

# Configuration de la position de Cisco ISE 3.1 avec Linux

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configurations sur ISE](#)

[Configurations sur le commutateur](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit la procédure de configuration et d'implémentation d'une stratégie de posture de fichier pour Linux et Identity Services Engine (ISE).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AnyConnect
- Identity Services Engine (ISE)
- Linux

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Anyconnect 4.10.05085
- ISE version 3.1 P1
- Linux Ubuntu 20.04
- Commutateur Cisco Catalyst 3650. Version 03.07.05.E (15.12(3)E5)

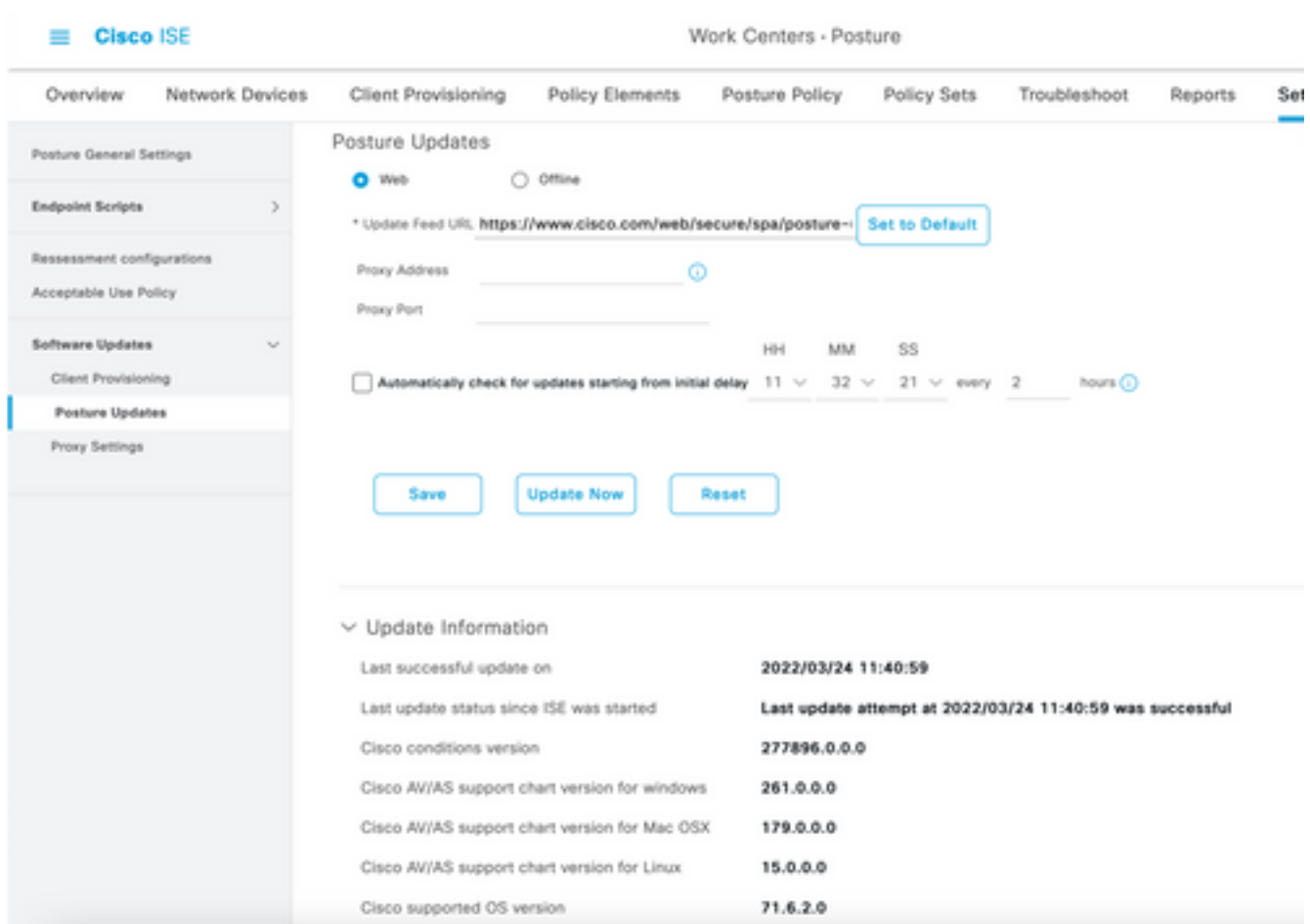
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configuration

# Configurations sur ISE

Étape 1. Mettre à jour le service de posture :

Accédez à Centres de travail > Posture > Settings > Software Updates > Posture Updates. Sélectionnez Mettre à jour maintenant et attendez la fin du processus :



Un **package fourni par Cisco** est un package logiciel que vous téléchargez à partir du site Cisco.com, tel que les packages logiciels AnyConnect. Un **package créé par le client** est un profil ou une configuration que vous avez créé en dehors de l'interface utilisateur ISE et que vous souhaitez télécharger vers ISE pour une utilisation avec évaluation de la posture. Pour cet exercice, vous pouvez télécharger le package de déploiement Web AnyConnect " anyconnect-linux64-4.10.05085-webdéploiement-k9.pkg ".

**Note:** En raison des mises à jour et des correctifs, la version recommandée peut changer. Utilisez la dernière version recommandée du site cisco.com.

Étape 2. Télécharger le package AnyConnect :

À partir du centre de travail de la position, accédez à **Provisioning client > Ressources**

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

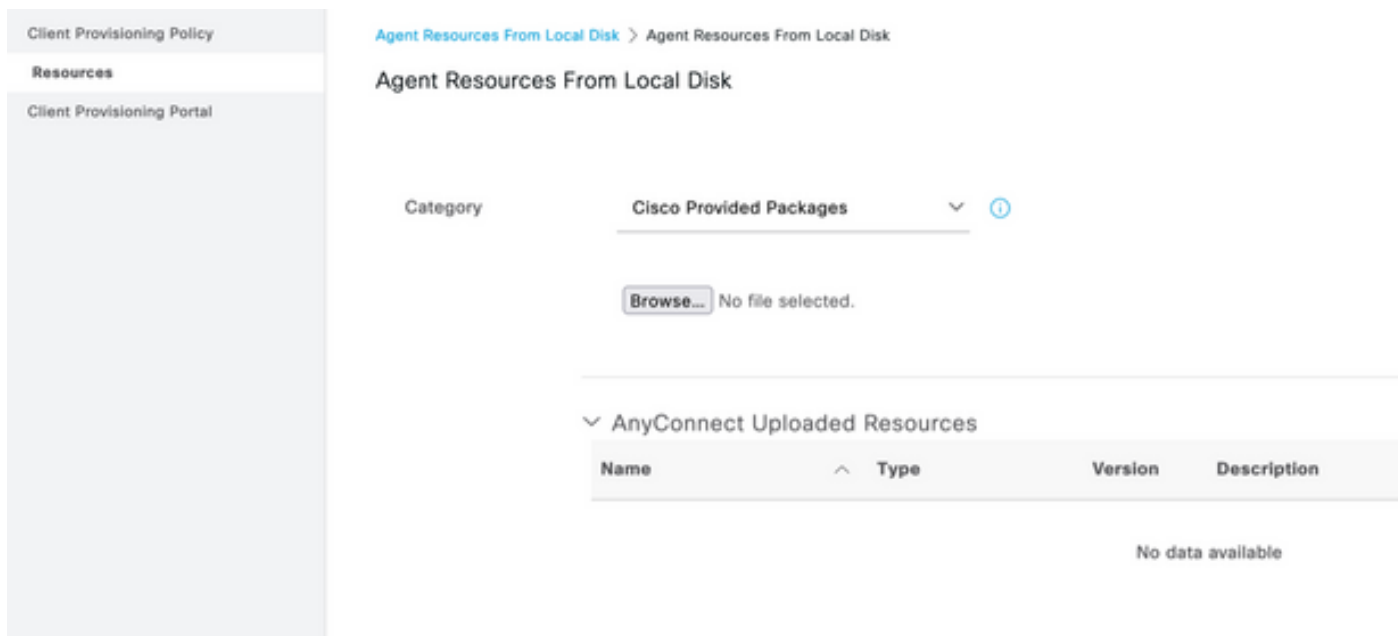
Étape 3. Sélectionnez **Ajouter > Ressources d'agent à partir du disque local**

