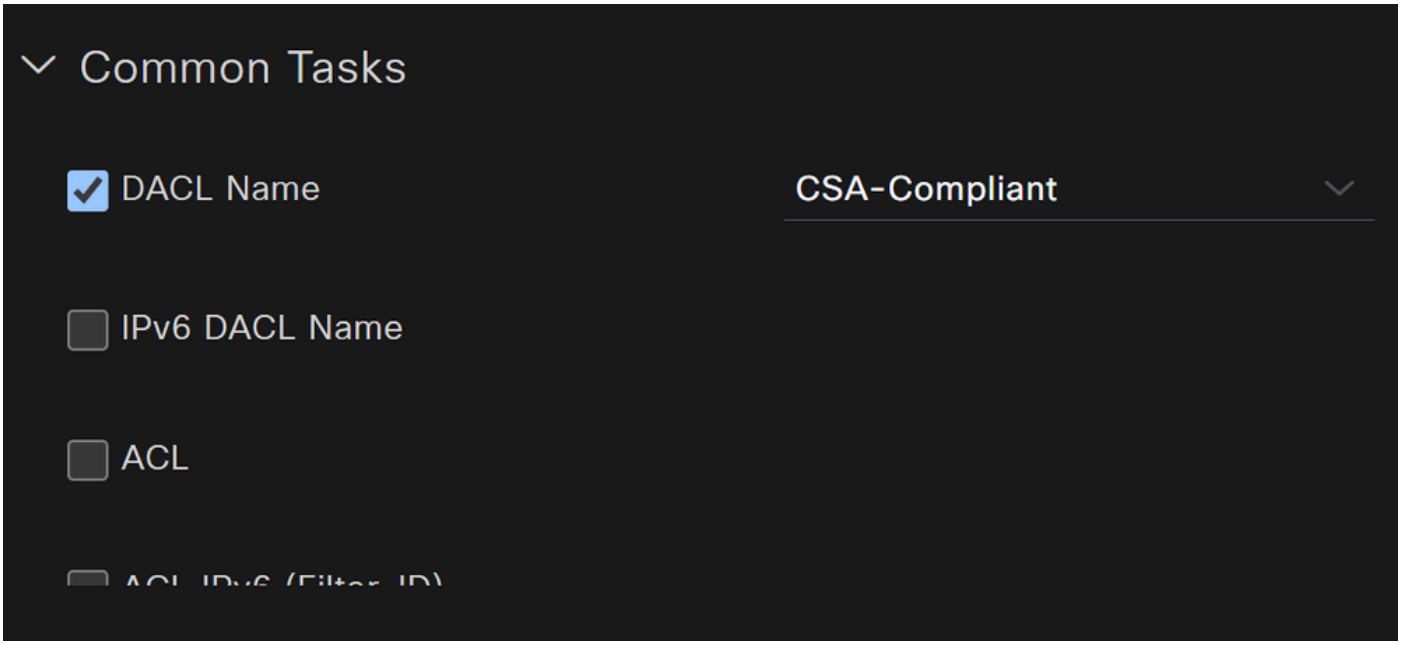
Opmerking: in dit scenario komt het IP-adres 192.168.10.206 overeen met de Cisco Identity Services Engine (ISE)-server en wordt poort 8443 aangewezen voor het provisioningportal. Dit betekent dat TCP-verkeer naar het IP-adres 192.168.10.206 via poort 8443 is toegestaan, waardoor toegang tot het provisioningportal mogelijk is.

Op dit punt hebt u de vereiste DACL om de autorisatieprofielen te maken.

Ga voor het configureren van autorisatieprofielen naar het ISE-dashboard:

- Klik op **Work Centers > Policy Elements > Authorization Profiles**
    - Klik op **+Add**
    - Maak de **Compliant Authorization Profile**





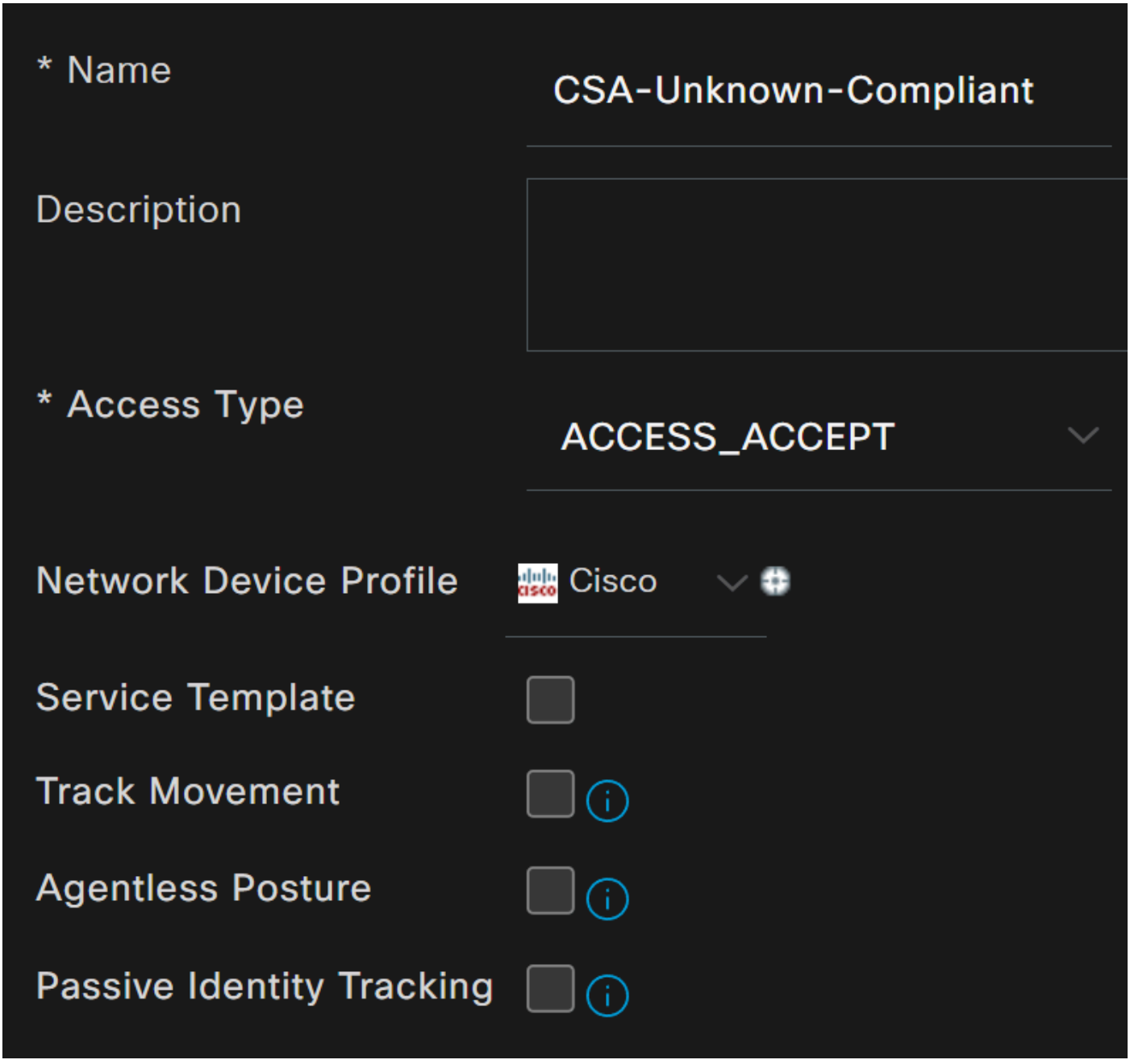
- **Name**: Een naam maken die verwijst naar het compatibele autorisatieprofiel
- Access Type: Kies **ACCESS_ACCEPT**

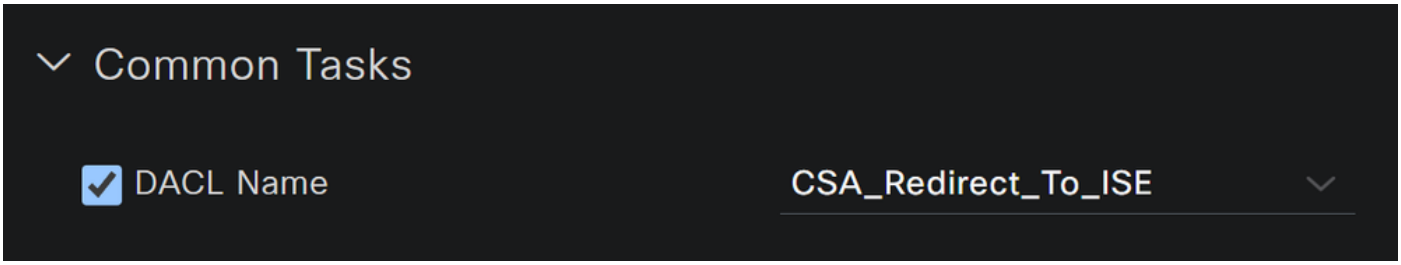
- **Common Tasks**
  - **DACL NAME**: Kies de DACL die is geconfigureerd in de stap Conforme DACL

Klik **Save** en maak de Unknown Authorization Profile

- Klik op **Work Centers > Policy Elements > Authorization Profiles**
- Klik op **+Add**

- Maak de **Uknown Compliant Authorization Profile**

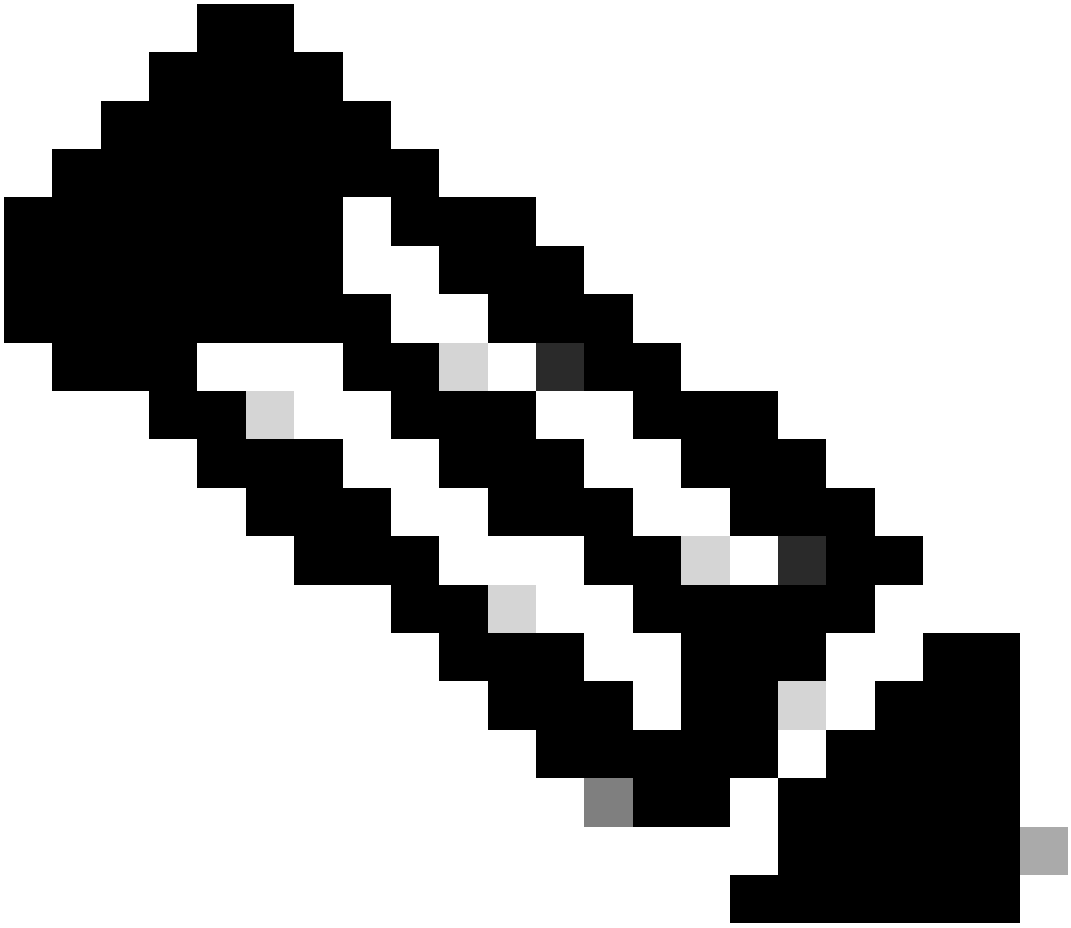




- **Name**: Een naam maken die verwijst naar het onbekende compatibele autorisatieprofiel
- Access Type: Kies **ACCESS_ACCEPT**

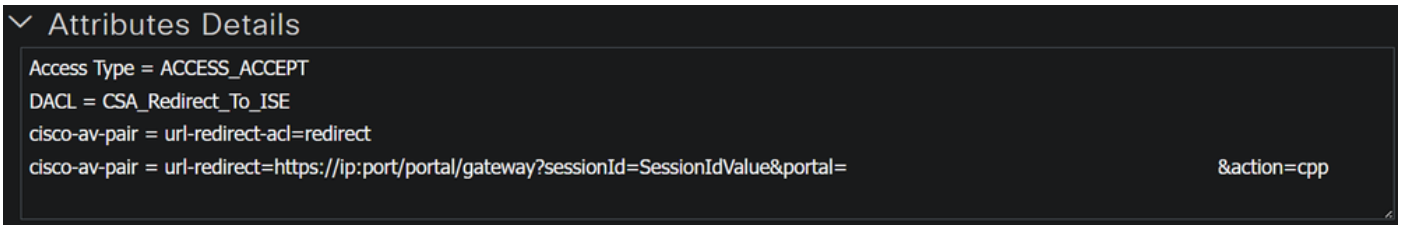
- **Common Tasks**
    - **DACL NAME**: Kies de DACL die is geconfigureerd in de stap Onbekende conforme DACL
        - **Web Redirection (CWA,MDM,NSP,CPP)**
            - Kiezen **Client Provisioning (Posture)**
                - **ACL**: Moet worden redirect
                - **Value**: Kies het standaard provisioningportal, of als u een andere hebt gedefinieerd, kies het

---



Opmerking: de naam voor de omleiding van ACL op Secure Access voor alle implementaties is **redirect**.

Nadat je al deze waarden gedefinieerd hebt, moet je iets gelijkaardigs onder Attributes Details hebben.



Klik op **Save** om de configuratie te beëindigen en met de volgende stap door te gaan.

Instellen van posteringsbeleid configureren

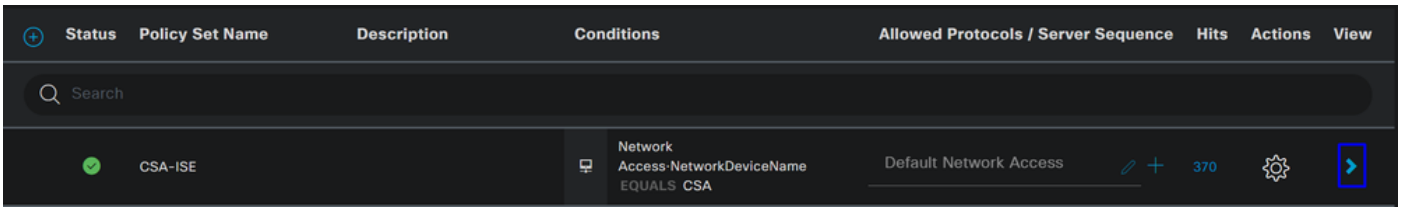
Deze drie beleidsregels die u maakt, zijn gebaseerd op de autorisatieprofielen die u hebt geconfigureerd; u hoeft **DenyAccess**bijvoorbeeld geen nieuw profiel te maken.

Policy Set - autorisatie	Autorisatieprofiel
conform	Vergunningsprofiel - conform
Onbekend conform	Vergunningsprofiel - Onbekend conform
Niet conform	Toegang weigeren

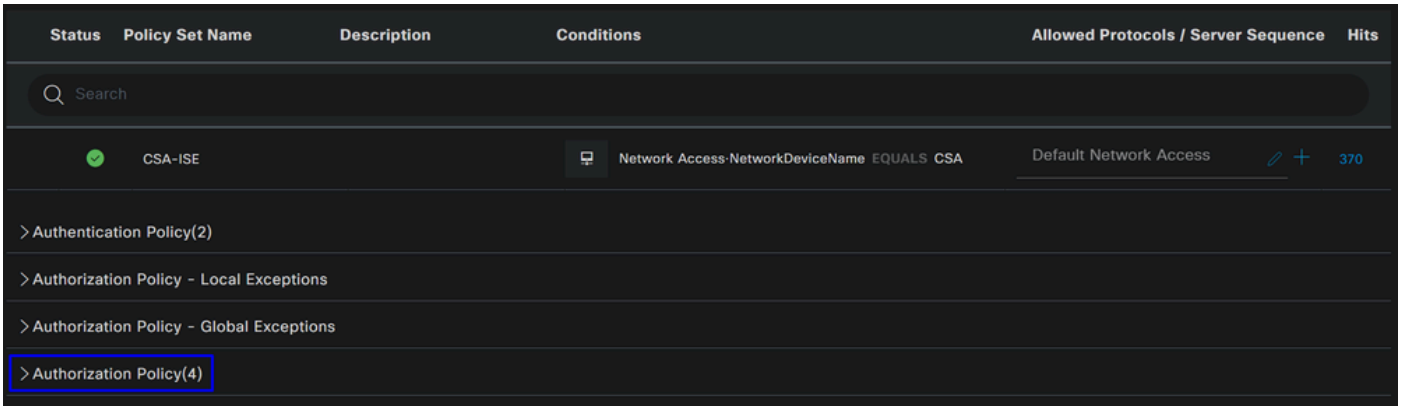
Naar uw ISE-dashboard navigeren

- Klik op **Work Center > Policy Sets**

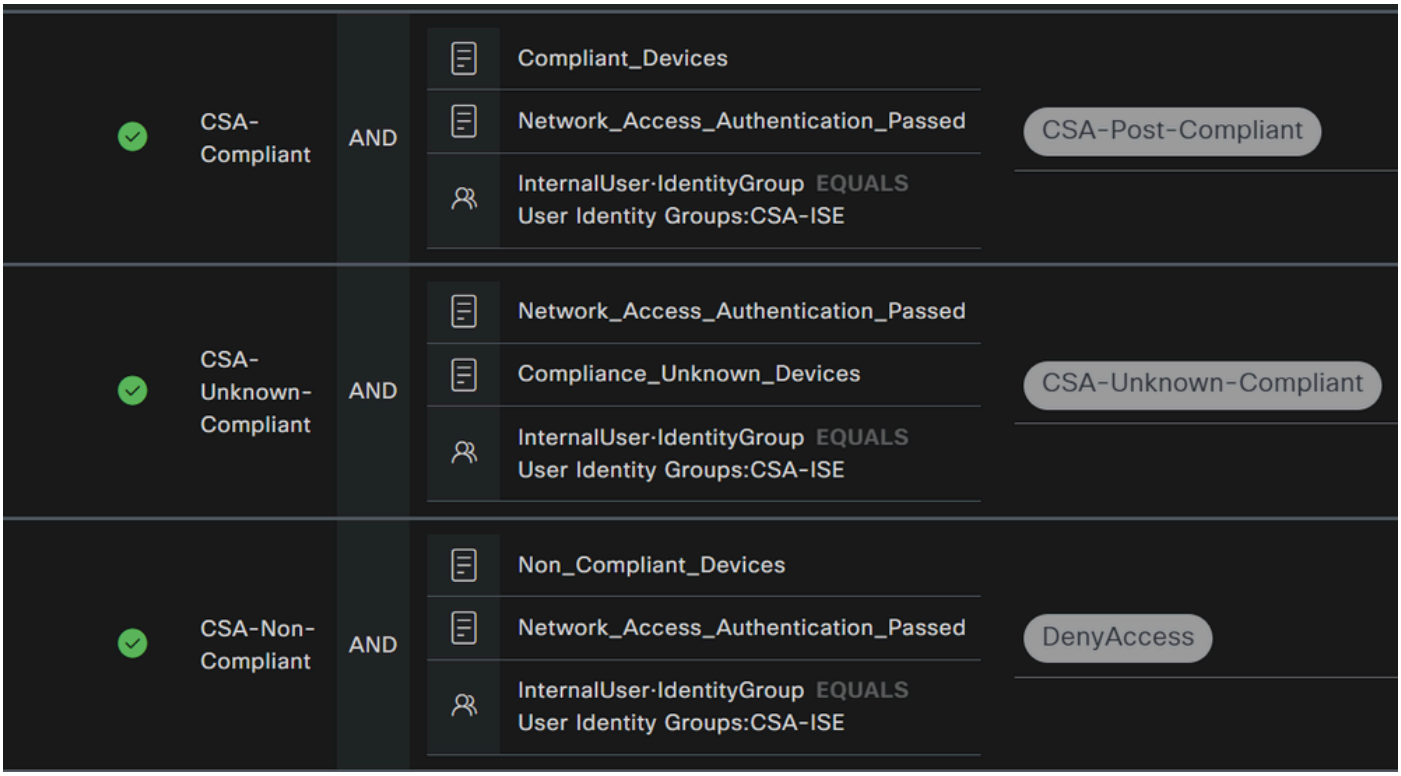
- Klik op > de pagina om toegang te krijgen tot het beleid dat u hebt gemaakt



