

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クセスメント

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[Duo設定](#)

[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](#)

[ISEを使用するためのVPNプロファイルの設定](#)

[全般設定](#)

[認証、許可、およびアカウントテイング](#)

[トラフィック操作](#)

[Cisco Secure Clientの設定](#)

[ISEの設定](#)

[ネットワークデバイスのリストの設定](#)

[グループの設定](#)

[ローカルユーザの設定](#)

[ポリシーセットの設定](#)

[ポリシーセット許可の設定](#)

[RADIUSローカルまたはActive Directoryユーザの設定](#)

[ISEポスチャの設定](#)

[ポスチャ条件の設定](#)

[ポスチャ要件の設定](#)

[ポスチャポリシーの設定](#)

[クライアントプロビジョニングの設定](#)

[クライアントプロビジョニングポリシーの設定](#)

[認可プロファイルの作成](#)

[ポスチャポリシーセットの設定](#)

[確認](#)

[ポスチャ検証](#)

[マシン上の接続](#)

[ISEでログを確認する方法](#)

[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](#)

[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](#)

[セキュアアクセスリモートアクセスログの確認方法](#)

[セキュアクライアントでのDARTバンドルの生成](#)

[関連情報](#)

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、およびアカウントティング

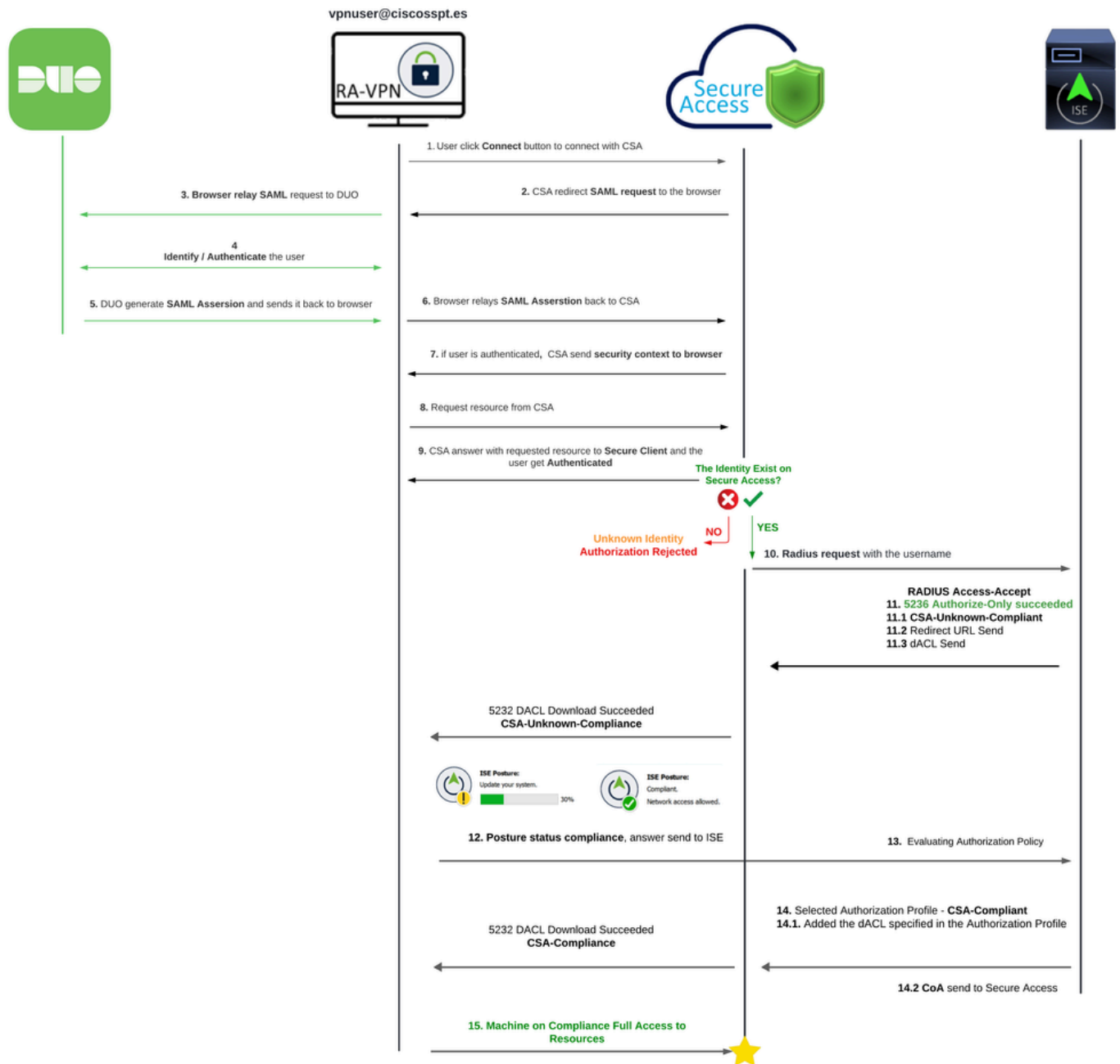
使用するコンポーネント

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



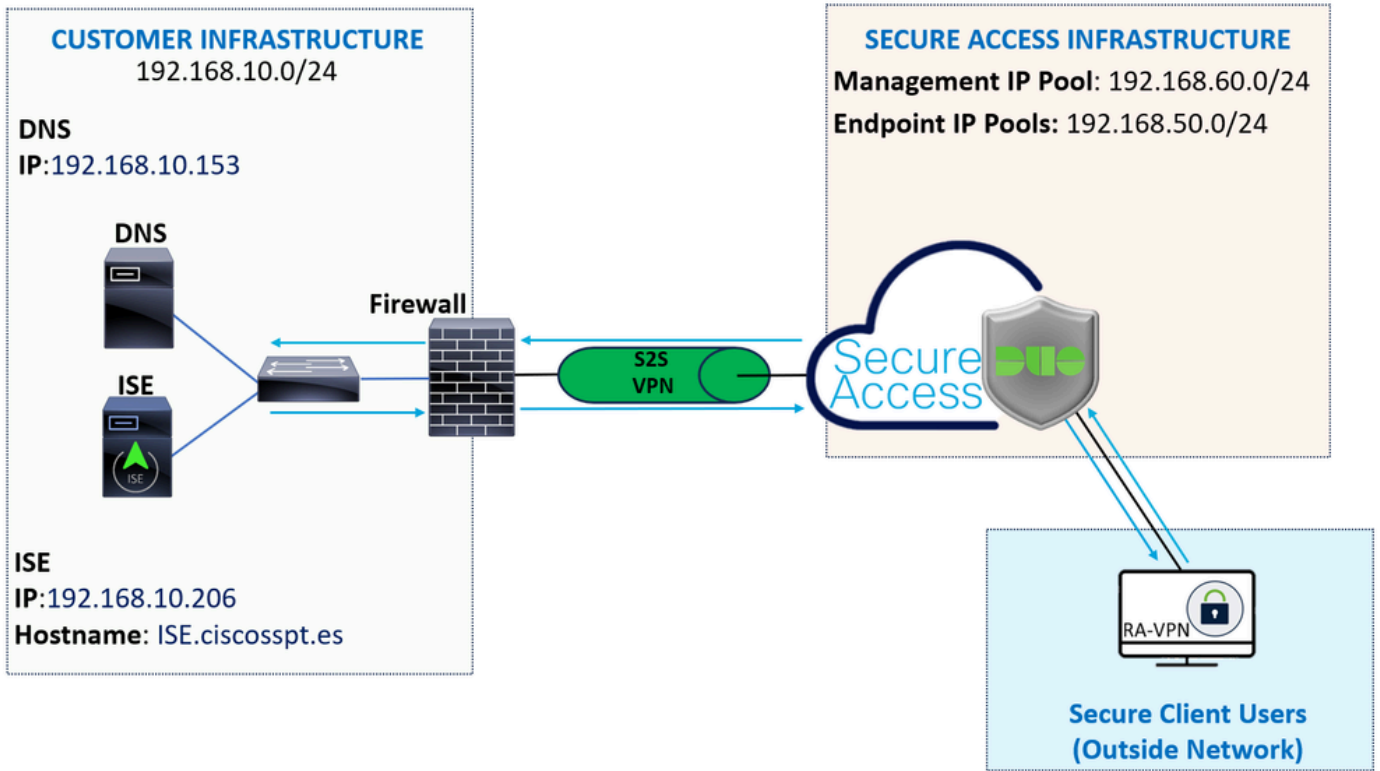
Duo SAMLとCisco Identity Services Engine(ISE)の統合により、認証プロセスが強化され、シスコセキュアアクセスソリューションに新たなセキュリティレイヤが追加されます。Duo SAMLは、高いセキュリティ標準を確保しながら、ユーザログインプロセスを簡素化するシングルサインオン(SSO)機能を提供します。

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



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

Protect an Application

Generic SAML Service Provider

Application

Protection Type



Generic SAML Service Provider

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

[Documentation](#)

Protect

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。

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

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

Generic SAML Service Provider - Single Sign-On

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

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

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata</code>	Copy

Certificate Fingerprints

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

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**

Manage IP Pools

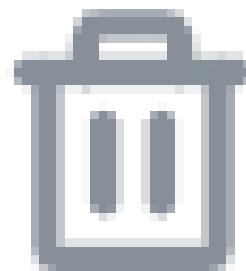
Manage

2 Regions mapped

- コマンドを選択し、**Radius Server**

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

- 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

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		

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

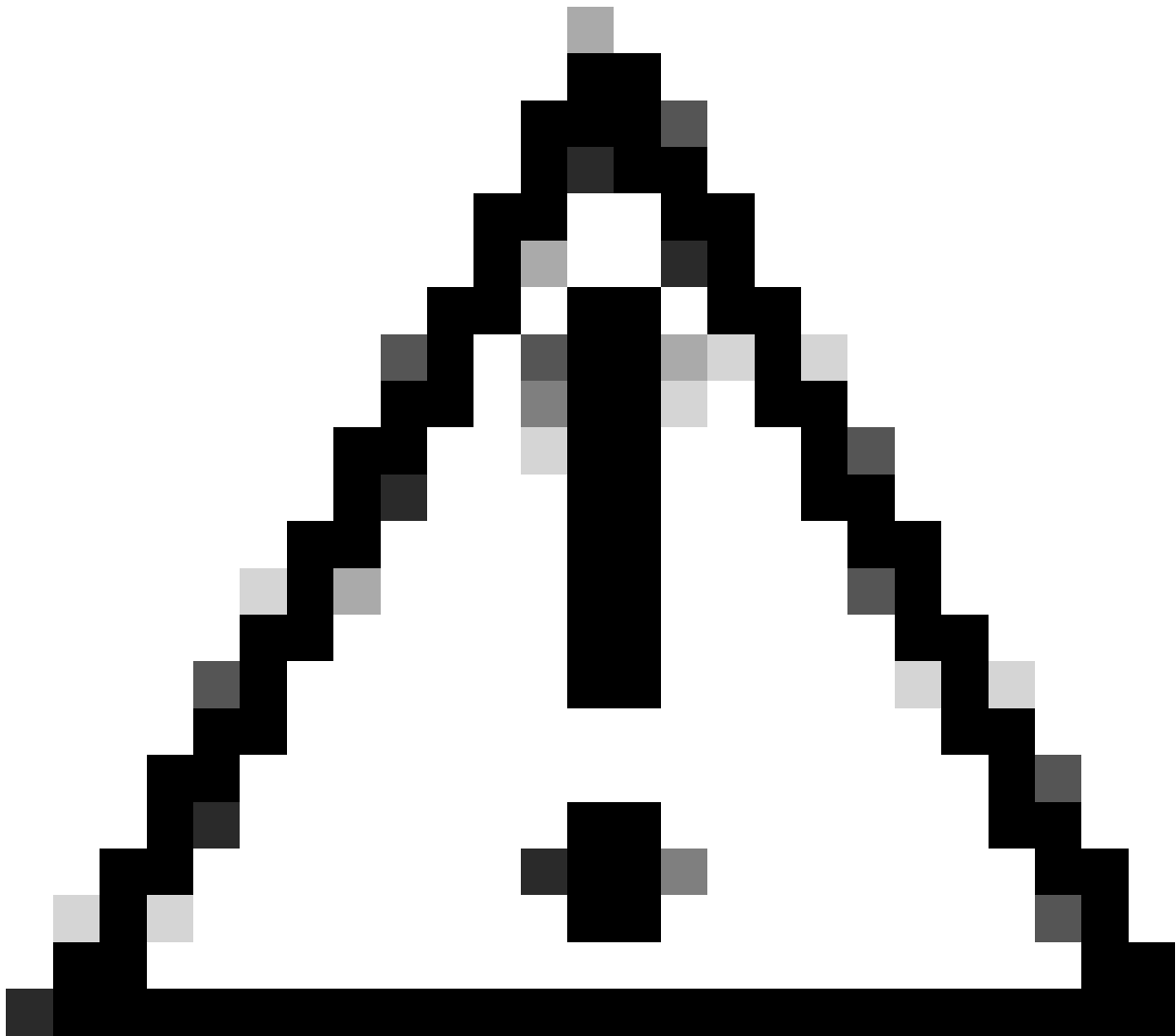
- **Authorization:Authorization**のチェックボックスをオンにし、ポートを選択します。デフォルトは1812です。

- 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、アカウントリングデータは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トリングデータ)
- 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

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

+ Add

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

- 次に、次のオプションを設定します。

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Show

Password

Show

Cancel

Save & Add server

Save

- **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。

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- 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。

The screenshot shows the Duo configuration interface for a Service Provider. On the left, there is an XML snippet for SAML metadata. On the right, there are configuration fields for the Service Provider. Arrows indicate the mapping between the XML fields and the configuration fields:

- Entity ID:** The XML field `entityID="https://...vpn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SAML"` is mapped to the `Entity ID *` field in the configuration form.
- Assertion Consumer Service (ACS) URL:** The XML field `Location="https://...vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=ISE_CSA_SAML"` is mapped to the `Assertion Consumer Service (ACS) URL *` field.
- Single Logout URL:** The XML field `Location="https://...vpn.sse.cisco.com/+CSCOE+/saml/sp/logout"` is mapped to the `Single Logout URL` field.

- 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

Settings

Type Generic SAML Service Provider - Single Sign-On

Name

ISE - SAML

Duo Push users will see this when approving transactions.

- Duoでアプリケ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**

ISE - SAML

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

Metadata

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

Certificate Fingerprints

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

Downloads

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

- 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。

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

Authentication, Authorization, and Accounting

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

Authentication **Authorization** Accounting

Enable Radius Authorization

Use defaults or customize groups to map to regions

Select one group for all regions

[+ Group](#)

ISE_CSA

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



Cancel

Back

Next

- **Authorization**

- **Enable Radius Authorization** : 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。

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

Authentication, Authorization, and Accounting

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

Authentication Authorization Accounting

Enable Radius Accounting
Use defaults or customize groups to map to regions

Select one group for all regions + Group

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	<input type="text" value="ISE_CSA"/>
RA VPN 1	192.168.60.0/24	<input type="text" value="ISE_CSA (default)"/>



Cancel

Back

Next

- **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。

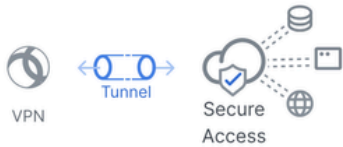
トラフィック誘導

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。

Tunnel Mode

Connect to Secure Access

All traffic is steered through the tunnel.



Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.



- **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**

Connect to Secure Access

All traffic is steered through the tunnel.



Add Exceptions

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

+ Add

Destinations

Exclude Destinations

Actions

proxy-
8195126.zpc.sse.cisco.com,
ztna.sse.cisco.com,acme.sse.
cisco.com,devices.api.umbrell
a.com,sseposture-routing-
commercial.k8s.5c10.org,sse
posture-routing-
commercial.posture.duosecuri
ty.com,data.eb.thousandeves.

