# Configuración de Secure Access para RA-VPNaaS con Duo SSO y evaluación de estado con ISE

## Contenido

# Introducción

Este documento describe cómo configurar la evaluación de estado para usuarios de VPN de acceso remoto con Identity Service Engine (ISE) y Secure Access con Duo.

# Prerequisites

- Configuración del aprovisionamiento de usuarios en Secure Access
- Configuración de Duo SSO con Proxy de autenticación o IDP de terceros
- Cisco ISE conectado a Secure Access a través del túnel

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Service Engine
- Acceso seguro
- Cliente seguro de Cisco
- Guía para la autenticación de dos factores: seguridad Duo
- Condición de ISE
- Autenticación, autorización y contabilidad

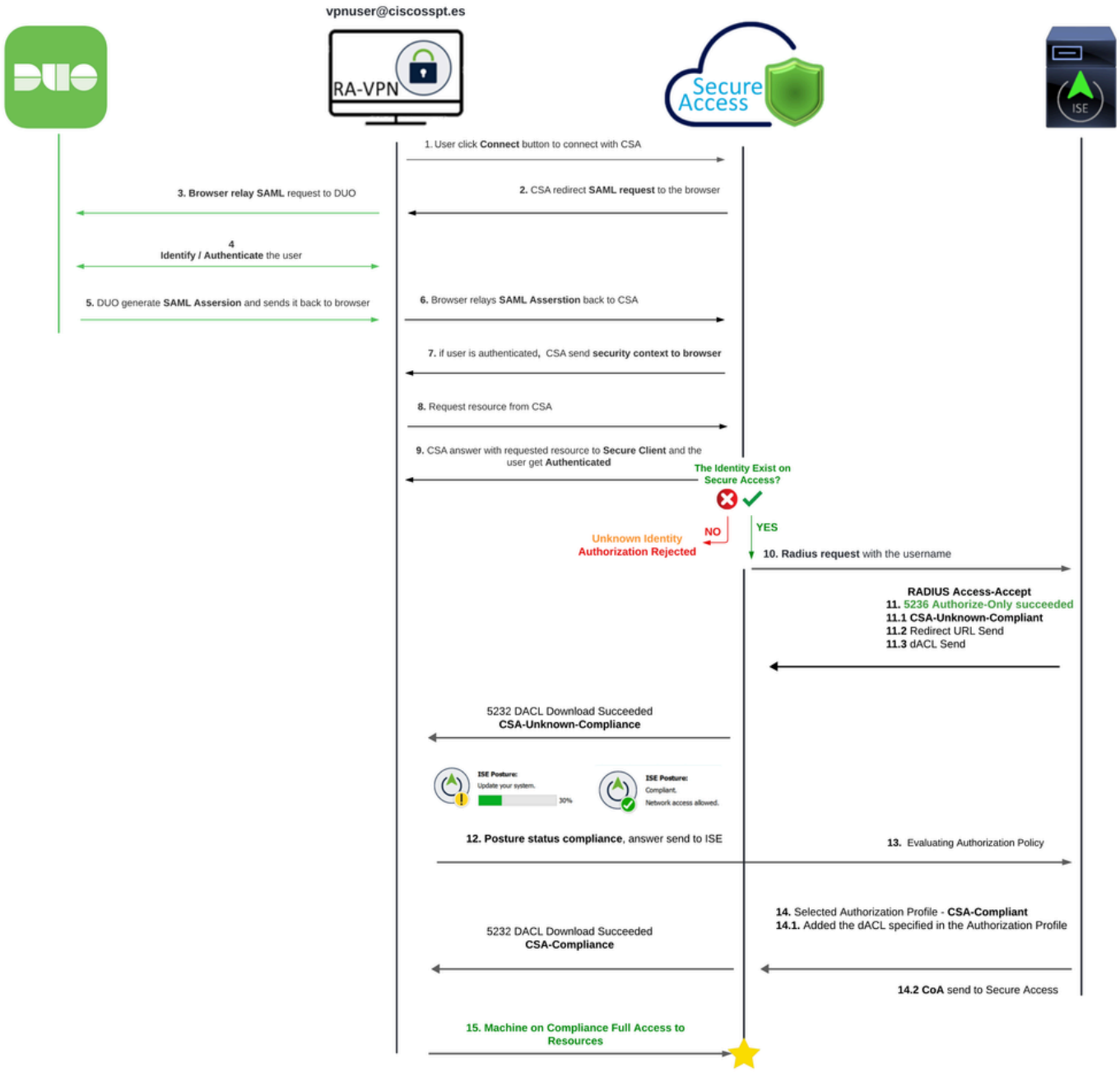
## Componentes Utilizados

La información de este documento se basa en:

- Parche 1 de Identity Service Engine (ISE) versión 3.3
- Acceso seguro
- Cisco Secure Client - Anyconnect VPN Versión 5.1.2.42

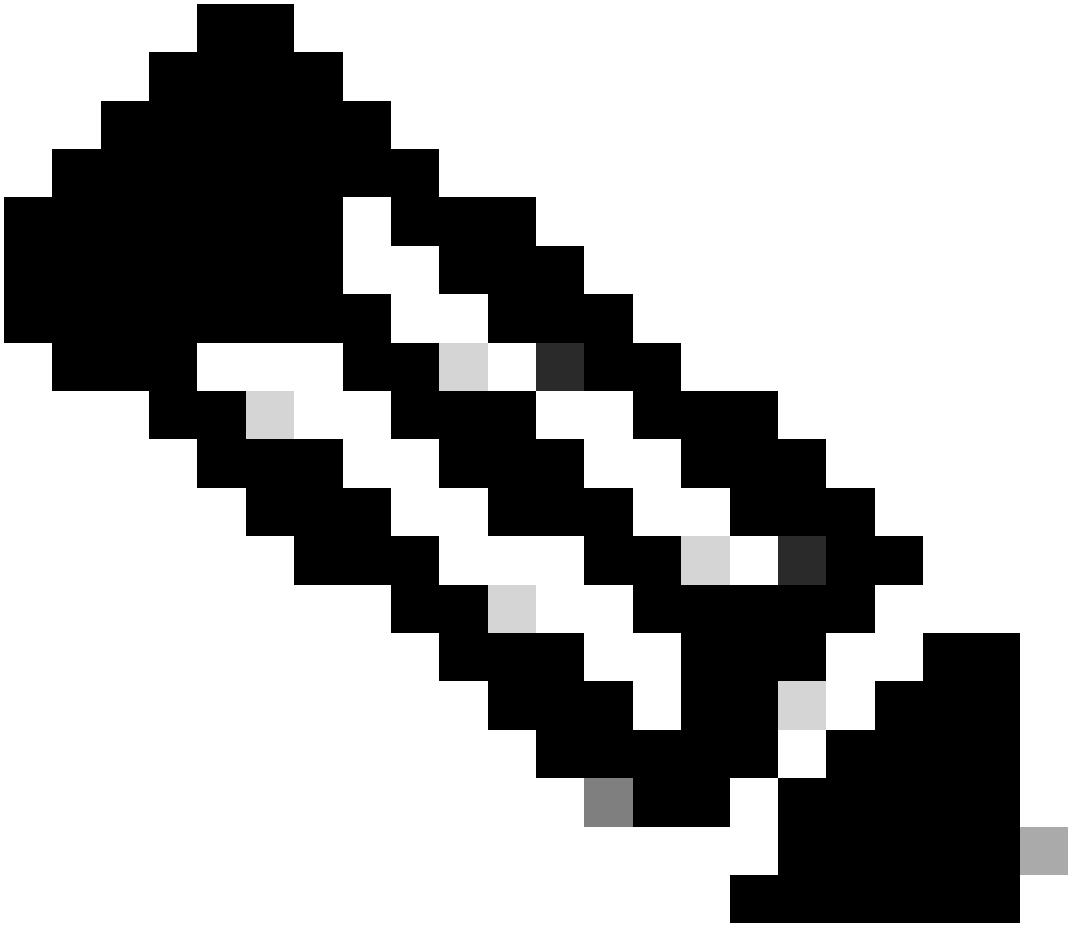
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes



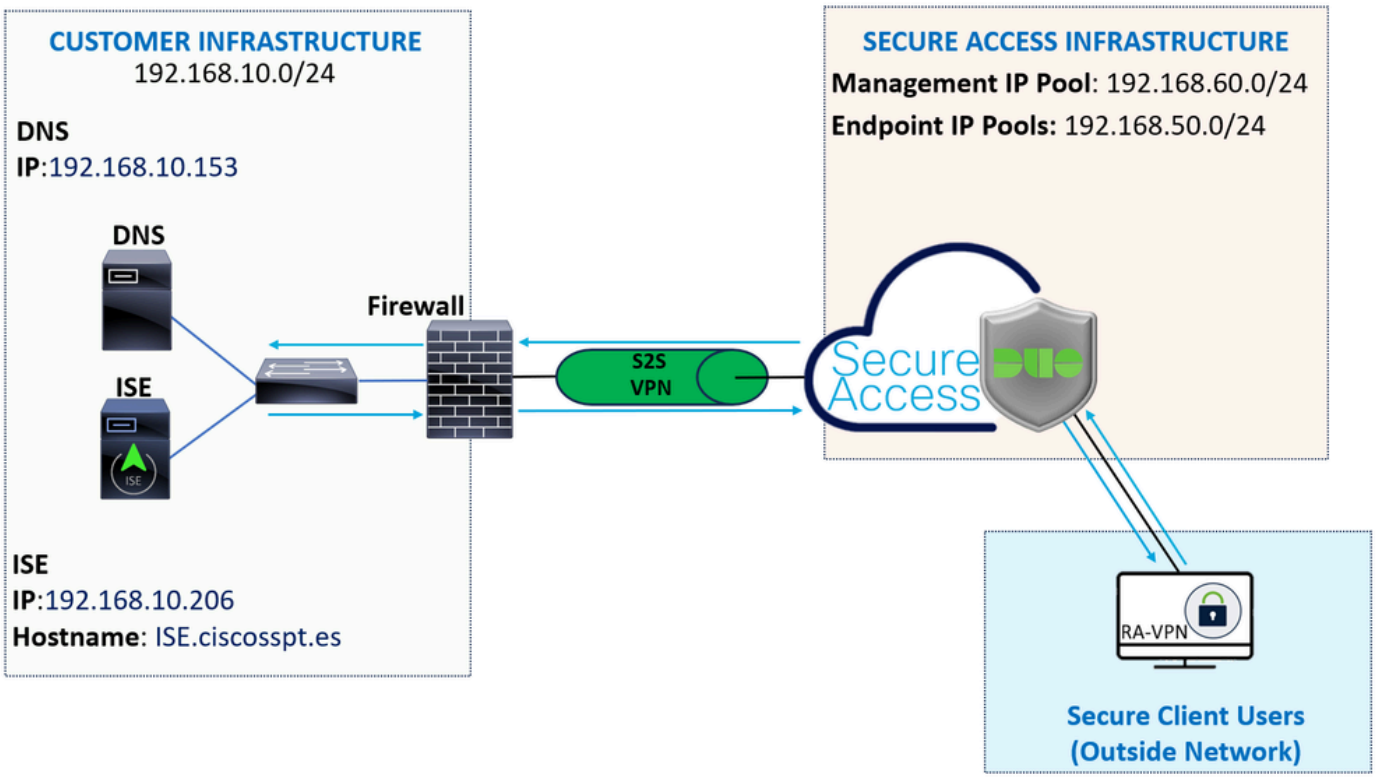

La integración de Duo SAML con Cisco Identity Services Engine (ISE) mejora el proceso de autenticación, añadiendo otra capa de seguridad a las soluciones Cisco Secure Access. Duo SAML proporciona una capacidad de inicio de sesión único (SSO) que simplifica el proceso de inicio de sesión del usuario al tiempo que garantiza unos altos estándares de seguridad.

Una vez autenticado a través de Duo SAML, el proceso de autorización es gestionado por Cisco ISE. Esto permite tomar decisiones de control de acceso dinámico basadas en la identidad del usuario y el estado del dispositivo. ISE puede aplicar políticas detalladas que establecen a qué recursos puede acceder un usuario, cuándo y desde qué dispositivos.

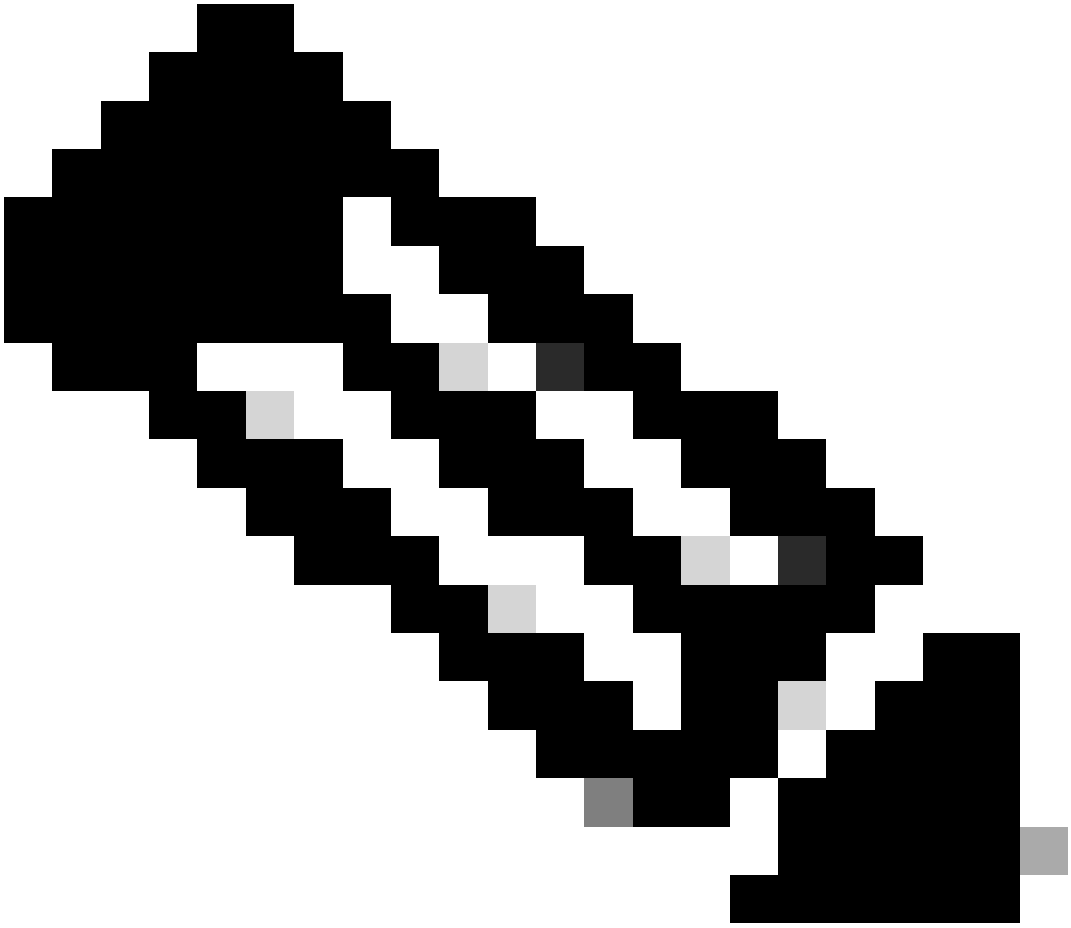


Nota: Para configurar la integración RADIUS, debe asegurarse de que tiene comunicación entre ambas plataformas.

## Diagrama de la red


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



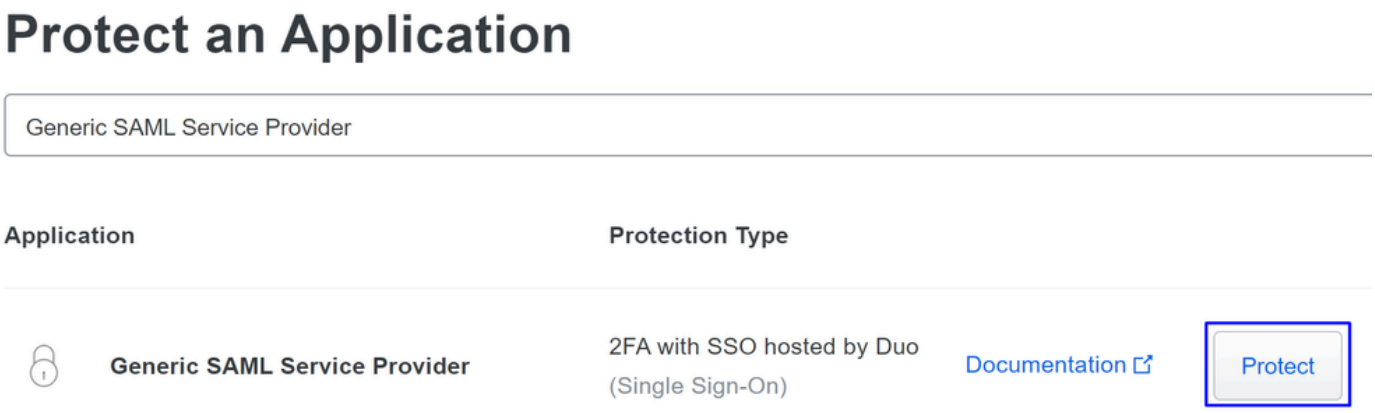
Nota: antes de comenzar el proceso de configuración, debe completar los Primeros pasos con Secure Access e integración con ISE.

## Configuración Duo

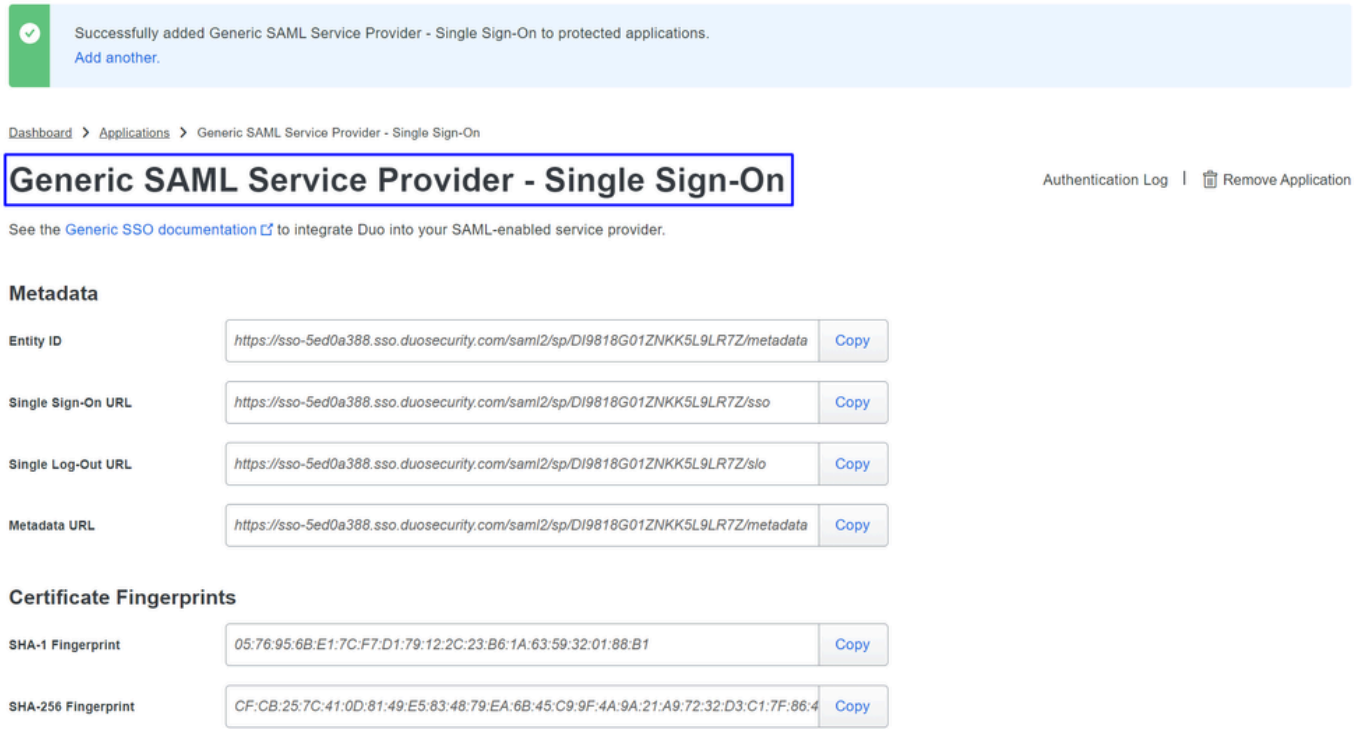
Para configurar la aplicación RA-VPN, continúe con los siguientes pasos:

Vaya al panel Duo Admin

- Desplácese hasta **Applications > Protect an Application**
  - Buscar por **Generic SAML Service Provider**
  - Haga clic en Protect




Debe mostrar la aplicación en la pantalla; recuerde el nombre de la aplicación para la configuración VPN.




En este caso es **Generic SAML Service Provider.**

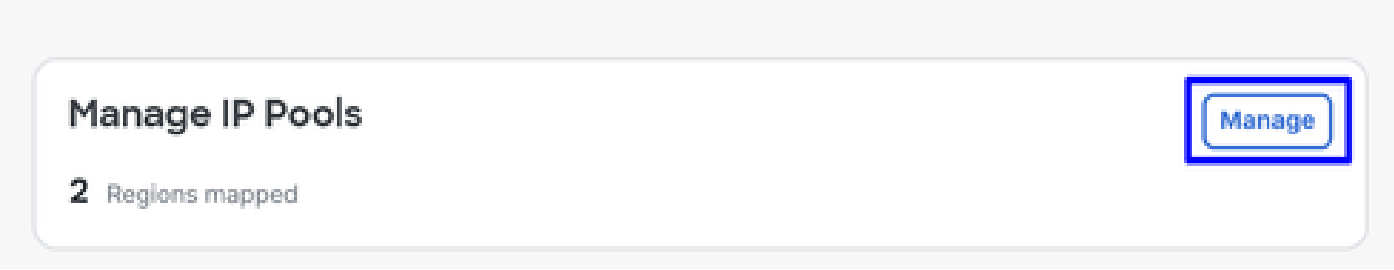
Configuración de Secure Access

Configuración del Grupo Radius en los Pools IP

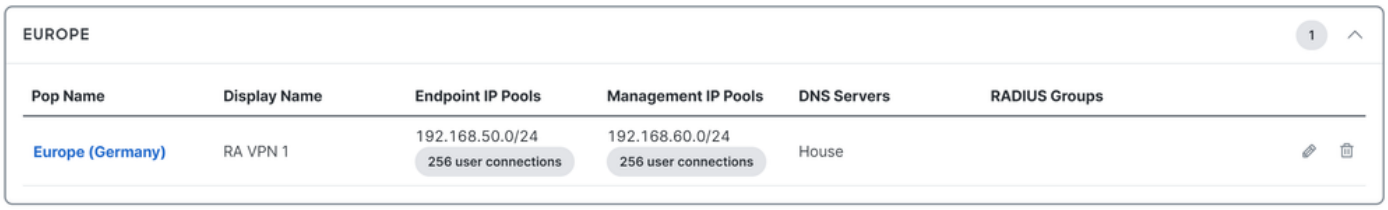
Para configurar el perfil VPN mediante Radius, siga con los siguientes pasos:

Desplácese hasta el panel de acceso seguro.

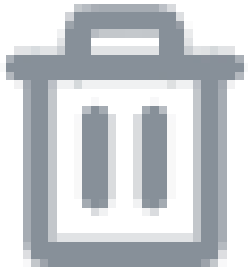
- Haga clic en **Connect > Enduser Connectivity > Virtual Private Network**
- En Configuración del grupo (**Manage IP Pools**), haga clic enManage




- Elija el **IP Pool Region** y configure el **Radius Server**

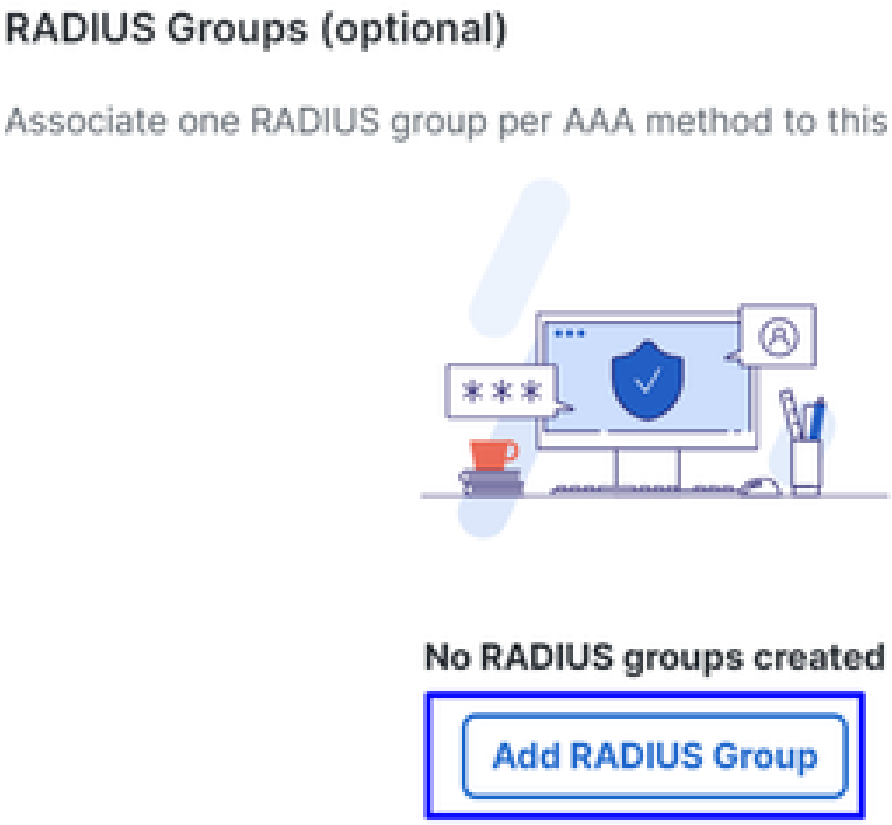



- Haga clic en el lápiz para editarlo



- Ahora, en el menú desplegable de configuración de la sección Pool IP, en **Radius Group (Optional)**

- Haga clic en 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 un nombre para la integración de ISE en Secure Access

- **AAA method**

  - **Authentication**: marque la casilla de verificación para **Authentication** y seleccione el puerto, de forma predeterminada, es 1812

    - En caso de que su autenticación requiera Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2) marcar la casilla de verificación

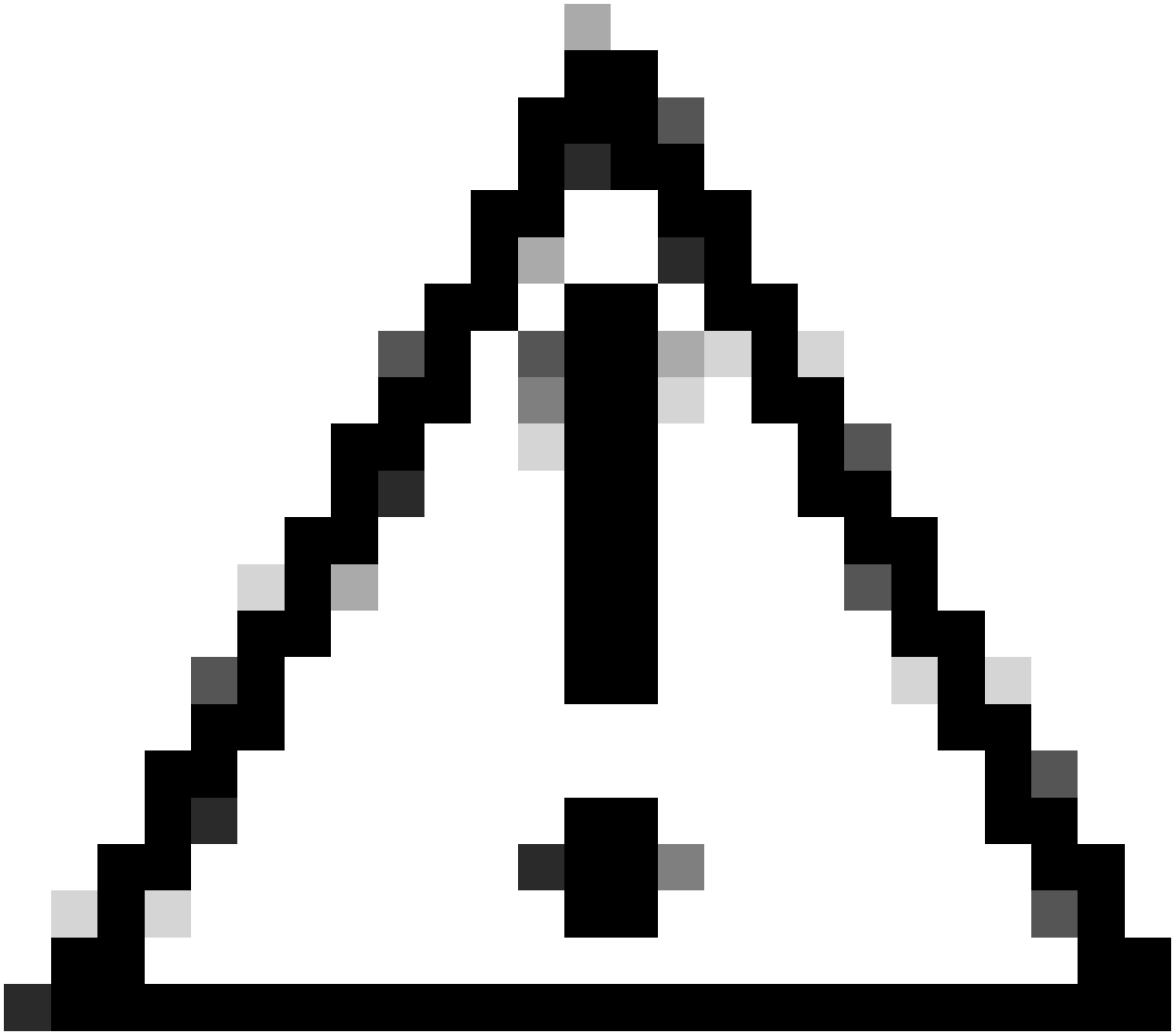
• **Authorization**: Marque la casilla de verificación Authorization y seleccione el puerto, de forma predeterminada, es 1812

  - Marque la casilla de verificación de **Authorization mode Only Change of Authorization (CoA) mode** y para permitir el estado y los cambios desde ISE

• **Accounting**: marque la casilla de verificación de Autorización y seleccione el puerto, de forma predeterminada, es 1813

  - Elija **Single or Simultaneous** (en modo único, los datos de cuentas se envían a un solo servidor. En modo simultáneo, contabilizando datos en todos los servidores del grupo)

    • Marque la casilla de verificación **Accounting update** para habilitar la generación periódica de mensajes de actualización de cuentas provisionales de RADIUS.

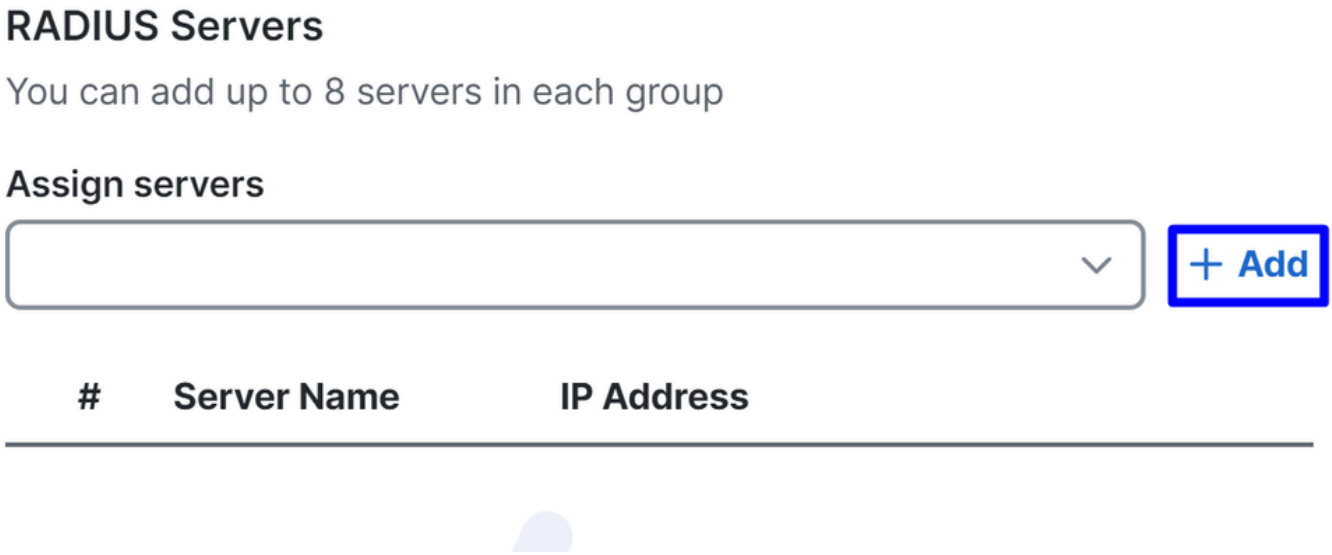


**Precaución**: tanto el Authenticationmétodo como los **Authorization** métodos, cuando se seleccionan, deben utilizar el mismo puerto.

---

- Después de eso, debe configurar el **RADIUS Servers** (ISE) que se utiliza para autenticarse a través de AAA en la sección **RADIUS Servers**:

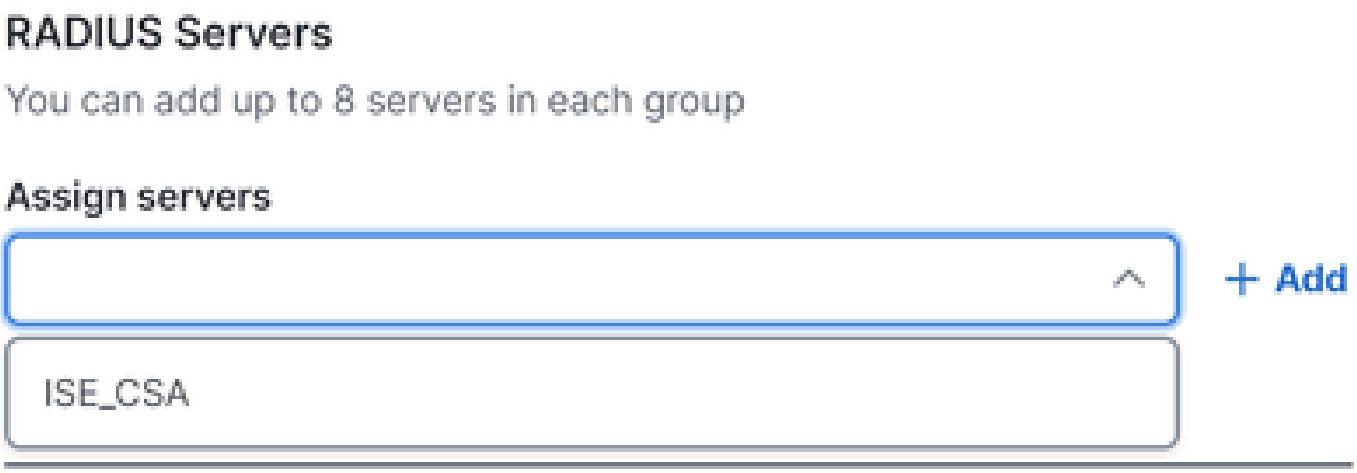
- Haga clic en + Add




- A continuación, configure las siguientes opciones:

- Server Name: configure un nombre para identificar su servidor ISE.
- **IP Address**: configure la IP de su dispositivo Cisco ISE a la que se puede acceder a través de Secure Access
- **Secret Key**: Configure la clave secreta RADIUS
- **Password**: Configure la contraseña de Radius

- Haga clic **Save** y asigne su servidor Radius en la Assign Serveropción y seleccione su servidor ISE:




- Haga clic de **Save** nuevo para guardar toda la configuración realizada

# ← 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**

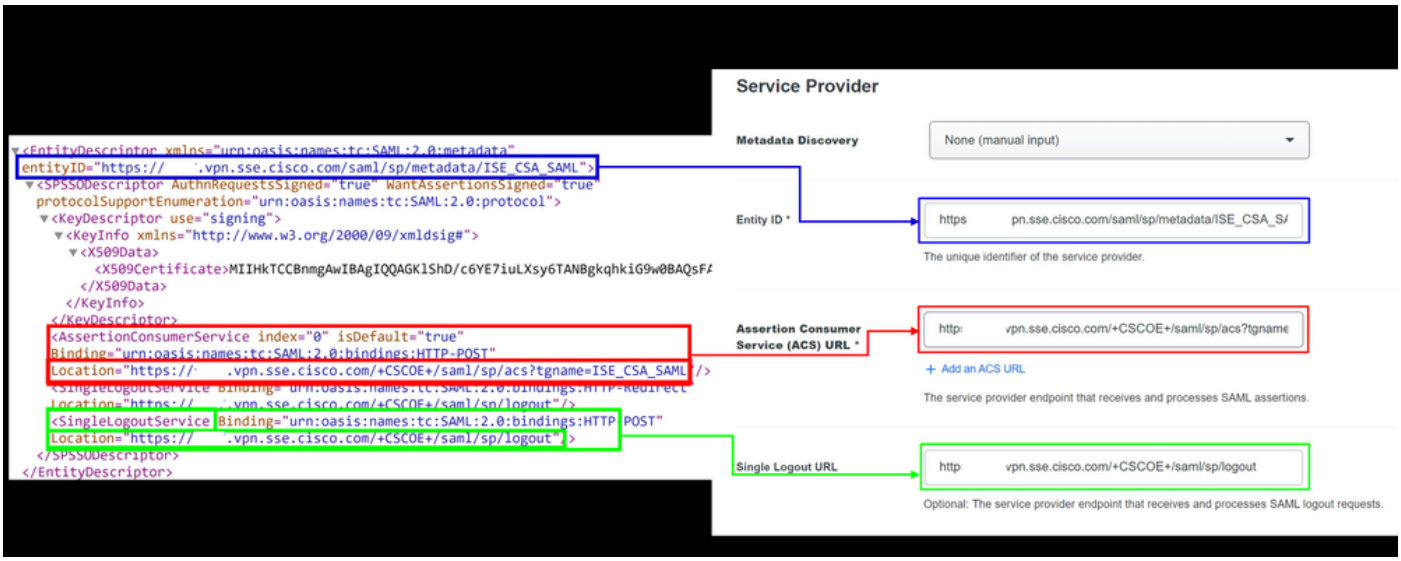
ISE_CSA

+ Add

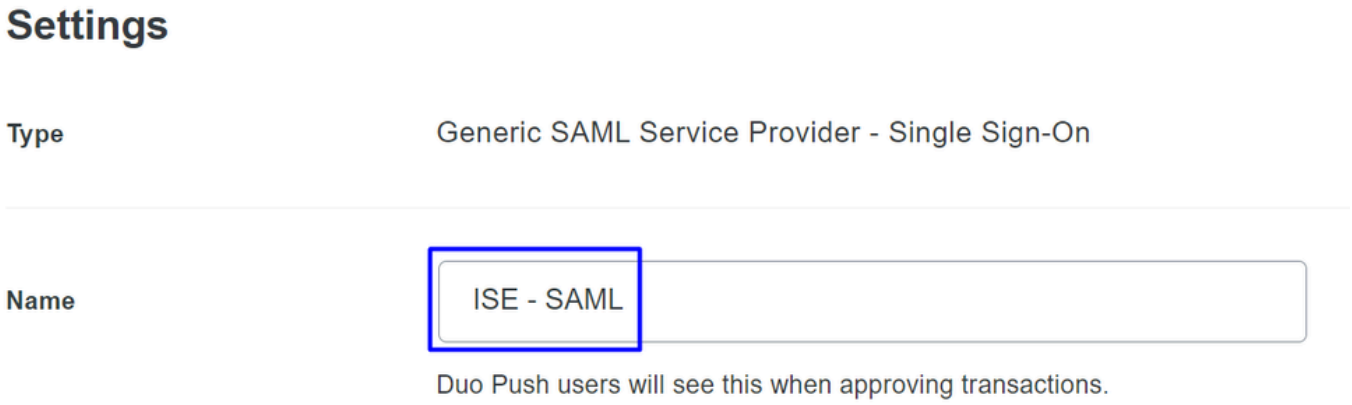
| # | Server Name | IP Address |
|---|---|---|
| 1 | ISE_CSA | 192.168.10.206 |

- **Protocols**: Elegir **SAML**

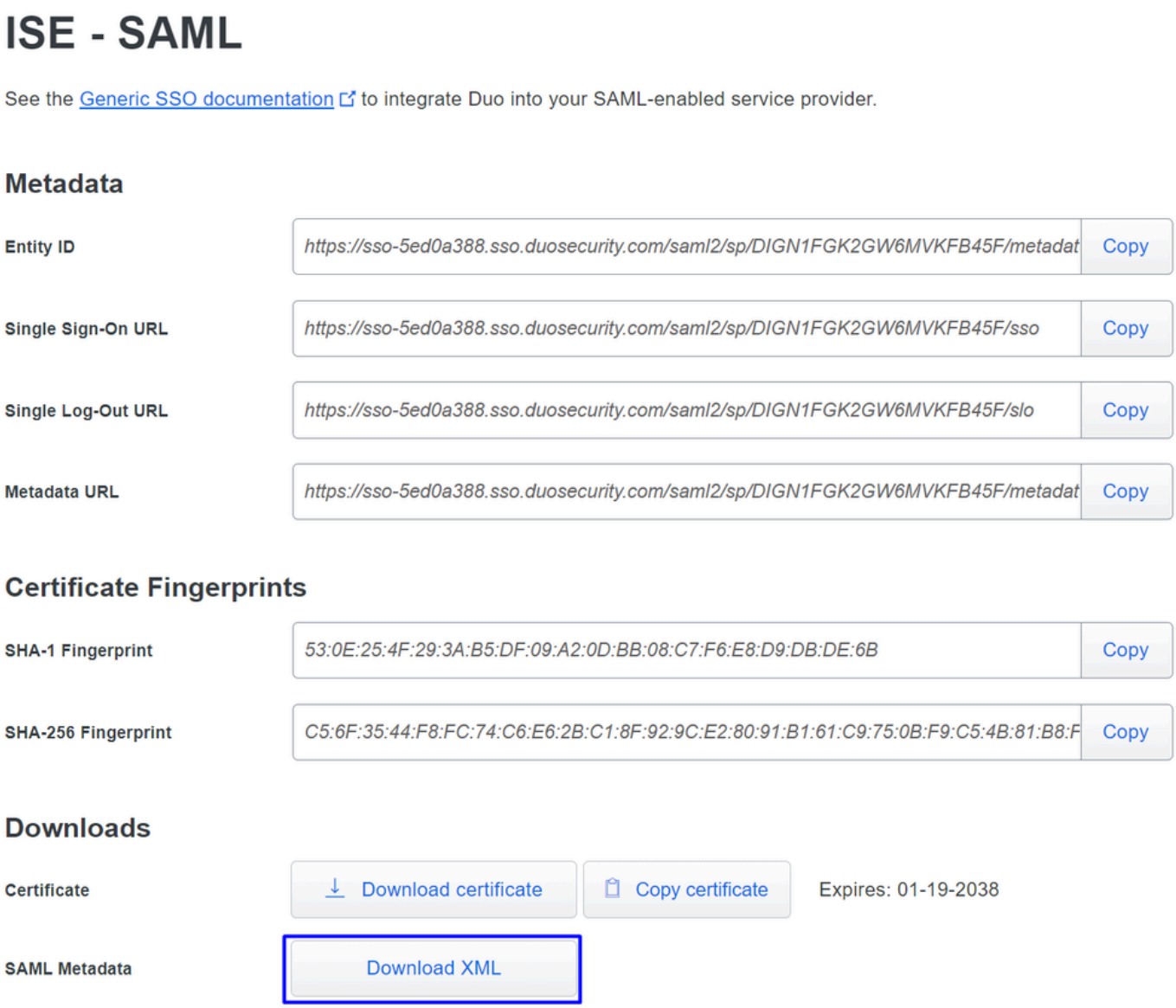
- Haga clic en Download Service Provider XML file
- Reemplace la información de la aplicación configurada en el paso Duo Configuration.



