

Configurar a postura do Cisco ISE 3.1 com Linux

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações no ISE](#)

[Configurações no switch](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve o procedimento para configurar e implementar uma política de postura de arquivo para Linux e o Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- AnyConnect
- Identity services engine (ISE)
- Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Anyconnect 4.10.05085
- ISE versão 3.1 P1
- Linux Ubuntu 20,04
- Switch Cisco Catalyst 3650. Versão 03.07.05.E (15.12(3)E5)

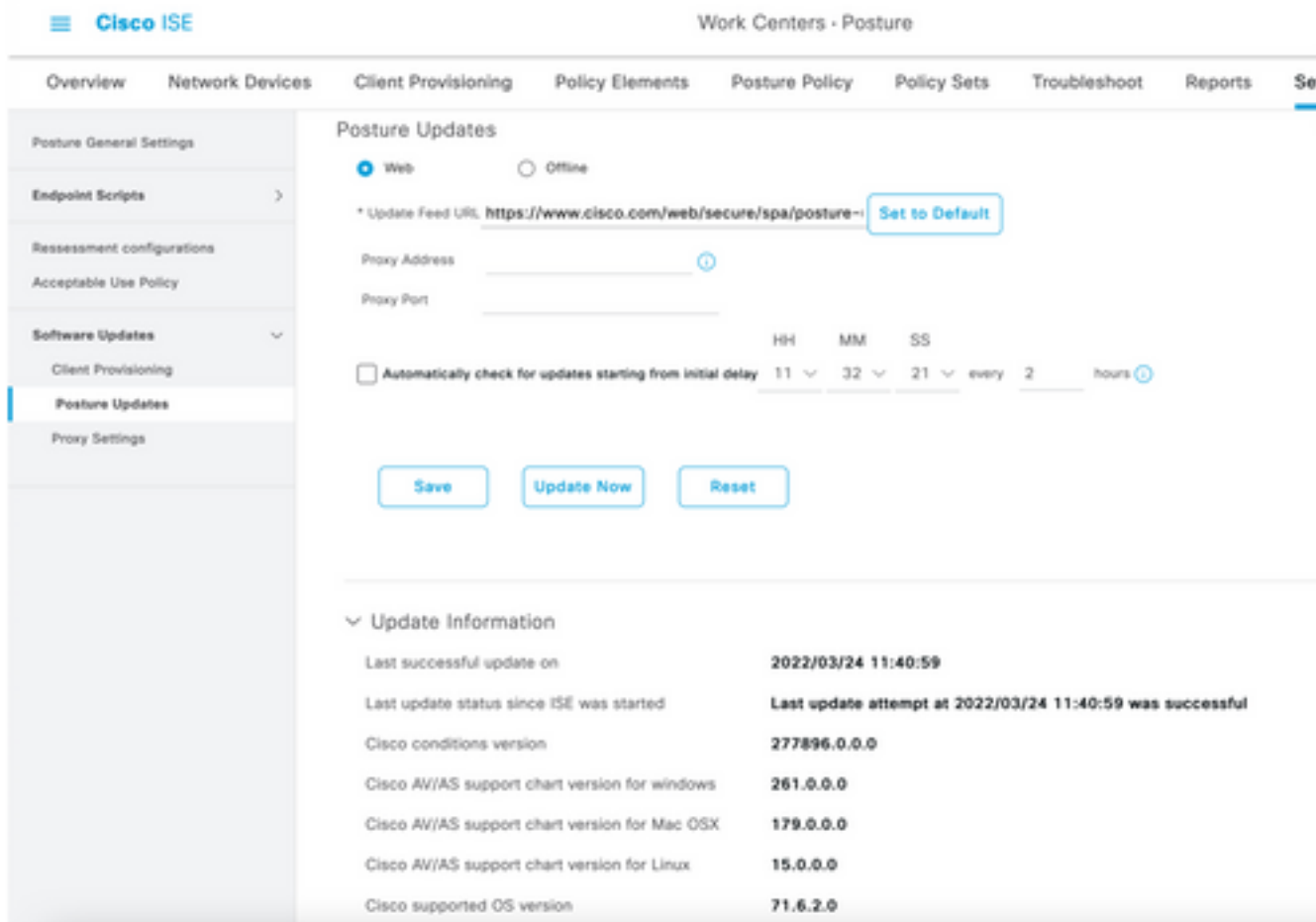
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configurações no ISE

Etapa 1. Atualizar serviço de postura:

Navegue até **Centros de trabalho > Postura > Configurações > Atualizações de software > Atualizações de postura**. Selecione **Atualizar agora** e aguarde a conclusão do processo:



The screenshot shows the Cisco ISE interface for 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 a radio button for 'Web' (selected) and 'Offline'. The 'Update Feed URL' is set to 'https://www.cisco.com/web/secure/spa/posture-...' with a 'Set to Default' button. There are input fields for 'Proxy Address' and 'Proxy Port'. A checkbox for 'Automatically check for updates starting from initial delay' is present, with a time picker set to 11:32:21 every 2 hours. At the bottom, there are 'Save', 'Update Now', and 'Reset' buttons. Below this is an 'Update Information' section with the following data:

Update Information	Value
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

Um **pacote fornecido pela Cisco** é um pacote de software que você baixa do site Cisco.com, como os pacotes de software do AnyConnect. Um **pacote criado pelo cliente** é um perfil ou uma configuração que você criou fora da interface de usuário do ISE e deseja carregar no ISE para uso com avaliação de postura. Para este exercício, você pode baixar o pacote de implantação na Web do AnyConnect "anyconnect-linux64-4.10.05085-webdeploy-k9.pkg".

Note: Devido a atualizações e patches, a versão recomendada pode ser alterada. Use a versão recomendada mais recente do site cisco.com.

Etapa 2. Carregar pacote do AnyConnect:

No Centro de trabalho com postura, navegue até **Provisionamento 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

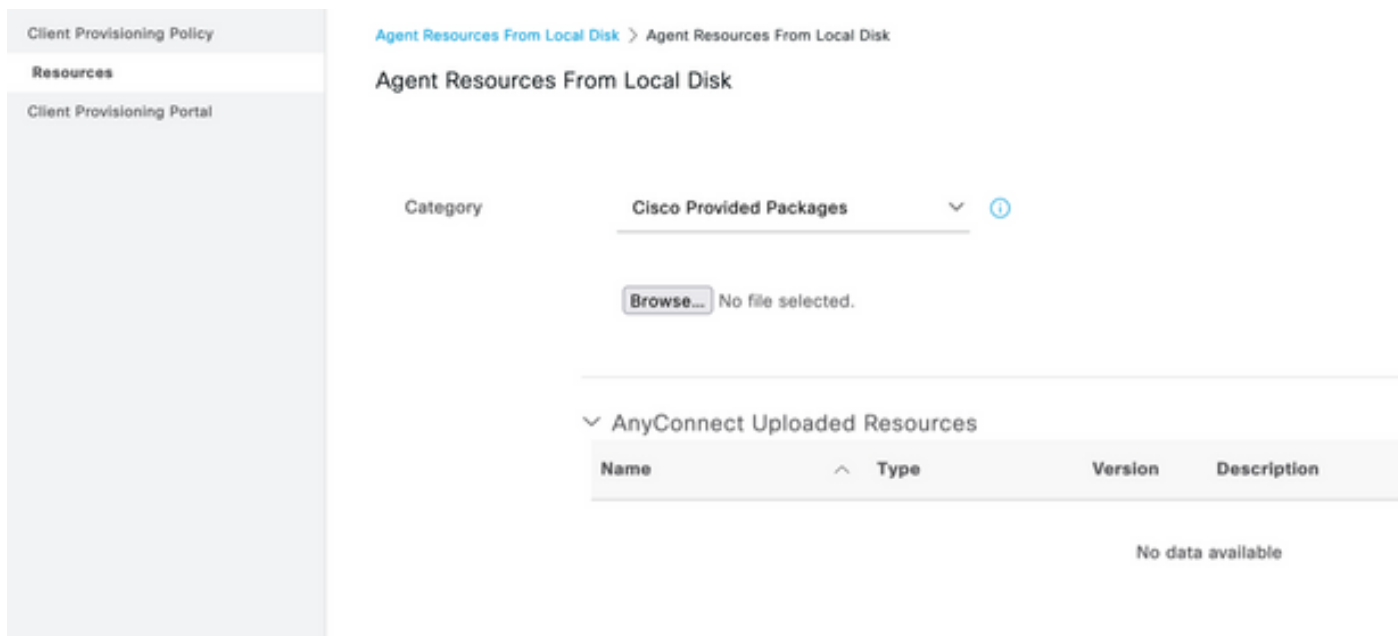
Etapa 3. Selezione **Add > Agent Resources from Local Disk**

