Configuration de l'accès sécurisé pour RA-VPNaaS avec Duo SSO et évaluation de la position avec ISE

Table des matières

Introduction

Ce document décrit comment configurer l'évaluation de position pour les utilisateurs VPN d'accès à distance avec Identity Service Engine (ISE) et l'accès sécurisé avec Duo.

Conditions préalables

- Configurer le provisionnement utilisateur sur un accès sécurisé
- Configuration de Duo SSO avec le proxy d'authentification ou le IDP tiers
- Cisco ISE connecté à Secure Access via le tunnel

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Service Engine
- Accès sécurisé
- Client sécurisé Cisco
- Guide d'authentification à deux facteurs - Duo Security
- Posture ISE
- Authentification, autorisation et administration (AAA)

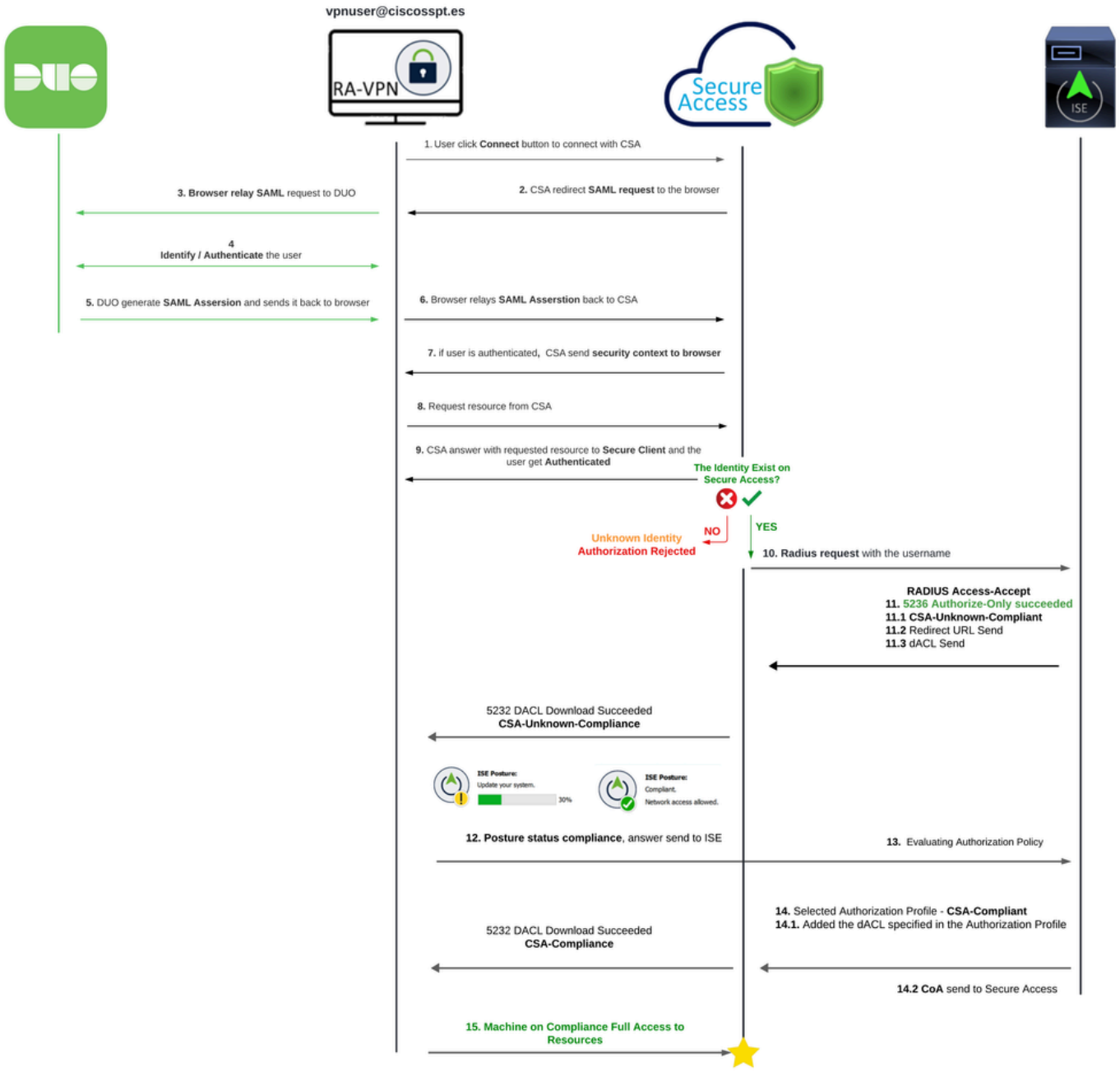
Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Identity Service Engine (ISE) version 3.3, correctif 1
- Accès sécurisé
- Client sécurisé Cisco - Anyconnect VPN Version 5.1.2.42

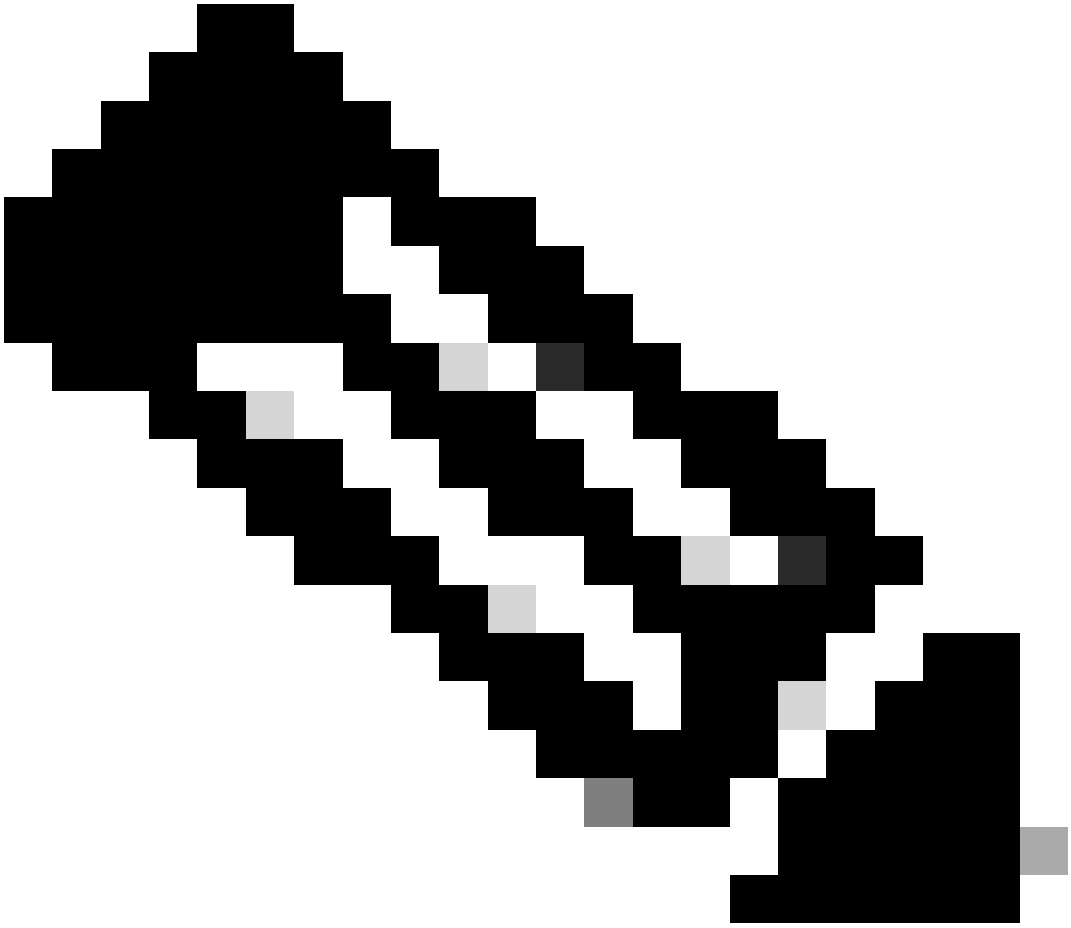
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales



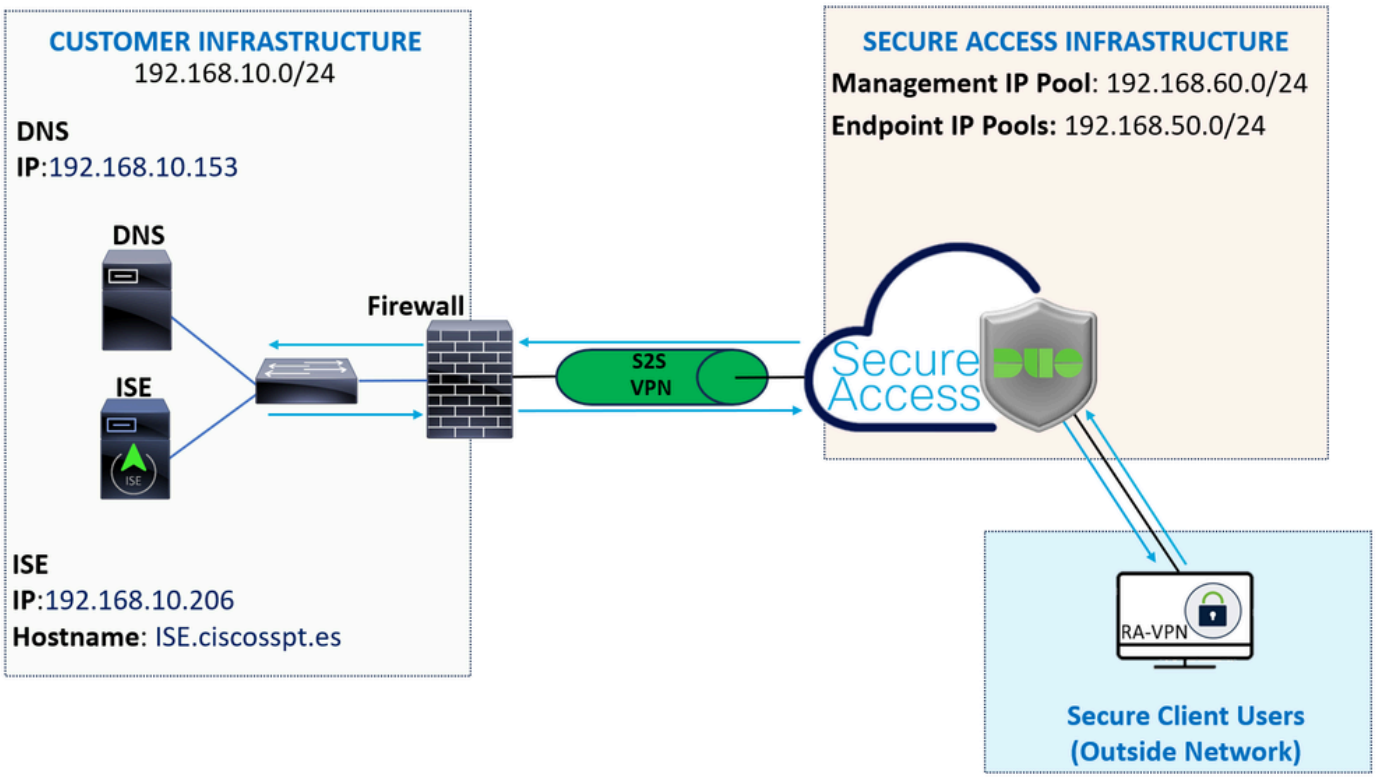
L'intégration de Duo SAML avec Cisco Identity Services Engine (ISE) améliore le processus d'authentification, ajoutant une couche de sécurité supplémentaire aux solutions Cisco Secure Access. Duo SAML fournit une fonctionnalité SSO (Single Sign-On) qui simplifie le processus de connexion des utilisateurs tout en garantissant des normes de sécurité élevées.

Une fois authentifié via Duo SAML, le processus d'autorisation est géré par Cisco ISE. Cela permet des décisions de contrôle d'accès dynamiques basées sur l'identité de l'utilisateur et la position du périphérique. ISE peut appliquer des politiques détaillées qui dictent quelles ressources un utilisateur peut accéder, quand et à partir de quels périphériques.

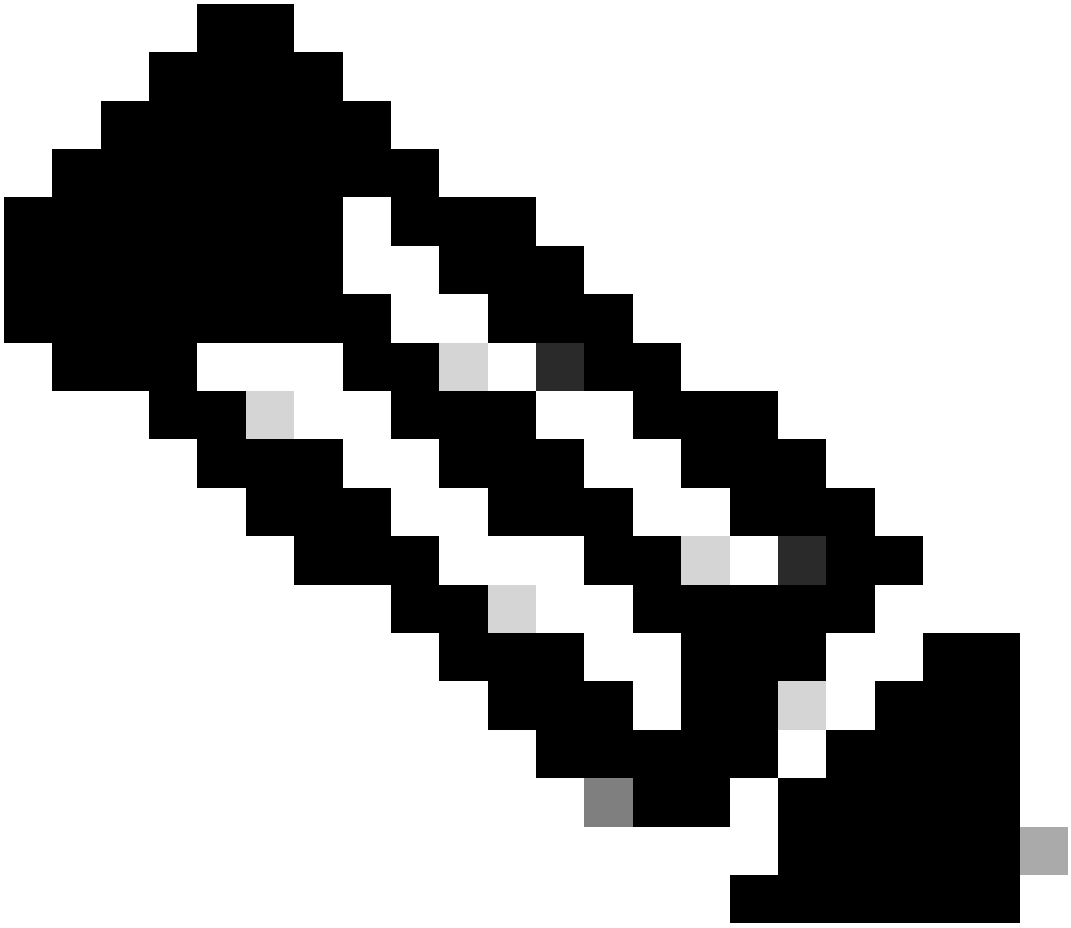


Remarque : Pour configurer l'intégration RADIUS, vous devez vous assurer que vous avez une communication entre les deux plates-formes.

Diagramme du réseau


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

Configurer



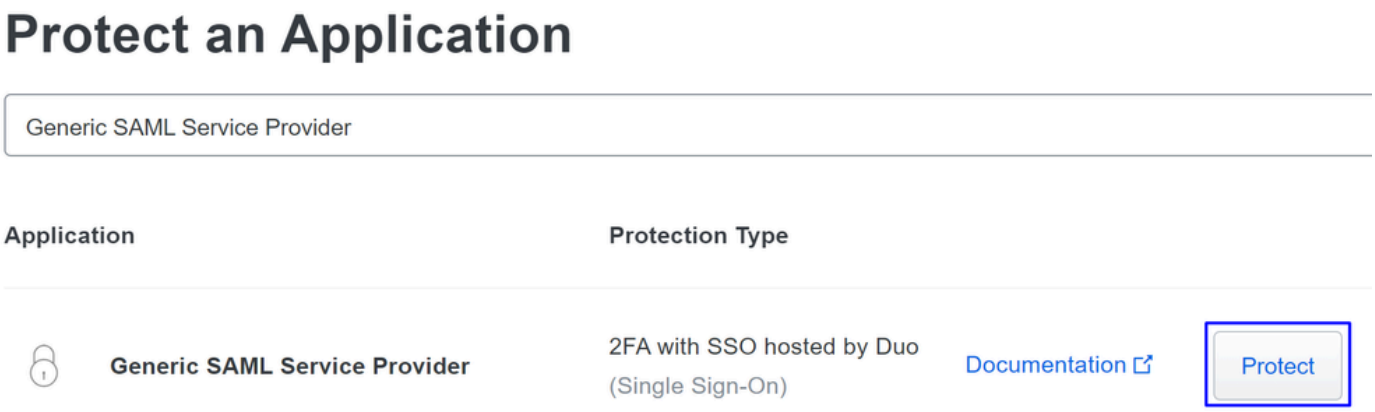
Remarque : avant de commencer le processus de configuration, vous devez effectuer les premières étapes avec Secure Access et l'intégration ISE.

Configuration Duo

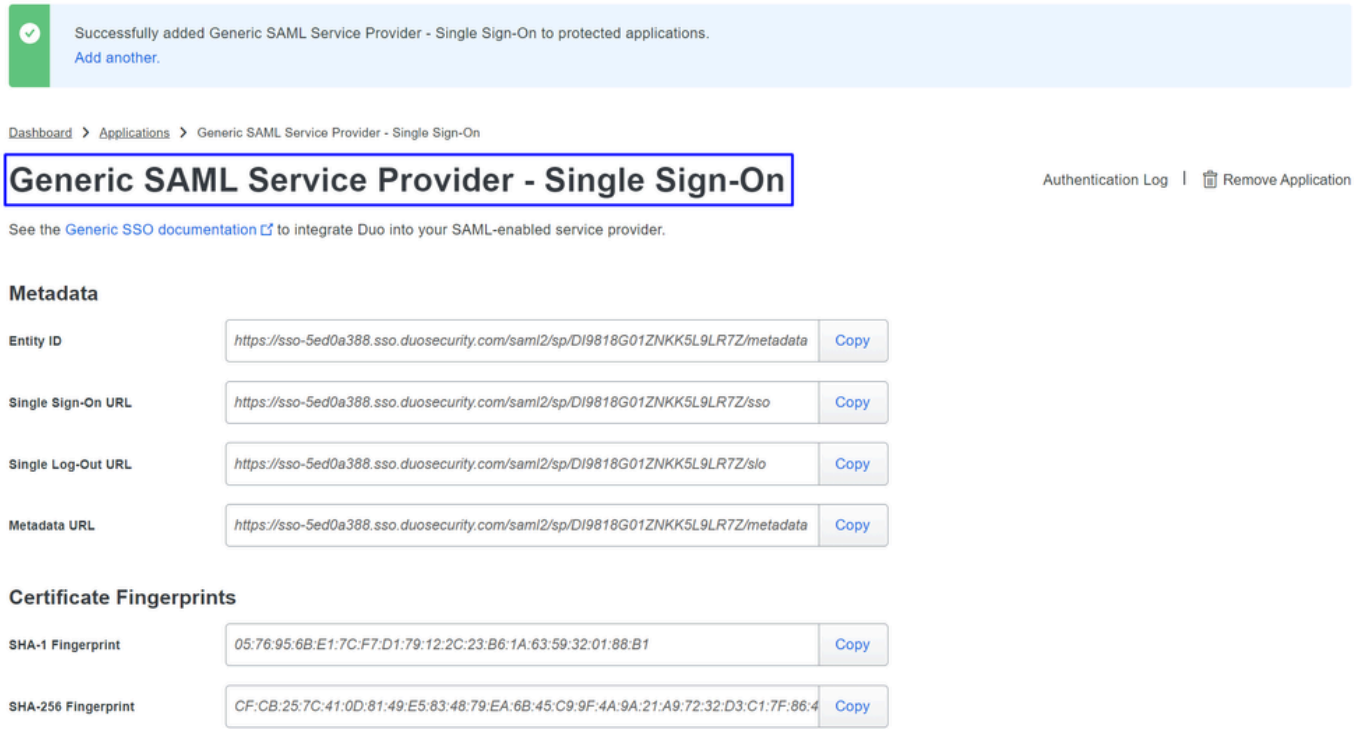
Pour configurer l'application RA-VPN, procédez comme suit :

Accédez à votre panneau d'administration Duo

- Naviguez jusqu'à **Applications > Protect an Application**
- Rechercher des **Generic SAML Service Provider**
- Cliquer Protect



L'application doit être affichée à l'écran ; mémorisez le nom de l'application pour la configuration VPN.



Dans ce cas, est **Generic SAML Service Provider.**

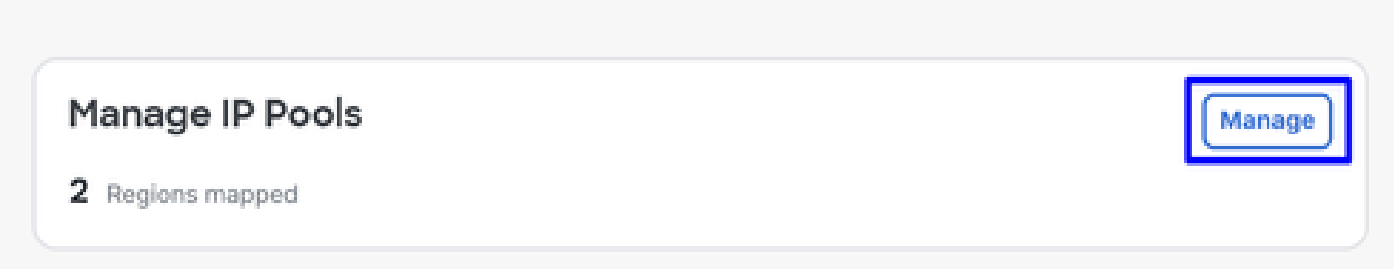
Configuration d'accès sécurisé

Configurer le groupe Radius sur les pools IP

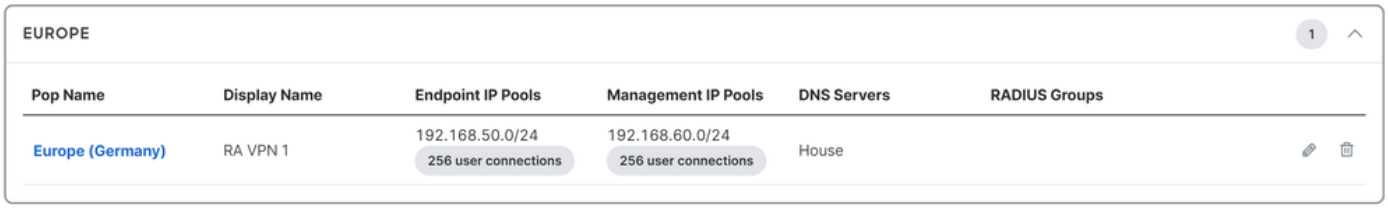
Pour configurer le profil VPN à l'aide de Radius, procédez comme suit :

Accédez à votre tableau de bord d'accès sécurisé.

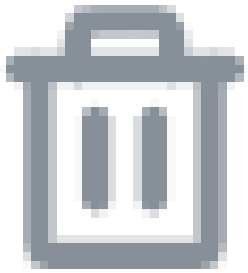
- Cliquez sur **Connect** > **Enduser Connectivity** > **Virtual Private Network**
- Sous votre configuration de pool (**Manage IP Pools**), cliquez surManage



- Sélectionnez le **IP Pool Region** et configurez le **Radius Server**



- Cliquez sur le crayon pour le modifier



- À présent, dans la liste déroulante de configuration de la section IP Pool, sous **Radius Group (Optional)**
- Cliquer Add RADIUS Group

RADIUS Groups (optional)

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

No RADIUS groups created

Add RADIUS Group

← Edit RADIUS Group

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

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

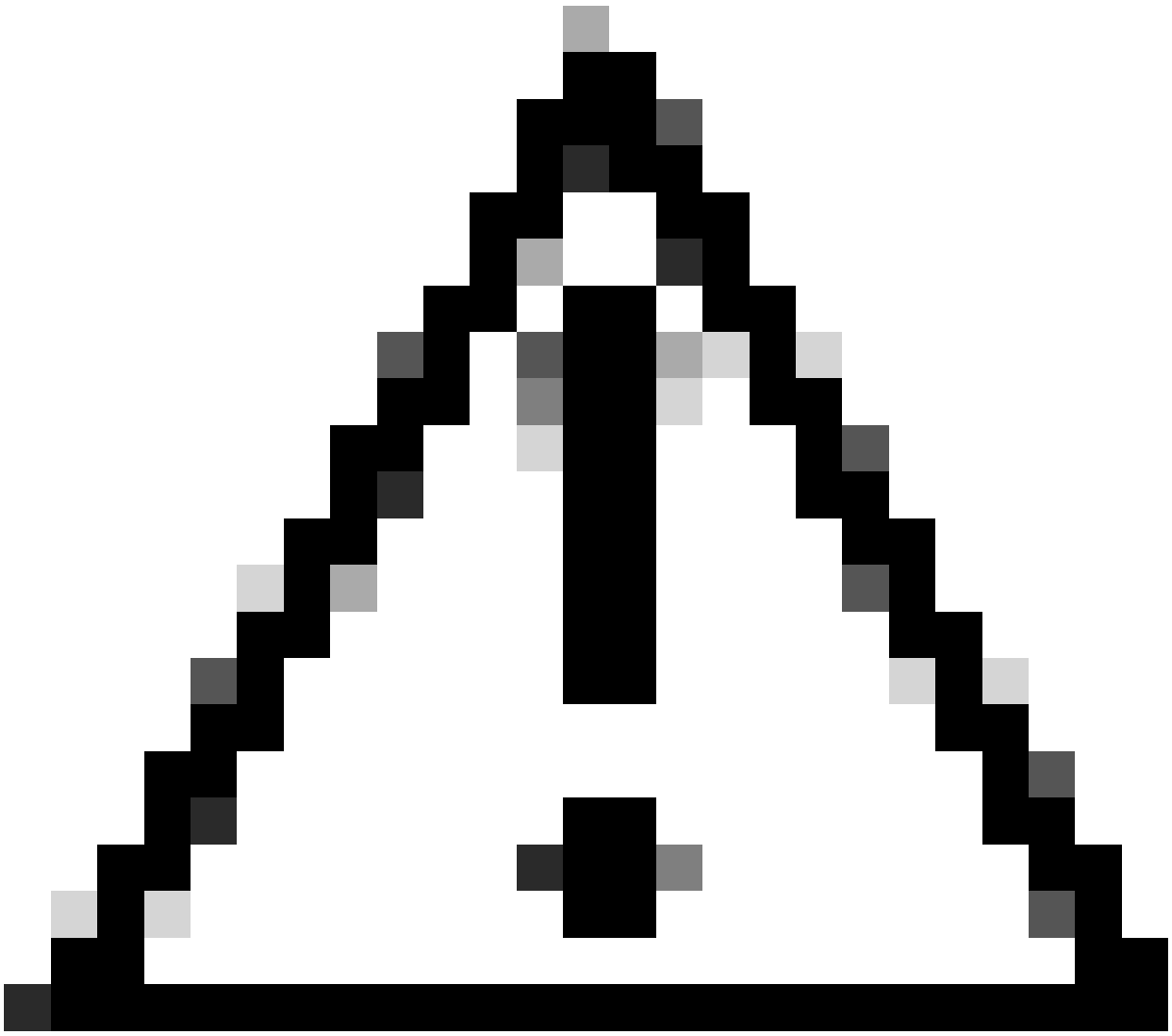
Assign servers

ISE_CSA

+ Add

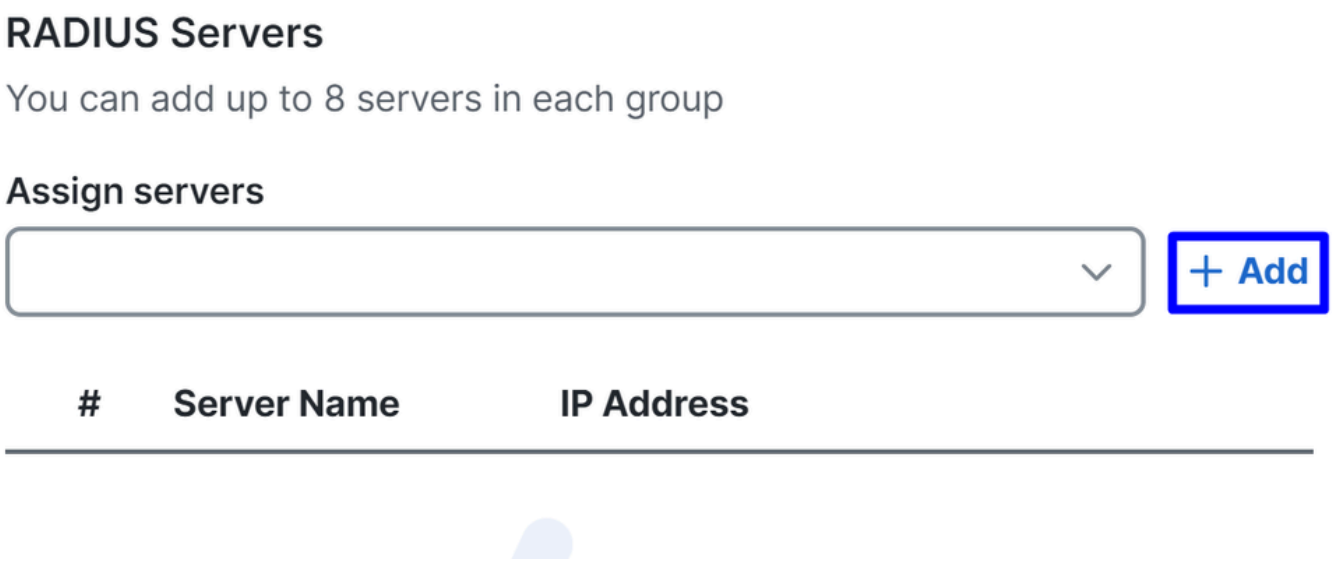
#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Authentication**: Cochez la case pour **Authentication** et sélectionnez le port, par défaut, 1812
  - Si votre authentification nécessite une case à cocher,Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)cochez-la
- **Authorization**: Cochez la case pourAuthorizationet sélectionnez le port 1812 par défaut
  - Cochez la case pour **Authorization mode Only** et pour autoriser les**Change of Authorization (CoA) mode** changements de position et d'ISE
- **Accounting**: cochez la case Autorisation et sélectionnez le port 1813 par défaut
  - Choisir **Single or Simultaneous** (En mode unique, les données de comptabilité sont envoyées à un seul serveur. En mode simultané, les données de gestion des comptes à tous les serveurs du groupe)
  - Cochez la case pour **Accounting update** activer la génération périodique de messages RADIUS Interim-accounting-update.

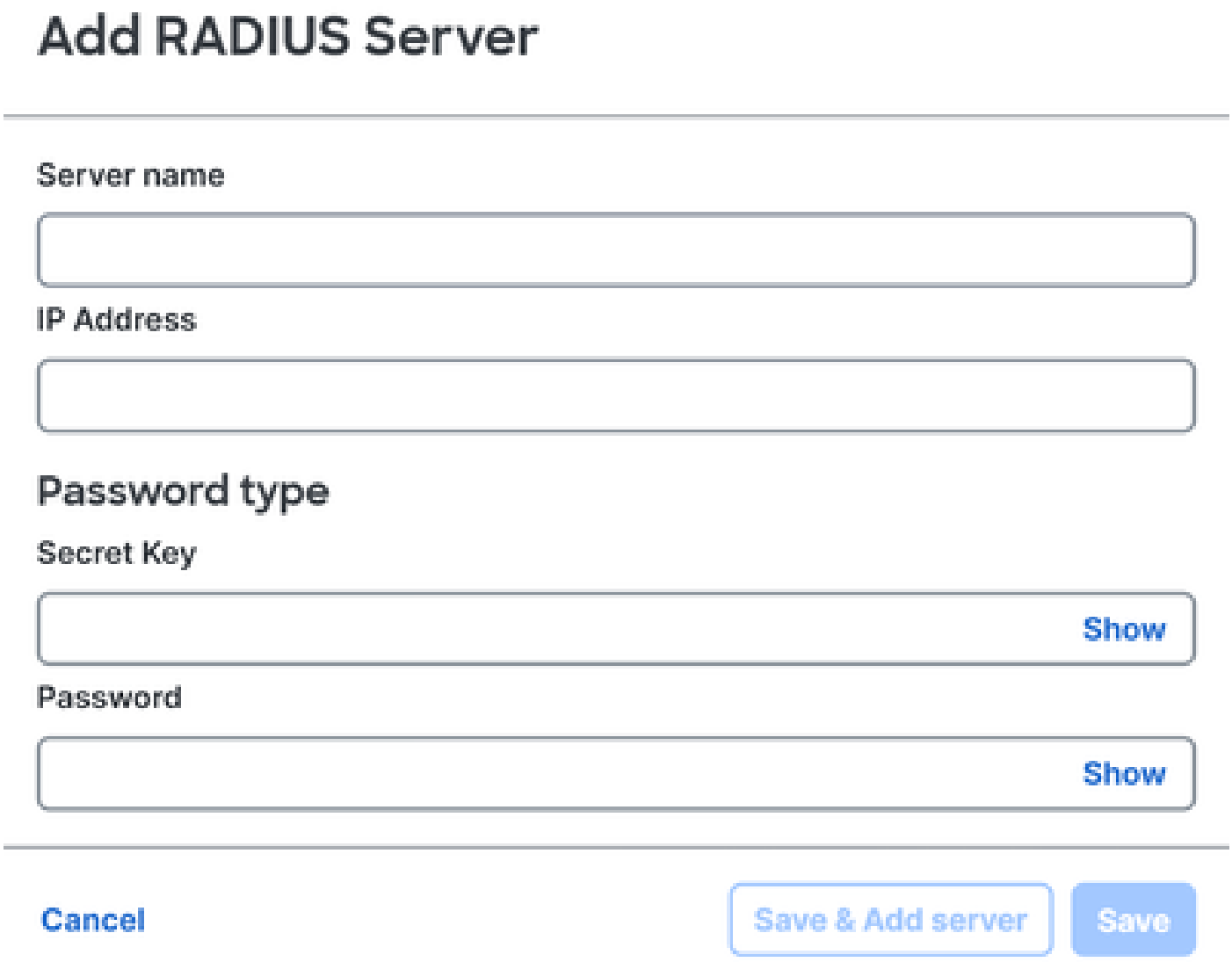


Mise en garde : Les méthodesAuthenticationet **Authorization** doivent, lorsqu'elles sont sélectionnées, utiliser le même port.

- Ensuite, vous devez configurer le **RADIUS Servers** (ISE) utilisé pour l'authentification via AAA dans la section **RADIUS Servers**:
- Cliquez sur + Add

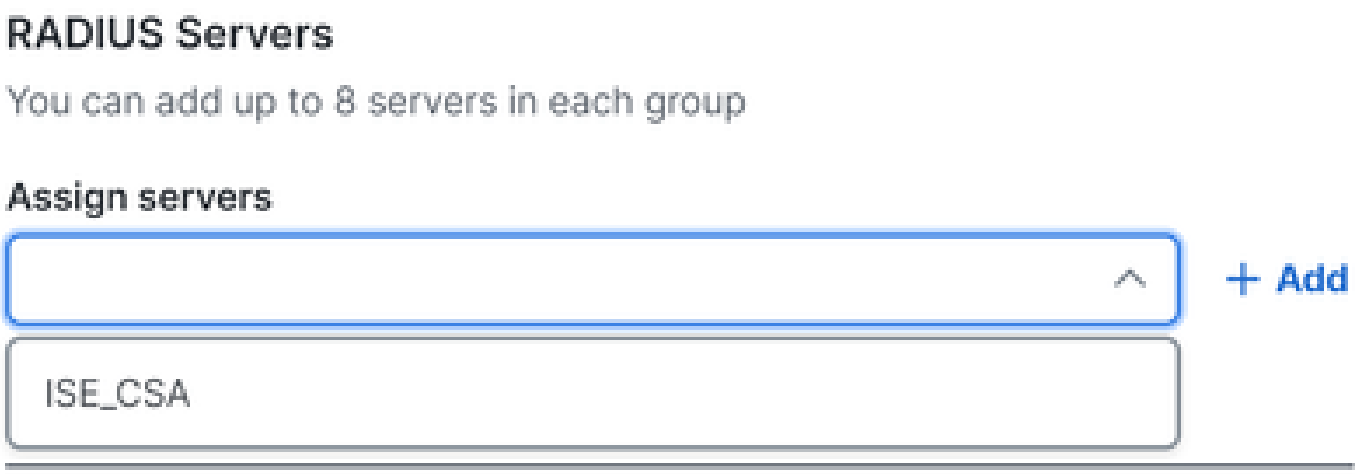


- Configurez ensuite les options suivantes :



- Server Name: Configurez un nom pour identifier votre serveur ISE.
- **IP Address**: Configurez l'adresse IP de votre périphérique Cisco ISE accessible via l'accès sécurisé
- **Secret Key**: Configurez votre clé secrète RADIUS
- **Password**: Configurez votre mot de passe Radius

- Cliquez sur **Save** et attribuez votre serveur Radius sous l'Assign Serveroption et sélectionnez votre serveur ISE :



- Cliquez **Save** à nouveau pour enregistrer toute la configuration effectuée

← 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

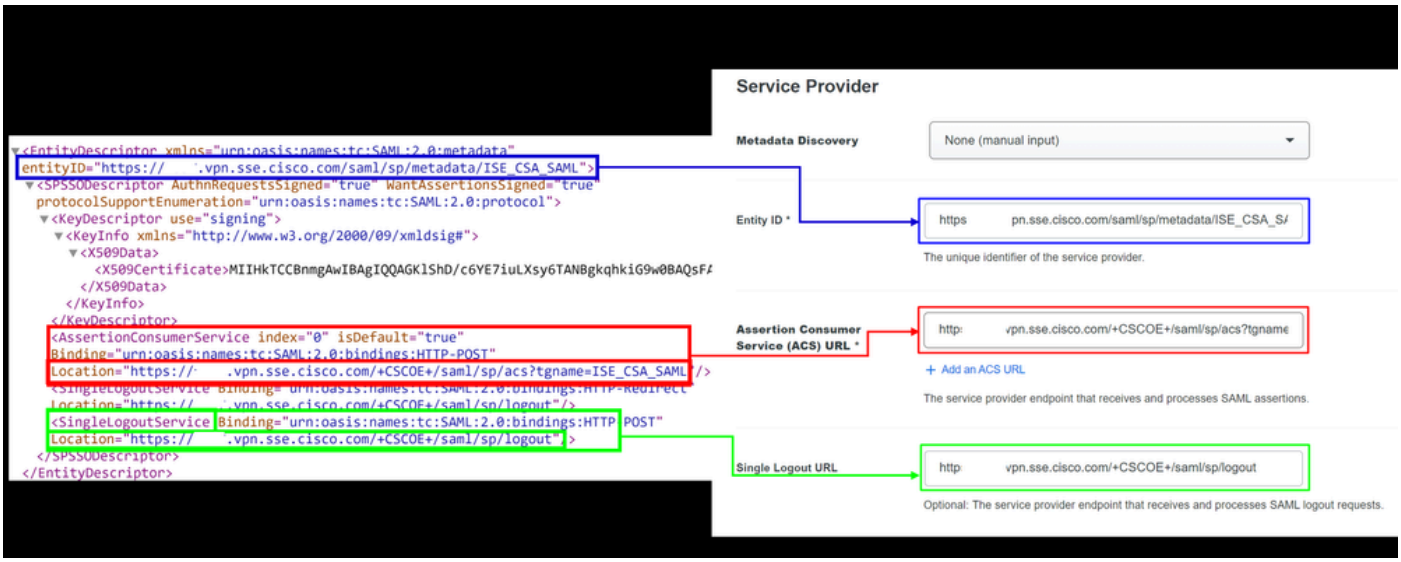
Assign servers

ISE_CSA

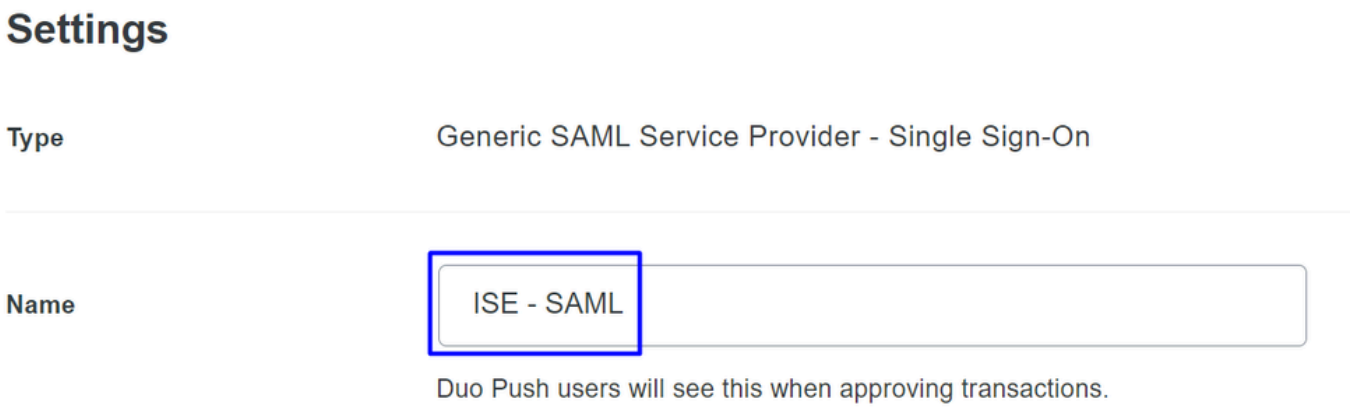
+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

    - **Protocols**: Choisir **SAML**
- Cliquer Download Service Provider XML file
- Remplacez les informations dans l'application configurée dans l'étape, Duo Configuration



- Une fois ces informations configurées, remplacez le nom du duo par un nom lié à l'intégration que vous effectuez



- Cliquez **Save** sur votre application sur Duo.
- Une fois que vous avez cliqué sur Enregistrer, vous devez télécharger le **SAML Metadata** en cliquant sur le bouton **Download XML**

ISE - SAML

See the Generic SSO documentation to integrate Duo into your SAML-enabled service provider.