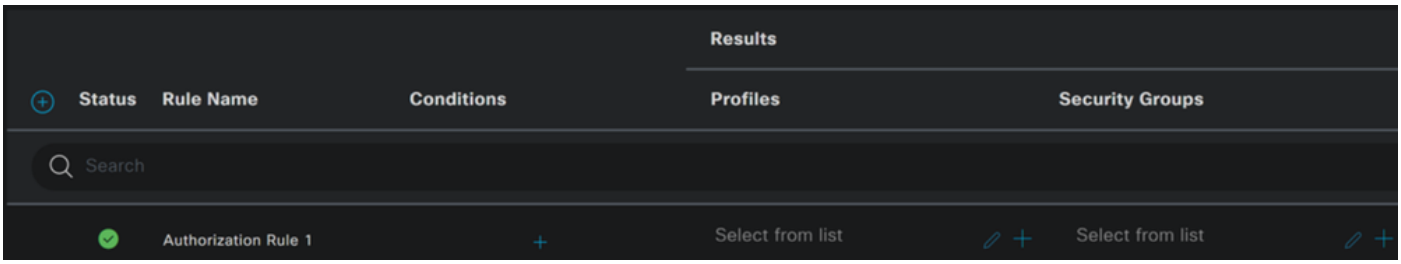
- Klik op de Authorization Policy



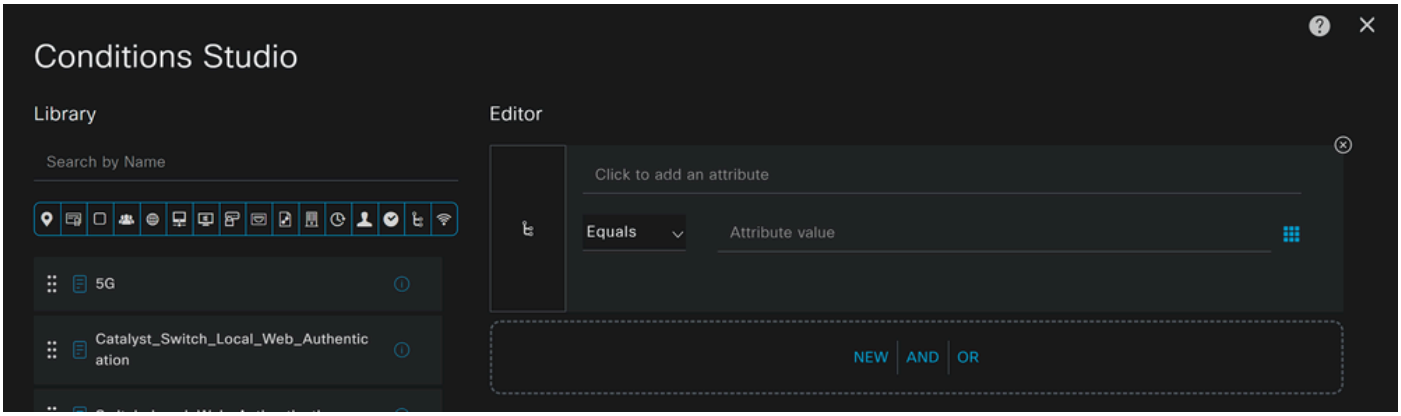
- Maak de volgende drie beleidslijnen in de volgende volgorde:



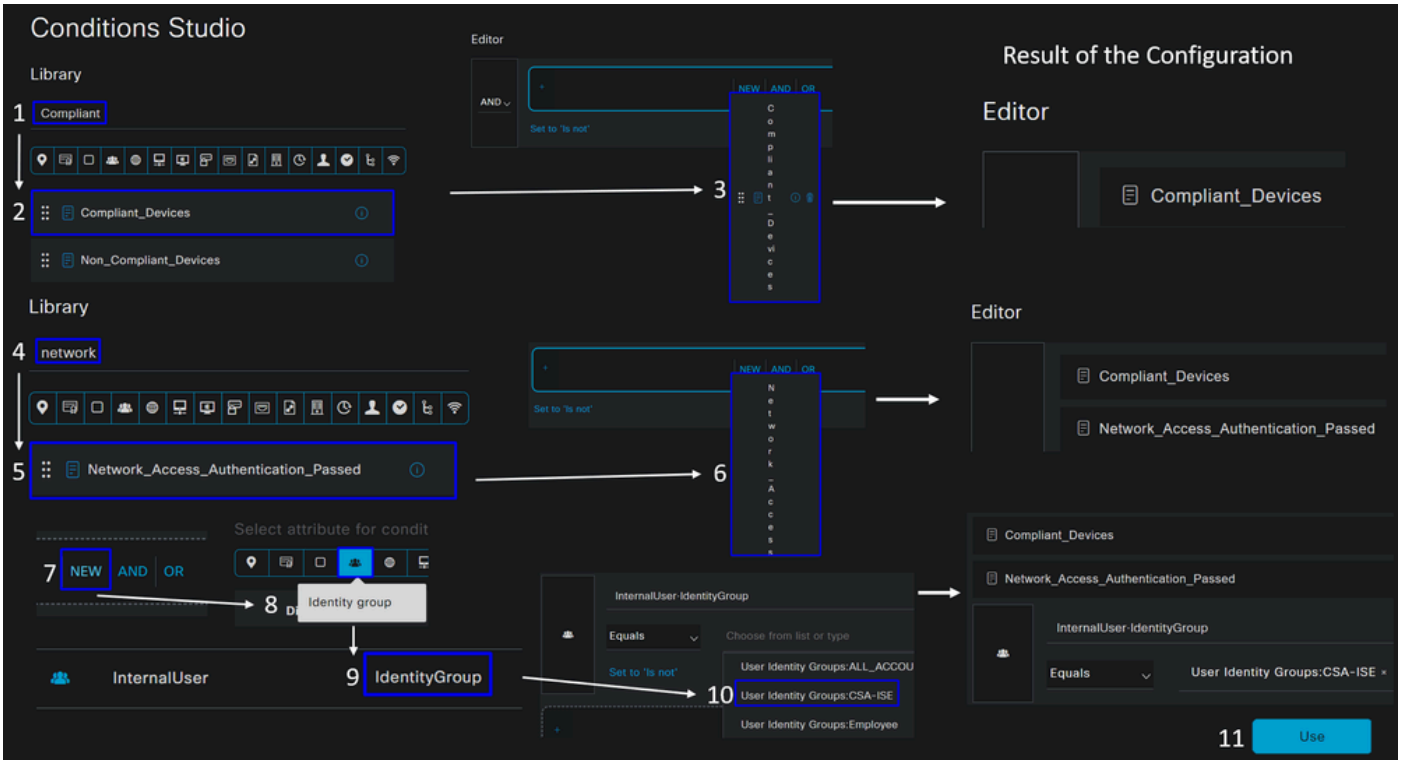
- Klik op + om het **CSA-Compliance** beleid te definiëren:



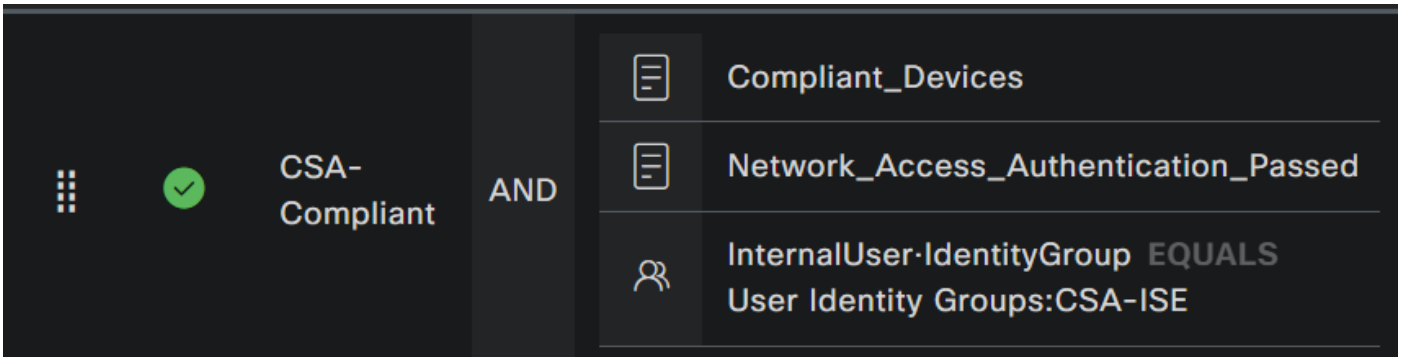
- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Compliance**
- Klik op het **Condition**veld +
- Onder **Condition Studio**, vindt u de informatie:



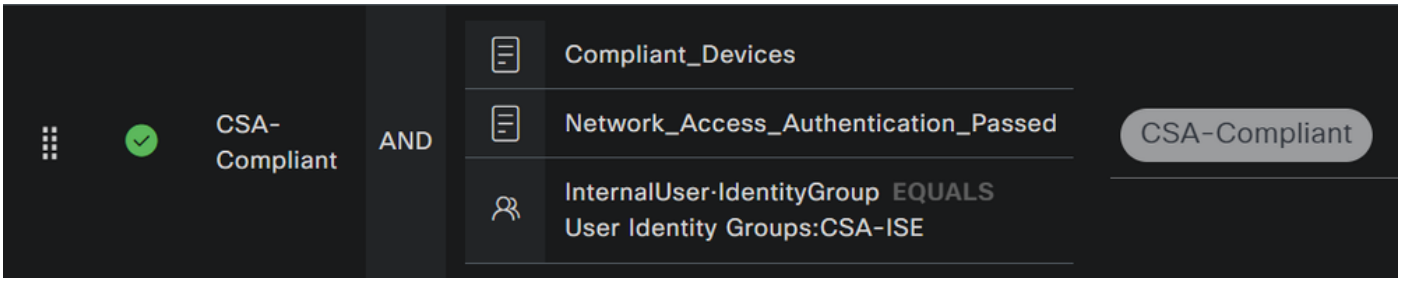
- Om de voorwaarde te creëren, zoekt u naar **compliant**
- U moet hebben weergegeven Compliant_Devices
- Sleep onder het **Editor**
- Om de tweede voorwaarde te maken, zoekt u naar **network**
- U moet hebben weergegeven Network_Access_Authentication_Passed
- Sleep onder het **Editor**
- Klik onder het Editor menu **New**
- Klik op het **Identity Group** pictogram
- Kiezen **Internal User Identity Group**
- Selecteer onder **Equals**het kopje **User Identity Group** dat u wilt afstemmen
- Klik op de knop **Use**



- Hierdoor hebt u de volgende afbeelding

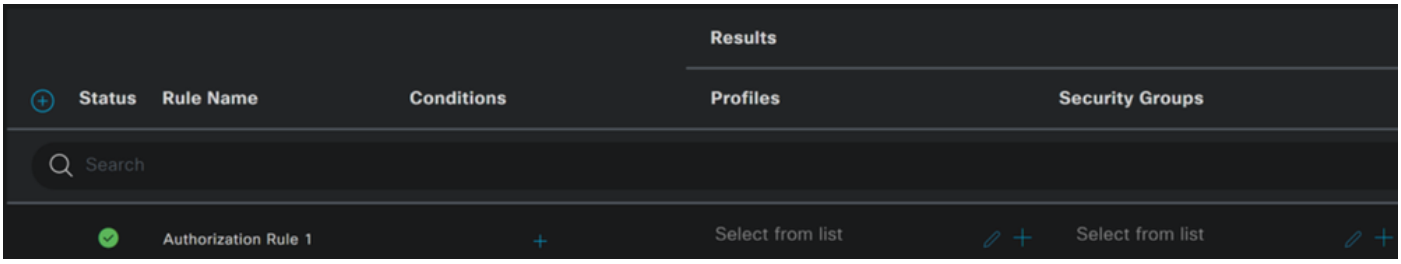


- Kies onder **Profile** klik onder de vervolgkeuzeknop en kies het profiel van de klachtenautorisatie dat op de stap is ingesteld, [conform autorisatieprofiel]

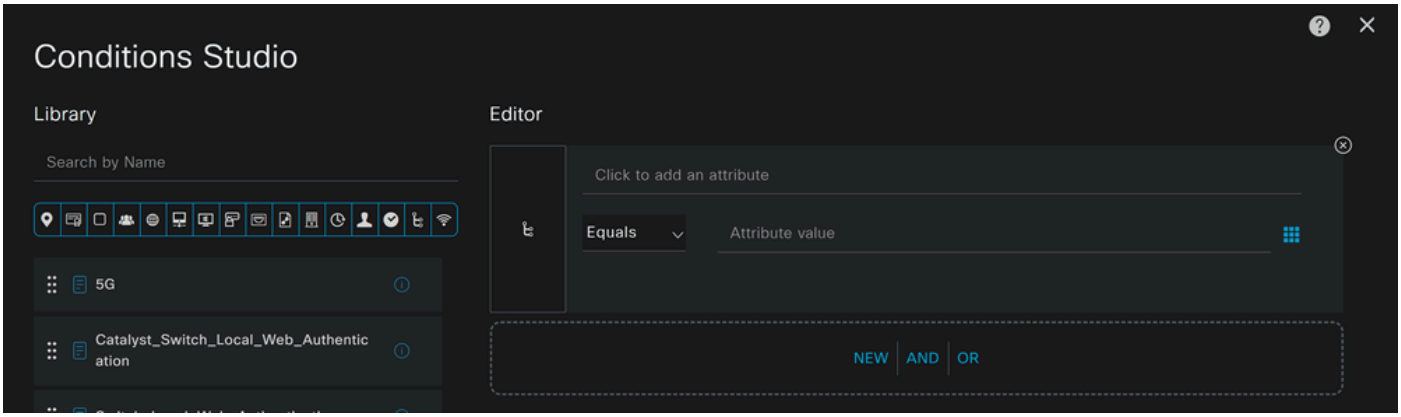


Nu hebt u de **Compliance Policy Set**instellingen ingesteld.

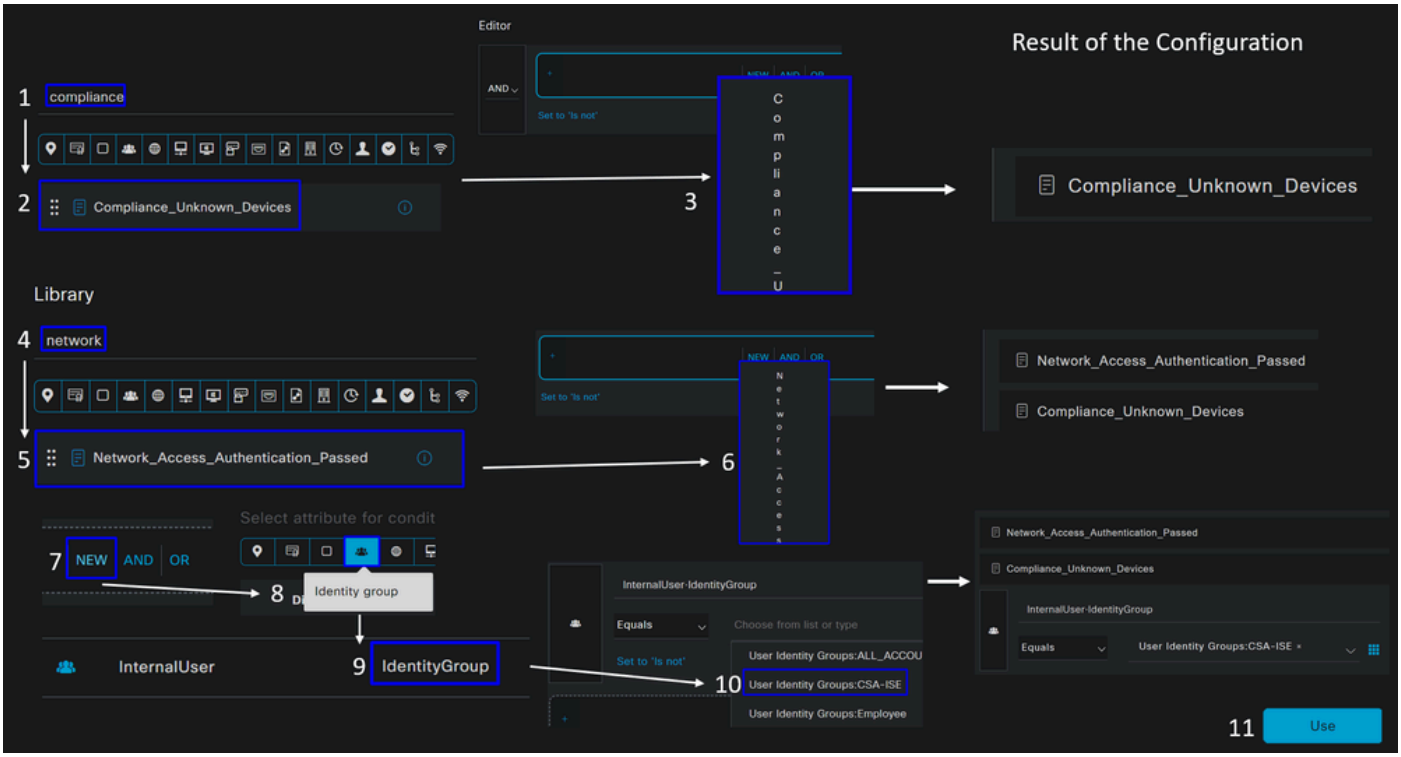
- Klik op + om het **CSA-Unknown-Compliance** beleid te definiëren:



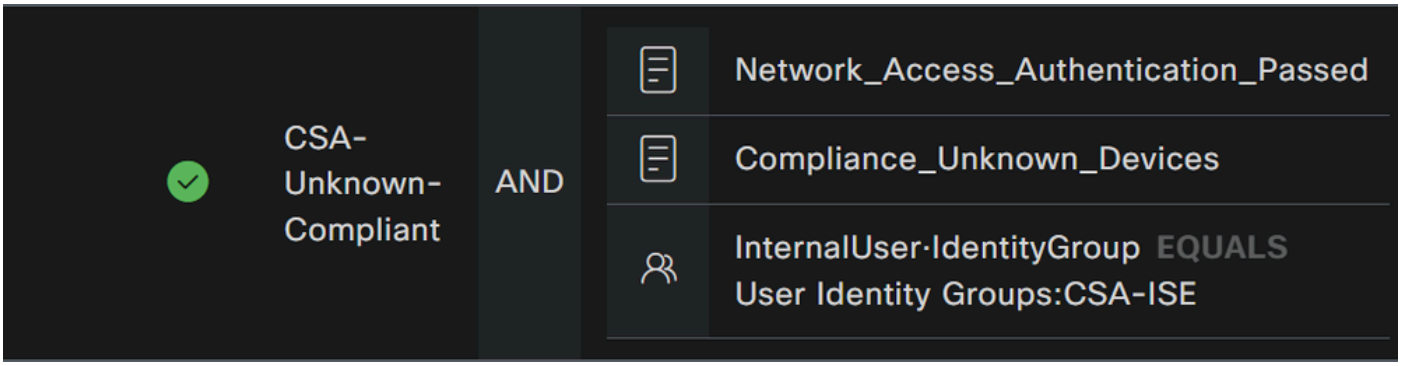
- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Unknown-Compliance**
- Klik op het **Condition**veld +
- Onder **Condition Studio**, vindt u de informatie:



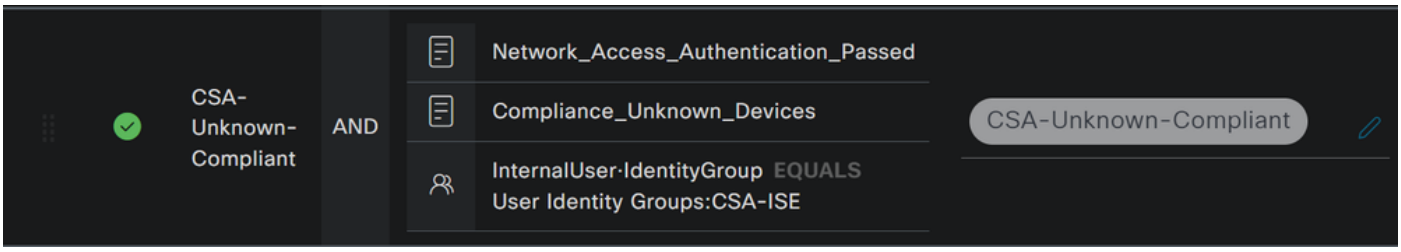
- Om de voorwaarde te creëren, zoekt u naar **compliance**
- U moet hebben weergegeven Compliant_Unknown_Devices
- Sleep onder het **Editor**
- Om de tweede voorwaarde te maken, zoekt u naar **network**
- U moet hebben weergegeven Network_Access_Authentication_Passed
- Sleep onder het **Editor**
- Klik onder het Editor menu **New**
- Klik op het **Identity Group** pictogram
- Kiezen **Internal User Identity Group**
- Selecteer onder **Equals**het kopje **User Identity Group** dat u wilt afstemmen
- Klik op de knop **Use**



- Hierdoor hebt u de volgende afbeelding

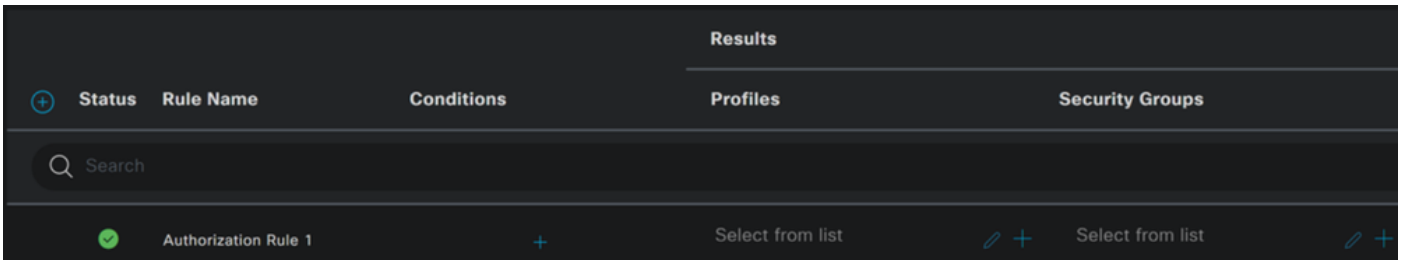


- Kies onder **Profile** klik onder de vervolgkeuzeknop en kies het profiel van de klachtenautorisatie dat op de stap is geconfigureerd, Onbekend conform autorisatieprofiel



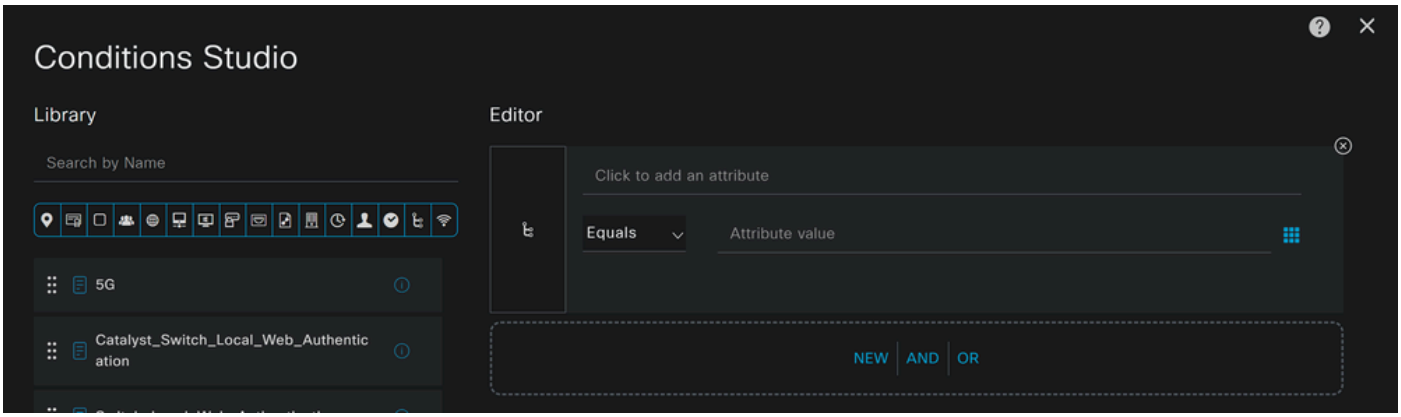
Nu hebt u de **Unknown Compliance Policy Set**instellingen ingesteld.

