

Cisco ISE 3.1 Uitstellen met Linux configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties op ISE](#)

[Configuraties van de switch](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de procedure om een beleid voor het plaatsen van bestanden voor Linux en de Identity Services Engine (ISE) te configureren en implementeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect
- Identity Services Engine (ISE)
- Linux

Gebruikte componenten

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

- AnyConnect 4.10.05085
- ISE versie 3.1 P1
- Linux Ubuntu 20.04
- Cisco Switch Catalyst 3650. Versie 3.07.05.E (15.12(3)E5)

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.

Configureren

Configuraties op ISE

Stap 1. Dienst postdiensten bijwerken:

navigeren naar **werkcentra > Posture > Instellingen > Software updates > Posture updates**.
Selecteer Nu bijwerken en wacht tot het proces is voltooid:

The screenshot shows the Cisco ISE Work Centers - Posture interface. The left sidebar contains navigation options: Posture General Settings, Endpoint Scripts, Reassessment configurations, Acceptable Use Policy, Software Updates (expanded), Client Provisioning, Posture Updates (selected), and Proxy Settings. The main content area is titled 'Posture Updates' and includes the following settings:

- Web Offline
- * Update Feed URL: <https://www.cisco.com/web/secure/spa/posture-...> [Set to Default](#)
- Proxy Address:
- Proxy Port:
- Automatically check for updates starting from initial delay: HH:MM:SS (11:32:21) every 2 hours

Buttons: Save, Update Now, Reset

Update Information:

Last successful update on	2022/03/24 11:40:59
Last update status since ISE was started	Last update attempt at 2022/03/24 11:40:59 was successful
Cisco conditions version	277896.0.0.0
Cisco AV/AS support chart version for windows	261.0.0.0
Cisco AV/AS support chart version for Mac OSX	179.0.0.0
Cisco AV/AS support chart version for Linux	15.0.0.0
Cisco supported OS version	71.6.2.0

Een **door Cisco meegeleverd pakket** is een softwarepakket dat u vanuit de Cisco.com-site kunt downloaden, zoals de AnyConnect-softwarepakketten. Een **door de klant gemaakt pakket** is een profiel of een configuratie die u buiten de ISE-gebruikersinterface hebt gemaakt en u wilt uploaden naar ISE voor gebruik met een beoordeling van de positie. Voor deze oefening kunt u het AnyConnect-webimplementatiepakket "anyconnect-linux64-4.10.05085-webimplementatie-k9.pkg" downloaden.

Opmerking: Vanwege updates en patches kan de aanbevolen versie wijzigen. Gebruik de nieuwste, aanbevolen versie op de cisco.com-site.

Stap 2.Upload AnyConnect:

Ga vanuit het Posture Work Center naar **Client Provisioning > Resources**

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy
Resources
 Client Provisioning Portal

Resources

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	CiscoTemporalAgentOSX 4...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.02...	CiscoAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoAgentlessWindows 4.1...	CiscoAgentlessWind...	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145

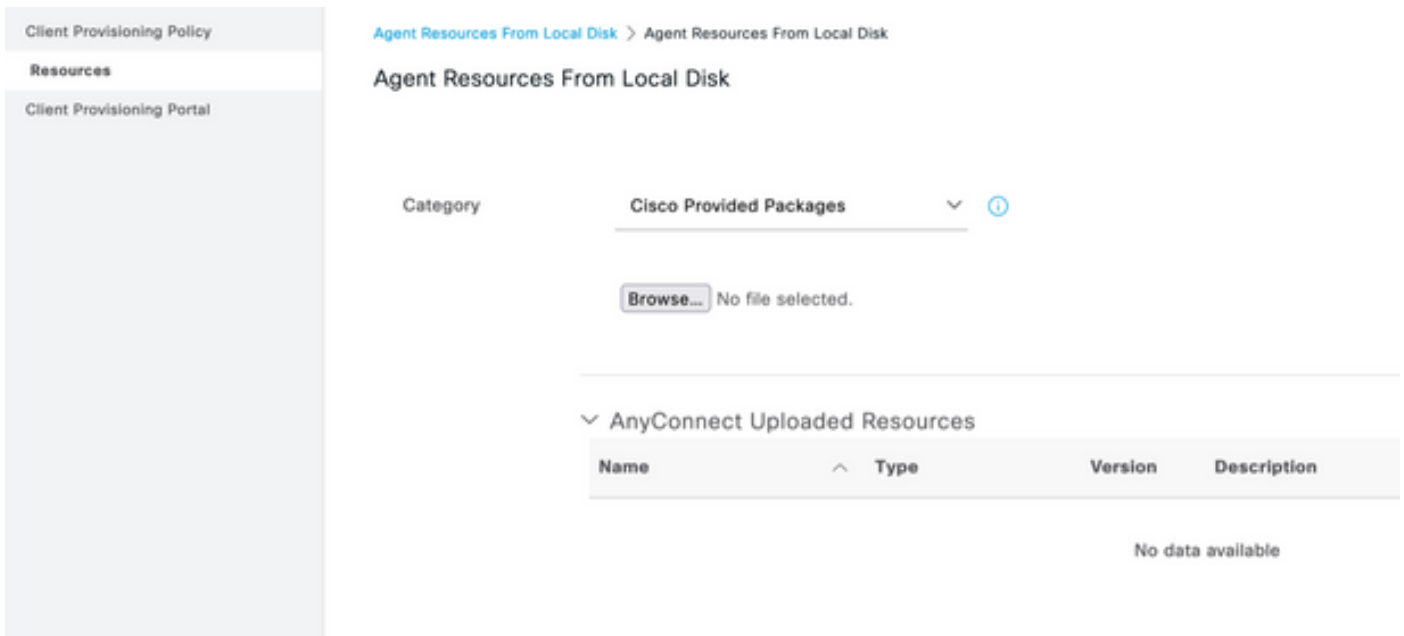
Step 3. Selecteer Add > Agent Resources van Local Disk

Resources

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

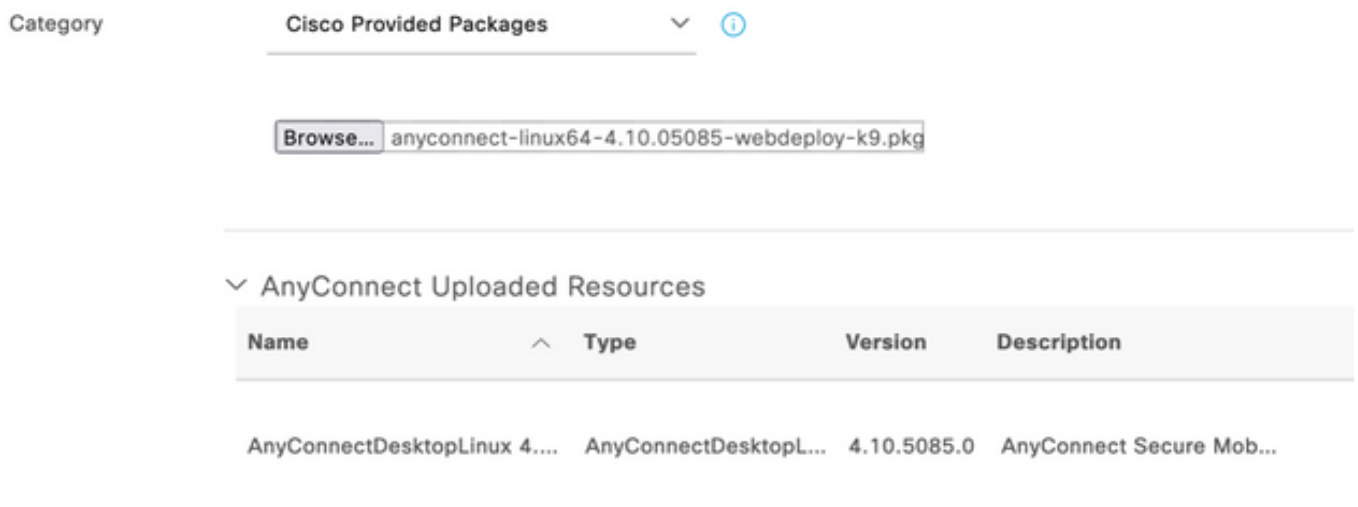
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Step 4. Selecteer Cisco de geleverde pakketten uit de vervolgkeuzelijst Category.



