Configurazione di Secure Access per RA-VPNaaS con Duo SSO e valutazione della postura con ISE

Sommario

Introduzione

Questo documento descrive come configurare la valutazione della postura per gli utenti VPN ad accesso remoto con Identity Service Engine (ISE) e Secure Access con Duo.

Prerequisiti

- Configura provisioning utenti su accesso protetto
- Configurazione di Duo SSO con proxy di autenticazione o IDP di terze parti
- Cisco ISE connesso per un accesso sicuro tramite tunnel

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Service Engine
- Accesso sicuro
- Cisco Secure Client
- Guida all'autenticazione a due fattori - Duo Security
- Postura ISE
- Autenticazione, autorizzazione e accounting

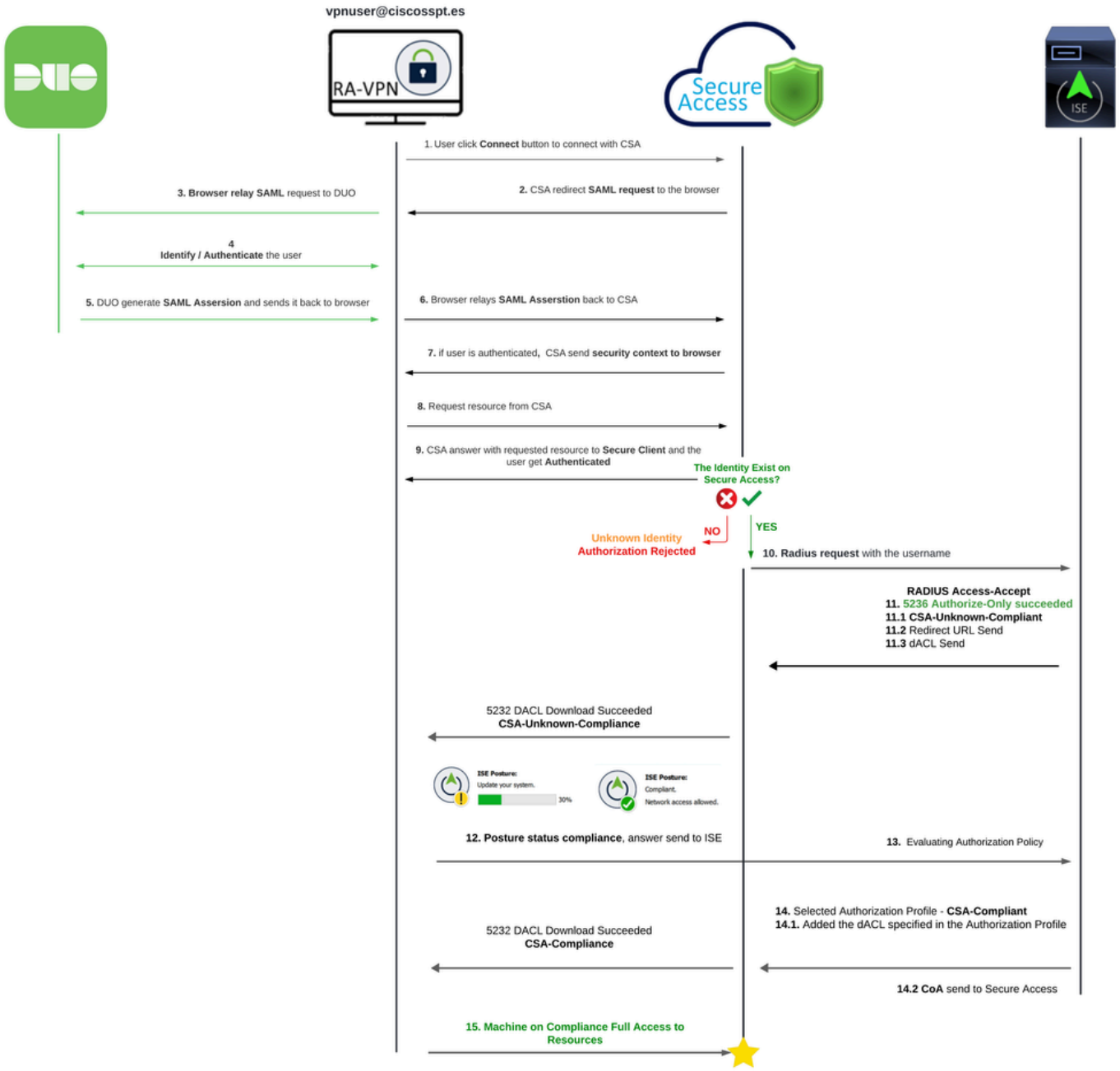
Componenti usati

Le informazioni fornite in questo documento si basano su:

- Patch 1 per Identity Service Engine (ISE) versione 3.3
- Accesso sicuro
- Cisco Secure Client - Anyconnect VPN versione 5.1.2.42

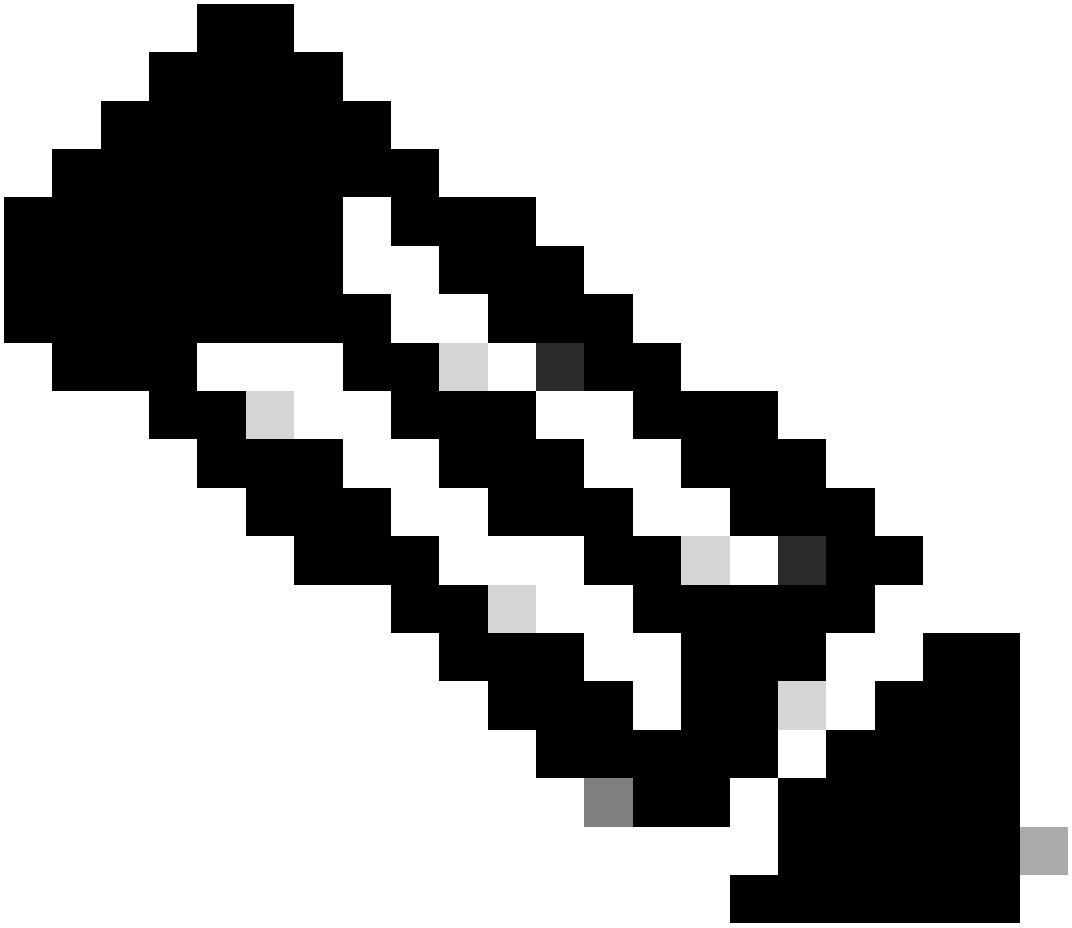
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse



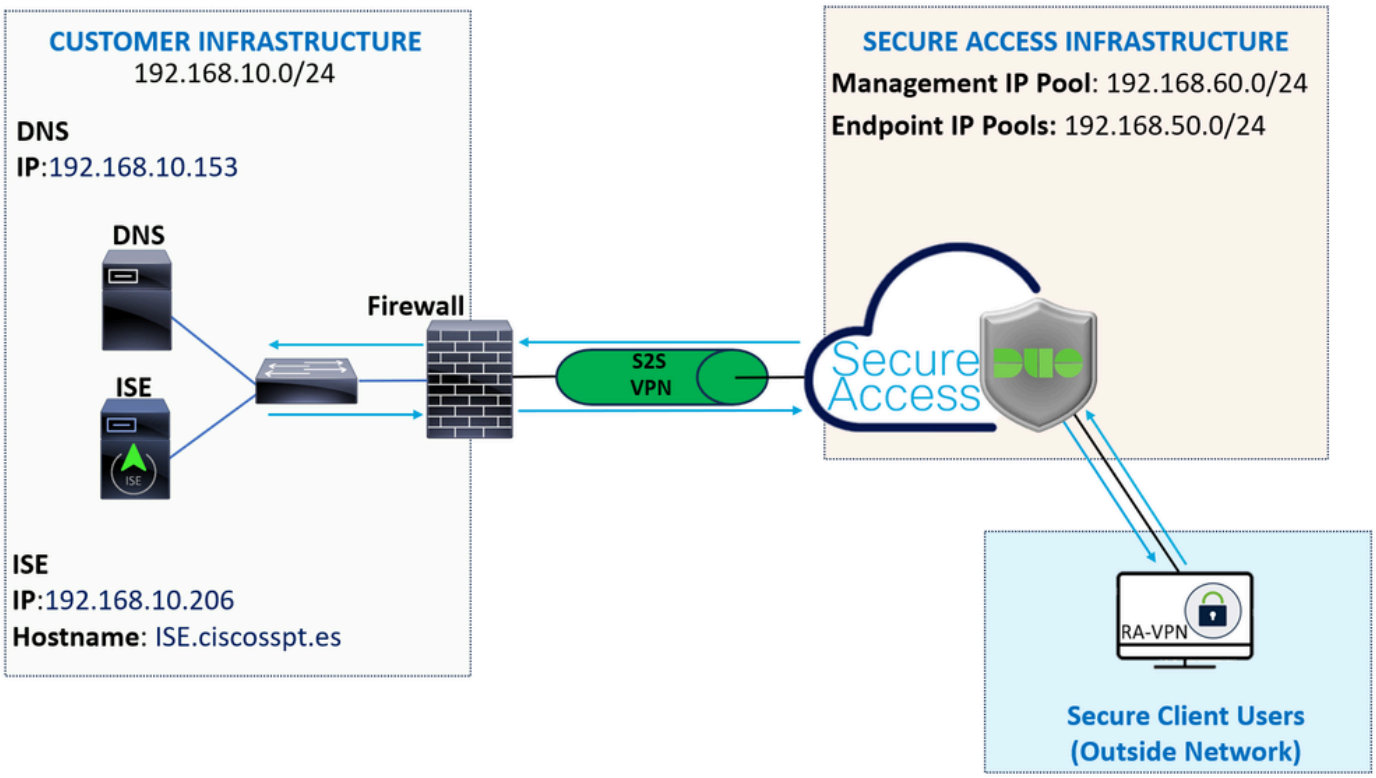
L'integrazione di Duo SAML con Cisco Identity Services Engine (ISE) migliora il processo di autenticazione e aggiunge un altro livello di sicurezza alle soluzioni Cisco Secure Access. Duo SAML fornisce una funzionalità Single Sign-On (SSO) che semplifica il processo di accesso dell'utente garantendo al contempo standard di sicurezza elevati.

Dopo l'autenticazione tramite Duo SAML, il processo di autorizzazione viene gestito da Cisco ISE. Ciò consente di prendere decisioni dinamiche sul controllo dell'accesso in base all'identità dell'utente e alla postura del dispositivo. ISE può applicare policy dettagliate che stabiliscono a quali risorse un utente può accedere, quando e da quali dispositivi.

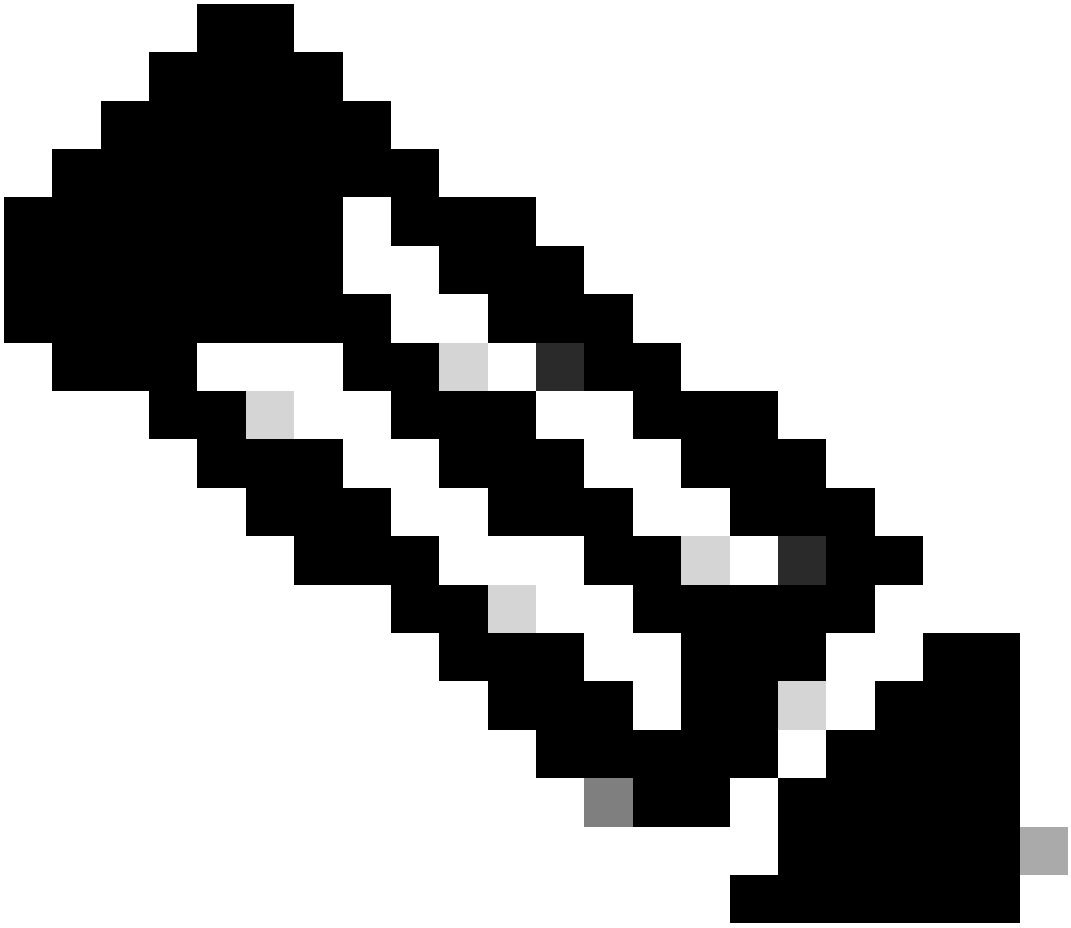


Nota: per configurare l'integrazione RADIUS, è necessario verificare la comunicazione tra entrambe le piattaforme.

Esempio di rete



Configurazione



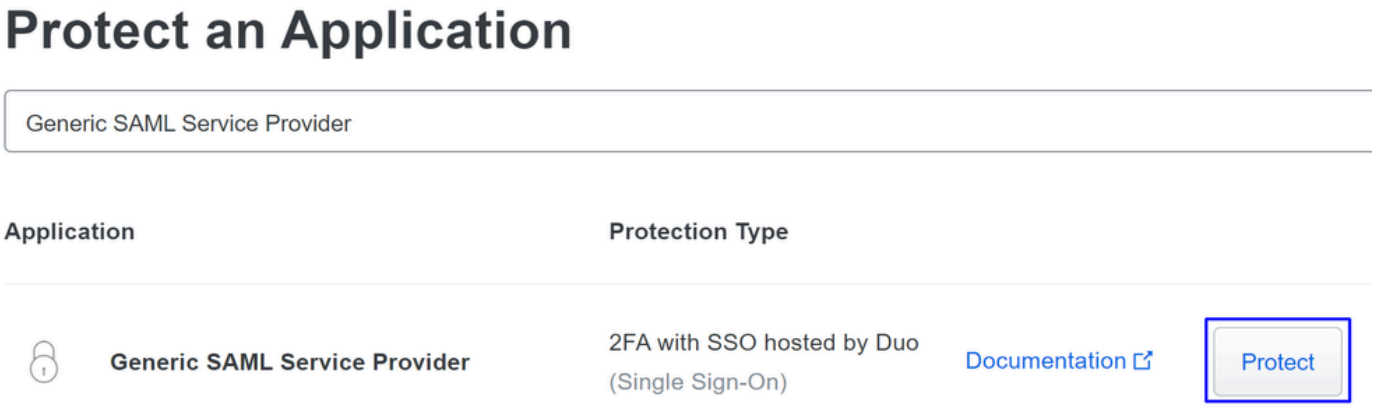
Nota: prima di iniziare il processo di configurazione, è necessario completare i primi passaggi con Secure Access e ISE Integration.

Configurazione Duo

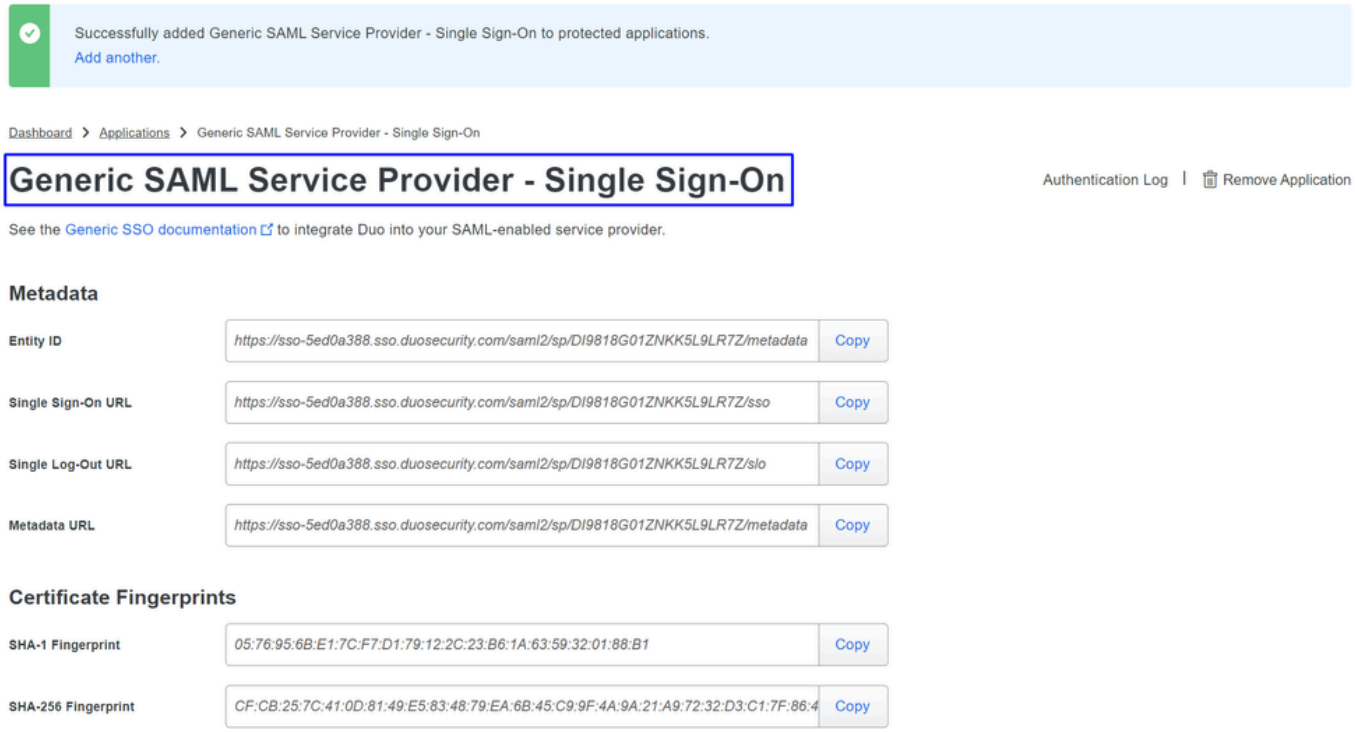
Per configurare l'applicazione RSA-VPN, procedere con i passi successivi:

Passare al pannello di amministrazione Duo

- Passa a **Applications > Protect an Application**
  - Cerca **Generic SAML Service Provider**
  - Fare clic su Protect



È necessario che l'applicazione sia visualizzata sullo schermo. Ricordare il nome dell'applicazione per la configurazione VPN.



