Configurar a postura do Cisco ISE 3.1 com Linux

Contents

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)

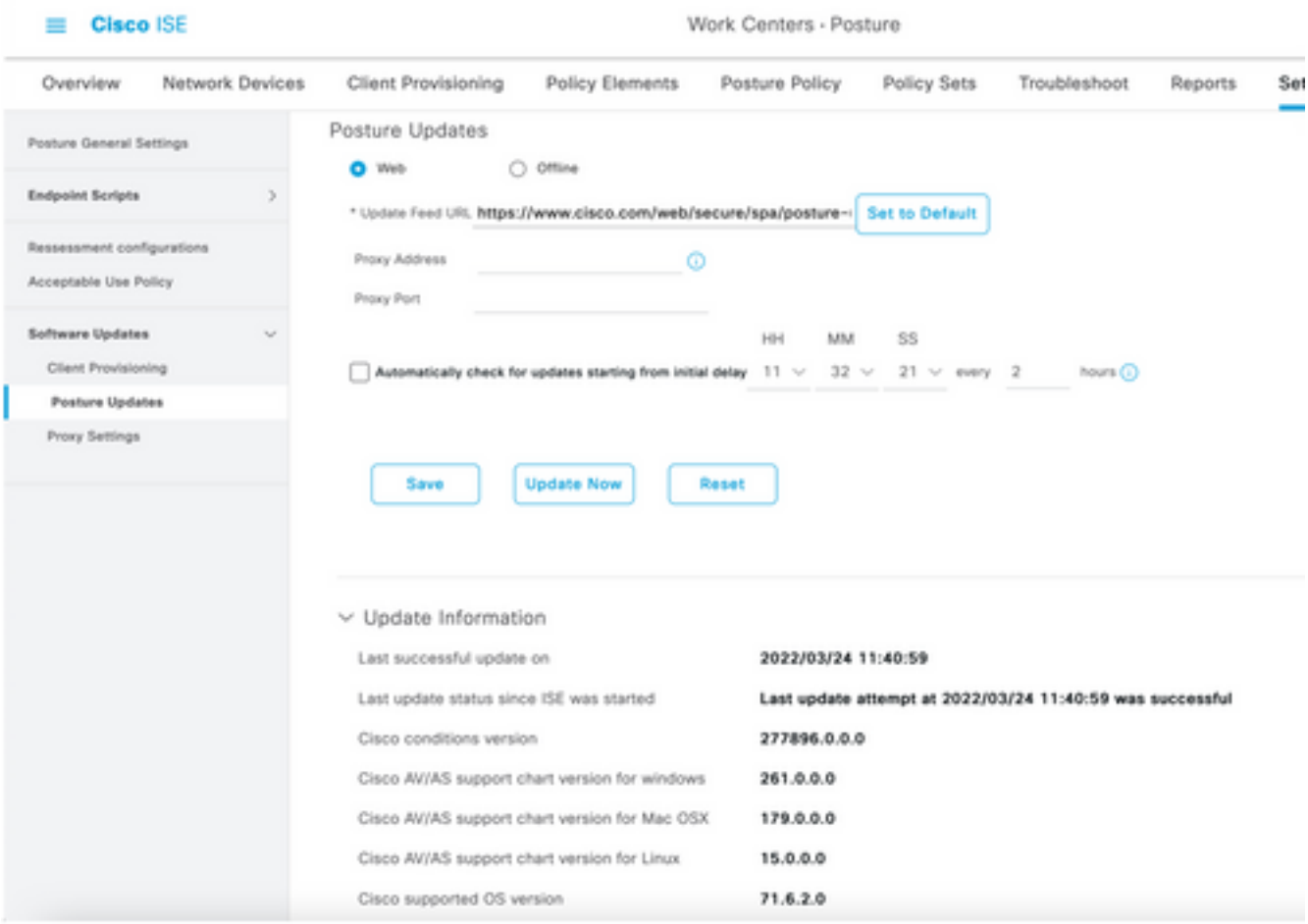
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

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:

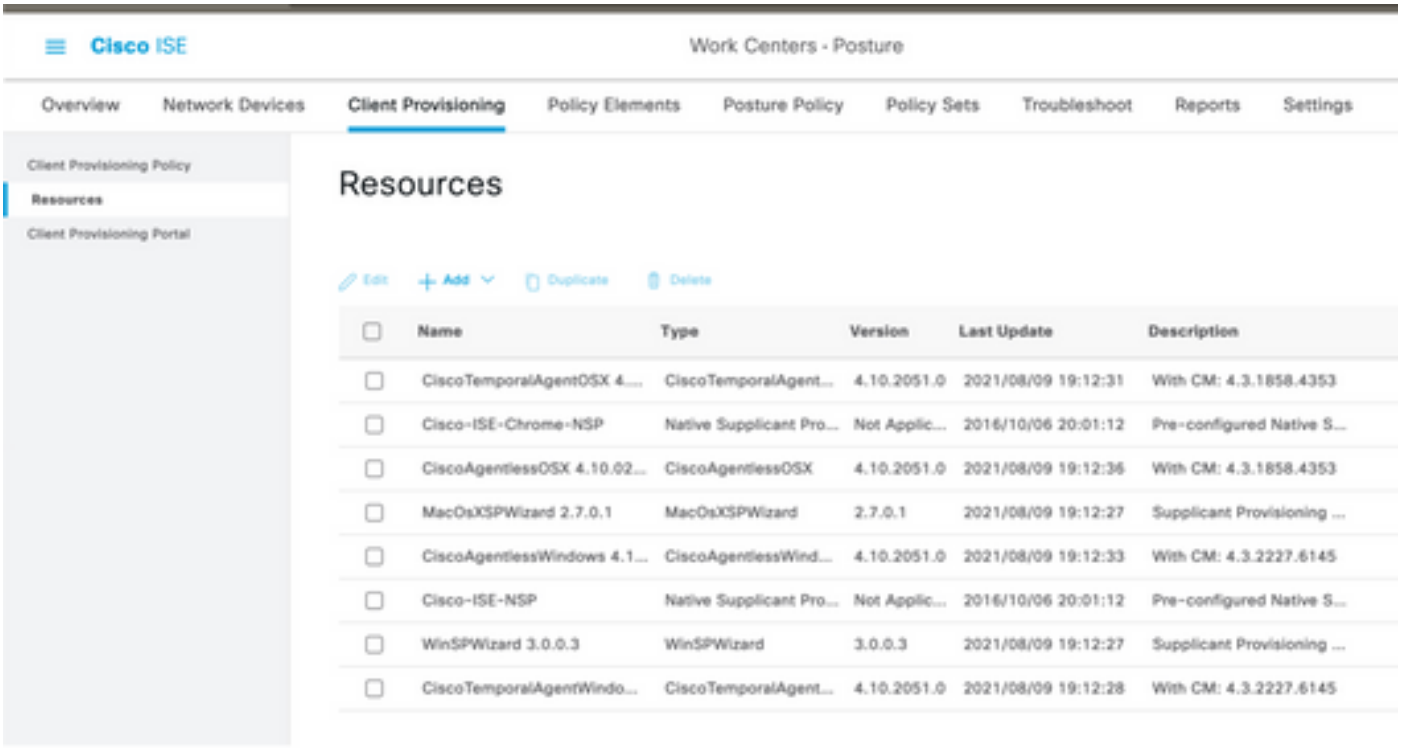


Um **pacote fornecido pela Cisco** é um pacote de software que você baixa do site Cisco.com, como os pacotes de software do AnyConnect. Um **pacote criado pelo cliente** é um perfil ou uma configuração que você criou fora da interface de usuário do ISE e deseja carregar no ISE para uso com avaliação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

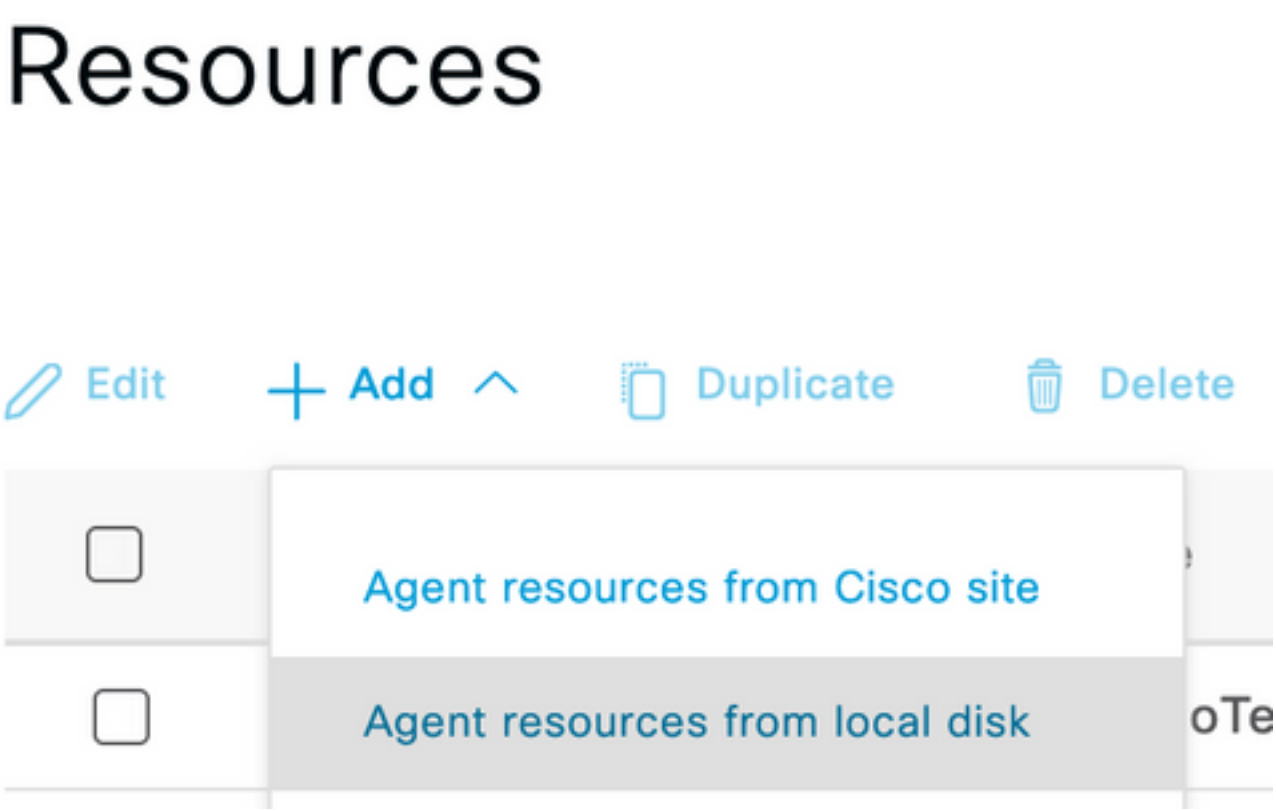
> **Note**: Devido a atualizações e patches, a versão recomendada pode ser alterada. Use a versão recomendada mais recente do site cisco.com.

Etapa 2. Carregar pacote do AnyConnect:

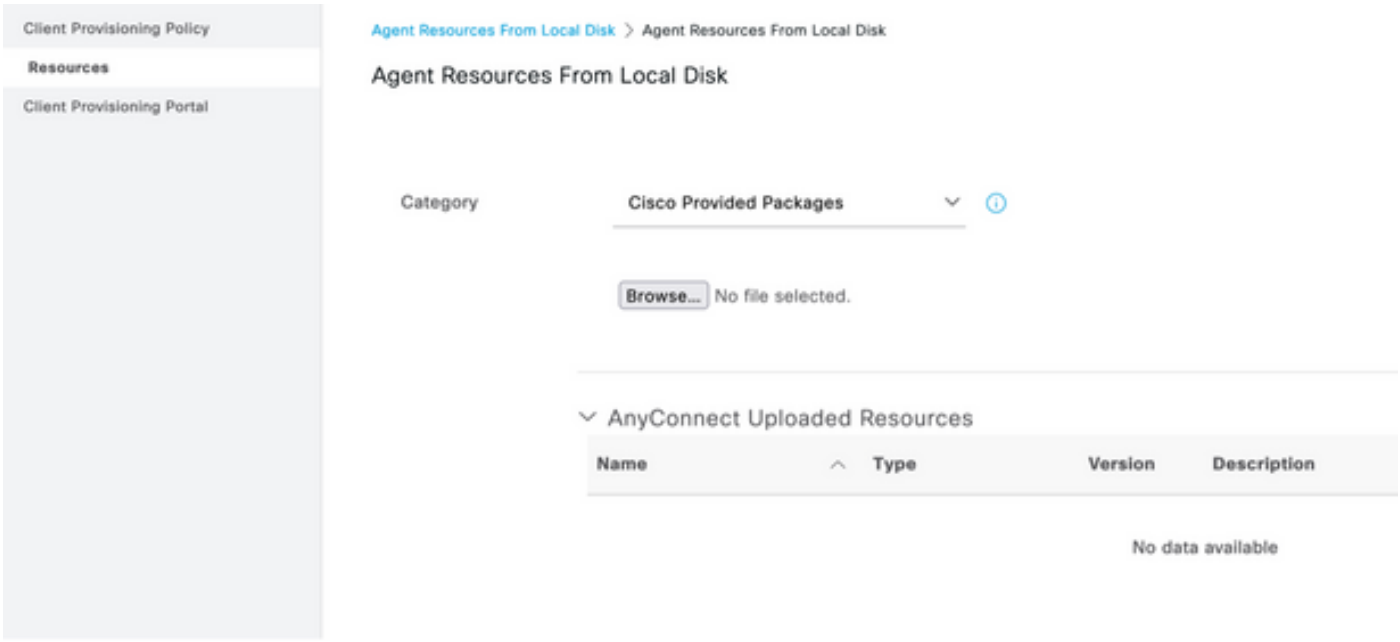
No Centro de trabalho com postura, navegue até **Provisionamento de cliente > Recursos**



