Configure o acesso seguro para RA-VPNaaS com SSO Duo e avaliação de postura com ISE

Contents

Gerar pacote DART no cliente seguro

Informações Relacionadas

Introdução

Este documento descreve como configurar a Avaliação de postura para usuários de VPN de acesso remoto com o Identity Service Engine (ISE) e o Secure Access com Duo.

Pré-requisitos

- Configurar Provisionamento de Usuário no Acesso Seguro
- Configurar SSO Duo com Proxy de Autenticação ou IDP de Terceiros
- Cisco ISE conectado ao acesso seguro através do túnel

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity Service Engine
- Acesso seguro
- Cisco Secure Client
- Guia para autenticação de dois fatores - Segurança dupla
- Postura do ISE
- Autenticação, autorização e contabilidade

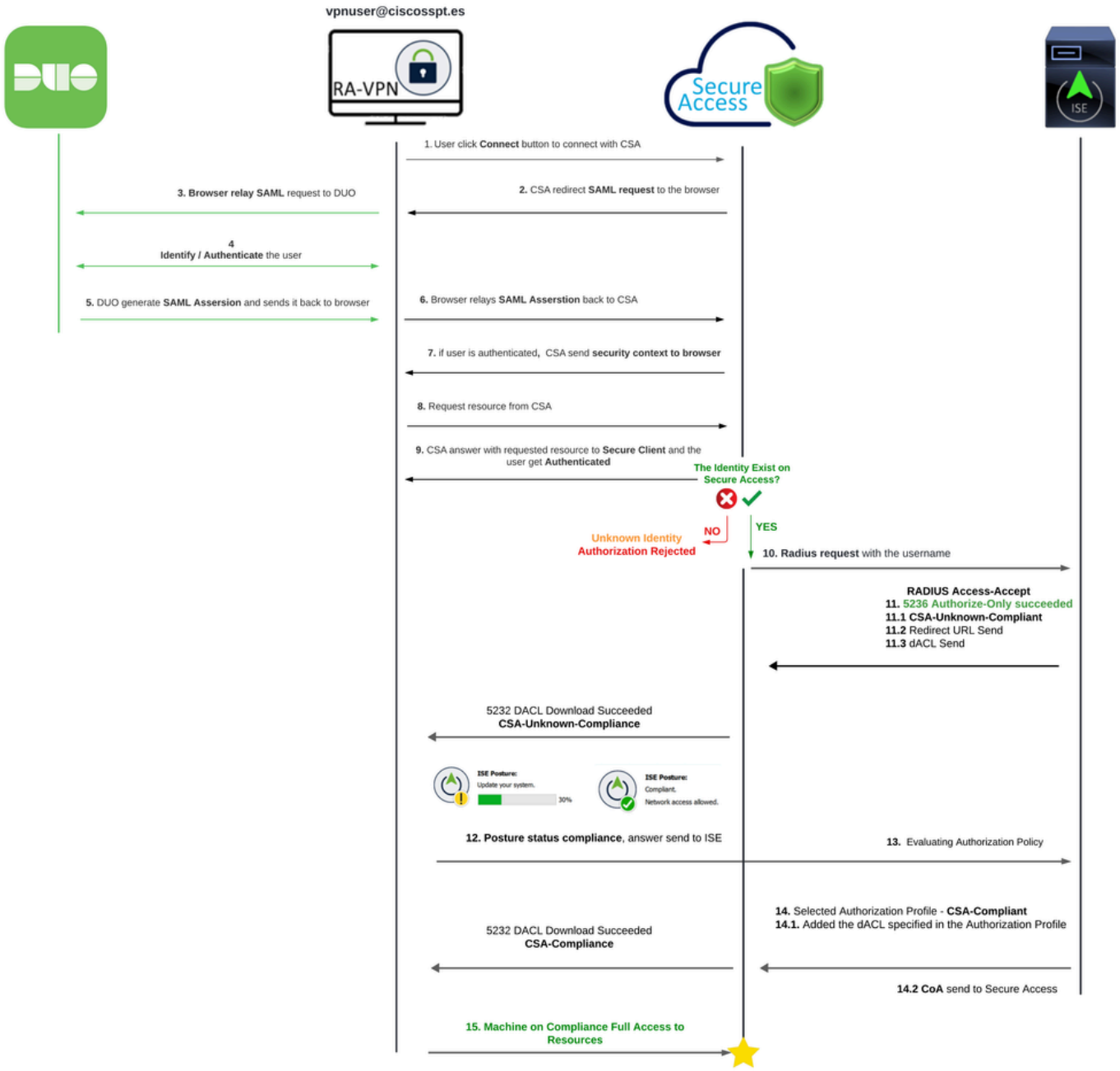
Componentes Utilizados

As informações neste documento são baseadas em:

- Patch 1 do Identity Service Engine (ISE) versão 3.3
- Acesso seguro
- Cisco Secure Client - Anyconnect VPN versão 5.1.2.42

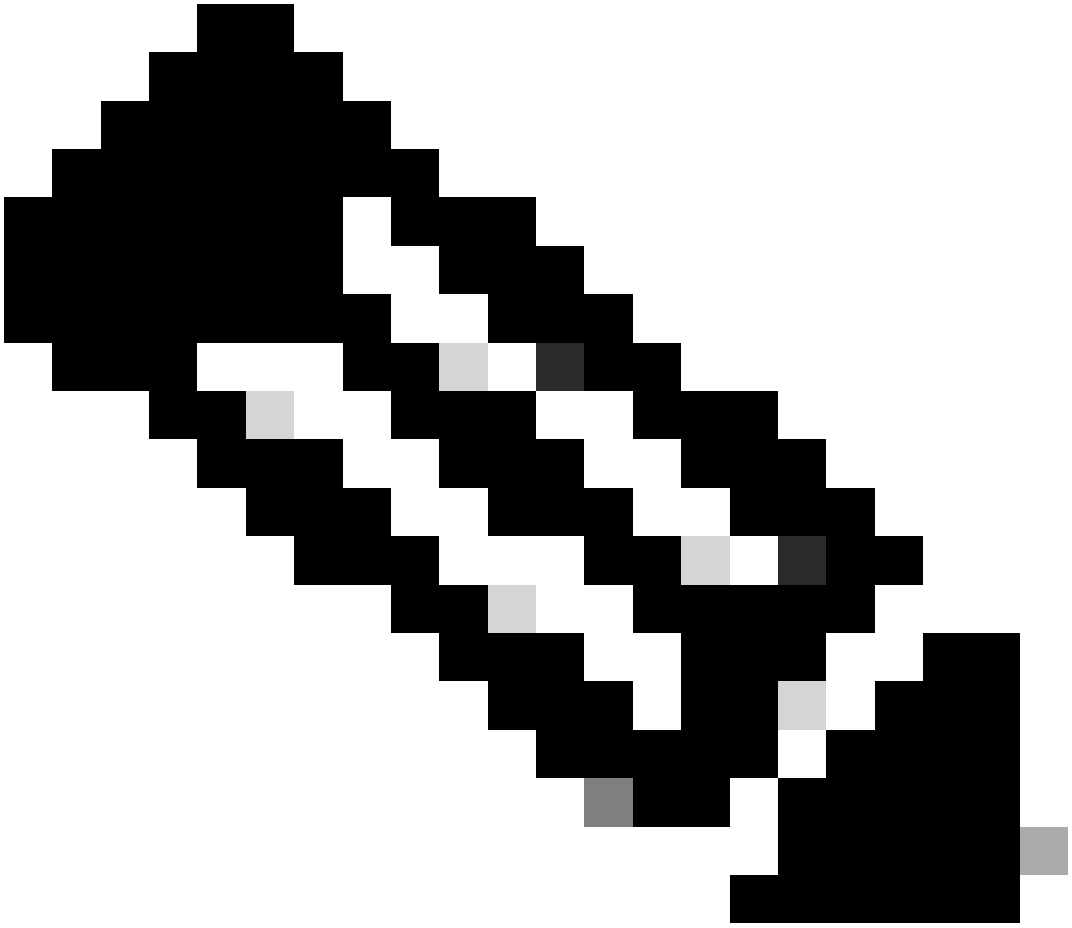
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio



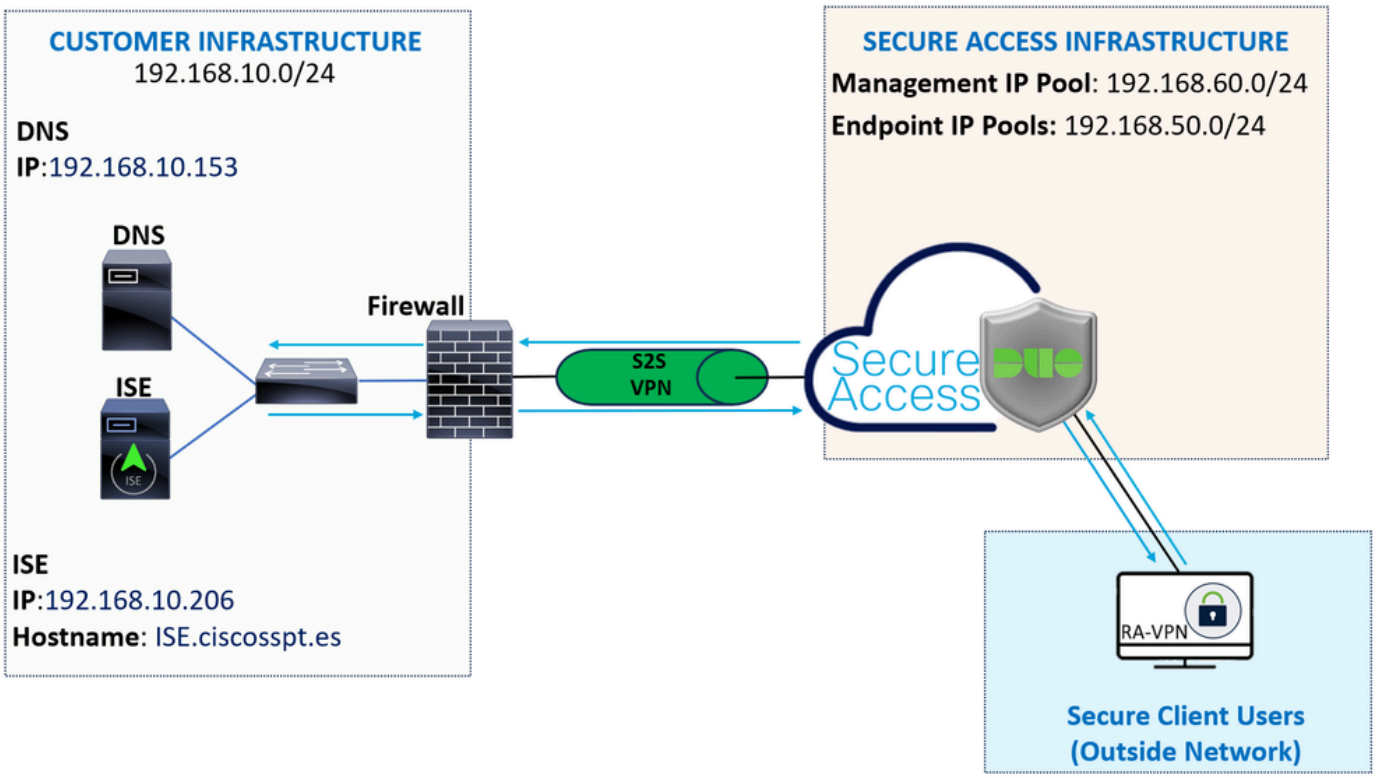
A integração do Duo SAML com o Cisco Identity Services Engine (ISE) aprimora o processo de autenticação, adicionando outra camada de segurança às soluções Cisco Secure Access. O Duo SAML fornece um recurso de Logon Único (SSO) que simplifica o processo de logon do usuário, garantindo altos padrões de segurança.

Depois de autenticado por meio do Duo SAML, o processo de autorização é tratado pelo Cisco ISE. Isso permite decisões de controle de acesso dinâmico com base na identidade do usuário e na postura do dispositivo. O ISE pode aplicar políticas detalhadas que determinam quais recursos um usuário pode acessar, quando e de quais dispositivos.

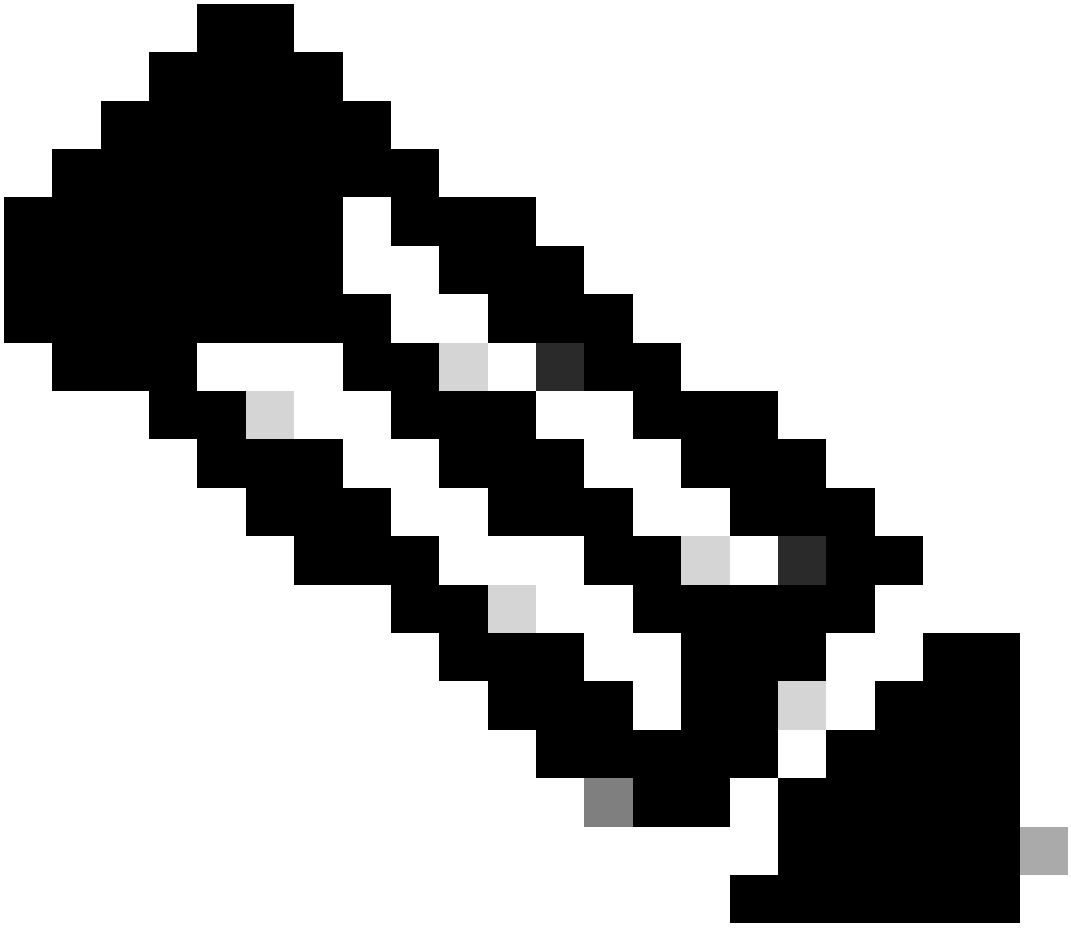


Observação: para configurar a integração do RADIUS, você precisa se certificar de que haja comunicação entre as duas plataformas.

Diagrama de Rede


CUSTOMER INFRASTRUCTURE
192.168.10.0/24
DNS
IP:192.168.10.153
DNS
ISE
Firewall
S2S
VPN
ISE
IP:192.168.10.206
Hostname: ISE.ciscosspt.es
SECURE ACCESS INFRASTRUCTURE
Management IP Pool: 192.168.60.0/24
Endpoint IP Pools: 192.168.50.0/24
Secure
Access
RA-VPN
Secure Client Users
(Outside Network)

Configurar



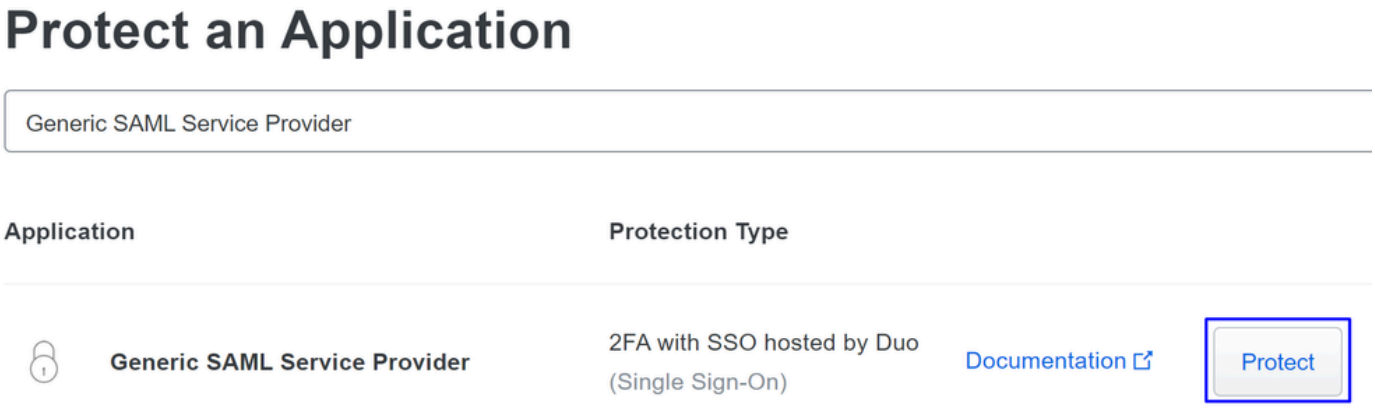
Observação: antes de iniciar o processo de configuração, você deve concluir as primeiras etapas com acesso seguro e integração do ISE.

Configuração Duo

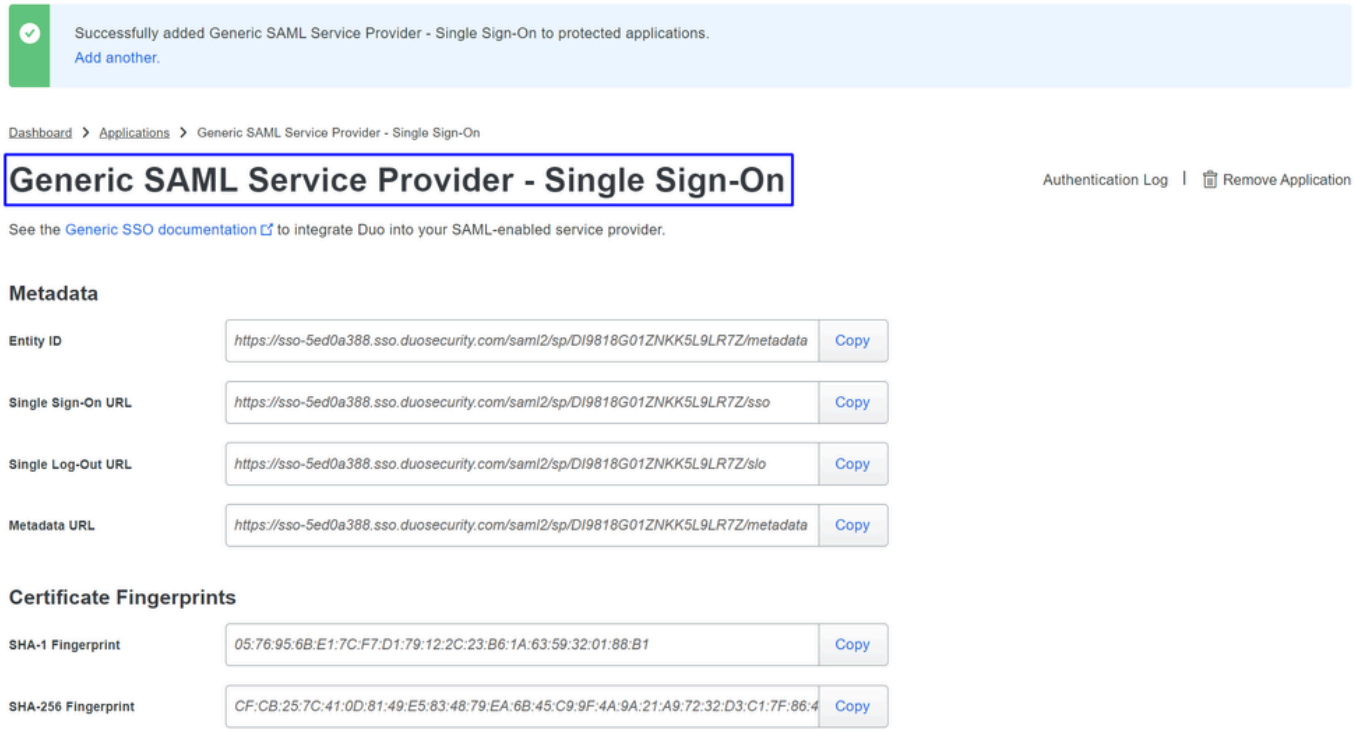
Para configurar o aplicativo RA-VPN, continue com as próximas etapas:

Navegue até o Painel de administração do Duo

- Navegue até **Applications** > **Protect an Application**
  - Procurar **Generic SAML Service Provider**
  - Clique em Protect



Você deve ter o aplicativo exibido na tela; lembre-se do nome do aplicativo para a configuração da VPN.



Neste caso, **Generic SAML Service Provider.**

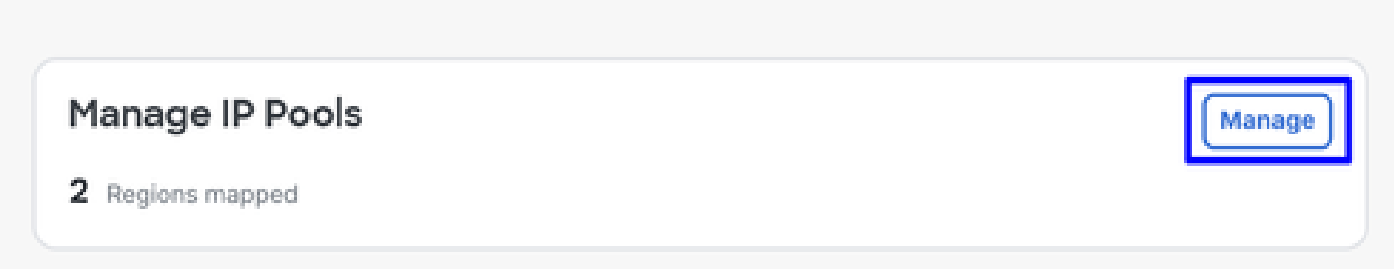
Configuração de acesso seguro

Configurar o grupo Radius nos pools IP

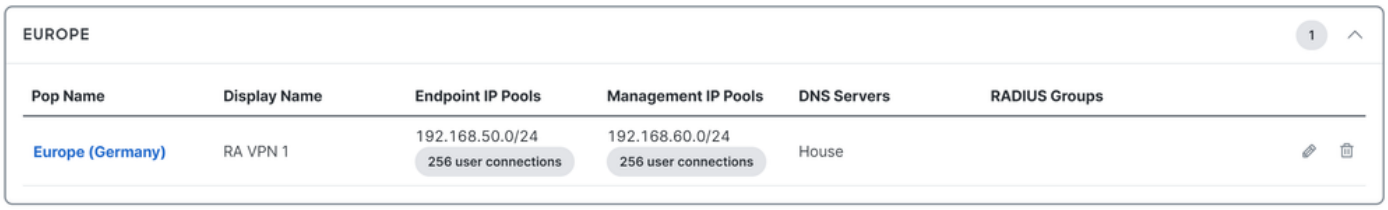
Para configurar o perfil de VPN usando Radius, continue com as próximas etapas:

Navegue até o Painel do Secure Access.

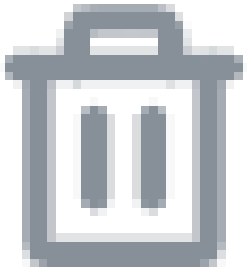
- Clique em **Connect > Enduser Connectivity > Virtual Private Network**
- Em sua Configuração de Pool (**Manage IP Pools**), clique emManage



- Selecione **IP Pool Region** e configure o **Radius Server**

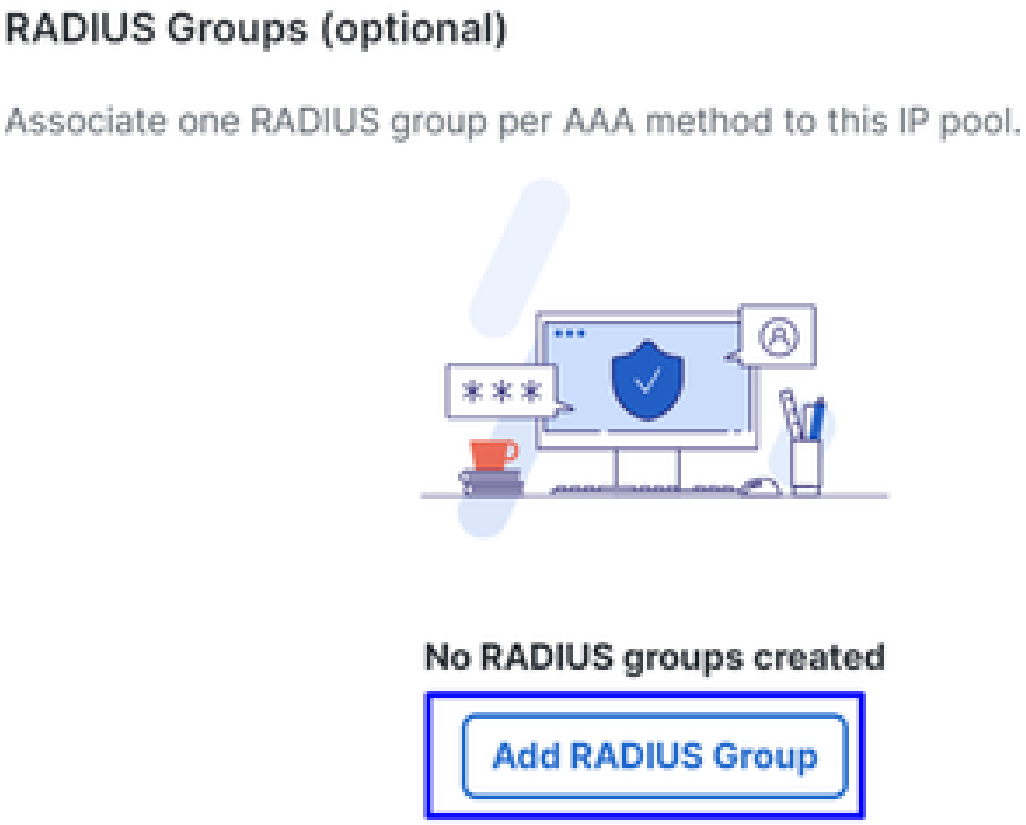


- Clique no lápis para editar



- Agora, na lista suspensa de configuração da seção IP Pool, em **Radius Group (Optional)**

- Clique em Add RADIUS Group



← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

Group Name: Configure um nome para sua integração do ISE no Secure Access

- **AAA method**

  - **Authentication**: Marque a caixa de seleção para **Authentication** e selecione a porta, por padrão, é 1812

    - Caso sua autenticação exijaMicrosoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2), marque a caixa de seleção

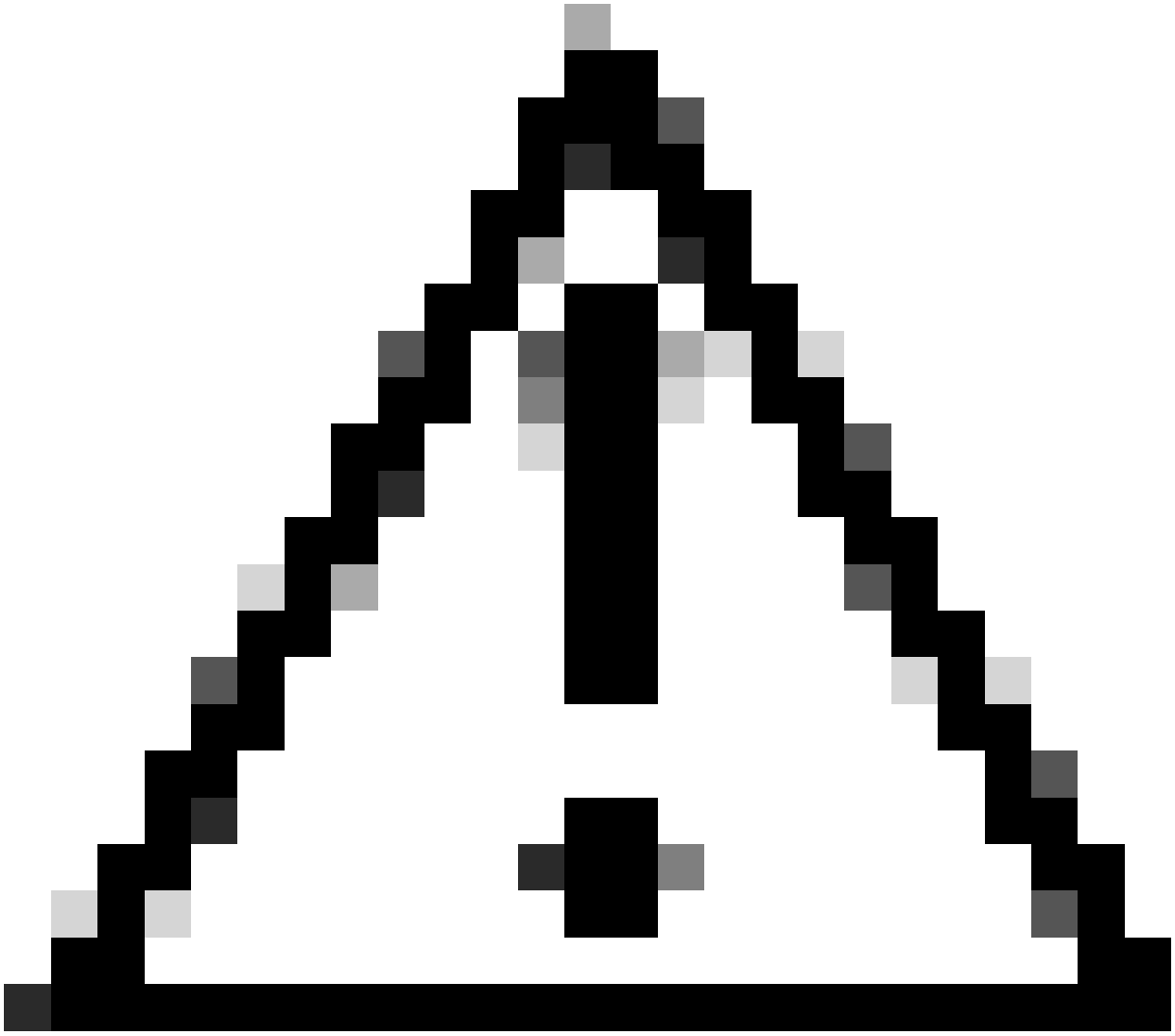
- **Authorization**: Marque a caixa de seleção para Authorization e selecione a porta, por padrão, é 1812

  - Marque a caixa de seleção para **Authorization mode Only Change of Authorization (CoA) mode** epara permitir a postura e as alterações do ISE

- **Accounting**: Marque a caixa de seleção para Autorização e selecione a porta, por padrão, é 1813

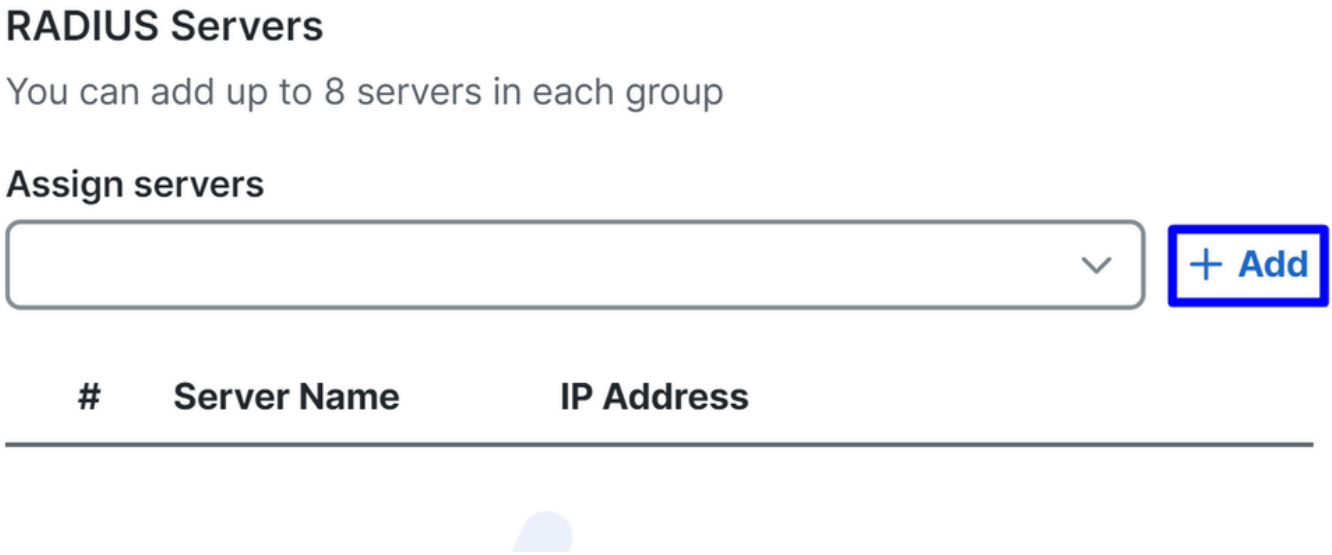
  - Escolha **Single or Simultaneous** (em modo simples, os dados de contabilização são enviados para apenas um servidor. No modo simultâneo, contabilizar dados para todos os servidores do grupo)

    - Marque a caixa de seleção de **Accounting update** para ativar a geração periódica de mensagens de atualização de contabilidade provisória RADIUS.

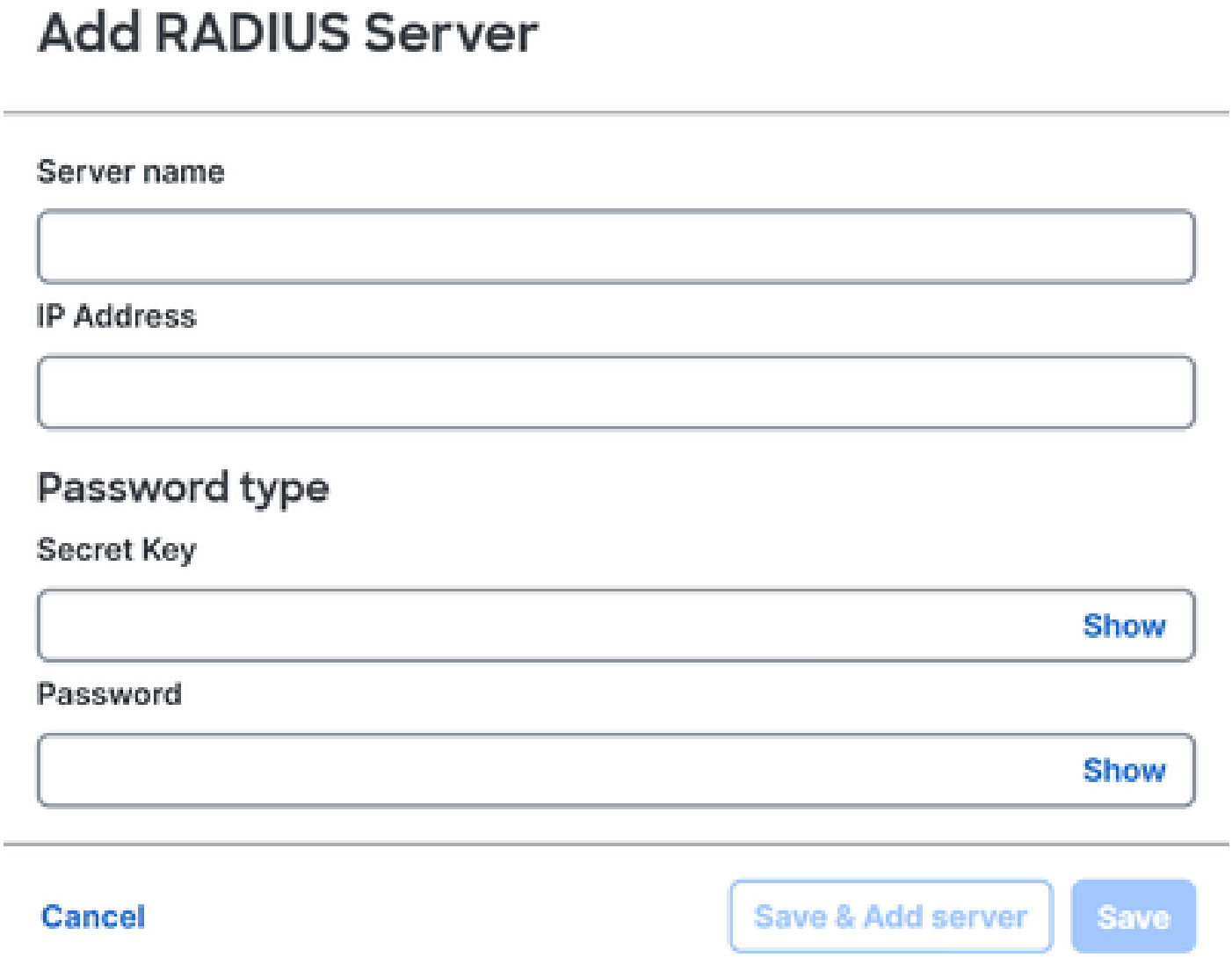


Cuidado: os Authentication **Authorization** métodos e, quando selecionados, devem usar a mesma porta.

- Depois disso, você precisa configurar o **RADIUS Servers** (ISE) que é usado para autenticar via AAA na seção **RADIUS Servers**:
- Clique em + Add

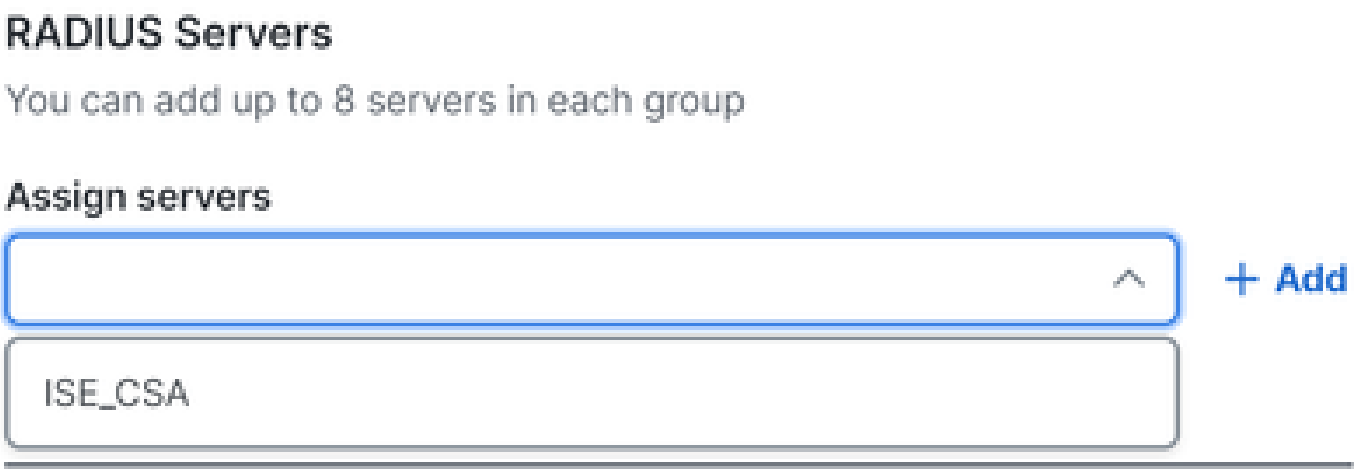


- Em seguida, configure as próximas opções:



- Server Name: Configure um nome para identificar seu servidor ISE.
- **IP Address**: Configure o IP do seu dispositivo Cisco ISE que pode ser acessado por meio do acesso seguro
- **Secret Key**: Configure sua chave secreta RADIUS
- **Password**: Configure sua senha do Radius

- Clique **Save** e atribua seu servidor Radius sob a Assign Server opção e selecione seu servidor ISE:



- Clique **Save** novamente para salvar todas as configurações feitas

← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

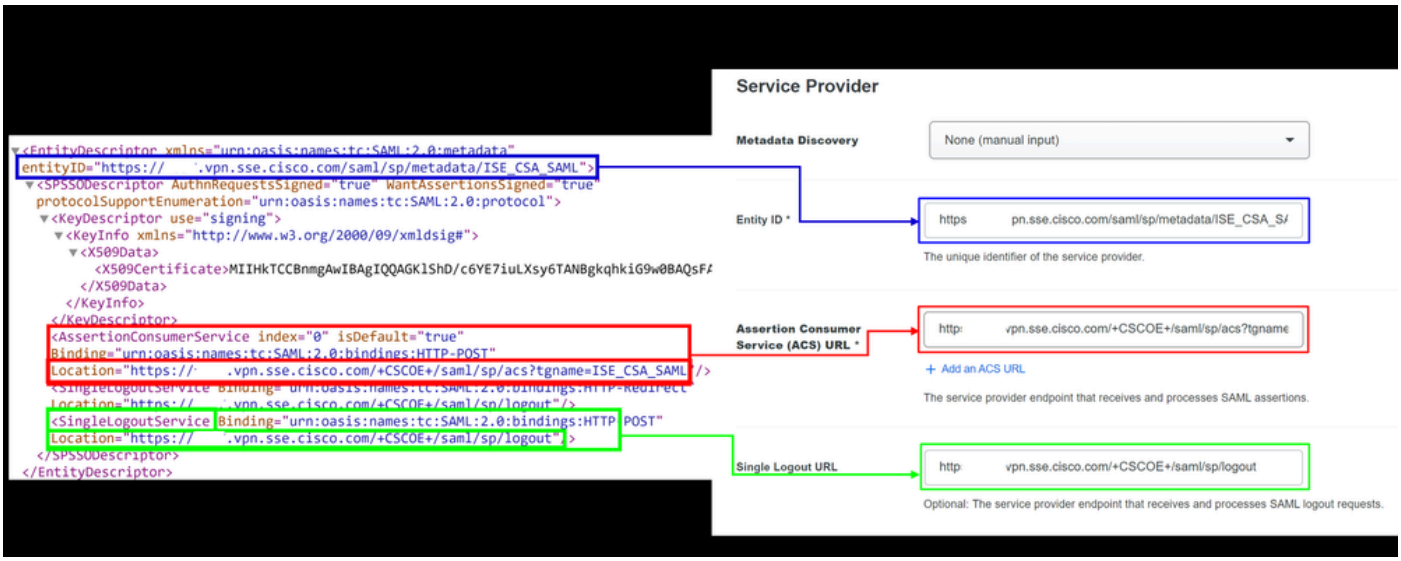
ISE_CSA

+ Add

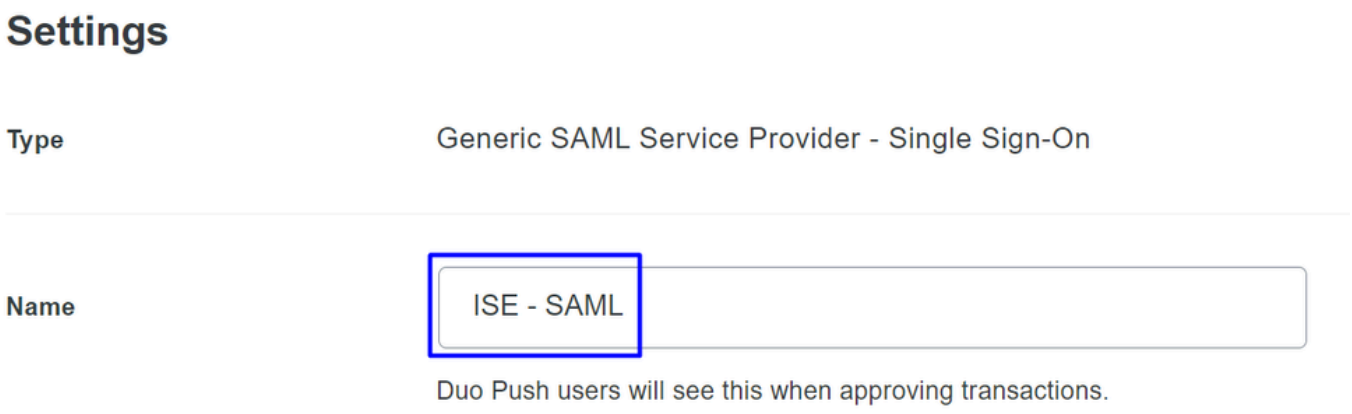
#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**: Escolher **SAML**

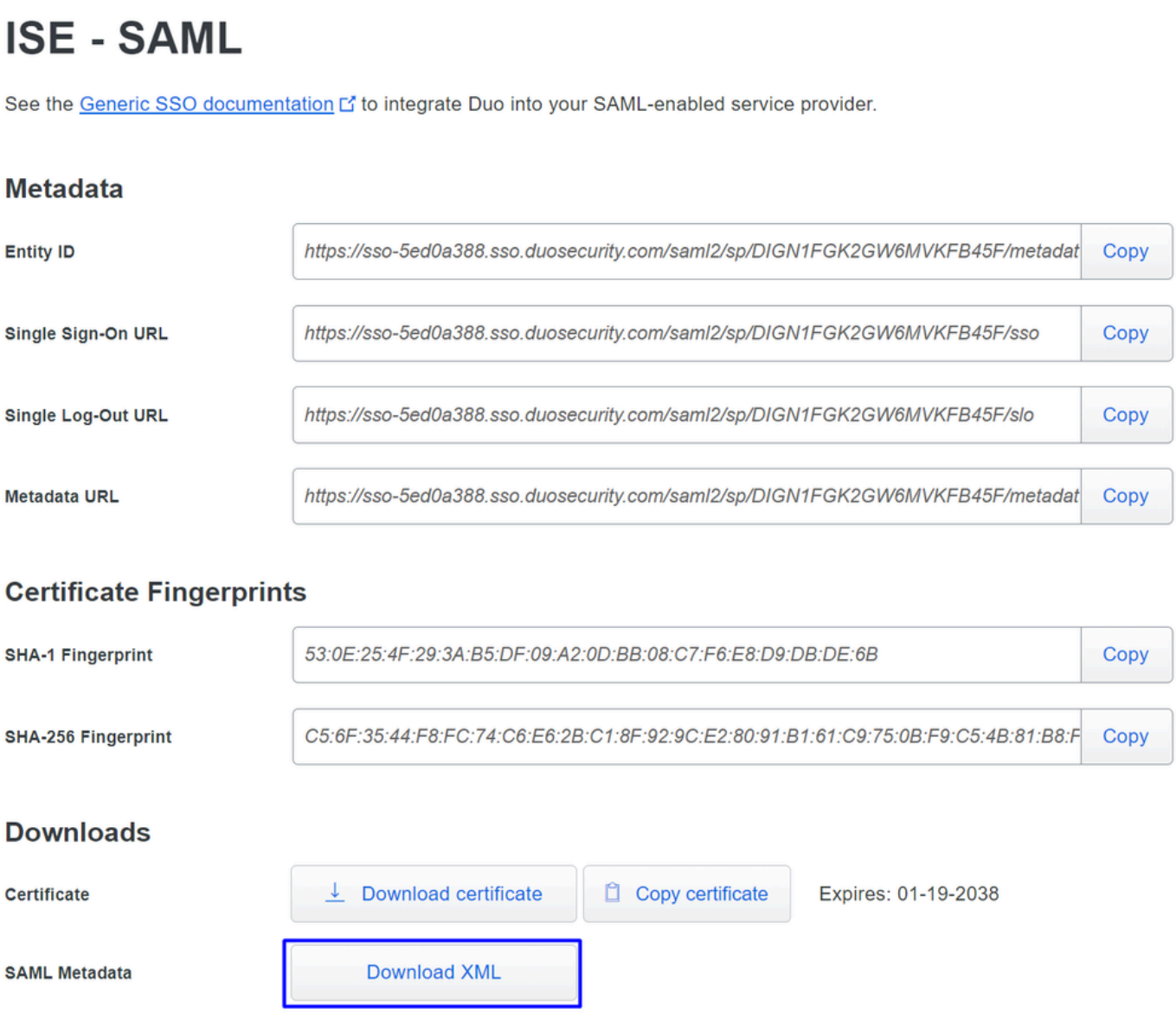
- Clique em Download Service Provider XML file
- Substitua as informações no aplicativo configurado na etapa Configuração Duo



