

Secure Client NAM Profile via ISE 3.3 op Windows configureren en implementeren

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Netwerkdigram](#)

[Gegevensstroom](#)

[Switch configureren](#)

[Het Secure-clientpakket downloaden](#)

[ISE-configuratie](#)

[Stap 1. Upload het pakket op ISE](#)

[Stap 2. Een NAM-profiel maken vanuit de profieleditor](#)

[Stap 3. Upload het NAM Profile op ISE](#)

[Stap 4. Een postenprofiel maken](#)

[Stap 5. Configuratie van agent maken](#)

[Stap 6. Clientprovisioningbeleid](#)

[Stap 7. posterisatiebeleid](#)

[Stap 8. Netwerkapparaat toevoegen](#)

[Stap 9. Autorisatieprofiel](#)

[Stap 10. Toegestane protocollen](#)

[Stap 11. Active Directory](#)

[Stap 12. Beleidsverzamelingen](#)

[Verifiëren](#)

[Stap 1. Download en installeer de Secure Client Posture/NAM-module van ISE](#)

[Stap 2. EAP-FAST](#)

[Stap 3. Posture Scan](#)

[Problemen oplossen](#)

[Stap 1. NAM Profile](#)

[Stap 2. Uitgebreide NAM-vastlegging](#)

[Stap 3. Debugs op Switch](#)

[Stap 4. Debugs op ISE](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u het profiel Cisco Secure Client Network Access Manager (NAM) kunt implementeren via Identity Services Engine (ISE).

Achtergrondinformatie

EAP-FAST-verificatie vindt in twee fasen plaats. In de eerste fase maakt EAP-FAST gebruik van een TLS-handdruk om sleuteluitwisselingen te verstrekken en te verifiëren met behulp van Type-Length-Values (TLV)-objecten om een beschermde tunnel tot stand te brengen. Deze TLV-objecten worden gebruikt om verificatiegerelateerde gegevens tussen de client en server over te brengen. Zodra de tunnel is opgezet, begint de tweede fase met de client en de ISE-knooppunt die verdere gesprekken voeren om het vereiste verificatie- en autorisatiebeleid vast te stellen.

Het NAM-configuratieprofiel is ingesteld om EAP-FAST te gebruiken als de verificatiemethode en is beschikbaar voor administratief gedefinieerde netwerken.

Daarnaast kunnen zowel machine- als gebruikerstypen worden geconfigureerd binnen het NAM-configuratieprofiel.

Het Windows-apparaat van het bedrijf krijgt volledige bedrijfstoegang met behulp van de NAM met Posture check.

Het persoonlijke Windows-apparaat krijgt toegang tot een beperkt netwerk met dezelfde NAM-configuratie.

Dit document bevat instructies voor de implementatie van het profiel Cisco Secure Client Network Access Manager (NAM) via het poortportal van Identity Services Engine (ISE) met behulp van webimplementatie, samen met de controle op naleving van posteringen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE)
- AnyConnect NAM en profieleditor
- posturisatiebeleid
- Cisco Catalyst configuratie voor 802.1x-services

Gebruikte componenten

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

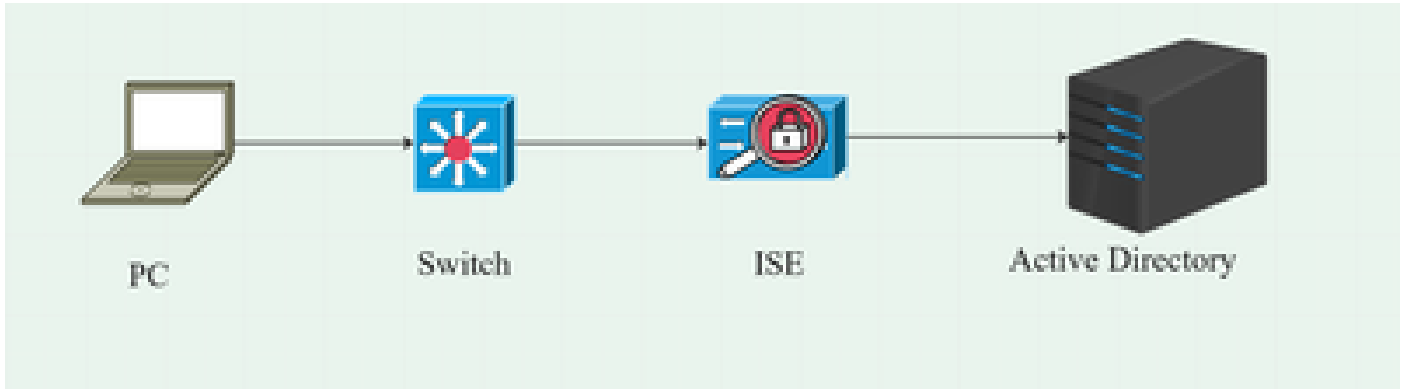
- Cisco ISE, release 3.3 en hoger
- Windows 10 met Cisco Secure Mobility Client 5.1.4.74 en hoger
- Cisco Catalyst 9200 switch met software, Cisco IOS® XE 17.6.5 en hoger
- Active Directory 2016

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.

Configuratie

Netwerkdigram



Gegevensstroom

Wanneer een pc verbinding maakt met het netwerk, biedt de ISE het autorisatiebeleid voor omleiding naar het Posture Portal.

Het http-verkeer op de pc wordt omgeleid naar de ISE-pagina voor clientprovisioning, waar de NSA-toepassing wordt gedownload van ISE.

De NSA installeert vervolgens de Secure Client Agent-modules op de PC.

Nadat de installatie van de agent is voltooid, downloadt de agent het Posteringprofiel en het NAM-profiel dat op ISE is geconfigureerd.

De installatie van de NAM module brengt een nieuw begin op PC teweeg.

Na het opnieuw opstarten voert de NAM-module EAP-FAST-verificatie uit op basis van het NAM-profiel.

De Posture-scan wordt dan geactiveerd en de naleving wordt gecontroleerd op basis van het ISE Posture Policy.

Switch configureren

Configureer de access switch voor dot1x-verificatie en omleiding.

```
aaa new-model  
  
aaa verificatie dot1x standaardgroepstraal  
Standaard netwerkgroepstraal voor aaa-autorisatie  
aaa accounting dot1x standaard start-stop groepsstraal  
aaa server straal dynamisch-auteur  
client 10.127.197.53 server-key Qwerty123  
van het auth-type
```

```
aaa sessie-id gemeenschappelijk
IP-straal vanaf bron-interface VLAN1000
radius-server attribuut 6 on-for-login-auth
RADIUS-serverkenmerk 8 inclusief-in-access-req
25 access-request omvatten
radius-server attribuut 31 mac formaat ietf hoofdletters
radius server RAD1
IP-adres4 <ISE-server> 1812-poorts 1813 met automatische poort
toets <geheime toets>

dot1x-systeem met automatische controle
```

Configureer omleiding van ACL zodat gebruiker kan worden omgeleid naar ISE-clientprovisioningportal.

```
IP-toegangslijst - uitgebreid, omgeleid-acl
10 ontkennen udp elk eq-domein
20 ontken tcp elk eq domein
30 ontkennen udp een eq bootpc een eq bootps
40 Geen IP-host weigeren <ISE-server>
50 vergunning tcp elk eq www
60 vergunningen tcp elke willekeurige eq 443
```

Schakel apparaatracering en http-omleiding op de switch in.

```
beleid voor apparaatracering <naam van beleid voor apparaatracering>
volgen inschakelen
interface <naam interface>
<naam van beleid voor apparaatracering>

IP-http server
IP-http: beveiligde server
```

Het Secure-clientpakket downloaden

Download de profieeditor, beveiligde clientvensters en de nalevingsmodule webimplementatiebestanden handmatig van software.cisco.com

Type Secure Client 5 in de zoekbalk voor productnamen.

Downloads - Home > Beveiliging > Endpoint Security > Beveiligde client (inclusief AnyConnect) > Beveiligde client 5 > AnyConnect VPN-clientsoftware

- Cisco-Secure-Client-win-5.1.4.74-webopstellen-k9.pkg

- Cisco-secure-client-win-4.3.4164.8192-iscompliance-webimplementation-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

ISE-configuratie

Stap 1. Upload het pakket op ISE

Als u de beveiligde client- en nalevingsmodule wilt uploaden via de webimplementatiepakketten van ISE, navigeer naar Workcenter > houding > clientprovisioning > resources > toevoegen > resources van agent vanaf lokale schijf.

Client Provisioning Policy

Resources

Client Provisioning Portal

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

Choose File: cisco-secure-...deploy-k9.pkg

Agent Uploaded Resources

Name	Type	Version	Description
CiscoSecureClientDesktopWindows 5.1...	CiscoSecureClientDesktopWindows	5.1.4.74	Cisco Secure Client for ...

Submit Cancel

Resources

Edit + Add Duplicate Delete

Name	Type	Version	Last Update	Description
Lab Profile	AgentProfile	Not Applicable	2024/07/26 17:23:41	
Agent Configuration	AgentConfig	Not Applicable	2024/07/26 16:00:49	
NAM Profile	AgentProfile	Not Applicable	2024/07/26 16:00:00	
CiscoSecureClientComplianceModuleWindows 4.3.4164.8192	CiscoSecureClientCo...	4.3.4164.8192	2024/07/26 15:58:44	Cisco Secure Client Win...
CiscoSecureClientDesktopWindows 5.1.4.074	CiscoSecureClientDe...	5.1.4.74	2024/07/26 15:56:27	Cisco Secure Client for ...
Cisco-ISE-NSP	Native Supplicant Pro...	Not Applicable	2023/07/04 05:25:16	Pre-configured Native S...
CiscoAgentlessOSX 5.0.03061	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 04:24:14	With CM: 4.3.3045.6400

Stap 2. Een NAM-profiel maken vanuit de profieleditor

Voor informatie over hoe u een NAM-profiel kunt configureren raadpleegt u deze handleiding [Secure Client NAM Profile configureren](#).