In questo caso è **Generic SAML Service Provider.**

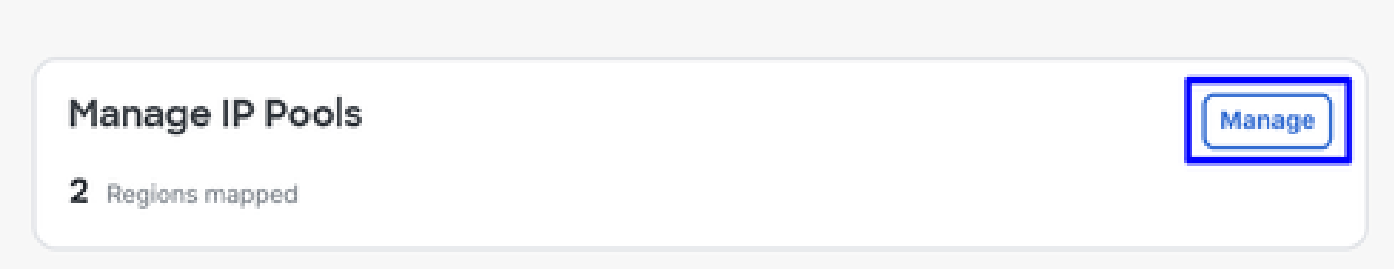
Configurazione accesso sicuro

Configurazione del gruppo Radius sui pool IP

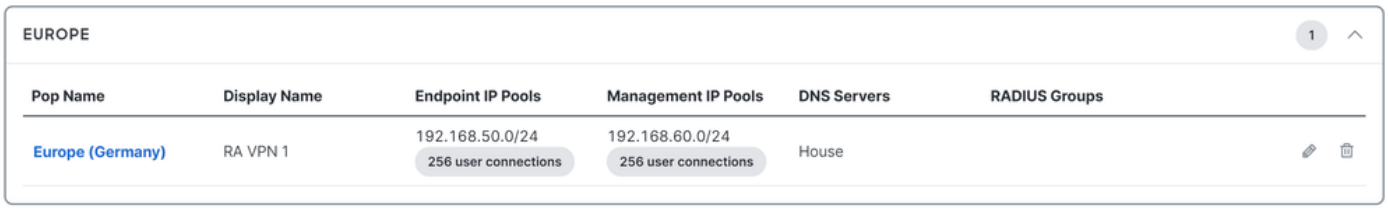
Per configurare il profilo VPN utilizzando Radius, procedere con i passaggi seguenti:

Passare al Dashboard di accesso sicuro.

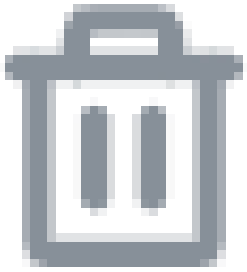
- Fare clic su **Connect > Enduser Connectivity > Virtual Private Network**
- In Configurazione pool (**Manage IP Pools**), fare clic suManage



- Scegliere **IP Pool Region** e configurare **Radius Server**

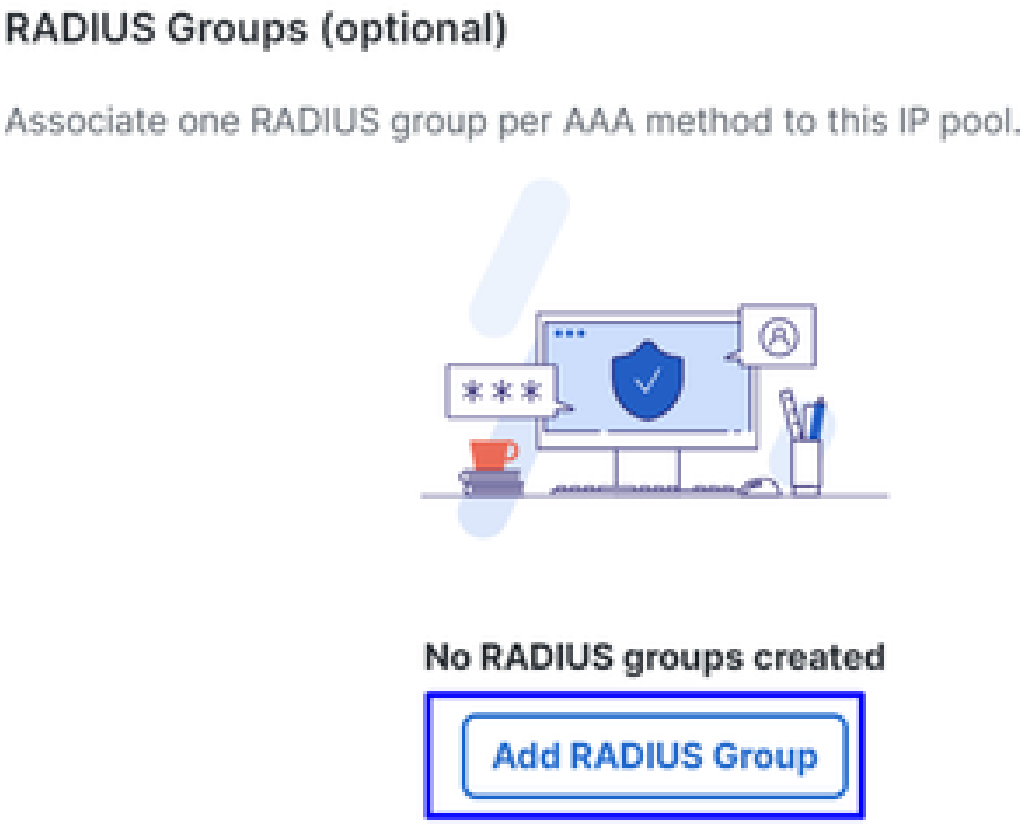


- Fare clic sulla matita da modificare



- A questo punto, nell'elenco a discesa Configurazione della sezione Pool IP in **Radius Group (Optional)**

- Fare clic su Add RADIUS Group



← Edit RADIUS Group

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

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

Group Name: configurare un nome per l'integrazione ISE in Secure Access

- **AAA method**

  - **Authentication**: selezionare la casella di controllo **Authentication** e, per impostazione predefinita, selezionare la porta 1812

    - Se per l'autenticazione è necessario Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2) selezionare la casella di controllo

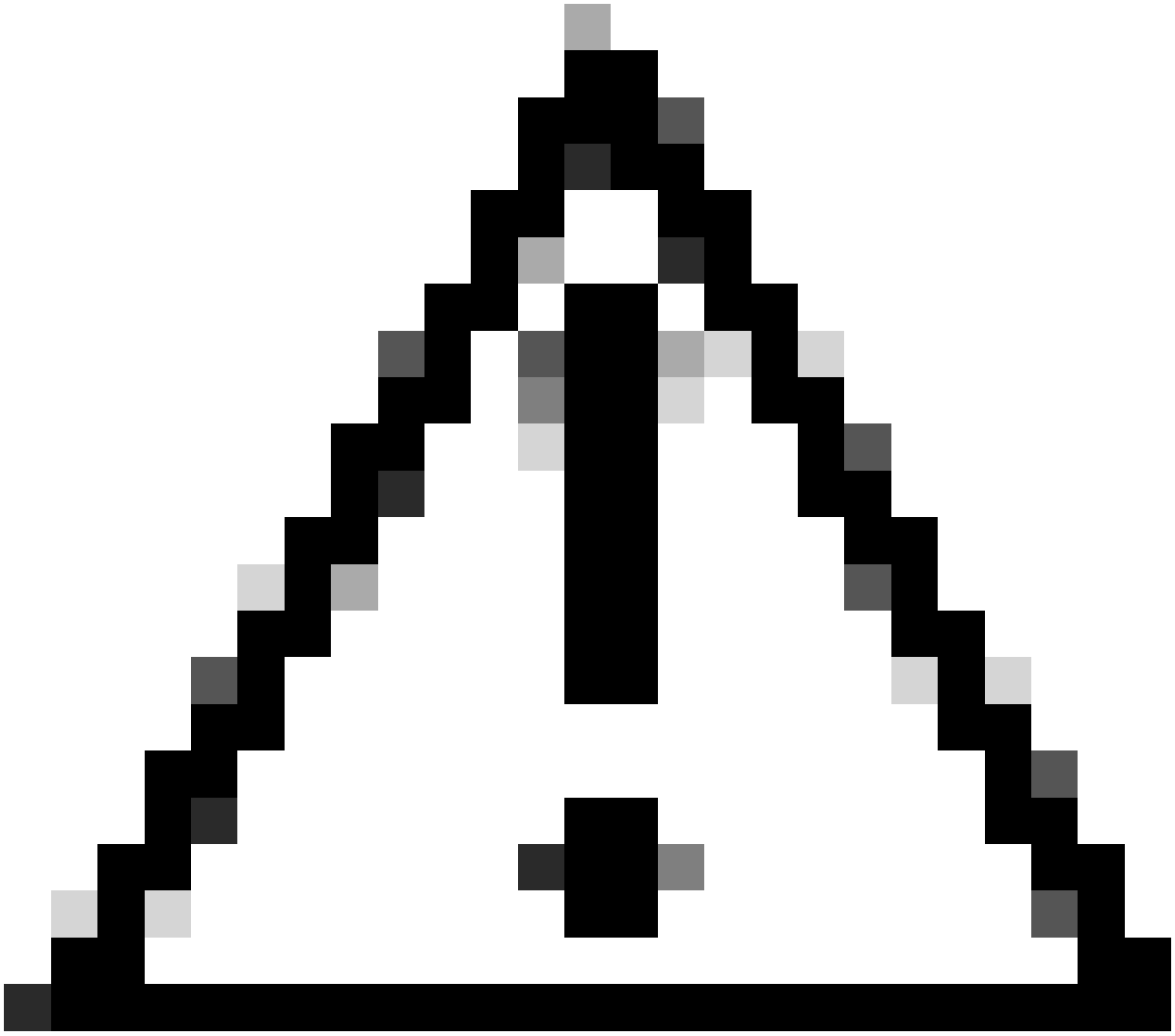
  • **Authorization**: selezionare la casella di controllo per Authorization e selezionare la porta, per impostazione predefinita, 1812

    - Contrassegnare la casella di controllo per **Authorization mode Only Change of Authorization (CoA) mode** e per consentire la postura e le modifiche da ISE

  • **Accounting**: selezionare la casella di controllo Autorizzazione e selezionare la porta predefinita, 1813

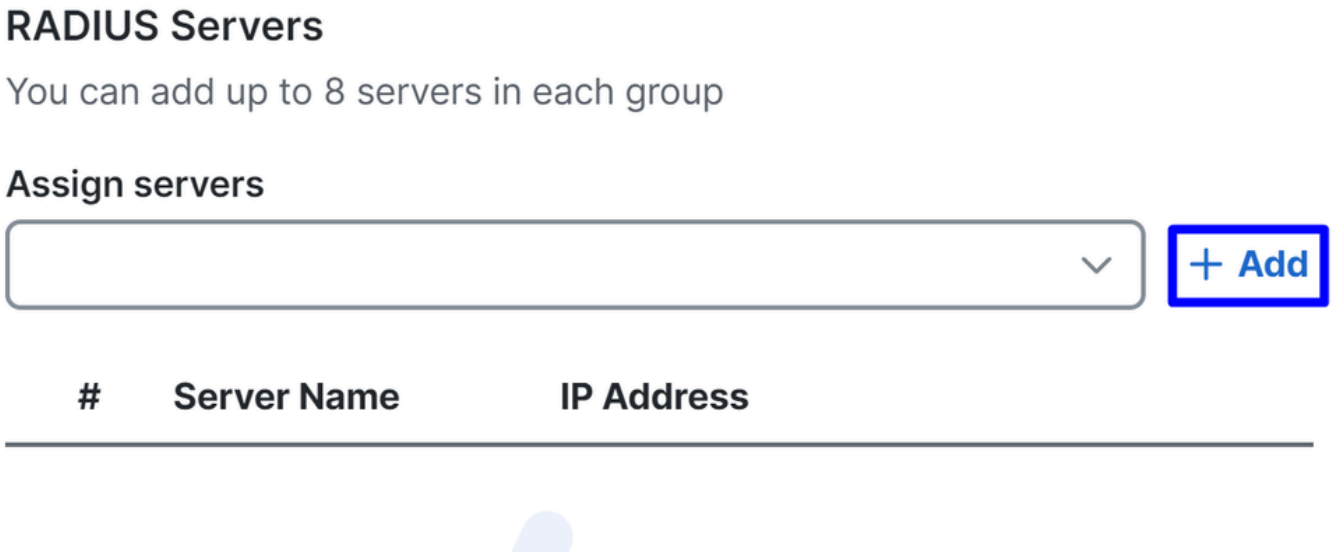
    - Scegliere **Single or Simultaneous** (in modalità singola i dati di accounting vengono inviati a un solo server. in modalità simultanea, dati di accounting per tutti i server del gruppo)

      • Selezionare la casella di controllo per **Accounting update** abilitare la generazione periodica dei messaggi di aggiornamento dell'accounting intermedio RADIUS.



Attenzione: entrambi i Authentication metodi e, quando vengono selezionati, devono utilizzare la stessa porta. **Authorization** Nota

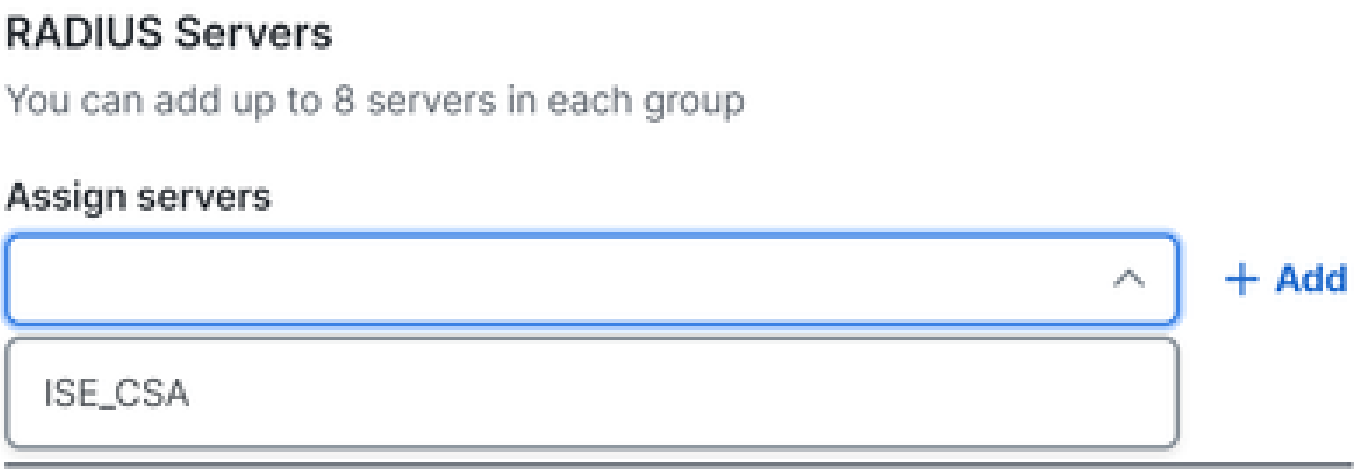
- Quindi, configurare l'**RADIUS Servers** (ISE) da utilizzare per l'autenticazione tramite AAA sulla sezione **RADIUS Servers**:
- Fare clic su + Add



- Quindi, configurare le opzioni successive:

- Server Name: configurare un nome per identificare il server ISE.
- **IP Address**: configurare l'indirizzo IP del dispositivo Cisco ISE raggiungibile tramite l'accesso sicuro
- **Secret Key**: configurare la chiave privata RADIUS
- **Password**: configurare la password Radius

- Fare clic **Save** e assegnare il server Radius sotto l'opzioneAssign Server e selezionare il server ISE:



- Fare di **Save** nuovo clic per salvare tutte le configurazioni

← 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

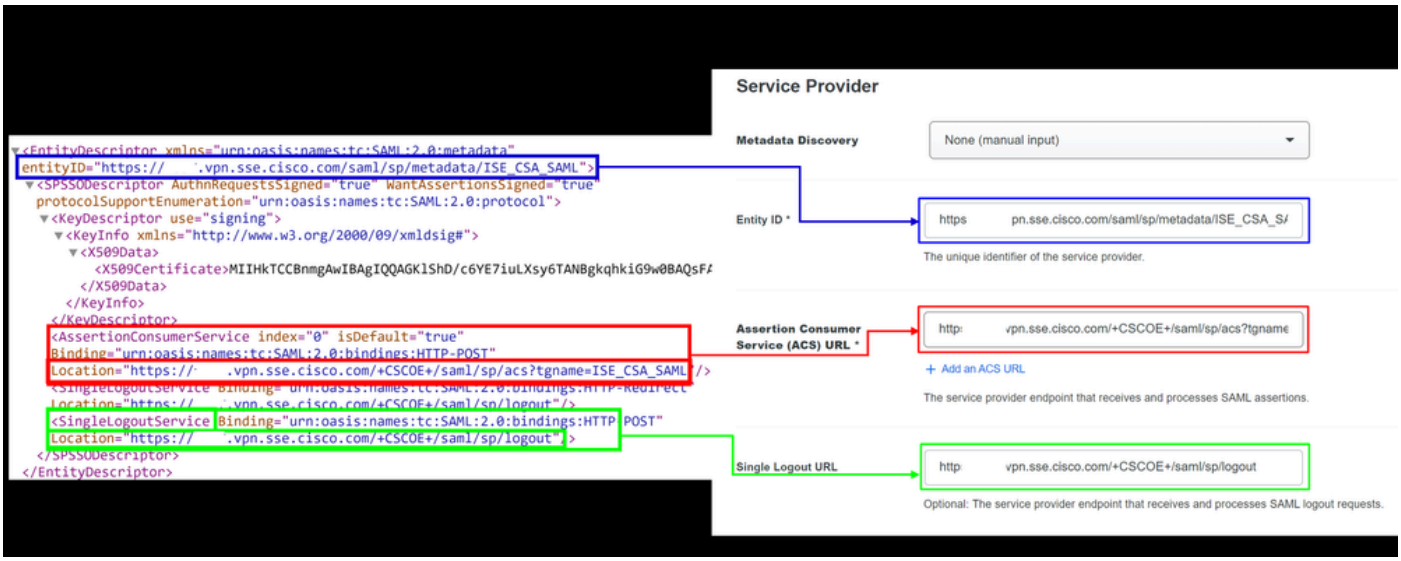
ISE_CSA

+ Add

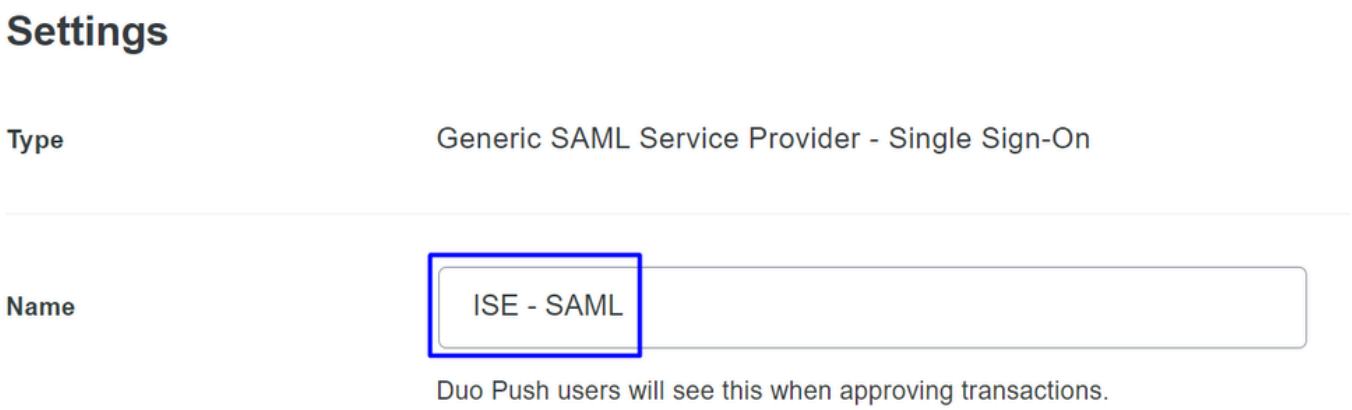
#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