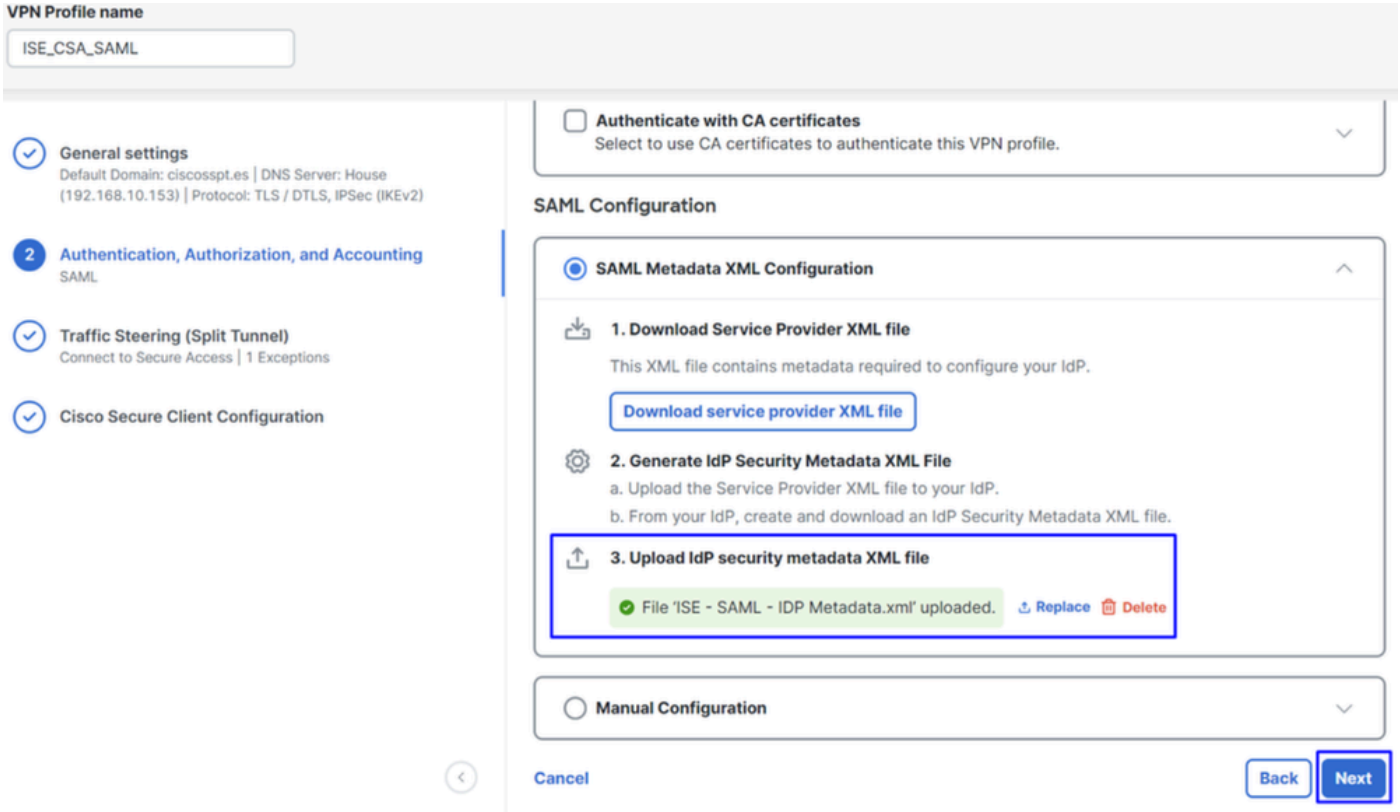

- Una vez que haya configurado esa información, cambie el nombre del Duo por otro relacionado con la integración que esté realizando



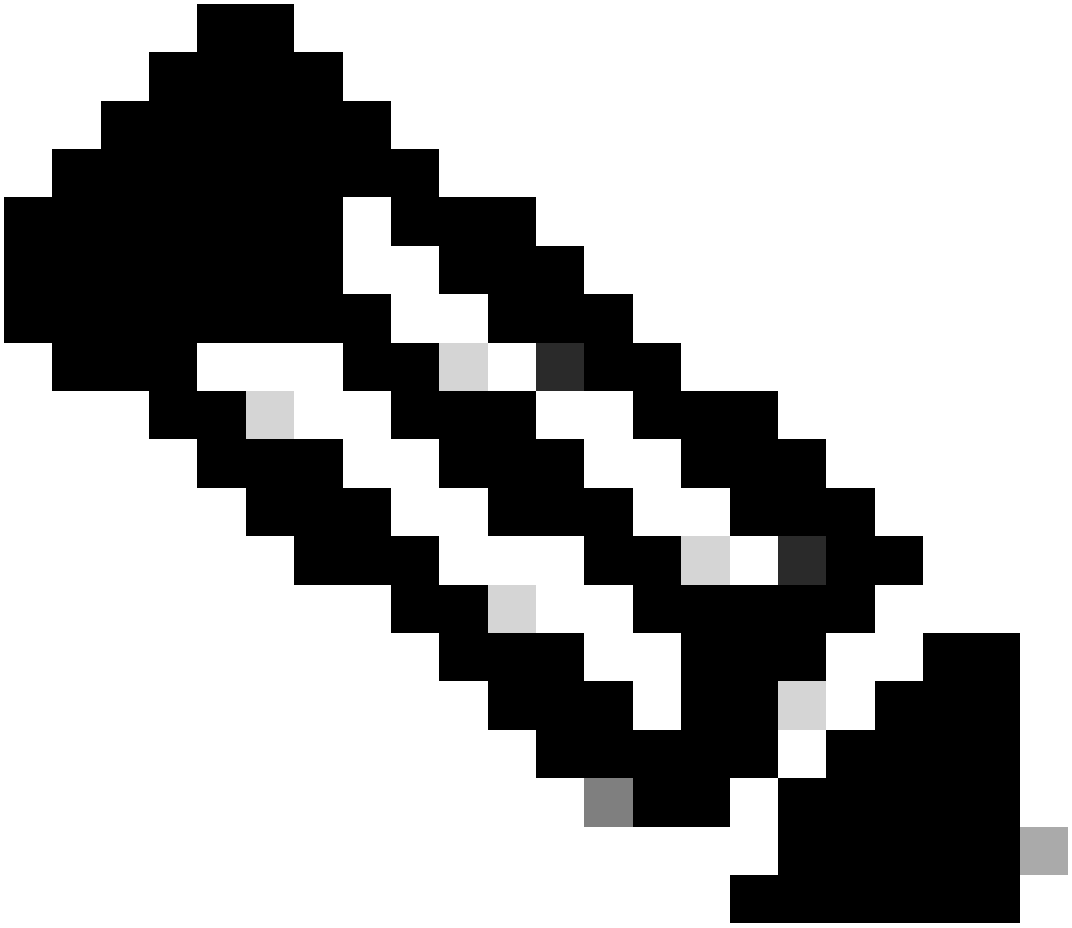

- Haga clic **Save** en Duo en la aplicación.
- Una vez que haga clic en Save (Guardar), debe descargar el **SAML Metadata** mediante el botón **Download XML**




- Cargue el **SAML Metadata** en Secure Access debajo de la opción **3. Upload IdP security metadata XML file** y haga clic en **Next**

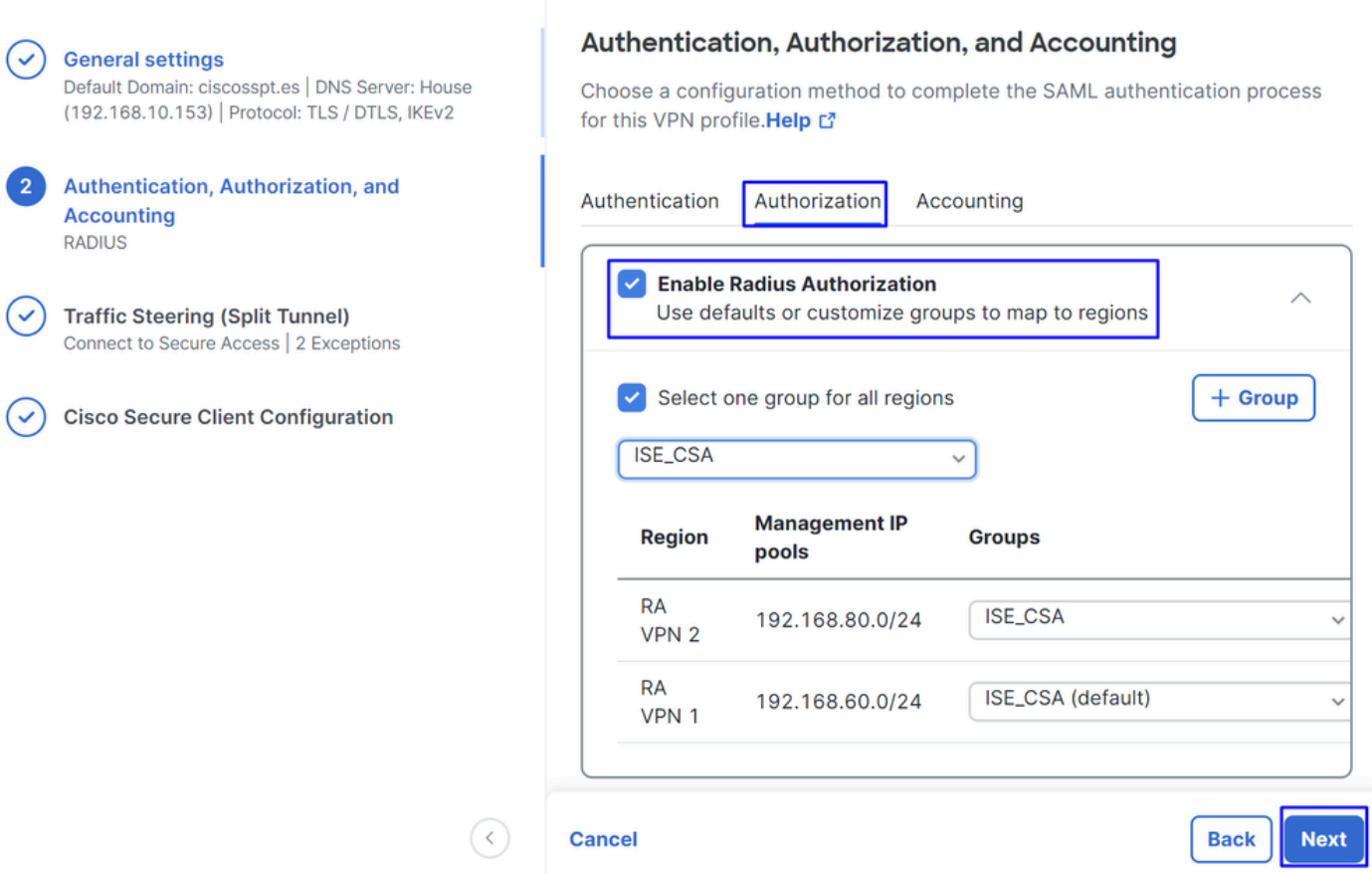



Continúe con la autorización.



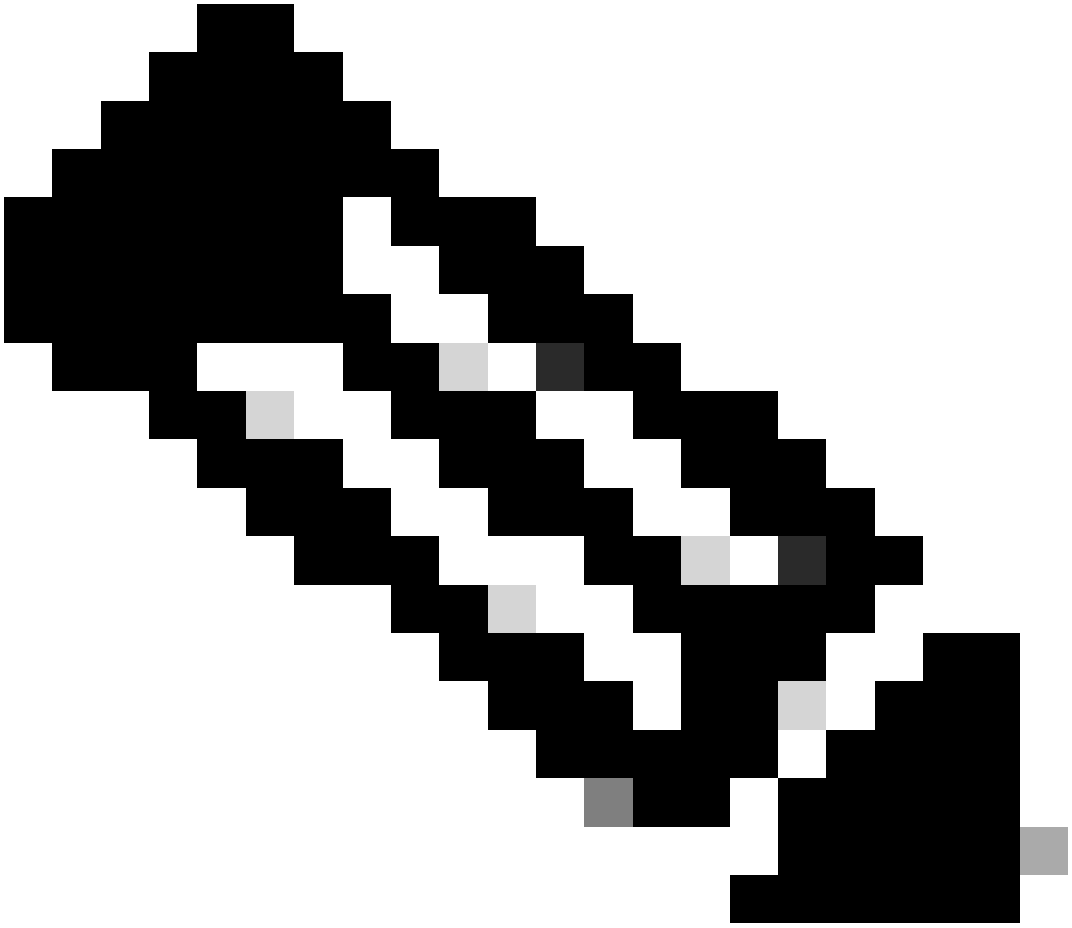
**Nota**: Una vez que configure la autenticación con SAML, la autorizará a través de ISE, lo que significa que el paquete RADIUS enviado por Secure Access sólo contendrá el nombre de usuario. El campo de contraseña no existe aquí.

**Autorización**



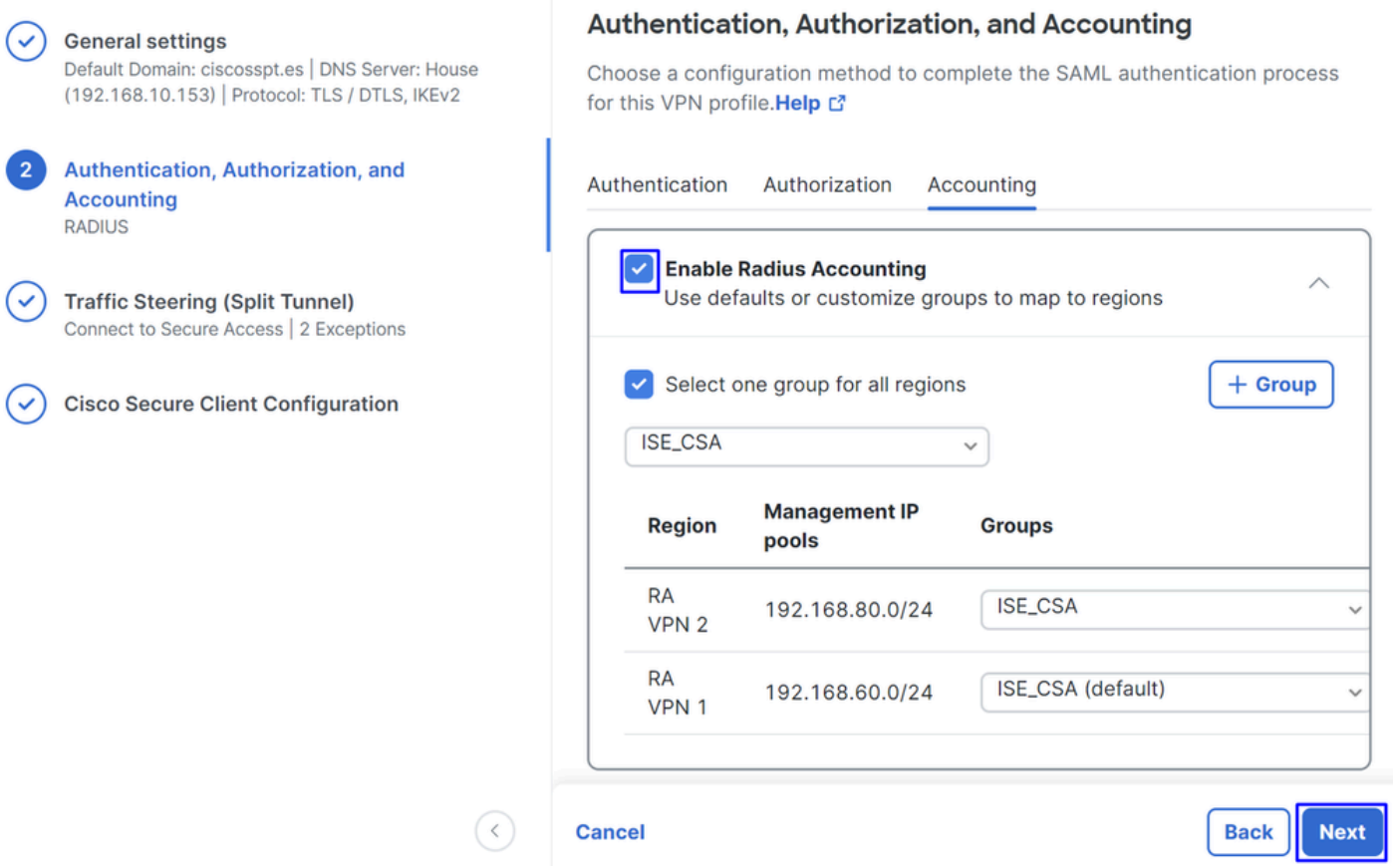

- **Authorization**
  - **Enable Radius Authorization**: marque la casilla de verificación para activar la autorización de RADIUS
  - **Seleccione un grupo para todas las regiones**: marque la casilla de verificación para utilizar un servidor RADIUS específico para todos los grupos de acceso remoto - Red privada virtual (RA-VPN) o defínalo para cada grupo por separado
- Haga clic en **Next**

Después de configurar toda la **Authorization** pieza, continúe con la **Accounting**.



**Nota**: Si no activa esta opción, **Radio Authorization**la postura no funcionará.

**Contabilidad**

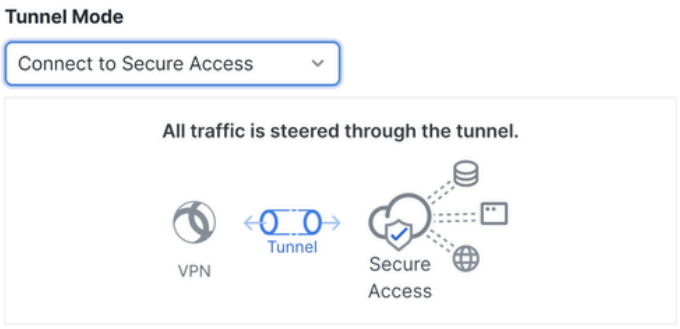


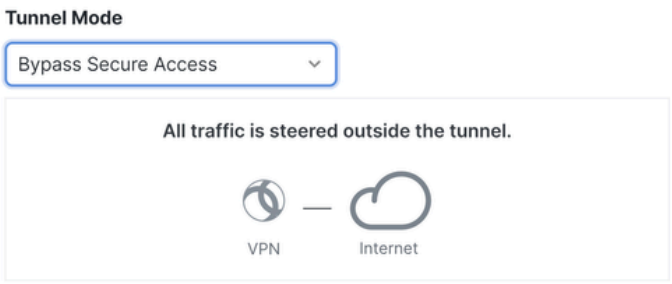

- **Accounting**
    - **Map Authorization groups to regions**: Elija las regiones y elija su **Radius Groups**
- Haga clic en **Next**

After you have done configured the Authentication, Authorization and Accounting continúe conTraffic Steering.

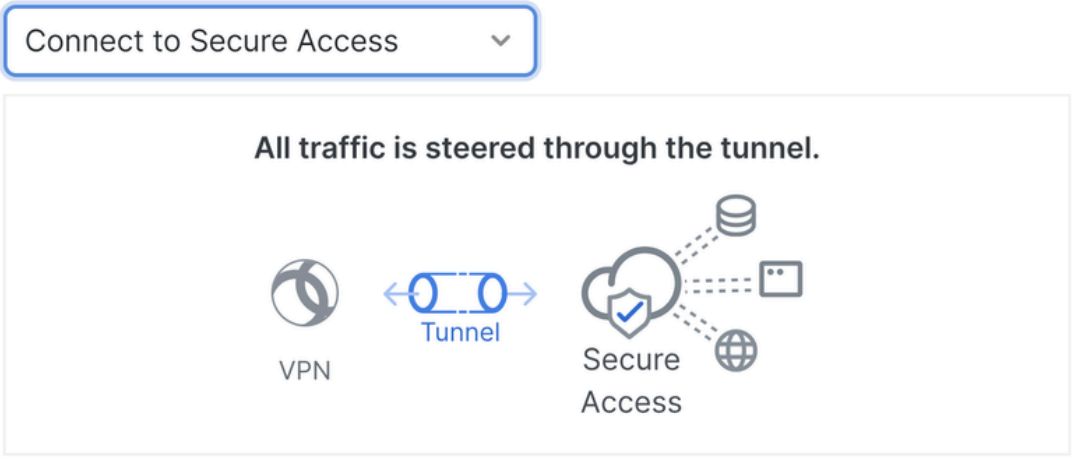
Dirección de tráfico

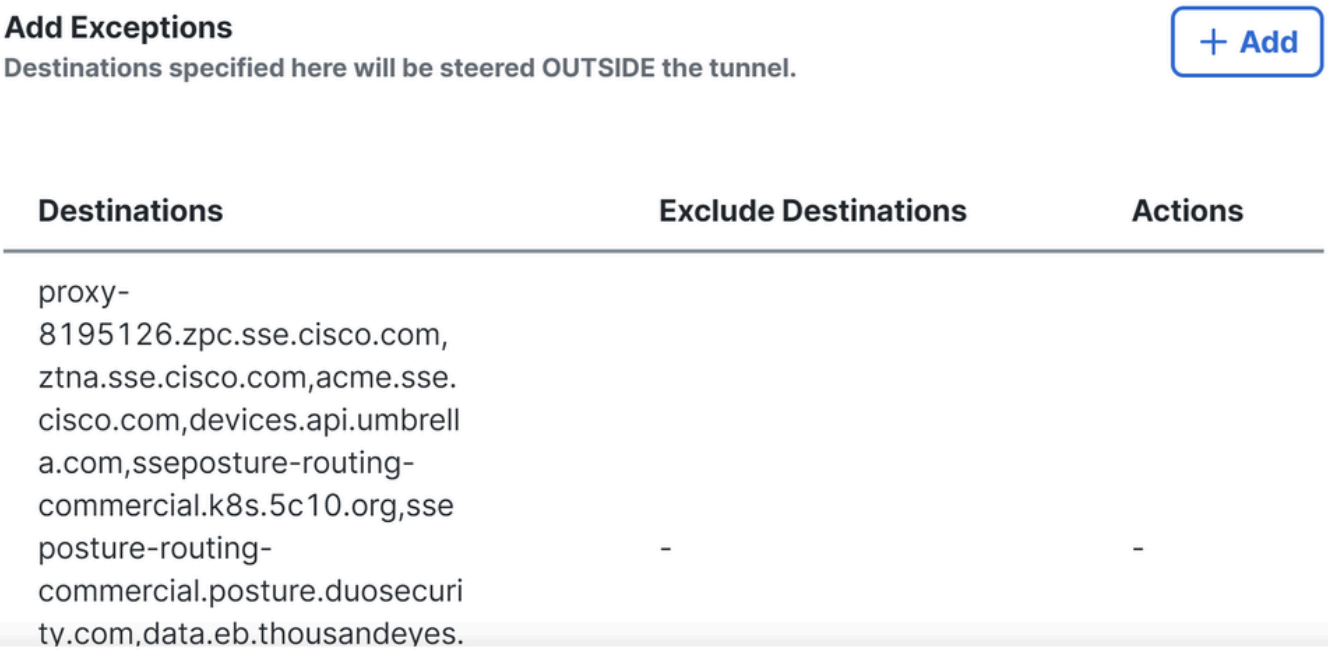
En la sección de dirección del tráfico, debe configurar el tipo de comunicación a través de Secure Access.



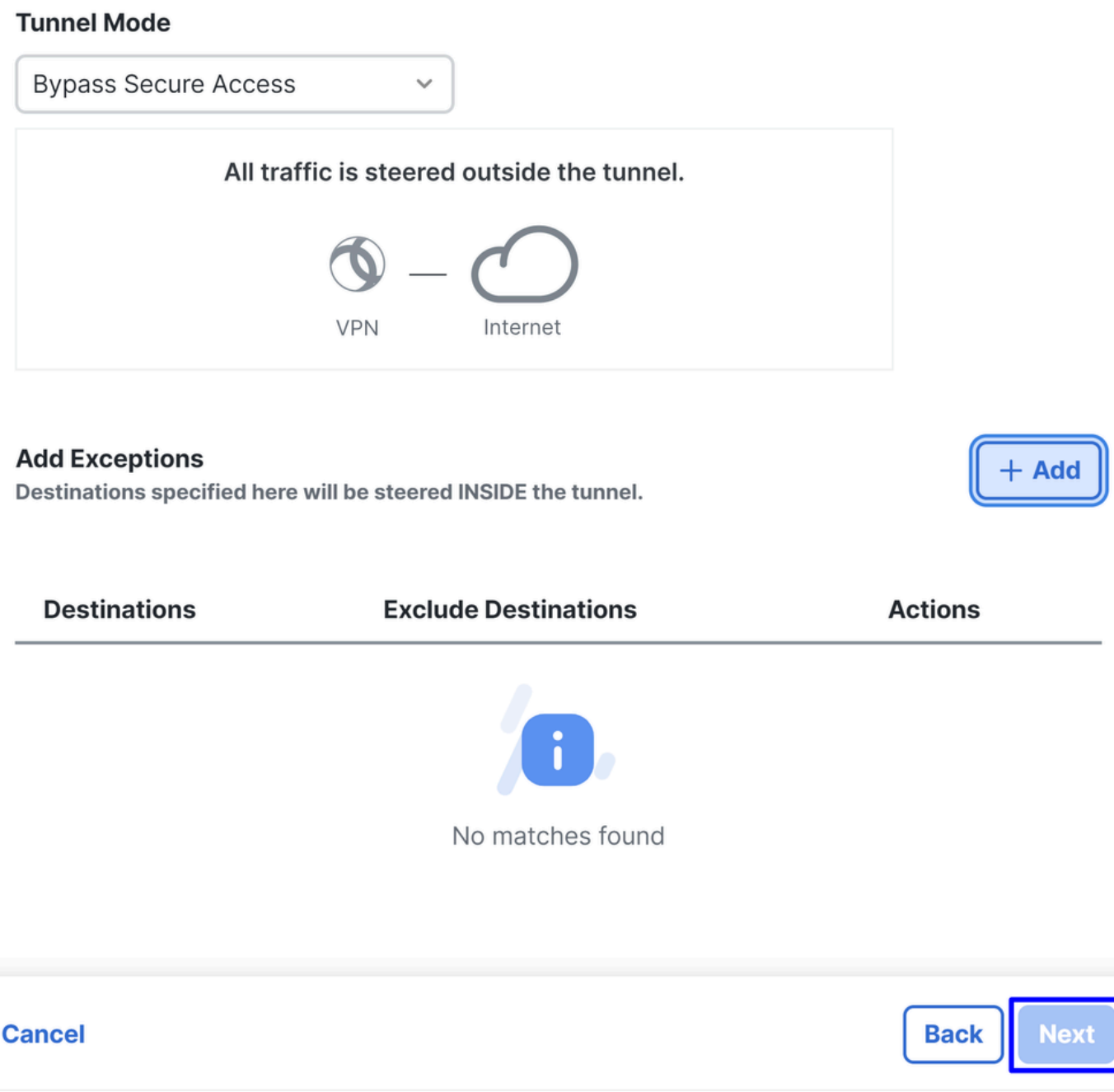

- Si lo desea, **Connect to Secure Access**todo el tráfico de Internet se dirige a través de **Secure Access**

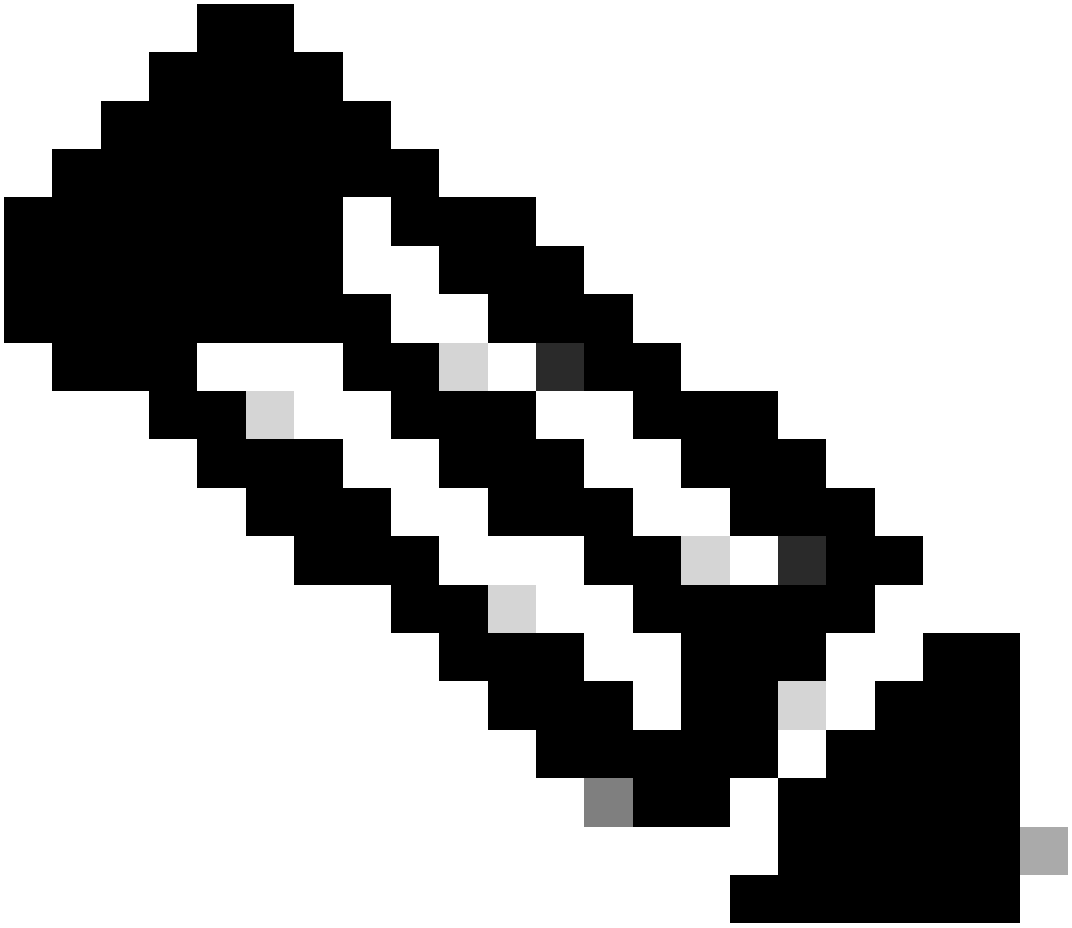



Si desea agregar exclusiones para dominios de Internet o IP, haga clic en el + **Add** botón y, a continuación, haga clic en **Next**.

- Si así lo decide, **Bypass Secure Access**todo el tráfico de Internet pasa a través de su proveedor de Internet, no a travésSecure Access de (Sin protección de Internet)



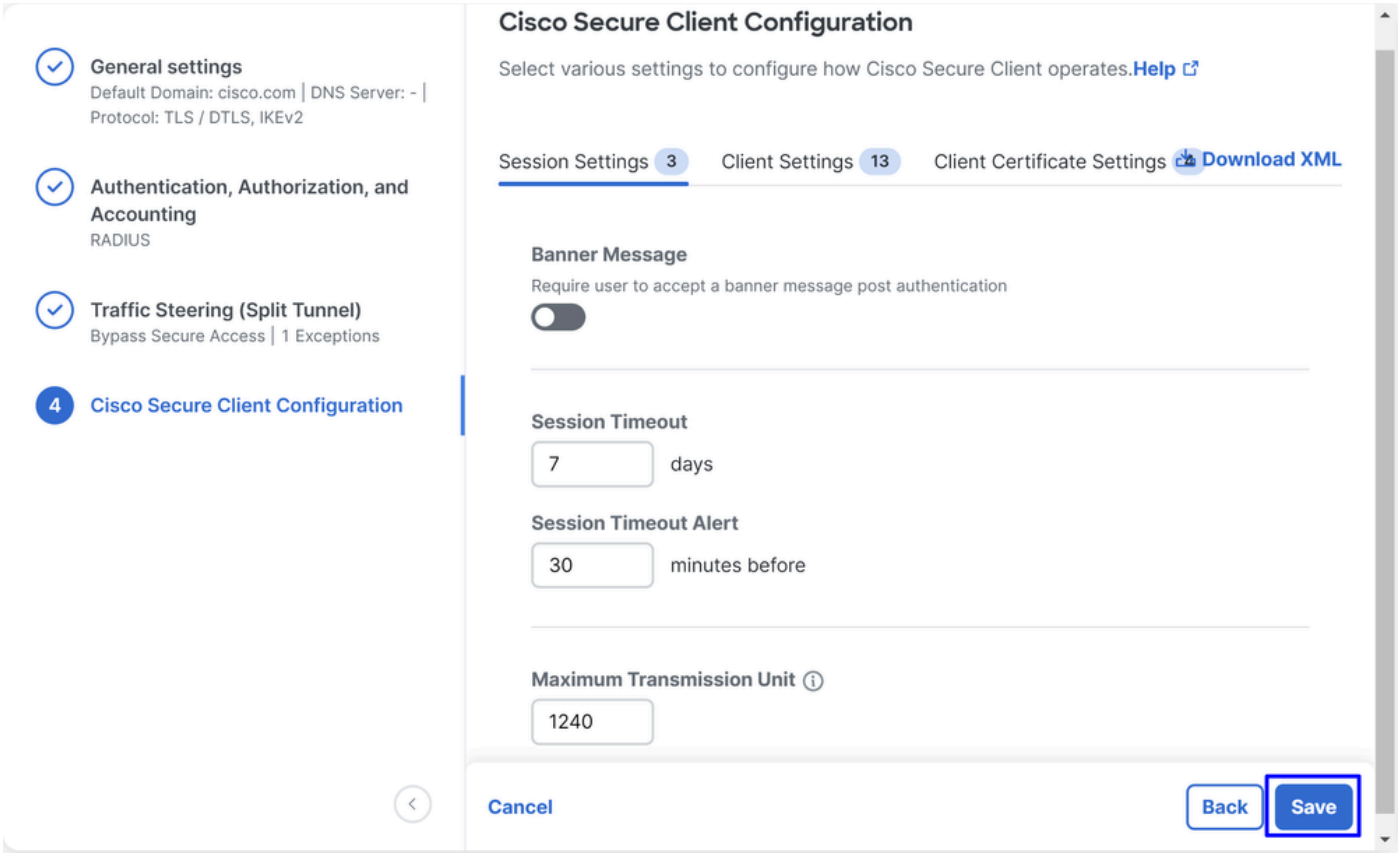


**Nota**: añada el estado **enroll.cisco.com** de ISE cuando lo desee **Bypass Secure Access**.

---

En este paso, seleccione todos los recursos de red privada a los que desea acceder a través de la VPN. Para ello, haga clic en **+ Add**y, a continuación, haga clic **Next** cuando haya agregado todos los recursos.

Configuración de Cisco Secure Client




En este paso, puede mantener todo como predeterminado y hacer clic en **Save**, pero si desea personalizar más su configuración, consulte la Guía de Cisco Secure Client Administrator.

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

Configuraciones de ISE

Configurar lista de dispositivos de red

Para configurar la autenticación a través de Cisco ISE, debe configurar los dispositivos permitidos que pueden realizar consultas a su Cisco ISE:

- Desplácese hasta **Administration > Network Devices**
- Haga clic en **+ 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

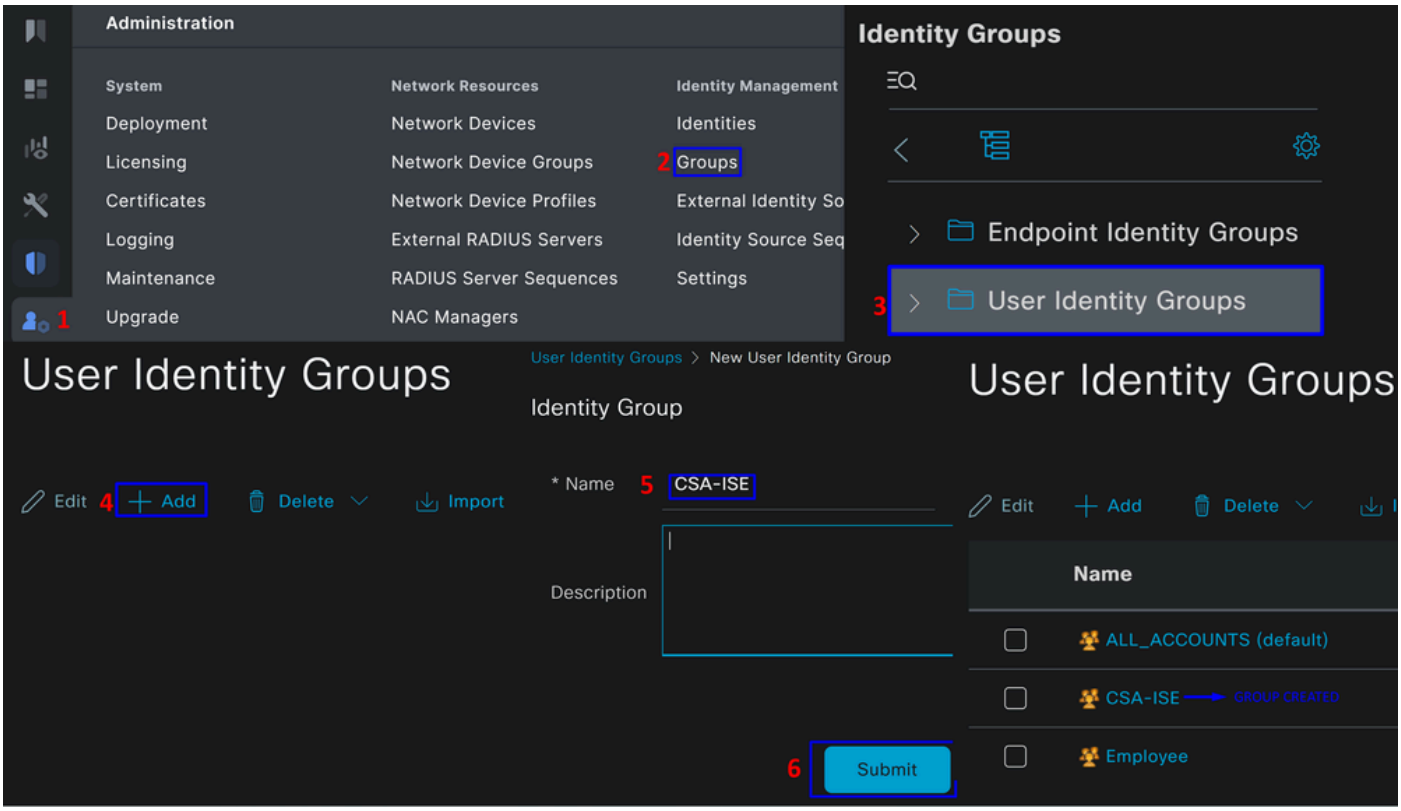
- **Name**: utilice un nombre para identificar el acceso seguro
- **IP  Address**: Configure el Management Interface del paso, IP Pool Region
- **Device Profile**: Elija Cisco
    - **Radius Authentication Settings**
        - Shared Secret: Configure el mismo secreto compartido configurado en el paso Clave secreta
            - **CoA Port**: déjelo como valor predeterminado; 1700 también se utiliza en Secure Access

Después de hacer clic en **Save**, para comprobar si la integración funciona correctamente, vaya a crear un usuario local para la verificación de la integración.

Configurar un grupo

Para configurar un grupo para utilizarlo con usuarios locales, siga estos pasos:

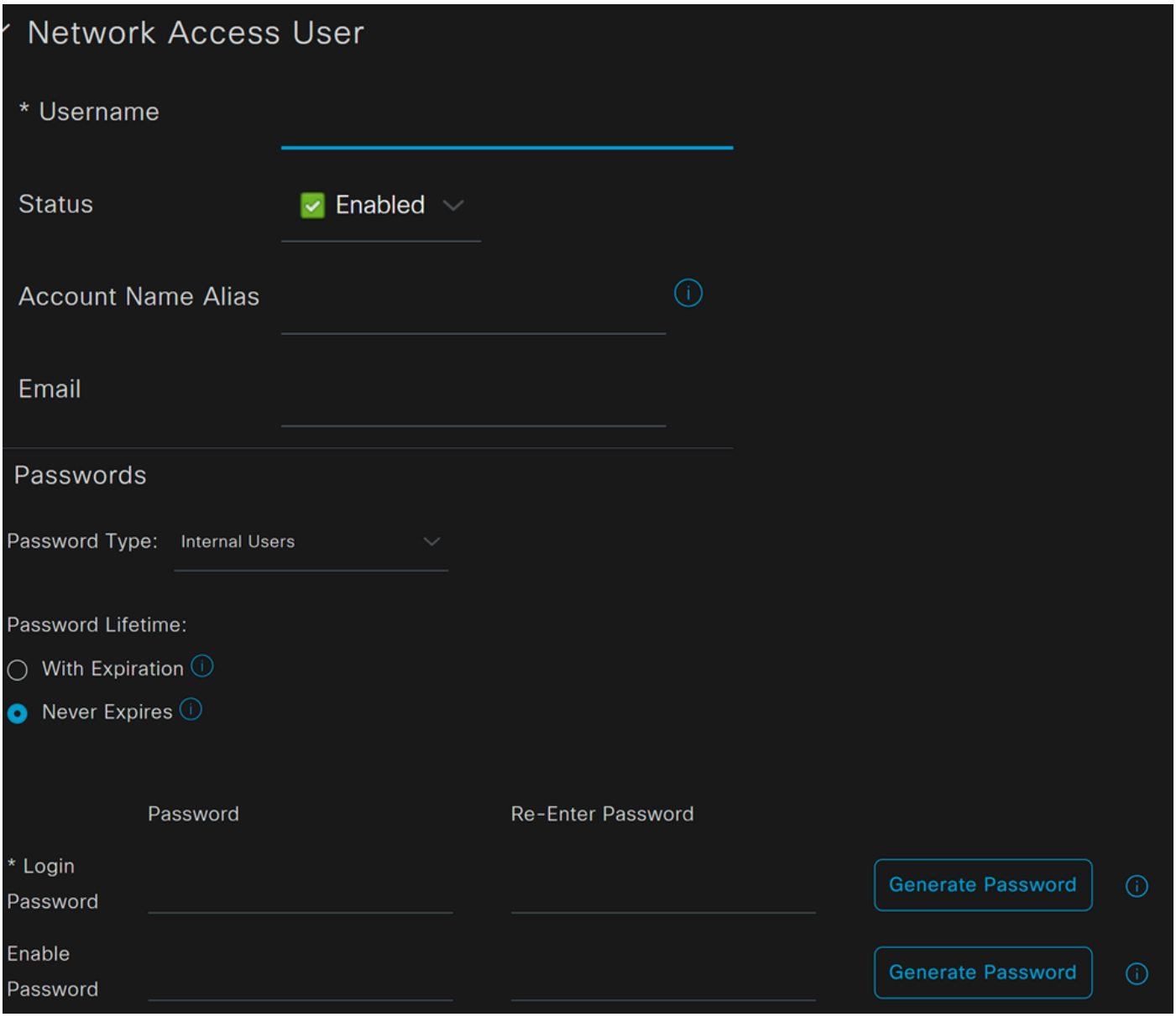
- Haga clic en **Administration > Groups**
- Haga clic en **User Identity Groups**
- Haga clic en + Add
- Cree un Namepara el grupo y haga clic en **Submit**

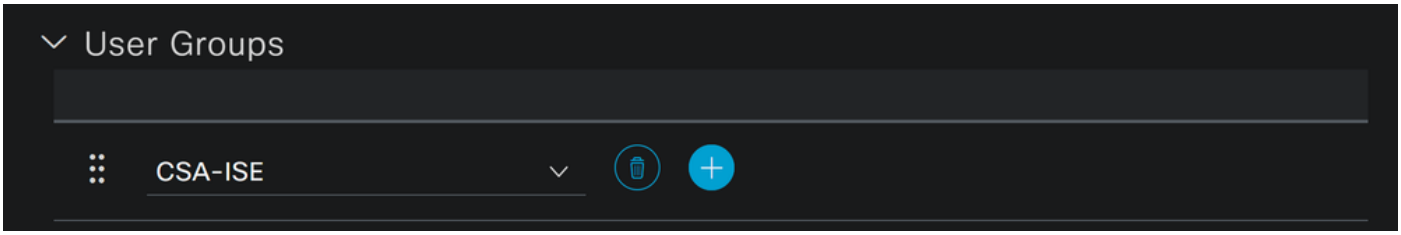



Configurar usuario local

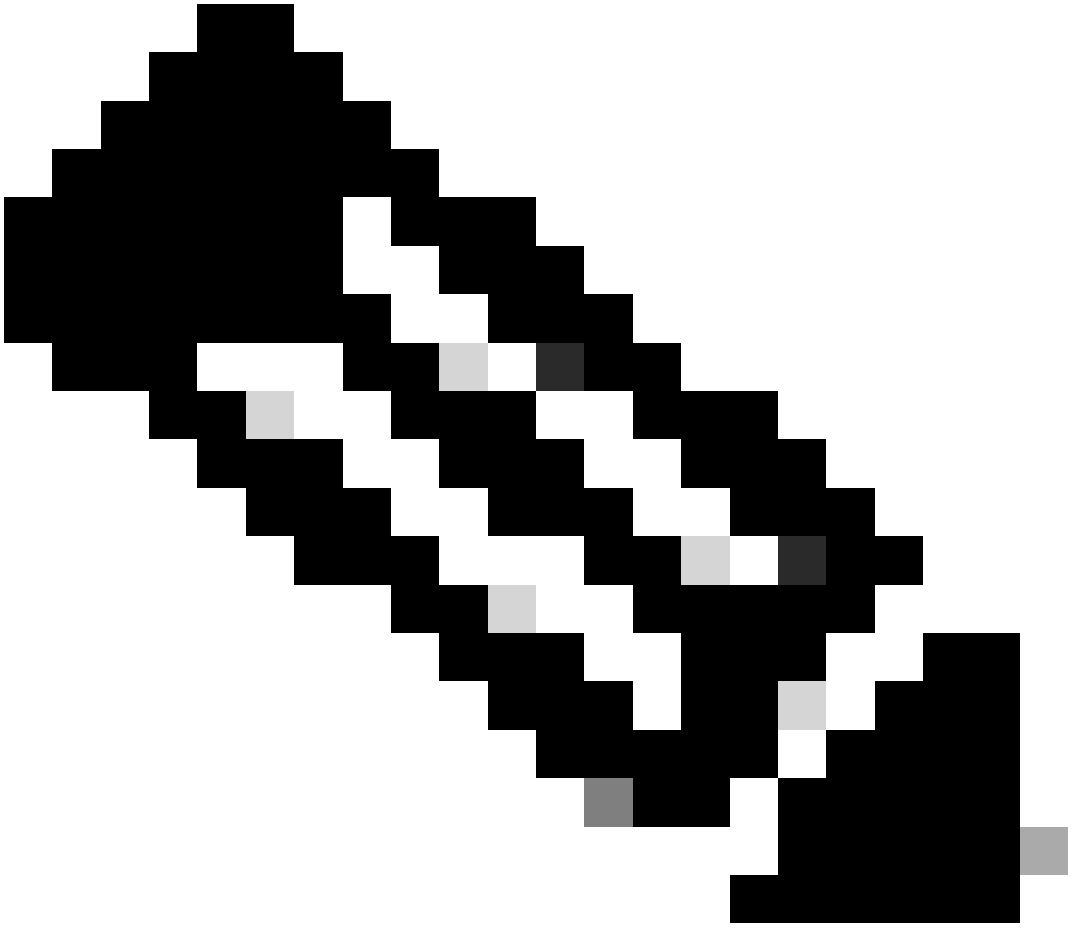
Para configurar un usuario local para verificar su integración:

- Desplácese hasta **Administration > Identities**
- Haga clic en **Add +**




- **Username**: Configure el nombre de usuario con un aprovisionamiento UPN conocido en Secure Access; esto se basa en el paso Prerrequisitos
- **Status**:Activo
- **Password Lifetime**: Puede configurarlo **With Expiration** o, Never Expiresen función de usted
- **Login Password**: cree una contraseña para el usuario
- **User Groups**: Seleccione el grupo creado en el paso Configurar un grupo



**Nota**: La autenticación basada en UPN está configurada para cambiar en las próximas versiones de Secure Access.

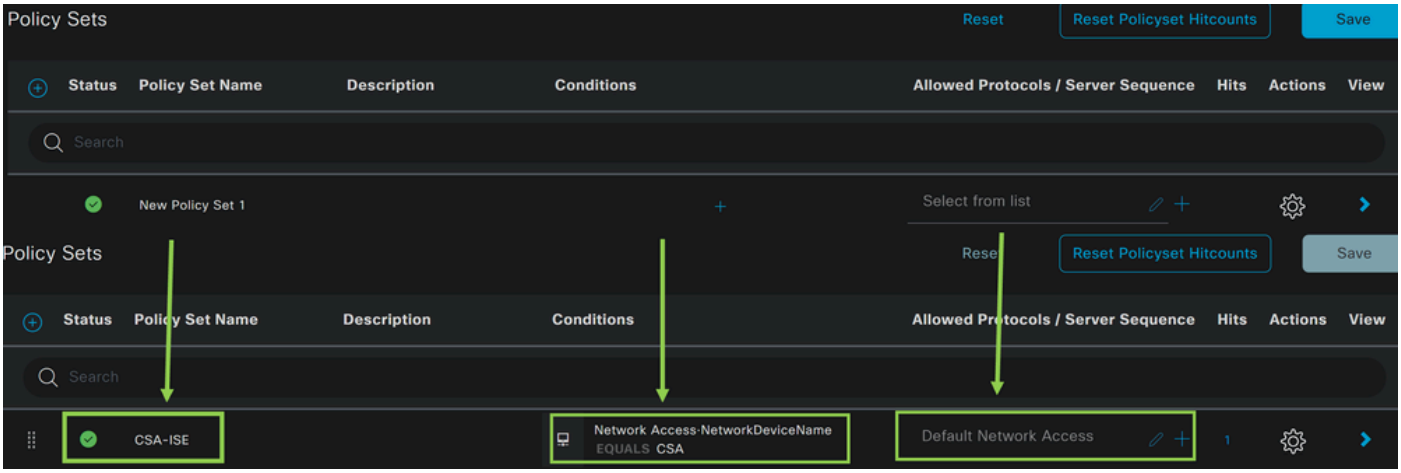
Después de esto, puede **Save** modificar la configuración y continuar con el paso **Configure Policy Set**.