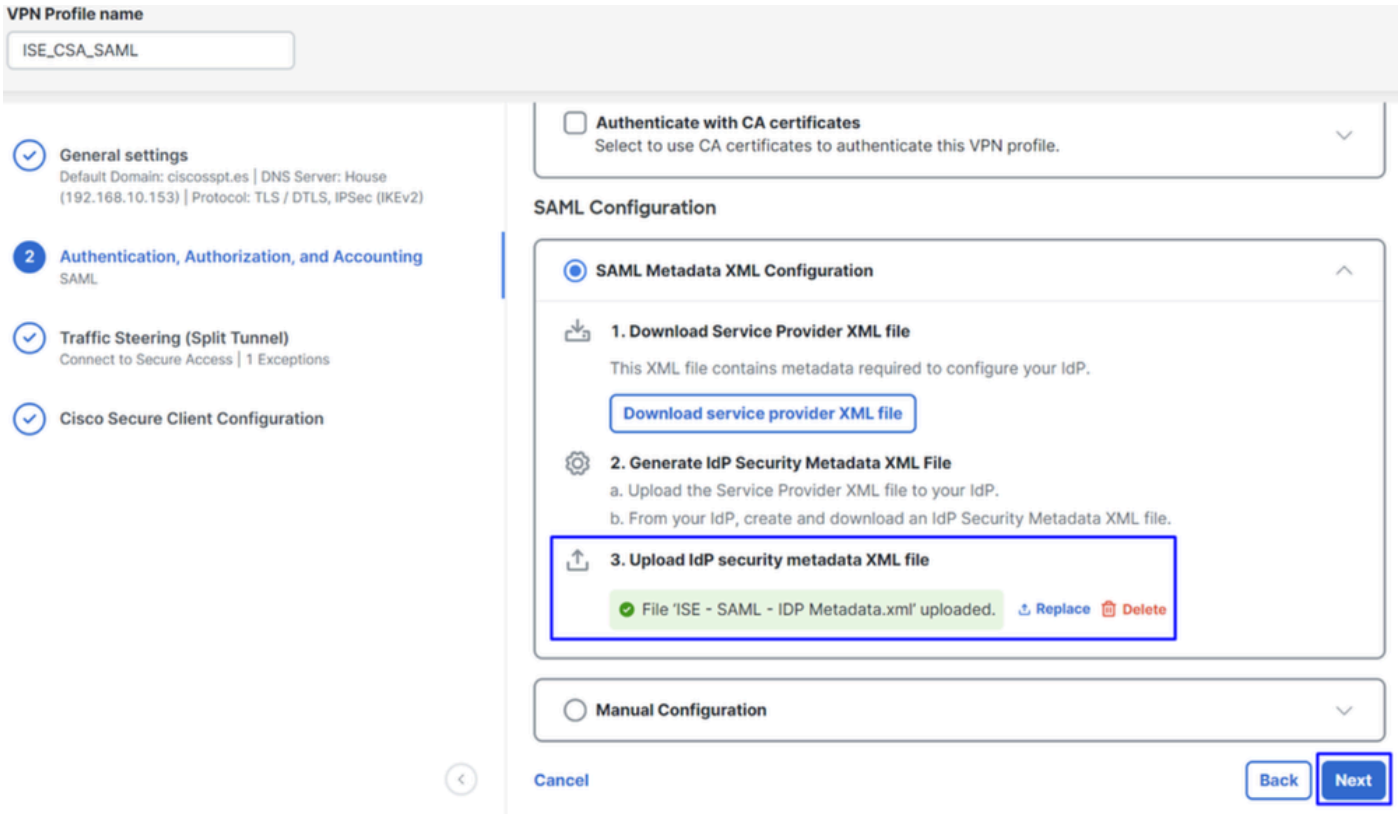
- Depois de ter configurado essas informações, mude o nome do Duo para algo relacionado à integração que você está fazendo



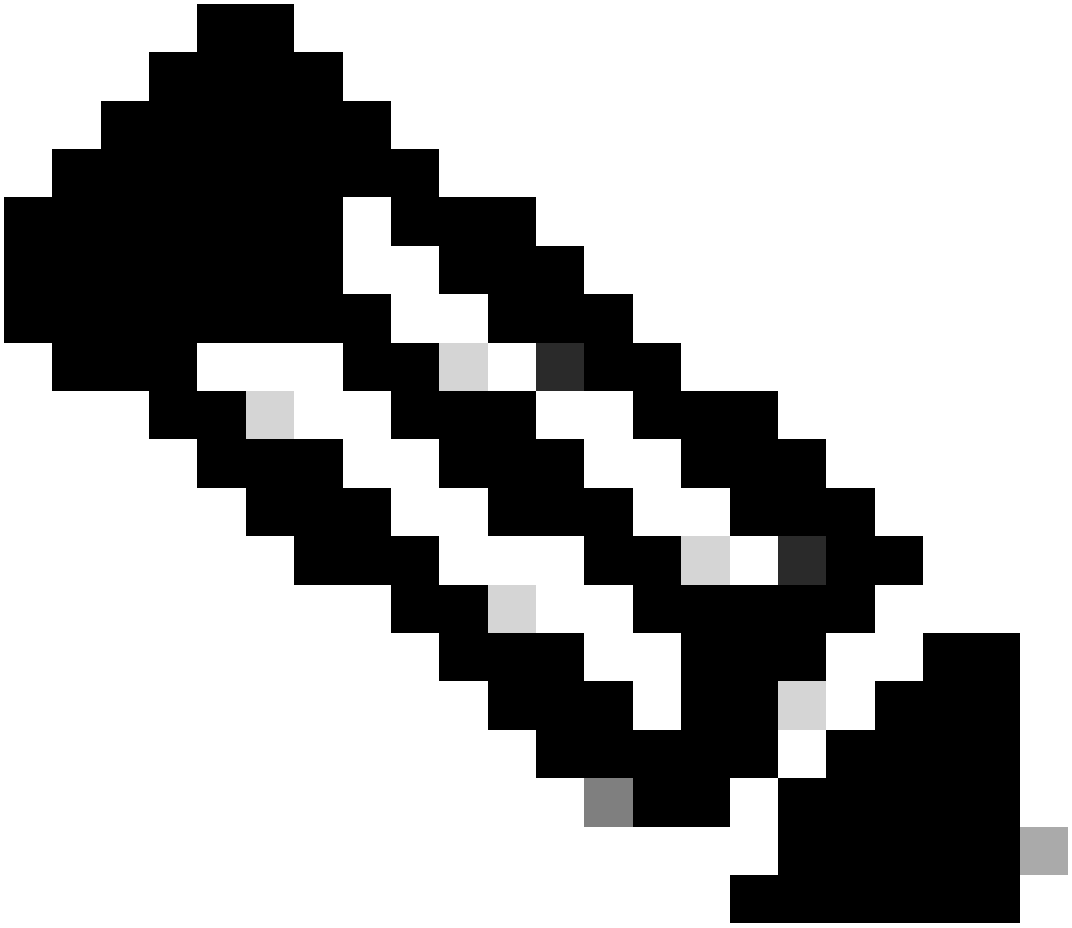
- Clique **Save** no aplicativo Duo.
- Ao clicar em Salvar, você deve fazer o download do **SAML Metadata** clicando no botão **Download XML**



- Carregue o **SAML Metadata** em Acesso seguro sob a opção **3. Upload IdP security metadata XML file** e clique em **Next**

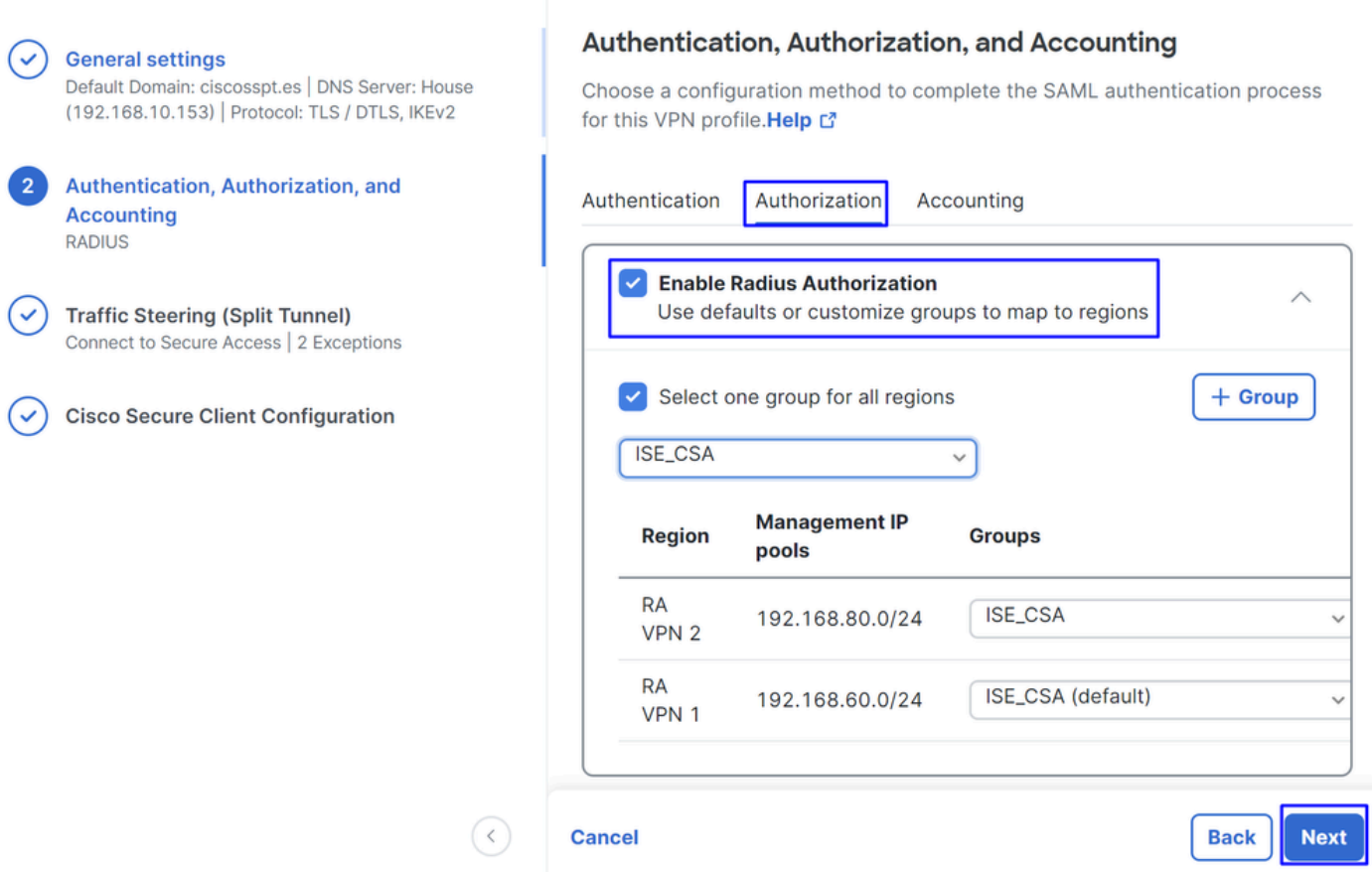


Continue com a autorização.



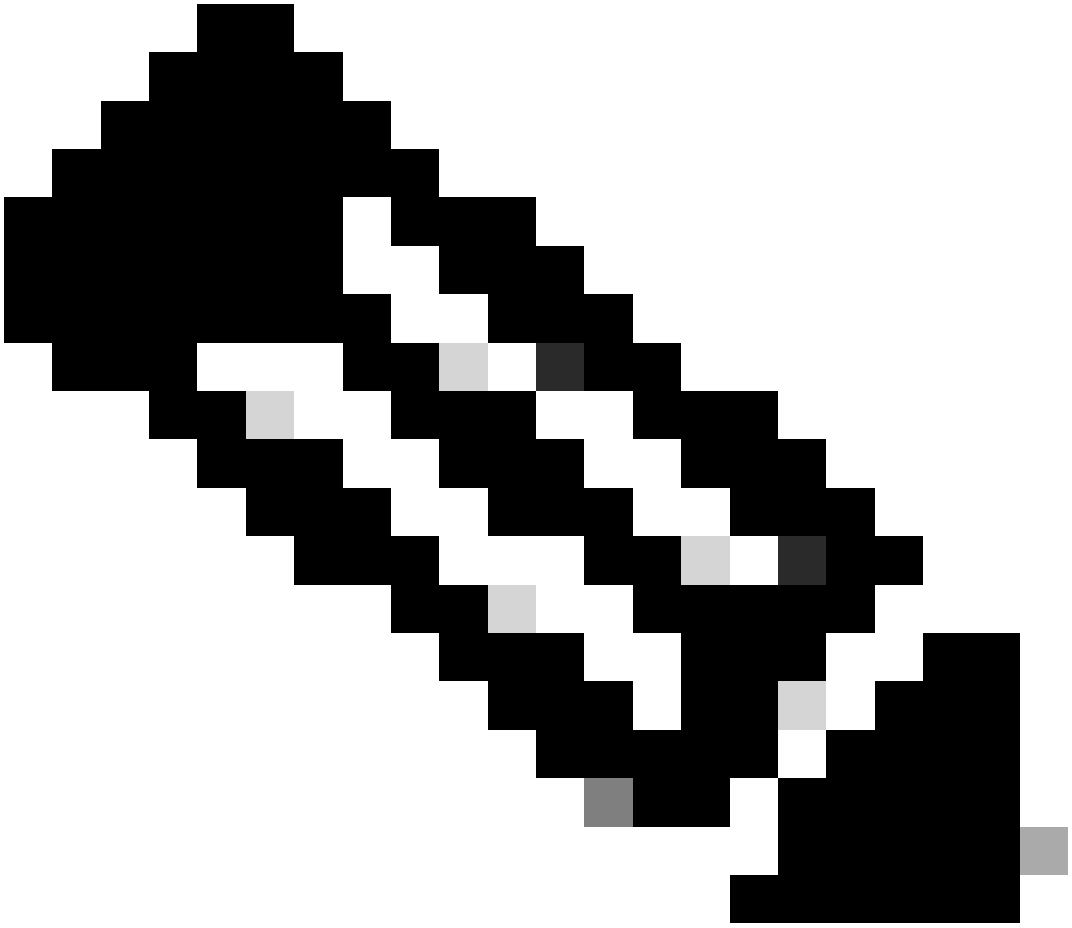
Observação: depois de configurar a autenticação com SAML, você a autorizará por meio do ISE, o que significa que o pacote radius enviado pelo Secure Access conterá apenas o nome de usuário. O campo de senha não existe aqui.

Autorização



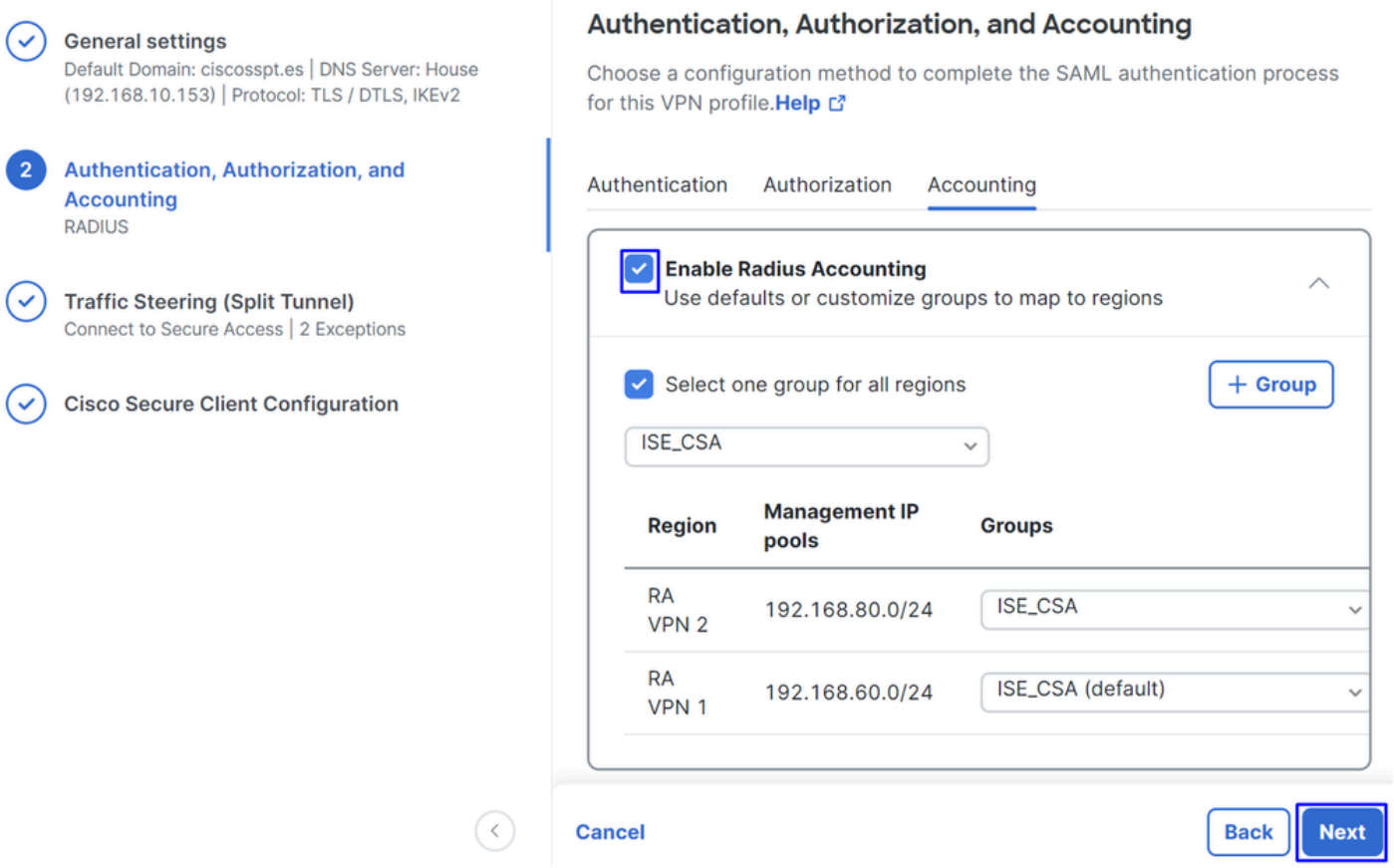
- **Authorization**
  - **Enable Radius Authorization**: Marque a caixa de seleção para habilitar a autorização radius
  - **Selecione um grupo para todas as regiões**: marque a caixa de seleção para usar um servidor radius específico para todos os pools de acesso remoto - rede virtual privada (RA-VPN) ou defina-o para cada pool separadamente
- Clique em **Next**

Depois de configurar toda a **Authorization** peça, prossiga com o **Accounting**.



Observação: se você não ativar **Radio Authorization**, a postura não funcionará.

Relatório



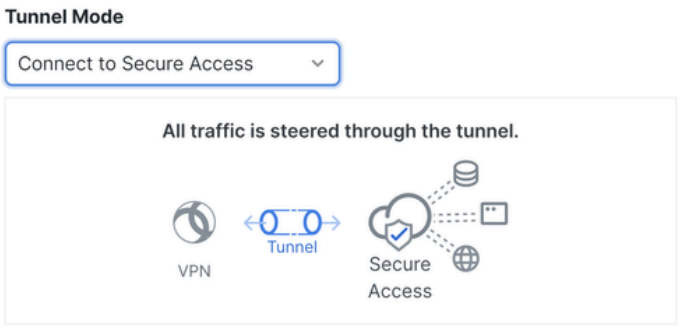
- **Accounting**
    - **Map Authorization groups to regions**: Escolha as regiões e escolha seu **Radius Groups**

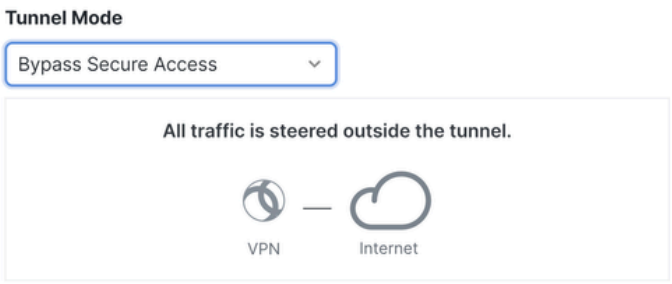
- Clique em **Next**

After you have done configured the Authentication, Authorization and Accounting continue comTraffic Steering.

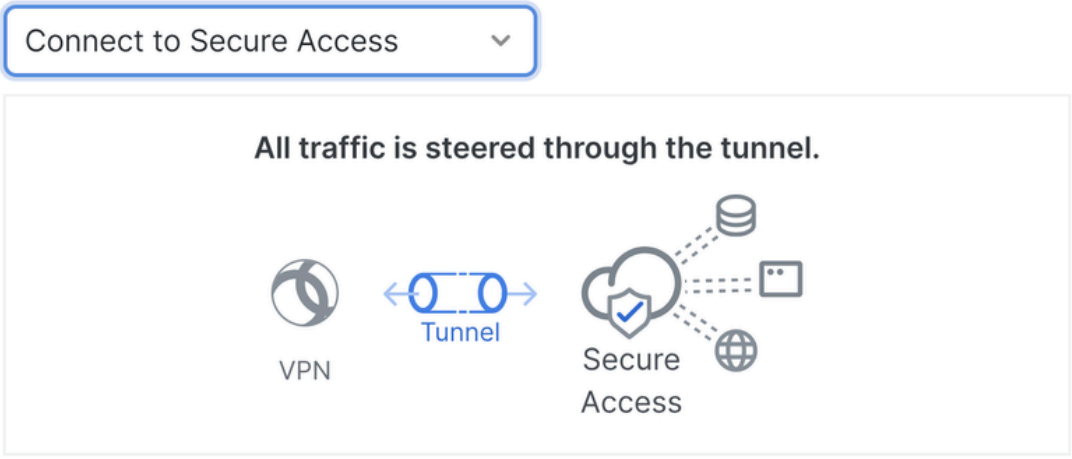
Direção de tráfego

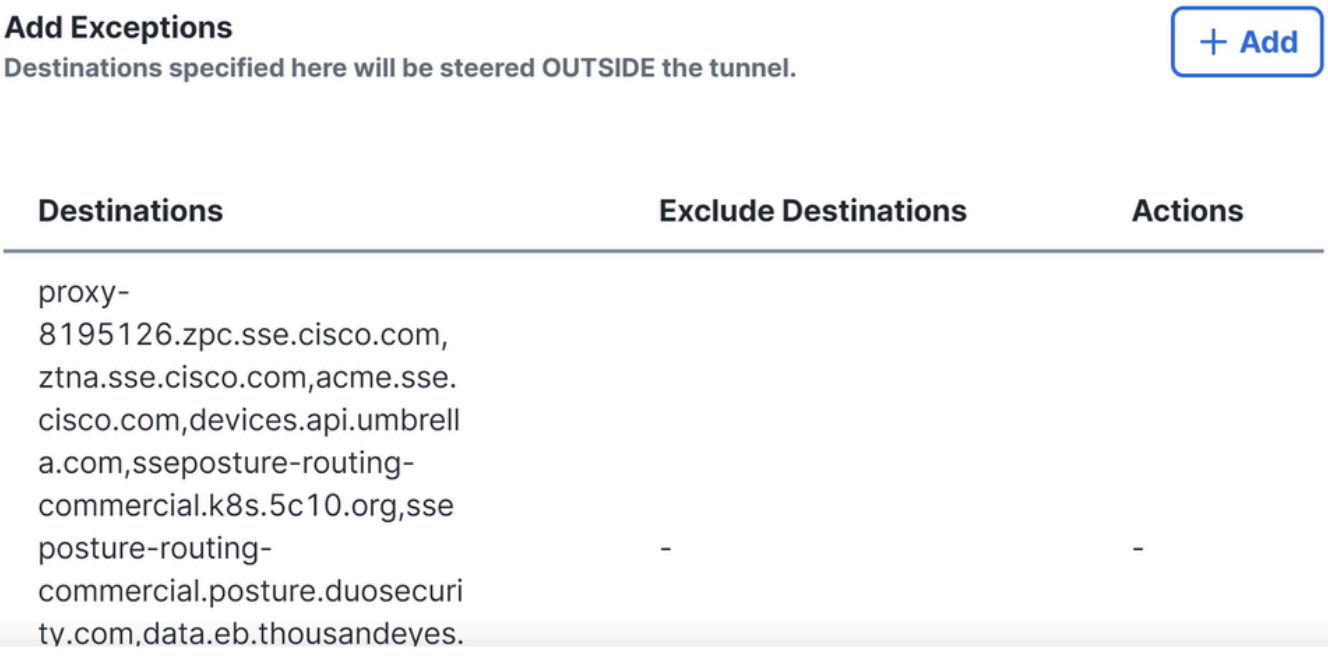
Sob o controle de tráfego, você precisa configurar o tipo de comunicação por meio do Secure Access.





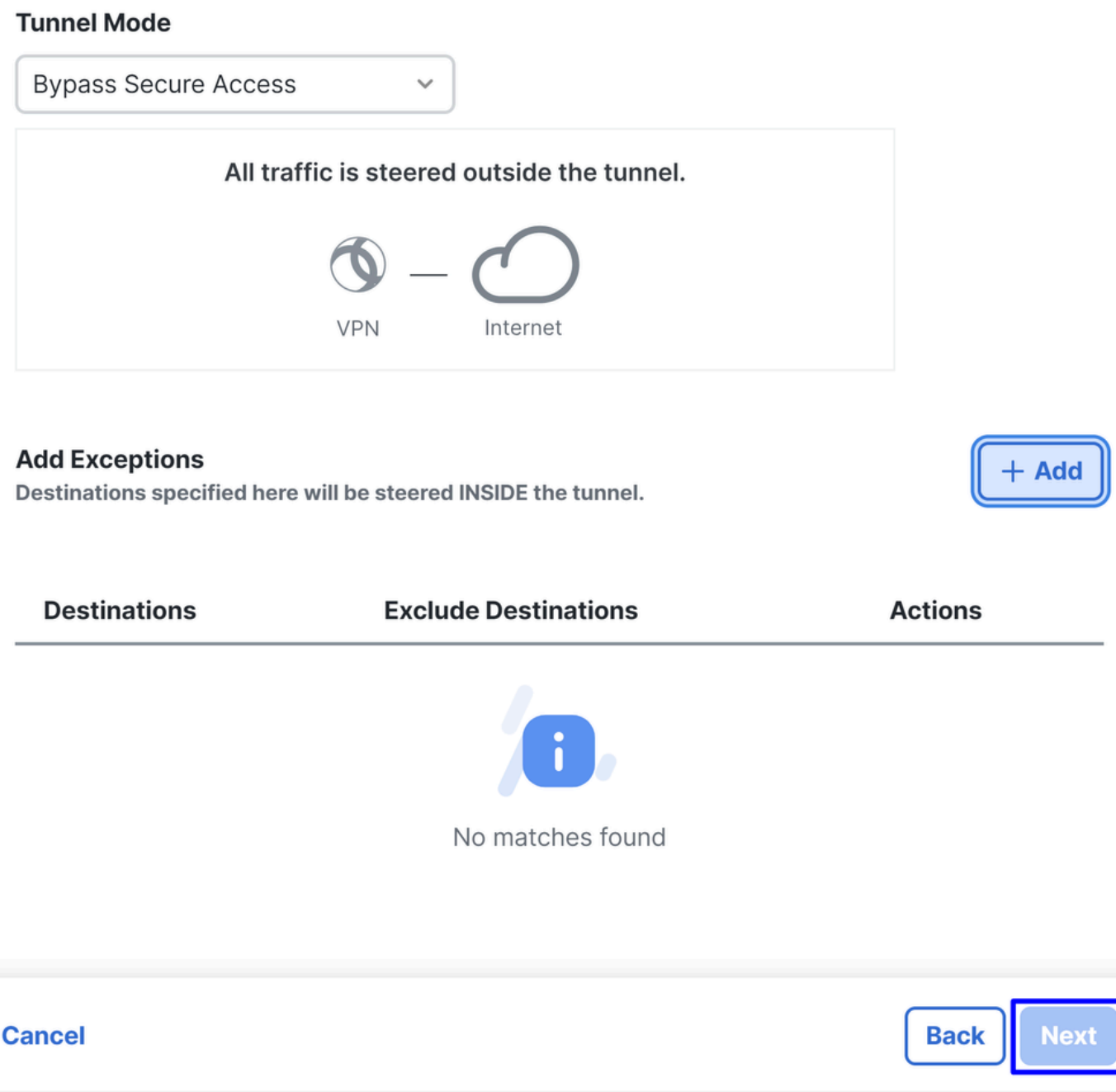
- Se você escolher, todo o tráfego da Internet **Connect to Secure Access**será encaminhado por **Secure Access**

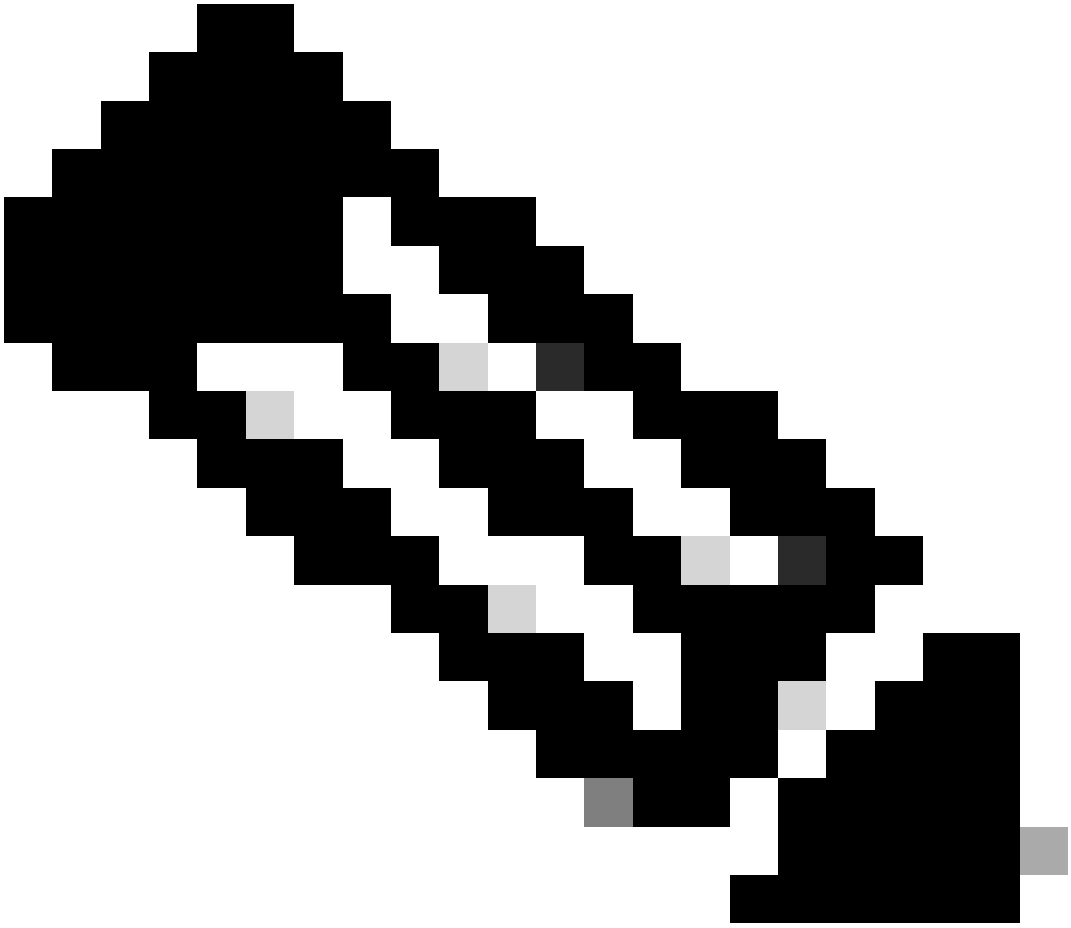




Se você quiser adicionar exclusões para domínios de Internet ou IPs, clique no **+ Add** botão e, em seguida, clique em **Next**.

- Se você decidir **Bypass Secure Access**fazer isso, todo o tráfego da Internet passará pelo seu provedor de Internet, não peloSecure Access (Sem proteção da Internet)

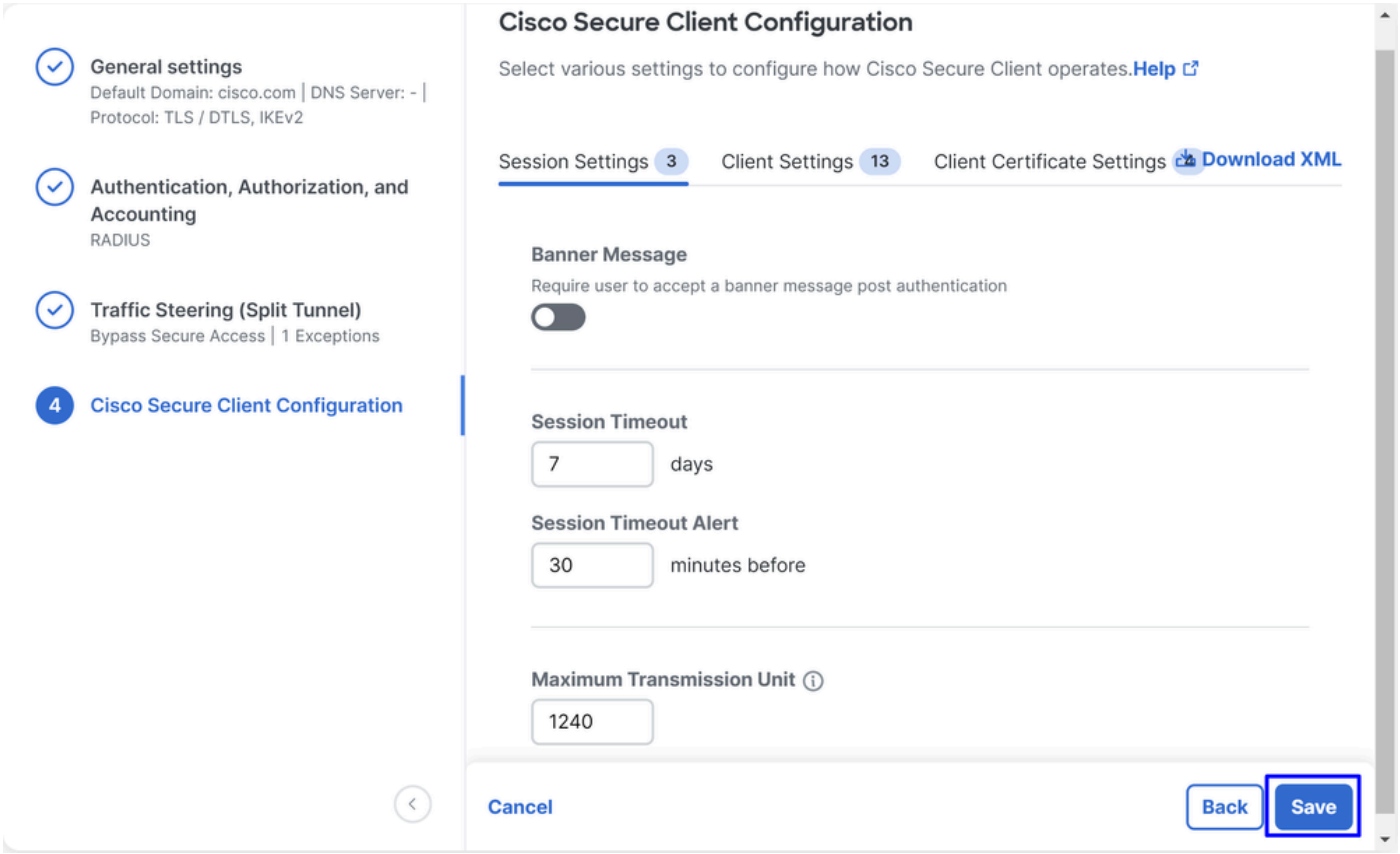




Observação: adicione **enroll.cisco.com** para postura do ISE ao escolher **Bypass Secure Access**.

Nesta etapa, você seleciona todos os recursos de rede privada que deseja acessar por meio da VPN. Para fazer isso, clique em **+ Add** e em **Next** quando tiver adicionado todos os recursos.

Configuração do Cisco Secure Client



Nesta etapa, você pode manter tudo como padrão e clicar em **Save**, mas se quiser personalizar mais sua configuração, consulte o Guia do Administrador do Cisco Secure Client.

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscosspt.es TLS, IPSec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

Configurações do ISE

Configurar lista de dispositivos de rede

Para configurar a autenticação por meio do Cisco ISE, você precisa configurar os dispositivos permitidos que podem fazer consultas ao Cisco ISE:

- Navegue até **Administration > Network Devices**
- Clique em **+ Add**

Network Devices List > CSA

Network Devices

Name CSA

Description

IP Address * IP : 192.168.60.0 / 24

Device Profile Cisco

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret •••••••• Show

Use Second Shared Secret

Second Shared Secret Show

CoA Port 1700 Set To Default

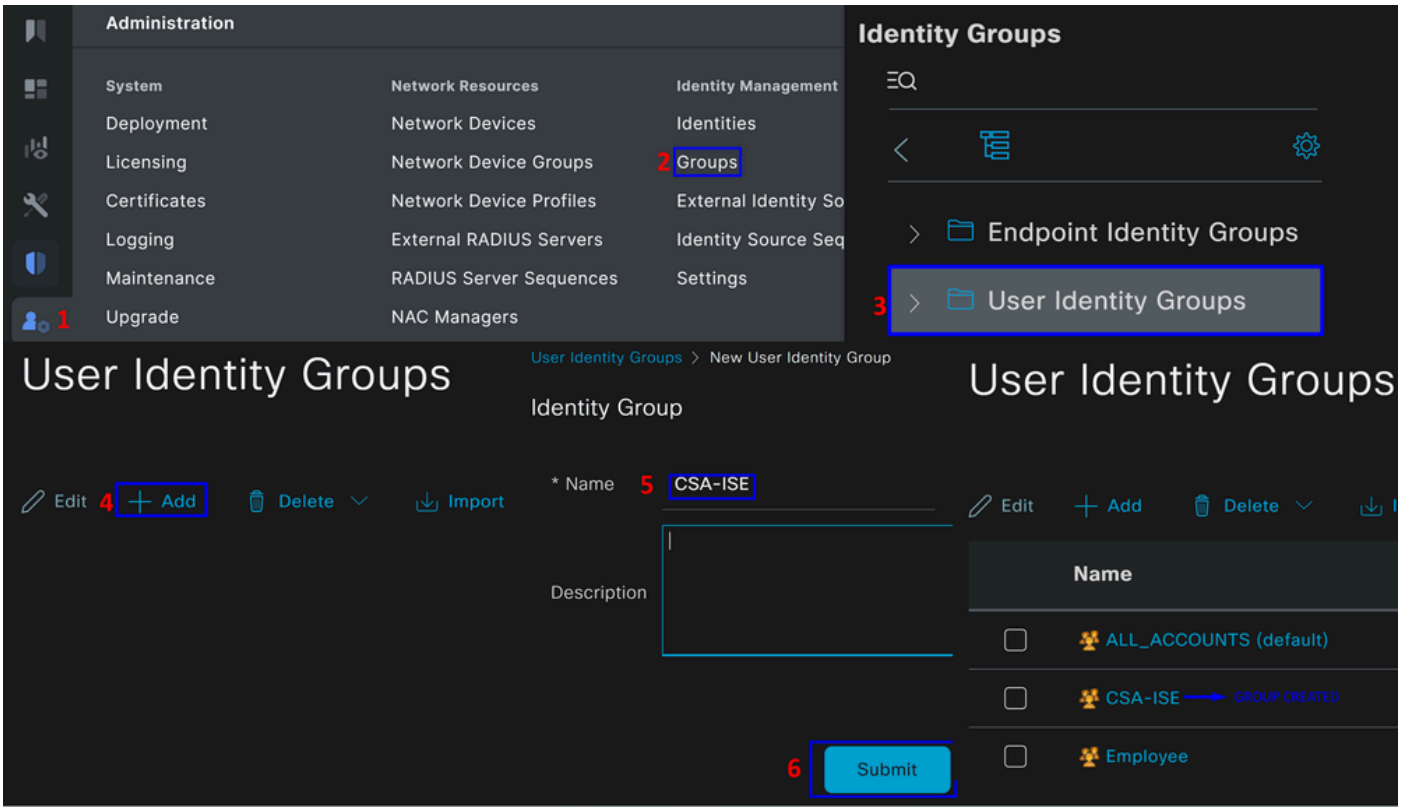
- **Name**: use um nome para identificar o acesso seguro
- **IP Address**: Configure o Management Interface da etapa, Região do pool de IP
- **Device Profile**: Escolha a Cisco
    - **Radius Authentication Settings**
        - Shared Secret: Configure o mesmo segredo compartilhado configurado na etapa, Chave secreta
        - **CoA Port**: Deixe como padrão; 1700 também é usado no acesso seguro

Após clicar em **Save**, para verificar se a integração funciona corretamente, continue para criar um usuário local para verificação da integração.

Configurar um grupo

Para configurar um grupo para uso com usuários locais, siga estas etapas:

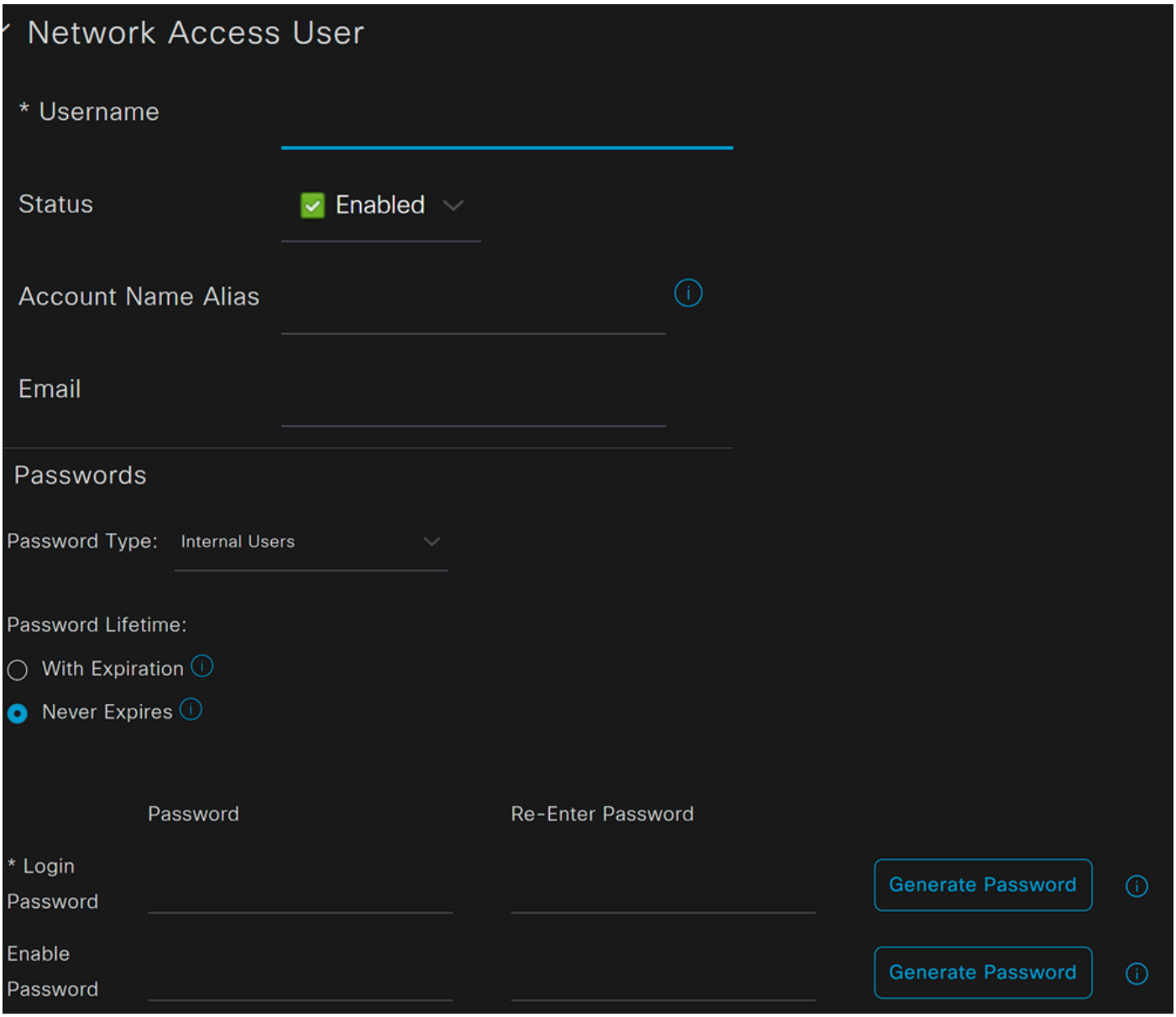
- Clique em **Administration > Groups**
- Clique em **User Identity Groups**
- Clique em + Add
- Crie um Namepara o grupo e clique em **Submit**

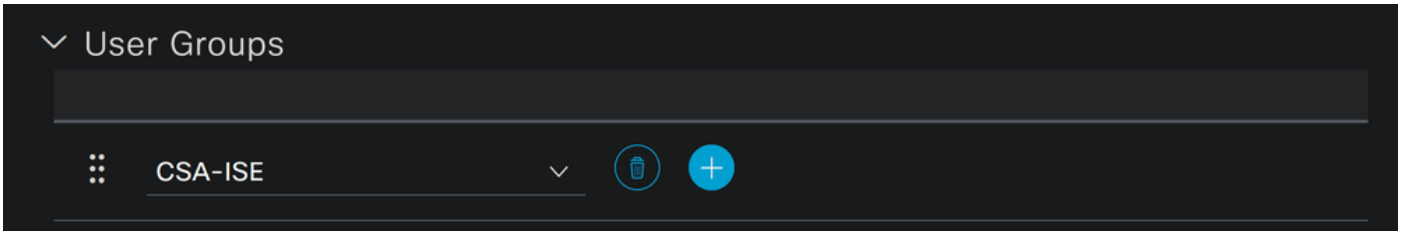


Configurar Usuário Local

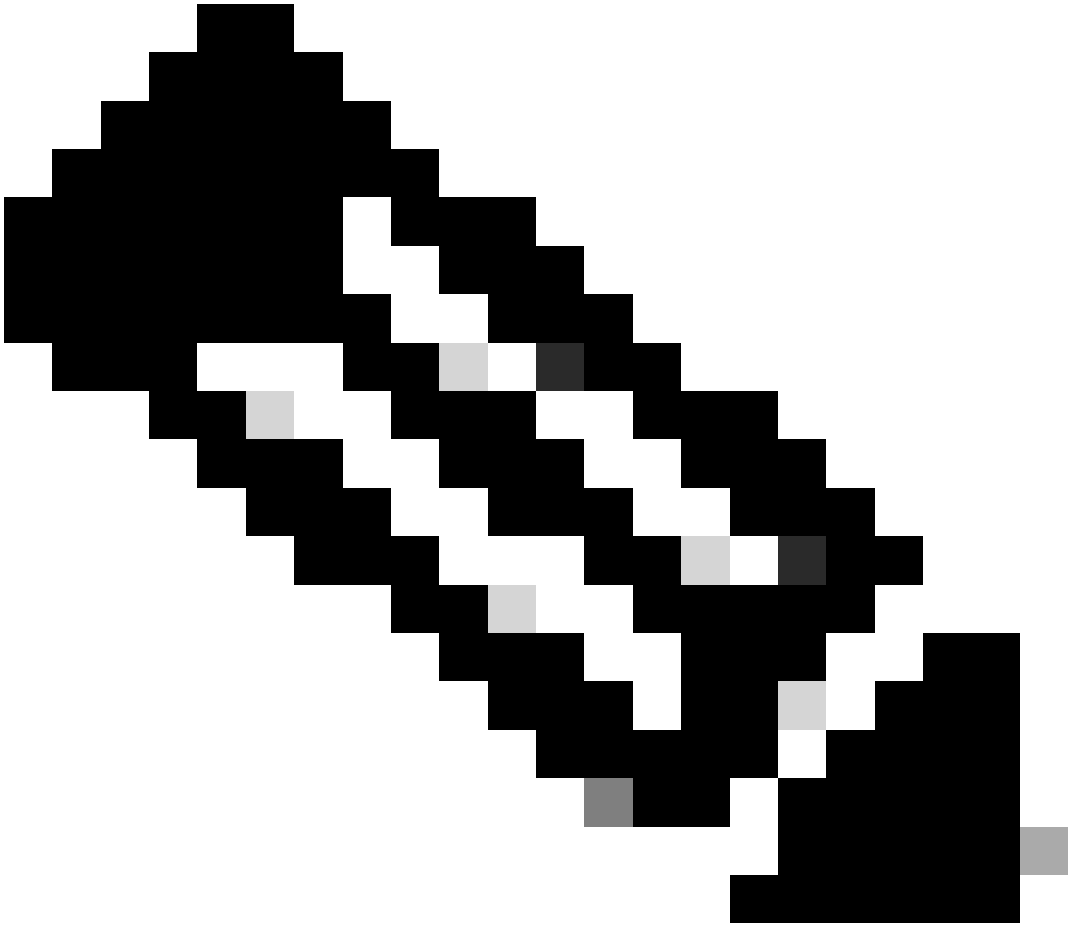
Para configurar um usuário local para verificar sua integração:

- Navegue até **Administration > Identities**
- Clique em **Add +**





- **Username**: Configure o nome de usuário com um provisionamento UPN conhecido no Secure Access; isso se baseia na etapa Pré-requisitos
- **Status**:Ativo
- **Password Lifetime**: Você pode configurá-lo **With Expiration** ou Never Expires, dependendo de você
- **Login Password**: criar uma senha para o usuário
- **User Groups**: Escolha o grupo criado na etapa, Configurar um grupo



Observação: a autenticação baseada em UPN está definida para alteração nas versões futuras do Secure Access.