Resources

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

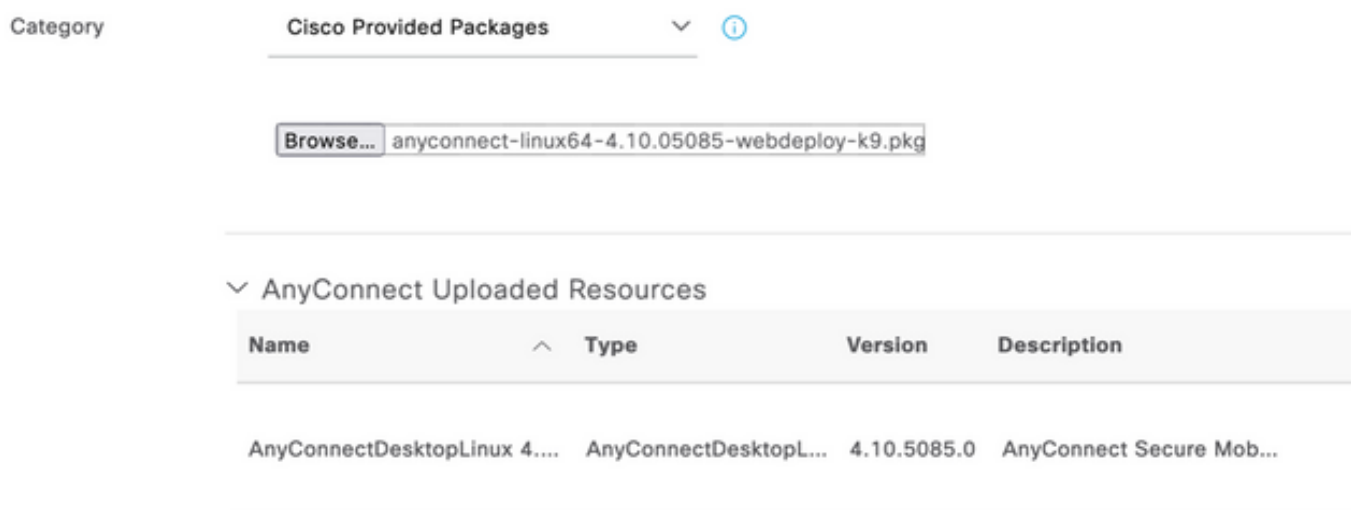
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Etapa 4. Selezione **Cisco Provided Packages** no menu suspenso Categoria.



Etapa 5. Clique em Procurar.

Etapa 6. Escolha um dos pacotes do AnyConnect que você baixou na etapa anterior. A imagem do AnyConnect é processada e as informações sobre o pacote são exibidas



Etapa 7. Clique em **Enviar**. Agora que o AnyConnect está carregado no ISE, você pode ter contato com o ISE e obter os outros recursos do cliente do Cisco.com.

Note: Os recursos do agente incluem módulos usados pelo AnyConnect Client que fornece a capacidade de avaliar a conformidade de um endpoint para uma variedade de verificações de condição, como Antivírus, Anti-Spyware, Anti-Malware, Firewall, Criptografia de disco, Arquivo e assim por diante.

Etapa 8. Clique em **Add > Agent Resources from Cisco Site**. Leva um minuto para a janela ser preenchida quando o ISE acessa Cisco.com e recupera um manifesto de todos os recursos publicados para provisionamento 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

Etapa 9. Selecione os módulos de conformidade mais recentes do AnyConnect para Linux. Além disso, você também pode selecionar o módulo de conformidade para Windows e 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

Etapa 10. Selecione os agentes temporais mais recentes para Windows e 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!

Etapa 11. Clique em **Salvar**.

Note: As configurações de postura MAC e Windows estão fora do escopo deste guia de configuração.

Neste ponto, você carregou e atualizou todas as peças necessárias. Agora é o momento de criar a configuração e os perfis necessários para usar esses componentes.

Etapa 12. Clique em Add > NAC Agent ou 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 checkboxes, names, versions, last update times, and descriptions. 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 page for 'AnyConnect Posture Profile' is shown. The 'Name' field is 'LinuxACPosture'. The 'Description' field is empty. Below this is the 'Agent Behavior' section with 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.

Os parâmetros que precisam ser modificados são:

- **Intervalo de detecção de VLAN:** Essa configuração permite que você defina o número de segundos que o módulo aguarda entre os testes de alterações de VLAN. A recomendação é de 5 segundos.
- **Ping ou ARP:** Este é o método real de detecção de alteração de VLAN. O agente pode fazer ping no gateway padrão ou monitorar o cache ARP para que a entrada do gateway padrão atinja o tempo limite ou ambos. A configuração recomendada é ARP.
- **Temporizador de correção:** Quando a postura de um endpoint é desconhecida, ele passa por um fluxo de avaliação de postura. É preciso tempo para corrigir falhas nas verificações de postura; o tempo padrão é de 4 minutos antes que o marque o endpoint como não compatível, mas os valores podem variar de 1 a 300 minutos (5 horas). A recomendação é de 15 minutos; no entanto, isso pode exigir ajustes se for esperado que a correção demore mais.

Note: A postura do arquivo Linux não oferece suporte à correção automática.

Para obter uma descrição abrangente de todos os parâmetros, consulte a documentação de postura do ISE ou do AnyConnect.

Etapa 13. Comportamento do agente, selecione Lista de backup de sondas de postura e selecione **Escolher**, selecione o FQDN PSN/autônomo e selecione **Salvar**

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

Etapa 14. Em Posture Protocols > Discovery Host, defina o endereço IP do nó PSN/independente.

