

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configuração Duo](#)

[Configuração de acesso seguro](#)

[Configurar o grupo Radius nos pools IP](#)

[Configure seu perfil VPN para usar o ISE](#)

[Configurações gerais](#)

[Autenticação, autorização e contabilidade](#)

[Direcionamento de tráfego](#)

[Configuração do Cisco Secure Client](#)

[Configurações do ISE](#)

[Configurar lista de dispositivos de rede](#)

[Configurar um grupo](#)

[Configurar Usuário Local](#)

[Configurar Conjunto de Políticas](#)

[Configurar Autorização de Definição de Política](#)

[Configurar usuários locais ou do Active Directory do Radius](#)

[Configurar a postura do ISE](#)

[Configurar Condições de Postura](#)

[Configurar Requisitos de Postura](#)

[Configurar política de postura](#)

[Configurar Provisionamento de Cliente](#)

[Configurar Política de Provisionamento de Cliente](#)

[Criar os perfis de autorização](#)

[Configurar Conjunto de Políticas de Postura](#)

[Verificar](#)

[Validação de postura](#)

[Conexão na máquina](#)

[Como verificar registros no ISE](#)

[Conformidade](#)

[Não-conformidade](#)

[Primeiras etapas com acesso seguro e integração do ISE](#)

[Troubleshooting](#)

[Como baixar logs de depuração de postura do ISE](#)

[Como verificar os registros de acesso remoto seguro](#)

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

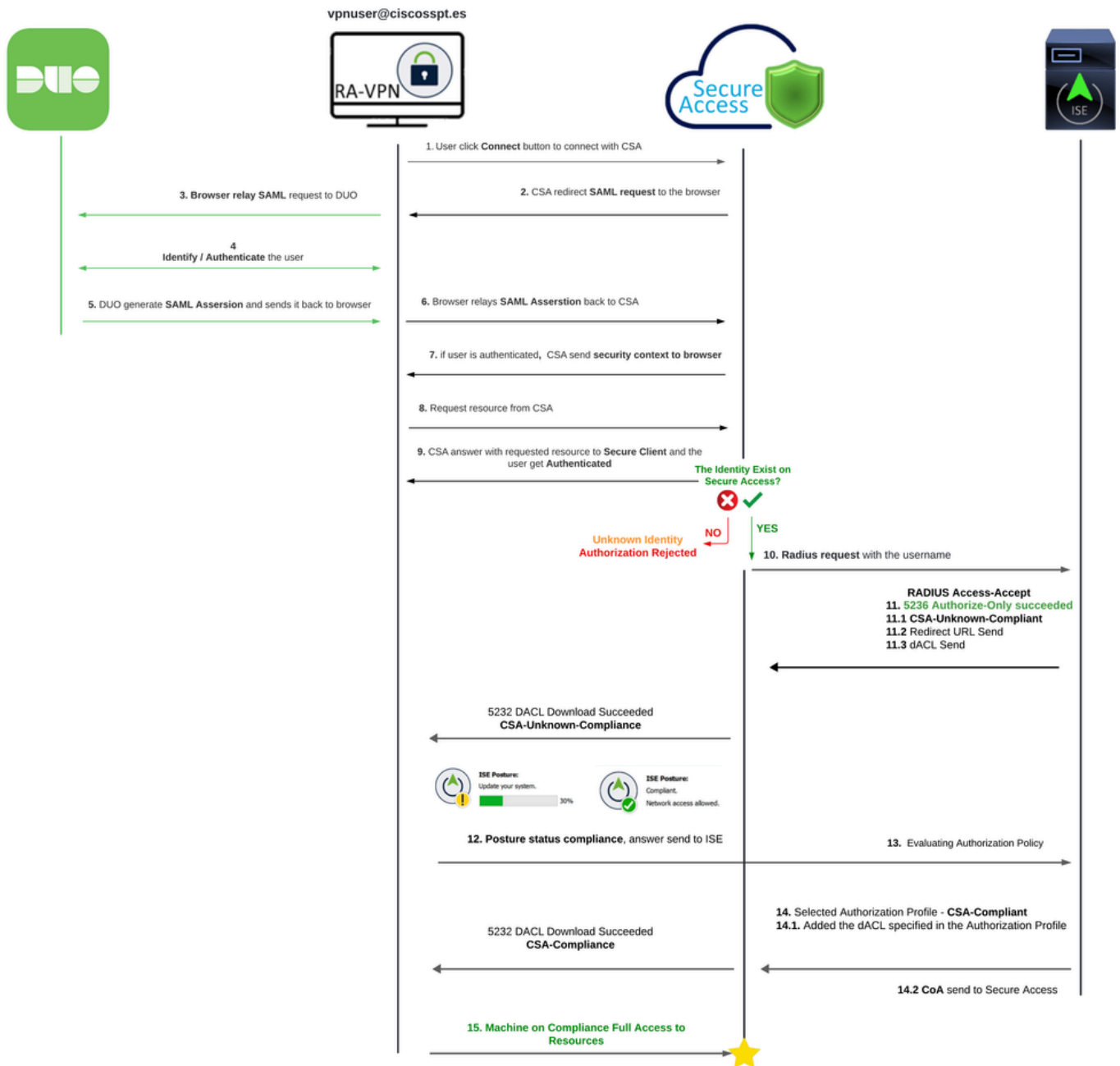
Componentes Utilizados

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

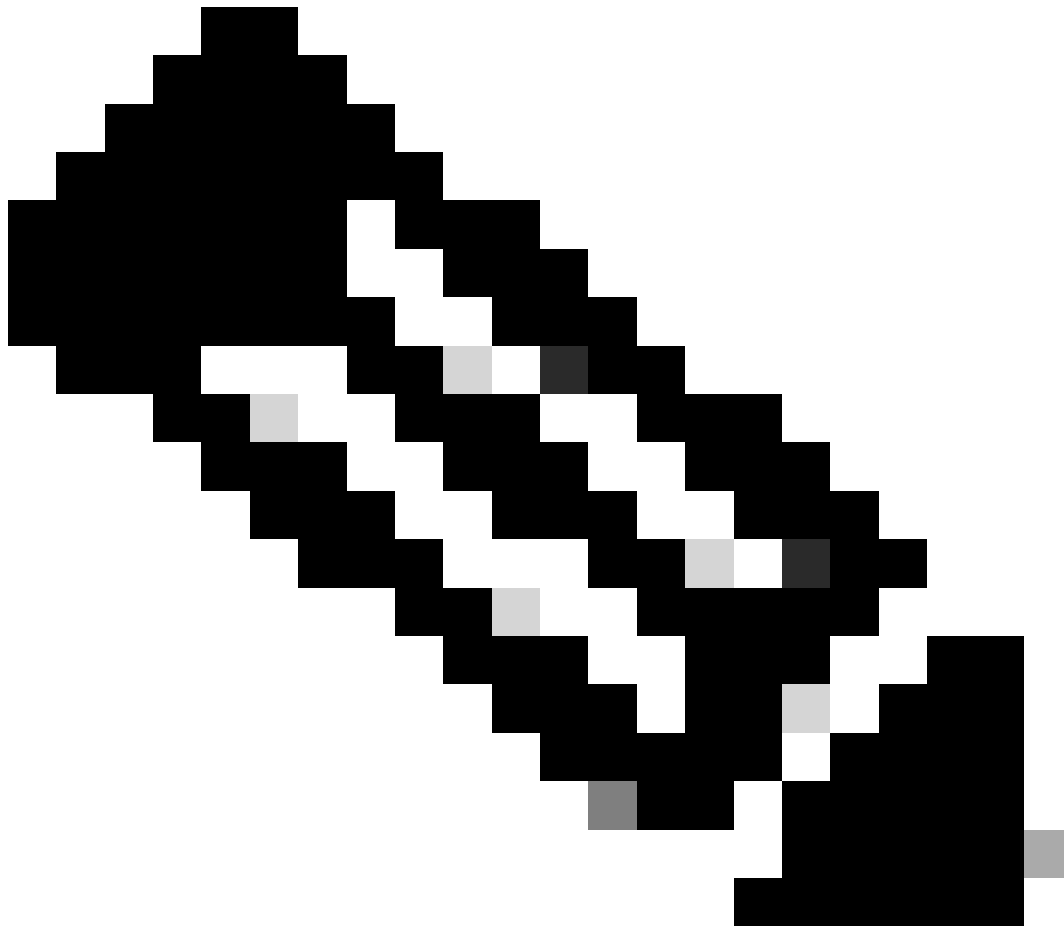
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Informações de Apoio



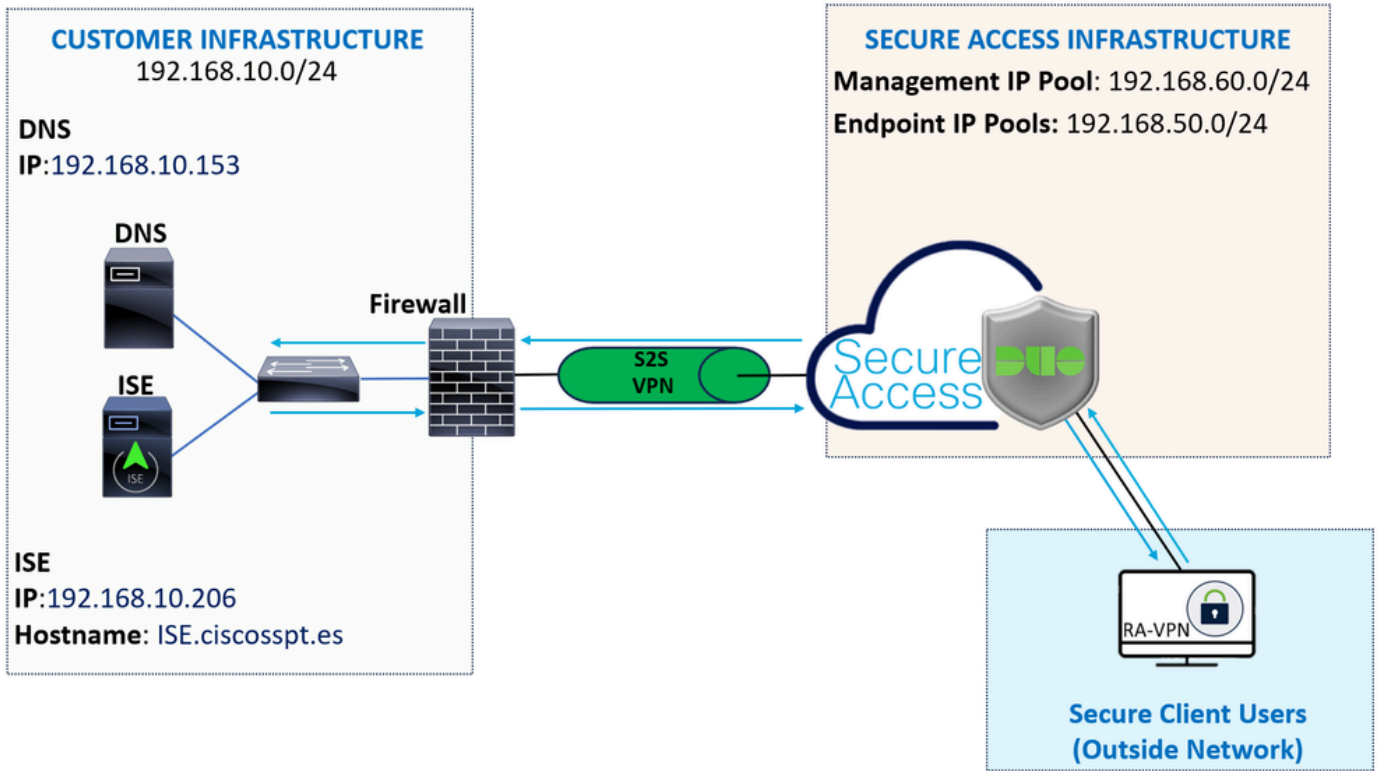
A integração do Duo SAML com o Cisco Identity Services Engine (ISE) aprimora o processo de autenticação, adicionando outra camada de segurança às soluções Cisco Secure Access. O Duo SAML fornece um recurso de Logon Único (SSO) que simplifica o processo de logon do usuário, garantindo altos padrões de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



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**

Protect an Application

Generic SAML Service Provider

Application

Protection Type



Generic SAML Service Provider

2FA with SSO hosted by Duo
(Single Sign-On)

[Documentation](#)

Protect

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

✓ Successfully added Generic SAML Service Provider - Single Sign-On to protected applications.
[Add another.](#)

Dashboard > Applications > Generic SAML Service Provider - Single Sign-On

Generic SAML Service Provider - Single Sign-On

[Authentication Log](#) | [Remove Application](#)

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata	Copy
Single Sign-On URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/sso	Copy
Single Log-Out URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/slo	Copy
Metadata URL	https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata	Copy

Certificate Fingerprints

SHA-1 Fingerprint	05:76:95:6B:E1:7C:F7:D1:79:12:2C:23:B6:1A:63:59:32:01:88:B1	Copy
SHA-256 Fingerprint	CF:CB:25:7C:41:0D:81:49:E5:83:48:79:EA:6B:45:C9:9F:4A:9A:21:A9:72:32:D3:C1:7F:86:4	Copy

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 em **Manage**

Manage IP Pools

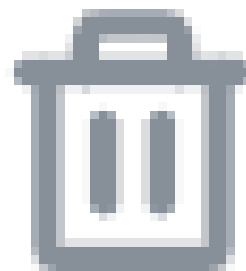
Manage

2 Regions mapped

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

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- Clique no lápis para editar



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

RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



No RADIUS groups created

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 exija Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2), marque a caixa de seleção

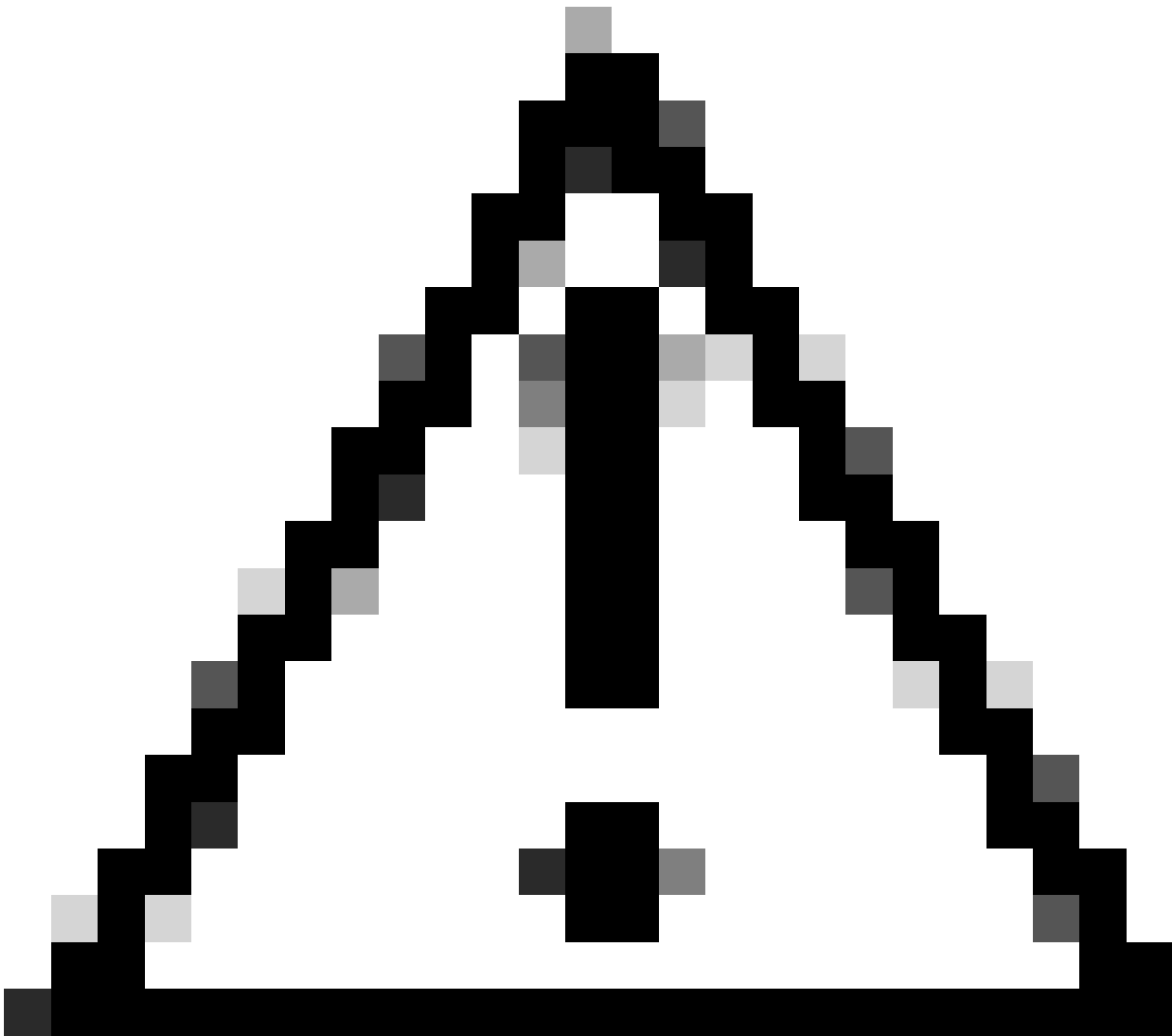
- **Authorization:** Marque a caixa de seleção para Authorization e selecione a porta, por padrão, é 1812

- Marque a caixa de seleção para **Authorization mode Only Change of Authorization (CoA) mode** e para 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

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

#	Server Name	IP Address
---	-------------	------------

- Em seguida, configure as próximas opções:

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Password

Cancel

Save & Add server

Save

- **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:

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- 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

Settings

Type Generic SAML Service Provider - Single Sign-On

Name

ISE - SAML

Duo Push users will see this when approving transactions.