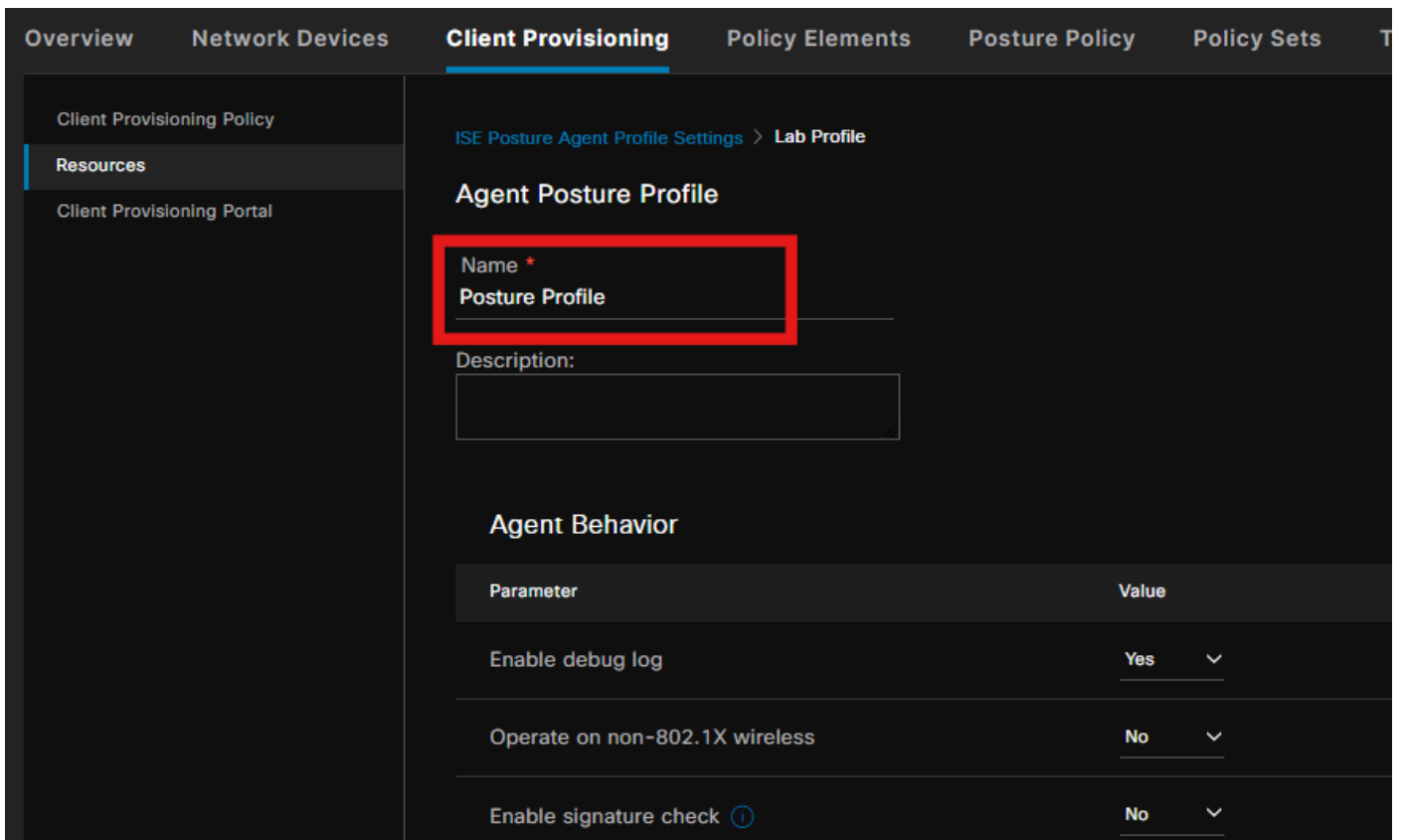
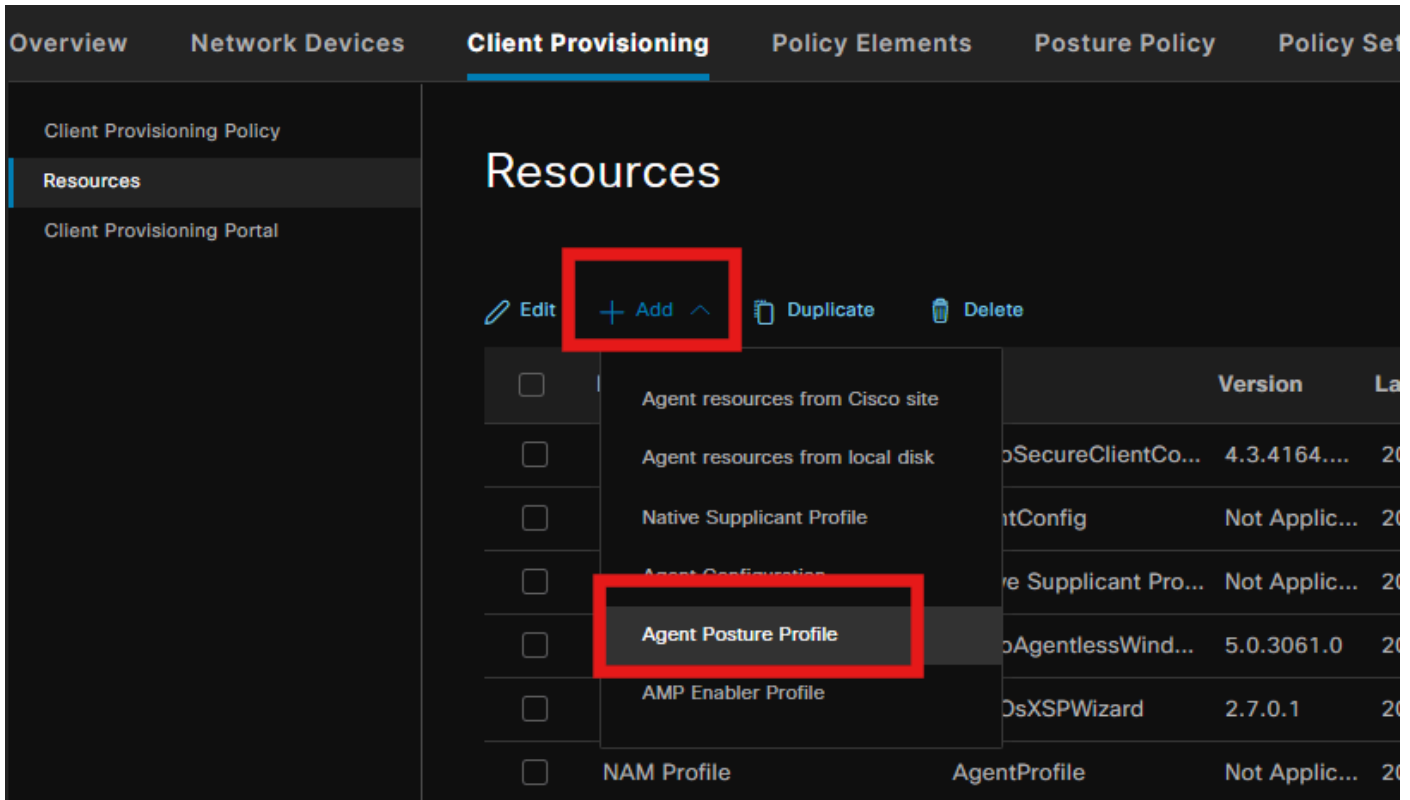
Stap 3. Upload het NAM Profile op ISE

Als u het NAM Profile "Configuration.xml" op ISE als Agent Profile wilt uploaden, navigeer dan naar Client Provisioning > Resources > Agent Resources From Local Disk.

The screenshot shows the ISE Client Provisioning interface. The breadcrumb navigation is "Agent Resources From Local Disk > Agent Resources From Local Disk". The page title is "Agent Resources From Local Disk". The form fields are as follows:

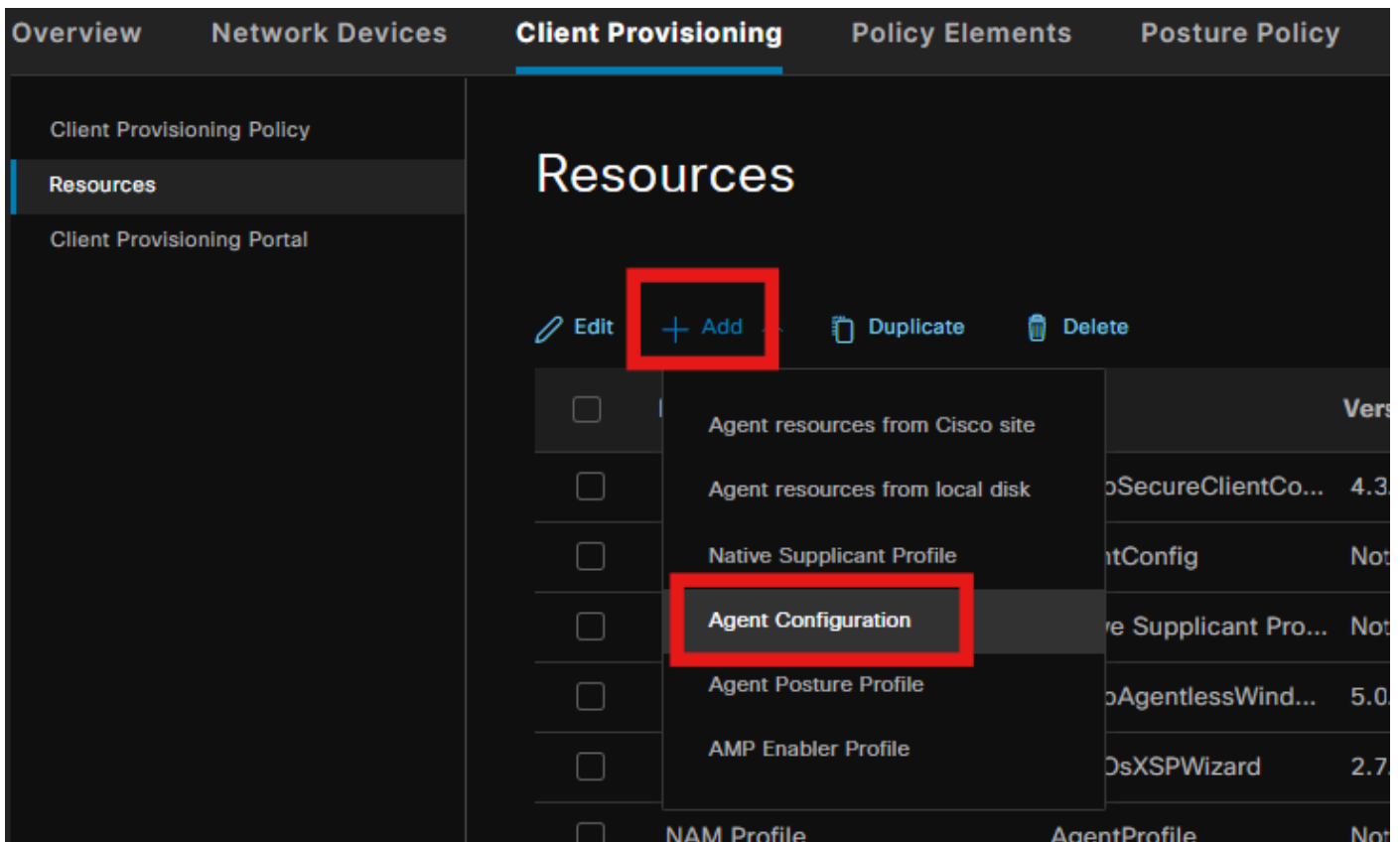
- Category: Customer Created Packs (dropdown menu)
- Type: Agent Profile (dropdown menu)
- * Name: New Profile (text input)
- Description: (empty text input)
- Choose File: configuration.xml (file selection button)
- Submit: (blue button)
- Cancel: (text link)

Stap 4. Een postenprofiel maken



Vergeet niet om in het gedeelte Posture Protocol * toe te voegen om de Agent in staat te stellen verbinding te maken met alle servers.