Metadata

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

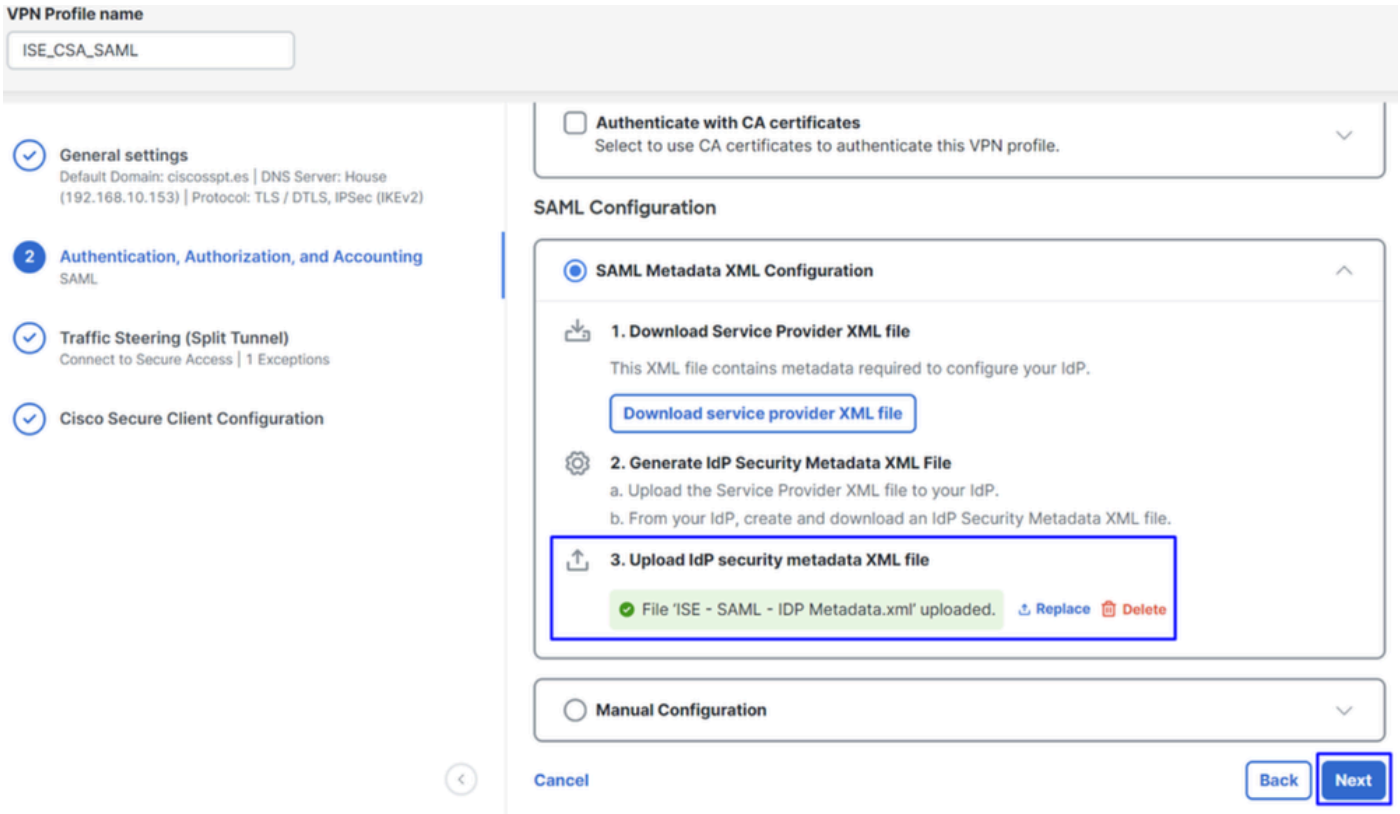
Certificate Fingerprints

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

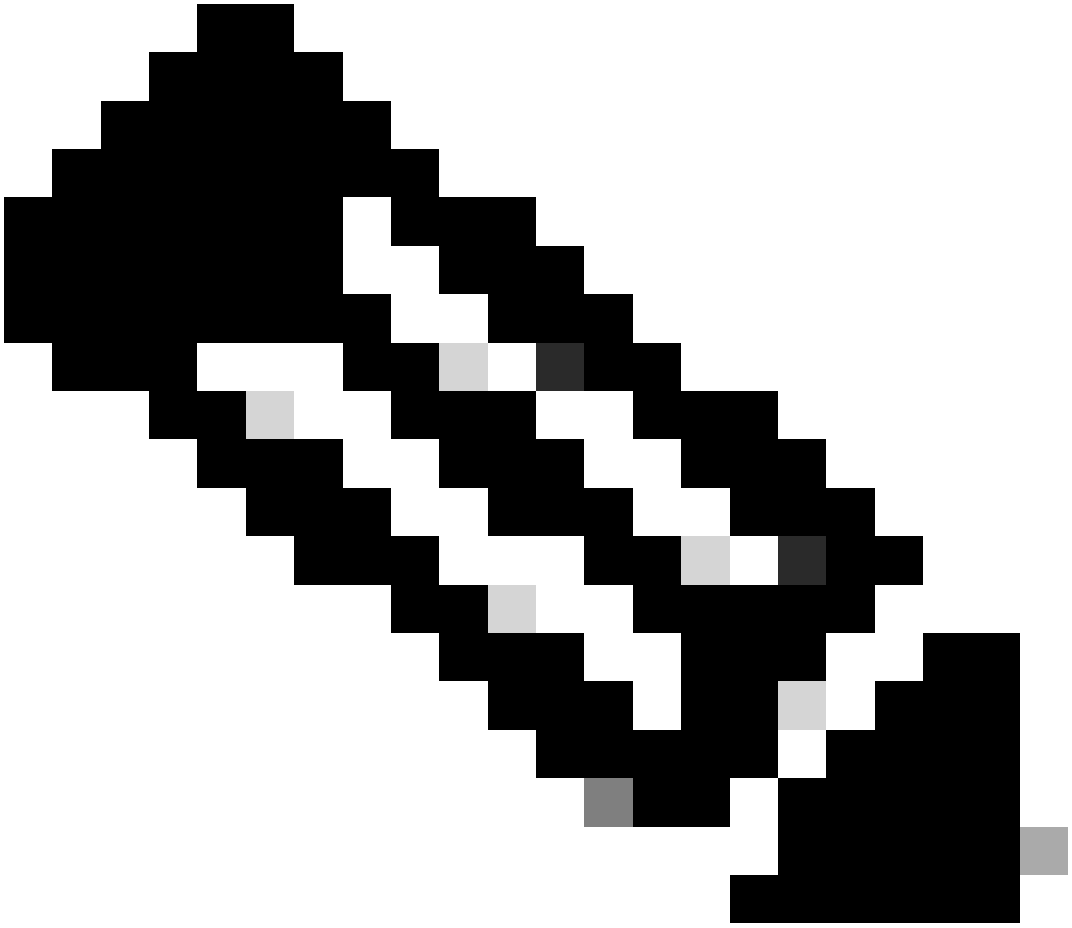
Downloads

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

- Téléchargez le **SAML Metadata** sur Secure Access sous l'option, **3. Upload IdP security metadata XML file** puis cliquez sur **Next**

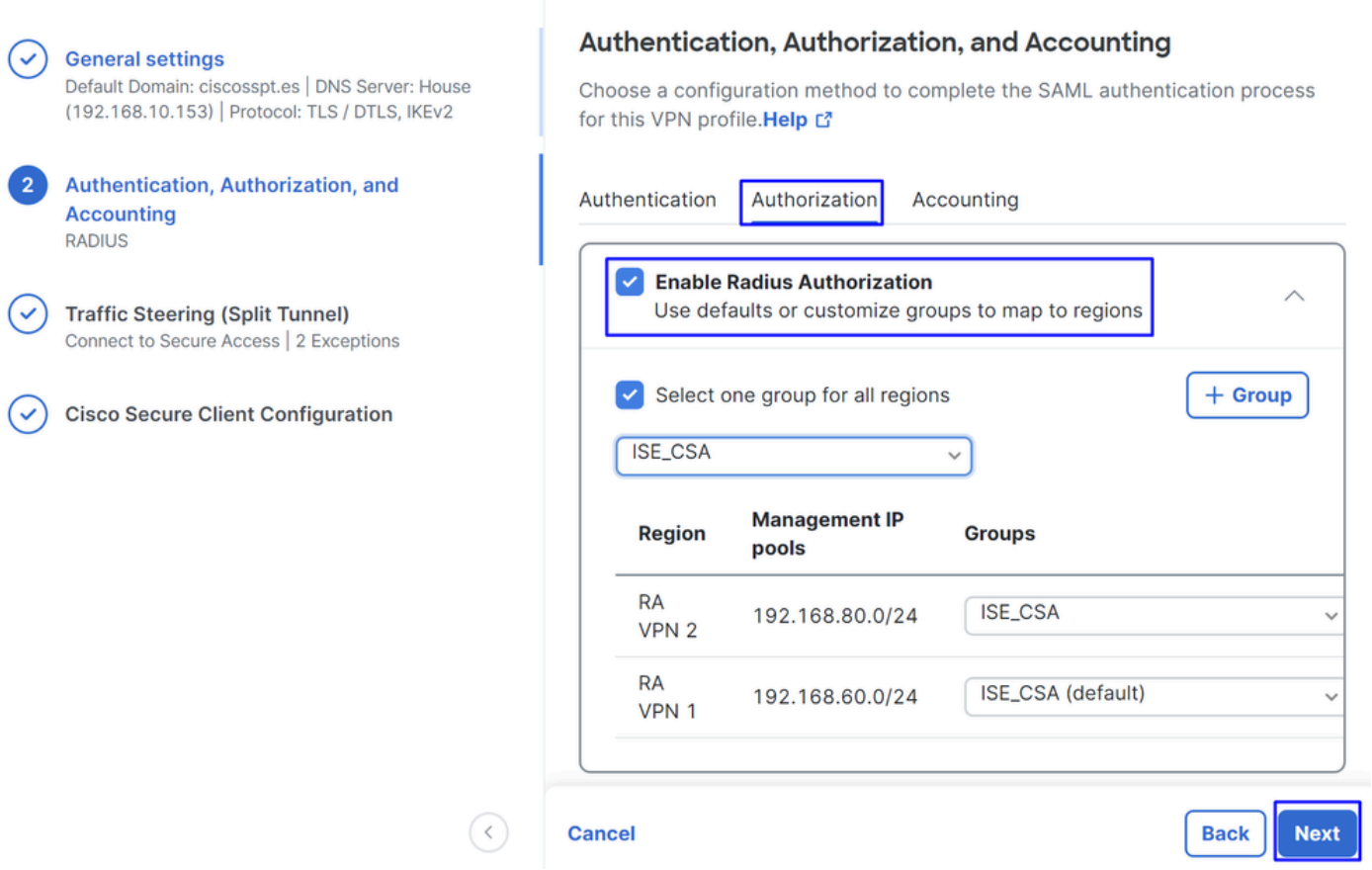


Passez à l'autorisation.



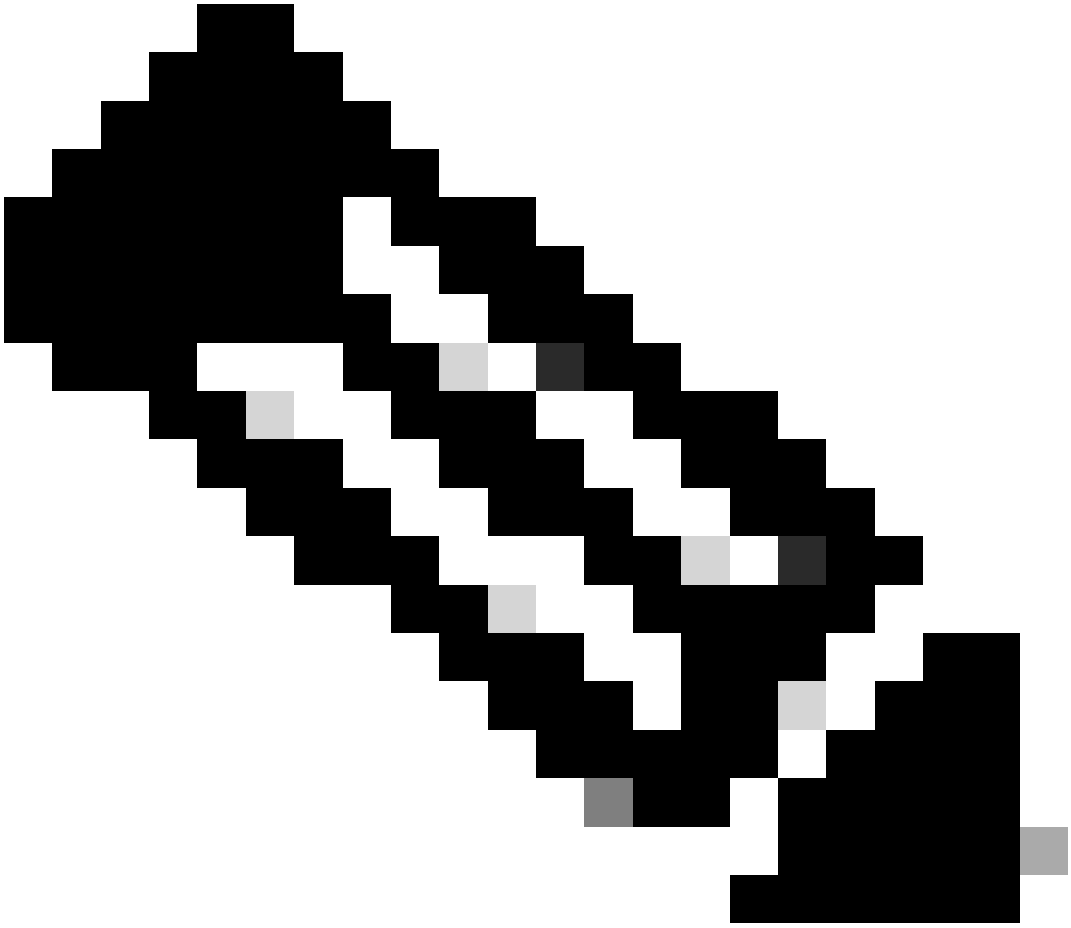
Remarque : Une fois que vous avez configuré l'authentification avec SAML, vous l'autorisez via ISE, ce qui signifie que le paquet radius envoyé par Secure Access contiendra uniquement le nom d'utilisateur. Le champ de mot de passe n'existe pas ici.

Autorisation



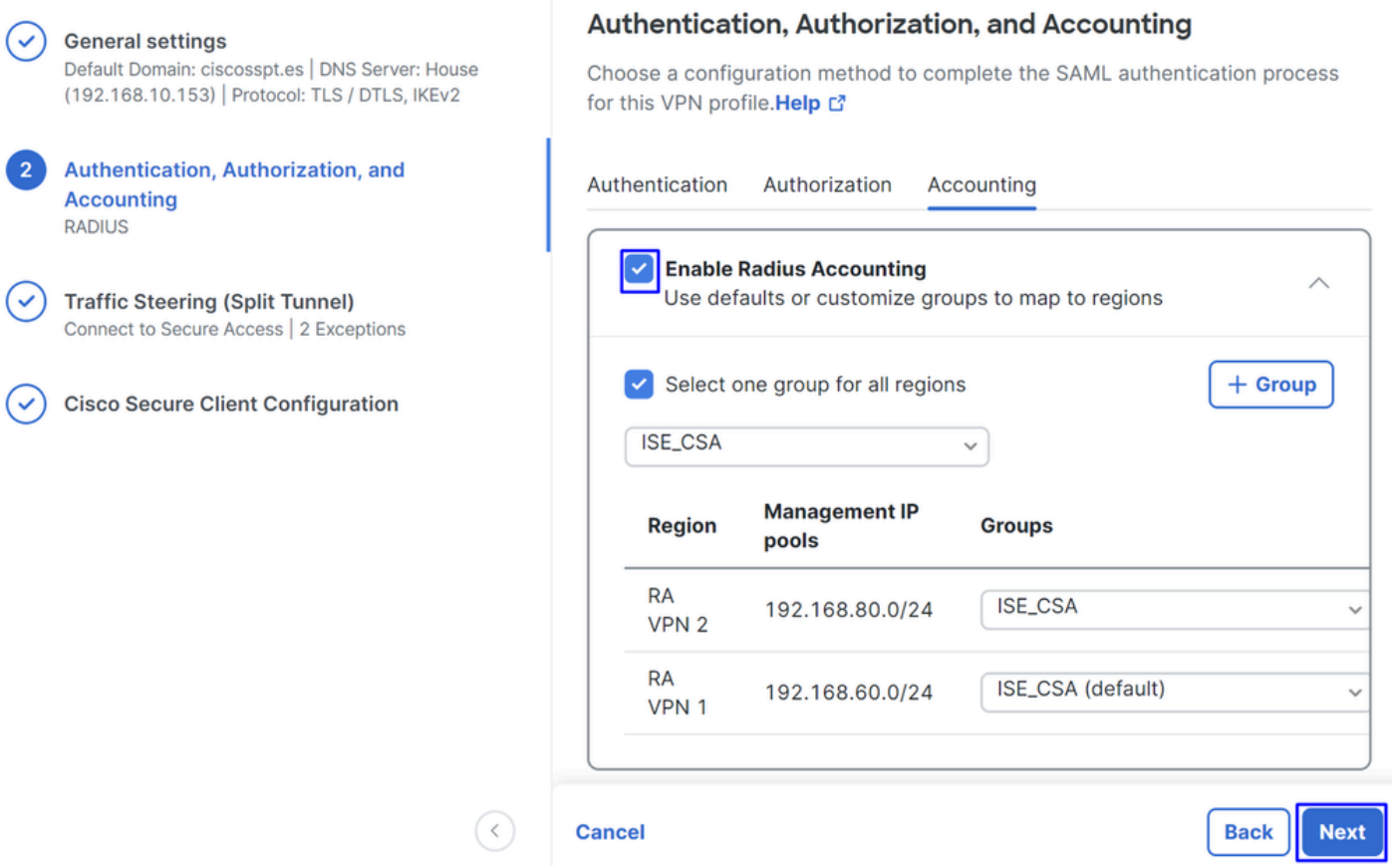
- **Authorization**
  - **Enable Radius Authorization**: Cochez la case pour activer le rayon Autorisation
  - Sélectionnez un groupe pour toutes les régions : Cochez cette case pour utiliser un serveur RADIUS spécifique pour tous les pools d'accès à distance - réseau privé virtuel (RA-VPN) ou définissez-le séparément pour chaque pool
- Cliquer **Next**

Après avoir configuré l'ensemble de la **Authorization** pièce, passez à l' **Accounting**.



Remarque : Si vous n'activez pas **Radio Authorization**, la posture ne peut pas fonctionner.

Gestion de comptes

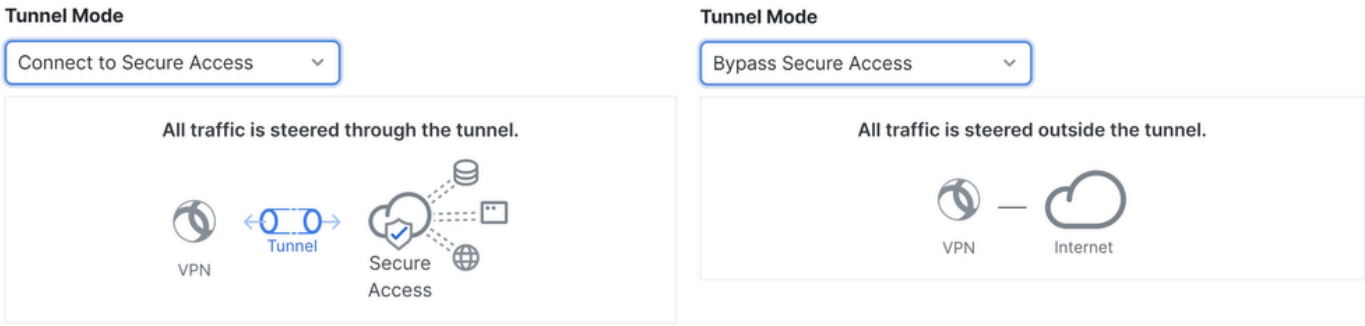


- **Accounting**
  - **Map Authorization groups to regions**: Choisissez les régions et choisissez votre **Radius Groups**
- Cliquer **Next**

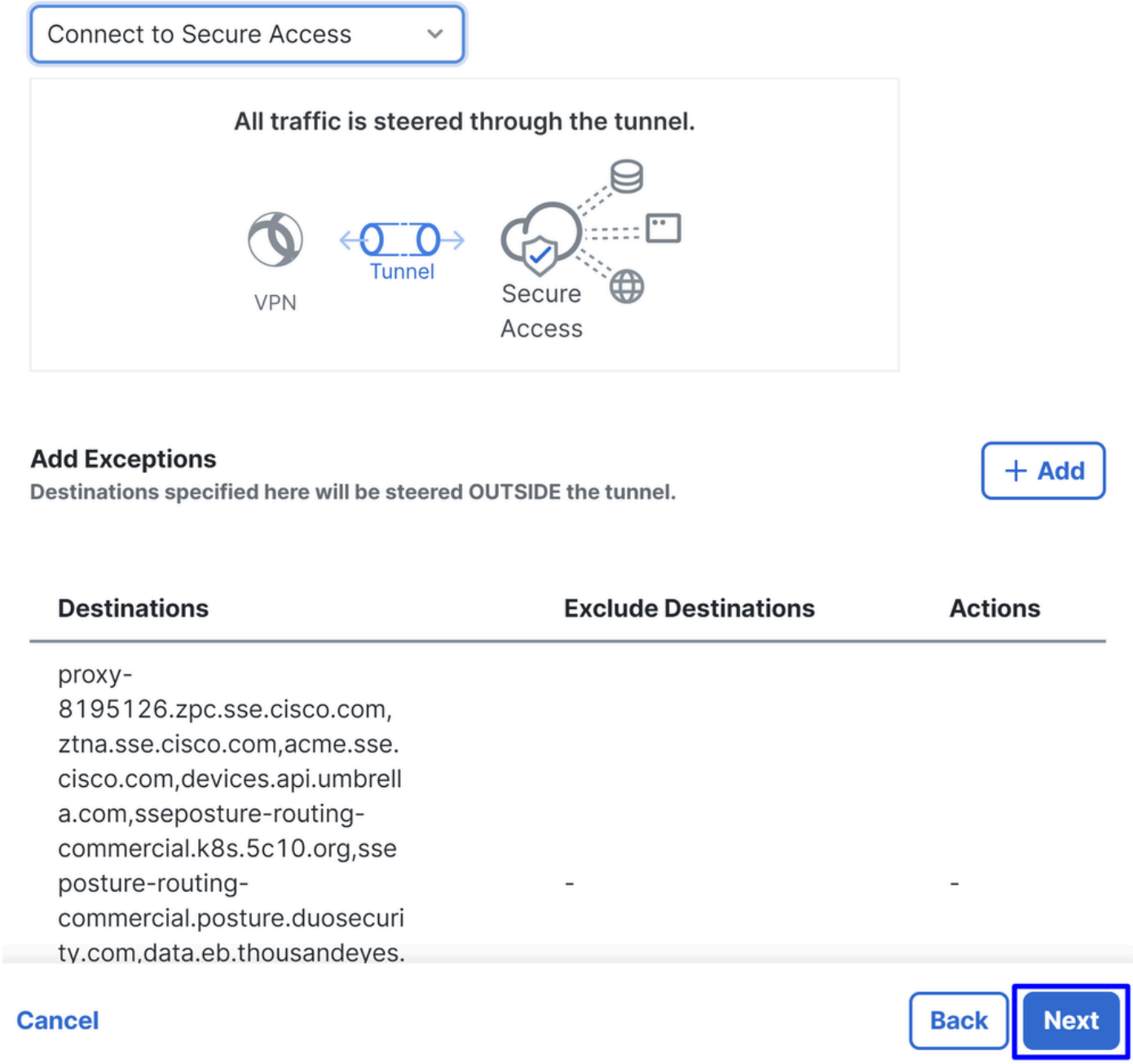
After you have done configured the Authentication, Authorization and Accounting please continue withTraffic Steering.

Orientation Du Trafic

Sous l'orientation du trafic, vous devez configurer le type de communication via l'accès sécurisé.



- Si vous le souhaitez **Connect to Secure Access**, tous vos trafics Internet passent par **Secure Access**



Si vous souhaitez ajouter des exclusions pour les domaines Internet ou les adresses IP, cliquez sur le **+ Add** bouton, puis cliquez sur **Next**.

- Si vous le souhaitez**Bypass Secure Access**, tout votre trafic Internet passe par votre fournisseur d'accès Internet, et non parSecure Access(Pas de protection Internet)

Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.

Add Exceptions

Destinations specified here will be steered INSIDE the tunnel.

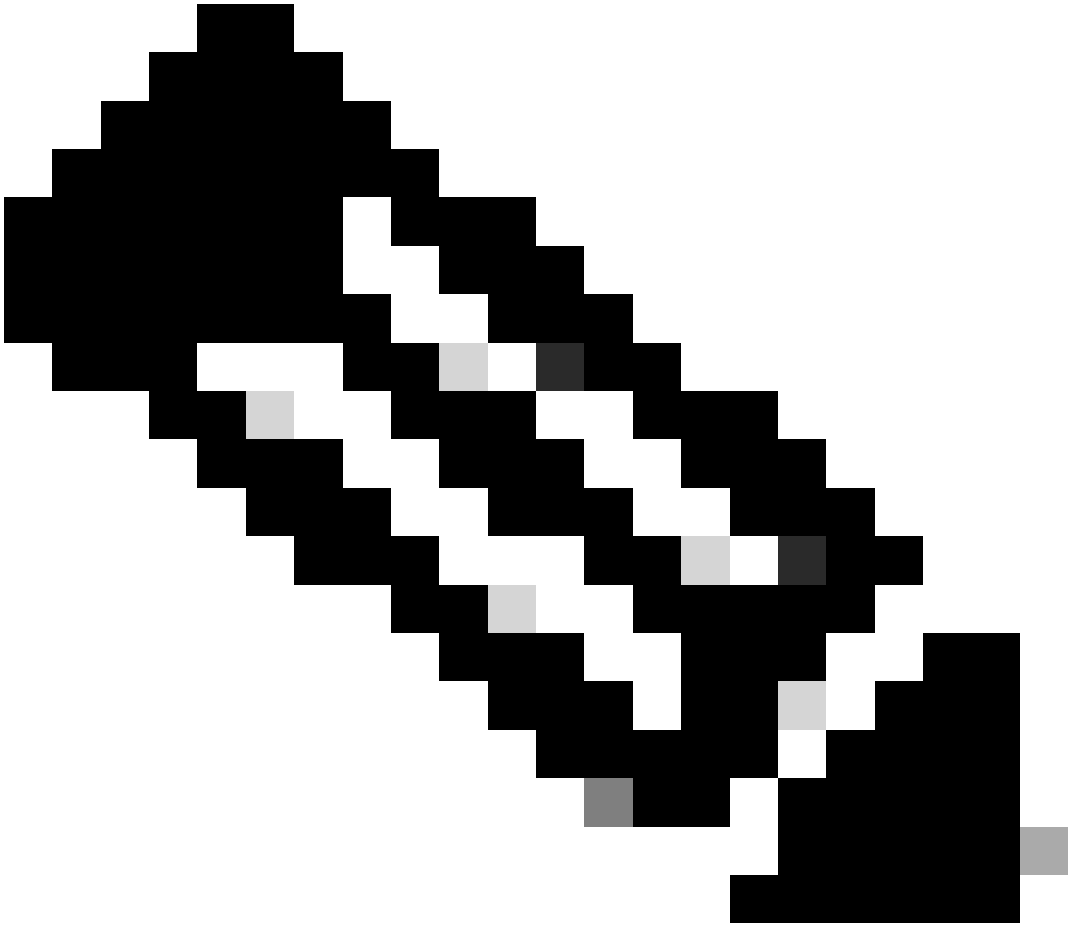
+ Add

Destinations	Exclude Destinations	Actions

No matches found

Cancel

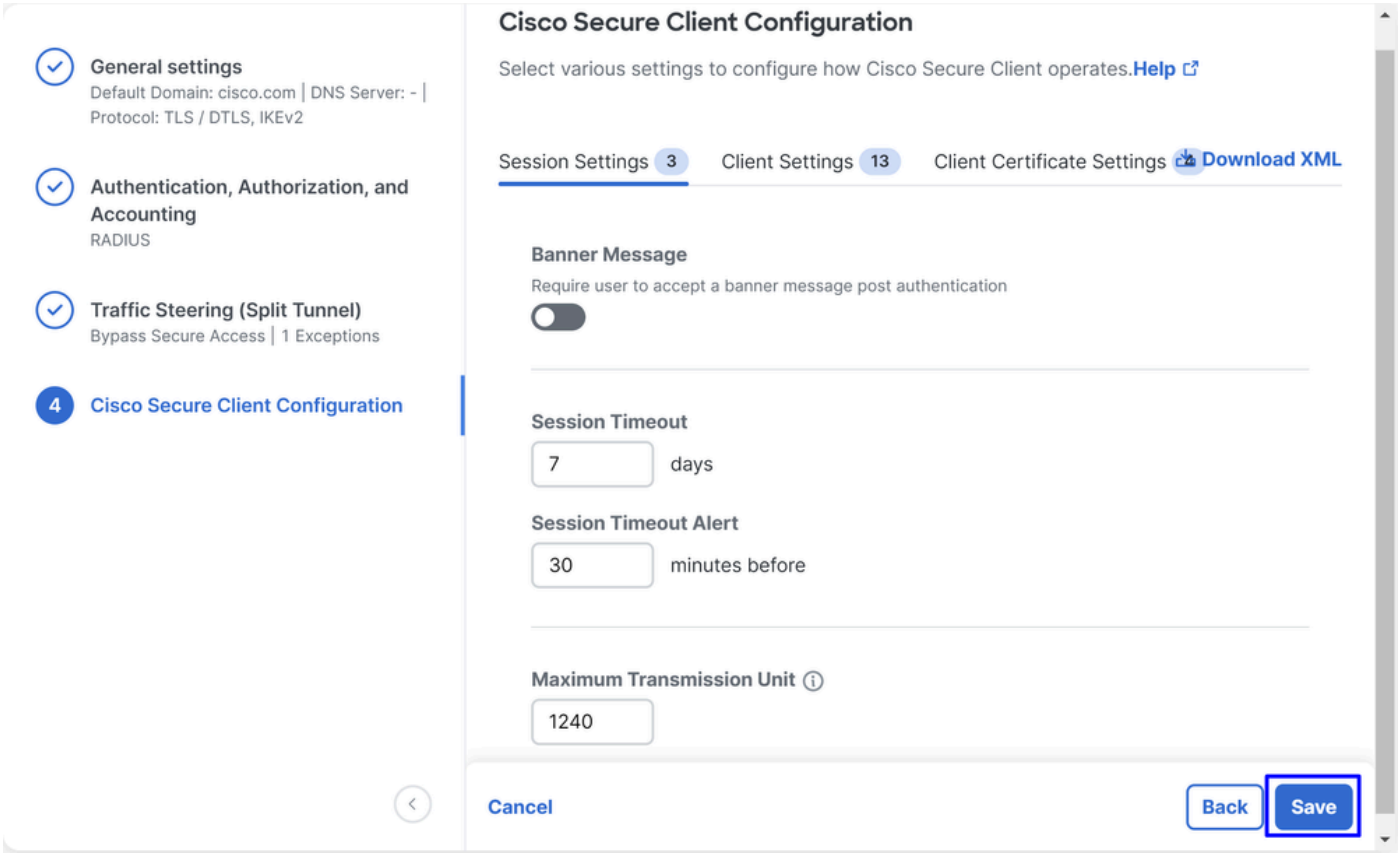
Back Next



Remarque : Veuillez ajouter **enroll.cisco.com** pour la position ISE lorsque vous choisissez **Bypass Secure Access**.

Au cours de cette étape, vous sélectionnez toutes les ressources réseau privées auxquelles vous souhaitez accéder via le VPN. Pour ce faire, cliquez sur **+ Add**, puis cliquez sur **Next** lorsque vous avez ajouté toutes les ressources.

Configuration du client sécurisé Cisco



Dans cette étape, vous pouvez tout conserver par défaut et cliquer sur **Save**, mais si vous souhaitez personnaliser davantage votre configuration, consultez le Guide de l'administrateur du client sécurisé Cisco.

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

Configurations ISE

Configurer la liste des périphériques réseau

Pour configurer l'authentification via Cisco ISE, vous devez configurer les périphériques autorisés qui peuvent émettre des requêtes vers votre Cisco ISE :

- Naviguez jusqu'à **Administration > Network Devices**
- Cliquez sur **+ 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

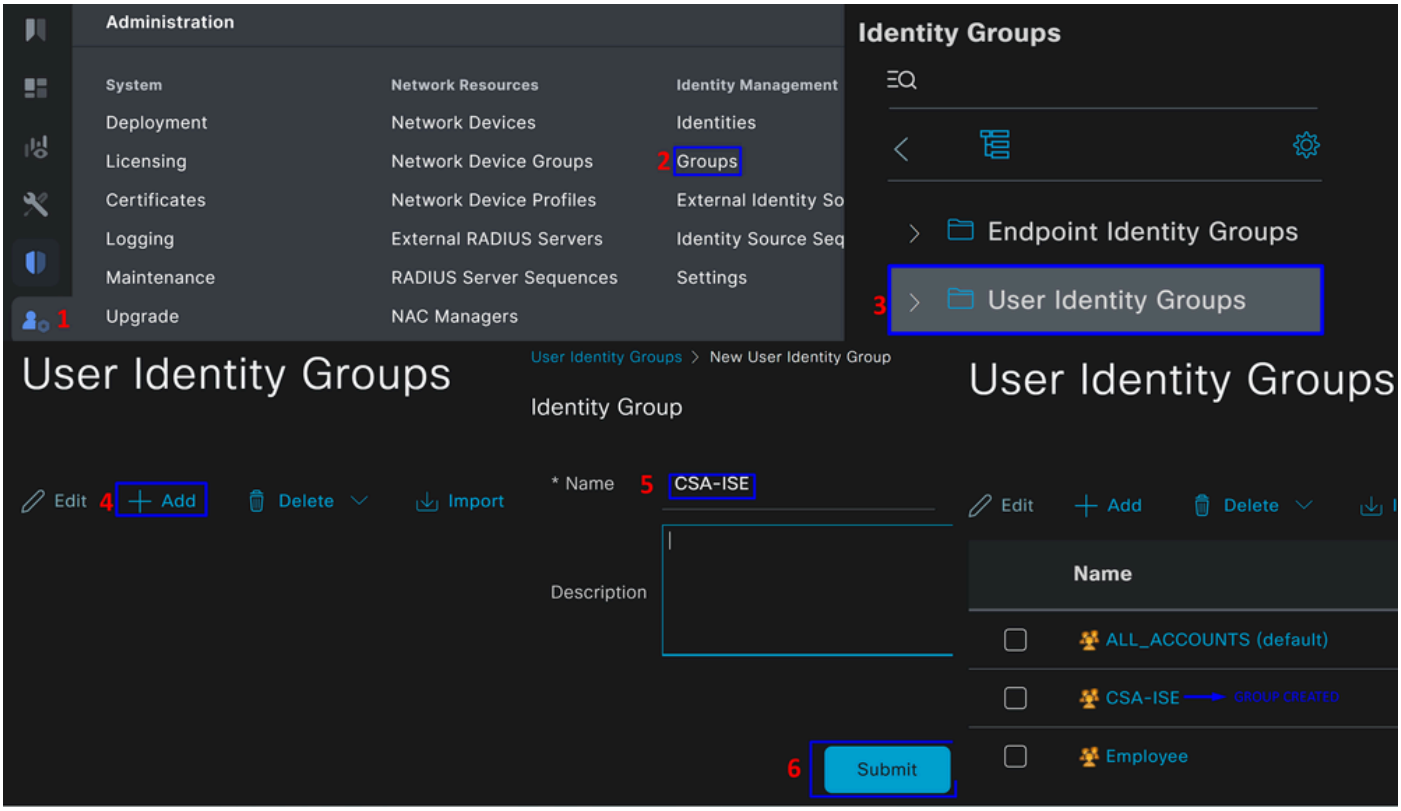
- **Name**: Utiliser un nom pour identifier l'accès sécurisé
- **IP Address**: Configurez le nomManagement Interfacede l'étape, IP Pool Region
- **Device Profile**: Choisir Cisco
  - **Radius Authentication Settings**
    - Shared Secret: Configurez le même secret partagé configuré à l'étape, Clé secrète
    - **CoA Port**: Laissez-le par défaut ; 1700 est également utilisé dans Secure Access

Après ce clic **Save**, pour vérifier si l'intégration fonctionne correctement, créez un utilisateur local pour la vérification de l'intégration.

Configurer un groupe

Pour configurer un groupe à utiliser avec des utilisateurs locaux, procédez comme suit :

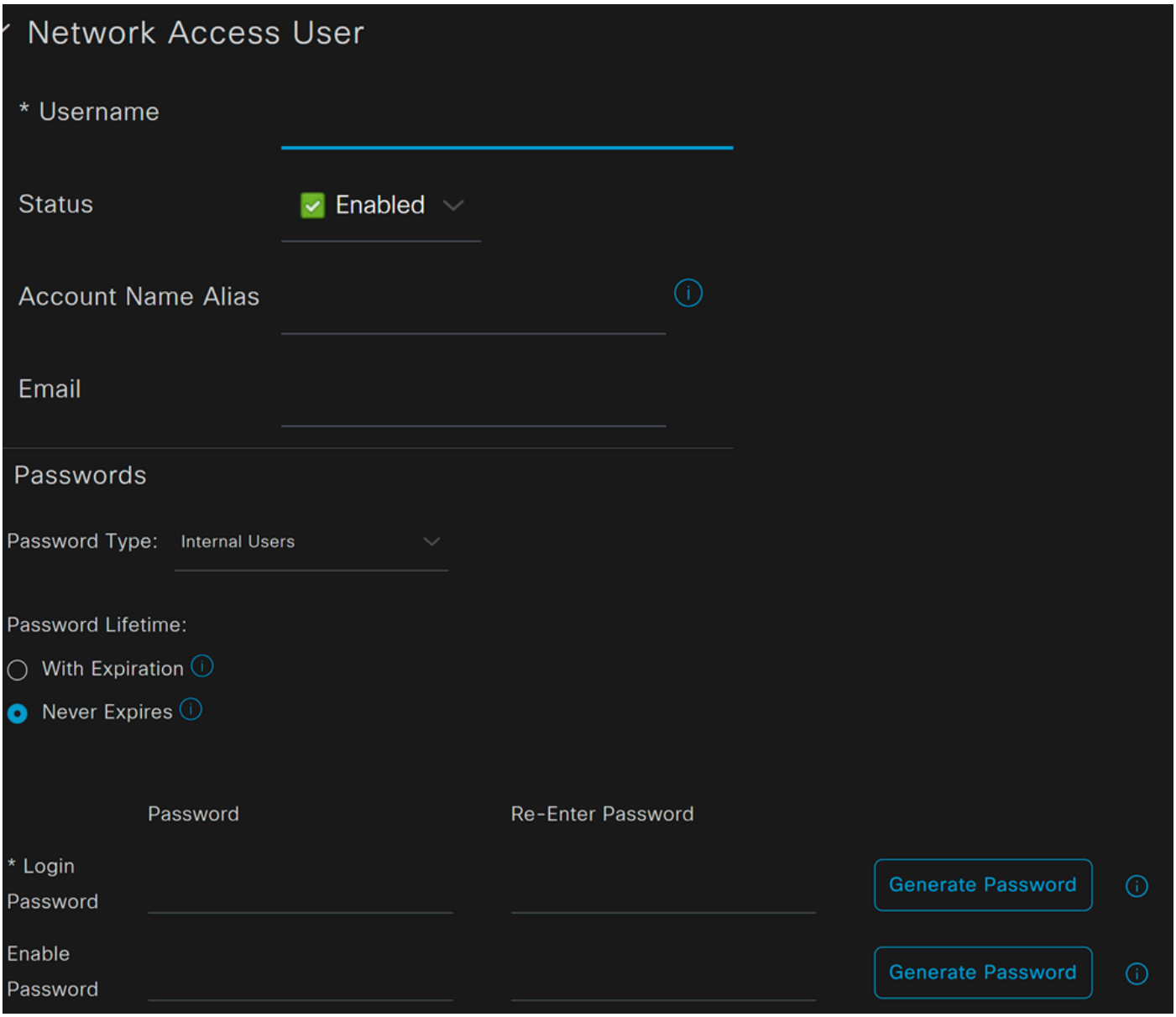
- Cliquez dans **Administration** > **Groups**
- Cliquer **User Identity Groups**
- Cliquer + Add
- Créez unNamepour le groupe et cliquez sur **Submit**

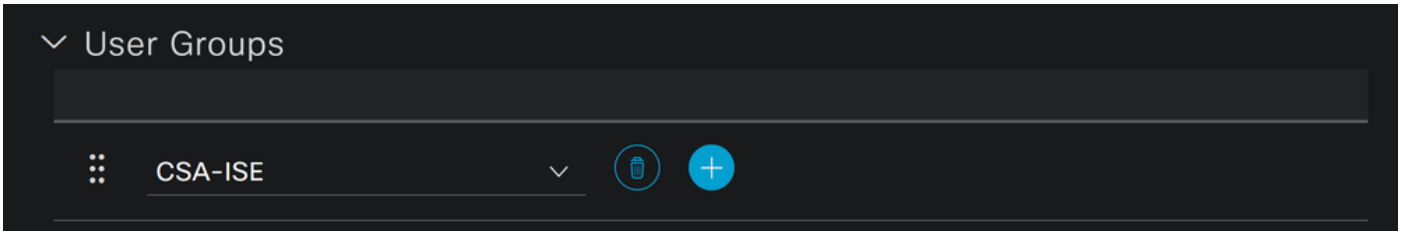


Configurer l'utilisateur local

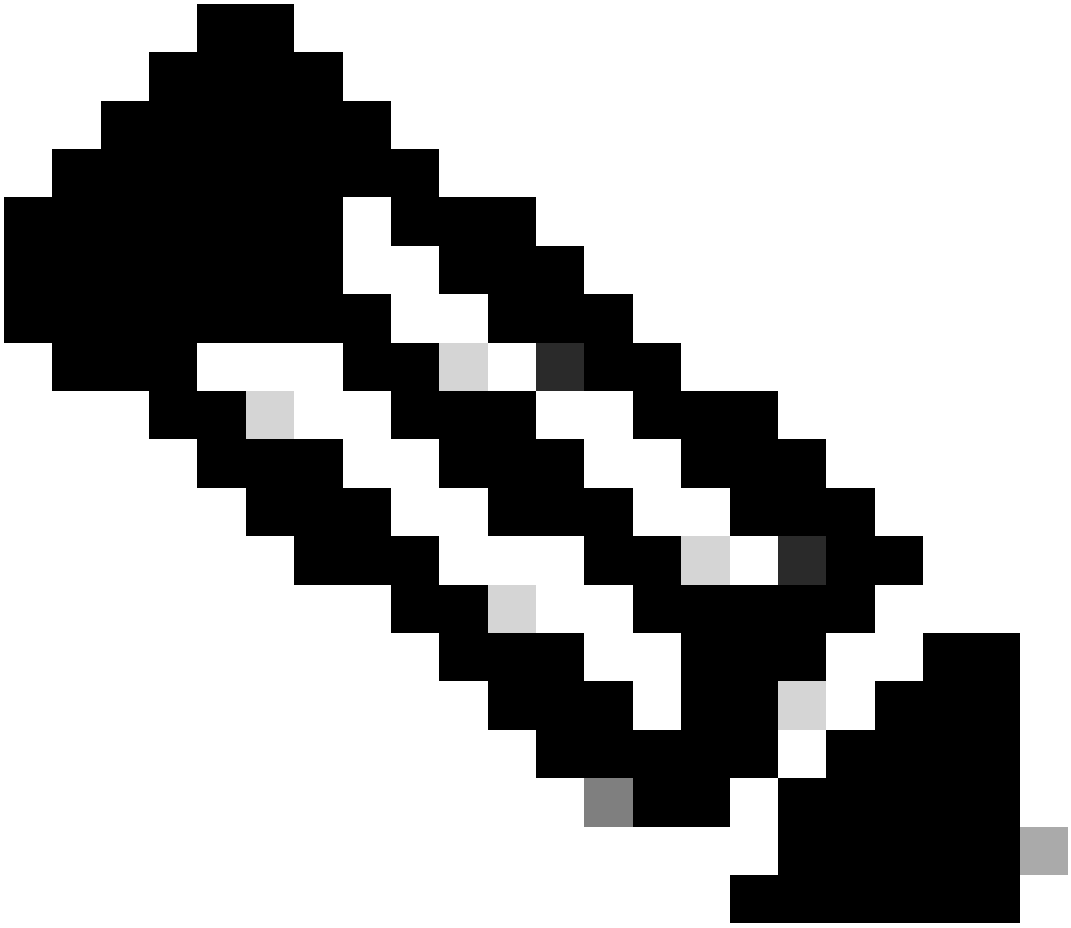
Pour configurer un utilisateur local afin de vérifier votre intégration :

- Naviguez jusqu'à **Administration** > **Identities**
- Cliquez sur **Add** +





- **Username**: Configurez le nom d'utilisateur avec un approvisionnement UPN connu dans Secure Access ; cela est basé sur l'étape, Prérequis
- **Status**: Actif
- **Password Lifetime**: Vous pouvez le configurer **With Expiration** ouNever Expires, selon vos besoins
- **Login Password**: Créer un mot de passe pour l'utilisateur
- **User Groups**: Sélectionnez le groupe créé à l'étape Configurer un groupe



Remarque : L'authentification basée sur UPN est configurée pour changer dans les prochaines versions de Secure Access.

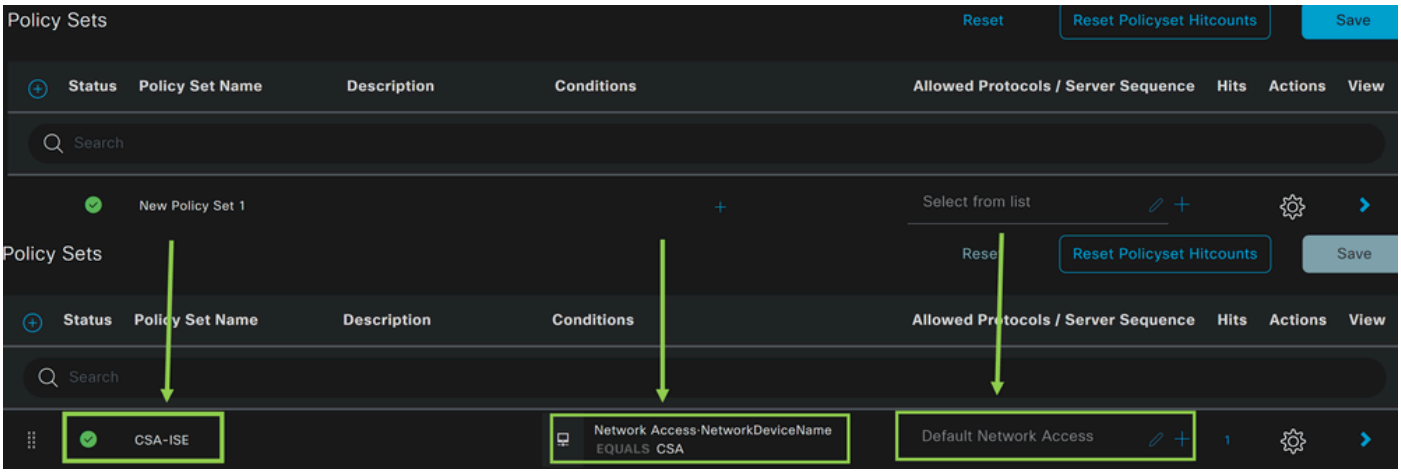
Après cela, vous pouvez **Save** modifier la configuration et poursuivre l'étape, **Configure Policy Set.**

Configurer le jeu de stratégies

Dans l'ensemble de stratégies, configurez l'action qu'ISE effectue pendant l'authentification et l'autorisation. Ce scénario illustre l'exemple d'utilisation de la configuration d'une stratégie simple pour fournir un accès utilisateur. Tout d'abord, ISE vérifie l'origine des authentifications RADIUS et vérifie si les identités existent dans la base de données utilisateur ISE pour fournir l'accès

Pour configurer cette stratégie, accédez à votre tableau de bord Cisco ISE :

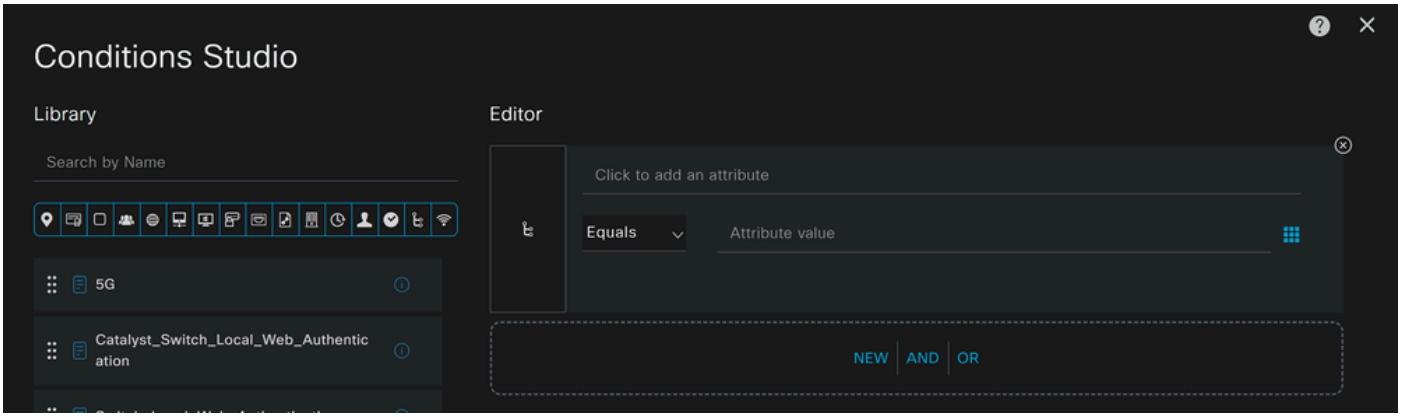
- Cliquez sur Policy > Policy Sets
- Cliquez sur + pour ajouter un nouvel ensemble de stratégies



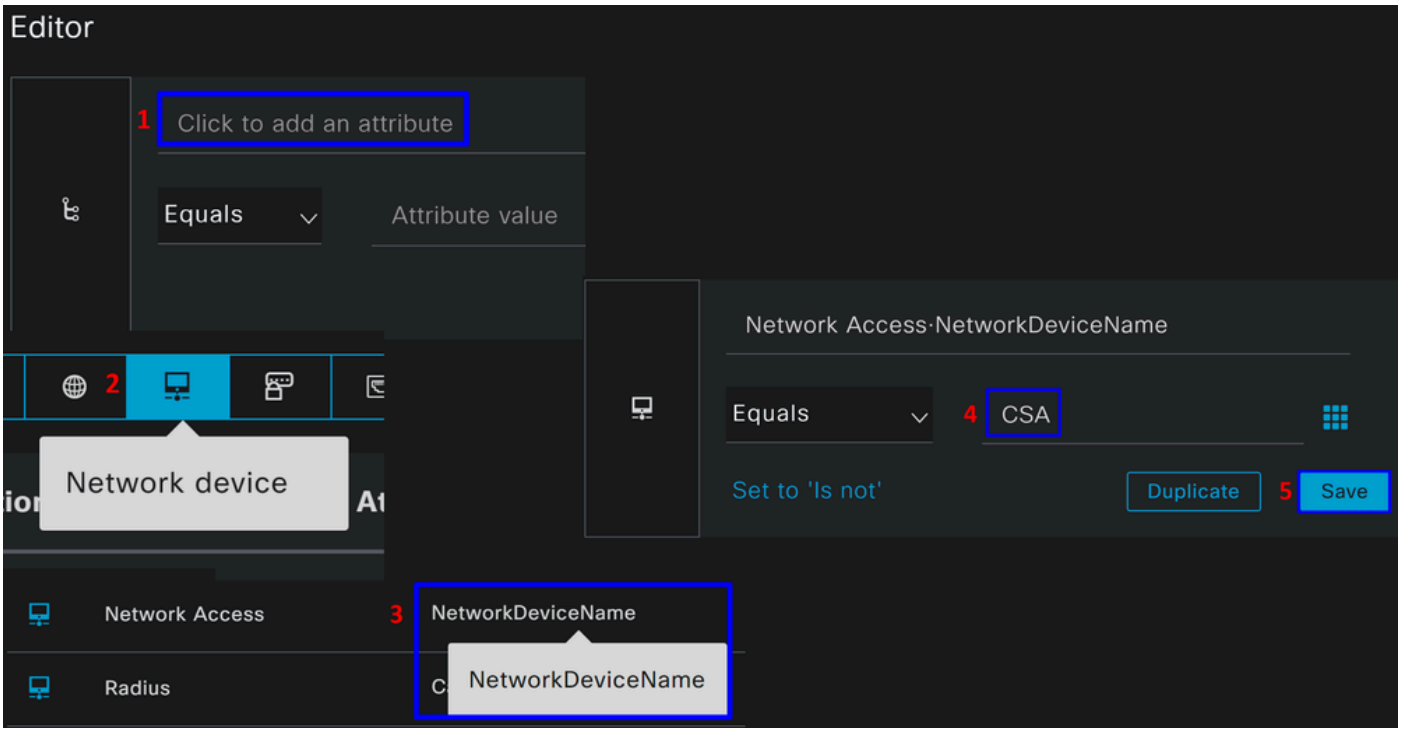
Dans ce cas, créez un nouvel ensemble de stratégies au lieu de travailler avec celui par défaut. Configurez ensuite l'authentification et l'autorisation en fonction de cet ensemble de stratégies. La stratégie configurée autorise l'accès au périphérique réseau défini à l'étape Configurer la liste des périphériques réseau pour vérifier que ces authentifications proviennent deCSA Network Device Listpuis entrent dans la stratégie en tant que **Conditions**. Et enfin, les protocoles autorisés, comme **Default Network Access**.

