Duo SSOを使用したRA-VPNaaSのセキュアアクセスの設定およびISEを使用したポスチャアセスメント

内容

はじめに

このドキュメントでは、Identity Service Engine(ISE)を使用したリモートアクセスVPNユーザのポスチャ評価と、Duoを使用したセキュアアクセスを設定する方法について説明します。

前提条件

- セキュアアクセスでのユーザプロビジョニングの設定
- 認証プロキシまたはサードパーティのIDPを使用したDuo SSOの設定
- トンネル経由でセキュアアクセスに接続されたCisco ISE

要件

次の項目に関する知識があることが推奨されます。

- アイデンティティサービスエンジン
- セキュアなアクセス
- Cisco Secureクライアント
- 二要素認証ガイド – Duoセキュリティ
- ISE ポスチャ
- 認証、許可、およびアカウンティング

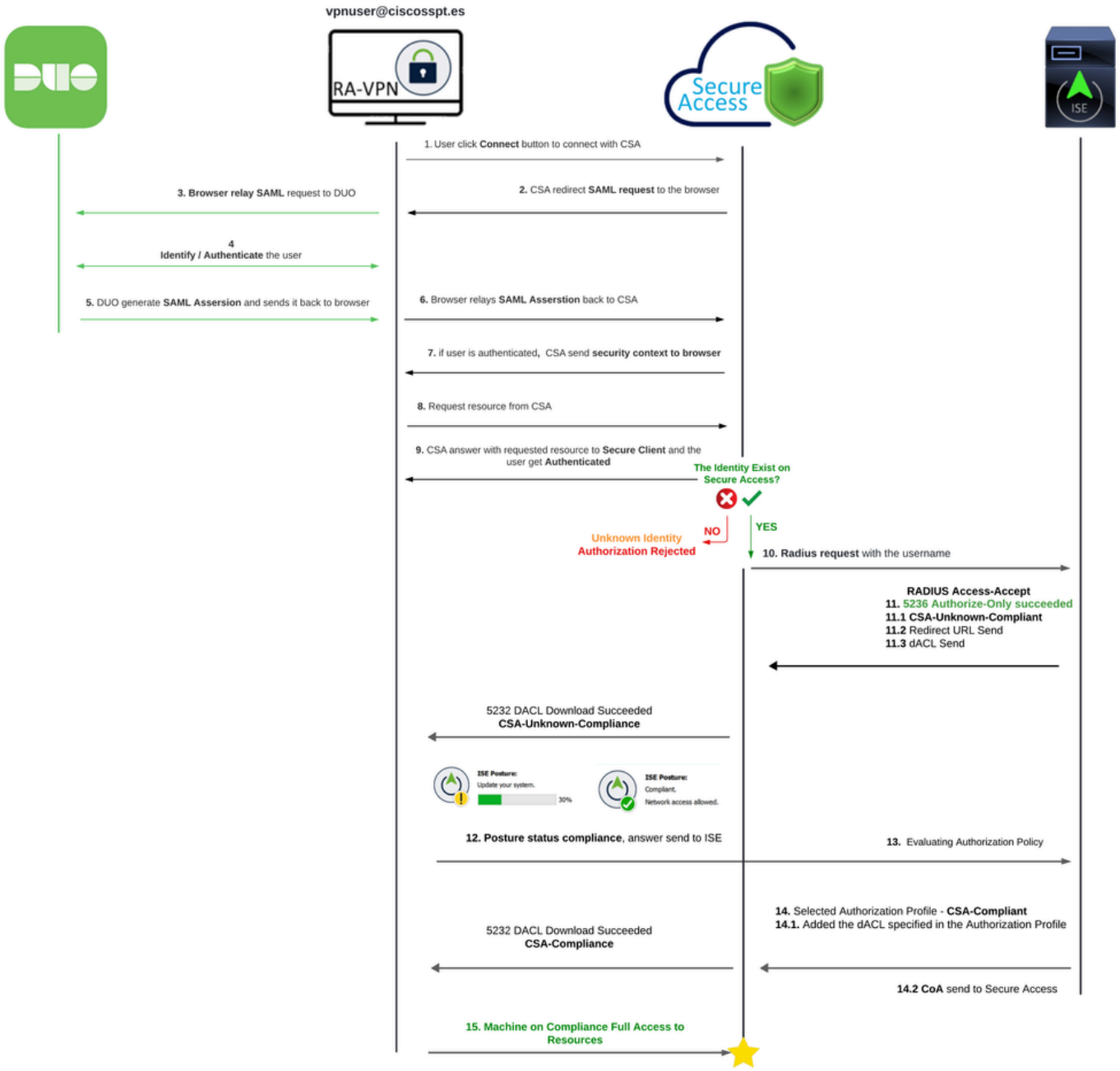
使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Identity Service Engine(ISE)バージョン3.3パッチ1
- セキュアなアクセス
- Cisco Secure Client:Anyconnect VPNバージョン5.1.2.42

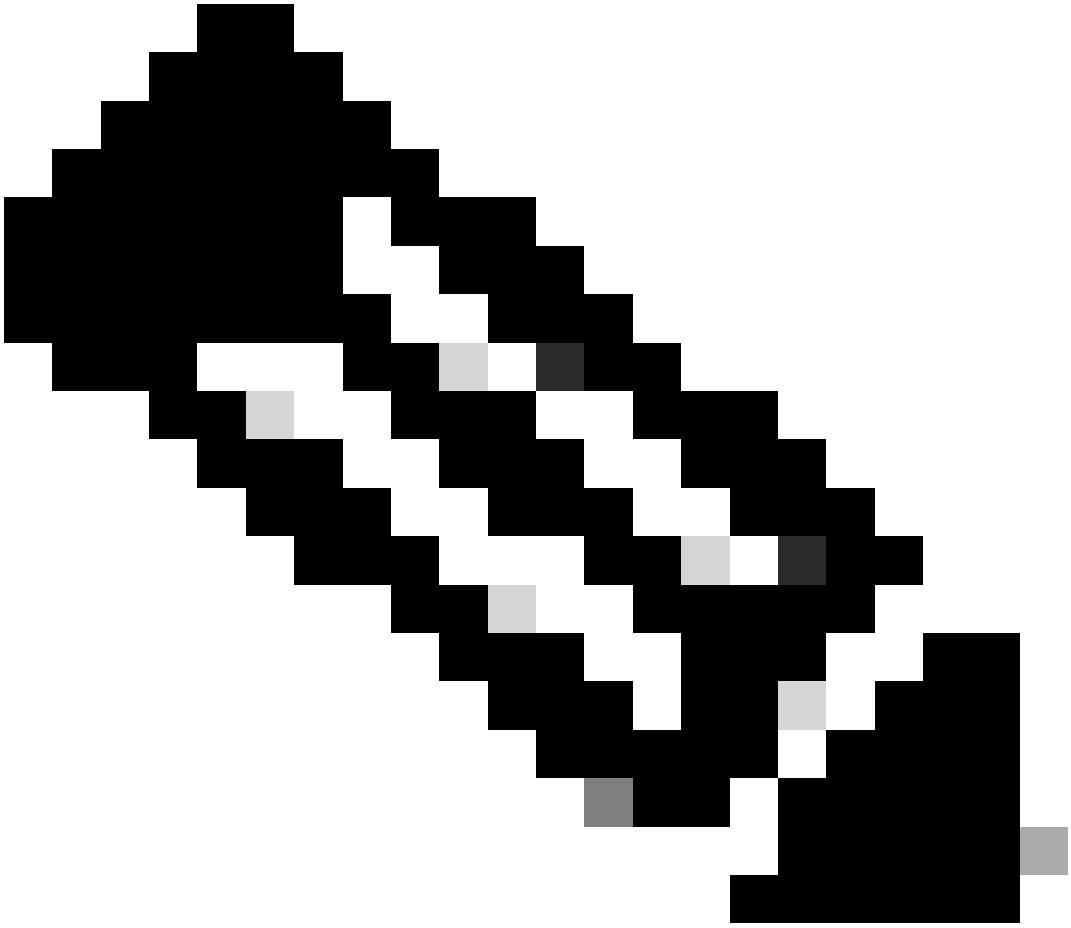
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明



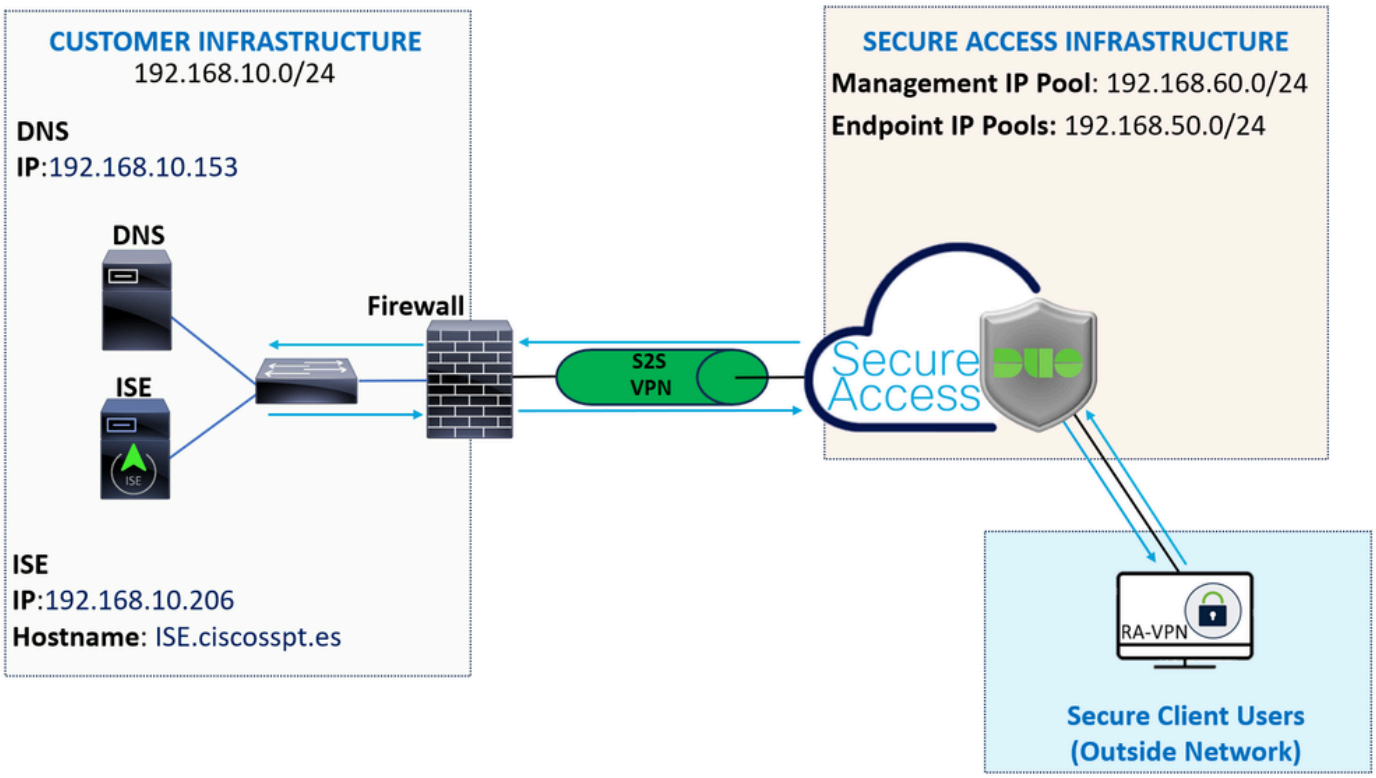
Duo SAMLとCisco Identity Services Engine(ISE)の統合により、認証プロセスが強化され、シスコセキュアアクセスソリューションに新たなセキュリティレイヤが追加されます。Duo SAMLは、高いセキュリティ標準を確保しながら、ユーザログインプロセスを簡素化するシングルサインオン(SSO)機能を提供します。

Duo SAMLで認証されると、Cisco ISEによって認証プロセスが処理されます。これにより、ユーザIDとデバイスのポスチャに基づいて動的なアクセス制御の決定が可能になります。ISEは、ユーザがアクセスできるリソース、時間、およびデバイスを決定する詳細なポリシーを適用できます。

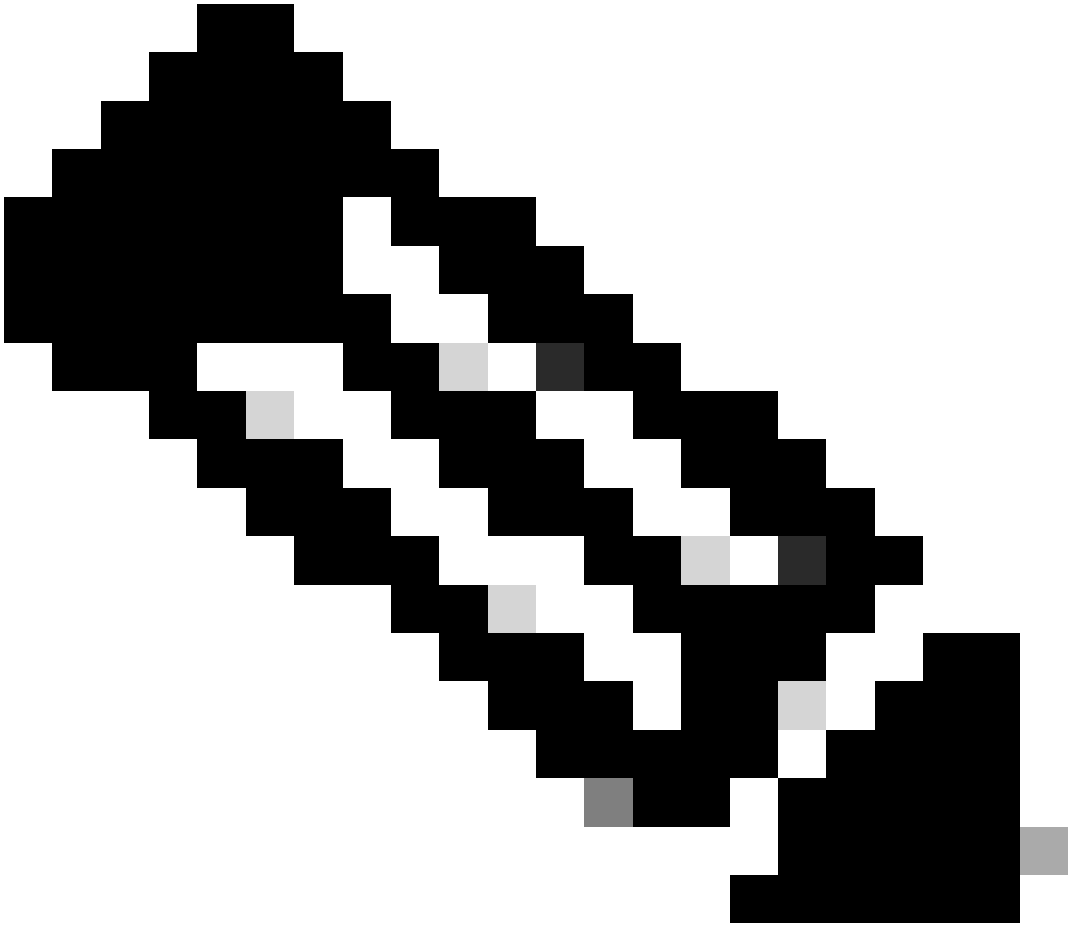


注:RADIUS統合を設定するには、両方のプラットフォーム間で通信が行われていることを確認する必要があります。

ネットワーク図


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)

設定



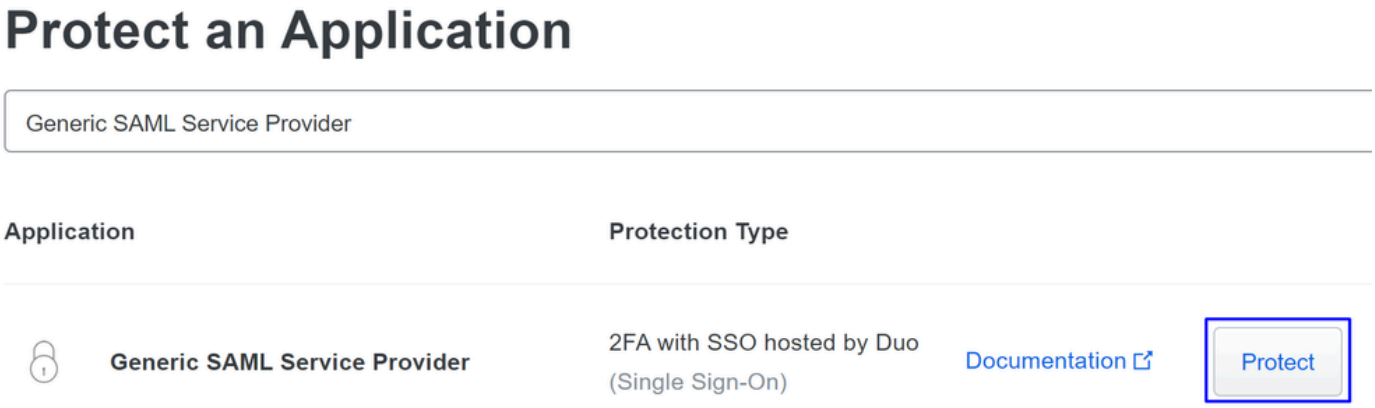
注：設定プロセスを開始する前に、「セキュアアクセスとISE統合の最初の手順」を完了する必要があります。

Duo設定

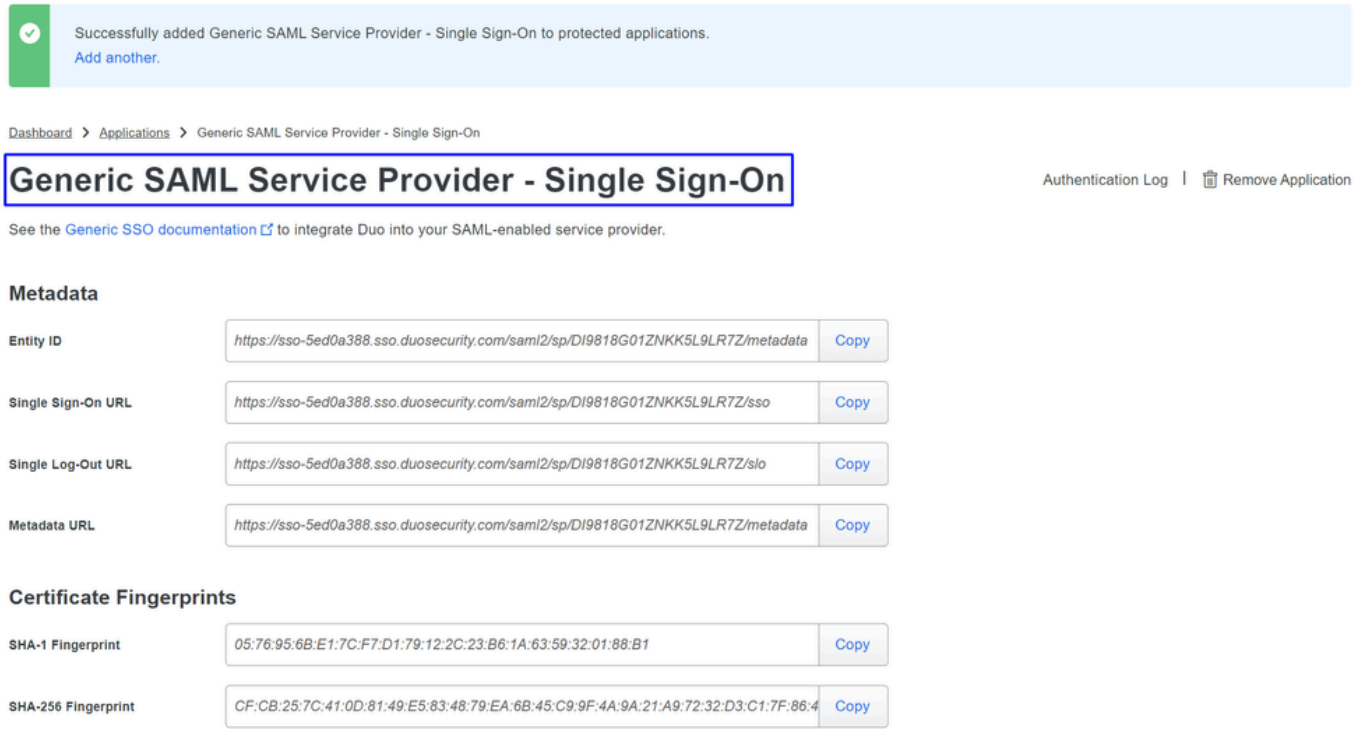
RA-VPNアプリケーションを設定するには、次の手順に従います。

Duo管理パネルに移動します。

- 移動先 **Applications > Protect an Application**
  - 検索 **Generic SAML Service Provider**
  - クリック Protect



アプリケーションが画面に表示されている必要があります。VPN設定のアプリケーション名を覚えておいてください。



この例では、 **Generic SAML Service Provider.**

セキュアアクセスの設定

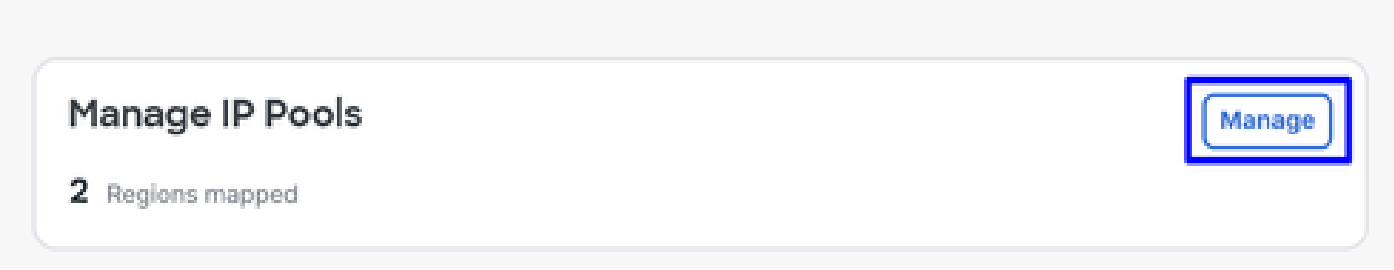
IPプールでのRADIUSグループの設定

Radiusを使用してVPNプロファイルを設定するには、次の手順に進みます。

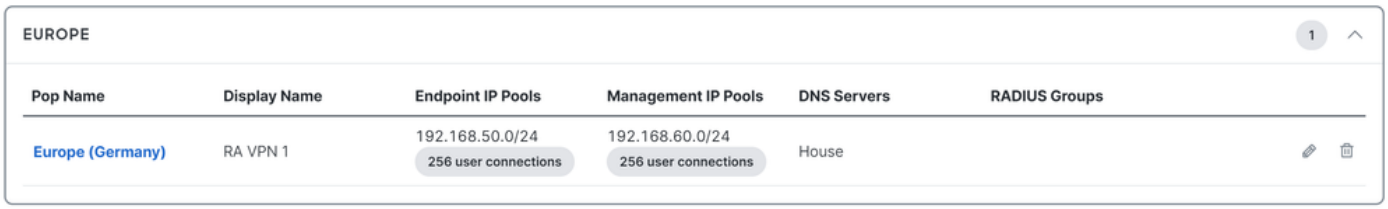
Secure Access Dashboardに移動します。

- クリック **Connect** > **Enduser Connectivity** > **Virtual Private Network**
- プール設定(**Manage IP Pools**)で、Manage

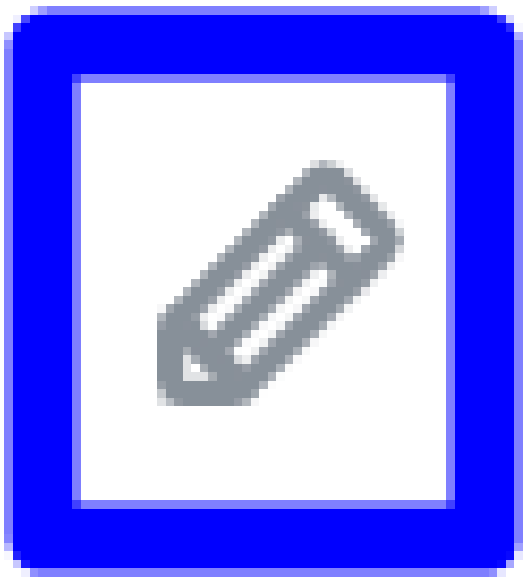
IP Pool Region

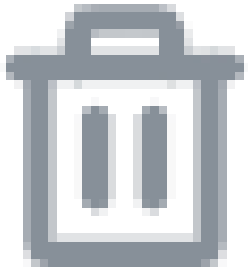


- コマンドを選択し、 **Radius Server**



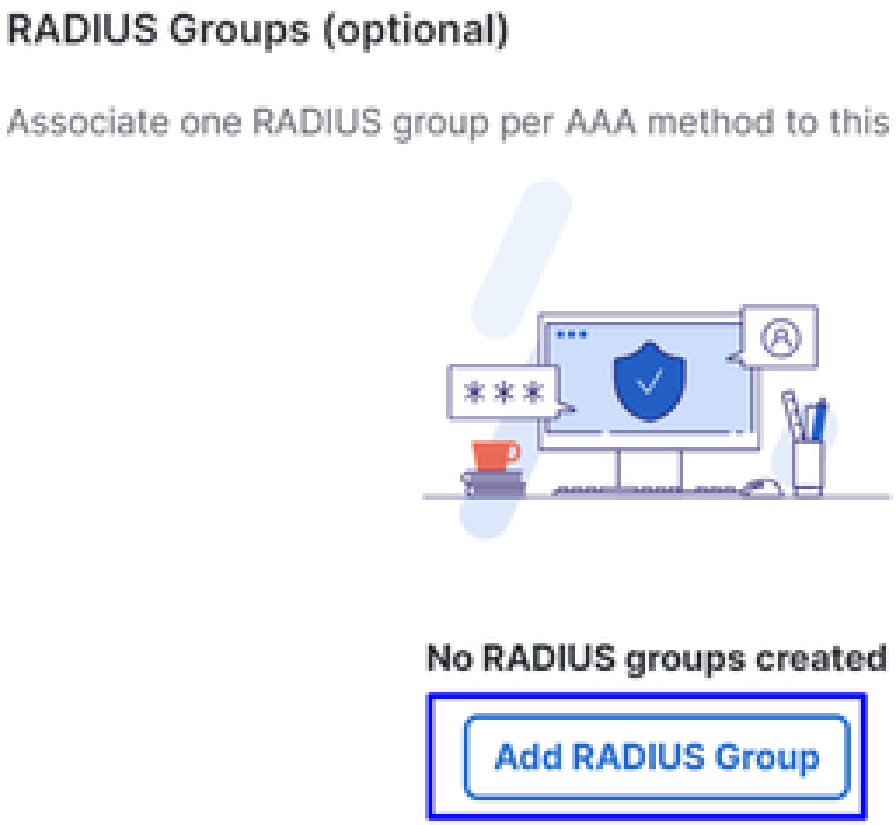
- 編集する鉛筆をクリックします





- ここで、IP Poolセクションのconfigurationドロップダウンで、 **Radius Group (Optional)**

- クリック 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

します。

- **AAA method**

  - **Authentication**:**Authentication** のチェックボックスをオンにし、ポートを選択します。デフォルトは1812です。

    - 認証でMicrosoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)が必要な場合は、チェックボックスをオンにします

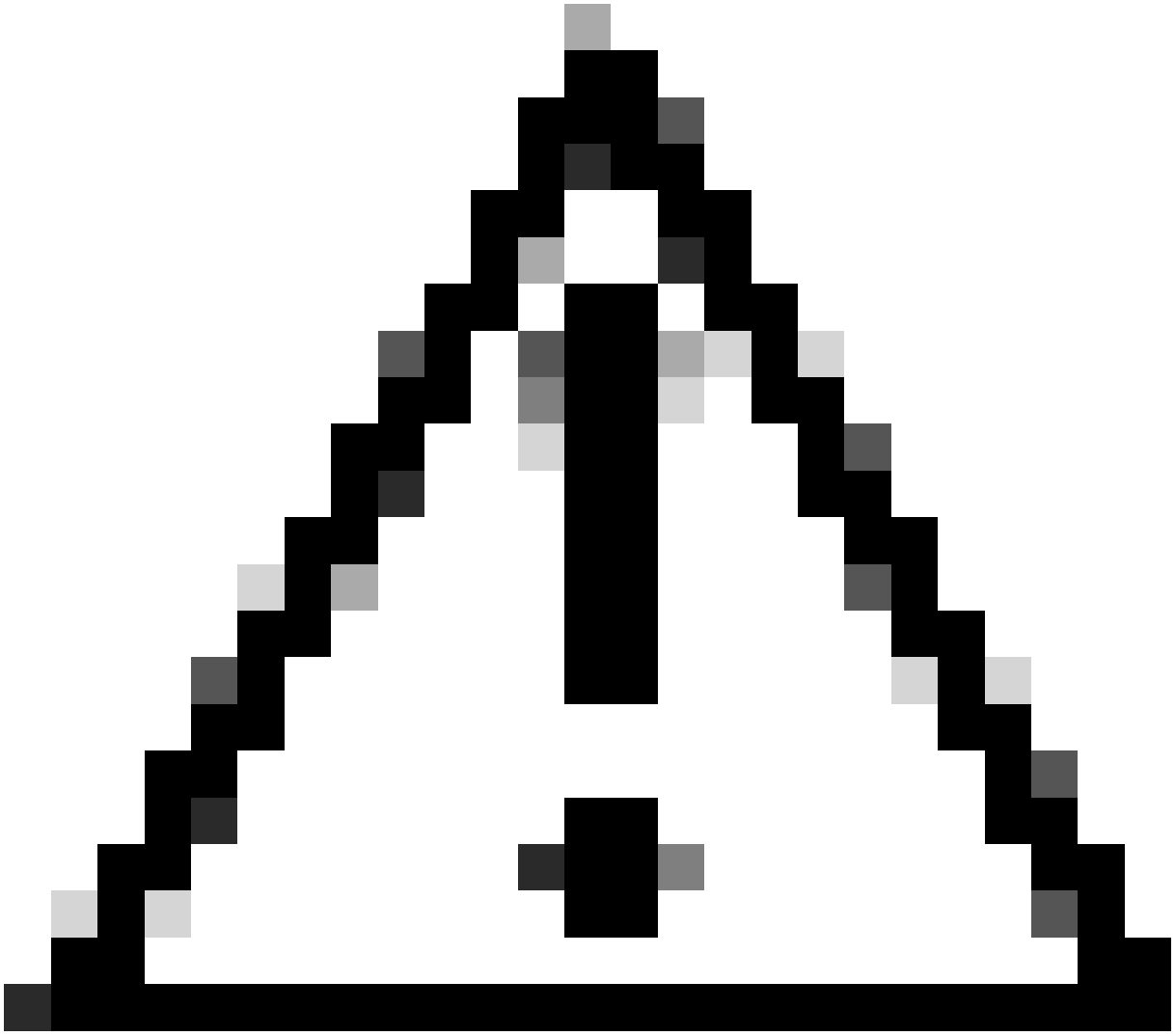
  • **Authorization**:Authorizationのチェックボックスをオンにし、ポートを選択します。デフォルトは1812です。

    - ISEからのポスチャと変更を許可する**Authorization mode Only Change of Authorization (CoA) mode** チェックボックスをオンにします。

  • **Accounting**:Authorizationのチェックボックスをオンにし、ポートを選択します。デフォルトは1813です。

    Single or Simultaneous
    • を選択します(シングルモードでは、アカウンティングデータは1台のサーバだけに送信されます。同時モードでは、グループ内のすべてのサーバへのアカウンティングデータ)

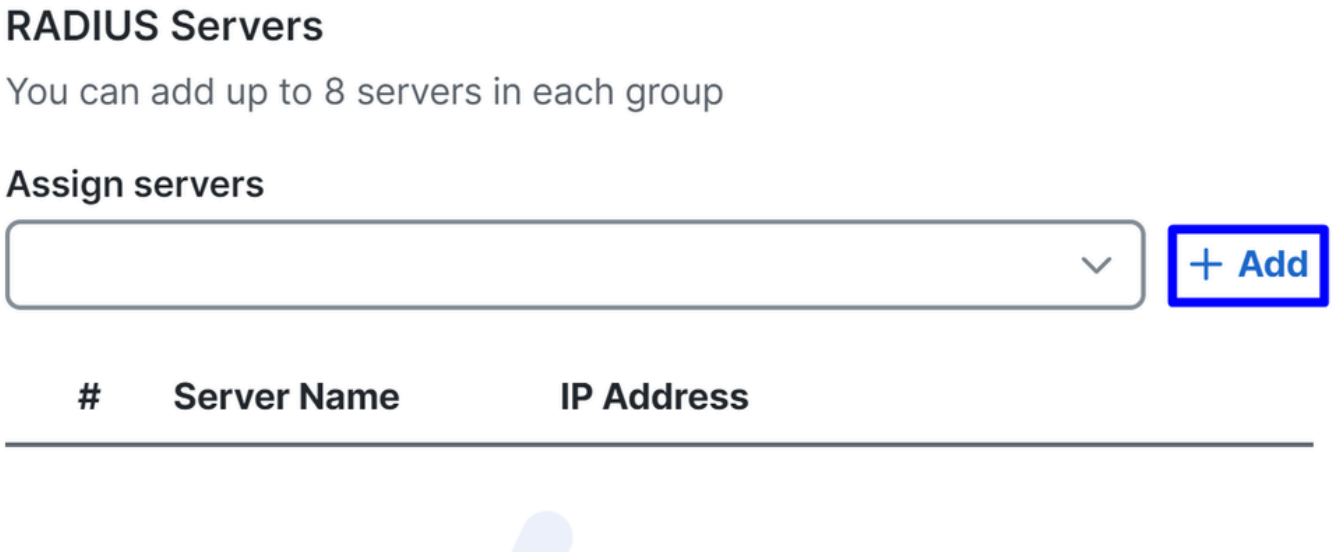
    • RADIUS interim-accounting-updateメッセージの定期的な生成を有効にするには、 **Accounting update** のチェックボックスをオンにします。



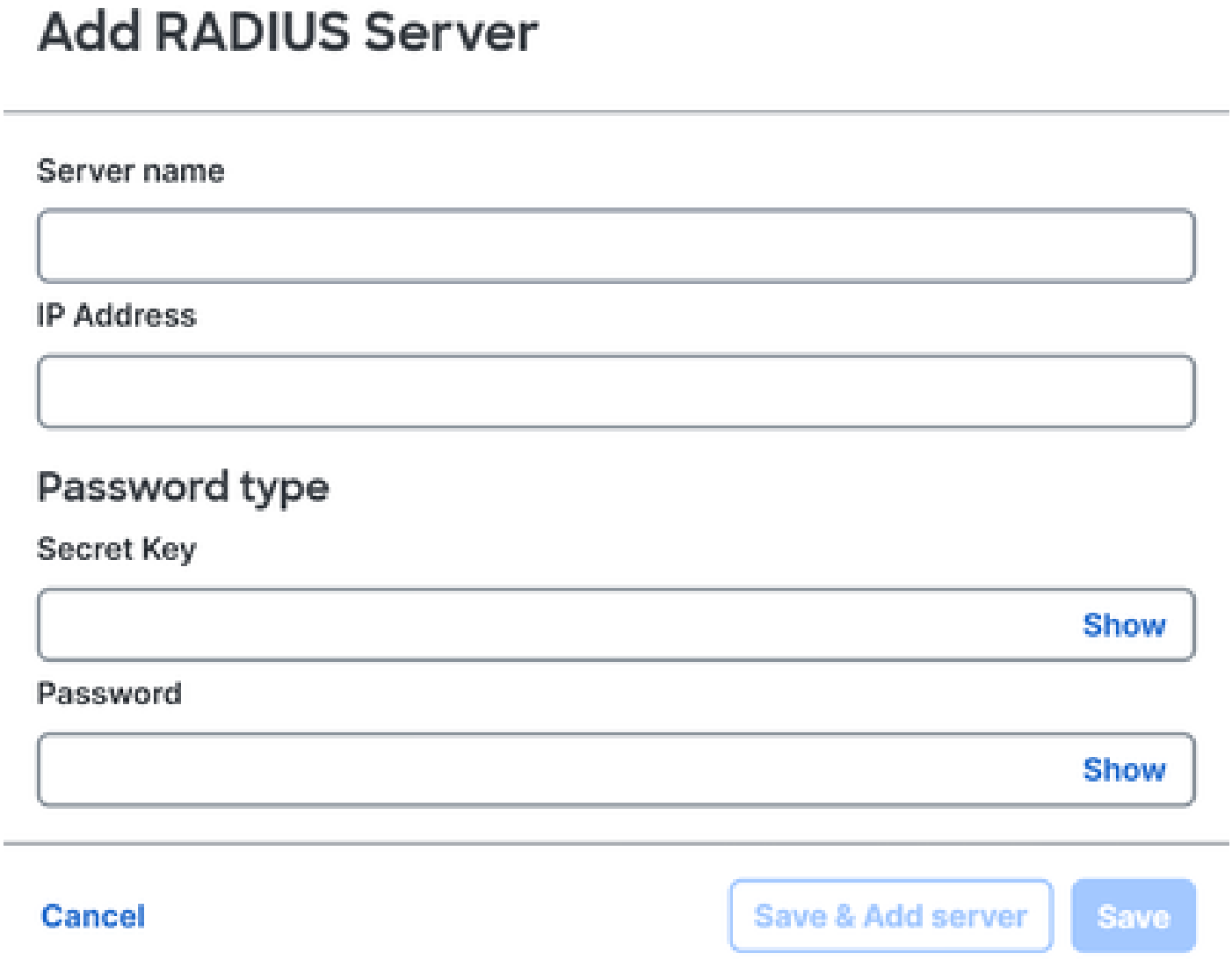
注意:Authenticationと**Authorization** の両方の方法を選択する場合は、同じポートを使用する必要があります。

RADIUS Servers

- その後、セクション **RADIUS Servers**:
- クリック + Add

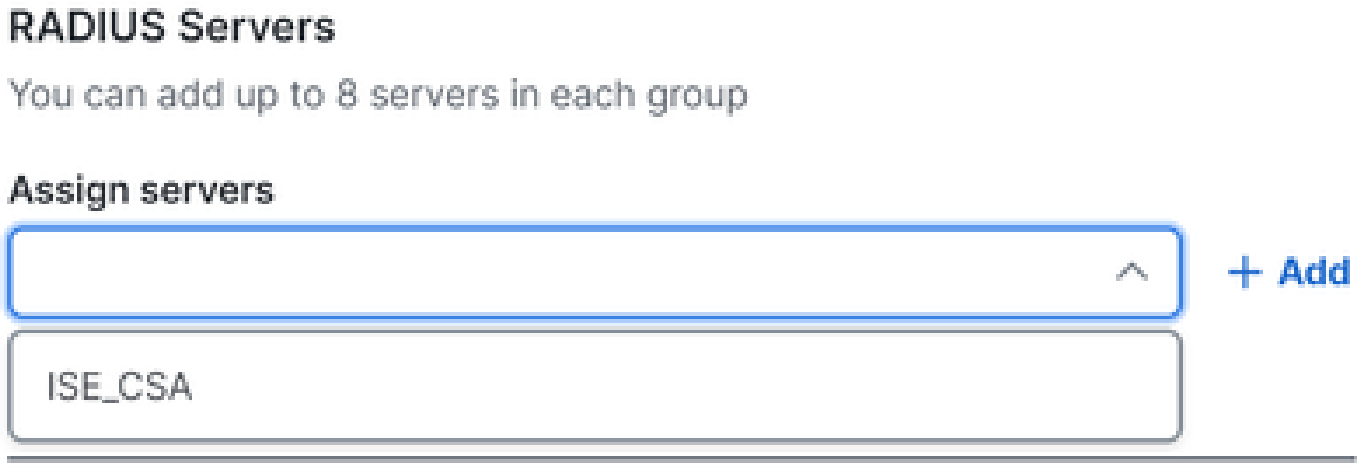


- 次に、次のオプションを設定します。



- Server Name:ISEサーバを識別するための名前を設定します。
- **IP Address**：セキュアアクセスを介して到達可能なCisco ISEデバイスのIPを設定します。
- **Secret Key**: RADIUS秘密キーの設定
- **Password**: RADIUSパスワードの設定

- をクリック**Save** し、Assign ServerのオプションでRadiusサーバを割り当て、ISEサーバを選択します。



- 完了したすべての設定を保存するには、**Save** をもう一度クリックします

← 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

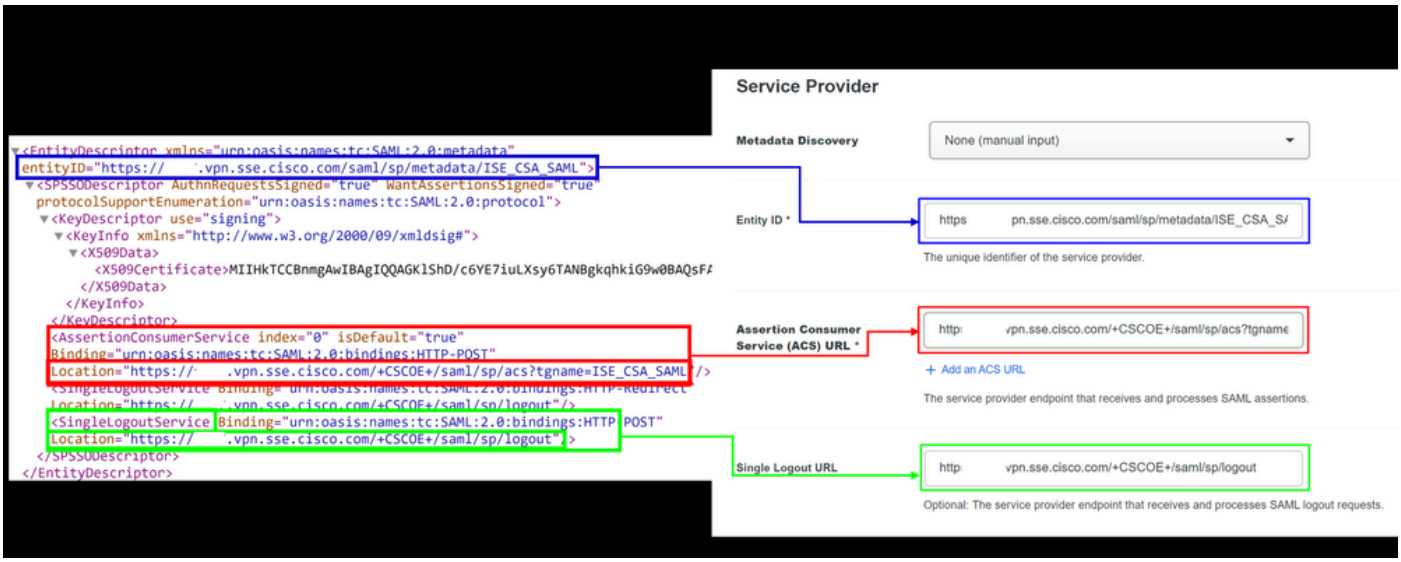
ISE_CSA

+ Add

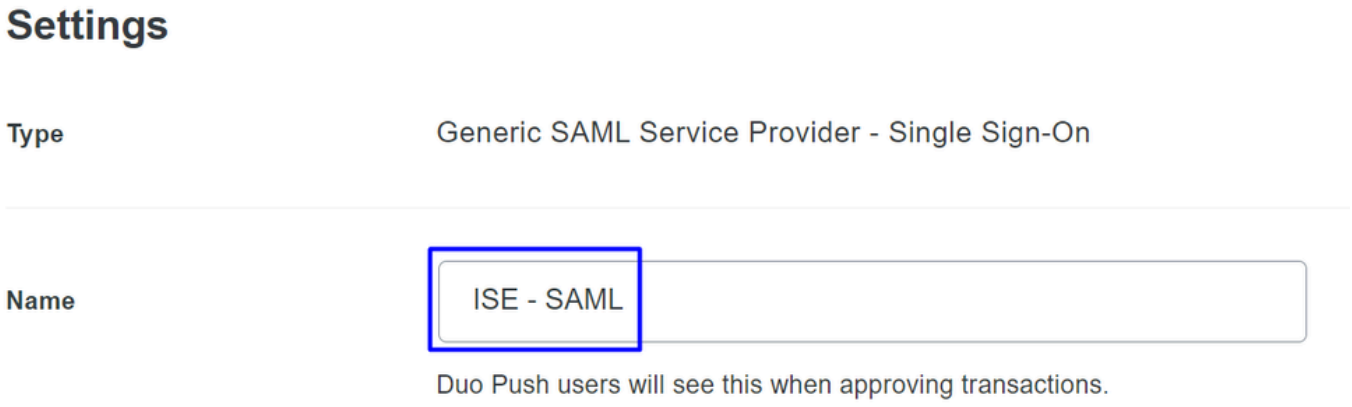
#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**:選択 **SAML**