Configurar conjunto de políticas

En el conjunto de políticas, configure la acción que ISE lleva a cabo durante la autenticación y la autorización. Este escenario muestra el caso práctico de configurar una política simple para proporcionar acceso de usuario. En primer lugar, ISE verifica el origen de las autenticaciones RADIUS y comprueba si las identidades existen en la base de datos de usuarios de ISE para proporcionar acceso

Para configurar esa política, navegue hasta el panel de Cisco ISE:

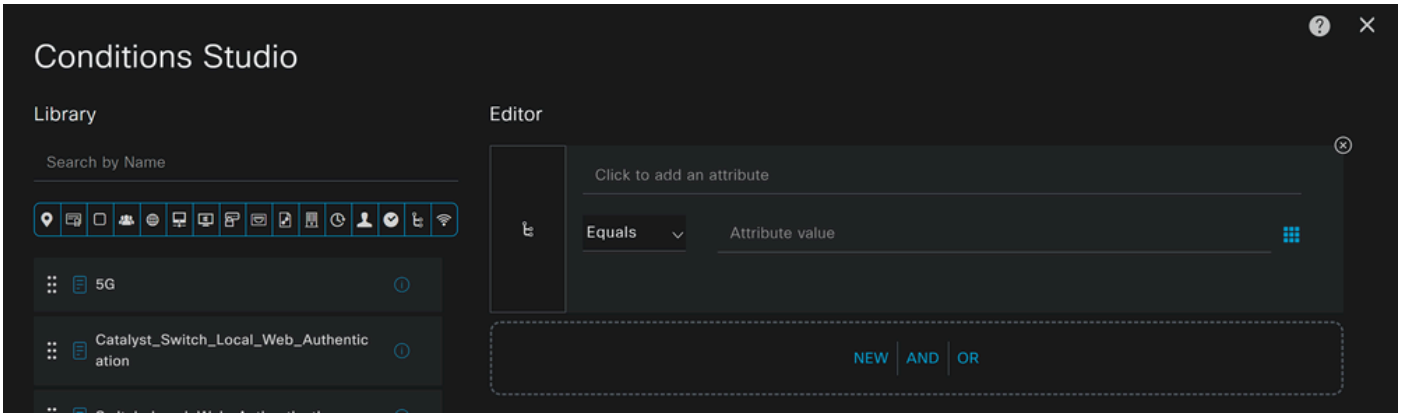
- Haga clic en Policy > Policy Sets
- Haga clic en + para agregar un nuevo conjunto de políticas




En este caso, cree un nuevo conjunto de directivas en lugar de trabajar con el predeterminado. A continuación, configure la Autenticación y la Autorización basadas en ese conjunto de políticas. La política configurada permite el acceso al dispositivo de red definido en el paso Configure Network Devices List para verificar que estas autenticaciones provienen CSA Network Device List y luego ingresan a la política como **Conditions**. Y finalmente, los Protocolos permitidos, como **Default Network Access**.

Para crear el **condition** que coincida con el conjunto de directivas, continúe con las siguientes instrucciones:

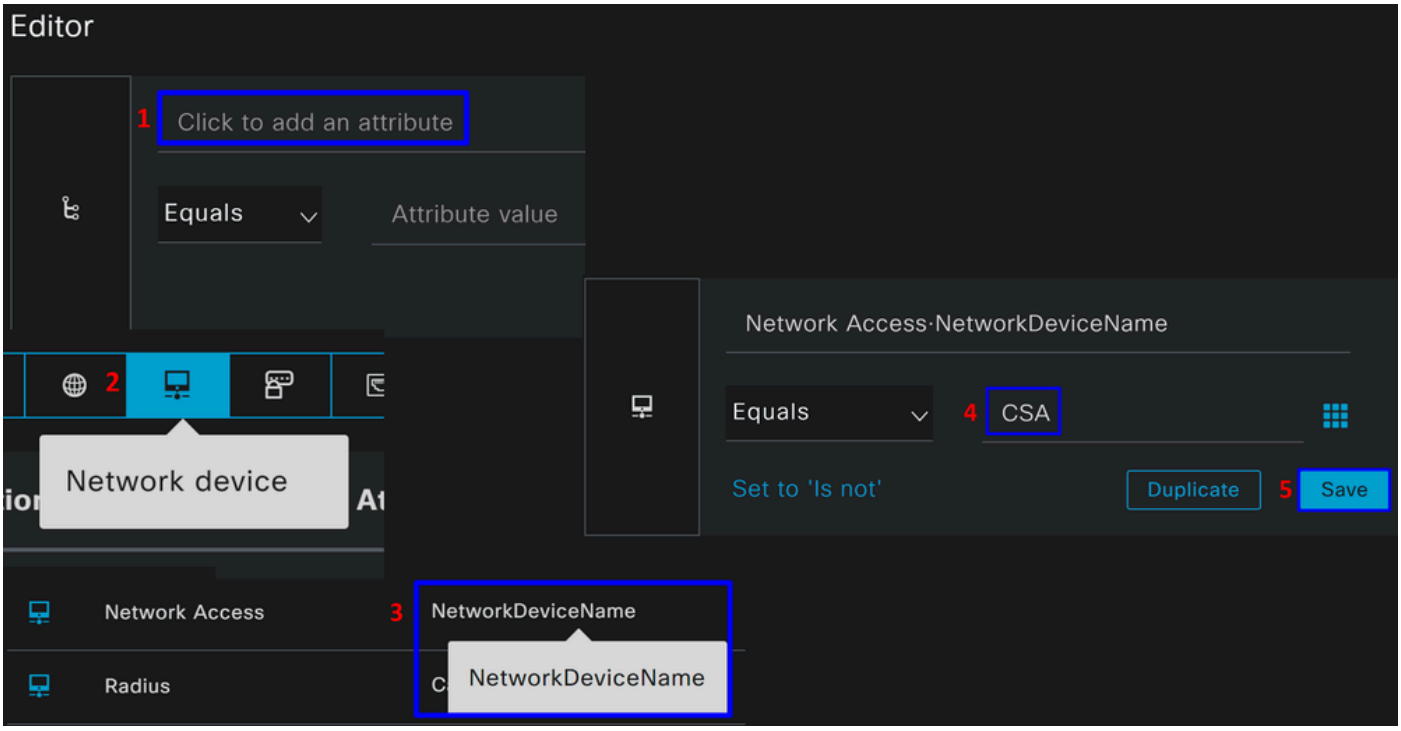
- Haga clic en +
- En **Condition Studio**, la información disponible incluye:




- Para crear las condiciones, haga clic en Click to add an attribute
- Haga clic en el **Network Device** botón
- En las opciones siguientes, haga clic en **Network Access - Network Device Name** opción
- En la opción Equals (Igual que), escriba el nombre del **Network Device** en el paso Configure Network Devices List (Configurar

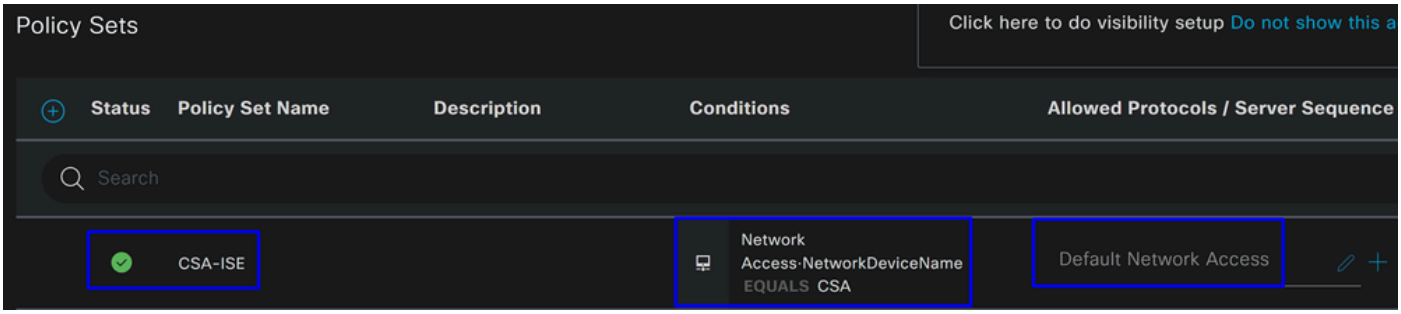
lista de dispositivos de red)

- Haga clic en **Save**




Esta política solo aprueba la solicitud del origen CSApara continuar con la configuración **Authentication** y **Authorization** configuración bajo el conjunto de políticas **CSA-ISE**, y también verifica los protocolos permitidos en función de la **Default Network Access** para los protocolos permitidos.

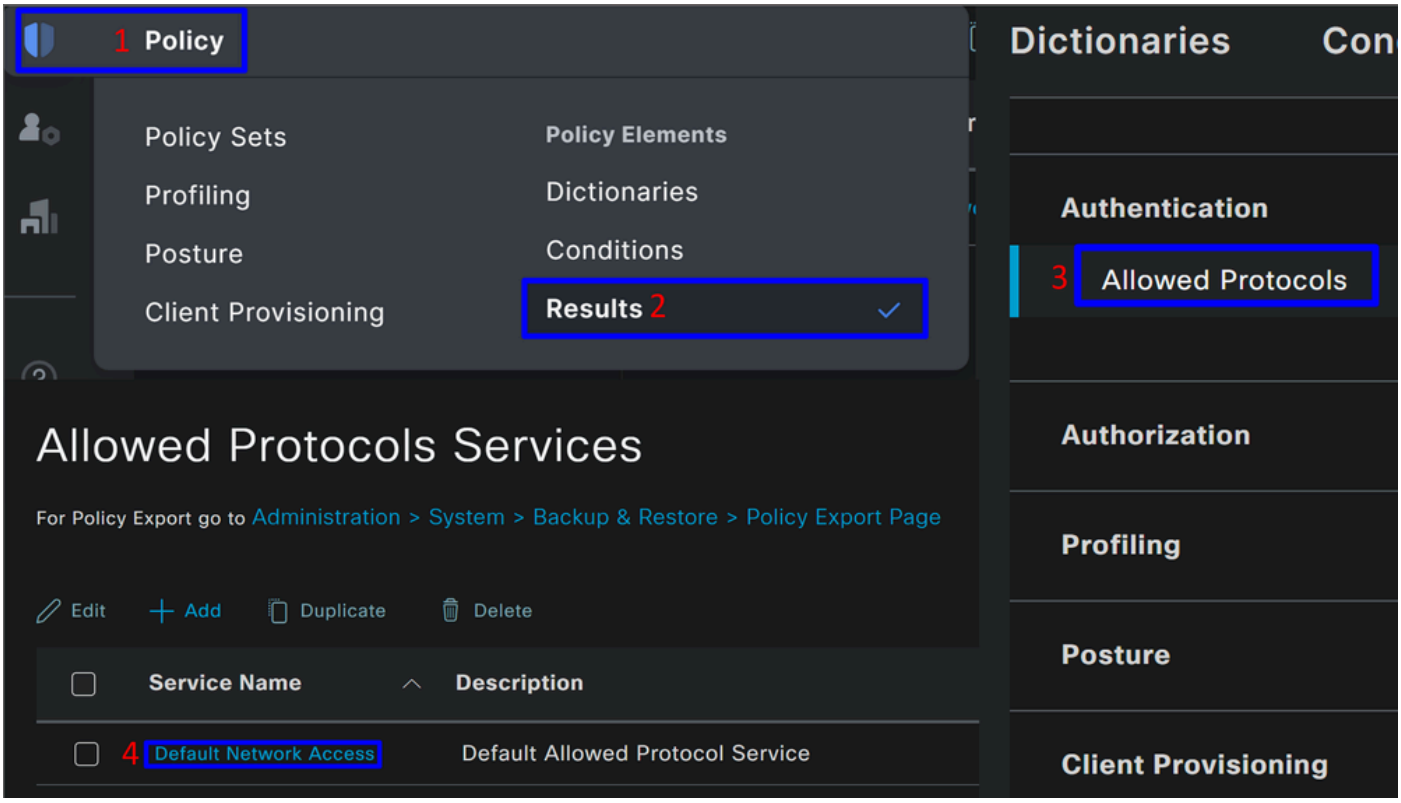
El resultado de la política definida debe ser:




- Para verificar los **Default Network Access Protocols** permisos, siga con las siguientes instrucciones:

  - Haga clic enPolicy > Results

    - Haga clic en **Allowed Protocols**
    - Haga clic en **Default Network Access**

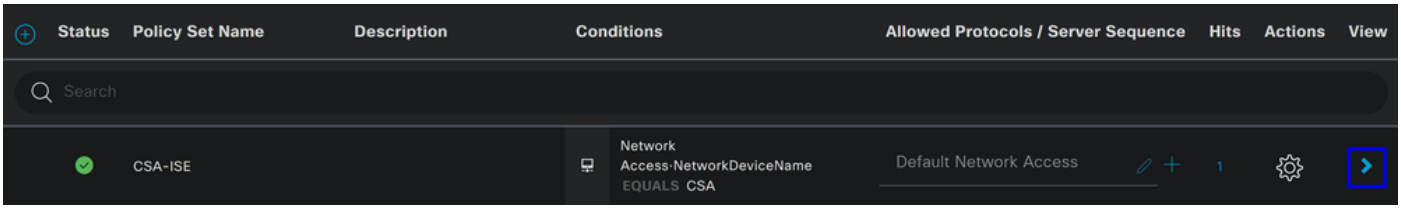



- A continuación, verá todos los protocolos permitidos en **Default Network Access**

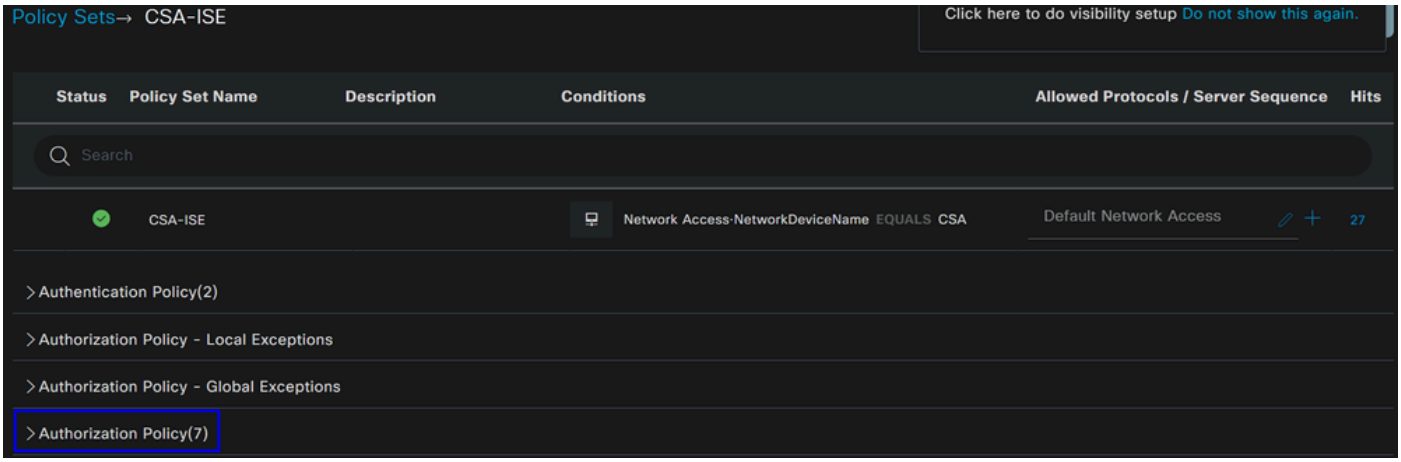
Configurar autorización de conjunto de políticas

Para crear la **Authorization** directiva en el **Policy Set**, siga con los pasos siguientes:

- Haga clic en >



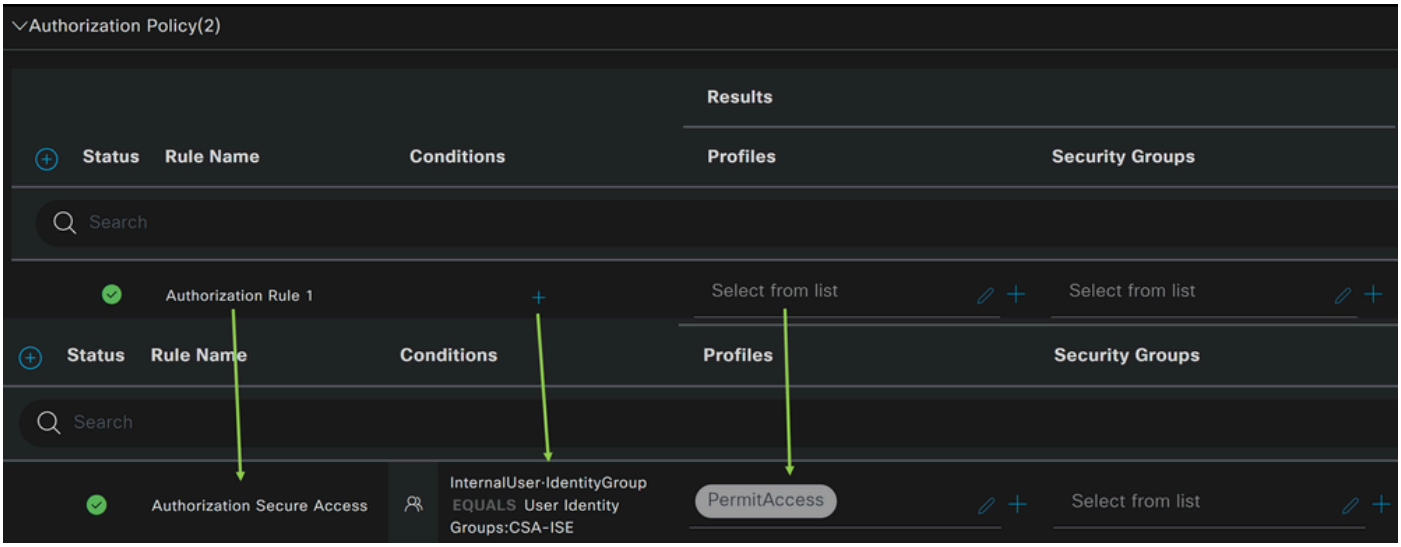

- Después de esto, verá **Authorization** laspolíticas mostradas:



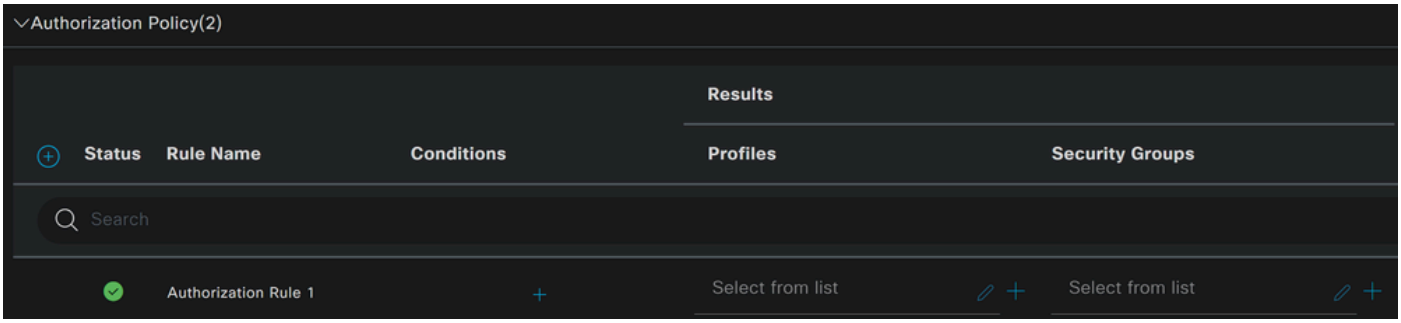

La política es la misma definida en el paso Configure Policy Set.

**Política de autorización**

Puede configurar la directiva de autorización de varias maneras. En este caso, autorice sólo a los usuarios del grupo definido en el paso Configurar un grupo.Vea el siguiente ejemplo para configurar su política de autorización:

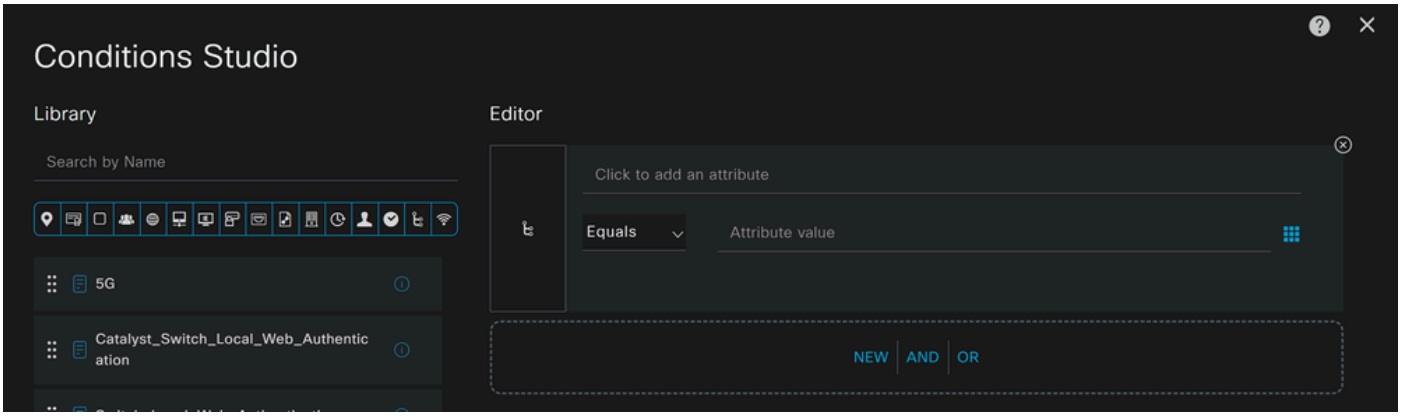



- Haga clic en **Authorization Policy**
- Haga clic en + para definir la política de autorización de la siguiente manera:

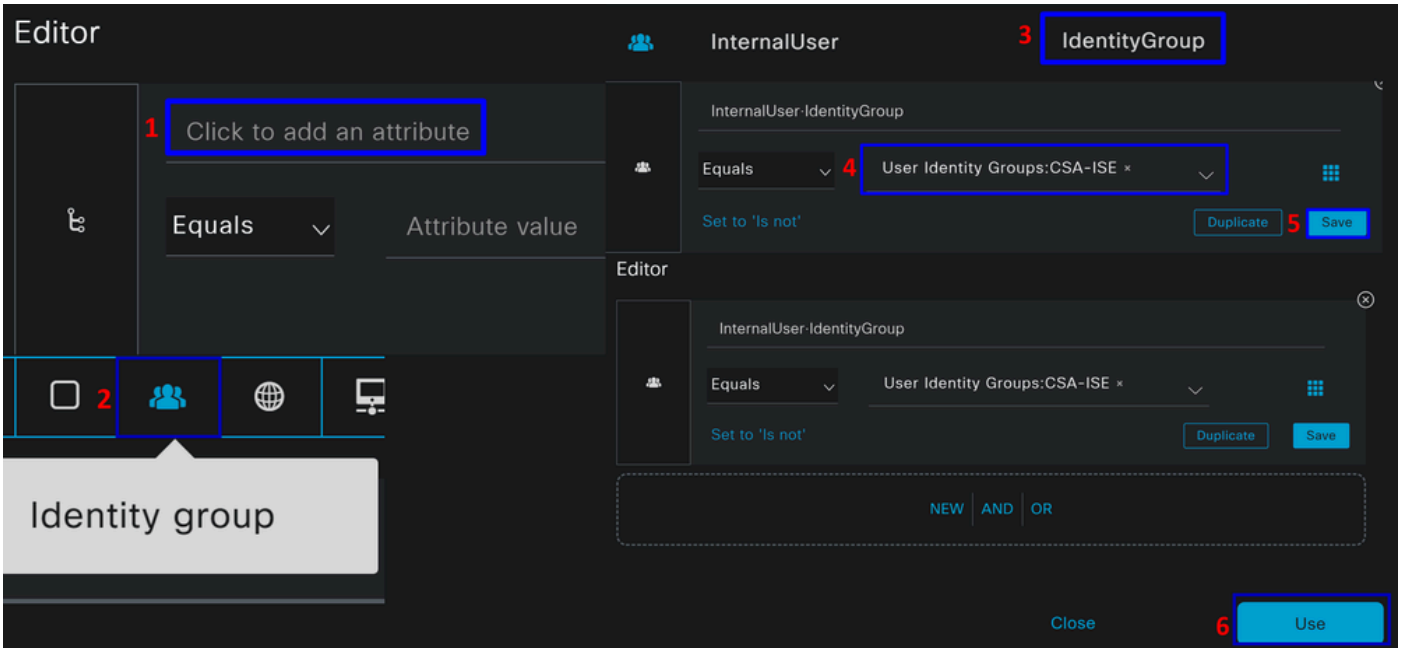


- Para el siguiente paso, cambie el Rule Name, Conditionsy Profiles

- Al establecer la **Name** configuración de un nombre para identificar fácilmente la directiva de autorización
- Para configurar el **Condition**, haga clic en el botón +
- En **Condition Studio**, encontrará la información siguiente:

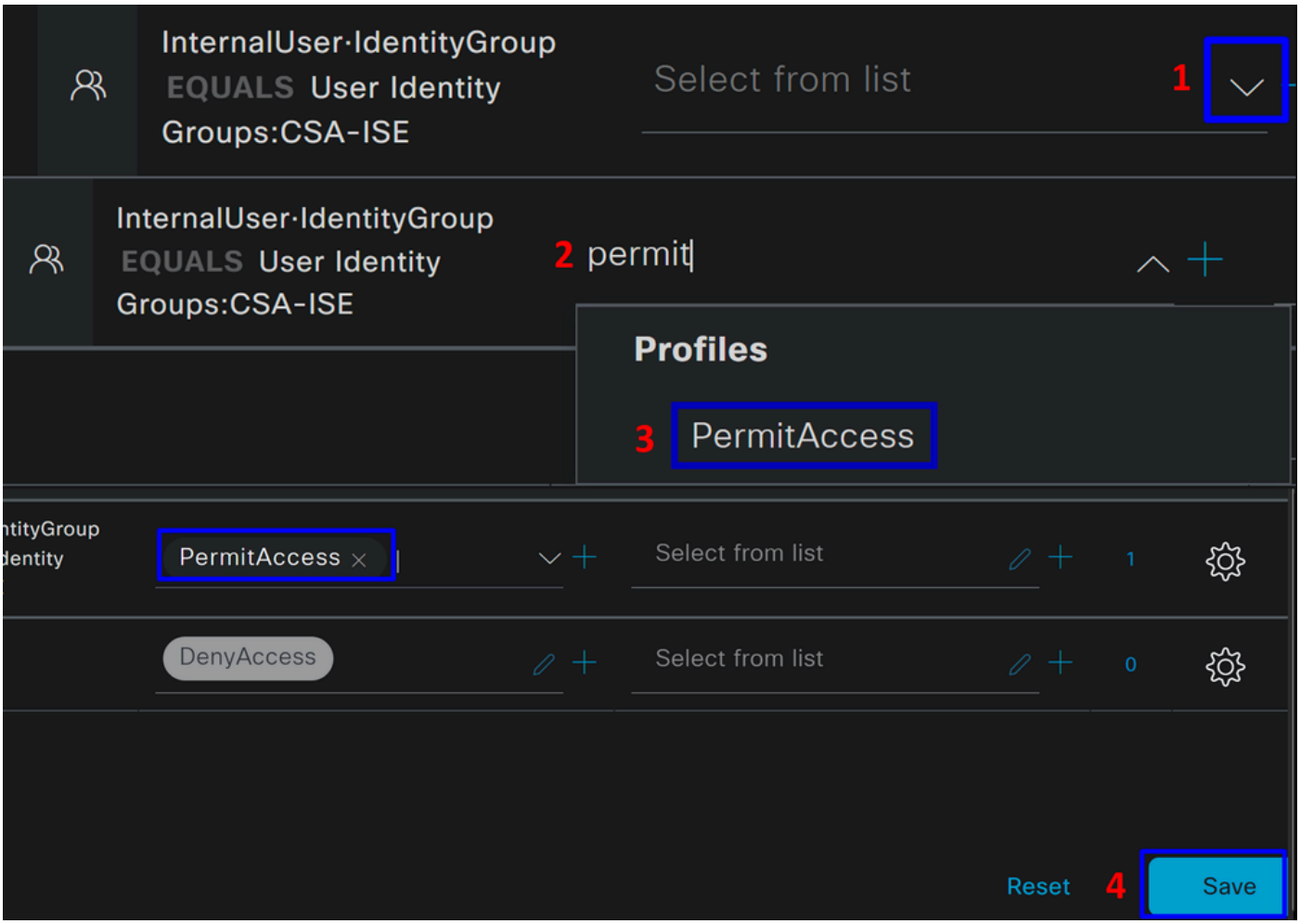



- Para crear las condiciones, haga clic en Click to add an attribute
- Haga clic en el **Identity Group** botón
- En las opciones siguientes, haga clic en **Internal User - IdentityGroup** option
- En la **Equals** opción, utilice el menú desplegable para buscar el **Group** aprobado para la autenticación en el paso [Configurar un grupo]
- Haga clic en **Save**
- Haga clic en **Use**



Después de esto, debe definir el **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- En la **Authorization Policy**, haga clic en el botón desplegable de **Profiles**
- Buscar por permiso
- Seleccionar **PermitAccess**
- Haga clic en Save

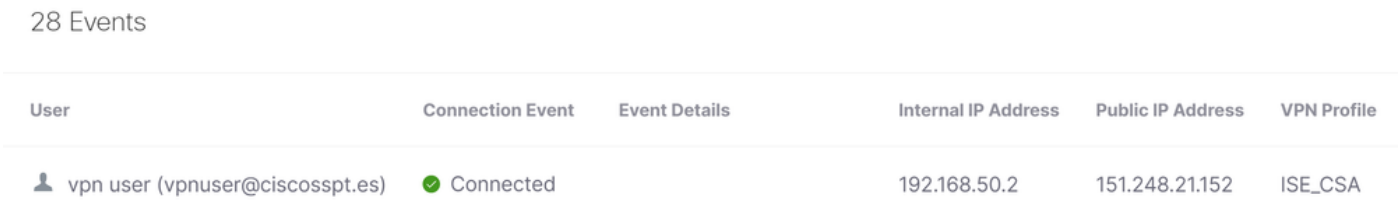



Después de eso, ha definido su **Authorization** política. Autentique para verificar si el usuario se conecta sin problemas y si puede ver los registros en Secure Access e ISE.

Para conectarse a la VPN, puede utilizar el perfil creado en Secure Access y conectarse a través de Secure Client con el perfil de ISE.

- **¿Cómo se muestra el registro en Secure Access cuando se aprueba la autenticación?**
  - Vaya al panel de acceso seguro

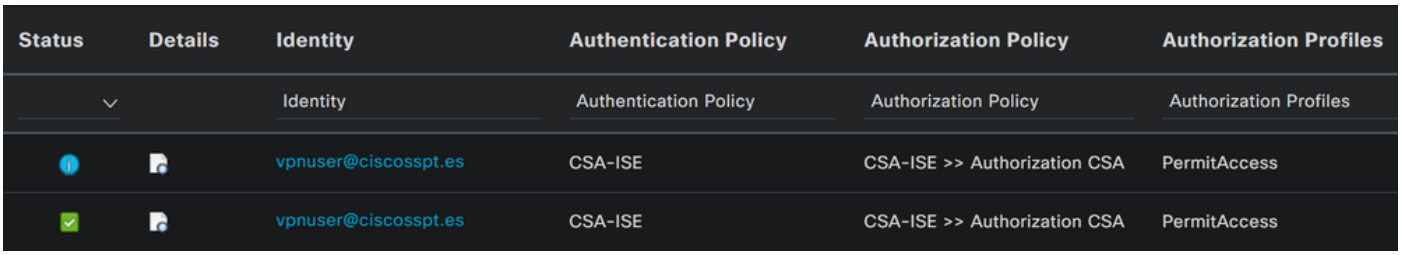
- Haga clic en **Monitor > Remote Access Log**




- **¿Cómo se muestra el registro en ISE cuando se aprueba la autenticación?**

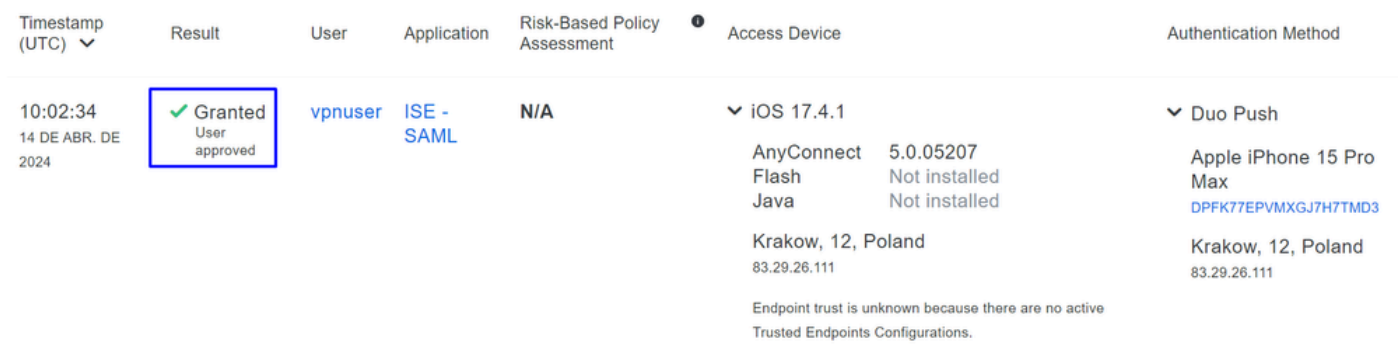
  - Desplácese hasta el **Cisco ISE Dashboard**

    - Haga clic en **Operations > Live Logs**




**¿Cómo se muestra el registro en Duo cuando se aprueba la autenticación?**

- Vaya al panel Duo Admin
- Haga clic en **Reports > Authentication Log**



Configuración de usuarios de Radius Local o Active Directory

Configuración del estado de ISE

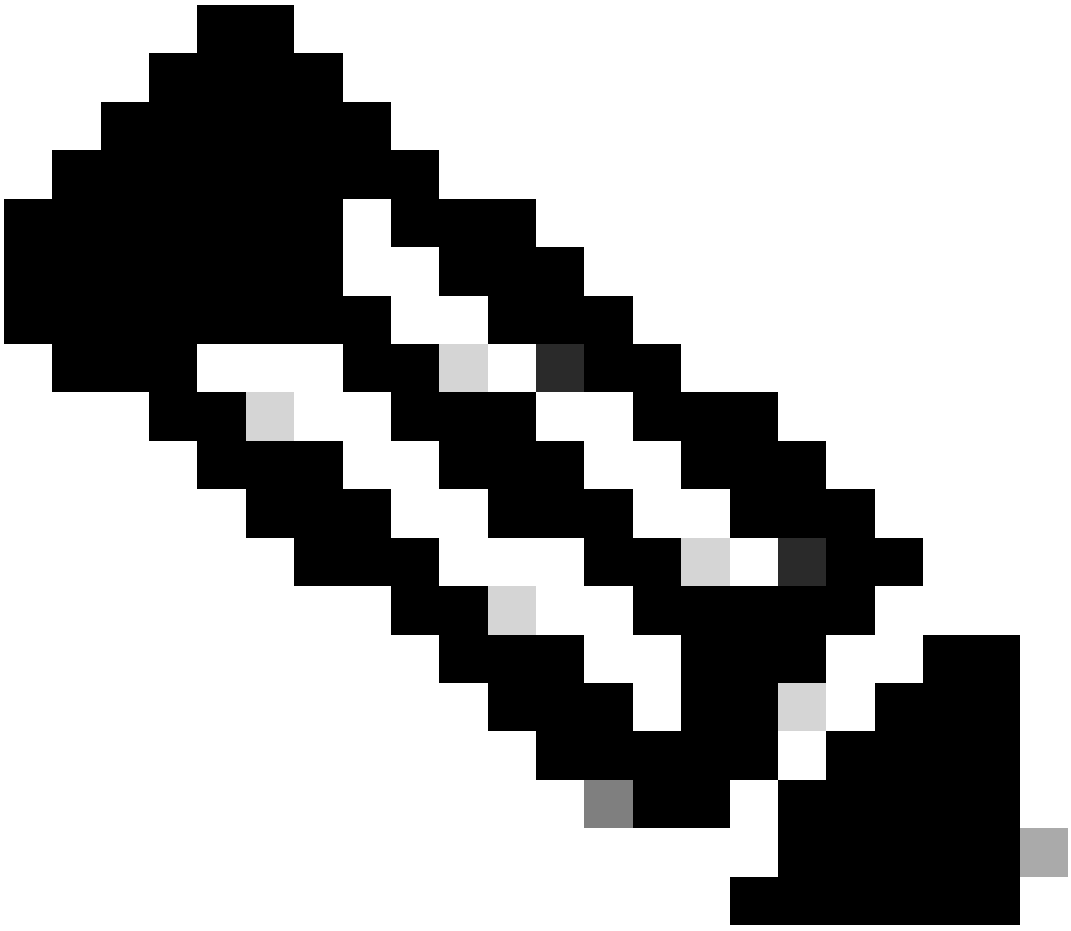
En esta situación, cree la configuración para verificar el cumplimiento de los terminales antes de conceder o denegar el acceso a los recursos internos.

Para configurarlo, continúe con los siguientes pasos:

Configurar condiciones de estado

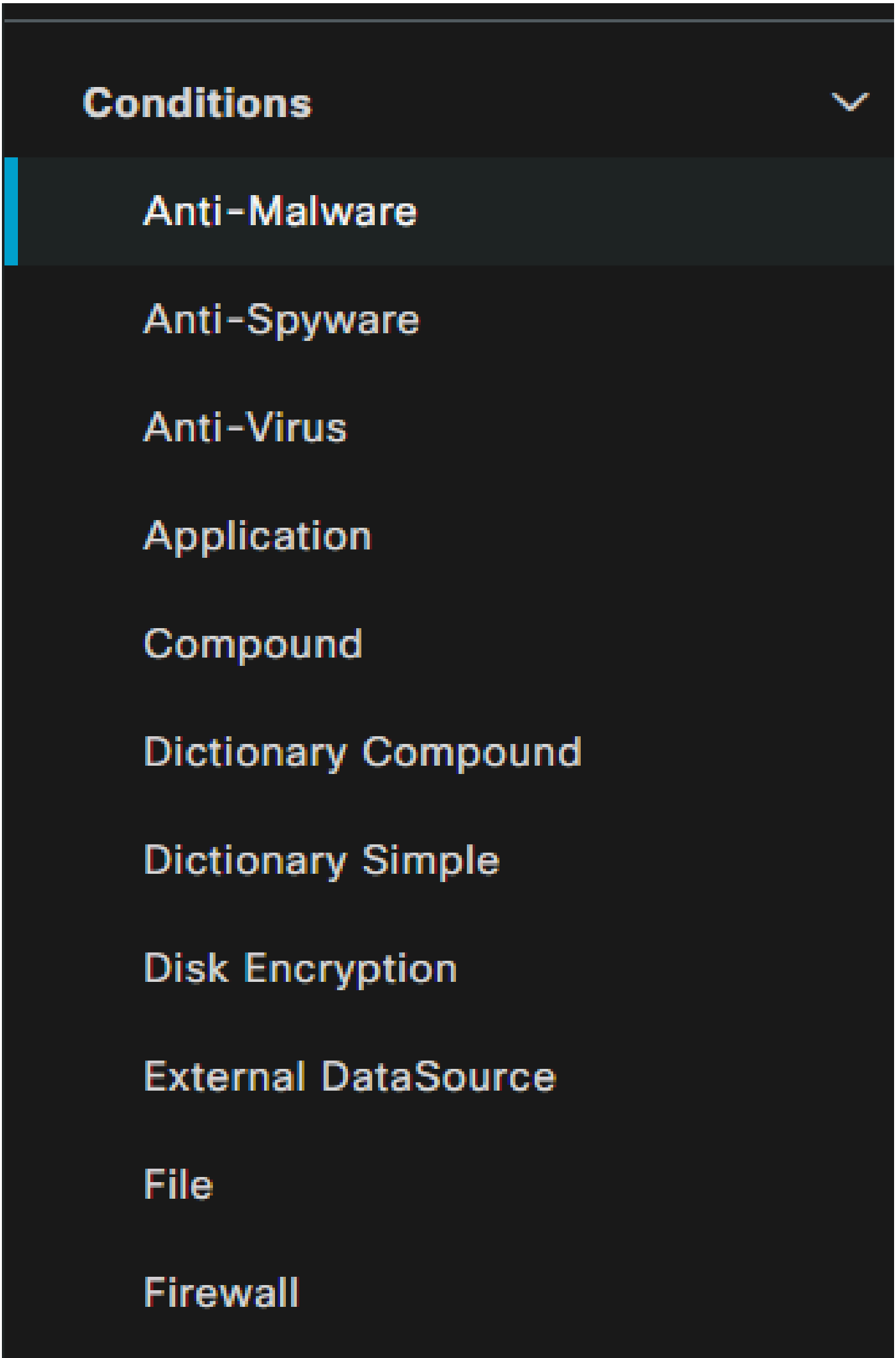
- Vaya a su panel de ISE
- Haga clic en **Work Center > Policy Elements > Conditions**
- Haga clic en **Anti-Malware**

---

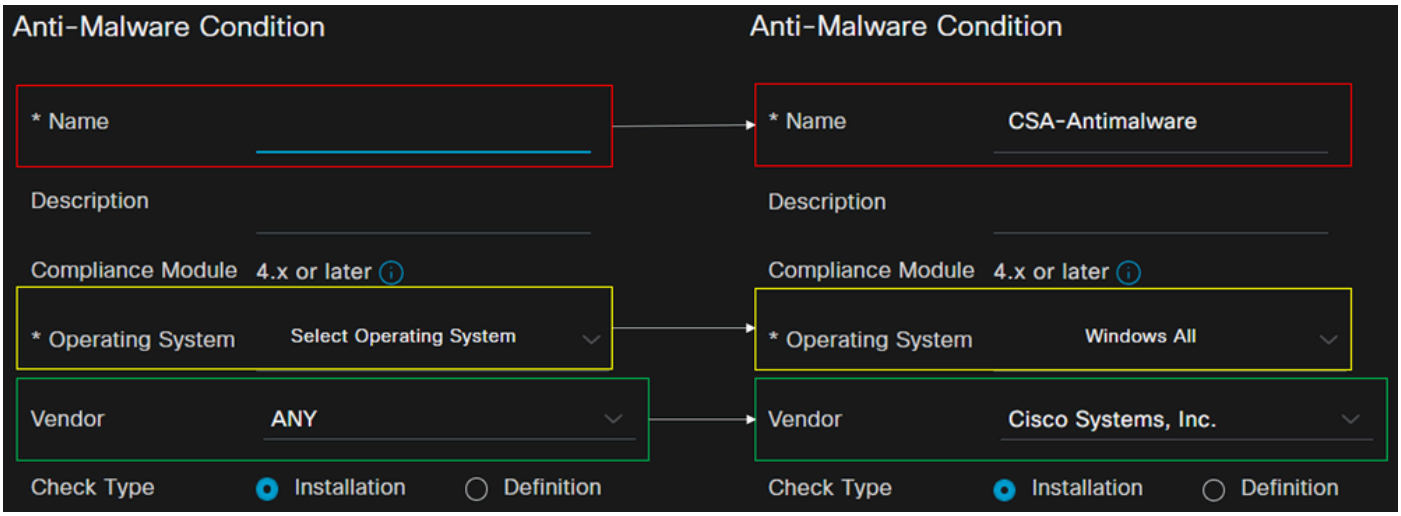


---

**Nota**: En ella encontrará muchas opciones para verificar el estado de sus dispositivos y realizar la evaluación correcta en función de sus políticas internas.