Pour créer le **condition** qui correspond au jeu de stratégies, procédez comme suit :

- Cliquez sur +
- Sous **Condition Studio**, les informations disponibles incluent :

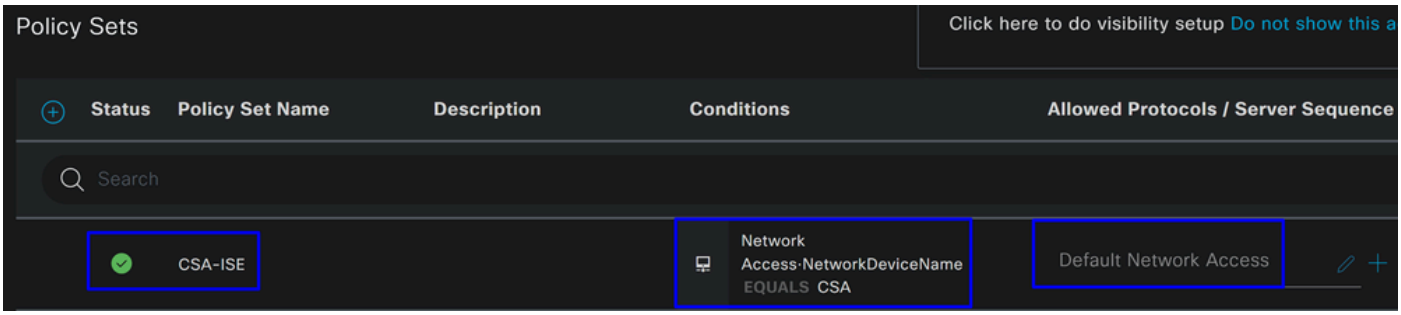


1. Pour créer les conditions, cliquez sur Click to add an attribute
2. Cliquez sur le **Network Device** bouton
3. Sous les options qui se trouvent derrière, cliquez sur **Network Access - Network Device Name** option
4. Sous l'option Est égal à, écrivez le nom du **Network Device** sous l'étape Configurer la liste des périphériques réseau
5. Cliquer **Save**

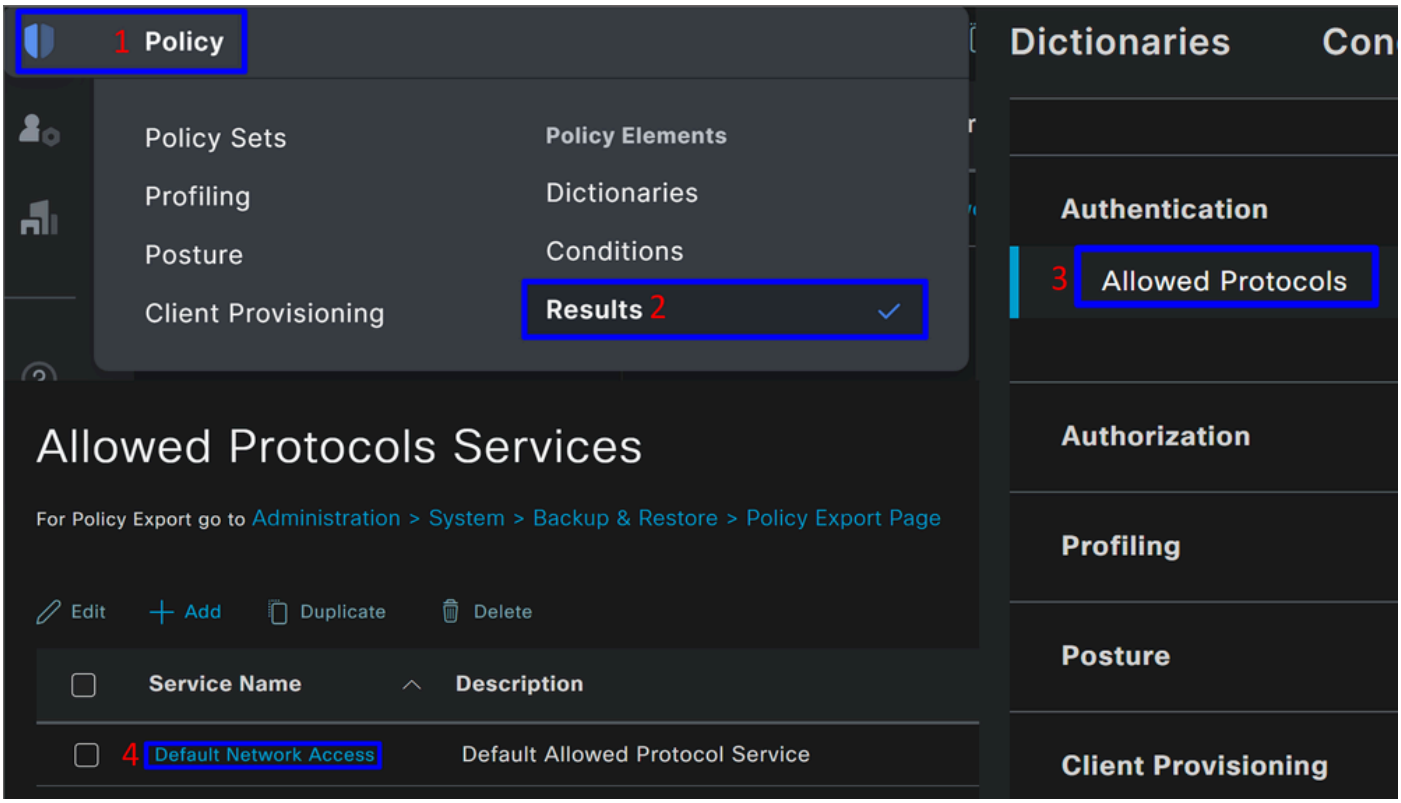


Cette stratégie approuve uniquement la demande de la sourceCSAde poursuivre l'**Authentication**installation et la configuration, **Authorization** sous l'ensemble de stratégies **CSA-ISE**, et vérifie également les protocoles autorisés en fonction de l' **Default Network Access** pour les protocoles autorisés.

Le résultat de la stratégie définie doit être :



- Pour vérifier l'**Default Network Access Protocols**autorisation, procédez comme suit :
  - Cliquez surPolicy > Results
  - Cliquez sur **Allowed Protocols**
  - Cliquez sur **Default Network Access**

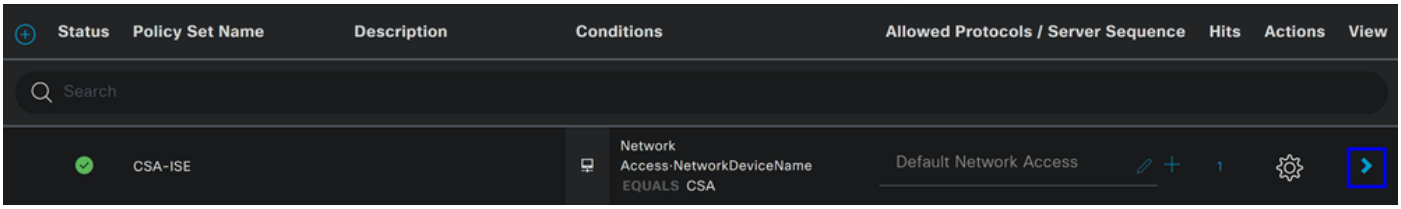


- Ensuite, vous voyez tous les protocoles autorisés sur **Default Network Access**

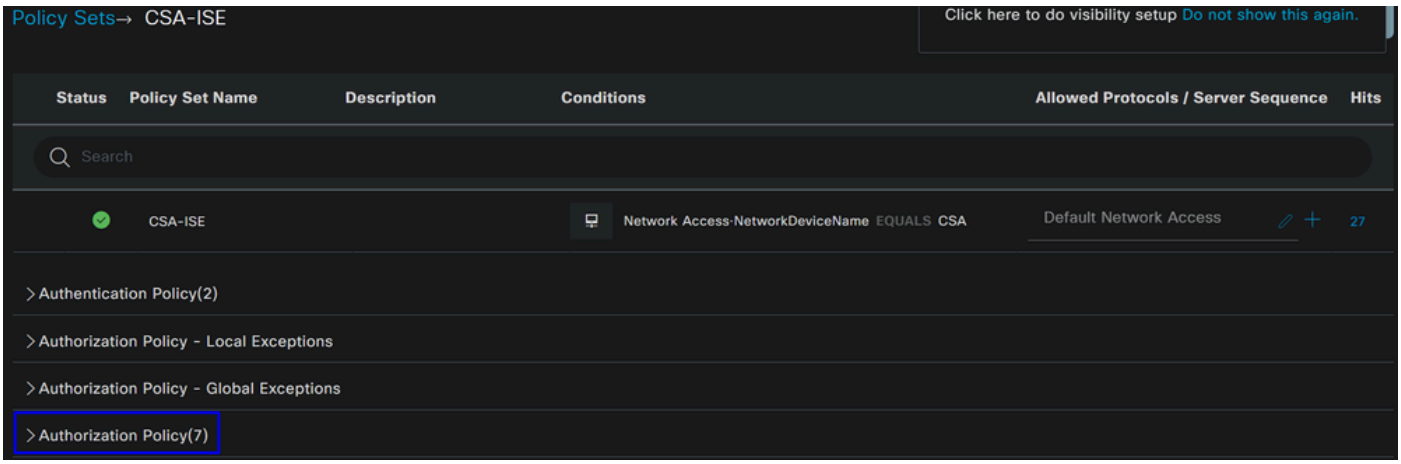
Configurer l'autorisation du jeu de stratégies

Pour créer la stratégie **Authorization** sous le **Policy Set**, procédez comme suit :

- Cliquez sur >



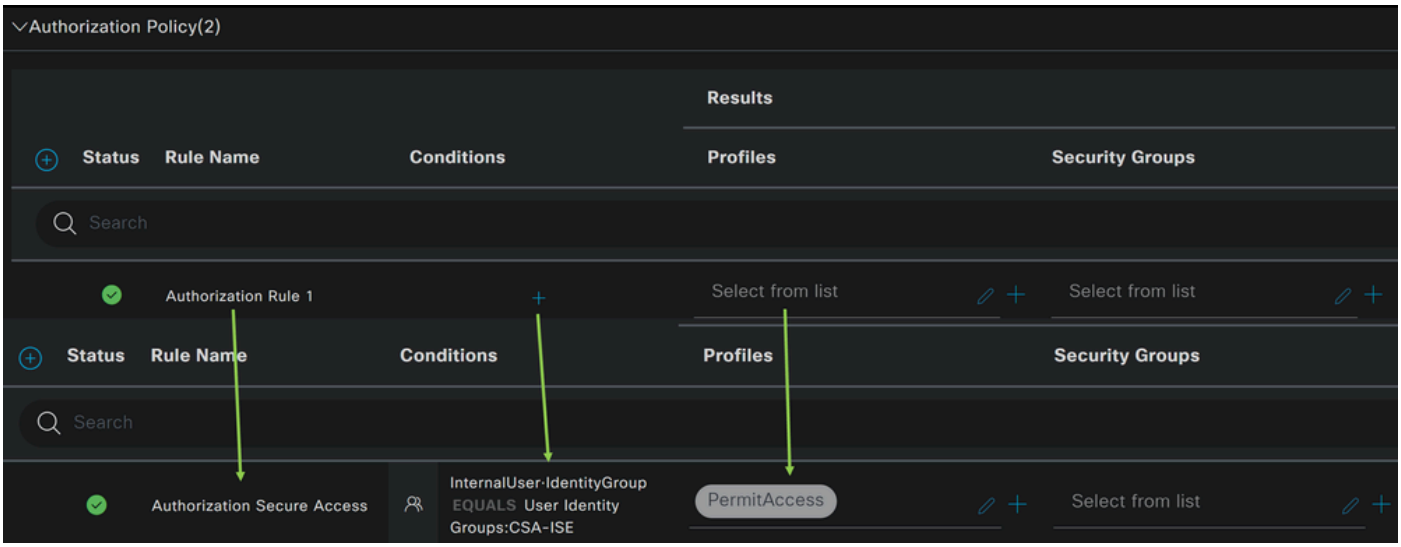
- Après cela, vous voyez les**Authorization** stratégies affichées :



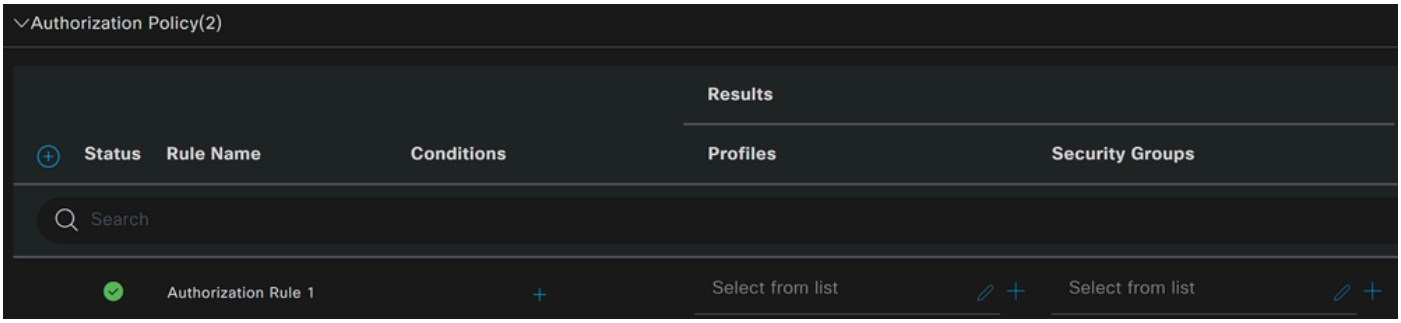
La stratégie est la même que celle définie à l'étape Configure Policy Set.

Politique d'autorisation

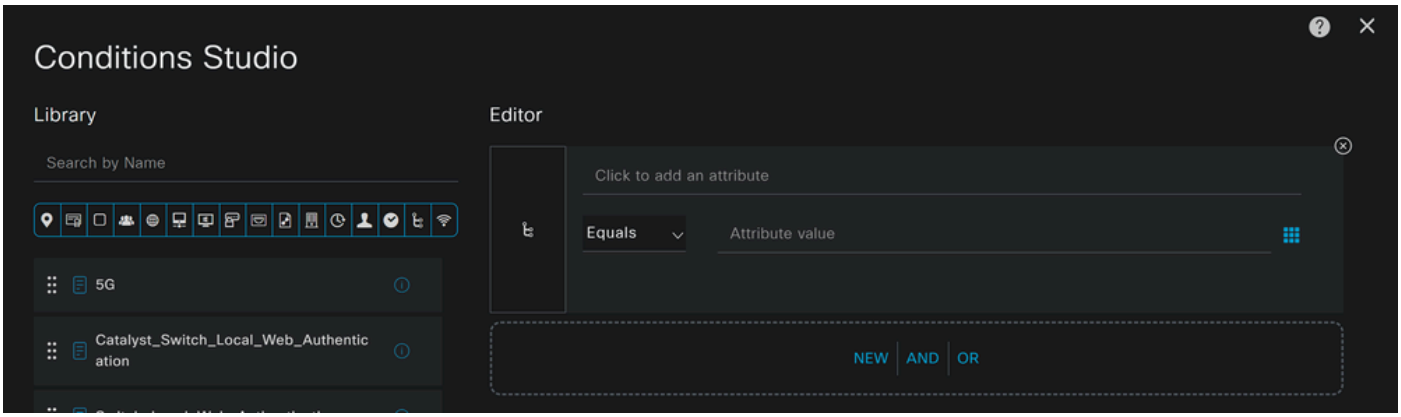
Vous pouvez configurer la stratégie d'autorisation de différentes manières. Dans ce cas, autorisez uniquement les utilisateurs du groupe défini à l'étape Configurer un groupe.Consultez l'exemple suivant pour configurer votre stratégie d'autorisation :



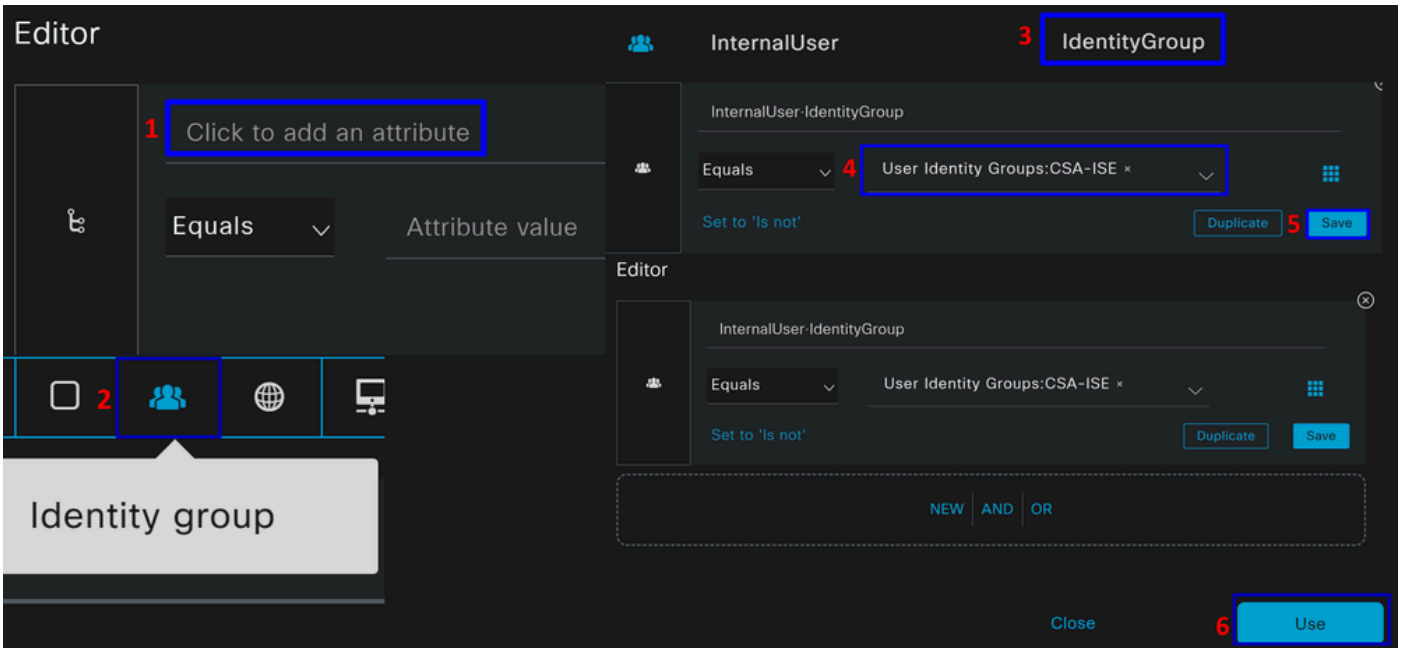
- Cliquez sur **Authorization Policy**
- Cliquez sur + pour définir la politique d'autorisation comme suit :



- Pour l'étape suivante, modifiez lesRule Name,Conditionset Profiles
- Lors de la configuration de la **Name** , configurez un nom pour identifier facilement la stratégie d'autorisation
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :

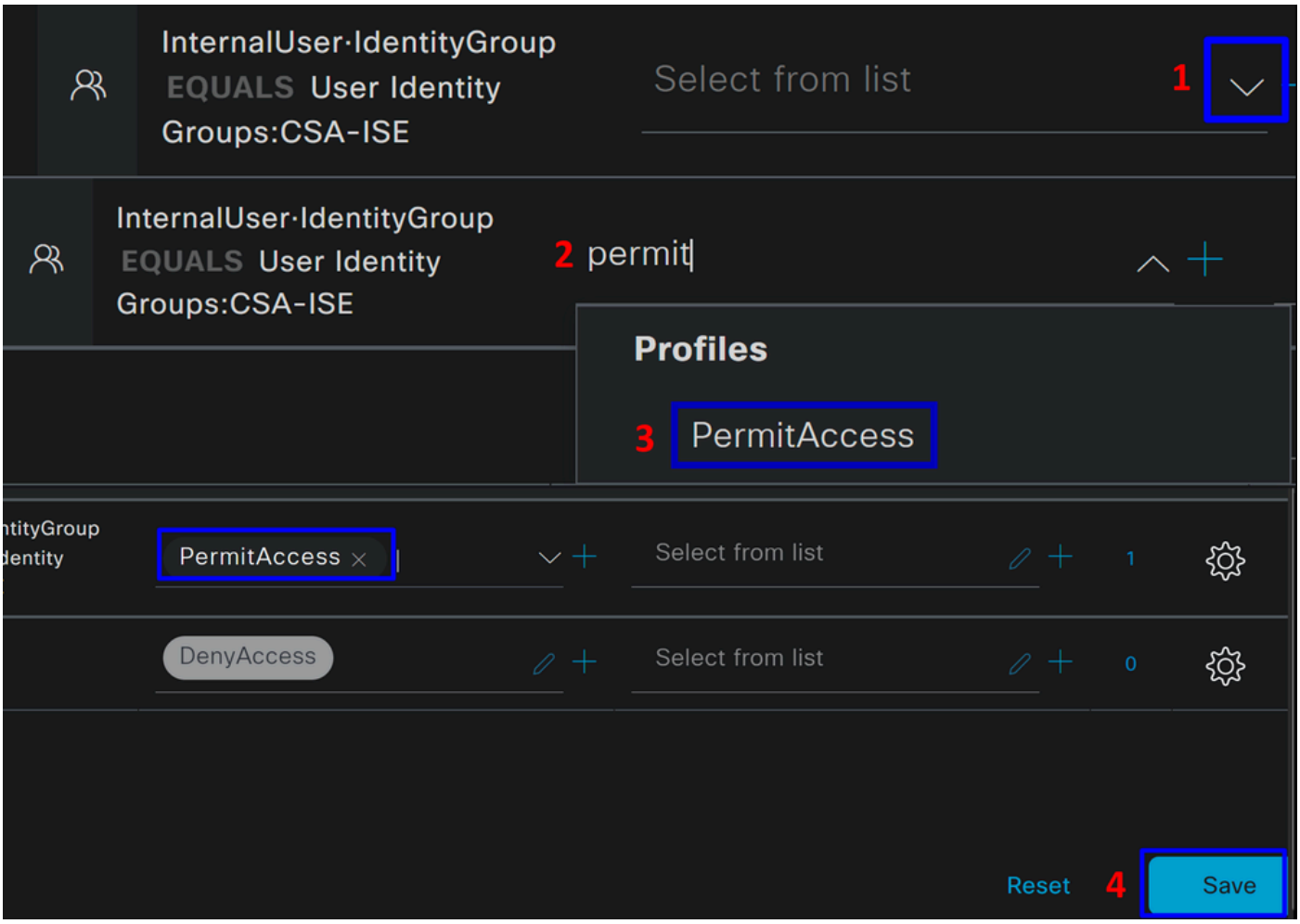


1. Pour créer les conditions, cliquez sur Click to add an attribute
2. Cliquez sur le **Identity Group** bouton
3. Sous les options derrière, cliquez sur Internal User - **IdentityGroup** option
4. Sous l'**Equals**option, utilisez la liste déroulante pour trouver le **Group**approuvé pour l'authentification à l'étape, Configurer un groupe
5. Cliquer **Save**
6. Cliquer **Use**



Après cela, vous devez définir le **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

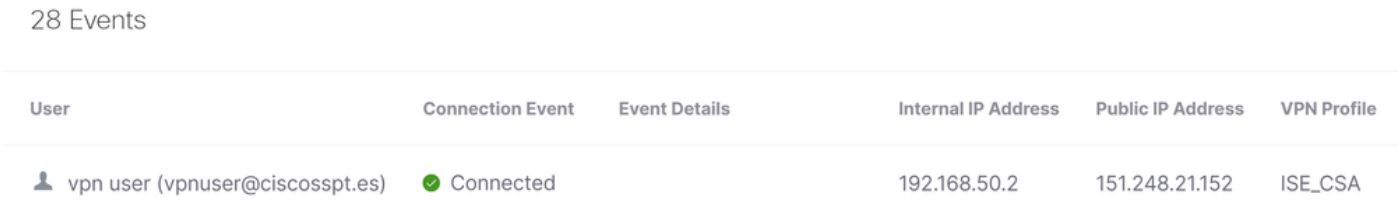
1. Sous le **Authorization Policy**, cliquez sur le bouton déroulant sur **Profiles**
2. Rechercher un permis
3. Sélectionner **PermitAccess**
4. Cliquer Save



Après cela, vous avez défini votre **Authorization** stratégie. Authentifiez-vous pour vérifier si l'utilisateur se connecte sans problème et si vous pouvez voir les journaux sur Secure Access et ISE.

Pour vous connecter au VPN, vous pouvez utiliser le profil créé sur Secure Access et vous connecter via Secure Client avec le profil ISE.

- Comment le journal s'affiche-t-il dans Secure Access lorsque l'authentification est approuvée ?
  - Accédez au tableau de bord Secure Access
  - Cliquez sur **Monitor** > **Remote Access Log**



- Comment le journal s'affiche-t-il dans ISE lorsque l'authentification est approuvée ?
  - Accédez à la page **Cisco ISE Dashboard**
  - Cliquez sur **Operations** > **Live Logs**

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

Comment le journal s'affiche-t-il dans Duo lorsque l'authentification est approuvée ?

- Accédez au panneau d'administration Duo
- Cliquez sur **Reports** > **Authentication Log**

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

Configuration des utilisateurs de Radius Local ou Active Directory

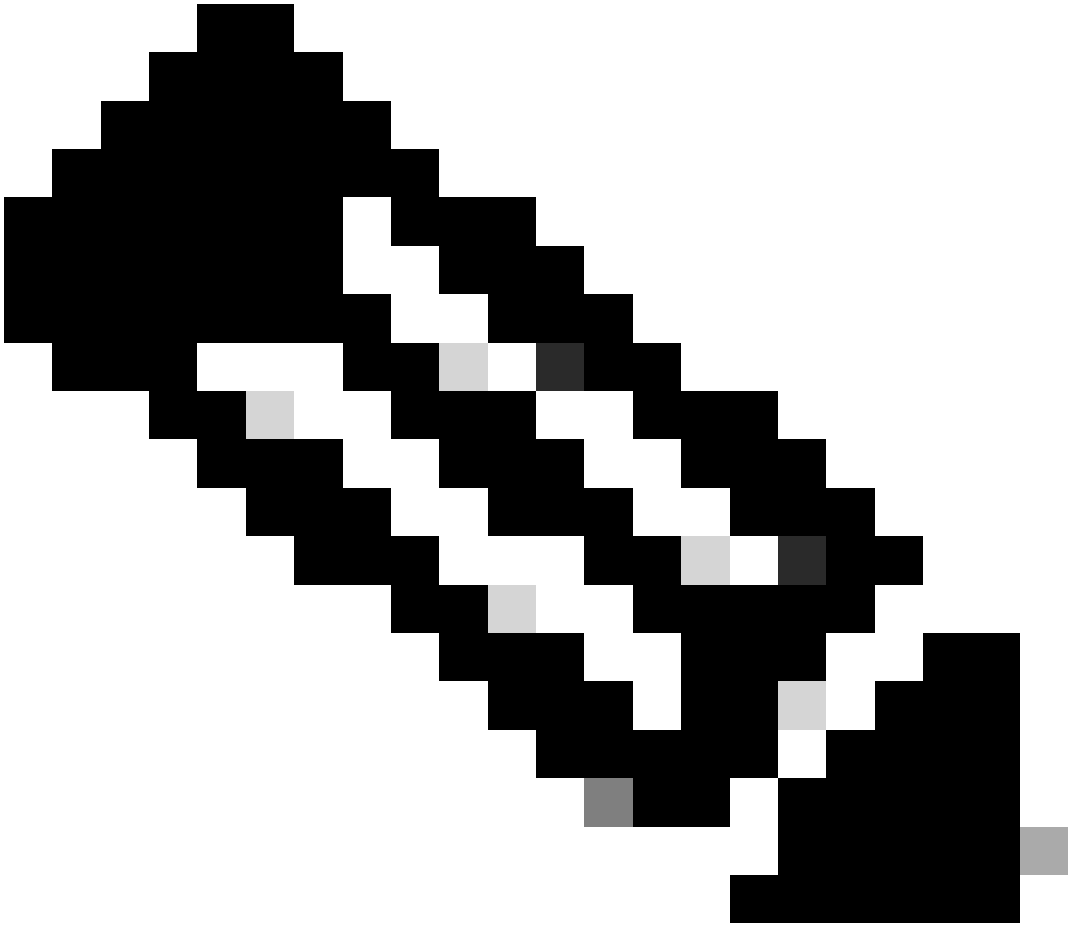
Configuration de la position ISE

Dans ce scénario, créez la configuration pour vérifier la conformité des terminaux avant d'accorder ou de refuser l'accès aux ressources internes.

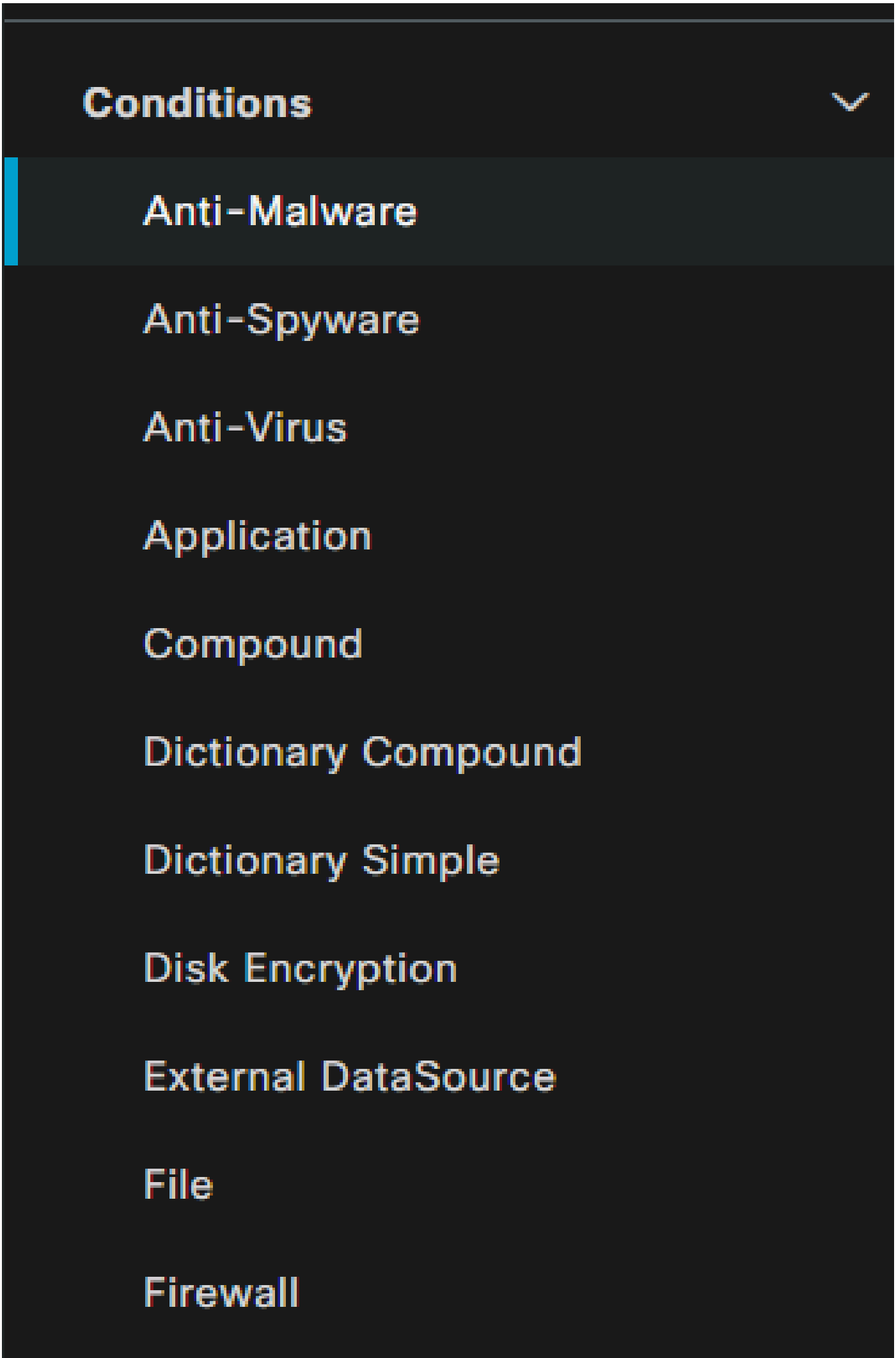
Pour le configurer, passez aux étapes suivantes :

Configuration des conditions de posture

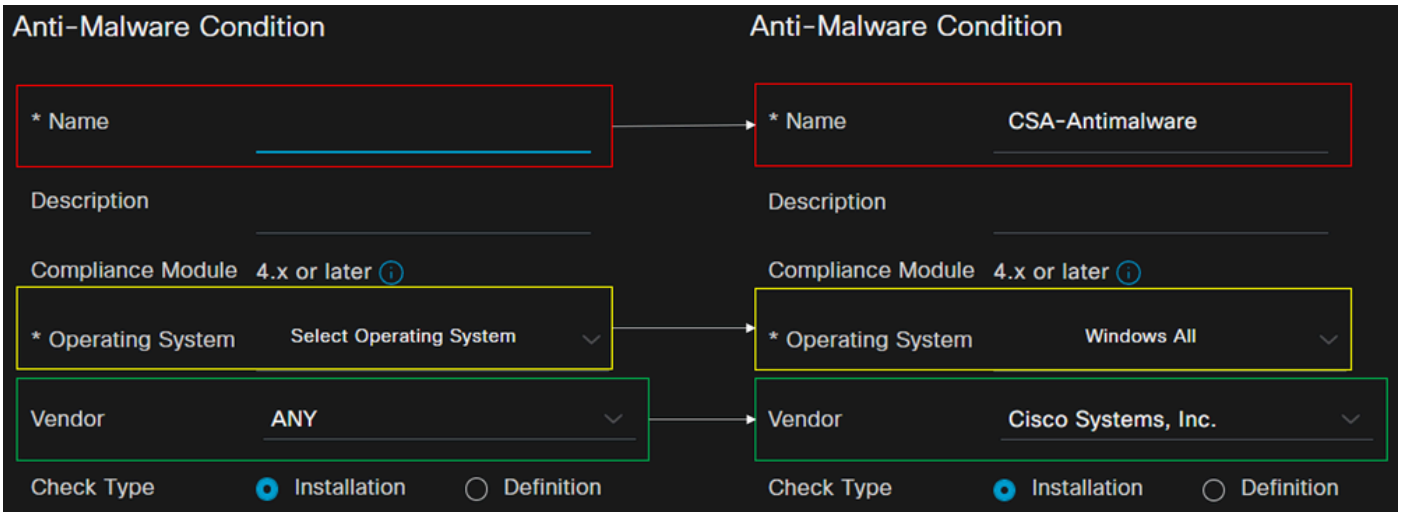
- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center** > **Policy Elements** > **Conditions**
- Cliquez sur **Anti-Malware**



Remarque : Vous y trouverez de nombreuses options pour vérifier la position de vos périphériques et effectuer l'évaluation correcte en fonction de vos politiques internes.

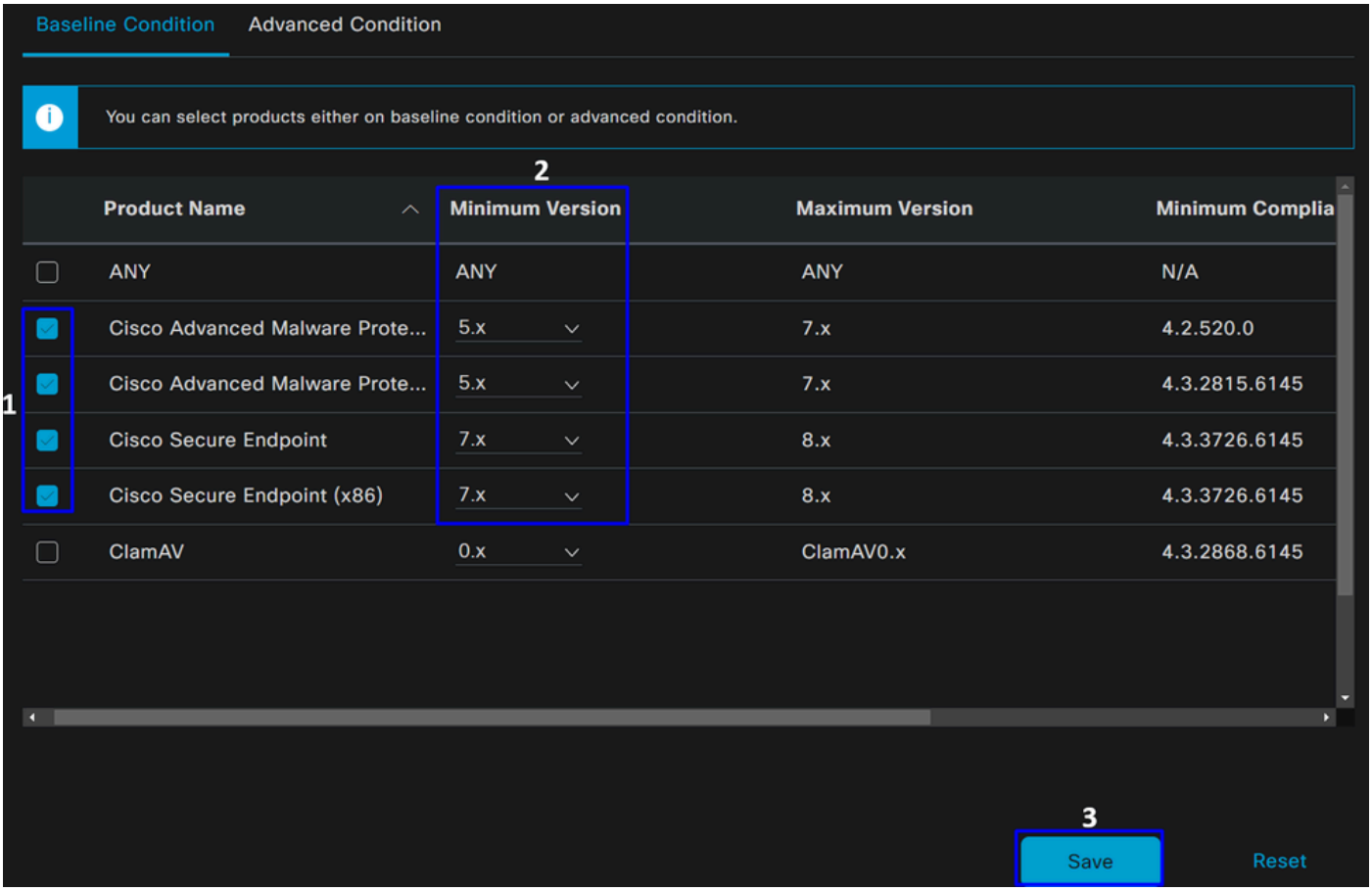

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

pour détecter l'installation de l'antivirus sur le système ; vous pouvez également choisir la version du système d'exploitation si nécessaire.



- **Name**: Utiliser un nom pour reconnaître la condition anti-programme malveillant
- **Operating System**: Choisissez le système d'exploitation que vous souhaitez mettre sous la condition
- **Vendor**: Choisissez un fournisseur ou ANY
- **Check Type**: Vous pouvez vérifier si l'agent est installé ou la version de définition de cette option.

- Pour **Products for Selected Vendor**, vous configurez ce que vous souhaitez vérifier à propos du logiciel anti-programme malveillant sur le périphérique.