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

ISE - SAML

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>53:0E:25:4F:29:3A:B5:DF:09:A2:0D:BB:08:C7:F6:E8:D9:DB:DE:6B</code>	Copy
SHA-256 Fingerprint	<code>C5:6F:35:44:F8:FC:74:C6:E6:2B:C1:8F:92:9C:E2:80:91:B1:61:C9:75:0B:F9:C5:4B:81:B8:F</code>	Copy

Downloads

Certificate	Download certificate	Copy certificate	Expires: 01-19-2038
SAML Metadata	Download XML		

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

VPN Profile name

ISE_CSA_SAML

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPsec (IKEv2)
- 2 Authentication, Authorization, and Accounting SAML**
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 1 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authenticate with CA certificates
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

SAML Metadata XML Configuration

 **1. Download Service Provider XML file**
This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

 **2. Generate IdP Security Metadata XML File**
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

 **3. Upload IdP security metadata XML file**

✓ File 'ISE - SAML - IDP Metadata.xml' uploaded. [Replace](#) [Delete](#)

Manual Configuration

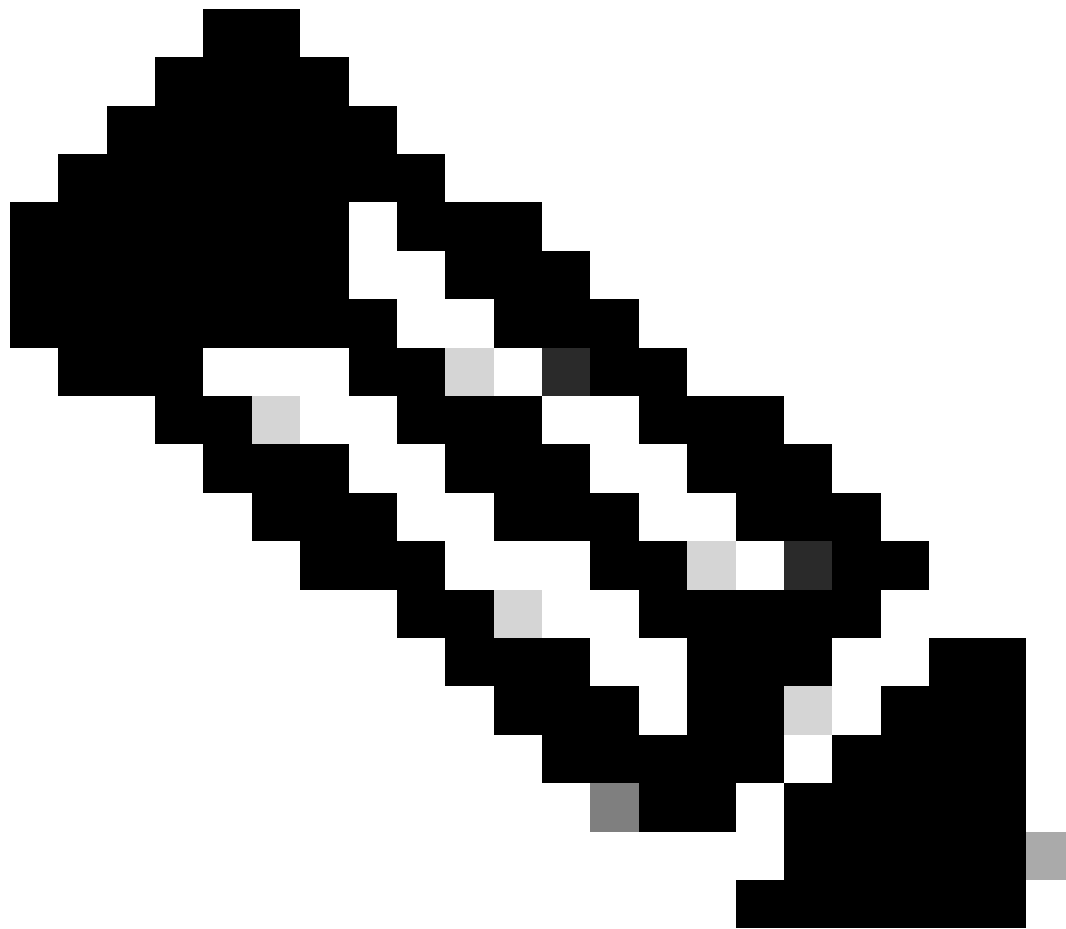


Cancel

Back

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

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

Enable Radius Authorization

Use defaults or customize groups to map to regions

Select one group for all regions

+ Group

ISE_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

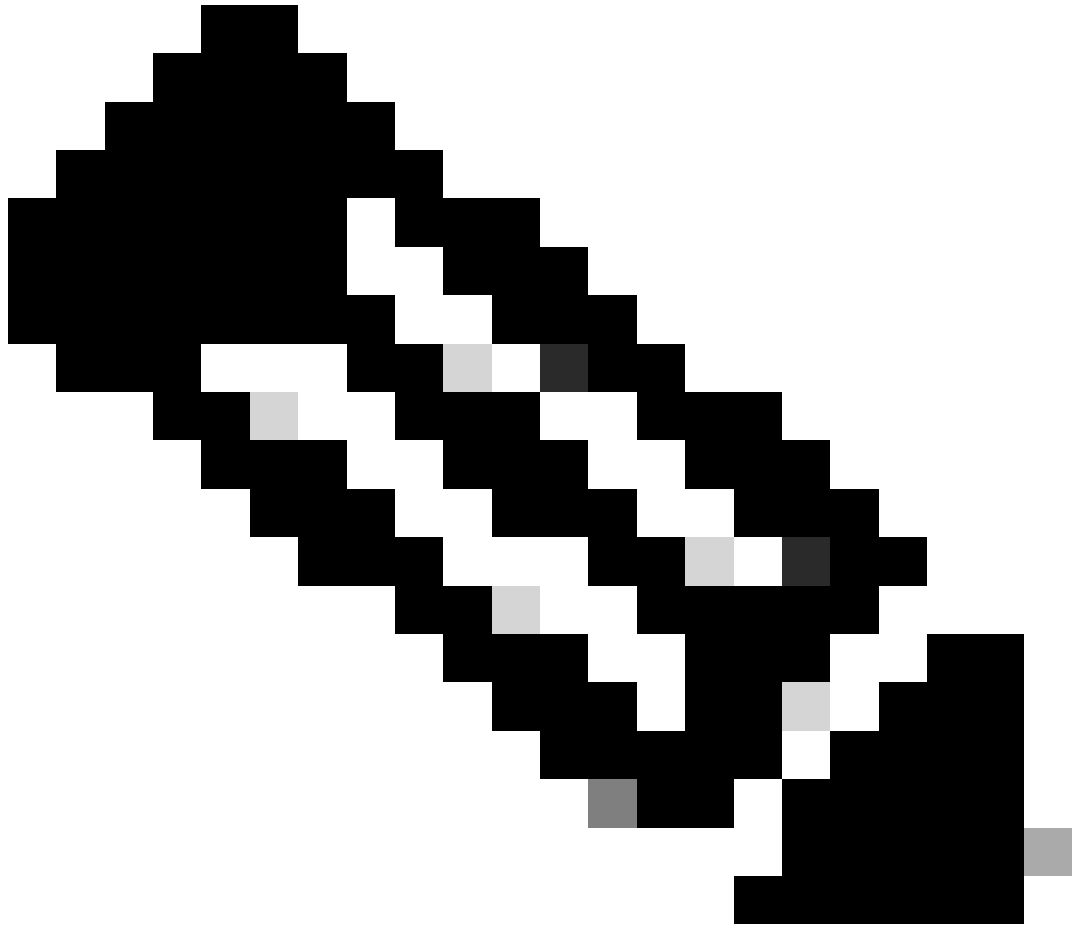
- **Authorization**

- **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

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Enable Radius Accounting

Use defaults or customize groups to map to regions

Select one group for all regions

[+ Group](#)

ISE_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

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

- Clique em **Next**

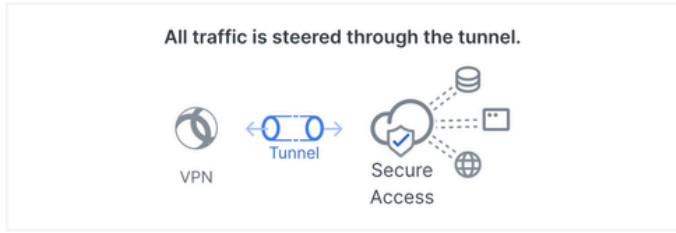
After you have done configured the Authentication, Authorization and Accounting continue com Traffic Steering.

Direção de tráfego

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

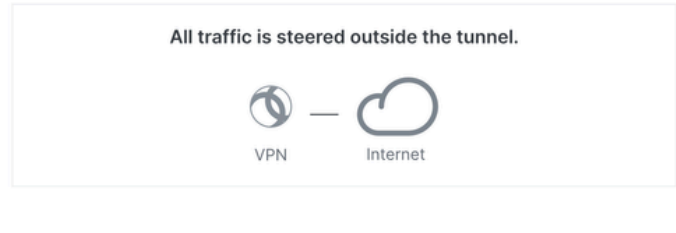
Tunnel Mode

Connect to Secure Access



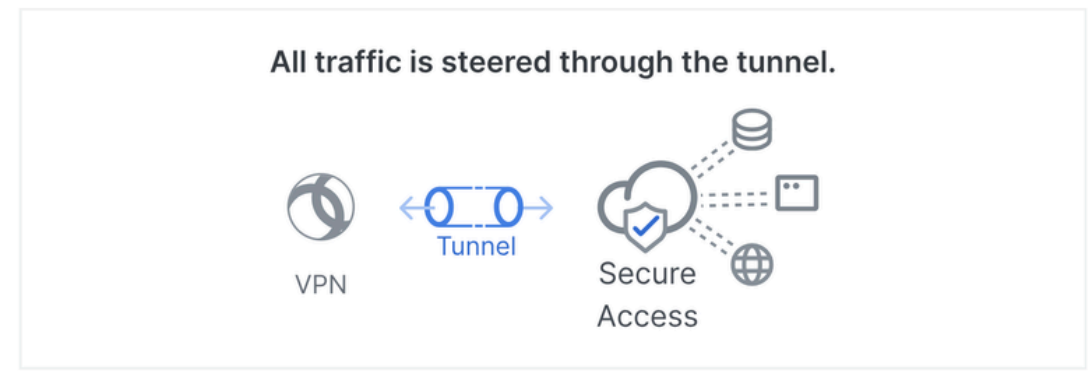
Tunnel Mode

Bypass Secure Access



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

Connect to Secure Access



Add Exceptions

Destinations specified here will be steered **OUTSIDE** the tunnel.

+ Add

Destinations	Exclude Destinations	Actions
proxy-8195126.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sseposture-routing-commercial.posture.duosecurity.com, data.eb.thousandeyes.	-	-

Cancel

Back Next

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 pelo Secure Access (Sem proteção da Internet)

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions

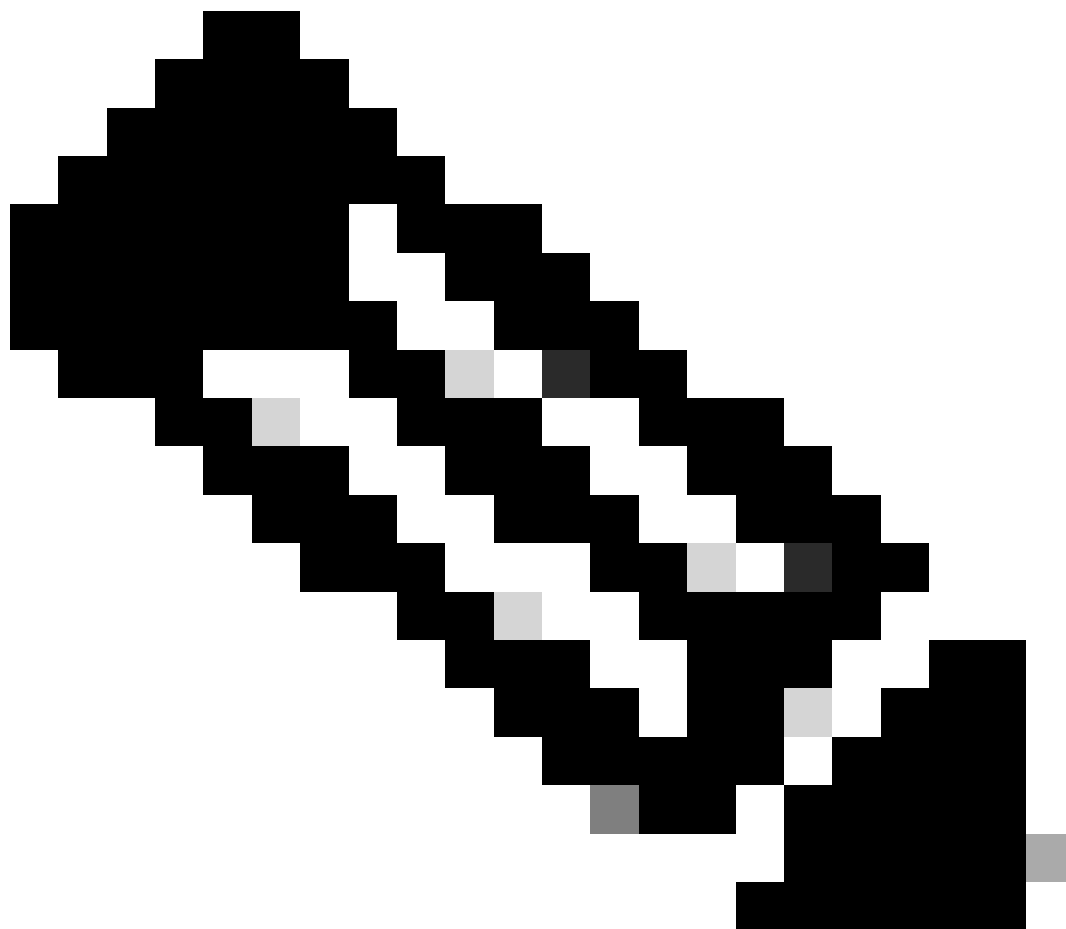


No matches found

[Cancel](#)

[Back](#)

[Next](#)



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

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

Banner Message
Require user to accept a banner message post authentication

Session Timeout
 days

Session Timeout Alert
 minutes before

Maximum Transmission Unit ⓘ

[Cancel](#) [Back](#) [Save](#)

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

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](#)

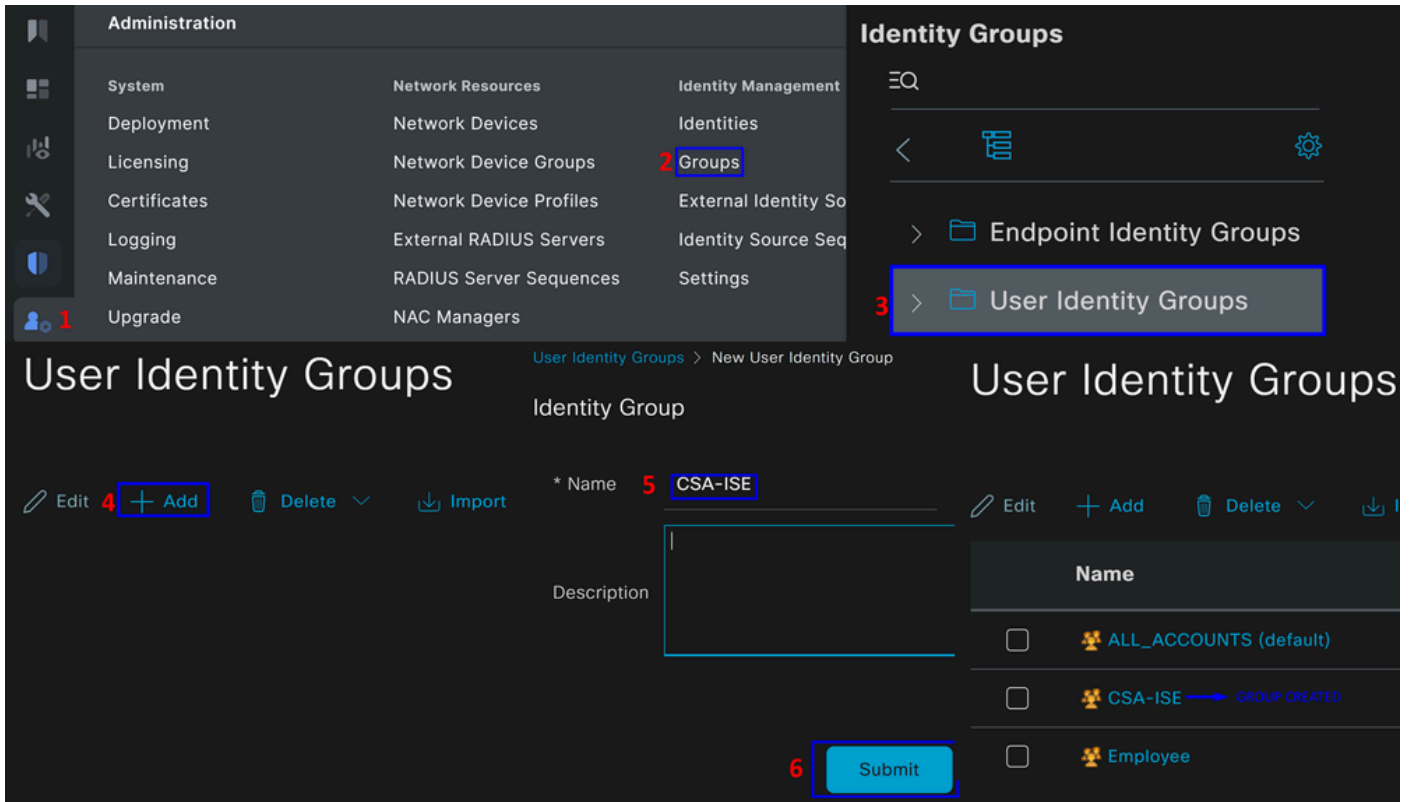
- **Name:** use um nome para identificar o acesso seguro
- **IP Address:** Configure o Management Interface da etapa, [Região do pool de IP](#)
- **Device Profile:** Escolha a Cisco
 - **Radius Authentication Settings**
 - Shared Secret: Configure o mesmo segredo compartilhado configurado na etapa, [Chave 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 Name para 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 +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ
Enable	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

▼ User Groups

⋮ CSA-ISE ▼ 🗑️ +

- **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.

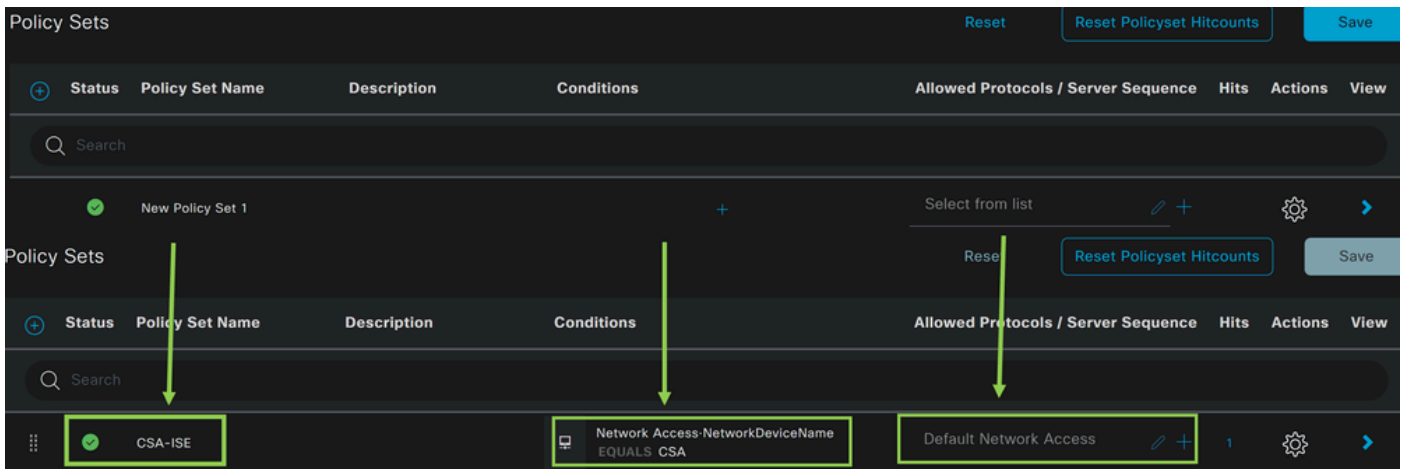
Depois disso, você poderá **Save** fazer a configuração e continuar com a etapa, **Configure Policy Set**.