# Resources

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

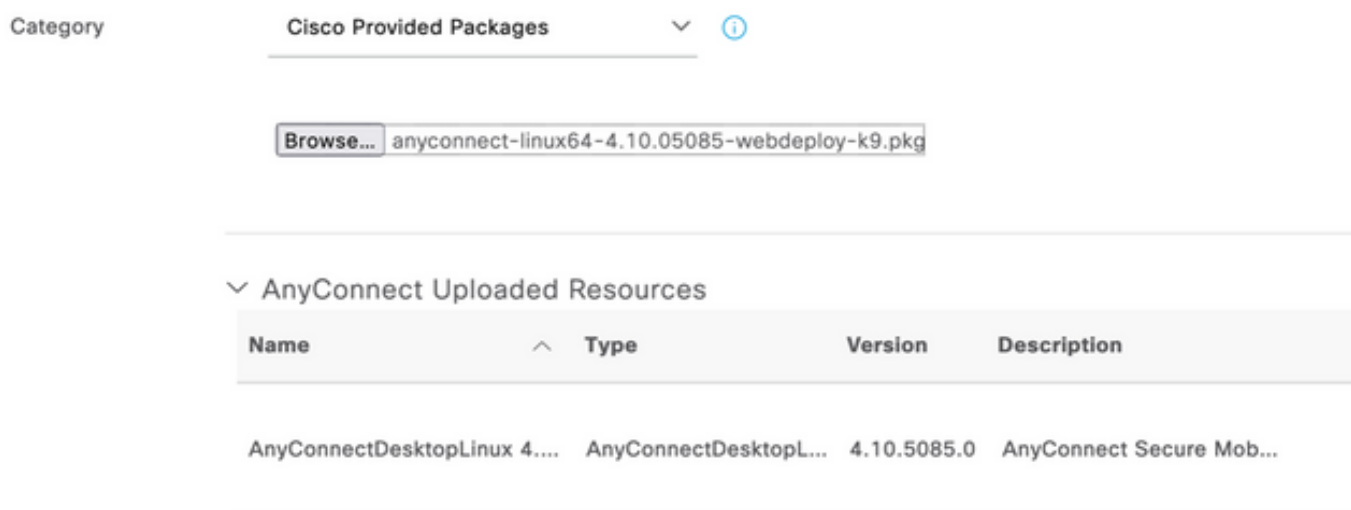
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Étape 4. Sélectionnez **Package fournis par Cisco** dans la liste déroulante **Catégorie**.



**Étape 5.** Cliquez sur Browse.

**Étape 6.** Choisissez l'un des packages AnyConnect que vous avez téléchargés à l'étape précédente. L'image AnyConnect est traitée et les informations relatives au package s'affichent



**Étape 7.** Cliquez sur Submit. Maintenant qu'AnyConnect est téléchargé vers ISE, vous pouvez avoir un contact ISE et obtenir les autres ressources client à partir de Cisco.com.

**Note:** Les ressources de l'agent comprennent des modules utilisés par le client AnyConnect qui permettent d'évaluer la conformité d'un terminal pour diverses vérifications de conditions telles que l'antivirus, l'anti-espion, l'anti-programme malveillant, le pare-feu, le chiffrement de disque, les fichiers, etc.

**Étape 8.** Cliquez sur **Add > Agent Resources from Cisco Site**. Il faut une minute pour que la fenêtre s'affiche lorsque ISE parvient à Cisco.com et récupère un manifeste de toutes les ressources publiées pour le provisionnement du client.

## 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

Étape 9. Sélectionnez les derniers modules de conformité AnyConnect pour Linux. Vous pouvez également sélectionner le module de conformité pour Windows et Mac.



## 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

Étape 10. Sélectionnez les derniers agents temporels pour Windows et 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!

## Étape 11. Cliquez sur **Save**.

**Note:** Les configurations MAC et Windows ne sont pas comprises dans ce guide de configuration.

À ce stade, vous avez téléchargé et mis à jour toutes les pièces requises. Il est maintenant temps de créer la configuration et les profils requis pour utiliser ces composants.

## Étape 12. Cliquez sur Add > NAC Agent ou sur AnyConnect Posture Profile.

The screenshot shows the Cisco ISE configuration interface. At the top, there are buttons for 'Edit', '+ Add', 'Duplicate', and 'Delete'. Below these is a table of installed agents with columns for 'Version', 'Last Update', and 'Description'. A dropdown menu is open under the '+ Add' button, listing 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. Below this is the 'Agent Behavior' section, which is 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.

Les paramètres à modifier sont les suivants :

- **Intervalle de détection VLAN** : Ce paramètre vous permet de définir le nombre de secondes que le module attend entre la recherche des modifications de VLAN. La recommandation est de 5 secondes.
- **Ping ou ARP** : Il s'agit de la méthode de détection de changement de VLAN réelle. L'agent peut envoyer une requête ping à la passerelle par défaut ou surveiller le cache ARP pour que la passerelle par défaut arrive à expiration, ou les deux. Le paramètre recommandé est ARP.
- **Minuteur de correction** : Lorsque la position d'un point de terminaison est inconnue, le point de terminaison est soumis à un flux d'évaluation de la position. Il faut du temps pour remédier aux échecs des contrôles de posture ; la durée par défaut est de 4 minutes avant de marquer le point de terminaison comme non conforme, mais les valeurs peuvent varier de 1 à 300 minutes (5 heures). La recommandation est de 15 minutes ; toutefois, cela peut nécessiter des ajustements si l'assainissement est censé prendre plus de temps.

**Note:** La position des fichiers Linux ne prend pas en charge la correction automatique.

Pour obtenir une description complète de tous les paramètres, reportez-vous à la documentation relative à la position ISE ou AnyConnect.

**Étape 13.** Comportement de l'agent sélectionnez Liste de sauvegarde des sondes de posture et sélectionnez **Choisir**, sélectionnez le nom de domaine complet PSN/autonome et sélectionnez **Enregistrer**.

## 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

**Étape 14.** Sous Posture Protocols > Discovery Host, définissez l'adresse IP du noeud PSN/autonome.

**Étape 15.** Dans la liste des serveurs de sauvegarde Discovery et sélectionnez **choisissez**, sélectionnez votre nom de domaine complet PSN ou autonome et sélectionnez **Sélectionner**.