- **Protocols**: Scegli **SAML**

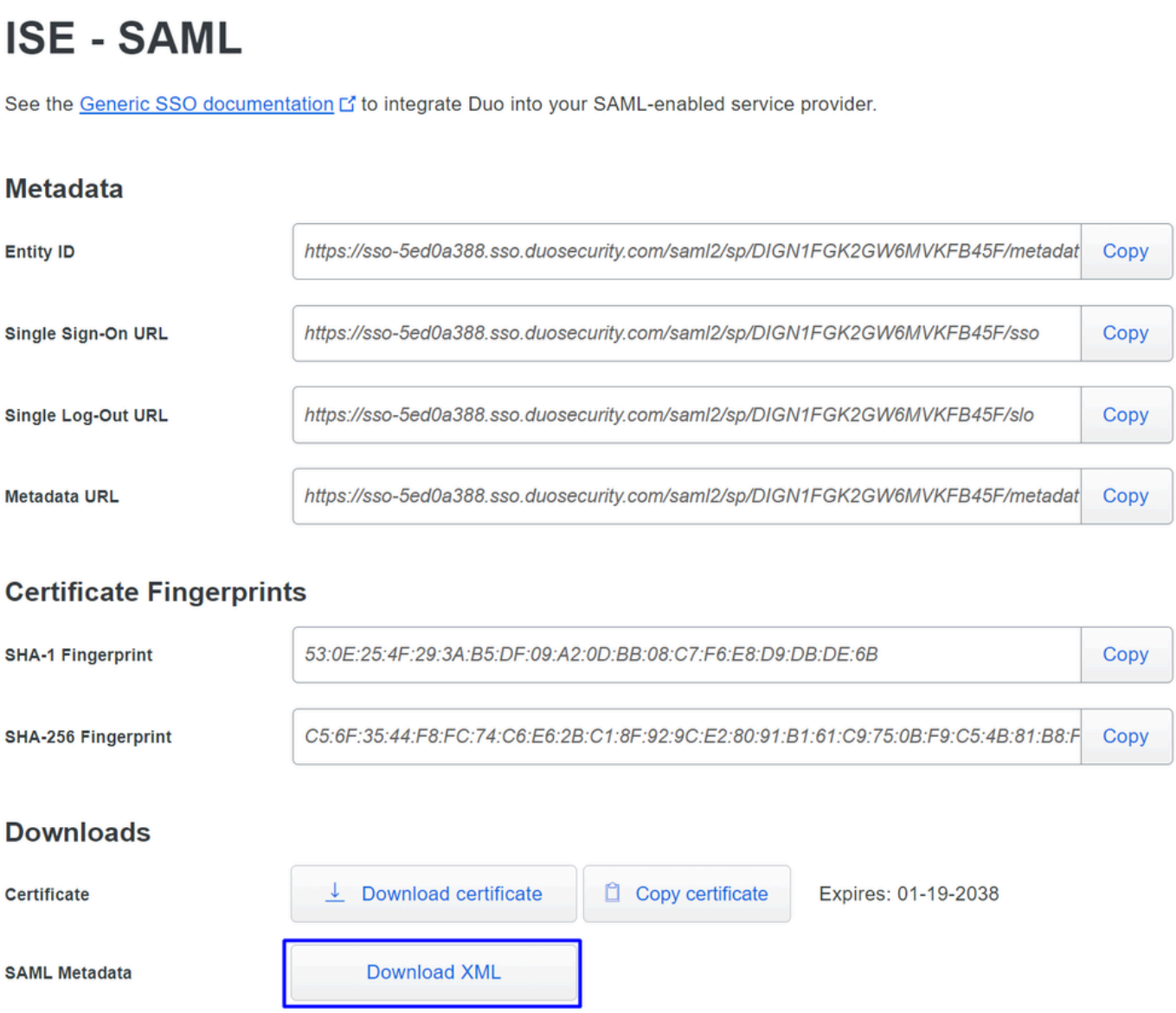
- Fare clic su Download Service Provider XML file
- Sostituire le informazioni nell'applicazione configurata nella fase Duo Configuration



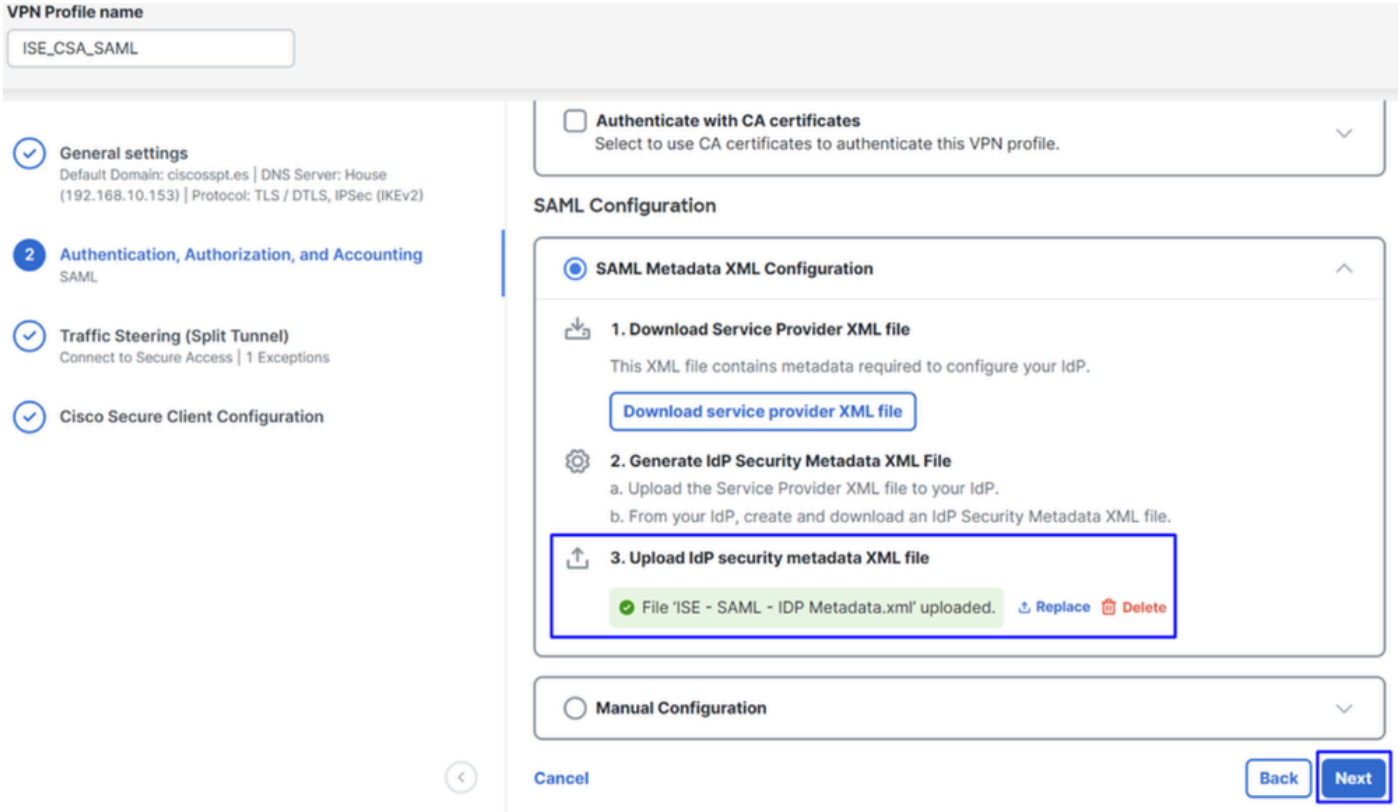
- Una volta configurate tali informazioni, modificare il nome della Duo in qualcosa relativo all'integrazione che si sta creando



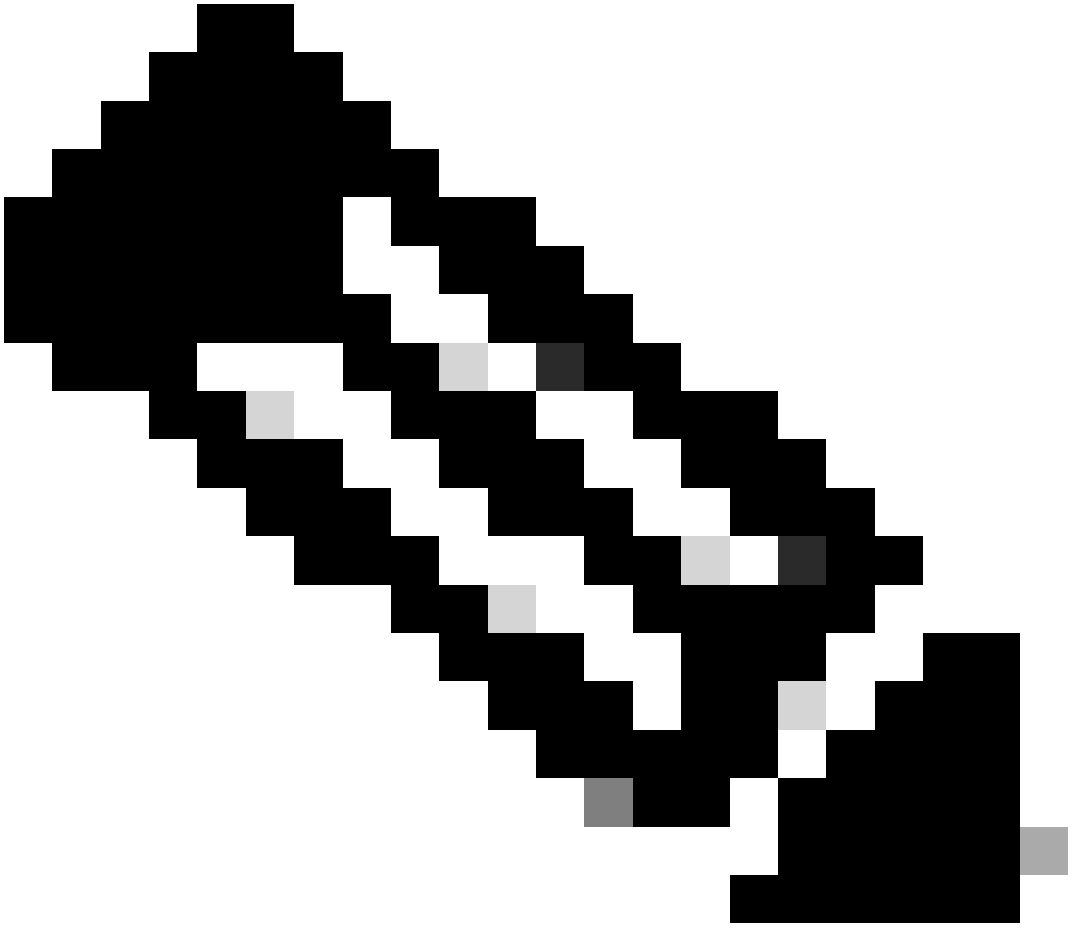
- Fare clic **Save** sull'applicazione su Duo.
- Dopo aver fatto clic su Salva, è necessario scaricare **SAML Metadata** facendo clic sul pulsante **Download XML**



- Caricare il file **SAML Metadata** su Secure Access nell'opzione **3. Upload IdP security metadata XML file** e fare clic su **Next**

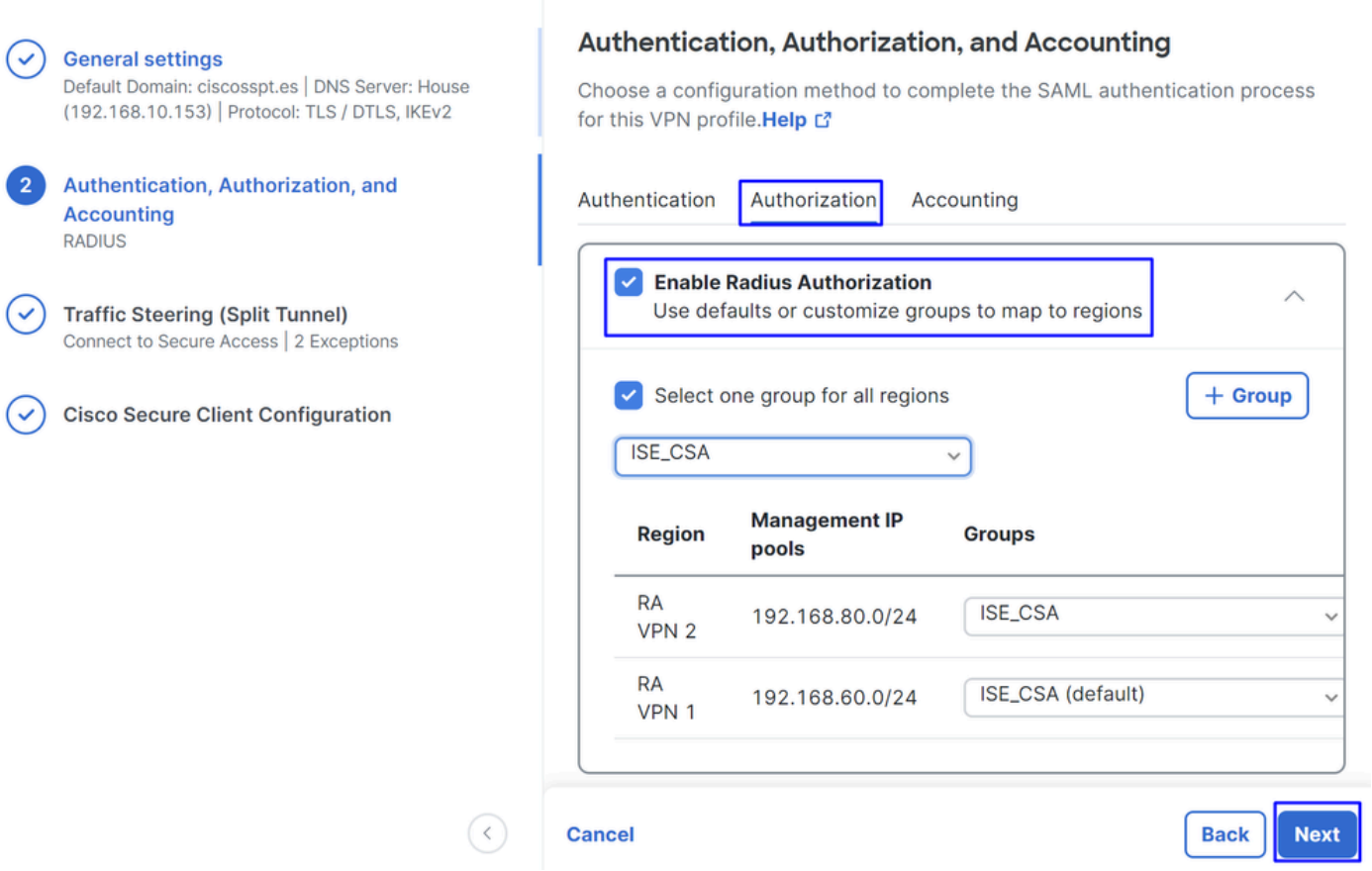


Procedere con l'autorizzazione.



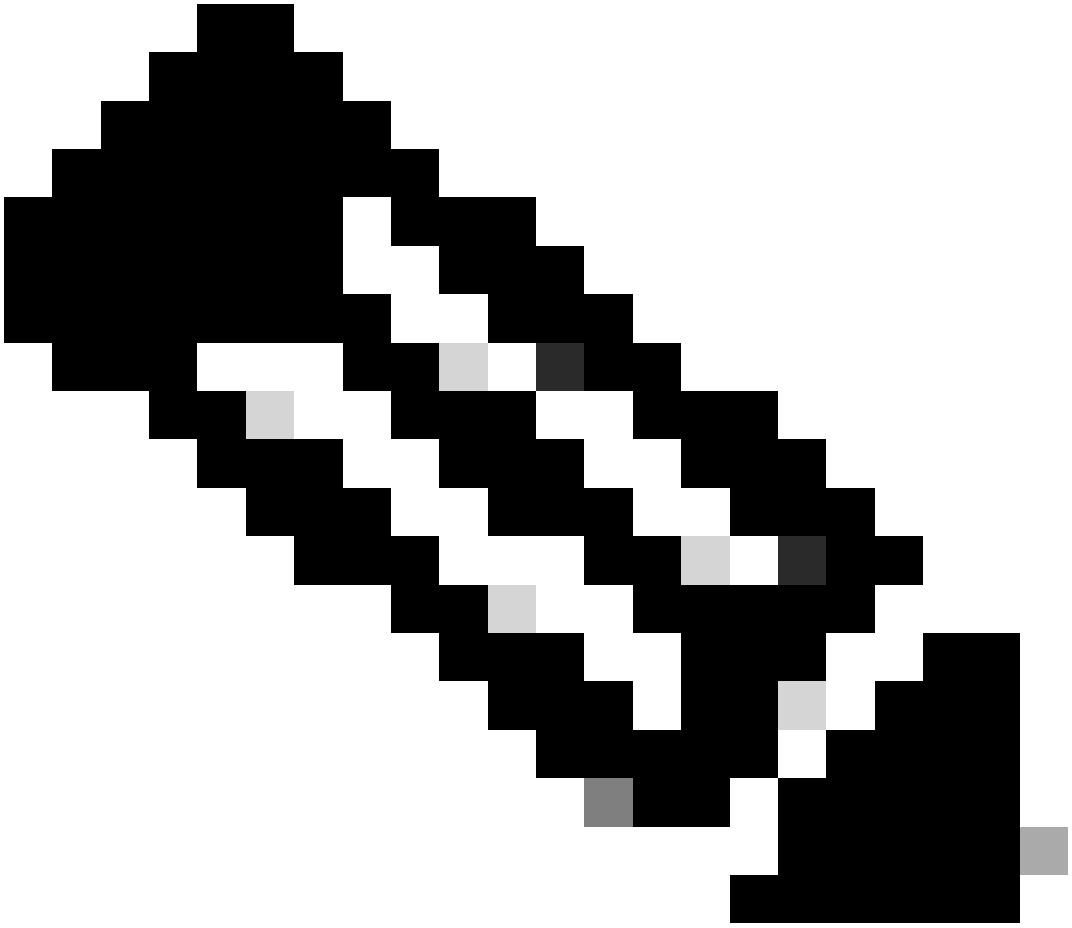
Nota: dopo aver configurato l'autenticazione con SAML, la si autorizzerà tramite ISE, ossia il pacchetto radius inviato da Secure Access conterrà solo il nome utente. Il campo della password non esiste.

Authorization



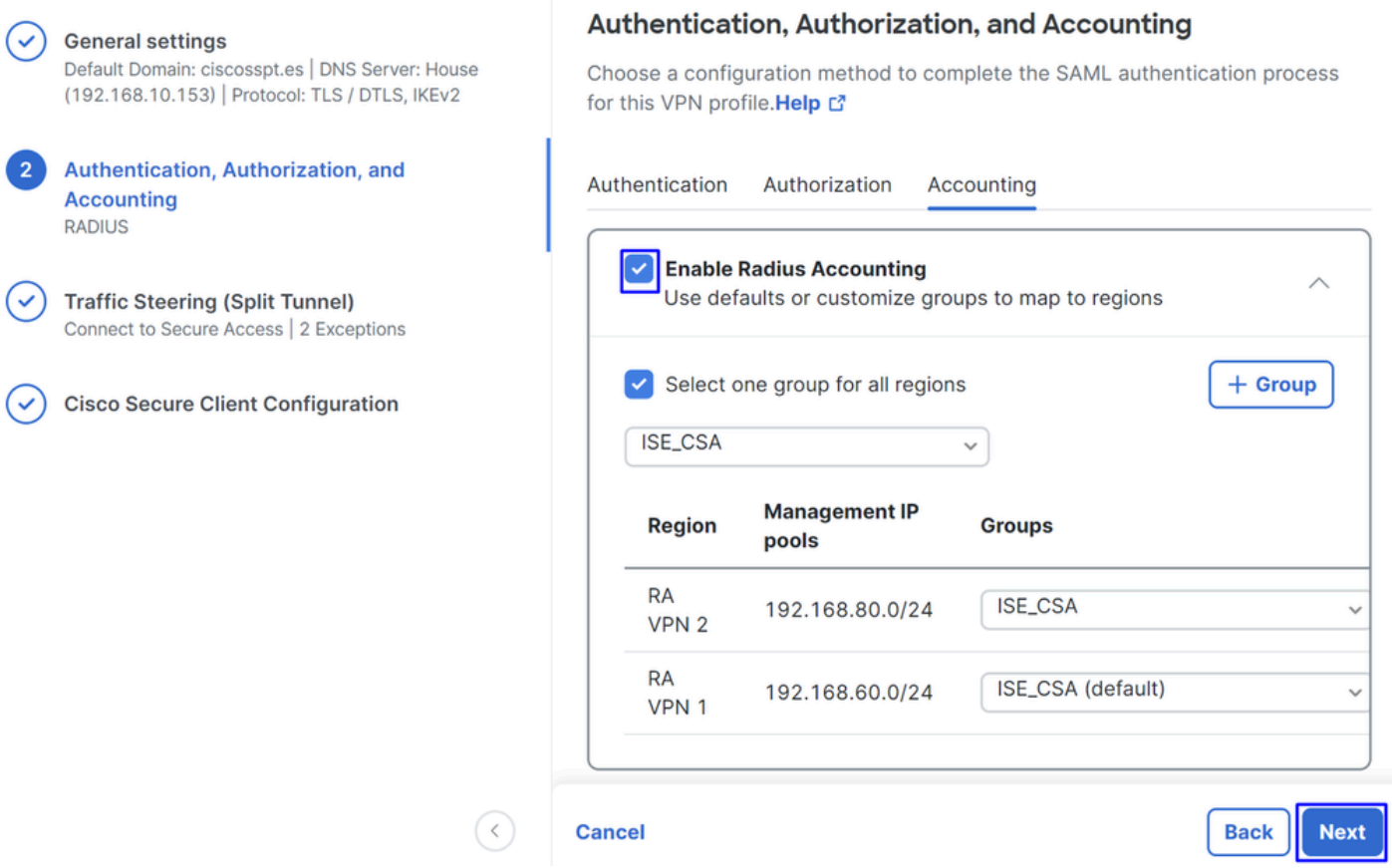
- **Authorization**
  - **Enable Radius Authorization**: selezionare la casella di controllo per attivare l'autorizzazione del raggio
  - **Selezionare un gruppo per tutte le aree**: selezionare la casella di controllo per utilizzare un server RADIUS specifico per tutti i pool di Accesso remoto - Rete privata virtuale (RA-VPN) oppure definirlo per ogni pool separatamente
- Fare clic su **Next**

Dopo aver configurato tutte le **Authorization** parti, procedere con la **Accounting**procedura.



Nota: se non si abilita **Radio Authorization**, la postura non può funzionare.