-

-

Cancel

Back

Next

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

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

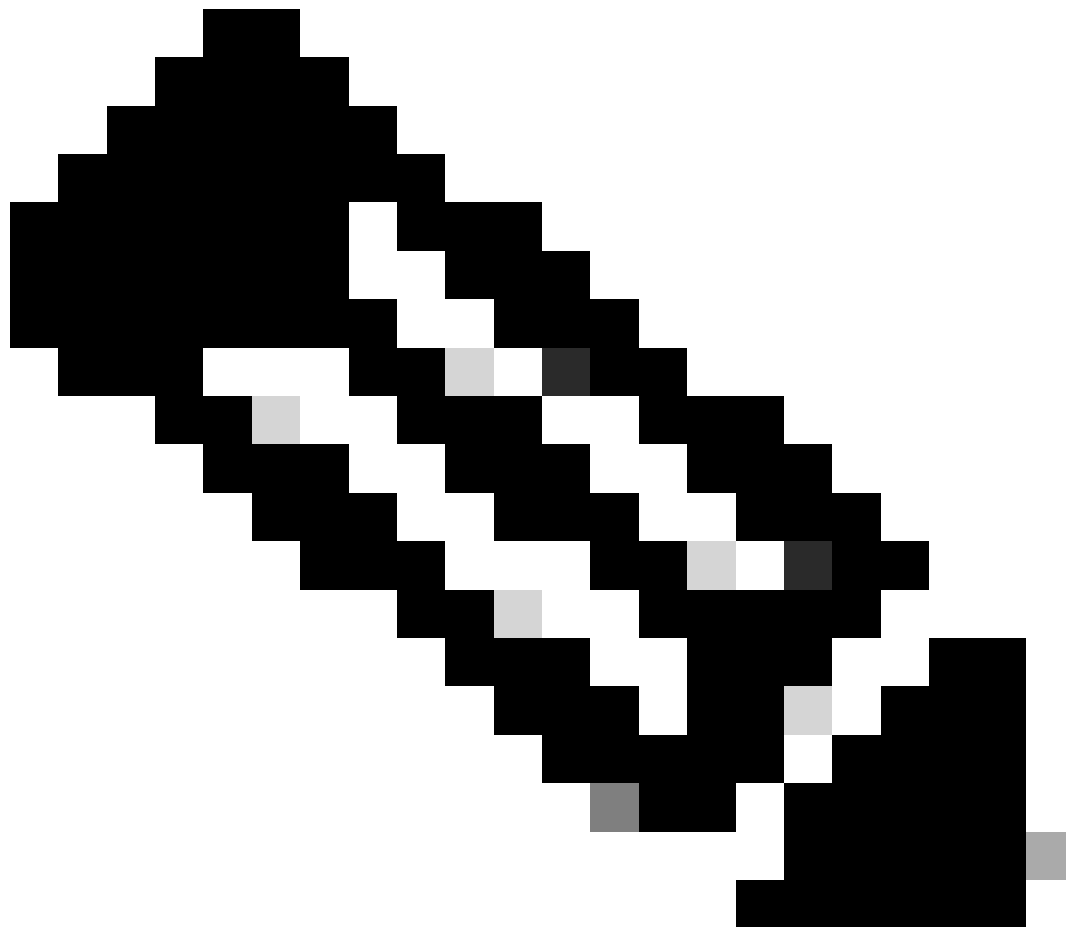


No matches found

[Cancel](#)

[Back](#)

[Next](#)



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	ciscospt.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

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**

The screenshot displays the Cisco ISE Administration console. The left sidebar shows the 'Administration' menu with 'Identities' > 'Groups' selected. The main content area is titled 'User Identity Groups' and shows a 'New User Identity Group' form. The form fields are: '* Name' (5) with 'CSA-ISE' entered, and 'Description' (empty). Below the form is a 'Submit' button (6). On the right, a list of existing groups is shown: 'ALL_ACCOUNTS (default)', 'CSA-ISE' (with a blue arrow and 'GROUP CREATED' text), and 'Employee'. The 'Add +' button (4) is highlighted in the top left of the form area.

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 +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

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

▼ User Groups

⋮ ▼

- **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。

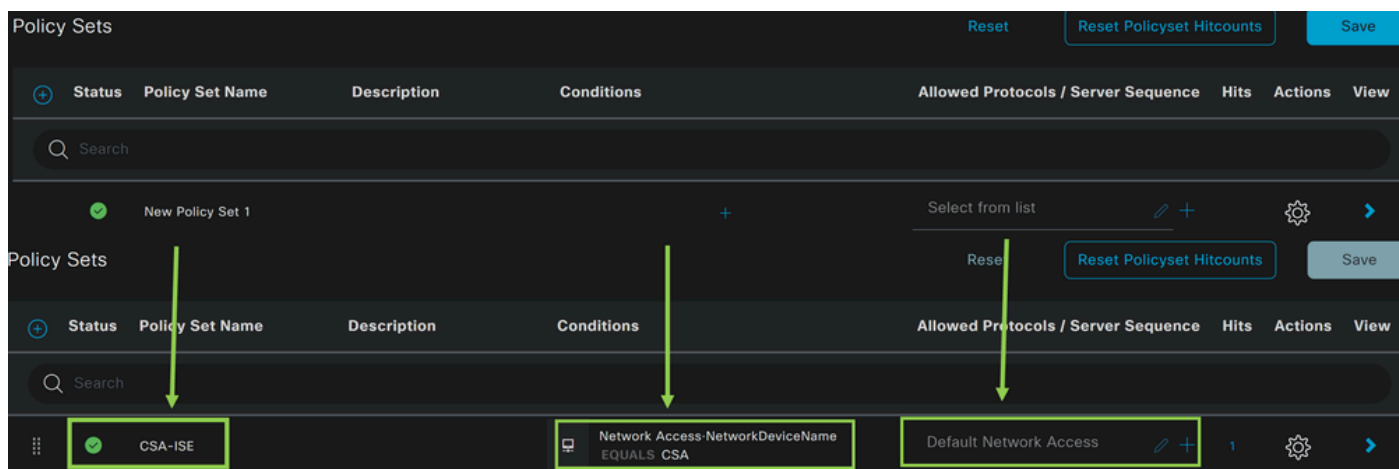
その後、設定Saveを行い、**Configure Policy Set**の手順に進みます。

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。

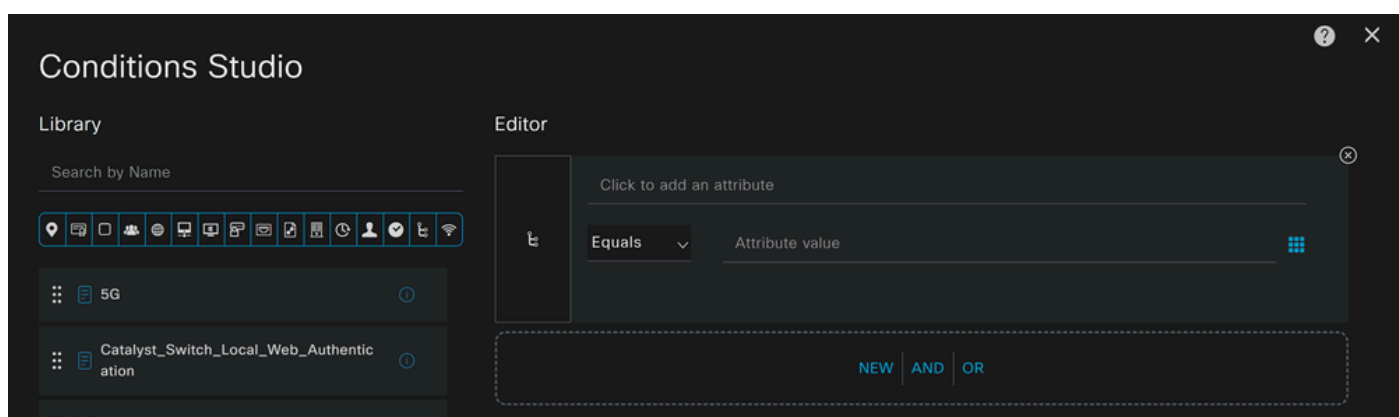
- クリック Policy > Policy Sets
- 新しいポリシーセットを追加するには、+ をクリックします。



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。

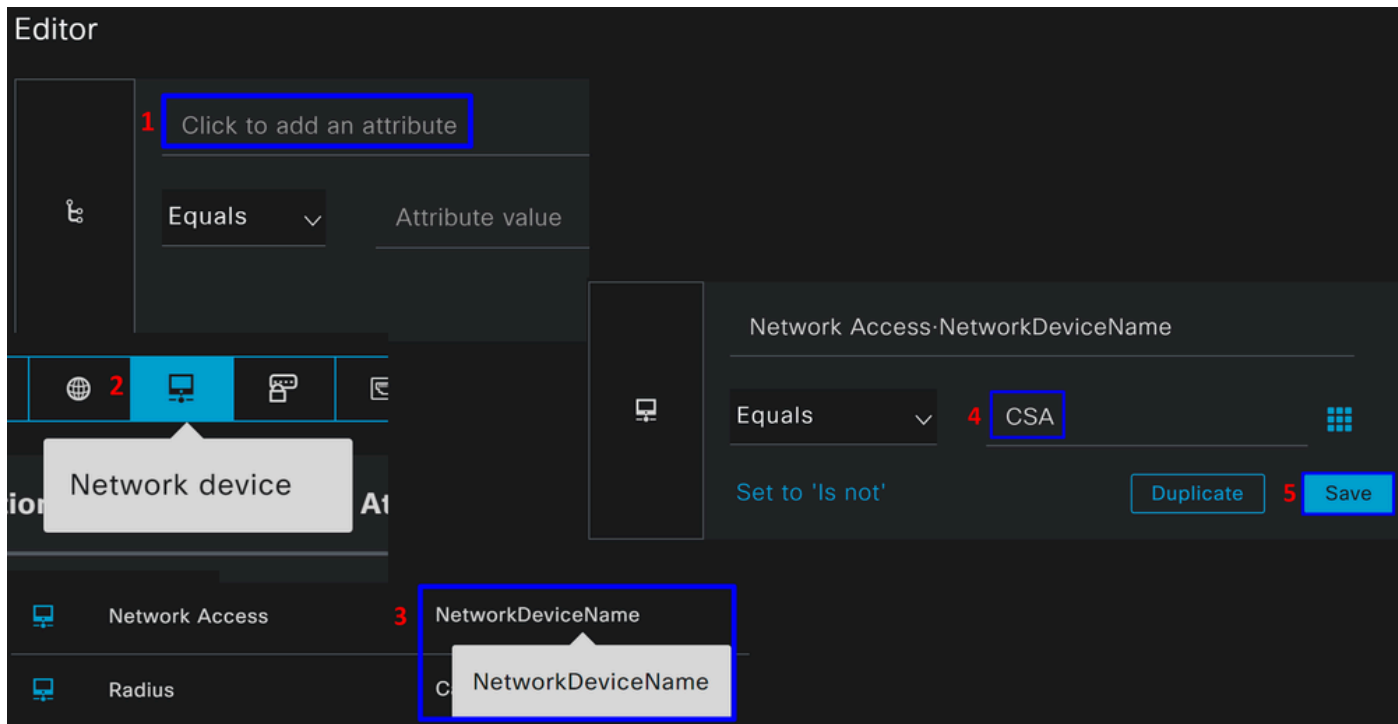
ポリシーセットに一致するconditionを作成するには、次の手順に進みます。

- クリック +
- Condition Studio**
- で使用可能な情報は次のとおりです。



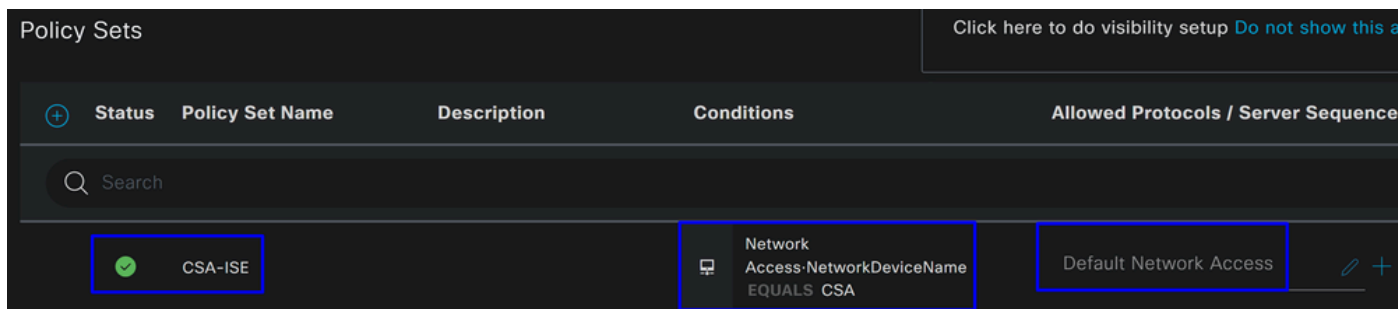
- 条件を作成するには、Click to add an attribute
- ボタNetwork Device をクリックします。
- 背後にあるオプションの下で、「Network Access - Network Device Name option」をクリックします。

- 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CSAAuthentication 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。

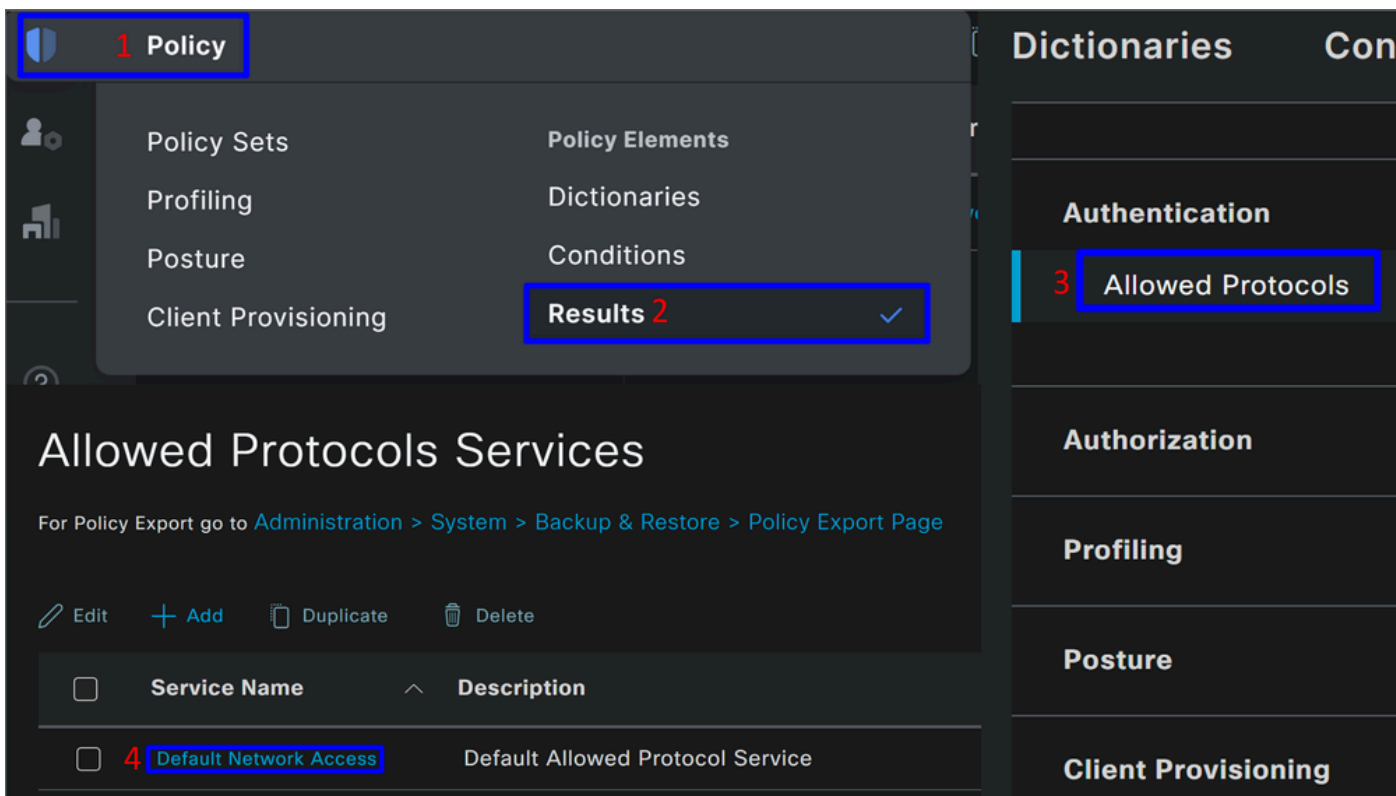
定義されたポリシーの結果は次のようになります。



- **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**

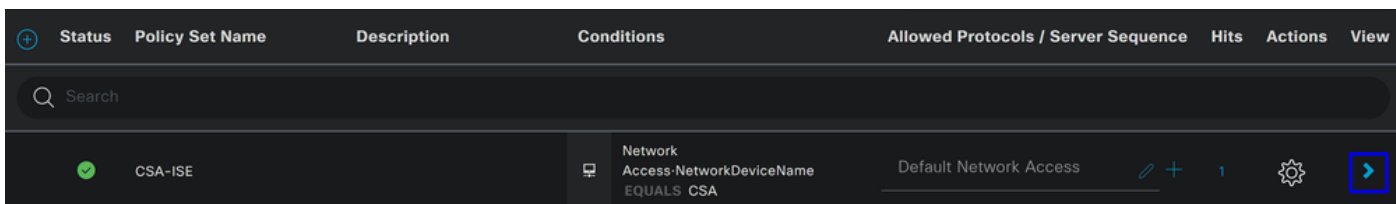


- 次に、許可されているすべてのプロトコルが表示されます **Default Network Access**

ポリシーセット許可の設定

Policy Setの下に**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。

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

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

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。

Authorization Policy(2)