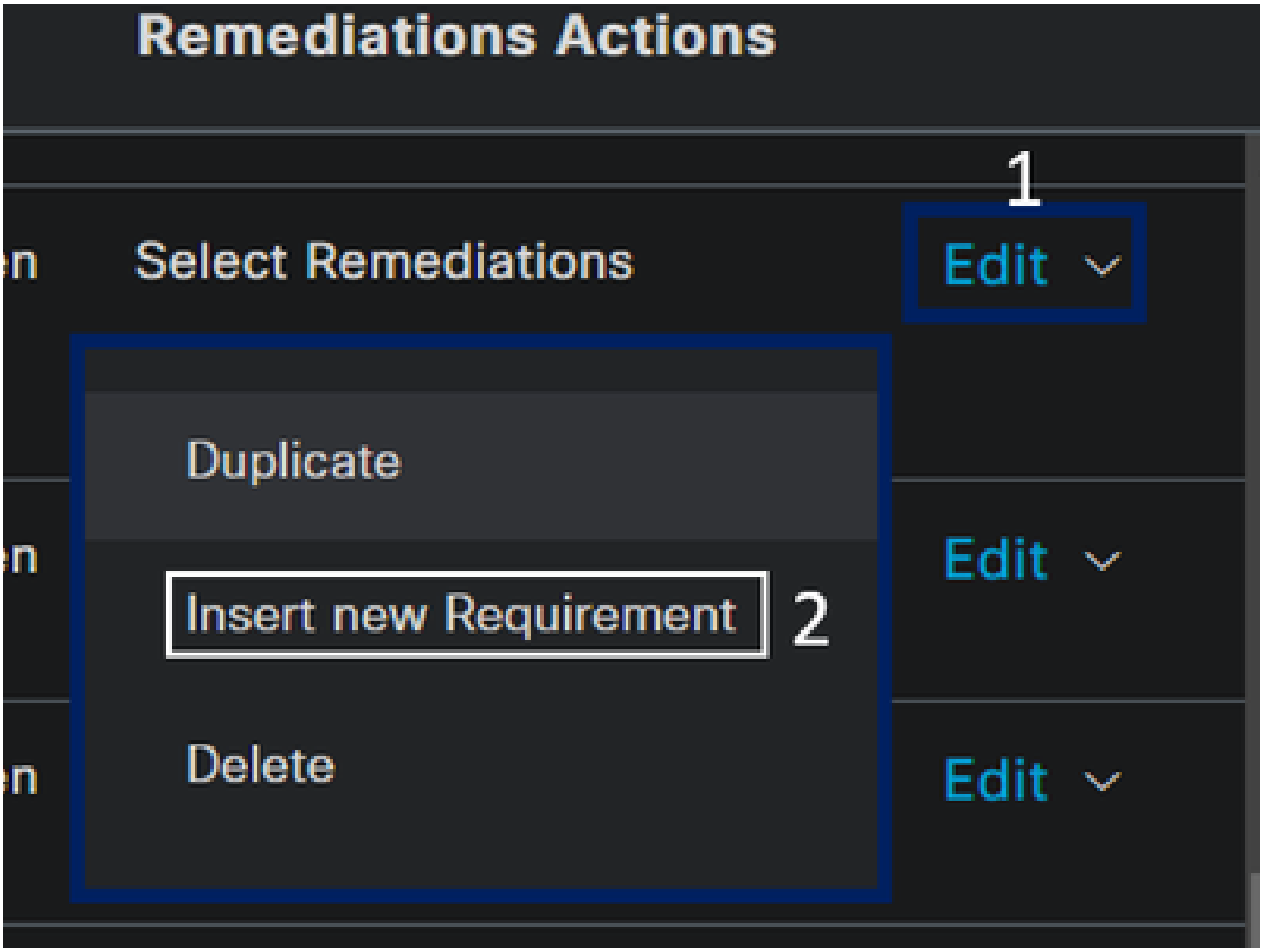


1. Cochez la case correspondant aux conditions que vous souhaitez évaluer
2. Configurez la version minimale à vérifier
3. Cliquez sur Enregistrer pour passer à l'étape suivante

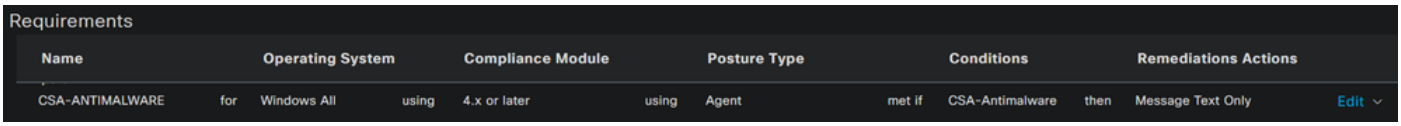
Une fois que vous l'avez configuré, vous pouvez passer à l'étape **Configure Posture Requirements.**

Configuration des exigences de posture

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center** > **Policy Elements** > **Requeriments**
- Cliquez sur **Edit** l'une des conditions requises, puis sur **Insert new Requirement**



- Sous la nouvelle condition, configurez les paramètres suivants :



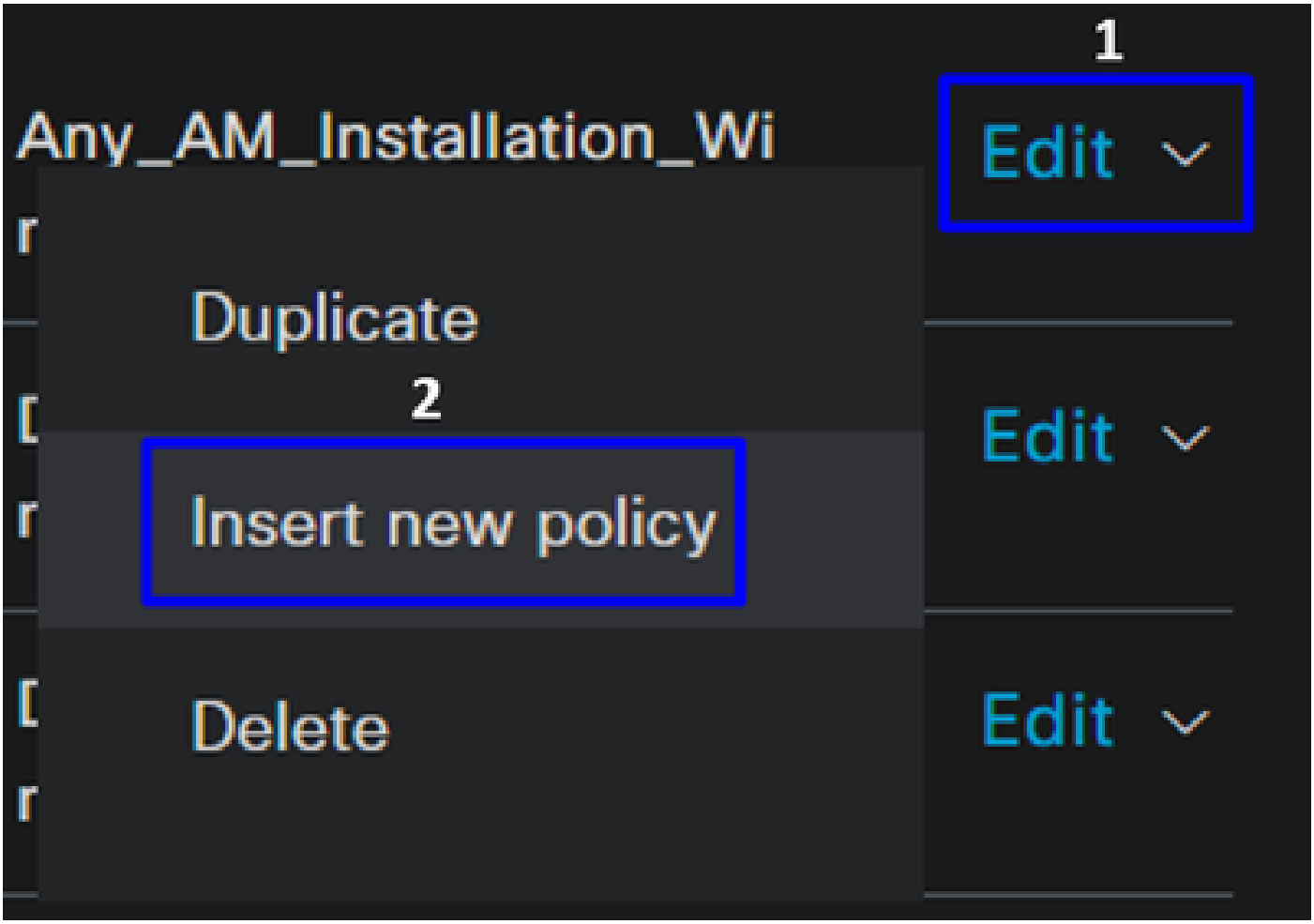
- **Name**: Configurer un nom pour reconnaître la condition requise pour la protection contre les programmes malveillants
- **Operating System**: Choisissez le système d'exploitation que vous choisissez dans l'étape de condition, Système d'exploitation

- **Compliance Module**: Vous devez vous assurer de sélectionner le même module de conformité que vous avez sous l'étape de condition, Condition anti-programme malveillant
- **Posture Type**: Choisir un agent
- **Conditions**: Choisissez la ou les conditions que vous avez créées à l'étape Configurer les conditions de posture
- **Remediations Actions**: Choisissez **Message Text Only** pour cet exemple, ou si vous avez une autre action corrective, utilisez-la
- Cliquer **Save**

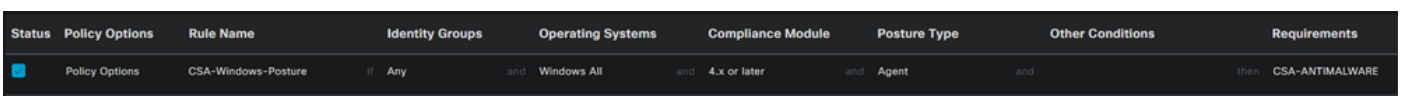
Une fois la configuration effectuée, vous pouvez passer à l'étape suivante : **Configure Posture Policy**

Configurer la politique de posture

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center** > **Posture Policy**
- Cliquez sur **Edit** l'une des stratégies, puis sur **Insert new Policy**



- Dans la nouvelle stratégie, configurez les paramètres suivants :



- **Status**: Cochez la case no enable the policy

- **Rule Name**: configurez un nom pour reconnaître la stratégie configurée
- **Identity Groups**: Choisissez les identités que vous souhaitez évaluer
- **Operating Systems**: Sélectionnez le système d'exploitation en fonction de la condition et de la condition configurées avant
- **Compliance Module**: Sélectionnez le module de conformité en fonction de la condition et de la condition configurées avant
- Posture Type: Choisir un agent
- **Requeriments**: Choisissez les exigences configurées à l'étape, Configurer les exigences de posture
- Cliquer **Save**

Configurer le provisionnement client

Pour fournir aux utilisateurs le module ISE, configurez le provisionnement client pour équiper les machines du module de posture ISE. Cela vous permet de vérifier la position des machines une fois l'agent installé. Pour poursuivre ce processus, voici les étapes suivantes :

Accédez à votre tableau de bord ISE.

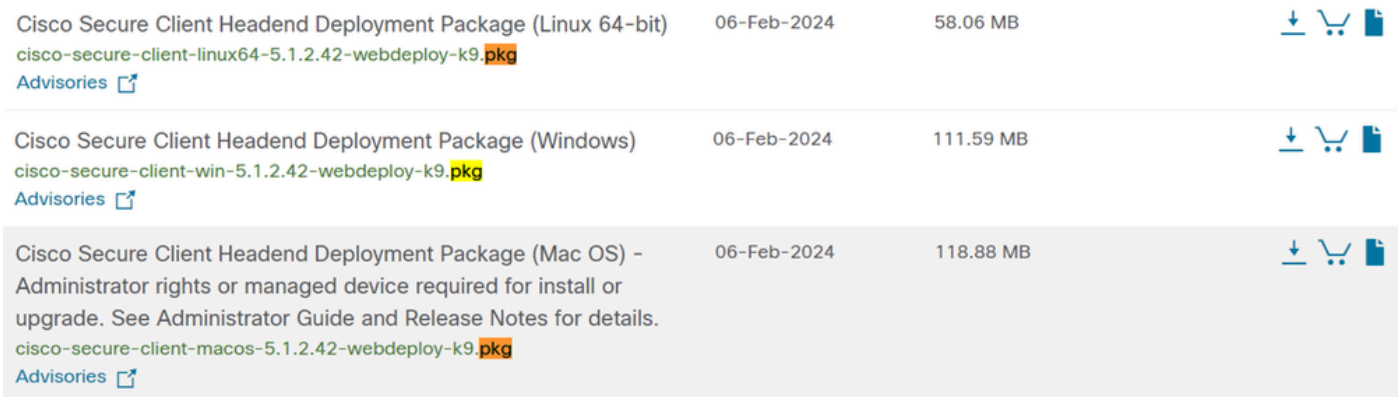
- Cliquez sur **Work Center** > **Client Provisioning**
- Choisir **Resources**

Vous devez configurer trois éléments dans le cadre du provisionnement du client :

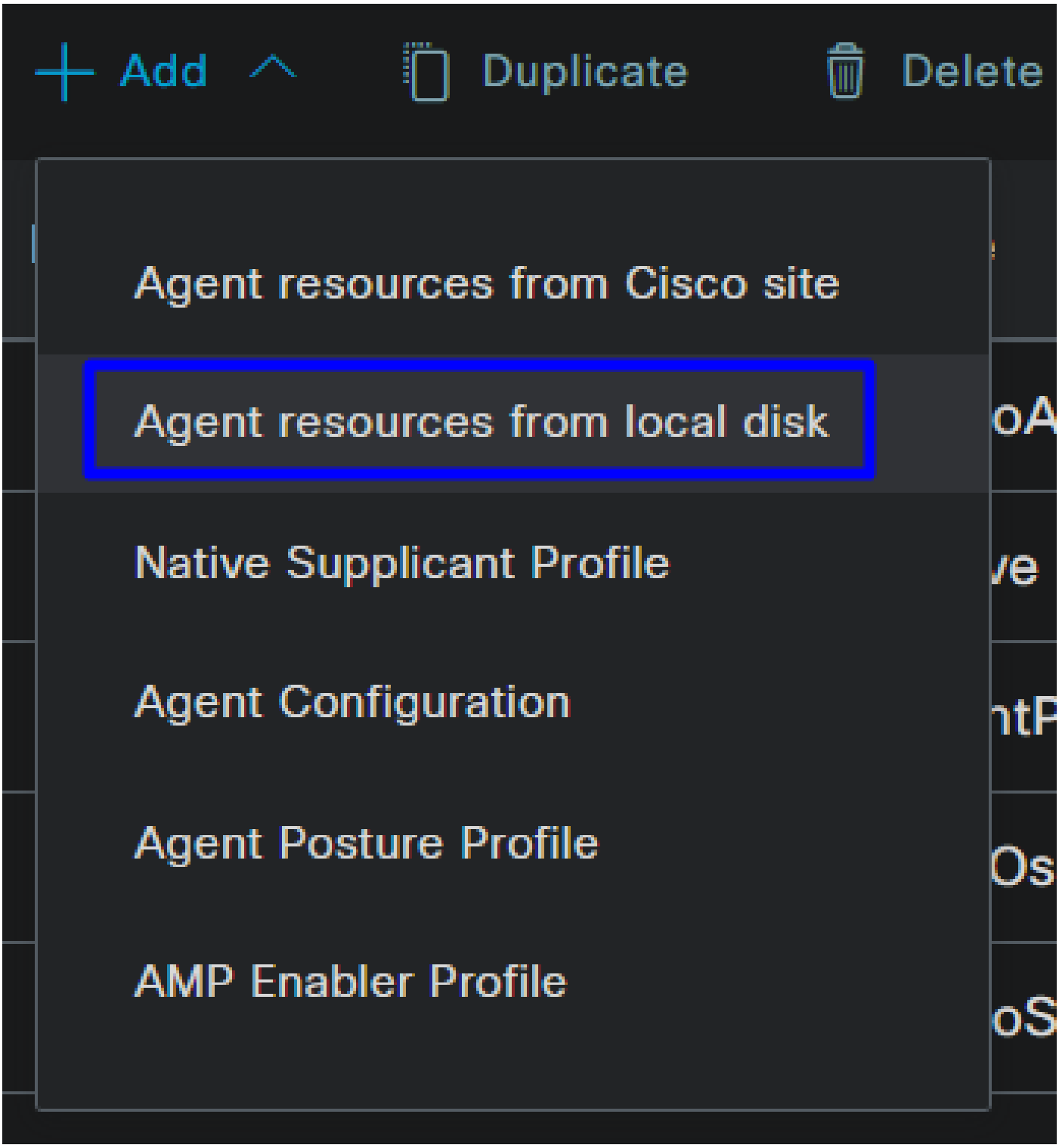
Ressources à configurer	Description
1. **Agent Resources**	Package d'approvisionnement Web du client sécurisé.
2. **Compliance Module**	Module de conformité Cisco ISE
3. **Agent Profile**	Contrôle du profil d'approvisionnement.
3. **Agent Configuration**	Définissez les modules à provisionner en configurant le portail de provisionnement, à l'aide du profil d'agent et des ressources d'agent.

Step 1 Télécharger et charger les ressources de l'agent

- Pour ajouter une nouvelle ressource d'agent, accédez au portail de téléchargement Cisco et téléchargez le package de déploiement Web ; le fichier web deploy doit être au format .pkg.

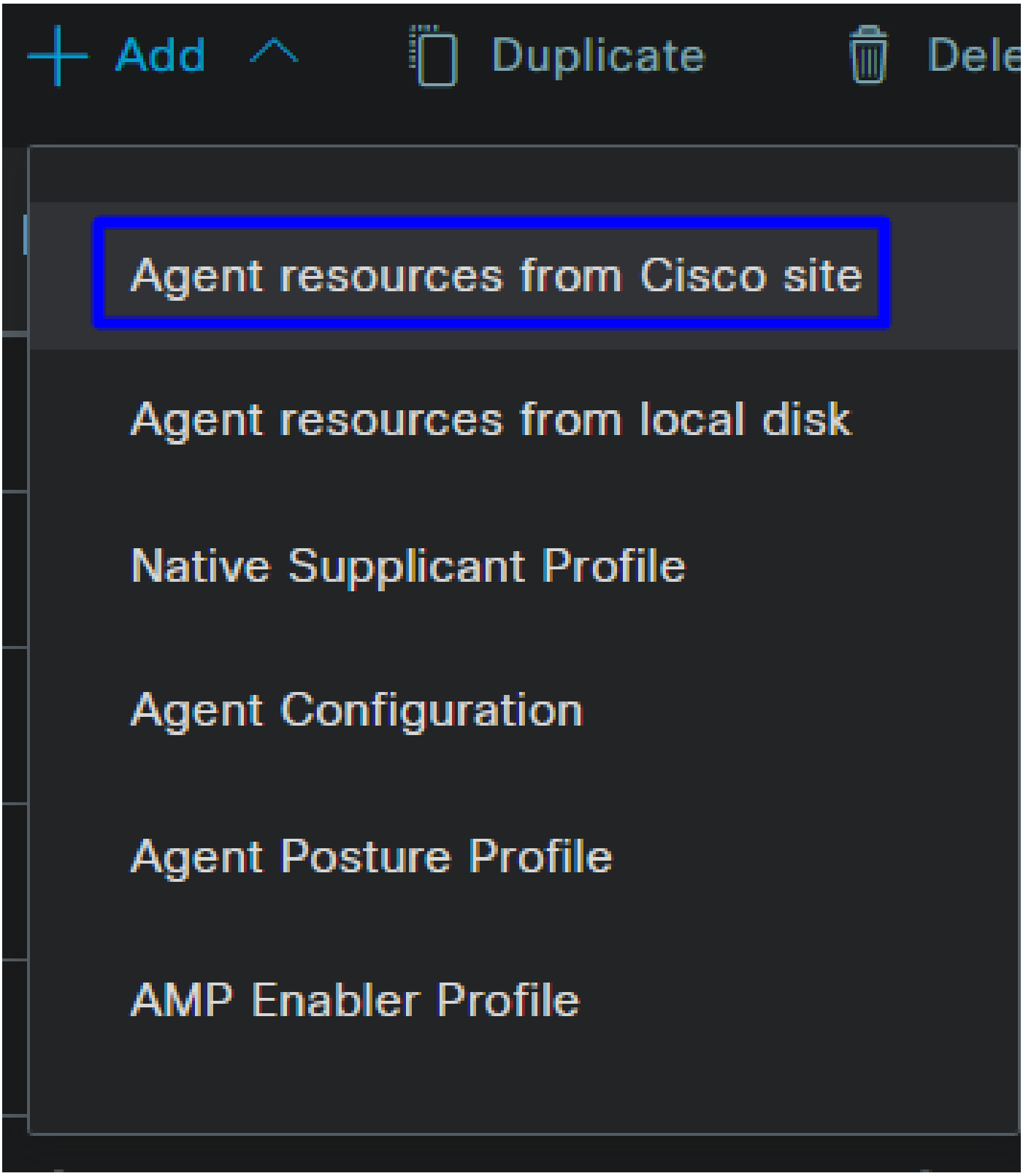


- Cliquez sur+ Add > Agent resources from local disk et téléchargez les packages

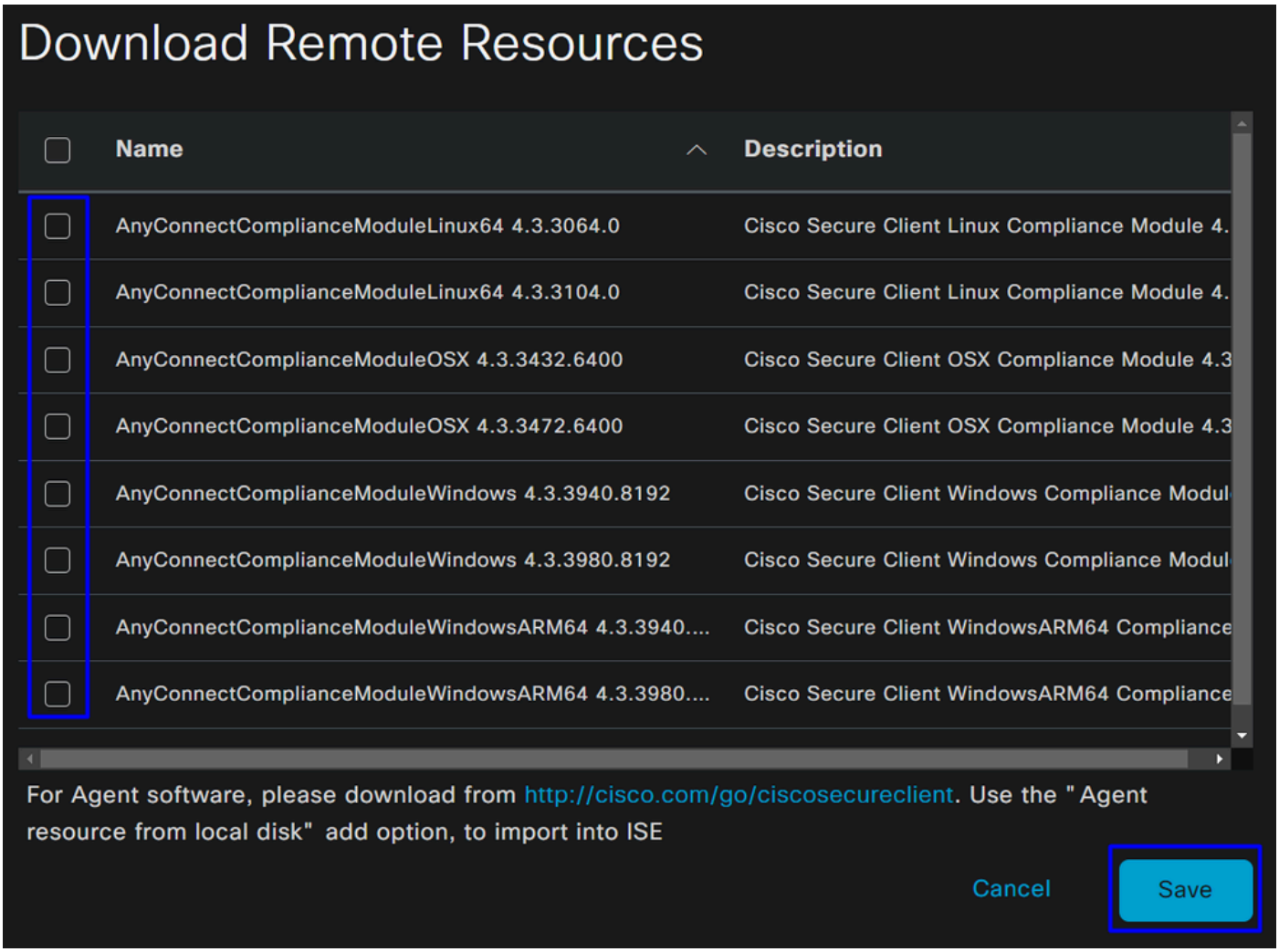


Step 2 Télécharger le module de conformité

- Cliquez sur + Add > Agent resources from Cisco Site

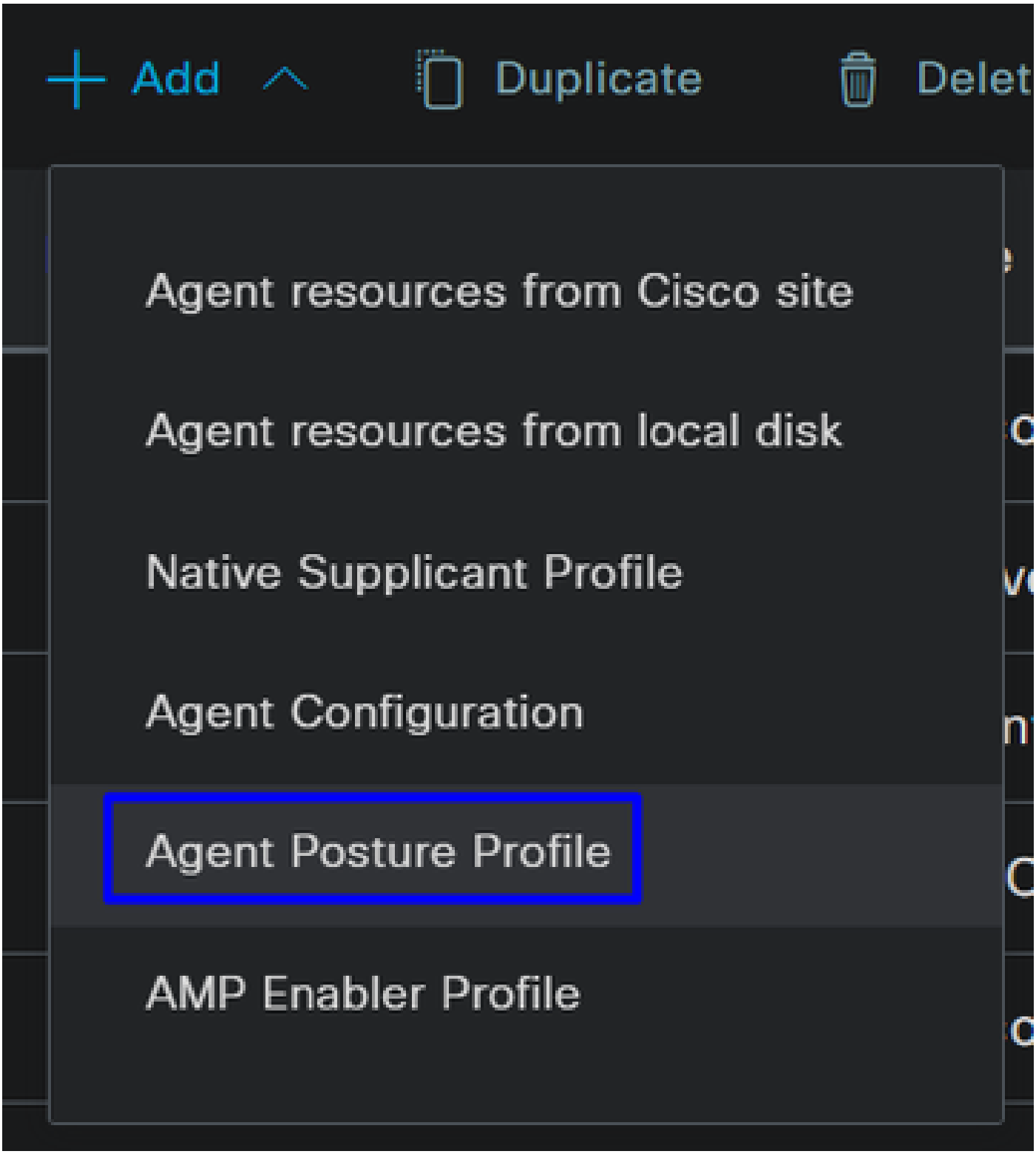


- Cochez la case correspondant à chaque module de conformité requis et cliquez sur **Save**

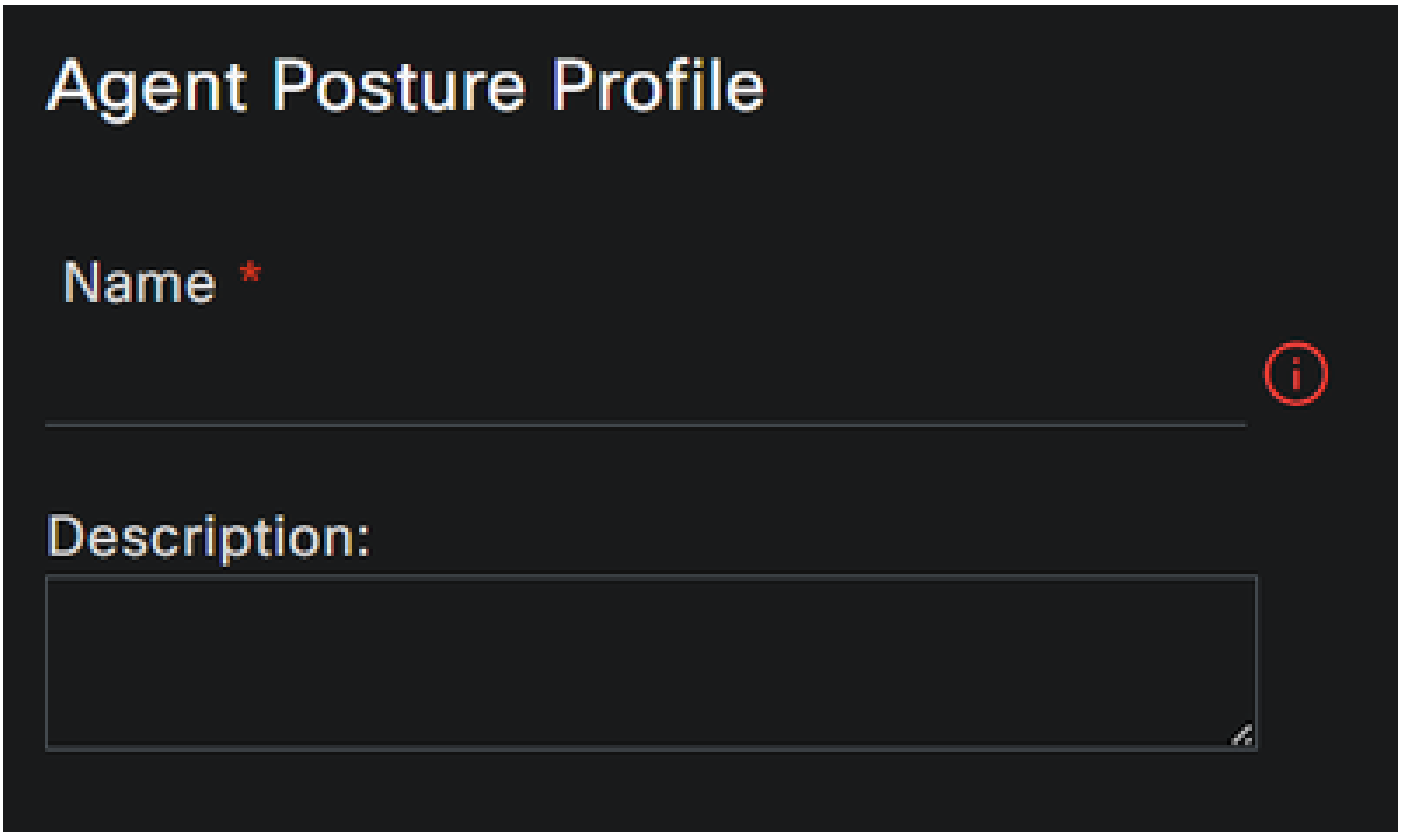


Step 3Configuration du profil d'agent

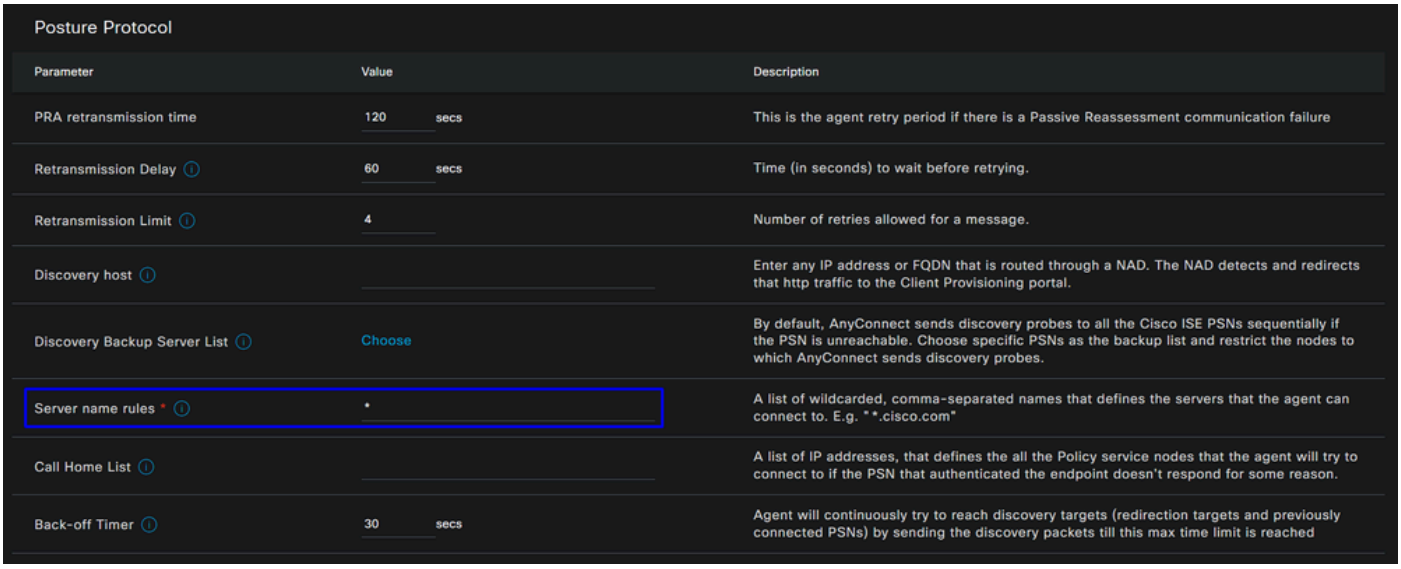
- Cliquez sur + Add > Agent Posture Profile



- Créez un **Name** pour le **Posture Profile**

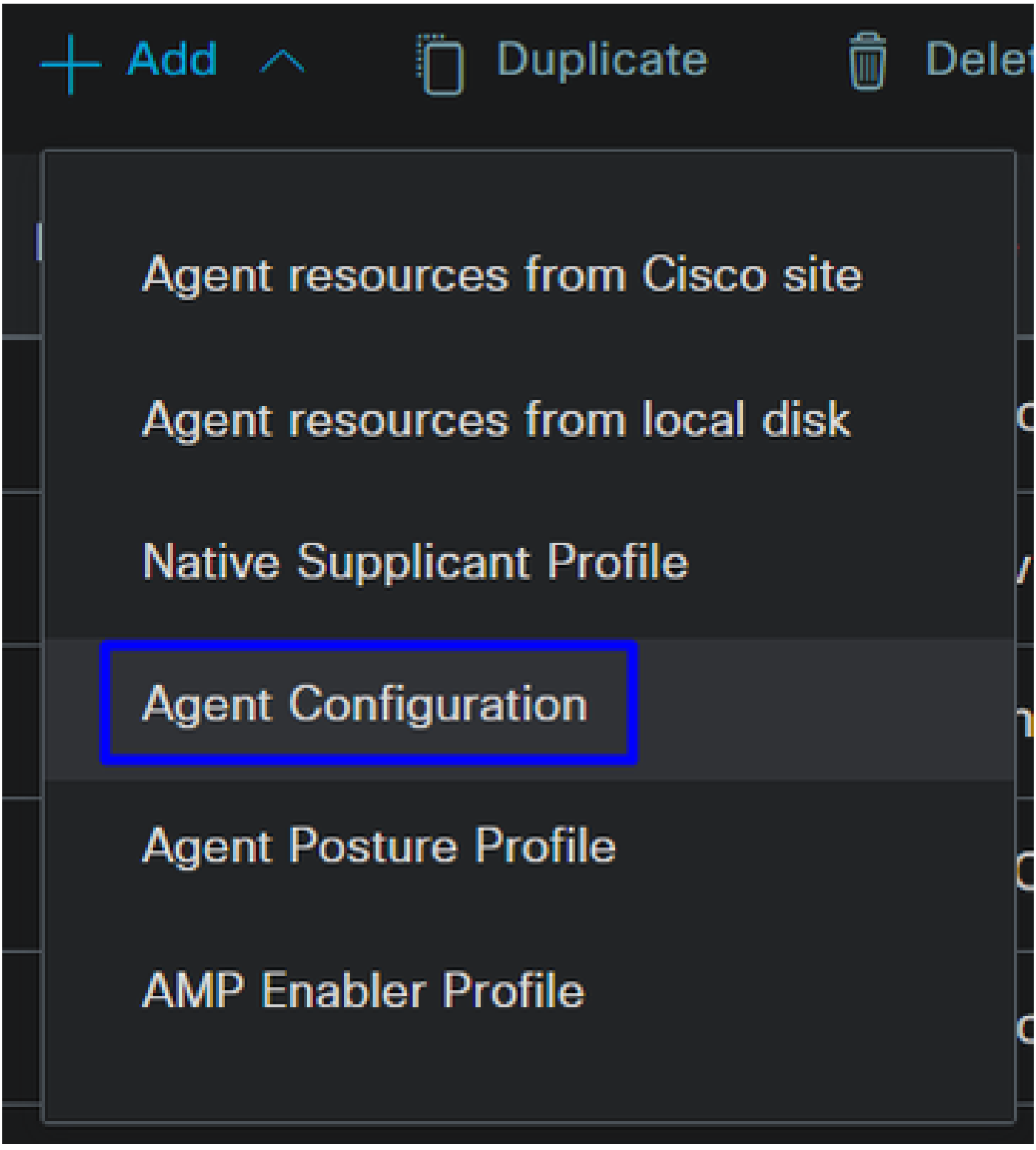


- Sous Règles de nom de serveur, placez un * et cliquez sur **Save** ensuite

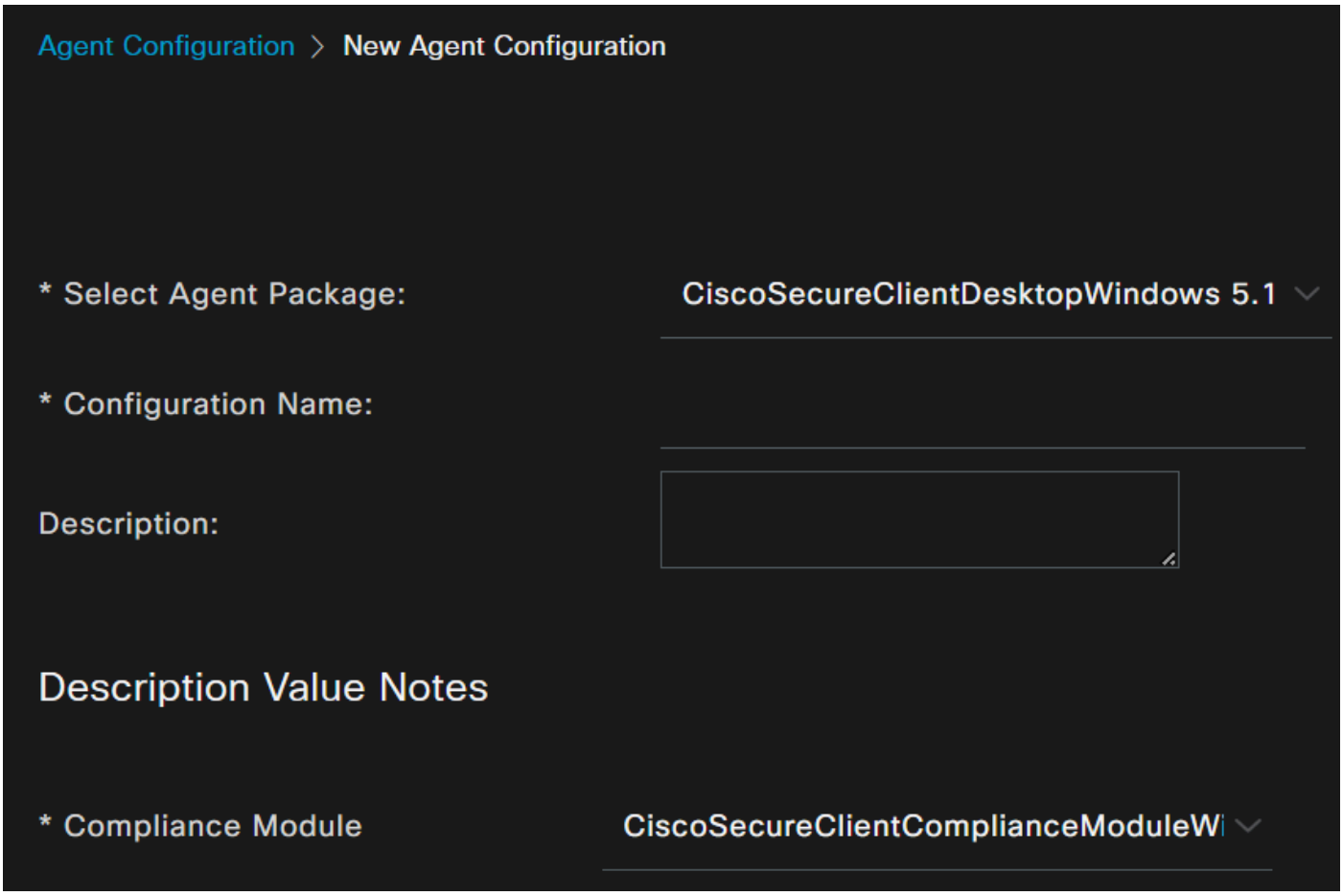


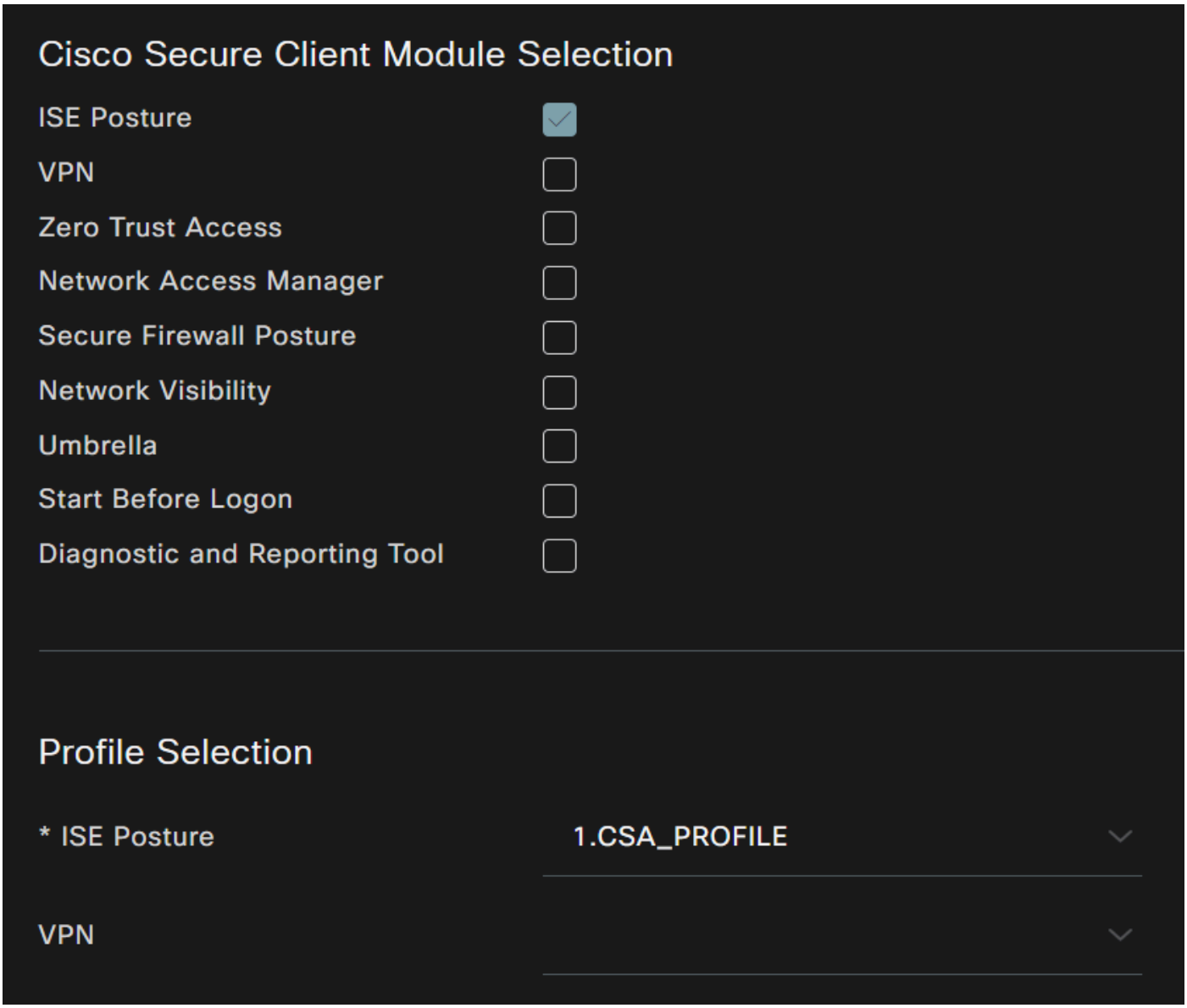
Step 4 Configuration de l'agent

- Cliquez sur + Add > Agent Configuration

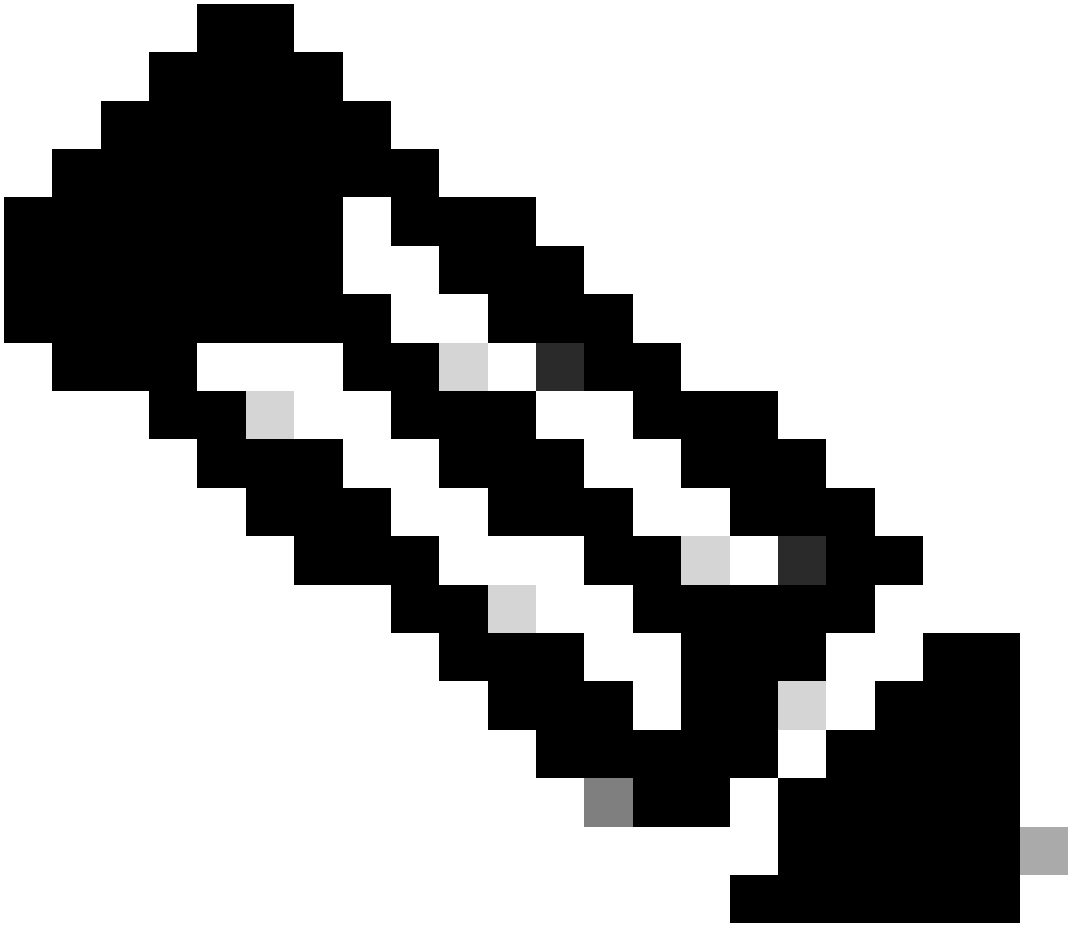


- Ensuite, configurez les paramètres suivants :


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



- Select Agent Package : Sélectionnez le package téléchargé à l'étape 1 Télécharger et télécharger les ressources de l'agent
- **Configuration Name**: Choisissez un nom pour reconnaître le **Agent Configuration**
- **Compliance Module**: Sélectionnez le module de conformité téléchargé à l'étape 2 Télécharger le module de conformité
- Cisco Secure Client Module Selection
  - **ISE Posture**: Cochez la case
- **Profile Selection**
  - **ISE Posture**: Sélectionnez le profil ISE configuré à l'étape 3 Configuration du profil d'agent
- Cliquer **Save**

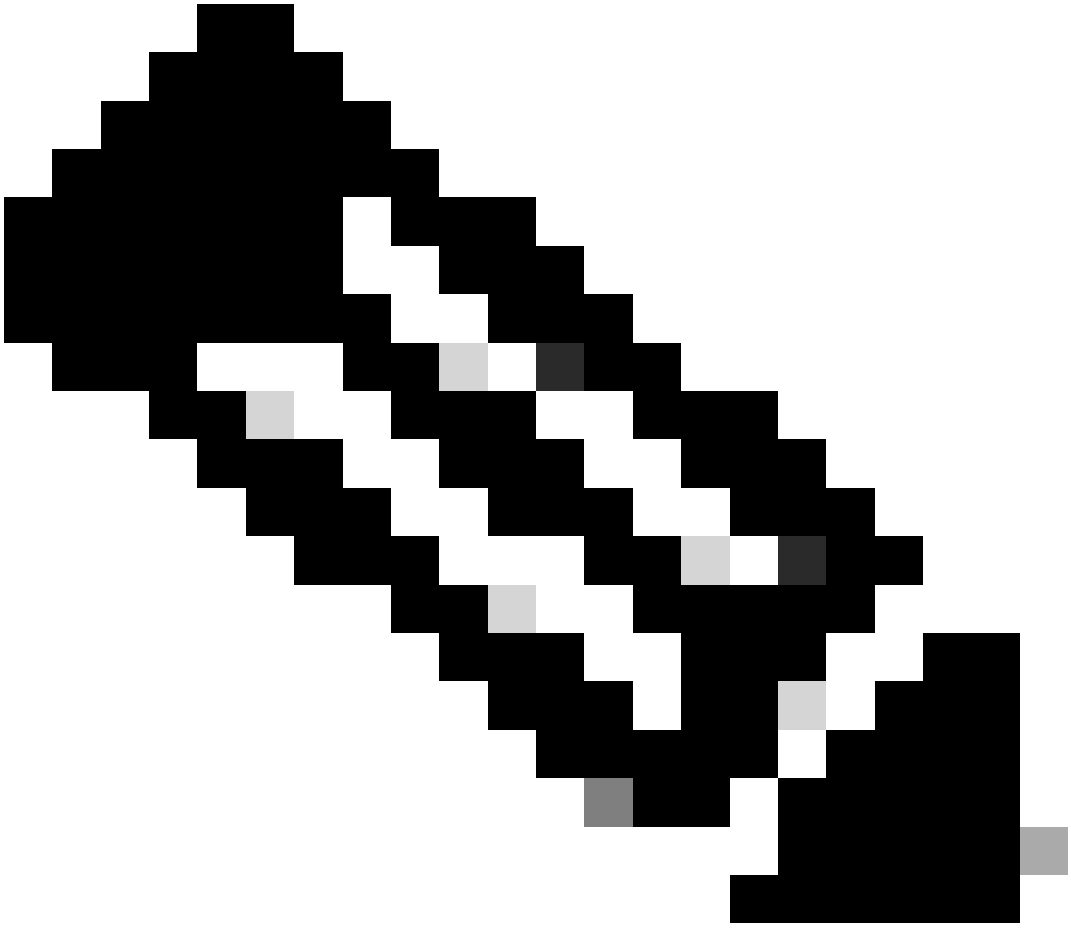


Remarque : Il est recommandé que chaque système d'exploitation, Windows, Mac OS ou Linux, dispose d'une configuration client indépendante.

