

Configuración de Cisco ISE 3.1 Posture con Linux

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones en ISE](#)

[Configuraciones en el switch](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para configurar e implementar una política de estado de archivo para Linux y Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- AnyConnect
- Identity Services Engine (ISE)
- Linux

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Anyconnect 4.10.05085
- ISE versión 3.1 P1
- Linux Ubuntu 20.04
- Switch Cisco Catalyst 3650. Versión 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuraciones en ISE

Paso 1. Actualizar servicio de estado:

Vaya a **Centros de Trabajo > Estado > Configuración > Actualizaciones de Software > Actualizaciones de Estado**. Seleccione **Actualizar ahora** y espere a que finalice el proceso:

The screenshot shows the Cisco ISE interface for configuring Posture Updates. 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:

- Mode: Web, Offline
- Update Feed URL: <https://www.cisco.com/web/secure/spa/posture-...> (with a 'Set to Default' button)
- Proxy Address: [Empty field]
- Proxy Port: [Empty field]
- Automatic check for updates: Automatically check for updates starting from initial delay: 11:32:21 every 2 hours

Buttons at the bottom: Save, Update Now, Reset.

Update Information section:

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

Un **paquete proporcionado por Cisco** es un paquete de software que se descarga desde el sitio Cisco.com, como los paquetes de software de AnyConnect. Un **paquete creado por el cliente** es un perfil o una configuración que ha creado fuera de la interfaz de usuario de ISE y que desea cargar en ISE para su uso con la evaluación de estado. Para este ejercicio, puede descargar el paquete de implementación web de AnyConnect "anyconnect-linux64-4.10.05085-webDeploy-k9.pkg".

Nota: Debido a las actualizaciones y los parches, la versión recomendada puede cambiar. Utilice la versión recomendada más reciente del sitio cisco.com.

Paso 2. Cargue el paquete AnyConnect:

Desde el centro de trabajo de estado, vaya a **Aprovisionamiento de cliente > Recursos**

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

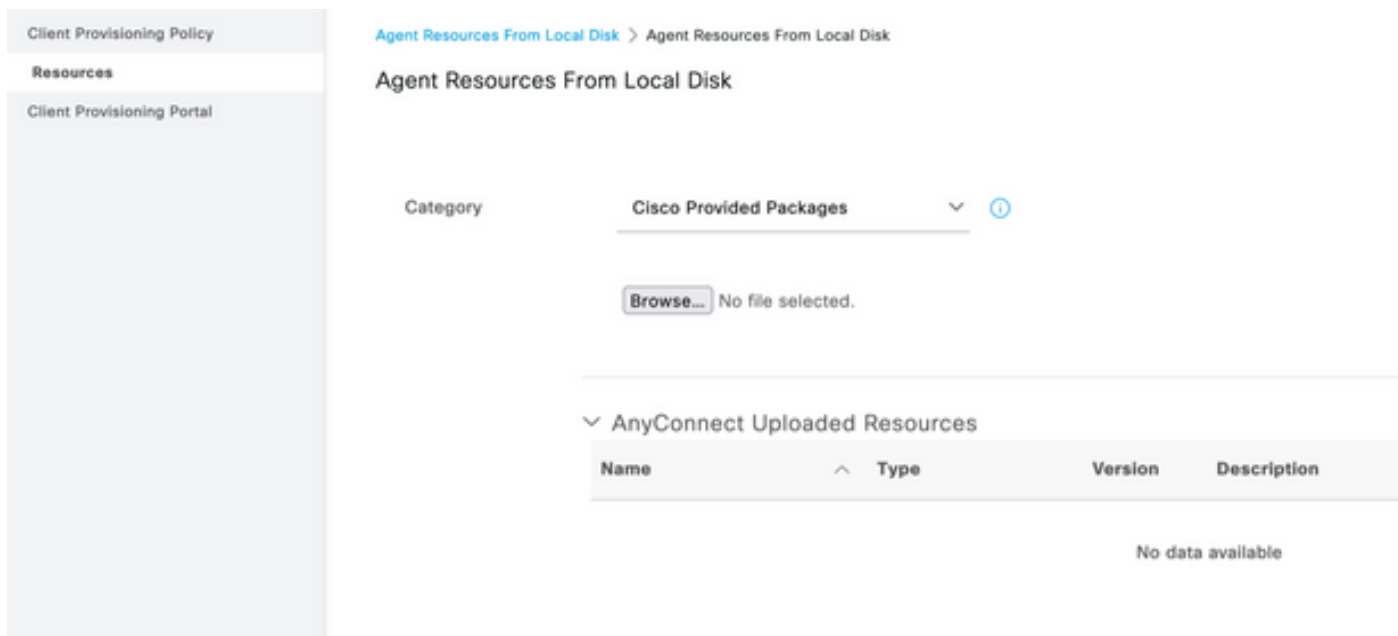
Paso 3. Seleccione **Agregar > Recursos de agente en Disco local**