Stap 5. Klik op Bladeren.

Stap 6. Kies een van de AnyConnect-pakketten die u in de vorige stap hebt gedownload. Het AnyConnect-beeld wordt verwerkt en de informatie over het pakket wordt weergegeven



Stap 7. Klik op **Inzenden**. Wanneer AnyConnect is geüpload naar ISE, kunt u contact met ISE opnemen en de andere clientbronnen van Cisco.com verkrijgen.

Opmerking: Agent-bronnen omvatten modules die worden gebruikt door de AnyConnect-client die de mogelijkheid biedt om de naleving van een eindpunt te beoordelen voor een verscheidenheid aan conditiecontroles zoals Anti-Virus, Anti-Spyware, Anti-Malware, Firewall, Schijf Encryptie, Bestand, enzovoort.

Stap 8. Klik op **Add > Agent Resources van Cisco Site**. Het kost een minuut voor het venster om te bevolken aangezien ISE Cisco.com bereikt en een manifest van alle gepubliceerde middelen voor de voorziening van klanten terugvindt.

Resources

Edit + Add ^ Duplicate Delete

<input type="checkbox"/>			Version	Last Update	Description
<input type="checkbox"/>	Agent resources from Cisco site				
<input type="checkbox"/>	Agent resources from local disk	oTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	Native Supplicant Profile	ve Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	AnyConnect Configuration	oAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	AnyConnect Posture Profile	OsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	AMP Enabler Profile	oAgentlessWind...	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145

Stap 9. Selecteer de nieuwste AnyConnect-nalevingsmodules voor Linux. Daarnaast kunt u ook de nalevingsmodule voor Windows en Mac selecteren.



Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.1968.0	AnyConnect Linux Compliance Module 4.3.1968.0
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.2028.0	AnyConnect Linux Compliance Module 4.3.2028.0
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.2277.4353	AnyConnect OSX Compliance Module 4.3.2277.4353
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.2338.4353	AnyConnect OSX Compliance Module 4.3.2338.4353
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.1168...	AnyConnect Windows Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.2617...	AnyConnect Windows Compliance Module 4.3.2617.6145
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.2716...	AnyConnect Windows Compliance Module 4.3.2716.6145
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.05050	With CM: 4.3.2277.4353

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

Cancel

Save

Stap 10. Selecteer de nieuwste tijdelijke agents voor Windows en Mac.

<input checked="" type="checkbox"/>	CiscoTemporalAgentOSX 4.10.06011	Cisco Temporal Agent for OSX With CM: 4.3.2338.4353
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.10.05050	Cisco Temporal Agent for Windows With CM: 4.3.2617.614!
<input checked="" type="checkbox"/>	CiscoTemporalAgentWindows 4.10.06011	Cisco Temporal Agent for Windows With CM: 4.3.2716.614!

Stap 1. Klik op Opslaan.

Opmerking: MAC- en Windows Postconfiguraties zijn buiten het bereik van deze configuratiehandleiding.

Op dit moment hebt u alle benodigde onderdelen geüpload en bijgewerkt. Het is nu tijd om de configuratie en profielen te bouwen die nodig zijn om die onderdelen te gebruiken.

Stap 12. Klik op Add > NAC Agent of AnyConnect Posture Profile.

The screenshot shows the Cisco ISE configuration interface. At the top, there are action buttons: Edit, Add, Duplicate, and Delete. Below these is a table of installed agents. A dropdown menu is open under the 'Add' button, showing options: Agent resources from Cisco site, Agent resources from local disk, Native Supplicant Profile, AnyConnect Configuration, AnyConnect Posture Profile (highlighted), and AMP Enabler Profile.

Below the table, the configuration page for 'AnyConnect Posture Profile' is shown. The 'Name' field is set to 'LinuxACPosture'. The 'Description' field is empty. The 'Agent Behavior' section contains a table of parameters:

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	AnyConnect can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled	Display user notifications even when in Stealth mode.

De parameters die moeten worden gewijzigd zijn:

- **VLAN-detectieinterval:** Deze instelling stelt u in staat om het aantal seconden dat de module wacht tussen het controleren van VLAN-wijzigingen in te stellen. De aanbeveling is 5 seconden.
- **Ping of ARP:** Dit is de eigenlijke VLAN-wijzigingsdetectiemethode. De agent kan de standaardgateway pingelen of het ARP cache bewaken voor de standaard poort naar timeout of beide. De aanbevolen instelling is ARP.
- **Remediation-timer:** Wanneer de houding van een eindpunt onbekend is, wordt het eindpunt in een postbeoordelingsstroom geplaatst. Het verhelpen van mislukte posteringscontroles vergt tijd. De standaardtijd is 4 minuten voordat het eindpunt wordt aangegeven als niet-conform, maar de waarden kunnen variëren van 1 tot 300 minuten (5 uur). De aanbeveling bedraagt 15 minuten; dit kan echter aanpassingen vergen indien verwacht wordt dat het herstel langer zal duren .

Opmerking: Linux File Posture ondersteunt automatische herstel niet.

Raadpleeg voor een uitgebreide beschrijving van alle parameters de ISE- of AnyConnect-documentatie.

Stap 13. Agent Behavior selecteert Back-uplijst met posterijproblemen en selecteert **Kies**, selecteer de PSN/STANDAARD FQDN en selecteer **Opslaan**

Choose PSNs

Choose specific PSNs or cluster virtual IPs as the backup list to which AnyConnect sends posture state synchronization probes. You can choose a maximum of 6 entries.

List of PSNs

ise30.ciscoise.lab ×



Cancel

Select

Stap 14. Onder Posture Protocols > Discovery Host definieert het ip-adres van het PSN/Standalone knooppunt.

Stap 15. Selecteer de optie **PSN of de optie FQDN-standalone** en selecteer **Selecteer de optie Discovery Back-upserverlijst** en selecteer **Select**.

Choose PSNs

Choose specific PSNs or cluster virtual IPs as the backup list to which AnyConnect sends posture state synchronization probes. You can choose a maximum of 6 entries.

List of PSNs

ise30.ciscoise.lab x



Cancel

Select

Stap 16. Onder **Server name regels** type * om met alle servers contact op te nemen en het PSN/Standalone IP-adres te definiëren onder **call home list**. In plaats hiervan kan een jokerteken ook worden gebruikt om alle mogelijke PSN's in uw netwerk aan te passen (dat is *.acme.com).

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 ⓘ	10.52.13.173	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 ⓘ	1 PSN(s)	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 ⓘ	10.52.13.173	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	Anyconnect 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

Stap 17. Klik op **Add > AnyConnect Configuration**

Client Provisioning Policy

Resources

Client Provisioning Portal

Resources

 Edit  Add ^  Duplicate  Delete

<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk
<input type="checkbox"/>	Native Supplicant Profile
<input type="checkbox"/>	AnyConnect Configuration
<input type="checkbox"/>	AnyConnect Posture Profile
<input type="checkbox"/>	AMP Enabler Profile

* Select AnyConnect Package:

0.5085.0 ▾

*

Configuration
Name:


LinuxAnyConnect Configuration

AnyConnectDesktopWindows 4.10.5085.0
AnyConnectDesktopLinux 4.10.5085.0

Description:

Description Value Notes

* Compliance
Module

3.2028.0 

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

AnyConnect Module Selection

ISE Posture

VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

Profile Selection

* ISE Posture CPosture ▾

VPN

Network
Visibility

Customer
Feedback

LinuxACPosture

▾

Scrollt omlaag en selecteer Indienen

Stap 18. Wanneer u klaar bent met het maken van selectie, klikt u op **Inzenden**.

Stap 19. Selecteer **Workcenters > Posture > Clientprovisioning > Clientprovisioningplatforms**.

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

Client Provisioning Policy
Resources
Client Provisioning Portal

Client Provisioning Portals

You can edit and customize the default Client Provisioning portal and create additional ones

[Create](#) [Edit](#) [Duplicate](#) [Delete](#)

Client Provisioning Portal (default)

Default portal and user experience used to install the posture agents and verify compliance on user's devices

Stap 20. Onder het gedeelte **Portal Settings**, waar u de interface en poort kunt selecteren, evenals de groepen die zijn geautoriseerd om de pagina Select Workyee, SISE_Gebruikers en Domain Gebruikers te selecteren.