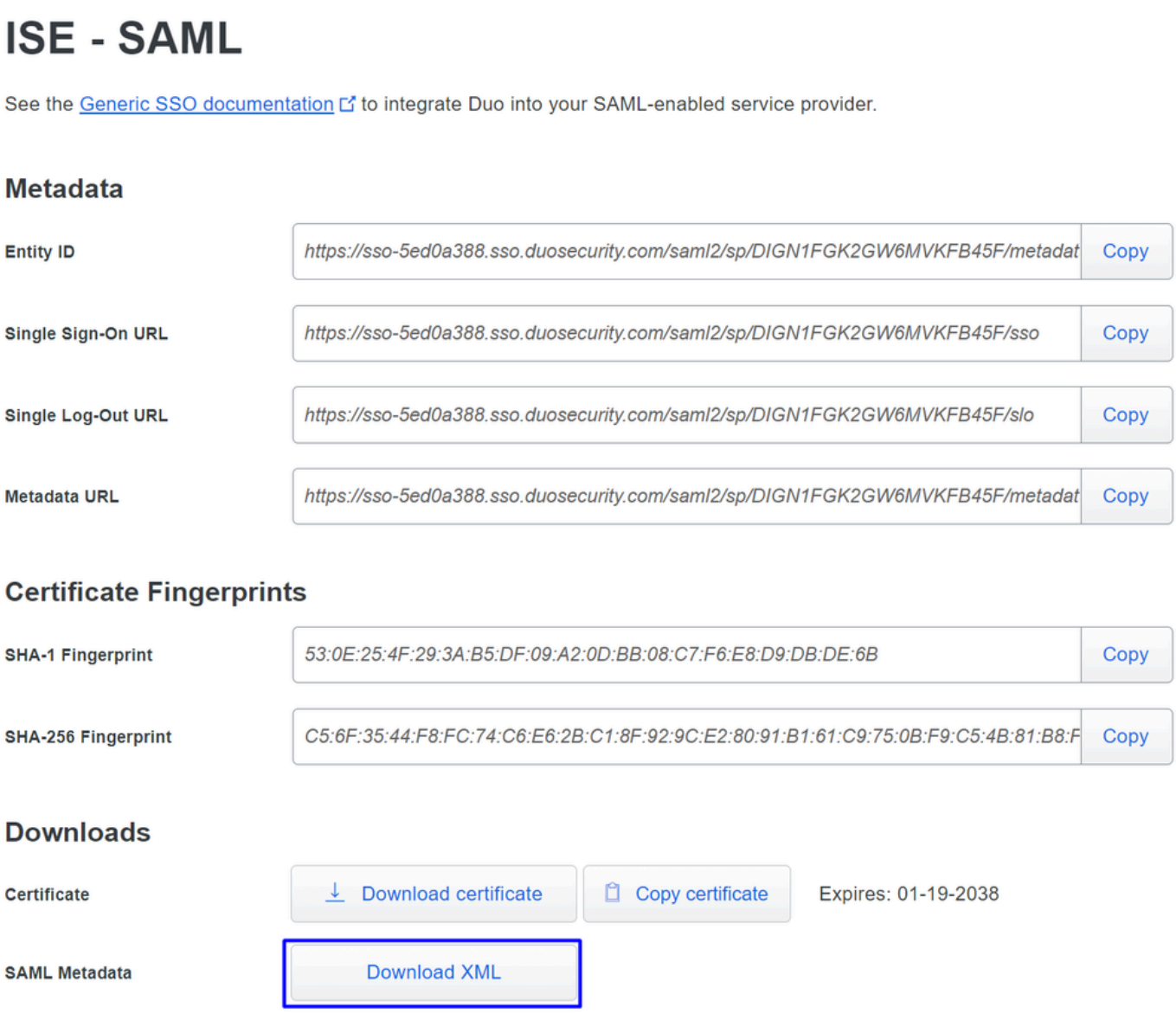
- クリック Download Service Provider XML file
- 手順「Duo Configuration」で設定したアプリケーションの情報を置き換えます。



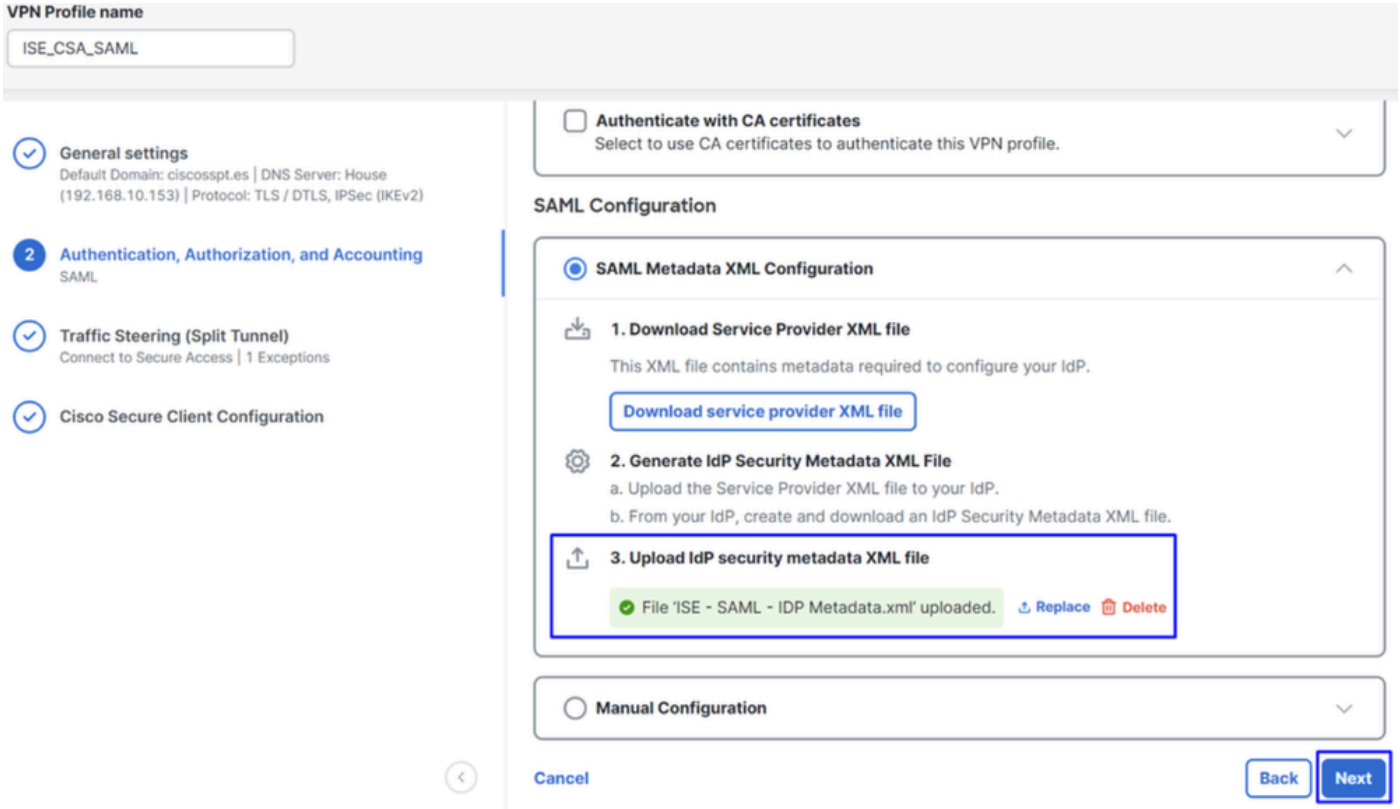
- その情報を設定したら、Duoの名前を、作成している統合に関連したものに変更します



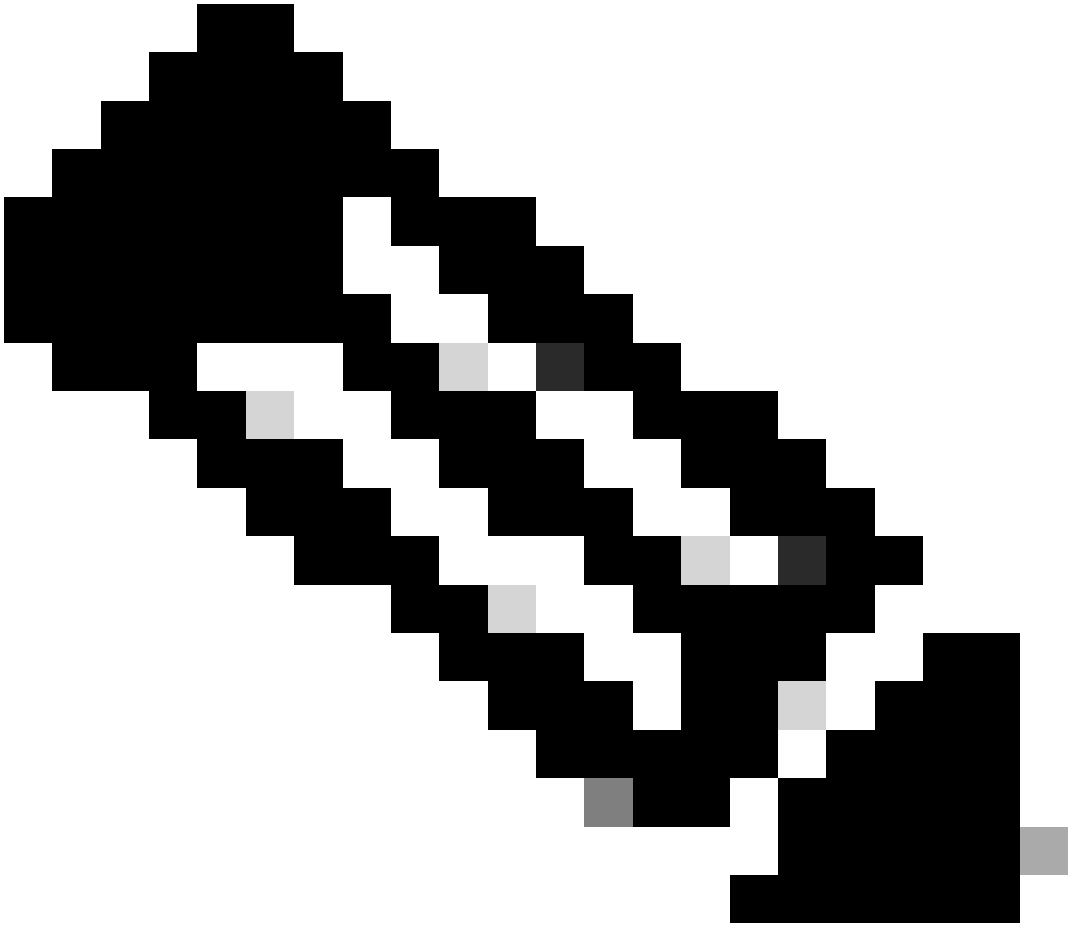
- Duoでアプリケ**Save** ーションをクリックします。
- Saveをクリックしたら、ボタンをクリックして**SAML Metadata** をダウンロードする必要があります **Download XML**



- オプションの下に**SAML Metadata** on Secure Accessをアップロード**3. Upload IdP security metadata XML file** し、 **Next**

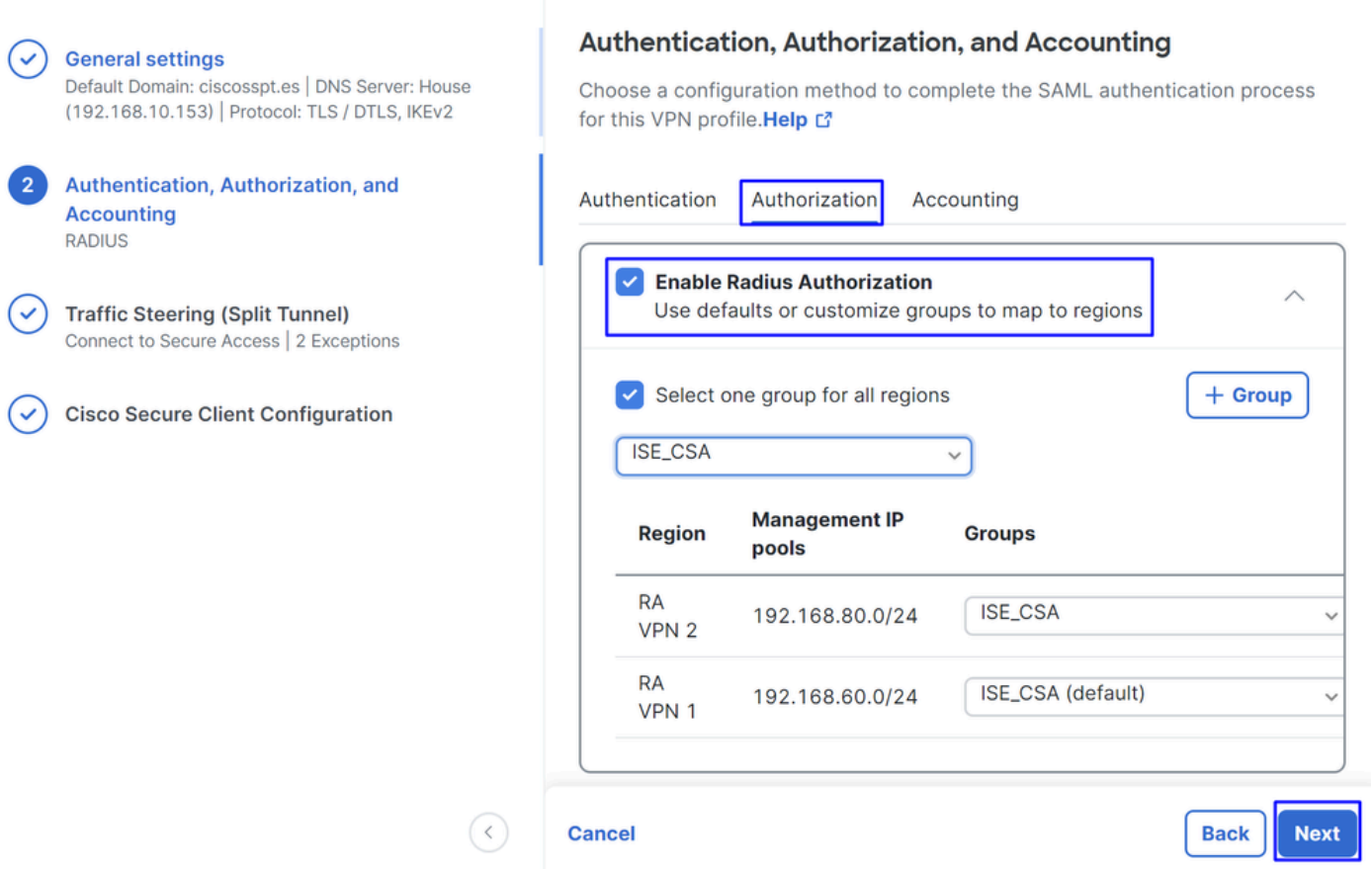

VPN Profile name
ISE_CSA_SAML
General settings
Default Domain: ciscosspt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPSec (IKEv2)
2
Authentication, Authorization, and Accounting
SAML
Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions
Cisco Secure Client Configuration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

許可に進みます。



注:SAMLで認証を設定すると、ISEを介して認証が認可されます。つまり、Secure Accessによって送信されるRADIUSパケットにはユーザ名のみが含まれます。ここではパスワードフィールドは存在しません。

許可



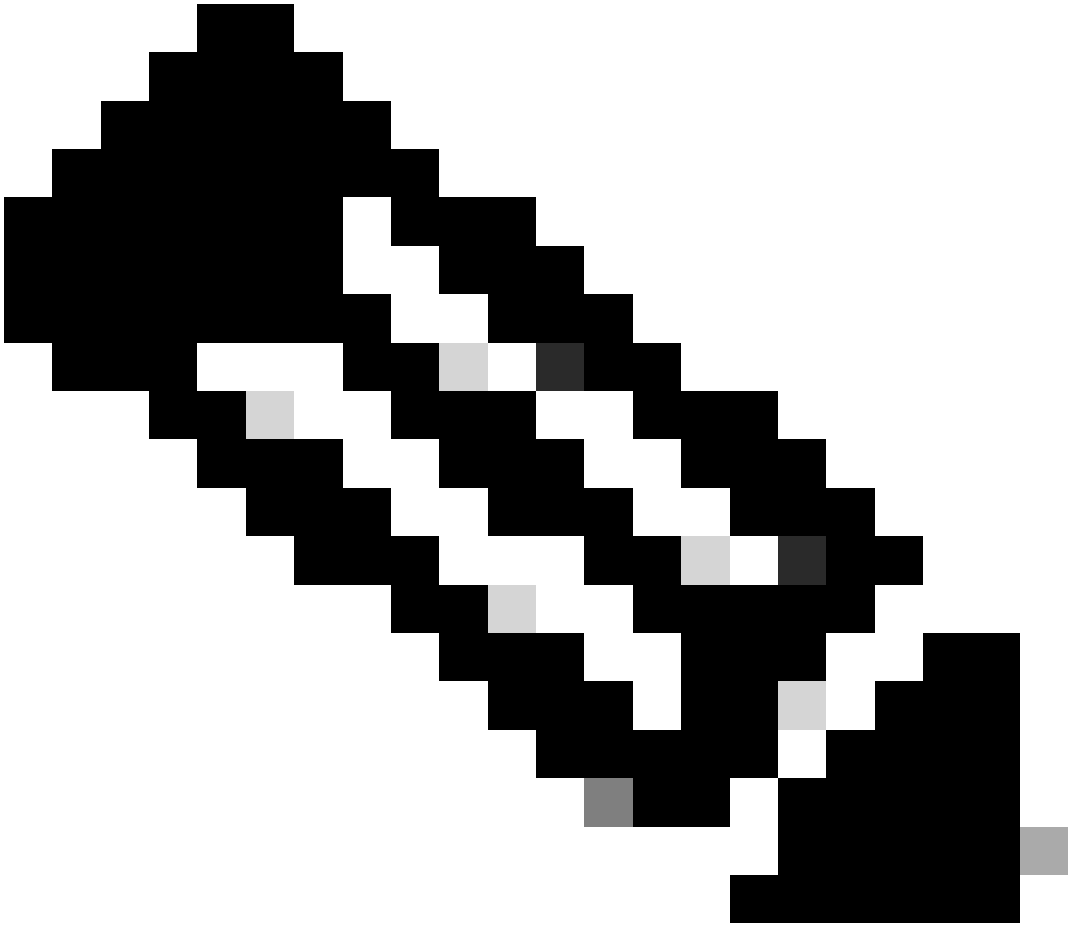
- **Authorization**

  - **Enable Radius Authorization**：チェックボックスをオンにして、RADIUS認証を有効にします。

    - すべてのリージョンに対して**1**つのグループを選択する：チェックボックスをオンにすると、すべてのリモートアクセス – バーチャルプライベートネットワーク(RA-VPN)プールに対して1つの特定のRADIUSサーバーが使用されます。または、プールごとに個別に定義します

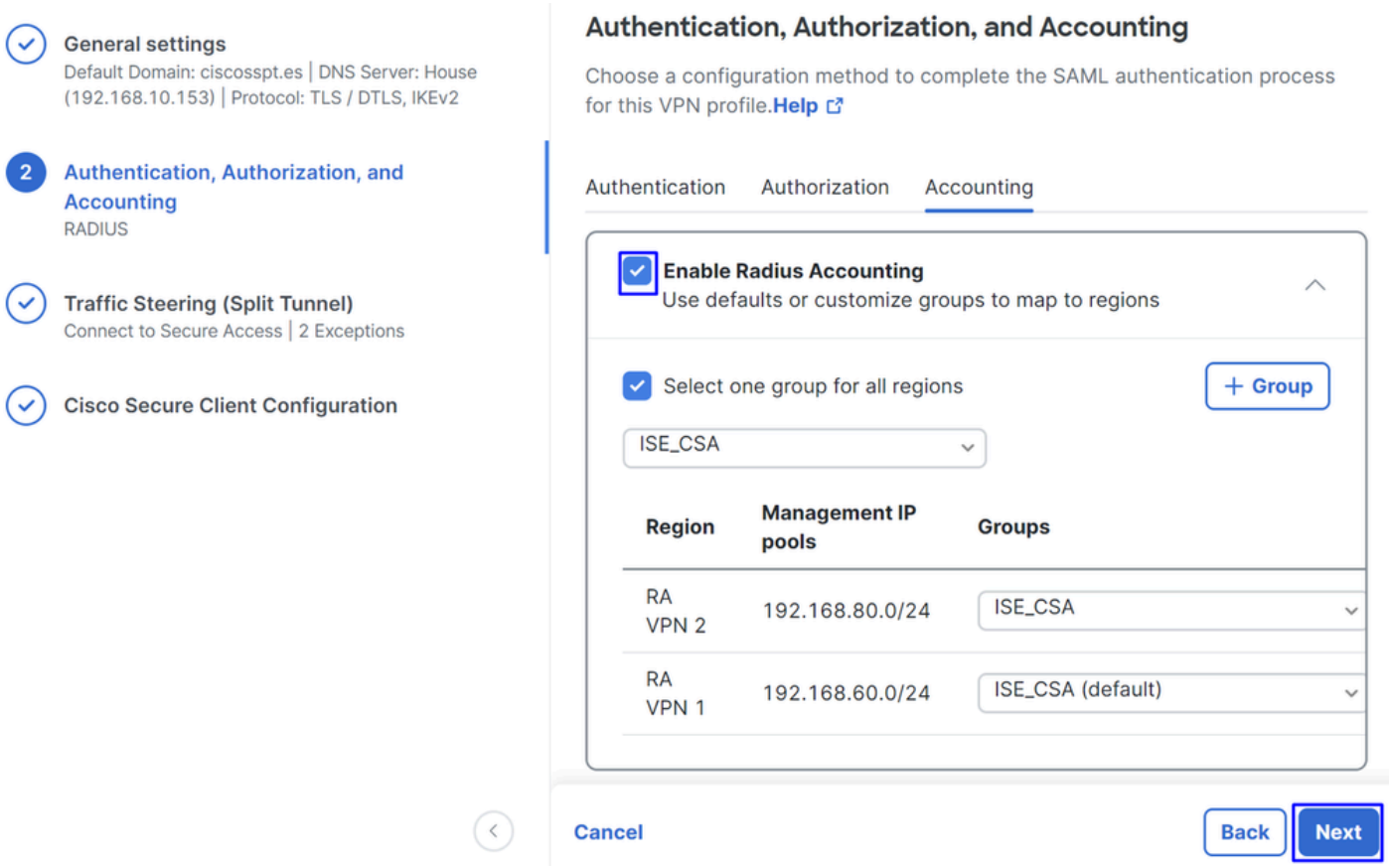
- クリック **Next**

すべての**Authorization** 部品を設定した後、 **Accounting**に進みます。



注: **Radio Authorization**を有効にしないと、ポスチャは機能しません。

アカウンティング

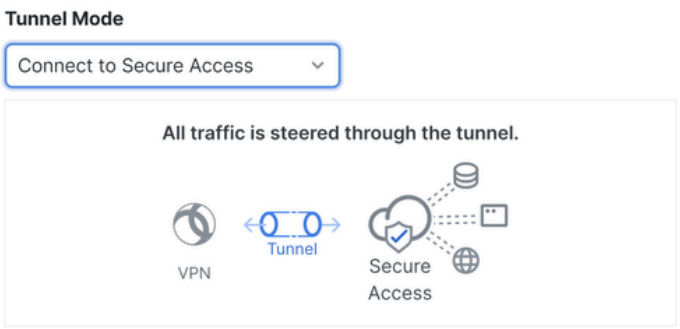


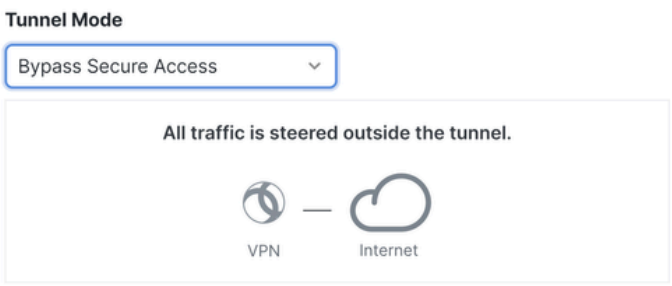
- **Accounting**
  - **Map Authorization groups to regions**：リージョンを選択し、 **Radius Groups**
- クリック **Next**

After you have done configured the Authentication, Authorization and Accounting 続行してくださいTraffic Steering。

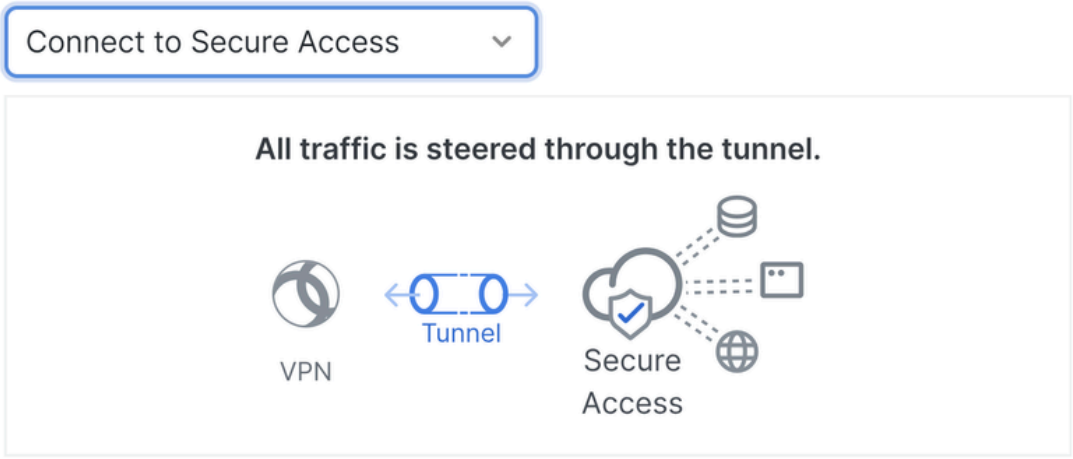
トラフィック誘導

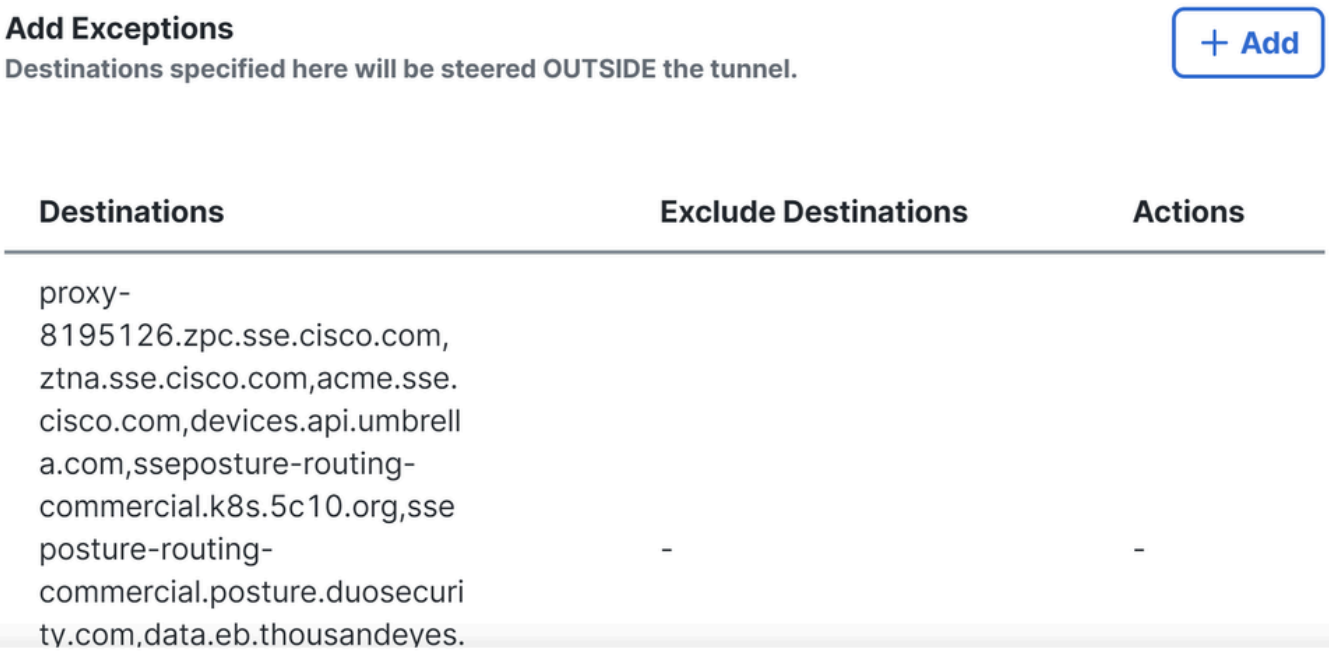
トラフィックステアリングの下で、セキュアアクセスを介した通信のタイプを設定する必要があります。





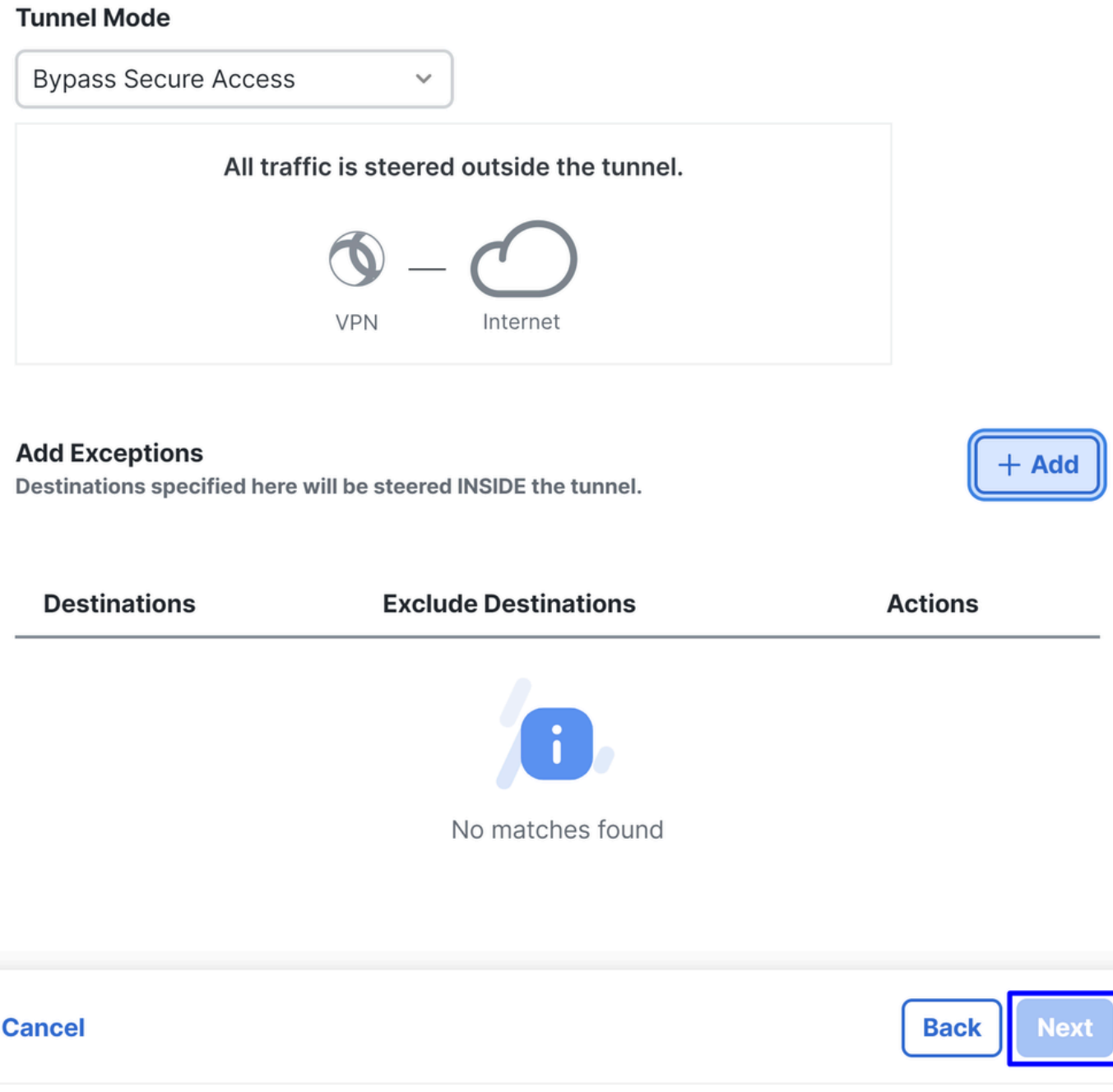
- **Connect to Secure Access**を選択すると、すべてのインターネットトラフィックは **Secure Access**

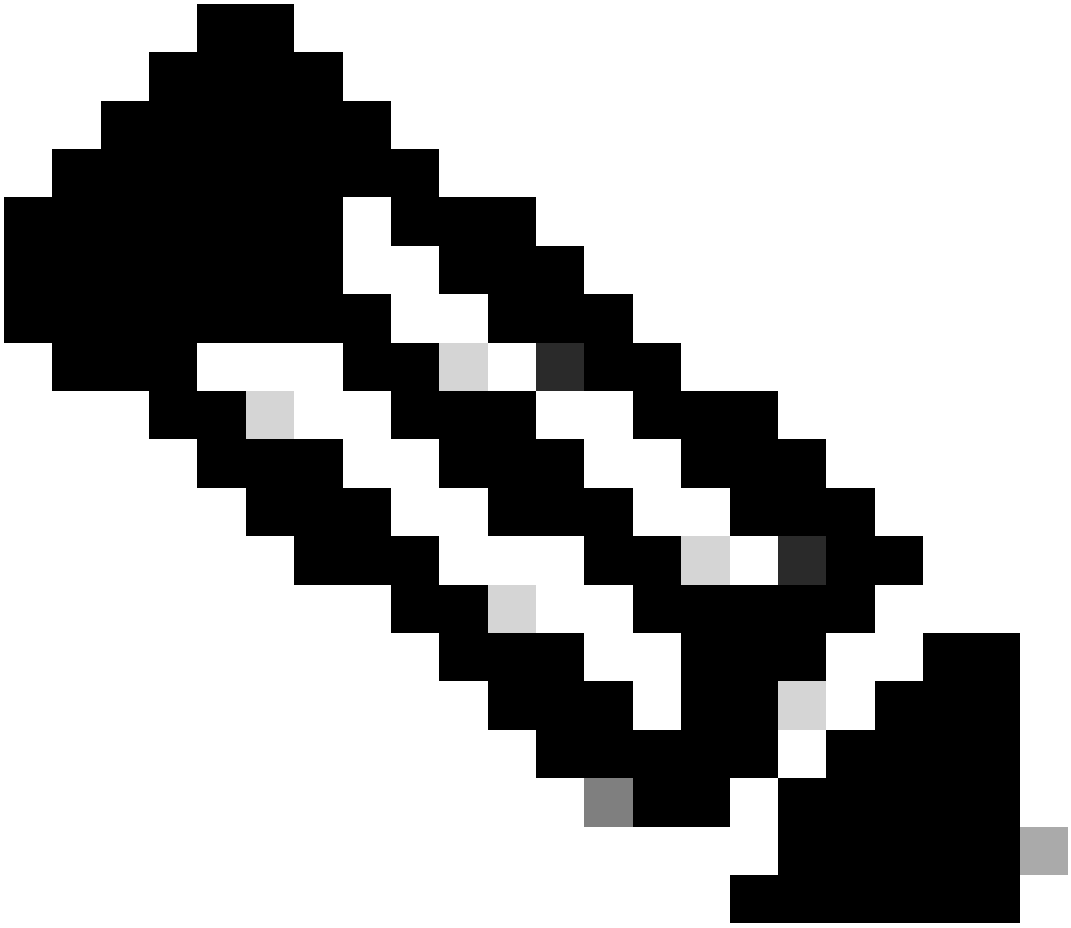




インターネットドメインまたはIPの除外を追加する場合は、**+ Add** ボタンをクリックし、**Next**をクリックします。

- **Bypass Secure Access**を選択した場合、すべてのインターネットトラフィックはSecure Access（インターネット保護なし）ではなく、インターネットプロバイダーを通過します

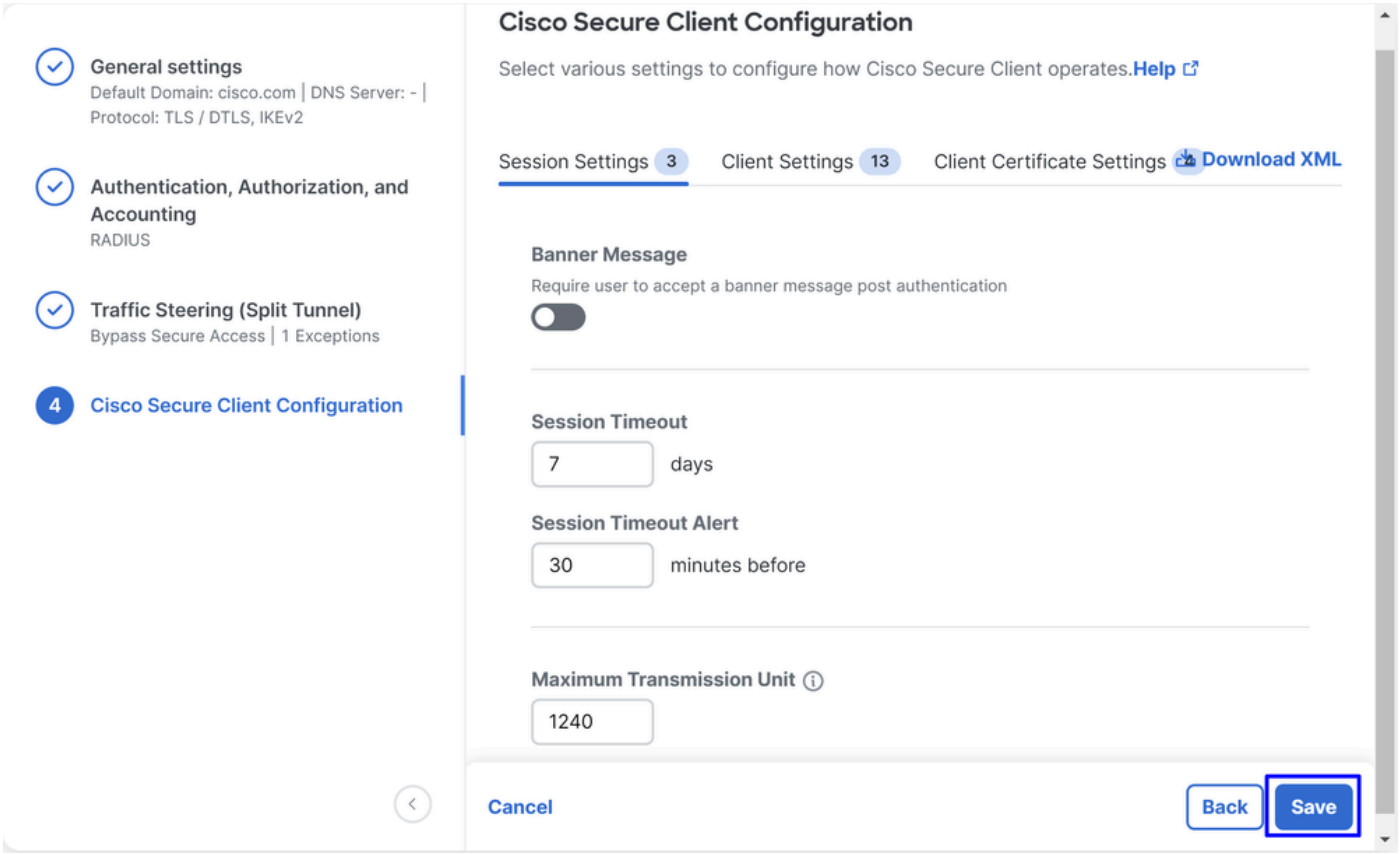




注:**Bypass Secure Access**を選択する際は、ISEポスチャに**enroll.cisco.com** を追加してください。

この手順では、VPN経由でアクセスするすべてのプライベートネットワークリソースを選択します。これを行うには、「**+ Add**」をクリックし、すべてのリソースを追加したら「**Next** 」をクリックします。

Cisco Secure Clientの設定



このステップでは、すべてをデフォルトのままにして「 **Save**」をクリックすることもできますが、設定をさらにカスタマイズする場合は、『Cisco Secure Client管理者ガイド』を確認してください。

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の設定

ネットワークデバイスのリストの設定

Cisco ISE経由で認証を設定するには、Cisco ISEに対してクエリを実行できる許可デバイスを設定する必要があります。

- 移動先 **Administration** > **Network Devices**
- クリック + **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

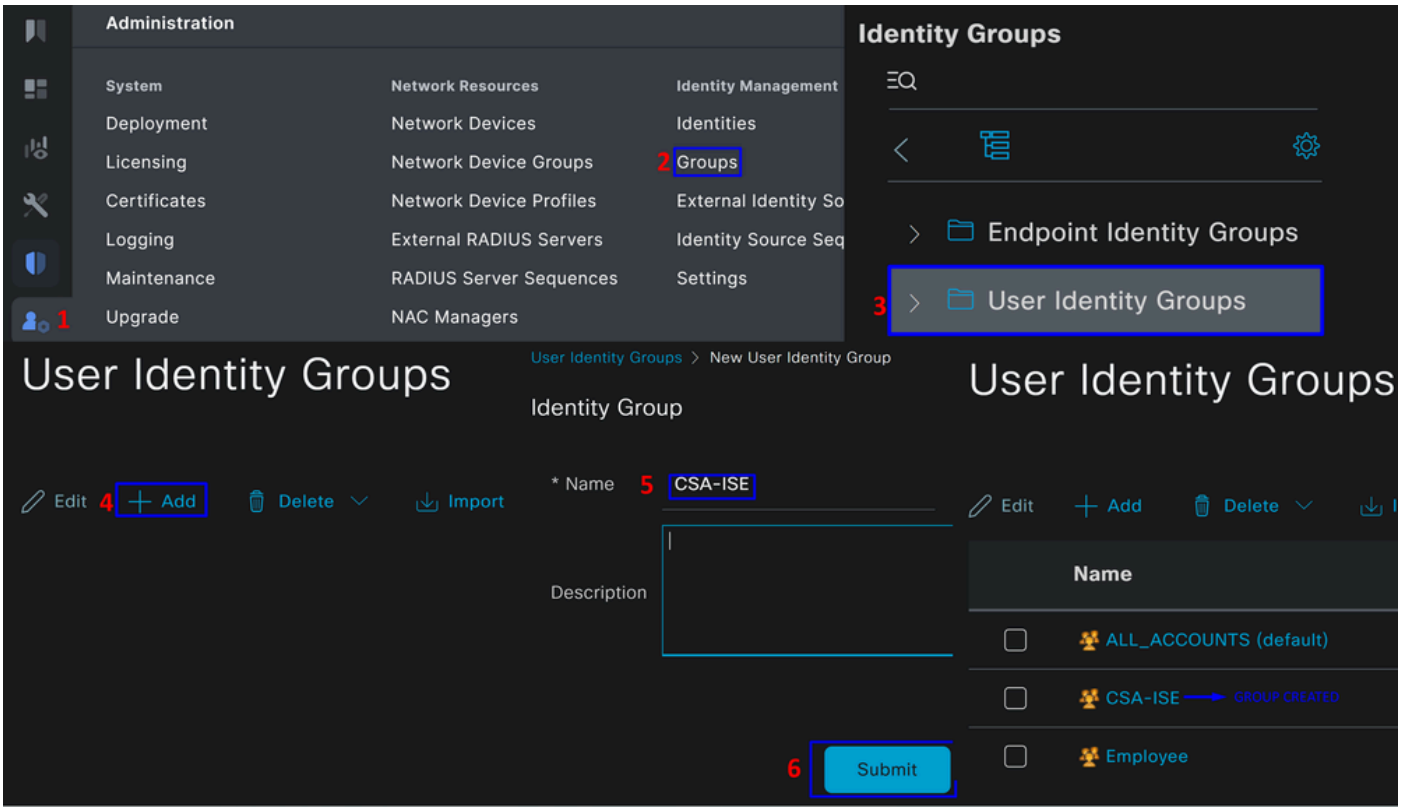
- **Name**：名前を使用してセキュアアクセスを識別する
- **IP Address**：ステップのManagement Interface、IPプール領域を設定します。
- **Device Profile**：シスコを選択
    - **Radius Authentication Settings**
        - Shared Secret：ステップで設定したのと同じ共有秘密を設定します(秘密キー)。
            - **CoA Port**：デフォルトのままにしておきます。セキュアアクセスでは1700も使用されます。

