

# Configureer beveiligde toegang voor RA-VPNaaS postenbeoordeling met ISE

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Configuratie van beveiligde toegang](#)

[Radius-groep op de IP-pools configureren](#)

[Configureer uw VPN-profiel voor gebruik ISE](#)

[Algemene instellingen](#)

[Verificatie, autorisatie en accounting](#)

[Traffic Steering](#)

[Cisco Secure-clientconfiguratie](#)

[ISE-configuraties](#)

[Lijst met netwerkapparaten configureren](#)

[Een groep configureren](#)

[Lokale gebruiker configureren](#)

[Beleidsset configureren](#)

[Configuratie van verificatie en autorisatie van beleidsset](#)

[Lokale of actieve mapgebruikers van RADIUS configureren](#)

[ISE-houding configureren](#)

[Posteringvoorwaarden configureren](#)

[Houdingsvereisten configureren](#)

[Posturebeleid configureren](#)

[Clientprovisioning configureren](#)

[Clientprovisioningbeleid configureren](#)

[De autorisatieprofielen maken](#)

[Instellen van posteringsbeleid configureren](#)

[Verifiëren](#)

[Posture Validation](#)

[Verbinding op de machine](#)

[Hoe logboeken te verzamelen in ISE](#)

[Naleving](#)

[Niet-naleving](#)

[Eerste stappen met beveiligde toegang en ISE-integratie](#)

[Problemen oplossen](#)

[Hoe te downloaden ISE postuur Debug logboeken](#)

[Hoe te om de Veilige Logboeken van de Toegang Verre Toegang te verifiëren](#)

[DART-bundel op beveiligde client genereren](#)

---

## 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

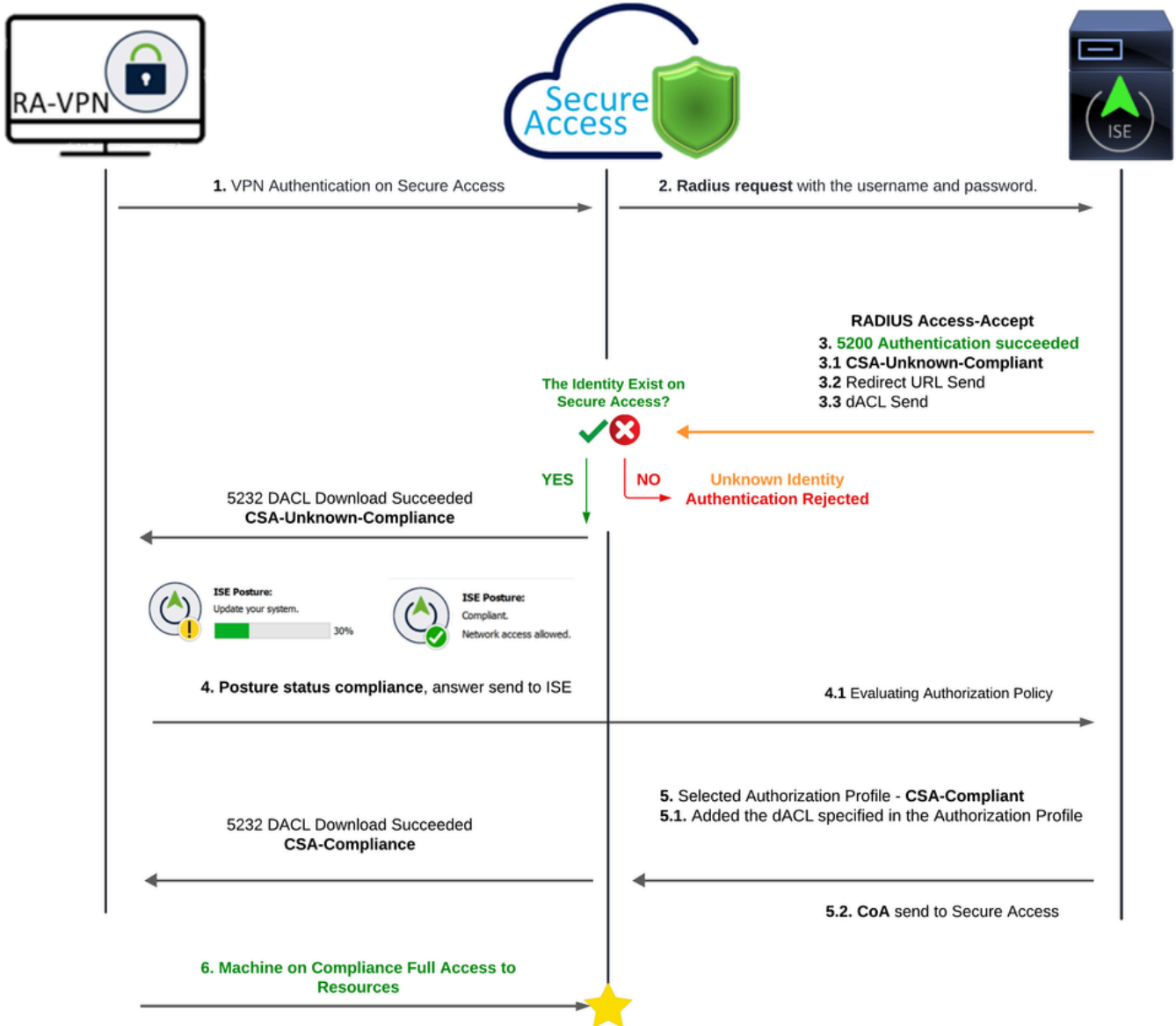
De informatie in dit document is gebaseerd op:

- 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

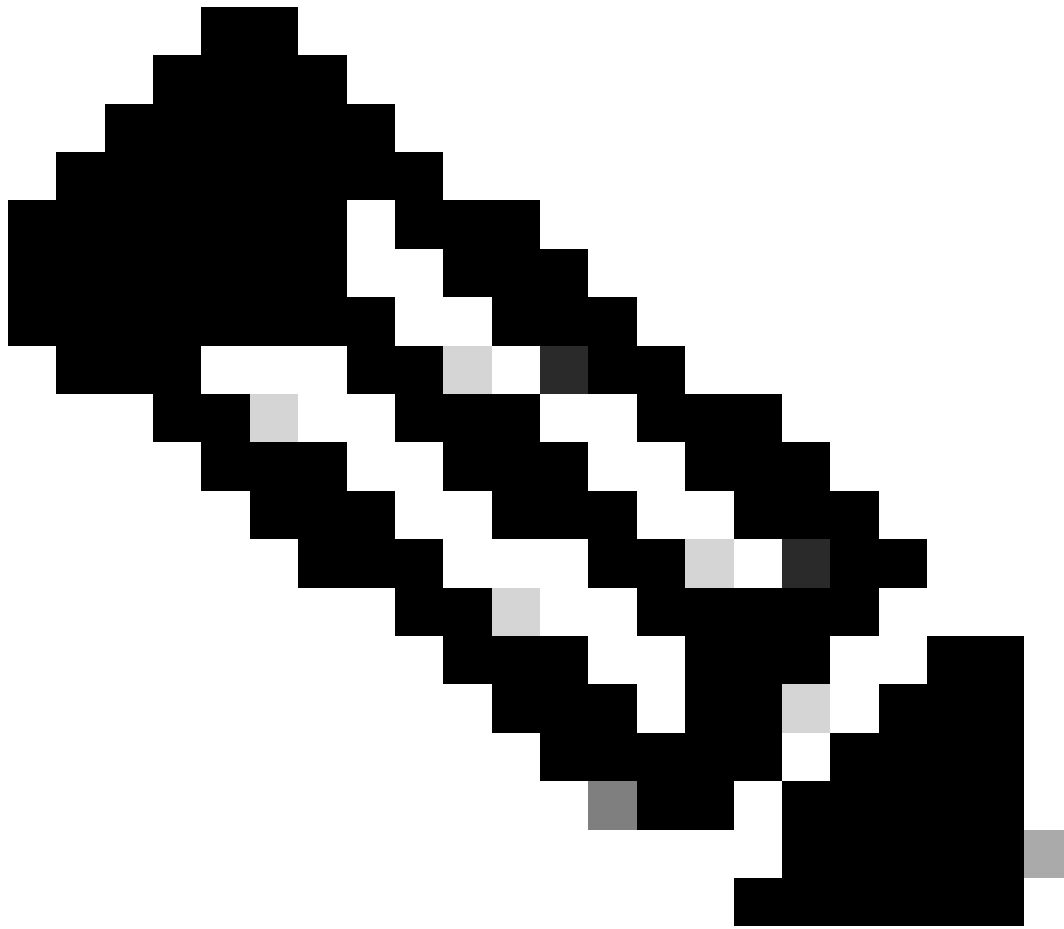
vpnuser@ciscospt.es



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.

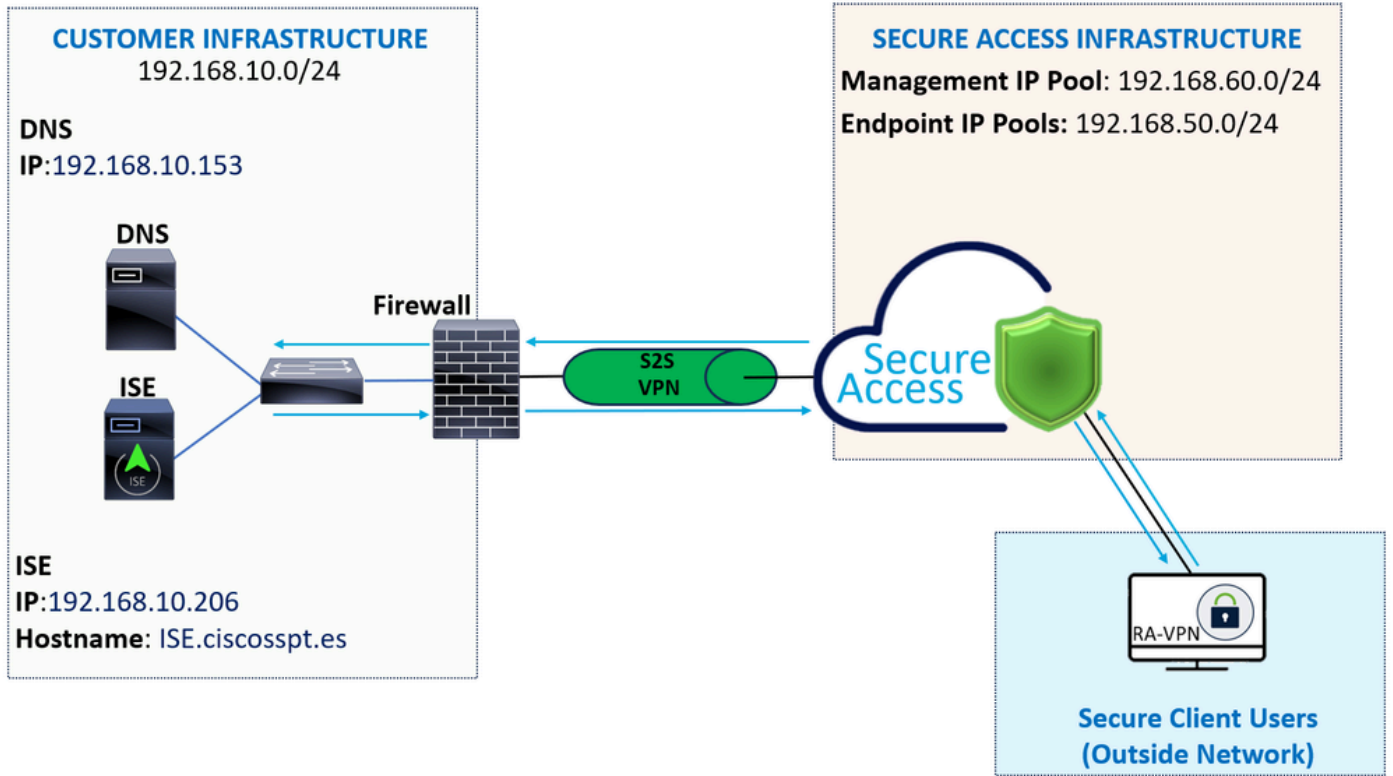


Opmerking: om de RADIUS-integratie te configureren, moet u ervoor zorgen dat u communicatie tussen beide platforms hebt.

---

## Netwerkdigram





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**) op **Manage**

## Manage IP Pools

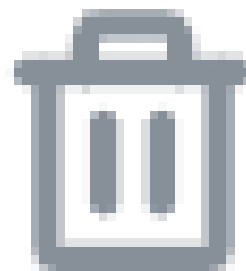
Manage

2 Regions mapped

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

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- 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

## RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



**No RADIUS groups created**

**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

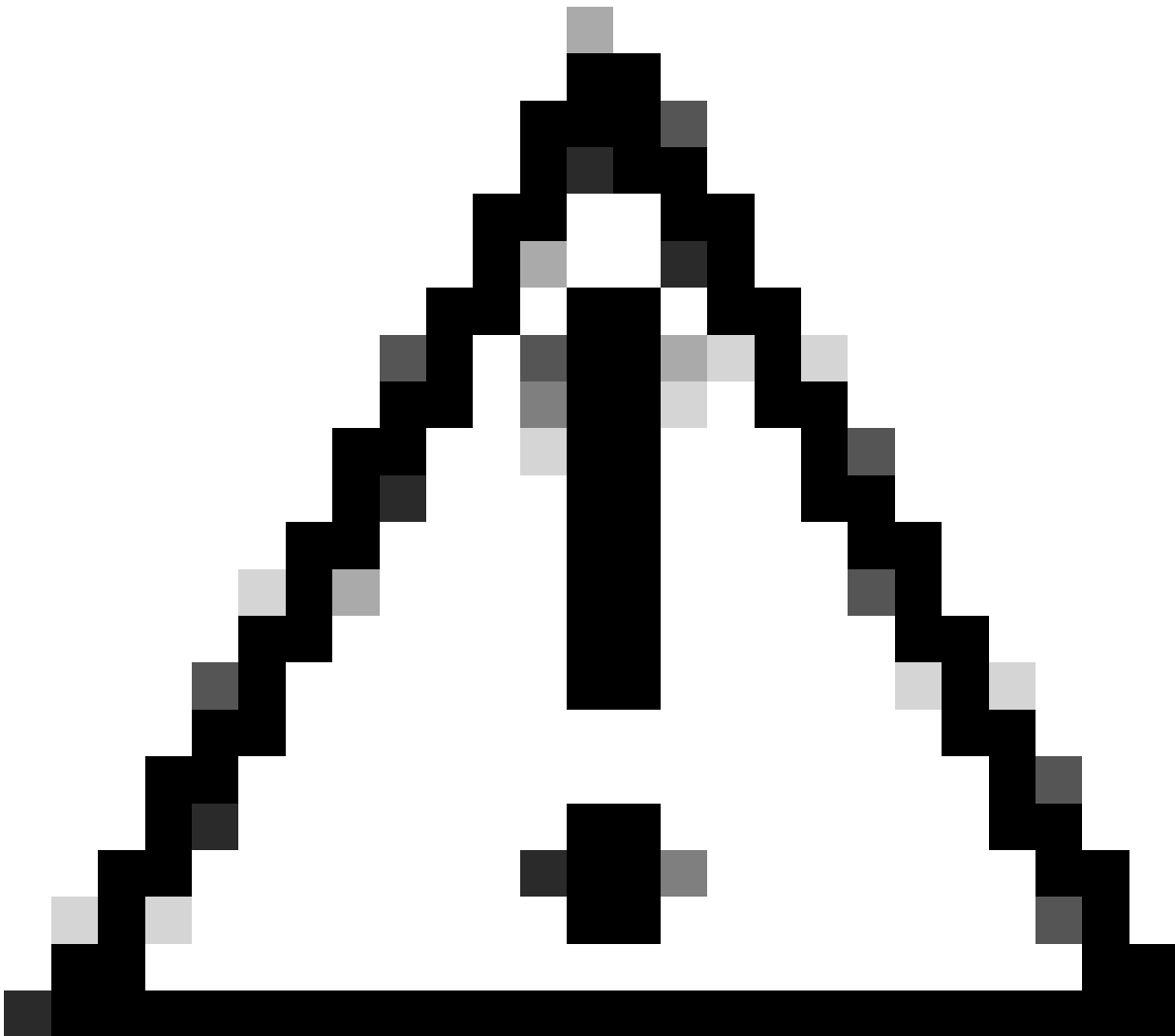
- **Authorization:** Vink het selectievakje aan Authorization en selecteer de poort, standaard, is 1812

- 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

## RADIUS Servers

You can add up to 8 servers in each group

### Assign servers

**+ Add**

#	Server Name	IP Address
---	-------------	------------

- Configureer vervolgens de volgende opties:

## Add RADIUS Server

Server name

IP Address

Password type

Secret Key

 [Show](#)

Password

 [Show](#)

**Cancel**

**Save & Add server**

**Save**



- **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:

## RADIUS Servers

You can add up to 8 servers in each group

### Assign servers

^

ISE\_CSA

[+ Add](#)

---

- 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

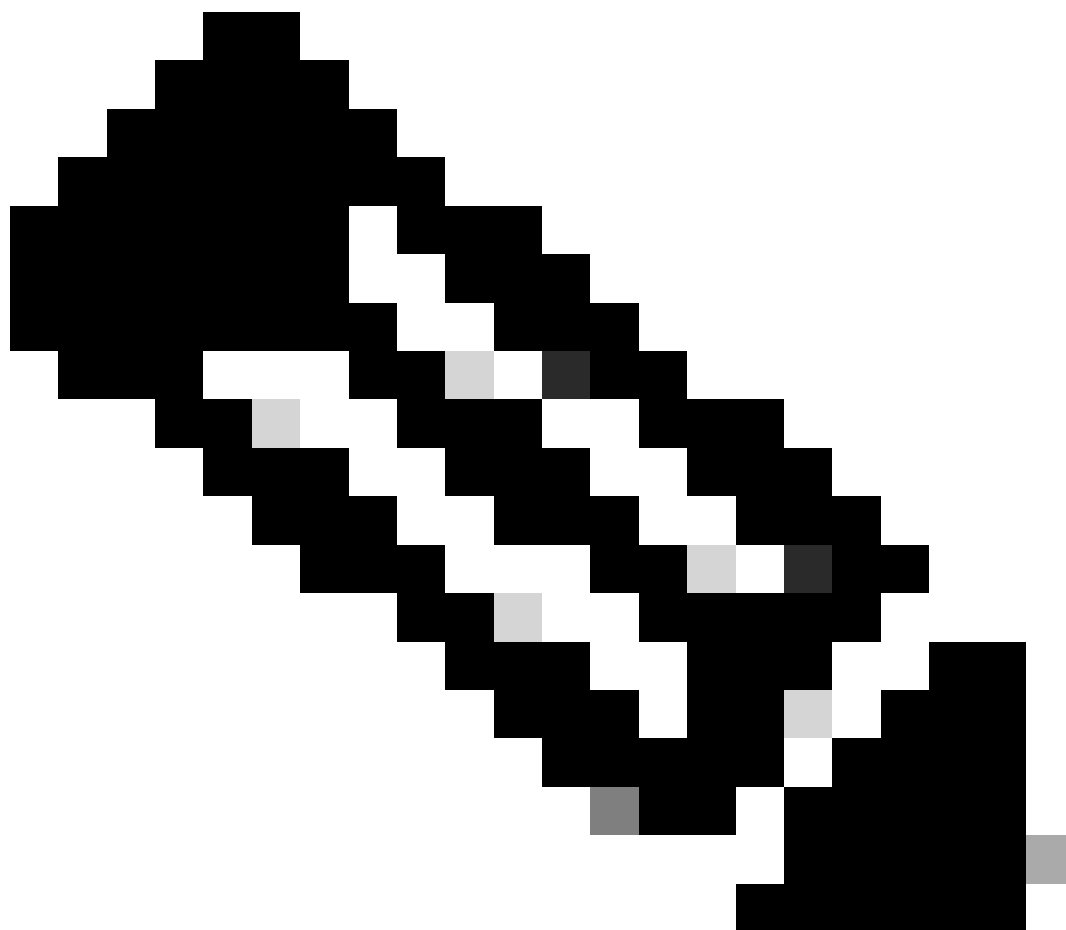
Assign servers

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

- ✓ **General settings**  
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**  
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**  
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

### Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

**Enable Radius Authorization**  
Use defaults or customize groups to map to regions

Select one group for all regions + Group

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

< Cancel Back Next

- **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.

