通过Duo SSO和ISE安全评估为RA-VPNaaS配置安全访问

目录

在安全客户端上生成DART捆绑包

相关信息

简介

本文档介绍如何为使用身份服务引擎(ISE)的远程访问VPN用户配置状态评估以及使用Duo的安全访问。

先决条件

- 在Secure Access上配置用户调配
- 使用身份验证代理或第三方IDP配置Duo SSO
- 思科ISE通过隧道连接到安全访问

要求

Cisco 建议您了解以下主题：

- 身份服务引擎
- 安全访问
- 思科安全客户端
- 双因素身份验证-双安全指南
- ISE终端安全评估
- 验证、授权和记帐

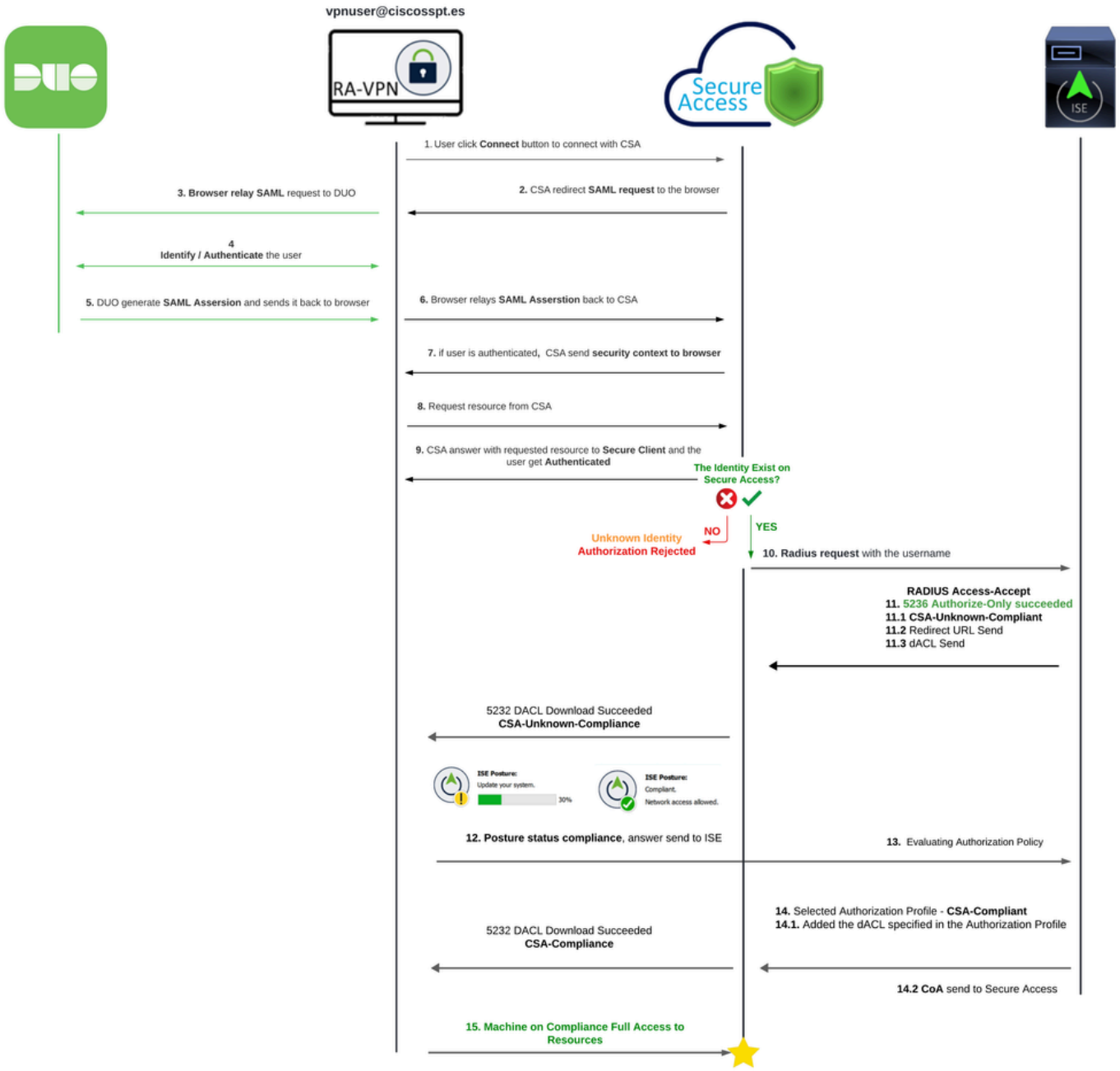
使用的组件

本文档中的信息基于：

- 身份服务引擎(ISE)版本3.3补丁1
- 安全访问
- 思科安全客户端- Anyconnect VPN版本5.1.2.42

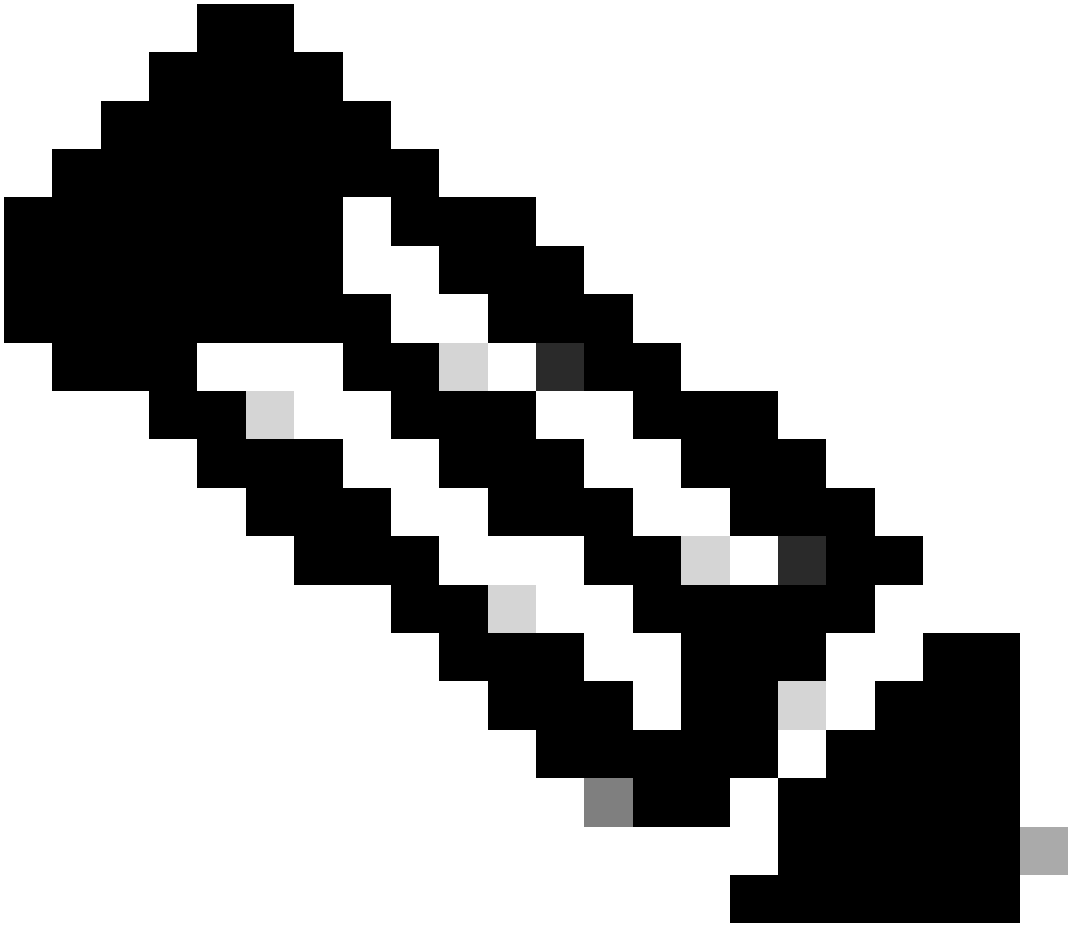
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息



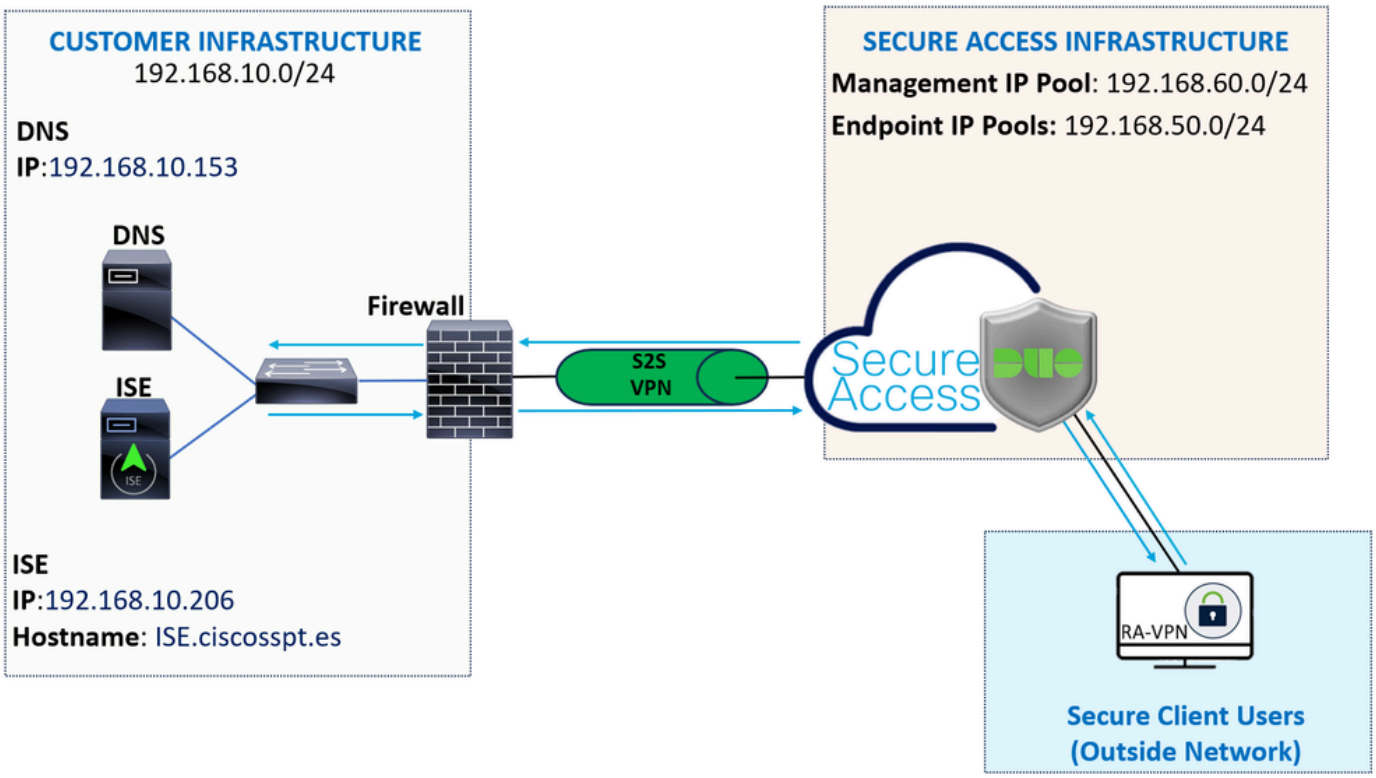
将Duo SAML与思科身份服务引擎(ISE)集成可增强身份验证流程，从而为思科安全访问解决方案添加另一层安全性。双核SAML提供单点登录(SSO)功能，可简化用户登录流程，同时确保高安全性标准。

通过双向SAML进行身份验证后，授权过程由Cisco ISE处理。这允许根据用户身份和设备状态做出动态访问控制决策。ISE可以实施详细策略，规定用户可以访问哪些资源、何时访问以及从哪些设备访问哪些资源。

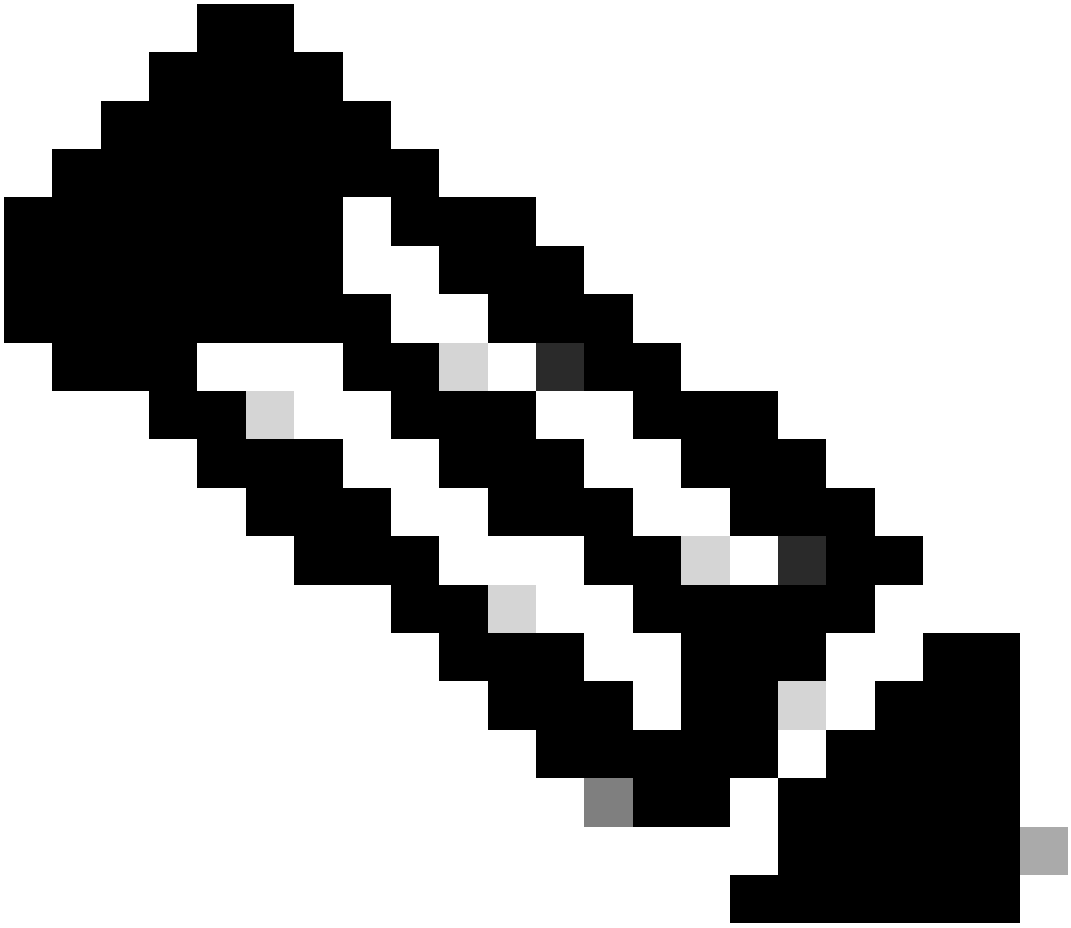


注意：要配置RADIUS集成，您需要确保两个平台之间有通信。

网络图


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)

配置



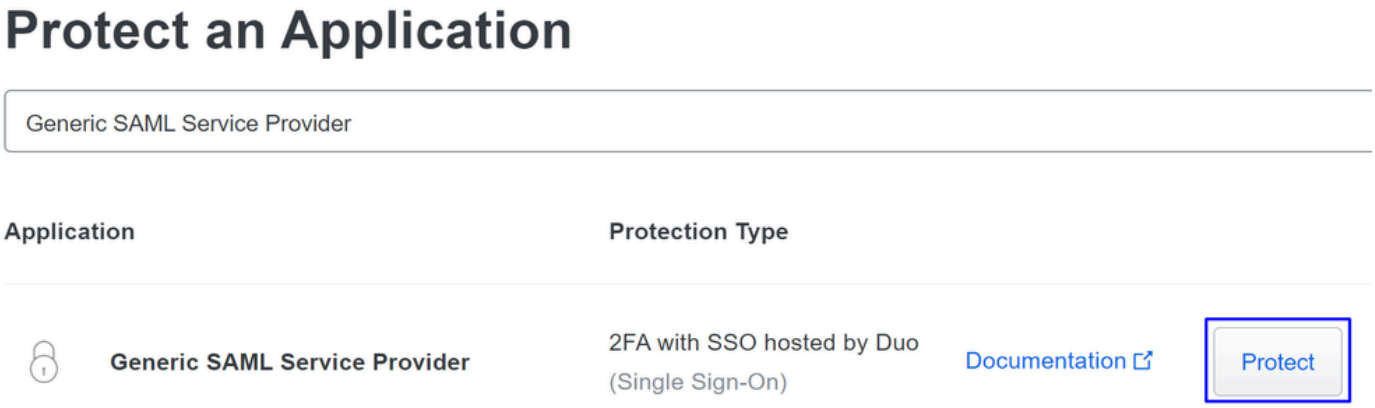
注意：在开始配置过程之前，您必须完成安全访问和ISE集成的第一步。

Duo配置

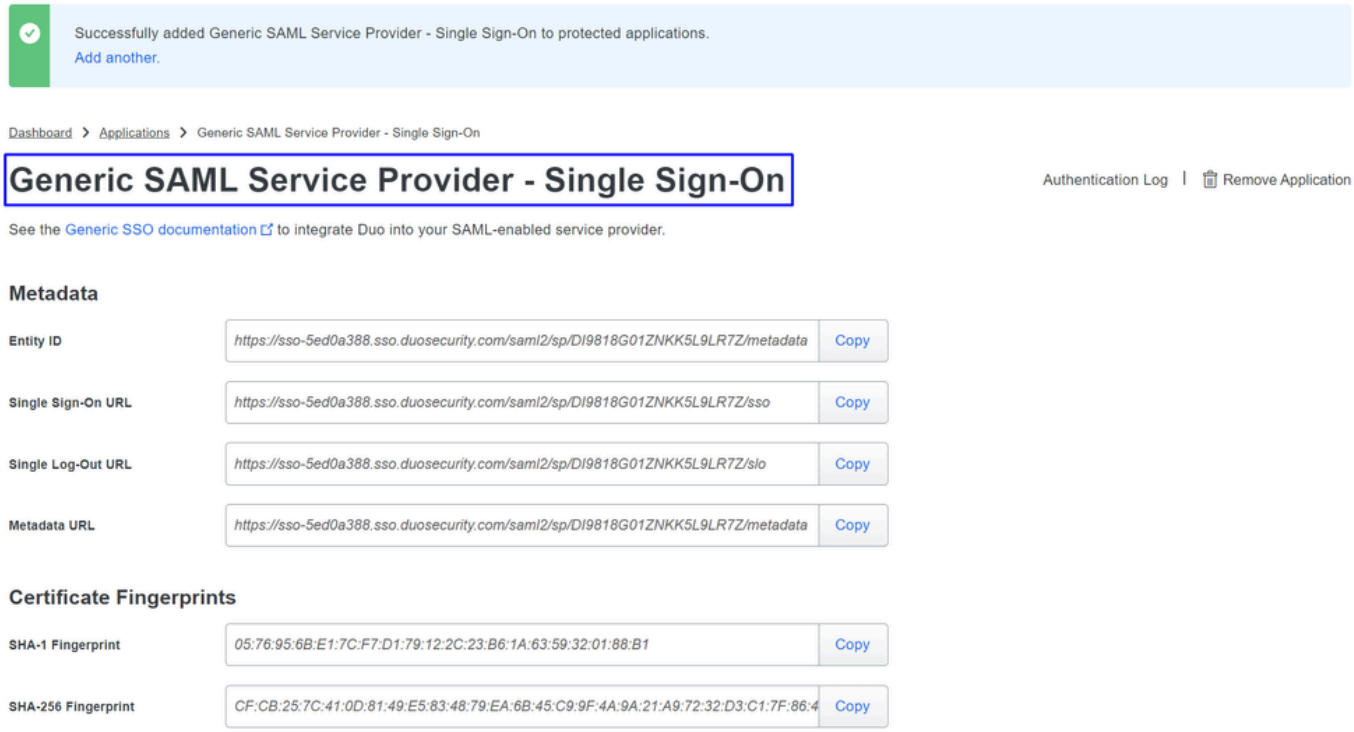
要配置RA-VPN应用，请执行以下步骤：

导航至双核管理面板

- 导航至 **Applications > Protect an Application**
  - 搜索 **Generic SAML Service Provider**
  - 点击 Protect



您必须在屏幕上显示应用；请记住VPN配置的应用名称。



在本例中， **Generic SAML Service Provider.**

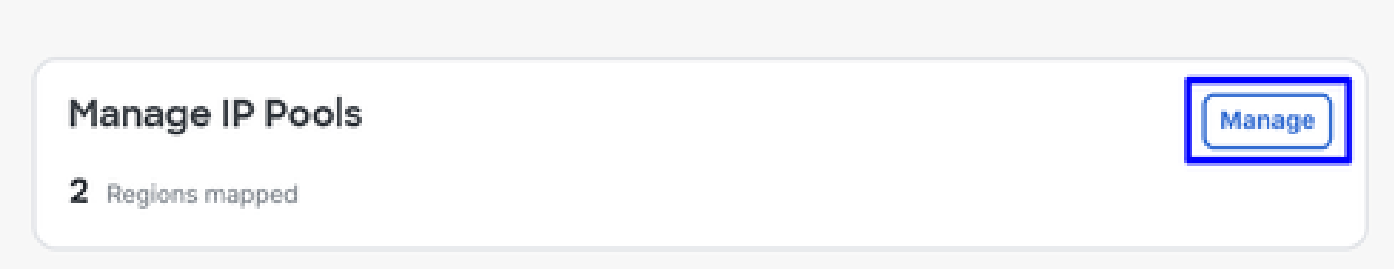
安全访问配置

在IP池上配置RADIUS组

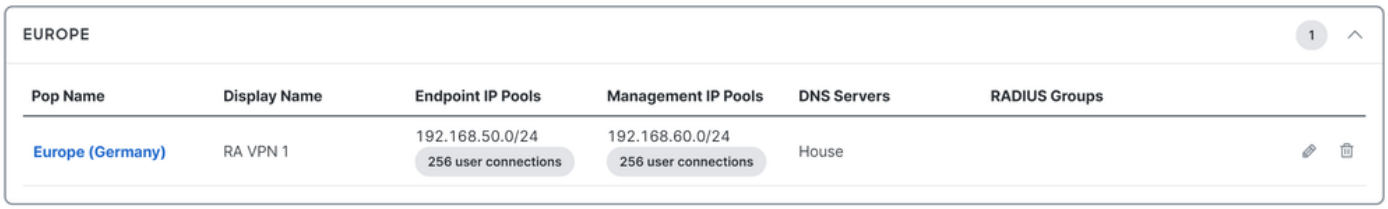
要使用Radius配置VPN配置文件，请继续执行以下步骤：

导航到安全访问控制面板。

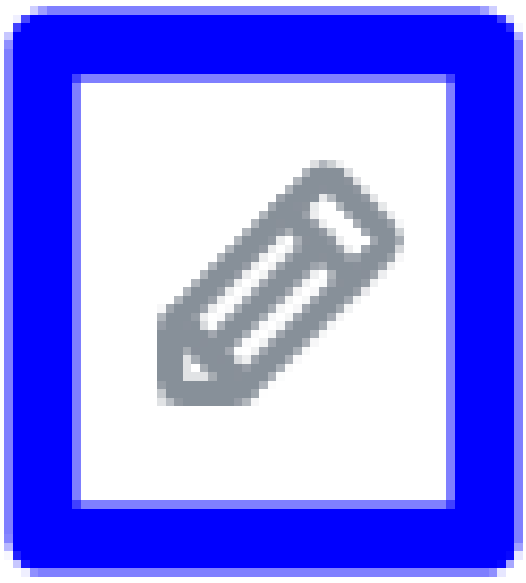
- 点击 **Connect > Enduser Connectivity > Virtual Private Network**
- 在“您的池配置”(**Manage IP Pools**)下，单击Manage

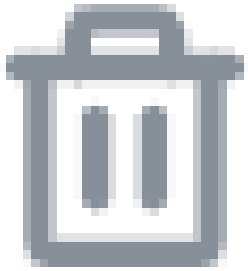


- 选择**IP Pool Region** 并 **Radius Server**



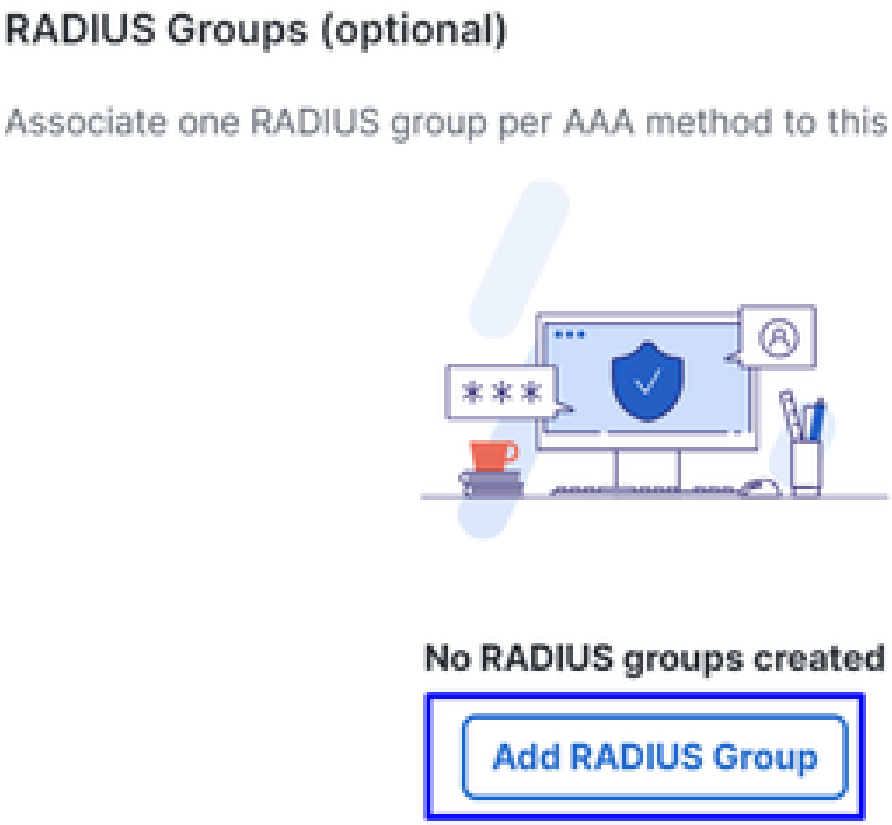
- 点击铅笔编辑





- 现在，在“IP池”(IP Pool)部分的“配置”(configuration)下拉列表中， **Radius Group (Optional)**

- 点击 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

集成的名称

- **AAA method**

  - **Authentication**：标记**Authentication** 的复选框并选择端口，默认情况下为1812

    - 如果您的身份验证需要标记Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)此复选框

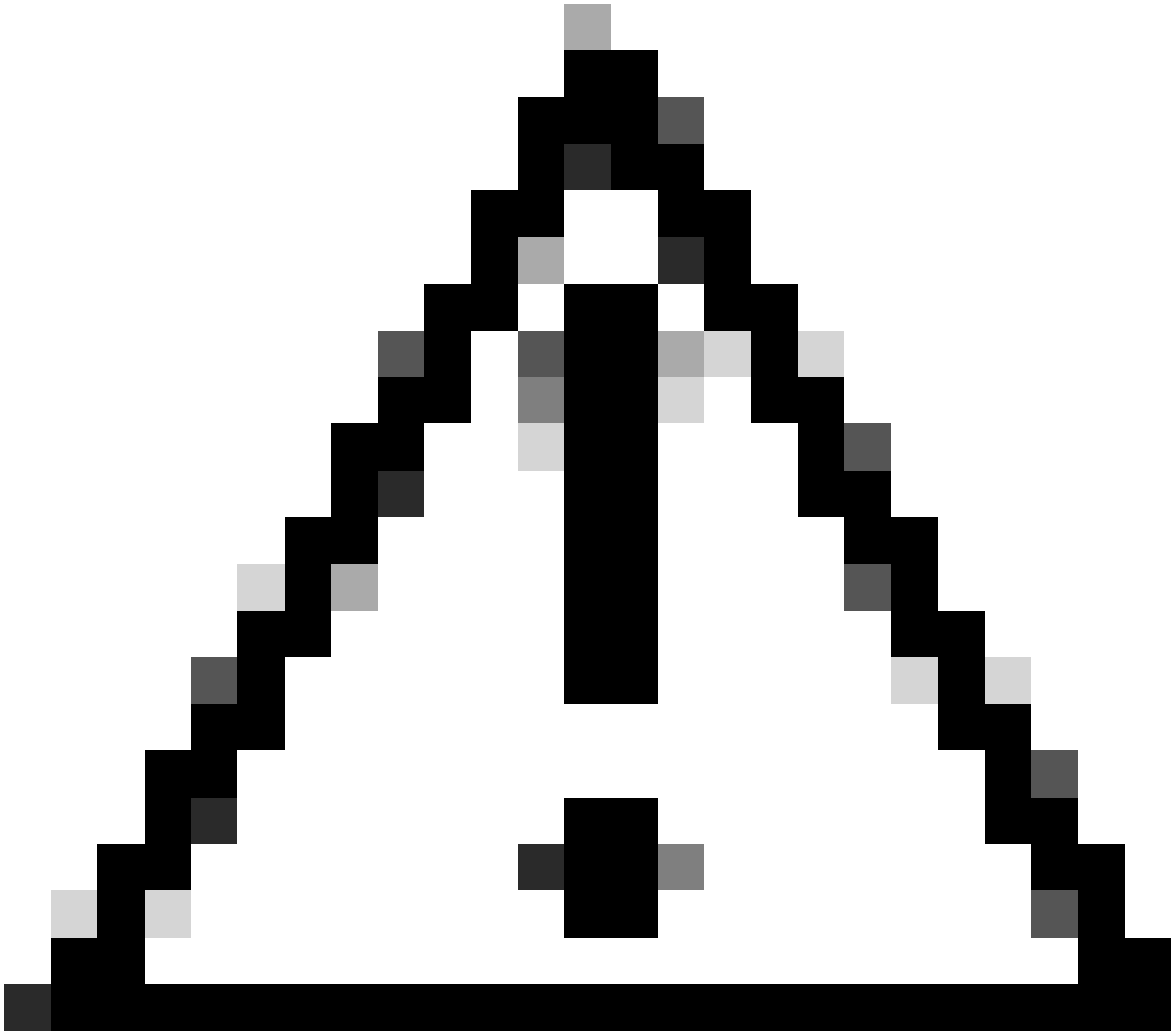
- **Authorization**：标记Authorization复选框并选择端口，默认情况下为1812

  - 标记**Authorization mode Only Change of Authorization (CoA) mode** 复选框并允许来自ISE的状态和更改

- **Accounting**：标记Authorization的复选框，并选择端口，默认情况下为1813

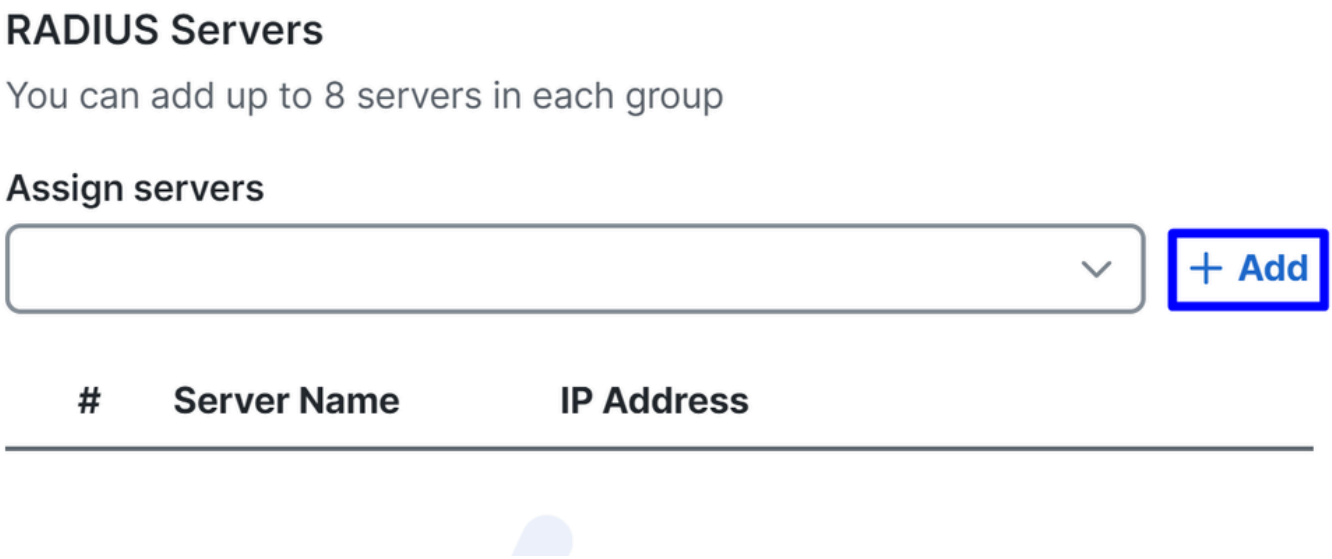
  - 选择**Single or Simultaneous** (在单模式中，记账数据只发送到一台服务器。在同步模式下，将记帐数据发送到组中的所有服务器)

    - 选中 **Accounting update** 复选框以启用定期生成RADIUS临时记账更新消息。

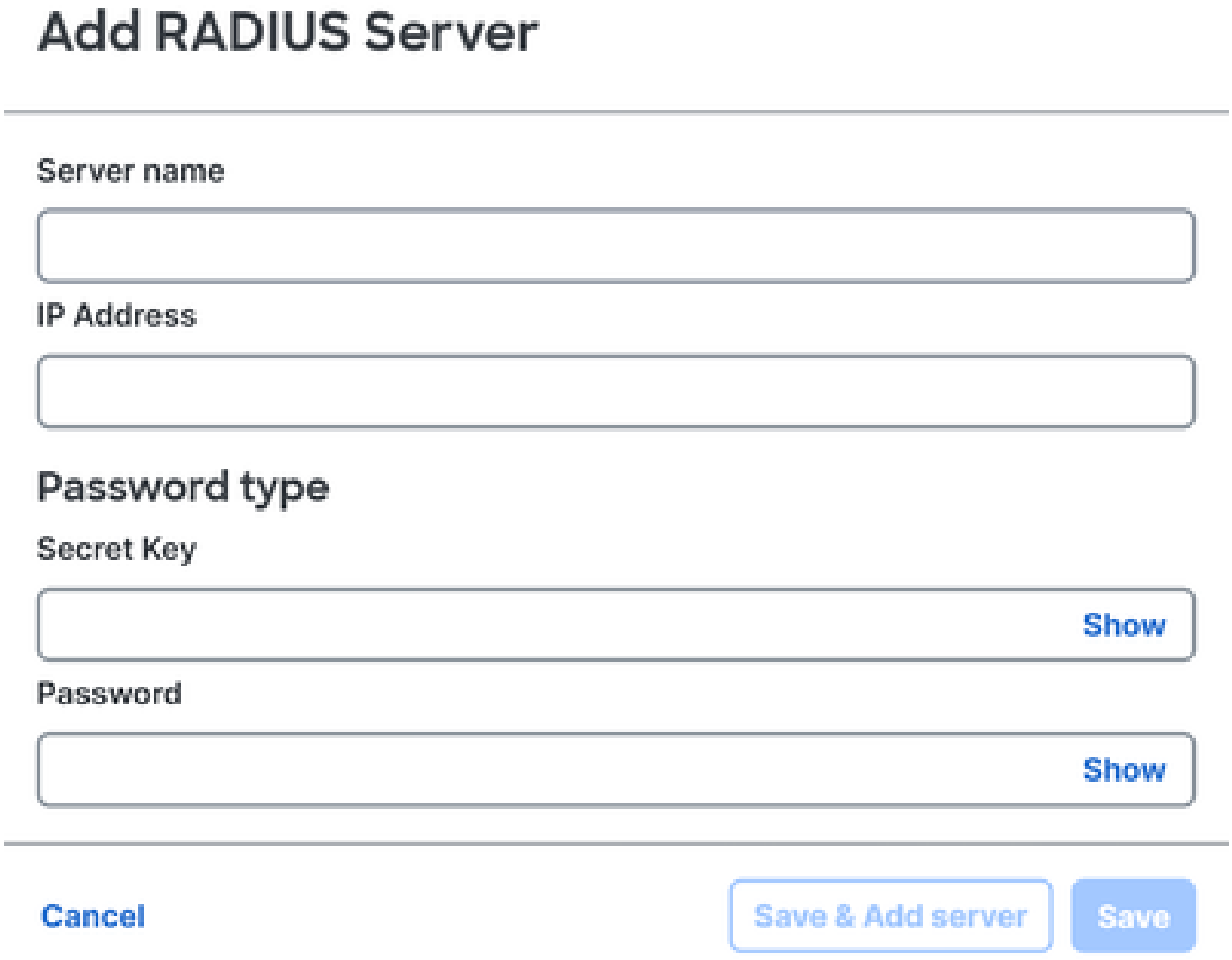


注意：选择Authentication时和**Authorization** 方法必须使用同一端口。

- 之后，您需要在 **RADIUS Servers**部分配置用于通过AAA进行身份验证的**RADIUS Servers** (ISE)：
- 点击 + Add

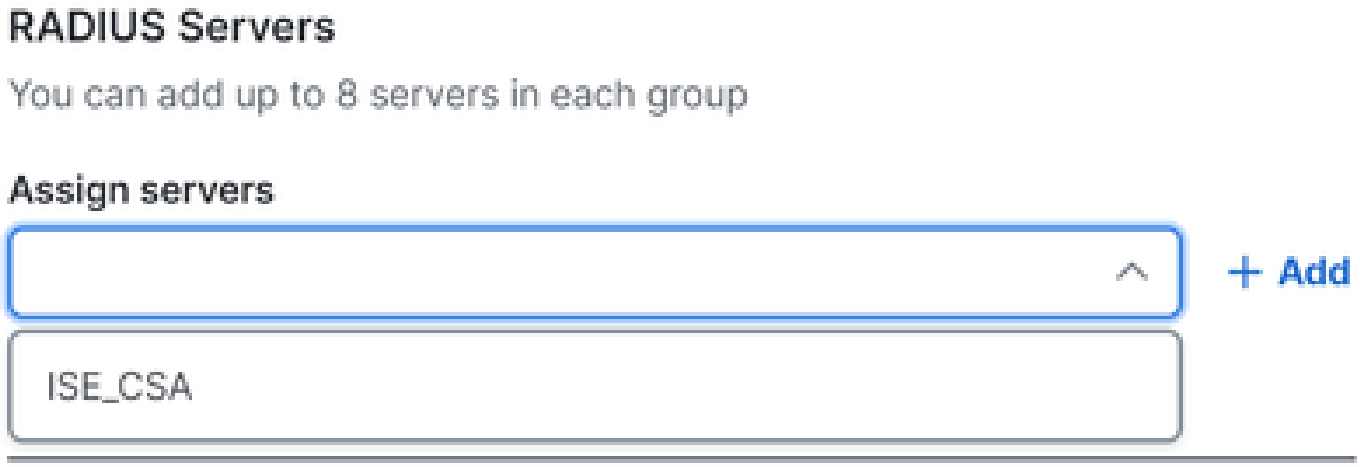

RADIUS Servers
You can add up to 8 servers in each group
Assign servers
+ Add
# Server Name IP Address

- 然后，配置以下选项：


Add RADIUS Server
Server name
IP Address
Password type
Secret Key
Show
Password
Show
Cancel
Save & Add server
Save

- Server Name：配置名称以标识ISE服务器。
- **IP Address**：配置可通过安全访问访问的Cisco ISE设备的IP
- **Secret Key**：配置RADIUS密钥
- **Password**：配置您的Radius密码

- 点击**Save** 并在Assign Server选项下分配您的RADIUS服务器并选择您的ISE服务器：



- 再次点击**Save** 以保存所有配置完成

← 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

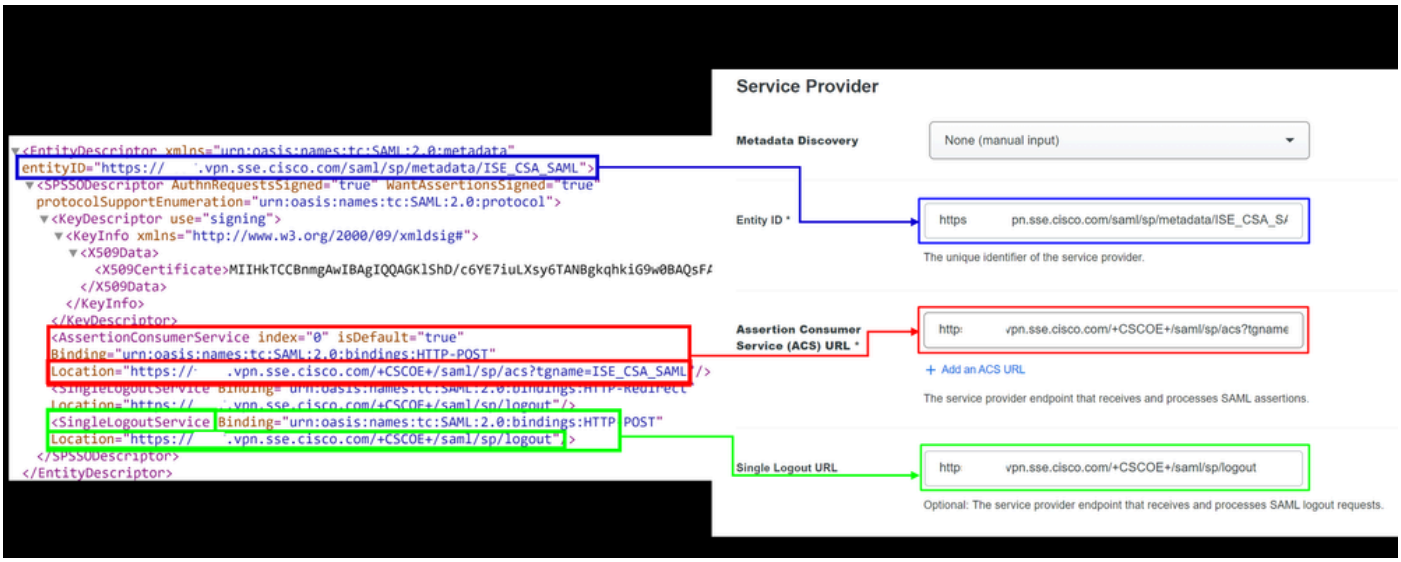
ISE_CSA

+ Add

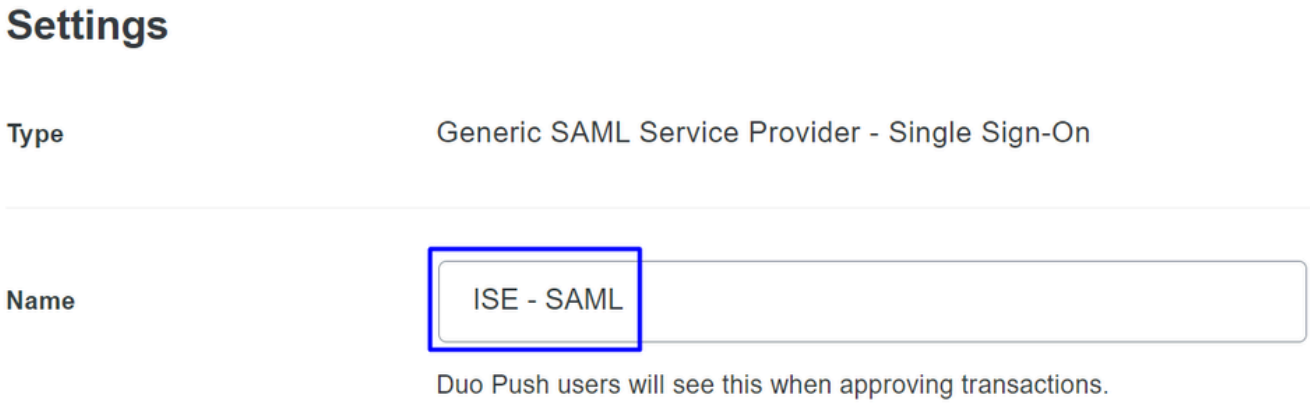
#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**：选择 **SAML**