Stap 5. Configuratie van agent maken



Selecteer het geüploade beveiligde client- en nalevingsmodulepakket en selecteer onder de Moduleselectie de ISE Positie-, NAM- en DART-modules

Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets

Client Provisioning Policy
Resources
Client Provisioning Portal

[Agent Configuration](#) > **New Agent Configuration**

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 ▾

* Configuration Name:

Description:

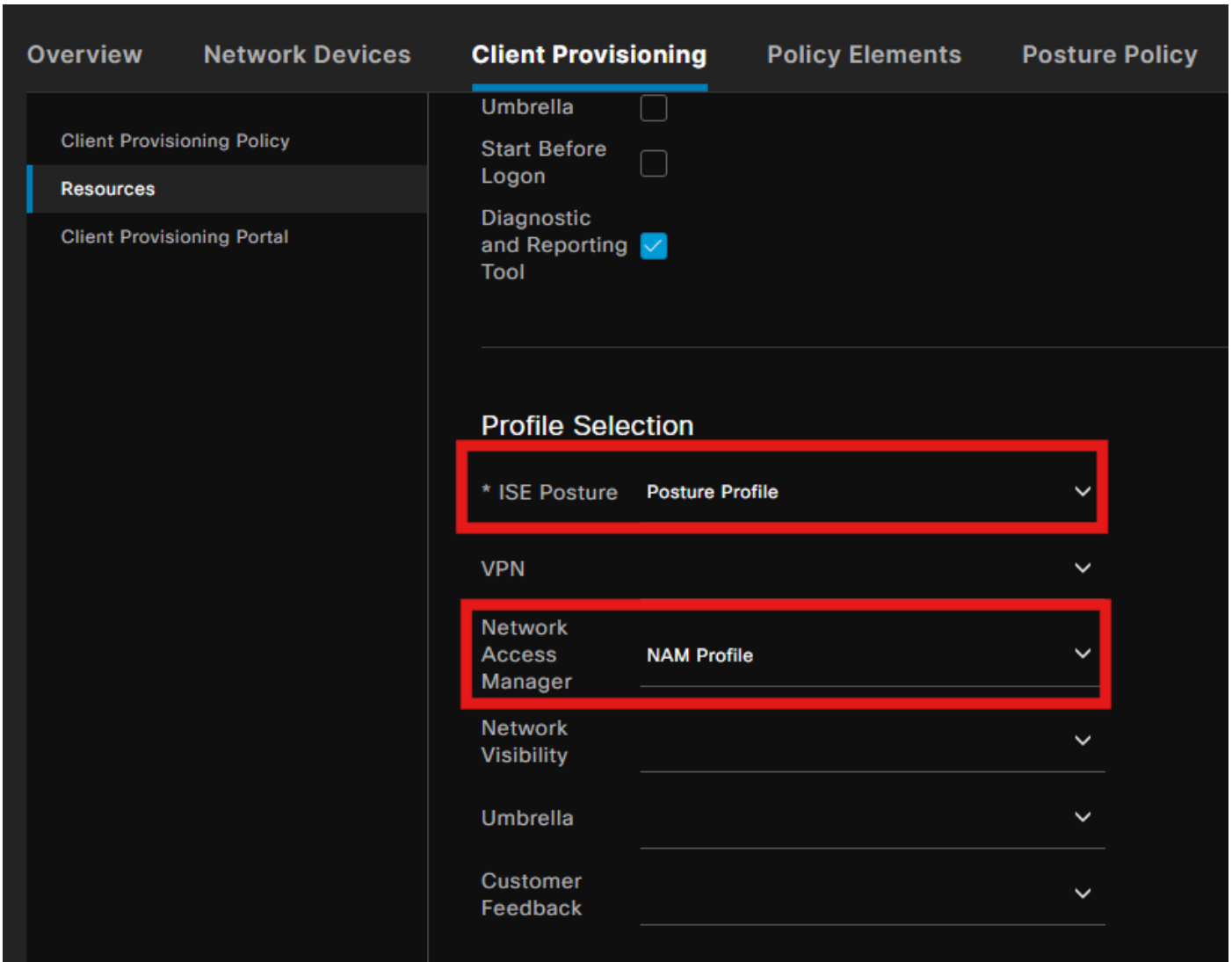
Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleW ▾

Cisco Secure Client Module Selection

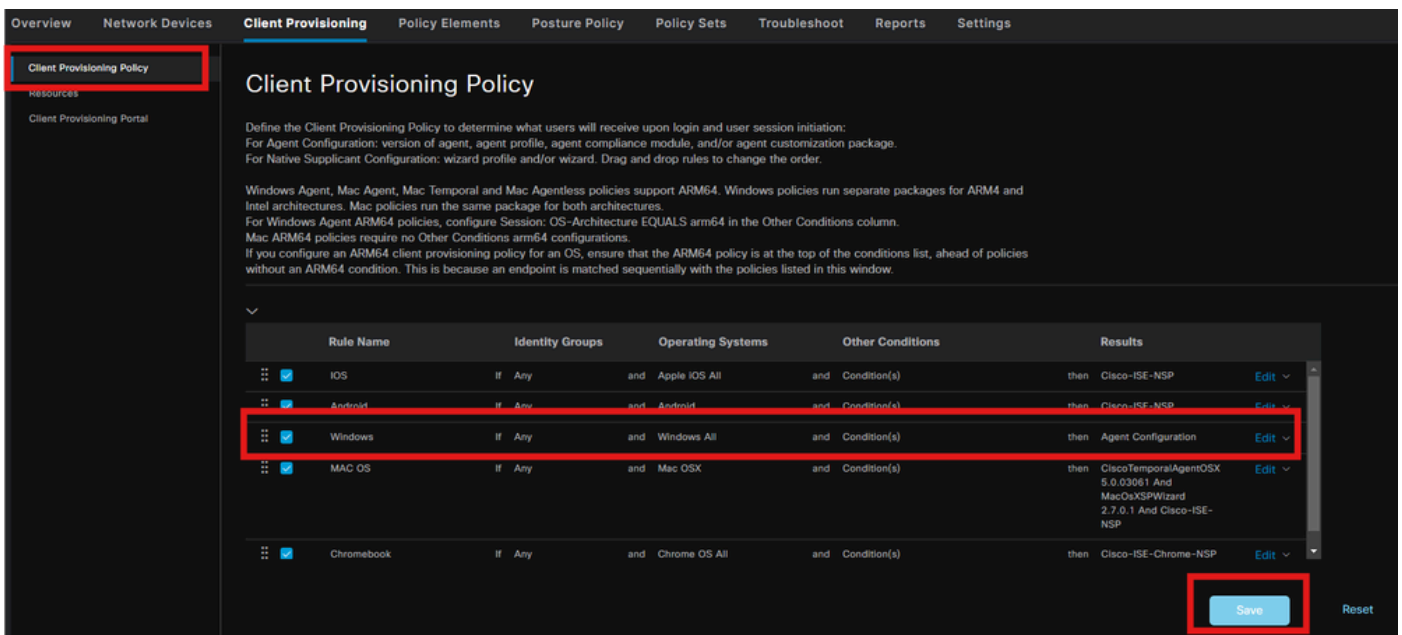
ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input checked="" type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>

Selecteer onder Profielselectie de optie Positie en NAM-profiel en klik op Indienen.



Stap 6. Clientprovisioningbeleid

Maak een client provisioningbeleid voor Windows-besturingssysteem en selecteer de Agent Configuration die in de vorige stap is gemaakt.