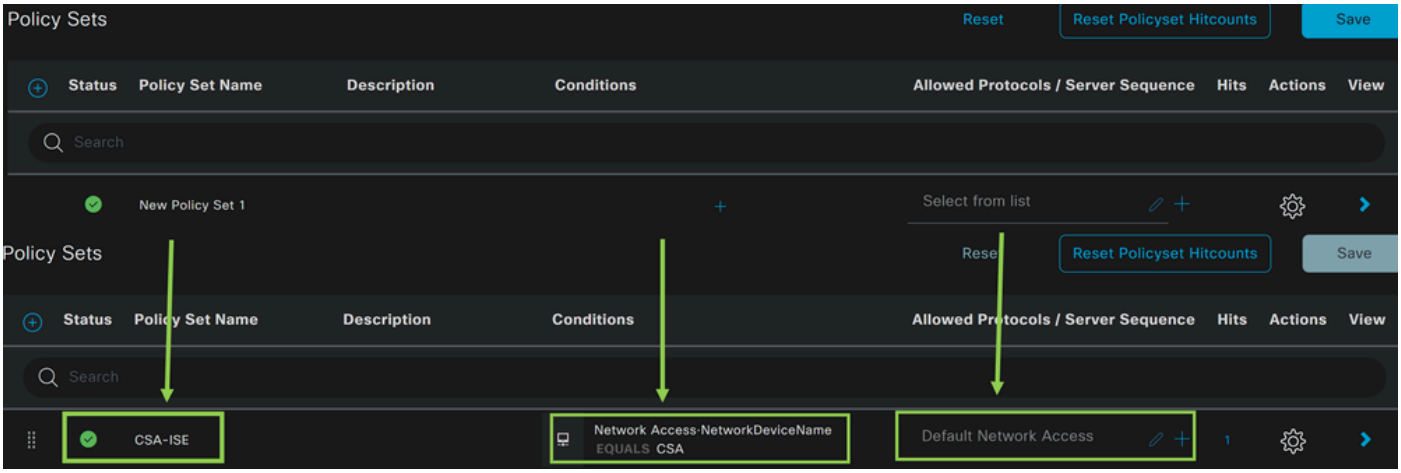
Depois disso, você poderá **Save** fazer a configuração e continuar com a etapa, **Configure Policy Set**.

Configurar Conjunto de Políticas

No conjunto de políticas, configure a ação que o ISE executa durante a autenticação e a autorização. Este cenário demonstra o caso de uso para configurar uma política simples para fornecer acesso ao usuário. Primeiro, o ISE verifica a origem das autenticações RADIUS e se as identidades existem no banco de dados de usuários do ISE para fornecer acesso

Para configurar essa política, navegue até o painel do Cisco ISE:

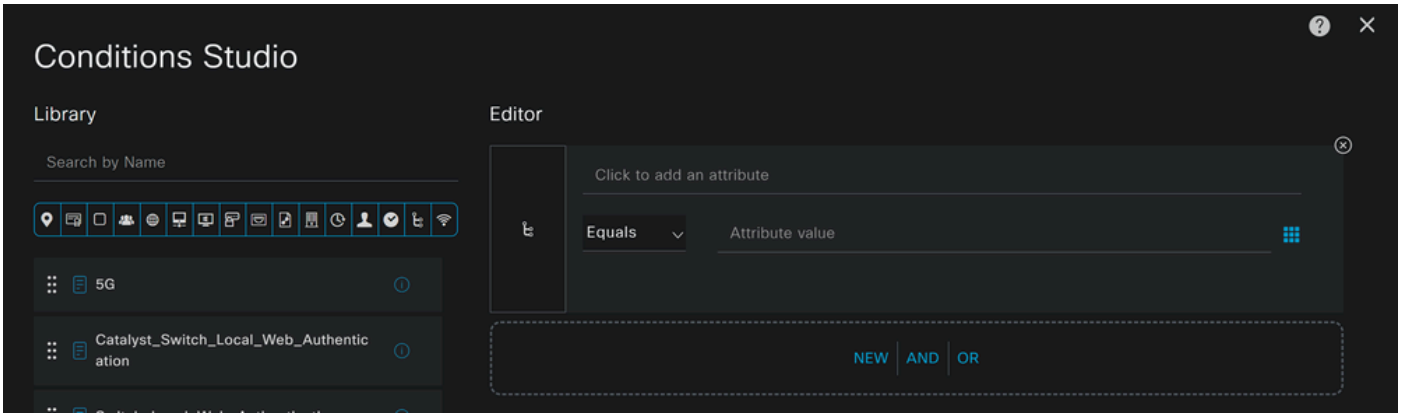
- Clique em Policy > Policy Sets
- Clique em + para adicionar um novo conjunto de políticas



Nesse caso, crie um novo conjunto de políticas em vez de trabalhar com o padrão. Em seguida, configure a Autenticação e Autorização com base nesse conjunto de políticas. A política configurada permite o acesso ao dispositivo de rede definido na etapa Configurar lista de dispositivos de rede para verificar se essas autenticações vêm CSA Network Device List e, em seguida, entrar na política como **Conditions**. E, finalmente, os protocolos permitidos, como **Default Network Access**.

Para criar o **condition** que corresponde ao conjunto de políticas, continue com as próximas instruções:

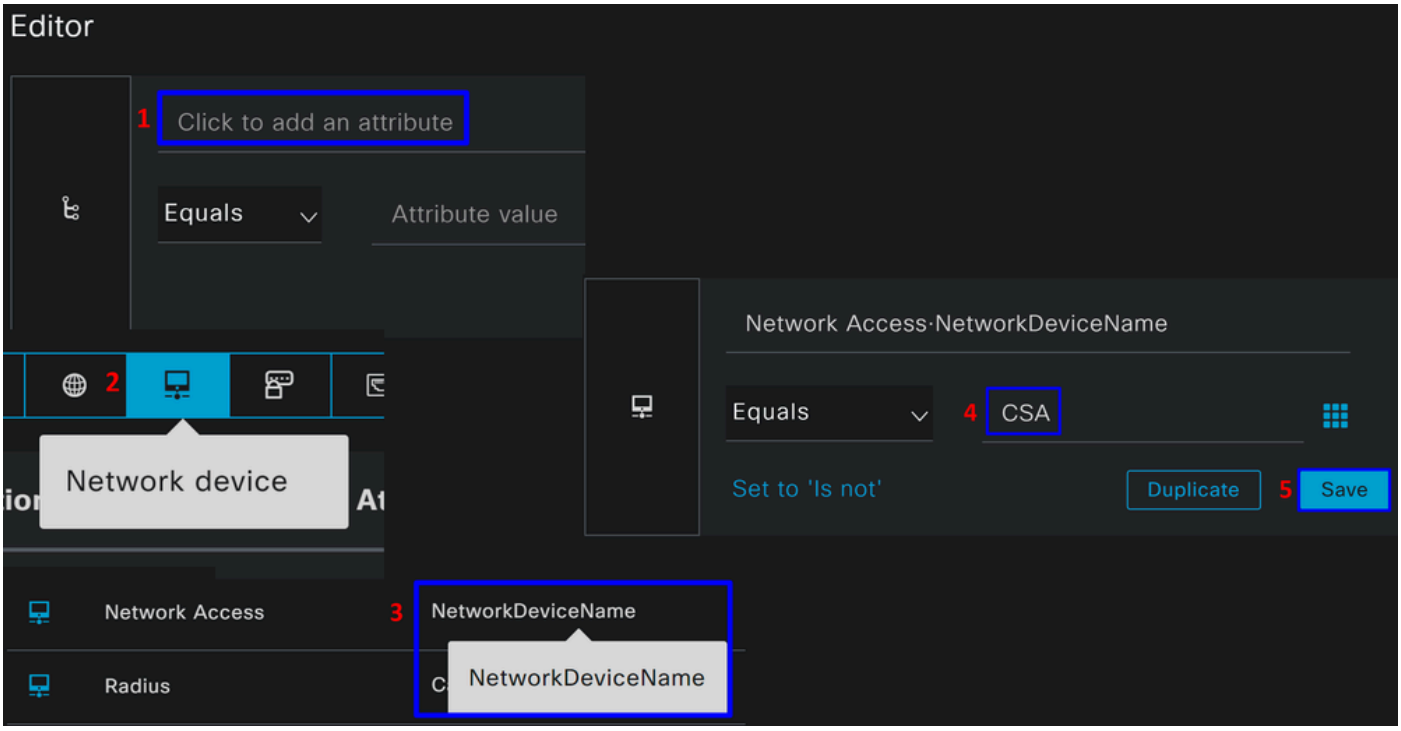
- Clique em +
- Na seção **Condition Studio**, as informações disponíveis incluem:



- Para criar as Condições, clique em Click to add an attribute
- Clique no **Network Device** botão
- Nas opções atrás, clique em **Network Access - Network Device Name** opção
- Na opção Equals (Iguais), escreva o nome do **Network Device** na etapa Configure Network Devices List (Configurar lista de

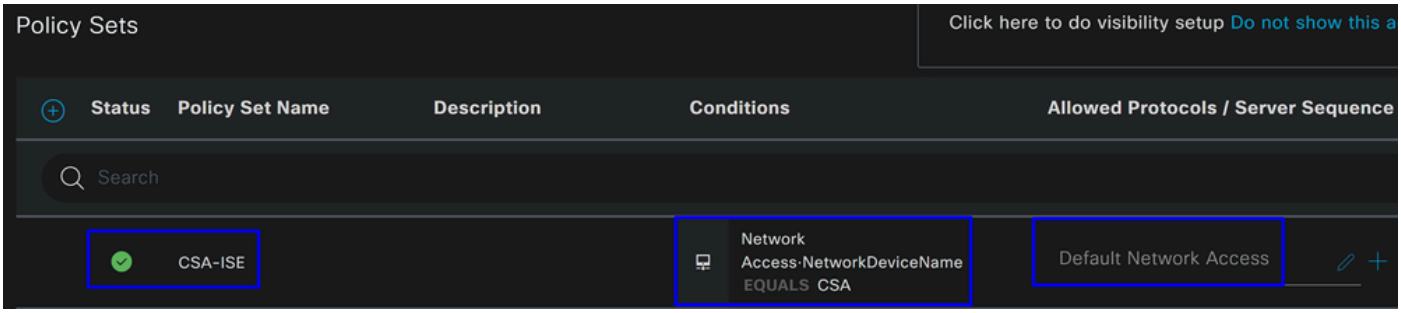
dispositivos de rede)

- Clique em **Save**

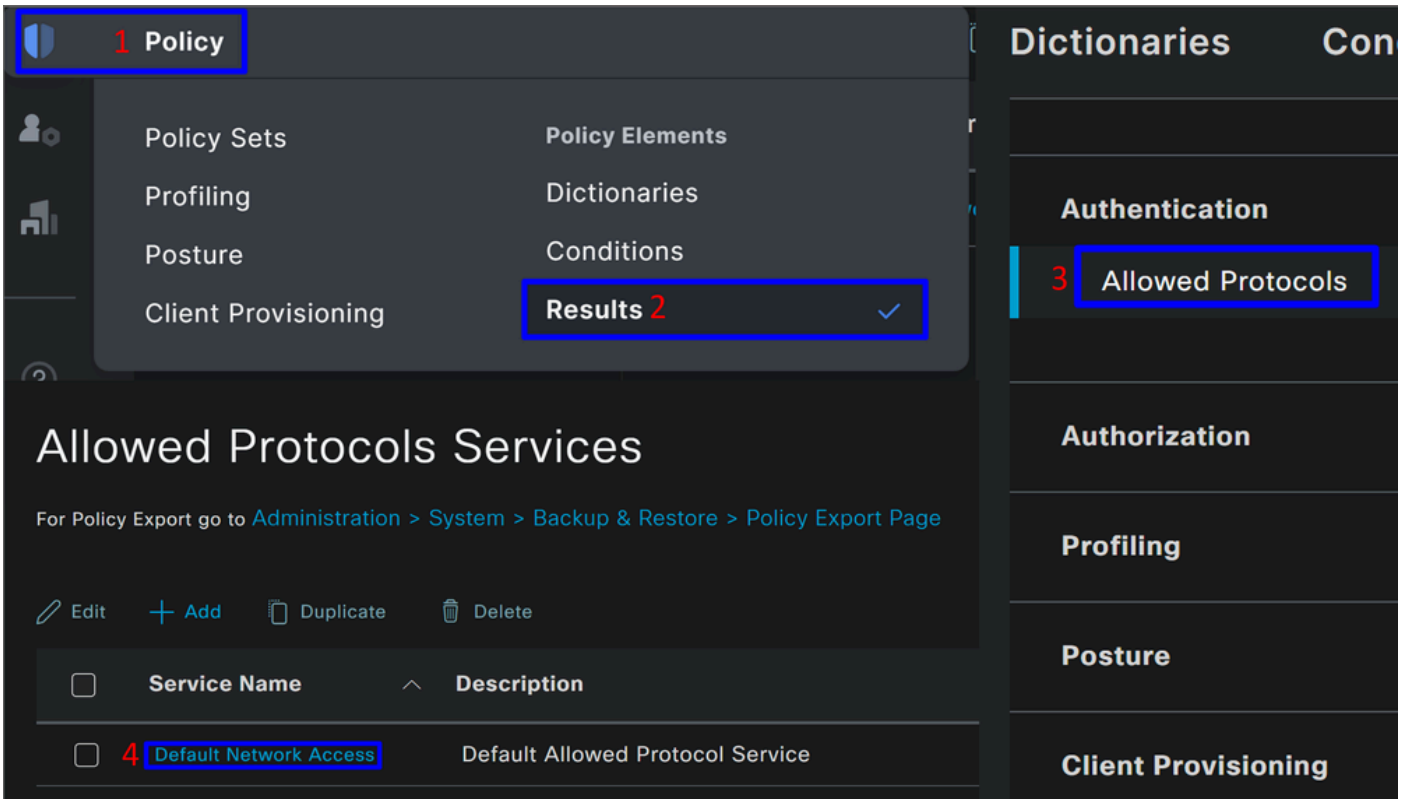


Essa política apenas aprova a solicitação da origem CSA para continuar o **Authentication** e a **Authorization** configuração no conjunto de políticas **CSA-ISE**, e também verifica os protocolos permitidos com base no **Default Network Access** para os protocolos permitidos.

O resultado da política definida deve ser:



- Para verificar o **Default Network Access Protocols** permitido, continue com as próximas instruções:
  - Clique emPolicy > Results
    - Clique em **Allowed Protocols**
    - Clique em **Default Network Access**

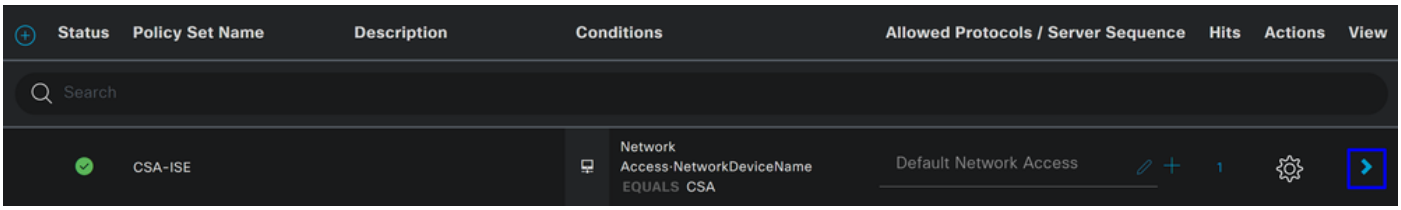


- Em seguida, você verá todos os protocolos permitidos em **Default Network Access**

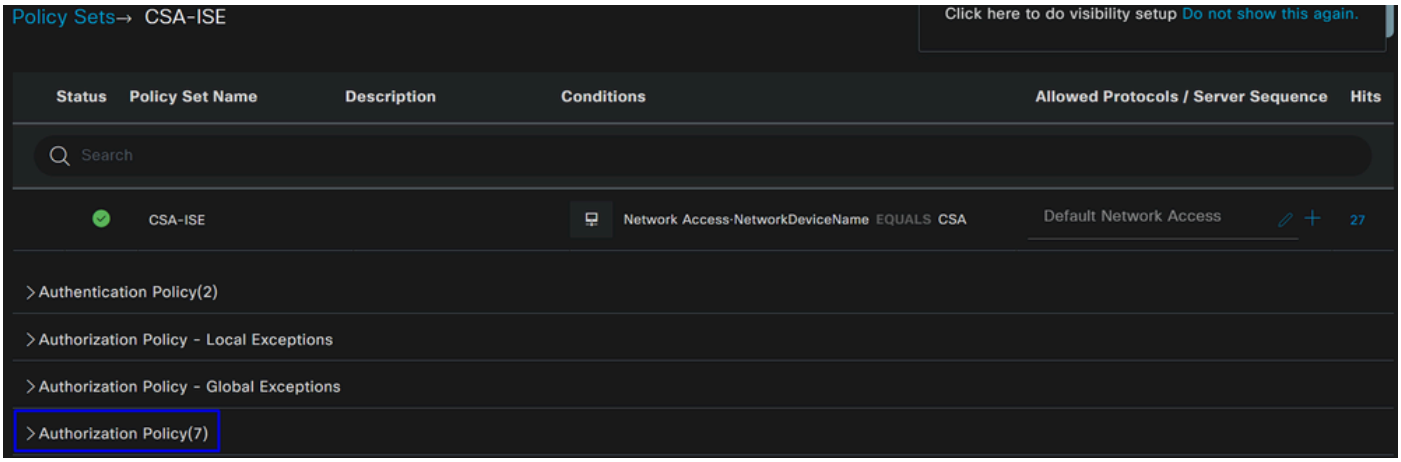
Configurar Autorização de Definição de Política

Para criar a **Authorization** política na **Policy Set**, siga as próximas etapas:

- Clique em >



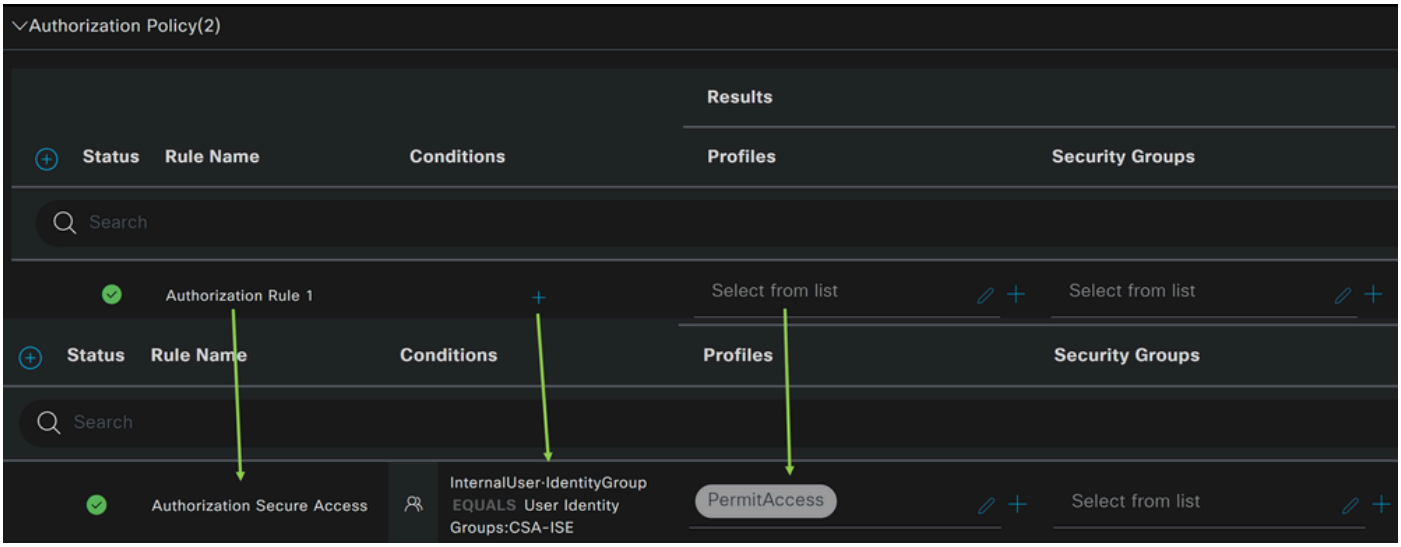
- Depois disso, você verá **Authorization** as políticas exibidas:



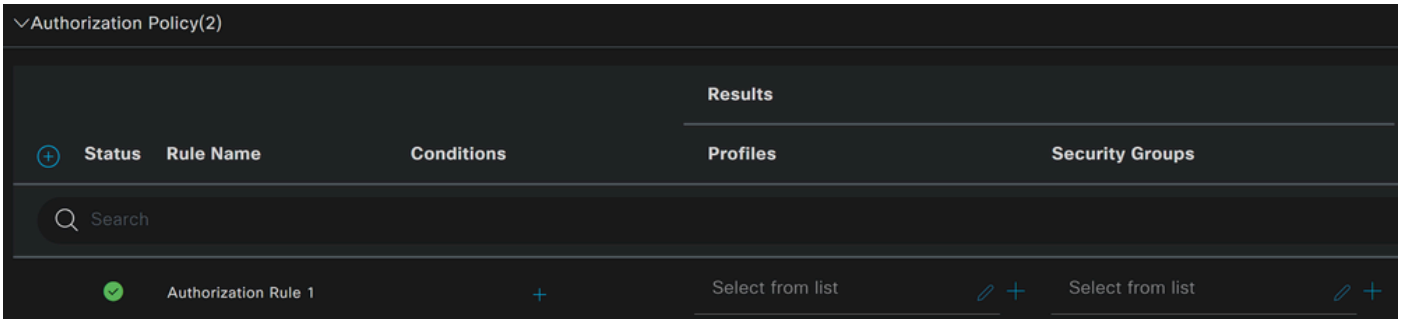
A política é a mesma definida na etapa Configure Policy Set.

Política de Autorização

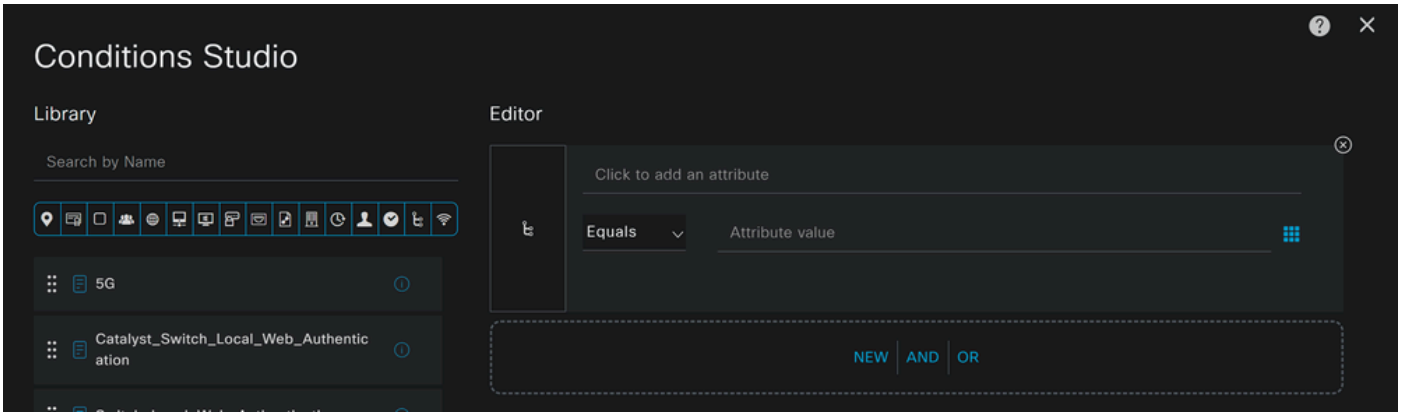
Você pode configurar a política de autorização de várias maneiras. Nesse caso, autorize apenas os usuários no grupo definido na etapa Configurar um Grupo.Consulte o próximo exemplo para configurar sua política de autorização:



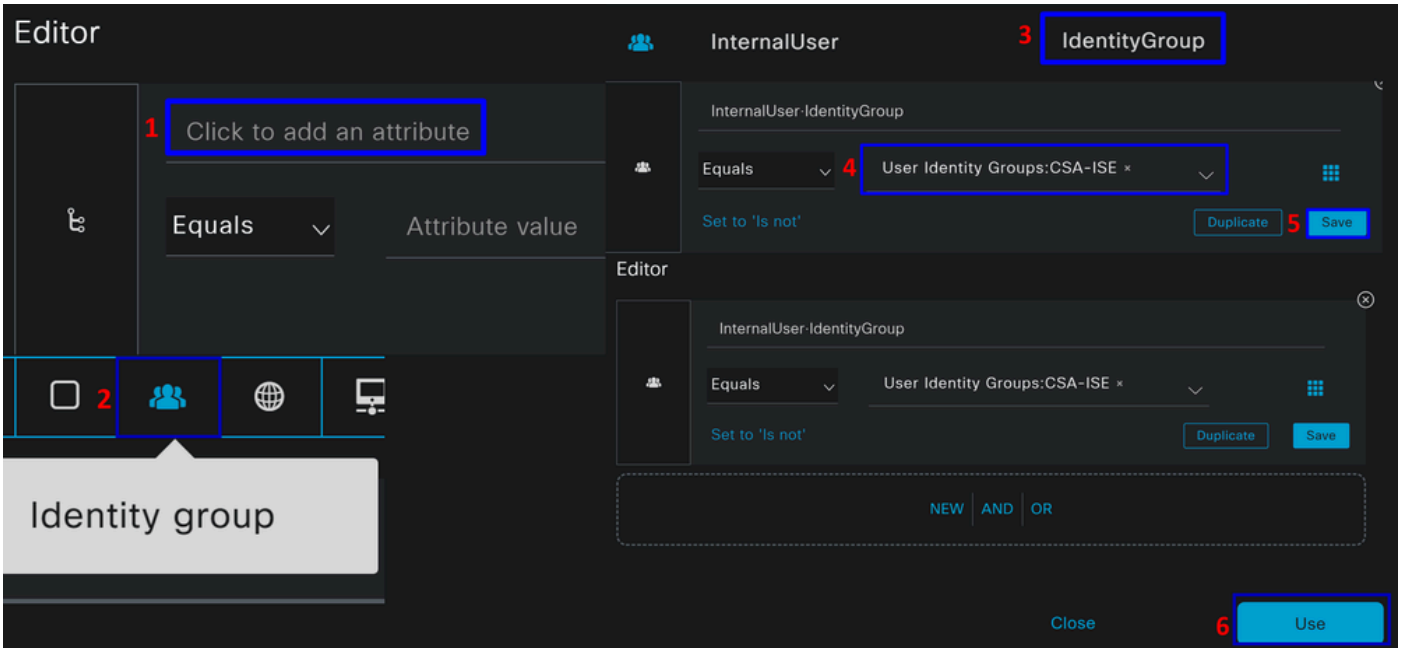
- Clique em **Authorization Policy**
- Clique em + para definir a política de autorização da seguinte forma:



    - Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a **Name** configuração de um nome para identificar facilmente a política de autorização
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:

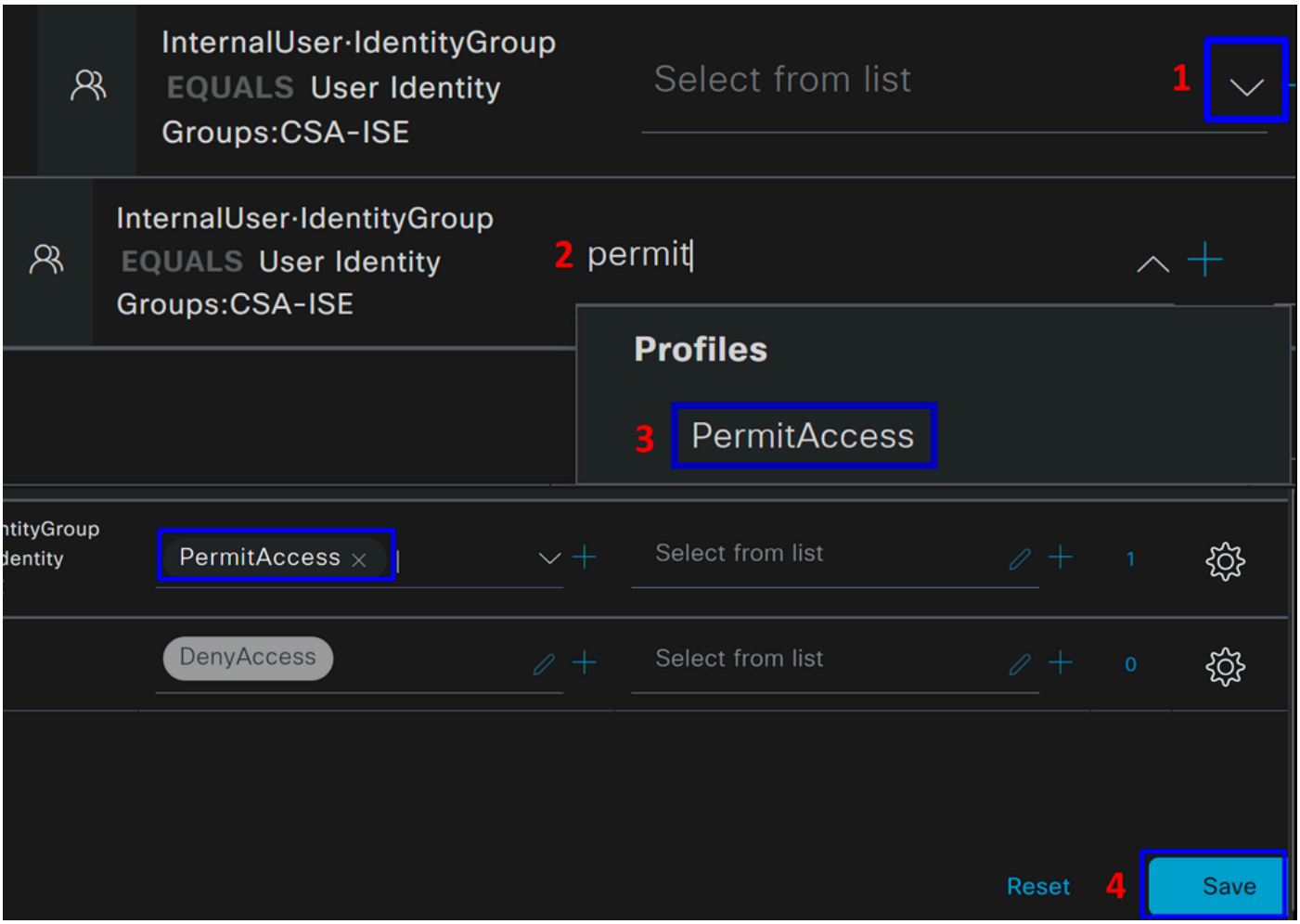


- Para criar as Condições, clique em Click to add an attribute
- Clique no **Identity Group** botão
- Nas opções atrás, clique em **Internal User - IdentityGroup** opção
- Na **Equals** opção, use o menu suspenso para localizar o **Group** aprovado para autenticação na etapa, [Configurar um grupo]
- Clique em **Save**
- Clique em **Use**



Depois disso, você precisa definir o **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Na **Authorization Policy**, clique no botão suspenso em **Profiles**
- Procurar permissão
- Selecionar **PermitAccess**
- Clique em Save

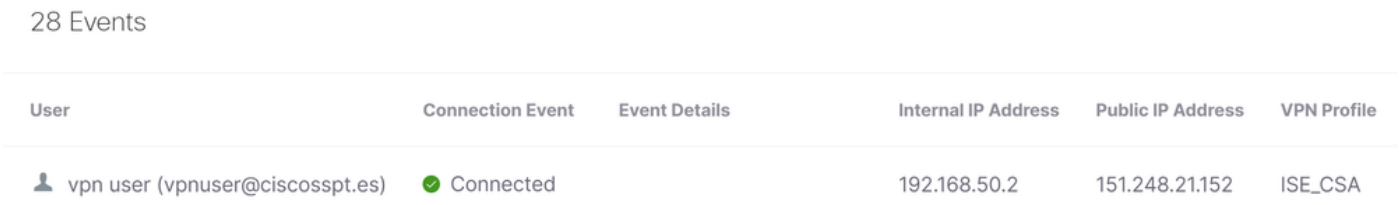


Depois disso, você definiu sua **Authorization** política. Autentique para verificar se o usuário se conecta sem problemas e se você pode ver os logs no Secure Access e no ISE.

Para se conectar à VPN, você pode usar o perfil criado no Secure Access e conectar-se através do Secure Client com o perfil do ISE.

- **Como o registro é exibido no Secure Access quando a autenticação é aprovada?**
  - Navegue até o Painel do Secure Access

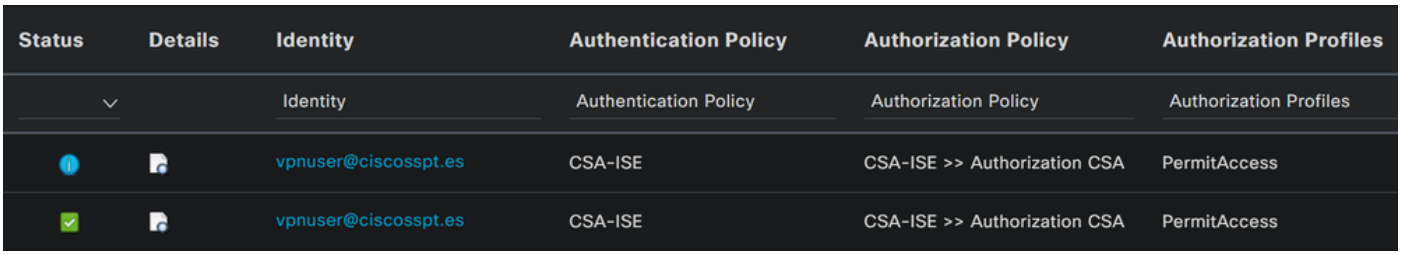
- Clique em **Monitor > Remote Access Log**



- **Como o registro é exibido no ISE quando a autenticação é aprovada?**

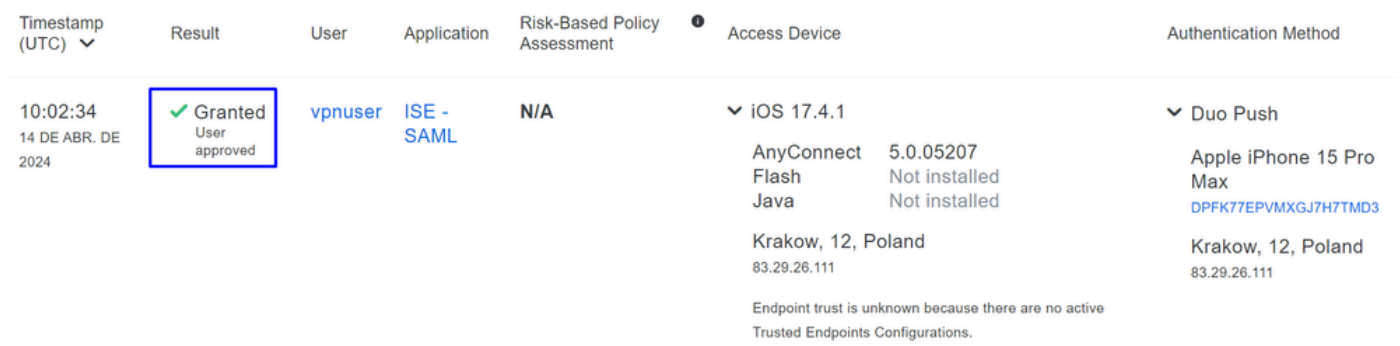
  - Navegue até a página **Cisco ISE Dashboard**

    - Clique em **Operations > Live Logs**



Como o registro é exibido no Duo quando a autenticação é aprovada?

- Navegue até o painel de administração do Duo
- Clique em **Reports > Authentication Log**



Configurar usuários locais ou do Ative Diretory do Radius

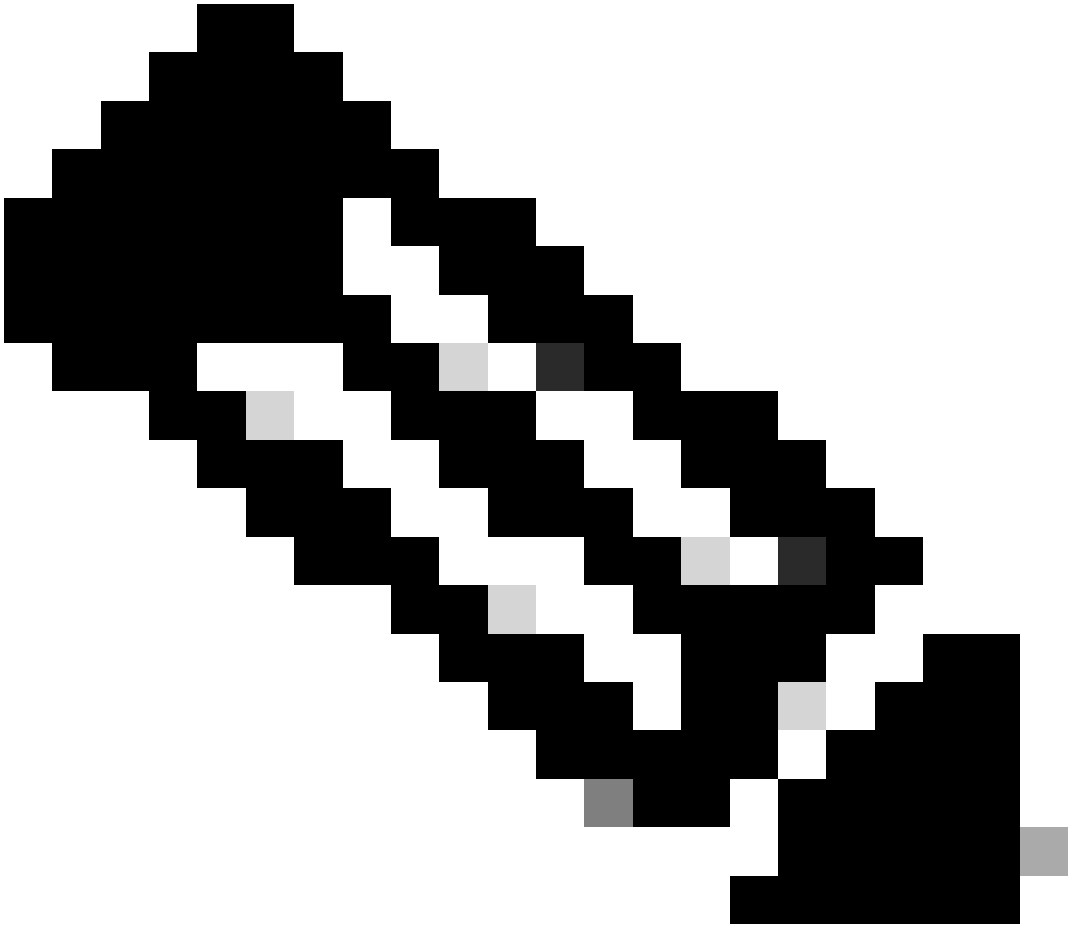
Configurar a postura do ISE

Neste cenário, crie a configuração para verificar a conformidade do endpoint antes de conceder ou negar acesso a recursos internos.

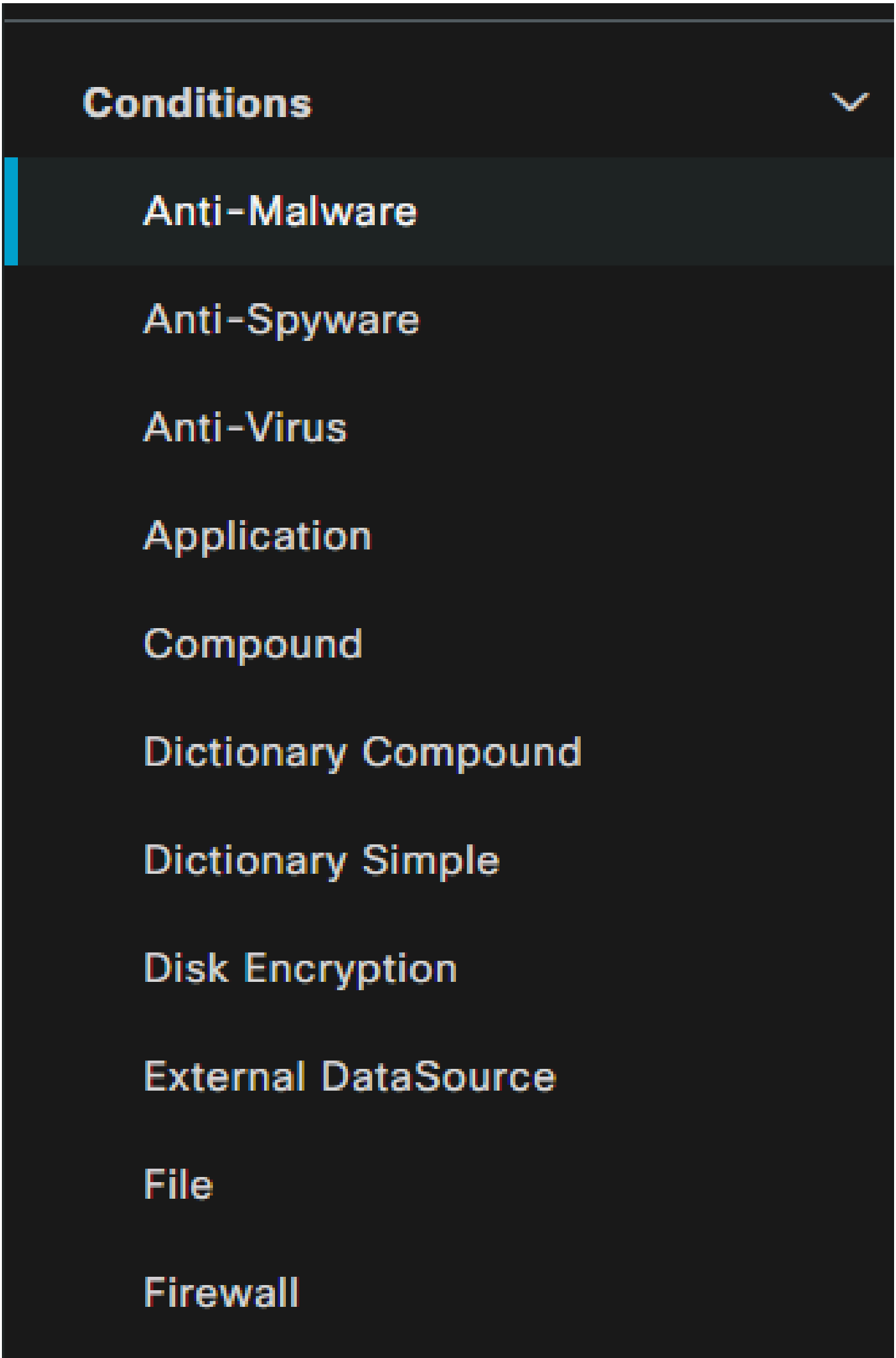
Para configurá-lo, siga para as próximas etapas:

Configurar Condições de Postura

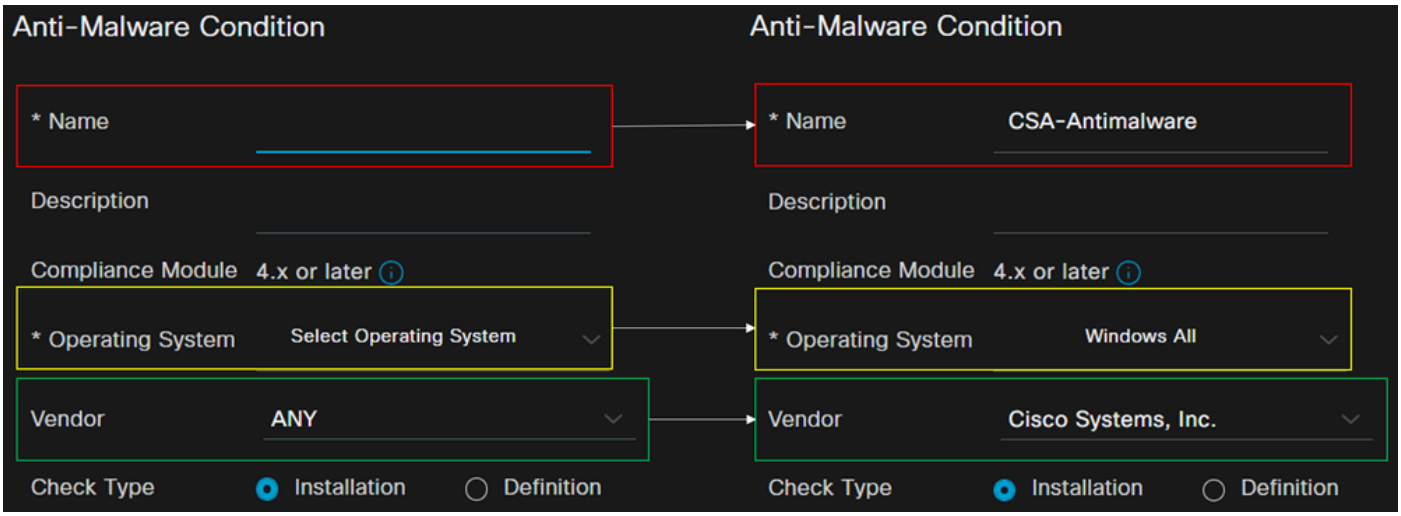
- Navegue até o painel do ISE
- Clique em **Work Center > Policy Elements > Conditions**
- Clique em **Anti-Malware**



Observação: lá, você encontrará muitas opções para verificar a postura de seus dispositivos e fazer a avaliação correta com base em suas políticas internas.