- Klik op + om het **CSA- Non-Compliant** beleid te definiëren:

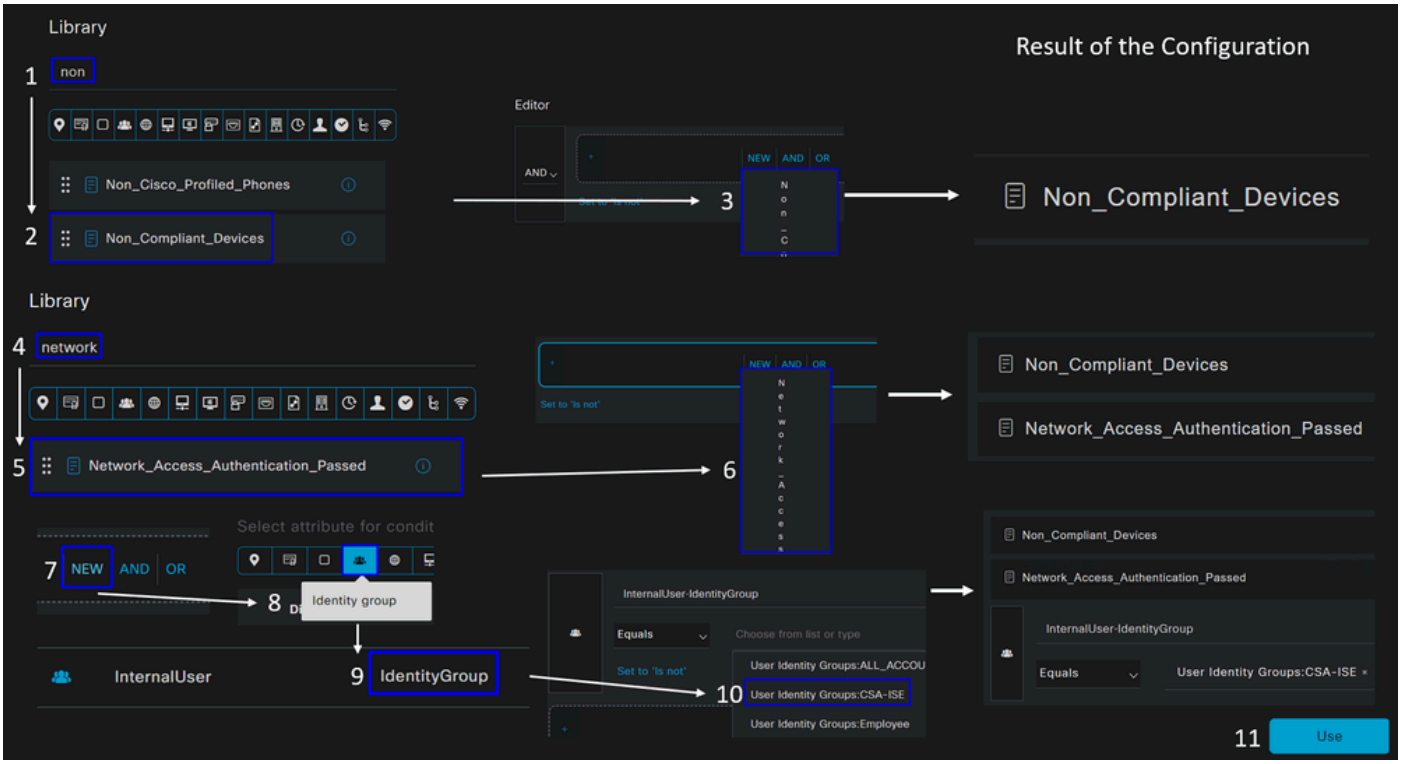


- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Non-Compliance**
- Klik op het **Condition**veld +

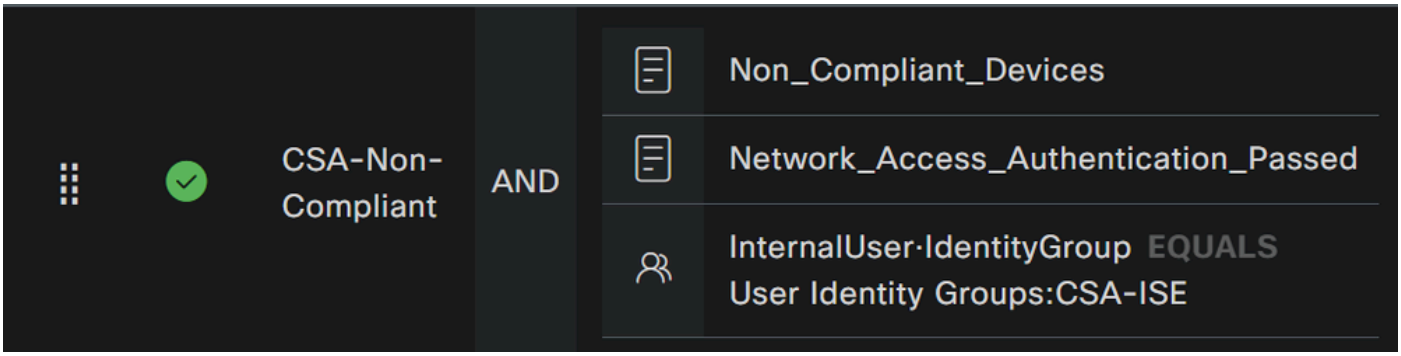
- Onder **Condition Studio**, vindt u de informatie:



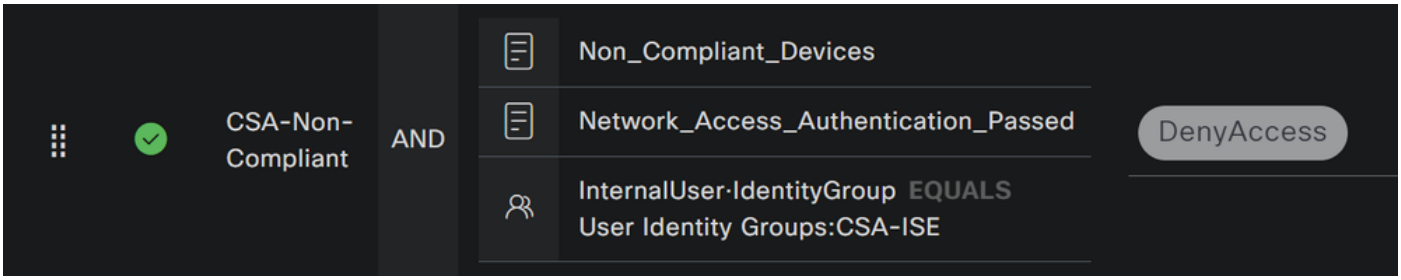
- Om de voorwaarde te creëren, zoekt u naar **non**
- U moet hebben weergegeven Non_Compliant_Devices
- Sleep onder het **Editor**
- Om de tweede voorwaarde te maken, zoekt u naar **network**
- U moet hebben weergegeven Network_Access_Authentication_Passed
- Sleep onder het **Editor**
- Klik onder het Editor menu **New**
- Klik op het **Identity Group** pictogram
- Kiezen **Internal User Identity Group**
- Selecteer onder **Equals**het kopje **User Identity Group** dat u wilt afstemmen
- Klik op de knop **Use**



- Hierdoor hebt u de volgende afbeelding



- Kies onder **Profile** klik onder de vervolgkeuzelijst en kies het profiel voor de klachtenautorisatie **DenyAccess**



Zodra u de configuratie van de drie profielen beëindigt, bent u bereid om uw integratie met houding te testen.

Verifiëren

Posture Validation

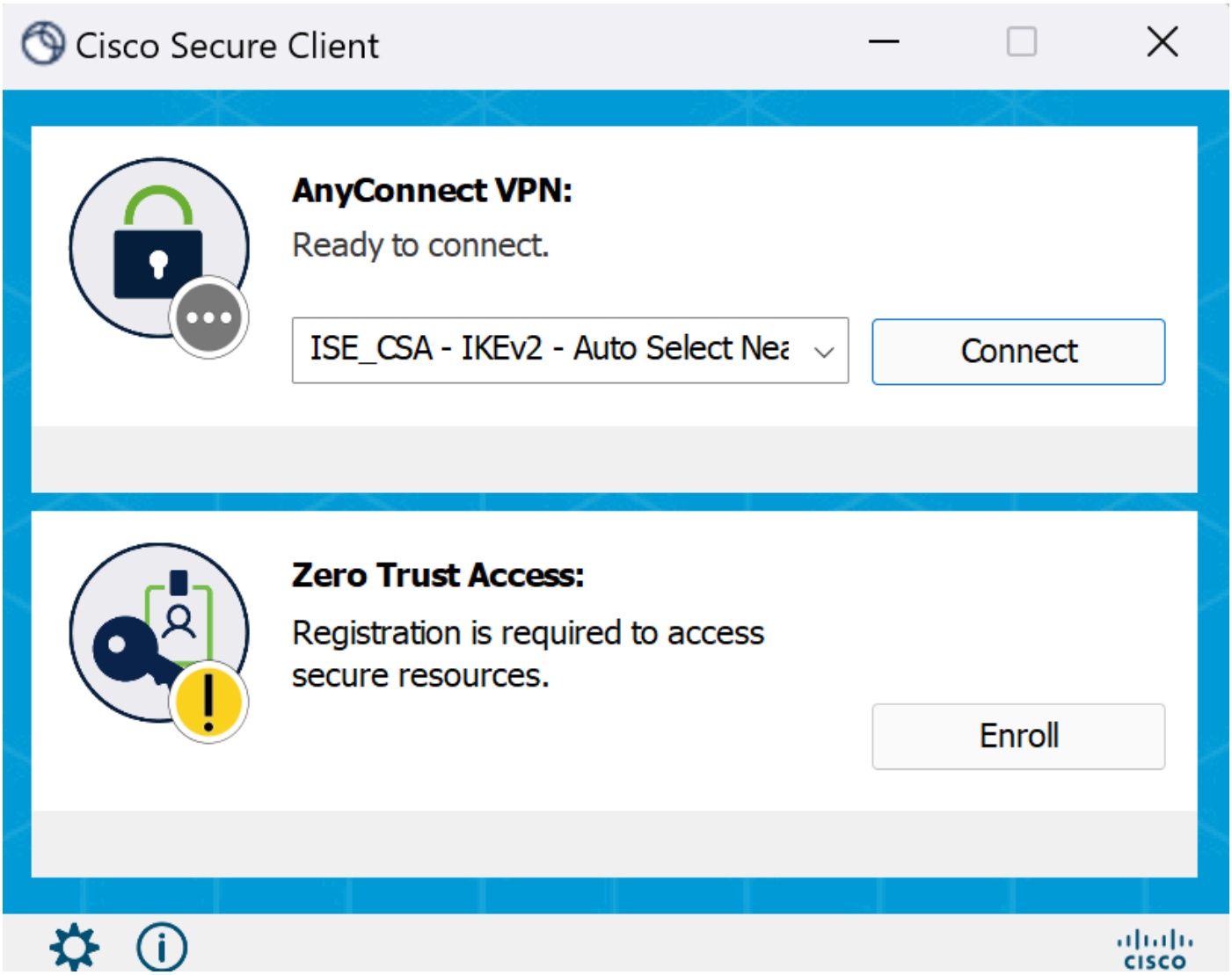
Verbinding op de machine

Maak verbinding met uw FQDN RA-VPN-domein op Secure Access via Secure Client.

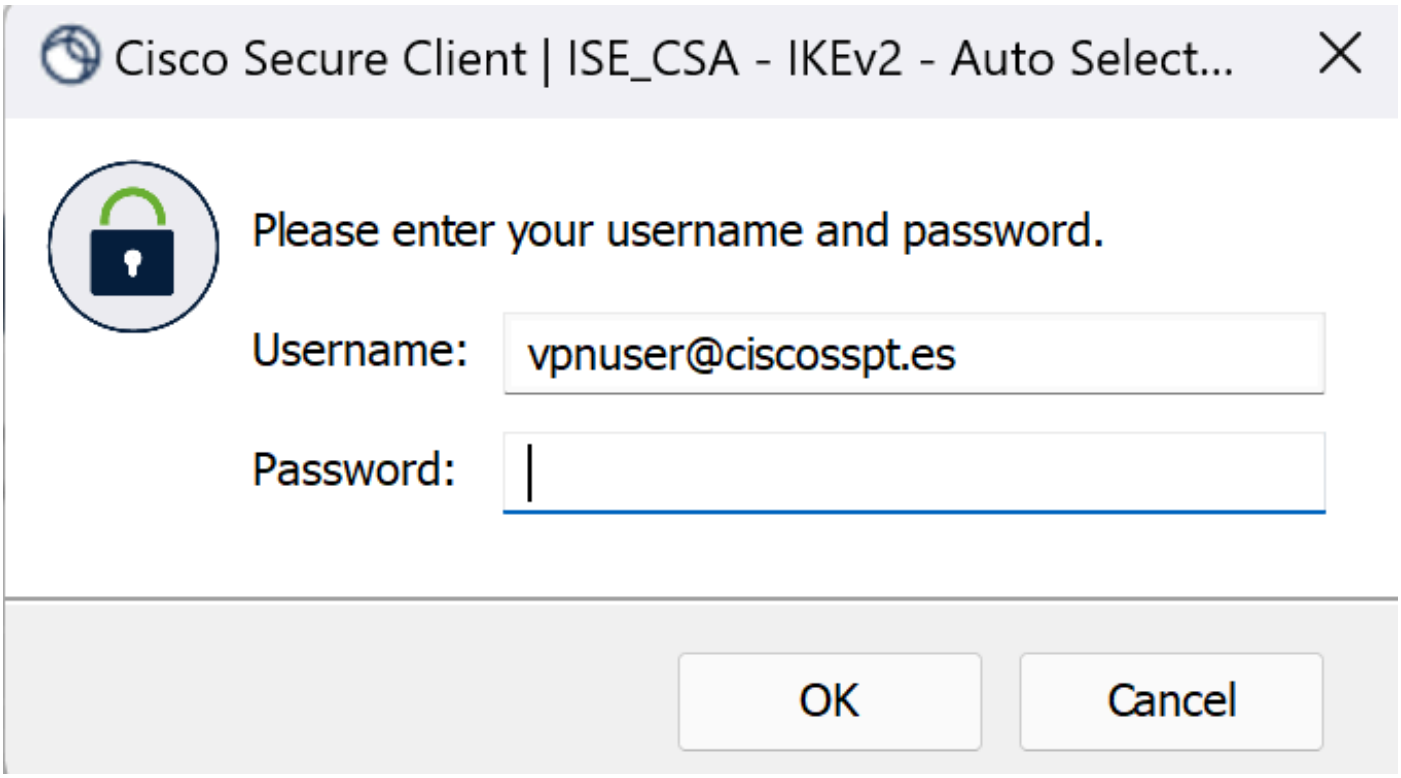
Opmerking: voor deze stap moet geen ISE-module worden geïnstalleerd.

---

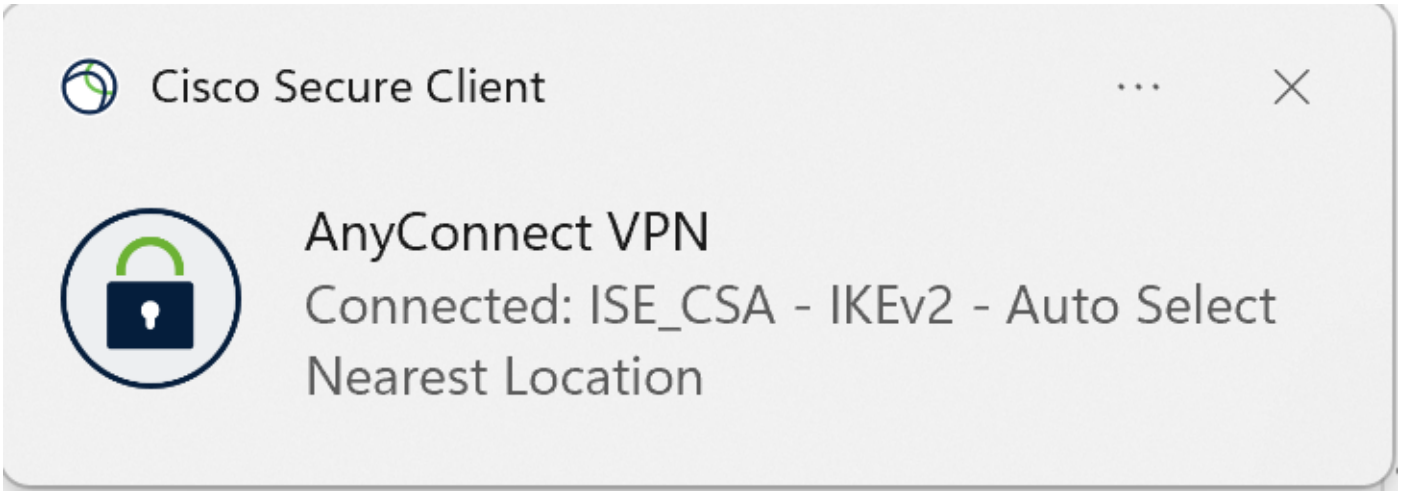
1. Verbinding maken met Secure Client.

