

# Configurar e implantar o perfil NAM do cliente seguro por meio do ISE 3.3 no Windows

## Contents

---

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração](#)

[Diagrama de Rede](#)

[Fluxo de dados](#)

[Configurar o switch](#)

[Baixe o Pacote de Cliente Seguro](#)

[Configuração do ISE](#)

[Etapa 1. Carregar o pacote no ISE](#)

[Etapa 2. Criar um perfil NAM a partir da ferramenta Editor de perfis](#)

[Etapa 3. Carregar o perfil NAM no ISE](#)

[Etapa 4. Criar um perfil de postura](#)

[Etapa 5. Criar configuração do agente](#)

[Etapa 6. Política de Provisionamento de Cliente](#)

[Passo 7. Política de postura](#)

[Etapa 8. Adicionar dispositivo de rede](#)

[Etapa 9. Perfil de Autorização](#)

[Etapa 10. Protocolos permitidos](#)

[Etapa 11. Diretório ativo](#)

[Etapa 12. Conjuntos de políticas](#)

[Verificar](#)

[Etapa 1. Baixe e instale o módulo Secure Client Posture/NAM do ISE](#)

[Etapa 2. EAP-FAST](#)

[Etapa 3. Varredura de postura](#)

[Troubleshooting](#)

[Etapa 1. Perfil NAM](#)

[Etapa 2. Log Estendido do NAM](#)

[Etapa 3. Depurações no Switch](#)

[Etapa 4. Depurações no ISE](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como implantar o perfil do Cisco Secure Client Network Access Manager (NAM) através do Identity Services Engine (ISE).

## Informações de Apoio

A autenticação EAP-FAST ocorre em duas fases. Na primeira fase, o EAP-FAST emprega um handshake TLS para fornecer e autenticar trocas de chaves usando objetos Type-Length-Values (TLV) para estabelecer um túnel protegido. Esses objetos TLV são usados para transmitir dados relacionados à autenticação entre o cliente e o servidor. Uma vez estabelecido o túnel, a segunda fase começa com o cliente e o nó ISE iniciando outras conversas para estabelecer as políticas de autenticação e autorização necessárias.

O perfil de configuração NAM é configurado para usar EAP-FAST como o método de autenticação e está disponível para redes definidas administrativamente.

Além disso, os tipos de conexão de máquina e usuário podem ser configurados no perfil de configuração do NAM.

O dispositivo Windows corporativo obtém acesso corporativo completo usando o NAM com verificação de postura.

O dispositivo pessoal do Windows obtém acesso a uma rede restrita usando a mesma configuração NAM.

Este documento fornece instruções para implantar o perfil do Cisco Secure Client Network Access Manager (NAM) através do Portal de Postura do Identity Services Engine (ISE) usando a implantação da Web, juntamente com a Verificação de Conformidade de Postura.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity services engine (ISE)
- AnyConnect NAM e Editor de perfis
- Política de postura
- Configuração do Cisco Catalyst para serviços 802.1x

### Componentes Utilizados

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

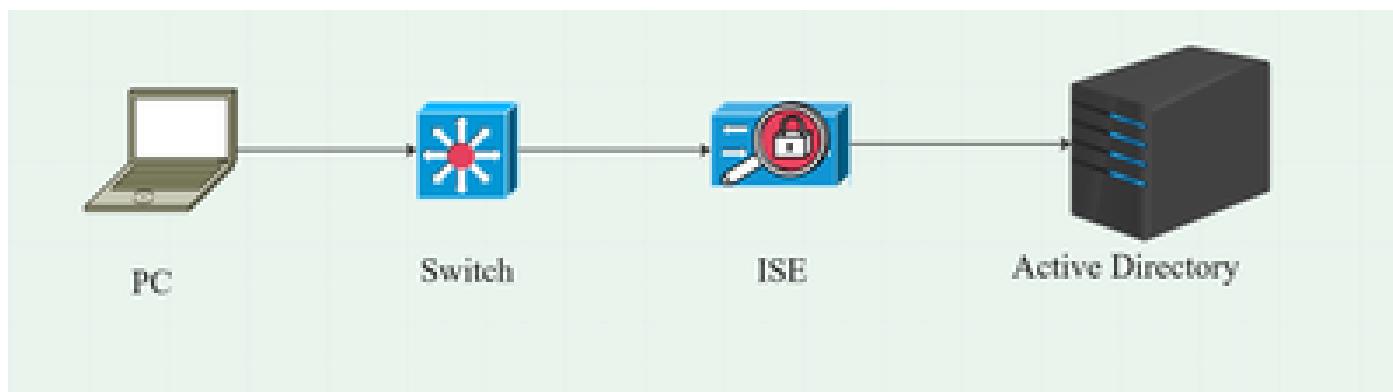
- Cisco ISE, versão 3.3 e posterior
- Windows 10 com Cisco Secure Mobility Client 5.1.4.74 e posterior
- Switch Cisco Catalyst 9200 com software Cisco IOS® XE 17.6.5 e posterior
- Ative Directory 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configuração

### Diagrama de Rede



### Fluxo de dados

Quando um PC se conecta à rede, o ISE fornece a política de autorização para redirecionamento ao Portal de postura.

O tráfego http no PC é redirecionado para a página de provisionamento do cliente ISE, onde o aplicativo NSA é baixado do ISE.

Em seguida, o NSA instala os módulos do agente do Secure Client no PC.

Após a conclusão da instalação do agente, o agente faz o download do perfil de postura e do perfil NAM configurados no ISE.

A instalação do módulo NAM aciona uma reinicialização no PC.

Após a reinicialização, o módulo NAM executa a autenticação EAP-FAST com base no perfil NAM.

A verificação de postura é acionada e a conformidade é verificada com base na política de postura do ISE.

### Configurar o switch

Configure o switch de acesso para autenticação e redirecionamento dot1x.

```
aaa new-model  
  
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting dot1x default start-stop group radius  
aaa server radius dynamic-author  
cliente 10.127.197.53 chave-servidor Qwerty123  
auth-type any
```

```
aaa session-id common
ip radius source-interface Vlan1000
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
RAD1 de servidor radius
address ipv4 <IP do servidor ISE> auth-port 1812 acct-port 1813
key <secret-key>

dot1x system-auth-control
```

Configure a ACL de redirecionamento para o usuário a ser redirecionado para o Portal de provisionamento do cliente ISE.

```
ip access-list extended redirect-acl
10 deny udp any any eq domain
20 deny tcp any any eq domain
30 deny udp any eq bootpc any eq bootps
40 deny ip any host <IP do servidor ISE>
50 permit tcp any any eq www
60 permit tcp any any eq 443
```

Habilite o rastreamento de dispositivo e o redirecionamento http no switch.

```
device-tracking policy <device tracking policy name>
tracking enable
interface <interface name>
device-tracking attach-policy <device tracking policy name>

ip http server
ip http secure-server
```

## Baixe o Pacote de Cliente Seguro

Baixe manualmente os arquivos do Editor de perfis, das janelas de Cliente seguro e do módulo de conformidade do [software.cisco.com](https://software.cisco.com).

Na barra de pesquisa do nome do produto, digite Secure Client 5.

Downloads Home > Segurança > Segurança de endpoint > Cliente seguro (incluindo AnyConnect) > Cliente seguro 5 > Software AnyConnect VPN Client

- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

## Configuração do ISE

### Etapa 1. Carregar o pacote no ISE

Para carregar os pacotes de implantação da Web do Secure Client and Compliance Module no ISE, navegue até Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk.

The screenshot shows the 'Agent Resources From Local Disk' configuration page in the ISE Workcenter. The 'Category' dropdown is set to 'Cisco Provided Packages'. A file named 'cisco-secure-...deploy-k9.pkg' is selected for upload. Below the upload section, there is a table of 'Agent Uploaded Resources' with the following data:

Name	Type	Version	Description
CiscoSecureClientDesktopWindows 5.1...	CiscoSecureClientDesktopWindows	5.1.4.74	Cisco Secure Client for ...

A 'Submit' button is highlighted at the bottom of the page.

The screenshot shows the 'Resources' page in the ISE Workcenter. The table lists various resources with the following data:

Name	Type	Version	Last Update	Description
Lab Profile	AgentProfile	Not Applicable	2024/07/26 17:23:41	
Agent Configuration	AgentConfig	Not Applicable	2024/07/26 16:00:49	
NAM Profile	AgentProfile	Not Applicable	2024/07/26 16:00:00	
CiscoSecureClientComplianceModuleWindows 4.3.4164.8192	CiscoSecureClientCo...	4.3.4164.8192	2024/07/26 15:58:44	Cisco Secure Client Win...
CiscoSecureClientDesktopWindows 5.1.4.074	CiscoSecureClientDe...	5.1.4.74	2024/07/26 15:56:27	Cisco Secure Client for ...
Cisco-ISE-NSP	Native Supplicant Pro...	Not Applicable	2023/07/04 05:25:16	Pre-configured Native S...
CiscoAgentlessOSX 5.0.03061	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 04:24:14	With CM: 4.3.3045.6400

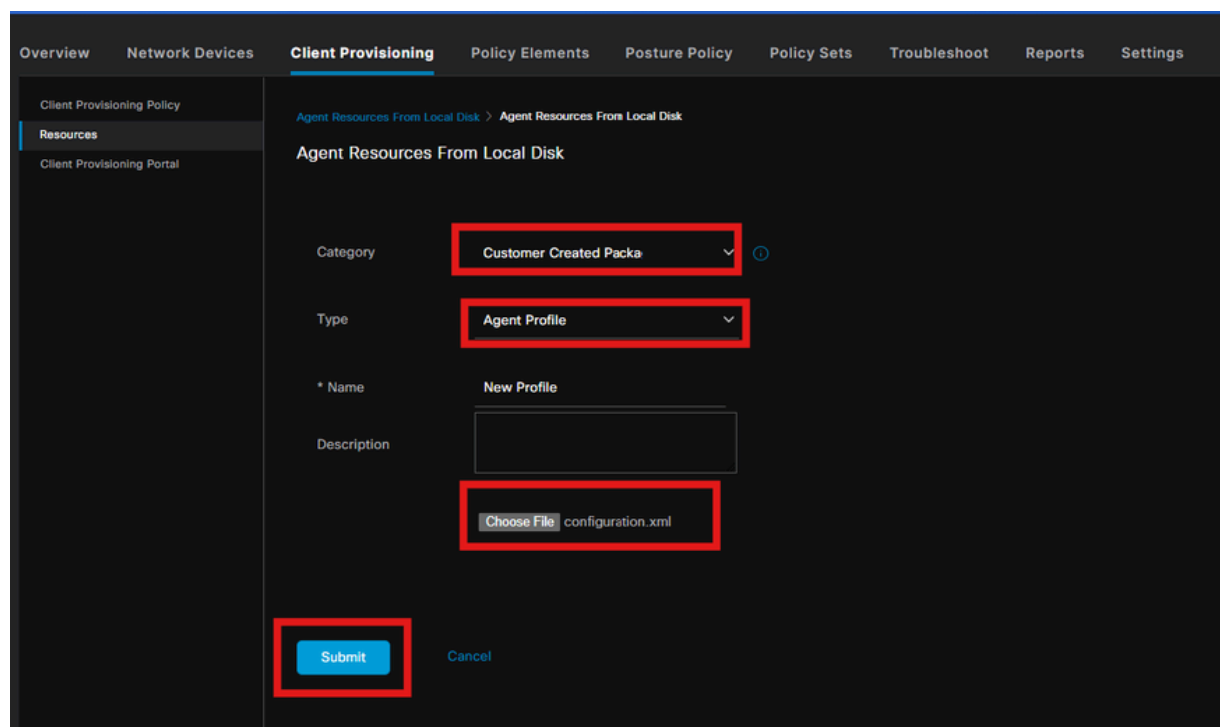
The rows for 'CiscoSecureClientComplianceModuleWindows 4.3.4164.8192' and 'CiscoSecureClientDesktopWindows 5.1.4.074' are highlighted with a red box.