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

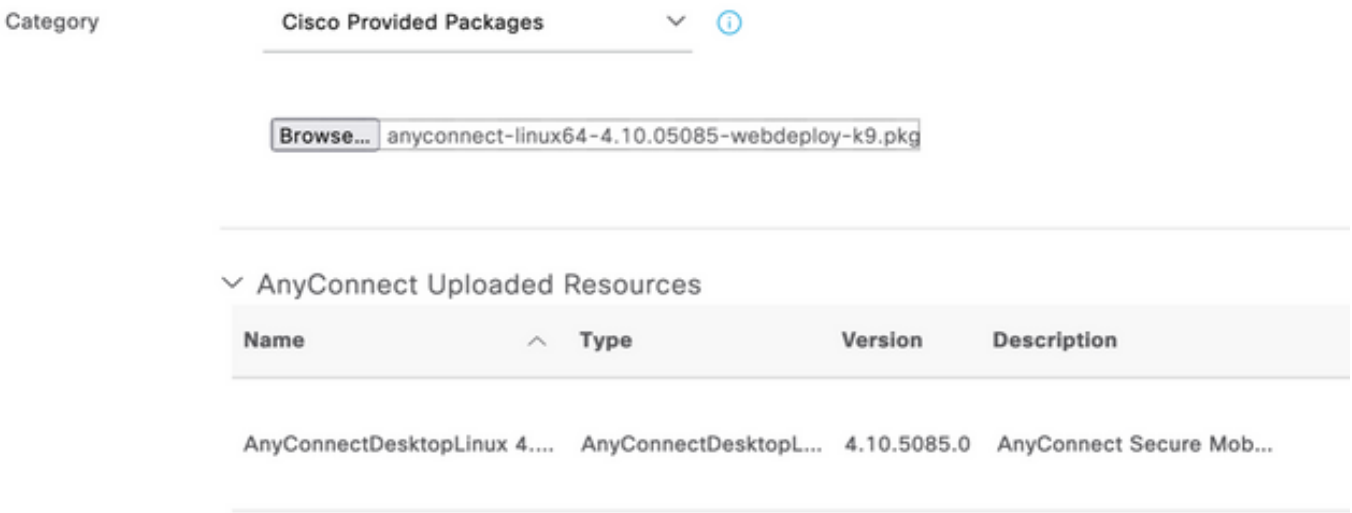


Etapa 4. Selecione **Cisco Provided Packages** no menu suspenso Categoria.



Etapa 5. Clique em Procurar.

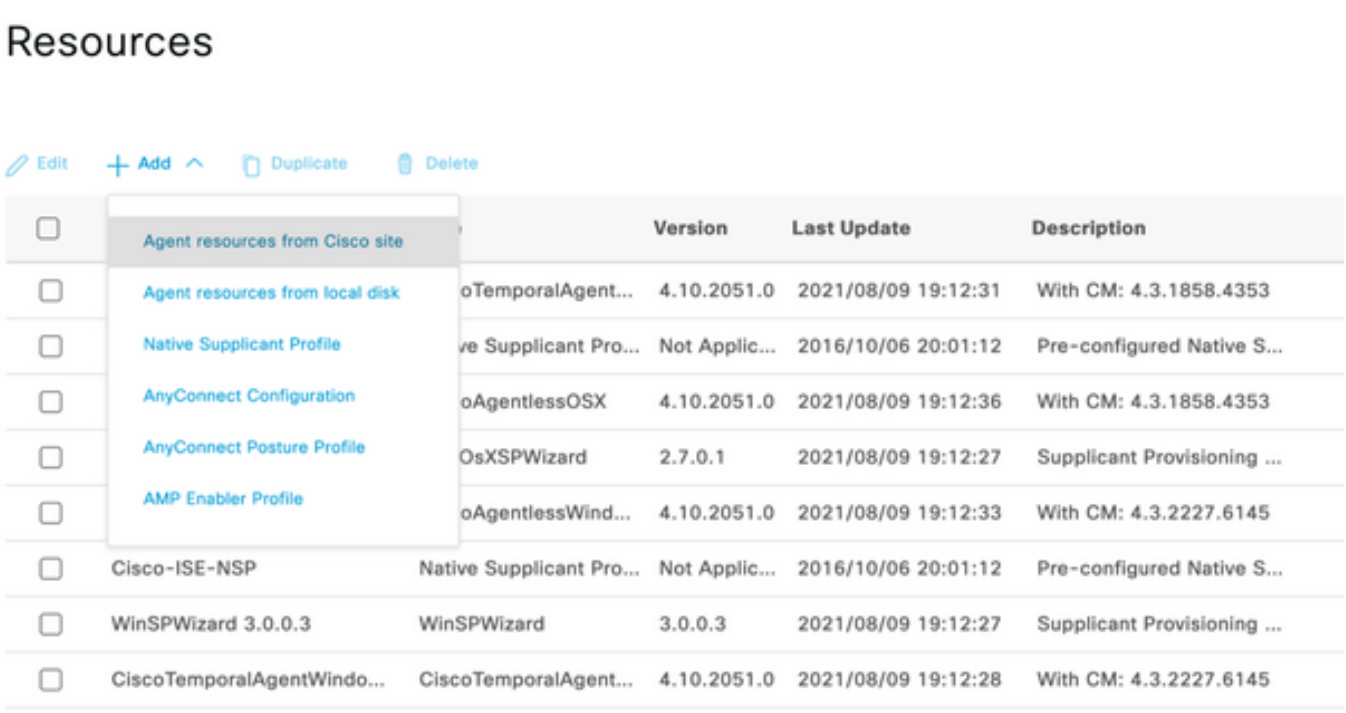
Etapa 6. Escolha um dos pacotes do AnyConnect que você baixou na etapa anterior. A imagem do AnyConnect é processada e as informações sobre o pacote são exibidas



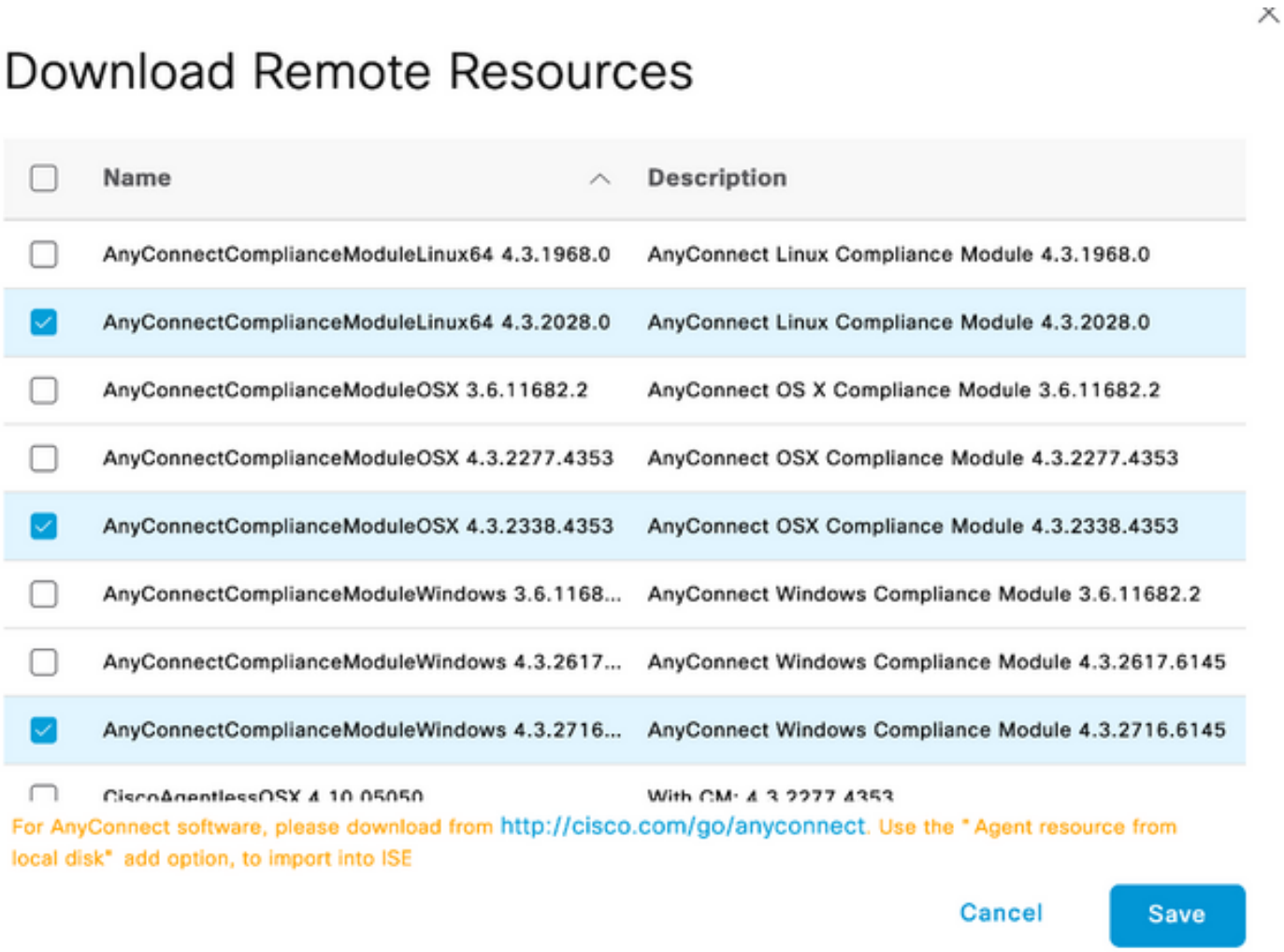
Etapa 7. Clique em **Enviar**. Agora que o AnyConnect está carregado no ISE, você pode ter contato com o ISE e obter os outros recursos do cliente do Cisco.com.

> **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.



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.



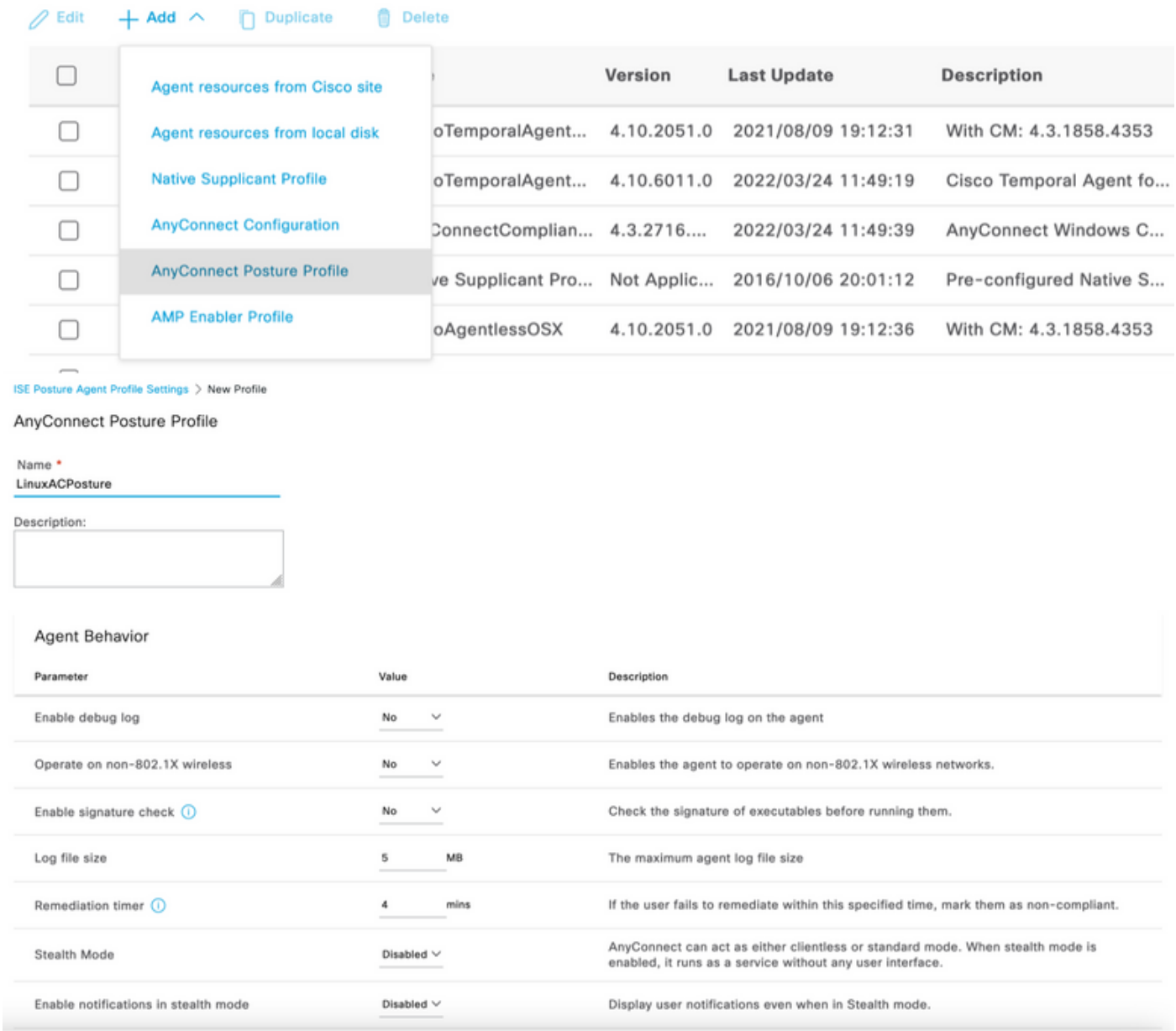
Etapa 10. Selecione os agentes temporais mais recentes para Windows e Mac.