Resources

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

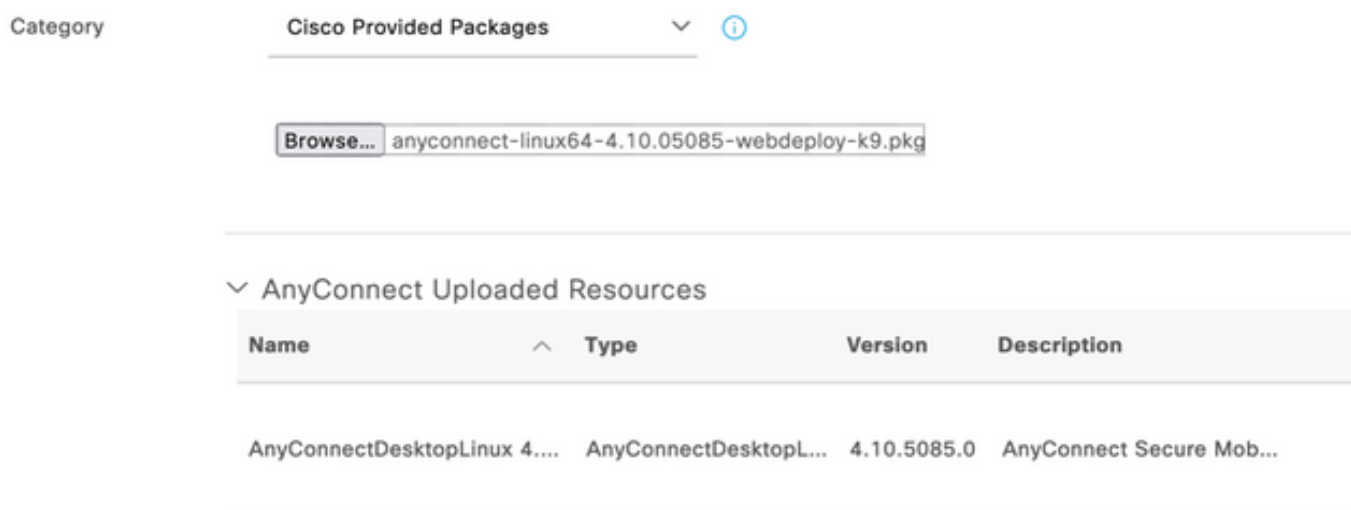
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Paso 4. Seleccione **Cisco Provided Packages** en el menú desplegable Category (Categoría).



Paso 5. Haga clic en Examinar.

Paso 6. Elija uno de los paquetes de AnyConnect que descargó en el paso anterior. Se procesa la imagen de AnyConnect y se muestra la información sobre el paquete



Paso 7. Haga clic en Submit (Enviar). Ahora que AnyConnect se carga en ISE, puede tener contacto con ISE y obtener los otros recursos de cliente de Cisco.com.

Nota: Los recursos de agente incluyen los módulos utilizados por AnyConnect Client que proporcionan la capacidad de evaluar el cumplimiento de un terminal para una variedad de comprobaciones de condiciones, como antivirus, antispyware, antimalware, firewall, cifrado de disco, archivo, etc.

Paso 8. Haga clic en Agregar > Recursos de agente desde el sitio de Cisco. La ventana tardará un minuto en completarse, ya que ISE se pondrá en contacto con Cisco.com y recuperará un manifiesto de todos los recursos publicados para el aprovisionamiento de clientes.

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

Paso 9. Seleccione los últimos módulos de cumplimiento de AnyConnect para Linux. Además, también puede seleccionar el módulo de cumplimiento para Windows y 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

Paso 10. Seleccione los agentes temporales más recientes para Windows y 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!

Paso 11. Click Save.

Nota: Las configuraciones de estado de MAC y Windows están fuera del alcance de esta guía de configuración.

En este momento, ha cargado y actualizado todas las piezas necesarias. Ha llegado el momento de crear la configuración y los perfiles necesarios para utilizar esos componentes.

Paso 12. Haga clic en Add > NAC Agent o AnyConnect Status 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 agent profiles with columns for Name, Version, Last Update, and Description. A dropdown menu is open over the table, 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 form for 'AnyConnect Posture Profile' is visible. The 'Name' field is set to 'LinuxACPosture'. The 'Description' field is empty. Below this is the 'Agent Behavior' section, which 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.

Los parámetros que deben modificarse son:

- **Intervalo de detección de VLAN:** Esta configuración le permite establecer el número de segundos que el módulo espera entre sondeos para los cambios de VLAN. La recomendación es de 5 segundos.
- **Ping o ARP:** Este es el método de detección de cambio de VLAN real. El agente puede hacer ping al gateway predeterminado o monitorear la memoria caché ARP para que la entrada del gateway predeterminado se detenga o ambas. La configuración recomendada es ARP.
- **Temporizador de remediación:** Cuando se desconoce el estado de un terminal, éste pasa por un flujo de evaluación de estado. Se tarda tiempo en remediar los errores en las comprobaciones de estado; el tiempo predeterminado es 4 minutos antes de marcar el terminal como no conforme, pero los valores pueden oscilar entre 1 y 300 minutos (5 horas). La recomendación es de 15 minutos; sin embargo, esto puede requerir ajustes si se espera que la remediación tome más tiempo.

Nota: El estado del archivo Linux no admite la corrección automática.

Para obtener una descripción completa de todos los parámetros, consulte la documentación de estado de ISE o AnyConnect.

Paso 13. Comportamiento del agente seleccione Lista de copias de seguridad de sondas de estado y seleccione **Elegir**, seleccione el FQDN de PSN/Standalone y seleccione **Guardar**

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

Paso 14. En Status Protocols > Discovery Host (Protocolos de estado > Host de detección), defina la dirección IP del nodo PSN/independiente.

Paso 15. En la lista de servidores de respaldo de Discovery y Select **elija**, seleccione su FQDN PSN o FQDN independiente y seleccione **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

Paso 16. En **Reglas de nombre de servidor**, escriba * para ponerse en contacto con todos los servidores y definir la dirección IP PSN/Standalone en **lista de inicio de llamada**. Alternativamente, se puede utilizar un comodín para que coincida con todos los PSN potenciales de la red (es decir, *.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

Paso 17. Haga clic en **Agregar > Configuración de AnyConnect**

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

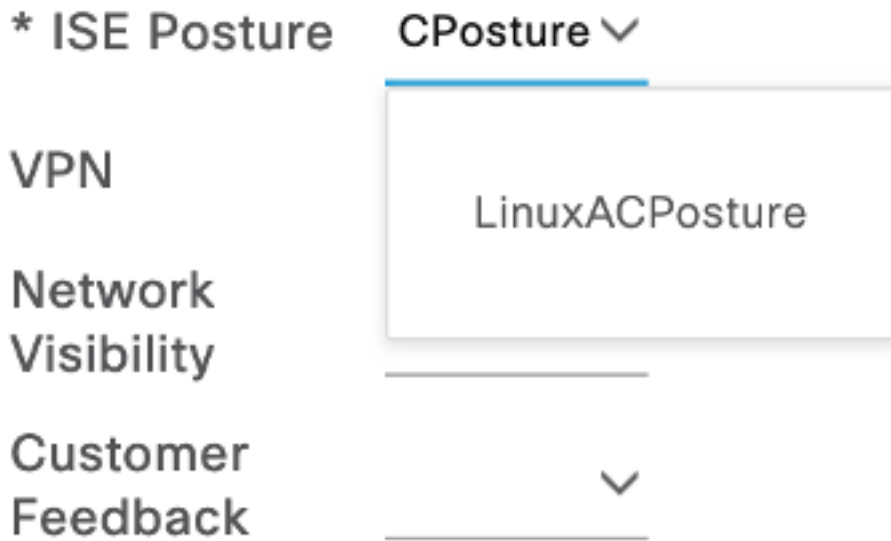
VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