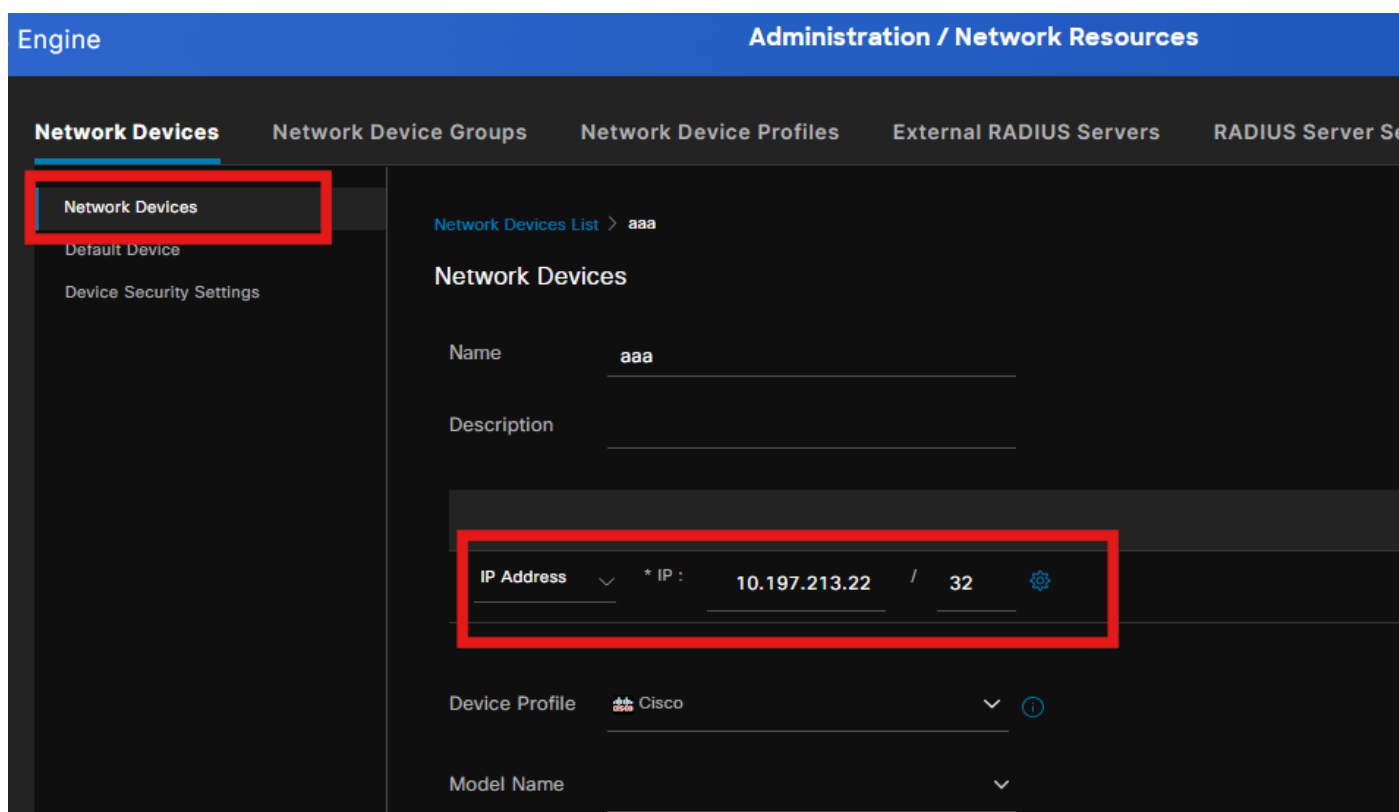


Stap 7. posterisatiebeleid

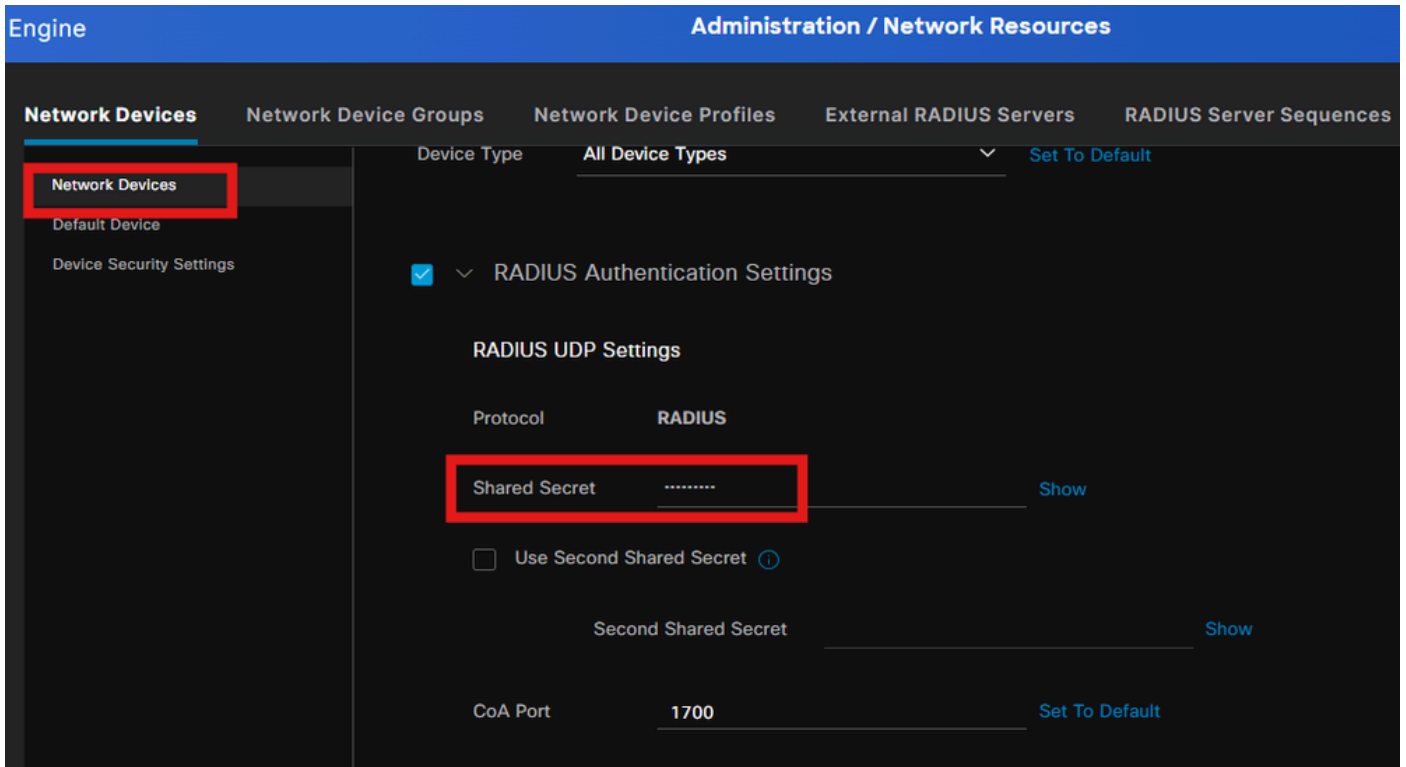
Voor meer informatie over het maken van de Posture Policy en voorwaarden, raadpleegt u deze handleiding [ISE Posture Prescriptive Implementation Guide](#).

Stap 8. Netwerkkapparaat toevoegen

Als u het IP-adres van de switch en de gedeelde geheime sleutel voor de radius wilt toevoegen, navigeert u naar Beheer > Netwerkbronnen.

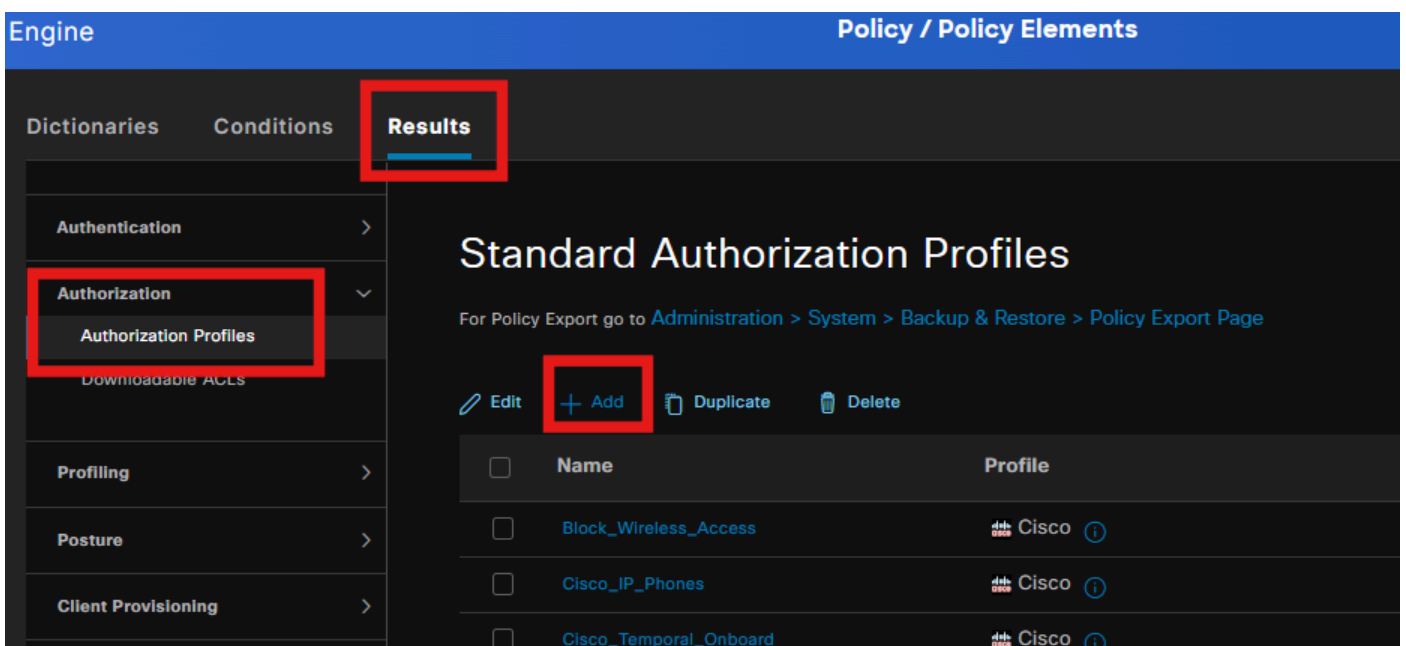


The screenshot displays the Cisco ISE Administration console interface. The top navigation bar is blue and contains the text "Engine" on the left and "Administration / Network Resources" on the right. Below this, a dark grey navigation menu lists several options: "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", and "RADIUS Server Se". The "Network Devices" option is highlighted with a red rectangular box. The main content area is titled "Network Devices List > aaa" and "Network Devices". It shows configuration fields for a device named "aaa": "Name" (aaa), "Description" (empty), "IP Address" (10.197.213.22 / 32), "Device Profile" (Cisco), and "Model Name" (empty). The "IP Address" field is highlighted with a red rectangular box. A gear icon is visible next to the IP address field.

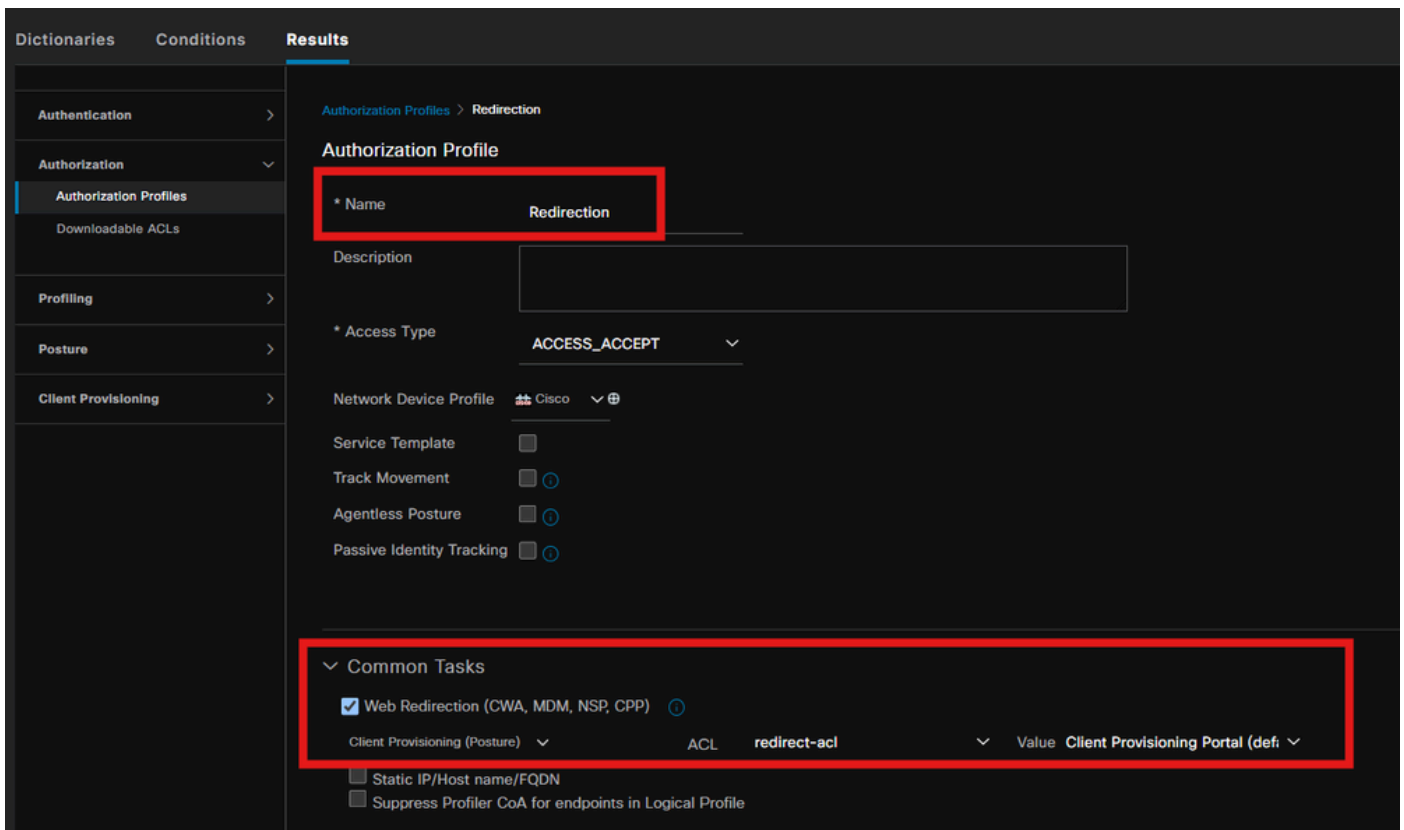


Stap 9. Autorisatieprofiel

Als u een posteringsprofiel wilt maken, navigeert u naar Policy > Policy Elements > Results.

