Configure Secure Access for RA-VPNaaS with Duo SSO and Posture Assessment with ISE

Contents

Related Information

Introduction

This document describes how to configure Posture Assessment for Remote Access VPN users with Identity Service Engine (ISE) and Secure Access with Duo.

Prerequisites

- Configure User Provisioning on Secure Access
- Configure Duo SSO with Authentication Proxy or Third-Party IDP
- Cisco ISE connected to Secure Access through the tunnel

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Service Engine
- Secure Access
- Cisco Secure Client
- Guide to Two-Factor Authentication - Duo Security
- ISE Posture
- Authentication, Authorization, and Accounting

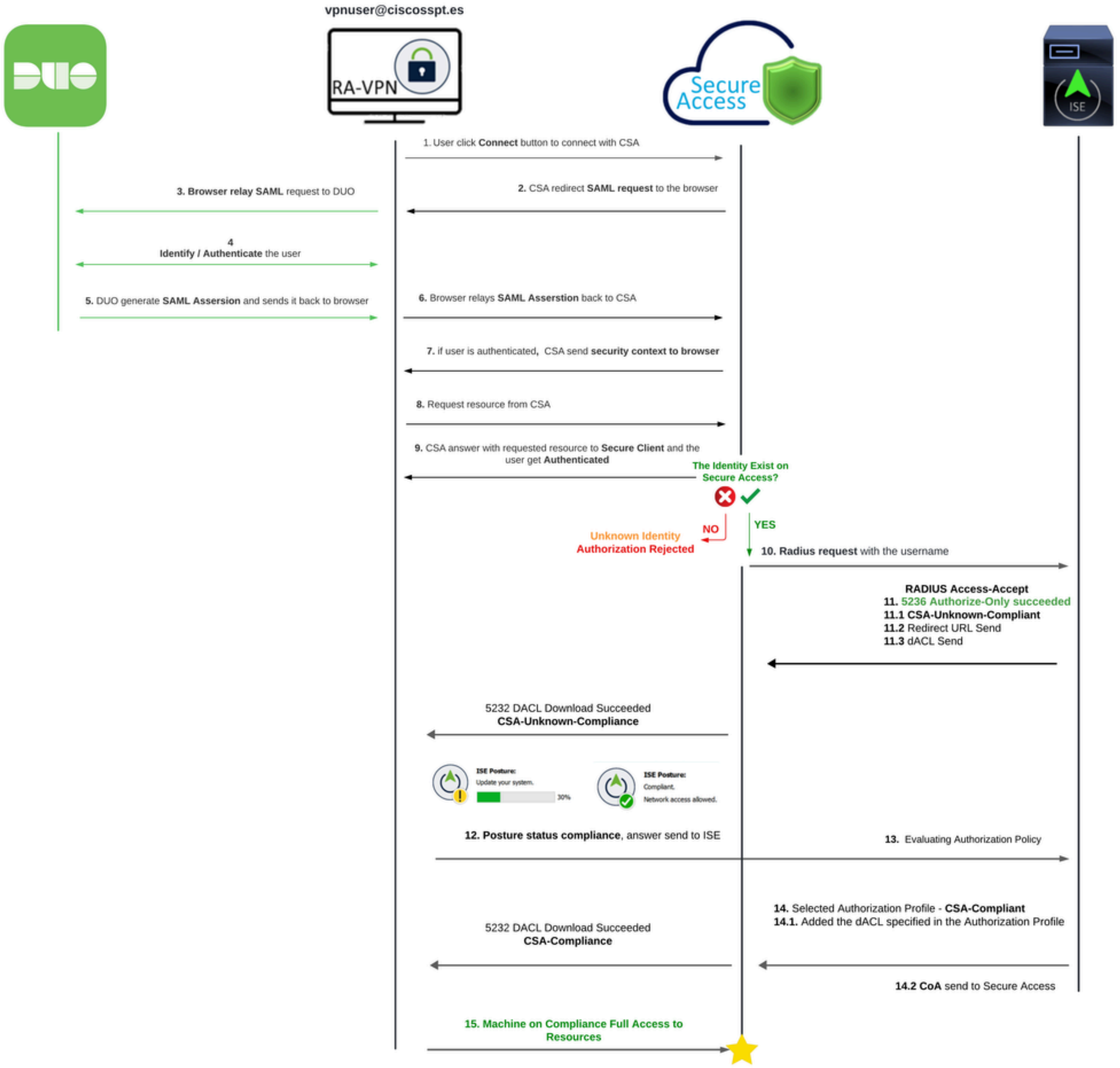
Components Used

The information in this document is based on:

- Identity Service Engine (ISE) Version 3.3 Patch 1
- Secure Access
- Cisco Secure Client - Anyconnect VPN Version 5.1.2.42

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information



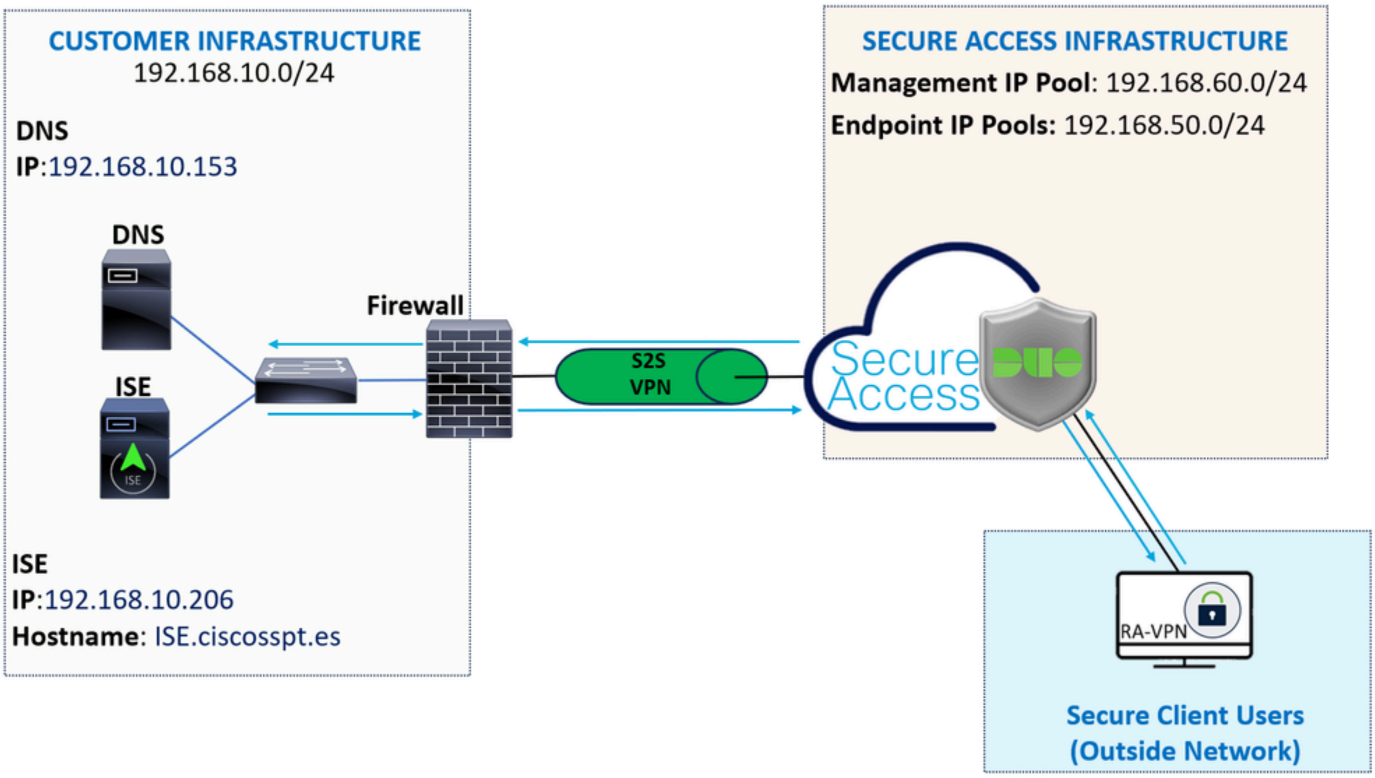
vpnuser@ciscosspt.es
RA-VPN
Secure Access
ISE
1. User click Connect button to connect with CSA
2. CSA redirect SAML request to the browser
3. Browser relay SAML request to DUO
4
Identify / Authenticate the user
5. DUO generate SAML Assersion and sends it back to browser
6. Browser relays SAML Asserstion back to CSA
7. if user is authenticated, CSA send security context to browser
8. Request resource from CSA
9. CSA answer with requested resource to Secure Client and the user get Authenticated
The Identity Exist on Secure Access?
NO
YES
Unknown Identity
Authorization Rejected
10. Radius request with the username
RADIUS Access-Accept
11. 5236 Authorize-Only succeeded
11.1 CSA-Unknown-Compliant
11.2 Redirect URL Send
11.3 dACL Send
5232 DACL Download Succeeded
CSA-Unknown-Compliance
ISE Posture:
Update your system.
30%
ISE Posture:
Compliant.
Network access allowed.
12. Posture status compliance, answer send to ISE
13. Evaluating Authorization Policy
14. Selected Authorization Profile - CSA-Compliant
14.1. Added the dACL specified in the Authorization Profile
5232 DACL Download Succeeded
CSA-Compliance
14.2 CoA send to Secure Access
15. Machine on Compliance Full Access to Resources

Integrating Duo SAML with Cisco Identity Services Engine (ISE) enhances the authentication process, adding another layer of security to Cisco Secure Access solutions. Duo SAML provides a Single Sign-On (SSO) capability that simplifies the user login process while ensuring high-security standards.

Once authenticated through Duo SAML, the authorization process is handled by Cisco ISE. This allows for dynamic access control decisions based on user identity and device posture. ISE can enforce detailed policies that dictate what resources a user can access, when, and from which devices.

Note: To configure the RADIUS integration, you need to make sure you have communication between both platforms.

Network Diagram


CUSTOMER INFRASTRUCTURE
192.168.10.0/24
DNS
IP:192.168.10.153
DNS
Firewall
ISE
ISE
ISE
IP:192.168.10.206
Hostname: ISE.ciscosspt.es
S2S
VPN
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)

Configure

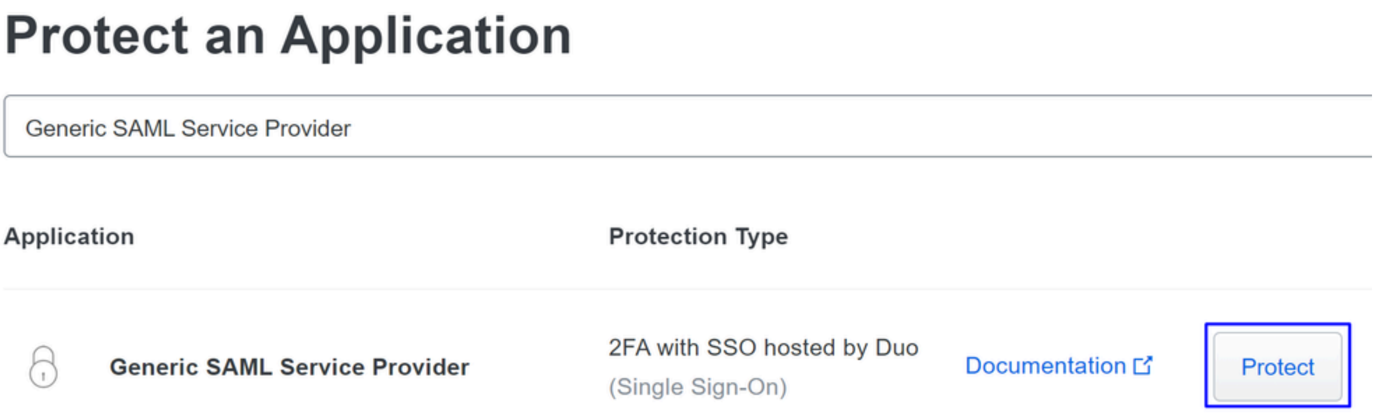
Note: Before you begin the configuration process, you must complete the First Steps with Secure Access and ISE Integration.

Duo Configuration

To configure the RA-VPN Application, proceed with the next steps:

Navigate to your Duo Admin Panel

- Navigate to **Applications > Protect an Application**
- Search for **Generic SAML Service Provider**
- Click Protect

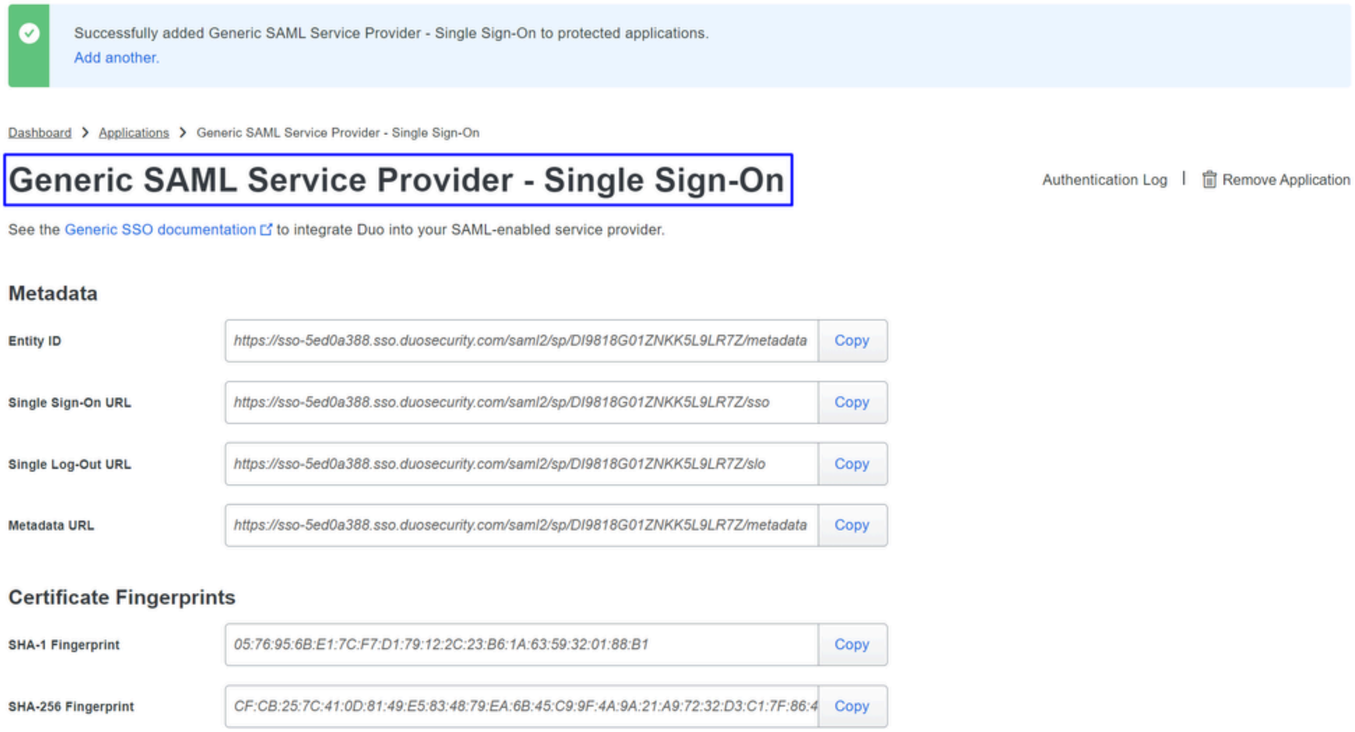


Protect an Application

Generic SAML Service Provider

Application	Protection Type		
Generic SAML Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

You must have the application displayed on the screen; remember the application name for the VPN configuration.



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

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

Metadata

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

Certificate Fingerprints

SHA-1 Fingerprint	05:76:95:6B:E1:7C:F7:D1:79:12:2C:23:B6:1A:63:59:32:01:88:B1	Copy
SHA-256 Fingerprint	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	Copy

In this case is **Generic SAML Service Provider.**

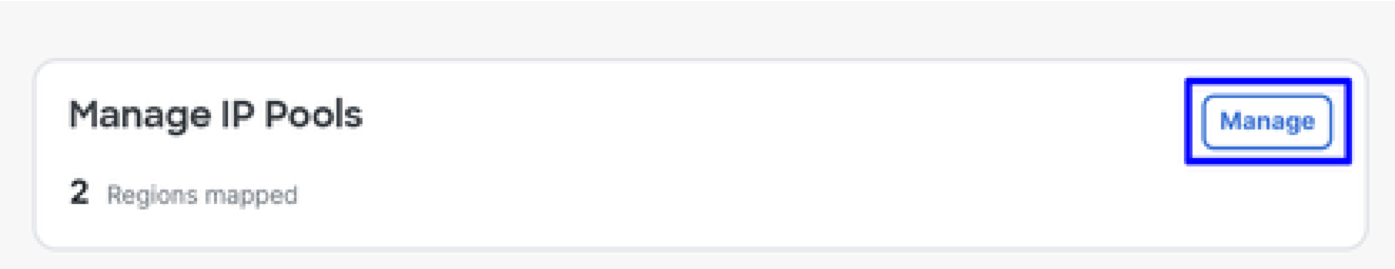
Secure Access Configuration

Configure Radius Group on the IP Pools

To configure the VPN Profile using Radius, proceed with the next steps:

Navigate to your Secure Access Dashboard.

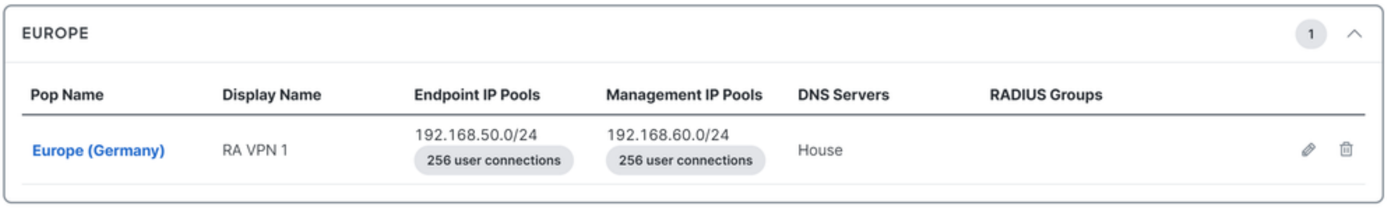
- Click on **Connect** > **Enduser Connectivity** > **Virtual Private Network**
- Under your Pool Configuration (**Manage IP Pools**), clickManage



Manage IP Pools

2 Regions mapped

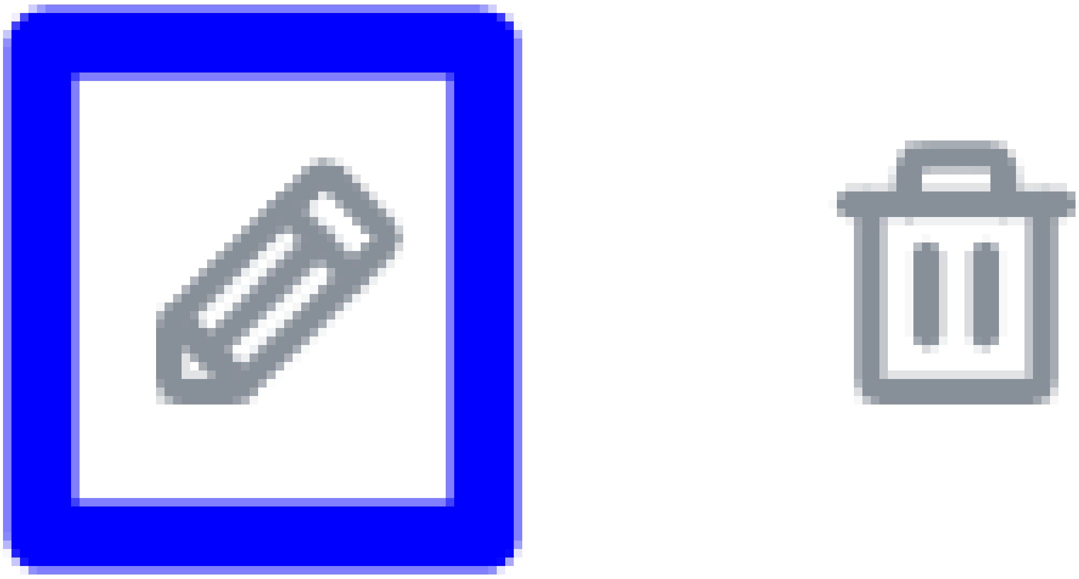
- Choose the **IP Pool Region** and configure the **Radius Server**



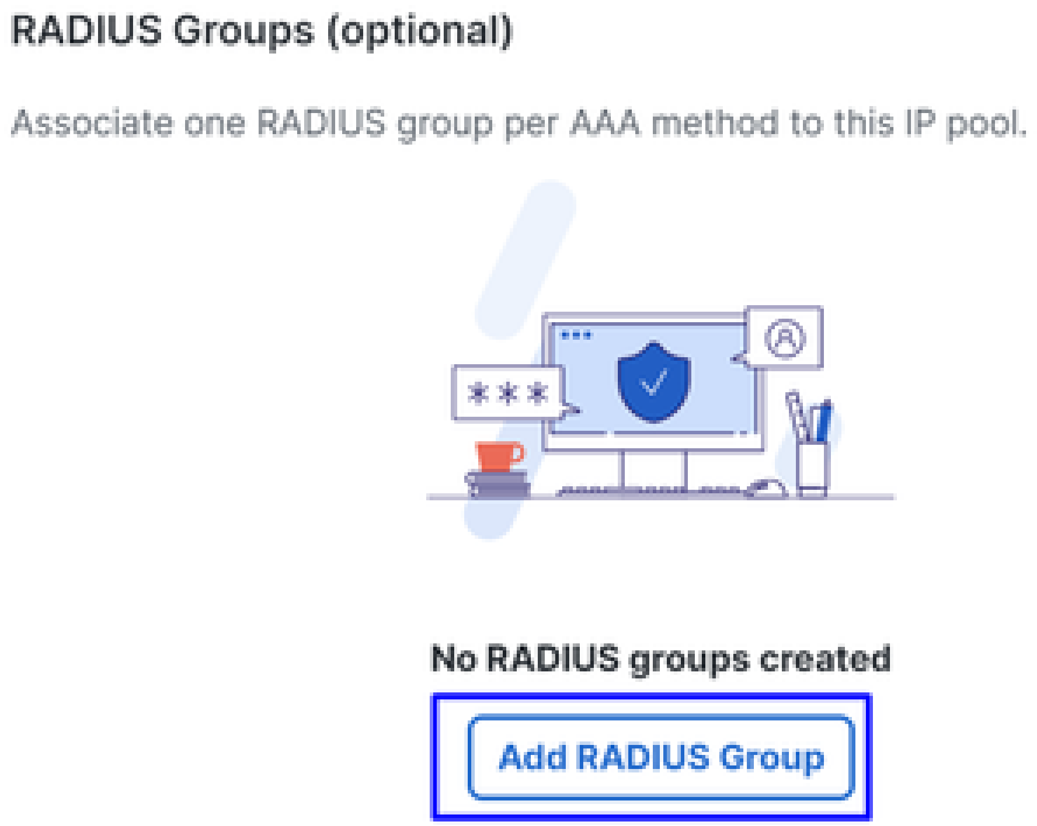
EUROPE 1

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	

- Click the pencil to edit



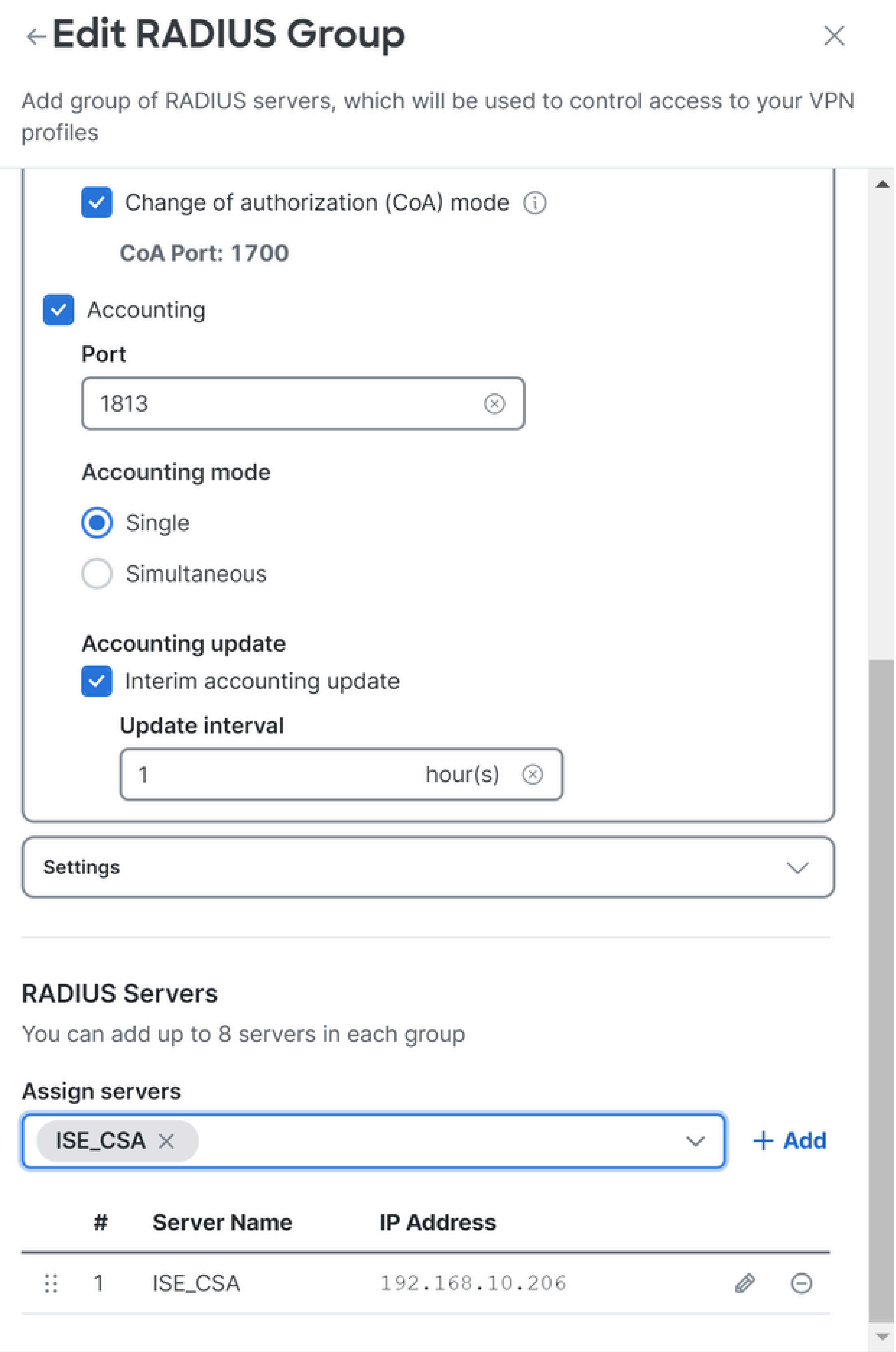
- Now, under the IP Pool section configuration drop-down under **Radius Group (Optional)**
- Click Add RADIUS Group



RADIUS Groups (optional)

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

No RADIUS groups created



Edit RADIUS Group

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

☑ Change of authorization (CoA) mode

CoA Port: 1700

☑ Accounting

Port

1813

Accounting mode

● Single

○ Simultaneous

Accounting update

☑ Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

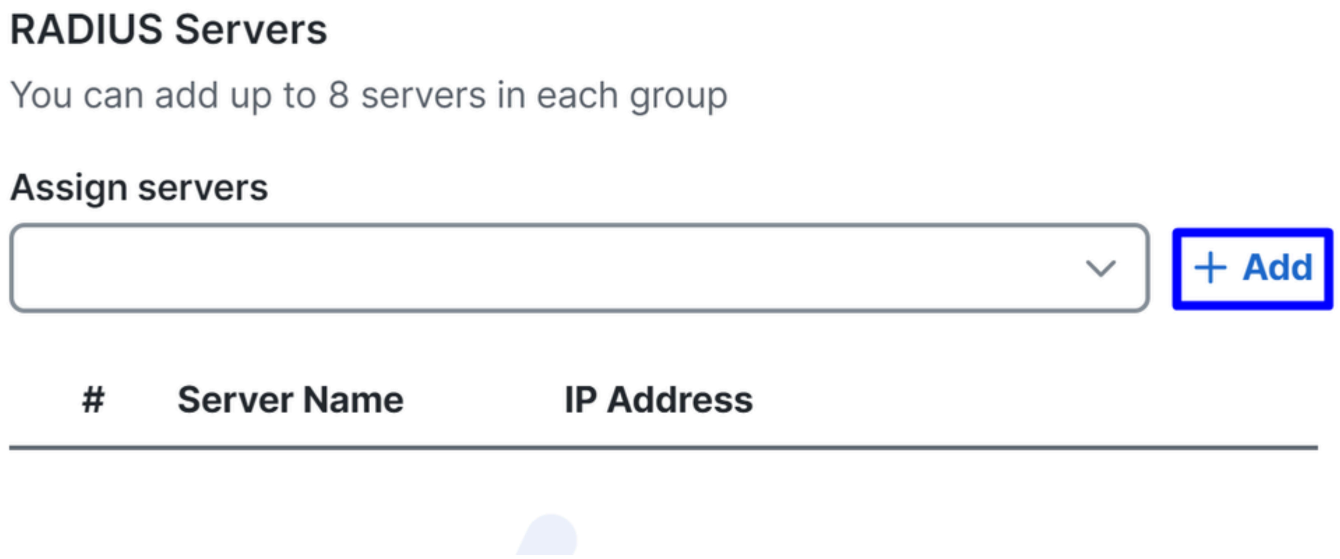
+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

    - **Authentication**: Mark the checkbox for **Authentication** and select the port, by default, is 1812
        - In the case that your authentication requires Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2) mark the checkbox
    - **Authorization**: Mark the checkbox for Authorization and select the port, by default, is 1812
        - Mark the checkbox for **Authorization mode Only** and**Change of Authorization (CoA) mode** to permit the posture and changes from ISE
    - **Accounting**: Mark the checkbox for Authorization and select the port, by default, is 1813
        - Choose **Single or Simultaneous** (In single mode, accounting data is sent to only one server. In simultaneous mode, accounting data to all servers in the group)
        - Mark the checkbox for **Accounting update** to enable the periodic generation of RADIUS interim-accounting-update messages.

Caution: Both the Authentication and **Authorization** methods, when selected, must use the same port.

- After that, you need to configure the **RADIUS Servers** (ISE) that is used to authenticate via AAA on the section **RADIUS Servers**:
- Click on + Add



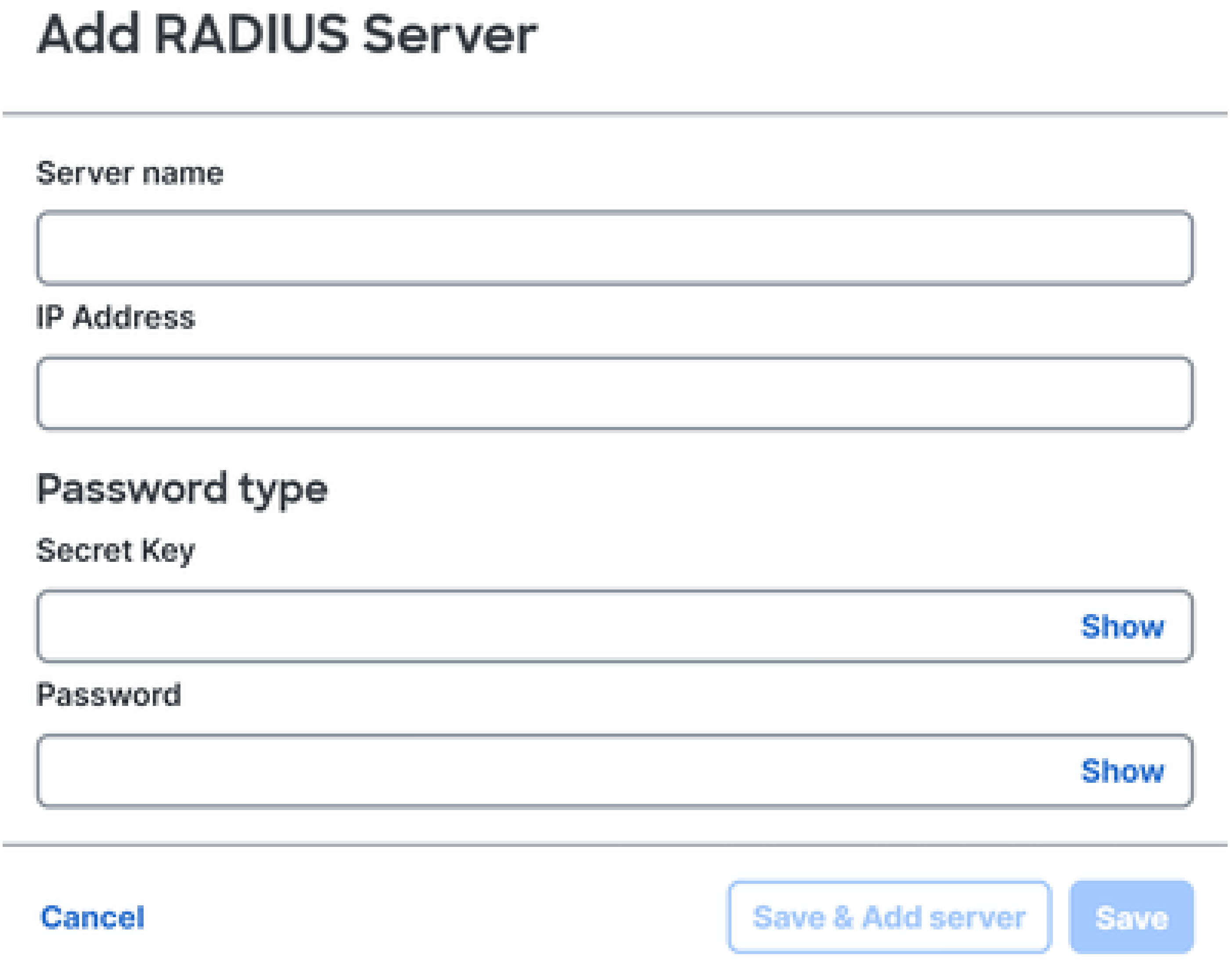
RADIUS Servers

You can add up to 8 servers in each group

Assign servers

#	Server Name	IP Address

- Then, configure the next options:



Add RADIUS Server

Server name

IP Address

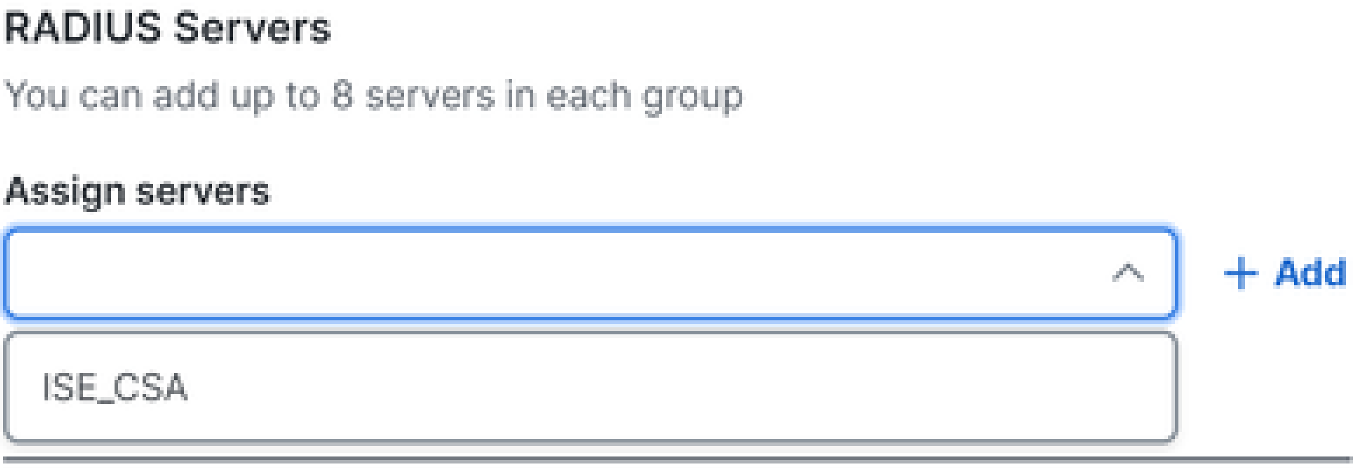
Password type

Secret Key

Password

- Server Name: Configure a name to identify your ISE Server.
- **IP Address**: Configure the IP of your Cisco ISE device that is reachable through Secure Access
- **Secret Key**: Configure your RADIUS secret Key

- **Password**: Configure your Radius password
- Click **Save** and assign your Radius Server under the Assign Server option and select your ISE server:



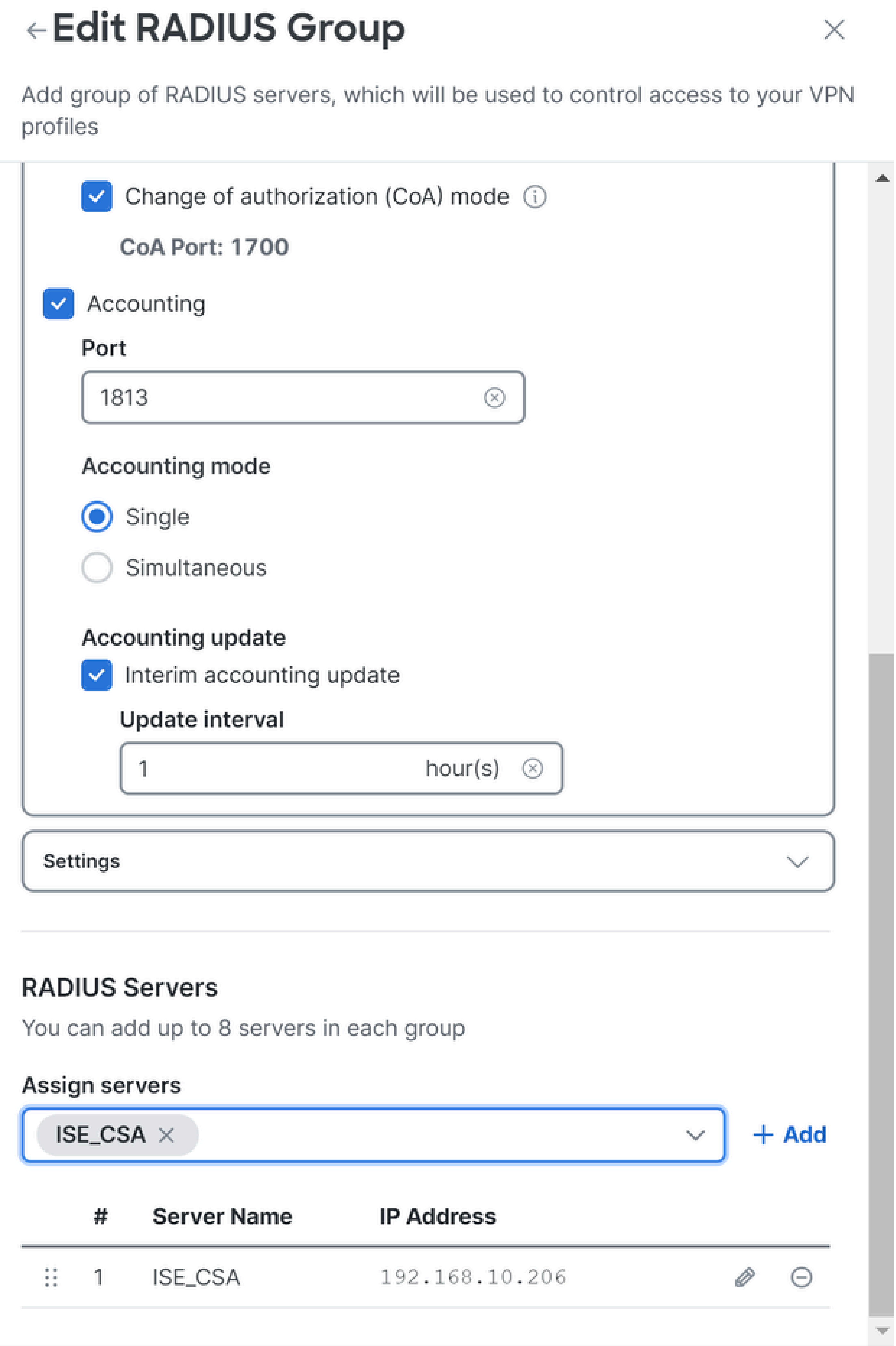
RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