その後、**Save**をクリックして、統合が正しく機能するかどうかを確認してから、統合検証用のローカルユーザの作成に進みます。

グループの設定

ローカルユーザで使用するグループを設定するには、次の手順を実行します。

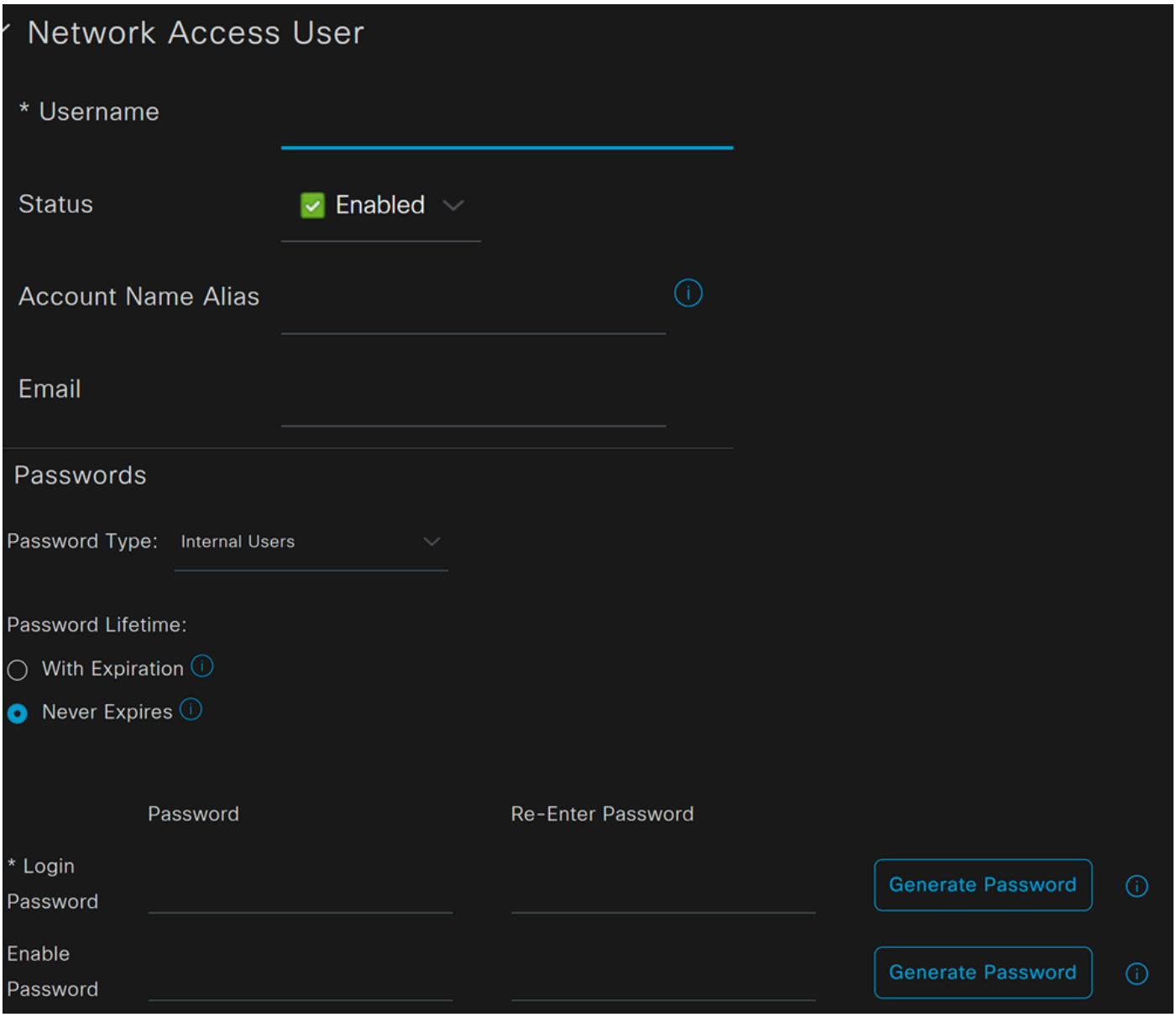
- クリック **Administration** > **Groups**
- クリック **User Identity Groups**
- クリック + Add
- グループのNameを作成し、 **Submit**

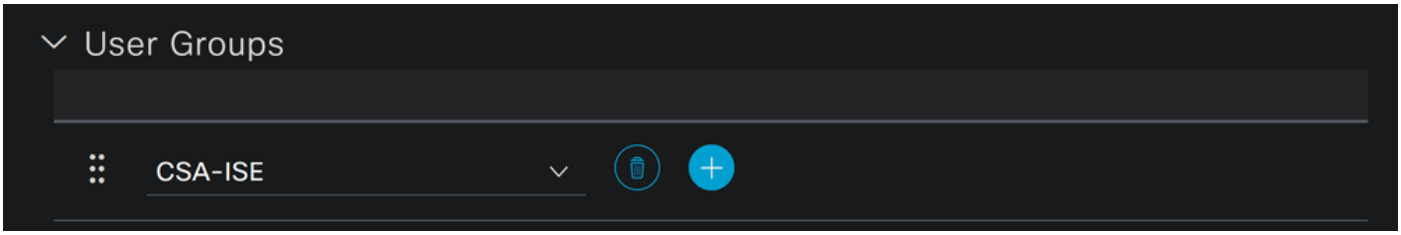


ローカルユーザの設定

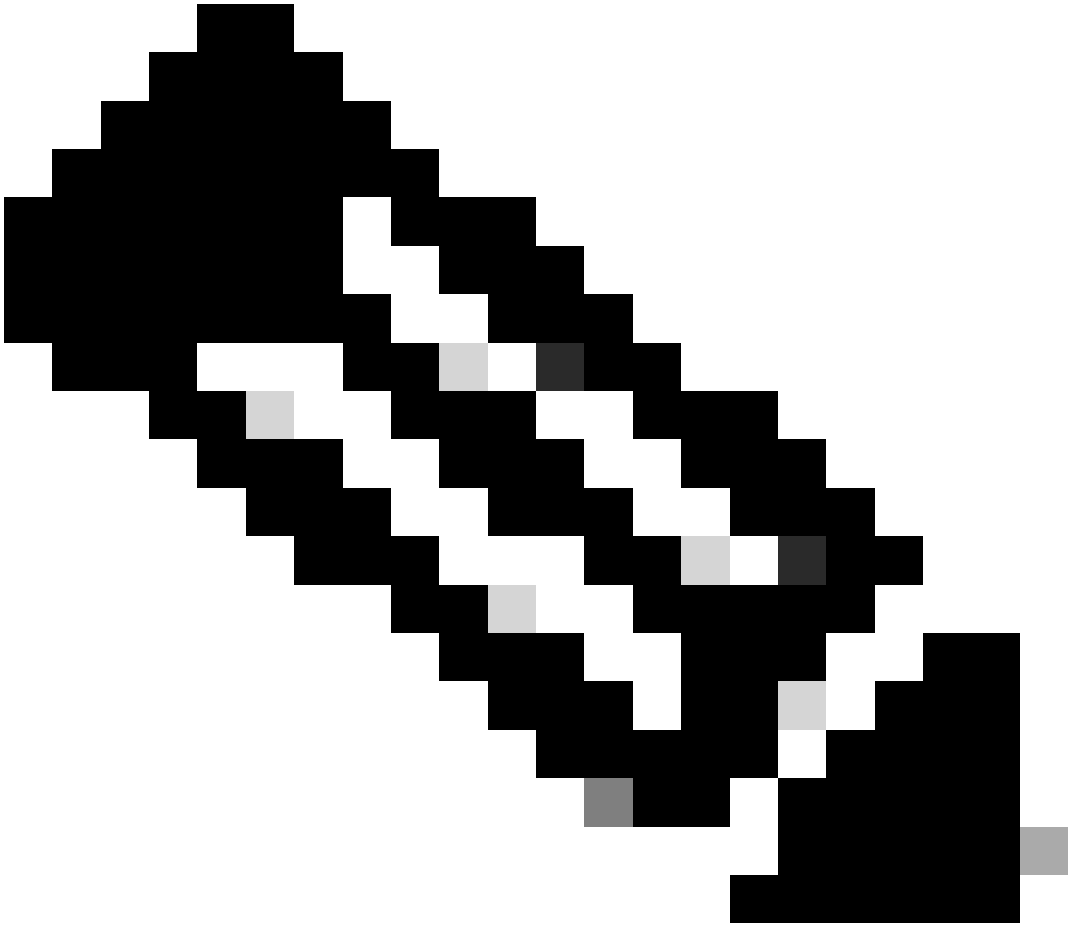
統合を確認するようにローカルユーザを設定するには、次の手順を実行します。

- 移動先 **Administration** > **Identities**
- クリック **Add** +





- **Username**：セキュアアクセスで既知のUPNプロビジョニングを使用してユーザ名を設定します。これは、手順「前提条件
- **Status**:アクティブ
- **Password Lifetime**：設定する**With Expiration** か、Never Expiresを使用します
- **Login Password**：ユーザのパスワードを作成します。
- **User Groups**：ステップ「グループの設定」で作成したグループを選択します。



注:UPNに基づく認証は、セキュアアクセスの今後のバージョンで変更されるように設定されています。

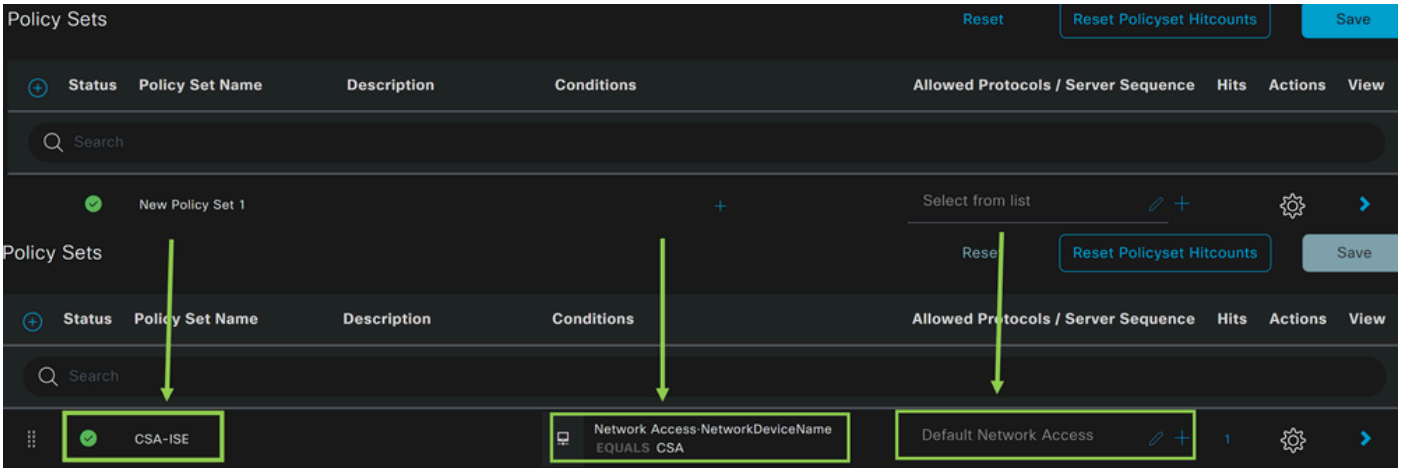
その後、設定**Save** を行い、 **Configure Policy Set**の手順に進みます。

ポリシーセットの設定

ポリシーセットの下で、認証および認可時にISEが実行するアクションを設定します。このシナリオでは、ユーザアクセスを提供する簡単なポリシーを設定する使用例を示します。最初に、ISEはRADIUS認証の送信元を確認し、アクセスを提供するためにISEユーザデータベースにIDが存在するかどうかを確認します

このポリシーを設定するには、Cisco ISEダッシュボードに移動します。

- クリック Policy > Policy Sets
- 新しいポリシーセットを追加するには、+ をクリックします。



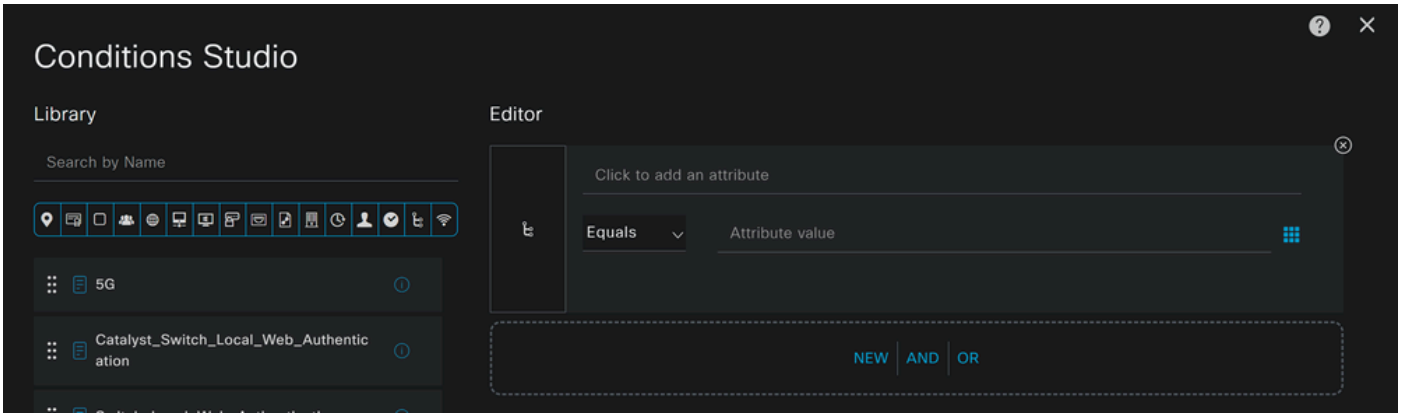
この場合は、デフォルトのポリシーセットで動作するのではなく、新しいポリシーセットを作成します。次に、そのポリシーセットに基づいて認証と認可を設定します。設定されたポリシーは、「ネットワークデバイスのリストの設定」の手順で定義されたネットワークデバイスへのアクセスを許可し、これらの認証がCSA Network Device Listから到達したことを確認してから、**Conditions**としてポリシーに到達するようにします。最後に、**Default Network Access**のように、許可されるプロトコルです。

ポリシーセットに一致する**condition** を作成するには、次の手順に進みます。

- クリック +

Condition Studio

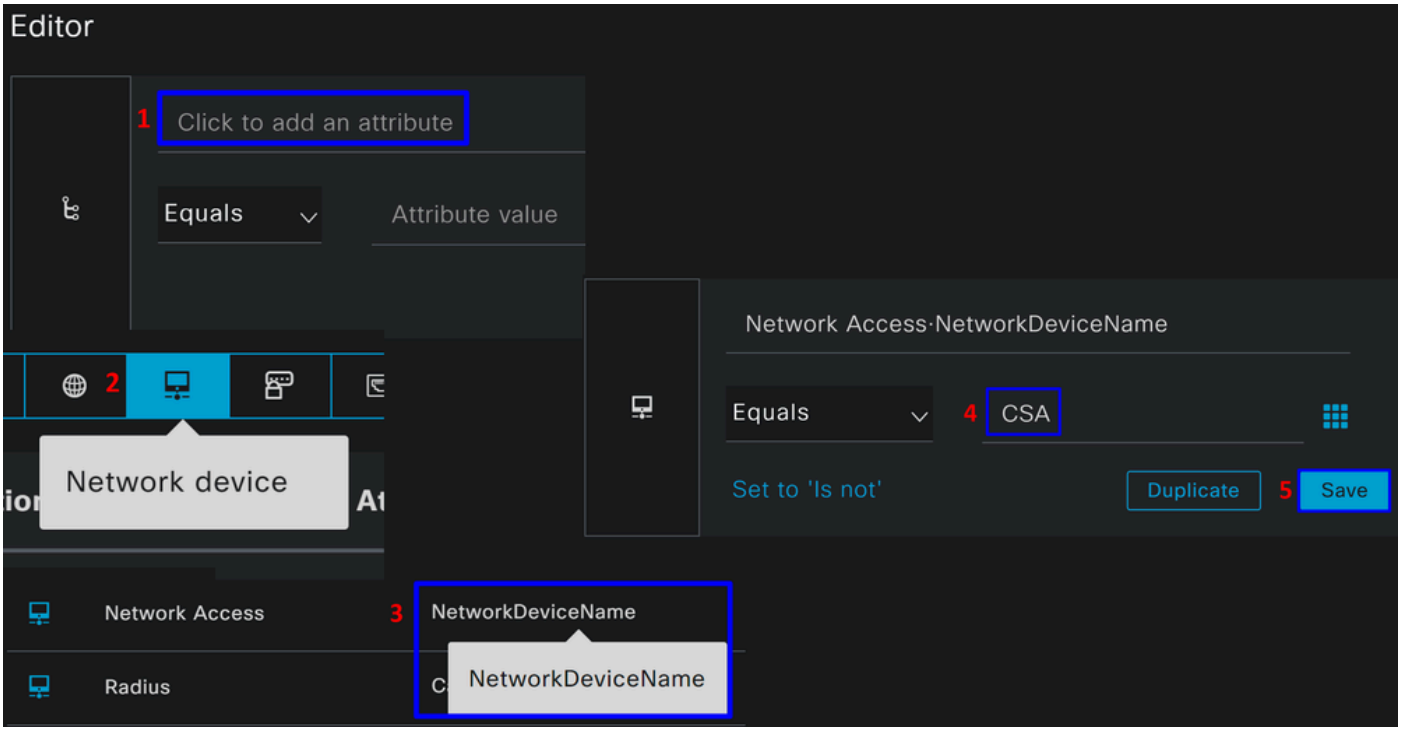
- で使用可能な情報は次のとおりです。



- 条件を作成するには、 Click to add an attribute
- ボタ**Network Device** ンをクリックします。
- 背後にあるオプションの下で、「**Network Access - Network Device Name** option」をクリックします。

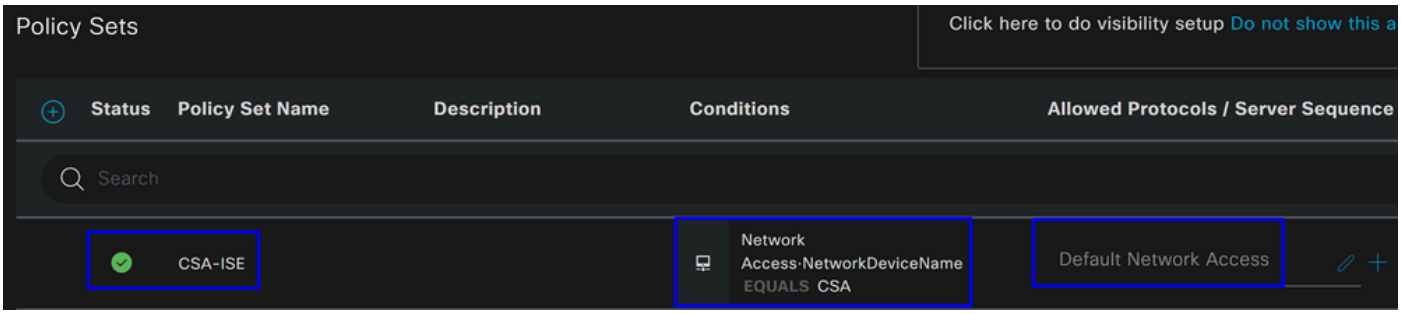
- Equalsオプションの下に、手順Configure Network Devices Listの下のNetwork Device の名前を書き込みます

- クリック **Save**



このポリシーは、ポリシーセットに基づいてCSA**Authentication** および**Authorization** 設定を続行するための送信元からの要求だけを承認し、許可されたプロトコルに対して **CSA-ISE**に基づいて許可されたプロトコル **Default Network Access** を検証します。

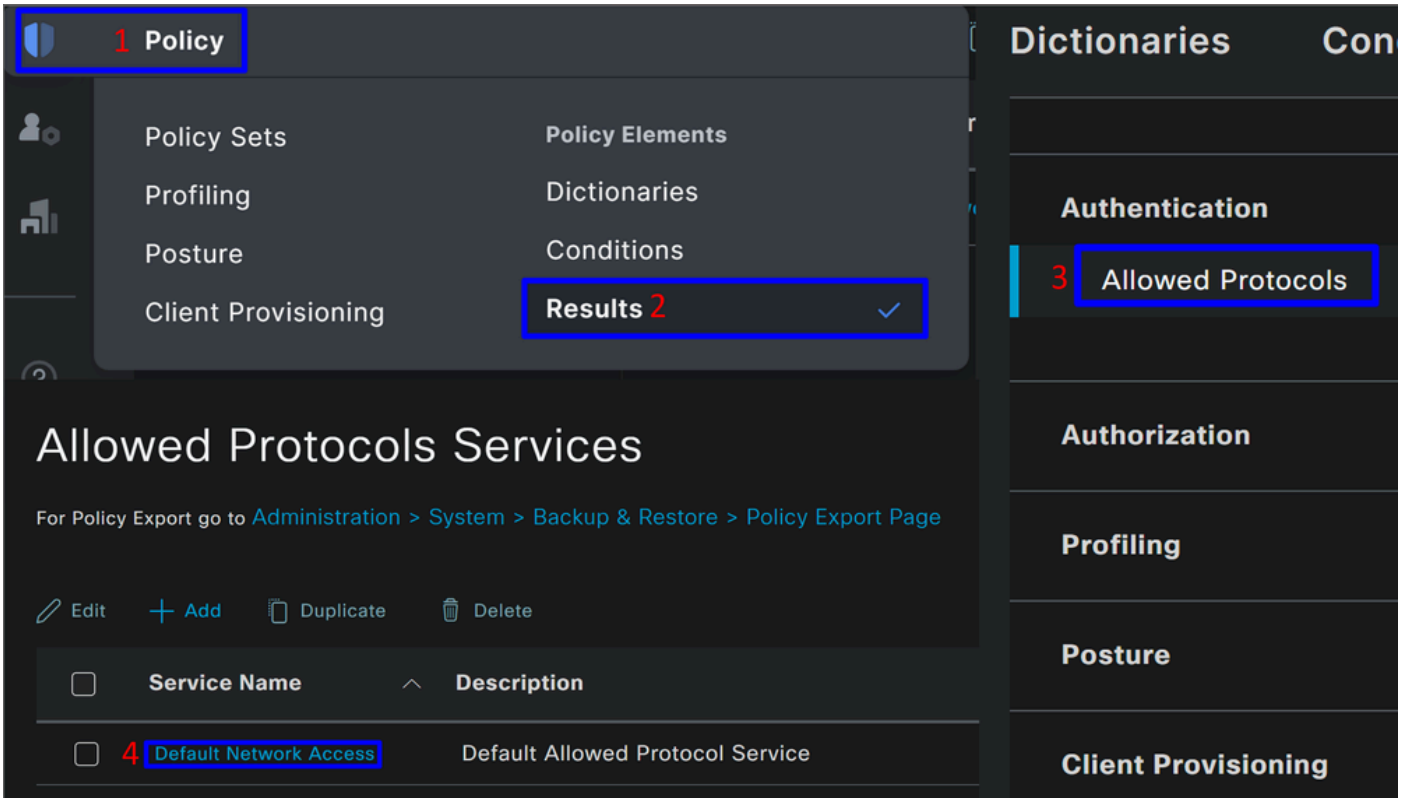
定義されたポリシーの結果は次のようになります。



- **Default Network Access Protocols** が許可されていることを確認するには、次の手順に進みます。

  - クリックPolicy > Results

    - クリック **Allowed Protocols**
    - クリック **Default Network Access**

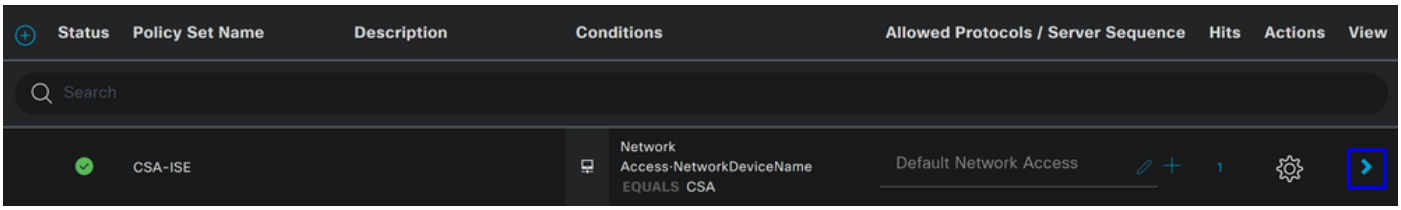


- 次に、許可されているすべてのプロトコルが表示されます **Default Network Access**

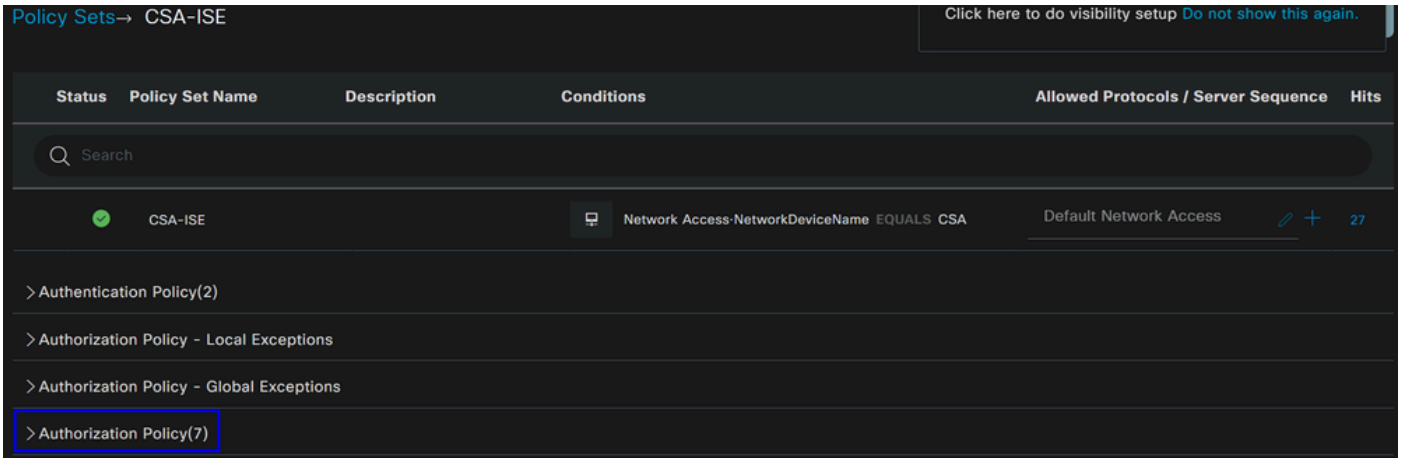
ポリシーセット許可の設定

Policy Setの下にポ**Authorization** リシーを作成するには、次の手順に進みます。

- クリック >



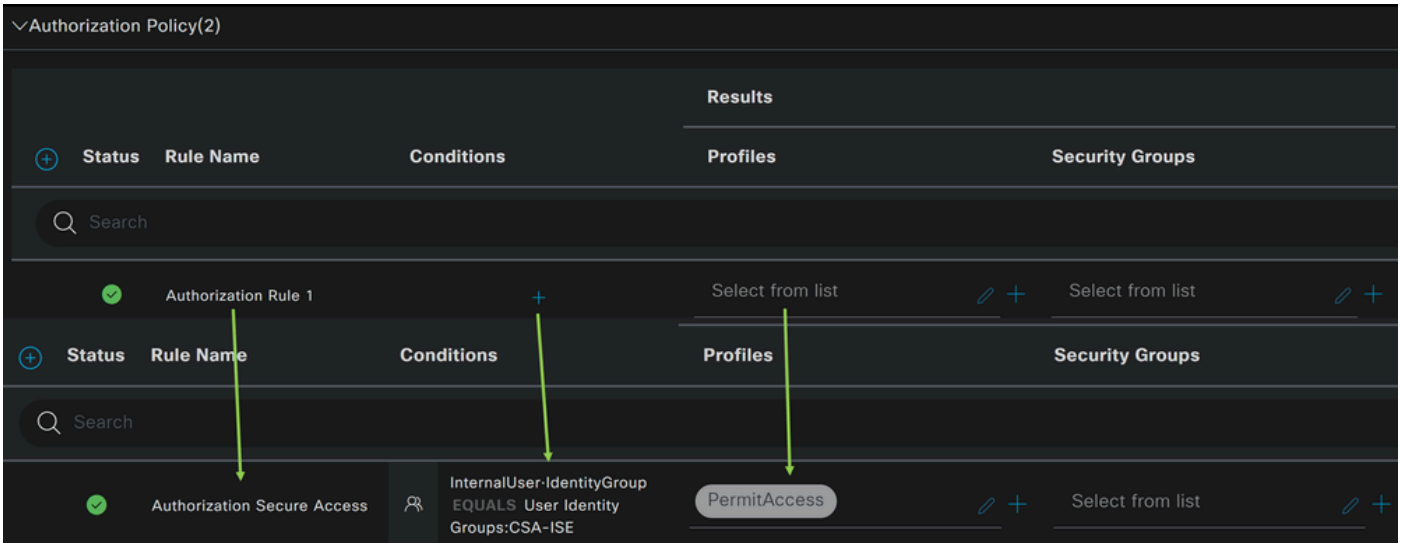
- その後、表示されるポリシー**Authorization** が表示されます。



ポリシーは、[ポリシーセットの設定](#)のステップで定義したポリシーと同じです。

認可ポリシー

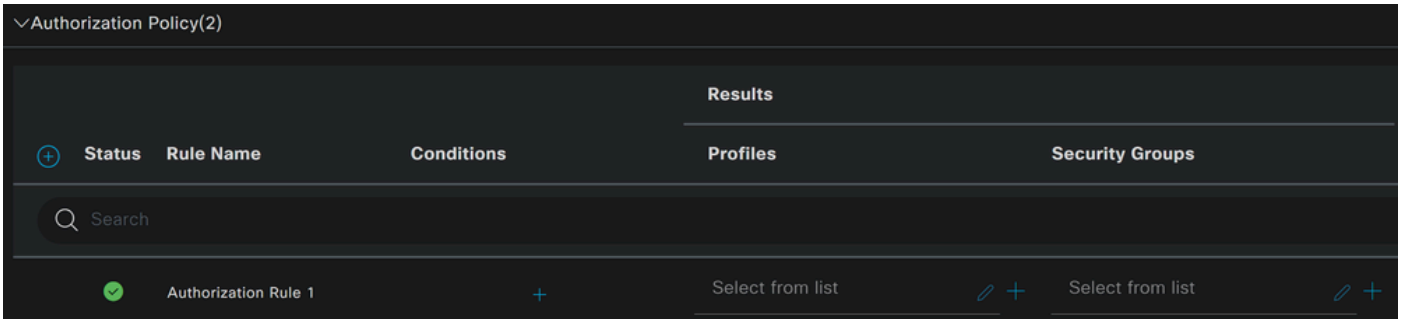
認可ポリシーはさまざまな方法で設定できます。この場合、「グループの設定」の手順で定義したグループ内のユーザだけを認可します。認可ポリシーを設定するには、次の例を参照してください。



- クリック **Authorization Policy**

+

- をクリックして、次のような認可のポリシーを定義します。



- 次の手順では、Rule NameConditions および Profiles

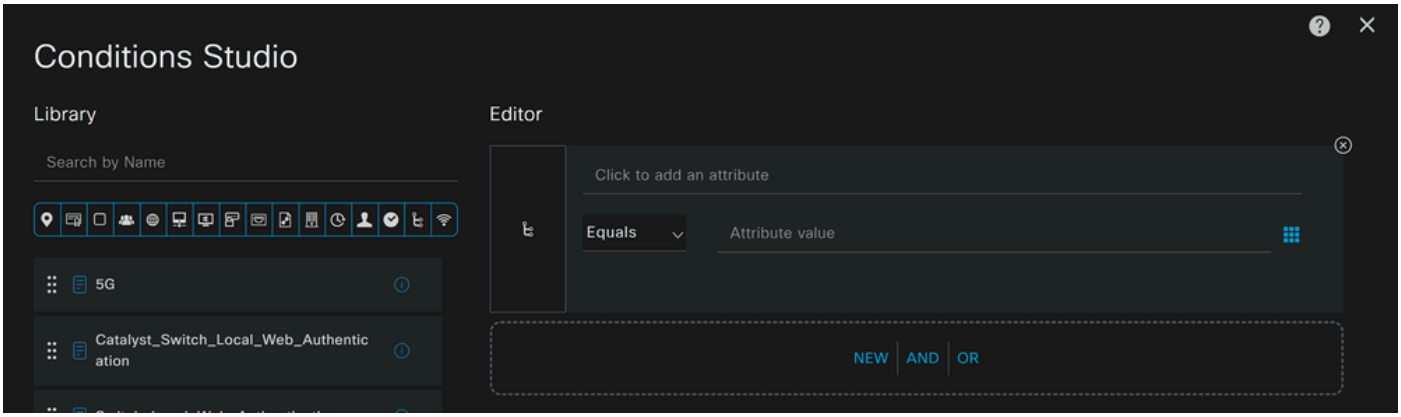
- 認可ポリシーを簡単に識別できるように名前を設**Name** 定する場合

Condition

- を設定するには、 +

Condition Studio

- の下に、次の情報があります。



- 条件を作成するには、 Click to add an attribute

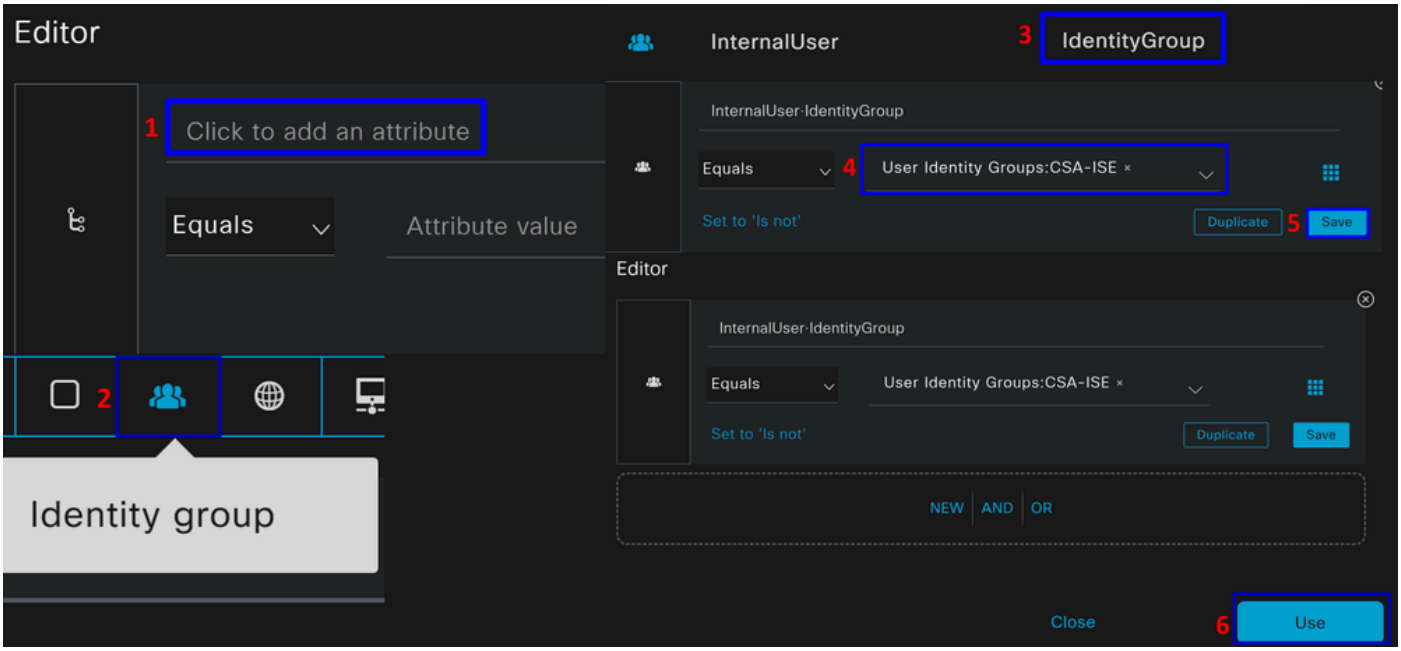
- ボタ**Identity Group** ンをクリックします。

- 背後にあるオプションで**Internal User** - **IdentityGroup** optionをクリックします

- オプ**Equals** ションの下のドロップダウンを使用して、手順「Configure a Group」で認証の承**Group** 認済みを見つけます

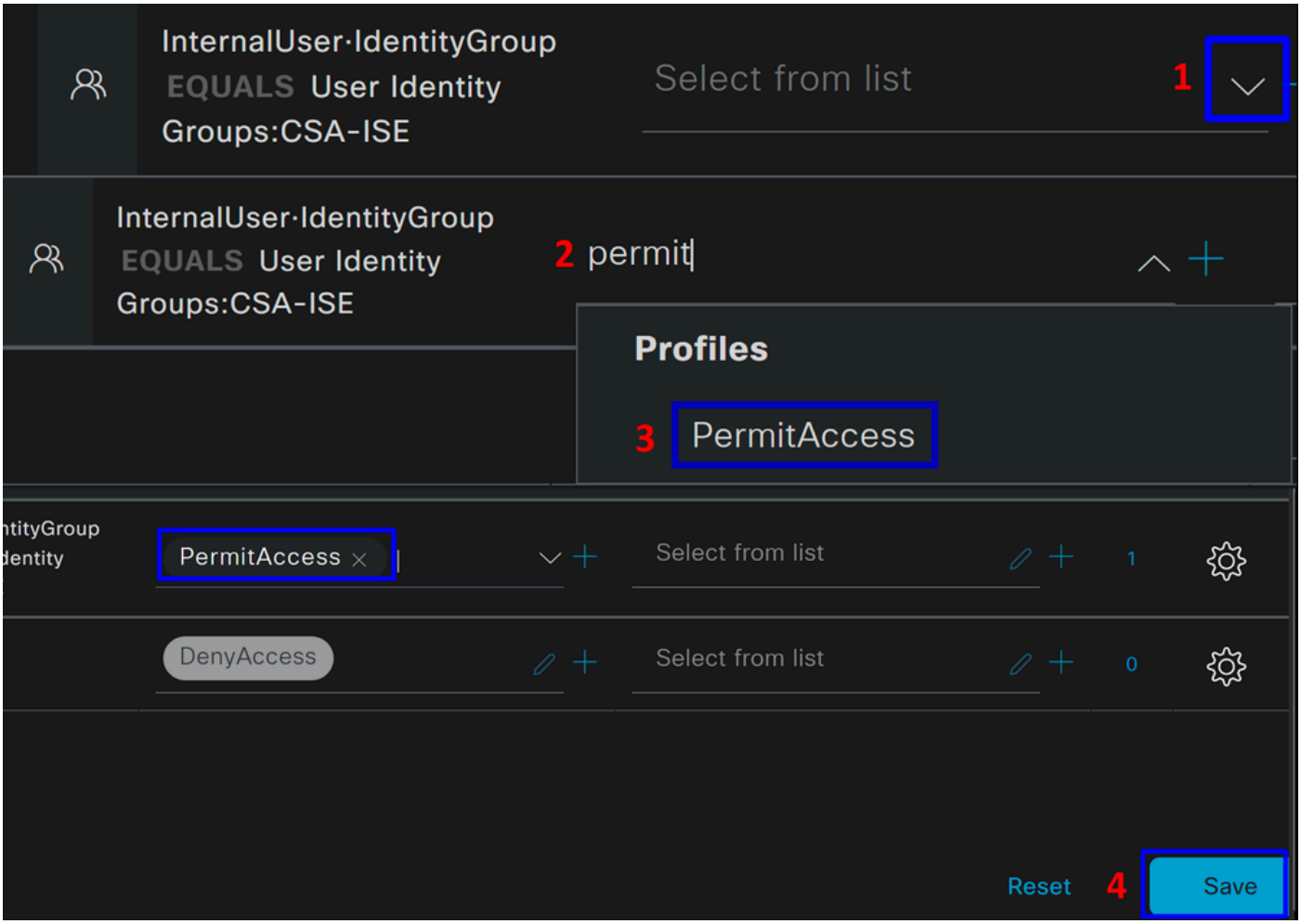
- クリック **Save**

- クリック **Use**



その後で、 **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- 「 **Authorization Policy**」の下にあるドロップダウンボタンをクリックして、 **Profiles**
- 許可の検索
- 選択 **PermitAccess**
- クリック Save

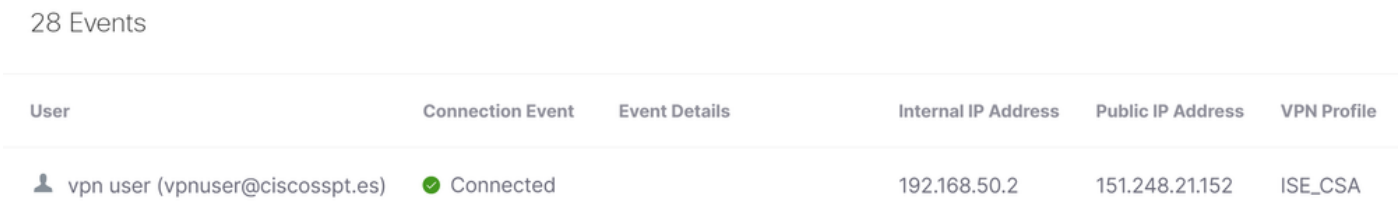


その後、ポ **Authorization** リシーを定義しました。ユーザが問題なく接続するかどうか、およびセキュアアクセスとISEの口グを表示できるかどうかを確認するために認証します。

VPNに接続するには、セキュアアクセスで作成されたプロファイルを使用し、ISEプロファイルを使用してセキュアクライアント経由で接続します。

- **認証が承認されると、セキュアアクセスでログはどのように表示されますか。**
  - セキュアアクセスダッシュボードに移動します

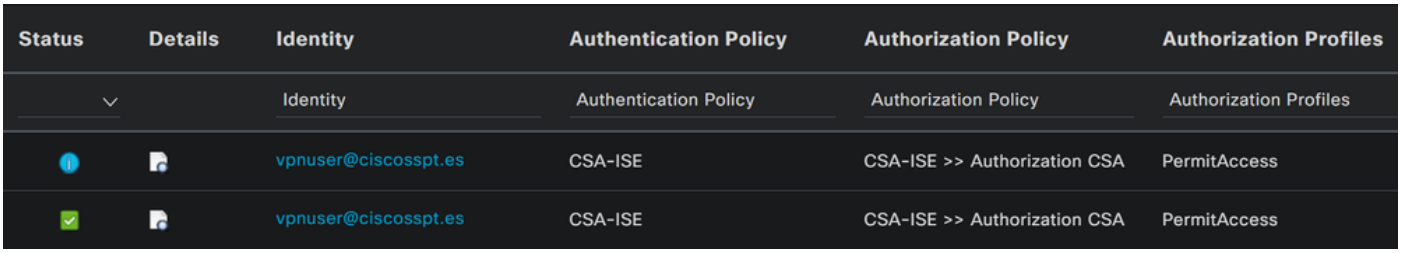
- クリック **Monitor** > **Remote Access Log**



- **認証が承認されると、ログはどのようにISEに表示されますか。**

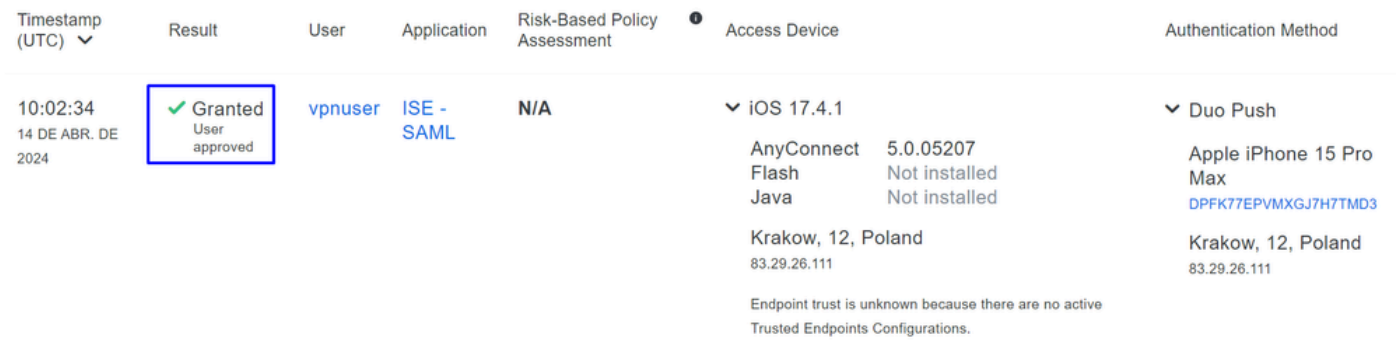
  - に移動します。 **Cisco ISE Dashboard**

    - クリック **Operations** > **Live Logs**



認証が承認されると、Duoでログはどのように表示されますか。

- Duo Admin Panelに移動します。
- クリック **Reports** > **Authentication Log**



RADIUSローカルまたはActive Directoryユーザの設定

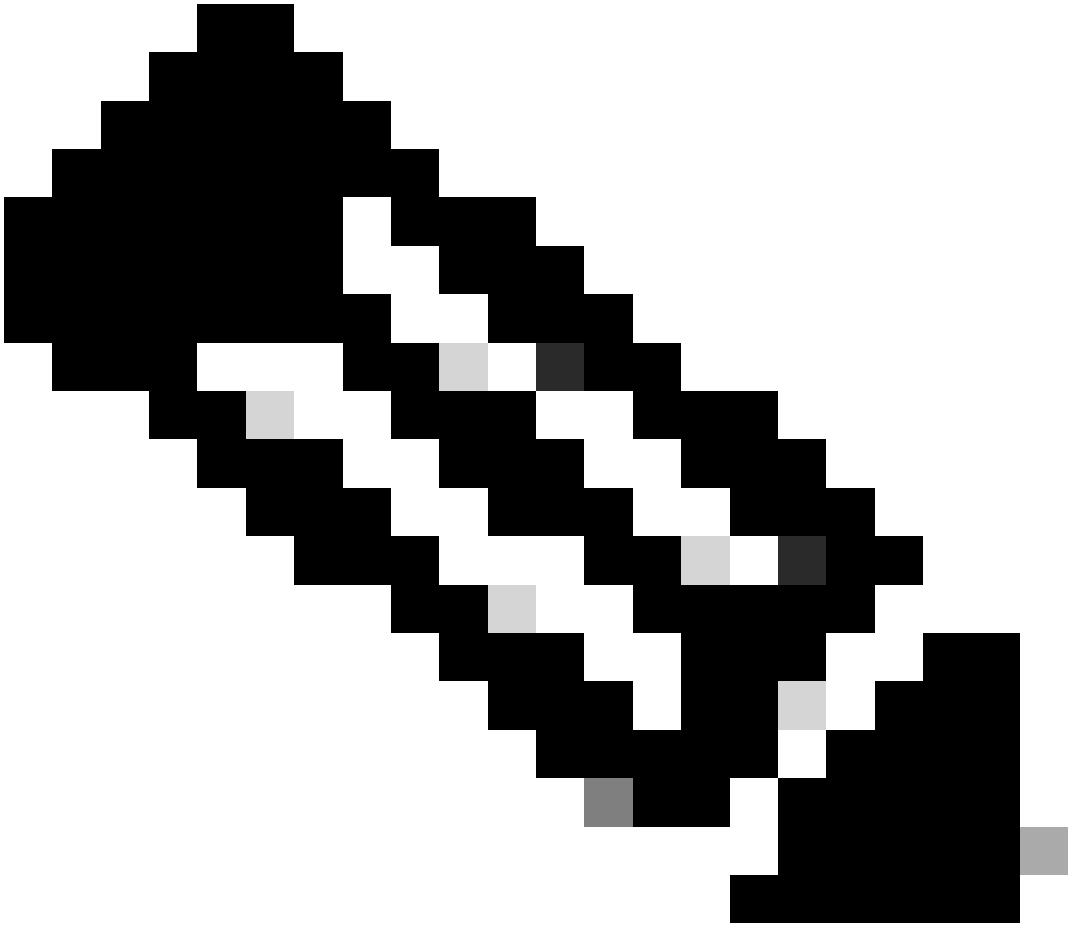
ISEポスチャの設定

このシナリオでは、内部リソースへのアクセスを許可または拒否する前に、エンドポイントのコンプライアンスを確認する設定を作成します。

これを設定するには、次の手順に進みます。

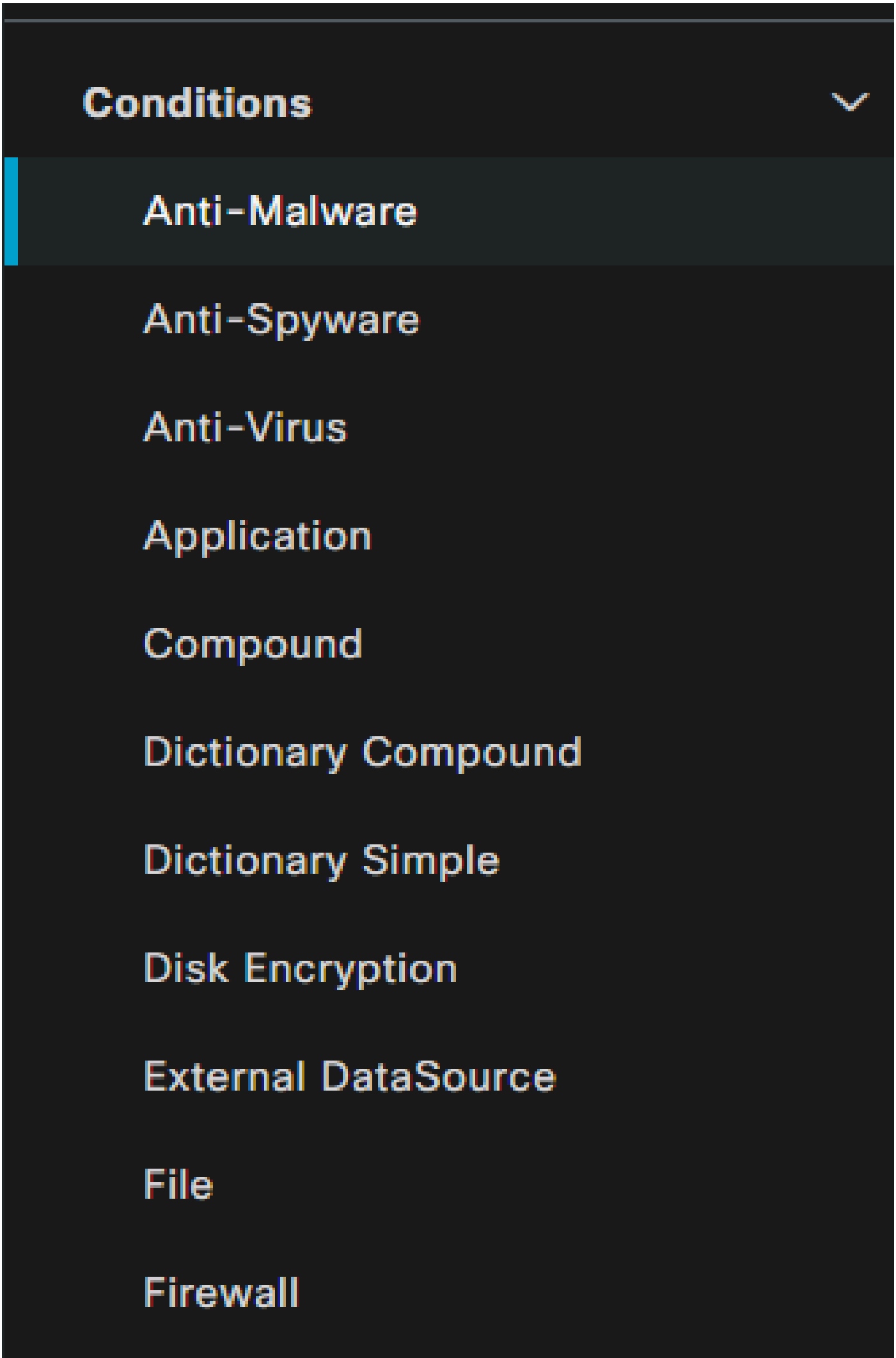
ポスチャ条件の設定

- ISEダッシュボードに移動します
- クリック **Work Center** > **Policy Elements** > **Conditions**
- クリック **Anti-Malware**