Etapa 15. Em **Discovery backup server list** e Select **escolha**, selecione seu PSN ou FQDN independente e selecione **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 ✕



Cancel

Select

Etapa 16. Em **Server name rules** digite * para entrar em contato com todos os servidores e definir o endereço IP PSN/Standalone sob **call home list**. Como alternativa, um curinga pode ser usado para corresponder todos os PSNs em potencial em sua rede (ou seja, *.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

Etapa 17. Clique em **Adicionar > Configuração do 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 v

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

AnyConnect Module Selection

ISE Posture

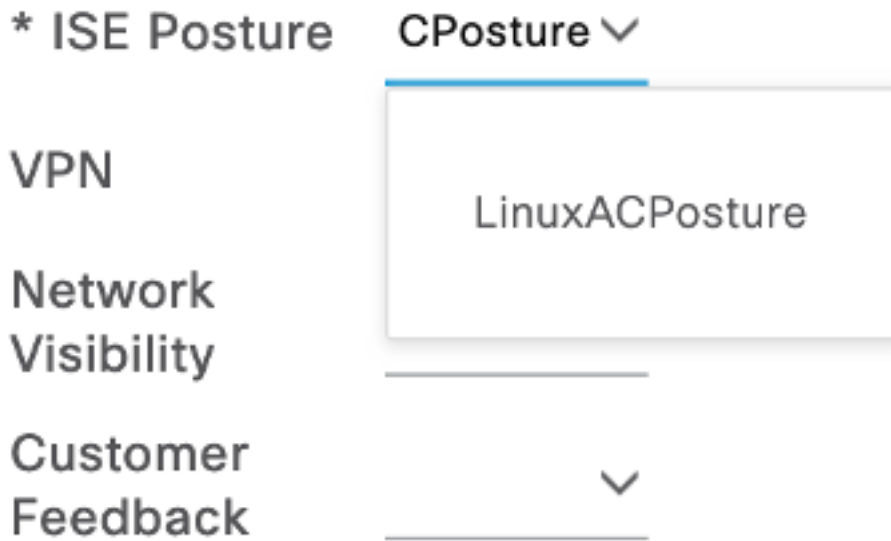
VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

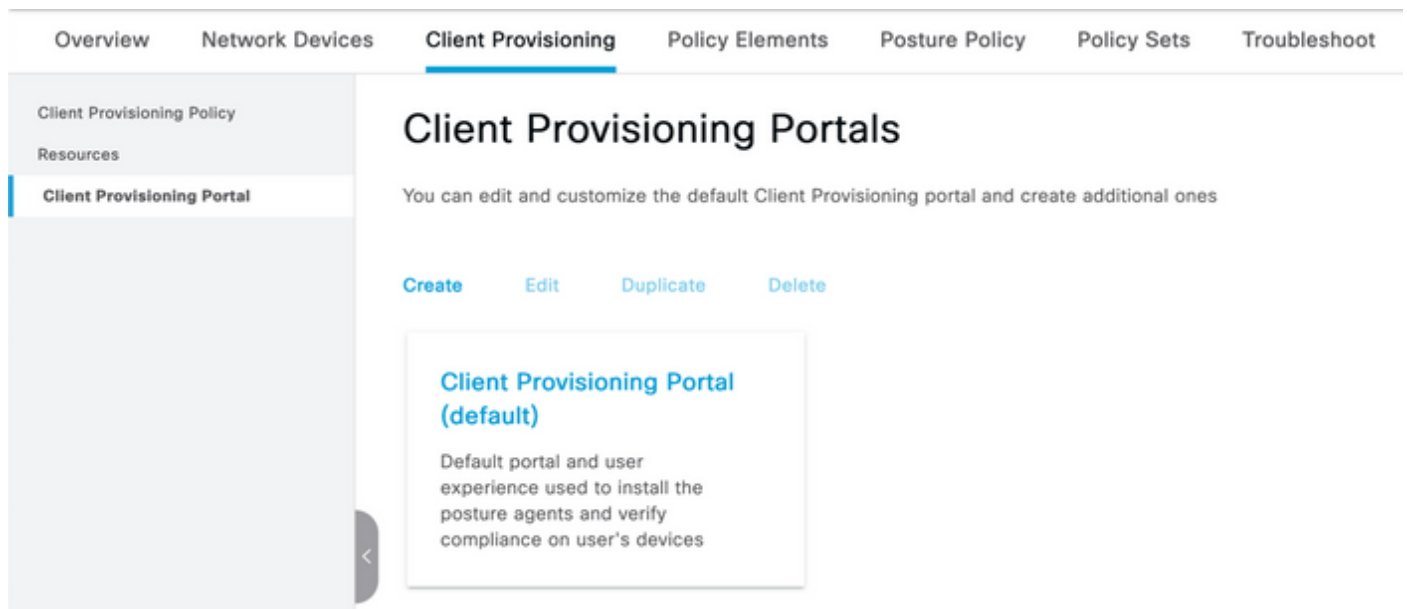
Profile Selection



Role para baixo e selecione Enviar

Etapa 18. Quando terminar de fazer seleções, clique em **Enviar**.

Etapa 19. Selecione **Centros de Trabalho > Postura > Provisionamento de Cliente > Portais de Provisionamento de Cliente**.



Etapa 20. Na seção **Configurações do portal**, onde você pode selecionar a interface e a porta, bem como os grupos autorizados para a página, selecione **Funcionário, SISE_Users e Usuários do domínio**.

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)		

Etapa 21. Em Log in Page Settings, certifique-se de que a opção **Enable auto Log In** esteja ativada

✓ 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

Etapa 22. No canto superior direito, selecione **Save**

Etapa 23.Selecione **Centros de trabalho > Postura > Provisionamento de cliente > Política de provisionamento de cliente.**

Etapa 24. Clique na seta para baixo ao lado da **regra do IOS no CPP** e escolha **Duplicar Acima**

Etapa 25. Nomear a regra **LinuxPosture**

Etapa 26. Para Resultados, selecione a **Configuração do AnyConnect** como o agente.

Note: Nesse caso, você não verá um módulo de conformidade suspenso porque ele está configurado como parte da configuração do 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

Etapa 27.Clique em **Concluído**.

Etapa 28. Clique em **Salvar**.

Elementos da política de postura

Etapa 29.Selecione **Centros de trabalho > Postura > Elementos de política > Condições > Arquivo**. Selecione **Adicionar**.

Etapa 30.Defina **TESTFile** como o nome da condição do arquivo e defina os próximos 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

Note: O caminho é baseado no local do arquivo.

Etapa 31. Selecione **Save**

FileExistence. Este tipo de arquivo de condição procura ver se um arquivo existe no sistema onde ele deveria estar — e isso é tudo. Com essa opção selecionada, não há nenhuma preocupação para validar as datas de arquivo, hashes e assim por diante

Etapa 32. Selecione Requisitos e crie uma nova política da seguinte maneira:

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: O Linux não suporta mensagens de texto somente como ação de correção

Componentes de requisito

- **Sistema operacional:** Todos no Linux
- **Módulo de conformidade:** 4.x
- **Tipo de postura:** AnyConnect
- **Condições:** Módulos e agentes de conformidade (que ficam disponíveis depois que você seleciona o SO)
- **Ações de correção:** Remediações que ficam disponíveis para seleção depois que todas as outras condições são escolhidas.