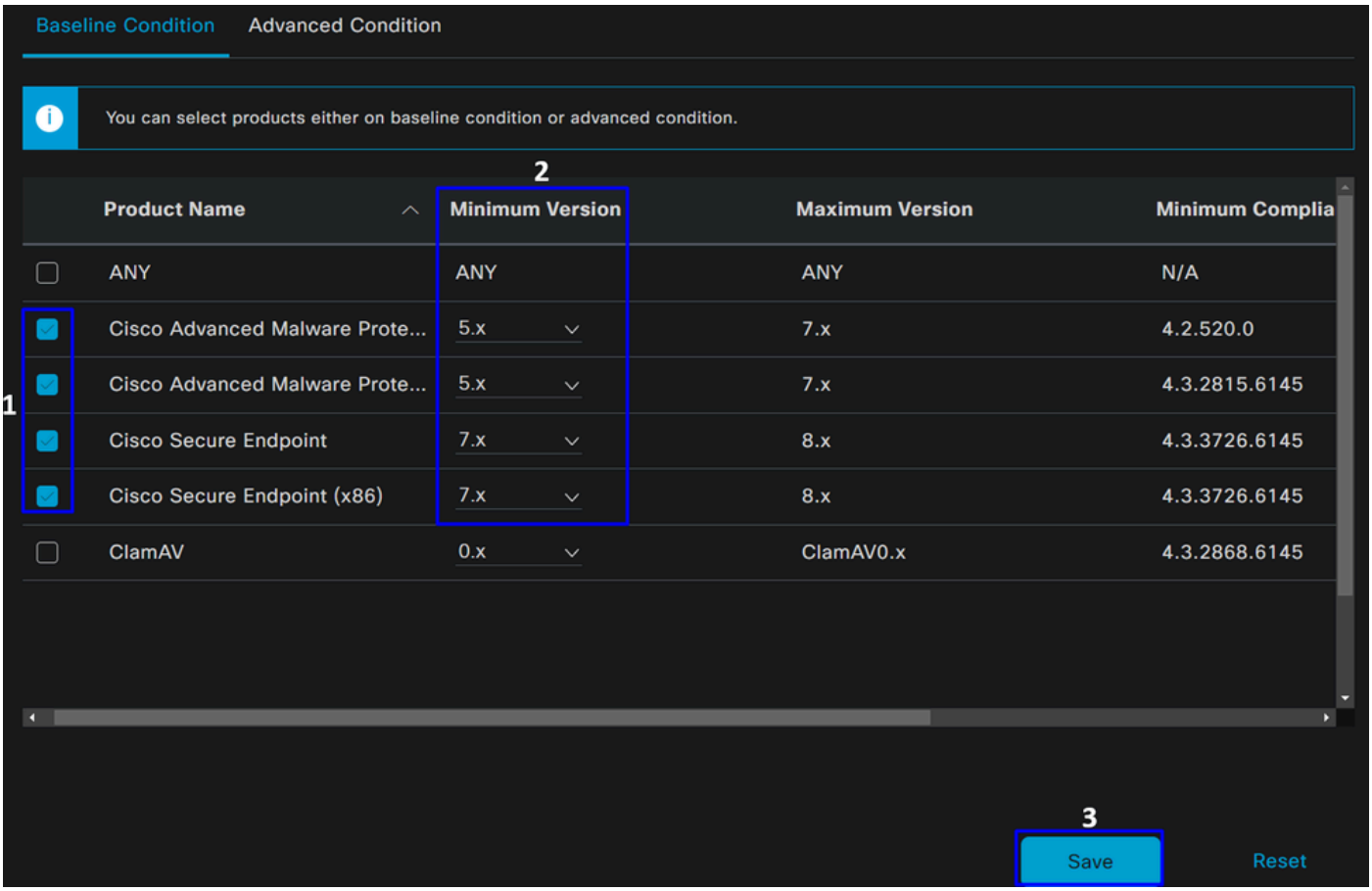

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

Anti-Malware Condition para detectar la instalación del antivirus en el sistema; también puede elegir la versión del sistema operativo si es necesario.




- **Name**: utilice un nombre para reconocer la condición anti-malware
- **Operating System**: Elija el sistema operativo que desea poner bajo la condición
- **Vendor**: elija un proveedor o ANY
- **Check Type**: puede comprobar si el agente está instalado o la versión de definición de esa opción.

- Por ejemplo, **Products for Selected Vendor**, puede configurar lo que desea verificar sobre el antimalware en el dispositivo.

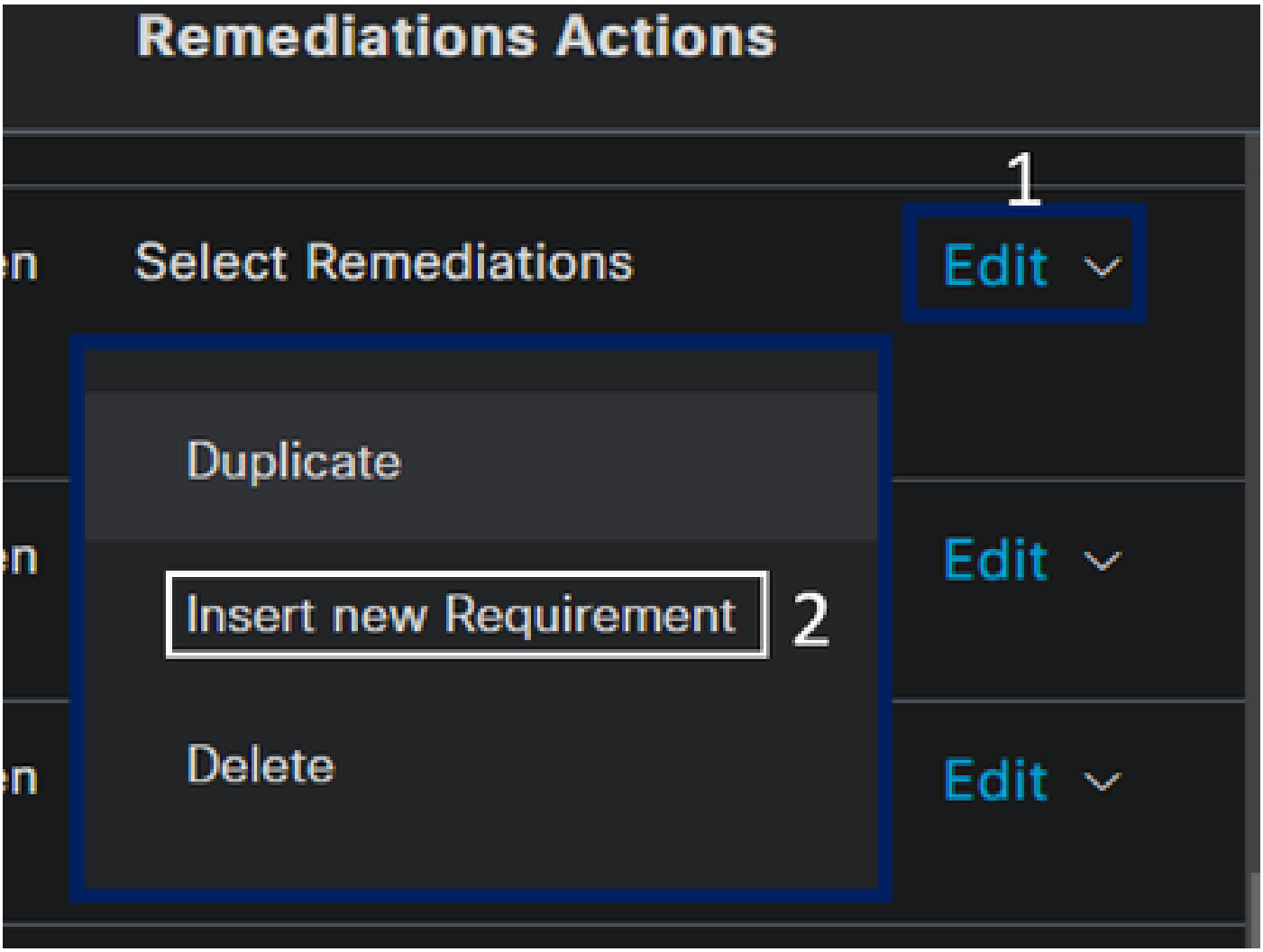



- Marque la casilla de verificación de las condiciones que desea evaluar
- Configurar la versión mínima para verificar
- Haga clic en Guardar para continuar con el paso siguiente

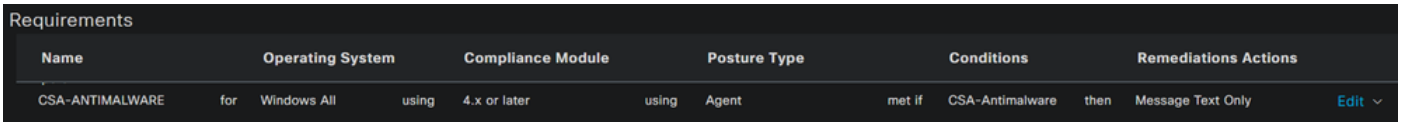
Una vez configurado, puede continuar con el paso **Configure Posture Requirements**.

Configurar requisitos de estado

- Vaya a su panel de ISE
- Haga clic en **Work Center > Policy Elements > Requeriments**
- Haga clic en uno **Edit** de los requisitos y haga clic en **Insert new Requirement**




- En el nuevo requisito, configure los siguientes parámetros:

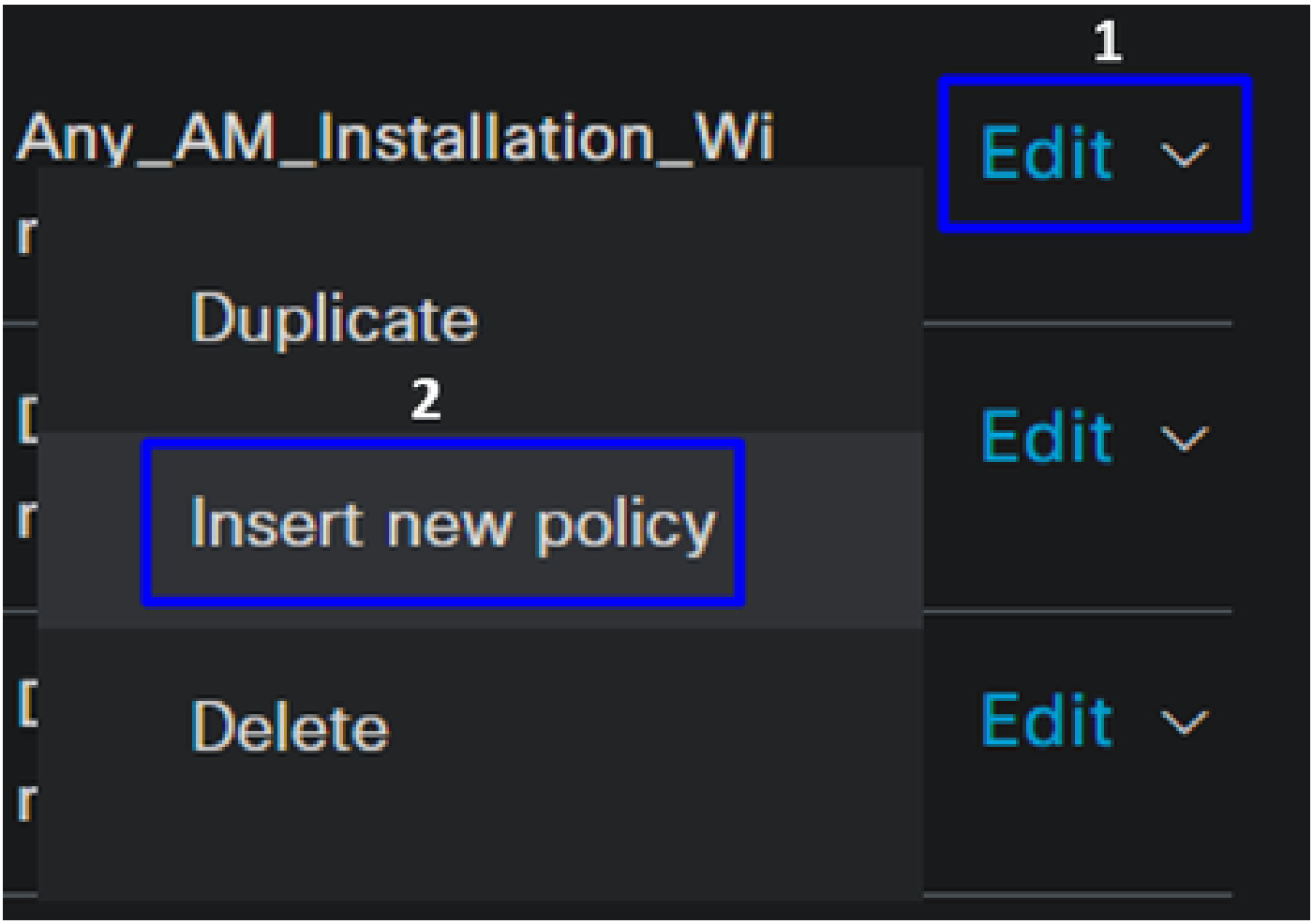



- **Name**: configure un nombre para reconocer el requisito antimalware
- **Operating System**: Seleccione el sistema operativo que desee en el paso de condición, Sistema operativo
- **Compliance Module**: Debe asegurarse de seleccionar el mismo módulo de cumplimiento que tiene en el paso de condición, Condición Anti-Malware
- **Posture Type**: Elegir agente
- **Conditions**: Seleccione la condición o condiciones que ha creado en el paso Configurar condiciones de postura
- **Remediations Actions**: elija **Message Text Only** para este ejemplo o, si tiene otra acción de remediación, utilícela
- Haga clic en **Save**

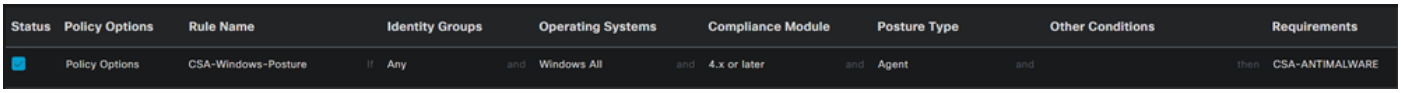
Una vez configurado, puede continuar con el paso, **Configure Posture Policy**

Configurar política de estado

- Vaya a su panel de ISE
- Haga clic en **Work Center > Posture Policy**
- Haga clic en una **Edit** de las directivas y haga clic en **Insert new Policy**




- En la nueva directiva, configure los siguientes parámetros:




- **Status**: marque la casilla de verificación no enable the policy
- **Rule Name**: configure un nombre para reconocer la política configurada
- **Identity Groups**: elija las identidades que desea evaluar

- **Operating Systems**: elija el sistema operativo en función de la condición y los requisitos configurados anteriormente
- **Compliance Module**: elija el módulo de conformidad en función de la condición y los requisitos configurados anteriormente
- Posture Type: Elegir agente
- **Requeriments**: Elija los requisitos configurados en el paso, Configure Posture Requirements
- Haga clic en **Save**

Configurar el aprovisionamiento de clientes

Para proporcionar a los usuarios el módulo ISE, configure el aprovisionamiento del cliente para equipar los equipos con el módulo de estado ISE. Esto le permite verificar el estado de las máquinas una vez que se ha instalado el agente. Para continuar con este proceso, estos son los siguientes pasos:

Vaya al panel de ISE.

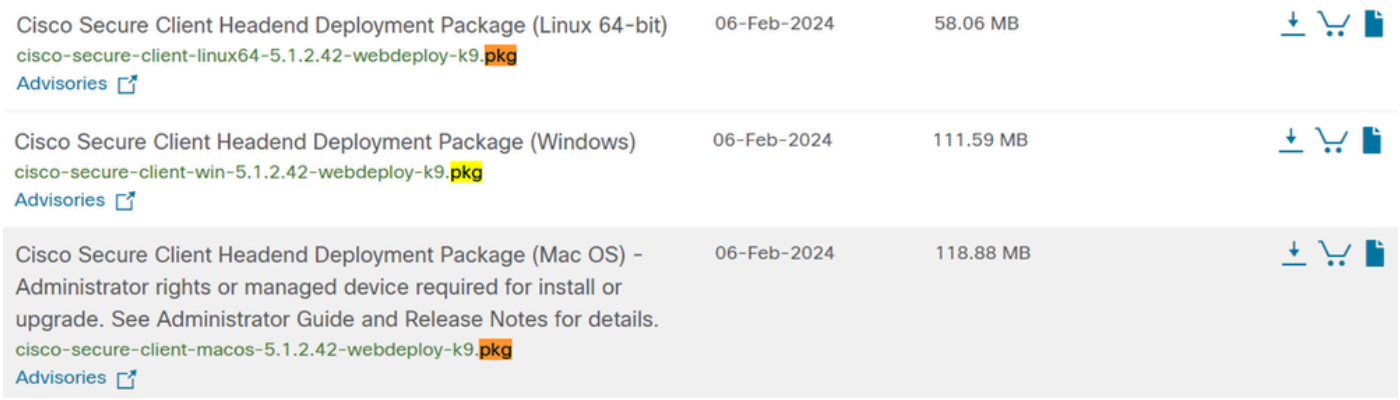
- Haga clic en **Work Center > Client Provisioning**
- Elegir **Resources**

Hay tres cosas que debe configurar en el aprovisionamiento de clientes:

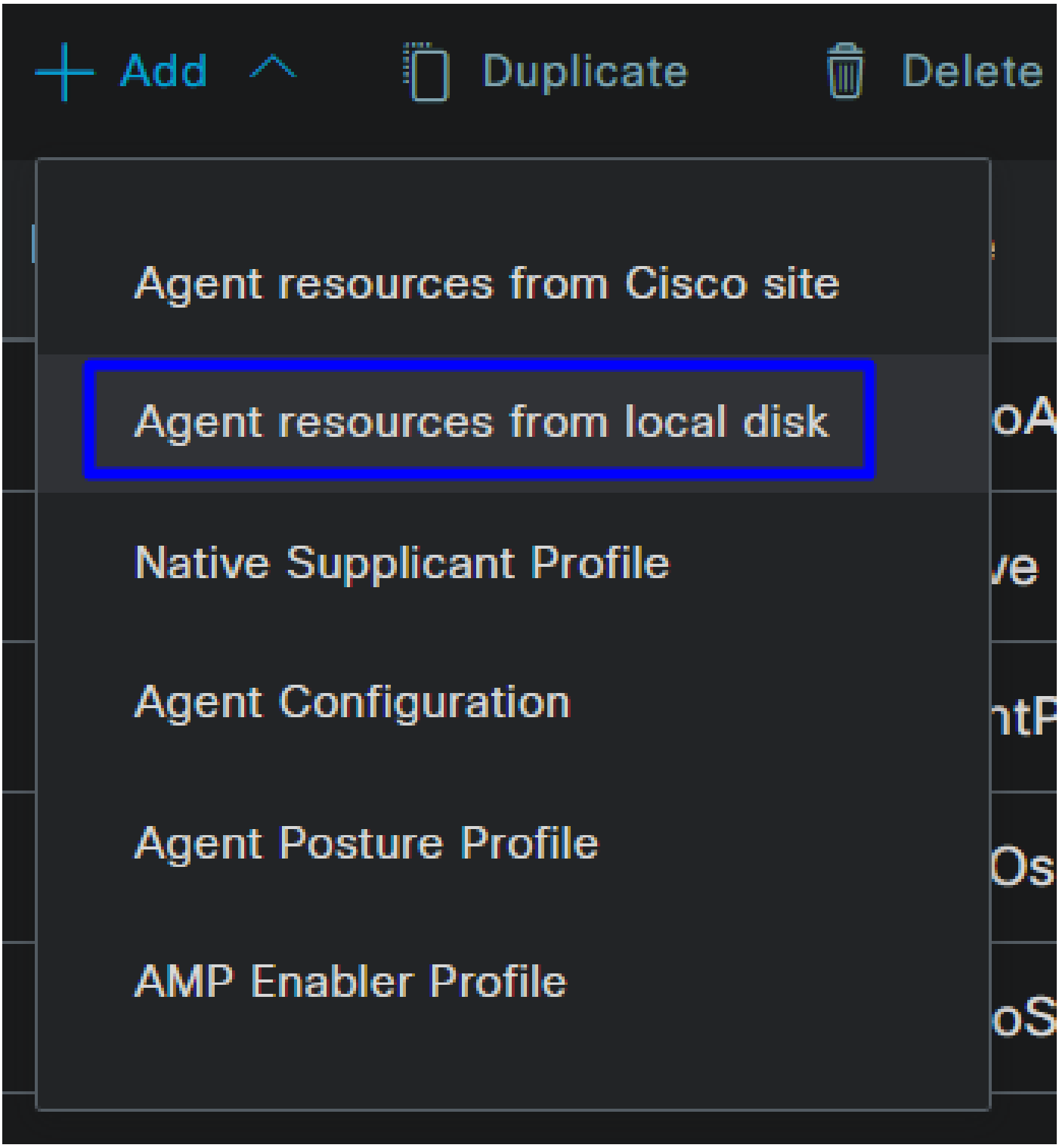
| Recursos para configurar | Descripción |
|---|---|
| 1. **Agent Resources** | Paquete Secure Client Web Provisioning. |
| 2. **Compliance Module** | Módulo de cumplimiento de Cisco ISE |
| 3. **Agent Profile** | Control del perfil de aprovisionamiento. |
| 3. **Agent Configuration** | Defina qué módulos se aprovisionan configurando el portal de aprovisionamiento mediante el perfil de agente y los recursos de agente. |

**Step 1** Descargar y cargar recursos de agente

- Para agregar un nuevo recurso de agente, navegue hasta el portal de descarga de Cisco y descargue el paquete de despliegue web; el archivo de despliegue web debe tener el formato .pkg.

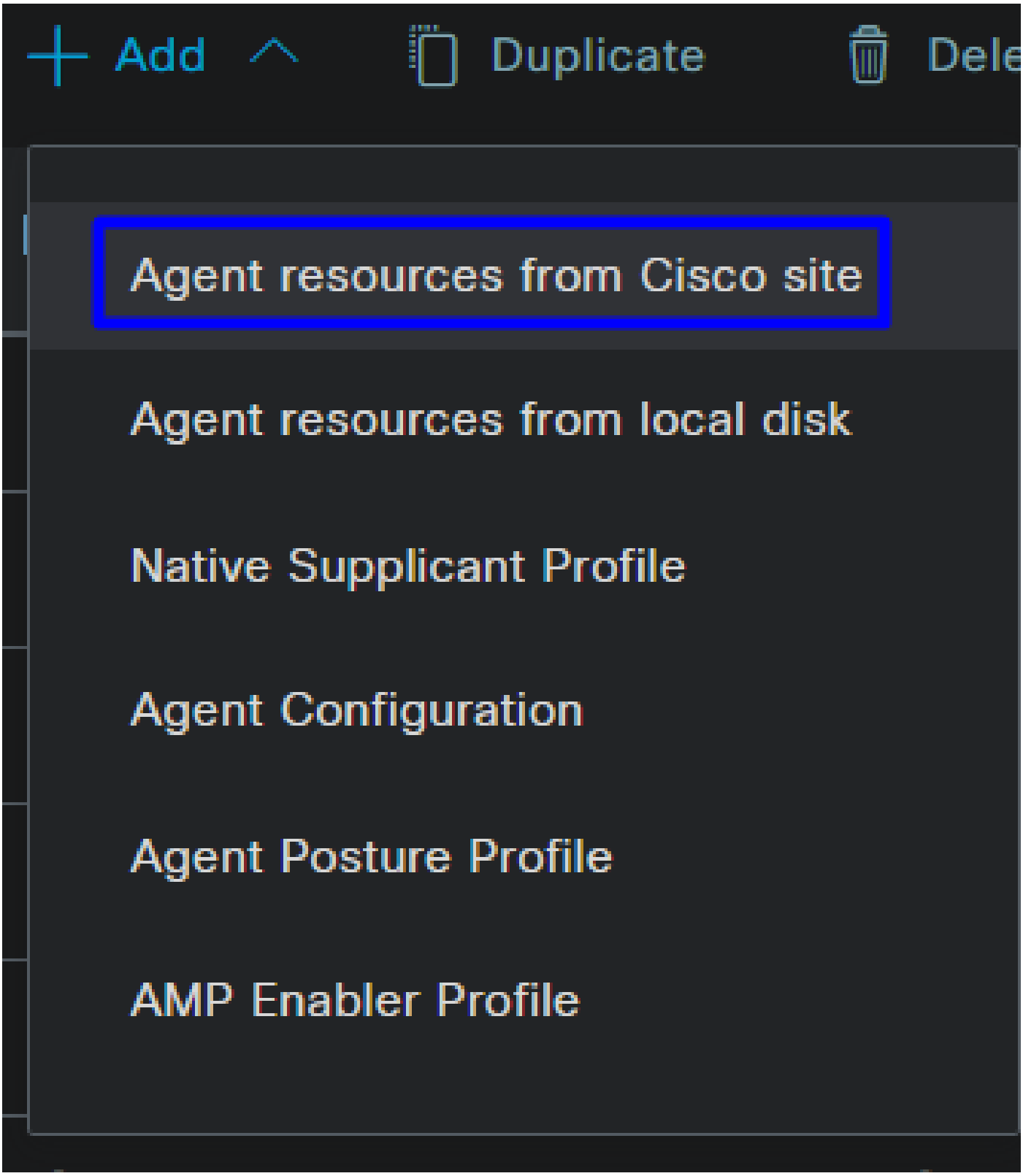



- Haga clic en + Add > Agent resources from local disk y cargue los paquetes

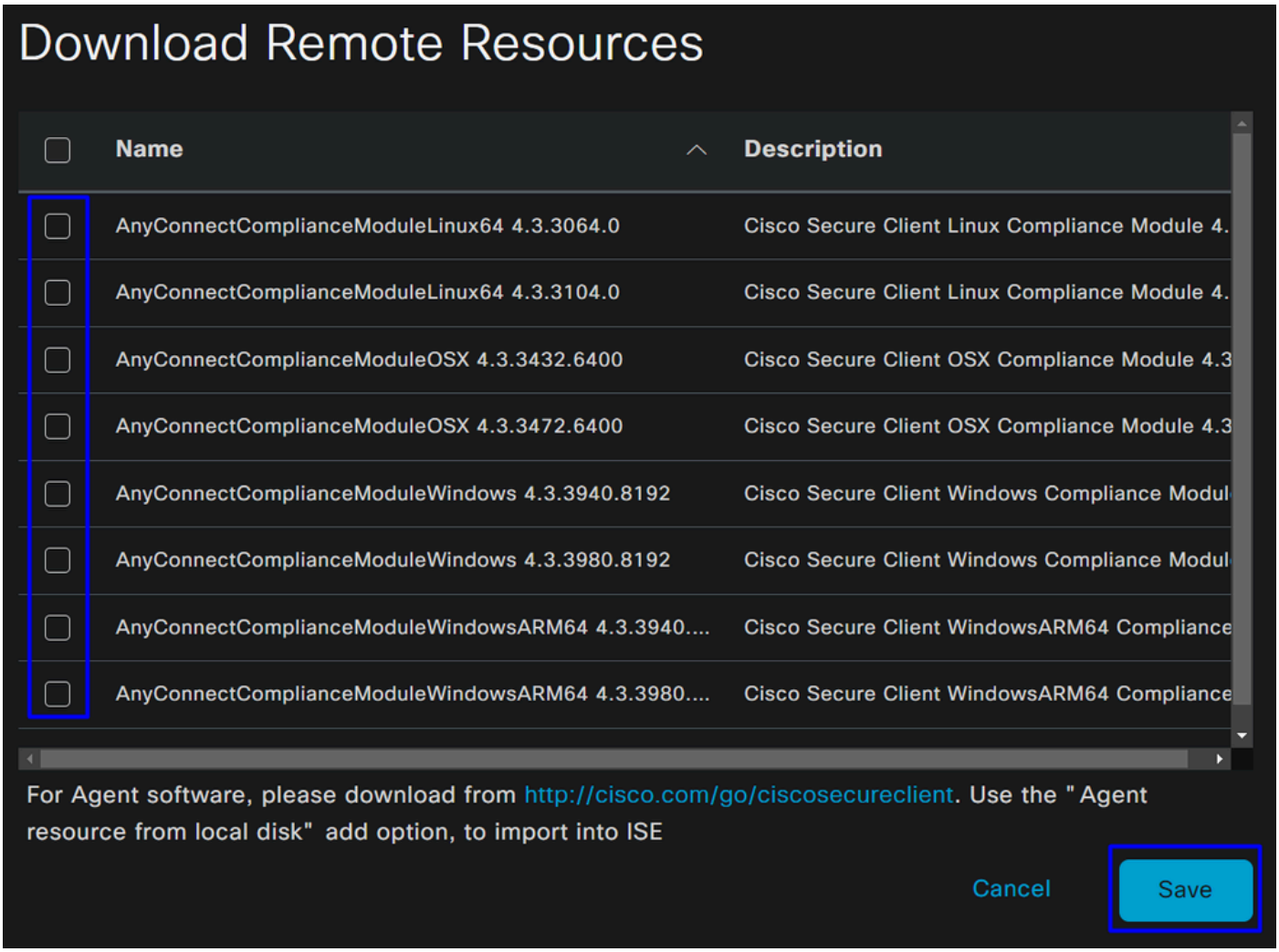



**Step 2**Descargue el módulo de conformidad

- Haga clic en + Add > Agent resources from Cisco Site

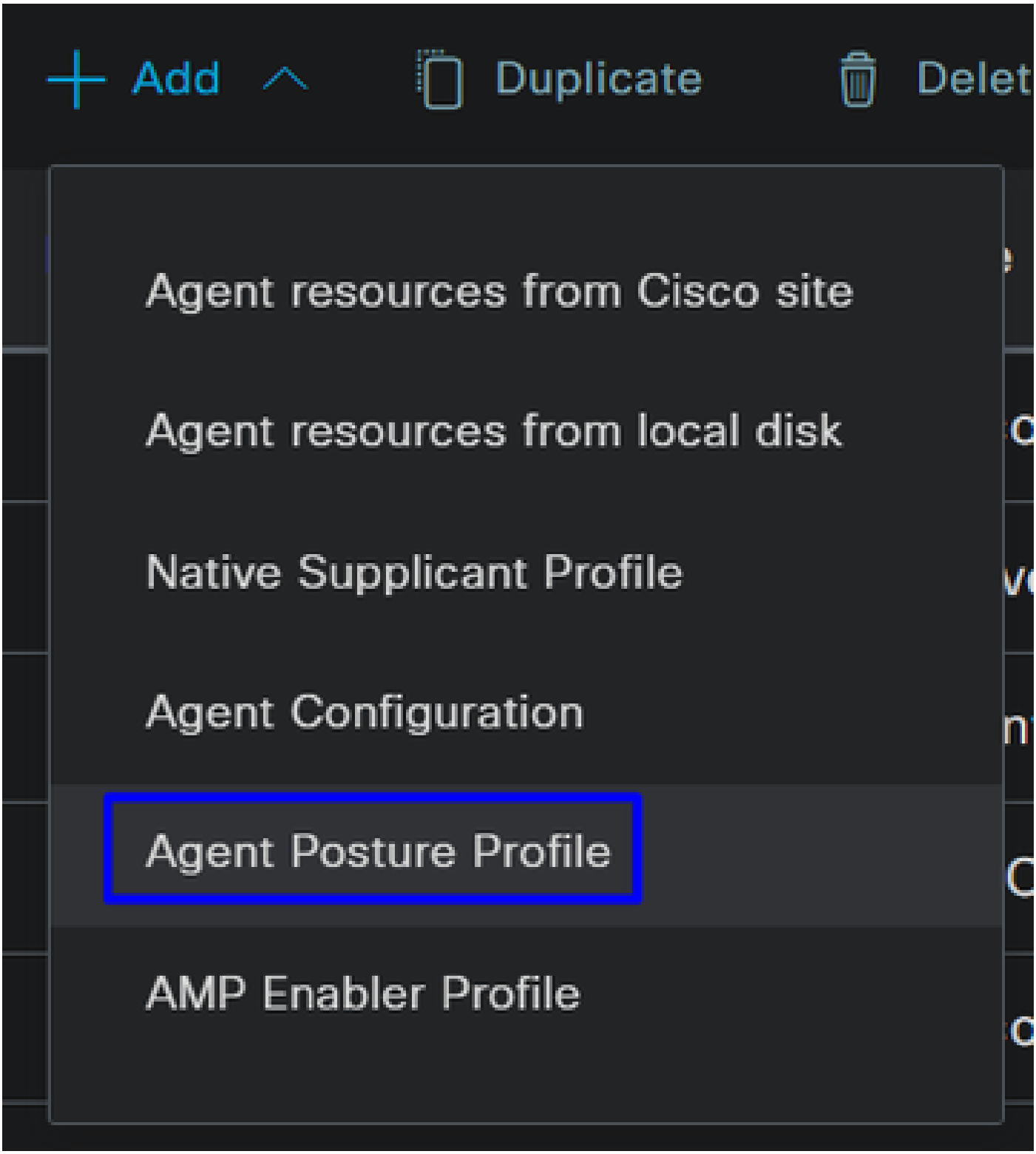



- Marque la casilla de cada módulo de conformidad necesario y haga clic en **Save**

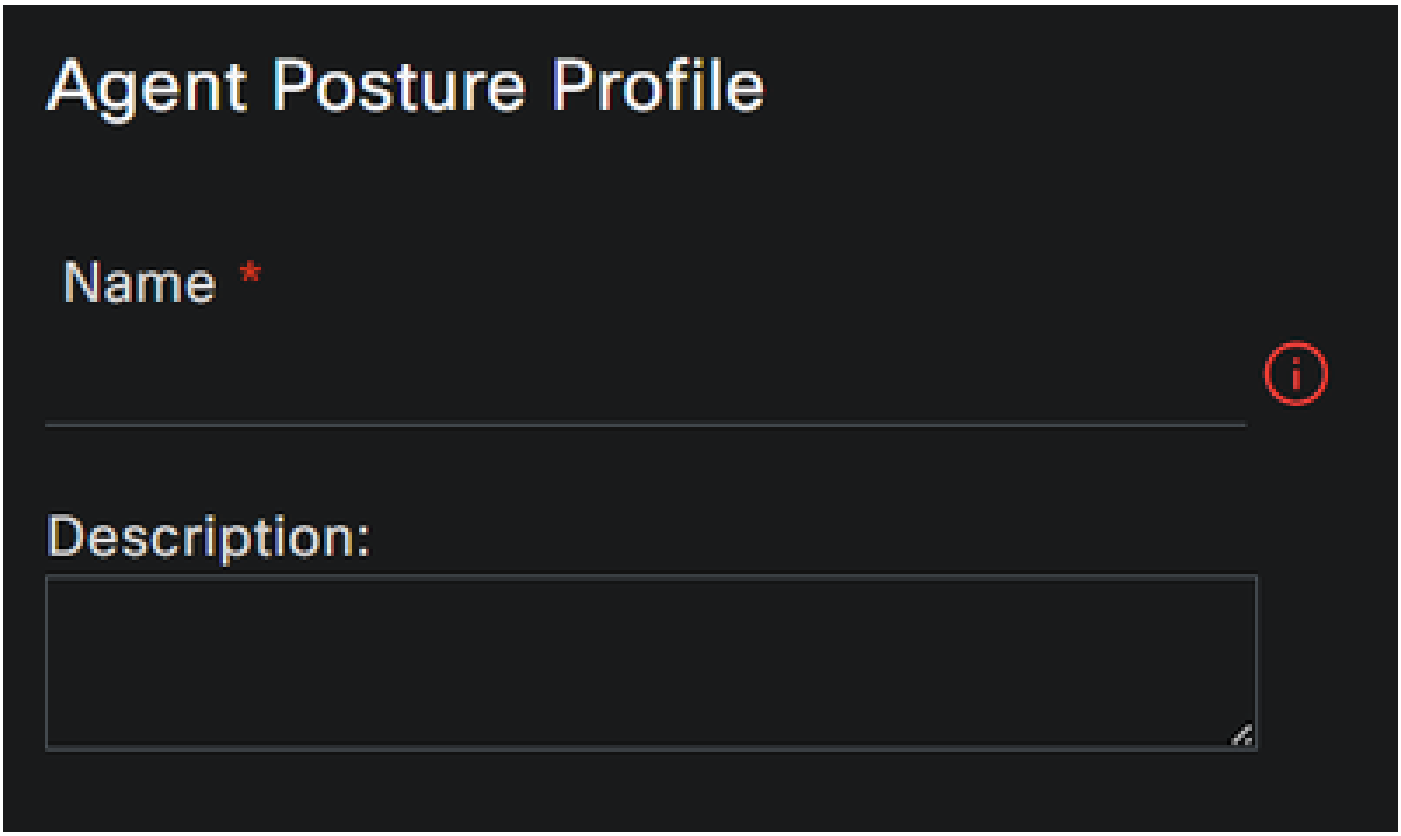



Step 3Configuración del perfil de agente

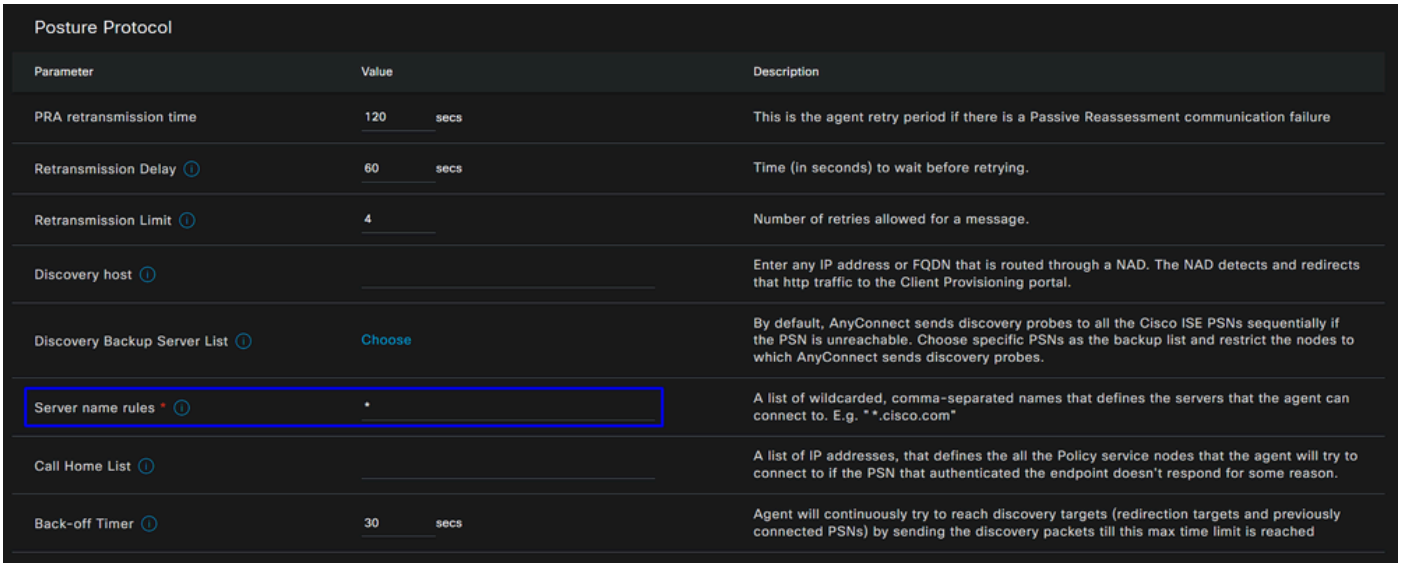
- Haga clic en + Add > Agent Posture Profile




- Cree un **Name** para el **Posture Profile**

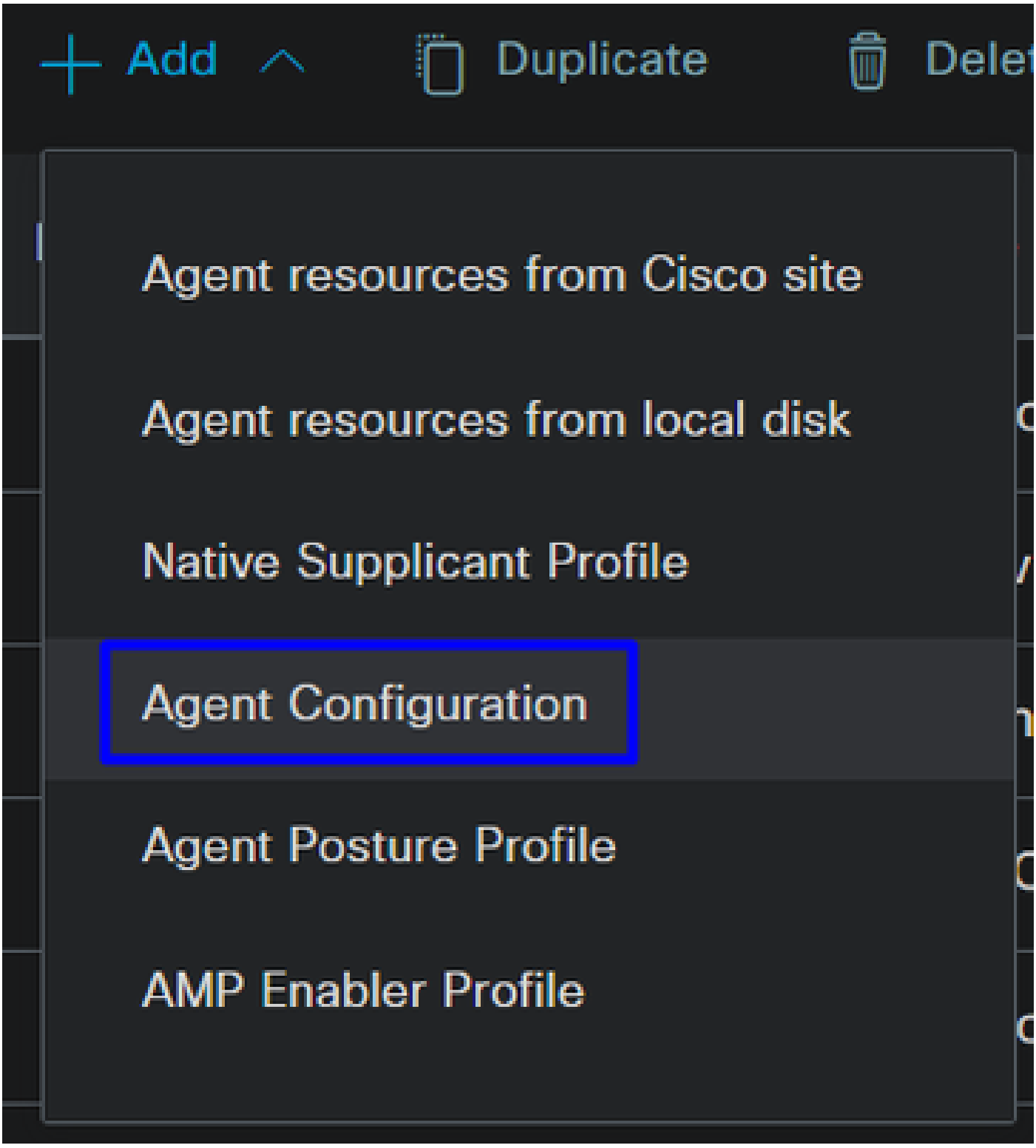



- En Reglas de nombre de servidor, coloque una ***** y haga clic **Save** después de ella

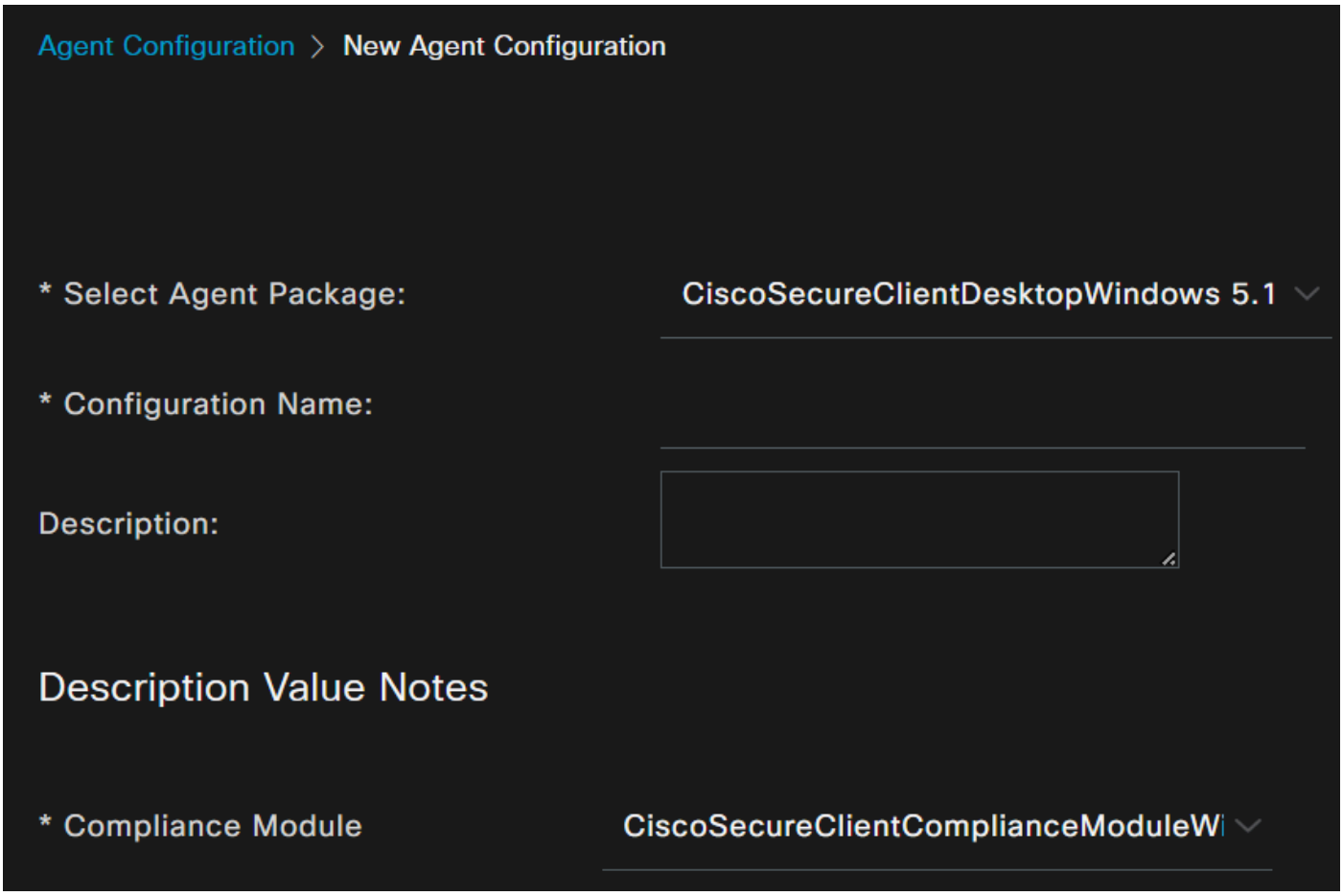


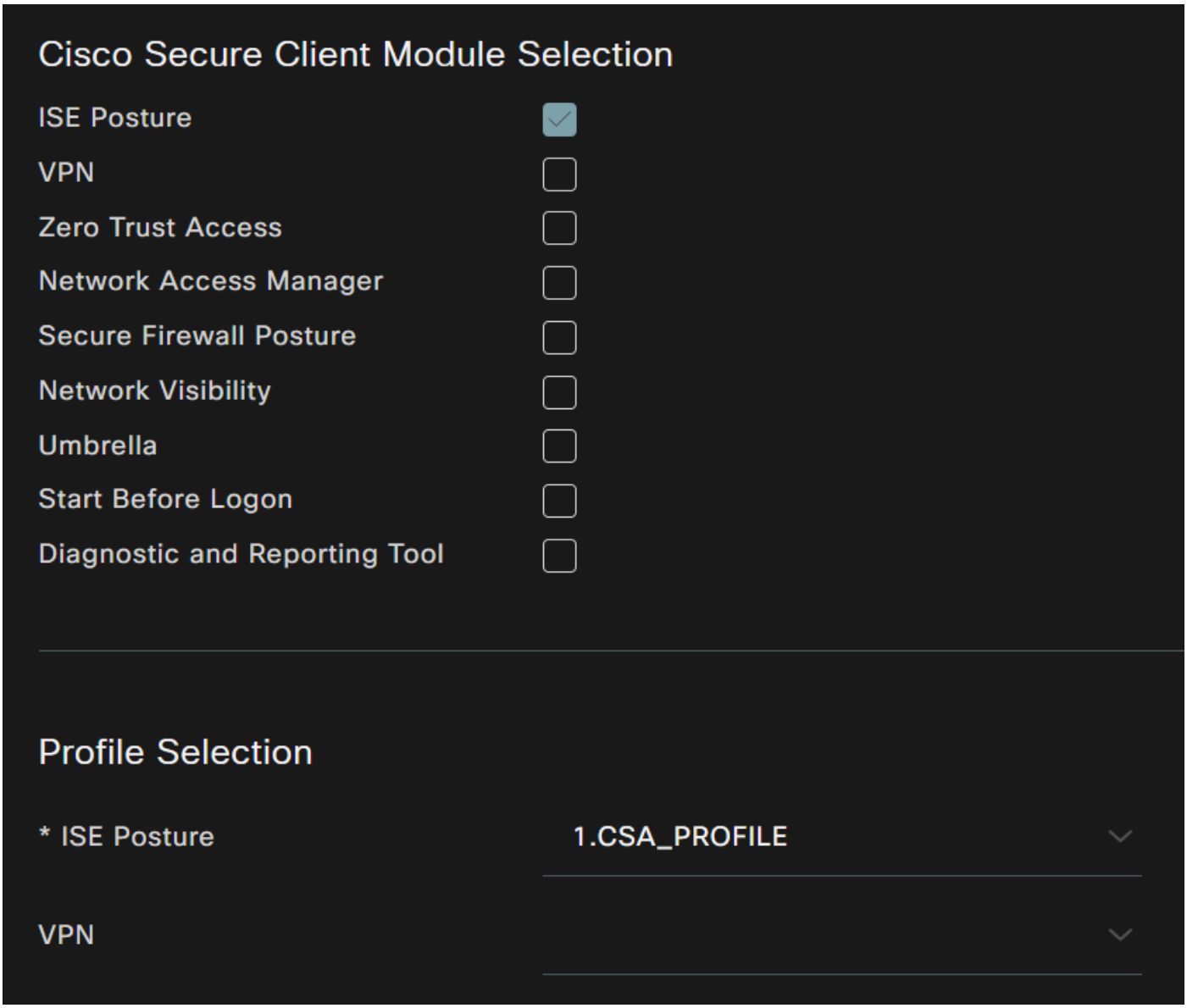

**Step 4** Configuración de la configuración del agente

- Haga clic en + Add > Agent Configuration




- Después de eso, configure los siguientes parámetros:


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

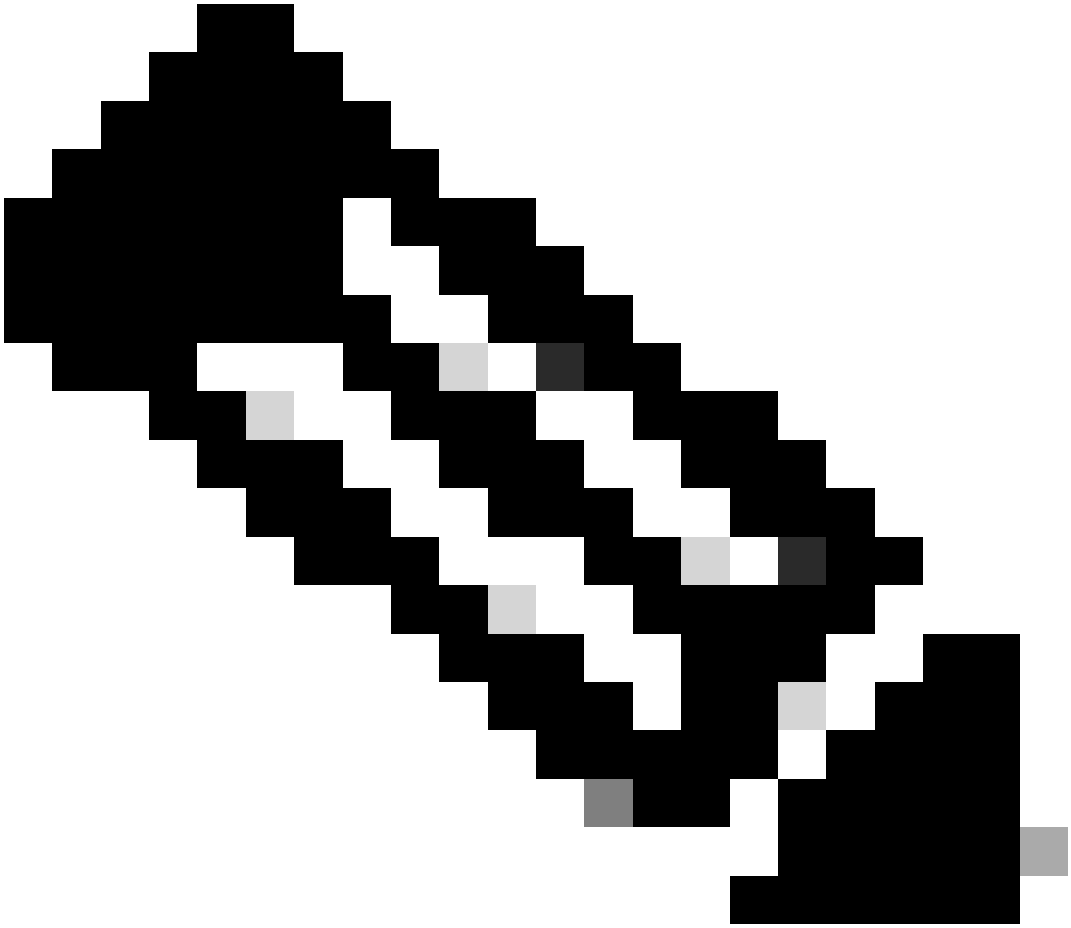



- Select Agent Package : Elija el paquete cargado en Step1 Download and Upload Agent Resources
- **Configuration Name**: elija un nombre para reconocer el **Agent Configuration**
- **Compliance Module**: Elija el módulo de cumplimiento descargado en el paso 2 Descargue el módulo de cumplimiento
- Cisco Secure Client Module Selection
    - **ISE Posture**: Marque la casilla de verificación
- **Profile Selection**

- **ISE Posture**: Elija el perfil de ISE configurado en el paso 3 Configuración del perfil de agente

- Haga clic en **Save**

---



**Nota**: se recomienda que cada sistema operativo, Windows, Mac OS o Linux, tenga una configuración de cliente independiente.