- Click **Save** again to save all the configuration done



← 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

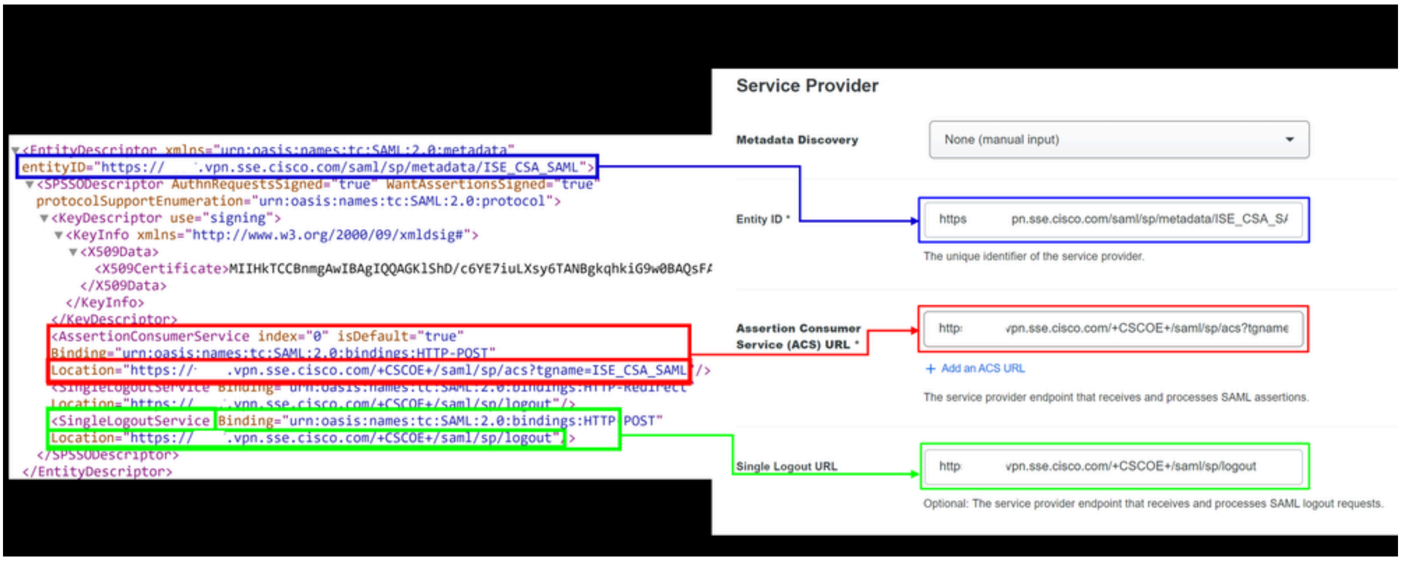
ISE_CSA ×

+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**: Choose **SAML**

- Click Download Service Provider XML file
- Replace the information in the application configured in the step, Duo Configuration



```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://    .vpn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SAML">
 ▼<SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   ▼<KeyDescriptor use="signing">
     ▼<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
       ▼<X509Data>
          <X509Certificate>MIIHkTCCBnmgAwIBAgIQQAGKlShD/c6YE7iuLXsy6TANBgkqhkiG9w0BAQsFA
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <AssertionConsumerService index="0" isDefault="true"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://    .vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=ISE_CSA_SAML"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://    .vpn.sse.cisco.com/+CSCOE+/saml/sp/logout"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://    .vpn.sse.cisco.com/+CSCOE+/saml/sp/logout"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

Service Provider

Metadata Discovery: None (manual input)

Entity ID *: https   pn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SA

The unique identifier of the service provider.

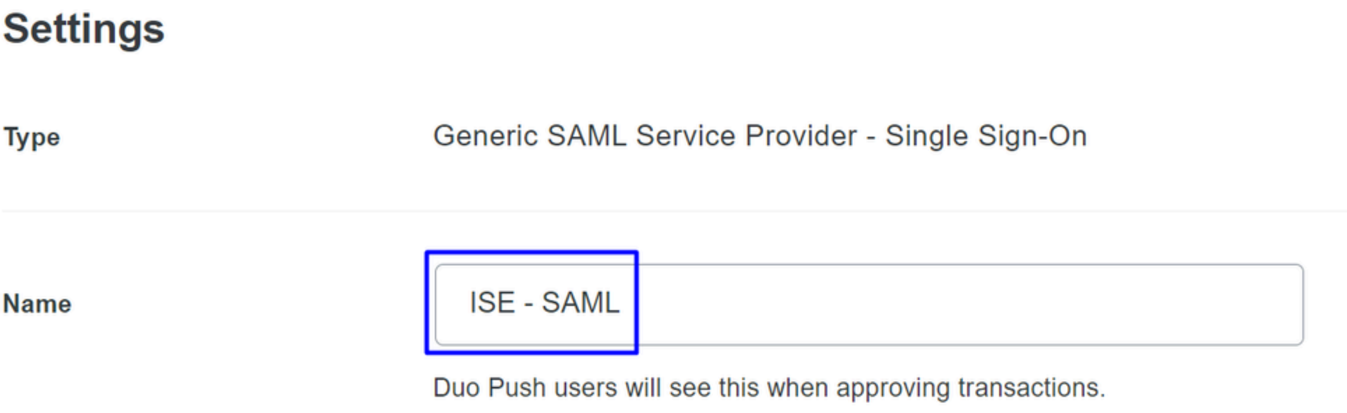
Assertion Consumer Service (ACS) URL *: http: vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: http: vpn.sse.cisco.com/+CSCOE+/saml/sp/logout

Optional: The service provider endpoint that receives and processes SAML logout requests.

- Once you have configured that information, change the name of the Duo to something related to the integration that you are making



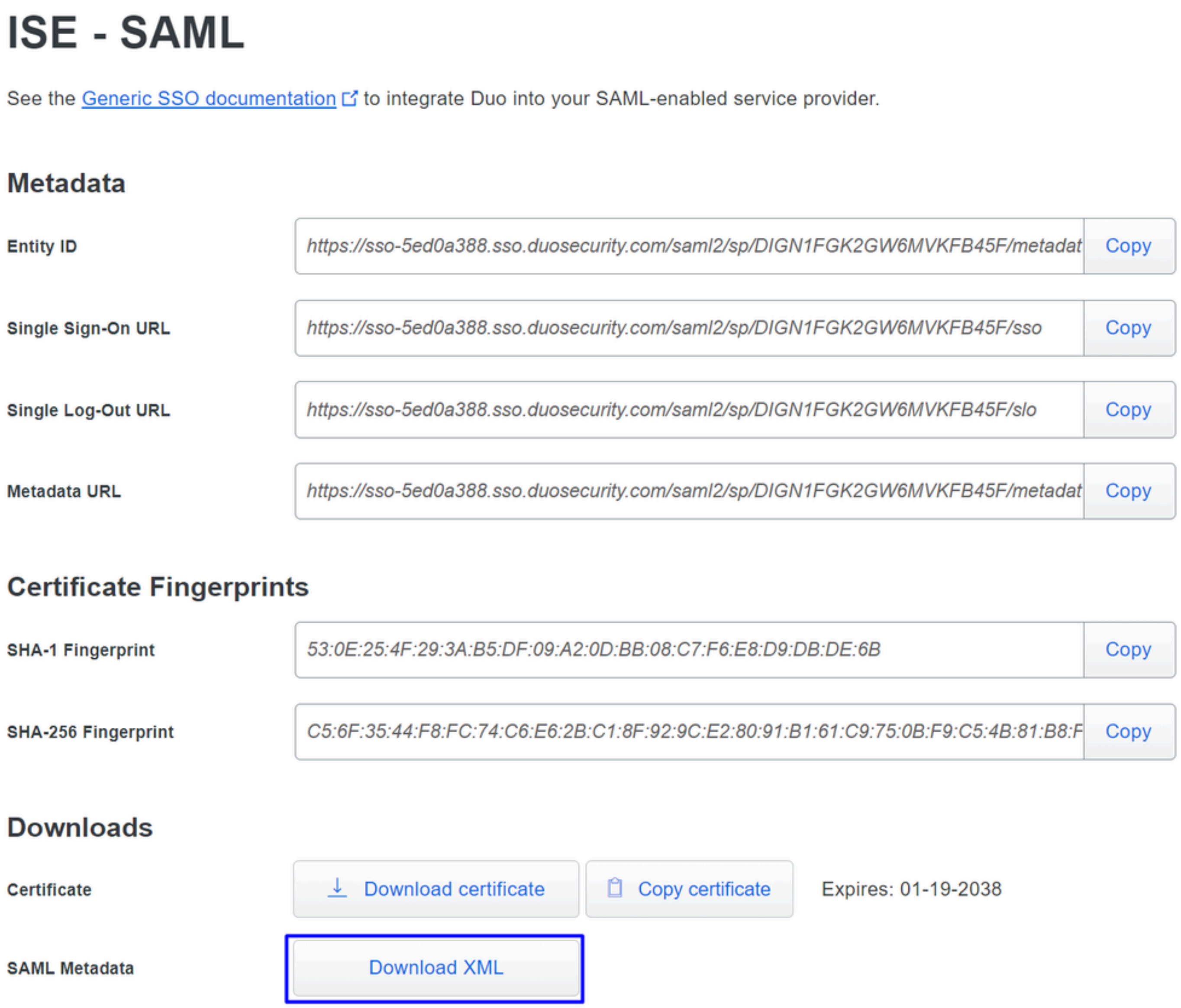
Settings

Type: Generic SAML Service Provider - Single Sign-On

Name: ISE - SAML

Duo Push users will see this when approving transactions.

- Click **Save** on your application on Duo.
- Once you click Save, you must download the **SAML Metadata** by clicking on the button **Download XML**



ISE - SAML

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

Metadata

Entity ID: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadat Copy

Single Sign-On URL: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/sso Copy

Single Log-Out URL: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/slo Copy

Metadata URL: https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadat Copy

Certificate Fingerprints

SHA-1 Fingerprint: 53:0E:25:4F:29:3A:B5:DF:09:A2:0D:BB:08:C7:F6:E8:D9:DB:DE:6B Copy

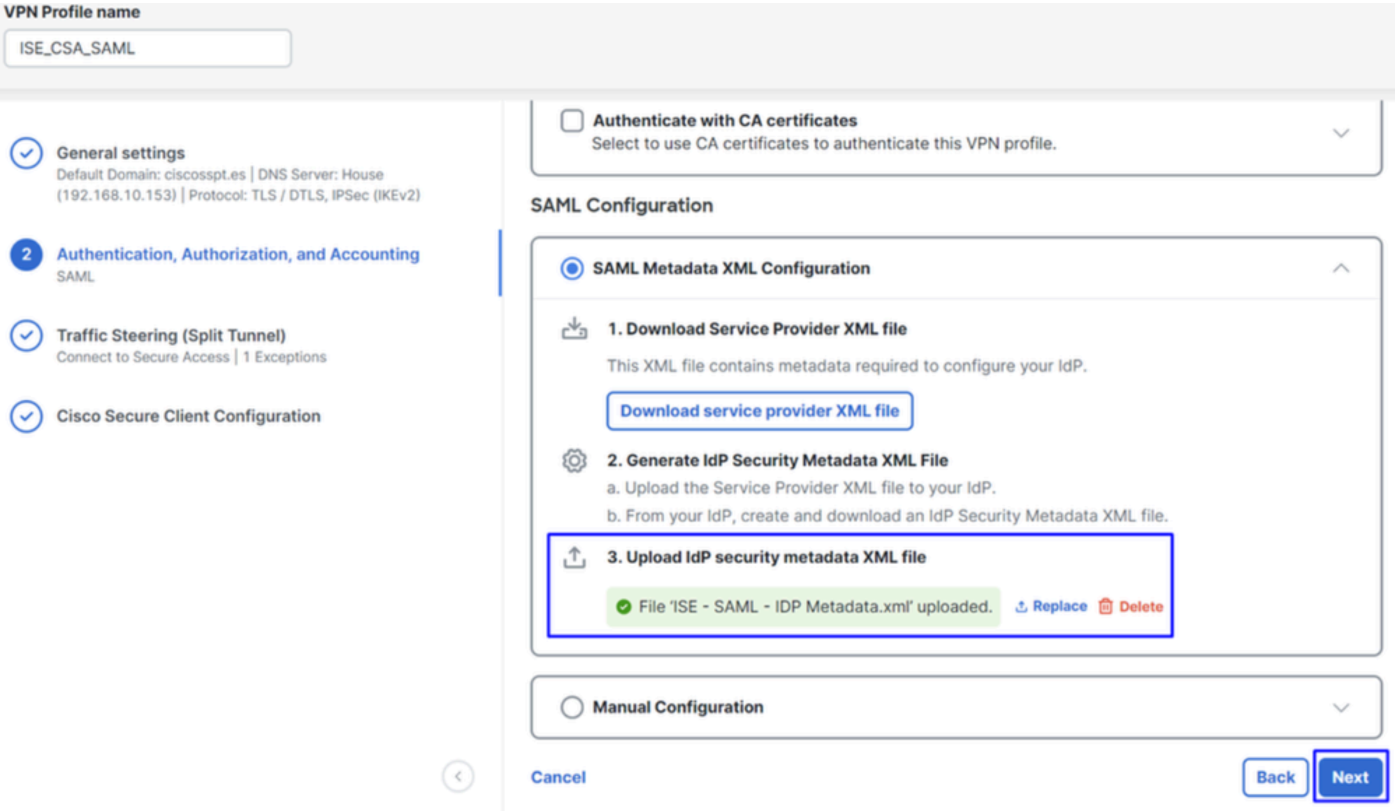
SHA-256 Fingerprint: C5:6F:35:44:F8:FC:74:C6:E6:2B:C1:8F:92:9C:E2:80:91:B1:61:C9:75:0B:F9:C5:4B:81:B8:F Copy

Downloads

Certificate: Download certificate | Copy certificate | Expires: 01-19-2038

SAML Metadata: Download XML

- Upload the **SAML Metadata** on Secure Acces under the option **3. Upload IdP security metadata XML file** and click **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

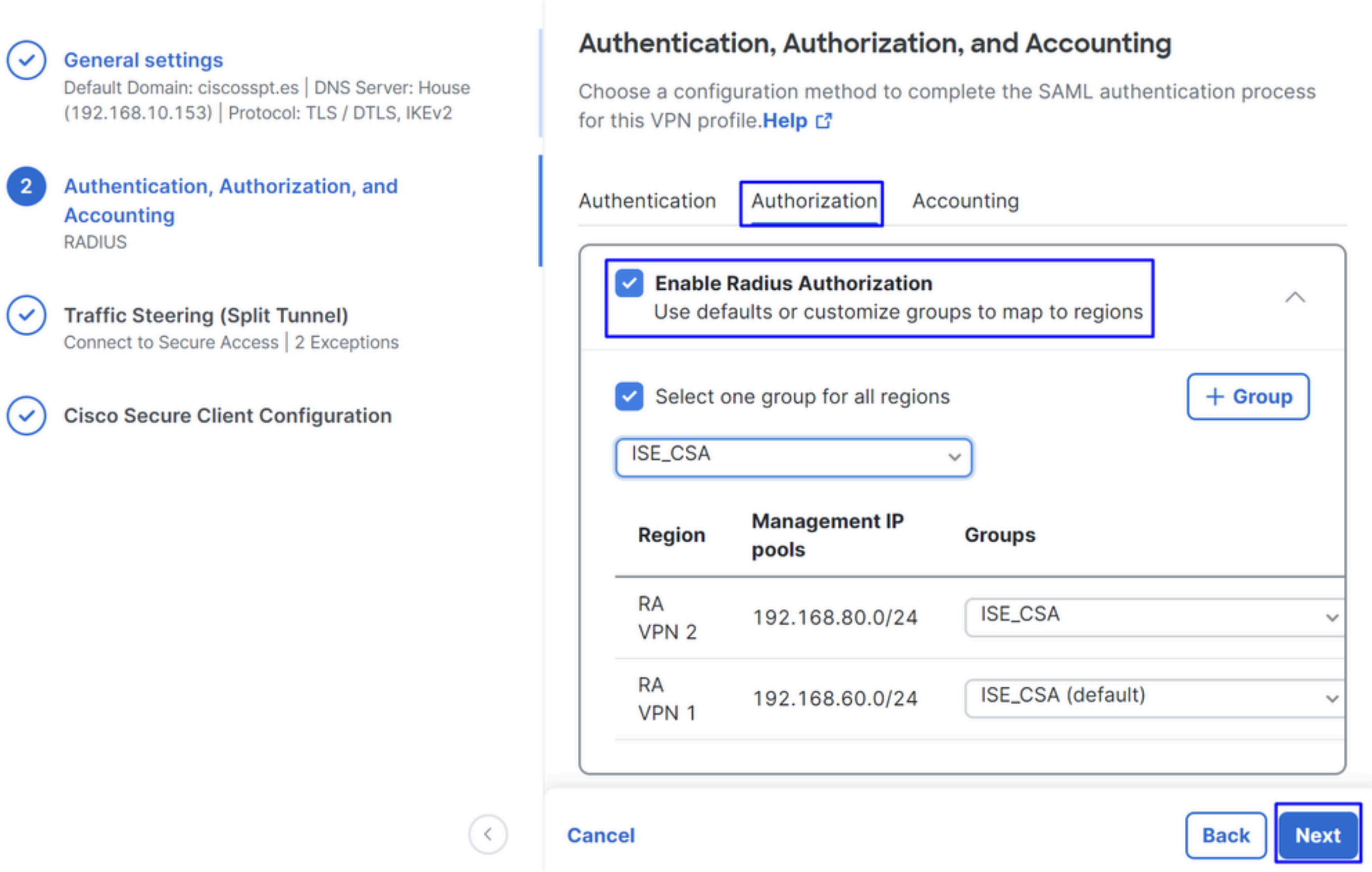
✓ File 'ISE - SAML - IDP Metadata.xml' uploaded.

○ Manual Configuration

Proceed with the Authorization.

Note: Once you configure the authentication with SAML, you will authorize it through ISE, which means the radius packet sent by Secure Access will only contain the username. The password field does not exist here.

Authorization



General settings
Default Domain: ciscosspt.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
Cancel
Back
Next

☑ Enable Radius Authorization
Use defaults or customize groups to map to regions

☑ Select one group for all regions

+ Group

ISE_CSA

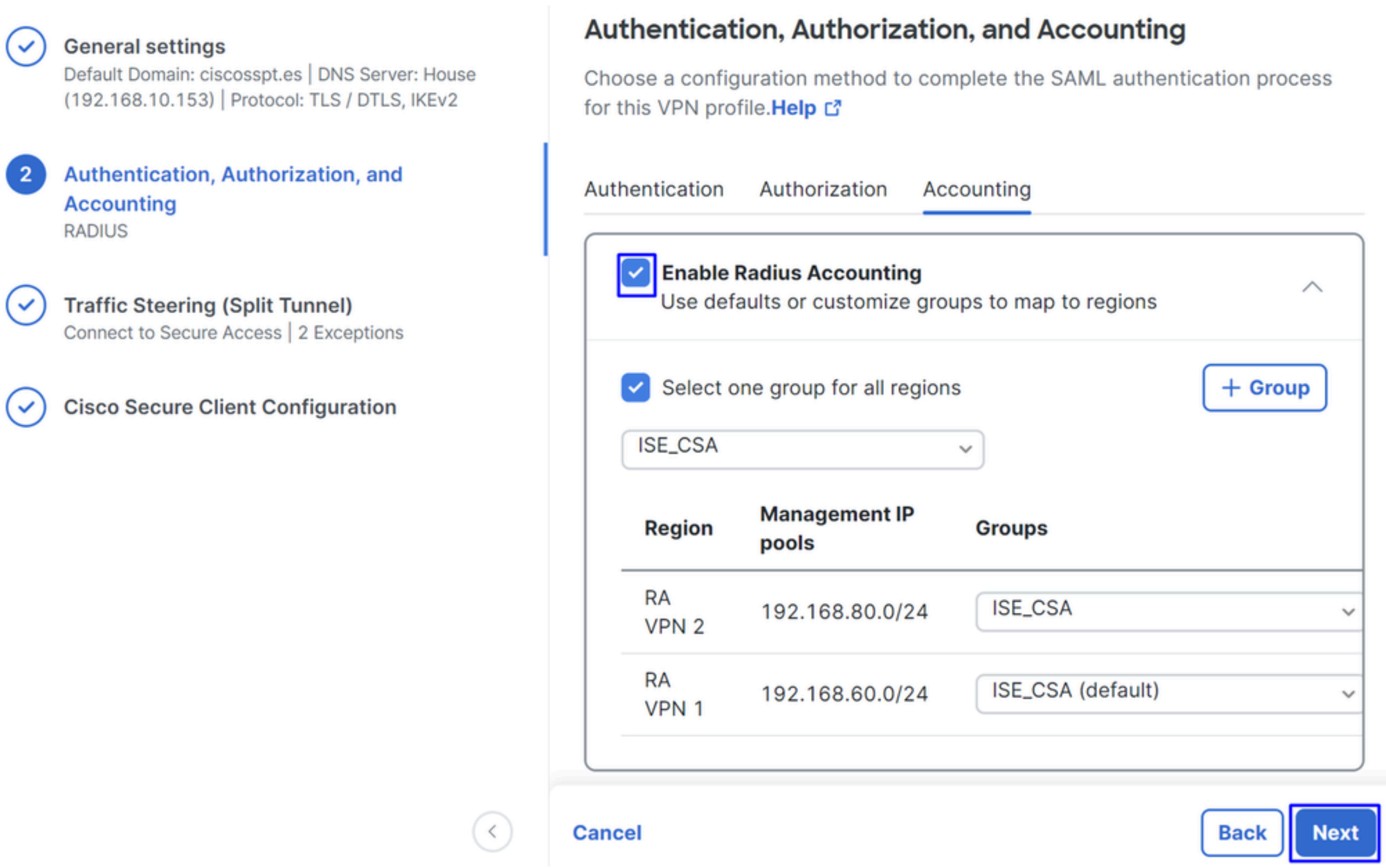
Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

- **Authorization**
  - **Enable Radius Authorization**: Mark the checkbox to enable the radius Authorization
  - **Select one group for all regions**: Mark the checkbox to use one specific radius server for all the Remote Access - Virtual Private Network (RA-VPN) Pools, or define it for every pool separately
- Click **Next**

After you configure all the **Authorization** part, please proceed with the **Accounting**.

Note: If you do not enable **Radio Authorization**, posture cannot work.

Accounting



✓ General settings
Default Domain: ciscosspt.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

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

☑ Select one group for all regions

ISE_CSA

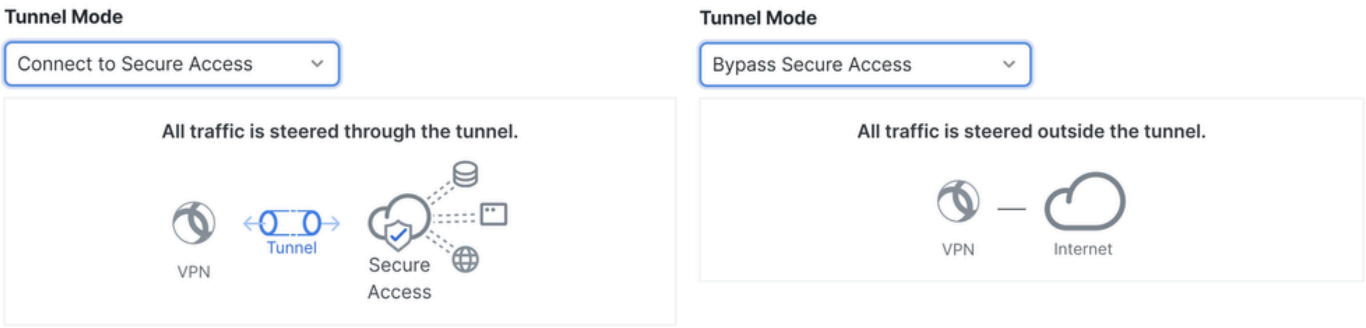
Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

- **Accounting**
  - **Map Authorization groups to regions**: Choose the regions and choose your **Radius Groups**
- Click **Next**

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

Traffic Steering

Under traffic steering, you need to configure the type of communication through Secure Access.



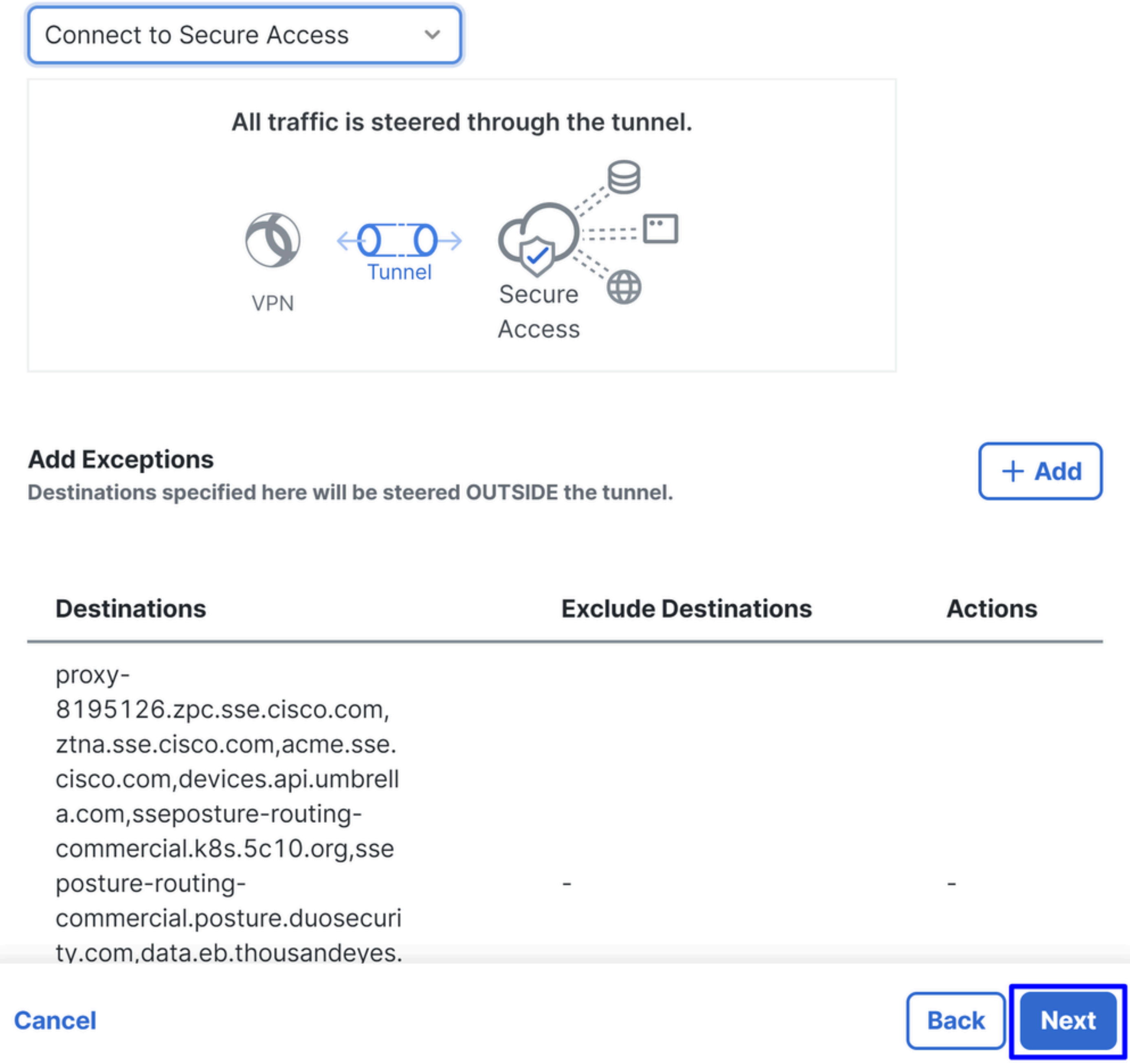
Tunnel Mode
Connect to Secure Access

All traffic is steered through the tunnel.

Tunnel Mode
Bypass Secure Access

All traffic is steered outside the tunnel.

- If you choose **Connect to Secure Access**, all your internet traffic routes through **Secure Access**



Connect to Secure Access

All traffic is steered through the tunnel.

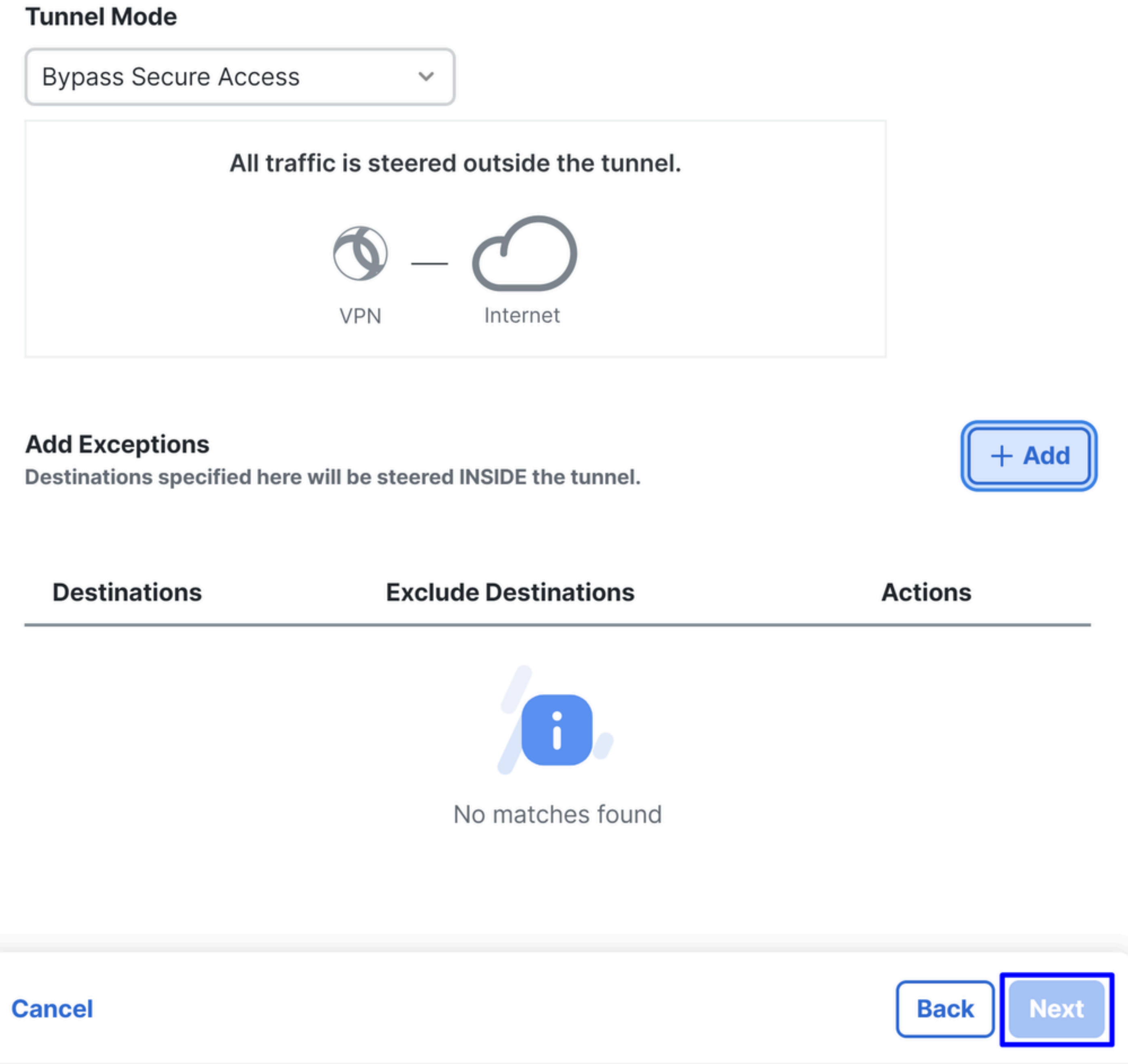
Add Exceptions

Destinations specified here will be steered OUTSIDE the tunnel.

Destinations	Exclude Destinations	Actions
proxy-8195126.zpc.sse.cisco.com, ztna.sse.cisco.com,acme.sse.cisco.com,devices.api.umbrella.com,sseposture-routing-commercial.k8s.5c10.org,sseposture-routing-commercial.posture.duosecurity.com,data.eb.thousandeyes.	-	-

If you want to add exclusions for internet domains or IPs, please Click on the **+ Add** button, then click **Next.**

- If you decide to **Bypass Secure Access**, all your internet traffic passes through your internet provider, not throughSecure Access (No Internet Protection)



Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.

Add Exceptions

Destinations specified here will be steered INSIDE the tunnel.

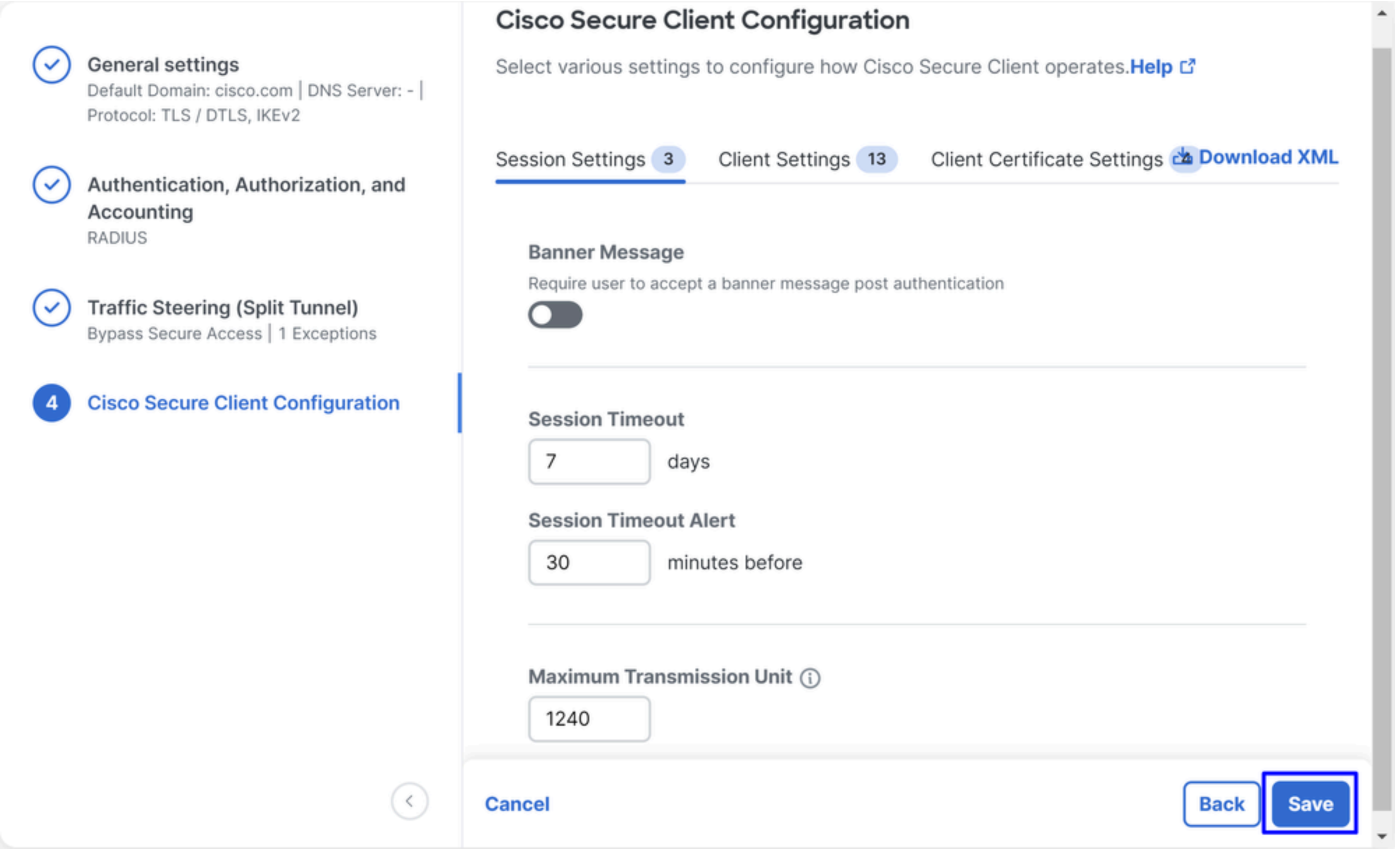
Destinations	Exclude Destinations	Actions

No matches found

Note: Please add **enroll.cisco.com** for ISE posture when you choose **Bypass Secure Access.**

In this step, you select all the private network resources that you want to access through the VPN. To do so, click **+ Add**, then click **Next** when you have added all the resources.

Cisco Secure Client Configuration



General settings
Default Domain: cisco.com | DNS Server: - | Protocol: TLS / DTLS, IKEv2

Authentication, Authorization, and Accounting
RADIUS

Traffic Steering (Split Tunnel)
Bypass Secure Access | 1 Exceptions

4 Cisco Secure Client Configuration

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates.Help

Session Settings 3 | Client Settings 13 | Client Certificate Settings | Download XML

Banner Message
Require user to accept a banner message post authentication

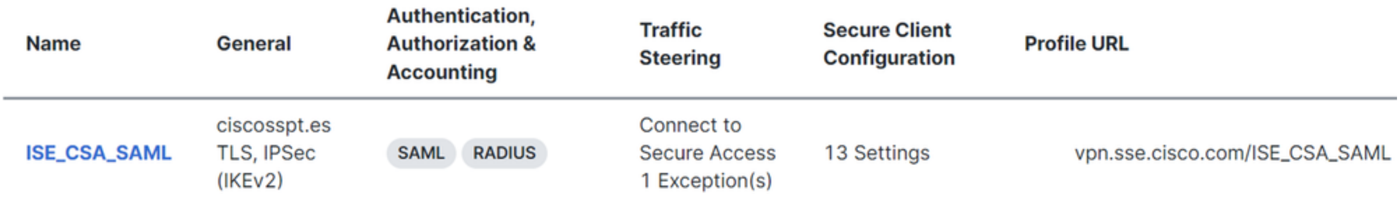
Session Timeout
7 days

Session Timeout Alert
30 minutes before

Maximum Transmission Unit
1240

Cancel | Back | Save

In this step, you can maintain everything as default and click **Save**, but if you want to customize your configuration more, please check Cisco Secure Client Administrator Guide.



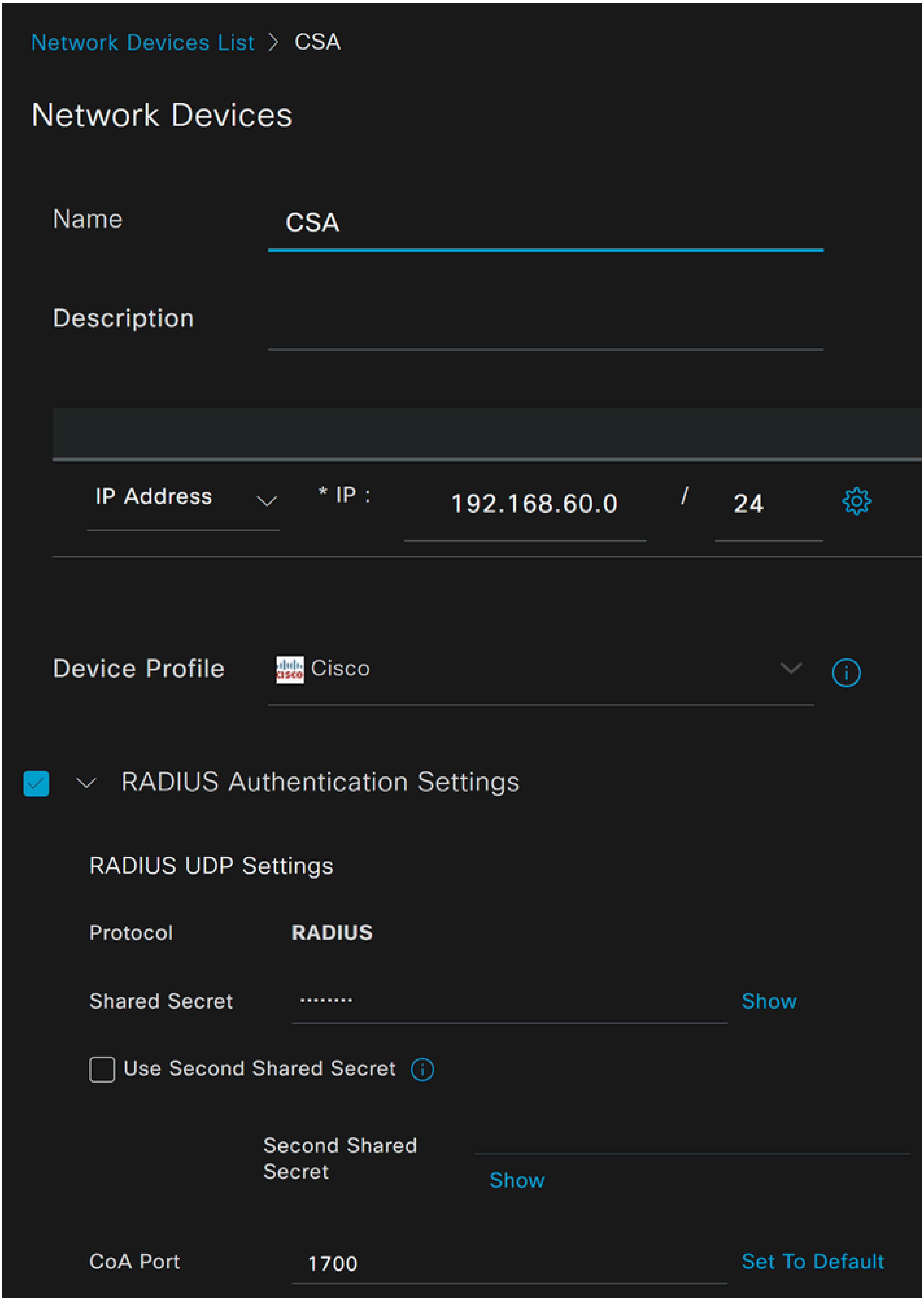
Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscosspt.es TLS, IPSec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

ISE Configurations

Configure Network Devices List

To configure the authentication through Cisco ISE, you need to configure the permitted devices that can make queries to your Cisco ISE:

- Navigate to **Administration > Network Devices**
- Click on **+ 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

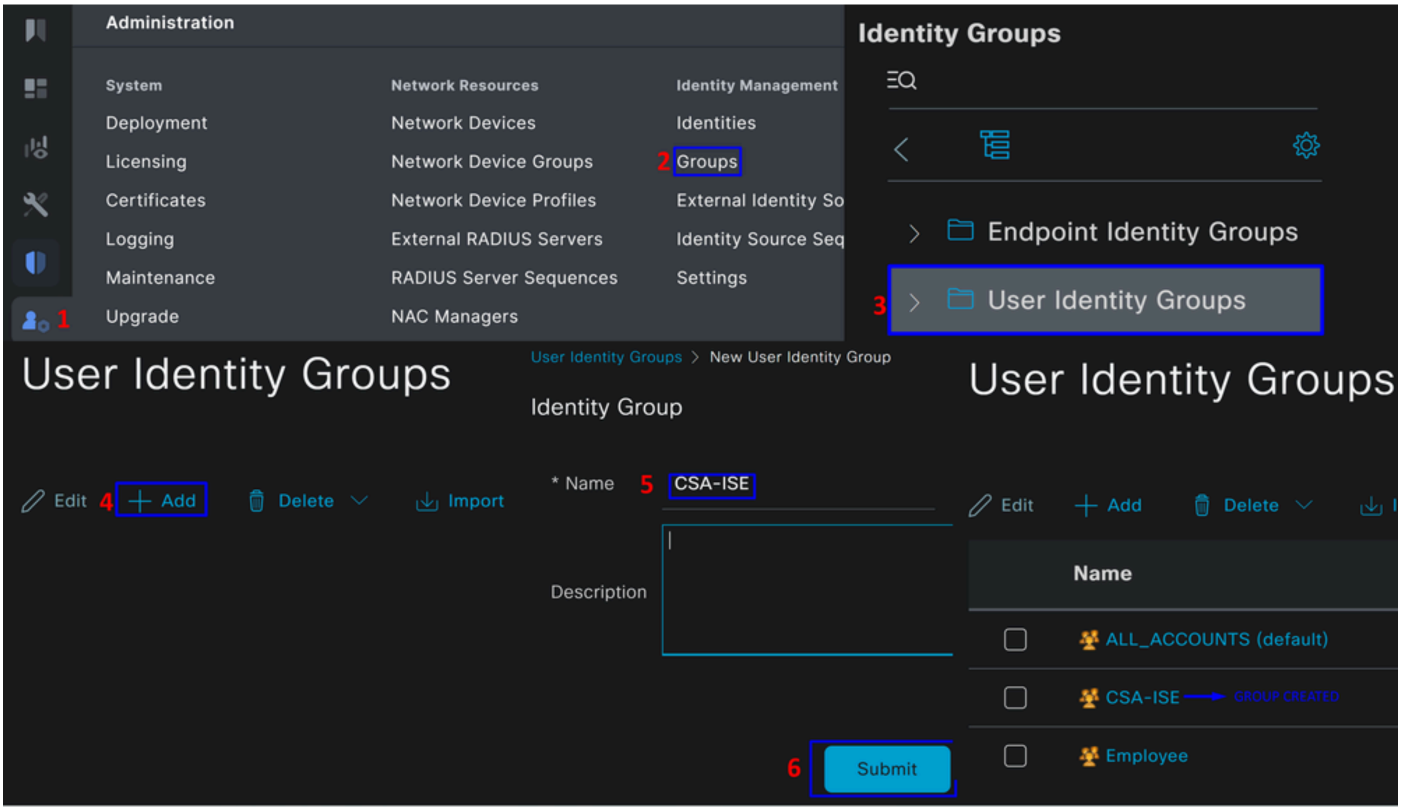
- **Name**: Use a name to Identify Secure Access
- **IP Address**: Configure the Management Interface of the step, IP Pool Region
- **Device Profile**: Choose Cisco
  - **Radius Authentication Settings**
    - Shared Secret: Configure the same shared secret configured on the step, Secret Key
    - **CoA Port**: Let it as default; 1700 is also used in Secure Access

After that click **Save**, to verify if the integration works properly, proceed to create a local user for integration verification.

Configure a Group

To configure a group for use with local users, proceed with these steps:

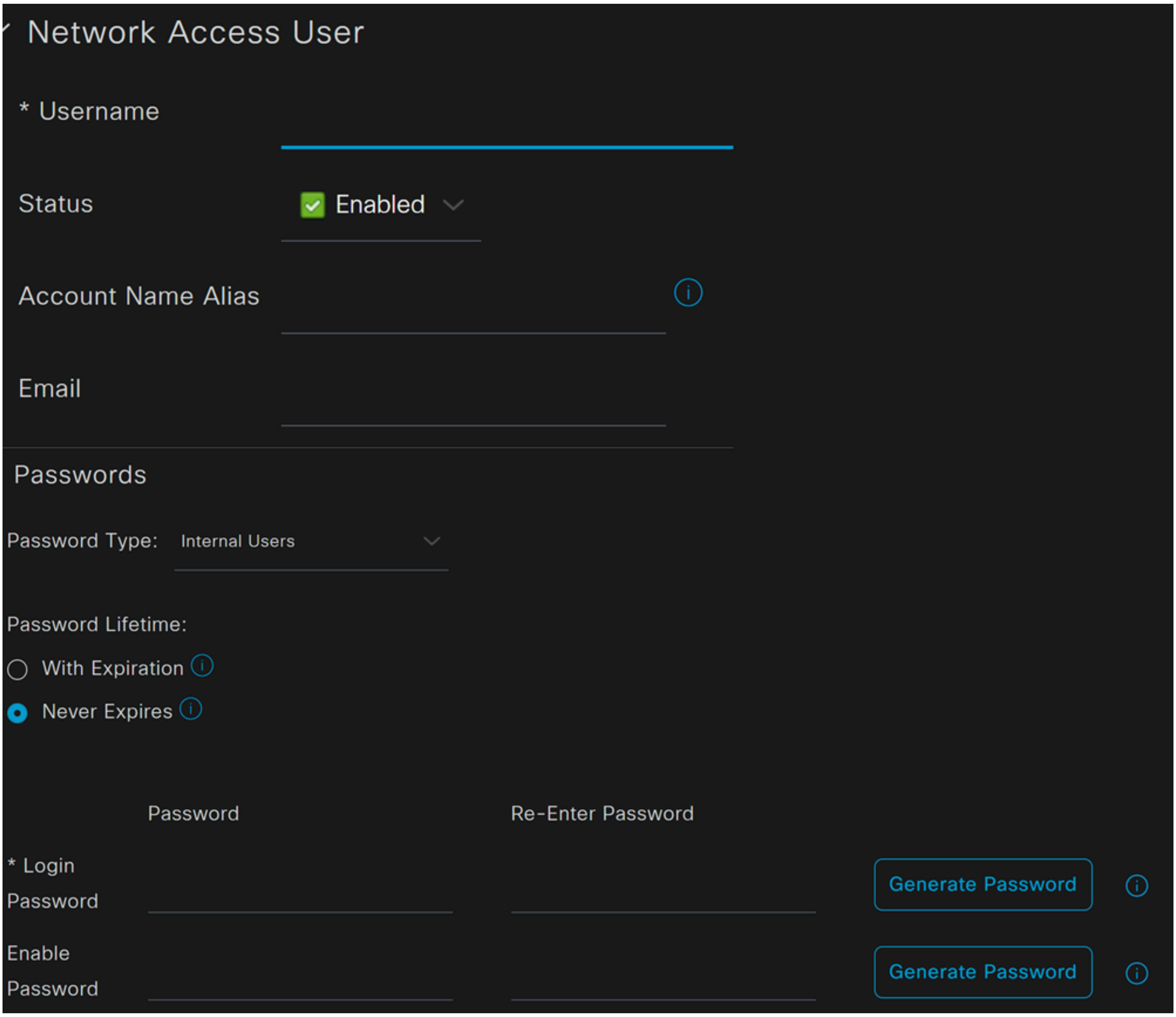
- Click in **Administration** > **Groups**
- Click **User Identity Groups**
- Click + Add
- Create a Namefor the Group and click **Submit**



Configure Local User

To configure a local user to verify your integration:

- Navigate to **Administration** > **Identities**
- Click on **Add +**



Network Access User

* Username

Status: ☑ Enabled

Account Name Alias

Email

Passwords

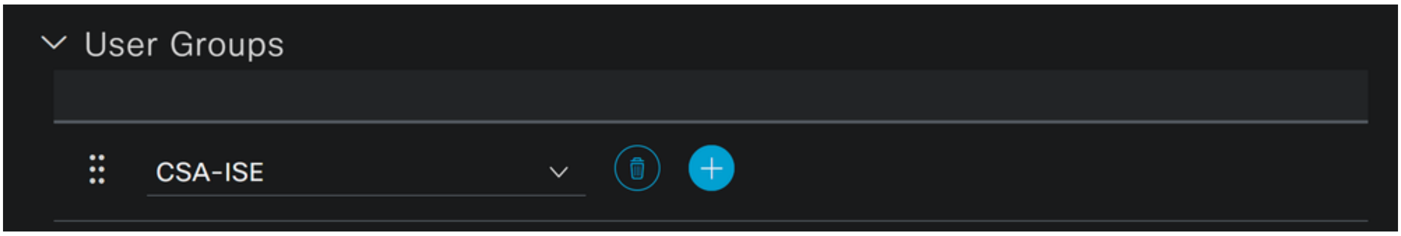
Password Type: Internal Users

Password Lifetime:

○ With Expiration

● Never Expires