Contabilità

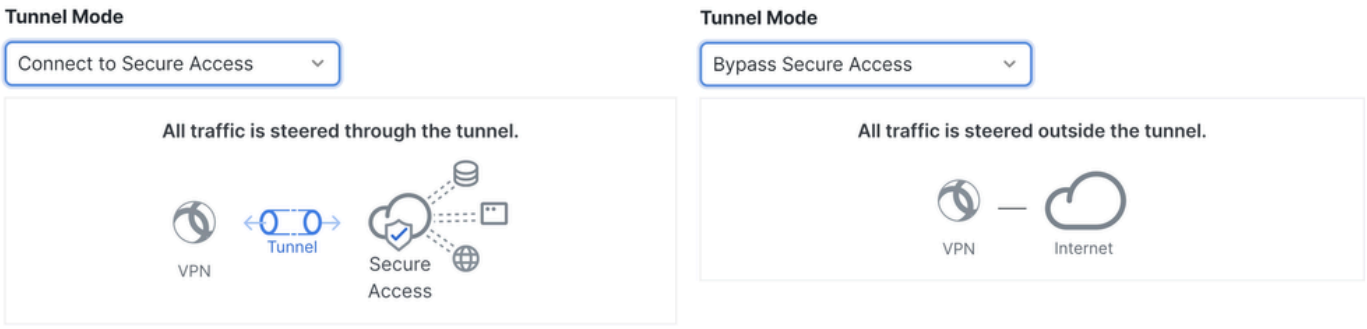


- **Accounting**
    - **Map Authorization groups to regions**: Scegliere le aree e scegliere il proprio **Radius Groups**
- Fare clic su **Next**

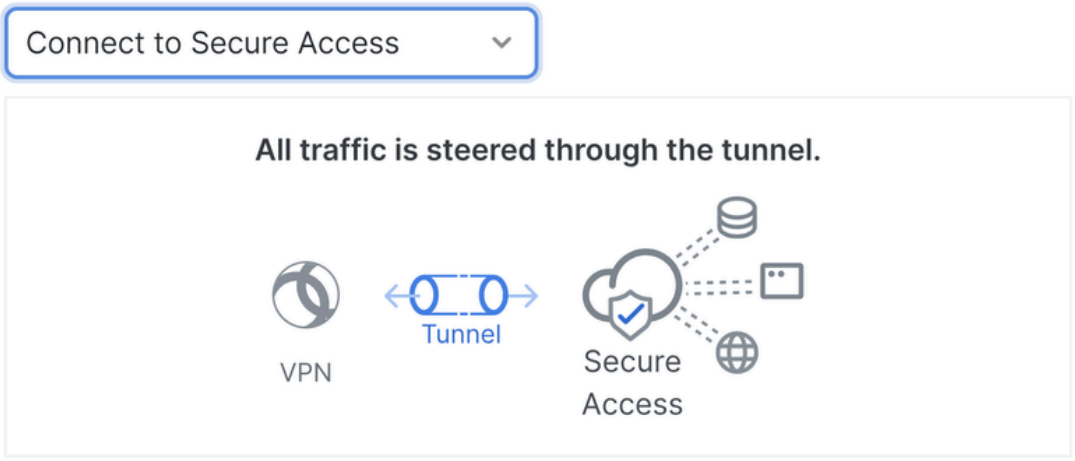
After you have done configured the Authentication, Authorization and Accounting continuare conTraffic Steering.

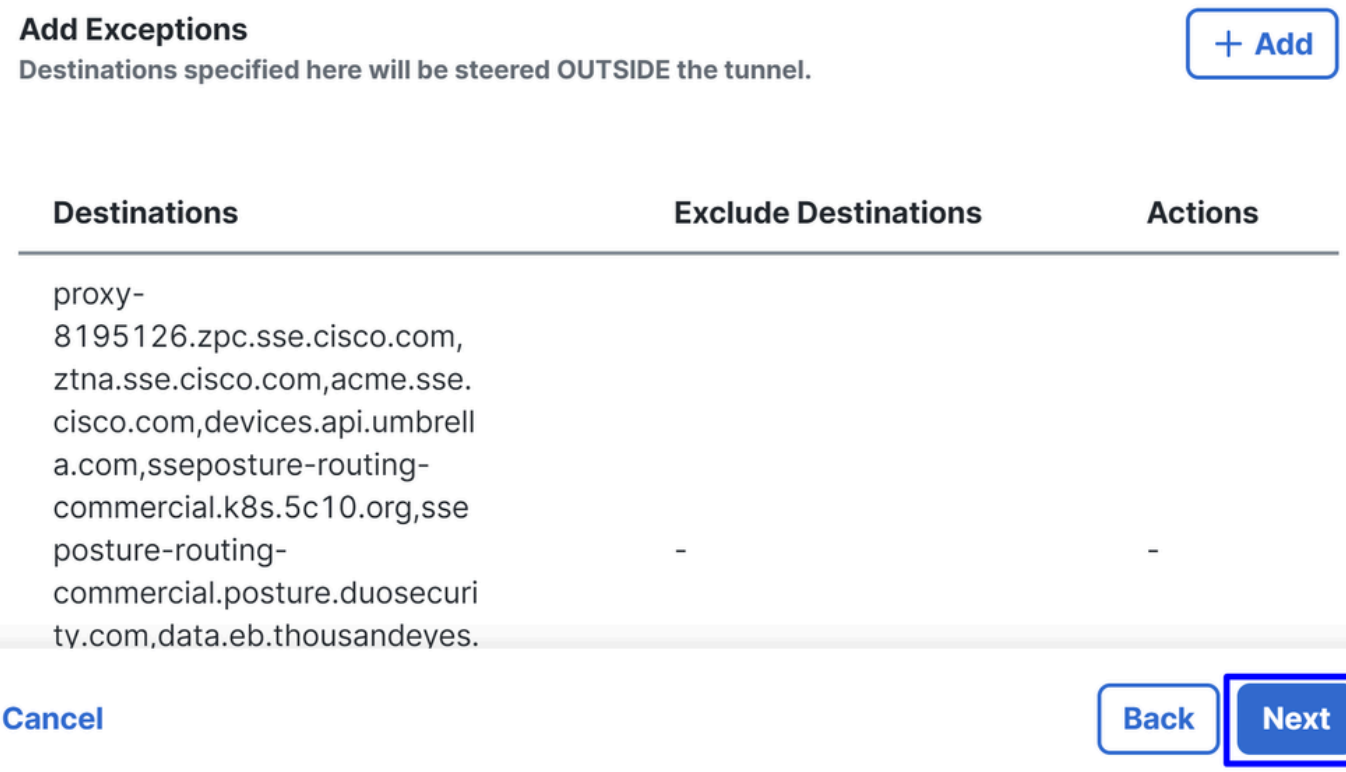
Traffic Steering

In Traffic Steering è necessario configurare il tipo di comunicazione tramite l'accesso sicuro.



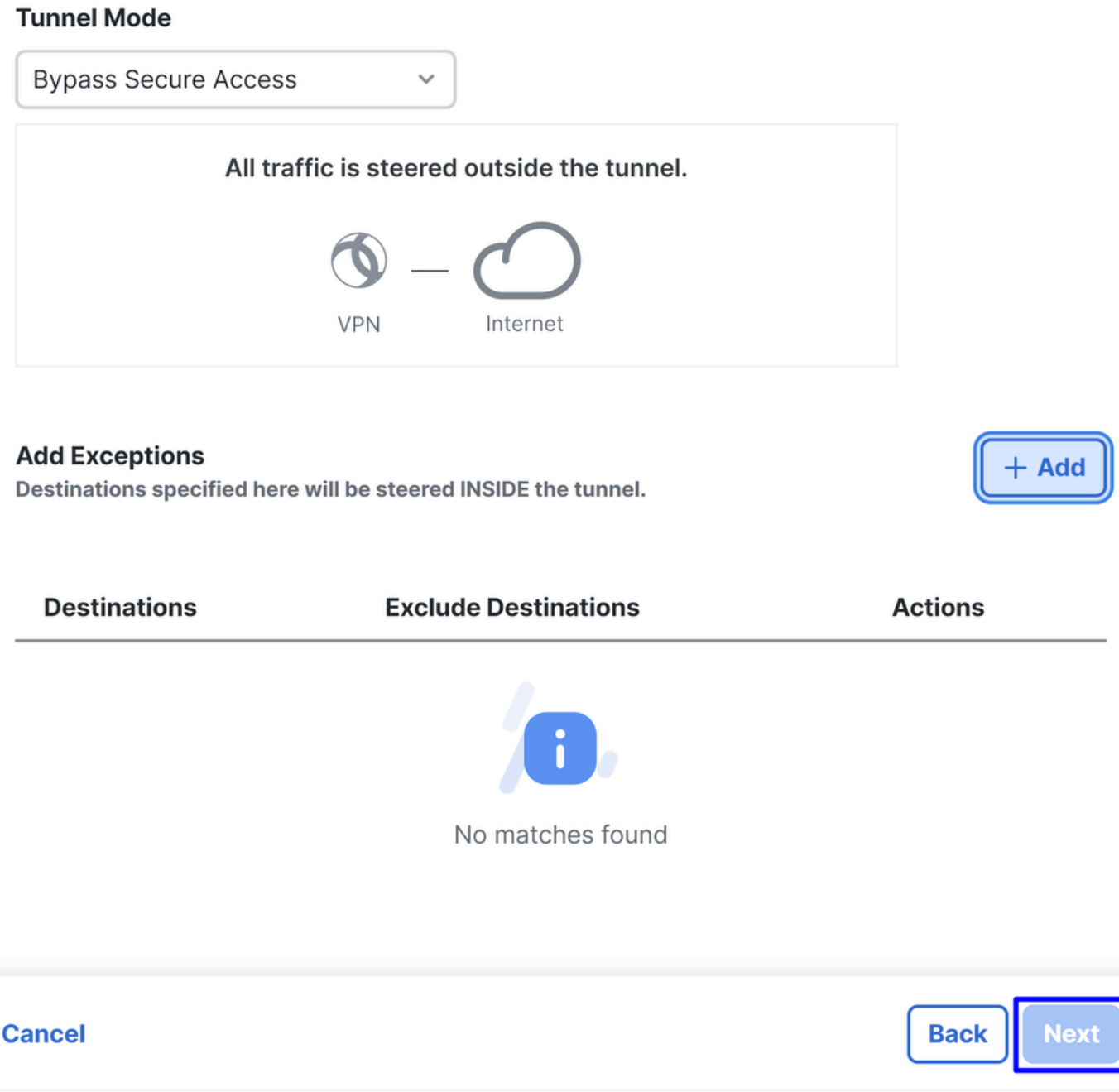
- Se lo si desidera, **Connect to Secure Access**il traffico Internet verrà instradato **Secure Access**

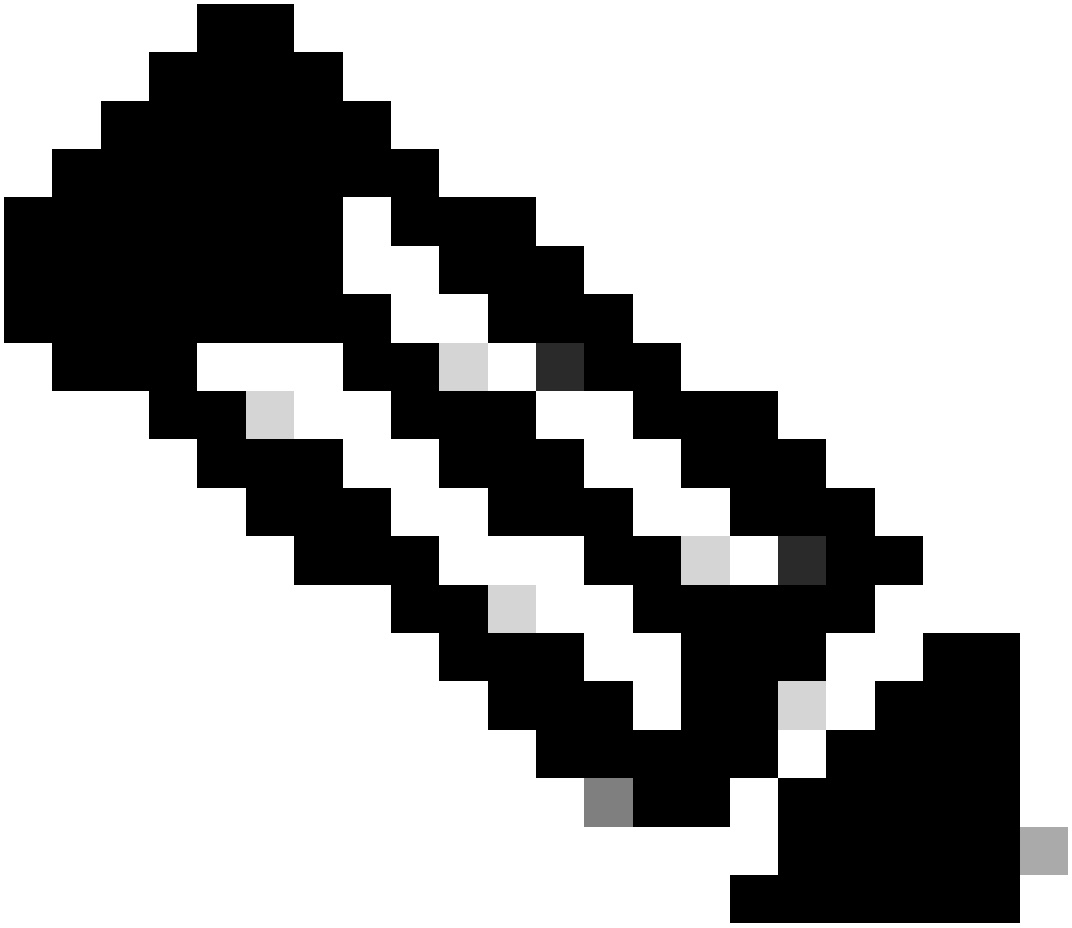




Se si desidera aggiungere esclusioni per domini Internet o IP, fare clic sul **+ Add** pulsante, quindi fare clic su **Next**.

- Se si decide di **Bypass Secure Access**farlo, tutto il traffico Internet passa attraverso il provider Internet, non attraversoSecure Access (nessuna protezione Internet)

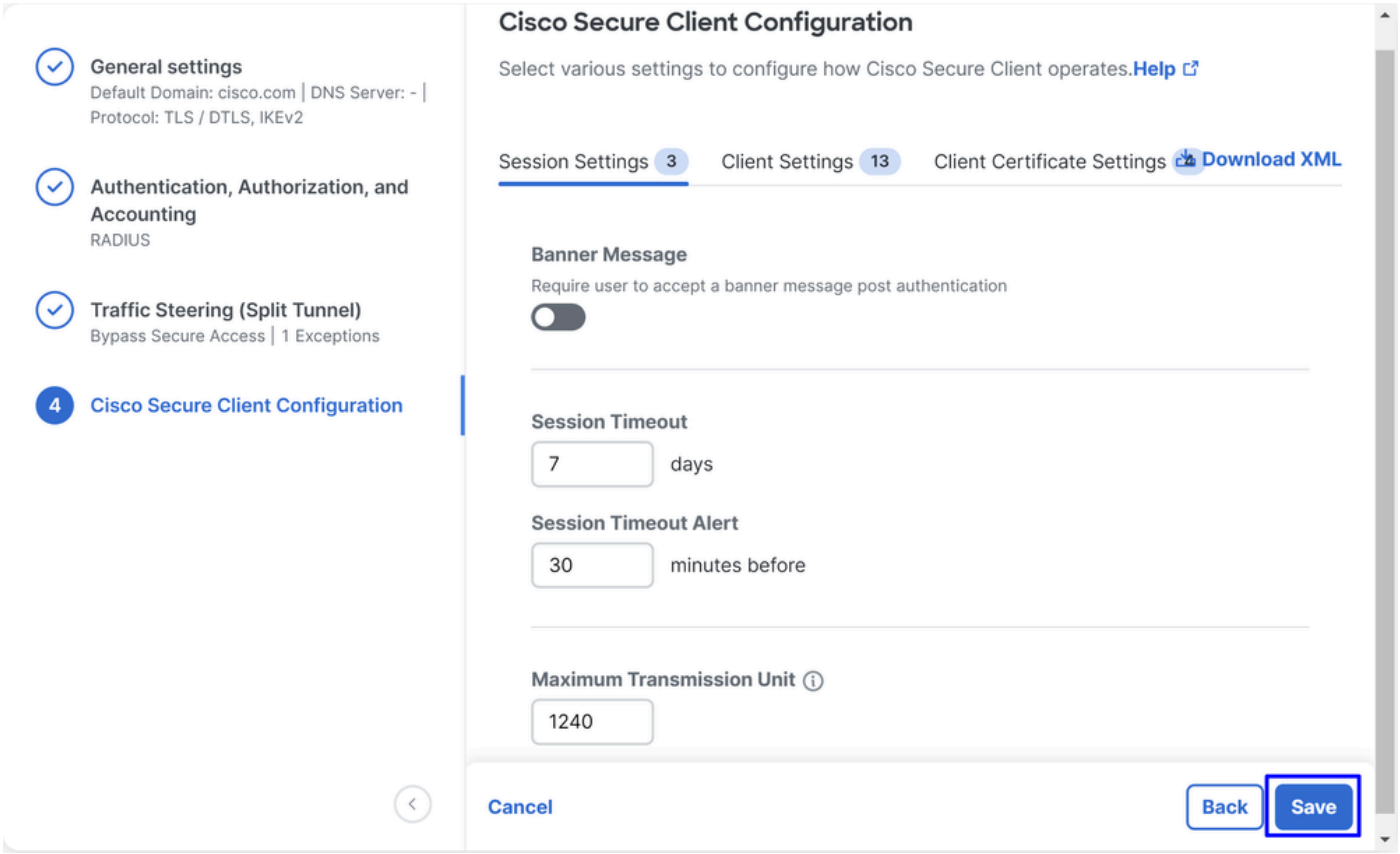




Nota: aggiungere **enroll.cisco.com** per la postura ISE quando si sceglie **Bypass Secure Access**.

In questo passaggio verranno selezionate tutte le risorse di rete private a cui si desidera accedere tramite la VPN. A tale scopo, fare clic su **+ Add**, quindi su **Next** dopo aver aggiunto tutte le risorse.

Cisco Secure Client Configuration



In questo passaggio è possibile mantenere tutto come predefinito e fare clic su **Save**, ma se si desidera personalizzare ulteriormente la configurazione, consultare la 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

Configurazioni ISE

Configura elenco dispositivi di rete

Per configurare l'autenticazione tramite Cisco ISE, è necessario configurare i dispositivi autorizzati che possono inviare query a Cisco ISE:

- Passa a **Administration > Network Devices**
- Fare clic su **+ 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

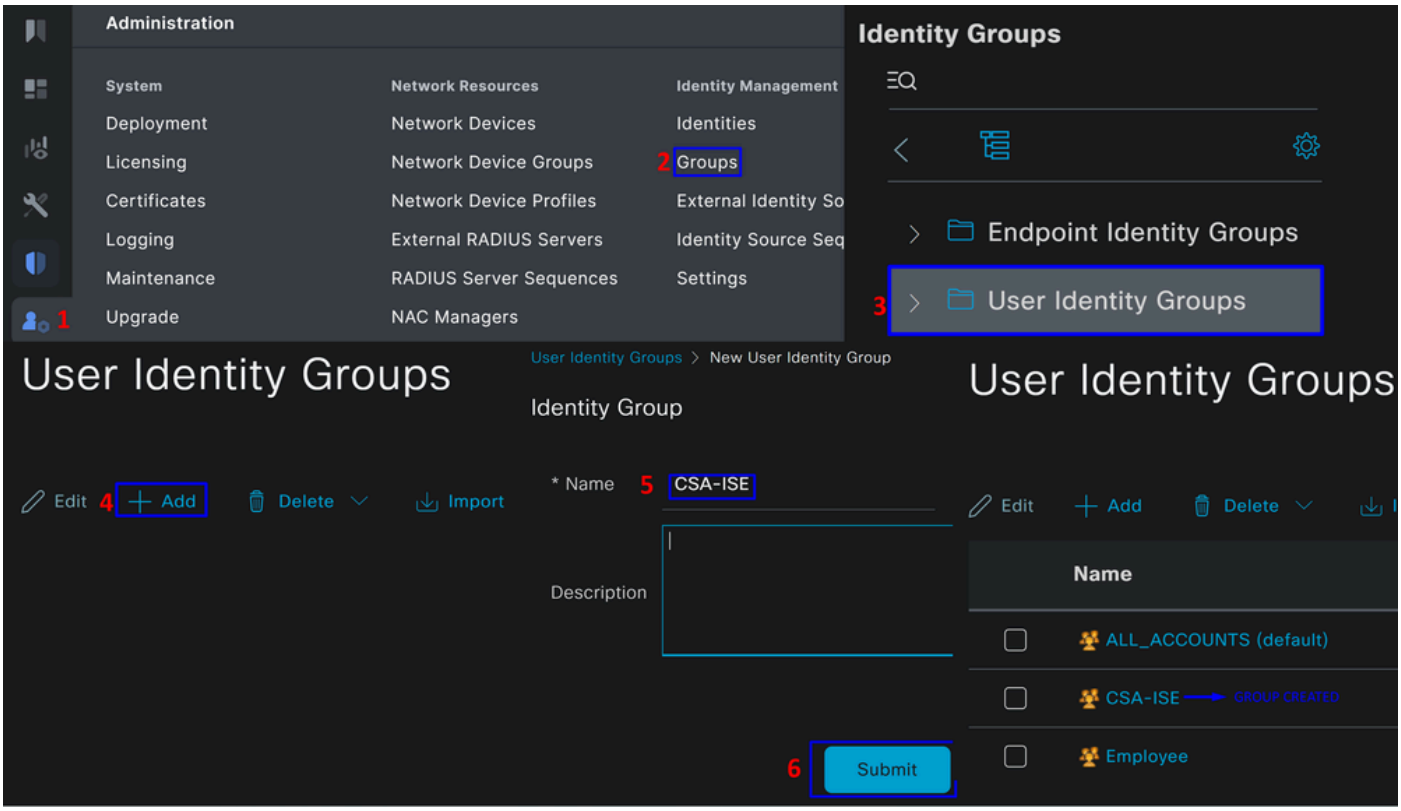
- **Name**: utilizzare un nome per identificare l'accesso sicuro
- **IP Address**: configurare il valoreManagement Interface della fase, Area pool IP
- **Device Profile**: Scegli Cisco
    - **Radius Authentication Settings**
        - Shared Secret: configurare lo stesso segreto condiviso configurato nella fase, Chiave privata
        - **CoA Port**: non utilizzare questa impostazione come predefinita. Il valore 1700 viene utilizzato anche in Accesso protetto

Dopo aver fatto clic su **Save**, per verificare se l'integrazione funziona correttamente, procedere con la creazione di un utente locale per la verifica dell'integrazione.