注：デバイスのポスチャを確認し、内部ポリシーに基づいて正しい評価を行うための多くのオプションがあります。

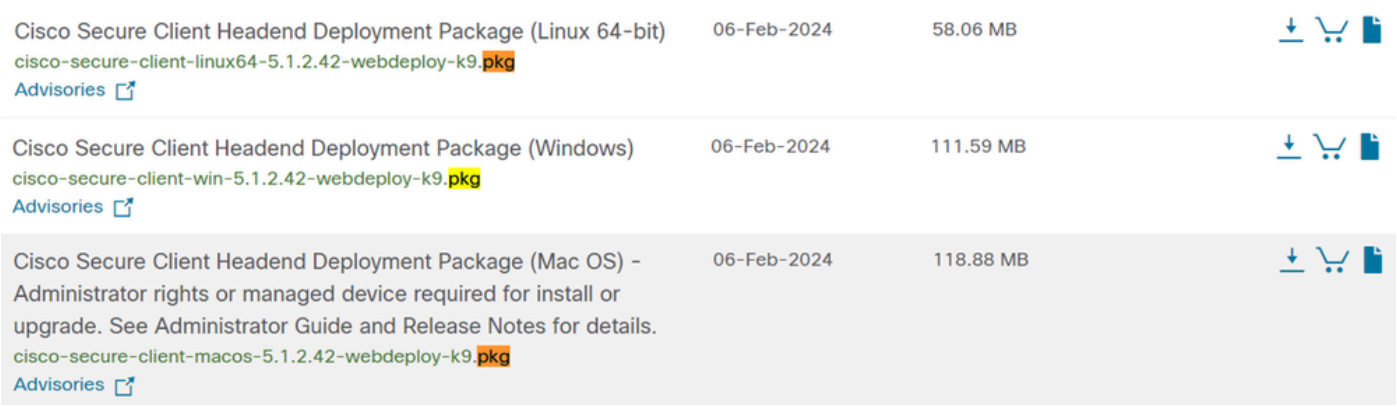
Anti-Malware Conditions


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

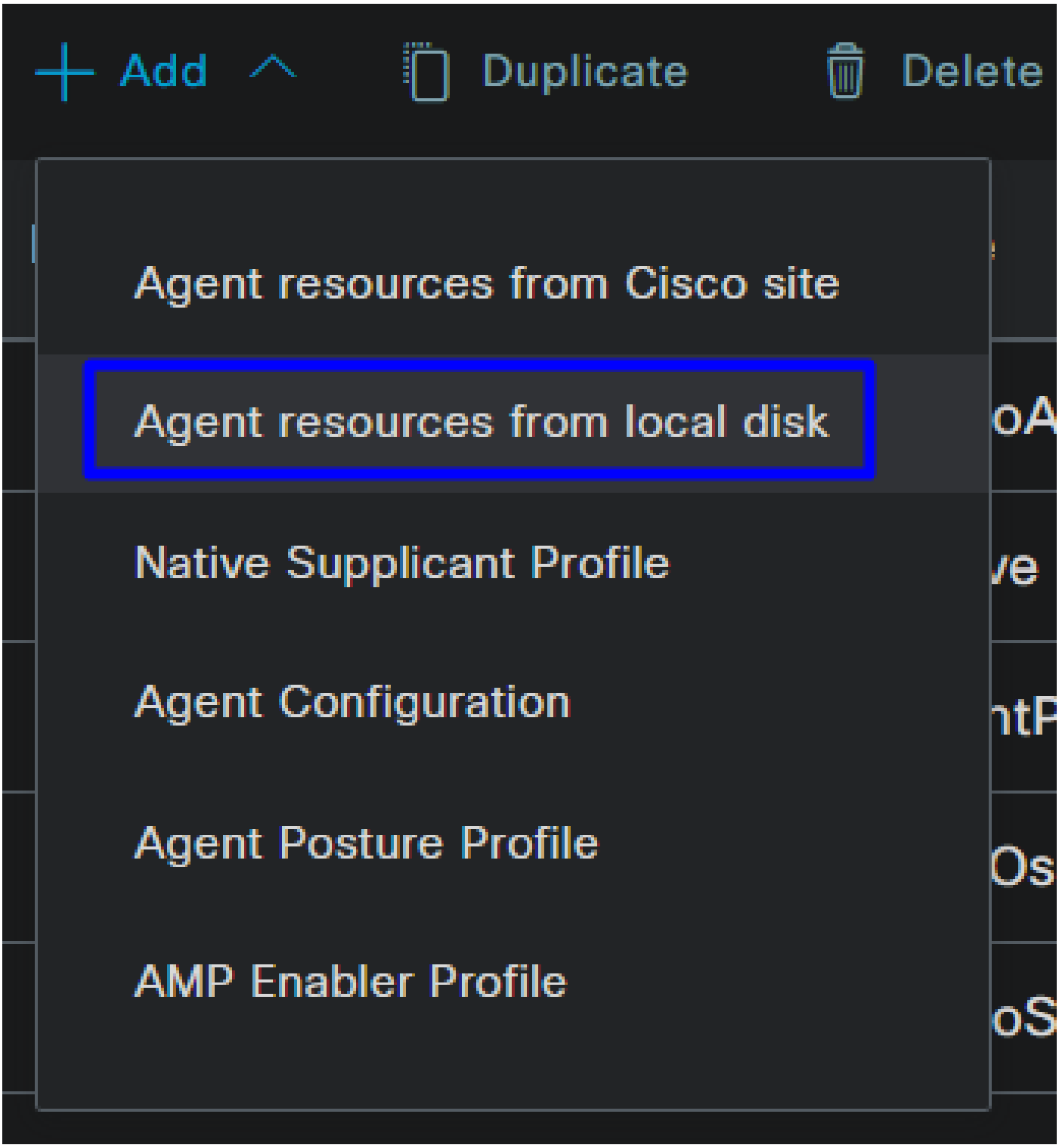
1. **Agent Resources**	Secure Client Web Provisioningパッケージ。
2. **Compliance Module**	Cisco ISEコンプライアンスモジュール
を選択します。 **Agent Profile**	プロビジョニングプロファイルの制御。
を選択します。 **Agent Configuration**	エージェントプロファイルとエージェントリソースを使用してプロビジョニングポータルを設定し、プロビジョニングするモジュールを定義します。

Step 1 エージェントリソースのダウンロードとアップロード

- 新しいエージェントリソースを追加するには、シスコダウンロードポータルに移動し、Web展開パッケージをダウンロードします。Web展開ファイルは.pkg形式である必要があります。

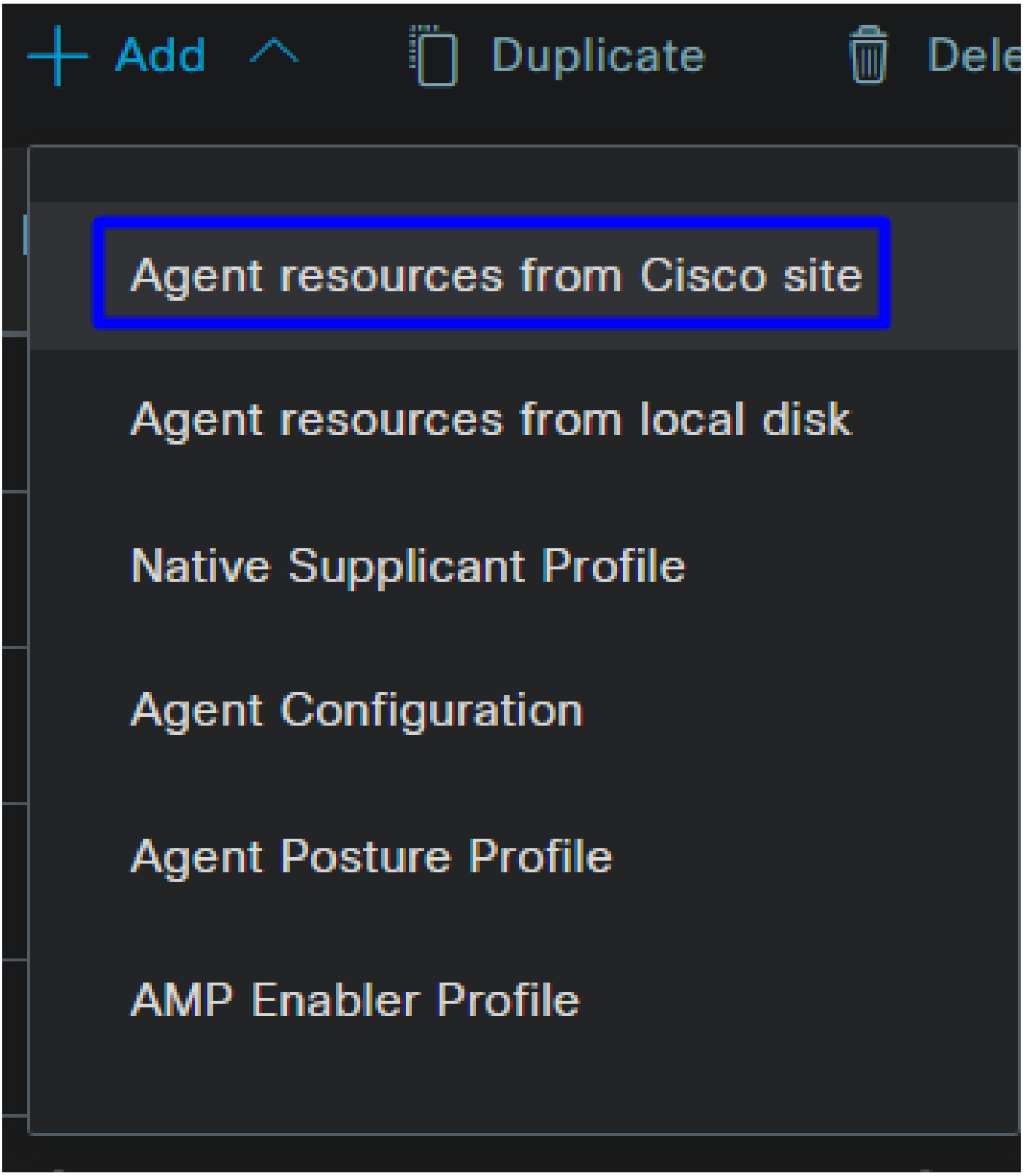


- をクリック+ Add > Agent resources from local disk し、パッケージをアップロードします。

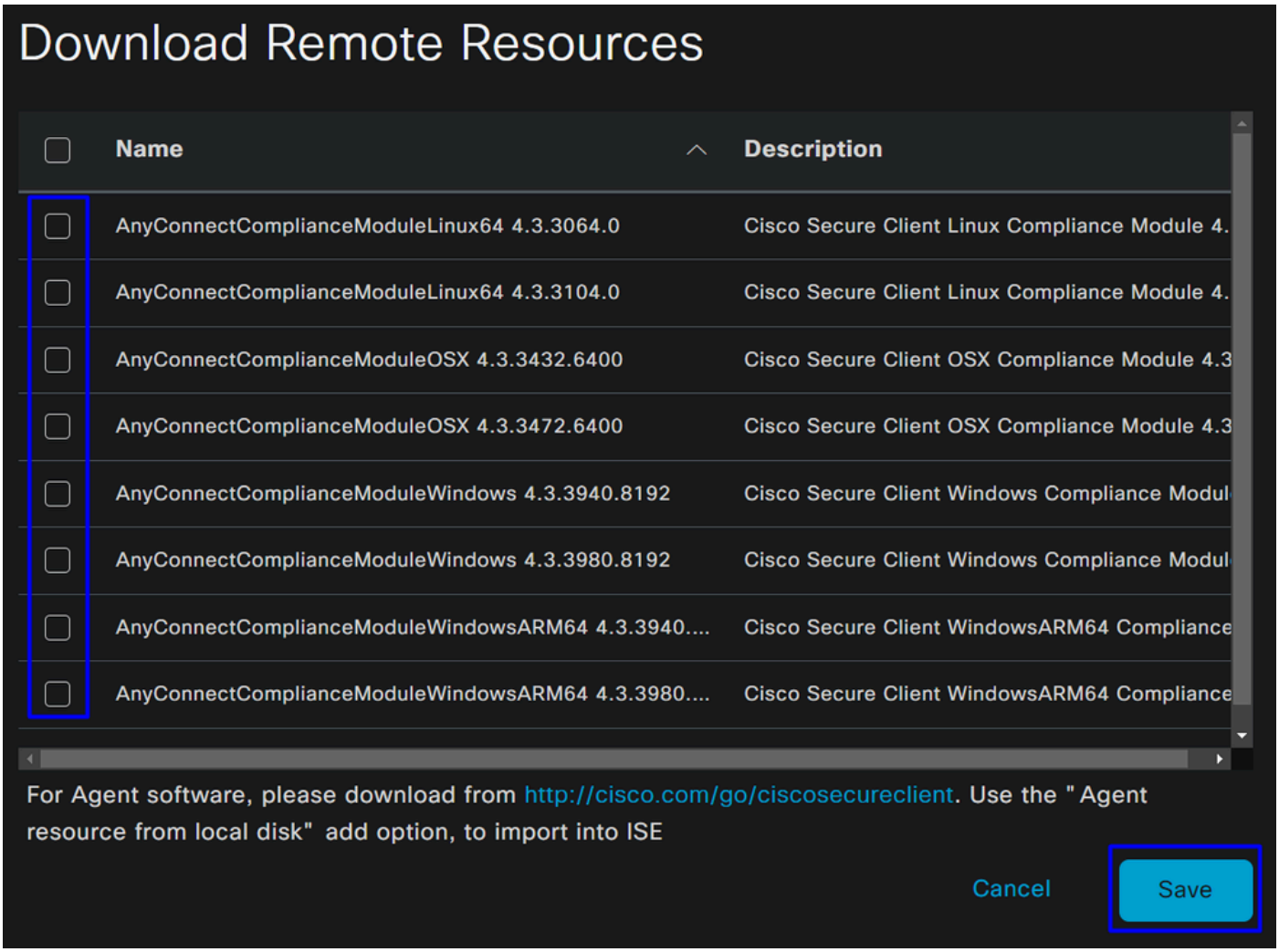


Step 2コンプライアンスモジュールのダウンロード

- クリック + Add > Agent resources from Cisco Site



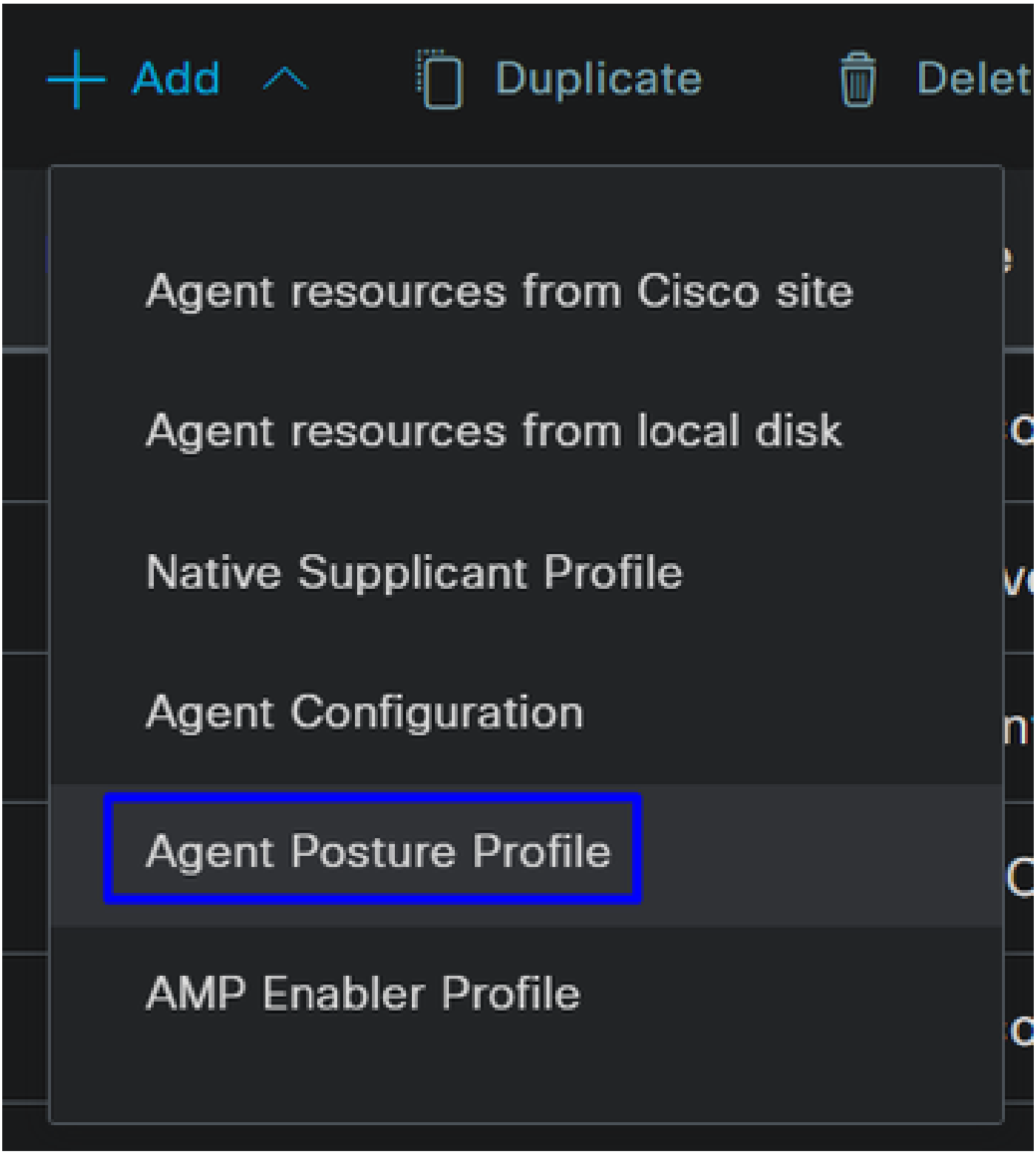
- 必要なすべてのコンプライアンスモジュールのチェックボックスをオンにして、 **Save**



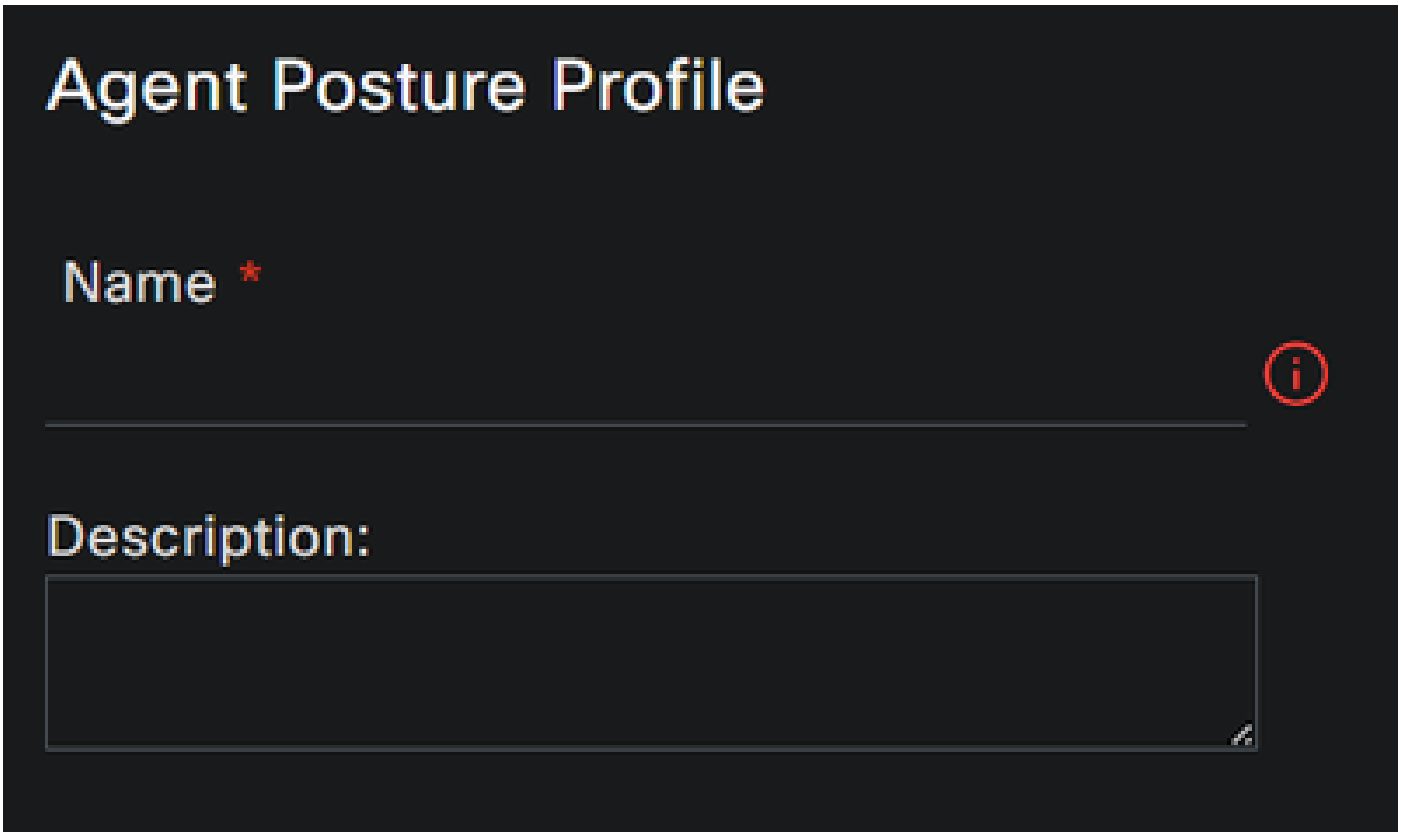
Step 3エージェントプロファイルの設定

- クリック + Add > Agent Posture Profile

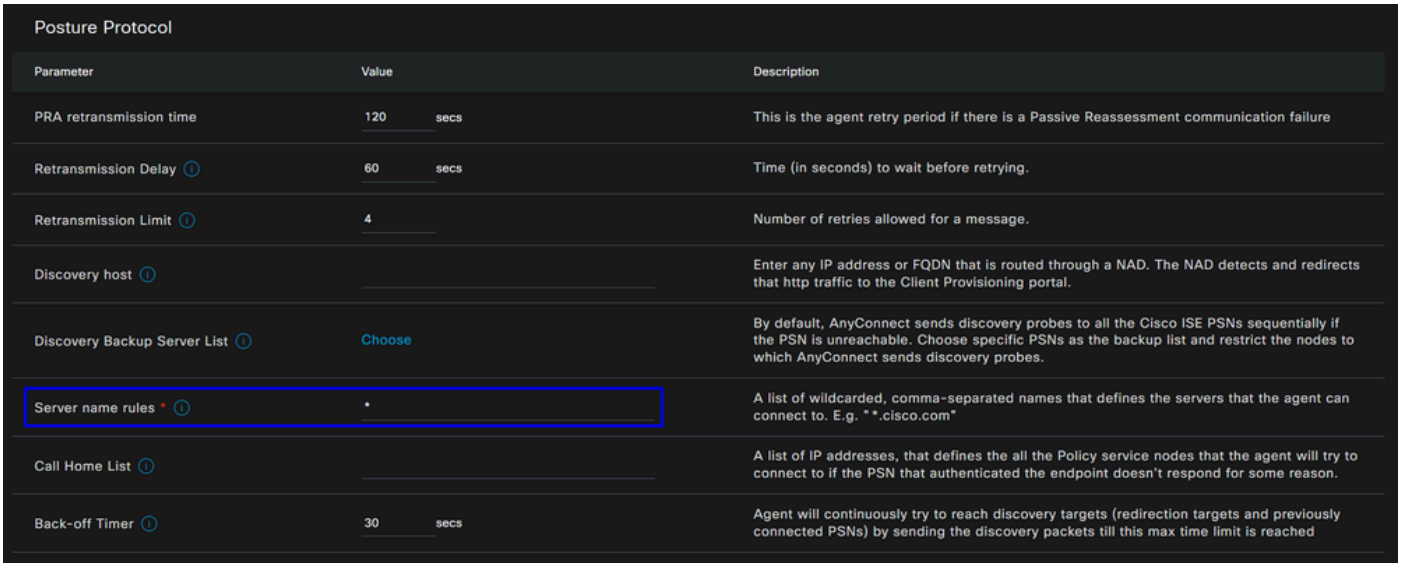
Name



- 用の **Posture Profile**

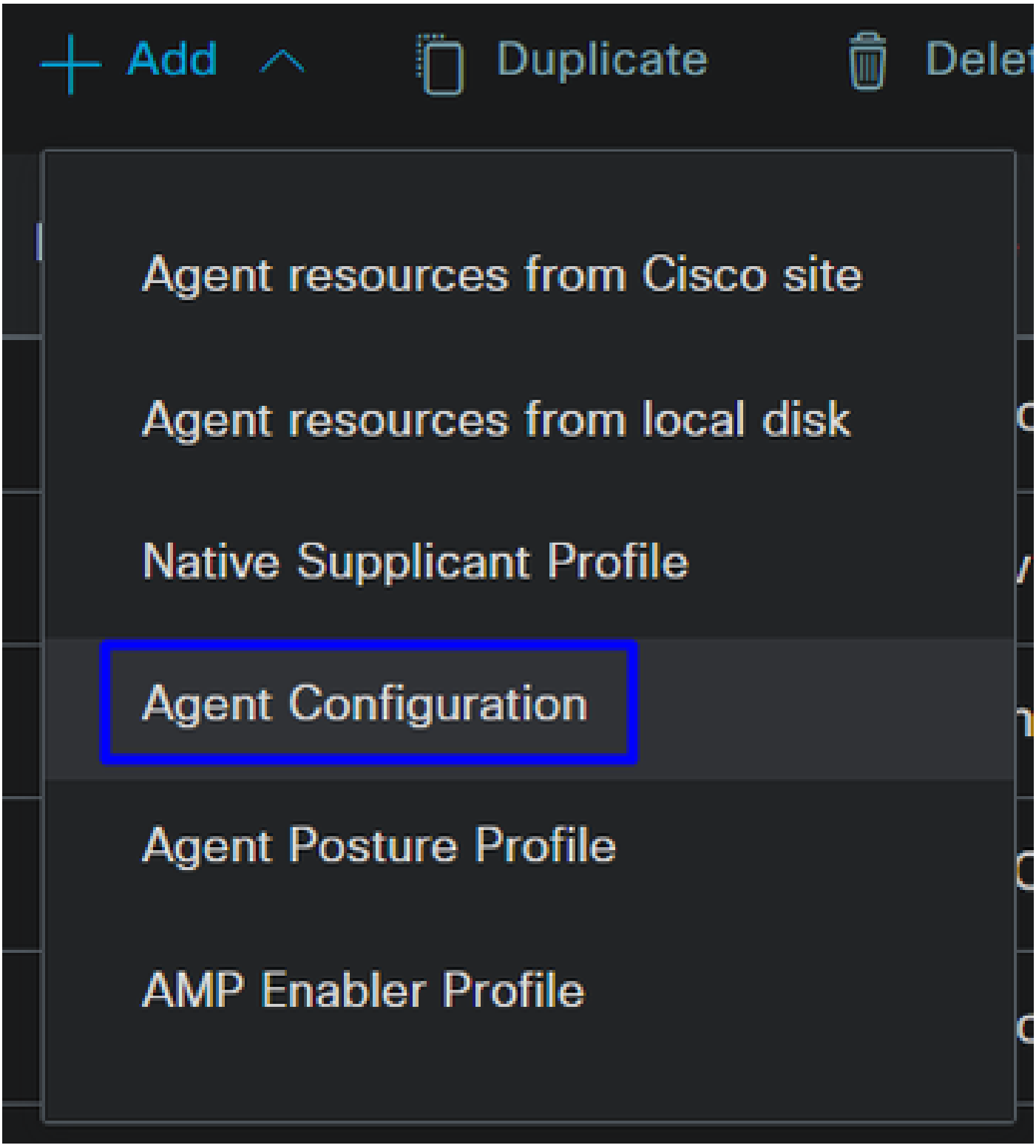


- Server name rulesの下に* を置き、そのSave 後にクリックします

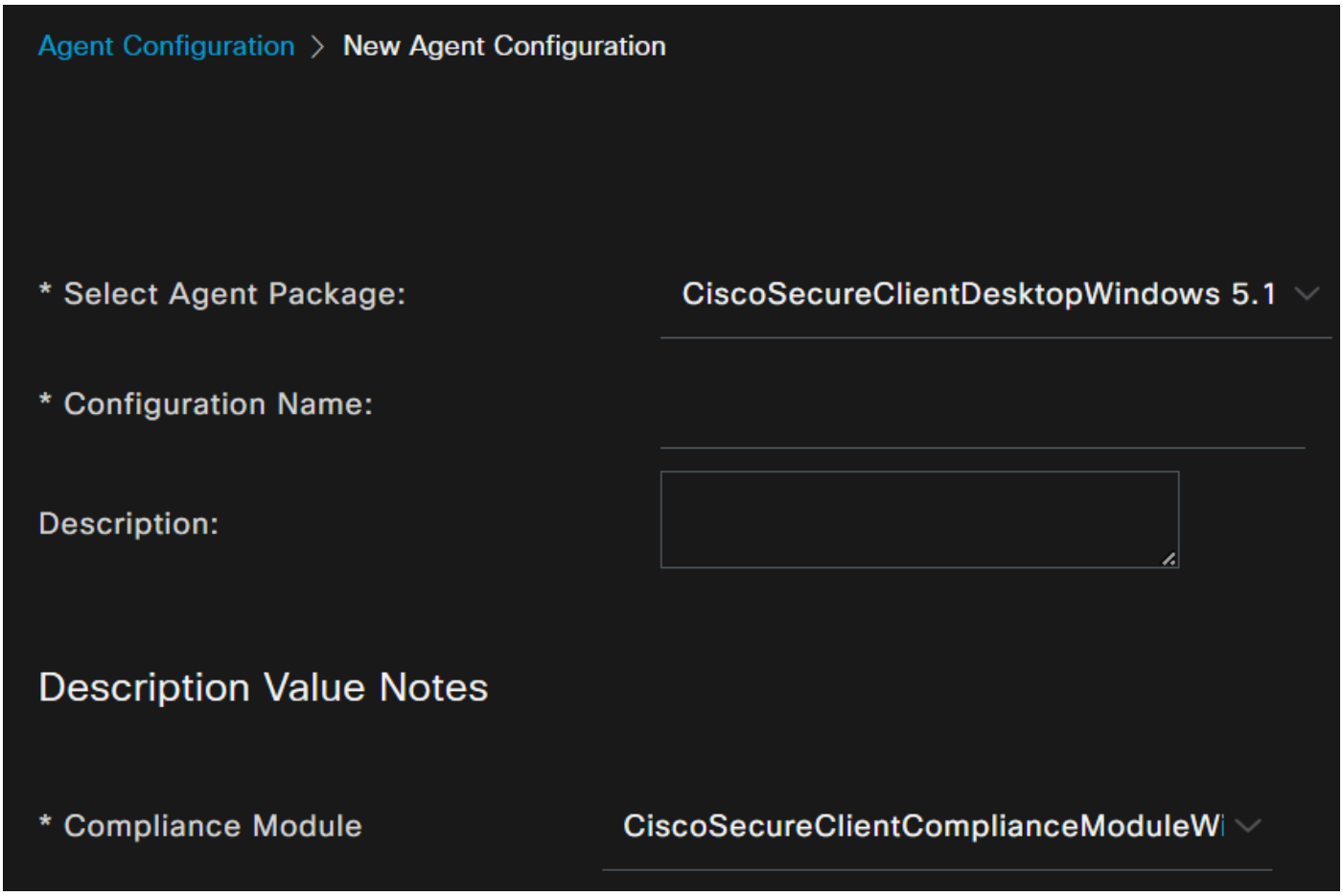


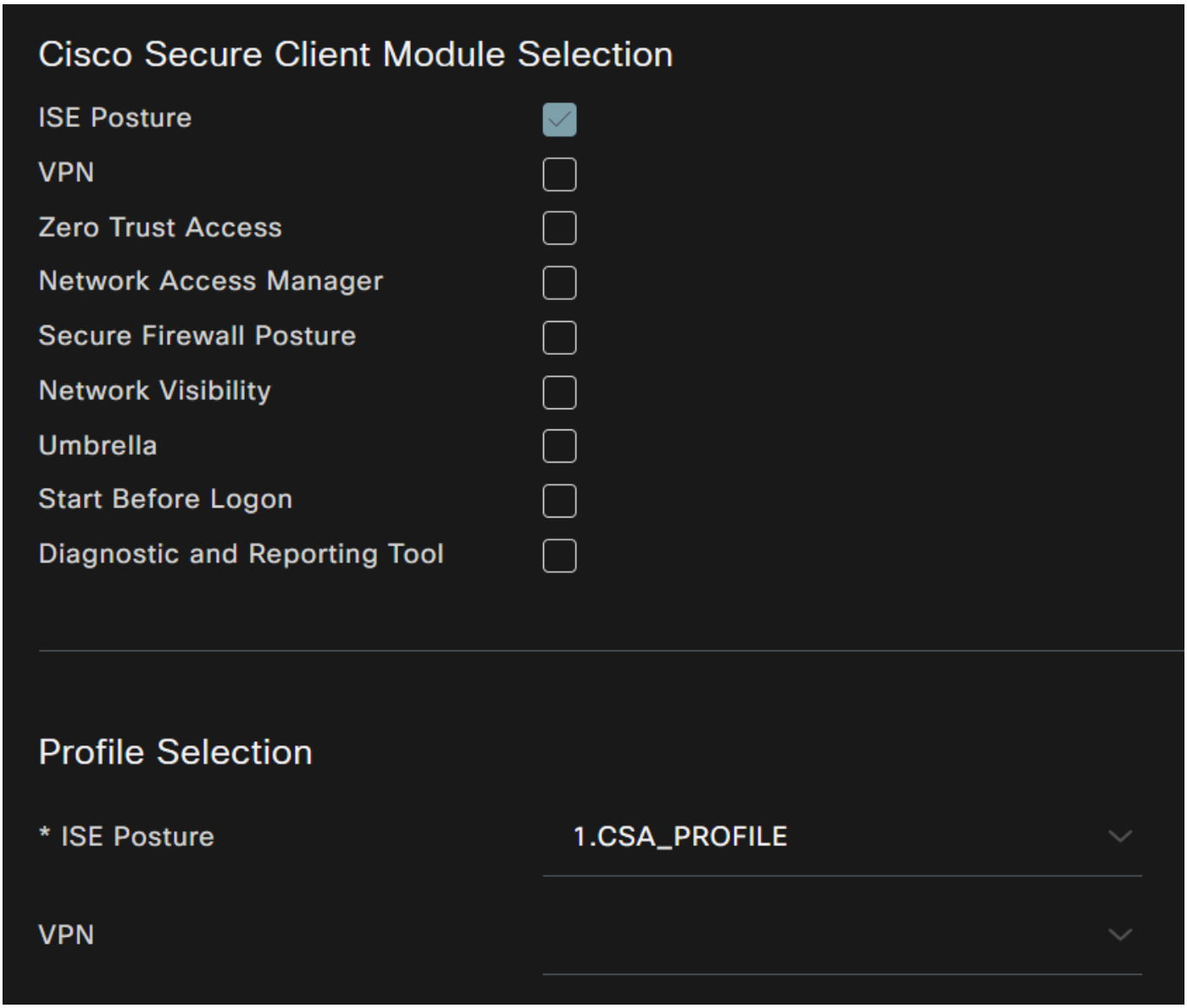
Step 4 エージェントの設定

- クリック + Add > Agent Configuration



- その後、次のパラメータを設定します。

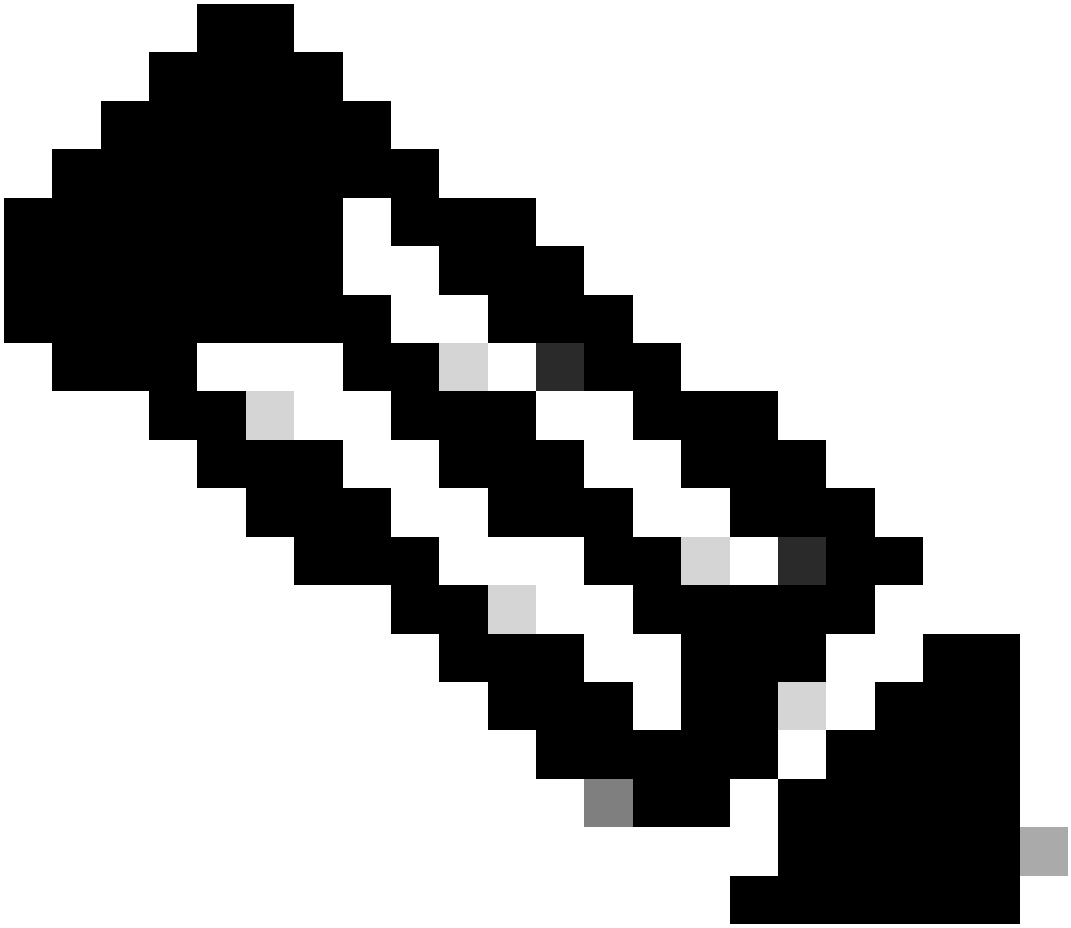

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package :Step1 Download and Upload Agent Resourcesでアップロードしたパッケージを選択します。
- **Configuration Name**：名前を選択して、 **Agent Configuration**
- **Compliance Module**：ステップ2コンプライアンスモジュールのダウンロードでダウンロードしたコンプライアンスモジュールを選択します
- Cisco Secure Client Module Selection
  - **ISE Posture**：チェックボックスをオンにする
- **Profile Selection**