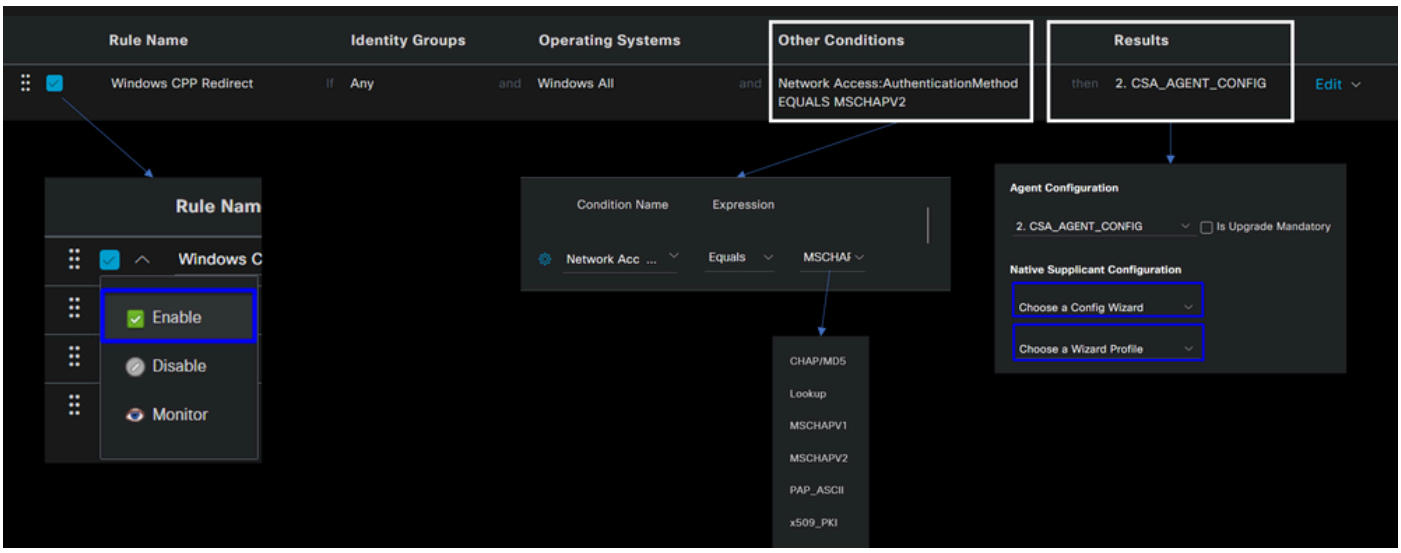
Configurer la politique de provisionnement client

Pour activer le provisionnement de la position ISE et des modules configurés à la dernière étape, vous devez configurer une stratégie pour effectuer le provisionnement.

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center** > **Client Provisioning**



Remarque : Il est recommandé que chaque système d'exploitation, Windows, Mac OS ou Linux, dispose d'une stratégie de configuration client.



- **Rule**

Name: Configurez le nom de la stratégie en fonction du type de périphérique et du groupe d'identités sélectionnés afin d'identifier facilement chaque stratégie

- **Identity Groups**: Sélectionnez les identités que vous souhaitez évaluer dans la stratégie
- **Operating Systems**: Choisissez le système d'exploitation en fonction du package d'agent sélectionné à l'étape Sélectionner un package d'agent
- **Other Condition**: Choisissez **Network Access** en fonction de la méthode **Authentication Method**EQUALSconfigurée à l'étape, Ajouter un groupe RADIUS ou laissez vide
- **Result**: Sélectionnez la configuration de l'agent configurée à l'étape 4. Configurez la configuration de l'agent
  - **Native Supplicant Configuration**: ChoisissezConfig Wizardet Wizard Profile
- Marquez la stratégie comme étant activée si elle n'est pas répertoriée comme étant activée dans la case à cocher.

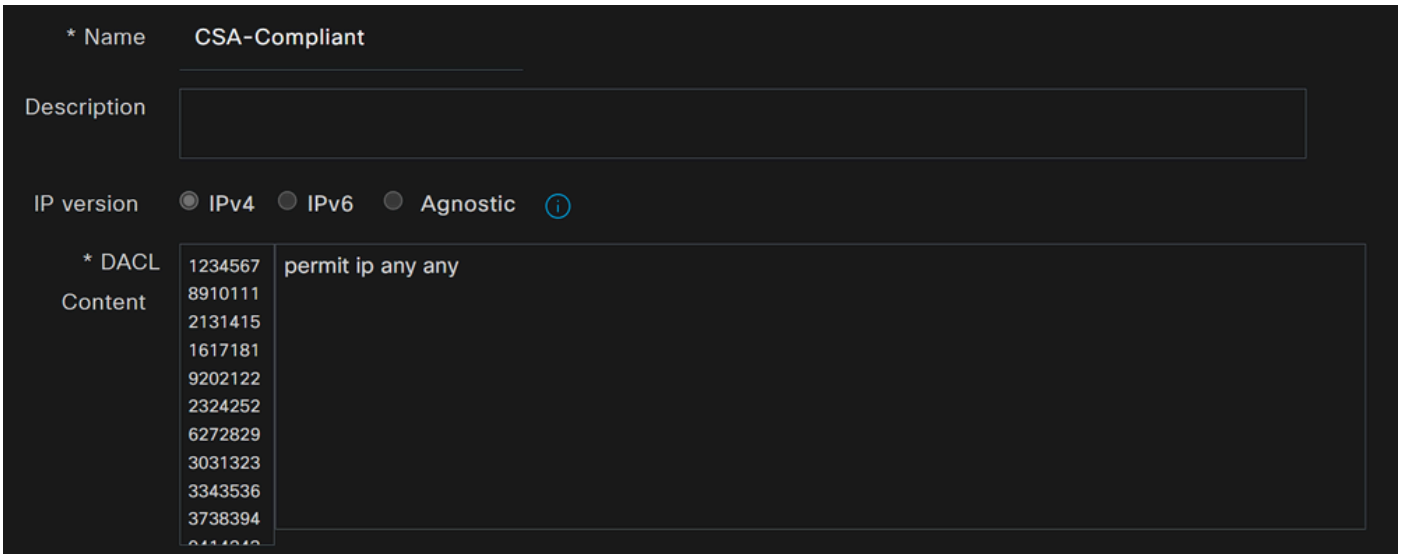
Créer les profils d'autorisation

Le profil d'autorisation limite l'accès aux ressources en fonction de la position des utilisateurs après le passage de l'authentification. L'autorisation doit être vérifiée pour déterminer les ressources auxquelles l'utilisateur peut accéder en fonction de la position.

Profil d'autorisation	Description
Conforme	Compatible utilisateur - Agent installé - Posture vérifiée
Conformité inconnue	User Uknown Compliant - Rediriger pour installer l'agent - Position en attente à vérifier
RefuserAccès	Utilisateur non conforme - Refuser l'accès

Pour configurer la liste de contrôle d'accès, accédez au tableau de bord ISE :

- Cliquez sur **Work Centers > Policy Elements > Downloadable ACLs**
- Cliquez sur **+Add**
- Créez le **Compliant DACL**

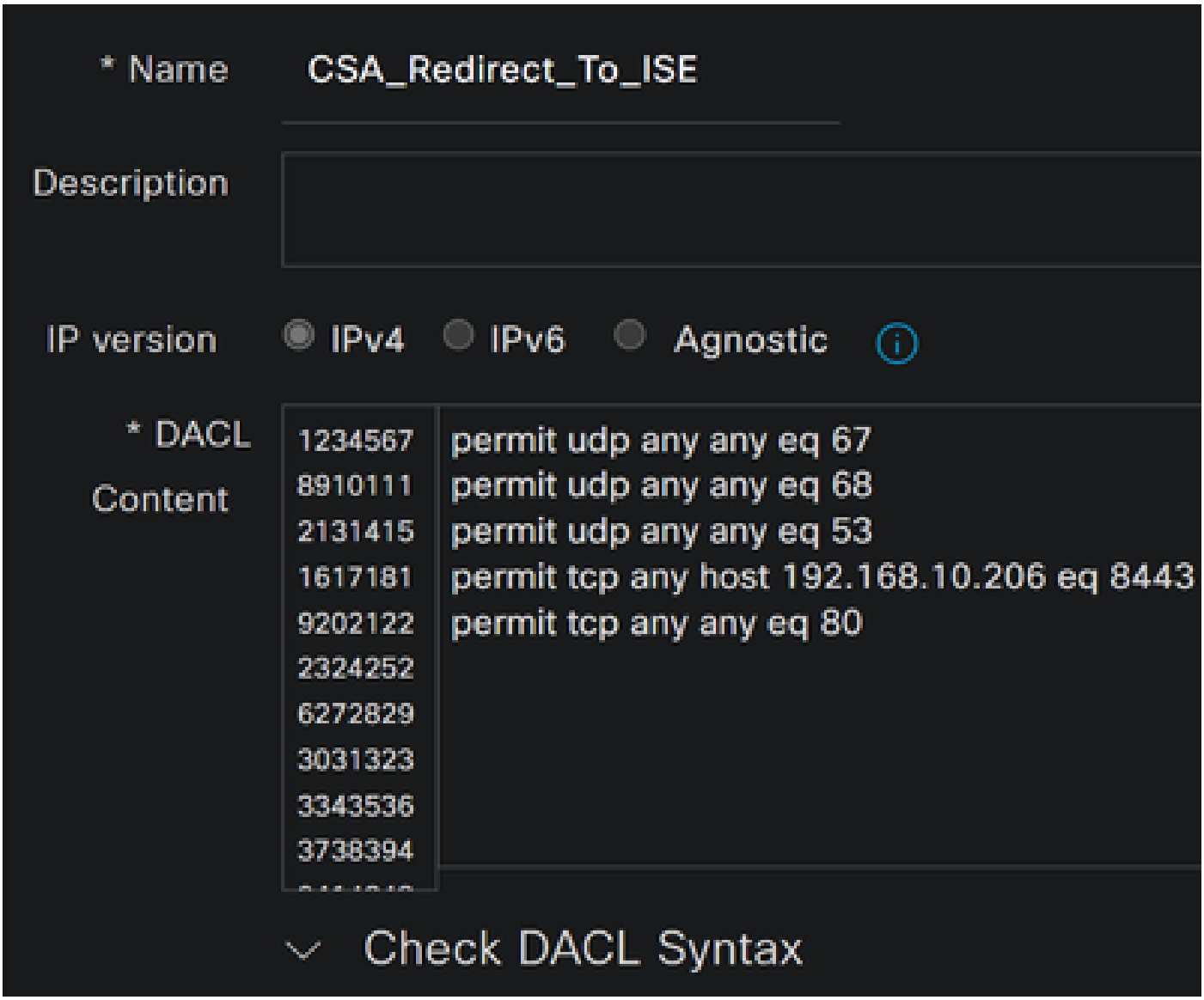


- **Name**: Ajoutez un nom faisant référence à la liste de contrôle d'accès DACL
- **IP version**: Choisir **IPv4**
- DACL Content: Créez une liste de contrôle d'accès téléchargeable (DACL) qui donne accès à toutes les ressources du réseau

```
permit ip any any
```

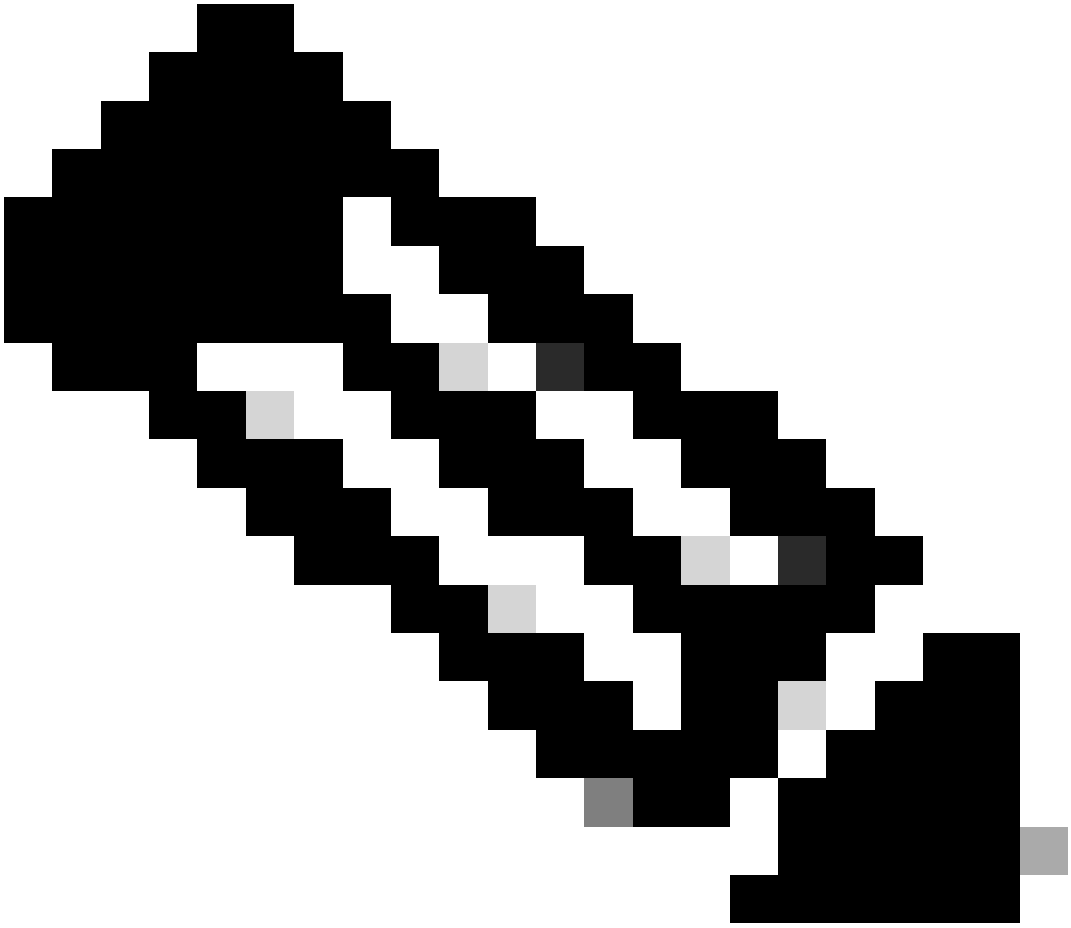
Cliquez sur **Save** et créez la DACL de conformité inconnue

- Cliquez sur **Work Centers > Policy Elements > Downloadable ACLs**
- Cliquez sur **+Add**
- Créez le **Unknown Compliant DACL**