# 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

**Étape 16.** Sous **Règles de nom de serveur**, tapez \* pour contacter tous les serveurs et définir l'adresse IP PSN/autonome dans la **liste d'appel à domicile**. Vous pouvez également utiliser un caractère générique pour faire correspondre tous les PSN potentiels de votre réseau (c'est-à-dire \*.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

**Étape 17.** Cliquez sur **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"/>	<b>AnyConnect Configuration</b>
<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
<b>AnyConnectDesktopLinux 4.10.5085.0</b>

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

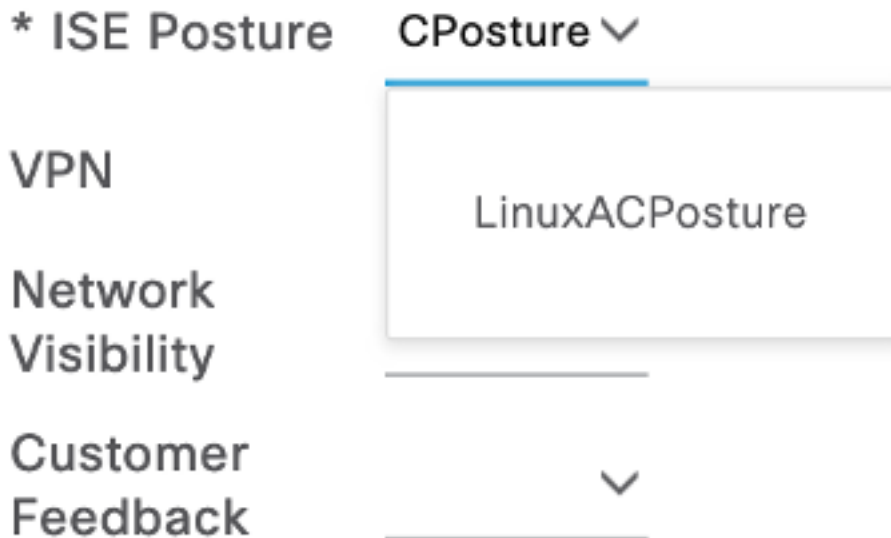
VPN

ASA Posture

Network  
Visibility

Diagnostic  
and Reporting  
Tool

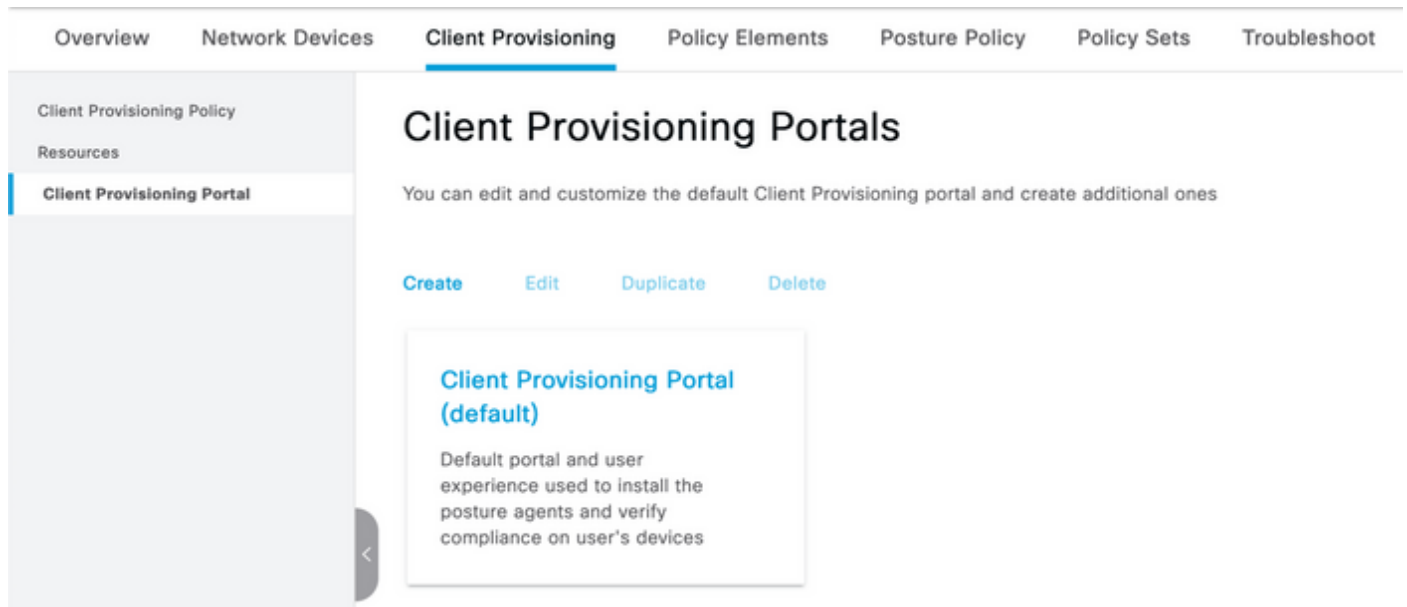
# Profile Selection



Faites défiler la liste vers le bas et sélectionnez **Soumettre**.

**Étape 18.** Lorsque vous avez terminé de sélectionner, cliquez sur **Soumettre**.

**Étape 19.** Sélectionnez **Centres de travail > Posture > Provisioning client > Portals d'approvisionnement client**.



**Étape 20.** Dans la section **Paramètres du portail**, où vous pouvez sélectionner l'interface et le port, ainsi que les groupes autorisés à la page Sélectionner un employé, SISE\_Users et Utilisateurs du domaine.

### 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="&gt;"/>	
ALL_ACCOUNTS (default)		Employee
GROUP_ACCOUNTS (default)	<input type="button" value="&lt;"/>	
OWN_ACCOUNTS (default)		

Étape 21. Sous Paramètres de la page de connexion, assurez-vous que l'option **Activer la connexion automatique** est activée

✓ Login Page Settings

Enable Auto Login (i)

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

Étape 22. Dans le coin supérieur droit, sélectionnez **Enregistrer**.

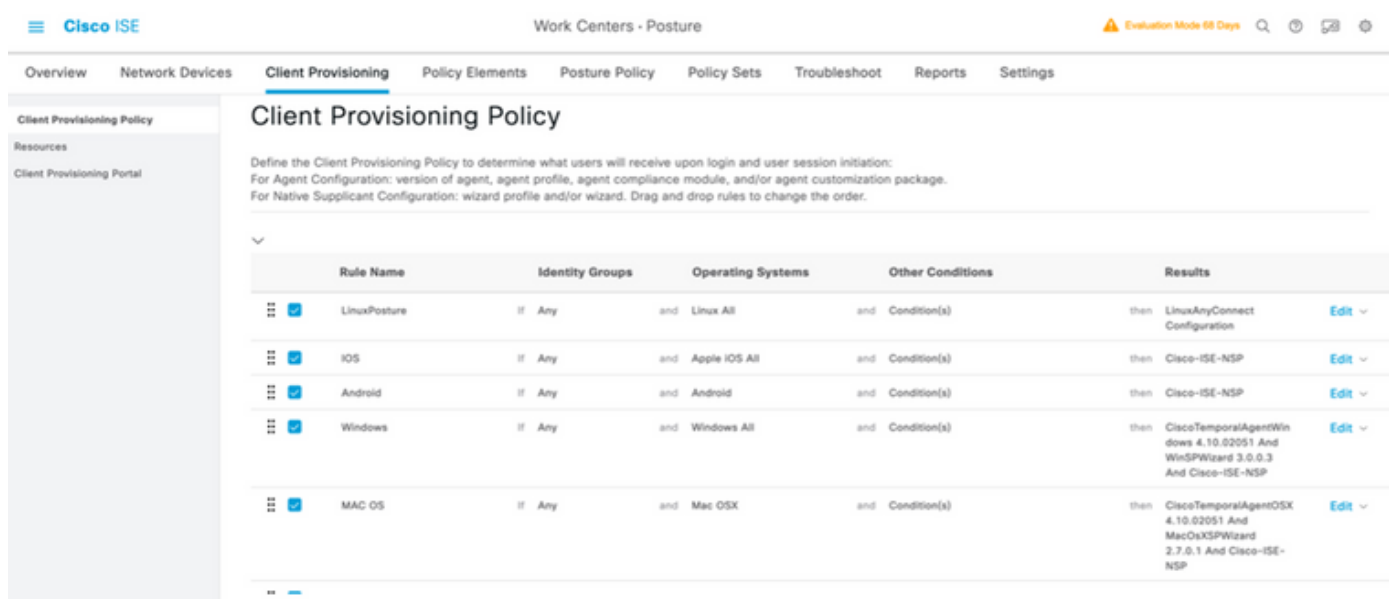
Étape 23. Sélectionnez **Centres de travail > Position > Approvisionnement client > Stratégie d'approvisionnement client.**

Étape 24. Cliquez sur la flèche vers le bas en regard de la **règle IOS** dans le **CPP** et choisissez **Dupliquer au-dessus**

Étape 25. Nommez la règle **LinuxPosture**

Étape 26. Pour Résultats, sélectionnez la **configuration AnyConnect** comme agent.