- ✓ **General settings**  
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**  
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**  
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

## Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication   Authorization   Accounting

**Enable Radius Accounting**  
Use defaults or customize groups to map to regions

Select one group for all regions + Group

ISE\_CSA ▼

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA <span style="float: right;">▼</span>
RA VPN 1	192.168.60.0/24	ISE_CSA (default) <span style="float: right;">▼</span>



Cancel

Back

Next

- **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 met Traffic Steering.

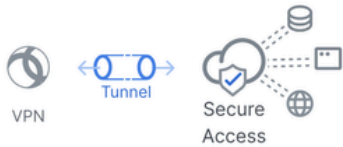
Besturing van verkeer

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

**Tunnel Mode**

Connect to Secure Access

All traffic is steered through the tunnel.



**Tunnel Mode**

Bypass Secure Access

All traffic is steered outside the tunnel.



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

Connect to Secure Access

All traffic is steered through the tunnel.



**Add Exceptions**

Destinations specified here will be steered **OUTSIDE** the tunnel.

+ Add

**Destinations**

**Exclude Destinations**

**Actions**

proxy-8195126.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sseposture-routing-commercial.posture.duosecurity.com, data.eb.thousandeyes.

-

-

Cancel

Back

Next

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 via Secure Access (geen internetbescherming)

### Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



### Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions



No matches found

[Cancel](#)

[Back](#)

[Next](#)





**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 + **Adden** klik vervolgens **Next** wanneer u alle bronnen hebt toegevoegd.

Cisco Secure-clientconfiguratie

**Cisco Secure Client Configuration**

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

**Banner Message**  
Require user to accept a banner message post authentication

**Session Timeout**  
 days

**Session Timeout Alert**  
 minutes before

**Maximum Transmission Unit** ⓘ

[Cancel](#) [Back](#) [Save](#)

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

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 Name voor de groep en klik op **Submit**

**Administration**

- System
- Deployment
- Licensing
- Certificates
- Logging
- Maintenance
- Upgrade

**Network Resources**

- Network Devices
- Network Device Groups
- Network Device Profiles
- External RADIUS Servers
- RADIUS Server Sequences
- NAC Managers

**Identity Management**

- Identities
- Groups**
- External Identity So
- Identity Source Seq
- Settings

**Identity Groups**

Endpoint Identity Groups

**User Identity Groups**

## User Identity Groups

User Identity Group

Edit **4** + Add Delete Import

\* Name **5** CSA-ISE

Description

**6** Submit

Name

- ALL\_ACCOUNTS (default)
- CSA-ISE → GROUP CREATED
- Employee

Lokale gebruiker configureren

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

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

## Network Access User

\* Username

Status  Enabled ▼

Account Name Alias  ⓘ

Email

---

### Passwords

Password Type:  ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ
Enable	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

## ▼ User Groups

⋮
CSA-ISE ▼
🗑️
+

- **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.

---

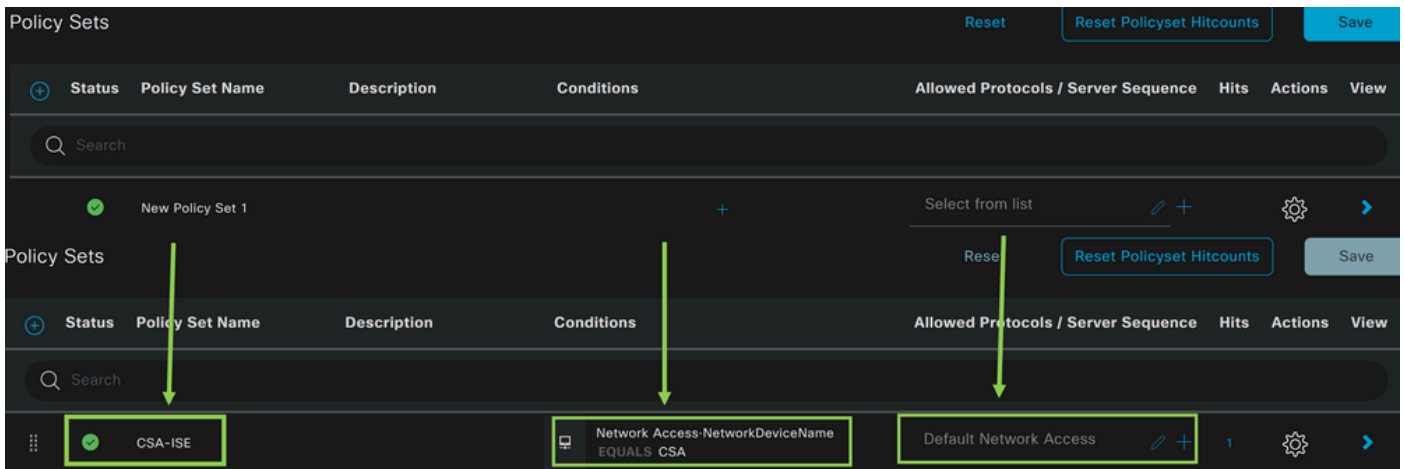
Daarna kunt u **Save** de configuratie aanpassen en doorgaan met de stap, **Configure Policy Set**.

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:

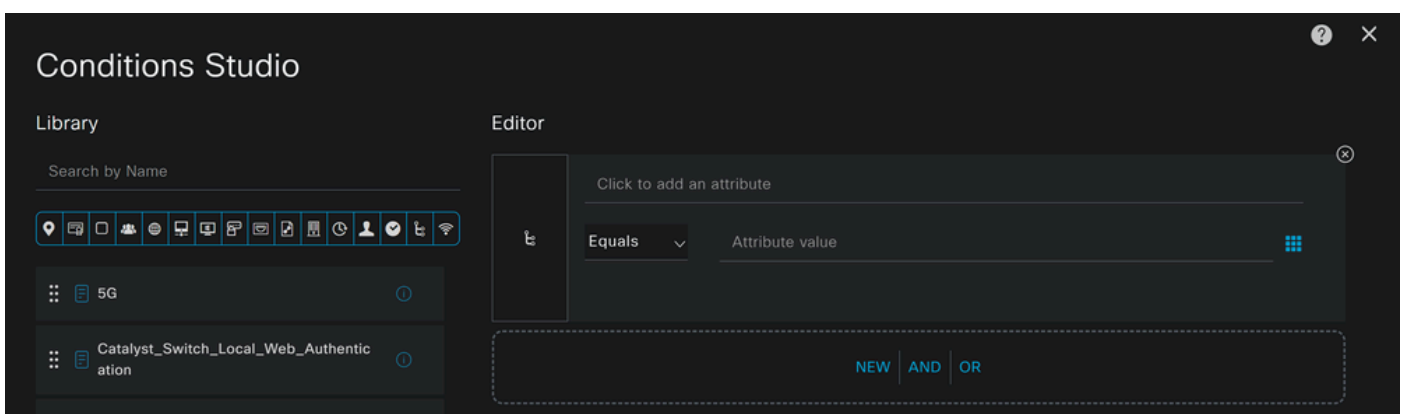
- Klik op Policy > Policy Sets
- Klik op om een nieuwe beleidsset toe + te voegen



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:

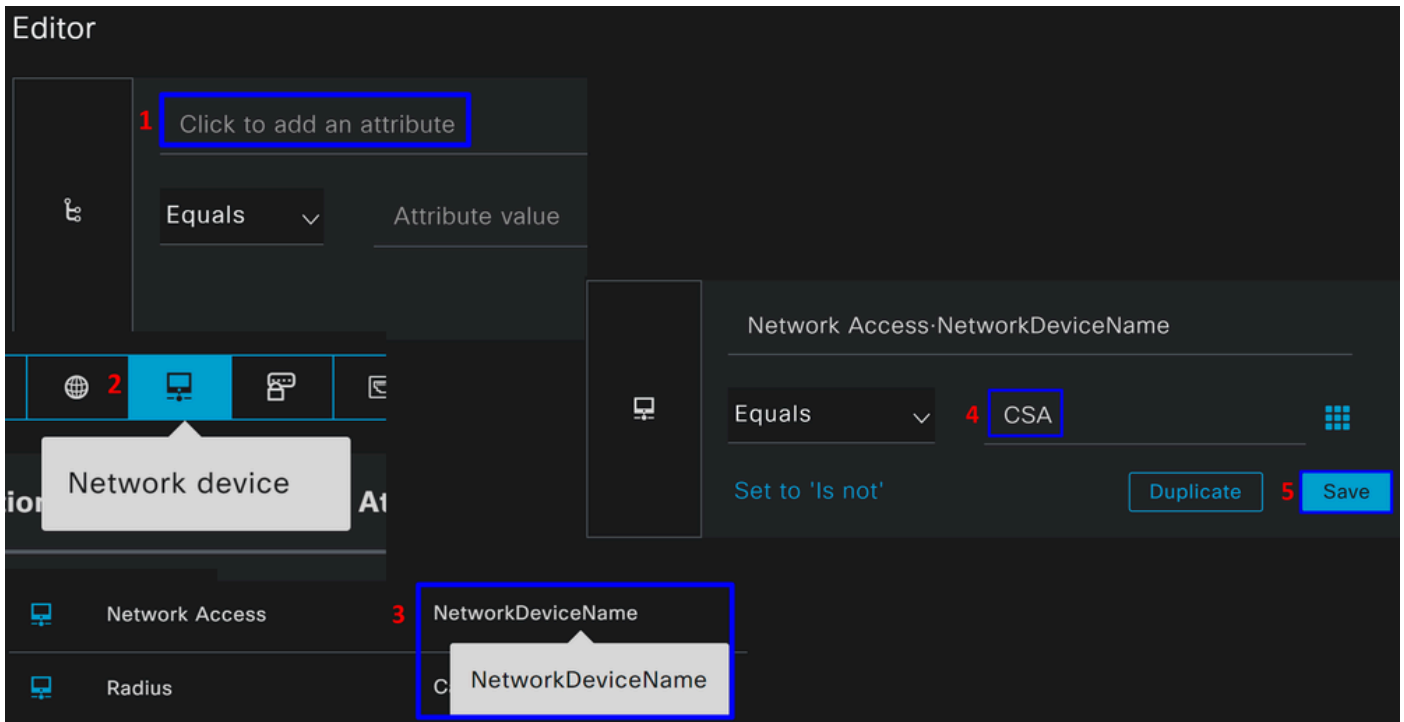
- Klik op +
- Onder **Condition Studio** beschikbare informatie vallen:



- 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](#)

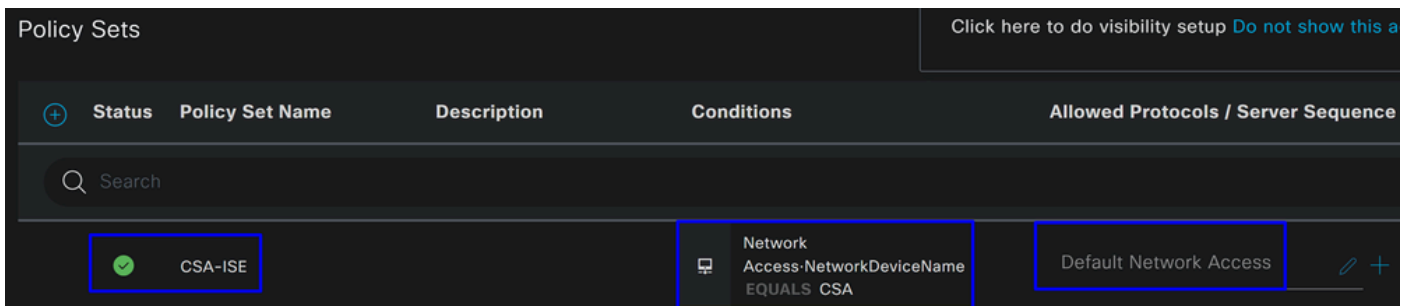


- Klik op de knop **Save**

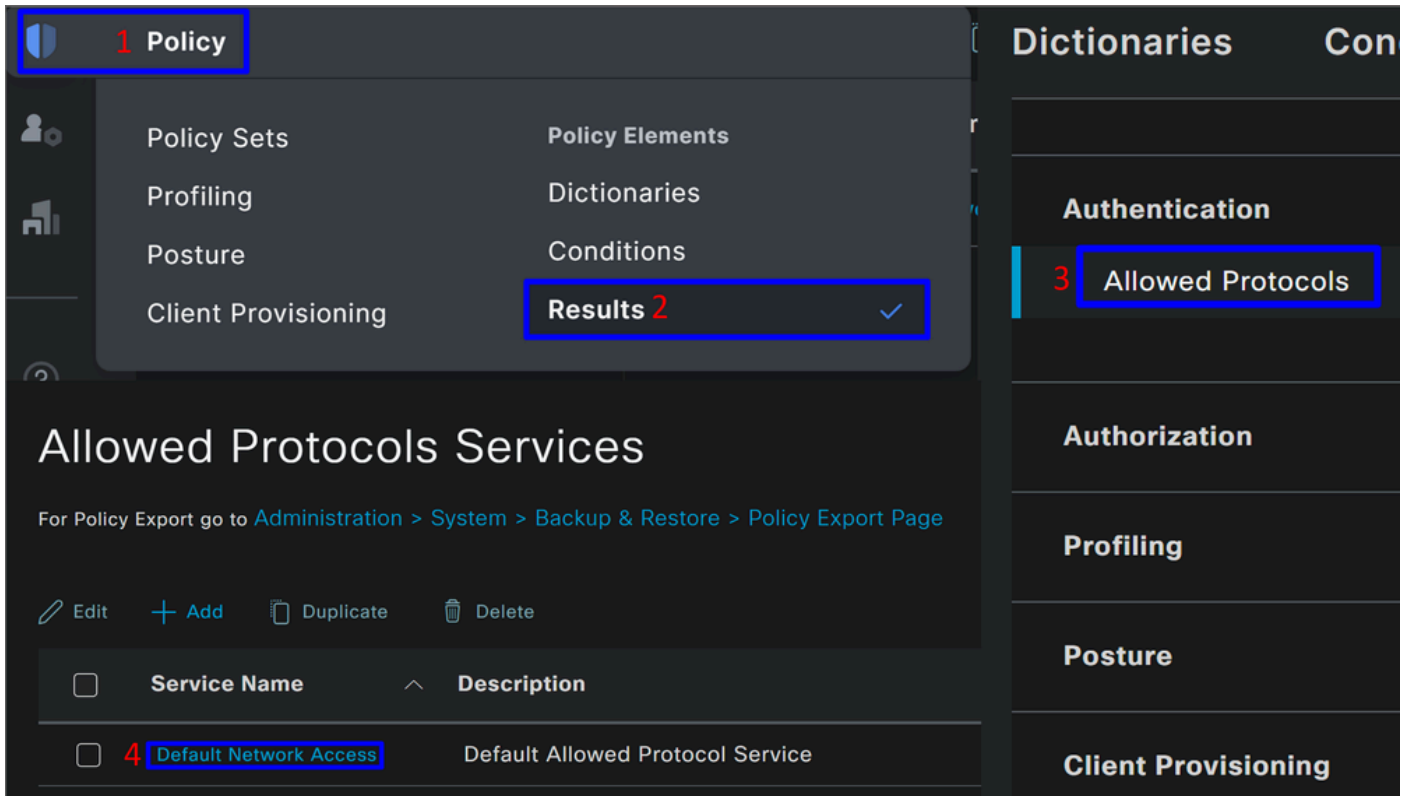


Dit beleid keurt alleen het verzoek van de bron goed CSA om door te gaan met de **Authentication** en **Authorization** installatie onder de reeks beleid **CSA-ISE**, en verifieert ook de toegestane protocollen gebaseerd op de **Default Network Access** voor de toegestane protocollen.

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 op **Policy > Results**
    - Klik op **Allowed Protocols**
    - Klik op **Default Network Access**

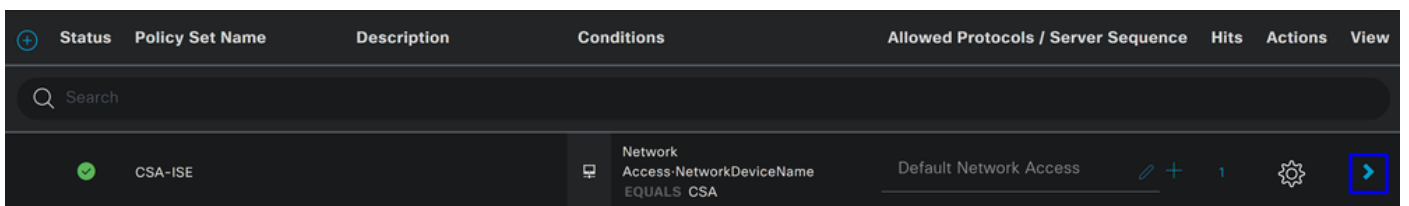


- Vervolgens ziet u alle protocollen die zijn toegestaan op **Default Network Access**

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:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
🟢	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access
<a href="#">&gt; Authentication Policy(2)</a>				
<a href="#">&gt; Authorization Policy - Local Exceptions</a>				
<a href="#">&gt; Authorization Policy - Global Exceptions</a>				
<a href="#">&gt; Authorization Policy(2)</a>				

## 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 de verificatie op basis van specifieke criteria:

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

Authentication Policy(2)				
+ Status	Rule Name	Conditions	Use	
🟢	Authentication Secure Access	Network Access:NetworkDeviceName EQUALS CSA	Internal Users	✎ +
<a href="#">&gt; Options</a>				

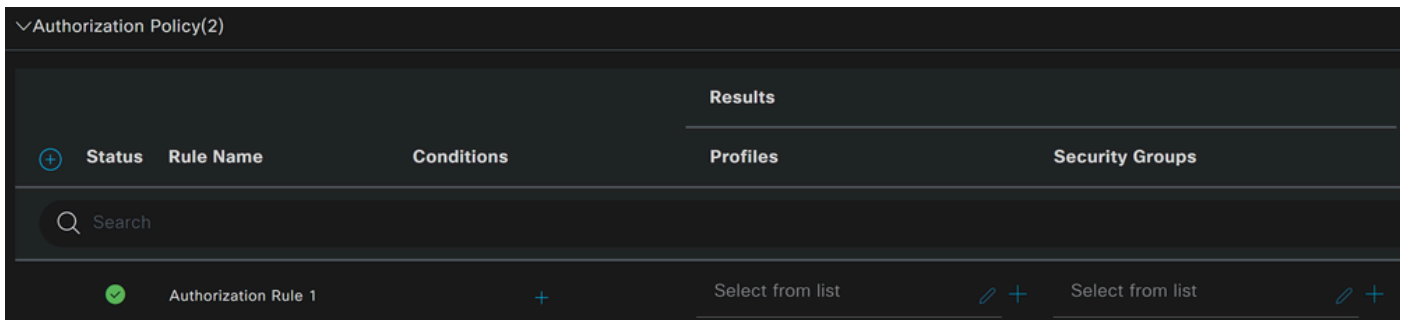
Het beleid is hetzelfde beleid dat is gedefinieerd onder de stap [Reeks beleid configureren](#).