Configurare un gruppo

Per configurare un gruppo per l'utilizzo con utenti locali, procedere come segue:

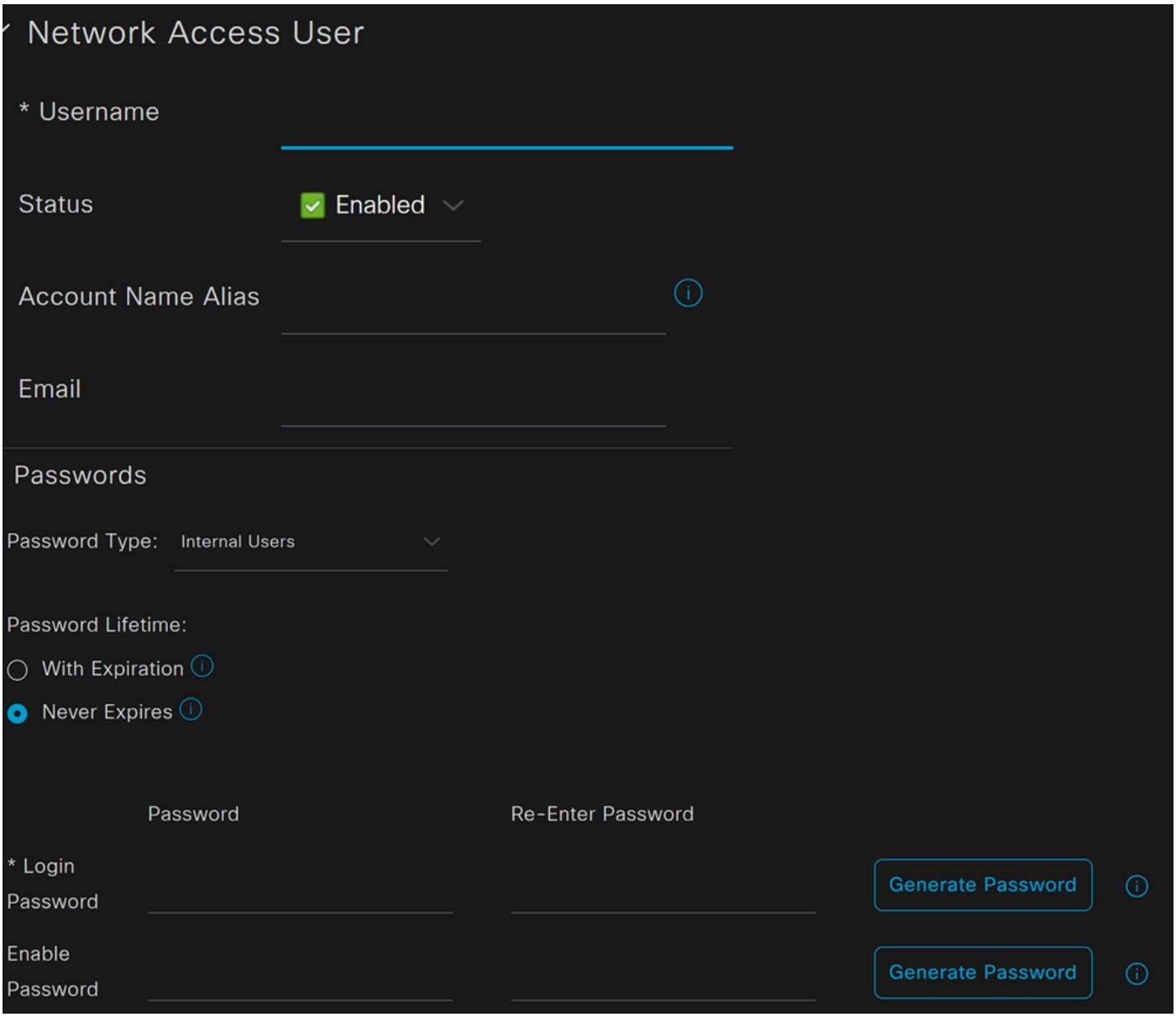
- Fare clic su **Administration > Groups**
- Fare clic su **User Identity Groups**
- Fare clic su + Add
- Creare una Nameper il gruppo e fare clic su **Submit**

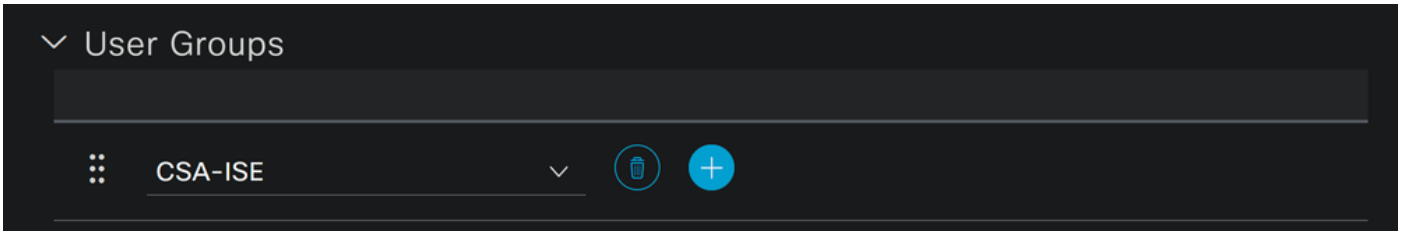


Configura utente locale

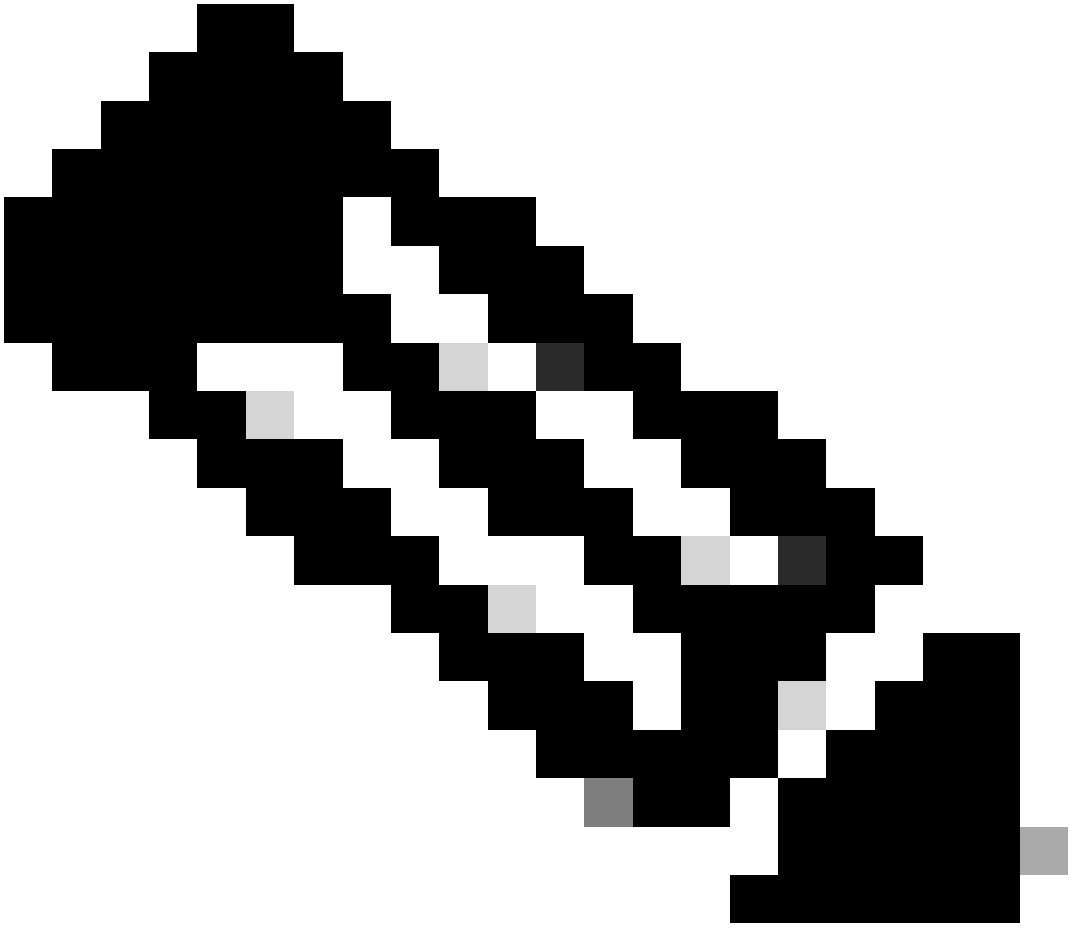
Per configurare un utente locale per la verifica dell'integrazione:

- Passa a **Administration > Identities**
- Fare clic su **Add +**





- **Username**: configurare il nome utente con un provisioning UPN noto in Secure Access. Tale configurazione è basata sul passo Prerequisiti
- **Status**:Attiva
- **Password Lifetime**: è possibile configurarlo **With Expiration** o Never Expires, a seconda delle
- **Login Password**: crea una password per l'utente
- **User Groups**: scegliere il gruppo creato nel passo, Configurare un gruppo



Nota: l'autenticazione basata sull'UPN verrà modificata nelle versioni future di Secure Access.

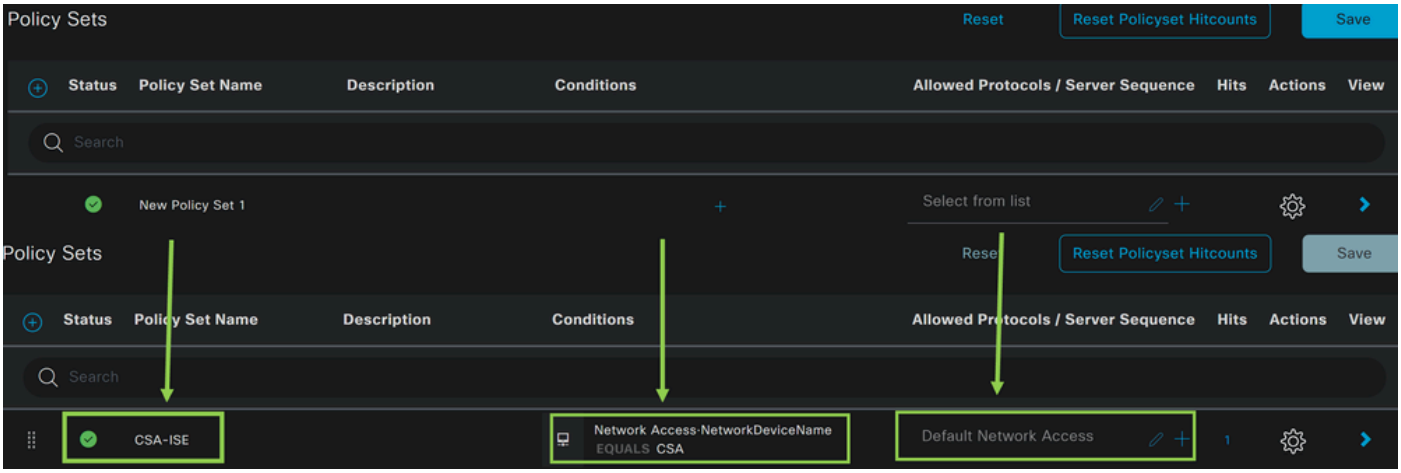
Quindi, è possibile eseguire **Save** la configurazione e continuare con il passaggio **Configure Policy Set**.

Configura set di criteri

In base al set di criteri, configurare l'azione intrapresa da ISE durante l'autenticazione e l'autorizzazione. In questo scenario viene illustrato lo scenario di utilizzo per la configurazione di un criterio semplice per consentire l'accesso degli utenti. In primo luogo, ISE verifica l'origine delle autenticazioni RADIUS e verifica se le identità esistono nel database utenti ISE per fornire l'accesso

Per configurare tale criterio, passare al proprio Cisco ISE Dashboard:

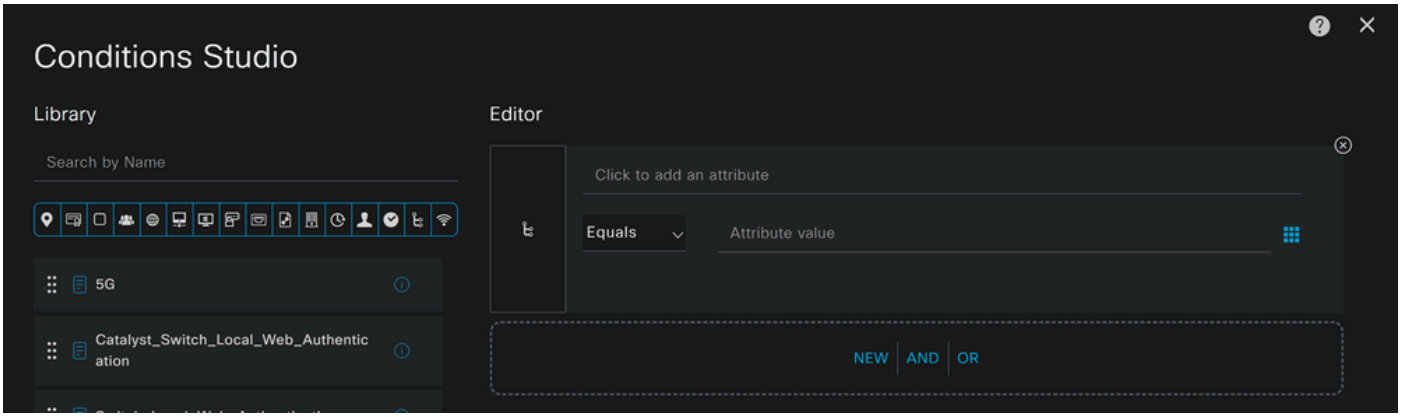
- Fare clic su Policy > Policy Sets
- Fare clic per + aggiungere un nuovo set di criteri



In questo caso, creare un nuovo set di criteri anziché utilizzare quello predefinito. Configurare quindi l'autenticazione e l'autorizzazione in base al criterio impostato. Il criterio configurato consente l'accesso al dispositivo di rete definito nel passaggio Configura elenco dispositivi di rete per verificare che le autenticazioni provengano da CSA Network Device List e quindi accedere al criterio come **Conditions**. E infine, i Protocolli permessi, come **Default Network Access**.

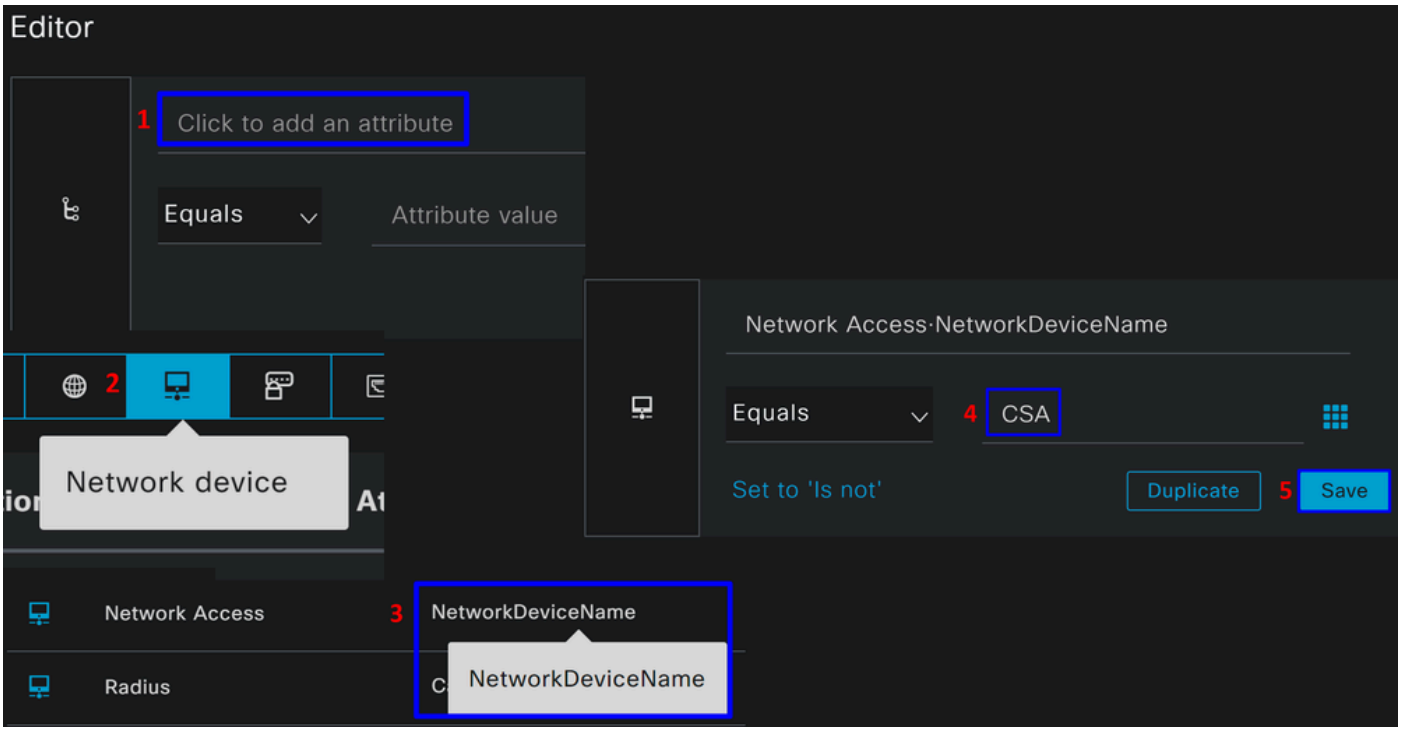
Per creare l'oggetto **condition** che corrisponde al set di criteri, procedere con le istruzioni seguenti:

- Fare clic su +
- Nella sezione **Condition Studio**, le informazioni disponibili includono:



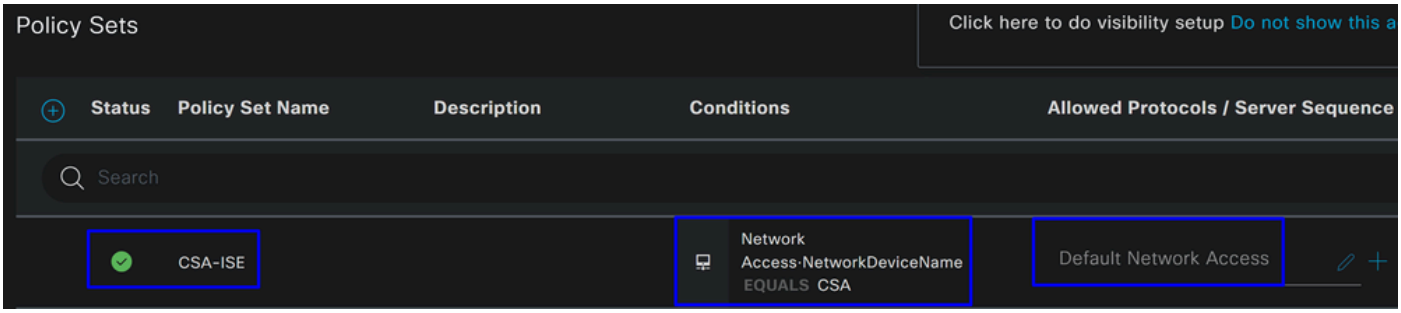
- Per creare le Condizioni, fare clic su Click to add an attribute
- Fare clic sul **Network Device** pulsante
- Sotto le opzioni sottostanti, fare clic su **Network Access - Network Device Name** opzione
- Sotto l'opzione Equals, scrivere il nome del **Network Device** sotto il passaggio Configure Network Devices List

- Fare clic su **Save**

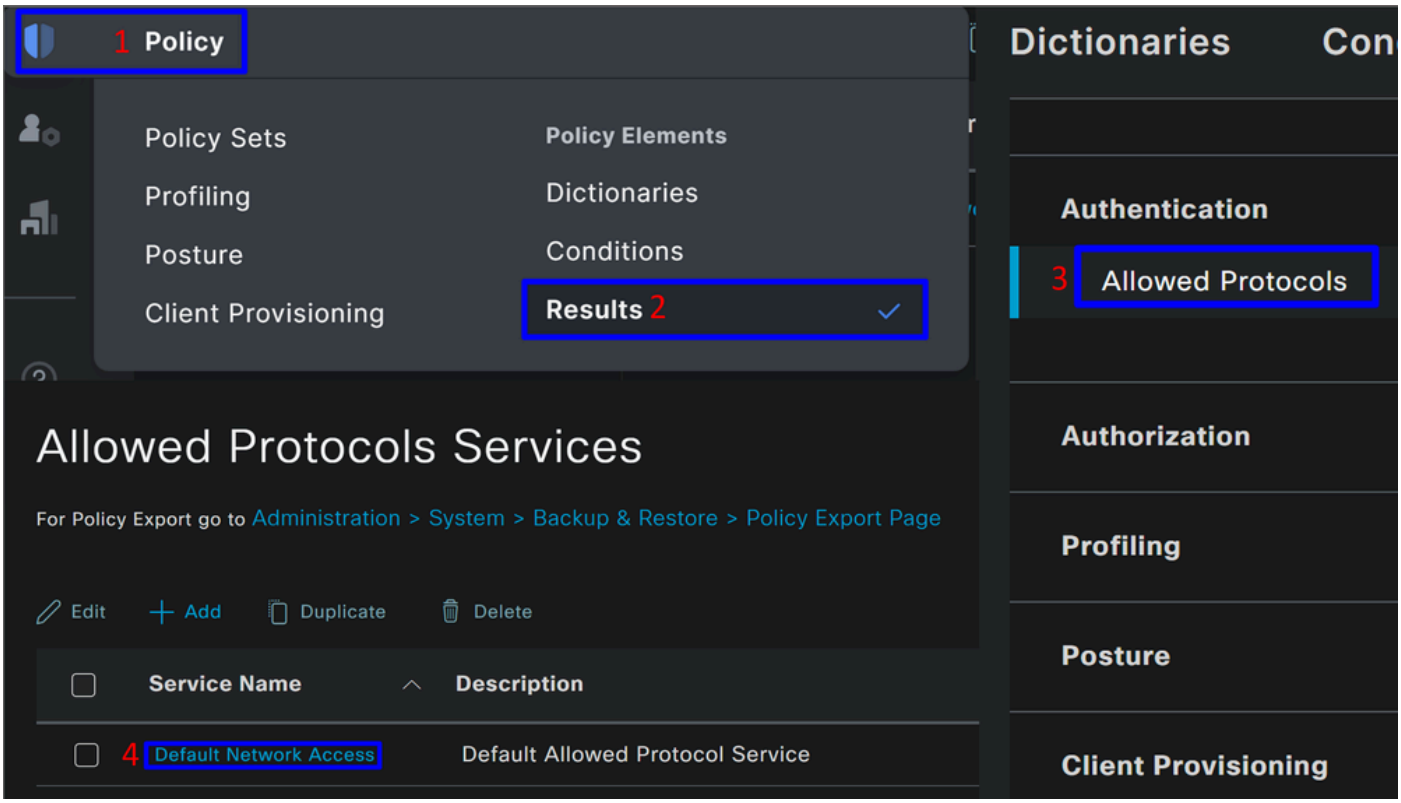


Questo criterio approva solo la richiesta dell'origine CSA di continuare l'installazione **Authentication** e la **Authorization** configurazione in base al set di criteri **CSA-ISE**e verifica i protocolli consentiti in base al **Default Network Access** per i protocolli consentiti.