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:

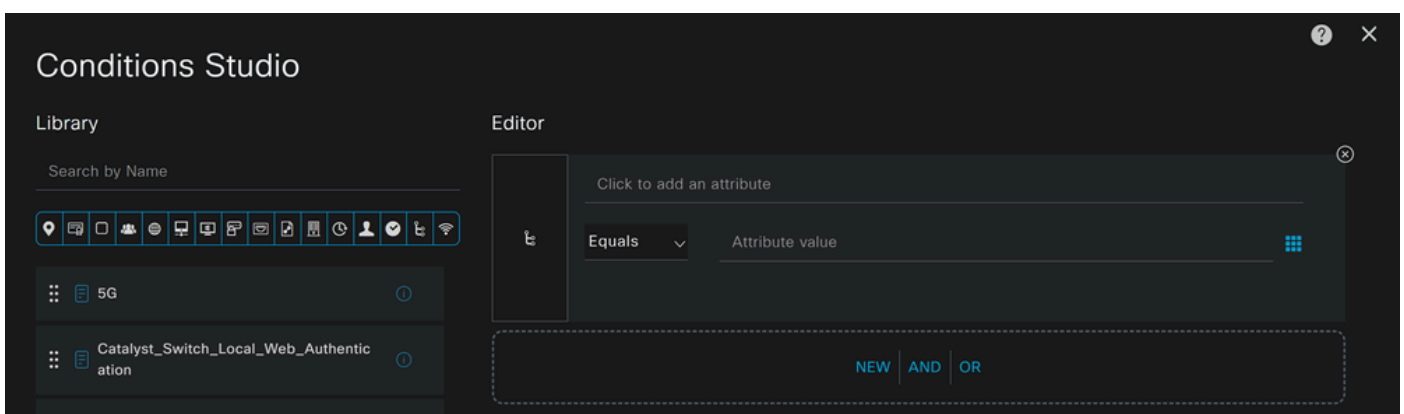
- Clique em Policy > Policy Sets
- Clique em + para adicionar um novo conjunto de políticas



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:

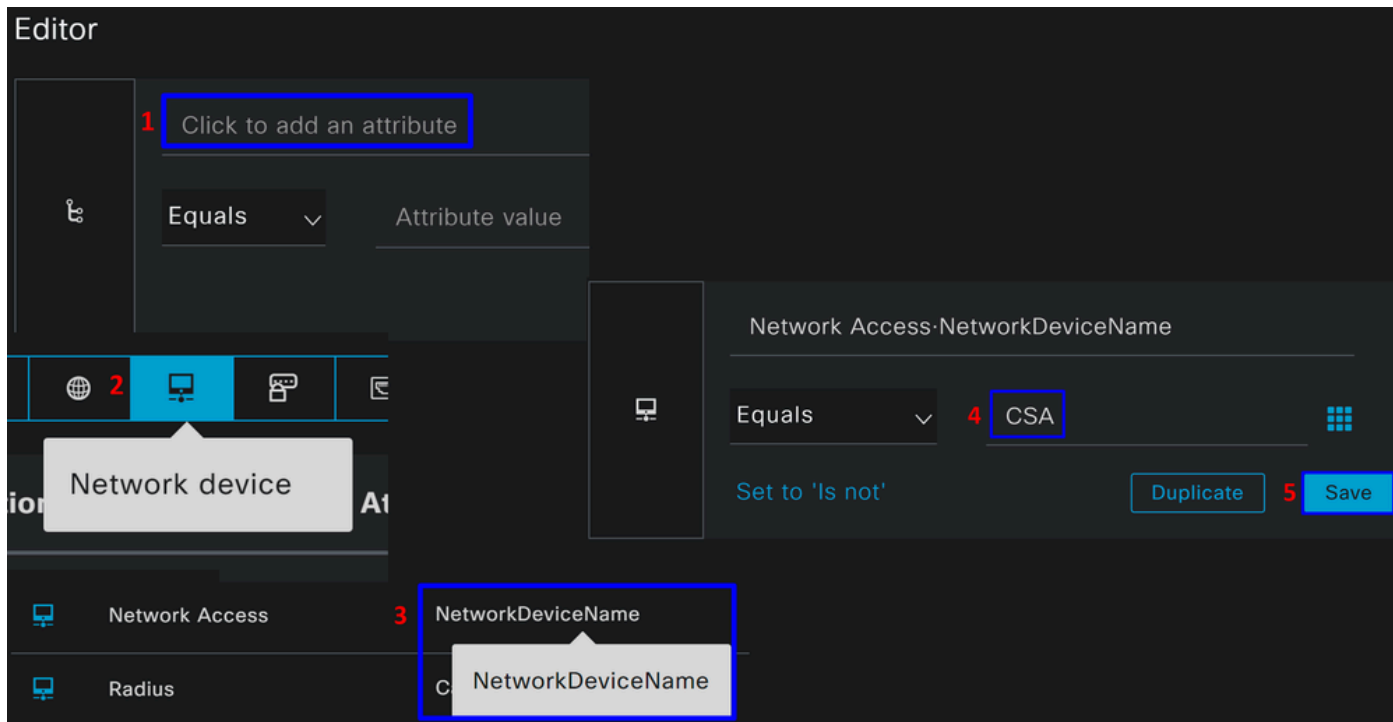
- Clique em +
- Na seção **Condition Studio**, as informações disponíveis incluem:



- 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](#)

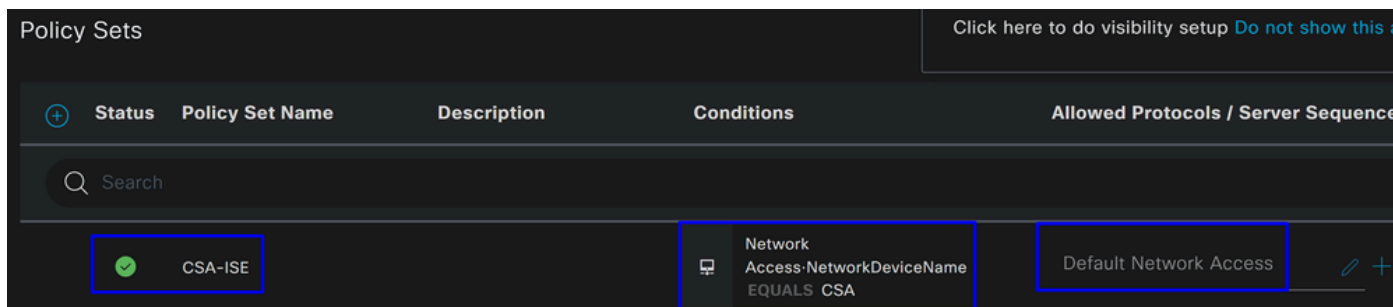
[dispositivos de rede](#))

- 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.

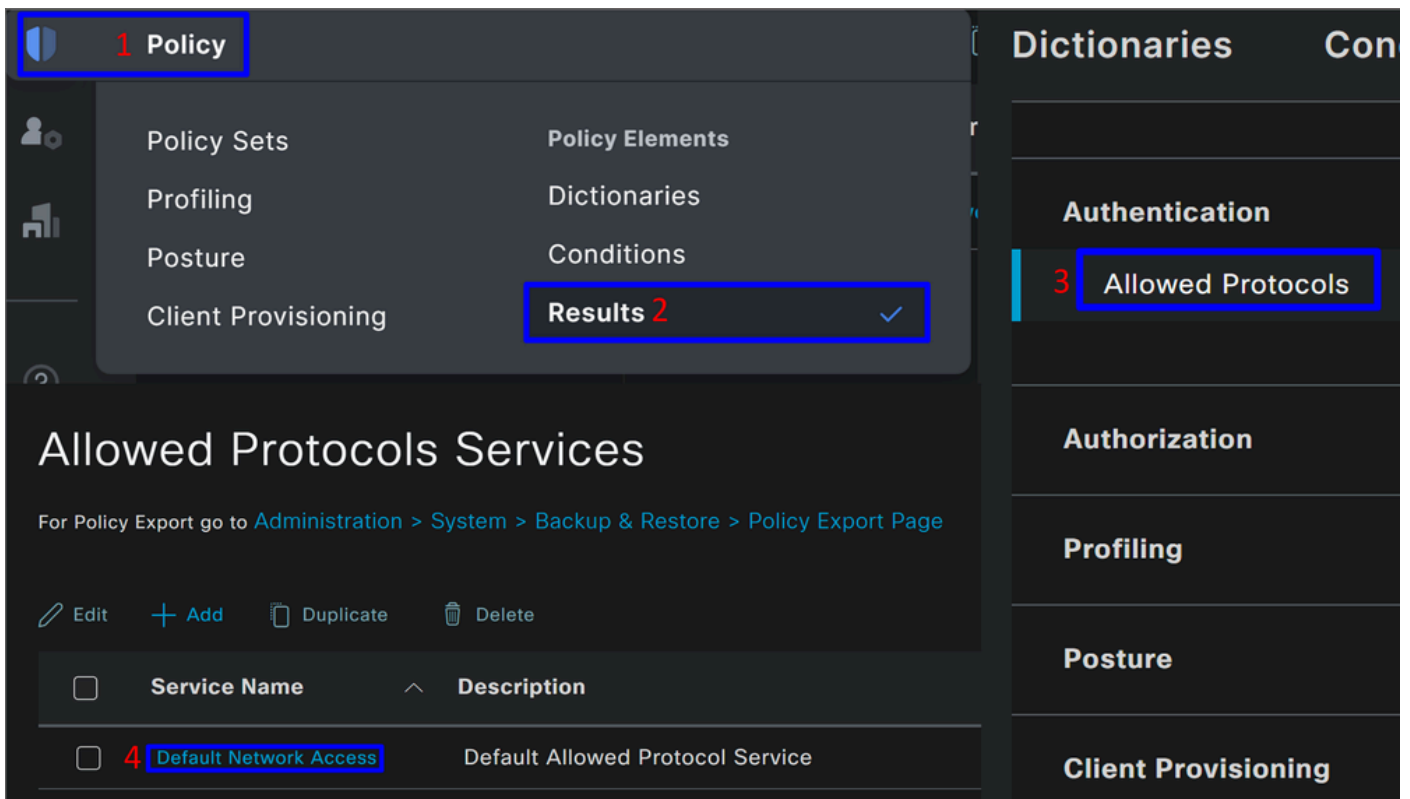
O resultado da política definida deve ser:



- Para verificar o **Default Network Access Protocols** permitido, continue com as próximas instruções:

- Clique em **Policy > Results**

- Clique em **Allowed Protocols**
- Clique em **Default Network Access**

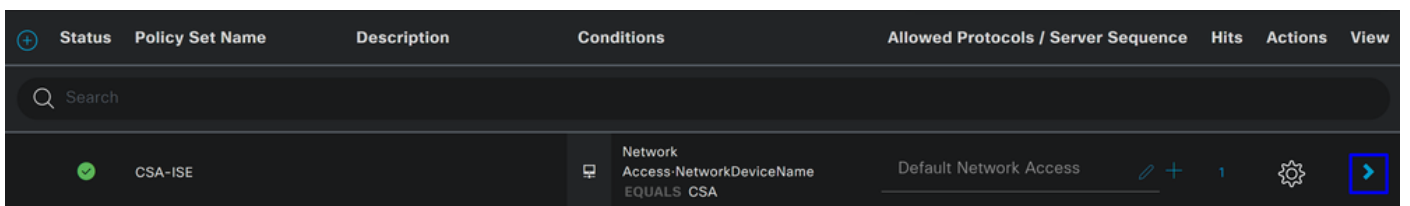


- Em seguida, você verá todos os protocolos permitidos em **Default Network Access**

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:

Policy Sets → CSA-ISE Click here to do visibility setup [Do not show this again.](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	27
> Authentication Policy(2) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions > Authorization Policy(7)					

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:

Authorization Policy(2)

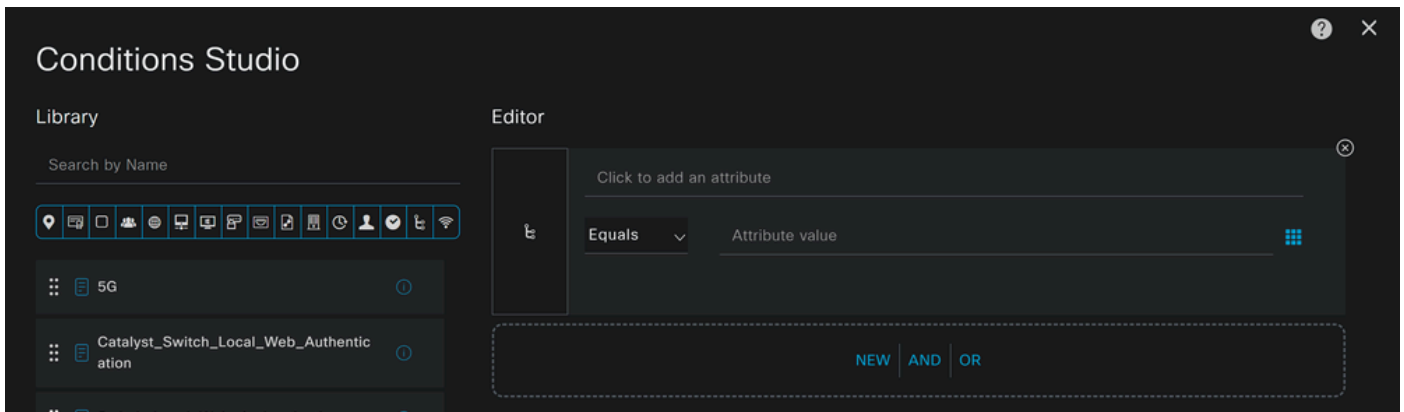
			Results		
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Rule 1		Select from list	Select from list	
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list	

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

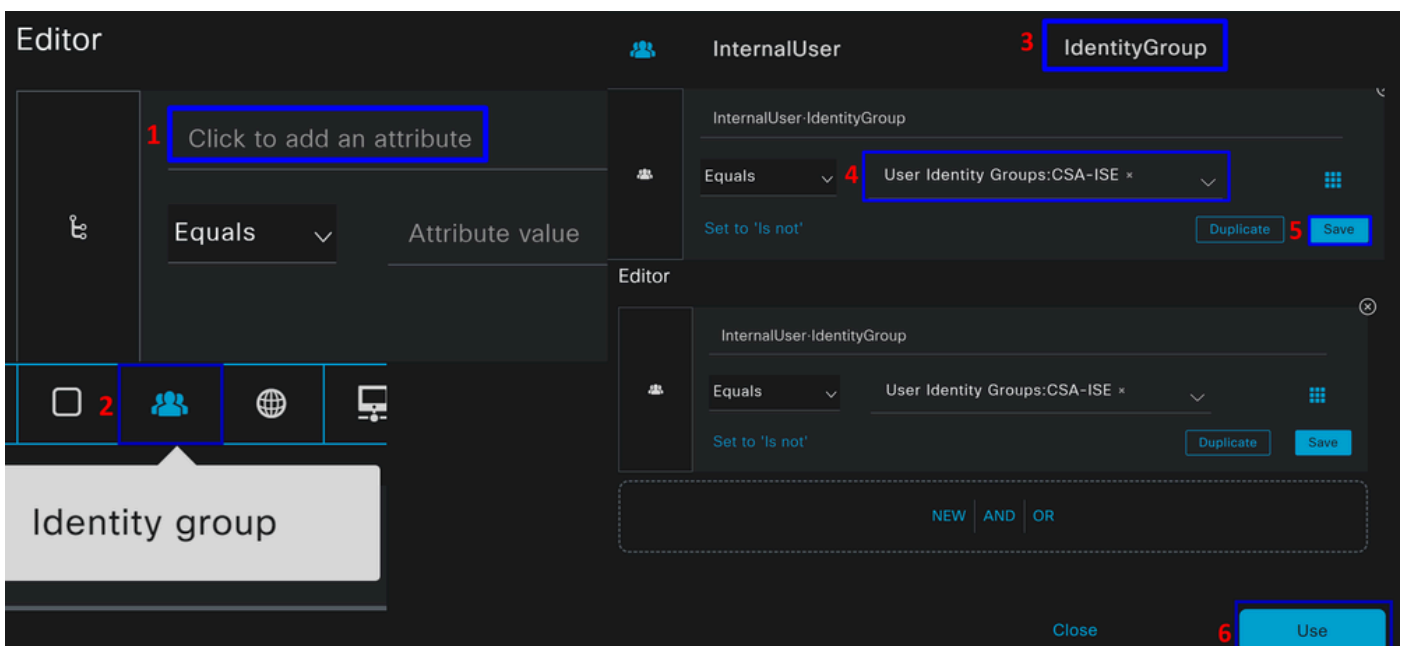
Authorization Policy(2)

			Results		
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Rule 1		Select from list	Select from list	

- 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:

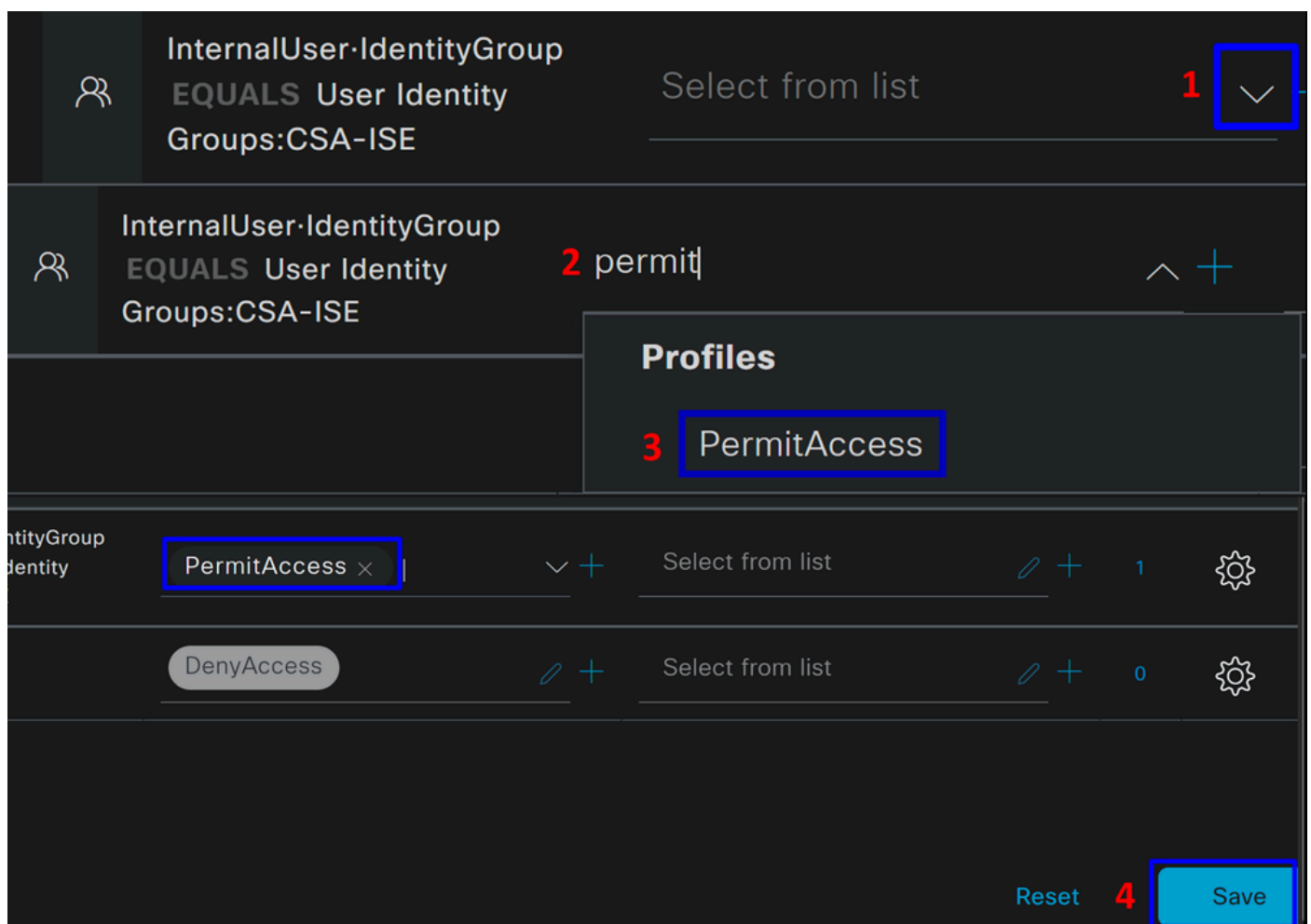


- Para criar as Condições, clique em Click to add an attribute
- Clique no **Identity Group** botão
- Nas opções atrás, clique em **Internal User - IdentityGroup** opção
- Na **Equals** opção, use o menu suspenso para localizar o **Group** aprovado para autenticação na etapa, [Configurar um grupo](#)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





28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.2	151.248.21.152	ISE_CSA

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

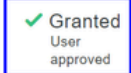
- Navegue até a página **Cisco ISE Dashboard**

- Clique em **Operations > Live Logs**

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
▼		Identity	Authentication Policy	Authorization Policy	Authorization Profiles
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess

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**

Timestamp (UTC) ▼	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
10:02:34 14 DE ABR. DE 2024	 Granted User approved	vpnuser	ISE - SAML	N/A	▼ iOS 17.4.1 AnyConnect 5.0.05207 Flash Not installed Java Not installed Krakow, 12, Poland 83.29.26.111 <small>Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.</small>	▼ Duo Push Apple iPhone 15 Pro Max DPFK77EPVMXGJ7H7TMD3 Krakow, 12, Poland 83.29.26.111

Configurar usuários locais ou do Ative Directory do Radius

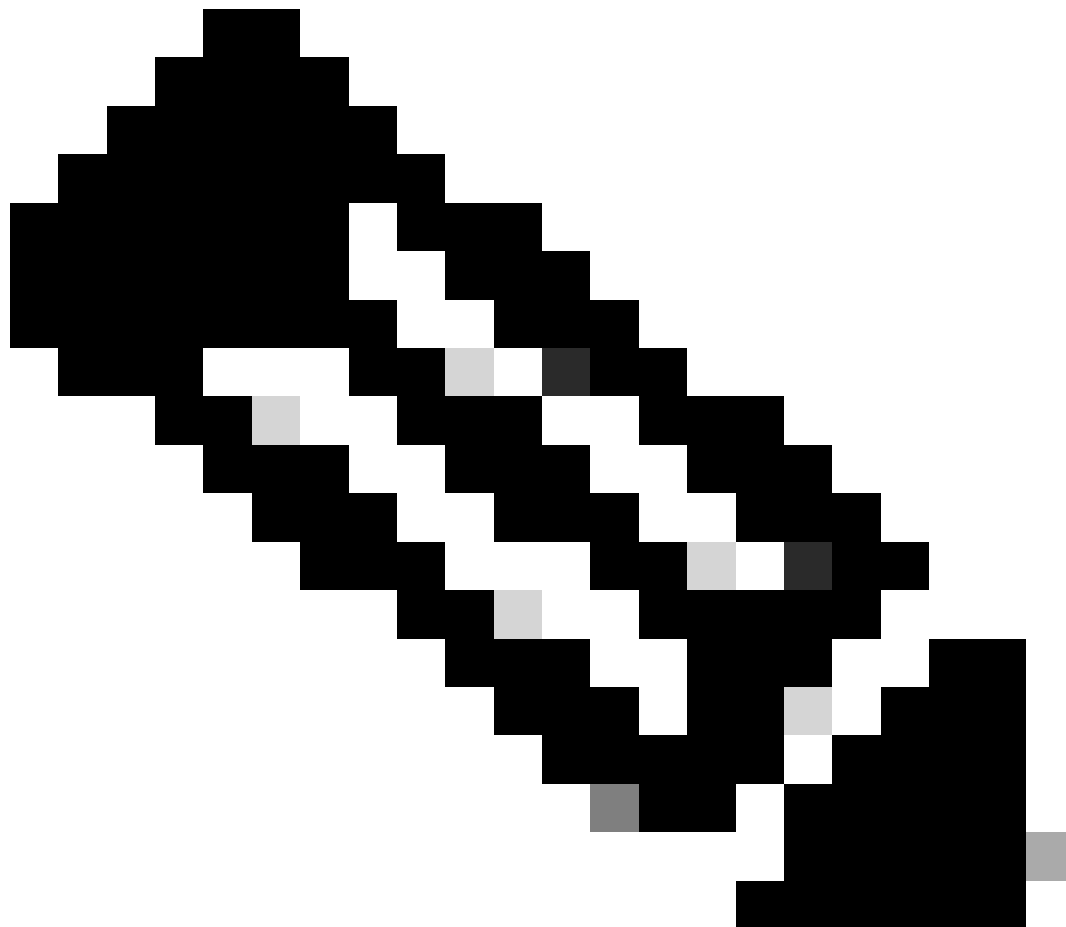
Configurar a postura do ISE

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.