			Results														
+	Status	Rule Name	Conditions	Profiles	Security Groups												
+	✓	Authorization Rule 1		Select from list	Select from list												
<table border="1"> <thead> <tr> <th>+</th> <th>Status</th> <th>Rule Name</th> <th>Conditions</th> <th>Profiles</th> <th>Security Groups</th> </tr> </thead> <tbody> <tr> <td>+</td> <td>✓</td> <td>Authorization Secure Access</td> <td>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</td> <td>PermitAccess</td> <td>Select from list</td> </tr> </tbody> </table>						+	Status	Rule Name	Conditions	Profiles	Security Groups	+	✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list
+	Status	Rule Name	Conditions	Profiles	Security Groups												
+	✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list												

- 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。

Authorization Policy(2)

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

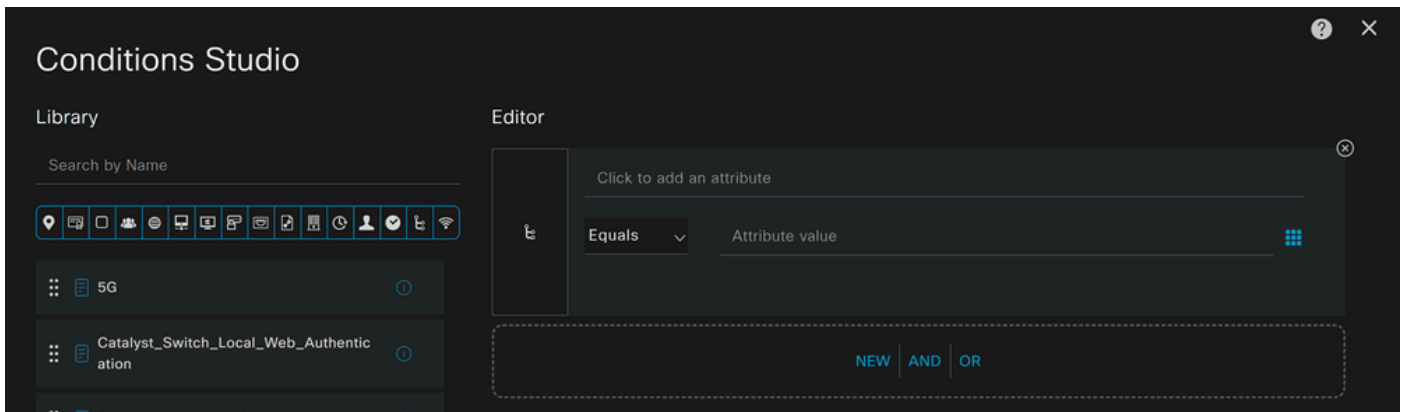
- 次の手順では、Rule NameConditions および Profiles
- 認可ポリシーを簡単に識別できるように名前を設定する場合

Condition

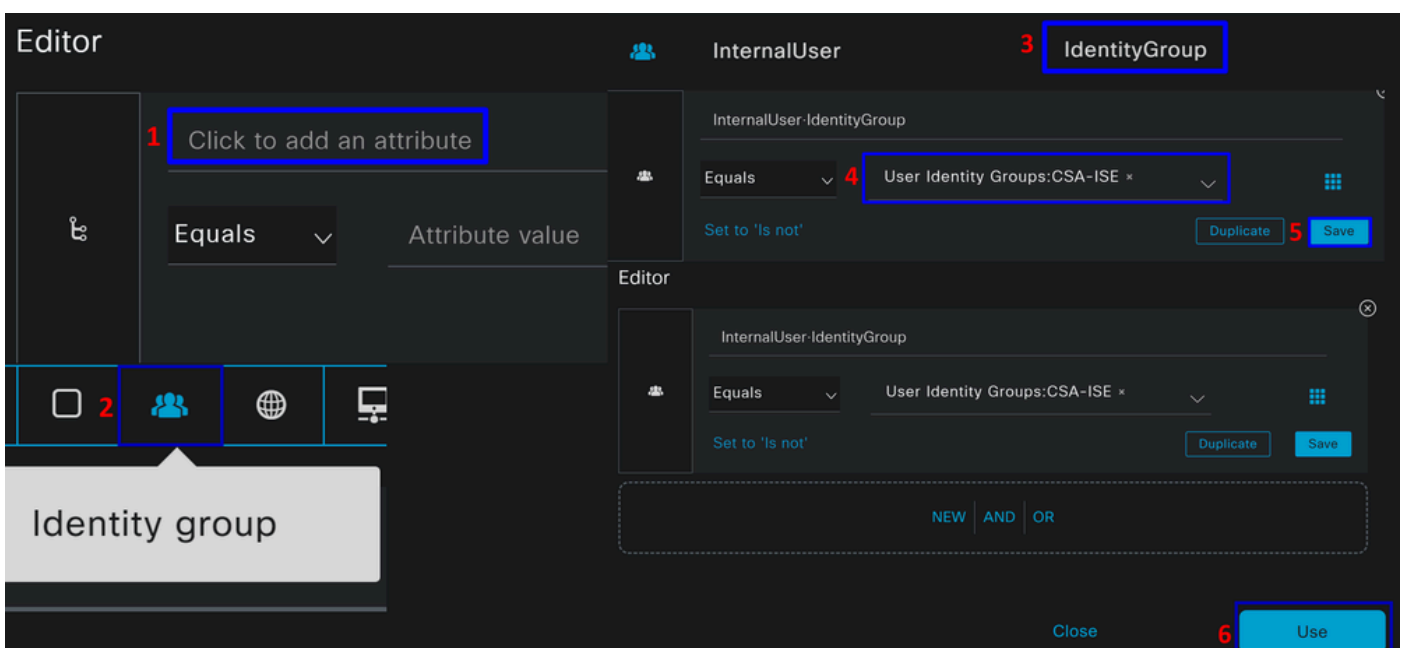
- を設定するには、 +

Condition Studio

- の下に、次の情報があります。

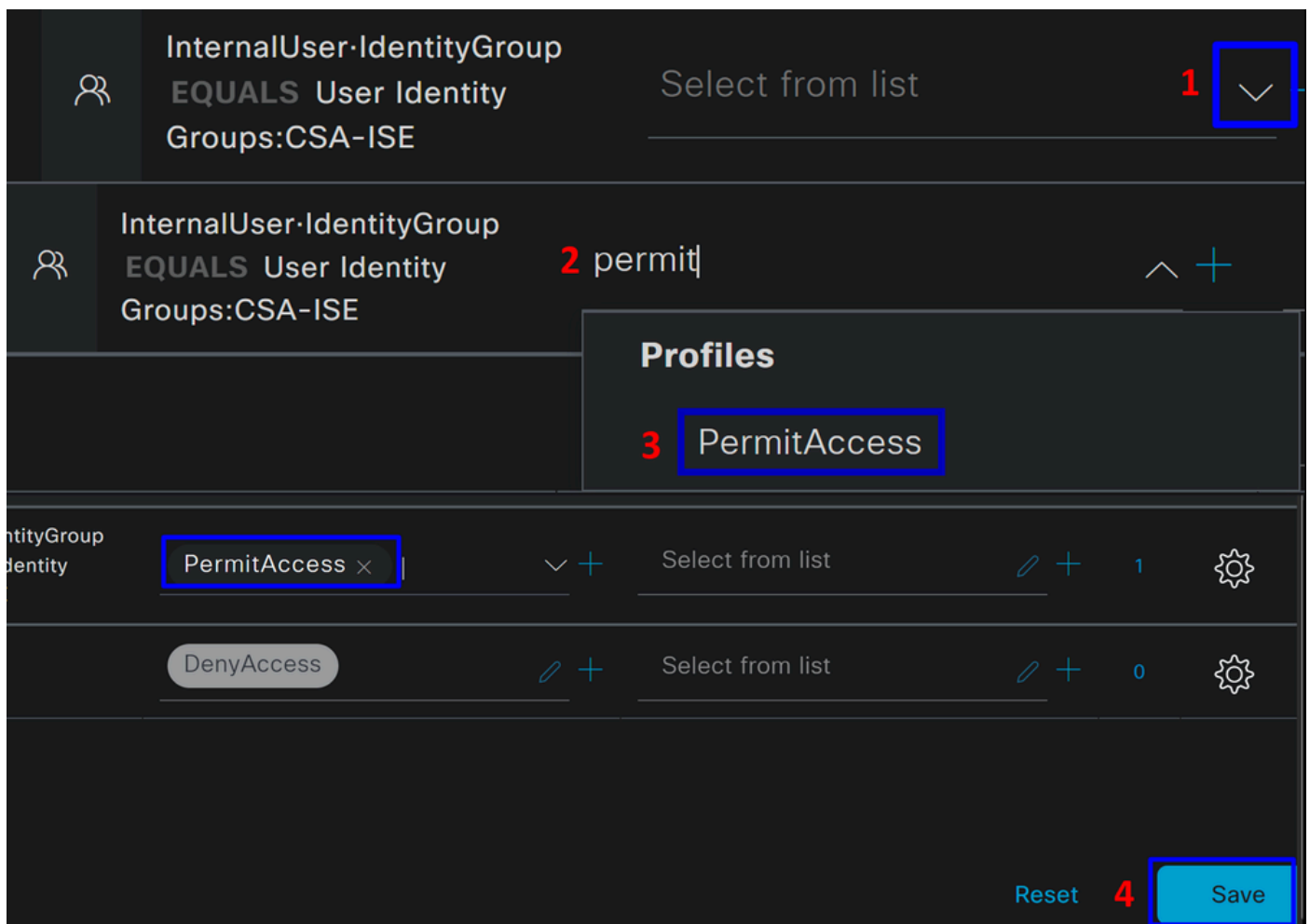


- 条件を作成するには、 Click to add an attribute
- ボタIdentity Group をクリックします。
- 背後にあるオプションでInternal User - IdentityGroup optionをクリックします
- オプEquals ションの下のドロップダウンを使用して、手順「[Configure a Group](#)」で認証の承Group 認済みを見つけます
- クリック Save
- クリック Use



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のロ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**





28 Events

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

- 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**

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

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**

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

RADIUSローカルまたはActive Directoryユーザの設定

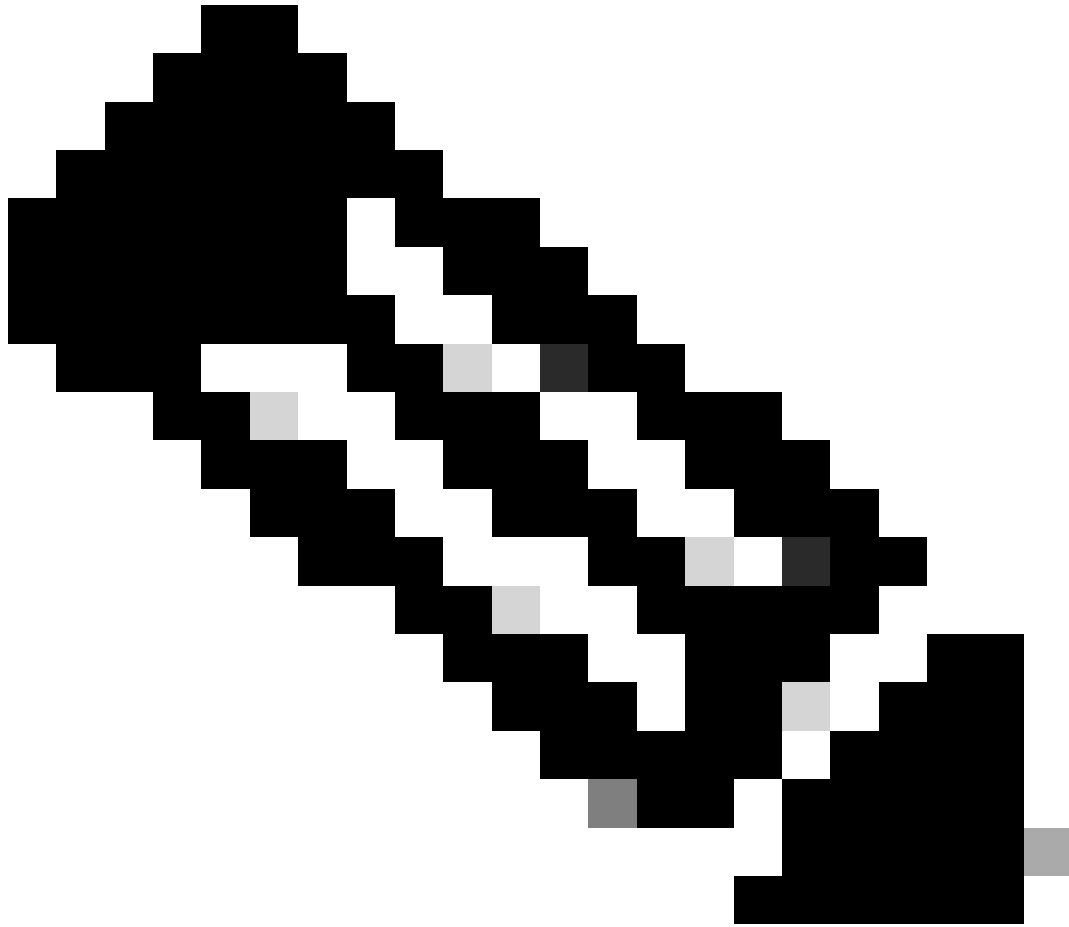
ISEポスチャの設定

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

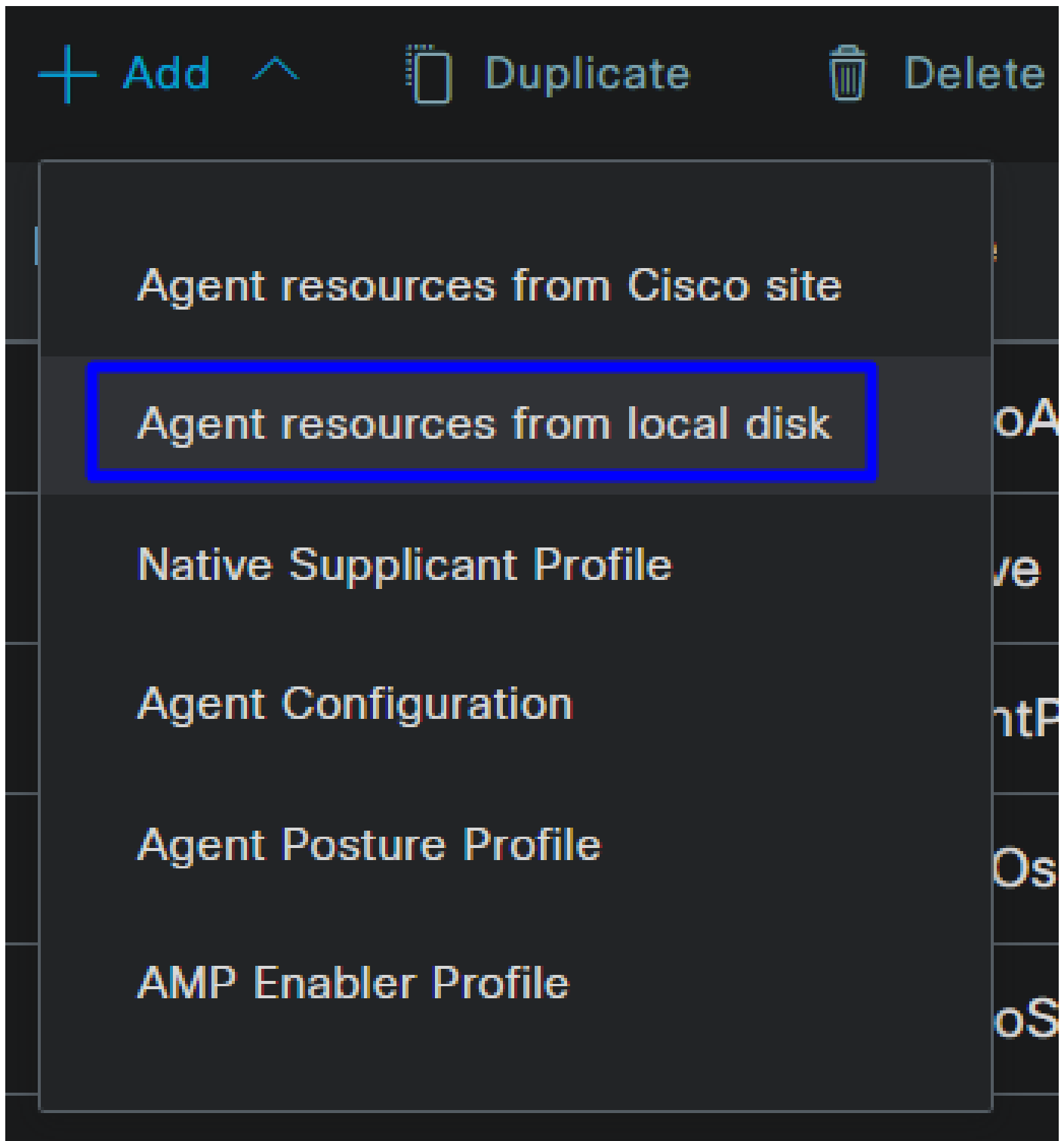
1. Agent Resources	Secure Client Web Provisioningパッケージ。
2. Compliance Module	Cisco ISEコンプライアンスモジュール
を選択します。 Agent Profile	プロビジョニングプロファイルの制御。
を選択します。 Agent Configuration	エージェントプロファイルとエージェントリソースを使用してプロビジョニングポータルを設定し、プロビジョニングするモジュールを定義します。