Il risultato del criterio definito deve essere:



- Per verificare il **Default Network Access Protocols** permesso, procedere con le istruzioni seguenti:
  - Fare clic suPolicy > Results
    - Fare clic su **Allowed Protocols**
    - Fare clic su **Default Network Access**

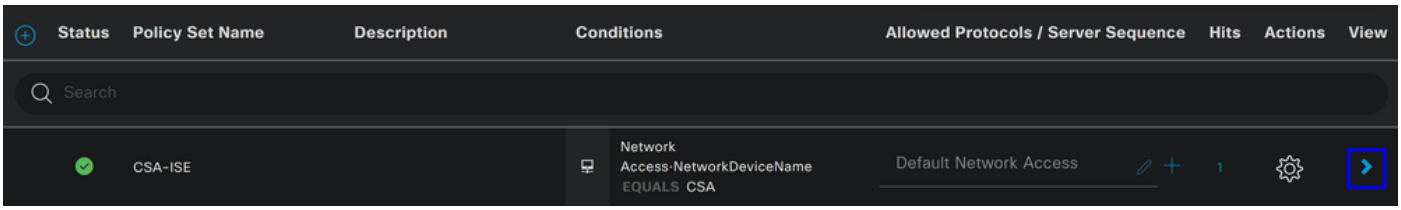


- Quindi, vengono visualizzati tutti i protocolli consentiti su **Default Network Access**

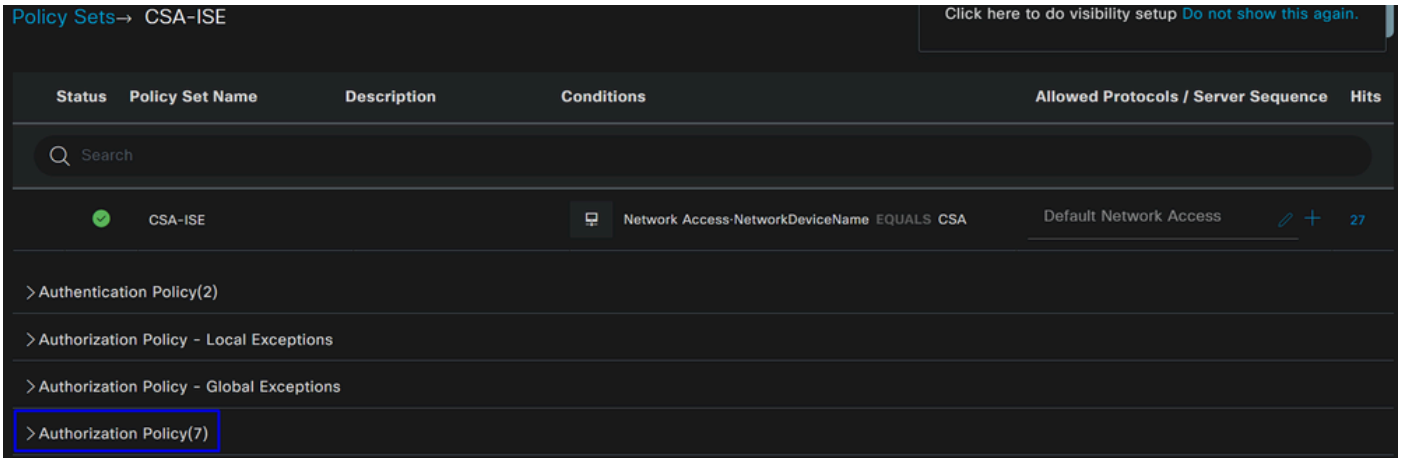
Configura autorizzazione set di criteri

Per creare il **Authorization** criterio in, **Policy Set**procedere come segue:

- Fare clic su >



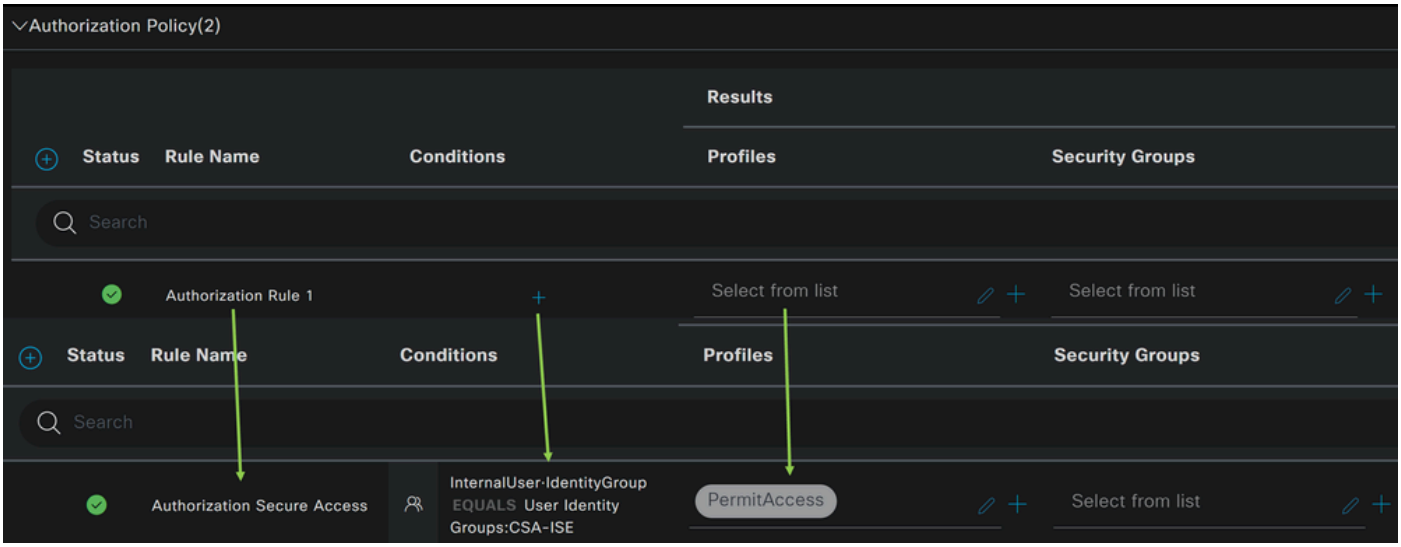
- Successivamente, verranno visualizzati **Authorization** i criteri:



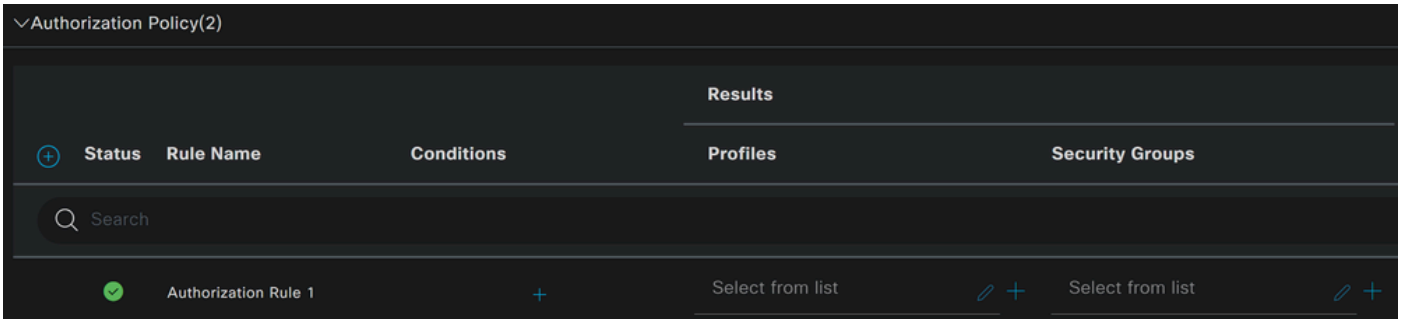
Il criterio è lo stesso definito nel passaggio Configura set di criteri.

Criteri di autorizzazione

È possibile configurare i criteri di autorizzazione in diversi modi. In questo caso, autorizzare solo gli utenti del gruppo definito nel passaggio Configurare un gruppo. Vedere l'esempio successivo per configurare i criteri di autorizzazione:

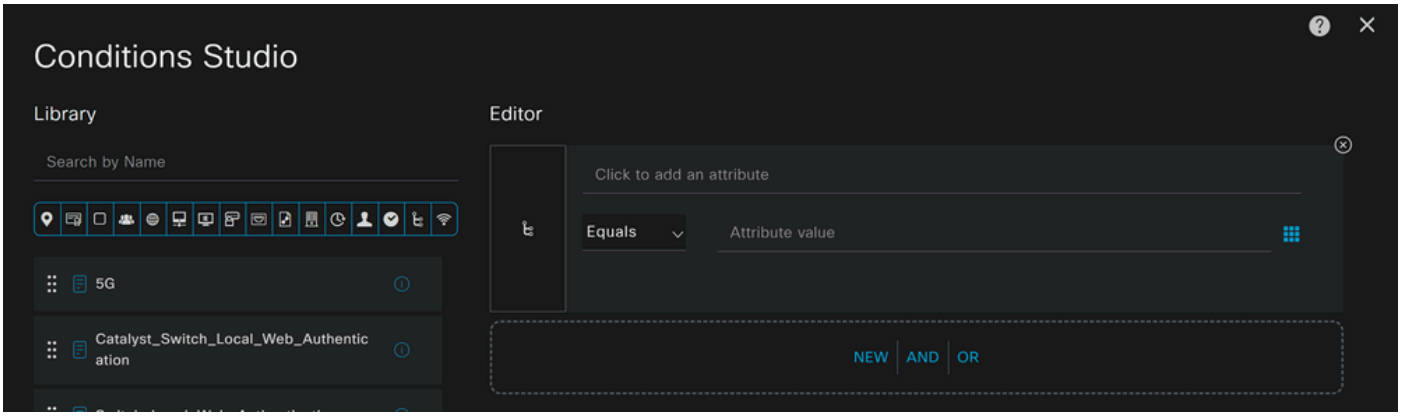


- Fare clic su **Authorization Policy**
- Fare clic su + per definire i criteri per l'autorizzazione nel modo seguente:

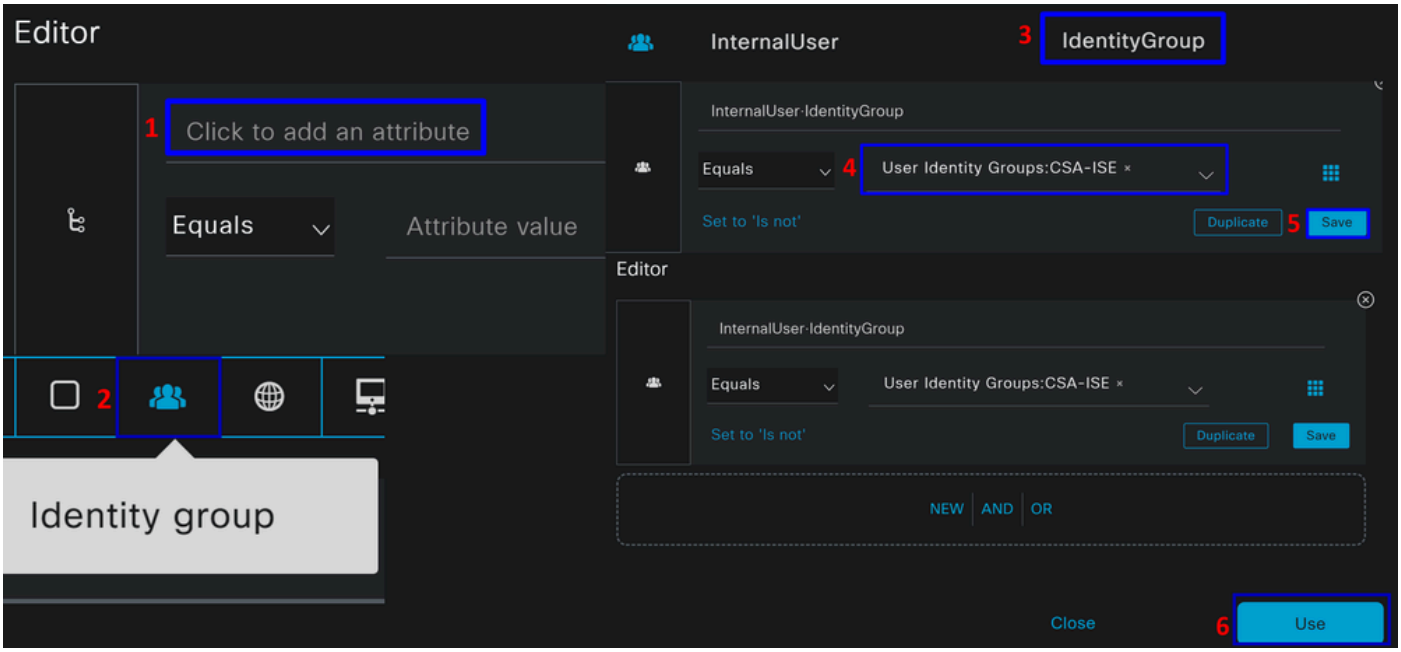


- Per il passo successivo, modificare le Rule Name, Conditionse Profiles

- Quando si imposta il criterio **Name** Configura un nome per identificare facilmente il criterio di autorizzazione
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:

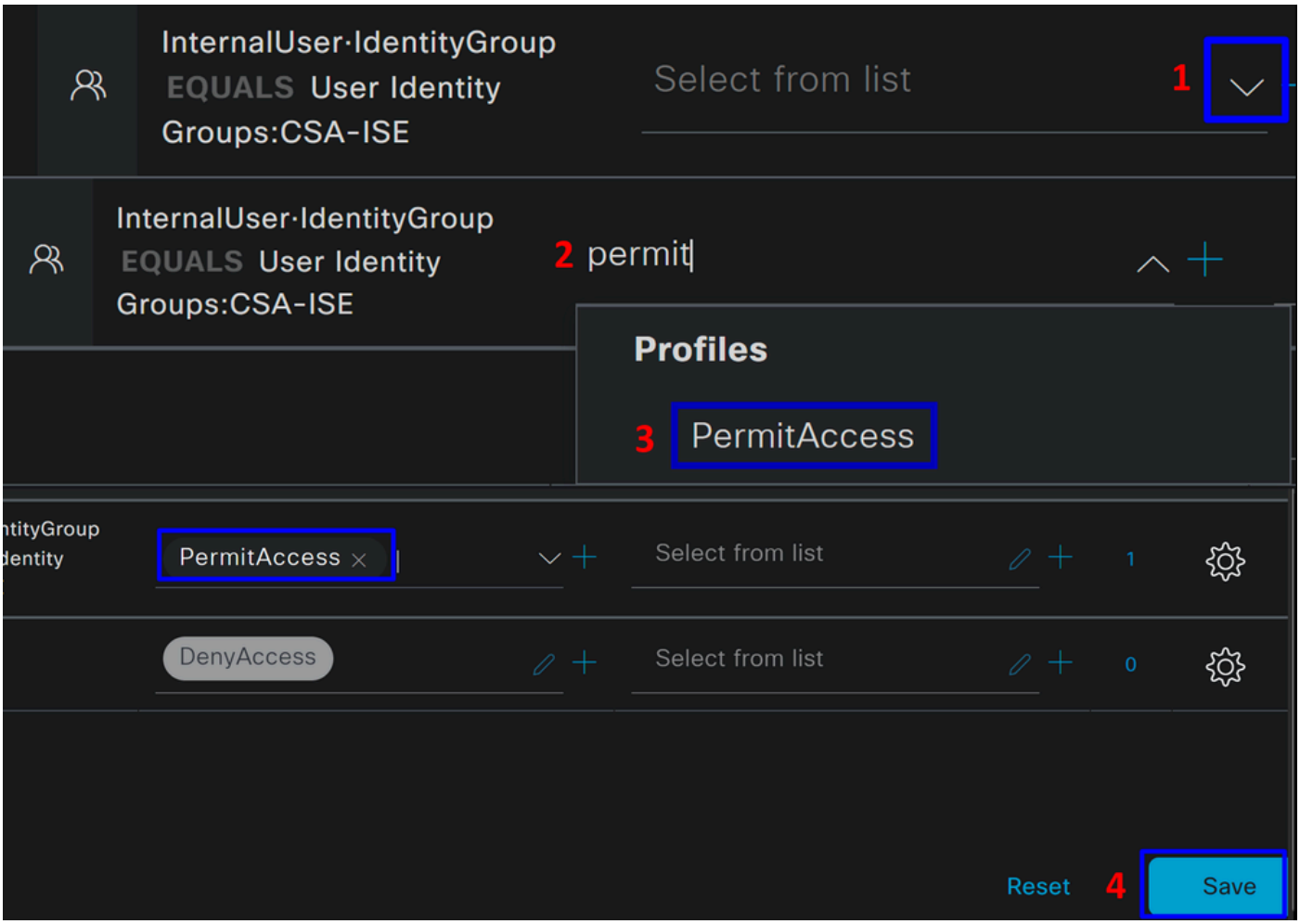


- Per creare le Condizioni, fare clic su Click to add an attribute
- Fare clic sul **Identity Group** pulsante
- Sotto le opzioni sottostanti, fare clic su **Internal User - IdentityGroup** option (Utente interno - opzione)
- Sotto l'**Equals** opzione, utilizzare l'elenco a discesa per trovare il **Group** approvato per l'autenticazione nel passo, Configurare un gruppo
- Fare clic su **Save**
- Fare clic su **Use**



Successivamente, è necessario definire **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Sotto il **Authorization Policy**, fare clic sul pulsante a discesa **Profiles**
- Cerca permesso
- Seleziona **PermitAccess**
- Fare clic su Save

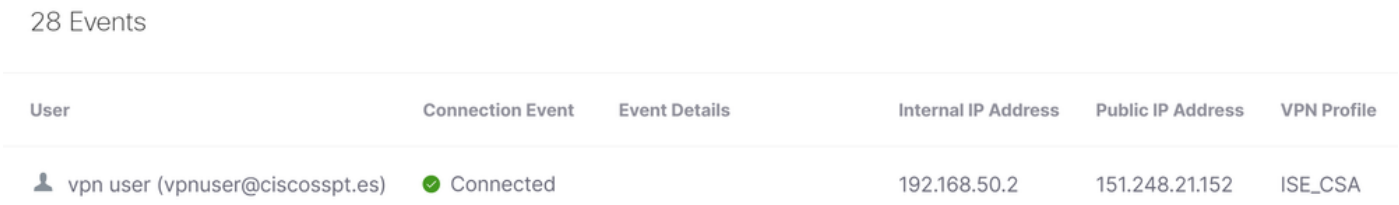


In seguito, hai definito la tua **Authorization** politica. Eseguire l'autenticazione per verificare se l'utente si connette senza problemi e se è possibile visualizzare i log su Secure Access e ISE.