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.



Os parâmetros que precisam ser modificados são:

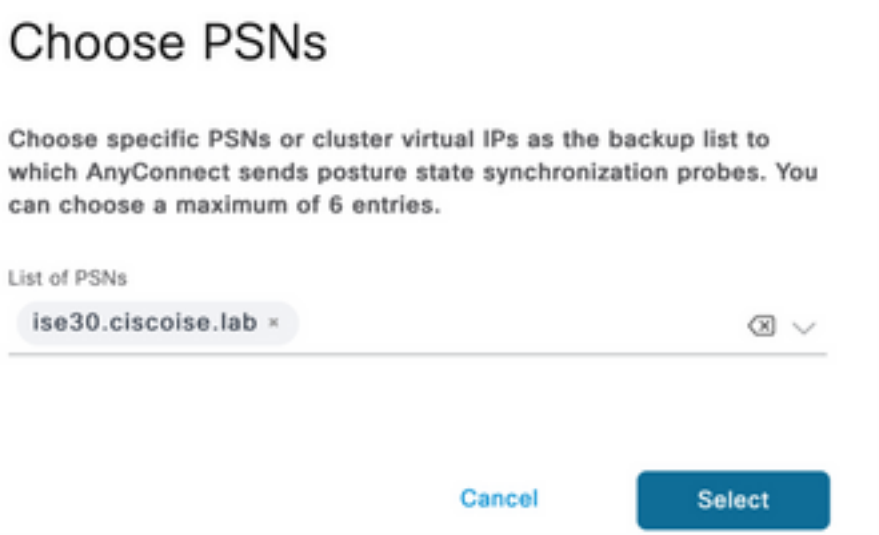
- **Intervalo de detecção de VLAN**: Essa configuração permite que você defina o número de segundos que o módulo aguarda entre os testes de alterações de VLAN. A recomendação é de 5 segundos.
- **Ping ou ARP**: Este é o método real de detecção de alteração de VLAN. O agente pode fazer ping no gateway 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.

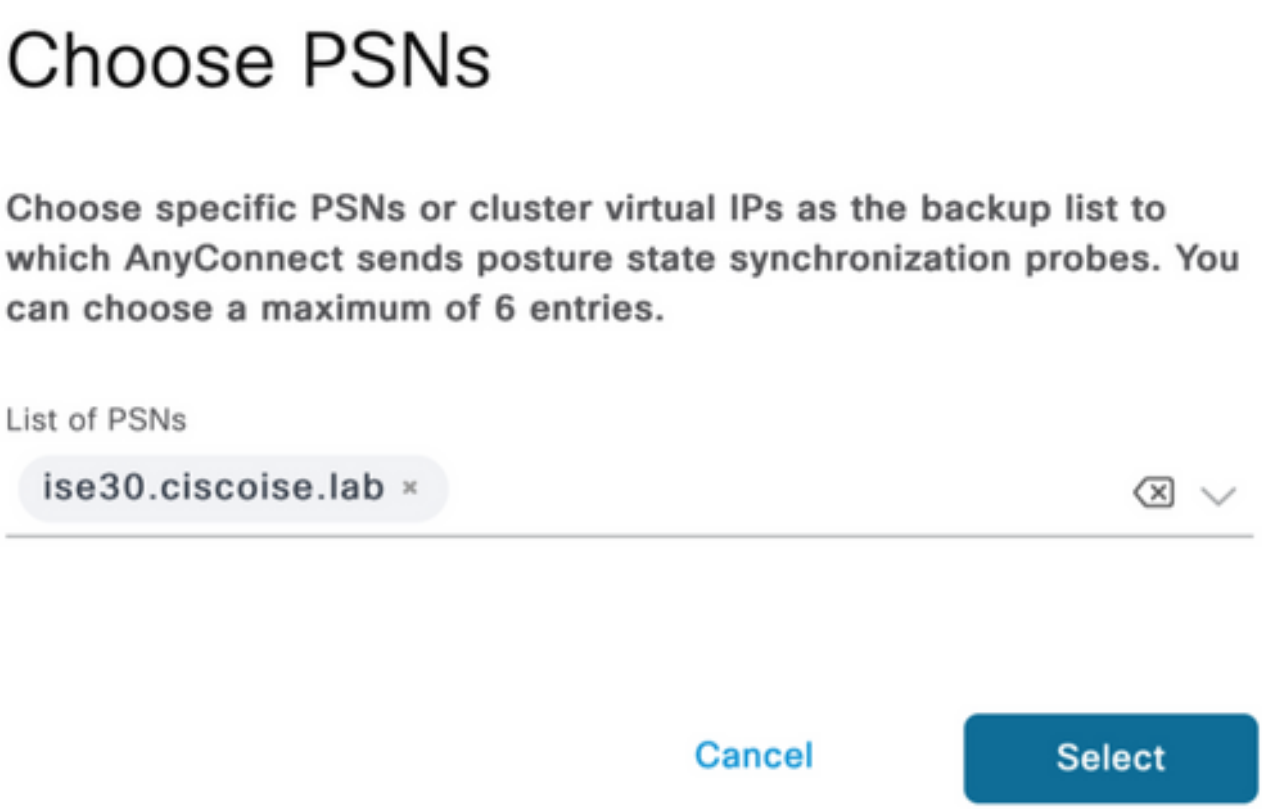
Para obter uma descrição abrangente de todos os parâmetros, consulte a documentação de postura do ISE ou do AnyConnect.

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

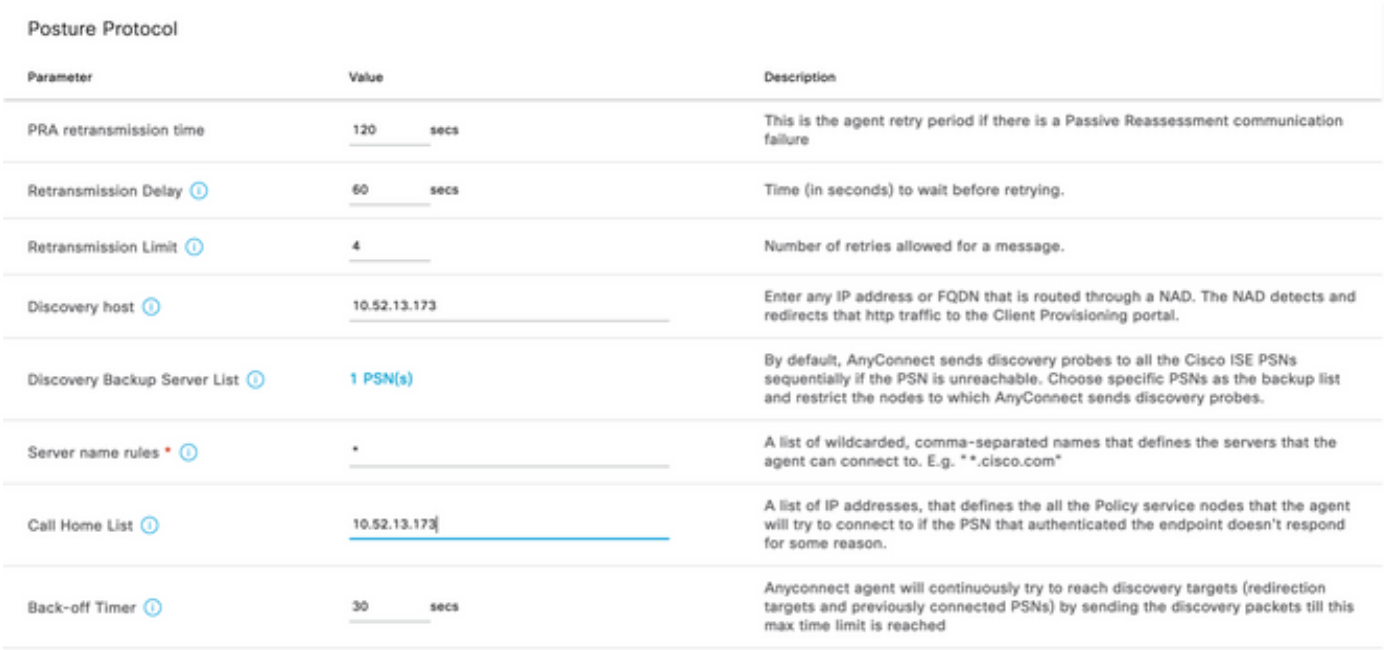


Etapa 14. Em Posture Protocols > Discovery Host, defina o endereço IP do nó PSN/independente.

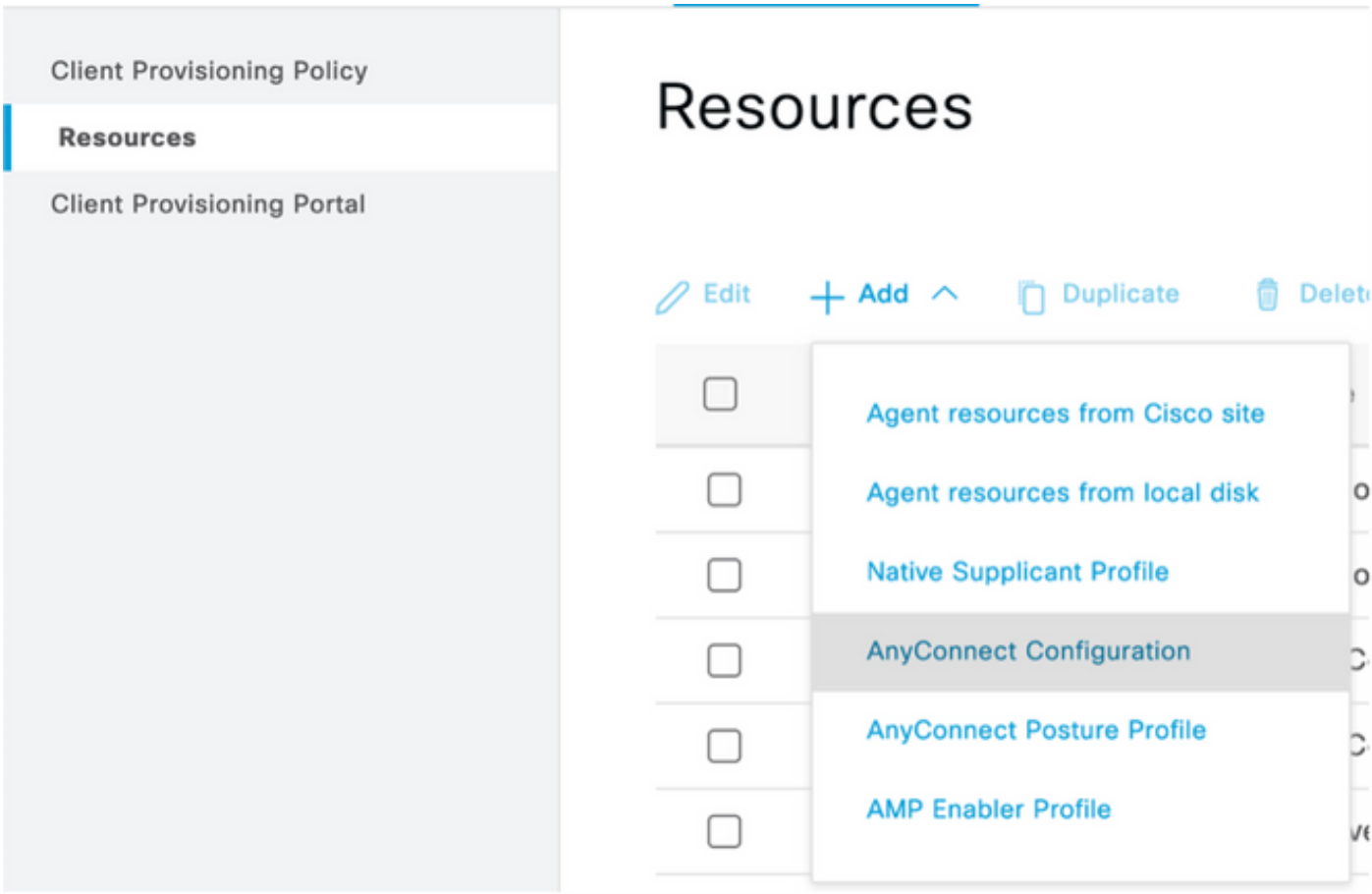
Etapa 15. Em **Discovery backup server list** e Select **escolha,** selecione seu PSN ou FQDN independente e selecione **Select.**