## Vergunningsbeleid

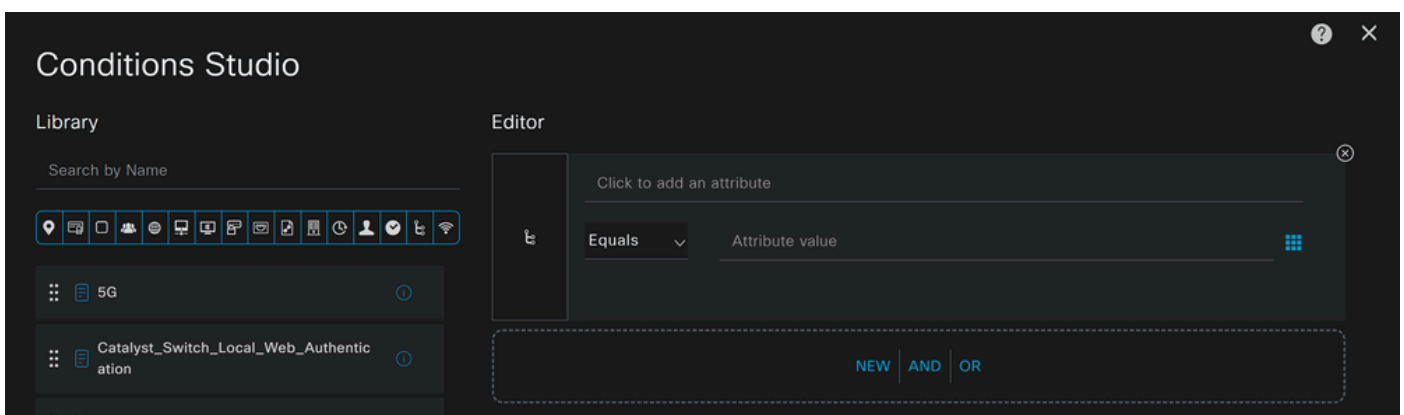
U kunt het autorisatiebeleid op vele manieren configureren. In dit geval, autoriseer alleen de gebruikers in de groep die gedefinieerd is in de stap [Een groep configureren](#). Zie het volgende voorbeeld om uw autorisatiebeleid te configureren:

Authorization Policy(2)				
+ Status	Rule Name	Conditions	Profiles	Security Groups
🟢	Authorization Rule 1		Select from list	Select from list
🟢	Authorization Secure Access	InternalUser:IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

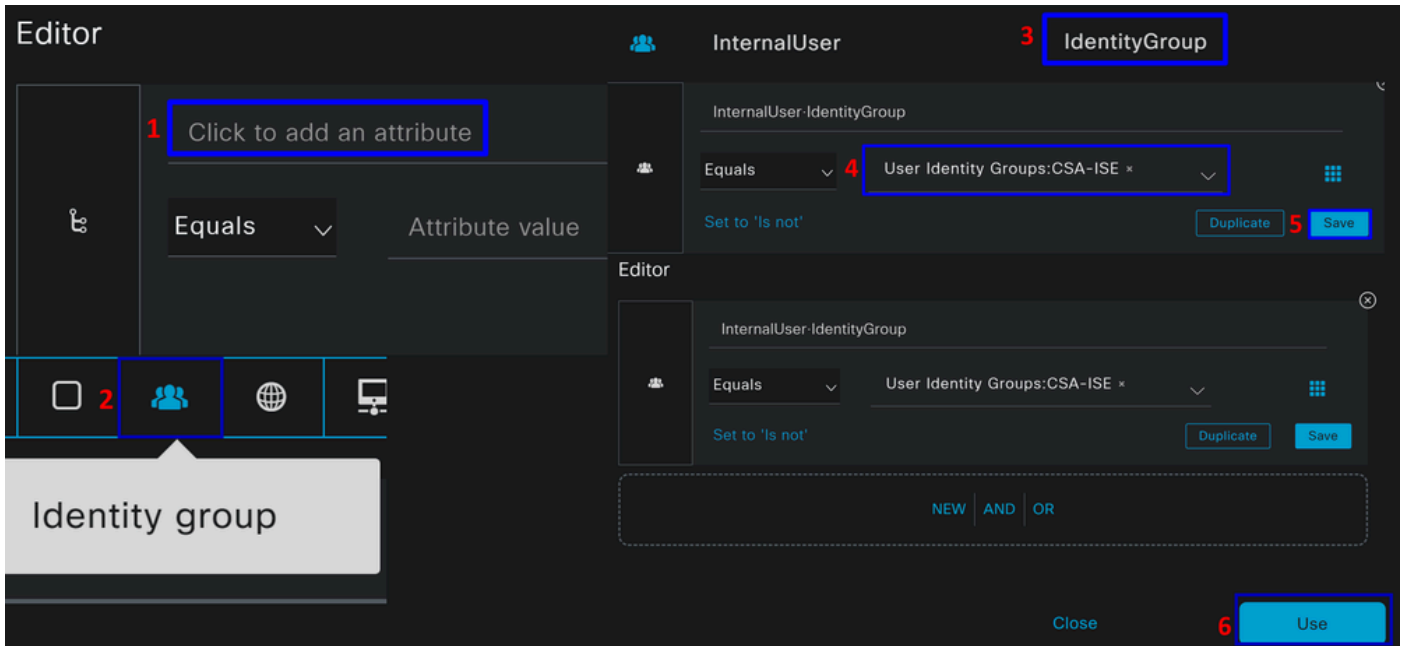
- Klik op **Authorization Policy**
- Klik op om het beleid voor autorisatie als volgt + te definiëren:



- 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:

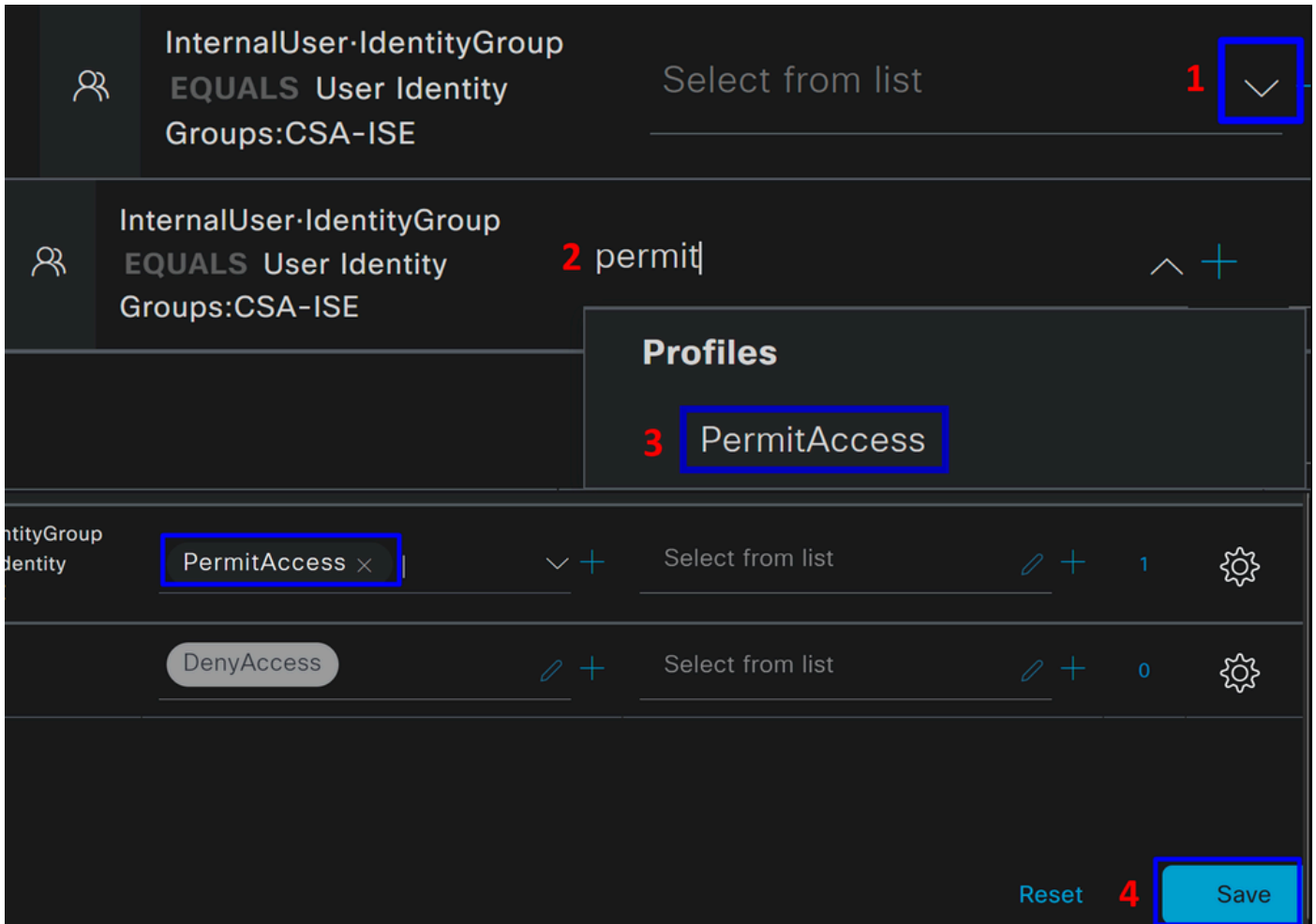


- Om de Voorwaarden te creëren, klik op Click to add an attribute
- Klik op de **Identity Group** knop
- Klik onder de achterliggende opties op **Interne Gebruiker - IdentityGroup** optie
- Gebruik onder de **Equals** optie de vervolgkeuzelijst om de **Group** goedgekeurde verificatiestap in de stap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

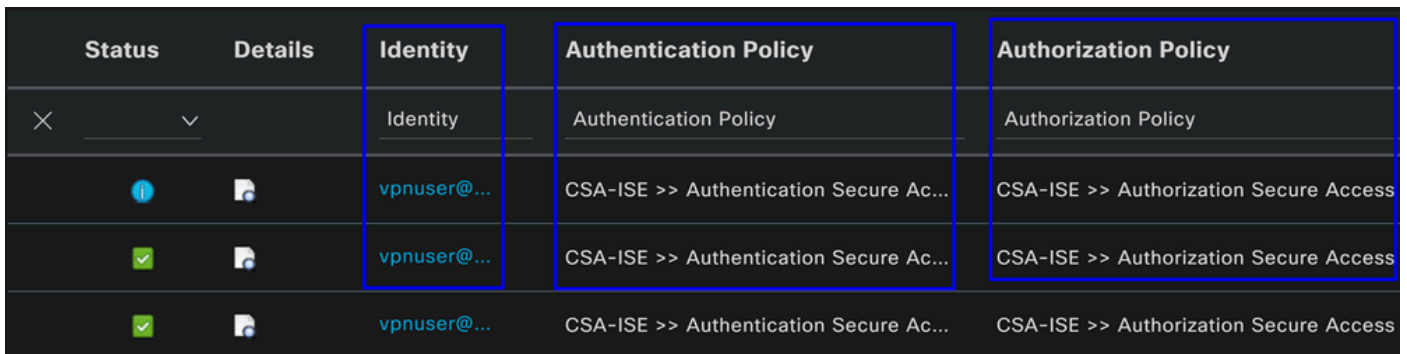
## 28 Events







User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
 vpn user (vpnuser@ciscospt.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**



Status	Details	Identity	Authentication Policy	Authorization Policy
×	∨	Identity	Authentication Policy	Authorization Policy
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access

Lokale of actieve mapgebruikers van RADIUS configureren

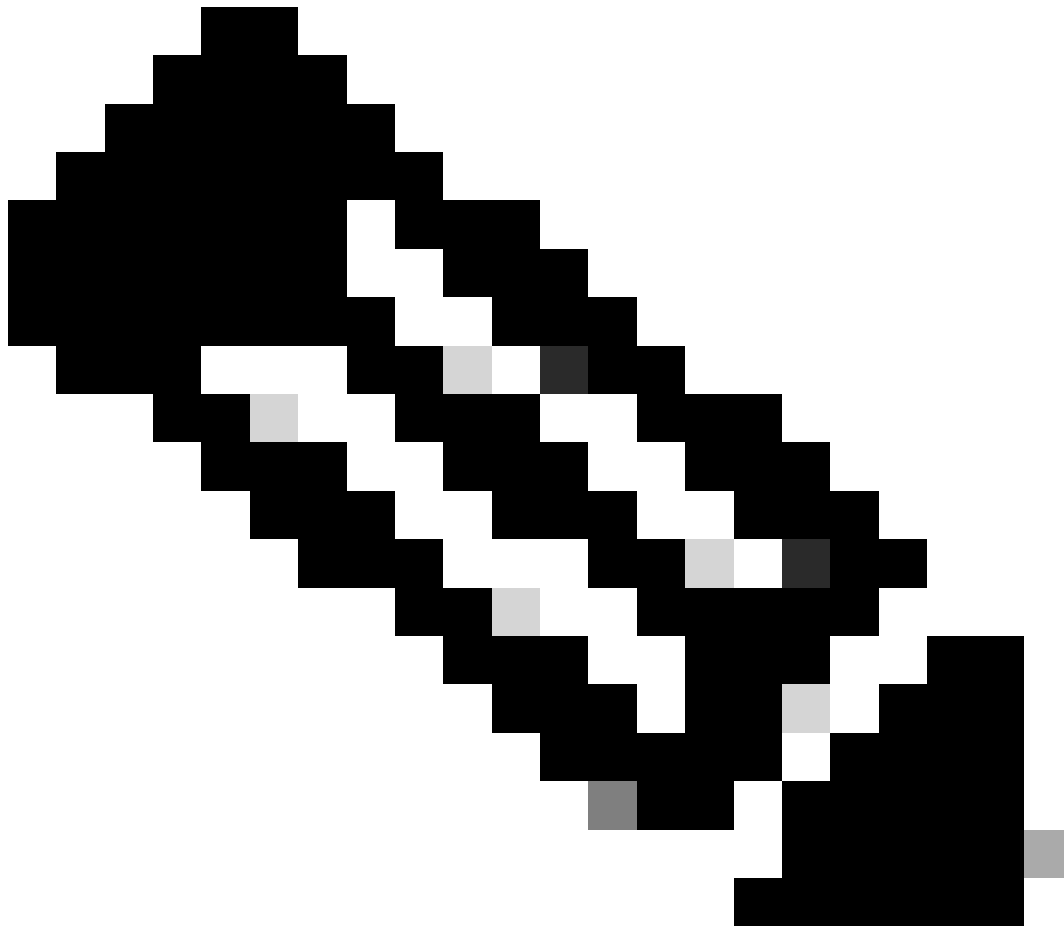
ISE-houding configureren

In dit scenario, creëer 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.

The image shows two side-by-side screenshots of the 'Anti-Malware Condition' configuration interface. The left screenshot shows the default configuration: Name is empty, Description is empty, Compliance Module is '4.x or later', Operating System is 'Select Operating System', and Vendor is 'ANY'. The right screenshot shows a specific configuration: Name is 'CSA-Antimalware', Description is empty, Compliance Module is '4.x or later', Operating System is 'Windows All', and Vendor is 'Cisco Systems, Inc.'. Arrows indicate the mapping of fields between the two configurations. At the bottom of each configuration, there are radio buttons for 'Check Type', with 'Installation' selected in both.

- **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.