- **ISE Posture**:手順3で設定したISEプロファイルを選択します。エージェントプロファイルを設定します

- クリック **Save**

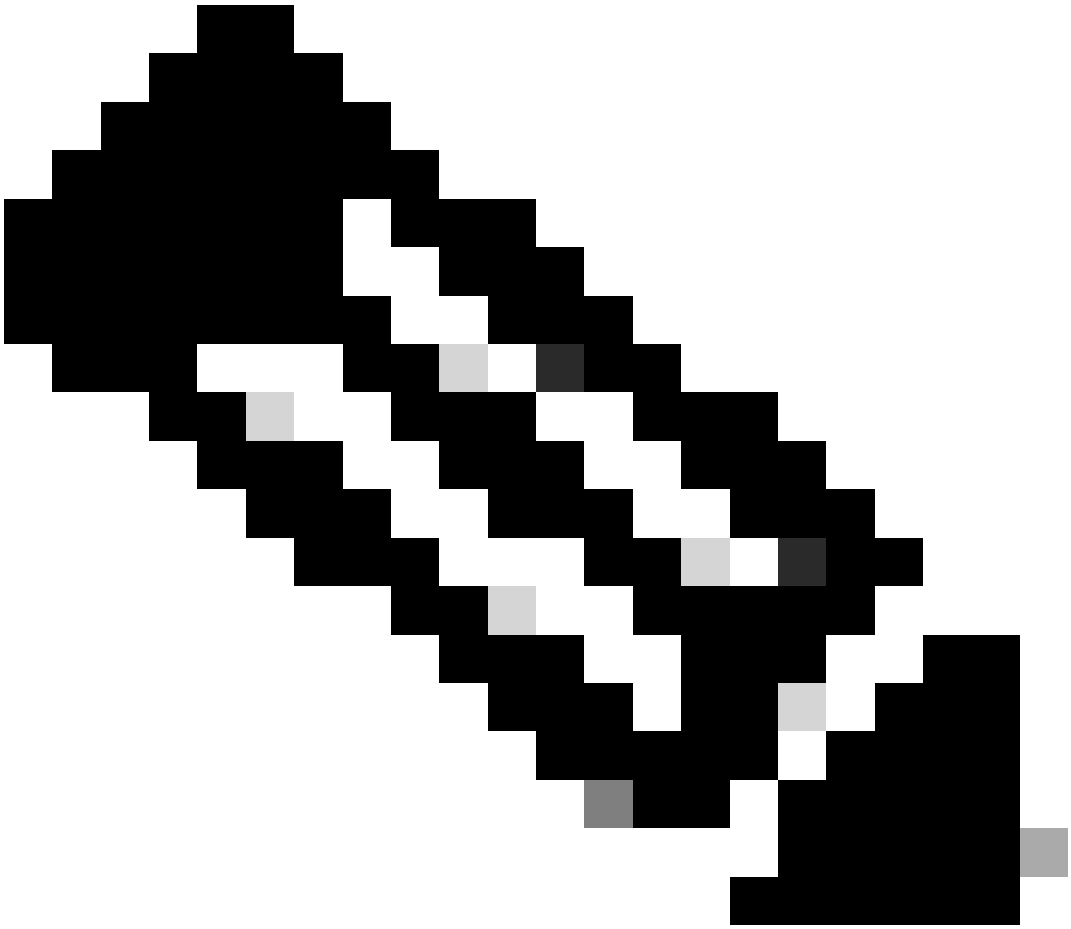


注：各オペレーティングシステム、Windows、Mac OS、またはLinuxで、1つのクライアント設定を個別に使用することをお勧めします。

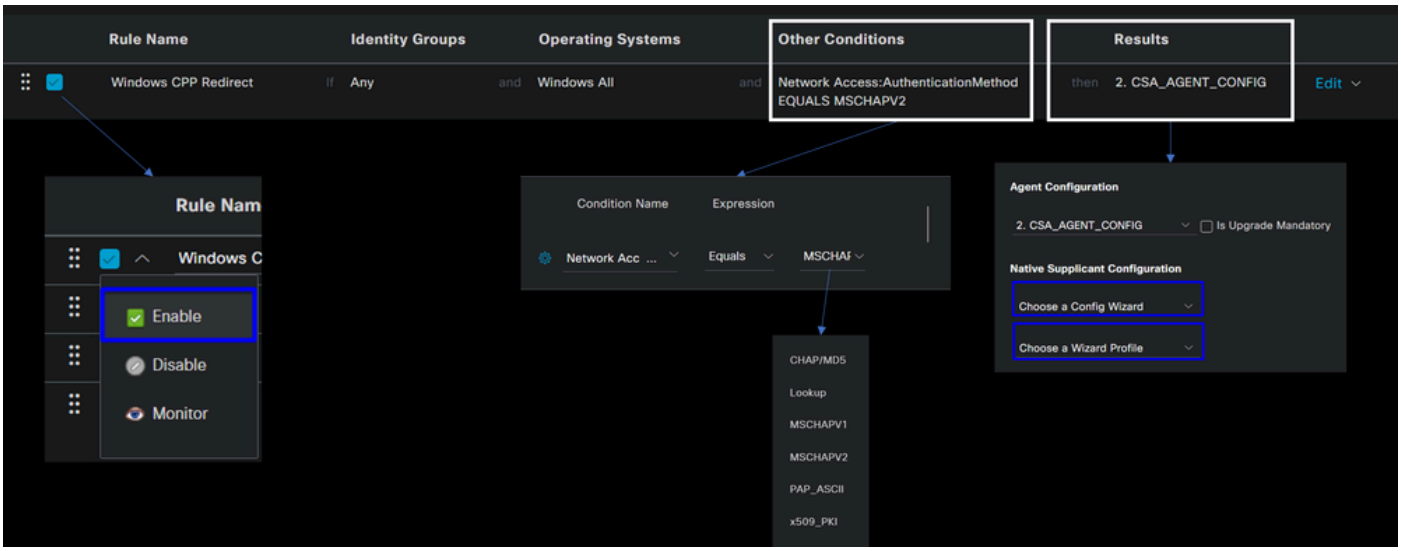
クライアントプロビジョニングポリシーの設定

最後の手順で設定したISEポスチャとモジュールのプロビジョニングを有効にするには、プロビジョニングを行うようにポリシーを設定する必要があります。

- ISEダッシュボードに移動します
- クリック **Work Center** > **Client Provisioning**



注：オペレーティングシステム、Windows、Mac OS、またはLinuxごとに1つのクライアント設定ポリシーを設定することをお勧めします。



- **Rule Name**：デバイスタイプとアイデンティティグループの選択に基づいてポリシー名を設定し、各ポリシーを簡単に識別できるようにします
- **Identity Groups**：ポリシーで評価するIDを選択します
- **Operating Systems**：ステップ「エージェントパッケージの選択」で選択したエージェントパッケージに基づいてオペレーティングシステムを選択します
- **Other Condition**:ステップで設定した方式に**Network Access** 基づいて**Authentication Method**EQUALS、RADIUSグループの追加を選択します。または、空欄のままにしておきます
- **Result**:手順4で設定したエージェント設定を選択します。エージェント設定
  - **Native Supplicant Configuration**:Config Wizardを選択し、 Wizard Profile
- チェックボックスでポリシーが有効としてリストされていない場合は、有効としてマークします。

認可プロファイルの作成

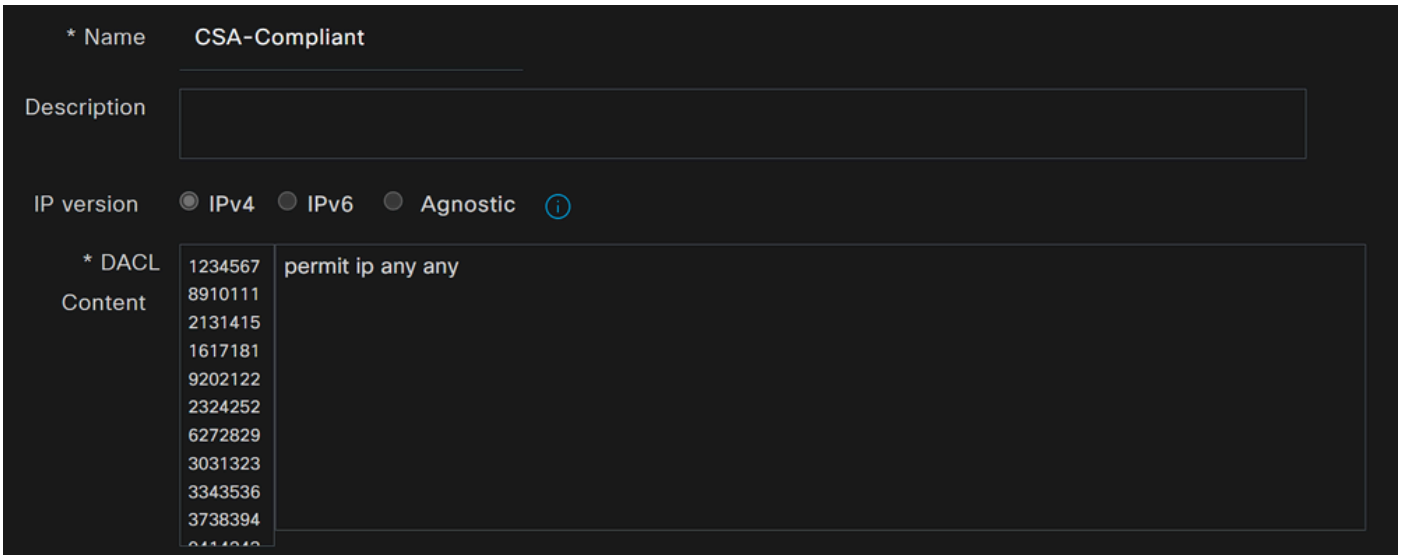
認可プロファイルは、認証パス後のユーザポスチャに応じて、リソースへのアクセスを制限します。ユーザがポスチャに基づいてアクセスできるリソースを判別するには、認可を確認する必要があります。

許可プロファイル	説明
準拠	ユーザ準拠 – エージェントがインストール済み – ポスチャ検証済み

不明な準拠	ユーザUknown Compliant – エージェントのインストールへのリダイレクト – ポスチャ確認待ち
アクセス拒否	ユーザが非準拠 – アクセス拒否

DACLを設定するには、ISEダッシュボードに移動します。

- クリック **Work Centers** > **Policy Elements** > **Downloadable ACLs**
- クリック **+Add**
- 作成： **Compliant DACL**



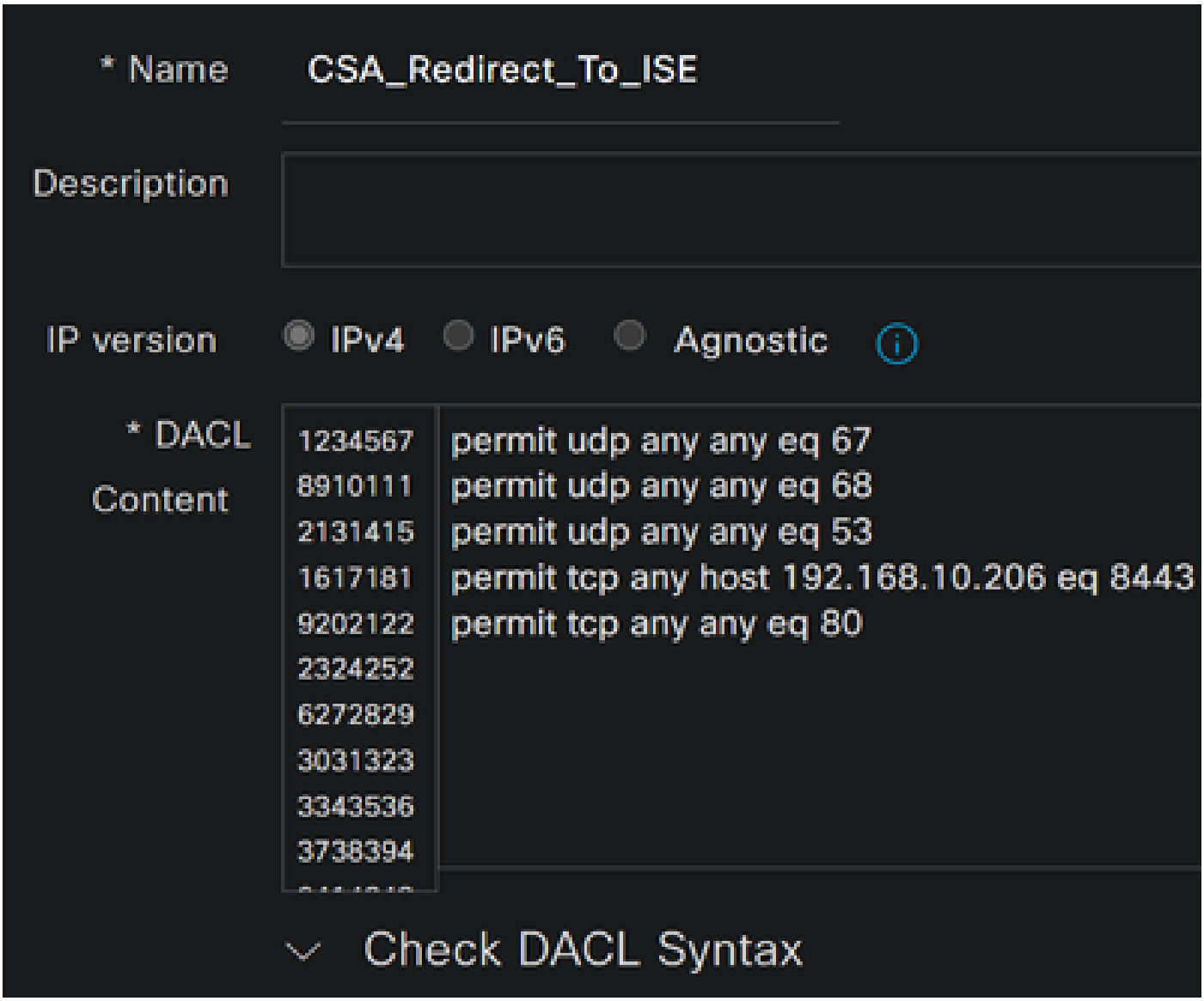
- **Name**: DACL準拠を参照する名前を追加します。
- **IP version**:選択 **IPv4**
- DACL Content：ネットワークのすべてのリソースへのアクセスを許可するダウンロード可能アクセスコントロールリスト(DACL)を作成します。

<#root>

```
permit ip any any
```

をクリック**Save** し、不明なコンプライアンスDACLを作成します

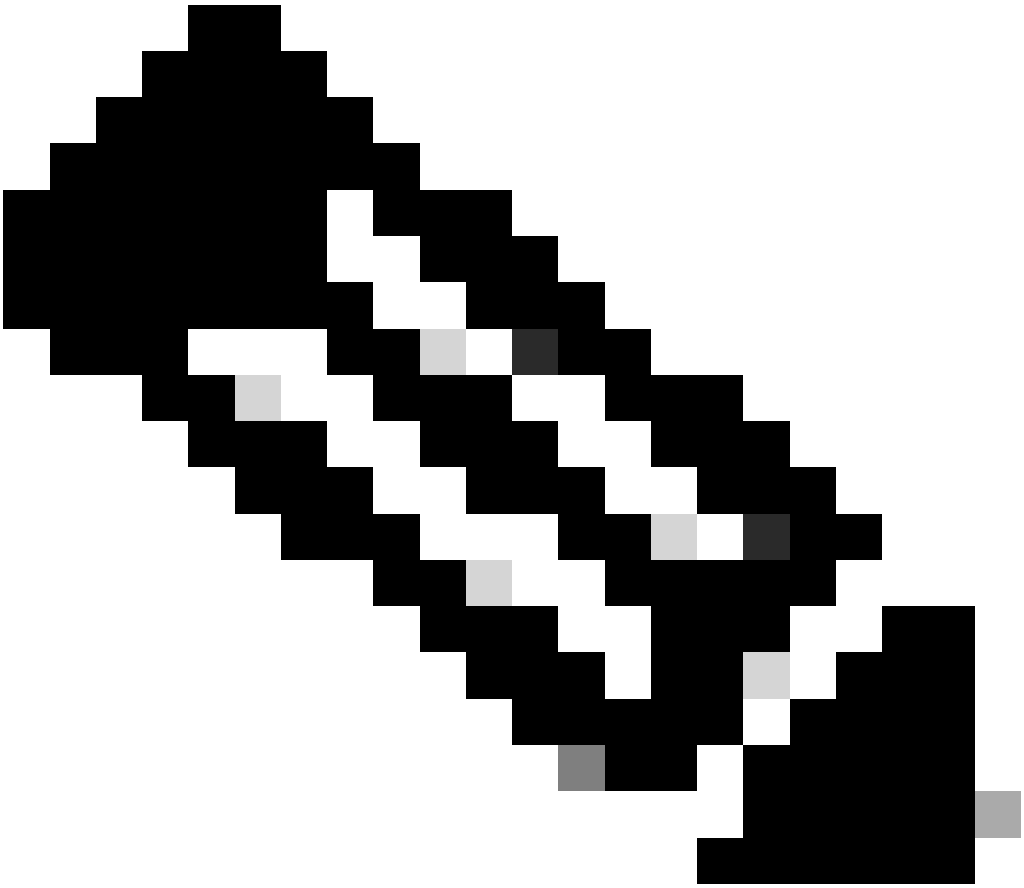
- クリック **Work Centers > Policy Elements > Downloadable ACLs**
- クリック **+Add**
- 作成： **Unknown Compliant DACL**



- **Name**:DACL-Unknown-Compliantを参照する名前を追加します。
- **IP version**:選択 **IPv4**
- **DACL Content**: ポート8443を介したネットワーク、DHCP、DNS、HTTP、およびプロビジョニングポータルへの制限付きアクセスを提供するDACLを作成します

```
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
```

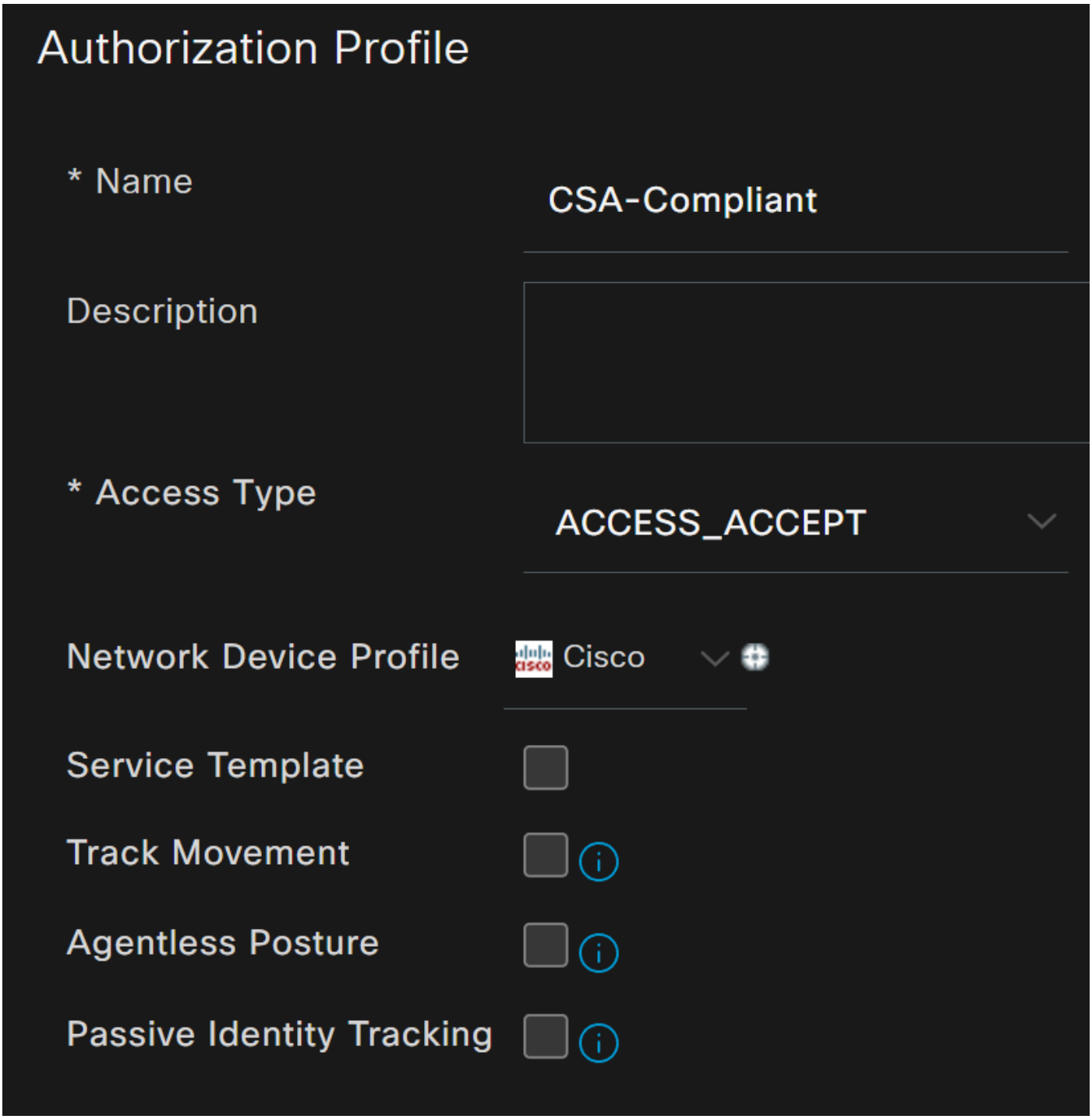


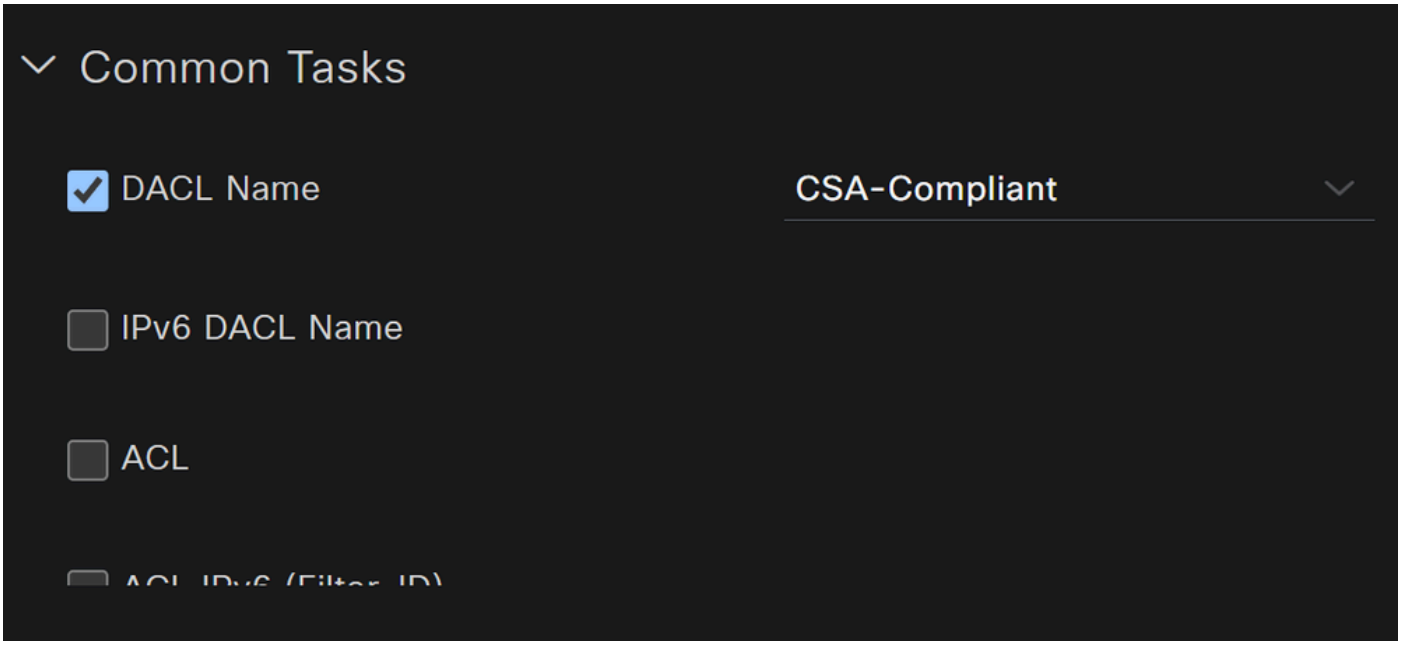
注：このシナリオでは、IPアドレス192.168.10.206はCisco Identity Services Engine(ISE)サーバに対応し、ポート8443はプロビジョニングポータル用に指定されています。つまり、ポート8443を経由するIPアドレス192.168.10.206へのTCPトラフィックが許可され、プロビジョニングポータルへのアクセスが容易になります。

この時点で、認可プロファイルを作成するために必要なDACLが完成します。

認可プロファイルを設定するには、ISEダッシュボードに移動します。

- クリック **Work Centers > Policy Elements > Authorization Profiles**
  - クリック **+Add**
  - 作成： **Compliant Authorization Profile**





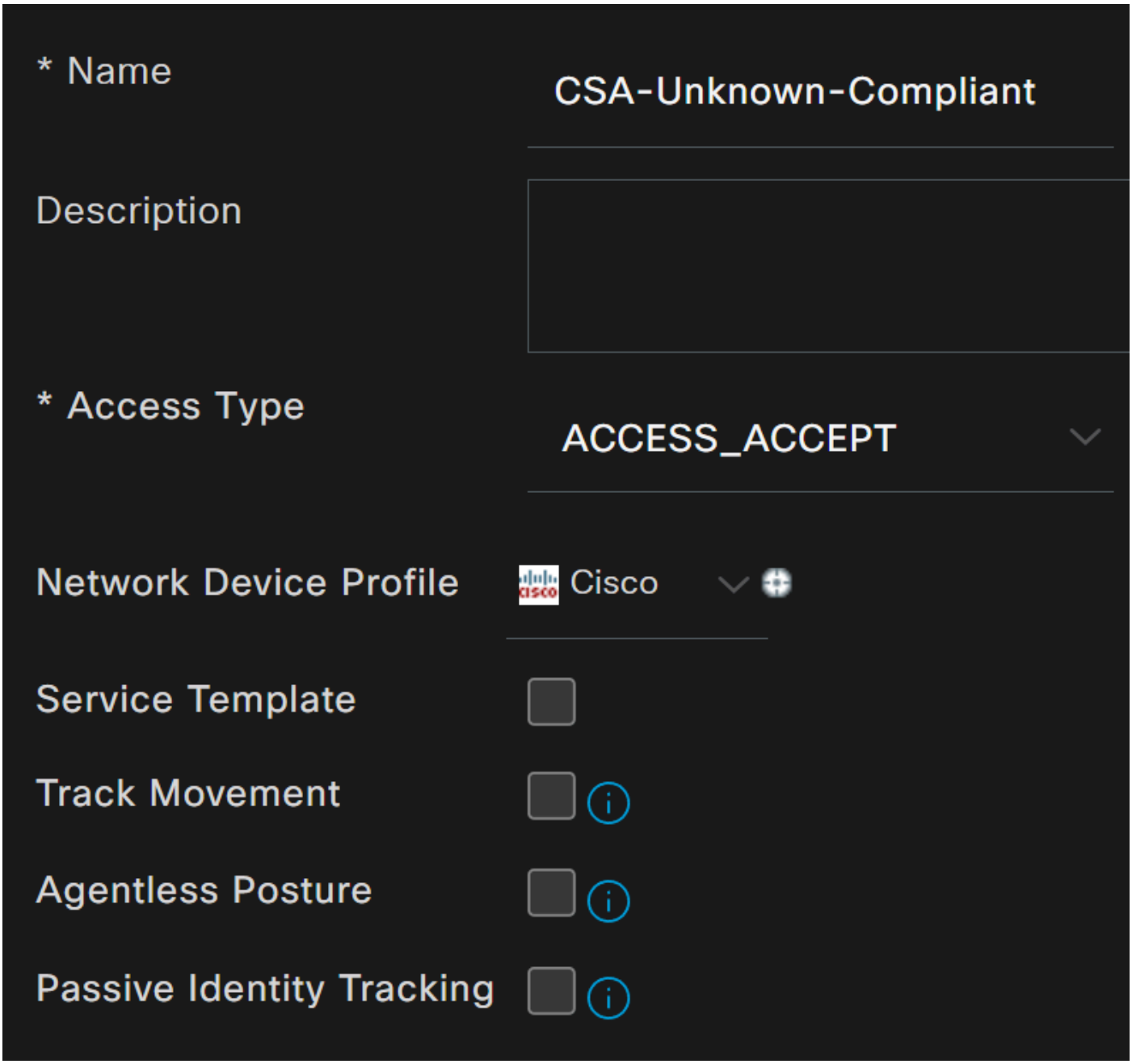
- **Name**：準拠する認可プロファイルを参照する名前を作成します。
- Access Type:選択 **ACCESS_ACCEPT**

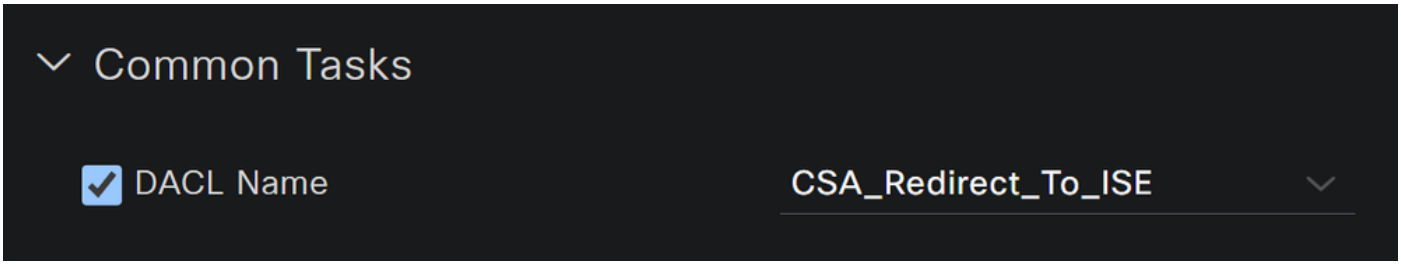
- **Common Tasks**
  - **DACL NAME**：ステップCompliant DACLで設定したDACLを選択します。

をクリック**Save** し、 Unknown Authorization Profile

- クリック **Work Centers** > **Policy Elements** > **Authorization Profiles**
- クリック **+Add**

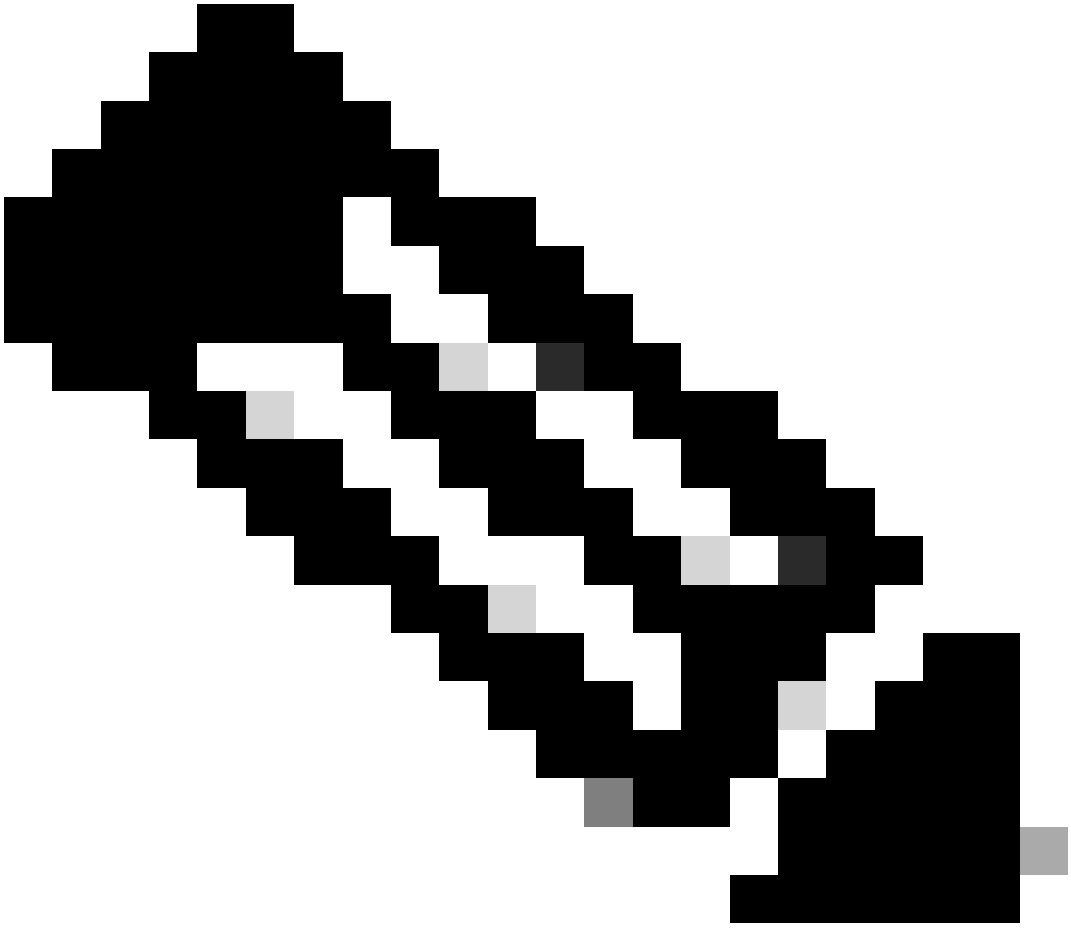
- 作成： **Uknown Compliant Authorization Profile**





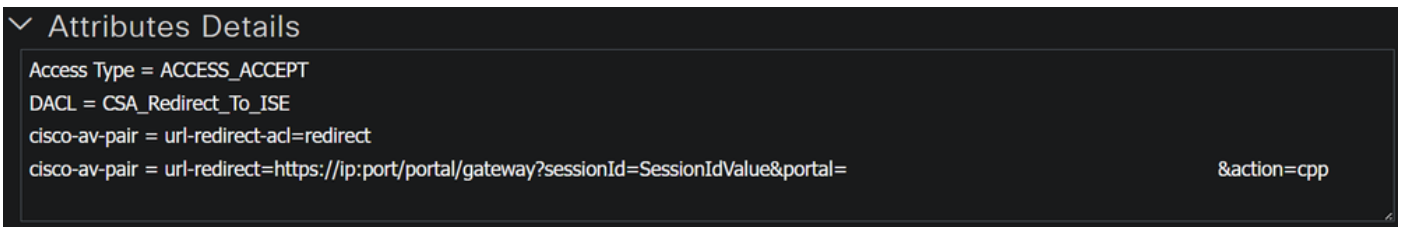
- **Name**：不明な準拠する認可プロファイルを参照する名前を作成します。
- Access Type:選択 **ACCESS_ACCEPT**

- **Common Tasks**
  - **DACL NAME**：ステップUnknown Compliant DACLで設定したDACLを選択します。
    - **Web Redirection (CWA,MDM,NSP,CPP)**
      - 選択 **Client Provisioning (Posture)**
        - **ACL**：次の値でなければなりません。 redirect
        - **Value**：デフォルトのプロビジョニングポータルを選択します。別のポータルを定義した場合は、それを選択します



注：すべての導入でのセキュアアクセスのリダイレクトACLの名前は、 **redirect**です。

これらの値をすべて定義した後は、Attributes Detailsの下に同様の値を設定する必要があります。



Save をクリックして設定を終了し、次の手順に進みます。

ポスチャポリシーセットの設定

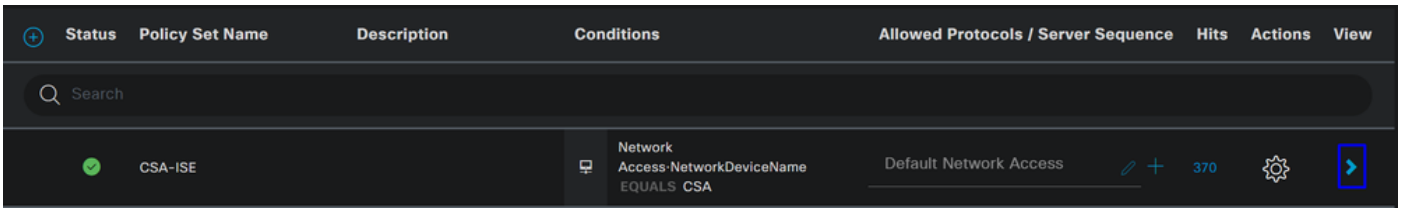
作成するこれらの3つのポリシーは、設定した認可プロファイルに基づいています。 **DenyAccess**では、別のポリシーを作成する必要はありません。

ポリシーセット – 許可	許可プロファイル
準拠	許可プロファイル – 準拠
不明な準拠	認可プロファイル – 非準拠
非準拠	アクセス拒否

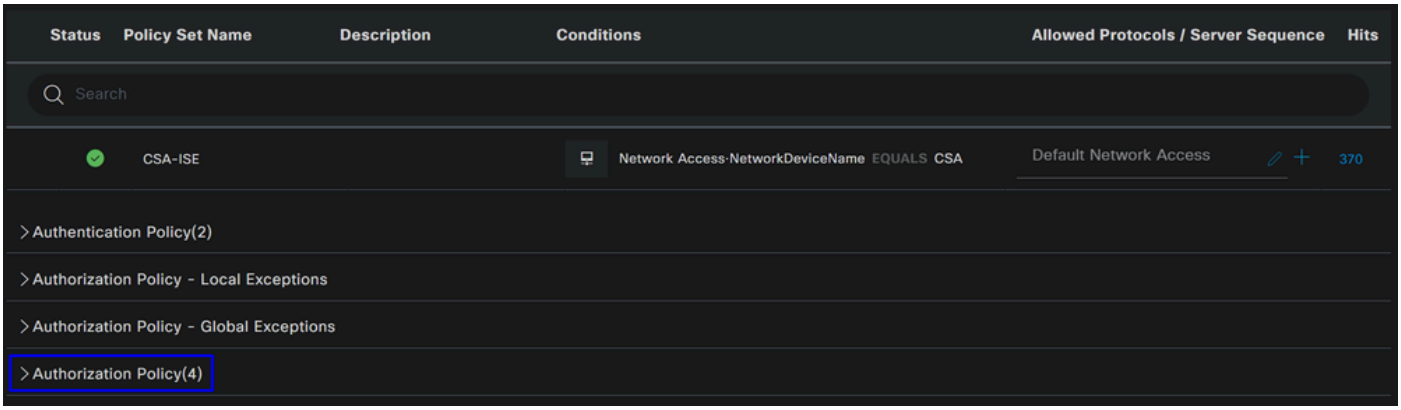
ISEダッシュボードに移動します

- クリック **Work Center** > **Policy Sets**

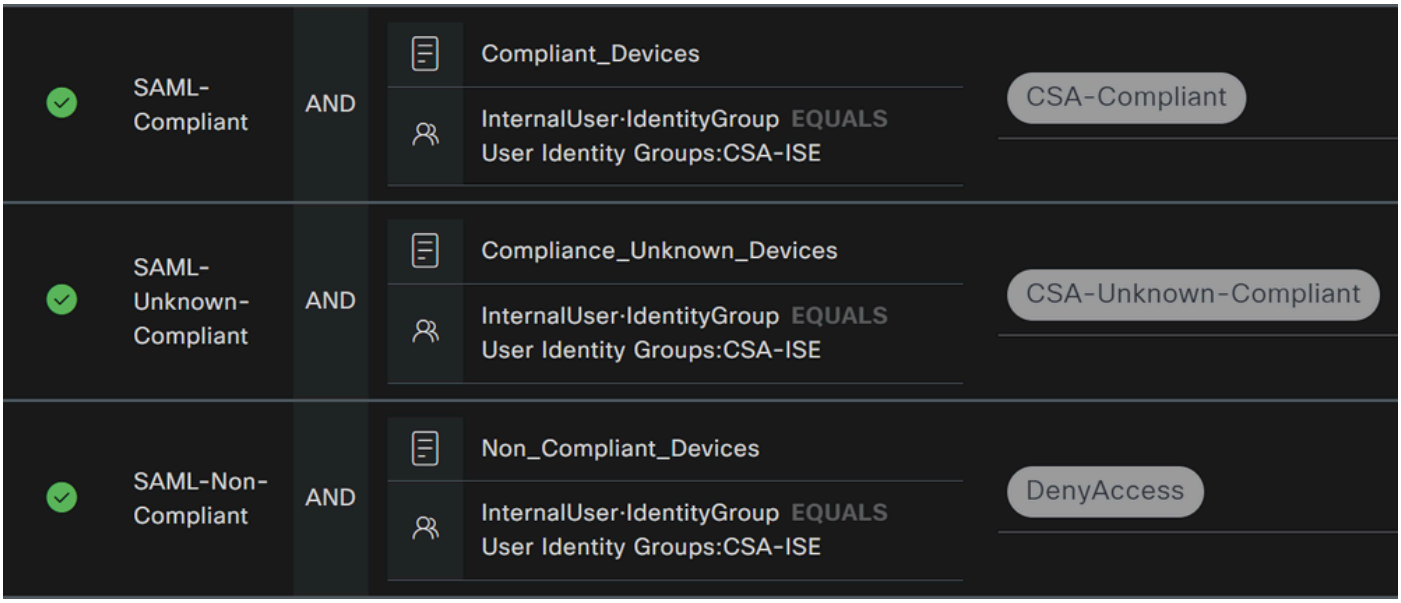
- をクリック> して、作成したポリシーにアクセスします



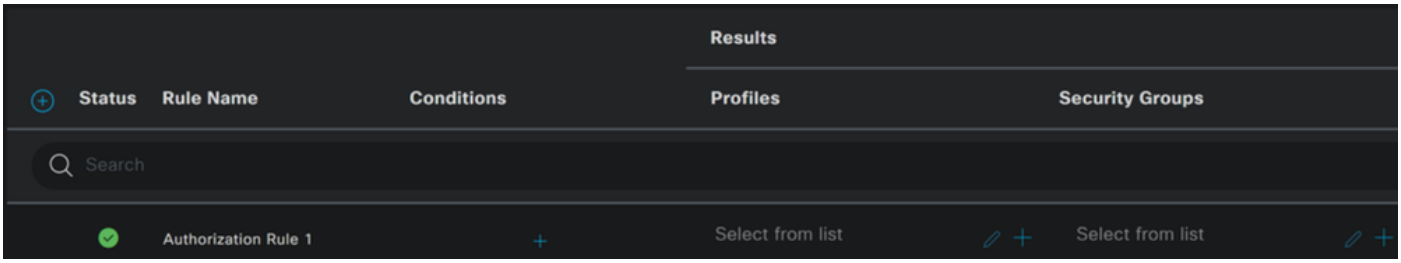
- をクリックします。 Authorization Policy



- 次の3つのポリシーを次の順序で作成します。



- をクリックし+ てポ**CSA-Compliance** リシーを定義します。



- 次の手順では、Rule NameConditions および Profiles

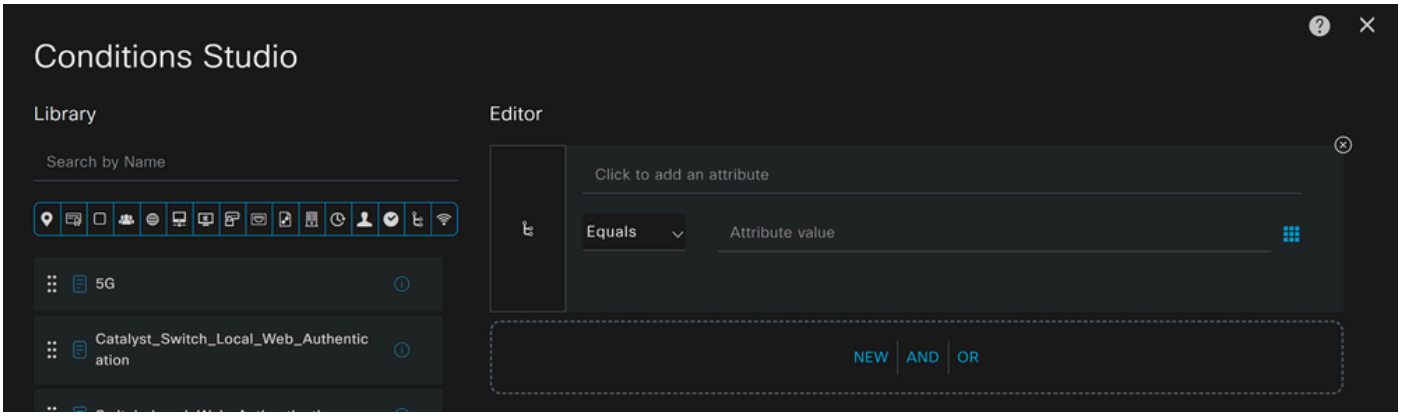
- 名前をに設**Name** 定する場合 **CSA-Compliance**

Condition

- を設定するには、 +

Condition Studio

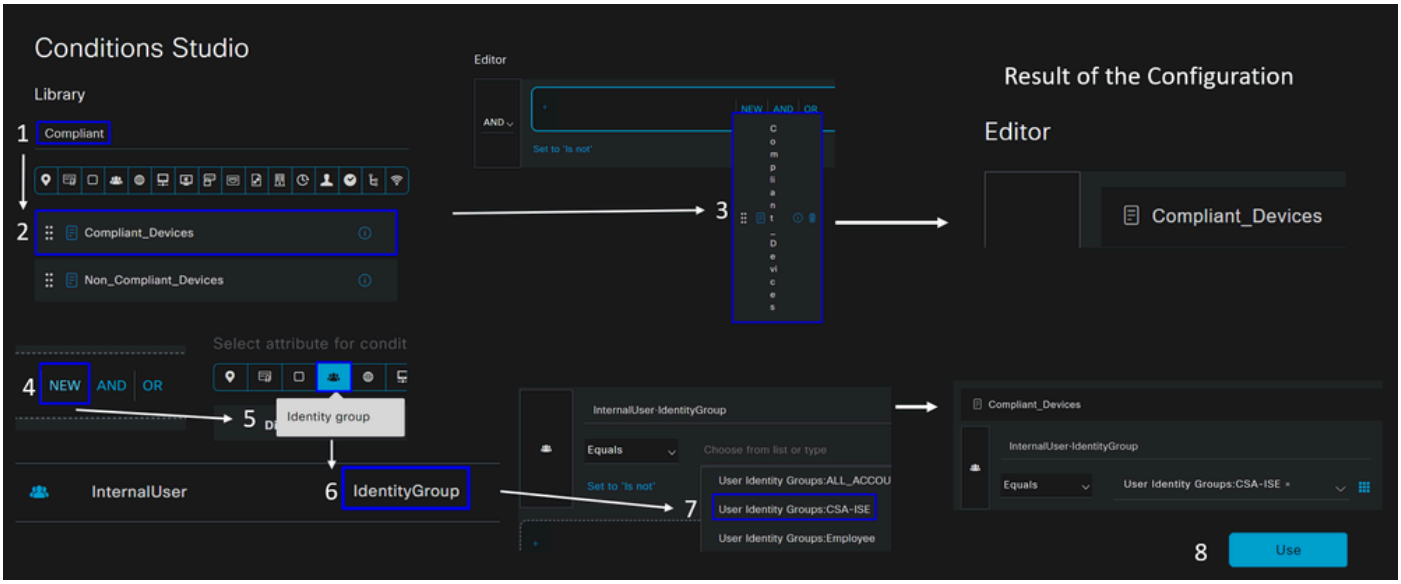
- の下に、次の情報があります。



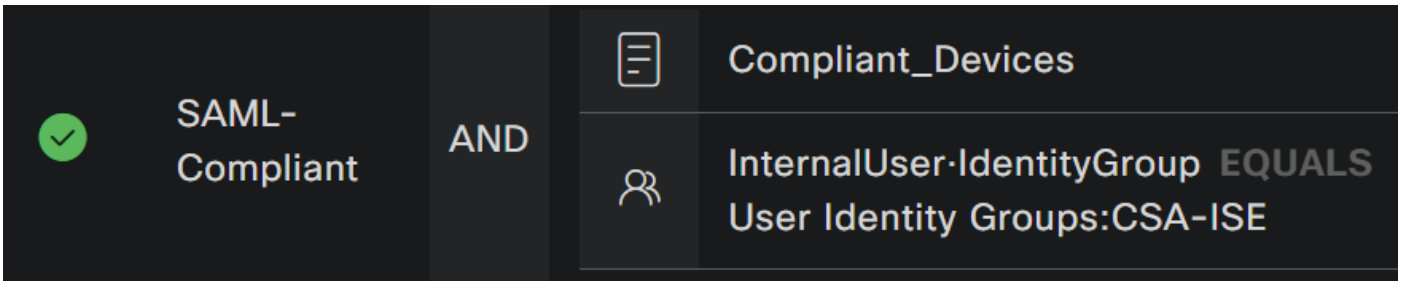
- 条件を作成するには、 **compliant**
- 表示されているはずです。 Compliant_Devices
- 下にドラッグアンドドロップします。 **Editor**

