Posture Agentless configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Posture Agentless in ISE kunt configureren en wat er nodig is in het eindpunt om het Agent-less script uit te voeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE).
- Houding.
- PowerShell en SSH
- Windows 10 of hoger.

Gebruikte componenten

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

- Identity Services Engine (ISE) 3.3 versie.
- Pakket Cisco Agentless Windows 5.1.6.6
- Windows 10

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

ISE Posture voert een klantbeoordeling uit. De klant ontvangt het postuur vereiste beleid van ISE, voert de postuur gegevensverzameling uit, vergelijkt de resultaten met het beleid en stuurt de beoordelingsresultaten terug naar de ISE.

ISE bepaalt vervolgens of het apparaat een klacht is of niet-conform op basis van Posture Report.

Agent less postuur is een van postuur methoden die postuur informatie van klanten verzamelen en automatisch zelf verwijdert na voltooiing zonder enige actie van de eindgebruiker te vereisen. Positie zonder agents maakt verbinding met de client met behulp van beheerrechten.

Aan de slag

Voorwaarden:

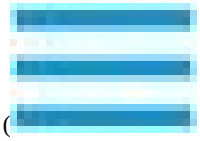
- De client moet bereikbaar zijn via zijn IPv4- of IPv6-adres en dat IP-adres moet in RADIUS-accounting beschikbaar zijn.
- De client moet via zijn IPv4- of IPv6-adres bereikbaar zijn via Cisco Identity Services Engine (ISE). Bovendien moet dit IP-adres in RADIUS-accounting beschikbaar zijn.

- Windows- en Mac-clients worden momenteel ondersteund:
    - Voor Windows-clients moet poort 5985 voor toegang tot powershell op de client geopend zijn. PowerShell moet v7.1 of hoger zijn. De client moet cURL v7.34 of hoger hebben.
    - Voor MacOS-clients moet poort 22 voor toegang tot SSH open zijn voor toegang tot de client. De client moet cURL v7.34 of hoger hebben.
- Clientreferenties voor shell-aanmelding moeten lokale beheerdersrechten hebben.
- Draai de postuur update om de laatste clients te krijgen, zoals beschreven in de configuratie stappen. Controleer:
- Voor MacOS, zorg ervoor dat dit item wordt bijgewerkt in het sudoers bestand om te voorkomen dat certificaat installatie fout op de eindpunten:

<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

•

Voor MacOS moet de gebruikersaccount die is geconfigureerd een beheerdersaccount zijn. De postuur van Agent voor MacOS werkt



niet met een ander accounttype, zelfs als u meer rechten verleent.Om dit venster te bekijken, klikt u op de menuicon ( ) en **kiest u Beheer > Systeem > Instellingen > Endpoint Scripts** > Login **Configuration > MAC Local User.**

•

In het geval van wijzigingen in poortgerelateerde activiteiten in Windows-clients als gevolg van updates van Microsoft, moet u de poortconfiguratie-workflow zonder agents voor Windows-clients opnieuw configureren.

Ondersteunde houdingsvoorwaarden

•

Bestandsvoorwaarden, behalve de voorwaarden die de USER_DESKTOP en USER_PROFILE bestandspaden gebruiken

•

Servicevoorwaarden, behalve controles van System Daemon en Daemon of User Agent op macOS

•

Toepassingsvoorwaarden

- Externe gegevensbronomstandigheden
- Samengestelde condities
- Voorwaarden tegen malware
- Voorwaarde voor patchbeheer, behalve **de** controles **Enabled andUp To** DataCondition
- Firewallomstandigheden
- De voorwaarden van de schijfcodering, behalve de op encryptie gebaseerde controle van de voorwaarde
- Registervoorwaarden, behalve de voorwaarden die HCSK als wortelsleutel gebruiken

Niet-ondersteunde houdingsvoorwaarden

- Oplossing
- respijtperiode
-

Periodieke herbeoordeling

-

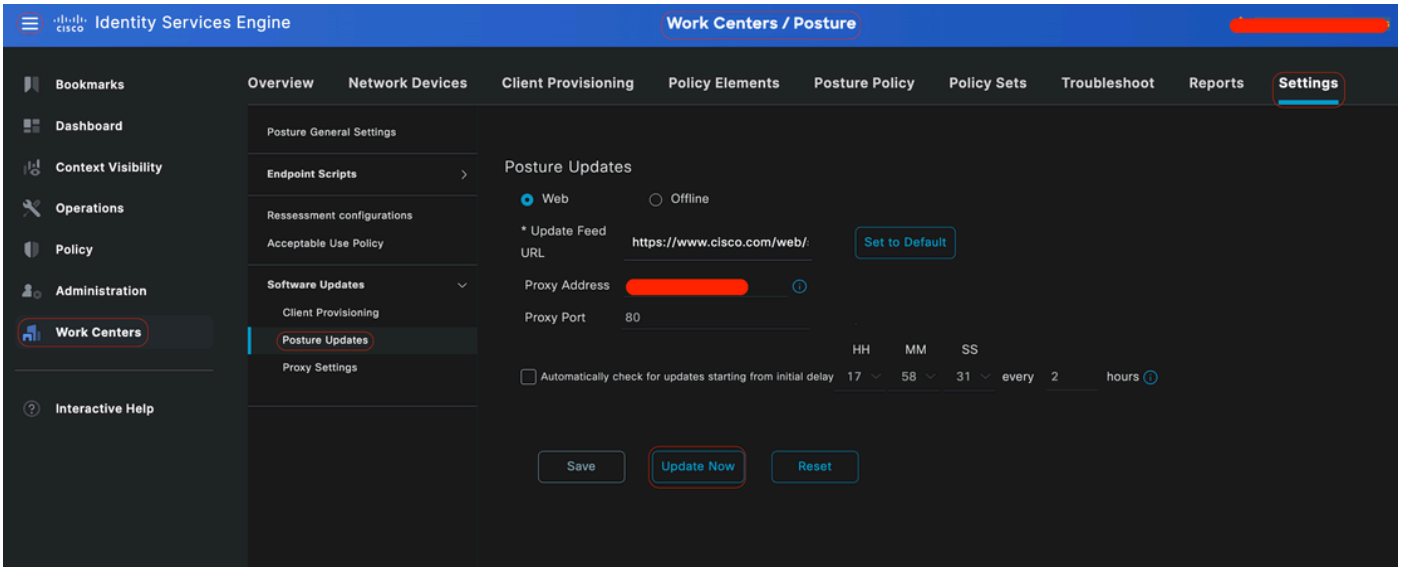
Aanvaardbaar gebruiksbeleid

Configureren ISE

Standaardinvoer bijwerken

Het is aan te raden om Posture Feed bij te werken voordat u begint met het configureren van Posture.

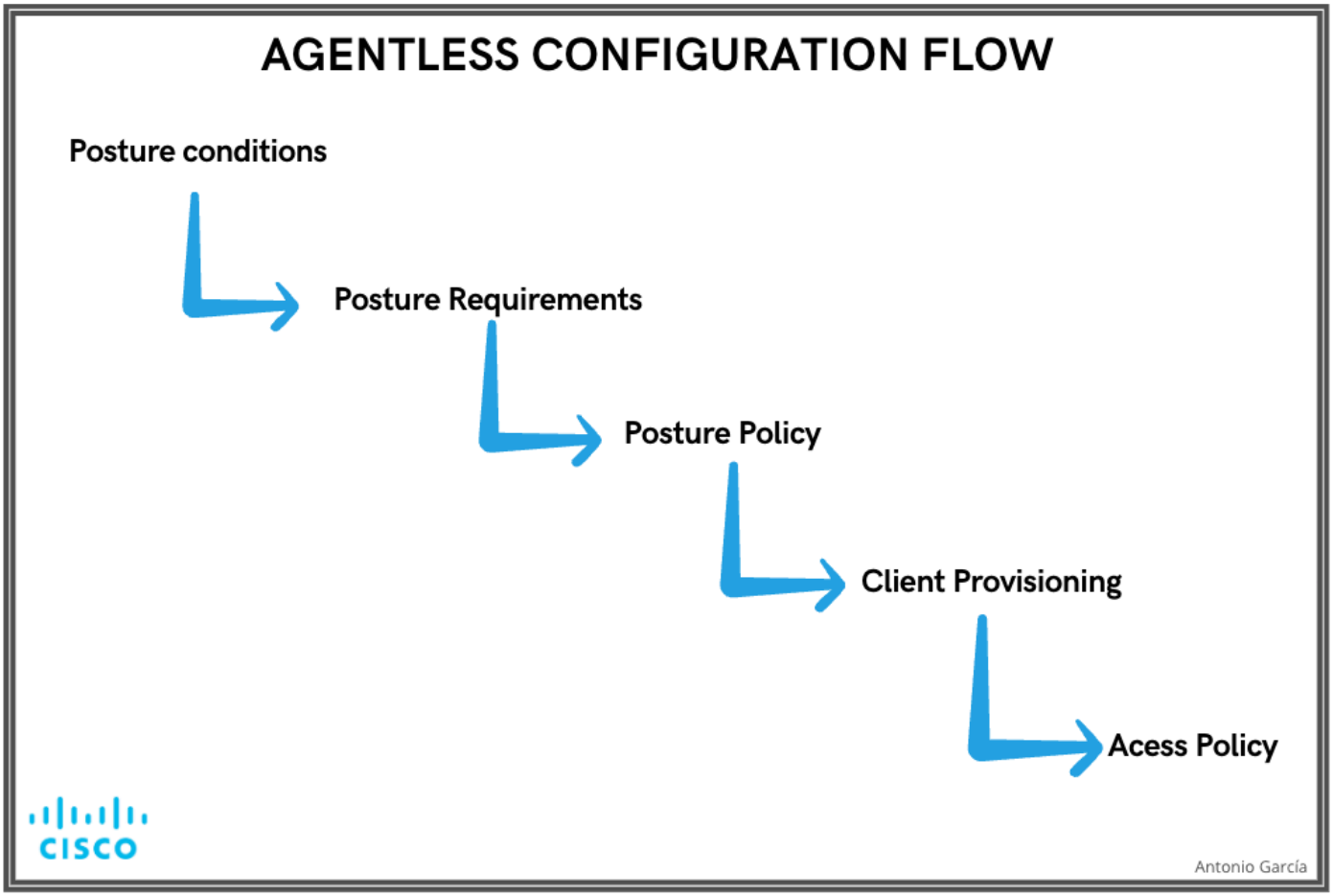
In de Cisco ISE GUI, klik op het pictogram Menuicon ( ) en kies **Work Centers > Positie > Instellingen** > **Software-updates** > **Nu bijwerken**.



Posture Feed bijwerken

Configuratie zonder posterijen

Posture Agentless moet worden geconfigureerd in volgorde als de eerste configuratie zal worden vereist voor de volgende en zo verder. Merk op dat Remediation niet in de flow is; echter, later gaat dit document een alternatief voor het configureren van Remediation dekken.



Config-stroom zonder agents

Stature-configuratie zonder agents

Houdbaarheid

Postervoorwaarden zijn de set regels in ons beveiligingsbeleid die een compatibel eindpunt definiëren. Enkele van deze items omvatten de installatie van een firewall, anti-virus software, anti-malware, hotfixes, schijfcodering en meer.

In de Cisco ISE GUI, klik op de menuicon (

) en kies **Workcenters > Positie > Beleidselementen** > Voorwaarden, klik op Add, en creëer een of meer posteringsvoorwaarden die Agent less postuur gebruiken om het vereiste te identificeren. Klik op **Opslaan** als de **voorwaarde** is gemaakt.

In dit scenario werd een Toepassingsvoorwaarde met de naam **"Agentless_Condition_Application"** geconfigureerd met deze parameters:

· **Besturingssysteem:** Windows All

Deze voorwaarde is van toepassing op elke versie van het Windows-besturingssysteem en zorgt voor een brede compatibiliteit in verschillende Windows-omgevingen.

· **Controleer op:** Proces

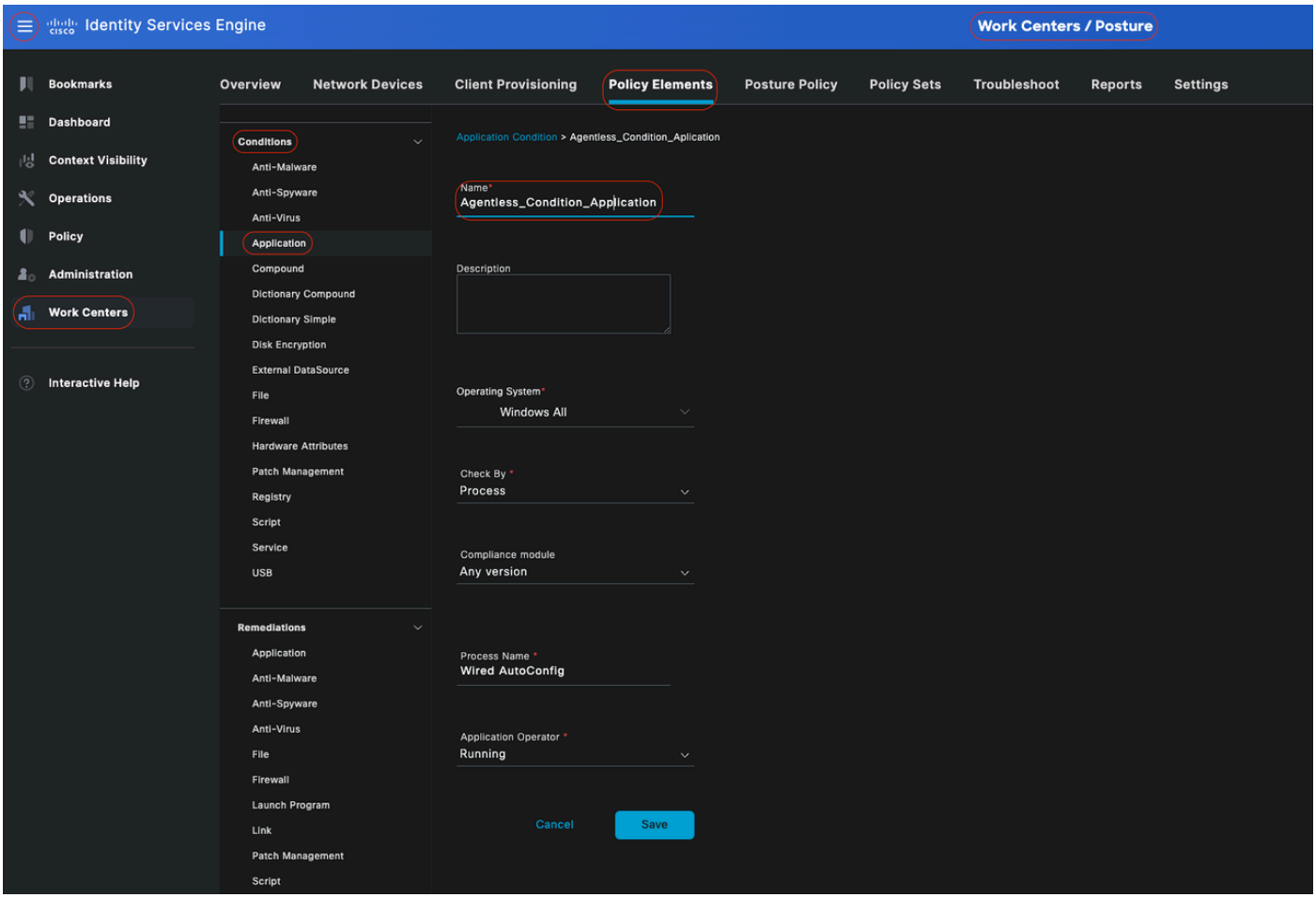
Het systeem controleert processen binnen het apparaat. U hebt de optie om **Proces** of **Toepassing** te selecteren; in dit geval, werd gekozen voor **Proces**.

· **Procesnaam:** bekabeld AutoConfig

Het **bekabelde AutoConfig-**proces bestaat uit de procesconforme module die het apparaat zal controleren. Dit proces is verantwoordelijk voor het configureren en beheren van bekabelde netwerkverbindingen, inclusief IEEE 802.1X-verificatie.

· **Toepassingsbeheerder:** actief

De compliancemodule verifieert of het **bekabelde AutoConfig-**proces op het apparaat momenteel wordt uitgevoerd. U kunt kiezen tussen **actief** of **niet actief**. In dit geval is de optie **Uitvoeren** geselecteerd om ervoor te zorgen dat het proces actief is.



Statusloze toestand

Positie-eis

Een postuur-eis is een reeks samengestelde voorwaarden of slechts één voorwaarde die kan worden gekoppeld aan een rol en een besturingssysteem. Alle clients die verbinding maken met uw netwerk moeten voldoen aan de verplichte eisen tijdens de postuur evaluatie om compatibel te worden op het netwerk.

In de Cisco ISE GUI, klik op het menupictogram ( ) en kies **Workcentres > Positie** > **Policy Elements** > **Requirement**. Klik op de **pijl-omlaag** en selecteer **Nieuwe eis invoegen**, en maak een of meer **PostureRequirement** die Agent-loze houding gebruiken. Klik op **Gereed** en vervolgens op **Opslaan** als de **vereiste** is gemaakt.

In dit geval werd een Application Requirement genaamd **"Agentless_Requirement_Application"** geconfigureerd met deze criteria:

· **Besturingssysteem:** Windows All

Deze vereiste is van toepassing op elke versie van het Windows-besturingssysteem en zorgt ervoor dat deze van toepassing is op alle Windows-omgevingen.