Baseline Condition    Advanced Condition

**1** You can select products either on baseline condition or advanced condition.

**2**

	Product Name	Minimum Version	Maximum Version	Minimum Complia
<input type="checkbox"/>	ANY	ANY	ANY	N/A
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
<input type="checkbox"/>	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

**3**

Save    Reset

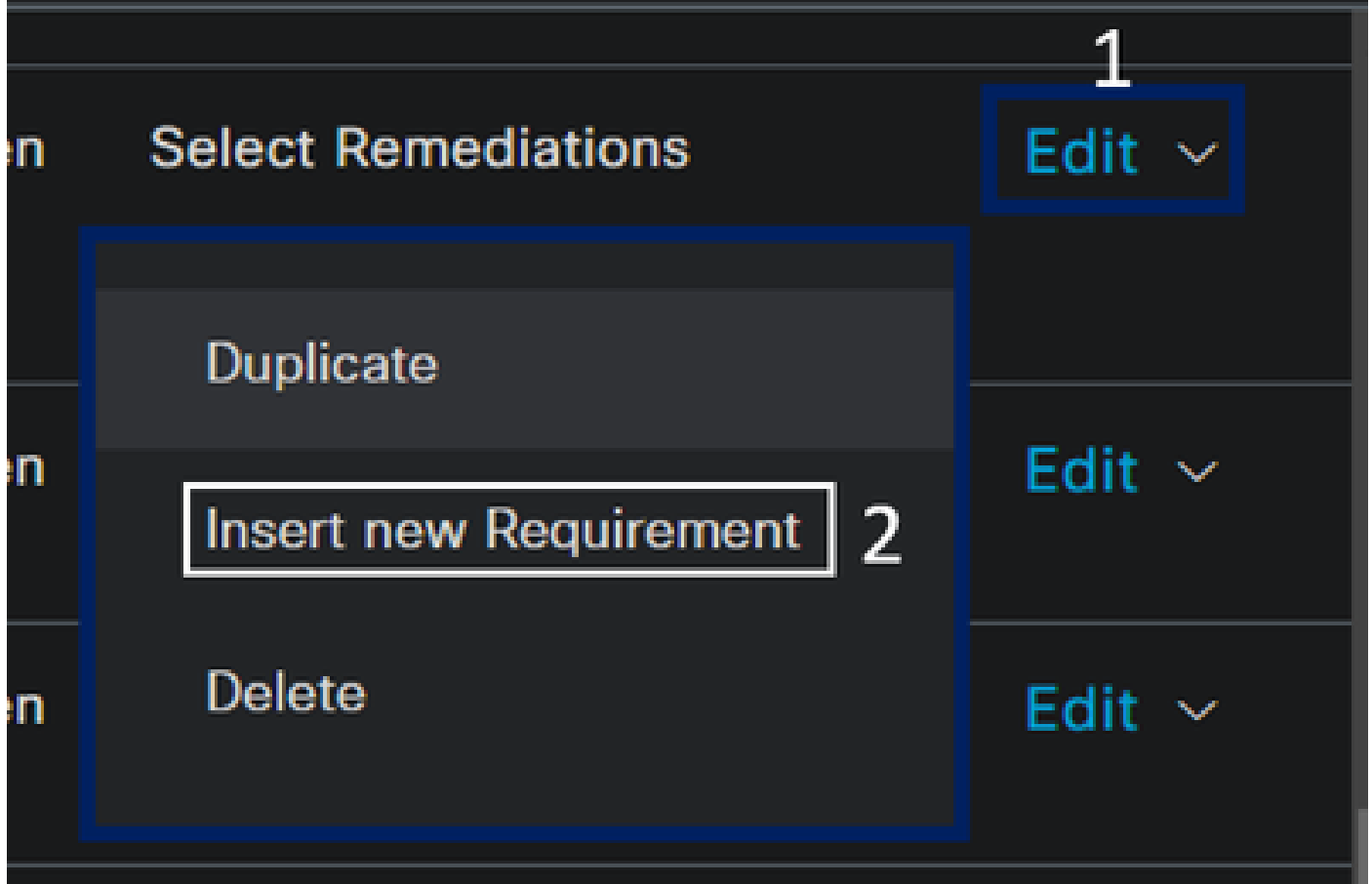
- Vink het aanvinkvakje aan voor de voorwaarden die u wilt evalueren
- Configureer de minimumversie om te verifiëren
- Klik op Opslaan om door te gaan met de volgende stap

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 > Requiriments**
- Klik op een **Edit** van de vereisten en klik op **Insert new Requirement**

# Remediations Actions



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

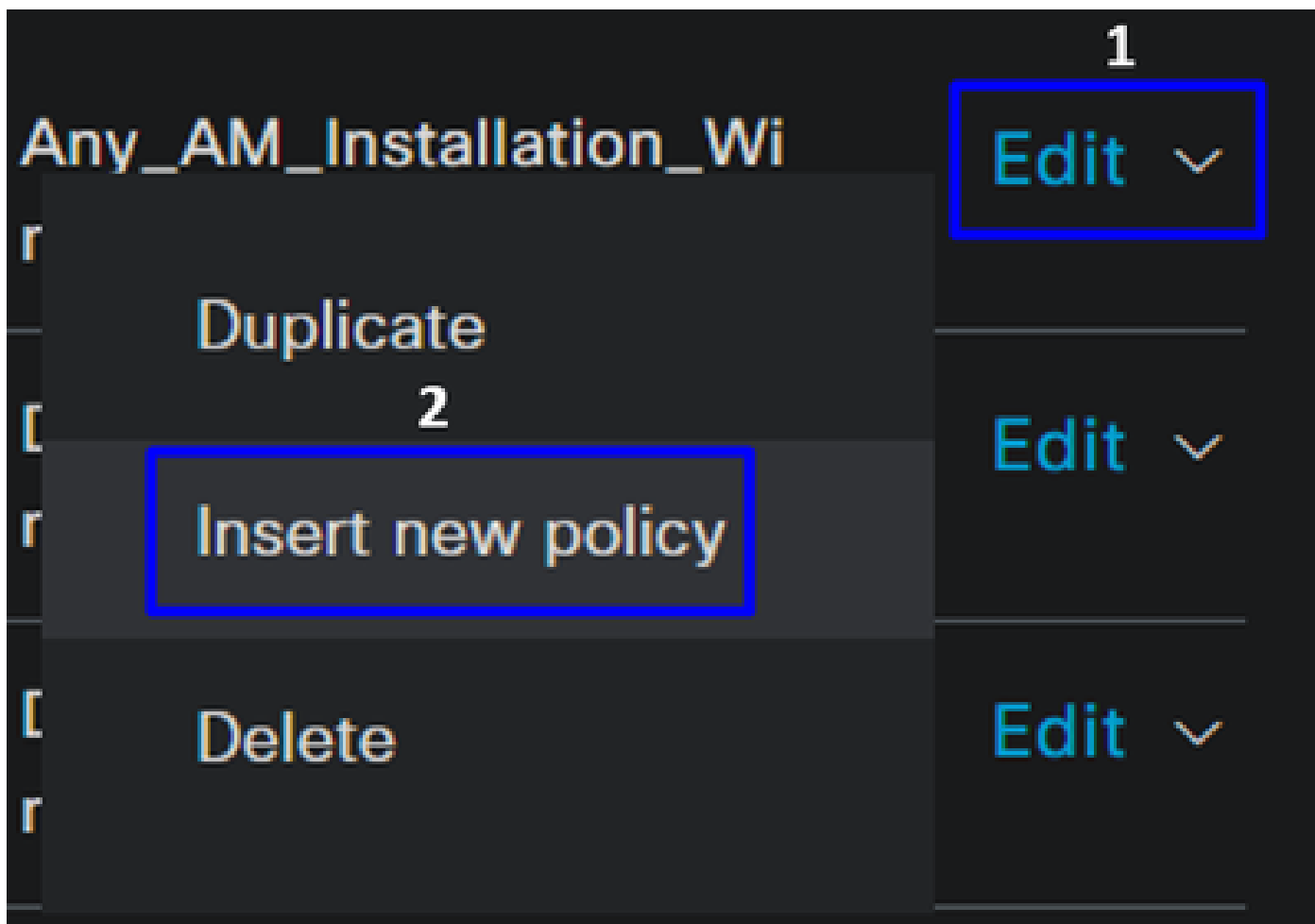
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
CSA-ANTIMALWARE	for Windows All	using 4.x or later	using Agent	met if CSA-Antimalware then	Message Text Only

- **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	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	CSA-Windows-Posture	If Any	and Windows All	and 4.x or later	and Agent	and	then CSA-ANTIMALWARE

- **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:

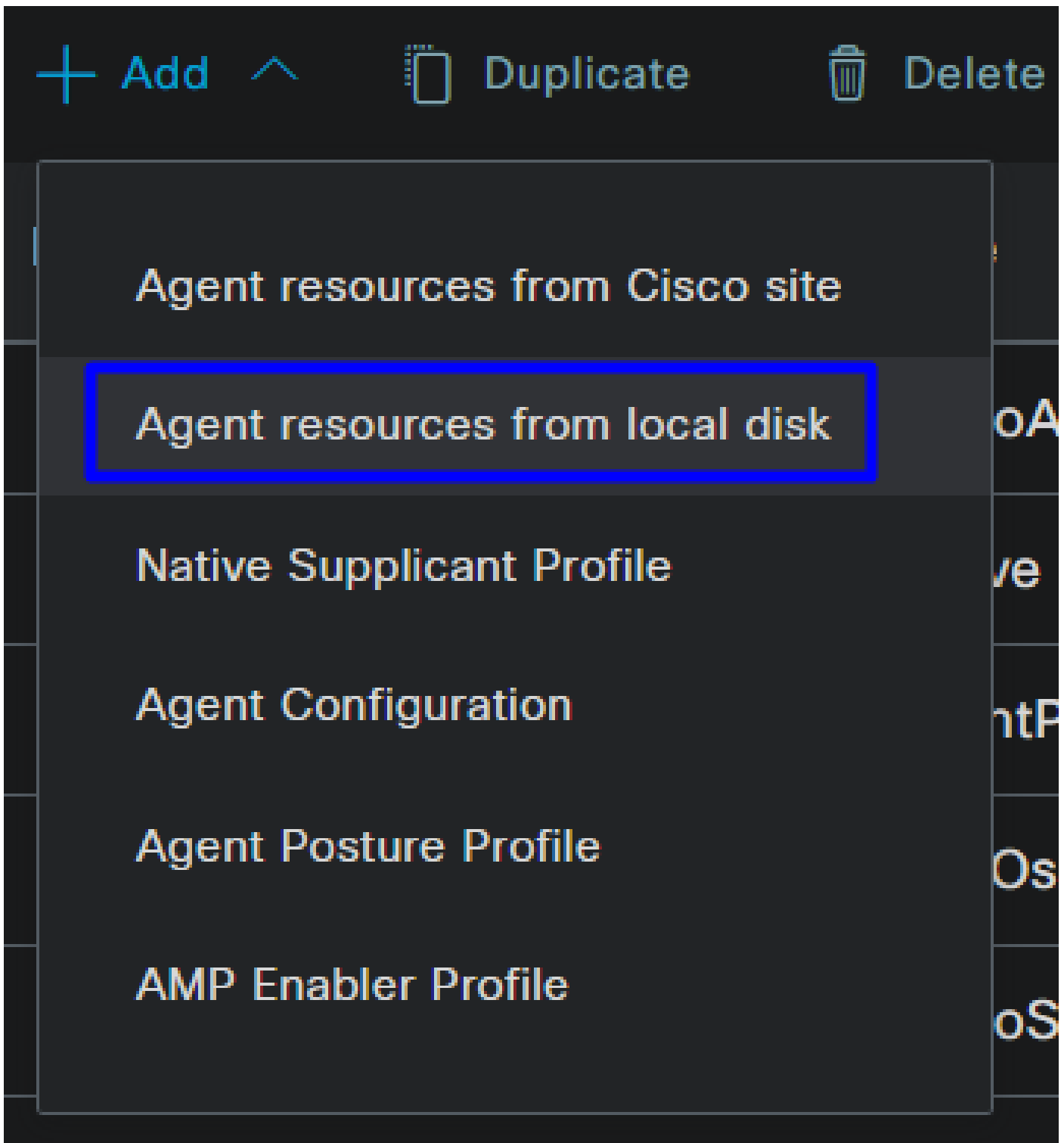
Te configureren bronnen	Beschrijving
1. <b>Agent Resources</b>	Secure Client-webprovisioningpakket
2. <b>Compliance Module</b>	Cisco ISE-nalevingsmodule
3. <b>Agent Profile</b>	Beheer van het provisioningprofiel.
3. <b>Agent Configuration</b>	Definieer welke modules zijn voorzien door het provisioningportal 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.

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	118.88 MB	  

- 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





Add



Duplicate



Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

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

# Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3Het Agent-profiel configureren

- Klik op + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑 Delet

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

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

# Agent Posture Profile

Name \*



Description:

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

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

## Step 4 De Agent-configuratie configureren

- Klik op + Add > Agent Configuration

+ Add ^

📱 Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- Daarna, vorm de volgende parameters:

\* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

\* Configuration Name:

Description:

### Description Value Notes

\* Compliance Module CiscoSecureClientComplianceModuleWi 

## Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

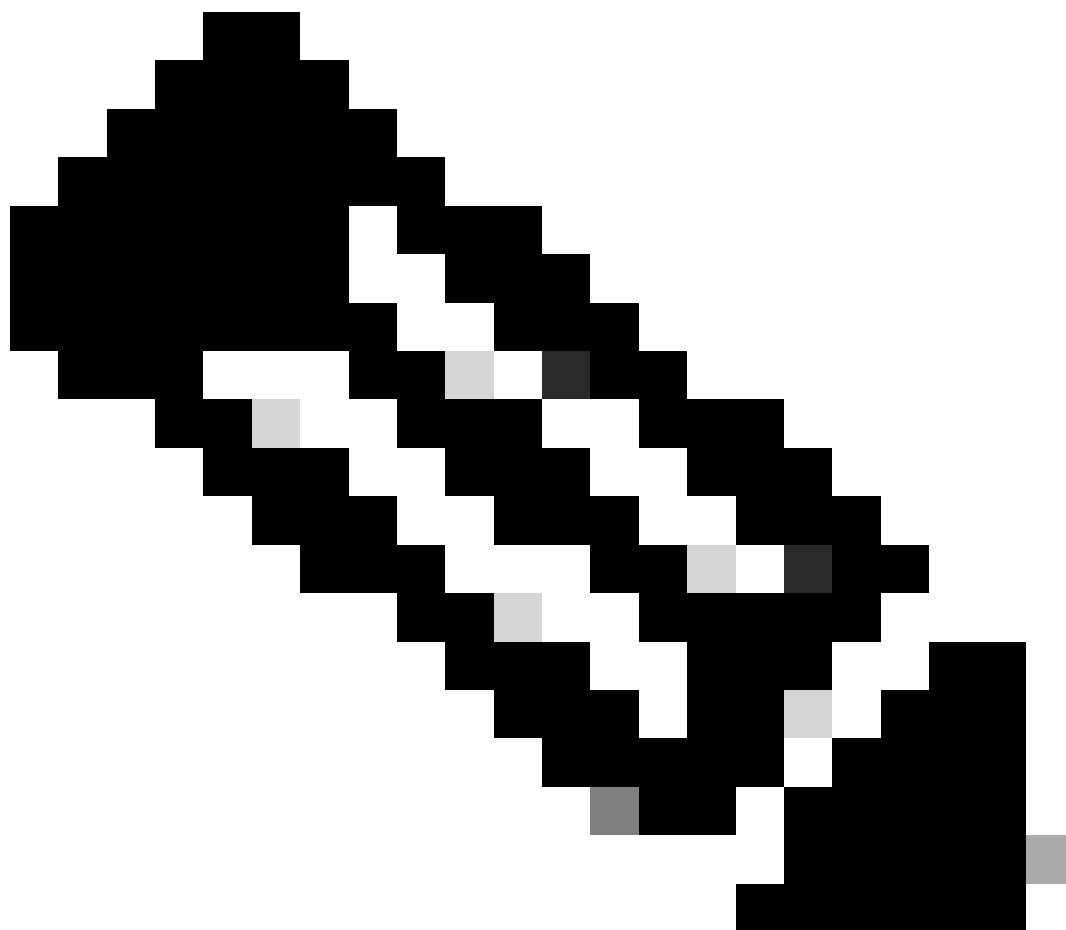
## Profile Selection

* ISE Posture	1.CSA_PROFILE	∨
VPN		∨

- 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**

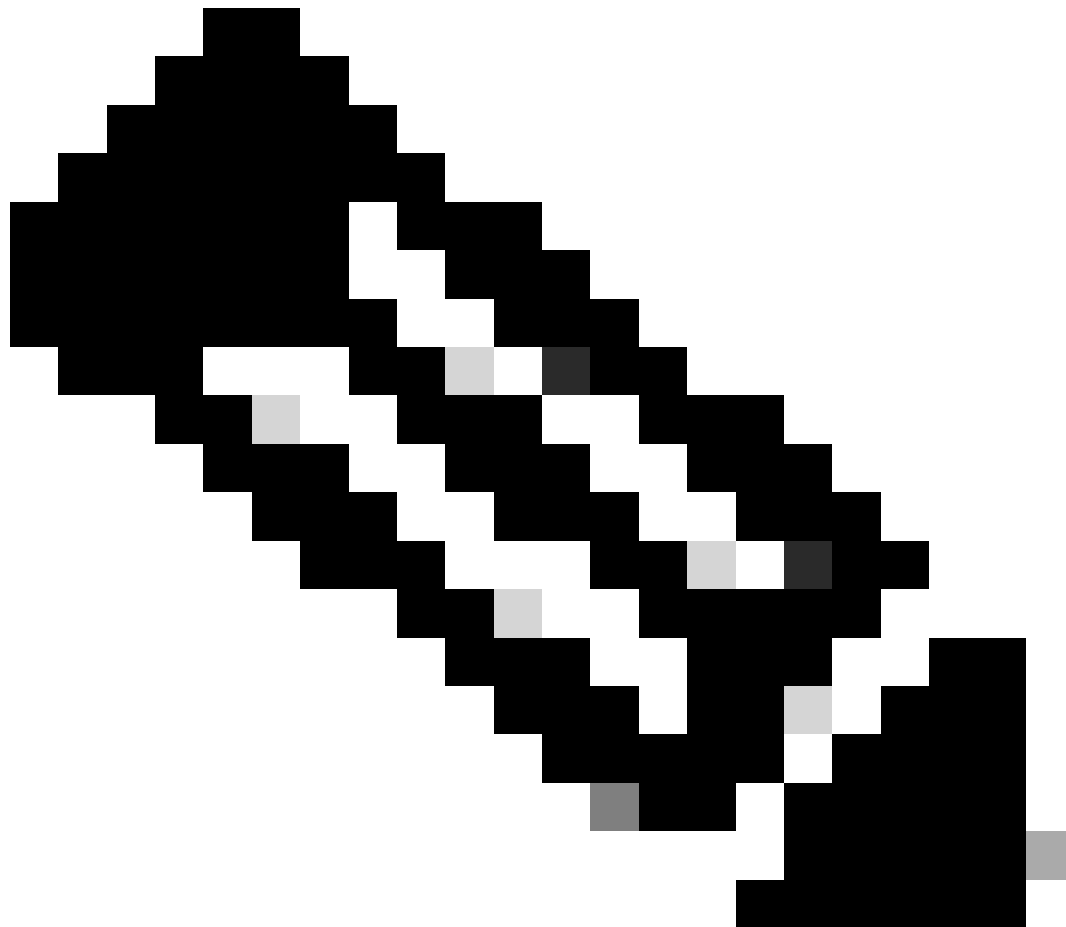


**Opmerking:** aanbevolen wordt dat elk besturingssysteem, Windows, Mac OS of Linux, één onafhankelijke client-configuratie heeft.



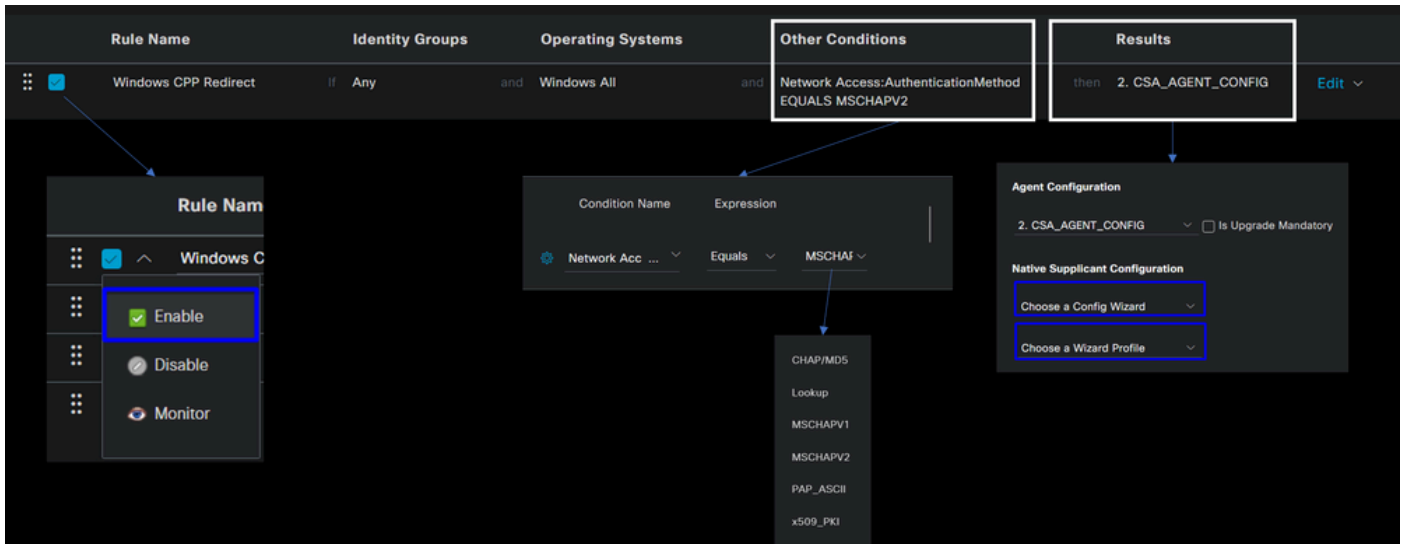
Om de levering van de houding van ISE en de modules die in de laatste stap worden gevormd toe te laten, moet u een beleid vormen om de levering te maken.