### Etapa 2. Criar um perfil NAM a partir da ferramenta Editor de perfis

Para obter informações sobre como configurar um perfil NAM, consulte este guia [Configure Secure Client NAM Profile](#) .

### Etapa 3. Carregar o perfil NAM no ISE

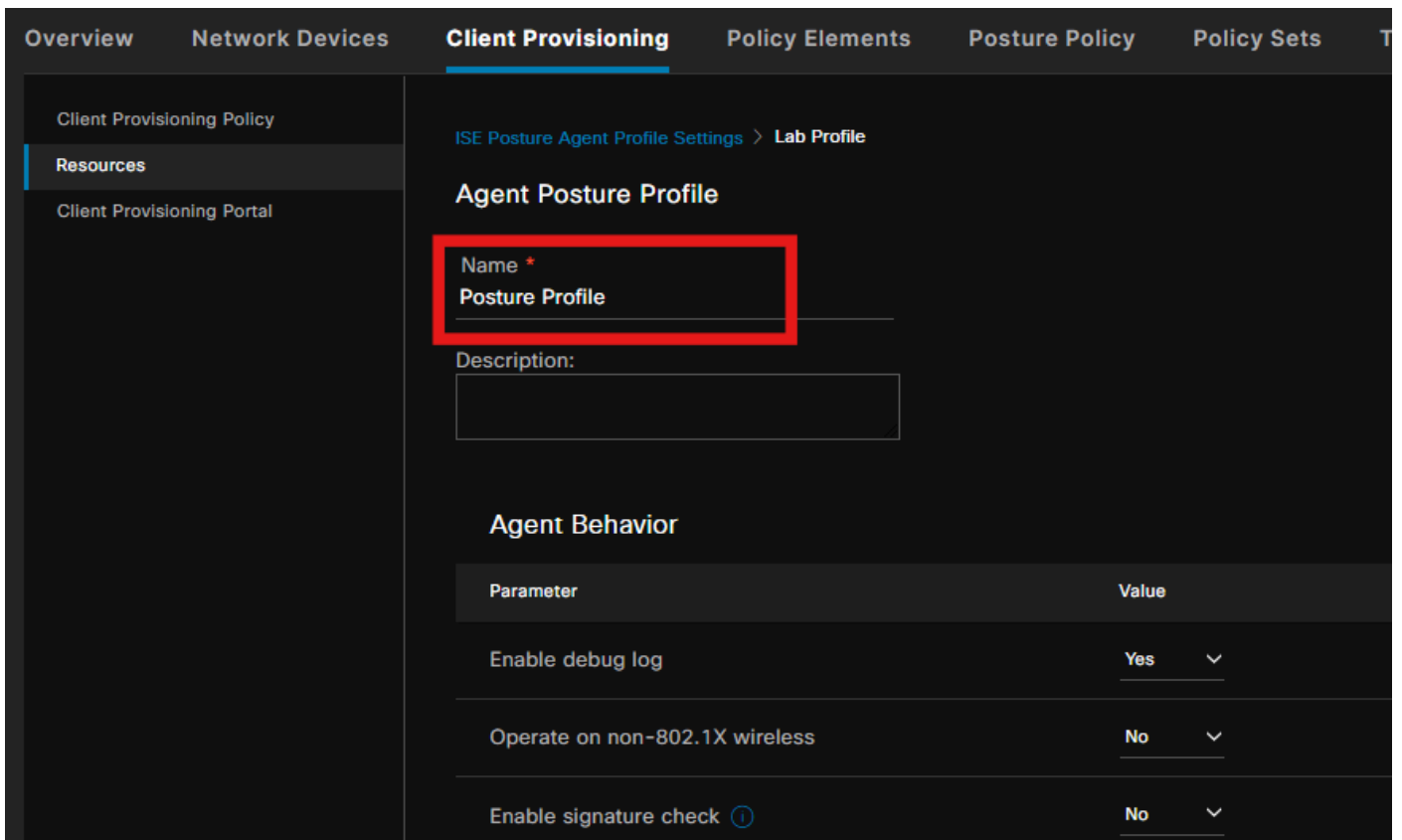
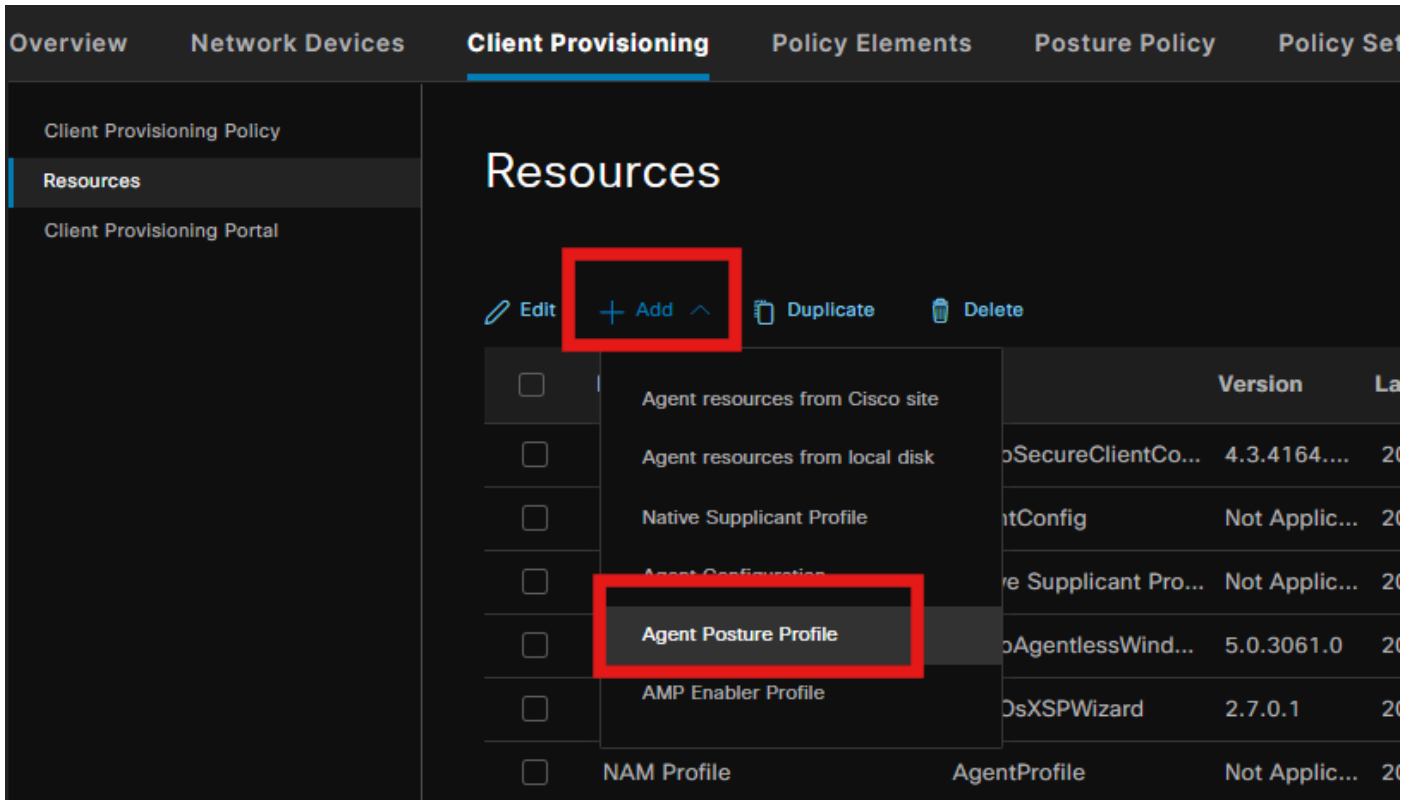
Para carregar o perfil NAM "Configuration.xml" no ISE como Perfil do agente, navegue para Provisionamento de cliente > Recursos > Recursos do agente do disco local.



The screenshot displays the Cisco ISE Client Provisioning interface. The breadcrumb navigation shows 'Agent Resources From Local Disk > Agent Resources From Local Disk'. The main heading is 'Agent Resources From Local Disk'. The form fields are as follows:

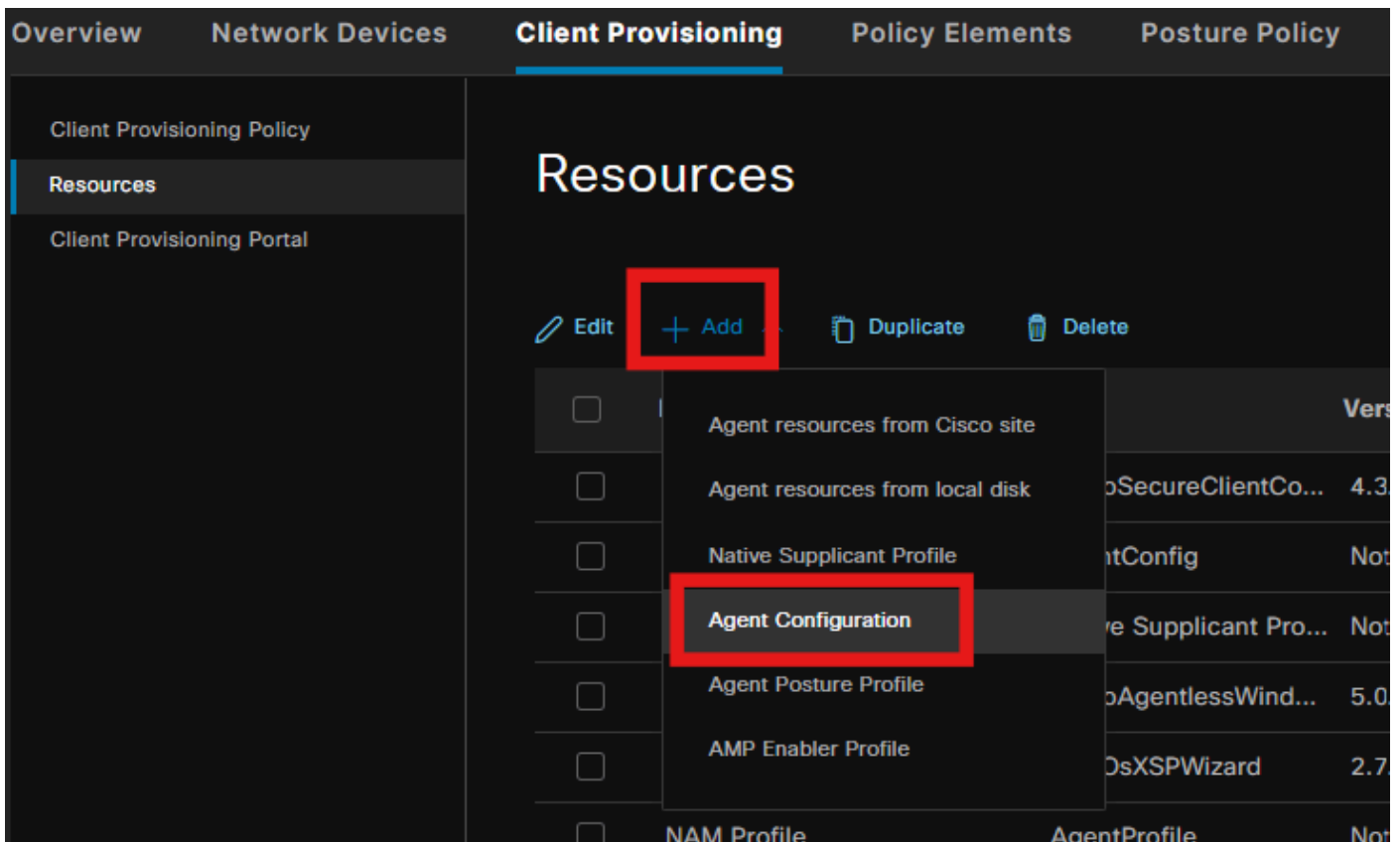
- Category:** Customer Created Packs (dropdown menu)
- Type:** Agent Profile (dropdown menu)
- \* Name:** New Profile (text input)
- Description:** (empty text input)
- File Selection:** Choose File configuration.xml (file upload button)
- Buttons:** Submit (highlighted in red), Cancel

### Etapa 4. Criar um perfil de postura



Na seção Protocolo de postura, não se esqueça de adicionar \* para permitir que o Agente se conecte a todos os servidores.