**Note:** Dans ce cas, vous ne voyez pas de liste déroulante de module de conformité car il est configuré dans le cadre de la configuration AnyConnect.



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 Supplciant 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

Étape 27. Cliquez sur **Terminé.**

Étape 28. Cliquez sur **Save.**

## Éléments de politique de positionnement

Étape 29. Sélectionnez **Centres de travail > Posture > Eléments de stratégie > Conditions > Fichier.** Sélectionnez **Ajouter.**

Étape 30. Définissez **TESTFile** comme nom de la condition de fichier et définissez les valeurs suivantes

## File Condition

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

**Note:** Le chemin d'accès est basé sur l'emplacement du fichier.

### Étape 31. Sélectionnez **Save (enregistrer)**

**FileExistence.** Ce type de condition de fichier cherche à voir si un fichier existe dans le système où il est censé exister, et c'est tout. Si cette option est sélectionnée, il n'y a aucune préoccupation quant à la validation des dates du fichier, des hachages, etc.

### Étape 32. Sélectionnez Exigences et créez une nouvelle stratégie comme suit :

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
LinuxFile	for Linux All	using 4.x or later	using AnyConnect	met if TESTFile	then Select Remediations

**Note:** Linux ne prend pas en charge le texte du message uniquement en tant qu'action corrective

### Composants requis

- **Système d'exploitation :** Tous Linux
- **Module de conformité :** 4.x
- **Type de posture :** AnyConnect
- **Modalités:** Modules et agents de conformité (disponibles après avoir sélectionné le système d'exploitation)
- **Actions de correction :** Corrections pouvant être sélectionnées après avoir choisi toutes les autres conditions.

### Étape 33. Sélectionnez Centres de travail > Posture > Posture Policy

Étape 34. Sélectionnez **Modifier** sur n'importe quelle stratégie et sélectionnez Insérer une nouvelle stratégie Définissez **LinuxPosturePolicy** comme nom et assurez-vous d'ajouter votre exigence créée à l'étape 32.

#### 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_Me	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	than Any_AM_Installation_Me	Edit
<input checked="" type="checkbox"/>	Policy Options	LinuxPostureP001	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxFile	Edit

### Étape 35. Sélectionnez Terminé et Enregistrer

Autres paramètres importants (section Paramètres généraux)

#### 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

Les paramètres importants de la section Paramètres généraux de la position sont les suivants :

- **Minuteur de correction** : Ce paramètre définit le temps nécessaire à un client pour corriger une condition de posture défaillante. Il existe également un compteur de correction dans la configuration AnyConnect ; ce compteur est pour ISE, pas pour AnyConnect.
- **État de la position par défaut** : Ce paramètre fournit l'état de position pour les périphériques sans agent de position ou les systèmes d'exploitation qui ne peuvent pas exécuter l'agent temporel, tels que les systèmes d'exploitation Linux.
- **Intervalle de surveillance continue** : Ce paramètre s'applique aux conditions d'application et

de matériel qui font l'inventaire du terminal. Ce paramètre spécifie la fréquence à laquelle AnyConnect doit envoyer les données de surveillance.

- **Politique d'utilisation acceptable en mode furtif** : Les deux seuls choix possibles pour ce paramètre sont de bloquer ou de continuer. Block empêche les clients AnyConnect en mode furtif de continuer si l'AUP n'a pas été accusé de réception. Continuer permet au client en mode furtif de continuer même sans reconnaître l'AUP (ce qui est souvent l'intention lors de l'utilisation du paramètre de mode furtif d'AnyConnect).

## Configurations de réévaluation

Les réévaluations de posture sont un élément essentiel du workflow de posture. Vous avez vu comment configurer l'agent AnyConnect pour la réévaluation de la position dans la section " du " Posture Protocol. L'agent se connecte régulièrement avec les PSN définis en fonction du compteur de cette configuration.

Lorsqu'une demande parvient au PSN, le PSN détermine si une réévaluation de la position est nécessaire, en fonction de la configuration ISE du rôle de ce point de terminaison. Si le client réussit la réévaluation, le PSN conserve l'état conforme à la posture du point d'extrémité et le bail de posture est réinitialisé. Si le point d'extrémité échoue à la réévaluation, l'état de la posture passe à Non conforme et tout bail de posture existant est supprimé.

**Étape 36.** Sélectionnez **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profil d'autorisation**. Sélectionner **Ajouter**

**Étape 37.** Définissez **Wired\_Redirect** comme profil d'autorisation et configurez les paramètres suivants

### ▼ 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

**Étape 38.** Sélectionnez **Save (enregistrer)**

**Étape 39.** Configurer les stratégies d'autorisation

Il existe trois règles d'autorisation préconfigurées pour la posture :

1. Le premier est configuré pour correspondre lorsque l'authentification réussit et la conformité d'un périphérique est inconnue.
2. La deuxième règle associe des authentifications réussies à des terminaux non conformes.

**Note:** Les deux premières règles ont le même résultat, qui est d'utiliser un profil d'autorisation préconfiguré qui redirige le point de terminaison vers le portail d'approvisionnement du client.

3. La règle finale correspond à l'authentification réussie et aux points de terminaison conformes à la position et utilise le profil d'autorisation PermitAccess prédéfini.



Sélectionnez **Policy > Policy Set** et sélectionnez la flèche droite pour **Wired 802.1x - MAB Créé** dans les travaux pratiques précédents.

**Étape 40.** Sélectionnez **Stratégie d'autorisation** et créez les règles suivantes



## Configurations sur le commutateur

**Note:** La configuration ci-dessous fait référence à IBNS 1.0. Il peut y avoir des différences pour les commutateurs compatibles IBNS 2.0. Il inclut le déploiement en mode à faible impact.

```
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
```