- **Name**: Ajoutez un nom faisant référence à la liste de contrôle d'accès DACL-Unknown-Compliant
- **IP version**: Choisir **IPv4**
- **DACL Content**: Créez une liste de contrôle d'accès DACL qui donne un accès limité au réseau, DHCP, DNS, HTTP et au portail d'approvisionnement sur le port 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
```

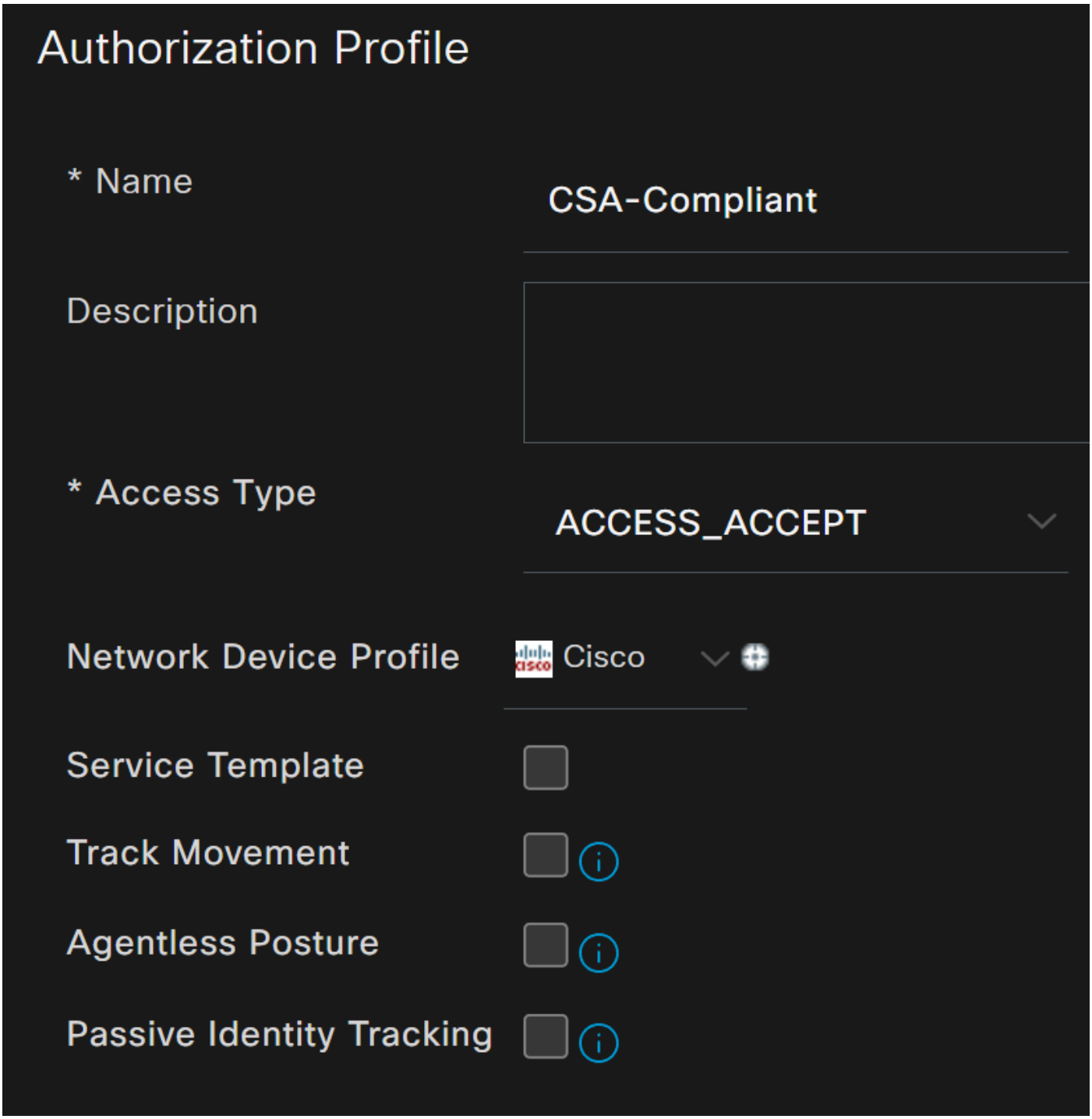


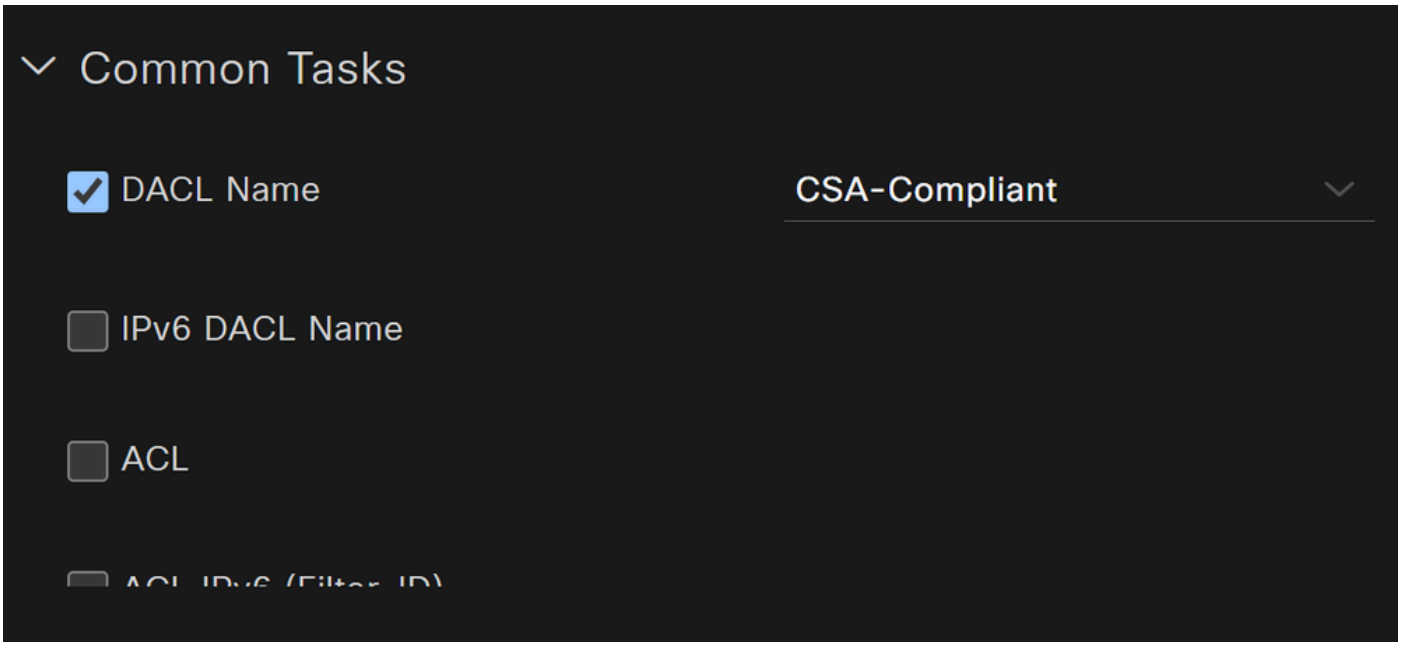
Remarque : Dans ce scénario, l'adresse IP 192.168.10.206 correspond au serveur Cisco Identity Services Engine (ISE) et le port 8443 est désigné pour le portail d'approvisionnement. Cela signifie que le trafic TCP vers l'adresse IP 192.168.10.206 via le port 8443 est autorisé, ce qui facilite l'accès au portail d'approvisionnement.

À ce stade, vous disposez de la liste de contrôle d’accès requise pour créer les profils d’autorisation.

Pour configurer les profils d'autorisation, accédez au tableau de bord ISE :

- Cliquez sur **Work Centers > Policy Elements > Authorization Profiles**
- Cliquez sur **+Add**
- Créez le **Compliant Authorization Profile**


Authorization Profile
* Name
CSA-Compliant
Description
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking

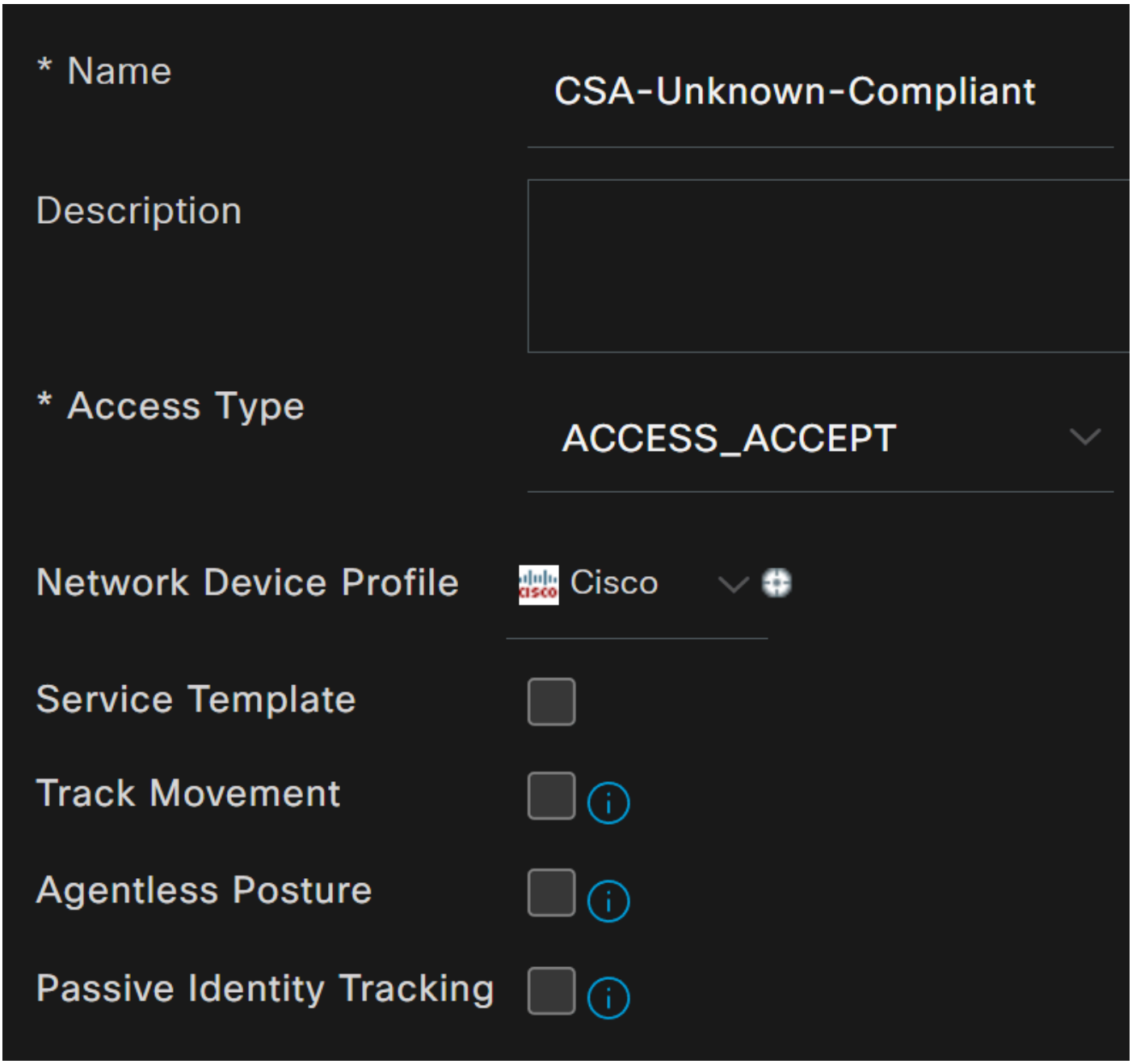


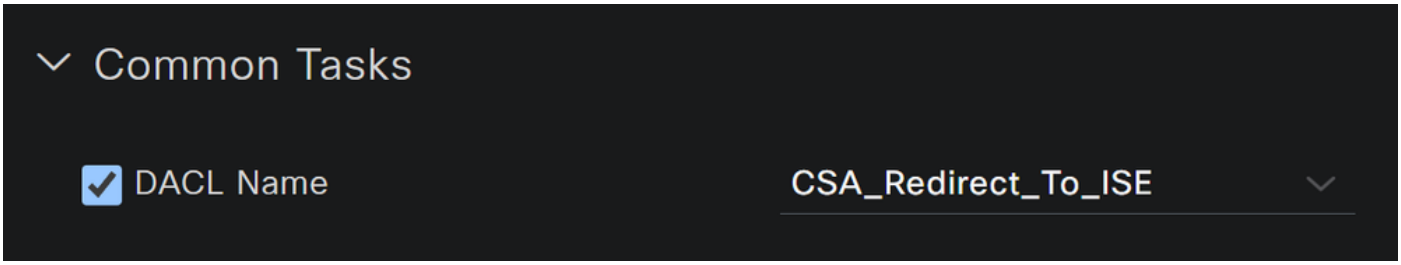
- **Name**: Créez un nom faisant référence au profil d'autorisation conforme
- Access Type: Choisir **ACCESS_ACCEPT**

- **Common Tasks**
  - **DACL NAME**: Sélectionnez la DACL configurée à l'étape DACL conforme

Cliquez sur **Save** et créez le Unknown Authorization Profile

- Cliquez sur **Work Centers > Policy Elements > Authorization Profiles**
- Cliquez sur **+Add**
- Créez le **Uknown Compliant Authorization Profile**



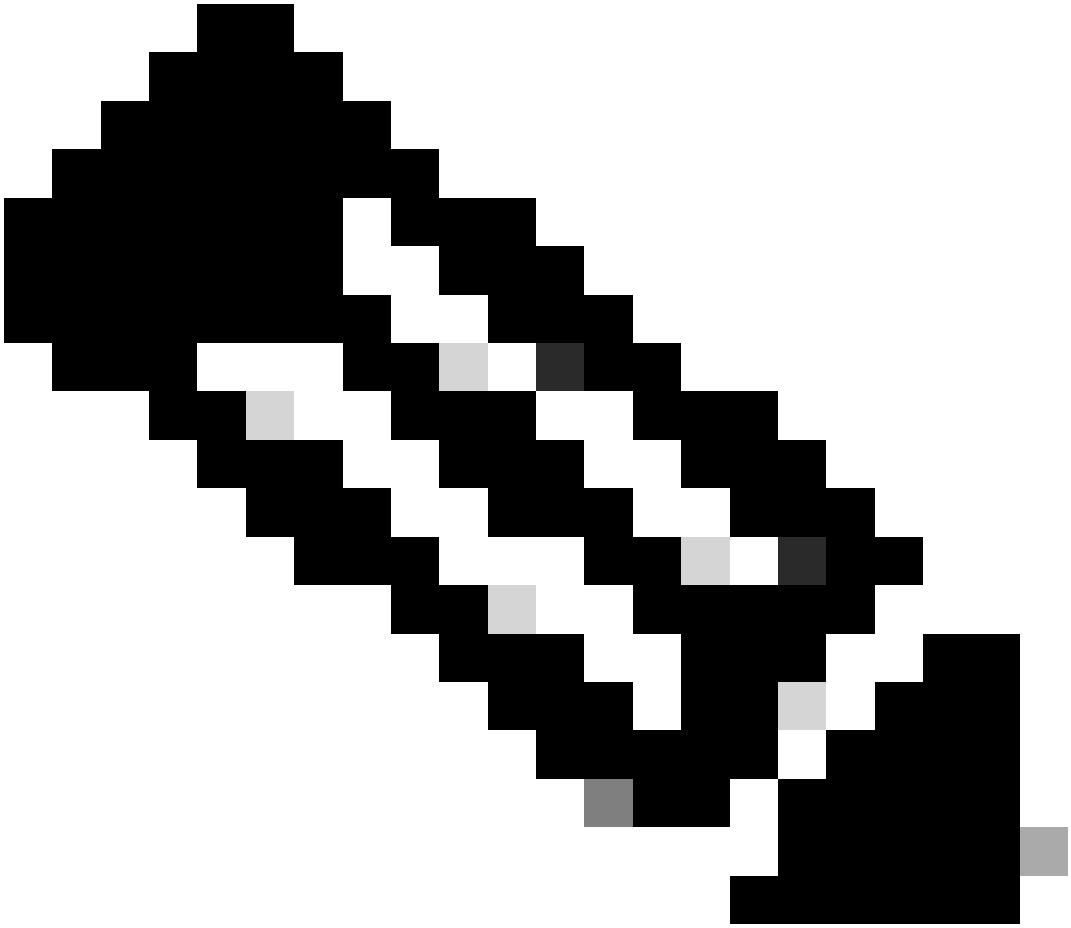


- **Name**: Créez un nom faisant référence au profil d'autorisation conforme inconnu
- Access Type: Choisir **ACCESS_ACCEPT**

- **Common Tasks**

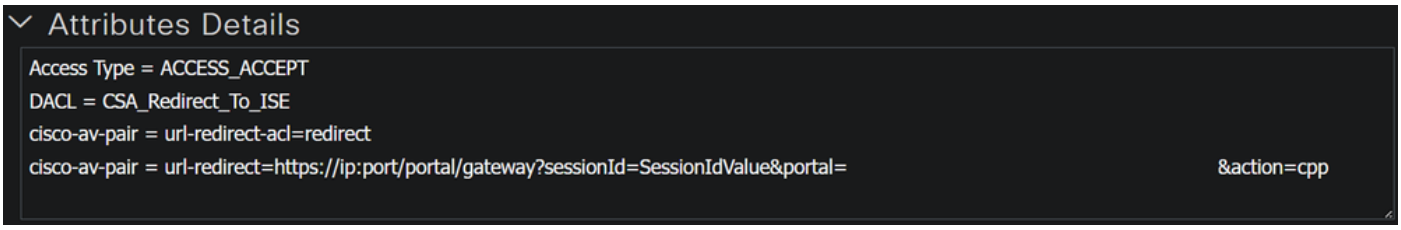
- **DACL NAME**: Choisissez la DACL configurée à l'étape DACL conforme inconnu
- **Web Redirection (CWA,MDM,NSP,CPP)**
  - Choisir **Client Provisioning (Posture)**
  - **ACL**: Doit être redirect
  - **Value**: choisissez le portail de mise en service par défaut ou, si vous en avez défini un autre, choisissez-le

---



Remarque : Le nom de la liste de contrôle d'accès de redirection sur l'accès sécurisé pour tous les déploiements est **redirect**.

Une fois que vous avez défini toutes ces valeurs, vous devez avoir quelque chose de similaire **SOUS**Attributes Details.



Cliquez **Save** sur ce bouton pour terminer la configuration et passer à l'étape suivante.

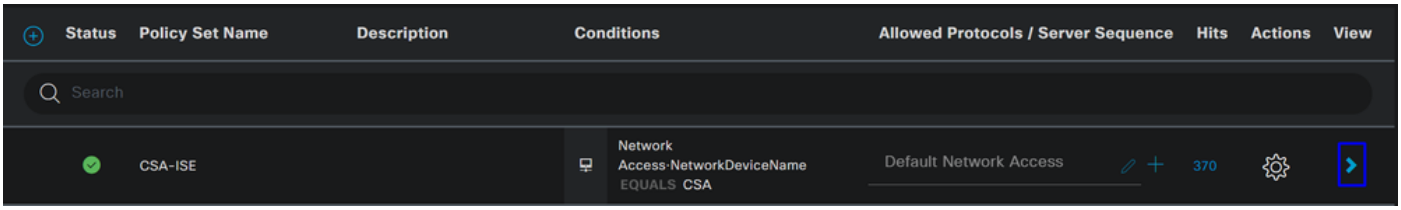
Configurer le jeu de stratégies de position

Ces trois stratégies que vous créez sont basées sur les profils d'autorisation que vous avez configurés ; pour **DenyAccess**, vous n'avez pas besoin d'en créer un autre.

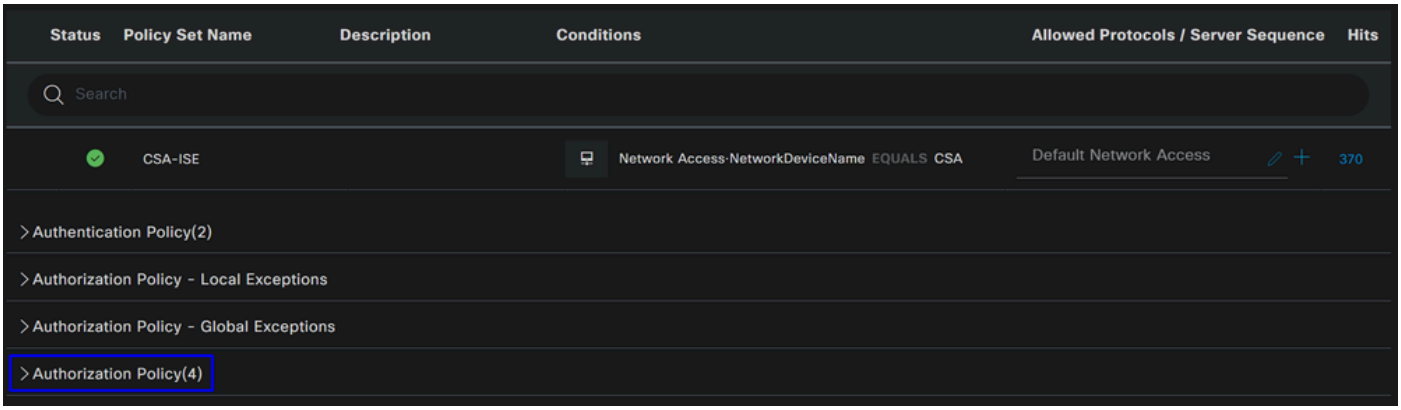
Ensemble de stratégies - Autorisation	Profil d'autorisation
Conforme	Profil d'autorisation - Conforme
Conformité inconnue	Profil d'autorisation - Inconnu Conforme
Non Conforme	RefuserAccès

Accédez à votre tableau de bord ISE

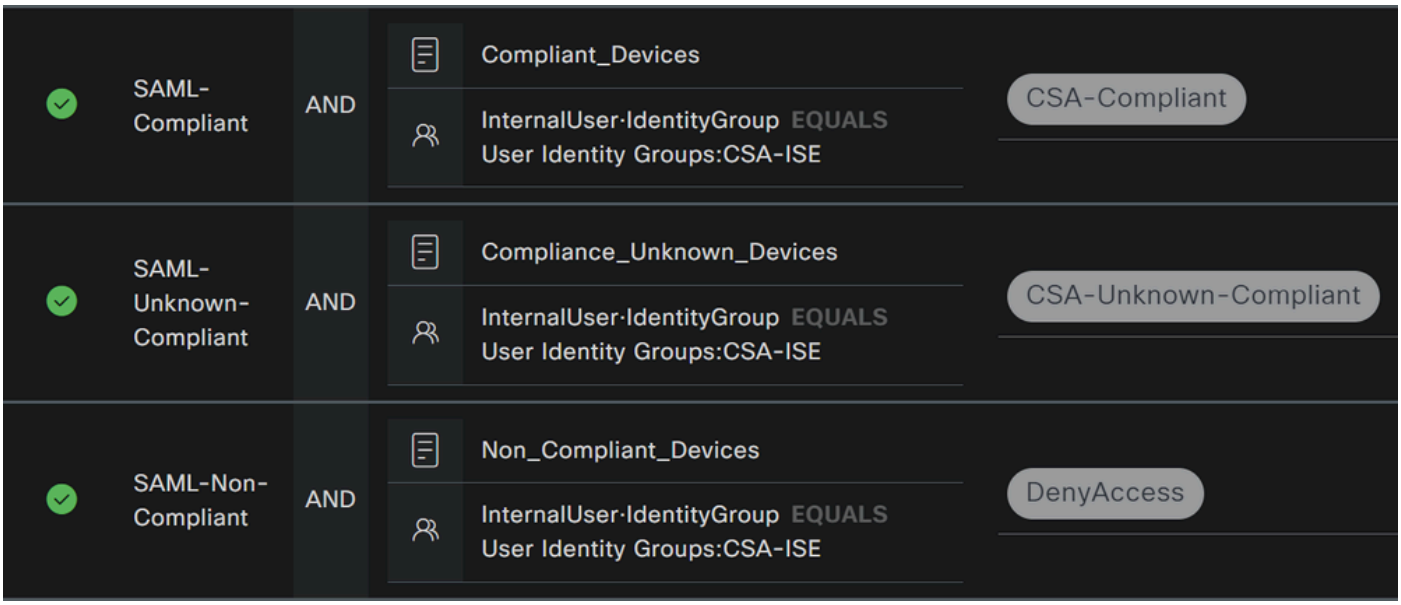
- Cliquez sur **Work Center** > **Policy Sets**
- Cliquez sur> pour accéder à la stratégie que vous avez créée



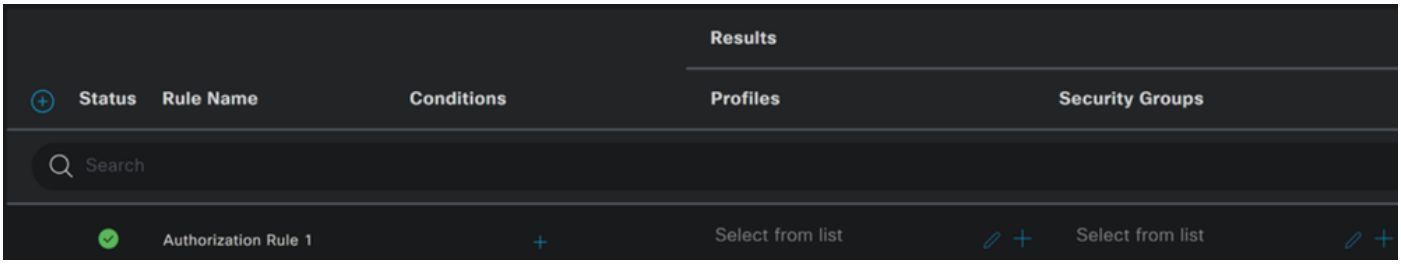
- Cliquez sur le bouton Authorization Policy



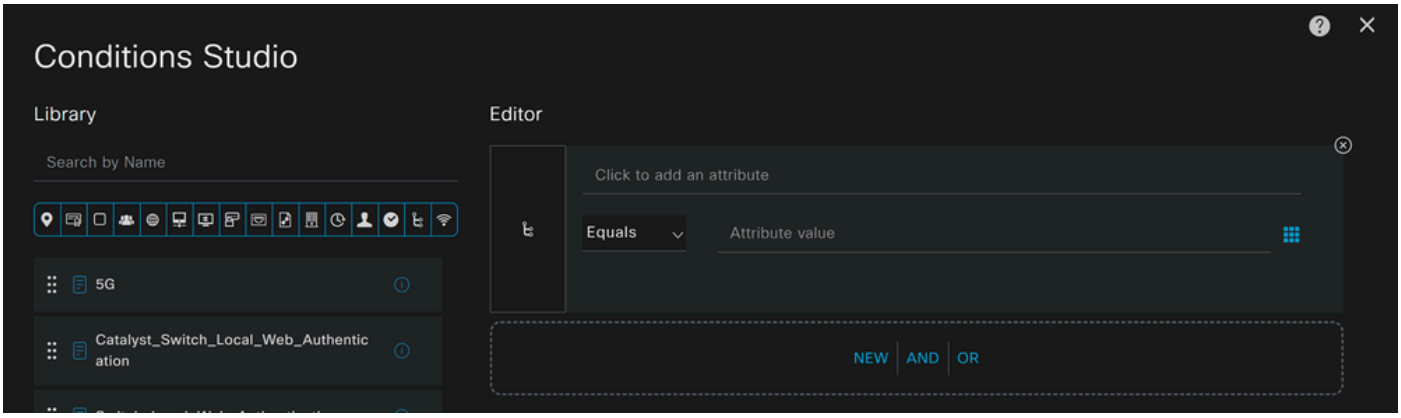
- Créez les trois stratégies suivantes dans l'ordre suivant :



- Cliquez sur + pour définir la **CSA-Compliance** politique :

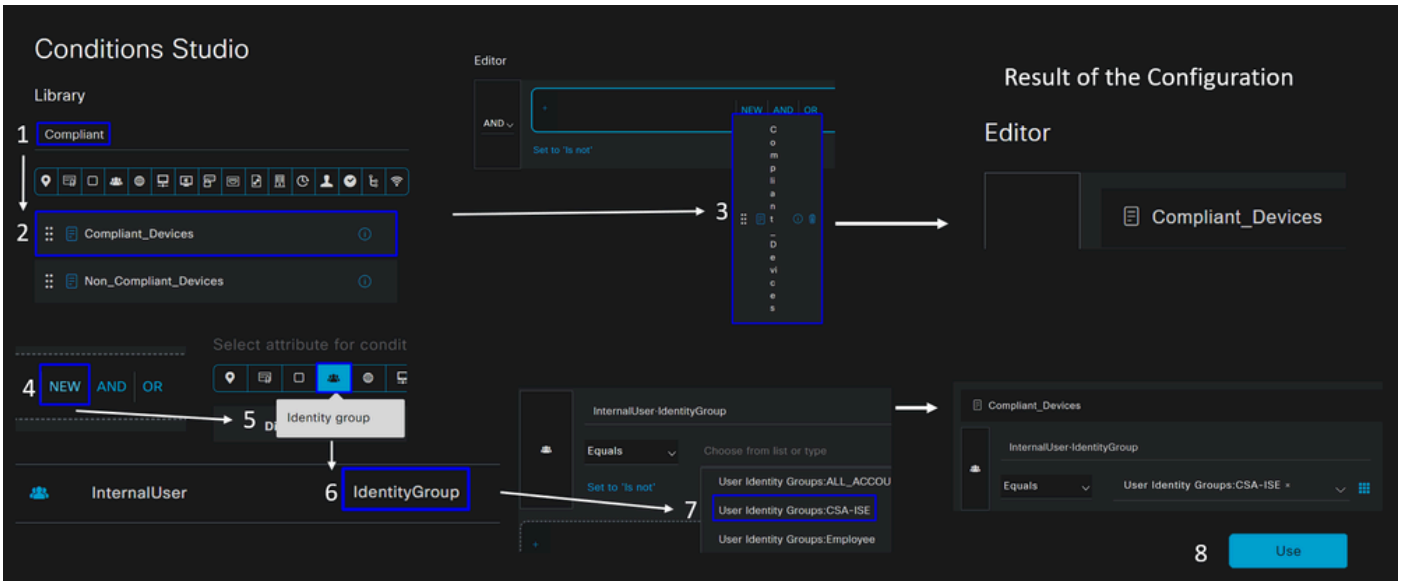


- Pour l'étape suivante, modifiez lesRule Name,Conditionset Profiles
- Lors de la définition du paramètre **Name** configure a name to **CSA-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :

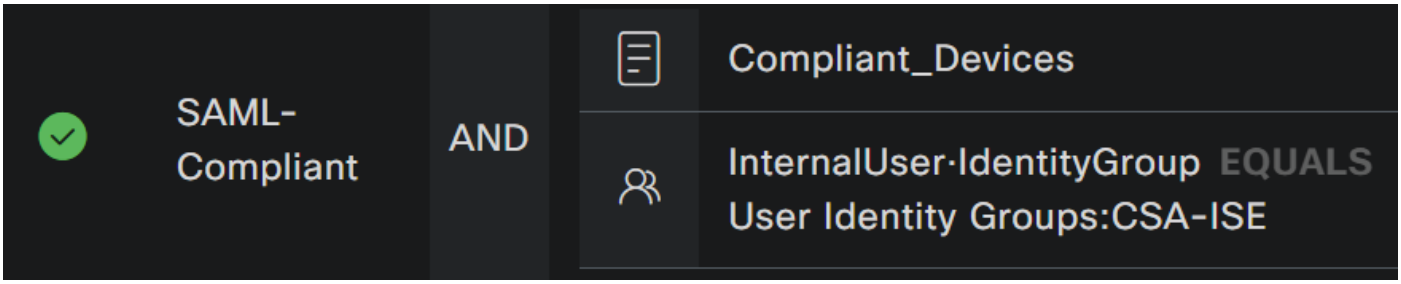


1. Pour créer la condition, recherchez **compliant**
2. Vous devez avoir affiché Compliant_Devices
3. Glisser-déplacer sous le **Editor**
4. Cliquez sous laEditordans **New**
5. Cliquez sur l'**Identity Group**icône

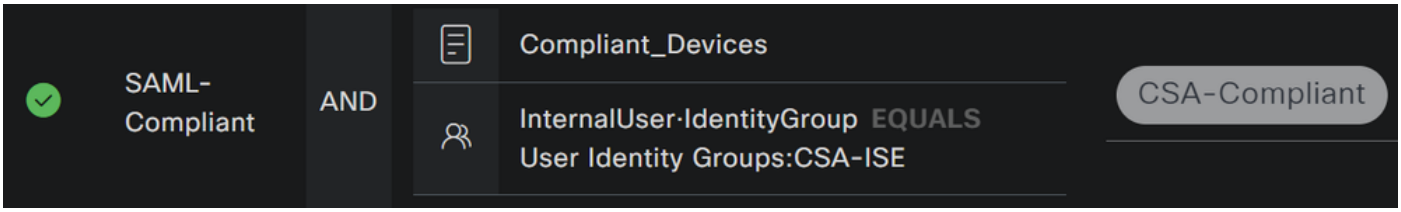
6. Choisir **Internal User Identity Group**
7. Sous **Equals**, choisissez le **User Identity Group** que vous souhaitez faire correspondre
8. Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante

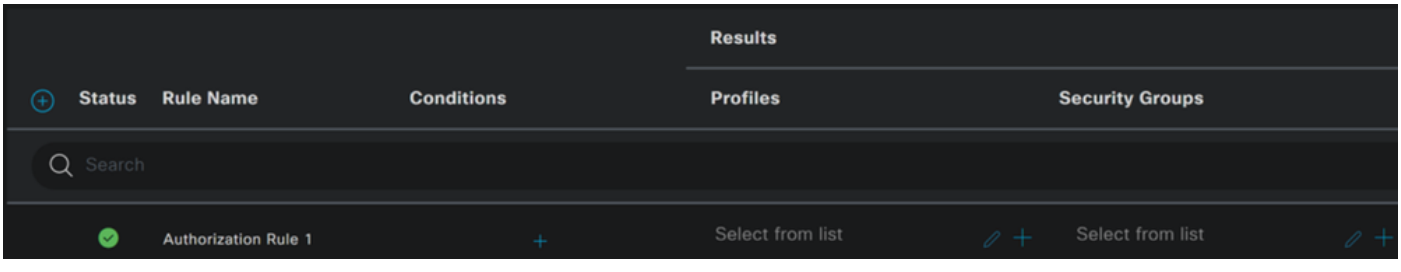


- Sous, **Profile** cliquez sur le bouton déroulant et sélectionnez le profil d'autorisation de réclamation configuré à l'étape Profil d'autorisation de conformité

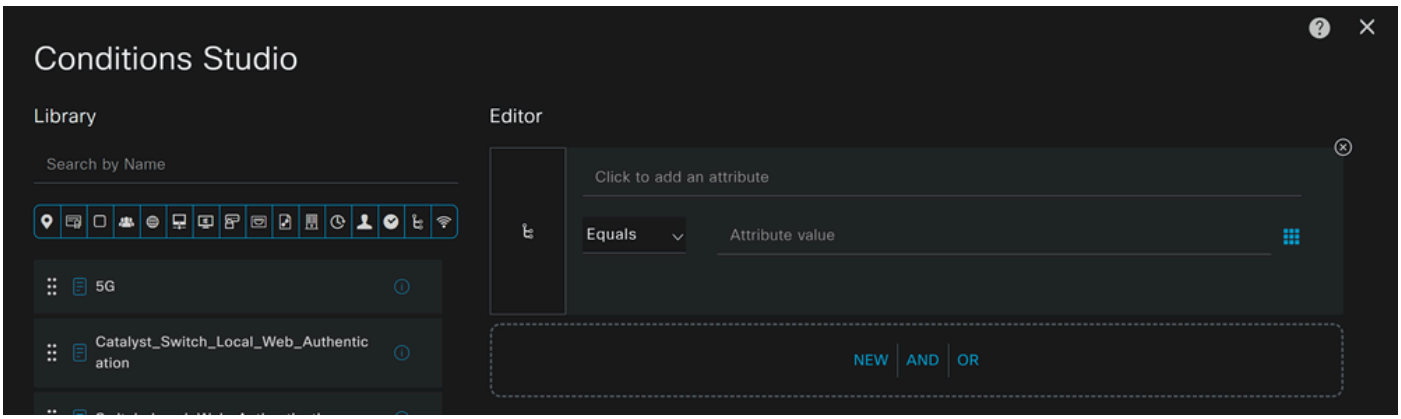


Vous venez de configurer le **Compliance Policy Set**.

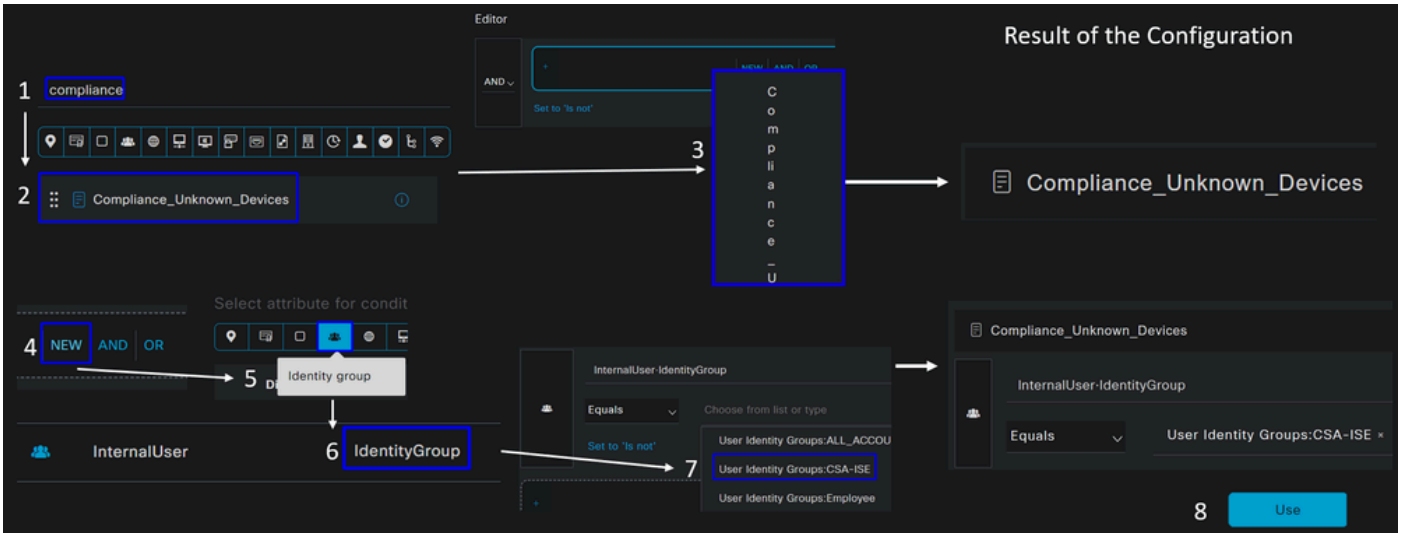
- Cliquez sur + pour définir la **CSA-Unknown-Compliance** politique :



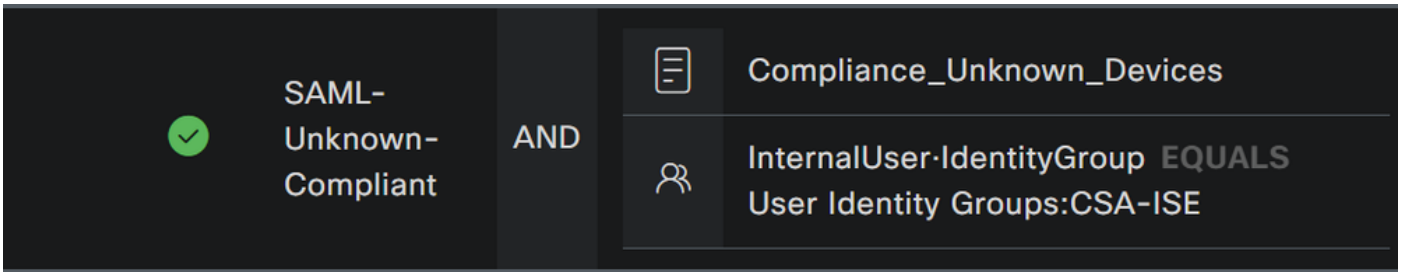
- Pour l'étape suivante, modifiez lesRule Name,Conditionset Profiles
- Lors de la définition du paramètre **Name** configure a name to **CSA-Unknown-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :



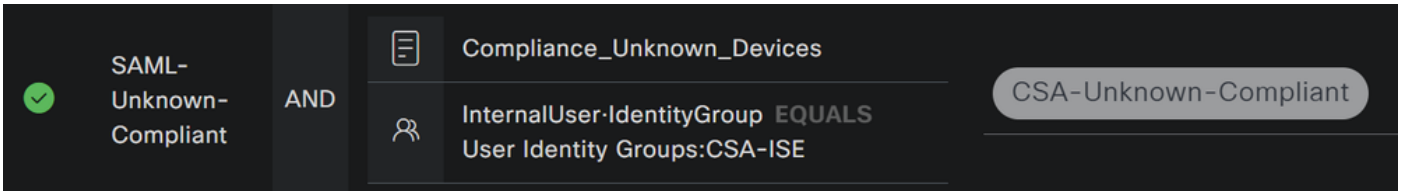
1. Pour créer la condition, recherchez **compliance**
2. Vous devez avoir affiché Compliant_Unknown_Devices
3. Glisser-déplacer sous le **Editor**
4. Cliquez sous laEditordans **New**
5. Cliquez sur l'**Identity Group**icône
6. Choisir **Internal User Identity Group**