Etapa 5. Criar configuração do agente



Selecione o cliente seguro carregado e o pacote do módulo de conformidade e, na seleção Module (Módulo), selecione os módulos ISE Posture, NAM e DART



Engine Work Centers / Posture

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

Client Provisioning Policy  
Resources  
Client Provisioning Portal

Agent Configuration > New Agent Configuration

\* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 ▾

\* Configuration Name: Agent Configuration

Description:

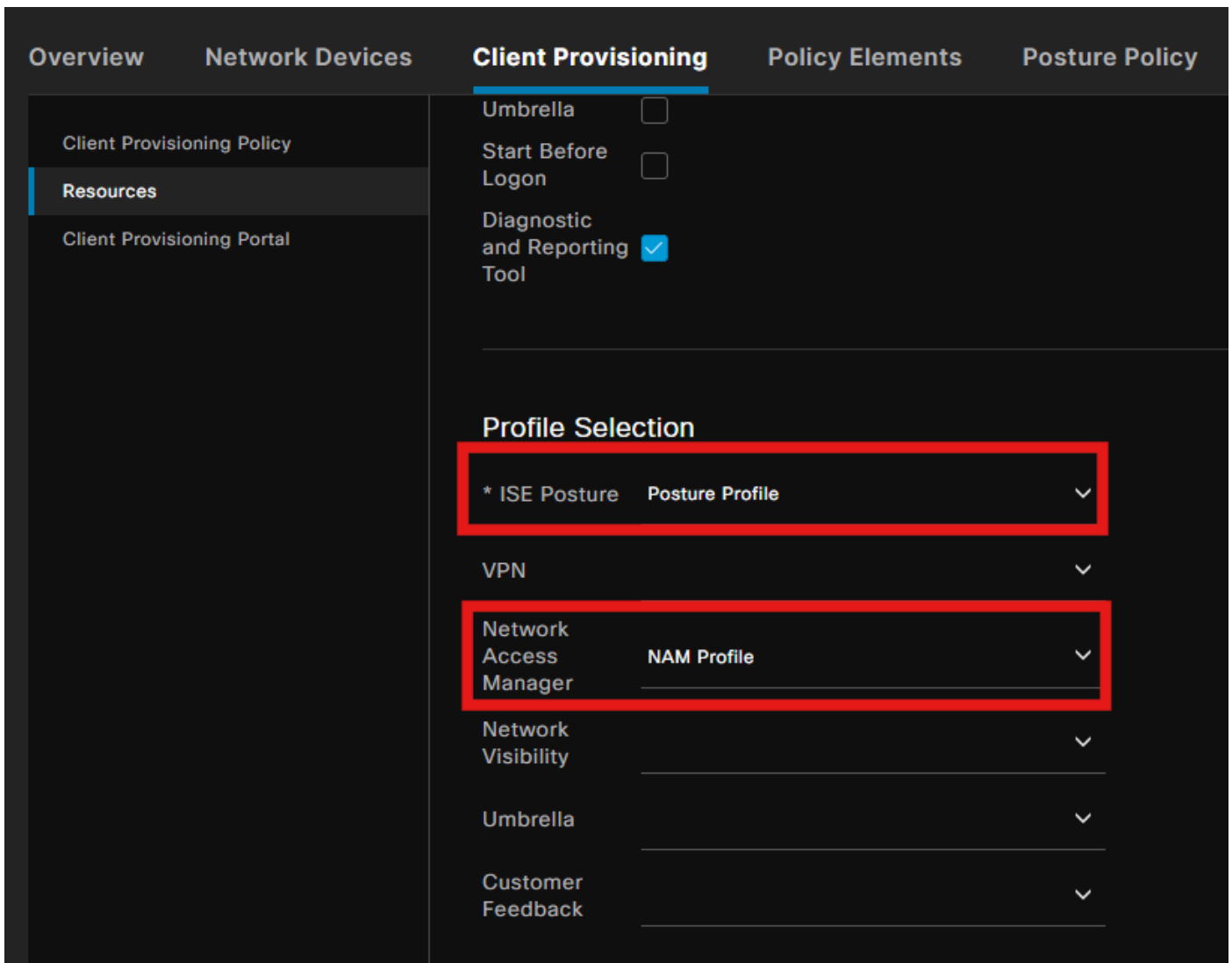
Description Value Notes

\* Compliance Module CiscoSecureClientComplianceModuleW ▾

Cisco Secure Client Module Selection

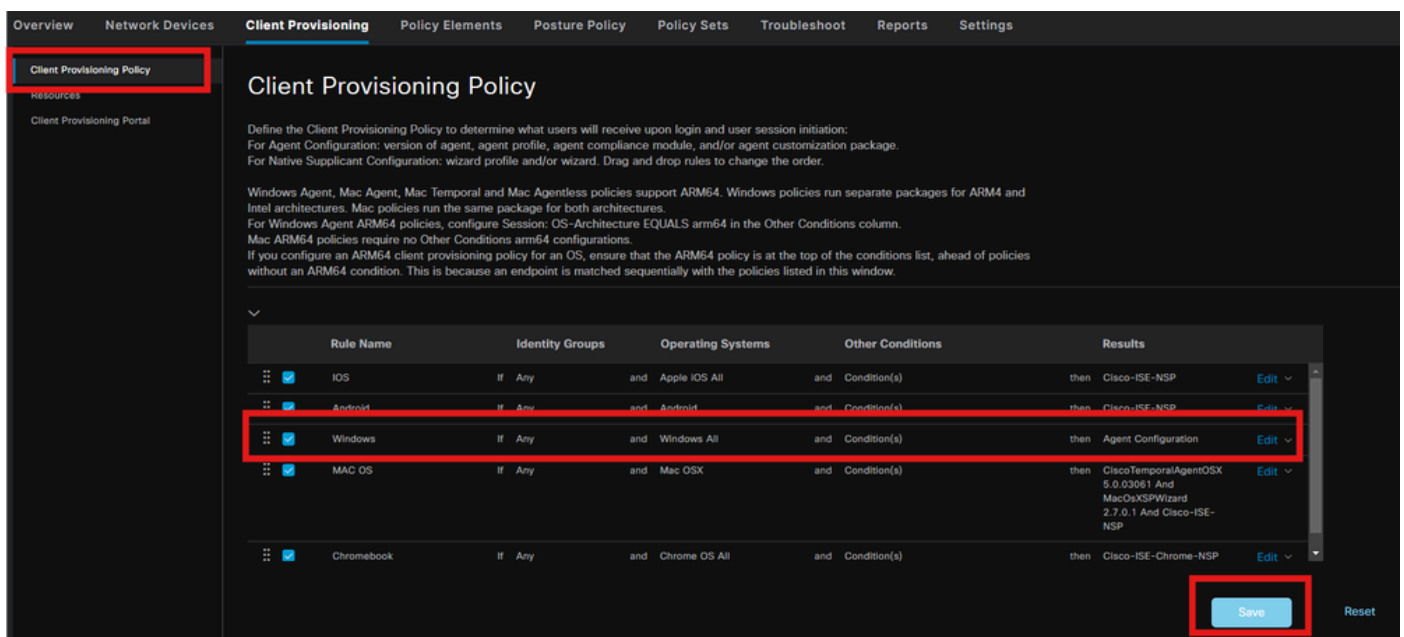
ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input checked="" type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>

Em Profile select (Seleção de perfil), escolha o perfil Posture e NAM e clique em Submit.



## Etapa 6. Política de Provisionamento de Cliente

Crie uma Política de Provisionamento do cliente para o sistema operacional Windows e selecione a Configuração do Agente criada na etapa anterior.

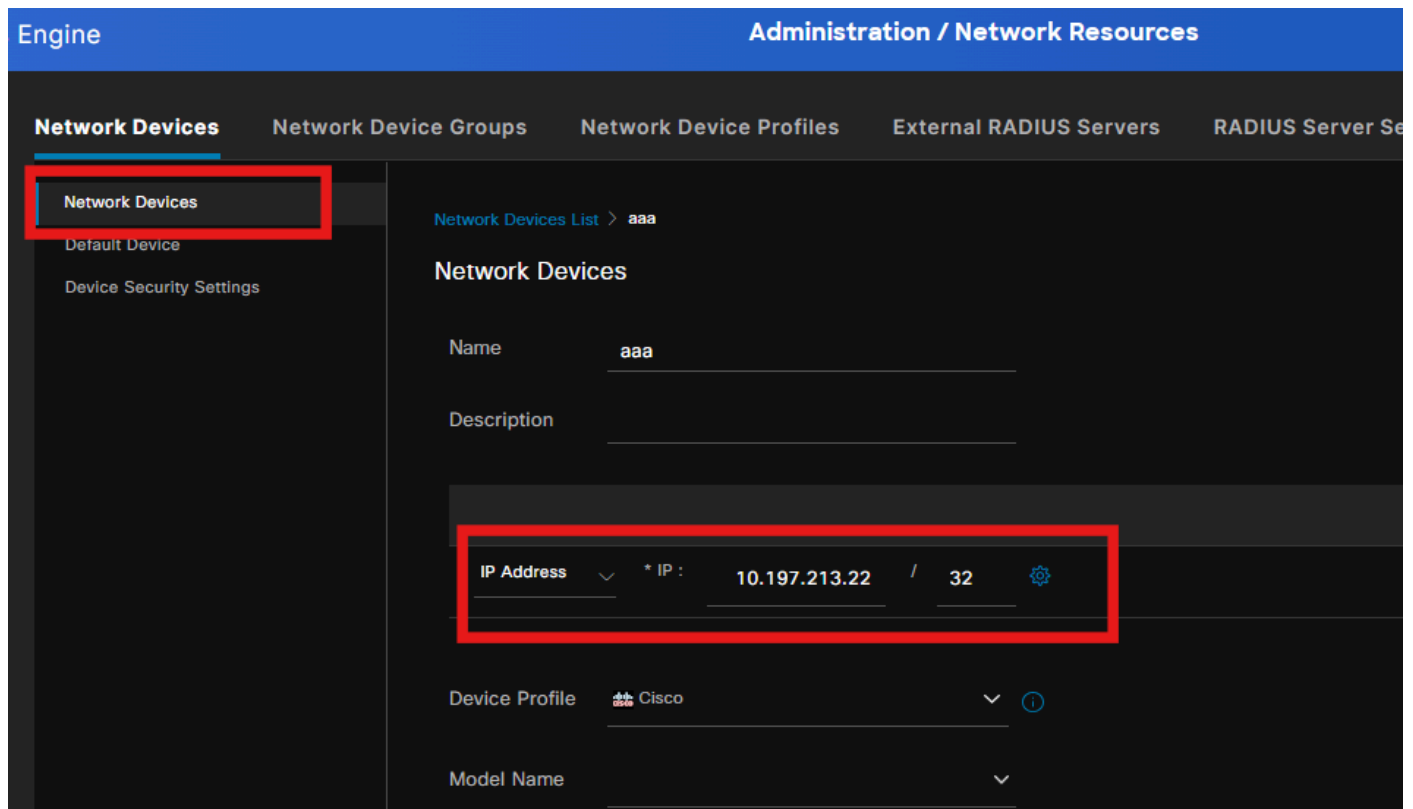


## Passo 7. Política de postura

Para obter informações sobre como criar as condições e a política de postura, consulte este guia [Guia de implantação prescritiva de postura do ISE](#).