· **Positie Type:** Agentless

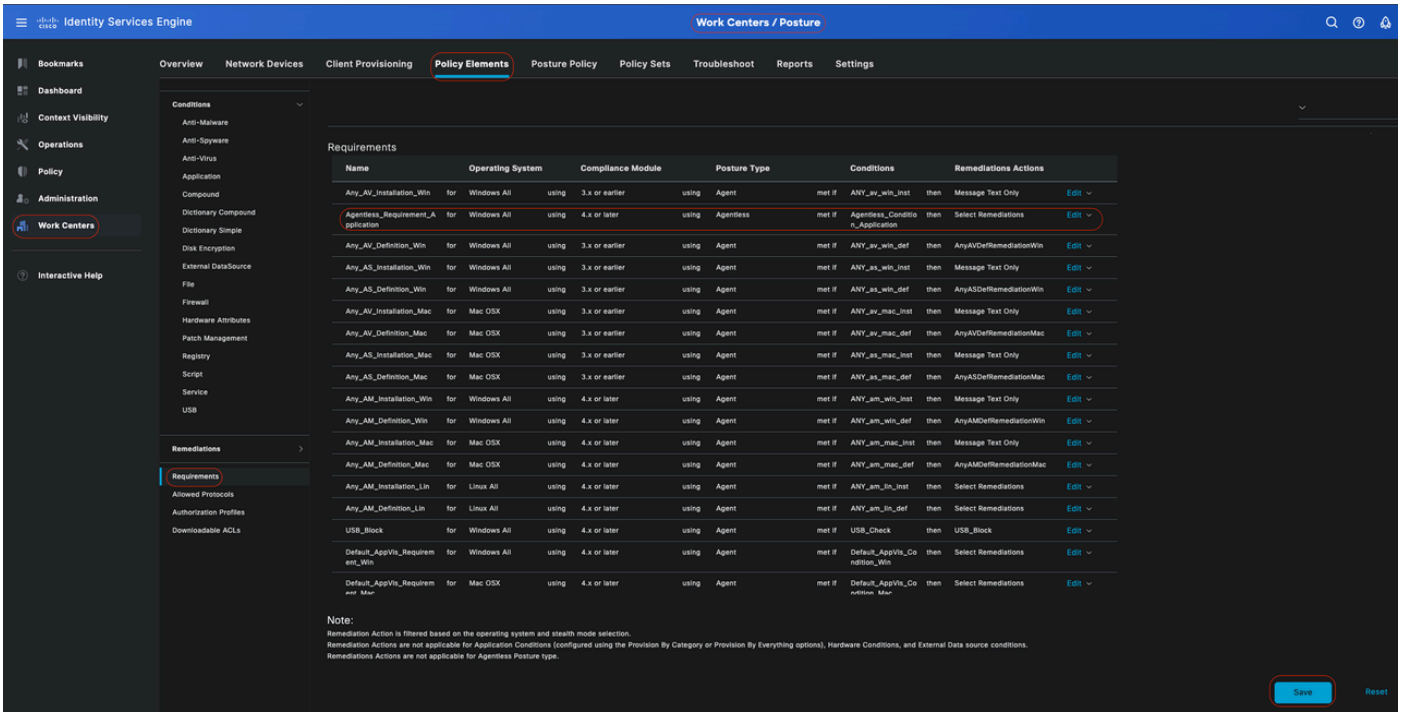
Deze configuratie is ingesteld voor een Agent-loze omgeving. Beschikbare opties zijn **Agent**, **Agent Stealth**, **Temporal Agent** en **Agent less**. In dit scenario werd **Agentless** geselecteerd.

· **Voorwaarden: Agent_Condition_Application**

Dit specificeert de voorwaarde dat de module van de Positie van ISE en de module van de Naleving binnen de processen van het apparaat zullen controleren. De geselecteerde voorwaarde is **Agentless_Condition_Application**.

· **Herstelmaatregelen:**

Aangezien deze configuratie bedoeld is voor een Agent-omgeving, worden Remediation Actions niet ondersteund en wordt dit veld grijs gemaakt.



Vereiste zonder agents

posterisatiebeleid

In de Cisco ISE GUI, klik op het pictogram Menuicon (

) en **kies Werkcentra** > **Houding** > **Houdbaarheid Beleid.** Klik op de **pijl-omlaag** en selecteer **Nieuwe eis invoegen**, en maak een of meer ondersteunde regels voor **het Posture Policy die Agent-less houding gebruiken voor die Posture Requirement.** Klik op **Gereed** en vervolgens op **Opslaan** als het **Posture Policy** is gemaakt.

In dit scenario is een Posture Policy met de naam **"Agentless_Policy_Application"** geconfigureerd met deze parameters:

· **Regel naam:** Agent_Policy_Application

Dit is de aangewezen naam voor het Posture Policy in dit configuratievoorbeeld.

· **Besturingssysteem:** Windows All

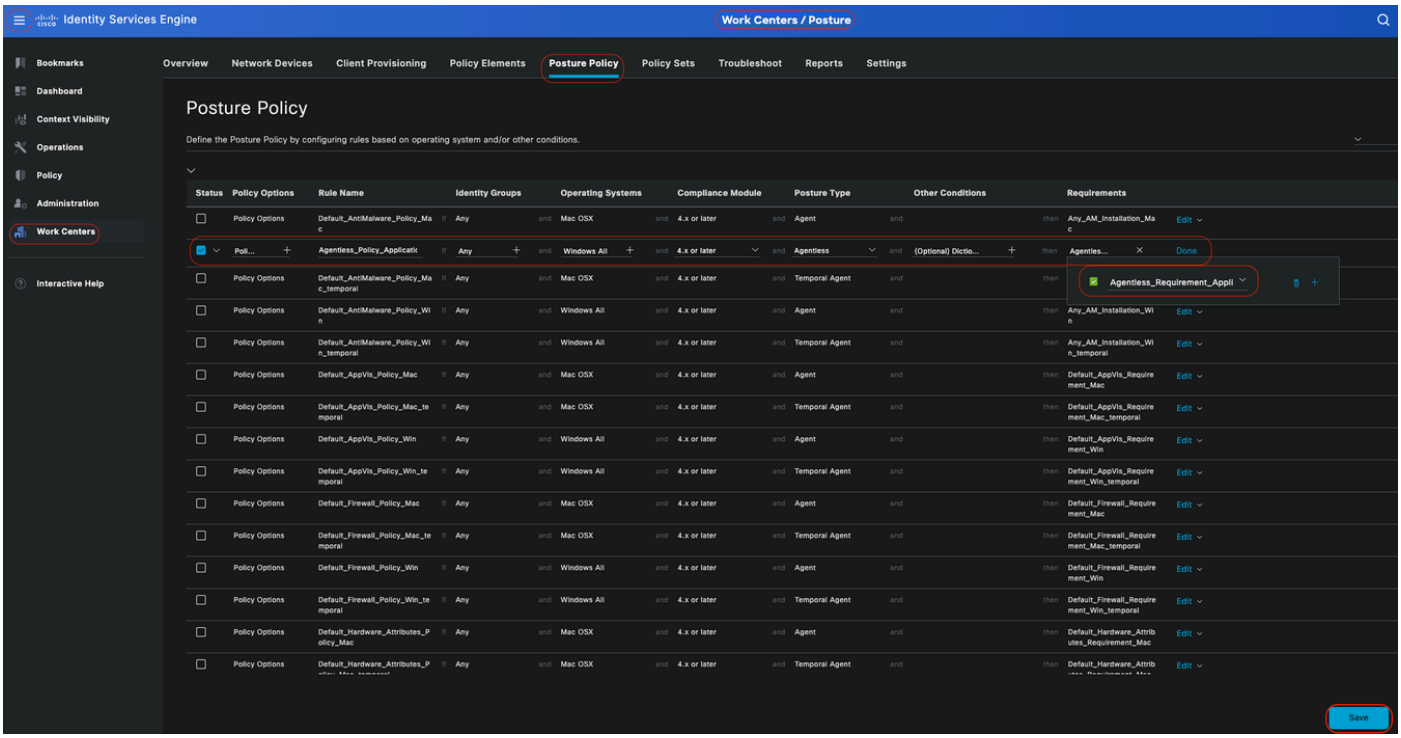
Het beleid is ingesteld om van toepassing te zijn op alle versies van het Windows-besturingssysteem, waardoor brede compatibiliteit in verschillende Windows-omgevingen wordt gegarandeerd.

· **Positie Type:** Agentless

Deze configuratie is ingesteld voor een Agent-loze omgeving. Beschikbare opties zijn **Agent**, **Agent Stealth**, **Temporal Agent** en **Agent less**. In dit scenario is **Agentless** geselecteerd.

· **Andere aandoeningen:**

In dit configuratievoorbeeld zijn geen extra voorwaarden gecreëerd. U hebt echter de optie om specifieke voorwaarden te configureren om ervoor te zorgen dat alleen gerichte apparaten onder dit Posture Policy vallen, in plaats van alle Windows-apparaten op het netwerk. Dit kan met name nuttig zijn voor netwerksegmentatie.



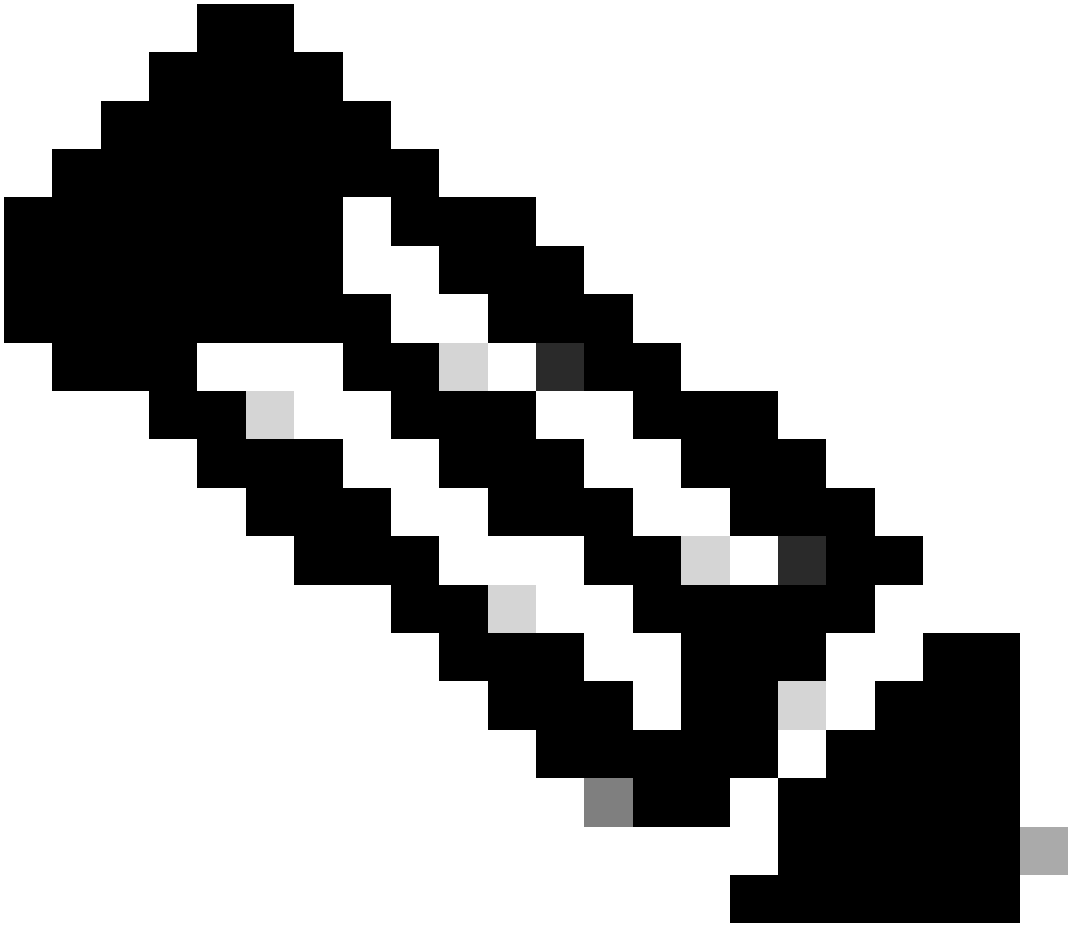
Positie Agentless Policy

Clientprovisioning

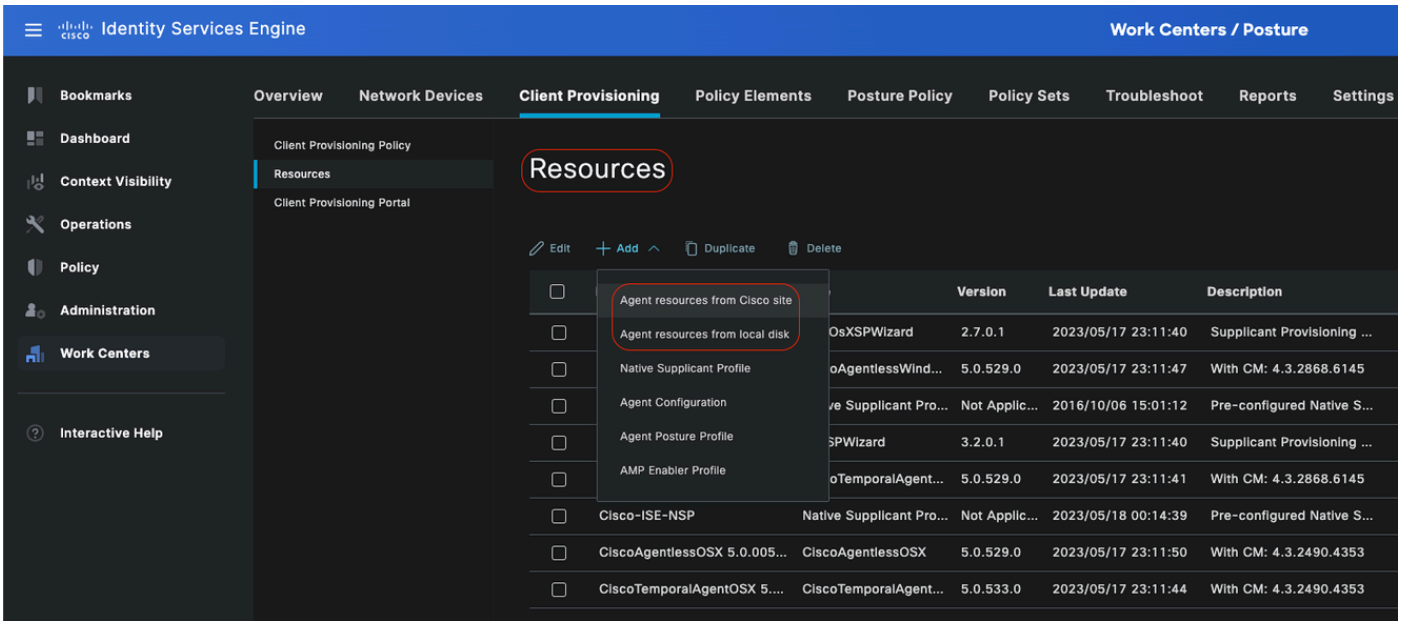
Stap 1 - Downloadresources

Als u wilt beginnen met het configureren van clientprovisioning, moet u eerst de vereiste bronnen downloaden en deze beschikbaar hebben in ISE, zodat u deze later kunt gebruiken in het clientprovisioningbeleid.

Er zijn twee manieren om resources aan ISE toe te voegen, namelijk **Agent Resources van Cisco site** en **Agent Resources van Local disk**. Aangezien u Agentless vormt, moet u door de **Middelen van de Agent van de plaats van Cisco** gaan om te downloaden.



Opmerking: om deze **Agent-bronnen van Cisco-site** te gebruiken, heeft ISE PAN internettoegang nodig.