7. Sous **Equals**, choisissez le **User Identity Group** que vous souhaitez faire correspondre
8. Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante

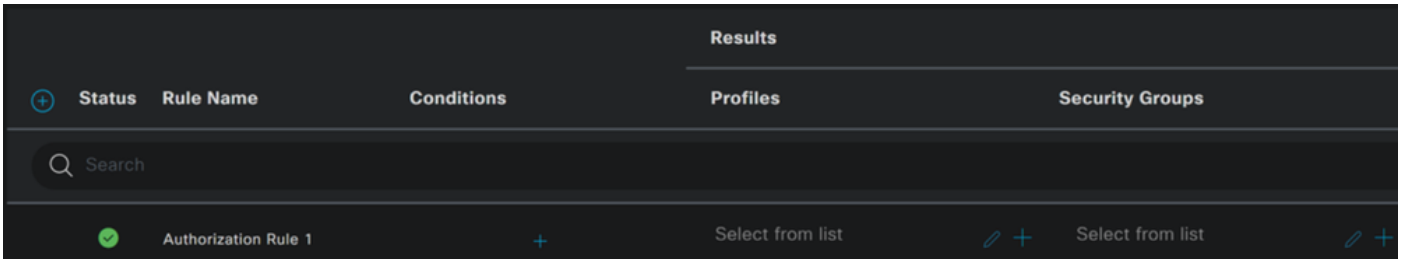


- Sous, **Profile** cliquez sous le bouton déroulant et sélectionnez le profil d'autorisation de réclamation configuré à l'étape, [Profil d'autorisation de conformité inconnu]

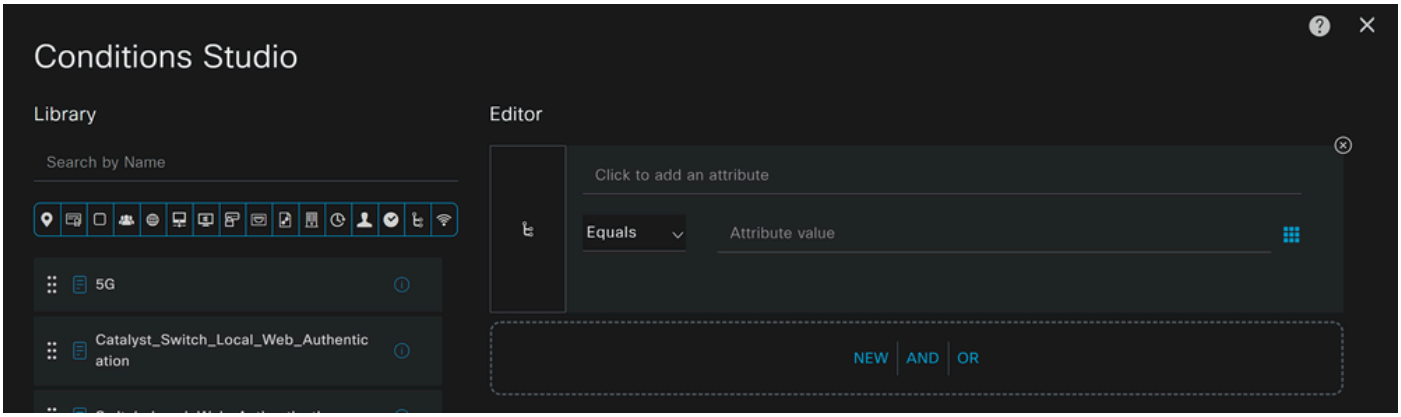


Vous venez de configurer le **Unknown Compliance Policy Set**.

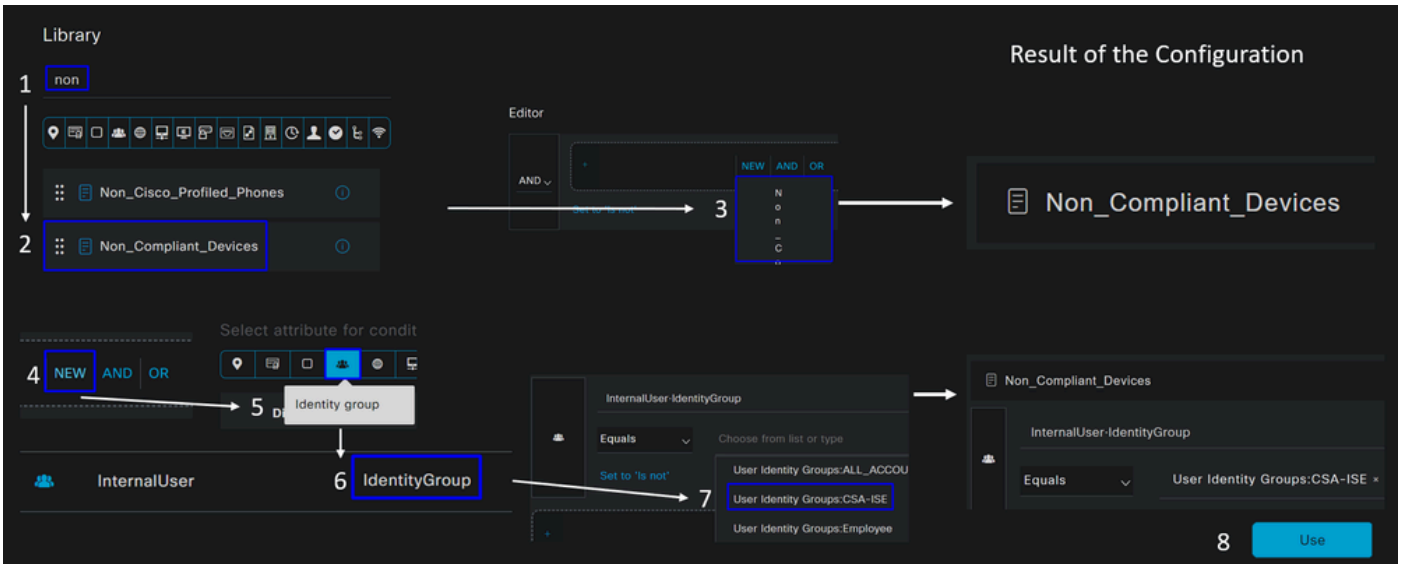
- Cliquez sur + pour définir la **CSA- Non-Compliant** politique :



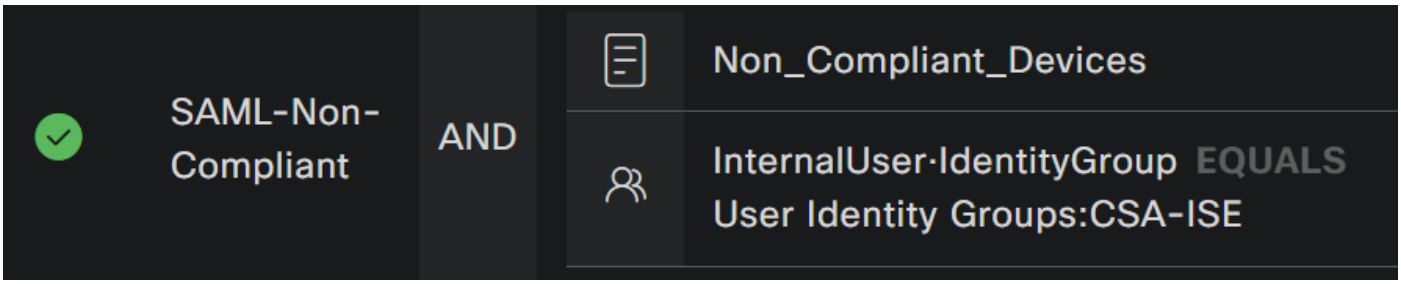
- Pour l'étape suivante, modifiez lesRule Name,Conditionset Profiles
- Lors de la définition du paramètre **Name** configure a name to **CSA-Non-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :



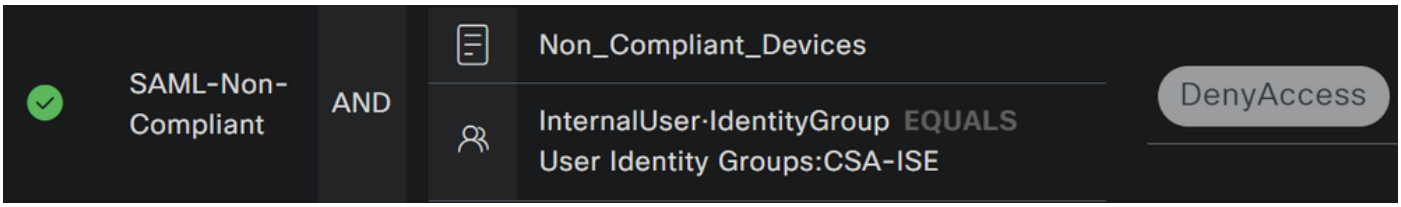
1. Pour créer la condition, recherchez **non**
2. Vous devez avoir affiché Non_Compliant_Devices
3. Glisser-déplacer sous le **Editor**
4. Cliquez sous laEditordans **New**
5. Cliquez sur l'**Identity Group**icône
6. Choisir **Internal User Identity Group**
7. Sous **Equals**, choisissez le **User Identity Group** que vous souhaitez faire correspondre
8. Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante



- Sous **Profile** cliquez sur le bouton déroulant et sélectionnez le profil d'autorisation de réclamation **DenyAccess**



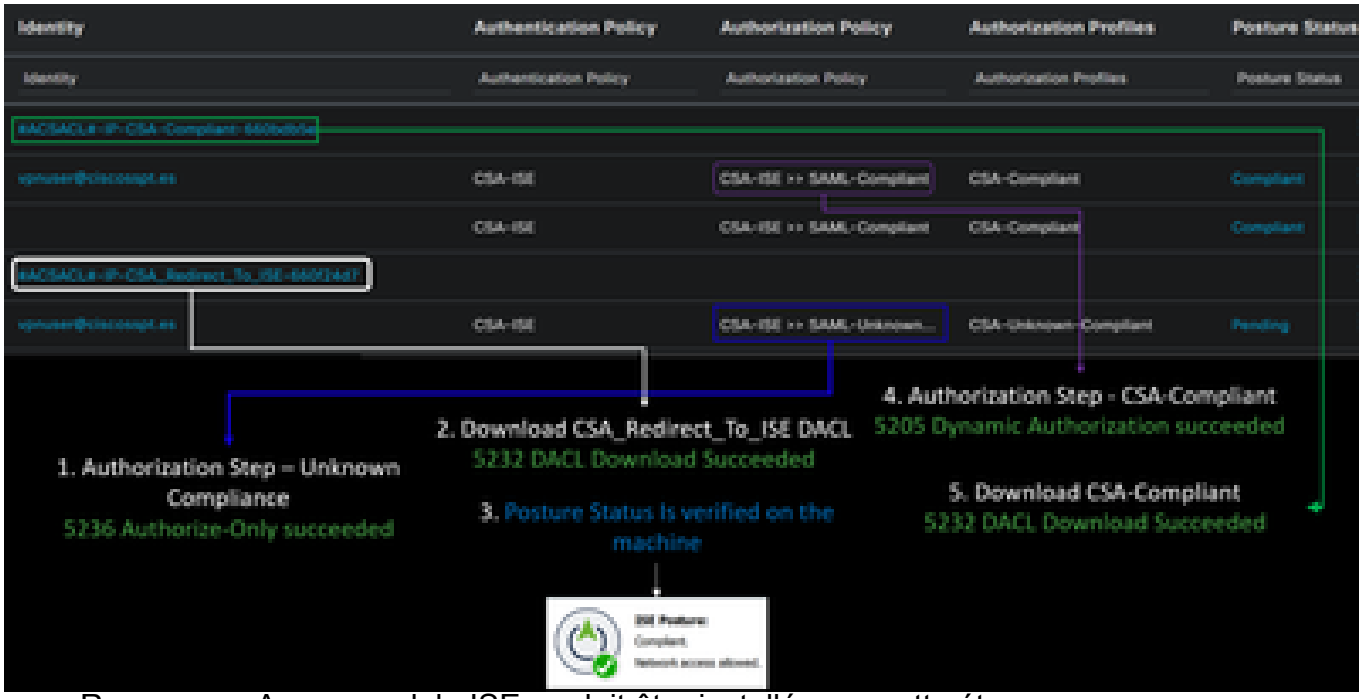
Une fois que vous avez terminé la configuration des trois profils, vous êtes prêt à tester votre intégration avec posture.

Vérifier

Validation de posture

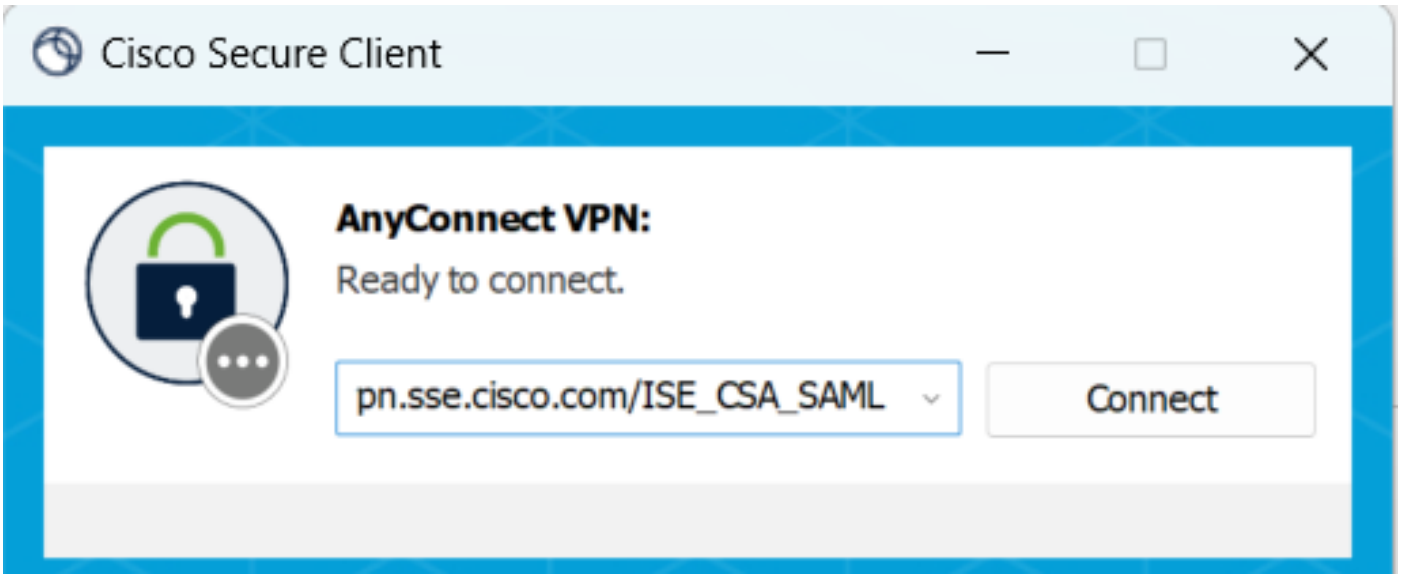
Connexion sur l'ordinateur

Connectez-vous à votre domaine FQDN RA-VPN fourni sur Secure Access via Secure Client.

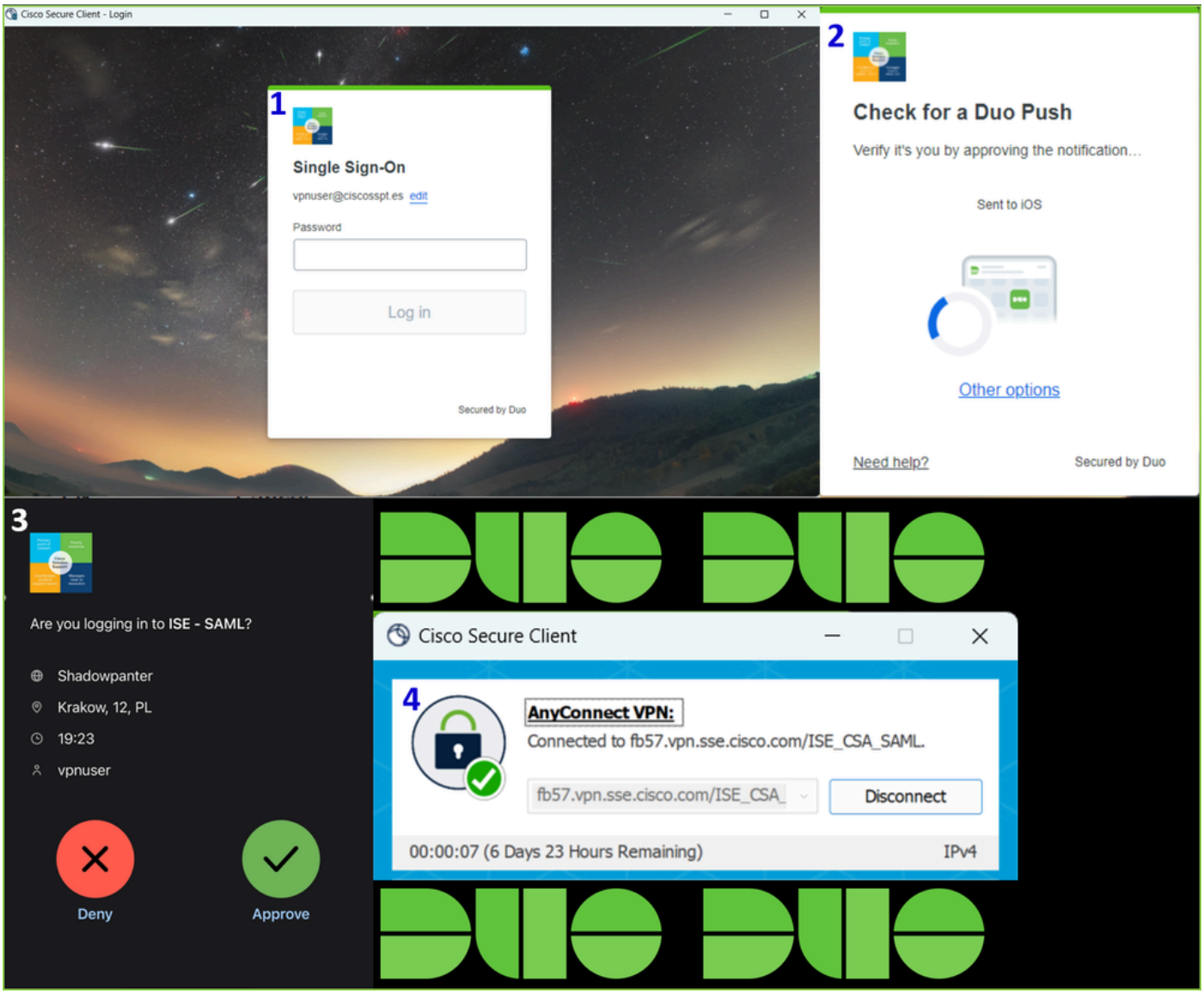


Remarque : Aucun module ISE ne doit être installé pour cette étape.

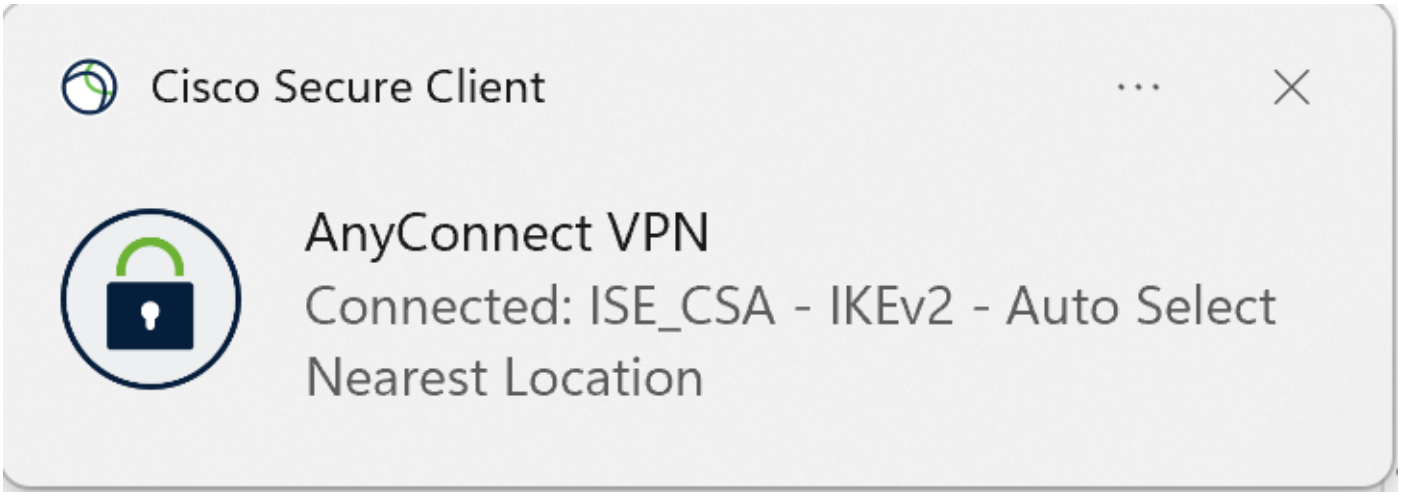
1. Connectez-vous à l'aide du client sécurisé.

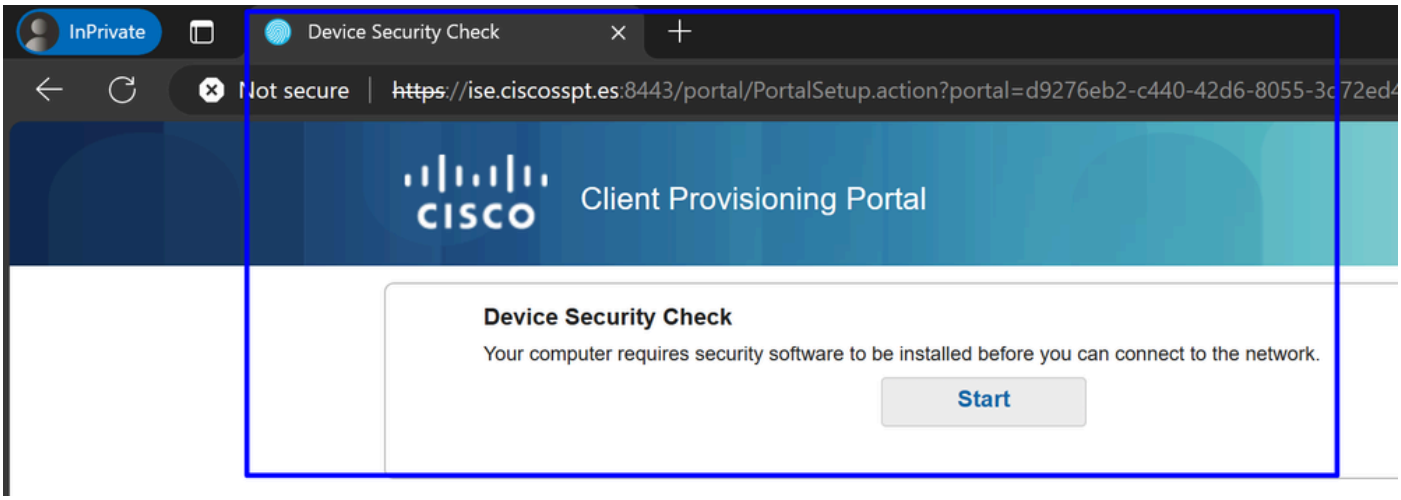


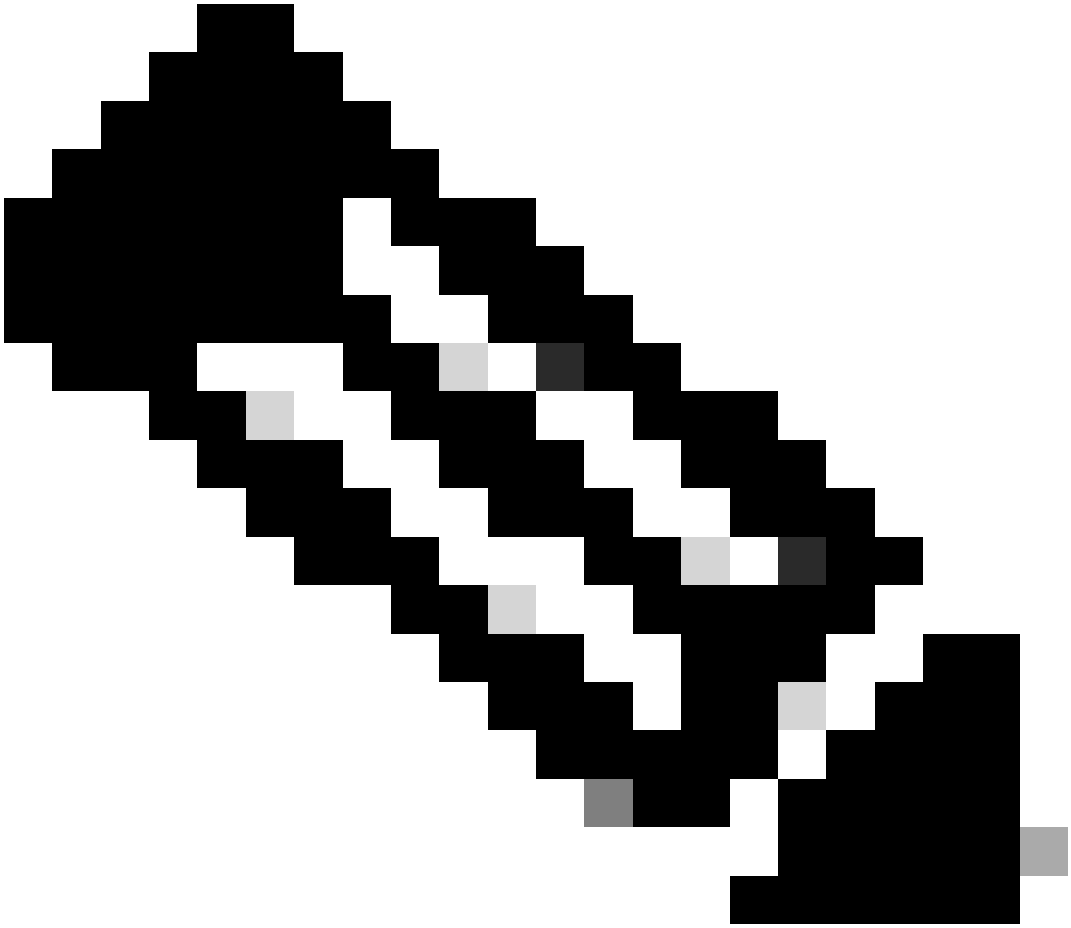
2. Fournissez les informations d'identification pour l'authentification via Duo.



3. À ce stade, vous vous connectez au VPN, et la plupart du temps, vous êtes probablement redirigé vers ISE ; si ce n'est pas le cas, essayez d'accéder à **http:1.1.1.1**.



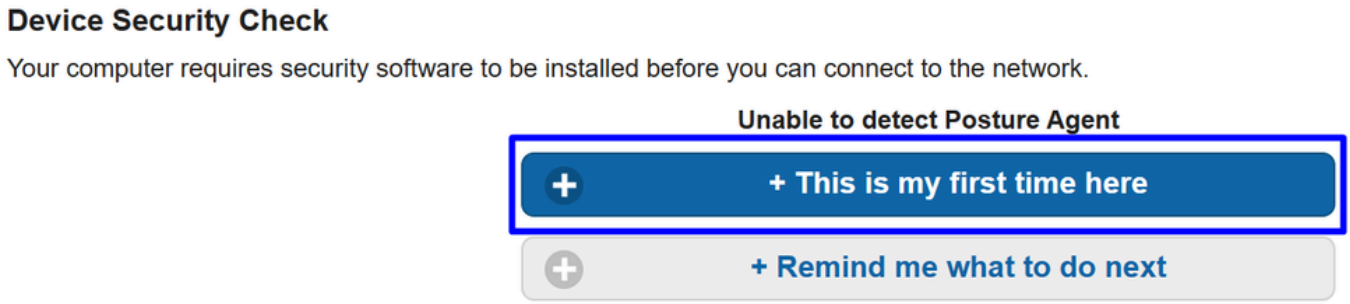




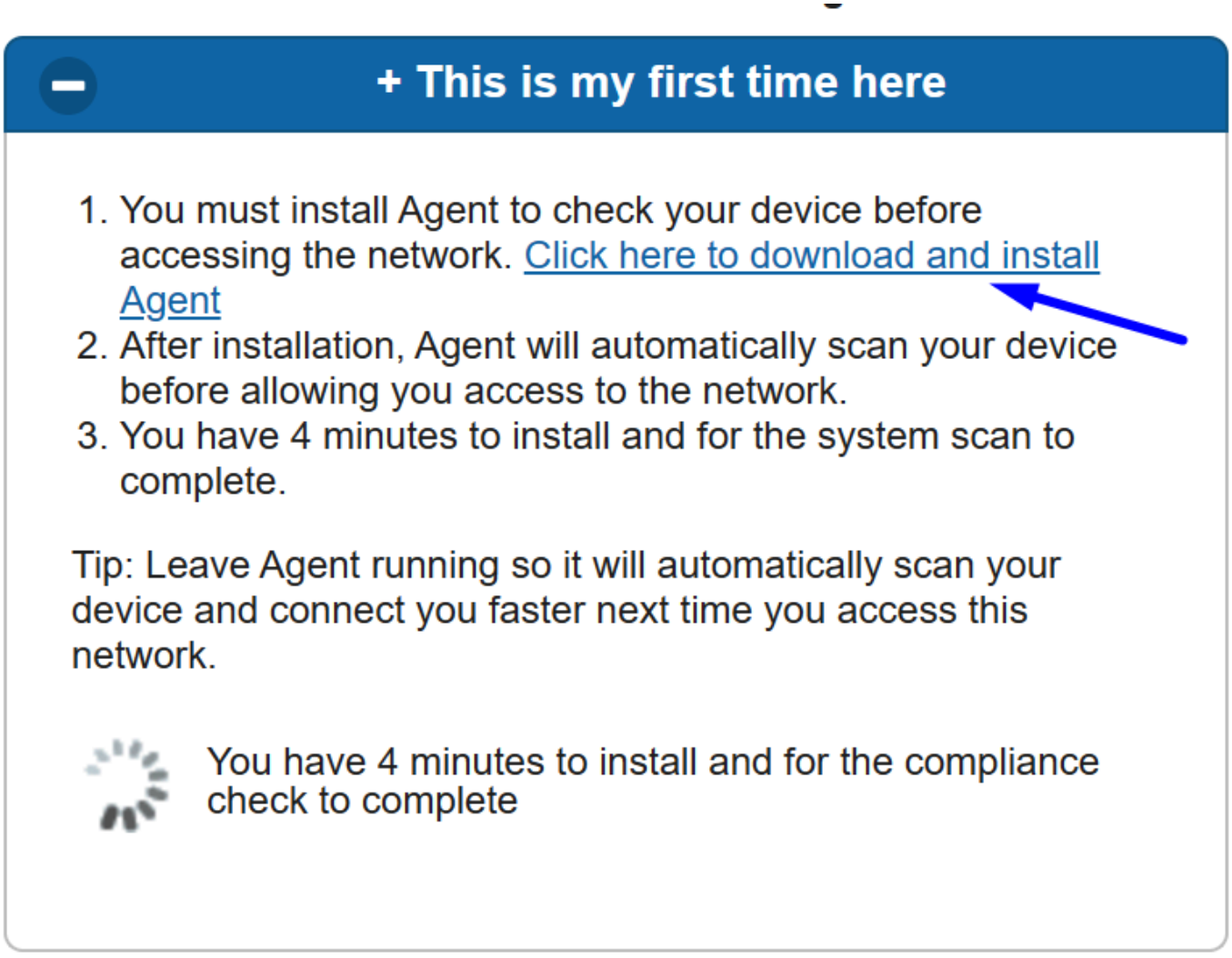
Remarque : À ce stade, vous tombez sous l'autorisation - ensemble de stratégies CSA-Unknown-Compliance parce que vous n'avez pas installé l'agent de posture ISE sur la machine et vous êtes redirigé vers le portail d'approvisionnement ISE pour installer l'agent.

4. Cliquez sur Démarrer pour poursuivre le provisionnement de l'agent.

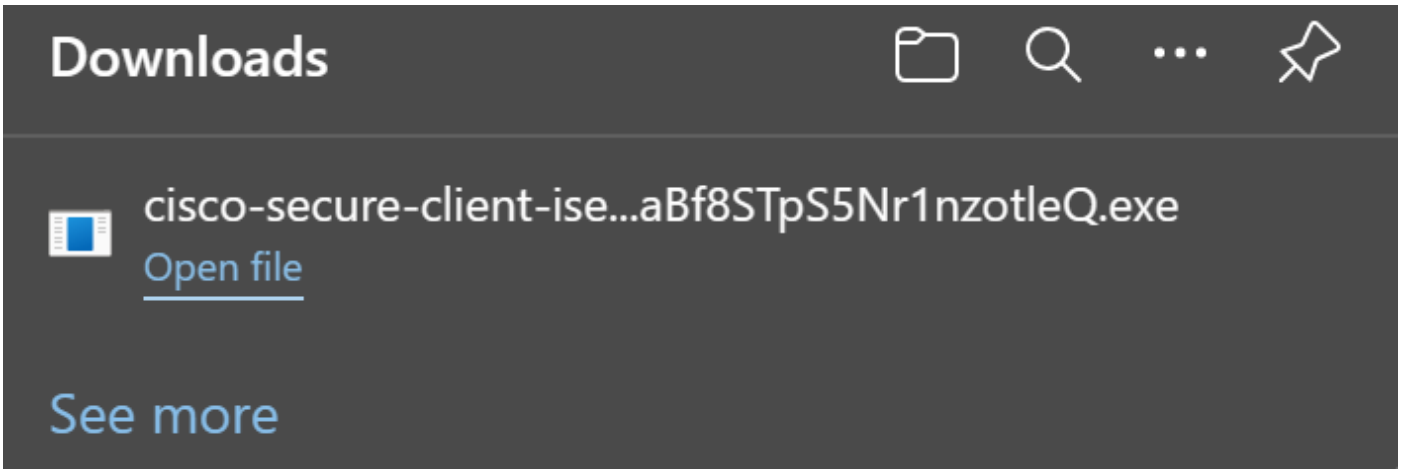
5. Cliquez sur **+ This is my first time here.**

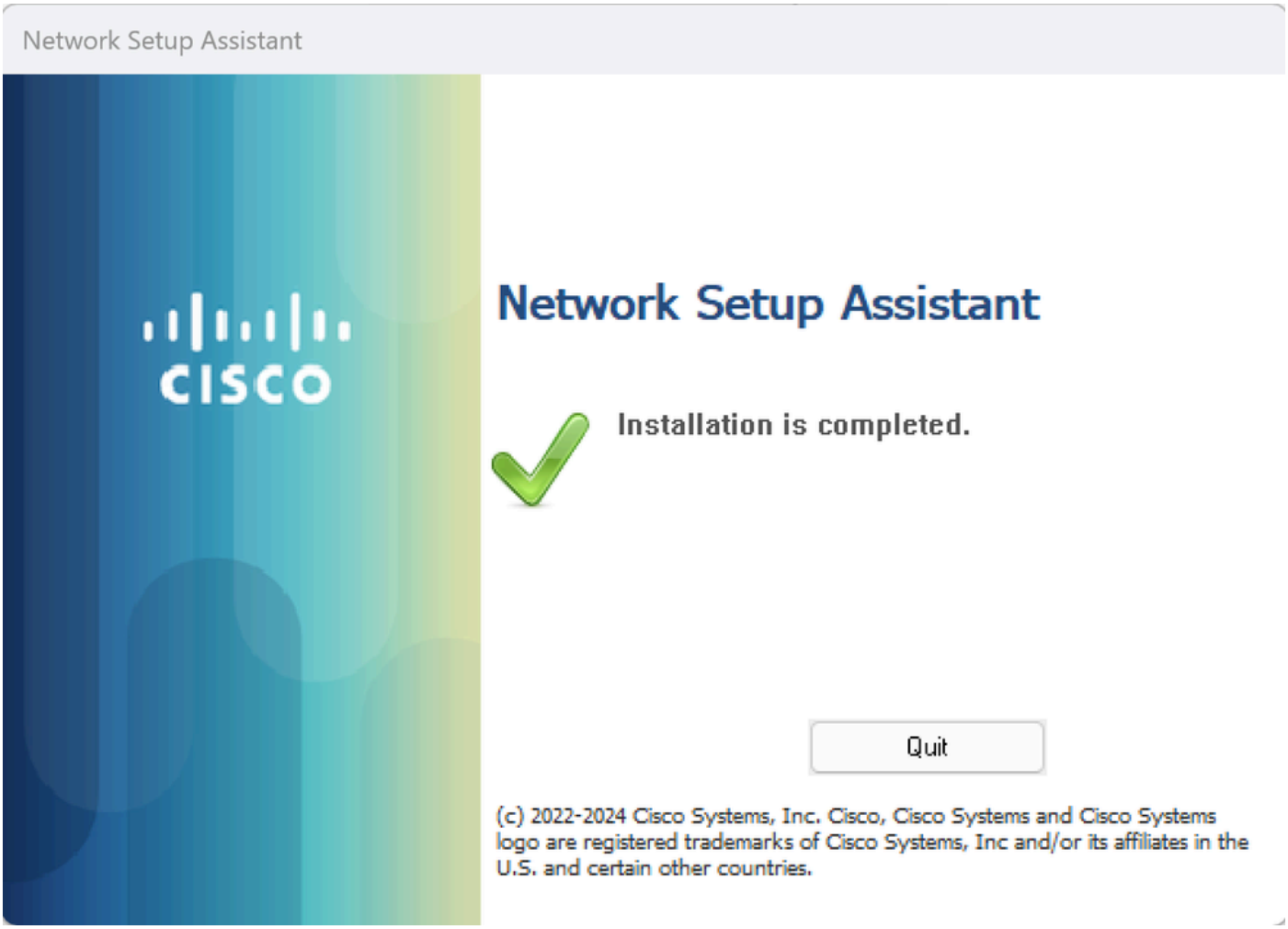


6. Cliquez sur **Click here to download and install agent**

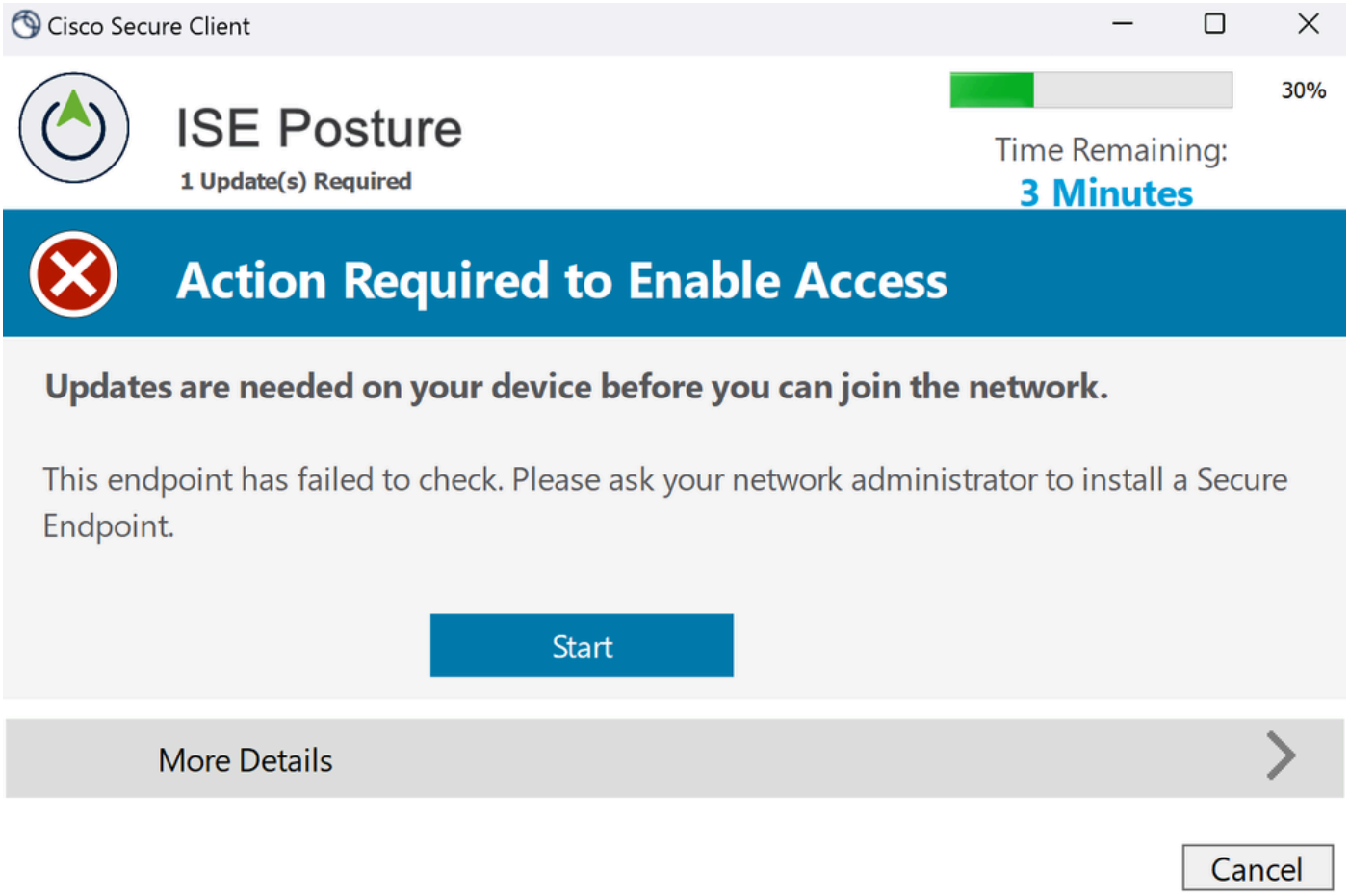


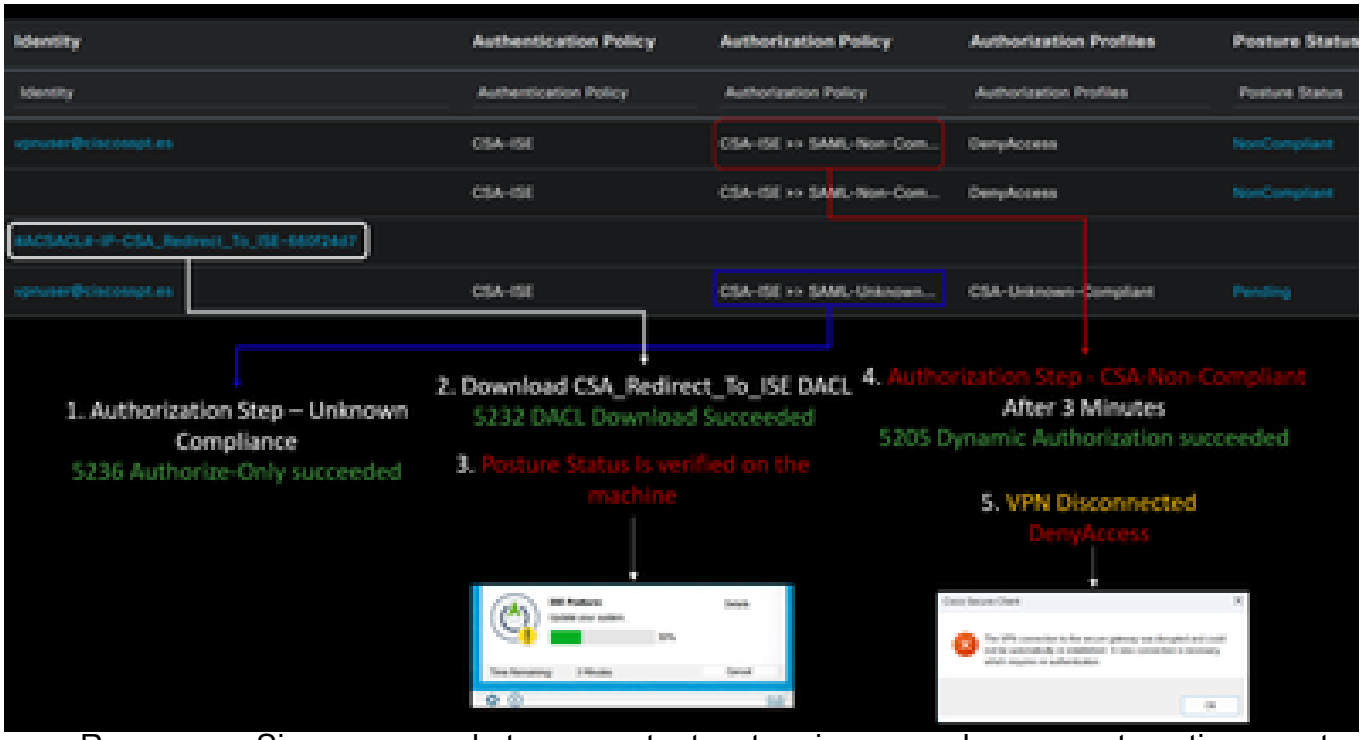
7. Installer l'agent





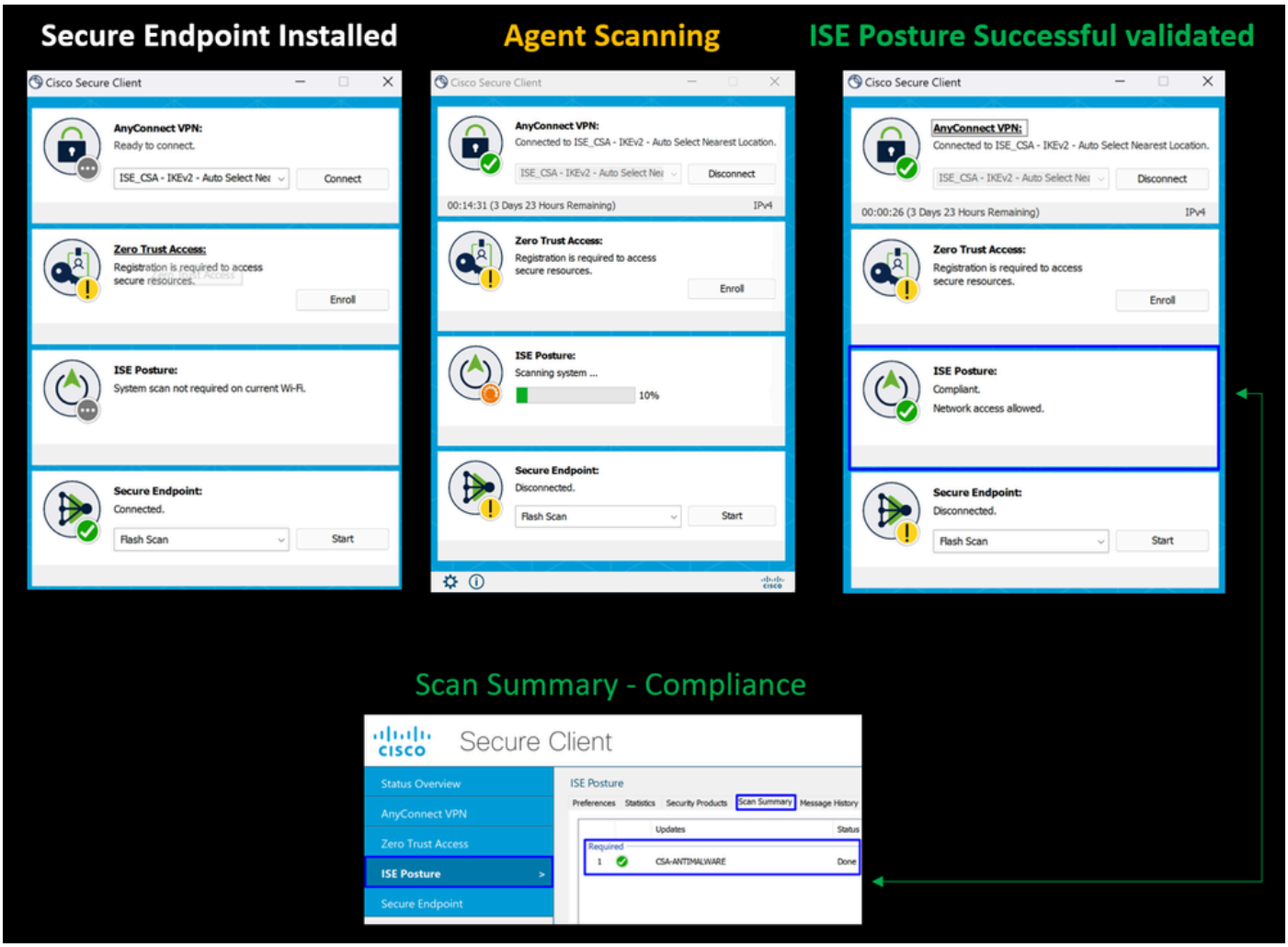
8. Une fois l'agent installé, la posture ISE commence à vérifier la posture actuelle des machines. Si les conditions de la stratégie ne sont pas remplies, une fenêtre contextuelle apparaît pour vous guider vers la conformité.



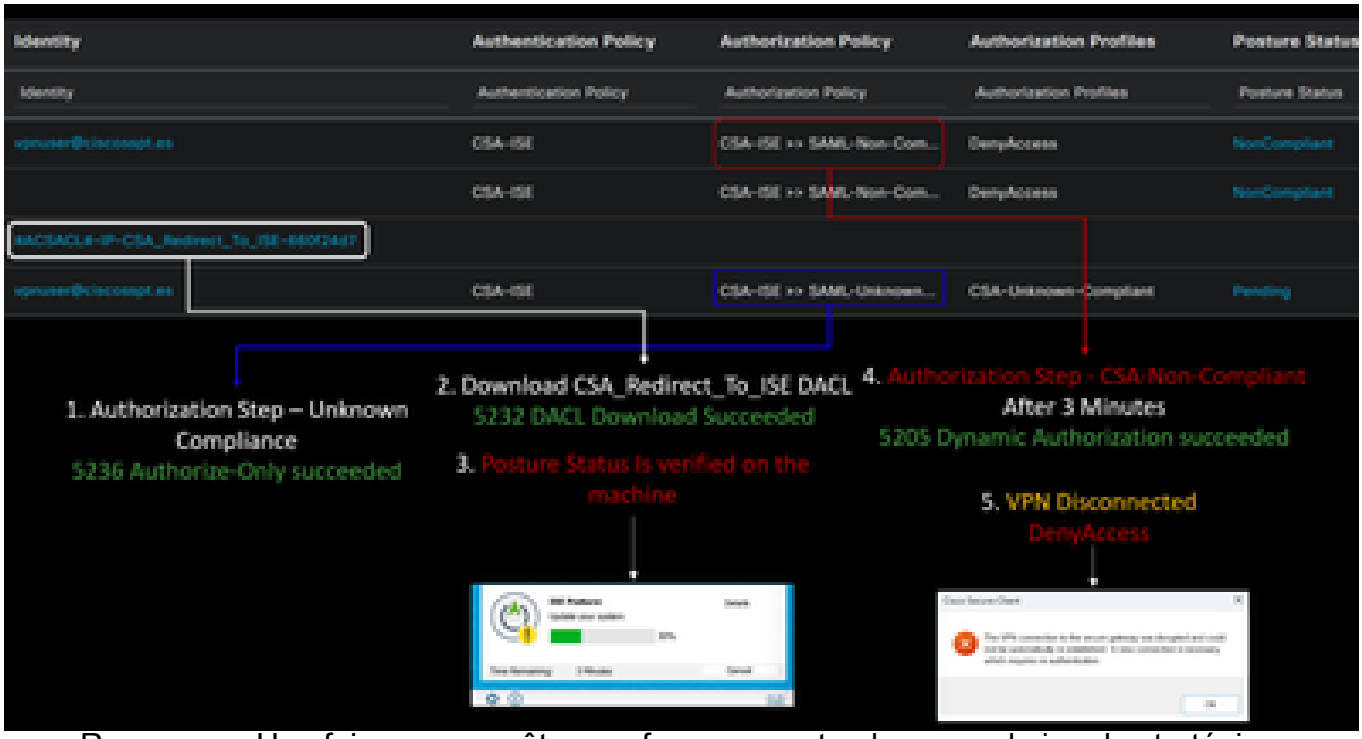


Remarque : Si vous Cancel ou le temps restant se termine, vous devenez automatiquement non conforme, tombez sous le jeu de stratégies d'autorisation CSA-Non-Compliance, et vous êtes immédiatement déconnecté du VPN.

9. Installez Secure Endpoint Agent et reconnectez-vous au VPN.



10. Une fois que l'agent a vérifié que la machine est conforme, votre position change pour être sur plainte et donner accès à toutes les ressources sur le réseau.

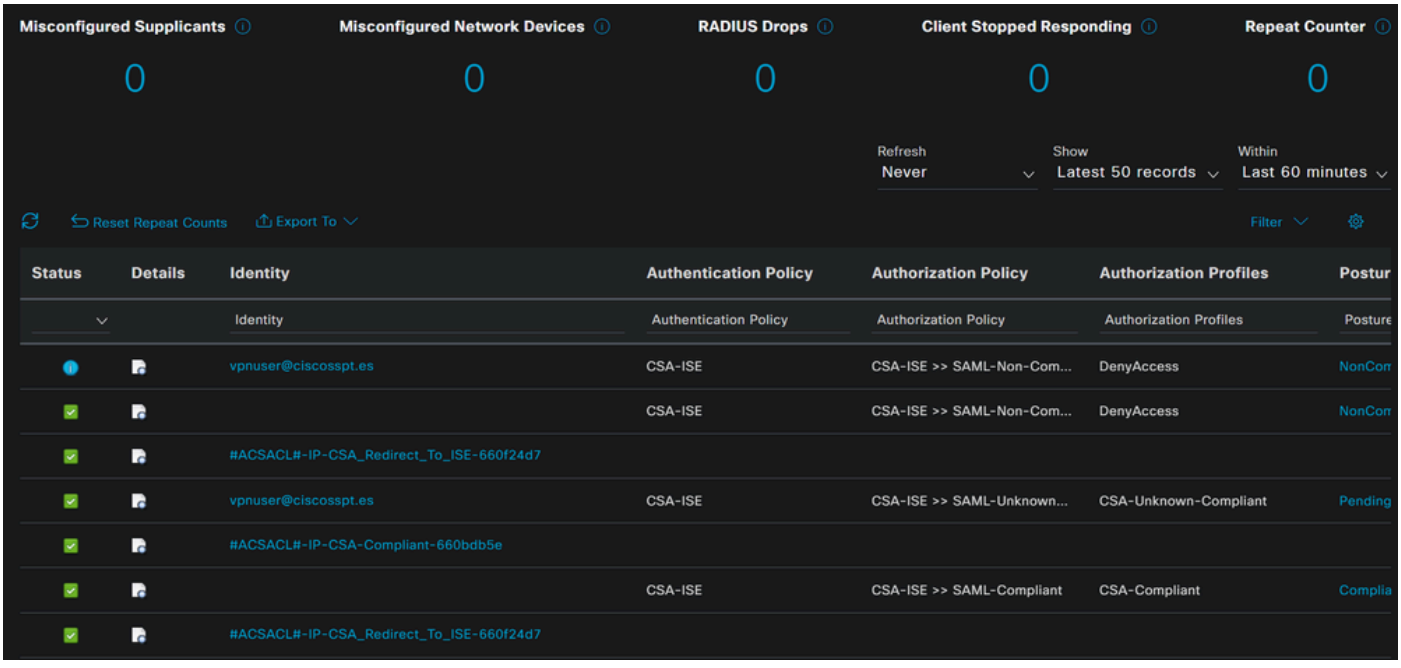


Remarque : Une fois que vous êtes conforme, vous tombez sous le jeu de stratégies d'autorisation CSA-Compliance, et vous avez immédiatement accès à toutes vos ressources réseau.

Vérification des journaux dans ISE

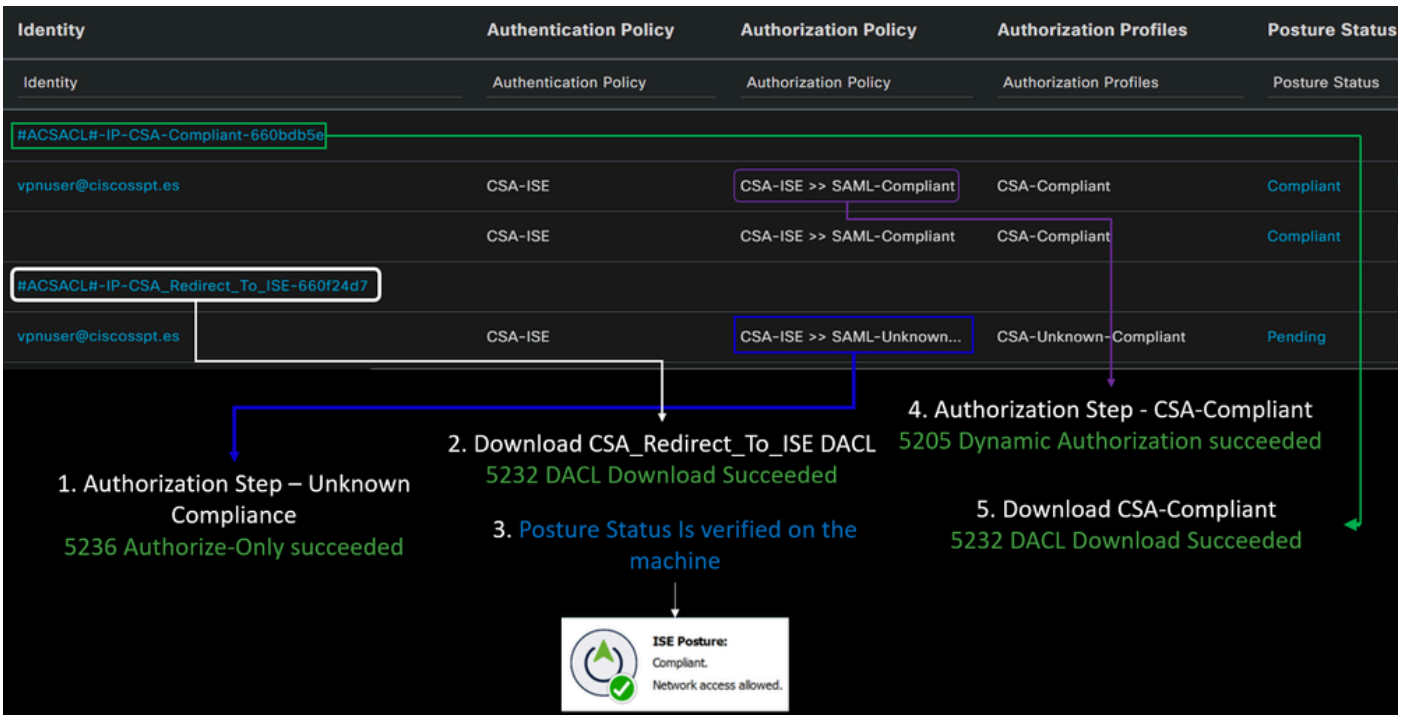
Pour vérifier le résultat de l'authentification d'un utilisateur, vous disposez de deux exemples de conformité et de non-conformité. Pour le consulter dans ISE, suivez les instructions suivantes :

- Accédez à votre tableau de bord ISE
- Cliquez sur Operations > Live Logs

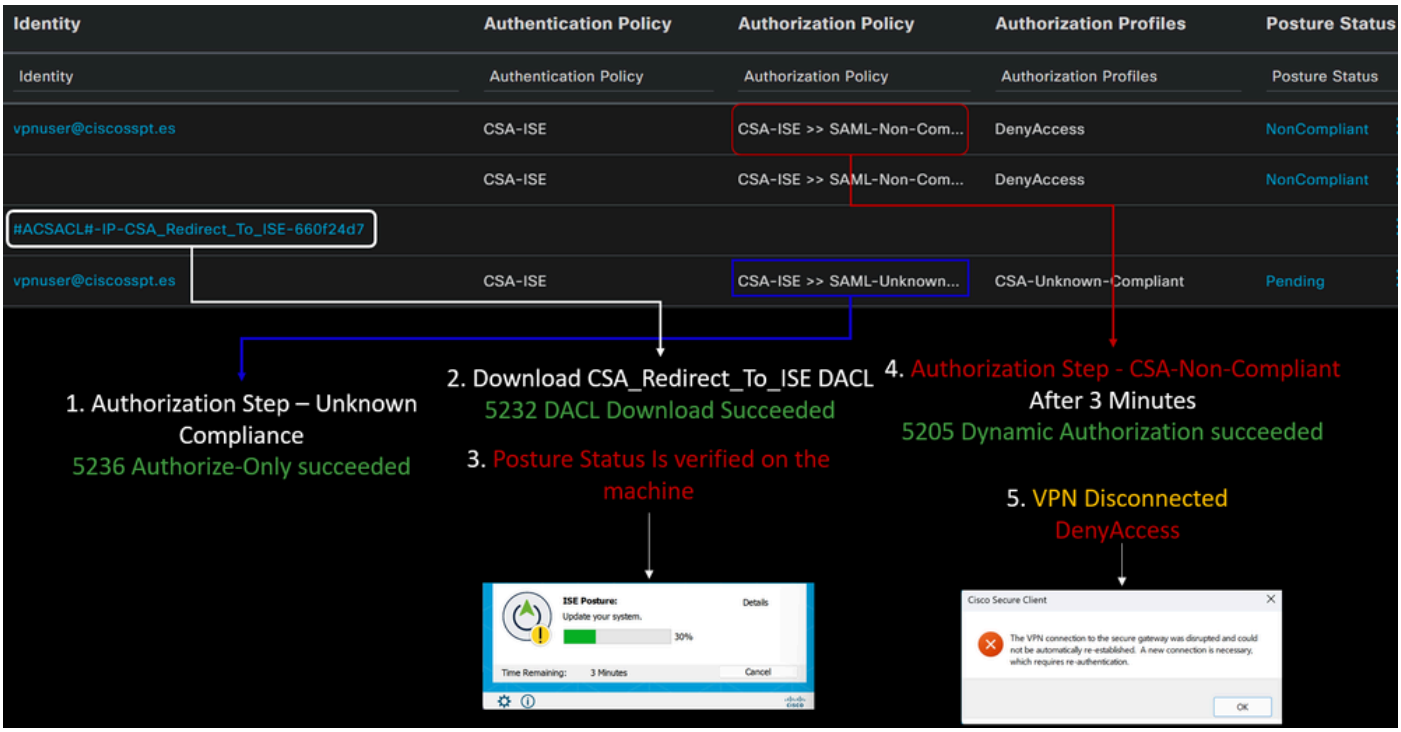


Le scénario suivant illustre l'affichage des événements de conformité et de non-conformité sous **Live Logs**:

Conformité



Non-conformité



Premiers pas vers l'accès sécurisé et l'intégration ISE

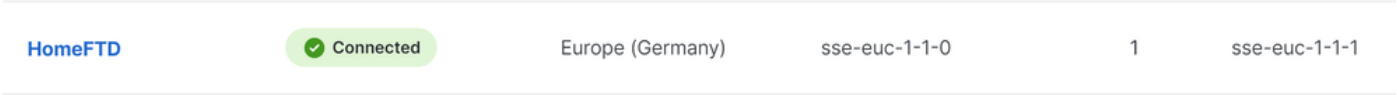
Dans l'exemple suivant, Cisco ISE se trouve sous le réseau 192.168.10.0/24 et la configuration

des réseaux accessibles via le tunnel doit être ajoutée sous la configuration du tunnel.

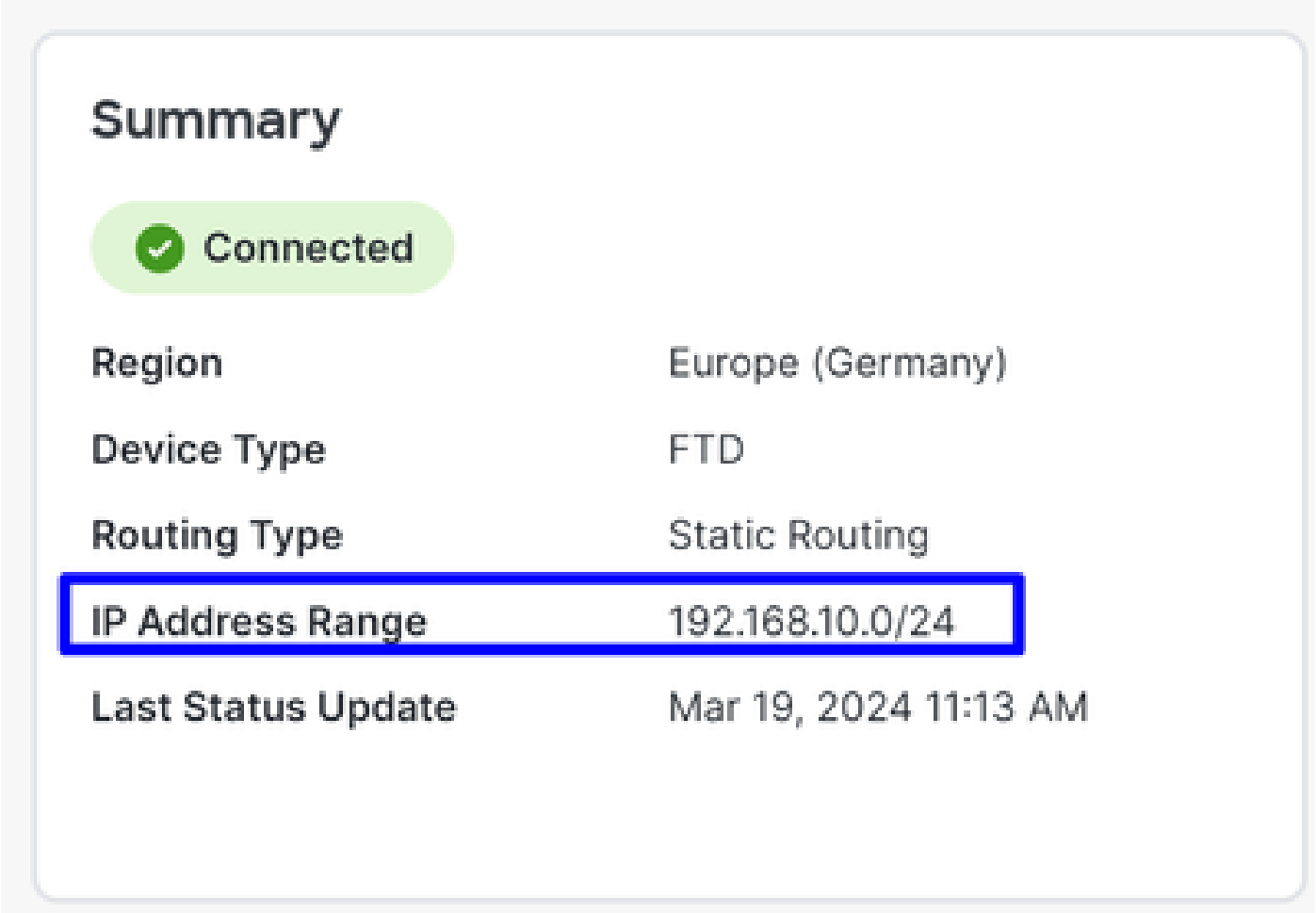
Step 1: Vérifiez votre configuration de tunnel :

Pour le vérifier, accédez à votre tableau de bord d'accès sécurisé.

- Cliquez sur **Connect** > **Network Connections**
- Cliquez sur **Network Tunnel Groups** > Votre tunnel



- Sous summary, vérifiez que le tunnel a configuré l'espace d'adressage où se trouve votre Cisco ISE :

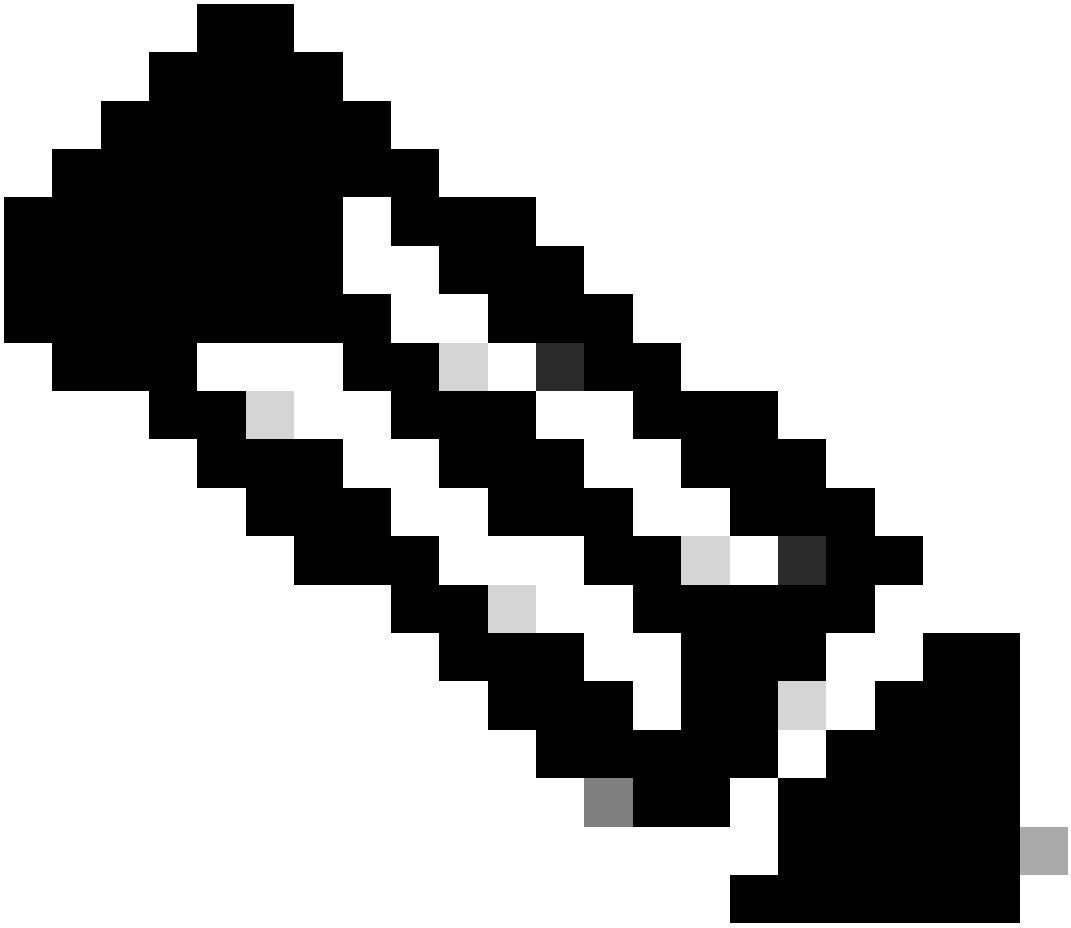


Step 2: Autorisez le trafic sur votre pare-feu.

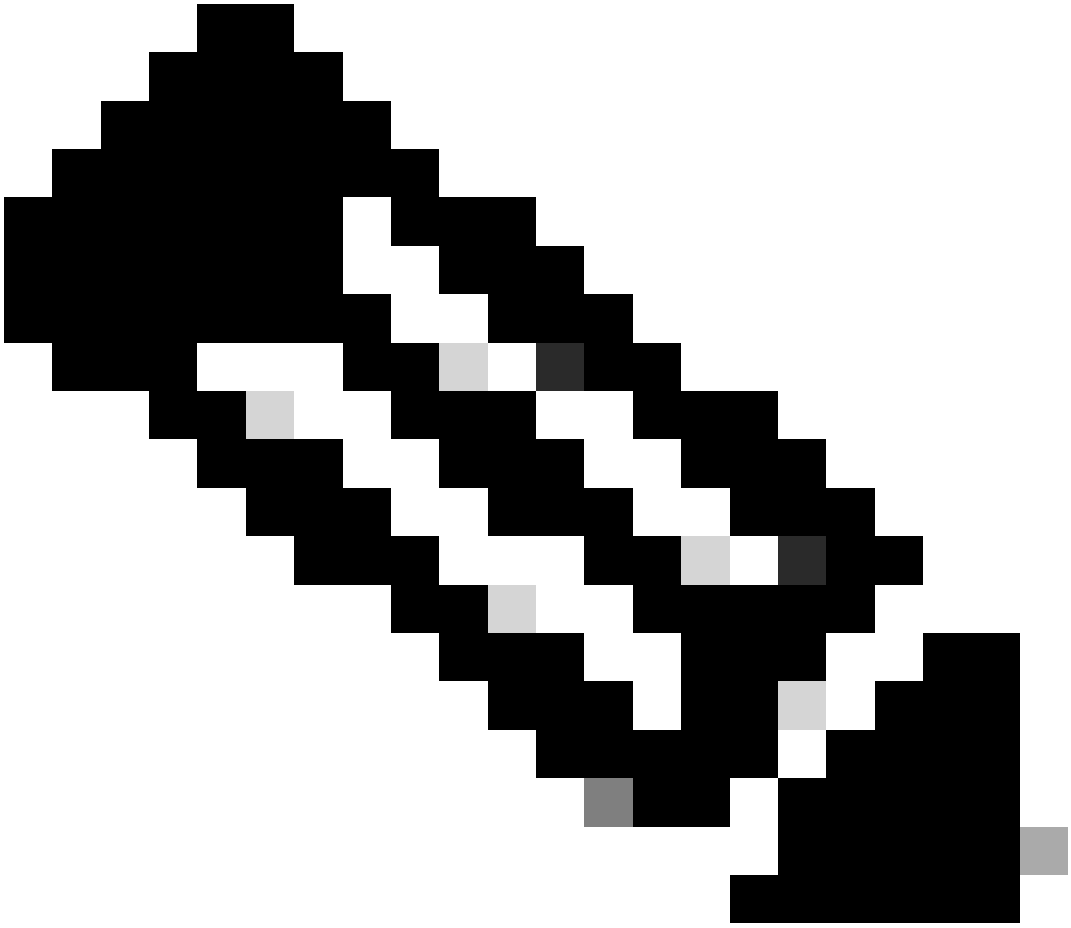