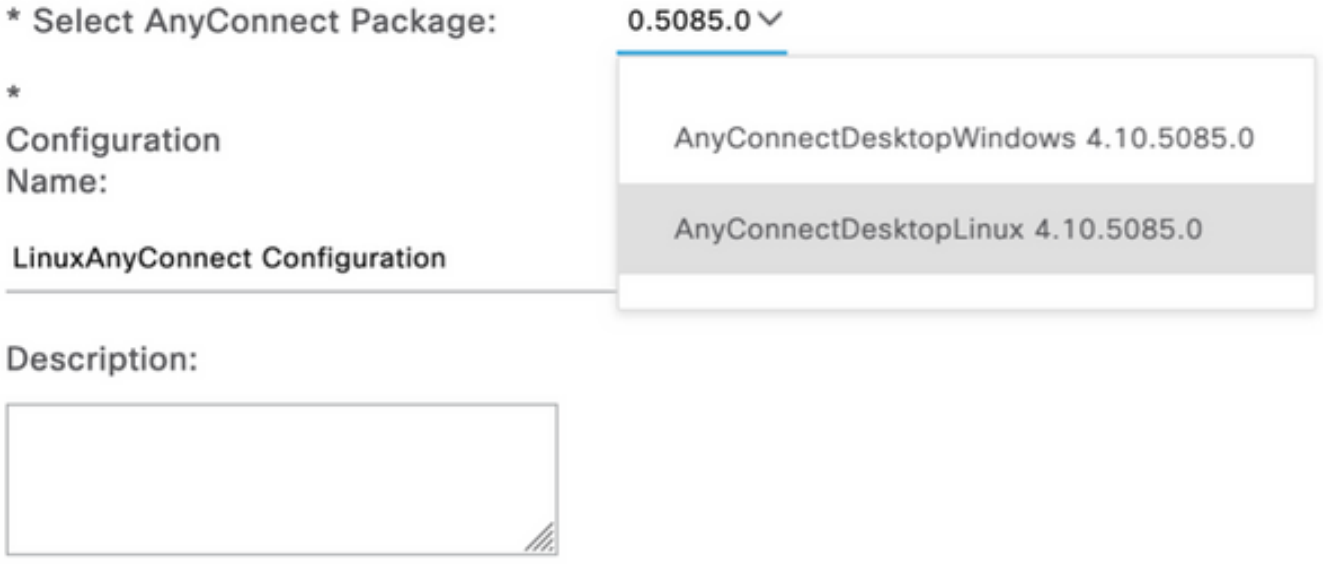


Etapa 16. Em **Server name rules** digite ***** para entrar em contato com todos os servidores e definir o endereço IP PSN/Standalone sob **call home list.** Como alternativa, um curinga pode ser usado para corresponder todos os PSNs em potencial em sua rede (ou seja, *.acme.com).



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


Client Provisioning Policy
Resources
Client Provisioning Portal
Resources
Edit
Add
Duplicate
Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
AnyConnect Configuration
AnyConnect Posture Profile
AMP Enabler Profile


* Select AnyConnect Package:
0.5085.0
*
Configuration
Name:
LinuxAnyConnect Configuration
Description:
AnyConnectDesktopWindows 4.10.5085.0
AnyConnectDesktopLinux 4.10.5085.0