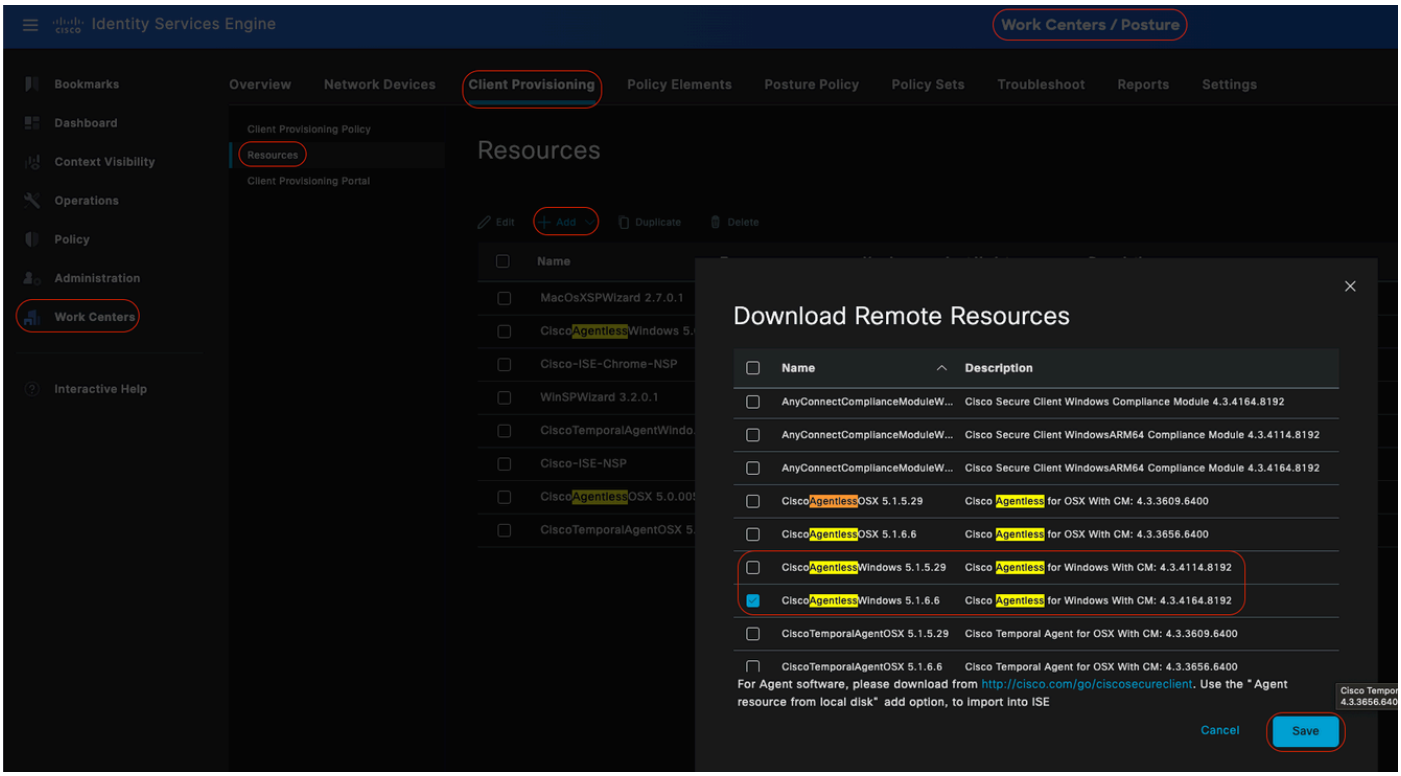
Bronnen

Agent-bronnen vanaf Cisco-site

In de Cisco ISE GUI, klik op het pictogram Menuicon ( ) en kies **Workcenters** > **Houding** > **Client Provisioning** > **Resources**. Klik op **Add** (**Toevoegen)**, selecteer **Agent Resources (Middelen) op Cisco-site**, klik op **Save**.

Van de plaats van Cisco, kunt u slechts de Module van de Naleving downloaden. Systeem toont de twee meest recente Compliance Modules om te downloaden. Resourcepakket **CiscoAgentlessWindows 5.1.6.6** is geselecteerd voor dit configuratievoorbeeld. Dit is alleen bedoeld voor Windows-apparaten.

1.



Agent-bronnen vanaf Cisco-site

Stap 2 - Clientprovisioningbeleid configureren

Bij het configureren van Posture Agent hebt u twee verschillende bronnen nodig (**AnyConnect** of **Secure Client** en **Compliance Module**),

Stel beide bronnen in onder **Agent Configuration** samen met het **Agent Posture Profile** zodat u deze **Agent Configuration** in uw **Client Provisioning Policy** kunt gebruiken**.**

Bij het configureren van Posture Agentless is het echter niet nodig om **Agent Configuration** of **Agent Posture Profile** te configureren, in plaats daarvan downloadt u alleen het agentless-pakket van **Agent Resources van Cisco-site**.

In de Cisco ISE GUI, klik op het pictogram Menuicon ( ) en kies **Workcenters** > **Houding** > **Client Provisioning** > **Clientprovisioningbeleid**. Klik op **pijl**-omlaag en selecteer **Nieuwe beleid invoegen** of **Nieuwe beleid invoegen**, **hierboven** of **hieronder dupliceren:**

- **Regel Naam: Agent_Client_Provisioning_Policy**

Hiermee geeft u de naam van het clientprovisioningbeleid op.

- **Besturingssysteem:** Windows All

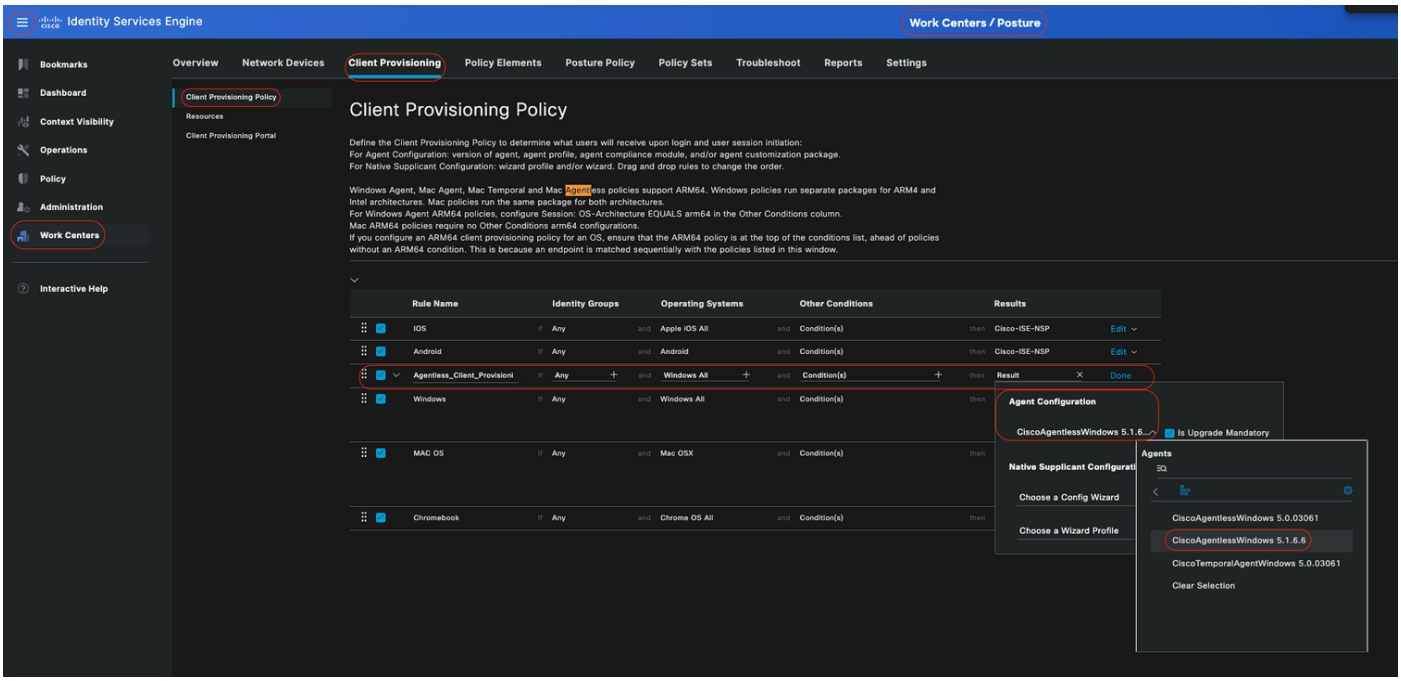
Dit zorgt ervoor dat het beleid van toepassing is op alle versies van het Windows-besturingssysteem.

- **Andere Voorwaarden:** In dit voorbeeld zijn geen specifieke voorwaarden ingesteld. U kunt echter wel voorwaarden configureren om ervoor te zorgen dat alleen de gewenste apparaten overeenkomen met dit beleid voor clientprovisioning, in plaats van met alle Windows-apparaten in het netwerk. Dit is met name nuttig voor netwerksegmentatie.

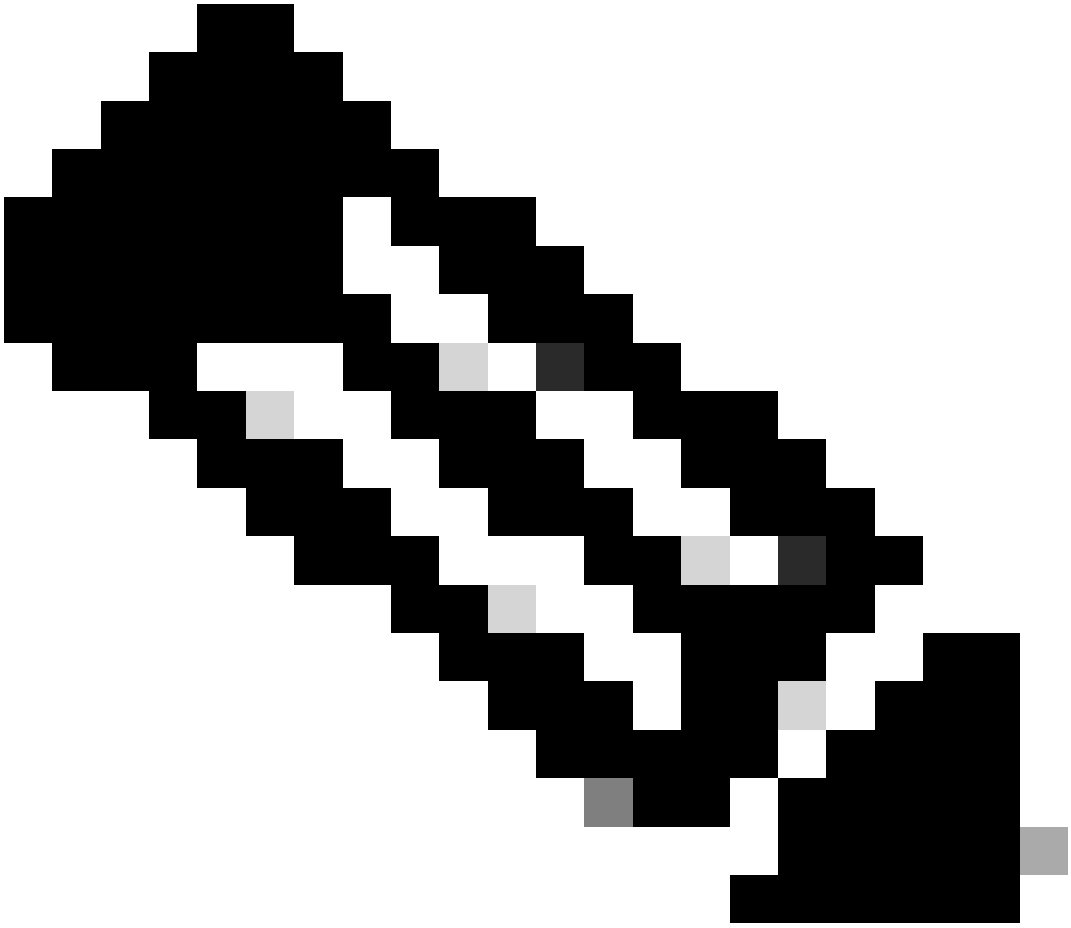
Voorbeeld: Als u Active Directory gebruikt, kunt u Active Directory-groepen in uw beleid opnemen om te verfijnen welke apparaten worden beïnvloed.

- **Resultaten:** Selecteer het juiste pakket of de juiste configurator. Aangezien u voor een agentless omgeving configureert, kies het pakket **CiscoAgentWindows 5.1.6.6**, dat u eerder van de **Agent Resources van de Cisco-site** hebt gedownload. Dit agentless-pakket bevat alle benodigde bronnen (**Agent-less Software** en **Compliance Module**) die nodig zijn om Posture Agent-less te kunnen gebruiken.

•Klik op Opslaan



Clientprovisioningbeleid zonder agents



Opmerking: zorg ervoor dat slechts één clientprovisioningbeleid voldoet aan de voorwaarden voor een bepaalde verificatiepoging. Als meervoudig beleid tegelijkertijd wordt geëvalueerd, kan dit leiden tot onverwacht gedrag en potentiële conflicten.

Autorisatieprofiel **zonder agent**

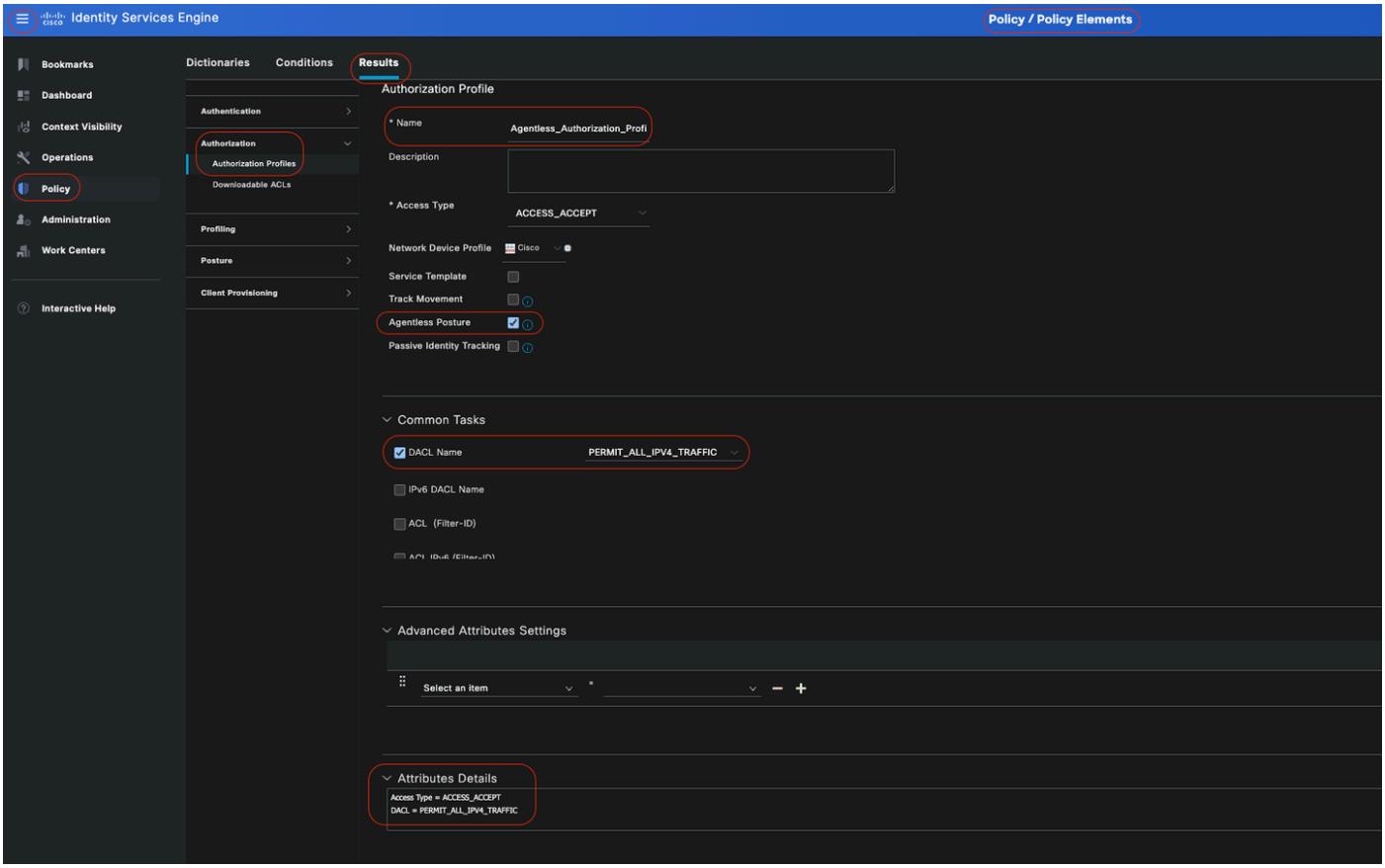
In de Cisco ISE GUI, klik op het menupictogram (

) en kies Beleid > Beleidselementen **> Resultaten > autorisatie > autorisatieprofielen en maak een autorisatieprofiel aan** dat de resultaten van de statuur zonder agents evalueert.

- In dit configuratievoorbeeld, genoemd Autorisatieprofiel als **Agentless_Authorisation_Profile**.
- Positie zonder agents inschakelen in het autorisatieprofiel.
- Gebruik dit profiel alleen voor **Agent Positie**. Gebruik dit niet ook voor andere postuur types.
- CWA en Redirect ACL is niet vereist voor agentless houding. U kunt VLAN’s, DACL’s of ACL’s gebruiken als deel van uw segmentatieregels. Om het simpel te houden, wordt naast de Agent Postal Check in dit configuratievoorbeeld alleen een dACL (die al ipv4 verkeer toestaat) geconfigureerd.

-

Klik op **Opslaan**.