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available		Chosen
<input type="text"/>	<input type="button" value="➤"/>	
ALL_ACCOUNTS (default)		
GROUP_ACCOUNTS (default)		
OWN_ACCOUNTS (default)	<input type="button" value="⬅"/>	Employee

Stap 21. Zorg er onder Instellingen inlogpagina voor dat de optie **Inloggen automatisch** inschakelen is ingeschakeld

✓ Login Page Settings

Enable Auto Login ⓘ

Maximum failed login attempts before rate limiting: 5 (1 - 999)

Time between login attempts when rate limiting: 2 (1 - 999)

Include an AUP as link ▾

- Require acceptance
- Require scrolling to end of AUP

Stap 2. Kies rechtsboven de optie **Opslaan**

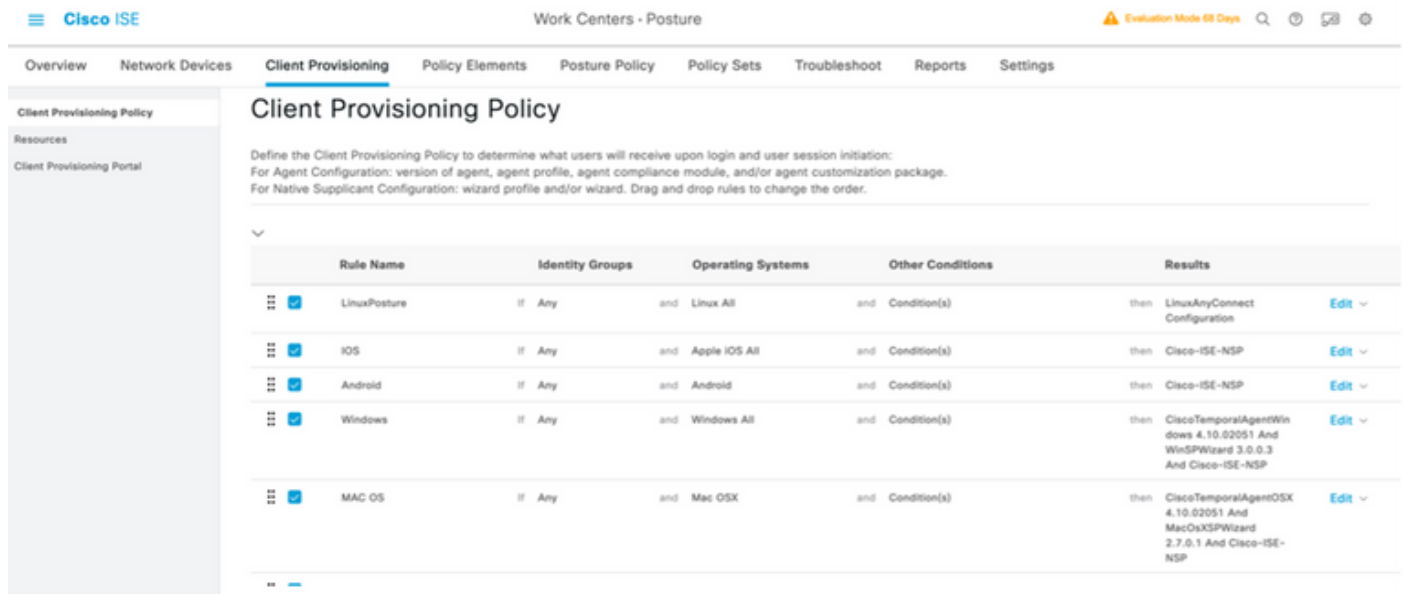
Stap 23. Selecteer **Workcenters > Posture > Clientprovisioning > Clientprovisioningbeleid**.

Stap 2. Klik op de pijl-omlaag naast de **IOS-regel** in de **CPP** en kies **Duplicaat hierboven**

Stap 25. Geef de regel **LinuxPosture** een naam

Stap 2. Kies voor de resultaten de **AnyConnect Configuration** als de agent.

Opmerking: In dit geval ziet u geen neerwaartse aanpassing van de module omdat deze is geconfigureerd als onderdeel van de AnyConnect-configuratie.



The screenshot shows the Cisco ISE interface for configuring a Client Provisioning Policy. The page title is "Client Provisioning Policy" and it includes a description: "Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order." Below this is a table of rules:

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
LinuxPosture	If Any	and Linux All	and Condition(s)	then LinuxAnyConnect Configuration
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP

Stap 27. Klik op **Gereedschap**.

Stap 28. Klik op **Opslaan**.

Elementen van het postbeleid

Stap 29. Selecteer **Workcenters > Posture > Beleidselementen > Voorwaarden > Bestand**. Selecteer **Toevoegen**.

Stap 3. Definieer **TESTFile** als de naam van de bestandstoestand en definieer de volgende waarden

File Condition

Name *	TESTFile	
Description		
* Operating System	Linux All	
Compliance Module	Any version	
* File Type	FileExistence	
* File Path	home	Testfile.csv
* File Operator	Exists	

Opmerking: Pad is gebaseerd op de bestandslocatie.

Stap 31. Selecteer Opslaan

Fileexistence. Dit bestand type conditie kijkt naar of er een bestand bestaat in het systeem waar het bestand—en dat is alles. Als deze optie geselecteerd is, is er helemaal geen zorg voor het valideren van de datums, hashes, enzovoort

Stap 3. Selecteer vereisten en kies als volgt een nieuw beleid:

Requirements										
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations	Actions				
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then	Message Text Only	Edit			
LinuxFile	for Linux All	using 4.x or later	using AnyConnect	met if TESTFile	then	Select Remediations	Edit			

Opmerking: Linux ondersteunt Berichttekst niet alleen als corrigerende actie

Vereiste onderdelen

- **Besturingssysteem:** Linux All
- **Nalevingsmodule:** 4,x
- **Posttype:** AnyConnect
- **Voorwaarden:** Naleving van modules en agents (die beschikbaar worden nadat u het besturingssysteem hebt geselecteerd)
- **Maatregelen ter verbetering van de situatie:** Wijzigingen die beschikbaar komen voor selectie nadat alle andere voorwaarden zijn geselecteerd.

Stap 3. Selecteer Workcenters > Posture > Posture Policy

Stap 34. Selecteer **Bewerken** op elk beleid en selecteer Nieuw beleid definiëren **LinuxPosturePolicy** als de naam en zorg ervoor dat u uw vereisten toevoegt die in stap 32 zijn gemaakt.

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Ma	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	than Any_AM_Installation_Ma	Edit
<input checked="" type="checkbox"/>	Policy Options	LinuxPostureP010	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxP010	Edit

Stap 35. Selecteer **Gereed** en **Opslaan**

Overige belangrijke Instellingen voor posterijen (sectie Algemene instellingen posterijen)

Posture General Settings (i)

Remediation Timer Minutes (i)

Network Transition Delay Seconds (i)

Default Posture Status (i)

Automatically Close Login Success Screen After Seconds (i)

Continuous Monitoring Interval Minutes (i)

Acceptable Use Policy in Stealth Mode

Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every Days (i)

Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

De belangrijkste instellingen in het gedeelte Instellingen voor posterijen en algemene instellingen zijn als volgt:

- **Versteltijd:** Deze instelling definieert de hoeveelheid tijd die een cliënt moet corrigeren om een verzuimde posteringsconditie te corrigeren. Er is ook een herstelltimer in de AnyConnect-configuratie; Deze timer is voor ISE en niet voor AnyConnect.
- **Standaard Poststatus:** Deze instelling geeft de status van houding aan voor apparaten zonder de postermiddel of besturingssystemen die de tijdagent niet kunnen gebruiken, zoals Linux-gebaseerde besturingssystemen.
- **Doorgaande bewaking Interval:** Deze instelling is van toepassing op de toepassing- en hardwareomstandigheden die een inventaris van het eindpunt maken. De instelling

specificeert hoe vaak AnyConnect de monitoringgegevens moet verzenden.

- **Aanvaardbaar gebruiksbeleid in Stealthwatch-modus:** De enige twee keuzes voor deze instelling zijn blokkeren of doorgaan. Blok verhindert dat klanten in de verborgen modus AnyConnect kunnen verdergaan als de AUP niet is erkend. Hiermee kan de klant van de verborgen modus doorgaan, zelfs zonder de AUP te erkennen (wat vaak de bedoeling is bij gebruik van de instelling voor de verborgen modus van AnyConnect).