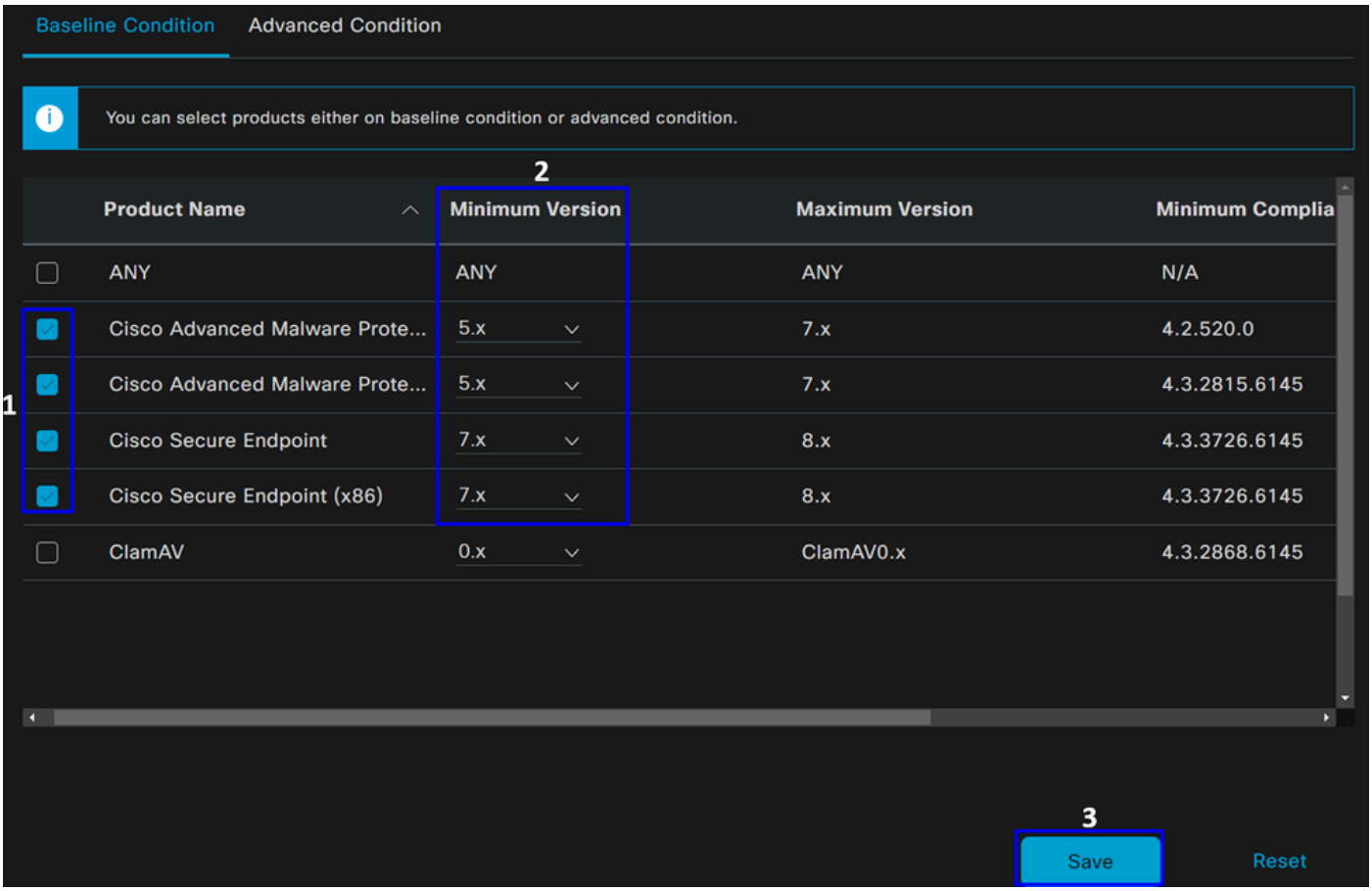

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

Anti-Malware Condition para detectar a instalação do antivírus no sistema; você também pode escolher a versão do sistema operacional, se necessário.



- **Name**: use um nome para reconhecer a condição antimalware
- **Operating System**: escolha o sistema operacional que você deseja colocar sob a condição
- **Vendor**: Escolha um fornecedor ou QUALQUER UM
- **Check Type**: você pode verificar se o agente está instalado ou a versão de definição para essa opção.

- Por **Products for Selected Vendor**exemplo, você configura o que deseja verificar sobre o antimalware no dispositivo.

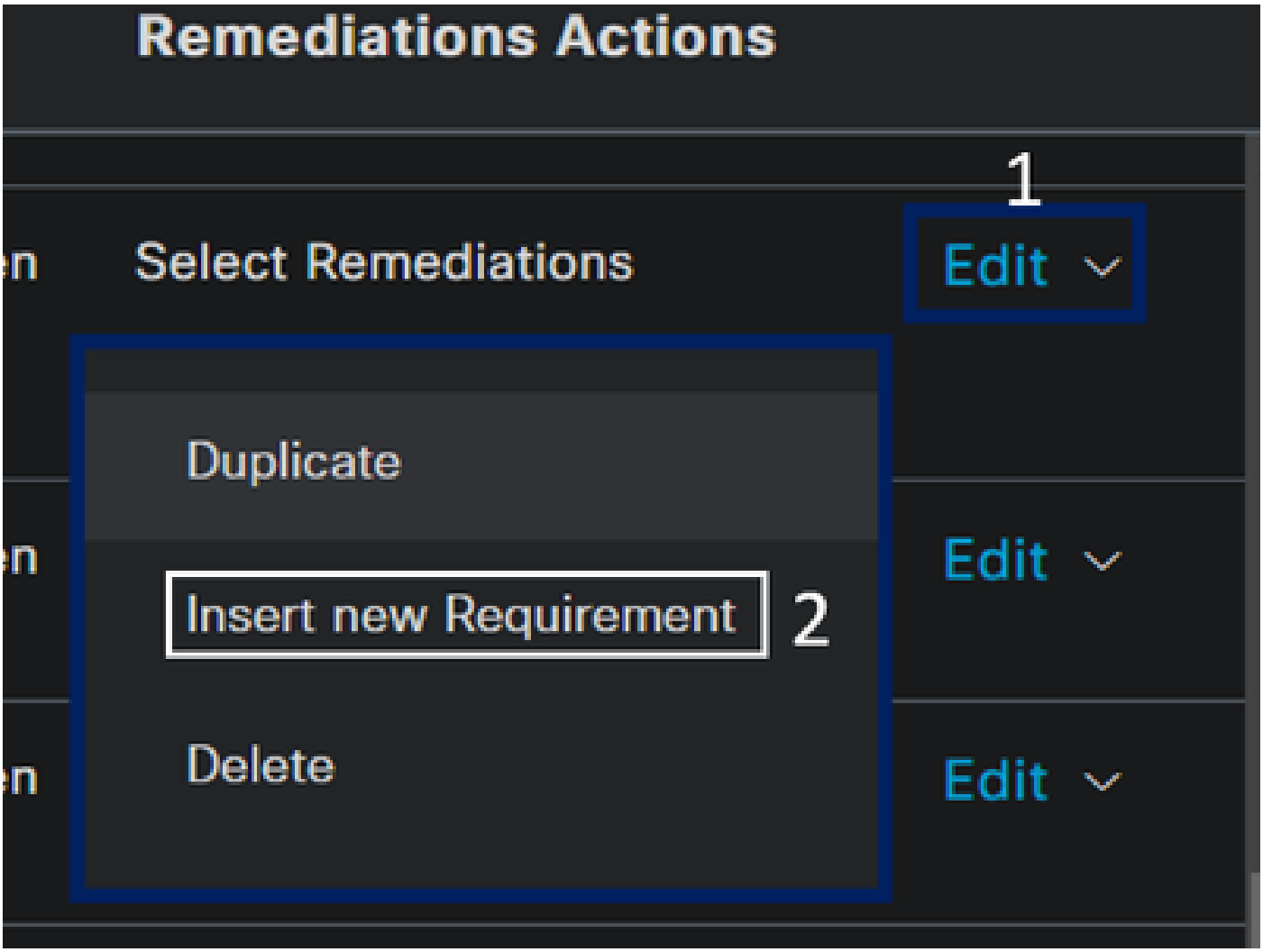


- Marque a caixa de seleção das condições que você deseja avaliar
- Configurar a versão mínima a ser verificada
- Clique em Salvar para continuar com a próxima etapa

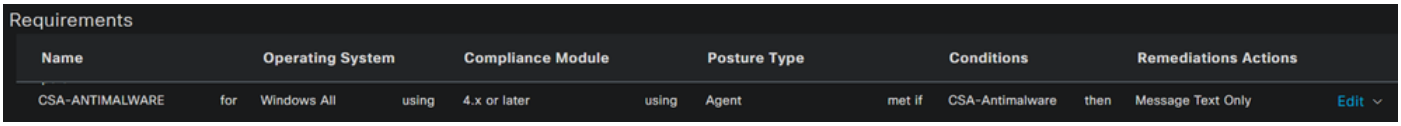
Depois de configurá-lo, você pode prosseguir com a etapa, **Configure Posture Requirements**.

Configurar Requisitos de Postura

- Navegue até o painel do ISE
- Clique em **Work Center > Policy Elements > Requeriments**
- Clique em um **Edit** dos requisitos e clique em **Insert new Requirement**



- Sob o novo requisito, configure os próximos parâmetros:

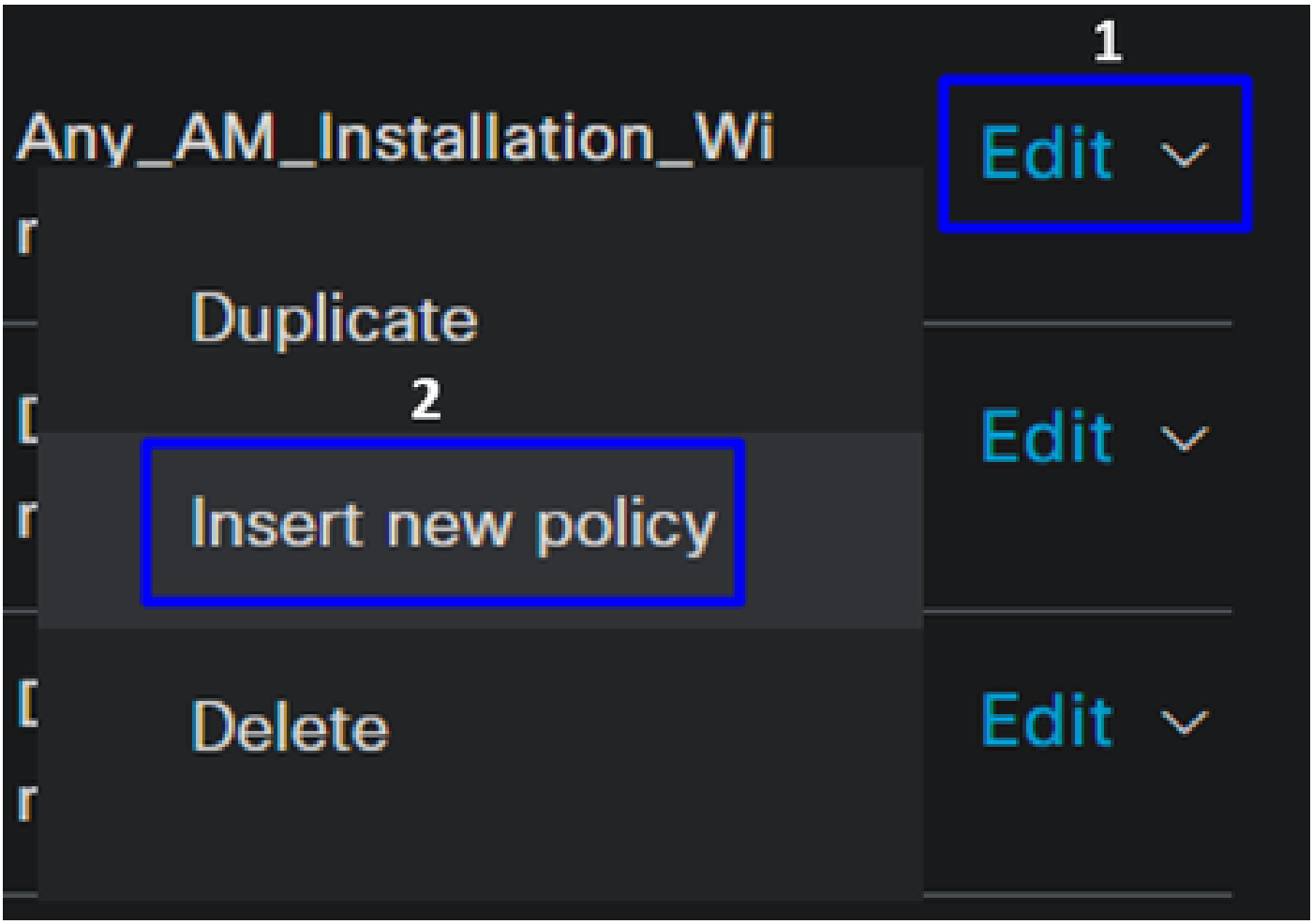


- **Name**: Configure um nome para reconhecer o requisito antimalware
- **Operating System**: Escolha o sistema operacional escolhido na etapa de condição Sistema Operacional
- **Compliance Module**: Você precisa certificar-se de selecionar o mesmo módulo de conformidade que você tem sob a etapa de condição, Condição Anti-Malware
- **Posture Type**: Escolher agente
- **Conditions**: Escolha a condição ou condições que você criou na etapa, Configurar Condições de Postura
- **Remediations Actions**: Escolha **Message Text Only** para este exemplo ou se você tiver outra ação de correção, use-a
- Clique em **Save**

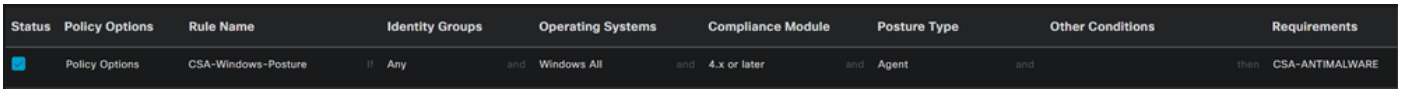
Depois de configurá-lo, você pode prosseguir com a etapa, **Configure Posture Policy**

Configurar política de postura

- Navegue até o painel do ISE
- Clique em **Work Center > Posture Policy**
- Clique em qualquer uma **Edit** das políticas e clique em **Insert new Policy**



- Na nova política, configure os próximos parâmetros:



- **Status**: Marque a caixa de seleção em habilitar a política
- **Rule Name**: Configure um nome para reconhecer a política configurada
- **Identity Groups**: escolha as identidades que deseja avaliar

- **Operating Systems**: Escolha o sistema operacional com base na condição e no requisito configurado antes
- **Compliance Module**: escolha o módulo de conformidade com base na condição e no requisito configurado antes
- Posture Type: Escolher agente
- **Requeriments**: Escolha os requisitos configurados na etapa, Configurar requisitos de postura
- Clique em **Save**

Configurar Provisionamento de Cliente

Para fornecer aos usuários o módulo ISE, configure o provisionamento do cliente para equipar as máquinas com o módulo de postura ISE. Isso permite verificar a postura do computador depois que o agente é instalado. Para continuar com esse processo, estas são as próximas etapas:

Navegue até o painel do ISE.

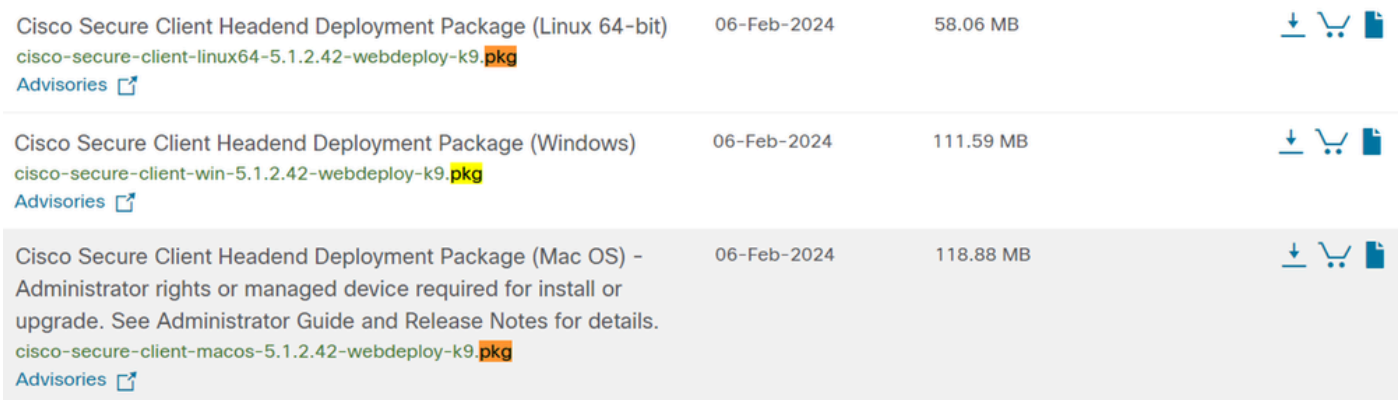
- Clique em **Work Center > Client Provisioning**
- Escolher **Resources**

Há três coisas que você precisa configurar no provisionamento de clientes:

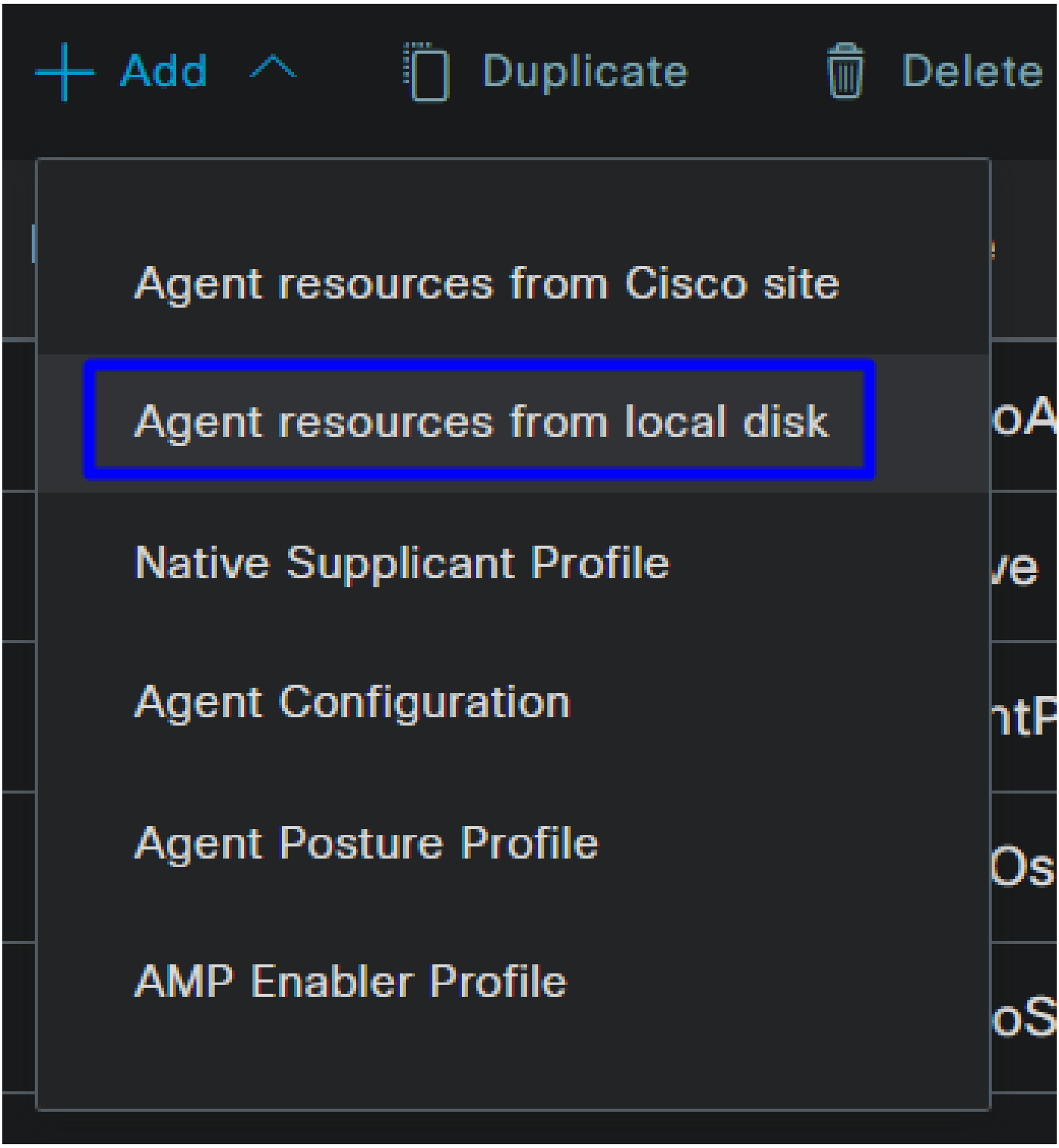
Recursos a serem configurados	Descrição
1. **Agent Resources**	Pacote de Provisionamento da Web para Cliente Seguro.
2. **Compliance Module**	Módulo de conformidade Cisco ISE
3. **Agent Profile**	Controle do perfil de provisionamento.
3. **Agent Configuration**	Defina quais módulos são provisionados configurando o portal de provisionamento, utilizando o Perfil do agente e os Recursos do agente.

Step 1 Fazer download e upload de recursos do agente

- Para adicionar um novo recurso de agente, navegue até o Cisco Download Portal e faça download do pacote de implantação na Web; o arquivo de implantação na Web deve estar no formato .pkg.

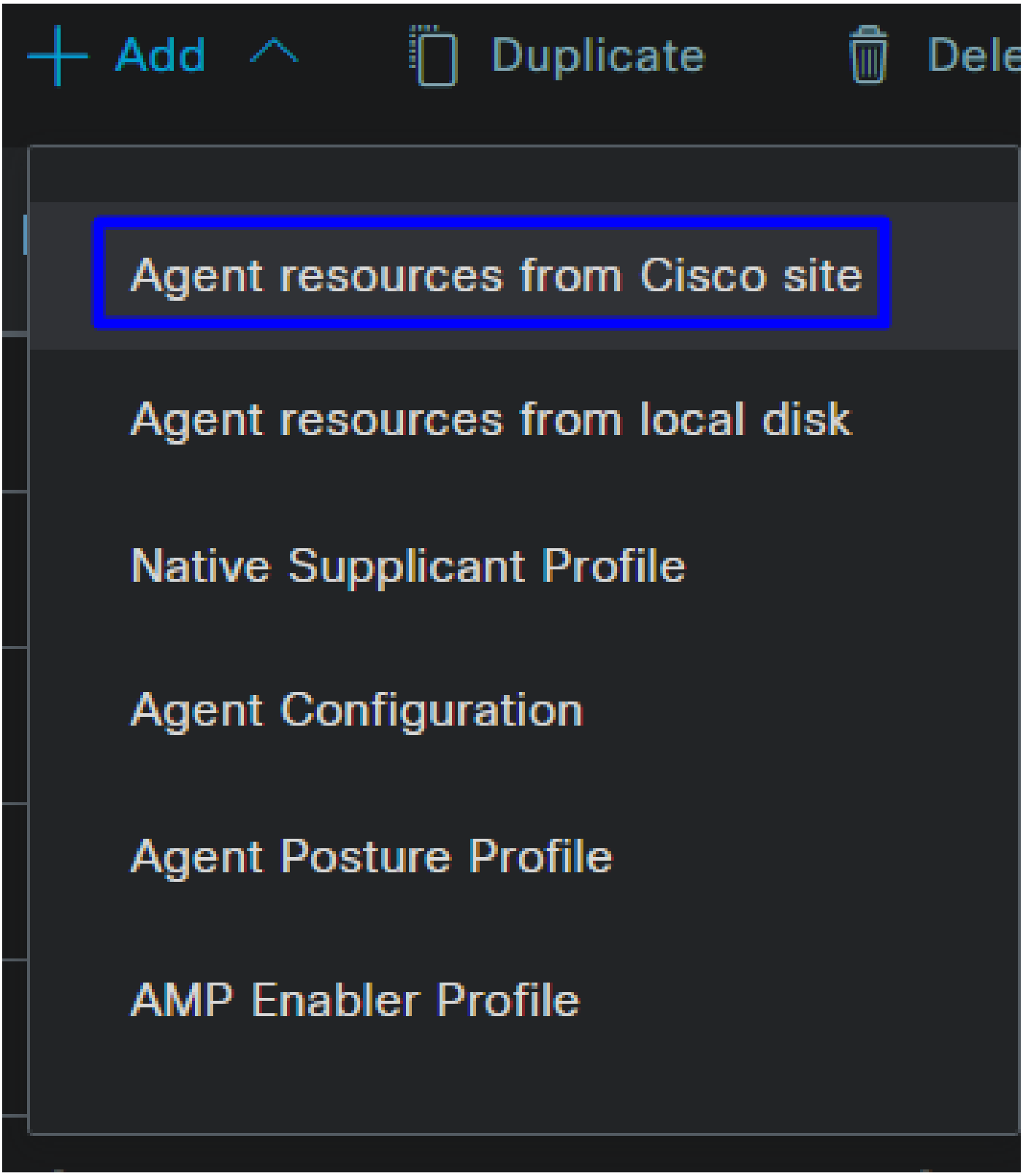


- Clique + Add > Agent resources from local disk e carregue os pacotes

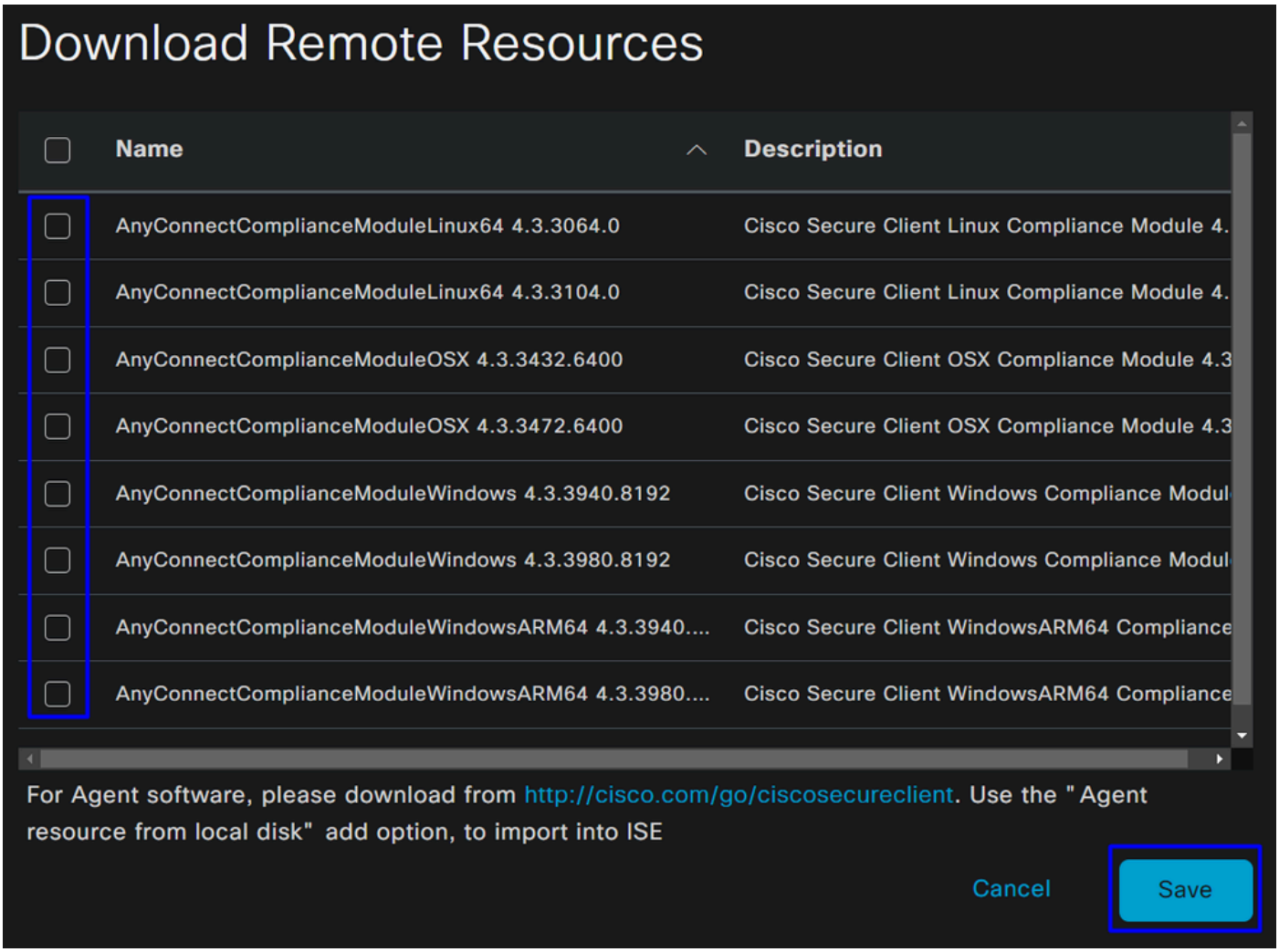


Step 2 Faça o download do módulo de conformidade

- Clique em + Add > Agent resources from Cisco Site

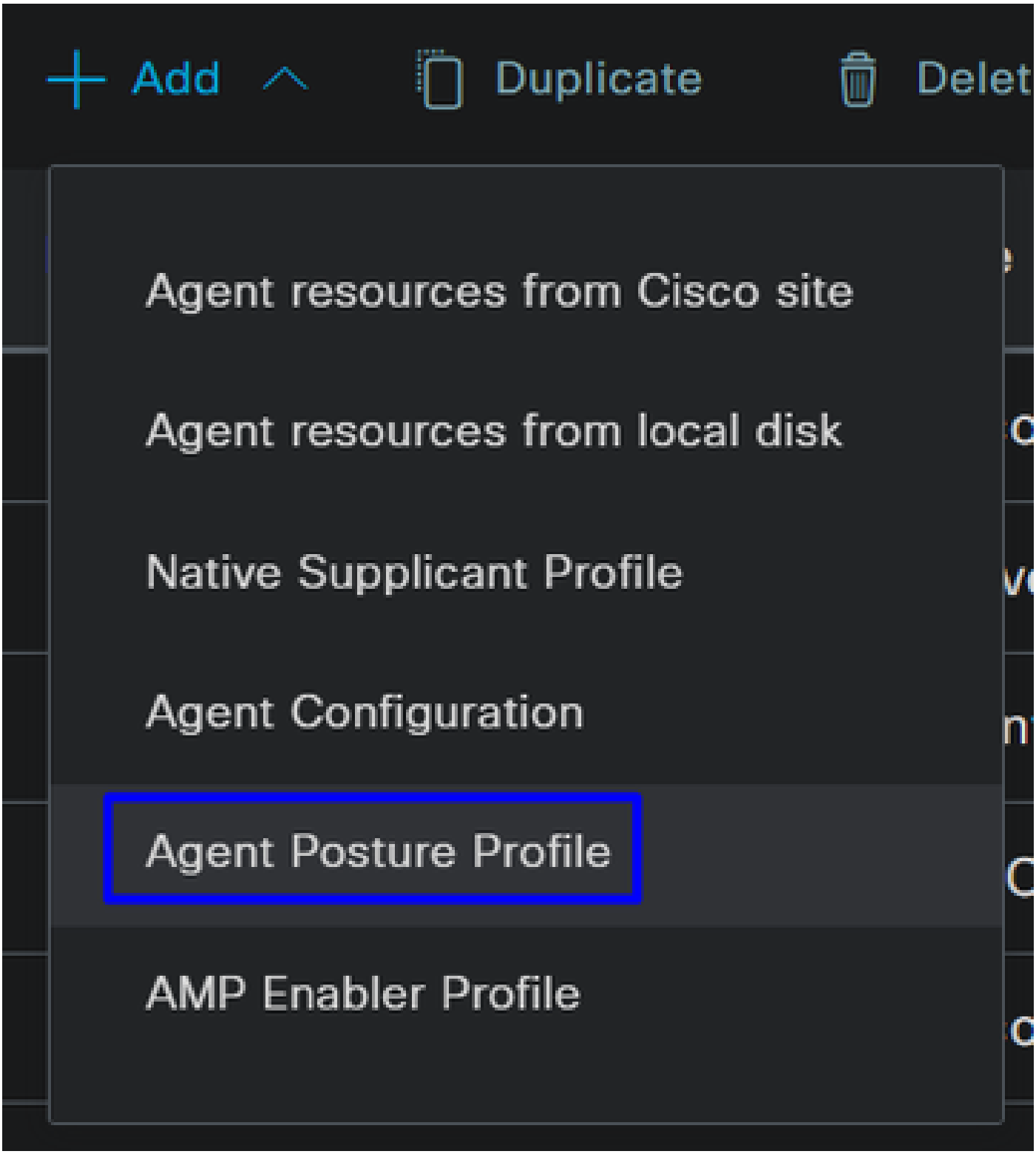


- Marque a caixa de seleção para cada módulo de conformidade necessário e clique em **Save**

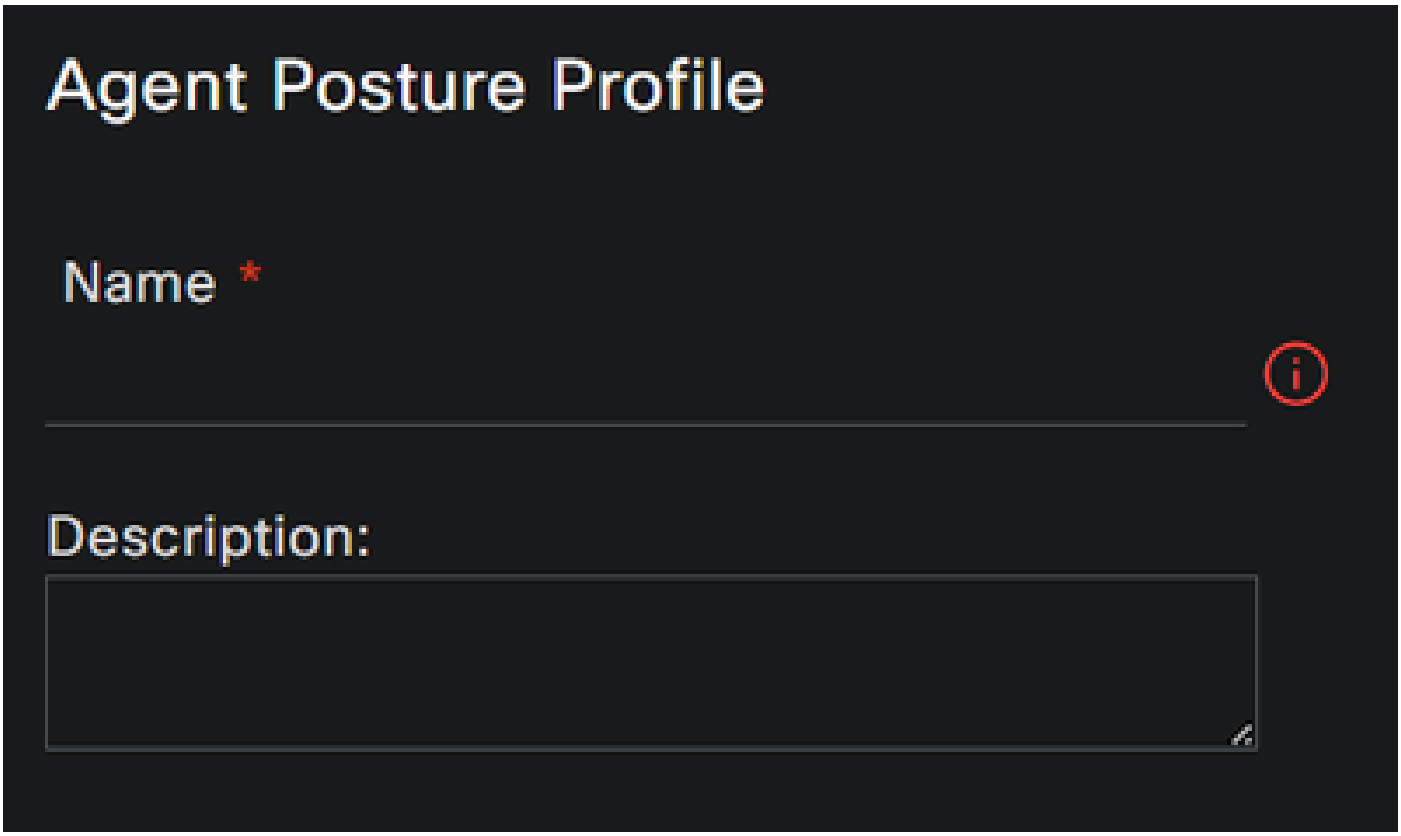


Step 3Configurar o perfil do agente

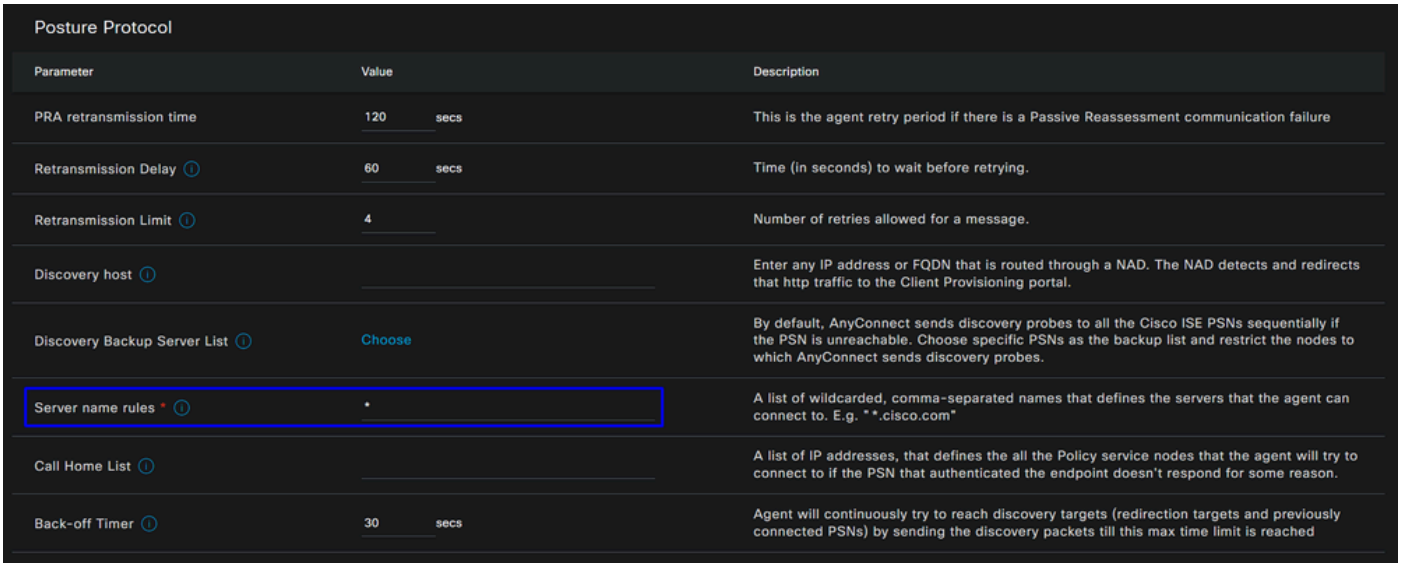
- Clique em + Add > Agent Posture Profile



- Crie um **Name** para o **Posture Profile**

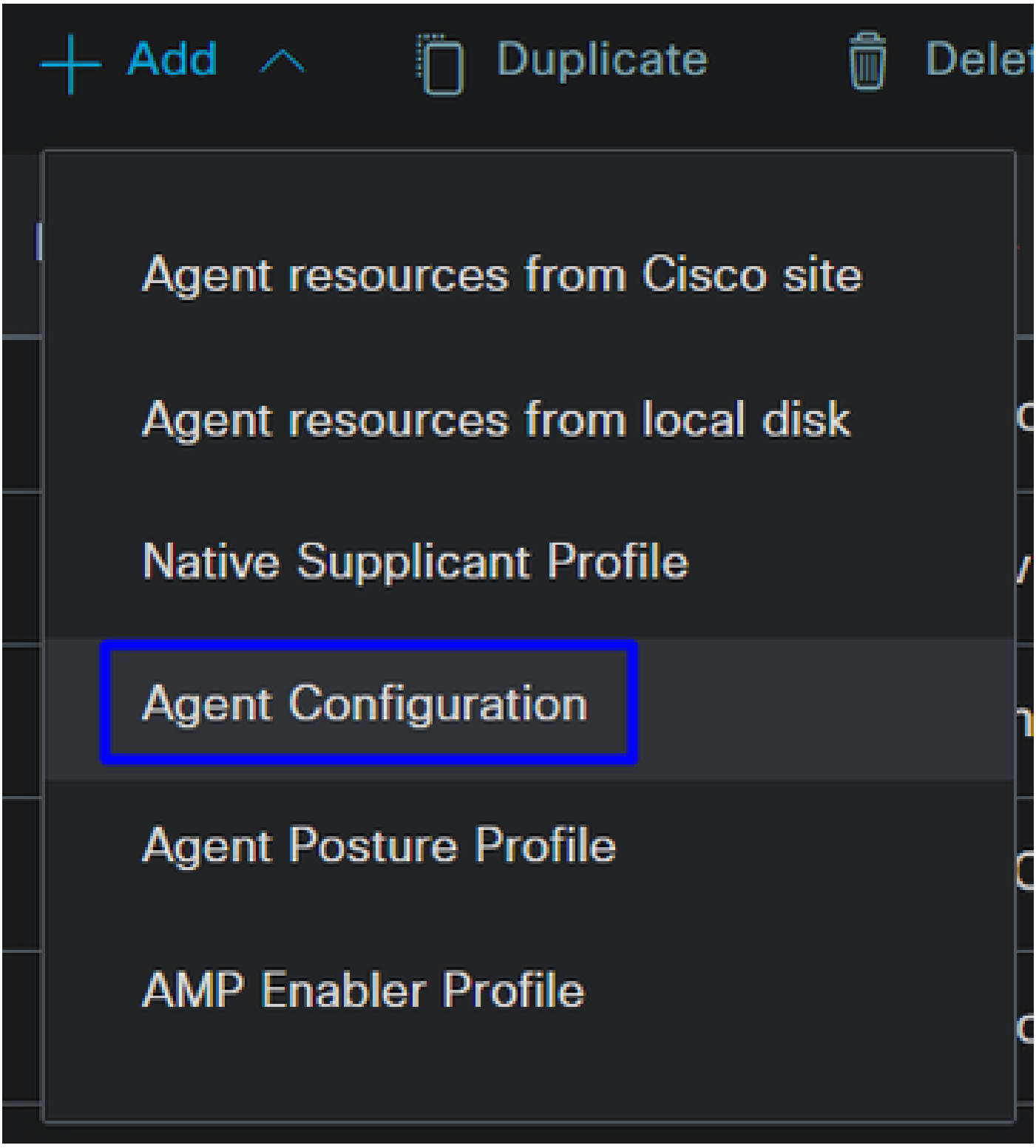


- Em Regras de nome do servidor, coloque um ***** e clique **Save** depois disso

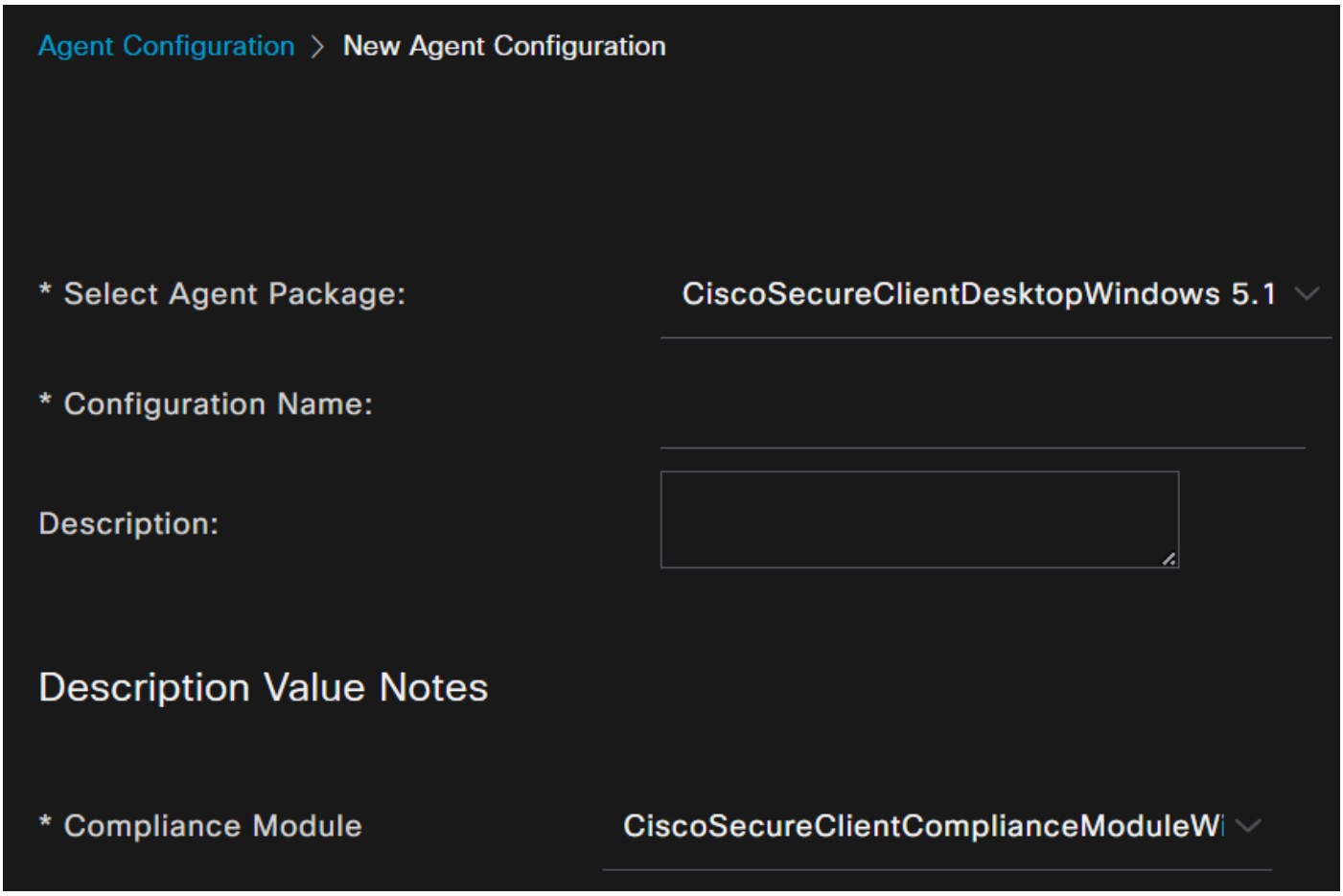


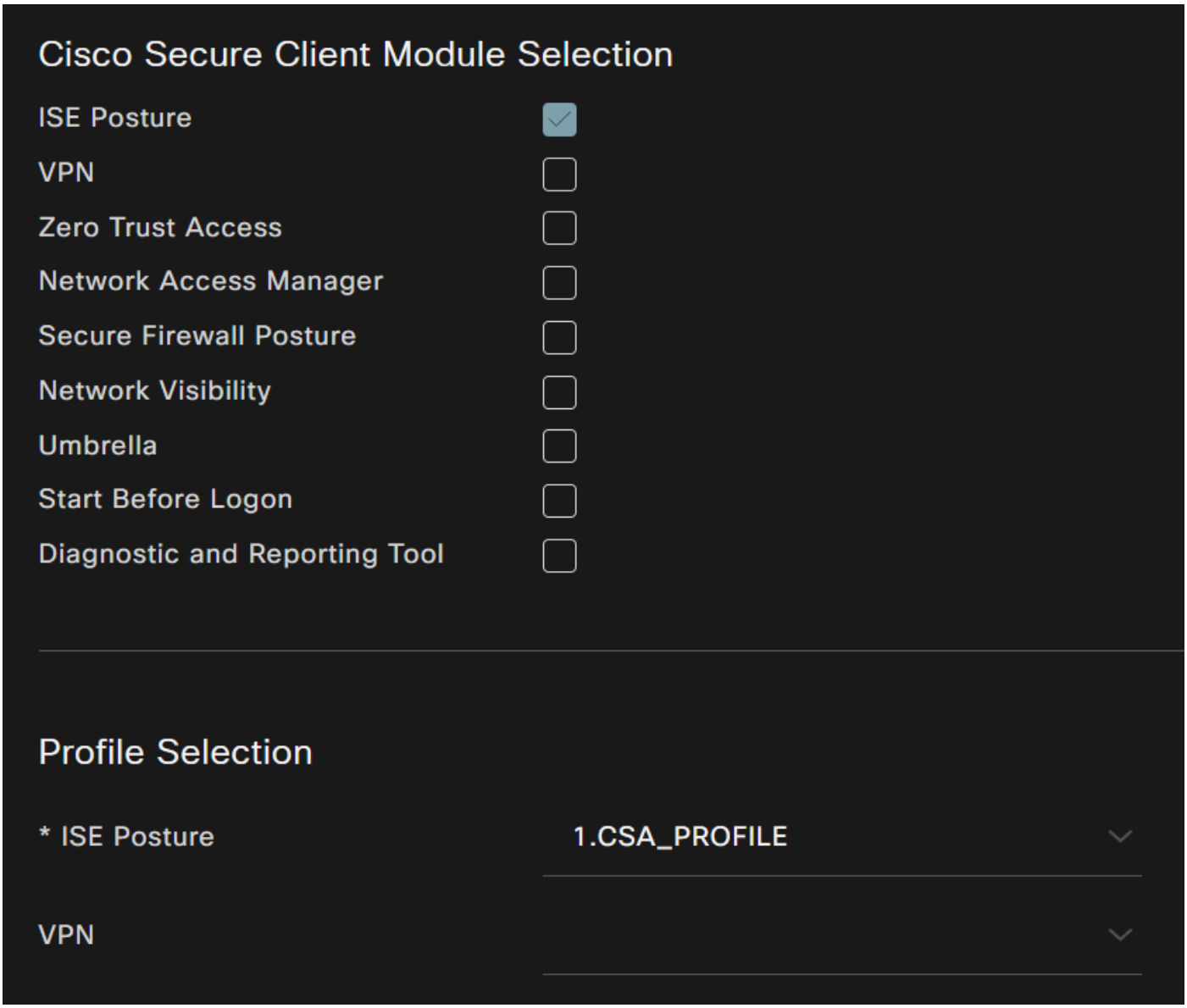
Step 4 Configurar a configuração do agente