	Password	Re-Enter Password	
* Login Password			Generate Password
Enable Password			Generate Password



User Groups

CSA-ISE

- **Username**: Configure the username with a known UPN provisioning in Secure Access; this is based on the step, Prerequisites
- **Status**: Active
- **Password Lifetime**: You can configure it **With Expiration** or Never Expires, depending on you
- **Login Password**: Create a password for the user
- **User Groups**: Choose the group created on the step, Configure a Group

Note: The authentication-based on UPN is set to change in upcoming versions of Secure Access.

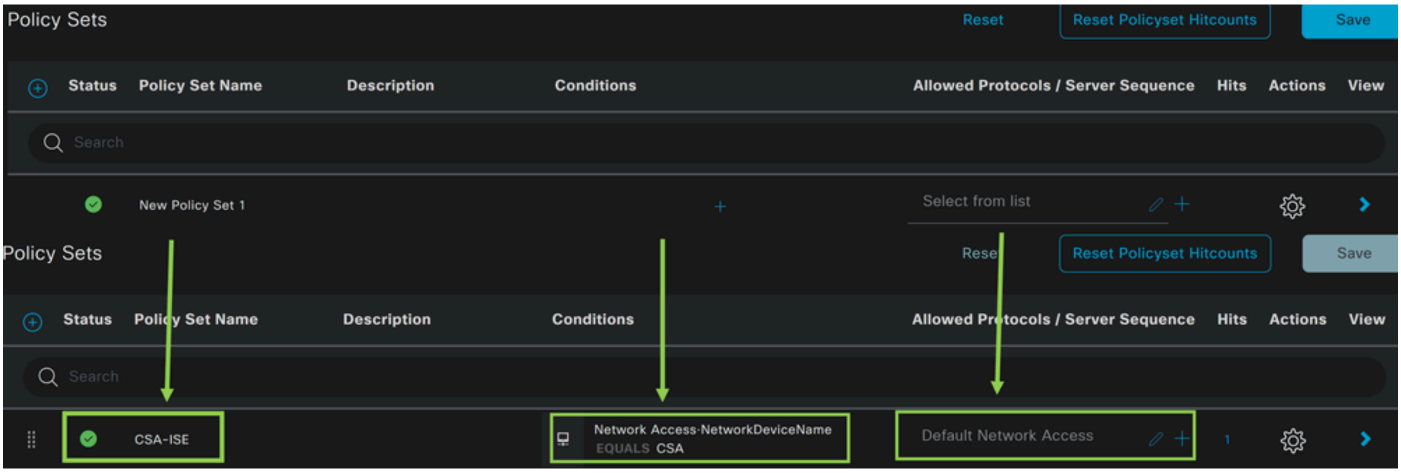
After that, you can **Save** the configuration and continue with the step, **Configure Policy Set**.

Configure Policy Set

Under the policy set, configure the action that ISE takes during authentication and authorization. This scenario demonstrates the use case for configuring a simple policy to provide user access. First, ISE verifies the origin of the RADIUS authentications and checks if the identities exist in the ISE user database to provide access

To configure that policy, navigate to your Cisco ISE Dashboard:

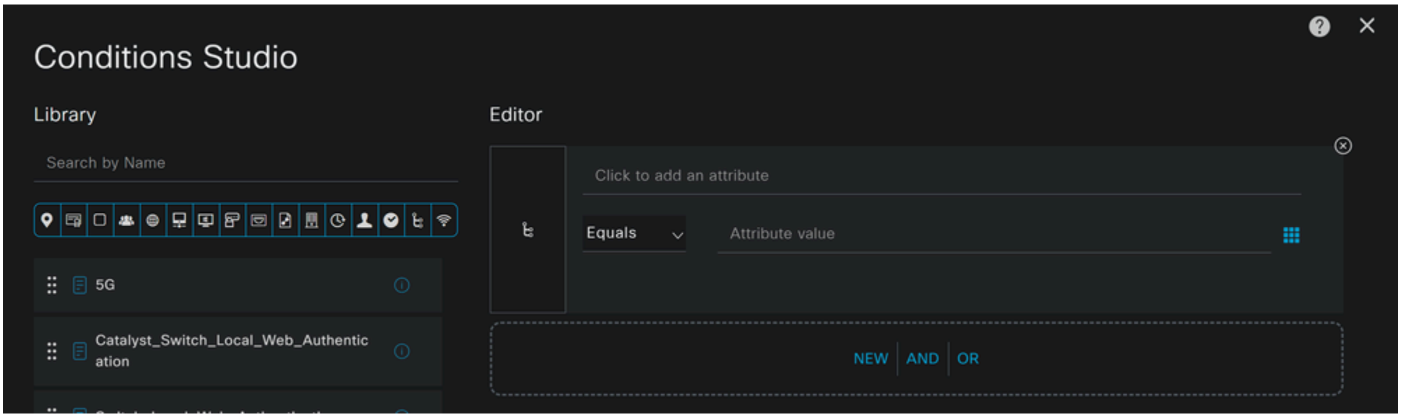
- Click on Policy > Policy Sets
- Click on + to add a new policy set



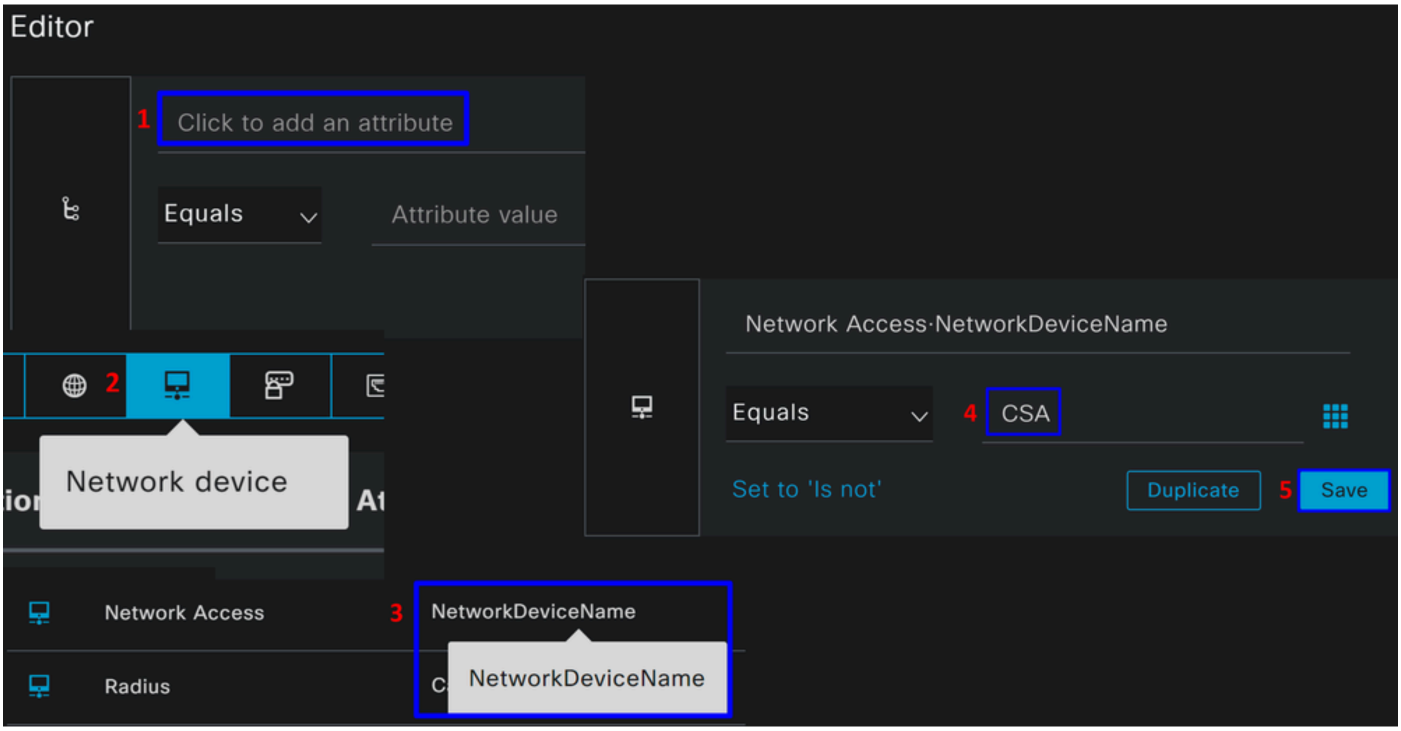
In this case, create a new policy set instead of working under the default one. Next, configure the Authentication and Authorization based on that policy set. The configured policy permits access to the network device defined in the step Configure Network Devices List to verify these authentications come from CSA Network Device List then get into the policy as **Conditions**. And finally, the allowed Protocols, as **Default Network Access.**

To create the **condition** that matches the policy set, proceed with the next instructions:

- Click on +
- Under **Condition Studio**, the information available includes:

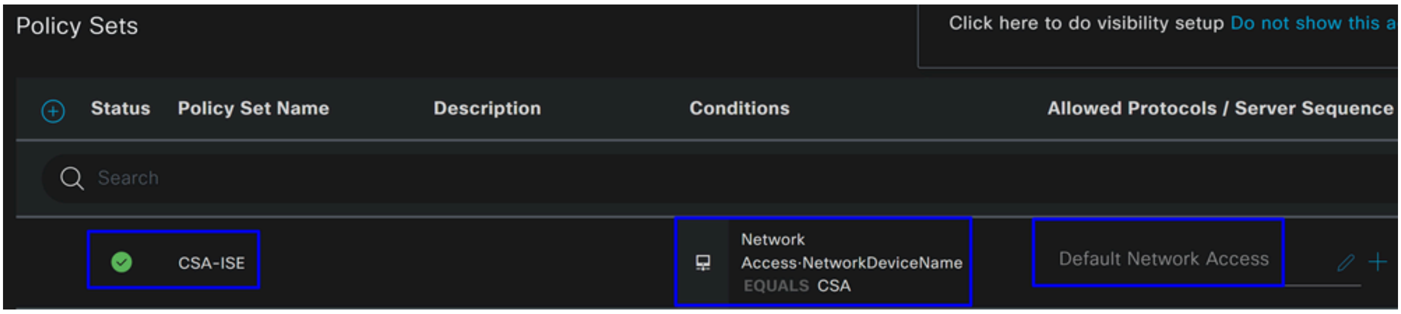


1. To create the Conditions, click on Click to add an attribute
2. Click on the **Network Device** button
3. Under the options behind, click on **Network Access - Network Device Name** option
4. Under the Equals option, write the name of the **Network Device** under the step, Configure Network Devices List
5. Click **Save**



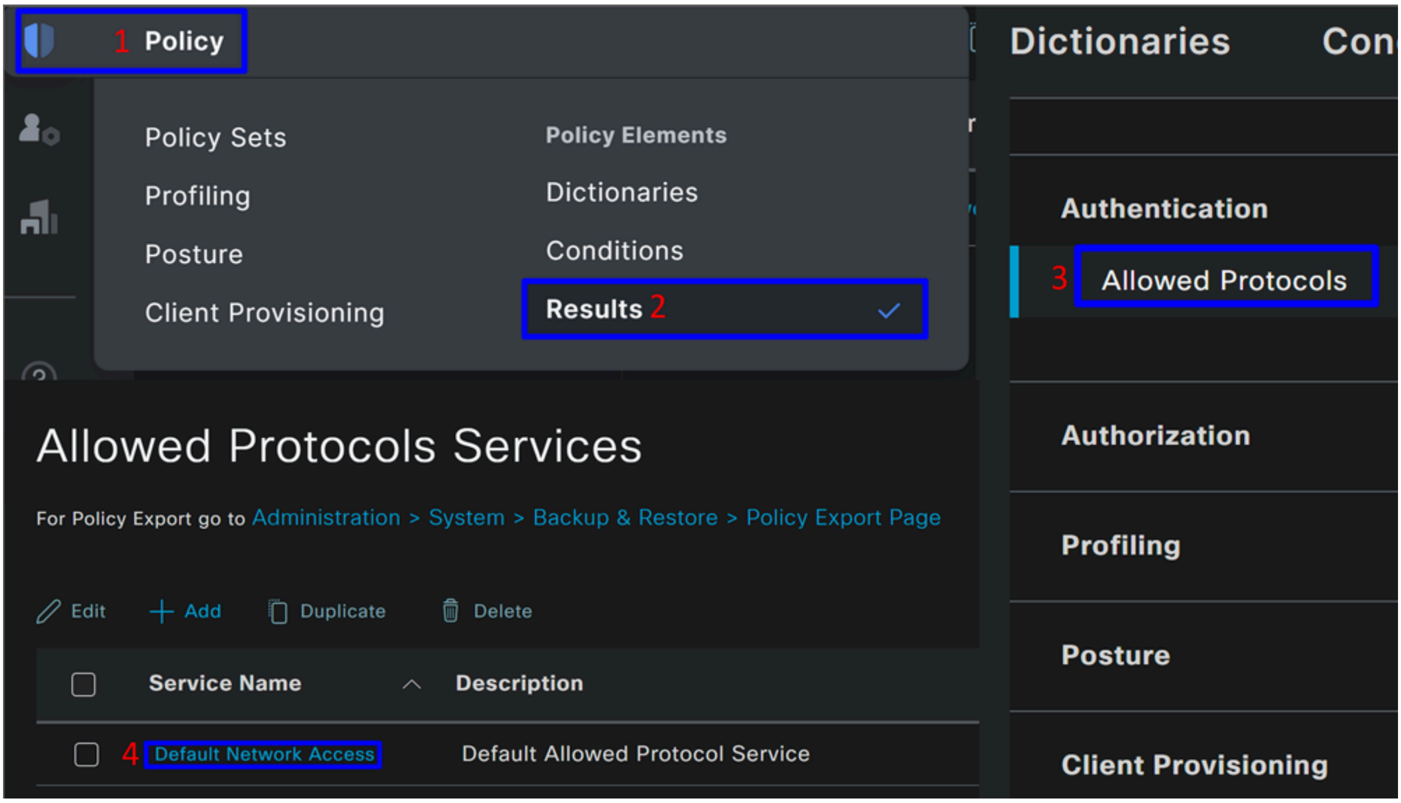
This policy only approves the request from the source CSA to continue the **Authentication** and **Authorization** setup under the policy set **CSA-ISE**, and also verifies the protocols permitted based on the **Default Network Access** for the allowed protocols.

The result of the Policy defined must be:



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	CSA-ISE		Network Access·NetworkDeviceName EQUALS CSA	Default Network Access

- To verify the **Default Network Access Protocols** allowed, proceed with the next instructions:
    - Click onPolicy > Results
    - Click on **Allowed Protocols**
    - Click on **Default Network Access**



Allowed Protocols Services

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

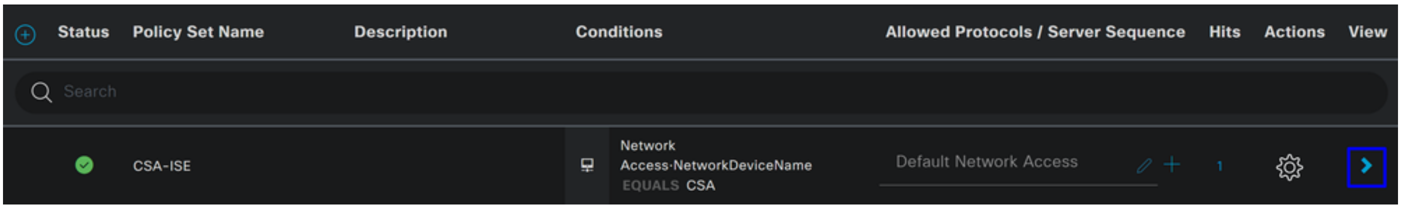
□	Service Name	Description
□	Default Network Access	Default Allowed Protocol Service

- Then, you see all the protocols permitted on **Default Network Access**

Configure Policy Set Authorization

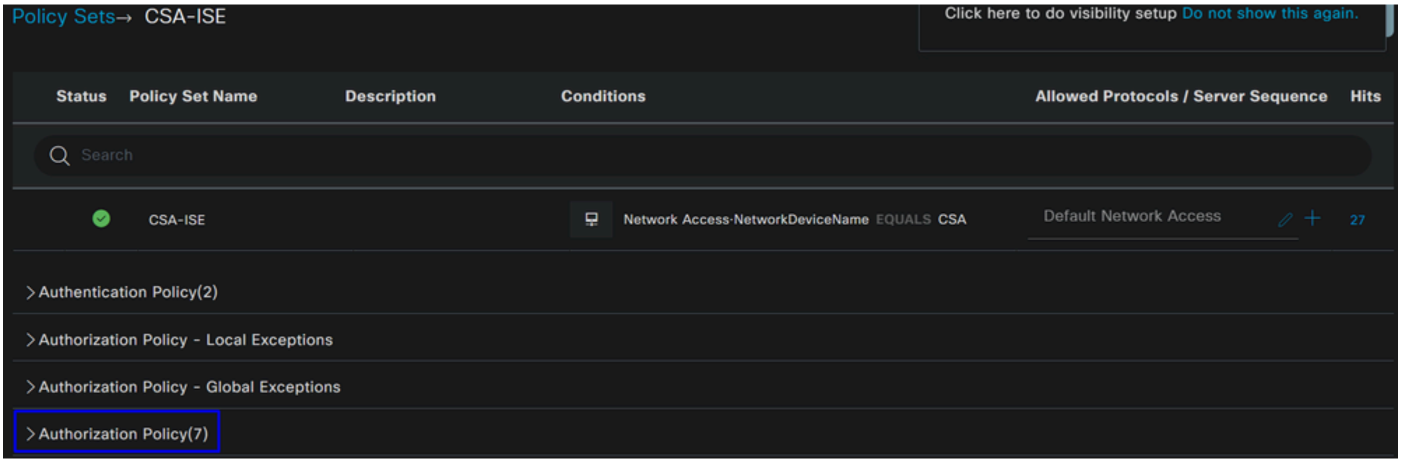
To create the **Authorization** Policy under the **Policy Set**, proceed with the next steps:

- Click on >



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSA-ISE		Network Access·NetworkDeviceName EQUALS CSA	Default Network Access	1	⚙	>

- After that, you see the**Authorization** policies displayed:



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

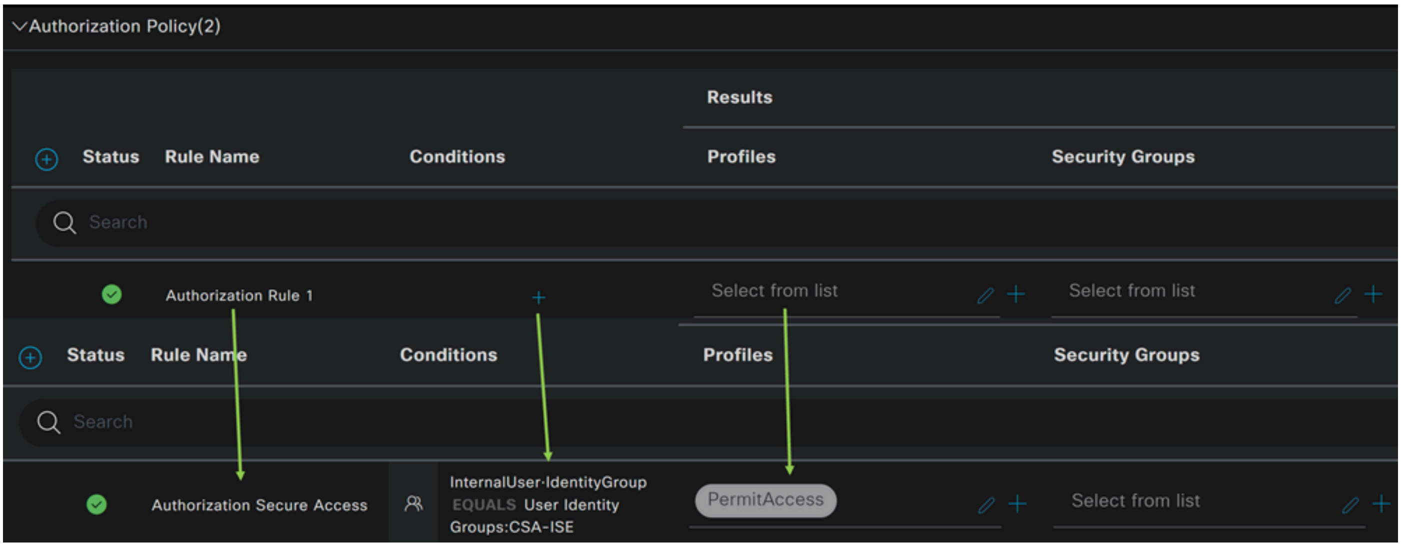
> Authorization Policy - Global Exceptions

> Authorization Policy(7)

The policy is the same one defined under the step Configure Policy Set.

Authorization Policy

You can configure the authorization policy in many ways. In this case, authorize only the users in the group defined in the step Configure a Group.See the next example to configure your authorization policy:

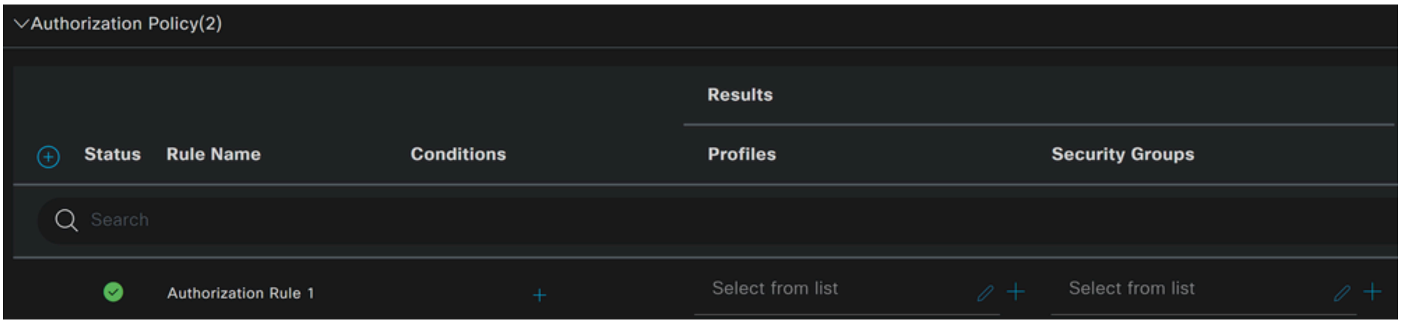


Authorization Policy(2)

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

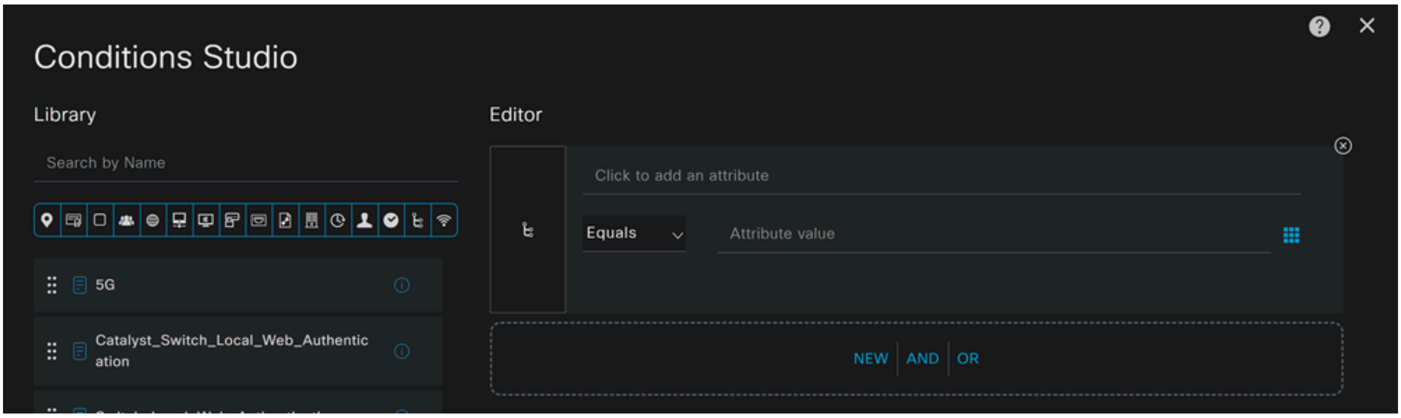
- Click on **Authorization Policy**
- Click on + to define the policy for authorization like this:



Authorization Policy(2)

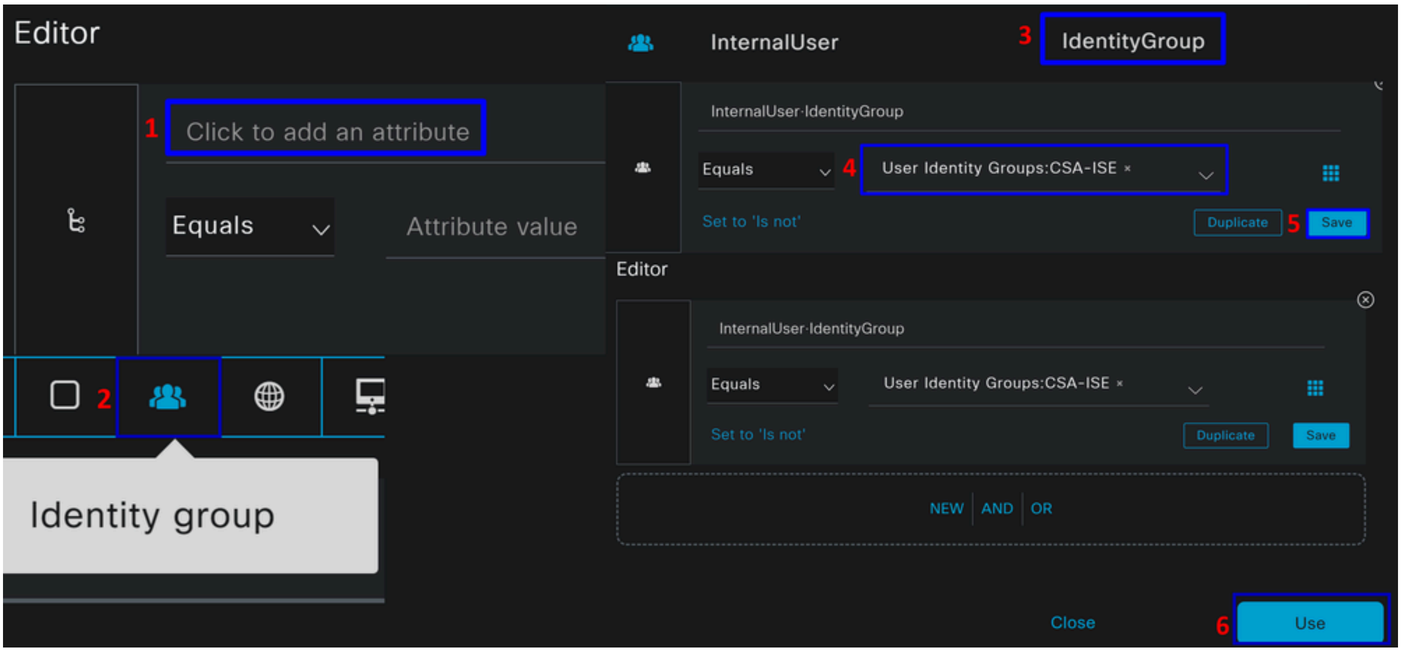
Status	Rule Name	Conditions	Profiles	Security Groups
✓	Authorization Rule 1	+	Select from list	Select from list

- For the next step, change the Rule Name, Conditions and Profiles
- When setting the **Name** configure a name to easily identify the authorization policy
- To configure the **Condition**, click on the +
- Under **Condition Studio**, you find the information:



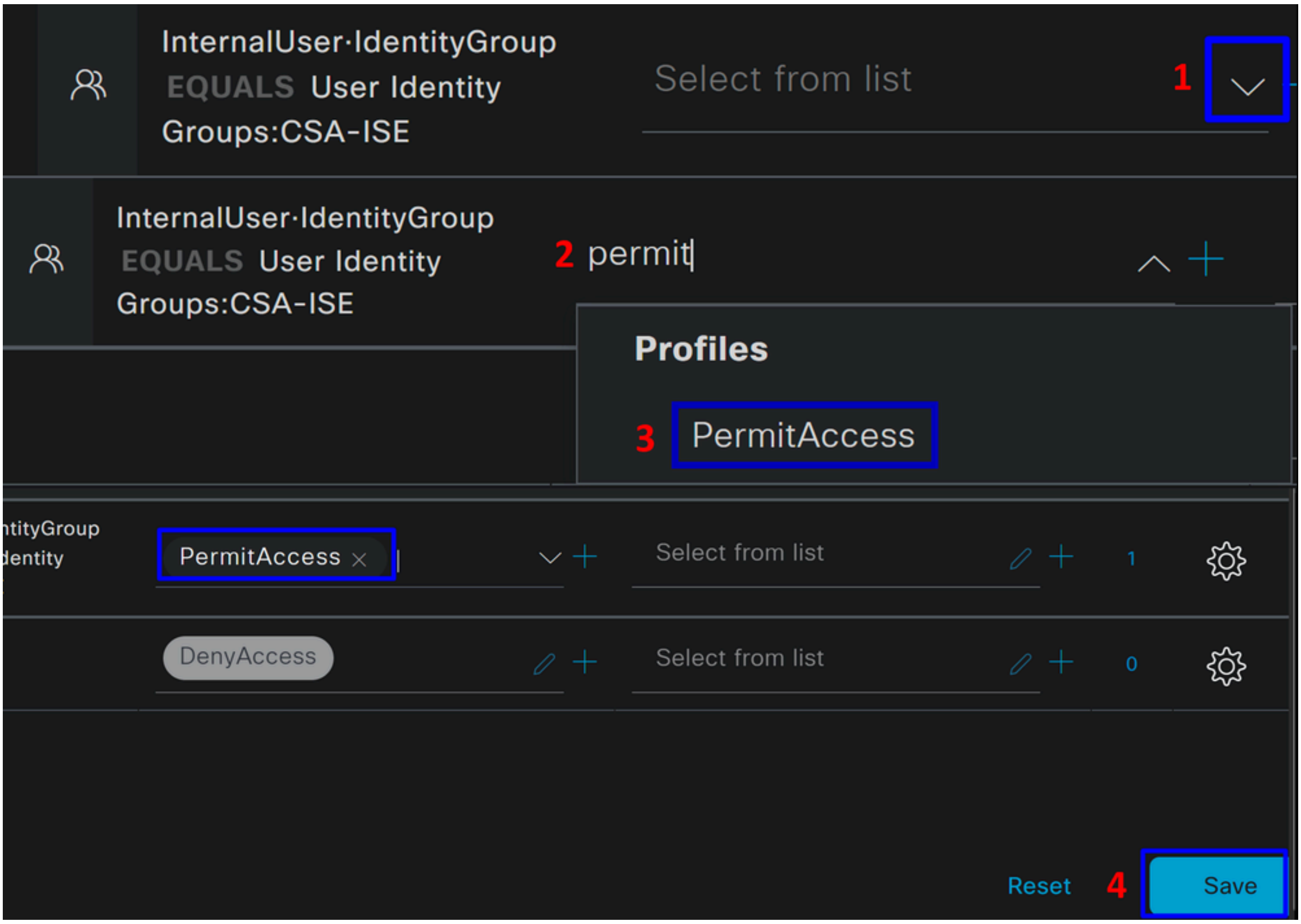
1. To create the Conditions, click on Click to add an attribute
2. Click on the **Identity Group** button
3. Under the options behind, click on **Internal User - IdentityGroup** option
4. Under the **Equals** option, use the dropdown to find the **Group** approved for authentication in the

step, Configure a Group
5. Click **Save**
6. Click **Use**



After that, you need to define the **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

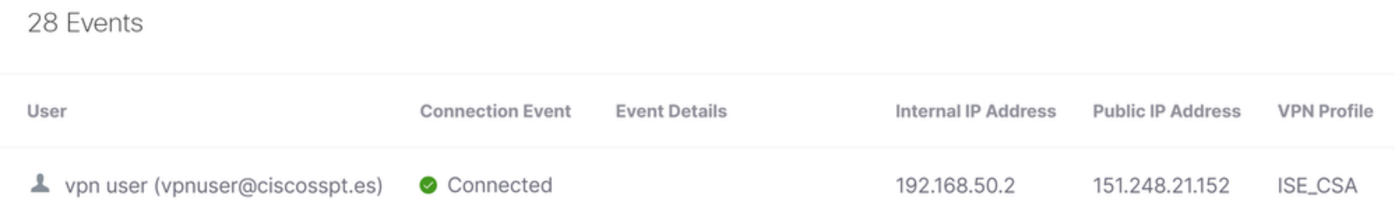
1. Under the **Authorization Policy**, click on the dropdown button on **Profiles**
2. Search for permit
3. Select **PermitAccess**
4. Click Save



After that, you have defined your **Authorization** policy. Authenticate to verify whether the user connects without a problem and whether you can see the logs on Secure Access and ISE.

To connect to the VPN, you can use the profile created on Secure Access and connect through Secure Client with the ISE profile.

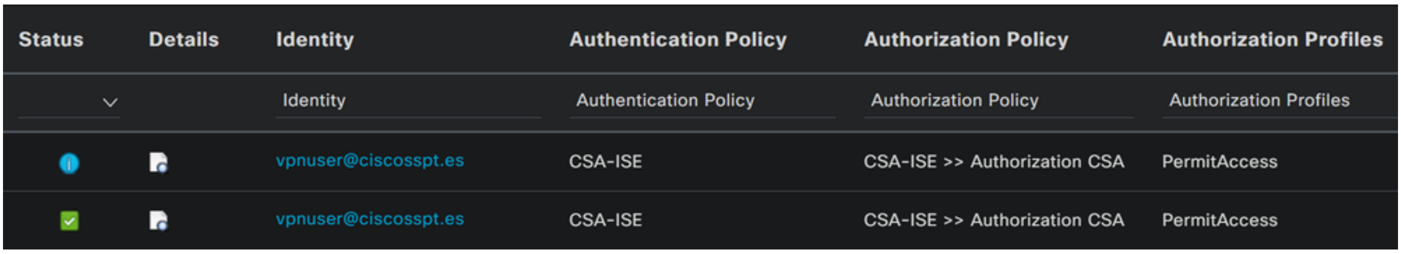
- **How is the log displayed in Secure Access when the authentication gets approved?**
  - Navigate to the [Secure Access Dashboard](https://dashboard.sse.cisco.com)
  - Click on **Monitor > Remote Access Log**



28 Events

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

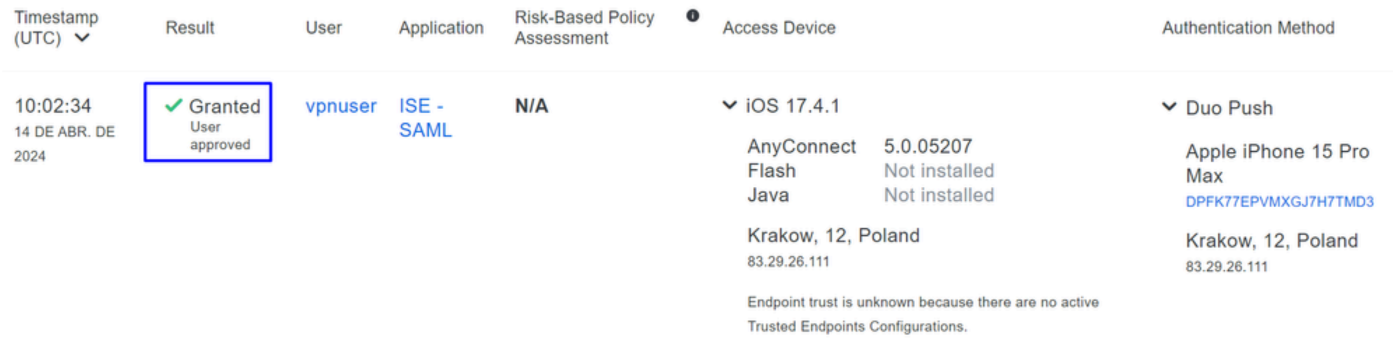
- **How is the log displayed in ISE when the authentication gets approved?**
  - Navigate to the **Cisco ISE Dashboard**
  - Click on **Operations > Live Logs**



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

How is the log displayed in Duo when the authentication gets approved?

- Navigate to the [Duo Admin Panel]()
- Click on **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

Configure Radius Local or Active Directory Users

Configure ISE Posture

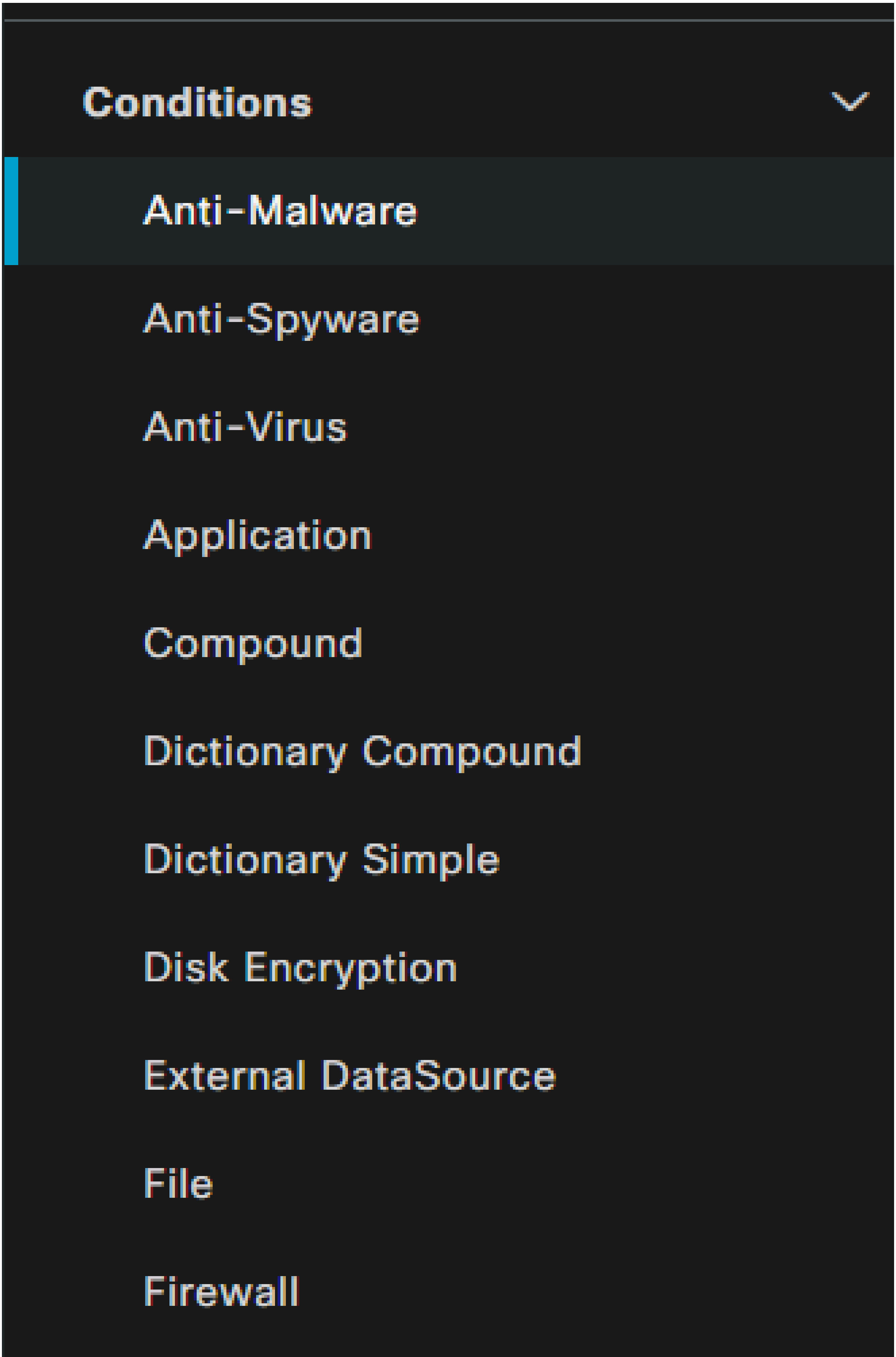
In this scenario, create the configuration to verify endpoint compliance before granting or denying access to internal resources.

To configure it, proceed to the next steps:

Configure Posture Conditions

- Navigate to your ISE Dashboard
- Click on **Work Center** > **Policy Elements** > **Conditions**
- Click on **Anti-Malware**

Note: There, you find many options to verify the posture of your devices and make the correct assessment based on your internal policies.



Conditions

Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

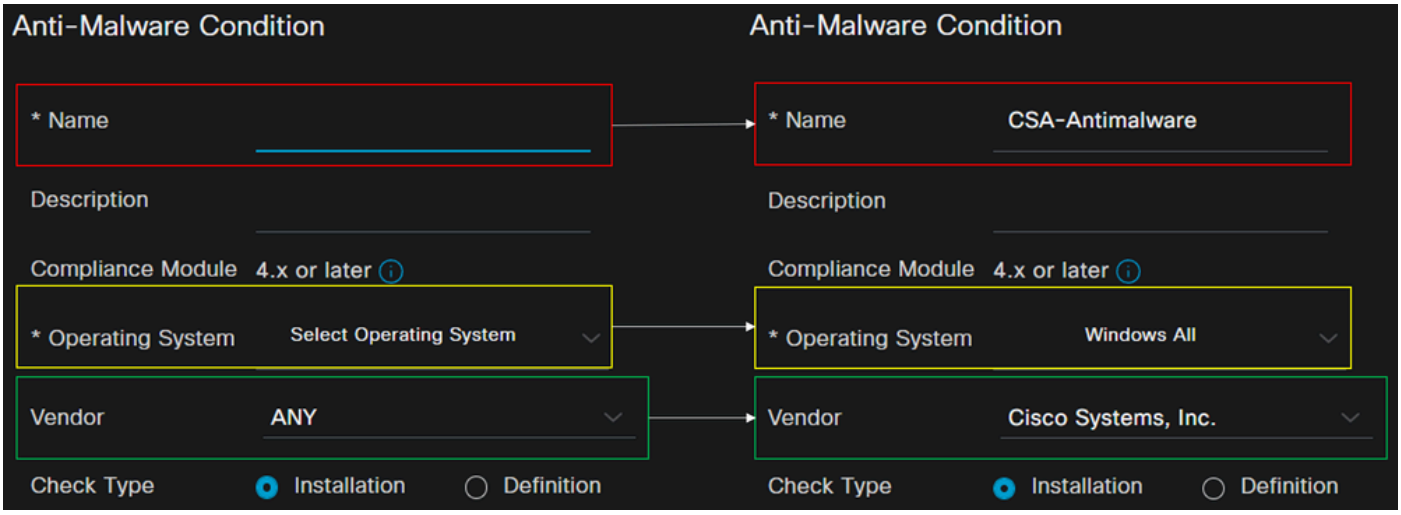
Disk Encryption

External DataSource

File

Firewall

to detect the antivirus installation on the system; you can also choose the operating system version if needed.



Anti-Malware Condition

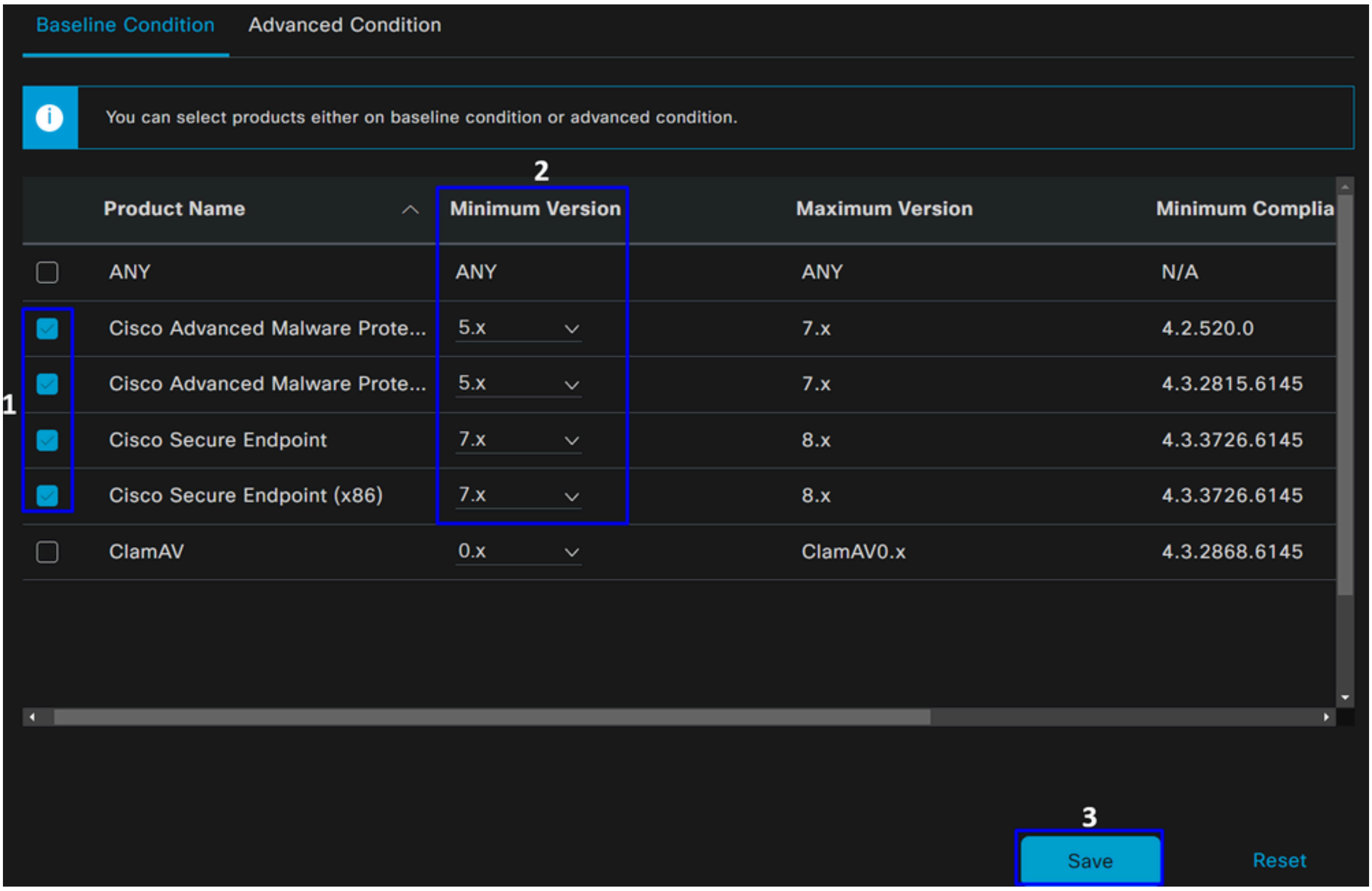
* Name
Description
Compliance Module 4.x or later
* Operating System: Select Operating System
Vendor: ANY
Check Type: ● Installation ○ Definition

Anti-Malware Condition

* Name: CSA-Antimalware
Description
Compliance Module 4.x or later
* Operating System: Windows All
Vendor: Cisco Systems, Inc.
Check Type: ● Installation ○ Definition

- **Name**: Use a name to recognize the anti-malware condition
- **Operating System**: Choose the operative system that you want to put under the condition
- **Vendor**: Choose a vendor or ANY
- **Check Type**: You can verify if the agent is installed or the definition version for that option.

- For **Products for Selected Vendor**, you configure what you want to verify about the antimalware on the device.



You can select products either on baseline condition or advanced condition.

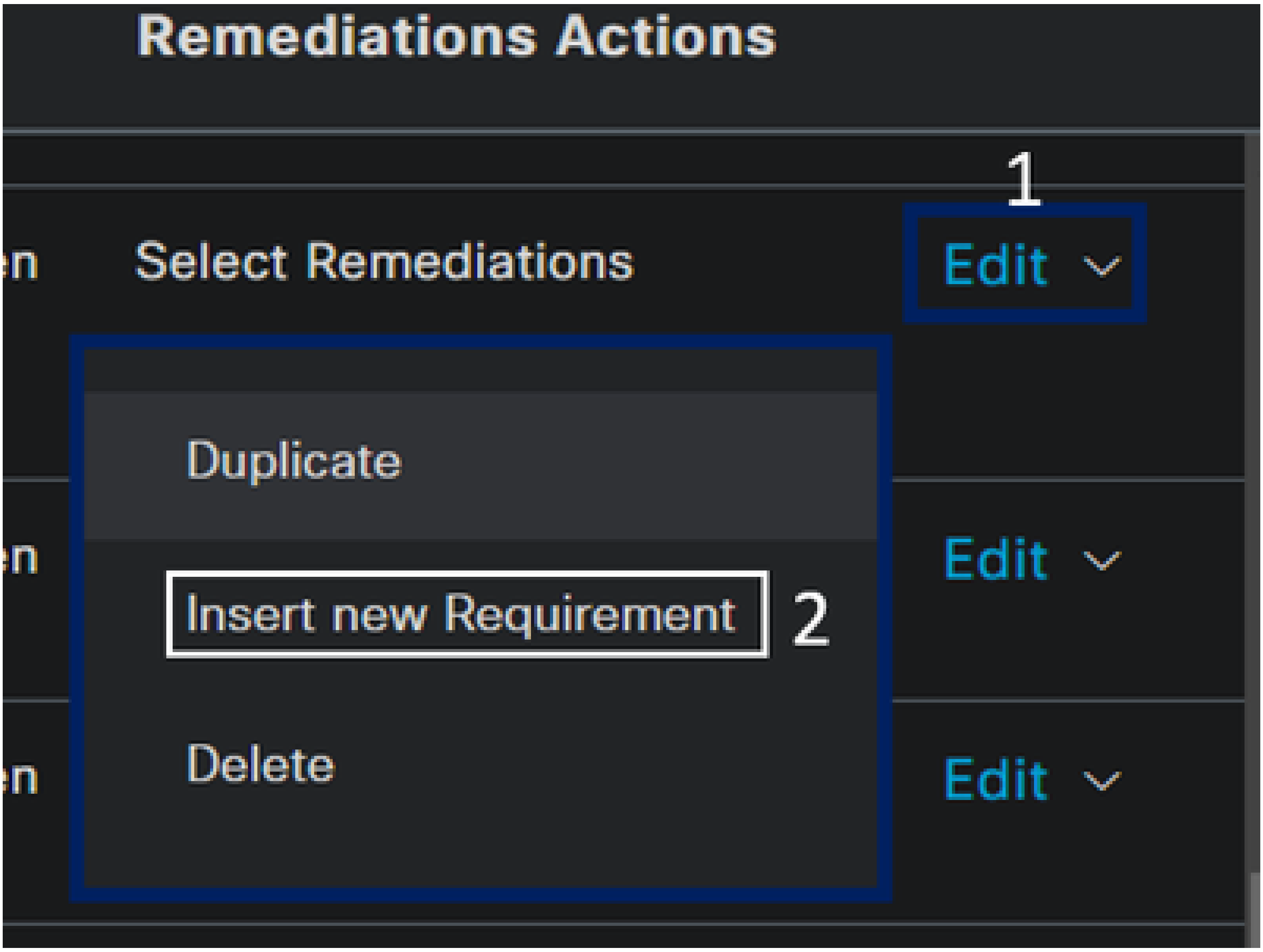
	Product Name	Minimum Version	Maximum Version	Minimum Complia
□	ANY	ANY	ANY	N/A
☑	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
☑	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
☑	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
☑	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
□	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

1. Mark the checkbox for the conditions that you wanted to evaluate
2. Configure the minimum version to verify
3. Click Save to continue with the next step

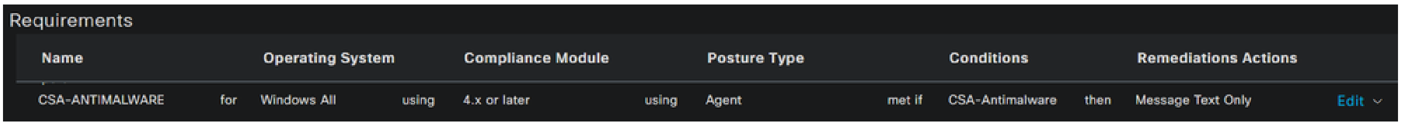
Once you configure it, you can proceed with the step, **Configure Posture Requirements**.