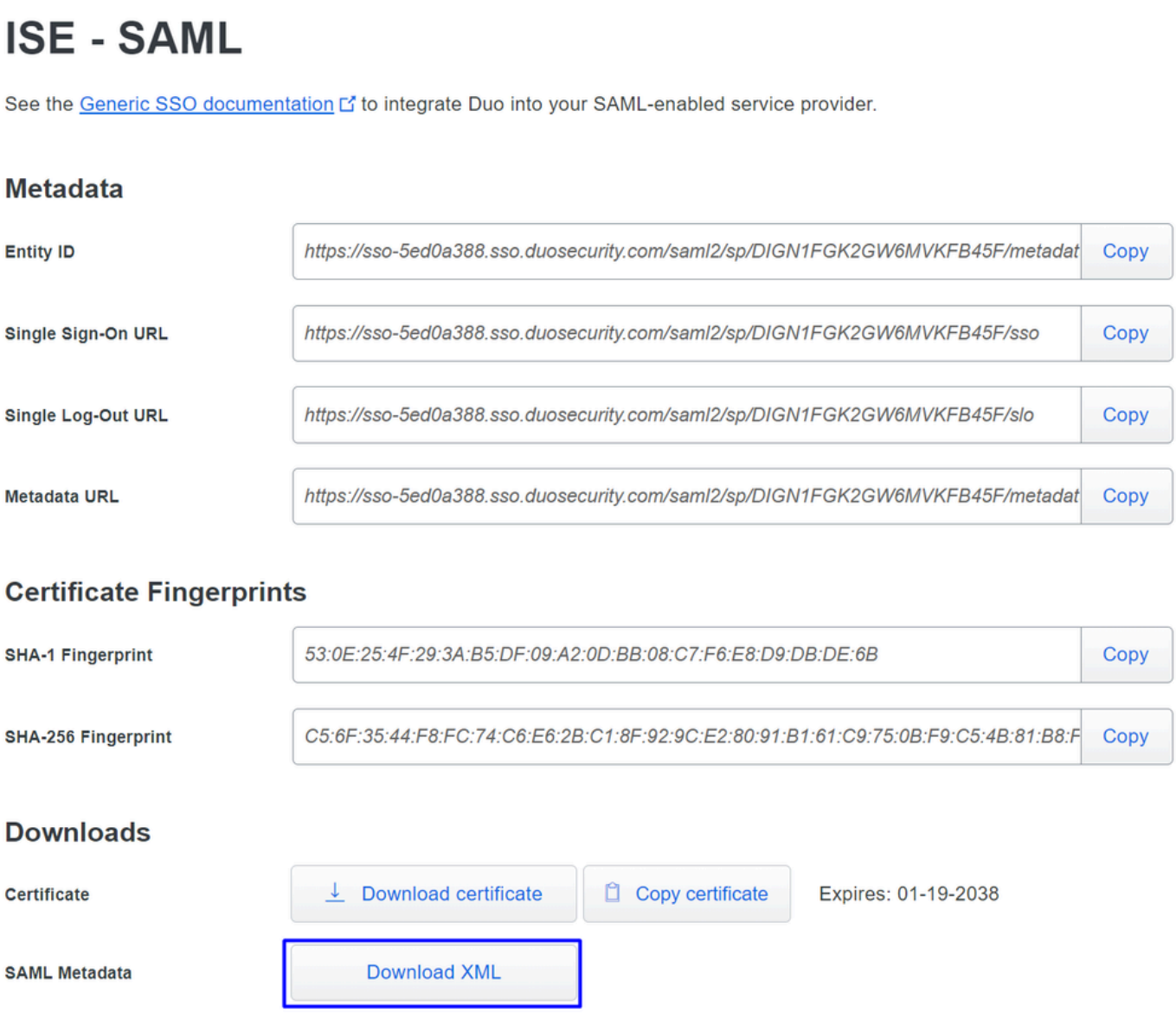
- 点击 Download Service Provider XML file
- 替换步骤Duo配置中配置的应用程序中的信息



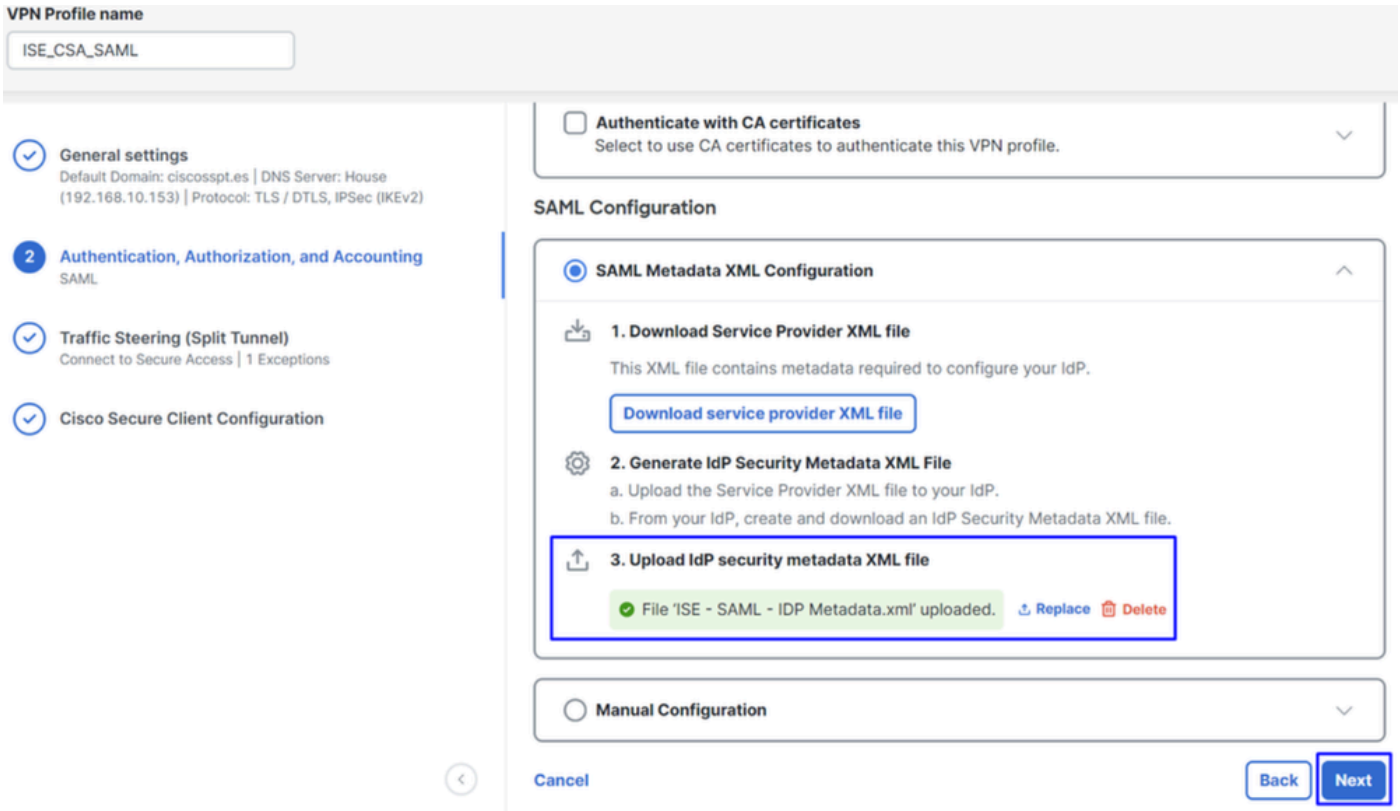
- 配置该信息后，请将Duo的名称更改为与您正在进行的集成相关的名称



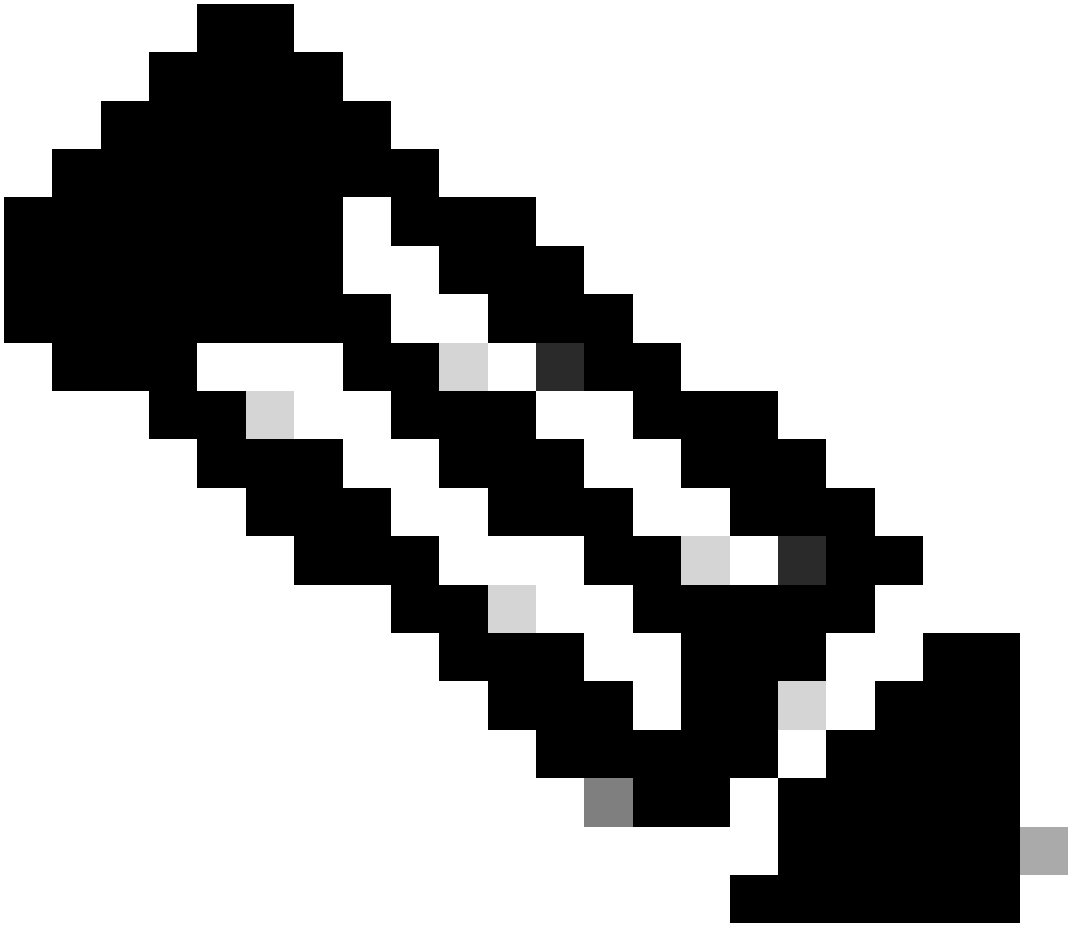
- 在Duo上单击**Save** 您的应用程序。
- 点击Save后，必须点击按钮下载**SAML Metadata** 的 **Download XML**



- 上传选项**3. Upload IdP security metadata XML file** 下的**SAML Metadata** on Secure Access，然后单击 **Next**

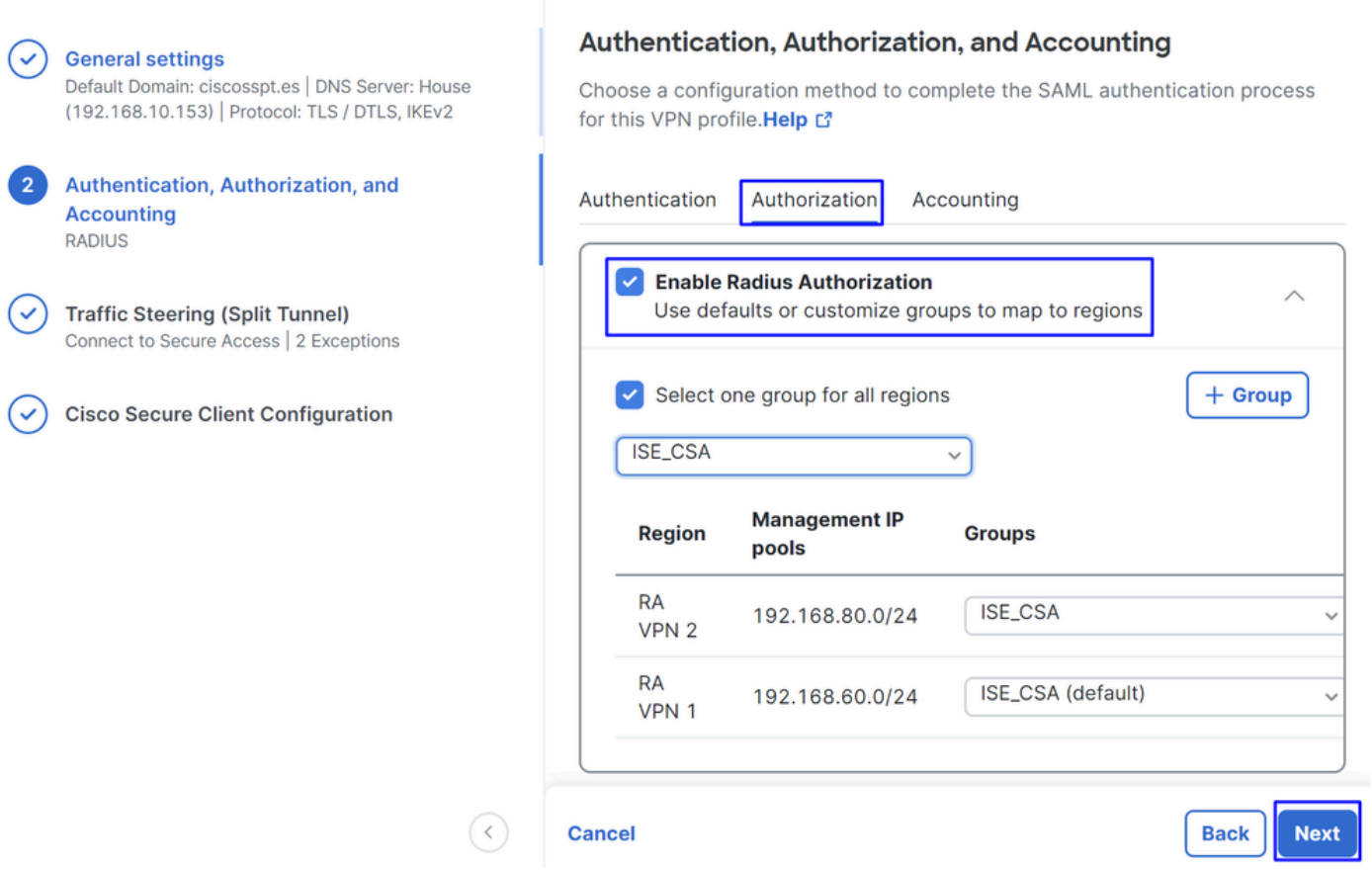

VPN Profile name
ISE_CSA_SAML
General settings
Default Domain: ciscosspt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPSec (IKEv2)
2
Authentication, Authorization, and Accounting
SAML
Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions
Cisco Secure Client Configuration
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

继续授权。



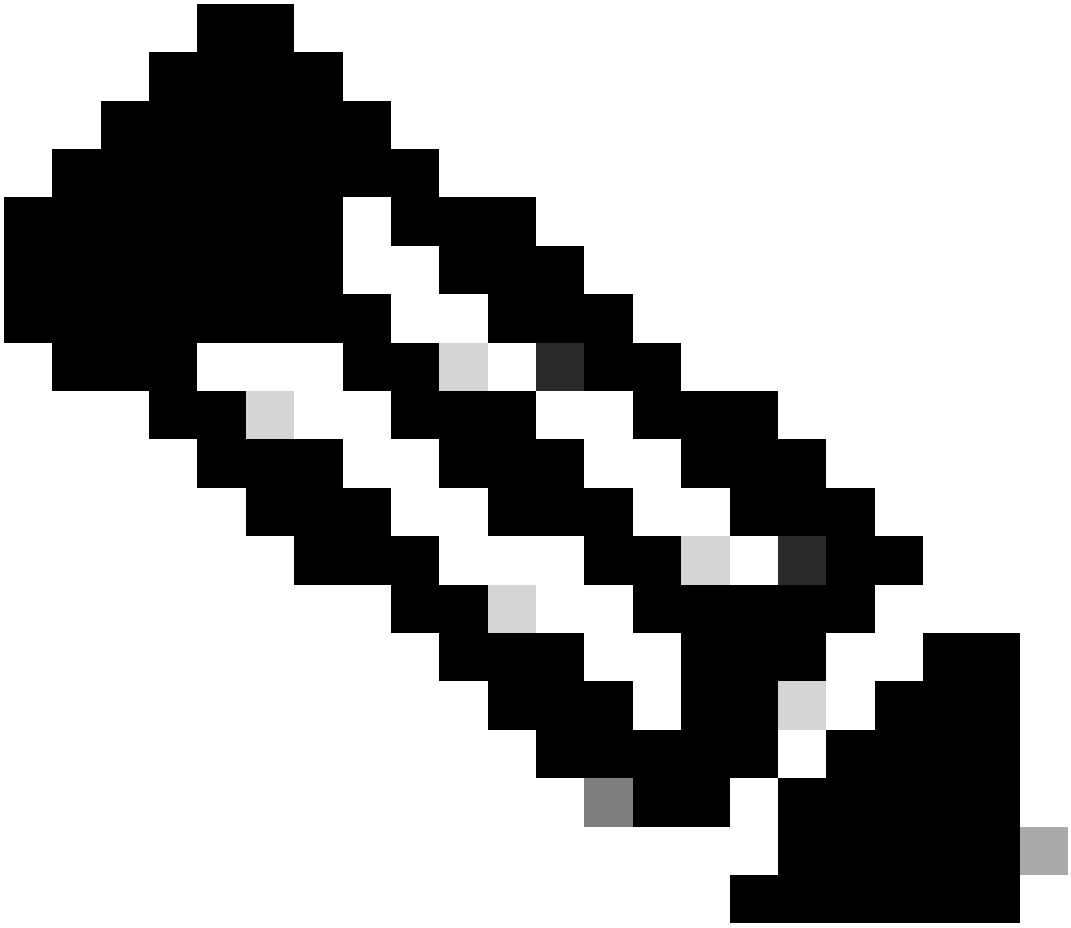
注意：一旦您使用SAML配置身份验证，您将通过ISE对其进行授权，这意味着安全访问发送的RADIUS数据包将仅包含用户名。此处不存在密码字段。

授权



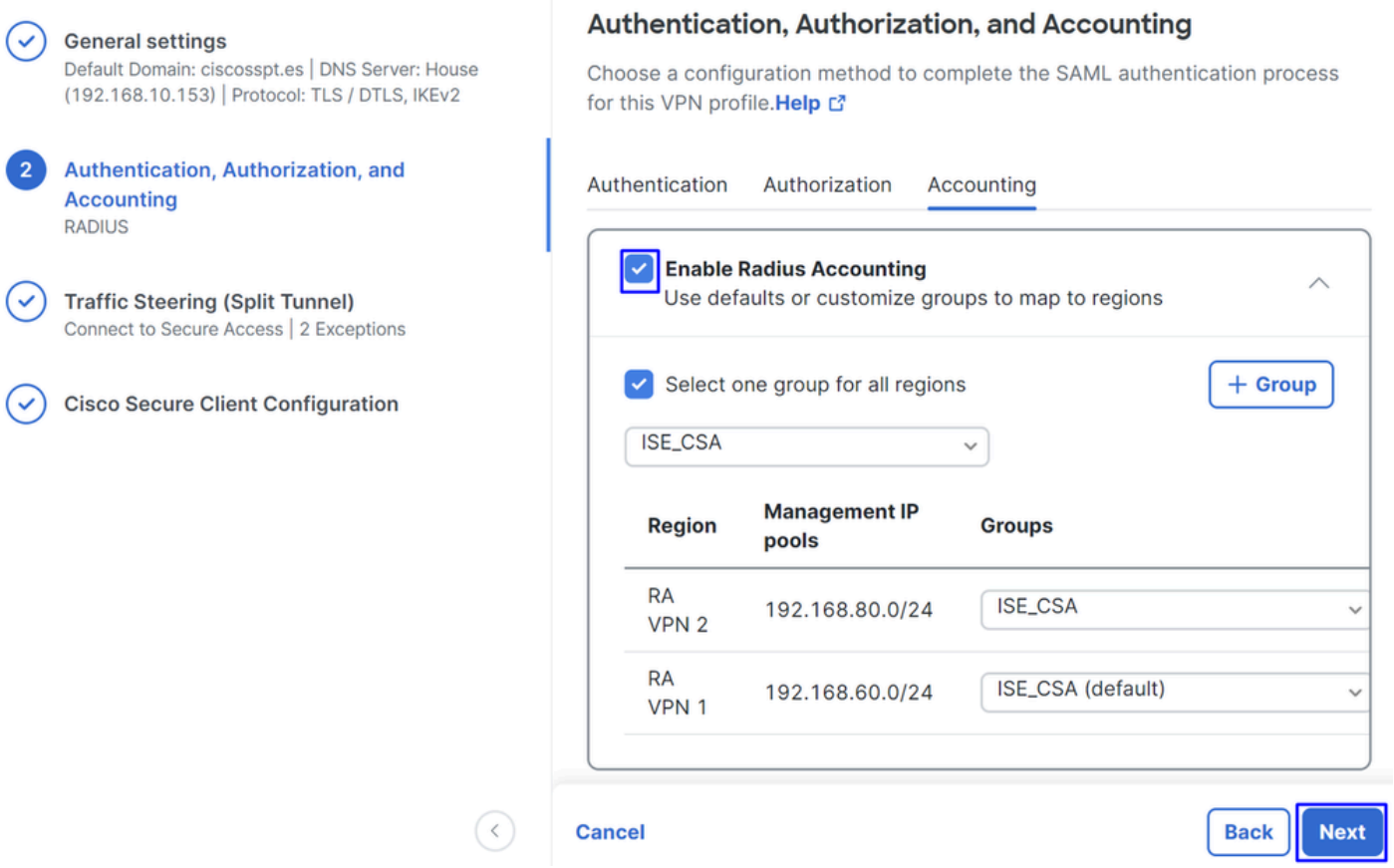
- **Authorization**
  - **Enable Radius Authorization**：标记复选框以启用RADIUS授权
    - 为所有区域选择一个组：选中该复选框以将一个特定RADIUS服务器用于所有远程访问-虚拟专用网络(RA-VPN)池，或为每个池单独定义它
- 点击 **Next**

配置完所有**Authorization** 部分后，请继续执行 **Accounting**。



注意：如果不启用 **Radio Authorization**，则终端安全评估无法工作。

记账

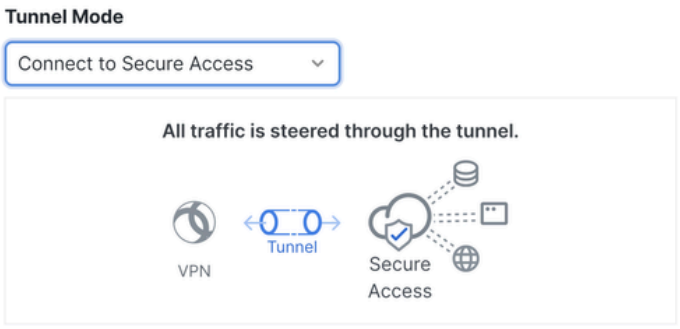


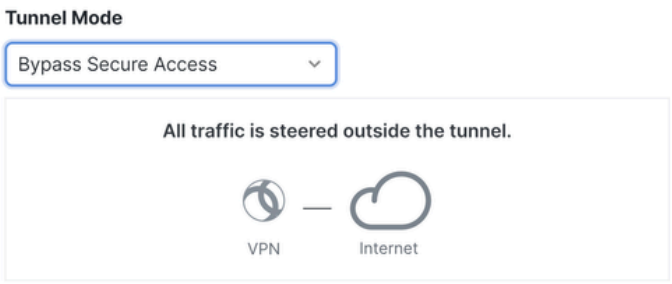
- **Accounting**
  - **Map Authorization groups to regions**：选择地区并选择 **Radius Groups**
- 点击 **Next**

After you have done configured the Authentication, Authorization and Accounting 请继续Traffic Steering。

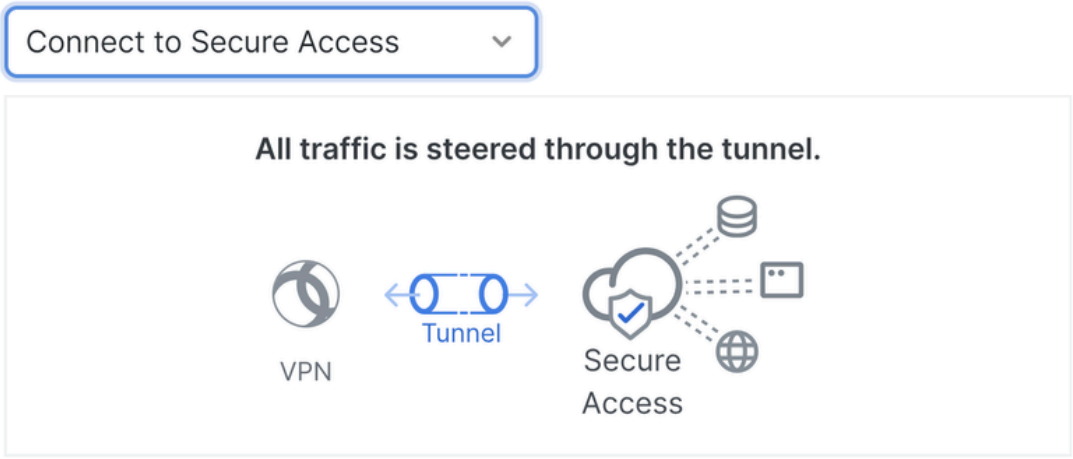
流量引导

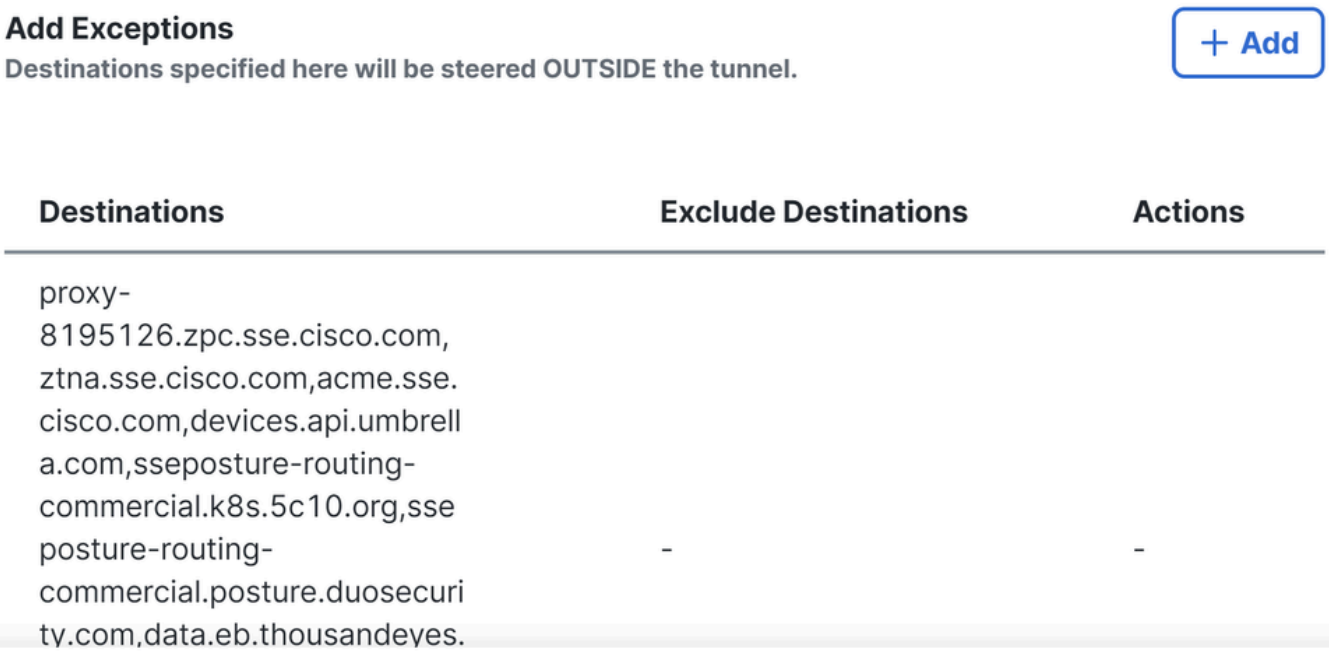
在流量引导下，您需要通过安全访问配置通信类型。





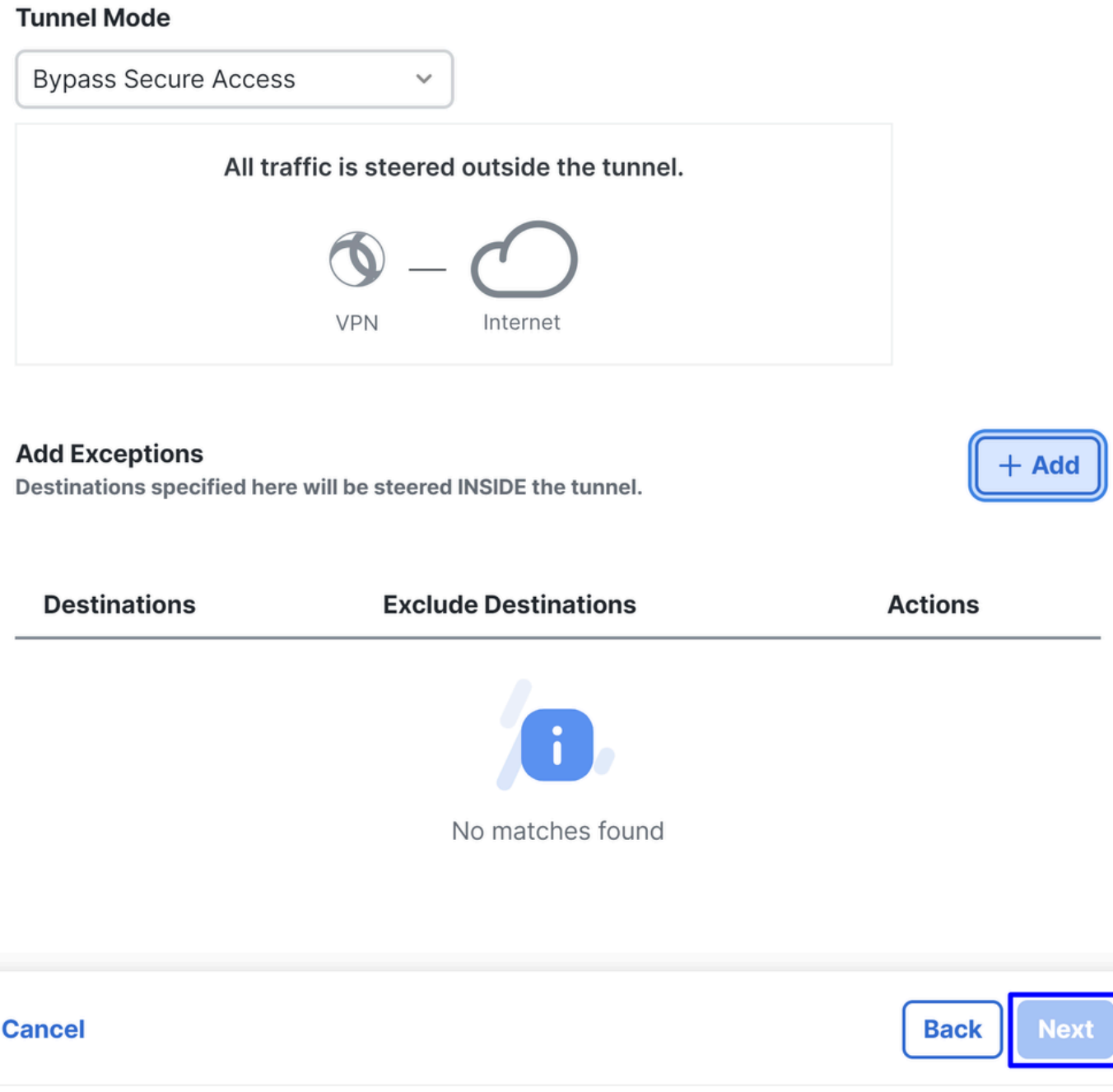
- 如果选择 **Connect to Secure Access**，则所有互联网流量都将通过 **Secure Access**

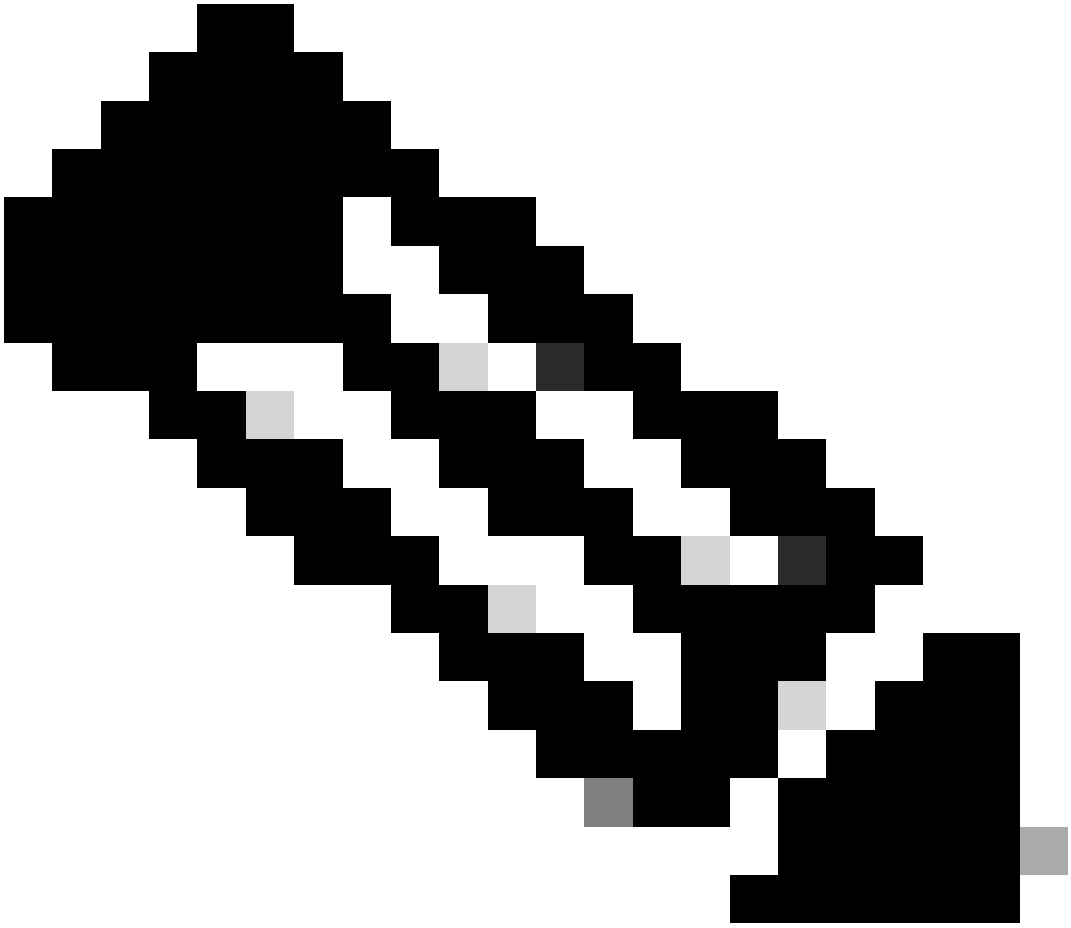




如果您想要添加Internet域或IP的例外项，请单击+ **Add** 按钮，然后单击**Next**。

- 如果您决定 **Bypass Secure Access**，则所有互联网流量都将通过您的互联网提供商，而不是通过Secure Access（无互联网保护）

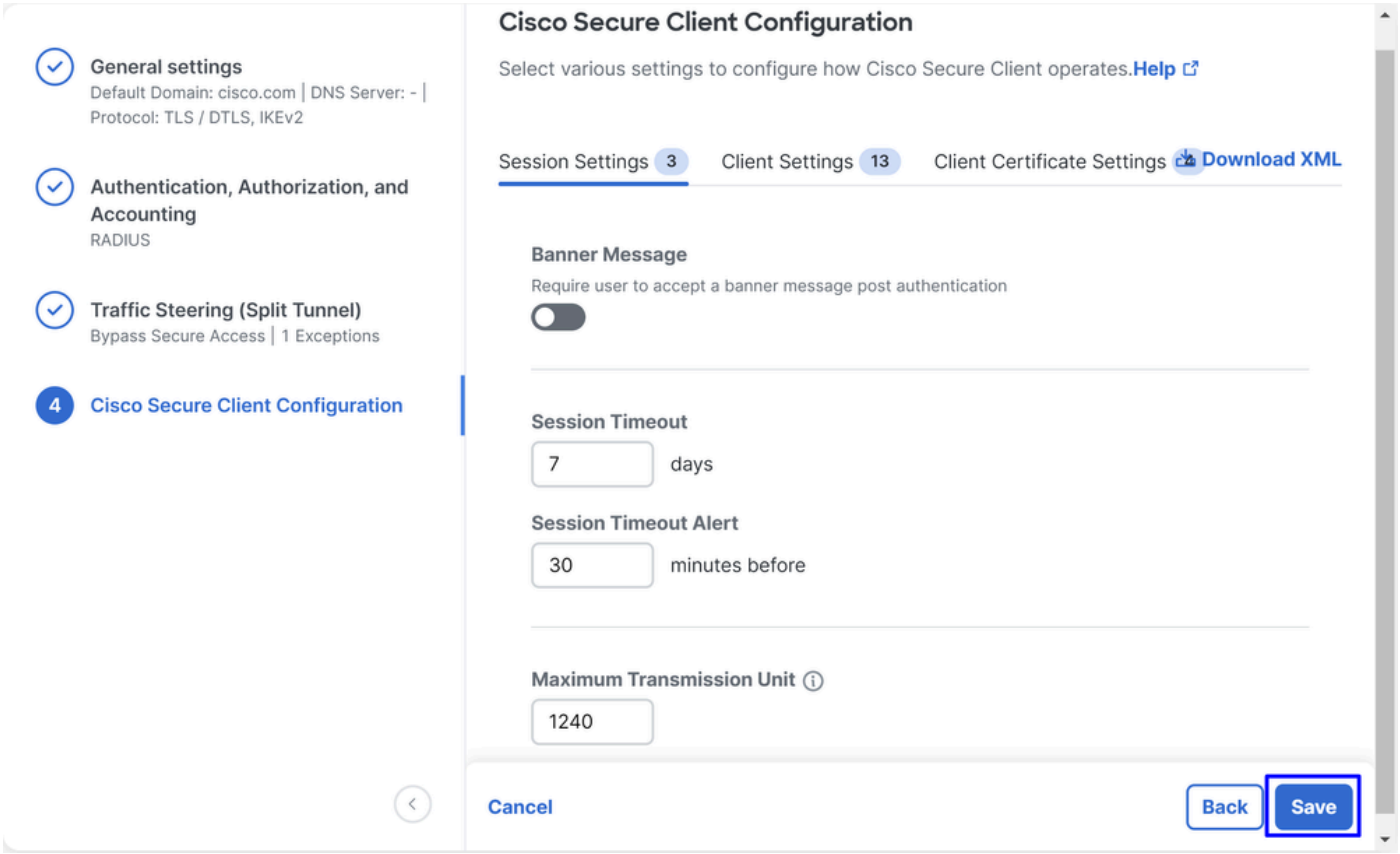




注意：选择**Bypass Secure Access**时，请添加**enroll.cisco.com** 用于ISE终端安全评估。

在此步骤中，选择要通过VPN访问的所有专用网络资源。要执行此操作，请点击 **+ Add**，然后在添加所有资源后点击**Next** 。

Cisco安全客户端配置



在此步骤中，您可以将所有内容都保持为默认值并单击 **Save**按钮，但如果您希望更自定义您的配置，请查看Cisco Secure Client管理员指南。

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

ISE配置

配置网络设备列表

要配置通过Cisco ISE的身份验证，您需要配置允许设备向您的Cisco ISE查询：

- 导航至 **Administration > Network Devices**
- 点击 **+ 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

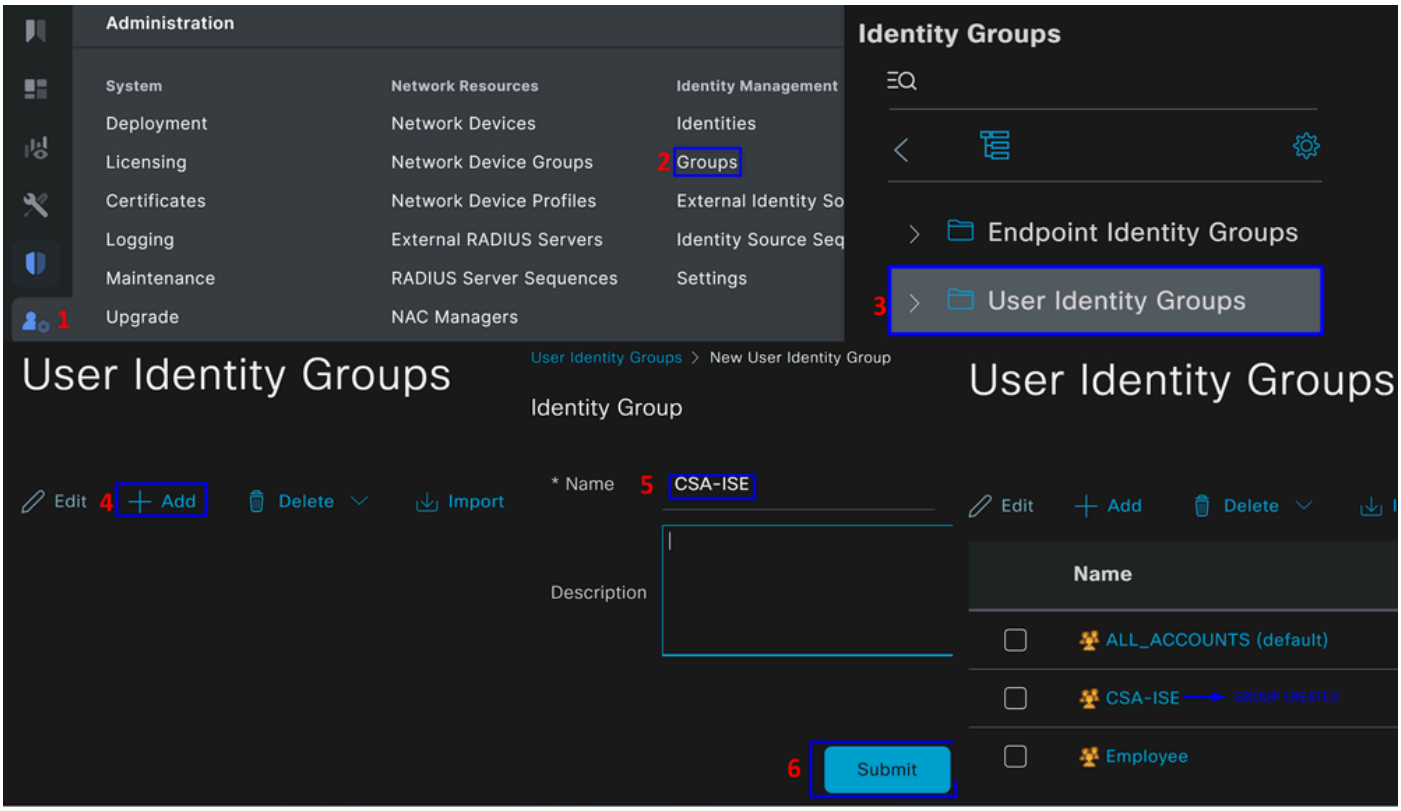
- **Name**：使用名称标识安全访问
- **IP Address**：配置IP池区域这一步骤的Management Interface
- **Device Profile**：选择思科
    - **Radius Authentication Settings**
        - Shared Secret：配置在步骤中配置的相同共享密钥：密钥
            - **CoA Port**：将其设置为默认值；1700也用于安全访问