- Clique em + Add > Agent Configuration



- Depois disso, configure os próximos parâmetros:

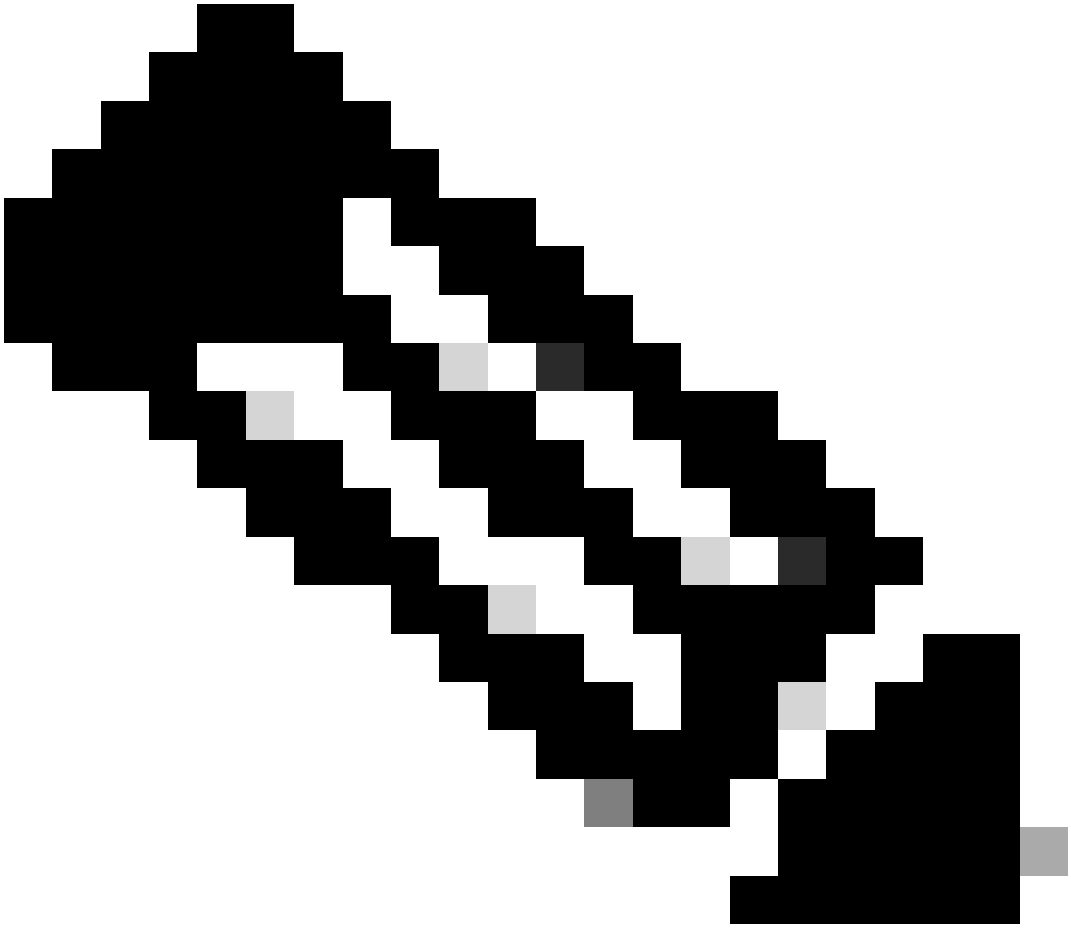

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package : Escolha o pacote carregado na Etapa 1 Fazer download e carregar recursos do agente
- **Configuration Name**: Escolha um nome para reconhecer o **Agent Configuration**
- **Compliance Module**: Escolha o módulo de conformidade baixado na Etapa 2 Faça o download do módulo de conformidade
- Cisco Secure Client Module Selection
    - **ISE Posture**: Marque a caixa de seleção
- **Profile Selection**

- **ISE Posture**: Escolha o perfil do ISE configurado na Etapa 3 Configurar o perfil do agente

- Clique em **Save**

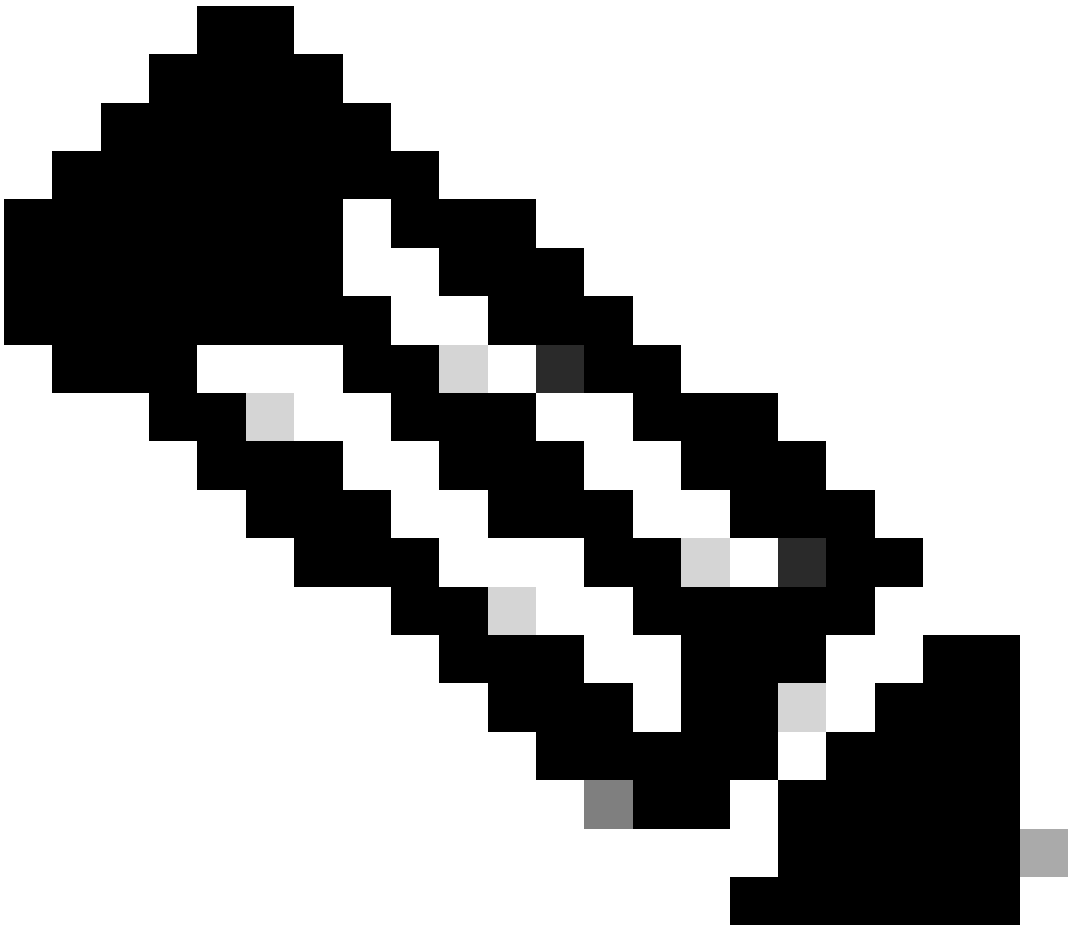


Observação: é recomendável que cada sistema operacional, Windows, Mac OS ou Linux, tenha uma configuração de cliente independente.

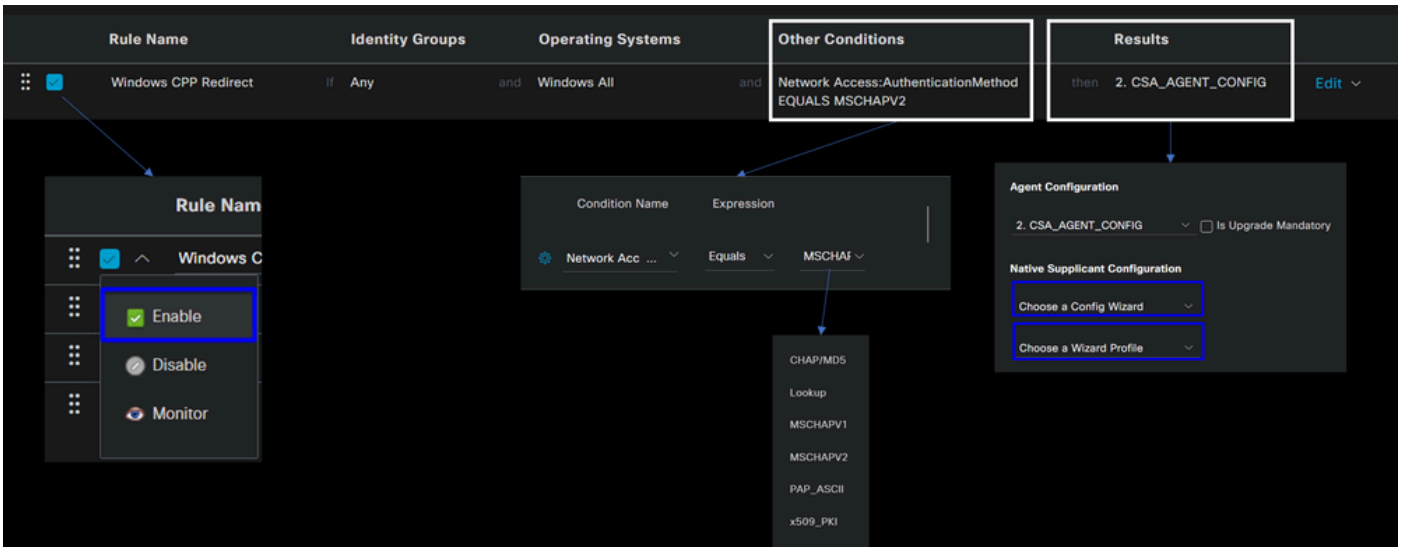
Configurar Política de Provisionamento de Cliente

Para habilitar o provisionamento da postura do ISE e dos módulos configurados na última etapa, você precisa configurar uma política para fazer o provisionamento.

- Navegue até o painel do ISE
- Clique em **Work Center > Client Provisioning**



Observação: é recomendável que cada sistema operacional, Windows, Mac OS ou Linux, tenha uma Política de Configuração de Cliente.



- **Rule Name**: configure o nome da política com base no tipo de dispositivo e na seleção do grupo de identidade para ter uma maneira fácil de identificar cada política
- **Identity Groups**: escolha as identidades que você deseja avaliar na política
- **Operating Systems**: Escolha o sistema operacional com base no pacote de agentes selecionado na etapa, Selecionar pacote de agentes
- **Other Condition**: Escolha com **Network Access** base no **Authentication Method**EQUALS para o método configurado na etapa, Adicionar grupo RADIUS ou você pode deixar em branco
- **Result**: Escolha a Configuração do agente configurada na Etapa 4 Configurar a configuração do agente
    - **Native Supplicant Configuration**: Escolha Config Wizard e Wizard Profile
- Marque a política como habilitada se ela não estiver listada como habilitada na caixa de seleção.

Criar os perfis de autorização

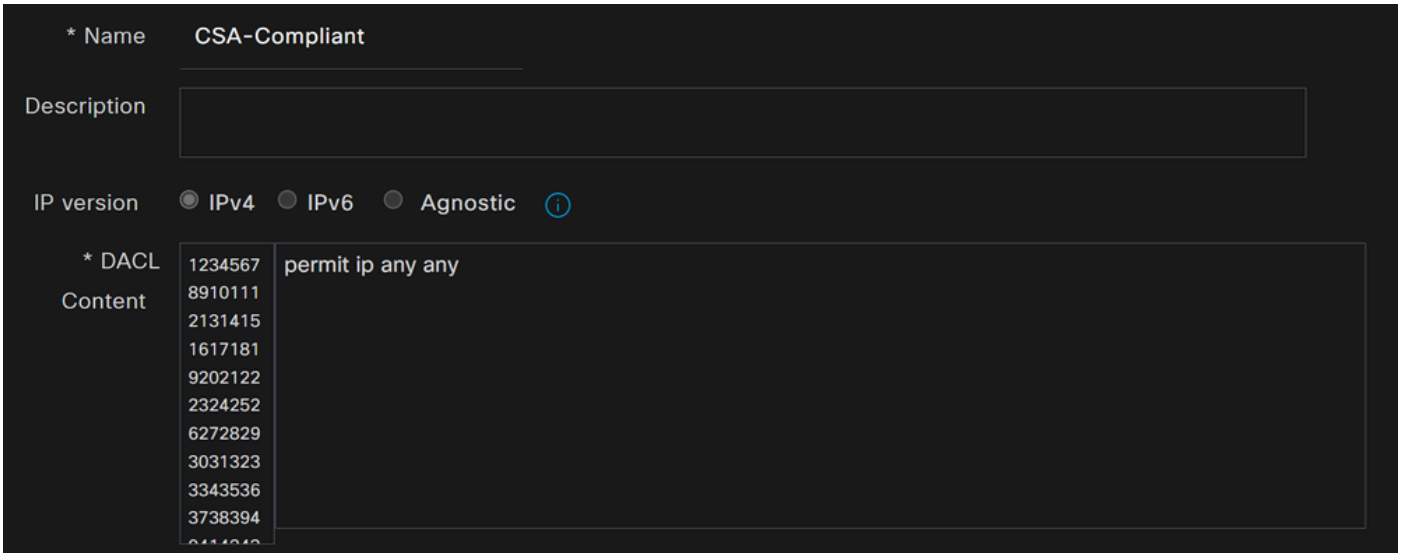
O perfil de autorização limita o acesso aos recursos, dependendo da postura dos usuários após a aprovação da autenticação. A autorização deve ser verificada para determinar quais recursos o usuário pode acessar com base na postura.

Perfil de Autorização	Descrição
Compatível	Compatível com Usuário - Agente Instalado - Postura Verificada
Compatível	Compatível com Usuário Desconhecido - Redirecionar para instalar o

Desconhecido	agente - Postura Pendente a ser verificada
NegarAcesso	Usuário Não Compatível - Negar Acesso

Para configurar o DACL, navegue até o painel do ISE:

- Clique em **Work Centers > Policy Elements > Downloadable ACLs**
- Clique em **+Add**
- Crie o **Compliant DACL**



- **Name**: Adicione um nome que faça referência ao DACL-Compliant
- **IP version**: Escolher **IPv4**
- DACL Content: criar uma lista de controle de acesso (DACL) que pode ser baixada e que dá acesso a todos os recursos da rede

<#root>

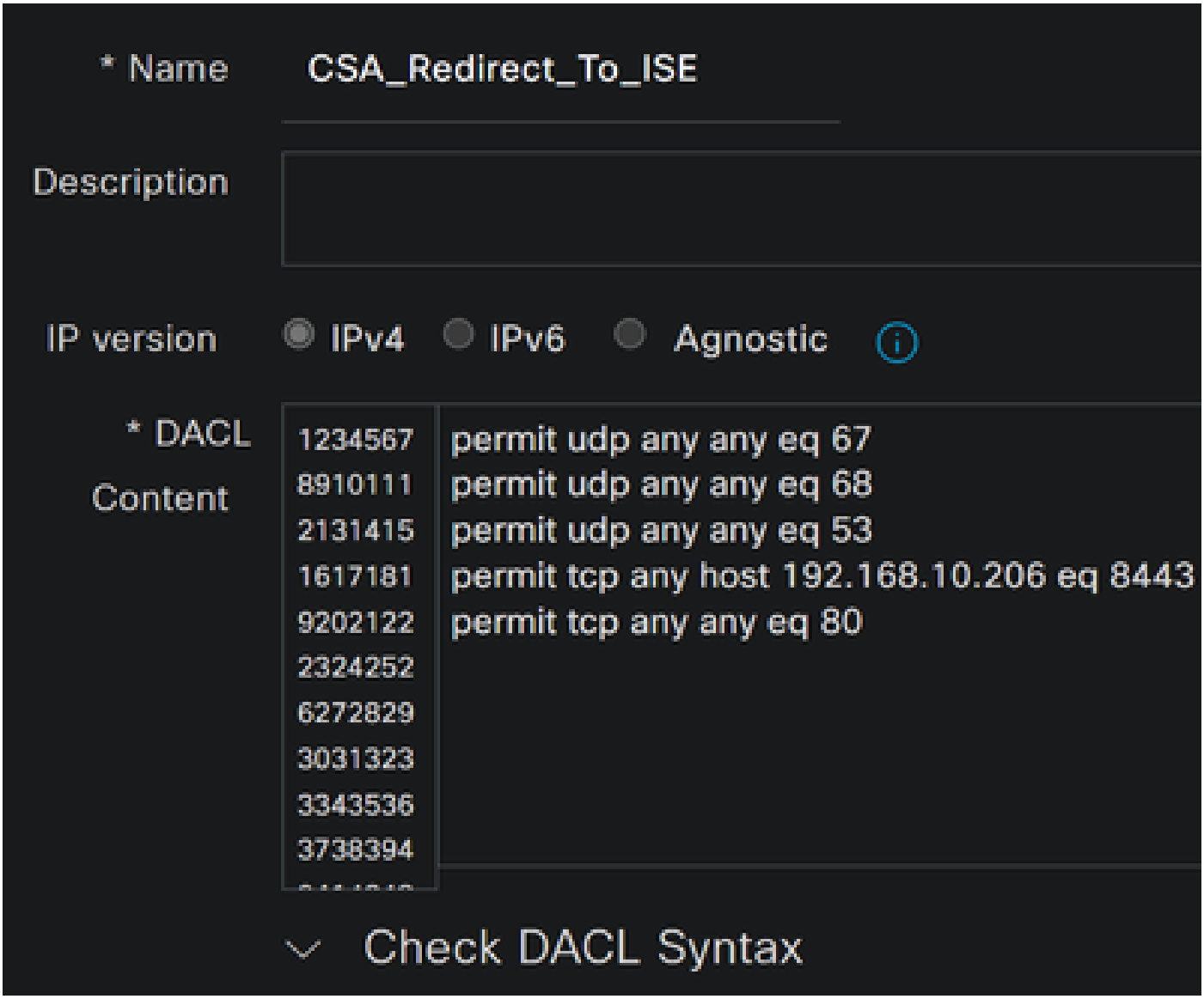
```
permit ip any any
```

Clique **Save** e crie a DACL de conformidade desconhecida

- Clique em **Work Centers > Policy Elements > Downloadable ACLs**

- Clique em **+Add**

- Crie o **Unknown Compliant DACL**

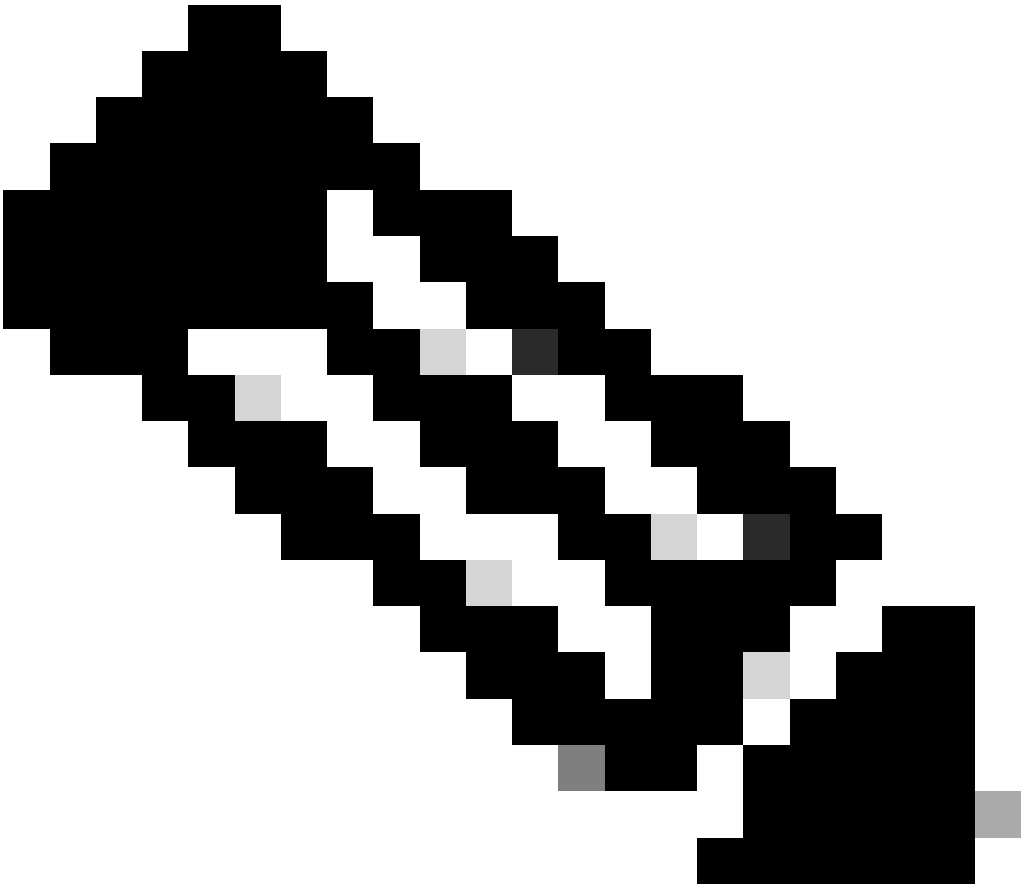


- **Name**: Adicione um nome que faça referência ao DACL-Unknown-Compliant

- **IP version**: Escolher **IPv4**

- **DACL Content**: Crie um DACL que forneça acesso limitado à rede, DHCP, DNS, HTTP e ao portal de provisionamento pela porta 8443

```
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443
```

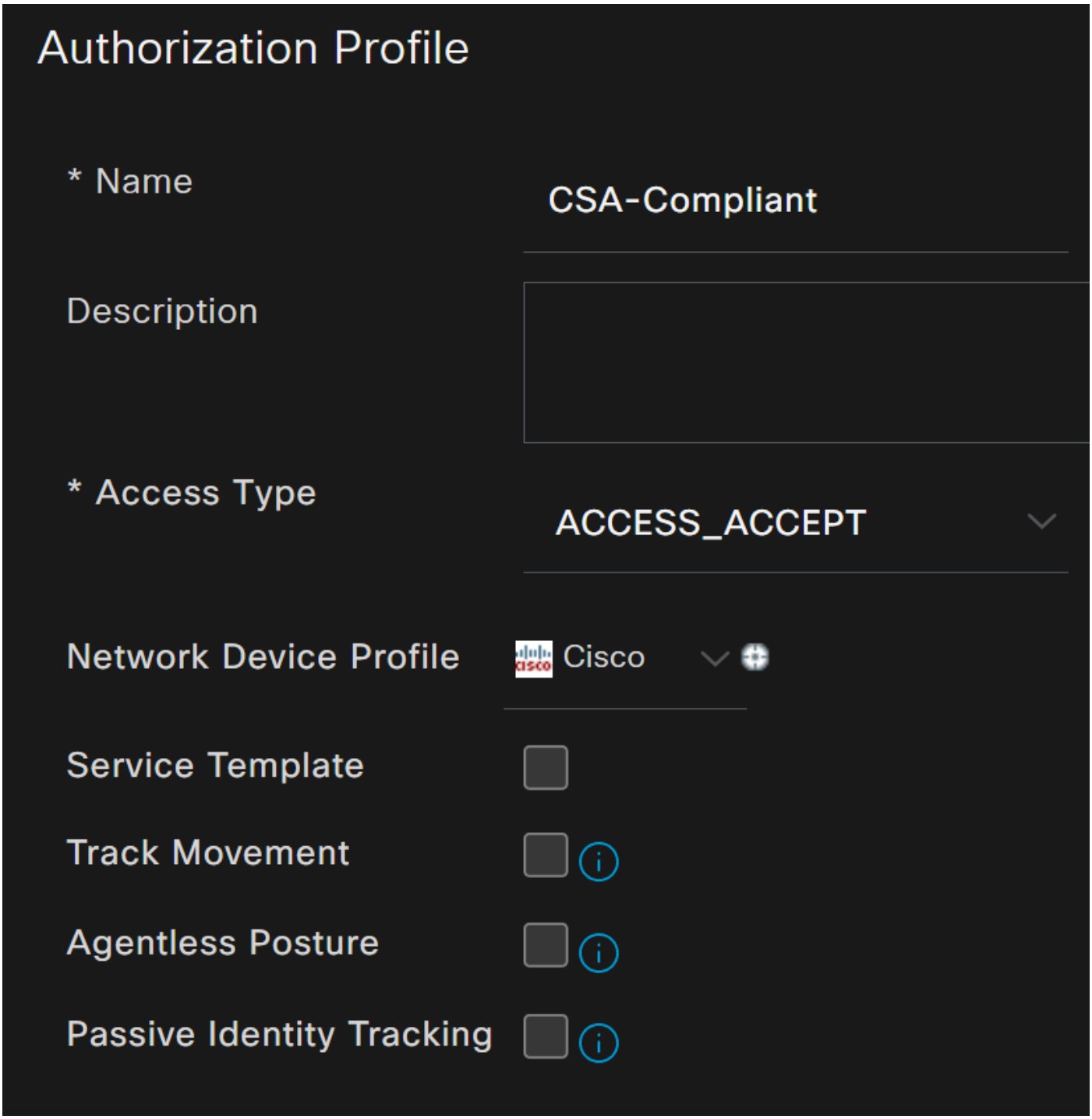


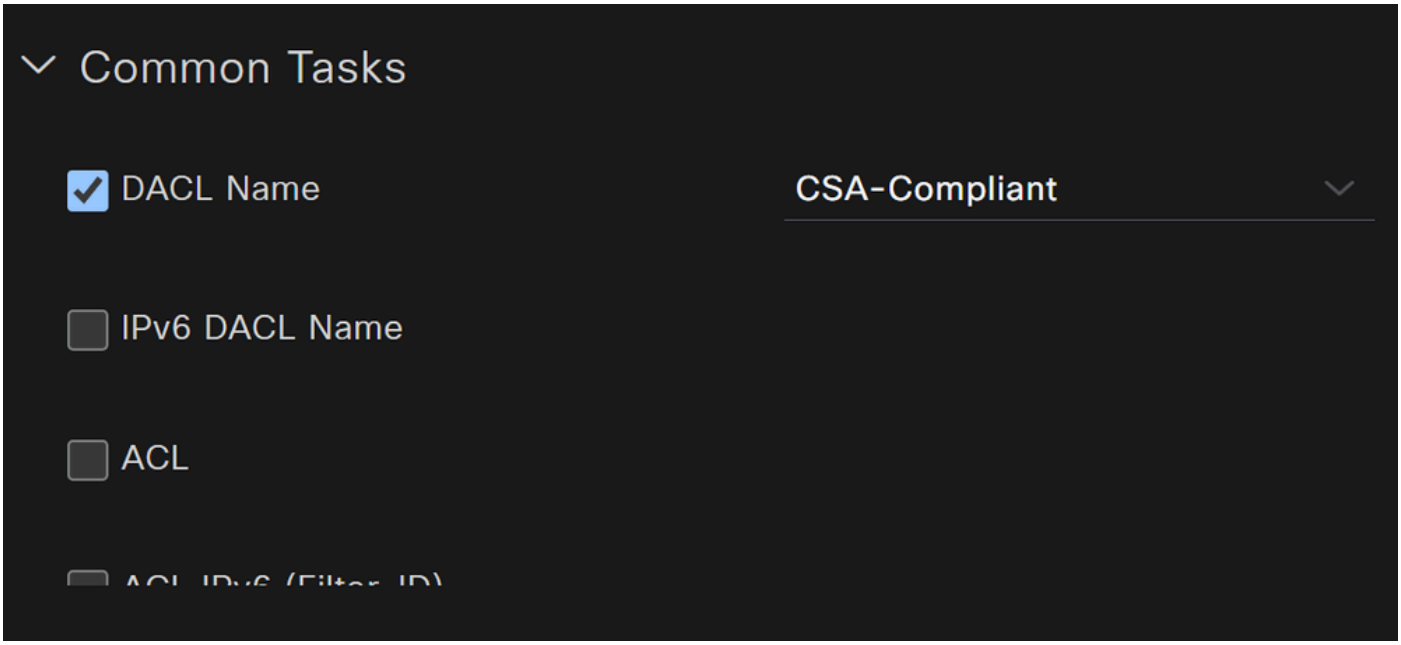
Observação: neste cenário, o endereço IP 192.168.10.206 corresponde ao servidor Cisco Identity Services Engine (ISE) e a porta 8443 é designada para o portal de provisionamento. Isso significa que o tráfego TCP para o endereço IP 192.168.10.206 através da porta 8443 é permitido, facilitando o acesso ao portal de provisionamento.

Neste ponto, você tem a DACL necessária para criar os perfis de autorização.

Para configurar os perfis de autorização, navegue até o Painel do ISE:

- Clique em **Work Centers > Policy Elements > Authorization Profiles**
    - Clique em **+Add**
    - Crie o **Compliant Authorization Profile**





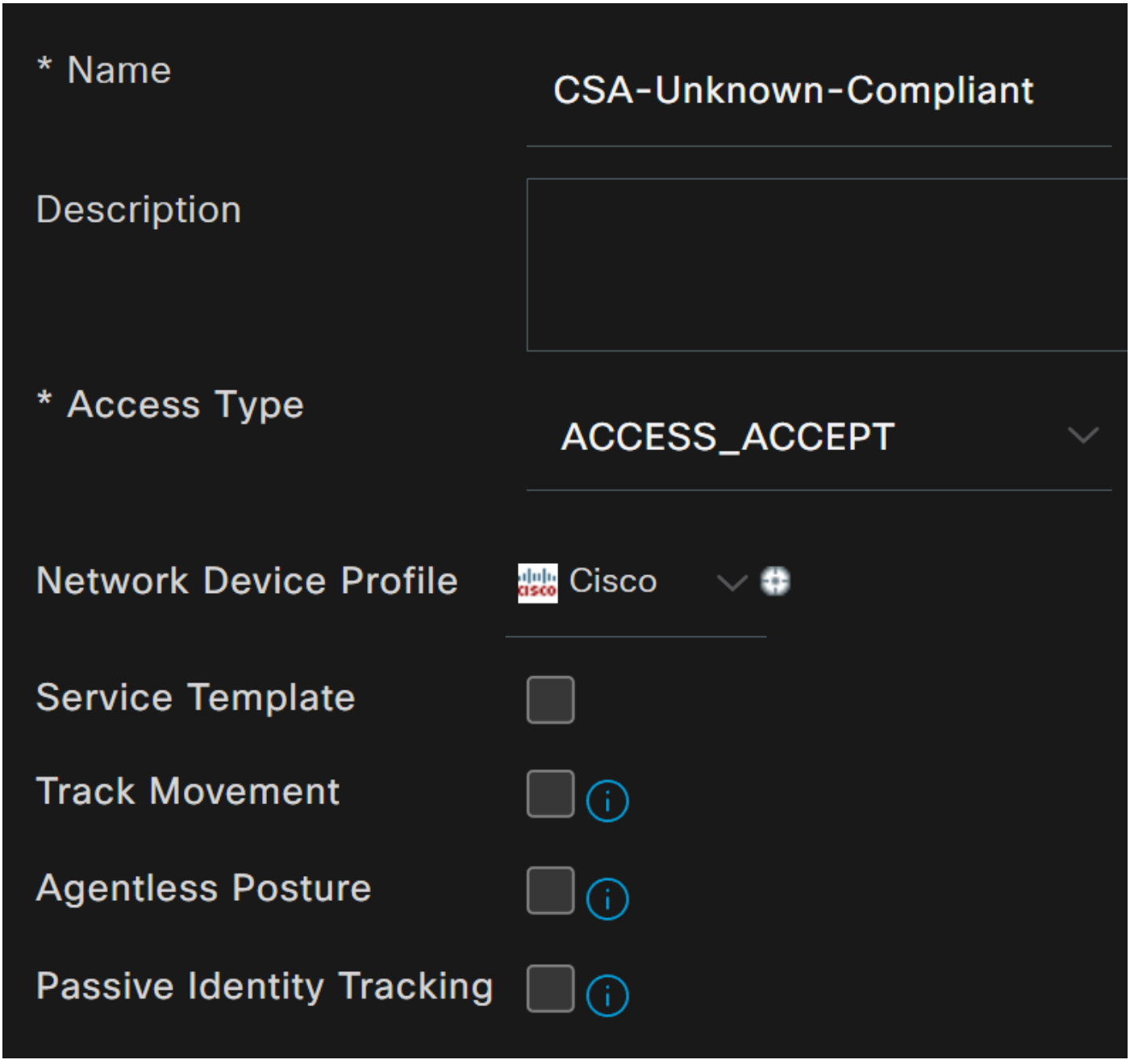
- **Name**: criar um nome que faça referência ao perfil de autorização compatível
- Access Type: Escolher **ACCESS_ACCEPT**

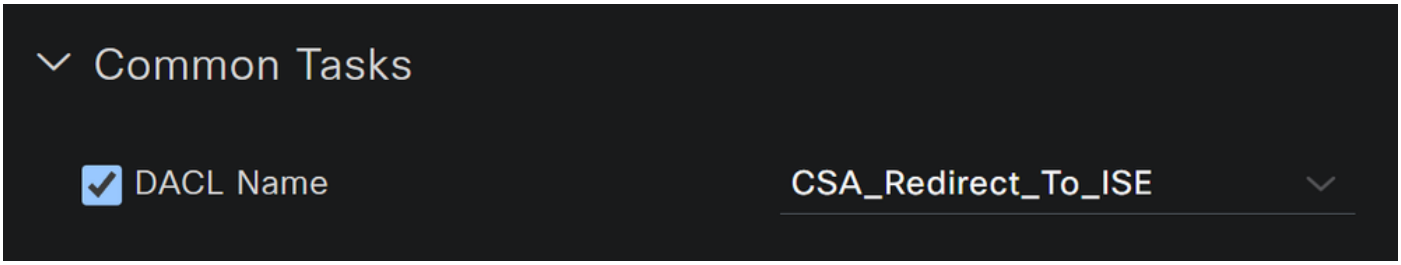
- **Common Tasks**
  - **DACL NAME**: Escolha a DACL configurada na etapa Compliant DACL

Clique **Save** e crie o Unknown Authorization Profile

- Clique em **Work Centers > Policy Elements > Authorization Profiles**
- Clique em **+Add**

- Crie o **Uknown Compliant Authorization Profile**

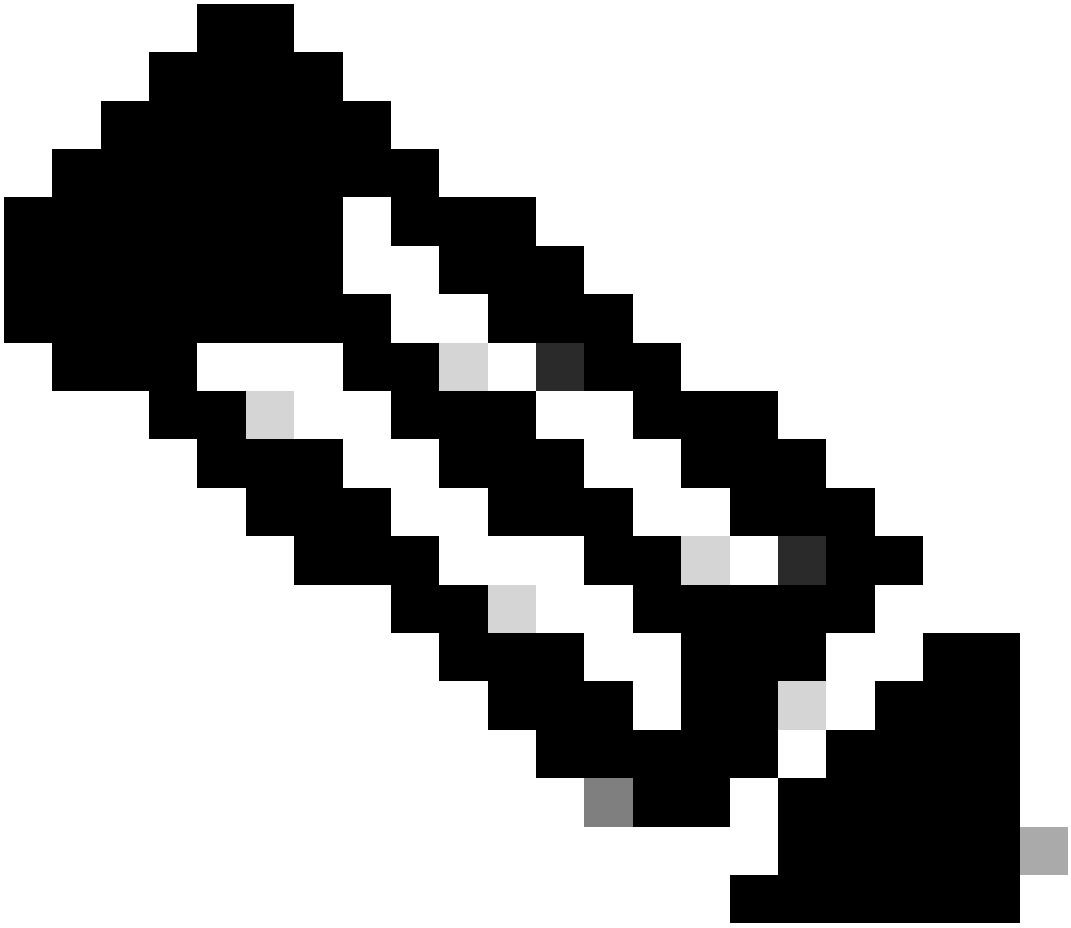




- **Name**: criar um nome que faça referência ao perfil de autorização em conformidade desconhecido
- Access Type: Escolher **ACCESS_ACCEPT**

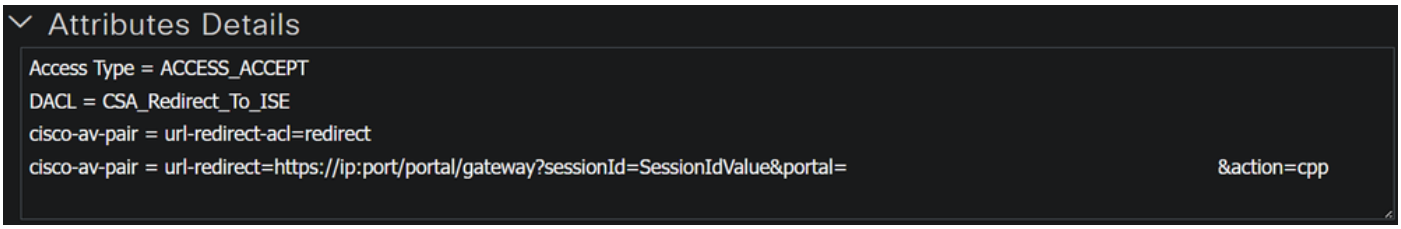
- **Common Tasks**
  - **DACL NAME**: Escolha a DACL configurada na etapa DACL em conformidade desconhecida
    - **Web Redirection (CWA,MDM,NSP,CPP)**
      - Escolher **Client Provisioning (Posture)**
        - **ACL**: Deve ser redirect
        - **Value**: Escolha o portal de provisionamento padrão ou, se você definiu outro, escolha-o

---



Observação: o nome da ACL de redirecionamento no Secure Access para todas as implantações é **redirect**.

Depois de definir todos esses valores, você deve ter algo semelhante em Attributes Details.



Clique **Save** para encerrar a configuração e continue com a próxima etapa.

Configurar Conjunto de Políticas de Postura

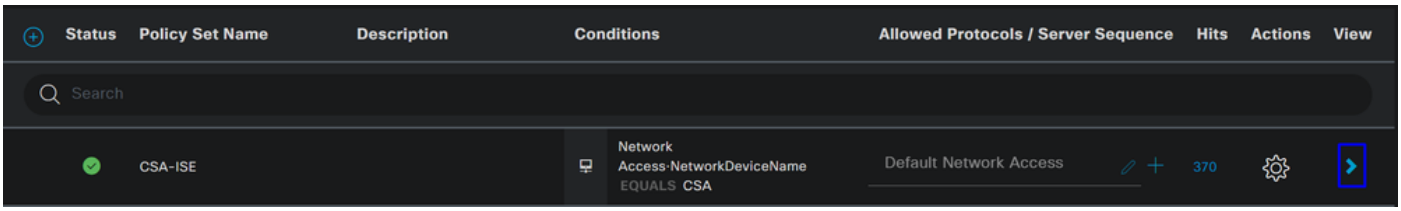
Essas três políticas que você cria são baseadas nos perfis de autorização que você configurou; por **DenyAccess**exemplo, você não precisa criar outra.