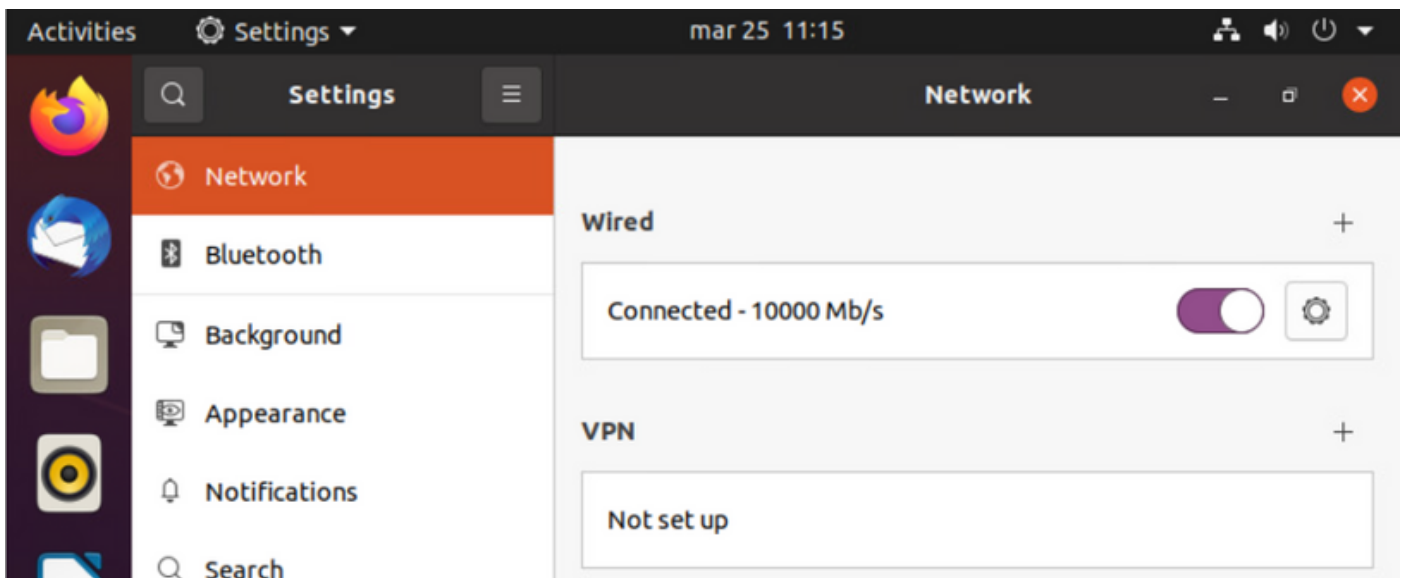
## Vérification

### Vérification ISE :

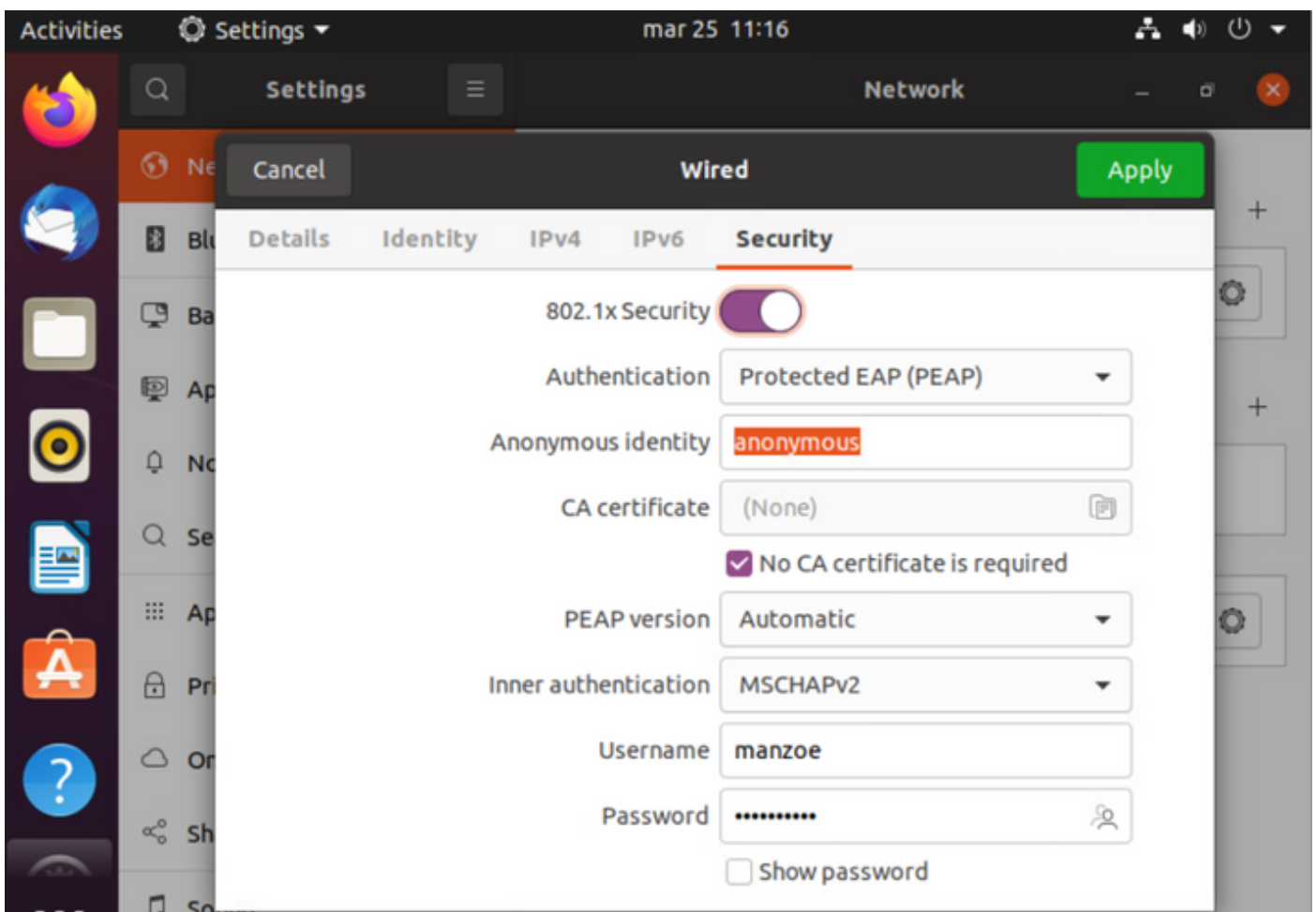
Cette section suppose qu'AnyConnect avec le module ISE a déjà été installé sur le système Linux.

### Authentifier le PC à l'aide de dot1x

#### Étape 1. Accéder aux paramètres réseau



Étape 2. Sélectionnez l'onglet Sécurité et fournissez la configuration 802.1x et les informations d'identification de l'utilisateur.



Étape 3. Cliquez sur “ Appliquer ”.

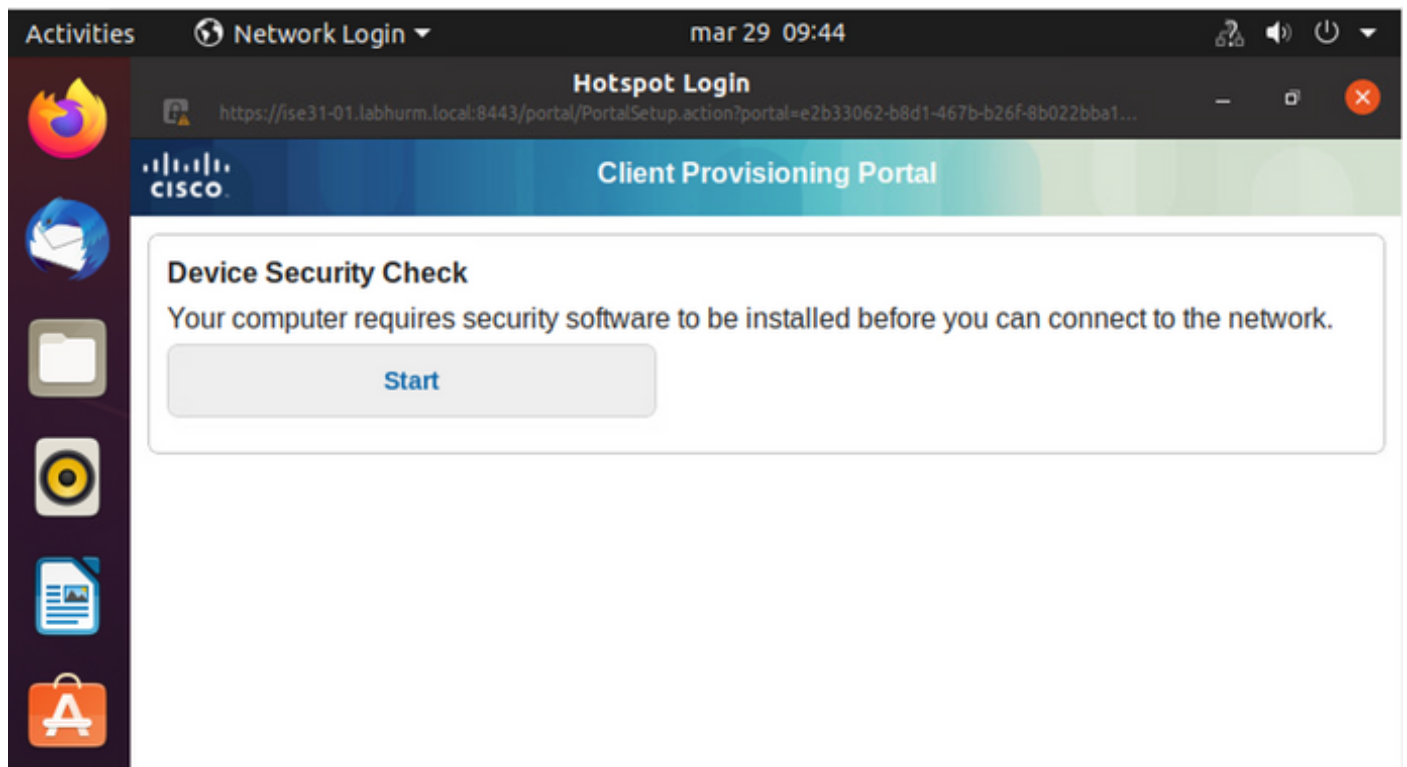
Étape 4. Connectez le système Linux au réseau câblé 802.1x et validez dans le journal ISE en direct :