Configure Posture Requirements

- Navigate to your ISE Dashboard
- Click on **Work Center** > **Policy Elements** > **Requeriments**
- Click on **Edit** of any one of the requirements and click **Insert new Requirement**



- Under the new requirement, configure the next parameters:



Requirements

Name		Operating System		Compliance Module		Posture Type		Conditions		Remediations Actions	
CSA-ANTIMALWARE	for	Windows All	using	4.x or later	using	Agent	met if	CSA-Antimalware	then	Message Text Only	Edit ⌄

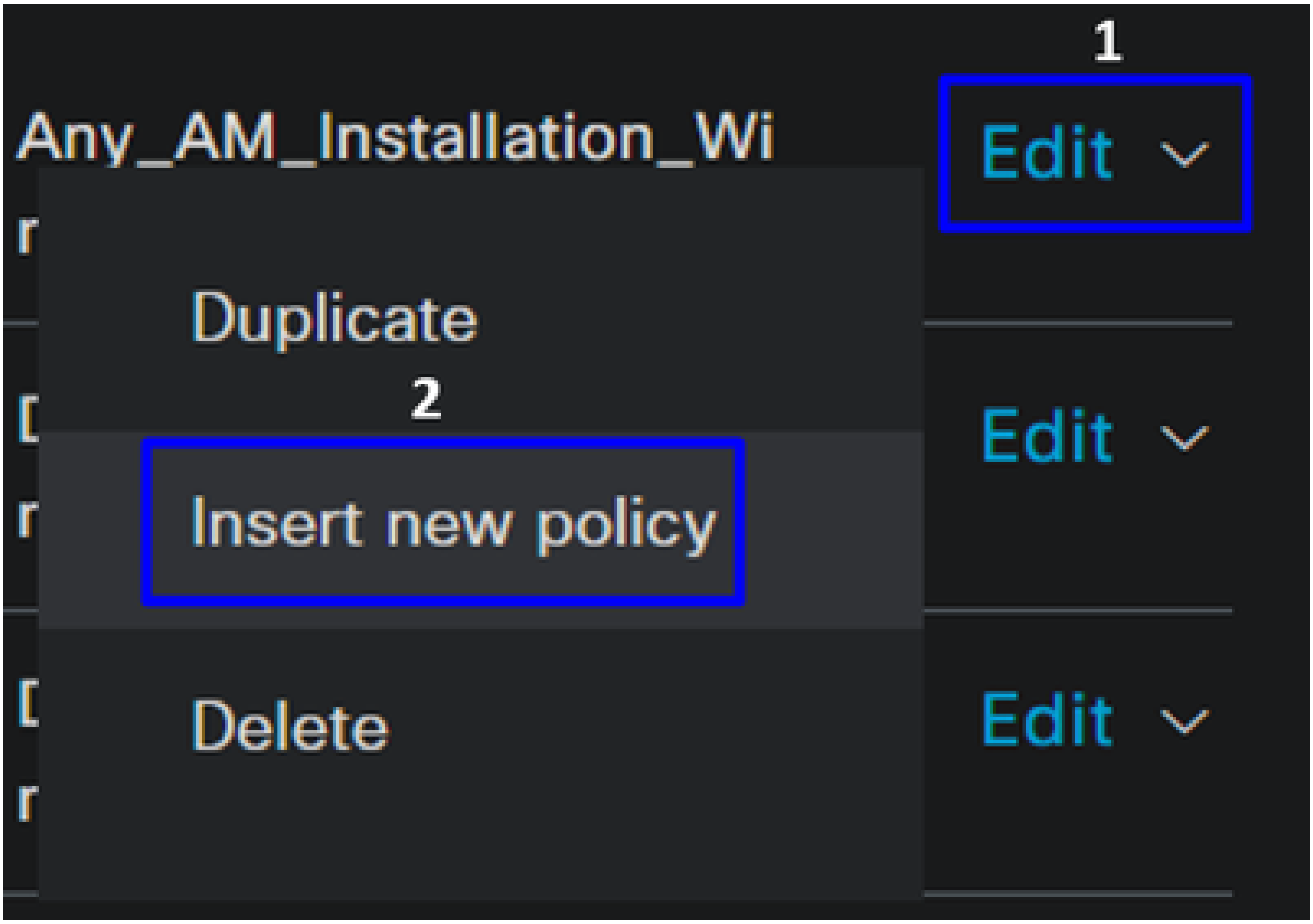
- **Name**: Configure a name to recognize the antimalware requirement
- **Operating System**: Choose the operating system that you choose under the condition step, Operating System
- **Compliance Module**: You need to make sure to select the same compliance module that you have under the condition step, Anti-Malware Condition
- **Posture Type**: Choose Agent
- **Conditions**: Choose the condition or conditions that you created under the step, Configure Posture Conditions
- **Remediations Actions**: Choose **Message Text Only** for this example, or if you have another remediation action, use it

- Click **Save**

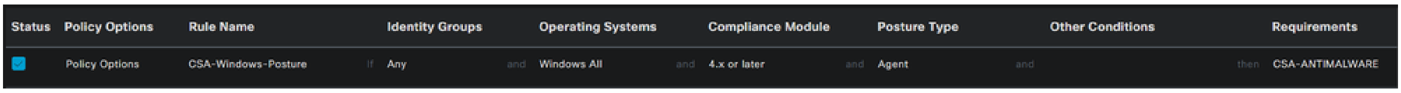
Once you configure it, you can proceed with the step, **Configure Posture Policy**

Configure Posture Policy

- Navigate to your ISE Dashboard
- Click on **Work Center** > **Posture Policy**
- Click on **Edit** of any one of the policies and click **Insert new Policy**



- Under the new policy, configure the next parameters:



Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements
☑	Policy Options	CSA-Windows-Posture	If	Any	and	Windows All	and	4.x or later	and	Agent	and		then	CSA-ANTIMALWARE

- **Status**: Mark the checkbox no enable the policy
- **Rule Name**: Configure a name to recognize the policy configured
- **Identity Groups**: Choose the identities that you want to evaluate
- **Operating Systems**: Choose the operating system based on the condition and requirement configured before
- **Compliance Module**: Choose the compliance module based on the condition and requirement configured before
- Posture Type: Choose Agent
- **Requeriments**: Choose the requirements configured on the step, Configure Posture Requirements
- Click **Save**

Configure Client Provisioning

To provide the users with the ISE module, configure the client provisioning to equip the machines with the ISE posture module. This enables you to verify the machines posture once the agent is installed. To continue with this process, here are the next steps:

Navigate to your ISE Dashboard.

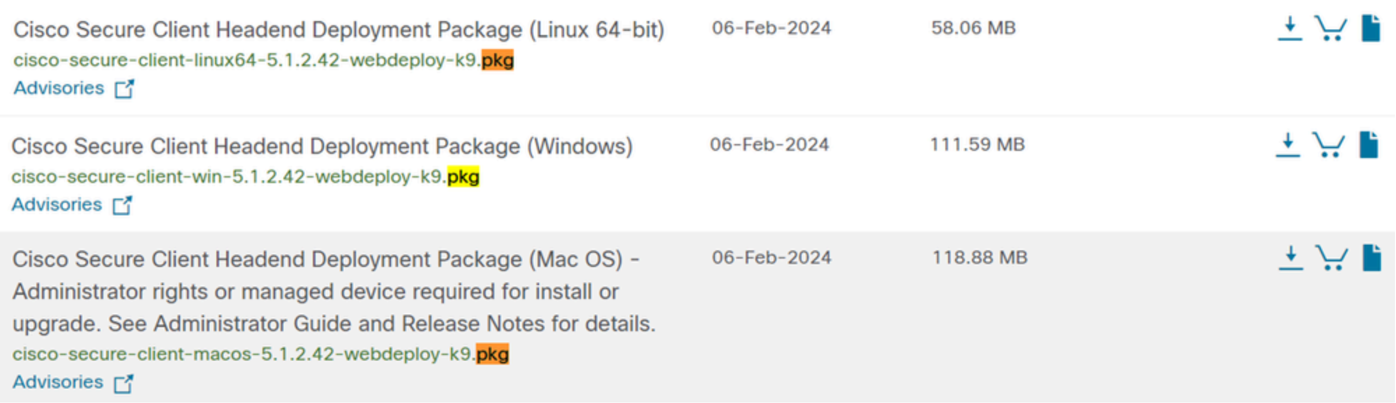
- Click on **Work Center > Client Provisioning**
- Choose **Resources**

There are three things that you need to configure under client provisioning:

Resources to configure	Description
1. **Agent Resources**	Secure Client Web Provisioning Package.
2. **Compliance Module**	Cisco ISE Compliance Module
3. **Agent Profile**	Control of the provisioning profile.
3. **Agent Configuration**	Define which modules are provisioned by setting up the provisioning portal, utilizing the Agent Profile and Agent Resources.

Step 1 Download and Upload Agent Resources

- To add a new agent resource, navigate to the Cisco Download Portal and download the web deploy package; the web deploy file must be .pkg format.

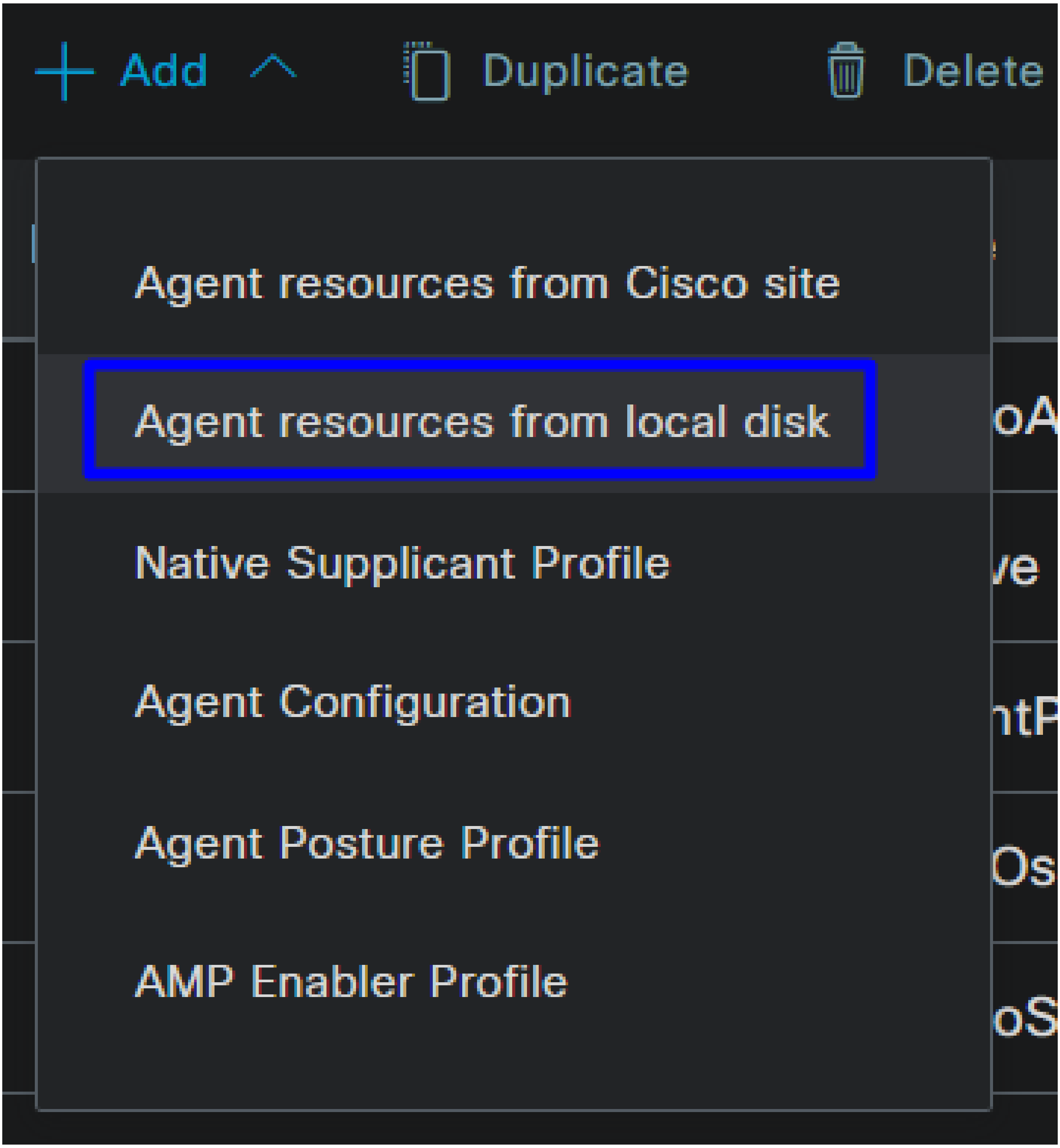


Cisco Secure Client Headend Deployment Package (Linux 64-bit) 06-Feb-2024 58.06 MB
cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg
Advisories

Cisco Secure Client Headend Deployment Package (Windows) 06-Feb-2024 111.59 MB
cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
Advisories

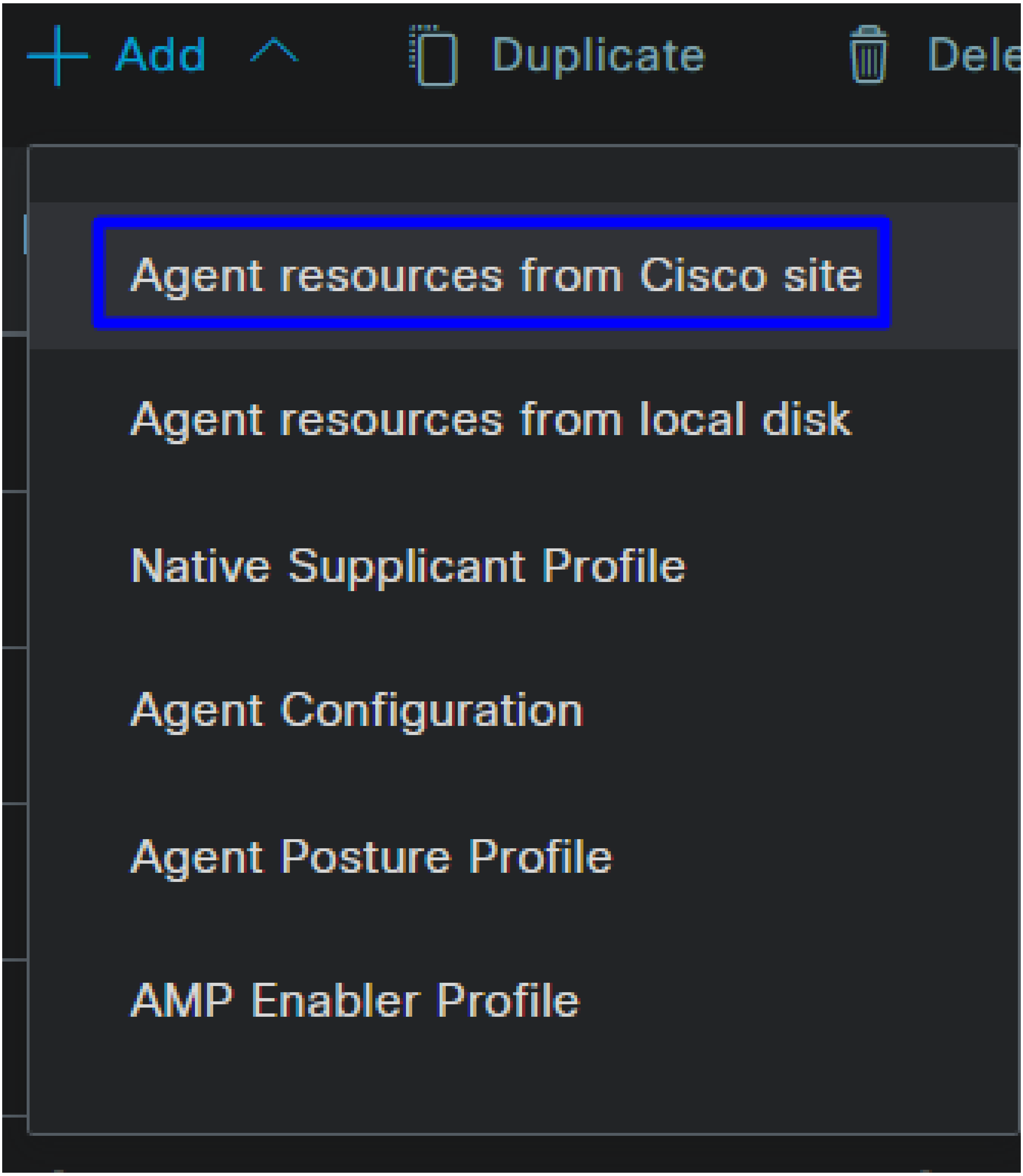
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. 06-Feb-2024 118.88 MB
cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg
Advisories

- Click on + Add > Agent resources from local disk and upload the packages


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

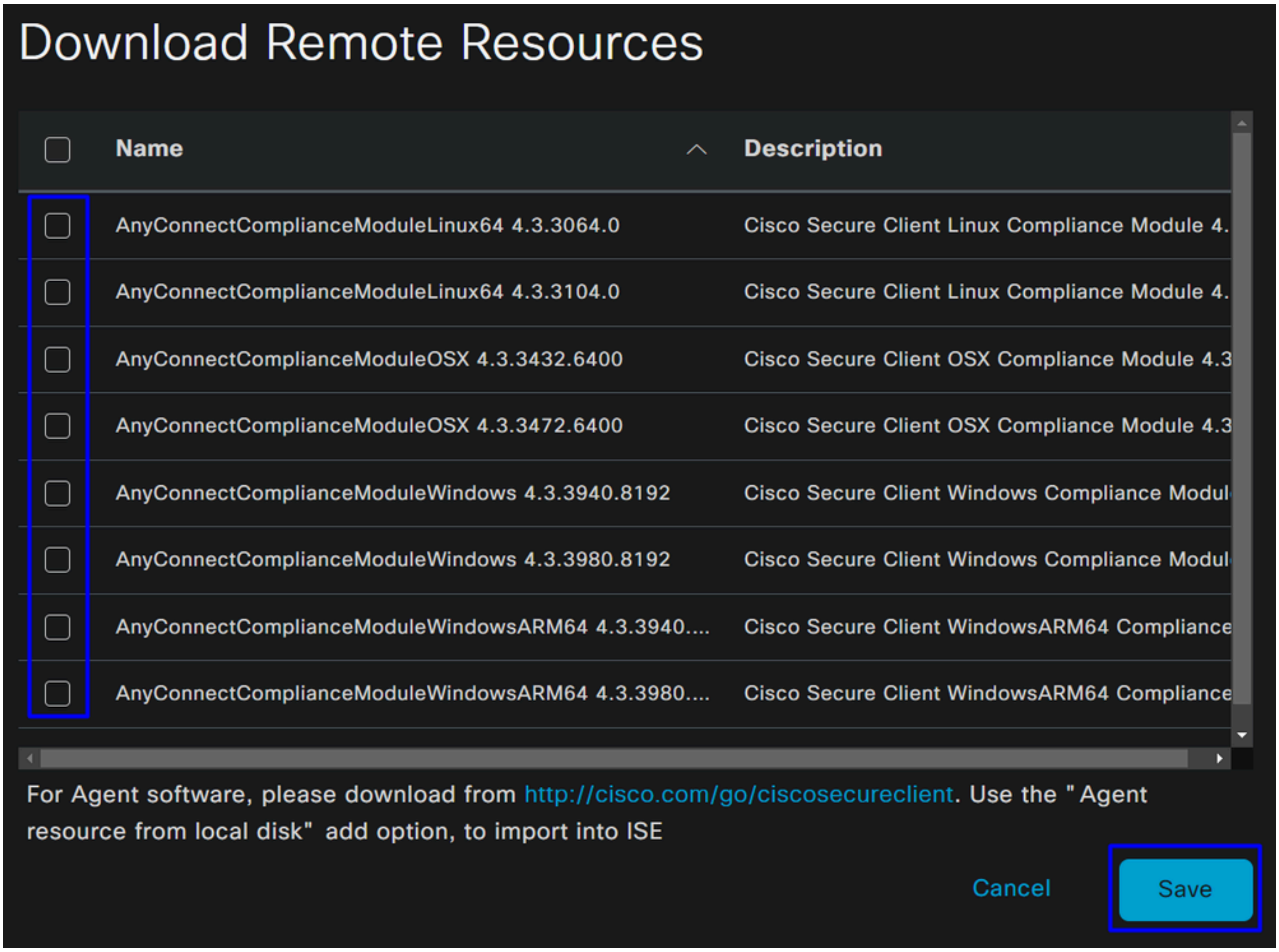
Step 2 Download the compliance module

- Click on + Add > Agent resources from Cisco Site



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

- Mark the checkbox for every compliance module needed and click **Save**



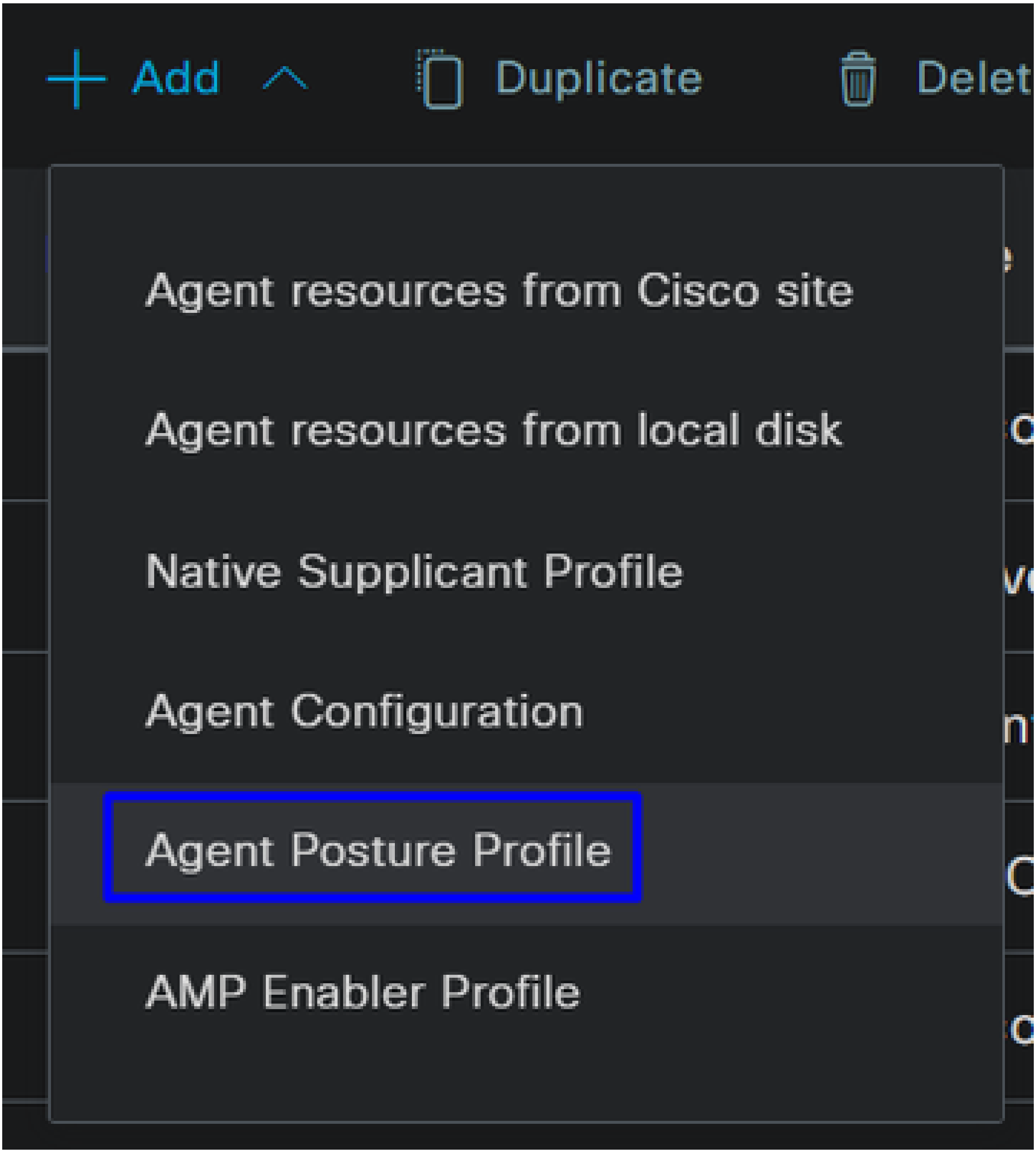
Download Remote Resources

□	Name	Description
□	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
□	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
□	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
□	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
□	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
□	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
□	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
□	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

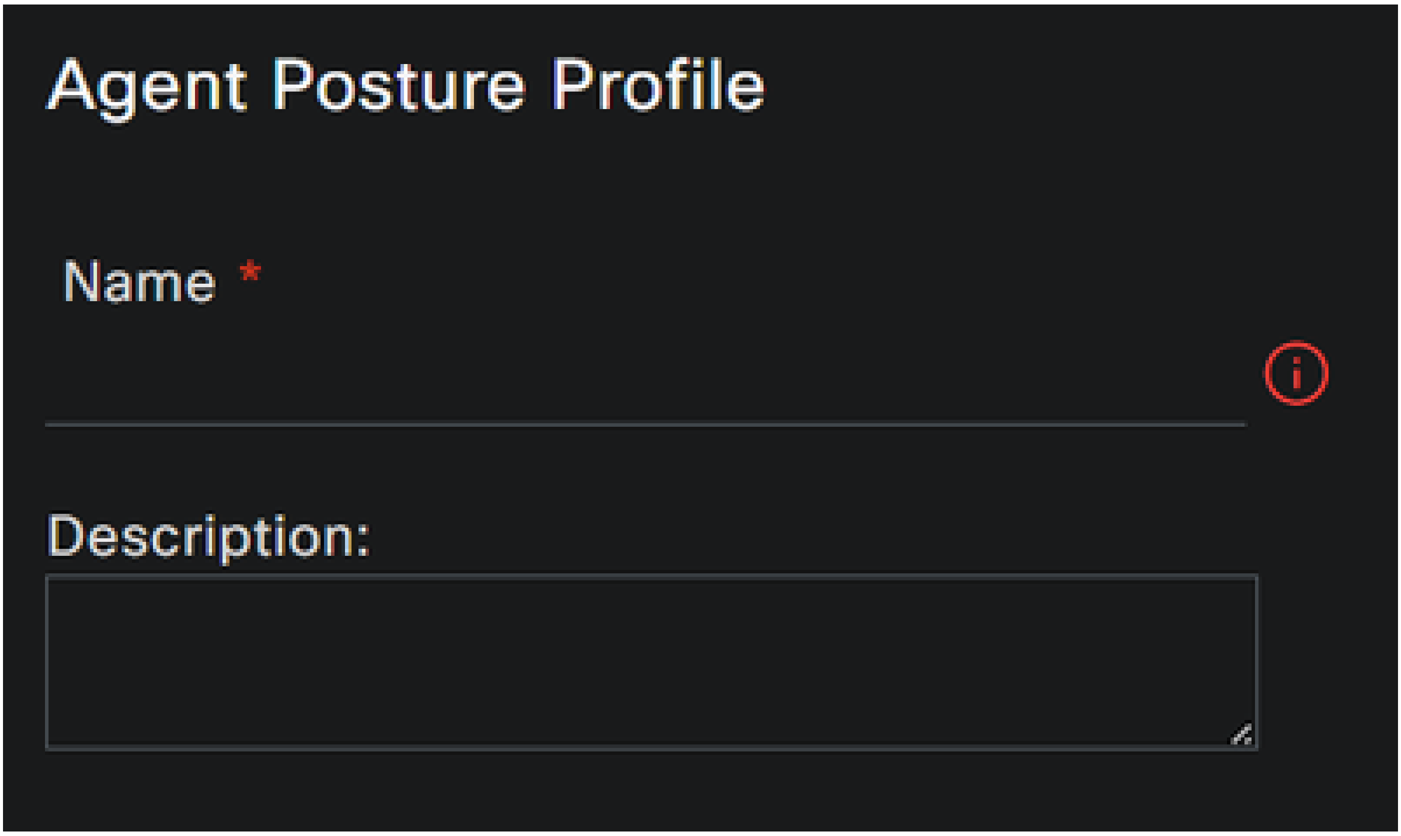
Step 3Configure the Agent Profile

- Click on + Add > Agent Posture Profile



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

- Create a **Name** for the **Posture Profile**

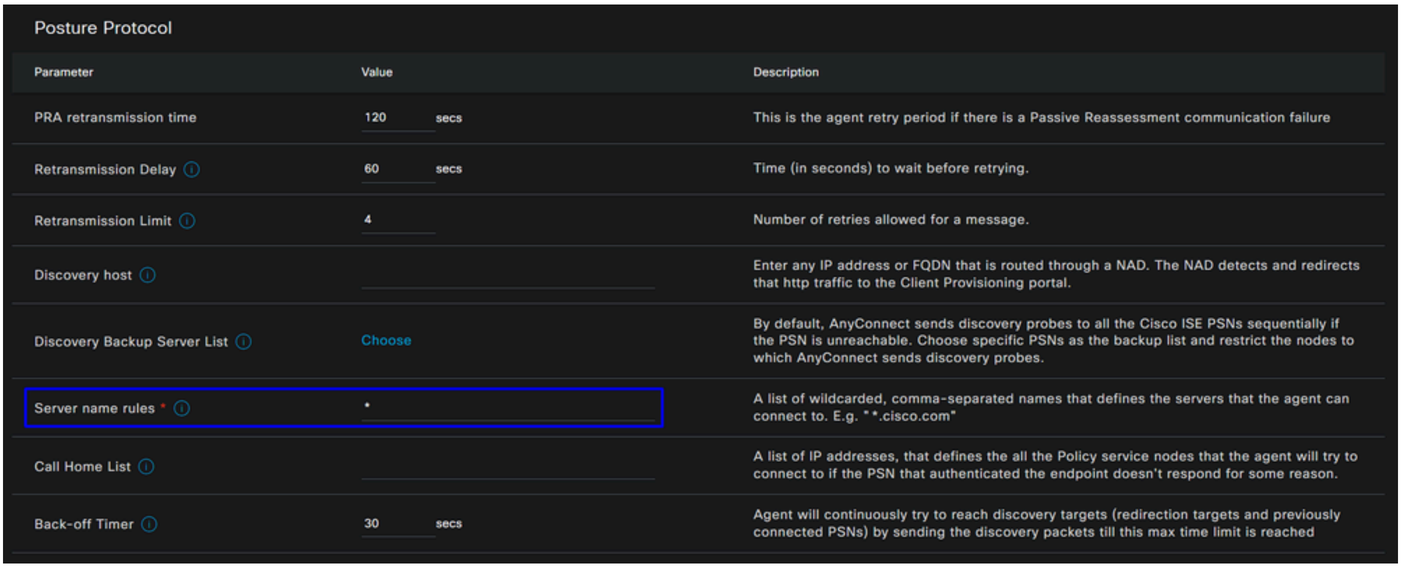


Agent Posture Profile

Name *

Description:

- Under Server name rules, put an ***** and click **Save** after that

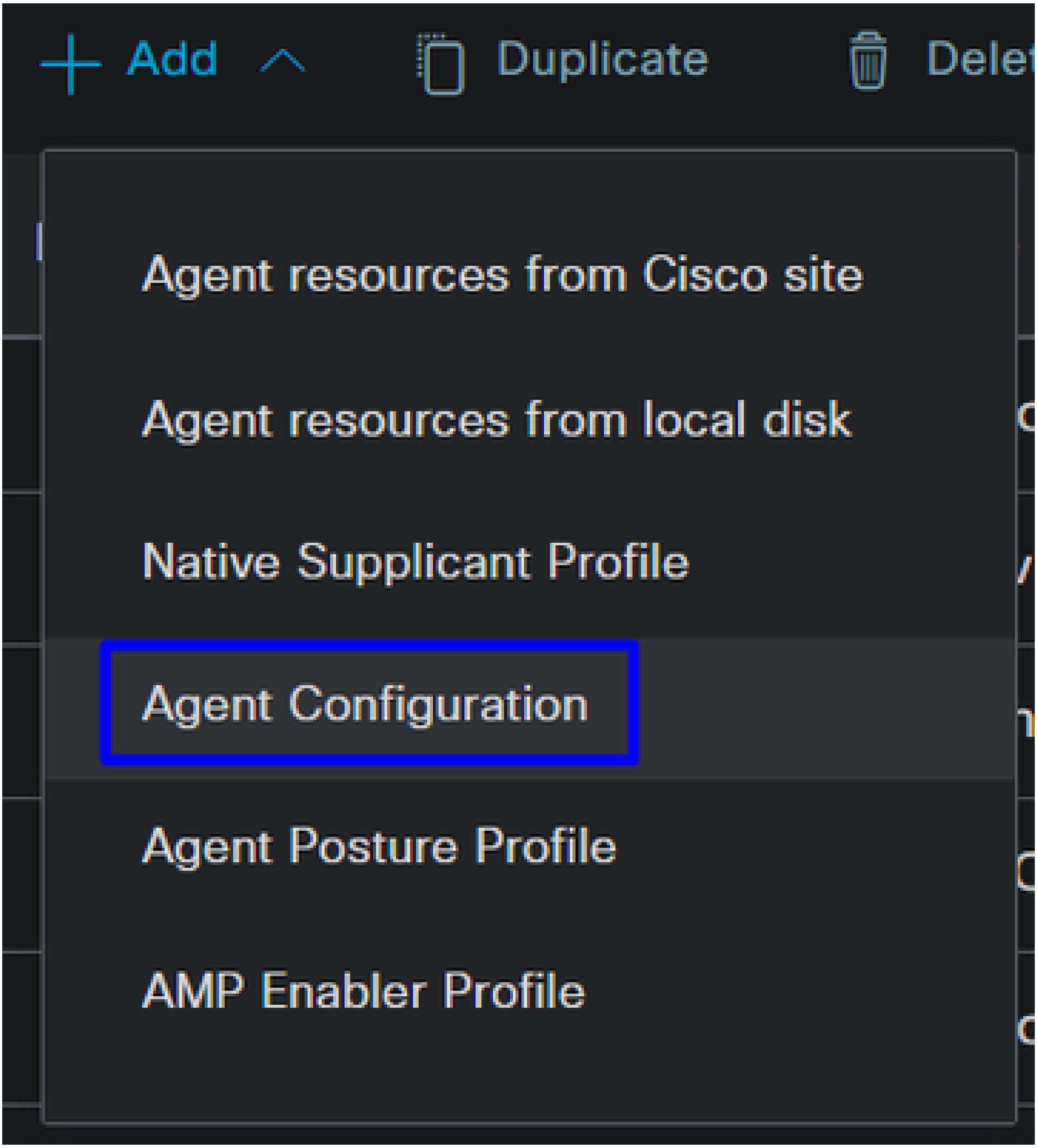


Posture Protocol

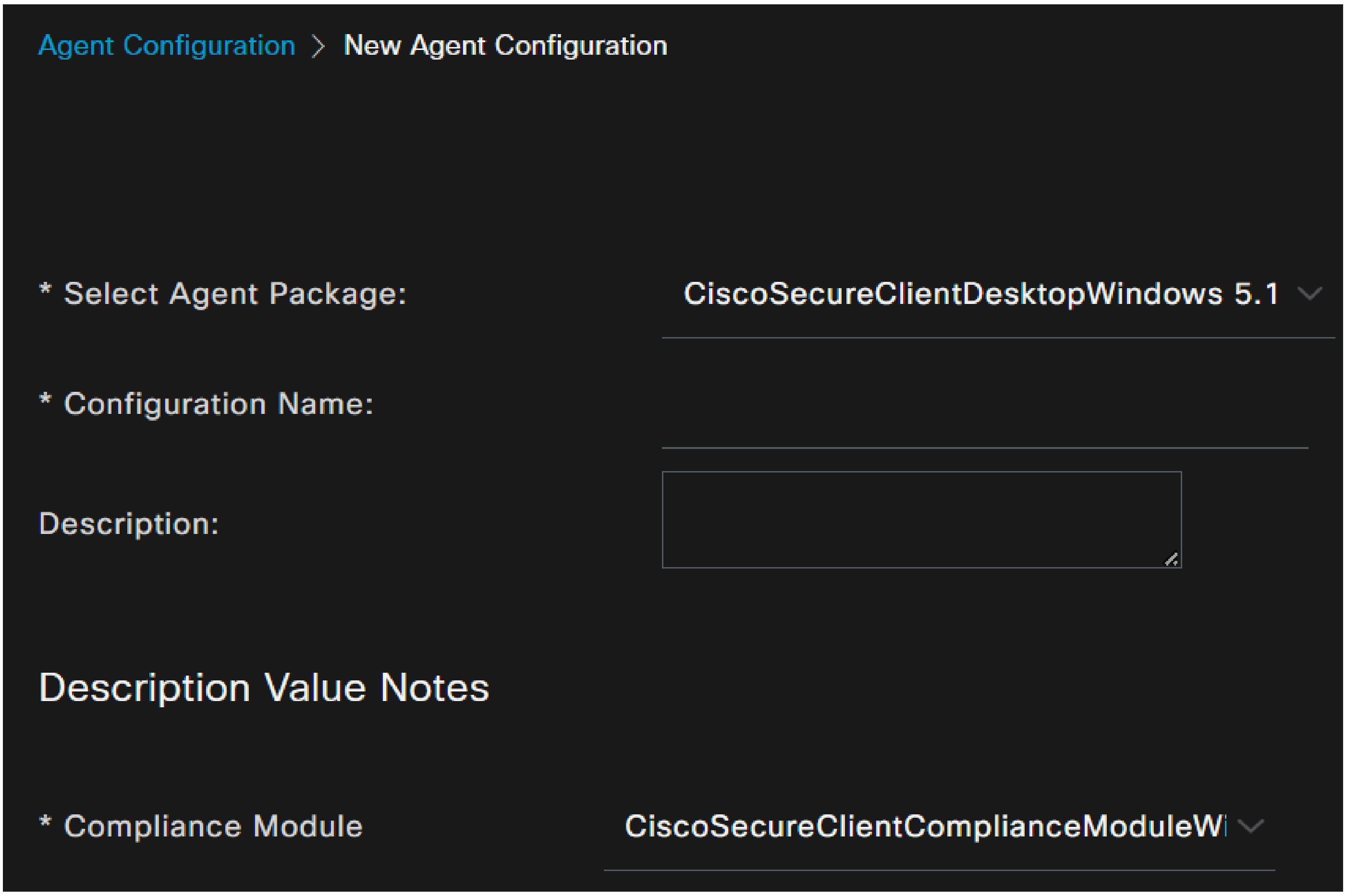
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		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 Configure the Agent Configuration

- Click on + Add > Agent Configuration


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

- After that, configure the next parameters:



Agent Configuration > New Agent Configuration

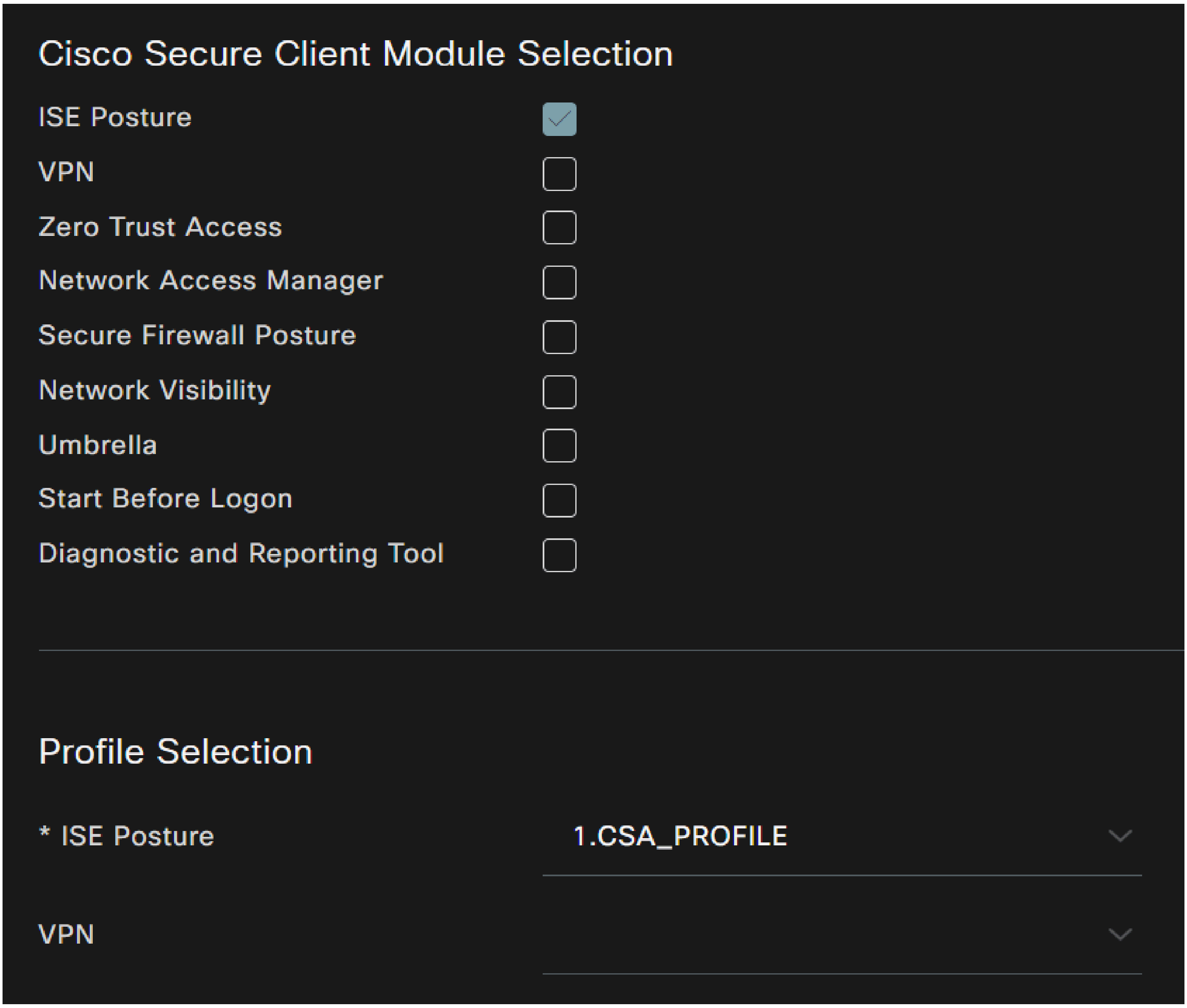
* Select Agent Package: CiscoSecureClientDesktopWindows 5.1

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi



Cisco Secure Client Module Selection

ISE Posture ☑

VPN □

Zero Trust Access □

Network Access Manager □

Secure Firewall Posture □

Network Visibility □

Umbrella □

Start Before Logon □

Diagnostic and Reporting Tool □

Profile Selection

* ISE Posture: 1.CSA_PROFILE

VPN:

- Select Agent Package : Choose the package uploaded on the Step1 Download and Upload Agent Resources
- **Configuration Name**: Choose a name to recognize the **Agent Configuration**
- **Compliance Module**: Choose the Compliance Module downloaded on the Step2 Download the compliance module
- Cisco Secure Client Module Selection
  - **ISE Posture**: Mark the Checkbox
- **Profile Selection**
  - **ISE Posture**: Choose the ISE profile configured on the Step3 Configure the Agent Profile
- Click **Save**

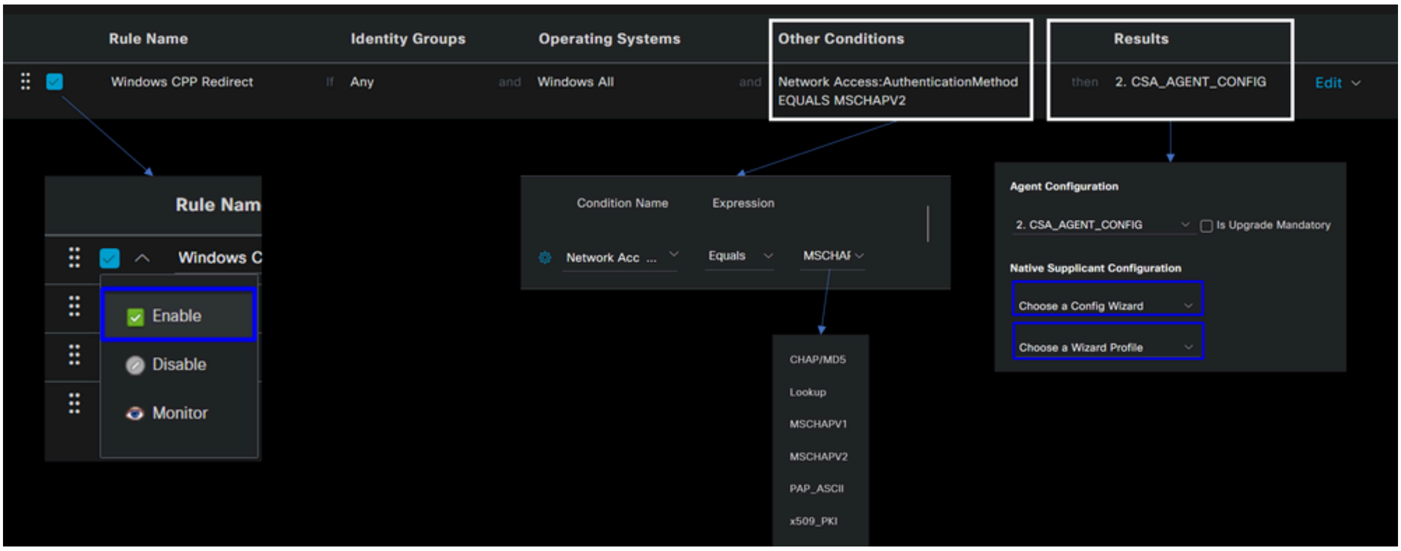
Note: It is recommended that each operating system, Windows, Mac OS, or Linux, has one Client Configuration independent.

Configure Client Provisioning Policy

To enable the provisioning of the ISE posture and modules configured in the last step, you need to configure a policy to make the provisioning.

- Navigate to your ISE Dashboard
- Click on **Work Center > Client Provisioning**

Note: It is recommended that each operating system, Windows, Mac OS, or Linux, has one Client Configuration Policy.



Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Windows CPP Redirect	If Any	and Windows All	and Network Access:AuthenticationMethod EQUALS MSCHAPV2	then 2. CSA_AGENT_CONFIG

Condition Name	Expression	
Network Acc ...	Equals	MSCHAF

Agent Configuration

2. CSA_AGENT_CONFIG ☐ Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard

Choose a Wizard Profile

- **Rule Name**: Configure the name of the policy based on the device type and identity group selection to have an easy way to identify each policy

- **Identity Groups**: Choose the identities you want to evaluate on the policy
- **Operating Systems**: Choose the operating system based on the agent package selected on the step, Select Agent Package
- **Other Condition**: Choose **Network Access** based on the **Authentication Method**EQUALS to the method configured on the step, Add RADIUS Group or you can leave in blank
- **Result**: Choose the Agent Config configured on the Step 4 Configure the Agent Configuration
  - **Native Supplicant Configuration**: Choose Config Wizard and Wizard Profile
- Mark the policy as enabled if it is not listed as enabled on the checkbox.

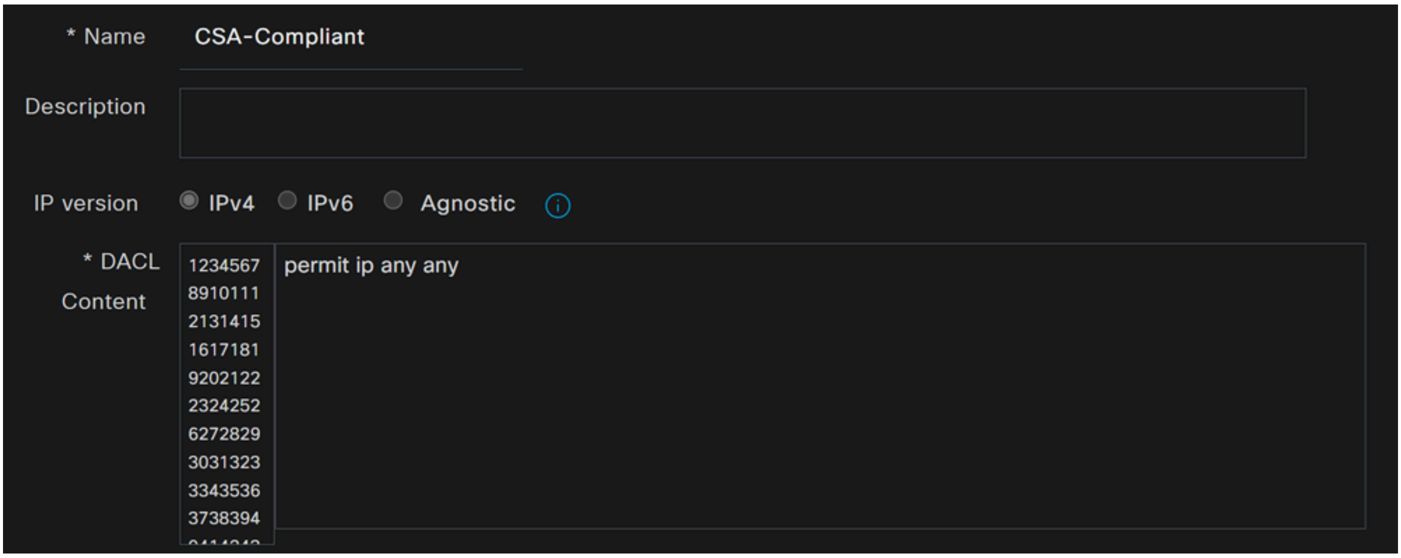
Create the Authorization Profiles

The authorization profile limits access to the resources depending on the users posture after the authentication pass. The authorization must be verified to determine which resources the user can access based on the posture.

Authorization Profile	Description
Compliant	User Compliant - Agent Installed - Posture Verified
Unknown Compliant	User Uknown Compliant - Redirect to install the agent - Posture Pending to be verified
DenyAccess	User Non Compliant - Deny Access

To configure the DACL, navigate to the ISE Dashboard:

- Click on **Work Centers > Policy Elements > Downloadable ACLs**
- Click on **+Add**
- Create the **Compliant DACL**



* Name: CSA-Compliant

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit ip any any
```