Conjunto de políticas - Autorização	**Perfil de Autorização**
Compatível	Perfil de Autorização - Compatível
Compatível Desconhecido	Perfil de Autorização - Compatível Desconhecido
Não compatível	NegarAcesso

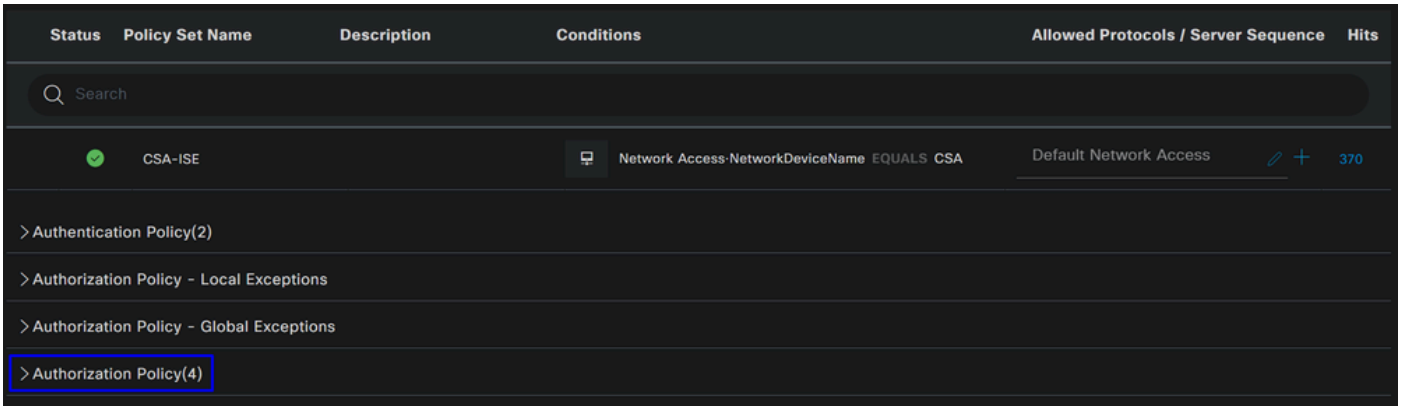
Navegue até o painel do ISE

- Clique em **Work Center > Policy Sets**

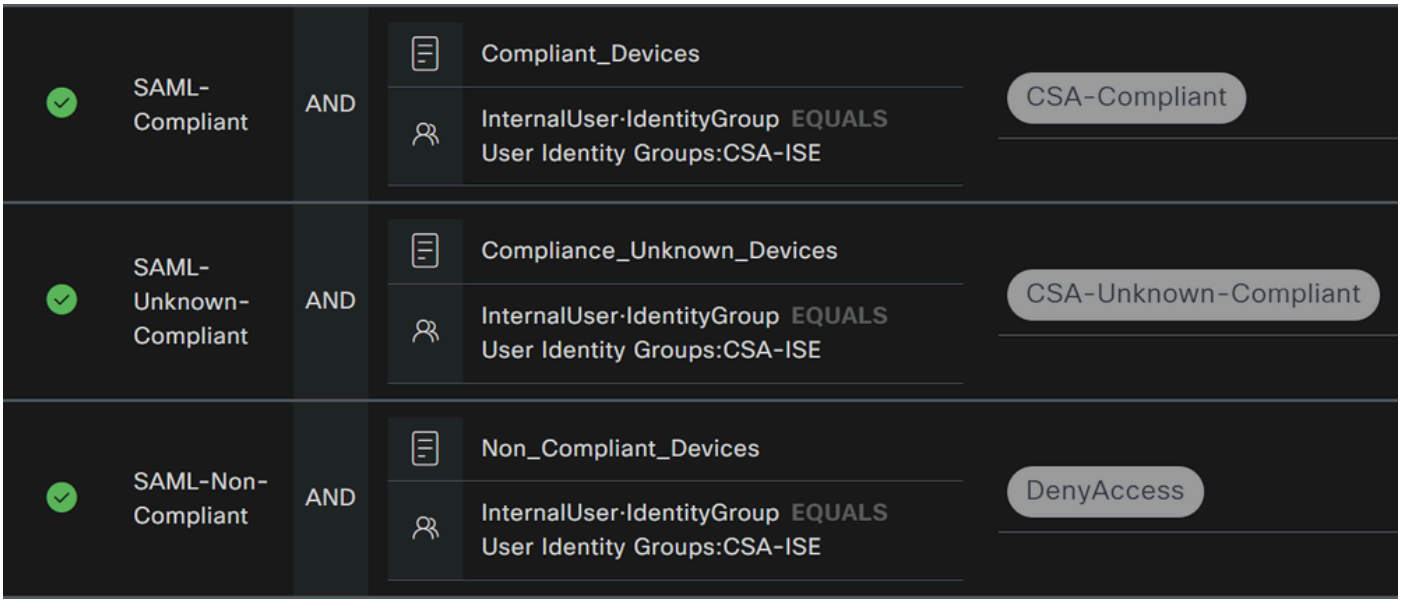
- Clique > na para acessar a política criada



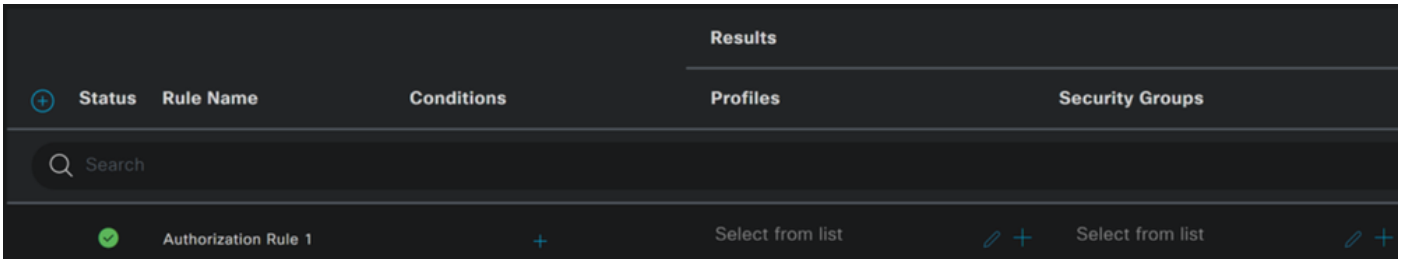
- Clique no botão Authorization Policy



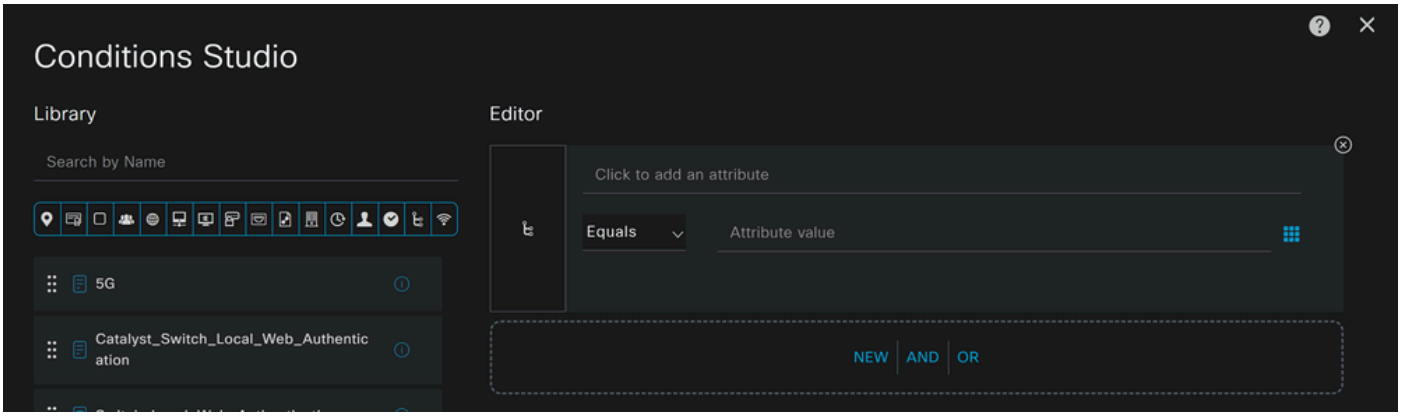
- Crie as três políticas a seguir na próxima ordem:



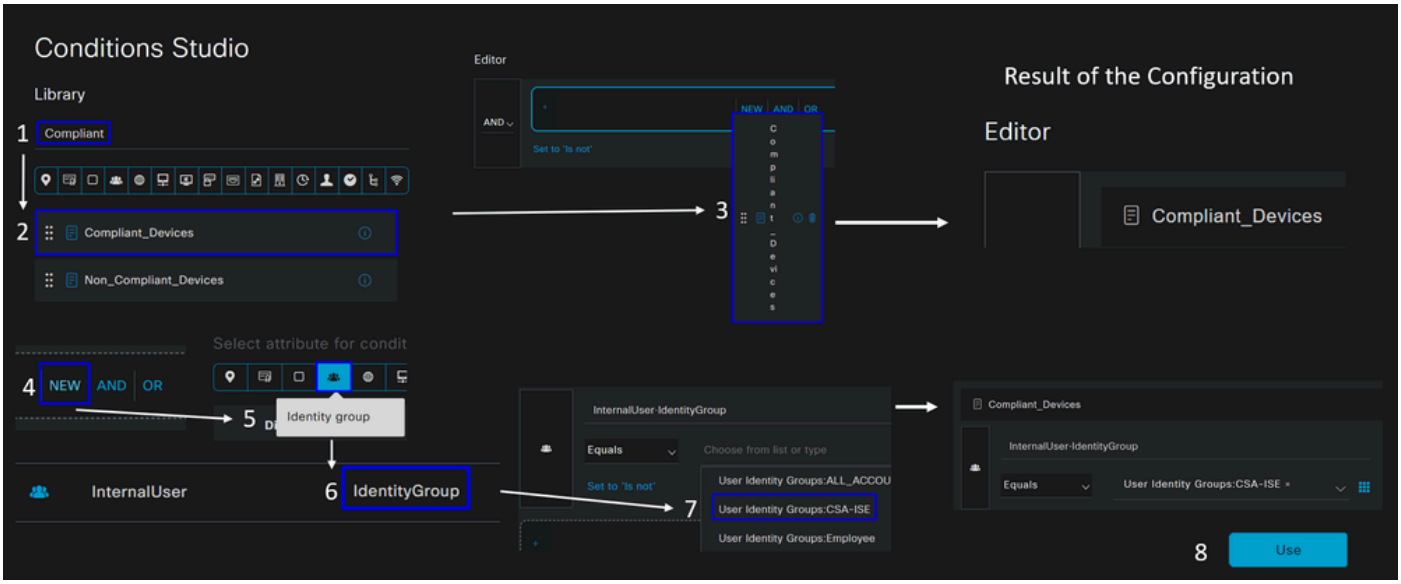
- Clique em **+** para definir a **CSA-Compliance** política:



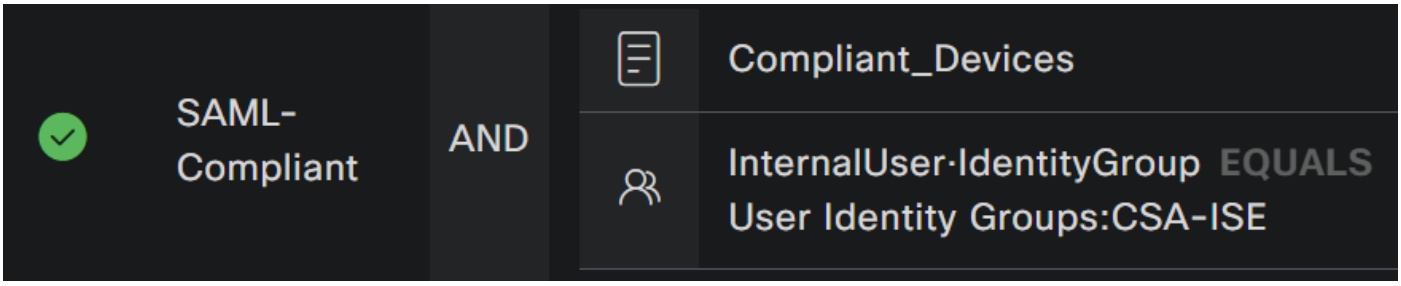
- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Compliance**
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



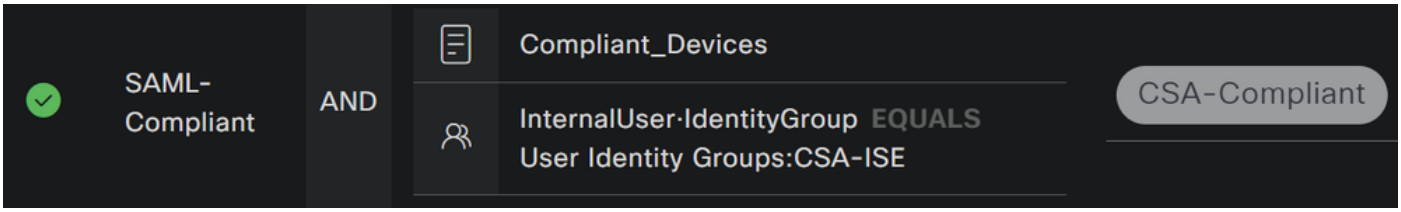
- Para criar a condição, procure **compliant**
- Você deve ter exibido Compliant_Devices
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group** que deseja corresponder
- Clique em **Use**



- Como resultado, você terá a próxima imagem

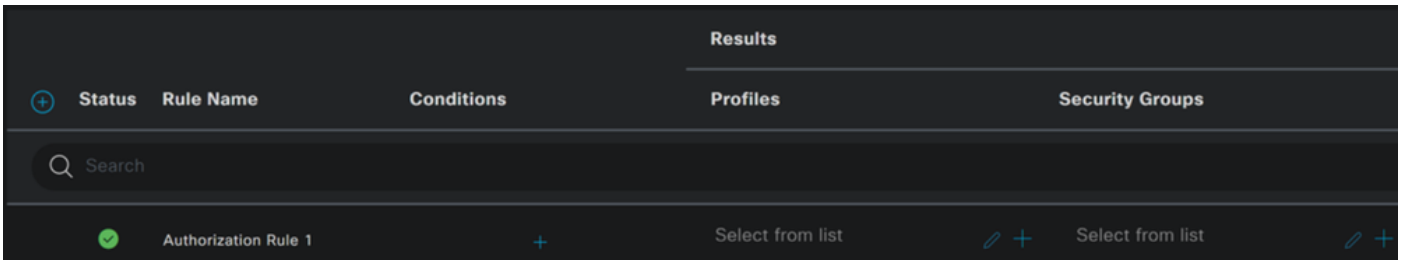


- Em **Profile** clique sob o botão suspenso e escolha o perfil de autorização de reclamação configurado na etapa, [Perfil de autorização de conformidade]



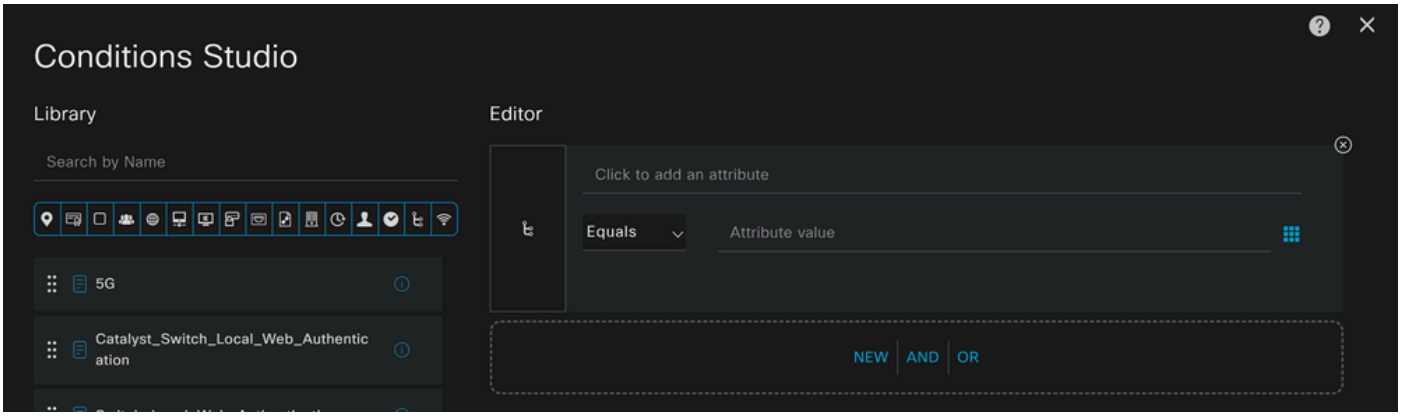
Agora você configurou o **Compliance Policy Set**.

- Clique em **+** para definir a **CSA-Unknown-Compliance** política:

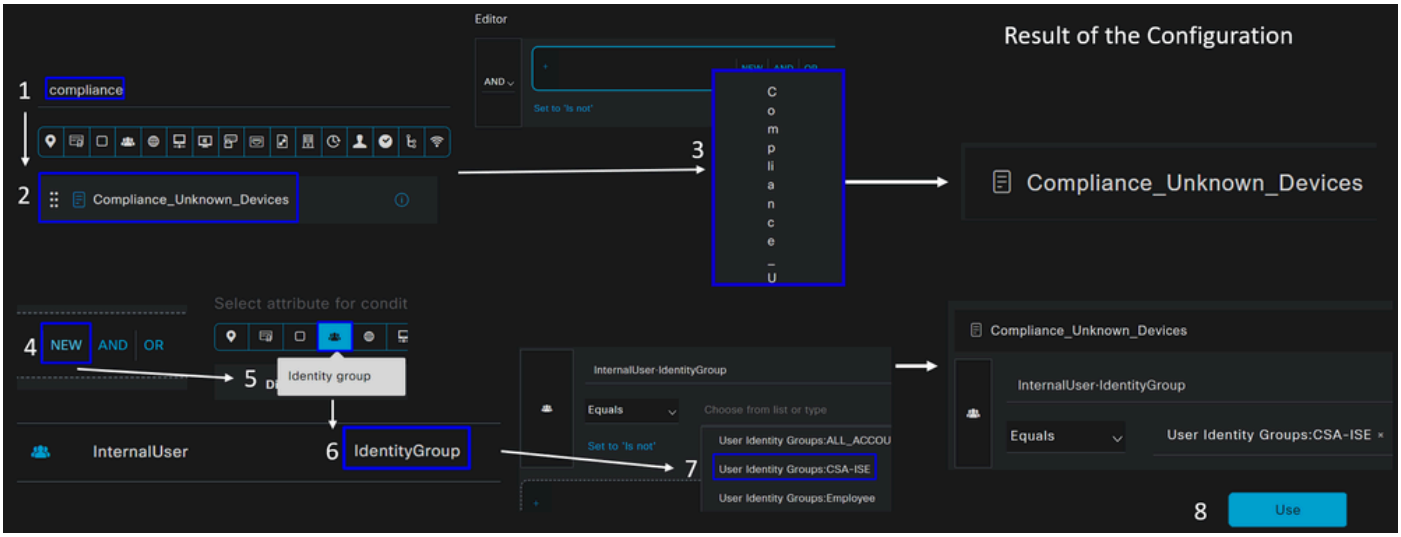


- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Unknown-Compliance**

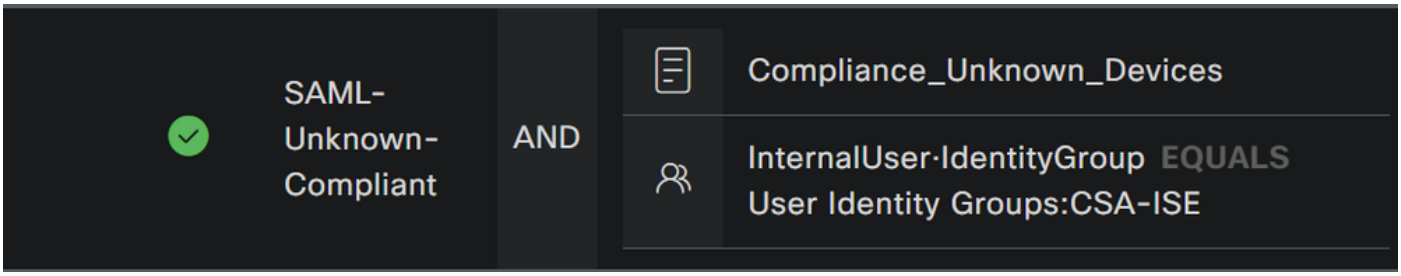
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



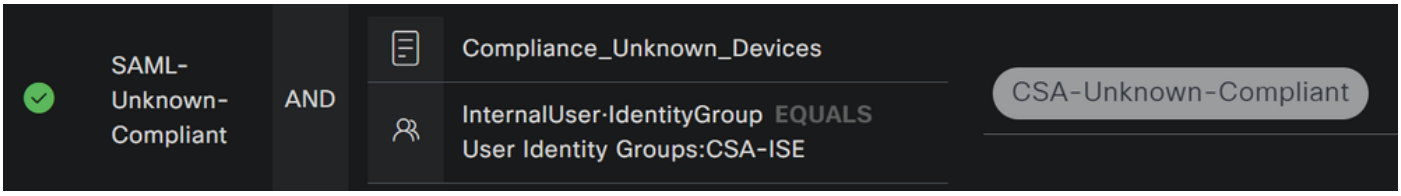
- Para criar a condição, procure **compliance**
- Você deve ter exibido Compliant_Unknown_Devices
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group** que deseja corresponder
- Clique em **Use**



- Como resultado, você terá a próxima imagem

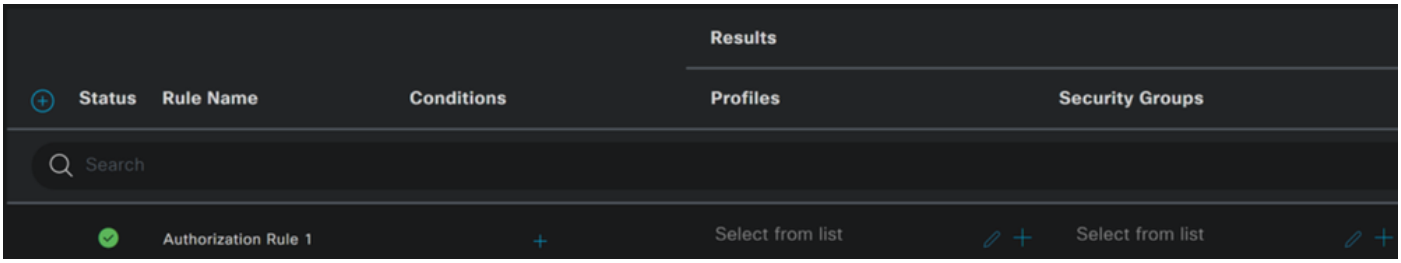


- Em **Profile** clique sob o botão suspenso e escolha o perfil de autorização de reclamação configurado na etapa, [Perfil de autorização de conformidade desconhecido]



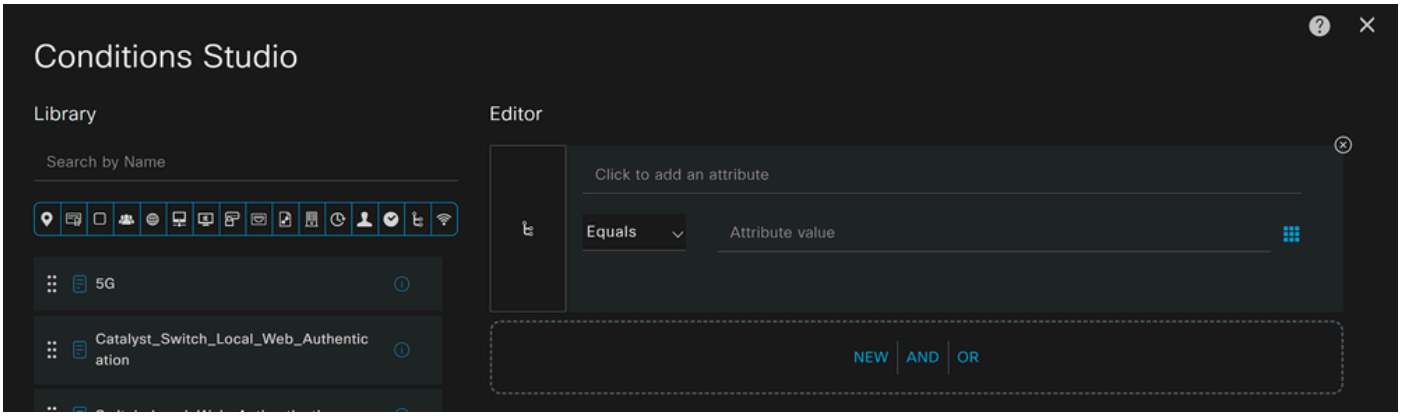
Agora você configurou o **Unknown Compliance Policy Set**.

- Clique em **+** para definir a **CSA- Non-Compliant** política:

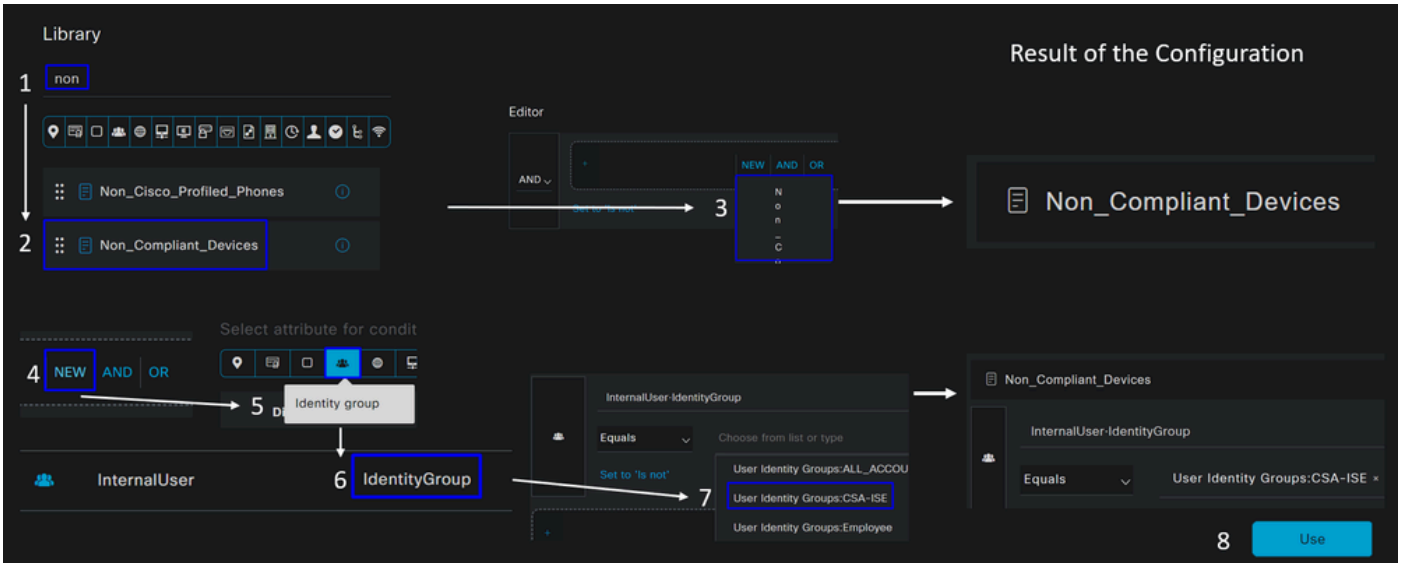


- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Non-Compliance**

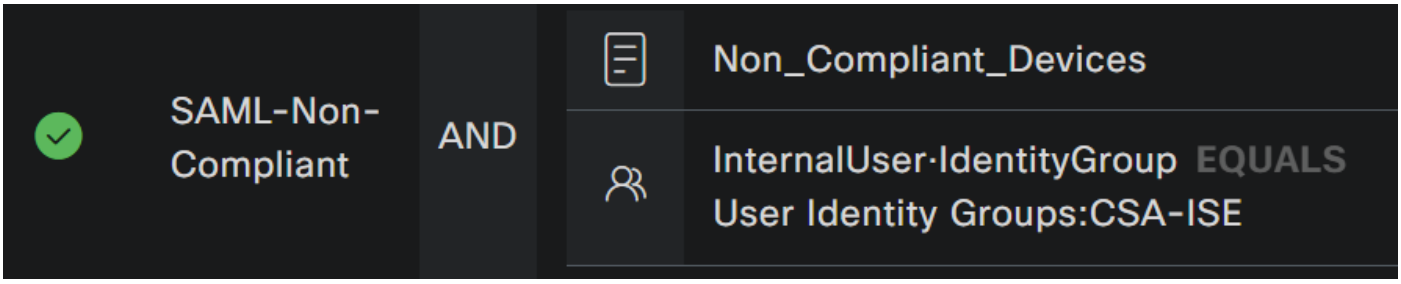
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



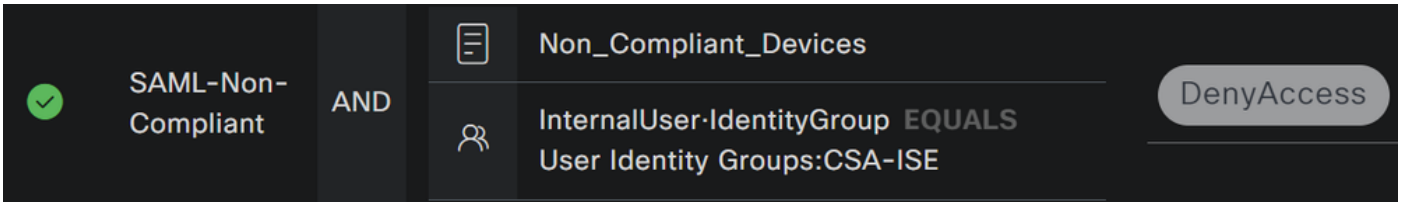
- Para criar a condição, procure **non**
- Você deve ter exibido Non_Compliant_Devices
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group** que deseja corresponder
- Clique em **Use**



- Como resultado, você terá a próxima imagem



- Em **Profile** clique no botão suspenso e escolha o perfil de autorização de reclamação **DenyAccess**



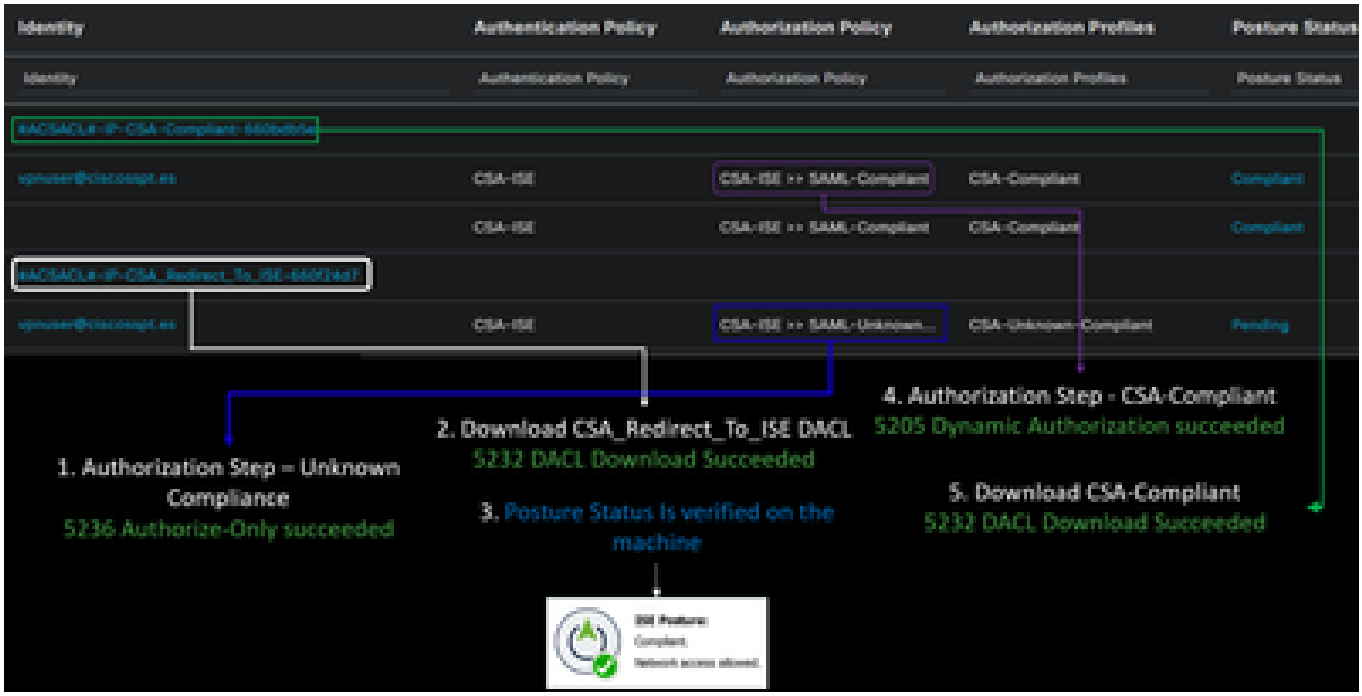
Quando terminar a configuração dos três perfis, você estará pronto para testar sua integração com a postura.

Verificar

Validação de postura

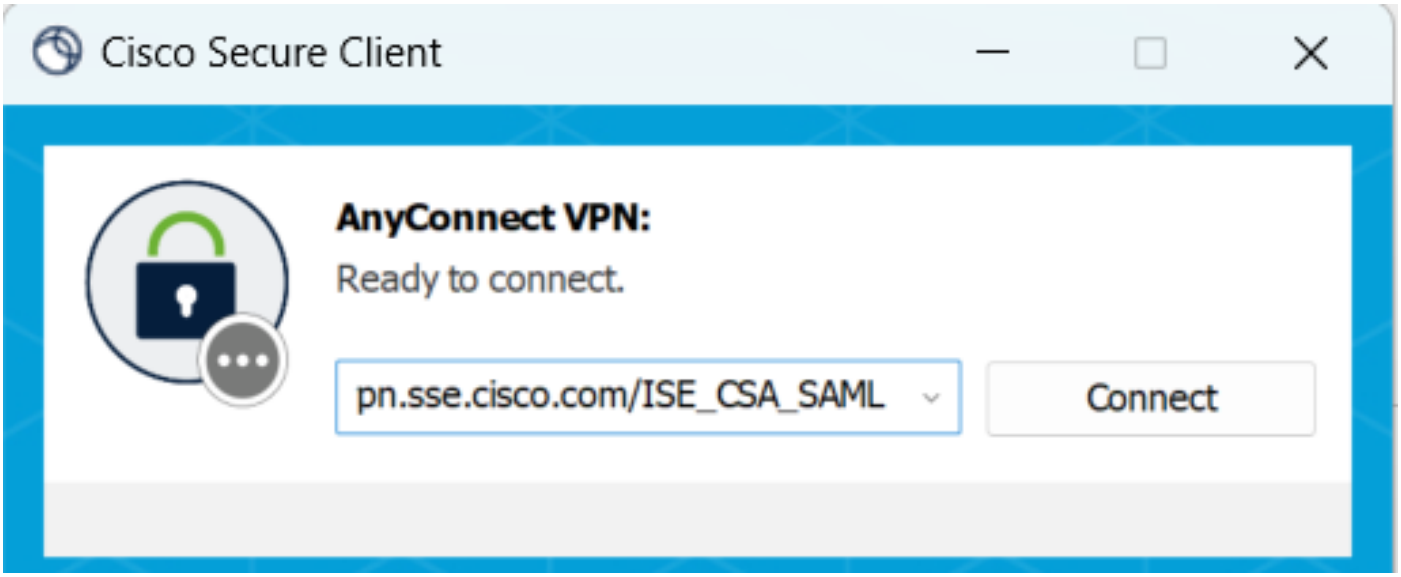
Conexão na máquina

Conecte-se ao domínio FQDN RA-VPN fornecido no Secure Access via Secure Client.

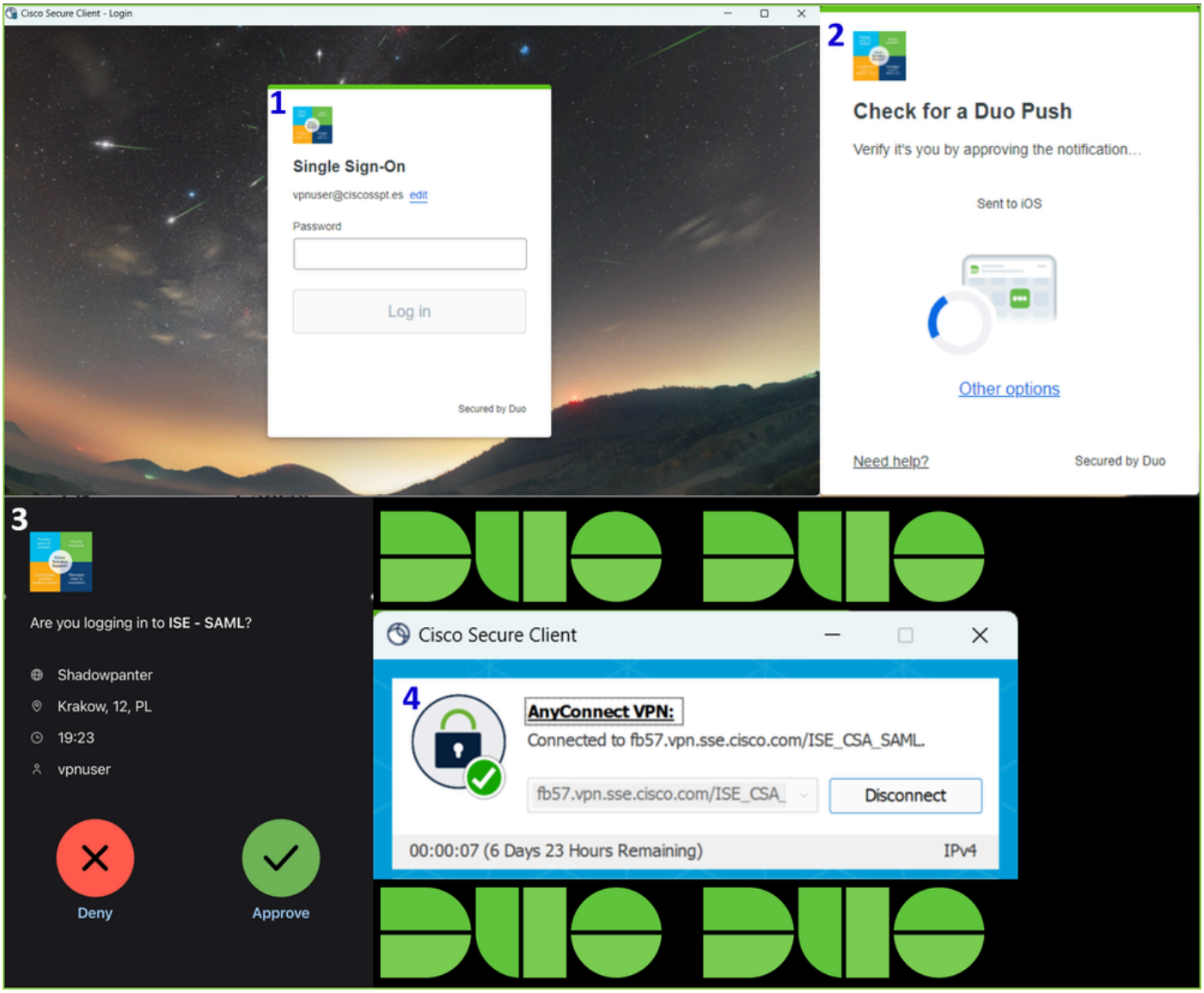


Observação: nenhum módulo ISE deve ser instalado para esta etapa.

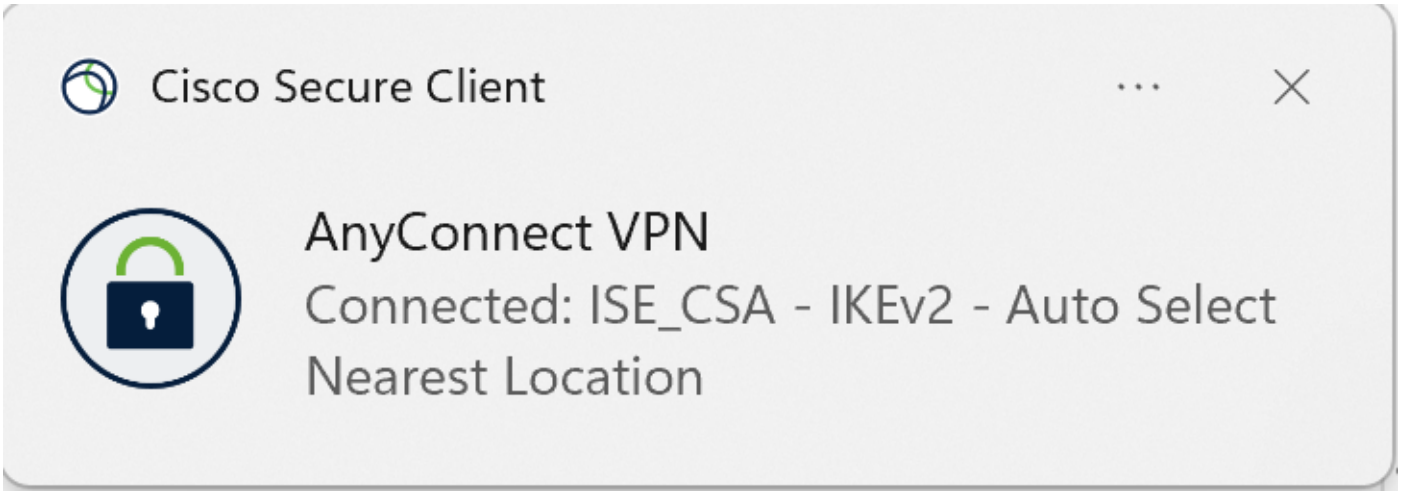
1. Conecte-se usando o Secure Client.

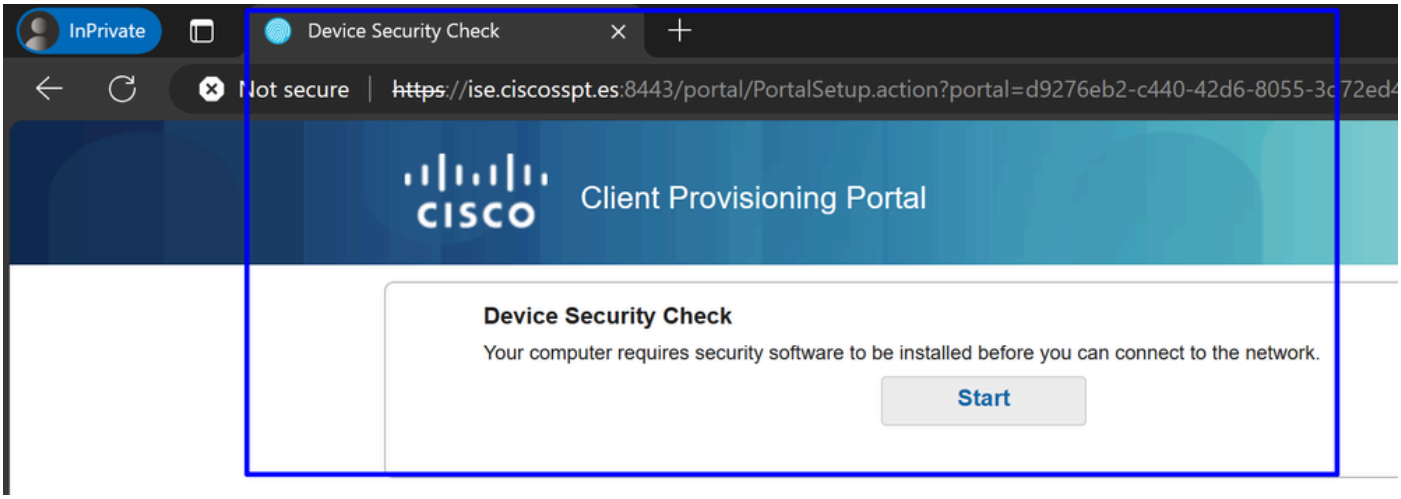


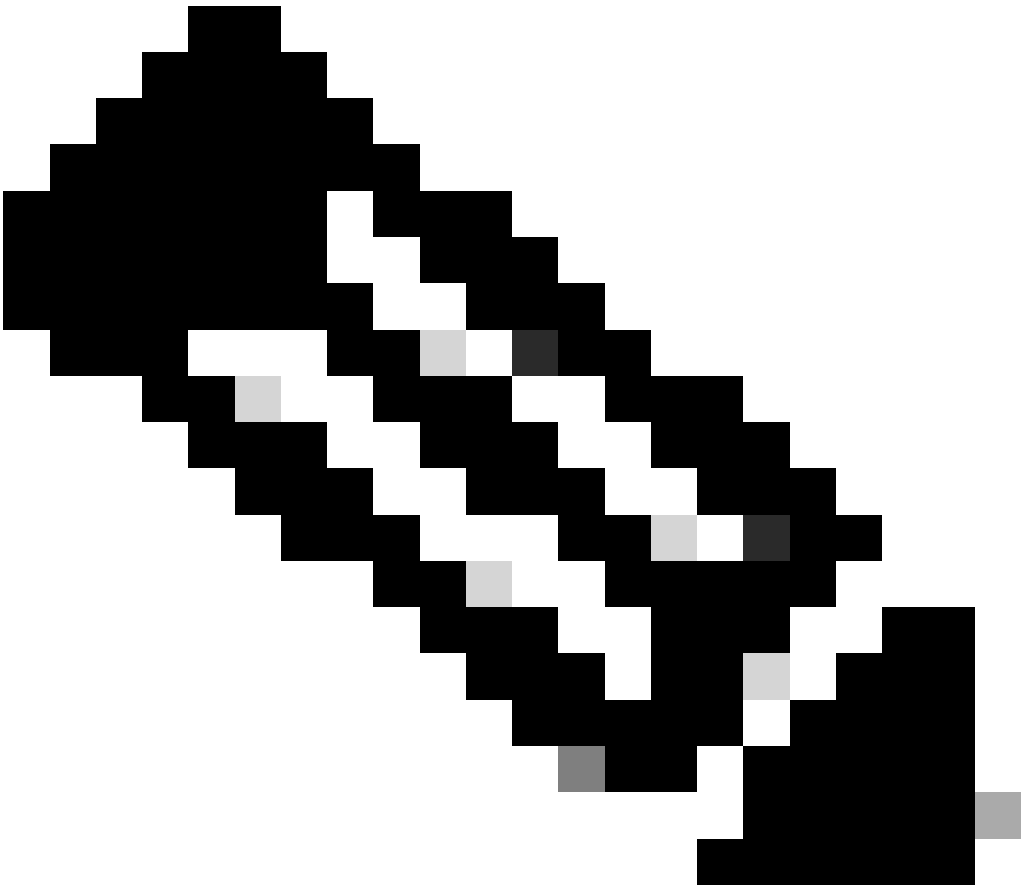
2. Forneça as credenciais para autenticação via Duo.



3. Neste ponto, você se conecta à VPN e, provavelmente, será redirecionado para o ISE; caso contrário, tente navegar para **http:1.1.1.1**.





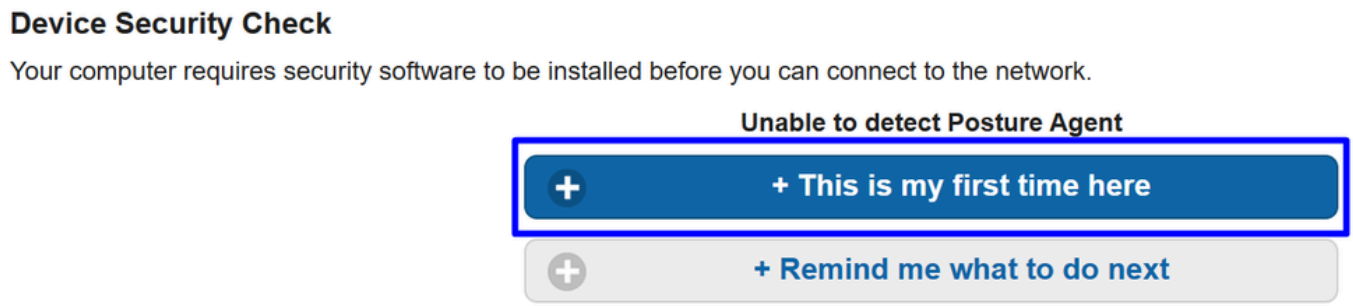


Observação: neste momento, você está sob autorização - a política define CSA-Unknown-Compliance porque você não tem o ISE

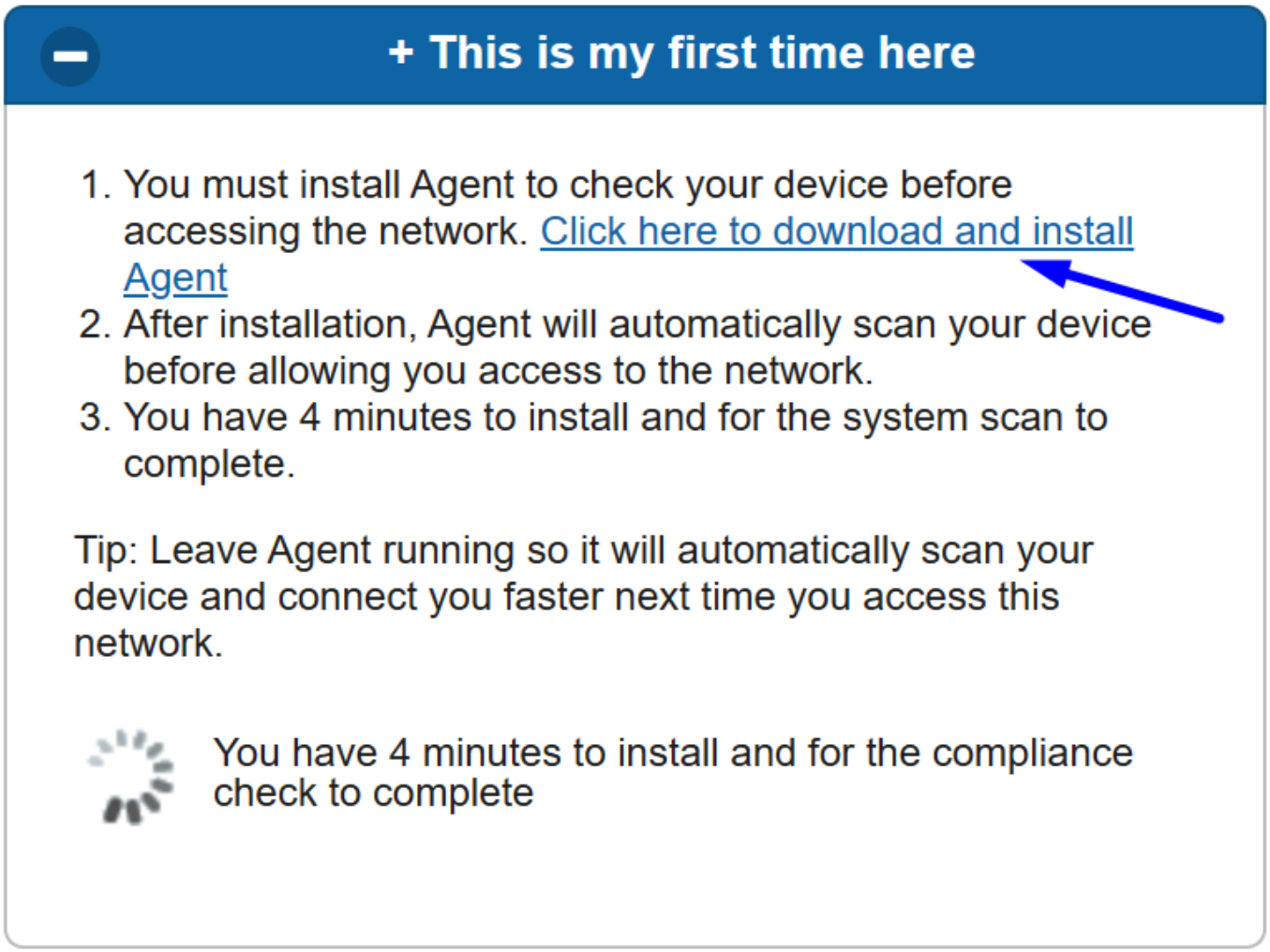
Posture Agent instalado na máquina e é redirecionado para o ISE Provisioning Portal para instalar o agente.