## Etapa 8. Adicionar dispositivo de rede

Para adicionar o endereço IP do switch e a chave secreta compartilhada radius, navegue para Administração > Recursos de rede.



The screenshot displays the Cisco ISE Administration console interface. The top navigation bar shows "Engine" and "Administration / Network Resources". The main navigation menu includes "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", and "RADIUS Server Se". The "Network Devices" menu item is highlighted with a red box. The main content area shows the configuration for a Network Device named "aaa". The "IP Address" field is highlighted with a red box and contains the value "10.197.213.22 / 32". Other fields include "Name" (aaa), "Description", "Device Profile" (Cisco), and "Model Name".

Engine Administration / Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Se

Network Devices List > aaa

Network Devices

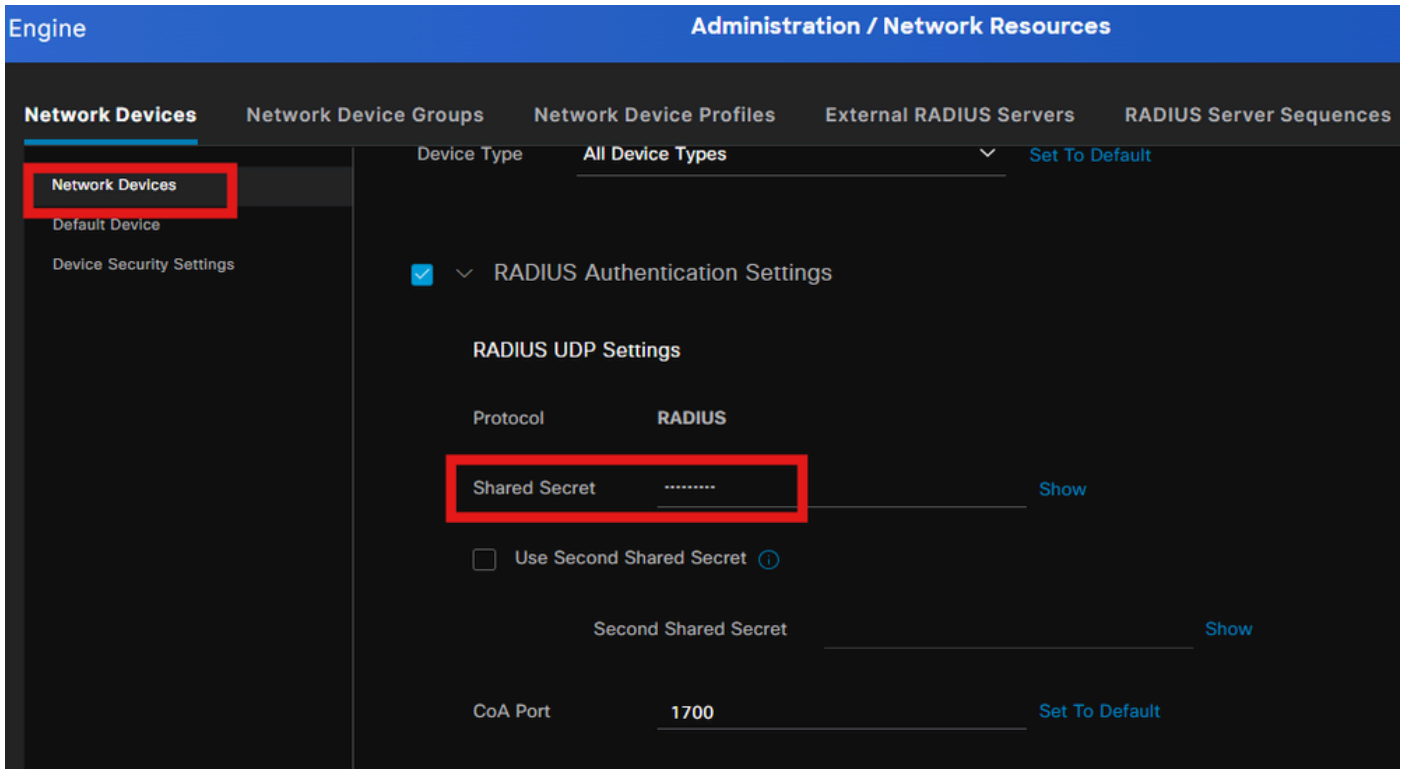
Name aaa

Description

IP Address \* IP : 10.197.213.22 / 32

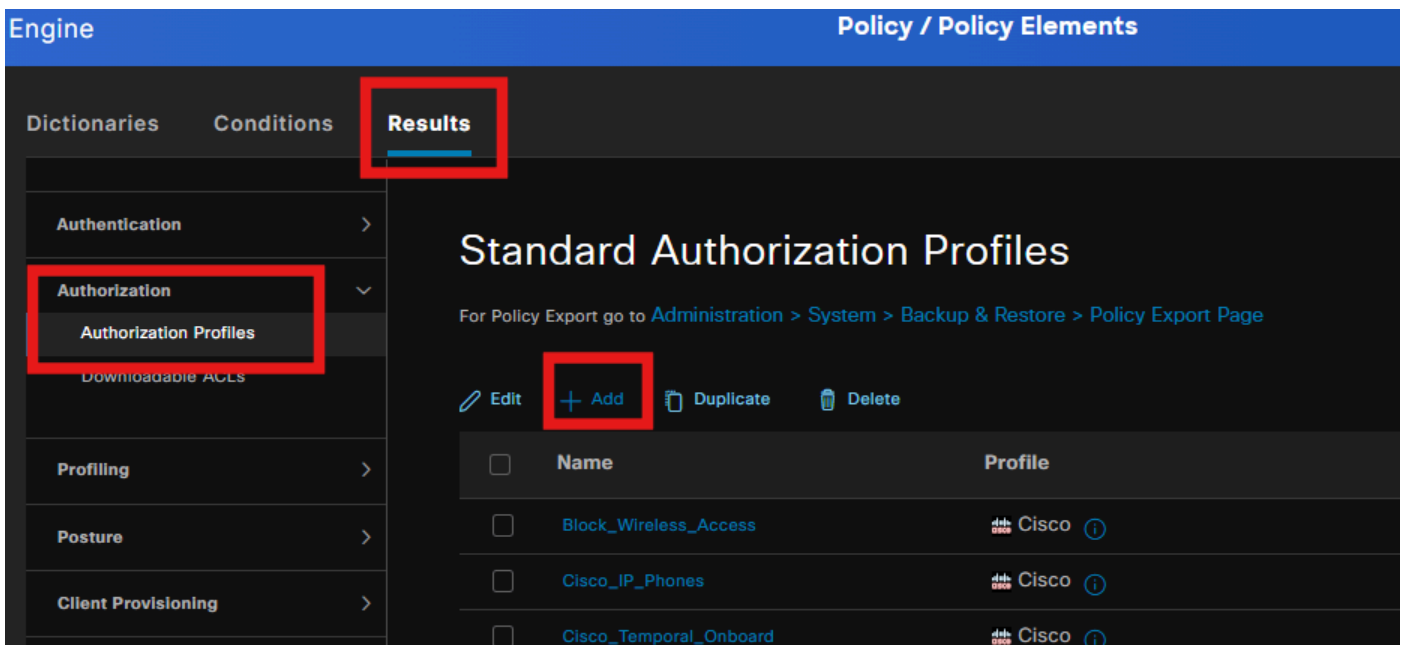
Device Profile Cisco

Model Name

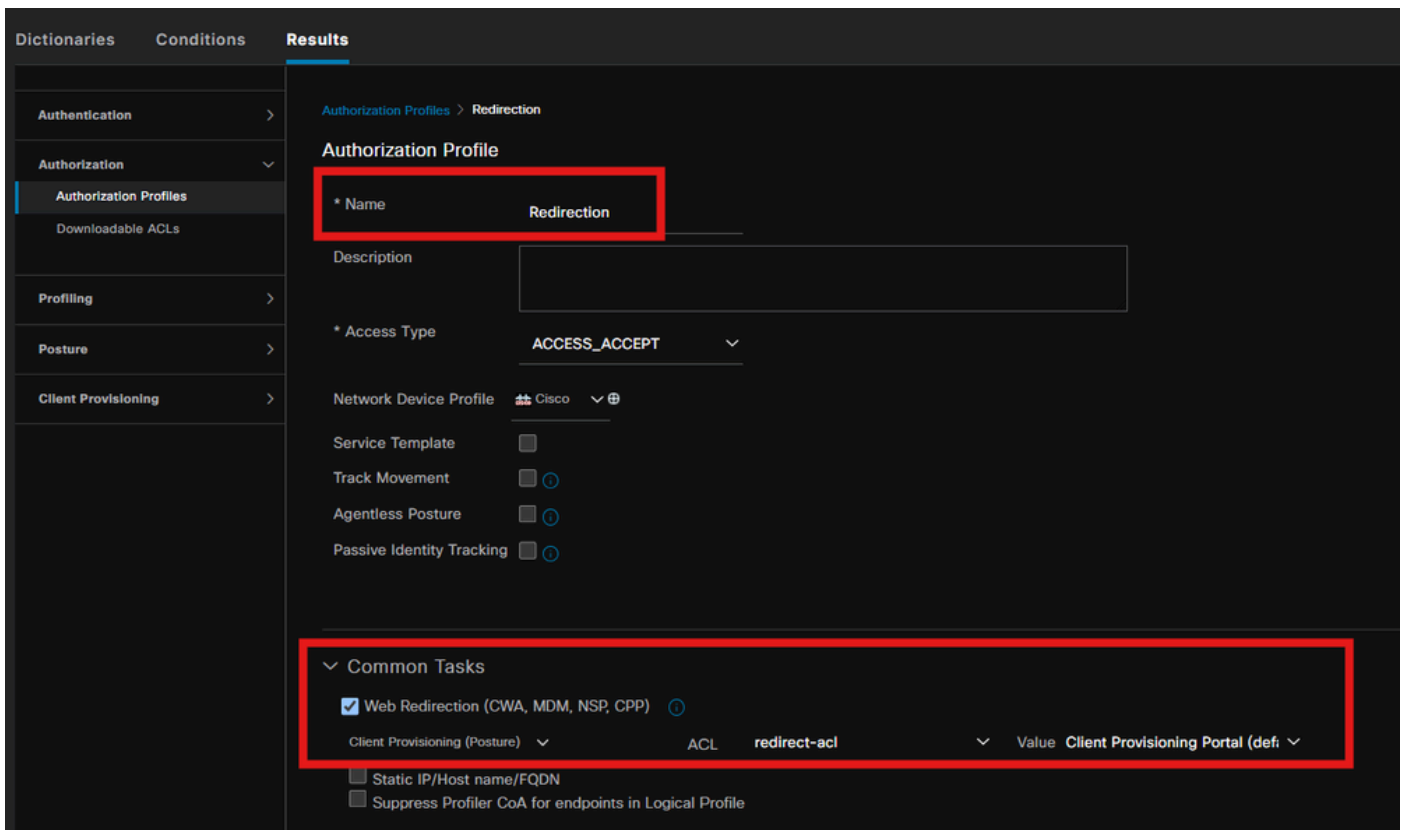


## Etapa 9. Perfil de Autorização

Para criar um perfil de redirecionamento de postura, navegue para Política > Elementos de política > Resultados.