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。

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

- 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

+ Add ^ Duplicate Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- 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

Download Remote Resources

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

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

Cancel

Save

Step 3 エージェントプロファイルの設定

- クリック + Add > Agent Posture Profile

Name

+ Add ^

☰ Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- 用の Posture Profile

Agent Posture Profile

Name *



Description:

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

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

Step 4 エージェントの設定

- クリック + Add > Agent Configuration

+ Add ^

📄 Duplicate

🗑 Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- その後、次のパラメータを設定します。

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

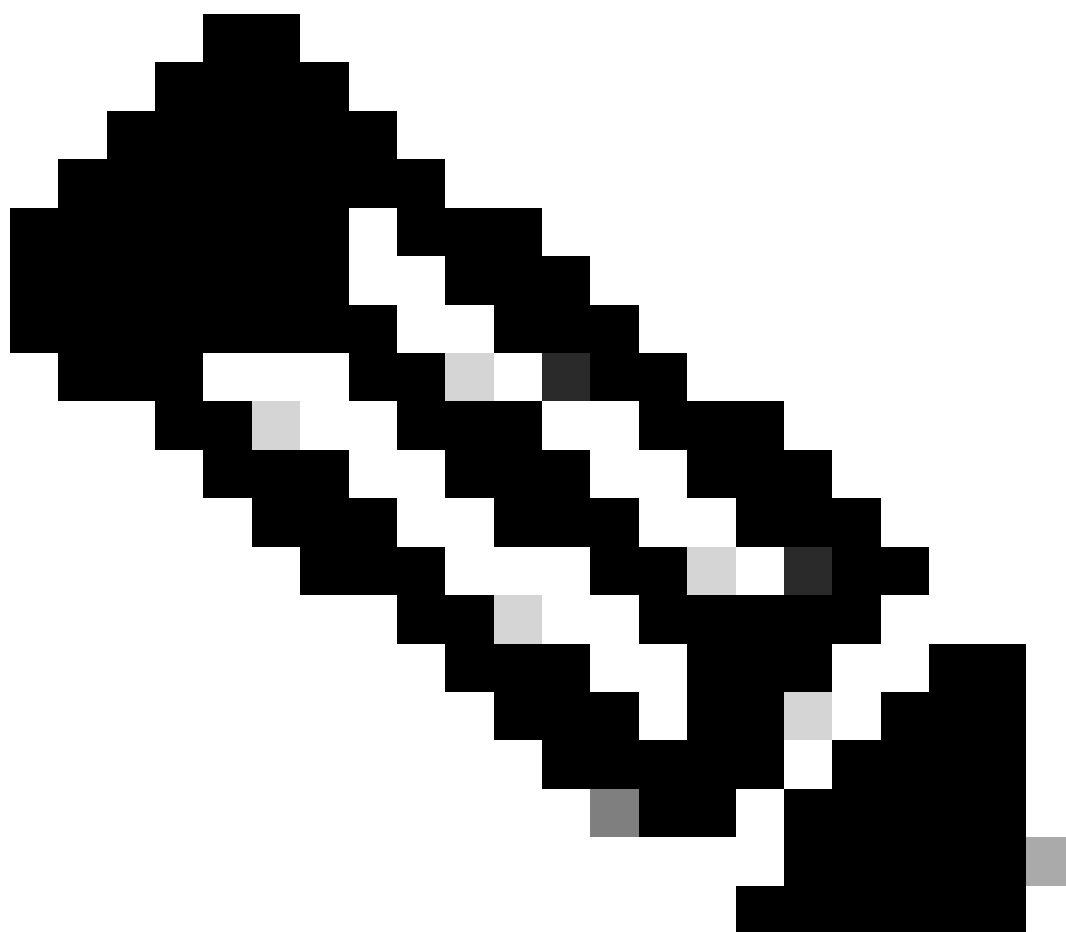
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- Select Agent Package :[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

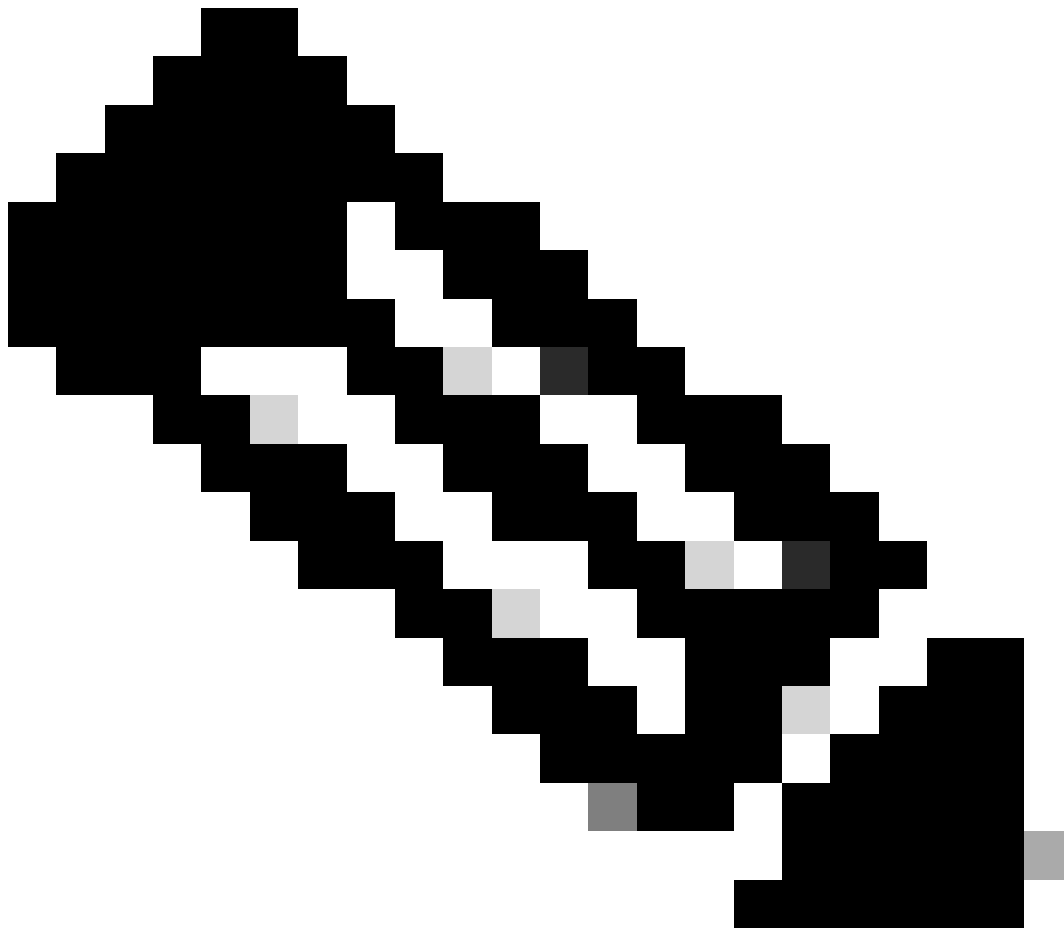


注：各オペレーティングシステム、Windows、Mac OS、またはLinuxで、1つのクライアント設定を個別に使用することをお勧めします。

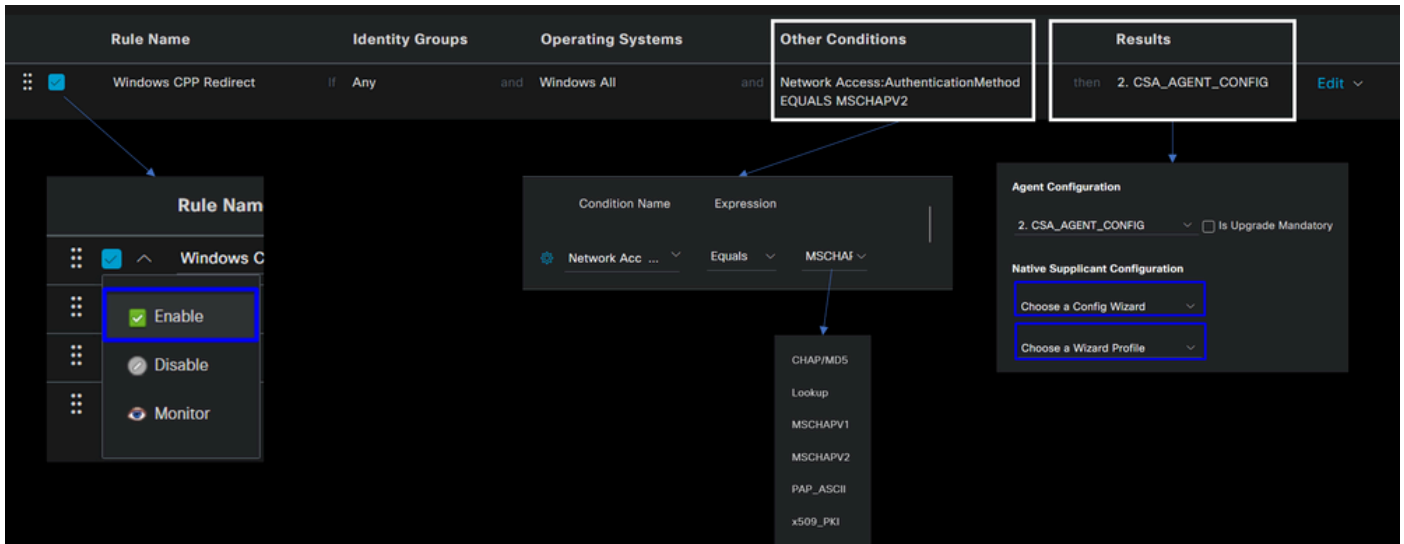
クライアントプロビジョニングポリシーの設定

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トチャに応じて、リソースへのアクセスを制限します。ユーザがポスト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 – ポストチャ検証済み

不明な準拠	ユーザUnknown 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: CSA-Compliant

Description: [Empty text box]

IP version: IPv4 IPv6 Agnostic ⓘ

* DACL Content	1234567	permit ip any any
	8910111	
	2131415	
	1617181	
	9202122	
	2324252	
	6272829	
	3031323	
	3343536	
	3738394	

- **Name:** 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 **CSA_Redirect_To_ISE**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

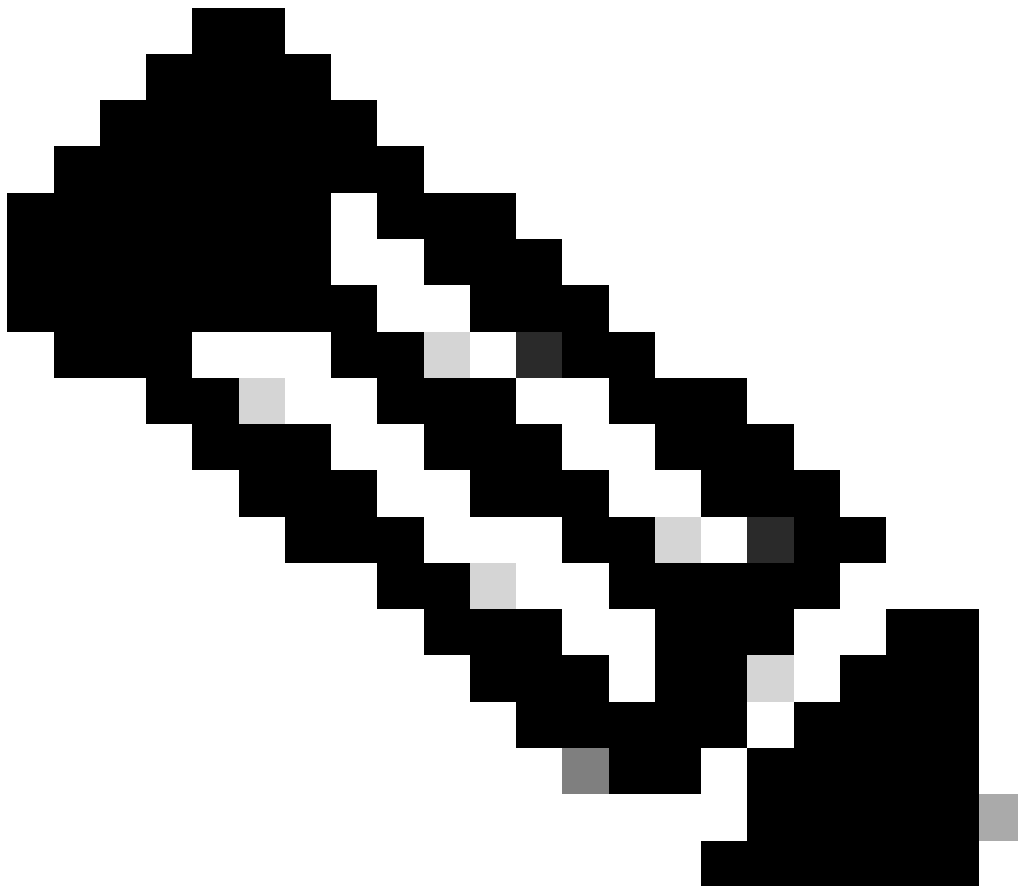
1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

✓ Check DACL Syntax

- Name: 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DAACL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

Authorization Profile

* Name

CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile



Cisco



Service Template

Track Movement



Agentless Posture



Passive Identity Tracking



Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL IPv6 (Filter ID)

- **Name** : 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 : Unknown Compliant Authorization Profile

* Name	CSA-Unknown-Compliant	
Description	<div style="border: 1px solid #ccc; height: 80px;"></div>	
* Access Type	ACCESS_ACCEPT ▼	
Network Device Profile	 Cisco ▼ 	
Service Template	<input type="checkbox"/>	
Track Movement	<input type="checkbox"/> 	
Agentless Posture	<input type="checkbox"/> 	
Passive Identity Tracking	<input type="checkbox"/> 	

▼ Common Tasks

<input checked="" type="checkbox"/> DACL Name	CSA_Redirect_To_ISE ▼
---	------------------------------------

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

Client Provisioning (Posture) ▾ ACL redirect

Value Client Provisioning Portal (... ▾

- **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**

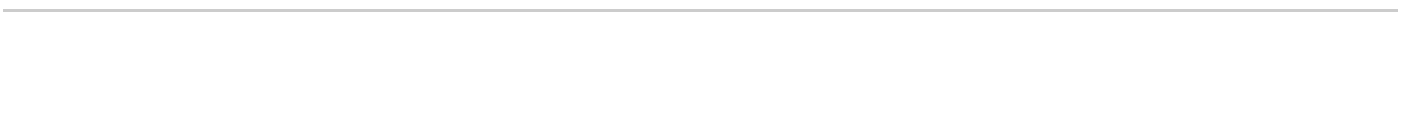
- **DACL NAME** : ステップ [Unknown Compliant DACL](#) で設定したDACLを選択します。