Etapa 33. Selecione **Centros de trabalho > Postura > Política de postura**

Etapa 34. Selecione **Edit** em qualquer política e selecione **Insert New policy Define LinuxPosturePolicy** como o nome e certifique-se de adicionar seu requisito criado na etapa 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

Etapa 35. Selecione **Concluído e Salvar**

Outras configurações importantes de postura (seção Configurações gerais de postura)

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

As configurações importantes na seção Configurações gerais de postura são as seguintes:

- **Temporizador de correção:** Essa configuração define o tempo que um cliente tem para corrigir uma condição de postura com falha. Há também um temporizador de remediação na configuração do AnyConnect; esse temporizador é para ISE, não para AnyConnect.
- **Status de postura padrão:** Essa configuração fornece o status de postura para dispositivos sem o agente de postura ou sistemas operacionais que não podem executar o agente temporal, como sistemas operacionais baseados em Linux.
- **Intervalo de monitoramento contínuo:** Essa configuração se aplica às condições de aplicativo e hardware que fazem o inventário do endpoint. A configuração especifica com que frequência o AnyConnect deve enviar os dados de monitoramento.

- **Política de uso aceitável no modo oculto:** As duas únicas opções para essa configuração são bloquear ou continuar. Bloquear impede que clientes AnyConnect em modo furtivo prossigam se a AUP não tiver sido confirmada. Continuar permite que o cliente do modo furtivo continue mesmo sem confirmar a AUP (que geralmente é a intenção ao usar a configuração do modo furtivo do AnyConnect).

Configurações de reavaliação

Reavaliações de postura são um componente crítico do fluxo de trabalho de postura. Você viu como configurar o agente do AnyConnect para reavaliação de postura na seção "Protocolo de postura". O agente verifica periodicamente as PSNs definidas com base no temporizador nessa configuração.

Quando uma solicitação alcança a PSN, a PSN determina se uma reavaliação de postura é necessária, com base na configuração do ISE para a função desse endpoint. Se o cliente for aprovado na reavaliação, a PSN manterá o estado de conformidade com a postura do endpoint e o aluguel da postura será redefinido. Se o endpoint falhar na reavaliação, o status da postura muda para não compatível e qualquer aluguel de postura existente é removido.

Etapa 36. Selecione **Policy > Policy Elements > Results > Authorization > Authorization Profile**.
Selecione **Adicionar**

Etapa 37. Definir **Wired_Redirect** como o Perfil de Autorização e configurar os próximos parâmetros

Common Tasks

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

Client Provisioning (Posture) ▾ ACL ACL_REDIRECT_AV ▾ Value Client Provisioning Portal (defi ▾

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Auto Smart Port

Etapa 38. Selecione **Save**

Etapa 39. Configurar políticas de Autorização

Há três regras de autorização pré-configuradas para a postura:

1. O primeiro é configurado para corresponder quando a autenticação for bem-sucedida, e a conformidade de um dispositivo é desconhecida.
2. A segunda regra corresponde a autenticações bem-sucedidas com pontos de extremidade não compatíveis.

Note: As duas primeiras regras têm o mesmo resultado, que é usar um perfil de autorização pré-configurado que redireciona o ponto final para o portal de Provisionamento de Cliente.

3. A regra final corresponde a pontos de extremidade de autenticação bem-sucedidos e compatíveis com a postura e usa o perfil de autorização PermitAccess pré-criado.

Selecione **Policy > Policy Set** e selecione a seta para a direita para **Wired 802.1x - MAB Created** no laboratório anterior.