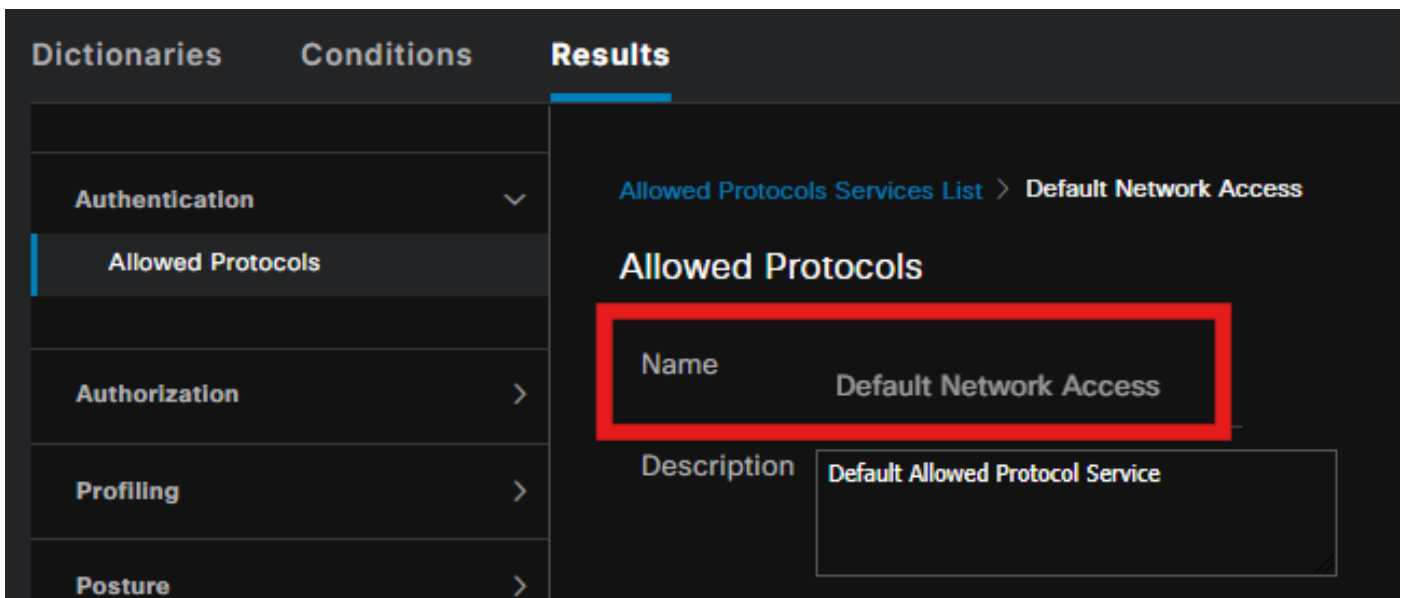


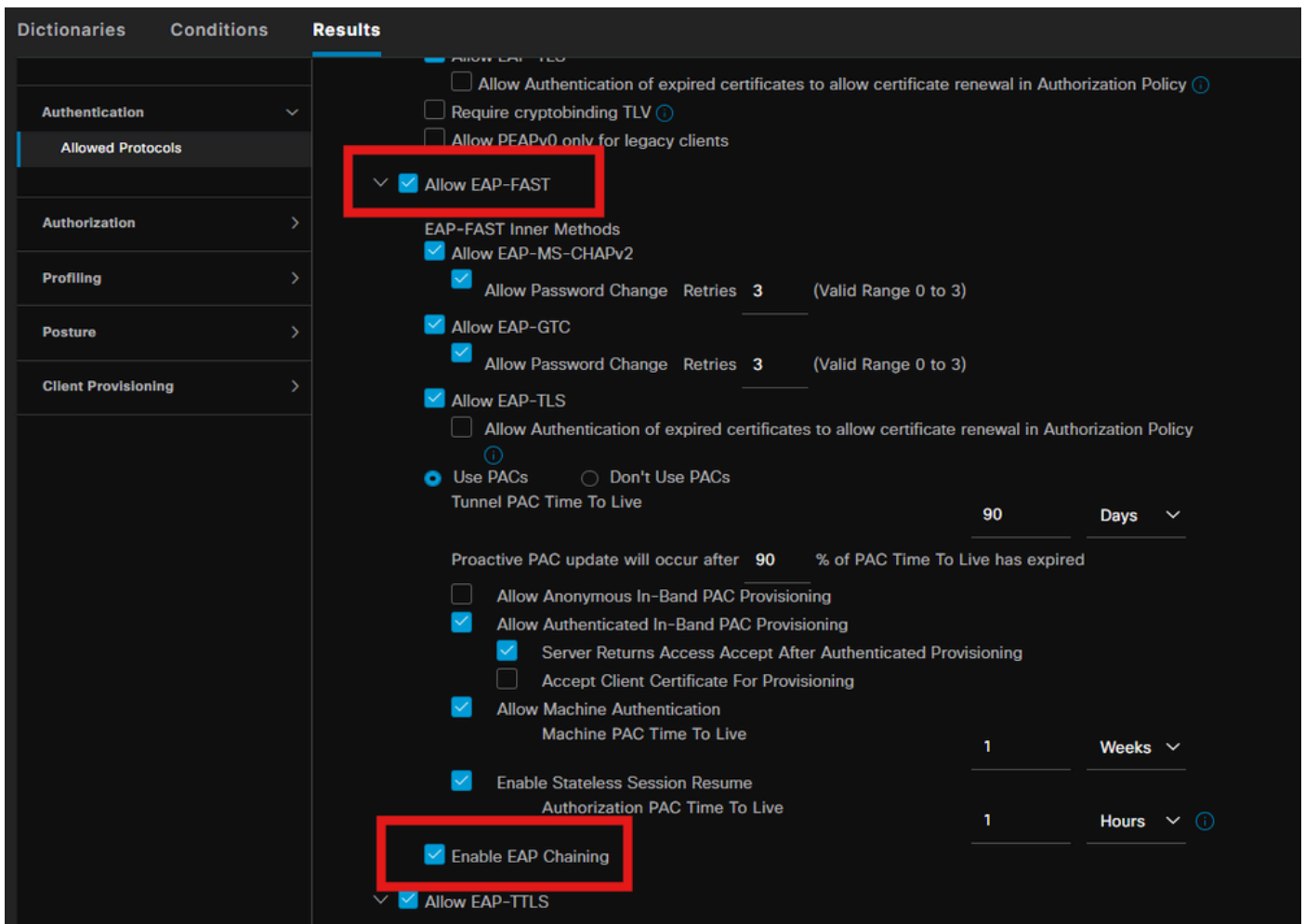
Na tarefa de comando, selecione o Portal de provisionamento do cliente com ACL de redirecionamento.



## Etapa 10. Protocolos permitidos

Navegue até Policy > Policy elements > Results > Authentication > Allowed Protocols, selecione as configurações de EAP Chaining,

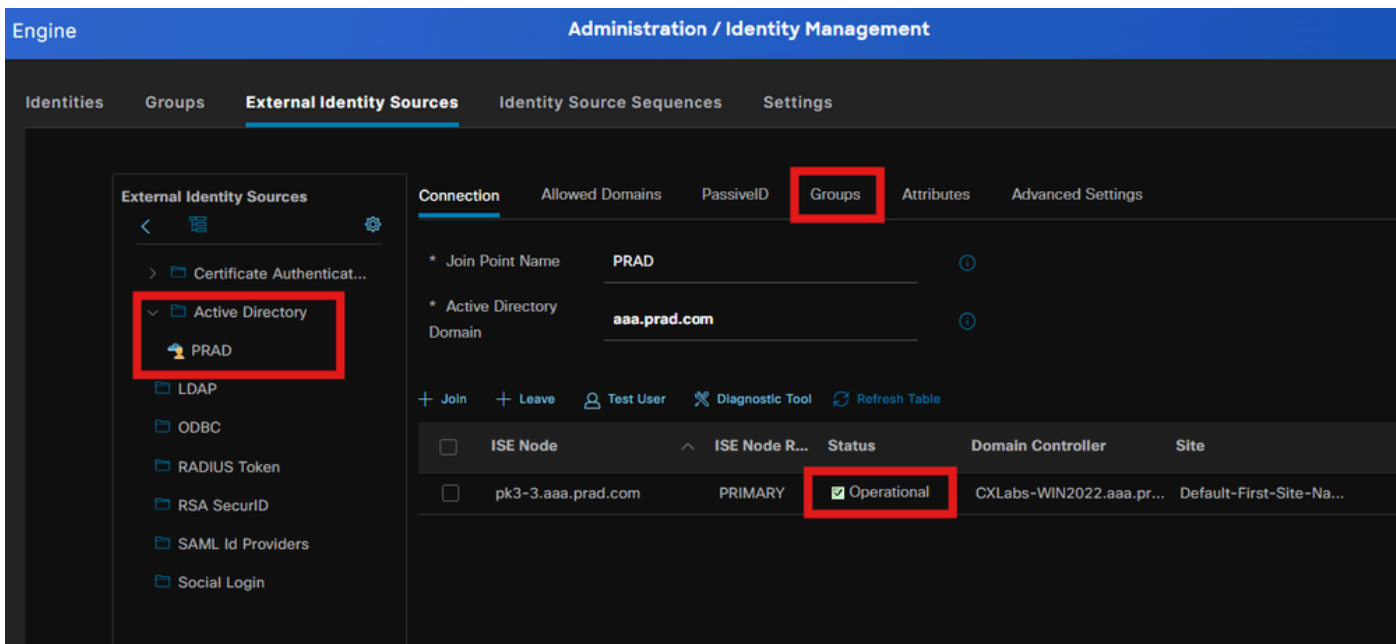




## Etapa 11. Diretório ativo

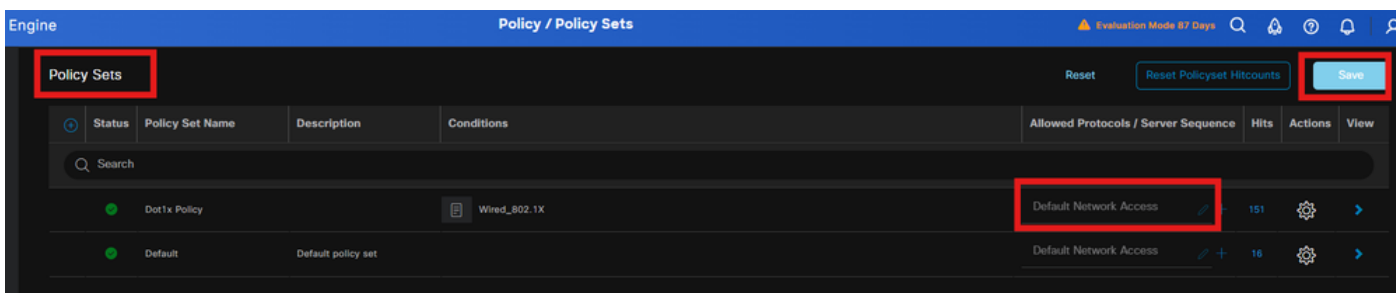
Validar se o ISE está associado ao domínio do Ative Diretorio e os grupos de domínio são selecionados, se necessário, para as condições de autorização.