- 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: CSA-Compliant

Description: [Empty text box]

IP version:  IPv4  IPv6  Agnostic ⓘ

* DACL Content	1234567	permit ip any any
	8910111	
	2131415	
	1617181	
	9202122	
	2324252	
	6272829	
	3031323	
	3343536	
	3738394	
	0000000	

- **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**

**Description**

**IP version**  IPv4  IPv6  Agnostic ⓘ

**\* DACL Content**

1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

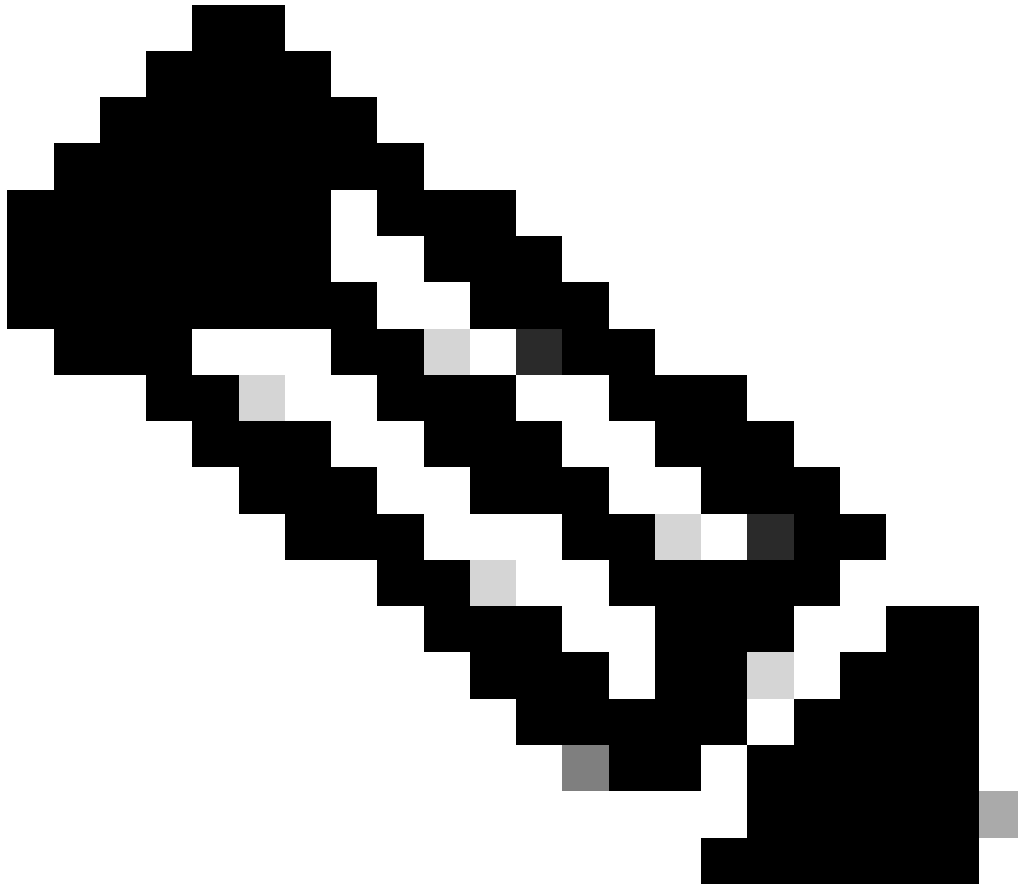
⌵ **Check DACL Syntax**

- **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**

## Authorization Profile

\* Name


CSA-Compliant

Description

\* Access Type

ACCESS\_ACCEPT

Network Device Profile

 Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

## ✓ Common Tasks

**DACL Name**

CSA-Compliant

**IPv6 DACL Name**

**ACL**

**ACL IPv6 (Filter ID)**

- **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 **Unknown Compliant Authorization Profile**



**\* Name** CSA-Unknown-Compliant

---

**Description**


**\* Access Type** ACCESS\_ACCEPT ▼


---


**Network Device Profile**  Cisco ▼ 

---

**Service Template**

**Track Movement**  

**Agentless Posture**  

**Passive Identity Tracking**  

▼ **Common Tasks**

**DACL Name** CSA\_Redirect\_To\_ISE ▼

---

**Web Redirection (CWA, MDM, NSP, CPP)** 

Client Provisioning (Posture) ▼ **ACL** **redirect** ▼ **Value** **Client Provisioning Portal (...)** ▼

---



- **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.

#### Attributes Details

Access Type = ACCESS\_ACCEPT

DACL = CSA\_Redirect\_To\_ISE

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=

&action=cpp

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.

<b>Policy Set - autorisatie</b>	<b>Autorisatieprofiel</b>
<b>conform</b>	<a href="#">Vergunningsprofiel - conform</a>
<b>Onbekend conform</b>	<a href="#">Vergunningsprofiel - Onbekend conform</a>
<b>Niet conform</b>	<a href="#">Toegang weigeren</a>

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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370		

- Klik op de Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
<b>&gt; Authorization Policy(4)</b>					

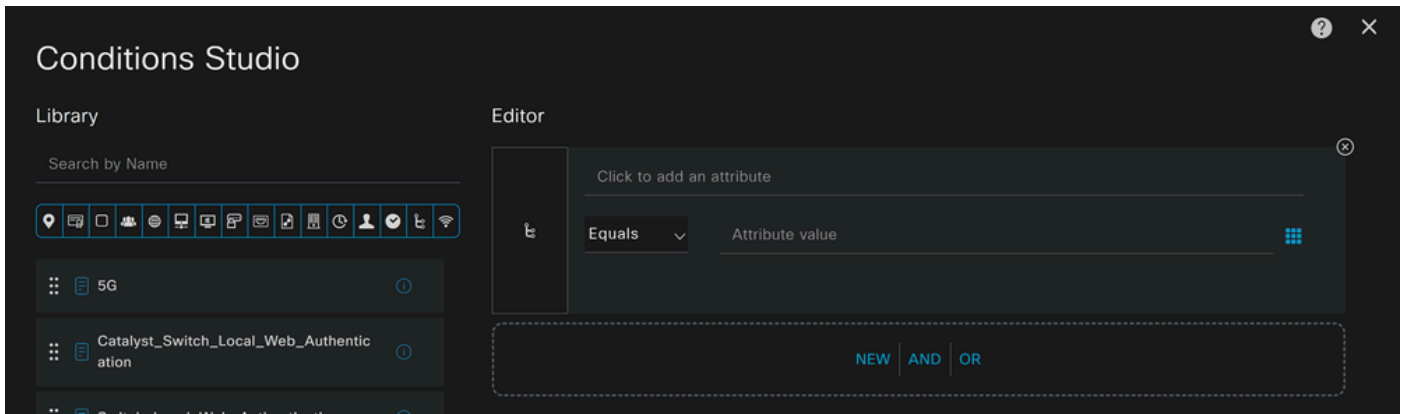
- Maak de volgende drie beleidslijnen in de volgende volgorde:

✓	CSA-Compliant	AND	<ul style="list-style-type: none"> <li>Compliant_Devices</li> <li>Network_Access_Authentication_Passed</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	CSA-Post-Compliant
✓	CSA-Unknown-Compliant	AND	<ul style="list-style-type: none"> <li>Network_Access_Authentication_Passed</li> <li>Compliance_Unknown_Devices</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	CSA-Unknown-Compliant
✓	CSA-Non-Compliant	AND	<ul style="list-style-type: none"> <li>Non_Compliant_Devices</li> <li>Network_Access_Authentication_Passed</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	DenyAccess

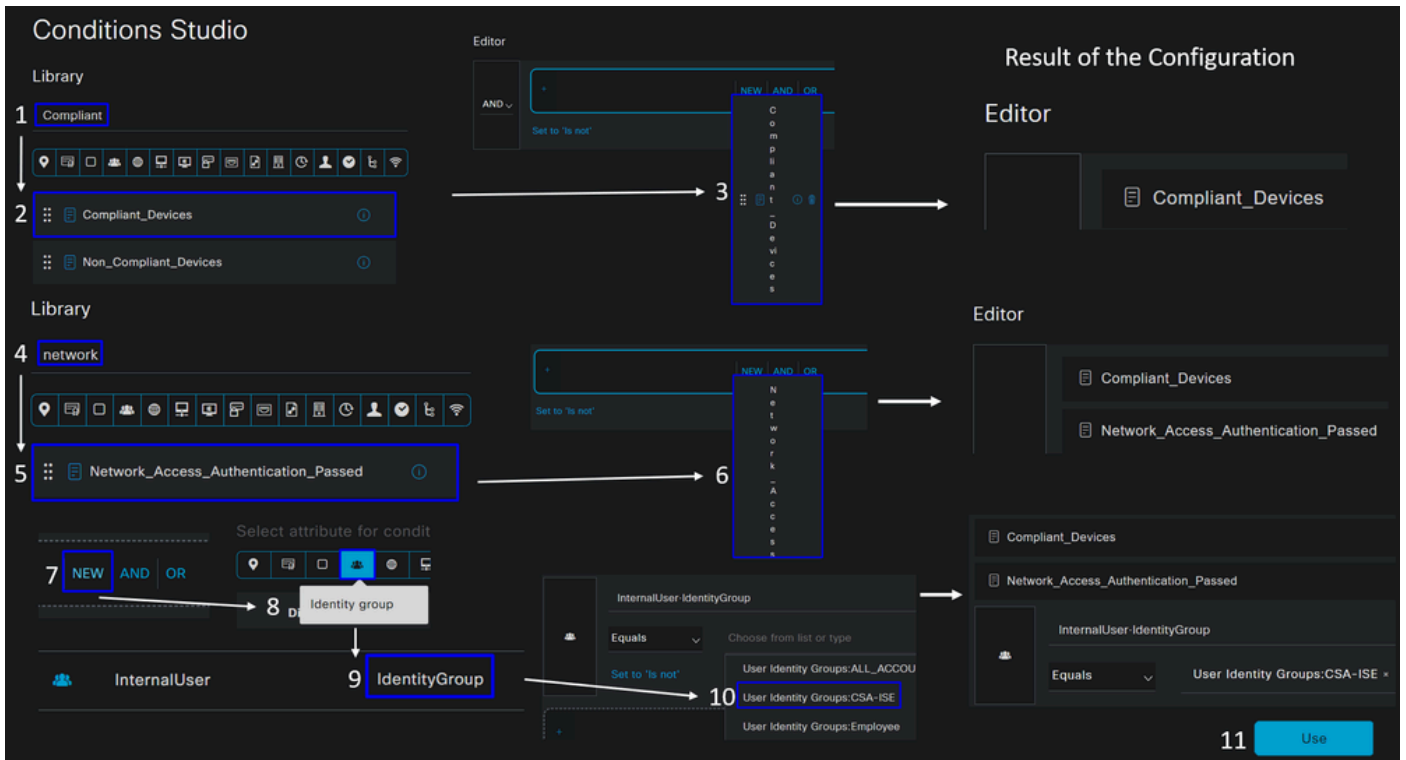
- Klik op + om het **CSA-Compliance** beleid te definiëren:

				Results	
+ Status	Rule Name	Conditions		Profiles	Security Groups
<input type="text" value="Search"/>					
✓	Authorization Rule 1	+		Select from list	Select from list

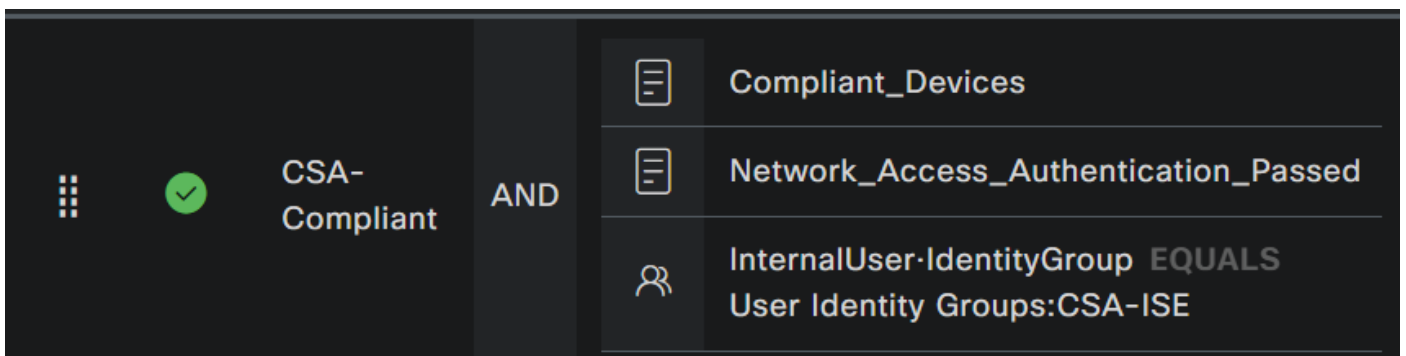
- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Compliance**
- Klik op het **Condition**veld +
- Onder **Condition Studio**, vindt u de informatie:



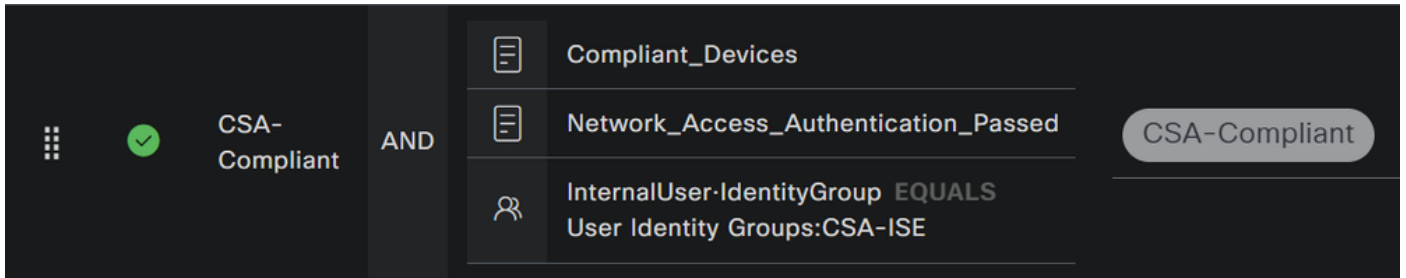
- Om de voorwaarde te creëren, zoekt u naar **compliant**
- U moet hebben weergegeven Compliant\_Devices
- Sleep onder het **Editor**
- Om de tweede voorwaarde te maken, zoekt u naar **network**
- U moet hebben weergegeven Network\_Access\_Authentication\_Passed
- Sleep onder het **Editor**
- Klik onder 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

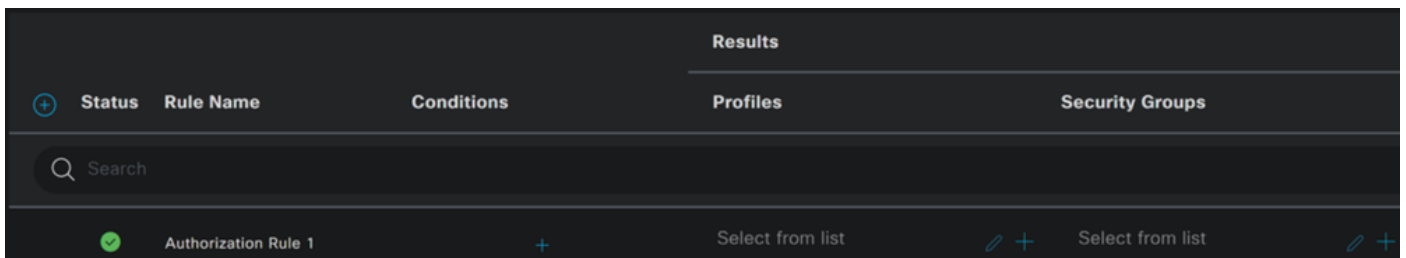


- Kies onder **Profile** klik onder de vervolgkeuzeknop en kies het profiel van de klachtenautorisatie dat op de stap is ingesteld, [conform autorisatieprofiel](#)

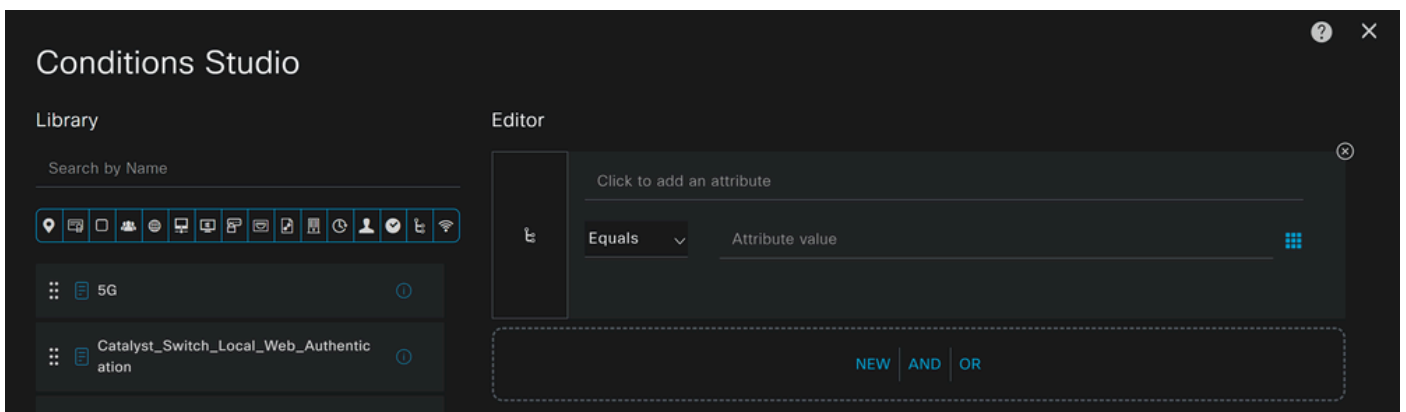


Nu hebt u de **Compliance Policy Set**instellingen ingesteld.