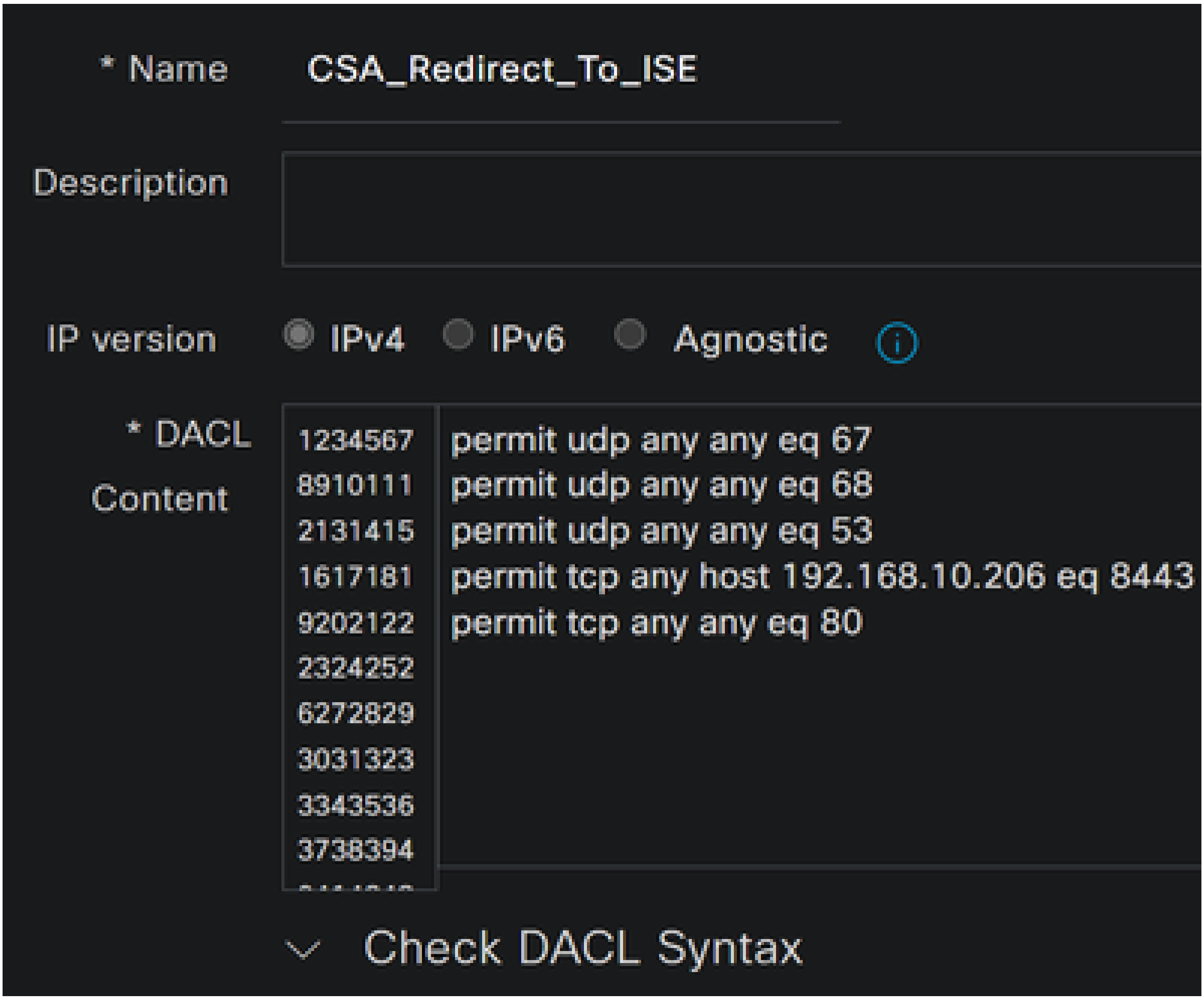
- **Name**: Add a name that makes reference to the DACL-Compliant