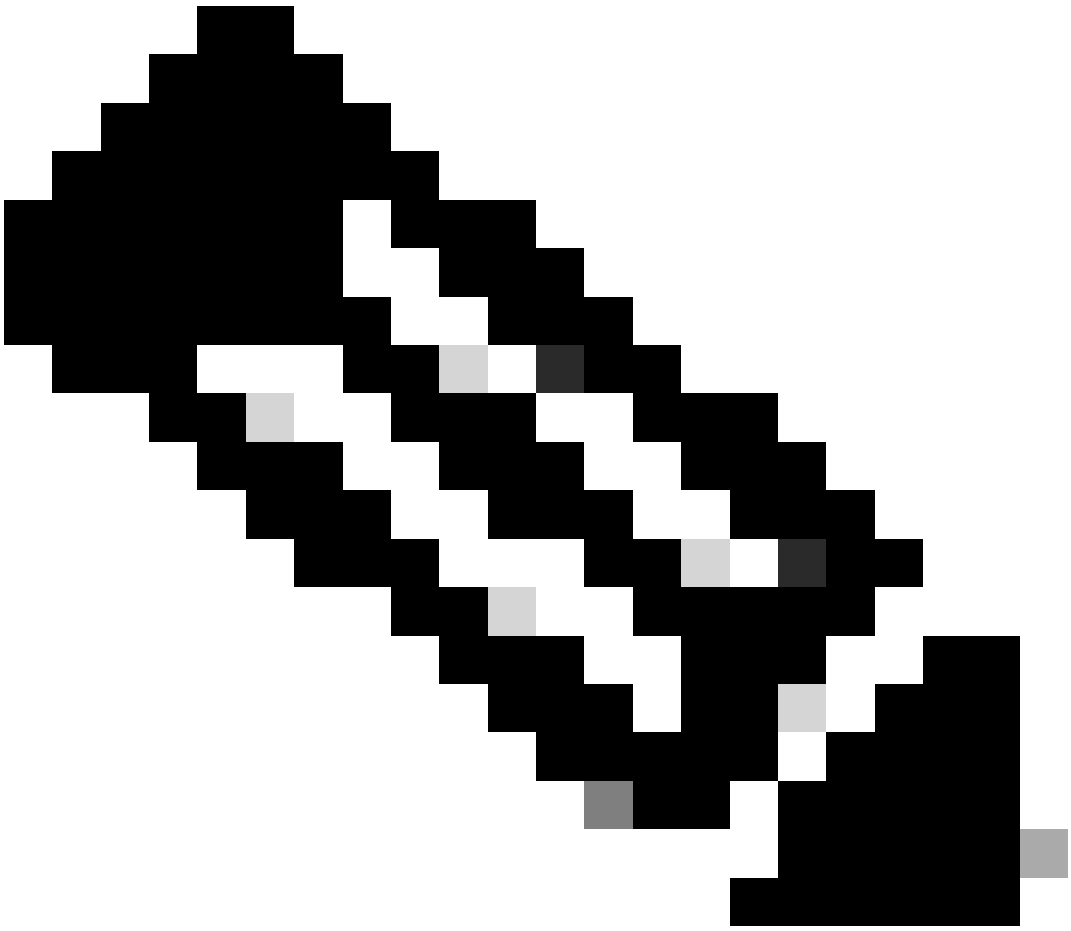
---

Configurar directiva de aprovisionamiento de clientes

Para habilitar el aprovisionamiento del estado de ISE y los módulos configurados en el último paso, debe configurar una política para realizar el aprovisionamiento.

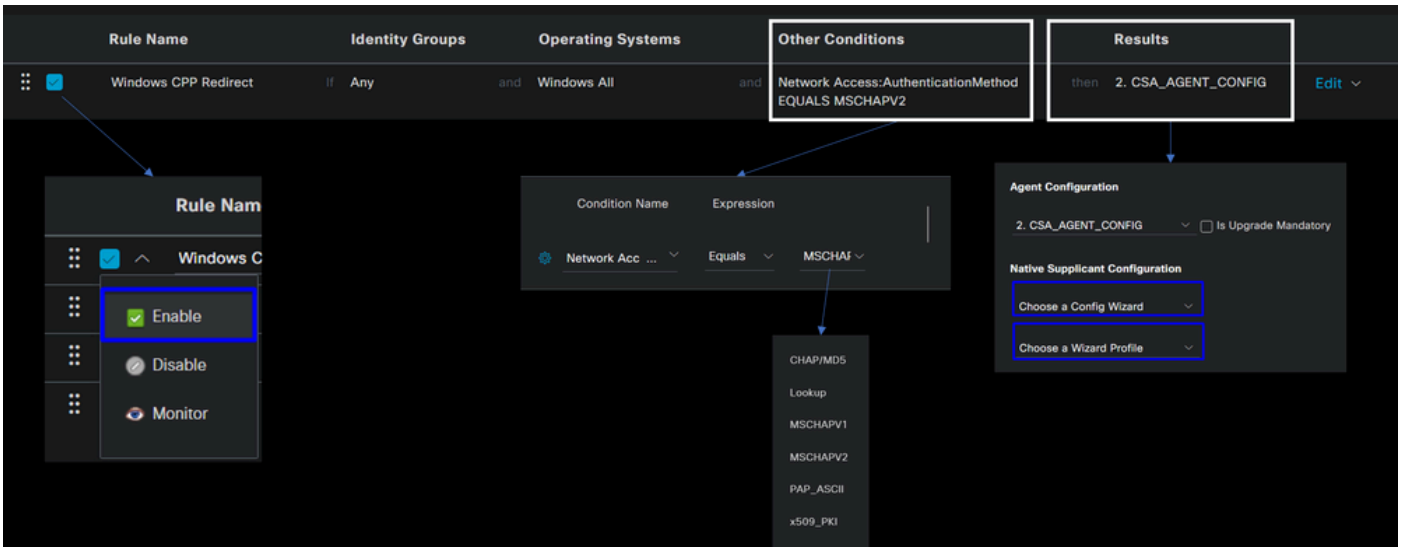
- Vaya a su panel de ISE
- Haga clic en **Work Center > Client Provisioning**

---



**Nota**: se recomienda que cada sistema operativo, Windows, Mac OS o Linux, tenga una política de configuración de cliente.

---




- **Rule Name**: configure el nombre de la política según el tipo de dispositivo y la selección del grupo de identidad para tener una manera fácil de identificar cada política
- **Identity Groups**: elija las identidades que desea evaluar en la política
- **Operating Systems**: elija el sistema operativo en función del paquete de agentes seleccionado en el paso Seleccionar paquete de agentes
- **Other Condition**: Elija **Network Access** en función del **Authentication Method**EQUALS al método configurado en el paso, Agregar grupo RADIUS o puede dejar en blanco
- **Result**: Seleccione la configuración del agente en el paso 4 Configuración de la configuración del agente
    - **Native Supplicant Configuration**: Elija Config Wizard y Wizard Profile
- Marque la directiva como habilitada si no aparece como habilitada en la casilla de verificación.

Crear los perfiles de autorización

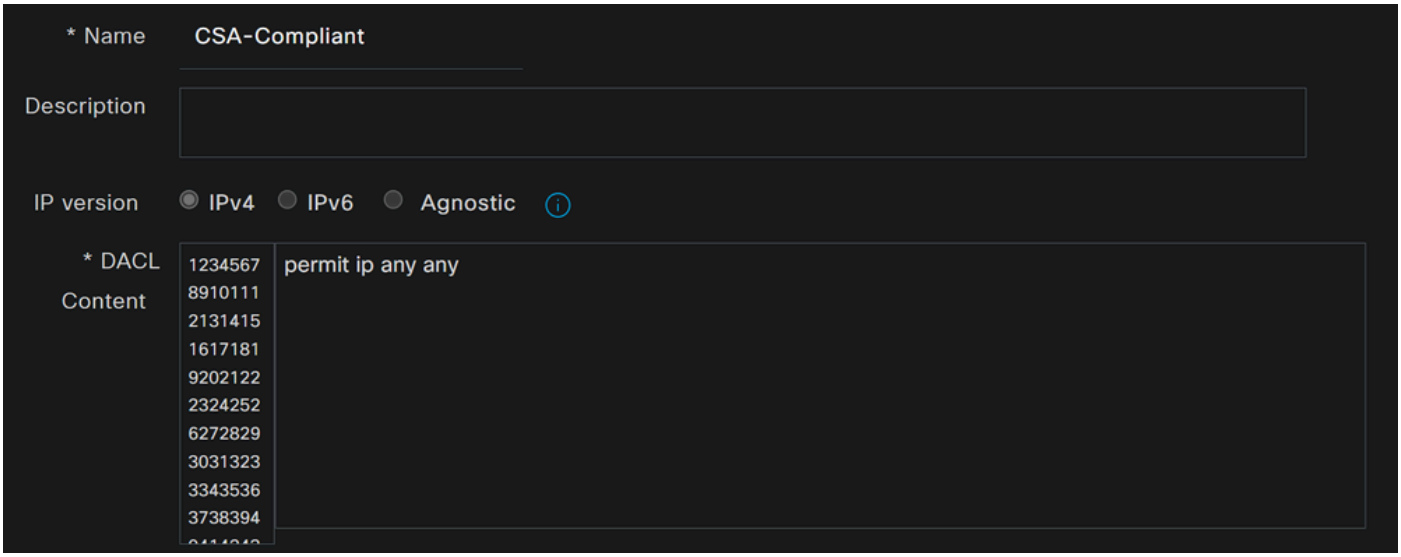
El perfil de autorización limita el acceso a los recursos en función del estado de los usuarios después de la autenticación. La autorización debe verificarse para determinar a qué recursos puede acceder el usuario en función del estado.

| Perfil de autorización | Descripción |
|---|---|
| Conforme | Compatible con el usuario - Agente instalado - Verificación de estado |
| Conformidad | Cumplimiento desconocido por el usuario - Redireccionamiento para |

| | |
|---|---|
| desconocida | instalar el agente - Estado pendiente de verificación |
| DenegarAcceso | Usuario no conforme - Denegar acceso |

Para configurar la DACL, navegue hasta el panel de ISE:

- Haga clic en **Work Centers > Policy Elements > Downloadable ACLs**
- Haga clic en **+Add**
- Cree el **Compliant DACL**




- **Name**: agregue un nombre que haga referencia a DACL-Compliant
- **IP version**: Elegir **IPv4**
- DACL Content: cree una lista de control de acceso (DACL) descargable que proporcione acceso a todos los recursos de la red