- **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。

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

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

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

- をクリックします。 Authorization Policy

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

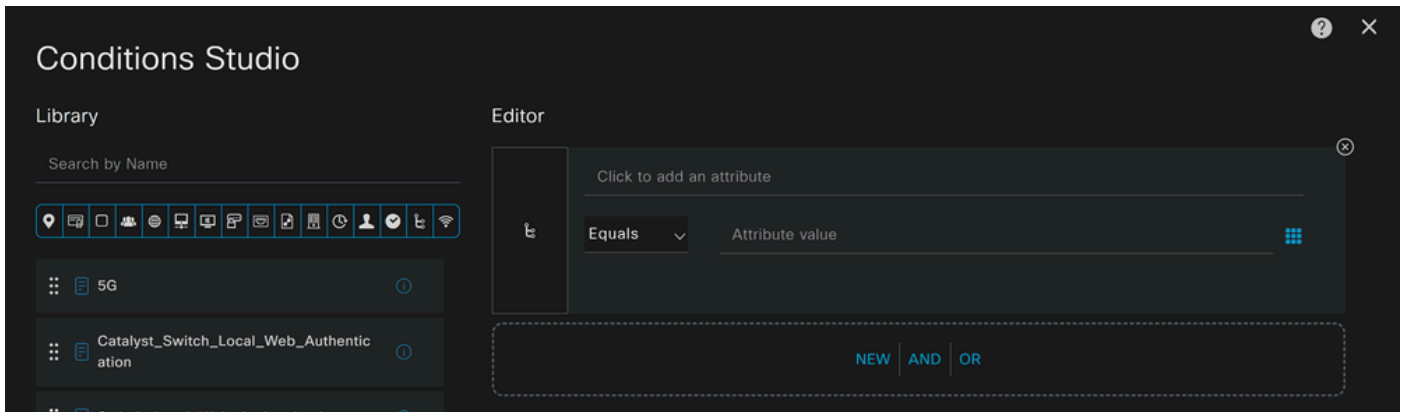
- 次の3つのポリシーを次の順序で作成します。

✓	SAML-Compliant	AND	<ul style="list-style-type: none"> Compliant_Devices InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Compliant
✓	SAML-Unknown-Compliant	AND	<ul style="list-style-type: none"> Compliance_Unknown_Devices InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Unknown-Compliant
✓	SAML-Non-Compliant	AND	<ul style="list-style-type: none"> Non_Compliant_Devices InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	DenyAccess

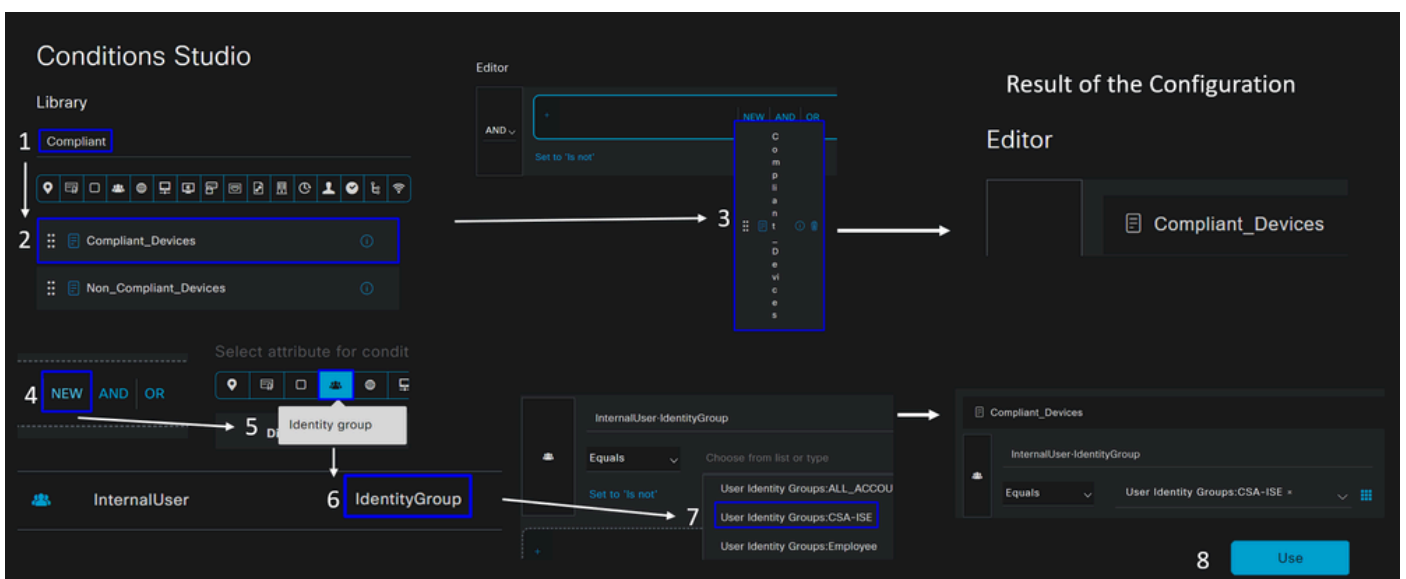
- ををクリックし+てポCSA-Compliance リシーを定義します。

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

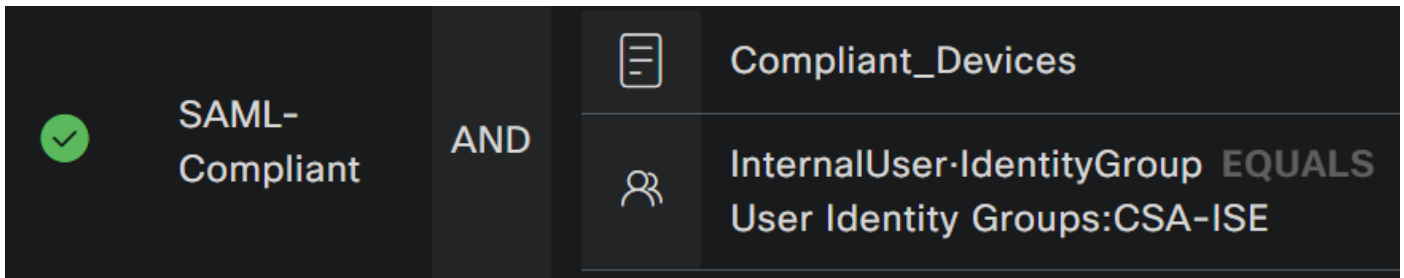
- 次の手順では、Rule NameConditions および Profiles
- 名前をに設Name 定する場合 CSA-Compliance Condition
 - を設定するには、+ Condition Studio
 - の下に、次の情報があります。



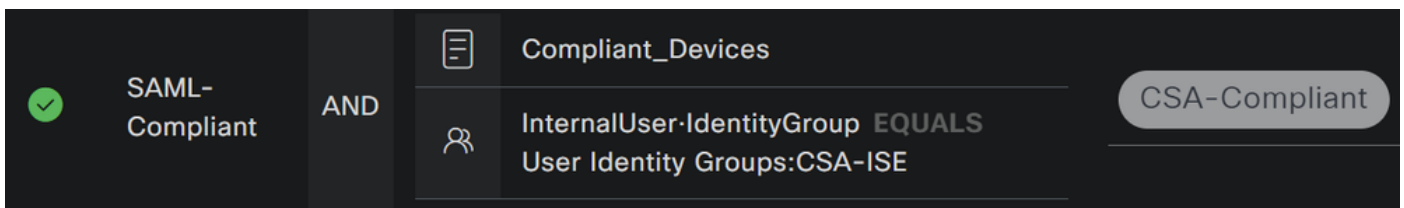
- 条件を作成するには、 **compliant**
- 表示されているはずですが、 **Compliant_Devices**
- 下にドラッグアンドドロップします。 **Editor**
- の下をクリックします。 **New**
- アイ **Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す **User Identity Group** 名を選択します
- クリック **Use**



- その結果、次のイメージが表示されます

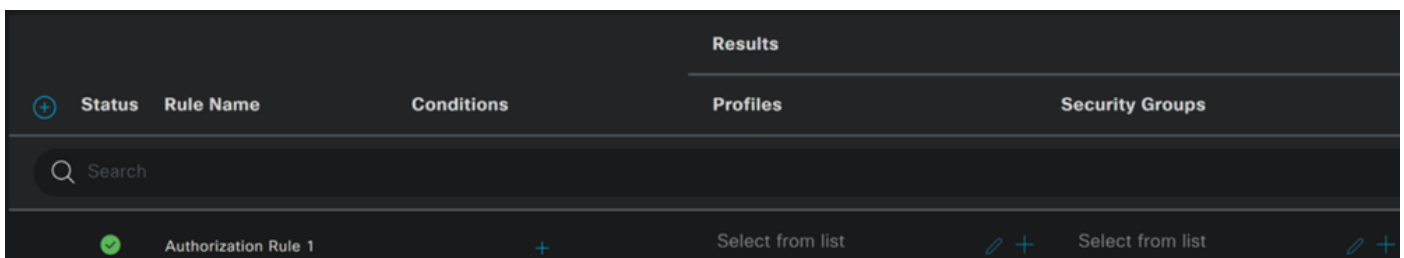


- の下でドロップダウンボタンの下をクリProfile ックし、手順で設定した苦情認証プロファイル、[Compliant Authorization Profile](#)を選択します。



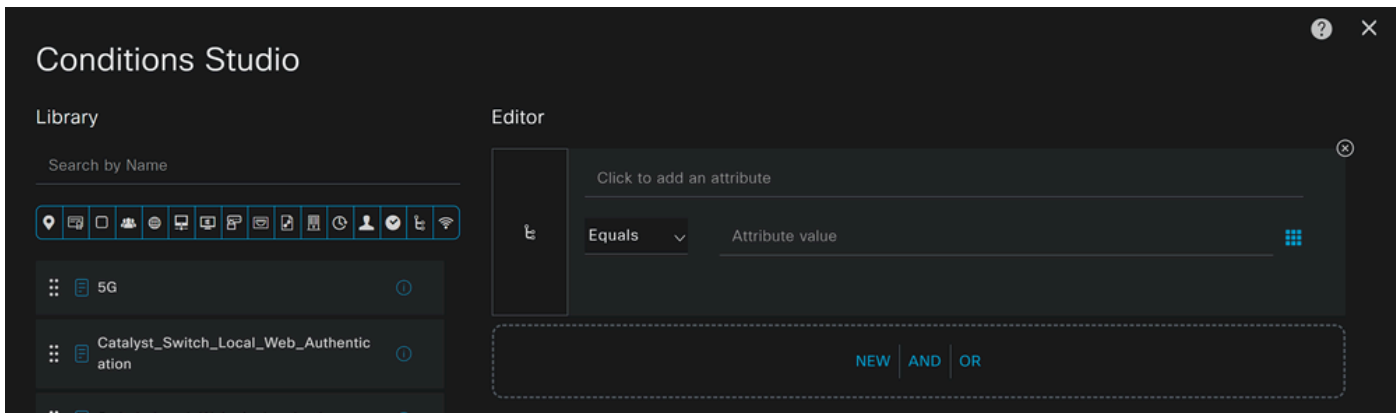
これで、 **Compliance Policy Set**が設定されました。

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

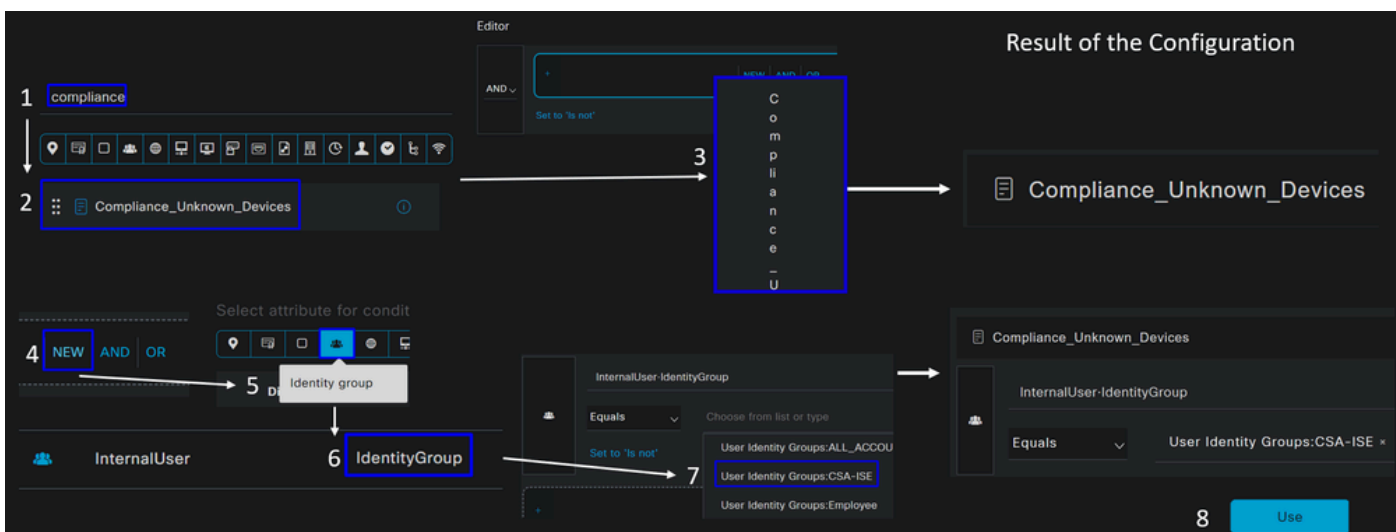


- 次の手順では、Rule NameConditions および Profiles

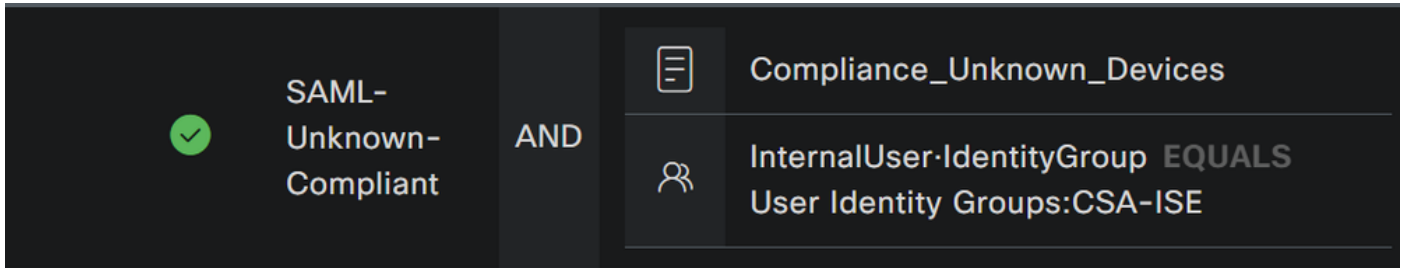
- 名前をに設Name 定する場合 **CSA-Unknown-Compliance Condition**
- を設定するには、 +
- **Condition Studio**
- の下に、次の情報があります。



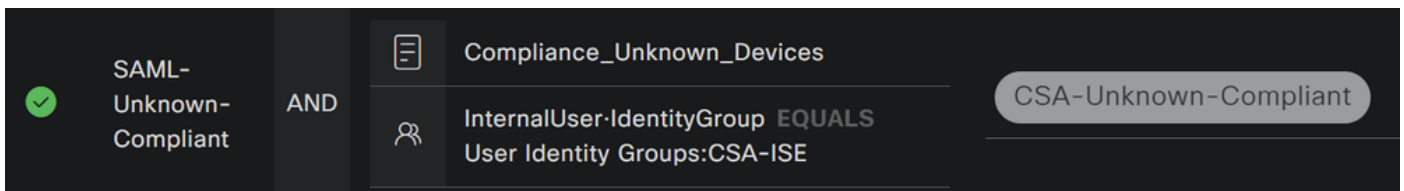
- 条件を作成するには、 **compliance**
- 表示されているはずですが、 **Compliant_Unknown_Devices**
- 下にドラッグアンドドロップします。 **Editor**
- の下をクリックします。 **New**
- アイ **Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す **User Identity Group** る名前を選択します
- クリック **Use**