Pour permettre à Secure Access d'utiliser votre périphérique ISE pour l'authentification Radius, vous devez avoir configuré une règle d'accès sécurisé à votre réseau avec les ports Radius requis :

Règle	Source	Destination	Port de destination

ISE pour un accès sécurisé Pool de gestion	Serveur_ISE	Pool IP de gestion (RA-VPN)	ACO UDP 1700 (port par défaut)
Pool IP de gestion d'accès sécurisé vers ISE	Pool IP de gestion	Serveur_ISE	Authentification, autorisation UDP 1812 (port par défaut) Gestion de comptes UDP 1813 (port par défaut)
Pool IP de terminaux d'accès sécurisé vers ISE	Pool d'adresses IP	Serveur_ISE	Provisioning Portal TCP 8443 (port par défaut)
Pool d'adresses IP de point d'accès sécurisé vers SERVEUR DNS	Pool d'adresses IP	Serveur DNS	DNS UDP et TCP 53



Remarque : Si vous voulez en savoir plus sur les ports liés à ISE, consultez le Guide de l'utilisateur - Référence des ports.



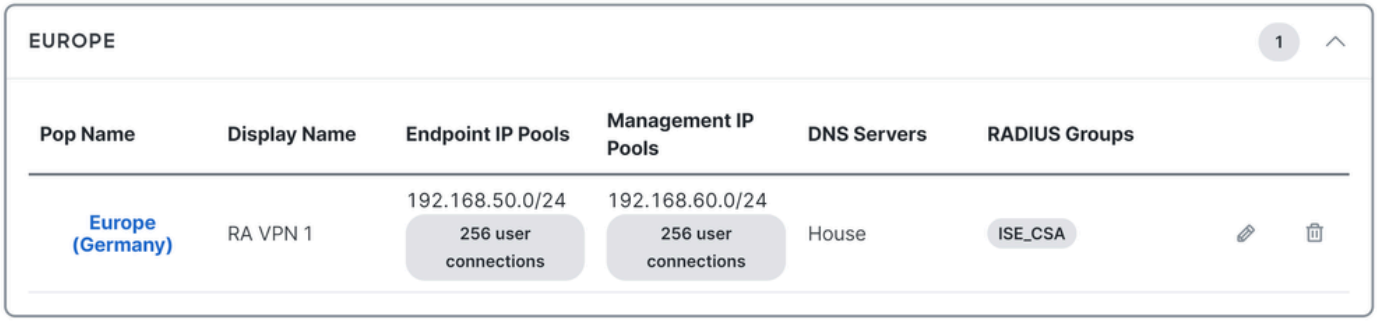
Remarque : Une règle DNS est nécessaire si vous avez configuré votre ISE pour qu'il soit détecté par un nom, tel que ise.ciscosspt.es

---

Pool de gestion et pools IP de terminaux

Pour vérifier votre pool d'adresses IP de gestion et de terminaux, accédez à votre tableau de bord d'accès sécurisé :

- Cliquez sur **Connect > End User Connectivity**
- Cliquez sur Virtual Private Network
- Sous **Manage IP Pools**
- Cliquez sur **Manage**

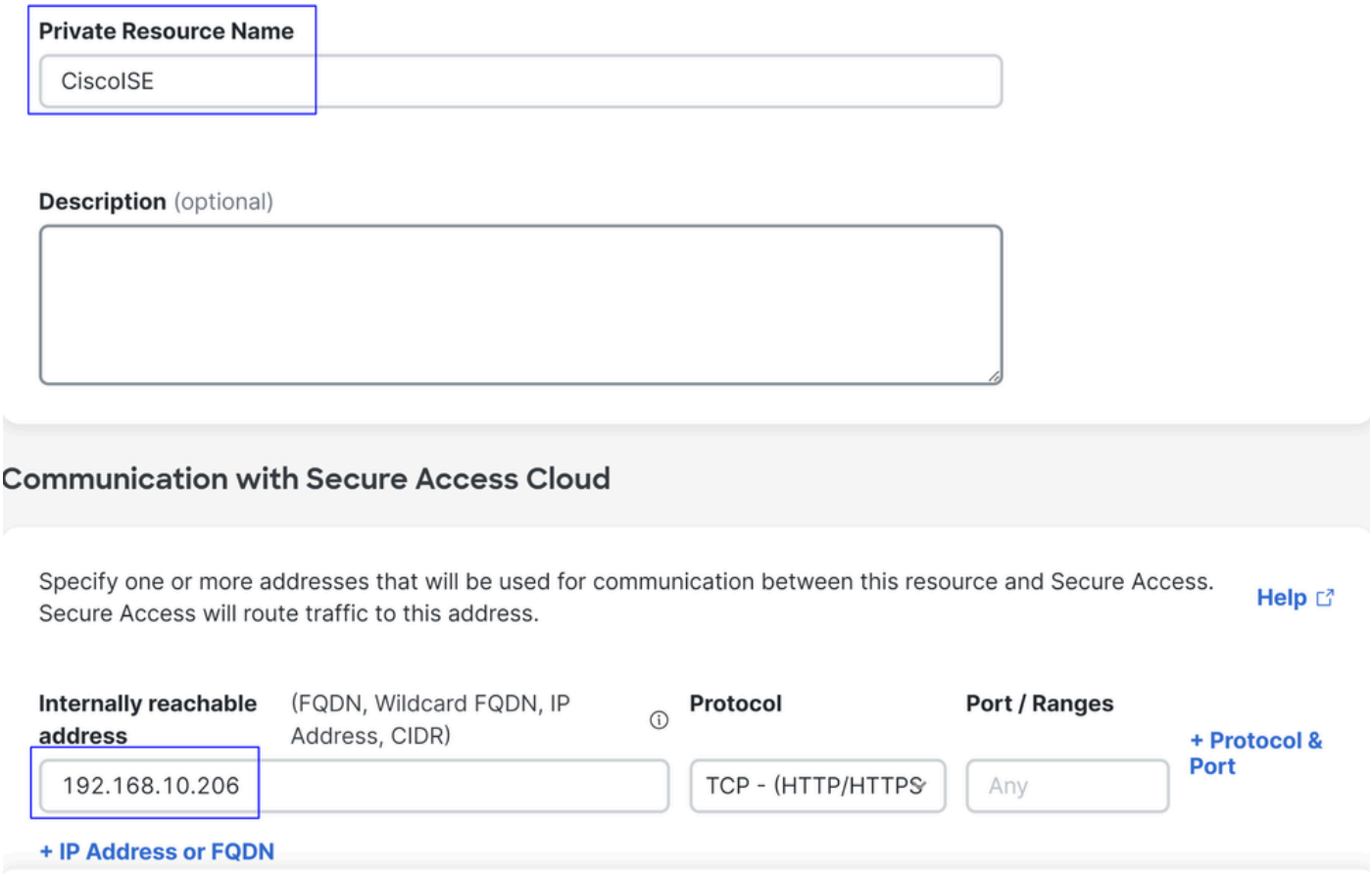


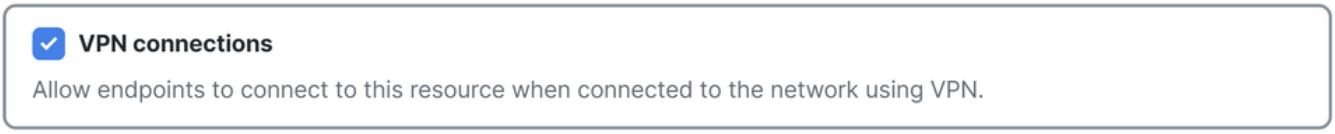
Étape 3 : Vérifiez que votre ISE est configuré sous Ressources privées

Pour permettre aux utilisateurs connectés via le VPN de naviguer vers **ISE Provisioning Portal**, vous devez vous assurer que vous avez configuré votre périphérique en tant que ressource privée pour fournir l'accès, qui est utilisé pour permettre le provisionnement automatique du**ISE Posture Module**via le VPN.

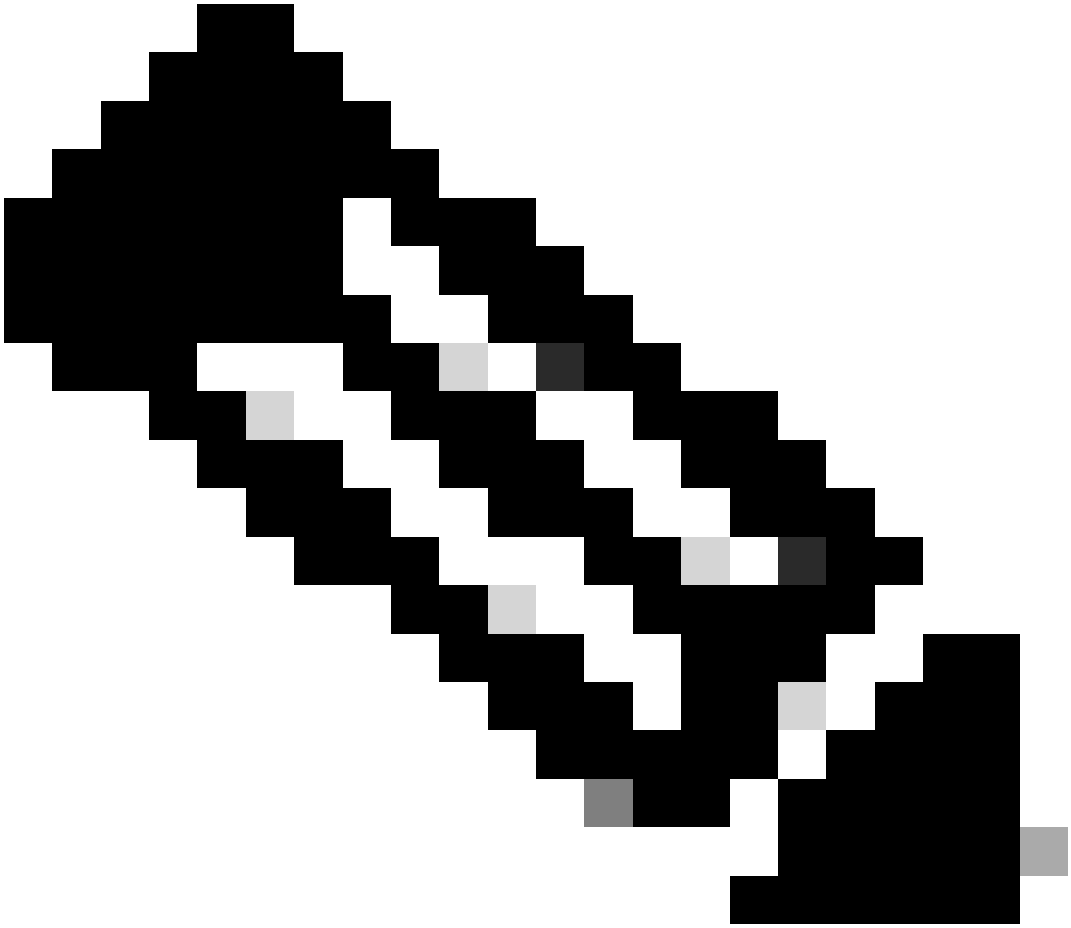
Pour vérifier que vous avez configuré ISE correctement, accédez à votre tableau de [bord d'accès sécurisé] :

- Cliquez sur **Resources** > **Private Resources**
- Cliquez sur la ressource ISE





Si nécessaire, vous pouvez limiter la règle au port du portail d'approvisionnement (8443).



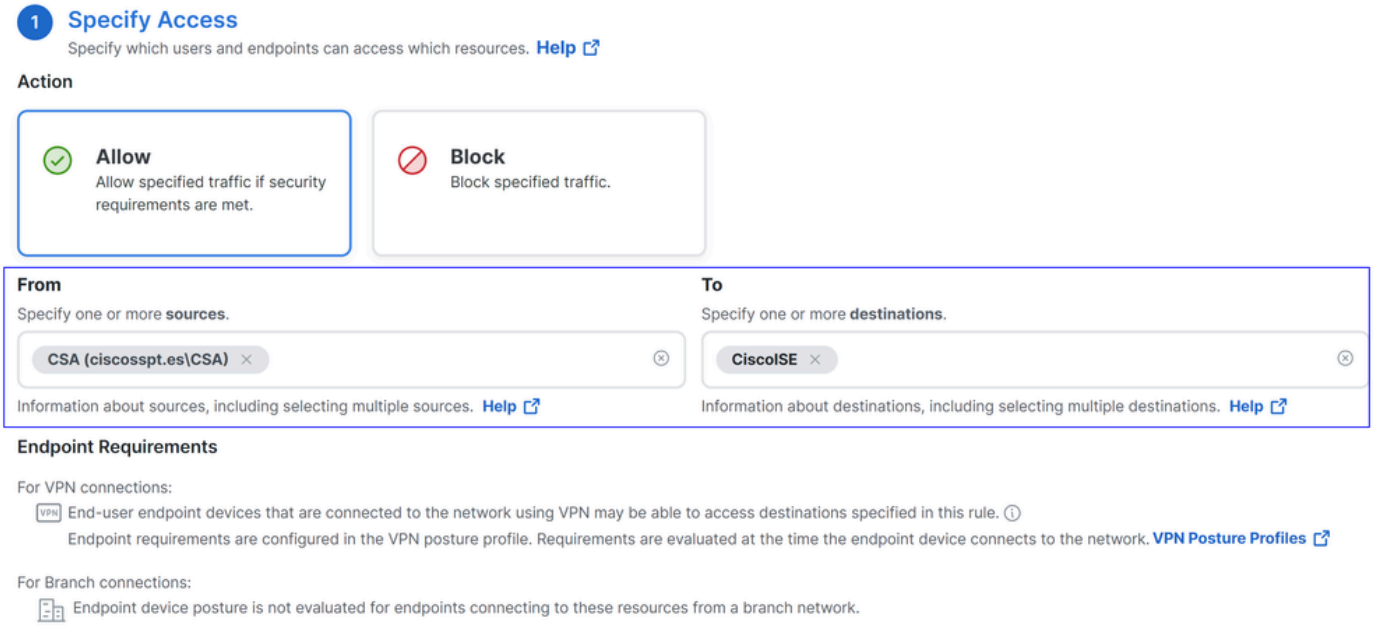
Remarque : Assurez-vous d'avoir coché la case pour les connexions VPN.

Étape 4 : Autoriser l'accès ISE dans la politique d'accès

Pour permettre aux utilisateurs connectés via le VPN de naviguer vers **ISE Provisioning Portal**, vous devez être sûr d'avoir configuré et **Access Policy** de permettre aux utilisateurs configurés sous cette règle d'accéder à la ressource privée configurée dansStep3.

Pour vérifier que vous avez configuré ISE correctement, accédez à votre tableau de bord d'accès sécurisé :

- Cliquez sur **Secure > Access Policy**
- Cliquez sur la règle configurée pour autoriser l'accès des utilisateurs VPN à ISE

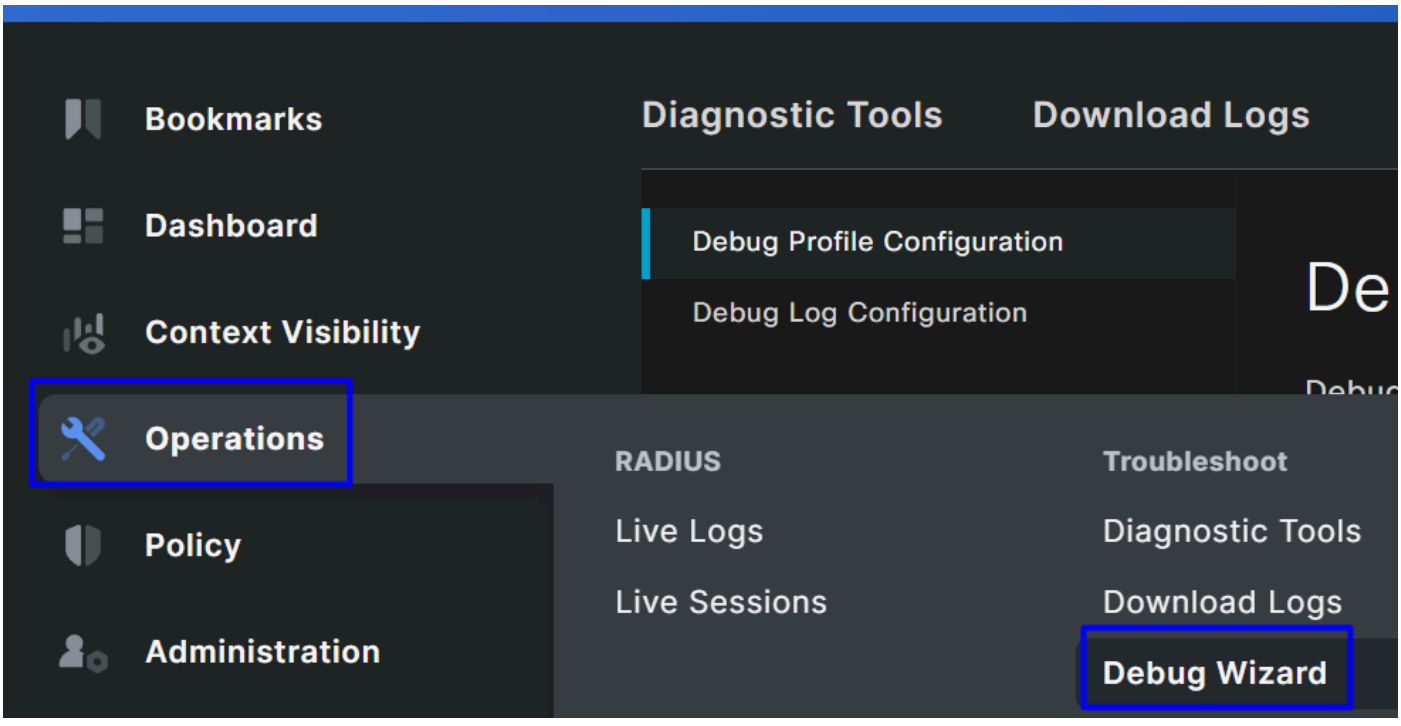


Dépannage

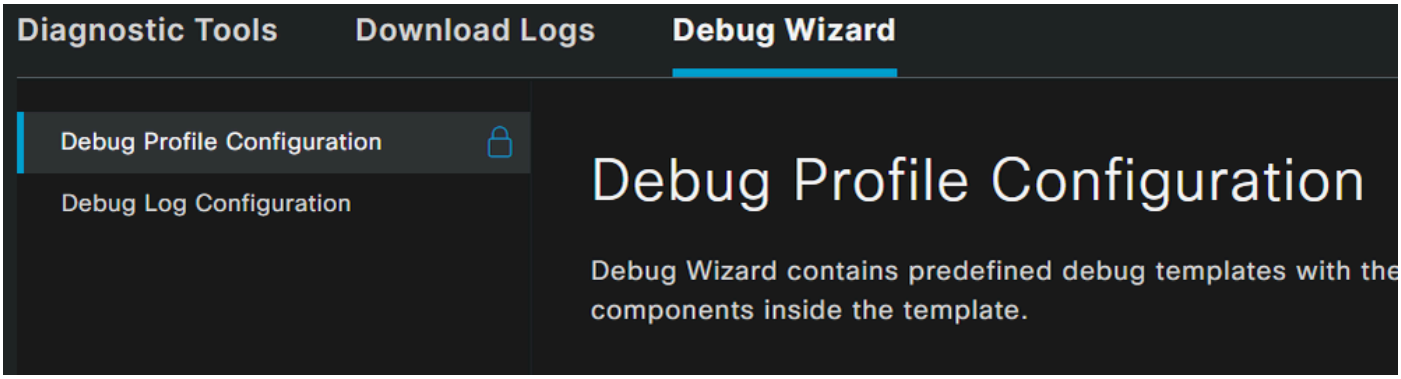
Téléchargement des journaux de débogage de la position ISE

Pour télécharger les journaux ISE afin de vérifier un problème lié à la position, procédez comme suit :

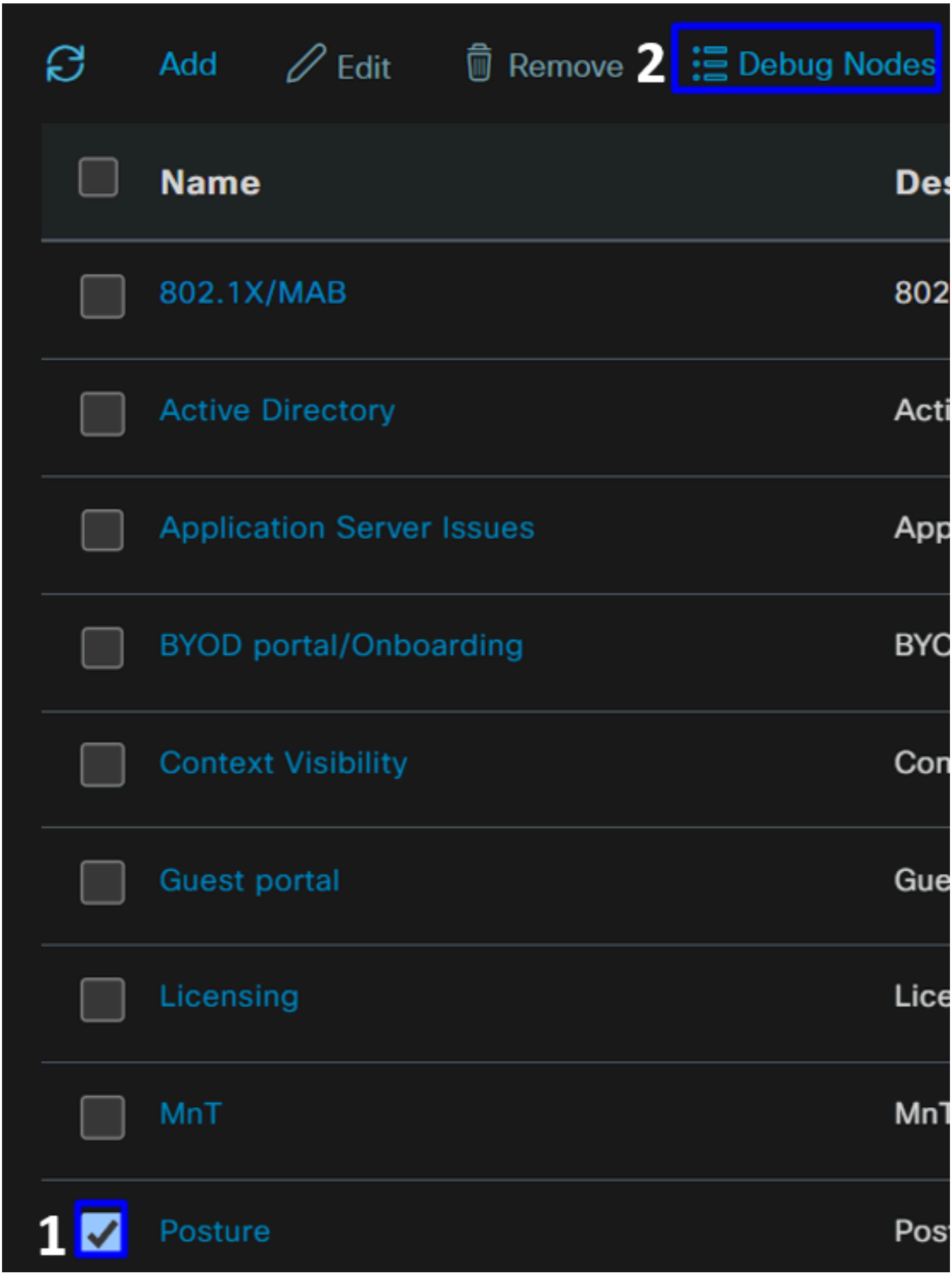
- Accédez à votre tableau de bord ISE
- Cliquez sur Operations > Troubleshoot > Debug Wizard



- Cliquez sur Debug Profile Configuration

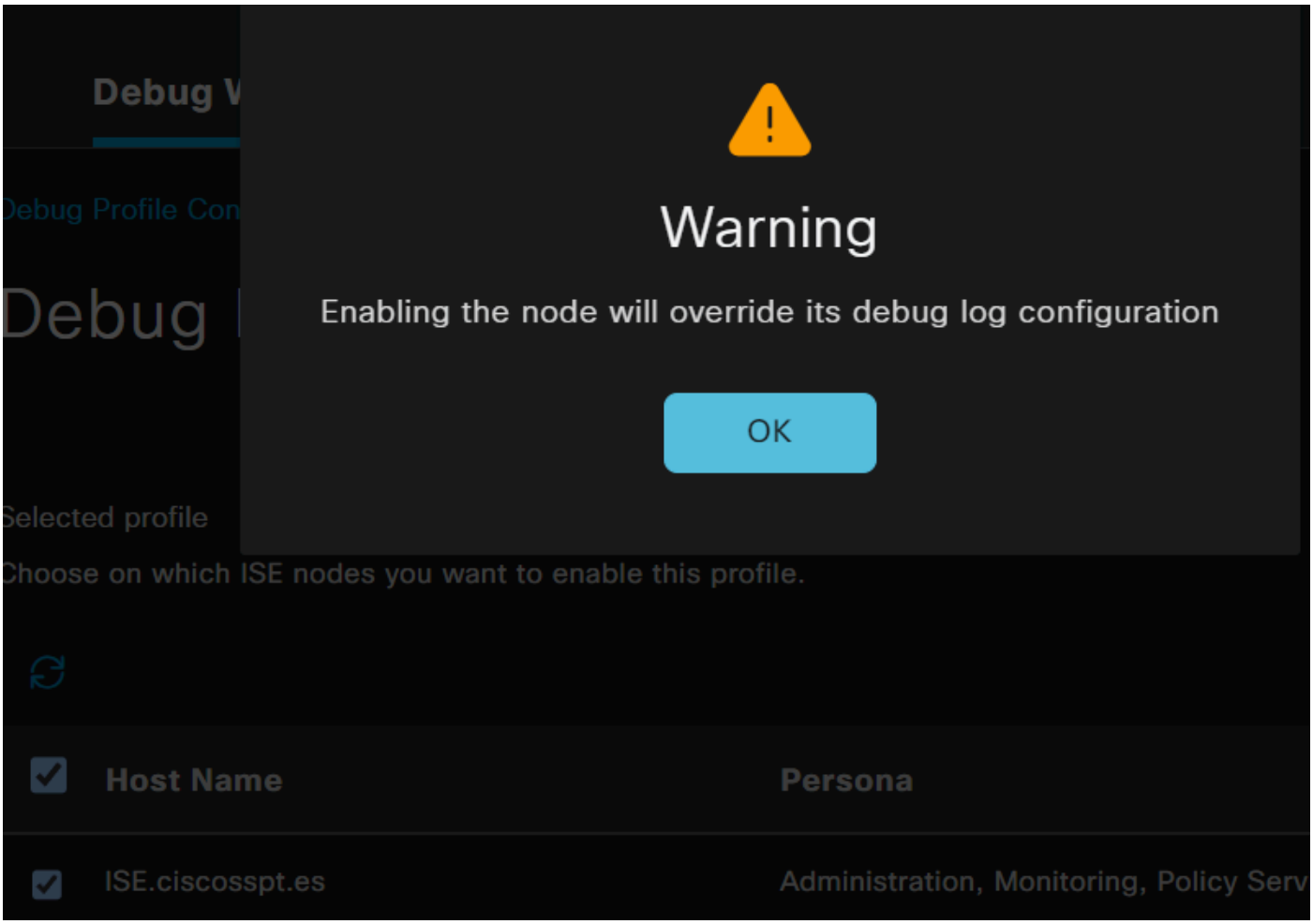


- Cochez la case correspondant à **Posture** > **Debug Nodes**

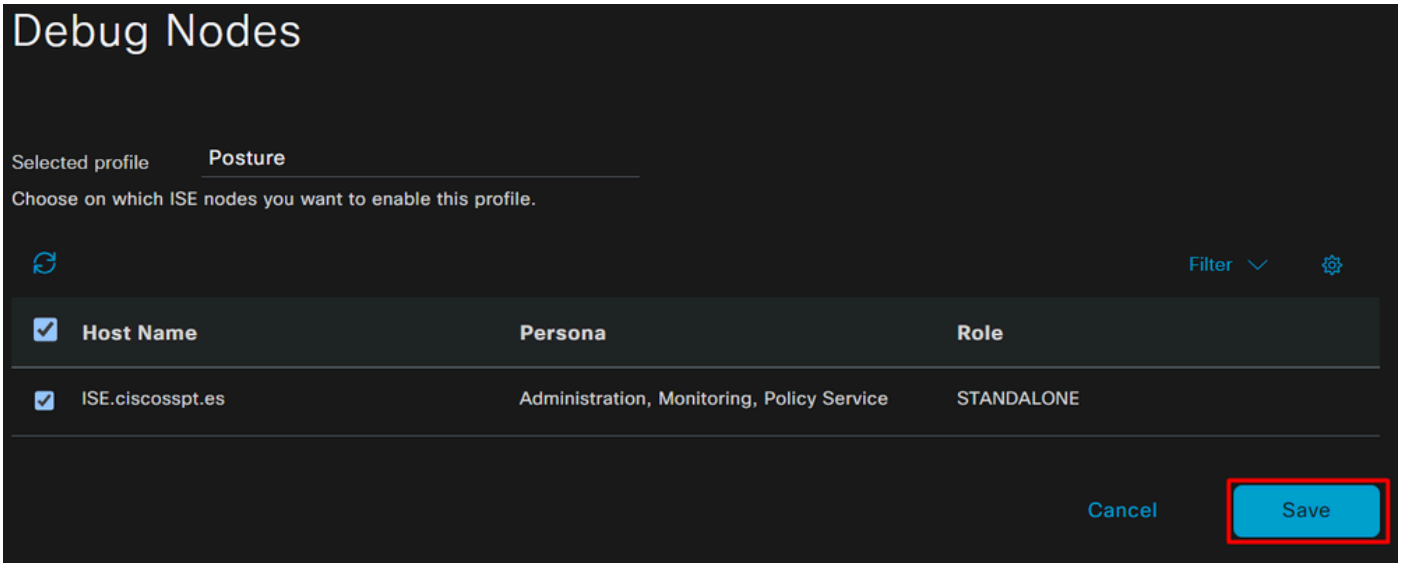


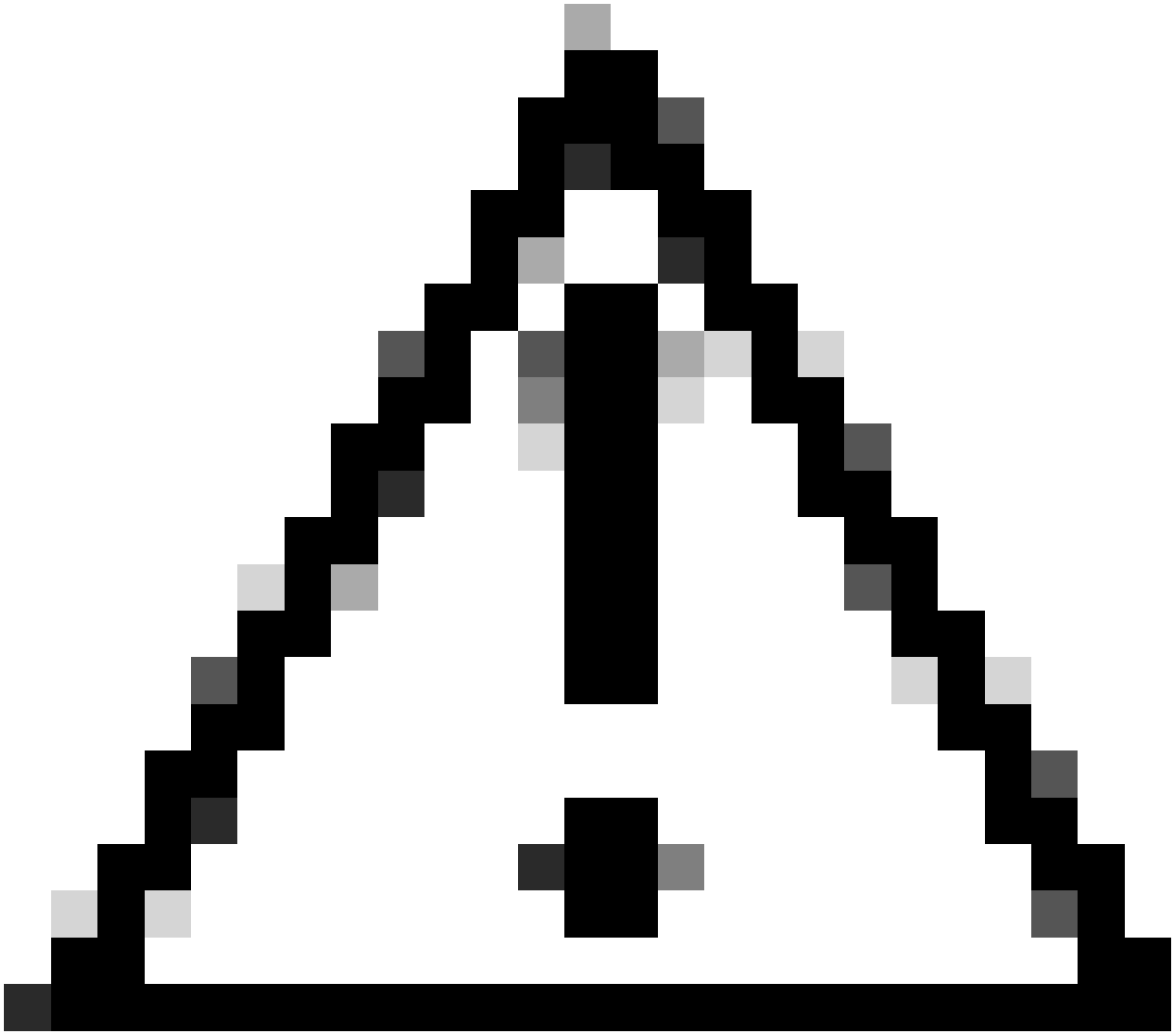
- Cochez la case des noeuds ISE sur lesquels vous devez activer le mode de débogage pour

résoudre votre problème



- Cliquer Save

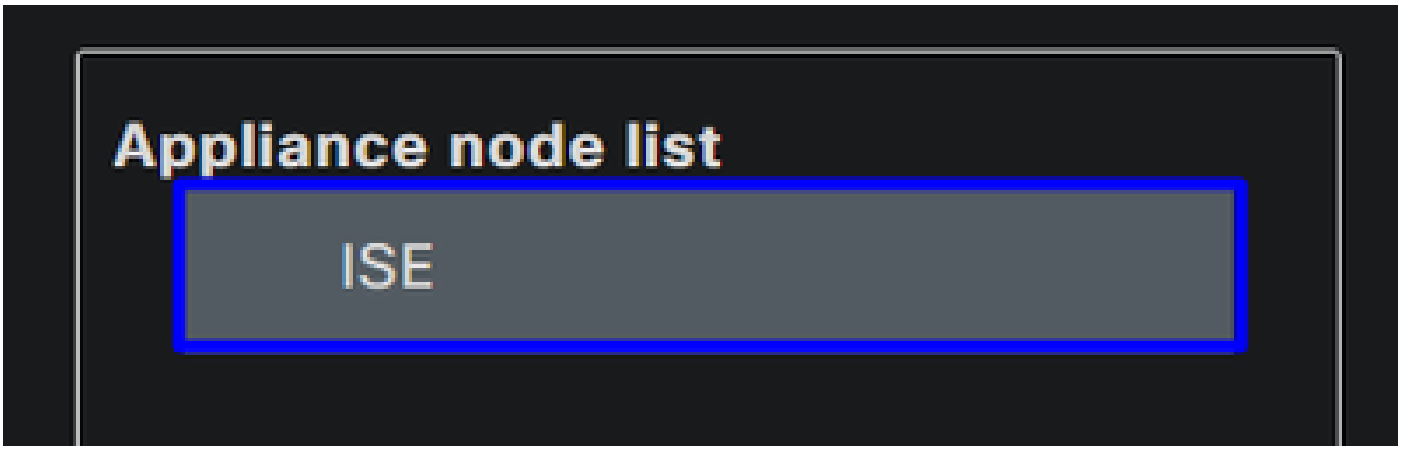




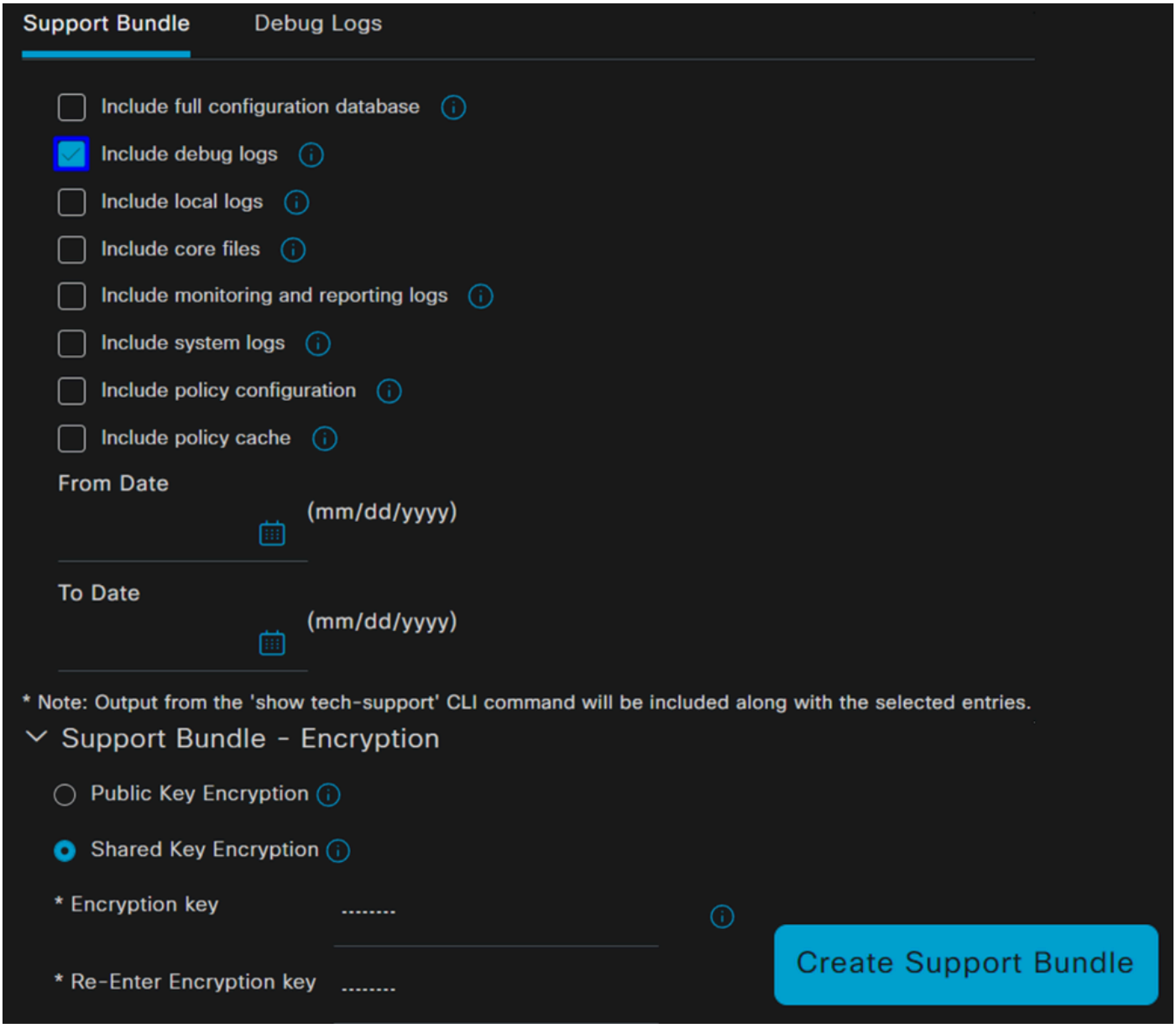
Mise en garde : Après ce point, vous devez commencer à reproduire votre numéro ; **the debug logs can affect the performance of your device.**

Une fois le problème reproduit, passez aux étapes suivantes :

- Cliquez sur Operations > Download Logs
- Sélectionnez le noeud à partir duquel vous voulez prendre les journaux

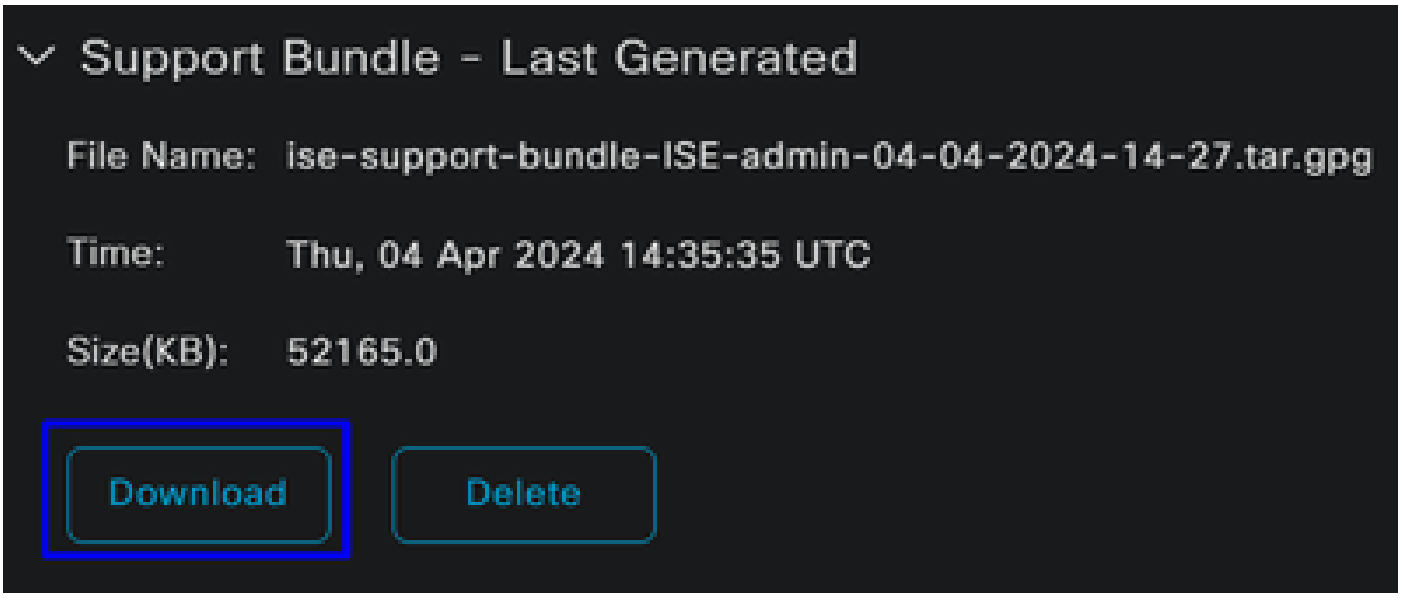


- Sous **Support Bundle**, choisissez les options suivantes :



- Include debug logs
- Sous **Support Bundle Encryption**
  - **Shared Key Encryption**
    - Remplir **Encryption key** et **Re-Enter Encryption key**

- Cliquer **Create Support Bundle**
- Cliquer **Download**

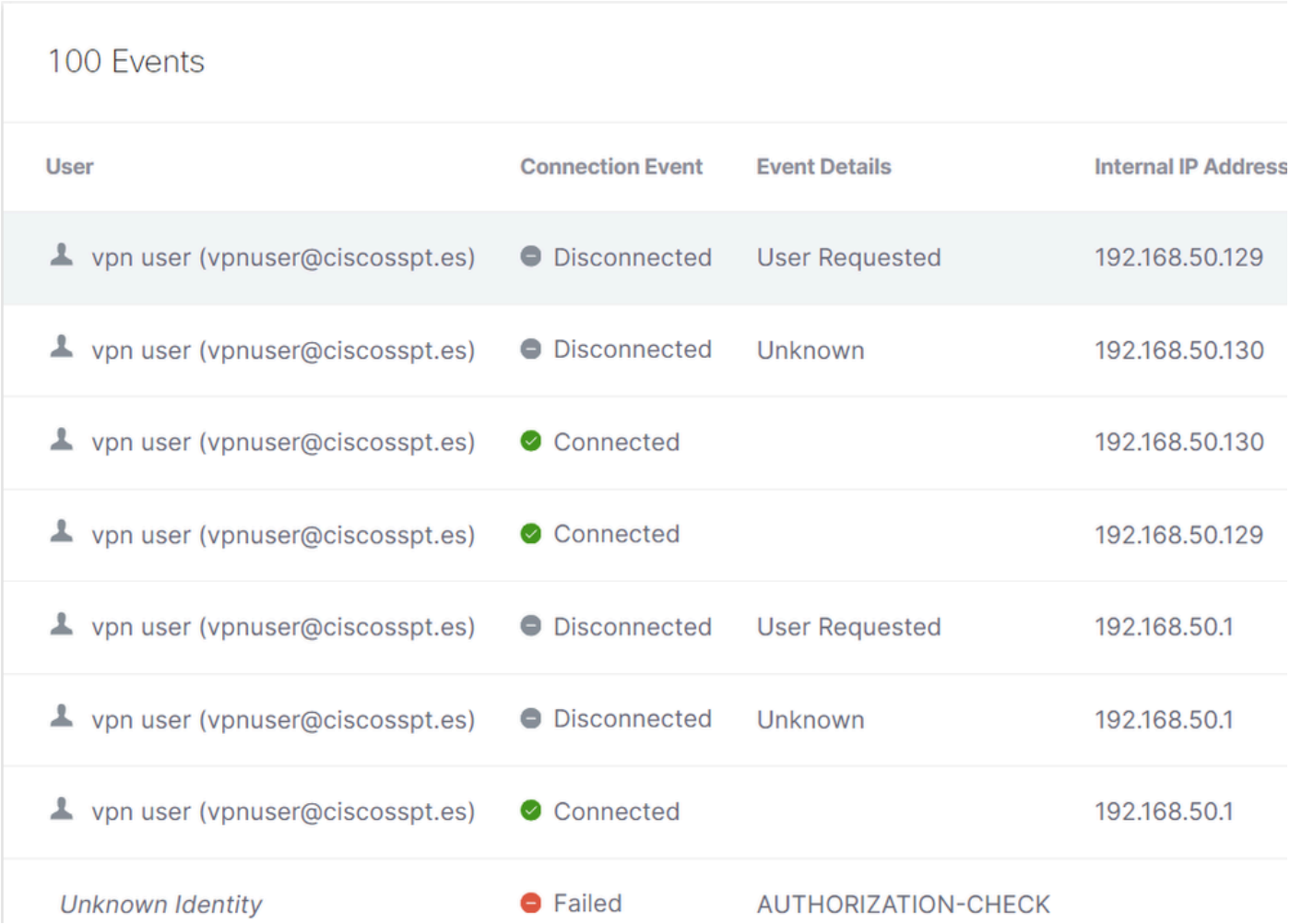


Avertissement : Désactivez le mode de débogage activé à l'étape Configuration du profil de débogage

Vérification des journaux d'accès à distance Secure Access

Accédez à votre tableau de bord Secure Access :

- Cliquez sur Monitor > Remote Access Logs



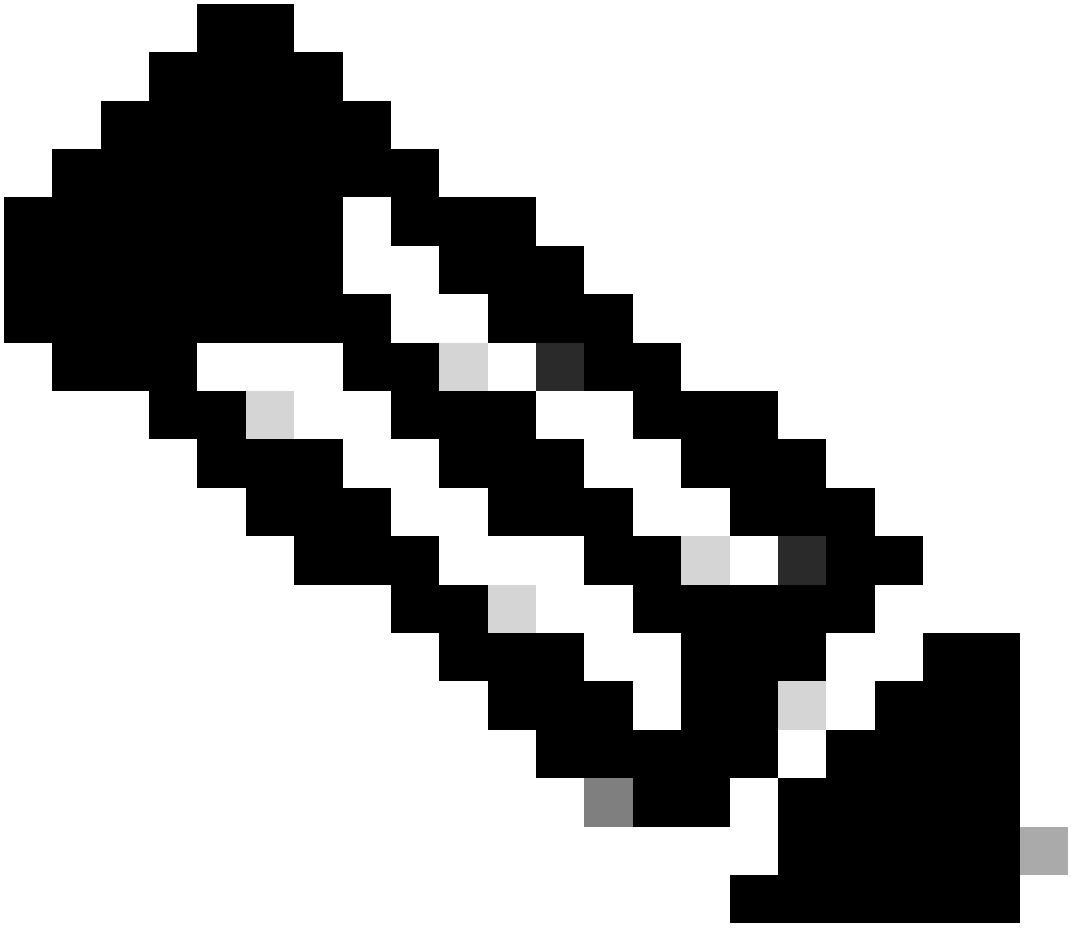
100 Events

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	

Générer un bundle DART sur le client sécurisé

Pour générer un bundle DART sur votre machine, vérifiez l'article suivant :

Outil Cisco Secure Client Diagnostic and Reporting Tool (DART)



Remarque : Une fois que vous avez collecté les journaux indiqués dans la section de dépannage, ouvrez un dossier avec TAC pour poursuivre l'analyse des informations.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Documentation et guide de l'utilisateur Secure Access
- Téléchargement du logiciel Cisco Secure Client
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.