Etapa 40. Selecione Política de Autorização e crie as próximas regras



Configurações no switch

Note: A configuração abaixo se refere ao IBNS 1.0. Pode haver diferenças entre os switches compatíveis com IBNS 2.0. Inclui a implantação do modo de baixo 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 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
```

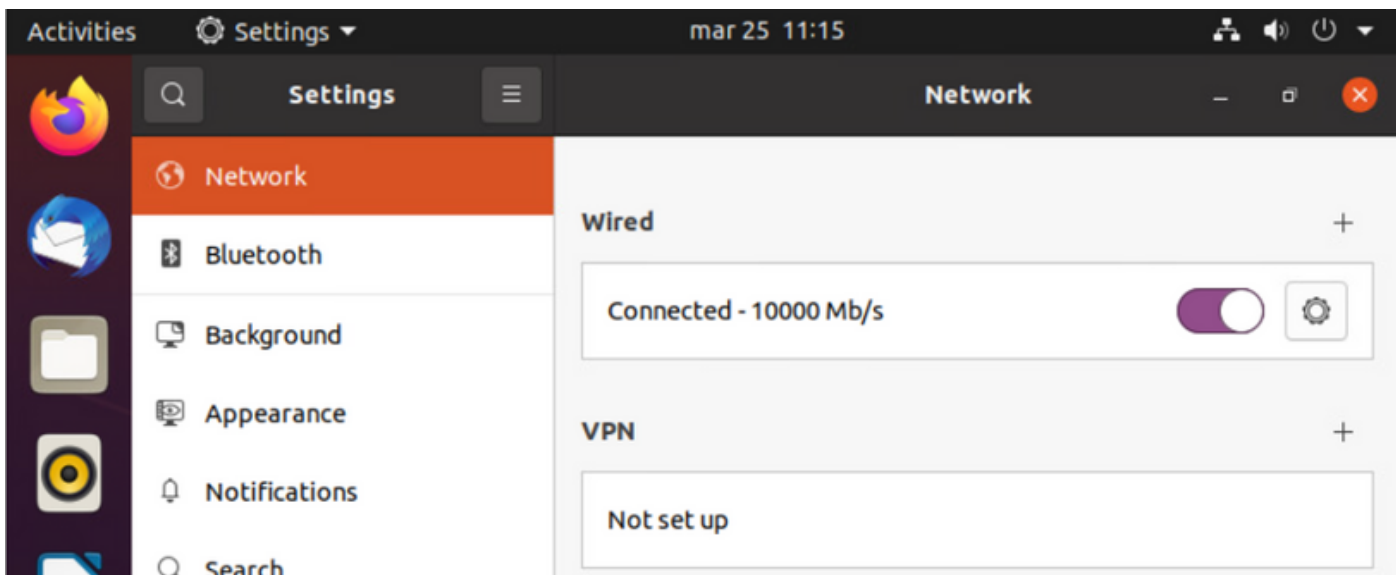
Verificar

Verificação do ISE:

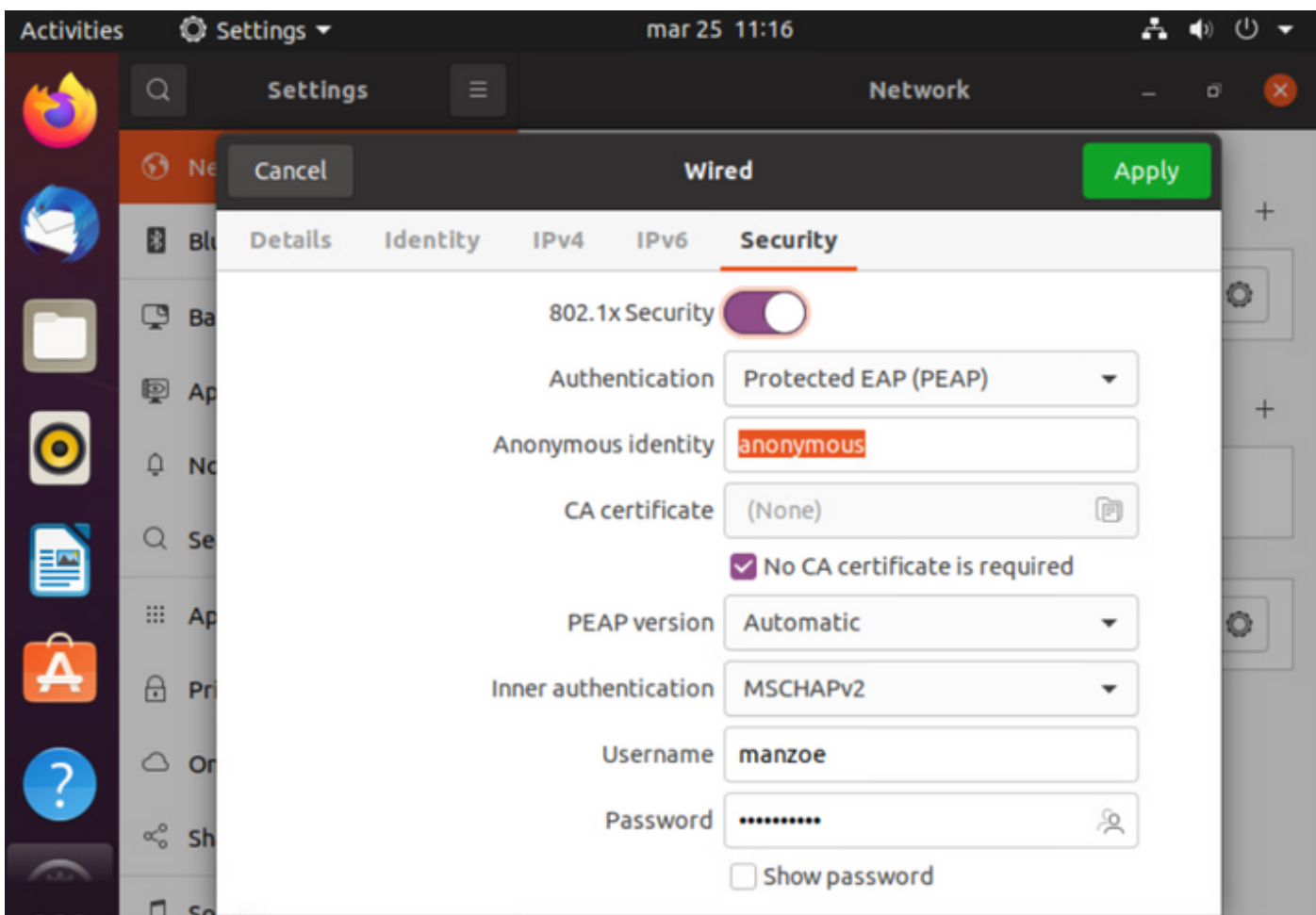
Esta seção pressupõe que o AnyConnect com o módulo de postura ISE foi instalado anteriormente no sistema Linux.

Autenticar o PC usando dot1x

Etapa 1. Navegue até Network Settings



Etapa 2. Selecione a guia Security e forneça a configuração 802.1x e as credenciais do usuário



Etapa 3. Clique em "Aplicar".