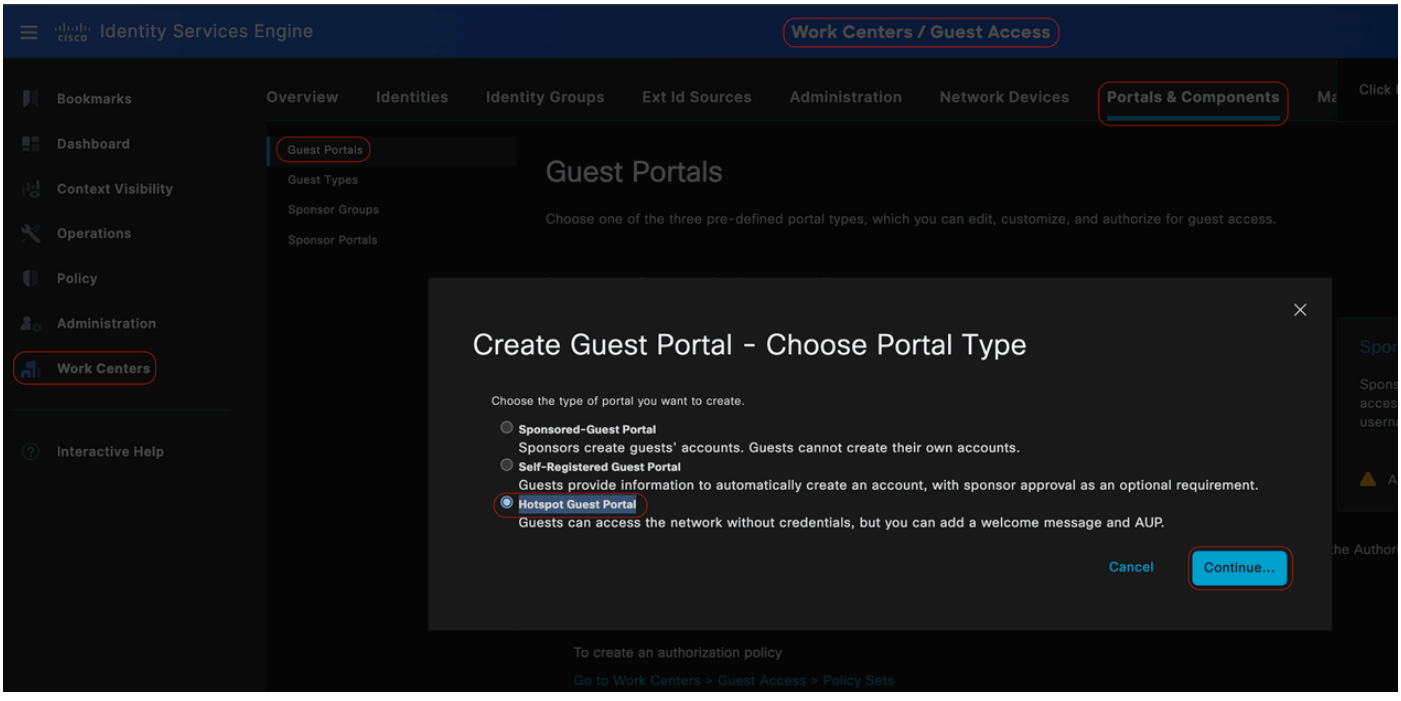
Autorisatieprofiel zonder agent

Alternatief voor het gebruik van probleemoplossing (optioneel)

Ondersteuning voor herstel in de stroom zonder agents is niet beschikbaar. Om dit aan te pakken, kunt u een aangepast hotspotportaal implementeren om gebruikersbewustzijn te verbeteren met betrekking tot endpointnaleving. Wanneer een eindpunt als niet-conform wordt geïdentificeerd, kunnen gebruikers naar dit portal worden doorgestuurd. Deze benadering zorgt ervoor dat gebruikers worden geïnformeerd over de nalevingsstatus van hun endpoints en passende maatregelen kunnen nemen om problemen te verhelpen.

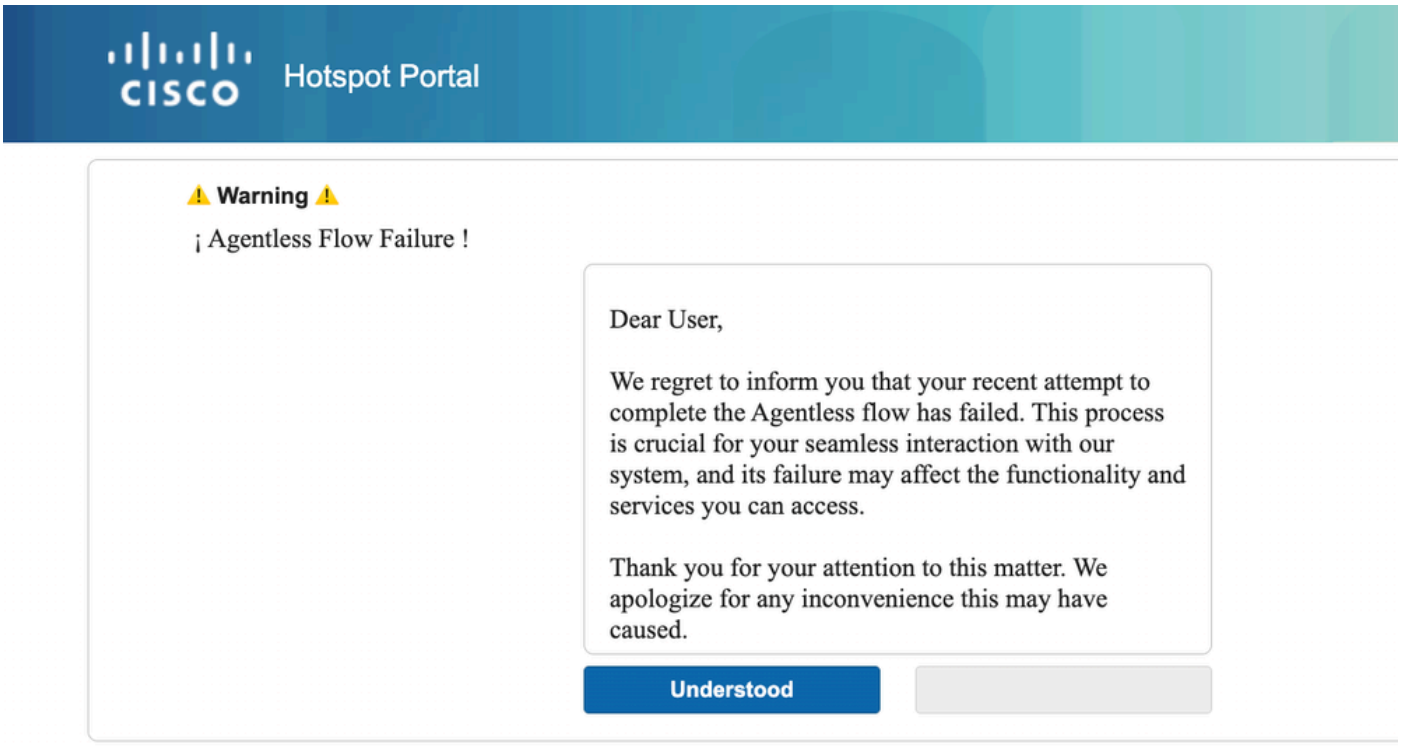
In de Cisco ISE GUI, klik op de menuicon (

) en kies **Work Centers** > **Guest Access** > **Portals & Components** >**Guest Portals.** Klik op **Maken** > **Hotspot Guest Portal** selecteren > **Doorgaan:** . In dit configuratievoorbeeld wordt Hotspot Portal **Agent less_Warning** genoemd.



Hotspot Guest Portal

In de portal-instellingen, hebt u de mogelijkheid om de berichten die worden weergegeven aan eindgebruikers aan te passen aan uw specifieke vereisten, dit is slechts een voorbeeld van aangepaste portal-weergave:



Posture Agent is mislukt

Autorisatieprofiel voor herstel (optioneel)

In de Cisco ISE GUI, klik op het menupictogram ( ) en kies Beleid > Beleidselementen **> Resultaten > Autorisatie > Autorisatieprofielen en maak een Autorisatieprofiel** voor uw herstel.

- In dit configuratievoorbeeld wordt het **autorisatieprofiel** aangeduid als **Remediation_Authorisation_Profile**.

-

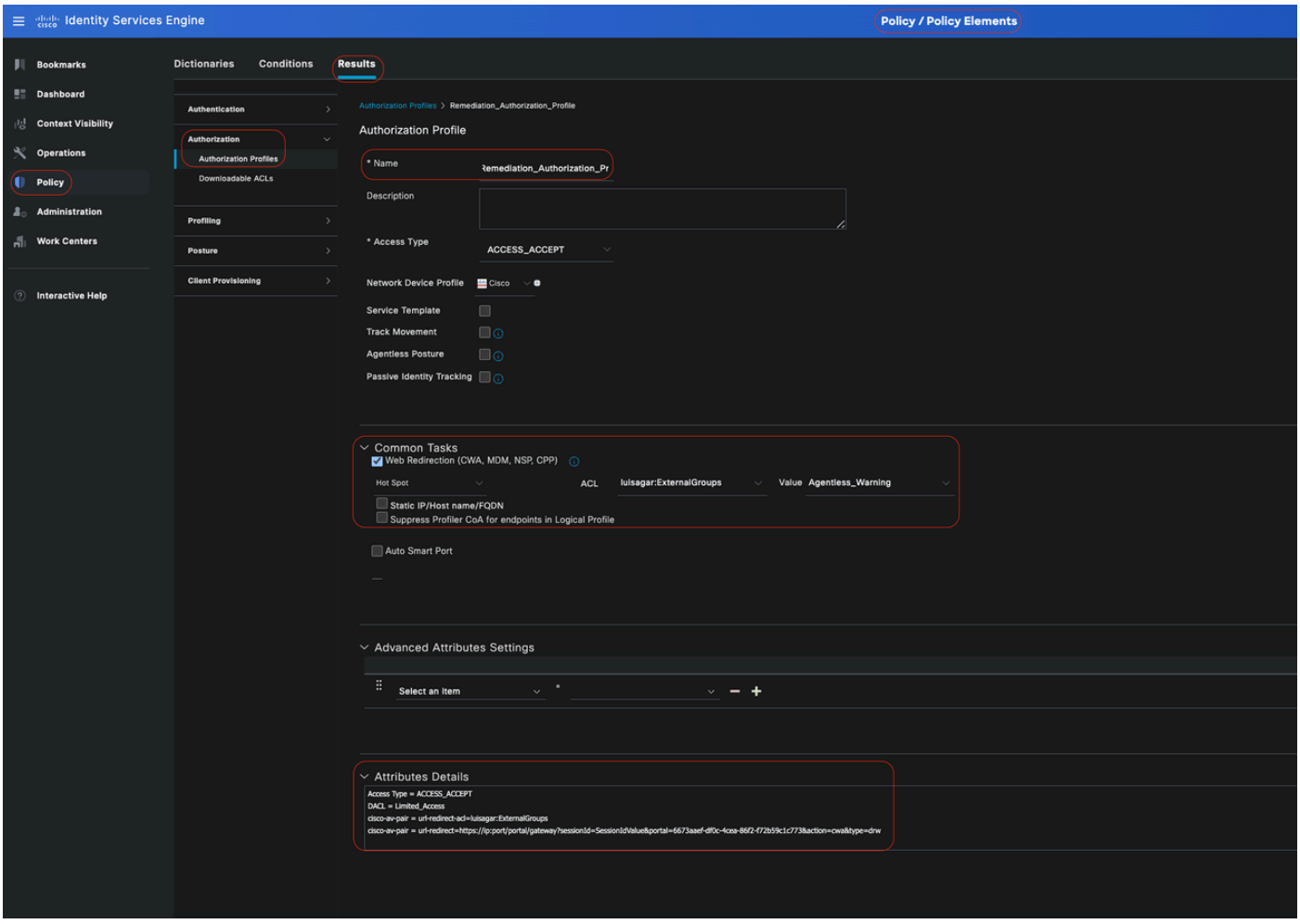
Omwille van de eenvoud bevat dit configuratievoorbeeld alleen een downloadbare toegangscontrolelijst (dACL) met de naam **Limited_Access** die beperkte toegang mogelijk maakt, afgestemd op de specifieke behoeften van uw organisatie.

-

De functie **Web Redirection** is geconfigureerd met een externe groep en de hotspot, waardoor de gebruiker zich meer bewust is van de naleving van endpoints.

-

Klik op **Save** (Opslaan).

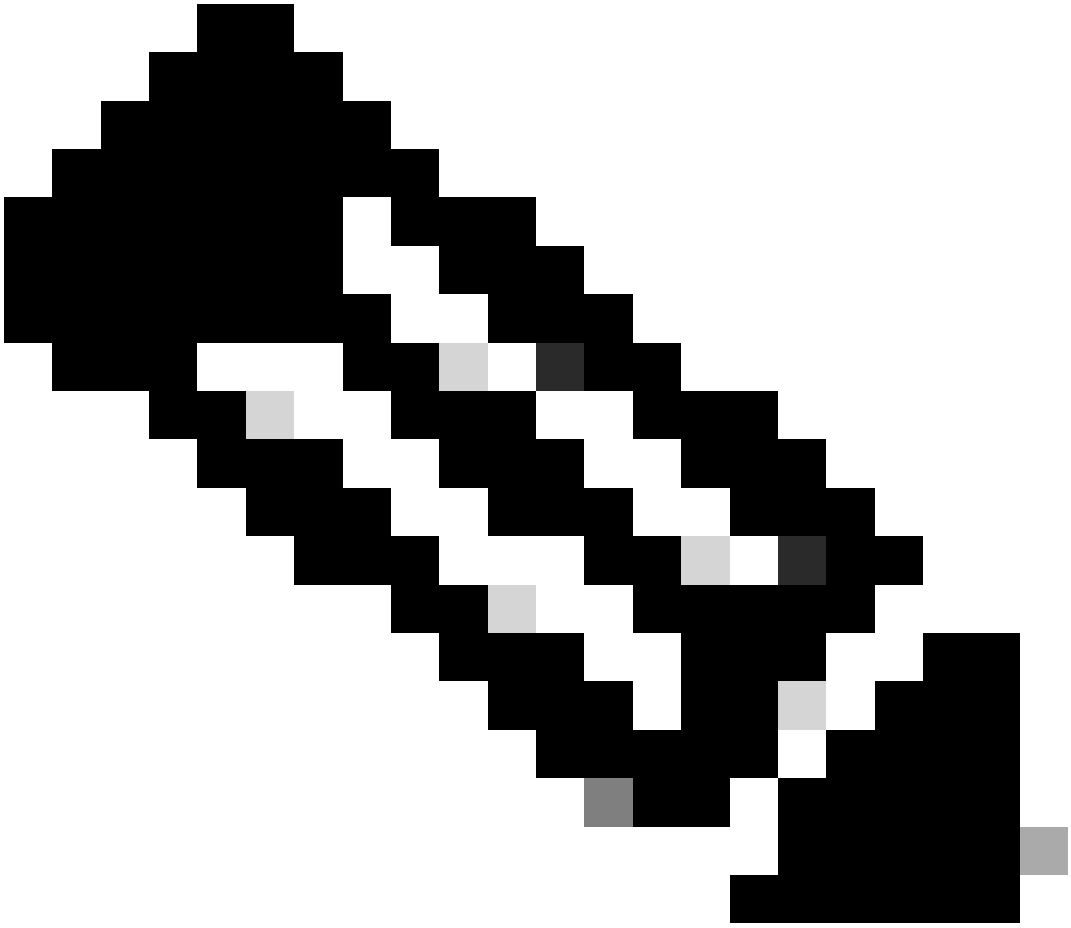


Regel voor toestemming voor herstel

Autorisatieregel zonder agent

In de Cisco ISE GUI, klik op de menuicon (

) en **kies Beleid** > **Beleidsinstellingen** en breid **het autorisatiebeleid uit**. Schakel dit drie autorisatiebeleid in en configureer dit:



Opmerking: deze autorisatieregels moeten in de opgegeven volgorde worden geconfigureerd om er zeker van te zijn dat de postuur correct werkt.

Unknown_Compliance_Redirect:

•**Voorwaarden:**

Configureer Network_Access_Authentication_Passed EN **Compliance_Unknown_Devices** met het resultaat ingesteld op Positie zonder Agent. Deze voorwaarde leidt tot de Stroom van de Agent.

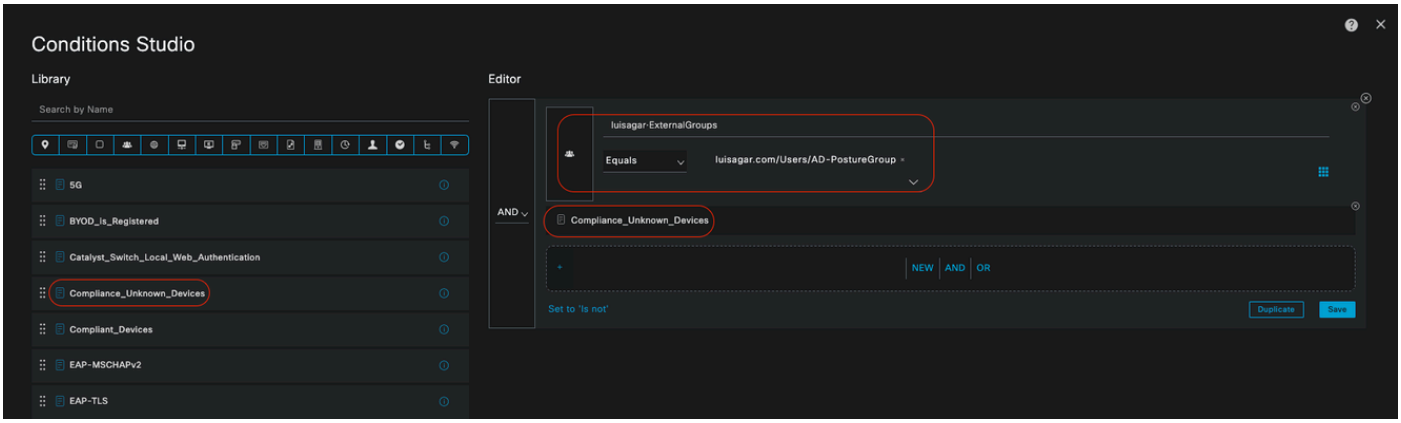
· **Voorbeeldomstandigheden:**

Configureer een groepsvoorwaarde van Active Directory (AD) om verkeer te segmenteren.

De voorwaarde **Compliance_Unknown_Devices** moet worden geconfigureerd als de initiële postuur is onbekend.

· **Autorisatieprofiel:**

Wijs **Agentless_Authorisation_Profile** toe aan deze Autorisatieregel om ervoor te zorgen dat apparaten door de Agentless Posture stroom gaan. Deze voorwaarde bevat Agentless Flow zodat apparaten die dit profiel raken Agent less flow kunnen initiëren.