之后，点击**Save**以验证集成是否正常工作，请继续创建本地用户进行集成验证。

配置组

要配置用于本地用户的组，请继续执行以下步骤：

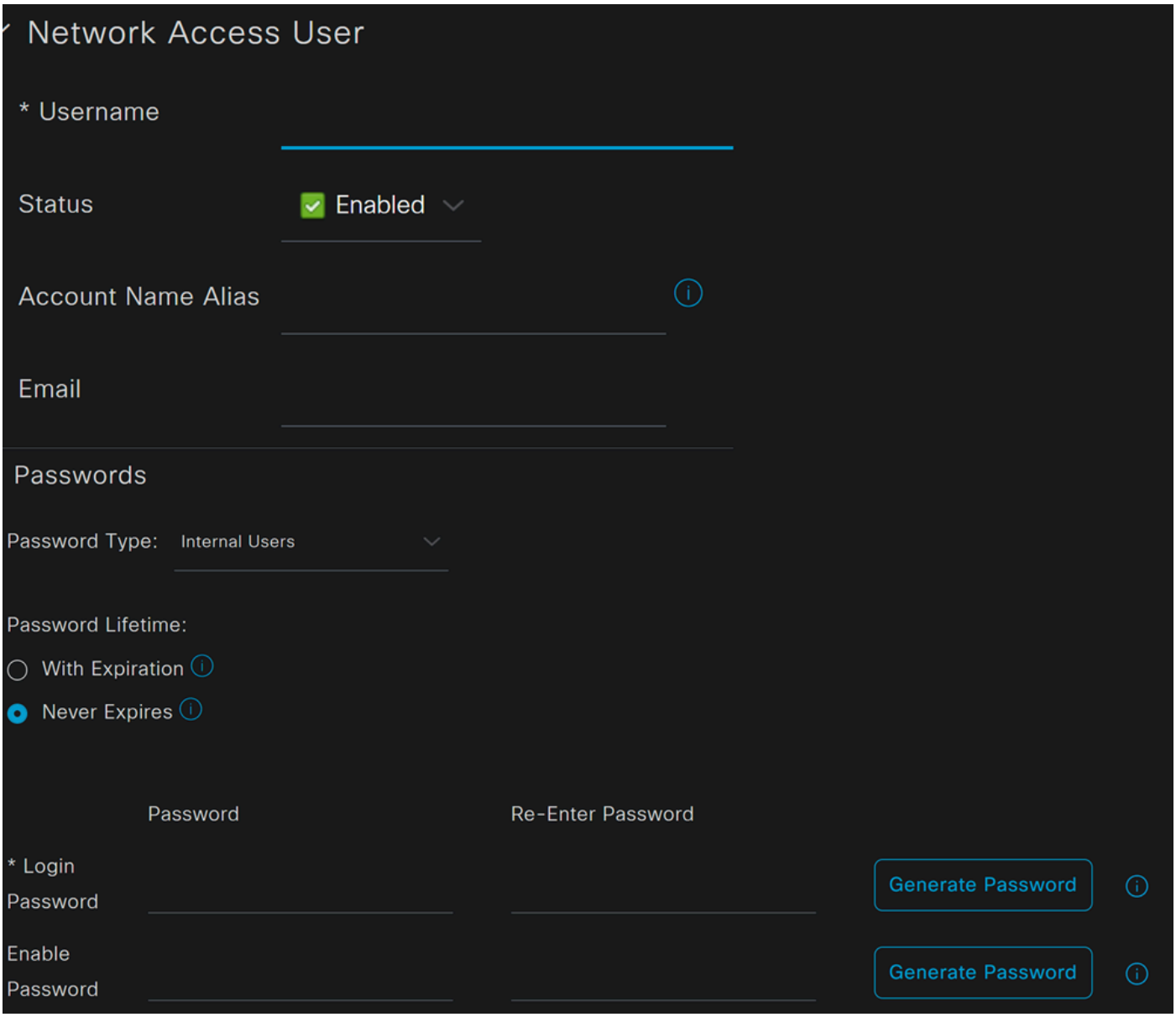
- 点击 **Administration > Groups**
- 点击 **User Identity Groups**
- 点击 + Add
- 为组创建Name并点击 **Submit**

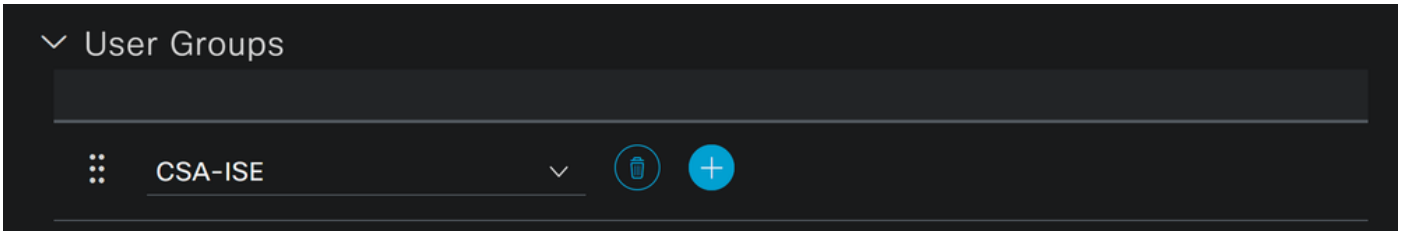


配置本地用户

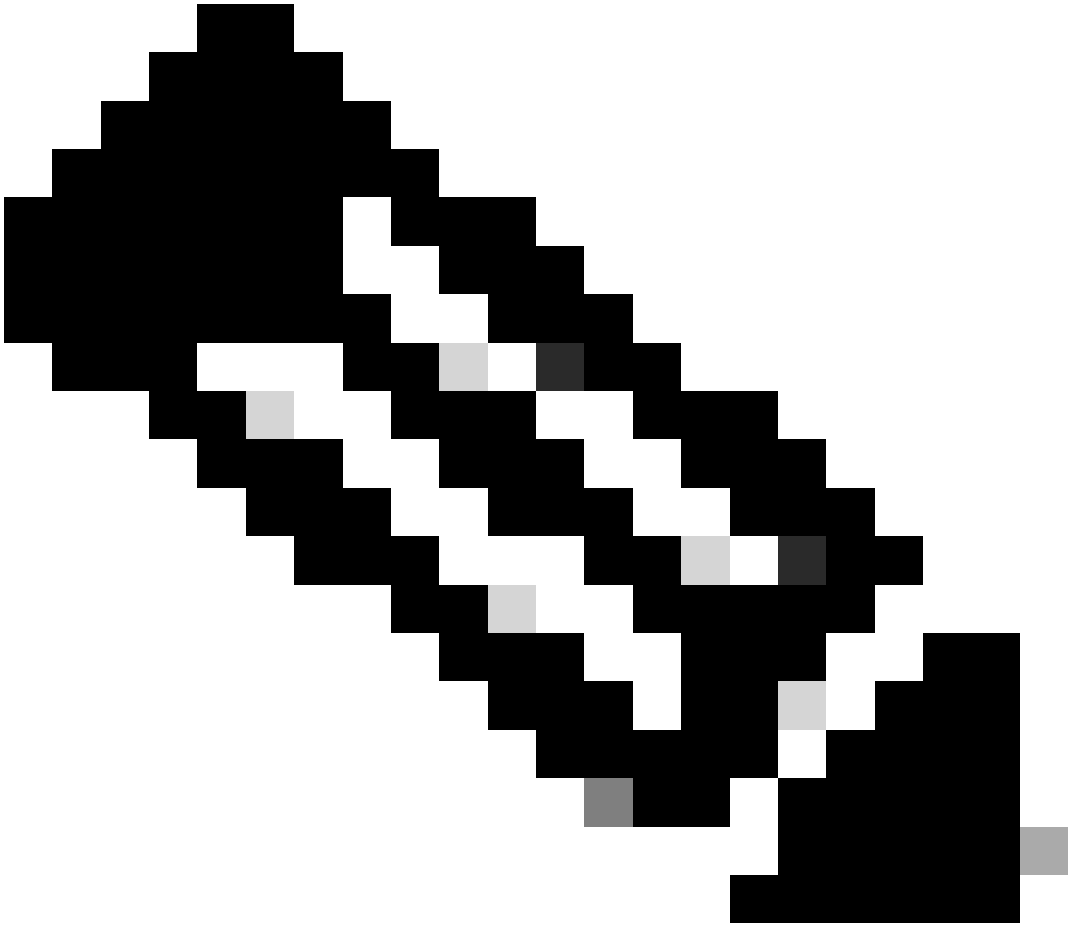
要配置本地用户以验证集成，请执行以下操作：

- 导航至 **Administration > Identities**
- 点击 **Add +**





- **Username**：使用安全访问中的已知UPN调配配置用户名；这基于步骤前提条件
- **Status**：活动
- **Password Lifetime**：您可以配置它**With Expiration** 或Never Expires，具体取决于您
- **Login Password**：为用户创建密码
- **User Groups**：选择在步骤Configure a Group中创建的组



注意：基于UPN的身份验证被设置为在即将推出的安全访问版本中更改。

之后，您可以**Save** 进行配置并继续执行 **Configure Policy Set**步骤。

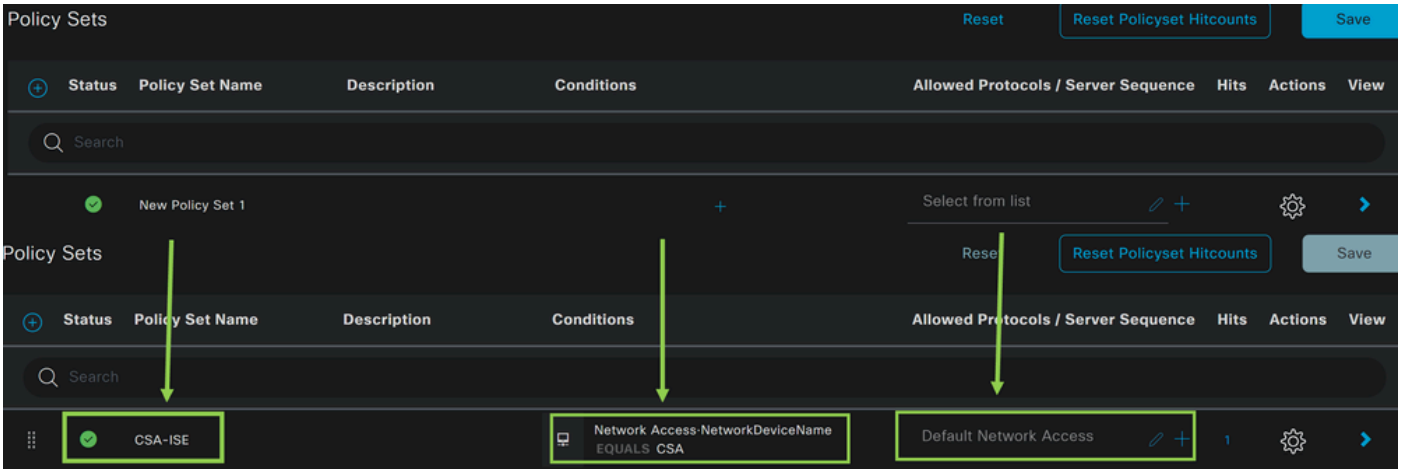
配置策略集

在策略集下，配置ISE在身份验证和授权过程中执行的操作。此场景演示了将简单策略配置为提供用户访问权限的使用案例。首先，ISE验证RADIUS身份验证的来源，并检查ISE用户数据库中是否存在提供访问权限的身份

要配置该策略，请导航到您的Cisco ISE控制面板：

- 点击 Policy > Policy Sets

- 点击+ 以添加新策略集

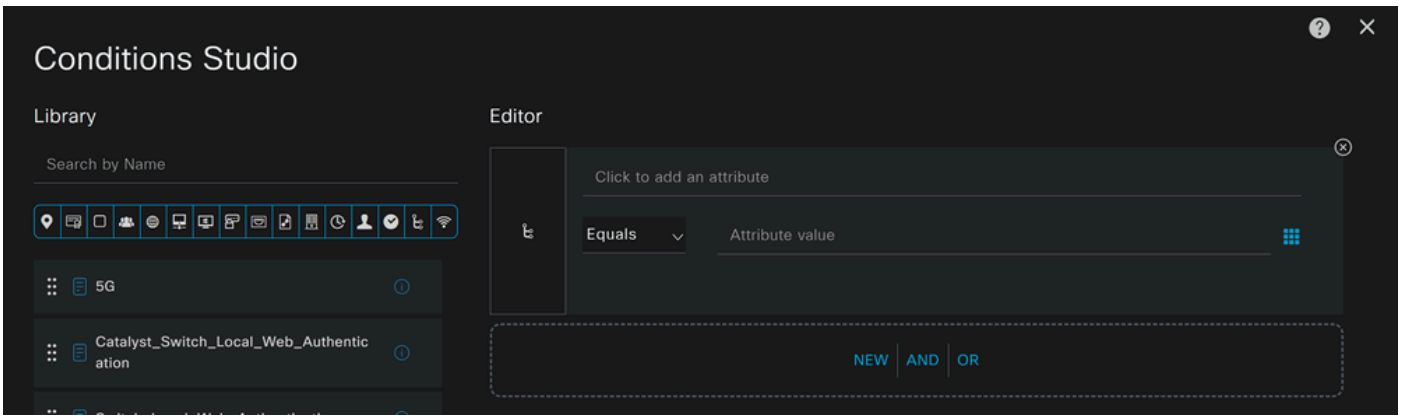


在这种情况下，请创建新的策略集，而不是使用默认策略集。接下来，根据该策略集配置身份验证和授权。已配置的策略允许访问在[配置网络设备列表]步骤中定义的网络设备，以验证这些身份验证是否来自CSA Network Device List，然后以**Conditions**身份进入策略。最后是允许的协议，如**Default Network Access**。

要创建与策略集匹配的**condition** 策略，请按照以下说明继续操作：

- 点击 +

- 在 **Condition Studio**下，可用的信息包括：



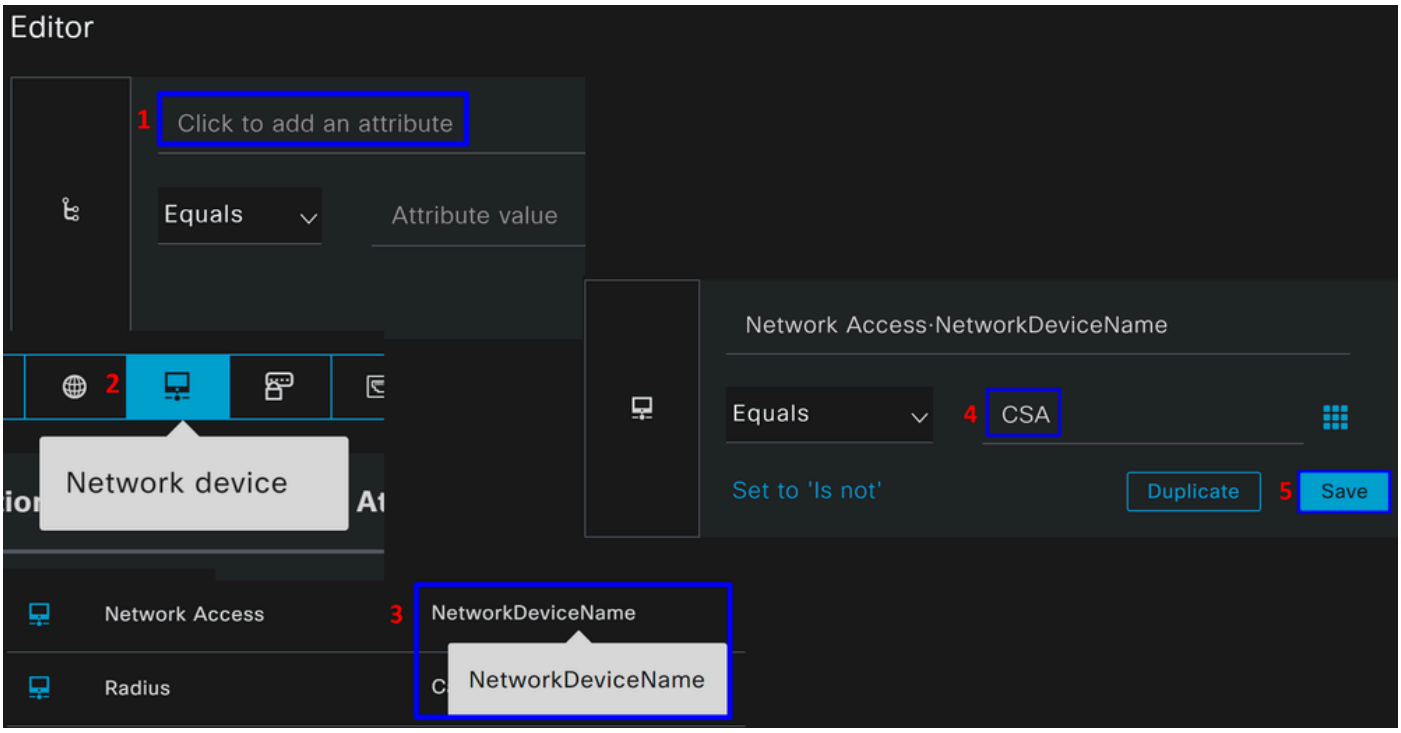
- 要创建条件，请点击 Click to add an attribute

- 点击**Network Device** 按钮

- 在后面的选项下，单击**Network Access - 选Network Device Name** 项

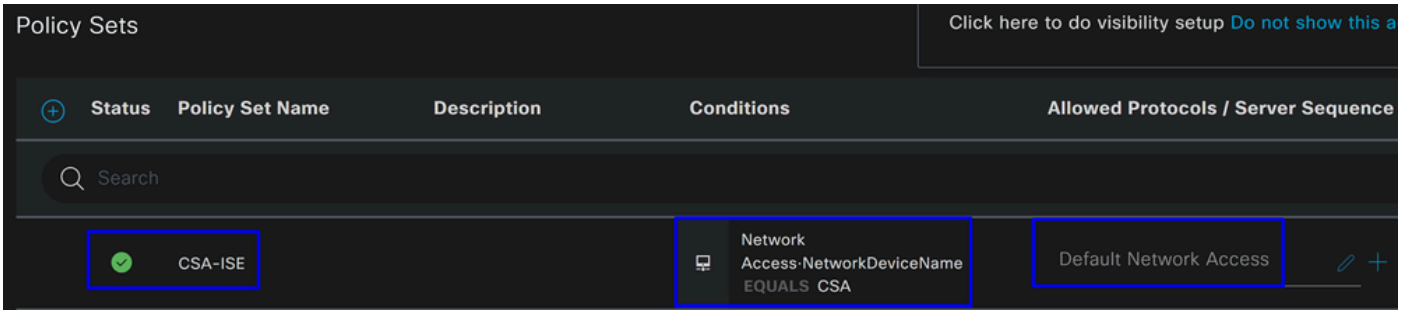
- 在Equals选项下，在[Configure Network Devices List]步骤下写入**Network Device** 的名称

- 点击 **Save**

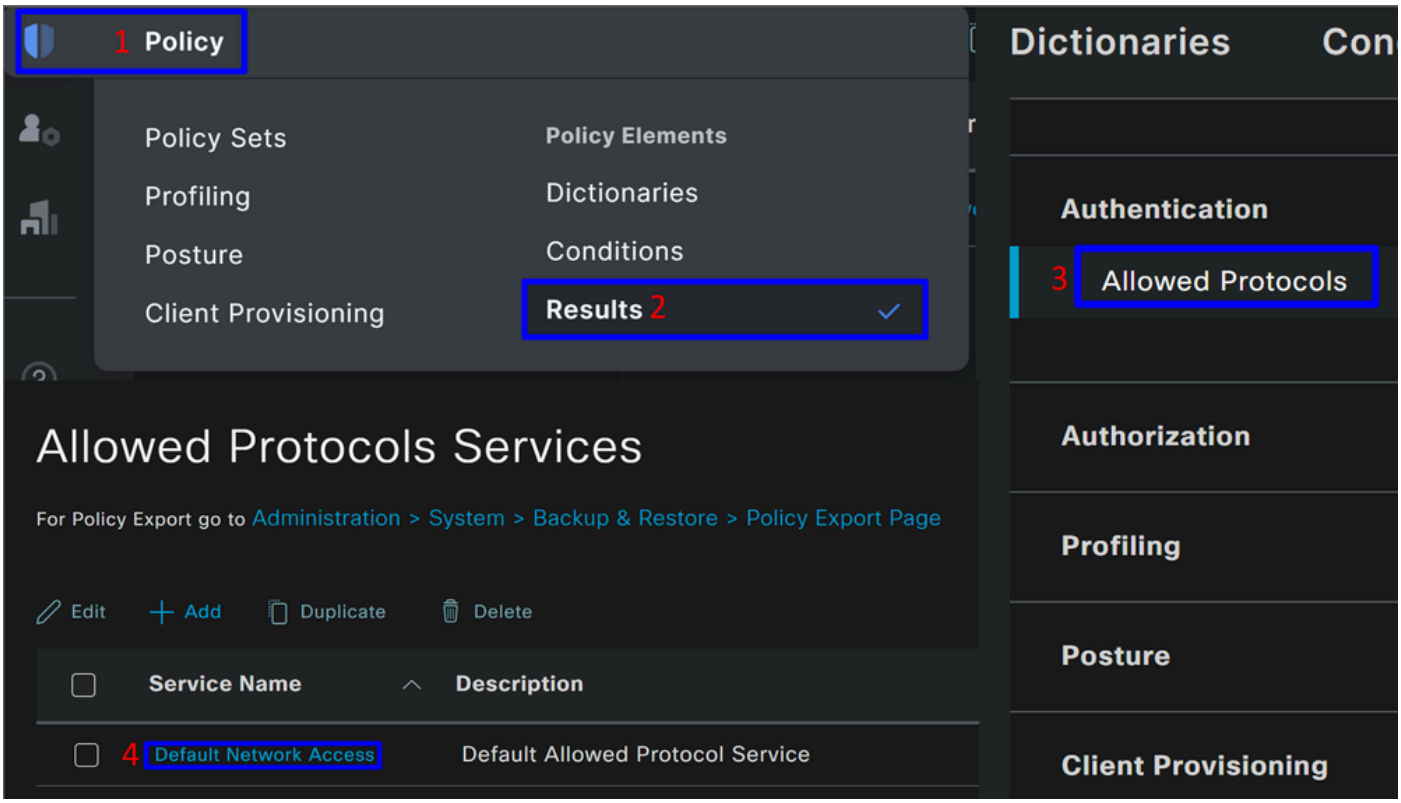


此策略仅批准来自源的CSA请求，以继续策略集 **CSA-ISE**下的**Authentication** 和**Authorization** 设置，并且还会验证根据允许的协议 **Default Network Access** 而允许的协议。

定义的策略的结果必须是：



- 要验证允许**Default Network Access Protocols** 的，请继续下一说明：
    - 点击Policy > Results
        - 点击 **Allowed Protocols**
        - 点击 **Default Network Access**

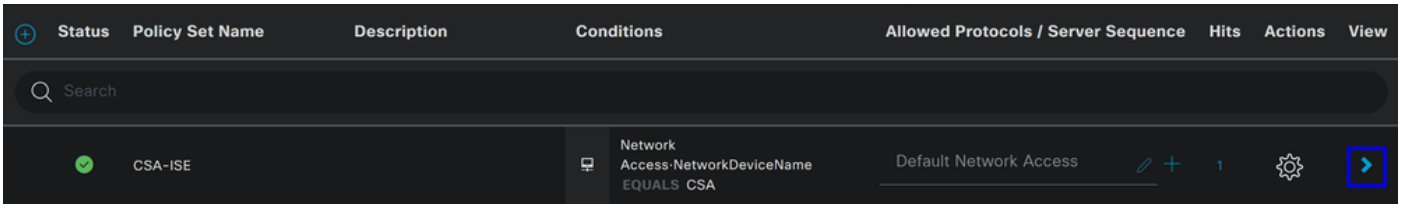


- 然后，您会看到允许的所有协议 **Default Network Access**

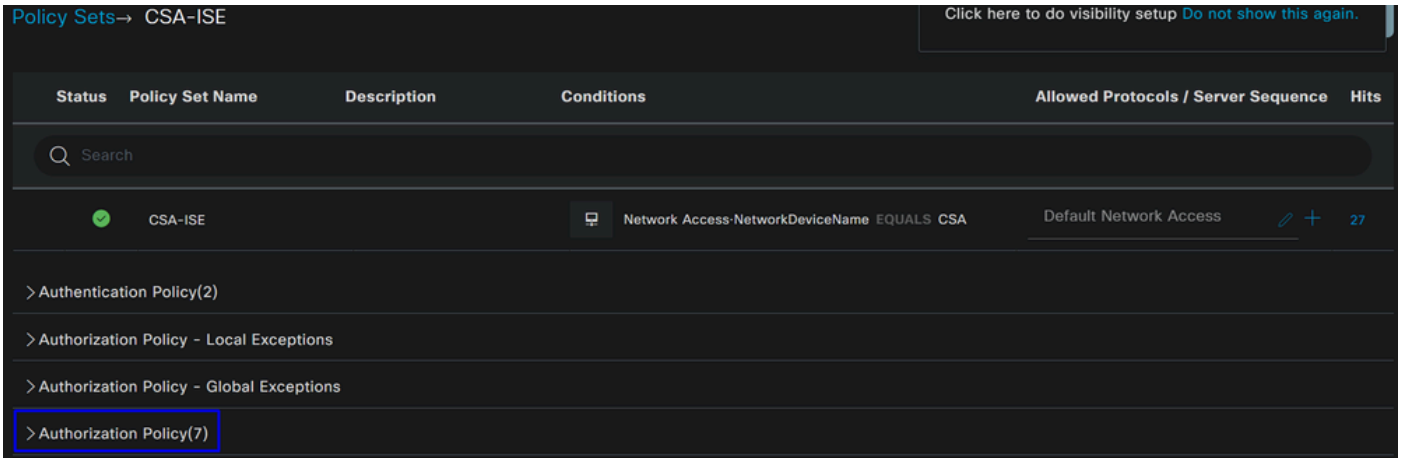
配置策略集授权

要在 **Policy Set**下创建**Authorization** 策略，请执行以下步骤：

- 点击 >



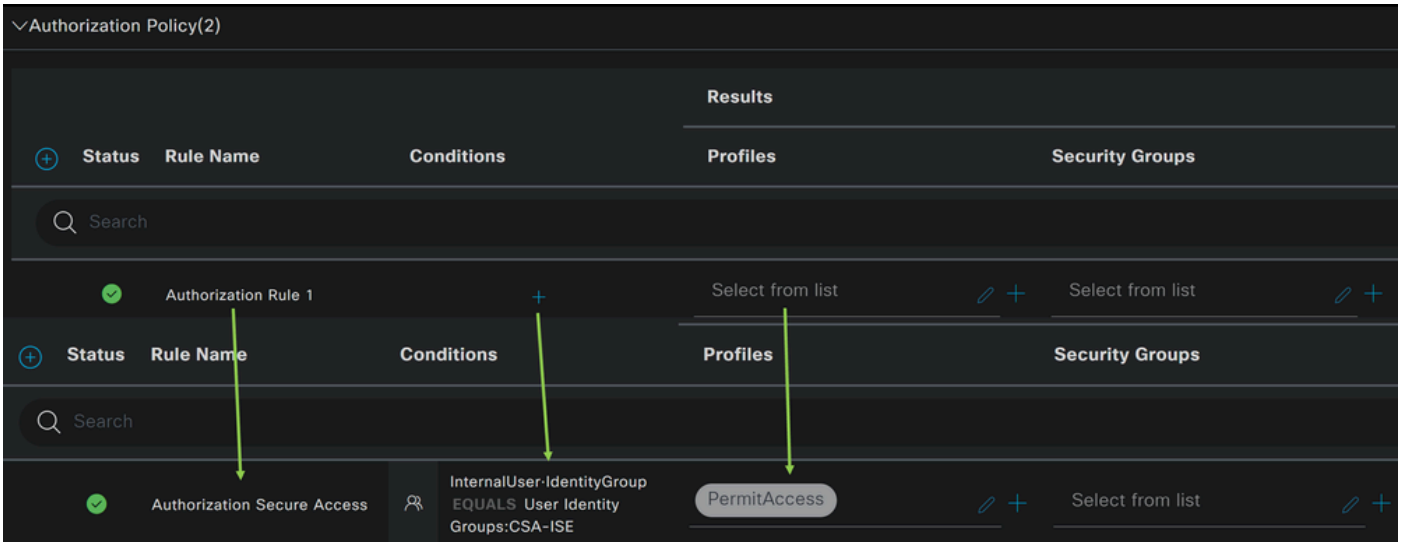
- 之后，您会看到显示**Authorization** 的策略：



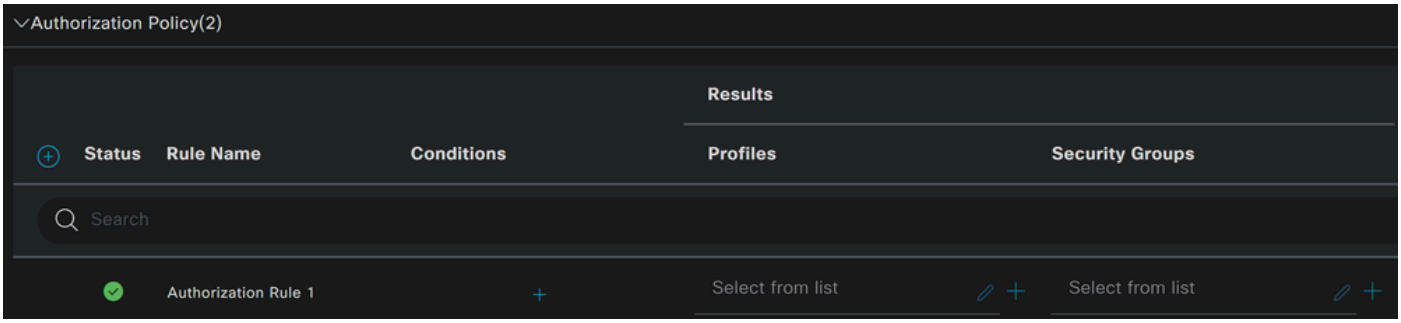
该策略与配置策略集步骤中定义的策略相同。

授权策略

您可以通过多种方式配置授权策略。在这种情况下，仅授权在配置组步骤中定义的组中的用户。请参阅以下配置授权策略的示例：

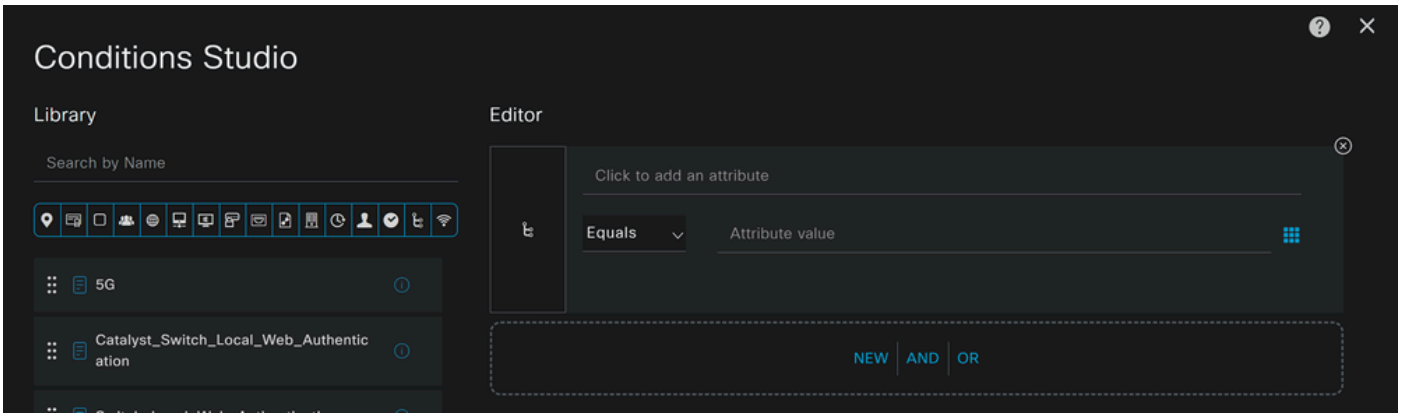


- 点击 **Authorization Policy**
- 点击+ 以定义授权策略，如下所示：

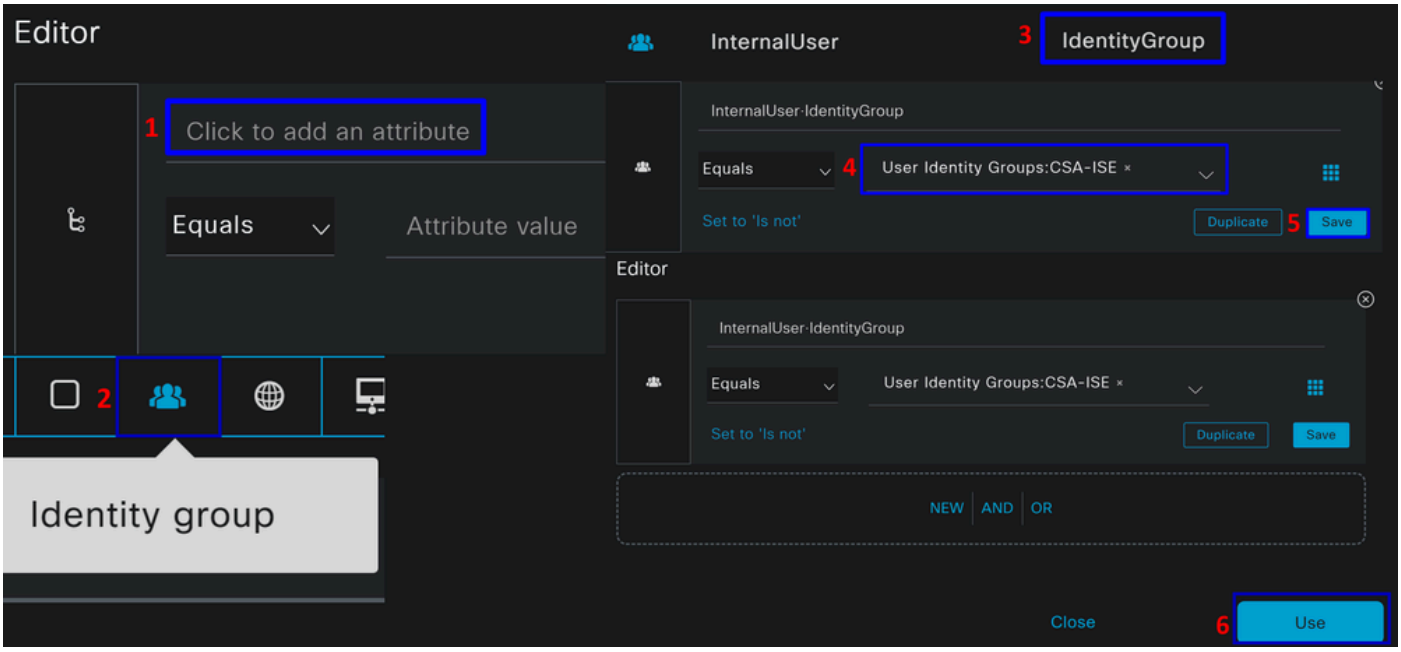


- 对于下一步，请更改Rule Name，和Conditions Profiles

- 设置**Name** 配置名称以轻松识别授权策略时
- 要配置 **Condition**命令，请点击 +
- 在 **Condition Studio**下，您可以找到以下信息：



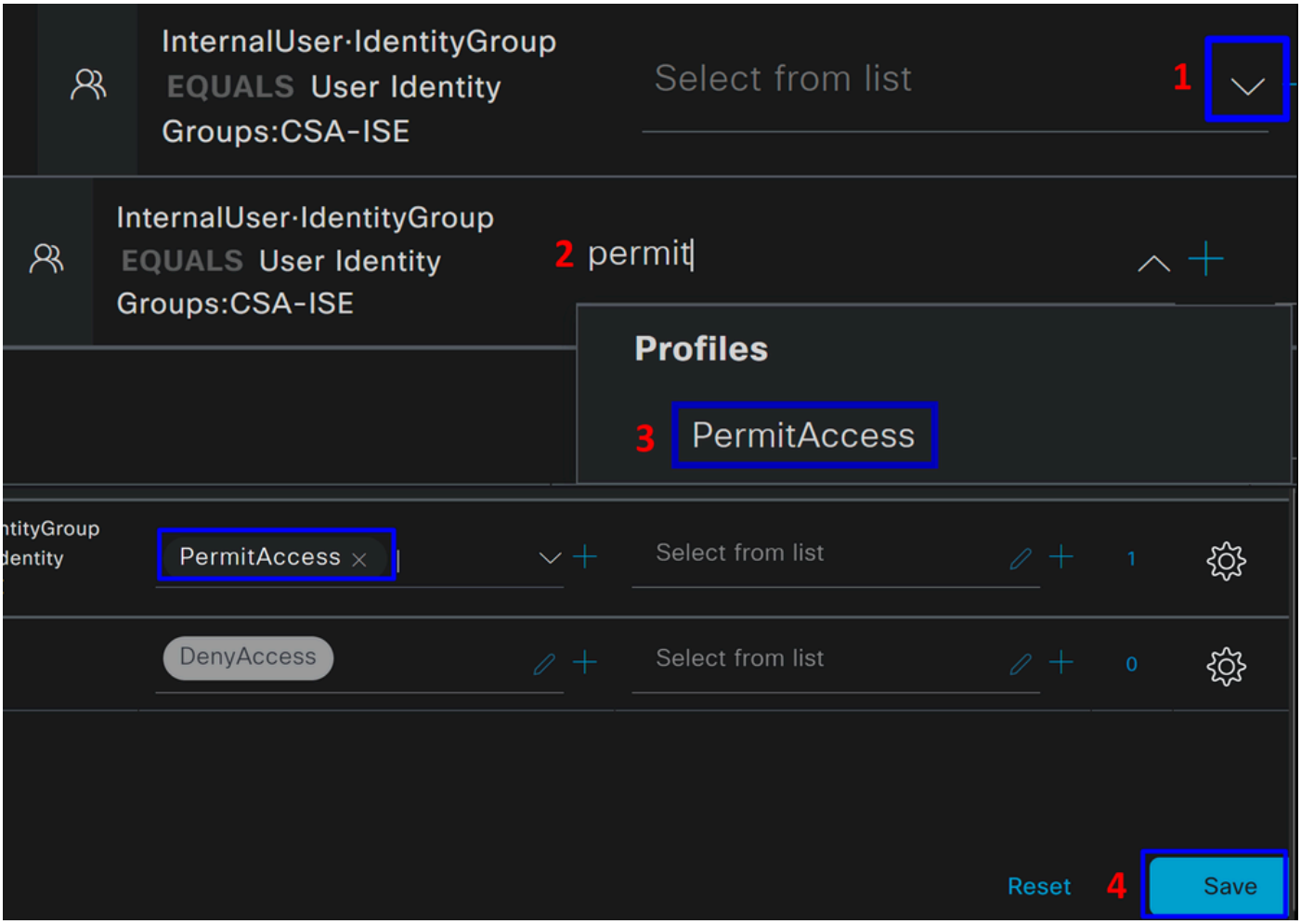
- 要创建条件，请点击 Click to add an attribute
- 点击**Identity Group** 按钮
- 在后面的选项下，单击**Internal User -IdentityGroup** 选项
- 在**Equals** 选项下，使用下拉列表查找步骤[配置组](#)中的**Group** 批准进行身份验证
- 点击 **Save**
- 点击 **Use**



之后，您需要定义 **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group

selected on the policy.