Editor

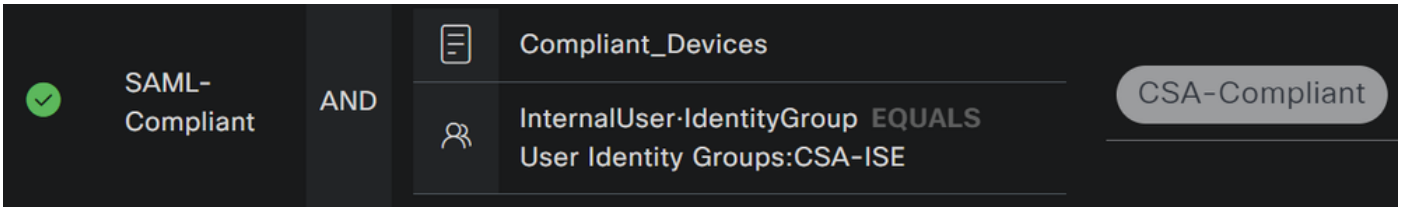
- の下をクリックします。 **New**
- アイ**Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す**User Identity Group** る名前を選択します
- クリック **Use**



- その結果、次のイメージが表示されます

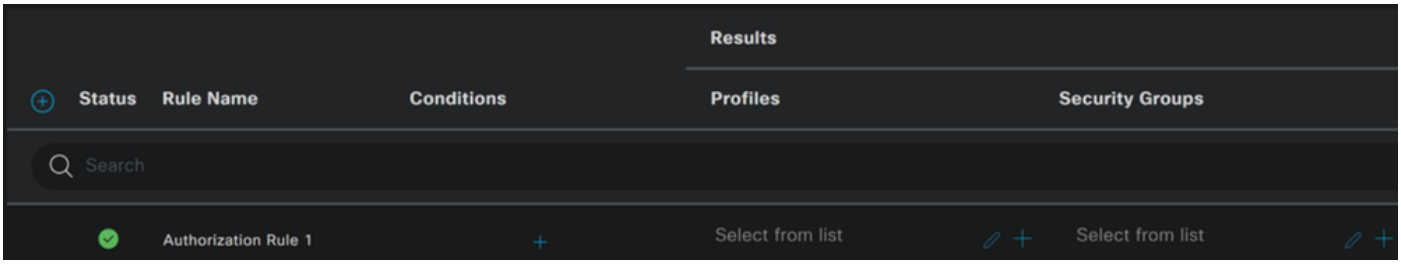


- の下でドロップダウンボタンの下をクリ**Profile** ックし、手順で設定した苦情認証プロファイル、Compliant Authorization Profileを選択します。



これで、 **Compliance Policy Set**が設定されました。

- をクリックし+ てポ**CSA-Unknown-Compliance** リシーを定義します。



- 次の手順では、Rule NameConditions および Profiles

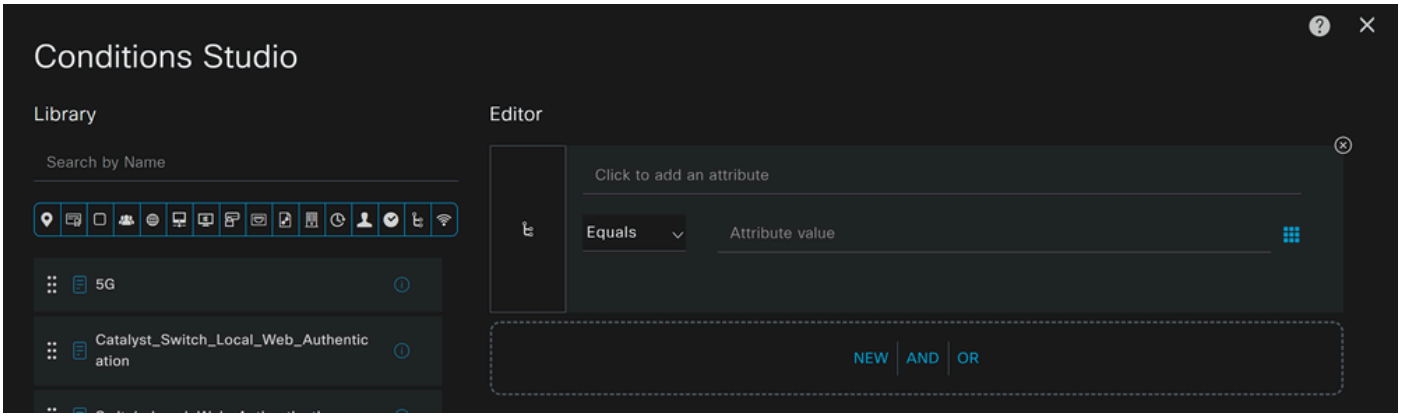
- 名前をに設Name 定する場合 **CSA-Unknown-Compliance**

Condition

- を設定するには、 +

Condition Studio

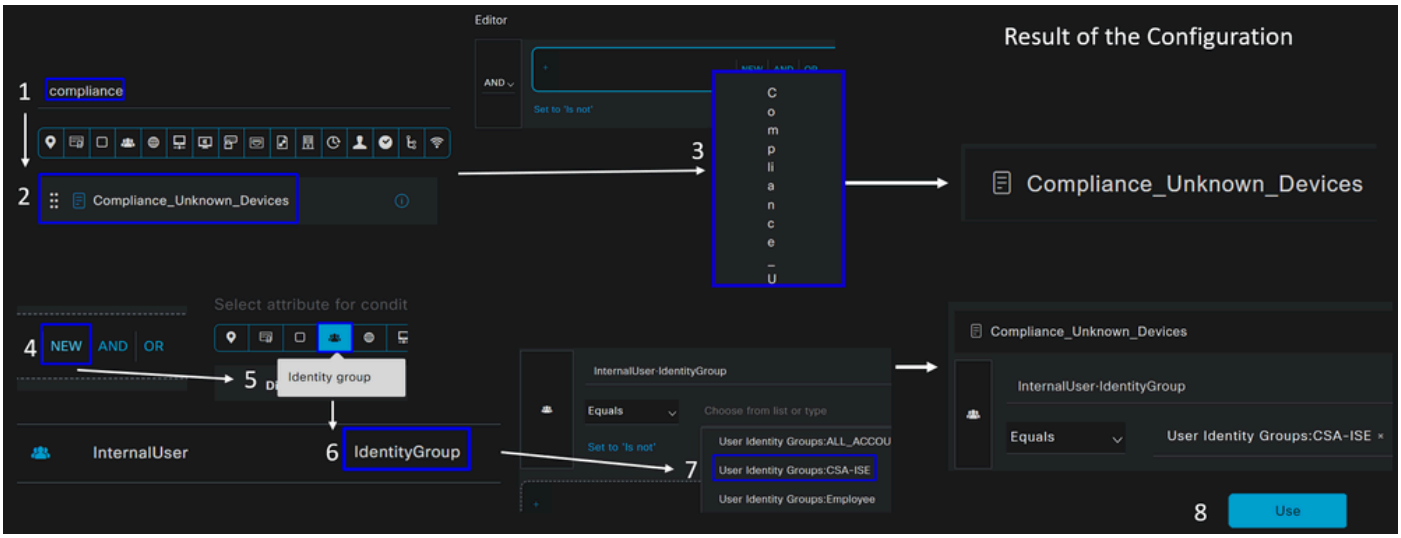
- の下に、次の情報があります。



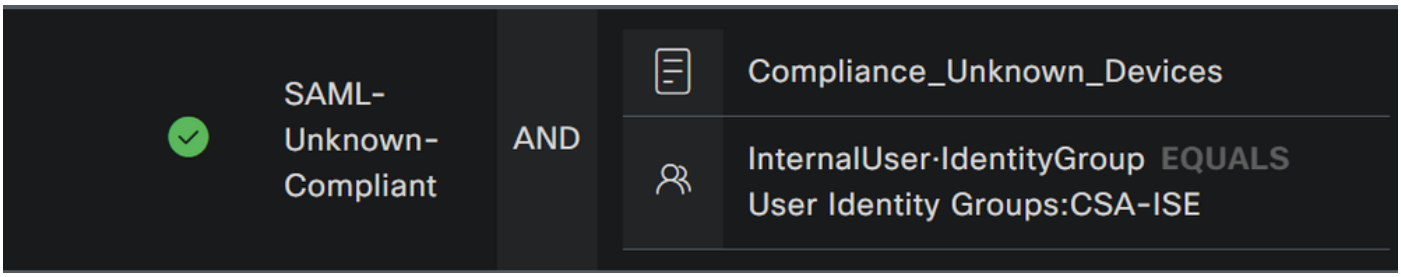
- 条件を作成するには、 **compliance**
- 表示されているはずです。 Compliant_Unknown_Devices
- 下にドラッグアンドドロップします。 **Editor**

Editor

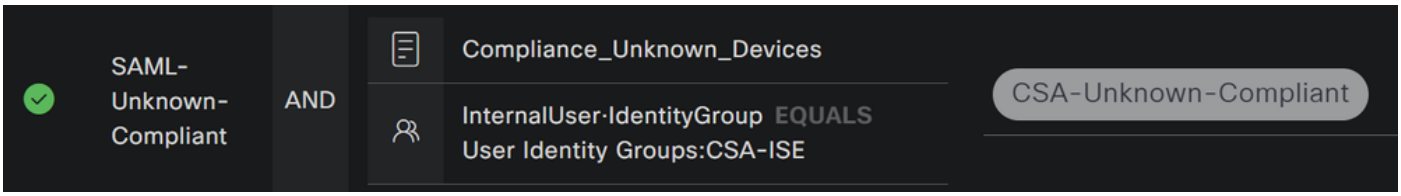
- の下をクリックします。 **New**
- アイ**Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す**User Identity Group** る名前を選択します
- クリック **Use**



- その結果、次のイメージが表示されます

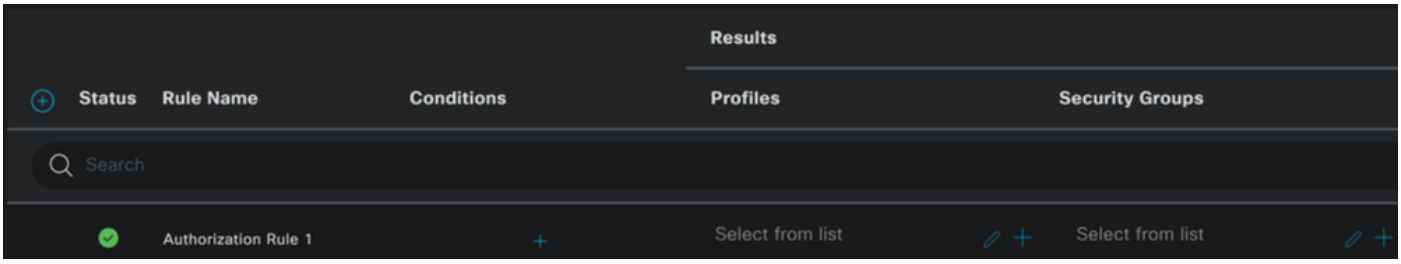


- の下でドロップダウンボタンの下をクリ**Profile** ックし、手順で設定した苦情認証プロファイル、[不明な準拠認証プロファイル]を選択します。



これで、 **Unknown Compliance Policy Set**が設定されました。

- クリックし+ てポ**CSA- Non-Compliant** リシーを定義します。



- 次の手順では、Rule NameConditions および Profiles

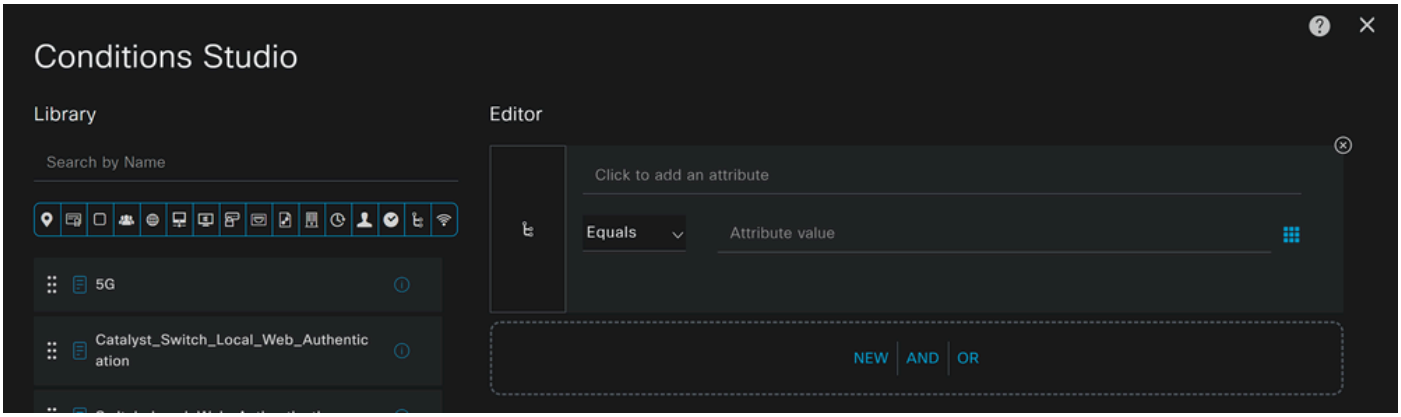
- 名前をに設**Name** 定する場合 **CSA-Non-Compliance**

Condition

- を設定するには、 +

Condition Studio

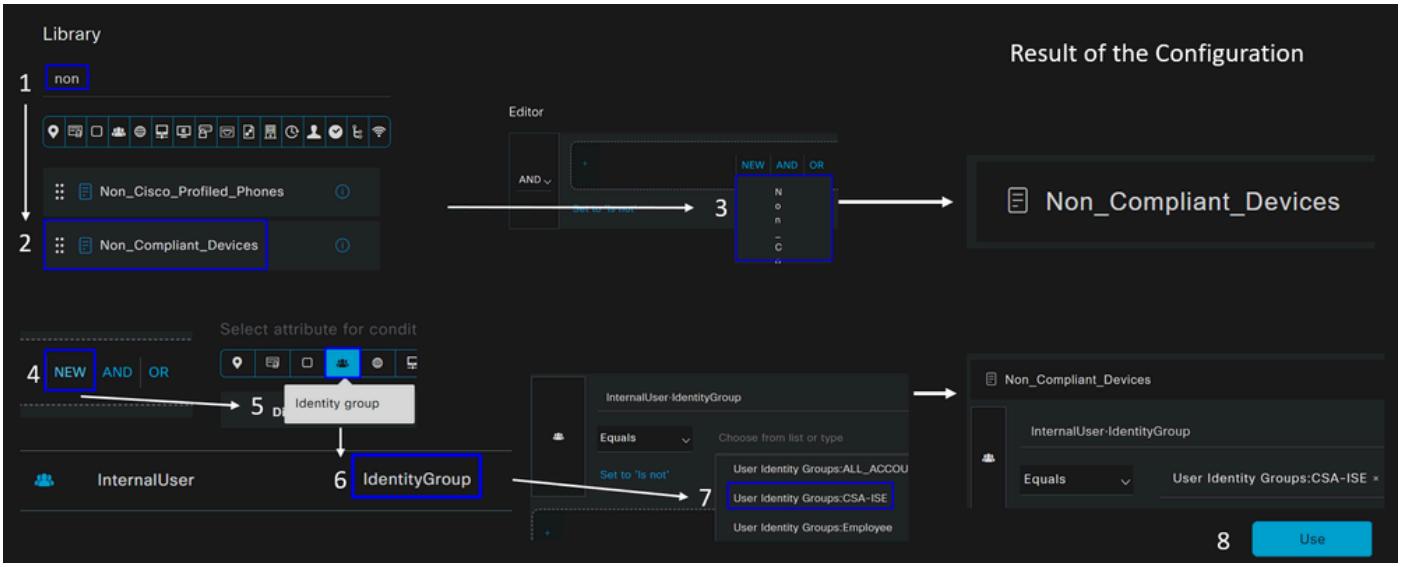
- の下に、次の情報があります。



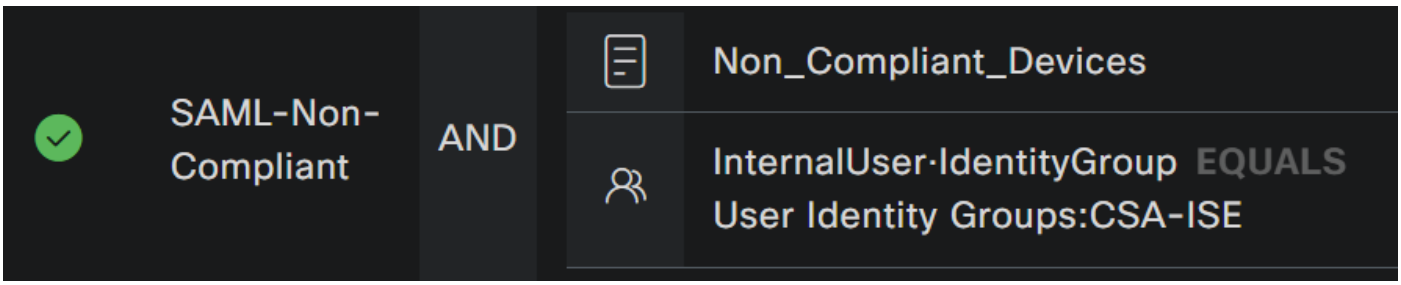
- 条件を作成するには、 **non**
- 表示されているはずです。 Non_Compliant_Devices
- 下にドラッグアンドドロップします。 **Editor**

Editor

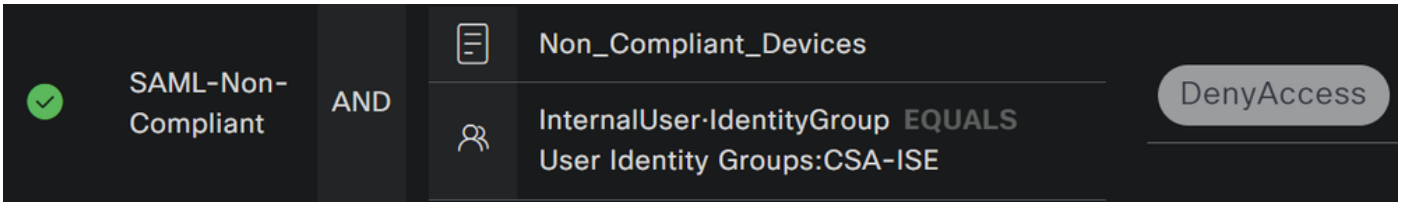
- の下をクリックします。 **New**
- アイ**Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す**User Identity Group** る名前を選択します
- クリック **Use**



- その結果、次のイメージが表示されます



- の下のドロップダウンボタンをク**Profile** リックし、クレーム承認プロファイルを選択します **DenyAccess**



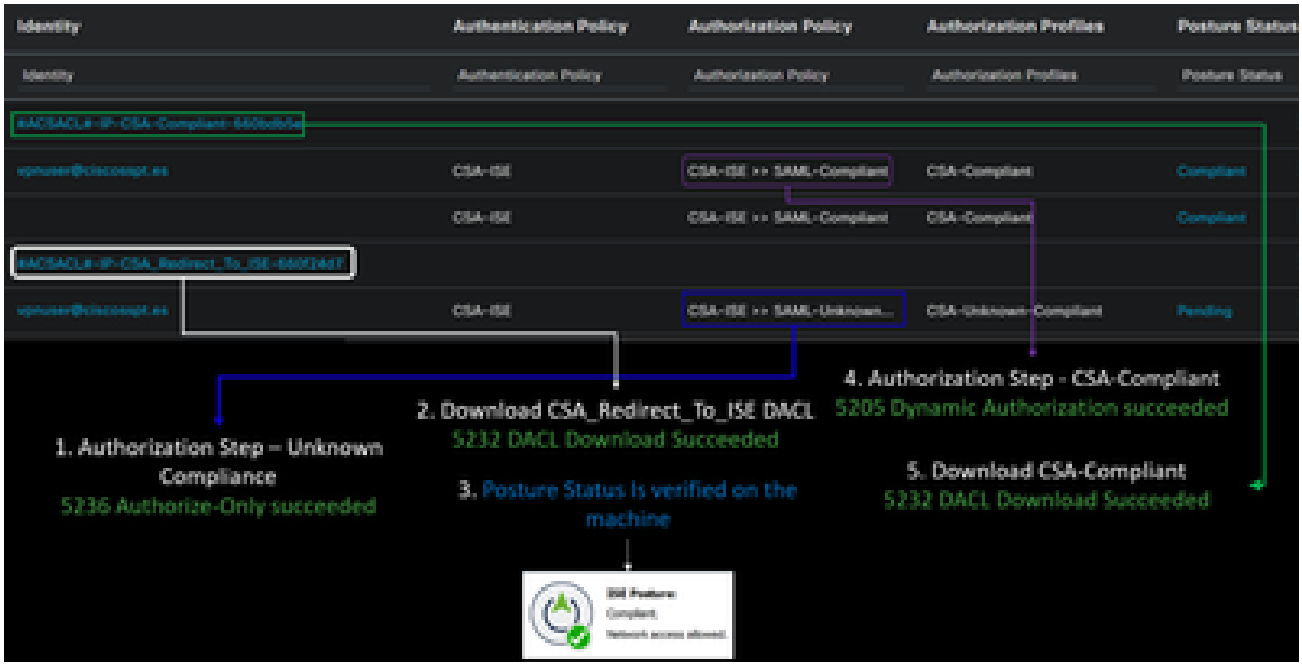
3つのプロファイルの設定を終了すると、ポスチャとの統合をテストする準備が整います。

確認

ポスチャ検証

マシン上の接続

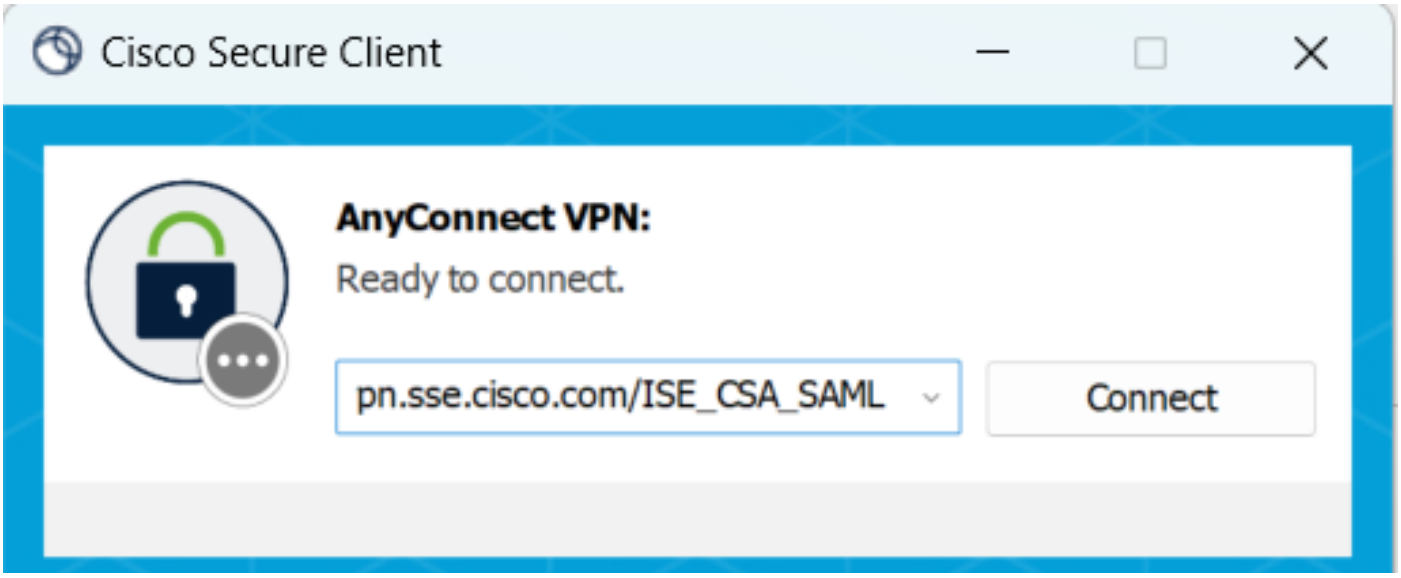
セキュアクライアント経由のセキュアアクセスで提供されるFQDN RA-VPNドメインに接続します。



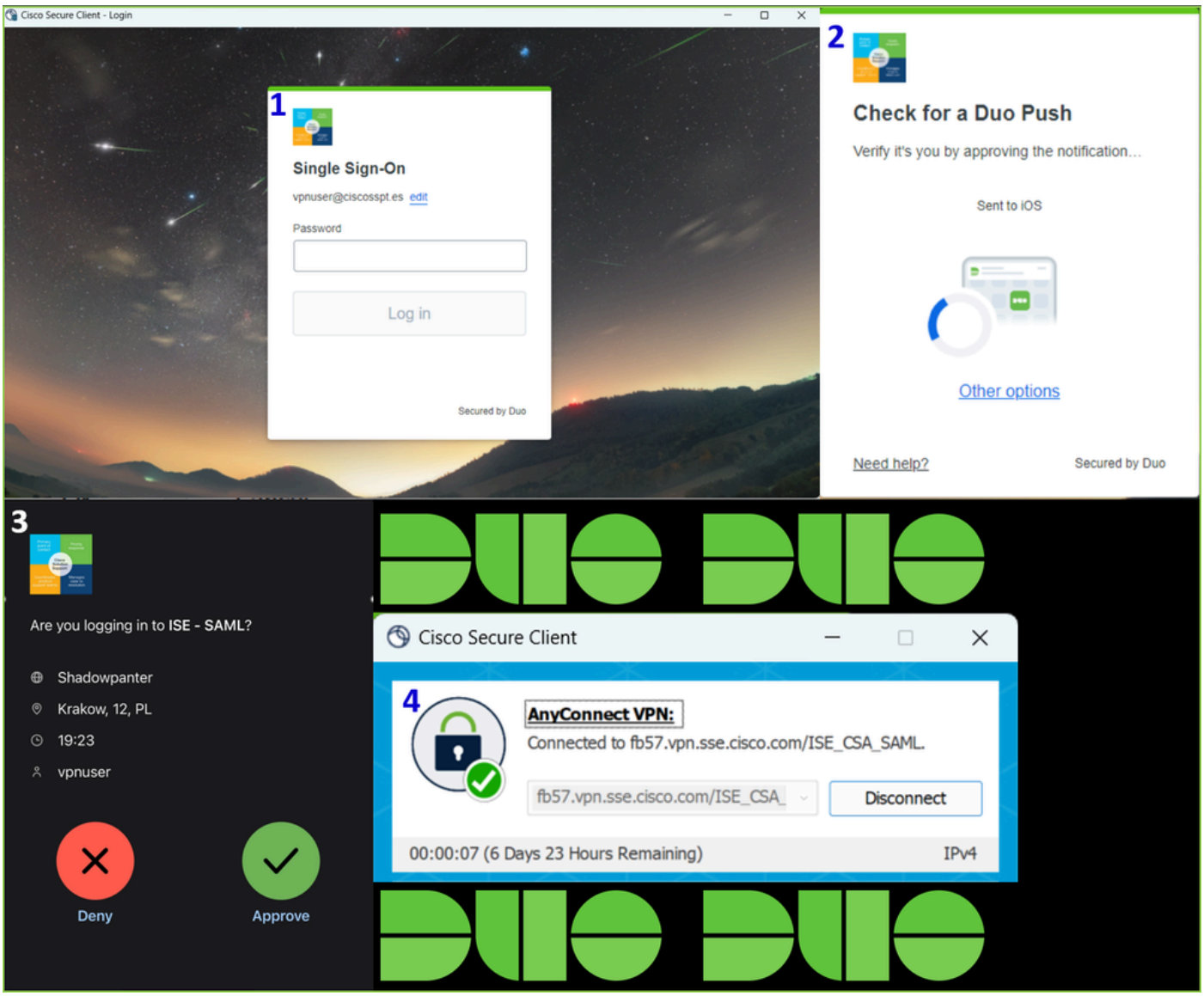
注：この手順では、ISEモジュールをインストールする必要はありません。

---

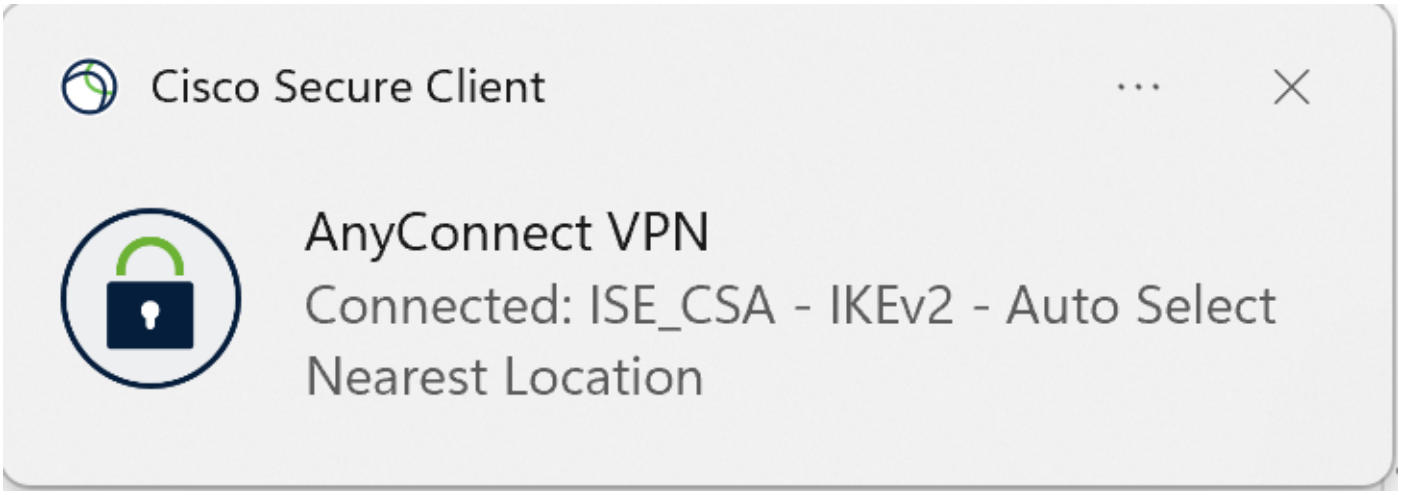
1. セキュアクライアントを使用して接続します。

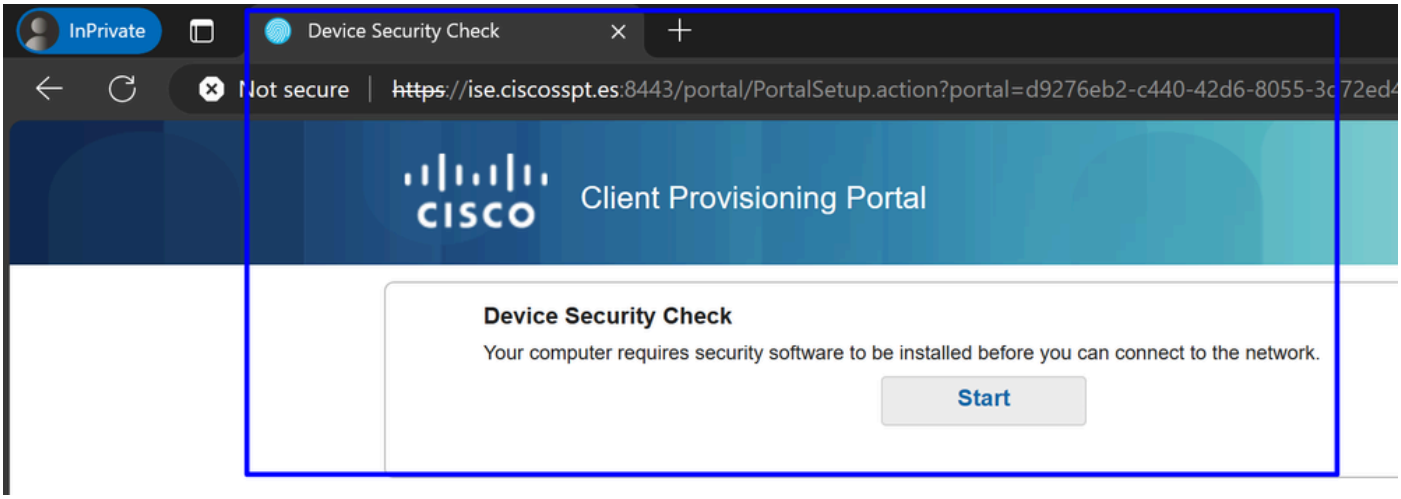


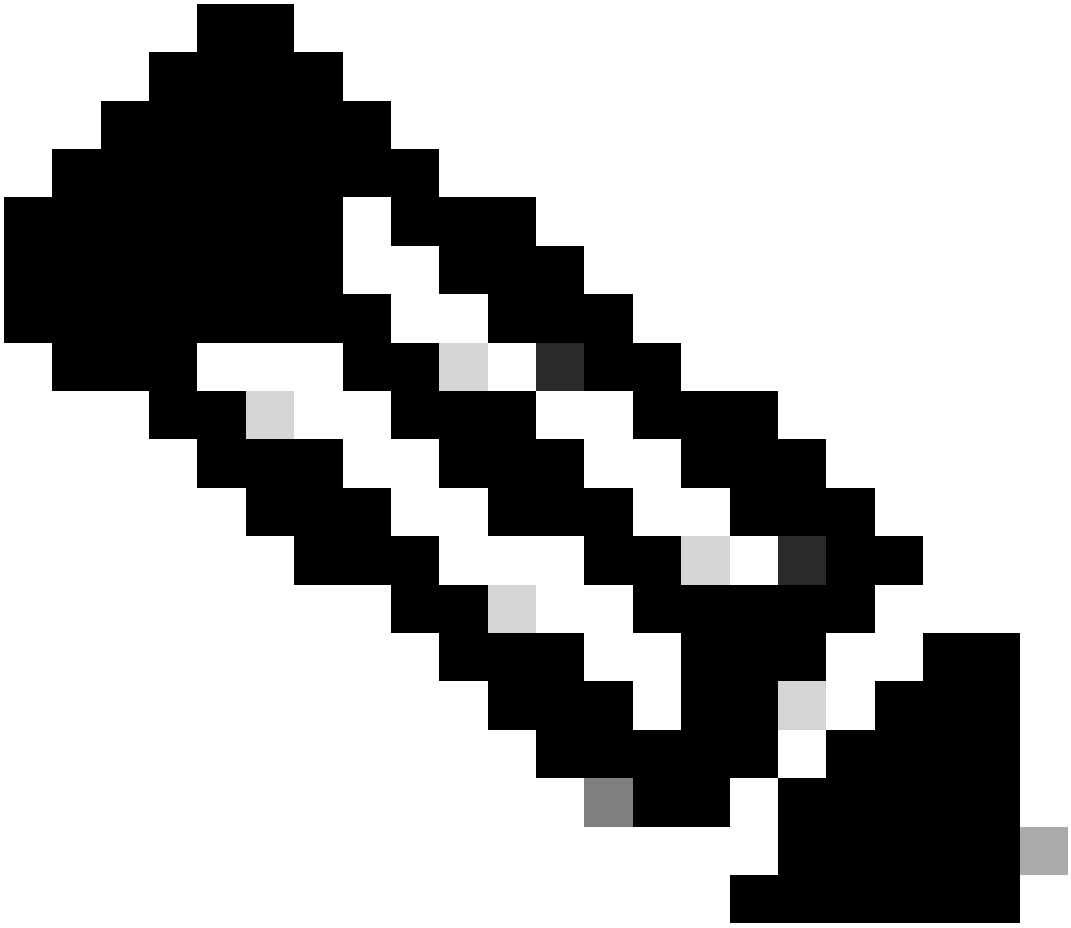
2. Duoを介して認証するための資格情報を入力します。



3. この時点で、あなたはVPNに接続し、たいていISEにリダイレクトされます。リダイレクトされない場合は、**http:1.1.1.1**に移動します。


Cisco Secure Client
AnyConnect VPN
Connected: ISE_CSA - IKEv2 - Auto Select
Nearest Location

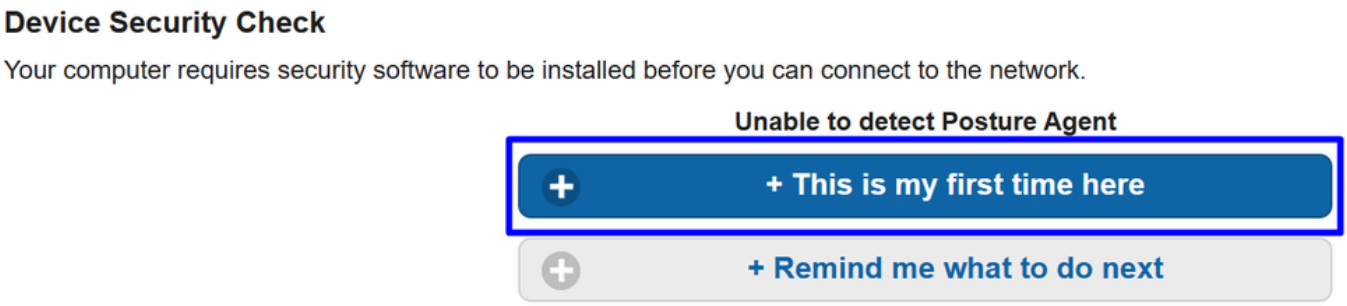

InPrivate
Device Security Check
Not secure
https://ise.ciscosspt.es:8443/portal/PortalSetup.action?portal=d9276eb2-c440-42d6-8055-3c72ed4
Client Provisioning Portal
Device Security Check
Your computer requires security software to be installed before you can connect to the network.
Start



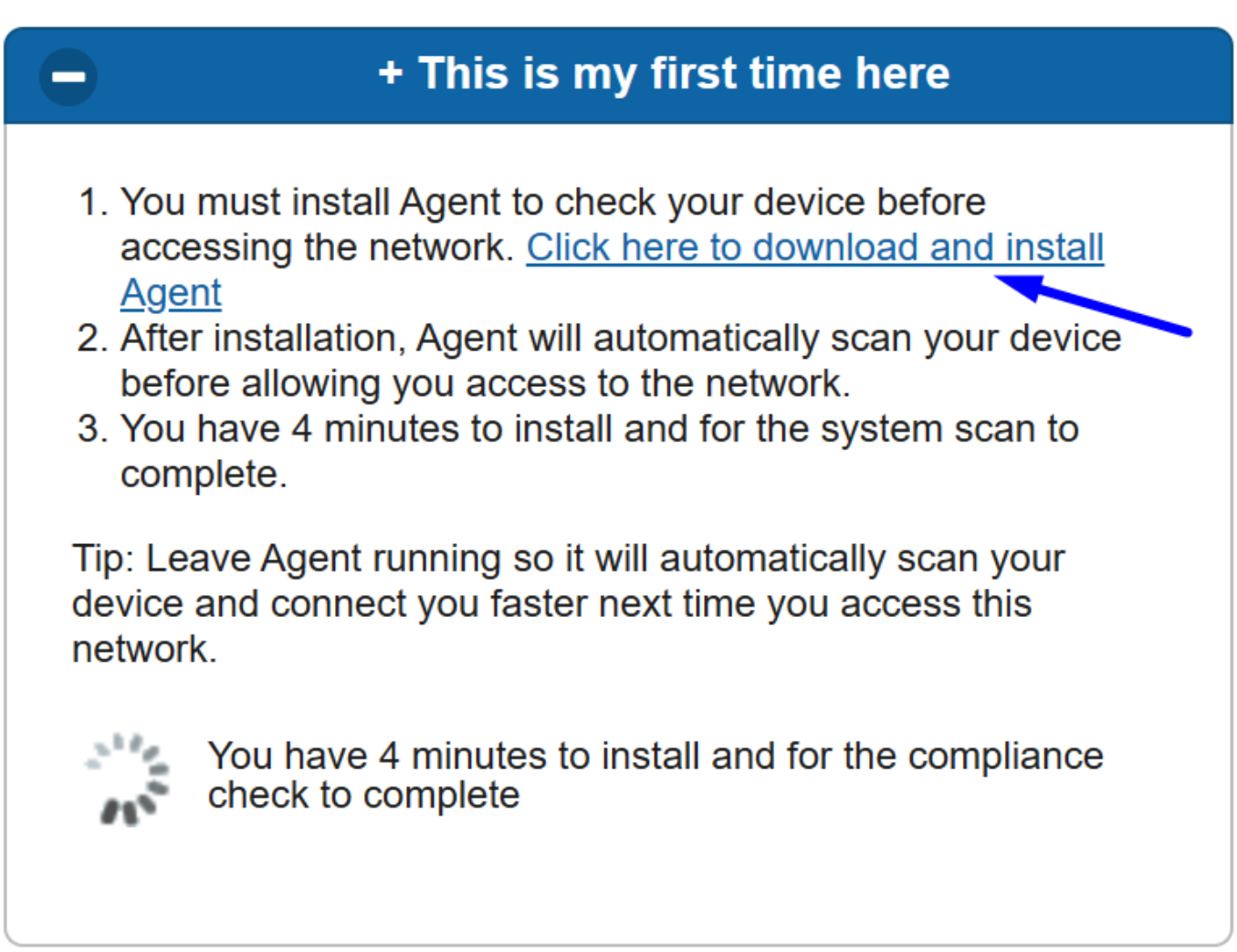
注：この時点では、マシンにISEポスチャエージェントがインストールされていないため、認証 – ポリシーセットCSA-Unknown-Complianceに分類されますが、ISEプロビジョニングポータルにリダイレクトされてエージェントがインストールされます。

4. [開始]をクリックして、エージェントのプロビジョニングを続行します。

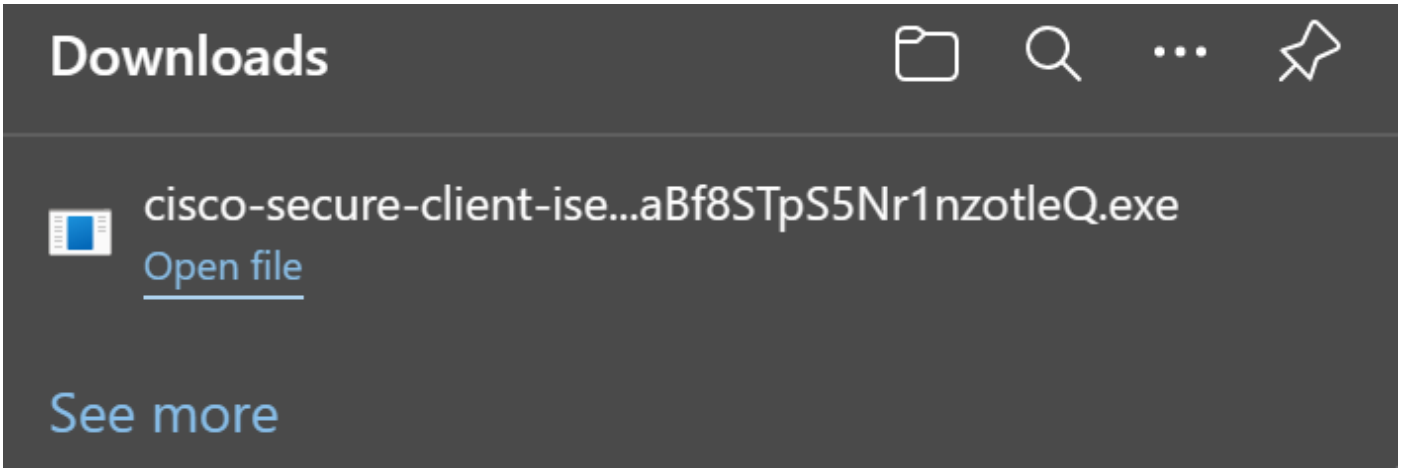
5. 「**+ This is my first time here**」をクリックします。