- **IP version**: Choose **IPv4**
- DACL Content: Create a Downloadable Access Control List (DACL) that gives access to all the resources of the network

```
permit ip any any
```

Click **Save** and create the Unknown Compliance DACL

- Click on **Work Centers > Policy Elements > Downloadable ACLs**
- Click on **+Add**
- Create the **Unknown Compliant DACL**



* Name: CSA_Redirect_To_ISE

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any host 192.168.10.206 eq 8443
permit tcp any any eq 80
```

- **Name**: Add a name that makes reference to the DACL-Unknown-Compliant
- **IP version**: Choose **IPv4**
- **DACL Content**: Create a DACL that gives limited access to the network, DHCP, DNS, HTTP, and the provisioning portal over port 8443

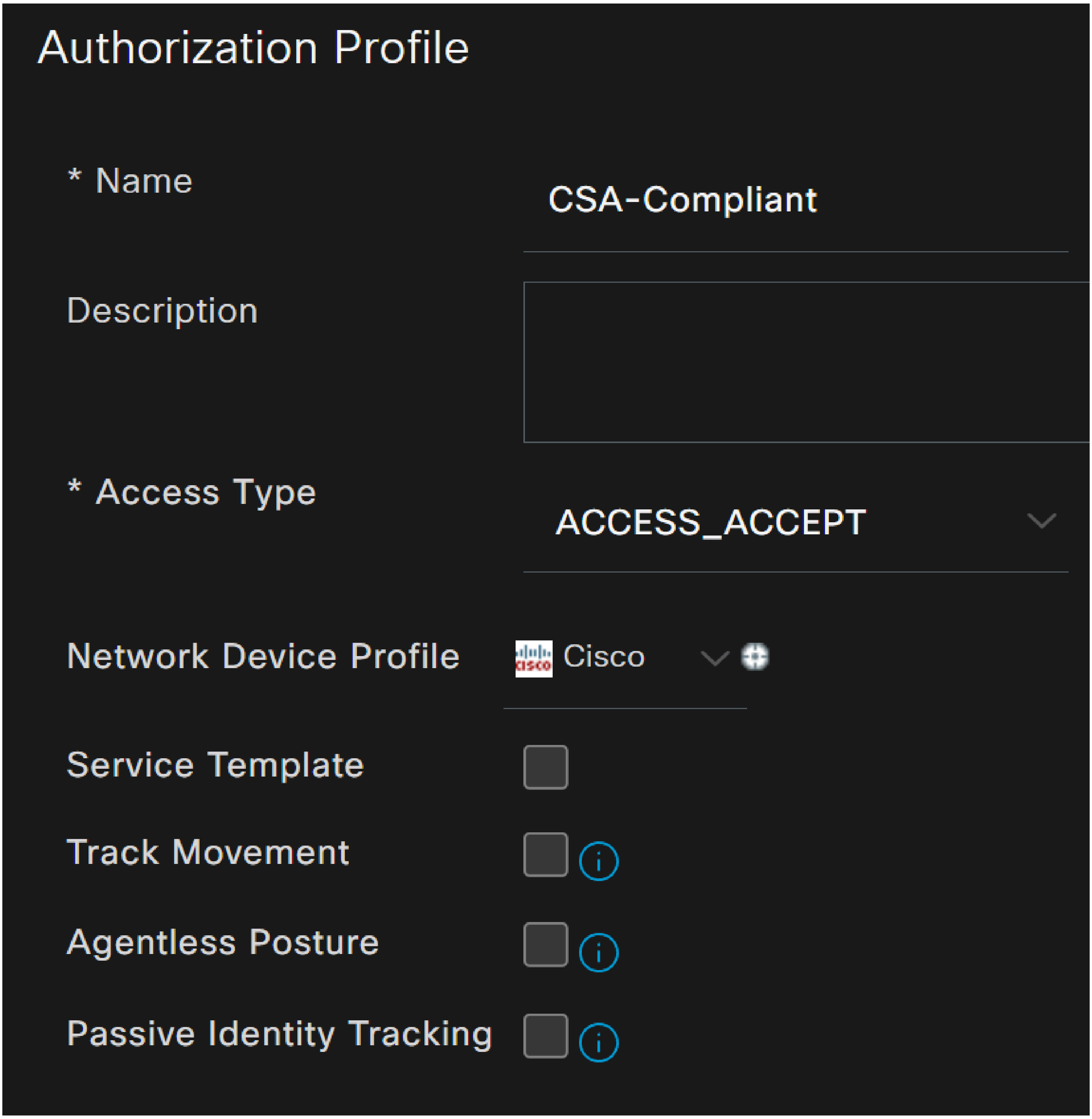
```
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443
```

Note: In this scenario, the IP address 192.168.10.206 corresponds to the Cisco Identity Services Engine (ISE) server, and port 8443 is designated for the provisioning portal. This means that TCP traffic to the IP address 192.168.10.206 via port 8443 is permitted, facilitating access to the provisioning portal.

At this point, you have the required DACL to create the authorization profiles.

To configure the authorization profiles, navigate to the ISE Dashboard:

- Click on **Work Centers > Policy Elements > Authorization Profiles**
- Click on **+Add**
- Create the **Compliant Authorization Profile**



Authorization Profile

* Name: CSA-Compliant

Description:

* Access Type: ACCESS_ACCEPT

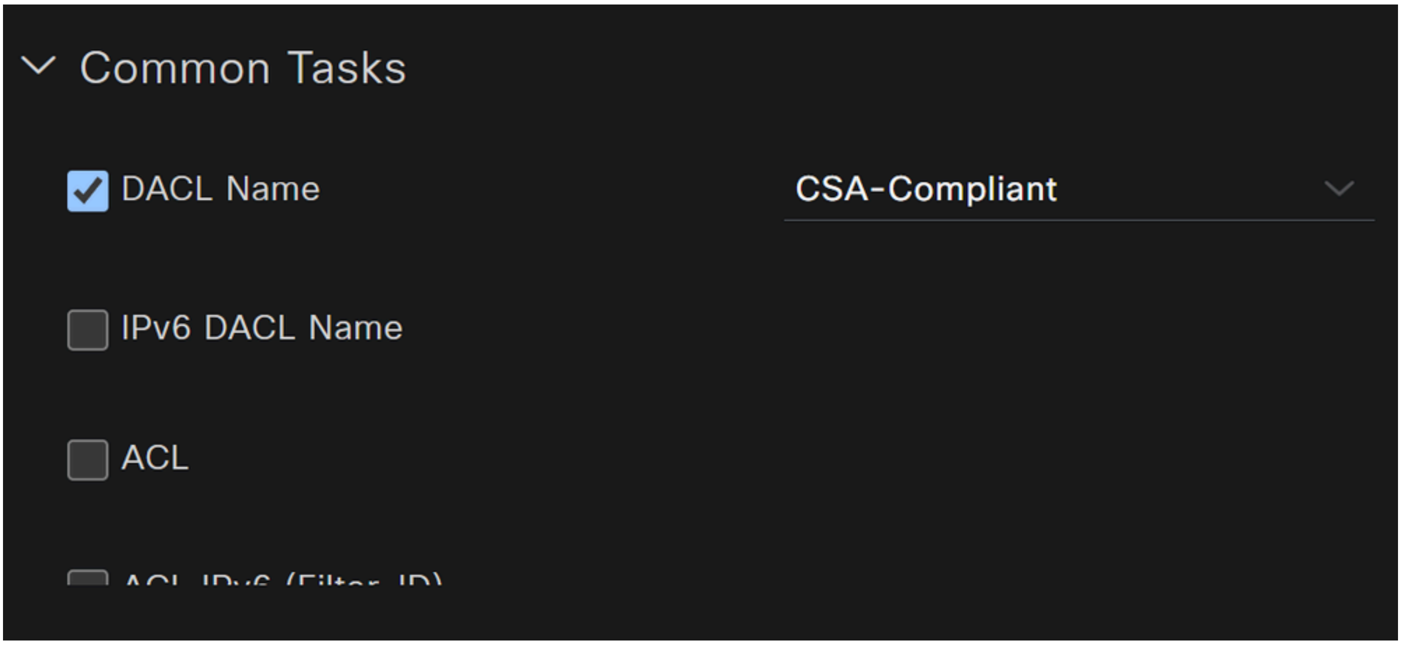
Network Device Profile: Cisco

Service Template □

Track Movement □ ⓘ

Agentless Posture □ ⓘ

Passive Identity Tracking □ ⓘ


Common Tasks

☑ DACL Name CSA-Compliant

□ IPv6 DACL Name

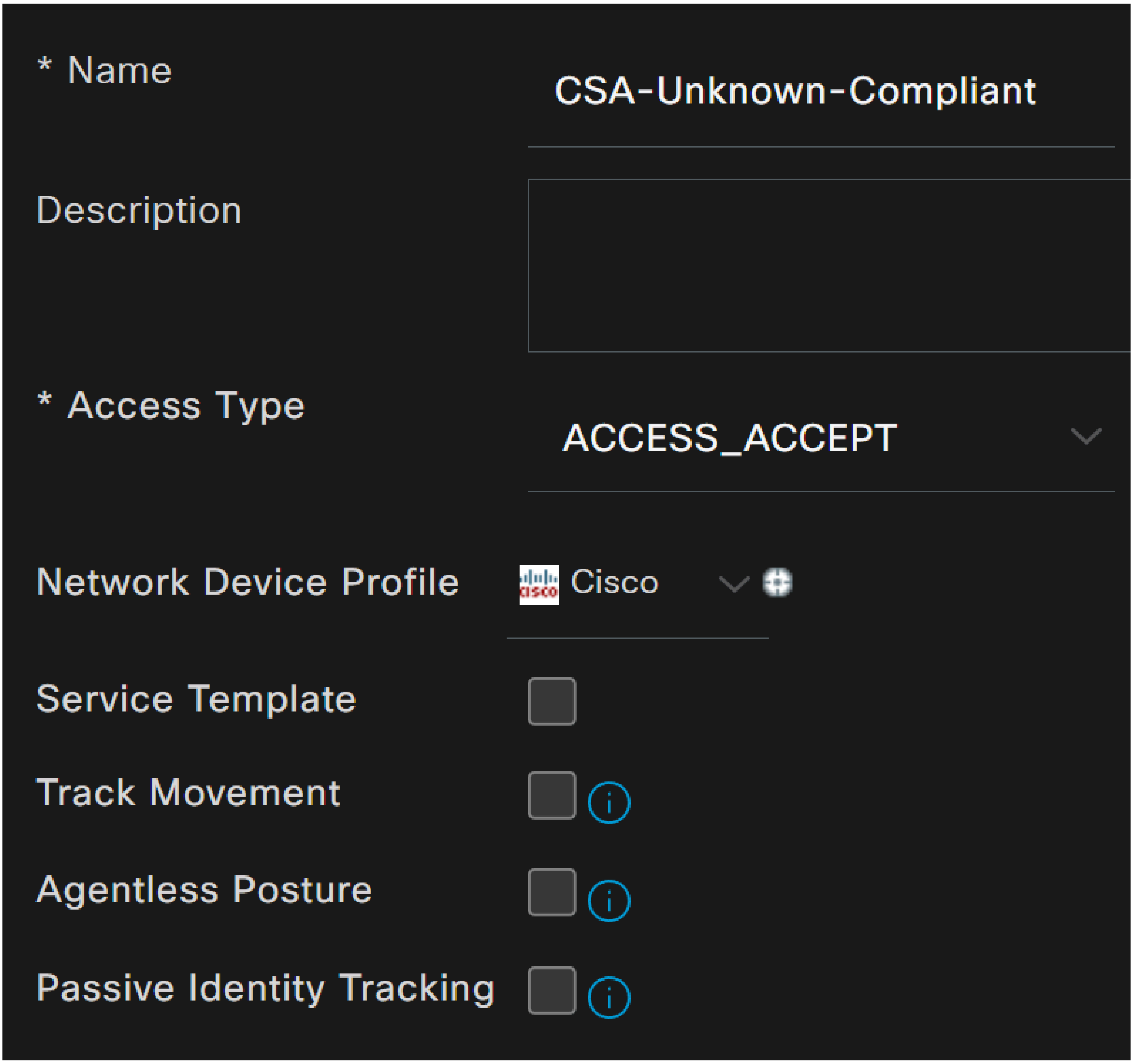
□ ACL

- **Name**: Create a name that makes reference to the compliant authorization profile
- Access Type: Choose **ACCESS_ACCEPT**

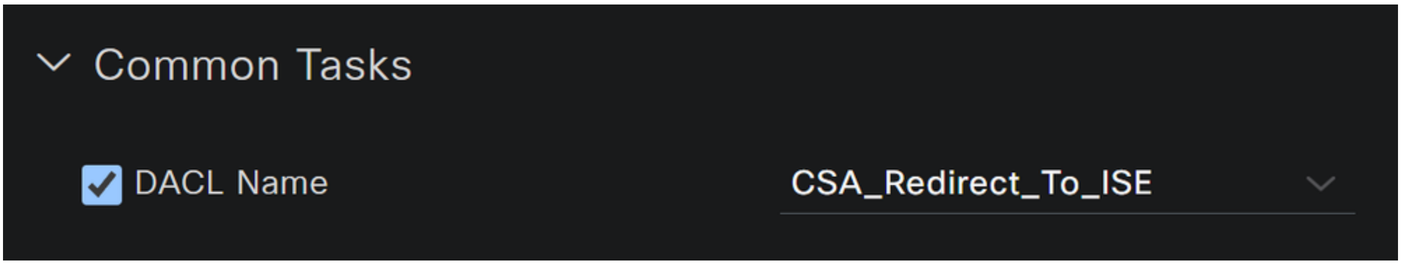
- **Common Tasks**
  - **DACL NAME**: Choose the DACL configured on the step Compliant DACL

Click **Save** and create the Unknown Authorization Profile

- Click on **Work Centers > Policy Elements > Authorization Profiles**
- Click on **+Add**
- Create the **Uknown Compliant Authorization Profile**

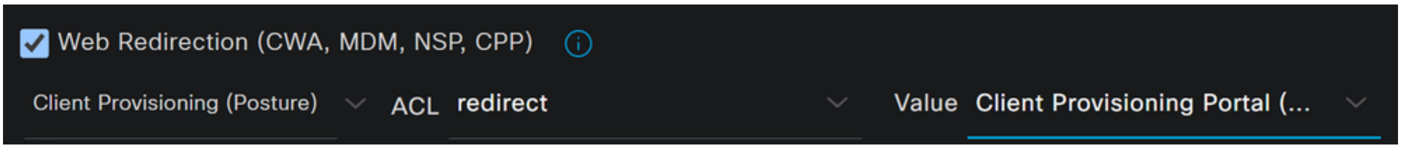


* Name	CSA-Unknown-Compliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Agentless Posture	□
Passive Identity Tracking	□



Common Tasks

☑ DACL Name CSA_Redirect_To_ISE



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

Client Provisioning (Posture) ACL redirect Value Client Provisioning Portal (...

- **Name**: Create a name that makes reference to the unknown compliant authorization profile
- Access Type: Choose **ACCESS_ACCEPT**

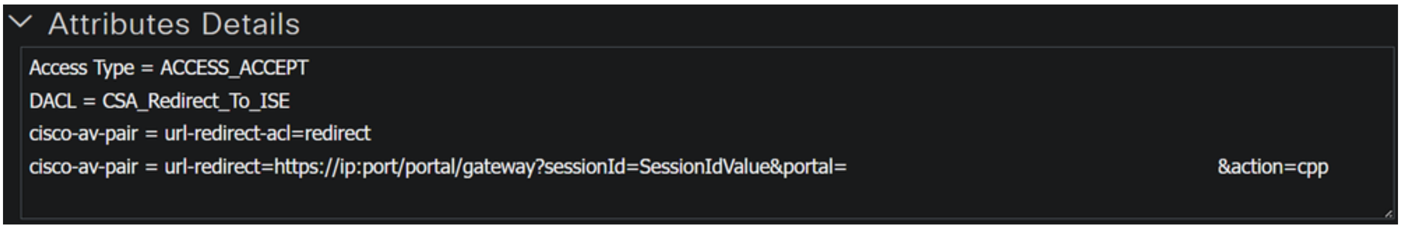
- **Common Tasks**

- **DACL NAME**: Choose the DACL configured on the step Unknown Compliant DACL
- **Web Redirection (CWA,MDM,NSP,CPP)**
    - Choose **Client Provisioning (Posture)**
    - **ACL**: Must be redirect
    - **Value**: Choose the default provisioning portal, or if you defined another, choose it

---

Note: The name for the redirection ACL on Secure Access for all the deployments is **redirect**.

After you define all of these values, you must have something similar under Attributes Details.



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

Click **Save** to end the configuration and continue with the next step.

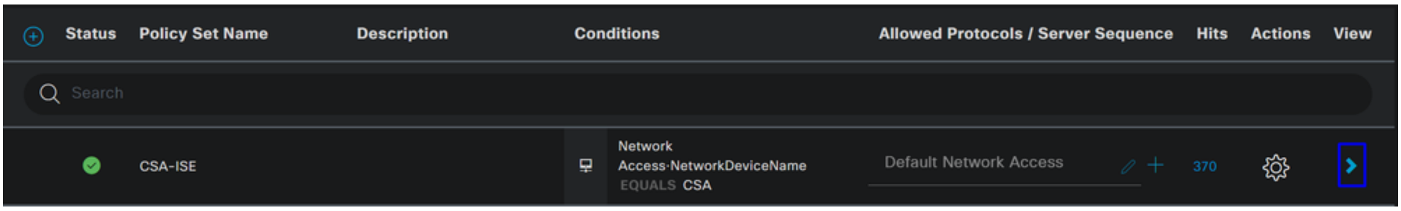
Configure Posture Policy Set

These three policies you create are based on the authorization profiles you configured; for **DenyAccess**, you do not need to create another one.

Policy Set - Authorization	Authorization Profile
Compliant	Authorization Profile - Compliant
Unknown Compliant	Authorization Profile - Uknown Compliant
Non Compliant	DenyAccess

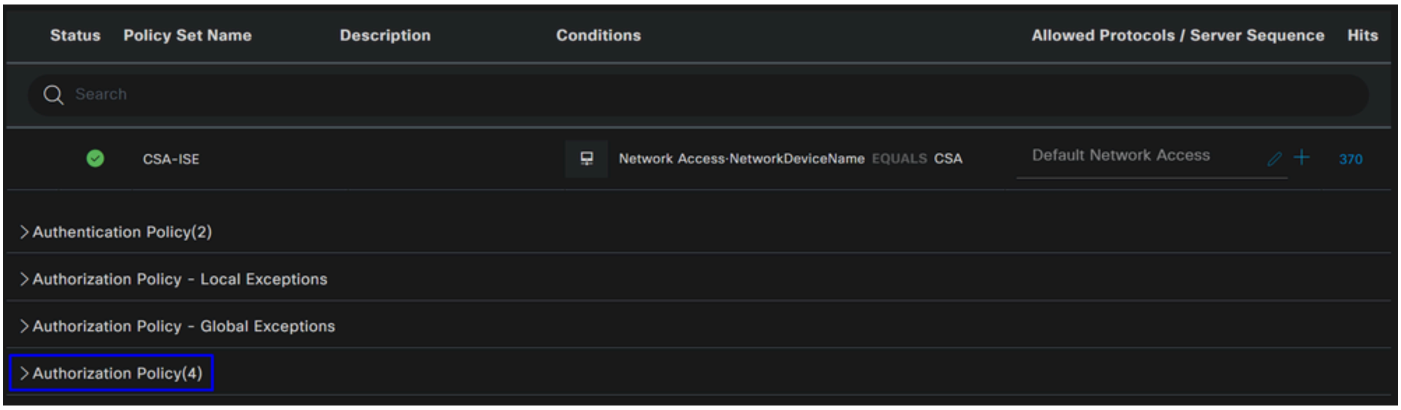
Navigate to your ISE Dashboard

- Click on **Work Center** > **Policy Sets**
- Click on the> to access to the policy that you have created



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

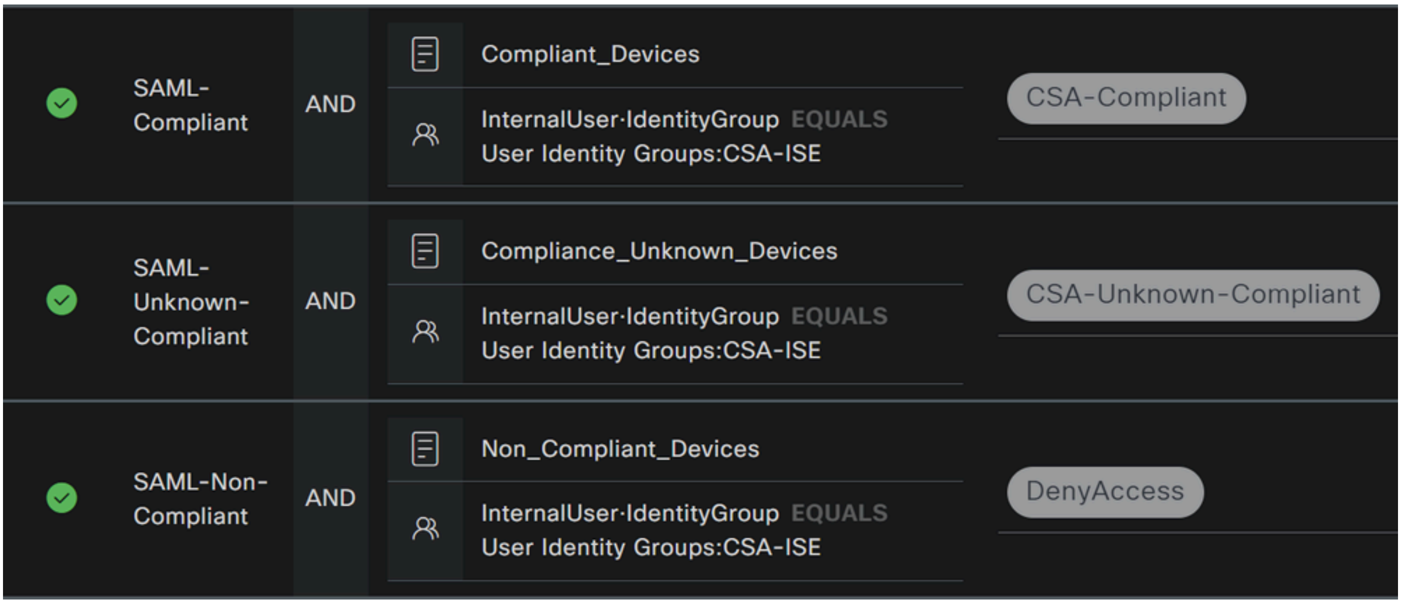
- Click on the Authorization Policy



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

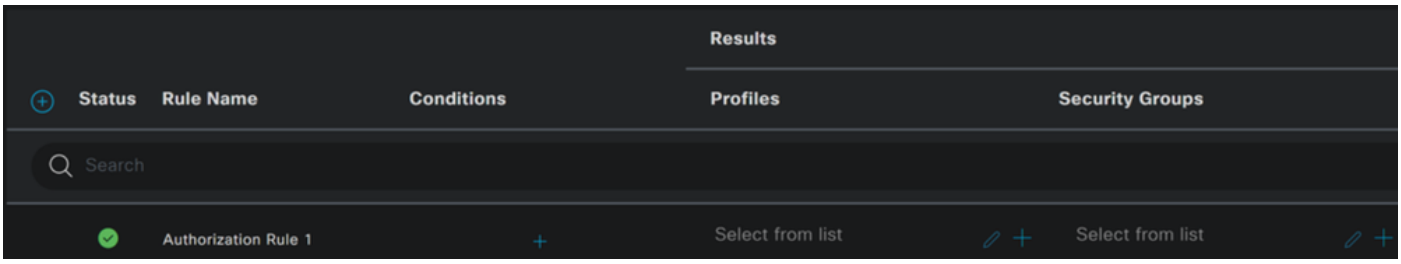
> Authentication Policy(2)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
> Authorization Policy(4)

- Create the next three policies in the next order:



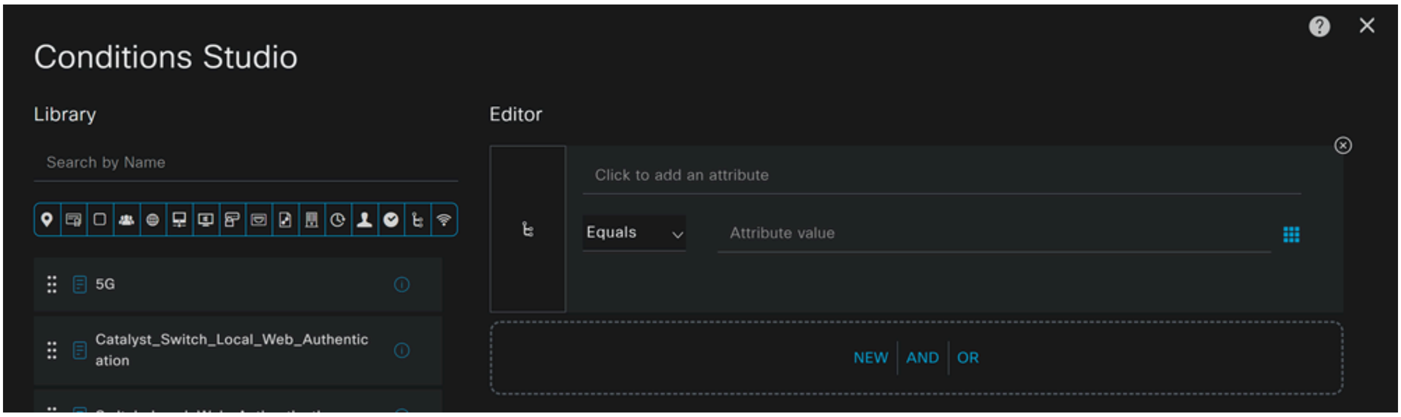
✓	SAML-Compliant	AND	Compliant_Devices InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE	CSA-Compliant
✓	SAML-Unknown-Compliant	AND	Compliance_Unknown_Devices InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE	CSA-Unknown-Compliant
✓	SAML-Non-Compliant	AND	Non_Compliant_Devices InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE	DenyAccess

- Click on + to define the **CSA-Compliance** policy :



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

- For the next step, change the Rule Name, Conditions and Profiles
- When setting the **Name** configure a name to **CSA-Compliance**
- To configure the **Condition**, click on the +
- Under **Condition Studio**, you find the information:



Conditions Studio

Library

Search by Name

5G

Catalyst_Switch_Local_Web_Authentication

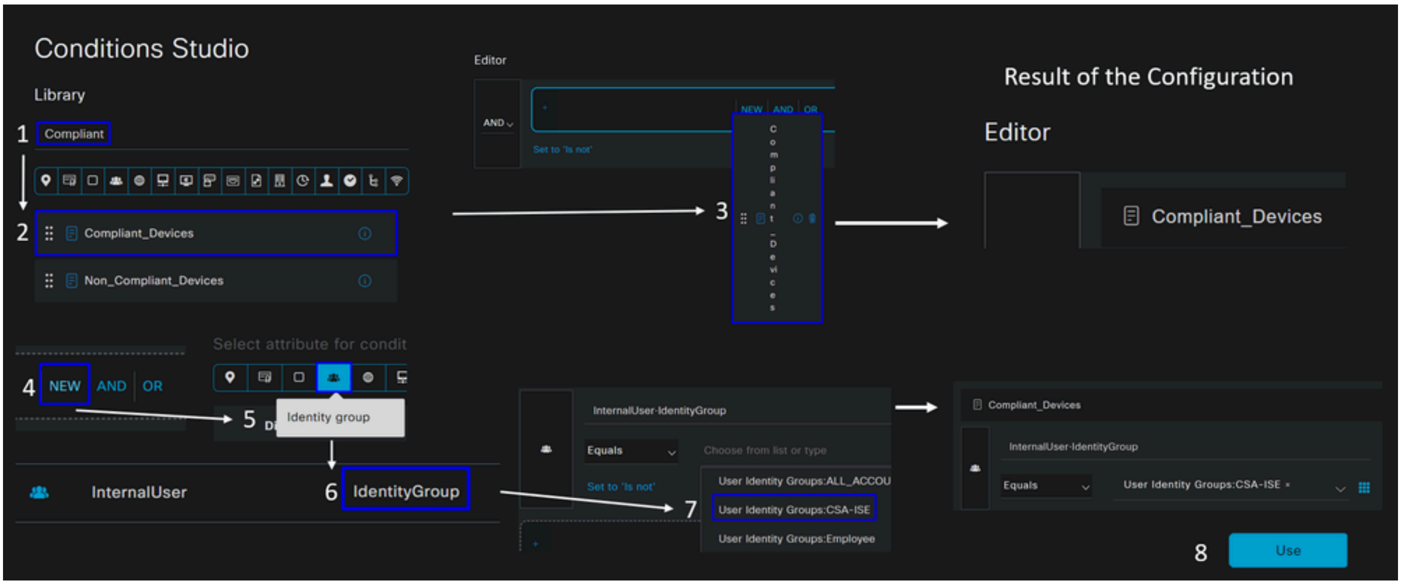
Editor

Click to add an attribute

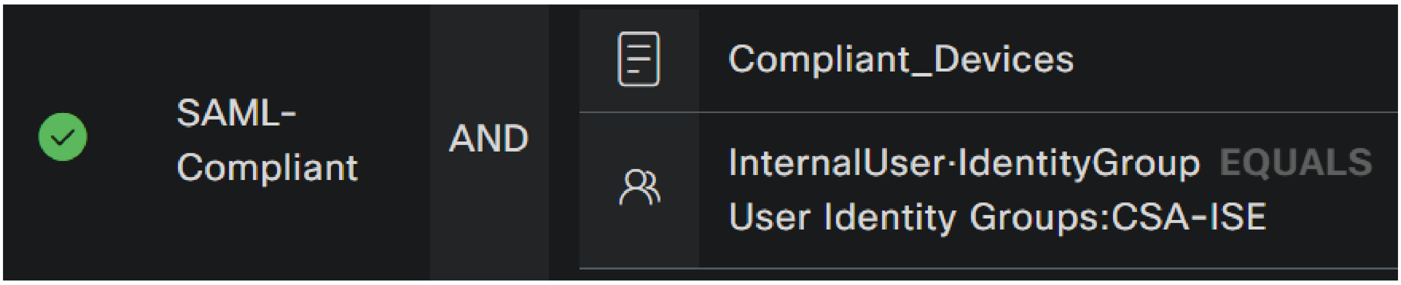
Equals

Attribute value

1. To create the condition, search for **compliant**
2. You must have displayed Compliant_Devices
3. Drag and drop under the **Editor**
4. Click under the Editor in **New**
5. Click on the **Identity Group** icon
6. Choose **Internal User Identity Group**
7. Under **Equals**, choose the **User Identity Group** that you want to match
8. Click **Use**



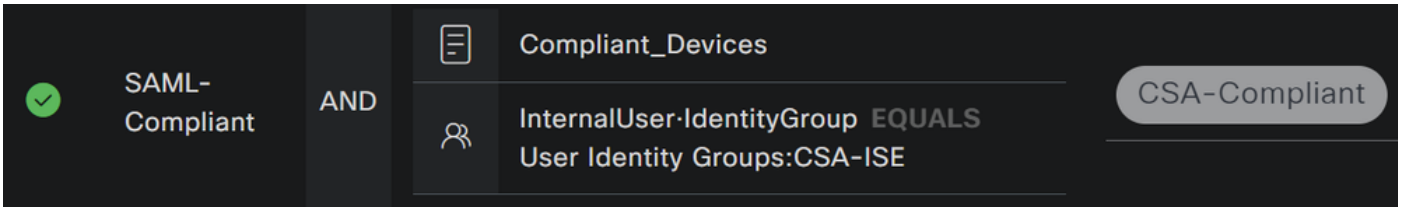
- As a result, you have the next image



SAML-Compliant AND Compliant_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

- Under **Profile** click under the drop-down button and choose the complaint authorization profile configured on the step, Compliant Authorization Profile



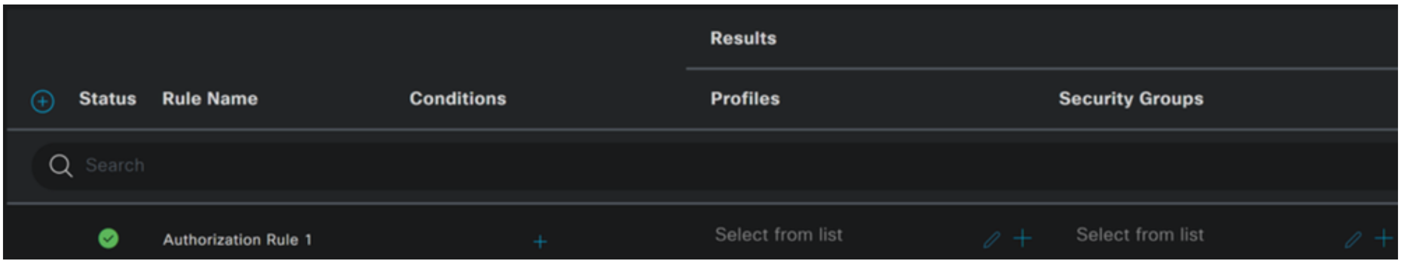
SAML-Compliant AND Compliant_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

CSA-Compliant

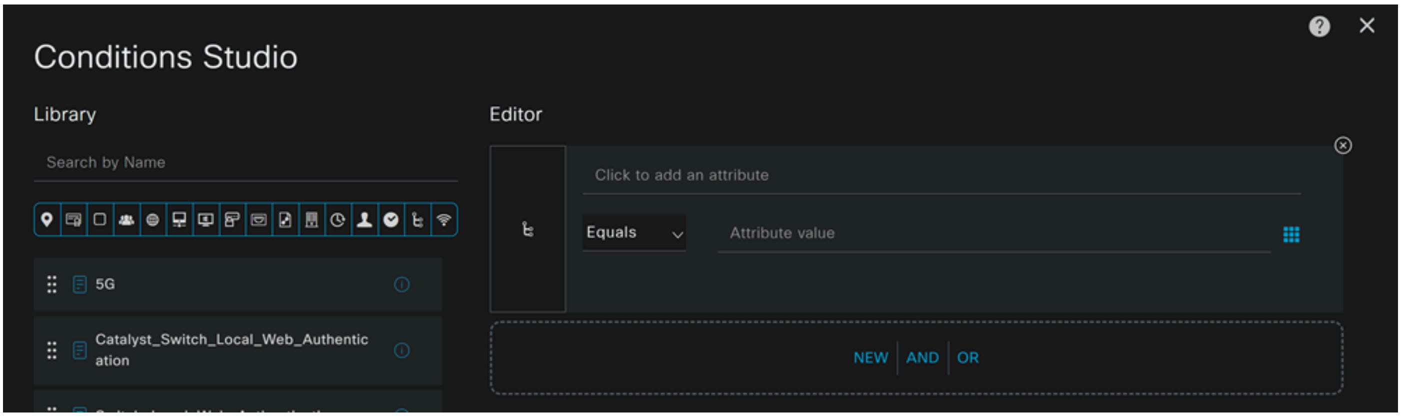
Now you have configured the **Compliance Policy Set.**

- Click on + to define the **CSA-Unknown-Compliance** policy :

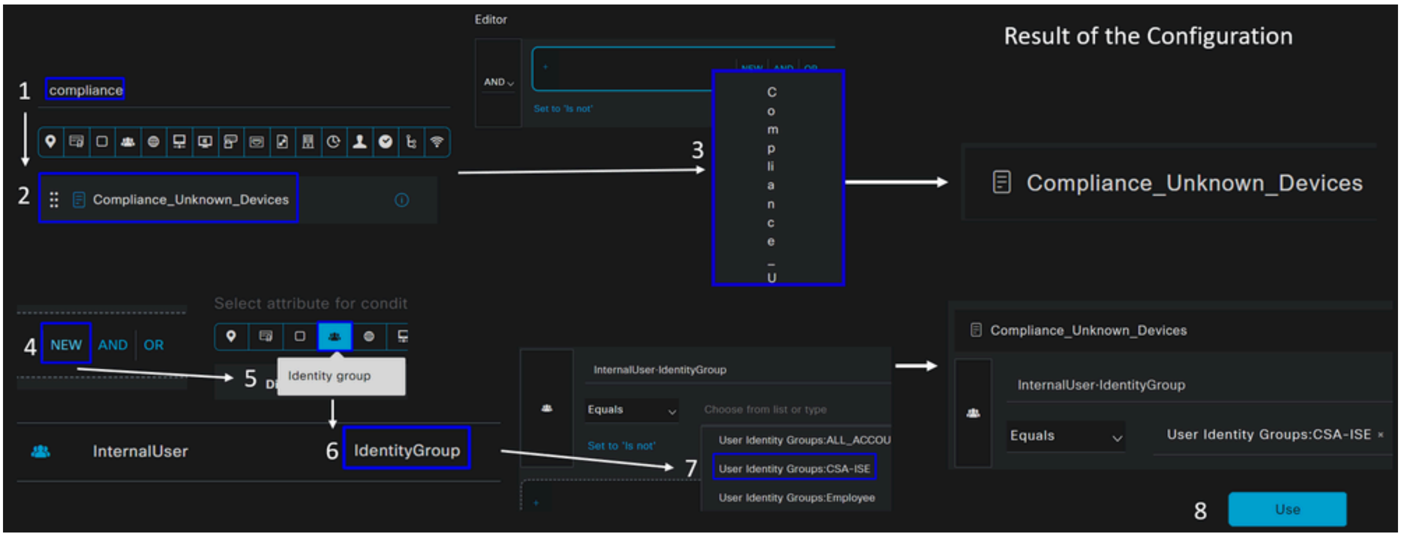


			Results	
Status	Rule Name	Conditions	Profiles	Security Groups
Search				
✓	Authorization Rule 1	+	Select from list	Select from list

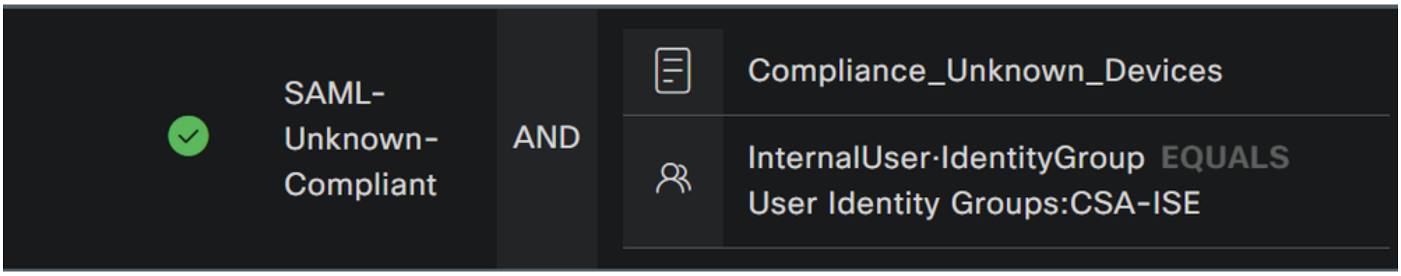
- For the next step, change the Rule Name, Conditions and Profiles
- When setting the **Name** configure a name to **CSA-Unknown-Compliance**
- To configure the **Condition**, click on the +
- Under **Condition Studio**, you find the information:



1. To create the condition, search for **compliance**
2. You must have displayed Compliant_Unknown_Devices
3. Drag and drop under the **Editor**
4. Click under the Editor in **New**
5. Click on the **Identity Group** icon
6. Choose **Internal User Identity Group**
7. Under **Equals**, choose the **User Identity Group** that you want to match
8. Click **Use**


Result of the Configuration
Editor
1
compliance
2
Compliance_Unknown_Devices
3
Compliance_Unknown_Devices
Select attribute for condit
4
NEW
AND
OR
5
Identity group
InternalUser
6
IdentityGroup
InternalUser·IdentityGroup
Equals
Choose from list or type
Set to 'Is not'
User Identity Groups:ALL_ACCOU
7
User Identity Groups:CSA-ISE
User Identity Groups:Employee
Compliance_Unknown_Devices
InternalUser·IdentityGroup
Equals
User Identity Groups:CSA-ISE
8
Use

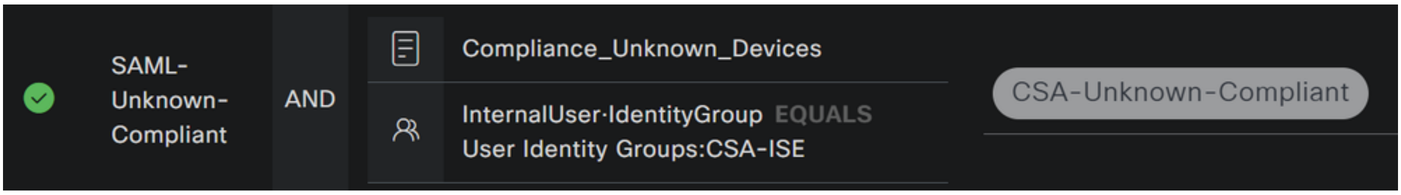
- As a result, you have the next image


SAML-Unknown-Compliant AND

Compliance_Unknown_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

- Under **Profile** click under the drop-down button and choose the complaint authorization profile configured on the step, Unknown Compliant Authorization Profile



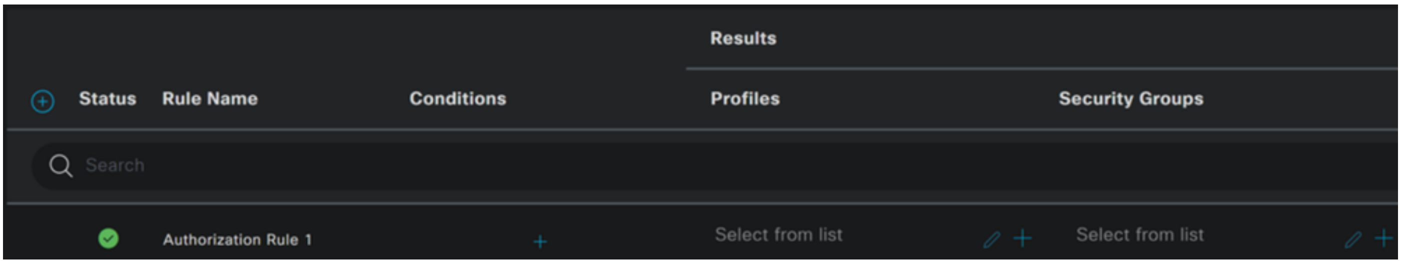
SAML-Unknown-Compliant AND Compliance_Unknown_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

CSA-Unknown-Compliant

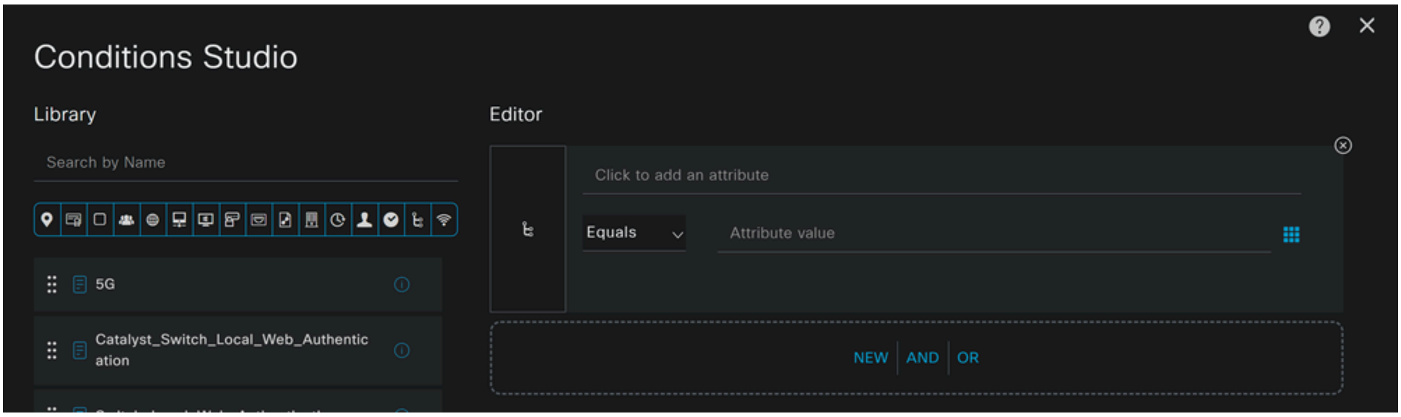
Now you have configured the **Unknown Compliance Policy Set.**

- Click on + to define the **CSA- Non-Compliant** policy:

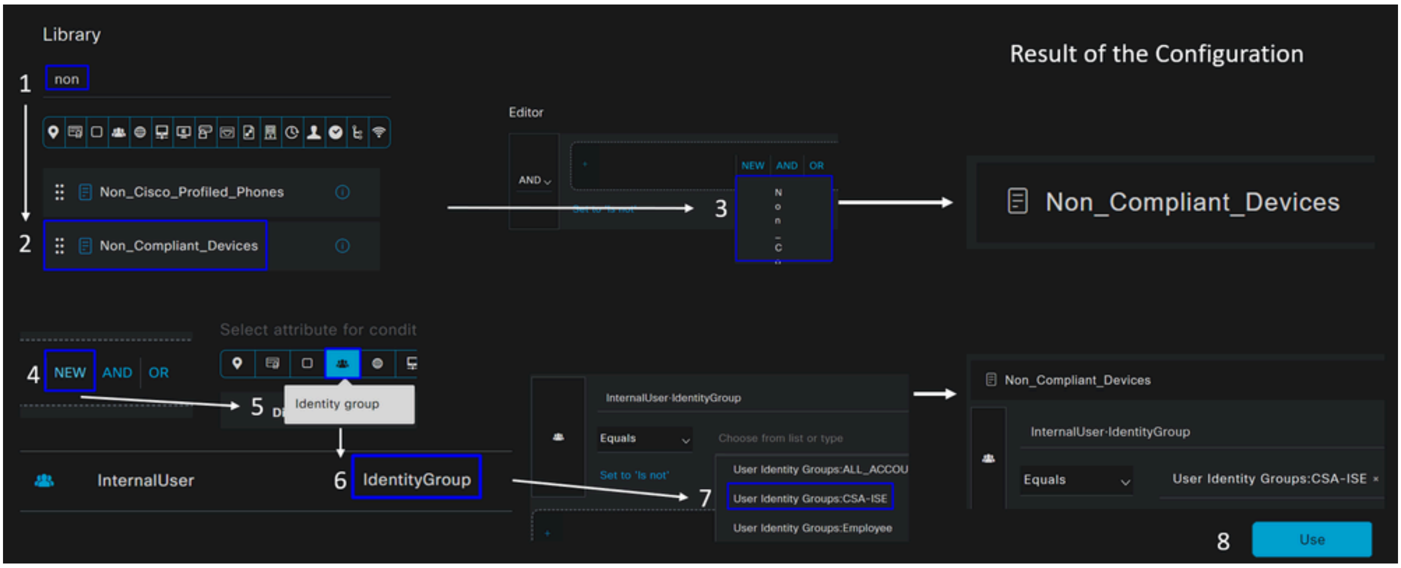


Status	Rule Name	Conditions	Profiles	Security Groups