Configuraties van herbeoordeling

Herbeoordelingen van de wacht zijn een cruciaal onderdeel van de postwerkstroom. U hebt gezien hoe u de AnyConnect-agent moest configureren voor een nieuwe beoordeling van de functie in het gedeelte "Posture Protocol". De agent controleert periodiek in met de PSNs die op basis van de timer in die configuratie worden gedefinieerd.

Wanneer een verzoek de PSN bereikt, bepaalt de PSN of een standpuntherbeoordeling nodig is, gebaseerd op de ISE-configuratie voor de rol van dat eindpunt. Als de cliënt de herbeoordeling doorgeeft, handhaaft de PSN de posteringsconforme staat van het eindpunt en wordt de postlease opnieuw ingesteld. Als het eindpunt niet voldoet aan de herbeoordeling, verandert de poststatus in niet-conforme, en wordt elke bestaande postlease verwijderd.

Stap 36. Selecteer **Beleidselementen > Resultaten > Vergunningverlening > Registratieprofiel**. Selecteer **Toevoegen**

Stap 37. Definieer **Wired_Redirect** als het autorisatieprofiel en stel de volgende parameters in

▼ Common Tasks

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

Client Provisioning (Posture) ▼ ACL ACL_REDIRECT_AV ▼ Value Client Provisioning Portal (def: ▼

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Auto Smart Port

Stap 38. Selecteer **Opslaan**

Stap 39. Het autorisatiebeleid configureren

Er zijn drie vooraf vastgestelde machtigingsregels voor de opstelling van een vacature:

1. De eerste is ingesteld om te passen wanneer de authenticatie slaagt en de conformiteit van een apparaat is onbekend.
2. De tweede regel komt succesvolle authenticaties met niet-conforme eindpunten aan.

Opmerking: Beide van de eerste twee regels hebben hetzelfde resultaat, namelijk het gebruik van een vooraf ingesteld autorisatieprofiel dat het eindpunt naar het Provisioning-portaal van de client omwijst.

3. De laatste regel komt overeen met succesvolle verificatie- en postconforme eindpunten en gebruikt het voorgebouwde vergunningsprofiel.

Selecteer **Policy > Policy Set** en selecteer de juiste pijl voor **bekabeld 802.1x - MAB** die in het vorige lab is gemaakt.

Stap 40. Selecteer autorisatiebeleid en kies de volgende regels

 SISE_UnknownCompliance_Redirect	AND	 Network_Access_Authentication_Passed  Compliance_Unknown_Devices  ISEAD_ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	 +	Select from list	+ 9	
 SISE_NonCompliance_Redirect	AND	 Non_Compliant_Devices  Network_Access_Authentication_Passed  ISEAD_ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	 +	Select from list	+ 0	
 SISE_Compliance_Device_Access	AND	 Compliant_Devices  Network_Access_Authentication_Passed  ISEAD_ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	 +	Select from list	+ 2	

Configuraties van de switch

Opmerking: De onderstaande configuratie verwijst naar IBNS 1.0. Er kunnen verschillen zijn voor IBNS 2.0-switches. Het omvat plaatsing in de lagedrukmodus.

```
username <admin> privilege 15 secret <password>
aaa new-model
!
aaa group server radius RAD_ISE_GRP
server name <isepsnode_1> server name ! aaa authentication dot1x default group RAD_ISE_GRP aaa
authorization network default group RAD_ISE_GRP aaa accounting update periodic 5 aaa accounting
dot1x default start-stop group RAD_ISE_GRP aaa accounting dot1x default start-stop group
RAD_ISE_GRP ! aaa server radius dynamic-author client server-key client server-key ! aaa
session-id common ! authentication critical recovery delay 1000 access-session template monitor
epm logging ! dot1x system-auth-control dot1x critical eapol ! # For Access Interfaces:
interface range GigabitEthernetx/y/z - zz
description VOICE-and-Data
switchport access vlan
switchport mode access
switchport voice vlan
ip access-group ACL_DEFAULT in
authentication control-direction in # If supported
authentication event fail action next-method
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto

# Enables periodic re-auth, default = 3,600secs
authentication periodic
# Configures re-auth and inactive timers to be sent by the server
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation restrict
mab
snmp trap mac-notification change added
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 10
dot1x timeout server-timeout 10
dot1x max-req 3
dot1x max-reauth-req 3
auto qos trust

# BEGIN - Dead Server Actions -
authentication event server dead action authorize vlan
```

```

authentication event server dead action authorize voice
authentication event server alive action reinitialize
# END - Dead Server Actions -
spanning-tree portfast
!

# ACL_DEFAULT #
! This ACL can be customized to your needs, this is the very basic access allowed prior
! to authentication/authorization. Normally ICMP, Domain Controller, DHCP and ISE
! http/https/8443 is included. Can be tailored to your needs.
!
ip access-list extended ACL_DEFAULT
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit icmp any any
permit udp any any eq tftp
permit ip any host
permit ip any host
permit tcp any host eq www
permit tcp any host eq 443
permit tcp any host eq 8443
permit tcp any host eq www
permit tcp any host eq 443
permit tcp any host eq 8443
!
# END-OF ACL_DEFAULT #
!

# ACL_REDIRECT #
! This ACL can be customized to your needs, this ACL defines what is not redirected
! (with deny statement) to the ISE. This ACL is used for captive web portal,
! client provisioning, posture remediation, and so on.
!
ip access-list extended ACL_REDIRECT_AV
remark Configure deny ip any host to allow access to
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
remark deny redirection for ISE CPP/Agent Discovery
deny tcp any host eq 8443
deny tcp any host eq 8905
deny udp any host eq 8905
deny tcp any host eq 8909
deny udp any host eq 8909
deny tcp any host eq 8443
deny tcp any host eq 8905
deny udp any host eq 8905
deny tcp any host eq 8909
deny udp any host eq 8909
remark deny redirection for remediation AV servers
deny ip any host
deny ip any host
remark deny redireciton for remediation Patching servers
deny ip any host
remark redirect any http/https
permit tcp any any eq www
permit tcp any any eq 443
!
# END-OF ACL-REDIRECT #
!
ip radius source-interface
!