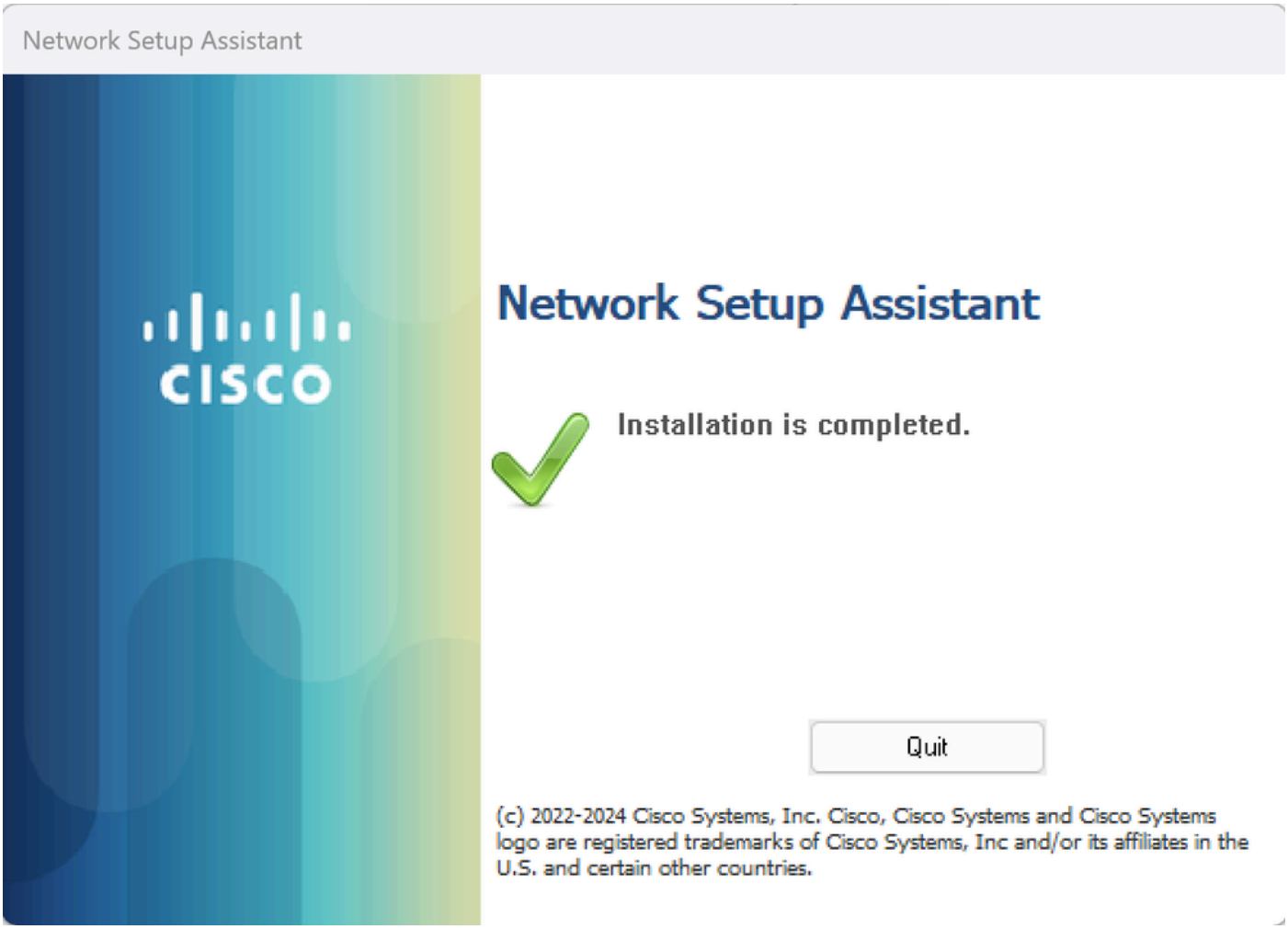


6. クリック **Click here to download and install agent**

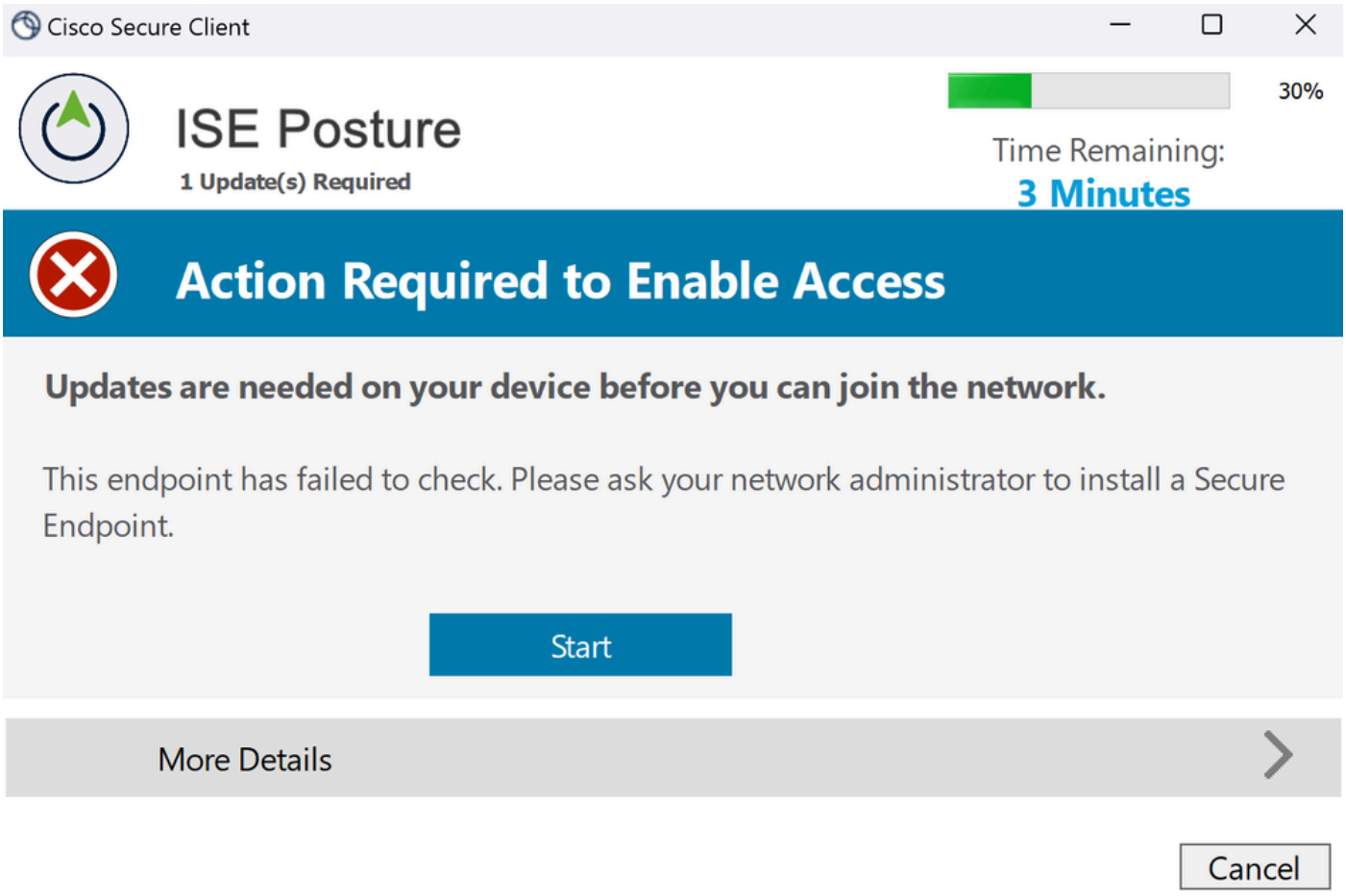


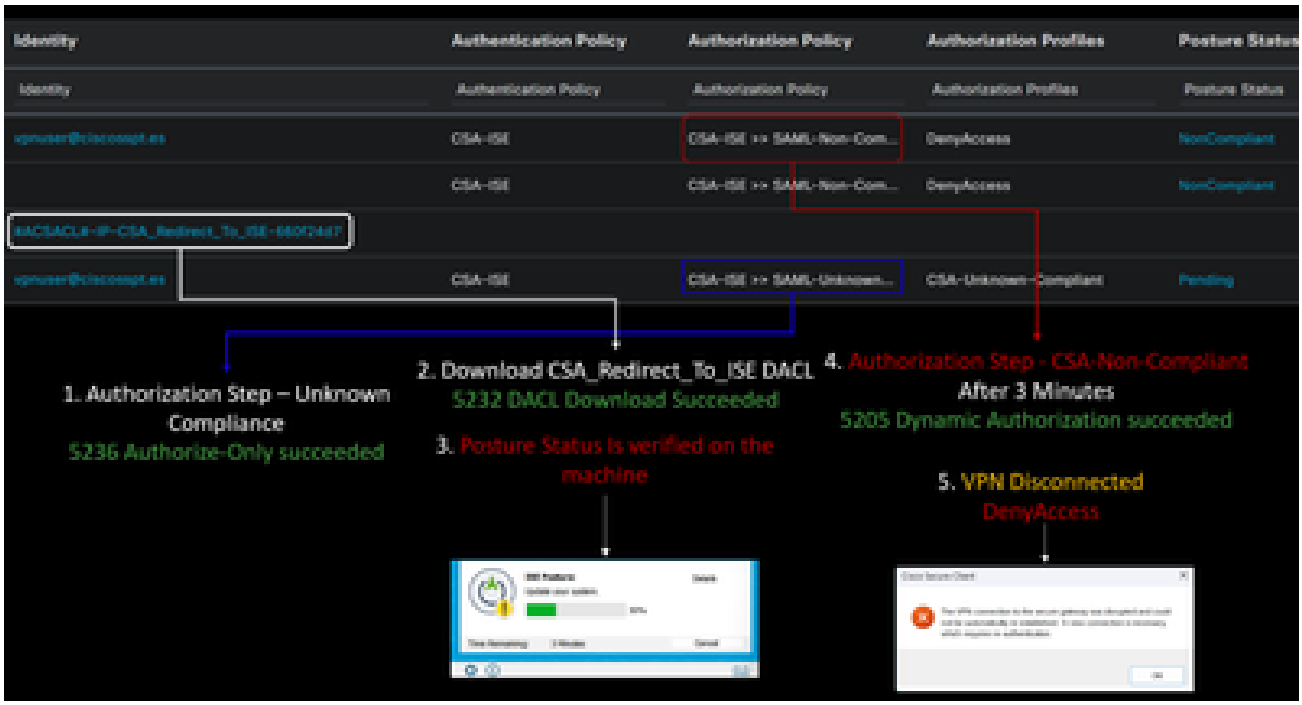
7. エージェントのインストール





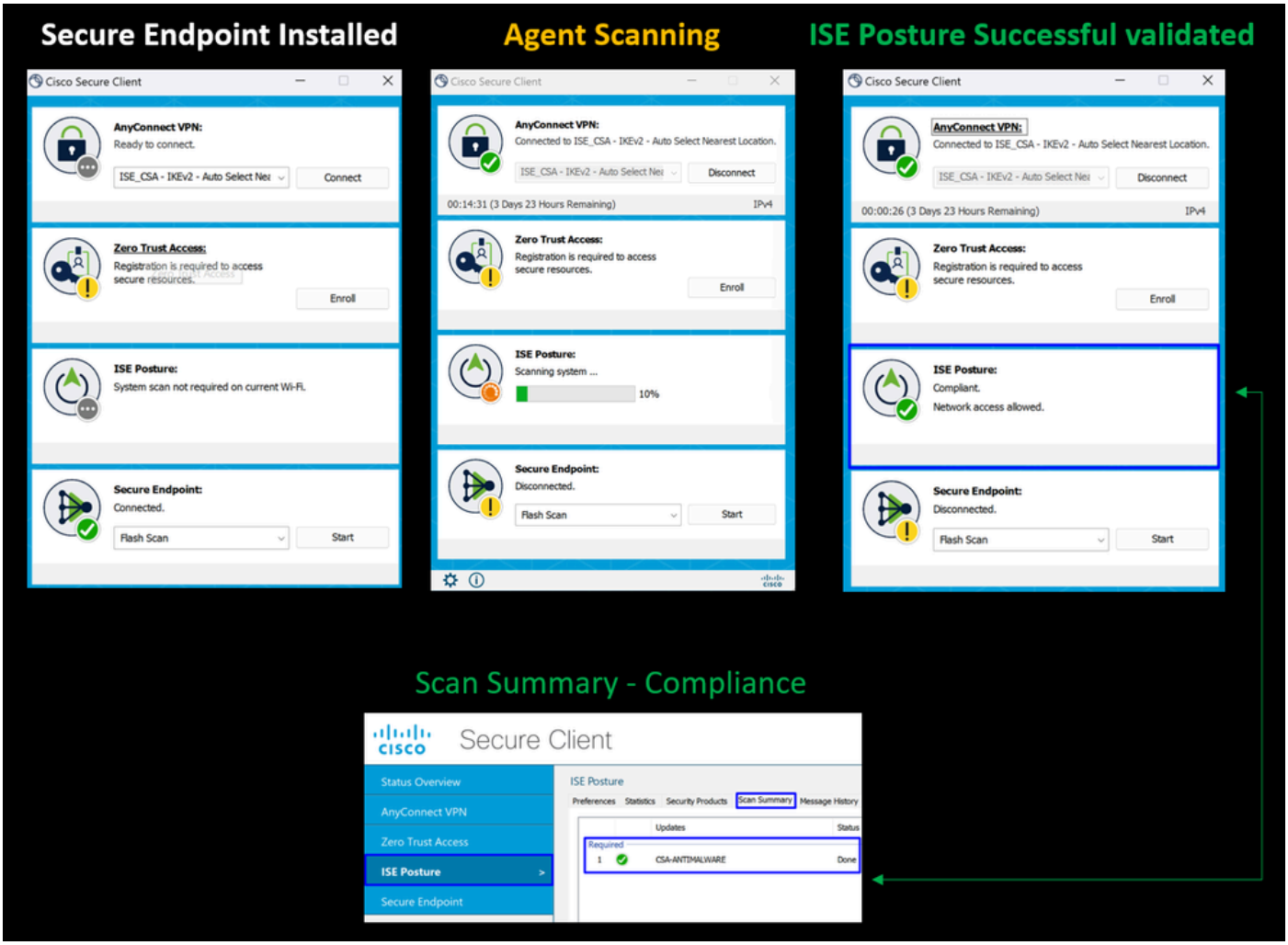
8. エージェントのインストール後、ISEポスチャはマシンの現在のポスチャの確認を開始します。ポリシー要件を満たしていない場合は、コンプライアンスに向けて誘導するポップアップが表示されます。


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

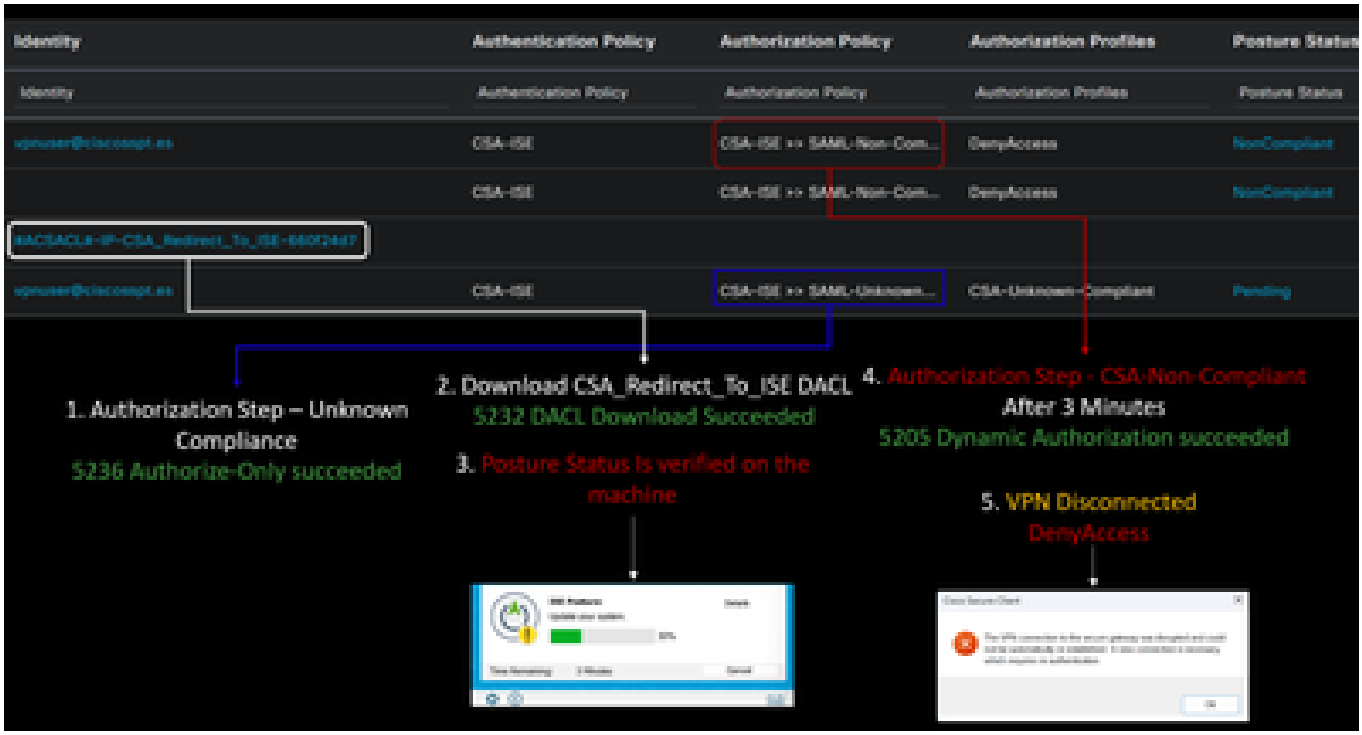

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE 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:Cancelまたは残りの時間が終了すると、自動的に非準拠になり、認可ポリシーセットCSA-Non-Complianceに分類され、すぐにVPNから切断されます。

9. セキュアエンドポイントエージェントをインストールし、VPNに再接続します。



10. エージェントがマシンが準拠していることを確認した後、ポスチャは準拠に変わり、ネットワーク上のすべてのリソースへのアクセスを許可します。

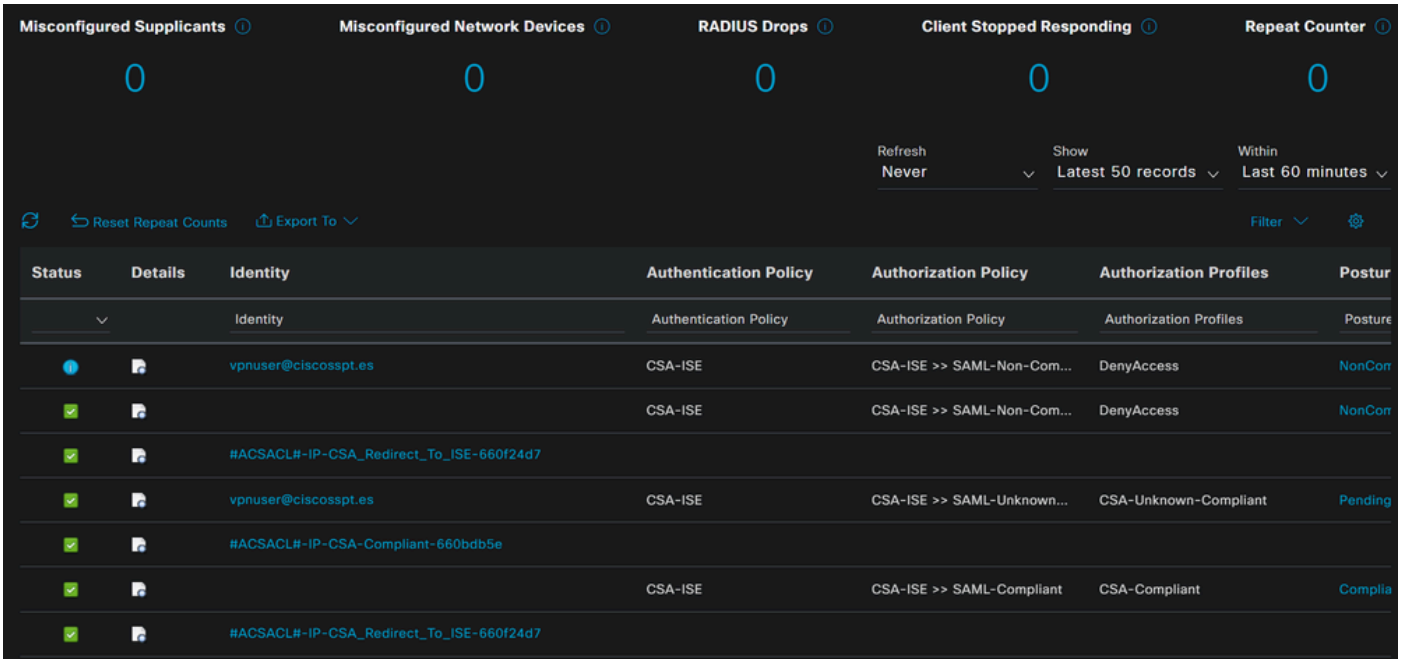


注：準拠レベルに達すると、許可ポリシーセットCSA-Complianceの対象となり、すべてのネットワークリソースにすぐにアクセスできるようになります。

ISEでログを確認する方法

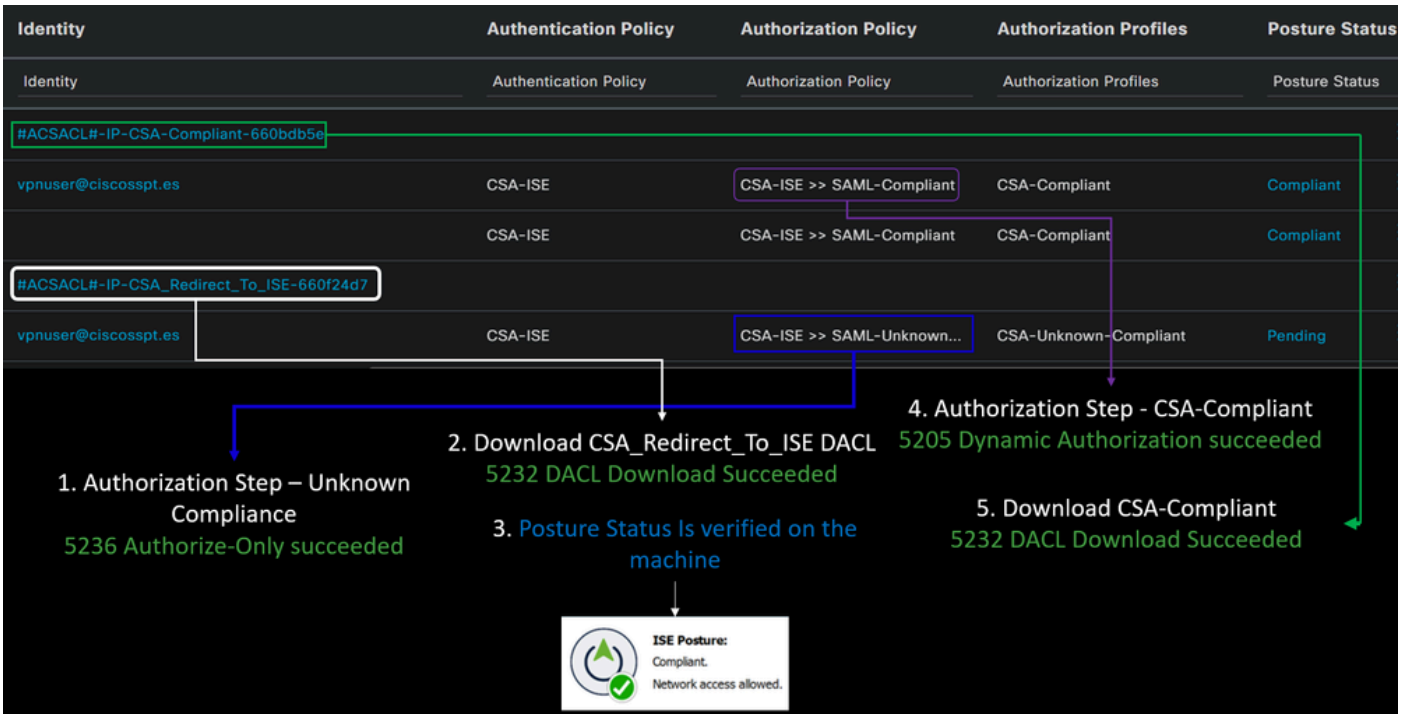
ユーザの認証結果を確認するには、コンプライアンスと非コンプライアンスの2つの例があります。ISEで確認するには、次の手順に従います。

- ISEダッシュボードに移動します
- クリック Operations > Live Logs

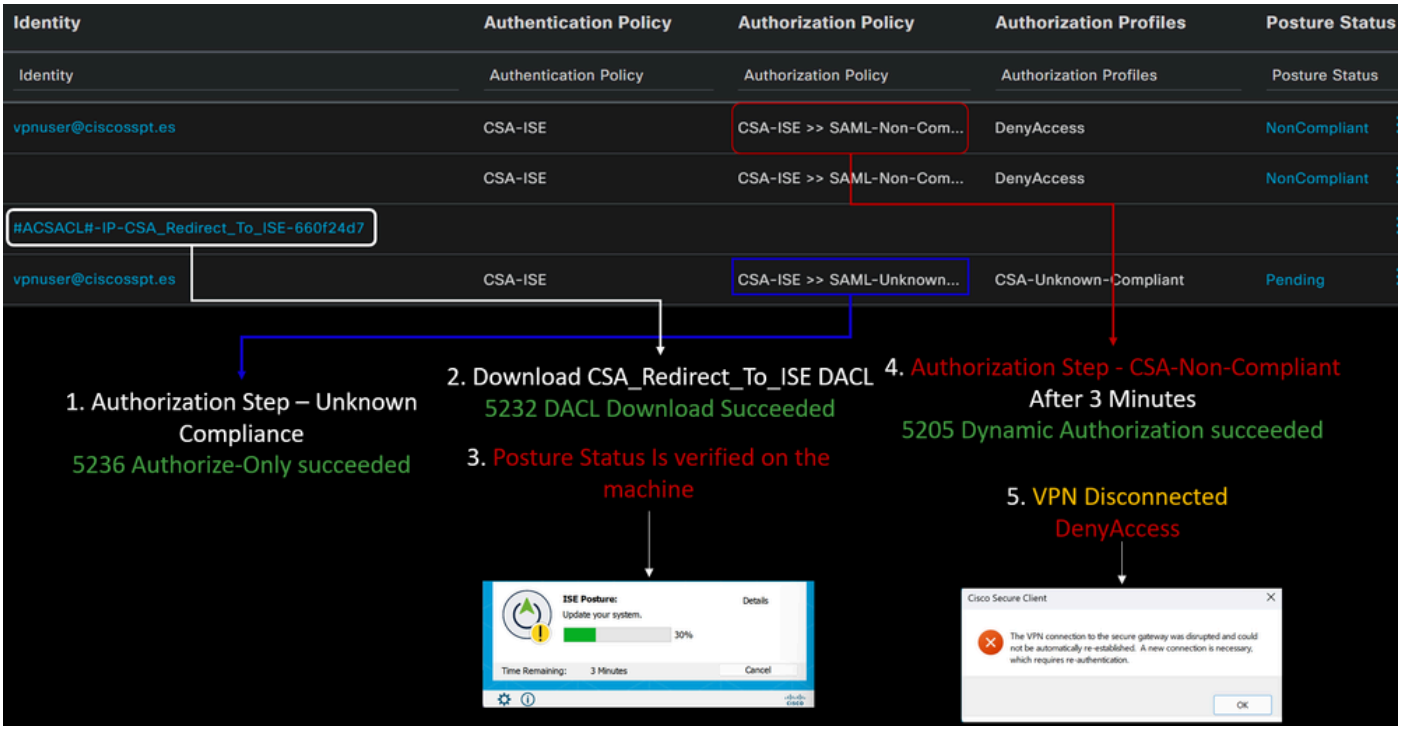


次のthoシナリオでは、 **Live Logs**に準拠イベントと非準拠イベントがどのように表示されるかを示します。

準拠



非準拠



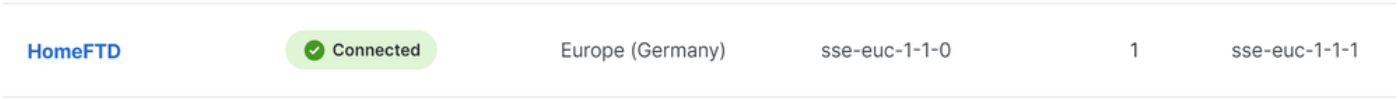
セキュアアクセスとISE統合の最初のステップ

次の例では、Cisco ISEはネットワーク192.168.10.0/24の下にあり、トンネルを介して到達可能なネットワークの設定をトンネル設定の下に追加する必要があります。

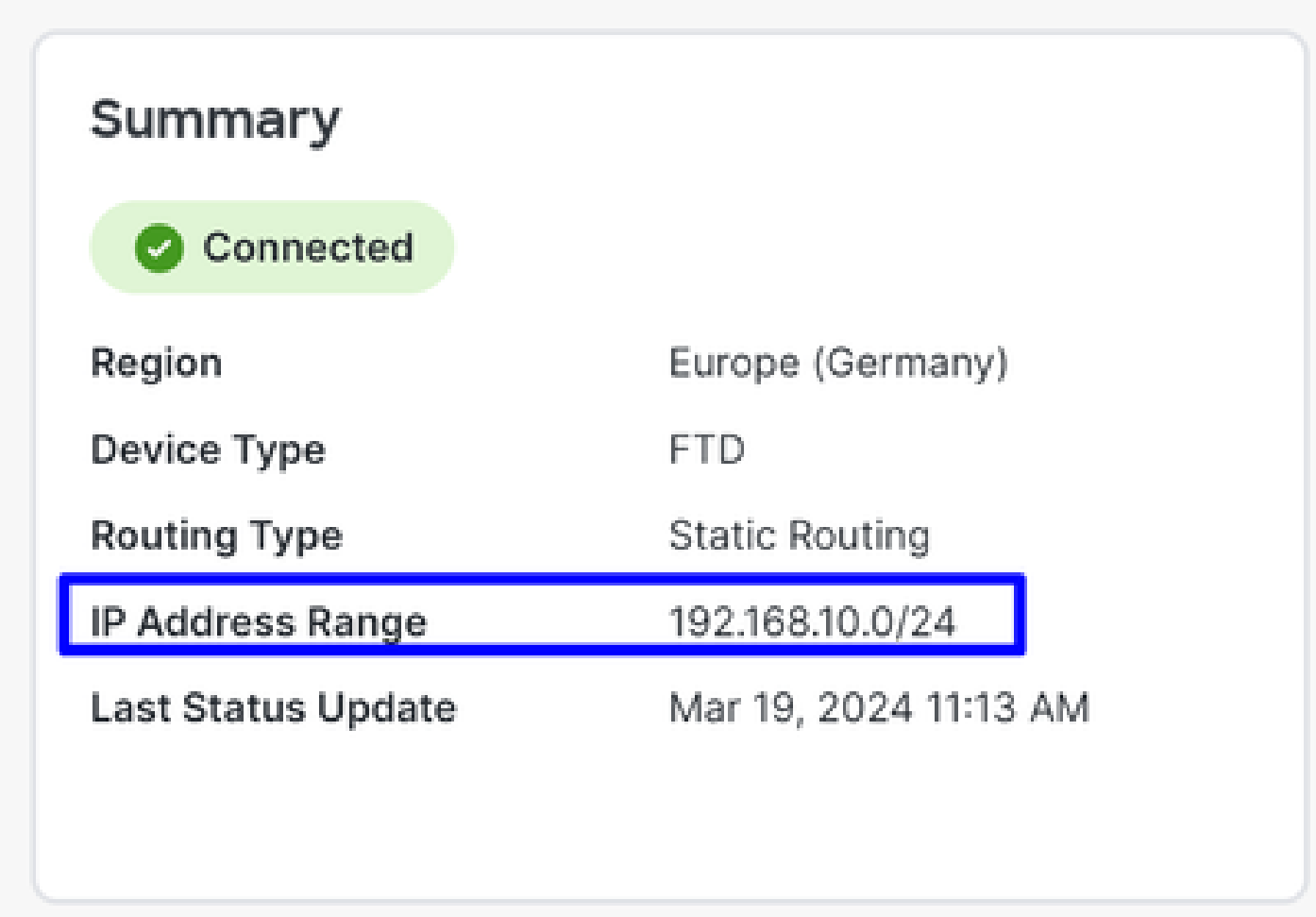
Step 1：トンネル設定を確認します。

これを確認するには、セキュアアクセスダッシュボードに移動してください。

- クリック **Connect** > **Network Connections**
  Network Tunnel Groups
- > Your Tunnelをクリックします。



- summaryの下で、Cisco ISEが存在するアドレス空間がトンネルに設定されていることを確認します。

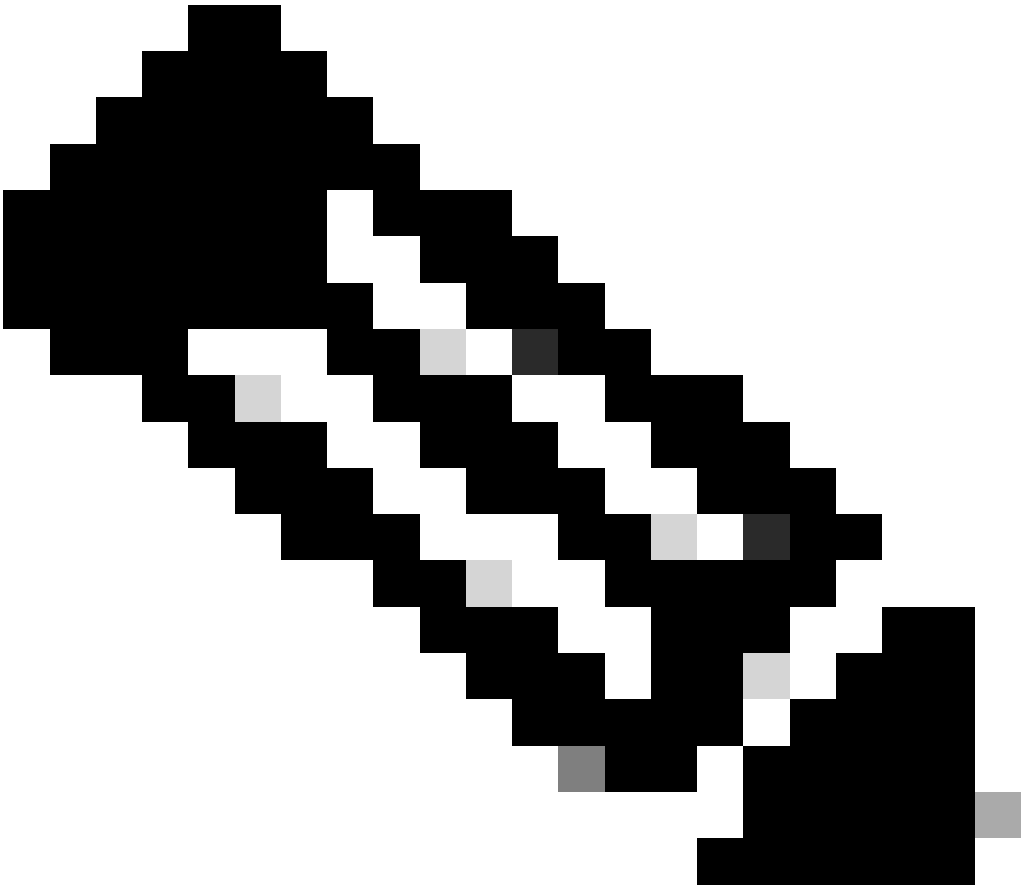


Step 2：ファイアウォールでトラフィックを許可します。

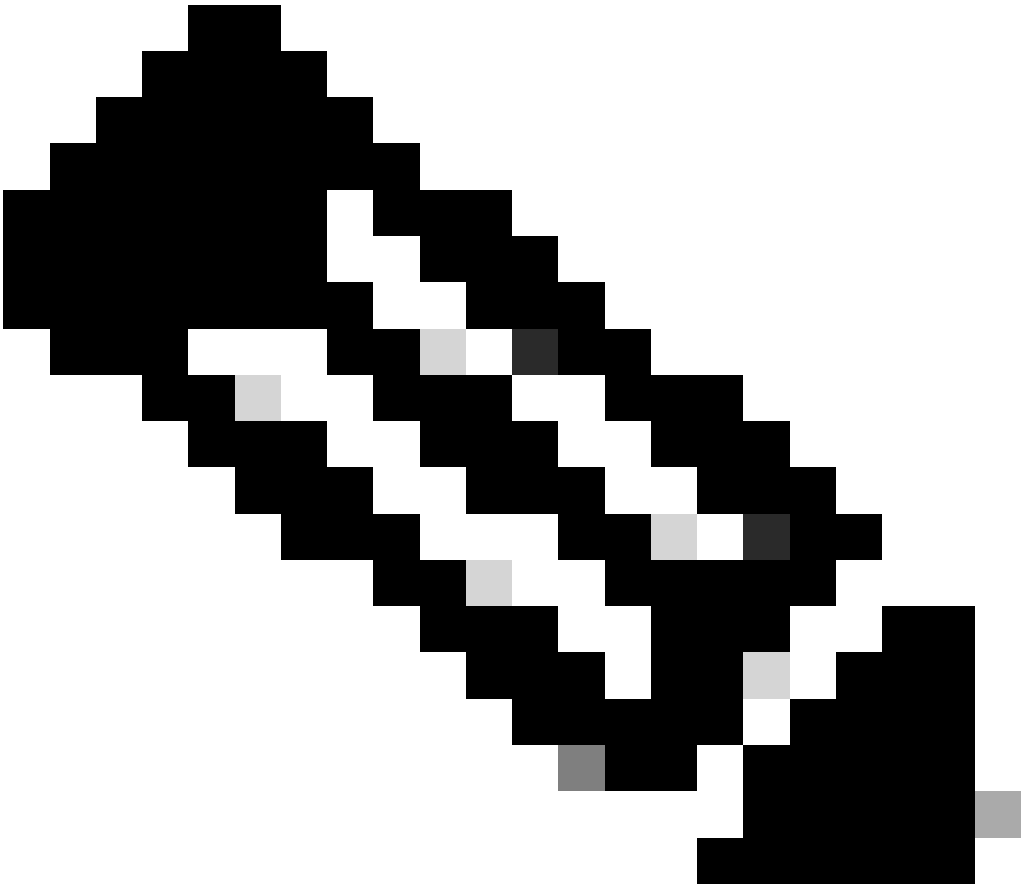
セキュアアクセスでRADIUS認証にISEデバイスを使用できるようにするには、ネットワークへのセキュアアクセスからのルールを、必要なRADIUSポートで設定する必要があります。

ルール	出典	宛先	宛先ポート
ISEによるセキュアなアクセス **管理プール**	ISE_サーバ	管理IPプール(RA-VPN)	**COA** UDP 1700（デフォルトポート）
ISEへのセキュアアクセス管理IPプール	管理IPプール	ISE_サーバ	**認証、許可** UDP 1812（デフォルトポート） **アカウンティング** UDP 1813（デフォルトポート）
ISEへのセキュアアクセスエンドポイントIPプール	エンドポイントIPプール	ISE_サーバ	**Provisioningポータル** TCP 8443（デフォルトポート）

DNSサーバへのセキュアアクセスエンドポイントIPプール	エンドポイントIPプール	DNS サーバ	**DNS** UDPおよびTCP 53



注：ISEに関連するポートの詳細については、『ユーザガイド：ポート参照』を参照してください。



注:ise.ciscosspt.esなどの名前で検出されるようにISEを設定した場合は、DNSルールが必要です。

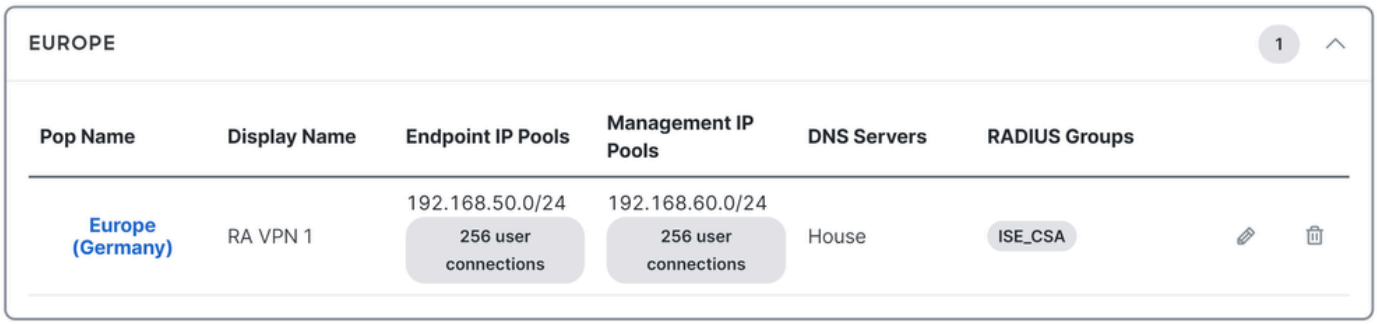
管理プールとエンドポイントIPプール

管理およびエンドポイントIPプールを確認するには、セキュアアクセスダッシュボードに移動します。

- クリック **Connect** > **End User Connectivity**
- クリック Virtual Private Network
-

通常の **Manage IP Pools**

- クリック **Manage**

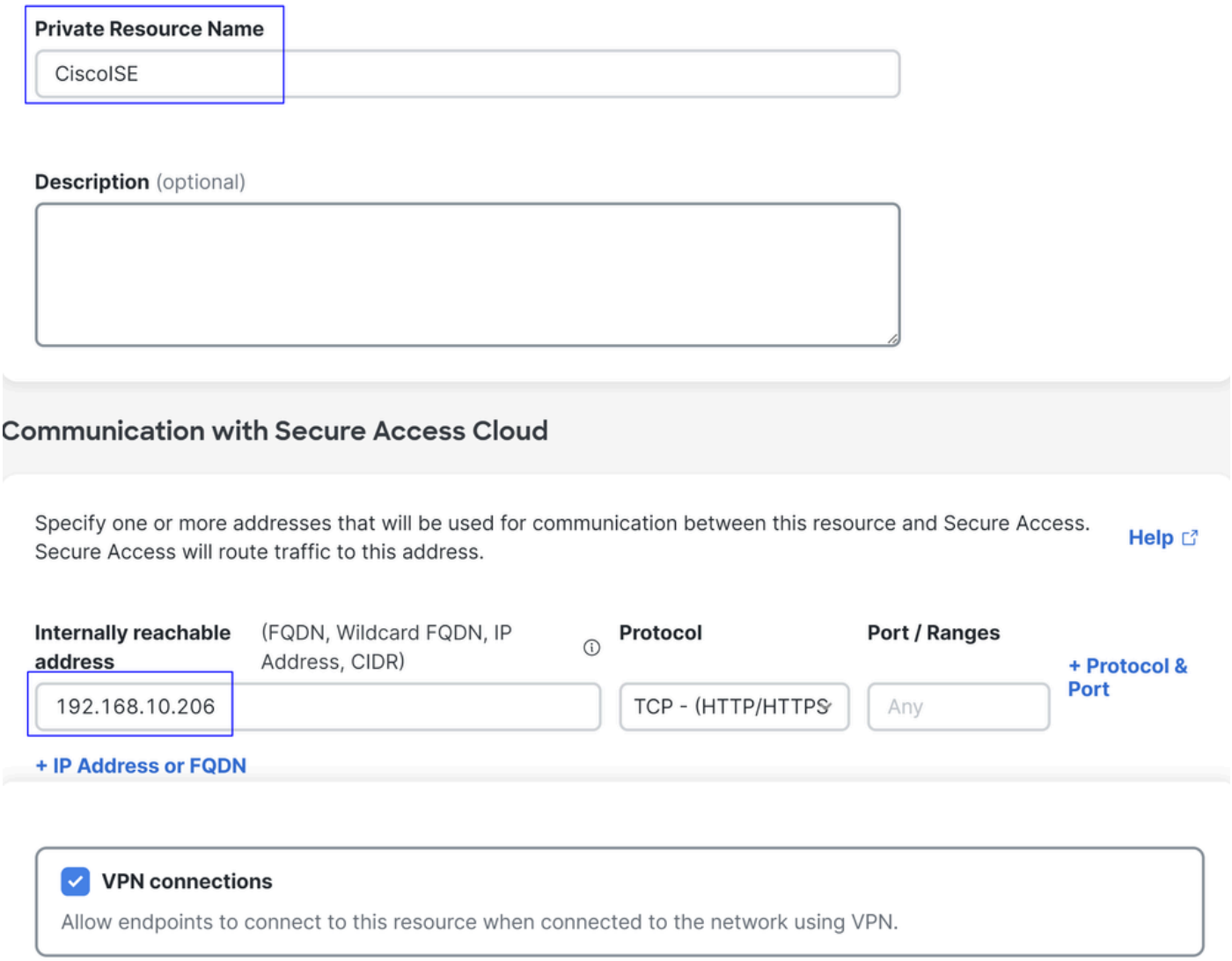


ステップ**3**:ISEがプライベートリソースで設定されていることを確認します

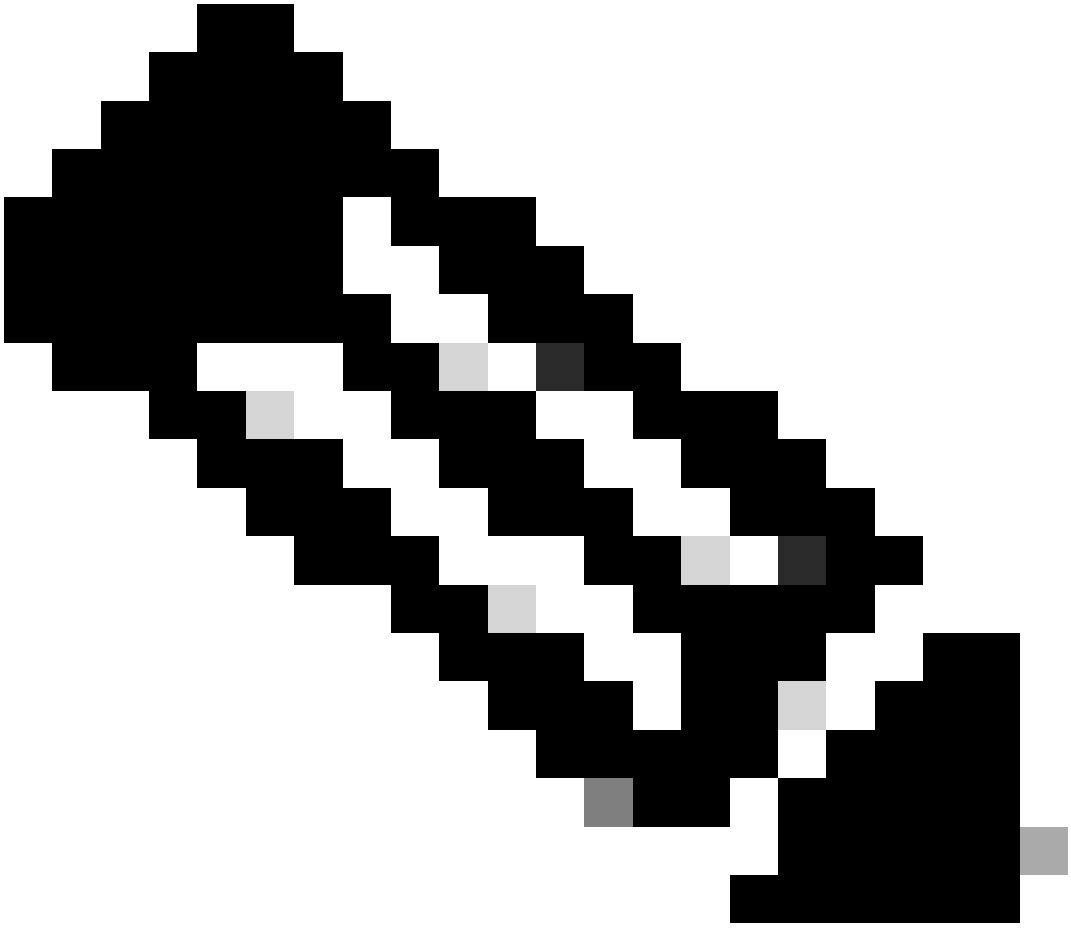
VPN経由で接続しているユーザが**ISE Provisioning Portal**に移動できるようにするには、アクセスを提供するプライベートリソースとしてデバイスを設定している必要があります。このリソースは、VPN経由でISE Posture Moduleの自動プロビジョニングを許可するために使用されます。