- その結果、次のイメージが表示されます

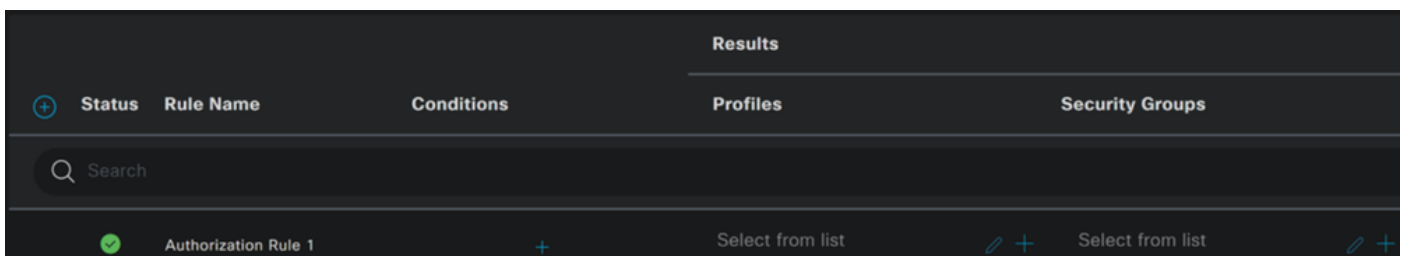


- の下でドロップダウンボタンの下をクリックしProfile を選択し、手順で設定した苦情認証プロファイル、[不明な準拠認証プロファイル](#)を選択します。



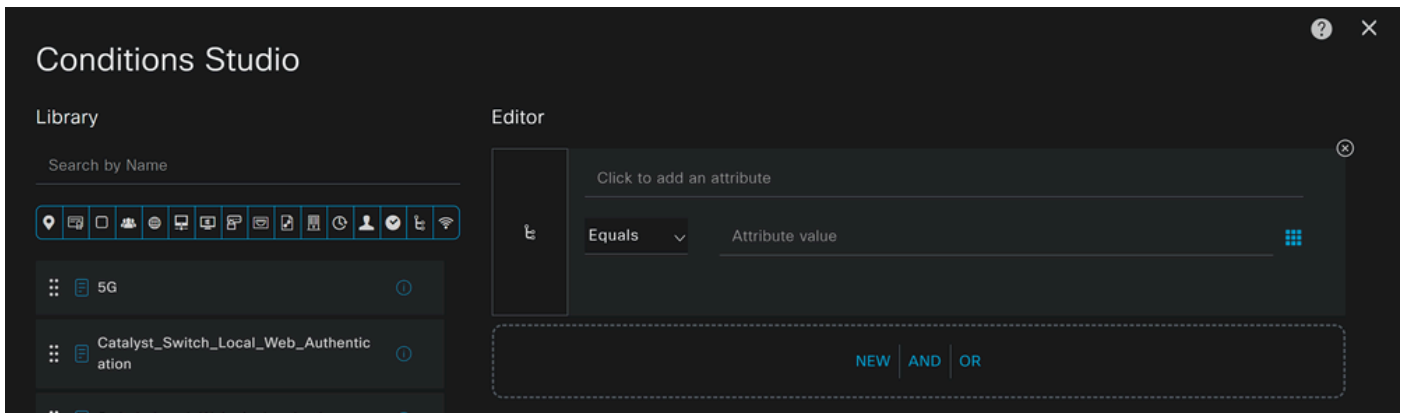
これで、 **Unknown Compliance Policy Set**が設定されました。

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

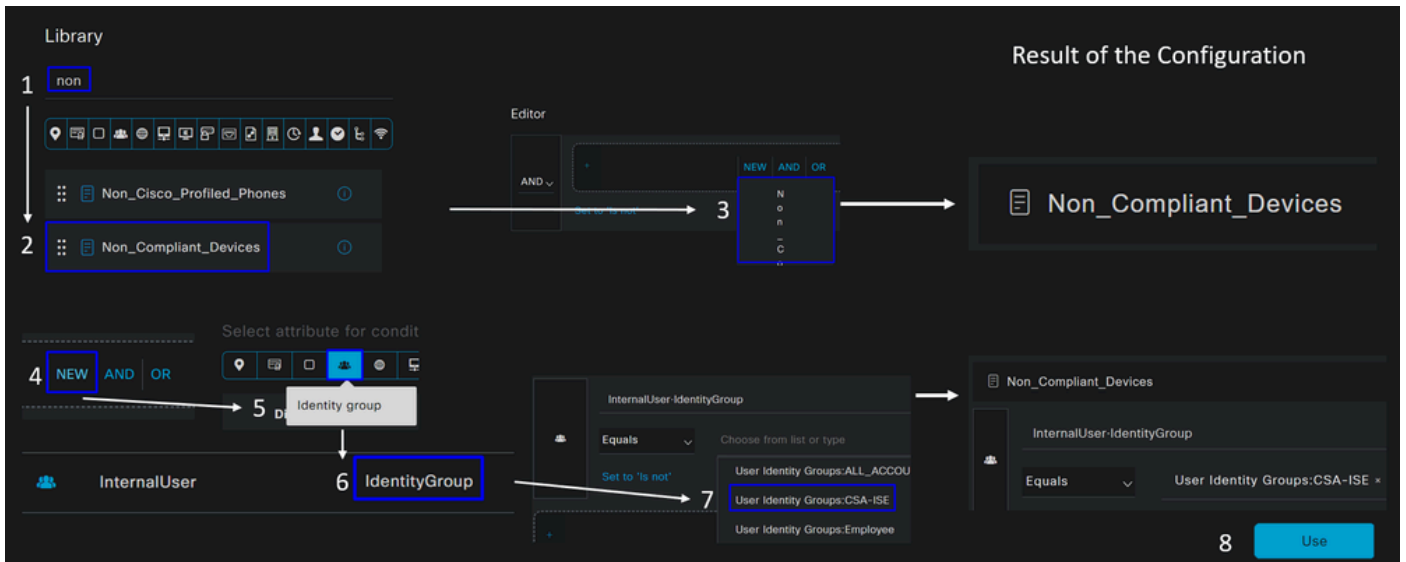


- 次の手順では、Rule NameConditions および Profiles

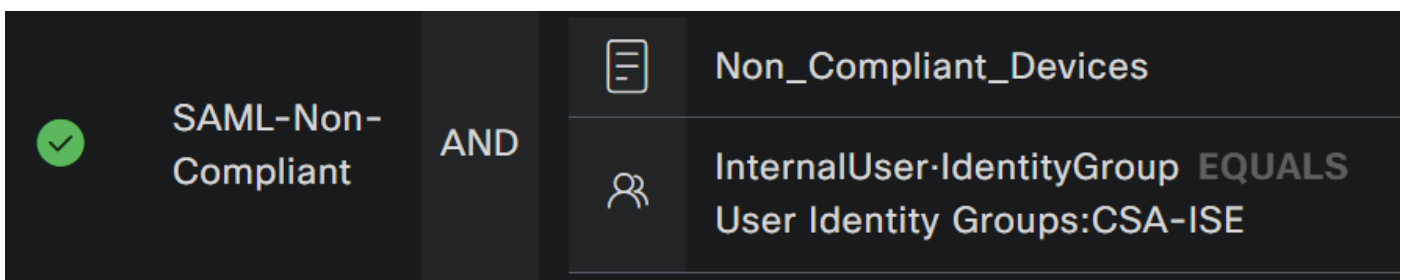
- 名前をに設Name 定する場合 **CSA-Non-Compliance Condition**
- を設定するには、 +
- **Condition Studio**
- の下に、次の情報があります。



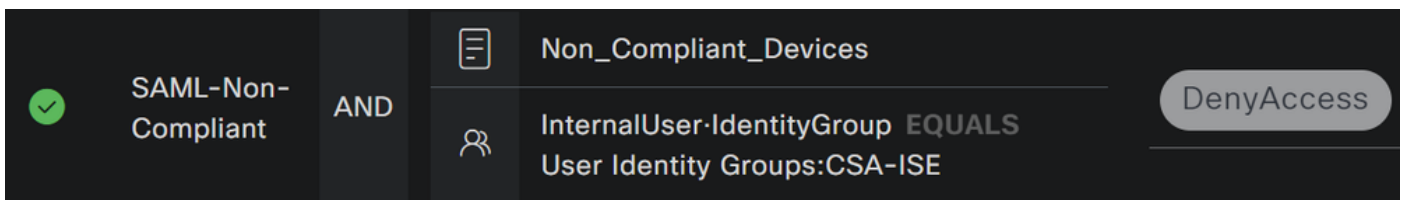
- 条件を作成するには、 **non**
- 表示されているはずですが、 **Non_Compliant_Devices**
- 下にドラッグアンドドロップします。 **Editor**
- の下をクリックします。 **New**
- アイ **Identity Group** コンをクリックします。
- 選択 **Internal User Identity Group**
- 「 **Equals**」で、照合す **User Identity Group** る名前を選択します
- クリック **Use**



- 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。

The screenshot displays the Cisco ISE GUI configuration for authorization policies. The table below summarizes the visible configuration:

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
MACSACL#-IP-CSA-Compliant-640b0b0a				
vphutan@Cisco.compt.es	CSA-ISE	CSA-ISE == SAML-Compliant	CSA-Compliant	Compliant
vphutan@Cisco.compt.es	CSA-ISE	CSA-ISE == SAML-Compliant	CSA-Compliant	Compliant
MACSACL#-IP-CSA_Redirect_To_ISE-640f14d1				
vphutan@Cisco.compt.es	CSA-ISE	CSA-ISE == SAML-Unknown...	CSA-Unknown-Compliant	Pending

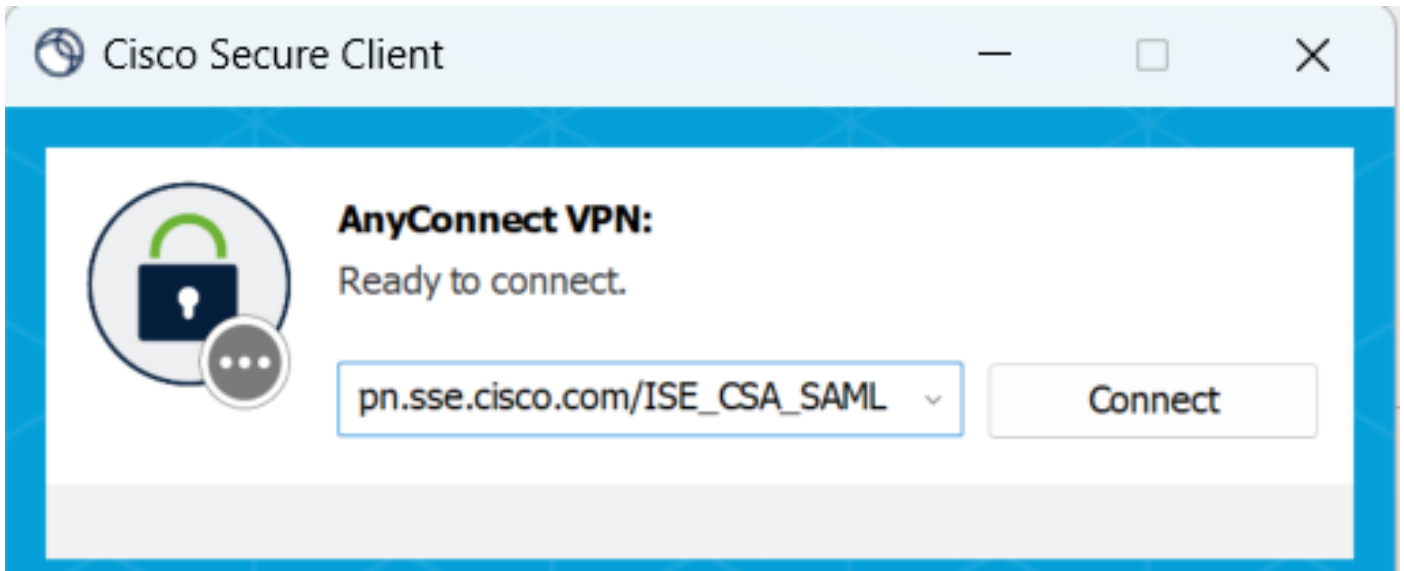
Below the table, a flow diagram illustrates the authorization process:

1. Authorization Step - Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Compliant
5205 Dynamic Authorization succeeded
5. Download CSA-Compliant
5232 DACL Download Succeeded

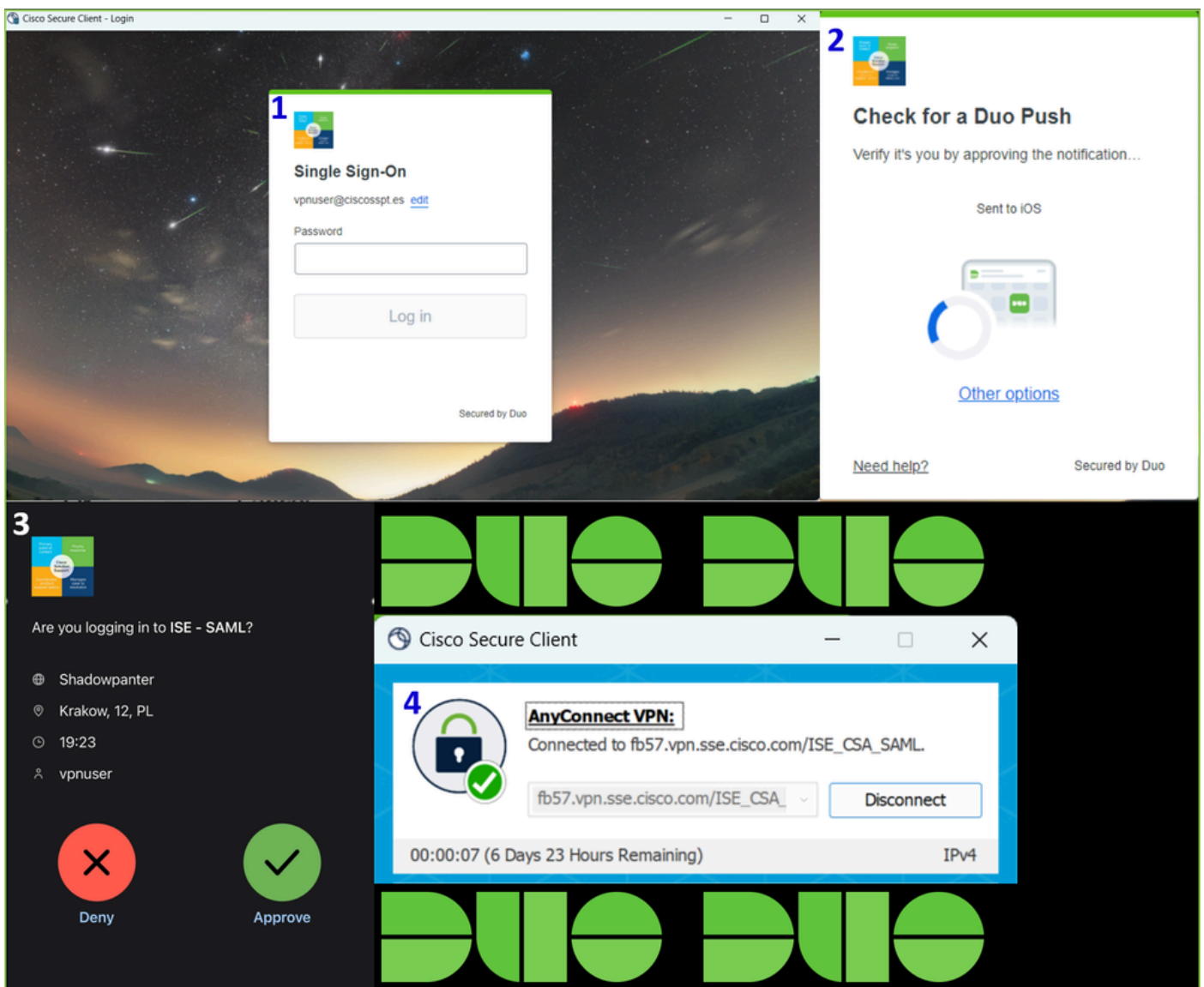
The diagram concludes with a status icon: **ISE Posture: Compliant, Network access allowed.**

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.ciscospt.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。

Device Security Check

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

9 Detecting if Agent is installed and running...

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

Device Security Check

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

Unable to detect Posture Agent

+ + This is my first time here


+ + Remind me what to do next

6. クリック [Click here to download and install agent](#)

− + This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

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

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

7. エージェントのインストール

Downloads



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

[Open file](#)

[See more](#)

Network Setup Assistant



Network Setup Assistant



Installation is completed.

Quit

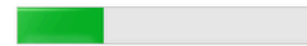
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. 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。



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.