```

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail
radius-server vsa send accounting
radius-server vsa send authentication
radius-server dead-criteria time 30 tries 3
!
ip http server
ip http secure-server
ip http active-session-modules none
ip http secure-active-session-modules none
!
radius server
  address ipv4  auth-port 1812 acct-port 1813
  timeout 10
  retransmit 3
  key
!
radius server
  address ipv4  auth-port 1812 acct-port 1813
  timeout 10
  retransmit 3
  key
!
aaa group server radius RAD_ISE_GRP
  server name
  server name
!
mac address-table notification change
mac address-table notification mac-move
```

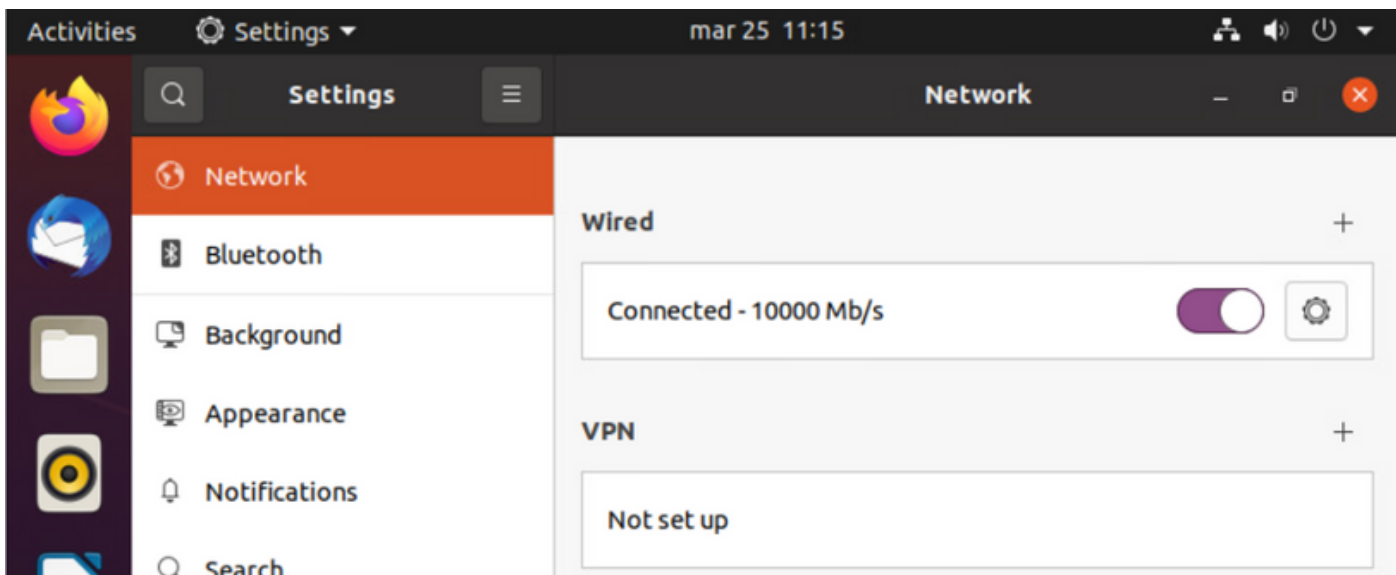
Verifiëren

ISE-verificatie:

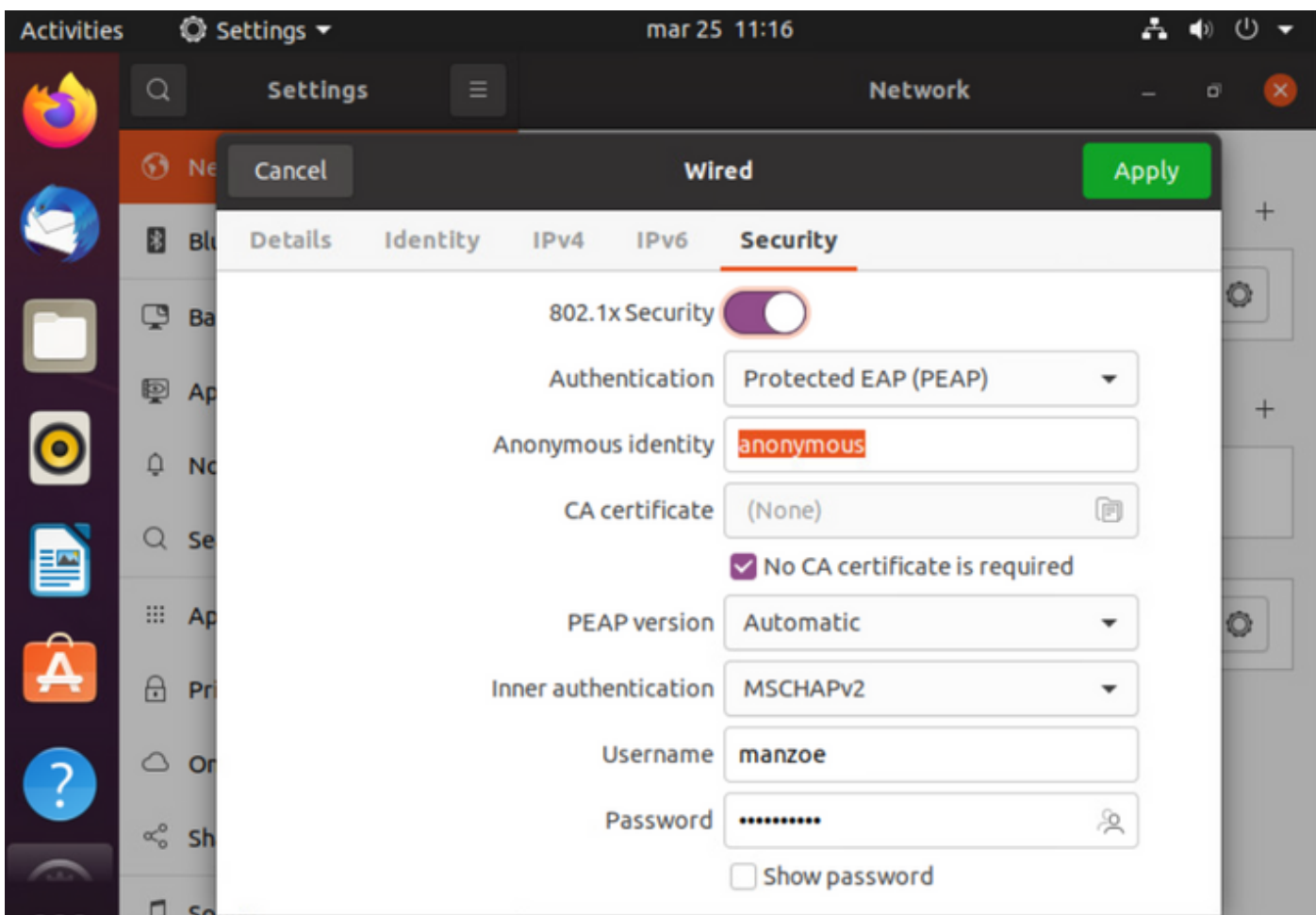
Deze paragraaf gaat ervan uit dat AnyConnect met de ISE-postmodule eerder op het Linux-systeem is geïnstalleerd.

Verifieer PC met dot1x

Stap 1. Navigeer naar netwerkinstellingen



Stap 2. Selecteer het tabblad Security en specificeer 802.1x-configuratie en gebruikersreferenties



Stap 3. Klik op "Toepassen".

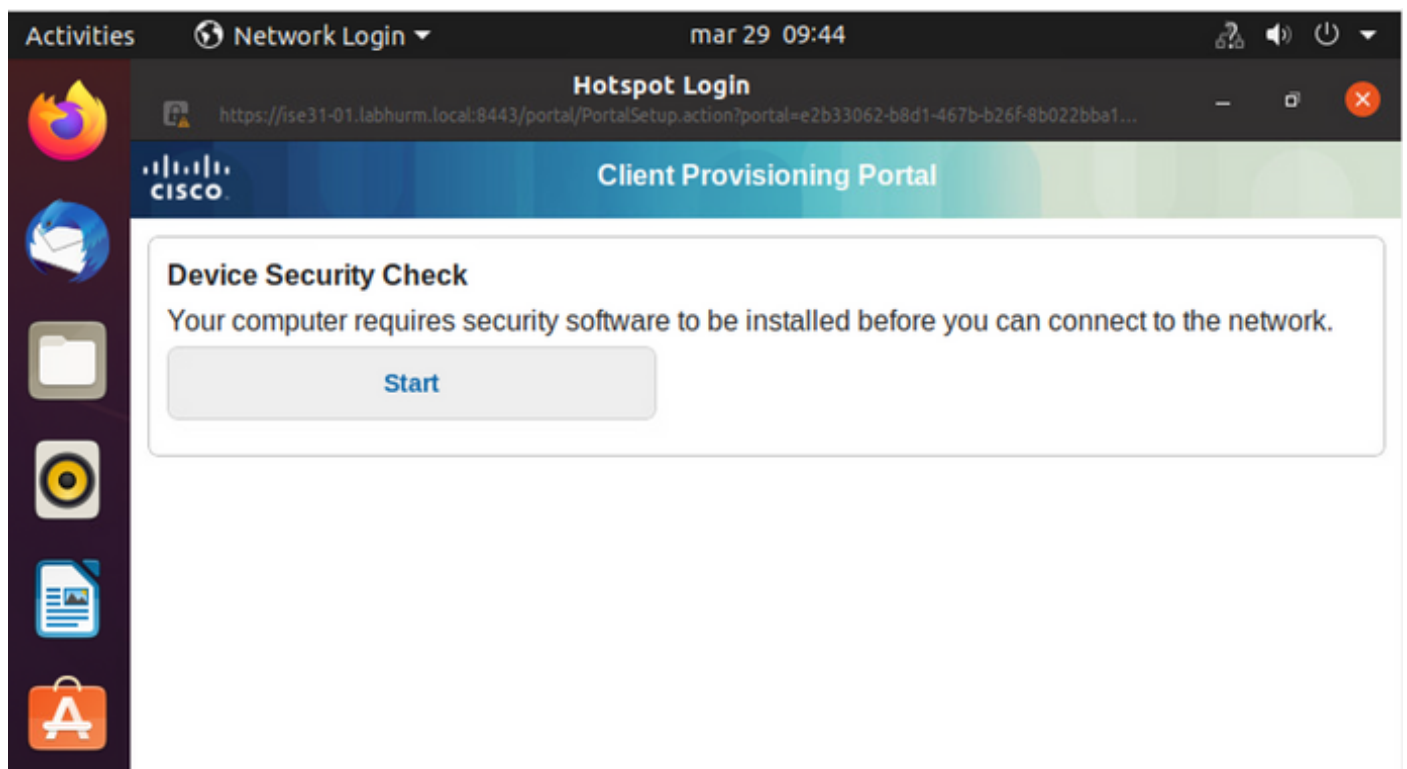