4. Clique em Iniciar para continuar com o provisionamento do agente.

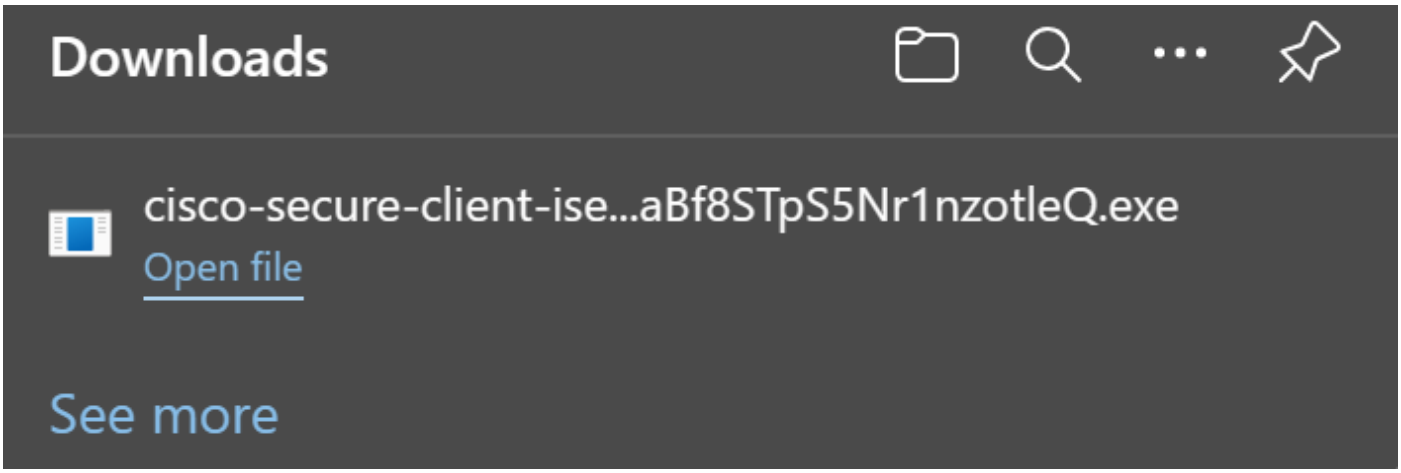
5. Clique em + **This is my first time here**.

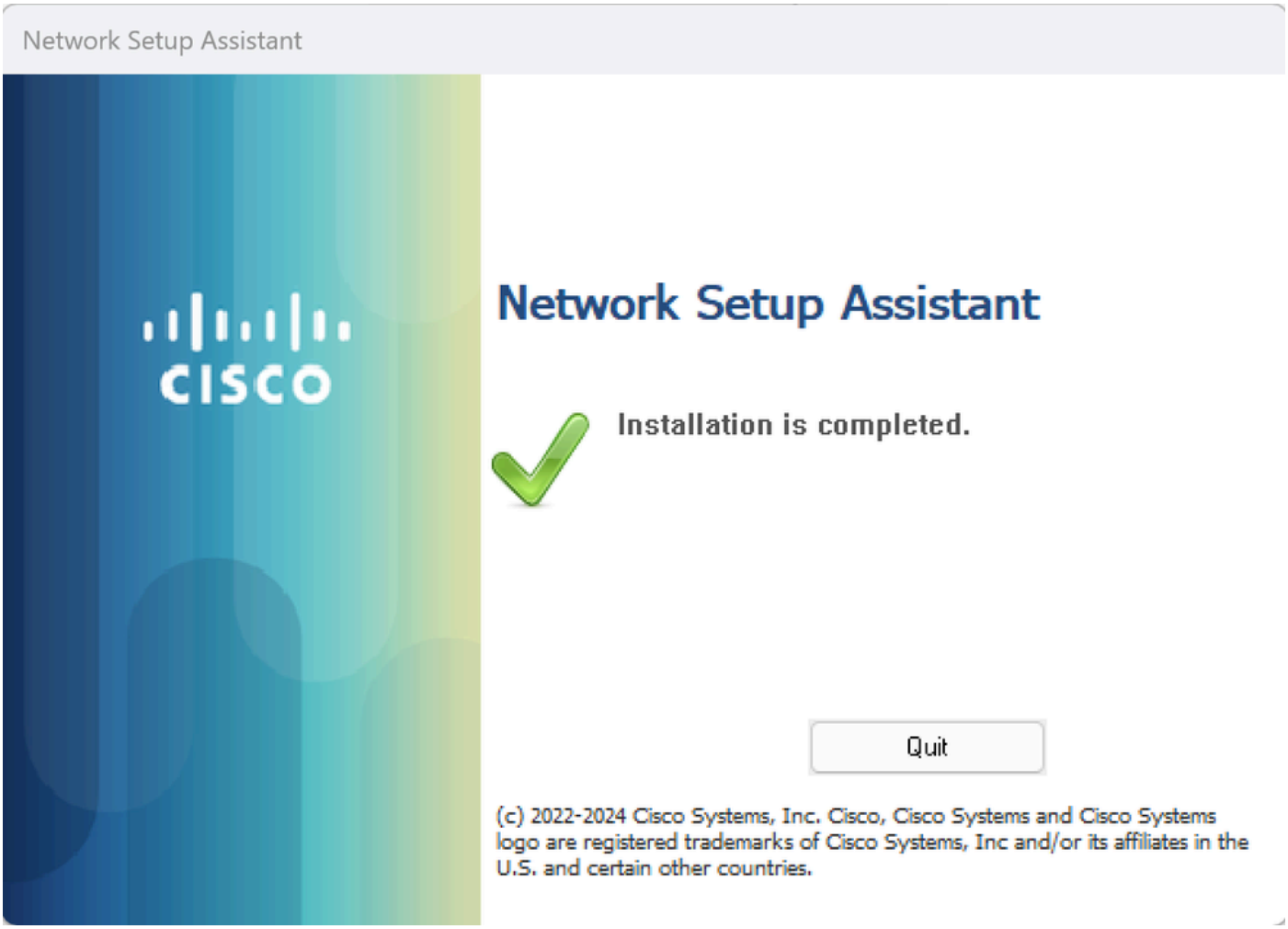


6. Clique em **Click here to download and install agent**

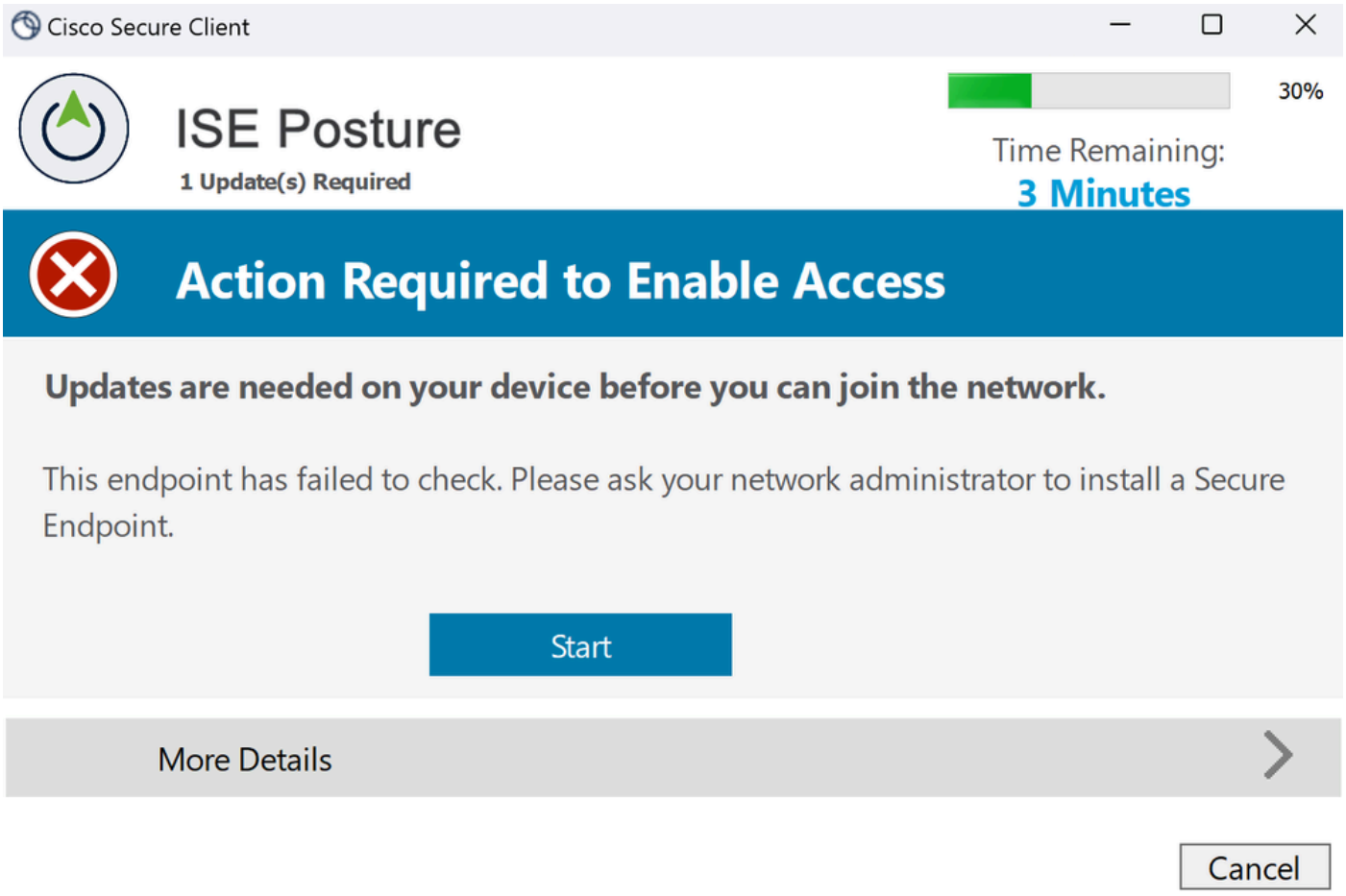


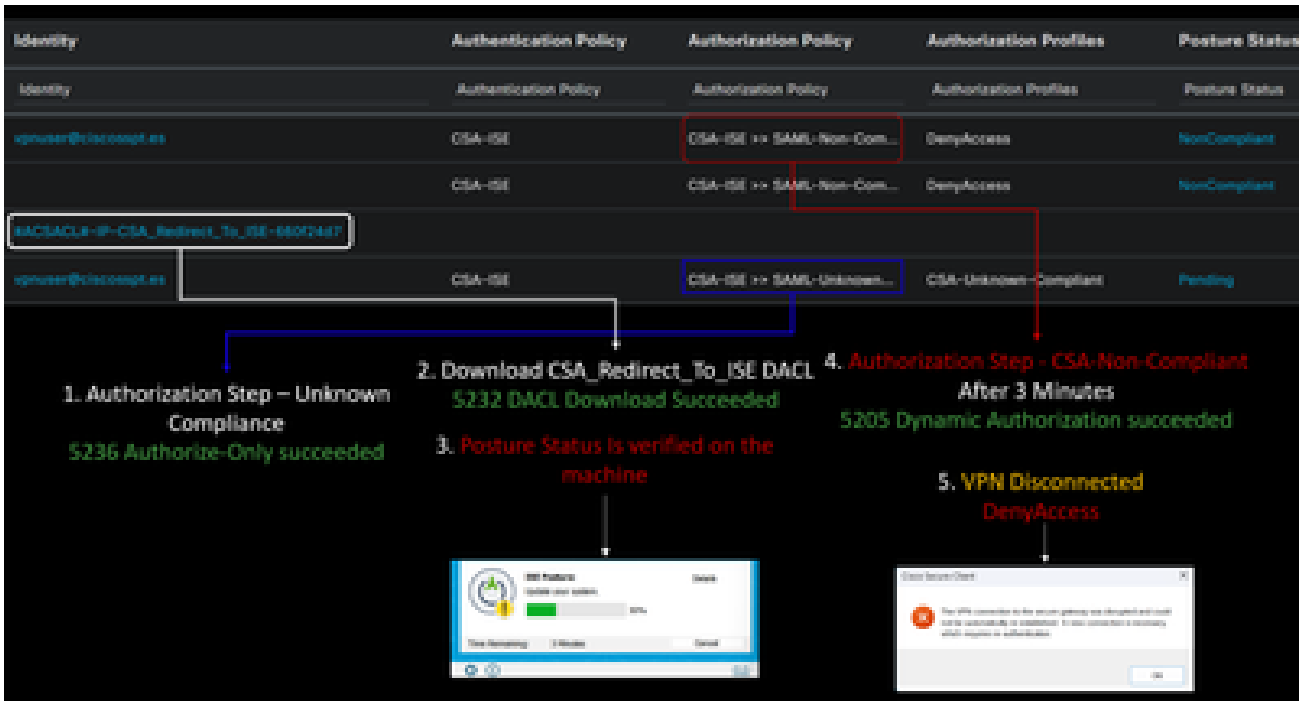
7. Instalar o agente





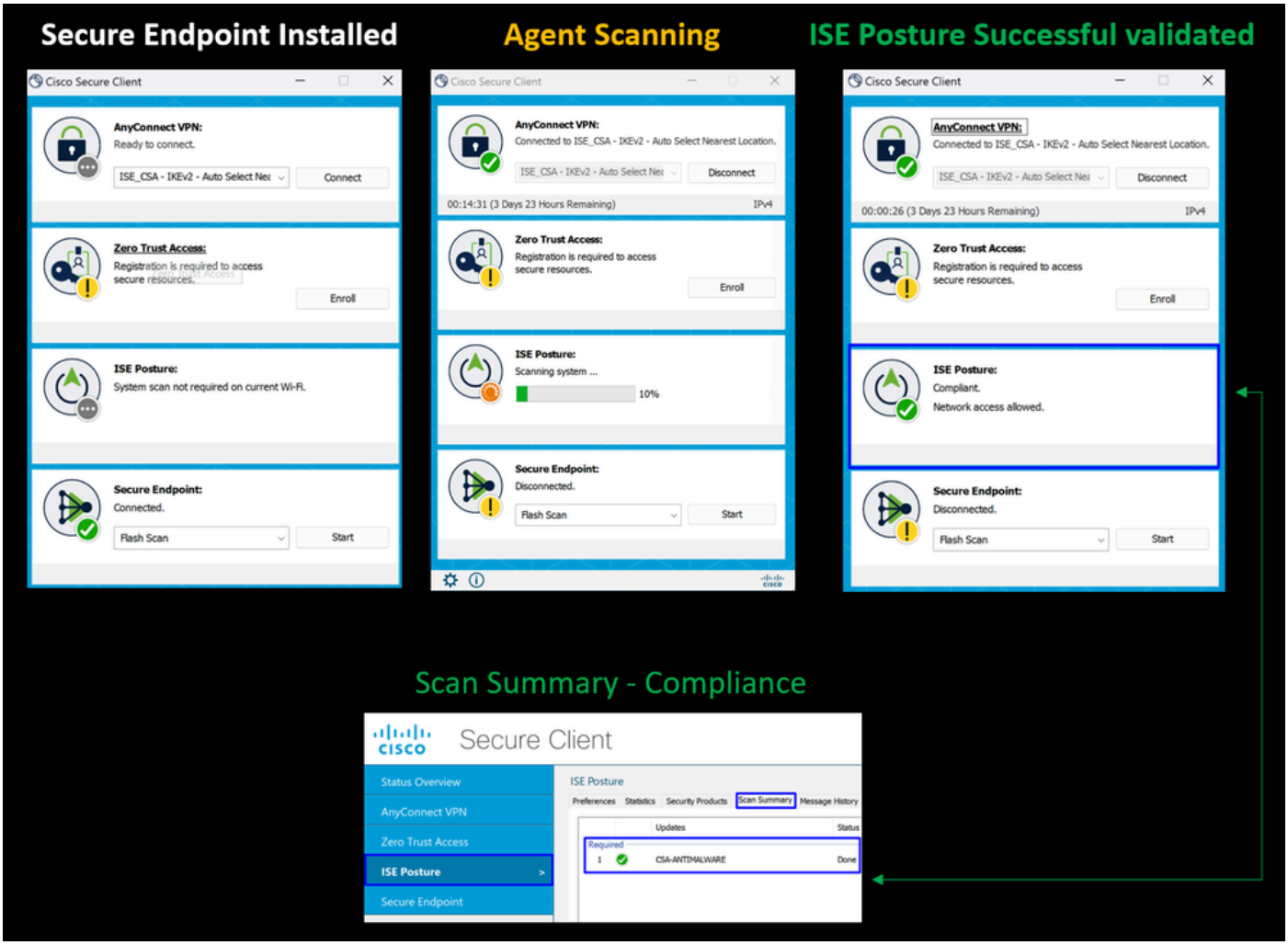
8. Após a instalação do agente, a Postura do ISE começa a verificar a postura atual das máquinas. Se os requisitos da política não forem atendidos, uma janela pop-up será exibida para orientá-lo em relação à conformidade.


Cisco Secure Client
ISE Posture
1 Update(s) Required
30%
Time Remaining:
3 Minutes
Action Required to Enable Access
Updates are needed on your device before you can join the network.
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.
Start
More Details
Cancel

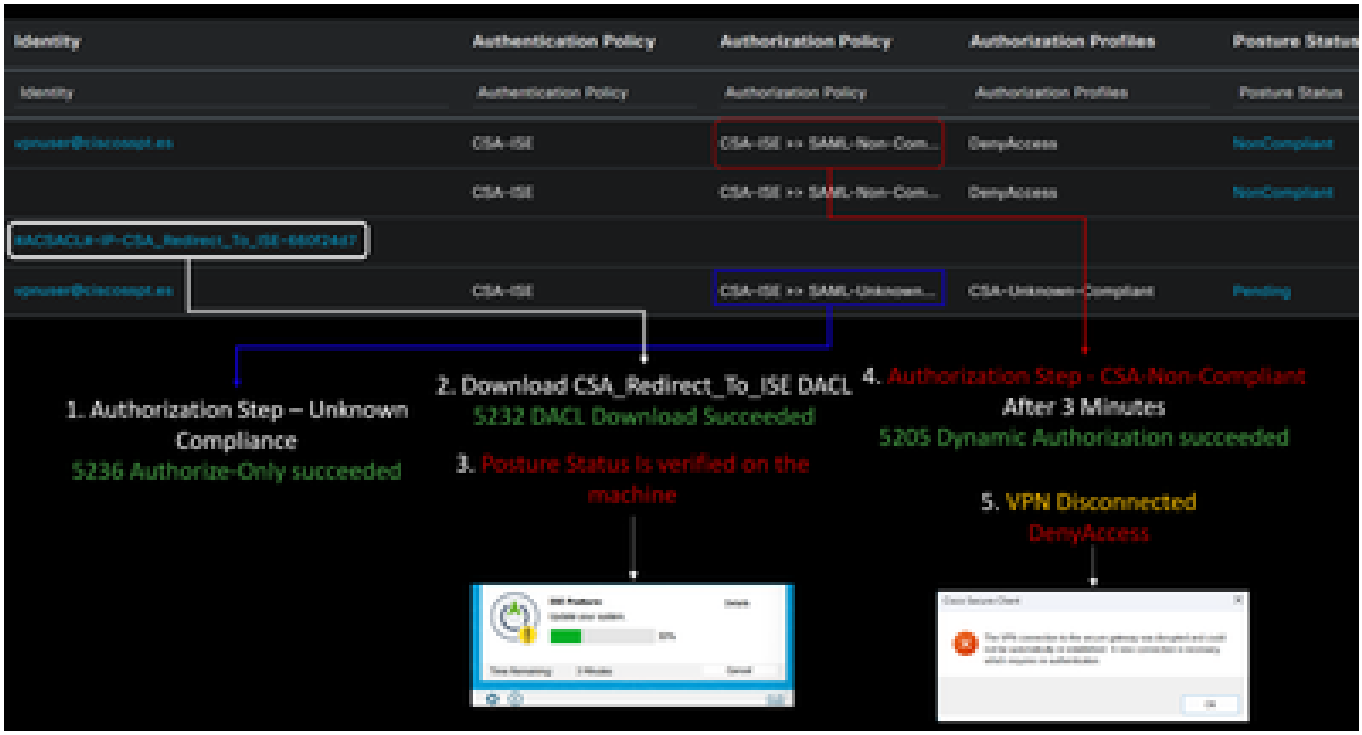

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status is verified on the machine
4. Authorization Step - CSA-Non-Compliant
After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected
DenyAccess

Observação: se vocêCancel ou o tempo restante terminar, você se tornará automaticamente não compatível, se enquadra no conjunto de políticas de autorização CSA-Não-Conformidade **e será imediatamente desconectado da VPN.**

9. Instale o Secure Endpoint Agent e conecte novamente à VPN.



10. Depois que o agente verifica se a máquina está em conformidade, sua postura muda para não receber reclamações e dar acesso a todos os recursos da rede.

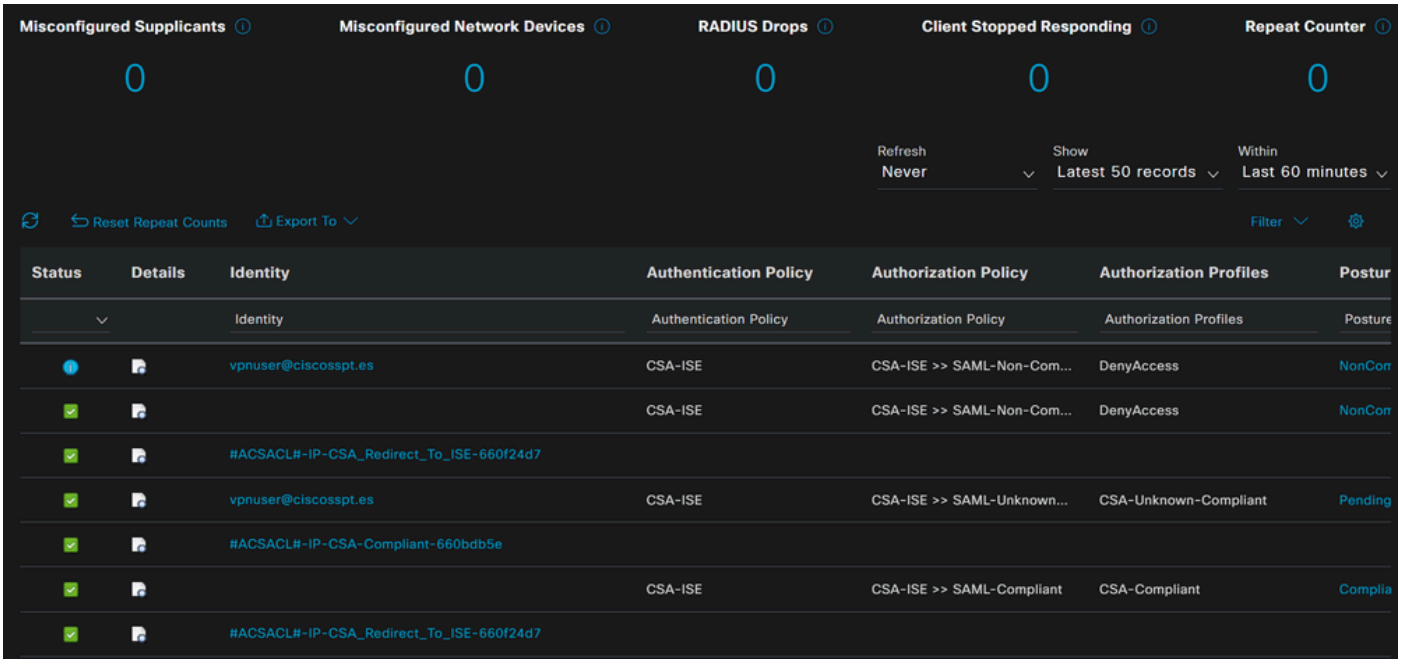


Observação: depois de se tornar compatível, você se enquadra no conjunto de políticas de autorização CSA-Compliance e tem acesso imediato a todos os seus recursos de rede.

Como verificar registros no ISE

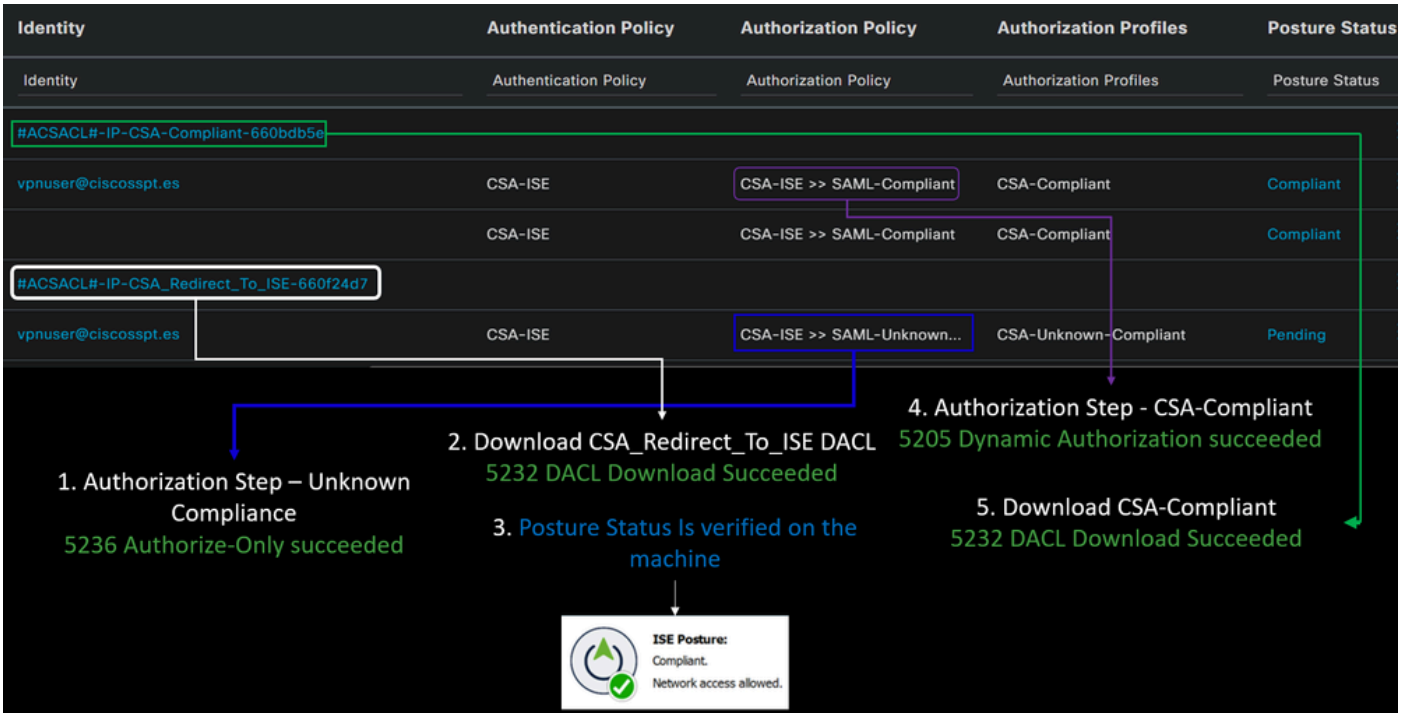
Para verificar o resultado da autenticação para um usuário, você tem dois exemplos de conformidade e não conformidade. Para revisá-lo no ISE, siga estas instruções:

- Navegue até o painel do ISE
- Clique em Operations > Live Logs

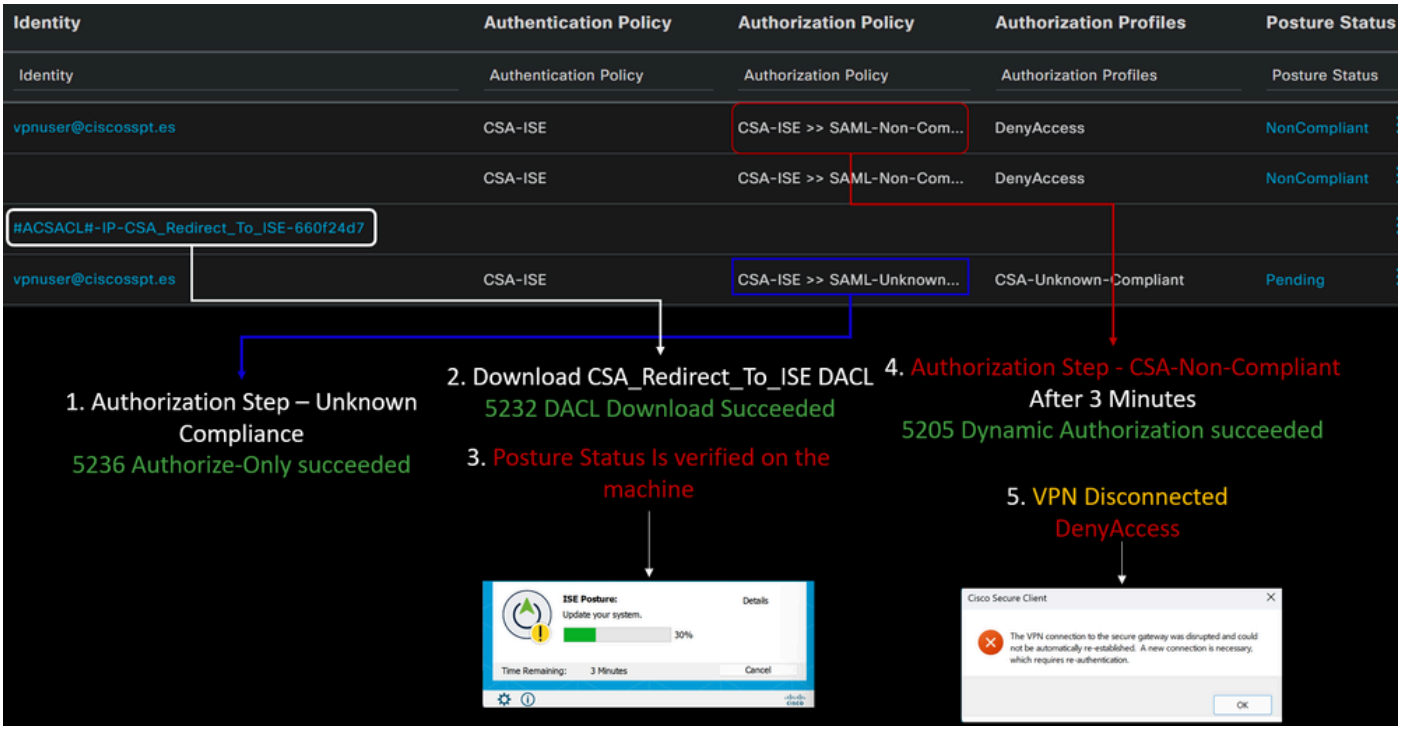


O próximo cenário demonstra como os eventos de conformidade e não-conformidade bem-sucedidos são exibidos em **Live Logs**:

Conformidade



Não-conformidade



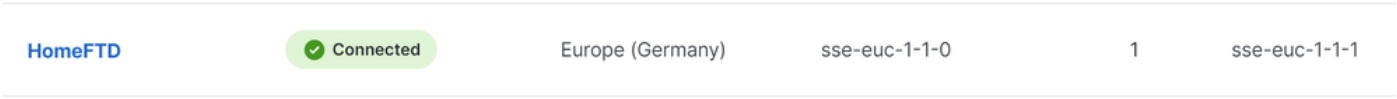
Primeiras etapas com acesso seguro e integração do ISE

No próximo exemplo, o Cisco ISE está na rede 192.168.10.0/24, e a configuração das redes alcançáveis através do túnel precisa ser adicionada na configuração do túnel.

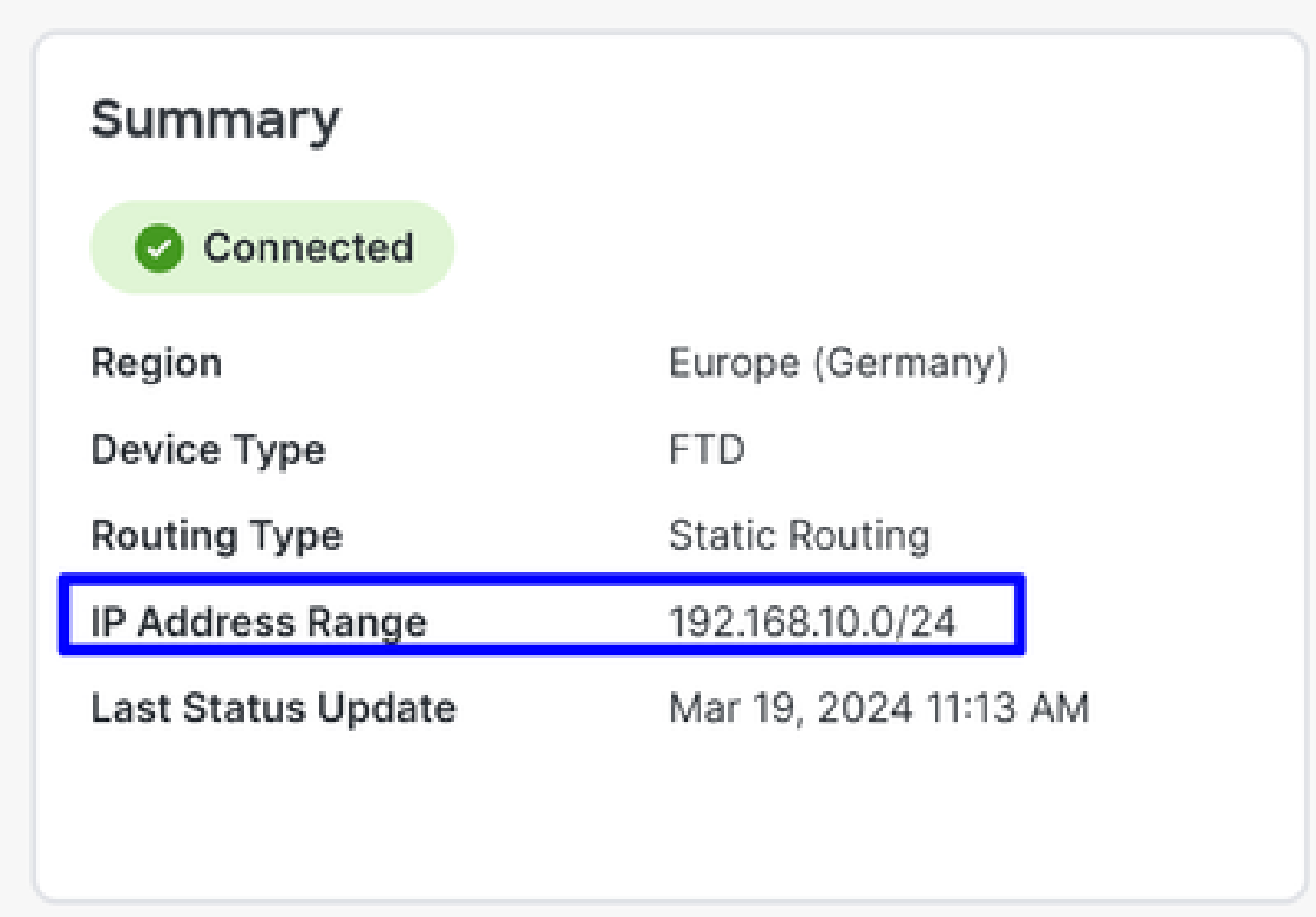
Step 1: Verifique a configuração do túnel:

Para verificar isso, navegue até o [Painel de acesso seguro](#).

- Clique em **Connect > Network Connections**
- Clique em **Network Tunnel Groups** > Your Tunnel



- Em resumo, verifique se o túnel configurou o espaço de endereço onde o Cisco ISE está:

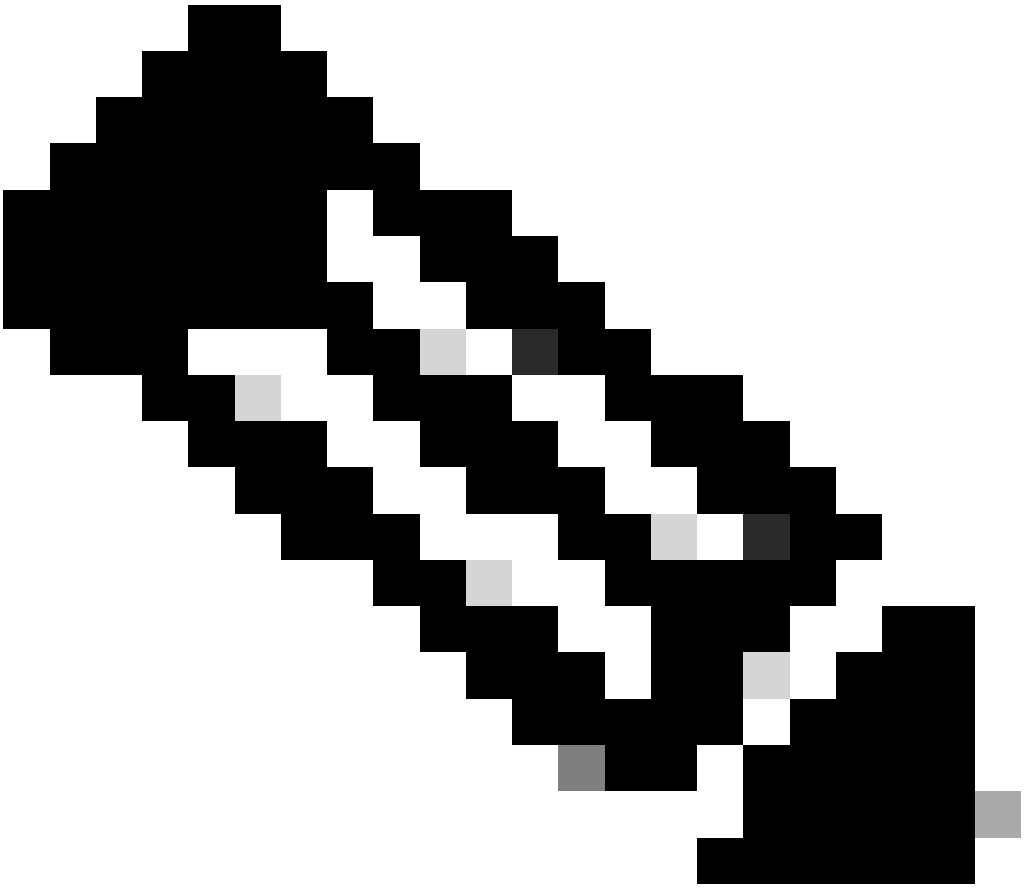


Step 2: permita o tráfego no seu firewall.

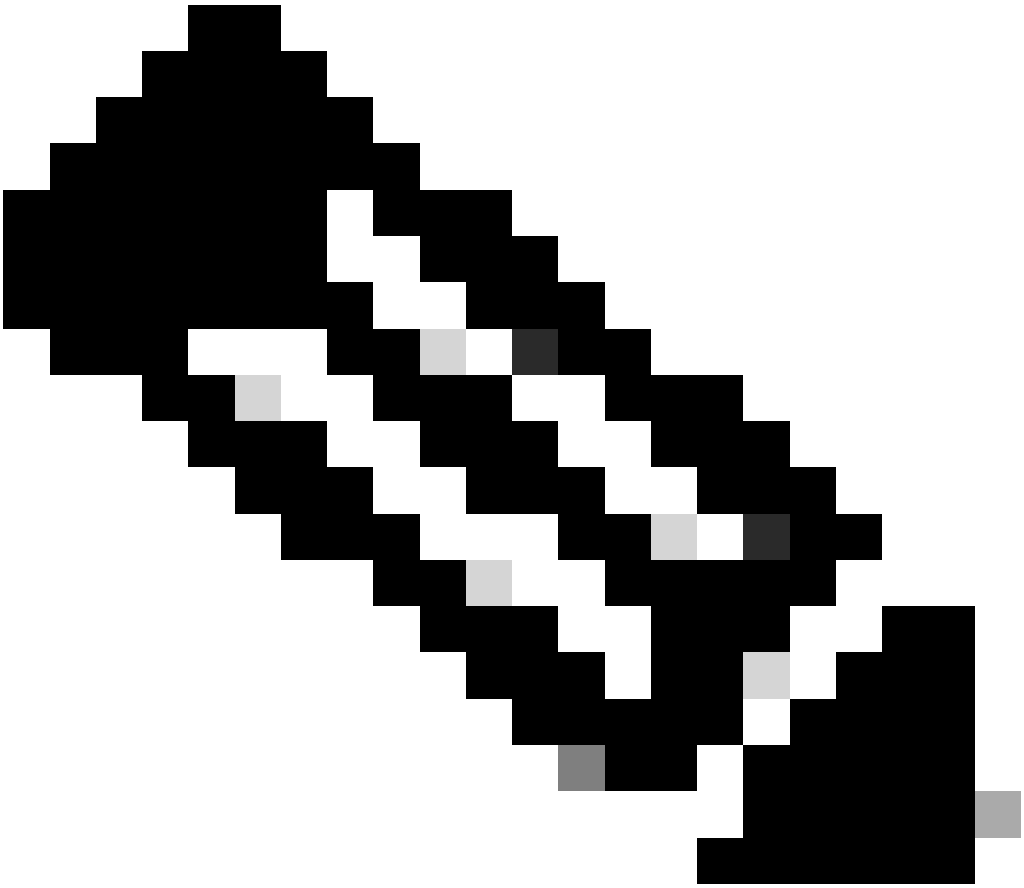
Para permitir o acesso seguro para usar seu dispositivo ISE para autenticação Radius, você precisa ter configurado uma regra de acesso seguro à sua rede com as portas Radius necessárias:

Regra	Fonte	Destino	Porta de Destino
ISE para acesso seguro **Pool de Gerenciamento**	Servidor_ISE	Pool de IPs de Gerenciamento (RA-VPN)	**COA** UDP 1700 (porta padrão)
Pool IP de gerenciamento de acesso seguro para ISE	Pool de IPs de Gerenciamento	Servidor_ISE	**Autenticação, autorização** UDP 1812 (Porta padrão) **Relatório** UDP 1813 (Porta padrão)
Pool de IPs de Ponto de Extremidade de Acesso Seguro para ISE	Pool de IPs de Ponto de Extremidade	Servidor_ISE	**Portal de provisionamento** TCP 8443 (Porta Padrão)

Pool IP de Ponto de Extremidade de Acesso Seguro para SERVIDOR DNS	Pool de IPs de Ponto de Extremidade	Servidor DNS	**DNS** UDP e TCP 53



Observação: se quiser saber mais sobre portas relacionadas ao ISE, consulte o Guia do usuário - Referência de porta.



Observação: uma regra DNS é necessária se você tiver configurado seu ISE para ser descoberto através de um nome, como ise.ciscosspt.es

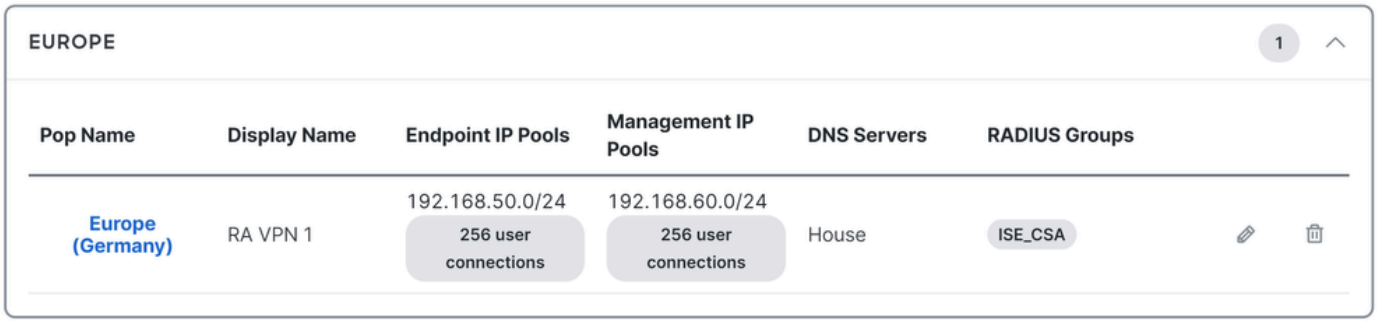
Pool de gerenciamento e pools de endpoints IP

Para verificar o pool de IPs de gerenciamento e endpoint, navegue até o painel de controle de acesso seguro:

- Clique em **Connect > End User Connectivity**
- Clique em Virtual Private Network

- Sob **Manage IP Pools**

- Clique em **Manage**



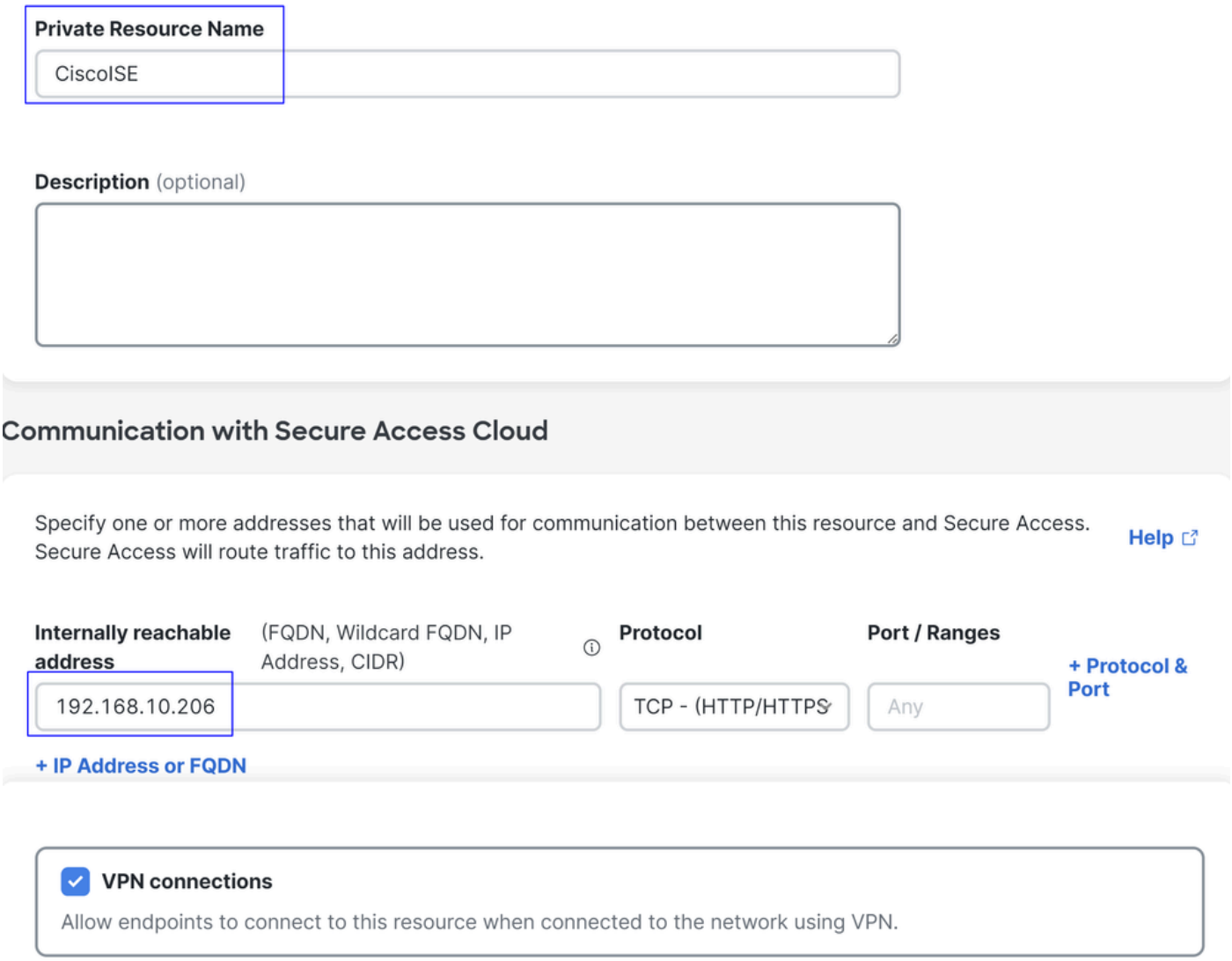
Etapa 3: Verifique se o ISE está configurado em Recursos privados

Para permitir que os usuários conectados por meio da VPN naveguem para o **ISE Provisioning Portal**, você precisa ter certeza de que configurou seu dispositivo como um recurso privado para fornecer acesso, que é usado para permitir o provisionamento automático do ISE Posture Module por meio da VPN.