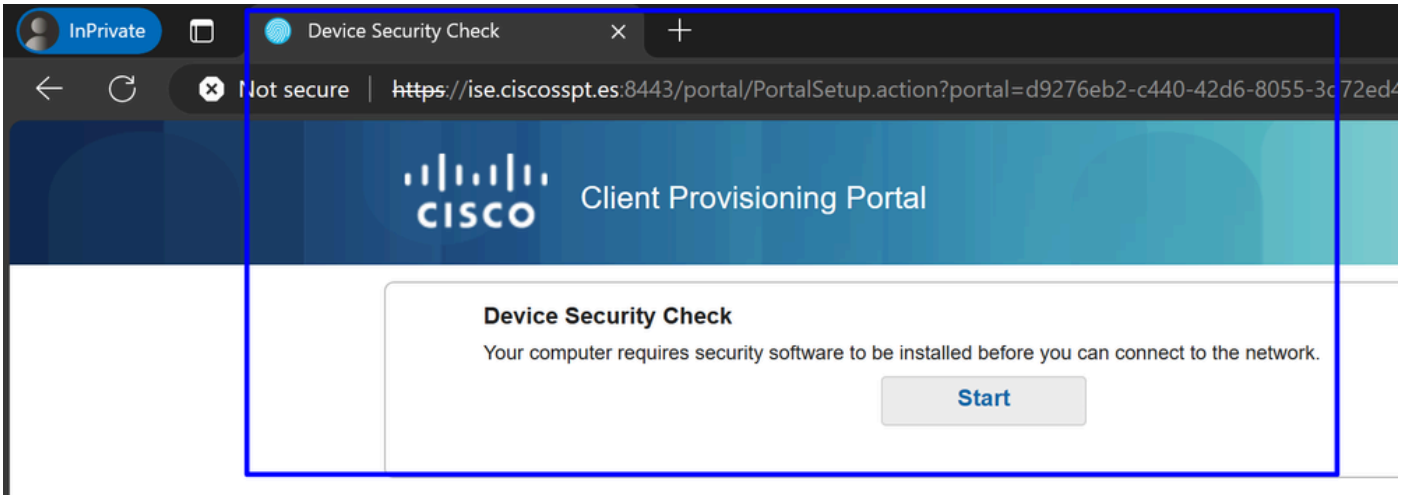


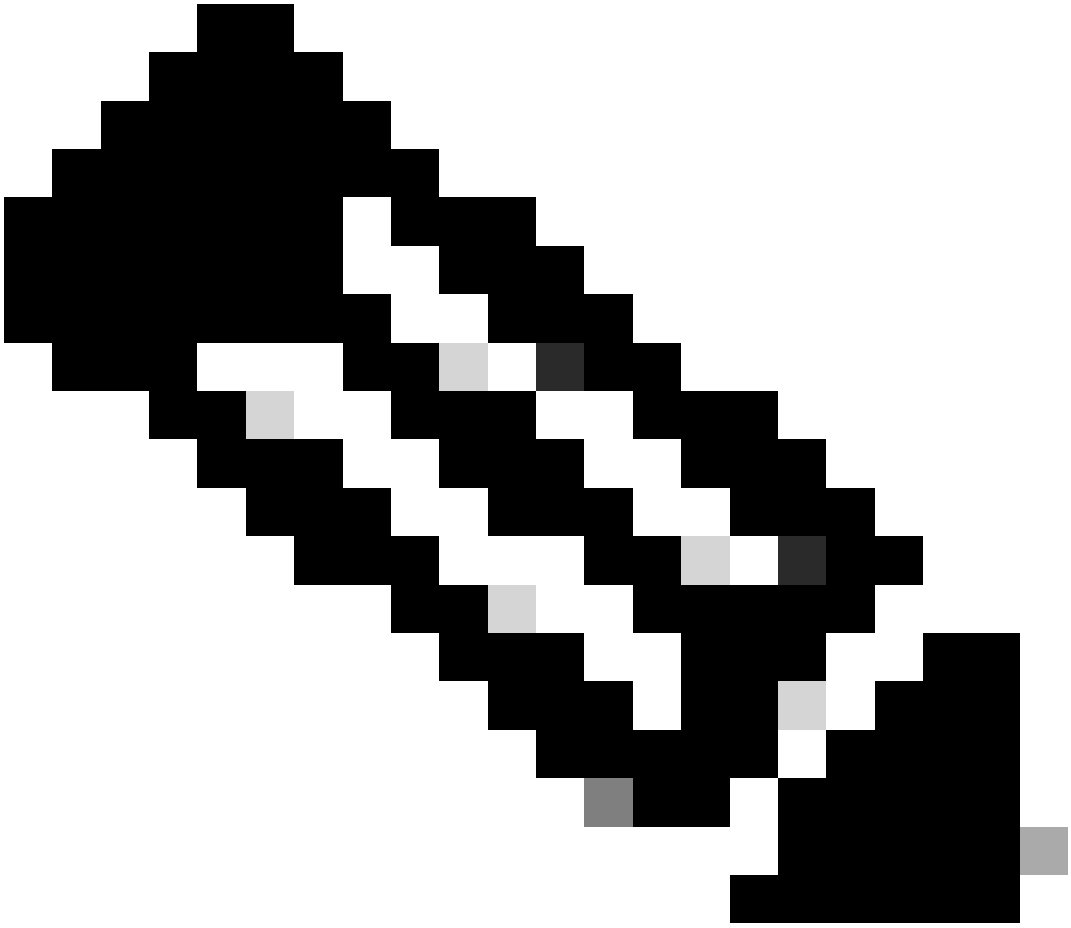
2. Geef de referenties op om te verifiëren.



3. Op dit punt wordt je verbonden met VPN en meestal wordt je doorgestuurd naar ISE. Als dat niet zo is, kun je proberen te navigeren naar **http:1.1.1.1**.



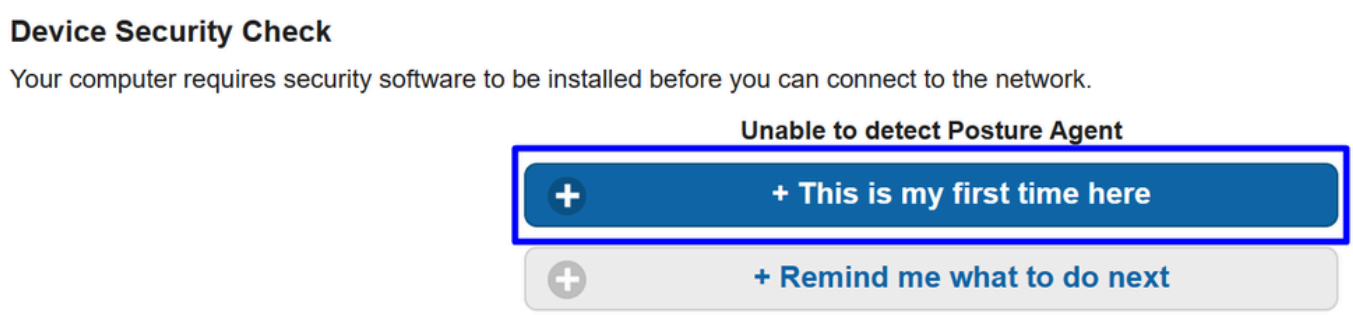




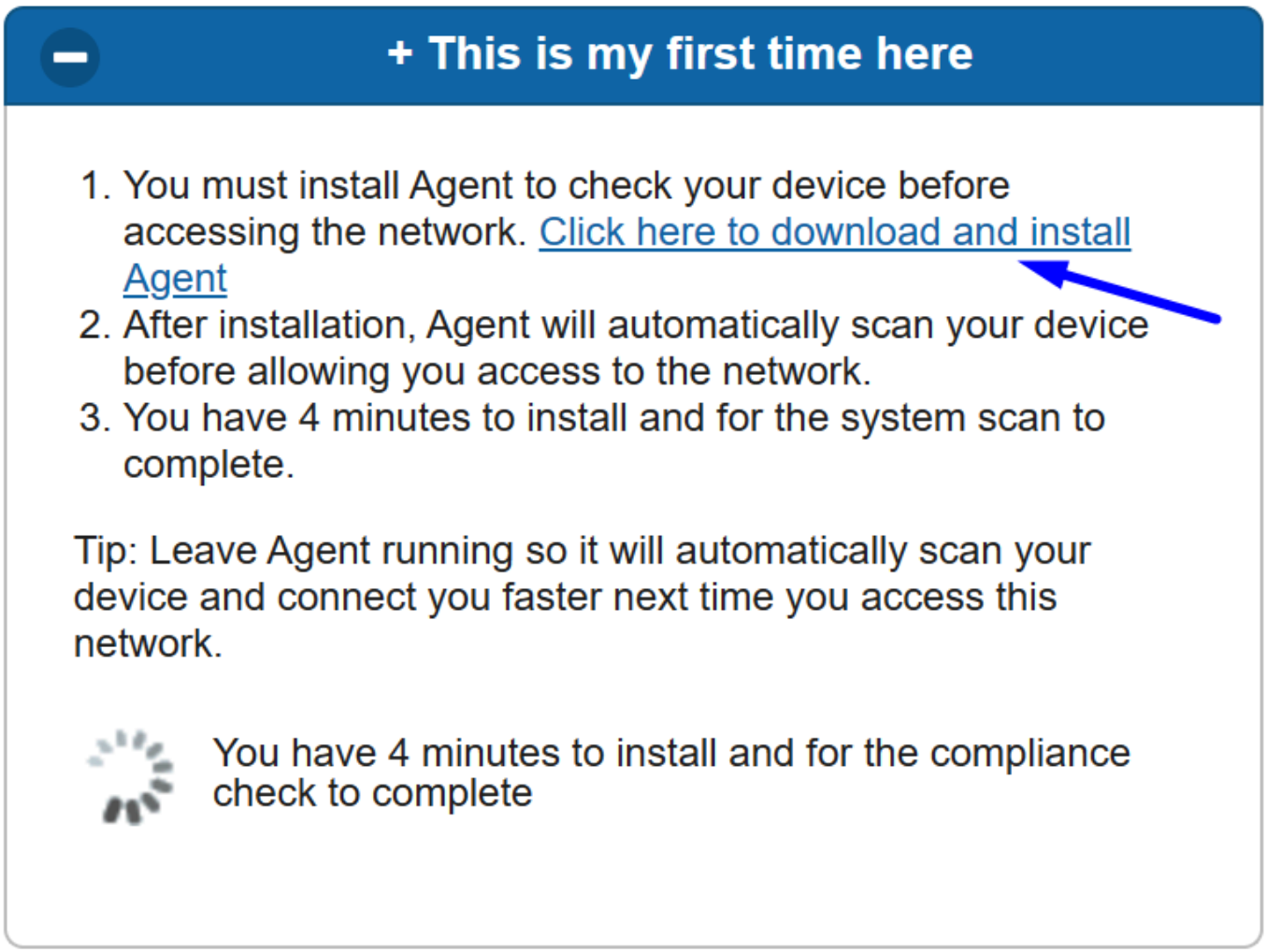
Opmerking: op dit punt valt u onder de autorisatie - beleidsset CSA-Unknown-Compliance omdat u niet de ISE Posture Agent op de machine hebt geïnstalleerd, en u wordt doorgestuurd naar de ISE Provisioning Portal om de agent te installeren.

4. Klik op Start om verder te gaan met de provisioning van de agent.

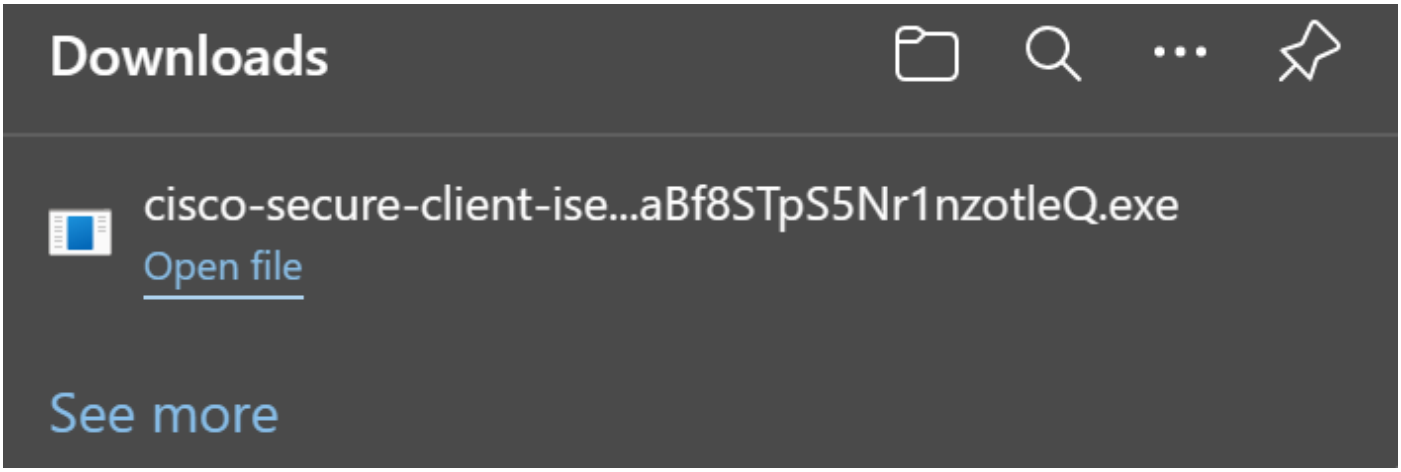
5. Klik op + **This is my first time here**.