Administração > Gerenciamento de Identidades > Origens de Identidades Externas > Ative Diretory

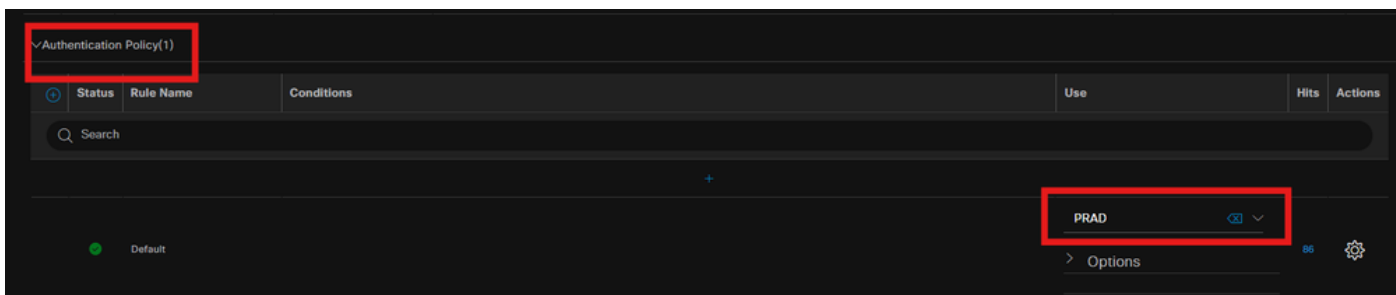


## Etapa 12. Conjuntos de políticas

Crie um conjunto de políticas no ISE para autenticar a solicitação dot1x. Navegue até Política > Conjuntos de política.



Selecione o Active Directory como origem de identidade para a Política de autenticação.



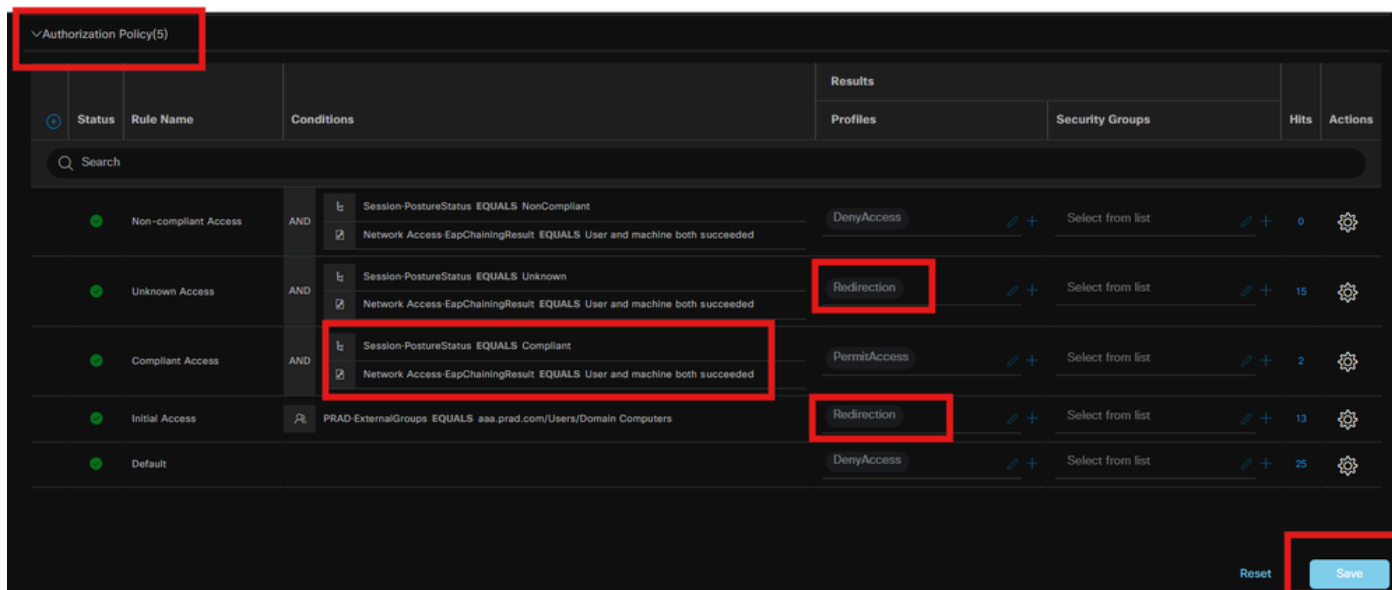
Configure diferentes regras de Autorização com base no status de postura desconhecido, não compatível e compatível.

Neste caso de uso.

- Acesso inicial : redirecionamento para o Portal de provisionamento do cliente ISE para instalar o agente de cliente seguro e o Perfil NAM
- Acesso desconhecido: acesso ao Portal de provisionamento do cliente para descoberta de

postura baseada em redirecionamento

- Acesso em conformidade: acesso total à rede
- Não compatível: negar acesso



## Verificar

Etapa 1. Baixe e instale o módulo Secure Client Posture/NAM do ISE

Selecione o endpoint autenticado por dot1x, pressionando a regra de autorização "Acesso inicial".  
Navegue até Operations > Radius > Live Logs

Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:09:31...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

No Switch, especifique a URL de redirecionamento e a ACL que está sendo aplicada ao Ponto de Extremidade.

```
Switch#show authentication session interface te1/0/24 details
```

```
Interface: TenGigabitEthernet1/0/24
```

```
IIF-ID: 0x19262768
```

```
Endereço MAC: x4x6.xxxx.xxxx
```

```
Endereço IPv6: desconhecido
```

```
Endereço IPv4: <client-IP>
```

```
Nome de usuário: host/DESKTOP-xxxxxx.aaa.prad.com
```

```
Status: Autorizado
```

```
Domínio: DADOS
```

```
Modo de host operacional: host único
```



Diretório de controle operacional: ambos  
Tempo limite da sessão: N/D  
ID de sessão comum: 16D5C50A0000002CF067366B  
ID da Sessão da Conta: 0x0000001f  
Identificador: 0x7a000017  
Política atual: POLICY\_Te1/0/24

Diretivas Locais:  
Modelo de serviço: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (prioridade 150)  
Política de segurança: deve proteger  
Status de Segurança: Link Não Protegido

Políticas de servidor:  
ACL de redirecionamento de URL: redirect-acl  
Redirecionamento de URL:  
<https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee397180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2>  
ACL ACS: xACSACLx-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

Lista de status do método:  
Estado do Método  
Êxito de Autenticação dot1x

Switch#sh device-tracking database interface te1/0/24

Endereço da Camada de Rede Endereço da Camada de Link Interface vlan prlv age state Tempo restan  
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn ALCANÇÁVEL 39 s try 0

No Endpoint, verifique o tráfego redirecionado para a Postura ISE e clique em Iniciar para fazer o download do Network Setup Assistant no Endpoint.

Google Chrome isn't your default browser

Set as default



Client Provisioning Portal

#### Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start

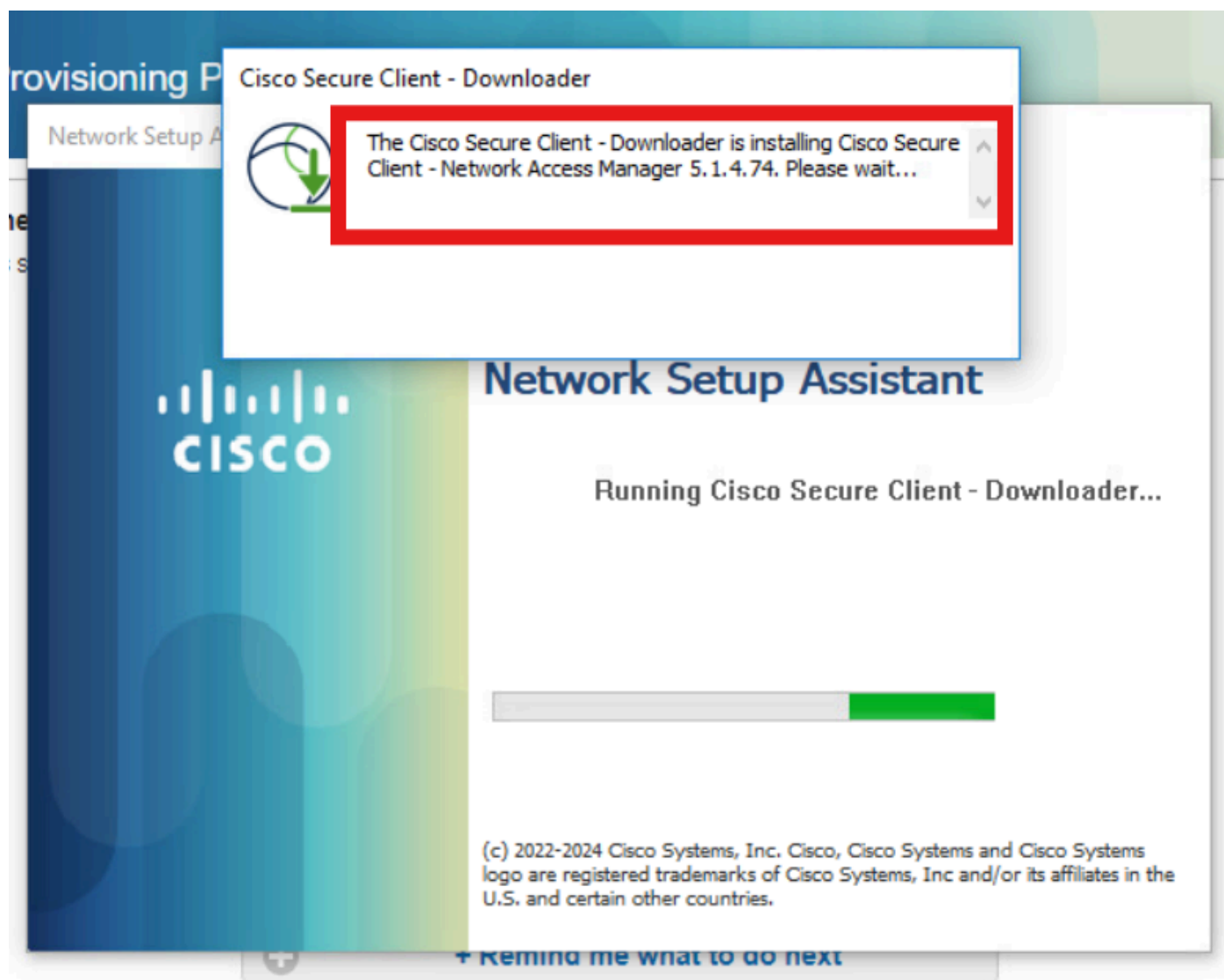
The screenshot shows the Cisco Client Provisioning Portal interface. At the top left, the logo 'isco' and the text 'Client Provisioning Portal' are visible. Below this, a 'Device Security Check' section states: 'Your computer requires security software to be installed before you can connect to the network.' A notification box titled 'Unable to detect Posture Agent' is displayed, containing the text: '+ This is my first time here', followed by instructions: '1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)', '2. After installation, Agent will automatically scan your device before allowing you access to the network.', and '3. You have 4 minutes to install and for the system scan to complete.' A tip follows: 'Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.' A progress indicator shows 'You have 4 minutes to install and for the compliance check to complete'. At the bottom of the notification is a '+ Remind me what to do next' button. In the top right corner, a 'Recent download history' window is open, showing a single entry: 'cisco-secure-client-ise-network-assistant-win-5.1.4.74\_pk3-3.aaa.prad.com\_8443\_WPTsDtDOR0SunsnMYB1glg.exe' with a size of '3.0 MB' and status 'Done'. A 'Full download history' link is also present.