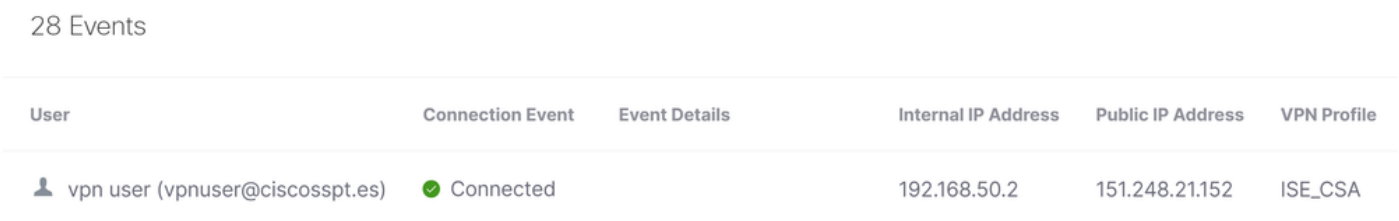
- 在 **Authorization Policy**下，单击 **Profiles**
- 搜索允许
- 选择 **PermitAccess**
- 点击 Save



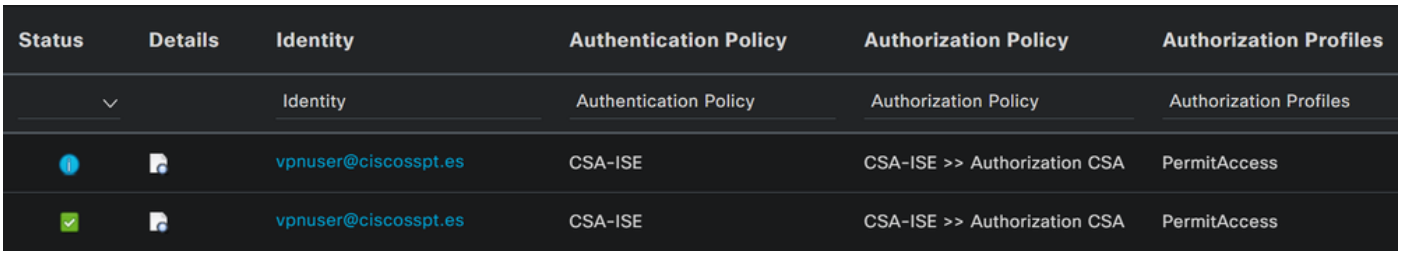
之后，您定义了 **Authorization** 策略。进行身份验证，验证用户连接是否正常，以及您是否能够看到安全访问和ISE上的日志。

要连接到VPN，您可以使用在Secure Access上创建的配置文件，并通过Secure Client与ISE配置文件连接。

- 当身份验证获得批准时，日志如何显示在安全访问中？
  - 导航到安全访问控制面板
  - 点击 **Monitor > Remote Access Log**

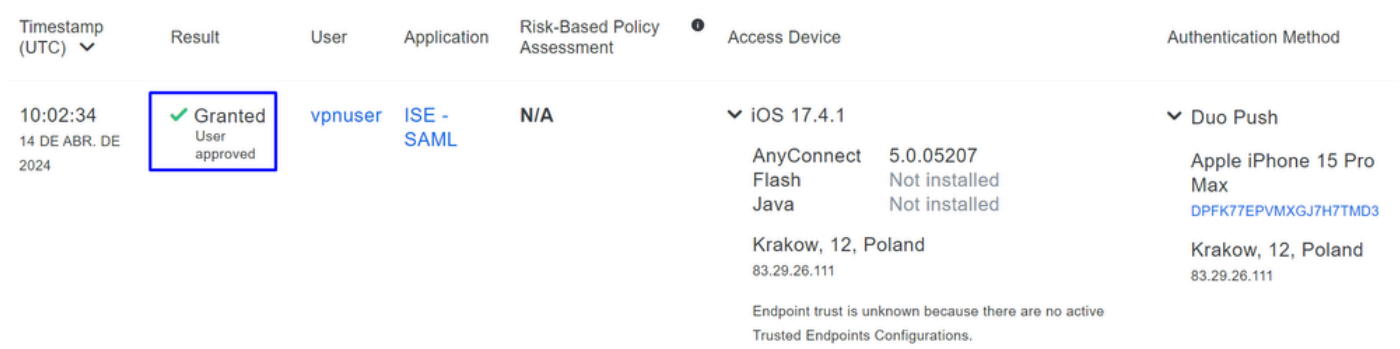


- 当身份验证获得批准时，日志在**ISE**中如何显示？
  - 导航至 **Cisco ISE Dashboard**
    - 点击 **Operations > Live Logs**



当身份验证获得批准时，如何在**Duo**中显示日志？

- 导航到双核管理面板
- 点击 **Reports > Authentication Log**



配置Radius本地或Active Directory用户

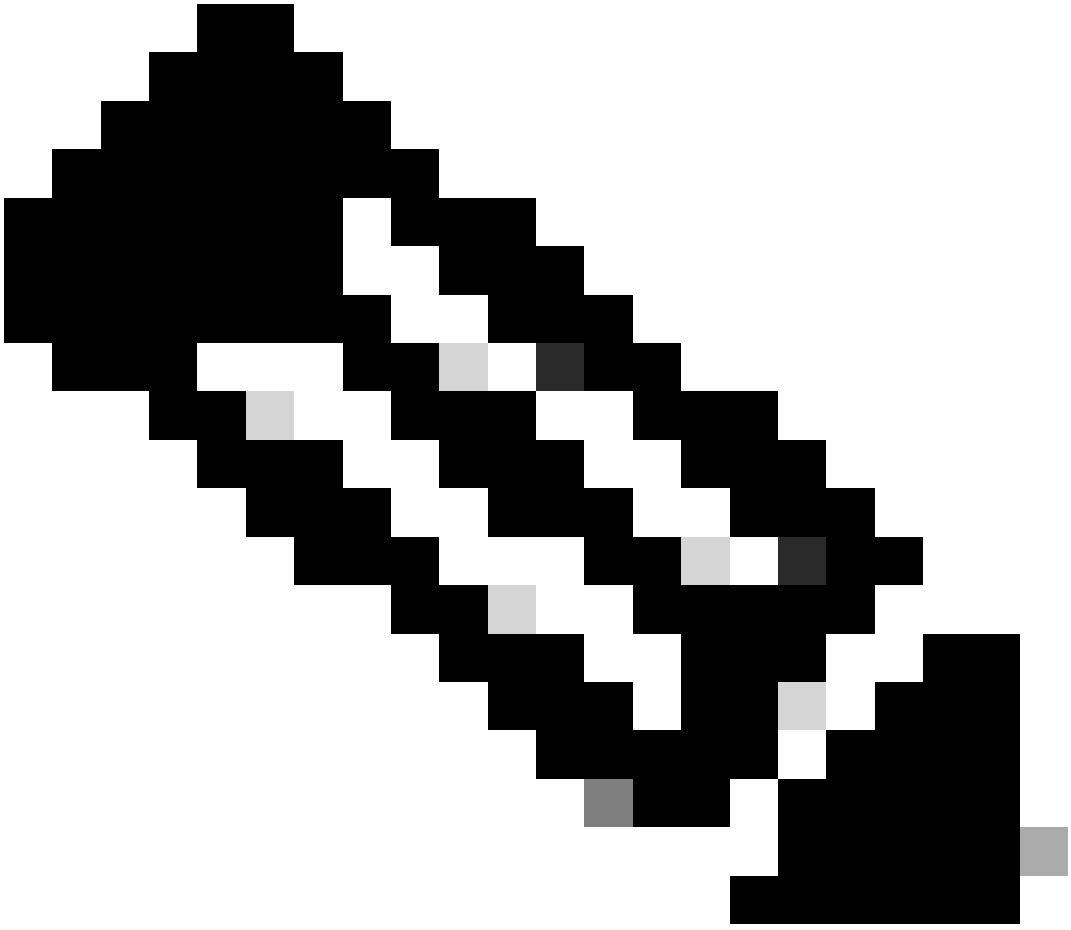
配置ISE安全评估

在这种情况下，请创建配置以在授予或拒绝对内部资源的访问权限之前验证终端合规性。

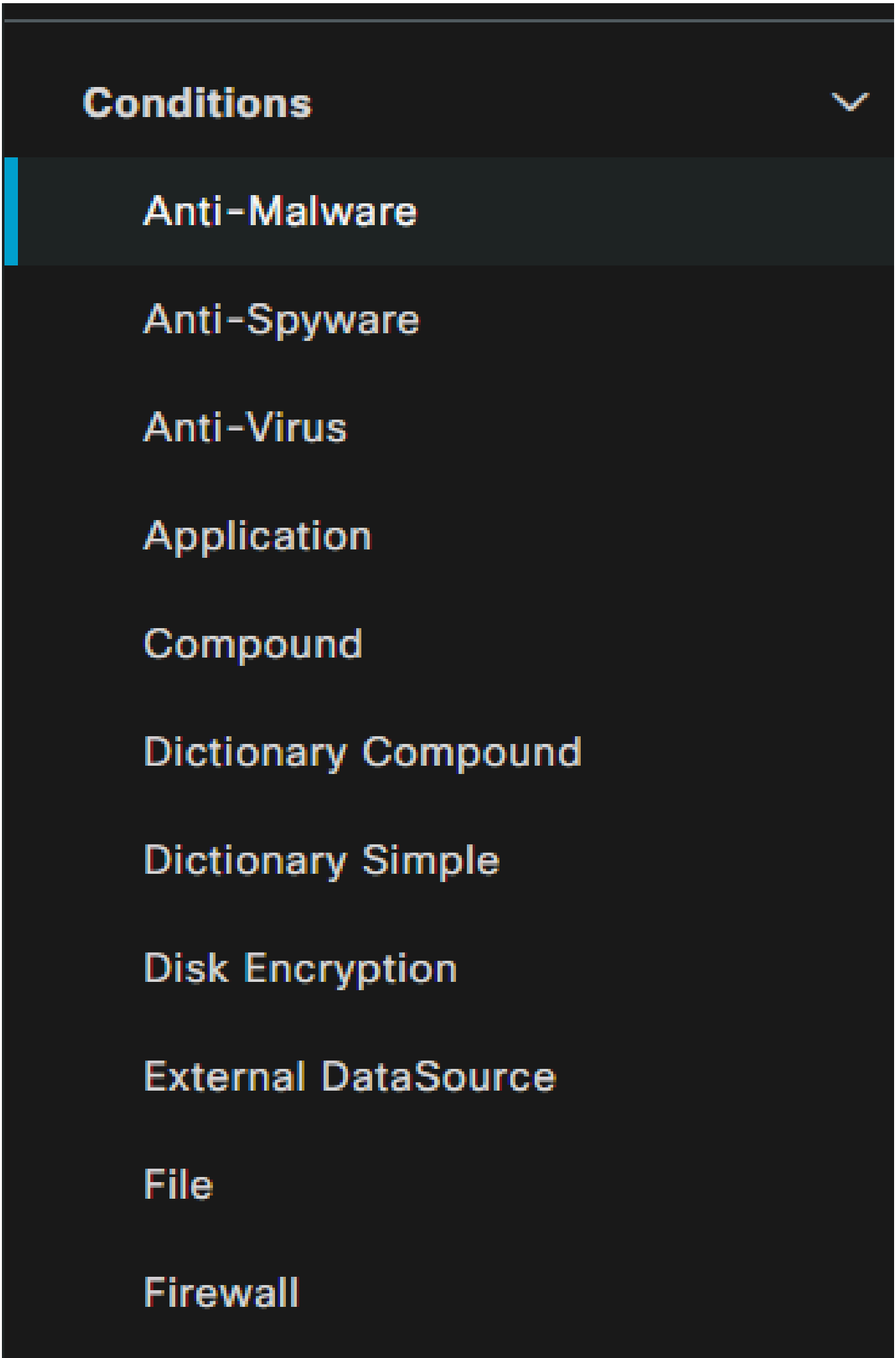
要进行配置，请继续执行以下步骤：

配置终端安全评估条件

- 导航到ISE控制面板
- 点击 **Work Center > Policy Elements > Conditions**
- 点击 **Anti-Malware**



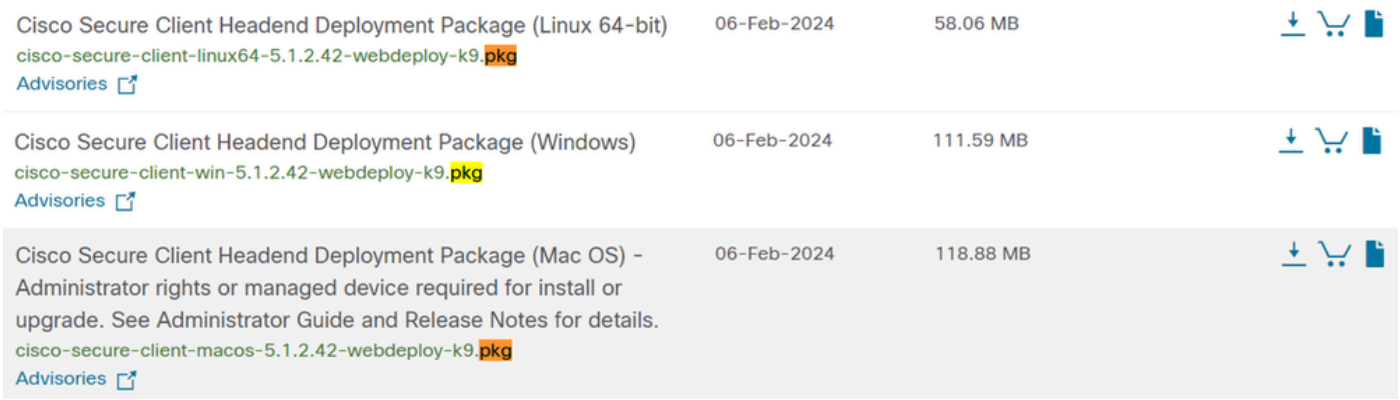
注意：您可以在此处找到许多选项，以验证设备的状态并根据内部策略进行正确的评估。


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

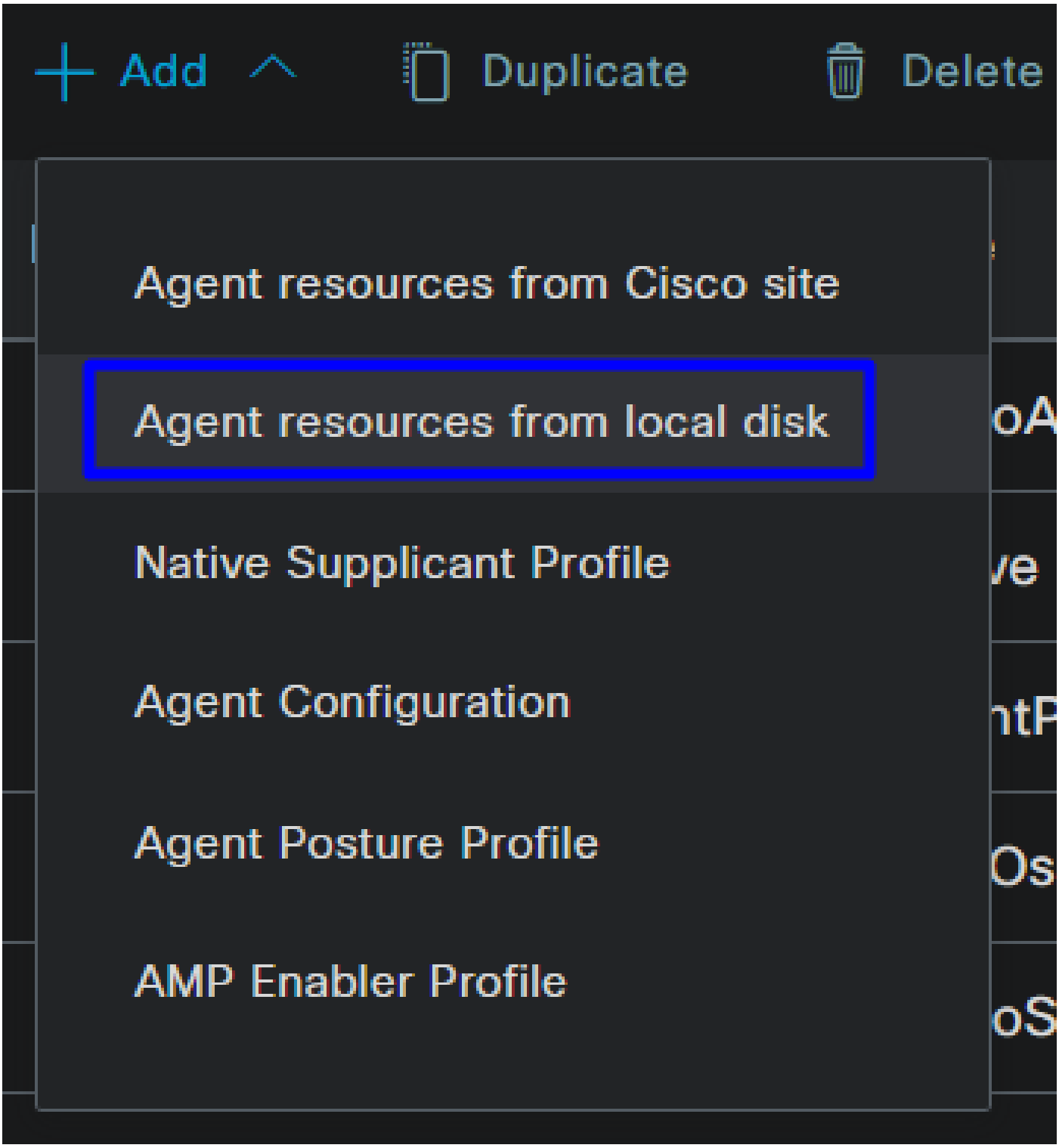
1. **Agent Resources**	安全客户端Web设置包。
2. **Compliance Module**	思科ISE合规性模块
3. **Agent Profile**	控制调配配置文件。
3. **Agent Configuration**	通过设置调配门户，使用代理配置文件和代理资源定义调配哪些模块。

Step 1 下载并上传代理资源

- 要添加新的代理资源，请导航到Cisco下载门户并下载Web部署软件包；Web部署文件必须是.pkg格式。

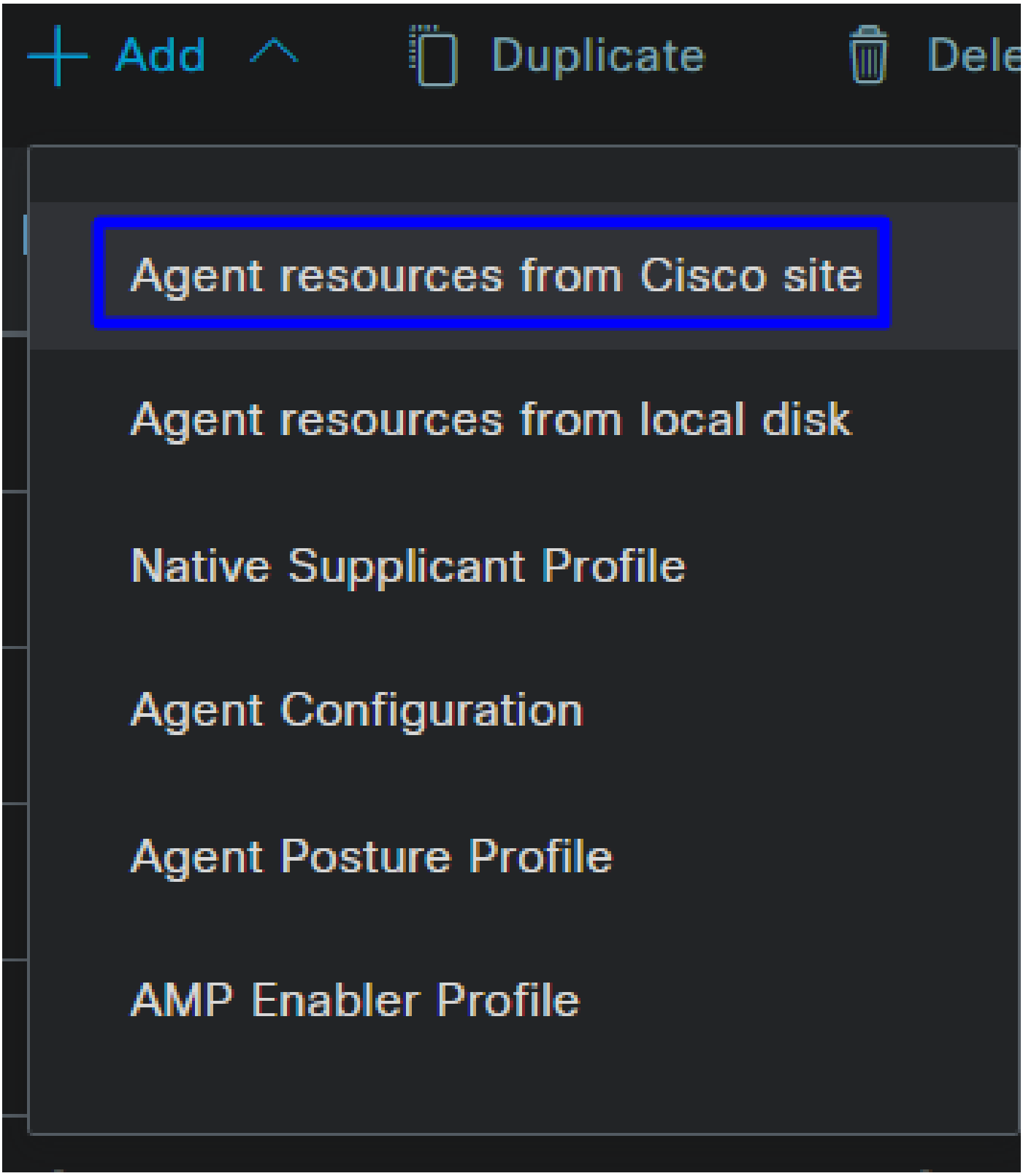


- 点击+ Add > Agent resources from local disk 并上传包

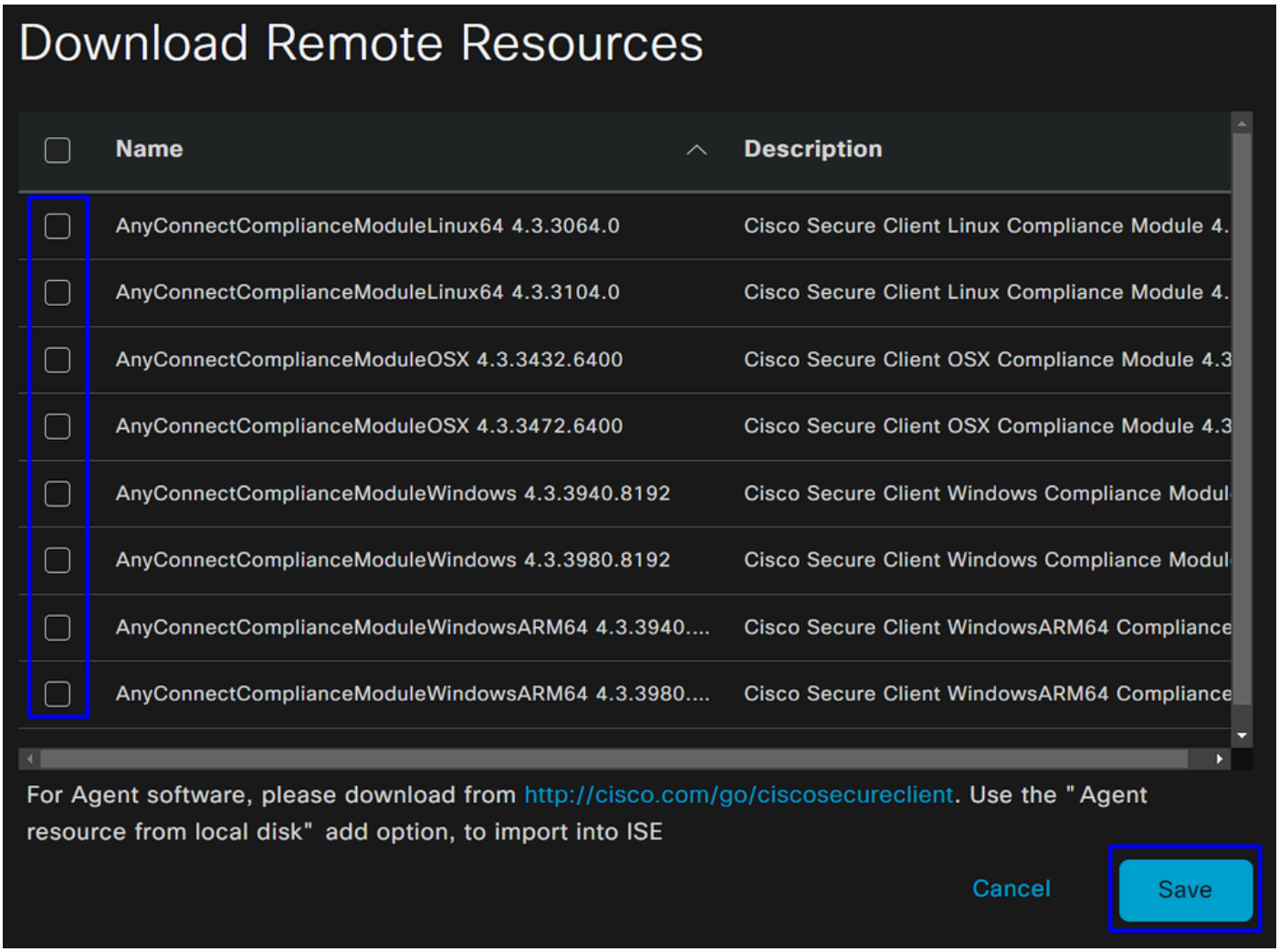


Step 2下载合规性模块

- 点击 + Add > Agent resources from Cisco Site

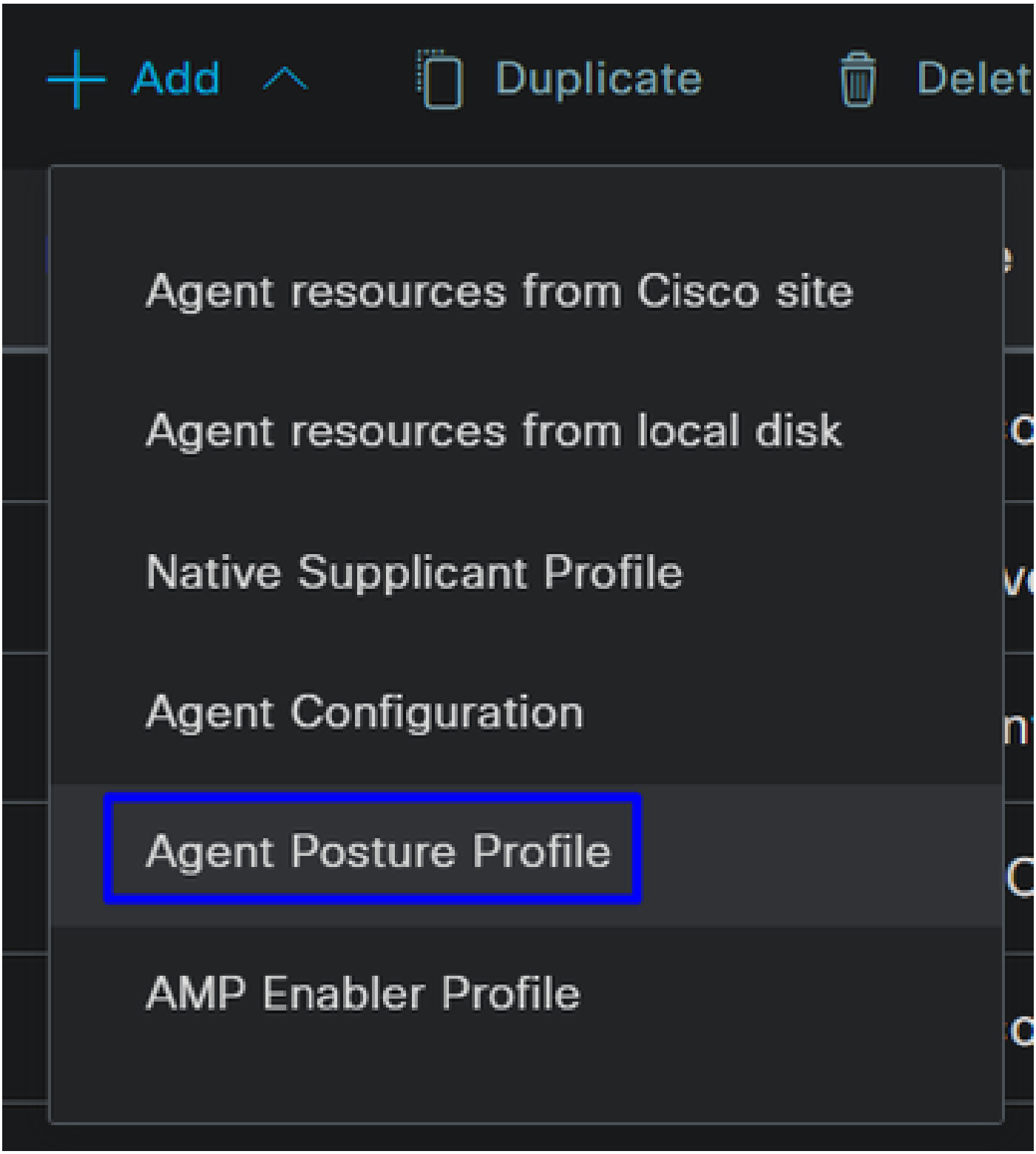


- 选中所需每个合规性模块的复选框，然后点击 **Save**

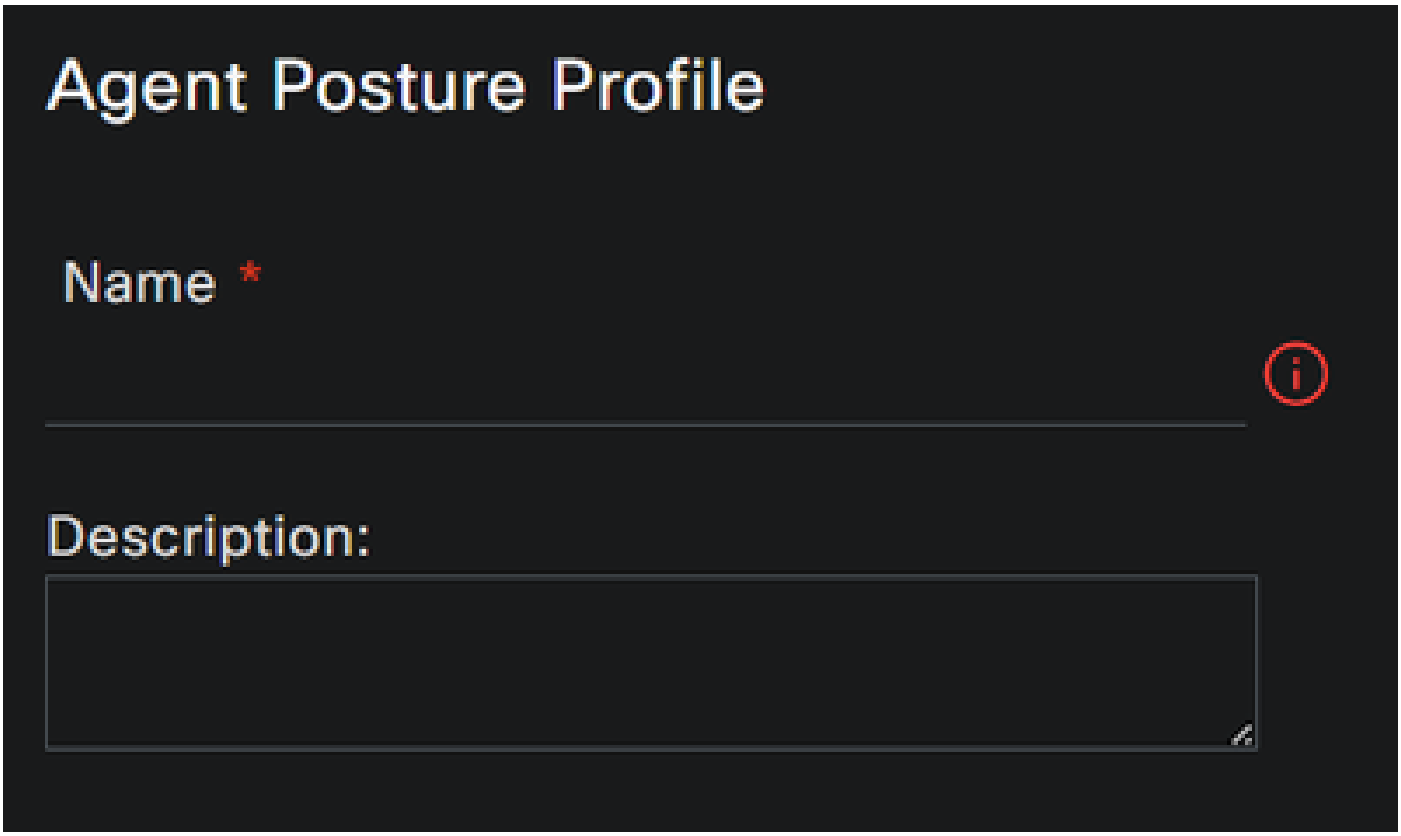


Step 3配置代理配置文件

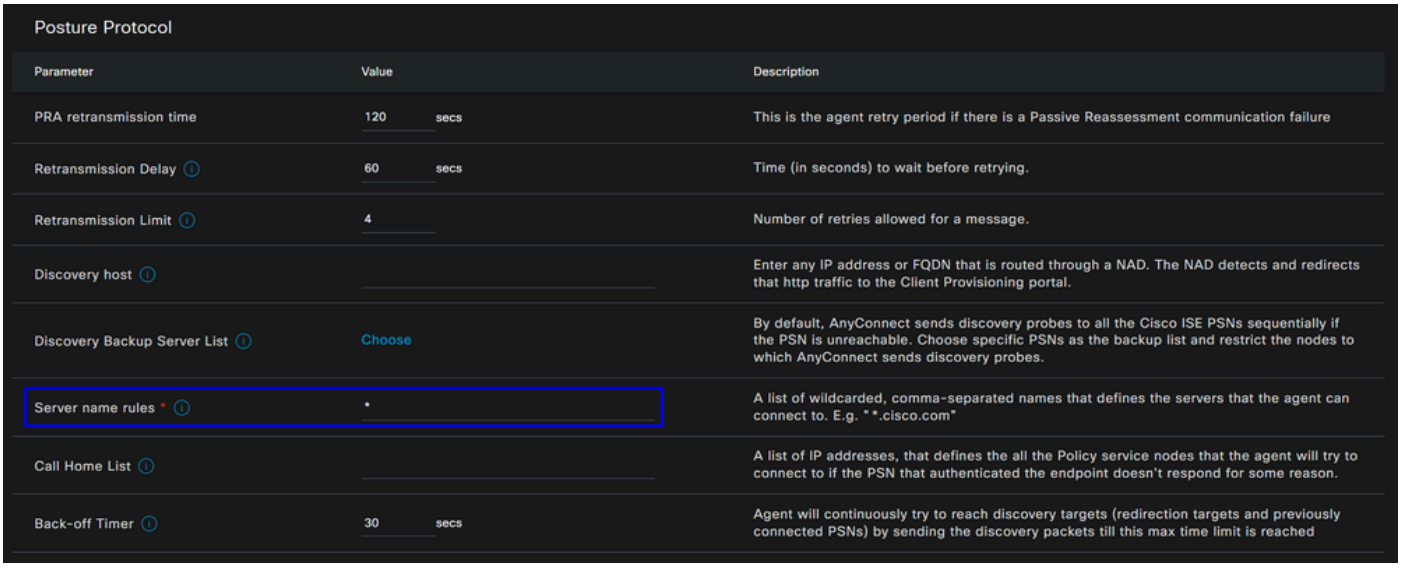
- 点击 + Add > Agent Posture Profile



- 为创建**Name** 一个 **Posture Profile**

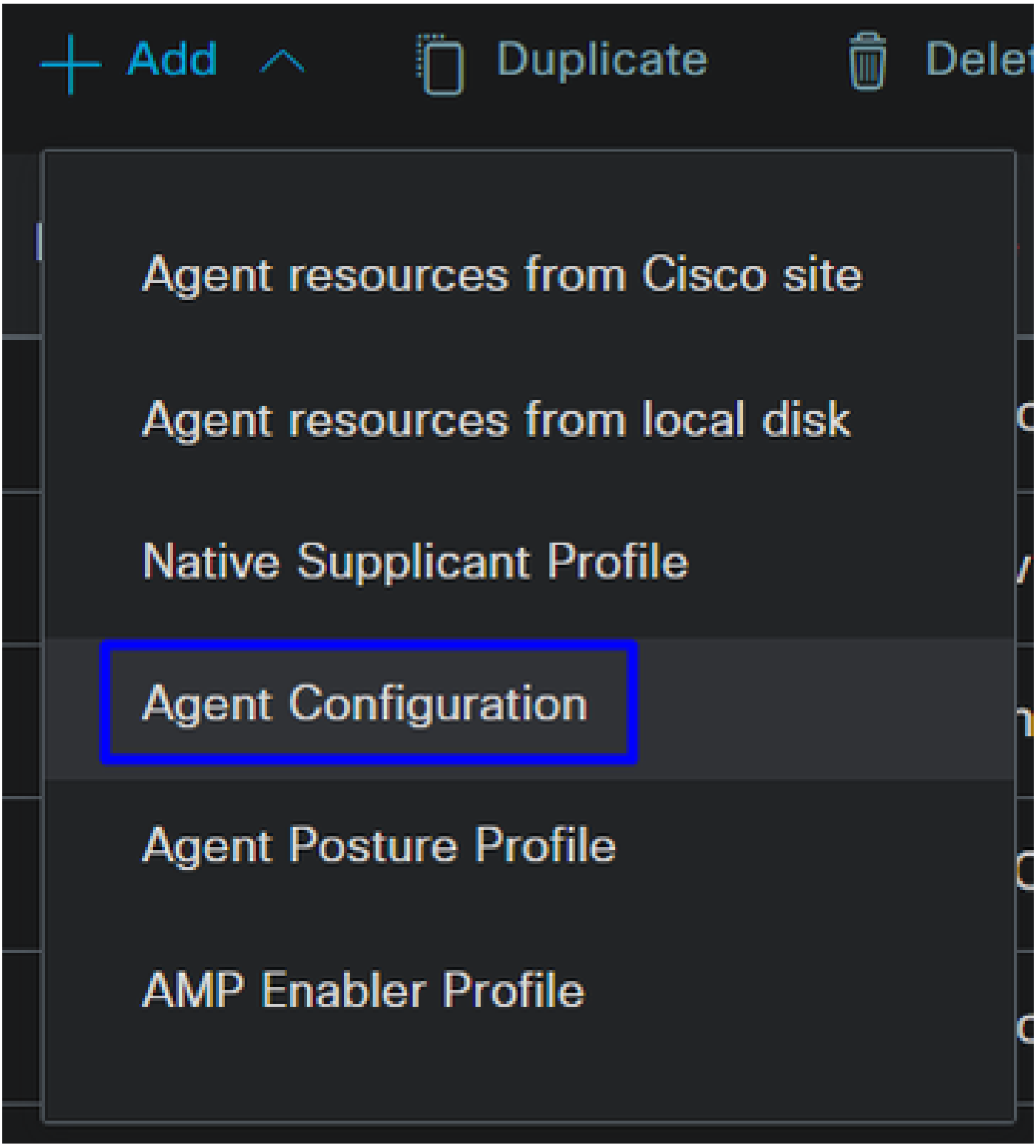


- 在“服务器名称规则”下，输入* 并在后面单击**Save**

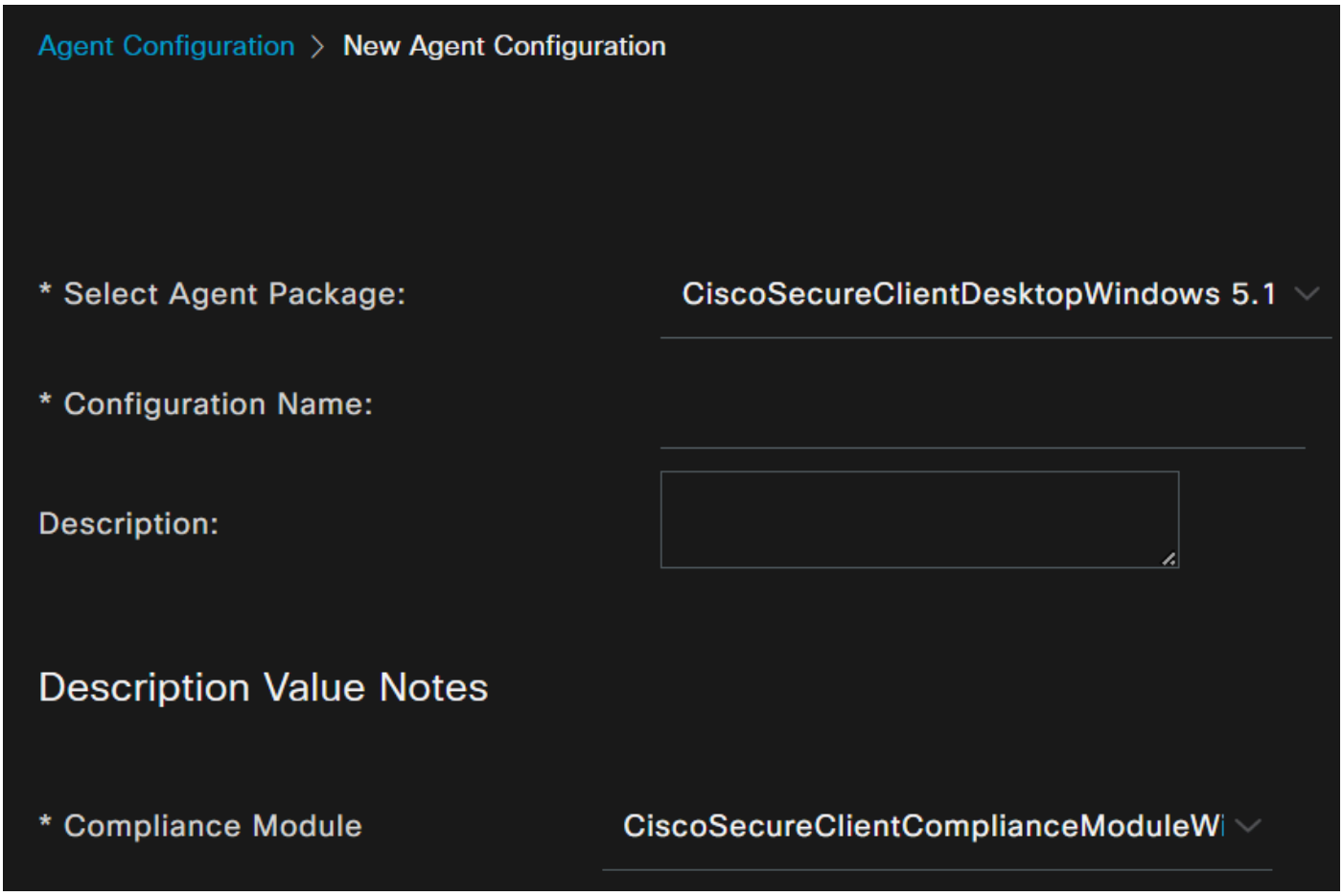


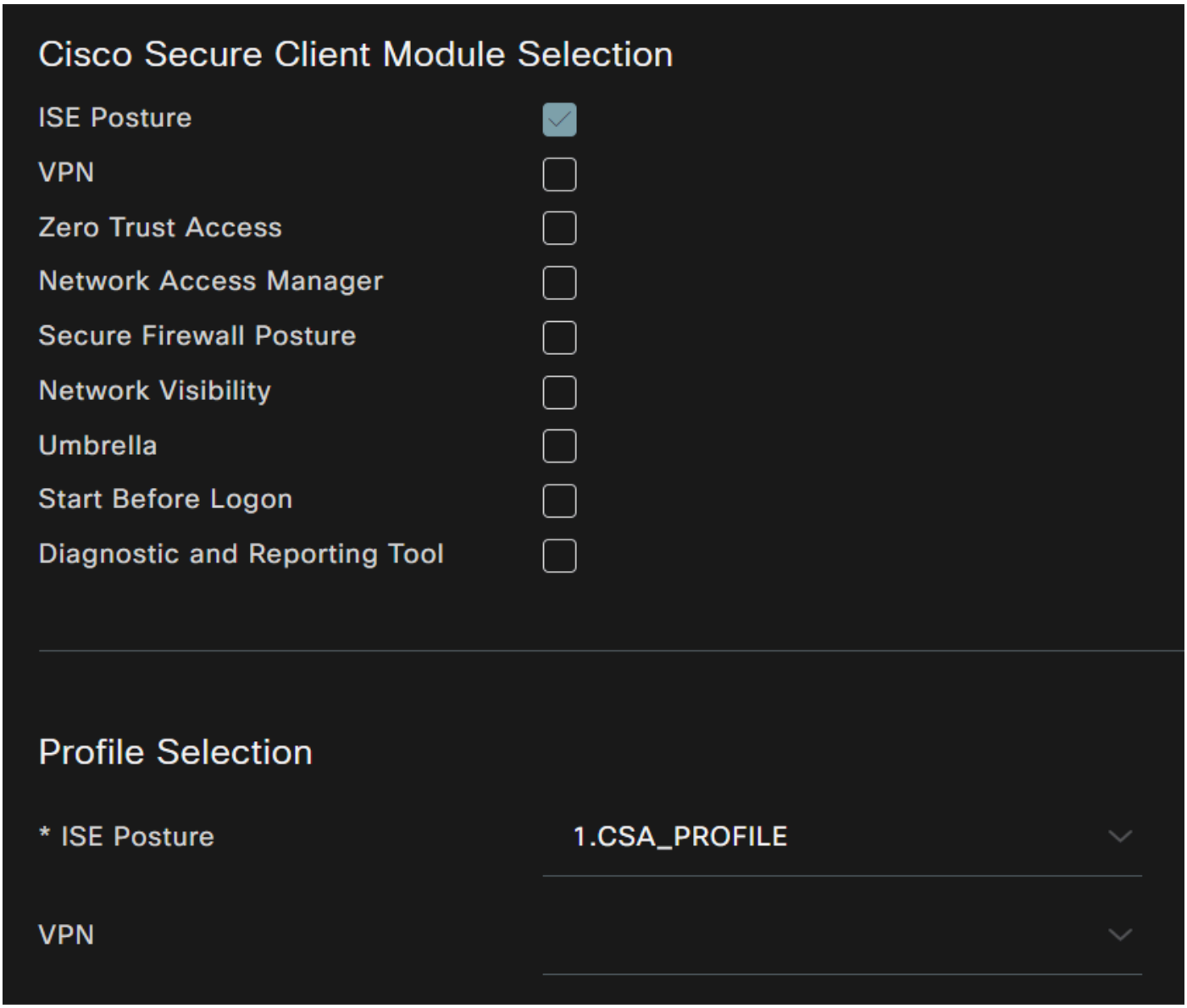
Step 4 配置代理配置

- 点击 + Add > Agent Configuration


Add
Duplicate
Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
Agent Configuration
Agent Posture Profile
AMP Enabler Profile

- 之后，配置以下参数：

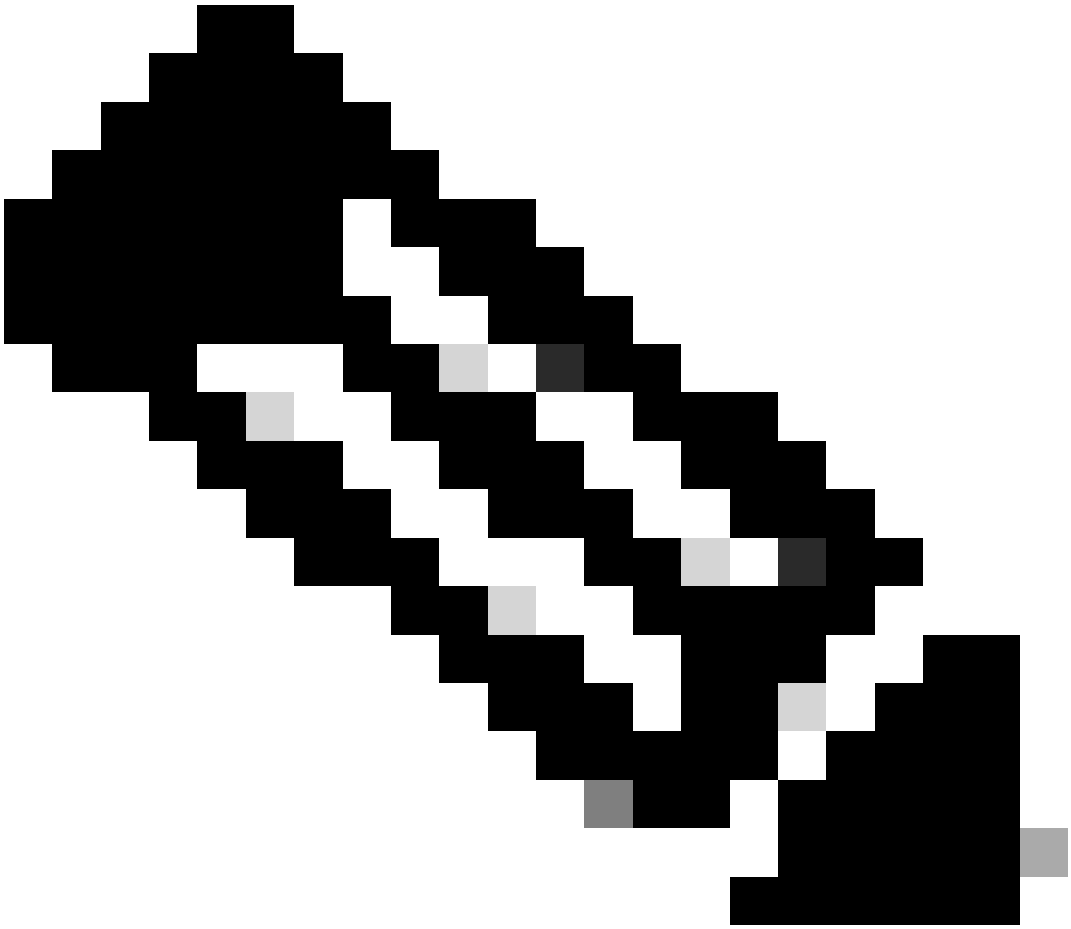

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package ：选择上传到步骤1下载和上传代理资源的包
- **Configuration Name**：选择一个名称以识别 **Agent Configuration**
- **Compliance Module**：选择在步骤2下载合规性模块上下载的合规性模块
- Cisco Secure Client Module Selection
  - **ISE Posture**：标记复选框
- **Profile Selection**