Stap 4. Sluit het Linux-systeem aan op het 802.1x-bekabelde netwerk en bevestig in het ISE-live-logbestand:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:08.2...	●		4	marcoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:48.2...	●			marcoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●			marcoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

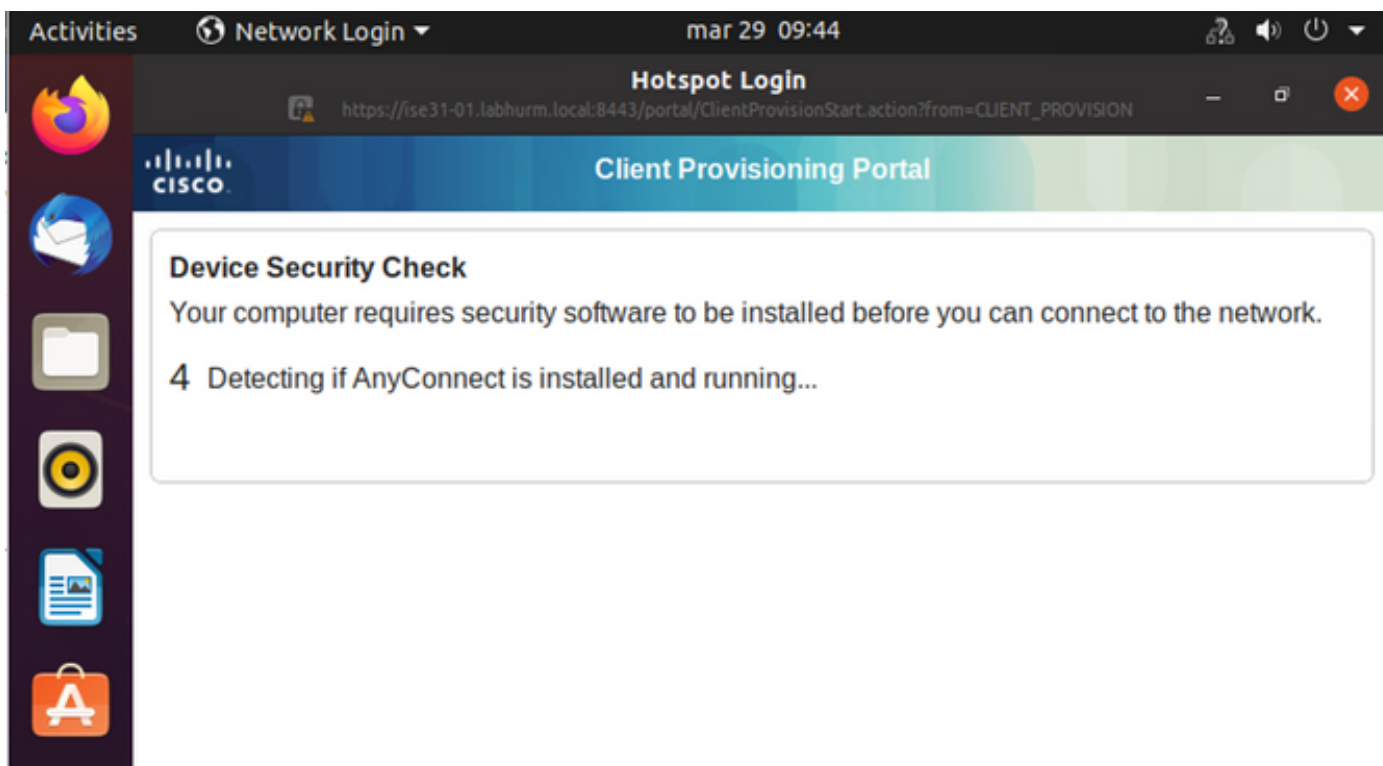
In ISE, gebruik de horizontale rolbalk om extra informatie te bekijken, zoals PSN dat de stroom of de status van de houding bediende:

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Device	Device Port	Identity Group	Posture Sta	Server
Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01

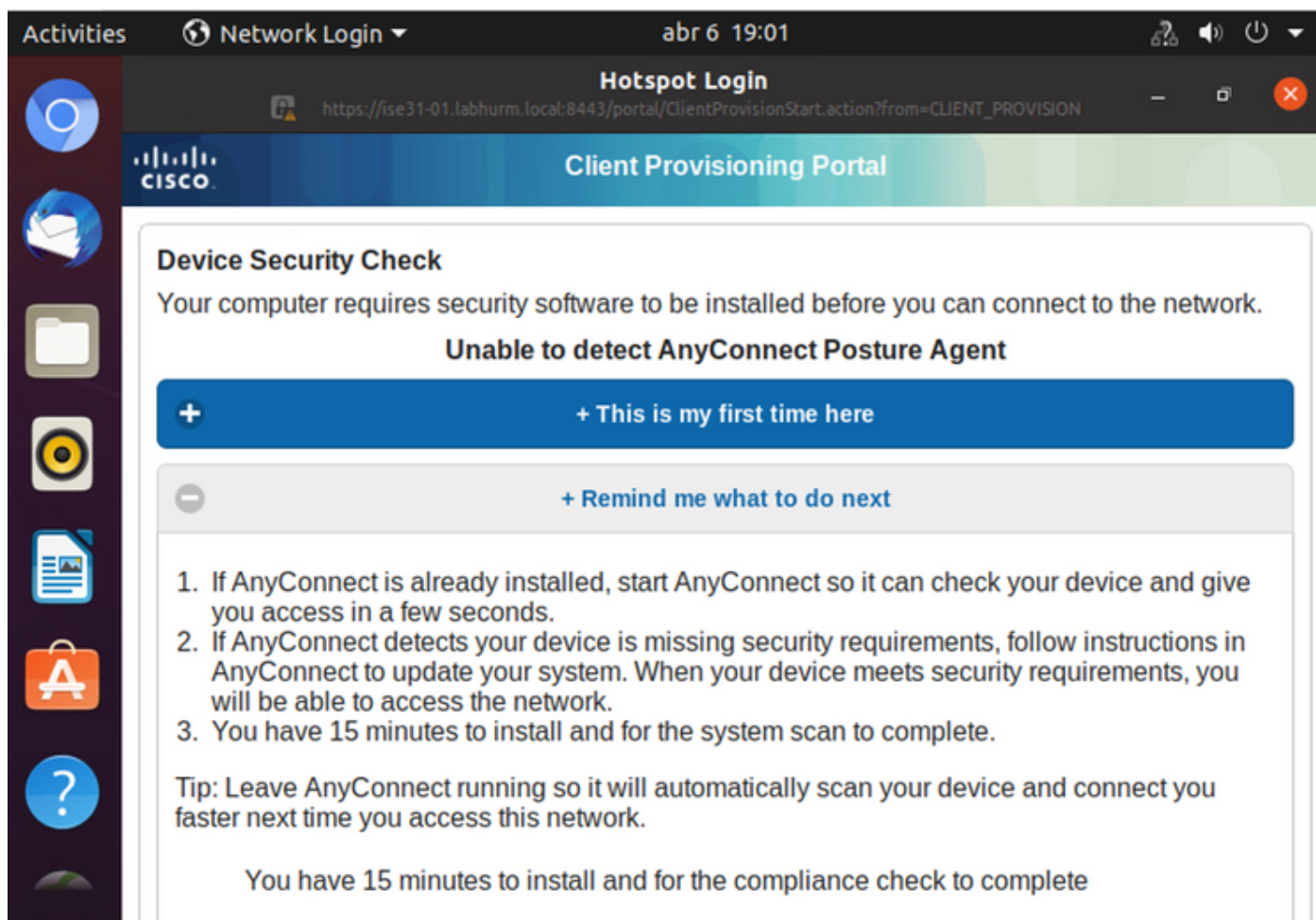
Step 5. Voor de Linux-client moet er een omleiding plaatsvinden en de client is voorzien van een provisioningportal voor postale controle en om op **"Start"** te klikken:



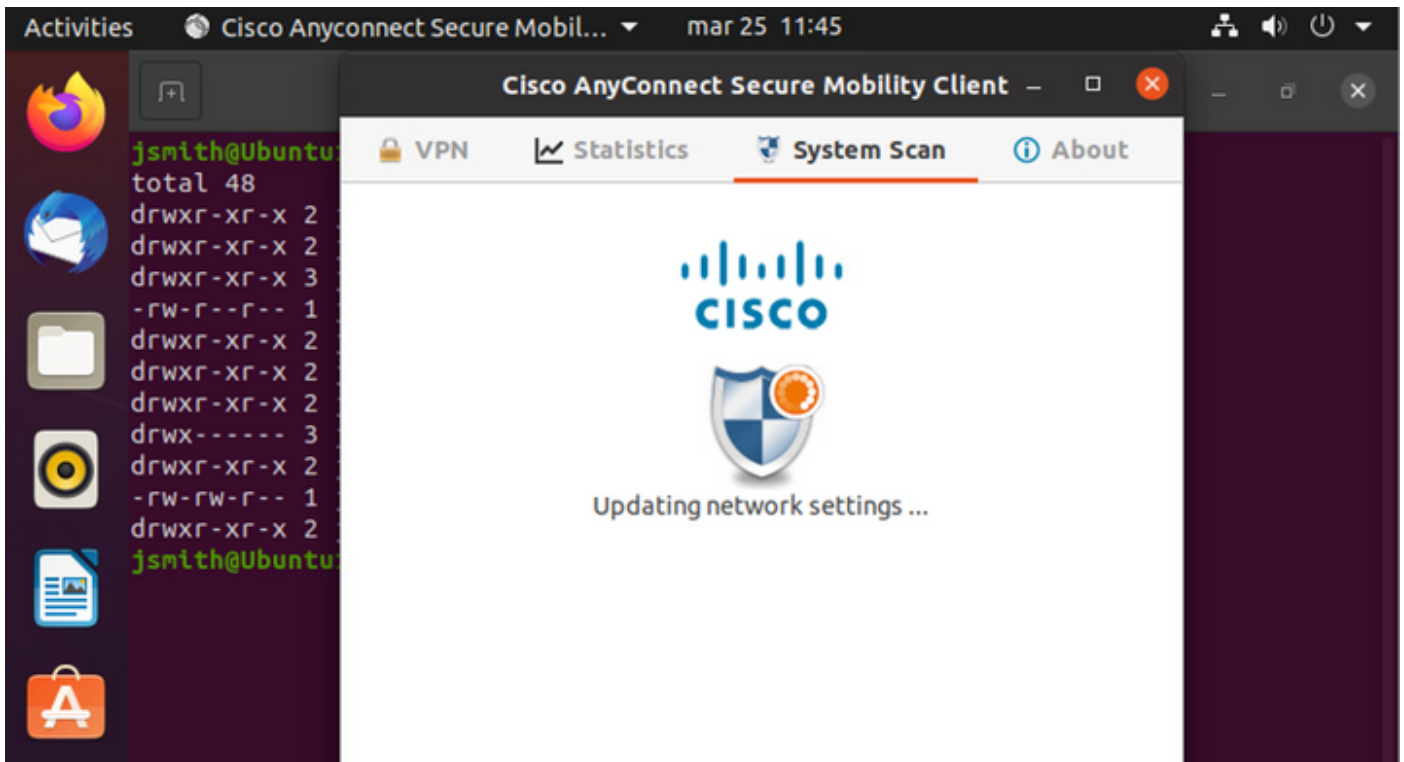
Wacht enkele seconden terwijl de connector AnyConnect probeert te detecteren:



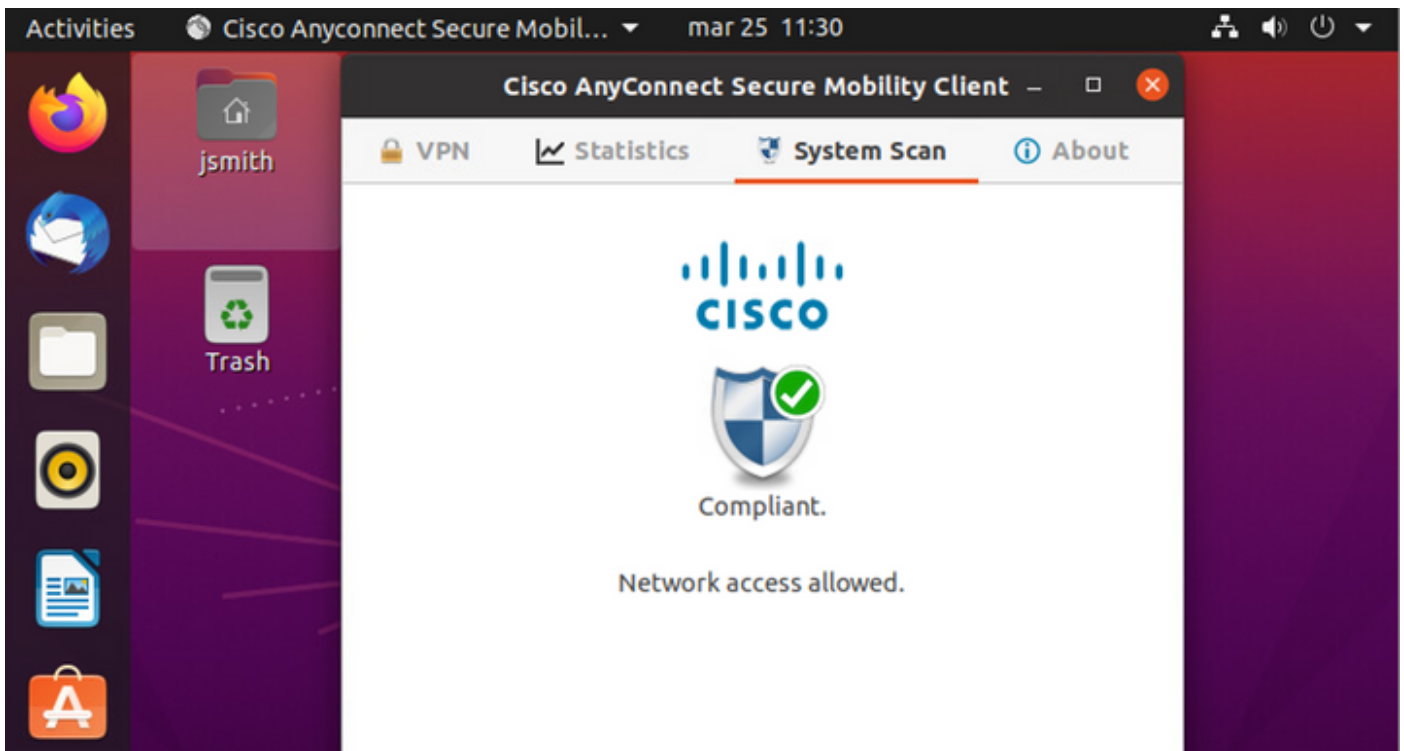
Als gevolg van een bekend voorbehoud, zelfs als AnyConnect is geïnstalleerd, detecteert het apparaat het niet. Gebruik **Alt-Tab** of het activiteitenmenu om op de AnyConnect-client te switches.

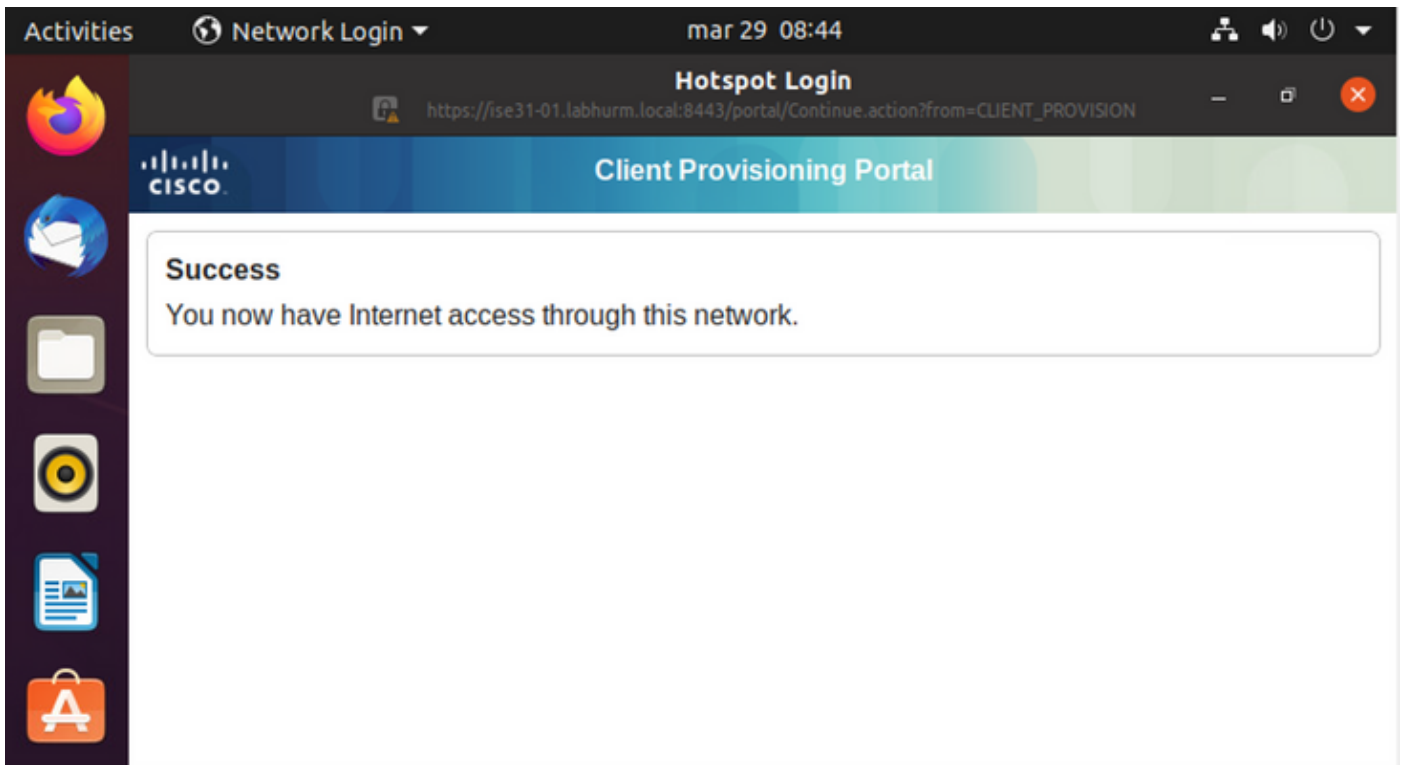


AnyConnect probeert het PSN voor uw postbeleid te bereiken en beoordeelt het eindpunt ertegen.