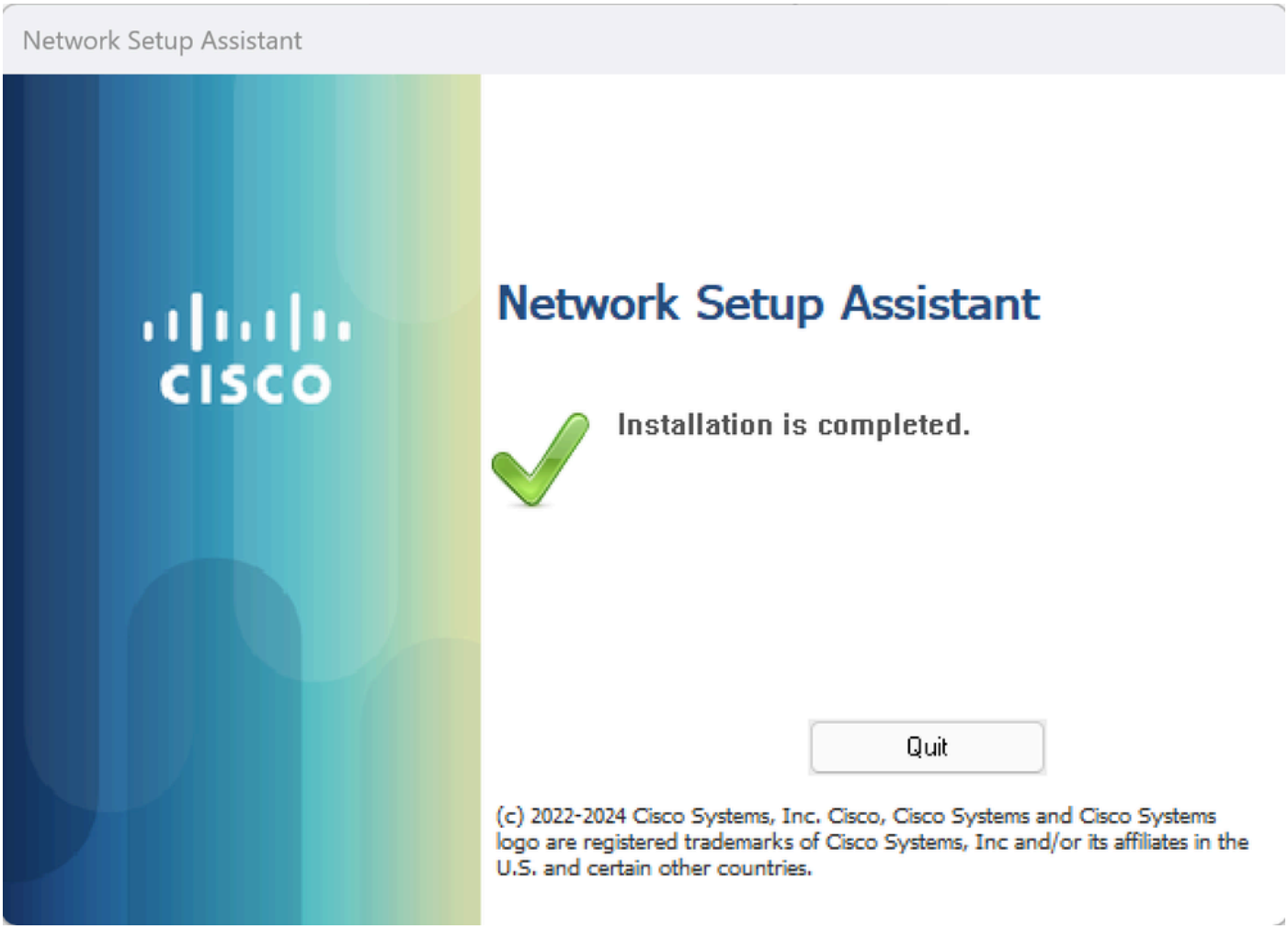


6. Klik op **Click here to download and install agent**

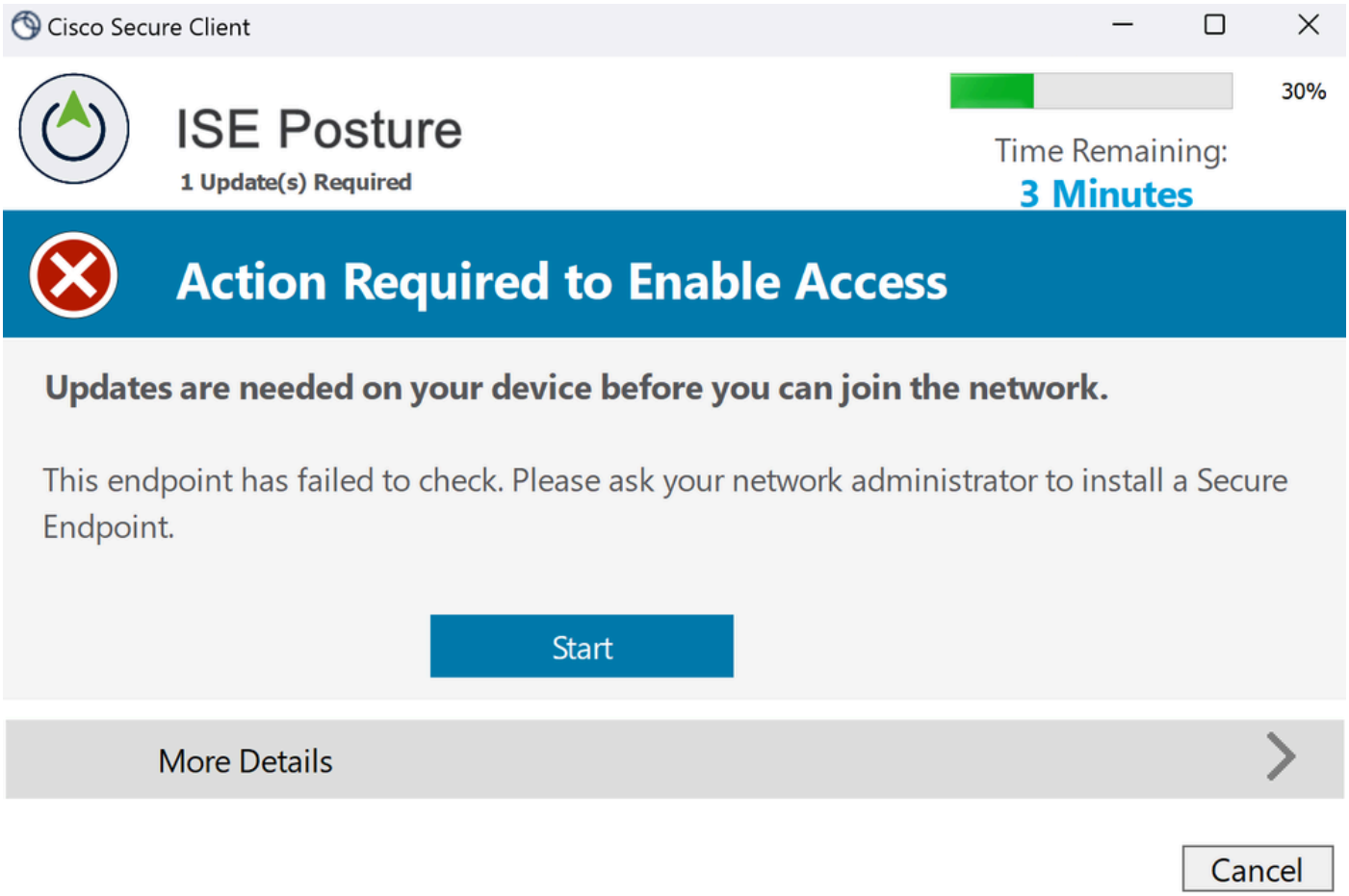


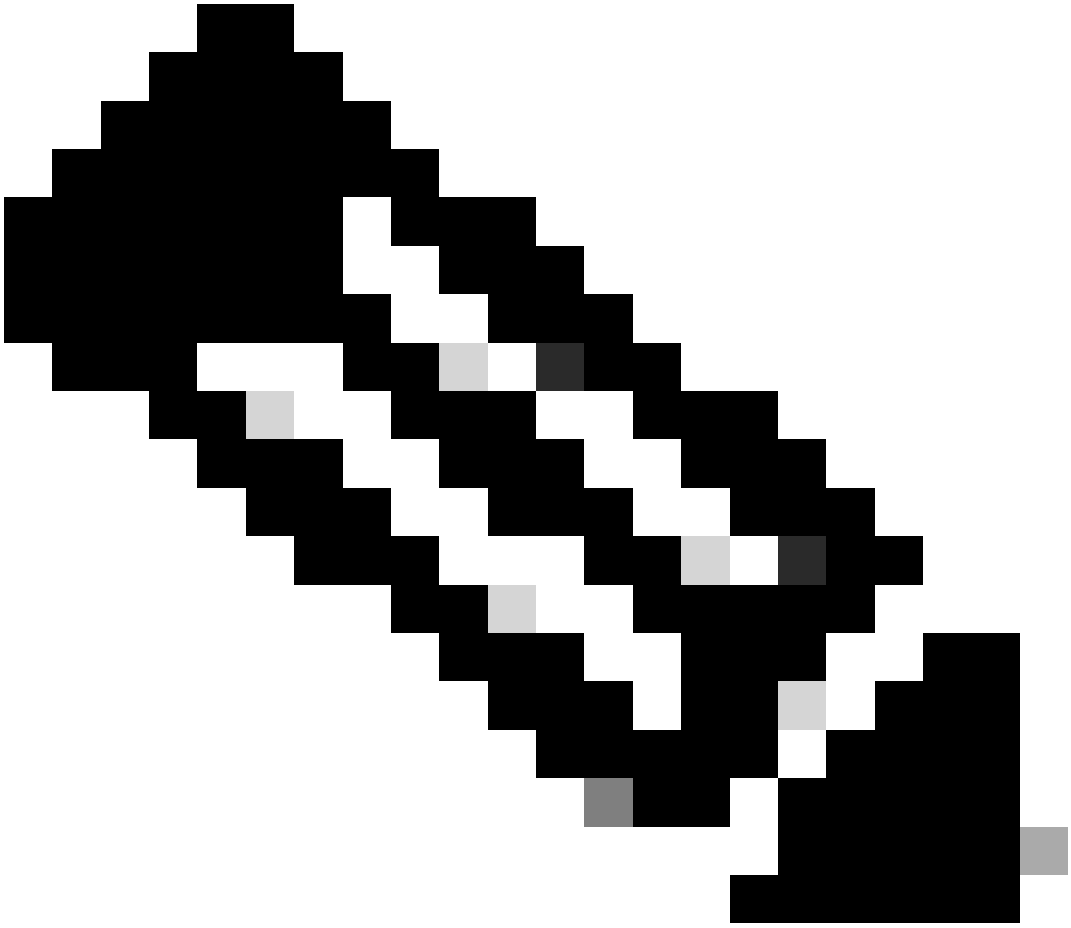
7. Installeer de agent





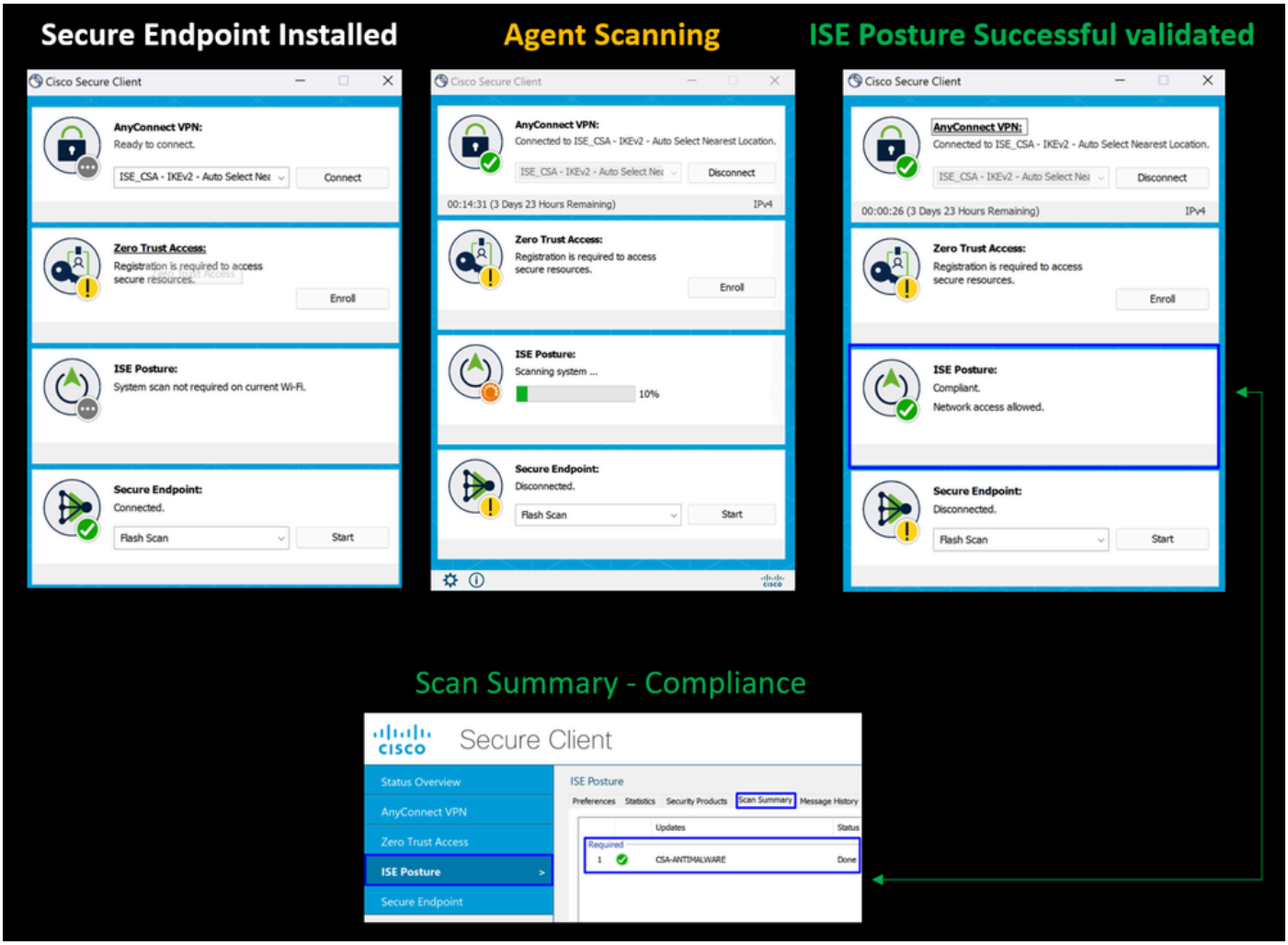
8. Nadat u de agent hebt geïnstalleerd, begint de ISE-houding de huidige houding van de machines te verifiëren. Als niet aan de beleidsvereisten wordt voldaan, verschijnt een pop-up om u naar naleving te begeleiden.


Cisco Secure Client
ISE Posture
1 Update(s) Required
30%
Time Remaining:
3 Minutes
Action Required to Enable Access
Updates are needed on your device before you can join the network.
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.
Start
More Details
Cancel

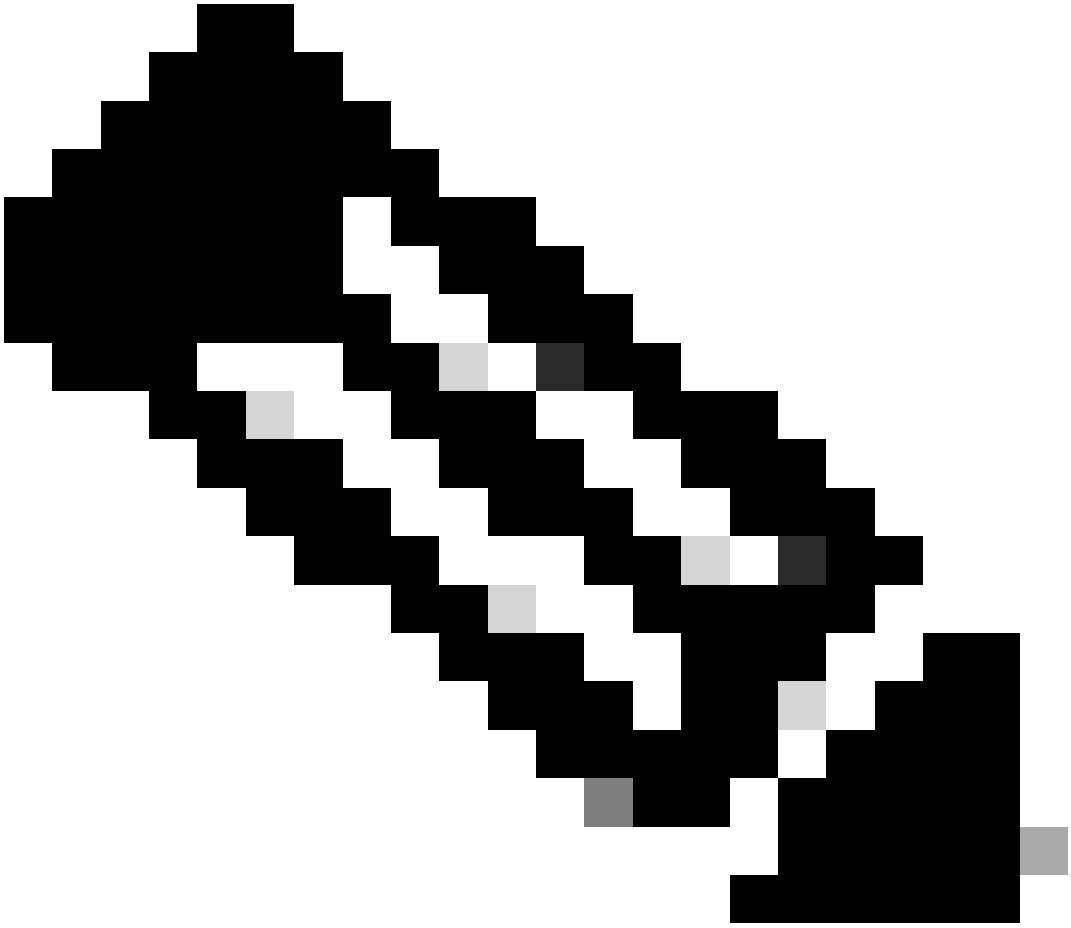


Opmerking: als u Cancel of de resterende tijd eindigt, wordt u automatisch niet-conform, valt u onder het autorisatiebeleid dat is ingesteld op CSA-Non-Compliance, en wordt u onmiddellijk losgekoppeld van de VPN.

9. Installeer de Secure Endpoint Agent en maak opnieuw verbinding met VPN.



10. Nadat de agent heeft gecontroleerd of de machine aan de eisen voldoet, verandert uw houding in een klachtenprocedure en geeft u toegang tot alle bronnen in het netwerk.



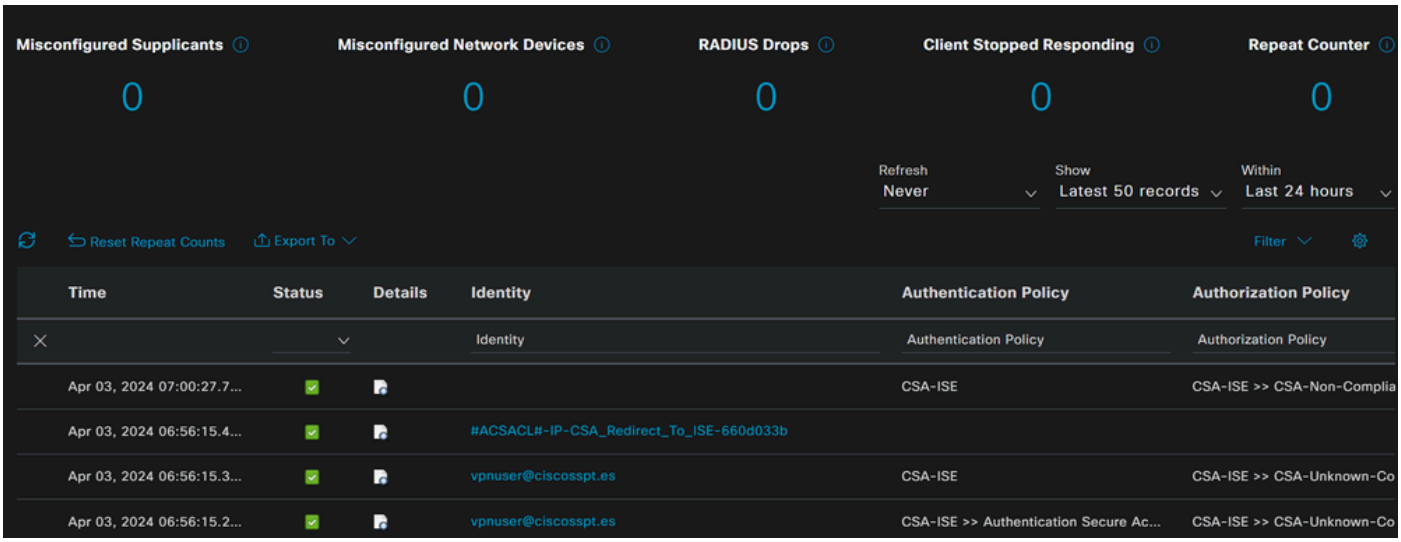
Opmerking: nadat u compatibel bent geworden, valt u onder het autorisatiebeleid CSA-Compliance, en hebt u onmiddellijk toegang tot al uw netwerkbronnen.

Hoe logboeken te verzamelen in ISE

Om de authenticatieresultaten voor een gebruiker te verifiëren, hebt u twee voorbeelden van naleving en niet-naleving. Om het in ISE te bekijken, volgt u deze instructies:

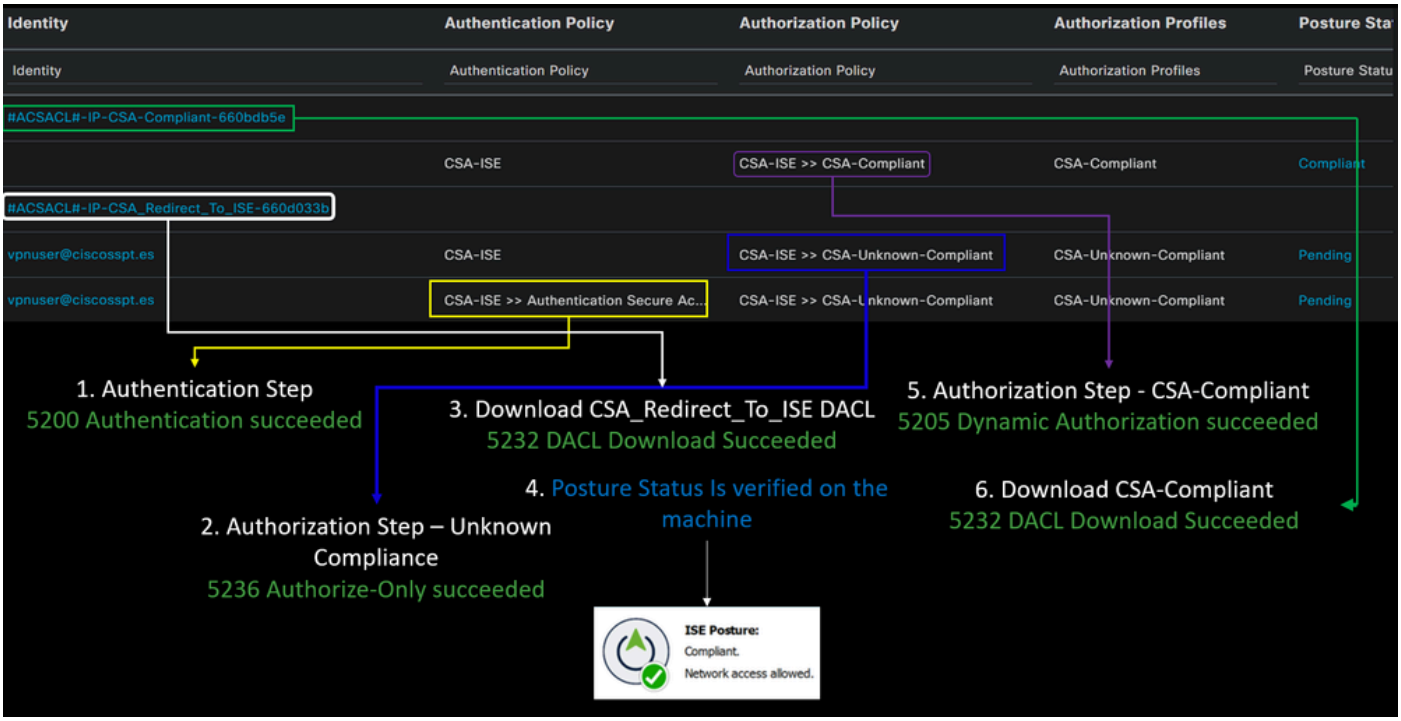
- Naar uw ISE-dashboard navigeren

- Klik op Operations > Live Logs

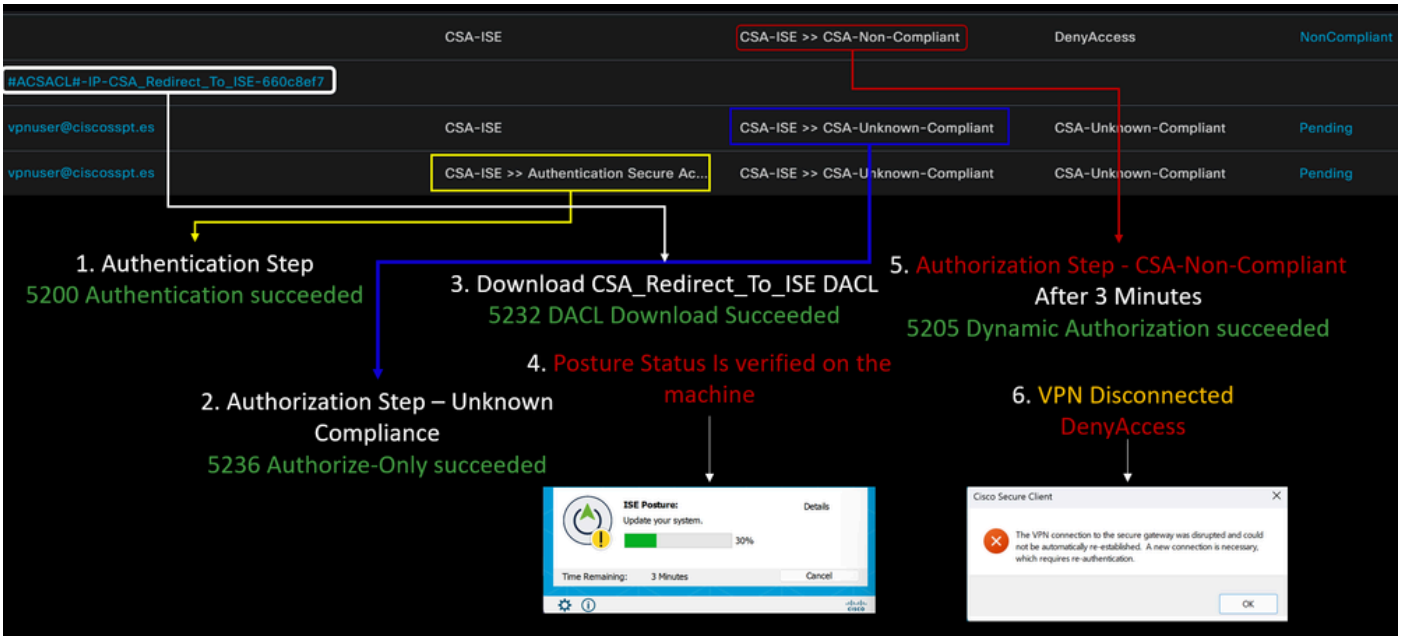


Het volgende tho-scenario toont aan hoe succesvolle compliance- en non-compliance-gebeurtenissen worden weergegeven onder **Live Logs**:

Naleving



Niet-naleving



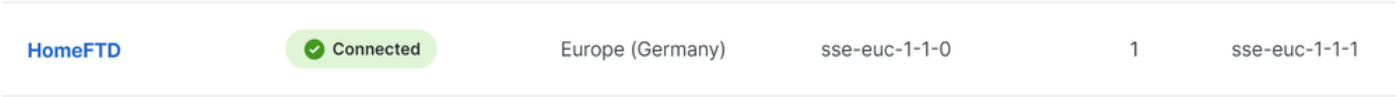
Eerste stappen met beveiligde toegang en ISE-integratie

In het volgende voorbeeld staat Cisco ISE onder netwerk 192.168.10.0/24 en moet de configuratie van de netwerken die via de tunnel bereikbaar zijn, worden toegevoegd onder de tunnelconfiguratie.