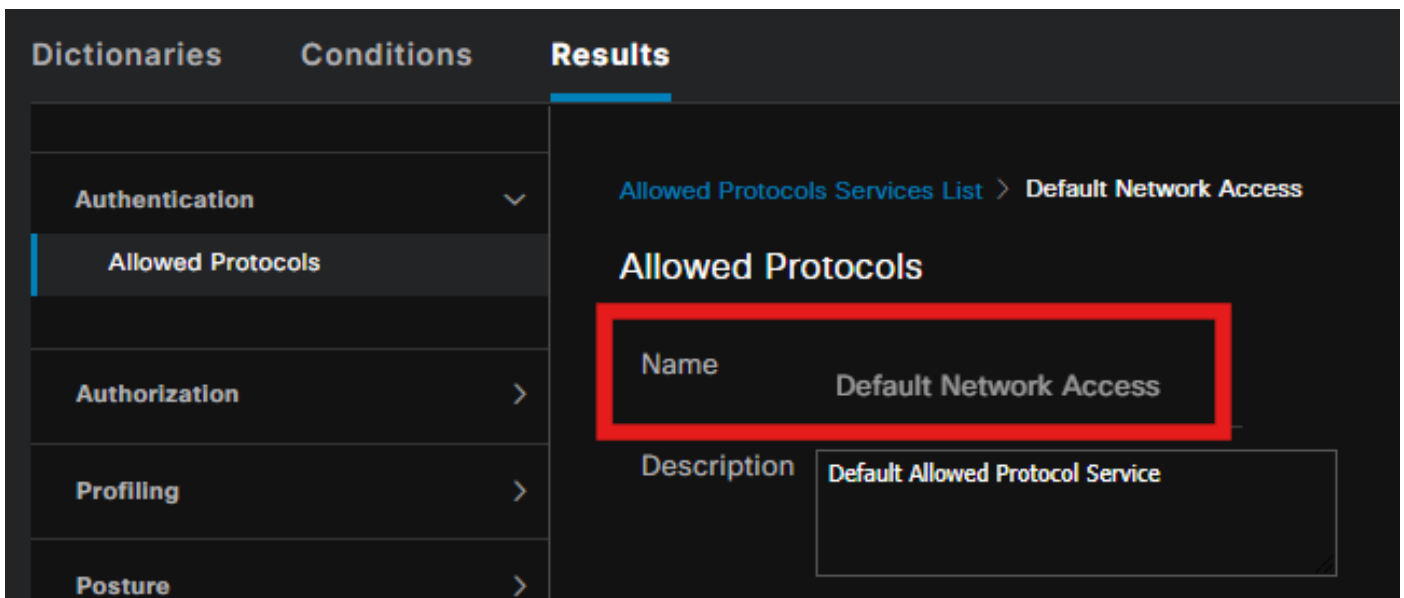


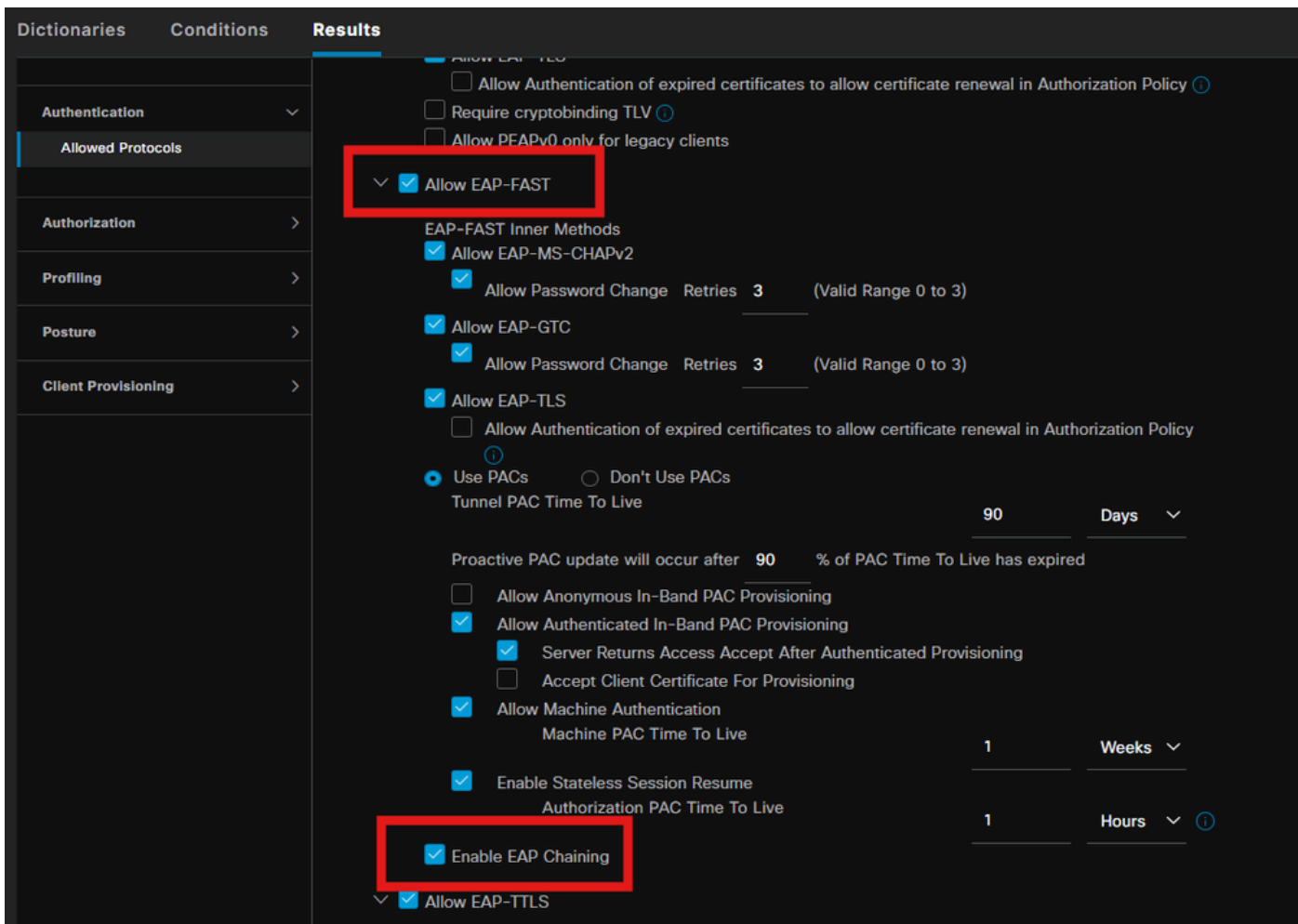
Selecteer onder opdrachttaak de client Provisioning Portal met omleiding van ACL.



Stap 10. Toegestane protocollen

Navigeren naar **Beleid > Beleidselementen > Resultaten > Verificatie > Toegestane protocollen**, selecteer de instellingen voor EAP-koppeling,

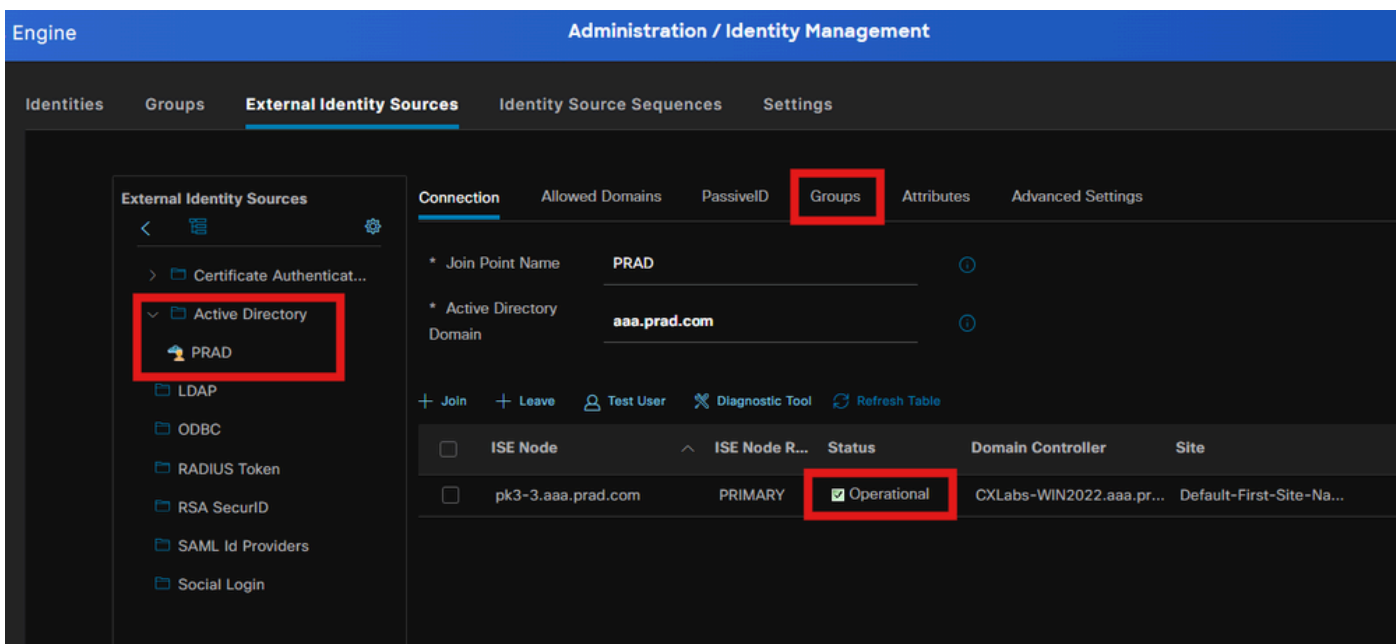




Stap 11. Active Directory

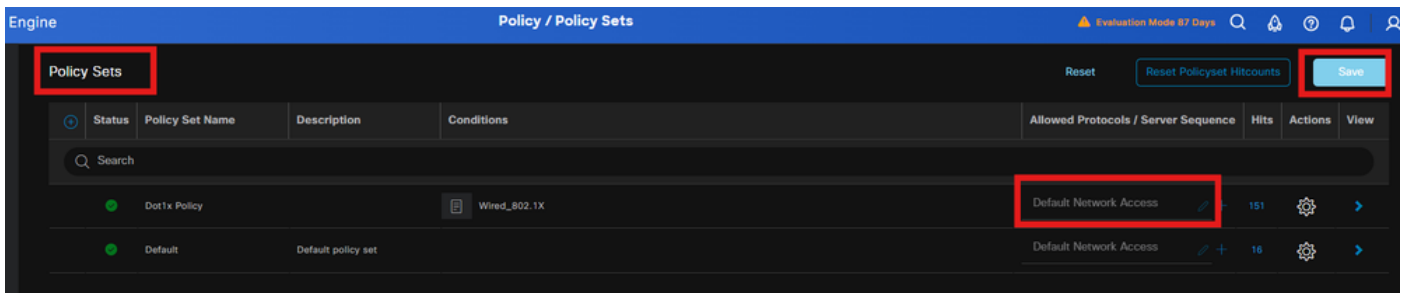
Validate ISE wordt aangesloten met Active Directory domein en de domeingroepen worden geselecteerd indien nodig voor de autorisatievoorwaarden.

Beheer > Identiteitsbeheer > Externe Identiteitsbronnen > Active Directory

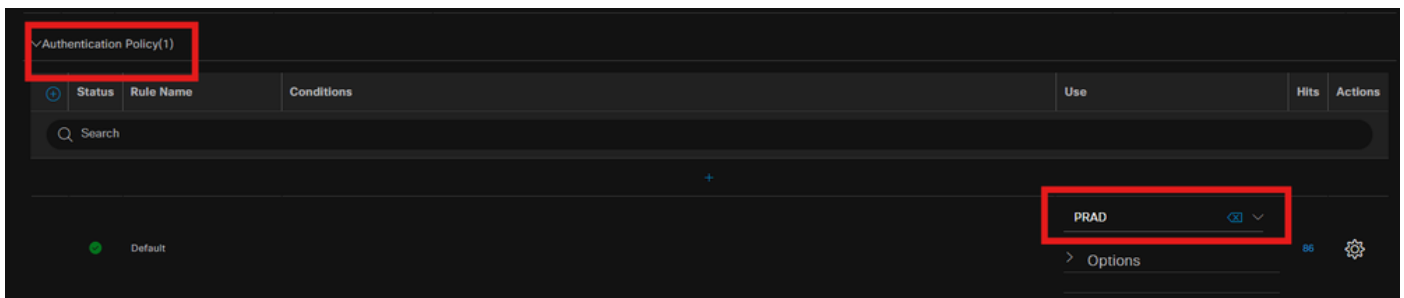


Stap 12. Beleidsverzamelingen

Maak een beleidsset op ISE om de dot1x aanvraag te authenticeren. Ga naar Beleidssets > Beleidssets.