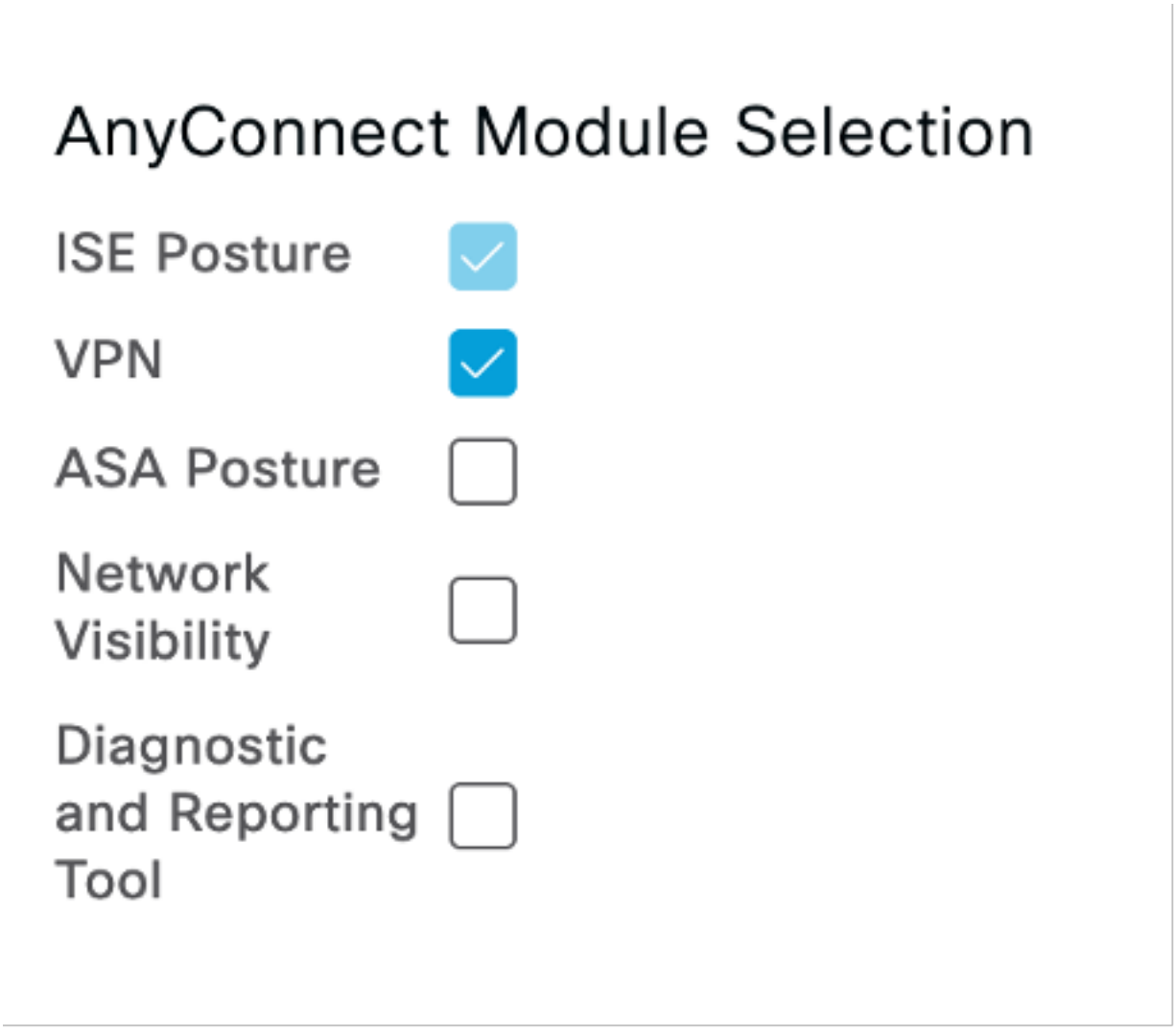
Description Value Notes

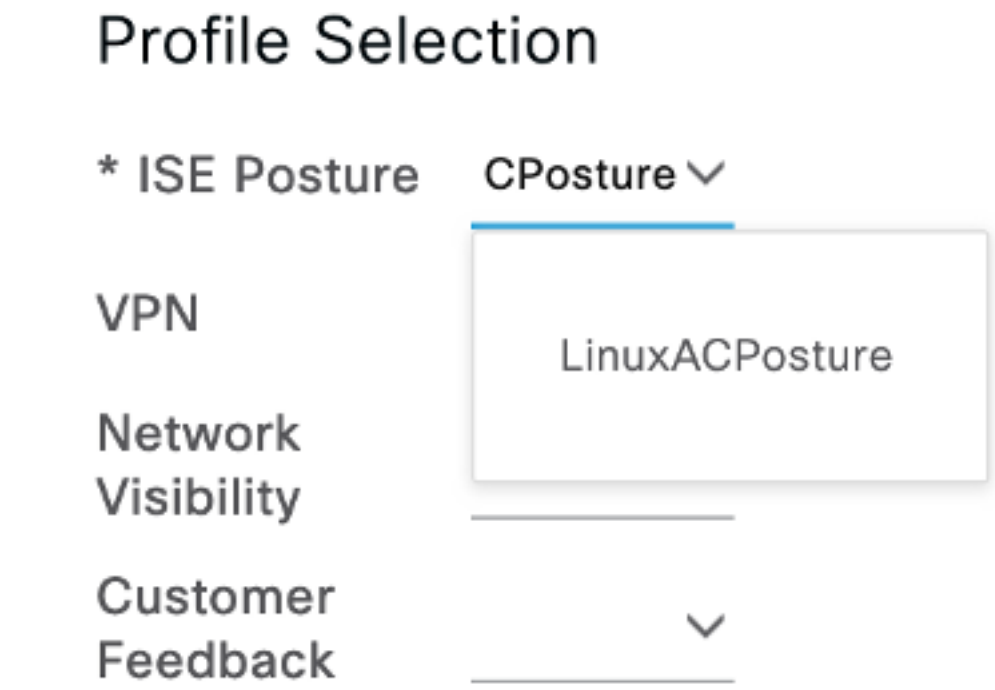
* Compliance Module 3.2028.0

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

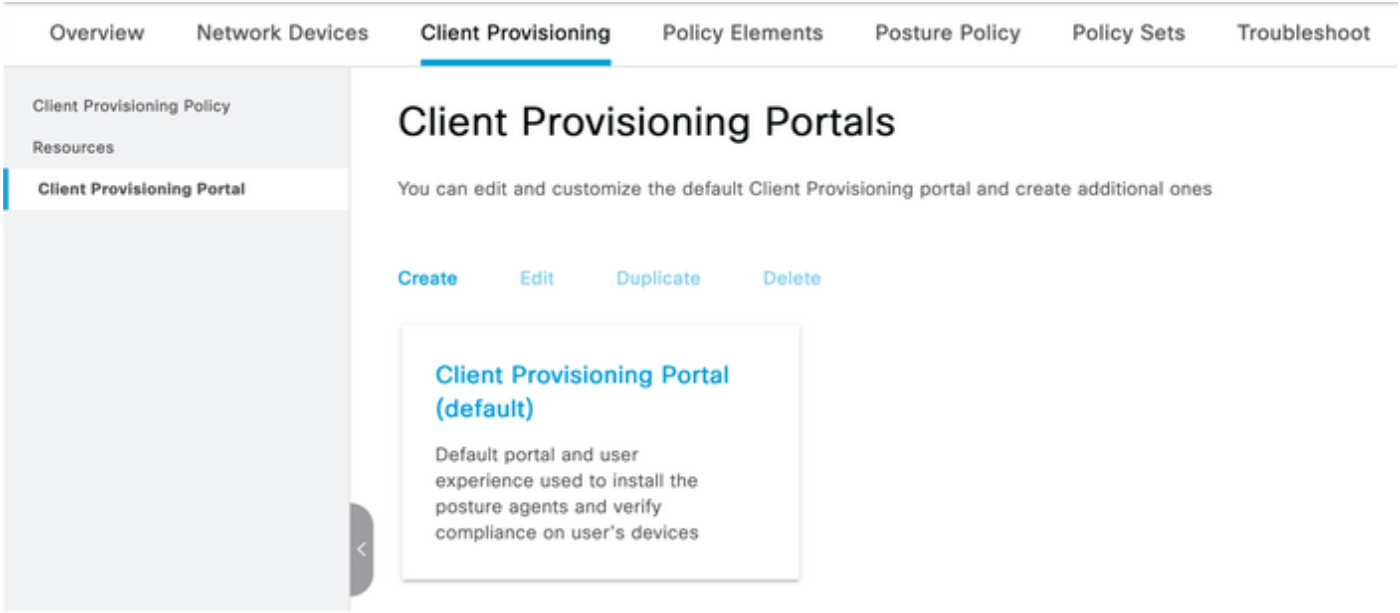




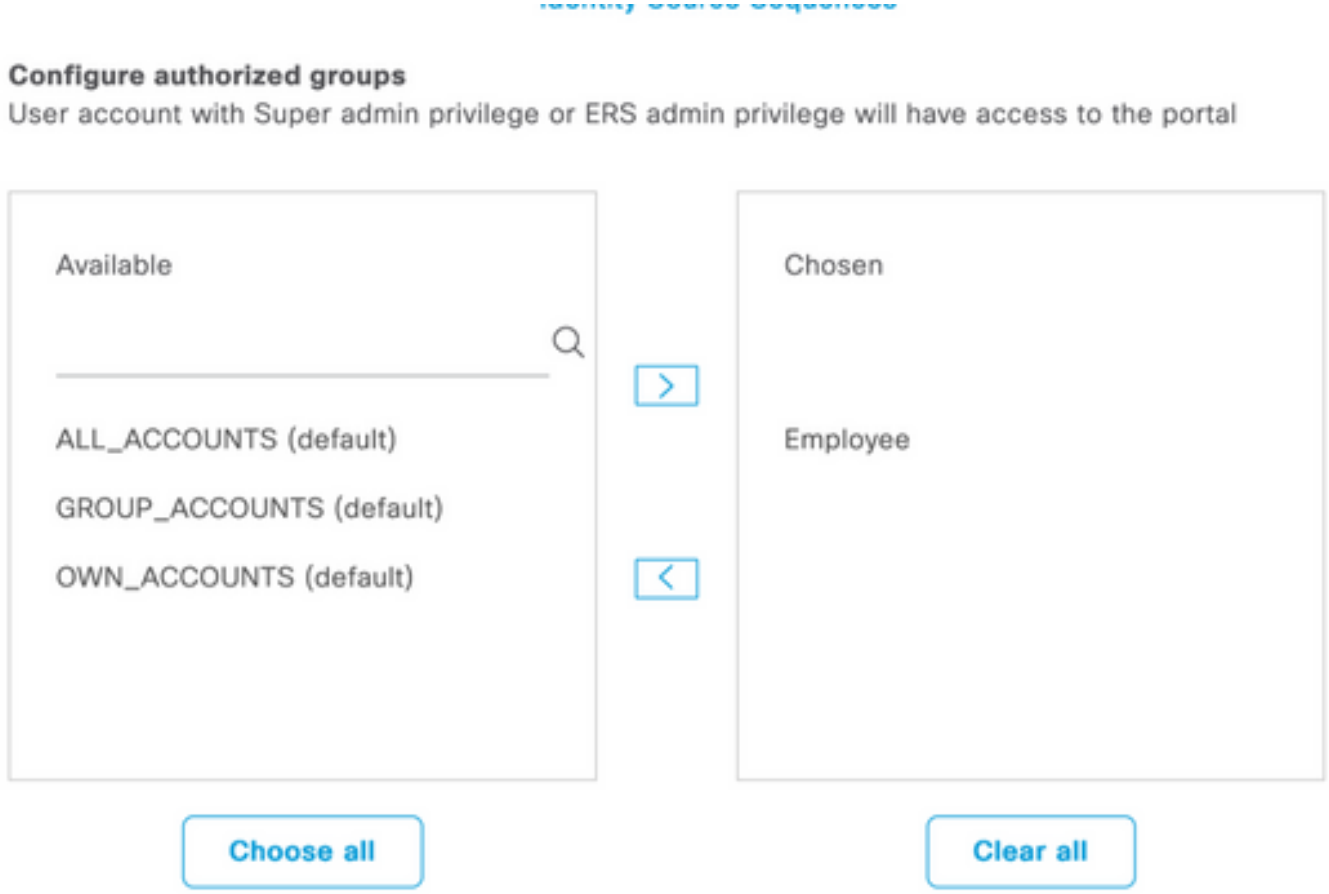
Role para baixo e selecione Enviar

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

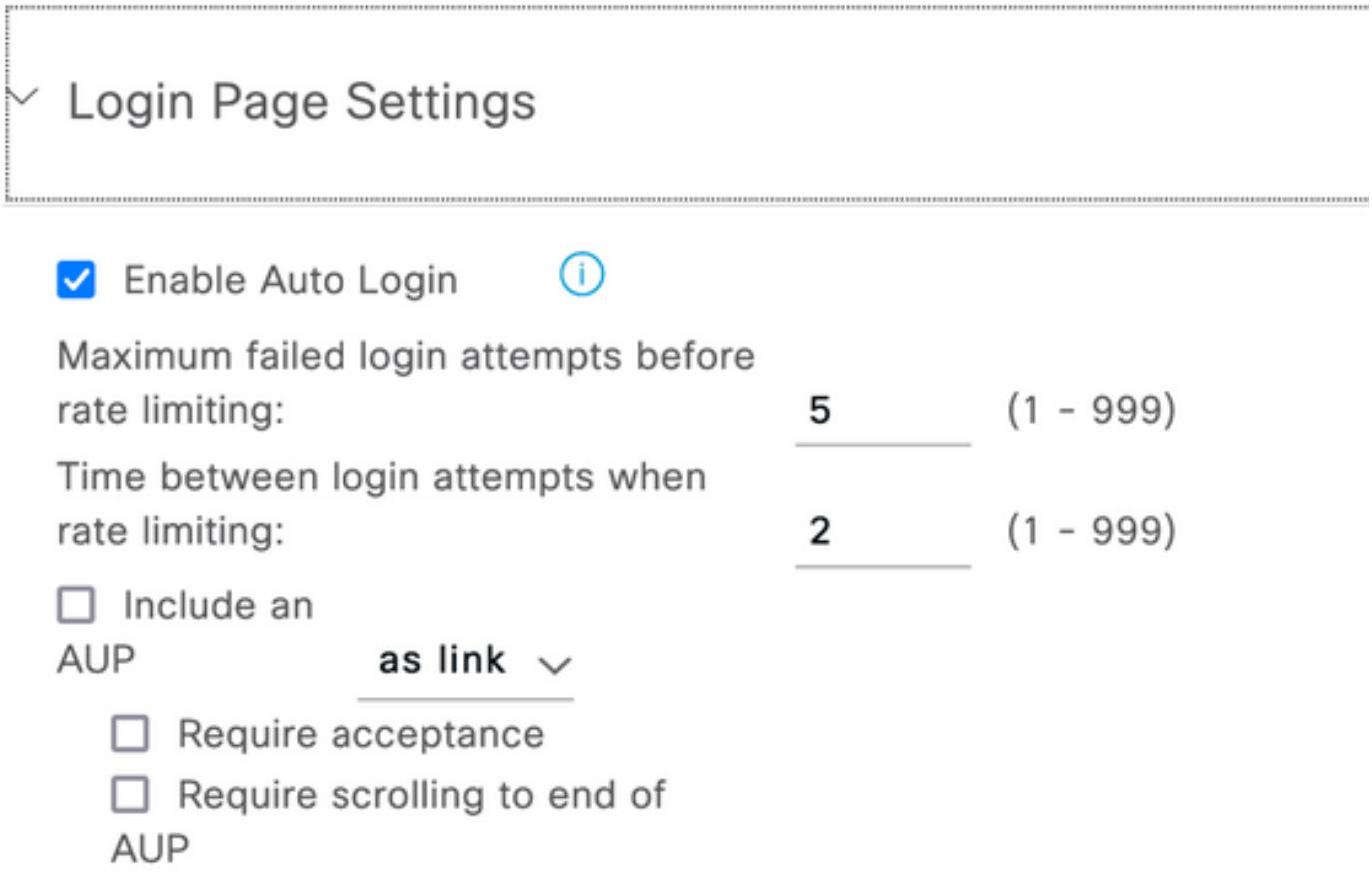
Etapa 19. Selecione **Centros de Trabalho > Postura > Provisionamento de Cliente > Portais de Provisionamento de Cliente.**



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.



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



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

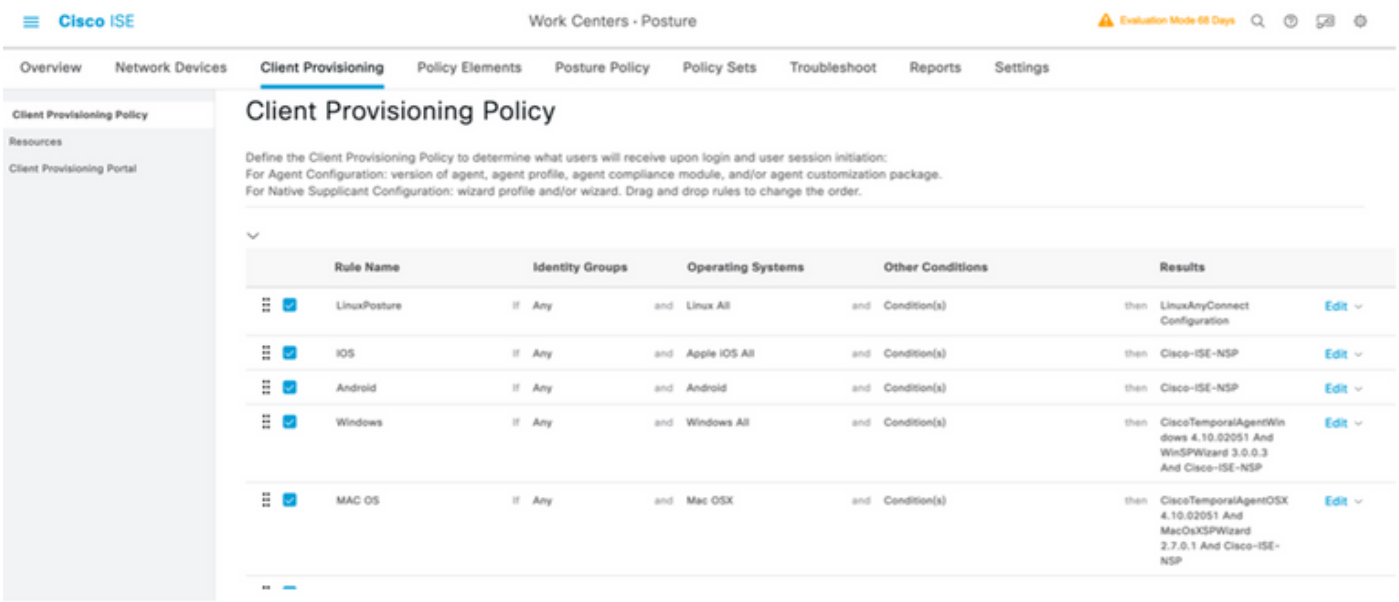
Etapa 23. Selecione **Centros de trabalho > Postura > Provisionamento de cliente > Política de provisionamento de cliente.**

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.



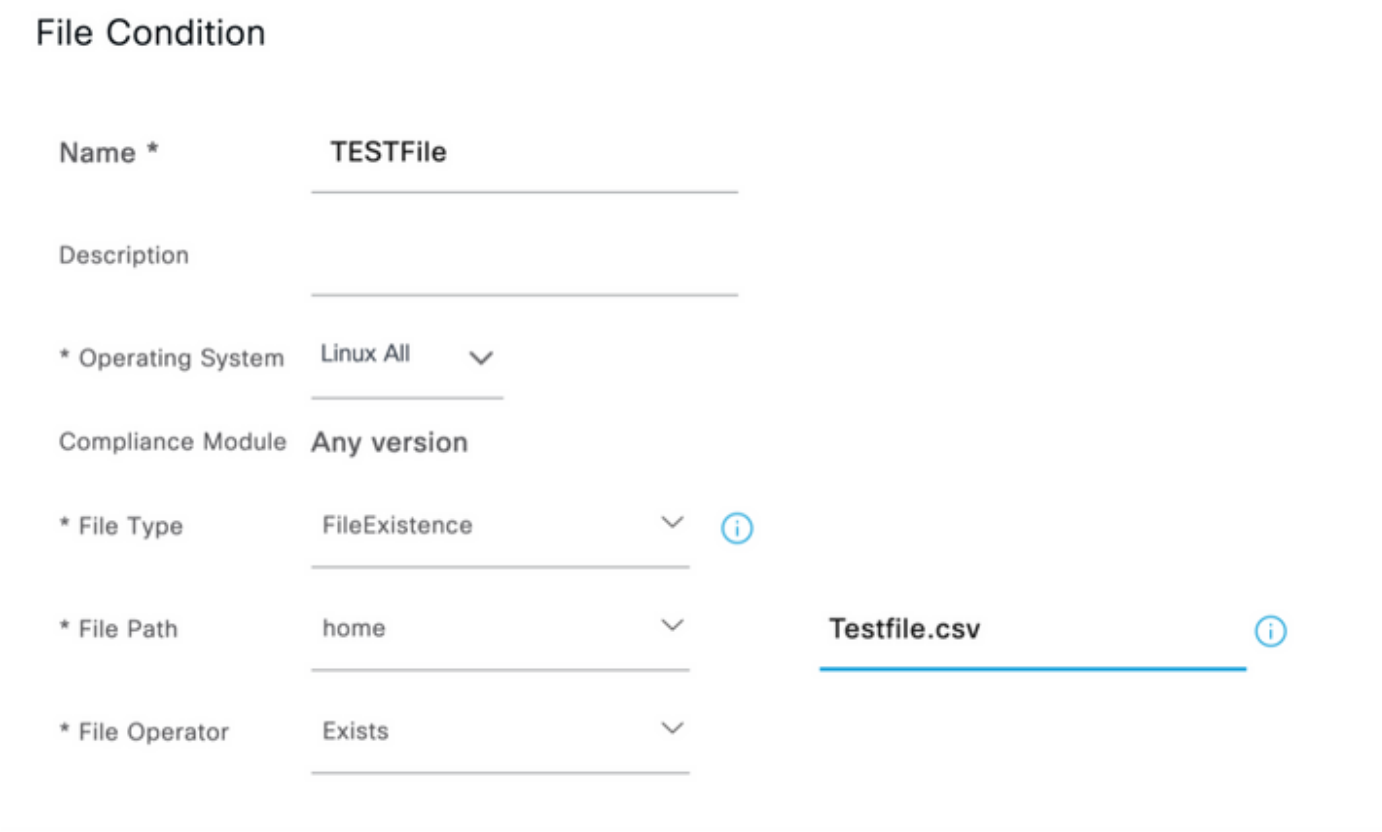
Etapa 27. Clique em **Concluído**.

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

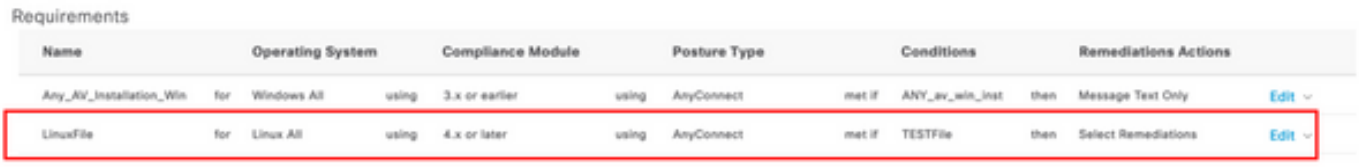


Note: O caminho é baseado no local do arquivo.