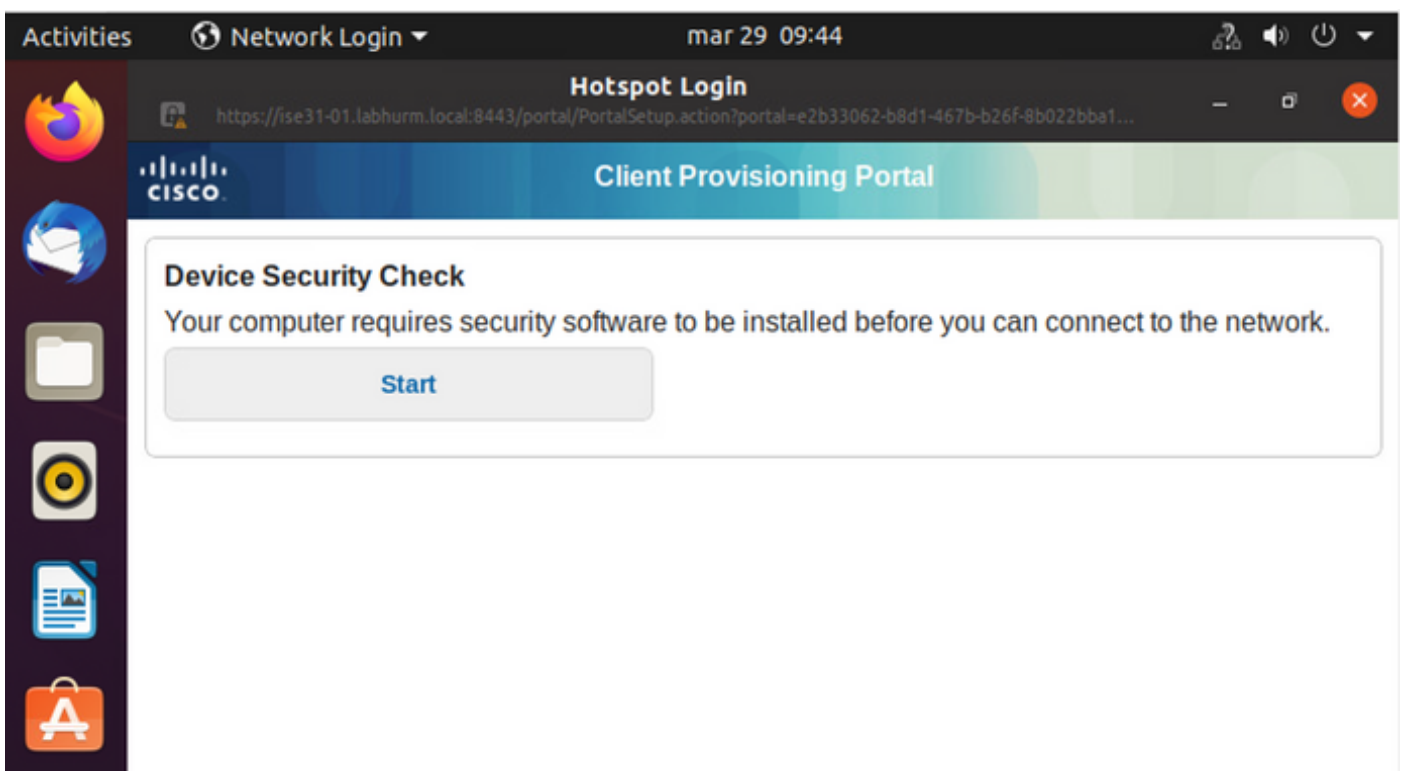
Etapa 4. Conecte o sistema Linux à rede com fio 802.1x e valide no registro ao vivo do ISE:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:09.2...	●		4	manzoe	00:0C:29:45:03:8F	Ubuntu_W...	Ubuntu_Po...	Ubuntu_Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:49.2...	●			manzoe	00:0C:29:45:03:8F	Ubuntu_W...	Ubuntu_Po...	Ubuntu_Po...	Wired_Re...		Car-1750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●			manzoe	00:0C:29:45:03:8F	Ubuntu_W...	Ubuntu_Po...	Ubuntu_Po...	Wired_Re...		Car-1750	FastEthernet1...	Workstation	Pending

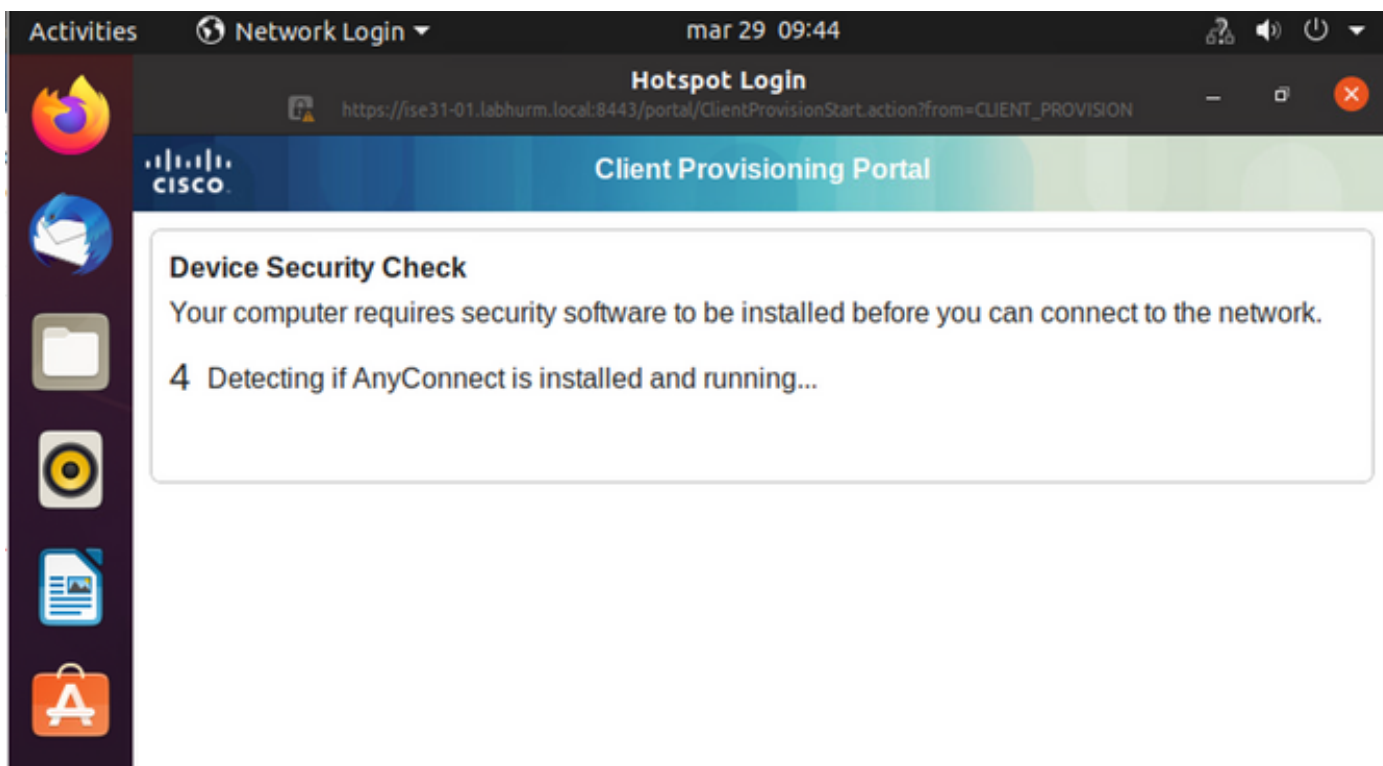
No ISE, use a barra de rolagem horizontal para exibir informações adicionais, como a PSN que serviu o fluxo ou o status da postura:

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Devicr	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

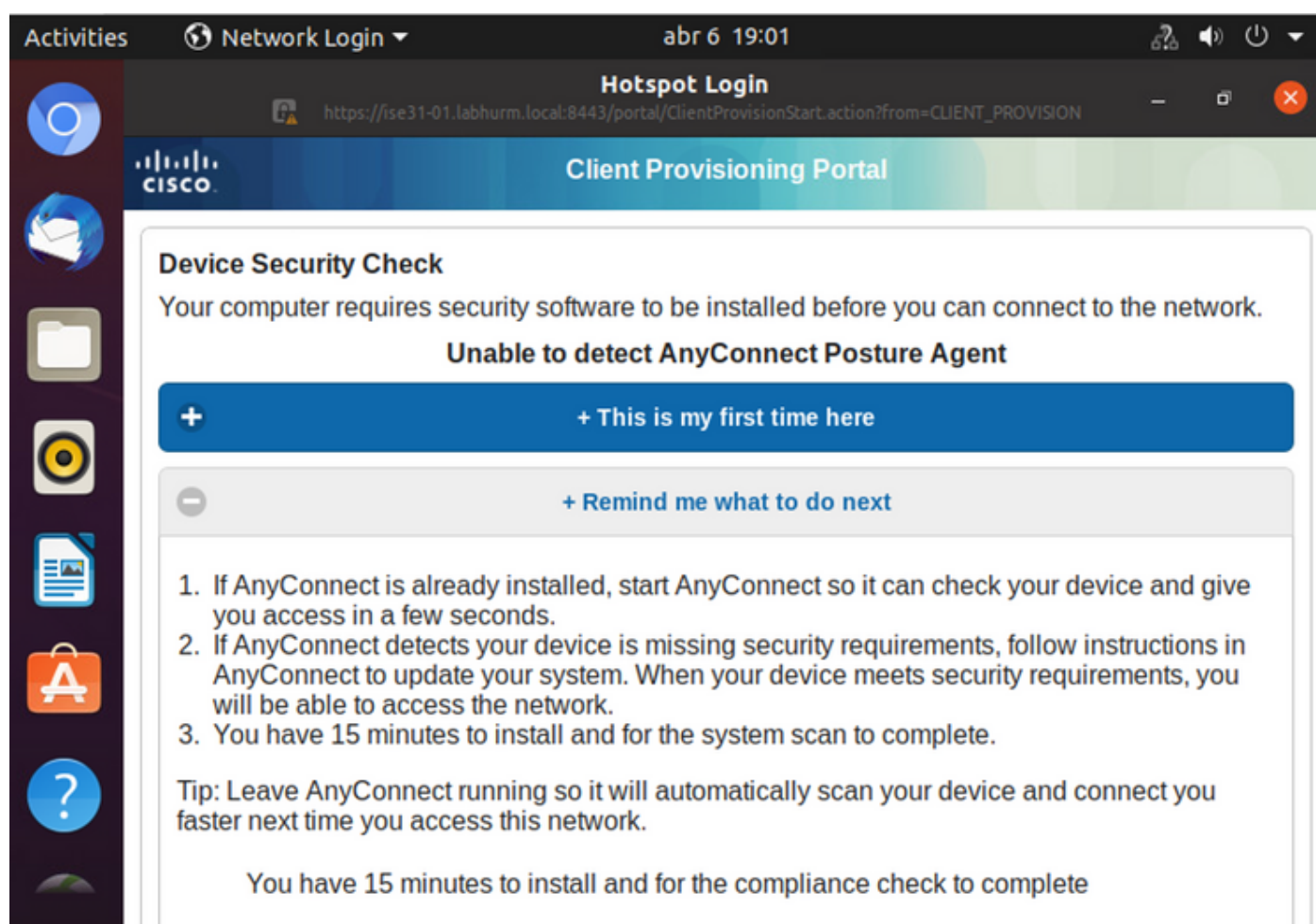
Etapa 5. No cliente Linux, o redirecionamento deve ocorrer, e ele apresenta o portal de provisionamento do cliente indicando a ocorrência da verificação de postura e para clicar em "Iniciar":



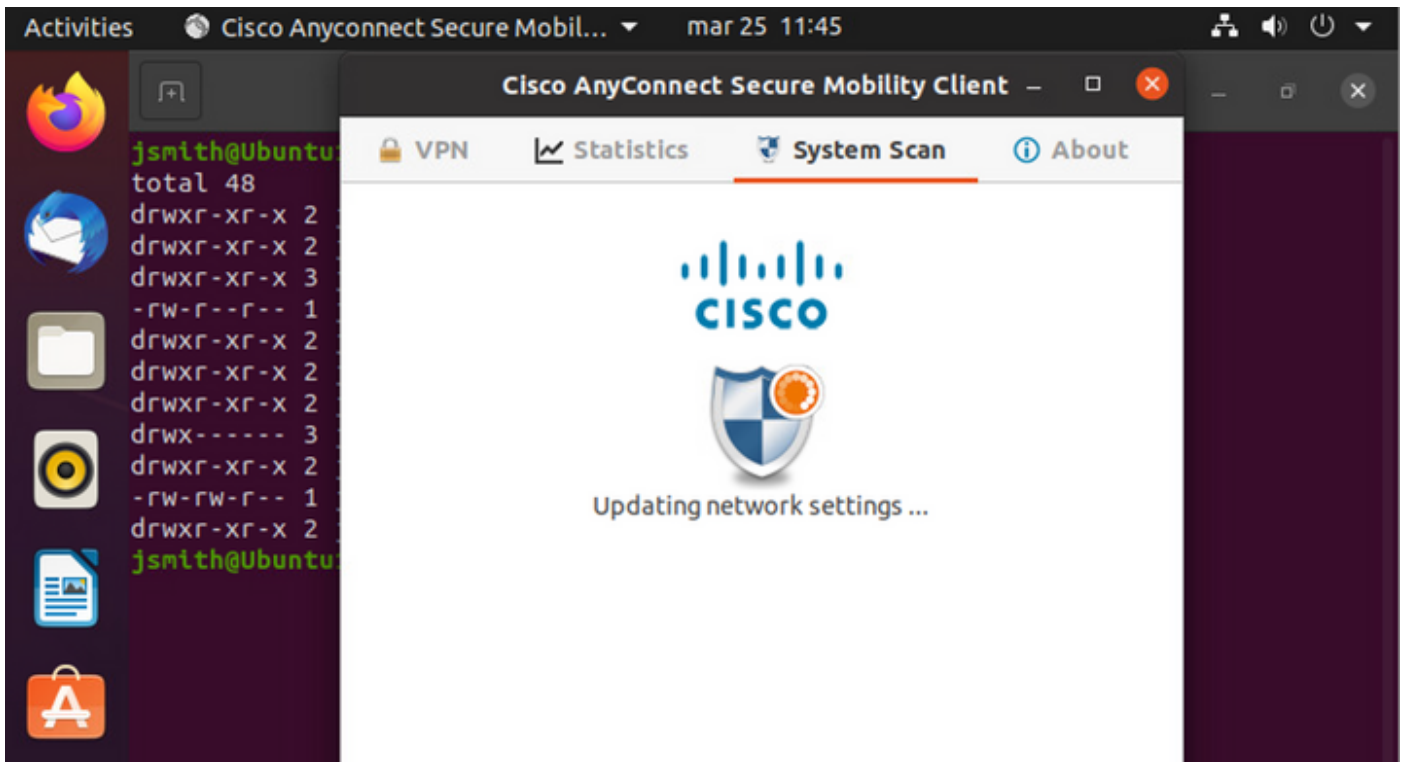
Aguarde alguns segundos enquanto o conector tenta detectar o AnyConnect:



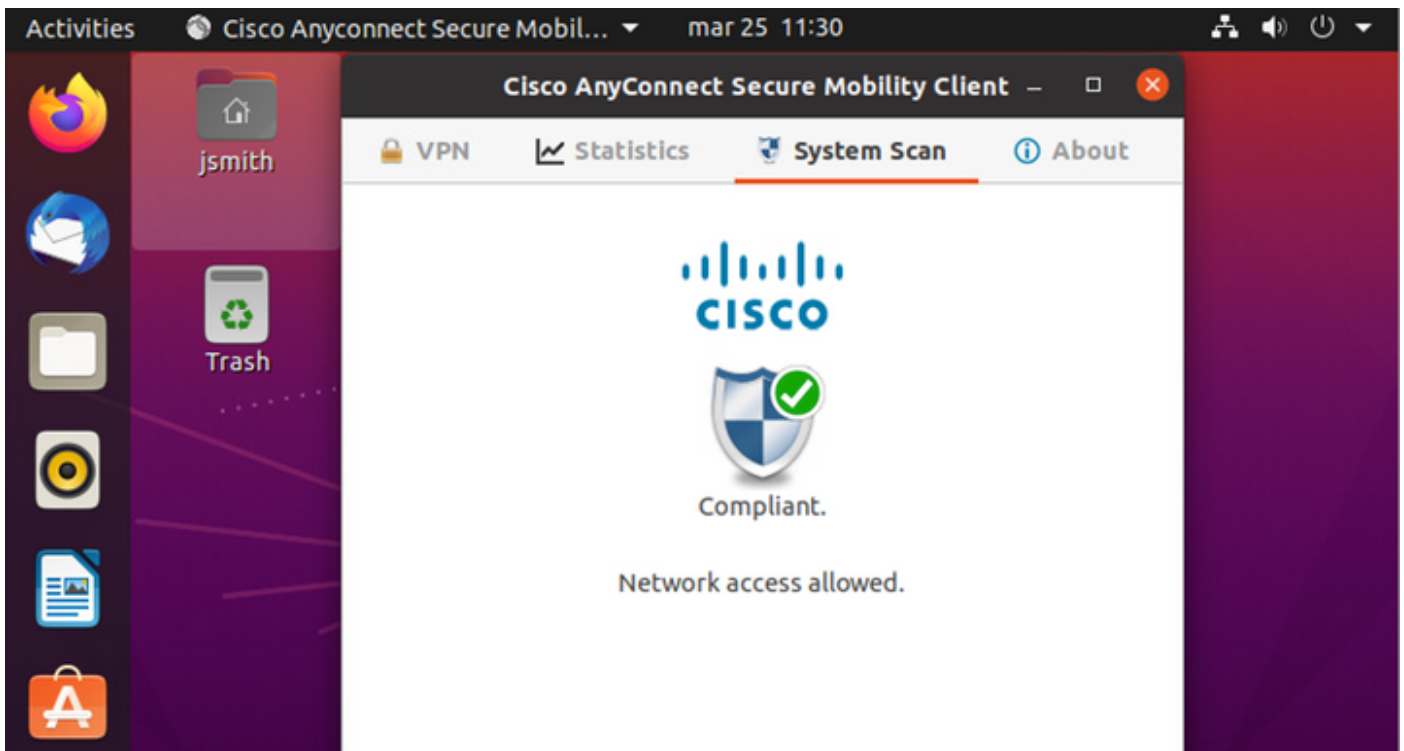
Devido a uma advertência conhecida, mesmo que o AnyConnect esteja instalado, ele não o detecta. Use **Alt-Tab** ou o menu **Atividades** para alternar para o cliente AnyConnect.

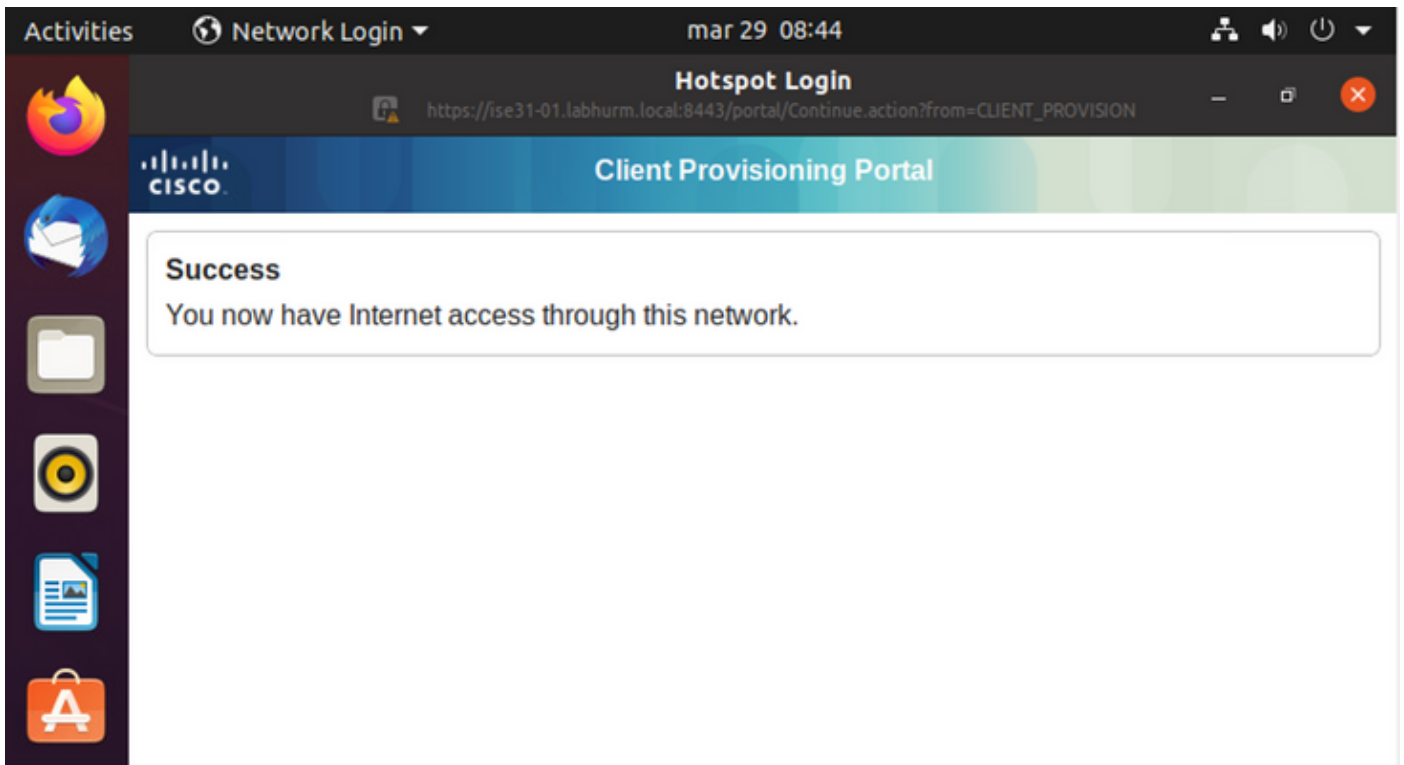


O AnyConnect tenta acessar a PSN para política de postura e avaliar o endpoint em relação a ela.