The image displays two side-by-side screenshots of the 'Anti-Malware Condition' configuration interface. The left screenshot shows the initial state with the following fields: * Name (empty), Description (empty), Compliance Module (4.x or later), * Operating System (Select Operating System), Vendor (ANY), and Check Type (Installation selected, Definition unselected). The right screenshot shows the configuration after changes: * Name (CSA-Antimalware), Description (empty), Compliance Module (4.x or later), * Operating System (Windows All), Vendor (Cisco Systems, Inc.), and Check Type (Installation selected, Definition unselected). Arrows indicate the changes between the two states.

- **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.

Baseline Condition Advanced Condition

1 You can select products either on baseline condition or advanced condition.

2

	Product Name	Minimum Version	Maximum Version	Minimum Compliant
<input type="checkbox"/>	ANY	ANY	ANY	N/A
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
<input type="checkbox"/>	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

3

Save Reset

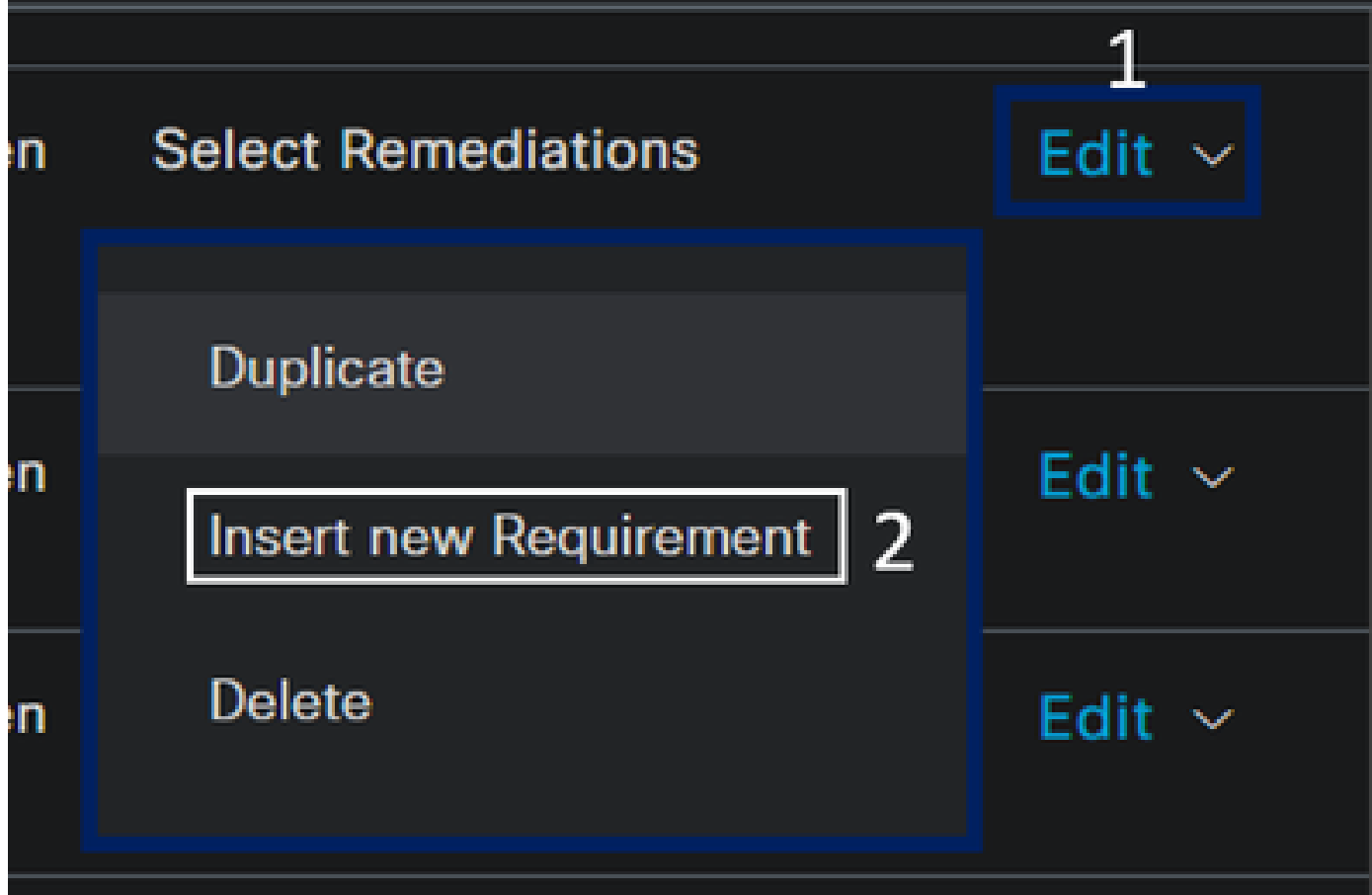
- Marque a caixa de seleção das condições que você deseja avaliar
- Configurar a versão mínima a ser verificada
- Clique em Salvar para continuar com a próxima etapa

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 > Requiriments**
- Clique em um **Edit** dos requisitos e clique em **Insert new Requirement**

Remediations Actions



- Sob o novo requisito, configure os próximos parâmetros:

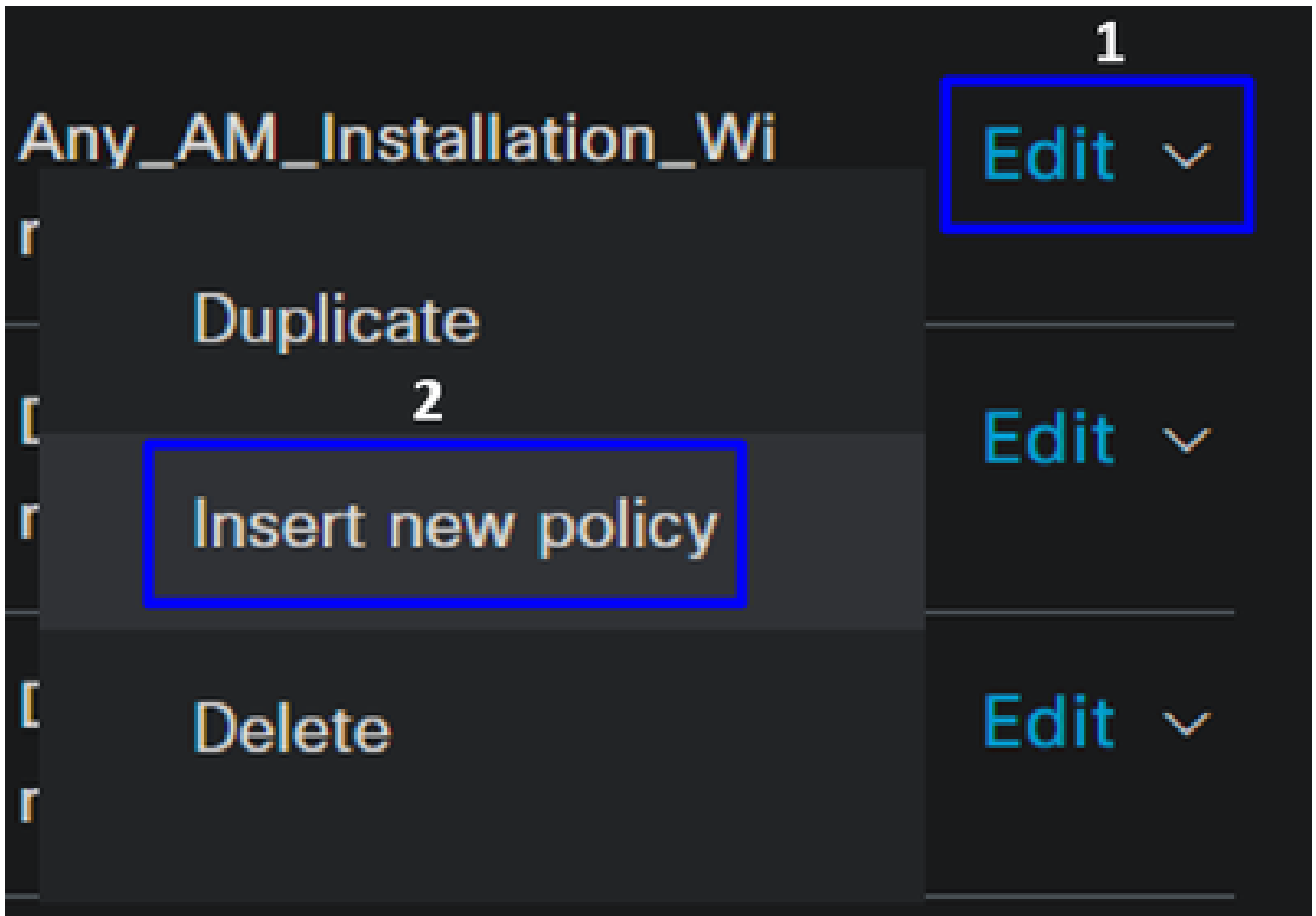
Requirements						
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
CSA-ANTIMALWARE	for Windows All	using 4.x or later	using Agent	met if CSA-Antimalware then	Message Text Only	Edit ▾

- **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	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	CSA-Windows-Posture	If Any	and Windows All	and 4.x or later	and Agent	and	then CSA-ANTIMALWARE

- **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:

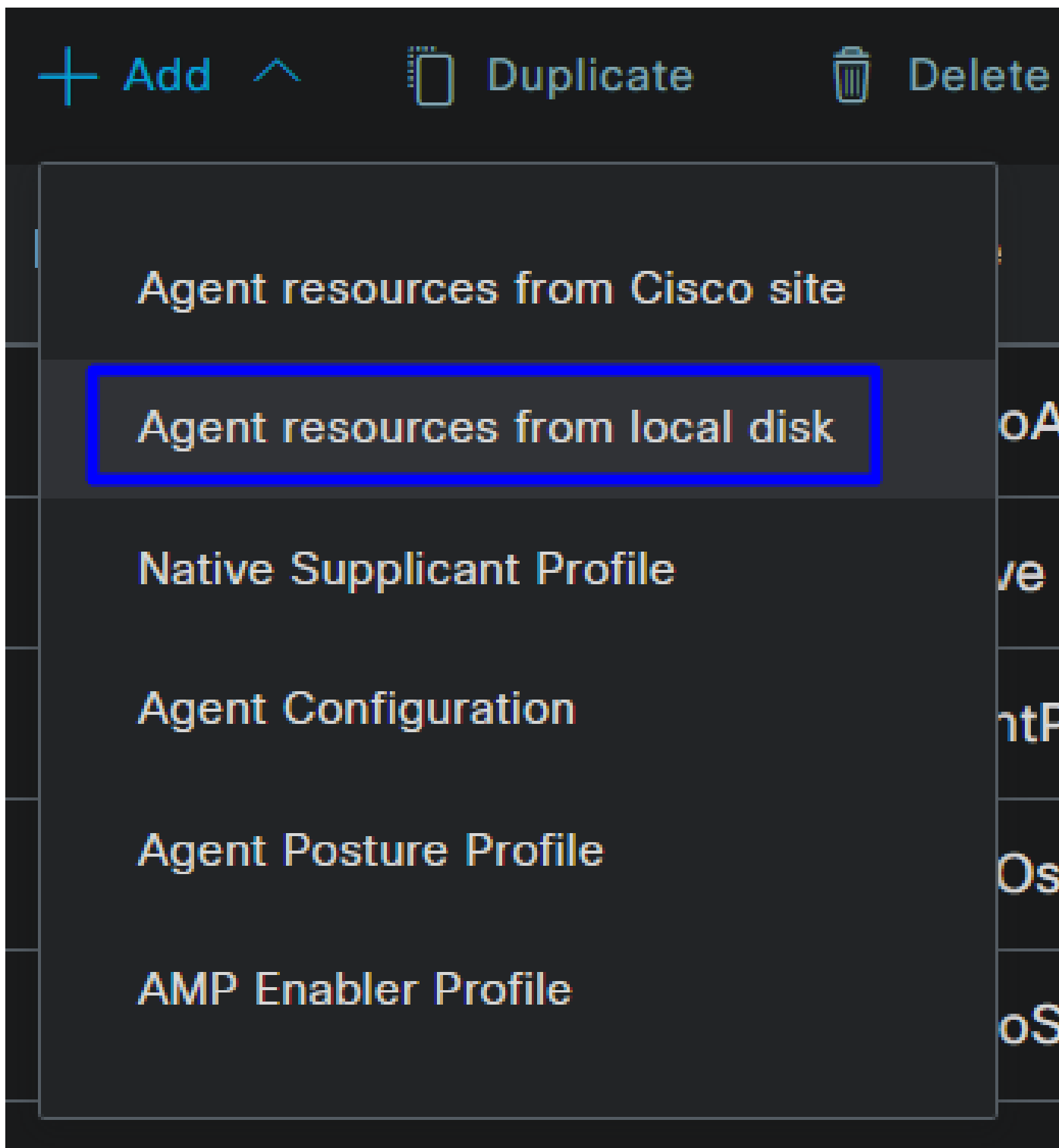
Recursos a serem configurados	Descrição
1. Agent Resources	Pacote de Provisionamento da Web para Cliente Seguro.
2. Compliance Module	Módulo de conformidade Cisco ISE
3. Agent Profile	Controle do perfil de provisionamento.
3. Agent Configuration	Defina quais módulos são provisionados configurando o portal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

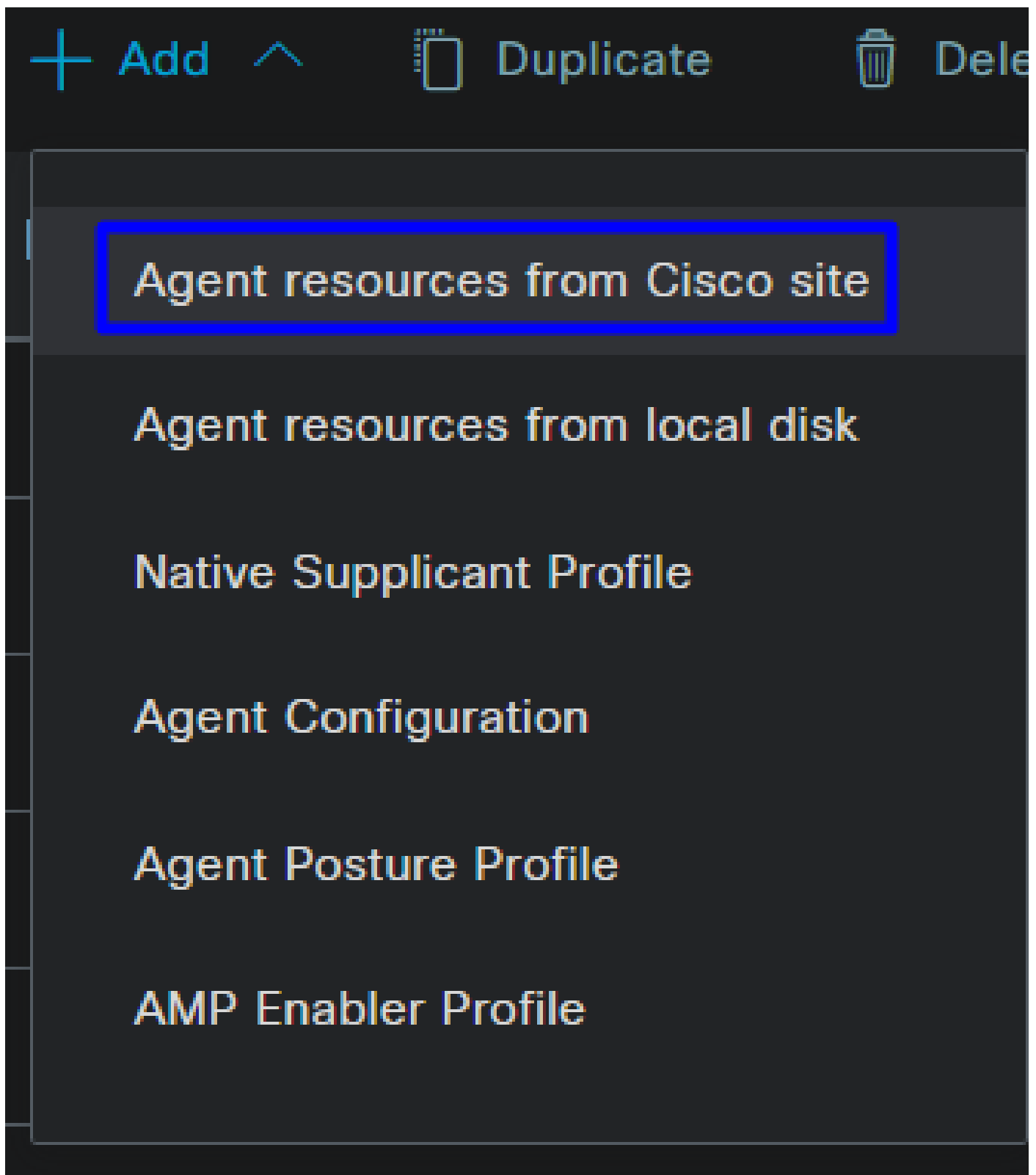
Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	118.88 MB	  

- 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**

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3 Configurar o perfil do agente

- Clique em + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑 Delet

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

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

Agent Posture Profile

Name *



Description:

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

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Step 4 Configurar a configuração do agente

- Clique em + Add > Agent Configuration

+ Add ^

📱 Duplicate

🗑 Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- Depois disso, configure os próximos parâmetros:

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

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 type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

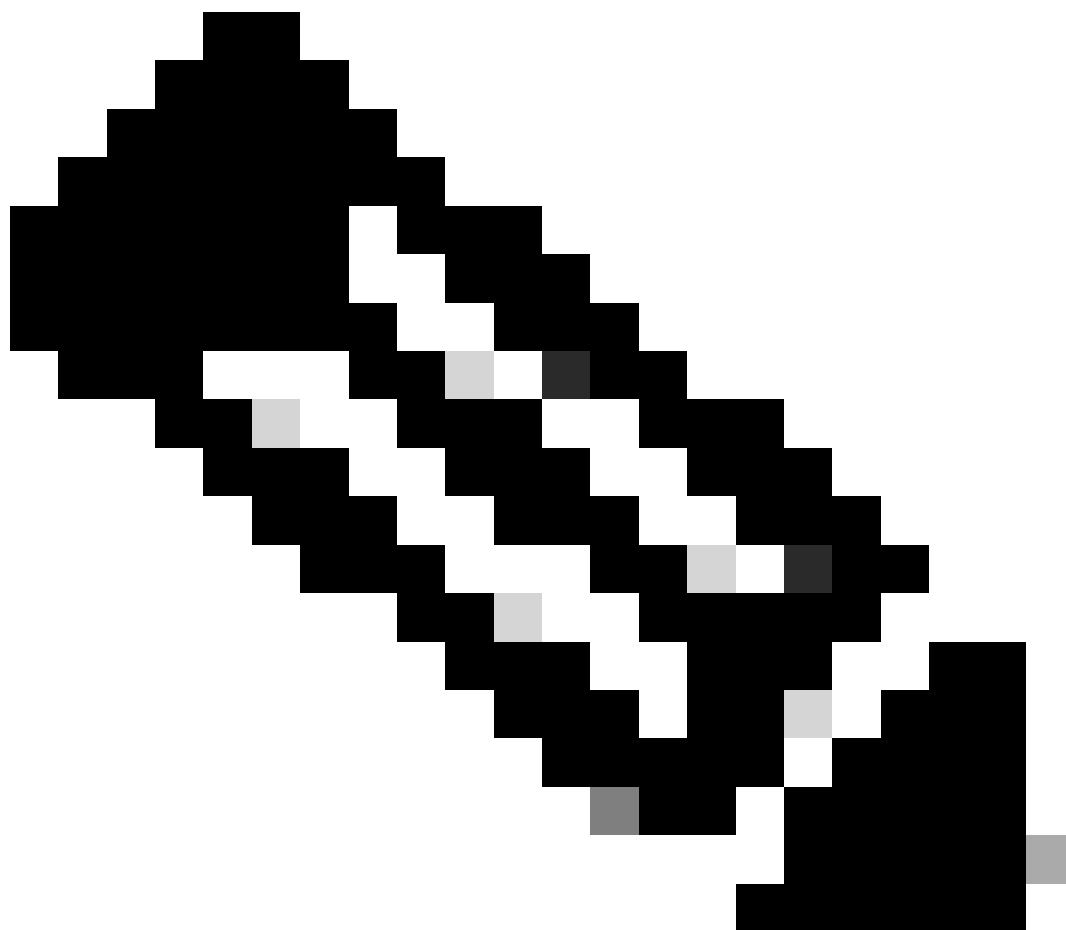
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- 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**