Onbekende autorisatieregel

Niet-conforme_devices_redirect:

· **Voorwaarden:** Configureer Network_Access_Authenticatie_Passed en Non_Compliant_Devices waarbij het resultaat is ingesteld op DenyAccess. U kunt ook de hersteloptie gebruiken, zoals in dit voorbeeld wordt aangetoond.

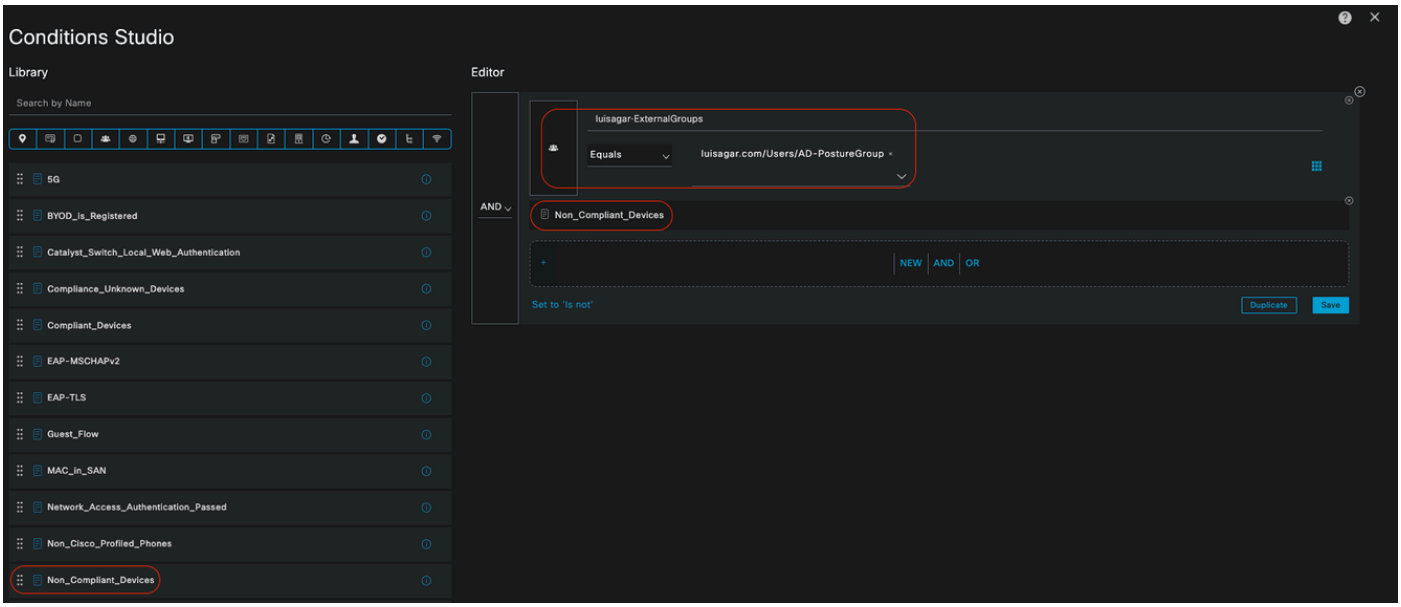
· **Voorbeeldomstandigheden:**

Configureer een AD Group-voorwaarde om verkeer te segmenteren.

De voorwaarde **Compliance_Unknown_Devices** moet worden geconfigureerd om beperkte resources toe te wijzen wanneer de postuur niet-compatibel is.

· **Autorisatieprofiel:**

Wijs **Remediation_Authorisation_Profile toe** aan deze Autorisatieregel om niet-conforme apparaten op de hoogte te stellen van hun huidige status via **Hotspot Portal** of om **toegang** te **weigeren**.



Niet-conforme autorisatieregel

Conforme_Apparaten_Toegang:

•Voorwaarden:

Configureer Network_Access_Authentication_Passed en **Compliant_Devices** terwijl het resultaat is ingesteld op PermitAccess.

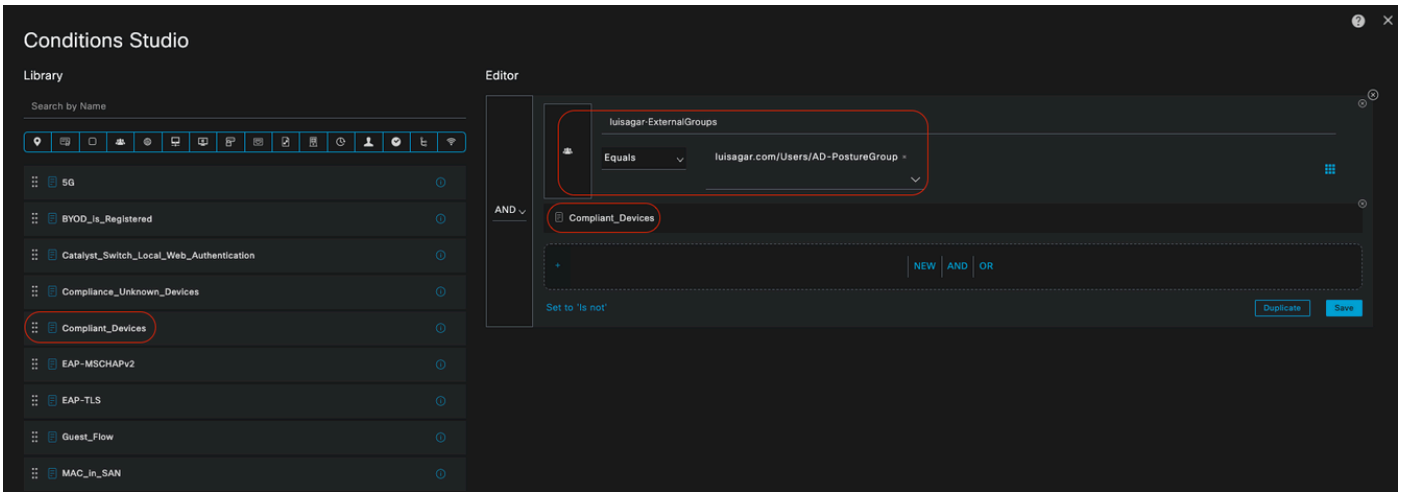
· Voorbeeldomstandigheden:

Configureer een AD Group-voorwaarde om verkeer te segmenteren.

De voorwaarde **Compliance_Unknown_Devices** moet zo worden geconfigureerd dat compatibele apparaten de juiste toegang krijgen.

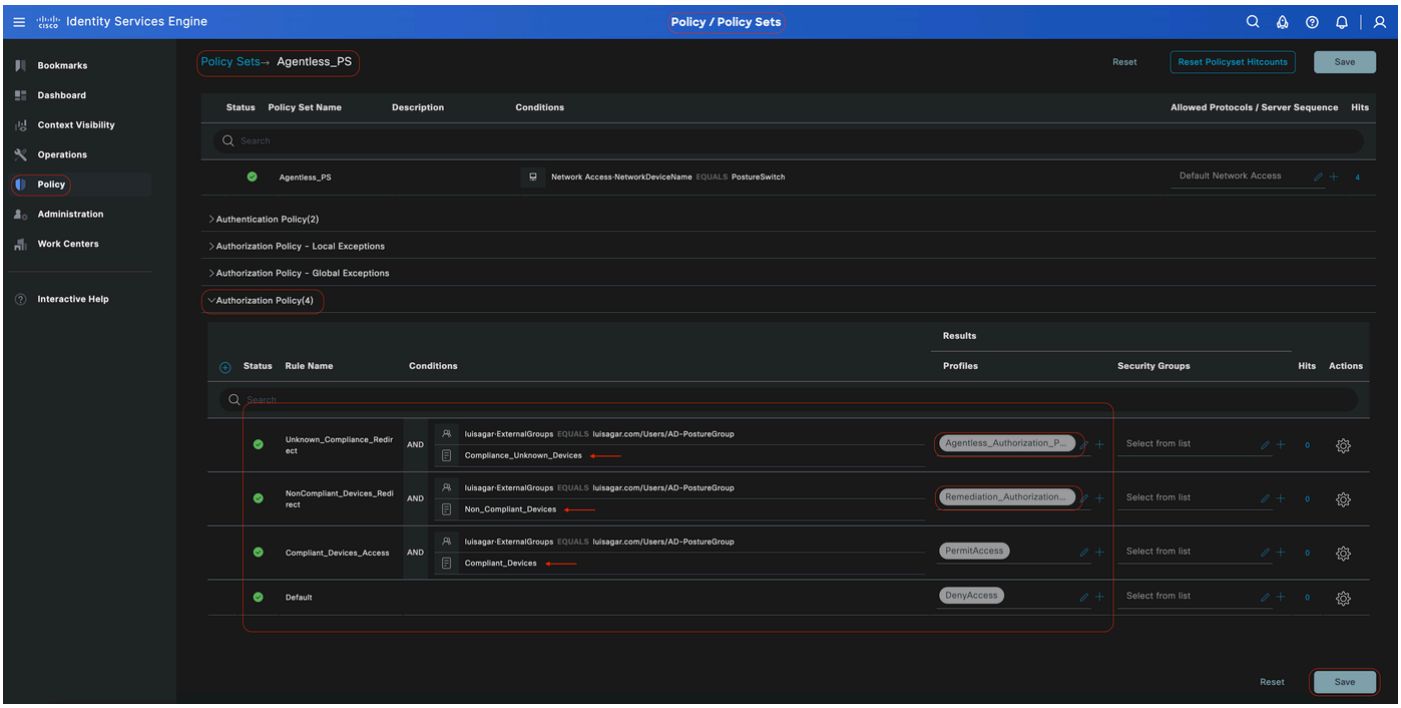
· Autorisatieprofiel:

Wijs **PermitAccess toe** aan deze autorisatieregel om ervoor te zorgen dat compatibele apparaten toegang hebben. Dit profiel kan worden aangepast aan de behoeften van uw organisatie.



Conforme autorisatieregel

Alle machtigingsregels



Vergunningsregels

Inlogreferenties voor endpoints configureren

In de Cisco ISE GUI, klik op het pictogram Menuicon ( ) en **kies Beheer** > **Instellingen** > **Endpoint Scripts** > **Aanmelden configuratie**, en configureer de clientreferenties om u op clients aan te melden.

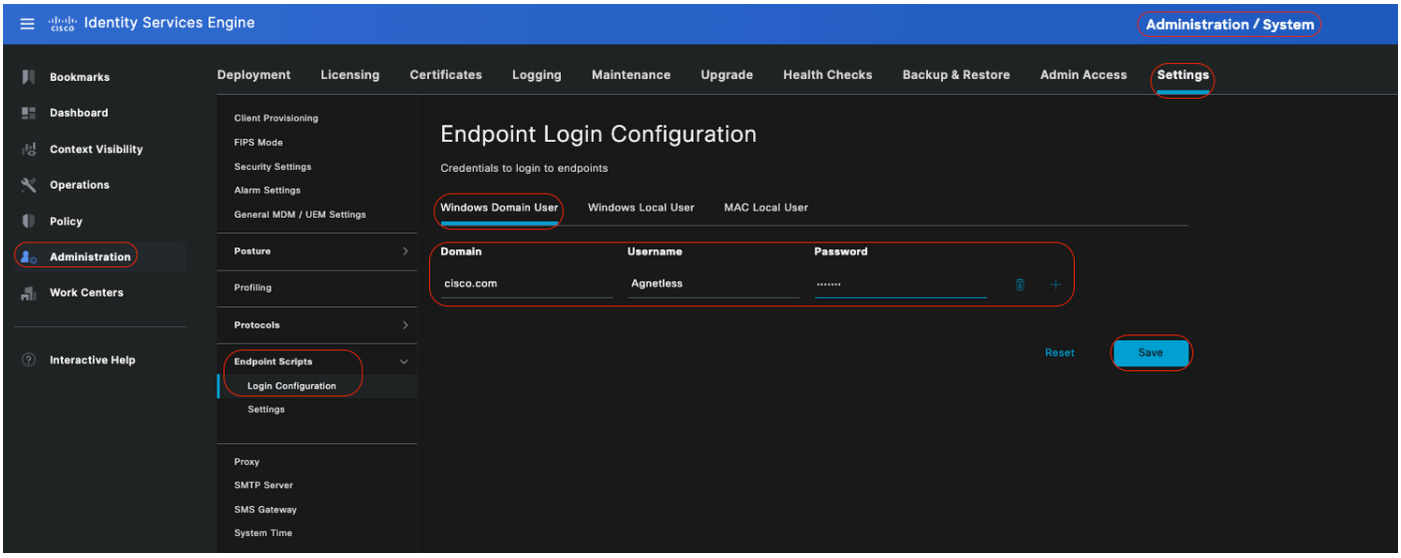
Deze zelfde referenties worden gebruikt door de Endpoint Scripts zodat Cisco ISE kan inloggen op clients.

Voor Windows-apparaten configureert u alleen de eerste twee tabbladen **(Windows Domain User en Windows Local User)**

- **Windows-domeingebruiker:**

Configureer de domeinreferenties die Cisco ISE moet gebruiken om in te loggen op een client via SSH. Klik op het pictogram Plus en voer zoveel Windows-logins in als u nodig hebt. Voer voor elk domein de gewenste waarden in de velden Domein, Gebruikersnaam, Wachtwoord. Als u domeinreferenties configureert, worden de lokale gebruikersreferenties die zijn geconfigureerd in het tabblad Lokale gebruiker van Windows genegeerd.

Als u Windows-endpoints beheert die gebruikmaken van een functiebeoordeling van Agent via een Active Directory-domein, zorg er dan voor dat u de domeinnaam levert, samen met referenties die lokale administratieve rechten bezitten.

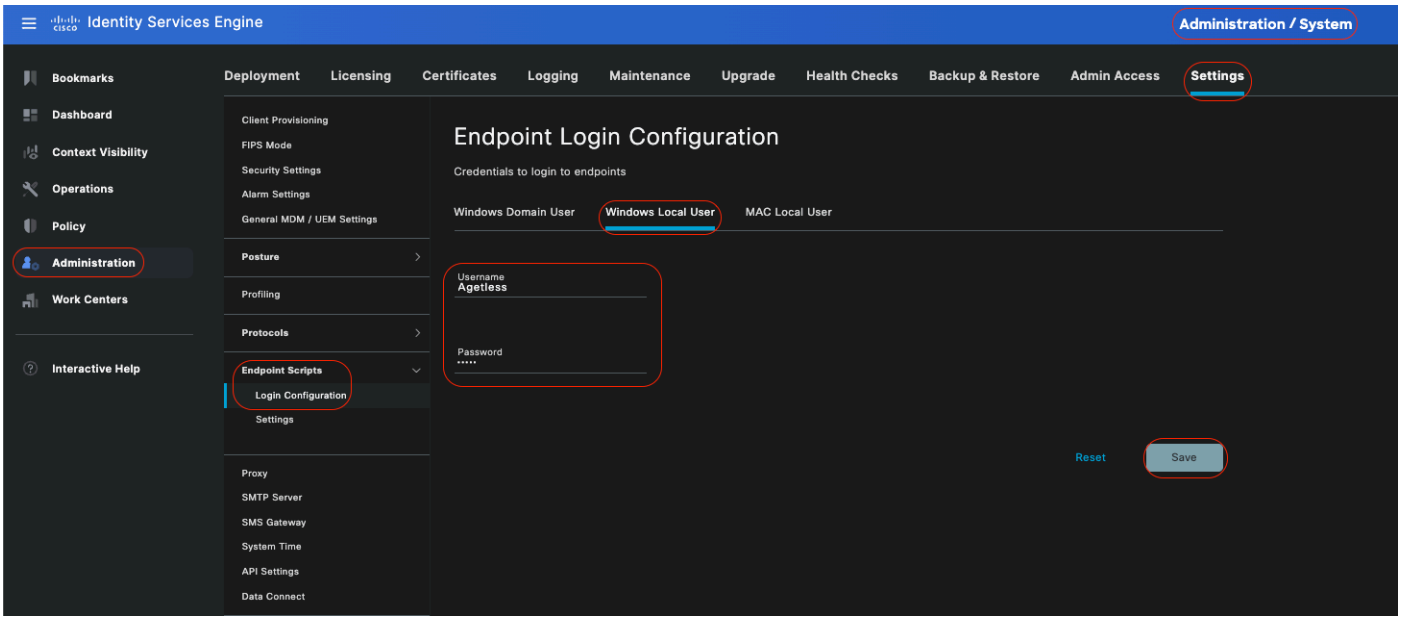


Windows-domeingebruiker

- **Lokale gebruiker van Windows:**

Configureer de lokale account die Cisco ISE gebruikt om de client via SSH te benaderen. De lokale account moet Powershell en Powershell Remote kunnen gebruiken.

Als u **geen** Windows-endpoints beheert die gebruikmaken van een functiebeoordeling Agent less via een Active Directory-domein, zorg er dan voor dat u aanmeldingsgegevens verstrekt die lokale beheerrechten hebben.