Clique em Executar para instalar o aplicativo NSA.

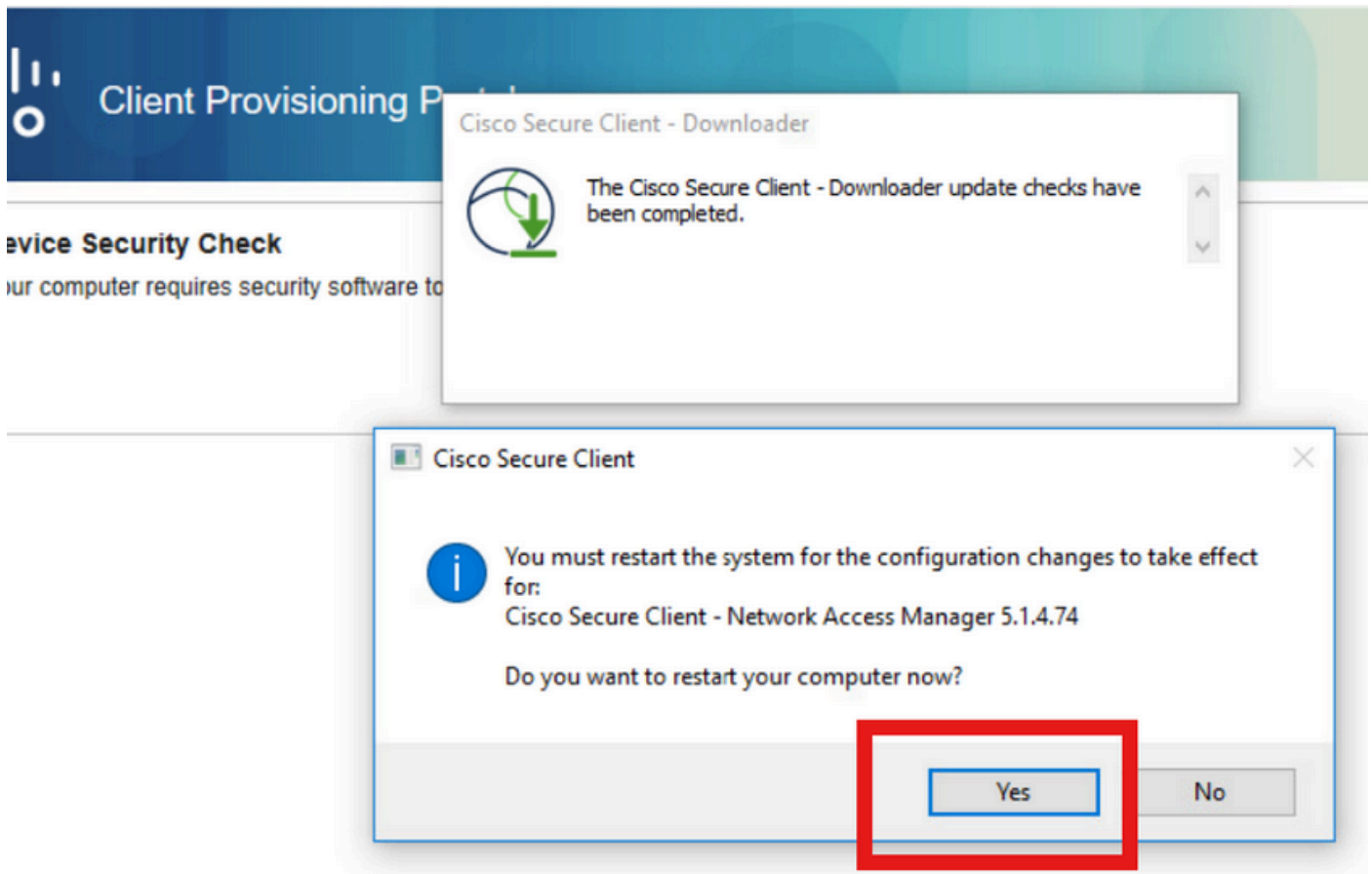
The screenshot shows a Windows SmartScreen warning dialog box overlaid on the Cisco Client Provisioning Portal. The dialog box has a blue background and white text. The title is 'SmartScreen can't be reached right now'. The main text reads: 'Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.' Below this, it lists the publisher as 'Cisco Systems, Inc.' and the app name as 'cisco-secure-client-ise-network-assistant-win-5.1.4.74\_pk3-...'. At the bottom right, there are two buttons: 'Run' and 'Don't Run'. The 'Run' button is highlighted with a red box.

Agora, o NSA chama o download do Secure Client Agent do ISE e instala o Posture, o módulo

NAM e o NAM Profile configuration.xml .



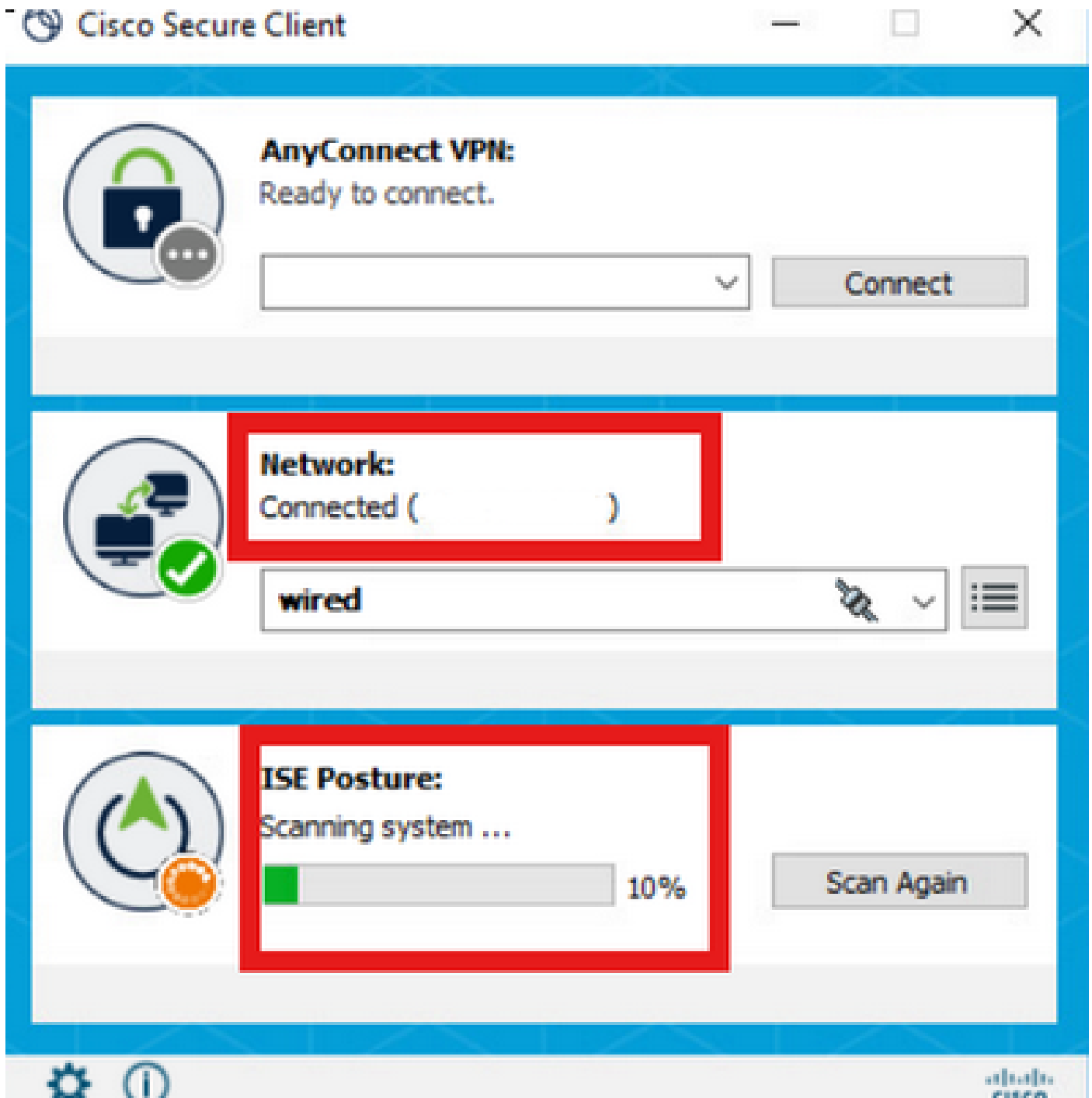
Um prompt de reinicialização disparado após a instalação do NAM. Clique em Sim.



## Etapa 2. EAP-FAST

Depois que o PC é reiniciado e o usuário faz login, o NAM autentica o usuário e a máquina através do EAP-FAST.

Se o endpoint for autenticado corretamente, o NAM exibirá que está conectado e o Módulo de postura acionará a Verificação de postura.



Nos registros ao vivo do ISE, o endpoint agora está atingindo a regra de acesso desconhecido.

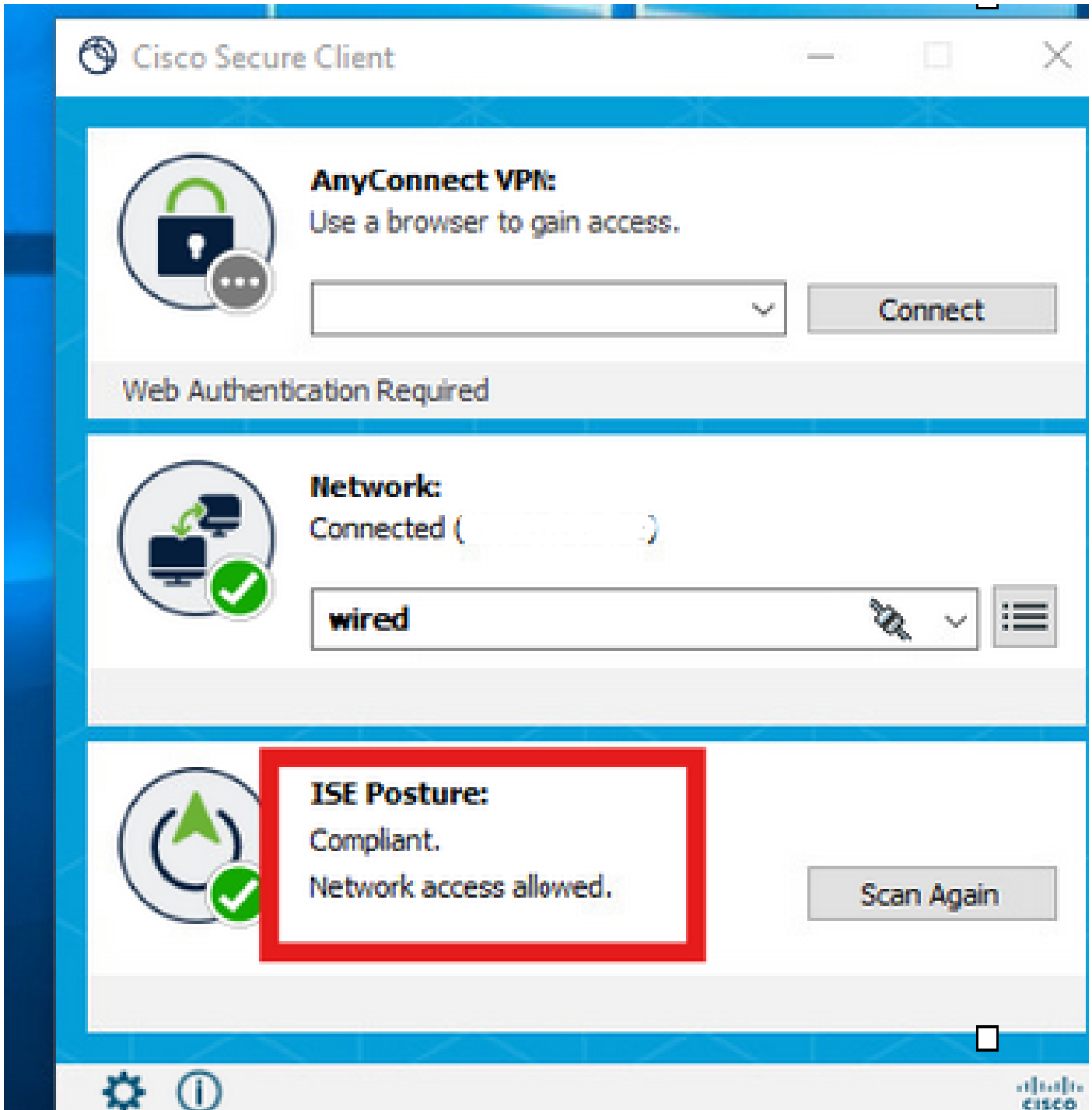
Jul 27, 2024 12:29:06...			user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	<b>Dot1x Policy &gt;&gt; Unknown Access</b>	Redirection	Pending
Jul 27, 2024 12:28:48...			host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Agora, o protocolo de autenticação é EAP-FAST com base na configuração do perfil NAM e o resultado do encadeamento EAP é "Success".