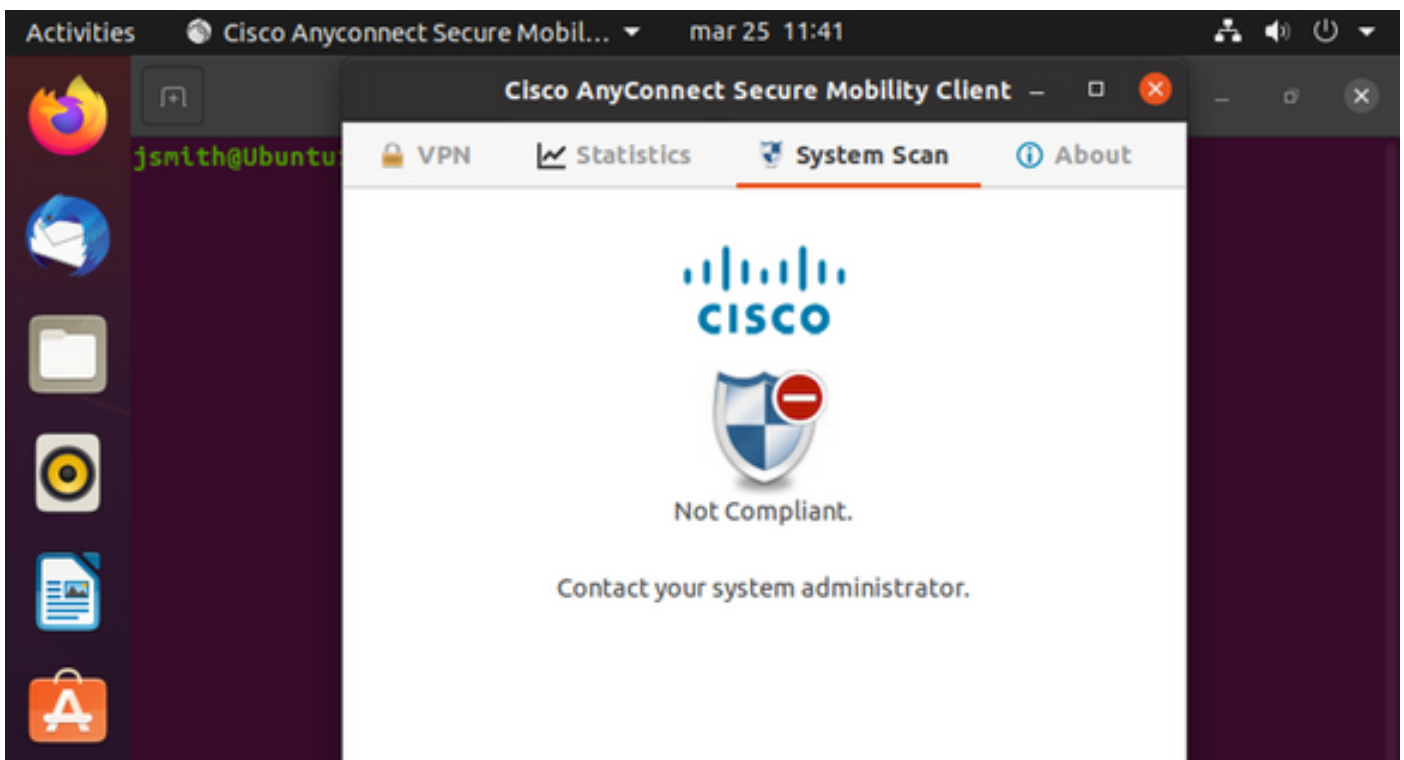
AnyConnect rapporteert de vaststelling van het postbeleid aan ISE. In dit geval, compatibel





Endpoint Profile	Authenti...	Authorizati...	Authorization P...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server
Endpoint Profile	Authenticat...	Authorization I...	Authorization Profile	IP Address	Network Device	Device Port	Identity Group	Posture Status	Server
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess	192.168.200.12				Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01

Indien het bestand echter niet bestaat, meldt de AnyConnect-posteringsmodule de vaststelling aan ISE



Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server	Mdm S
Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server	Mdm S
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51		FastEthernet1...		NonCompliant	ise31-01	
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51	Cat-3750	FastEthernet1...	Workstation	NonCompliant	ise31-01	

Opmerking: ISE FQDN moet op het Linux-systeem kunnen worden opgelost via DNS of lokaal host-bestand.

Problemen oplossen

show authentication sessions int fa1/0/35

Verrichten:

```

LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  URL Redirect ACL: ACL_REDIRECT_AV
  URL Redirect: https://ise31-01.labhurm.local:8443/portal/gateway?sessionId=C0A8C88300000010008044A&
33062-b8d1-467b-b26f-8b022bba10e7&action=cpp&token=05a438ecb872ce396c2912fecfe0d2aa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A8C88300000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

Runnable methods list:
  Method  State
  dot1x   Authc Success

```

De vergunning werd verleend:

```

LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
  Session timeout: 28800s (server), Remaining: 28739s
  Timeout action: Reauthenticate
  Idle timeout: N/A
  Common Session ID: C0A8C88300000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

Runnable methods list:
  Method  State
  dot1x   Authc Success
  mab     Not run

```

Niet compatibel, verplaatst naar quarantaineVLAN en ACL:

```
LABDEMOAC01#sh authe sess int fas1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: 777
  ACS ACL: xACSACLx-IP-DENY_ALL_IPV4_TRAFFIC-57f6b0d3
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A86E010000000000001724F
  Acct Session ID: 0x00000003
  Handle: 0x9A000000

Runnable methods list:
  Method  State
  dot1x   Authc Success
  mab     Not run
```