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...	<span style="color: blue;">●</span>		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...	<span style="color: green;">●</span>			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...	<span style="color: green;">●</span>			marcoe	00-0C-29-44-03-8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

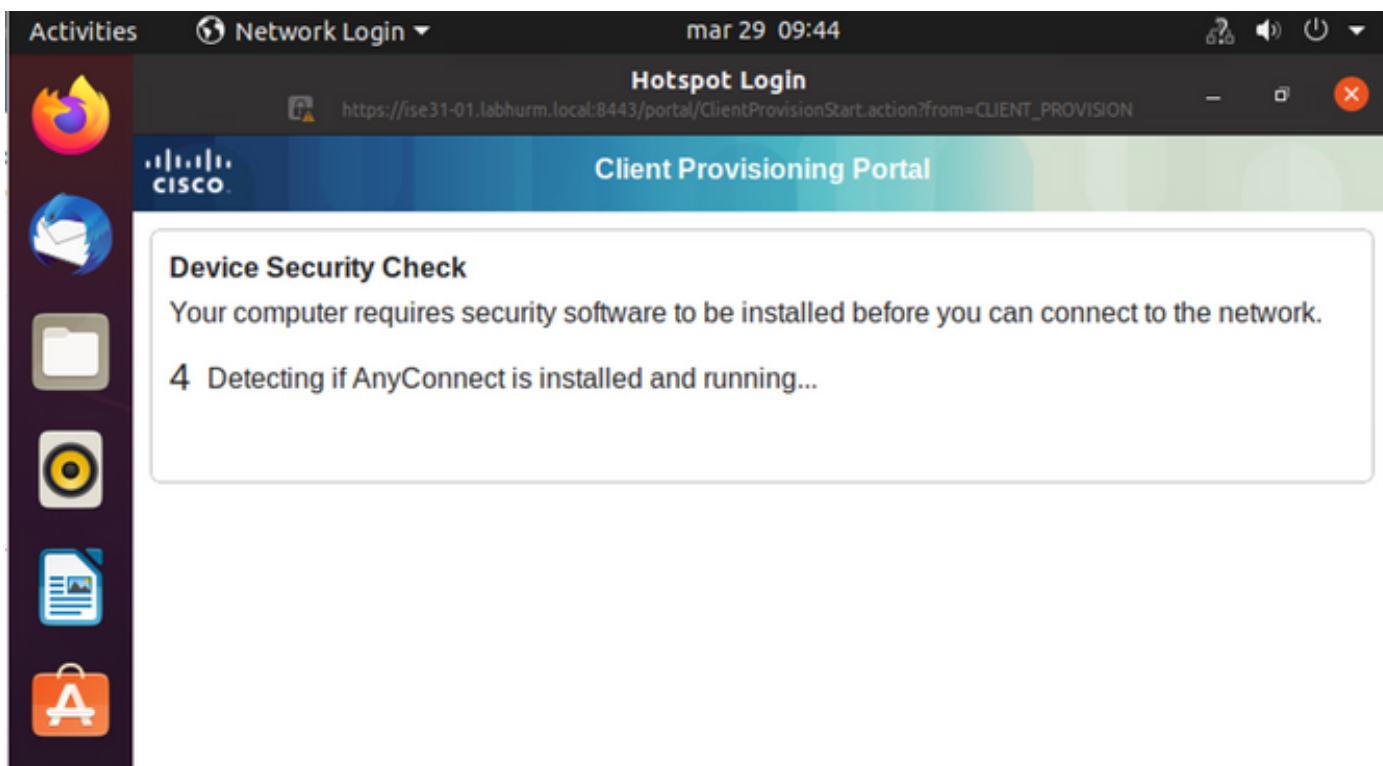
Dans ISE, utilisez la barre de défilement horizontale pour afficher des informations supplémentaires, telles que le PSN qui a servi le flux ou l'état de la position :

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

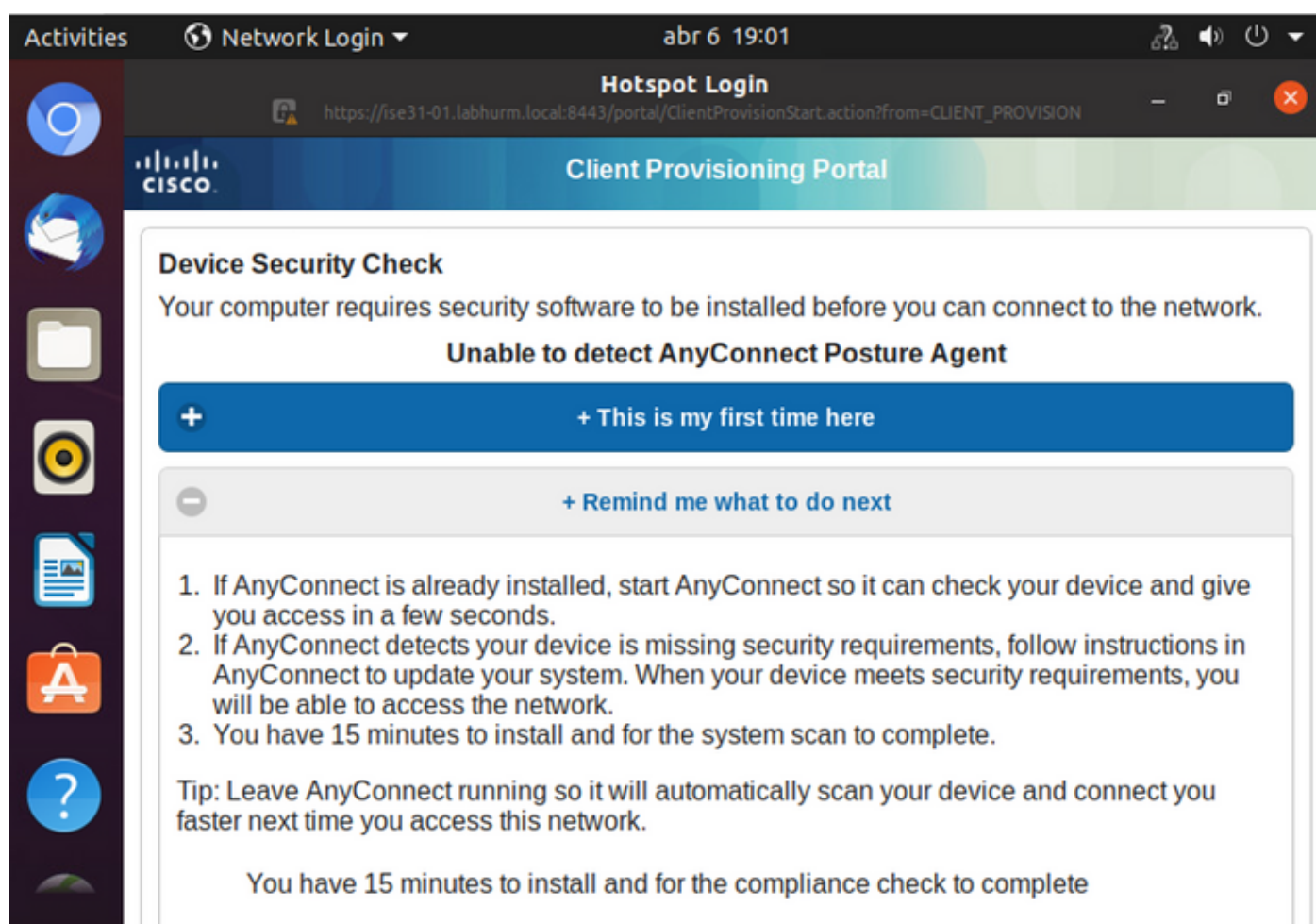
**Étape 5.** Sur le client Linux, une redirection doit se produire, et elle présente le portail d'approvisionnement du client indiquant que la vérification de la position a lieu et cliquez sur " Démarrer " :