<#root>

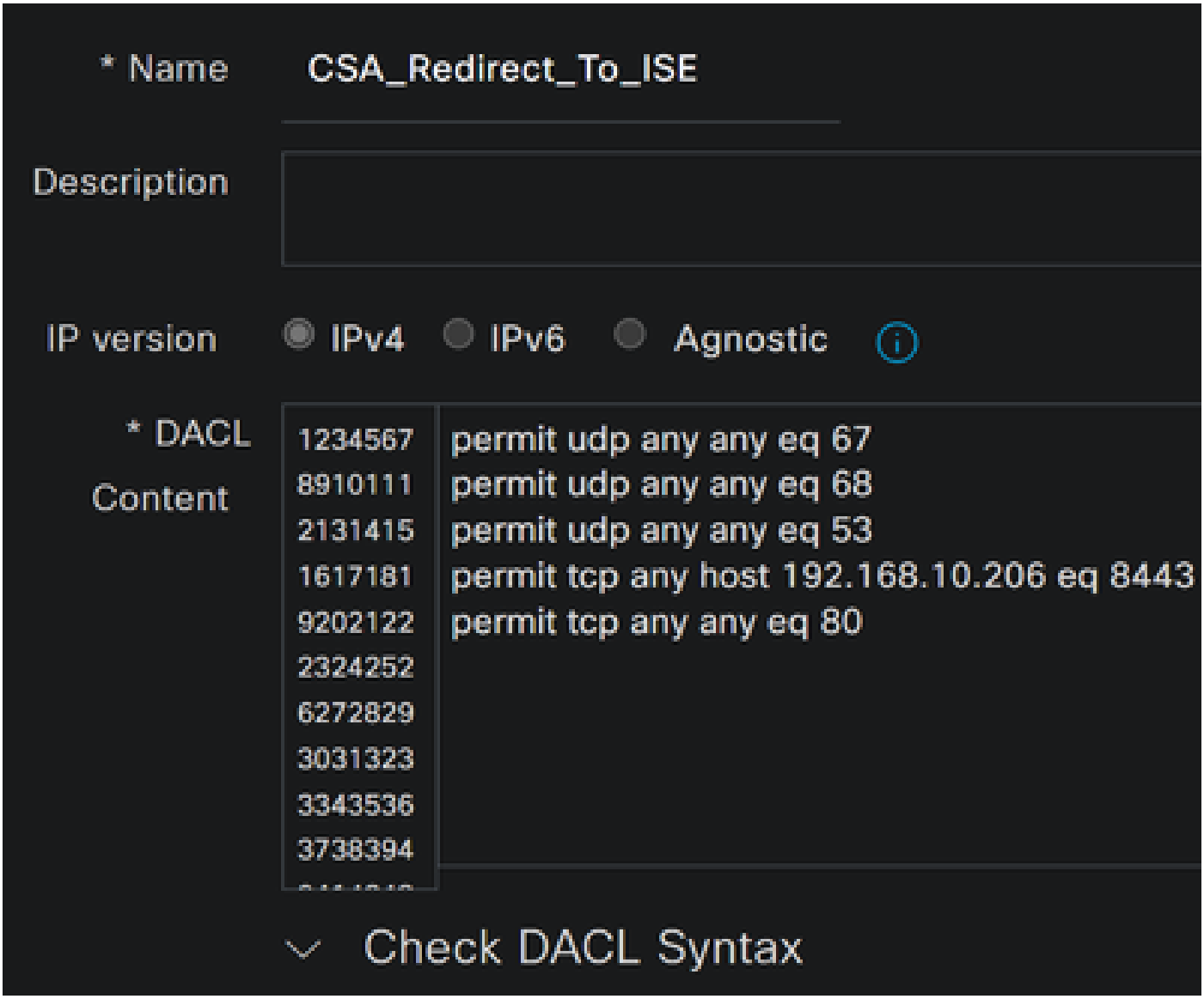
```
permit ip any any
```

Haga clic **Save** y cree la DACL de conformidad desconocida

- Haga clic en **Work Centers > Policy Elements > Downloadable ACLs**

- Haga clic en **+Add**

- Cree el **Unknown Compliant DACL**

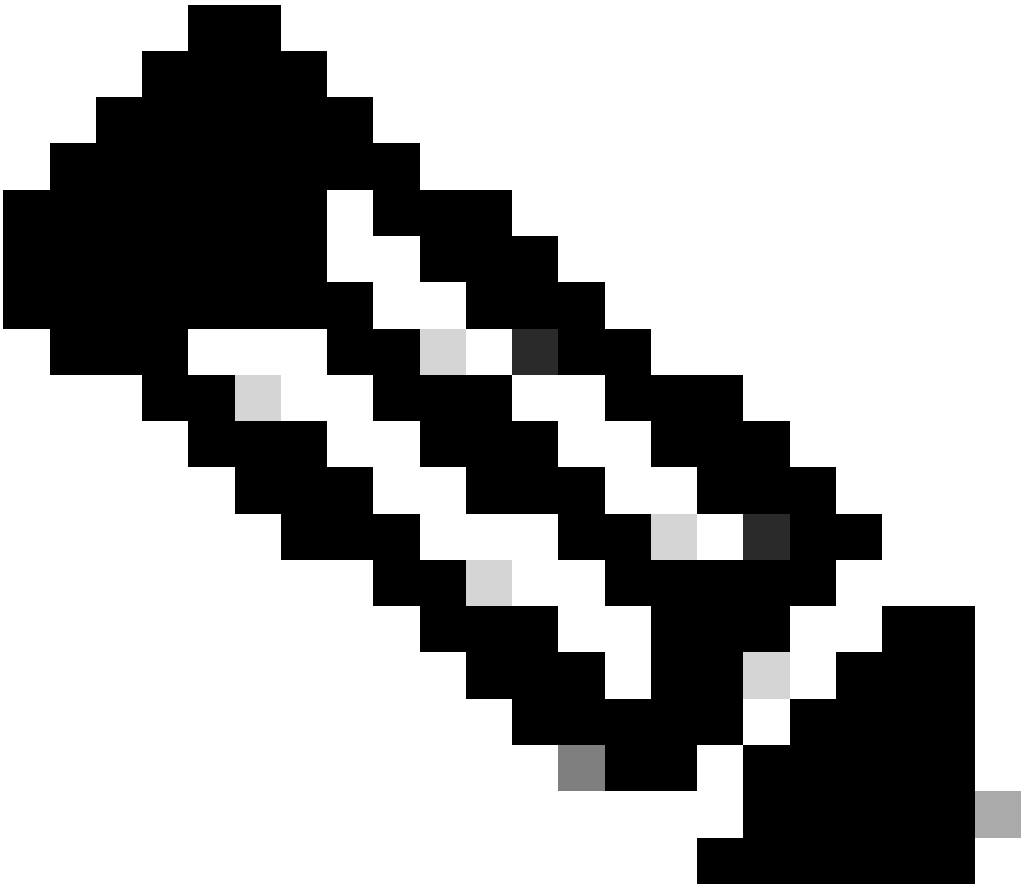



- **Name**: agregue un nombre que haga referencia a DACL-Unknown-Compliant

- **IP version**: Elegir **IPv4**

- **DACL Content**: Cree una DACL que ofrezca acceso limitado a la red, DHCP, DNS, HTTP y el portal de aprovisionamiento a través del puerto 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
```

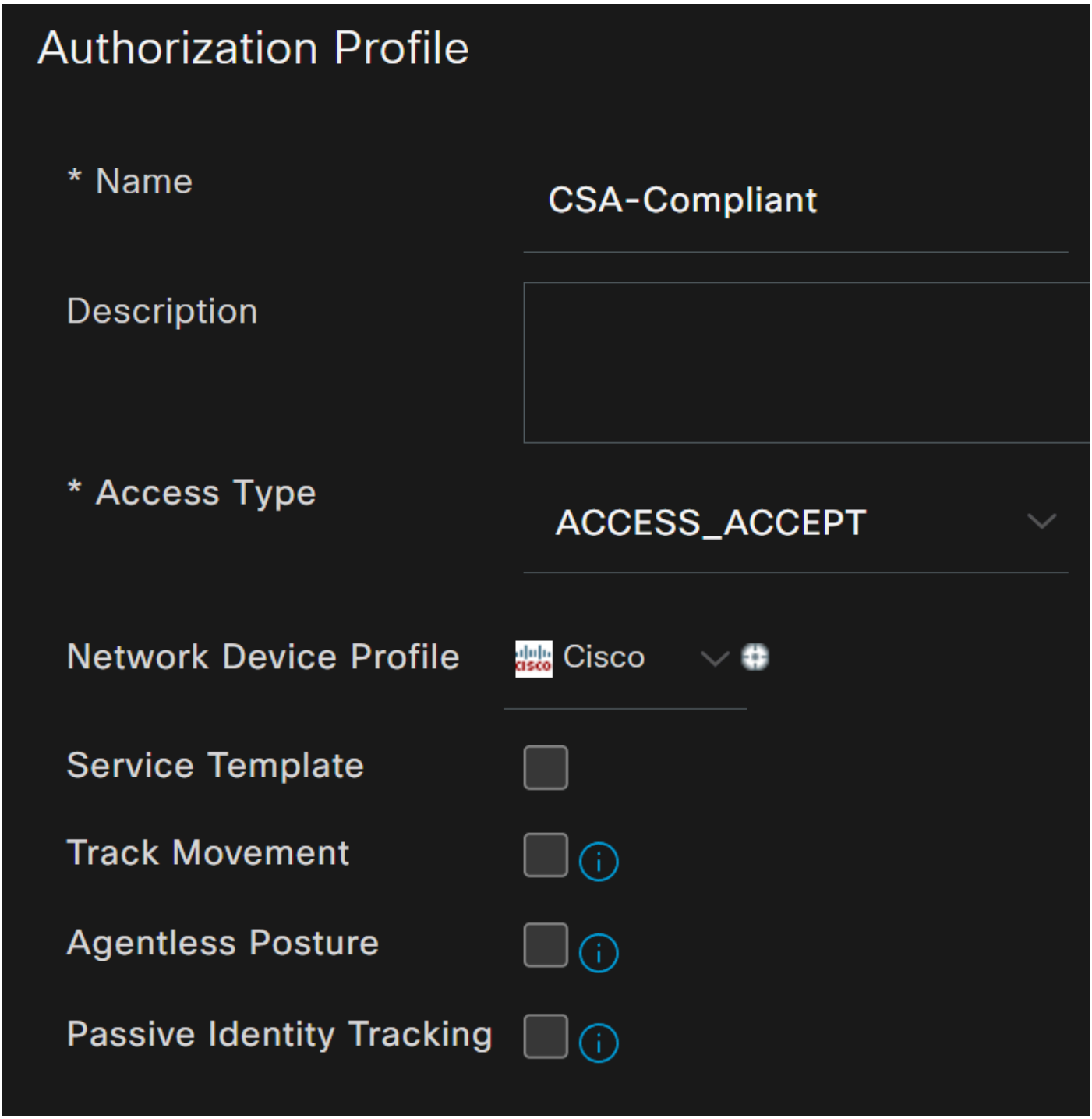


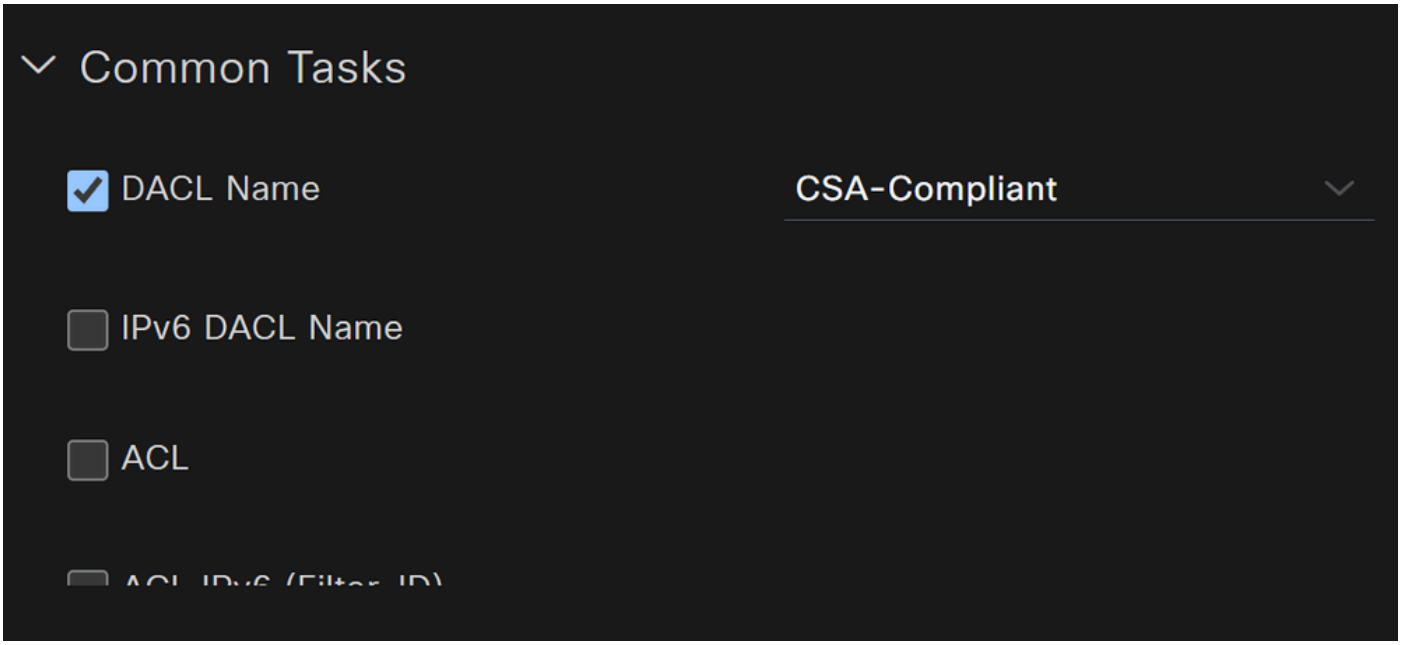
**Nota**: en esta situación, la dirección IP 192.168.10.206 corresponde al servidor de Cisco Identity Services Engine (ISE) y el puerto 8443 está designado para el portal de aprovisionamiento. Esto significa que se permite el tráfico TCP a la dirección IP 192.168.10.206 a través del puerto 8443, lo que facilita el acceso al portal de aprovisionamiento.

En este momento, dispone de la DACL necesaria para crear los perfiles de autorización.

Para configurar los perfiles de autorización, navegue hasta el panel de ISE:

- Haga clic en **Work Centers > Policy Elements > Authorization Profiles**
    - Haga clic en **+Add**
    - Cree el **Compliant Authorization Profile**





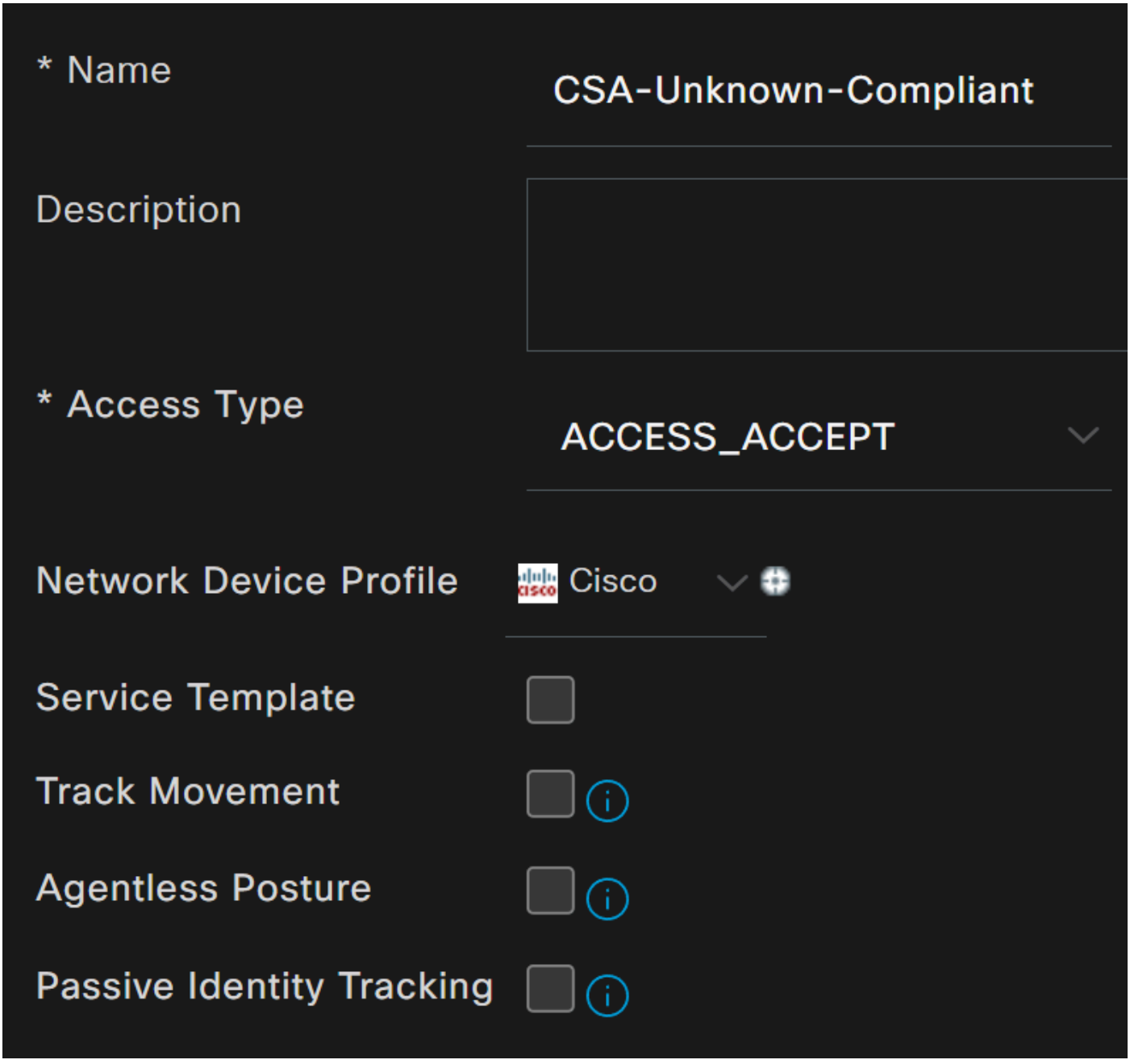

- **Name**: cree un nombre que haga referencia al perfil de autorización compatible
- Access Type: Elegir **ACCESS_ACCEPT**

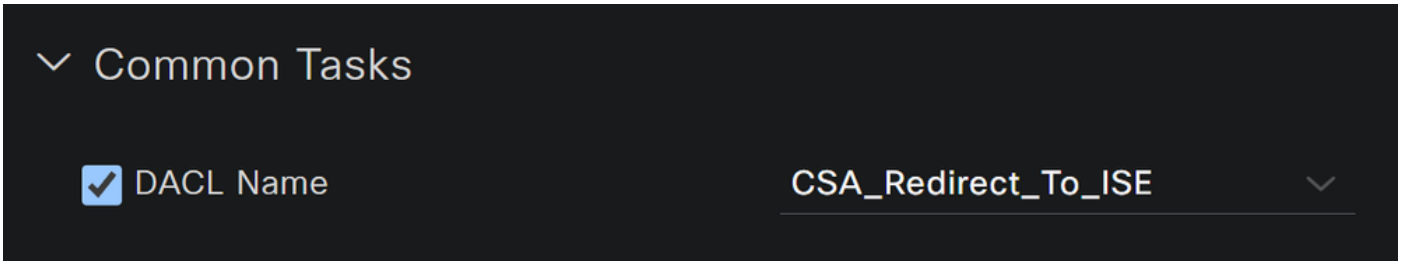
- **Common Tasks**
  - **DACL NAME**: Elija la DACL configurada en el paso DACL conforme

Haga clic **Save** y cree el Unknown Authorization Profile

- Haga clic en **Work Centers > Policy Elements > Authorization Profiles**
- Haga clic en **+Add**

- Cree el **Uknown Compliant Authorization Profile**



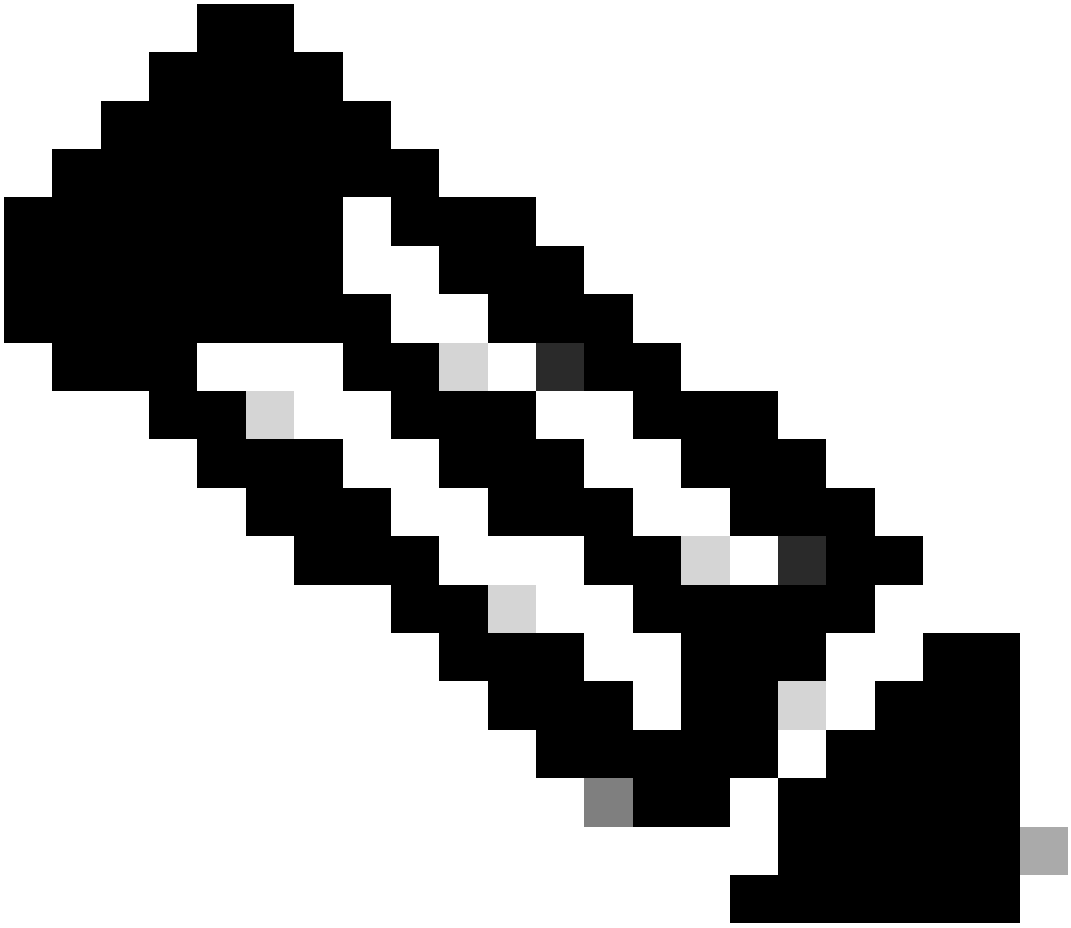




- **Name**: cree un nombre que haga referencia al perfil de autorización conforme desconocido
- Access Type: Elegir **ACCESS_ACCEPT**

- **Common Tasks**
    - **DACL NAME**: Elija la DACL configurada en el paso DACL conforme a desconocido
        - **Web Redirection (CWA,MDM,NSP,CPP)**
            - Elegir **Client Provisioning (Posture)**
                - **ACL**: debe ser redirect
                - **Value**: seleccione el portal de aprovisionamiento predeterminado o, si ha definido otro, selecciónelo

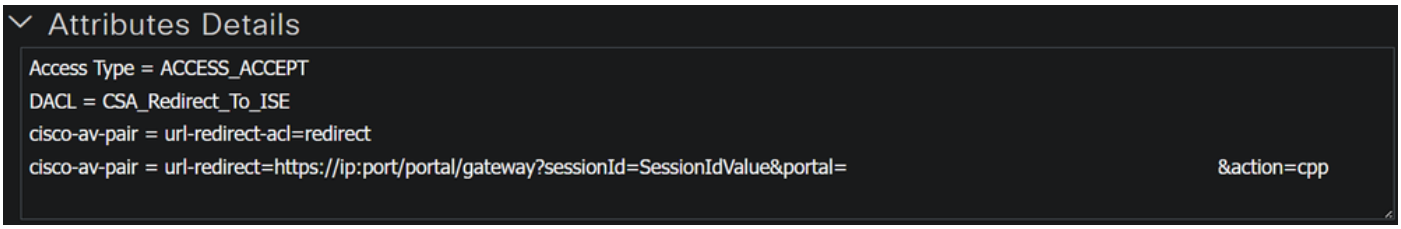
---

---



**Nota**: El nombre de la ACL de redirección en Secure Access para todas las implementaciones es **redirect**.

Después de definir todos estos valores, debe tener algo similar debajo de Attributes Details.




Haga clic **Save** para finalizar la configuración y continuar con el siguiente paso.

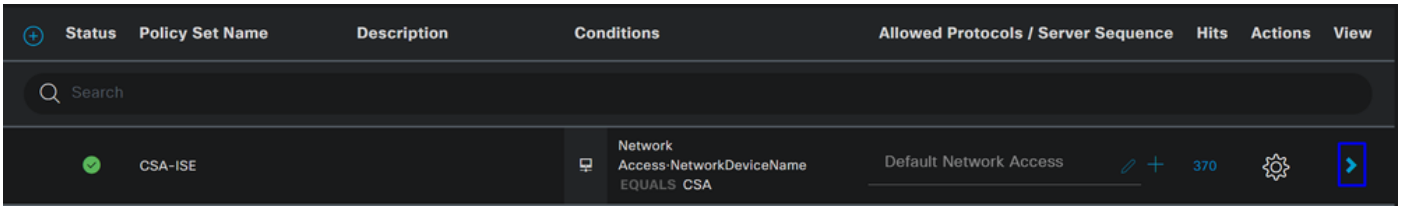
Configurar conjunto de políticas de estado

Estas tres políticas que crea se basan en los perfiles de autorización que ha configurado; por **DenyAccess**ejemplo, no necesita crear otra.

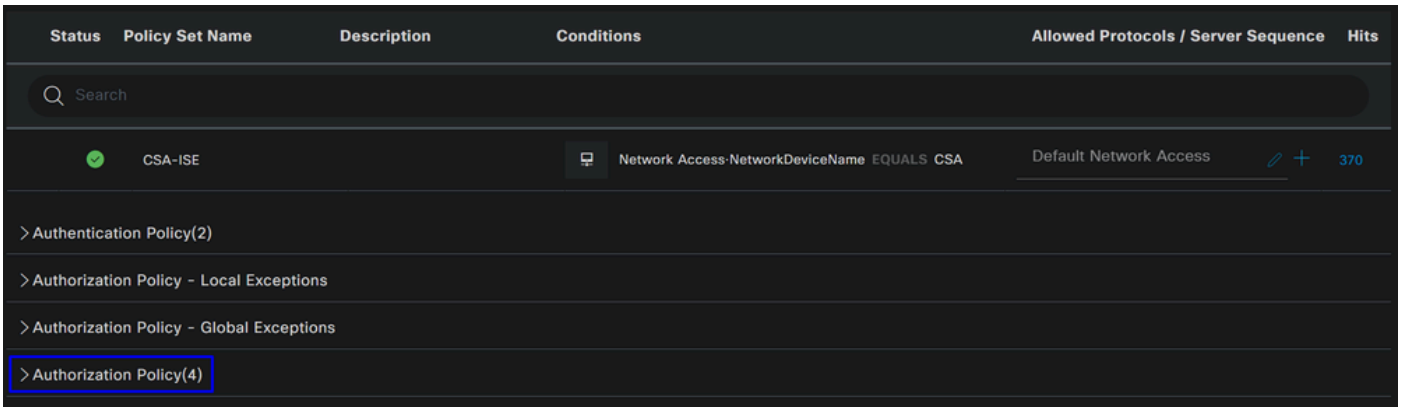
| **Conjunto de políticas - Autorización** | **Perfil de autorización** |
|---|---|
| **Conforme** | Perfil de autorización: compatible |
| **Conformidad desconocida** | Perfil de autorización: compatibilidad desconocida |
| **No conforme** | DenegarAcceso |

Vaya a su panel de ISE

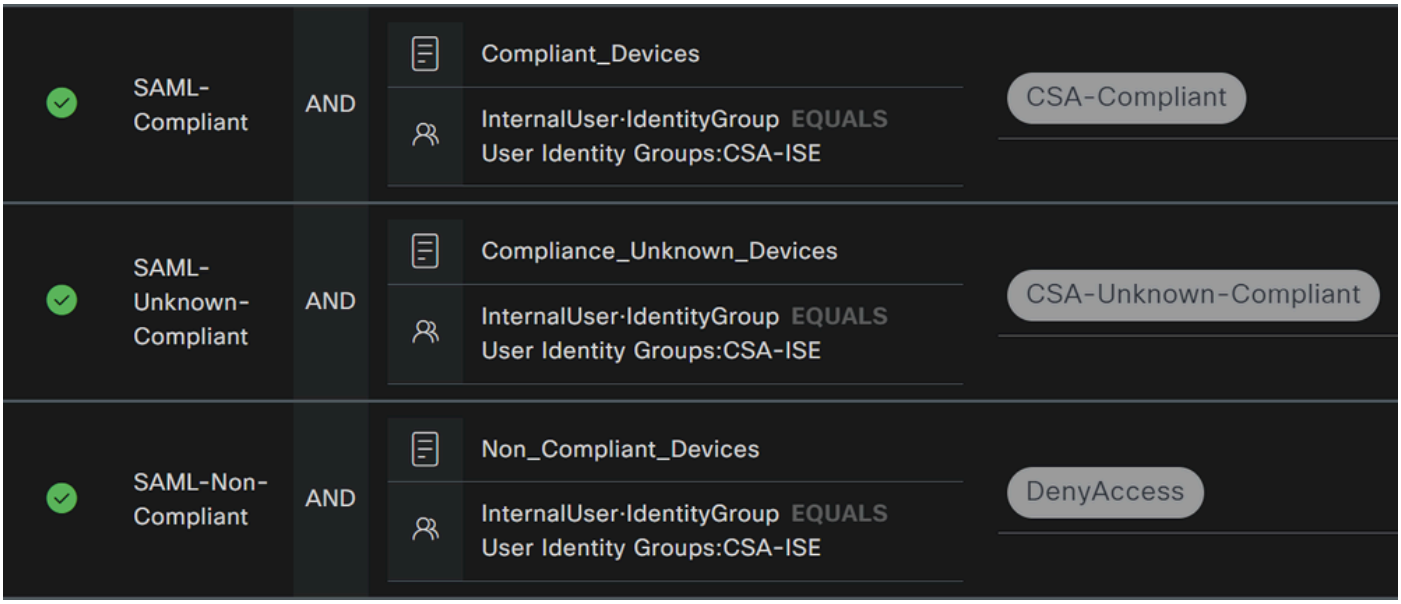
- Haga clic en **Work Center > Policy Sets**
- Haga clic en > elpara acceder a la política que ha creado



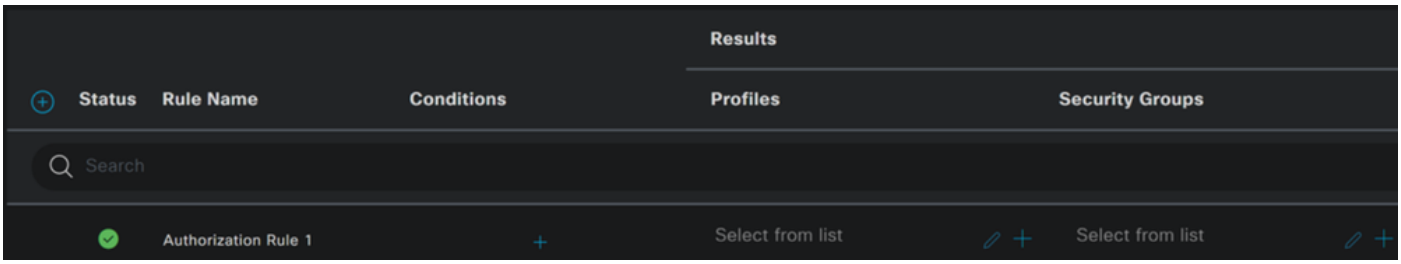

- Haga clic en el Authorization Policy



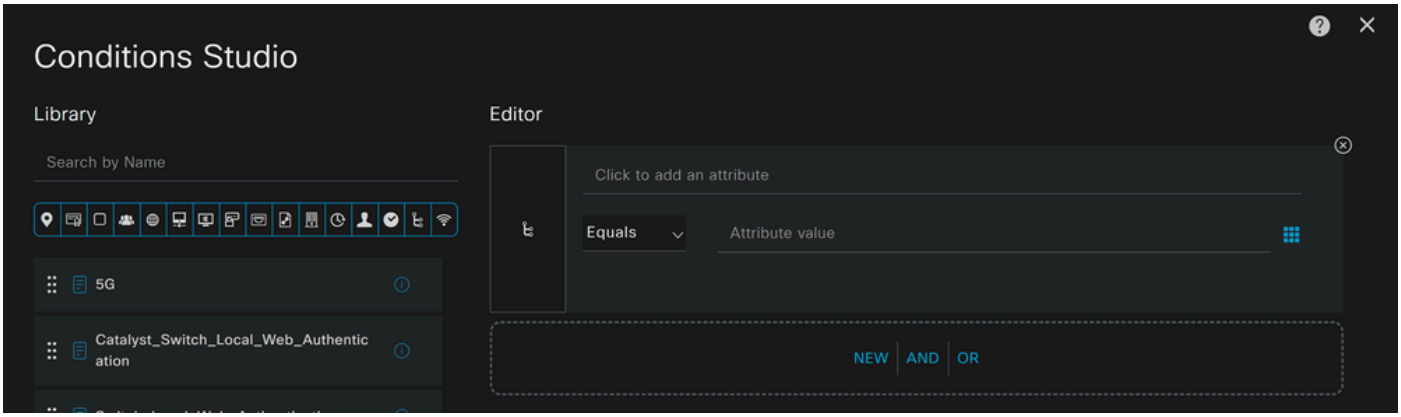

- Cree las tres políticas siguientes en el orden siguiente:



- Haga clic en **+** para definir la **CSA-Compliance** política:

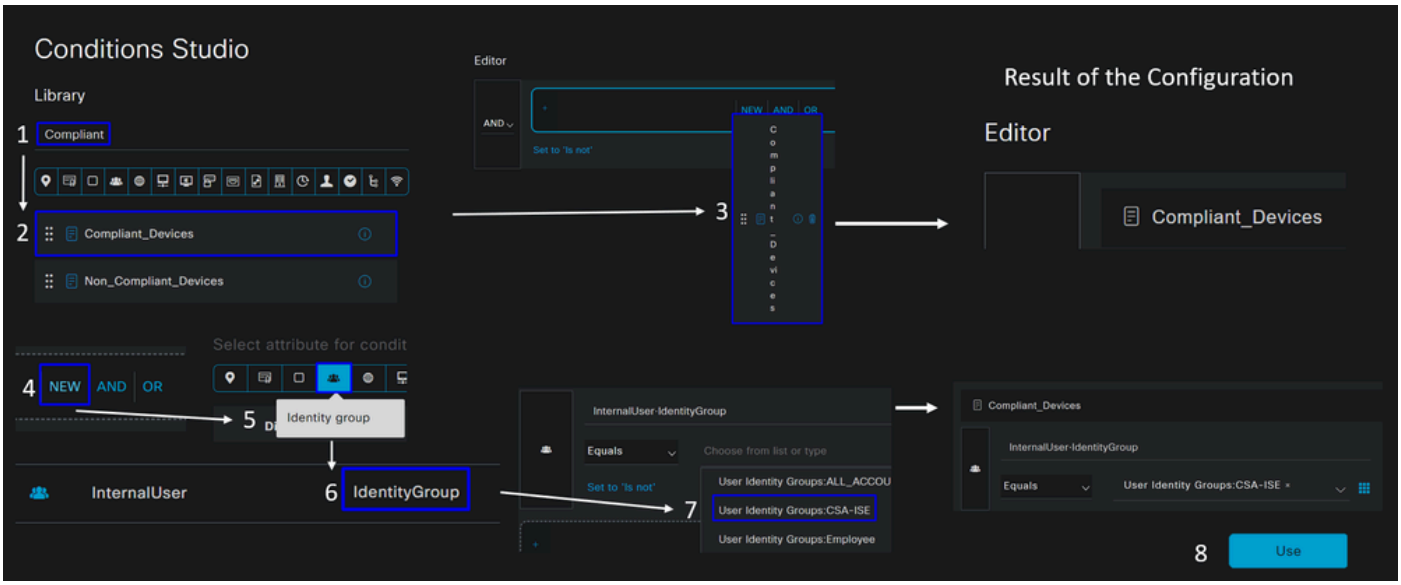



- Para el siguiente paso, cambie el Rule Name, Conditionsy Profiles
- Al establecer la **Name** configuración de un nombre en **CSA-Compliance**
- Para configurar el **Condition**, haga clic en el botón +
- En **Condition Studio**, encontrará la información siguiente:

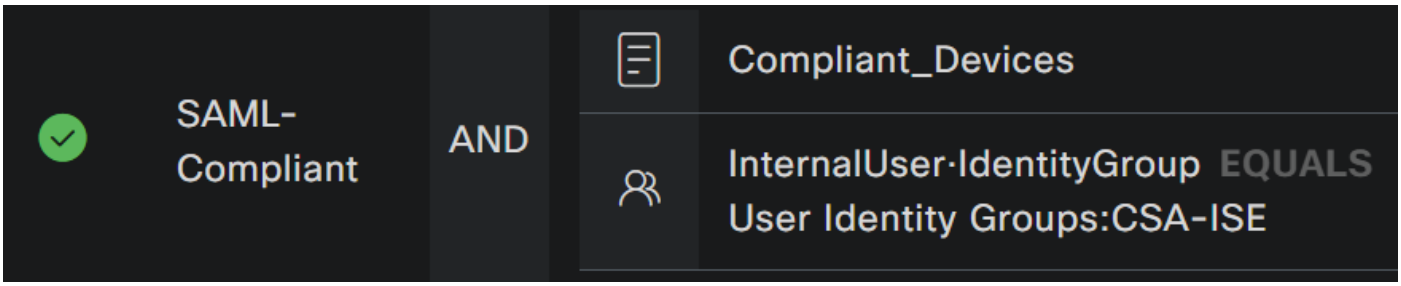



- Para crear la condición, busque **compliant**
- Usted debe haber mostrado Compliant_Devices
- Arrastre y suelte debajo del **Editor**

- Haga clic debajo del Editor botón en **New**
- Haga clic en el **Identity Group** icono
- Elegir **Internal User Identity Group**
- En **Equals**, elija el elemento **User Identity Group** que desee que coincida
- Haga clic en **Use**

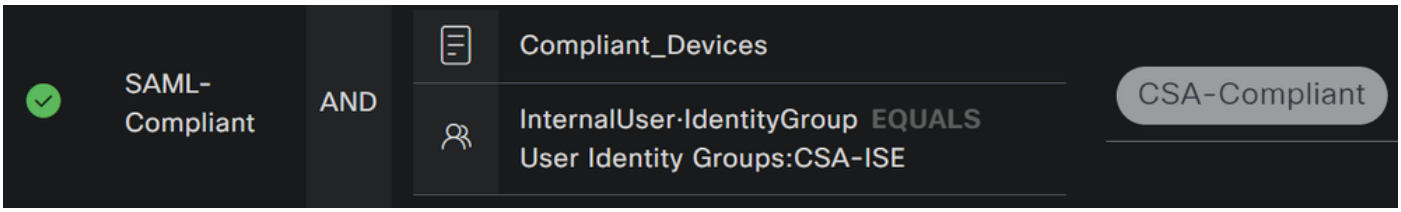



- Como resultado, tiene la siguiente imagen



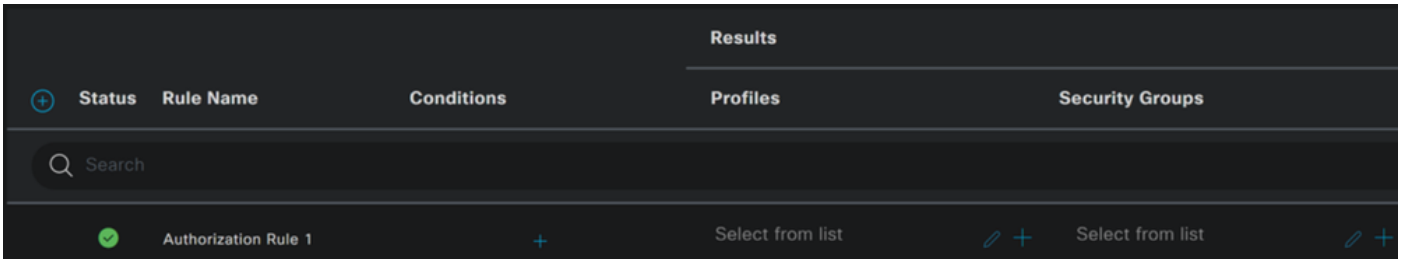

- En **Profile** haga clic en el botón desplegable y seleccione el perfil de autorización de queja configurado en el paso Perfil de

autorización conforme

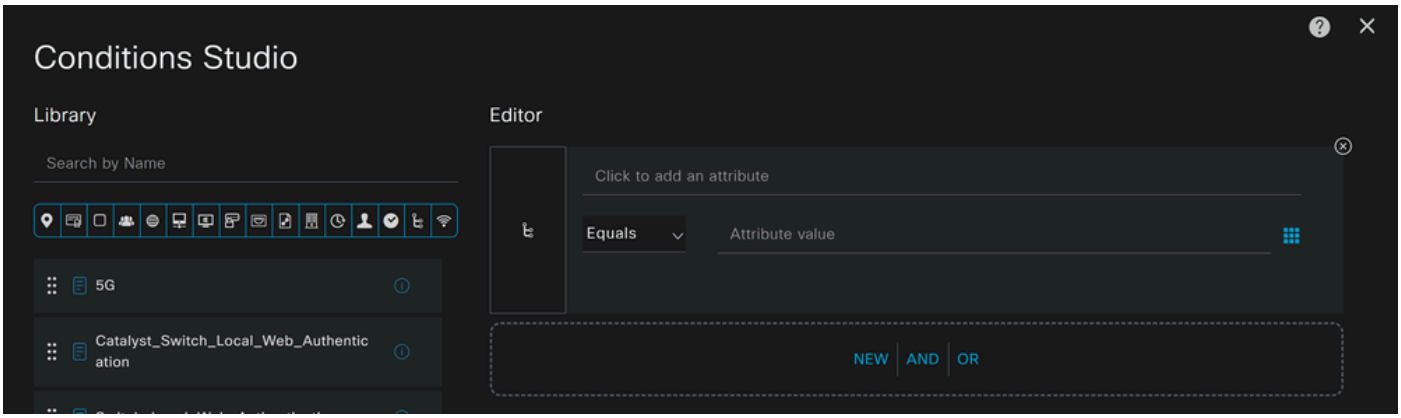



Ahora ya ha configurado el **Compliance Policy Set**.

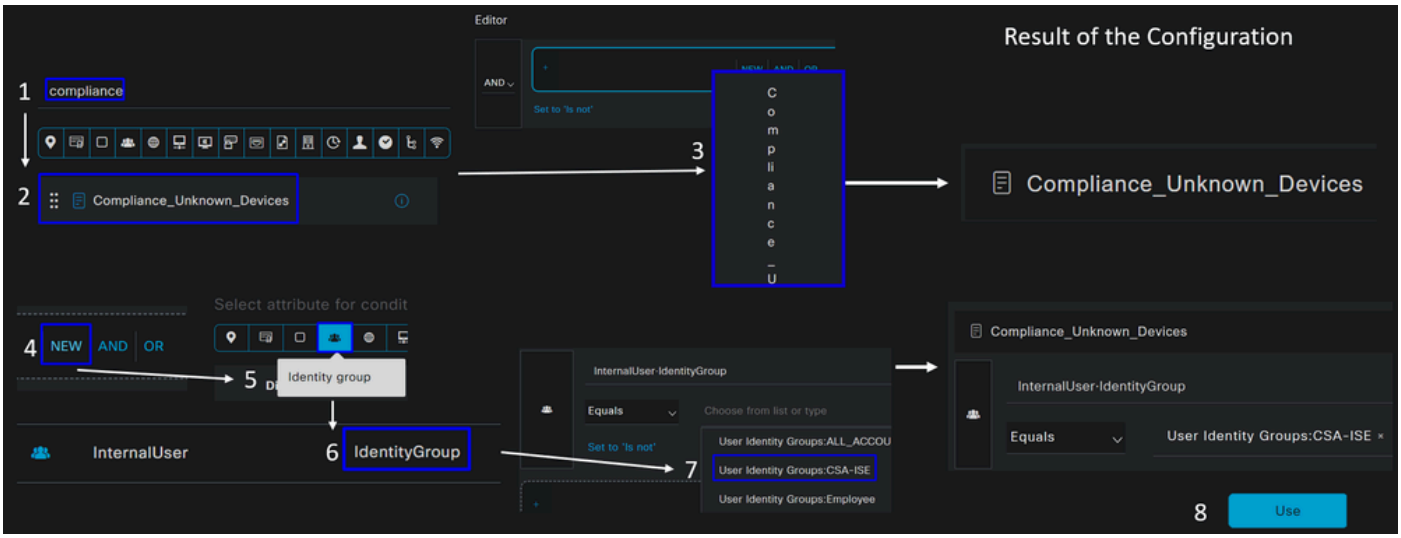
- Haga clic en + para definir la **CSA-Unknown-Compliance** política:



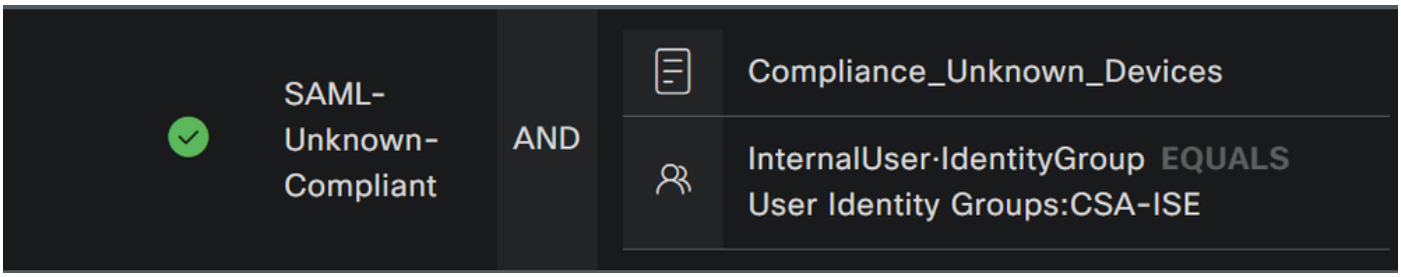

- Para el siguiente paso, cambie el Rule Name, Conditionsy Profiles
- Al establecer la **Name** configuración de un nombre en **CSA-Unknown-Compliance**
- Para configurar el **Condition**, haga clic en el botón +
- En **Condition Studio**, encontrará la información siguiente:



- Para crear la condición, busque **compliance**
- Usted debe haber mostrado Compliant_Unknown_Devices
- Arrastre y suelte debajo del **Editor**
- Haga clic debajo del Editor botón en **New**
- Haga clic en el **Identity Group** icono
- Elegir **Internal User Identity Group**