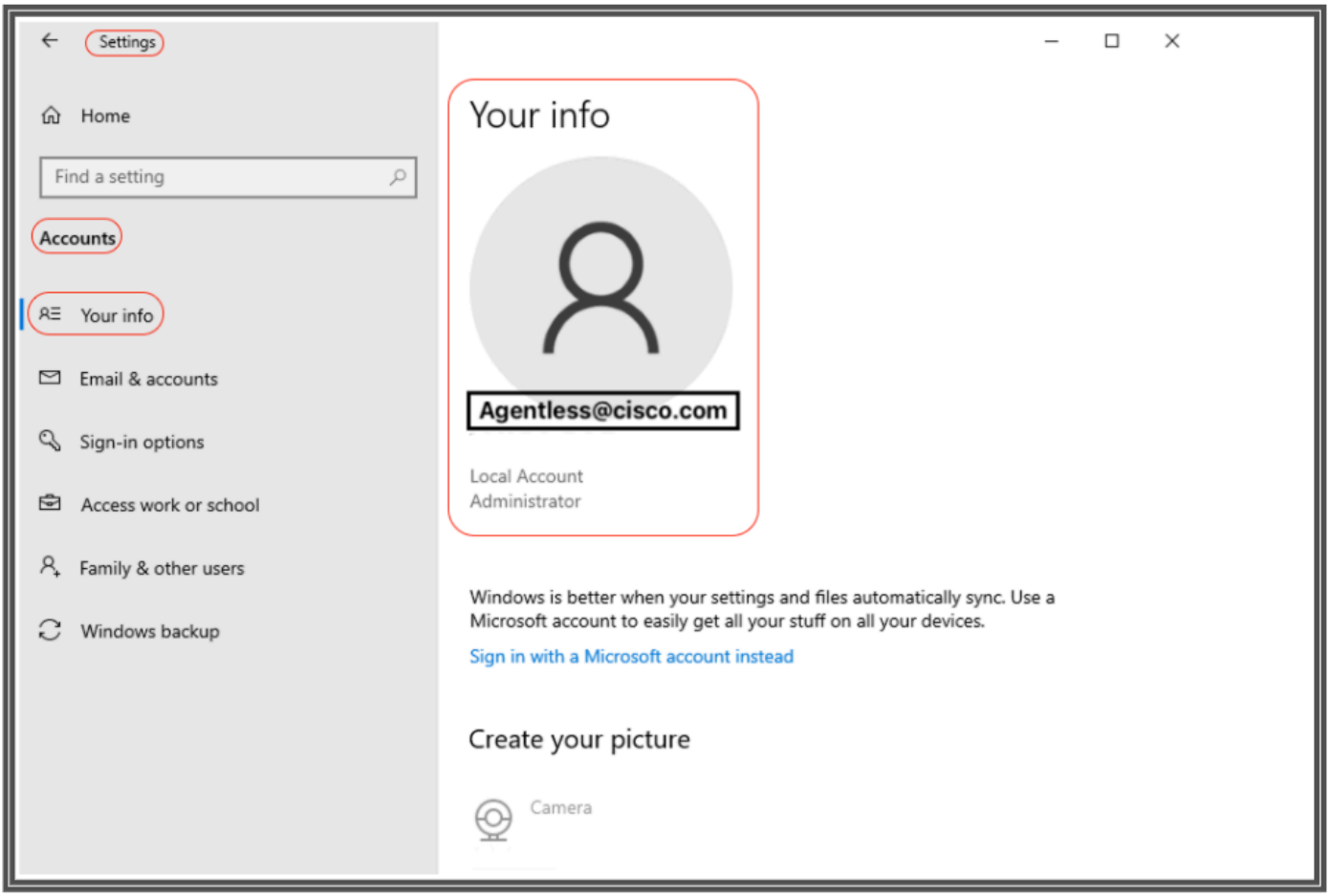


Lokale gebruiker van Windows

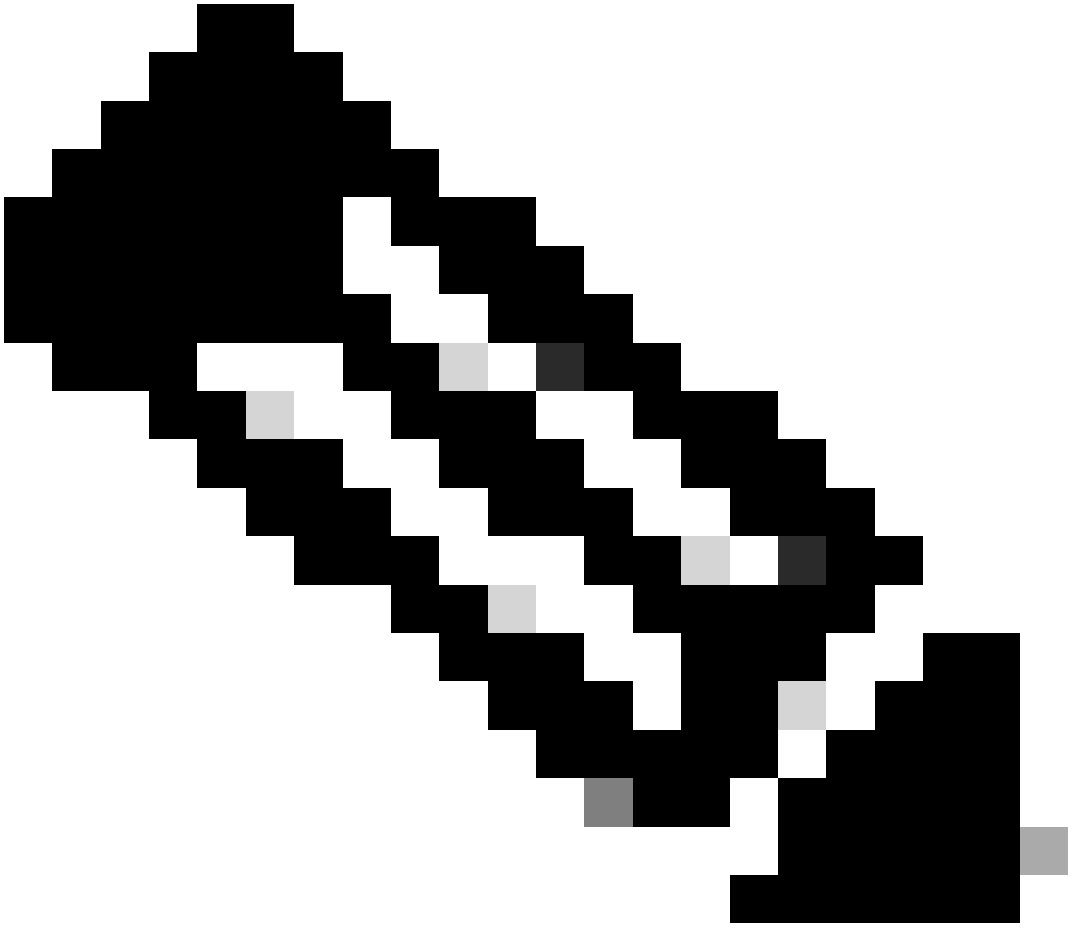
Accounts controleren

Om uw Windows domeingebruiker en Windows lokale gebruikersaccounts te verifiëren zodat u de juiste gegevens nauwkeurig kunt toevoegen onder Endpoint Login Credentials, gebruik deze procedure:

Windows lokale gebruiker: Met behulp van de GUI (Settings App) Klik op de **WindowsStart** knop, selecteer **Instellingen** (het tandwiel pictogram), klik op **Accounts**, en selecteer **Uw info**:



Accounts verifiëren



Opmerking: Voor MacOS kunt u verwijzen naar **MAC Local User**. In dit configuratievoorbeeld ga je echter geen MacOS-configuratie zien.

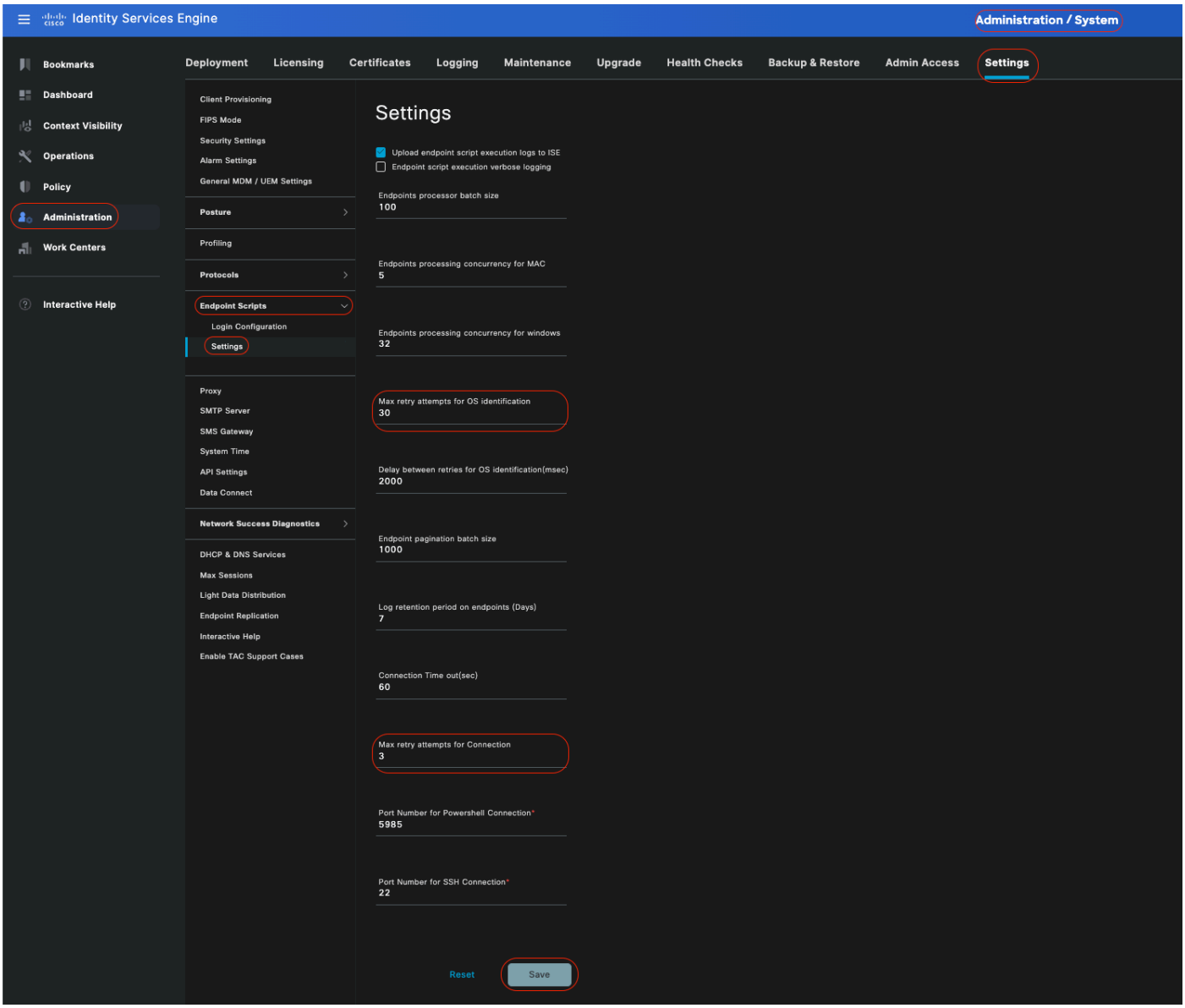
- **Lokale gebruiker van MAC:** Configureer de lokale account die Cisco ISE gebruikt om de client via SSH te benaderen. De lokale account moet Powershell en Powershell Remote kunnen gebruiken. Voer in het veld Gebruikersnaam de accountnaam in van de lokale account.

Om een Mac OS-accountnaam te bekijken, voert u deze opdrachtwhoami in de terminal uit:

Instellingen

In de Cisco ISE GUI, klik op het pictogram Menu () en **kies Beheer > Instellingen > Endpoint Scripts > Instellingen en stelMax-herhalingspogingen in** voor OS-identificatie, **Vertraging tussen herhalingen voor OS-identificatie** enzovoort. Deze instellingen bepalen hoe snel problemen met de connectiviteit kunnen worden bevestigd. Bijvoorbeeld, een fout dat de PowerShell poort niet open is, wordt in logbestanden alleen weergegeven nadat alle pogingen niet zijn uitgeput.

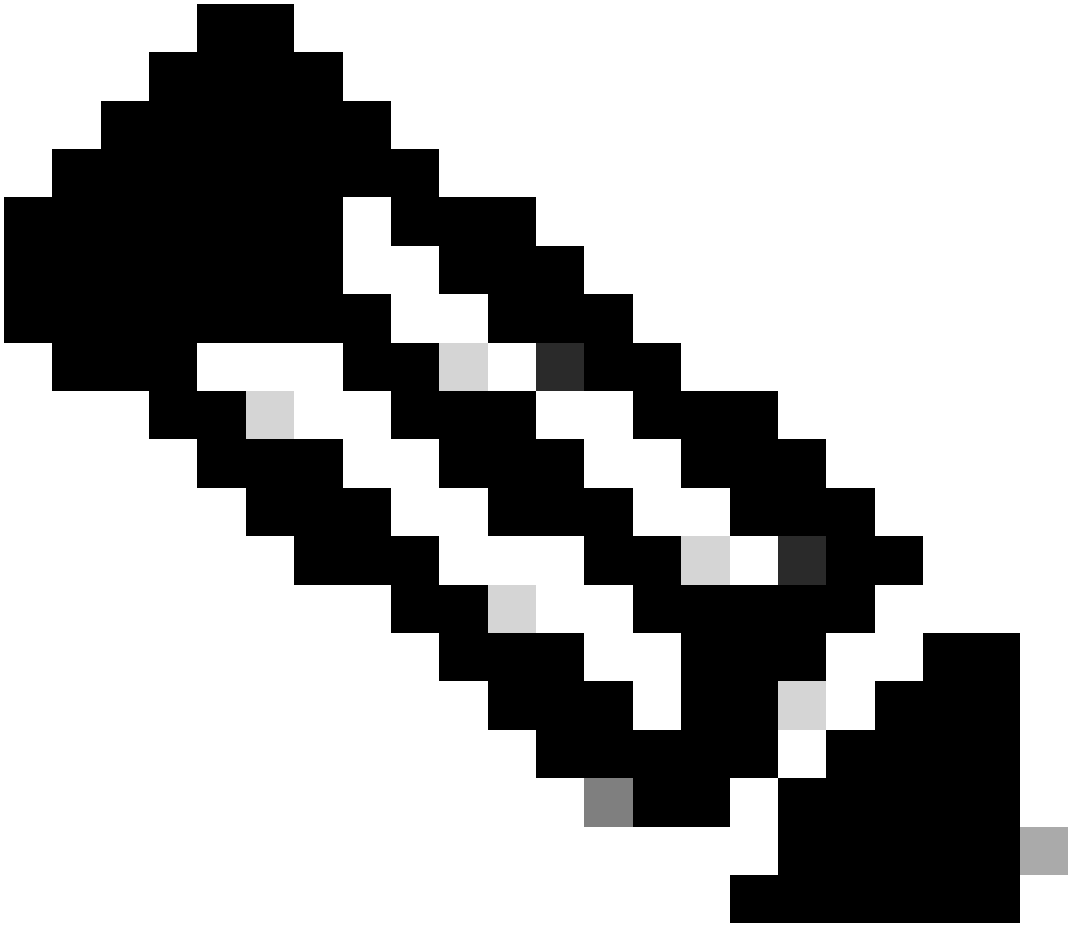
Deze screenshot toont de standaardinstellingen:



Instellingen endpointscripts

Als klanten verbinding maken met Agent-less houding, kunt u ze zien in de Live Logs.

Windows-endpoints configureren en problemen oplossen



Opmerking: dit zijn enkele aanbevelingen om te controleren en toe te passen op uw Windows-apparaat; u moet echter verwijzen naar Microsoft-documentatie of contact opnemen met Microsoft-ondersteuning als u problemen tegenkomt zoals gebruikersrechten, PowerShell-toegang enzovoort...