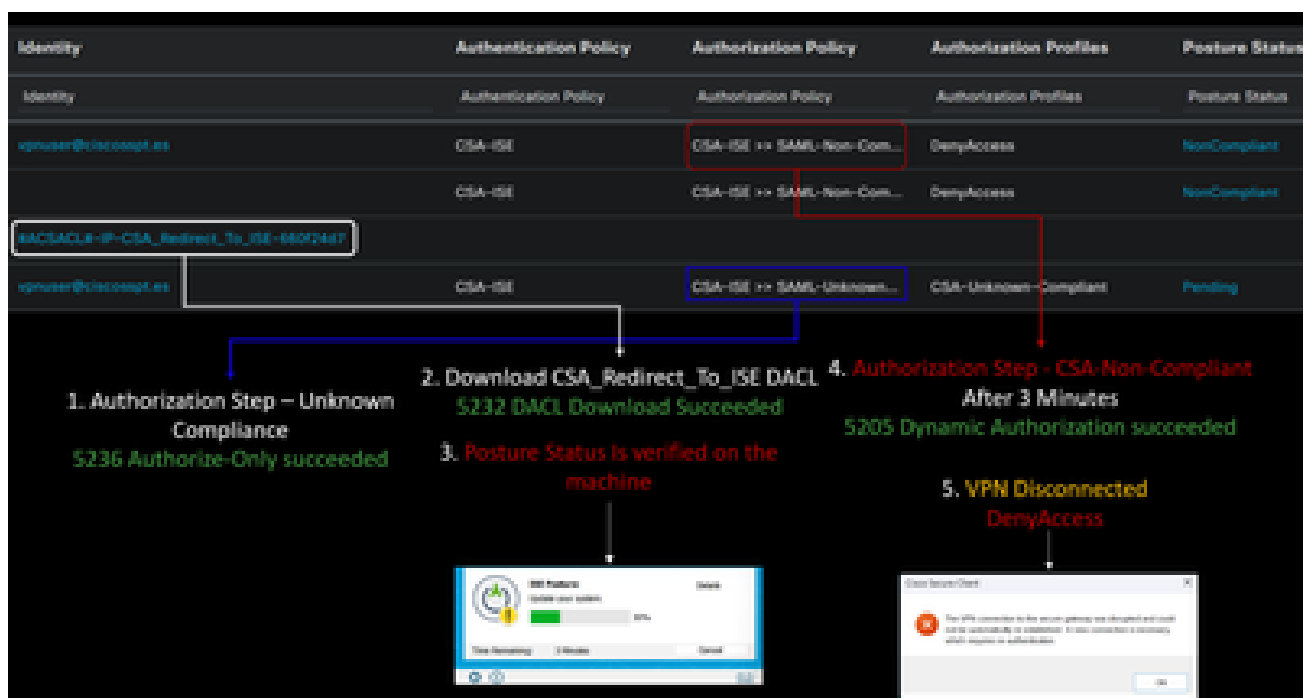
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



Cancel



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。

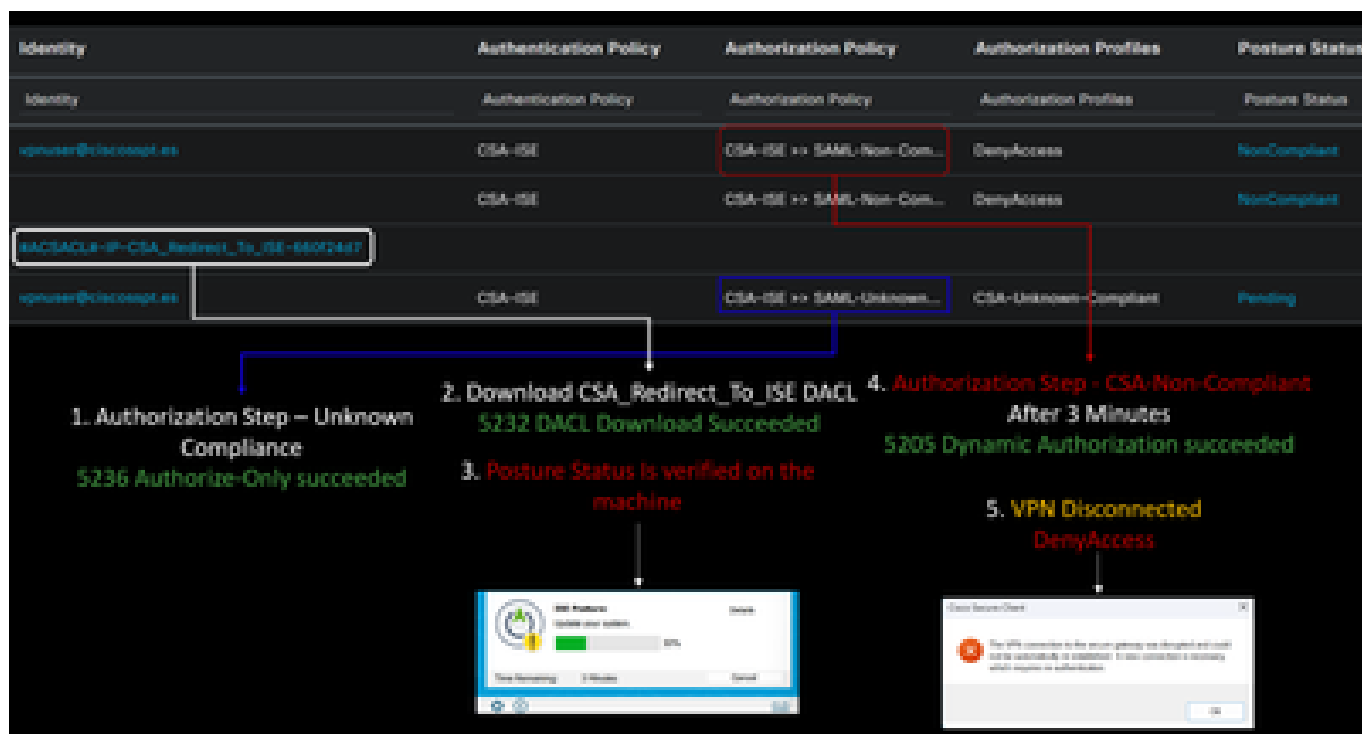
9. セキュアエンドポイントエージェントをインストールし、VPNに再接続します。

Secure Endpoint Installed **Agent Scanning** **ISE Posture Successful validated**

Scan Summary - Compliance

Required	Status
1 ✓	Done

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、ポスタ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

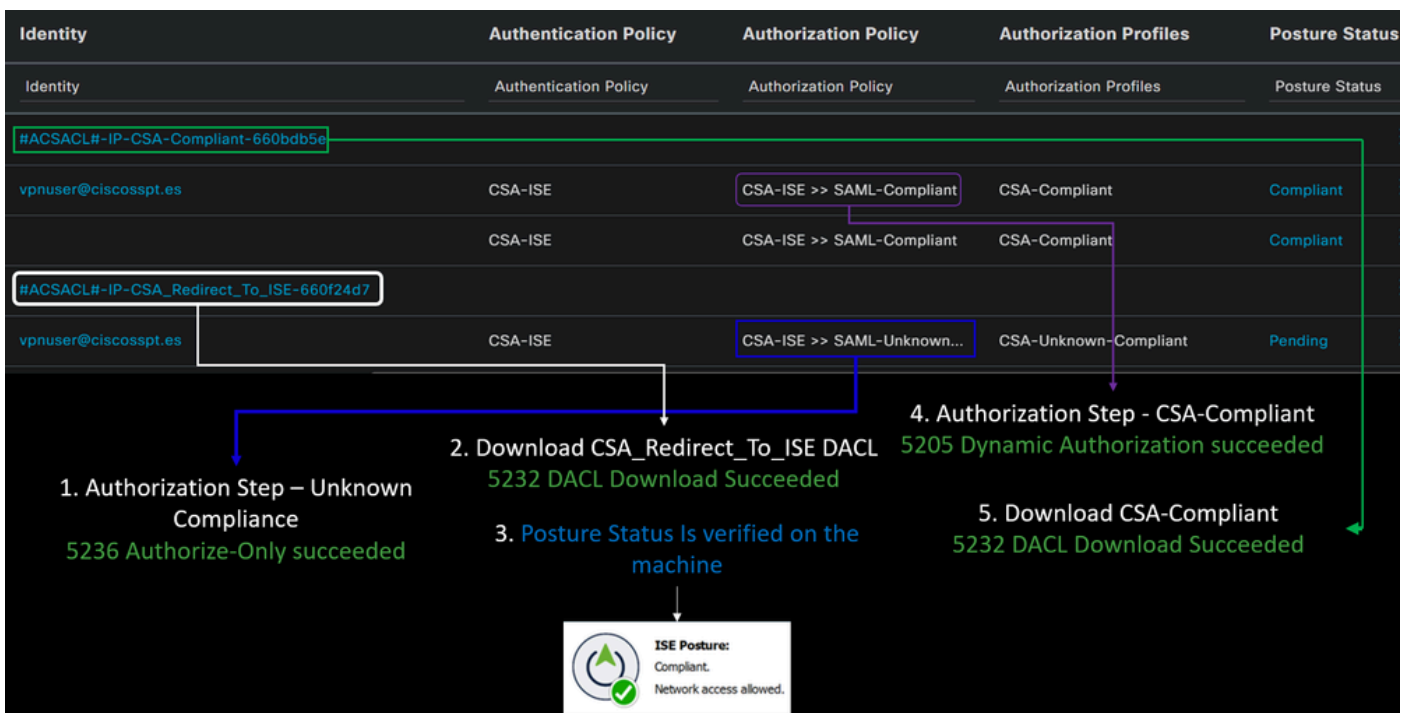
ユーザの認証結果を確認するには、コンプライアンスと非コンプライアンスの2つの例があります。ISEで確認するには、次の手順に従います。

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

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter		
0	0	0	0	0		
Refresh: Never Show: Latest 50 records Within: Last 60 minutes						
Reset Repeat Counts Export To Filter Settings						
Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
🔵	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
✅	📄	#ACSACL#-IP-CSA-Compliant-660bdb5e				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				

次のシナリオでは、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

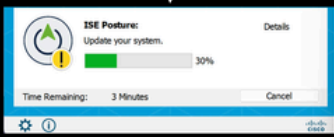



非準拠

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

#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7

1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Non-Compliant After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected DenyAccess

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。

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

- 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。

Summary



Connected

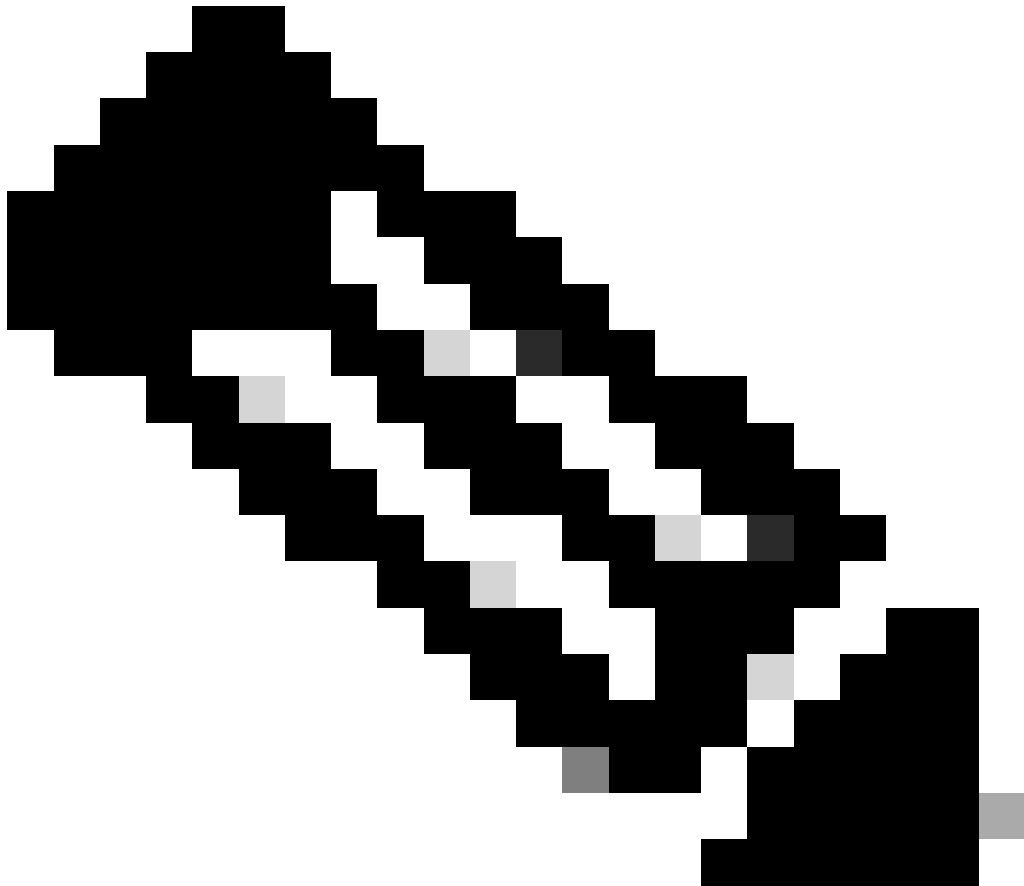
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2 : ファイアウォールでトラフィックを許可します。

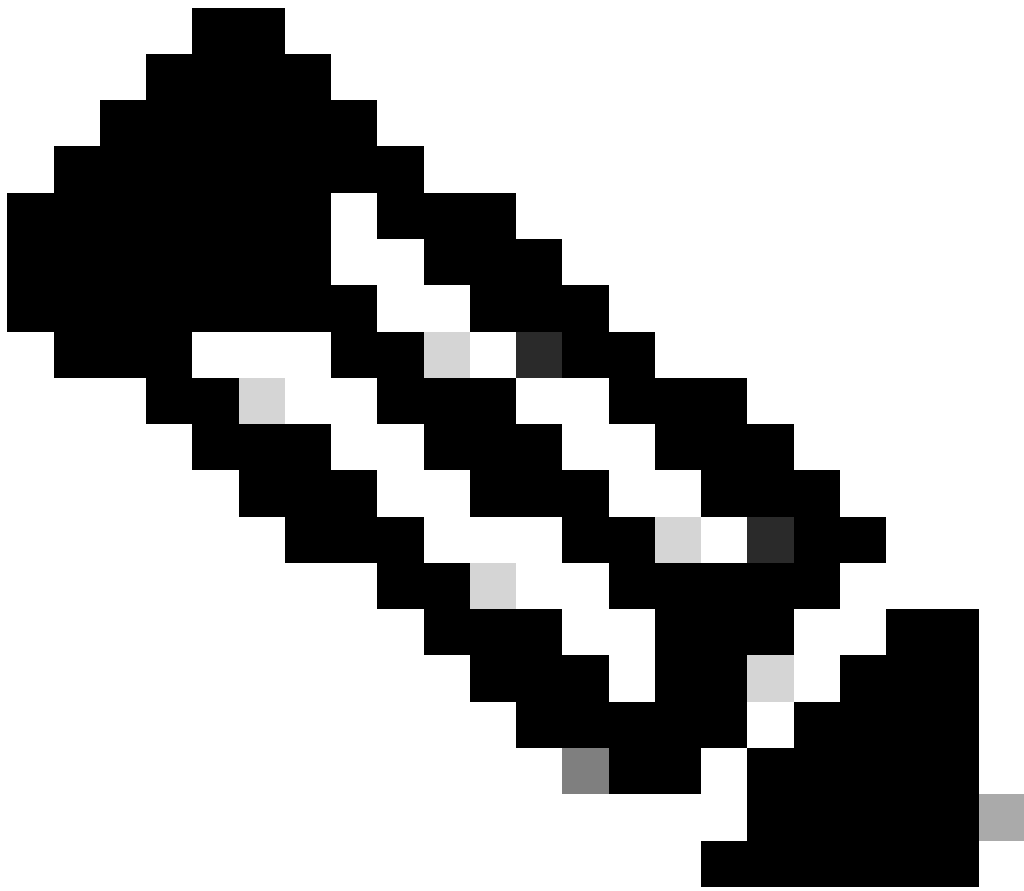
セキュアアクセスでRADIUS認証にISEデバイスを使用できるようにするには、ネットワークへのセキュアアクセスからのルールを、必要なRADIUSポートで設定する必要があります。

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

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などの名前を検出されるように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**

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

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する必要があります。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

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

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

[Help](#)

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

192.168.10.206

TCP - (HTTP/HTTPS)