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:



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

Componentes de requisito

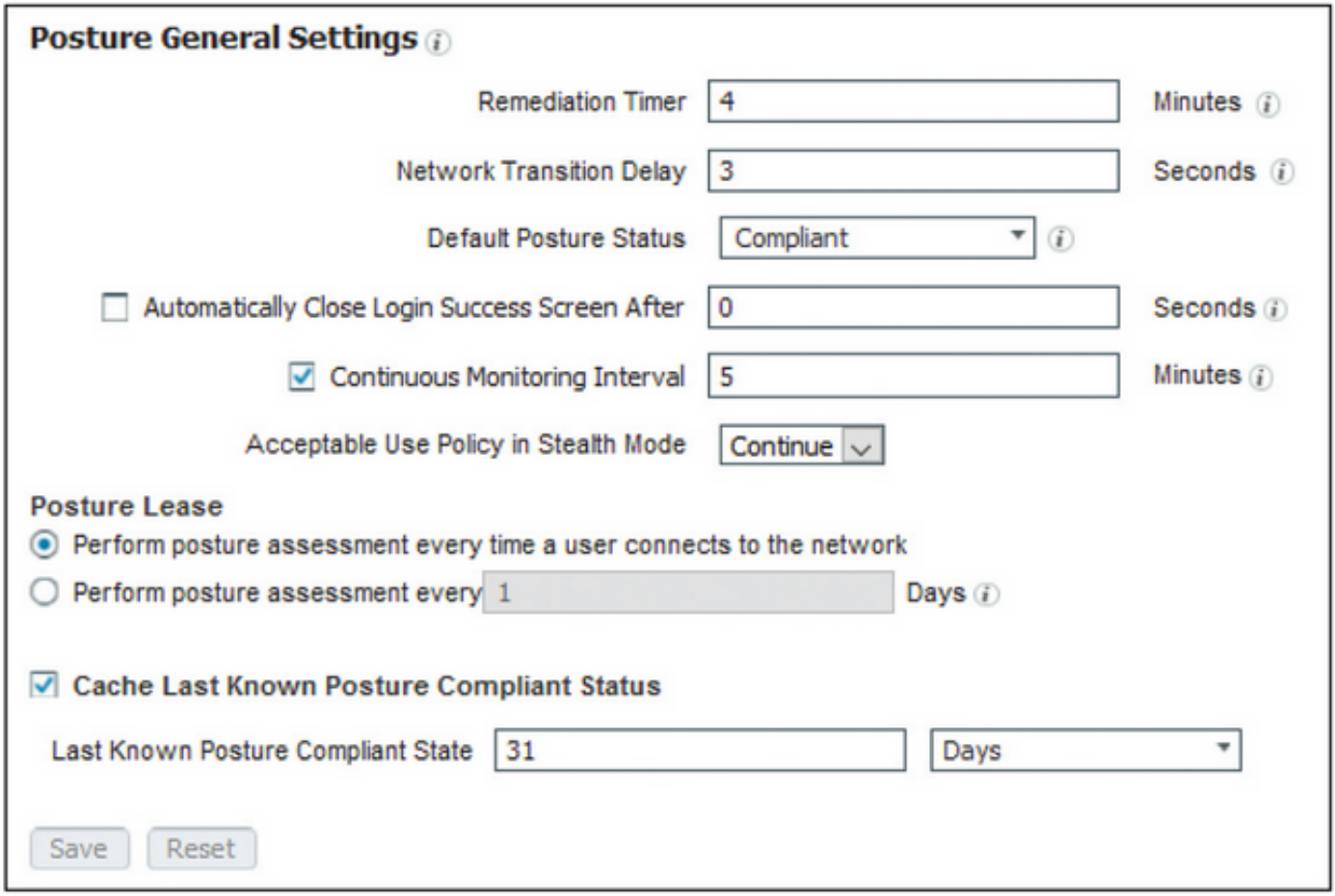
- **Sistema operacional:** Todos no Linux
- **Módulo de conformidade:** 4.x
- **Tipo de postura:** AnyConnect
- **Condições:** Módulos e agentes de conformidade (que ficam disponíveis depois que você seleciona o SO)
- **Ações de correção:** Remediações que ficam disponíveis para seleção depois que todas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