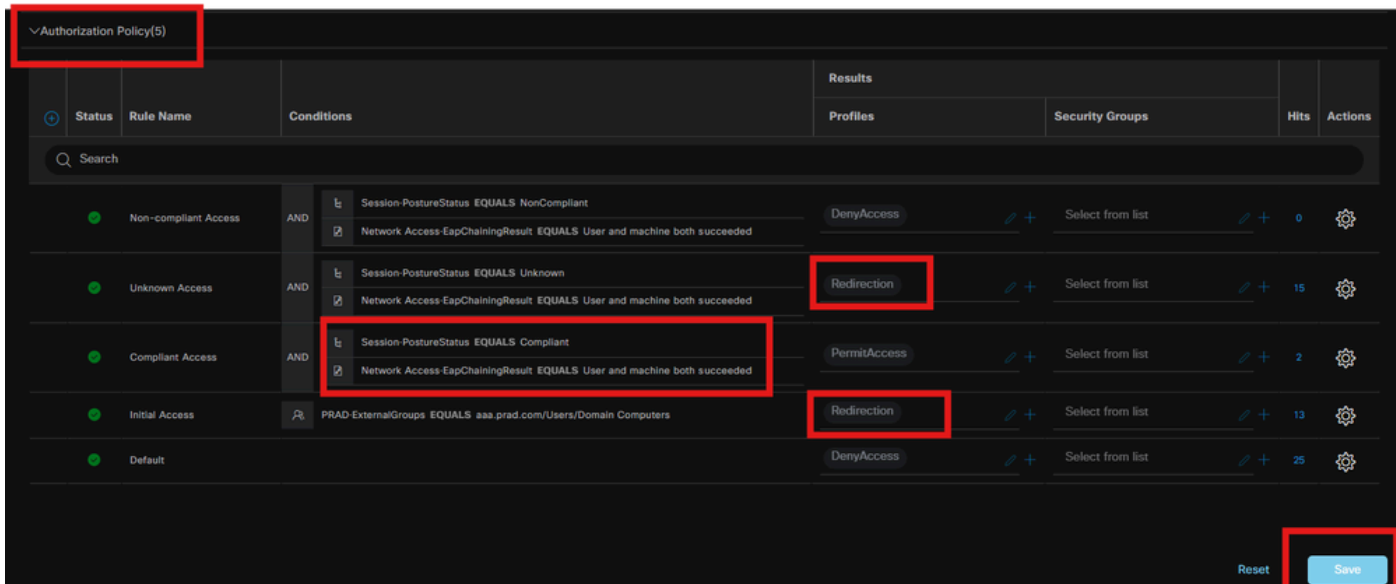
Selecteer de Active Directory als identiteitsbron voor Verificatiebeleid.



Configureer verschillende autorisatieregels op basis van status onbekend, niet-conform en conform.

In dit geval van gebruik.

- Initial Access: omleiding naar ISE Client Provisioning Portal om Secure Client Agent en NAM Profile te installeren
- Onbekende toegang: toegang tot client provisioningportal voor omleiding op basis van posture-detectie
- Conforme toegang: volledige netwerktoegang
- Niet-conform: toegang weigeren



Verifiëren

Stap 1. Download en installeer de Secure Client Posture/NAM-module van ISE

Selecteer het eindpunt dat met dot1x is geverifieerd en klik op de regel "Initial Access" om toestemming te geven. Naar bewerkingen > Straal > Live logs navigeren

Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:09:31...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Specificeer op de Switch de omleiding URL en ACL die voor het eindpunt worden toegepast.

```
Switch #show verificatiesessie-interface te1/0/24
Interface: TenGigabit Ethernet1/20/24
IF-ID: 0x19262768
MAC-adres: x4x6.xxxx.xxxx
IPv6-adres: onbekend
IPv4-adres: <client-IP>
Gebruikersnaam: host/DESKTOP-xxxxxx.aaa.prad.com
Status: geautoriseerd
Gebied: DATA
Oper host-modus: single-host
Oper control dir: beide
Sessietime-out: niet beschikbaar
Gemeenschappelijke sessie-ID: 16D5C50A0000002CF067366B
Sessie-ID: 0x0000001f
Handvat: 0x7a000017
```


Huidig beleid: POLICY_TE1/0/24

Plaatselijk beleid:

Service Template: DEFAULT_LINKSEC_POLICY_should_SECURE (prioriteit 150)

Beveiligingsbeleid: moet worden beveiligd

Beveiligingsstatus: link onbeveiligd

Serverbeleid:

URL omleiden ACL: omleiden-acl

URL omleiden:

<https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee397180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2>

ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Statuslijst methode:

Status methode

dot1x Authc Success

Switch #sh interface voor gegevensbank voor apparaattracing te1/0/24

Netwerklaag Adres Link Layer Address Interface VLAN prlvl leeftijdsstatus Resterende tijd

ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 005 4min BEREIKBARE 39 s probeer 0

Controleer op het Endpoint of het verkeer is omgeleid naar ISE Posture Posture en klik op Start om de Network Setup Assistant op het Endpoint te downloaden.

Google Chrome isn't your default browser

Set as default



Client Provisioning Portal

Device Security Check

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

Start

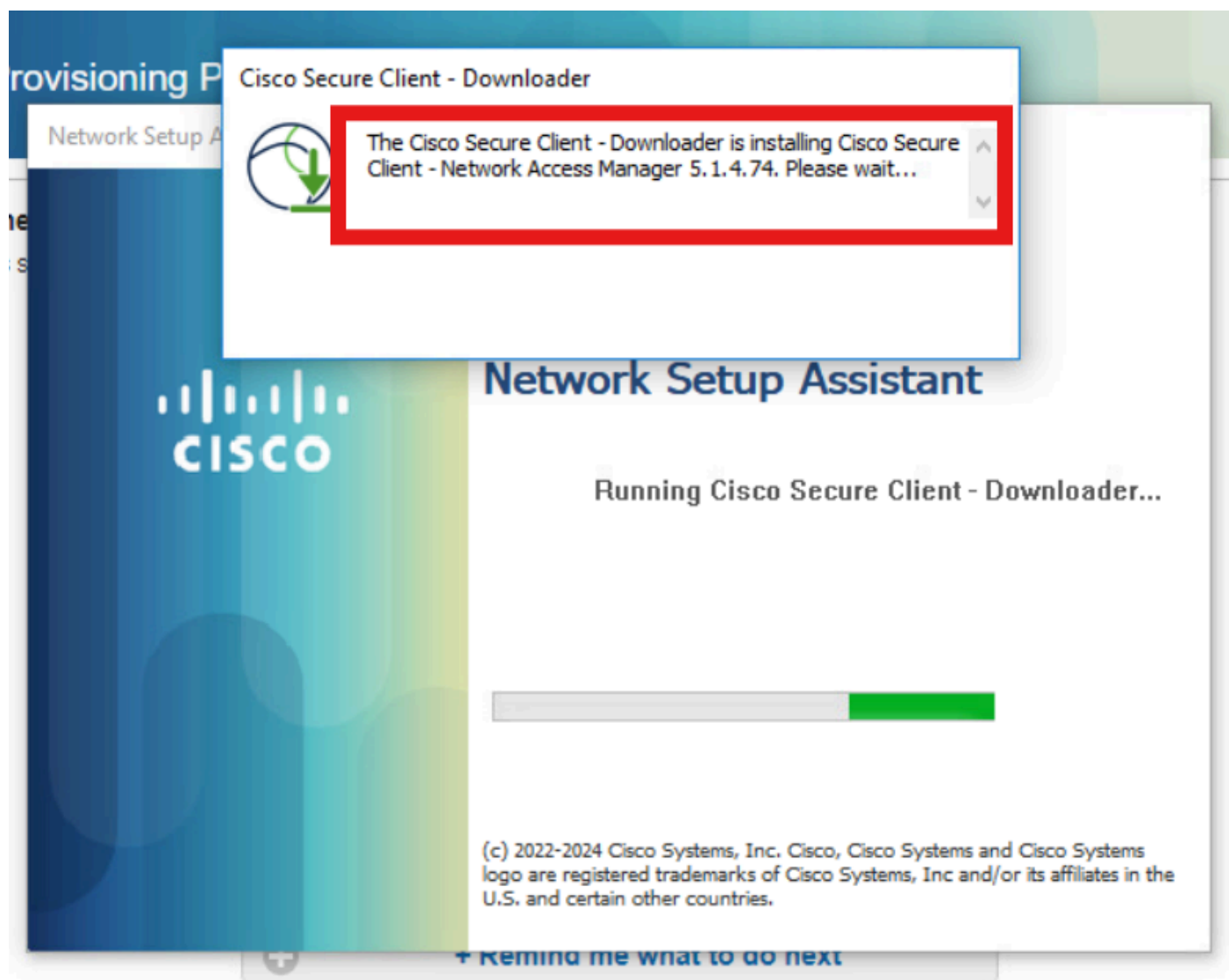
The screenshot shows the Cisco Client Provisioning Portal interface. At the top left, the logo and text "Client Provisioning Portal" are visible. Below this, a "Device Security Check" section states: "Your computer requires security software to be installed before you can connect to the network." A central message box titled "Unable to detect Posture Agent" contains the following text: "+ 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.", and "You have 4 minutes to install and for the compliance check to complete". At the bottom of this message box is a button that says "+ Remind me what to do next". In the top right corner, a "Recent download history" window is open, showing a single entry: "cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-3.aaa.prad.com_8443_WPTsDtDOR0SunsnMYB1glg.exe" with a size of "3.0 MB" and status "Done".

Klik op Uitvoeren om de NSA-toepassing te installeren.

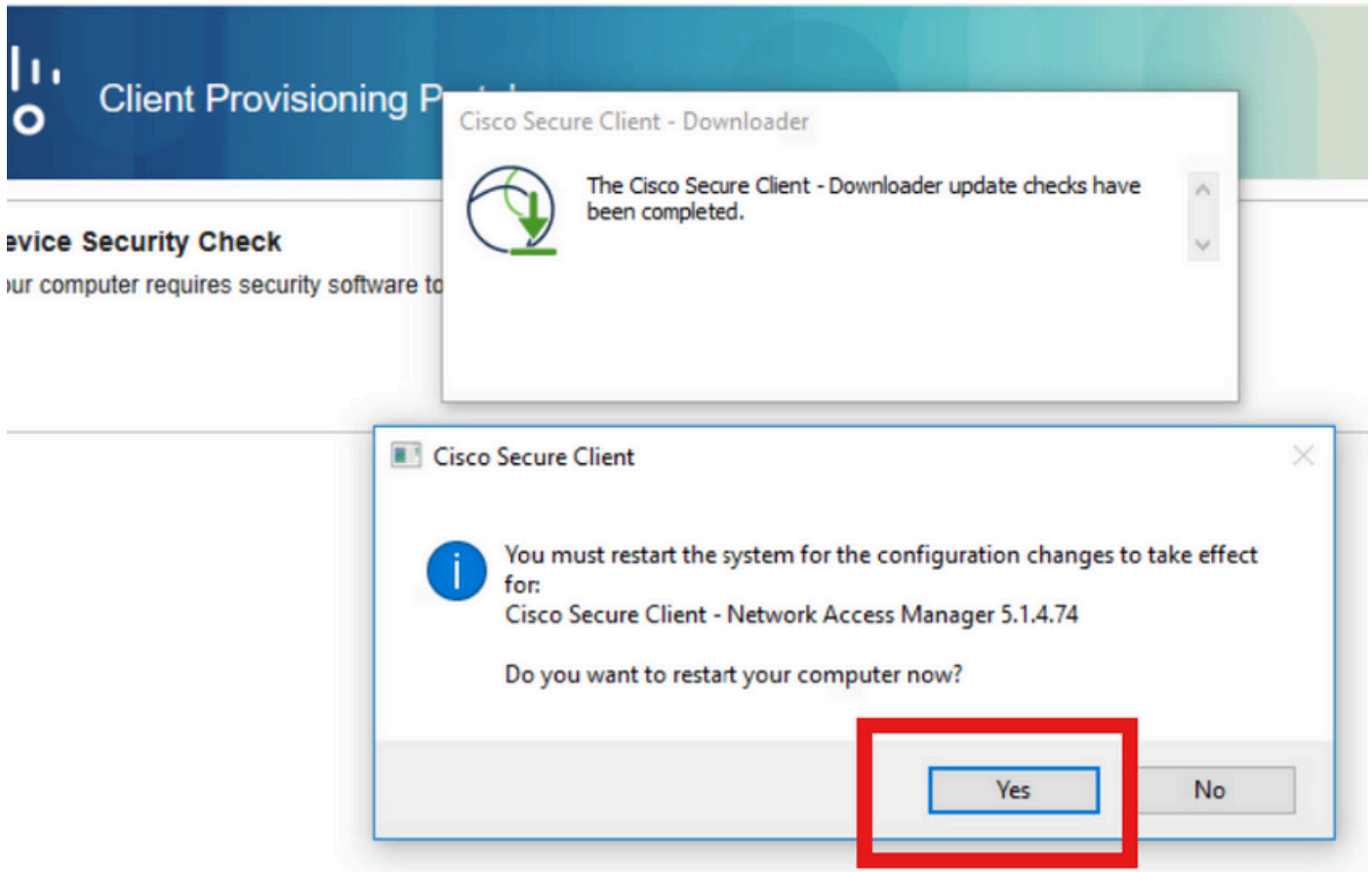
The screenshot shows a Windows SmartScreen warning dialog box overlaid on the Cisco Client Provisioning Portal. The dialog box has a blue background and white text. The title bar reads "SmartScreen can't be reached right now". The main text says: "Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run." Below this, it lists the publisher as "Cisco Systems, Inc." and the app name as "cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-...". At the bottom right, there are two buttons: "Run" and "Don't Run". The "Run" button is highlighted with a red box.