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

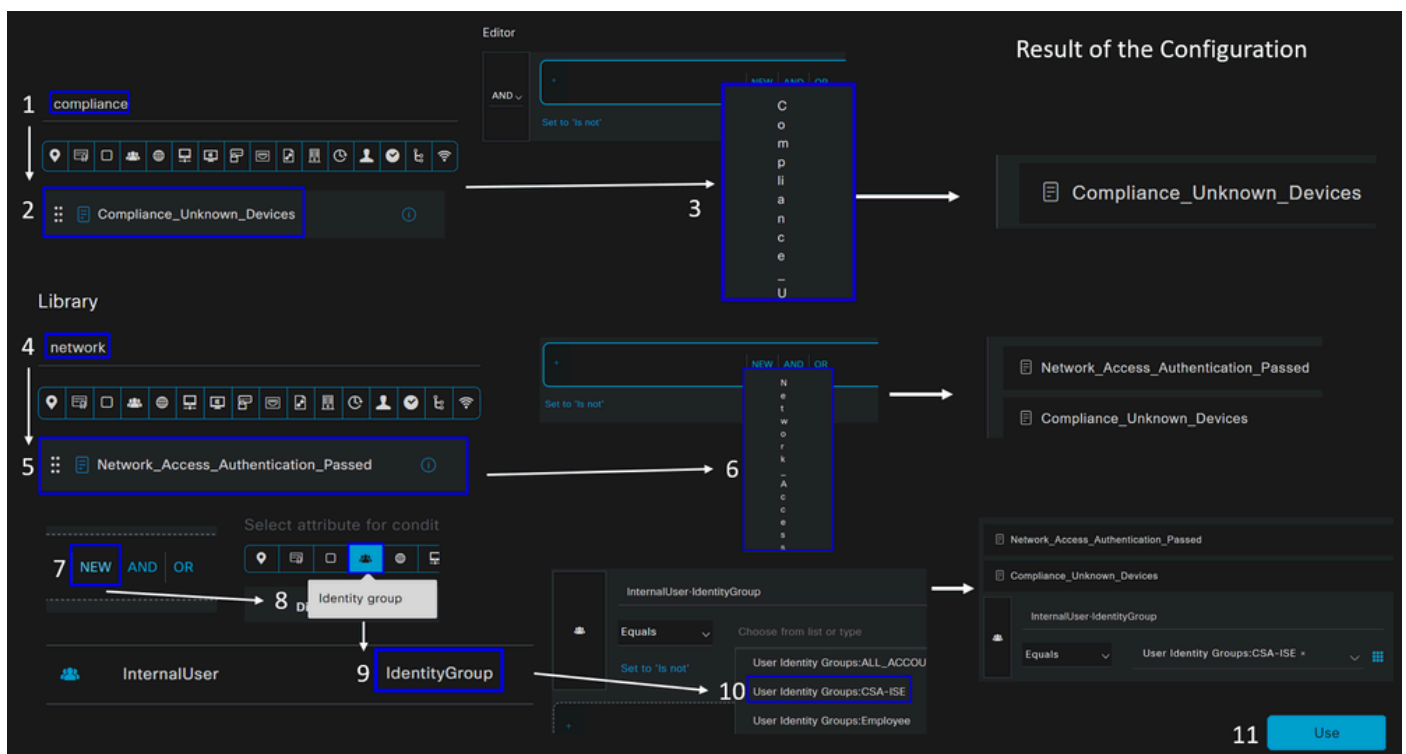


- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Unknown-Compliance**
- Klik op het **Condition**veld +
- Onder **Condition Studio**, vindt u de informatie:

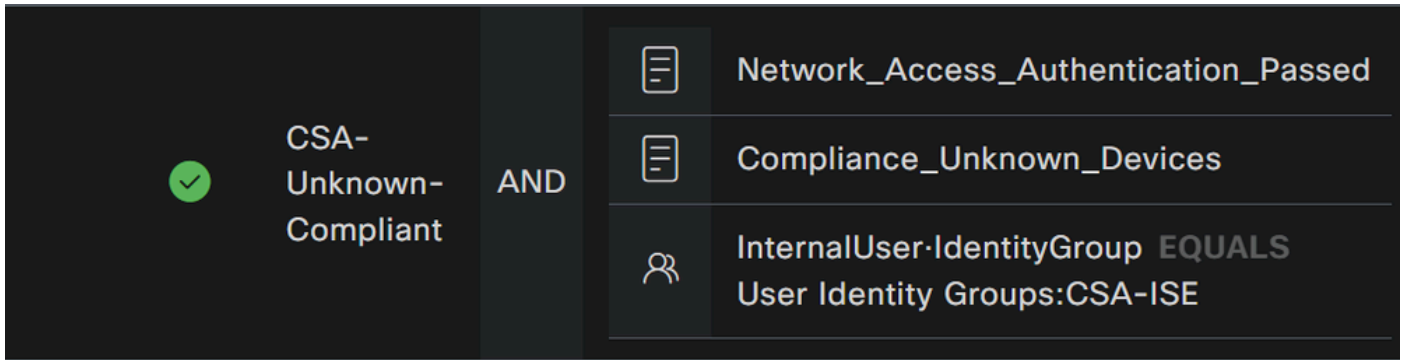




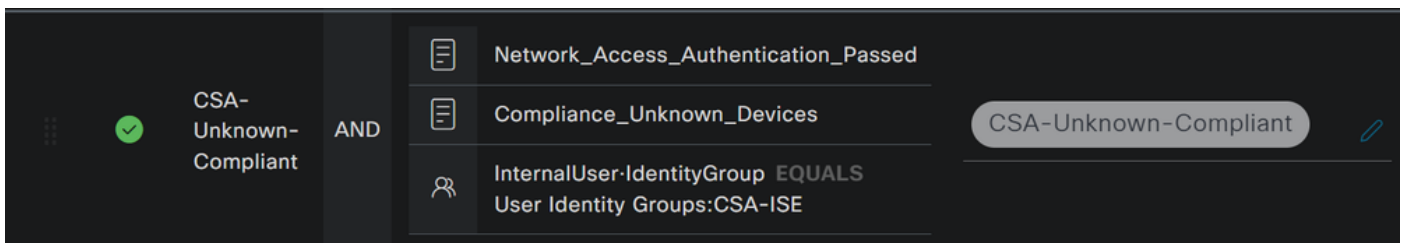
- Om de voorwaarde te creëren, zoekt u naar **compliance**
- U moet hebben weergegeven **Compliant\_Unknown\_Devices**
- Sleep onder het **Editor**
- Om de tweede voorwaarde te maken, zoekt u naar **network**
- U moet hebben weergegeven **Network\_Access\_Authentication\_Passed**
- Sleep onder het **Editor**
- Klik onder het Editor menu **New**
- Klik op het **Identity Group** pictogram
- Kies **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

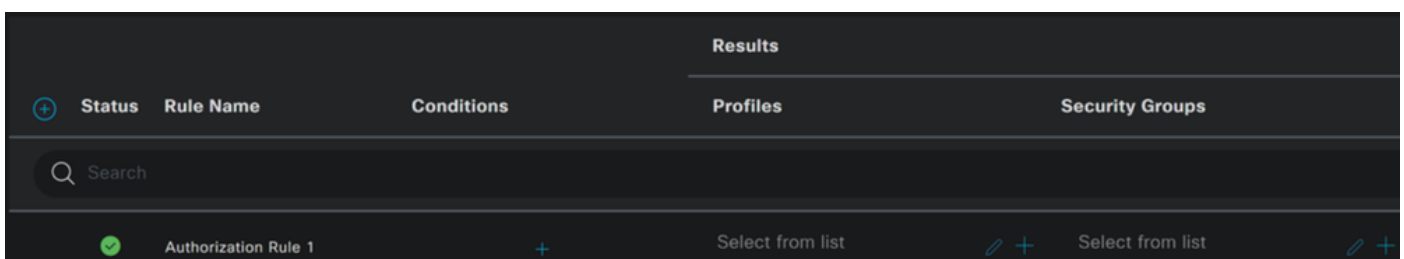


- Kies onder **Profile** klik onder de vervolgkeuzeknop en kies het profiel van de klachtenautorisatie dat op de stap is geconfigureerd, [Onbekend conform autorisatieprofiel](#)



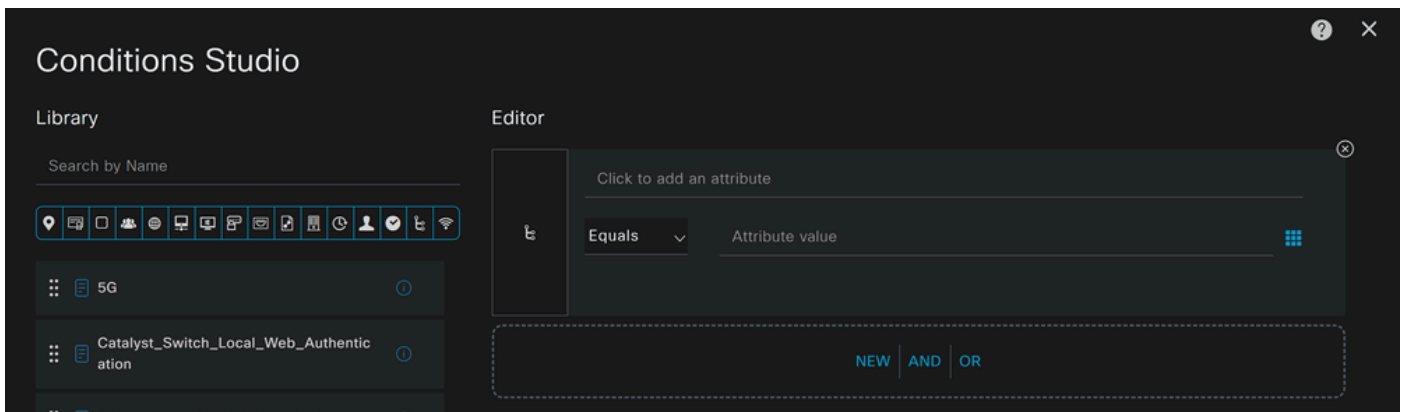
Nu hebt u de **Unknown Compliance Policy** Setinstellingen ingesteld.

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

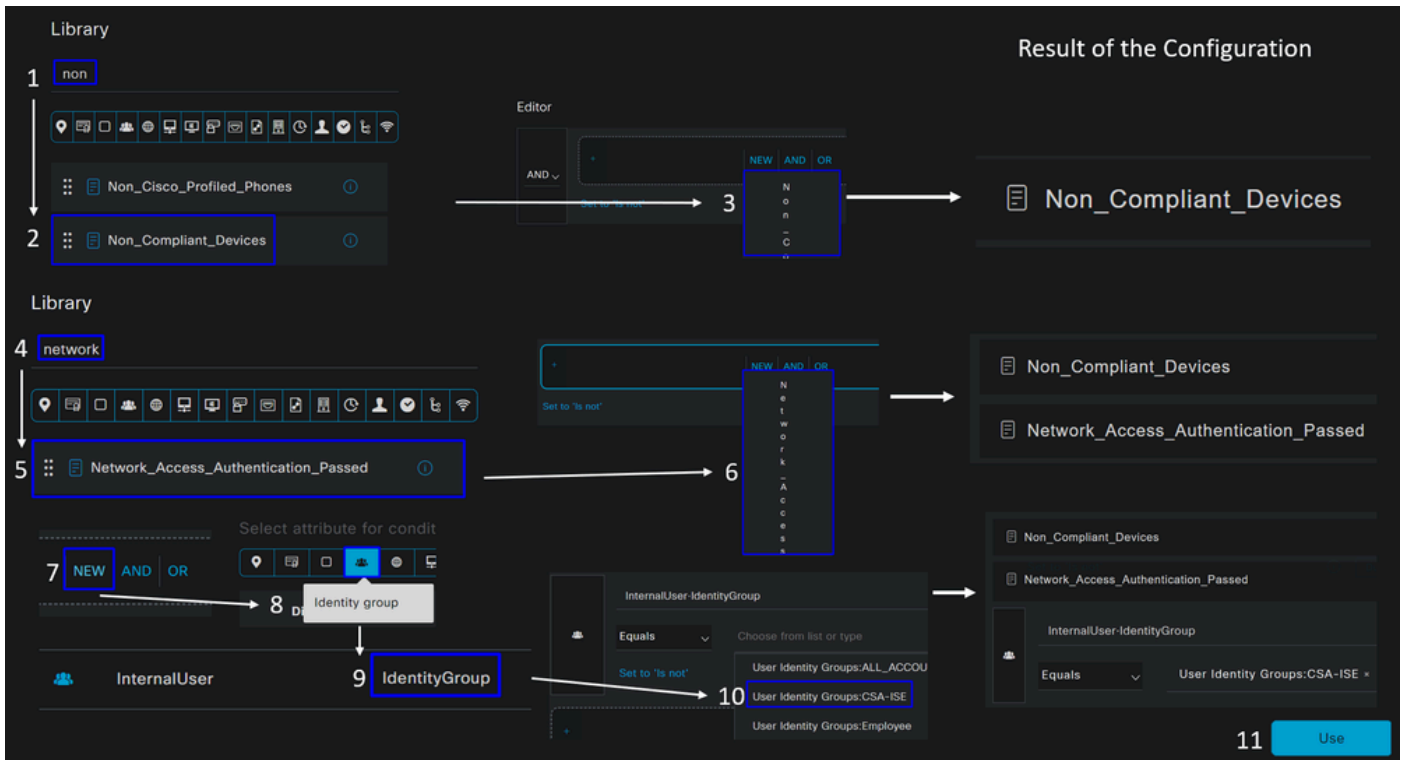


- Voor de volgende stap wijzigt u de Rule Name, Conditions en Profiles
- Wanneer u het **Name** configuratiebestand instelt op **CSA-Non-Compliance**
- Klik op het **Condition**veld +

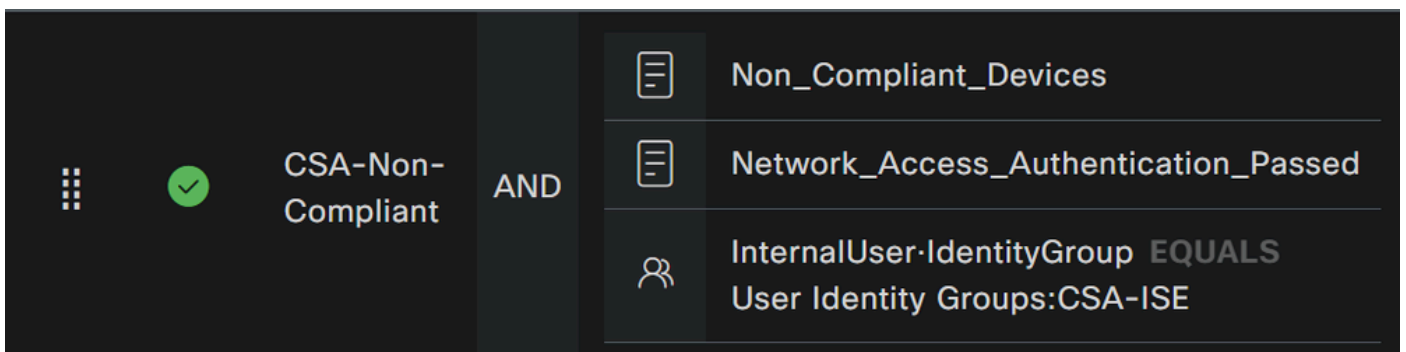
- Onder **Condition Studio**, vindt u de informatie:



- 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
- Kies **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**

⋮	✓	CSA-Non-Compliant	AND	☰	Non_Compliant_Devices	
				☰	Network_Access_Authentication_Passed	DenyAccess
				👤	InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE	

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

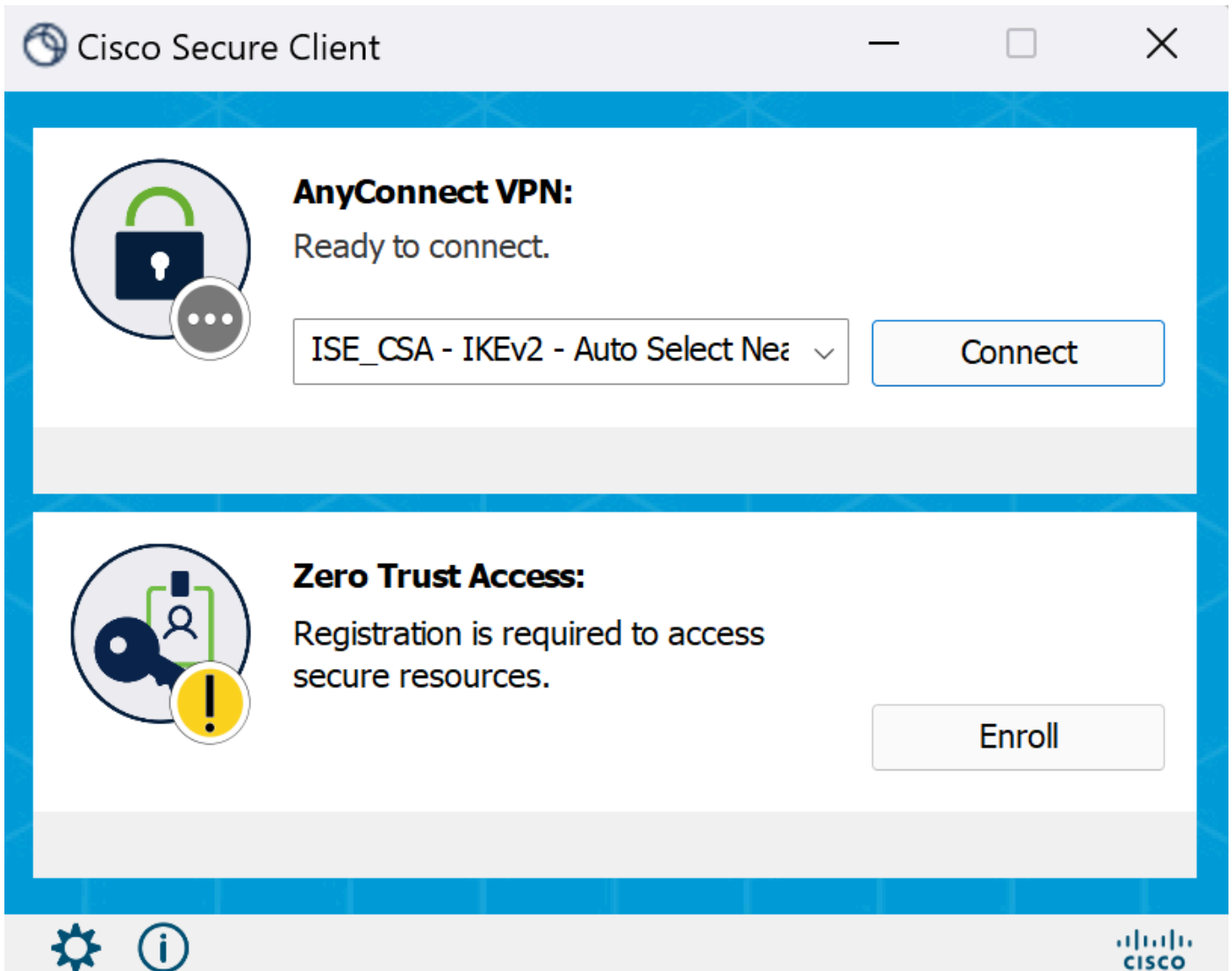
Maak verbinding met uw FQDN RA-VPN-domein op Secure Access via Secure Client.