✓	Authorization Rule 1	+	Select from list	Select from list

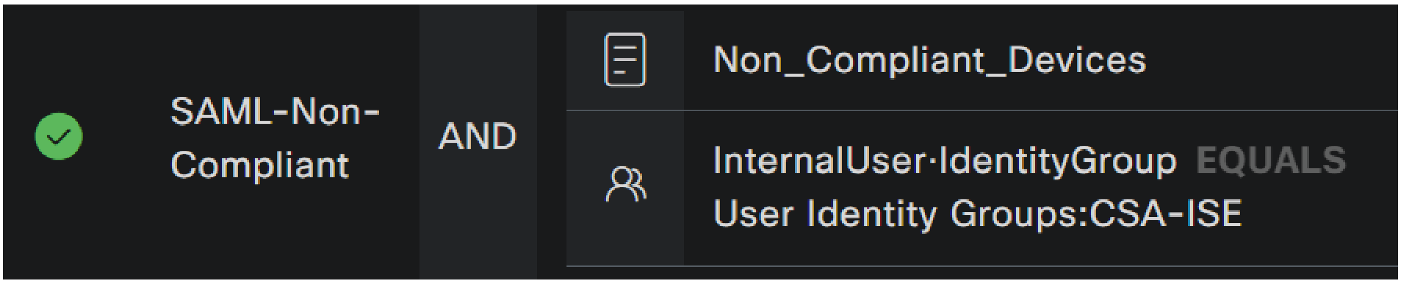
- For the next step, change the Rule Name, Conditions and Profiles
- When setting the **Name** configure a name to **CSA-Non-Compliance**
- To configure the **Condition**, click on the +
- Under **Condition Studio**, you find the information:



1. To create the condition, search for **non**
2. You must have displayed Non_Compliant_Devices
3. Drag and drop under the **Editor**
4. Click under the Editor in **New**
5. Click on the **Identity Group** icon
6. Choose **Internal User Identity Group**
7. Under **Equals**, choose the **User Identity Group** that you want to match
8. Click **Use**


Library
1
non
Non_Cisco_Profiled_Phones
2
Non_Compliant_Devices
Editor
AND
NEW AND OR
3
Result of the Configuration
Non_Compliant_Devices
Select attribute for condit
4
NEW AND OR
5
Identity group
6
InternalUser
IdentityGroup
InternalUser·IdentityGroup
Equals
Choose from list or type
Set to 'Is not'
User Identity Groups:ALL_ACCOU
User Identity Groups:CSA-ISE
User Identity Groups:Employee
7
Non_Compliant_Devices
InternalUser·IdentityGroup
Equals
User Identity Groups:CSA-ISE
8
Use

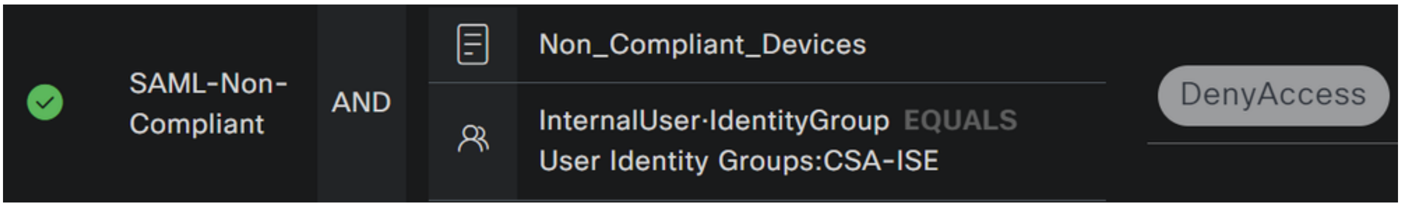
- As a result, you have the next image



SAML-Non-Compliant AND Non_Compliant_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

- Under **Profile** click under the drop-down button and choose the complaint authorization profile **DenyAccess**



SAML-Non-Compliant AND Non_Compliant_Devices

InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

DenyAccess

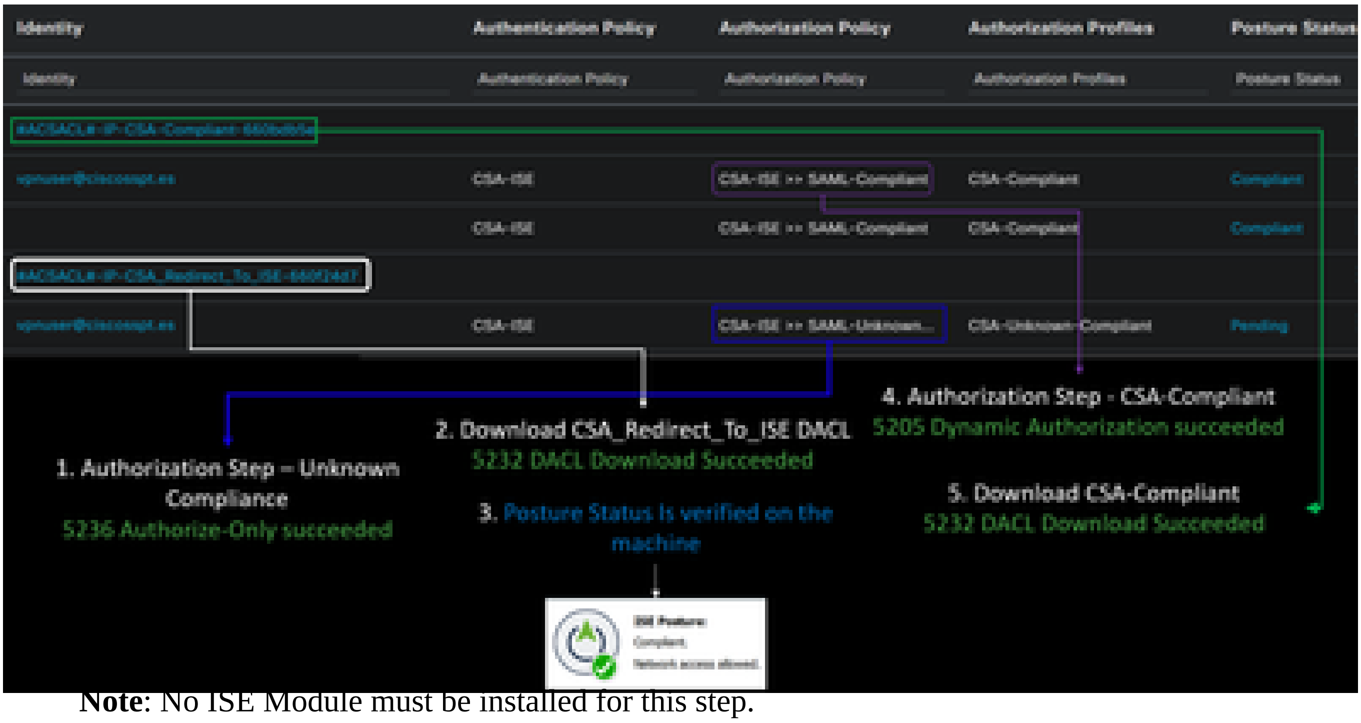
Once you end the configuration of the three profiles, you are ready to test your integration with posture.

Verify

Posture Validation

Connection on the Machine

Connect to your FQDN RA-VPN domain provided on Secure Access via Secure Client.



Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
#ACSACL#-IP-CSA-Compliant-660bdb5e				
vpnuser@ciscoospt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscoospt.es	CSA-ISE	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

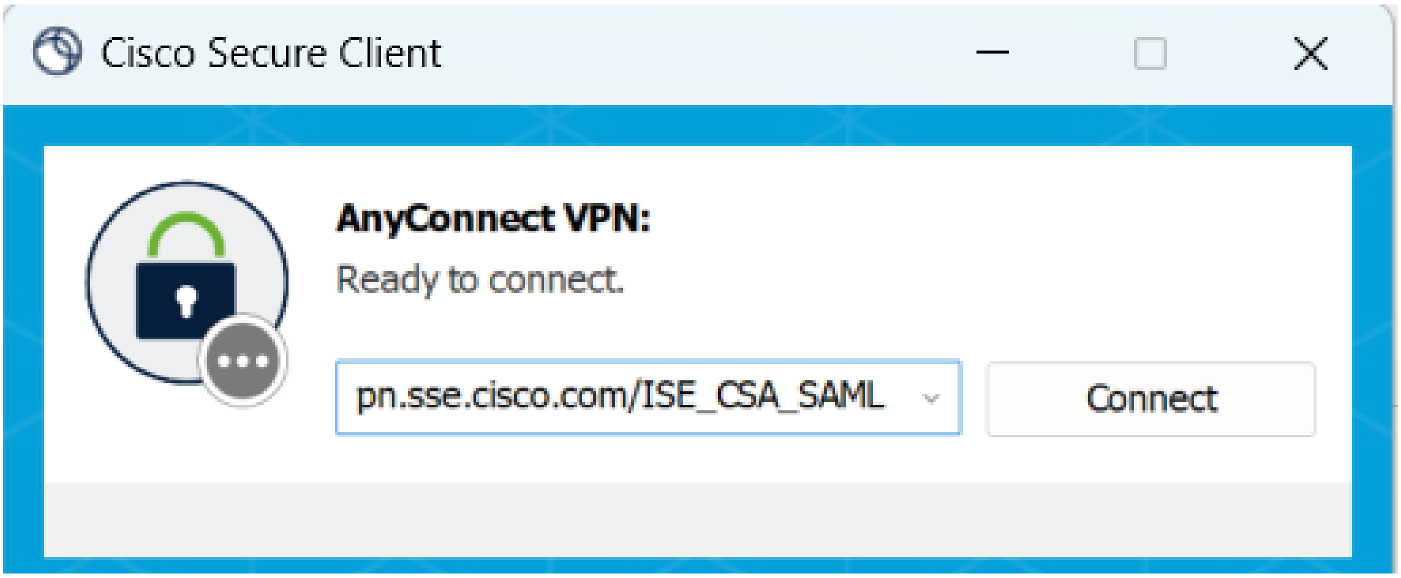
ISE Posture:
Compliant.
Network access allowed.

4. Authorization Step - CSA-Compliant
5205 Dynamic Authorization succeeded

5. Download CSA-Compliant
5232 DACL Download Succeeded

Note: No ISE Module must be installed for this step.

1. Connect using Secure Client.

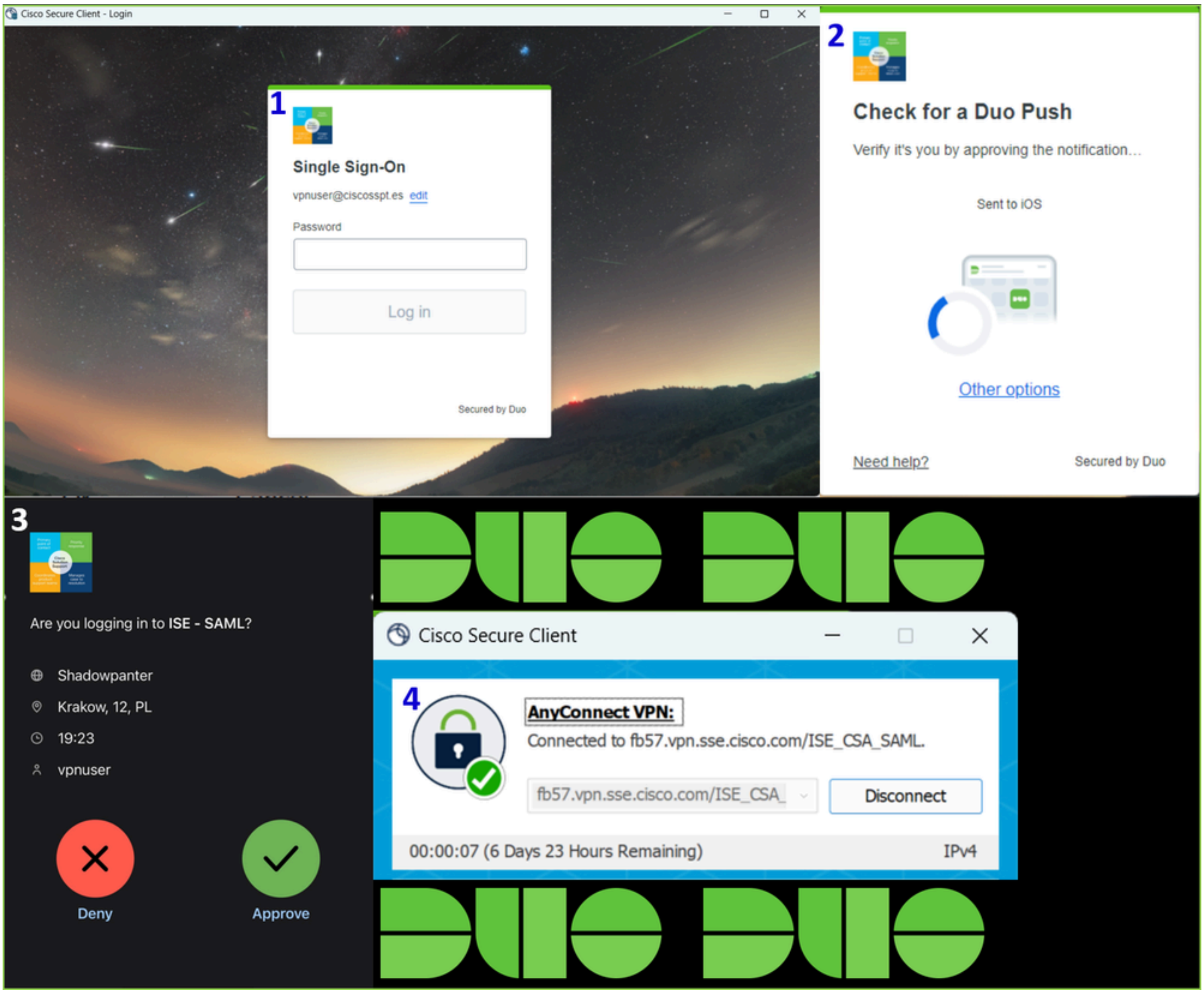


Cisco Secure Client

AnyConnect VPN:
Ready to connect.

pn.sse.cisco.com/ISE_CSA_SAML

2. Provide the credentials to authenticate via Duo.



Single Sign-On

vpnuser@ciscosspt.es edit

Password

Check for a Duo Push

Verify it's you by approving the notification...

Sent to iOS

Are you logging in to ISE - SAML?

Shadowpanter

Krakow, 12, PL

19:23

vpnuser

Cisco Secure Client

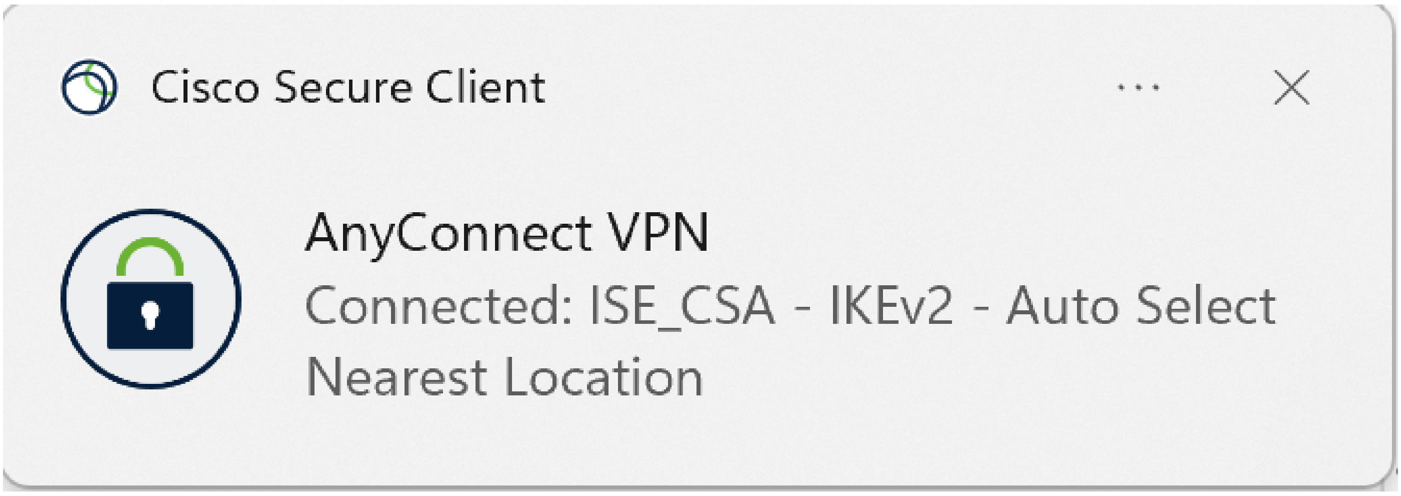
AnyConnect VPN:

Connected to fb57.vpn.sse.cisco.com/ISE_CSA_SAML.

fb57.vpn.sse.cisco.com/ISE_CSA_

00:00:07 (6 Days 23 Hours Remaining)

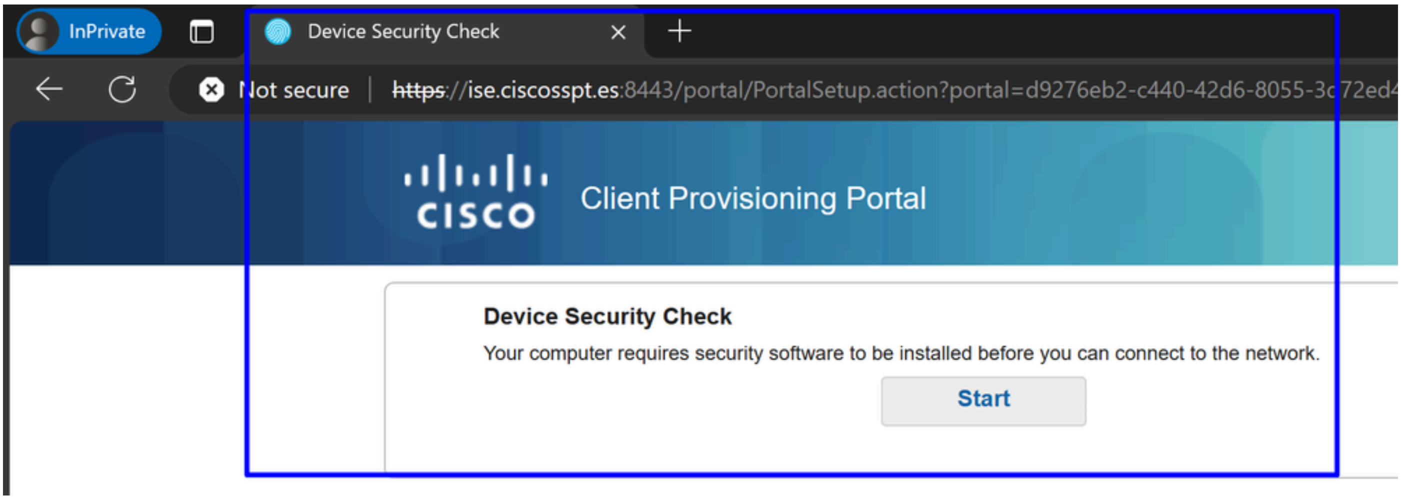
3. At this point, you get connected to the VPN, and mostly probably, you get redirected to ISE; if not, you can try navigating to **http:1.1.1.1**.



Cisco Secure Client

AnyConnect VPN

Connected: ISE_CSA - IKEv2 - Auto Select Nearest Location



https://ise.ciscosspt.es:8443/portal/PortalSetup.action?portal=d9276eb2-c440-42d6-8055-3c72ed4

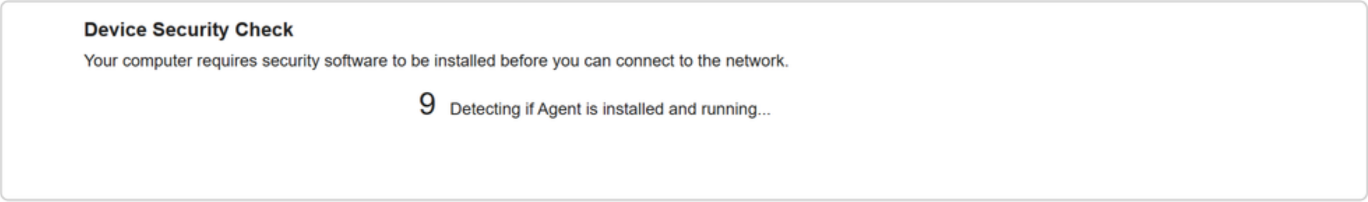
Client Provisioning Portal

Device Security Check

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

Note: At this point you are falling under the authorization - policy set CSA-Unknown-Compliance because you do not have the ISE Posture Agent installed on the machine, and you get redirected to the ISE Provisioning Portal to install the agent.

4. Click Start to proceed with the agent provisioning.

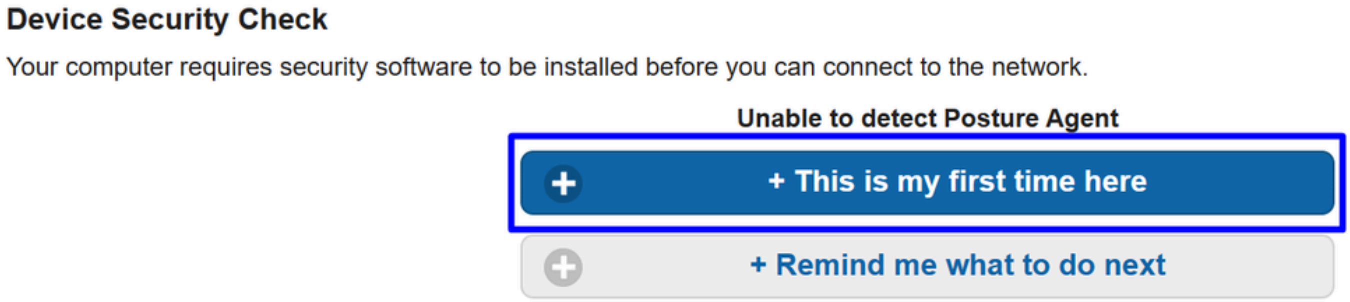


Device Security Check

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

9 Detecting if Agent is installed and running...

5. Click on **+ This is my first time here.**

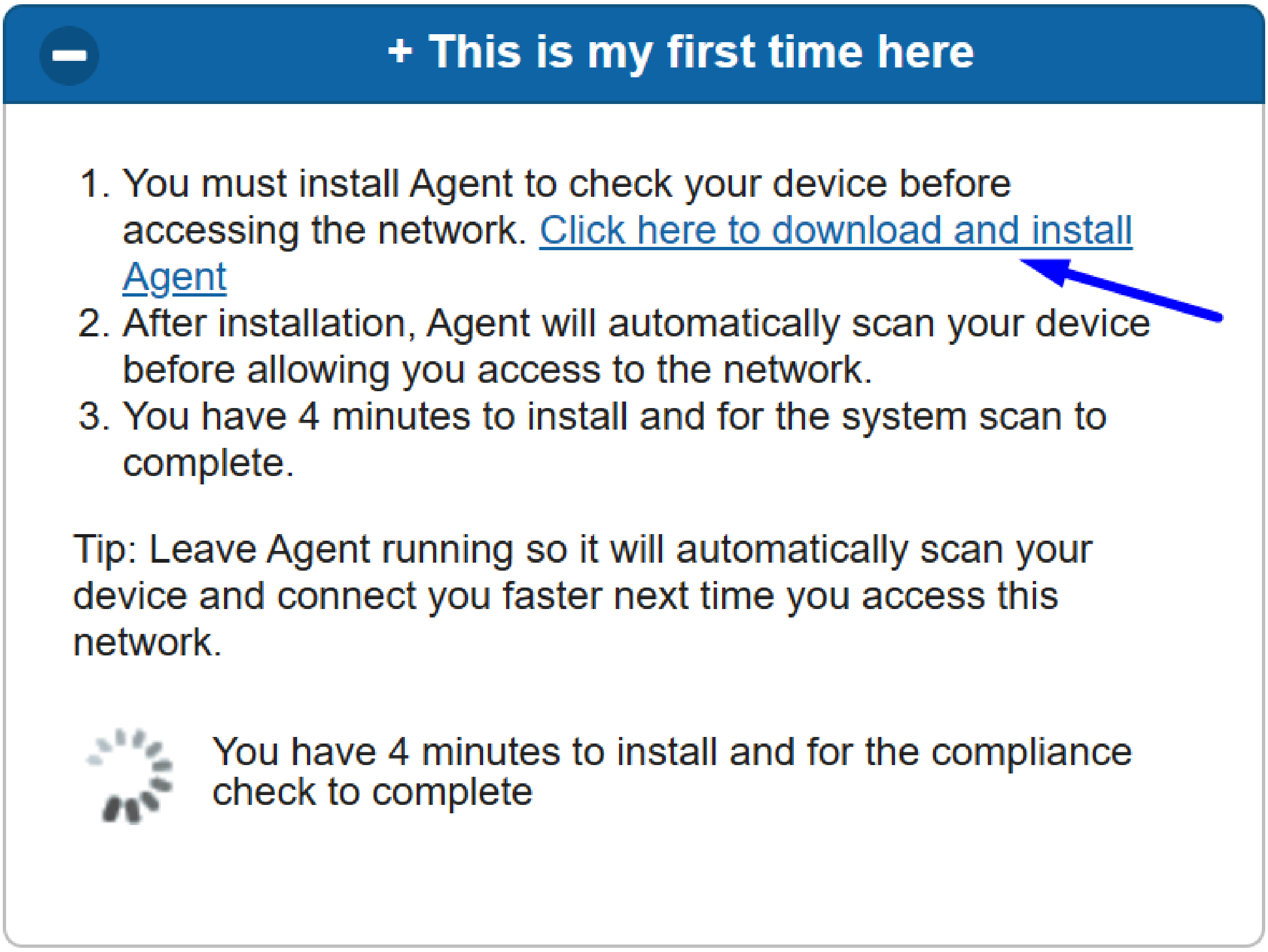


Device Security Check

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

Unable to detect Posture Agent

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

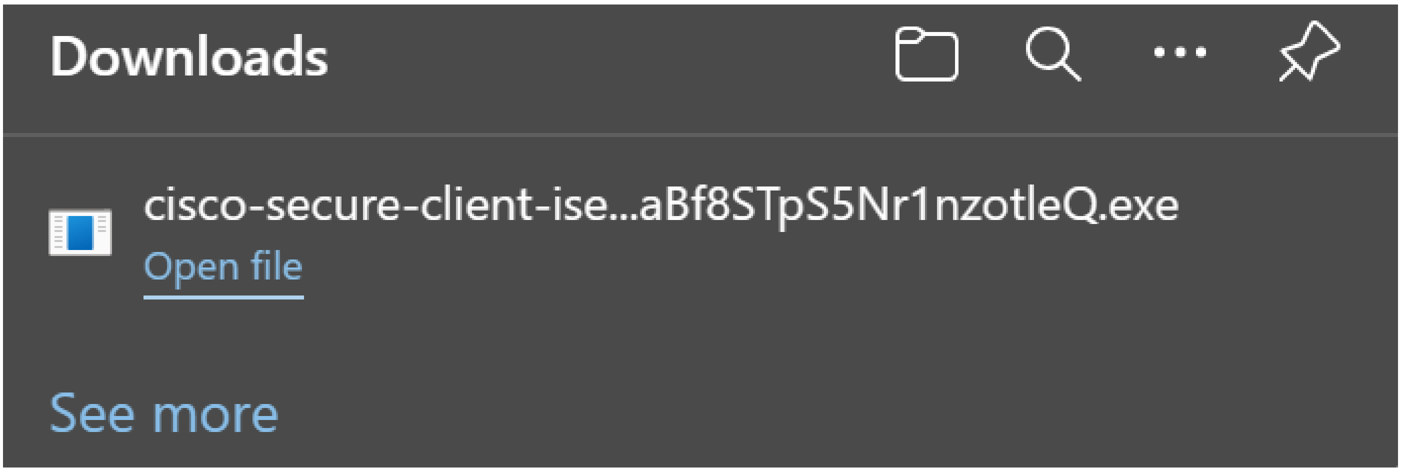


1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

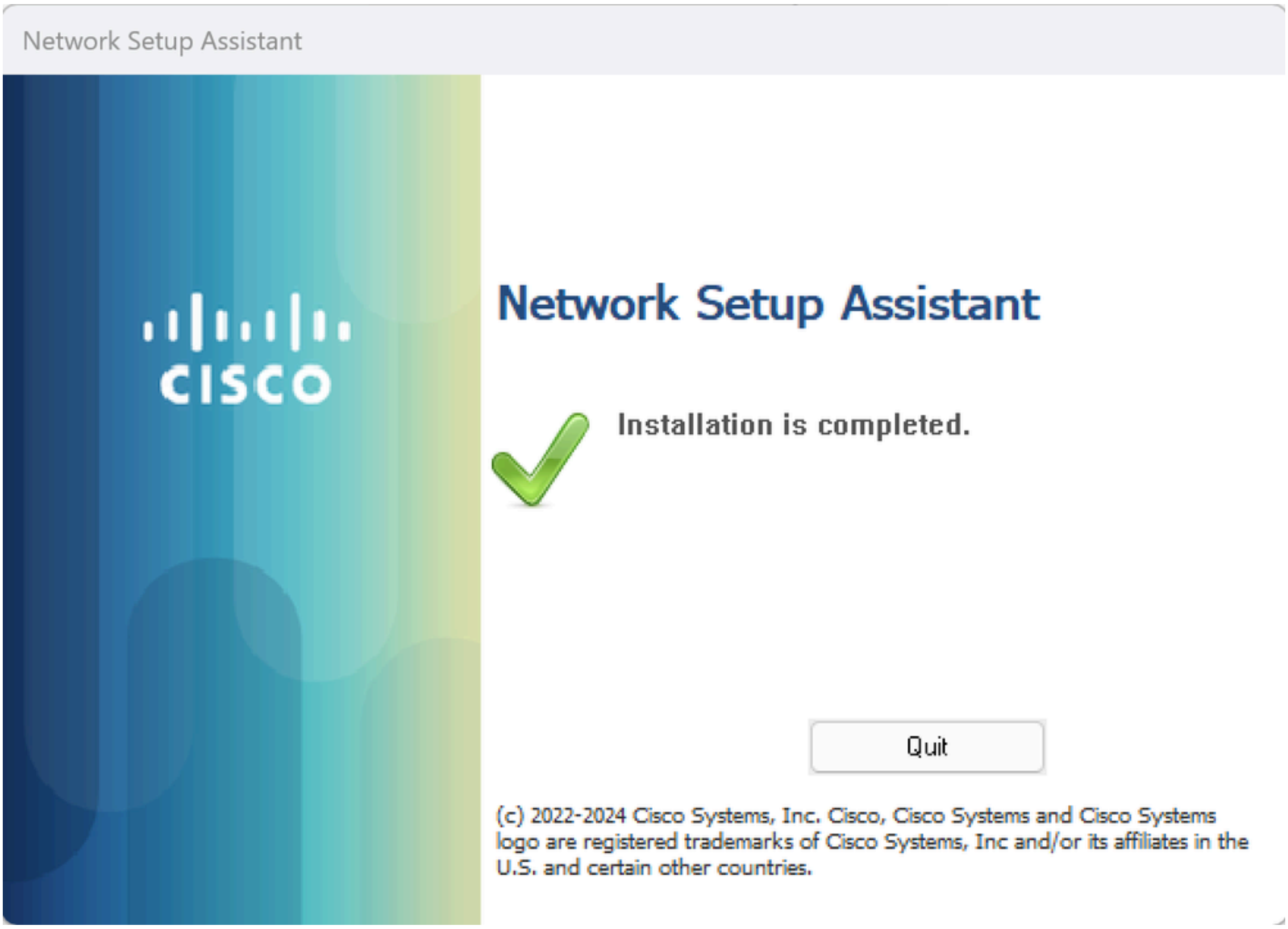
Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

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

7. Install the agent



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

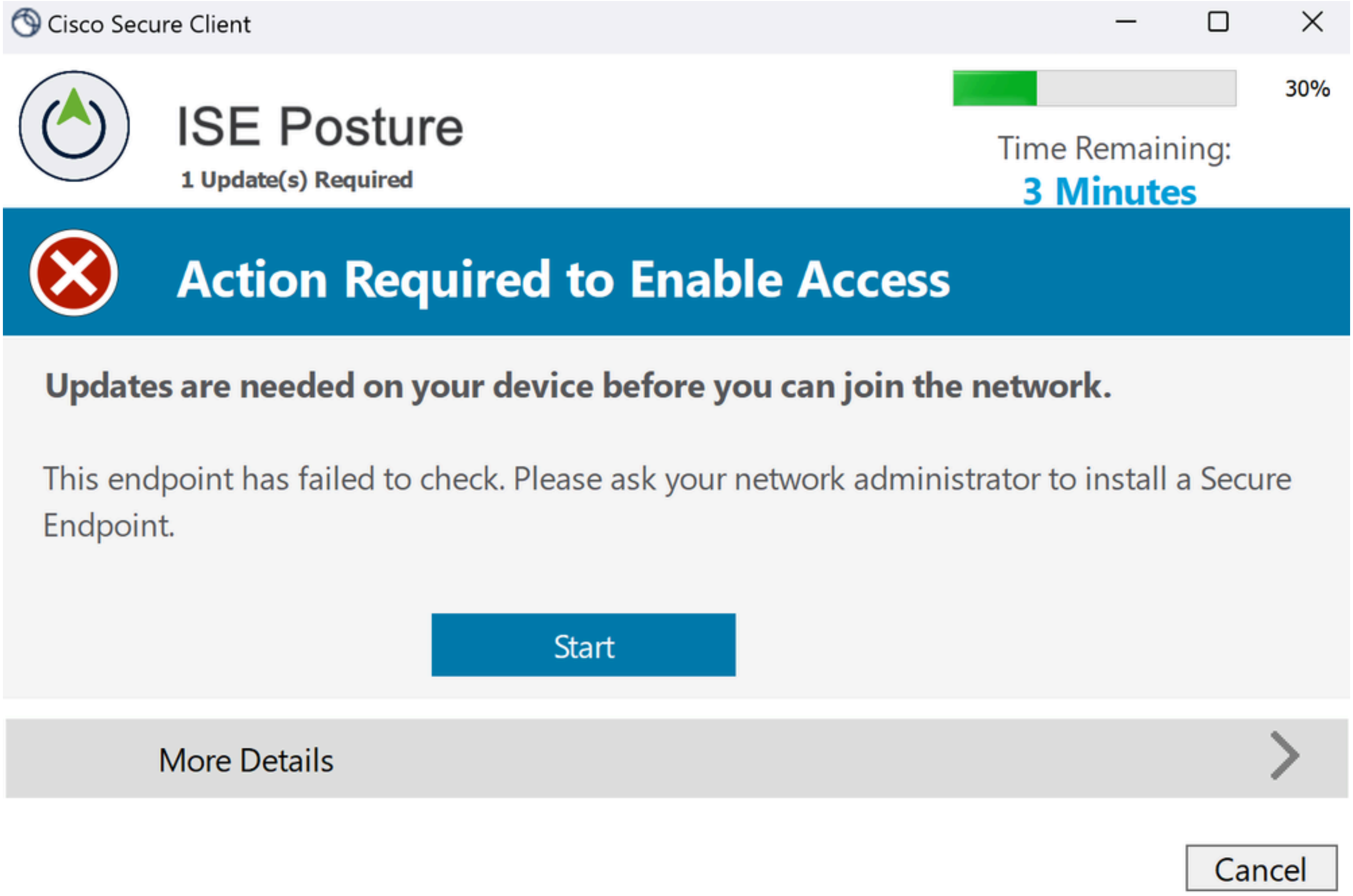


Network Setup Assistant

Installation is completed.

(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. After you install the agent, the ISE Posture begins verifying the machines current posture. If the policy requirements are not met, a pop-up appears to guide you towards compliance.



Cisco Secure Client

ISE Posture

1 Update(s) Required

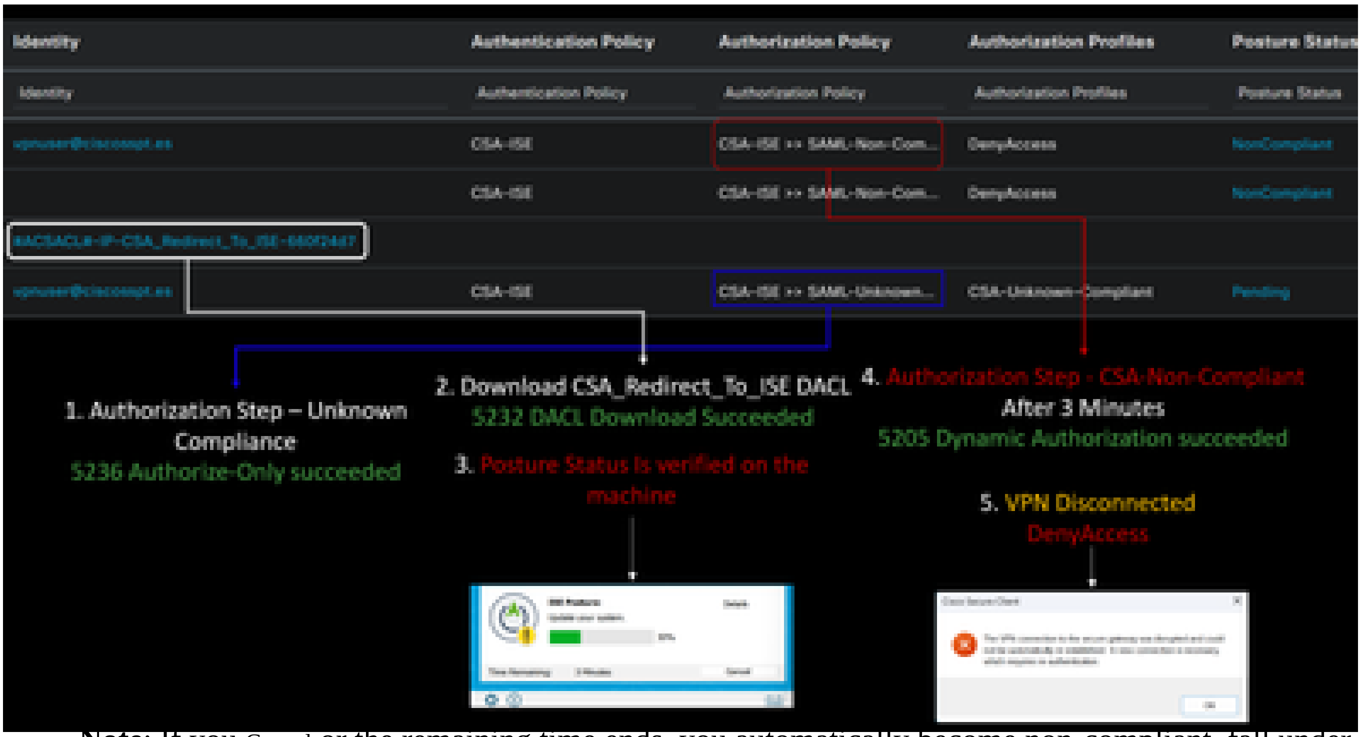
30%

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.



Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscoxpt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-66f2447				
vpnuser@ciscoxpt.es	CSA-ISE	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

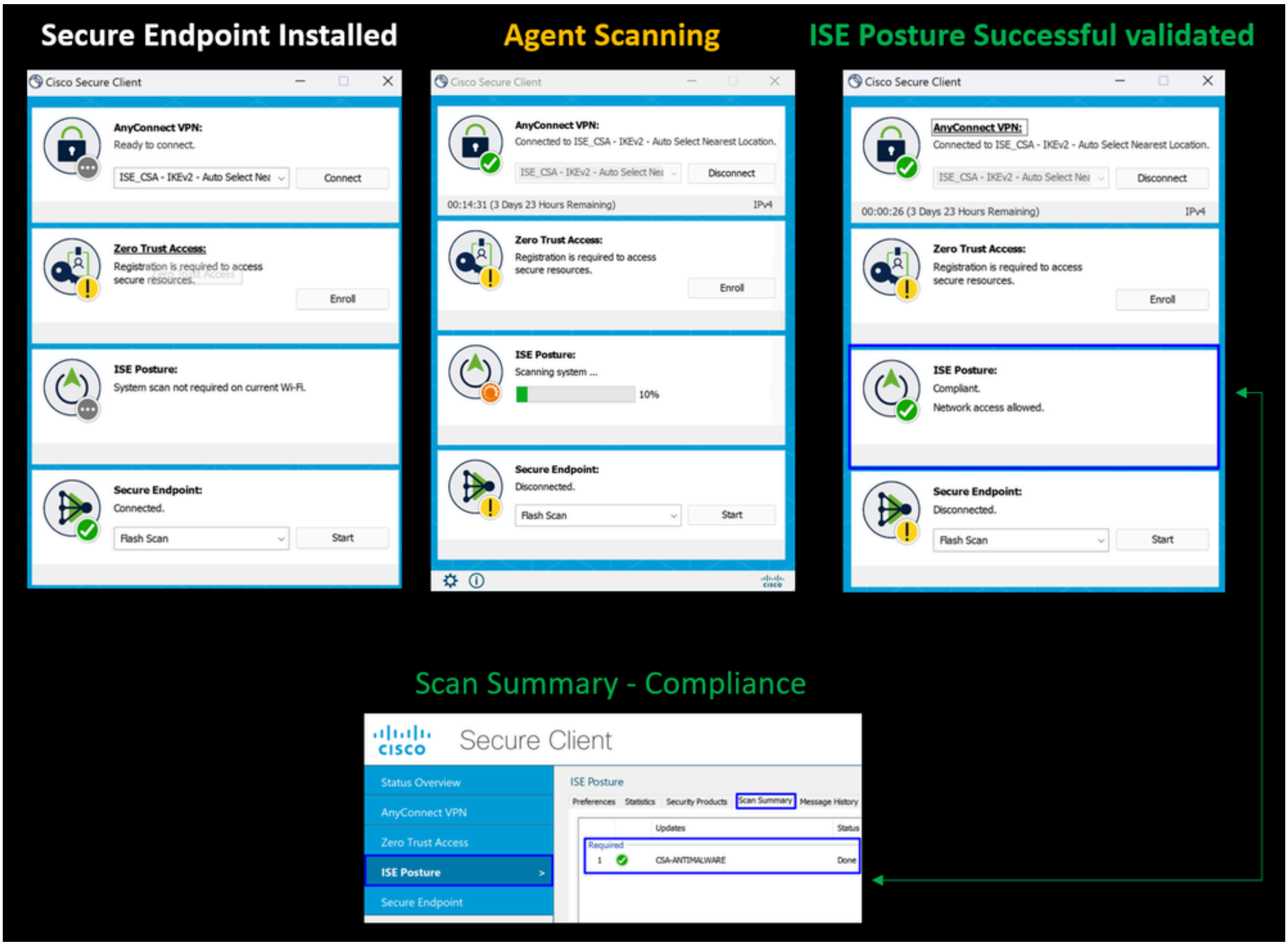
3. Posture Status is verified on the machine

4. Authorization Step - CSA-Non-Compliant
After 3 Minutes
5205 Dynamic Authorization succeeded

5. VPN Disconnected
DenyAccess

Note: If you Cancel or the remaining time ends, you automatically become non-compliant, fall under the authorization policy set CSA-Non-Compliance, and immediately get disconnected from the VPN.

9. Install the Secure Endpoint Agent and connect again to the VPN.


Secure Endpoint Installed
Agent Scanning
ISE Posture Successful validated
Scan Summary - Compliance

Cisco Secure Client

AnyConnect VPN: Ready to connect.
ISE_CSA - IKEv2 - Auto Select Nea | Connect

Zero Trust Access: Registration is required to access secure resources. | Enroll

ISE Posture: System scan not required on current Wi-Fi.

Secure Endpoint: Connected.
Flash Scan | Start

Cisco Secure Client

AnyConnect VPN: Connected to ISE_CSA - IKEv2 - Auto Select Nearest Location.
ISE_CSA - IKEv2 - Auto Select Nea | Disconnect
00:14:31 (3 Days 23 Hours Remaining) IPv4

Zero Trust Access: Registration is required to access secure resources. | Enroll

ISE Posture: Scanning system ... 10%

Secure Endpoint: Disconnected.
Flash Scan | Start

Cisco Secure Client

AnyConnect VPN: Connected to ISE_CSA - IKEv2 - Auto Select Nearest Location.
ISE_CSA - IKEv2 - Auto Select Nea | Disconnect
00:00:26 (3 Days 23 Hours Remaining) IPv4

Zero Trust Access: Registration is required to access secure resources. | Enroll

ISE Posture: Compliant. Network access allowed.

Secure Endpoint: Disconnected.
Flash Scan | Start

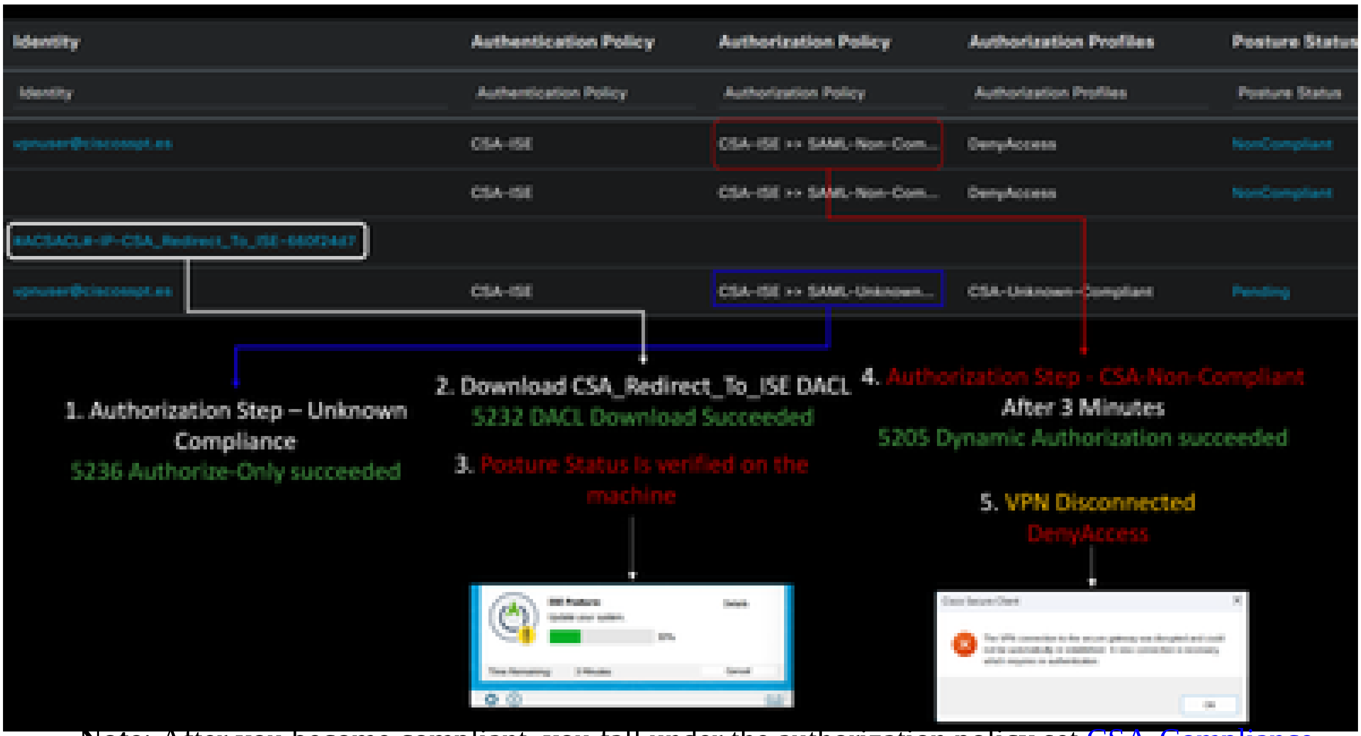
cisco Secure Client

Status Overview | AnyConnect VPN | Zero Trust Access | ISE Posture | Secure Endpoint

ISE Posture
Preferences | Statistics | Security Products | Scan Summary | Message History

	Updates	Status
Required		
1 ✓	CSA-ANTIMALWARE	Done

10. After the agent verifies the machine is in compliance, your posture changes to be on complaint and give access to all the resources on the network.



Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscoospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscoospt.es	CSA-ISE	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

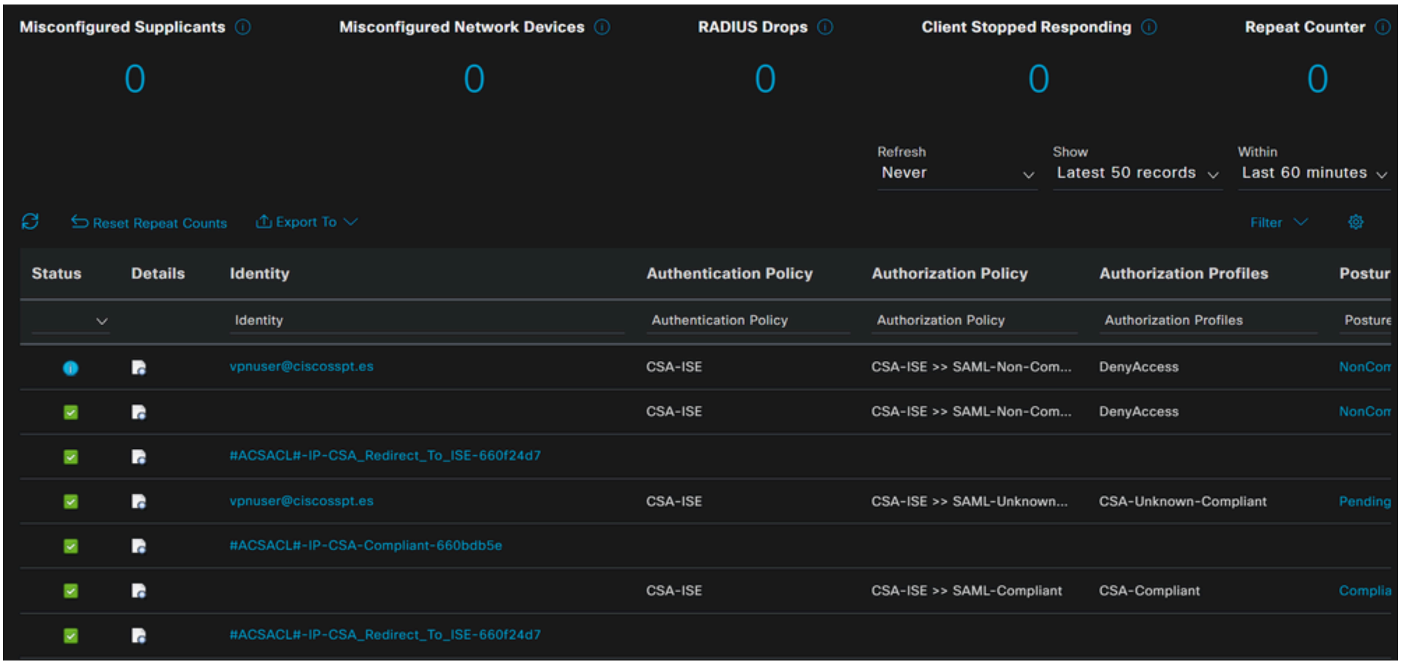
5. VPN Disconnected
DenyAccess

Note: After you become compliant, you fall under the authorization policy set CSA-Compliance, and you immediately have access to all your network resources.

How to Verify Logs in ISE

To verify the authentication outcome for a user, you have two examples of compliance and non-compliance. To review it in ISE, adhere to these instructions:

- Navigate to your ISE Dashboard
- Click on Operations > Live Logs



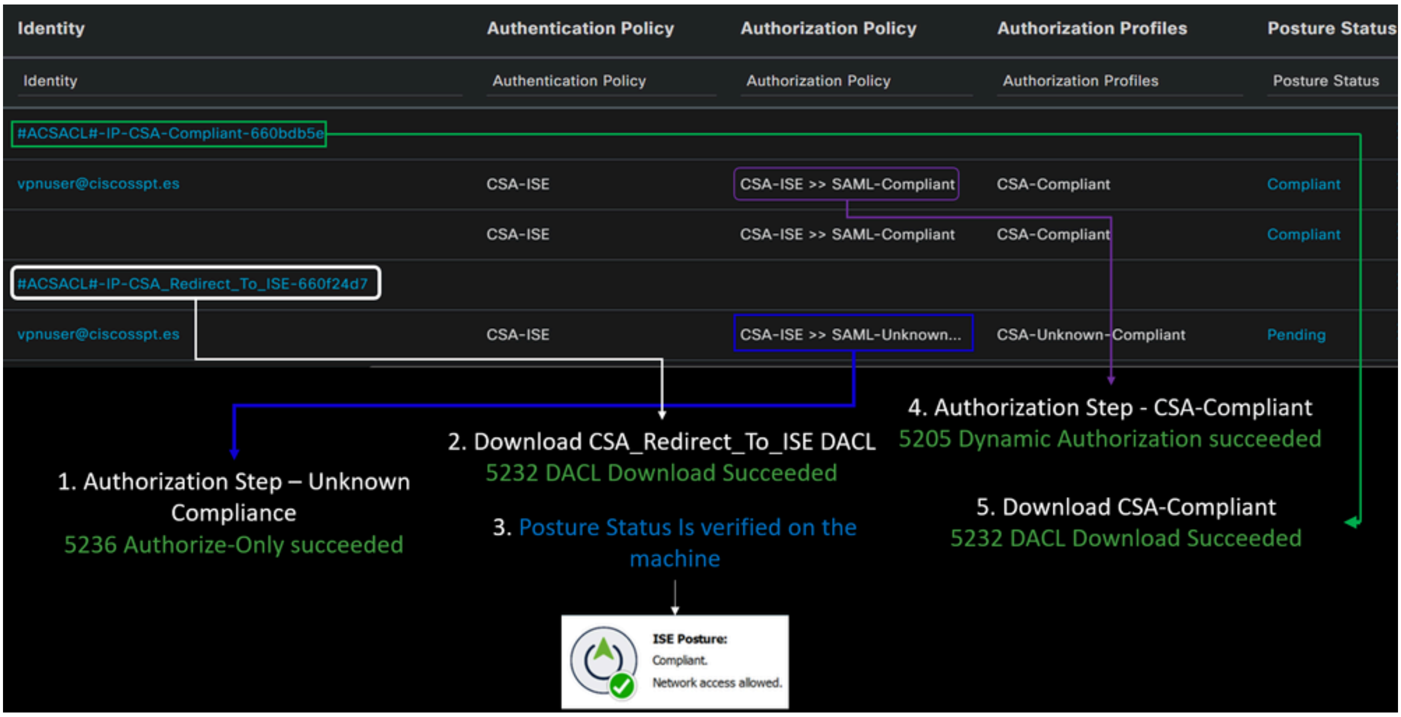
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never
Show: Latest 50 records
Within: Last 60 minutes

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Postur
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
ⓘ	🗎	vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
☑	🗎		CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
☑	🗎	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