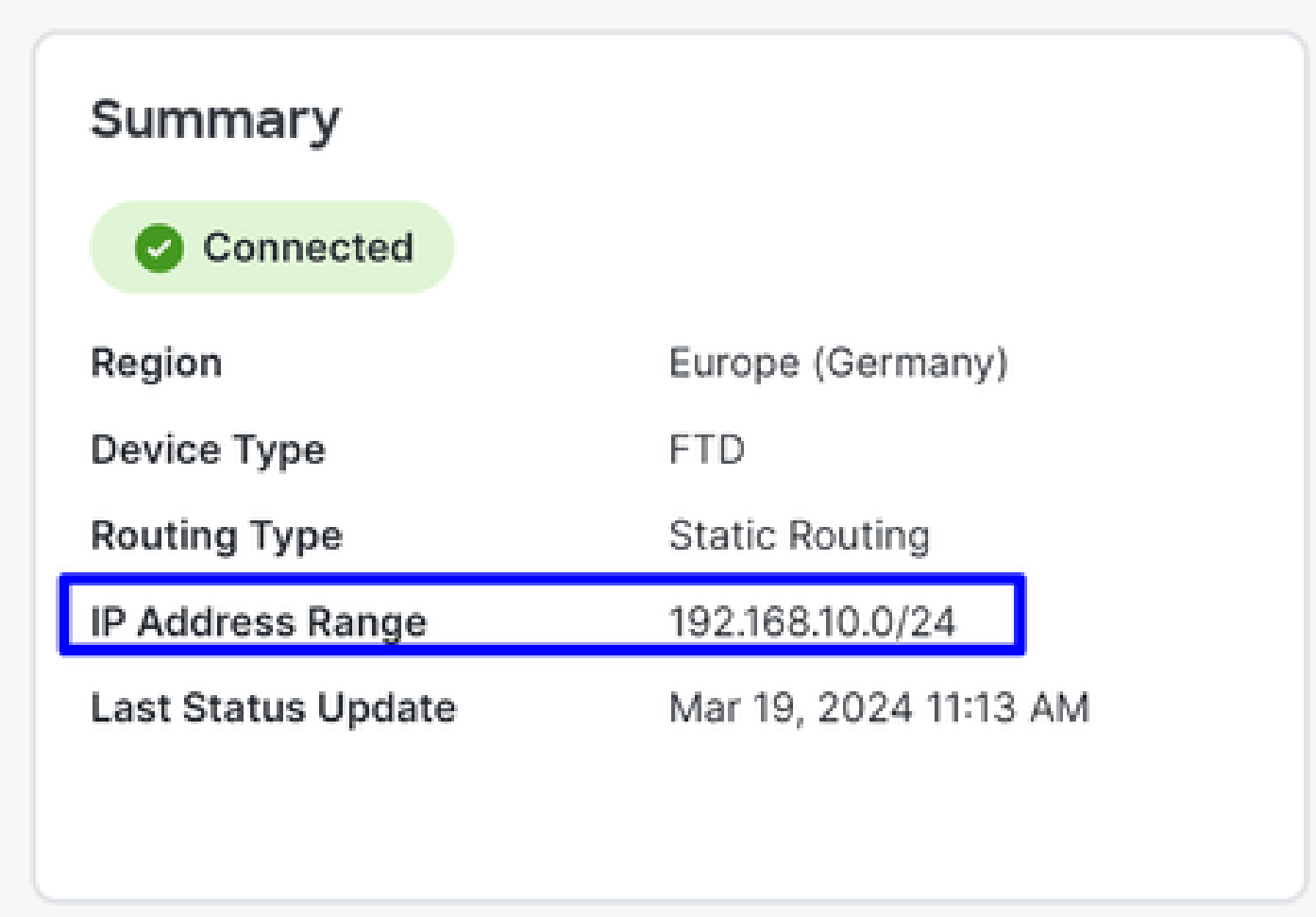
Step 1: Controleer uw tunnelconfiguratie:

Om dit te verifiëren, navigeer naar uw Secure Access Dashboard.

- Klik op **Connect > Network Connections**
- Klik op **Network Tunnel Groups** > Uw tunnel



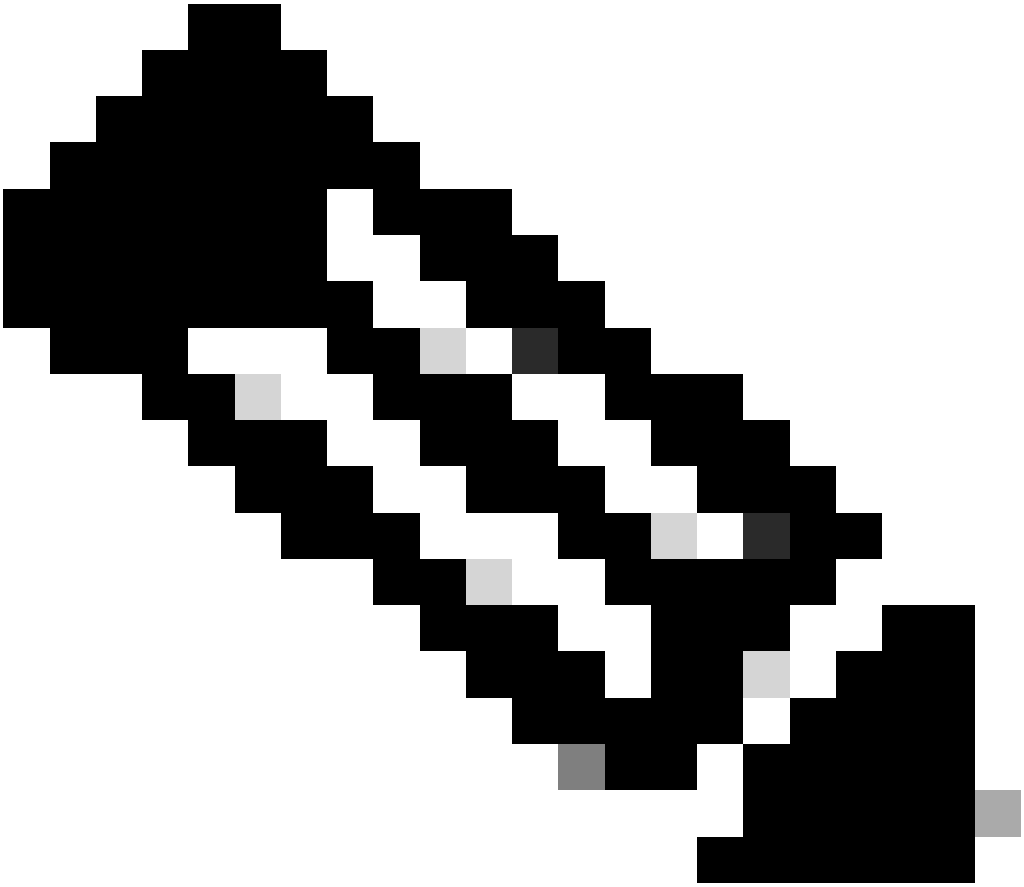
- Controleer onder Samenvatting of de tunnel de adresruimte heeft geconfigureerd waar Cisco ISE is:



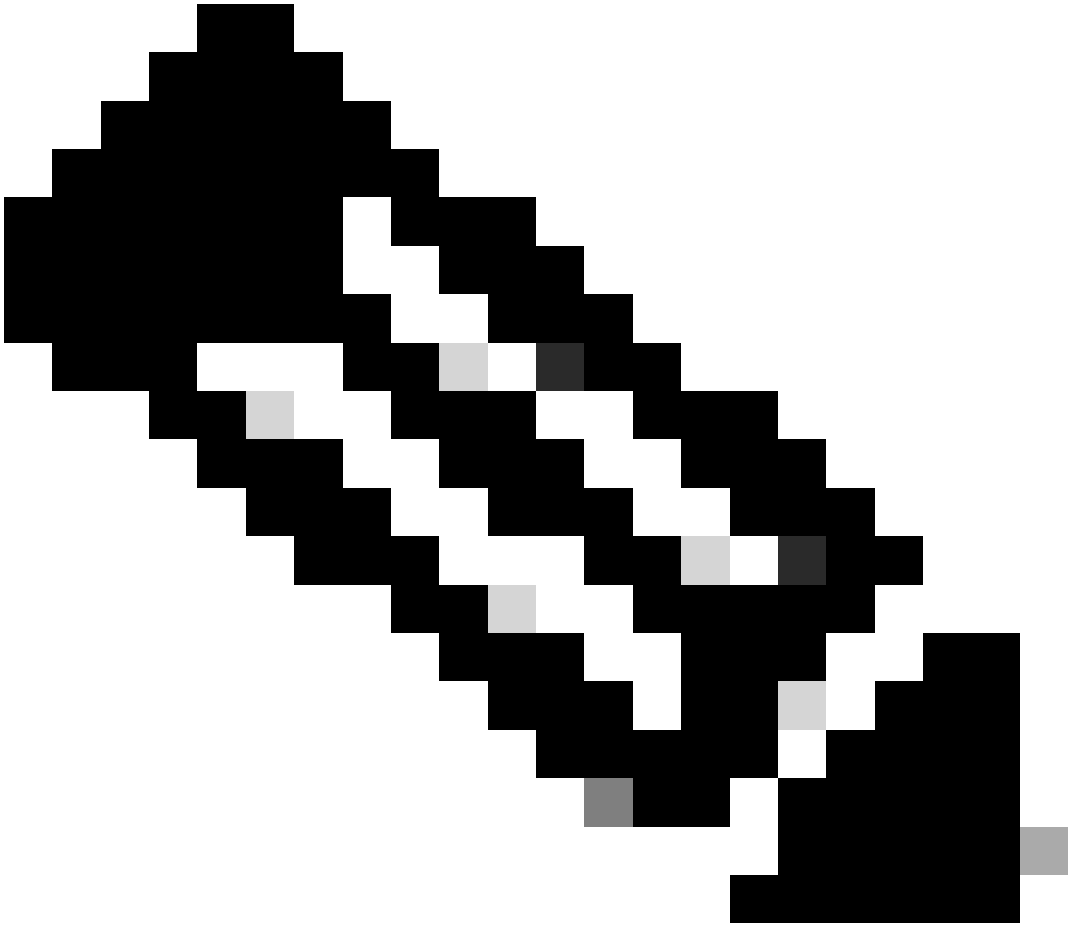
Step 2: Laat het verkeer op uw firewall toe.

Om Secure Access toe te staan om uw ISE-apparaat te gebruiken voor Radius-verificatie, moet u een regel van Secure Access naar uw netwerk geconfigureerd hebben met de vereiste Radius-poorten:

Regel	Bron	Bestemming	Doelpoort
ISE-naar-beveiligde toegang **Beheergroep**	ISE_server	IP-beheerpool (RA-VPN)	**CACAO** UDP 1700 (standaardpoort)
Secure Access Management IP-pool voor ISE-verkeer	IP-beheergroep	ISE_server	**Verificatie, autorisatie** UDP 1812 (standaardpoort) **Accounting** UDP 1813 (standaardpoort)
Secure Access Endpoint IP-pool naar ISE	Endpoint IP-groep	ISE_server	**Provisioning-portal** TCP 8443 (standaardpoort)
Secure Access Endpoint IP-pool naar DNS-SERVER	Endpoint IP-groep	DNS-server	**DNS** UDP en TCP/IP53



Opmerking: als u meer poorten met betrekking tot ISE wilt weten, raadpleegt u de Gebruikershandleiding - Poortreferentie.



Opmerking: er is een DNS-regel nodig als u hebt ingesteld dat uw ISE wordt ontdekt via een naam, zoals ise.ciscospt.es

---

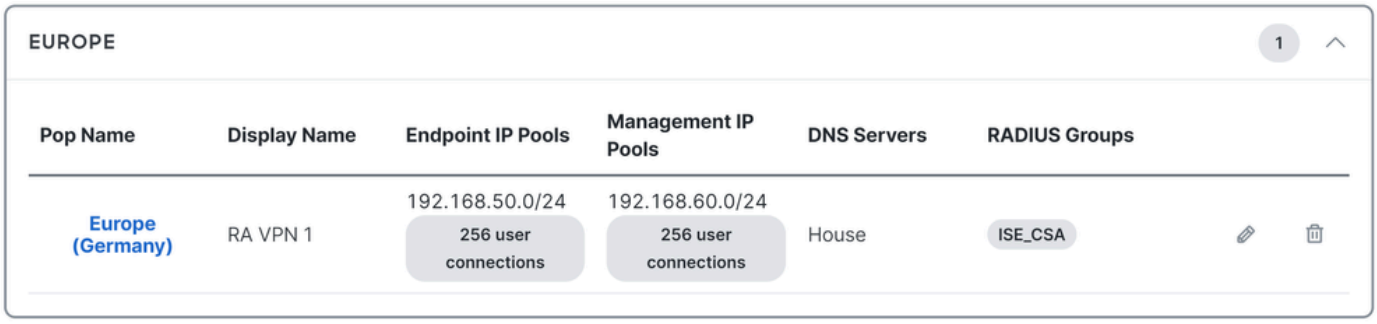
IP-beheerpool en endpoint

Om uw beheer en endpoint IP pool te verifiëren, navigeer aan uw Secure Access Dashboard:

- Klik op **Connect > End User Connectivity**
- Klik op Virtual Private Network

- Onder **Manage IP Pools**

- Klik op **Manage**



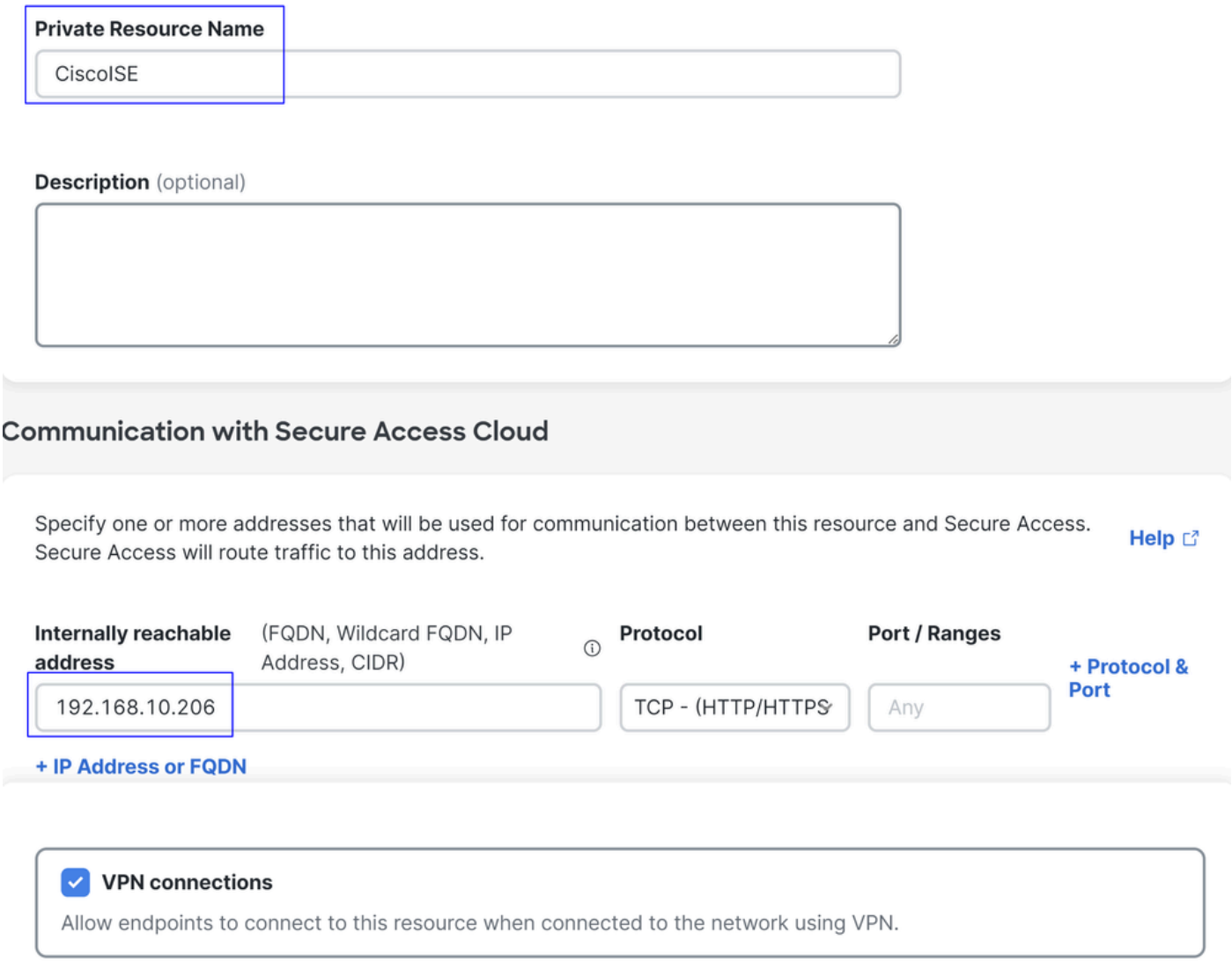
Stap 3: Controleer of uw ISE is geconfigureerd onder Private Resources

ISE Provisioning Portal Om de gebruikers die via VPN zijn verbonden toe te laten om naar te navigeren, moet u er zeker van zijn dat u uw apparaat hebt geconfigureerd als een Private Resource om toegang te bieden, die wordt gebruikt om de automatische provisioning van het ISE Posture Module via VPN toe te staan.

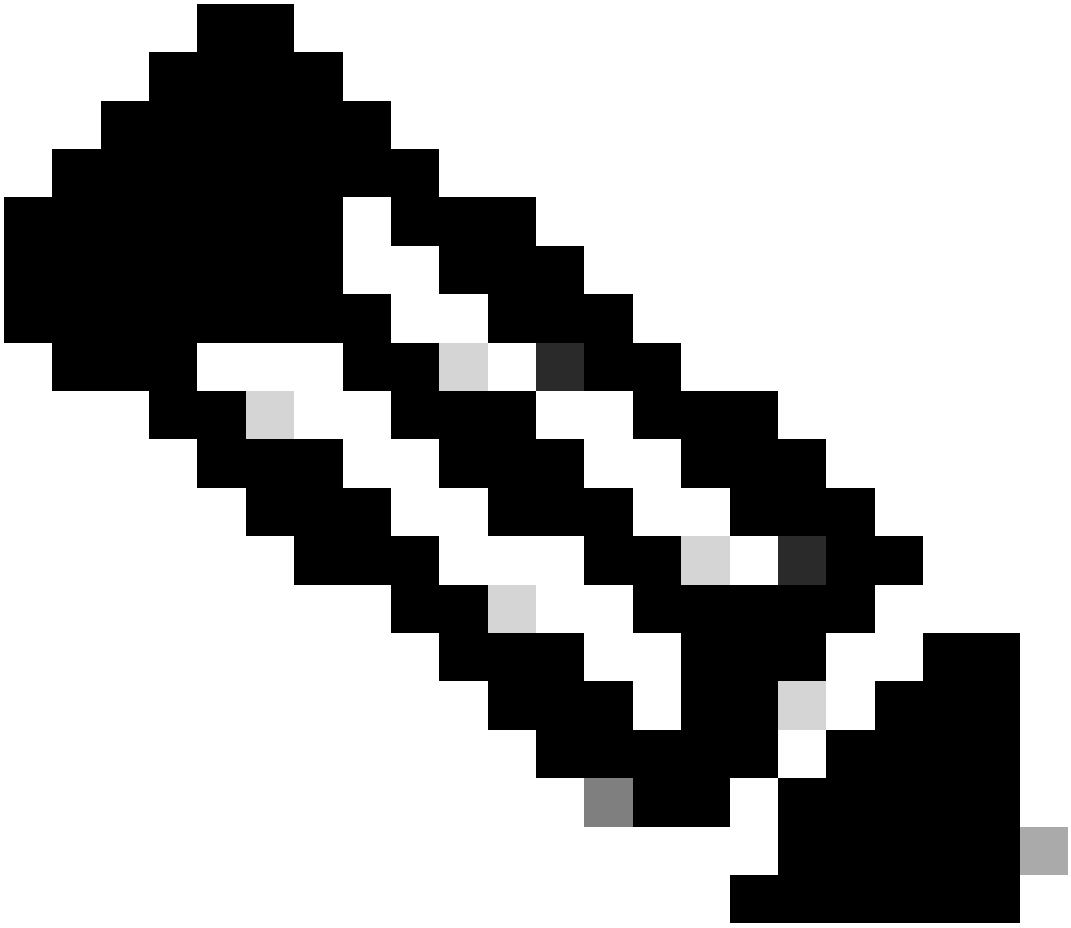
Om te verifiëren dat u ISE correct hebt geconfigureerd, navigeer dan naar uw Secure Access Dashboard:

- Klik op **Resources > Private Resources**

- Klik op de ISE-bron



Indien nodig kunt u de regel beperken tot de provisioningpoort (8443).



Opmerking: controleer of u het selectievakje voor VPN-verbindingen hebt gemarkeerd.