---

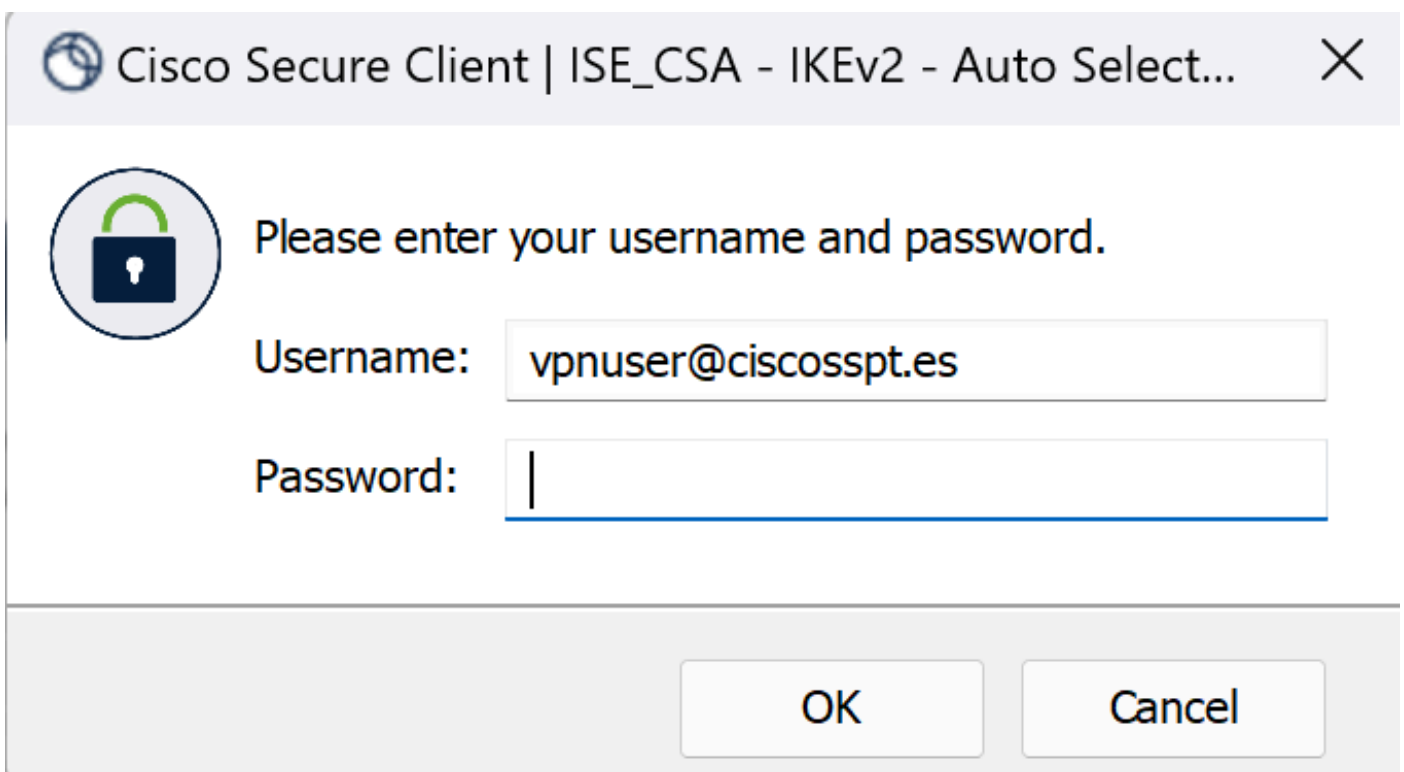
**Opmerking:** voor deze stap moet geen ISE-module worden geïnstalleerd.

---

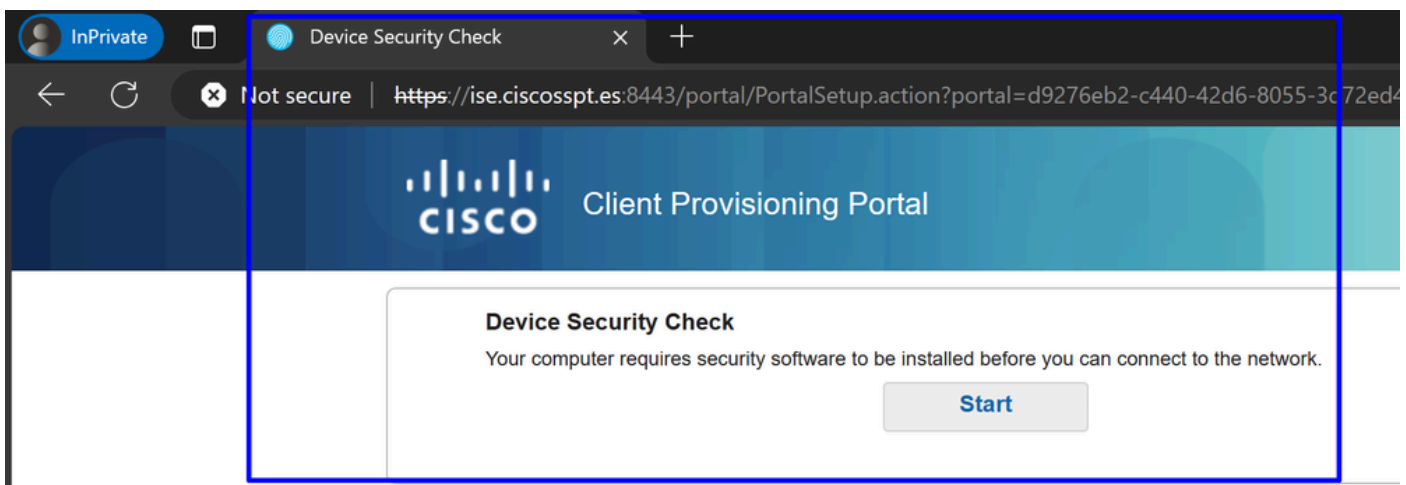
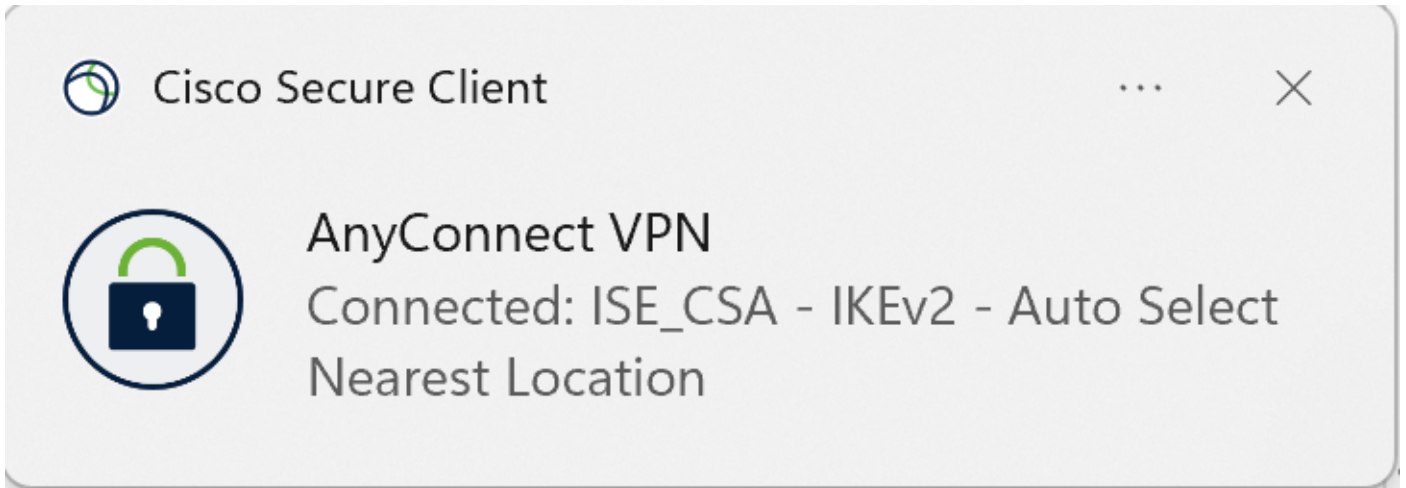
1. Verbinding maken met Secure Client.



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.

**Device Security Check**

Your computer requires security software to be installed before you can connect to the network.

9 Detecting if Agent is installed and running...

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



## Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent



+ This is my first time here




+ Remind me what to do next

6. Klik op [Click here to download and install agent](#)

**+ This is my first time here**

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

 You have 4 minutes to install and for the compliance check to complete

7. Installeer de agent

# Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

[See more](#)

Network Setup Assistant



## Network Setup Assistant



Installation is completed.

Quit

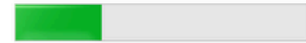
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

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.



# 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

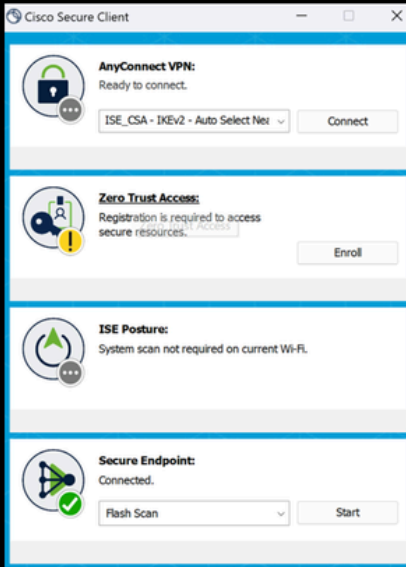


**Opmerking:** als u Cancel of de resterende tijd eindigt, wordt u automatisch niet-conform, valt u onder het autorisatiebeleid dat is ingesteld op [CSA-Non-Compliance](#), en wordt u onmiddellijk losgekoppeld van de VPN.

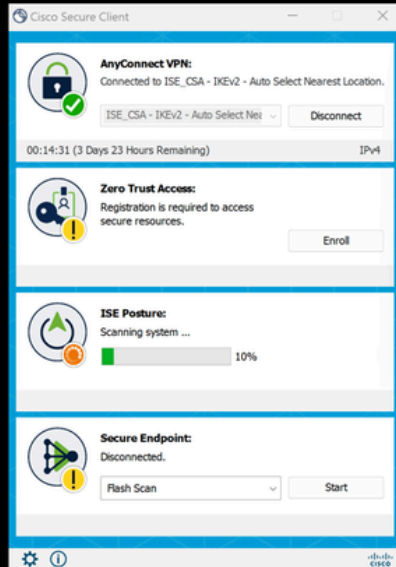
---

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

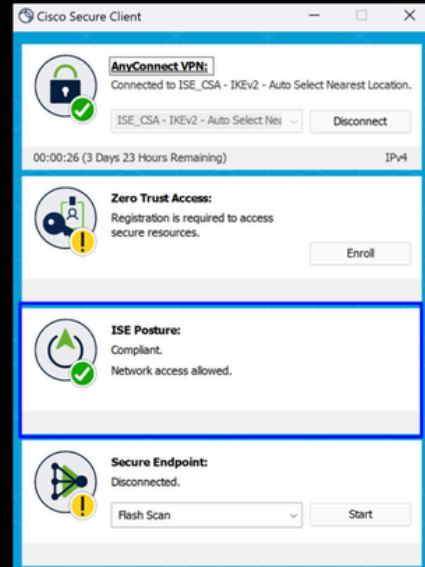
## Secure Endpoint Installed



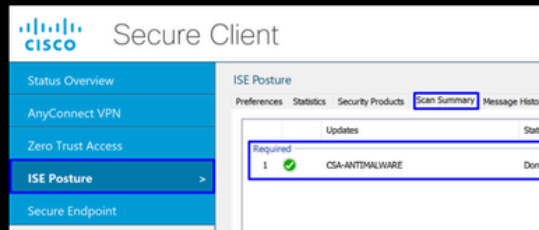
## Agent Scanning



## ISE Posture Successful validated



## Scan Summary - Compliance



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:

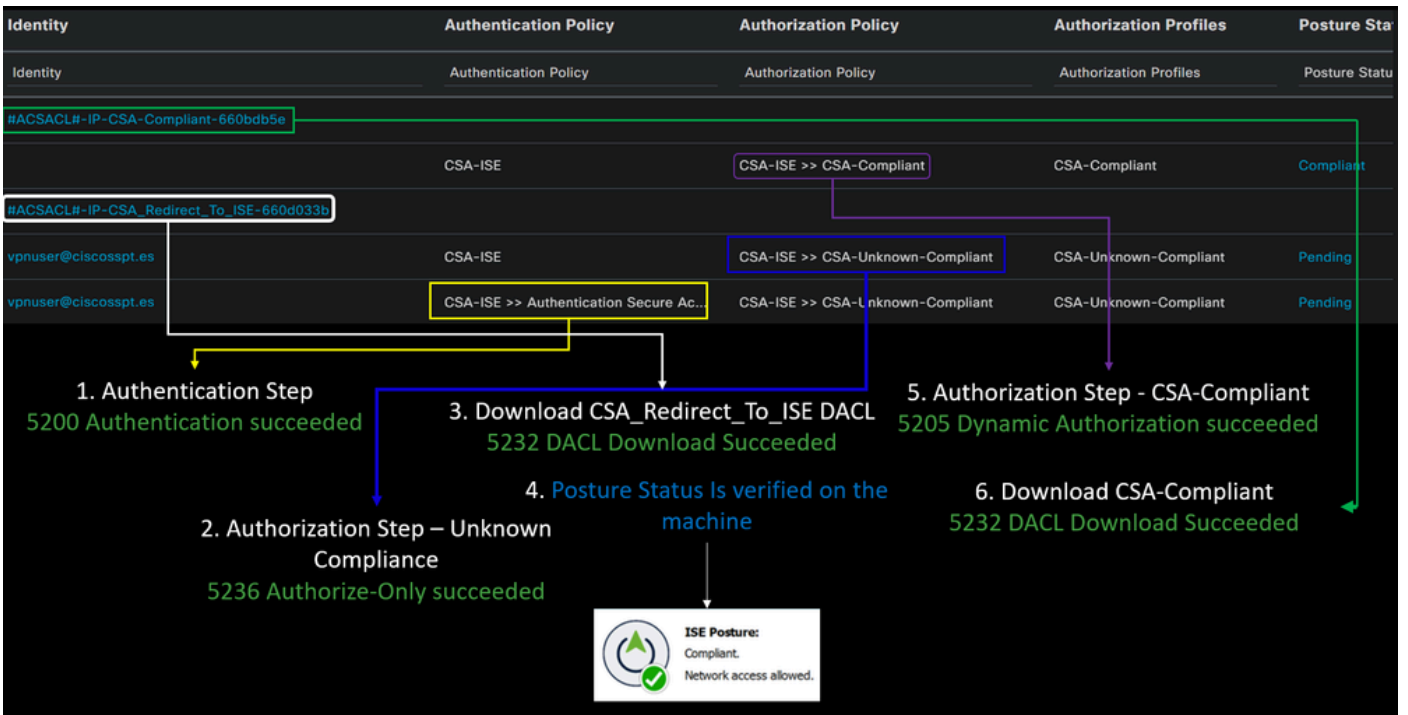
- Naar uw ISE-dashboard navigeren

- Klik op Operations > Live Logs

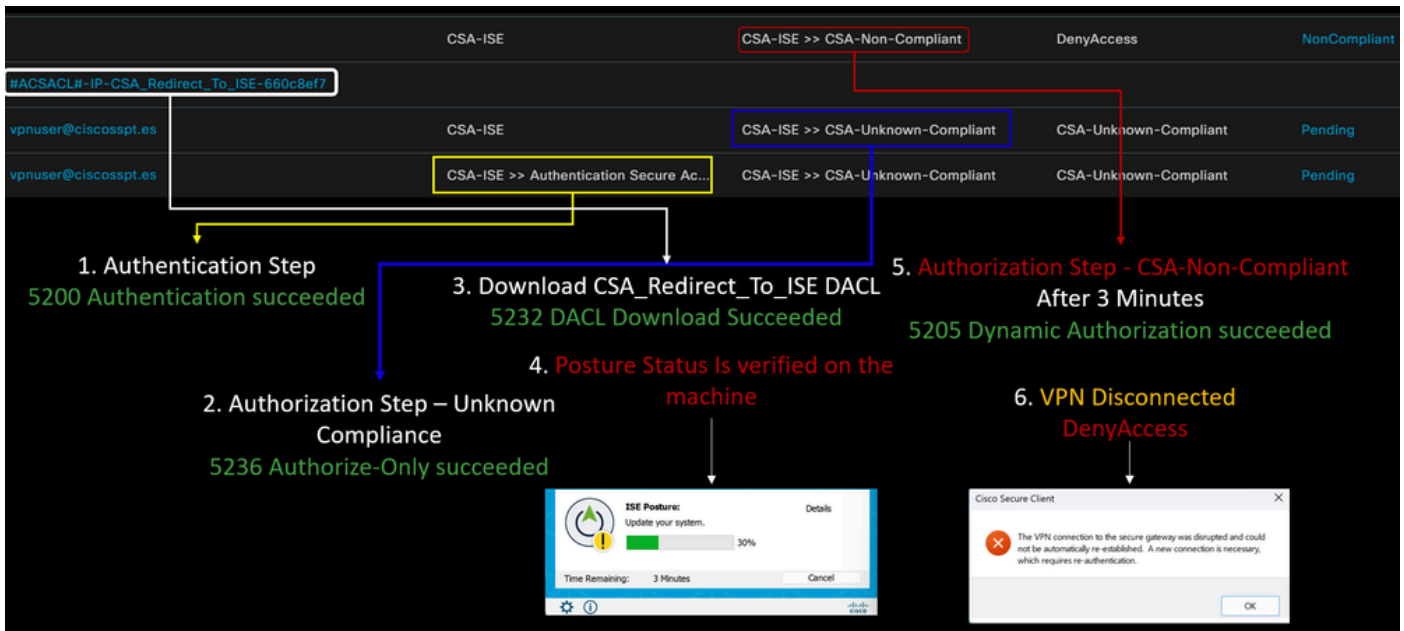
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter	
0	0	0	0	0	
Refresh Never		Show Latest 50 records		Within Last 24 hours	
Reset Repeat Counts		Export To		Filter	
Time	Status	Details	Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 07:00:27.7...	✓		Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 06:56:15.4...	✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660d033b	CSA-ISE	CSA-ISE >> CSA-Non-Complia
Apr 03, 2024 06:56:15.3...	✓		vpuser@ciscospt.es	CSA-ISE	CSA-ISE >> CSA-Unknown-Co
Apr 03, 2024 06:56:15.2...	✓		vpuser@ciscospt.es	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> CSA-Unknown-Co

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**

HomeFTD	✓ Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-------------	------------------	---------------	---	---------------

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



## Summary



Connected

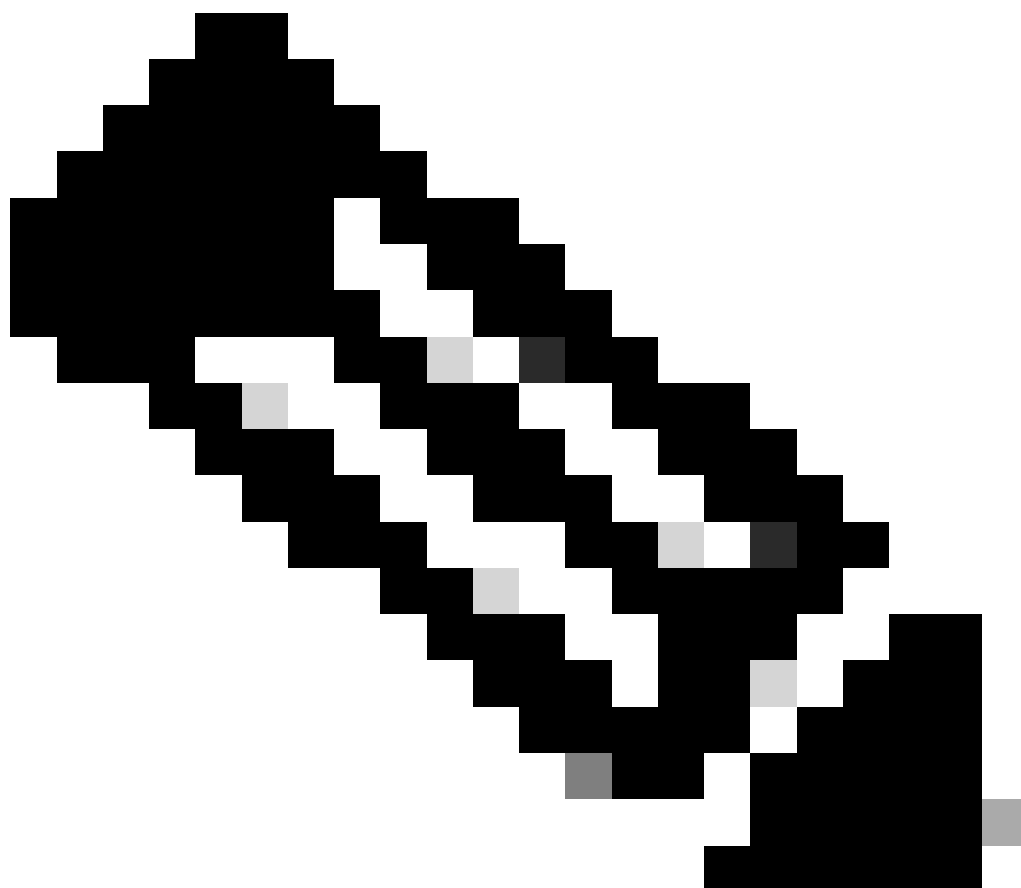
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

**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:

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

EUROPE						1	^
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups		
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA		 

**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

**Private Resource Name**

CiscoISE

**Description** (optional)

## Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#) 

Internally reachable address	(FQDN, Wildcard FQDN, IP Address, CIDR)	ⓘ	Protocol	Port / Ranges	+ Protocol & Port
192.168.10.206			TCP - (HTTP/HTTPS)	Any	

[+ IP Address or FQDN](#)

**VPN connections**

Allow endpoints to connect to this resource when connected to the network using VPN.