ISEが正しく設定されていることを確認するには、セキュアアクセスダッシュボードに移動します。

- クリック **Resources** > **Private Resources**
- ISEリソースをクリックします



必要に応じて、プロビジョニングポータルポート(8443)にルールを制限できます。



注:VPN接続のチェックボックスがオンになっていることを確認してください。

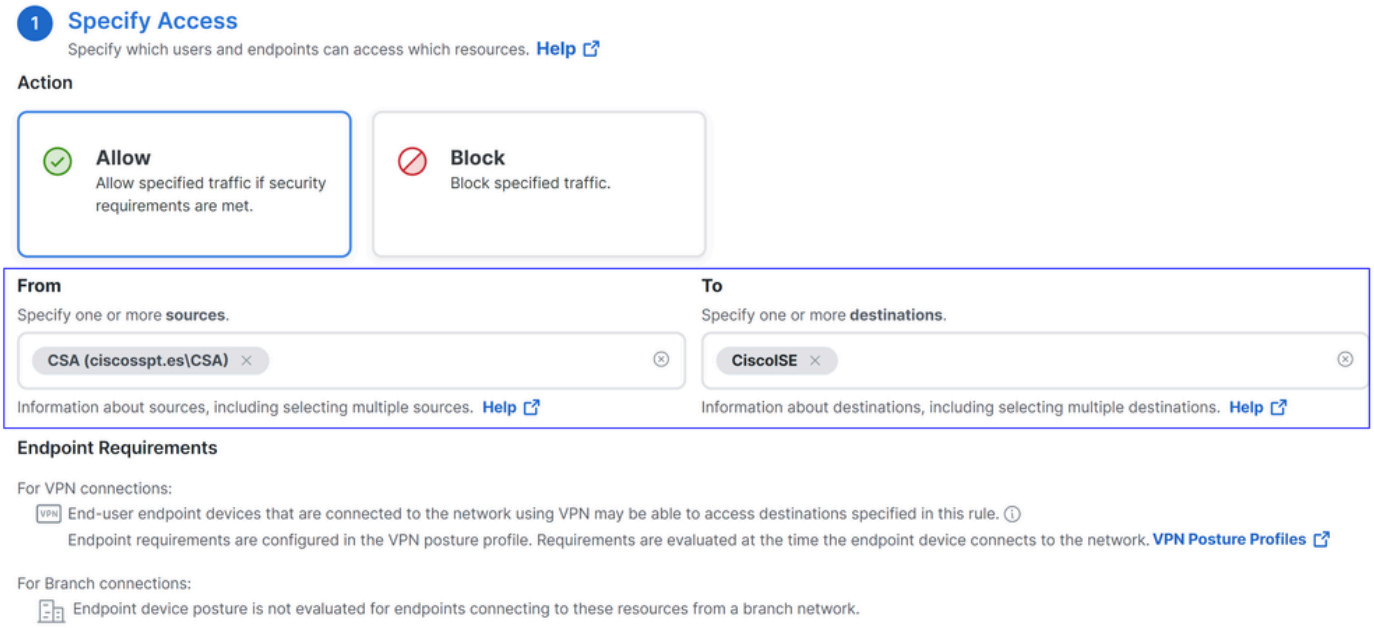
ステップ4：アクセスポリシーでISEアクセスを許可する

VPN経由で接続しているユーザが**ISE Provisioning Portal**に移動できるようにするには、そのルールの下で設定されているユーザに、Step3で設定されているプライベートリソースへのアクセスを許可する**Access Policy** を設定していることを確認する必要があります。

ISEが正しく設定されていることを確認するには、セキュアアクセスダッシュボードに移動します。

- クリック **Secure** > **Access Policy**

- ISEへのVPNユーザのアクセスを許可するために設定されたルールをクリックします



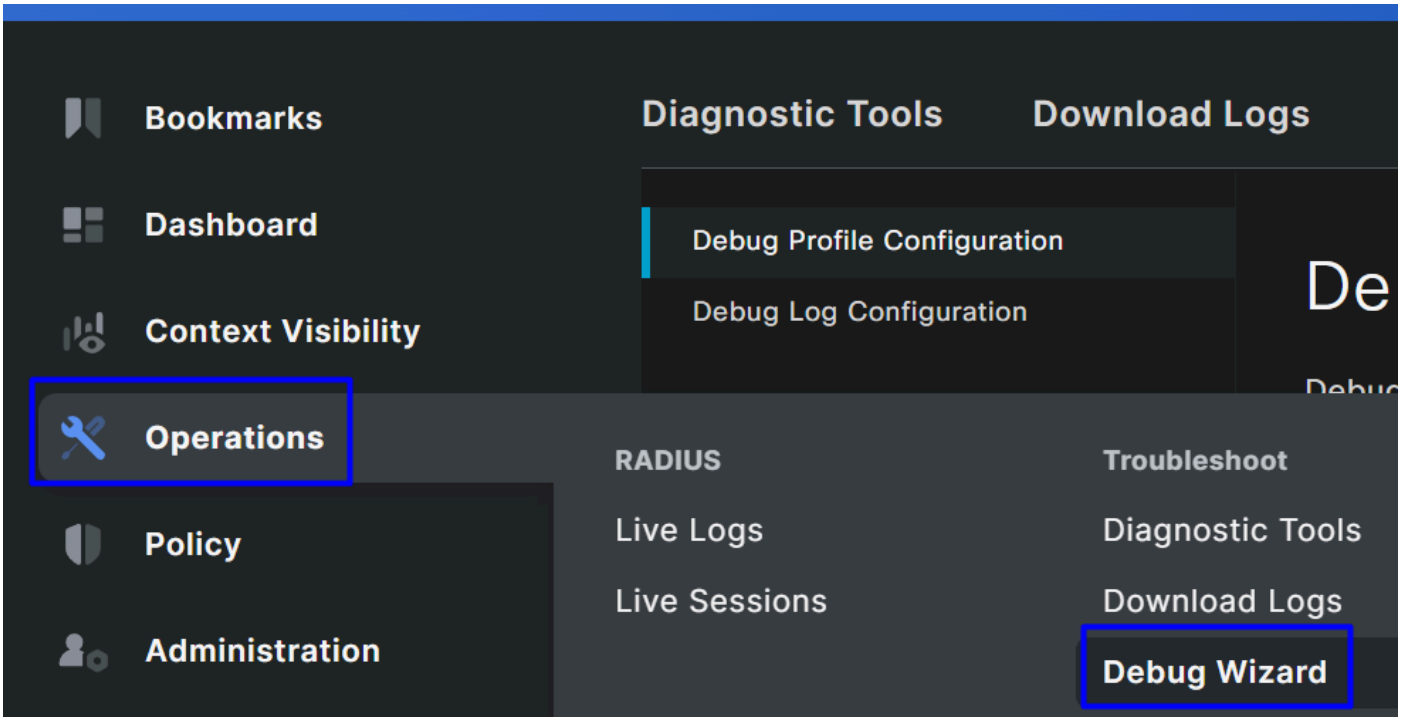
トラブルシュート

ISEポスチャデバッグログのダウンロード方法

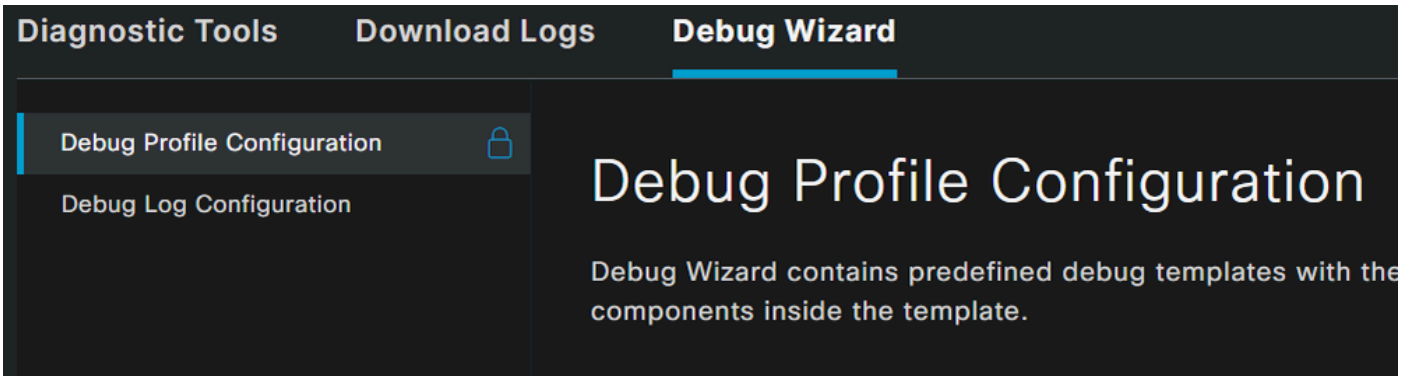
ISEログをダウンロードしてポスチャに関連する問題を確認するには、次の手順に進みます。

- ISEダッシュボードに移動します

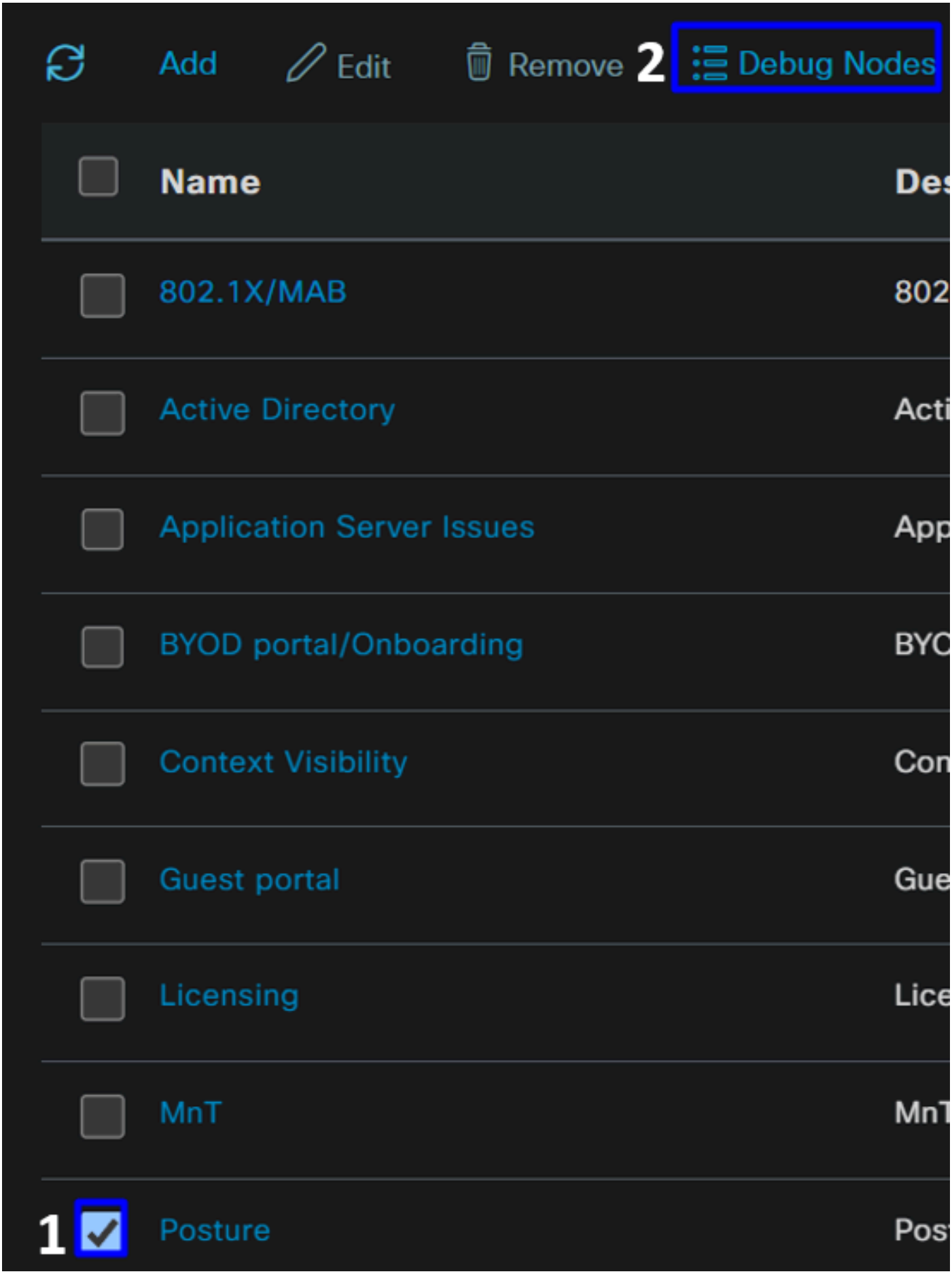
- クリック Operations > Troubleshoot > Debug Wizard



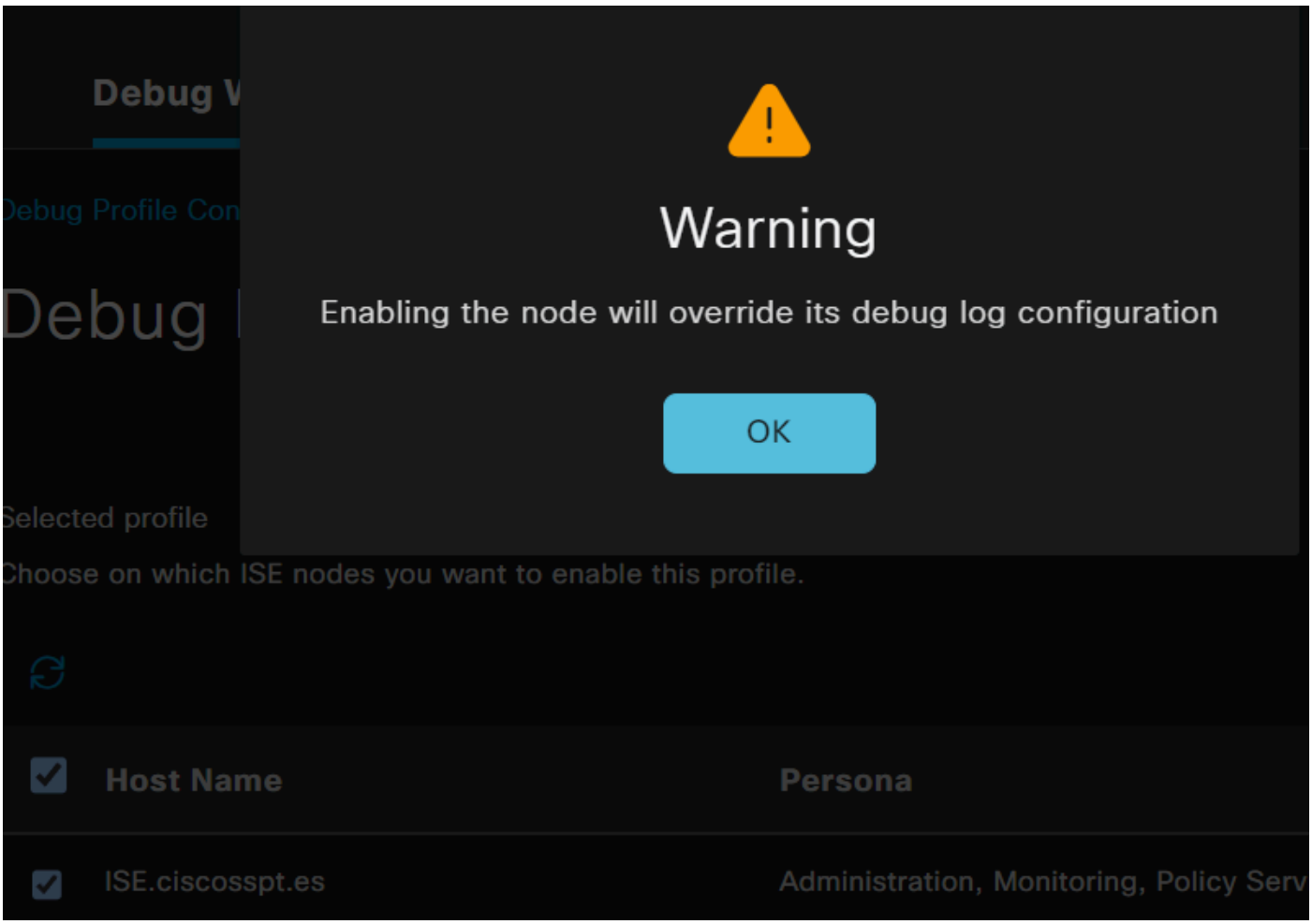
- クリック Debug Profile Configuration



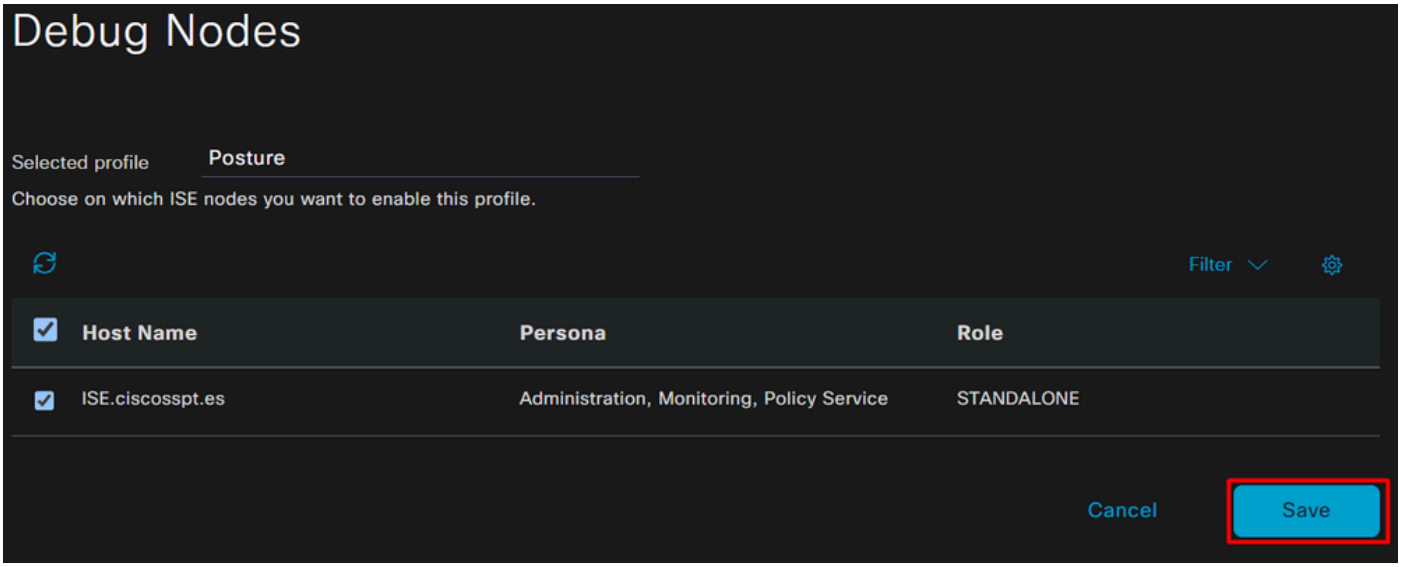
- チェックボックスをオンにする **Posture** > **Debug Nodes**

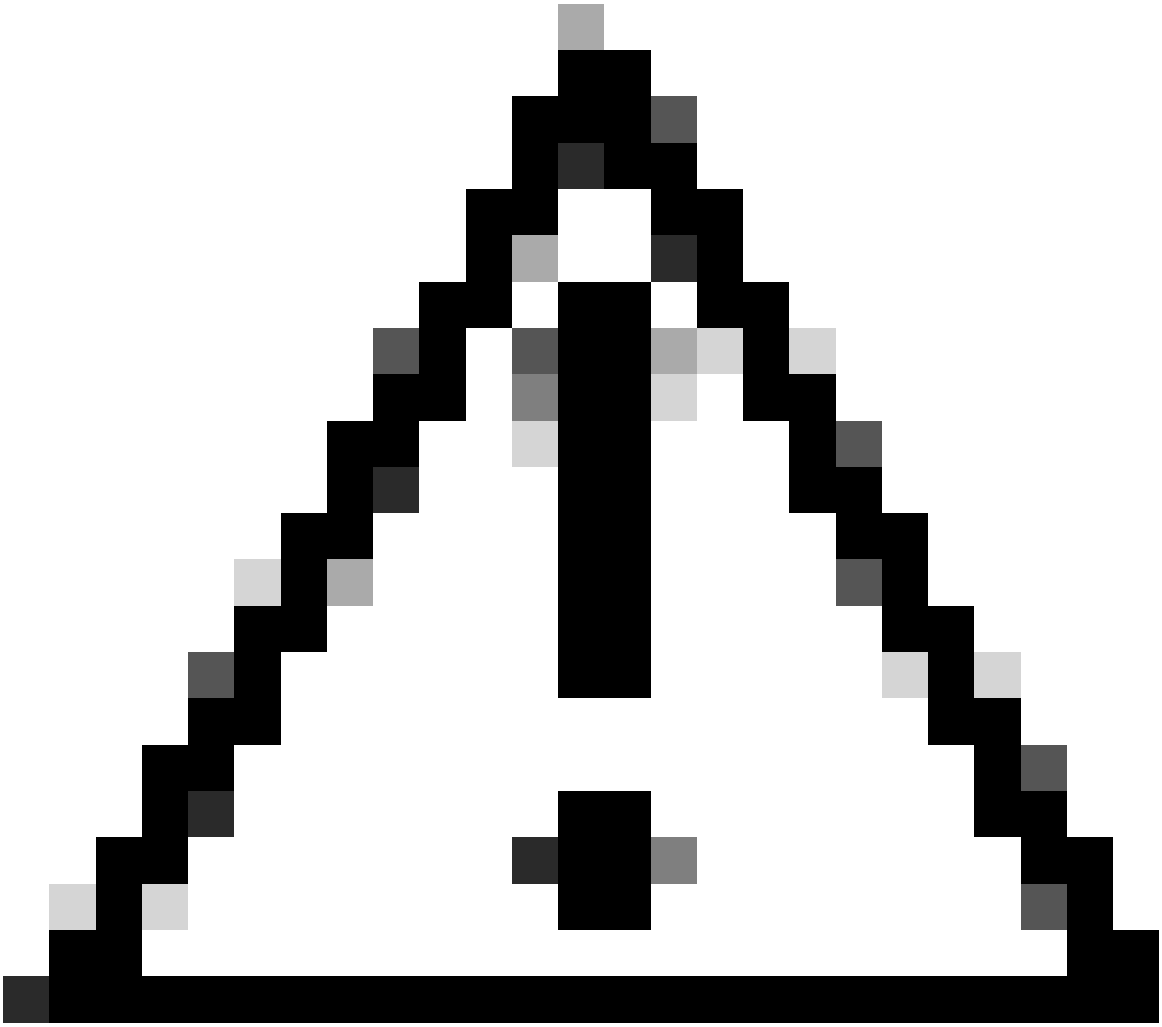

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- 問題をトラブルシューティングするためにデバッグモードを有効にするISEノードのチェックボックスをオンにします



- クリック Save

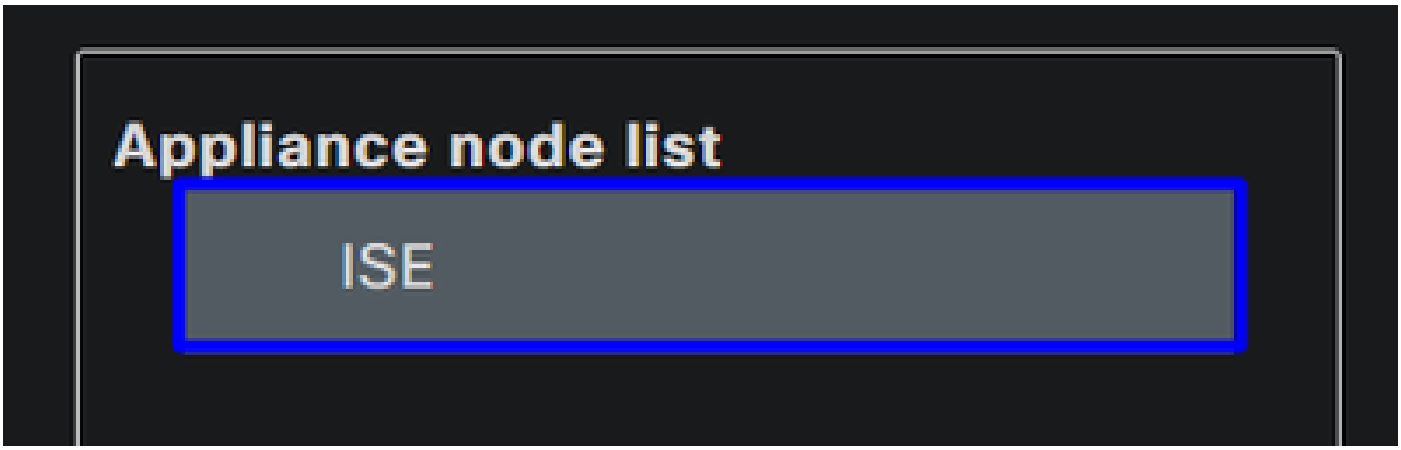

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



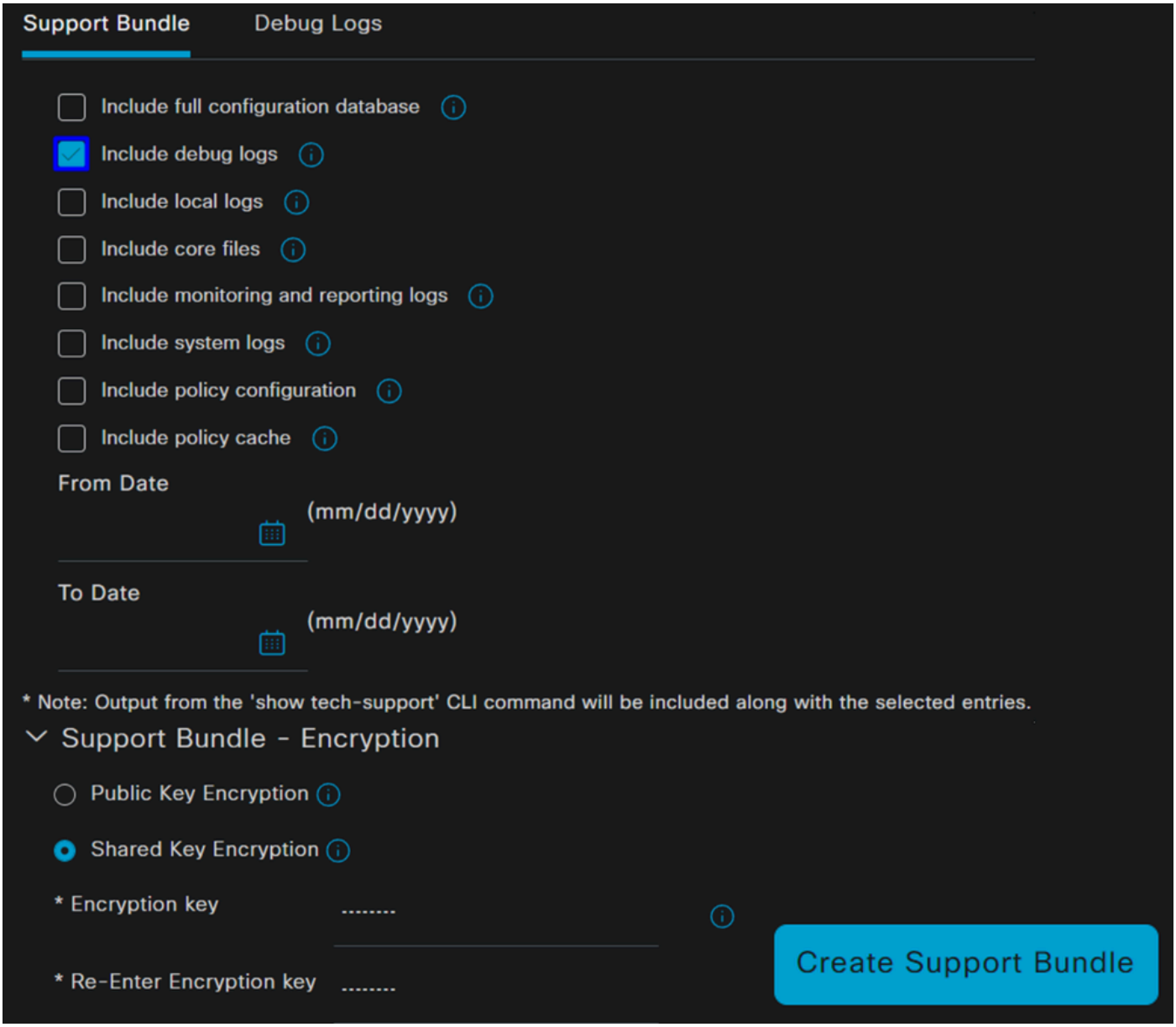
注意：この後、問題の再現を開始してください。 **the debug logs can affect the performance of your device**

問題が再現されたら、次の手順に進みます。

- クリック Operations > Download Logs
- ログを取得するノードを選択します

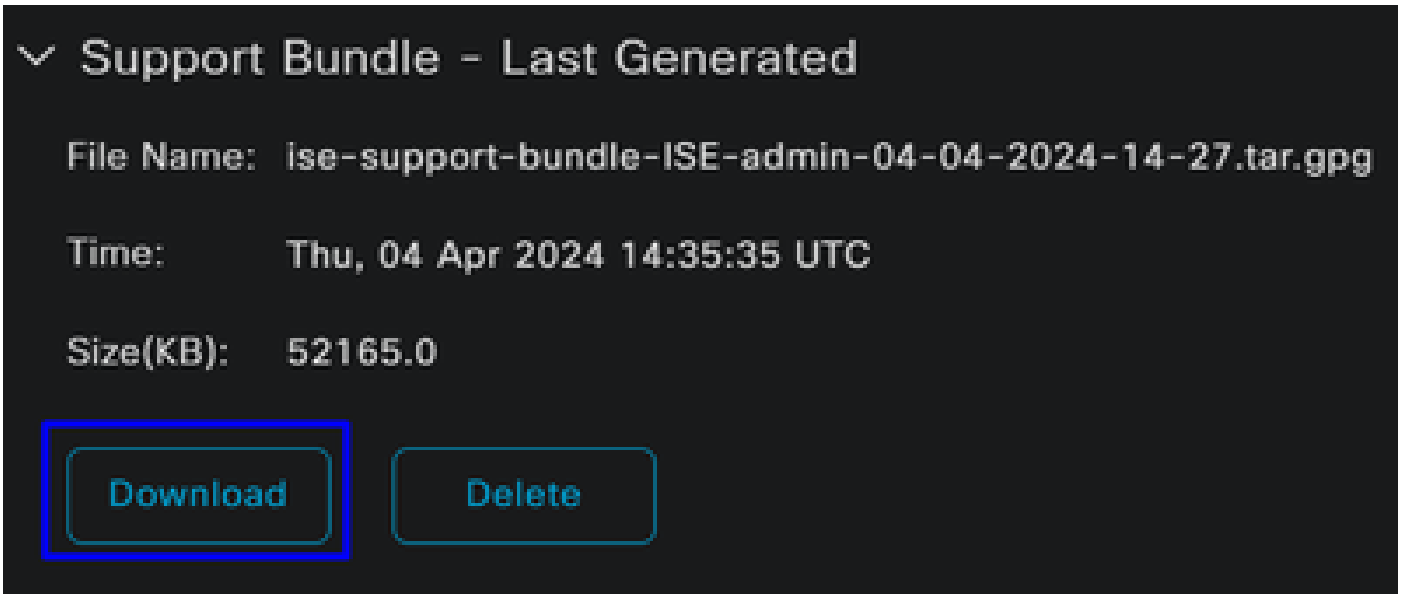


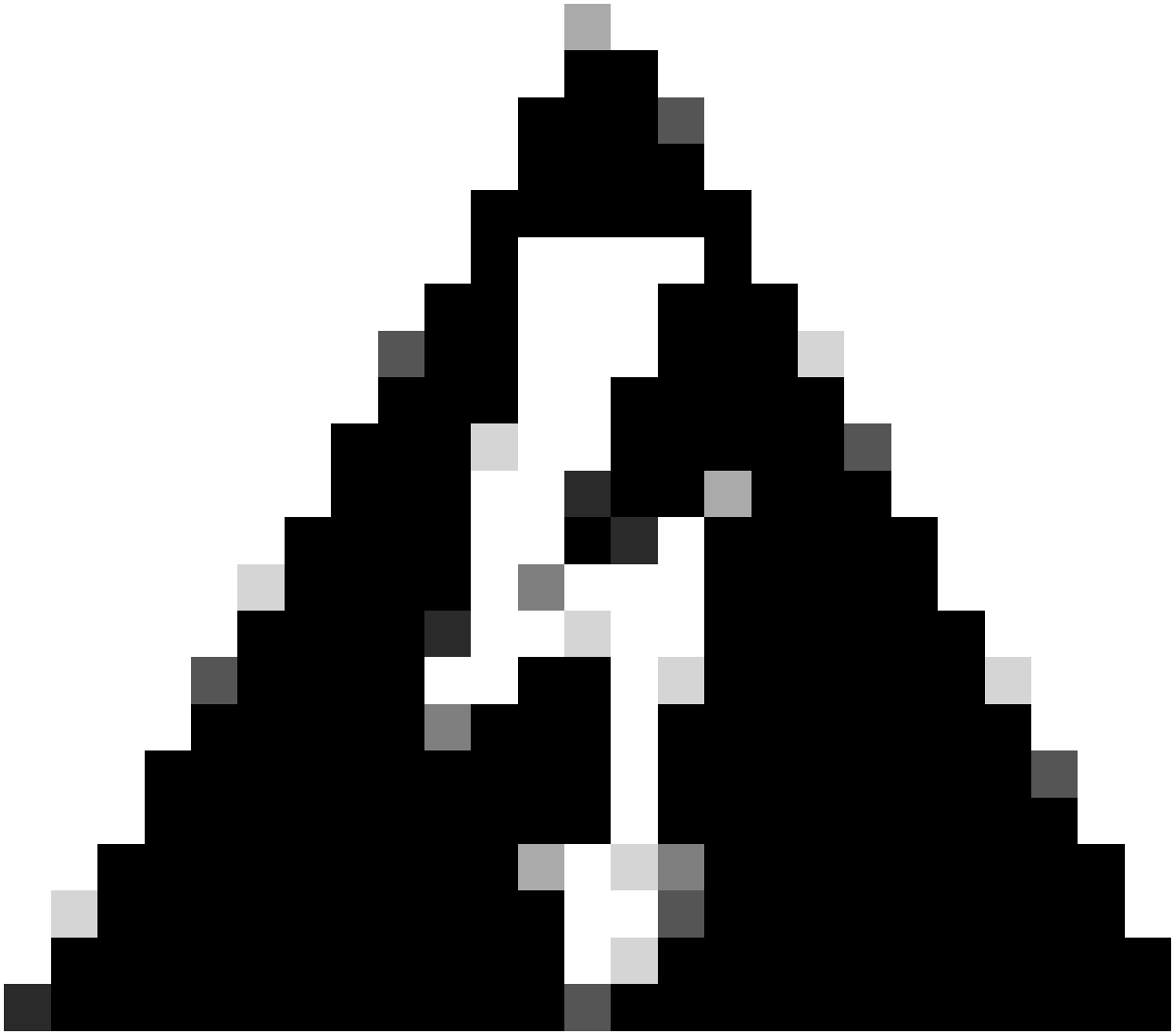
- で **Support Bundle**、次のオプションを選択します。



- Include debug logs
- 通常の **Support Bundle Encryption**
    - **Shared Key Encryption**
        - フィル**Encryption key** と **Re-Enter Encryption key**

- クリック **Create Support Bundle**
- クリック **Download**



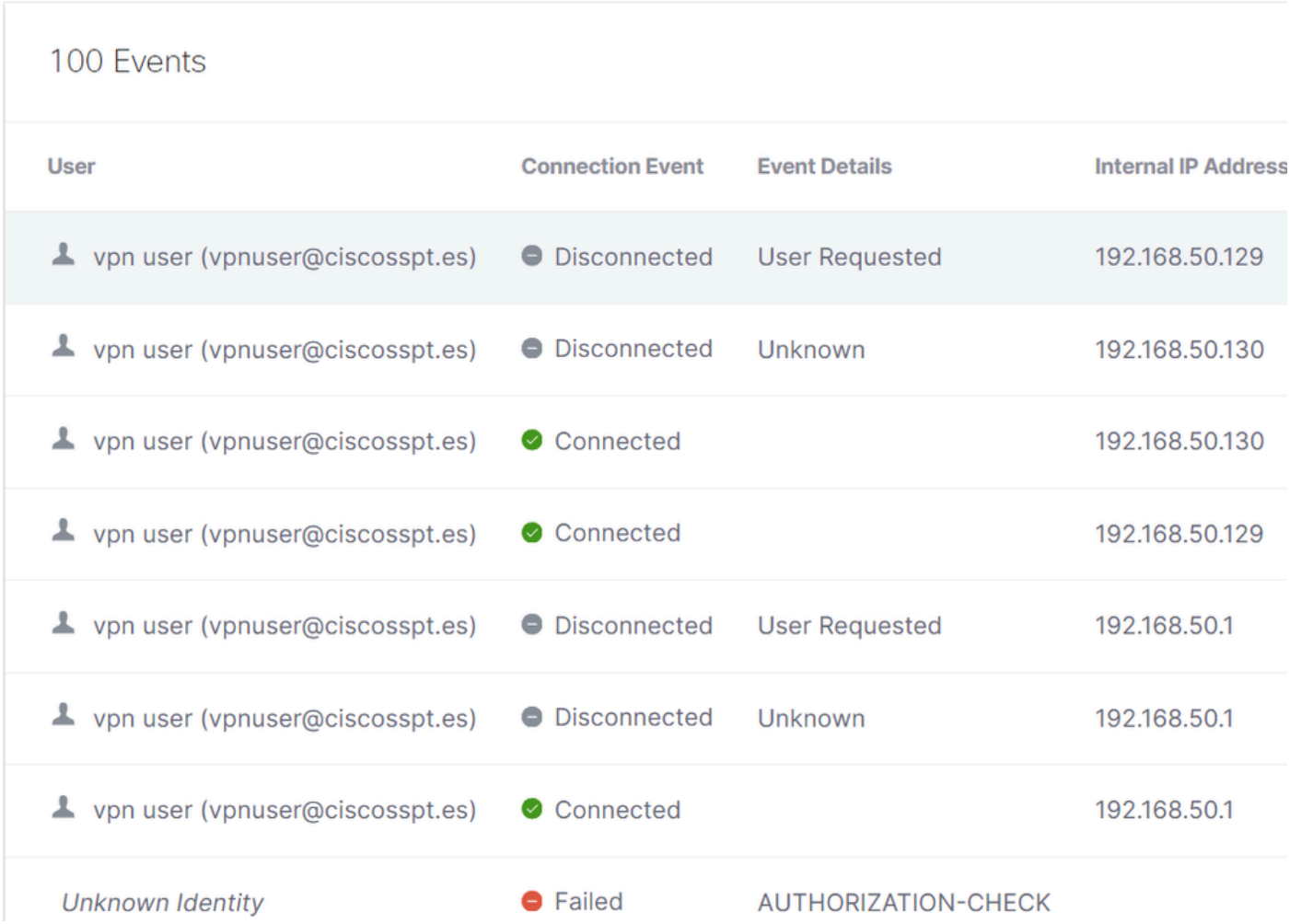


警告：ステップ「プロファイル設定のデバッグ」で有効にしたデバッグモードを無効にします

セキュアアクセスリモートアクセスログの確認方法

セキュアアクセスダッシュボードに移動します。

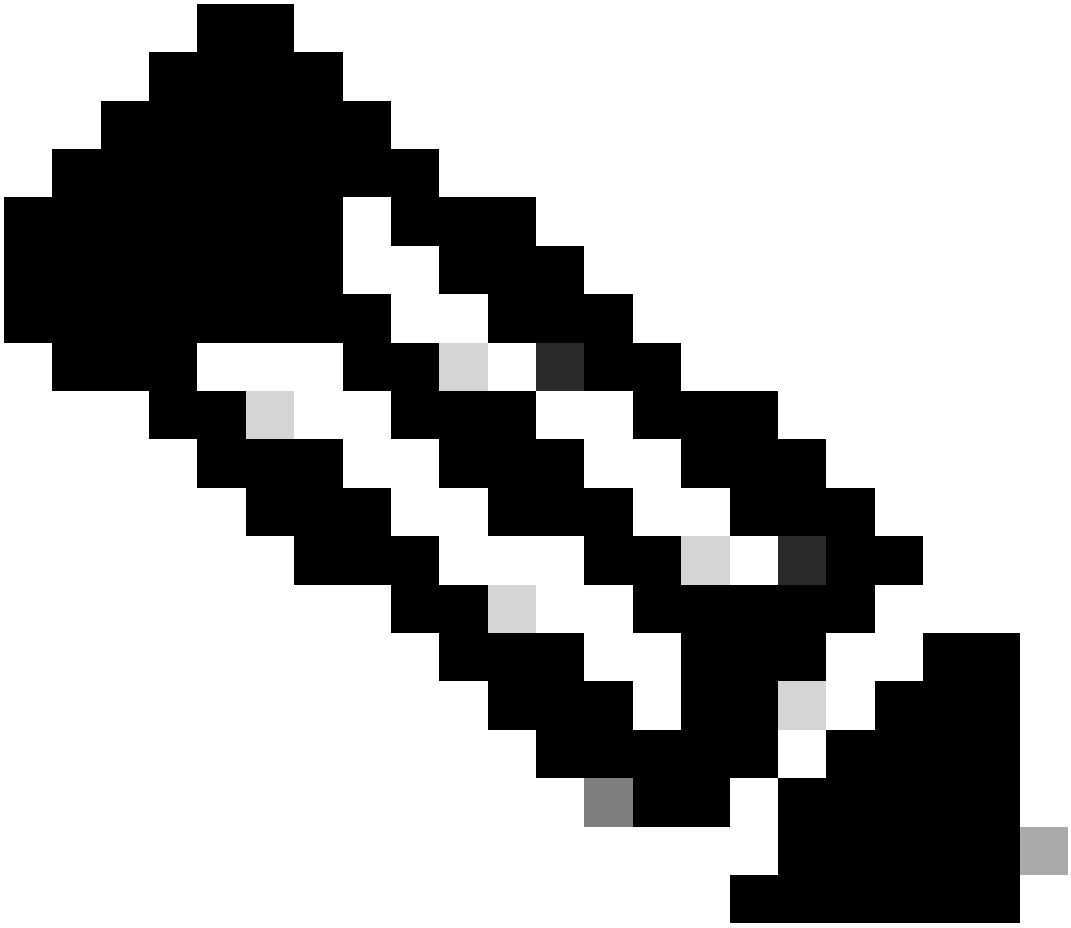
- クリック Monitor > Remote Access Logs



セキュアクライアントでのDARTバンドルの生成

マシンでDARTバンドルを生成するには、次の記事を確認してください。

Cisco Secure Client Diagnostic and Reporting Tool(DART)



注：トラブルシューティングセクションで示したログを収集したら、**TAC** でサービスリクエストをオープンし、情報の分析を進めてください。

関連情報

- シスコのテクニカルサポートとダウンロード
- セキュアアクセスに関するドキュメントおよびユーザガイド

- **Cisco Secure Clientソフトウェアのダウンロード**
- **Cisco Identity Services Engine 管理者ガイド リリース 3.3**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。