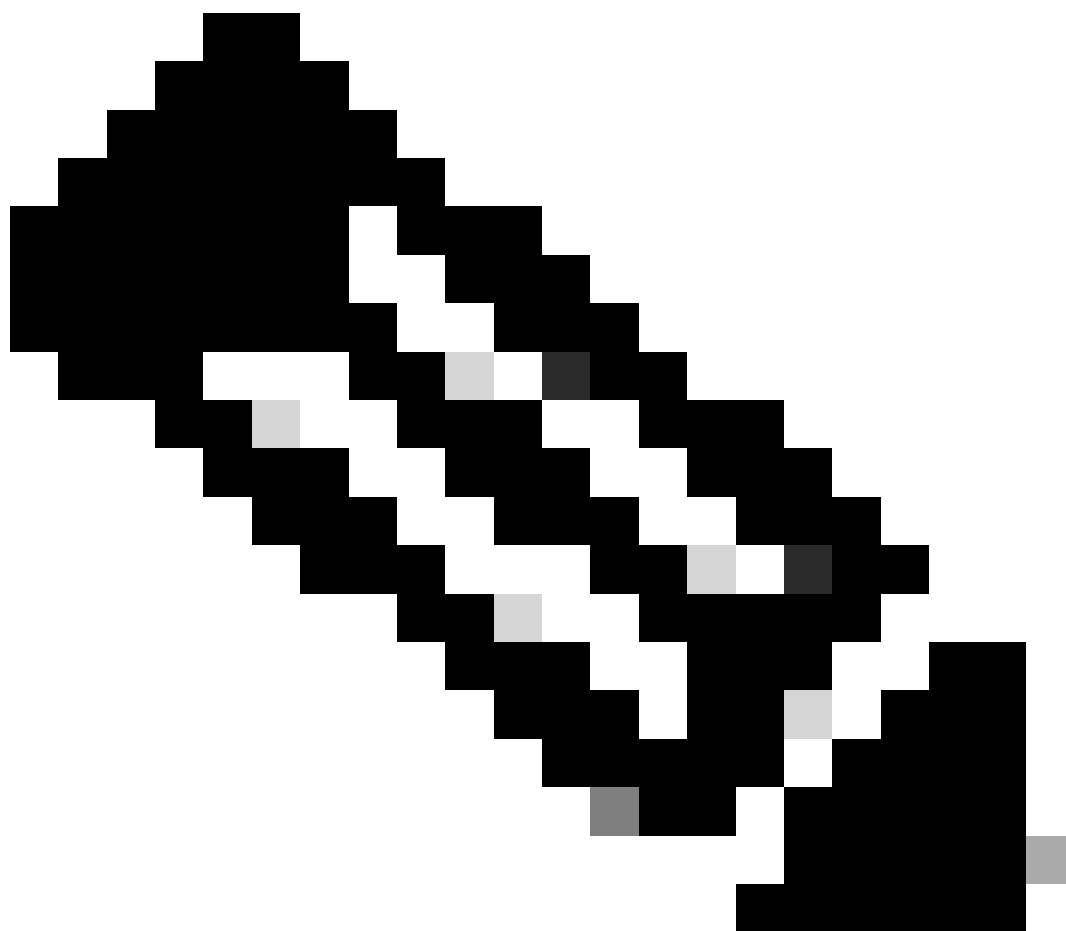


Observação: é recomendável que cada sistema operacional, Windows, Mac OS ou Linux, tenha uma configuração de cliente independente.

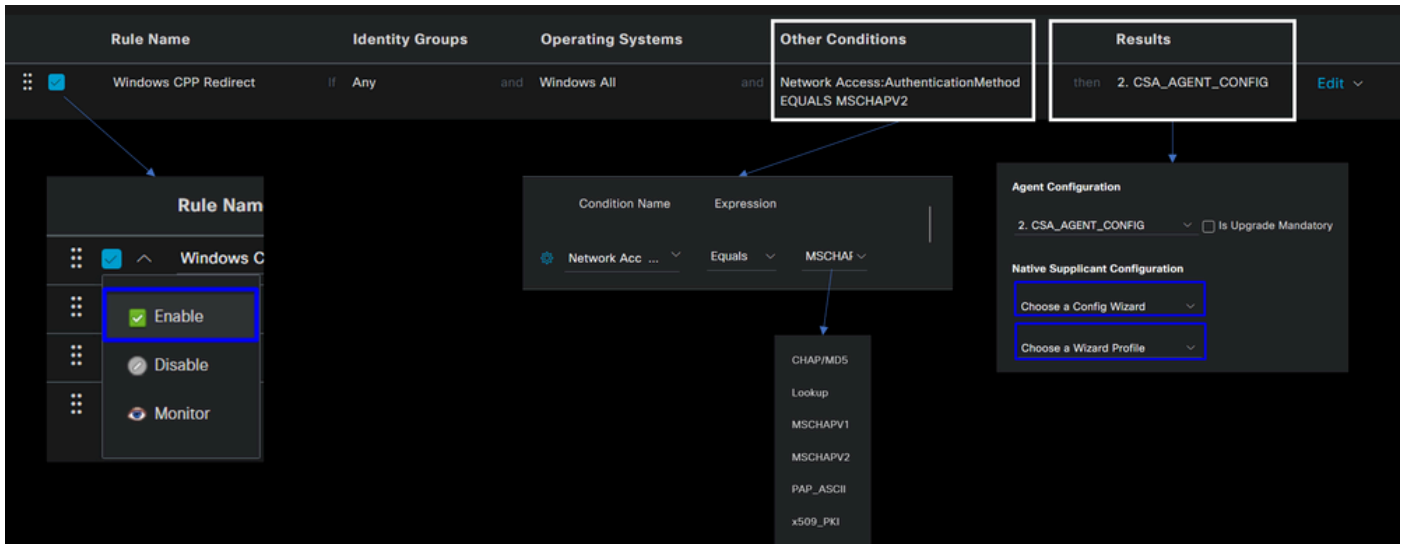
Configurar Política de Provisionamento de Cliente

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: CSA-Compliant

Description: [Empty text box]

IP version: IPv4 IPv6 Agnostic ⓘ

* DACL Content:

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
...	

- **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**

Description

IP version IPv4 IPv6 Agnostic (i)

*** DACL Content**

1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

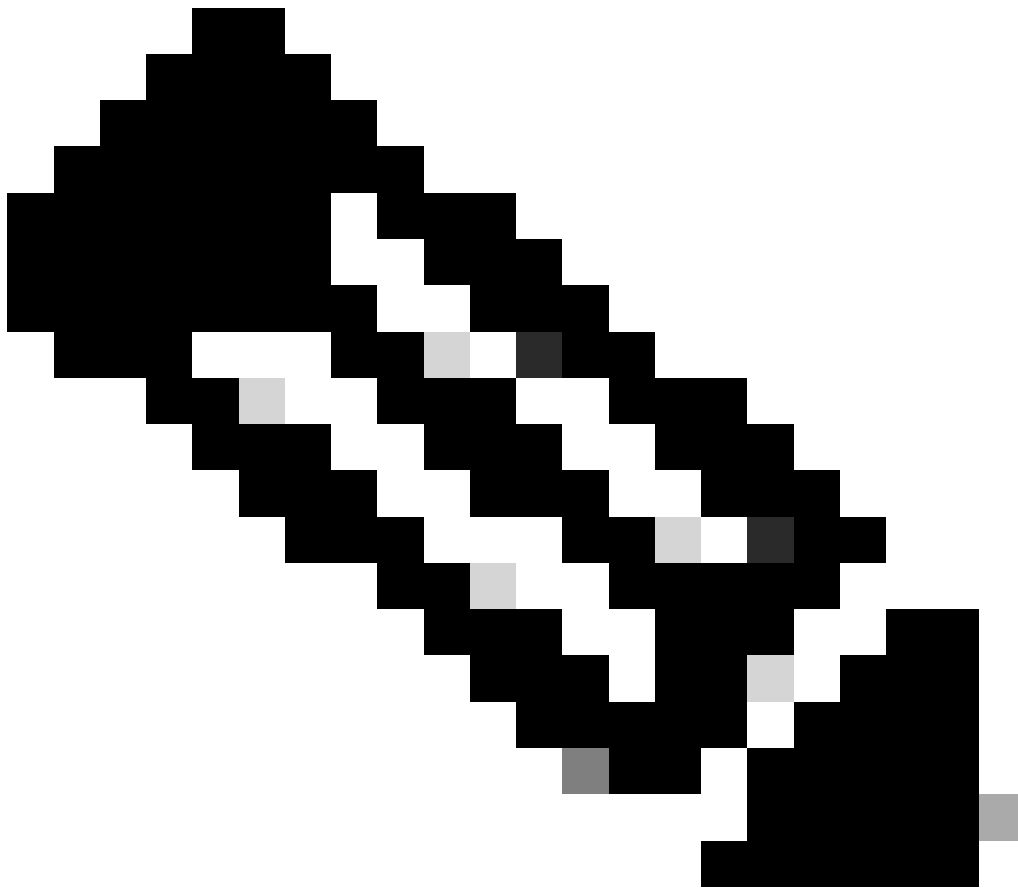
Check DACL Syntax

- **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**

Authorization Profile

* Name


CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

 Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

✓ Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL IPv6 (Filter ID)

- **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 Unknown Compliant Authorization Profile

* Name **CSA-Unknown-Compliant**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile  Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name **CSA_Redirect_To_ISE**

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

Client Provisioning (Posture) ACL **redirect** Value **Client Provisioning Portal (...)**

- **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.

```
Attributes Details
Access Type = ACCESS_ACCEPT
DAACL = CSA_Redirect_To_ISE
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=
&action=cpp
```

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	Negar Acesso

Navegue até o painel do ISE

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

- Clique > na para acessar a política criada

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access	370		

- Clique no botão Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy(4)					

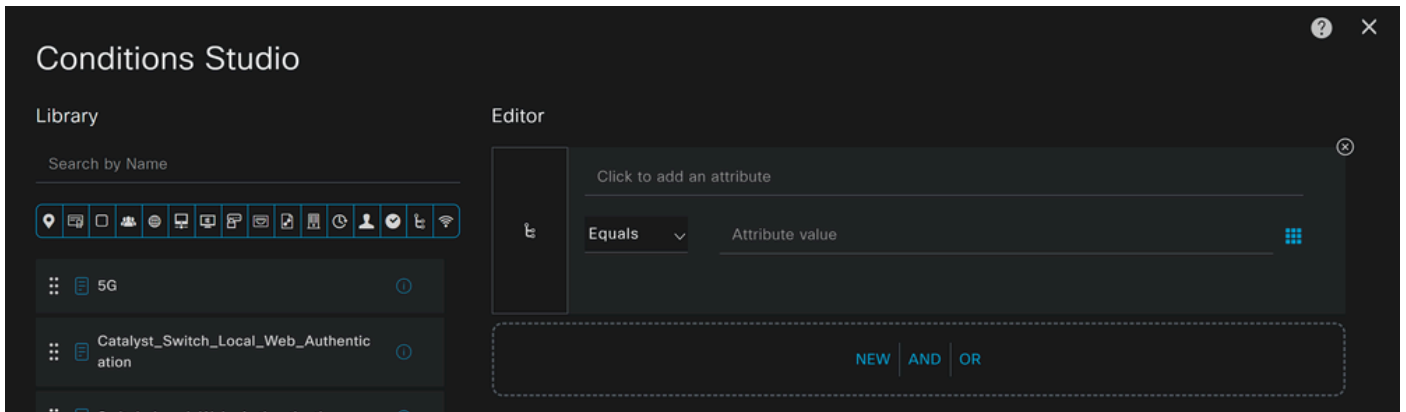
- Crie as três políticas a seguir na próxima ordem:

✓	SAML-Compliant	AND	<div>Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Compliant
✓	SAML-Unknown-Compliant	AND	<div>Compliance_Unknown_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Unknown-Compliant
✓	SAML-Non-Compliant	AND	<div>Non_Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	DenyAccess

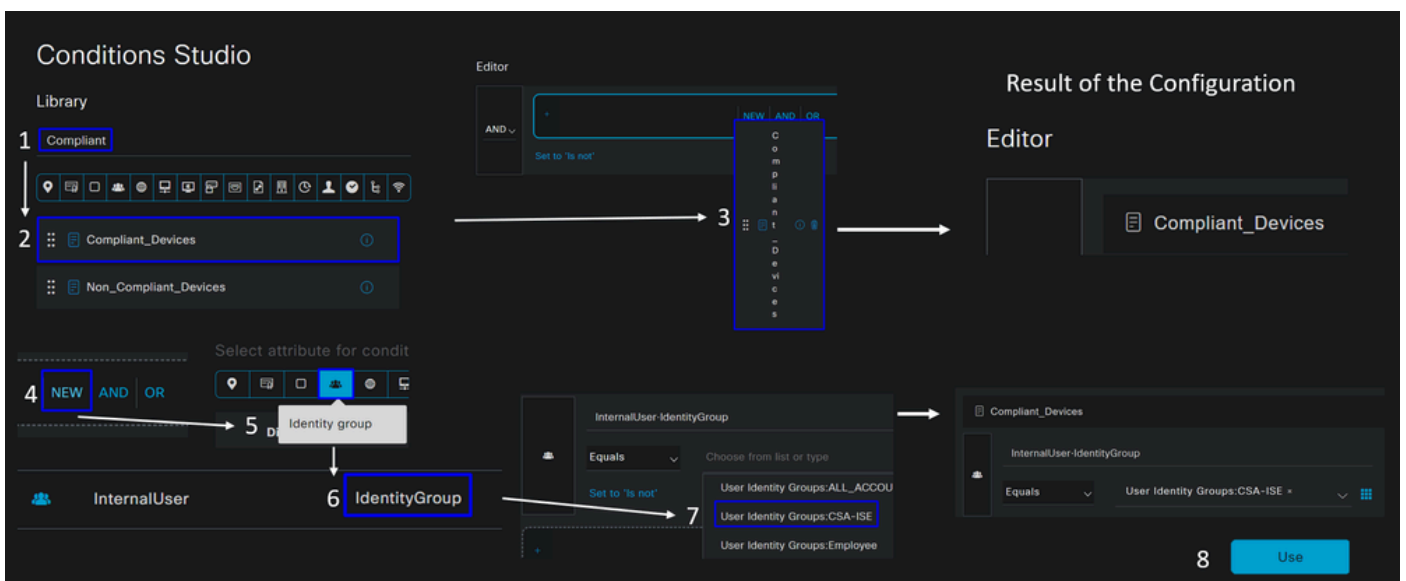
- Clique em + para definir a **CSA-Compliance** política:

					Results
+ Status	Rule Name	Conditions	Profiles	Security Groups	
Search					
✓	Authorization Rule 1	+	Select from list	✎ +	Select from list ✎ +

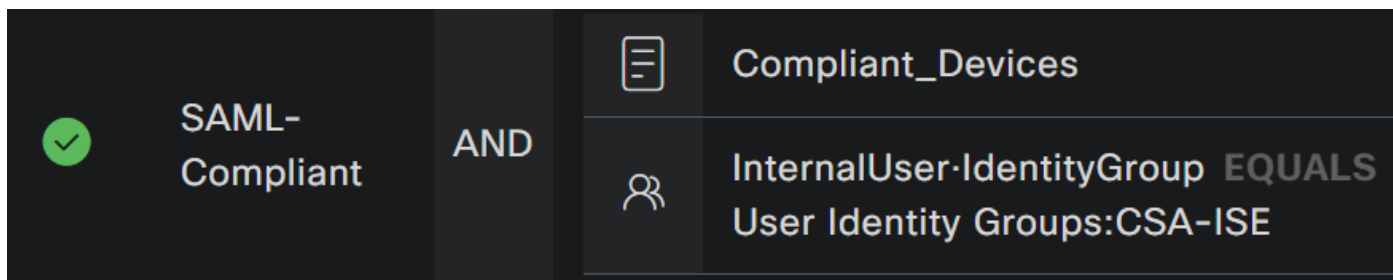
- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Compliance**
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



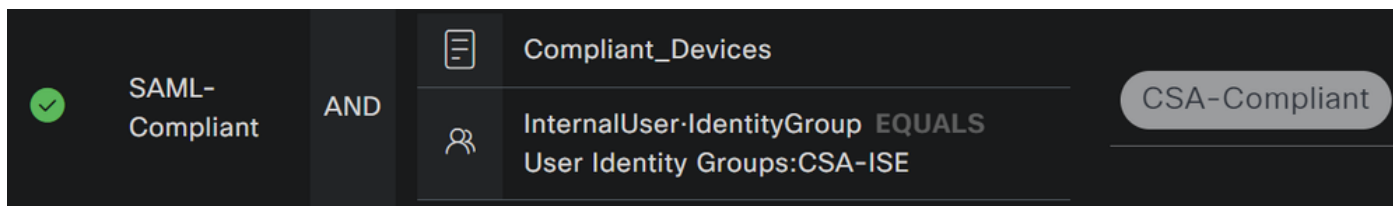
- Para criar a condição, procure **compliant**
- Você deve ter exibido Compliant_Devices
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group** que deseja corresponder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



- Como resultado, você terá a próxima imagem

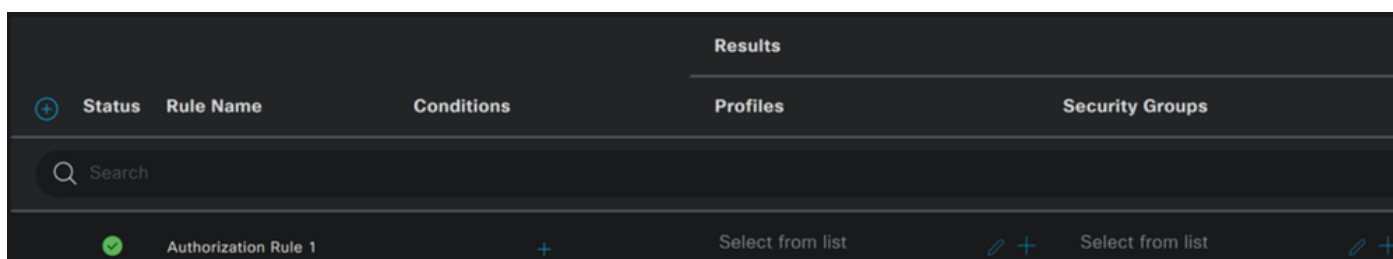


- Em **Profile** clique sob o botão suspenso e escolha o perfil de autorização de reclamação configurado na etapa, [Perfil de autorização de conformidade](#)



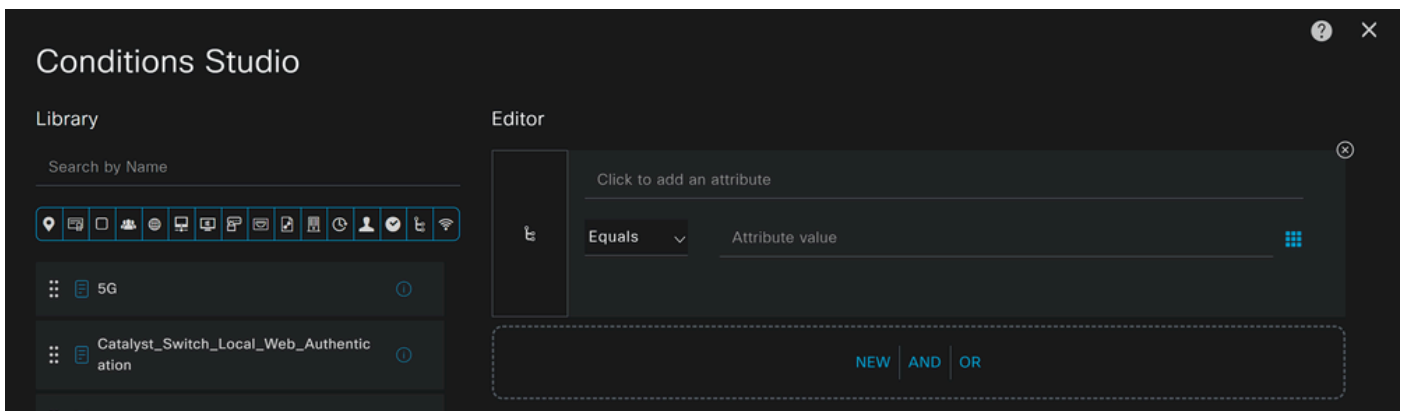
Agora você configurou o **Compliance Policy Set**.