- **ISE Posture**：选择在步骤3配置代理配置文件上配置的ISE配置文件

- 点击 **Save**

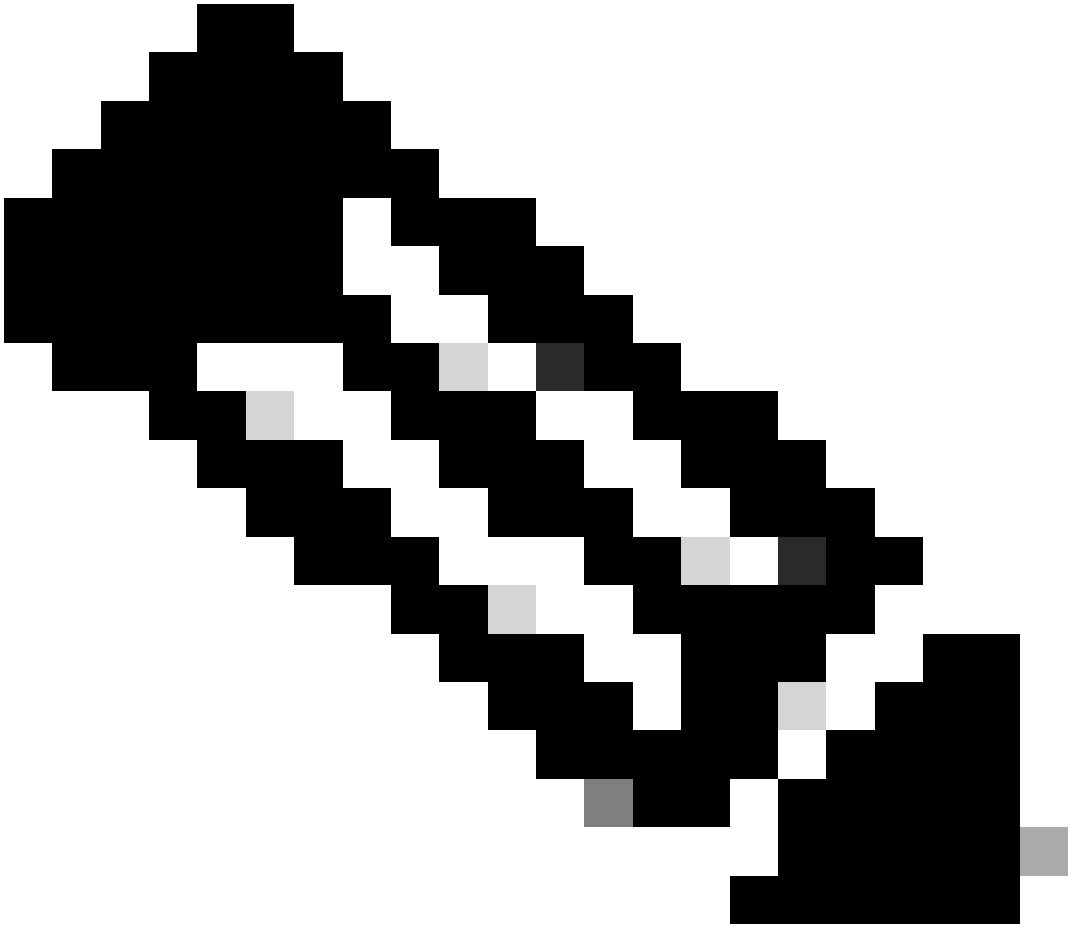


注意：建议每个操作系统（Windows、Mac OS或Linux）都有一个独立的客户端配置。

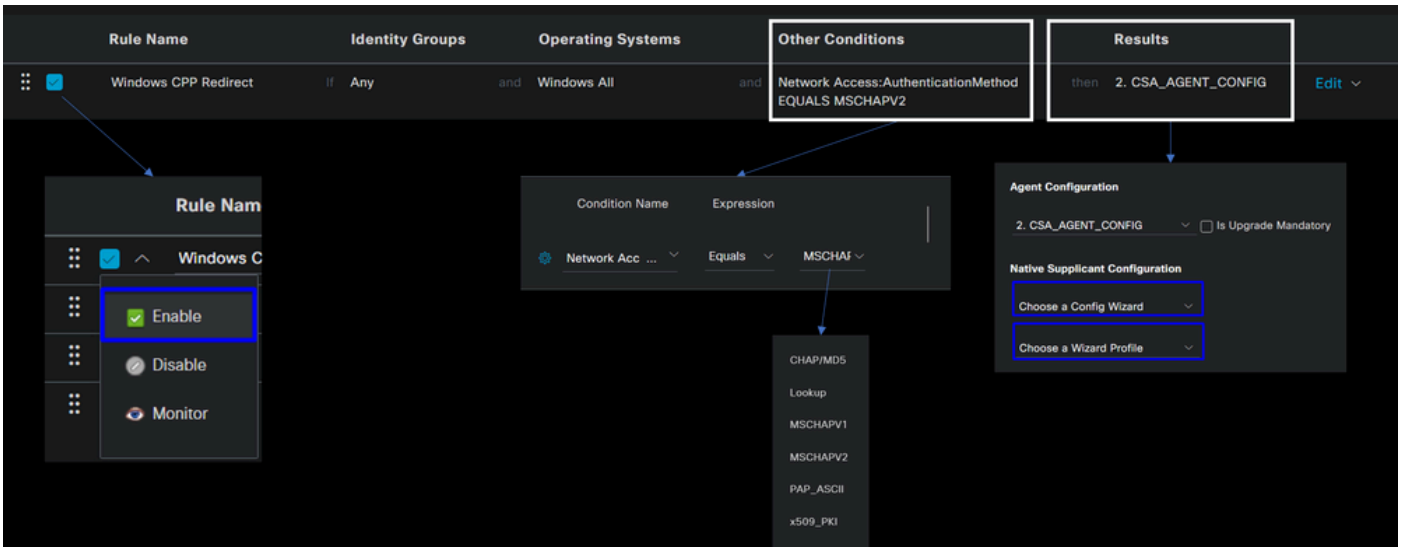
配置客户端调配策略

要启用调配在上一步配置的ISE终端安全评估和模块，您需要配置策略进行调配。

- 导航到ISE控制面板
- 点击 **Work Center > Client Provisioning**



注意：建议每个操作系统（Windows、Mac OS或Linux）都有一个客户端配置策略。



- **Rule Name**：根据设备类型和身份组选择配置策略名称，以轻松识别每个策略
- **Identity Groups**：选择要对策略进行评估的标识
- **Operating Systems**：根据在步骤"选择代理程序包"中选择的代理程序包选择操作系统
- **Other Condition**：根**Network Access** 据**Authentication Method**EQUALS选择添加RADIUS组步骤中配置的方法，或者您可以将其留空
- **Result**：选择在步骤4配置代理配置中配置的代理配置
    - **Native Supplicant Configuration**：选择Config Wizard和 Wizard Profile
- 如果策略未在复选框上列为已启用，请将其标记为已启用。

创建授权配置文件

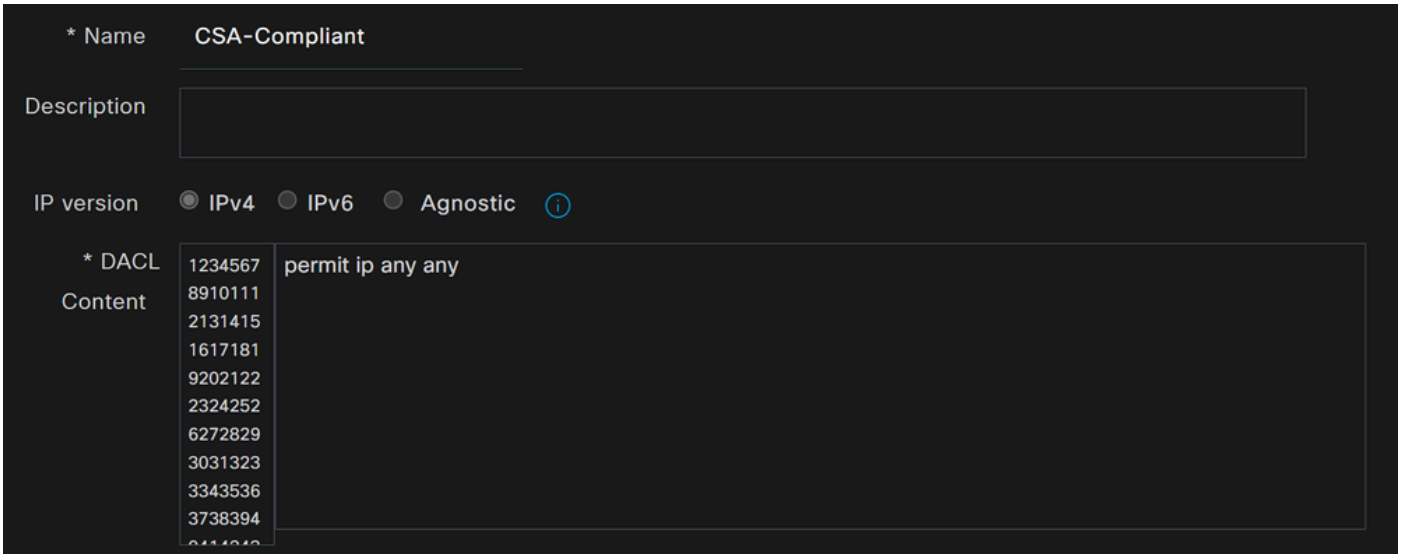
授权配置文件根据身份验证通过后的用户状态限制对资源的访问。必须验证授权才能根据状态确定用户可以访问哪些资源。

授权配置文件	描述
合规	用户兼容-已安装代理-状态已验证
未知兼容	用户未知合规性-重定向以安装代理-状态待验证的

拒绝访问	用户不合规-拒绝访问

要配置DACL，请导航到ISE控制面板：

- 点击 **Work Centers > Policy Elements > Downloadable ACLs**
- 点击 **+Add**
- 创建 **Compliant DACL**



- **Name**：添加引用符合DACL的名称
- **IP version**：选择 **IPv4**
- DACL Content：创建可下载访问控制列表(DACL)，用于访问网络的所有资源

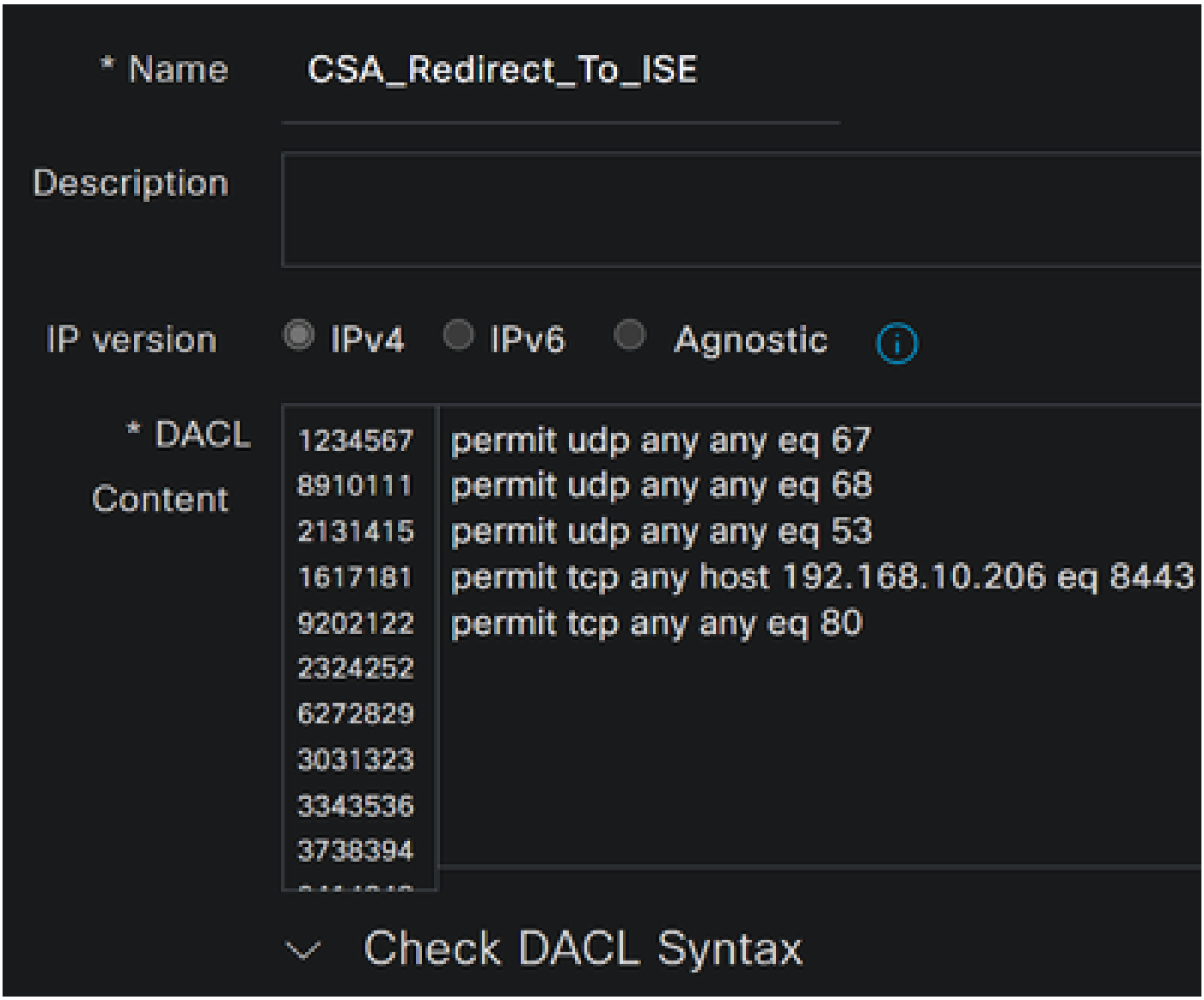
<#root>

```
permit ip any any
```

点击**Save** 并创建未知合规性DACL

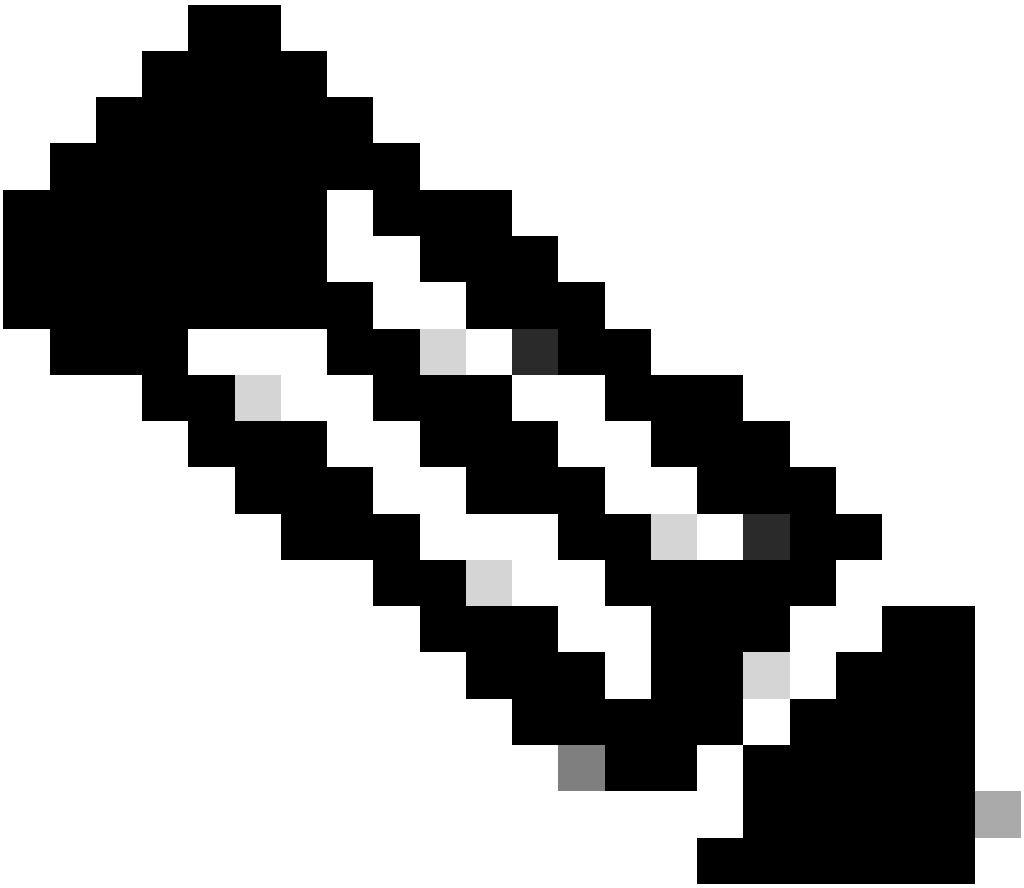
- 点击 **Work Centers > Policy Elements > Downloadable ACLs**
- 点击 **+Add**

- 创建 **Unknown Compliant DACL**



- **Name**：添加引用DACL-Unknown-Compliant的名称
- **IP version**：选择 **IPv4**
- **DACL Content**: 创建一个DACL，允许通过端口8443对网络、DHCP、DNS、HTTP和调配门户进行有限访问

```
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
```



注意：在此场景中，IP地址192.168.10.206与思科身份服务引擎(ISE)服务器对应，端口8443指定为调配门户。这意味着允许通过端口8443发往IP地址192.168.10.206的TCP流量，从而便于访问调配门户。

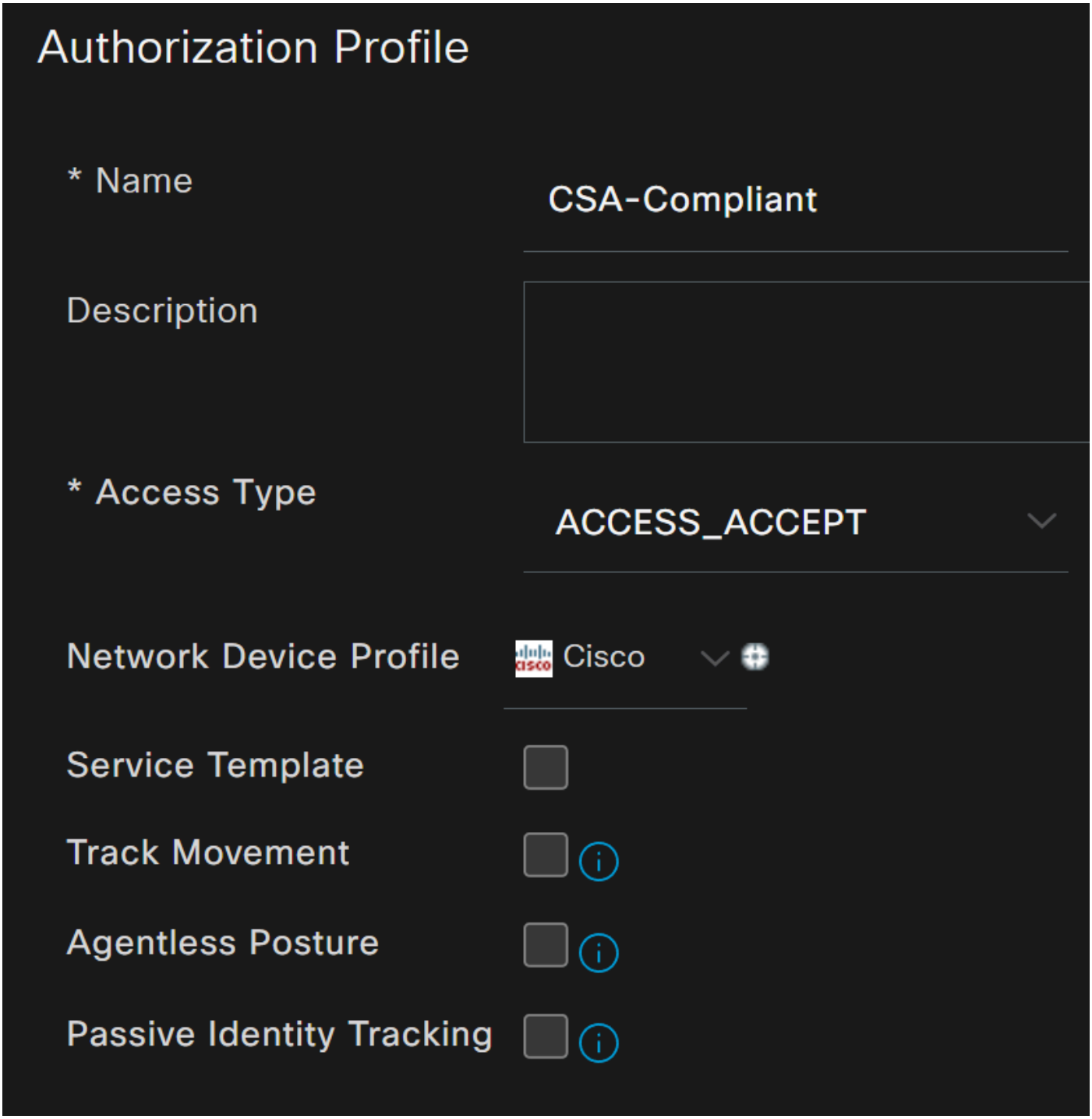
此时，您拥有创建授权配置文件所需的DACL。

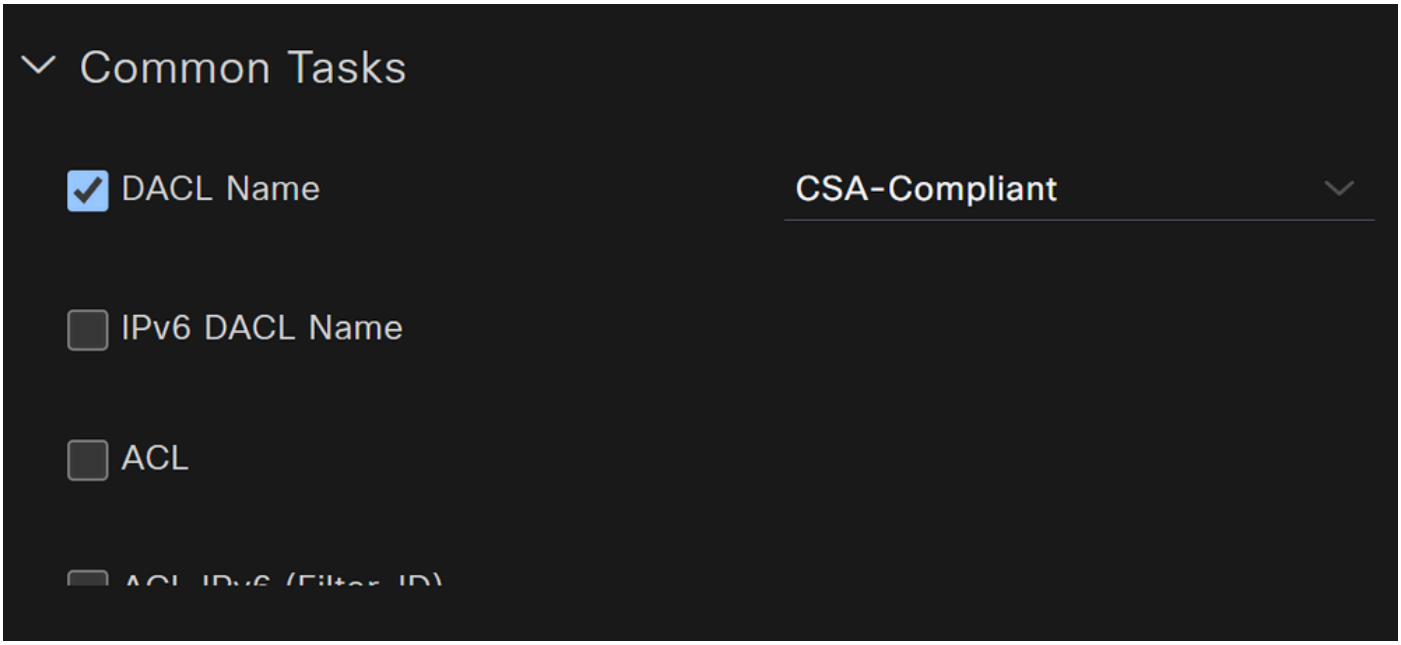
要配置授权配置文件，请导航到ISE控制面板：

- 点击 **Work Centers** > **Policy Elements** > **Authorization Profiles**
  -

点击 **+Add**

- 创建 **Compliant Authorization Profile**





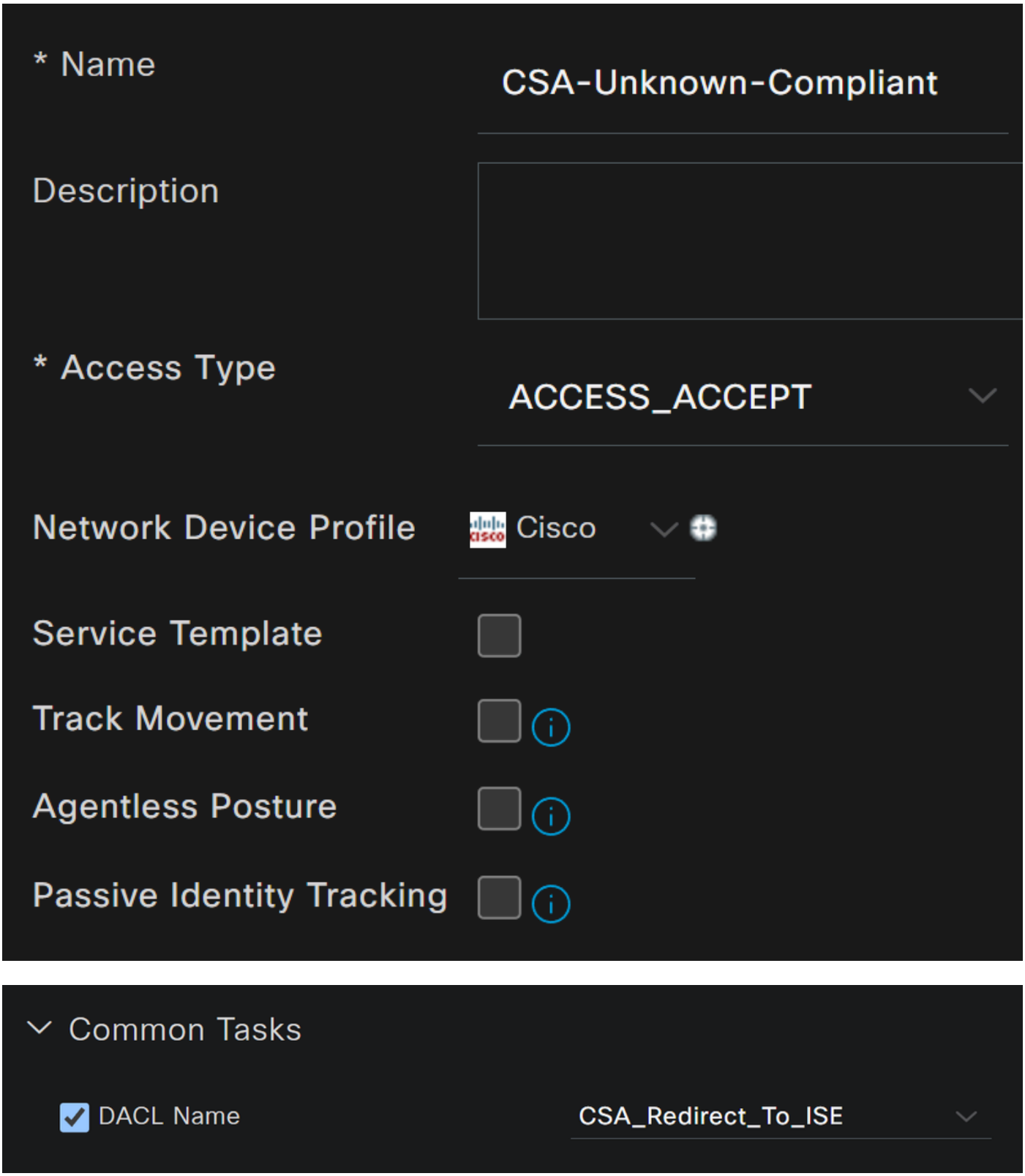
- **Name**：创建引用合规授权配置文件的名称
- Access Type：选择 **ACCESS_ACCEPT**

- **Common Tasks**
  - **DACL NAME**：选择在步骤兼容DACL中配置的DACL

点击**Save** 并创建 Unknown Authorization Profile

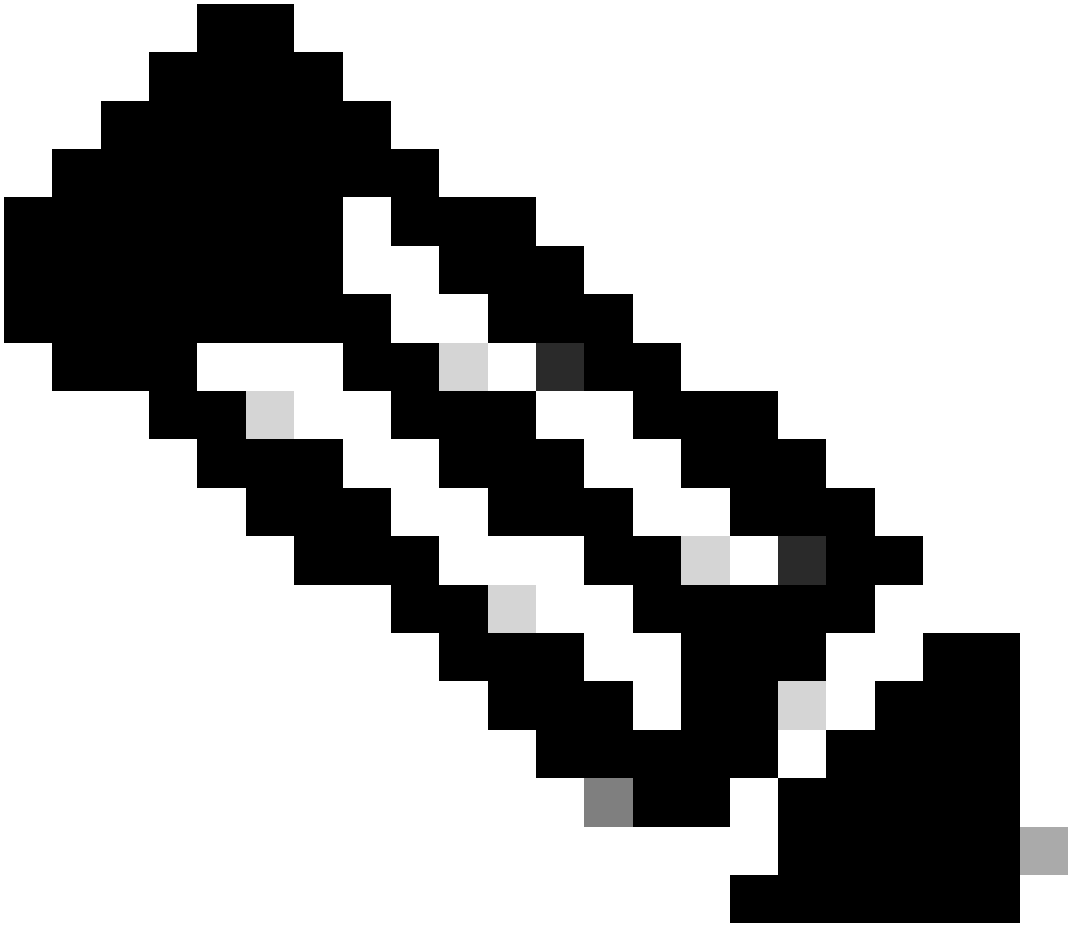
- 点击 **Work Centers > Policy Elements > Authorization Profiles**
- 点击 **+Add**

- 创建 **Uknown Compliant Authorization Profile**



- **Name**：创建引用未知合规授权配置文件的名称
- Access Type：选择 **ACCESS_ACCEPT**

- **Common Tasks**
  - **DACL NAME**：选择在未知兼容DACL步骤中配置的DACL
    - **Web Redirection (CWA,MDM,NSP,CPP)**
      - 选择 **Client Provisioning (Posture)**
        - **ACL**：必须是 redirect
        - **Value**：选择默认调配门户，或者如果您定义了其他门户，请选择它



注意：针对所有部署的安全访问重定向ACL的名称是 **redirect**。

定义所有这些值后，您必须在Attributes Details下具有类似内容。

```
Attributes Details
Access Type = ACCESS_ACCEPT
DACL = 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
```

点击**Save** 结束配置并继续下一步。

配置安全评估策略集

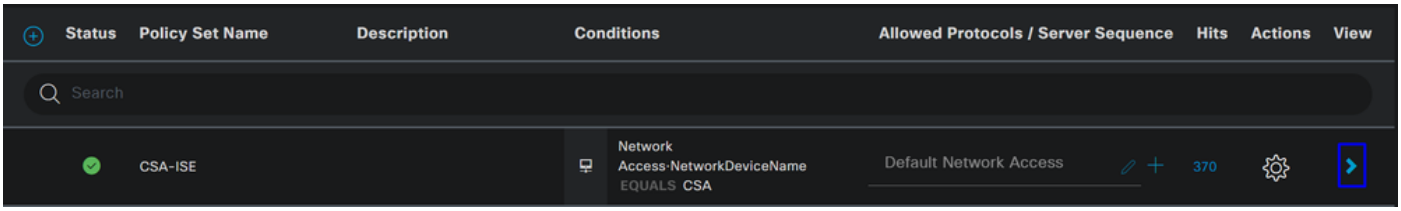
创建的这三个策略基于配置的授权配置文件；对于 **DenyAccess**，您不需要创建其他策略。

策略集-授权	授权配置文件
合规	授权配置文件-合规
未知兼容	授权配置文件-未知合规性
不合规	拒绝访问

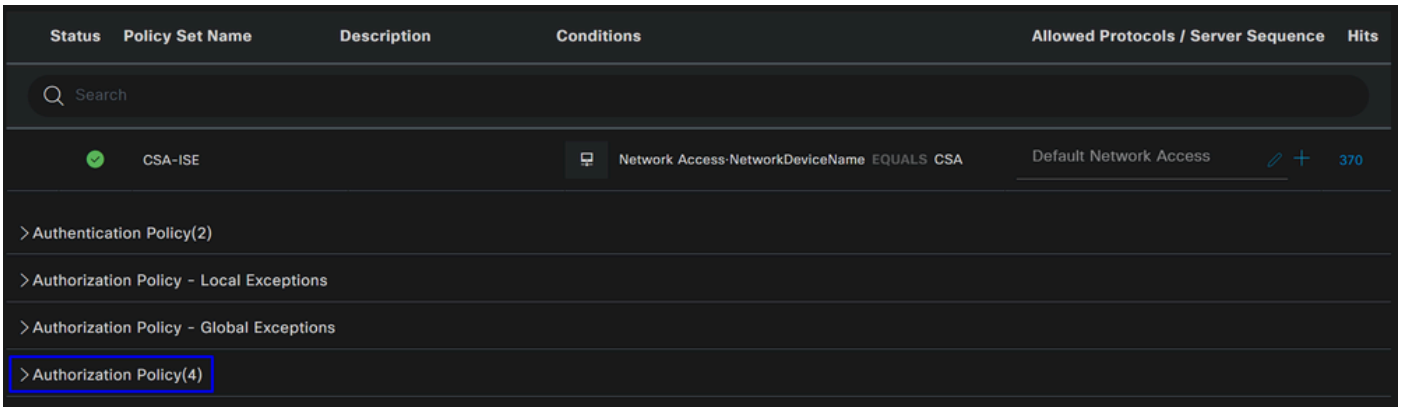
导航到ISE控制面板

- 点击 **Work Center > Policy Sets**

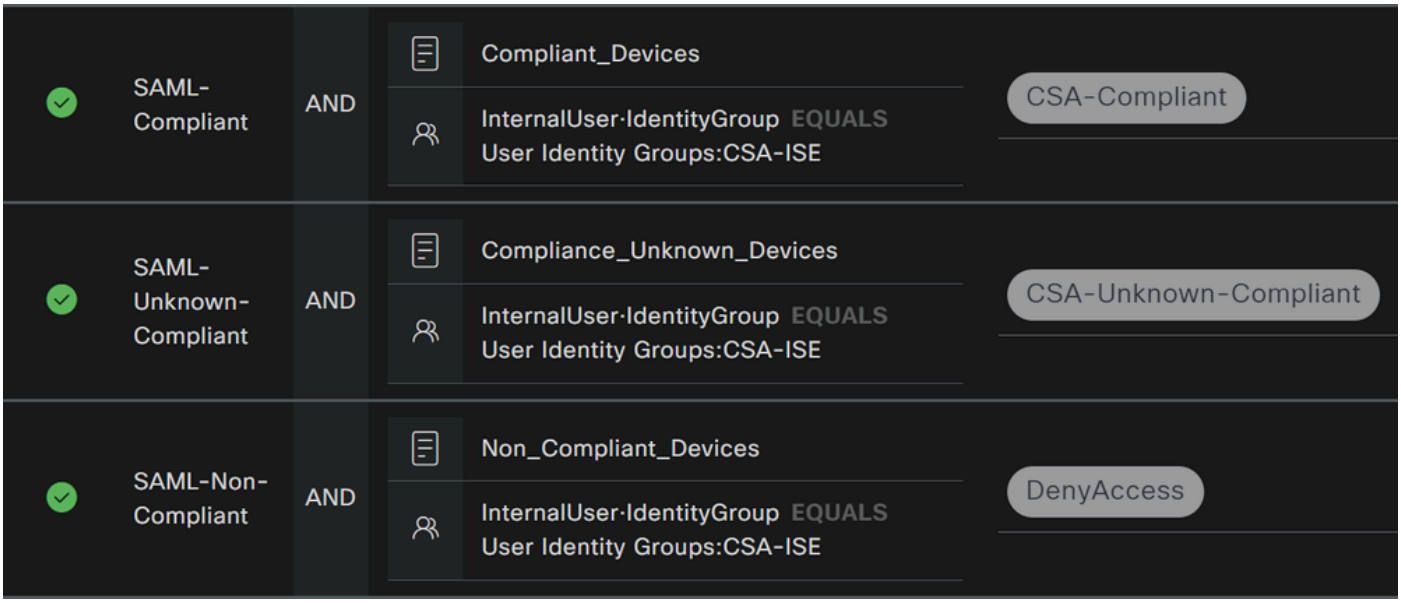
- 点击> 该选项可访问已创建的策略



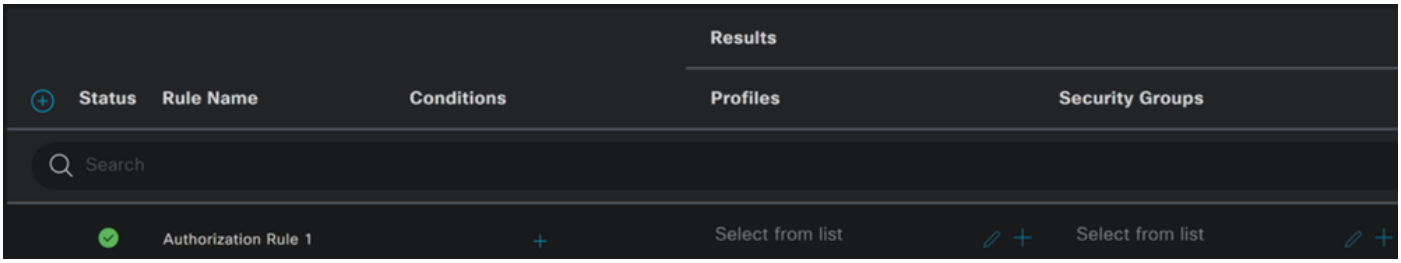
- 单击 Authorization Policy



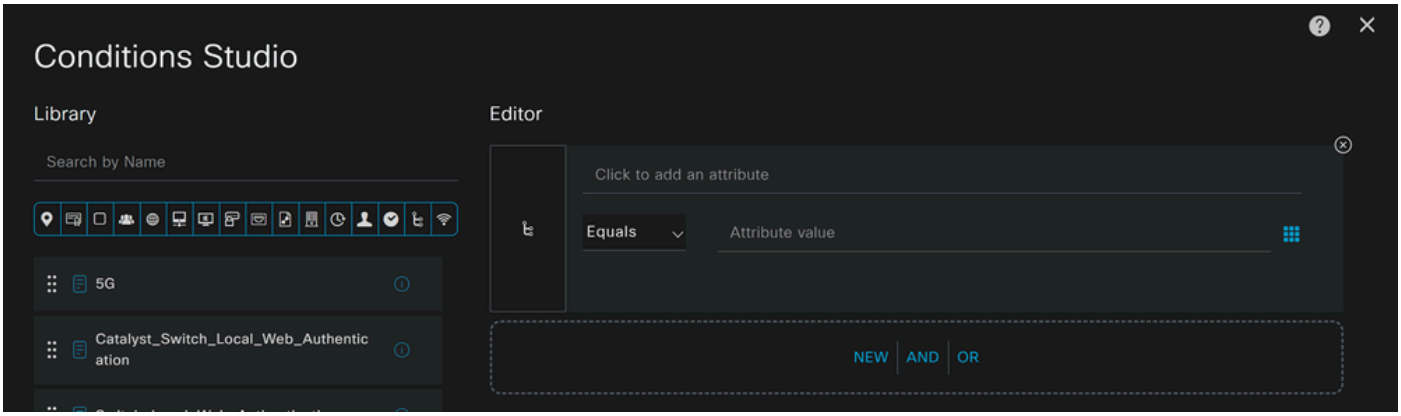
- 按下一个顺序创建接下来的三个策略：



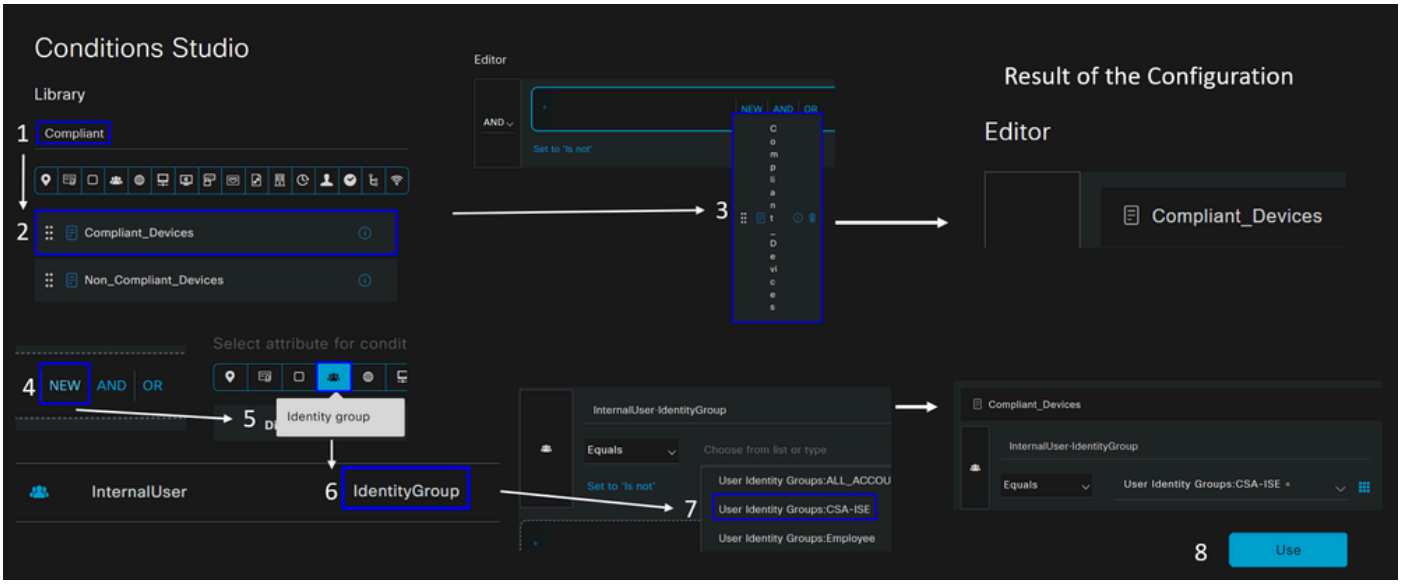
- 点击+ 以定义策**CSA-Compliance** 略：



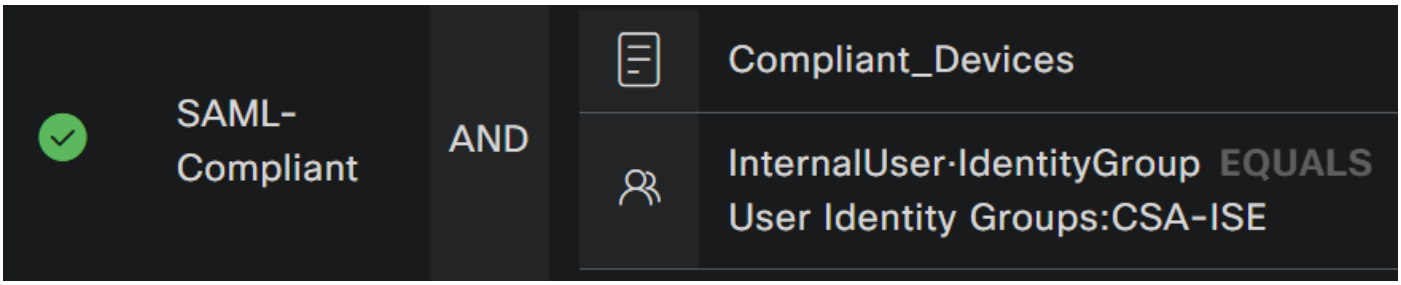
- 对于下一步，请更改Rule Name，和Conditions Profiles
- 将名称**Name** 配置为 **CSA-Compliance**
- 要配置 **Condition**命令，请点击 +
- 在 **Condition Studio**下，您可以找到以下信息：