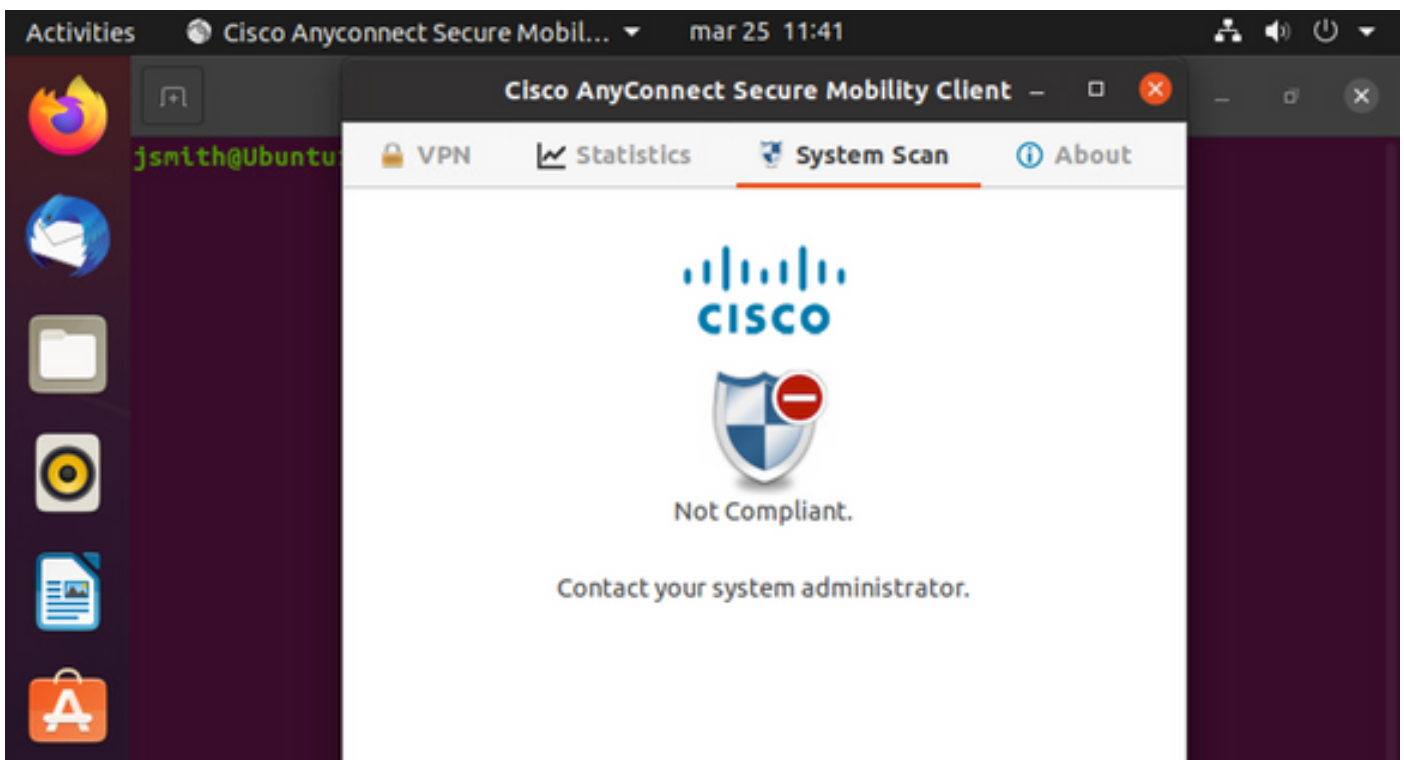
O AnyConnect reporta ao ISE sua determinação da política de postura. Neste caso, os





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 outro lado, se o arquivo não existir, o módulo de postura do AnyConnect relata a determinação ao 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: O FQDN do ISE precisa ser resolvível no sistema Linux através do DNS ou do arquivo de host local.

Troubleshoot

show authentication sessions int fa1/0/35

Redirecionamento no local:

```

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

```

Autorização bem-sucedida:

```

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

```

Não compatível, movido para VLAN e ACL de quarentena:

```
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
```