Per connettersi alla VPN, è possibile utilizzare il profilo creato su Secure Access e connettersi tramite Secure Client con il profilo ISE.

- **Come viene visualizzato il registro in Accesso sicuro quando l'autenticazione viene approvata?**
  - Passare al Dashboard di accesso protetto

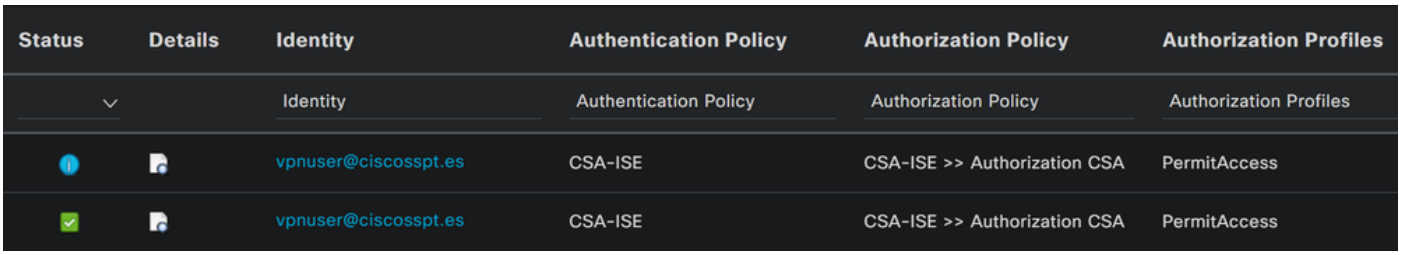
- Fare clic su **Monitor > Remote Access Log**



- **Come viene visualizzato il registro in ISE quando l'autenticazione viene approvata?**

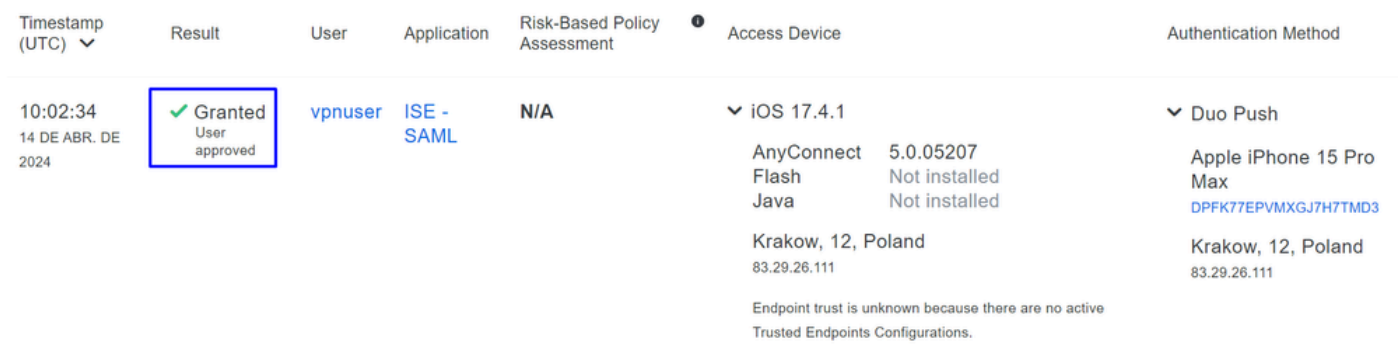
  - Passare alla **Cisco ISE Dashboard**

    - Fare clic su **Operations > Live Logs**



Come viene visualizzato il registro in Duo quando l'autenticazione viene approvata?

- Passare al Pannello Duo Admin
- Fare clic su **Reports > Authentication Log**



Configura utenti locali o di Active Directory Radius

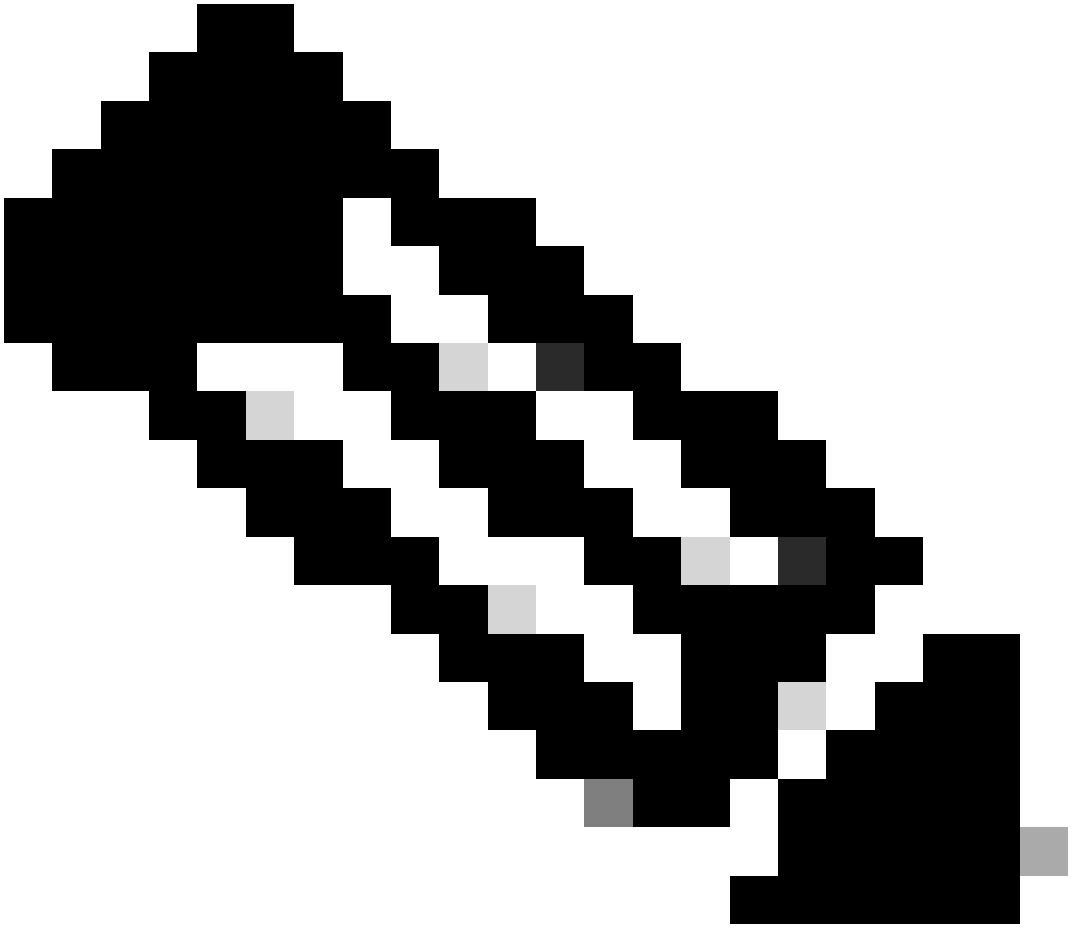
Configurazione della postura ISE

In questo scenario, creare la configurazione per verificare la conformità dell'endpoint prima di concedere o negare l'accesso alle risorse interne.

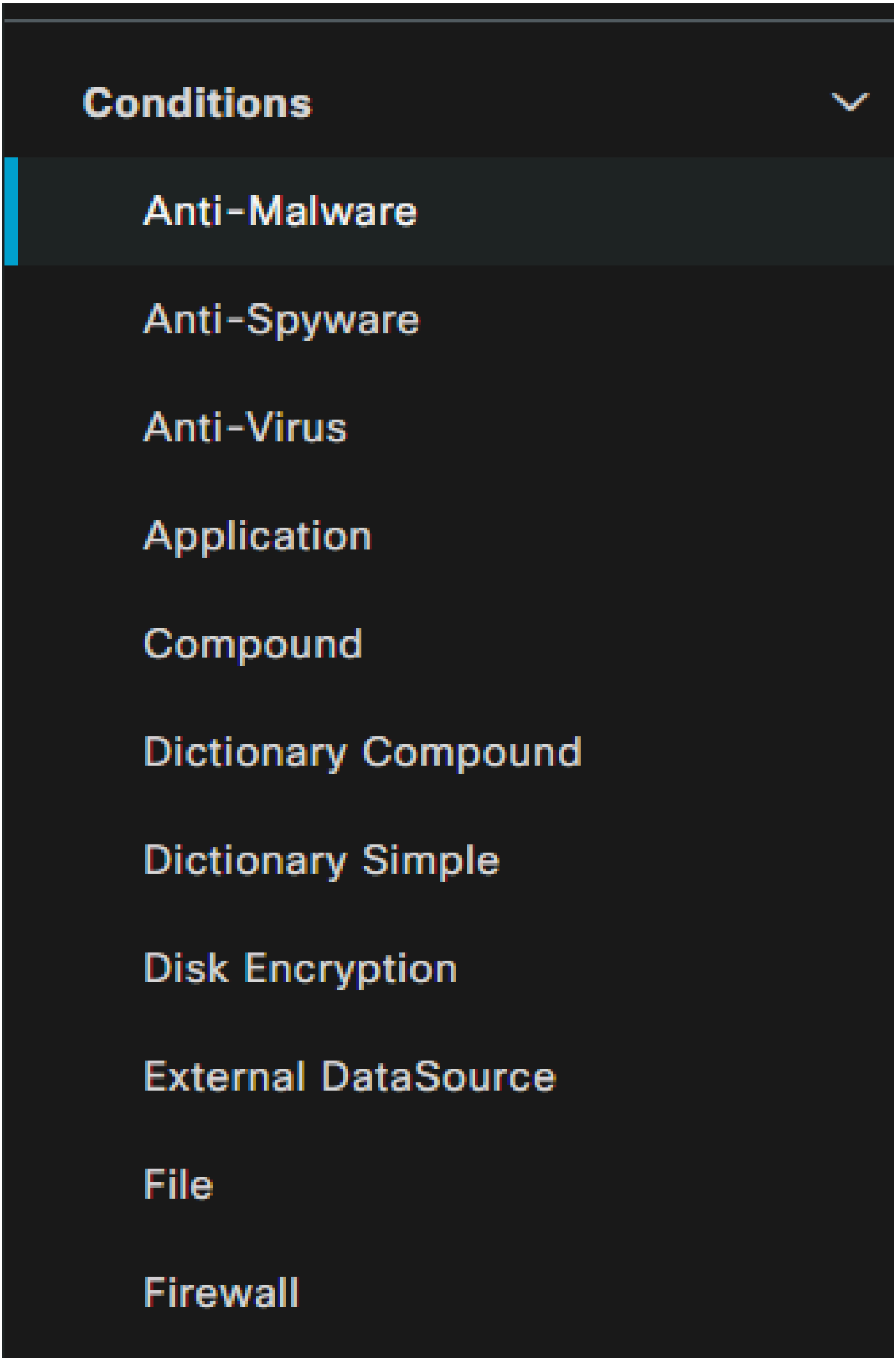
Per configurarlo, procedere con i passaggi seguenti:

Configura condizioni di postura

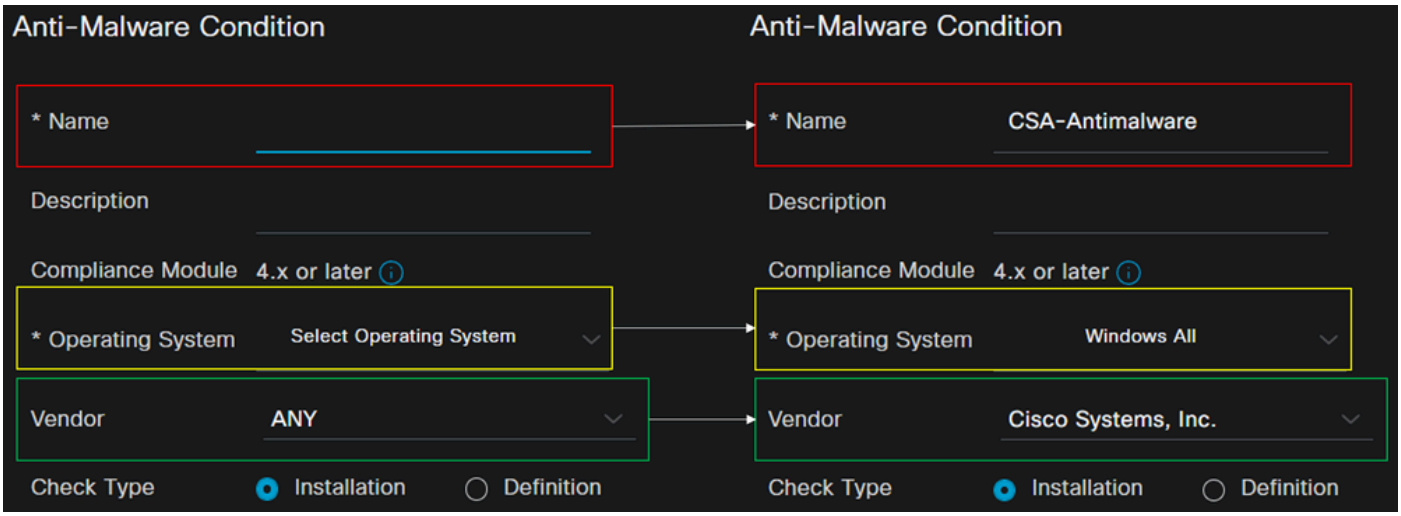
- Passa al dashboard ISE
- Fare clic su **Work Center > Policy Elements > Conditions**
- Fare clic su **Anti-Malware**



Nota: sono disponibili numerose opzioni per verificare la postura dei dispositivi e per effettuare la valutazione corretta in base alle policy interne.

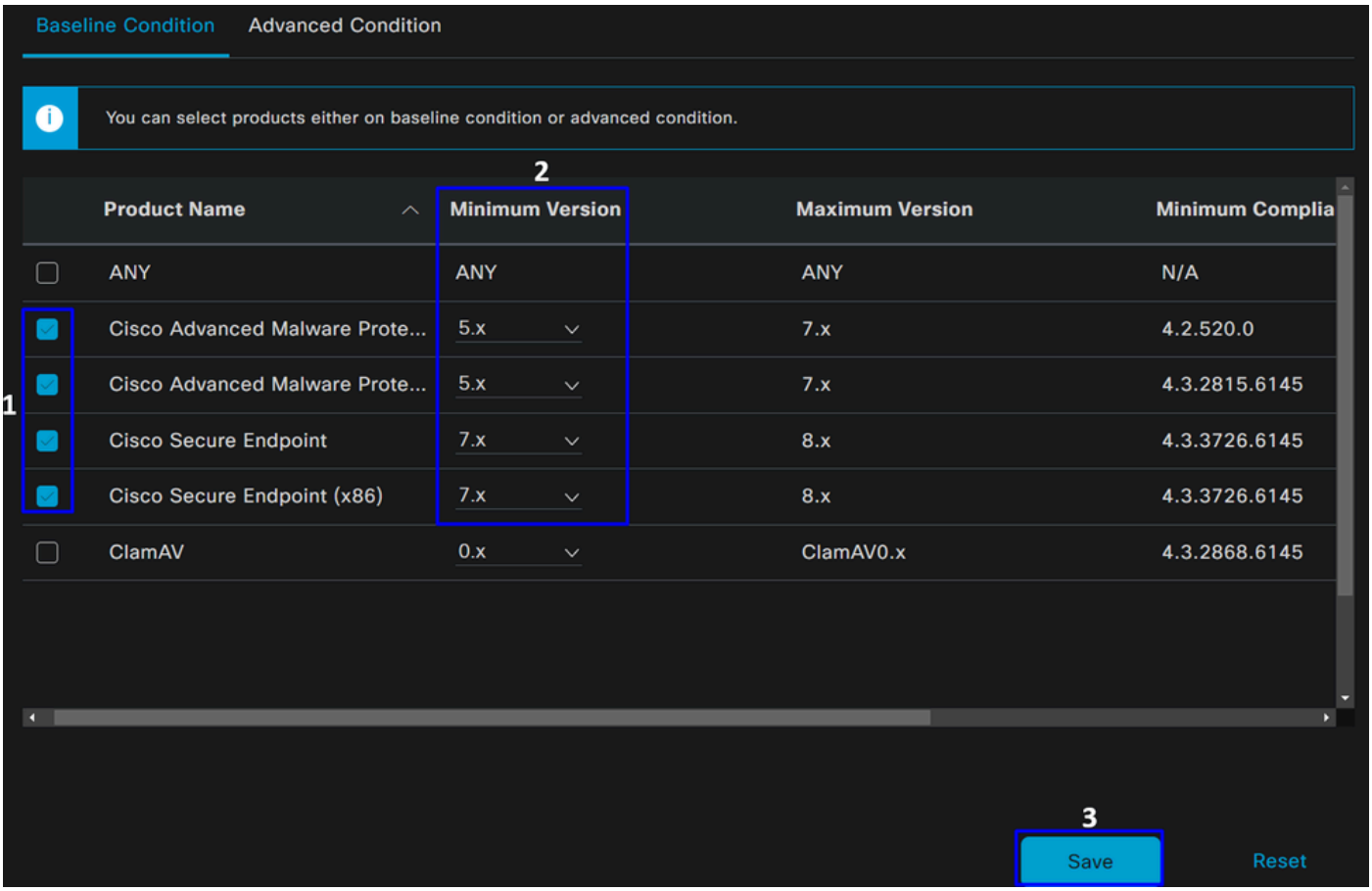

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

Anti-Malware Condition per rilevare l'installazione del software antivirus nel sistema. Se necessario, è inoltre possibile scegliere la versione del sistema operativo.



- **Name**: utilizzare un nome per riconoscere la condizione antimalware
- **Operating System**: scegliere il sistema operativo da impostare come condizione
- **Vendor**: scegliere un fornitore o QUALSIASI
- **Check Type**: è possibile verificare se l'agente è installato o la versione della definizione per l'opzione.

- Per **Products for Selected Vendor**, è possibile configurare ciò che si desidera verificare relativamente all'antimalware sul dispositivo.

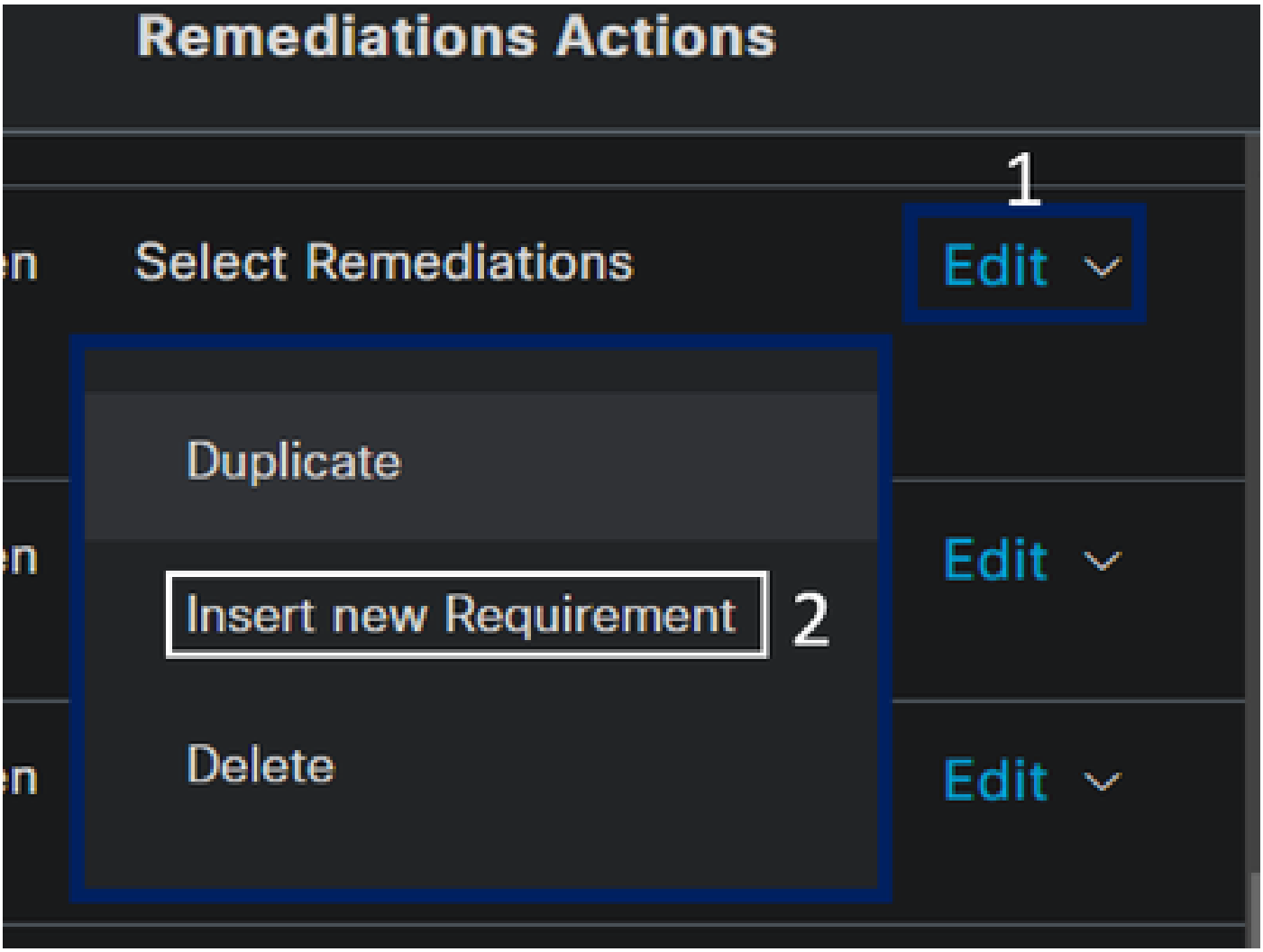


- Selezionare la casella di controllo relativa alle condizioni che si desidera valutare
- Configurare la versione minima da verificare
- Fare clic su Salva per continuare con il passaggio successivo

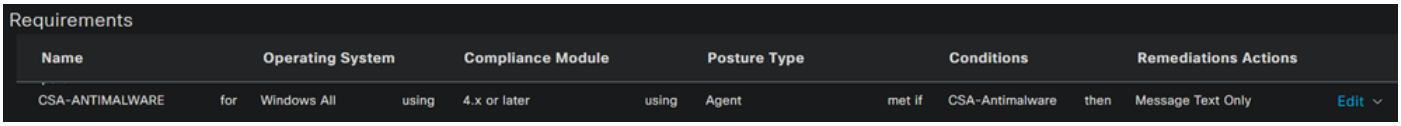
Una volta configurata, è possibile procedere con la procedura, **Configure Posture Requirements**.