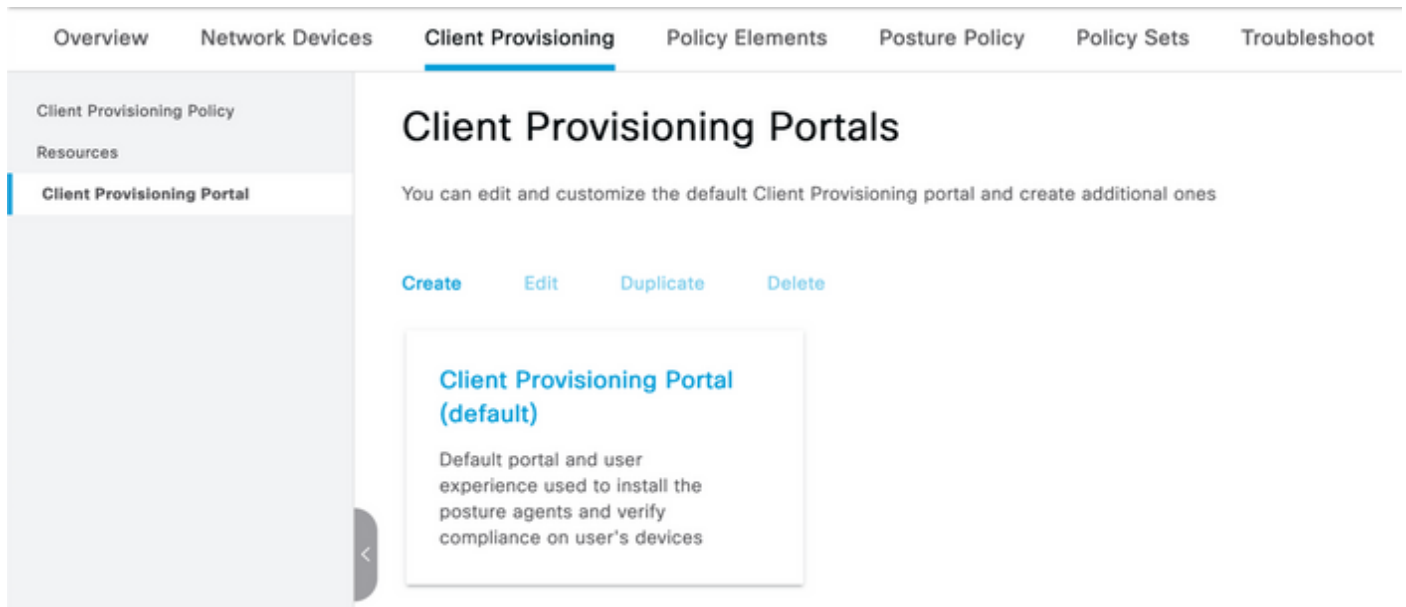
Profile Selection



Desplácese hacia abajo y seleccione Enviar

Paso 18. Cuando haya terminado de hacer selecciones, haga clic en **Enviar**.

Paso 19. Seleccione **Centros de Trabajo > Estado > Aprovisionamiento de Cliente > Portales de Aprovisionamiento de Cliente**.



Paso 20. En la sección **Configuración del portal**, puede seleccionar la interfaz y el puerto, así como los grupos autorizados a la página Seleccionar empleado, Usuarios SISE y Usuarios de dominio.

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)		Employee
GROUP_ACCOUNTS (default)	<input type="button" value="<"/>	
OWN_ACCOUNTS (default)		

Paso 21. En Configuración de inicio de sesión en la página, asegúrese de que la opción **Habilitar inicio de sesión automático** esté habilitada

✓ 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

Paso 22. En la esquina superior derecha, seleccione **Guardar**

Paso 23. Seleccione **Centros de Trabajo > Estado > Aprovisionamiento de Cliente > Política de Aprovisionamiento de Cliente.**

Paso 24. Haga clic en la flecha hacia abajo junto a la regla **IOS** en el **CPP** y elija **Duplicar** arriba

Paso 25. Nombre la regla **LinuxPosture**

Paso 26. Para Resultados, seleccione **AnyConnect Configuration** como agente.

Nota: En este caso, no verá un menú desplegable del módulo de cumplimiento porque está configurado como parte de la configuración de 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 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

Paso 27. Haga clic en **Finalizado**.

Paso 28. Click **Save**.

Elementos de la política de estado

Paso 29. Seleccione **Centros de Trabajo > Estado > Elementos de Política > Condiciones > Archivo**. Seleccione **Agregar**.

Paso 30. Defina **TESTFile** como el nombre de la condición de archivo y defina los siguientes valores

File Condition

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

Testfile.csv

Nota: La ruta se basa en la ubicación del archivo.

Paso 31. Seleccione **Save (Guardar)**.

FileExistence. Este tipo de condición de archivo busca ver si existe un archivo en el sistema donde se supone que debe existir, y eso es todo. Con esta opción seleccionada, no hay ningún problema para validar las fechas del archivo, los hash, etc.

Paso 32. Seleccione Requisitos y cree una nueva política de la siguiente manera:

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

Nota: Linux no admite el texto del mensaje sólo como acción de corrección

Componentes necesarios

- **Sistema operativo:** Linux All
- **Módulo de cumplimiento:** 4,x
- **Tipo de estado:** AnyConnect
- **Condiciones:** Módulos de cumplimiento y agentes (que estarán disponibles después de seleccionar el SO)
- **Acciones de remediación:** Remediaciones disponibles para su selección después de haber elegido el resto de condiciones.