☑	🗎	vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
☑	🗎	#ACSACL#-IP-CSA-Compliant-660bdb5e				
☑	🗎		CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
☑	🗎	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				

The next tho scenario demonstrates how successful compliance and Non-Compliance events are displayed under **Live Logs**:

Compliance



Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
#ACSACL#-IP-CSA-Compliant-660bdb5e				
vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Compliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscosspt.es	CSA-ISE	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

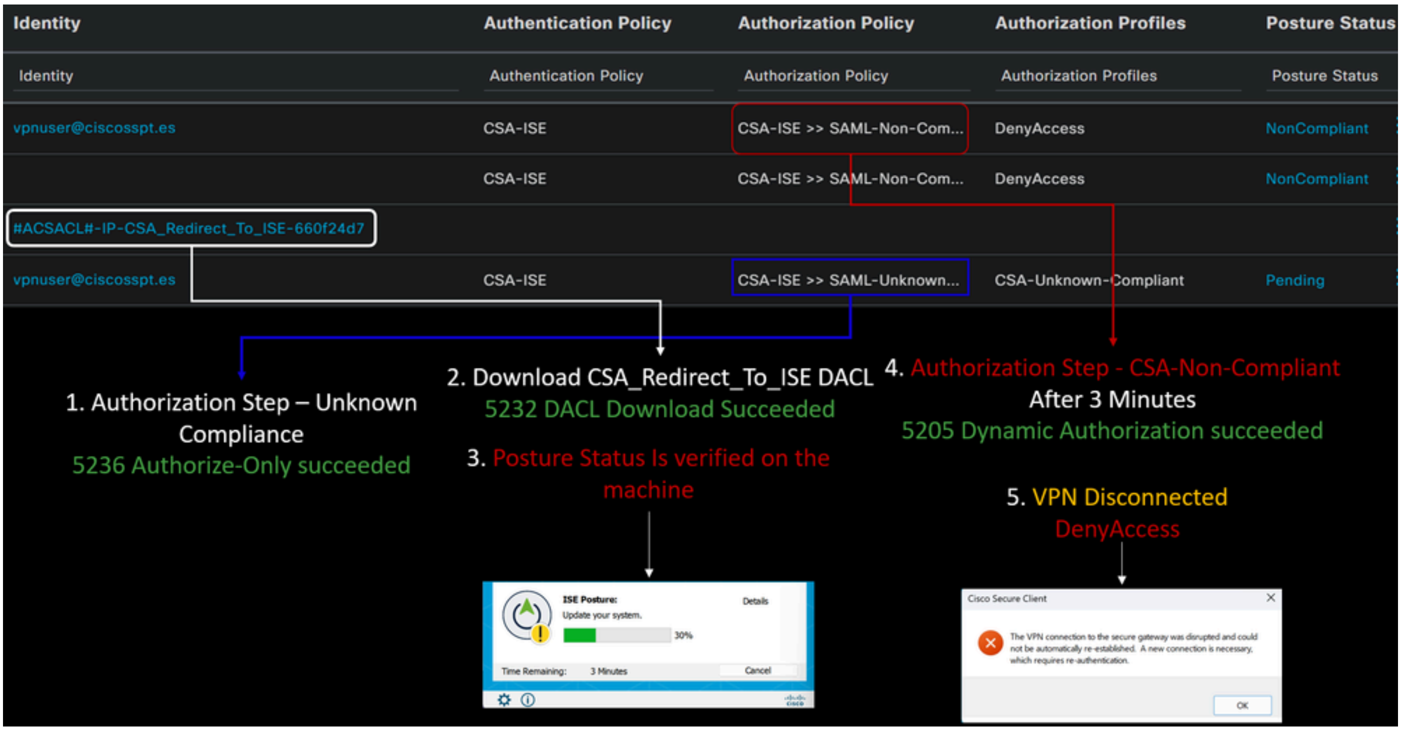
3. Posture Status Is verified on the machine

ISE Posture:
Compliant.
Network access allowed.

4. Authorization Step - CSA-Compliant
5205 Dynamic Authorization succeeded

5. Download CSA-Compliant
5232 DACL Download Succeeded

Non-Compliance



Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscosspt.es	CSA-ISE	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

ISE Posture:
Update your system.
30%
Time Remaining: 3 Minutes

4. Authorization Step - CSA-Non-Compliant
After 3 Minutes
5205 Dynamic Authorization succeeded

5. VPN Disconnected
DenyAccess

Cisco Secure Client

The VPN connection to the secure gateway was disrupted and could not be automatically re-established. A new connection is necessary, which requires re-authentication.

First Steps with Secure Access and ISE Integration

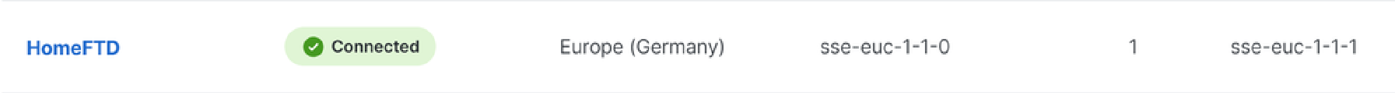
In the next example, Cisco ISE is under network 192.168.10.0/24, and the configuration of the networks reachable through the tunnel needs to be added under the tunnel configuration.

Step 1: Verify your Tunnel configuration:

To verify this, please navigate to your Secure Access Dashboard.

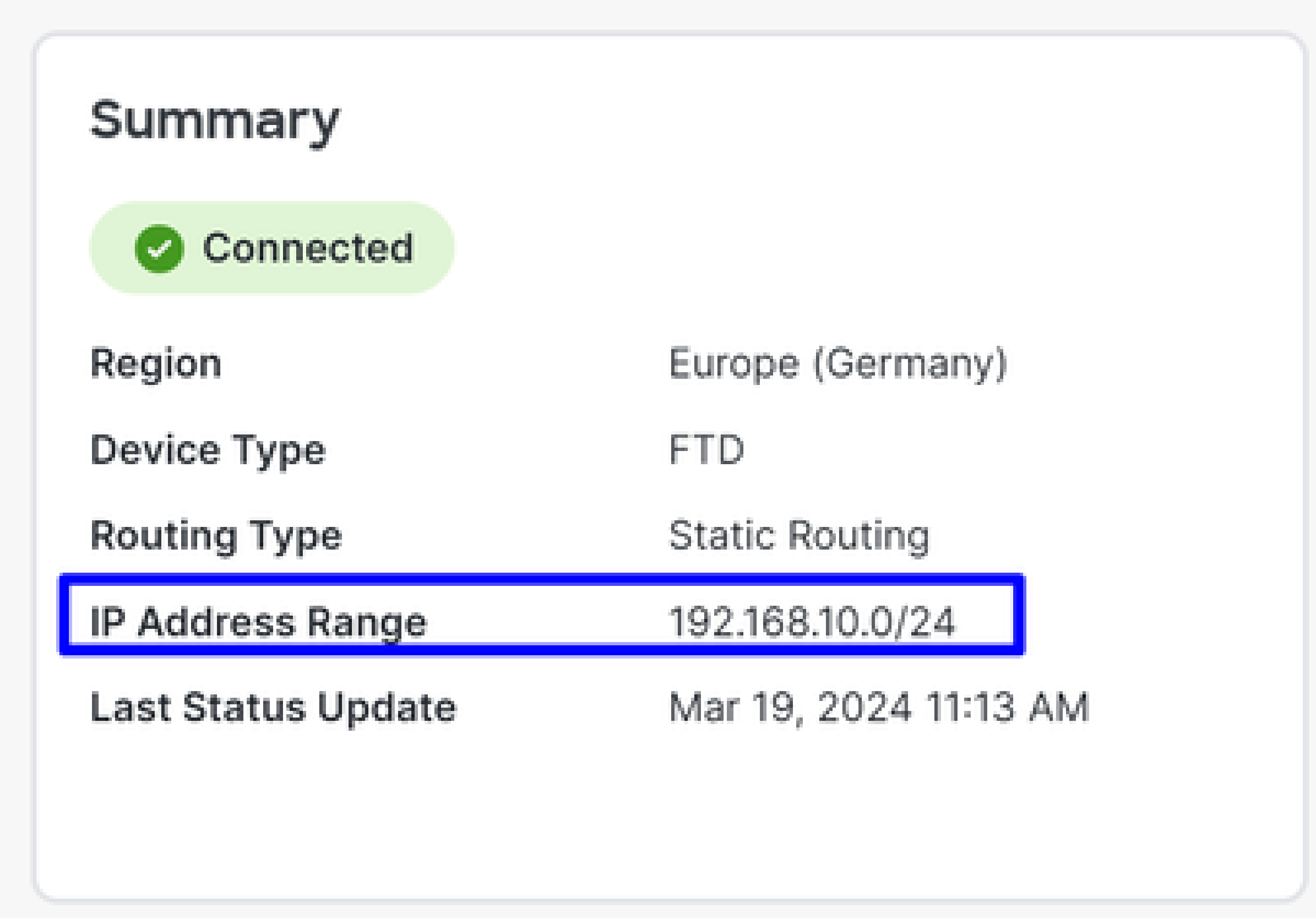
- Click on **Connect > Network Connections**

- Click on **Network Tunnel Groups** > Your Tunnel



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

- Under summary, verify the tunnel has configured the address space where your Cisco ISE is:



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: Permit the traffic on your firewall.

To permit Secure Access to use your ISE device for Radius authentication, you need to have configured a rule from Secure Access to your network with the Radius ports required:

Rule	Source	Destination	Destination Port
ISE to Secure Access **Management Pool**	ISE_Server	Management IP Pool (RA-VPN)	**COA** UDP 1700 (Default Port)
Secure Access Management IP Pool to ISE	Management IP Pool	ISE_Server	**Authentication, Authorization** UDP 1812 (Default Port)

			Accounting UDP 1813 (Default Port)
Secure Access Endpoint IP Pool to ISE	Endpoint IP Pool	ISE_Server	**Provisioning Portal** TCP 8443 (Default Port)
Secure Access Endpoint IP Pool to DNS SERVER	Endpoint IP Pool	DNS Server	**DNS** UDP and TCP 53

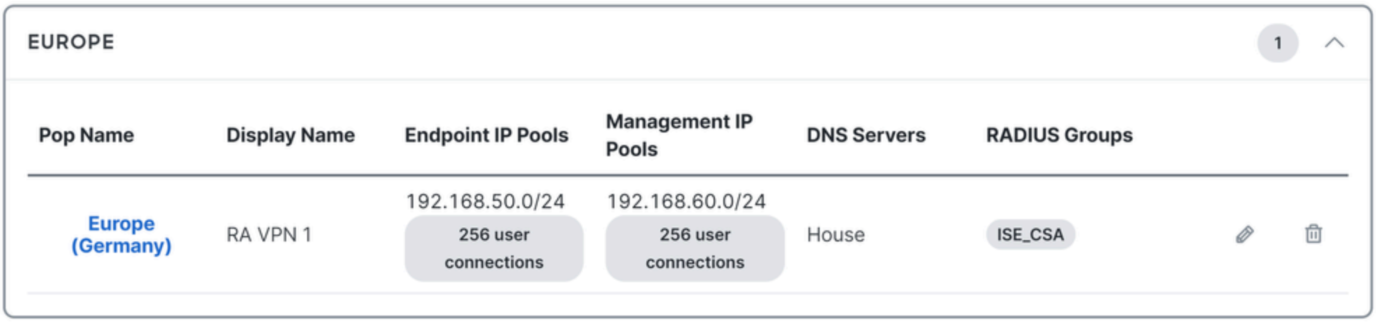
Note: If you want to know more ports related to ISE, check the User Guide - Port Reference.

Note: A DNS Rule is needed if you have configured your ISE to be discovered through a name, such as ise.ciscosspt.es

Management Pool and Endpoint IP Pools

To verify your Management and Endpoint IP Pool, navigate to your Secure Access Dashboard:

- Click on **Connect > End User Connectivity**
- Click on Virtual Private Network
- Under **Manage IP Pools**
- Click on **Manage**



EUROPE 1

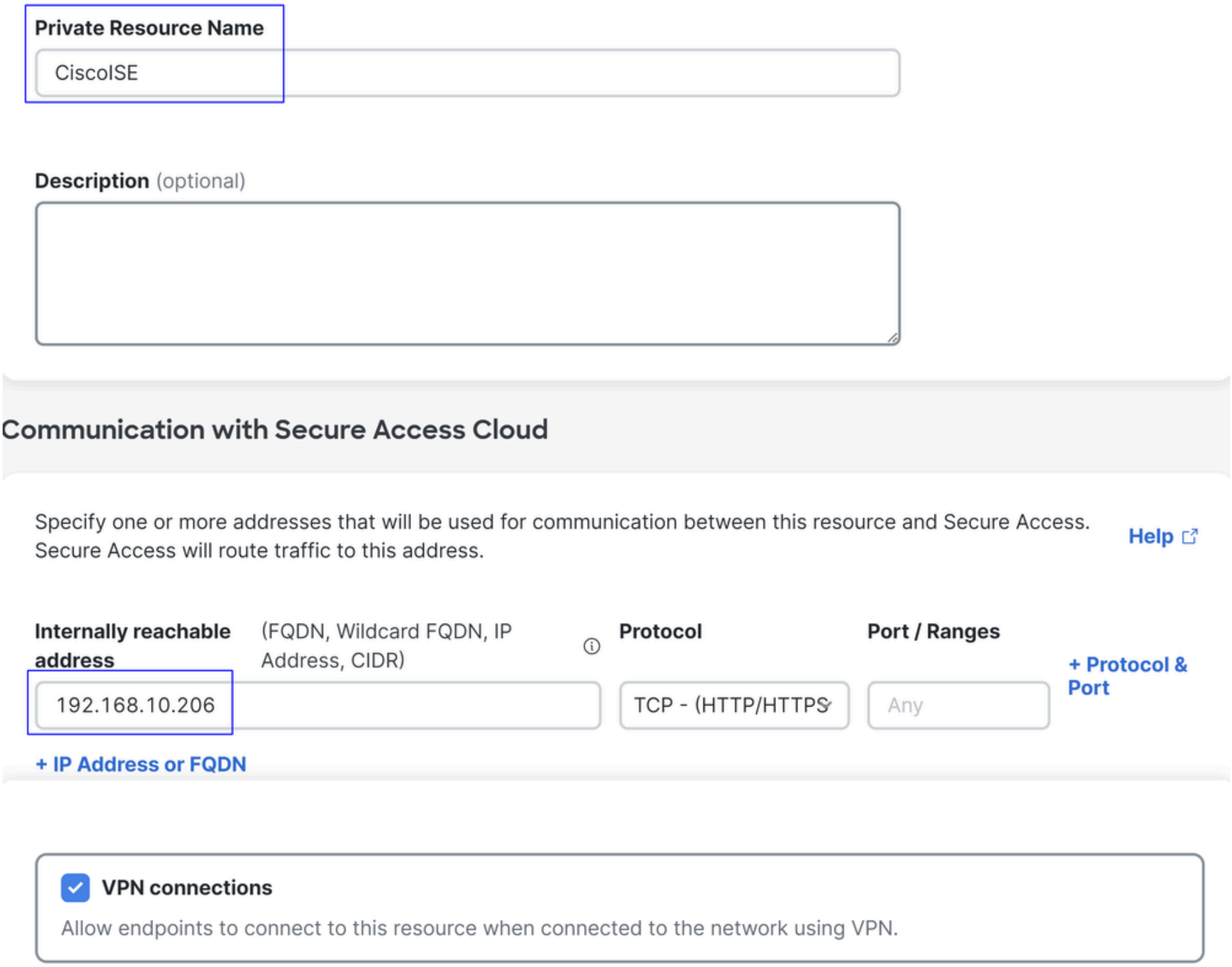
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA

Step3: Verify your ISE is configured under Private Resources

To permit the users connected through the VPN to navigate to **ISE Provisioning Portal**, you need to be sure you have configured your device as a Private Resource to provide access, which is used to permit the auto-provisioning of the ISE Posture Module through the VPN.

To verify that you have ISE configured correctly, navigate to your Secure Access Dashboard:

- Click on **Resources > Private Resources**
- Click the ISE Resource



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.

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)	Protocol	Port / Ranges
192.168.10.206	TCP - (HTTP/HTTPS	Any

☑ **VPN connections**

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

If needed, you can restrict the rule to the provisioning portal port (8443).

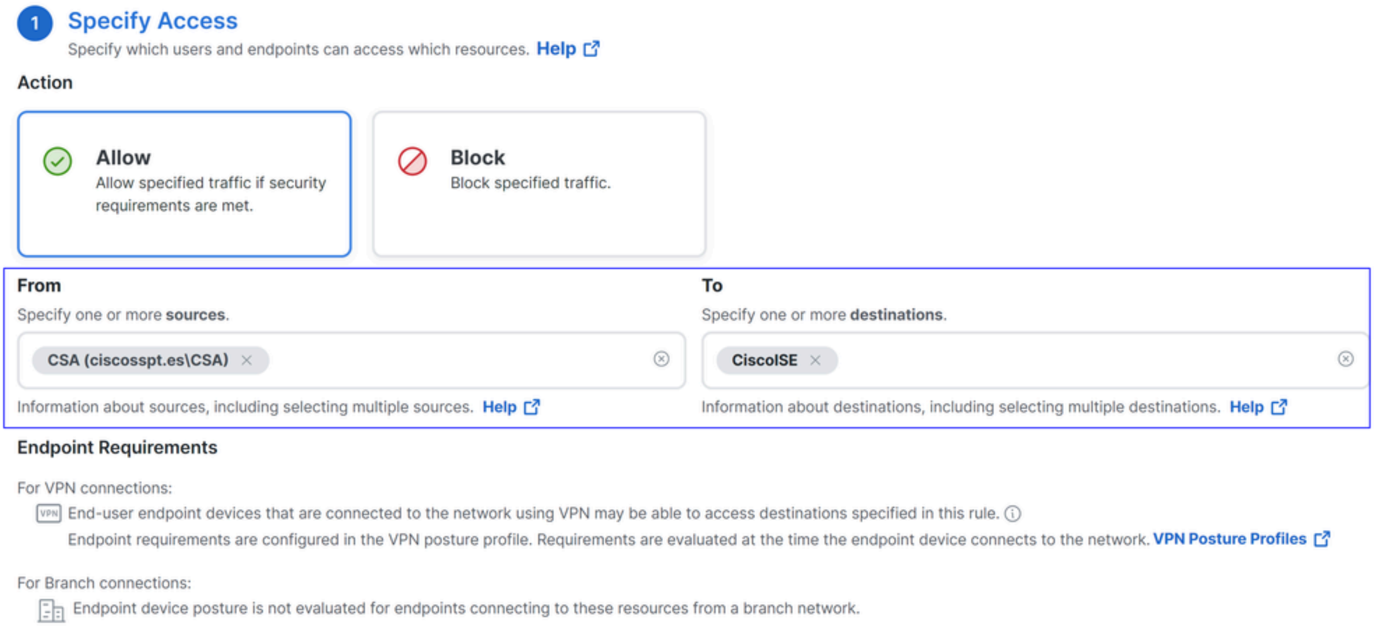
Note: Be sure you have marked the checkbox for VPN connections.

Step4: Permit ISE Access Under the Access Policy

To permit the users connected through the VPN to navigate to **ISE Provisioning Portal**, you need to be sure you have configured an **Access Policy** to permit the users configured under that rule to access the Private Resource configured in Step3.

To verify that you have ISE configured correctly, navigate to your Secure Access Dashboard:

- Click on **Secure** > **Access Policy**
- Click the rule configured to permit access to the VPN users to ISE



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**.
CSA (ciscosspt.es\CSA) ×
Information about sources, including selecting multiple sources. Help

To
Specify one or more **destinations**.
CiscoISE ×
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

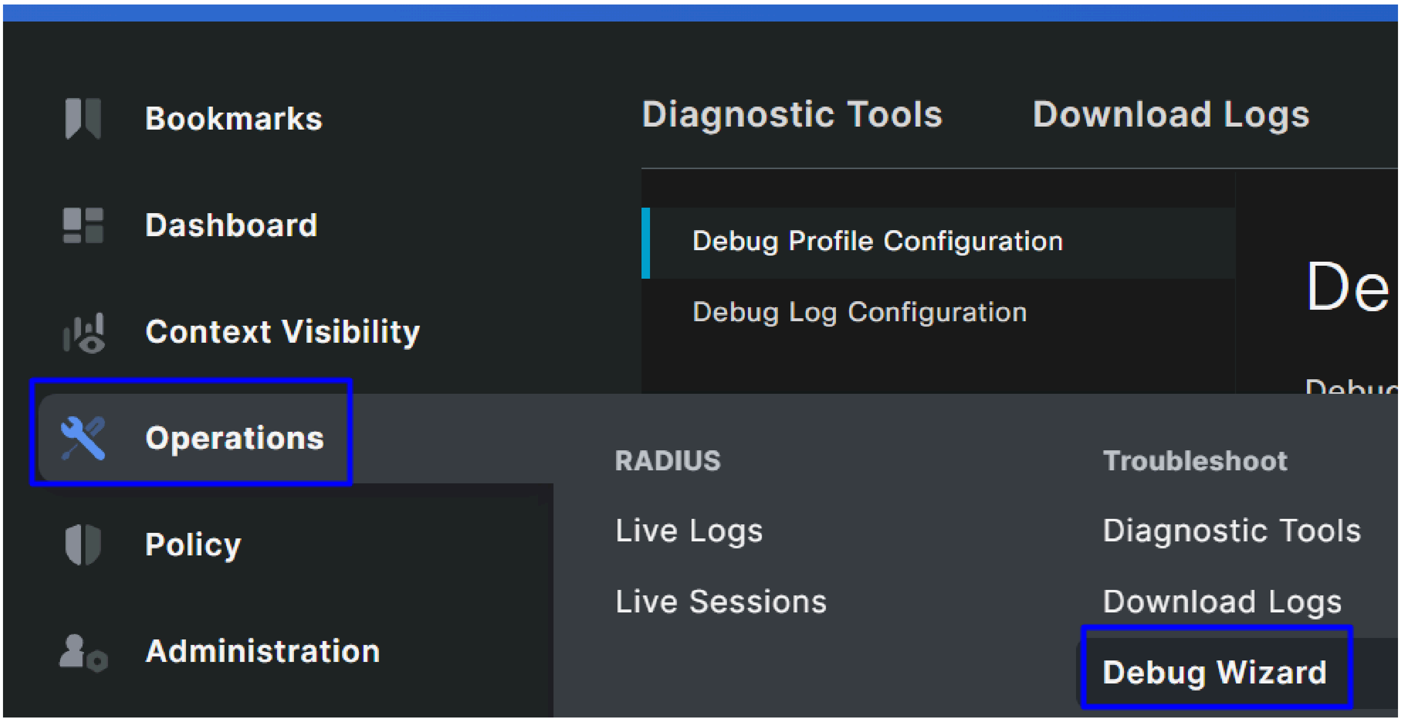
For Branch connections:
Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Troubleshoot

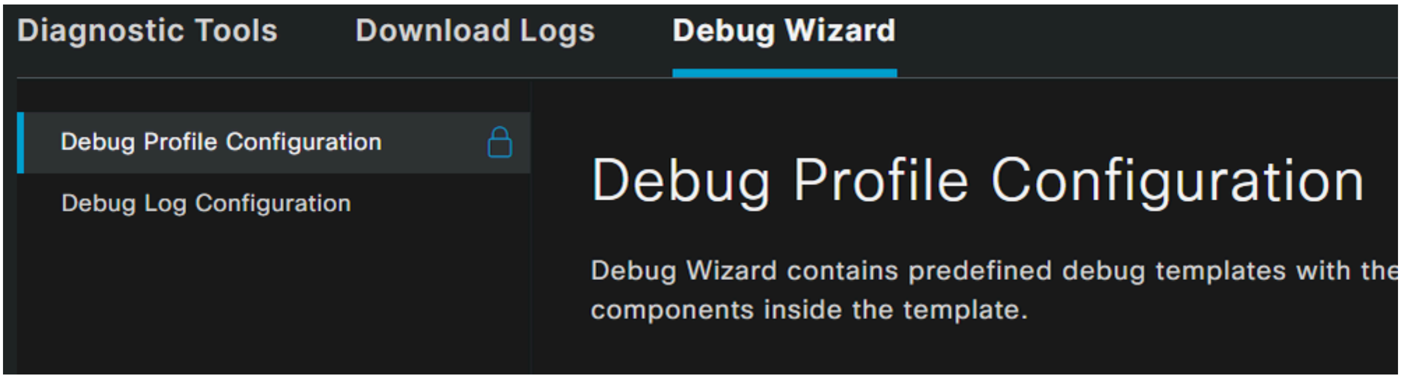
How to Download ISE Posture Debug Logs

To download ISE Logs to verify an issue related to posture, please proceed with the next steps:

- Navigate to your ISE Dashboard
- Click on Operations > Troubleshoot > Debug Wizard



- Click on Debug Profile Configuration



Diagnostic Tools

Download Logs

Debug Wizard

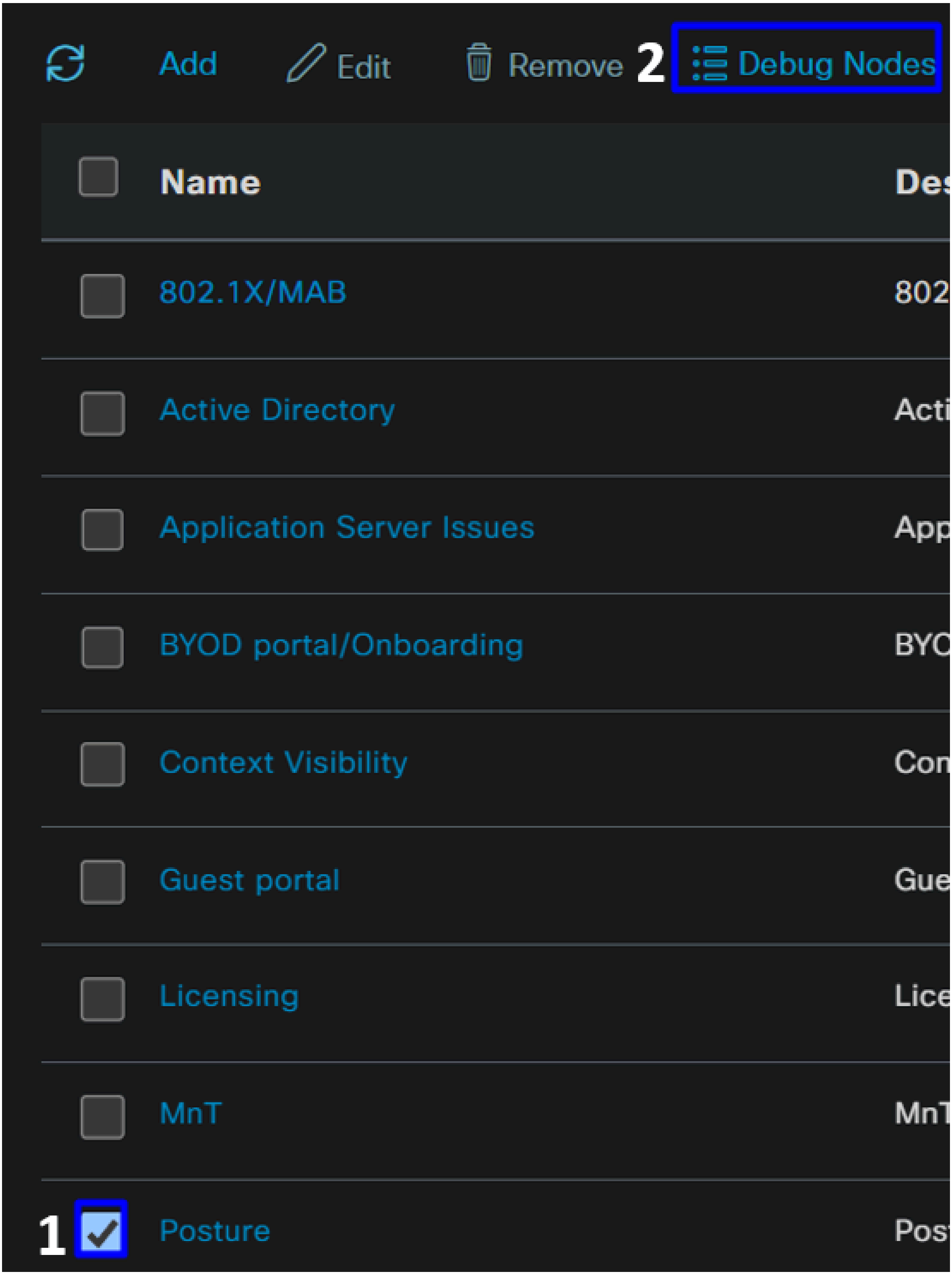
Debug Profile Configuration

Debug Log Configuration

Debug Profile Configuration

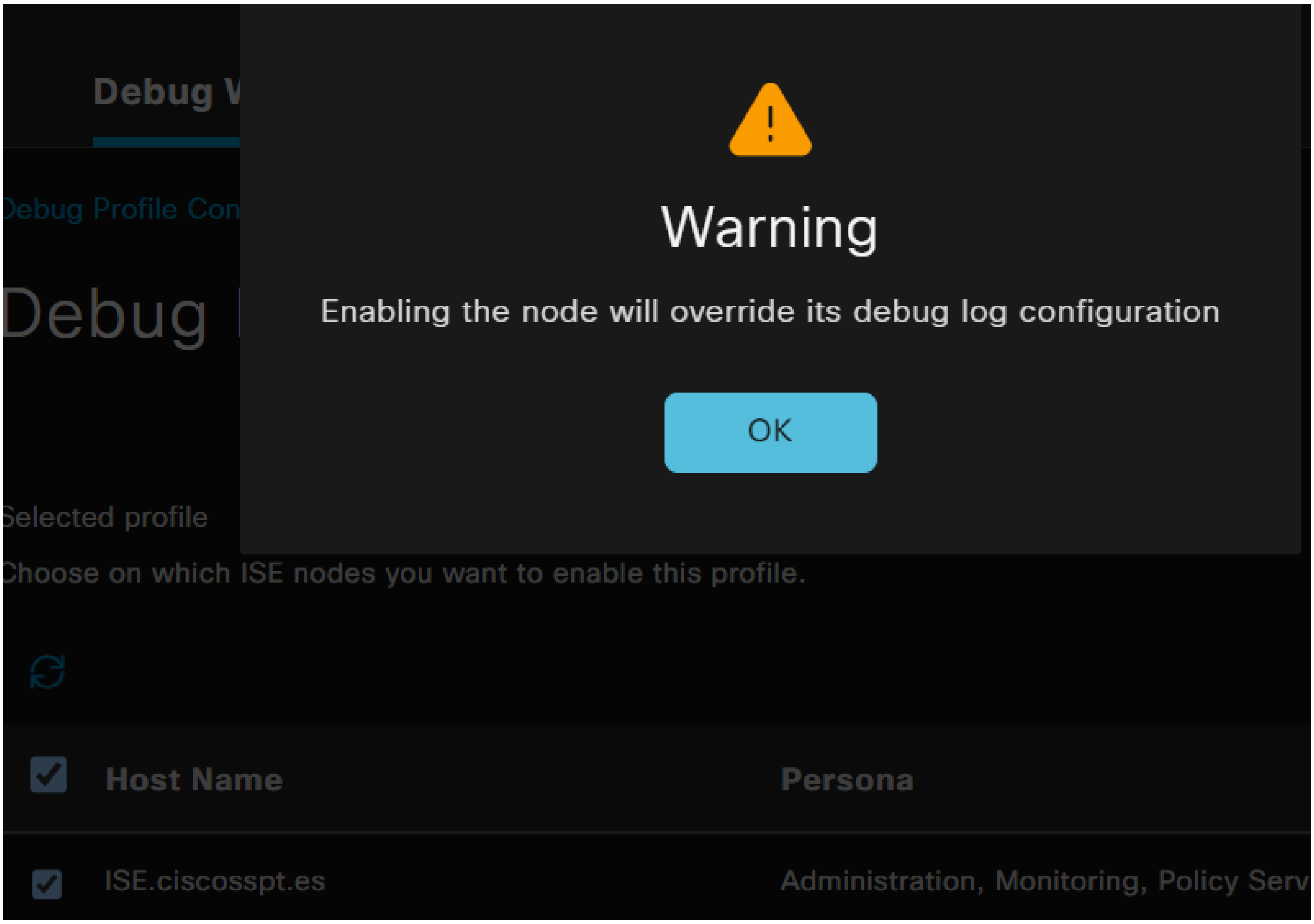
Debug Wizard contains predefined debug templates with the
components inside the template.

- Mark the checkbox for **Posture** > **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
☑	Posture	Pos

- Mark the checkbox for the ISE nodes on which you are to enable debug mode to troubleshoot your problem



Warning

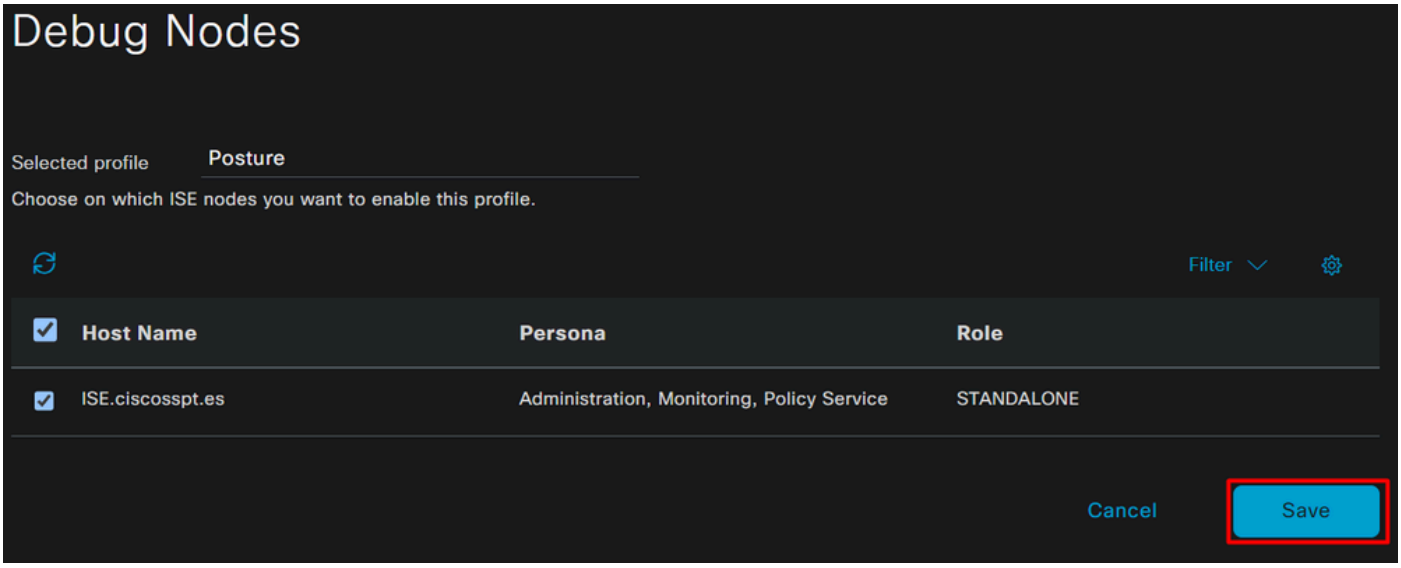
Enabling the node will override its debug log configuration

Selected profile

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

☑	Host Name	Persona
☑	ISE.ciscosspt.es	Administration, Monitoring, Policy Serv

- Click Save



Debug Nodes

Selected profile Posture

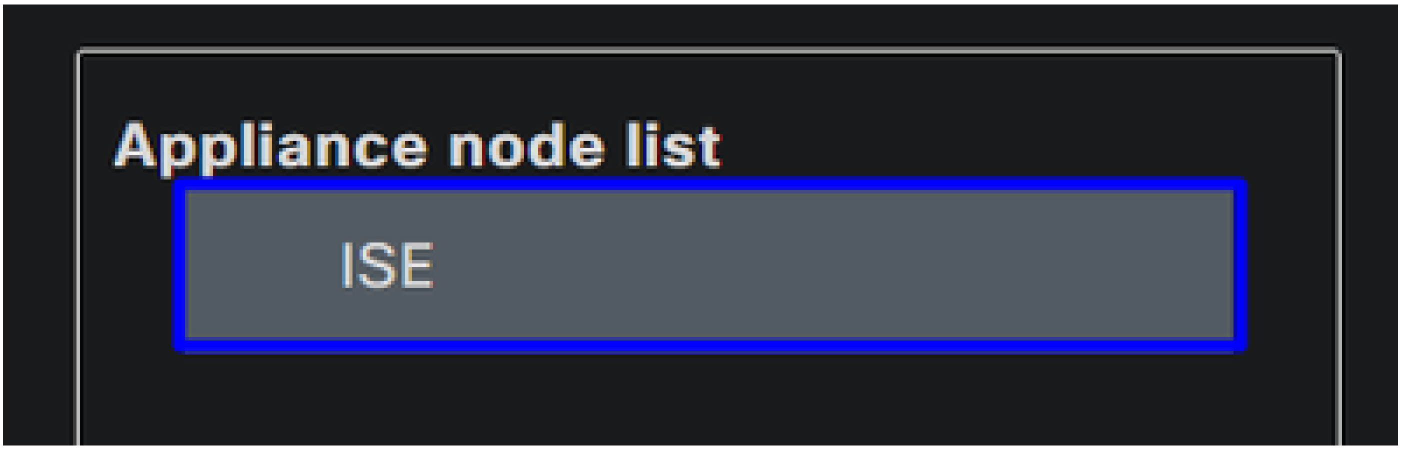
Choose on which ISE nodes you want to enable this profile.

☑	Host Name	Persona	Role
☑	ISE.ciscosspt.es	Administration, Monitoring, Policy Service	STANDALONE

Caution: After this point, you must start reproducing your issue; **the debug logs can affect the performance of your device.**

After you get the issue reproduced, proceed with the next steps:

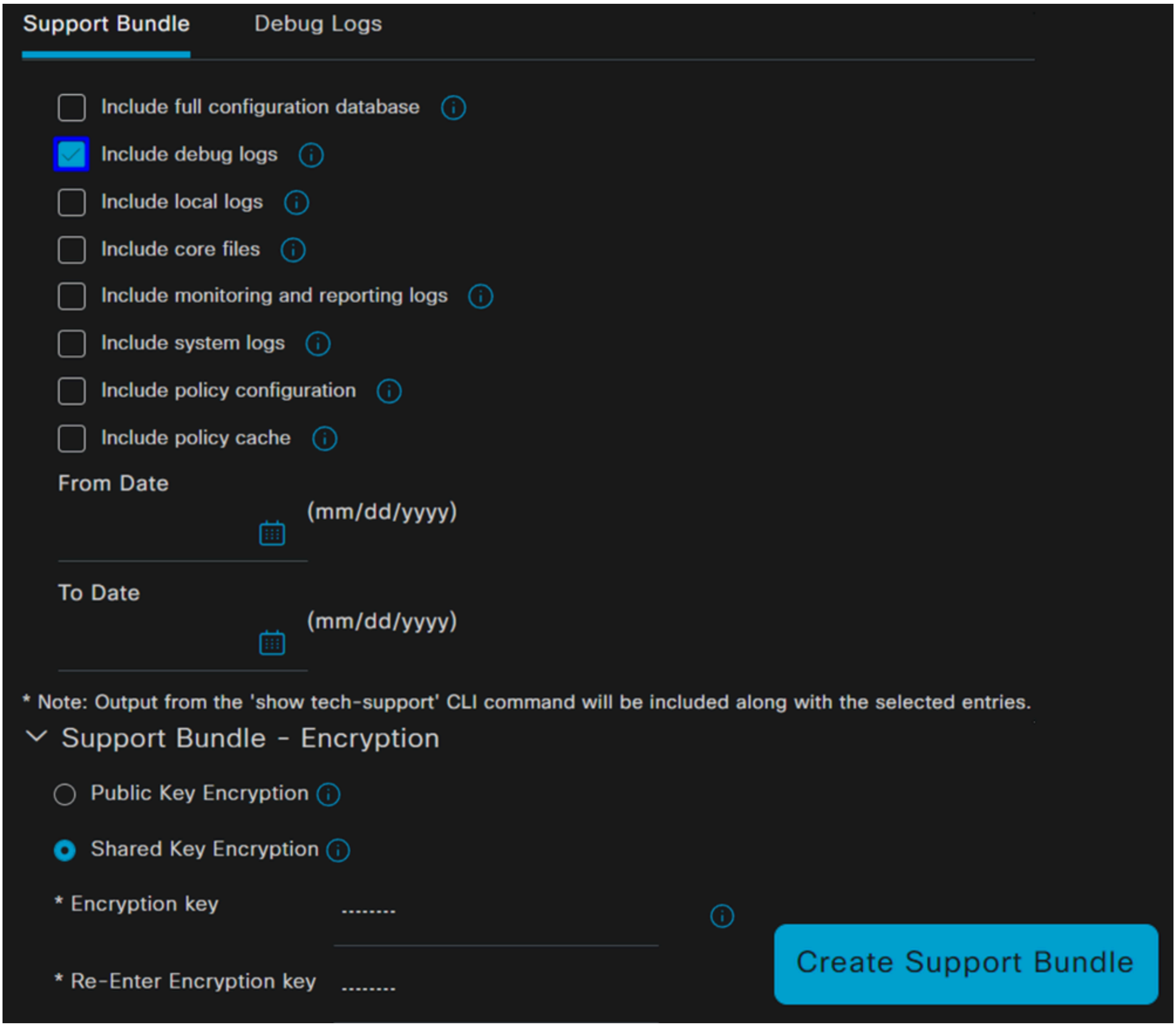
- Click on Operations > Download Logs
- Choose the node from where you want to take the logs



Appliance node list

ISE

- Under **Support Bundle**, choose the next options:



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

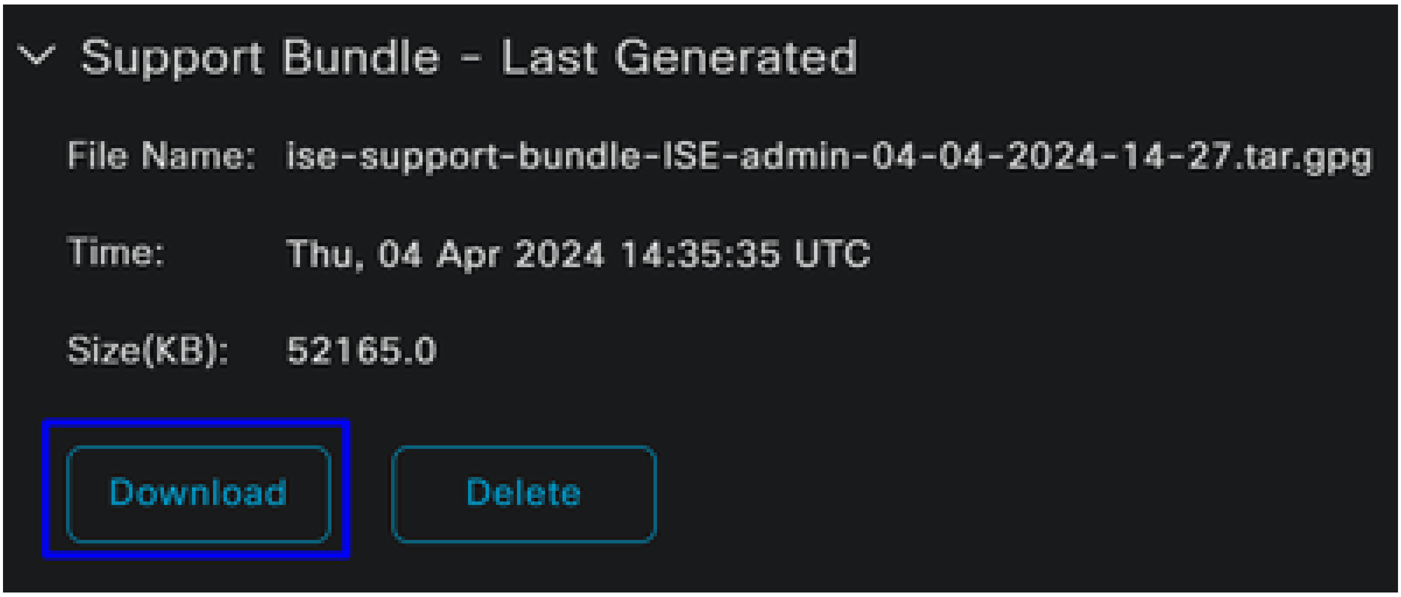
○ Public Key Encryption

● Shared Key Encryption

* Encryption key ....

* Re-Enter Encryption key ....

- Include debug logs
- Under **Support Bundle Encryption**
  - **Shared Key Encryption**
    - Fill **Encryption key** and **Re-Enter Encryption key**
- Click **Create Support Bundle**
- Click **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

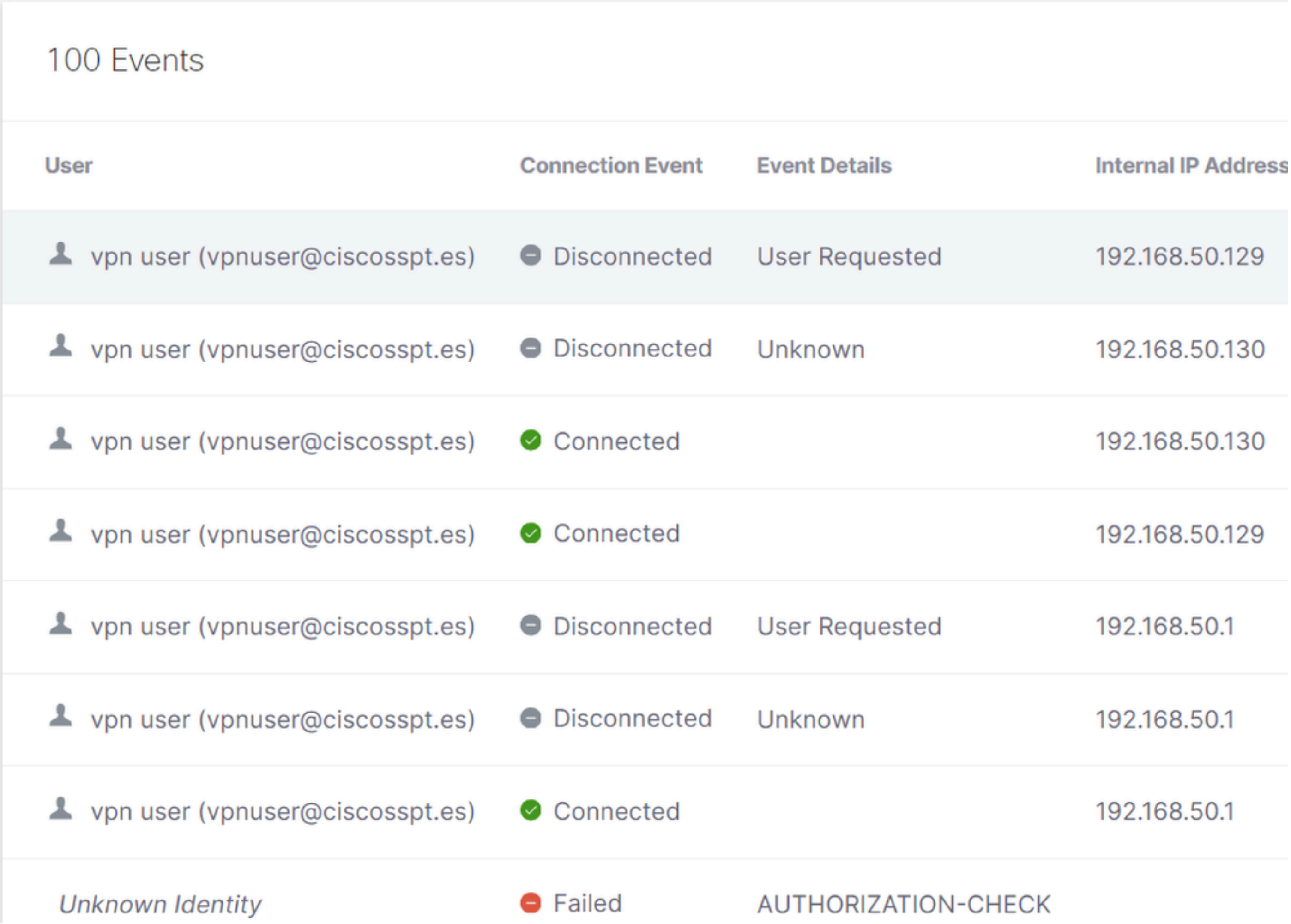
Size(KB): 52165.0

Warning: Disable the debug mode enabled on the step, Debug Profile Configuration

How to Verify Secure Access Remote Access Logs

Navigate to your Secure Access Dashboard:

- Click on Monitor > Remote Access Logs



100 Events

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

Generate DART Bundle on Secure Client

To generate DART Bundle on your machine, verify the next article:

[Cisco Secure Client Diagnostic and Reporting Tool (DART)]

Note: Once you have collected the logs indicated in the troubleshooting section, please open a case with **TAC** to proceed with the analysis of the information.

Related Information

- Cisco Technical Support & Downloads
- Secure Access Documentation and User Guide
- Cisco Secure Client Software Download
- Cisco Identity Services Engine Administrator Guide, Release 3.3