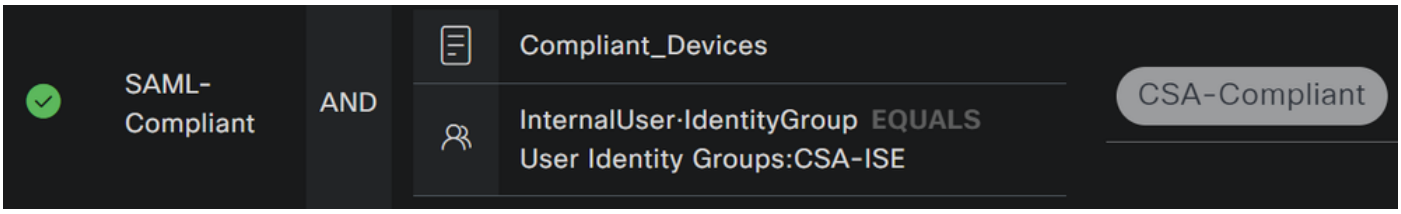
- 要创建条件，请搜索 **compliant**
- 您必须已显示 Compliant_Devices
- 拖放到 **Editor**
- 在Editor下单击 **New**
- 点击**Identity Group** 图标
- 选择 **Internal User Identity Group**
- 在 **Equals**下，选择要匹配的**User Identity Group** 路由
- 点击 **Use**



- 因此，您会看到下一个映像

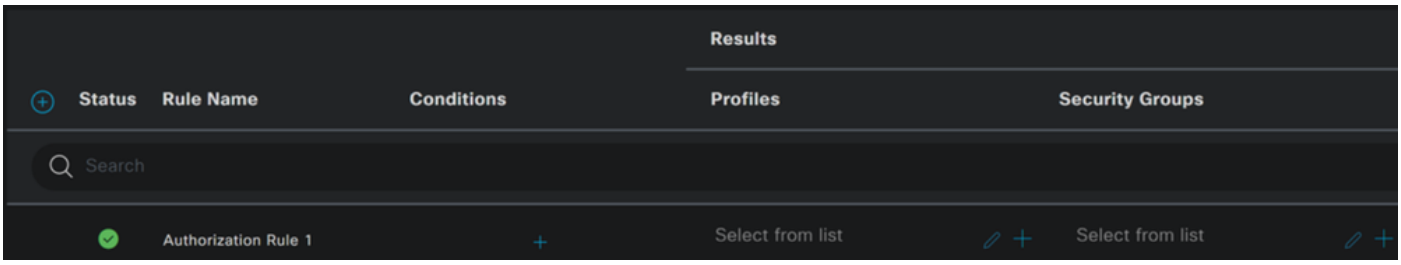


- 在**Profile** 单击下拉按钮下的并选择步骤中配置的投诉授权配置文件Compliant Authorization Profile



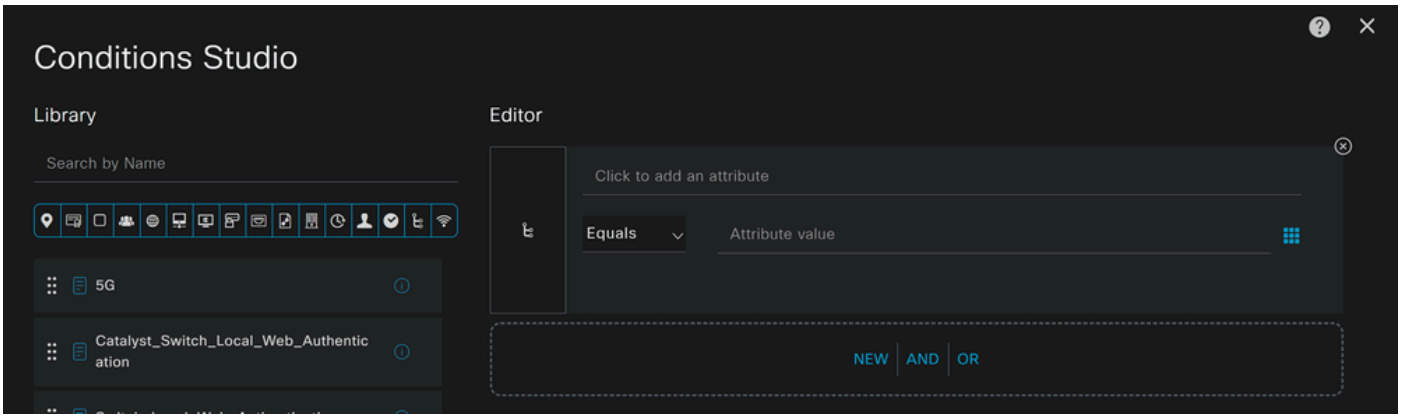
现在，您已经配置了 **Compliance Policy Set**。

- 点击+ 以定义策**CSA-Unknown-Compliance** 略：

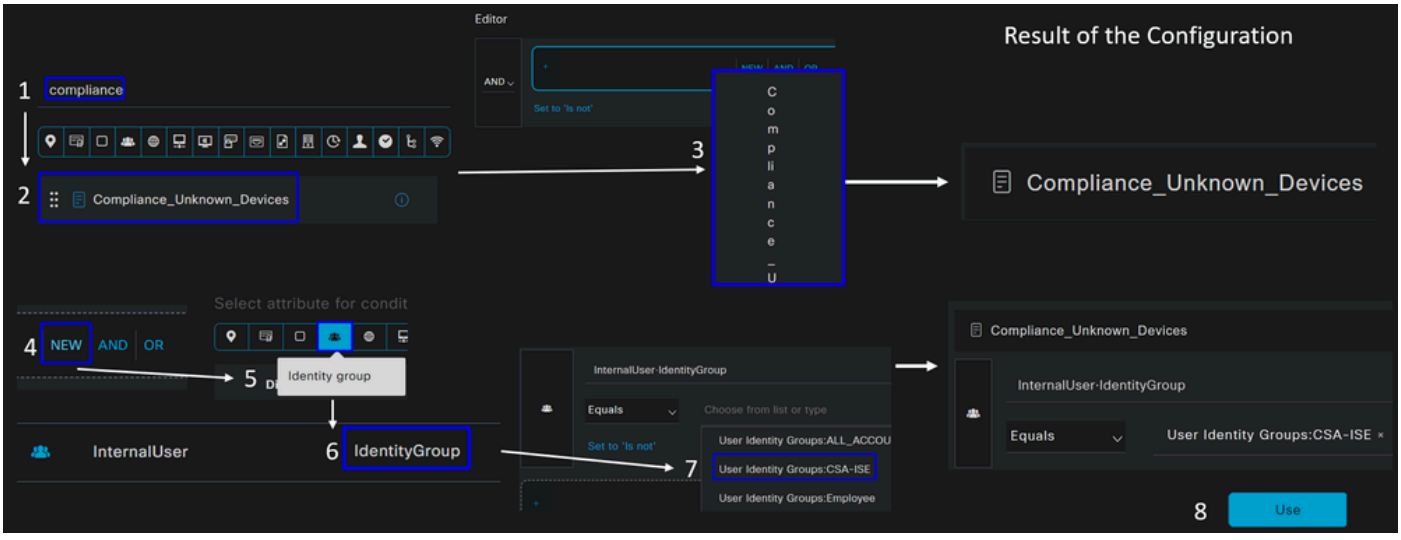


- 对于下一步，请更改Rule Name，和Conditions Profiles
- 将名称**Name** 配置为 **CSA-Unknown-Compliance**

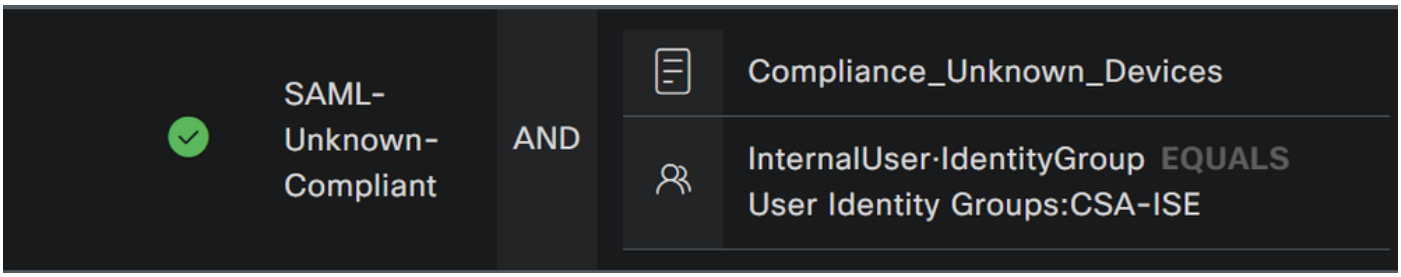
- 要配置 **Condition**命令，请点击 +
- 在 **Condition Studio**下，您可以找到以下信息：



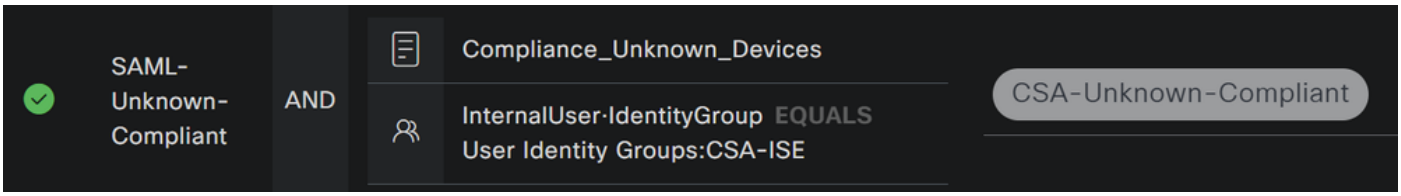
- 要创建条件，请搜索 **compliance**
- 您必须已显示 Compliant_Unknown_Devices
- 拖放到 **Editor**
- 在Editor下单击 **New**
- 点击**Identity Group** 图标
- 选择 **Internal User Identity Group**
- 在 **Equals**下，选择要匹配的**User Identity Group** 路由
- 点击 **Use**



- 因此，您会看到下一个映像

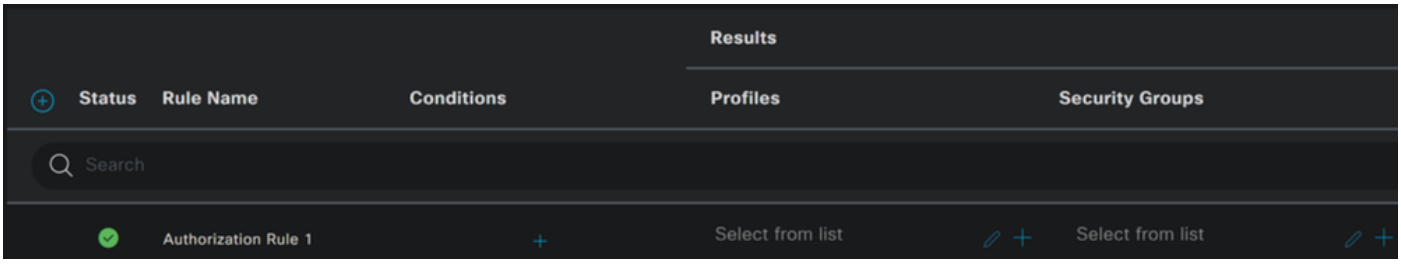


- 在**Profile** 单击下拉按钮下的并选择步骤中配置的投诉授权配置文件[Unknown Compliant Authorization Profile]



现在，您已经配置了 **Unknown Compliance Policy Set**。

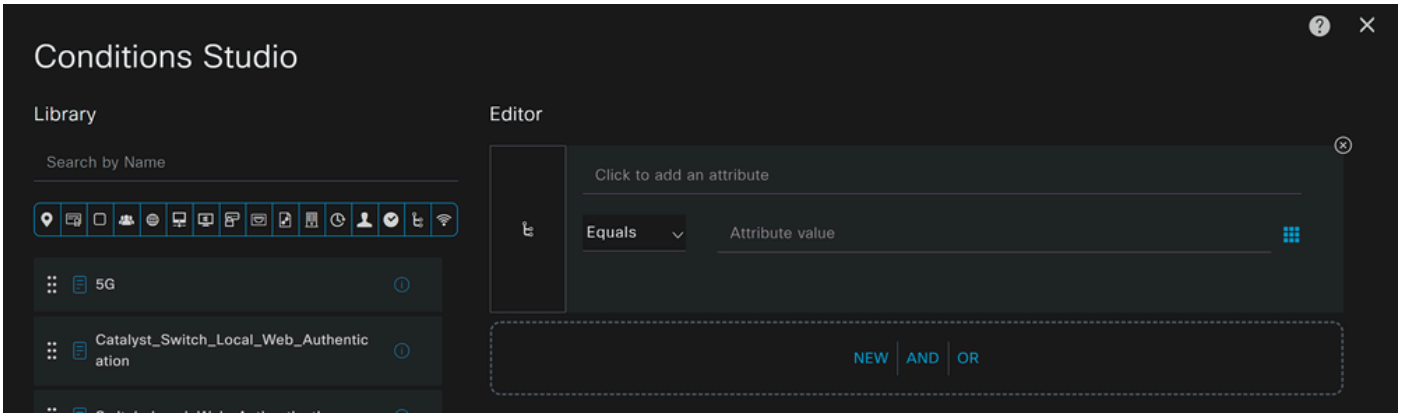
- 点击+ 以定义策**CSA- Non-Compliant** 略：



- 对于下一步，请更改Rule Name，和Conditions Profiles
- 将名称**Name** 配置为 **CSA-Non-Compliance**

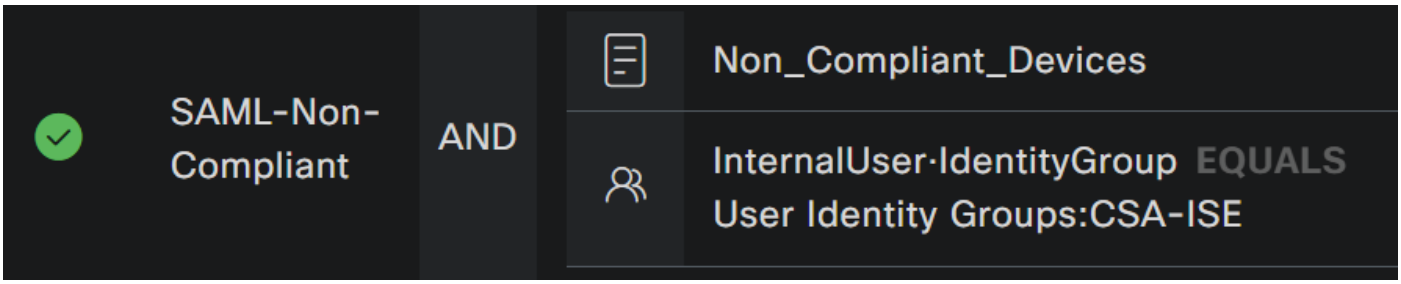
- 要配置 **Condition**命令，请点击 +

- 在 **Condition Studio**下，您可以找到以下信息：

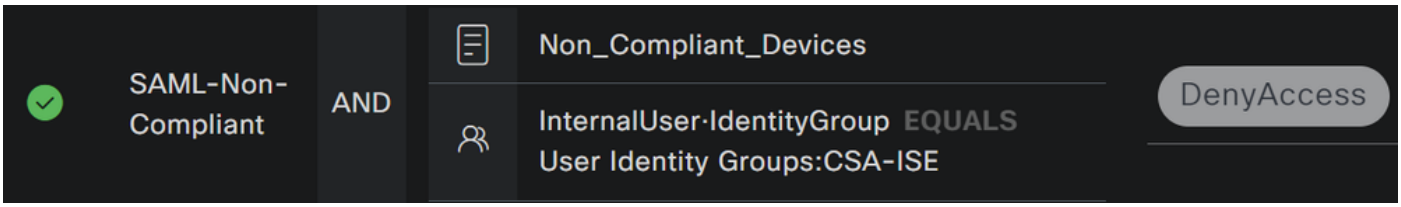


- 要创建条件，请搜索 **non**
- 您必须已显示 Non_Compliant_Devices
- 拖放到 **Editor**
- 在Editor下单击 **New**
- 点击**Identity Group** 图标
- 选择 **Internal User Identity Group**
- 在 **Equals**下，选择要匹配的**User Identity Group** 路由
- 点击 **Use**

- 因此，您会看到下一个映像



- 在**Profile** 点击下拉按钮下方并选择投诉授权配置文件 **DenyAccess**



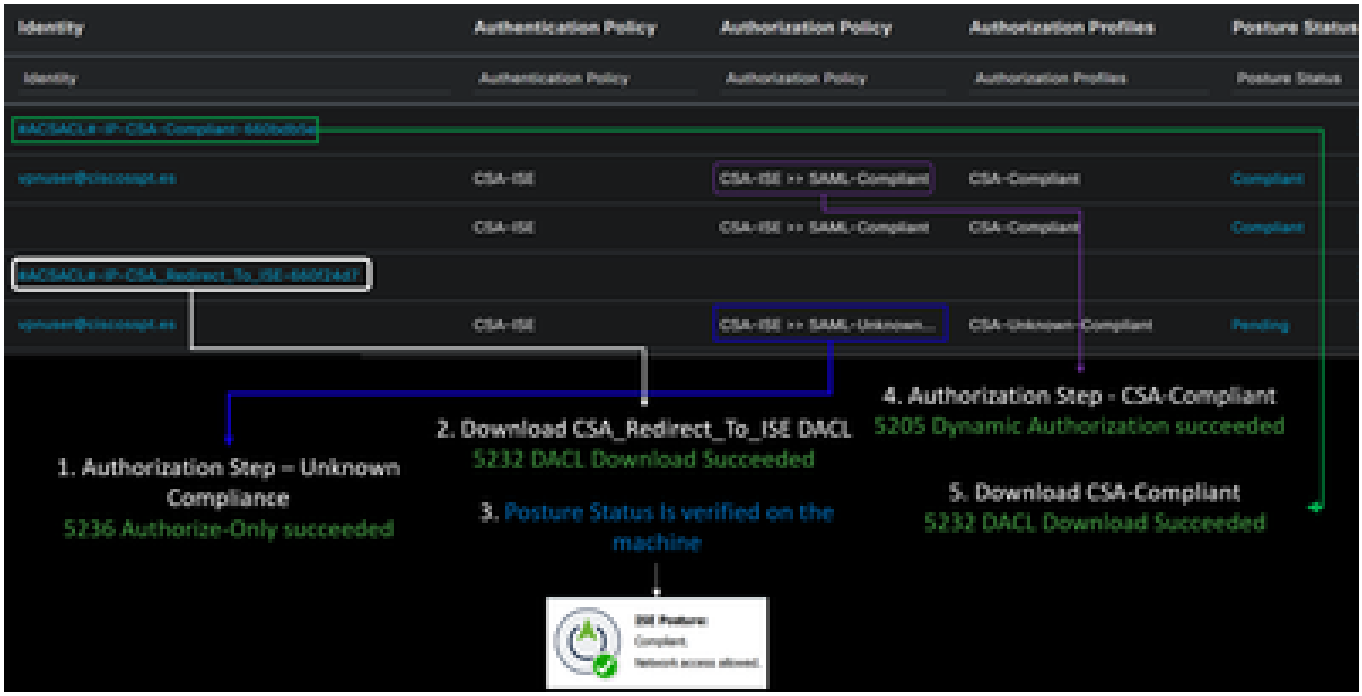
一旦您结束三个配置文件的配置，您就可以测试您与终端安全评估的集成了。

验证

状态验证

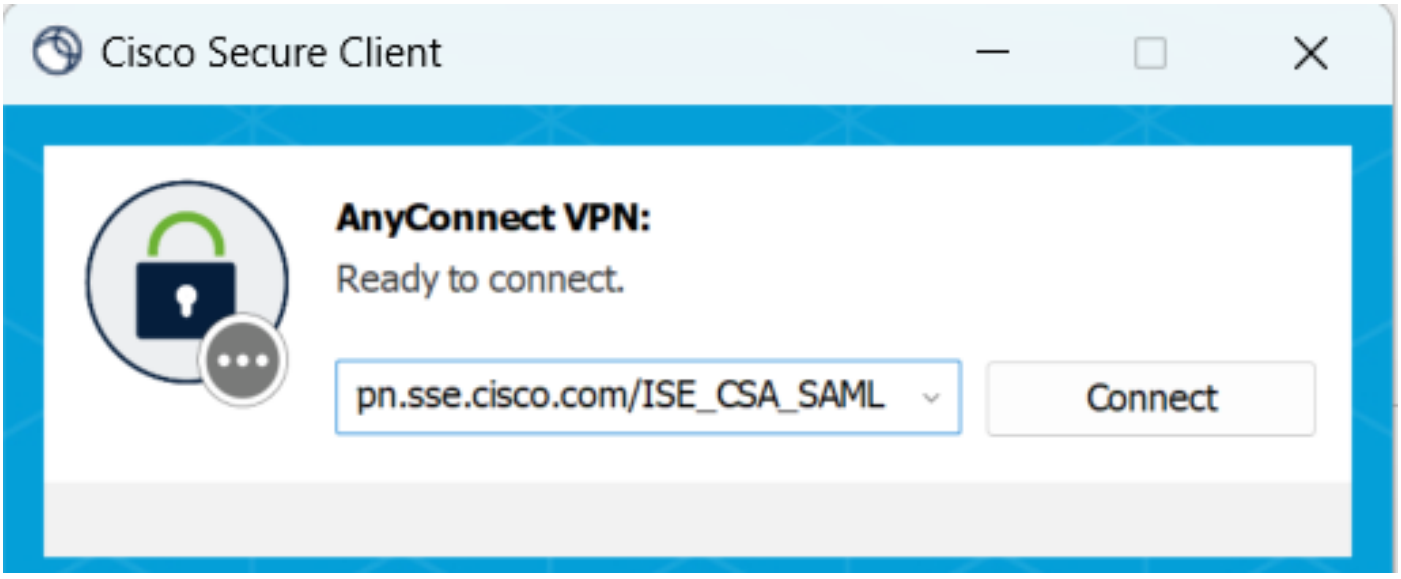
计算机上的连接

通过安全客户端连接到安全访问上提供的FQDN RA-VPN域。

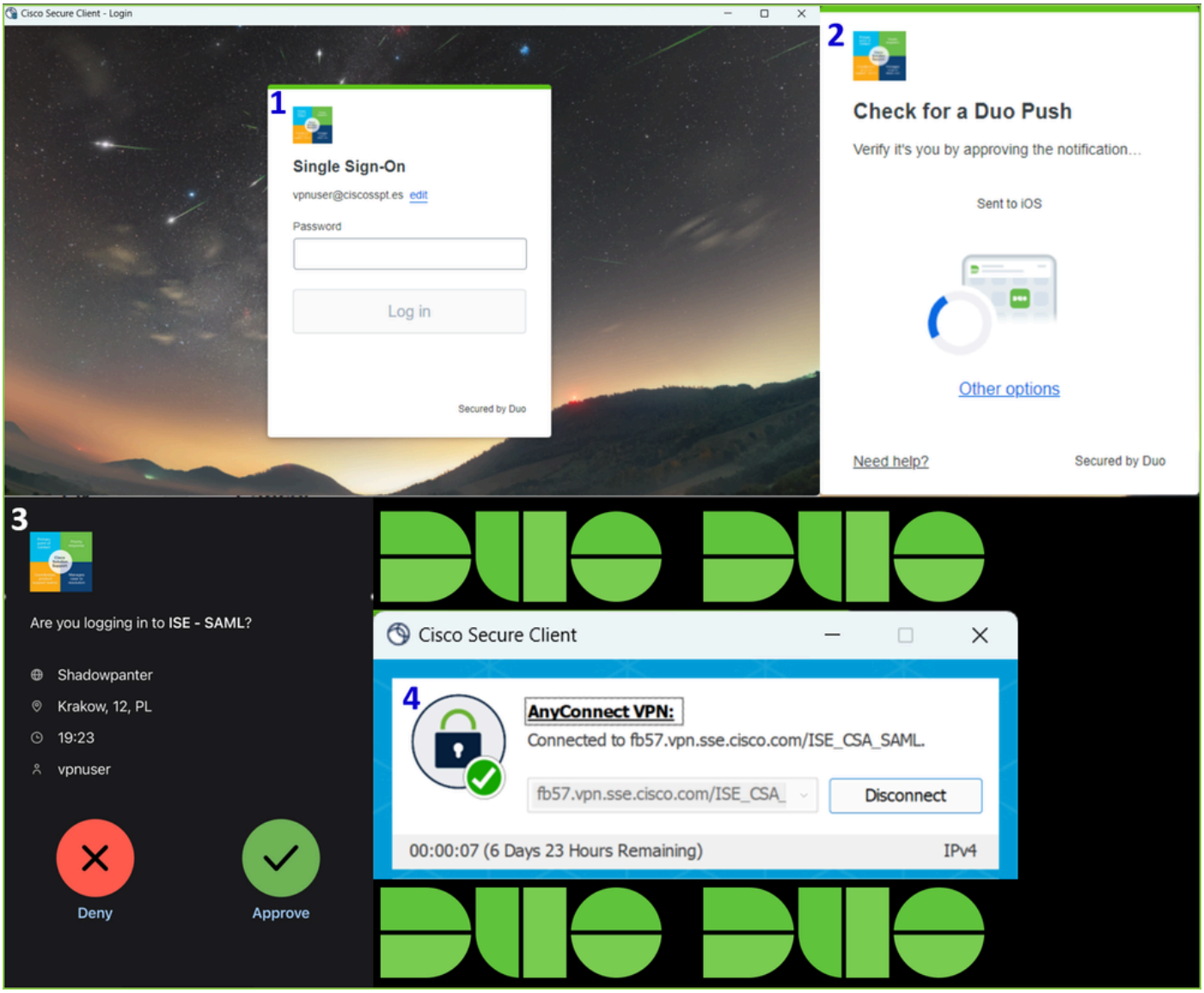


注意：此步骤无需安装ISE模块。

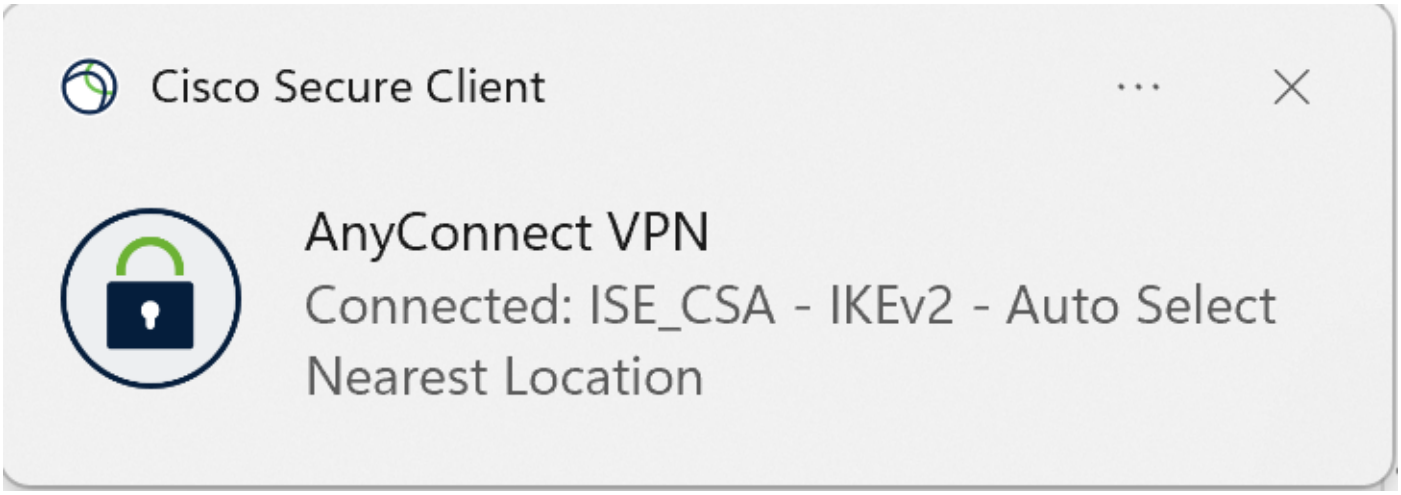
1. 使用安全客户端连接。

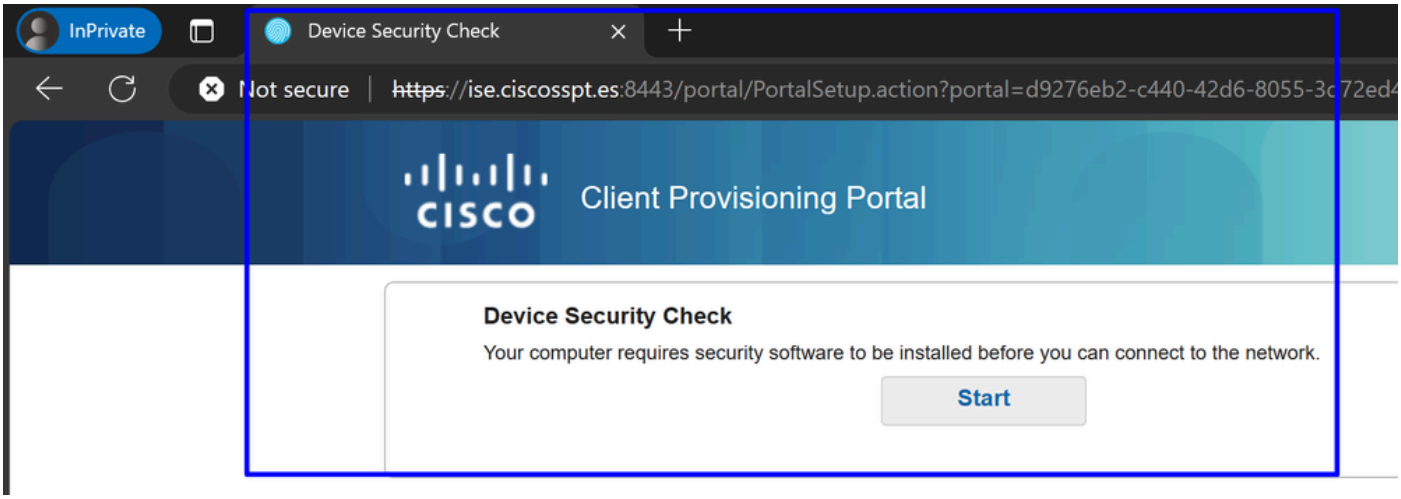


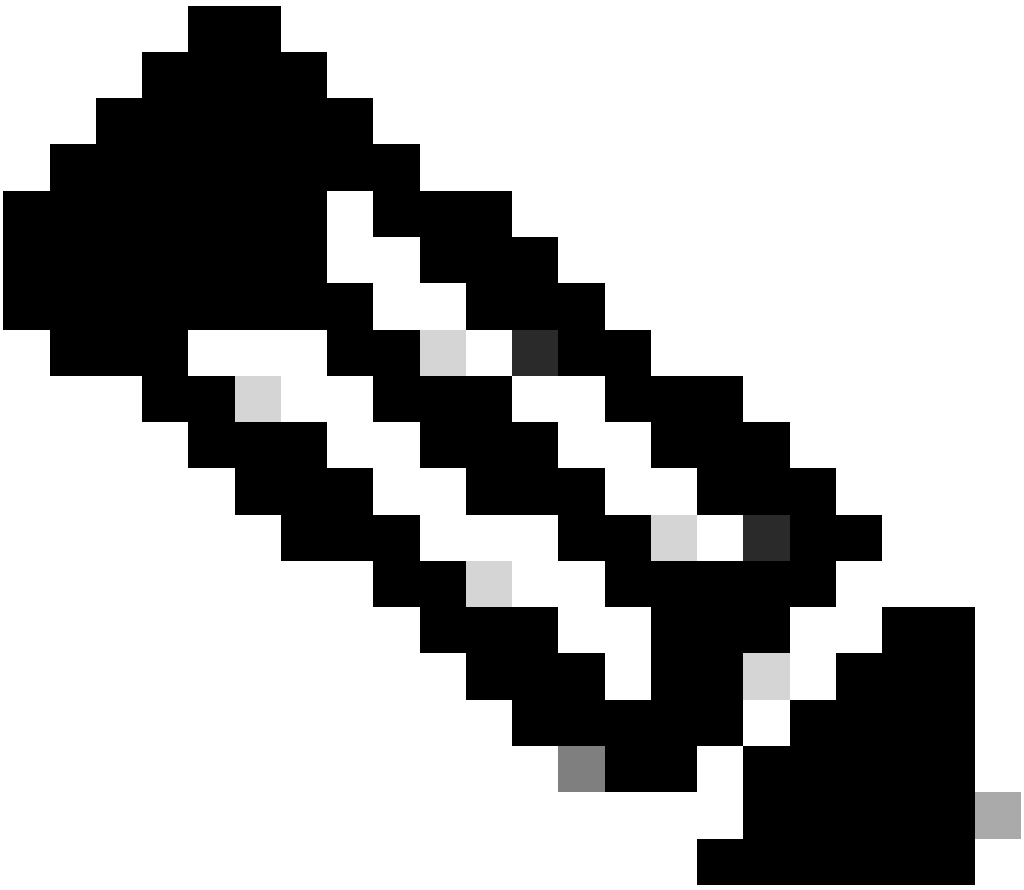
2. 提供凭证以通过Duo进行身份验证。



3. 此时，您连接到VPN，您很可能被重定向到ISE；否则，您可以尝试导航到**http:1.1.1.1**。



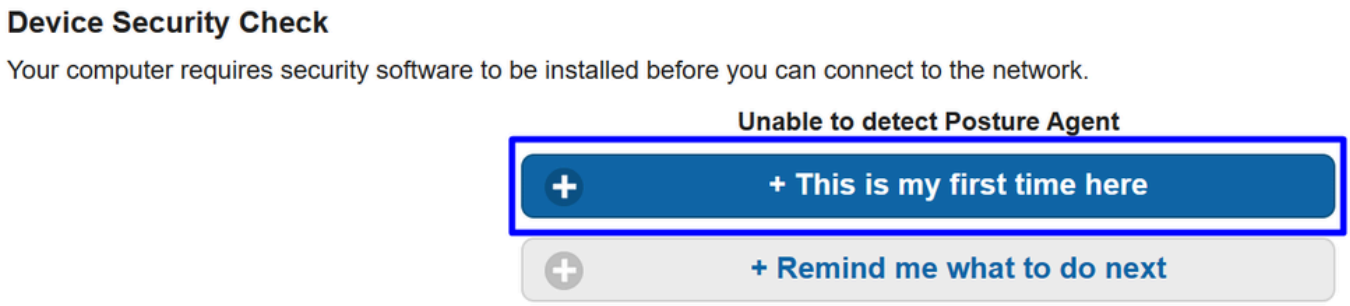

InPrivate
Device Security Check
Not secure
https://ise.ciscosspt.es:8443/portal/PortalSetup.action?portal=d9276eb2-c440-42d6-8055-3c72ed4
Client Provisioning Portal
Device Security Check
Your computer requires security software to be installed before you can connect to the network.
Start



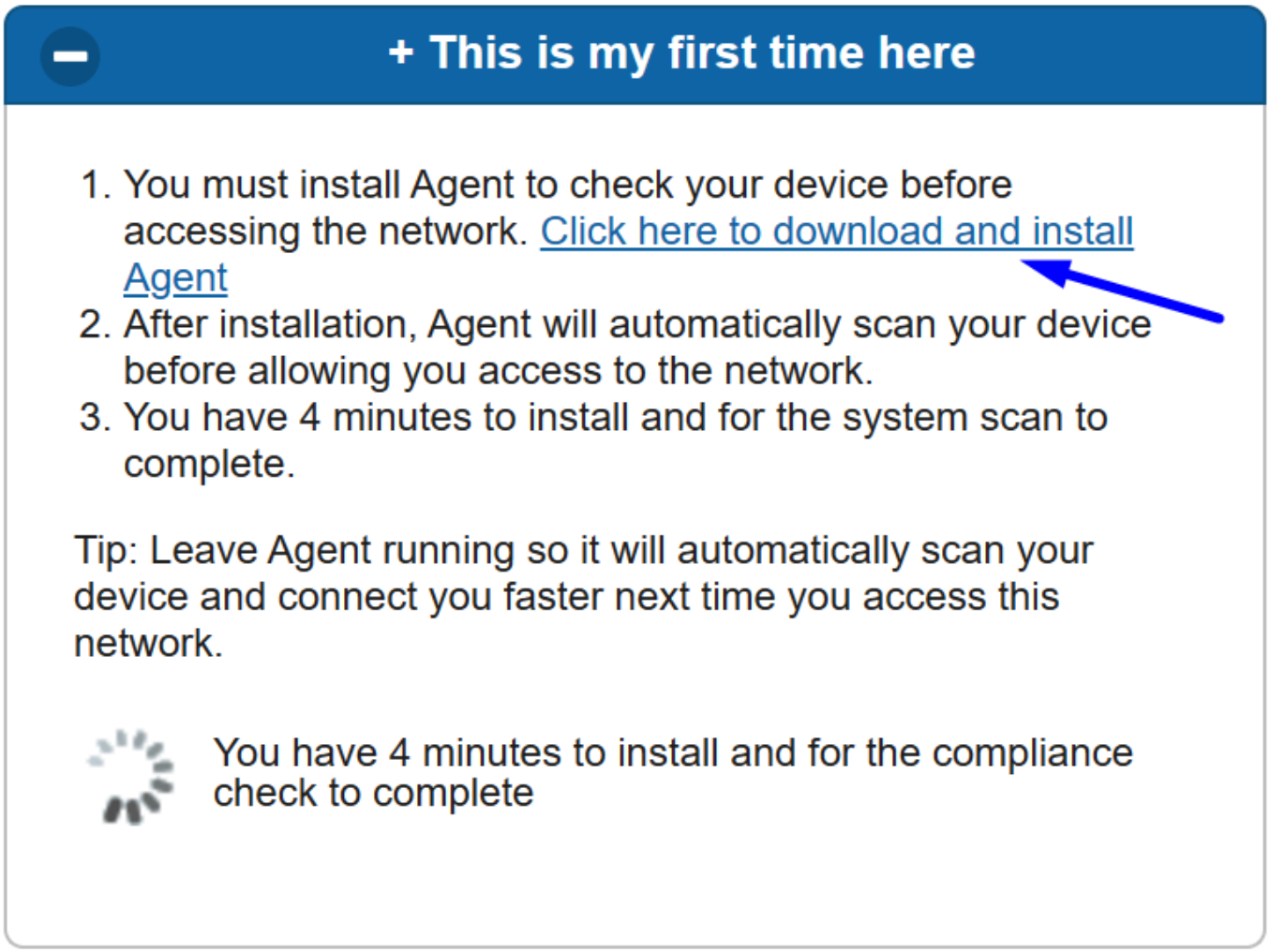
注意：此时，您处于授权-策略集CSA-Unknown-Compliance下，因为您未在计算机上安装ISE终端安全评估代理，并且已重定向到ISE调配门户以安装代理。