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

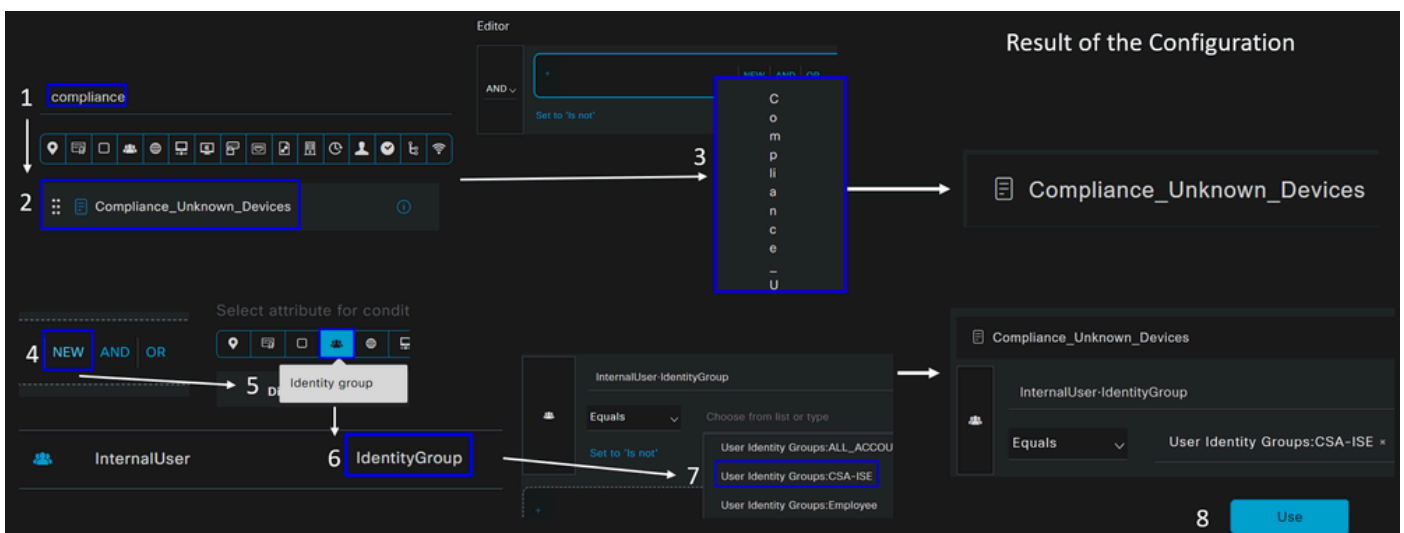


- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Unknown-Compliance**

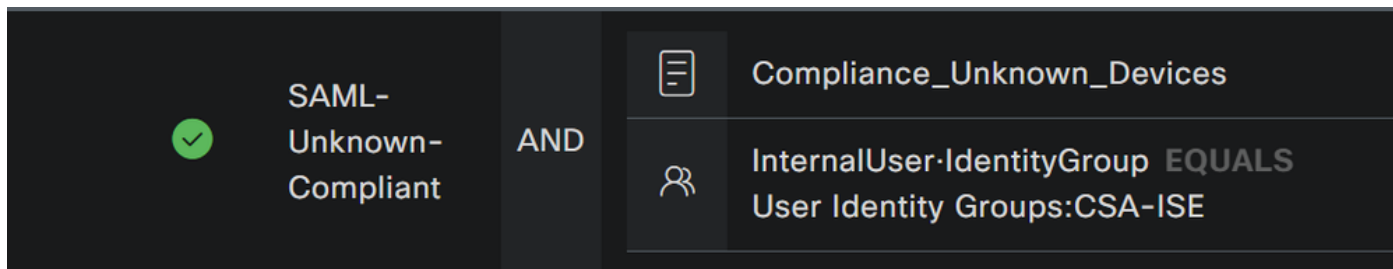
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



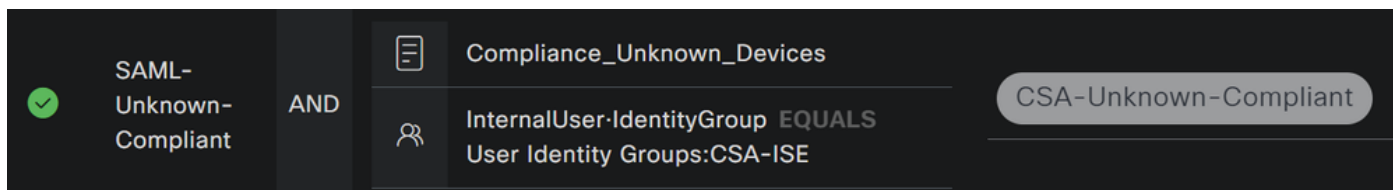
- Para criar a condição, procure **compliance**
- Você deve ter exibido **Compliant_Unknown_Devices**
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group**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



- Como resultado, você terá a próxima imagem

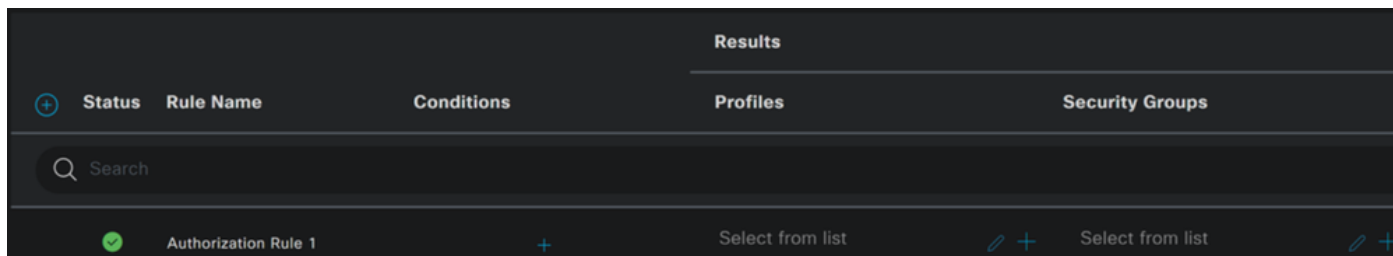


- Em **Profile** clique sob o botão suspenso e escolha o perfil de autorização de reclamação configurado na etapa, [Perfil de autorização de conformidade desconhecido](#)



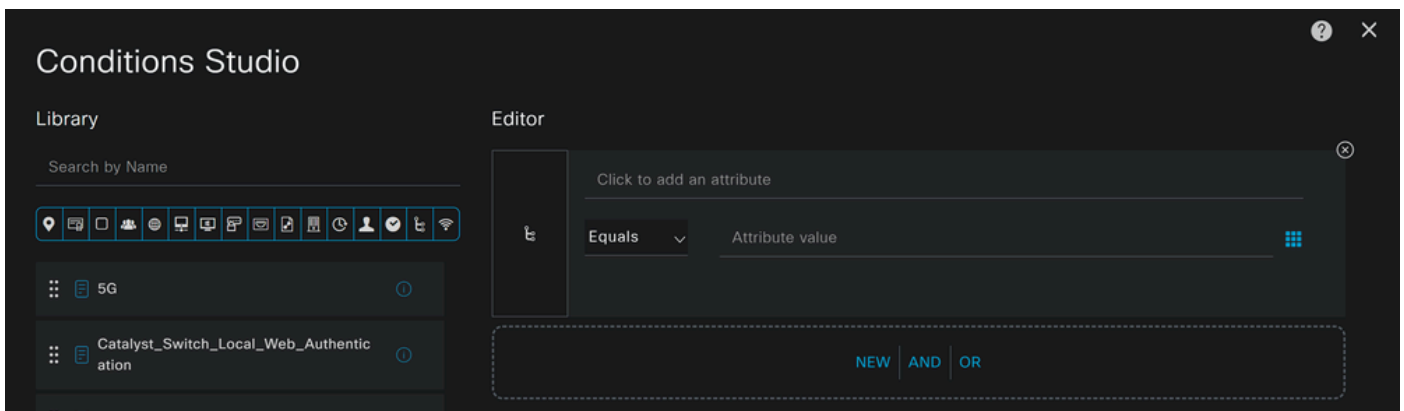
Agora você configurou o **Unknown Compliance Policy Set**.

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

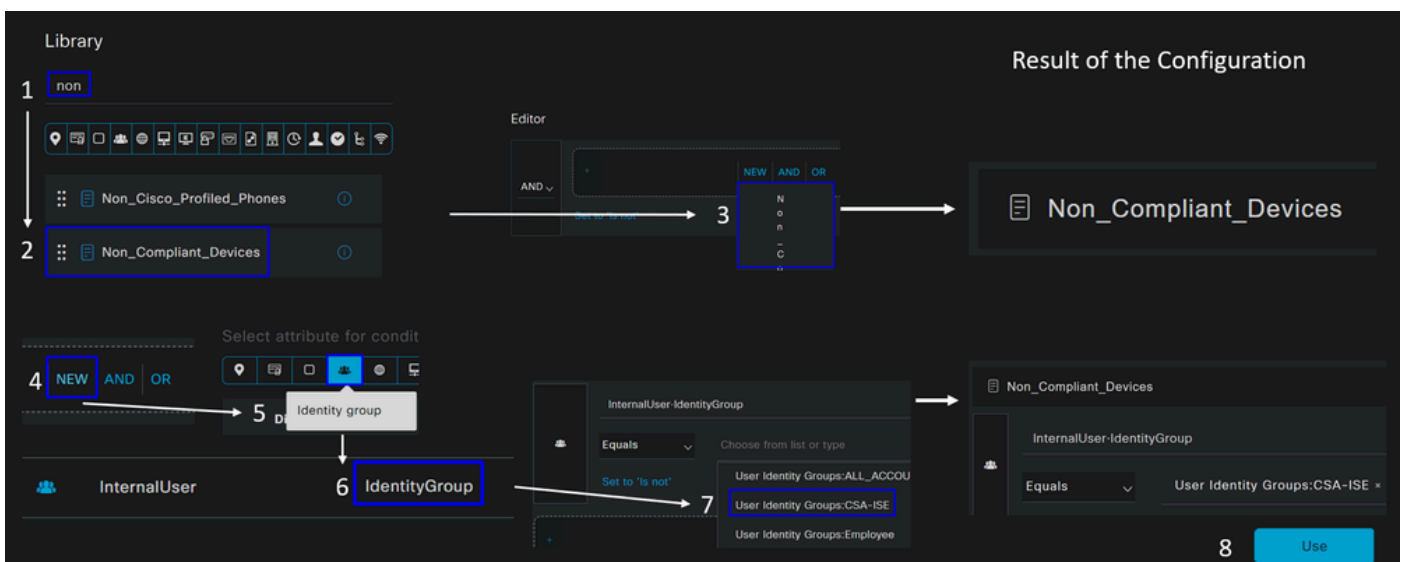


- Para a próxima etapa, altere o Rule Name Conditions e Profiles
- Ao definir a configuração **Name** de um nome para **CSA-Non-Compliance**

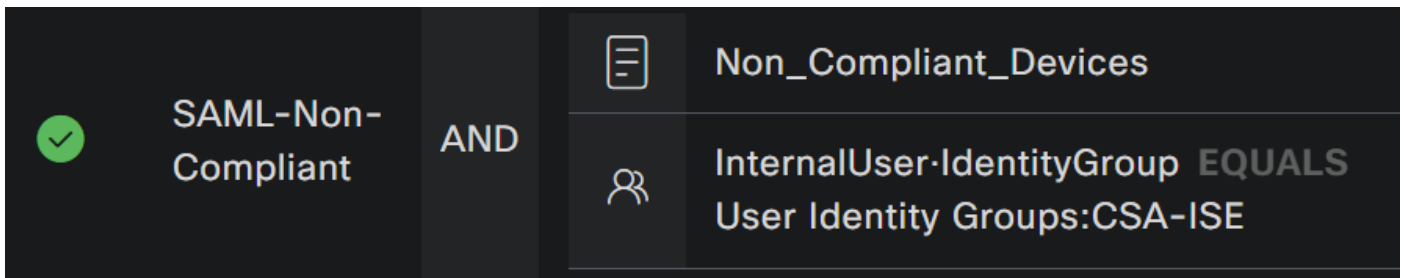
- Para configurar o **Condition**, clique no botão +
- Em **Condition Studio**, você encontrará as informações:



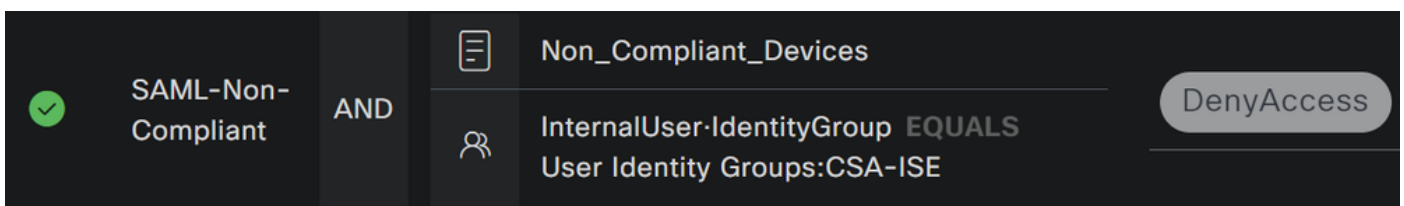
- Para criar a condição, procure **non**
- Você deve ter exibido **Non_Compliant_Devices**
- Arraste e solte sob a **Editor**
- Clique sob o Editor em **New**
- Clique no **Identity Group** ícone
- Escolher **Internal User Identity Group**
- Em **Equals**, escolha o **User Identity Group** que deseja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



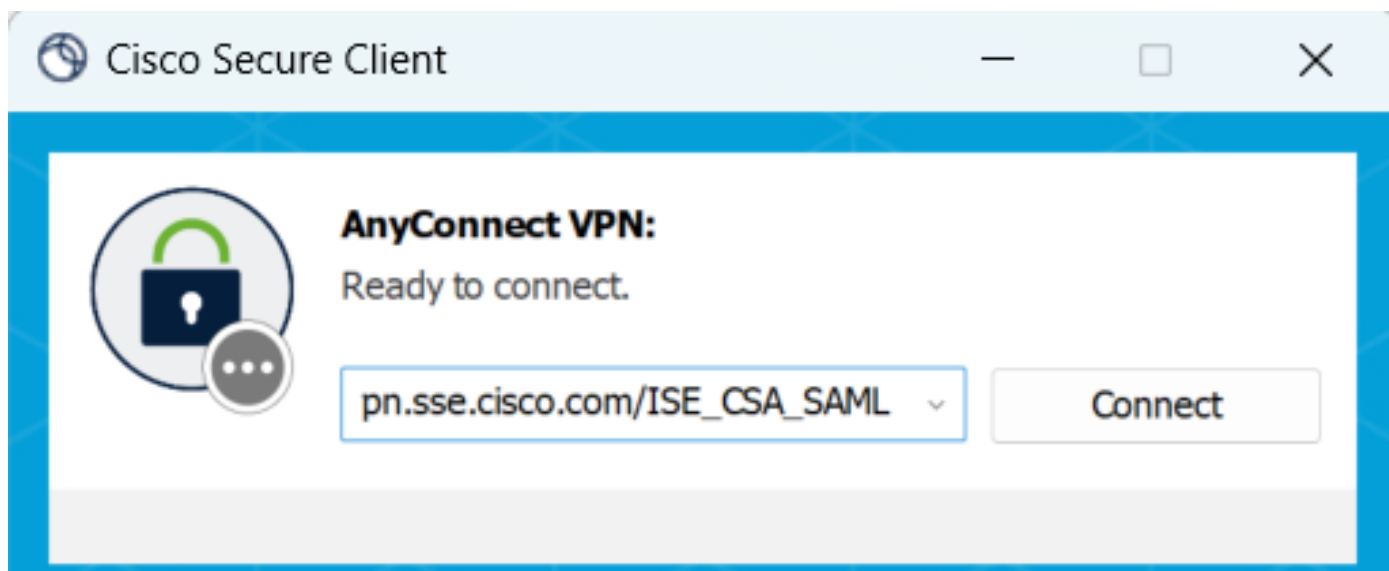
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
#ACISACL-IP-CSA-Compliant-M02b03a				
vphuser@cisconsp.tst	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
vphuser@cisconsp.tst	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
#ACISACL-IP-CSA_Redirect_To_ISE-M02b4d1				
vphuser@cisconsp.tst	CSA-ISE	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-Compliant
5205 Dynamic Authorization succeeded
5. Download CSA-Compliant
5232 DACL Download Succeeded

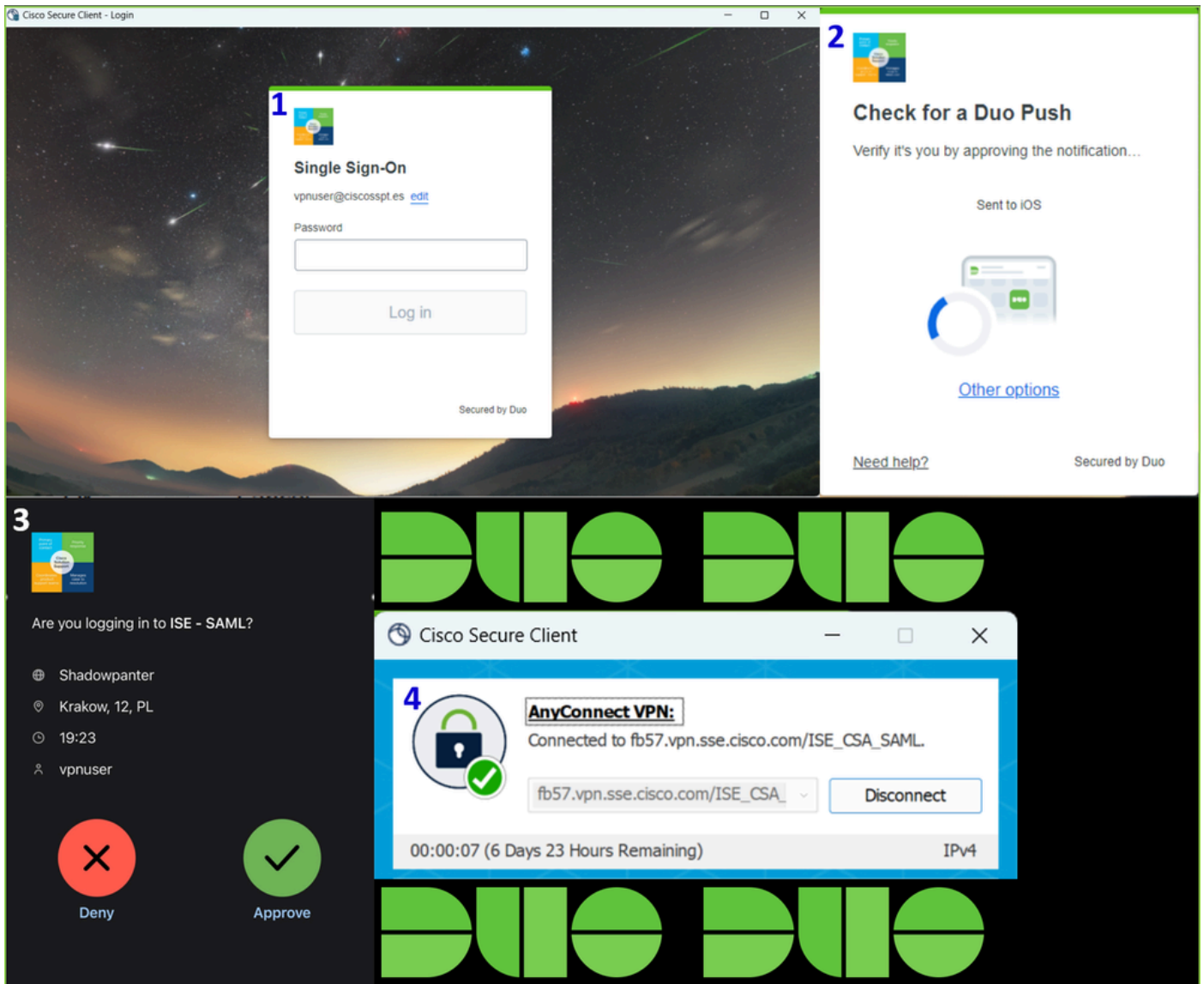


Observação: nenhum módulo ISE deve ser instalado para esta etapa.