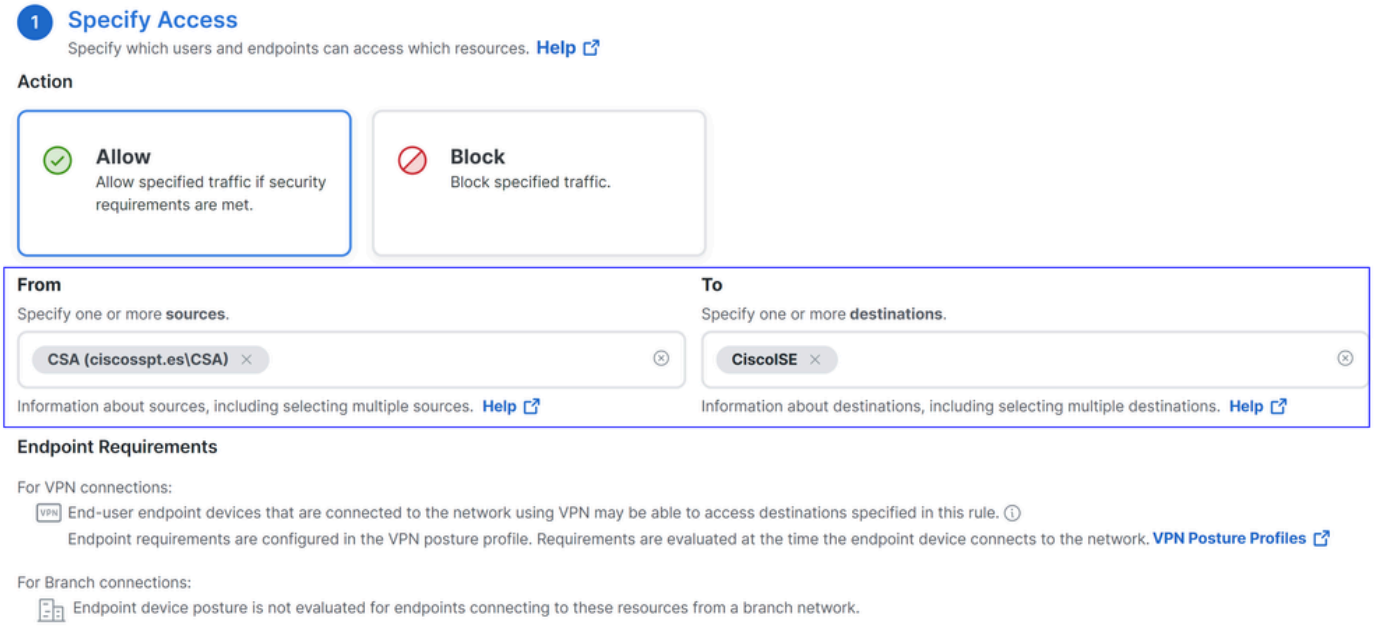
Stap 4: Laat ISE-toegang toe onder het toegangsbeleid

ISE Provisioning Portal Om de gebruikers die via VPN zijn verbonden toe te staan om naar te navigeren, moet u er zeker van zijn dat u hebt geconfigureerd en **Access Policy** om de gebruikers die onder die regel zijn geconfigureerd, toe te staan om toegang te krijgen tot de Private Resource die in Step3 is geconfigureerd.

Om te verifiëren dat u ISE correct hebt geconfigureerd, navigeer dan naar uw Secure Access Dashboard:

- Klik op **Secure** > **Access Policy**

- Klik op de regel die is ingesteld om toegang tot de VPN-gebruikers tot ISE toe te staan

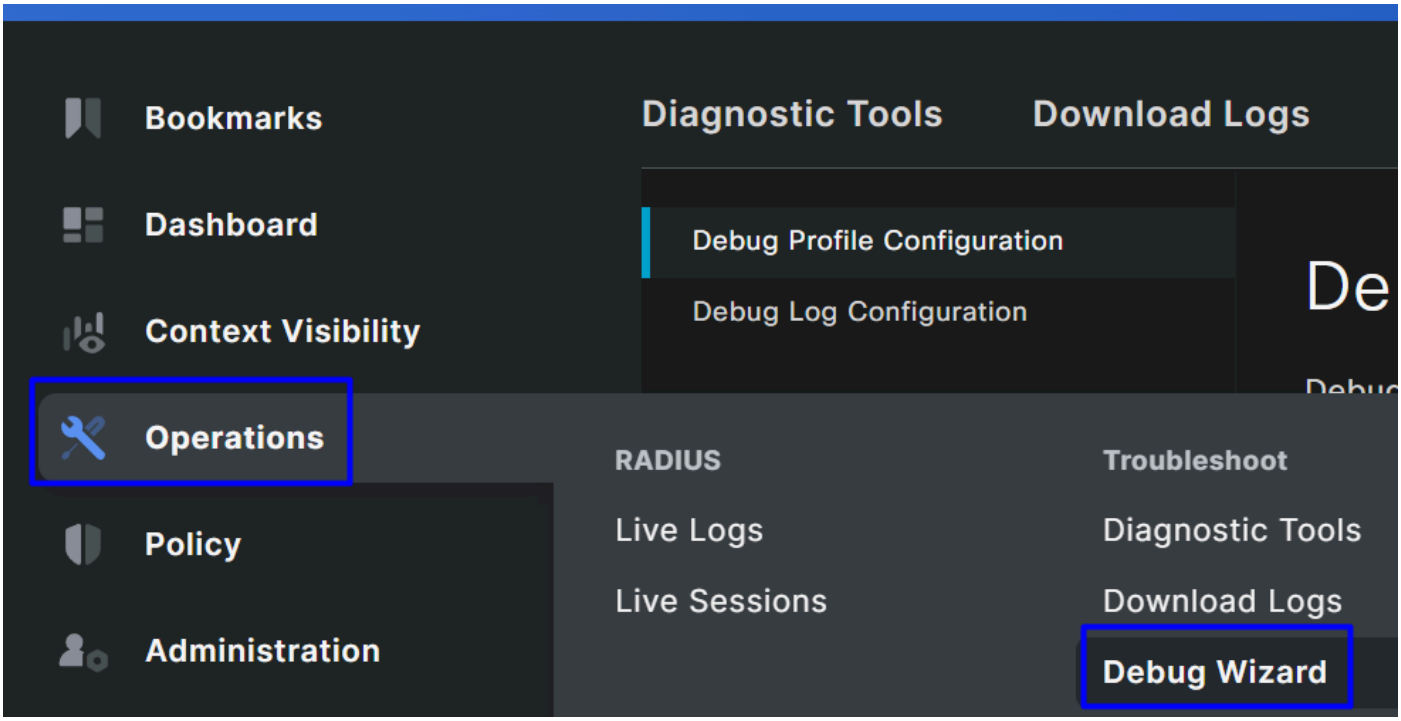


Problemen oplossen

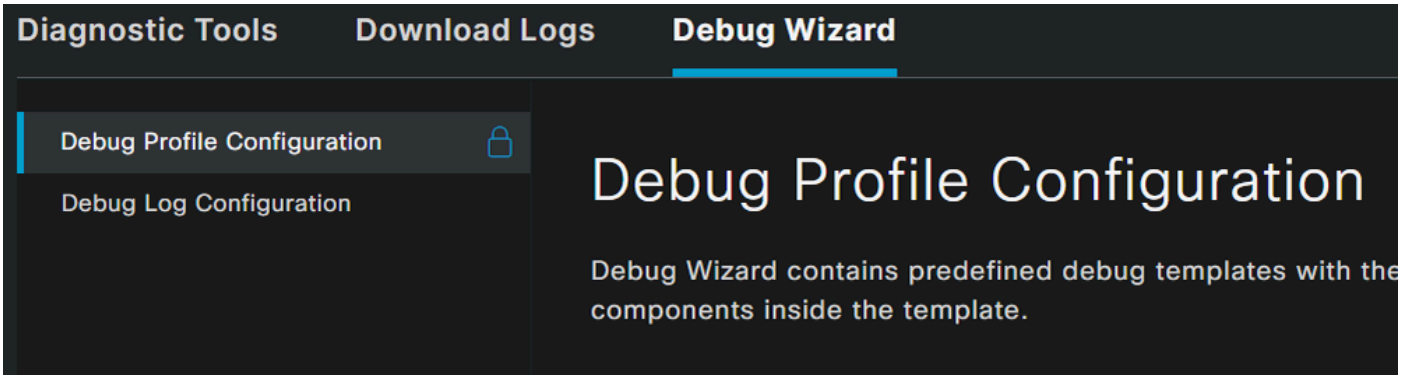
Hoe te downloaden ISE postuur Debug logboeken

Als u ISE Logs wilt downloaden om een probleem met betrekking tot postuur te verifiëren, gaat u verder met de volgende stappen:

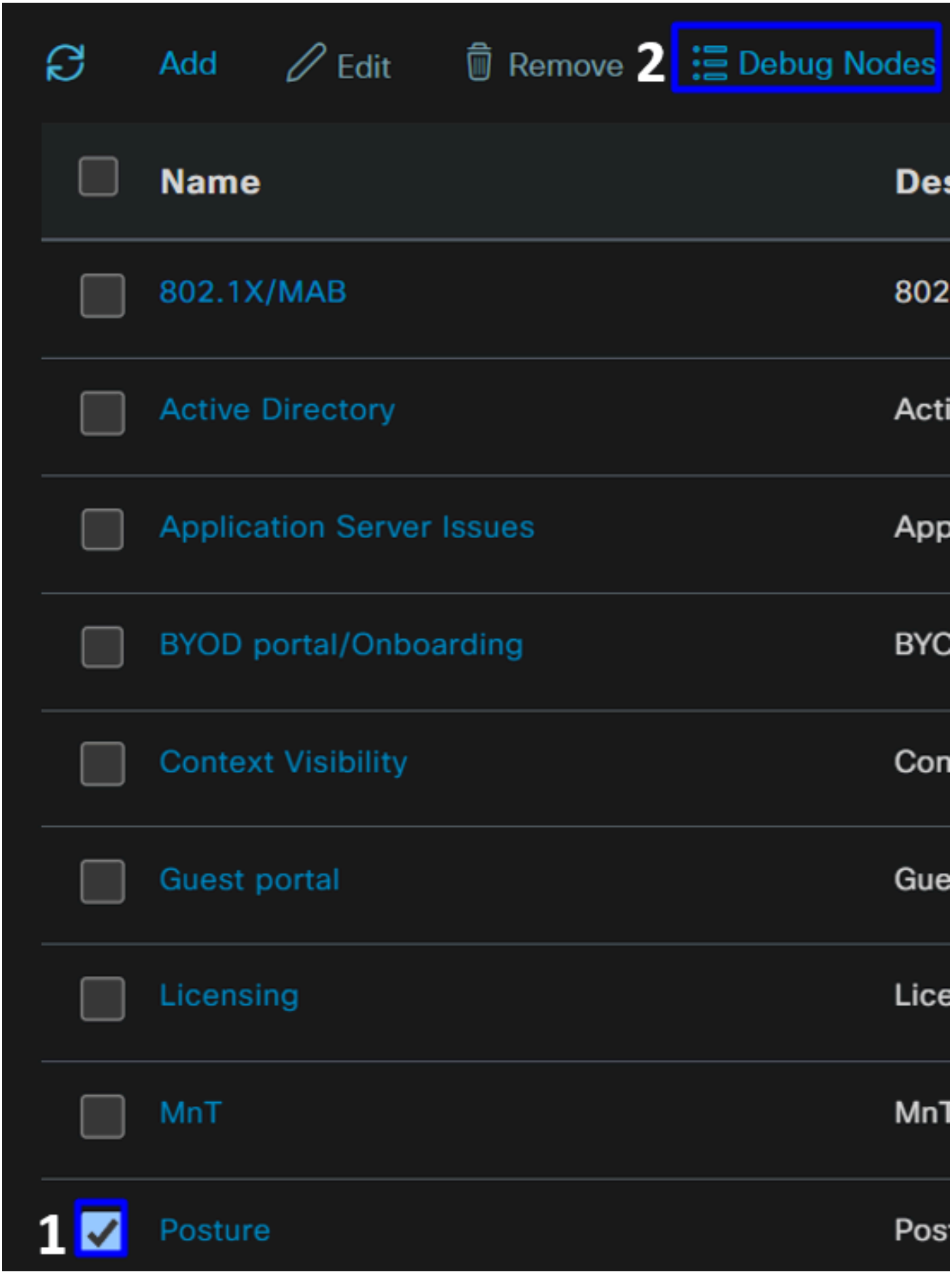
- Naar uw ISE-dashboard navigeren
- Klik op Operations > Troubleshoot > Debug Wizard



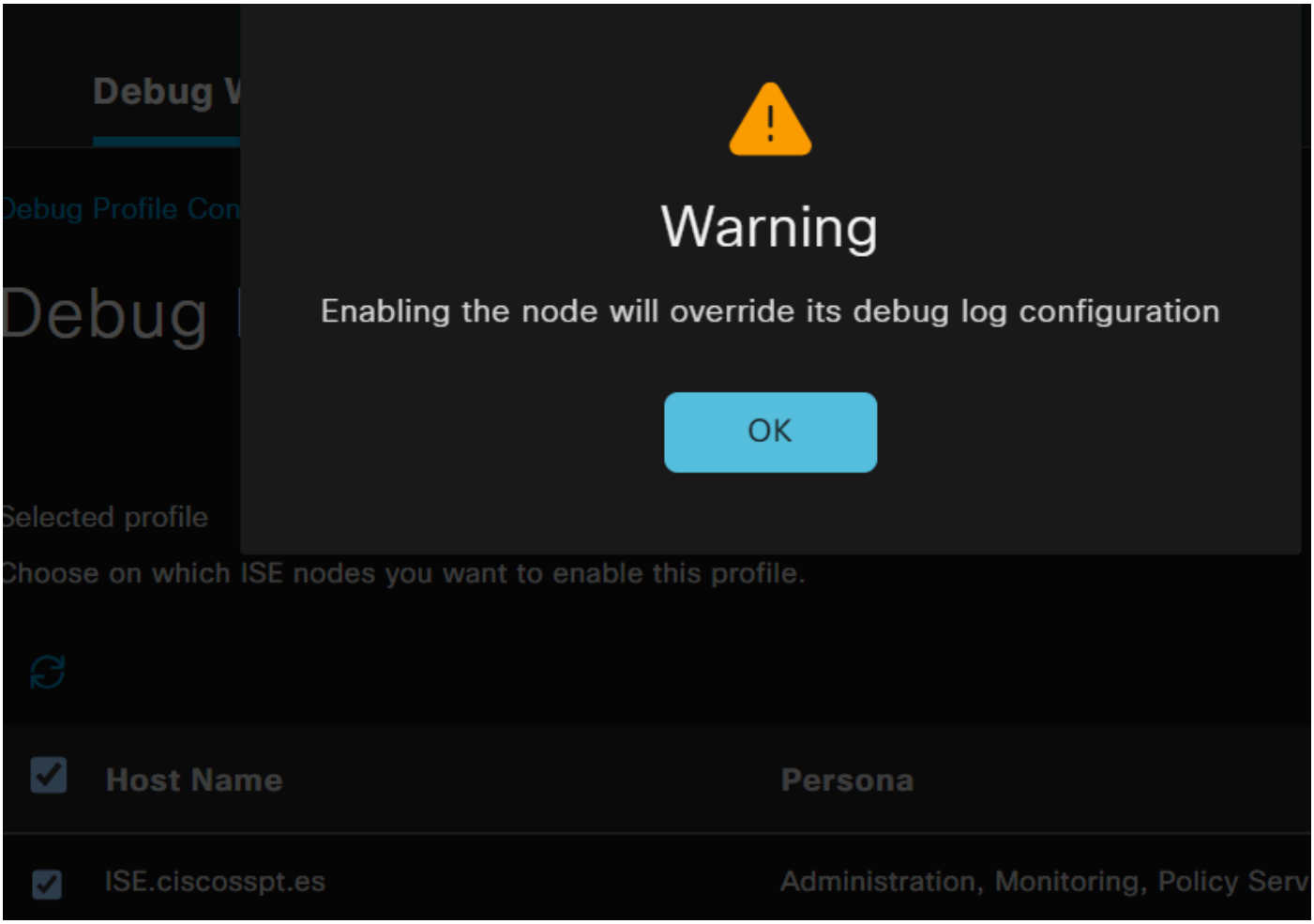
- Klik op Debug Profile Configuration



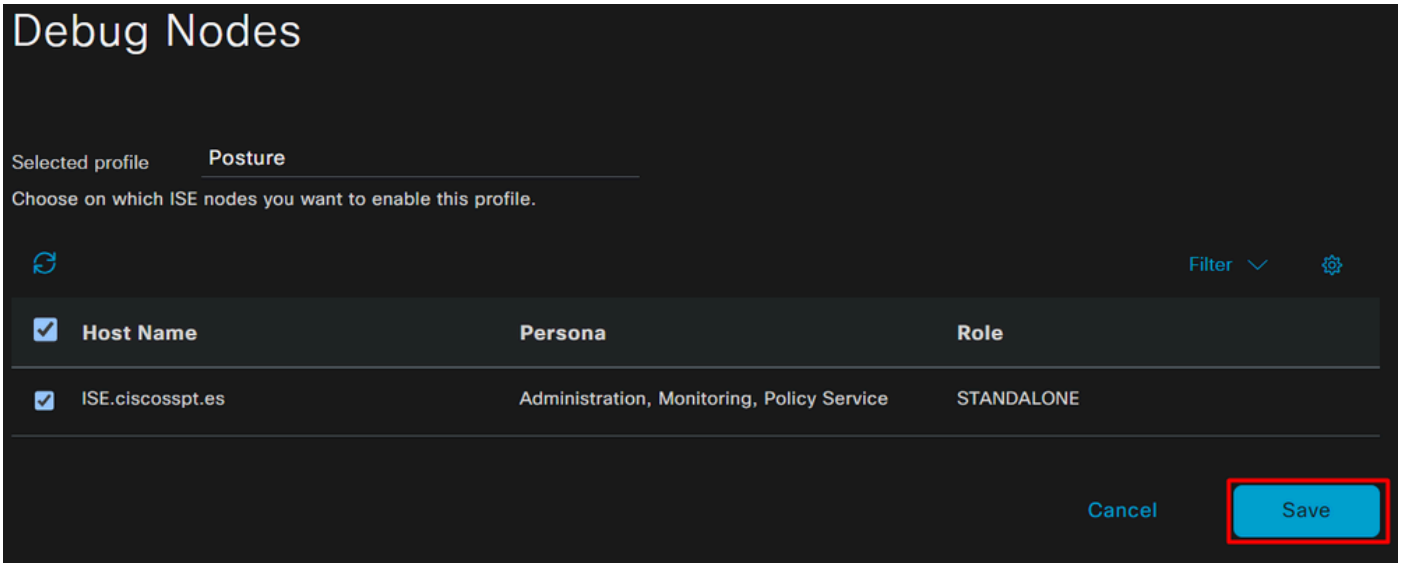
- Schakel het selectievakje in voor **Posture > Debug Nodes**

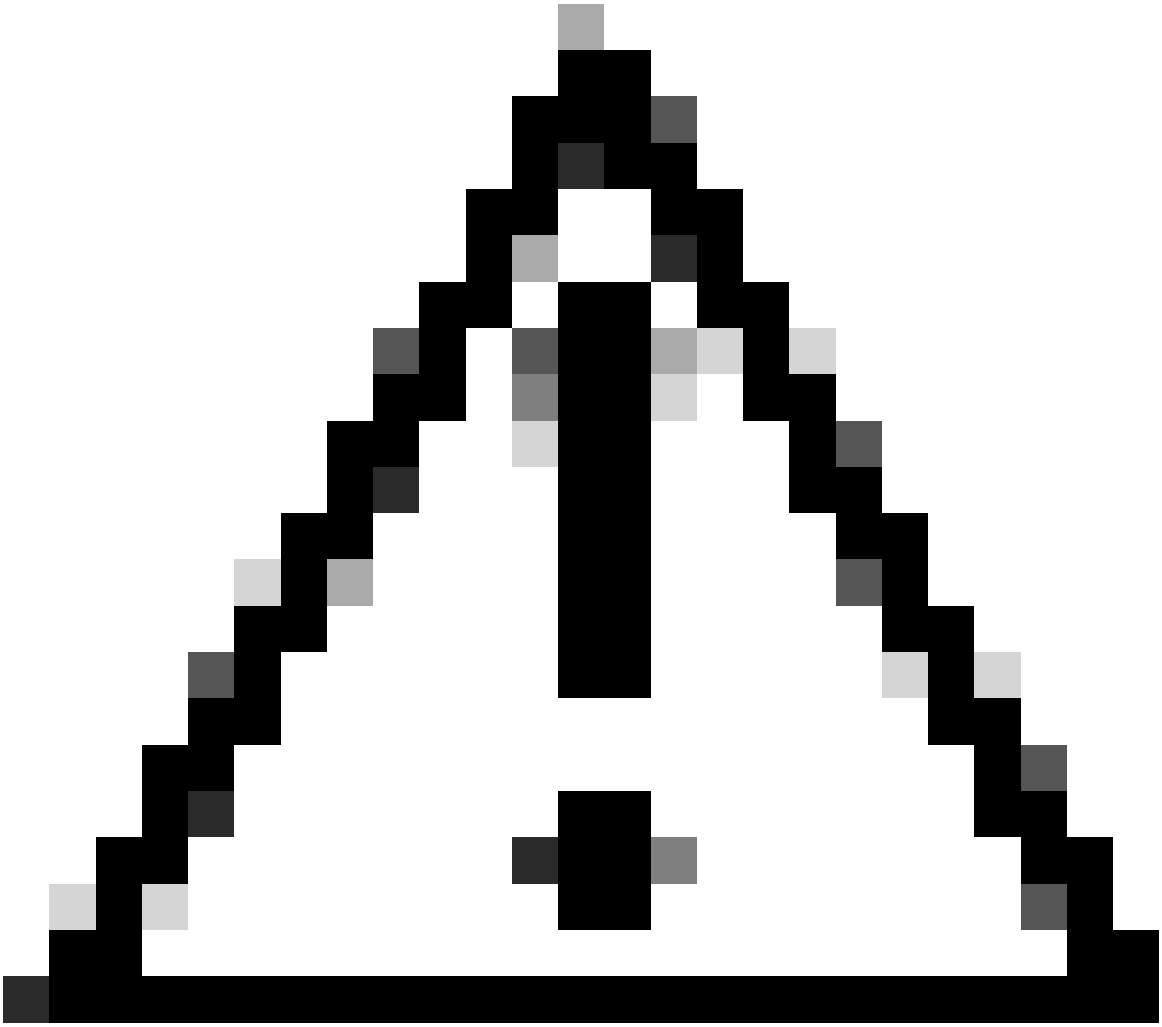

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- Markeer het aanvinkvakje voor de ISE-knooppunten waarop u de debug-modus wilt inschakelen om het probleem op te lossen