4. 单击“开始”继续代理程序设置。

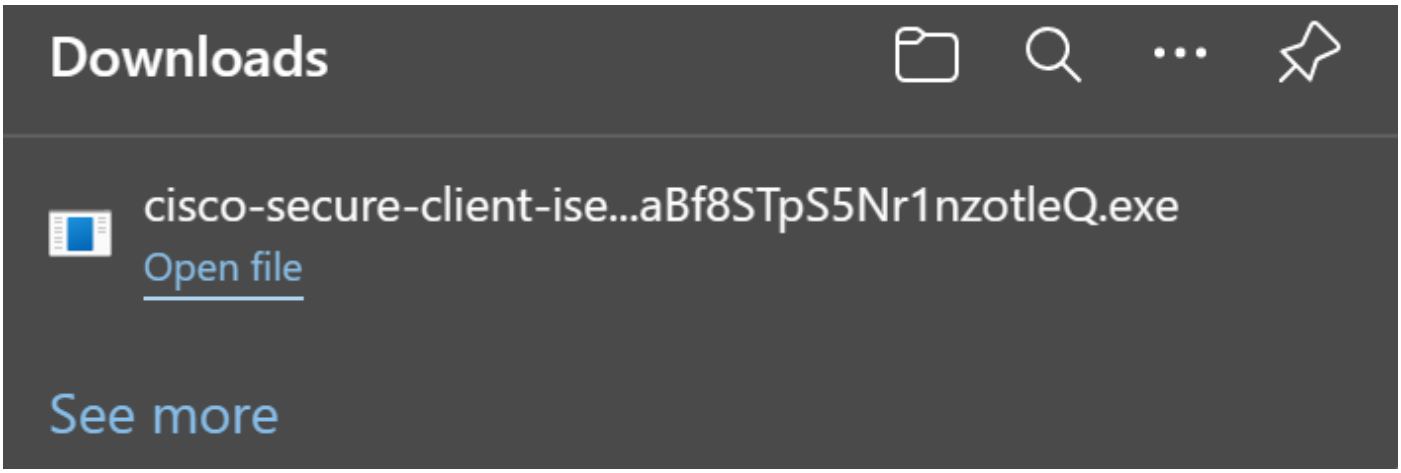
5. 单击+ **This is my first time here**。

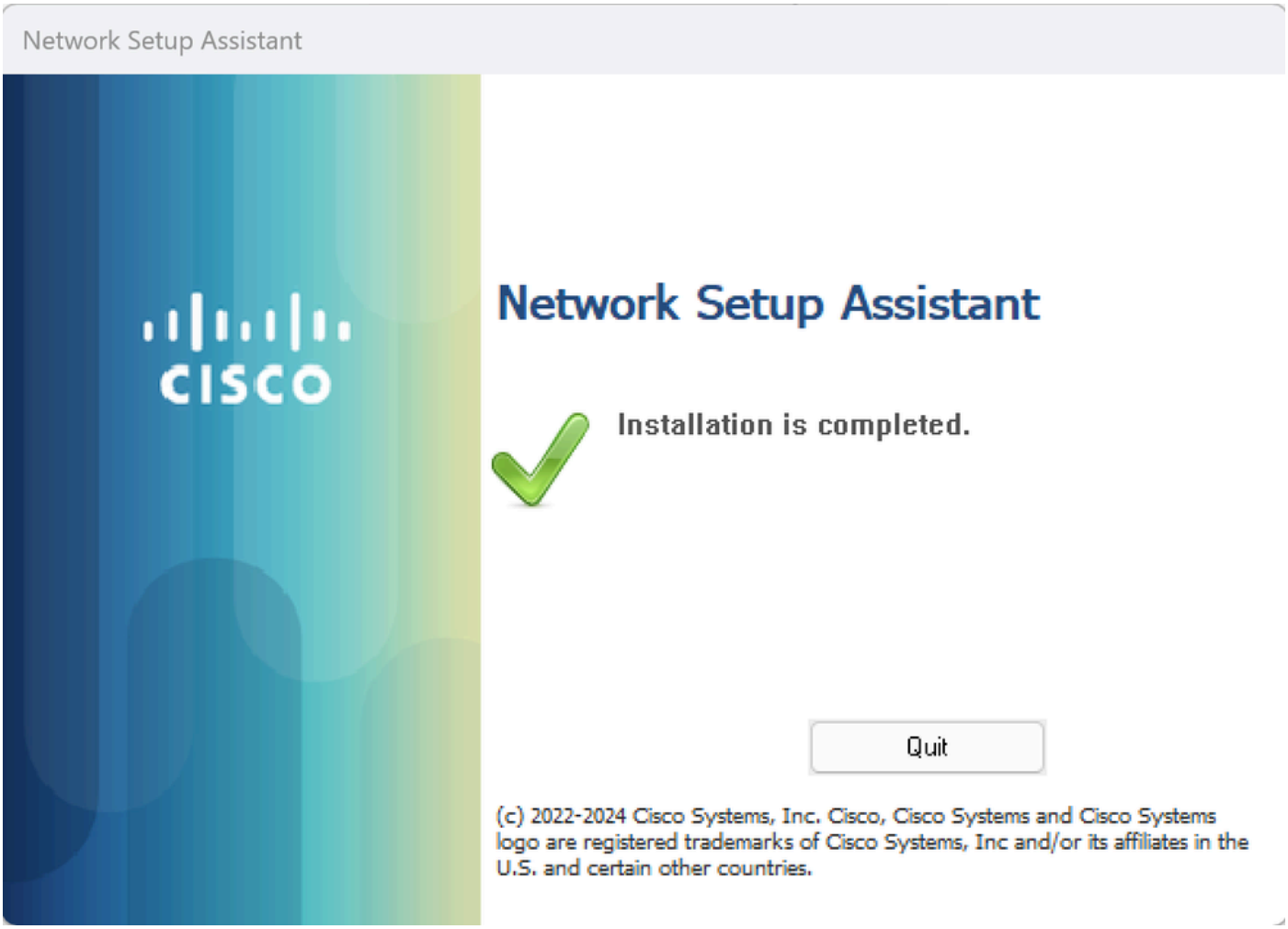


6. 单击 **Click here to download and install agent**

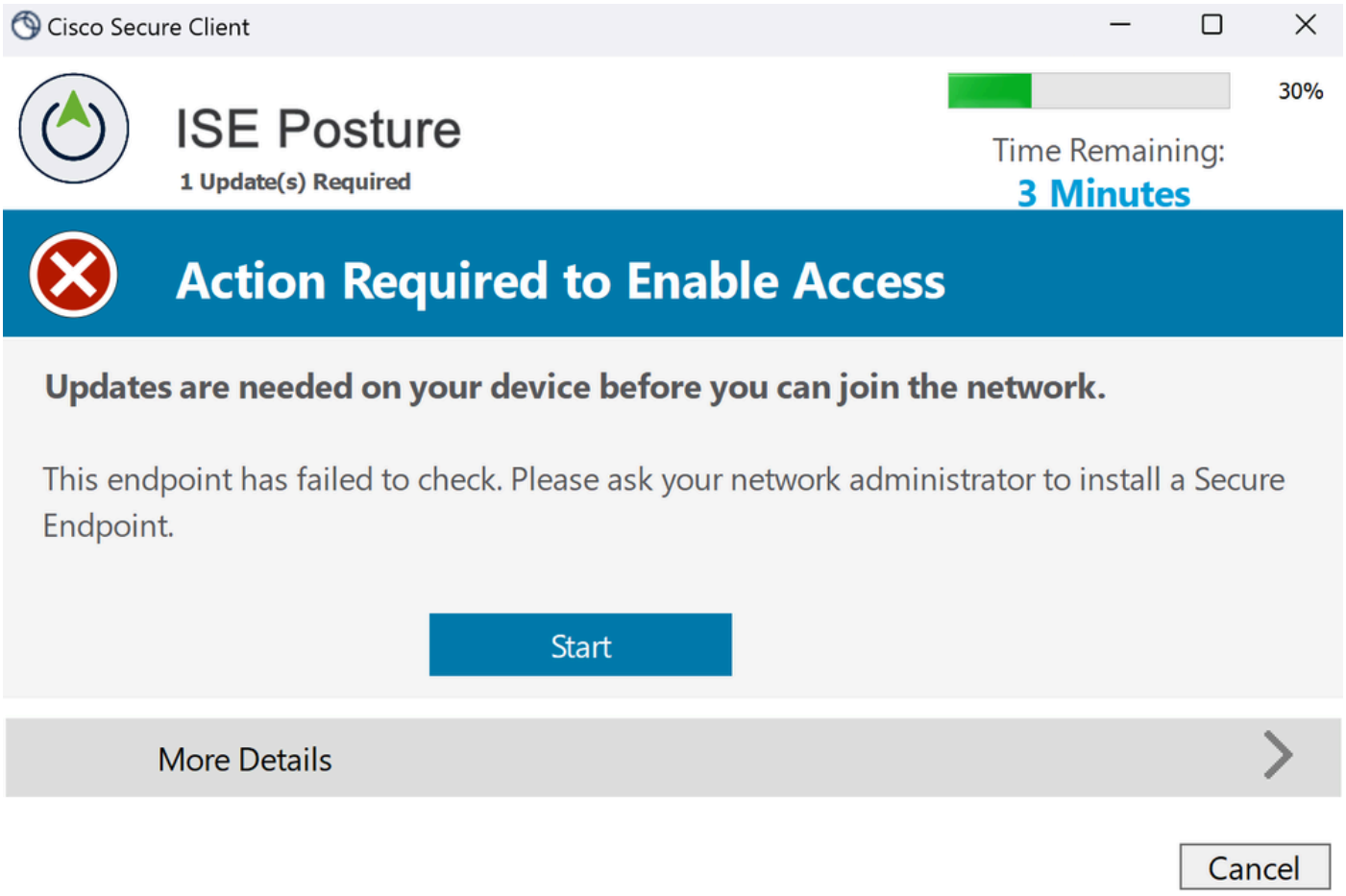

+ This is my first time here
1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system 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

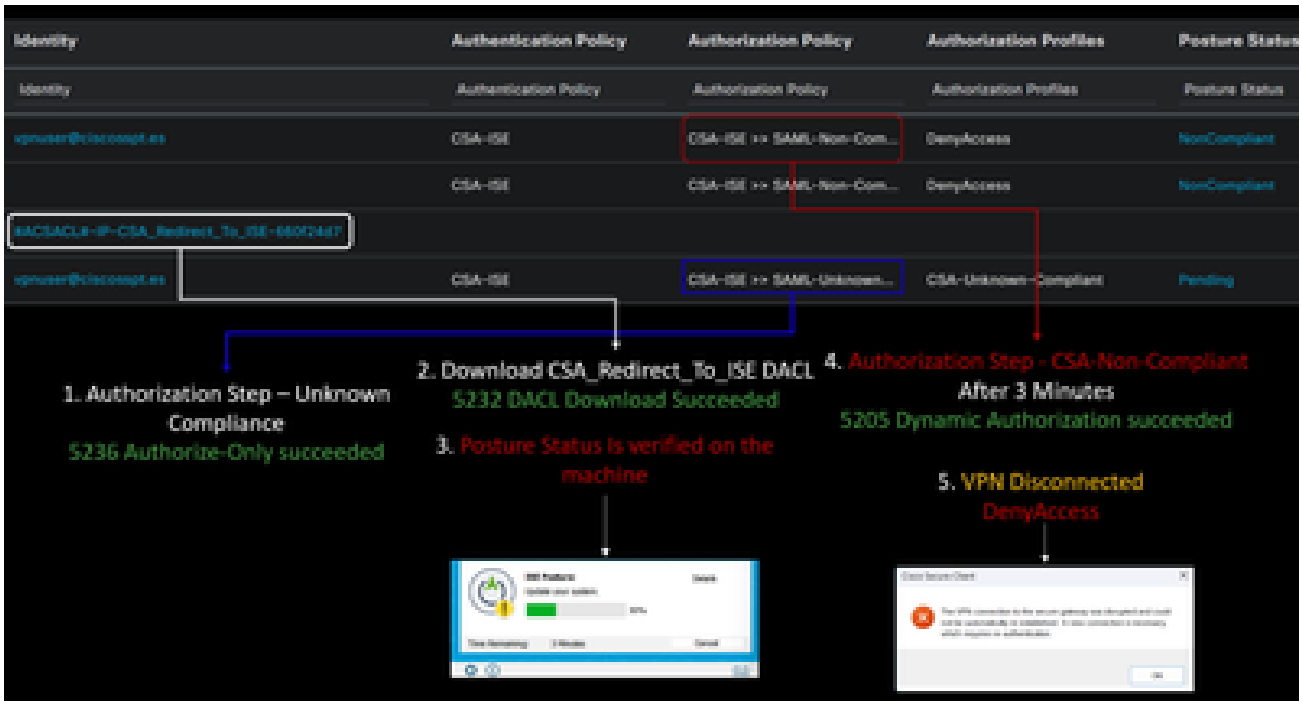
7. 安装代理


Downloads
cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe
Open file
See more



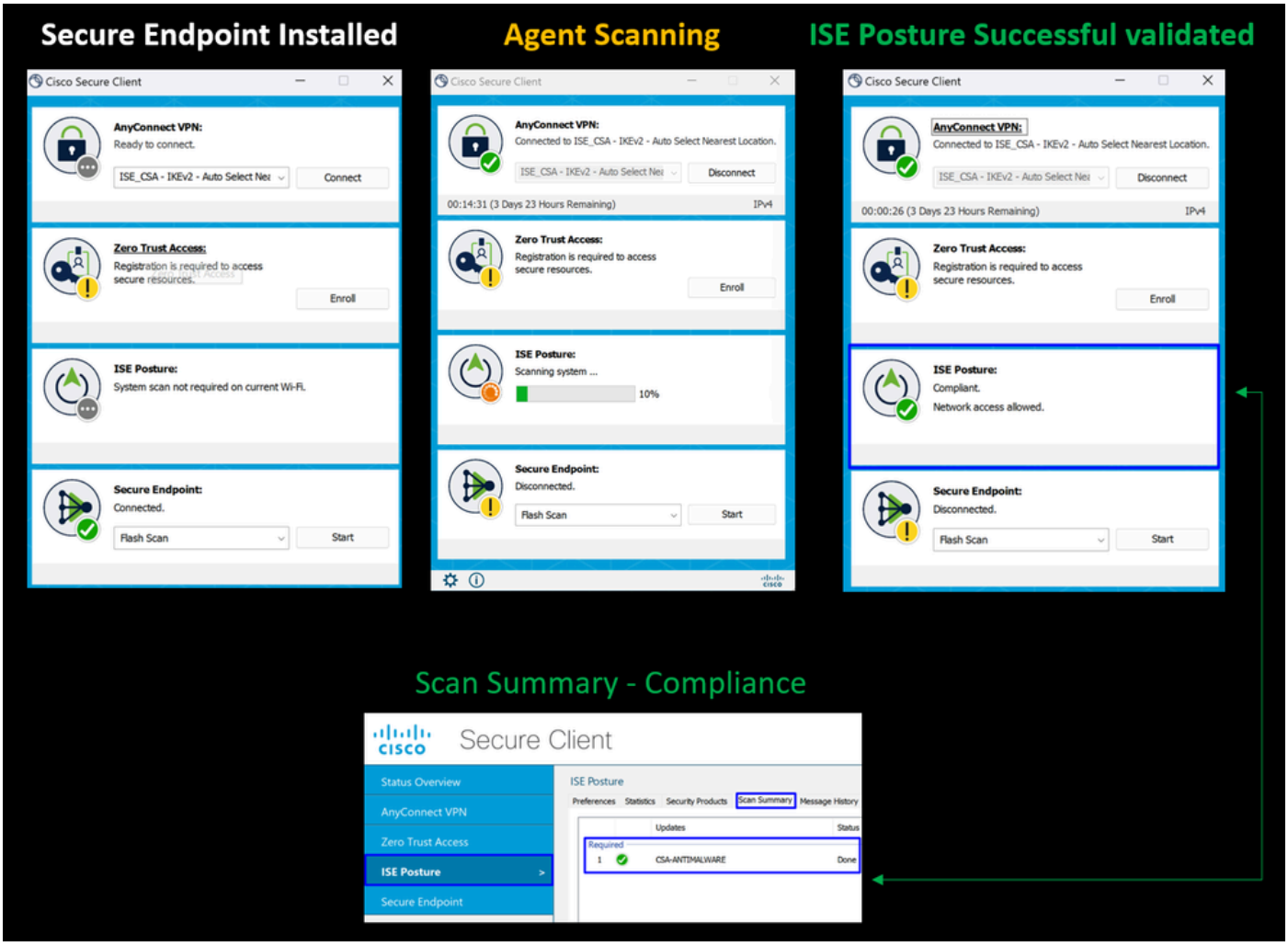
8. 安装代理后，ISE终端安全评估开始验证计算机的当前终端安全评估。如果不符合策略要求，系统将显示一个弹出窗口，指导您实现合规性。


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

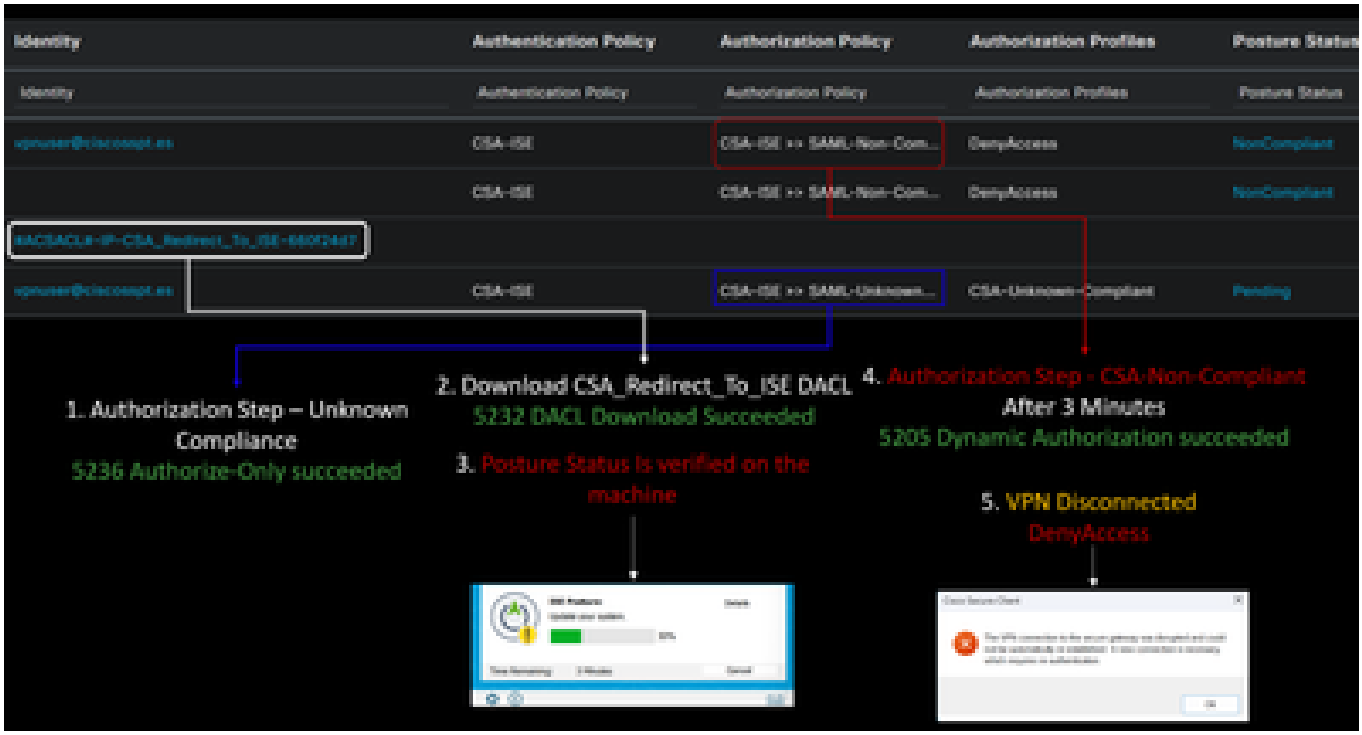

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE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

注意：如果Cancel您或剩余时间结束，您会自动变为不合规，并属于授权策略集CSA-Non-Compliance，然后立即与VPN断开连接。

9. 安装安全终端代理并再次连接到VPN。



10. 在代理验证计算机符合要求后，您的状态会变为处于投诉状态，并授予对网络上所有资源的访问权限。

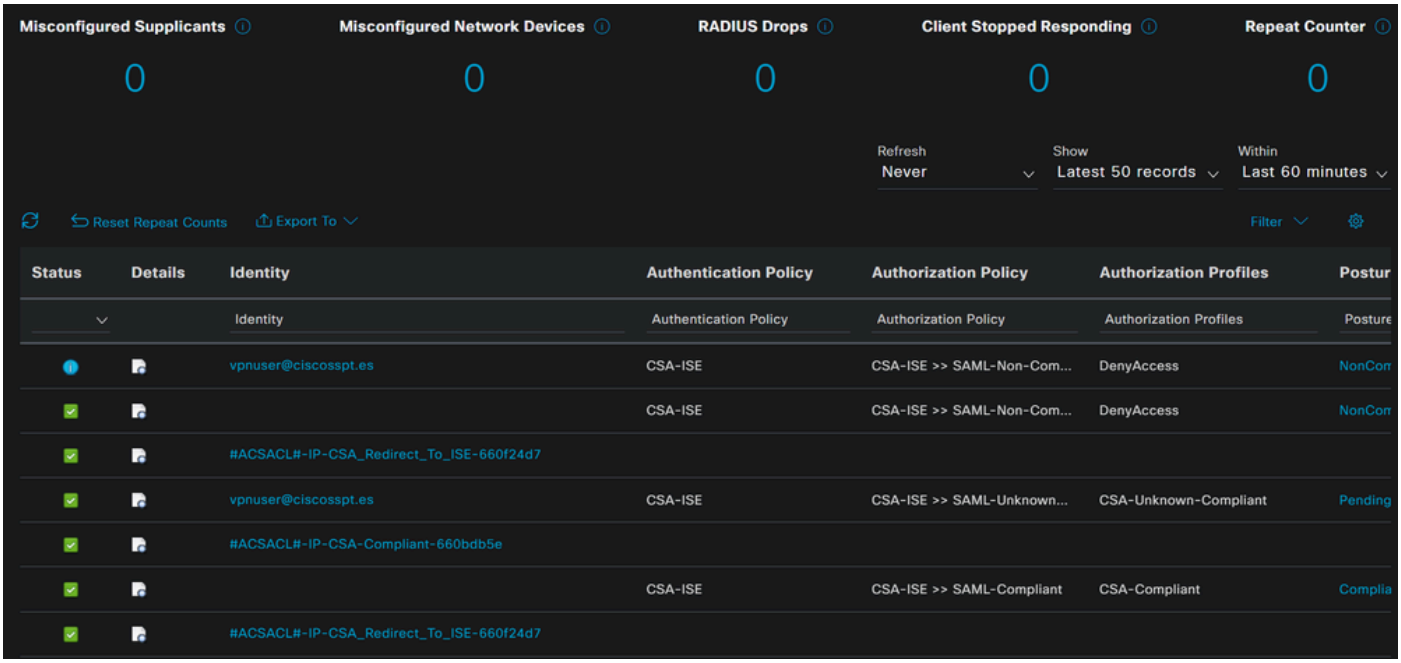


注意：在变为合规后，您属于授权策略集CSA-Compliance，并且您可以立即访问所有网络资源。

如何验证ISE中的日志

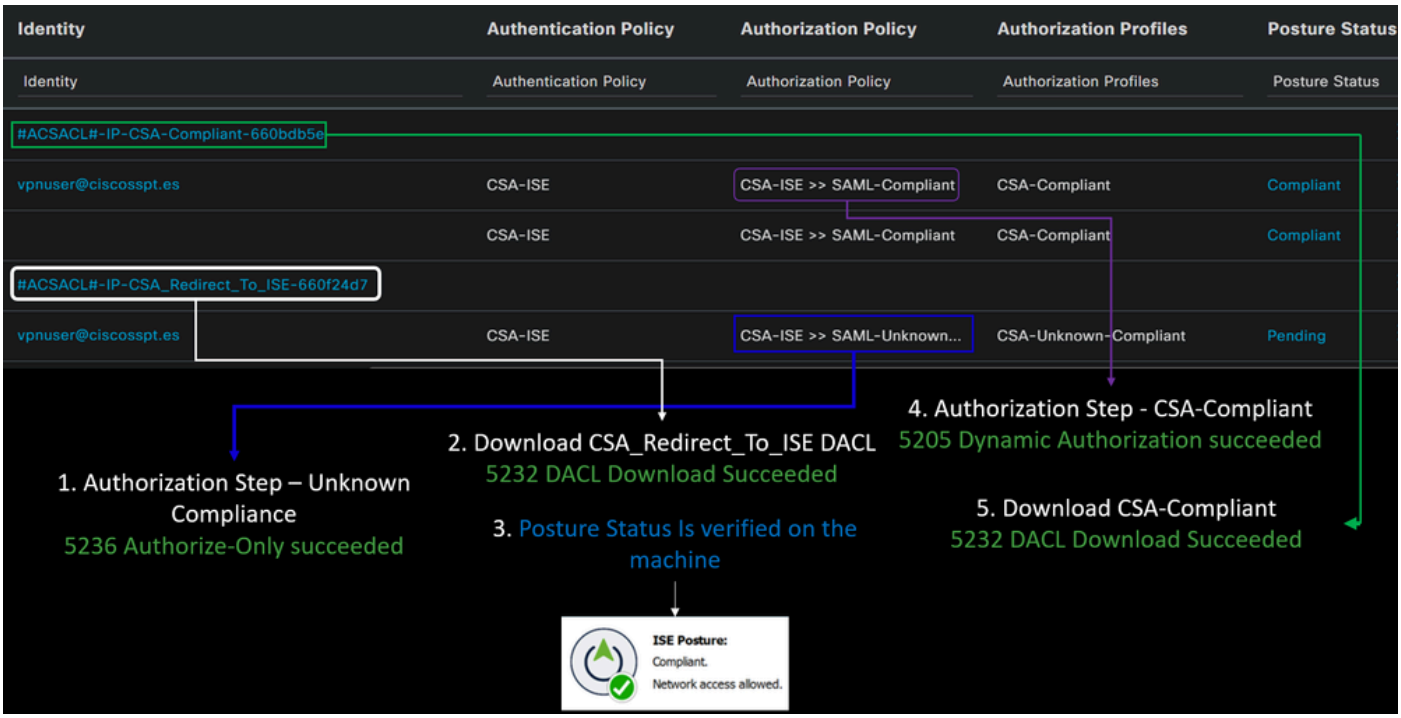
要验证用户的身份验证结果，您有两个合规和不合规的示例。要在ISE中查看该文档，请遵循以下说明：

- 导航到ISE控制面板
- 点击 Operations > Live Logs

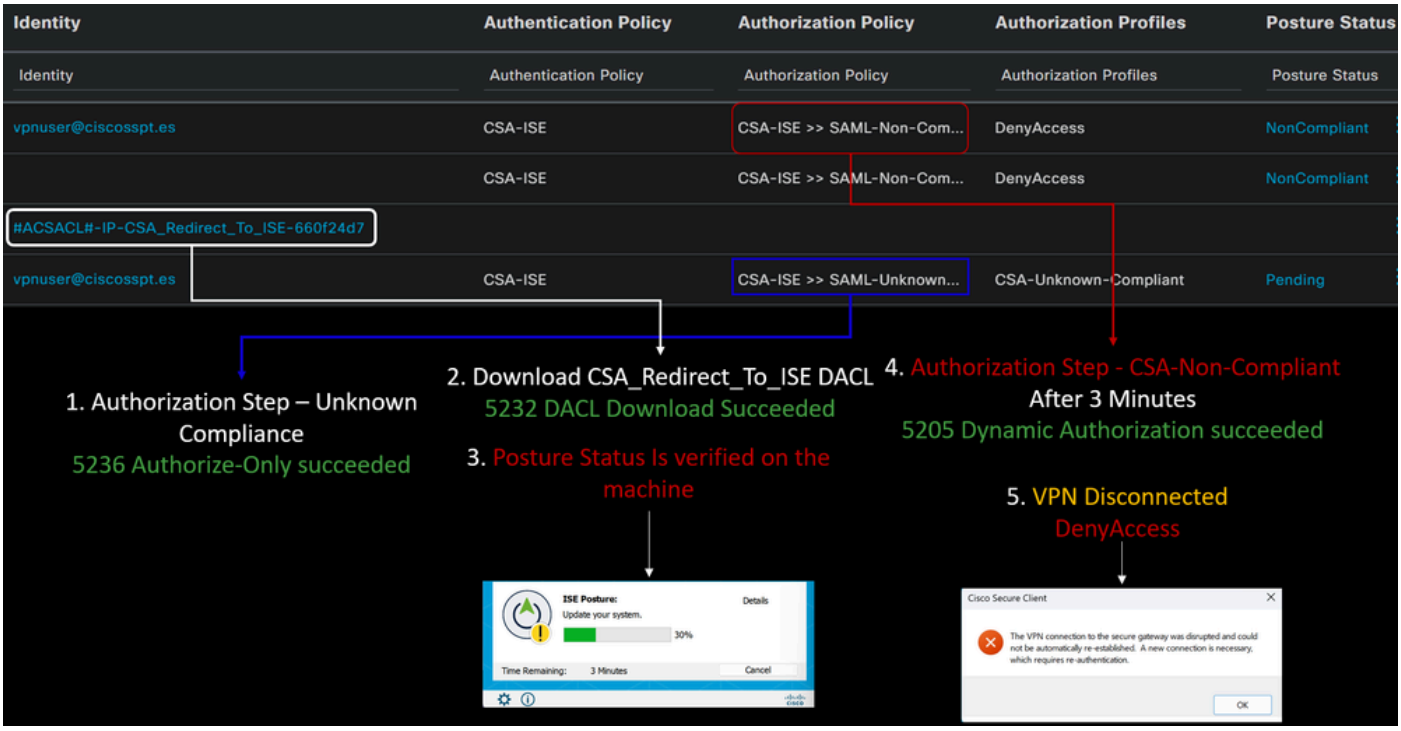


下一个主题方案演示如何在 **Live Logs**下显示成功的符合性和不遵从性事件：

合规性



不合规



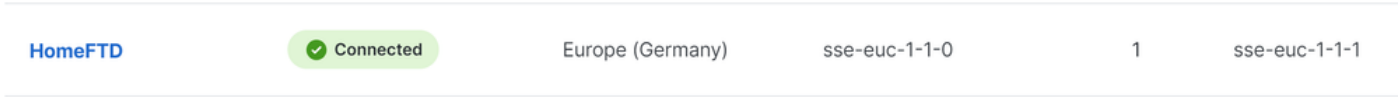
安全访问和ISE集成的第一步

在下一个示例中， Cisco ISE在网络192.168.10.0/24下，需要通过隧道配置添加可到达网络的配置。

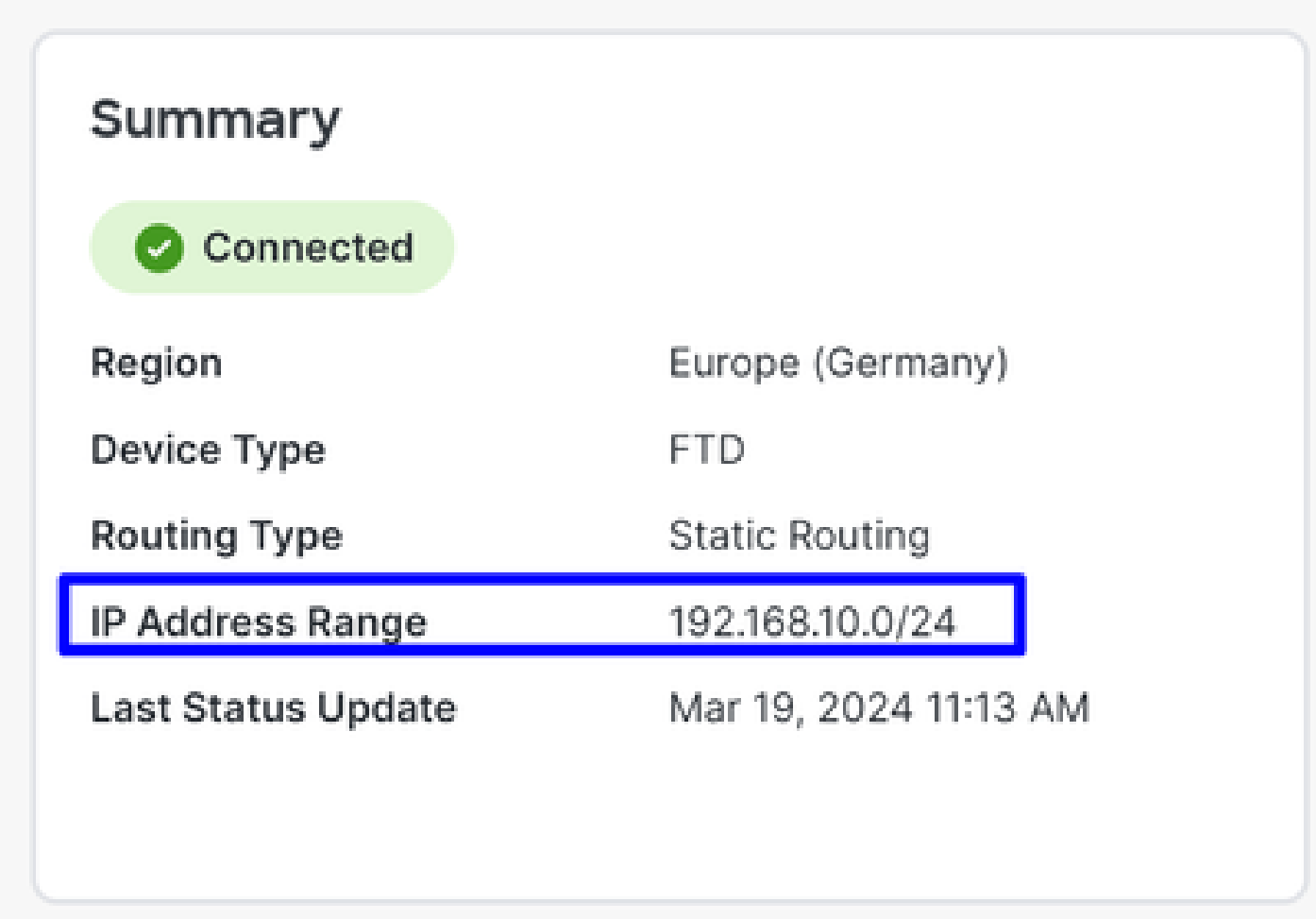
Step 1：验证您的隧道配置：

要对此进行验证，请导航到[安全访问控制面板]。

- 点击 **Connect > Network Connections**
- 点击**Network Tunnel Groups** >您的隧道



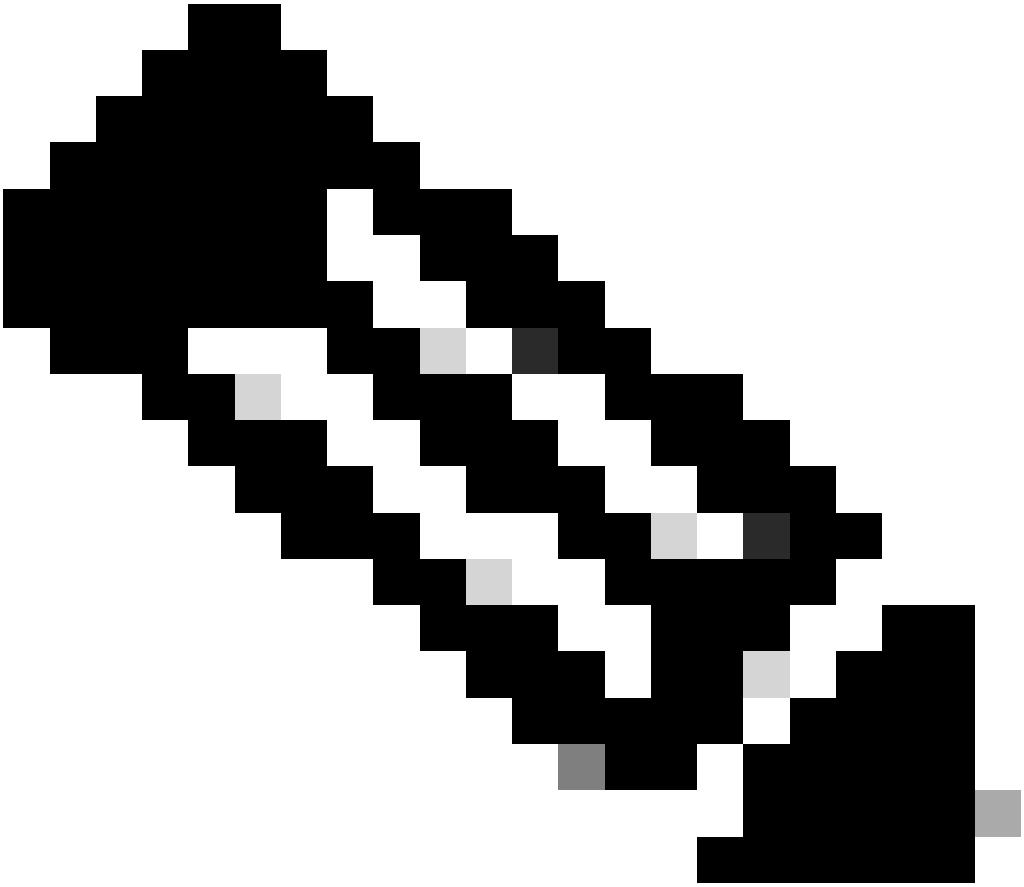
- 在summary下，验证隧道已配置您的思科ISE所在的地址空间：



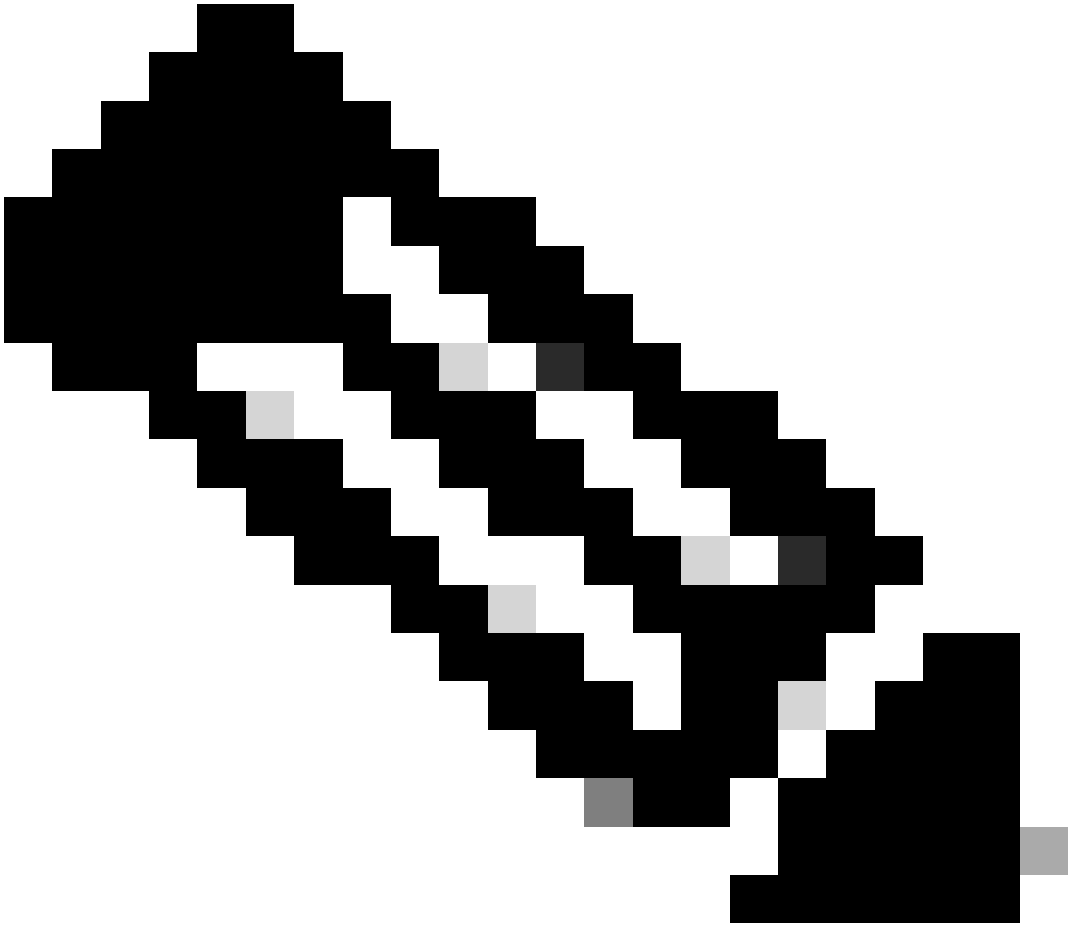
Step 2：允许防火墙上的流量。

要允许安全访问使用您的ISE设备进行RADIUS身份验证，您需要配置从安全访问到您的网络的规则以及所需的RADIUS端口：

规则	来源	目的地	目标端口
使用ISE保护访问 **管理池**	ISE_Server	管理IP池(RA-VPN)	**COA** UDP 1700（默认端口）
ISE的安全访问管理IP池	管理IP池	ISE_Server	**身份验证、授权** UDP 1812（默认端口） **记账** UDP 1813（默认端口）
安全访问终端IP池到ISE	终端IP池	ISE_Server	**调配门户** TCP 8443（默认端口）
安全访问终端IP池到DNS服务器	终端IP池	DNS 服务器	**DNS** UDP和TCP 53



注意：如果您想了解更多与ISE相关的端口，请查看用户指南-端口参考。



注意：如果已将ISE配置为通过某个名称（例如ise.ciscosspt.es）发现，则需要使用DNS规则

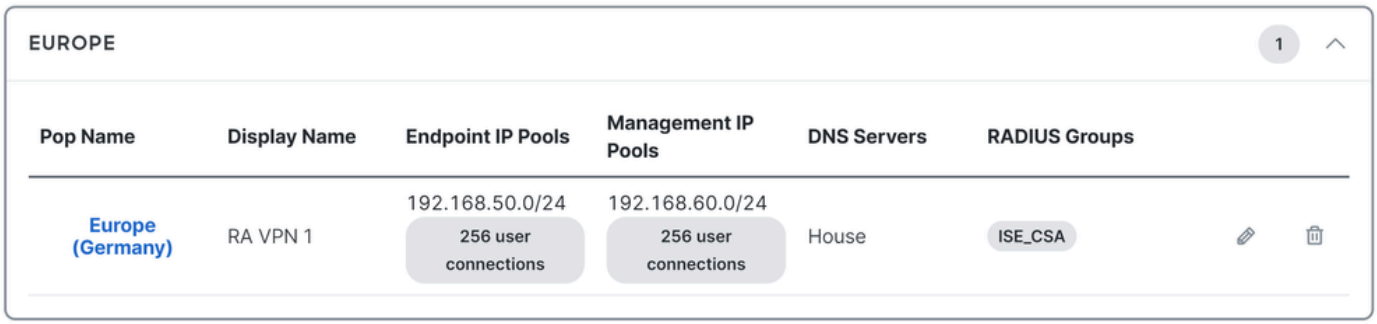
管理池和终端IP池

要验证您的管理和终端IP池，请导航到安全访问控制面板：

- 点击 **Connect > End User Connectivity**
- 点击 Virtual Private Network

- 低于 **Manage IP Pools**

- 点击 **Manage**



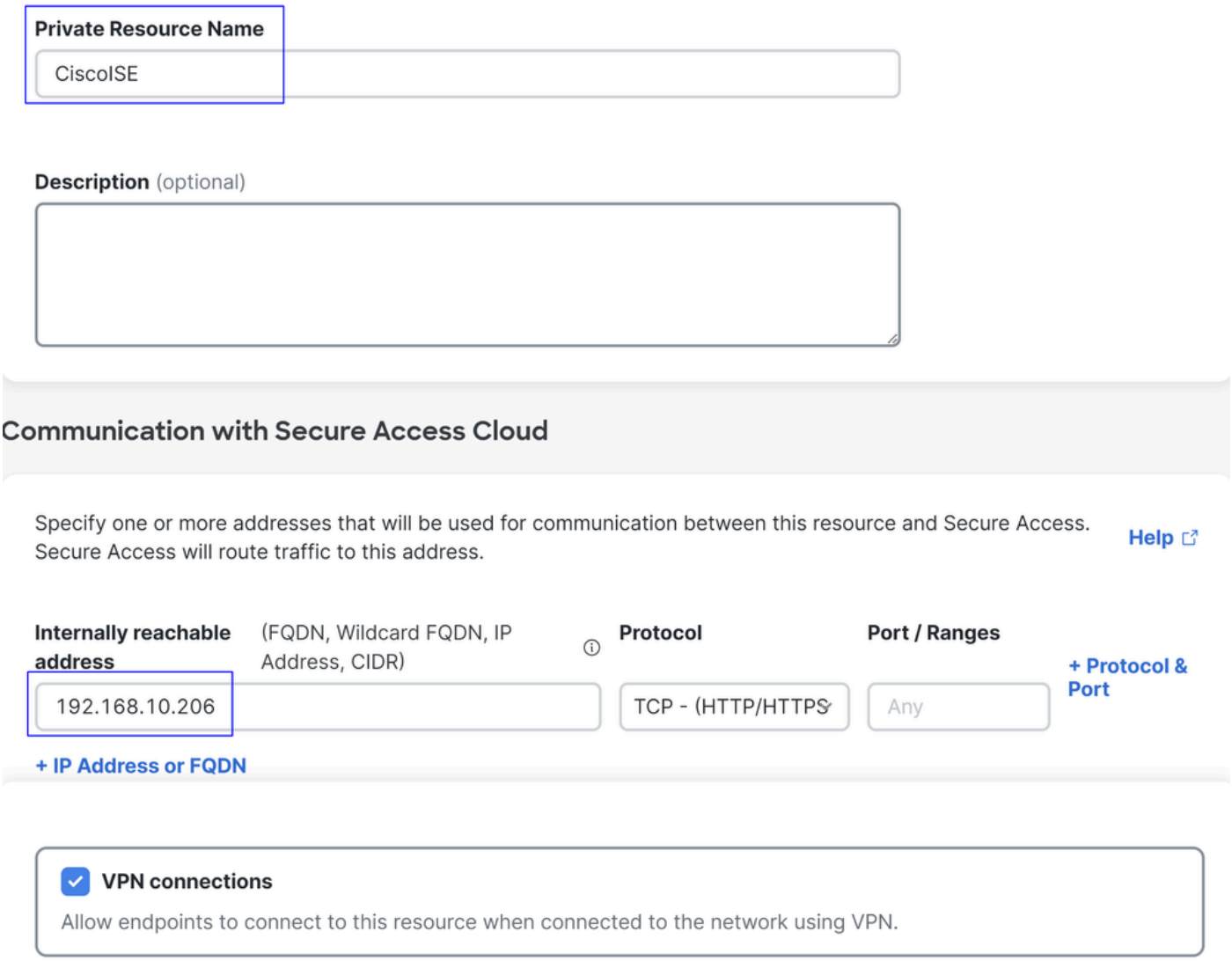
第3步：验证您的ISE是否在“Private Resources”（专用资源）下配置

要允许通过VPN连接的用户导航到**ISE Provisioning Portal**功能，您需要确保将设备配置为私有资源以提供访问，该资源用于允许通过VPN自动调配ISE Posture Module。