Etapa 35. Selecione **Concluído** e **Salvar**

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



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**

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 <isepsnnode_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 preiodic 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
```

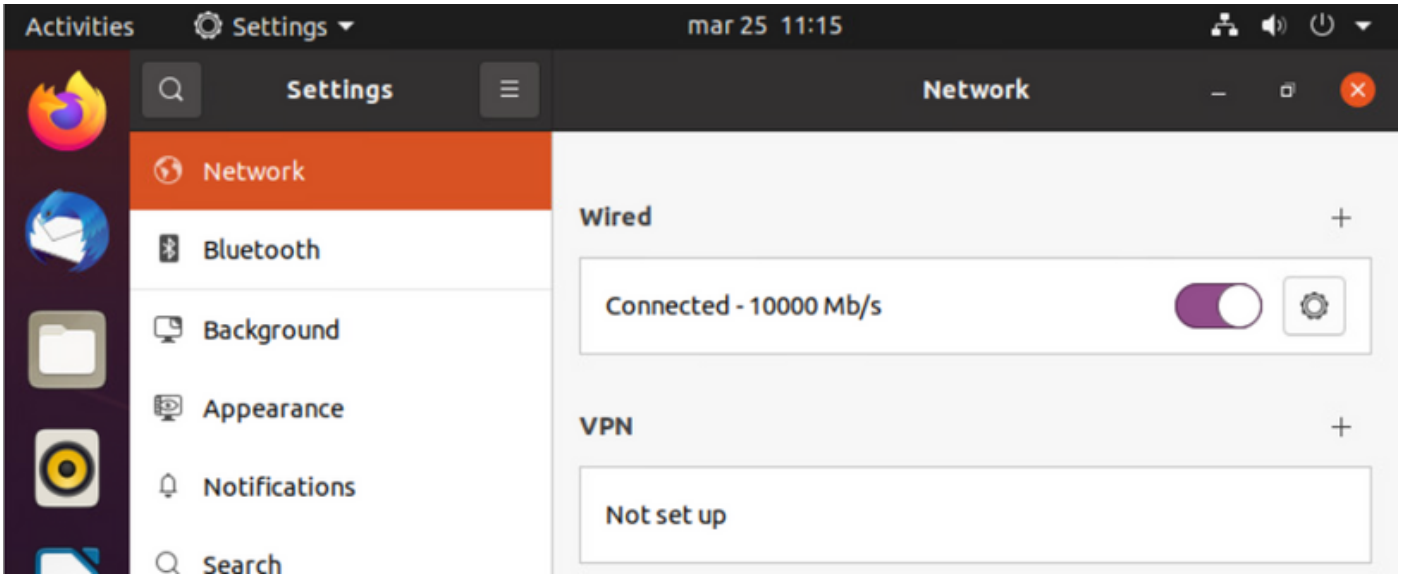
Verificar

Verificação do ISE:

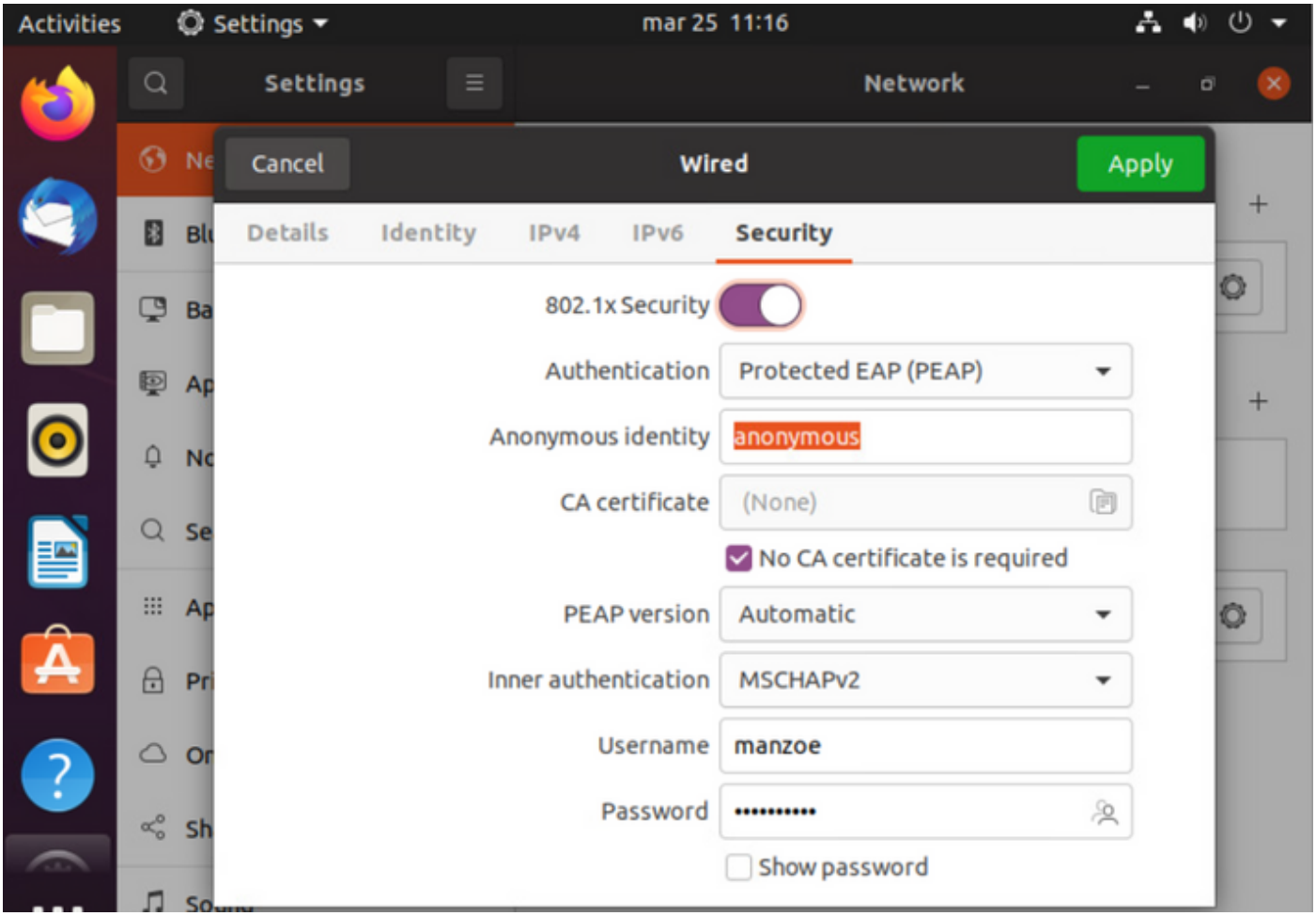
Esta seção pressupõe que o AnyConnect com o módulo de postura ISE foi instalado anteriormente no sistema Linux.

Autenticar o PC usando dot1x

Etapa 1. Navegue até Network Settings

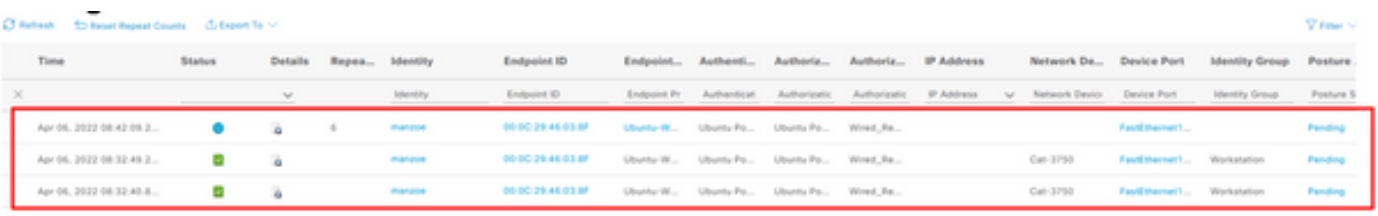


Etapa 2. Selecione a guia Security e forneça a configuração 802.1x e as credenciais do usuário

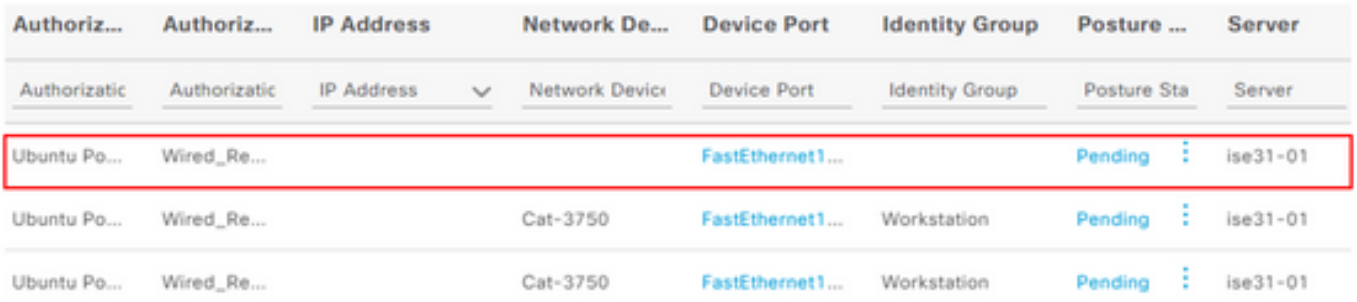


Etapa 3. Clique em **"Aplicar".**

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

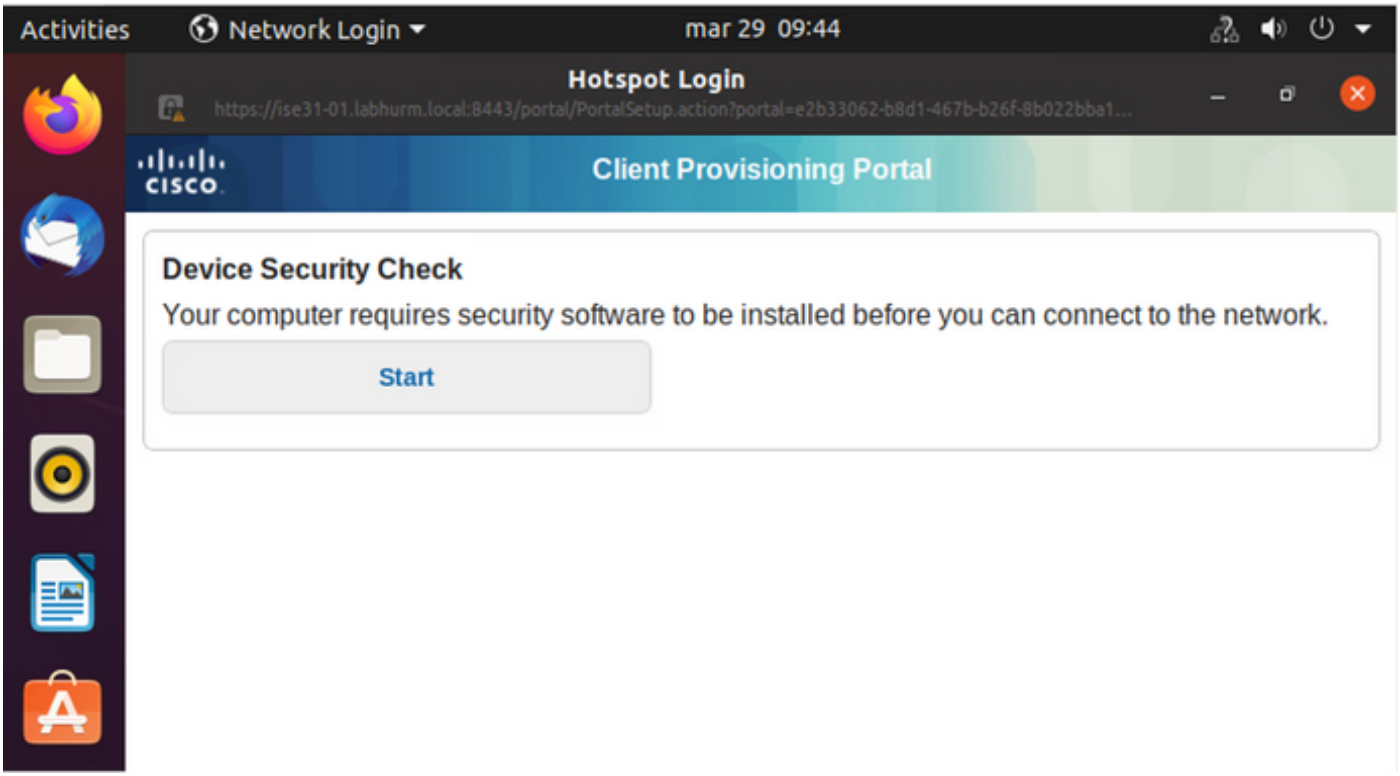


No ISE, use a barra de rolagem horizontal para exibir informações adicionais, como a PSN que serviu o fluxo ou o status da postura:

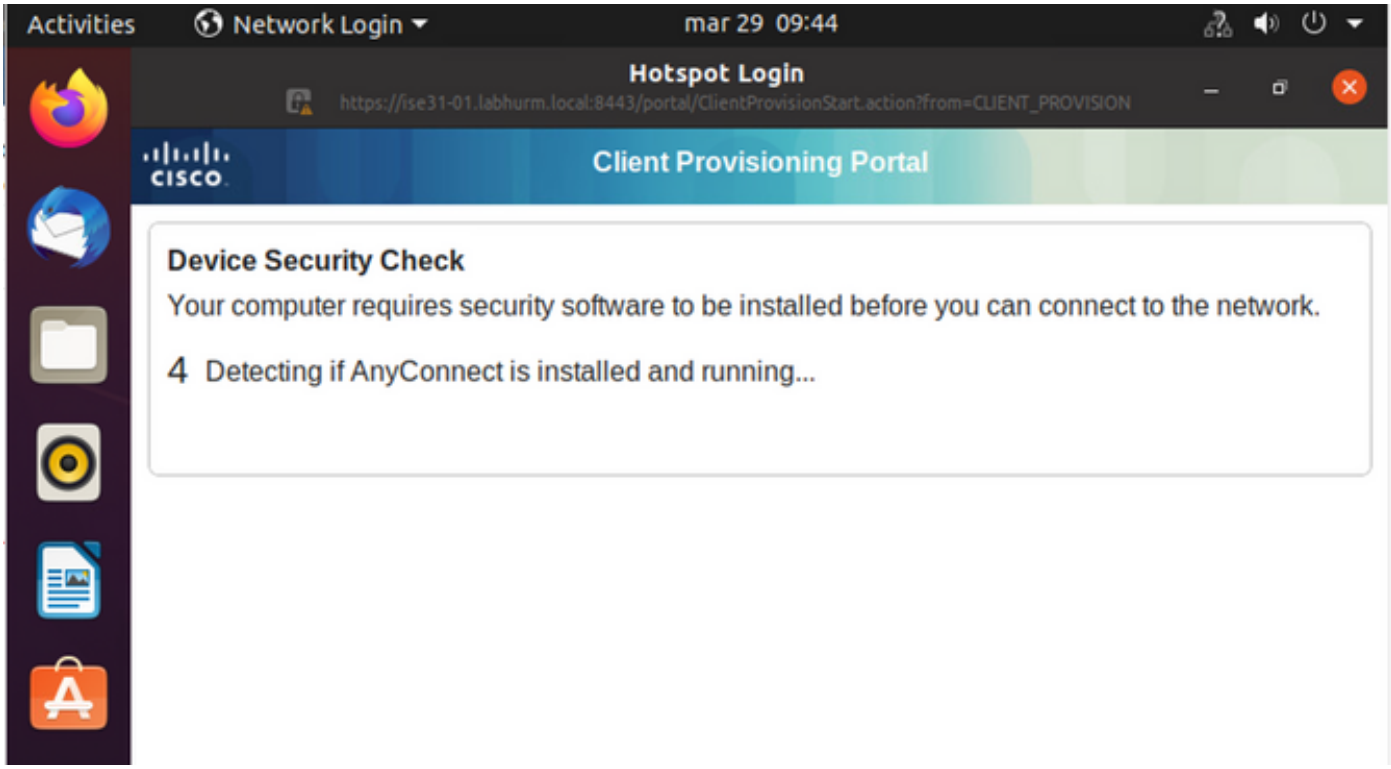


Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Posture Sta	Server
Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...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

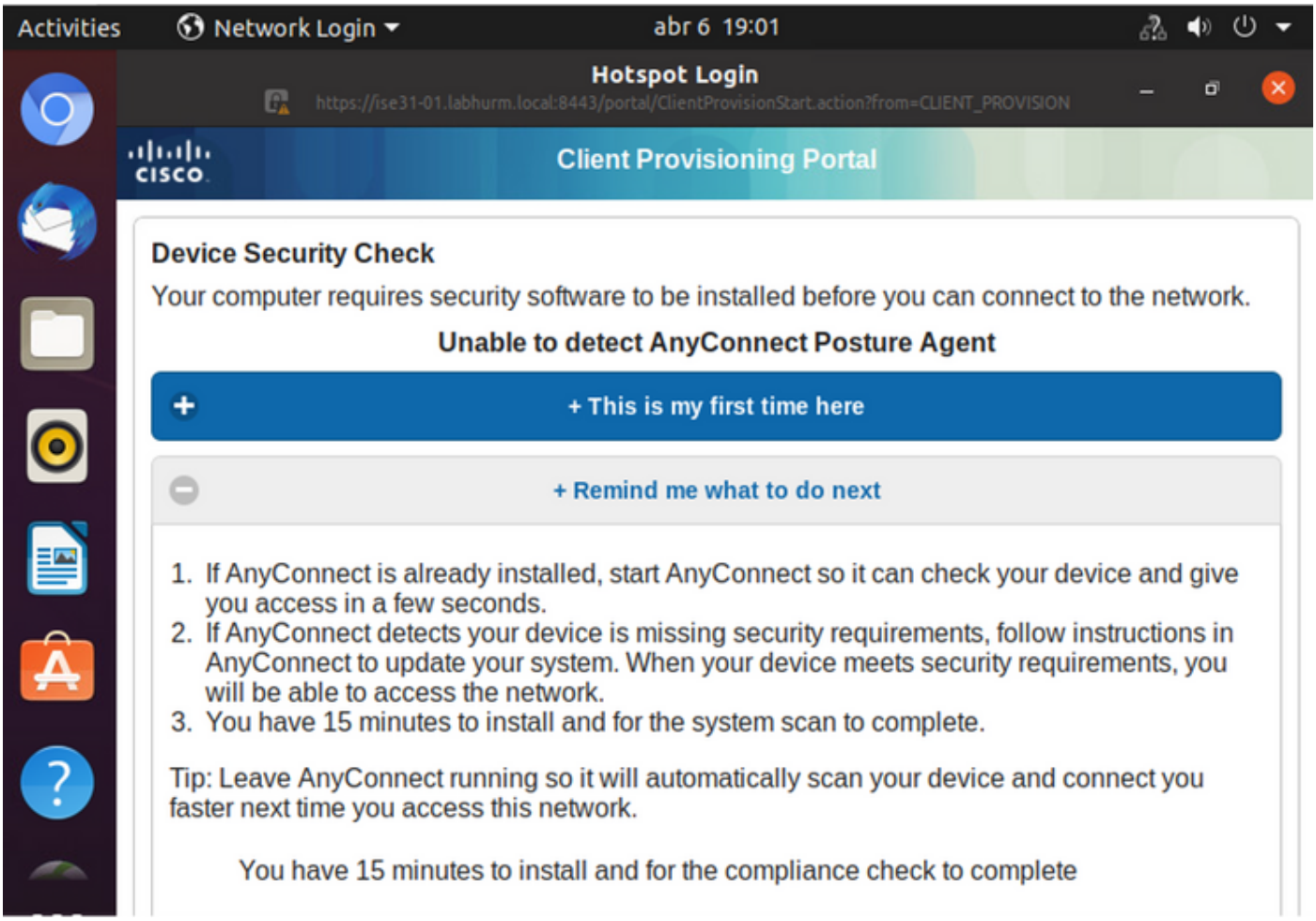
Etapa 5. No cliente Linux, o redirecionamento deve ocorrer, e ele apresenta o portal de provisionamento do cliente indicando a ocorrência da verificação de postura e para clicar em **"Iniciar":**