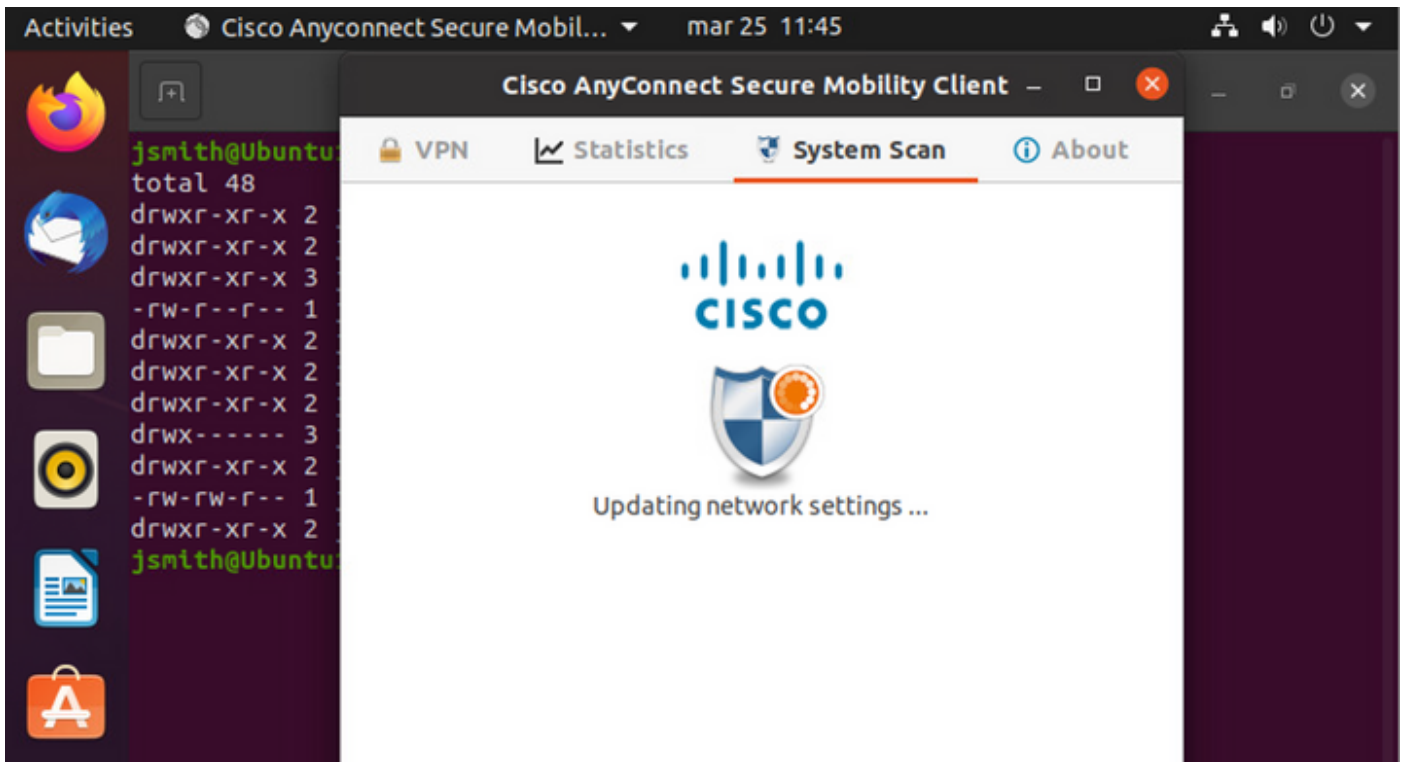
Patientez quelques secondes pendant que le connecteur tente de détecter AnyConnect :



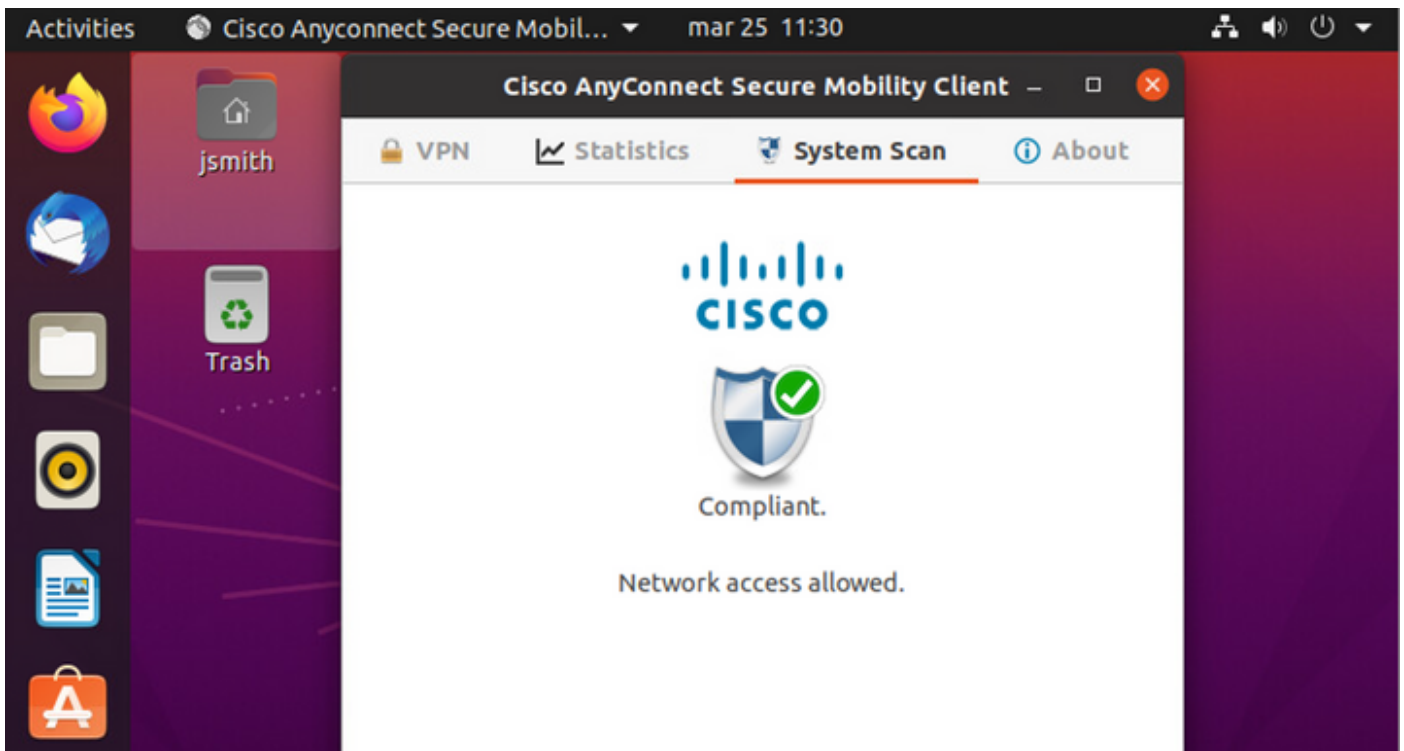
En raison d'une mise en garde connue, même si AnyConnect est installé, il ne le détecte pas. Utilisez **Alt-Tab** ou le menu **Activités** pour basculer vers le client AnyConnect.