Paso 33. Seleccione **Centros de trabajo > Estado > Política de estado**

Paso 34. Seleccione **Edit** en cualquier política y Seleccione **Insert New policy Define LinuxPosturePolicy** como el nombre y asegúrese de agregar el requisito creado en el paso 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_Ma	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Any_AM_Installation_Ma	Edit
<input checked="" type="checkbox"/>	Policy Options	LinuxPosturePolic	Any	and Linux All	and 4.x or later	and AnyConnect	and	then LinuxFile	Edit

Paso 35. Seleccione **Finalizado y Guardar**

Otras configuraciones importantes de estado (sección Configuración general de estado)

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

Los parámetros importantes de la sección Configuración general de estado son los siguientes:

- **Temporizador de remediación:** Esta configuración define la cantidad de tiempo que un cliente tiene para corregir una condición de estado fallida. También hay un temporizador de remediación en la configuración de AnyConnect; este temporizador es para ISE, no para AnyConnect.
- **Estado de estado predeterminado:** Esta configuración proporciona el estado de los dispositivos sin el agente de estado o los sistemas operativos que no pueden ejecutar el agente temporal, como los sistemas operativos basados en Linux.
- **Intervalo de monitoreo continuo:** Esta configuración se aplica a las condiciones de la aplicación y del hardware que están realizando el inventario del terminal. La configuración

especifica la frecuencia con la que AnyConnect debe enviar los datos de supervisión.

- **Política de uso aceptable en modo sigiloso:** Las dos únicas opciones para esta configuración son bloquear o continuar. Block evita que los clientes de AnyConnect en modo sigiloso continúen si la AUP no ha sido reconocida. Continue permite que el cliente del modo sigiloso continúe incluso sin reconocer la AUP (que suele ser la intención al utilizar la configuración del modo sigiloso de AnyConnect).

Configuraciones de reevaluación

Las reevaluaciones de estado son un componente fundamental del flujo de trabajo de estado. Ha visto cómo configurar el agente de AnyConnect para la reevaluación del estado en la sección "Protocolo de estado". El agente se conecta periódicamente con los PSN definidos en función del temporizador de esa configuración.

Cuando una solicitud llega al PSN, el PSN determina si se necesita una reevaluación del estado, en función de la configuración de ISE para la función de ese terminal. Si el cliente pasa la reevaluación, el PSN mantiene el estado de cumplimiento de estado del terminal y se restablece el arrendamiento de estado. Si el terminal falla en la reevaluación, el estado cambia a no conforme y se elimina el arrendamiento de estado existente.

Paso 36. Seleccione **Policy > Policy Elements > Results > Authorization > Authorization Profile**. Seleccione **Agregar**

Paso 37. Defina **Wired_Redirect** como el Perfil de autorización y configure los siguientes parámetros

▼ 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

Paso 38. Seleccione **Save (Guardar)**.

Paso 39. Configurar políticas de autorización

Hay tres reglas de autorización preconfiguradas para el estado:

1. El primero se configura para que coincida cuando la autenticación se realice correctamente y se desconoce el cumplimiento de un dispositivo.
2. La segunda regla coincide con las autenticaciones exitosas con los extremos no conformes.

Nota: Ambas de las dos primeras reglas tienen el mismo resultado, que es utilizar un perfil de autorización preconfigurado que redirige el extremo al portal de aprovisionamiento de clientes.

3. La regla final coincide con los terminales conformes con la autenticación y el estado y utiliza el perfil de autorización de PermitAccess predefinido.

Seleccione **Policy > Policy Set** y seleccione la flecha derecha para **Wired 802.1x - MAB** Creado en el laboratorio anterior.

Paso 40. Seleccione Política de autorización y cree las siguientes reglas

 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	

Configuraciones en el switch

Nota: La siguiente configuración se refiere a IBNS 1.0. Puede haber diferencias para los switches compatibles con IBNS 2.0. Incluye la implementación del modo de bajo impacto.

```
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 redirection 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
```

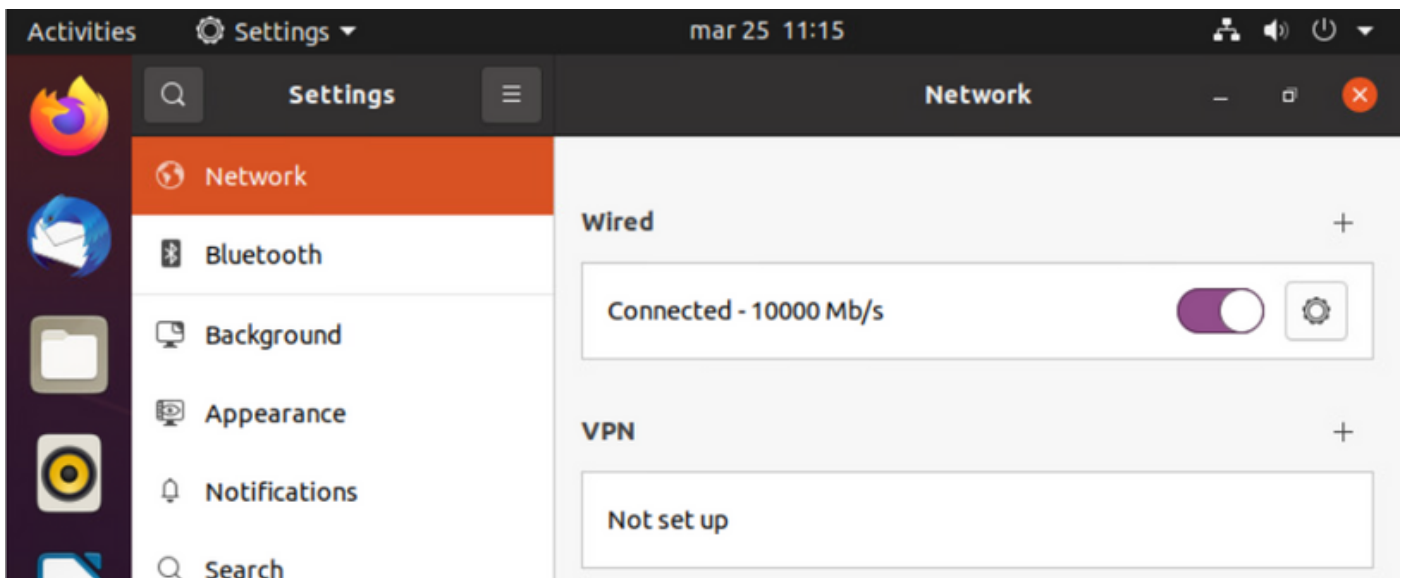
Verificación

Verificación de ISE:

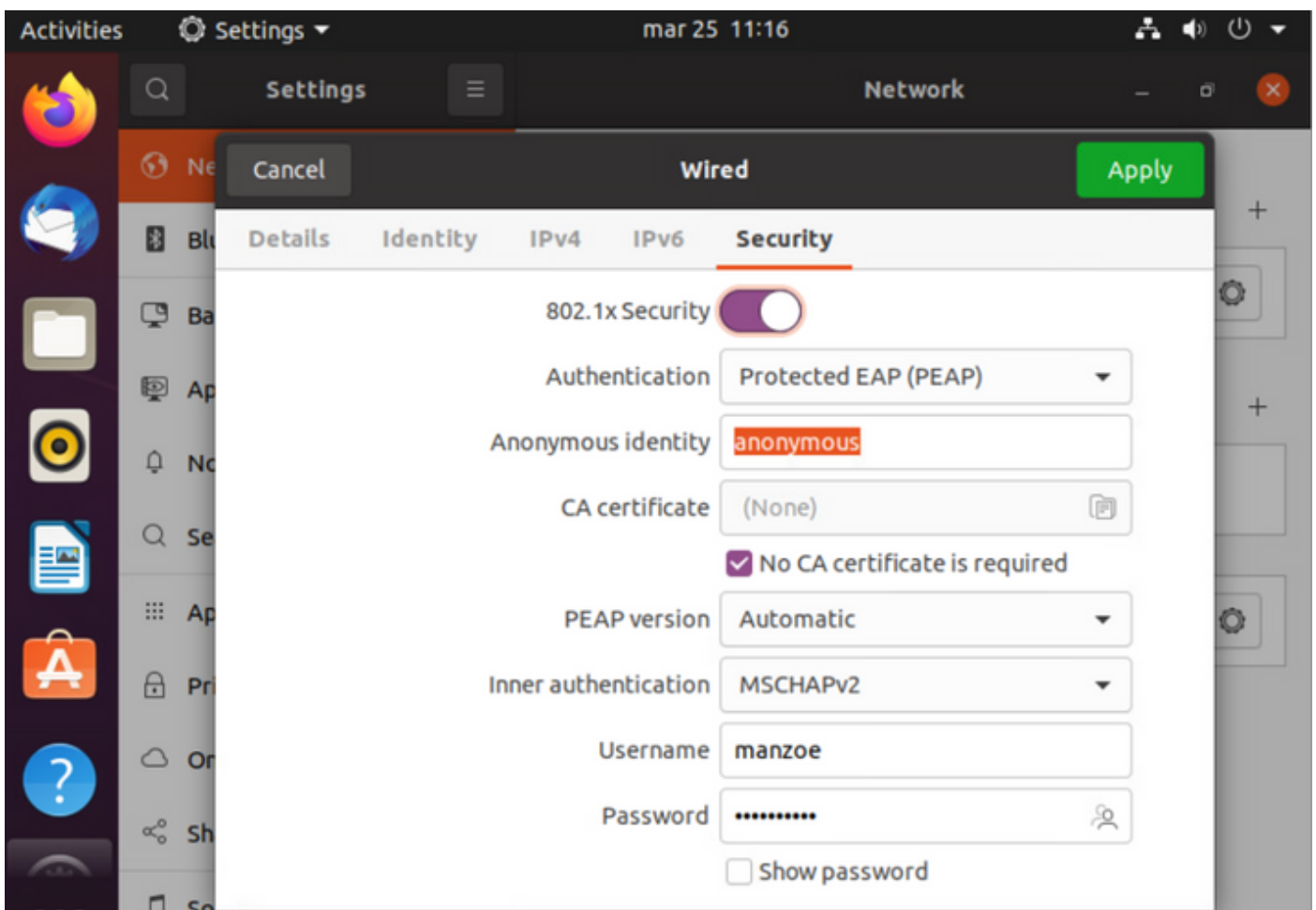
Esta sección asume que AnyConnect con el módulo de estado de ISE se ha instalado previamente en el sistema Linux.

Autenticar PC con dot1x

Paso 1. Vaya a Network Settings (Parámetros de red)



Paso 2. Seleccione la ficha Seguridad y proporcione la configuración 802.1x y las credenciales de usuario



Paso 3. Haga clic en "Aplicar".