Voorwaarden voor verificatie en probleemoplossing

TCP-verbinding met poort 5985 testen

Voor Windows-clients moet poort 5985 voor toegang tot powershell op de client worden geopend. Voer deze opdracht uit om de TCP-verbinding met poort 5985 te bevestigen: **Test-NetConnection -ComputerName localhost -Port 5985**

De uitvoer die in deze screenshot wordt getoond geeft aan dat de TCP verbinding met poort 5985 op localhost mislukt is. Dit betekent dat de

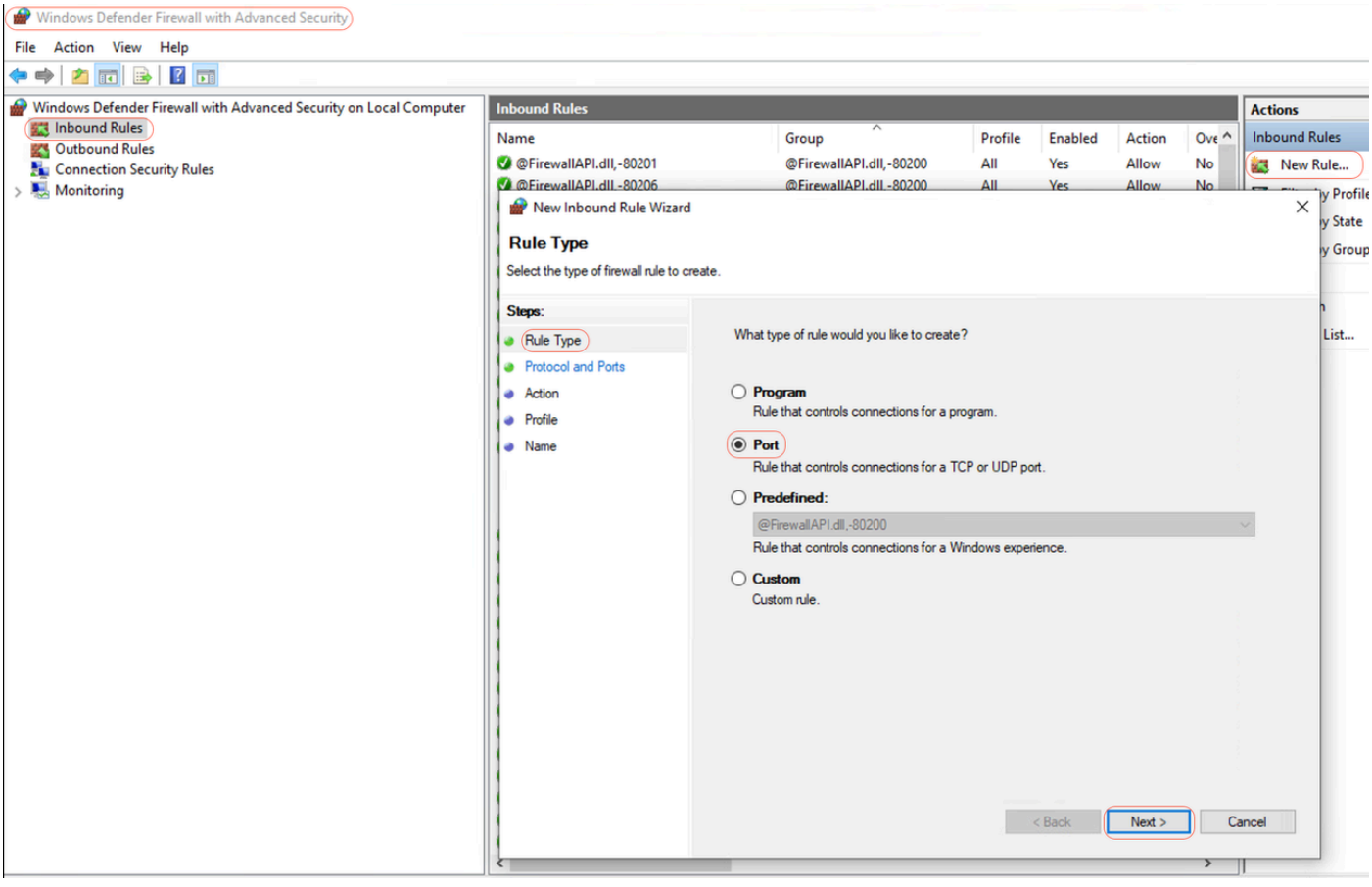
WinRM (Windows Remote Management) service, die poort 5985 gebruikt, niet actief is of niet goed is geconfigureerd.

```
PS C:\Windows\system32> Test-NetConnection -Computer localhost -Port 5985
WARNING: TCP connect to (::1 : 5985) failed
WARNING: TCP connect to (127.0.0.1 : 5985) failed


ComputerName            : localhost
RemoteAddress           : ::1
RemotePort              : 5985
InterfaceAlias          : Loopback Pseudo-Interface 1
SourceAddress           : ::1
PingSucceeded           : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False



PS C:\Windows\system32> ^C
```

Connection failed to WinRM

Inkomende regel maken om PowerShell op poort 5985 toe te staan

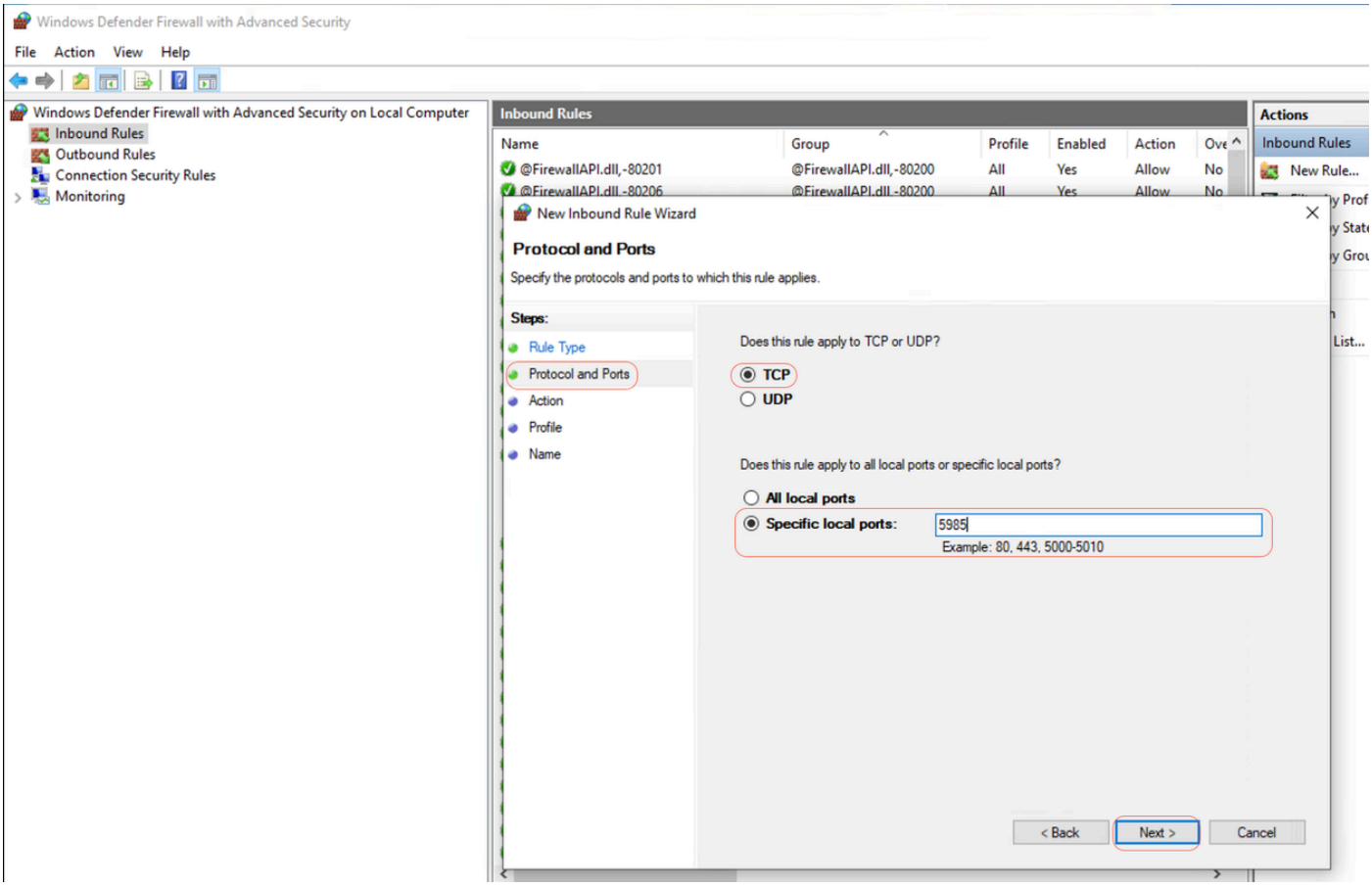
Stap 1 - In Windows GUI, ga naar de zoekbalk, typ Windows Firewall met geavanceerde security, klik erop en selecteer Uitvoeren als beheerder > Inkomende regels > Nieuwe regel > regeltype > poort > Volgende:



Nieuwe inkomende regel - poort

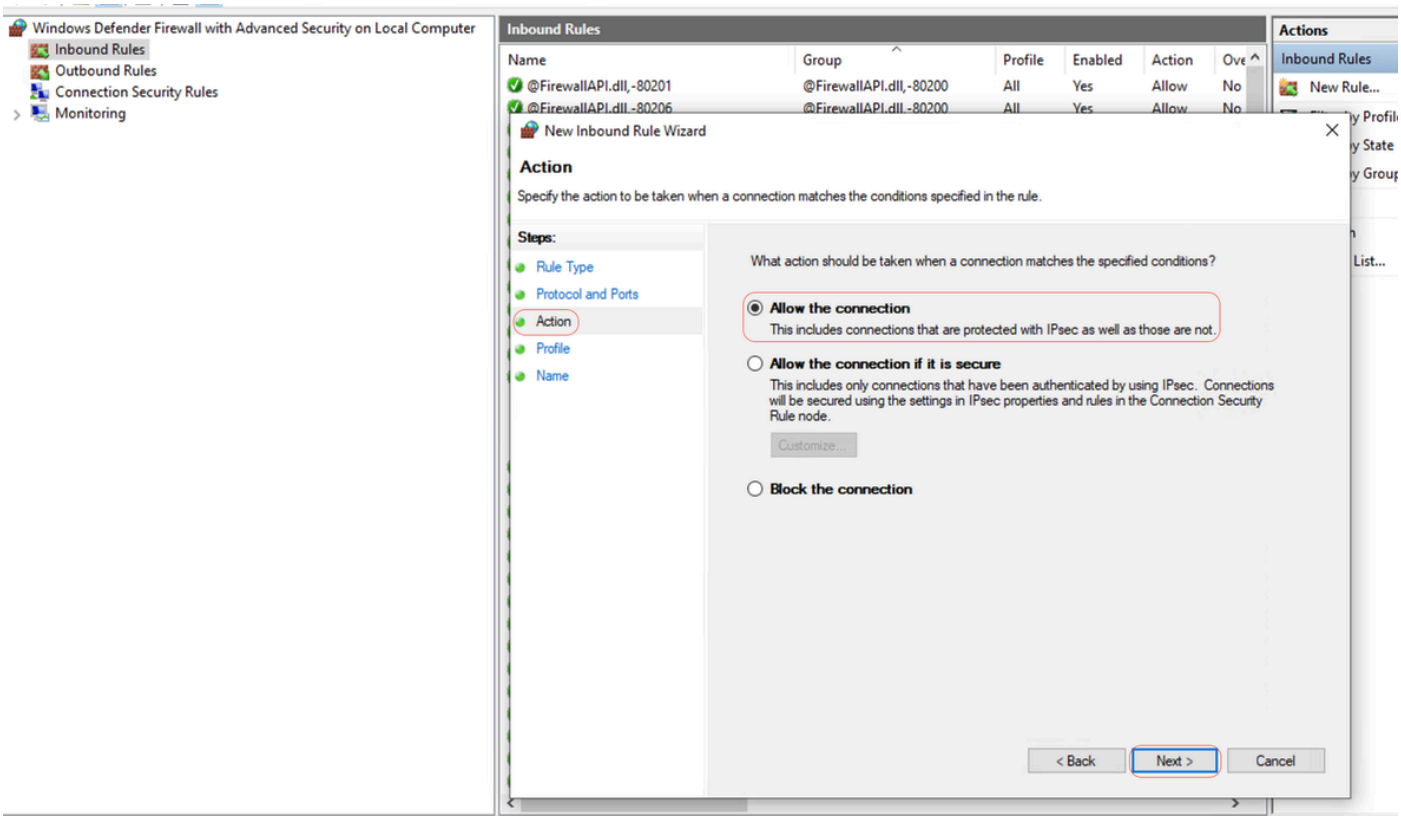
Stap 2 - Selecteer onder Protocollen en poorten TCP en specificeer lokale poorten, type poortnummer 5985 (standaardpoort voor

PowerShell-verwijdering) en klik op **Next**:



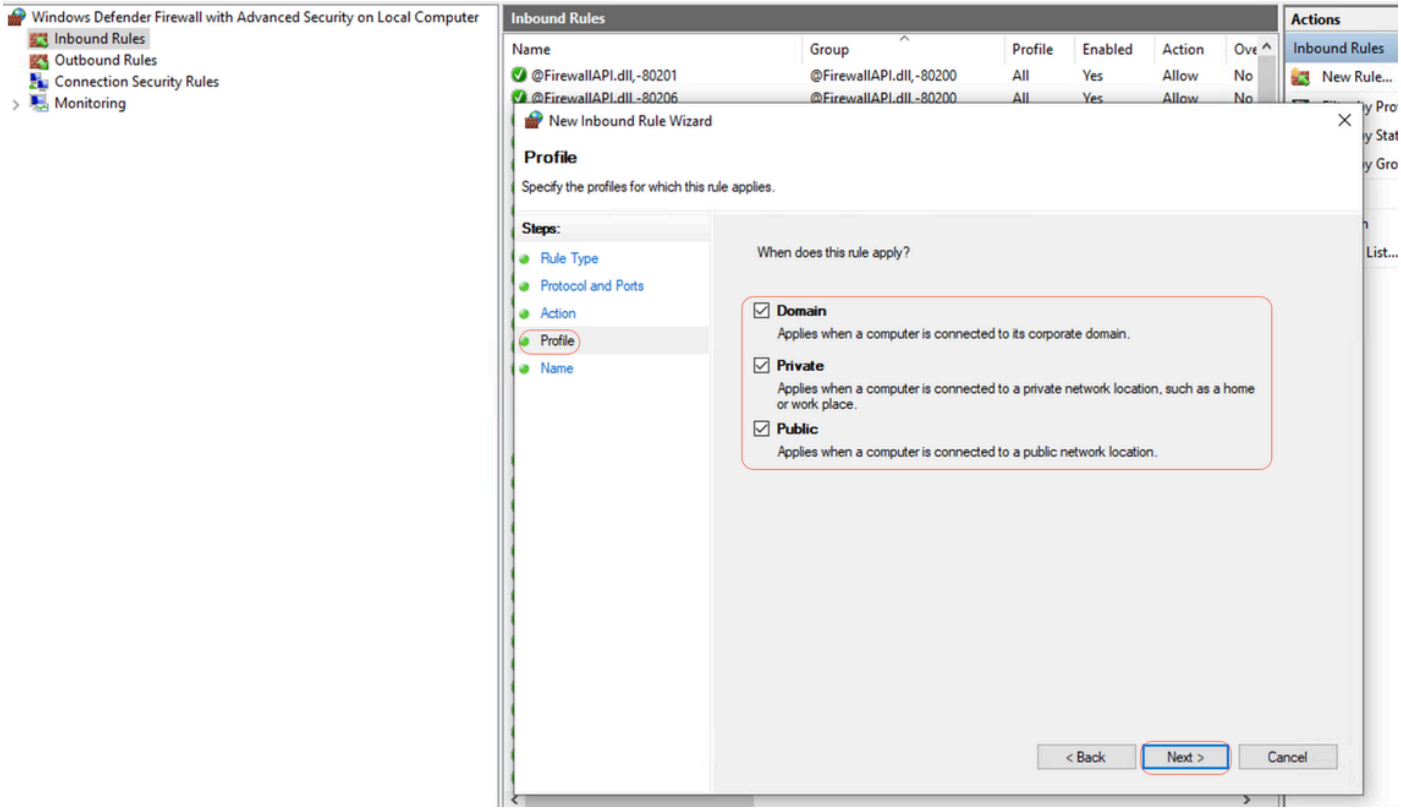
Protocollen en poorten

Stap 3- Onder **Actie** > Selecteer **Verbinding toestaan** > **Volgende**:



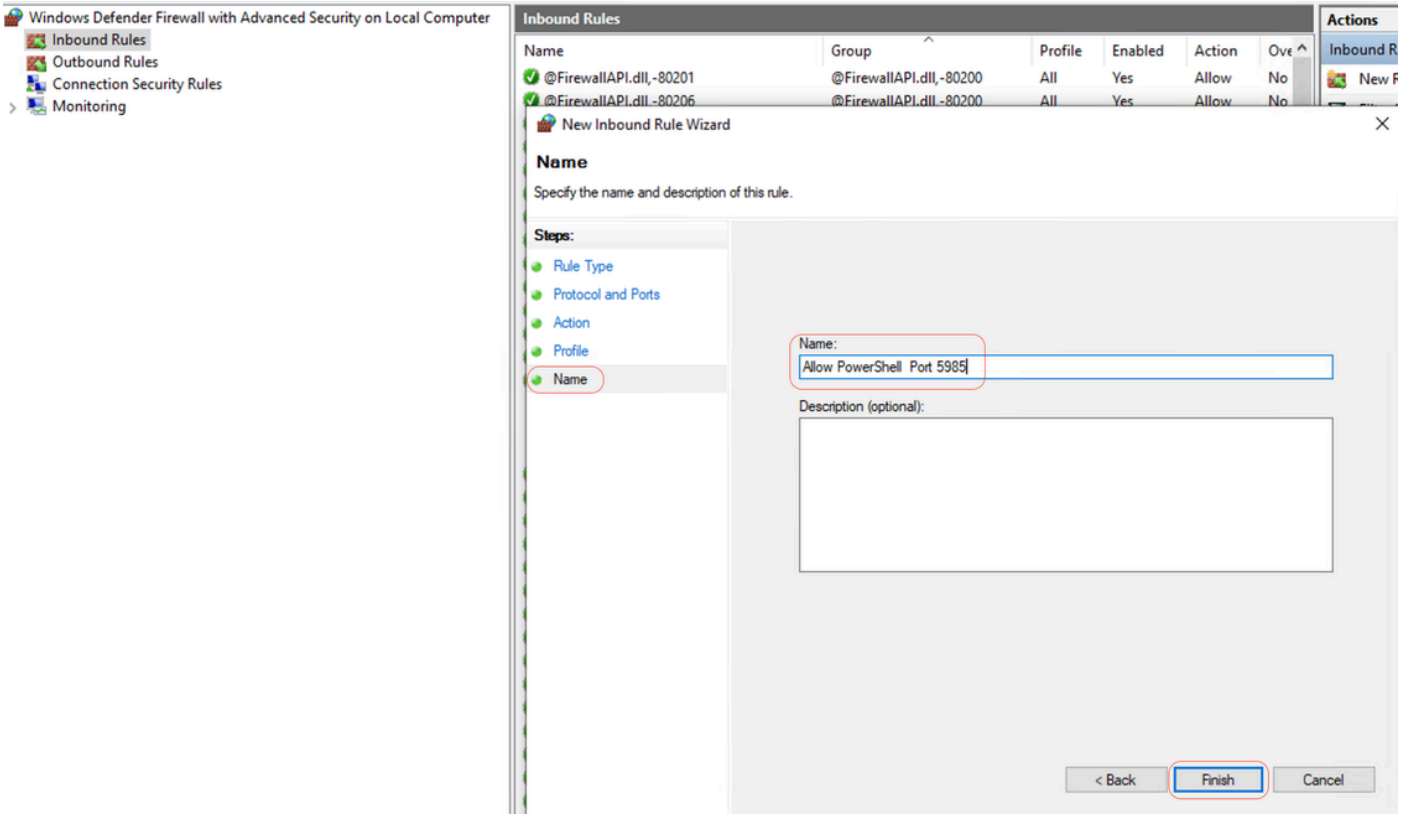
Actie

Stap 4 - Controleer onder Profile de selectievakjes Domain, **Private** en **Public** en klik op **Next**:



Profiel

Stap 5- Onder **Naam**, Voer een naam in voor de regel, zoals **Allow PowerShell op poort 5985** en klik op **Finish**:

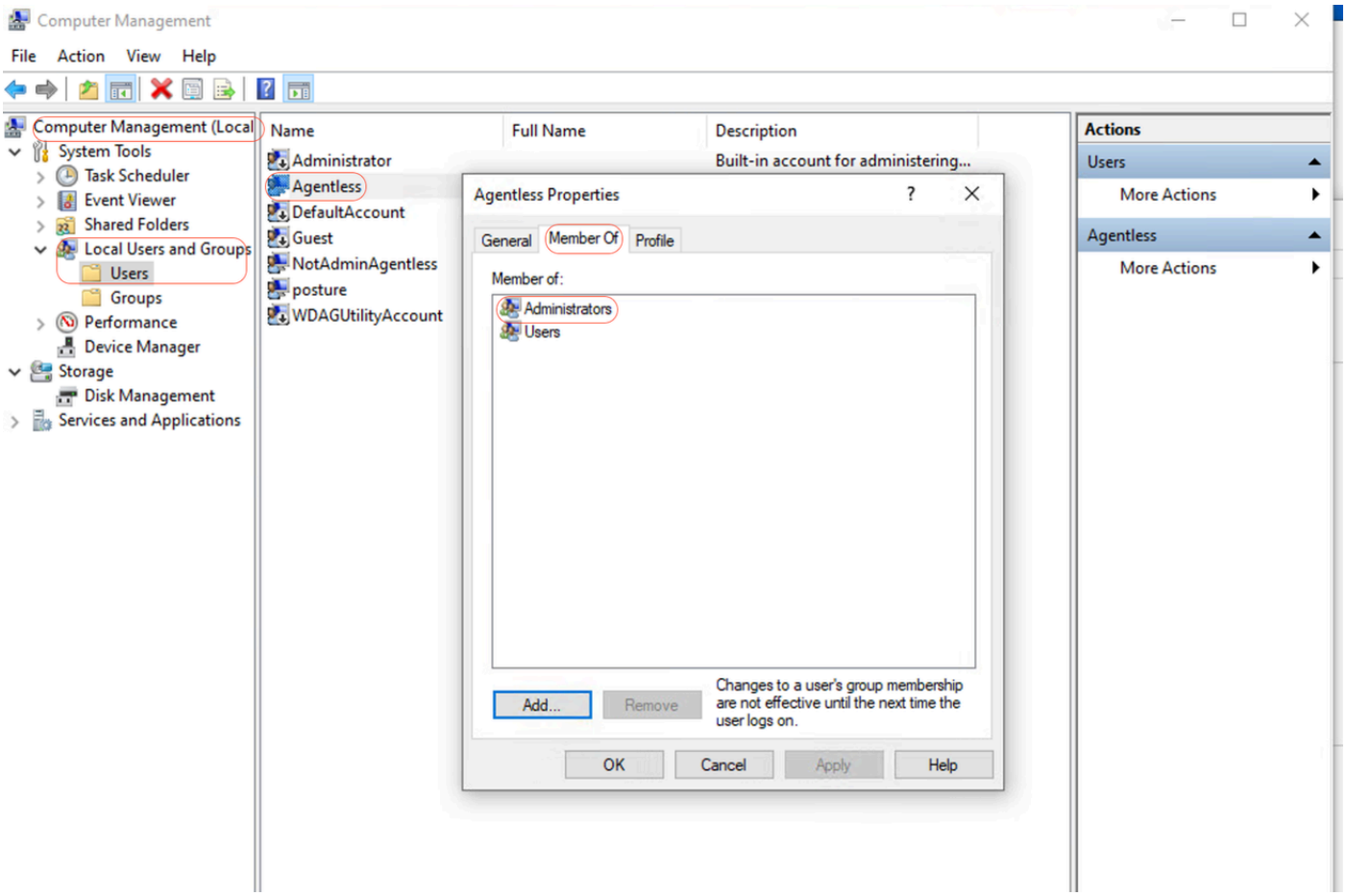


Naam

Clientreferenties voor shell-aanmelding moeten lokale beheerdersrechten hebben

Clientreferenties voor shell-aanmelding moeten lokale beheerdersrechten hebben. Controleer of u beheerdersrechten hebt. Controleer deze stappen:

In Windows GUI, ga naar Instellingen > Computerbeheer > Lokale gebruikers en groepen > Gebruikers > Selecteer de Gebruikersaccount (in dit voorbeeld **is** Agentless **Account geselecteerd) > Lid van, account moet Beheerdersgroep** hebben.



Lokale beheerdersrechten

WinRM-luisteraar valideren

Zorg ervoor dat de WinRM-luisteraar voor **HTTP** op poort **5985** is geconfigureerd:

C: \Windows\system32> **winrm enumerate winrm/config/listener** Listener Address = * **Transport = HTTP Port = 5985** Hostname Enabled = true URLPrefix = wsman CertificateThumbprint C: \Windows\system32>

PowerShell-afstandsbediening van WinRM inschakelen

Zorg ervoor dat de service actief is en is ingesteld om automatisch te starten, ga dan door deze stappen:

Enable the WinRM service **Enable-PSRemoting -Force** # Start the WinRM service **Start-Service WinRM** # Set the WinRM service to start automatically **Set-Service -Name WinRM -StartupType Automatic**

Verwachte output:

C: \Windows\system32> **Enable-PSRemoting -Force** WinRM is already set up to receive requests on this computer. WinRM has been updated for remote management. WinRM firewall exception enabled. -Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

C: \Windows\system32> **Start-Service WinRM**

C: \Windows\system32> **Set-Service -Name WinRM -StartupType Automatic**

PowerShell moet v7.1 of hoger zijn. De client moet cURL v7.34 of hoger hebben:

Hoe PowerShell en cURL versies op Windows controleren

Ervoor zorgen dat u de juiste versies van PowerShell gebruikt; cURL is essentieel voor Posture Agentless:

PowerShell-versie controleren

Voor Windows:

1. **Open PowerShell:**

・Druk op Win + X en selecteer **Windows PowerShell** of **Windows PowerShell (Admin)**.

2. Voer de opdracht uit:$PSVersionTable.PSVersion

・Deze opdracht geeft de versiedetails van PowerShell op uw systeem geïnstalleerd.

URL-versie controleren

Voor Windows:

1. Opdrachtprompt openen:

・Druk op Win + R, type cmd, en klik op **ENTER**.

2. Opdracht uitvoeren: curl --version

・Deze opdracht geeft de versie van cURL weer die op uw systeem is geïnstalleerd.

Output voor het controleren van de versies PowerShell en cURL op Windows-apparaten

C: \Windows\system32> **$PSVersionTable.PSVersion** Major Minor Build Revision ----- ----- ----- ----- 7 1 19041 4291

C: \Windows\system32>

C: \Windows\system32>

C: \Windows \system32>**curl --version curl 8.4.0 (Windows) libcurl/8.4.0 Schannel WinIDN** Release-Date: 2023-10-11 Protocols: dict file ftp ftps http https imap imaps pop3 pop3s smtp smtps telnet tftp ftps http https Features: AsynchNS HSTS HTTPS-proxy IDN IPv6 Kerberos Largefile NTLM SPNEGO SSL SSPI threadsafe Unicode UnixSockets c: \Windows\system32>

Aanvullende configuratie

Met deze opdracht wordt de machine geconfigureerd om specifieke externe hosts voor WinRM-verbindingen te vertrouwen: Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

C: \Windows\system32> **Set-Item WSMan:\localhost\Client\TrustedHosts -Value x.x.x.x** WinRM Security Configuration. This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list cannot be authenticated. The client can send credential information to these computers. Are you sure that you want to modify this list? [Y] Yes [N] No [S] Suspend [?] Help (default is "y"): **Y** PS C: \Windows \system32> -

De test-wsman cmdlet met de -Verificatie Onderhandelen en -Credential parameters is een krachtig hulpmiddel om de beschikbaarheid en configuratie van de WinRM-service op een externe machine te verifiëren: test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

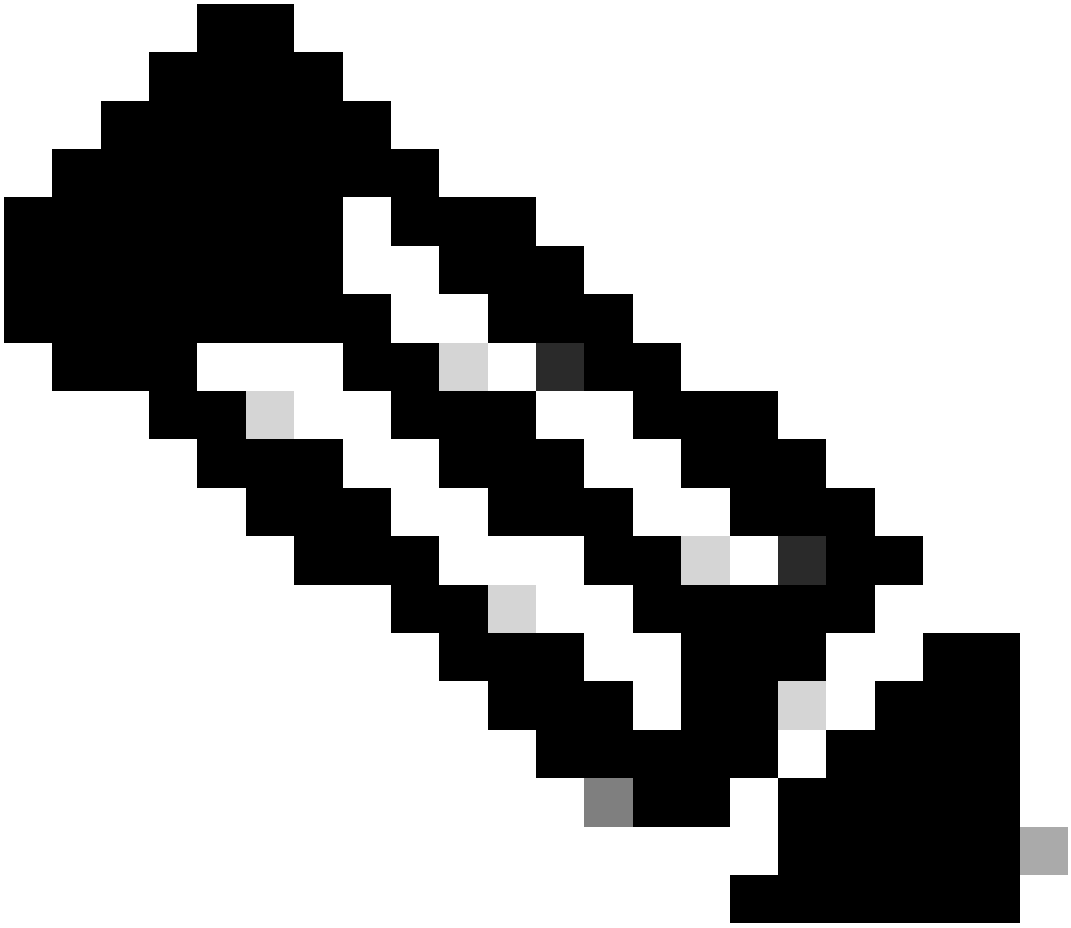
PowerShell moet v7.1 of hoger zijn. De client moet cURL v7.34 of hoger hebben:

Op macOS:

1. **Open terminal:**

・U kunt Terminal vinden in **Toepassingen > Hulpprogramma's**.

2. Opdracht uitvoeren: pwsh -Command '$PSVersionTable.PSVersion'



Opmerking: · Controleer of PowerShell Core (pwsh) is geïnstalleerd. Als dit niet het geval is, kunt u het installeren via Homebrew (zorg ervoor dat u Himebrew installeert): brew install --cask powershell

---

Op macOS:

1. **Open terminal:**

· U kunt Terminal vinden in **Toepassingen > Hulpprogramma's**.

2. Opdracht uitvoeren: curl --version

· Deze opdracht moet de versie van cURL tonen die op uw systeem is geïnstalleerd.

Voor MacOS-clients moet poort 22 voor toegang tot SSH open zijn voor toegang tot de client

Stapsgewijze gids:

1. **Voorkeuren voor Open System:**

・Navigeer naar **Systeemvoorkeuren** vanuit het Apple-menu.

2. **Aanmelden op afstand inschakelen:**

・Ga naar **Delen**.

・Vink het vakje naast **Remote Login aan**.

・Zorg ervoor dat de optie **Toegang toestaan voor** de juiste gebruikers of groepen is ingesteld. Door **Alle gebruikers te selecteren** kan elke gebruiker met een geldig account op de Mac inloggen via SSH.

3. **Controleer de firewallinstellingen:**

・Als de firewall is ingeschakeld, moet u ervoor zorgen dat deze SSH-verbindingen toestaat.

・Ga naar **Systeemvoorkeuren > Beveiliging en privacy > Firewall**.

・Klik op de knop **Firewallopties**.

・Controleer of **Remote Login** of **SSH** vermeld en toegestaan is. Als deze niet in de lijst staat, klikt u op de knop **Toevoegen** (+) om deze toe te voegen.

4. **Open poort 22 via terminal (indien nodig):**

・Open de **Terminal**-toepassing vanuit **Toepassingen > Hulpprogramma's**.

・Gebruik de opdracht pfctl om de huidige firewallregels te controleren en om er zeker van te zijn dat poort 22 open is:sudo pfctl -sr | grep 22

・Als poort 22 niet open is, kunt u handmatig een regel toevoegen om SSH toe te staan:echo "passeren in proto tcp van een willekeurige poort naar een poort 22" | sudo pfctl -ef -

5. **Toegang tot SSH testen:**

・Open vanaf een ander apparaat een terminal of SSH-client.

・Probeer verbinding te maken met de macOS-client met behulp van het IP-adres:ssh username@<macOS-client-IP>

・Vervang de gebruikersnaam door de juiste gebruikersaccount en <macOS-client-IP> door het IP-adres van de macOS-client.

Zorg er voor MacOS voor dat dit item wordt bijgewerkt in het bestand van gebruikers om te voorkomen dat de installatie van het certificaat mislukt op de eindpunten:

Bij het beheer van macOS-endpoints is het van cruciaal belang dat specifieke beheeropdrachten kunnen worden uitgevoerd zonder dat er een wachtwoordprompt vereist is.

Voorwaarden

・Beheerderstoegang op het macOS-systeem.

・Basis vertrouwdheid met Terminalopdrachten.

Stappen voor het bijwerken van het Sudoers-bestand

1. **Open terminal:**

・U kunt Terminal vinden in **Toepassingen > Hulpprogramma's**.

2. **Het Sudoers-bestand bewerken:**

・Gebruik de visudo-opdracht om het gebruikersbestand veilig te bewerken. Dit zorgt ervoor dat eventuele syntaxisfouten worden gedetecteerd voordat u het bestand opslaat.sudo visudo

・U wordt gevraagd het beheerderswachtwoord in te voeren.

3. **Vind de juiste rubriek:**

・Ga in de visudo-editor naar de sectie waar gebruikersspecifieke regels zijn gedefinieerd. Meestal is dit naar de onderkant van het bestand.

4. **Vereiste vermelding toevoegen:**

・Voeg deze regel toe om de gespecificeerde gebruikerstoestemming te verlenen voor het uitvoeren van de security en osascript opdrachten zonder wachtwoord: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

・Vervang **<macadminusername>** door de huidige gebruikersnaam van de macOS admin.

5. **Opslaan en afsluiten:**

・Als u de standaard editor (nano) gebruikt, drukt u op Ctrl + X om af te sluiten, drukt u vervolgens op Y om de wijzigingen te bevestigen en drukt u ten slotte op ENTER om het bestand op te slaan.

・**Als u** vi of vim **gebruikt**, drukt u op Esc, type :wq, en drukt u op ENTER om op te slaan en te beëindigen.

6. **Controleer de wijzigingen:**

・Om ervoor te zorgen dat de veranderingen van kracht zijn geworden, kunt u een opdracht uitvoeren die de bijgewerkte sudo toestemmingen vereist. Voorbeeld:

sudo /usr/bin/security find-certificate -a sudo /usr/bin/osascript -e 'tell application "Finder" to display dialog "Test"'

・Deze opdrachten kunnen worden uitgevoerd zonder om een wachtwoord te vragen.

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.