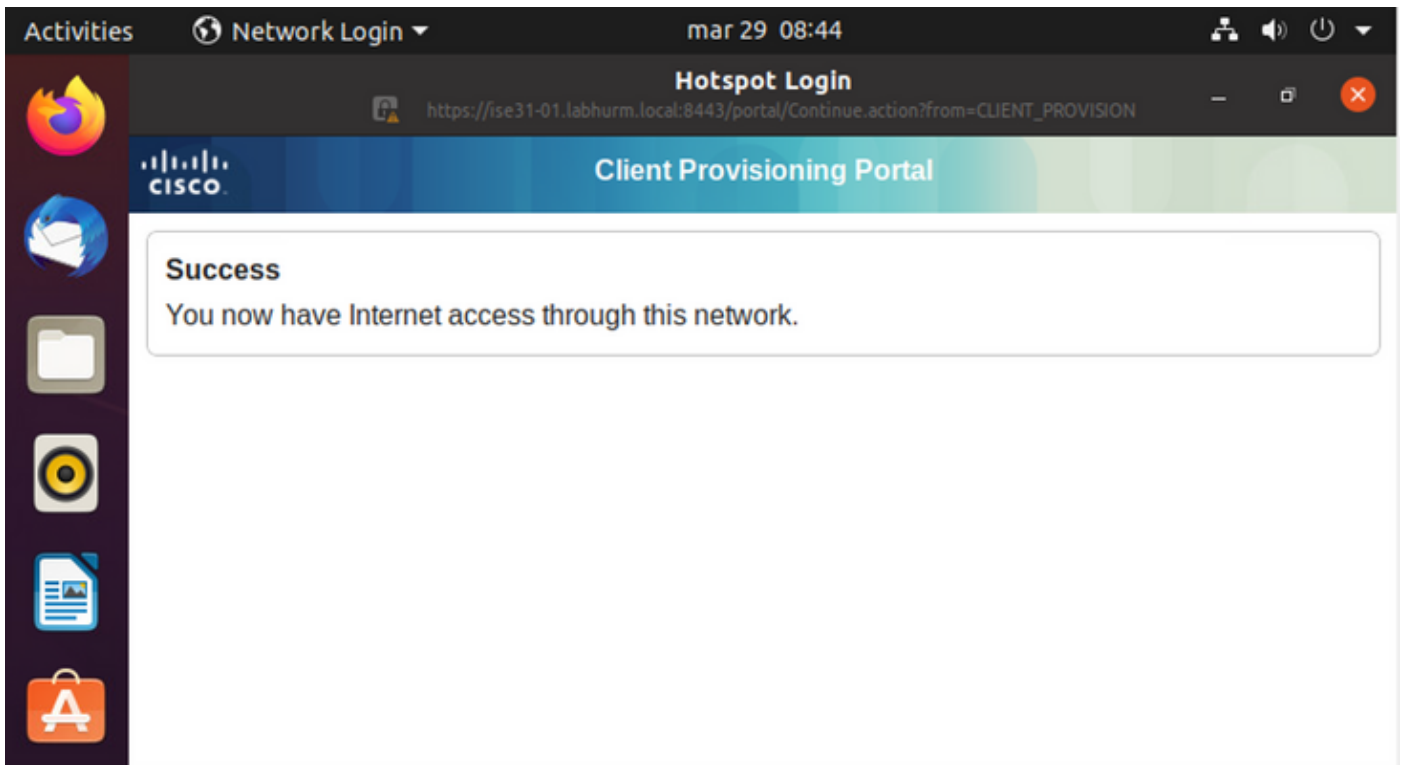


AnyConnect tente d'atteindre le PSN pour la politique de posture et d'évaluer le terminal par rapport à celui-ci.



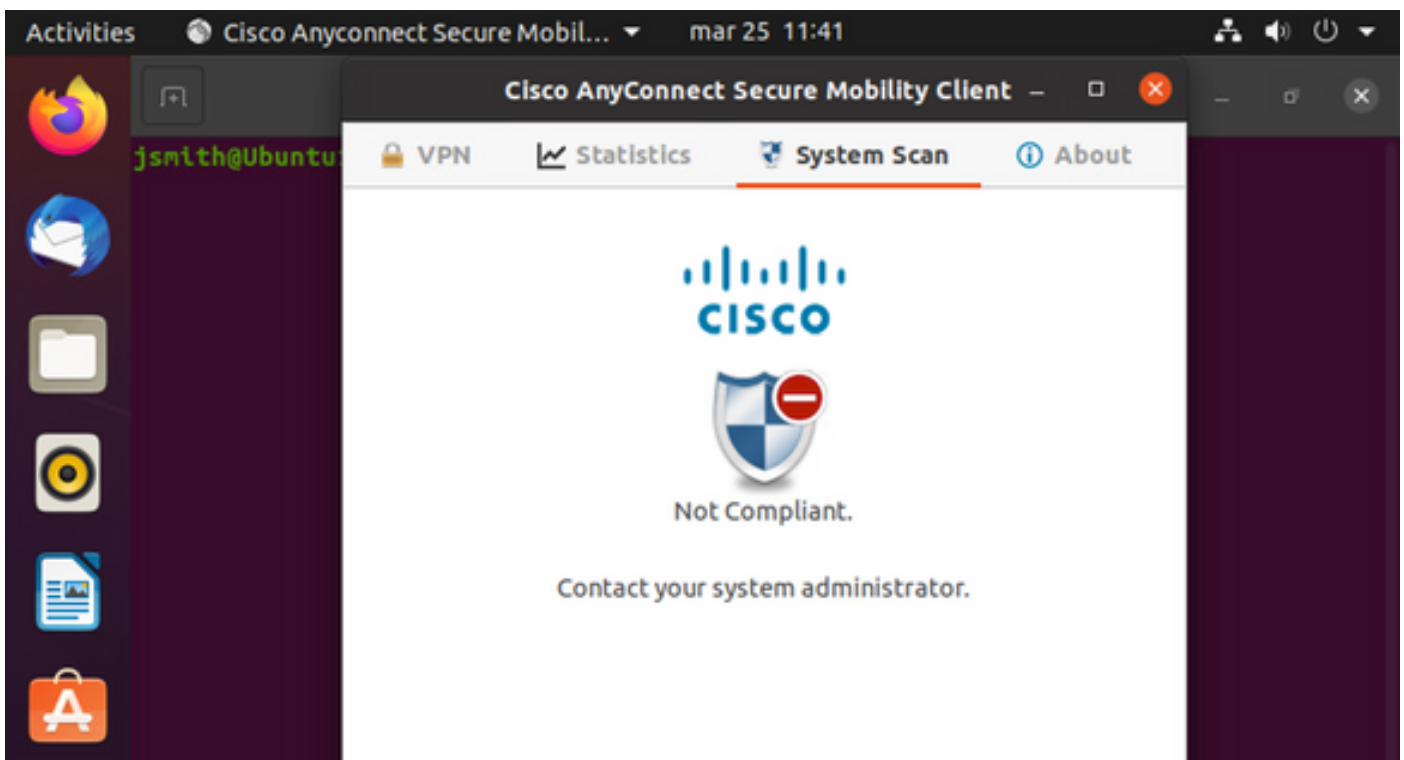
AnyConnect renvoie à ISE sa détermination de la politique de posture. Dans ce cas, conforme





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 Merak...	Wired Merak...	PermitAccess	192.168.200.12				Compliant	ise31-01
Ubuntu-Workstation	Wired Merak...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01
Ubuntu-Workstation	Wired Merak...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01

D'autre part, si le fichier n'existe pas, le module de posture AnyConnect signale la détermination à 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	

**Note:** Le FQDN ISE doit pouvoir être résolu sur le système Linux via le fichier DNS ou hôte local.

## Dépannage

```
show authentication sessions int fa1/0/35
```

Rediriger en place :

```
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&p
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
```

Autorisation réussie :

```
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
```

Non conforme, déplacé vers VLAN et ACL de quarantaine :

```
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
```