Nu, de NSA haalt de Secure Client Agent downloaden van ISE en installeert de Posture, NAM

module, en NAM Profile configuratie.xml .



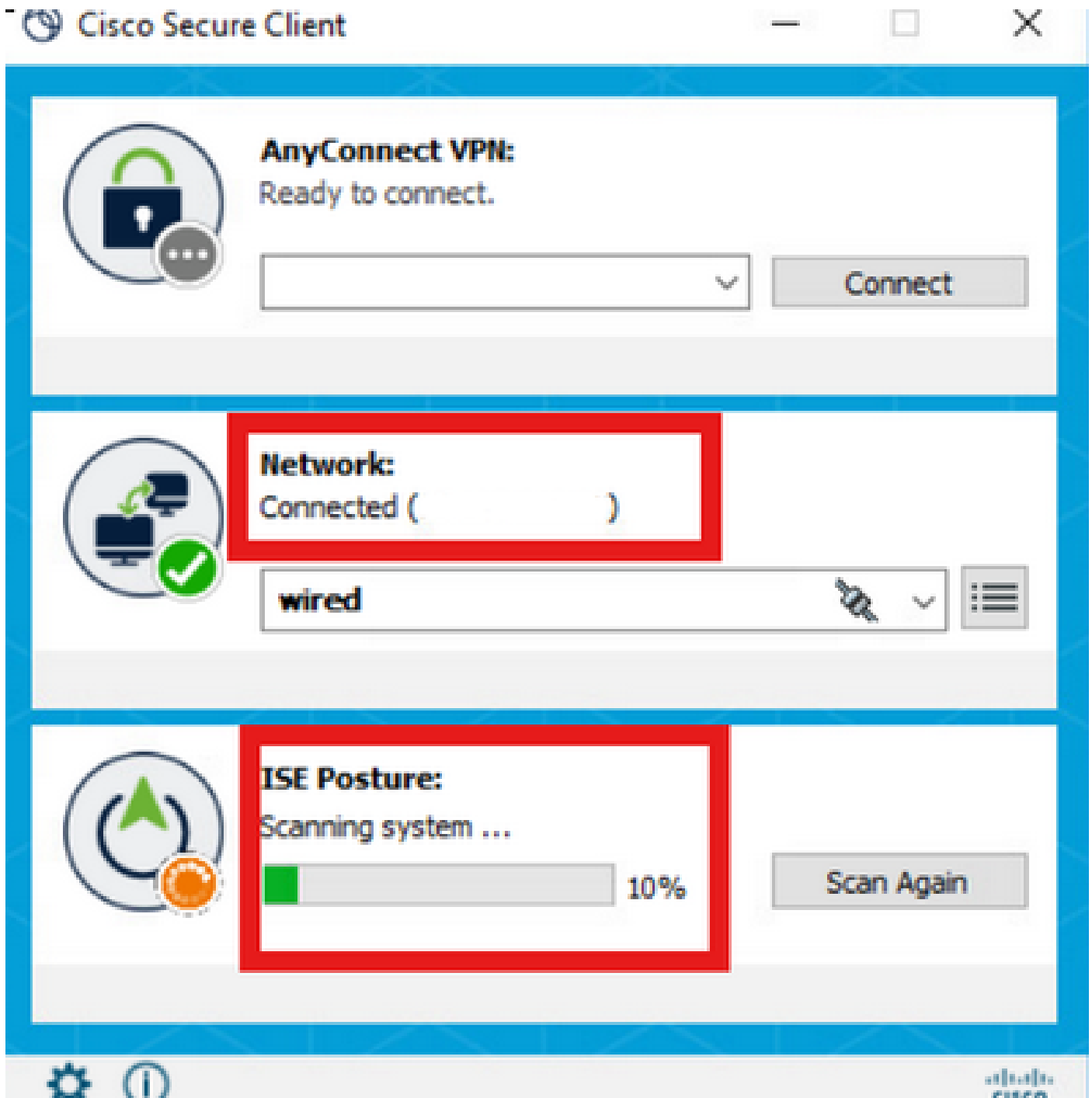
Een herstartprompt geactiveerd na de installatie van NAM. Klik op Ja.



Stap 2. EAP-FAST

Nadat de pc opnieuw is opgestart en de gebruiker is ingelogd, verifieert de NAM zowel de gebruiker als de machine via EAP-FAST.

Als het eindpunt op de juiste manier geverifieerd wordt, toont NAM aan dat het verbonden is en activeert de Posture Module de Posture Scan.



Op de Live Logs van ISE raakt het Endpoint nu de Onbekende Access Rule.

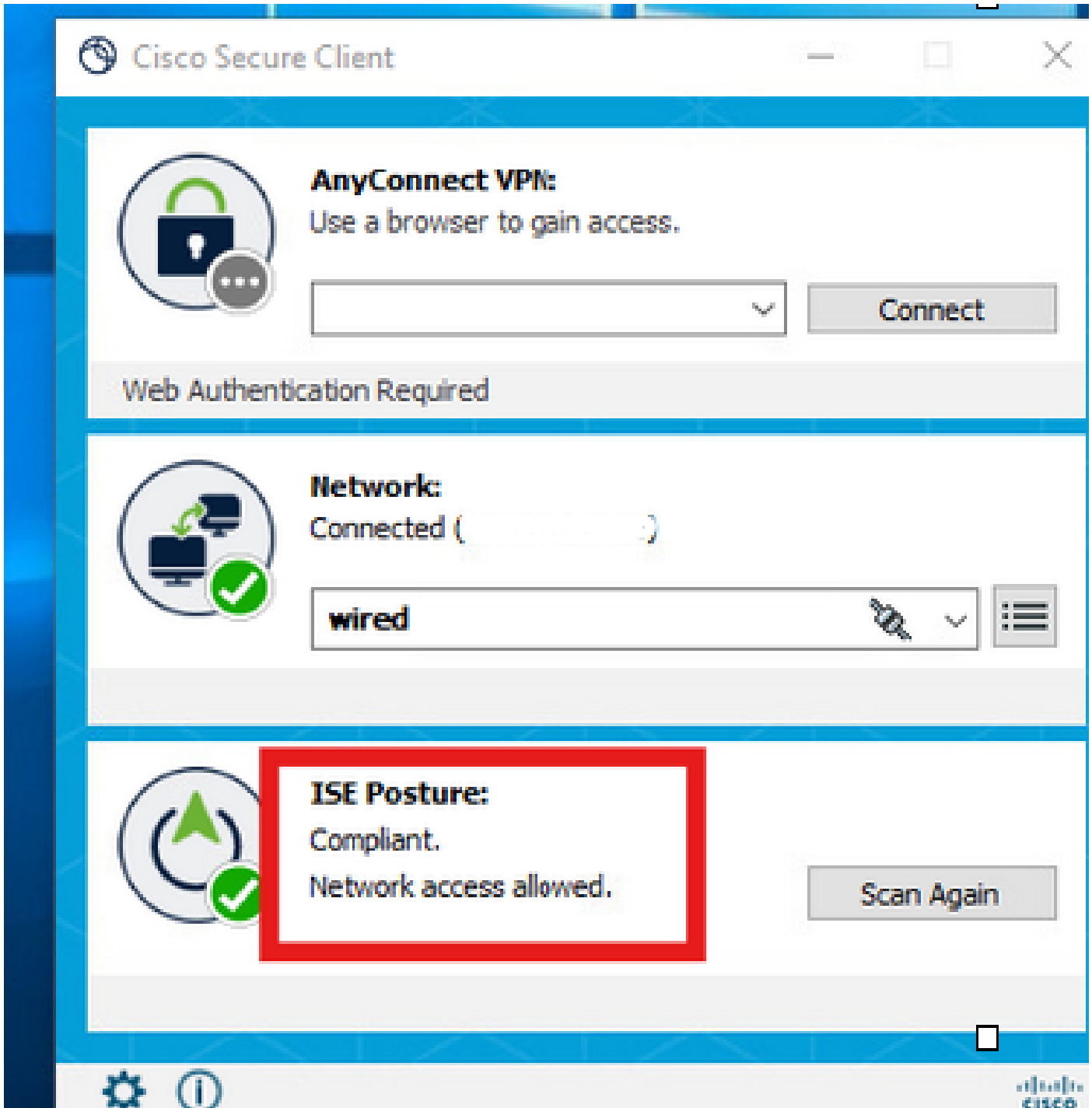
Jul 27, 2024 12:29:06...			user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...			host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Het verificatieprotocol is nu EAP-FAST op basis van de configuratie van het NAM-profiel en het EAP-ketingresultaat is "Succes".

AcsSessionID	pk3-3/511201330/230
NACRadiusUserName	user1
NACRadiusUserName	host/DESKTOP-QSCE4P3
SelectedAuthenticationIden...	PRAD
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	[REDACTED]
EapChainingResult	User and machine both succeeded
ISEPolicySetName	Dot1x Policy
IdentitySelectionMatchedRule	Default
AD-User-Resolved-Identities	user1@aaa.prad.com
AD-User-Candidate-Identities	user1@aaa.prad.com
AD-Host-Resolved-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com
AD-Host-Candidate-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com

Stap 3. Posture Scan

De Secure Client Posture Module activeert de Posture Scan en wordt gemarkeerd als Klacht op basis van het ISE Posture Policy.



De CoA wordt geactiveerd na de Posture Scan en nu raakt het Endpoint het Klachtentoegangsbeleid.