Any

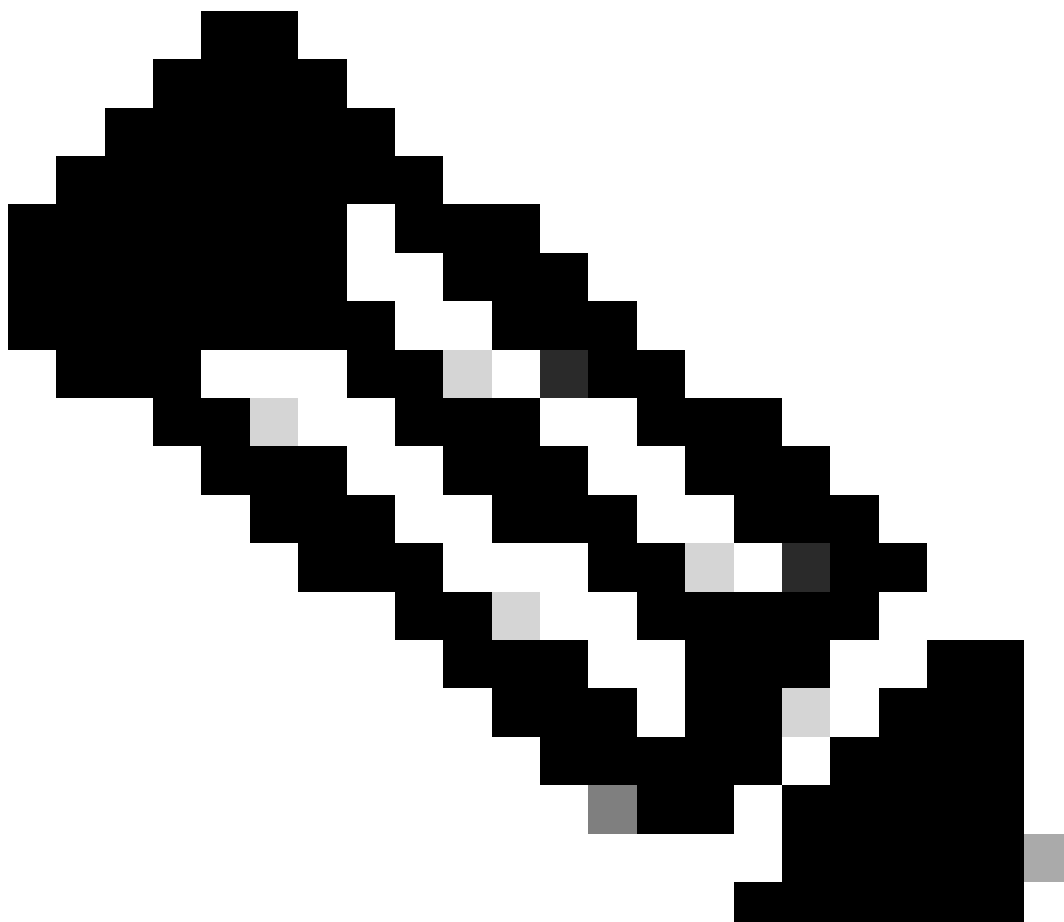
[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

VPN connections

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

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

1 Specify Access

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


Action

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


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

Endpoint Requirements

For VPN connections:

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

For Branch connections:

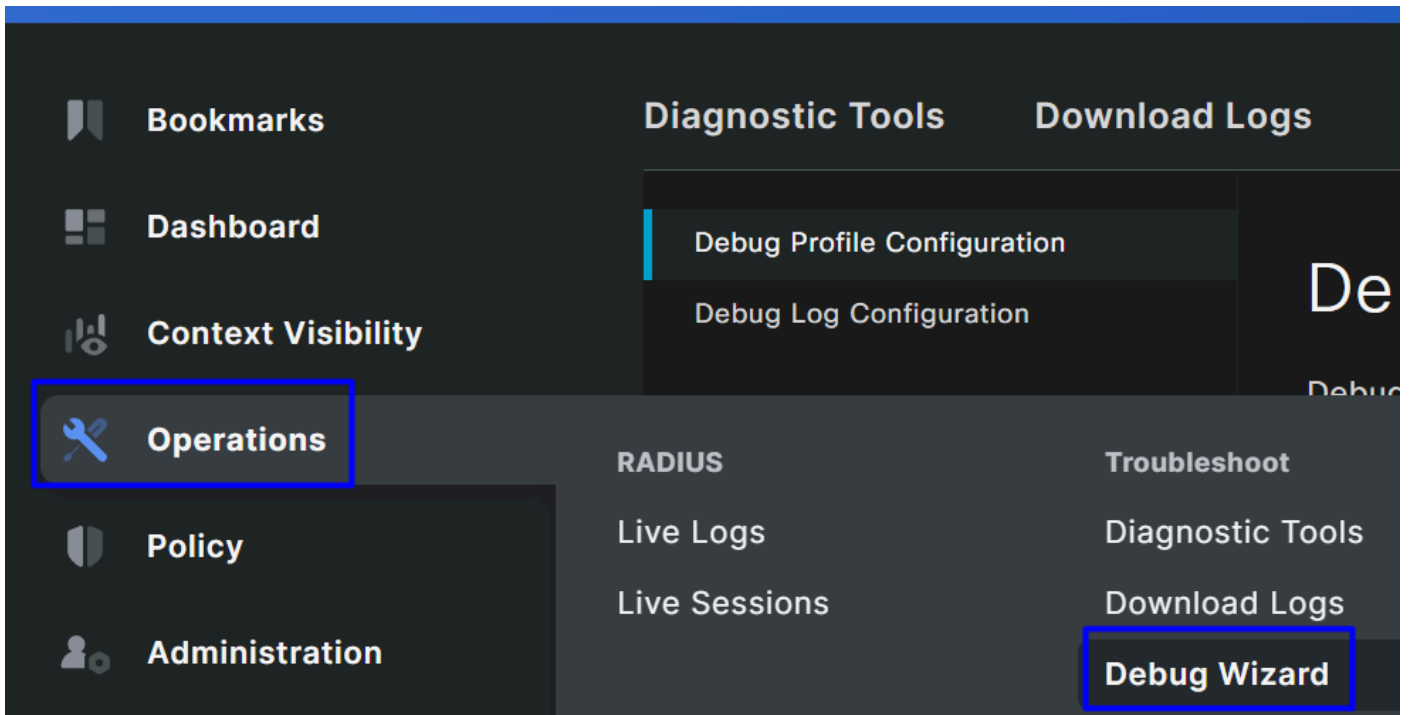
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

トラブルシューティング

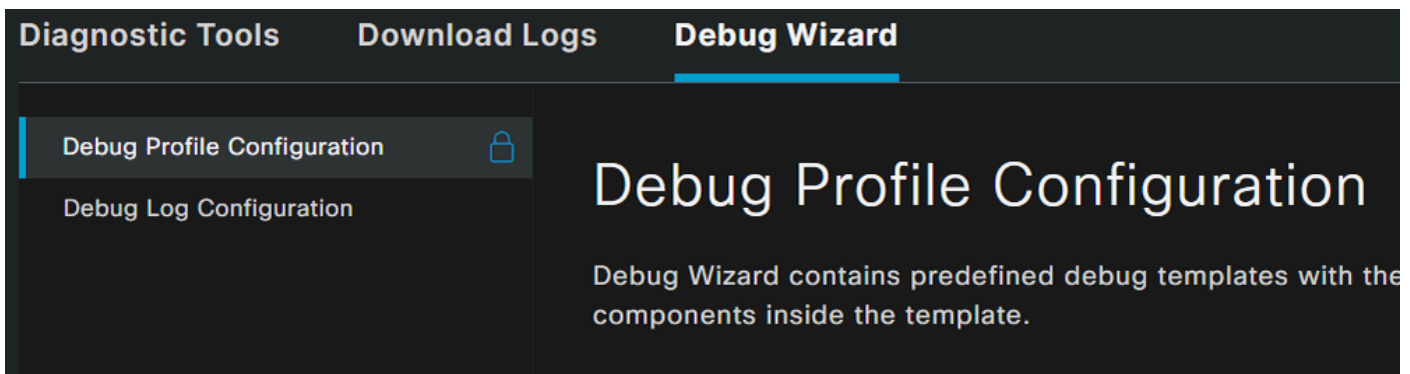
ISEポスチャデバッグログのダウンロード方法

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

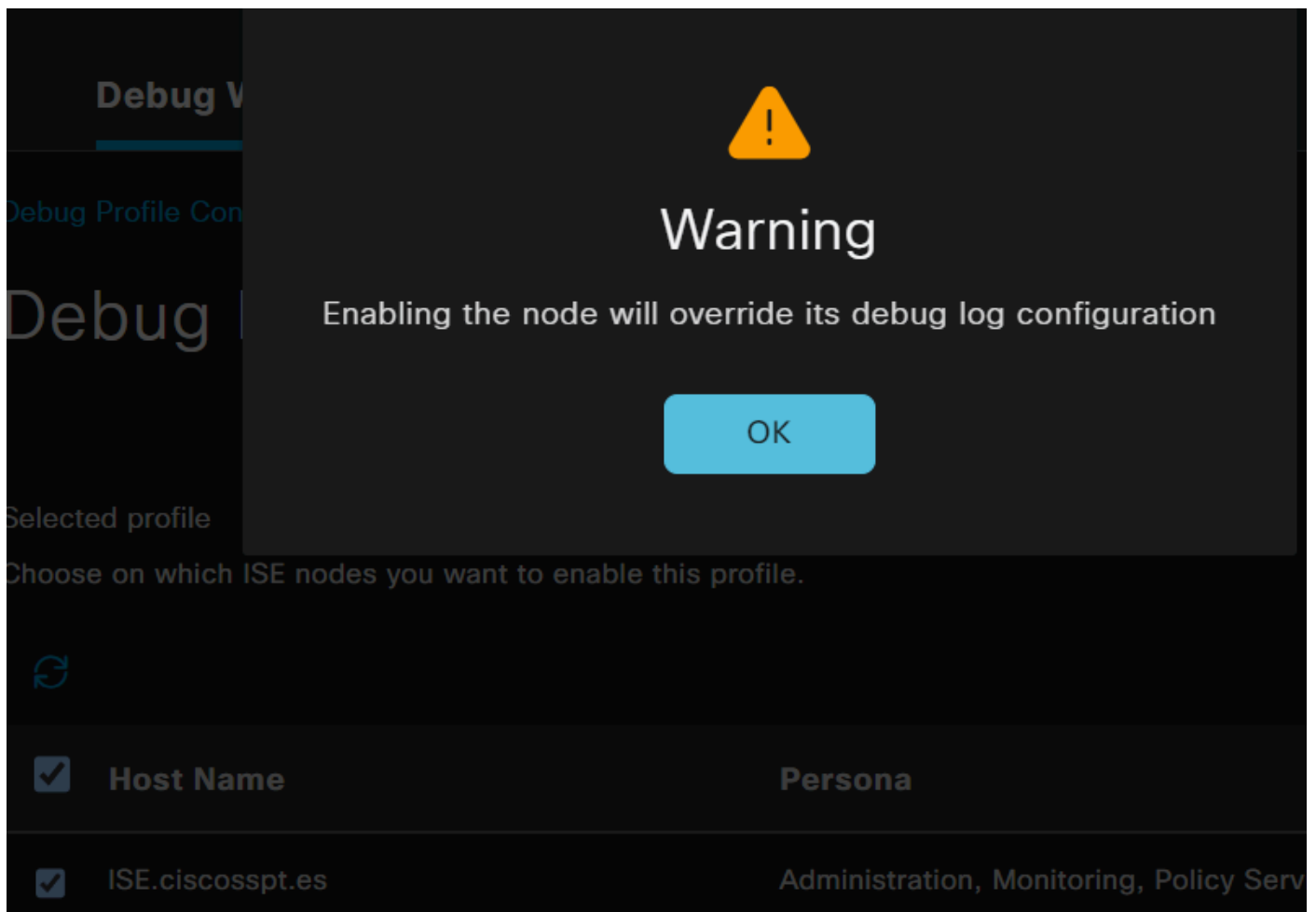
1



Posture

Pos

- 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



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

Debug V

Debug Profile Con

Warning

Enabling the node will override its debug log configuration

OK

Selected profile

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

Host Name Persona

ISE.ciscosspt.es Administration, Monitoring, Policy Serv

- クリック Save

Debug Nodes

Selected profile Posture

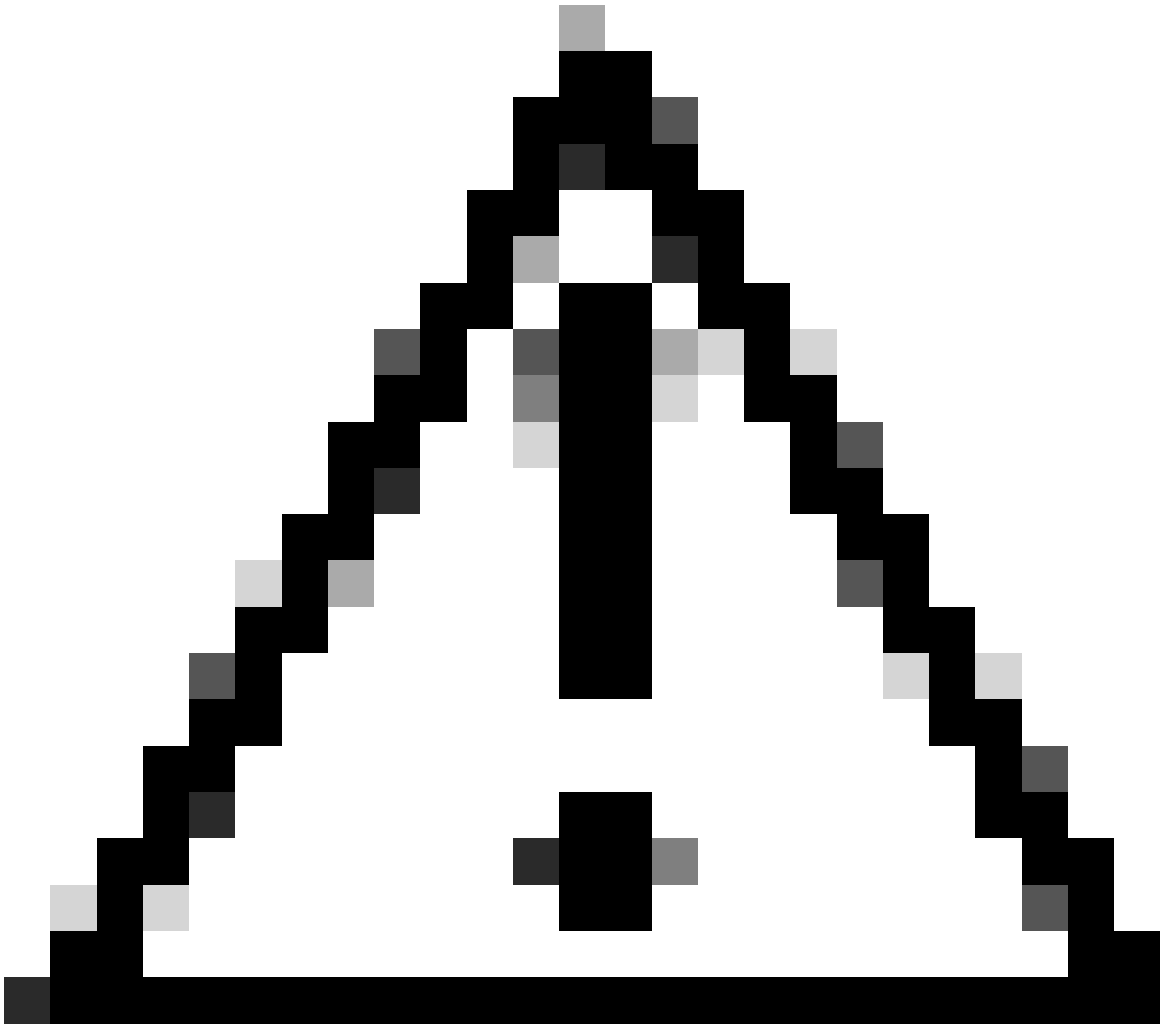
Choose on which ISE nodes you want to enable this profile.

 Filter  

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

Cancel

Save



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



Appliance node list

ISE

- で **Support Bundle**、次のオプションを選択します。

Support Bundle

Debug Logs

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

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

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

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- 通常の Support Bundle Encryption
 - Shared Key Encryption
 - ファイルEncryption key と Re-Enter Encryption key

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

▽ Support Bundle - Last Generated

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

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

Size(KB): 52165.0

Download

Delete


















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

100 Events

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

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。