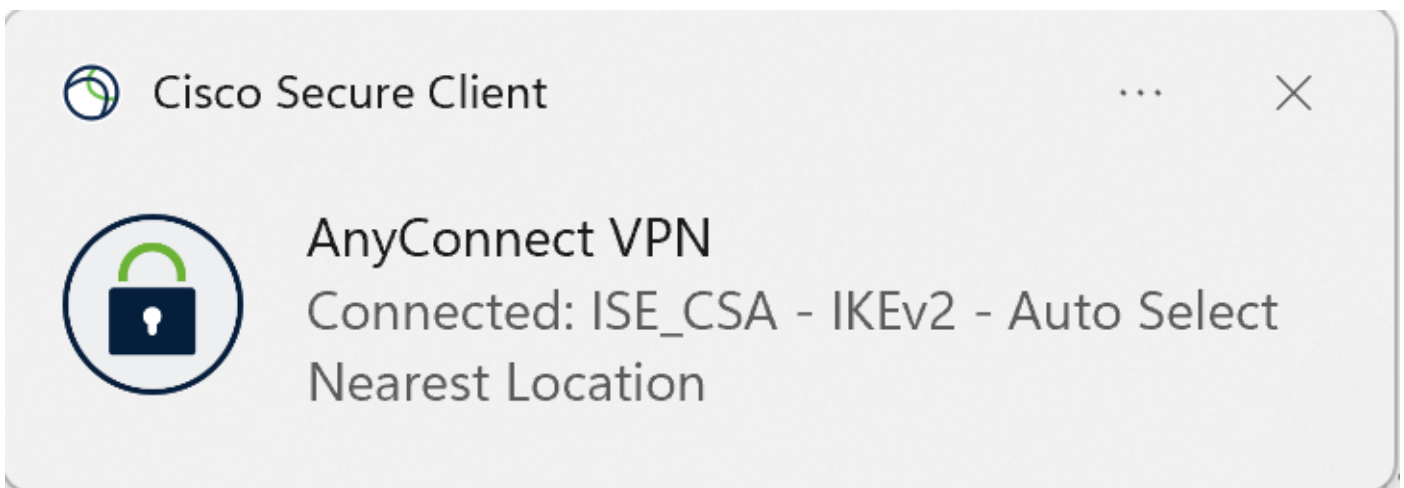
1. Conecte-se usando o Secure Client.

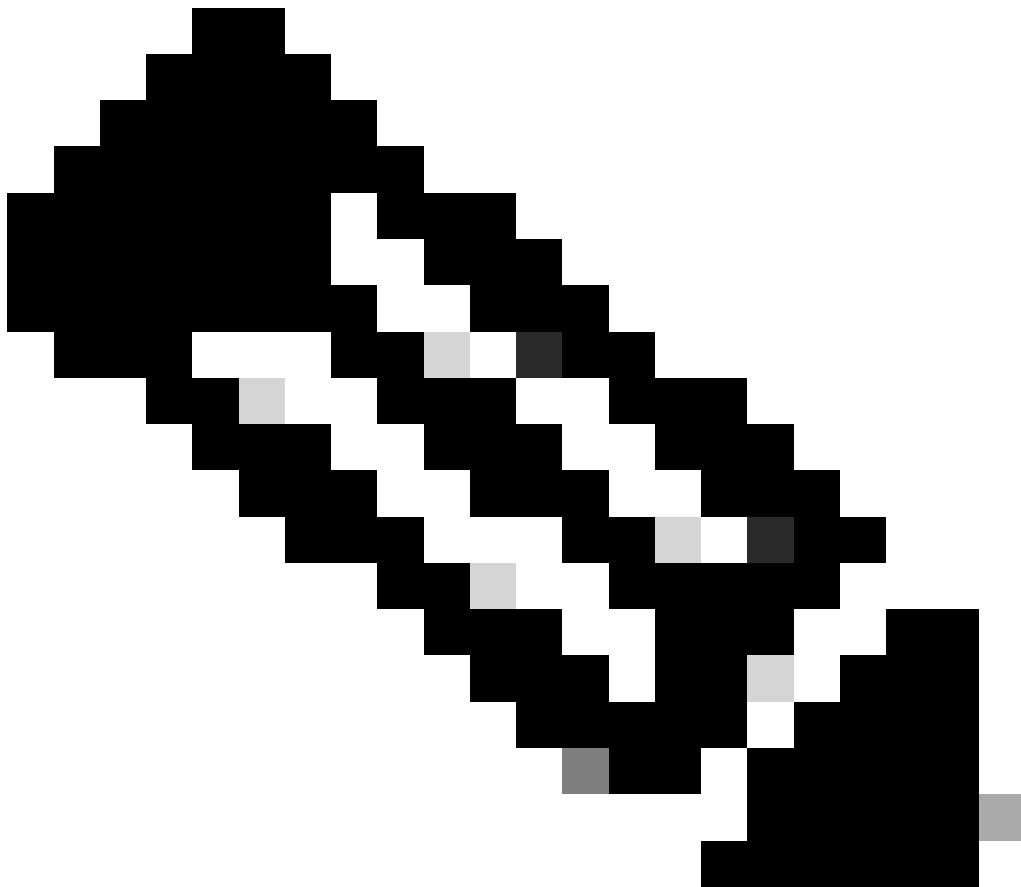
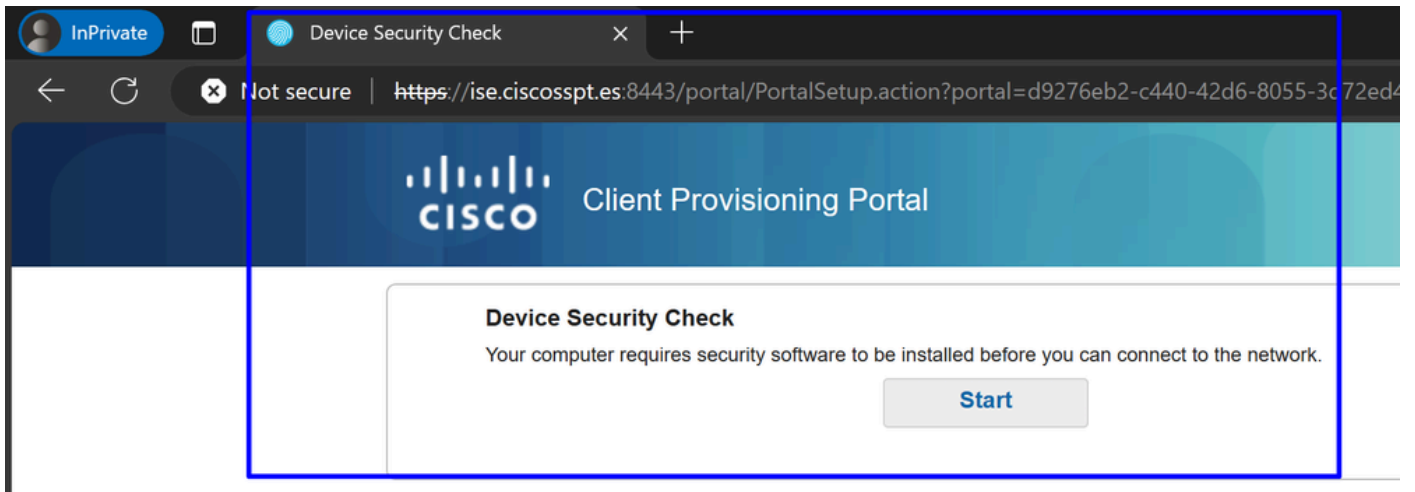


2. Forneça as credenciais para autenticação via Duo.



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.

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

9 Detecting if Agent is installed and running...

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

Device Security Check

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

Unable to detect Posture Agent

+ **+ This is my first time here**

+ + Remind me what to do next

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



+ This is my first time here

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.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.



You have 4 minutes to install and for the compliance check to complete

7. Instalar o agente

Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

See more



Network Setup Assistant



Installation is completed.

Quit

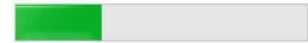
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

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.



ISE Posture

1 Update(s) Required



30%

Time Remaining:
3 Minutes



Action Required to Enable Access

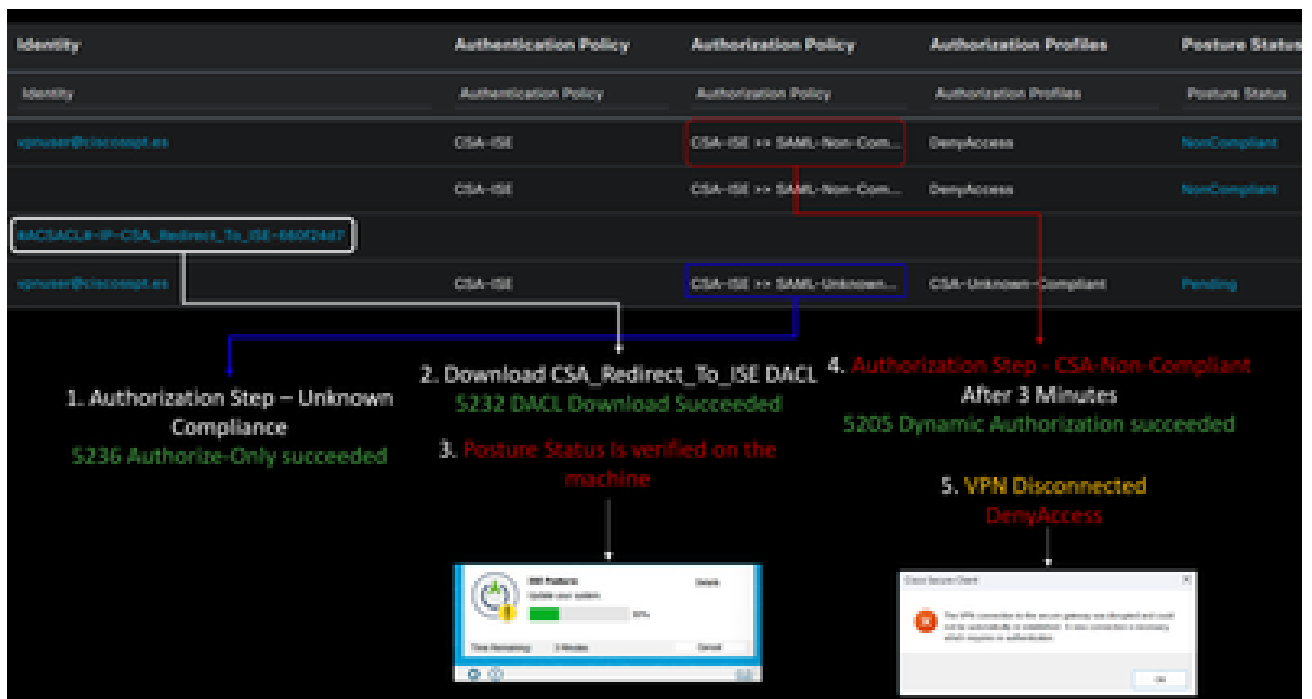
Updates are needed on your device before you can join the network.

This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

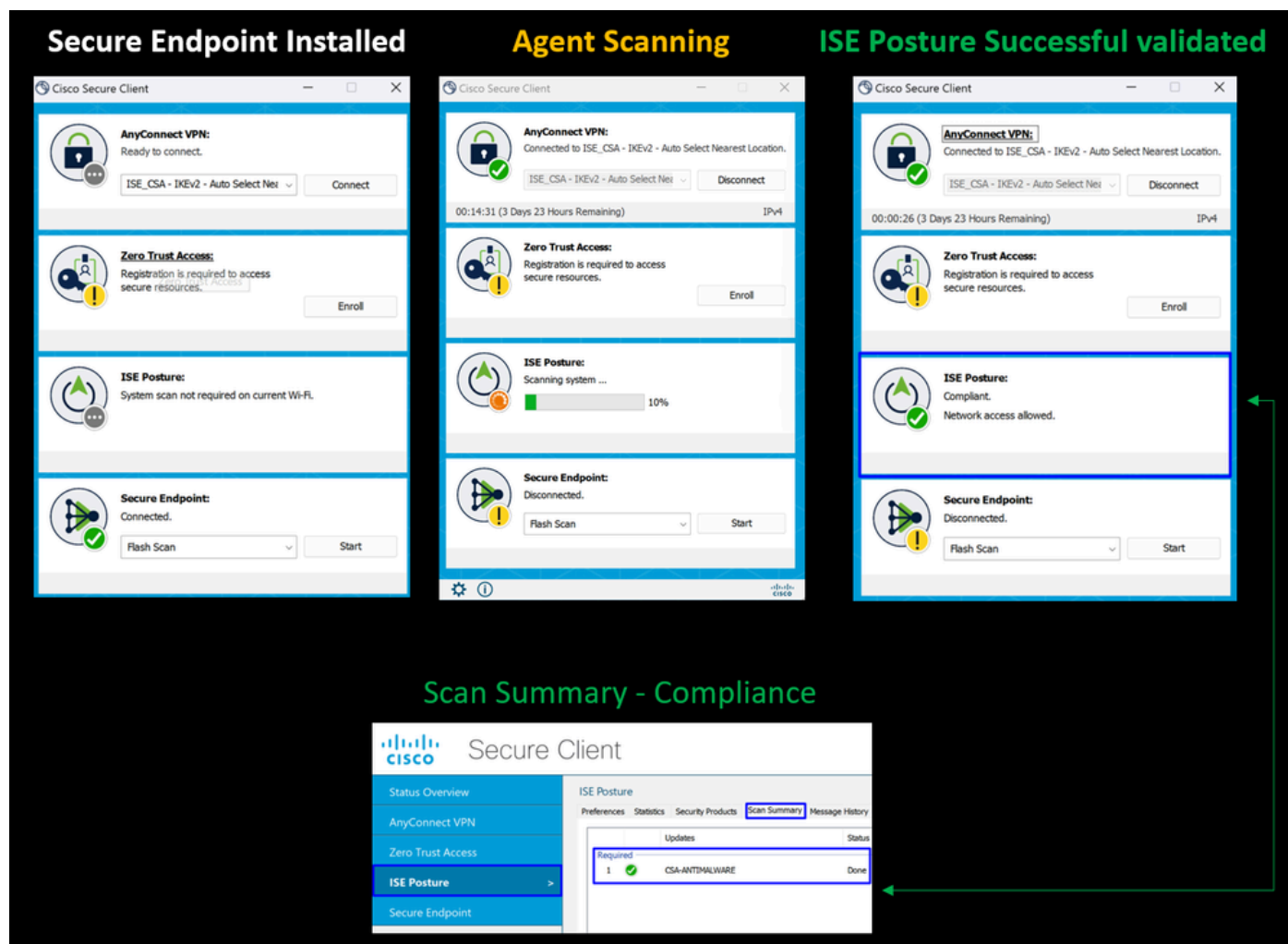
More Details >

Cancel

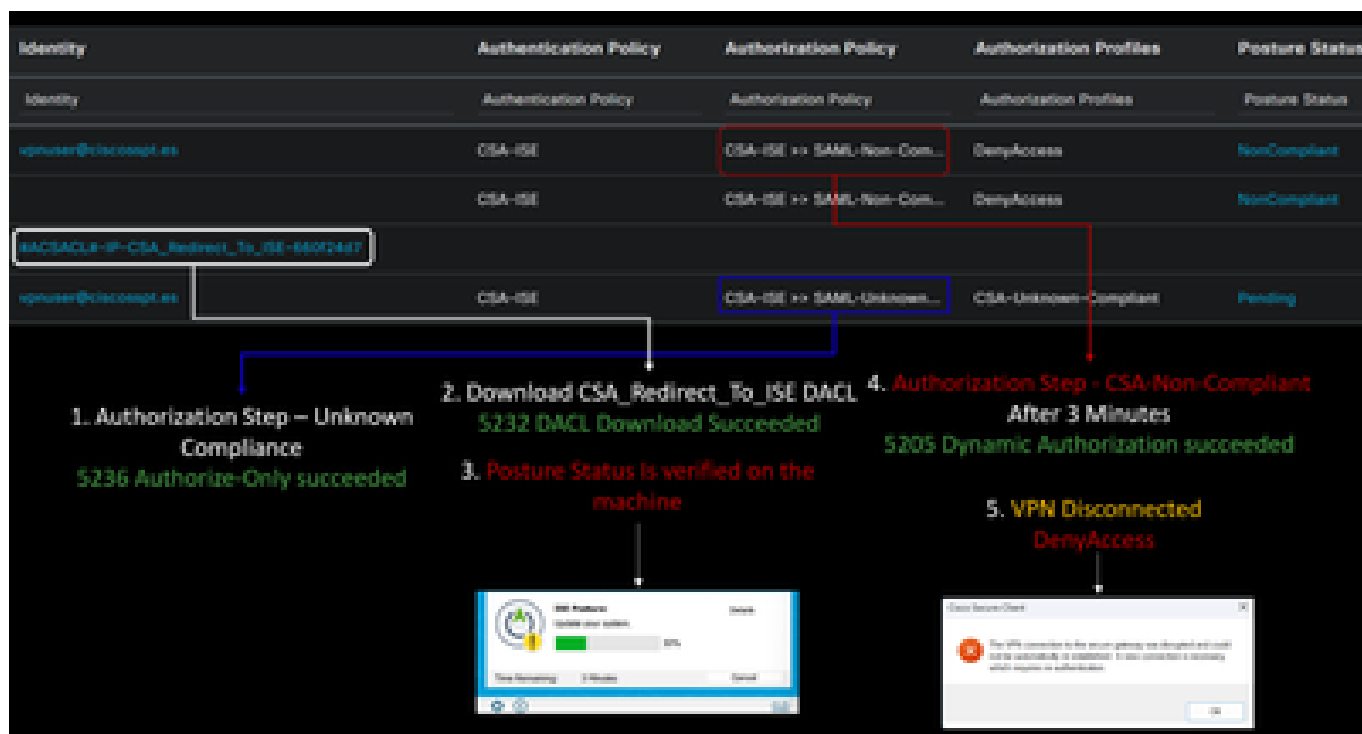


Observação: se você Cancel ou o tempo restante terminar, você se tornará automaticamente não compatível, se enquadra no conjunto de políticas de autorização [CSA-Não-Conformidade](#) e será imediatamente desconectado da VPN.

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

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
		#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
		#ACSACL#-IP-CSA-Compliant-660bdb5e	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
		#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia

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

Conformidade

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
#ACSACL#-IP-CSA-Compliant-660bdb5e				
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscospt.es	CSA-ISE	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-Compliant
5205 Dynamic Authorization succeeded

5. Download CSA-Compliant
5232 DACL Download Succeeded

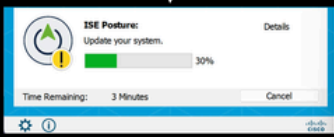

ISE Posture:
Compliant.
Network access allowed.