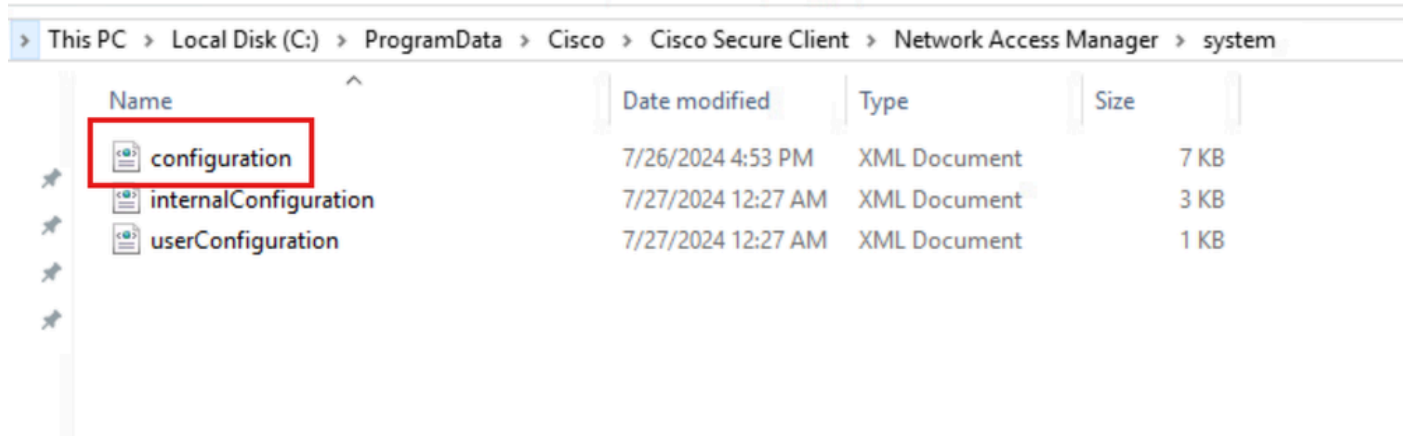
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...				user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:31...								Compliant
Jul 27, 2024 12:29:06...				user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...				host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Problemen oplossen

Stap 1. NAM Profile

Controleer of de NAM Profile configuratie.xml aanwezig is in dit pad op de PC na de installatie van de NAM module.

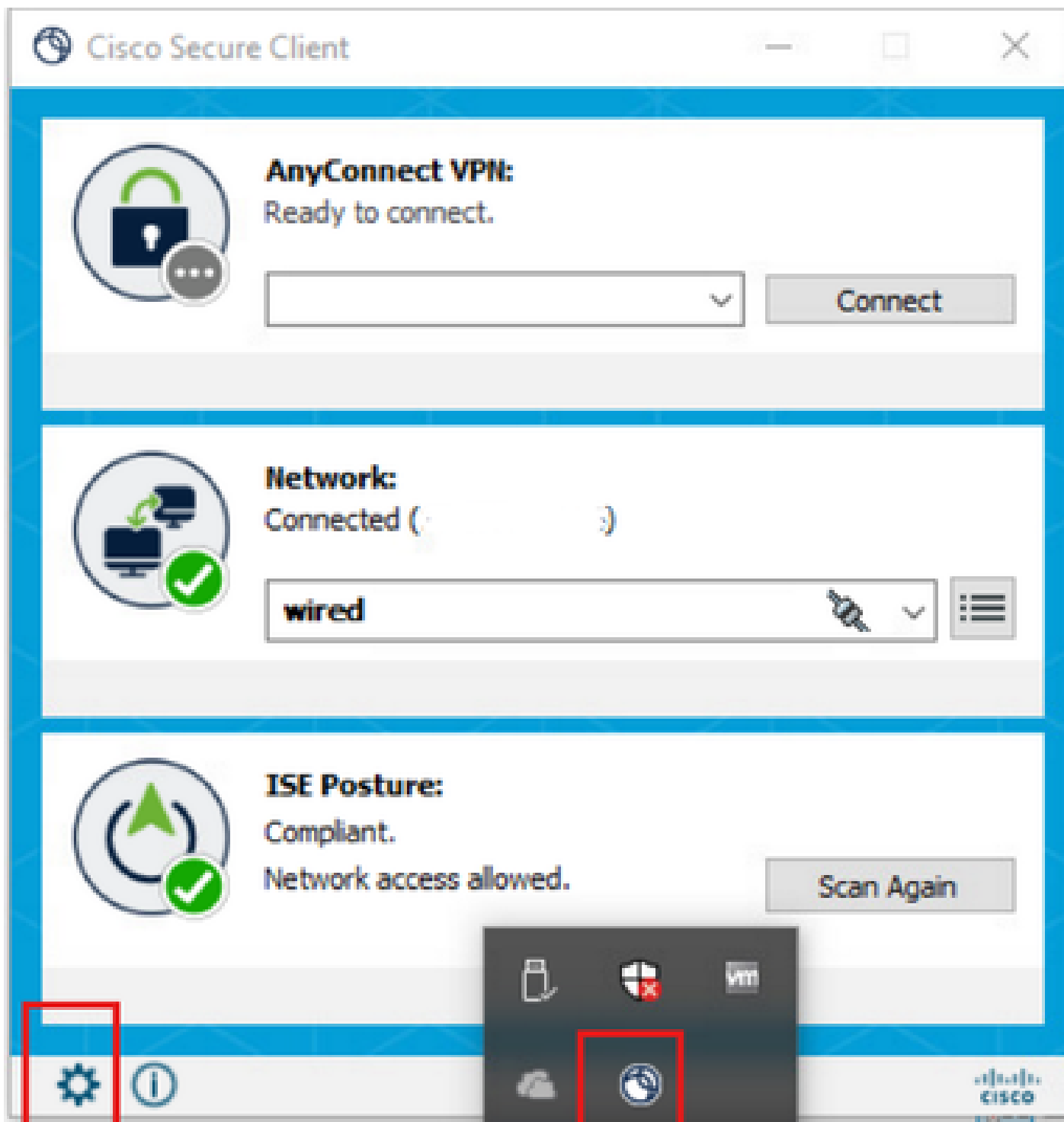
C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Name	Date modified	Type	Size
configuration	7/26/2024 4:53 PM	XML Document	7 KB
internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB
userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB

Stap 2. Uitgebreide NAM-vastlegging

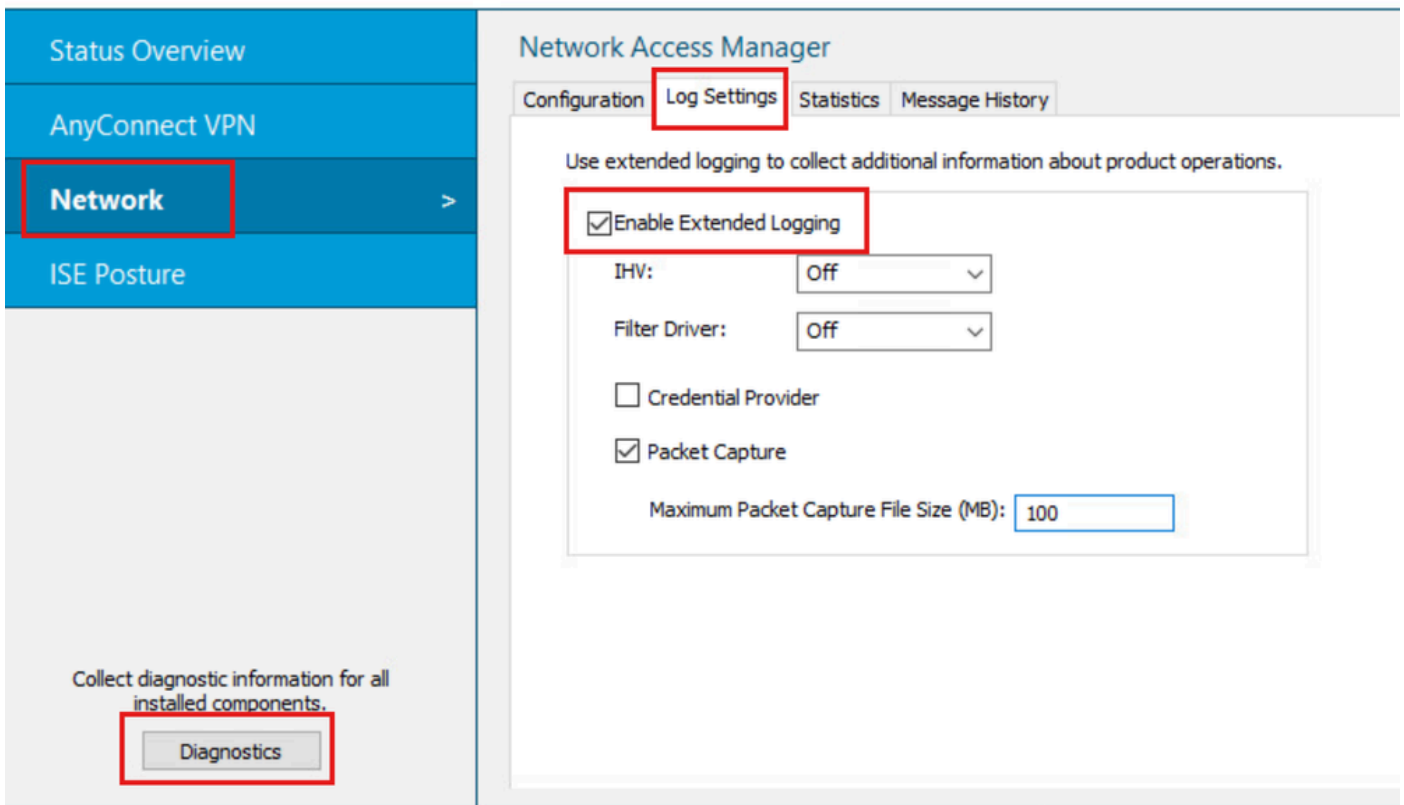
Klik op het pictogram Secure Client (Beveiligde client) op de taakbalk en selecteer het pictogram "Instellingen".



Navigeer naar het tabblad Network > Log Settings. Schakel het selectievakje Uitgebreid vastlegging inschakelen in.

Stel de grootte van het pakketopnamebestand in op 100 MB.

Na het reproduceren van het probleem, klik op Diagnostics om de bundel DART op het Endpoint te creëren.



De sectie Berichtgeschiedenis toont de details van elke stap die NAM heeft uitgevoerd.

Stap 3. Debugs op Switch

Laat deze debugs op de switch toe om dot1x en omleidingsstroom problemen op te lossen.

```
debug ip http all
```

```
debug ip http transacties
```

```
debug ip http URL
```

```
set platform software trace smd switch actief R0 aaa debug
```

```
set platform software trace smd switch actief R0 dot1x-all debug
```

```
set platform software trace smd switch actief R0 radius debug
```

```
set platform software trace smd switch actief R0 auth-mgr-all debug
```

```
set platform software trace smd switch actief R0 eap-all debug
```

```
set platform software trace smd switch actief R0 epm-all debug
```

```
set platform software trace smd switch actief R0 epm-redirect debug
```

```
set platform software trace smd switch actief R0 webauth-aaa debug
```

```
set platform software trace smd switch actief R0 webauth-httpd debug
```

De logbestanden weergeven

logboekregistratie tonen

toon registratieproces interne smd

Stap 4. Debugs op ISE

Verzamel de ISE-ondersteuningsbundel met deze kenmerken die op debugniveau moeten worden ingesteld:

- houding
- deuropening
- bevoorrading
- runtime-AAA
- nsf
- NSF-sessie
- zwitser
- clientwebapp

Gerelateerde informatie

[Secure-clientnaam configureren](#)

[ISE-implementatiegids voor postimplementaties](#)

[Probleemoplossing DotX op Catalyst 9000 Series Switches](#)

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.