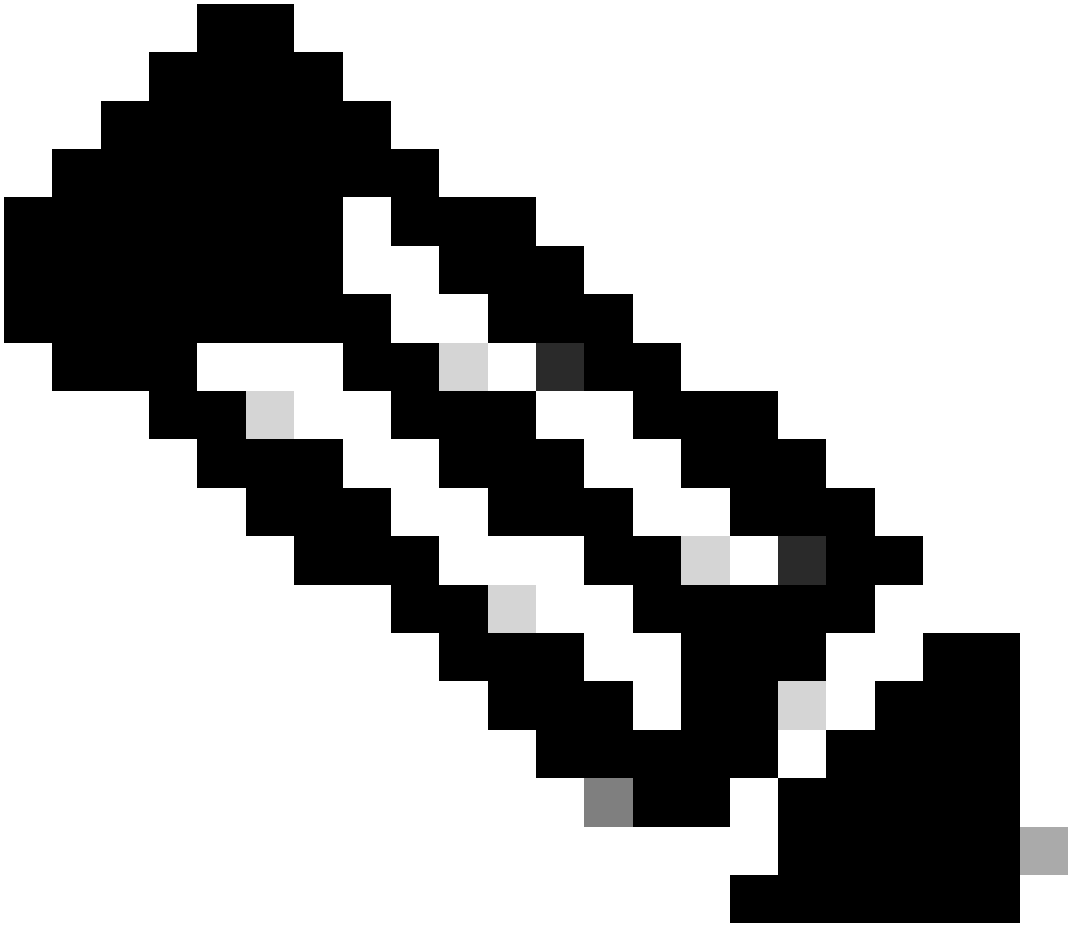
要验证您是否已正确配置ISE，请导航到安全访问控制面板：

- 点击 **Resources** > **Private Resources**

- 点击ISE资源



如果需要，您可以将规则限制为调配门户端口(8443)。



注意：请确保已标记VPN连接的复选框。

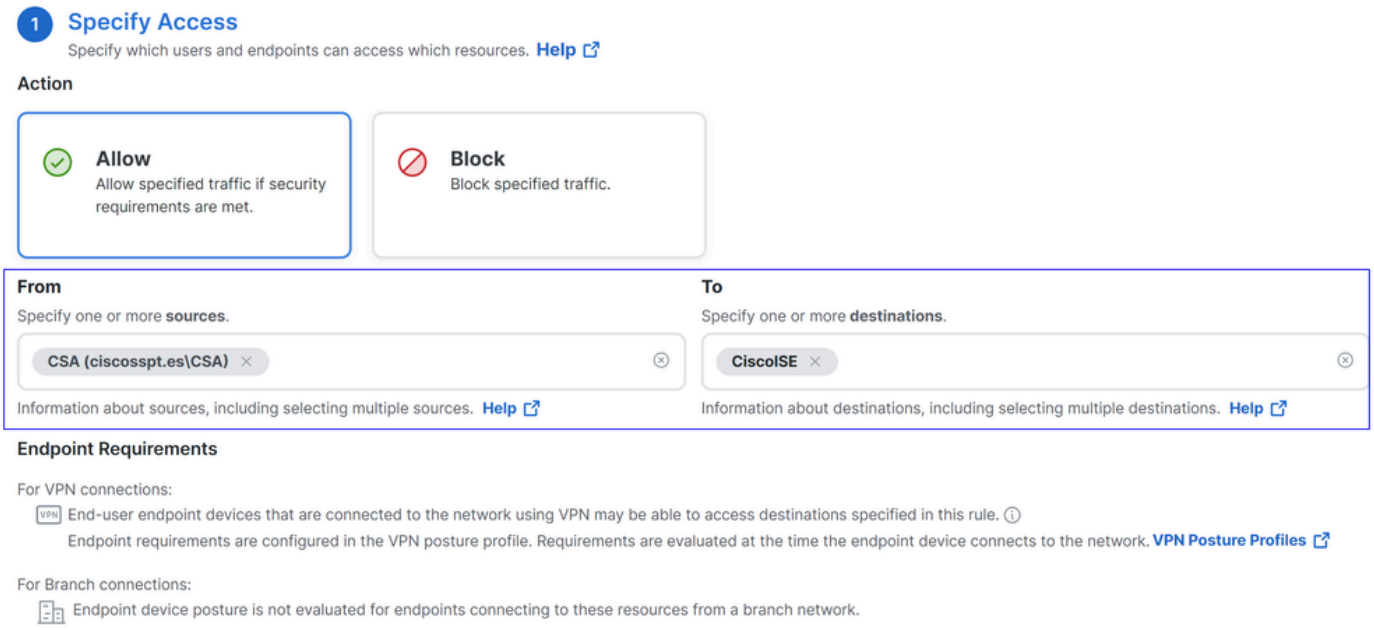
第4步：根据访问策略允许ISE访问

要允许通过VPN连接的用户导航到**ISE Provisioning Portal**命令，您需要确保已配置**Access Policy** 命令，以允许根据该规则配置的用户访问在Step3中配置的私有资源。

要验证您是否已正确配置ISE，请导航到安全访问控制面板：

- 点击 **Secure > Access Policy**

- 点击配置的规则，以允许对VPN用户访问ISE

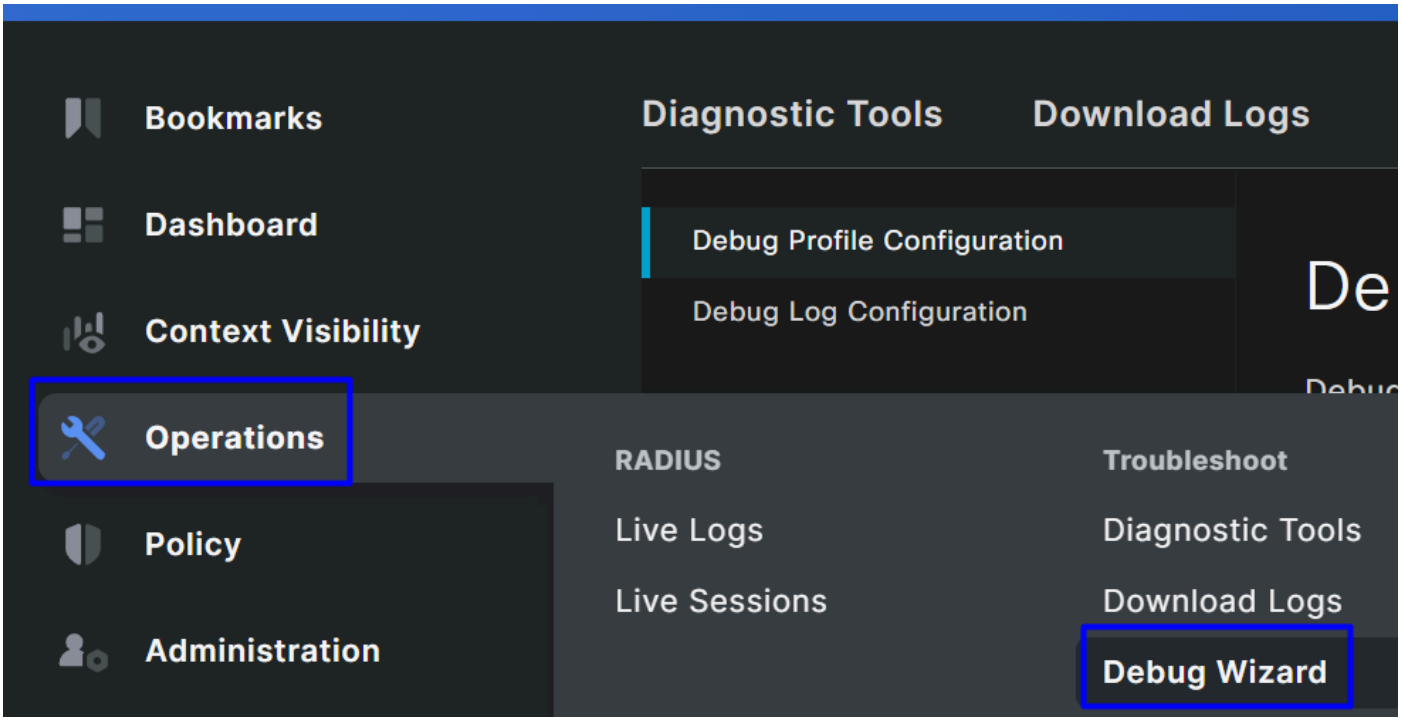


故障排除

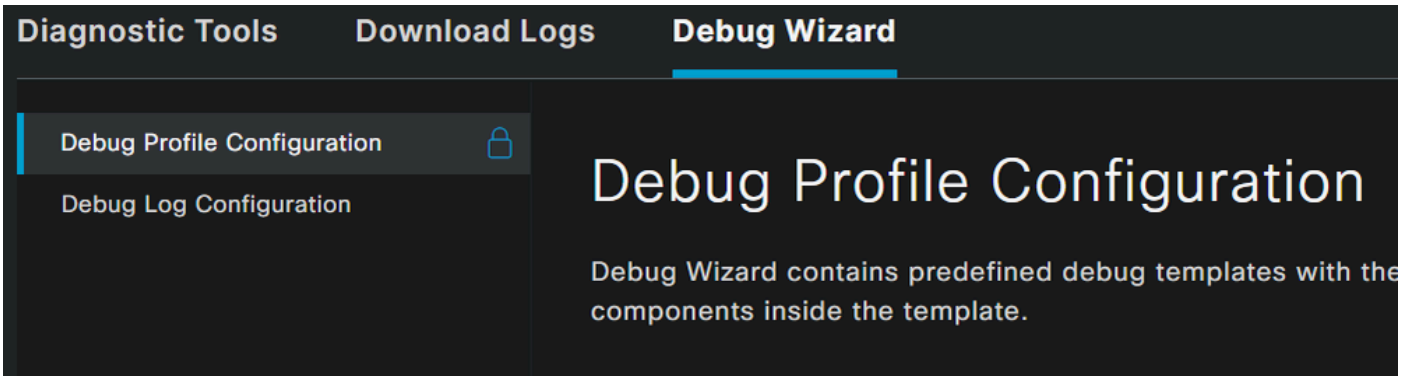
如何下载ISE终端安全评估调试日志

要下载ISE日志以验证与终端安全评估相关的问题，请继续执行以下步骤：

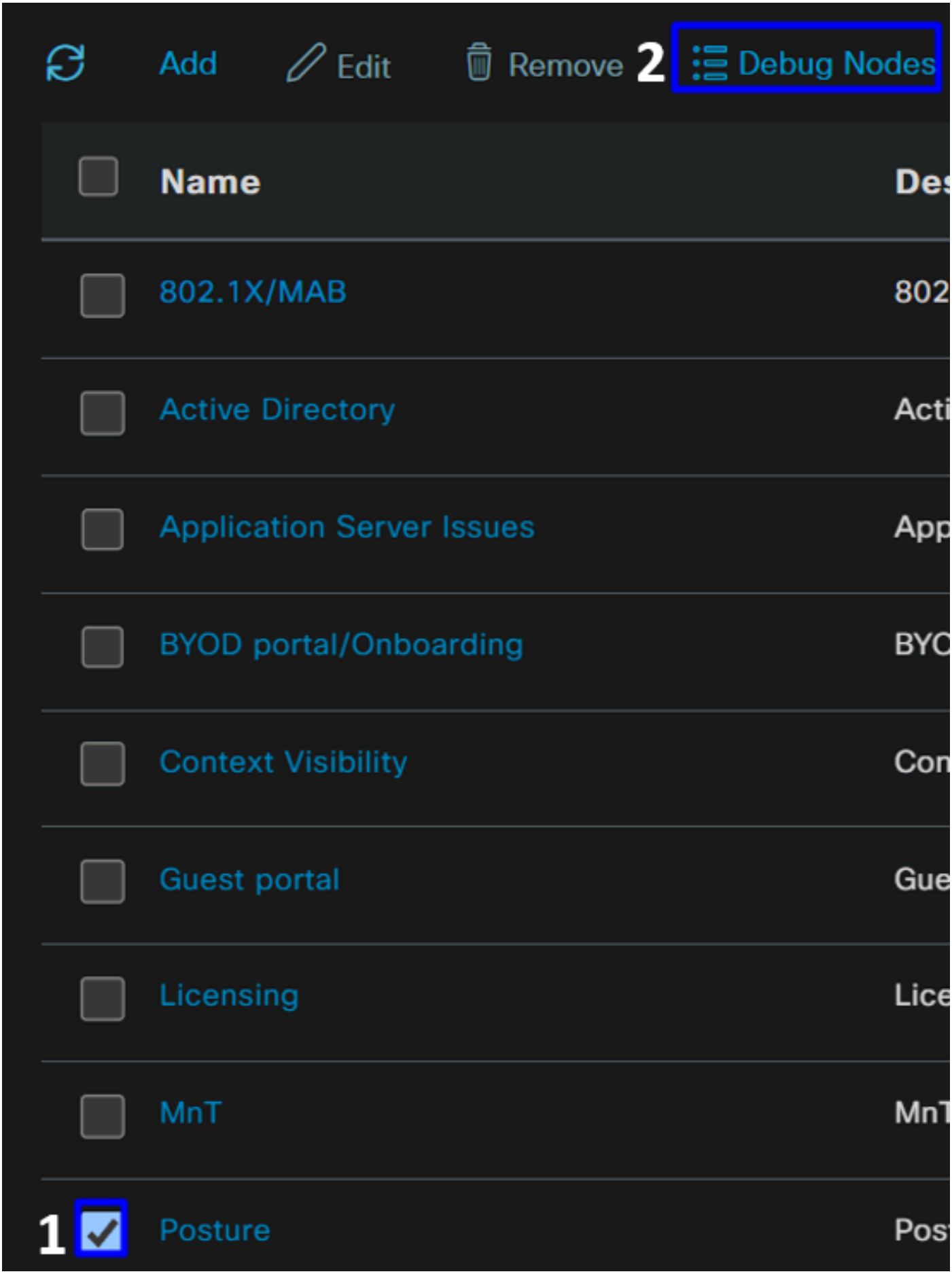
- 导航到ISE控制面板
- 点击 Operations > Troubleshoot > Debug Wizard



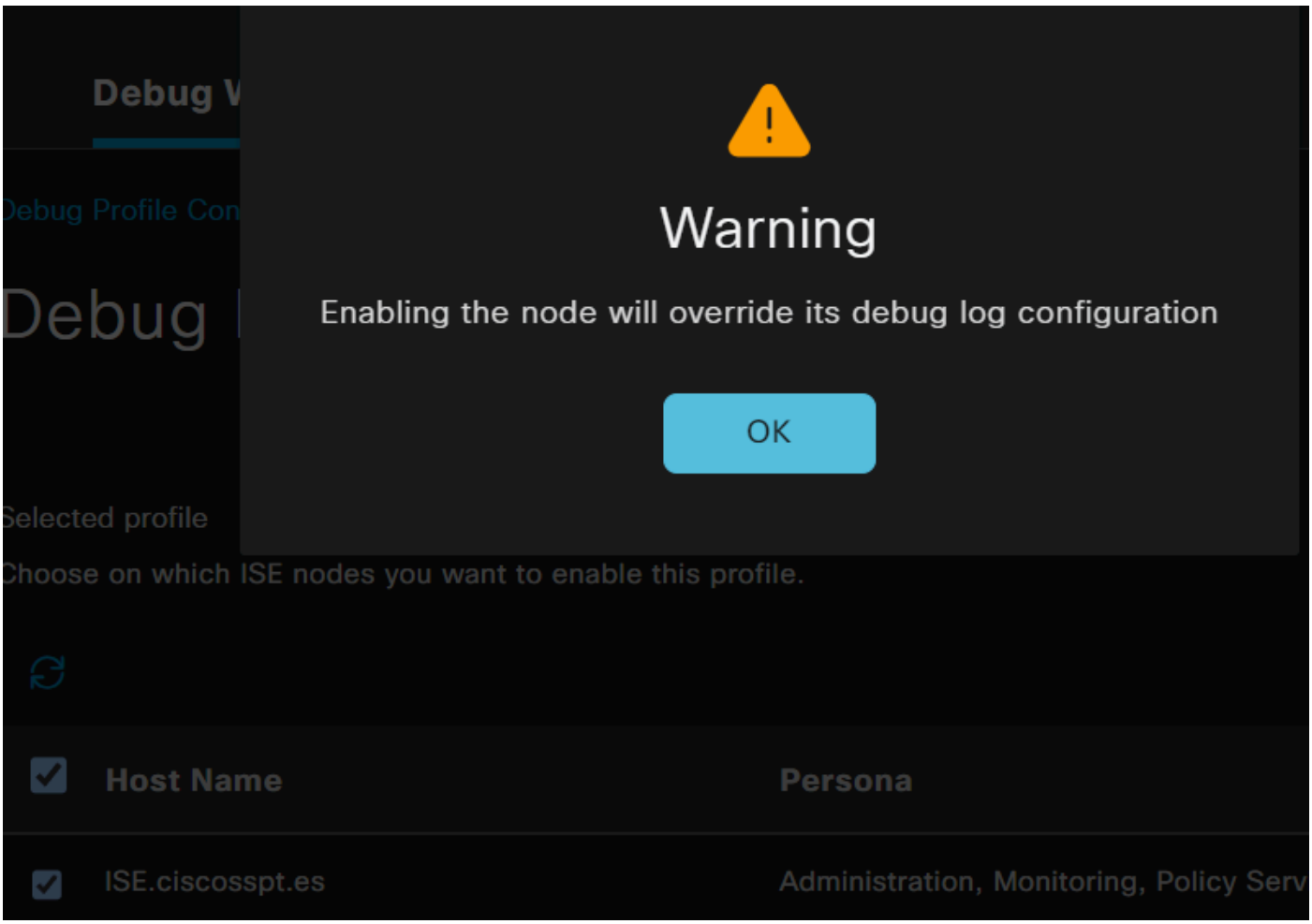
- 点击 Debug Profile Configuration



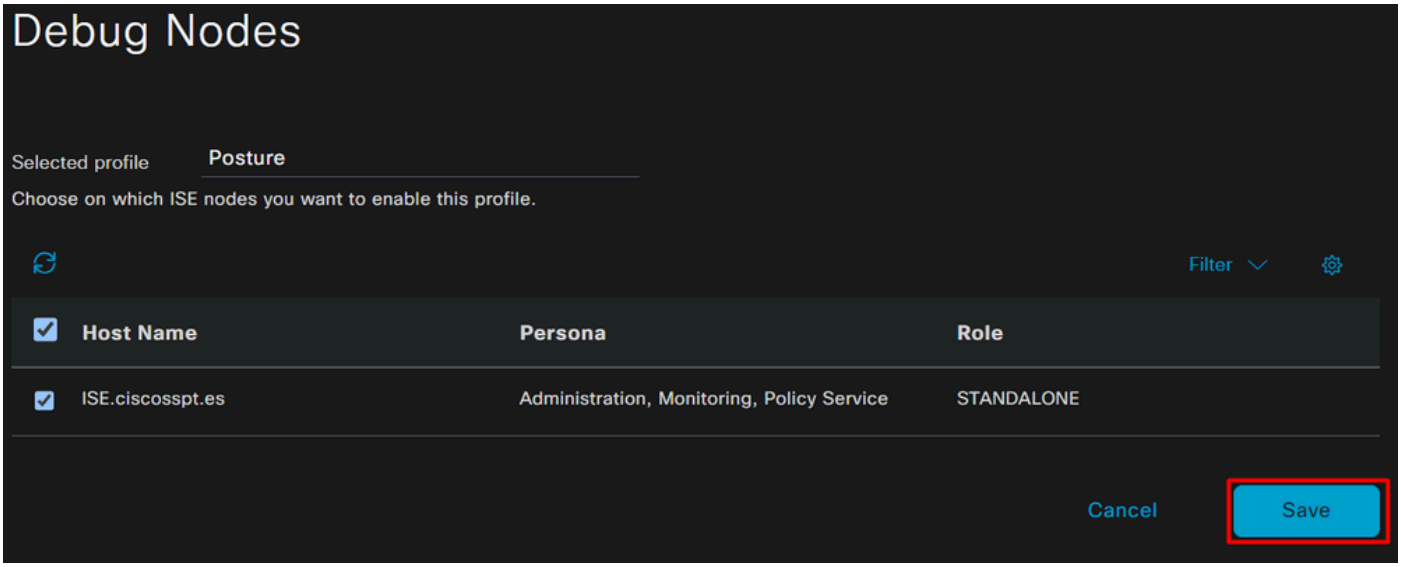
- 选中复选框 **Posture** > **Debug Nodes**

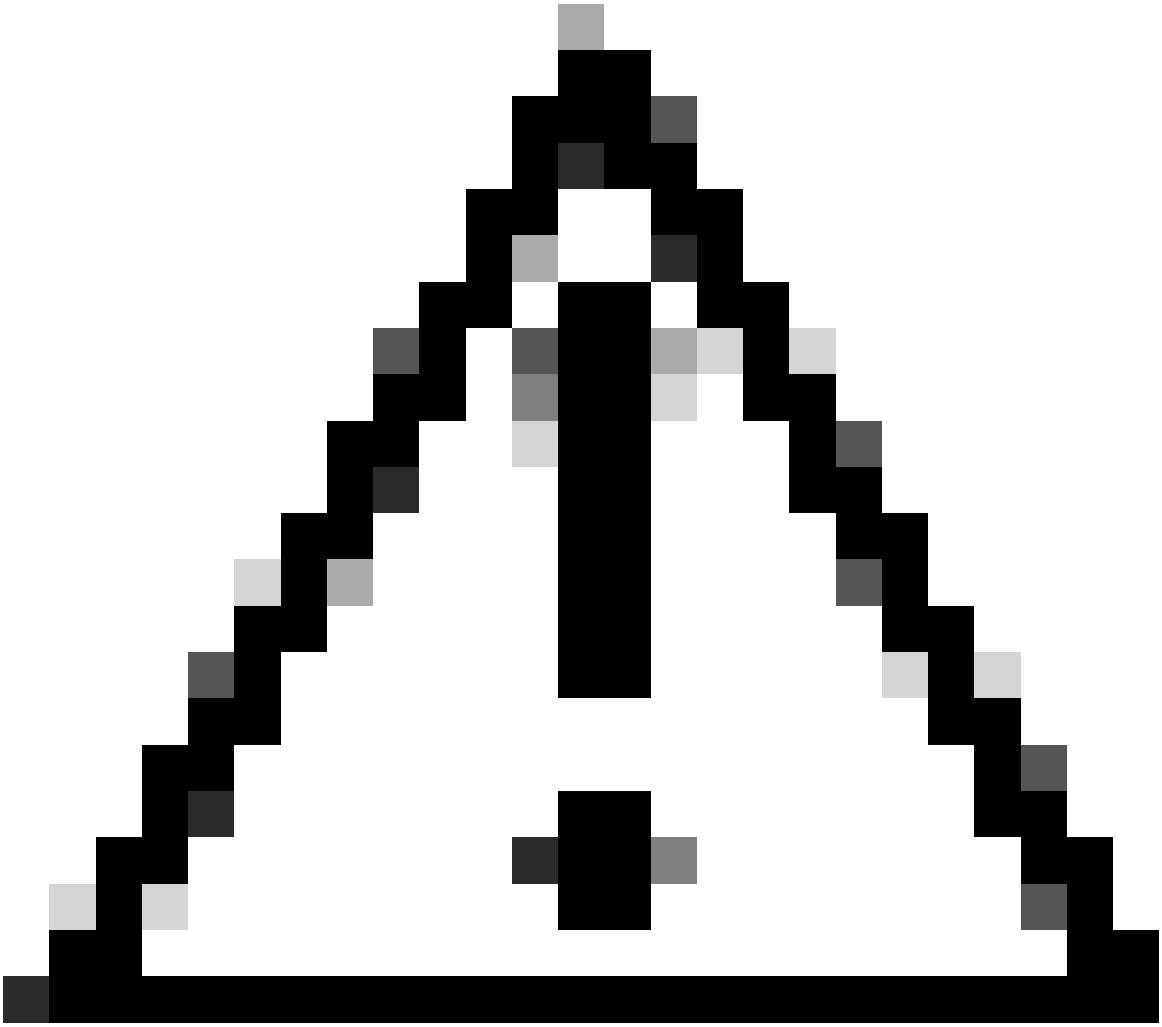

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- 选中您要在其中启用调试模式以解决问题的ISE节点的复选框



- 点击 Save

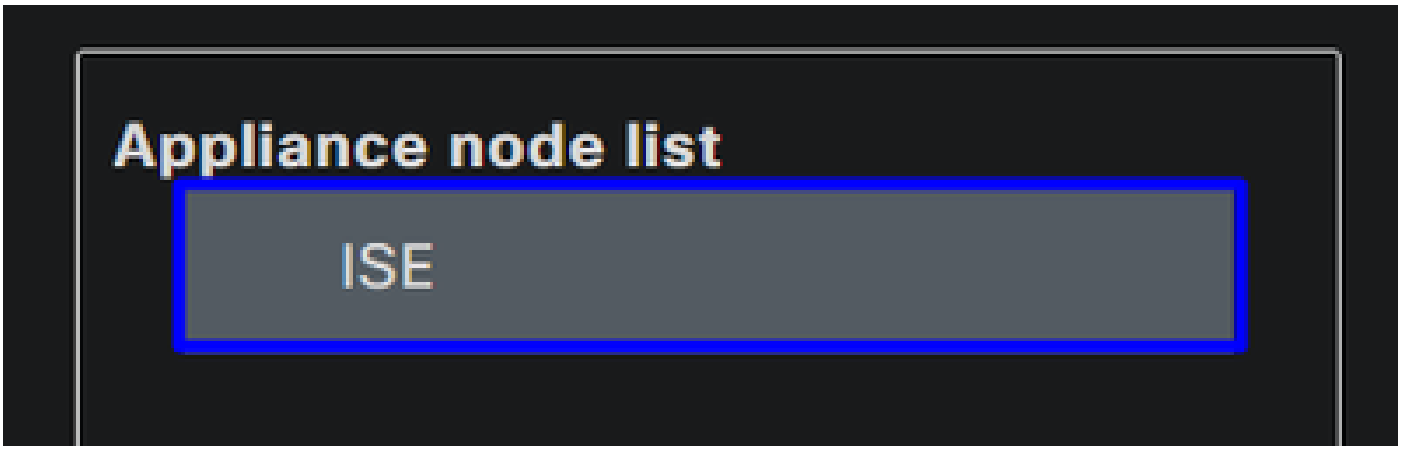

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



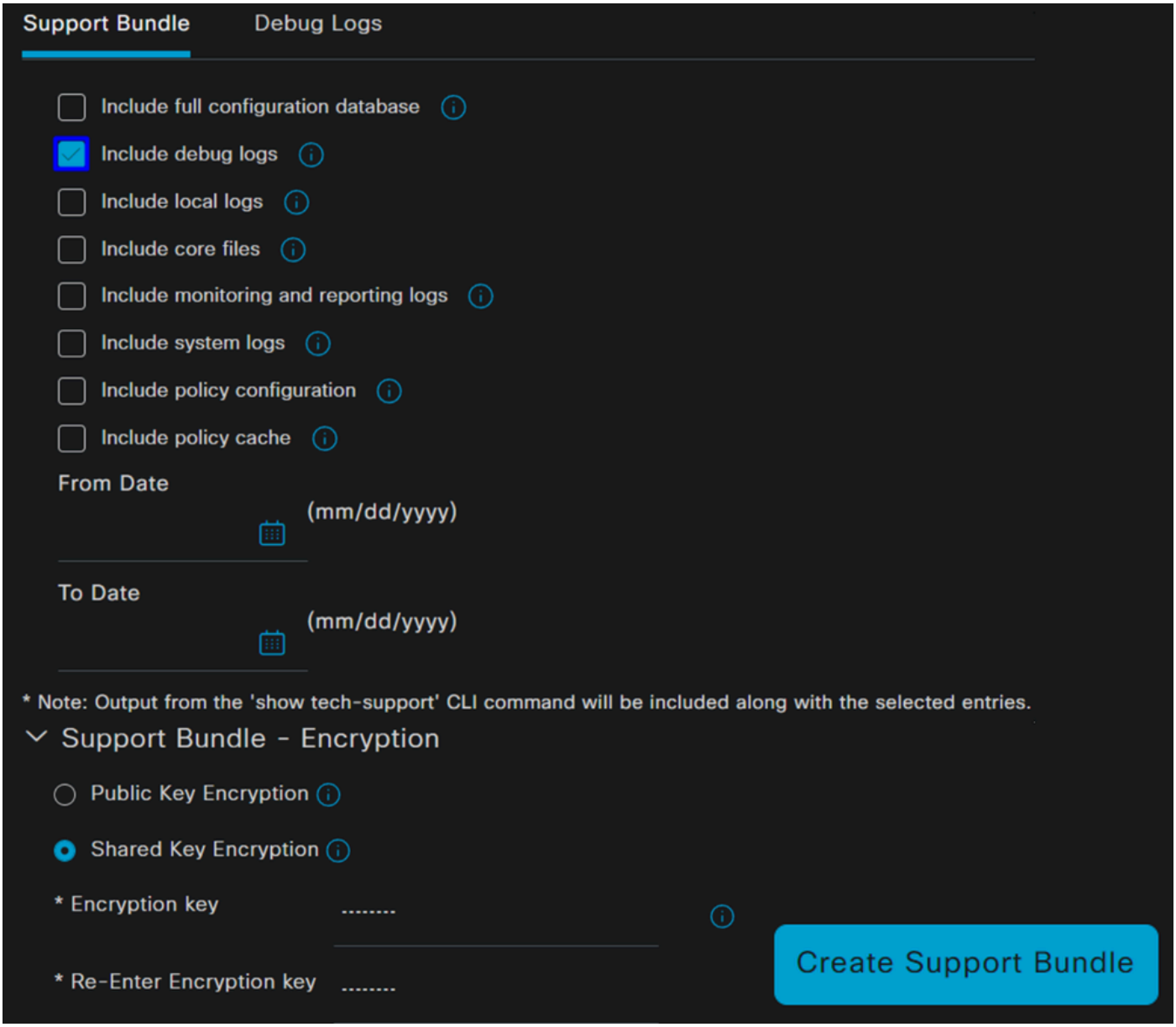
注意：在此点之后，您必须开始重现问题； **the debug logs can affect the performance of your device**。

在重现问题后，请继续后续步骤：

- 点击 Operations > Download Logs
- 选择要从中获取日志的节点

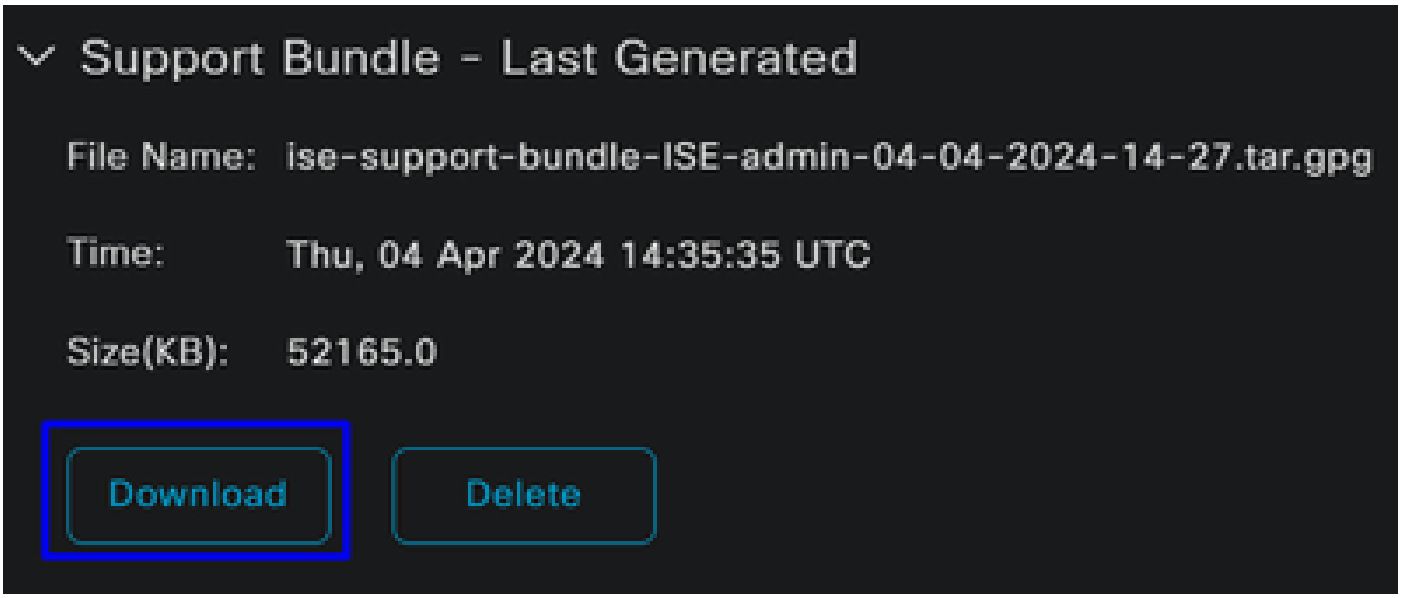


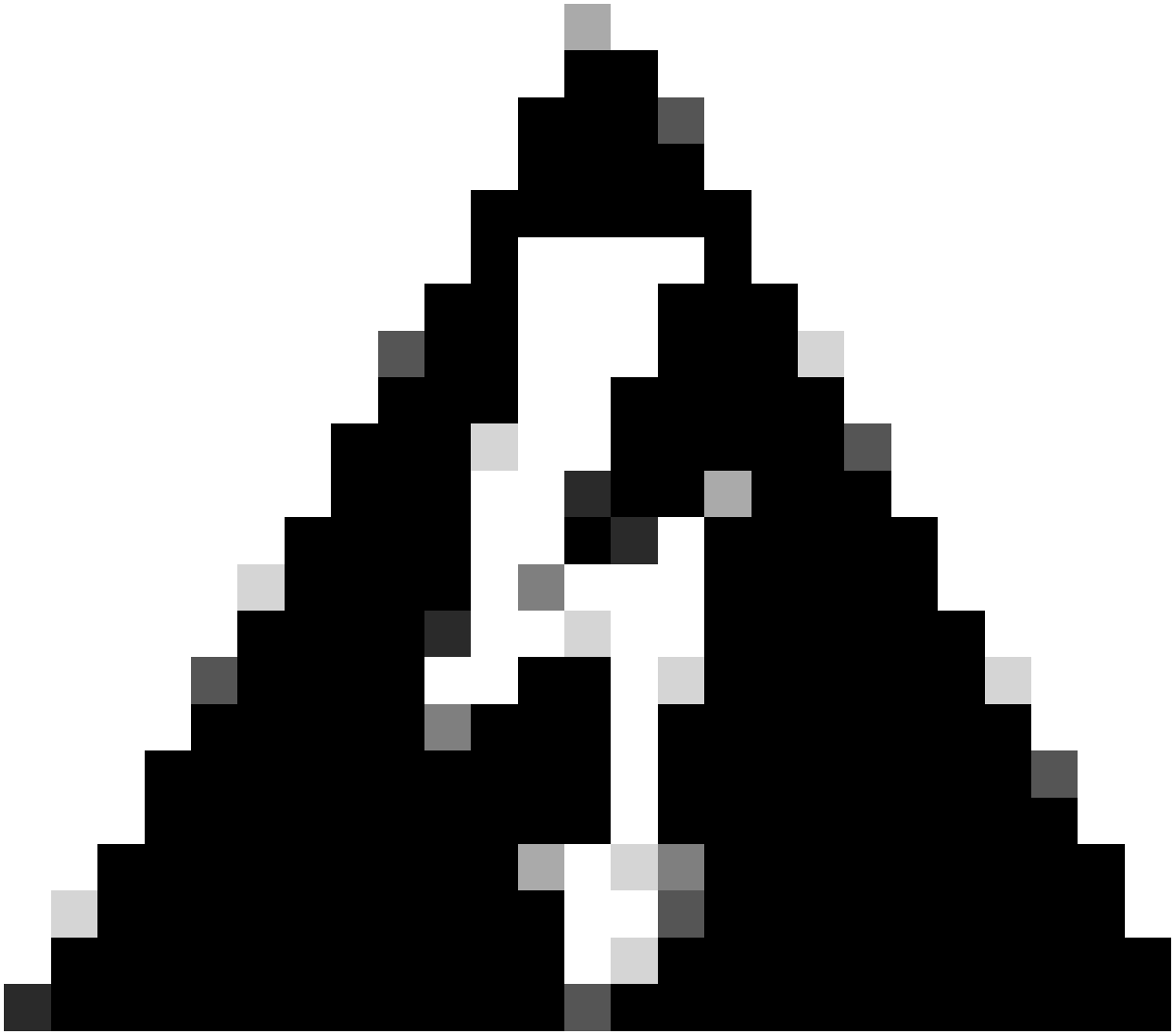
- 在 **Support Bundle**，选择以下选项：



- Include debug logs
- 低于 **Support Bundle Encryption**
    - **Shared Key Encryption**
        - 填充**Encryption key** 和 **Re-Enter Encryption key**

- 点击 **Create Support Bundle**
- 点击 **Download**



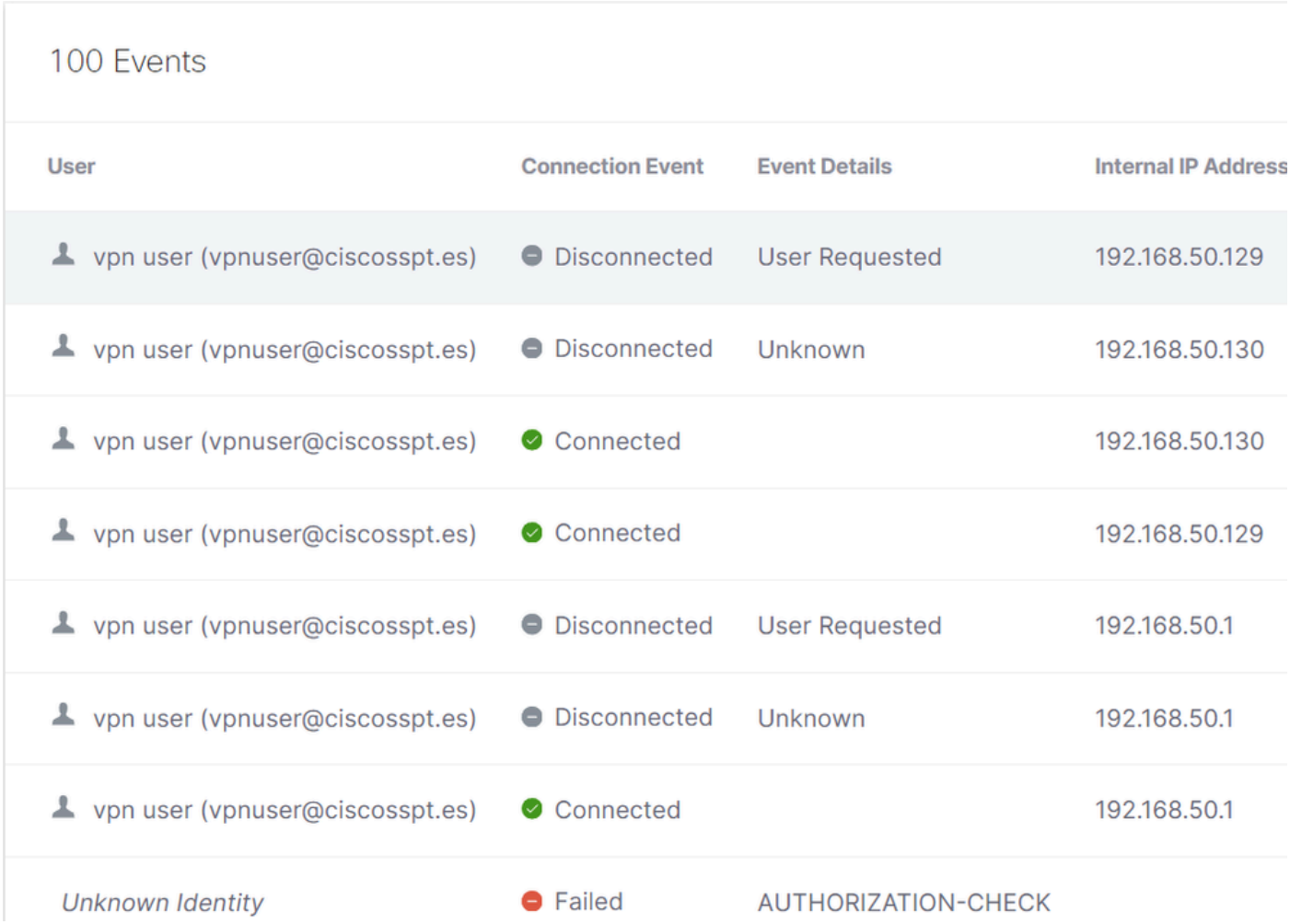


警告：禁用在步骤Debug Profile Configuration上启用的调试模式

如何验证安全访问远程访问日志

导航到您的安全访问控制面板：

- 点击 Monitor > Remote Access Logs



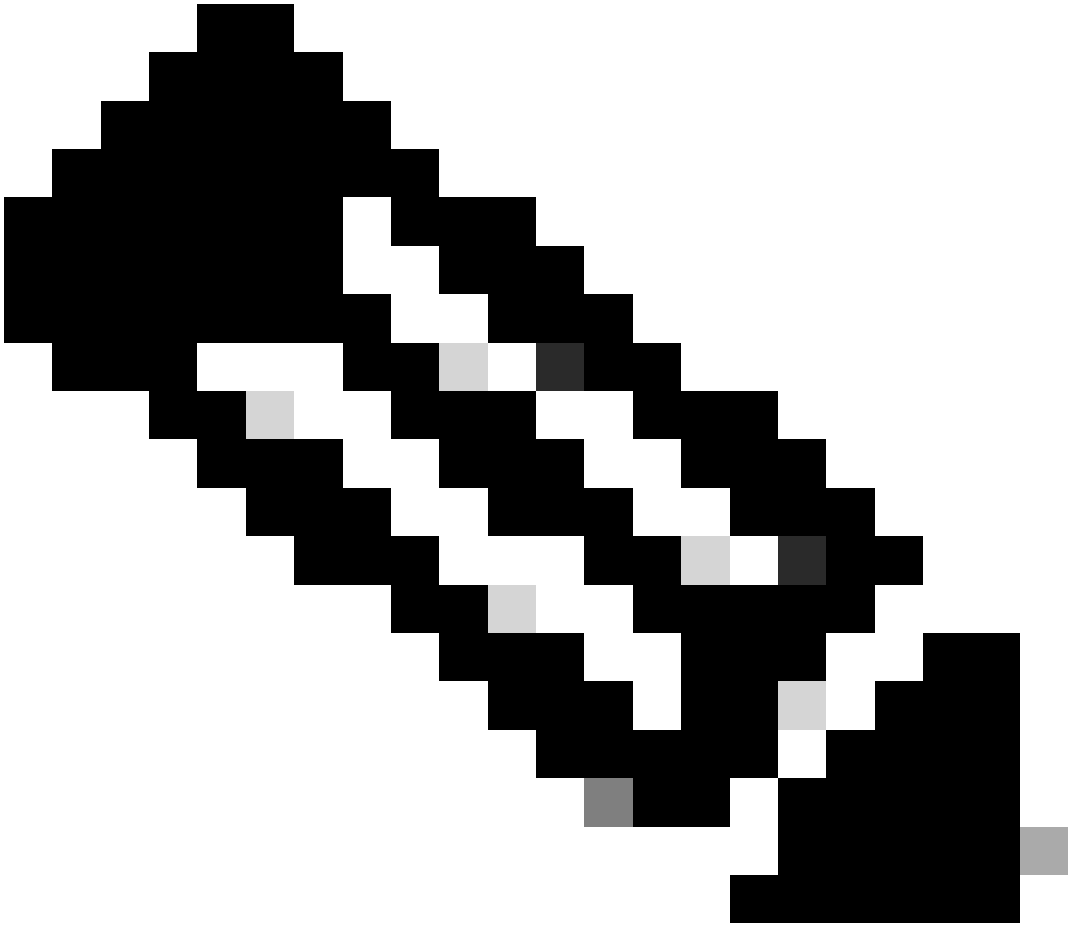
100 Events

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

在安全客户端上生成DART捆绑包

要在您的计算机上生成DART捆绑包，请验证以下文章：

思科安全客户端诊断和报告工具(DART)



注意：收集了故障排除部分所述的日志后，请通过**TAC** 提交支持请求，以继续分析信息。

相关信息

- 思科技术支持和下载
- 安全访问文档和用户指南

- **Cisco Secure Client软件下载**

- 思科身份服务引擎管理员指南，版本3.3

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。