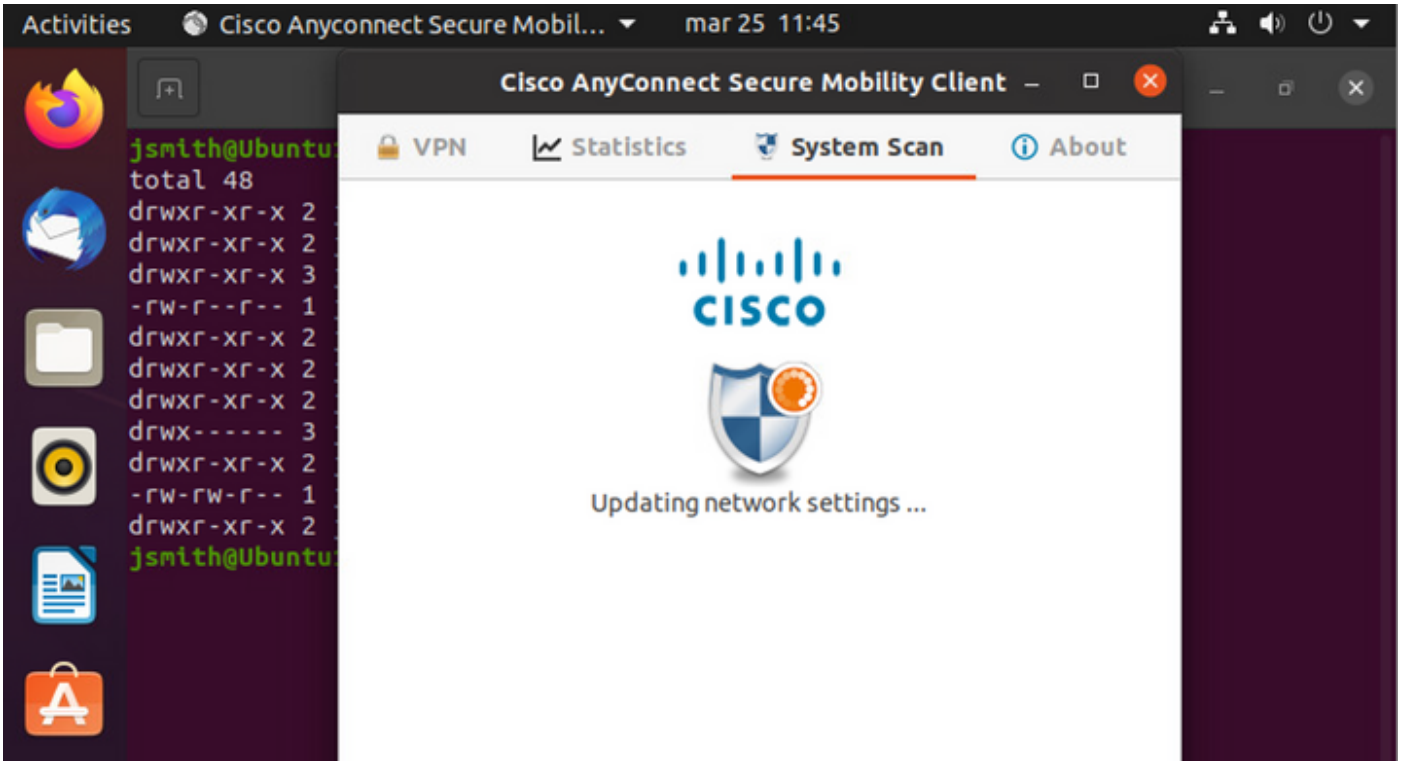
Aguarde alguns segundos enquanto o conector tenta detectar o AnyConnect:



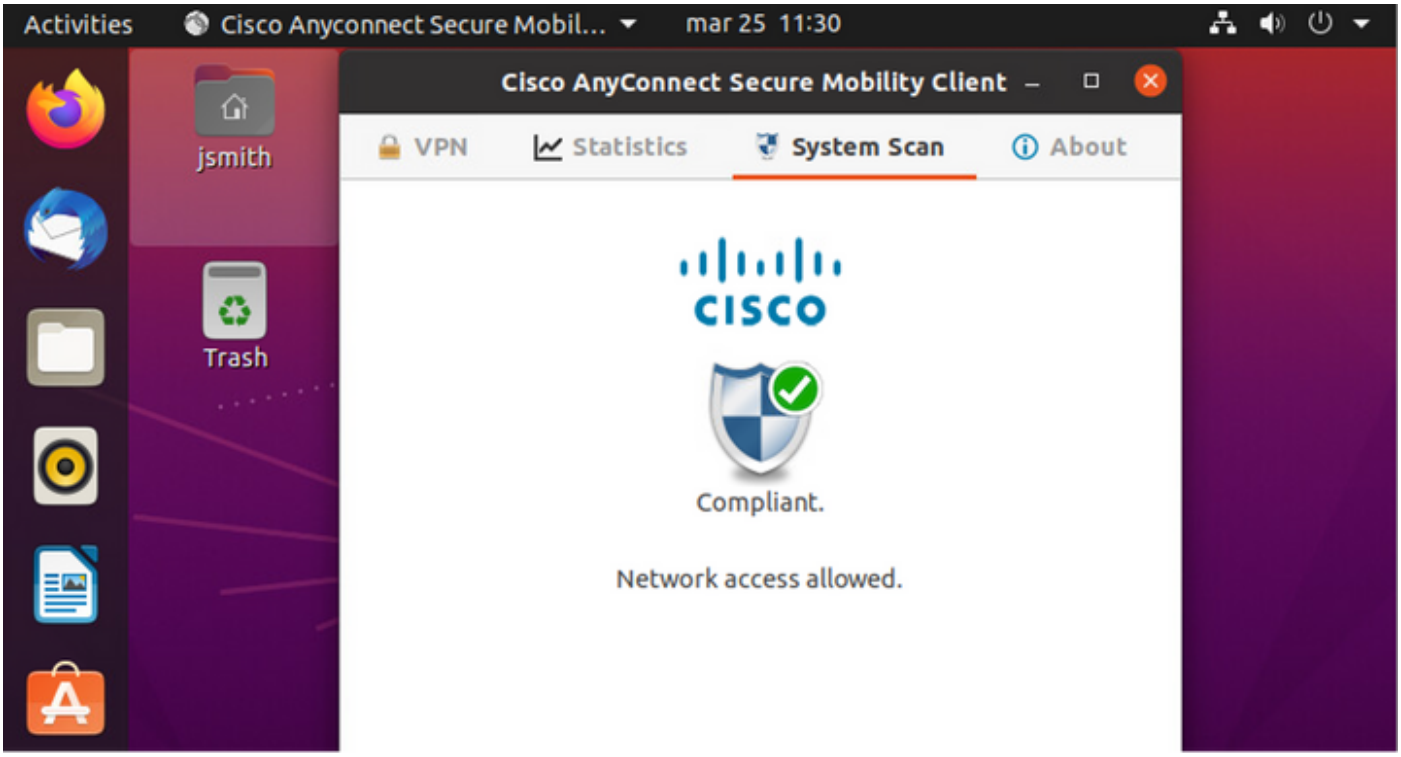
Devido a uma advertência conhecida, mesmo que o AnyConnect esteja instalado, ele não o detecta. Use **Alt-Tab** ou o menu **Atividades** para alternar para o cliente AnyConnect.

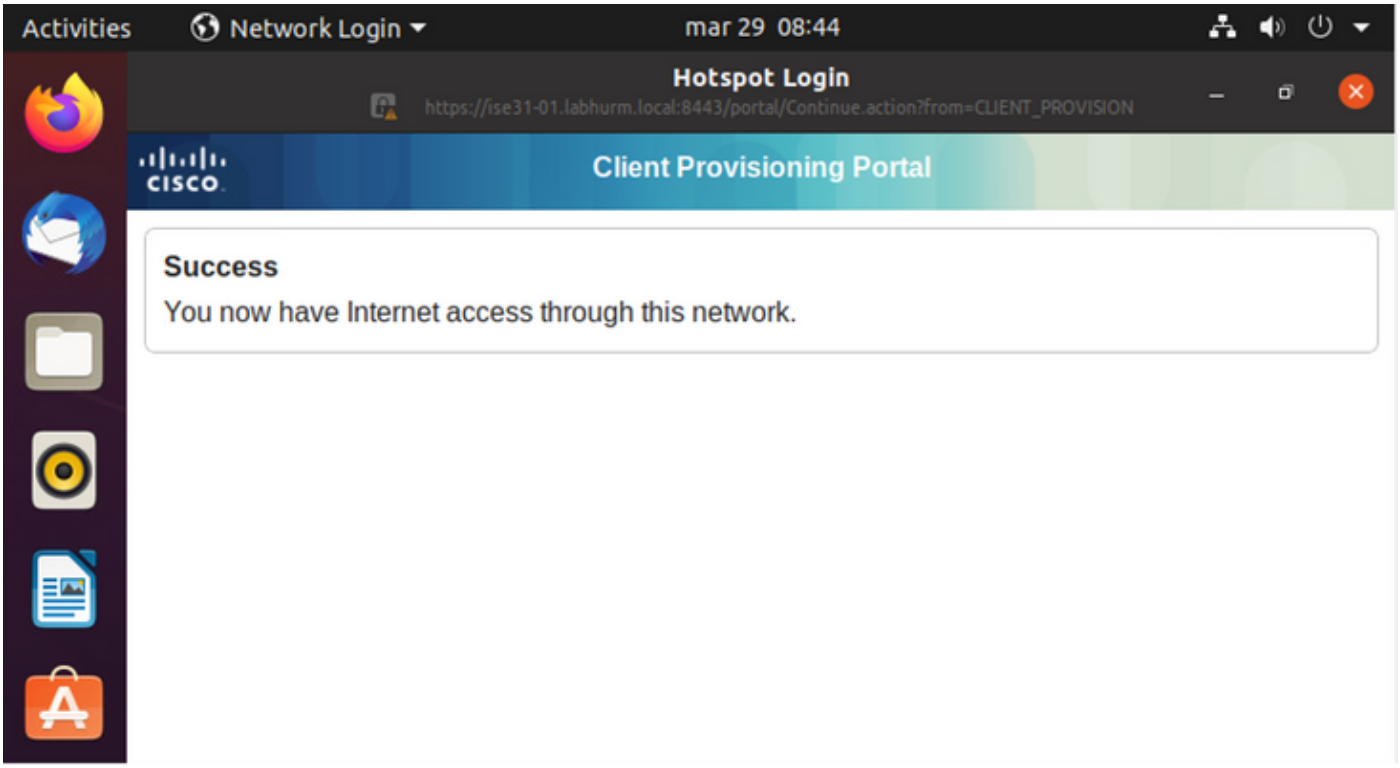


O AnyConnect tenta acessar a PSN para política de postura e avaliar o endpoint em relação a ela.



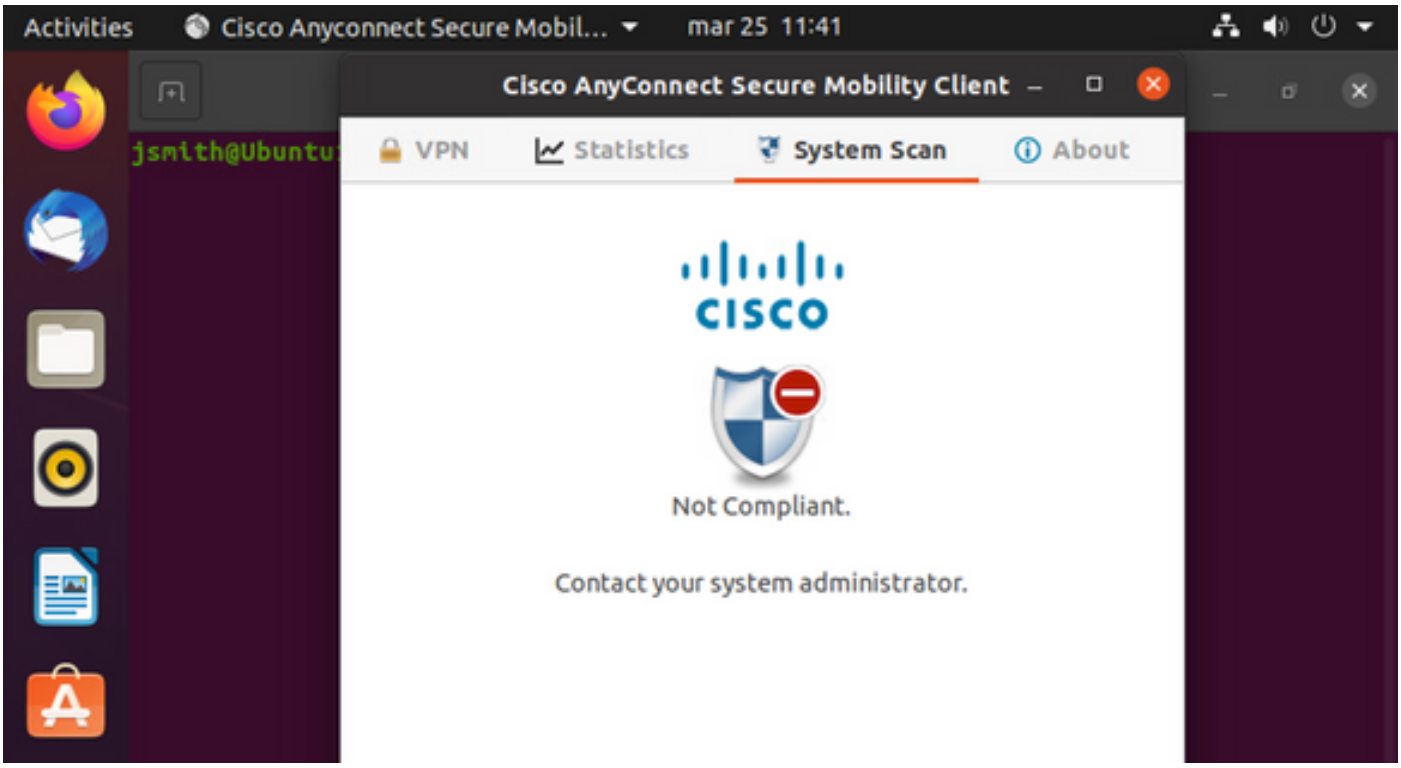
O AnyConnect reporta ao ISE sua determinação da política de postura. Neste caso, os

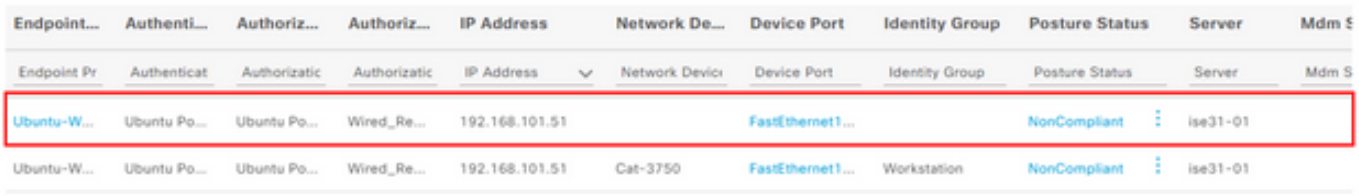




Endpoint Profile	Authenti...	Authorizati...	Authorization P...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server
Endpoint Profile	Authenticat	Authorization I	Authorization Profile	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server
Ubuntu-Workstation	Wired 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 Devici	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=C0A8C883000000010008044A&p
33062-b8d1-467b-b26f-8b022bba10e7&action=cpp&token=05a438ecb872ce396c2912fecfe0d2aa
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  C0A8C883000000010008044A
       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:  C0A8C883000000010008044A
       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:  C0A86E0100000000001724F
     Acct Session ID:  0x00000003
              Handle:  0x9A000000

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