- Klik op de knop Save

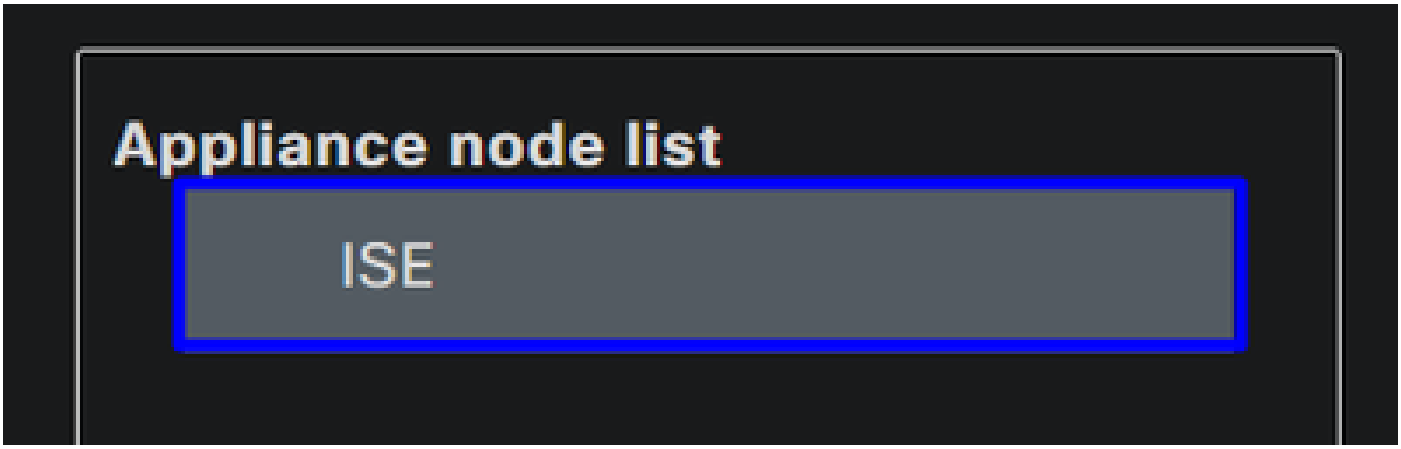

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



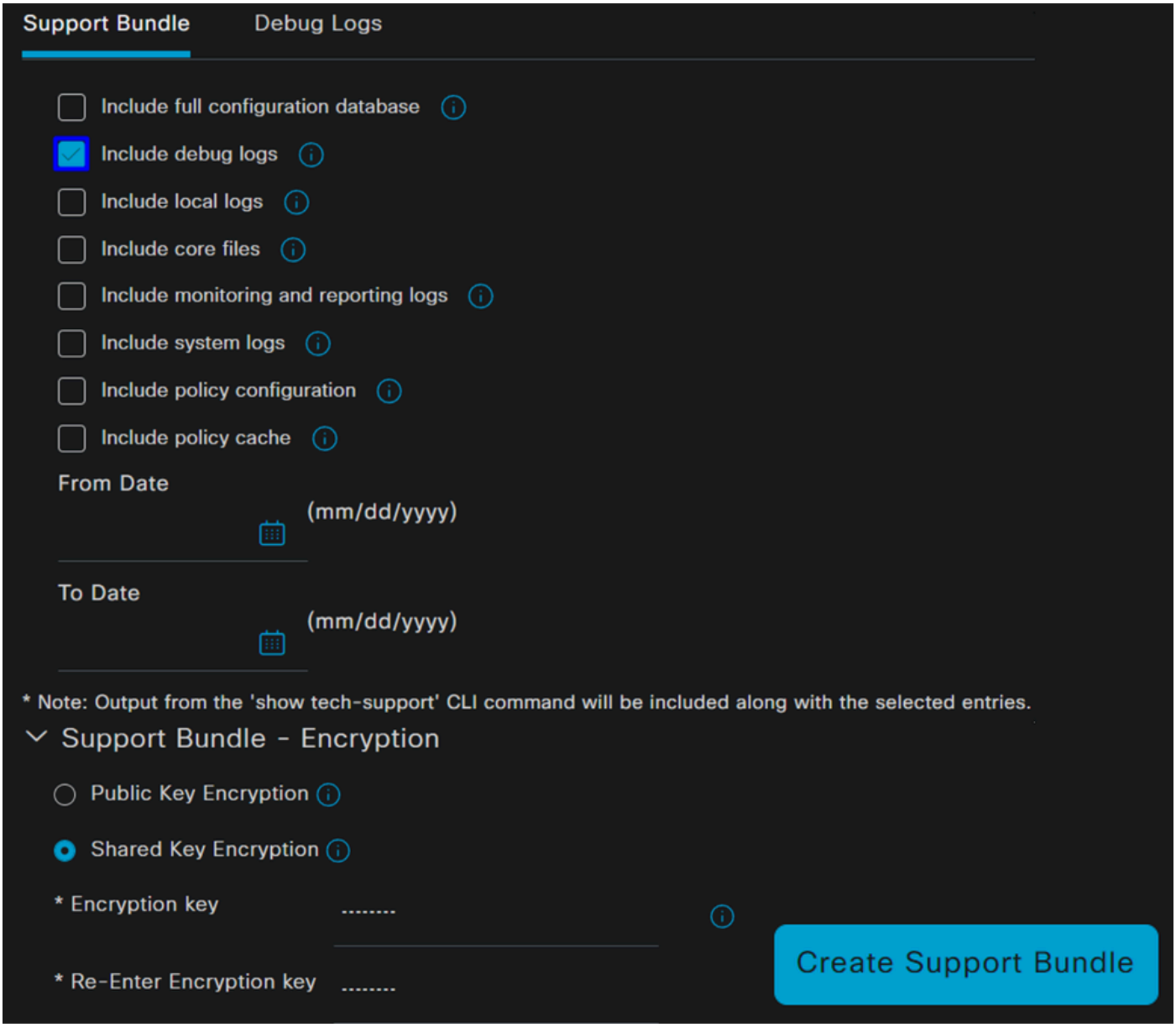
Waarschuwing: na dit punt moet je het probleem gaan reproduceren; **the debug logs can affect the performance of your device**.

Nadat u het probleem hebt gereproduceerd, gaat u verder met de volgende stappen:

- Klik op Operations > Download Logs
- Kies de knoop van waar u de logboeken wilt nemen

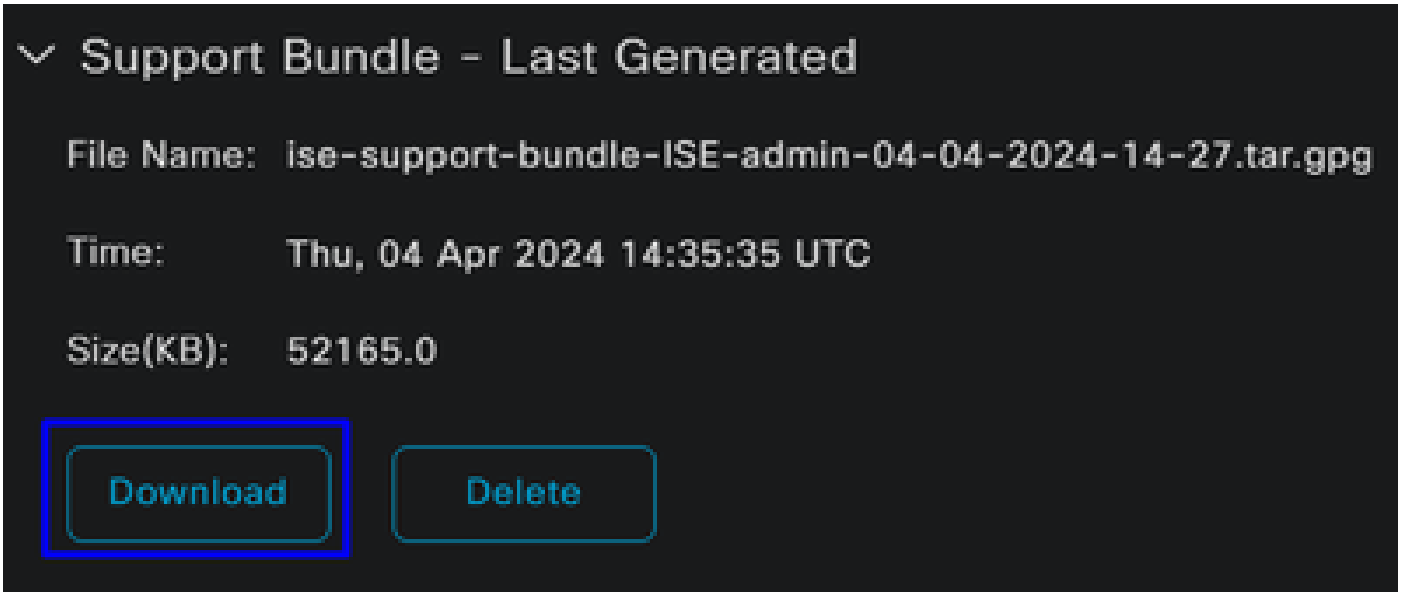


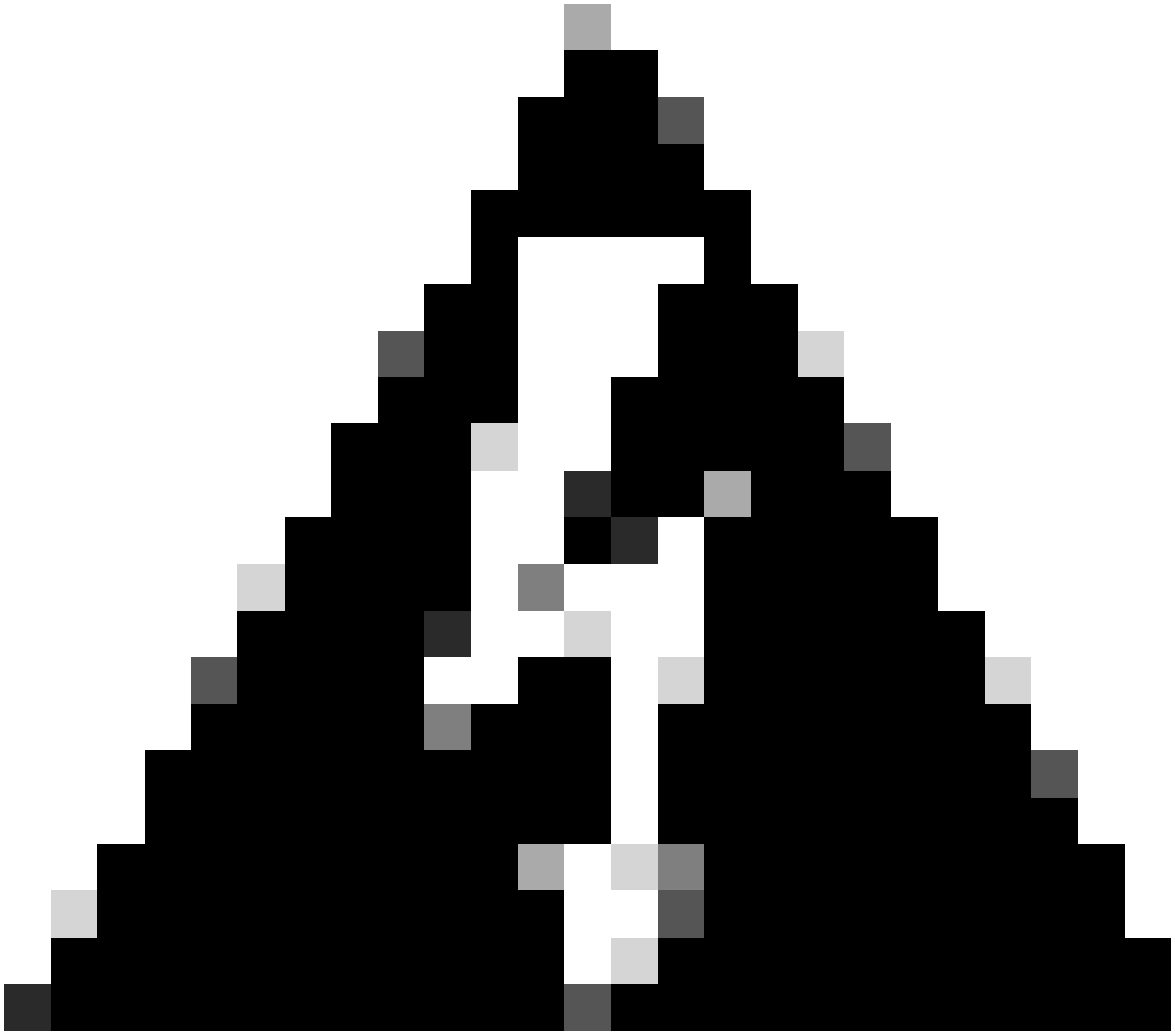
- Selecteer onder **Support Bundle** de volgende opties:



- Include debug logs
- Onder **Support Bundle Encryption**
    - **Shared Key Encryption**
        - Vullen **Encryption key** en **Re-Enter Encryption key**

- Klik op de knop **Create Support Bundle**
- Klik op de knop **Download**



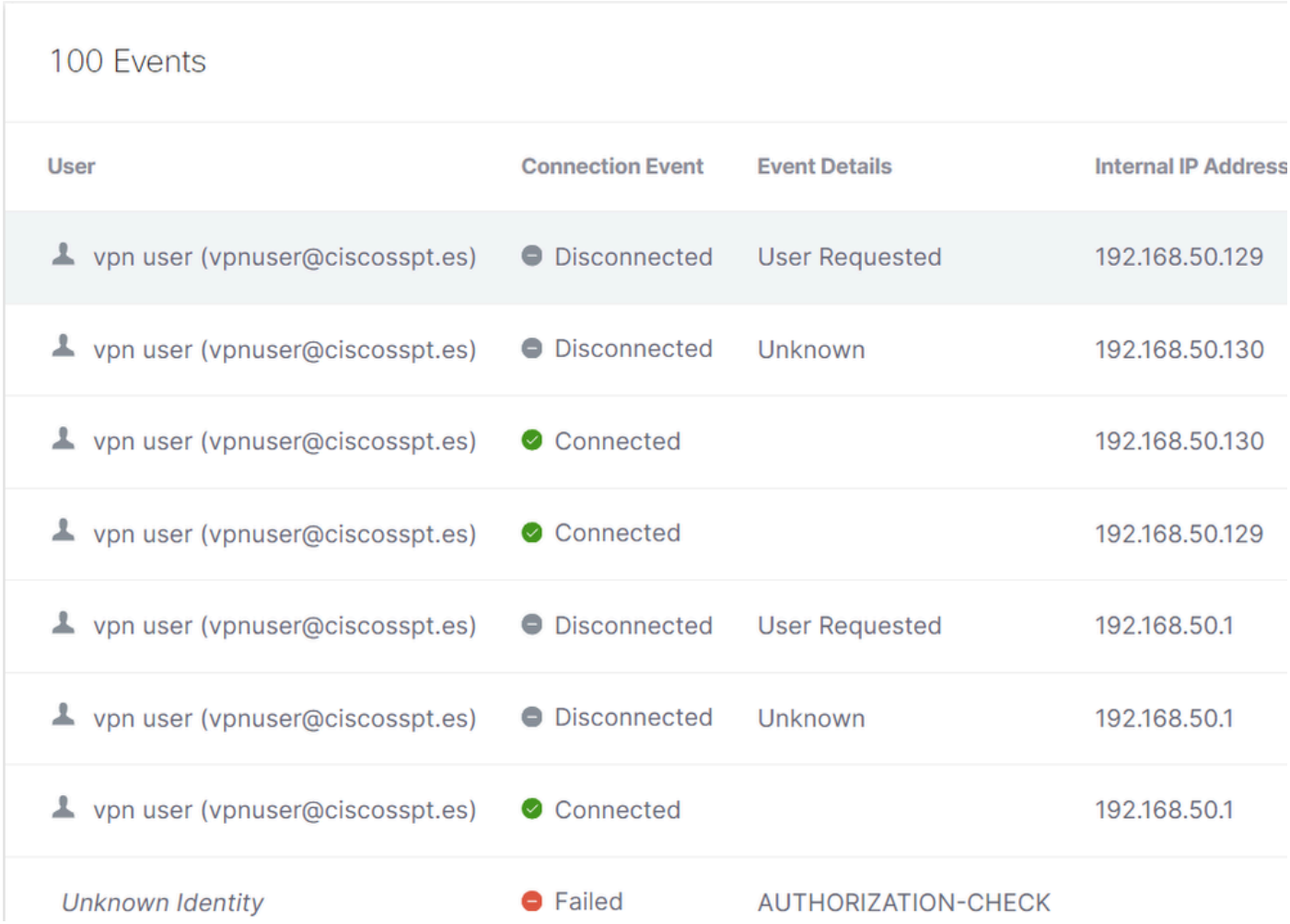


Waarschuwing: de debug-modus uitschakelen die is ingeschakeld bij de stap, debug profiel configureren

Hoe te om de Veilige Logboeken van de Toegang Verre Toegang te verifiëren

Navigeer naar uw Secure Access Dashboard:

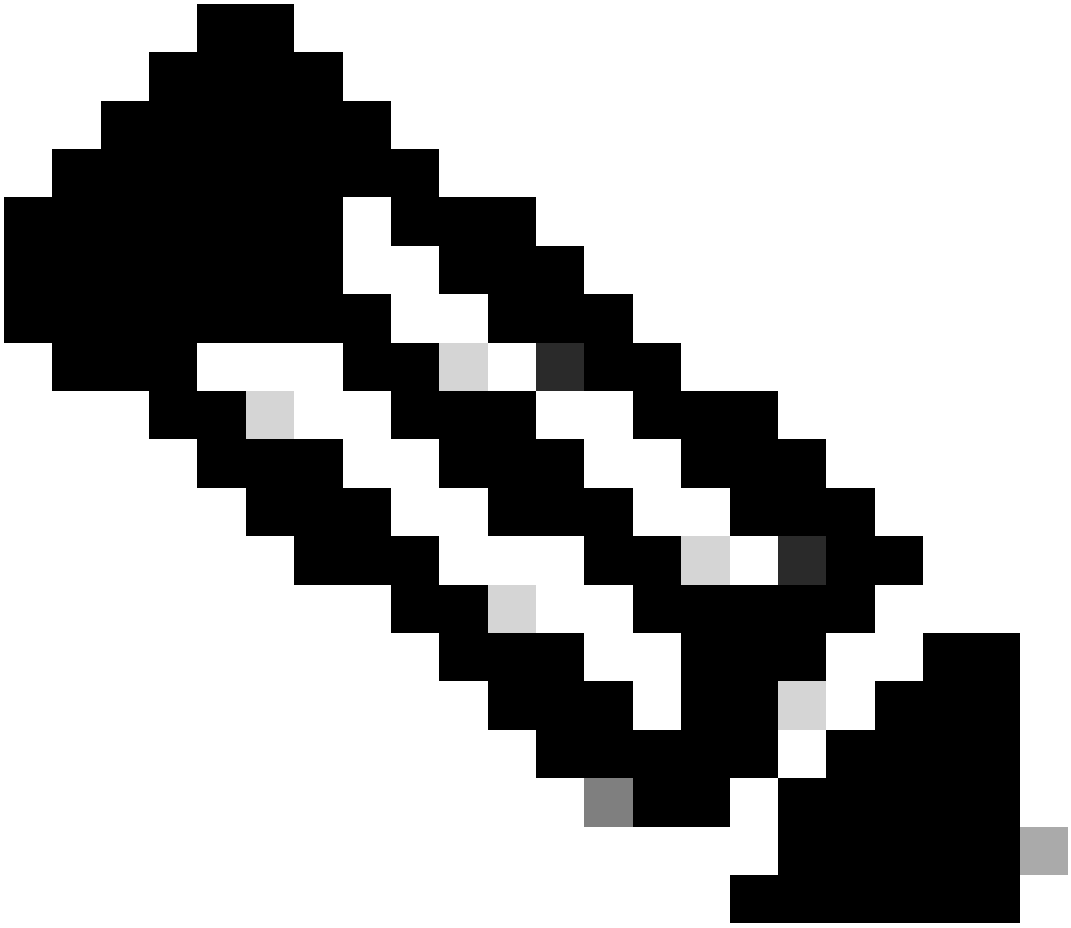
- Klik op Monitor > Remote Access Logs



DART-bundel op beveiligde client genereren

Om DART Bundle op uw machine te genereren, verifieert u het volgende artikel:

Cisco Secure Client-diagnostische en -rapportagetool (DART)



Opmerking: zodra u de logbestanden hebt verzameld die in de sectie Problemen oplossen worden aangegeven, opent u een case met **TAC** om door te gaan met de analyse van de informatie.

Gerelateerde informatie

- **Cisco Technical Support en downloads**
- **Secure Access-documentatie en gebruikershandleiding**

- **Cisco Secure-clientsoftware downloaden**
- **Beheerdershandleiding voor Cisco Identity Services Engine, release 3.3**

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.