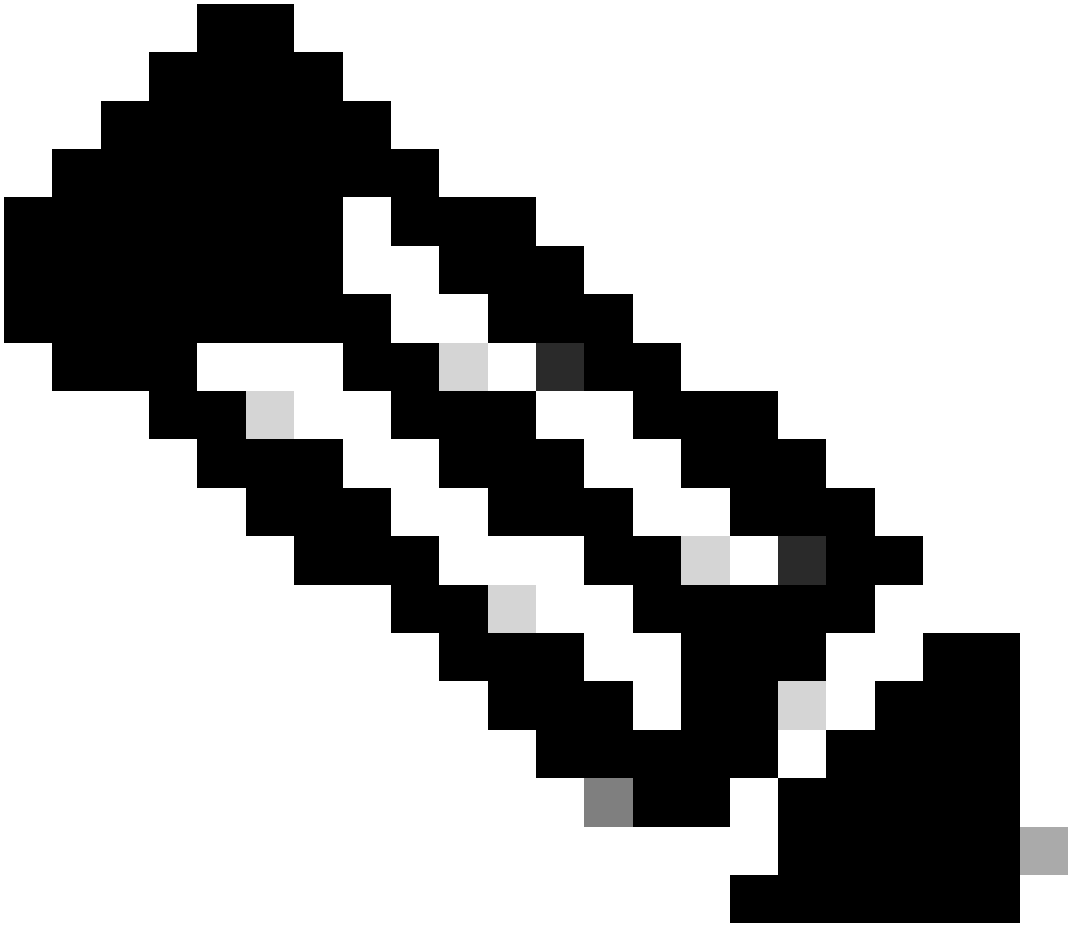
Para verificar se você tem o ISE configurado corretamente, navegue até o Painel de acesso seguro:

- Clique em **Resources > Private Resources**

- Clique no ícone ISE Resource



Se necessário, você pode restringir a regra à porta do portal de provisionamento (8443).



Observação: certifique-se de marcar a caixa de seleção para conexões VPN.

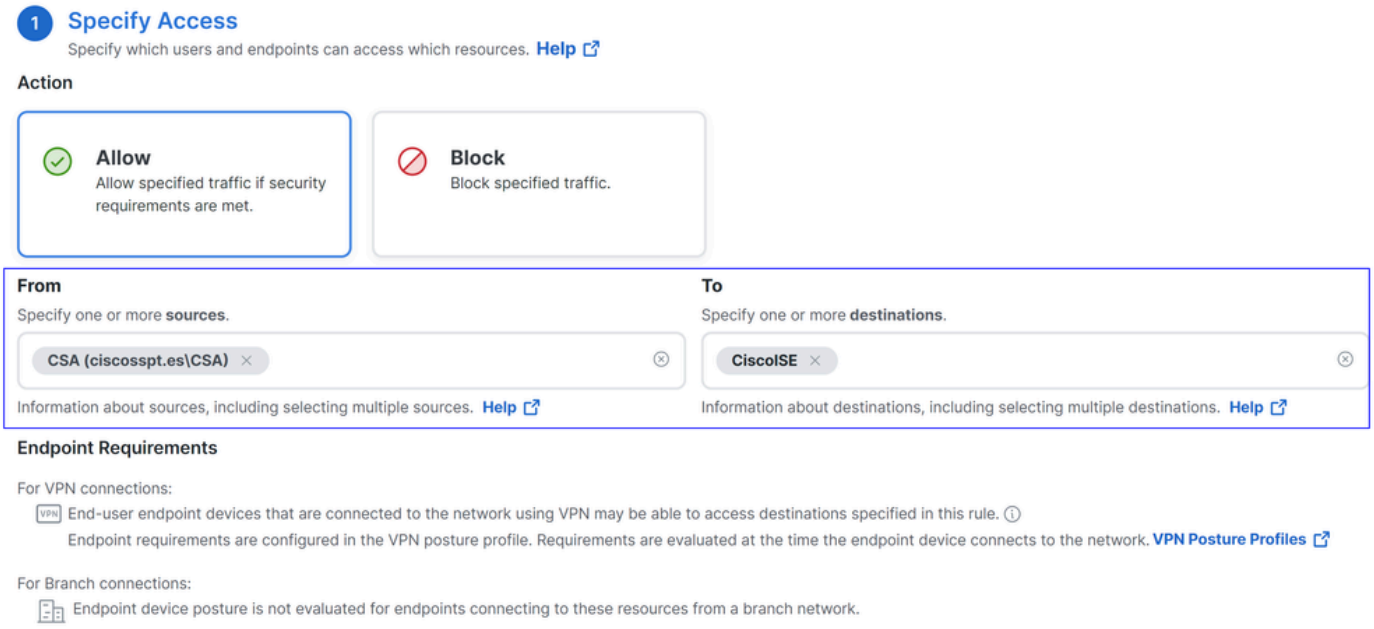
Etapa 4: Permitir o acesso ao ISE sob a política de acesso

Para permitir que os usuários conectados por meio da VPN naveguem até **ISE Provisioning Portal**o, você precisa ter certeza de que configurou um **Access Policy** para permitir que os usuários configurados sob essa regra acessem o recurso privado configurado no Step3.

Para verificar se você tem o ISE configurado corretamente, navegue até o Painel de acesso seguro:

- Clique em **Secure > Access Policy**

- Clique na regra configurada para permitir o acesso aos usuários VPN ao ISE

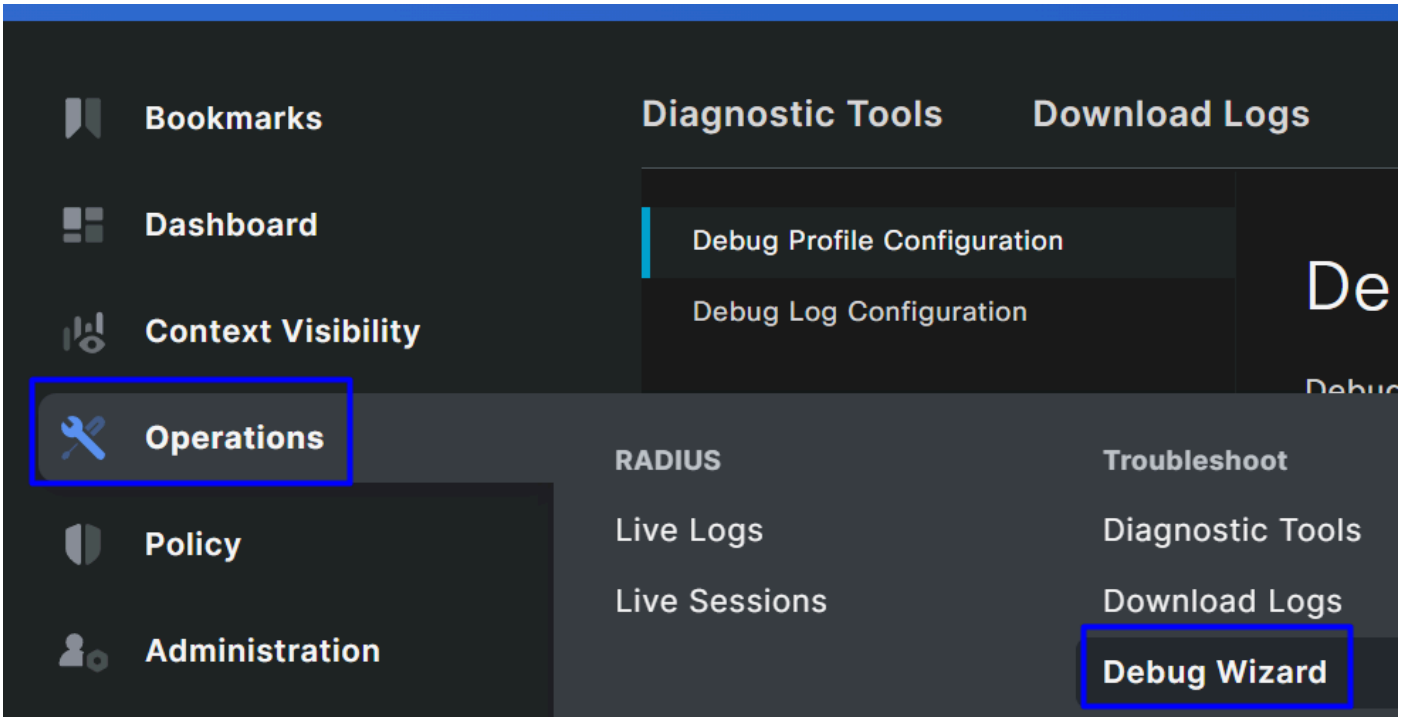


Troubleshooting

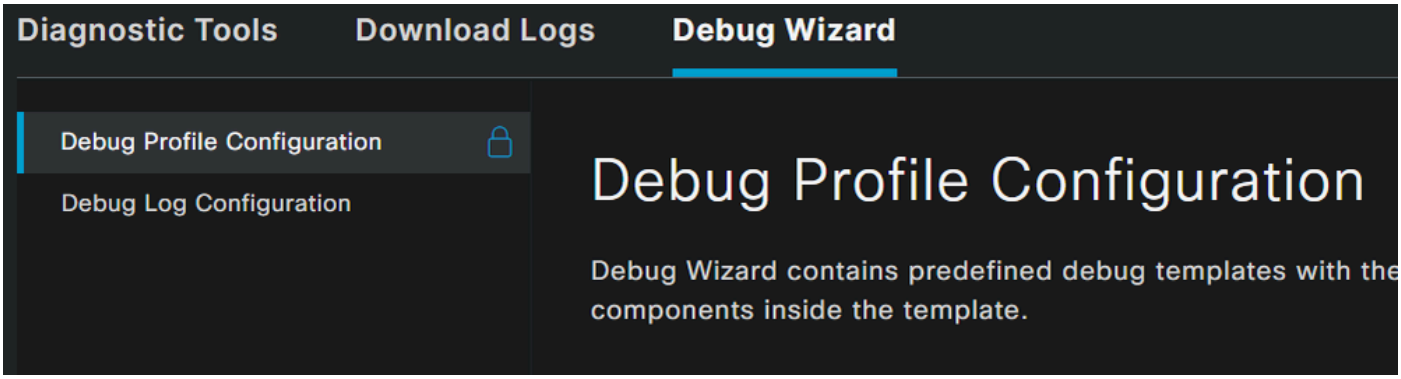
Como baixar logs de depuração de postura do ISE

Para fazer o download dos logs do ISE para verificar um problema relacionado à postura, siga as próximas etapas:

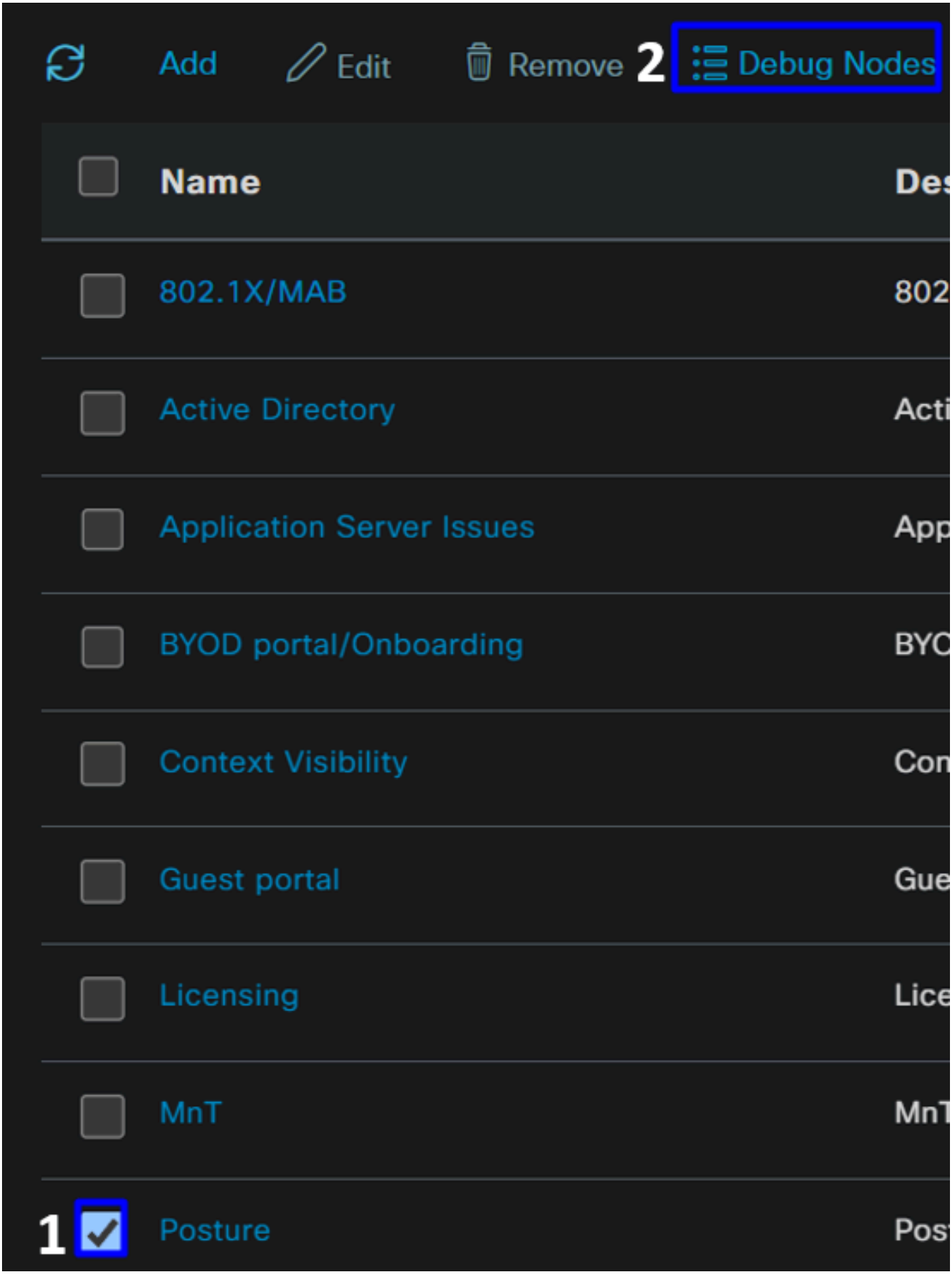
- Navegue até o painel do ISE
- Clique em Operations > Troubleshoot > Debug Wizard



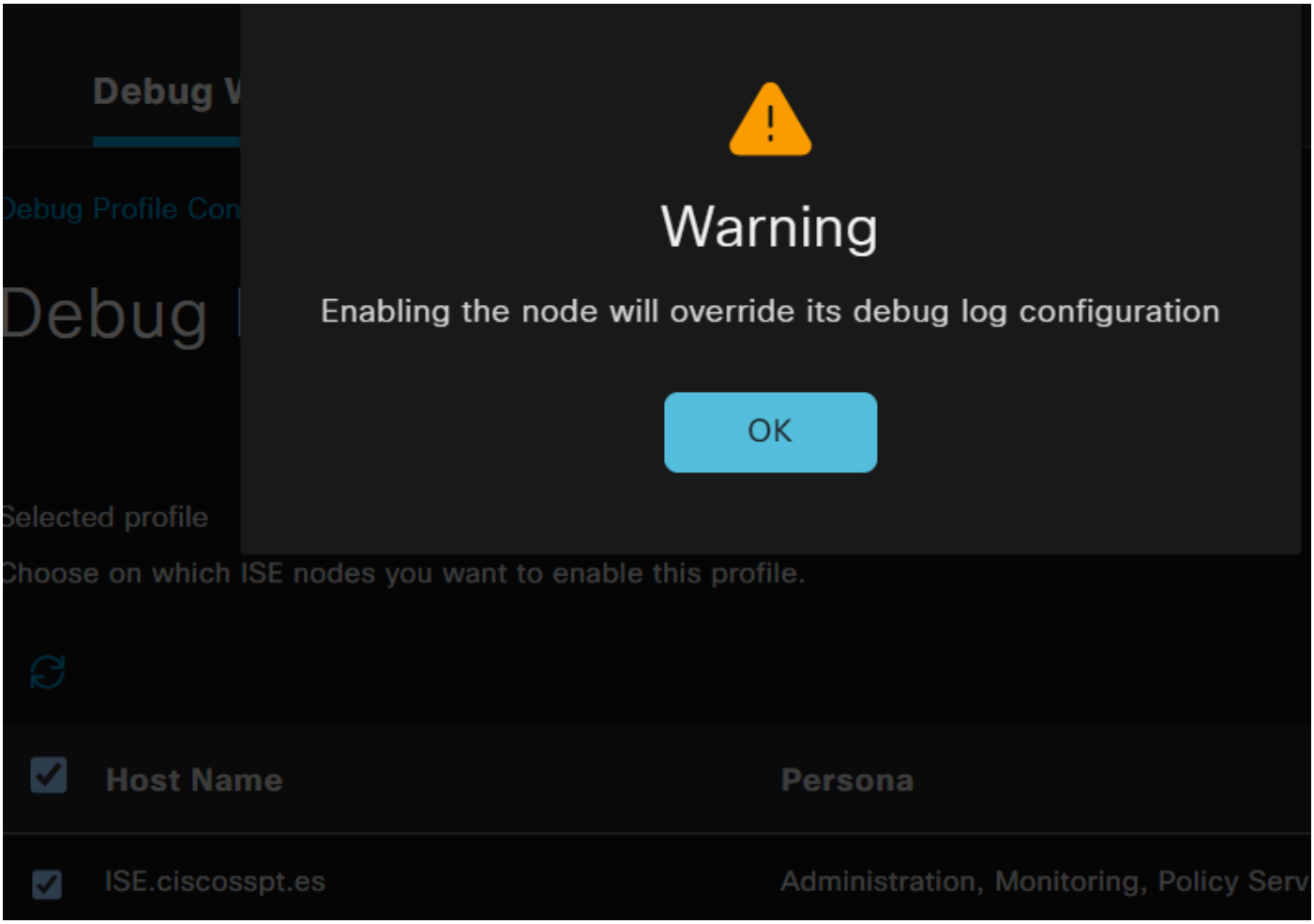
- Clique em Debug Profile Configuration



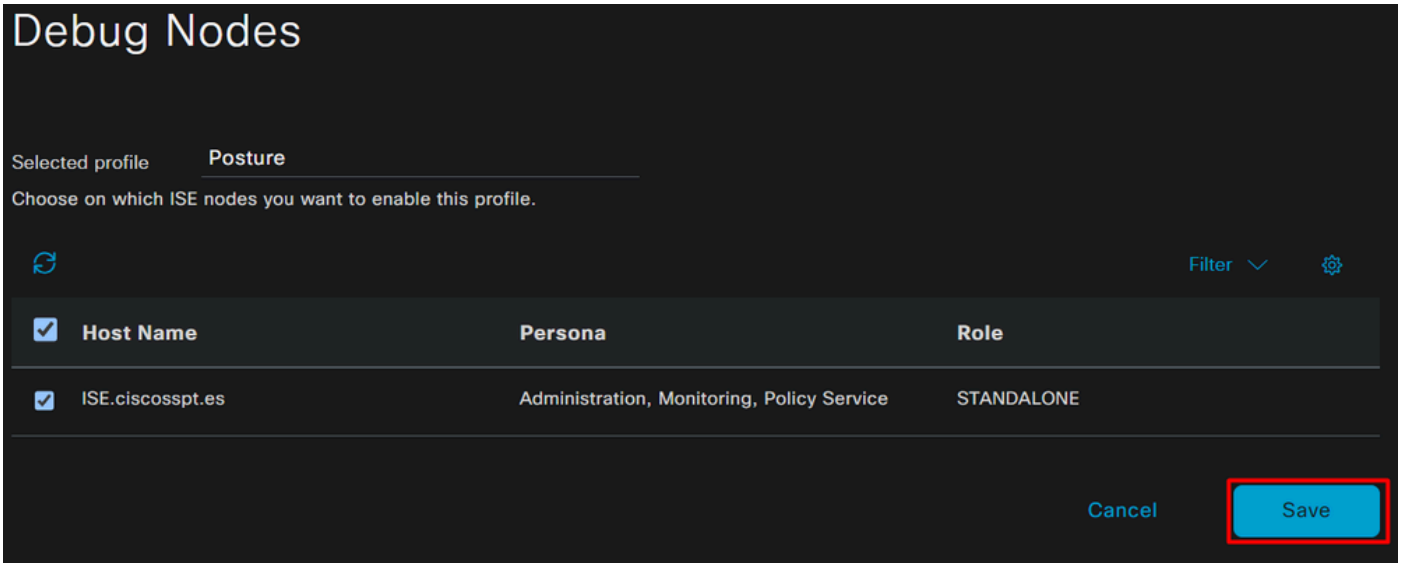
- Marcar a caixa de seleção para **Posture > Debug Nodes**

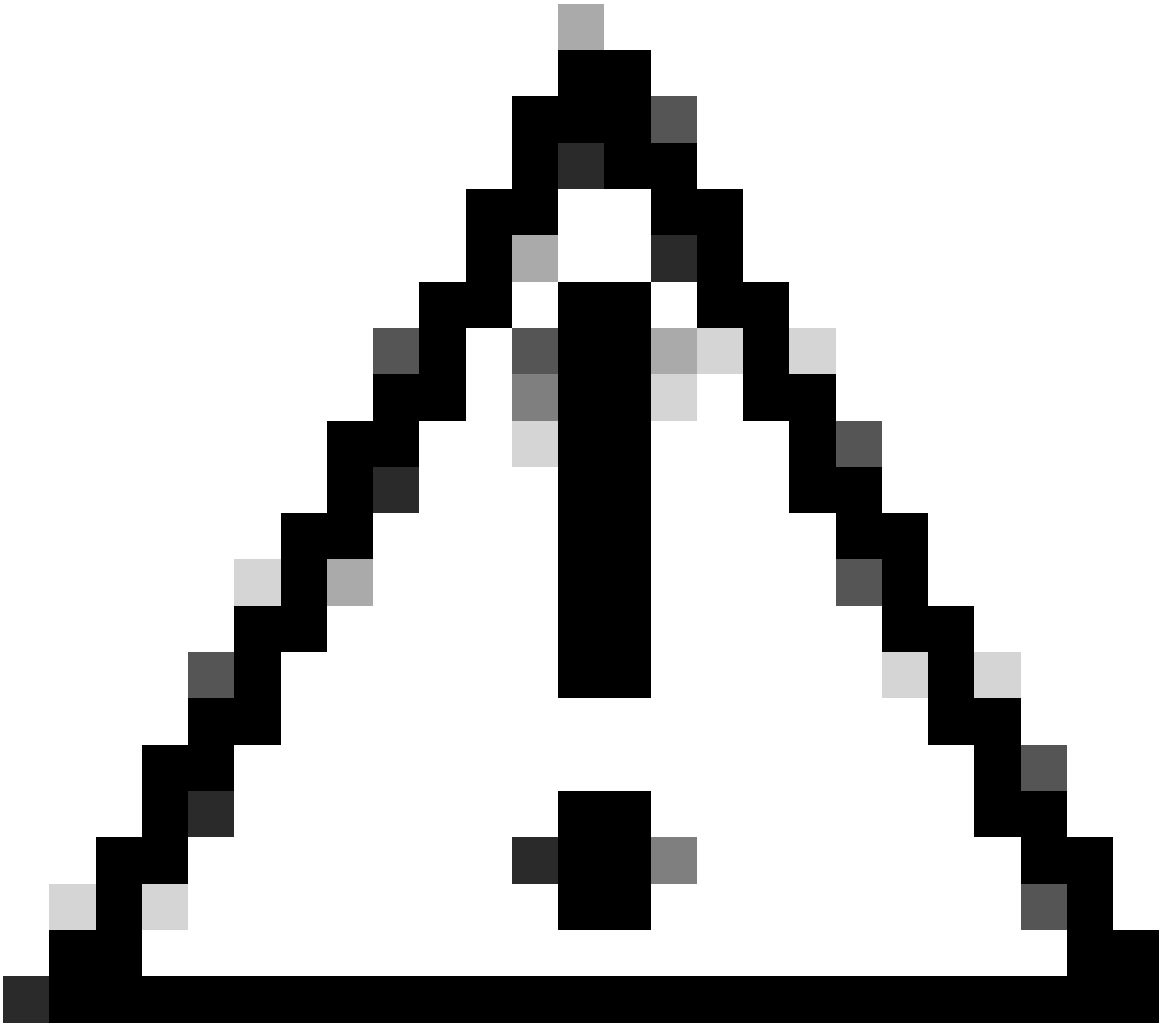

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- Marque a caixa de seleção dos nós do ISE nos quais você está habilitando o modo de depuração para solucionar o problema



- Clique em Save

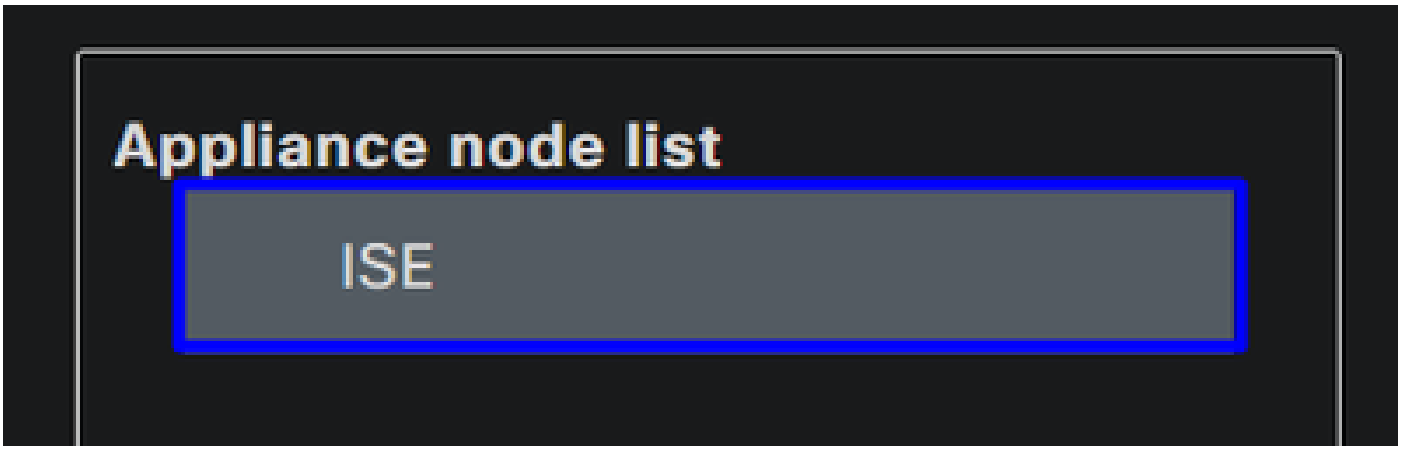

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



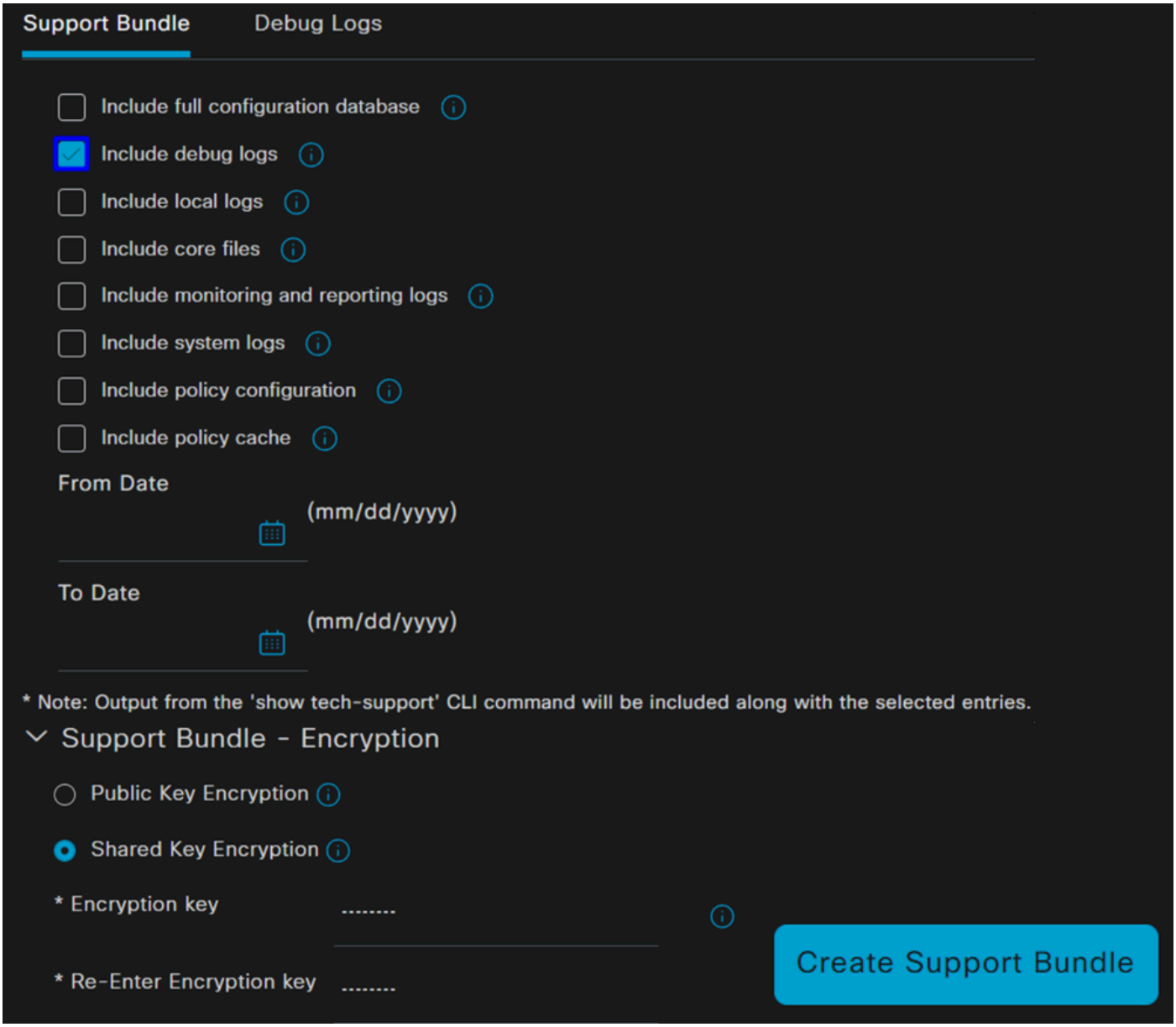
Cuidado: depois desse ponto, você deve começar a reproduzir o problema; **the debug logs can affect the performance of your device**.

Depois que o problema for reproduzido, continue com as próximas etapas:

- Clique em Operations > Download Logs
- Escolha o nó de onde deseja obter os logs

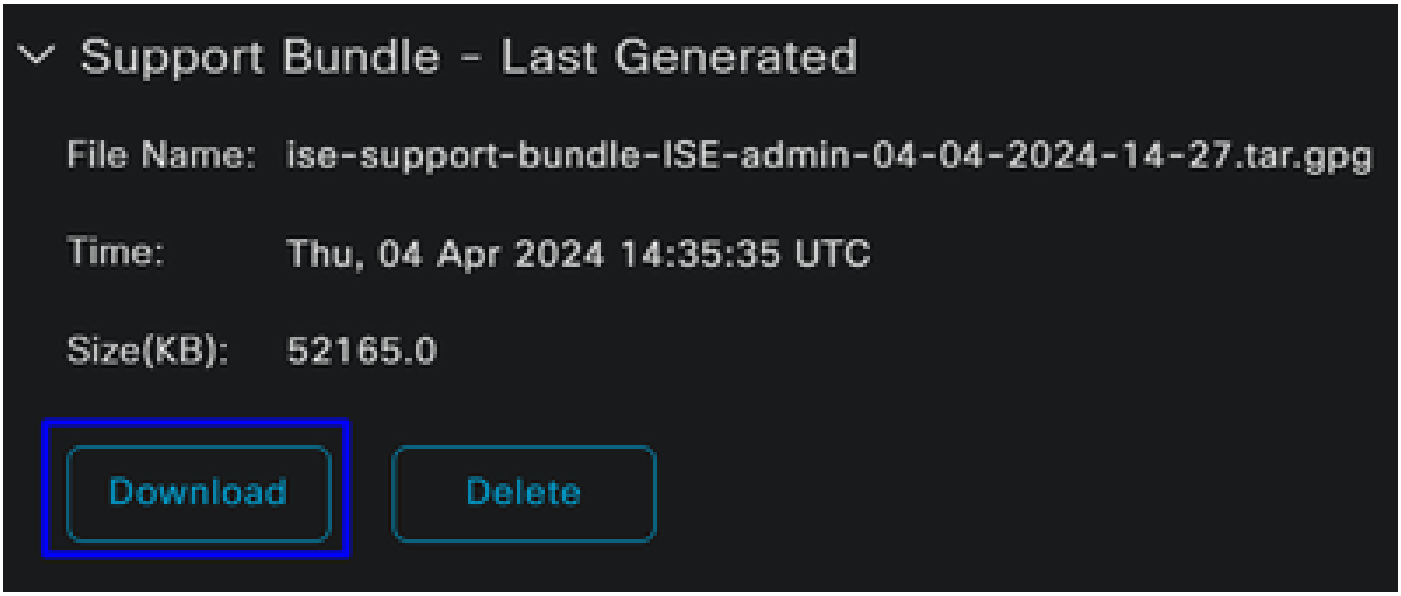


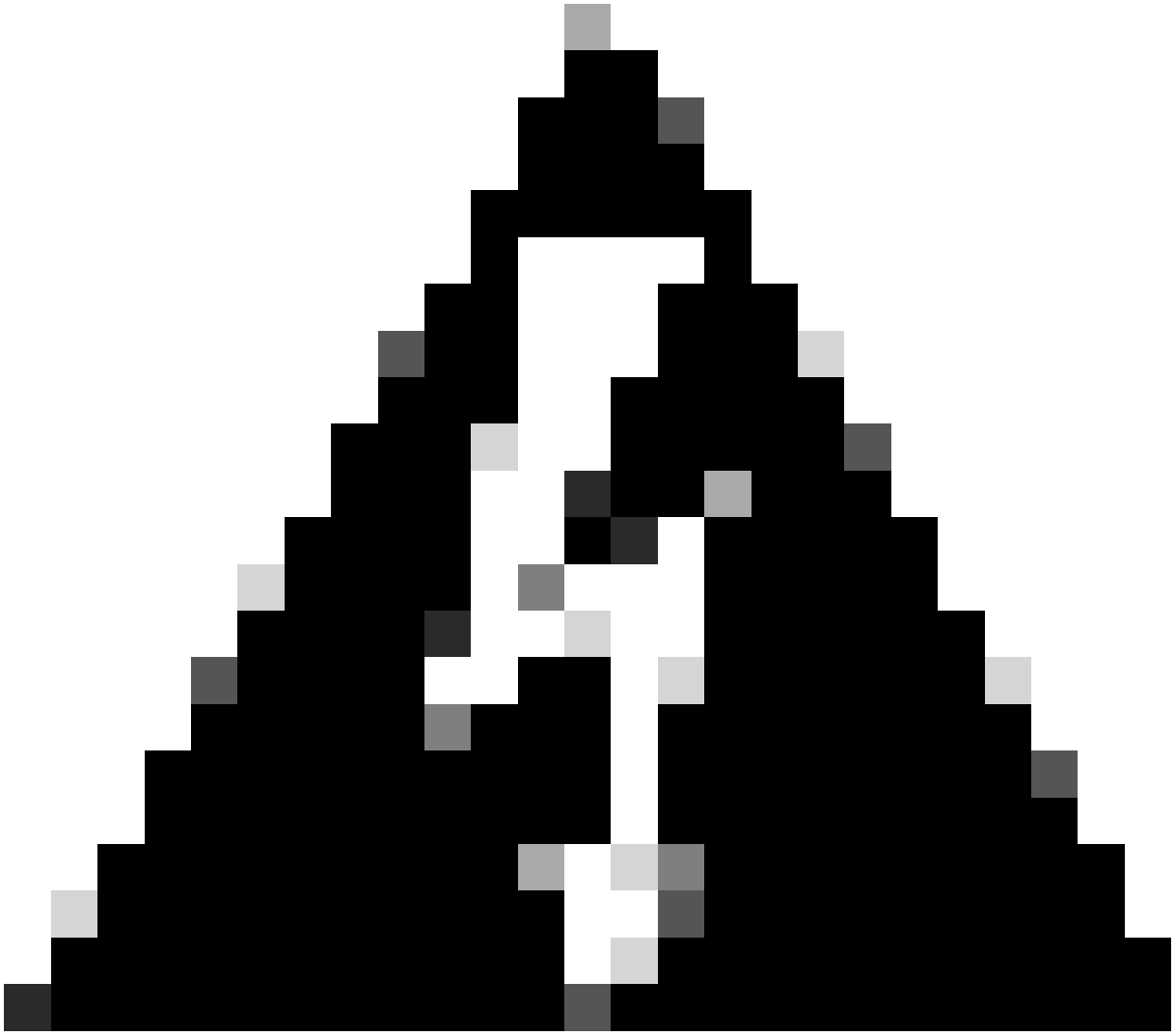
- Em **Support Bundle**, escolha as próximas opções:



- Include debug logs
- Sob **Support Bundle Encryption**
    - **Shared Key Encryption**
        - Preenchimento **Encryption key** e **Re-Enter Encryption key**

- Clique em **Create Support Bundle**
- Clique em **Download**





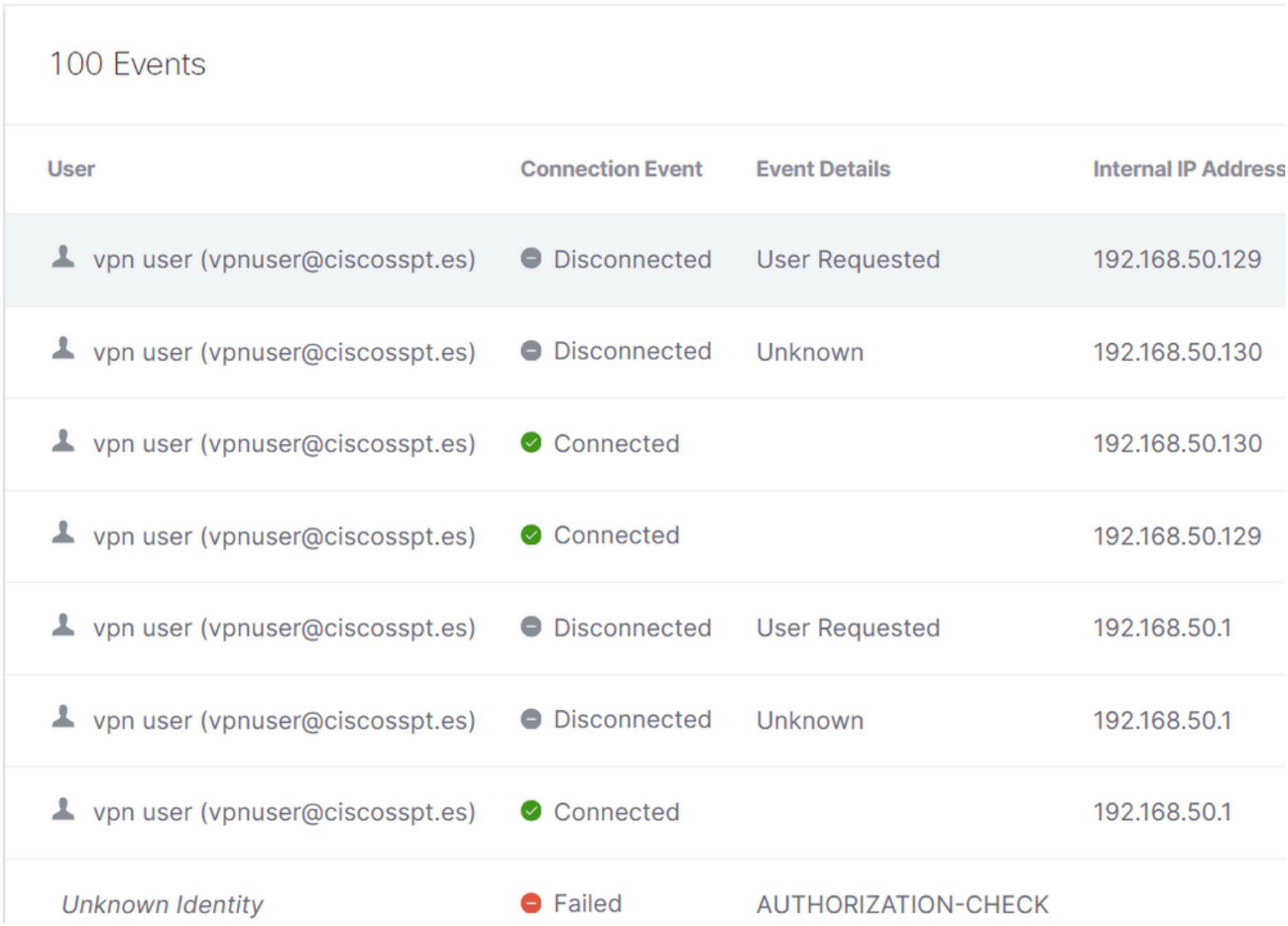
Aviso: Desative o modo de depuração ativado na etapa, Depurar Configuração de Perfil

---

Como verificar os registros de acesso remoto seguro

Navegue até o Painel do Secure Access:

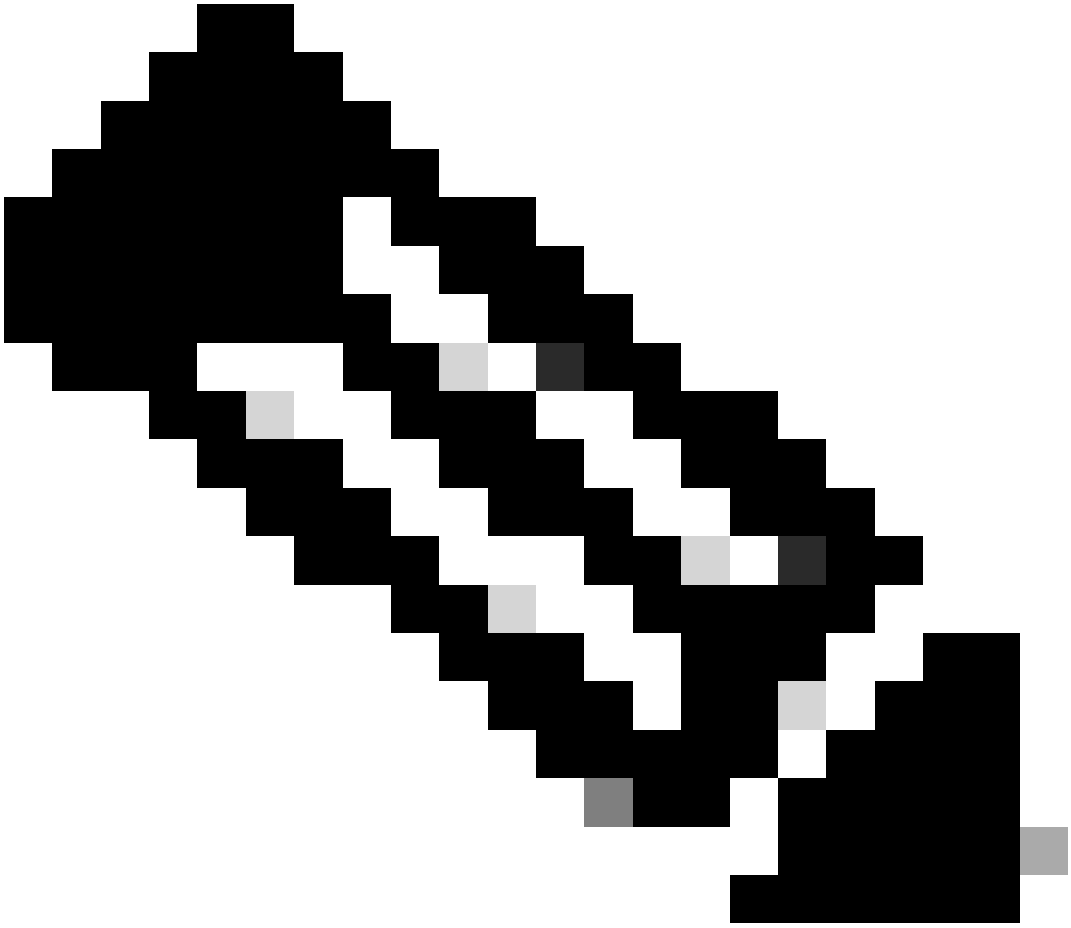
- Clique em Monitor > Remote Access Logs



Gerar pacote DART no cliente seguro

Para gerar um pacote DART em sua máquina, verifique o próximo artigo:

Ferramenta de Diagnóstico e Relatórios do Cisco Secure Client (DART)



Observação: depois de coletar os logs indicados na seção de solução de problemas, abra um caso com **TAC** o para continuar com a análise das informações.

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**
- **Documentação e Guia do Usuário do Secure Access**

- **Download do software Cisco Secure Client**
- **Guia do Administrador do Cisco Identity Services Engine, Versão 3.3**

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.