- En **Equals**, elija el elemento **User Identity Group** que desee que coincida
- Haga clic en **Use**

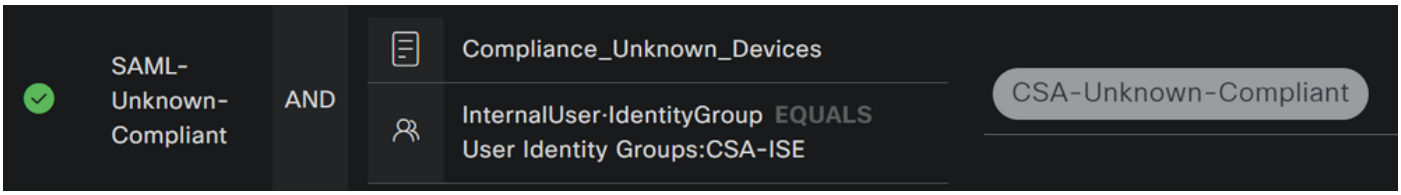



- Como resultado, tiene la siguiente imagen



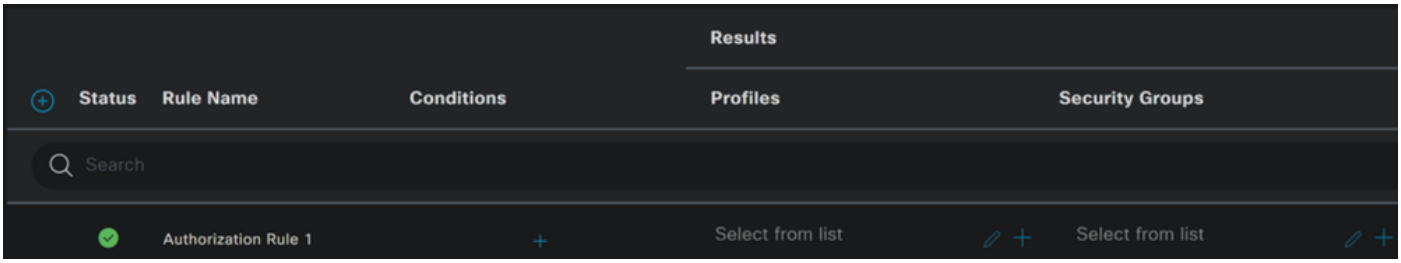

- En haga **Profile** clic en el botón desplegable y seleccione el perfil de autorización de quejas configurado en el paso Perfil de

autorización de conformidad desconocido

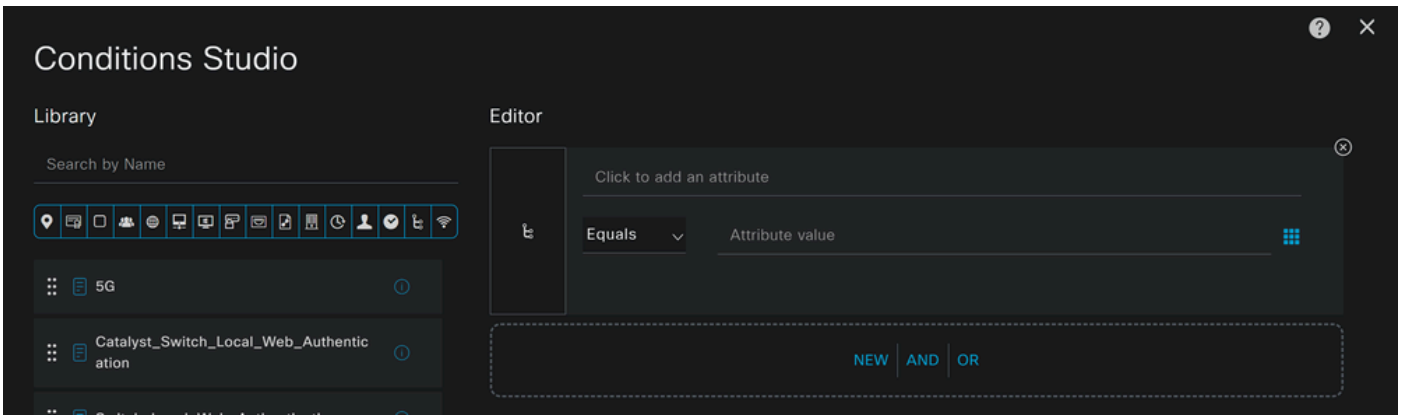



Ahora ya ha configurado el **Unknown Compliance Policy Set**.

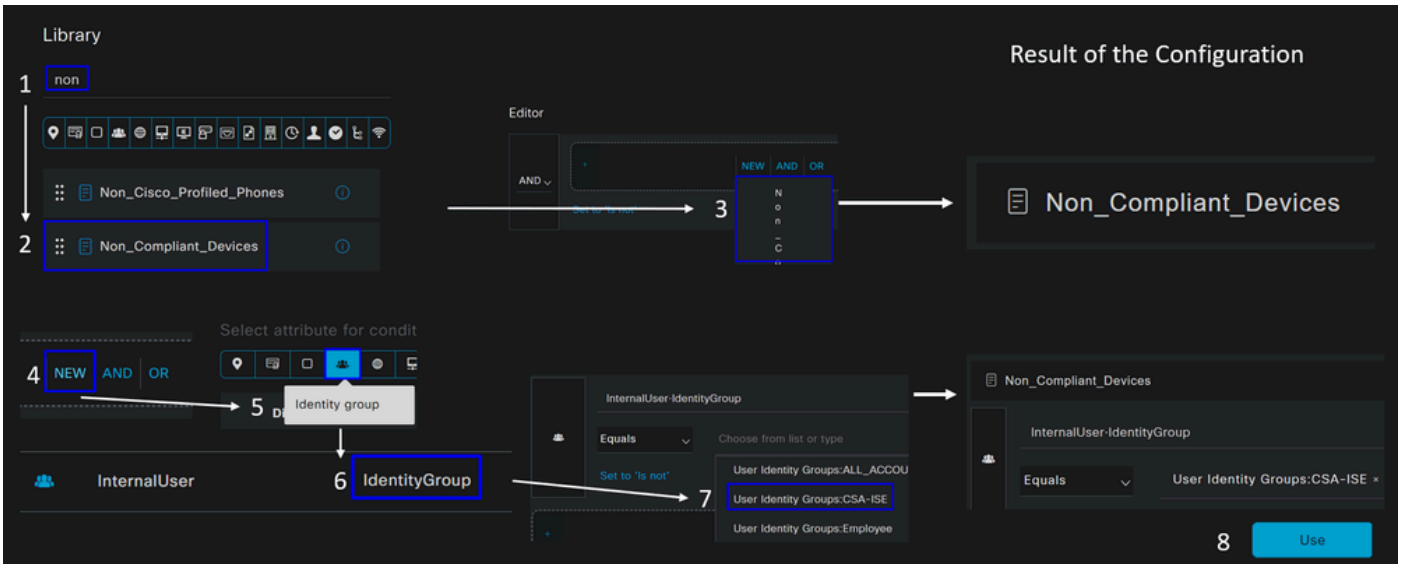
- Haga clic en **+** para definir la **CSA- Non-Compliant** política:



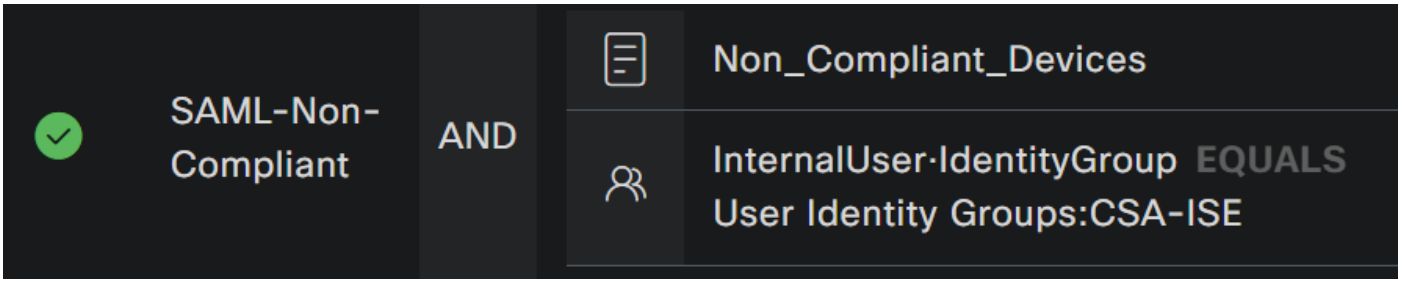

- Para el siguiente paso, cambie el Rule Name, Conditionsy Profiles
- Al establecer la **Name** configuración de un nombre en **CSA-Non-Compliance**
- Para configurar el **Condition**, haga clic en el botón +
- En **Condition Studio**, encontrará la información siguiente:



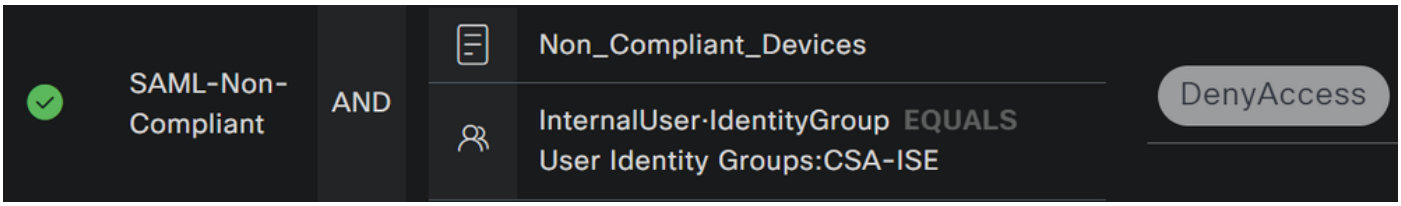
- Para crear la condición, busque **non**
- Usted debe haber mostrado Non_Compliant_Devices
- Arrastre y suelte debajo del **Editor**
- Haga clic debajo del Editor botón en **New**
- Haga clic en el **Identity Group** icono
- Elegir **Internal User Identity Group**
- En **Equals**, elija el elemento **User Identity Group** que desee que coincida
- Haga clic en **Use**




- Como resultado, tiene la siguiente imagen



- En haga **Profile** clic en el botón desplegable y seleccione el perfil de autorización de la queja **DenyAccess**




Una vez finalizada la configuración de los tres perfiles, estará listo para probar su integración con el estado.

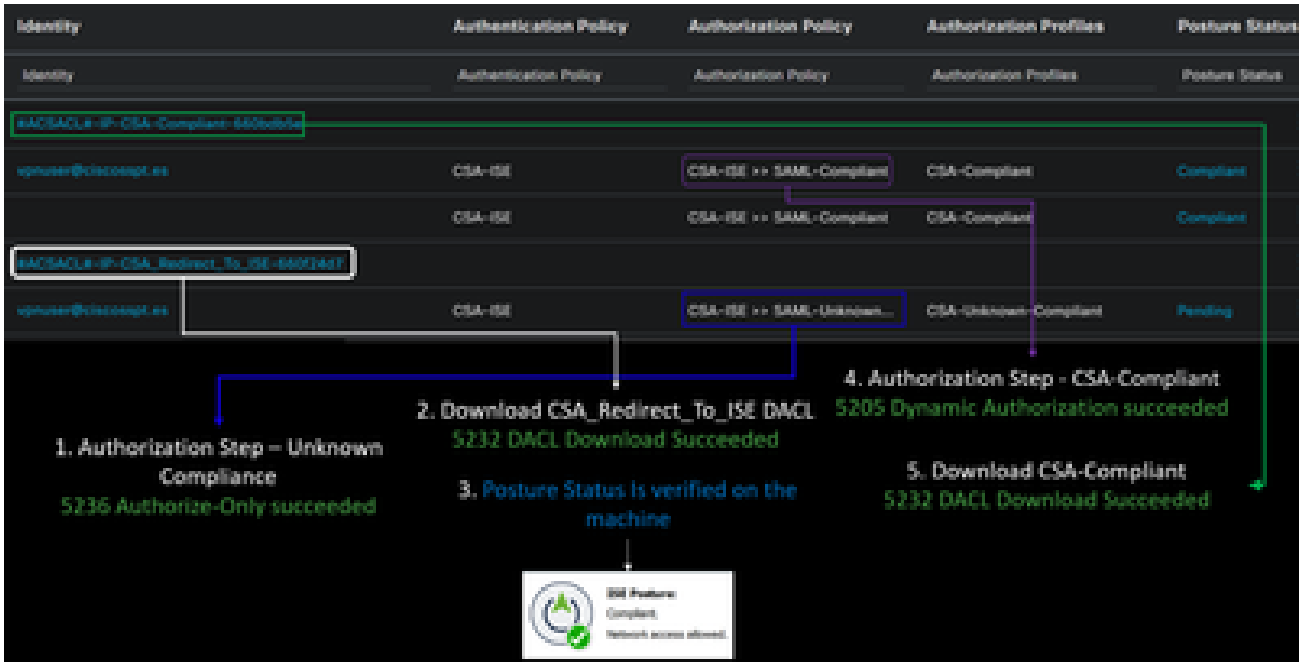
Verificación

Validación de estado

Conexión en el equipo

Conéctese al dominio FQDN RA-VPN proporcionado en Acceso seguro a través de Cliente seguro.

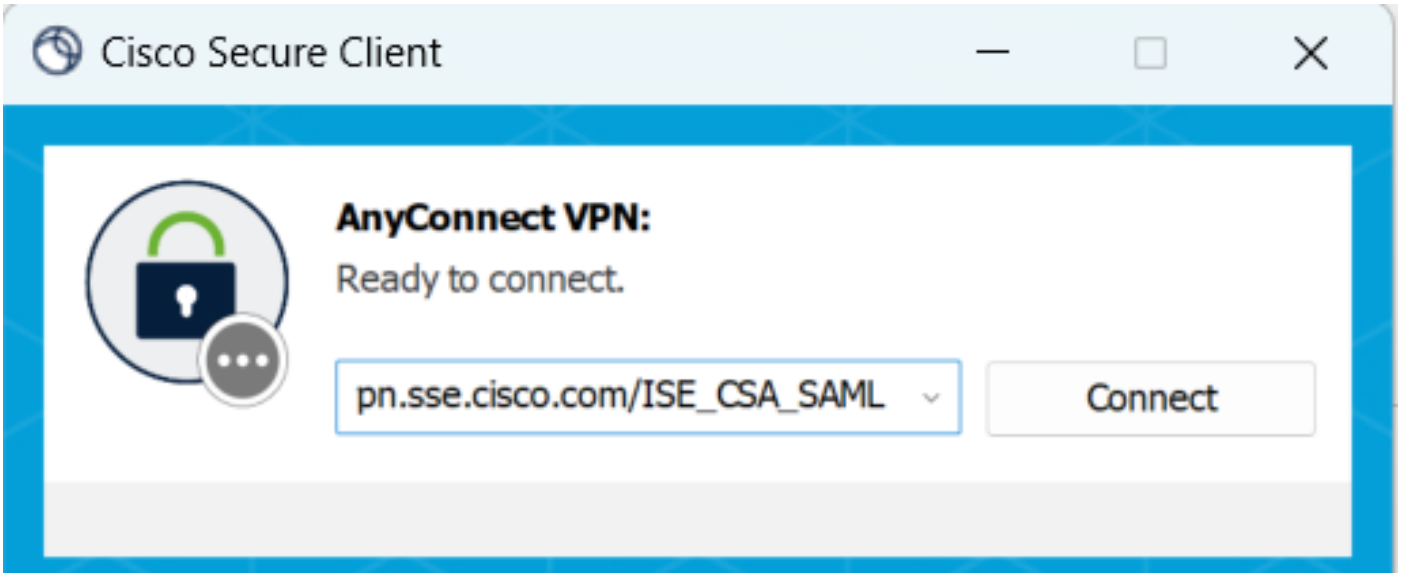
---



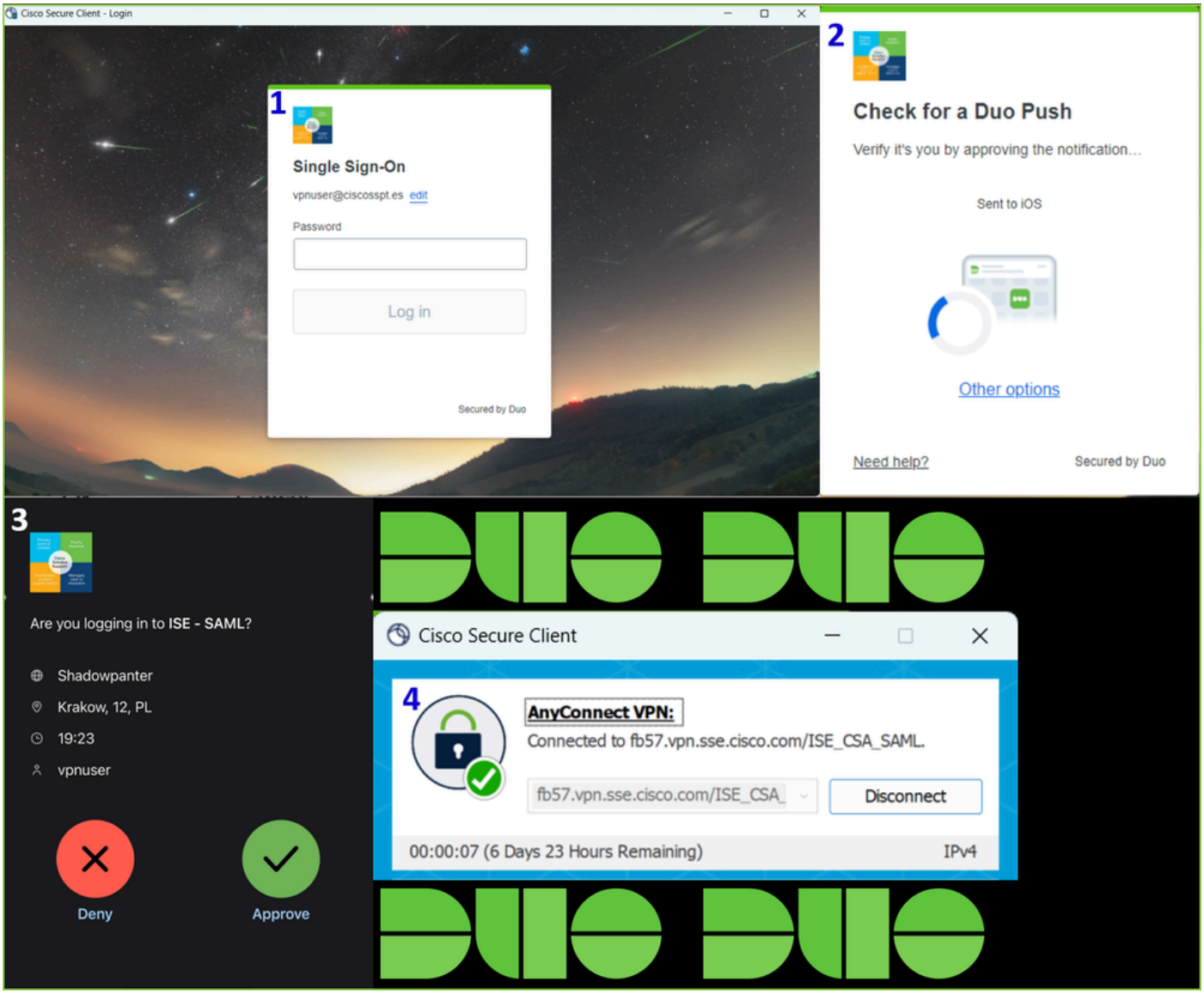

**Nota**: no se debe instalar ningún módulo ISE para este paso.

---

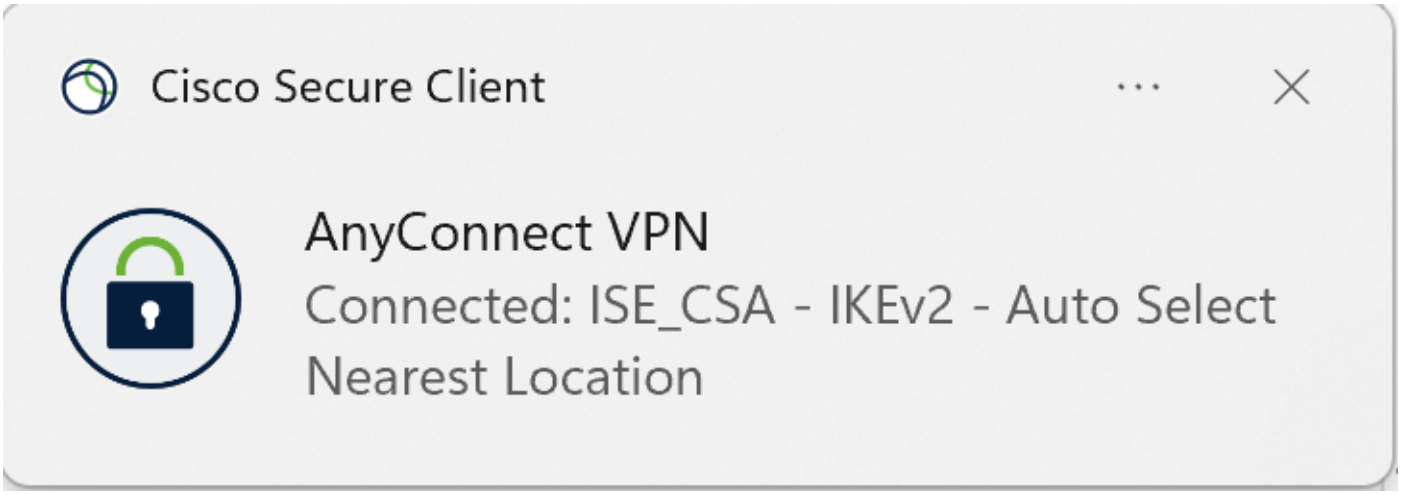
1. Conéctese mediante Secure Client.

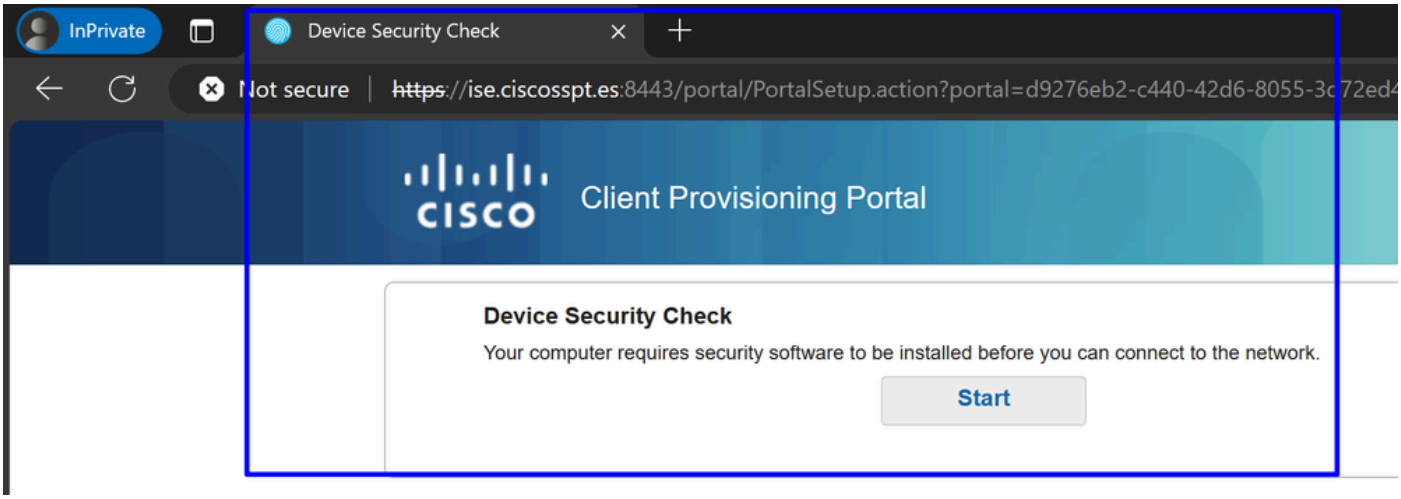



2. Proporcionar las credenciales para autenticarse a través de Duo.



3. En este momento, te conectas a la VPN y, probablemente, te redirigen a ISE; si no, puedes intentar navegar hasta **http:1.1.1.1**.

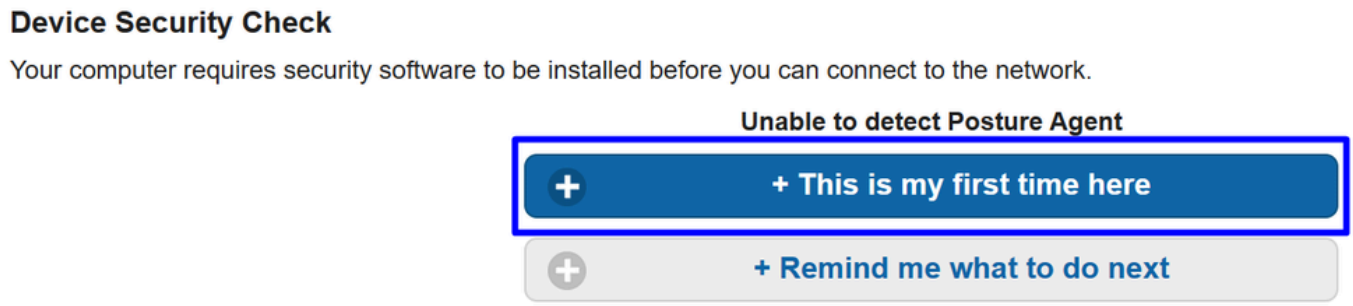


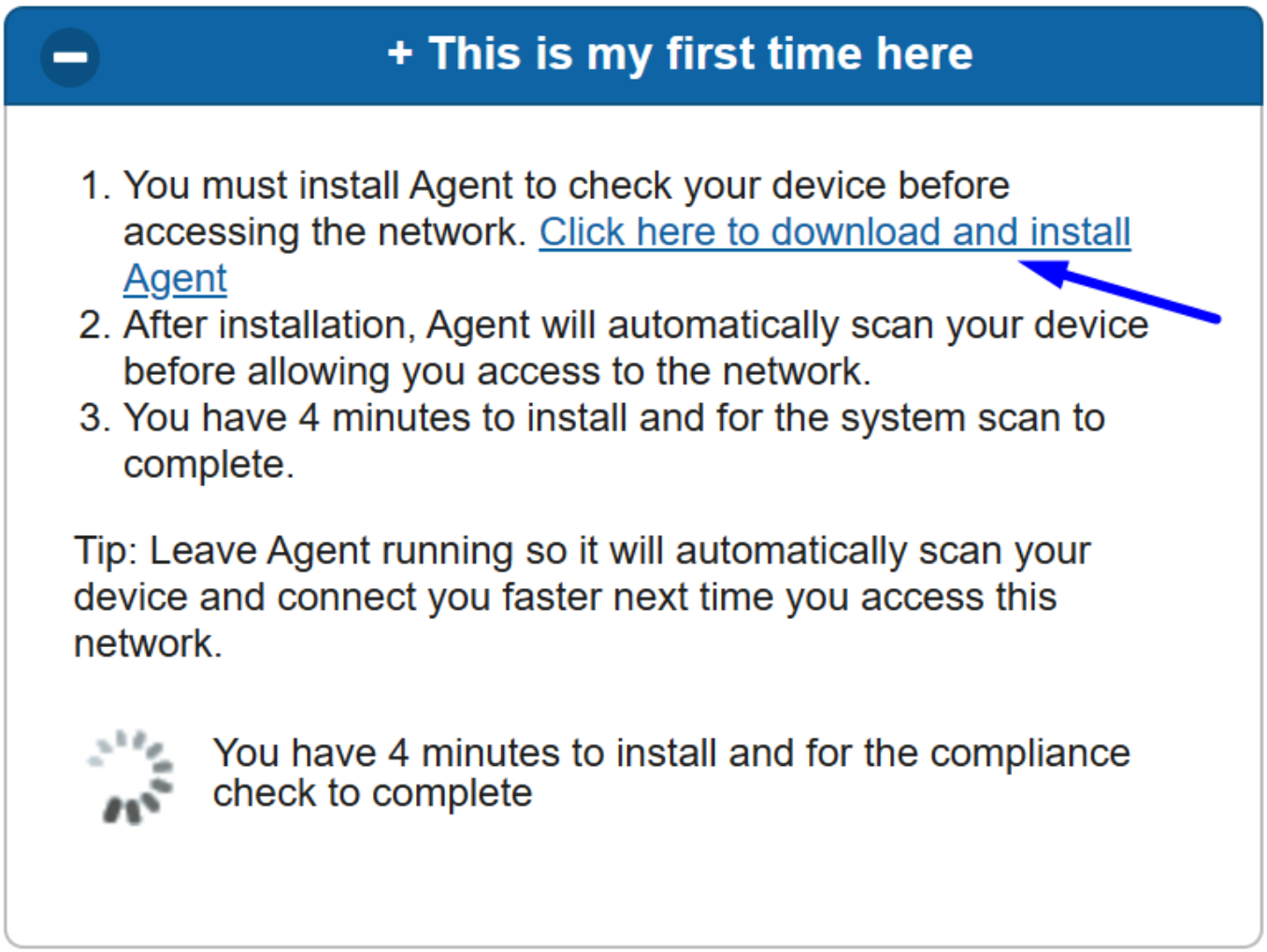
**Nota**: en este momento se encuentra en el grupo de políticas de autorización CSA-Unknown-Compliance porque no tiene el agente de estado de ISE instalado en el equipo y se le redirige al portal de aprovisionamiento de ISE para instalar el agente.

4. Haga clic en Iniciar para continuar con el aprovisionamiento de agentes.

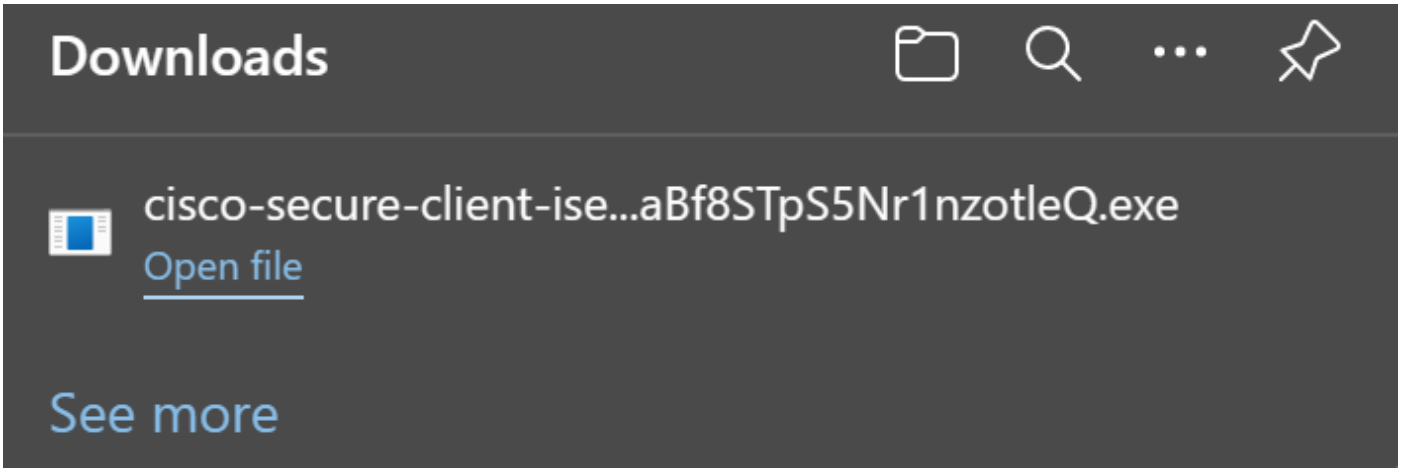

5. Haga clic en **+ This is my first time here**.

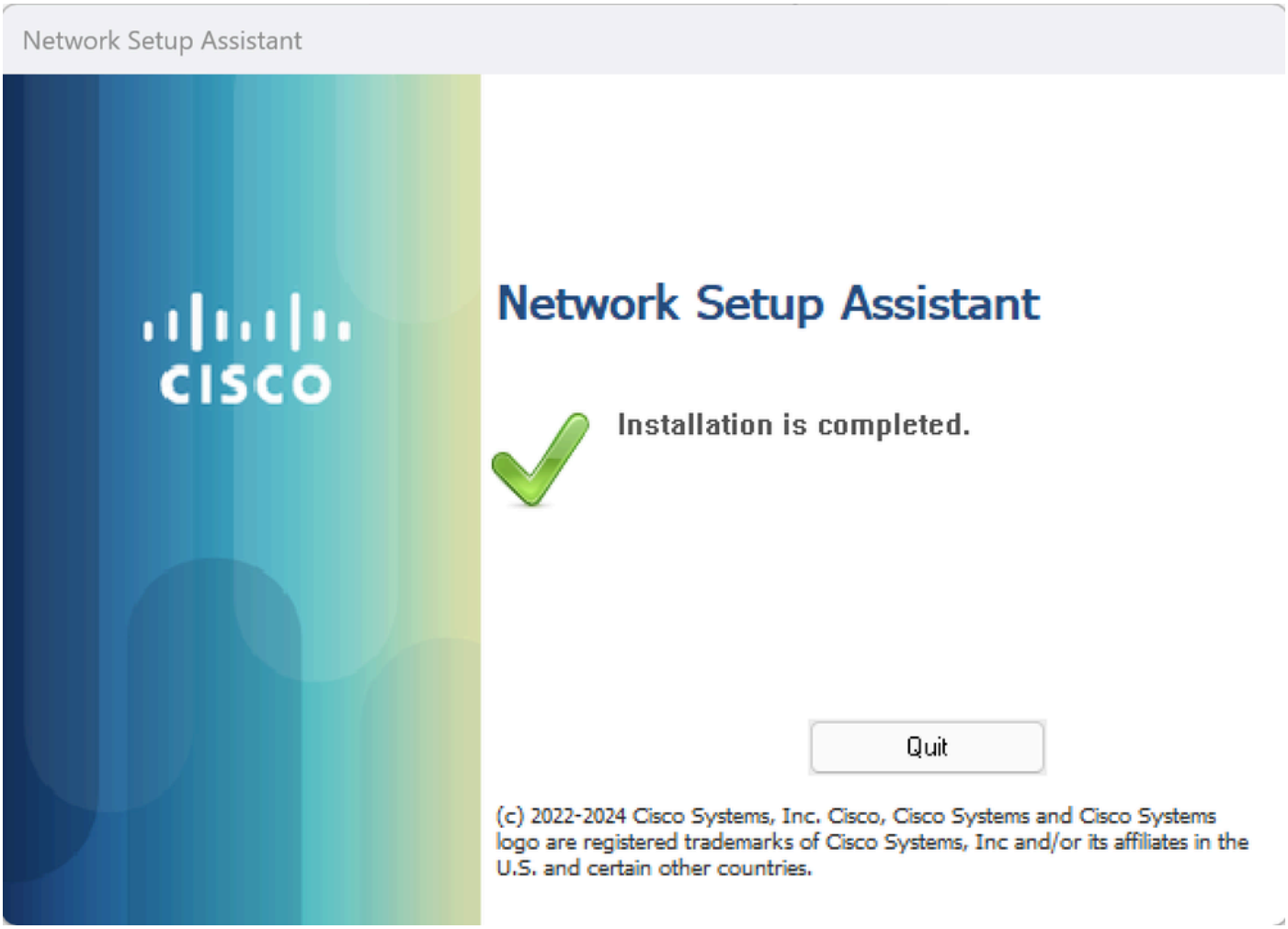



6. Haga clic en **Click here to download and install agent**

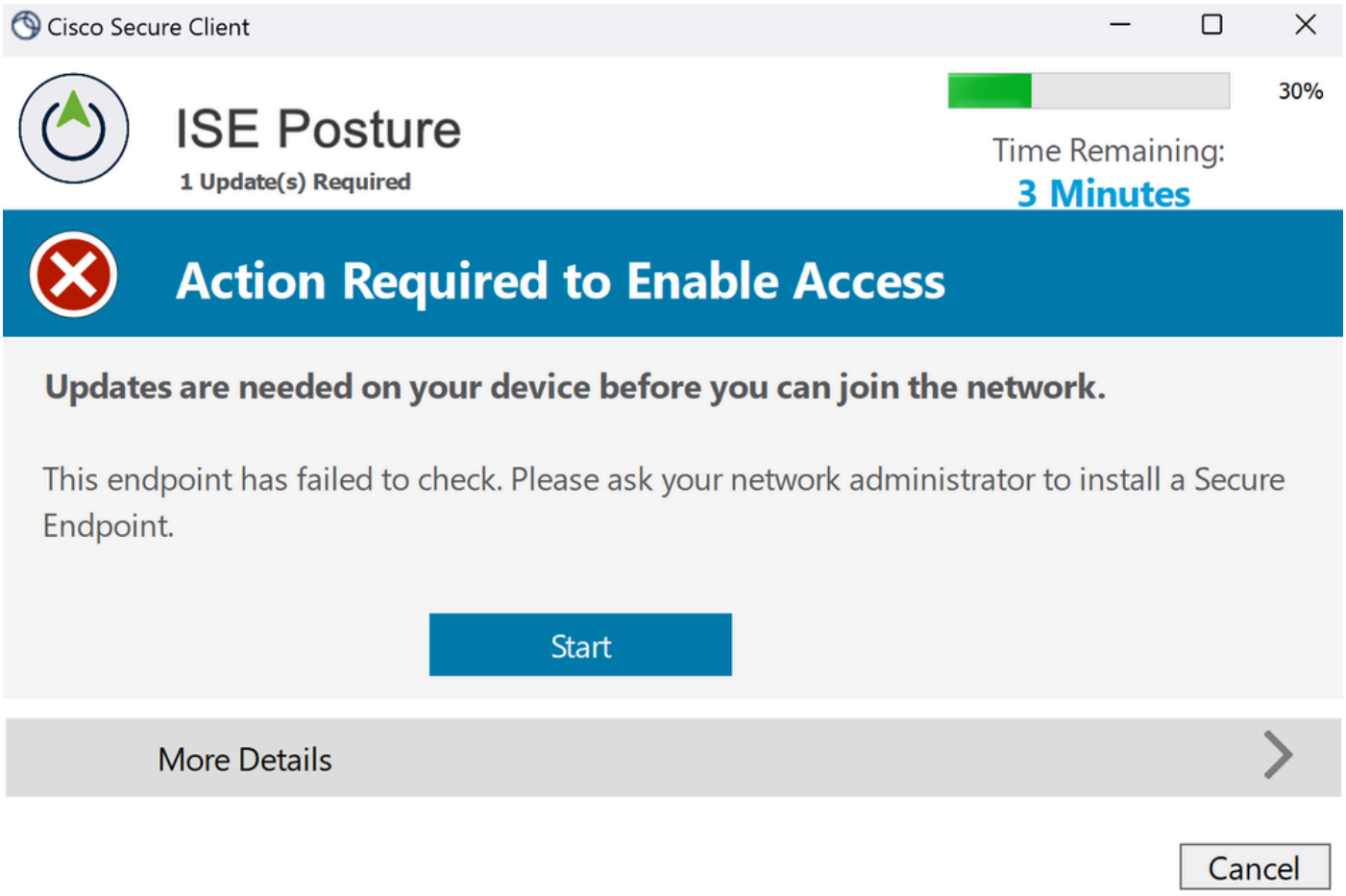


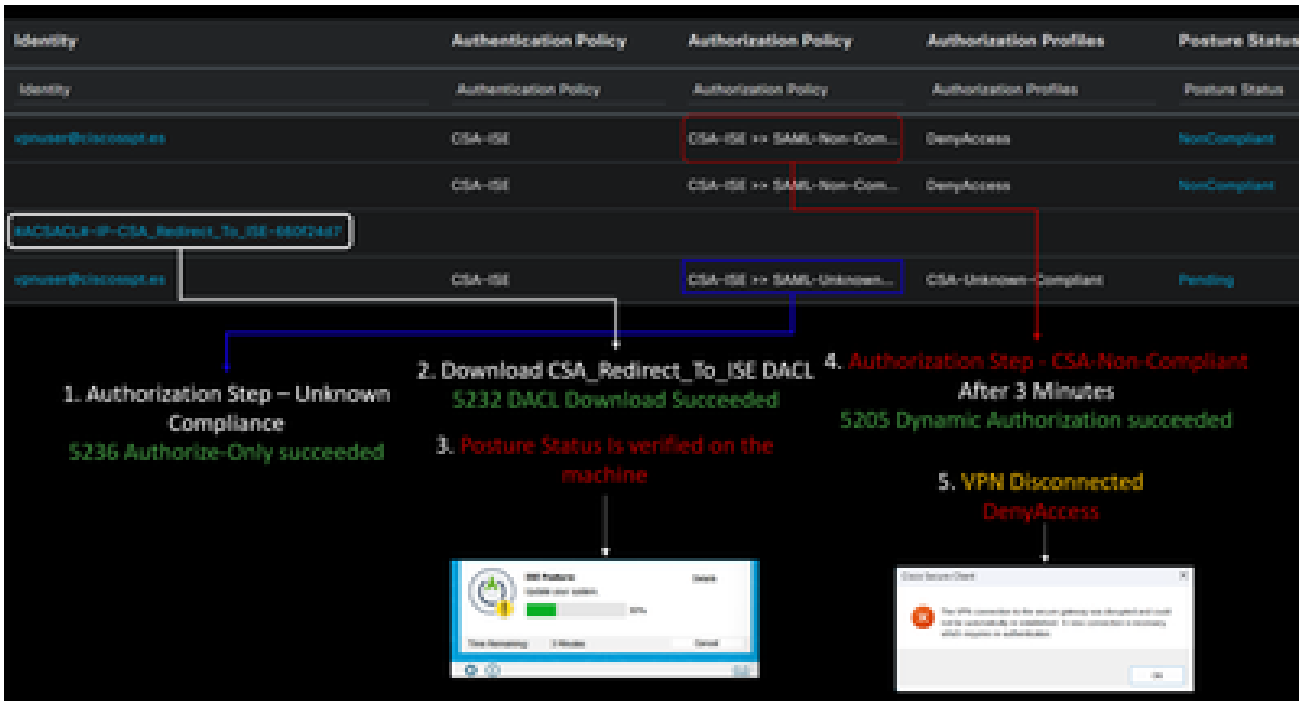

7. Instale el agente



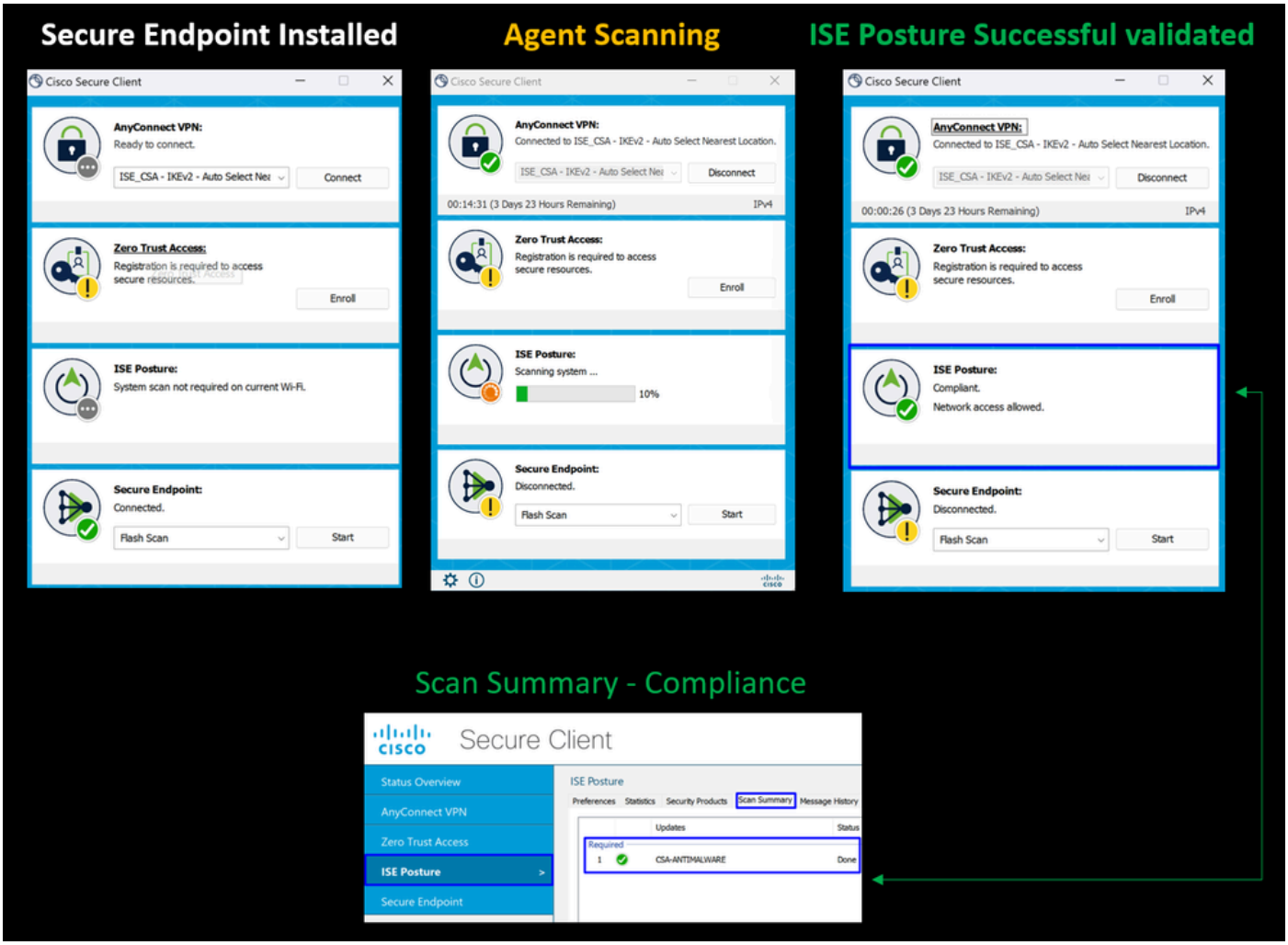

8. Después de instalar el agente, el estado de ISE comienza a verificar el estado actual de las máquinas. Si no se cumplen los requisitos de la política, aparecerá una ventana emergente que le guiará hacia el cumplimiento.


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

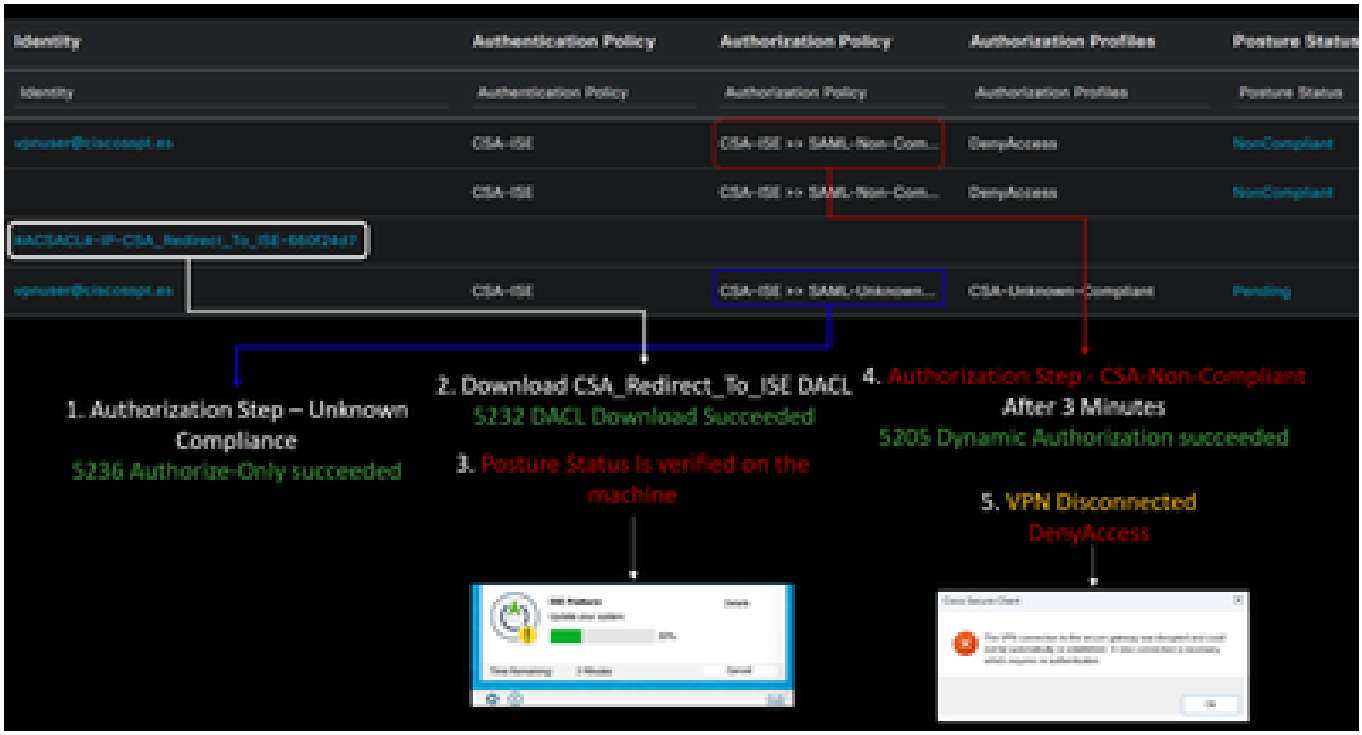

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE 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

**Nota**: Si Cancel usted o el tiempo restante finaliza, automáticamente se convierte en no conforme, cae bajo la política de autorización establecida como CSA-Non-Compliance**, e inmediatamente se desconecta de la VPN.**

9. Instale Secure Endpoint Agent y conéctese de nuevo a la VPN.




10. Una vez que el agente verifica que la máquina cumple los requisitos, su estado cambia para estar al día de la reclamación y dar acceso a todos los recursos de la red.



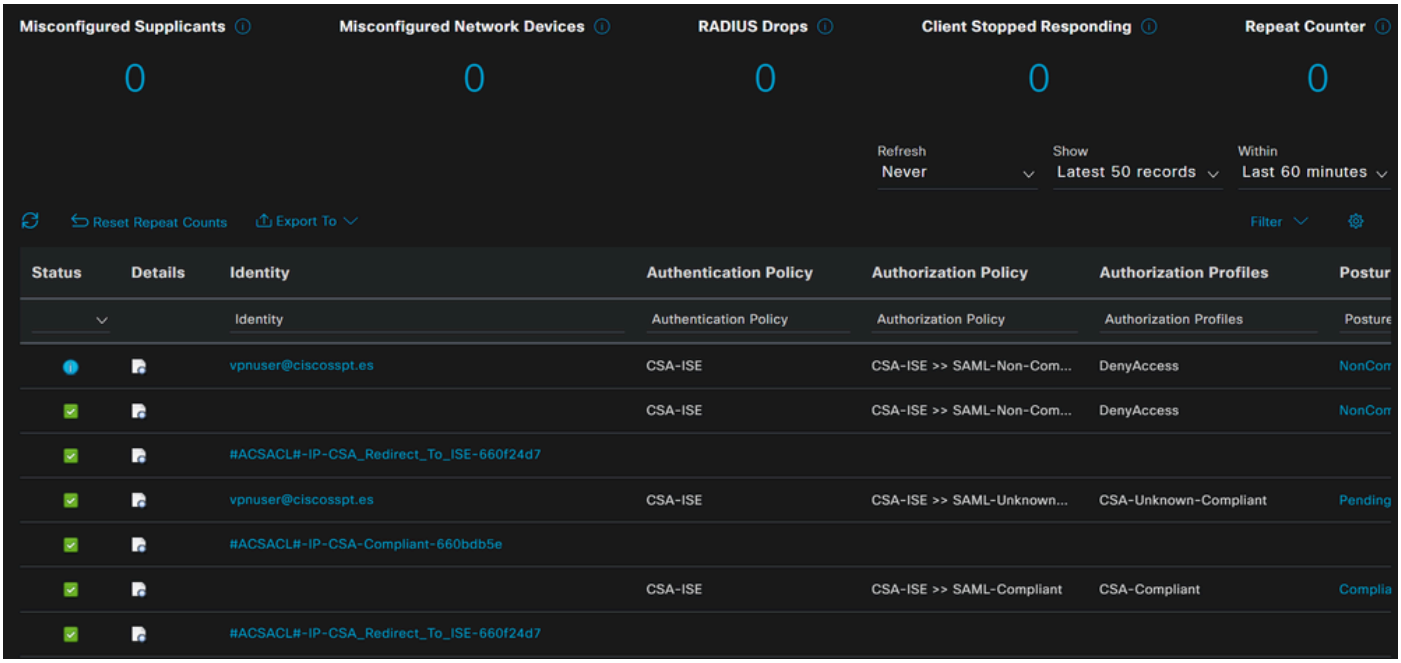

**Nota**: una vez que cumpla los requisitos, quedará incluido en el conjunto de políticas de autorización CSA-Compliance y tendrá acceso inmediatamente a todos los recursos de red.

---

Cómo verificar los registros en ISE

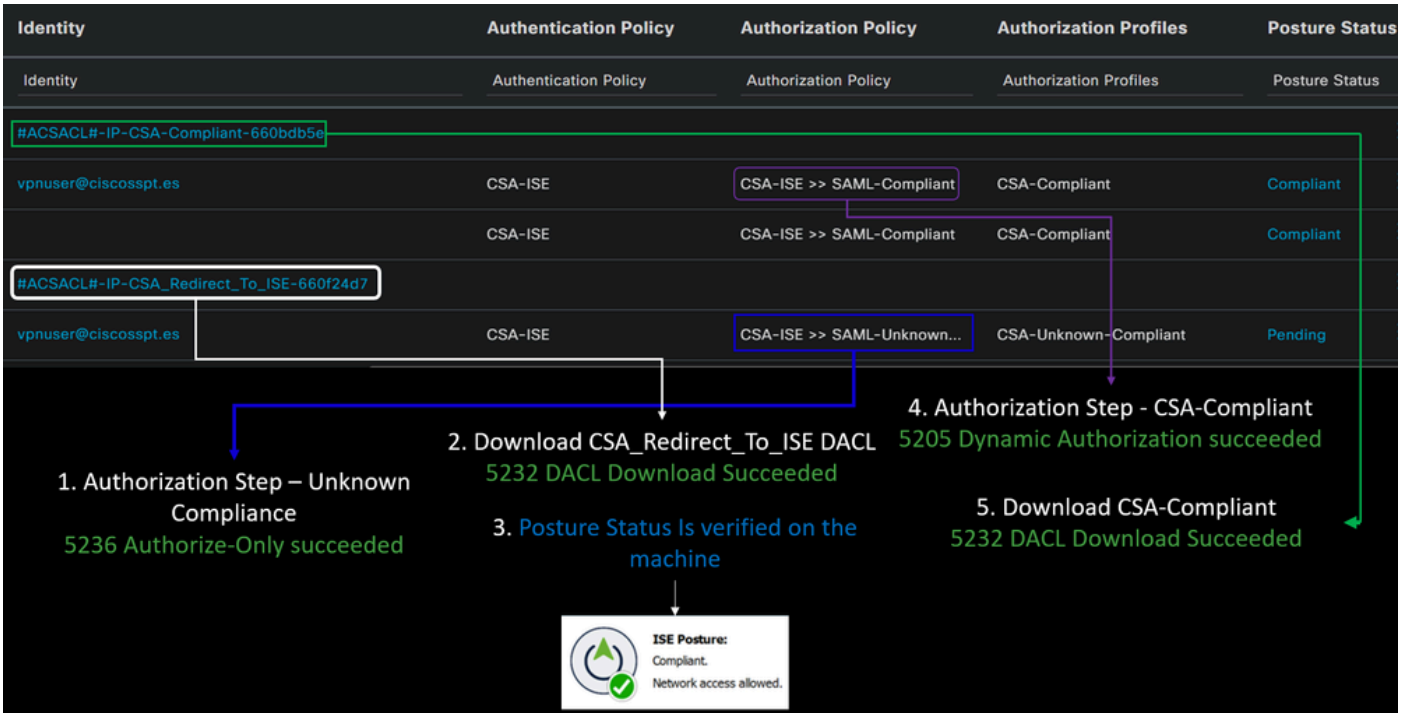
Para comprobar el resultado de la autenticación de un usuario, tiene dos ejemplos de conformidad e incumplimiento. Para revisarlo en ISE, siga estas instrucciones:

- Vaya a su panel de ISE
- Haga clic en Operations > Live Logs

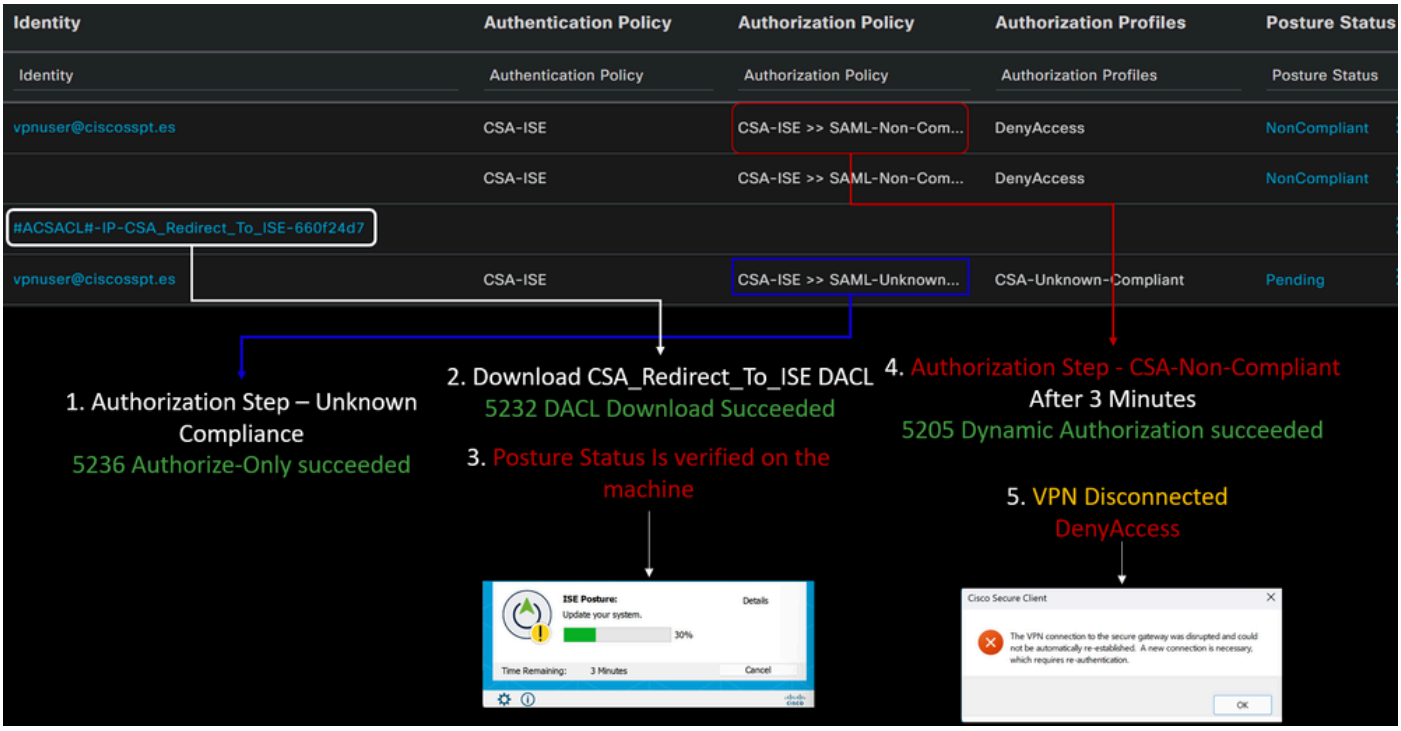



El siguiente escenario tho muestra cómo se muestran los eventos de cumplimiento e incumplimiento con éxito en **Live Logs**:

Conformidad




Incumplimiento



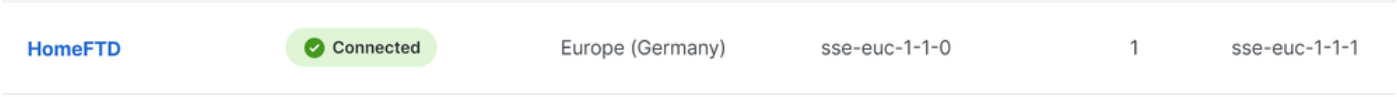

Primeros pasos con acceso seguro e integración con ISE

En el siguiente ejemplo, Cisco ISE se encuentra en la red 192.168.10.0/24, y la configuración de las redes a las que se puede acceder a través del túnel debe agregarse en la configuración del túnel.

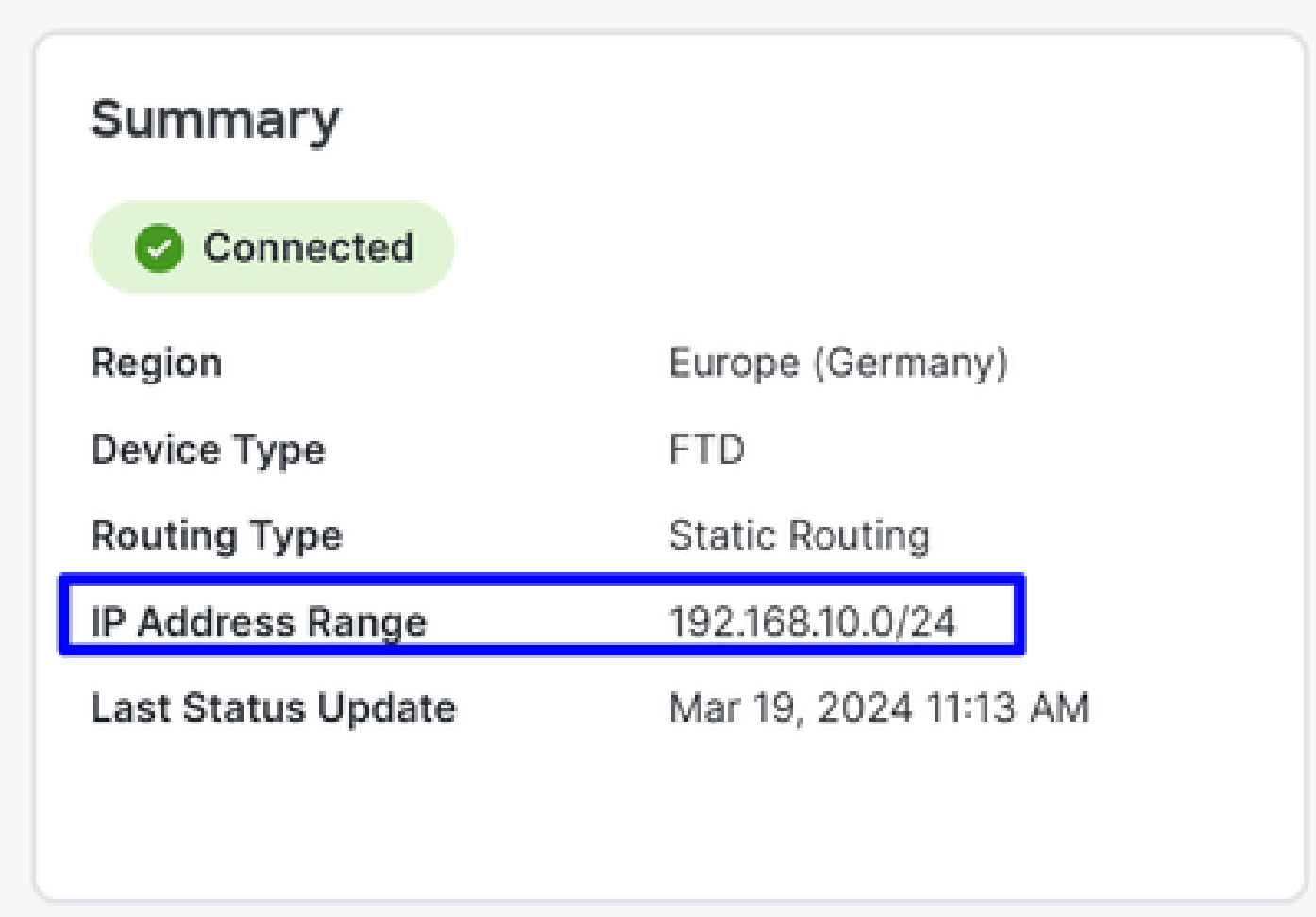
**Step 1**: Compruebe la configuración del túnel:

Para verificarlo, navegue hasta el [panel de acceso seguro](#).

- Haga clic en **Connect > Network Connections**
- Haga clic en **Network Tunnel Groups** > Su túnel




- En summary (Resumen), verifique que el túnel haya configurado el espacio de direcciones donde se encuentra Cisco ISE:

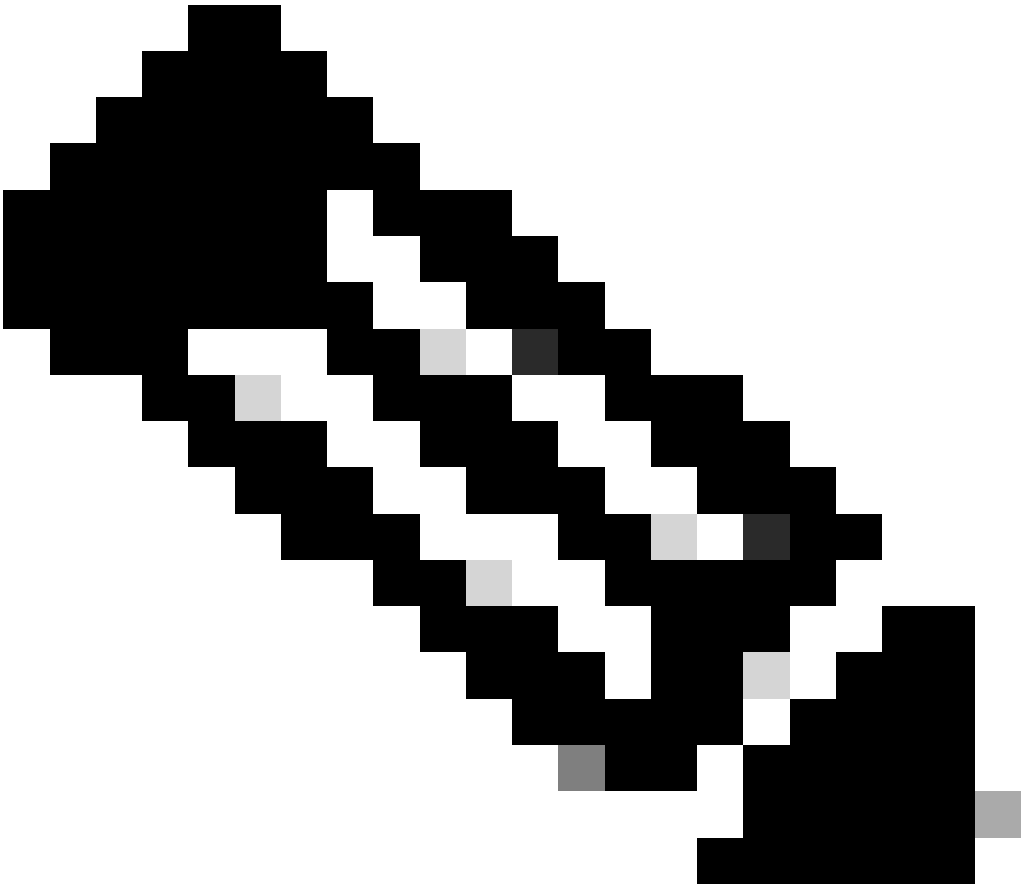



**Step 2**: permite el tráfico en el firewall.

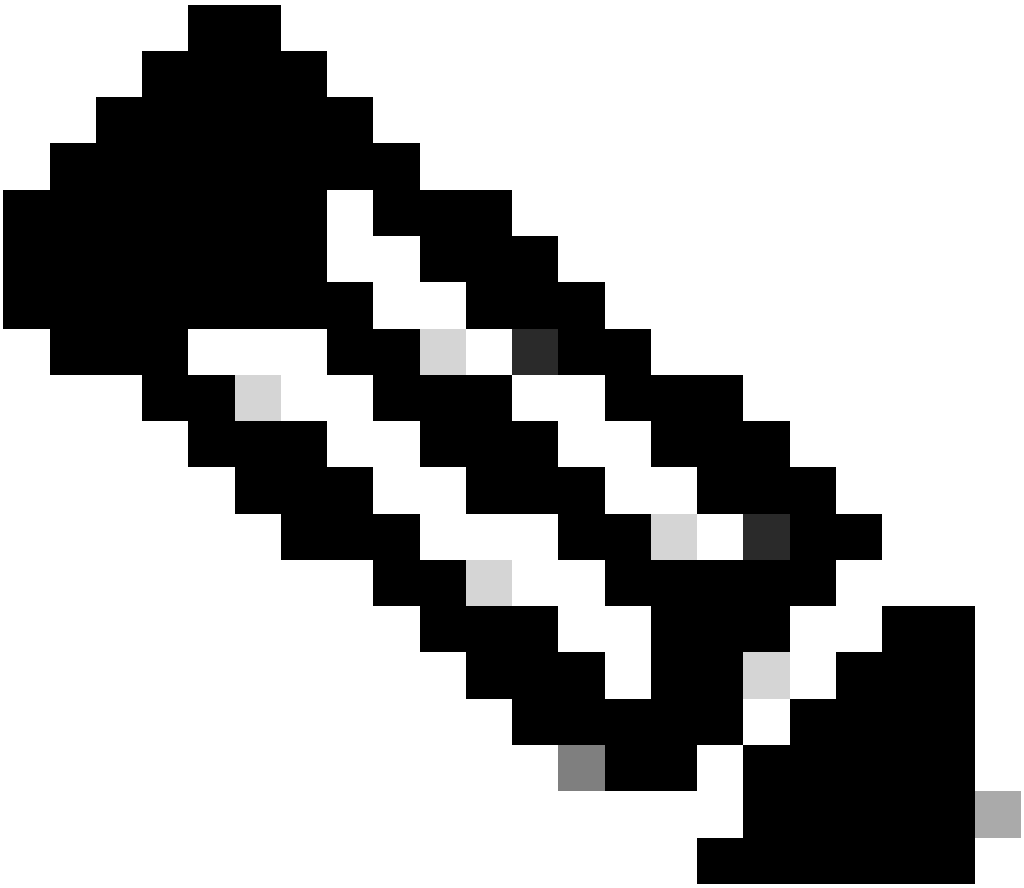
Para permitir que Secure Access utilice el dispositivo ISE para la autenticación Radius, debe haber configurado una regla de Secure Access en la red con los puertos Radius necesarios:

| Regla | Fuente | Destino | Puerto de Destino |
|---|---|---|---|
| **ISE para proteger el acceso**<br><br>**Grupo de gestión** | Servidor_ISE | Grupo de IP de gestión (RA-VPN) | **COA**<br><br>UDP 1700 (puerto predeterminado) |
| **Gestión de acceso seguro Grupo de IP a ISE** | Grupo IP de administración | Servidor_ISE | **Autenticación, autorización**<br><br>UDP 1812 (puerto predeterminado)<br><br>**Contabilidad**<br><br>UDP 1813 (puerto predeterminado) |
| **Conjunto IP de terminales de acceso seguro a ISE** | Conjunto IP de terminales | Servidor_ISE | **Portal de aprovisionamiento**<br><br>TCP 8443 (puerto predeterminado) |
| | | | |

| | | | |
|---|---|---|---|
| **Conjunto IP de terminales de acceso seguro al SERVIDOR DNS** | Conjunto IP de terminales | Servidor DNS | **DNS**<br><br>UDP y TCP 53 |



**Nota**: Si desea conocer más puertos relacionados con ISE, consulte la Guía del usuario - Referencia de puertos.



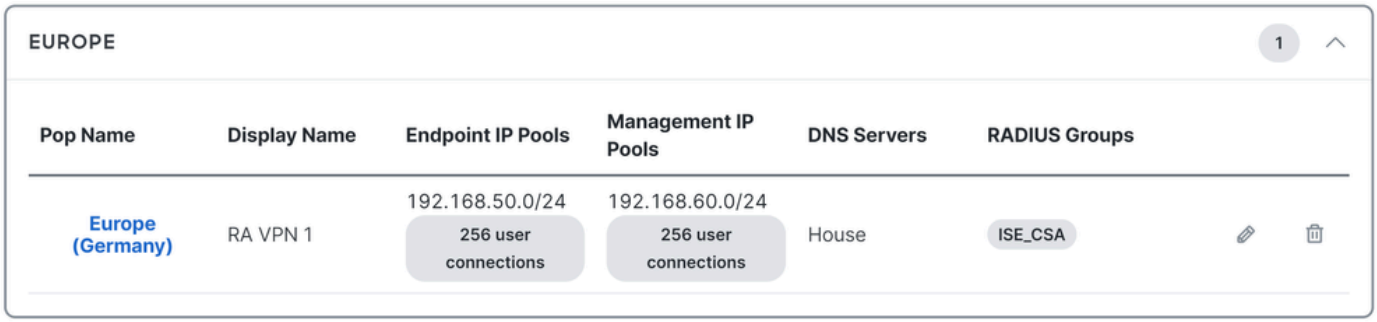
**Nota**: se necesita una regla DNS si ha configurado ISE para que se detecte mediante un nombre, como ise.ciscosspt.es

**Grupos IP de terminales y grupos de gestión**

Para verificar el grupo IP de administración y de terminales, navegue hasta el panel de acceso seguro:

- Haga clic en **Connect > End User Connectivity**
- Haga clic en Virtual Private Network
- Debajo **Manage IP Pools**

- Haga clic en **Manage**

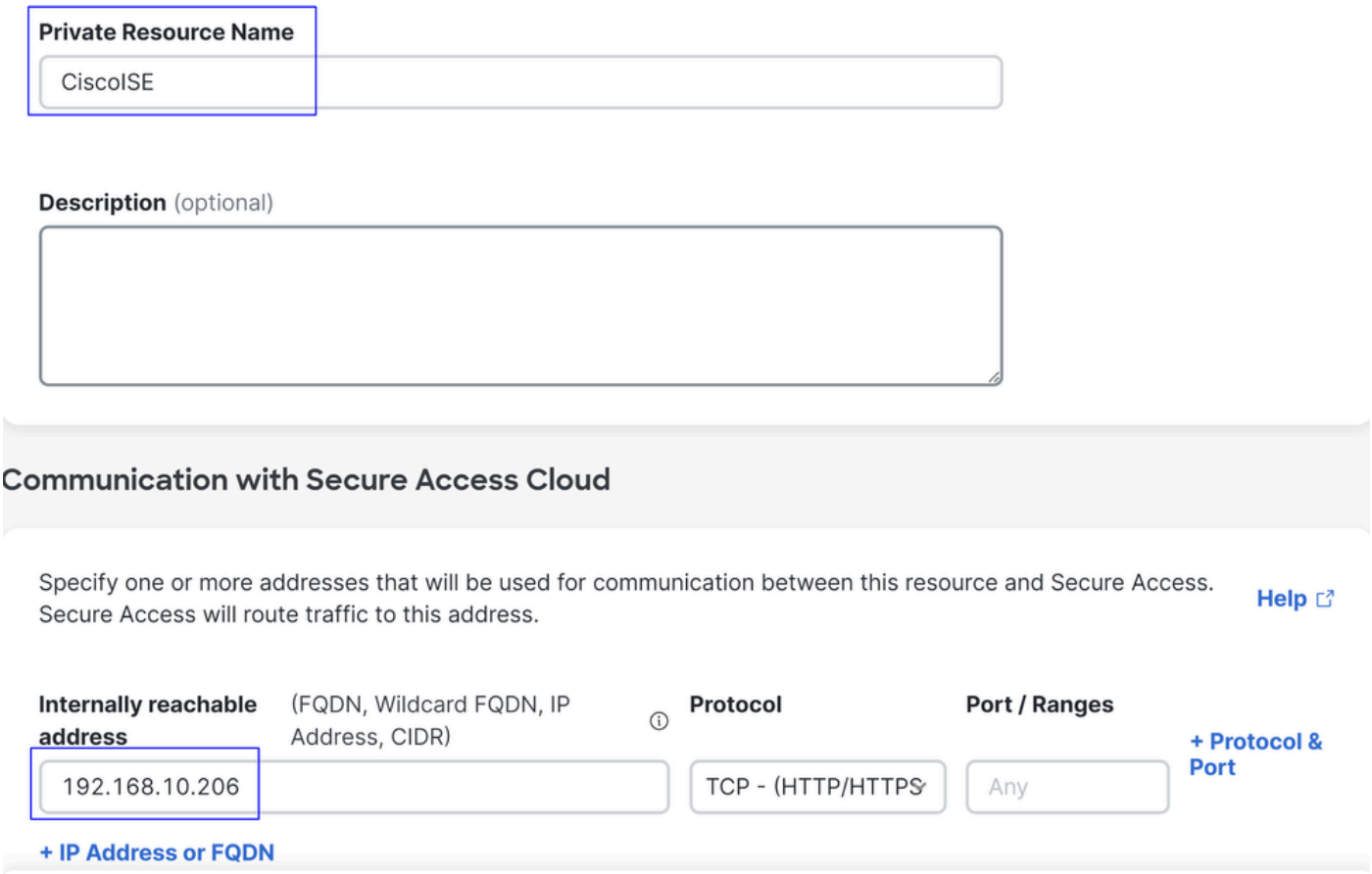


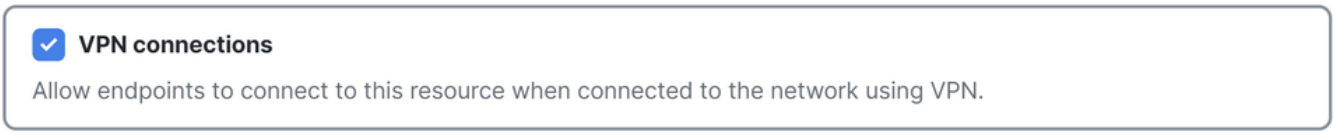

**Paso 3**: Compruebe que ISE está configurado en Recursos privados

Para permitir que los usuarios conectados a través de la VPN accedan a **ISE Provisioning Portal**, debe asegurarse de que ha configurado el dispositivo como un recurso privado para proporcionar acceso, que se utiliza para permitir el aprovisionamiento automático de la red ISE Posture Module a través de la VPN.

Para verificar que ISE está configurado correctamente, navegue hasta el panel de acceso seguro:

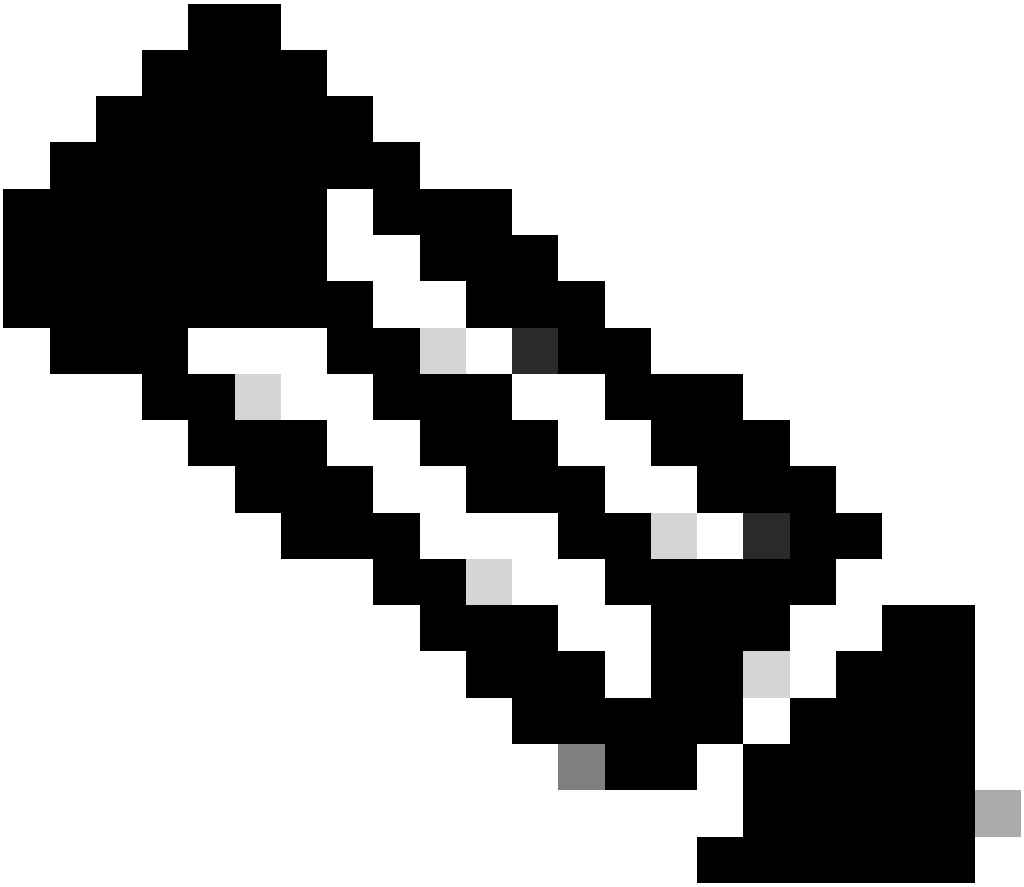
- Haga clic en **Resources** > **Private Resources**
- Haga clic en el recurso de ISE






Si es necesario, puede restringir la regla al puerto del portal de aprovisionamiento (8443).

---



**Nota**: Asegúrese de que ha marcado la casilla de verificación de las conexiones VPN.

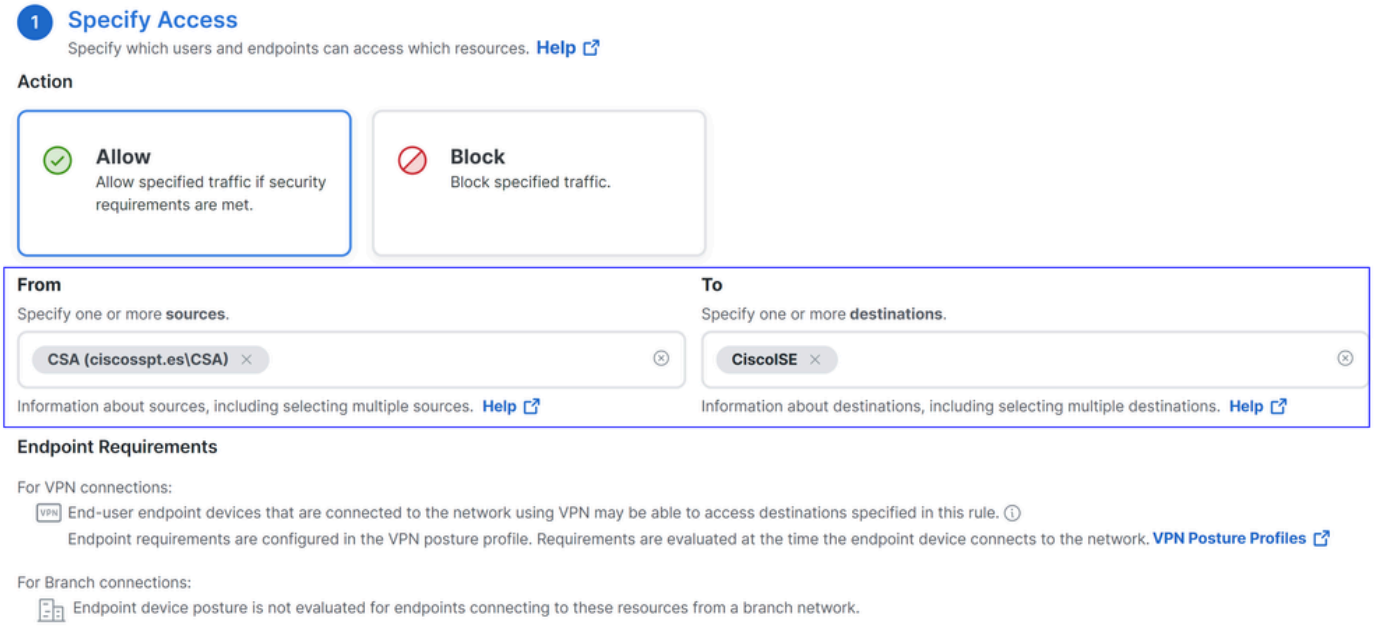
---

**Paso 4**: Permitir el acceso a ISE en la política de acceso

Para permitir que los usuarios conectados a través de la VPN se desplacen a **ISE Provisioning Portal**, debe asegurarse de que ha configurado un para permitir **Access Policy** que los usuarios configurados bajo esa regla accedan al recurso privado configurado en Step3.

Para verificar que ISE está configurado correctamente, navegue hasta el panel de acceso seguro:

- Haga clic en **Secure > Access Policy**
- Haga clic en la regla configurada para permitir el acceso de los usuarios VPN a ISE

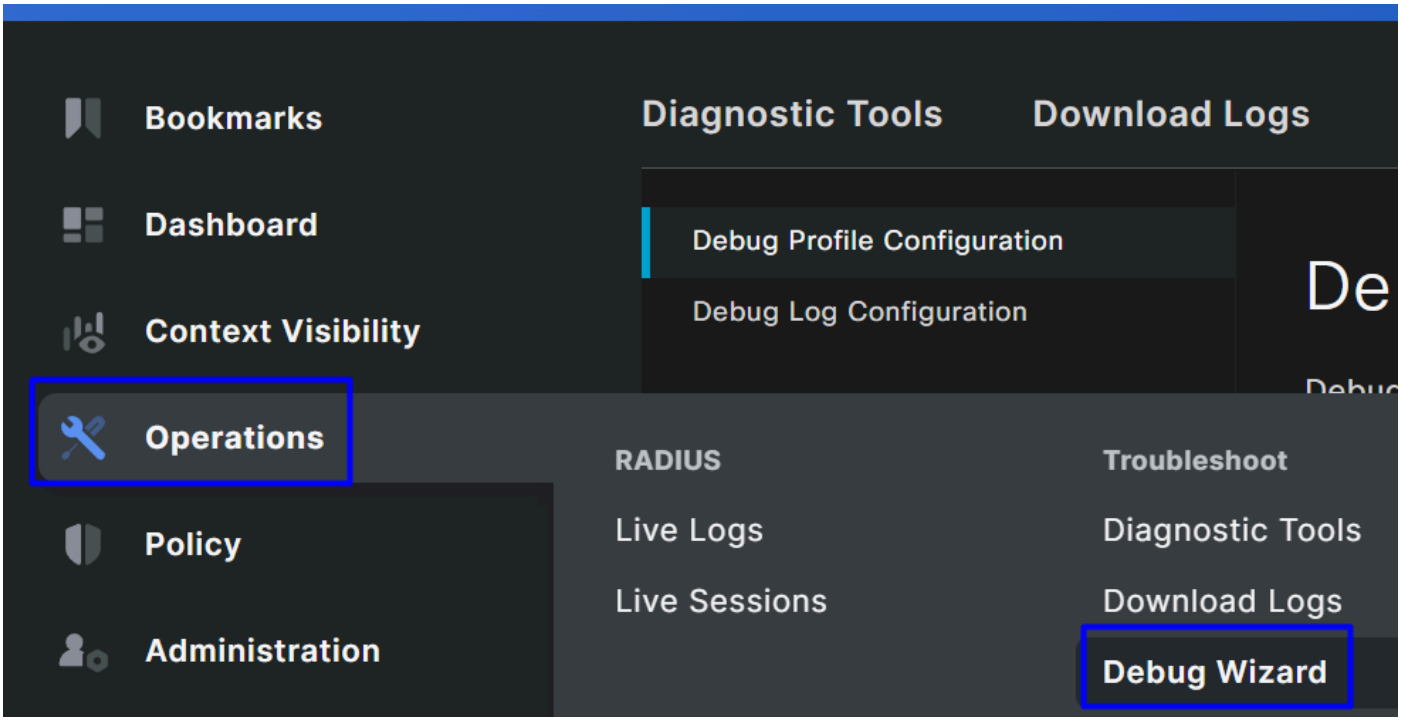



Troubleshoot

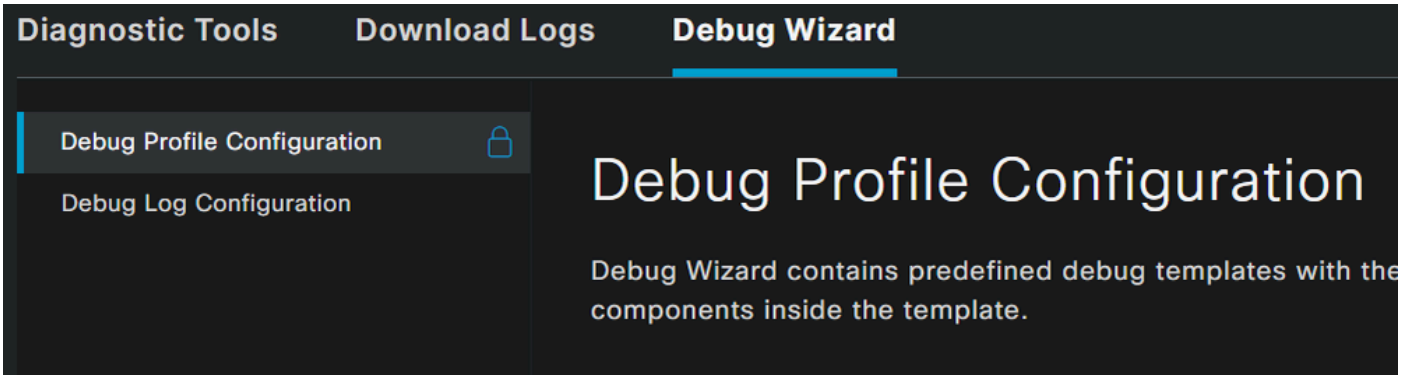
Cómo descargar registros de depuración de estado de ISE

Para descargar registros de ISE para verificar un problema relacionado con el estado, continúe con los siguientes pasos:

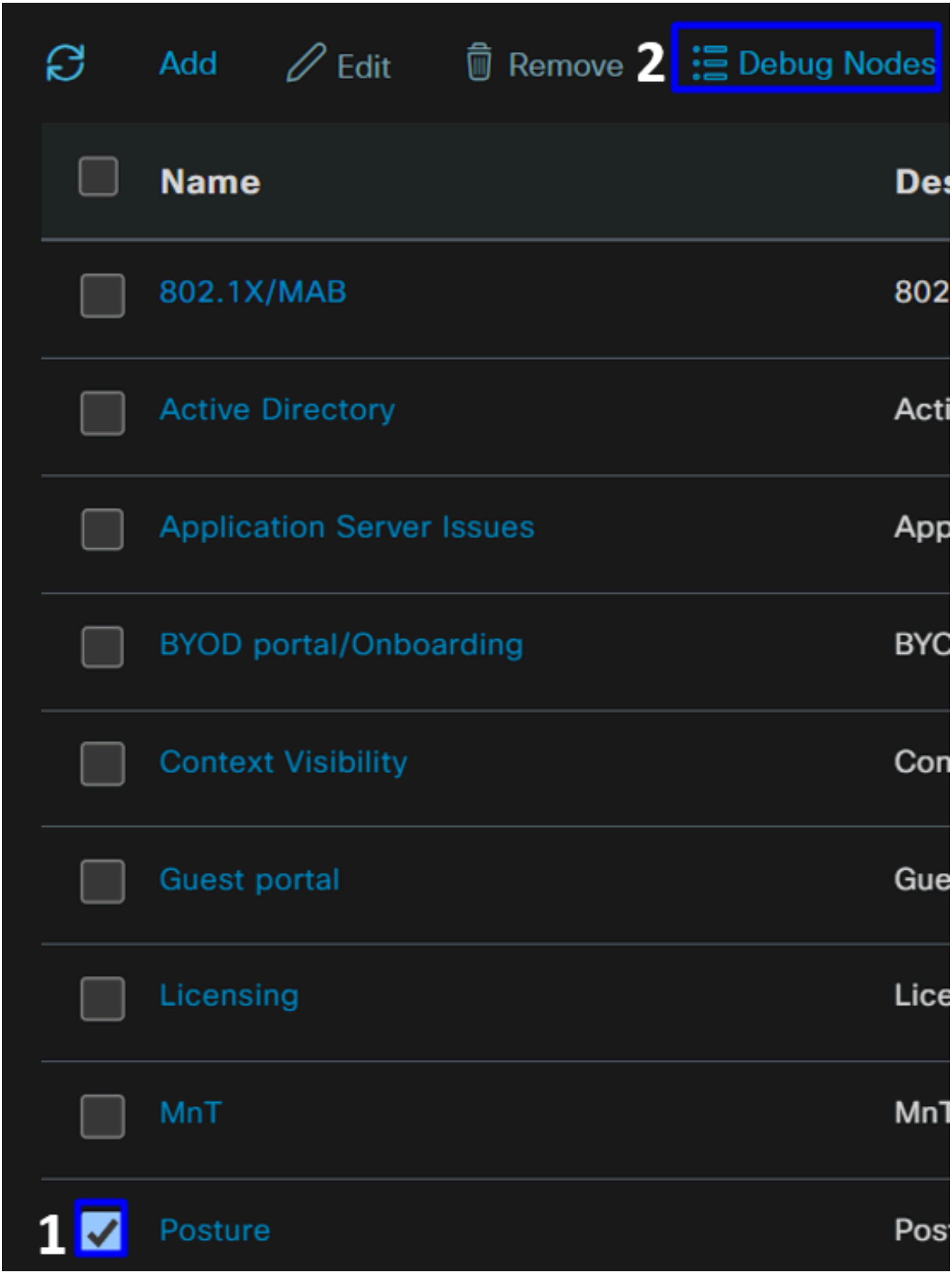
- Vaya a su panel de ISE
- Haga clic en Operations > Troubleshoot > Debug Wizard



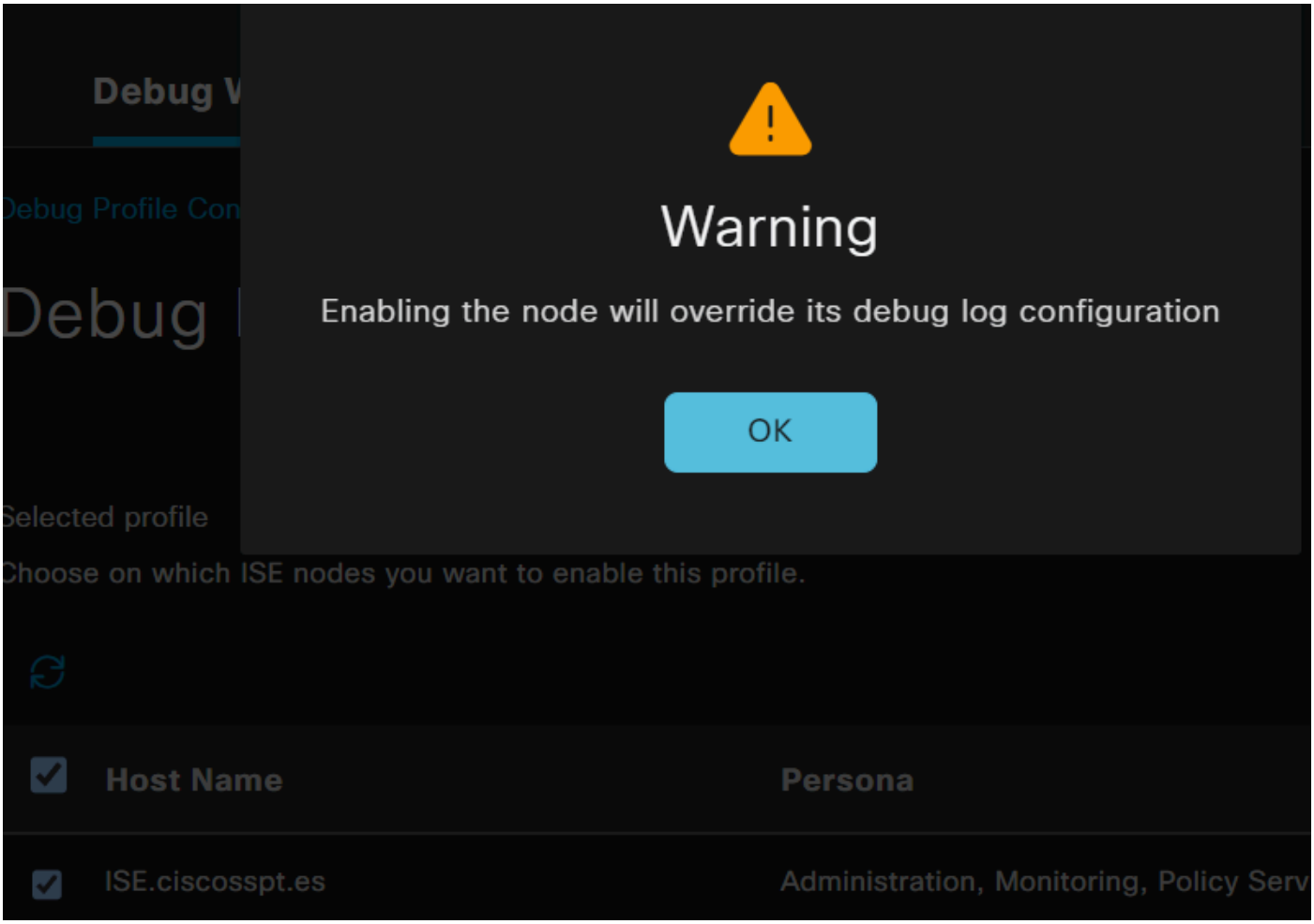

- Haga clic en Debug Profile Configuration



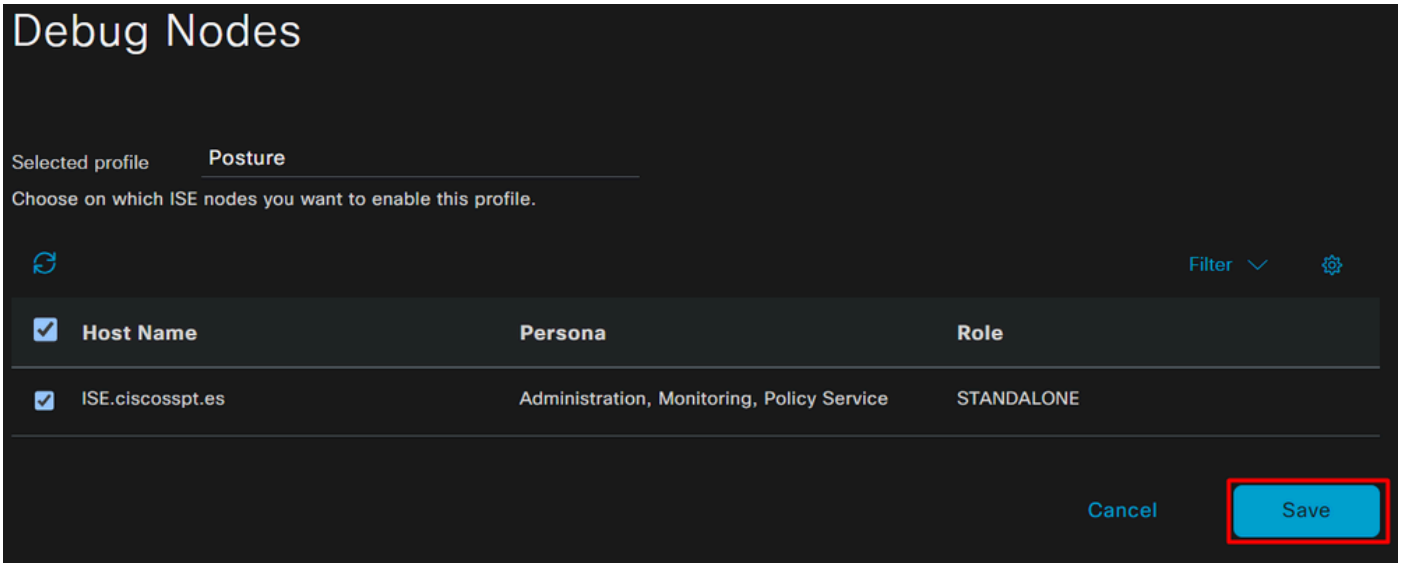

- Marque la casilla de verificación de **Posture > Debug Nodes**

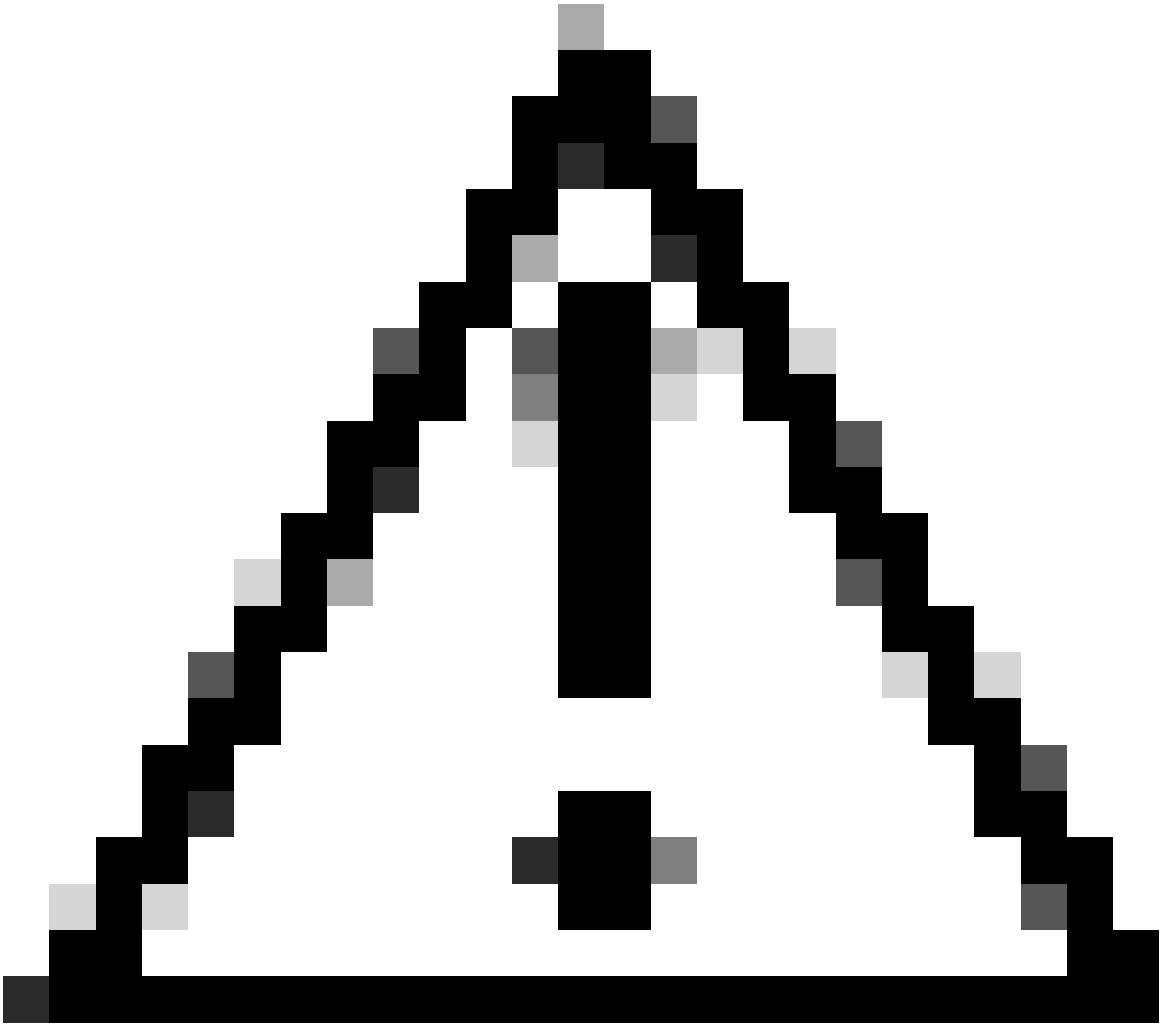

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- Marque la casilla de verificación de los nodos ISE en los que debe activar el modo de depuración para solucionar el problema




- Haga clic en 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

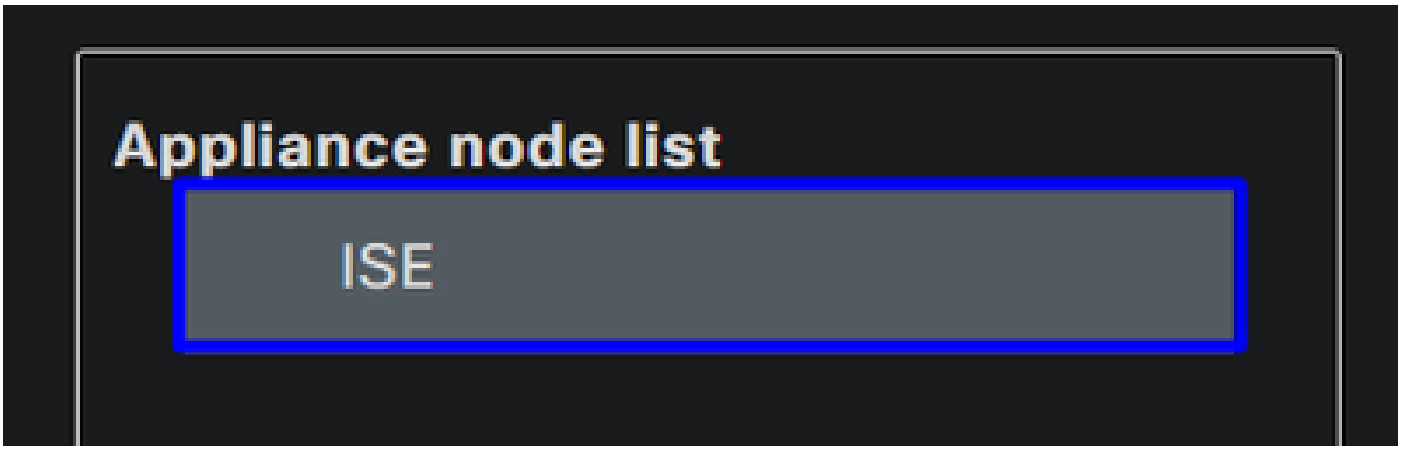


**Precaución**: después de este punto, debe empezar a reproducir el problema; **the debug logs can affect the performance of your device**.

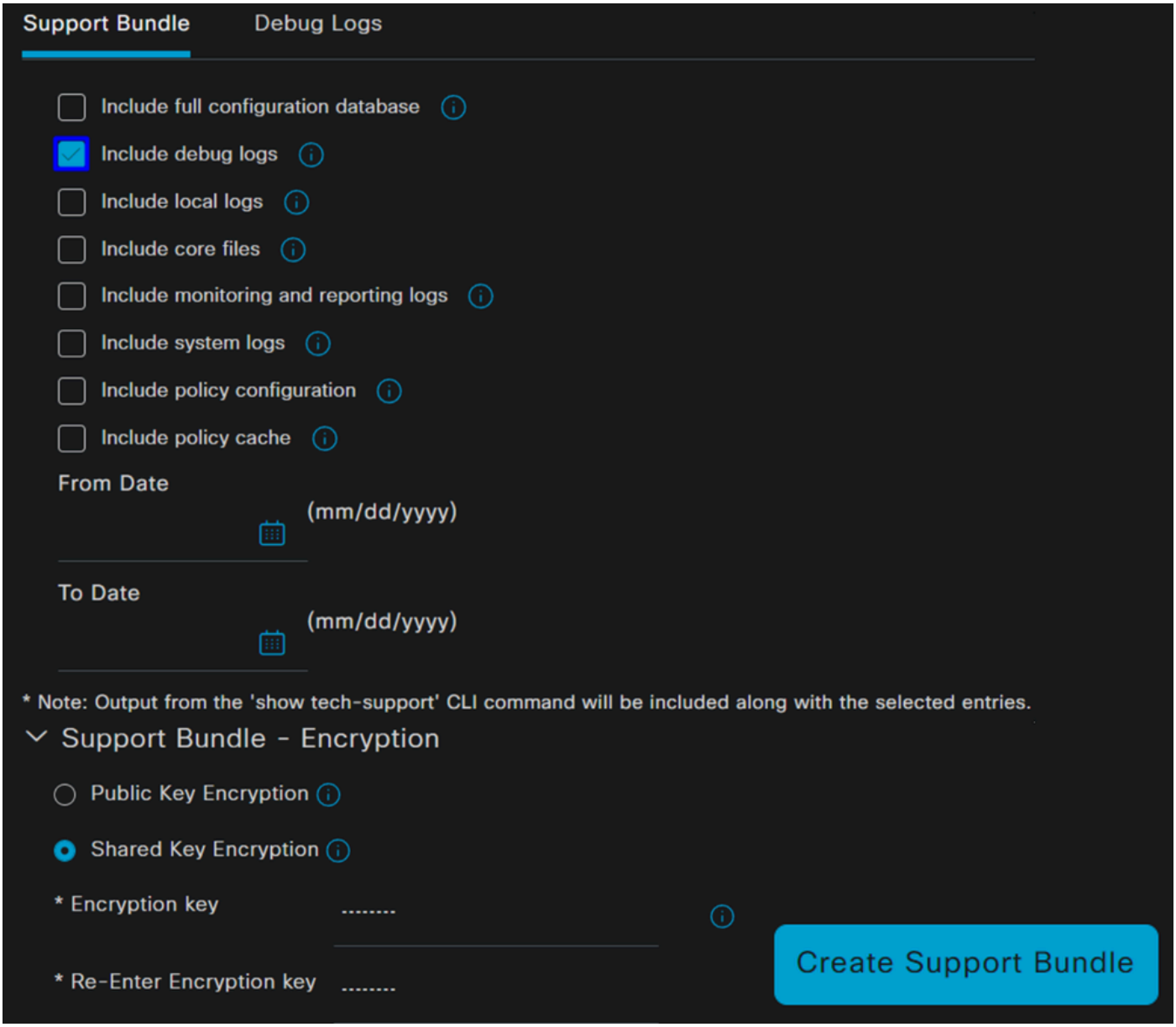
---

Después de reproducir el problema, continúe con los siguientes pasos:

- Haga clic en Operations > Download Logs
- Elija el nodo del que desea tomar los registros

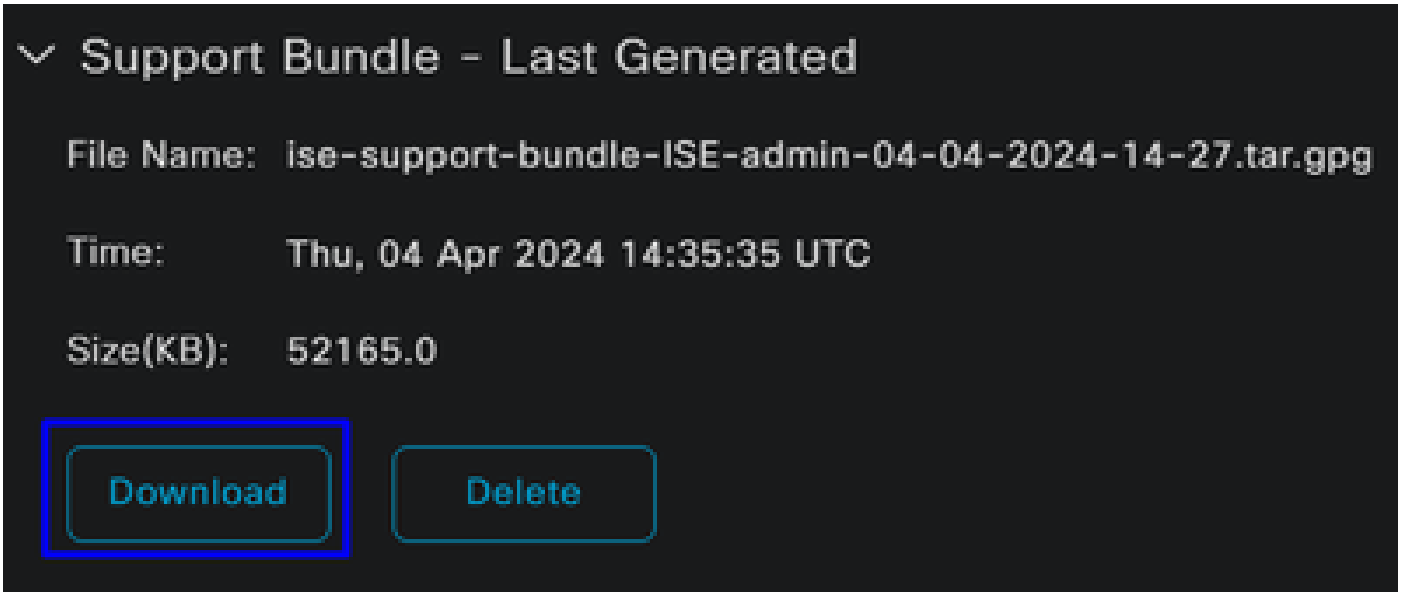


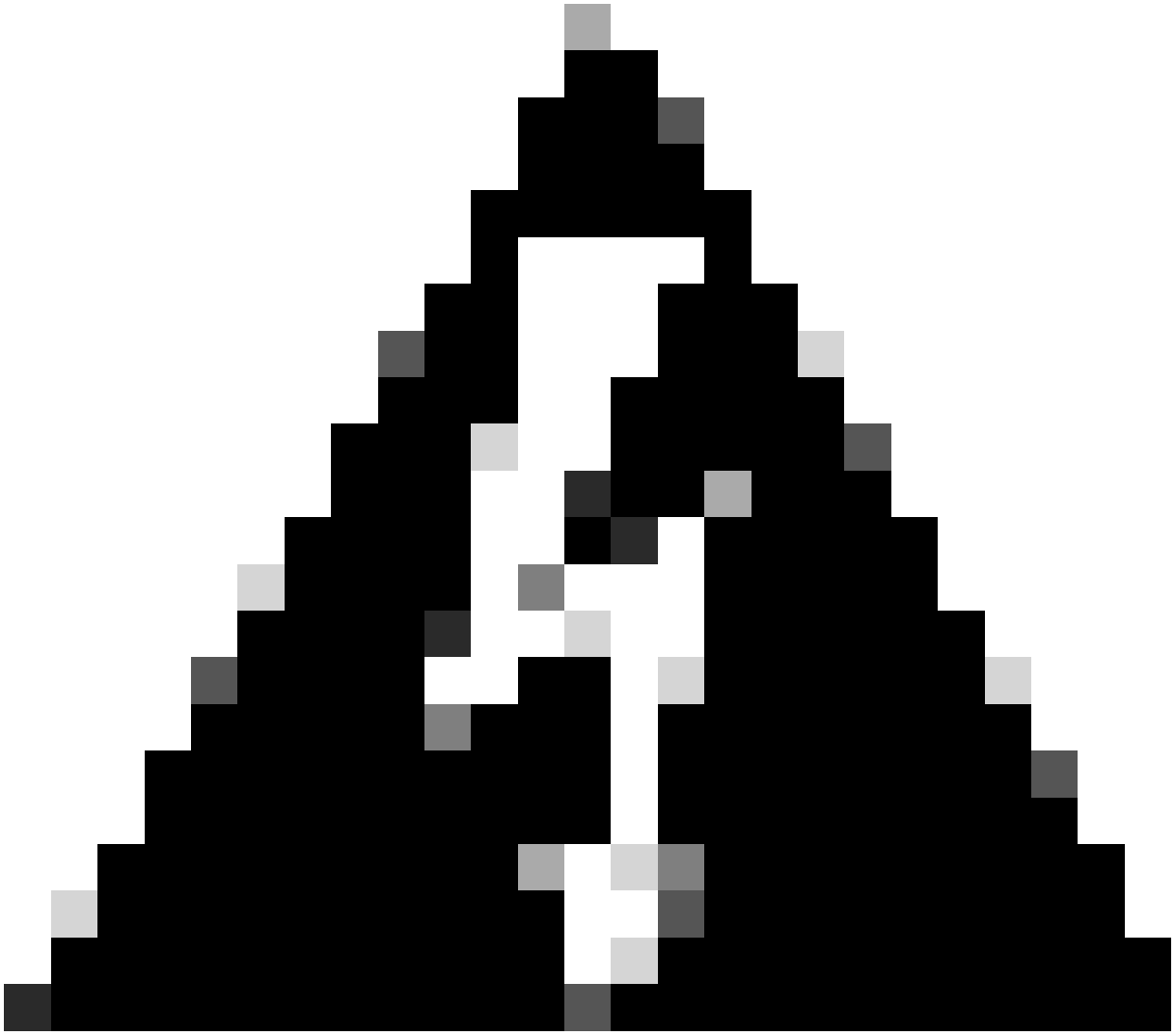

- En **Support Bundle**, elija las siguientes opciones:




- Include debug logs
- Debajo **Support Bundle Encryption**
    - **Shared Key Encryption**
        - Relleno **Encryption key** y **Re-Enter Encryption key**

- Haga clic en **Create Support Bundle**
- Haga clic en **Download**





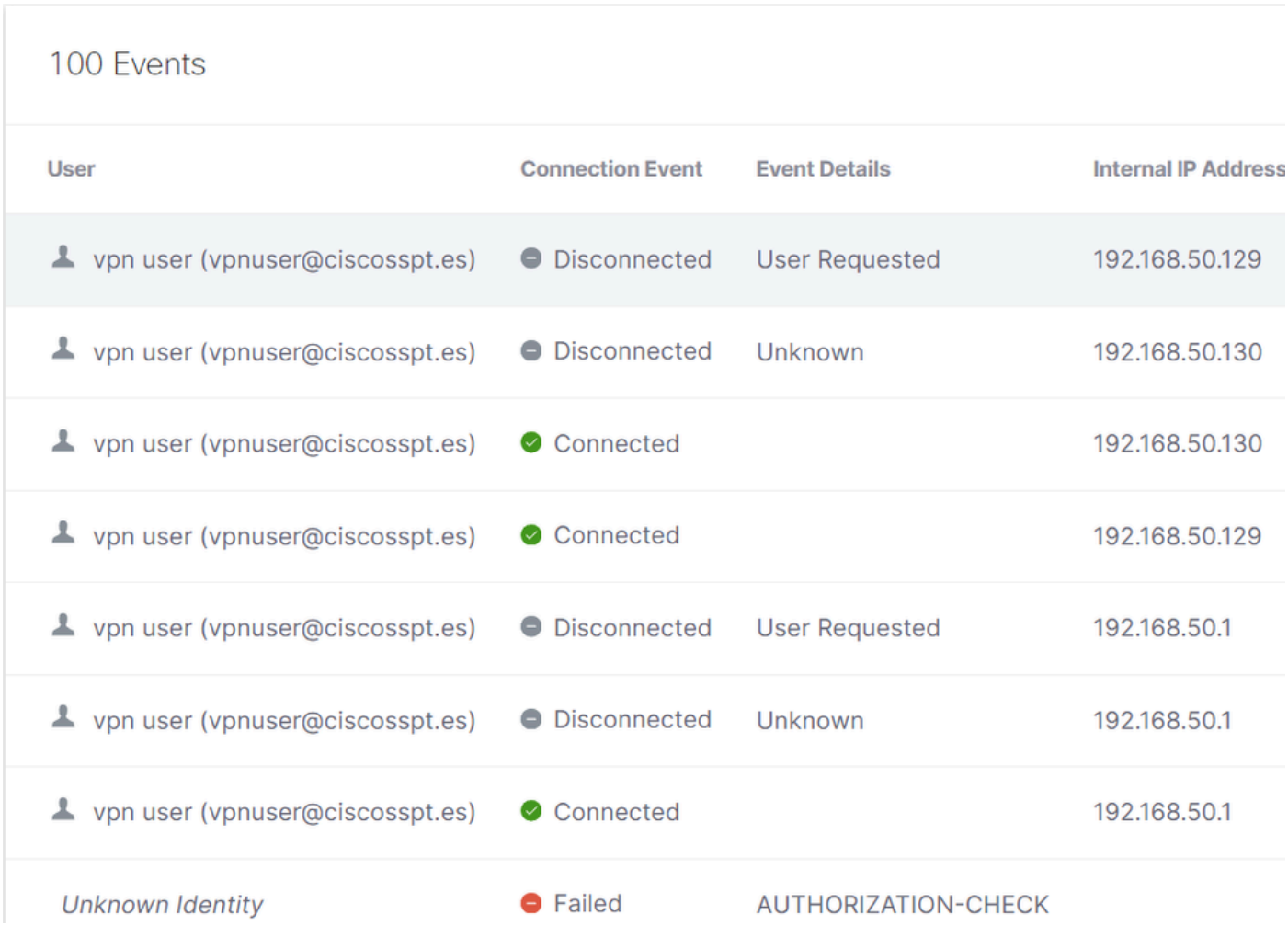
**Advertencia**: Desactive el modo de depuración habilitado en el paso Debug Profile Configuration

---

Cómo verificar los registros de acceso remoto de acceso seguro

Vaya al panel de acceso seguro:

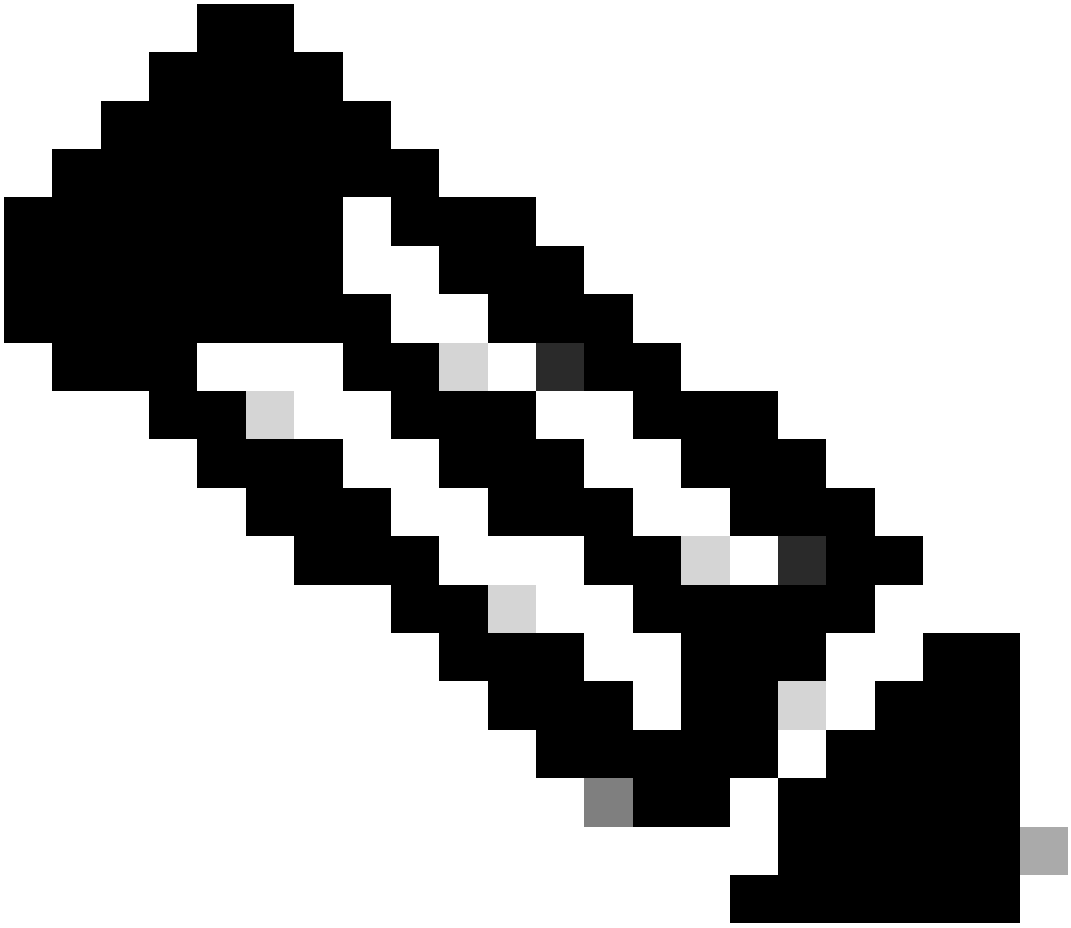
- Haga clic en Monitor > Remote Access Logs




Generar paquete DART en Secure Client

Para generar el paquete DART en su equipo, consulte el siguiente artículo:

Herramienta Cisco Secure Client Diagnostic and Reporting Tool (DART)



**Nota**: una vez que haya recopilado los registros indicados en la sección de solución de problemas, abra un caso con **TAC** para continuar con el análisis de la información.

Información Relacionada

- **Soporte técnico y descargas de Cisco**
- **Documentación de Secure Access y guía del usuario**

- **Descarga del software Cisco Secure Client**
- **Guía del administrador de Cisco Identity Services Engine, versión 3.3**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).