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

## 1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


### Action

 <b>Allow</b> Allow specified traffic if security requirements are met.	 <b>Block</b> Block specified traffic.
---	--


<b>From</b> Specify one or more <b>sources</b> . <input type="text" value="CSA (ciscospt.es\CSA)"/>	<b>To</b> Specify one or more <b>destinations</b> . <input type="text" value="CiscoISE"/>
Information about sources, including selecting multiple sources. <a href="#">Help</a>	Information about destinations, including selecting multiple destinations. <a href="#">Help</a>

### Endpoint Requirements

For VPN connections:

 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [?](#)  
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

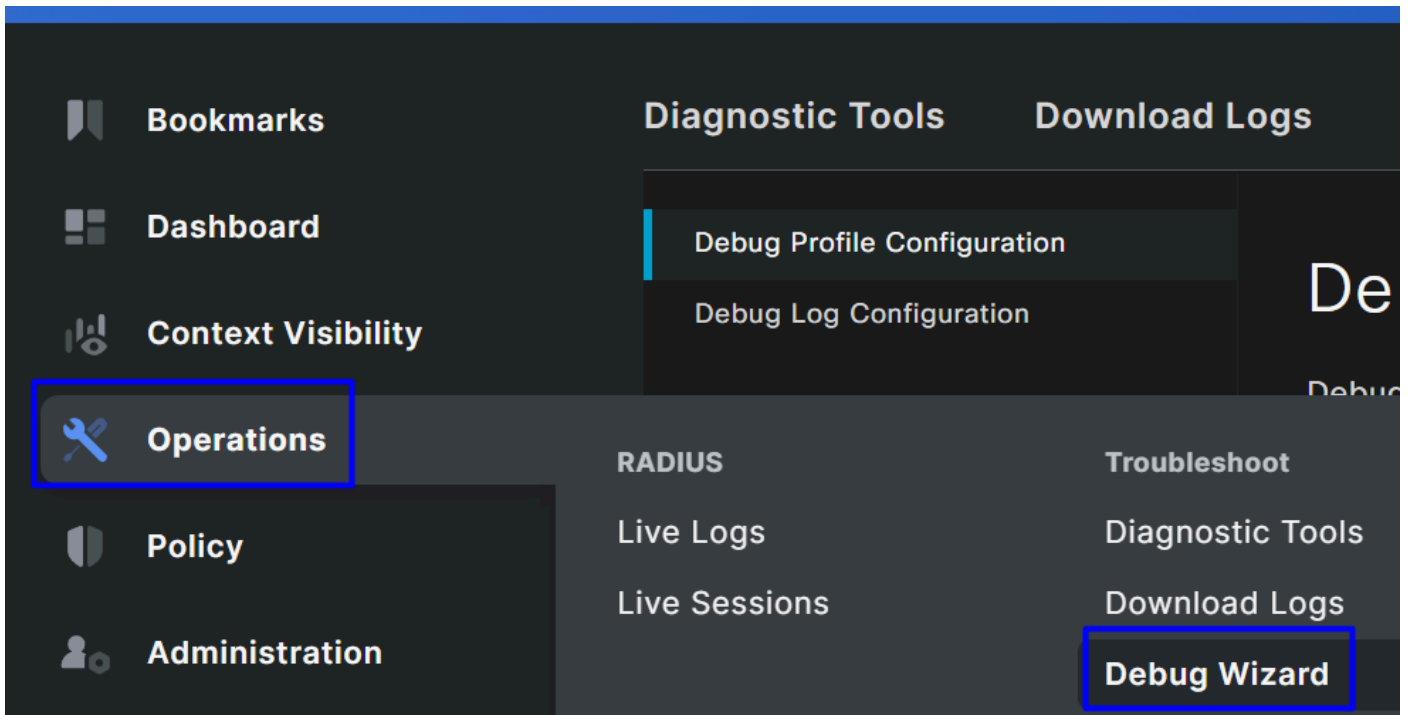
## Problemen oplossen

### Hoe te downloaden ISE postuur Debug logboeken

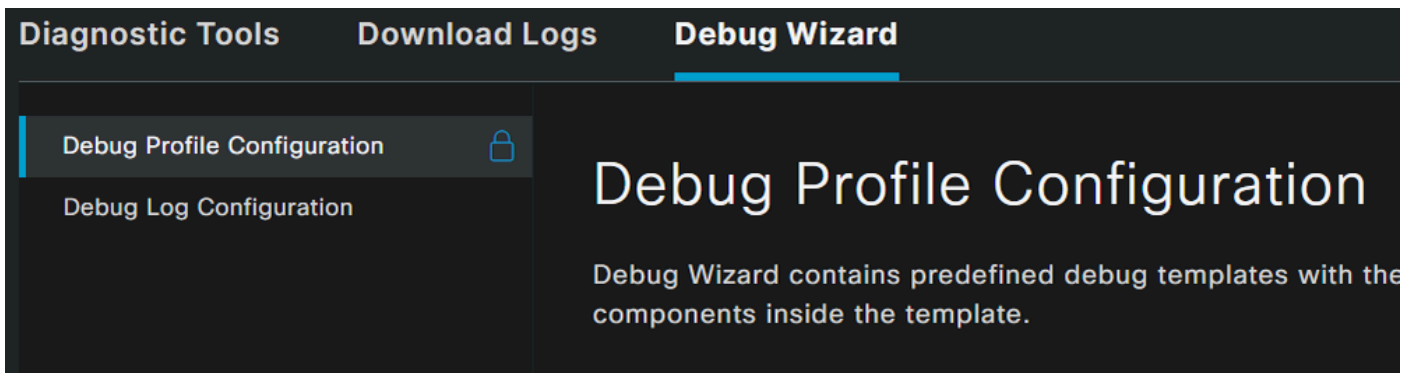
Als u ISE Logs wilt downloaden om een probleem met betrekking tot postuur te verifiëren, gaat u verder met de volgende stappen:

- 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

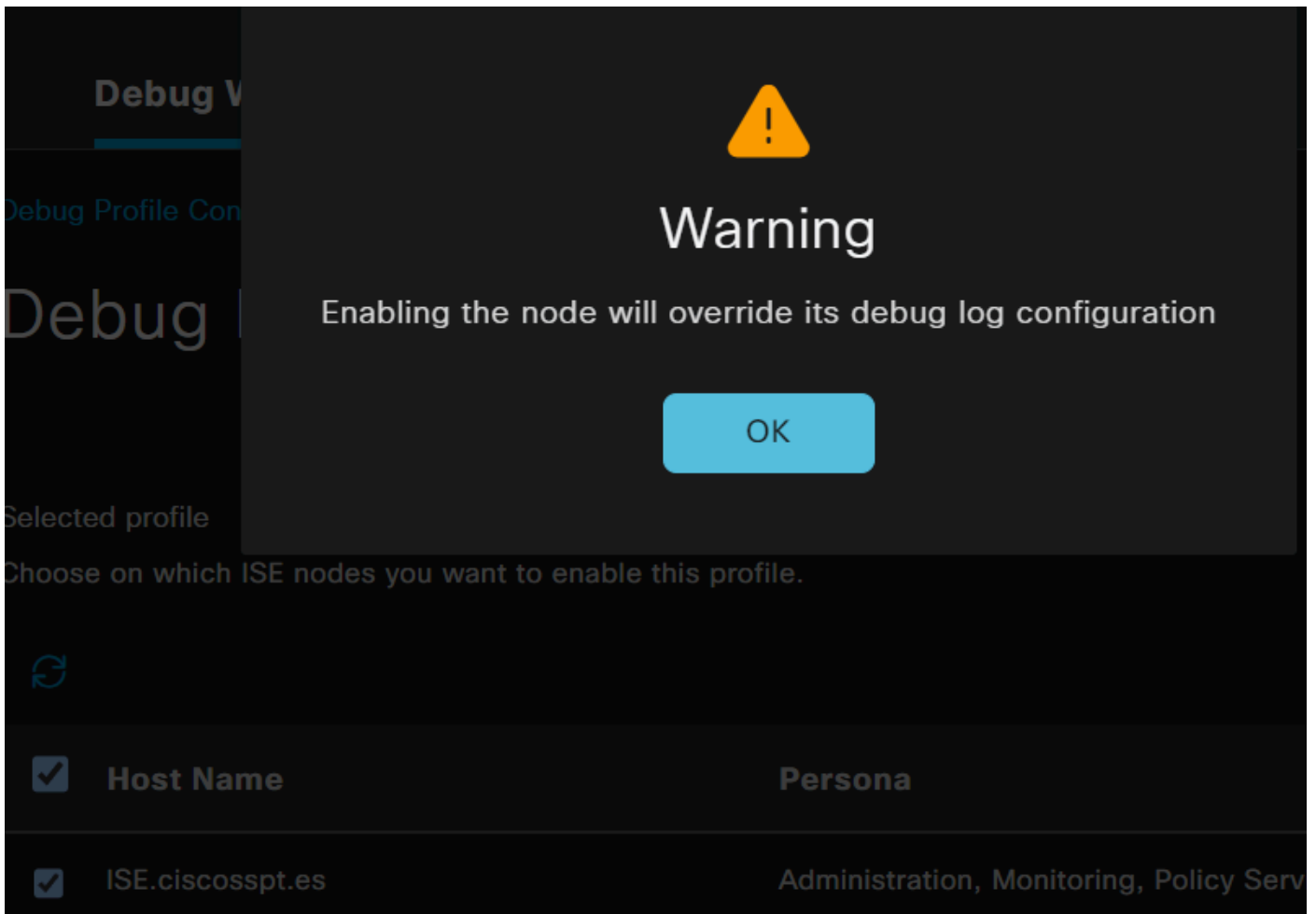
1



Posture

Pos

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



The image shows a warning dialog box overlaid on a configuration page. The dialog box has a dark background with a yellow warning triangle icon at the top center. Below the icon, the word "Warning" is displayed in a large, white font. Underneath, the message "Enabling the node will override its debug log configuration" is written in a smaller white font. At the bottom of the dialog box is a blue button with the text "OK".

The background configuration page is partially visible and includes the following elements:

- A header "Debug V" with a blue underline.
- A sub-header "Debug Profile Con".
- A large heading "Debug".
- A section titled "Selected profile".
- A prompt: "Choose on which ISE nodes you want to enable this profile."
- A refresh icon (circular arrow).
- A table with two columns: "Host Name" and "Persona".
- Two rows in the table, both with checked checkboxes in the first column:
  - Row 1: "Host Name" | "Persona"
  - Row 2: "ISE.ciscosspt.es" | "Administration, Monitoring, Policy Serv"

- Klik op de knop Save

# Debug Nodes

Selected profile Posture

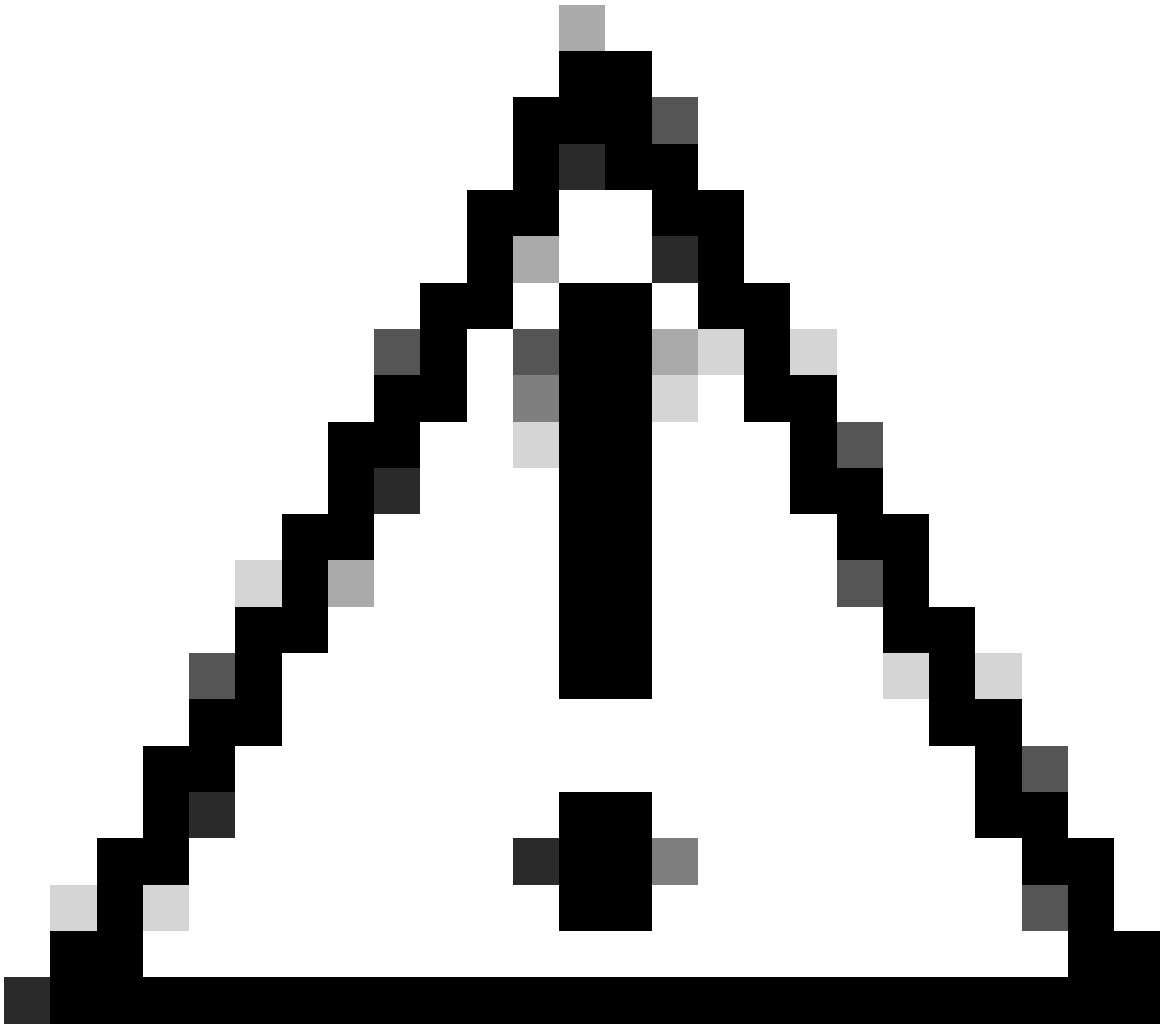
Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

Cancel

**Save**



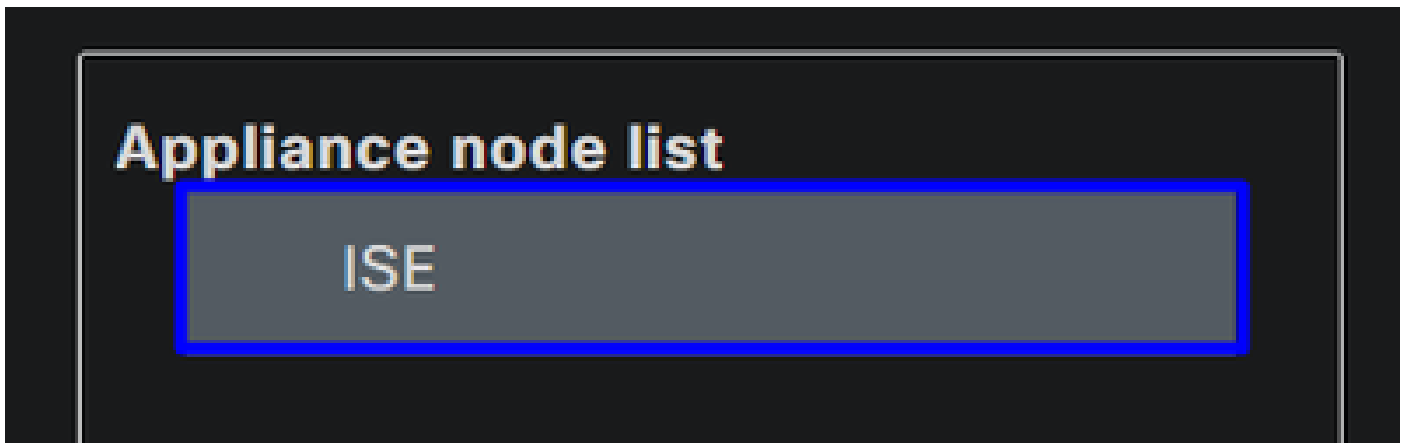
---

**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:

## Support Bundle

## Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

\* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

### Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

\* Encryption key  ⓘ

\* Re-Enter Encryption key

Create Support Bundle

- 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**

## Support Bundle - Last Generated

File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

[Download](#)

[Delete](#)



**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



## 100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

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.