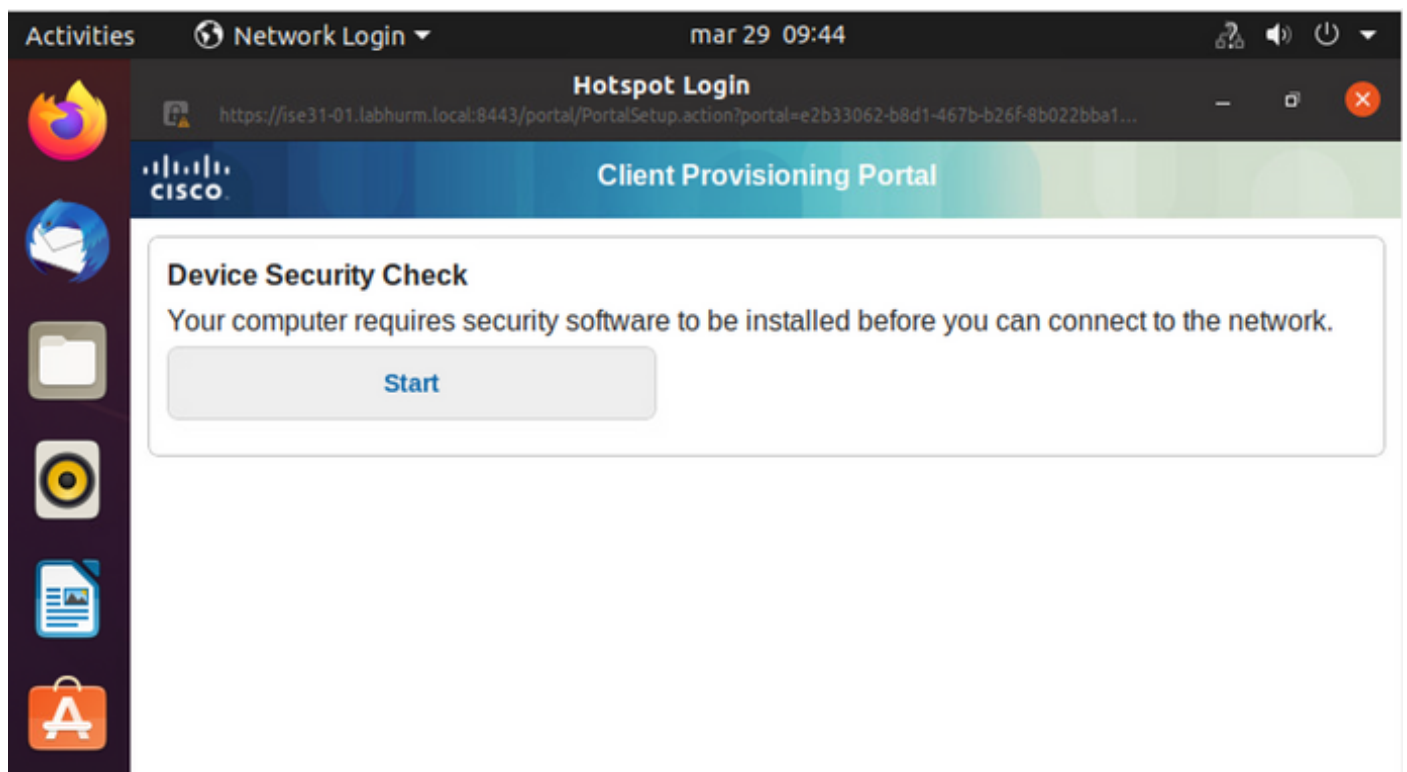
Paso 4. Conecte el sistema Linux a la red con cables 802.1x y valide en el registro en vivo de ISE:

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

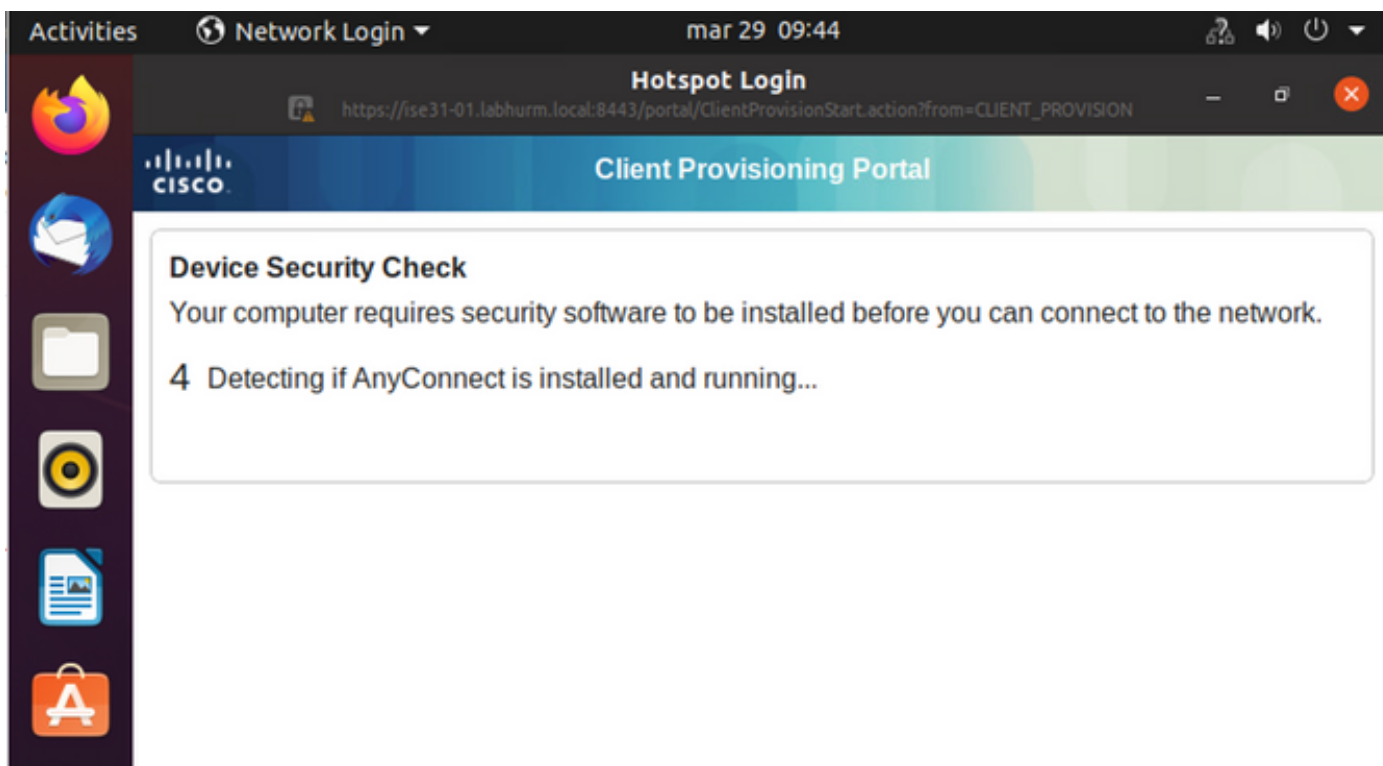
En ISE, utilice la barra de desplazamiento horizontal para ver información adicional, como el PSN que proporcionó el flujo o el estado de estado:

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

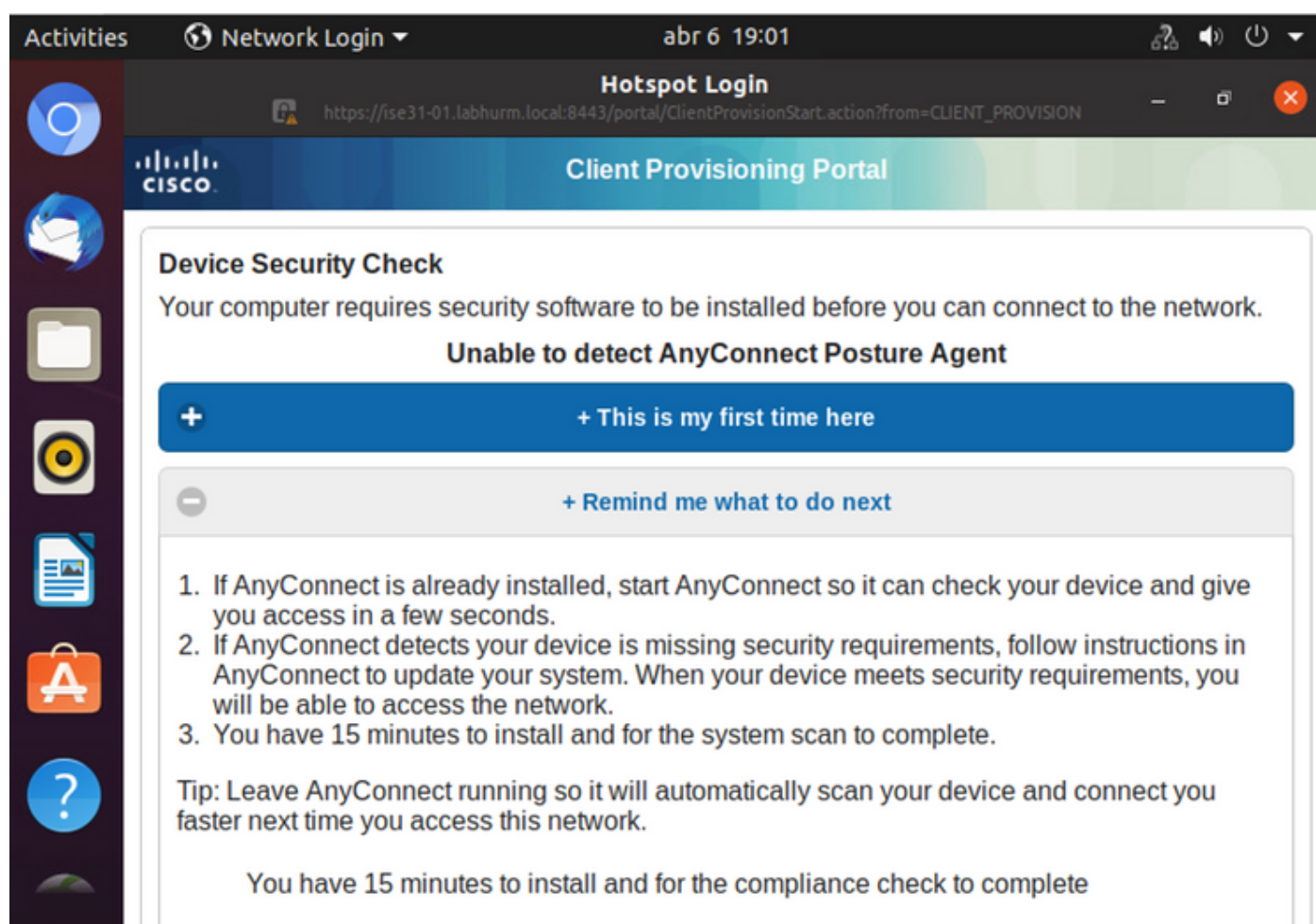
Paso 5. En el cliente Linux, se debe redireccionar, y presenta el portal de aprovisionamiento del cliente que indica que se produce la verificación de estado y para hacer clic en "Inicio":



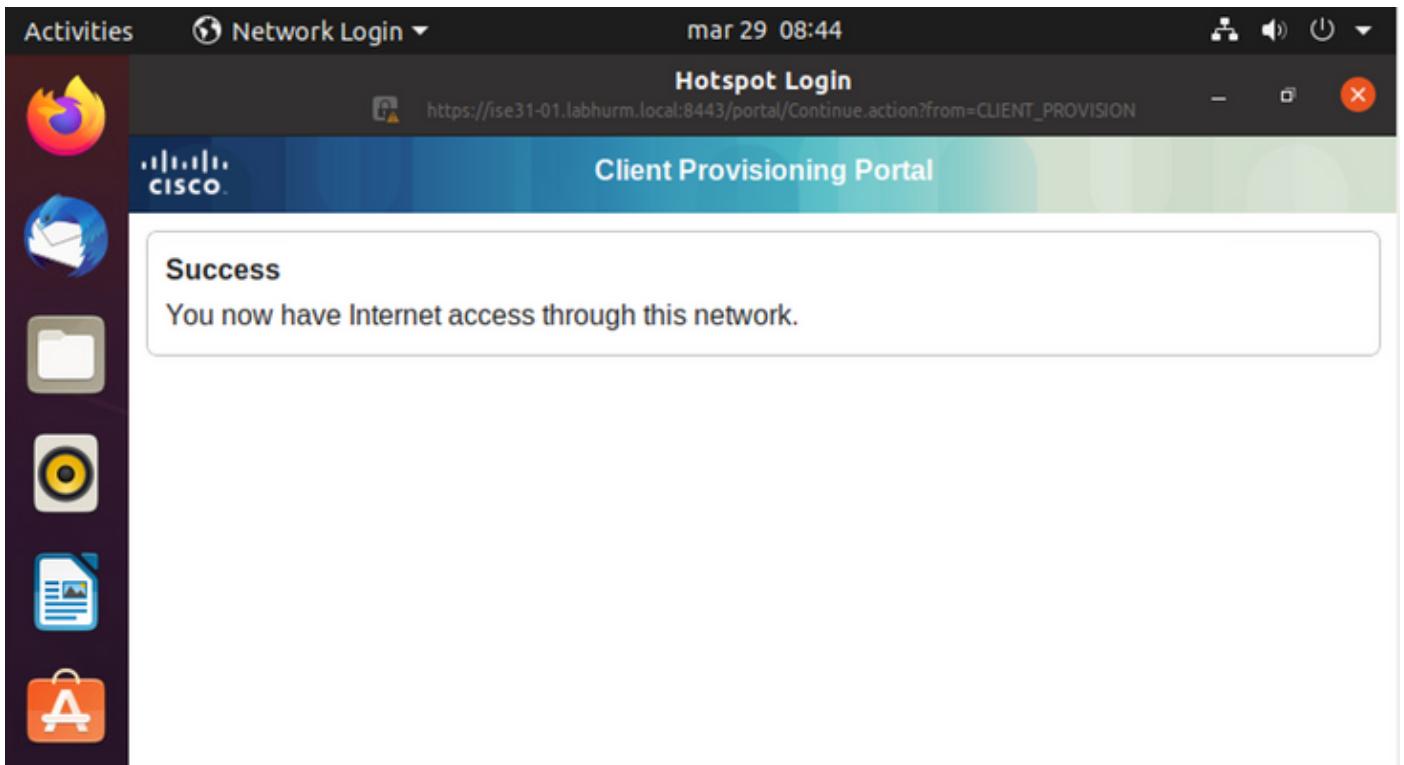
Espere unos segundos mientras el conector intenta detectar AnyConnect:



Debido a una advertencia conocida, aunque AnyConnect esté instalado, no la detecta. Utilice **Alt-Tab** o el menú **Actividades** para cambiar al cliente AnyConnect.

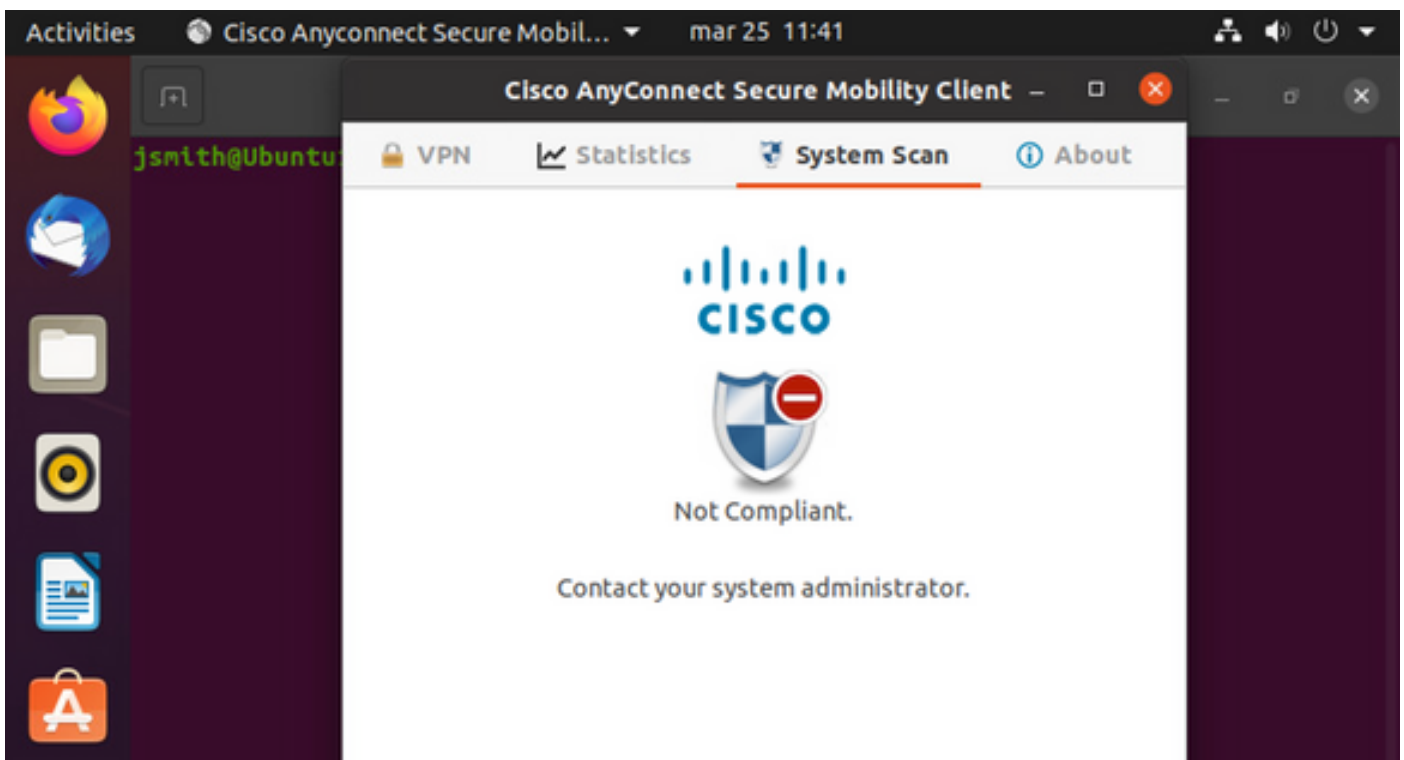


AnyConnect intenta alcanzar el PSN para la política de estado y evaluar el terminal en su contra.



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

Por otra parte, si el archivo no existe, el módulo de estado de AnyConnect informa de la determinación a 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	

Nota: El FQDN de ISE debe resolverse en el sistema Linux a través de DNS o archivo de host local.

Troubleshoot

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

Redirigir en su lugar:

```
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
```

Autorización correcta:

```
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
```

No conforme, se pasa a la VLAN y ACL de cuarentena:

```
LABDEMOAC01#sh auth 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
```