AcsSessionID	pk3-3/511201330/230
NACRadiusUserName	user1
NACRadiusUserName	host/DESKTOP-QSCE4P3
SelectedAuthenticationIden...	PRAD
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	[REDACTED]
EapChainingResult	User and machine both succeeded
ISEPolicySetName	Dot1x Policy
IdentitySelectionMatchedRule	Default
AD-User-Resolved-Identities	user1@aaa.prad.com
AD-User-Candidate-Identities	user1@aaa.prad.com
AD-Host-Resolved-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com
AD-Host-Candidate-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com

### Etapa 3. Varredura de postura

O Módulo de postura de cliente seguro aciona a Verificação de postura e é marcado como Reclamação com base na Política de postura do ISE.



O CoA é acionado após a Verificação de postura e agora o endpoint atinge a Política de acesso a reclamações.

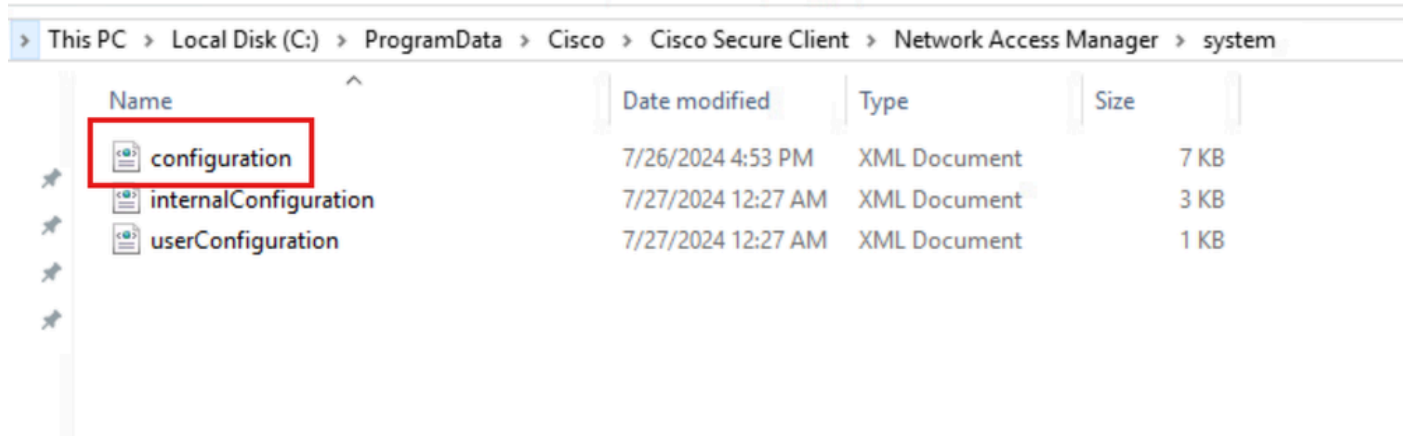
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...	Success	...	B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...	Success	...	...	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:31...	Success	...	...	...	...	...	...	Compliant
Jul 27, 2024 12:29:06...	Success	...	...	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...	Success	...	...	host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Troubleshooting

## Etapa 1. Perfil NAM

Verifique se o perfil NAM configuration.xml está presente neste caminho no PC após a instalação do módulo NAM.

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



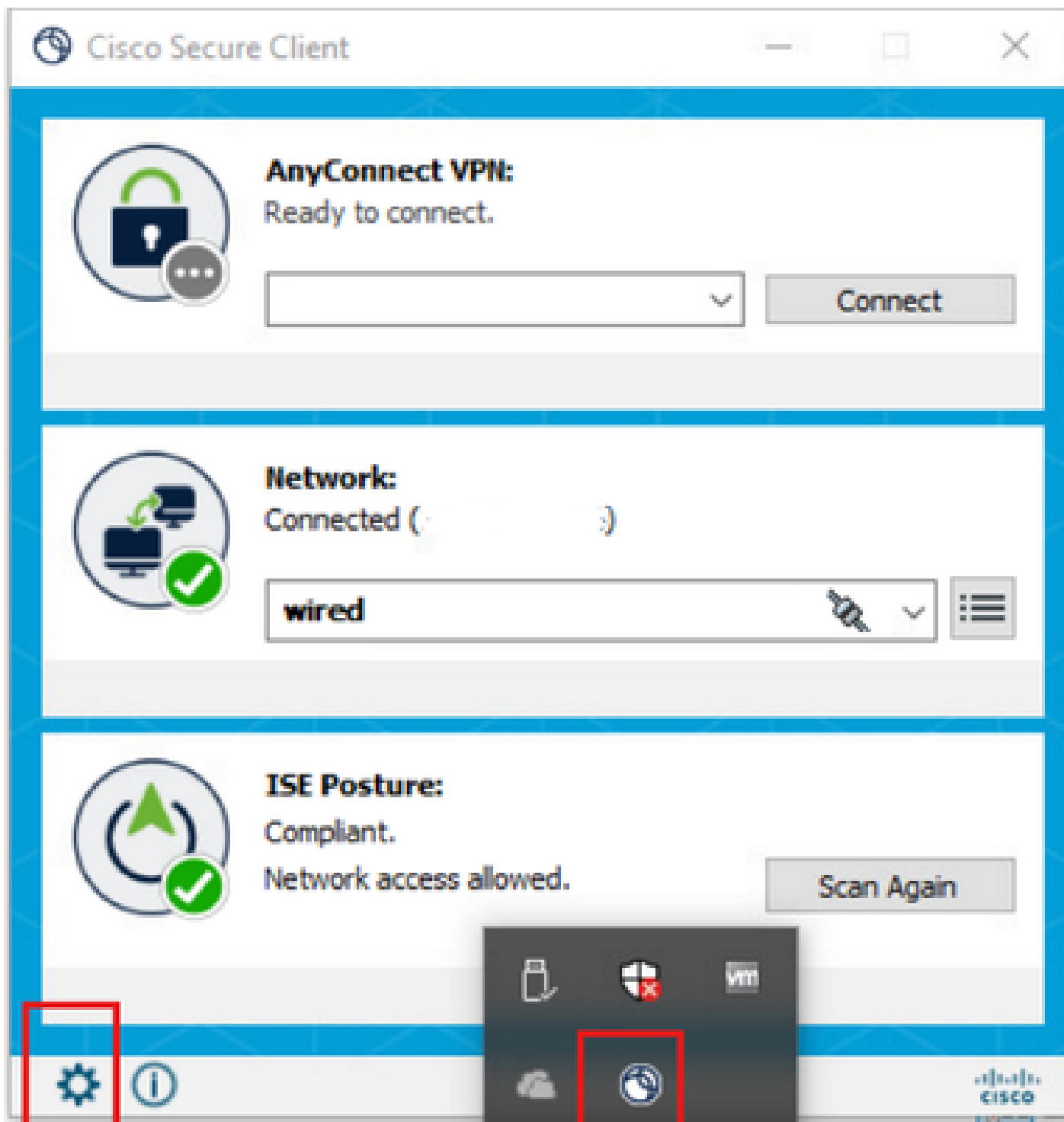
The screenshot shows a Windows File Explorer window with the address bar displaying the path: This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > Network Access Manager > system. The main area shows a list of files with columns for Name, Date modified, Type, and Size. The 'configuration' file is highlighted with a red box.

Name	Date modified	Type	Size
configuration	7/26/2024 4:53 PM	XML Document	7 KB
internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB
userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB

## Etapa 2. Log Estendido do NAM

Clique no ícone Secure Client (Cliente seguro) na barra de tarefas e selecione o ícone "Settings" (Configurações).





Navegue até a guia Network > Log Settings. Marque a caixa de seleção Enable Extended Logging.

Defina o tamanho do arquivo de captura de pacote como 100 MB.

Após reproduzir o problema, clique em Diagnostics para criar o pacote DART no endpoint.



The screenshot shows the Network Access Manager (NAM) interface. On the left, a navigation menu includes 'Status Overview', 'AnyConnect VPN', 'Network' (highlighted with a red box), and 'ISE Posture'. Below the menu, a button labeled 'Diagnostics' is also highlighted with a red box. The main content area is titled 'Network Access Manager' and has tabs for 'Configuration', 'Log Settings' (highlighted with a red box), 'Statistics', and 'Message History'. Under the 'Log Settings' tab, there is a section titled 'Use extended logging to collect additional information about product operations.' This section contains several settings: 'Enable Extended Logging' (checked, highlighted with a red box), 'IHV:' (set to 'Off'), 'Filter Driver:' (set to 'Off'), 'Credential Provider' (unchecked), 'Packet Capture' (checked), and 'Maximum Packet Capture File Size (MB):' (set to '100').

A seção Histórico de Mensagens exibe os detalhes de cada etapa executada pelo NAM.

### Etapa 3. Depurações no Switch

Ative essas depurações no switch para solucionar problemas de dot1x e fluxo de redirecionamento.

```
debug ip http all
```

```
debug ip http transactions
```

```
debug ip http url
```

```
set platform software trace smd switch ative R0 aaa debug
```

```
set platform software trace smd switch ative R0 dot1x-all debug
```

```
set platform software trace smd switch ative R0 radius debug
```

```
set platform software trace smd switch ative R0 auth-mgr-all debug
```

```
set platform software trace smd switch ative R0 eap-all debug
```

```
set platform software trace smd switch ative R0 epm-all debug
```

```
set platform software trace smd switch ative R0 epm-redirect debug
```

```
set platform software trace smd switch ative R0 webauth-aaa debug
```

```
set platform software trace smd switch ative R0 webauth-httpd debug
```

Para exibir os logs

```
show logging
```

```
show logging process smd internal
```

## Etapa 4. Depurações no ISE

Colete o pacote de suporte do ISE com estes atributos a serem definidos no nível de depuração:

- postura
- portal
- provisionamento
- runtime-AAA
- nsf
- nsf-session
- suíço
- client-webapp

## Informações Relacionadas

[Configurar o NAM do Secure Client](#)

[Guia de implantação prescritiva de postura do ISE](#)

[Identificar e Solucionar Problemas do Dot1x nos Catalyst 9000 Series Switches](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.