Não-conformidade

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending

#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7

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

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**

HomeFTD	Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-----------	------------------	---------------	---	---------------

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

Summary



Connected

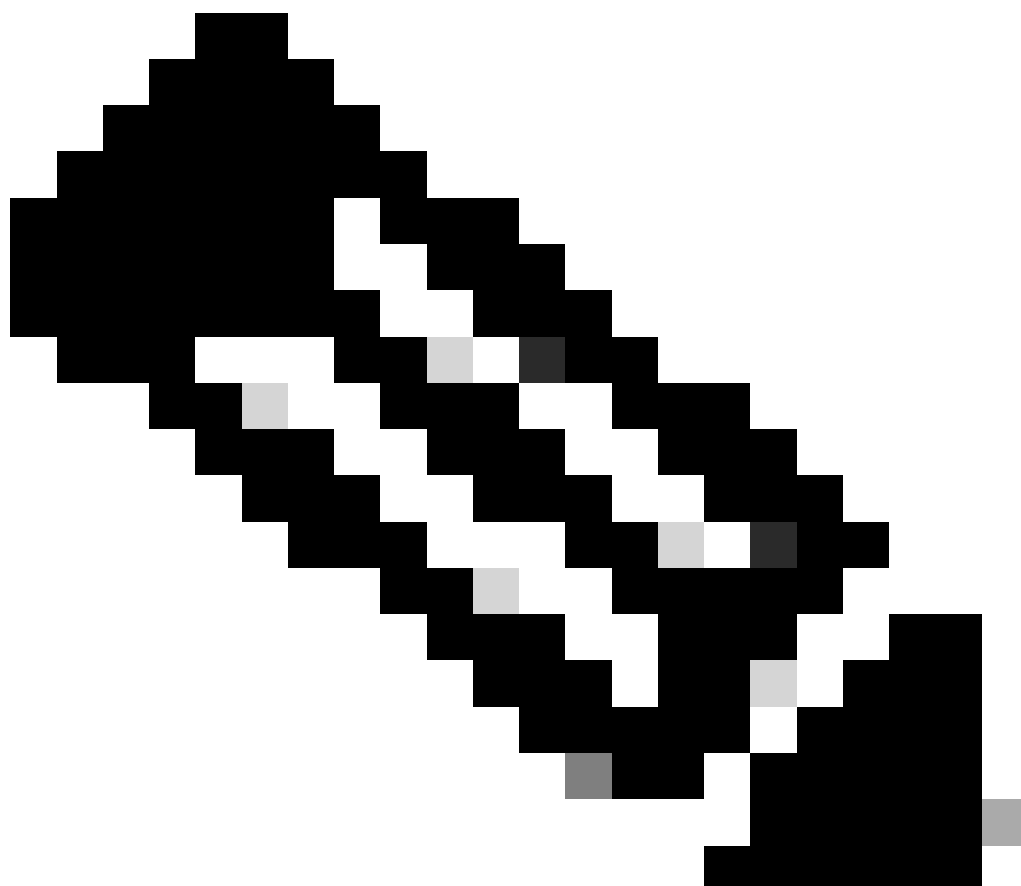
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2: permita o tráfego no seu firewall.

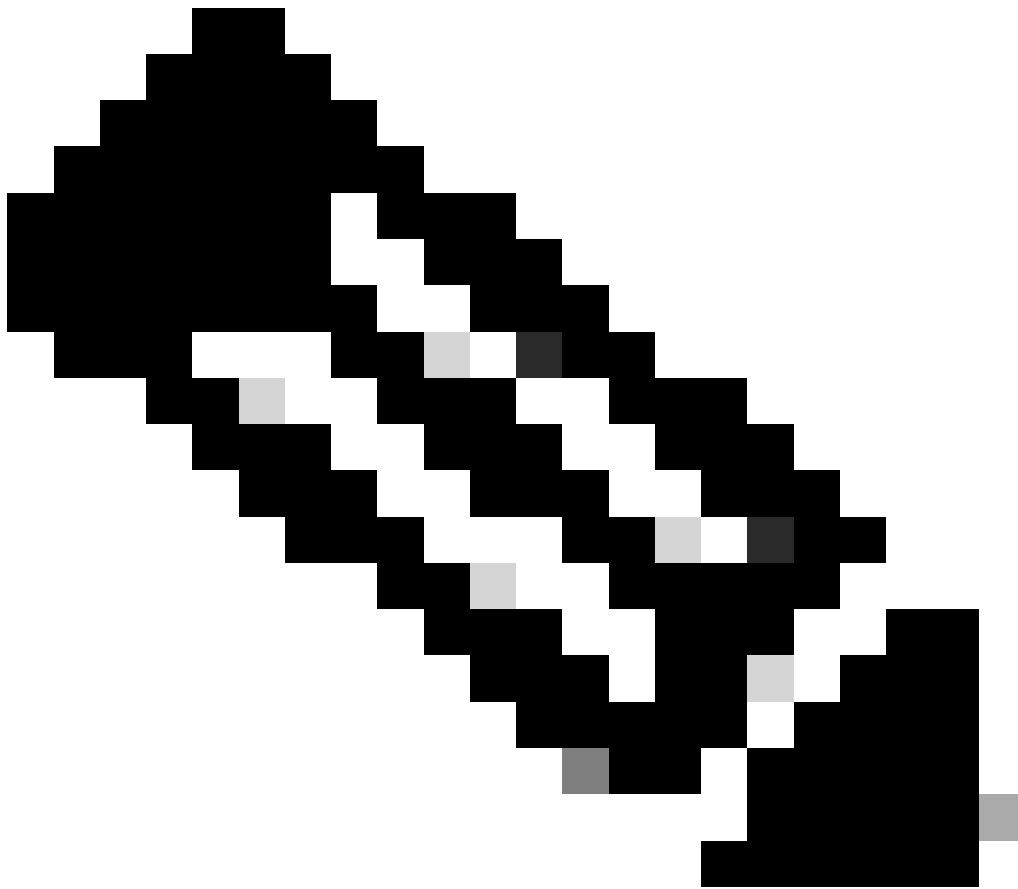
Para permitir o acesso seguro para usar seu dispositivo ISE para autenticação Radius, você precisa ter configurado uma regra de acesso seguro à sua rede com as portas Radius necessárias:

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**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups	
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA	 

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

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#) 

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

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**, 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

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


Action

 Allow Allow specified traffic if security requirements are met.	 Block Block specified traffic.
---	--


From Specify one or more sources . <input type="text" value="CSA (ciscospt.es\CSA)"/>	To Specify one or more destinations . <input type="text" value="CiscoISE"/>
Information about sources, including selecting multiple sources. Help	Information about destinations, including selecting multiple destinations. Help

Endpoint Requirements

For VPN connections:

-  End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [?](#)
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

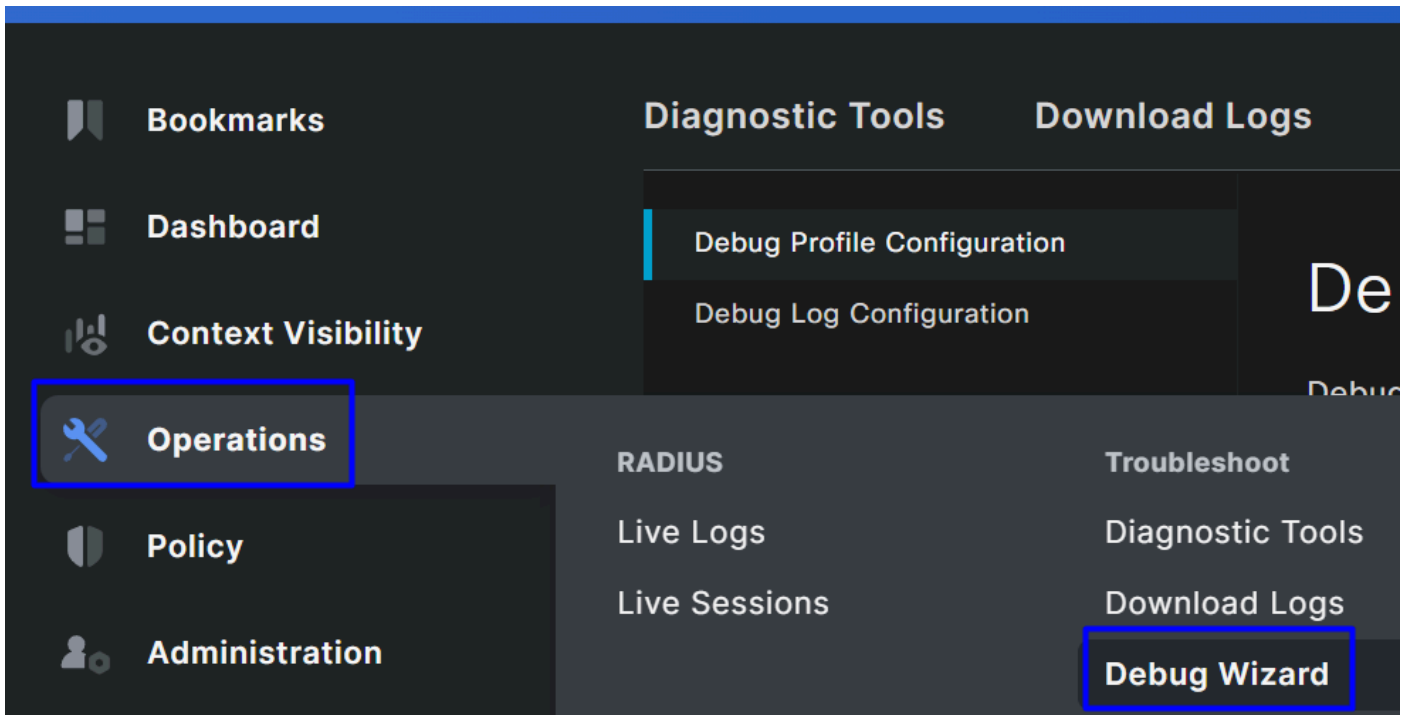
-  Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Troubleshooting

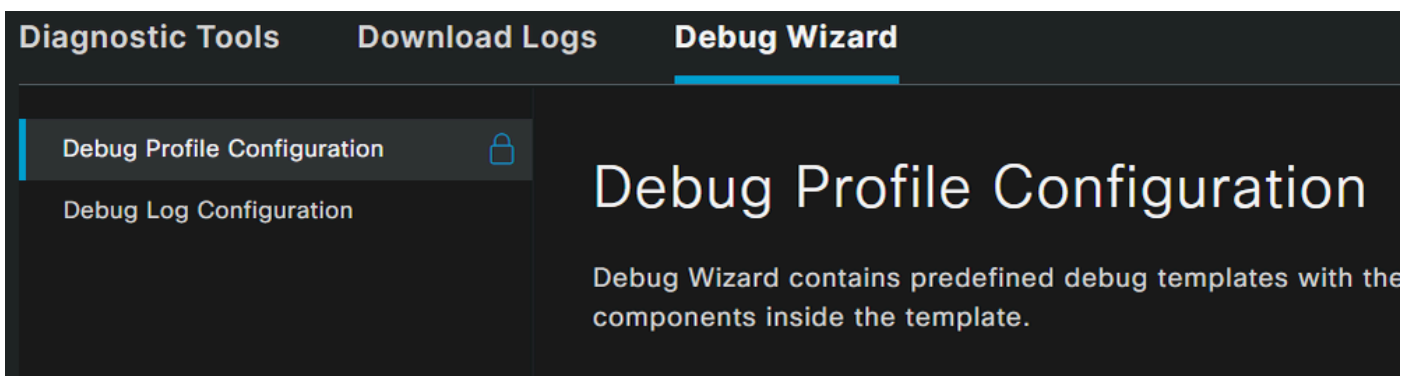
Como baixar logs de depuração de postura do ISE

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

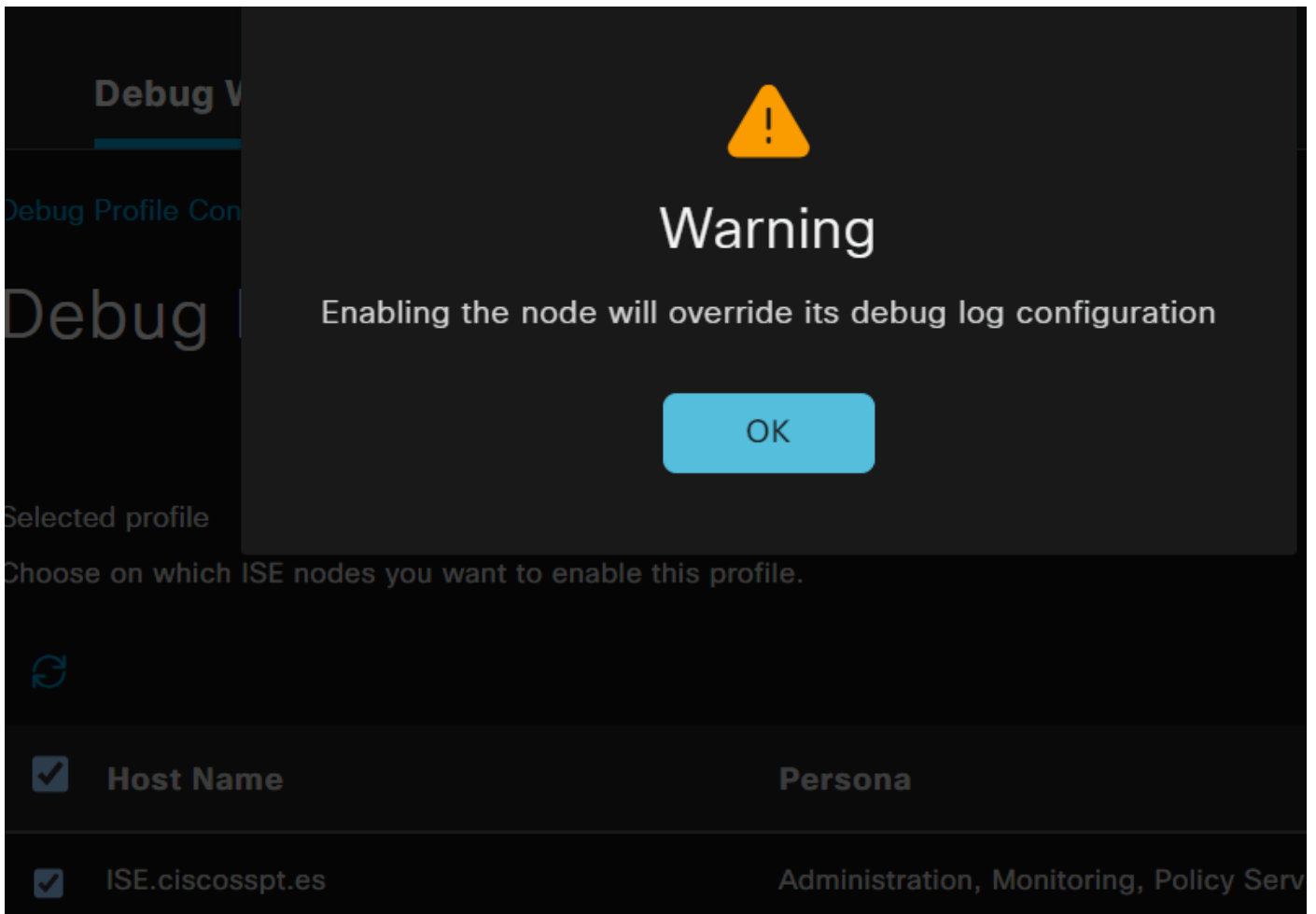
1



Posture

Pos

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



The image shows a warning dialog box overlaid on a configuration page. The dialog box has a dark background with a yellow warning triangle icon at the top center. Below the icon, the word "Warning" is displayed in a large, white font. Underneath, the message "Enabling the node will override its debug log configuration" is shown in a smaller white font. At the bottom of the dialog is a blue button with the text "OK".

The background configuration page is partially visible and includes the following elements:


- Section header: **Debug V**
- Section header: **Debug Profile Con**
- Section header: **Debug**
- Text: Selected profile
- Text: Choose on which ISE nodes you want to enable this profile.
- Refresh icon (circular arrow)
- Table with columns: **Host Name** and **Persona**
- Table row 1: Host Name, Persona
- Table row 2: ISE.ciscosspt.es, Administration, Monitoring, Policy Serv

- Clique em Save

Debug Nodes

Selected profile Posture

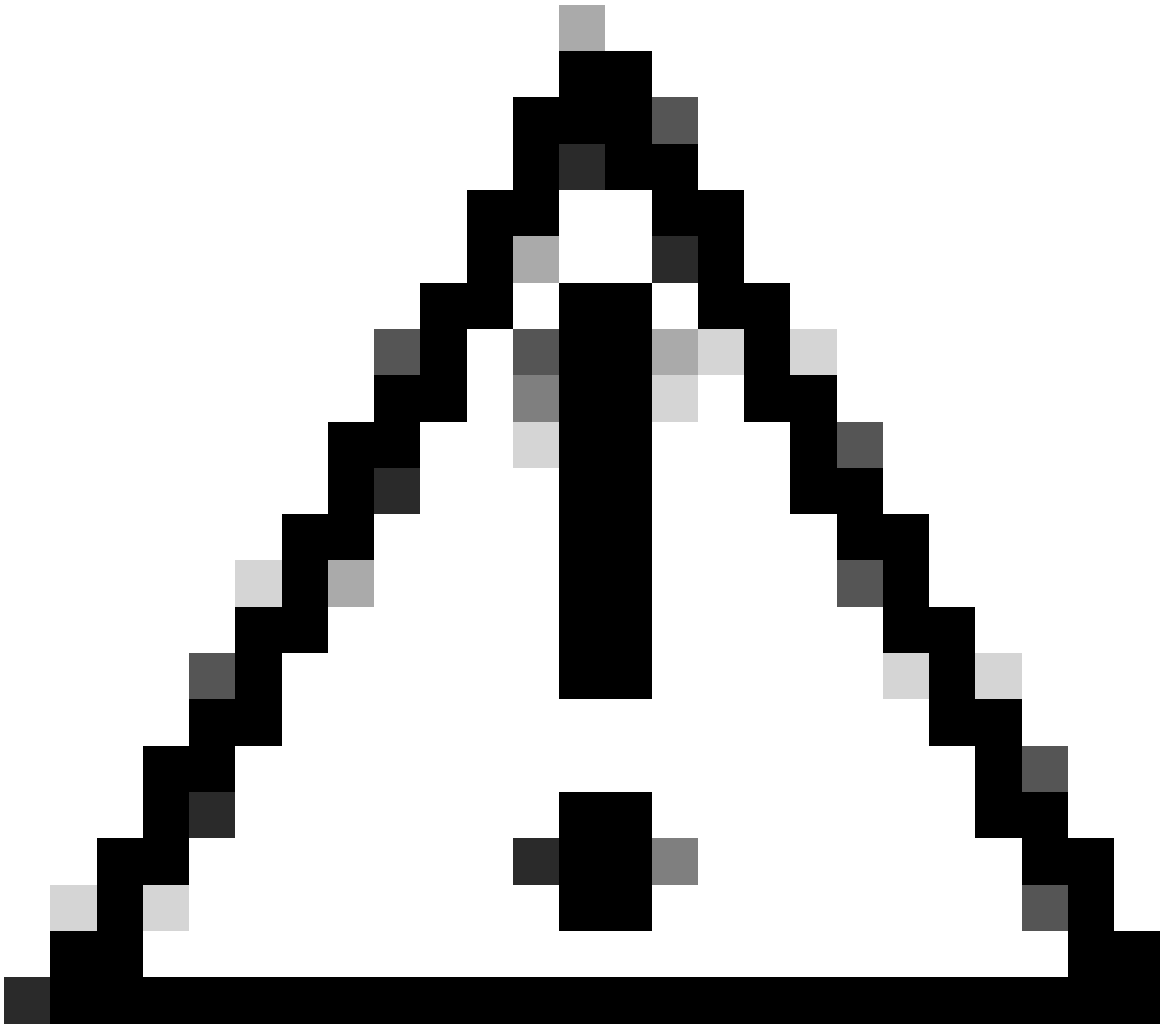
Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

Cancel

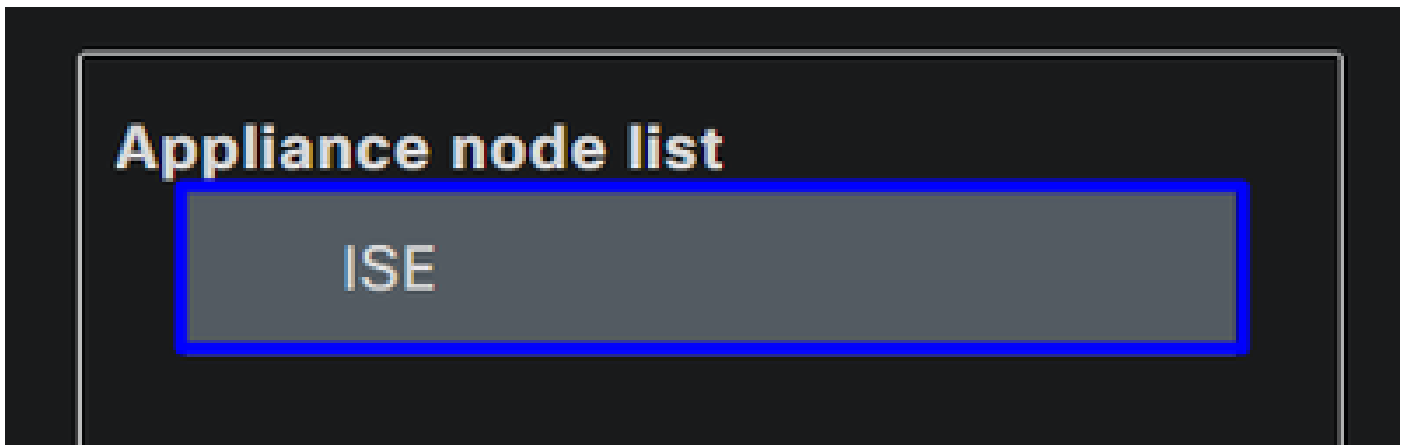
Save



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:

Support Bundle

Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- 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**

Support Bundle - Last Generated

File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

Download

Delete


















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

100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

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.