Configura requisiti postura

- Passa al dashboard ISE
- Fare clic su **Work Center > Policy Elements > Requeriments**
- Fare clic su uno **Edit** dei requisiti e selezionare **Insert new Requirement**



- In base al nuovo requisito, configurare i parametri successivi:

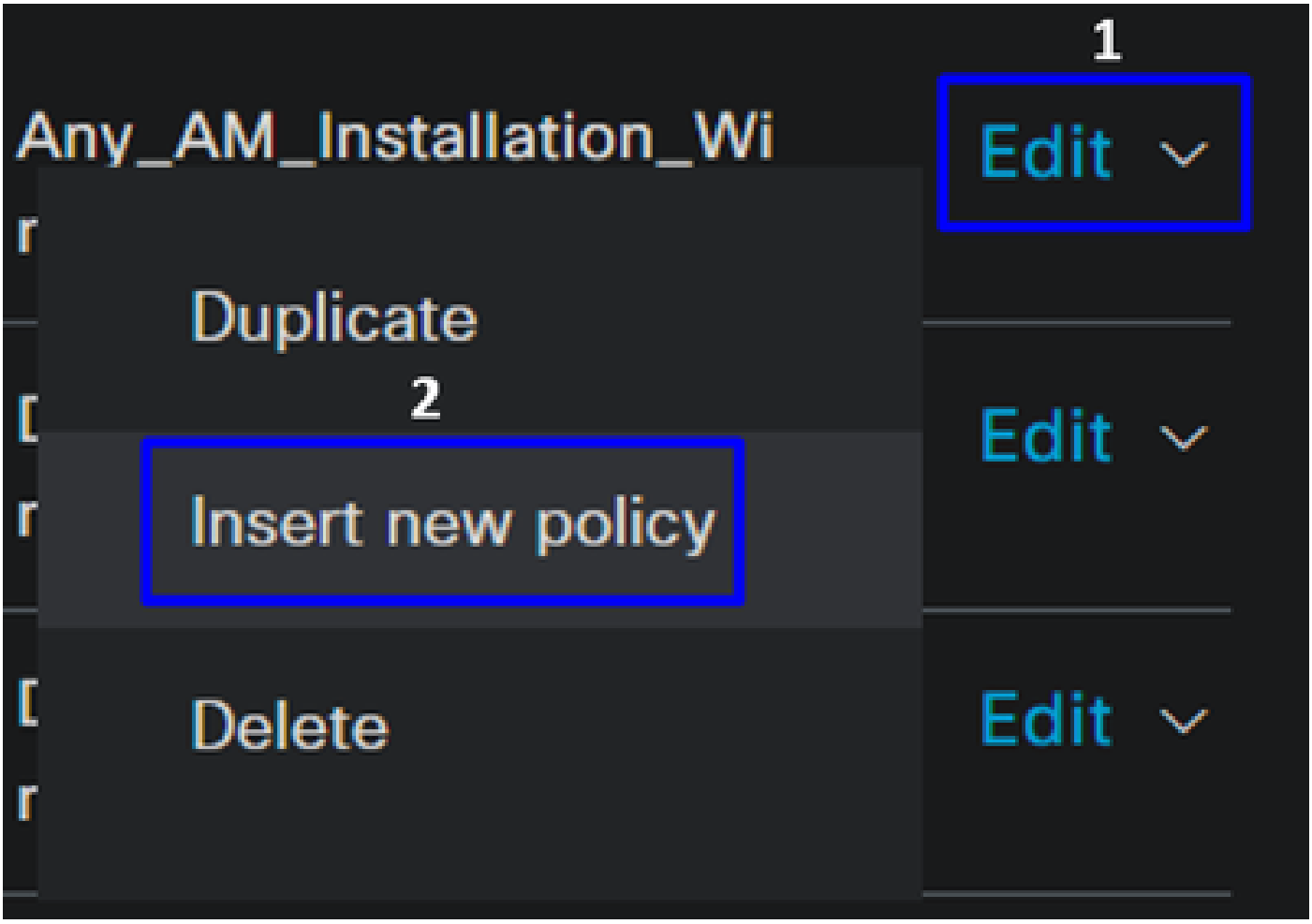


- **Name**: configurare un nome per il riconoscimento dei requisiti antimalware
- **Operating System**: scegliere il sistema operativo scelto nella fase della condizione Sistema operativo.
- **Compliance Module**: è necessario assicurarsi di selezionare lo stesso modulo di conformità che si ha nella fase della condizione Condizione antimalware
- **Posture Type**: Scegli agente
- **Conditions**: scegliere la condizione o le condizioni create nel passo Configura condizioni di postura.
- **Remediations Actions**: scegliere questa opzione **Message Text Only** per l'esempio oppure, se si dispone di un'altra azione correttiva, utilizzarla
- Fare clic su **Save**

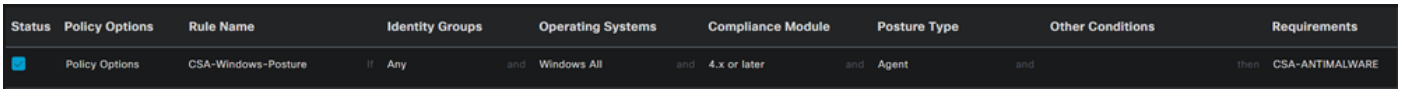
Una volta configurata, è possibile procedere con la procedura, **Configure Posture Policy**

Configura criterio postura

- Passa al dashboard ISE
- Fare clic su **Work Center > Posture Policy**
- Fare clic su uno **Edit** dei criteri e selezionare **Insert new Policy**



- In base al nuovo criterio, configurare i parametri successivi:



- **Status**: selezionare la casella di controllo per attivare il criterio
- **Rule Name**: configurare un nome per il riconoscimento del criterio configurato

- **Identity Groups**: scegliere le identità da valutare
- **Operating Systems**: scegliere il sistema operativo in base alla condizione e ai requisiti configurati prima
- **Compliance Module**: scegliere il modulo di conformità in base alla condizione e al requisito configurati prima
- Posture Type: Scegli agente
- **Requeriments**: scegliere i requisiti configurati nella fase, Configura requisiti postura.
- Fare clic su **Save**

Configura provisioning client

Per fornire agli utenti il modulo ISE, configurare il provisioning del client in modo che i computer dispongano del modulo ISE Posture. Ciò consente di verificare la postura dei computer dopo l'installazione dell'agente. Per continuare con questo processo, procedere come segue:

Passare al dashboard ISE.

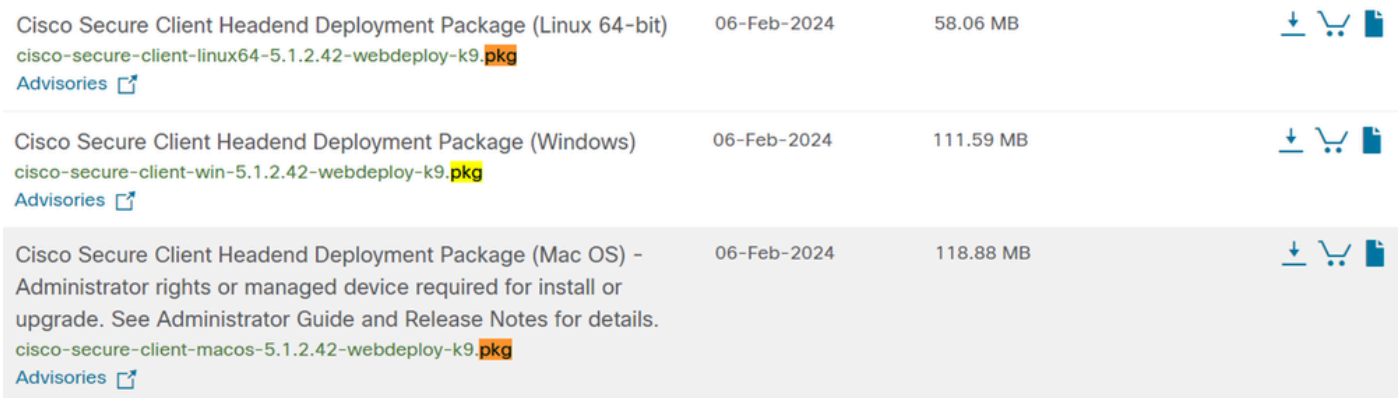
- Fare clic su **Work Center > Client Provisioning**
- Scegli **Resources**

In provisioning client è necessario configurare tre elementi:

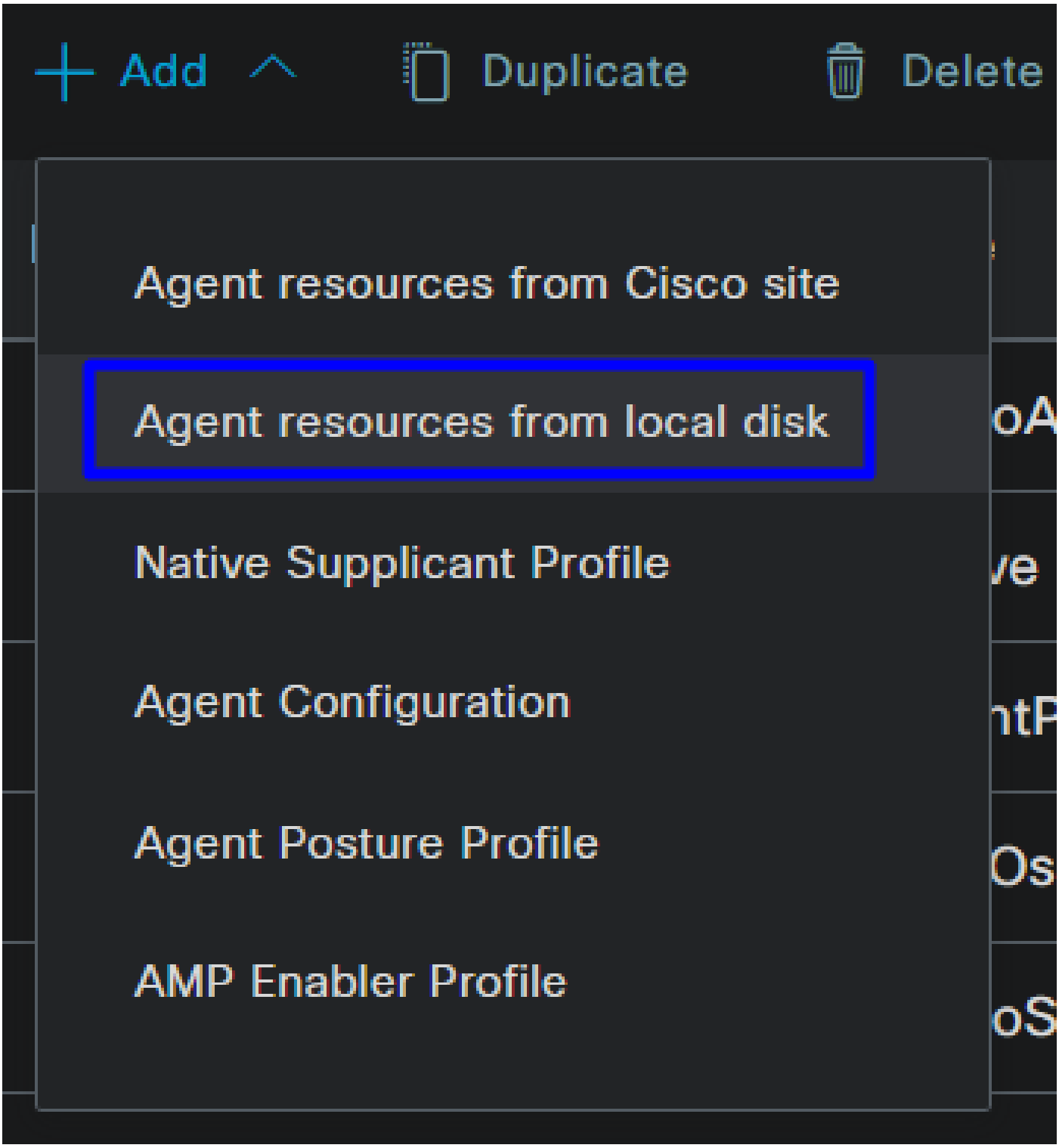
Risorse da configurare	Descrizione
1. **Agent Resources**	Pacchetto di provisioning Web client sicuro.
2. **Compliance Module**	Cisco ISE Compliance Module
3. **Agent Profile**	Controllo del profilo di provisioning.
3. **Agent Configuration**	Definire i moduli di cui eseguire il provisioning impostando il portale di provisioning, utilizzando il profilo agente e le risorse agente.

Step 1 Scarica e carica risorse agente

- Per aggiungere una nuova risorsa agente, accedere al portale di download Cisco e scaricare il pacchetto di distribuzione Web. Il file di distribuzione Web deve essere in formato .pkg.

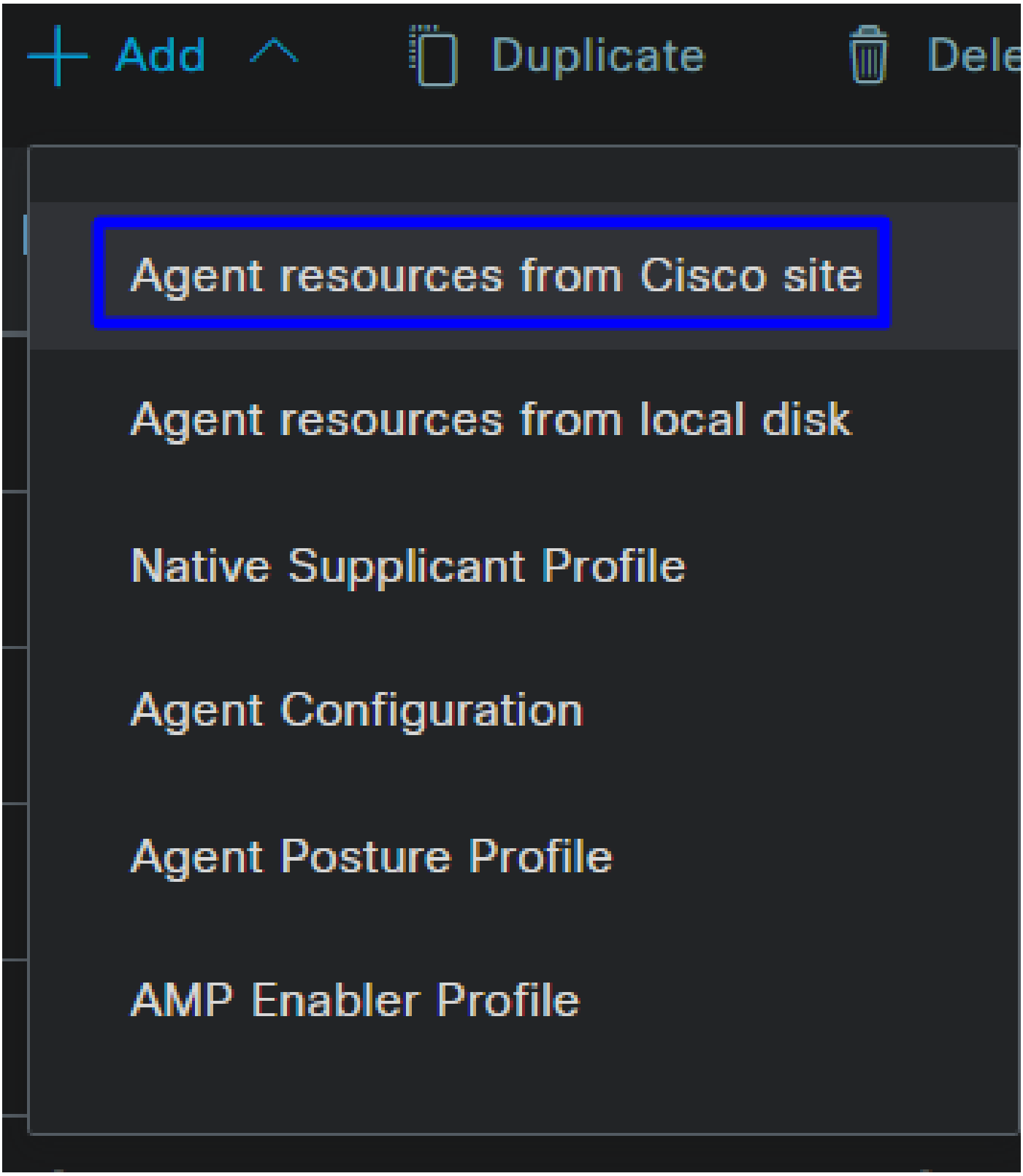


- Fare clic su + Add > Agent resources from local disk e caricare i pacchetti

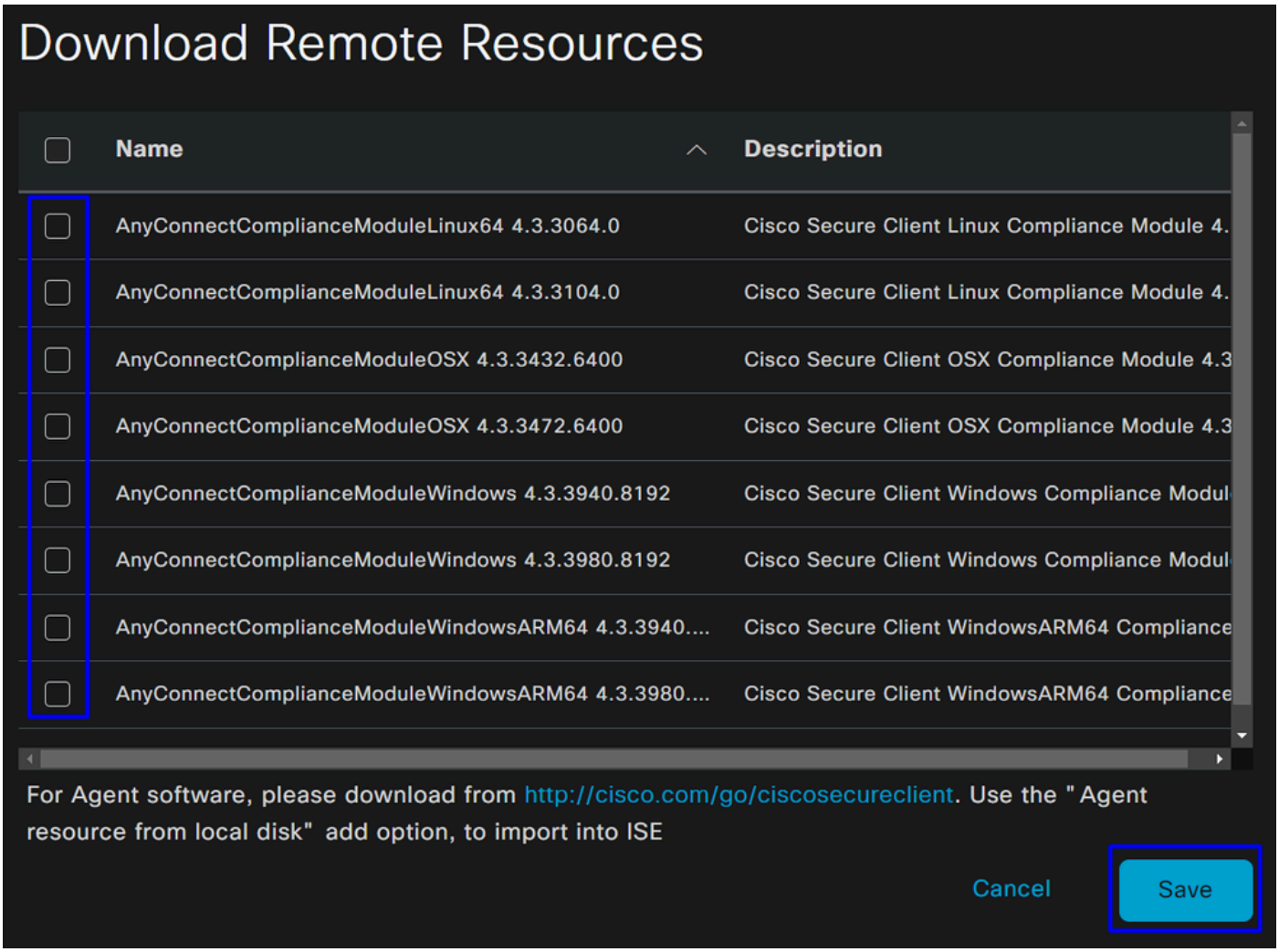


Step 2 Scarica il modulo sulla conformità

- Fare clic su + Add > Agent resources from Cisco Site

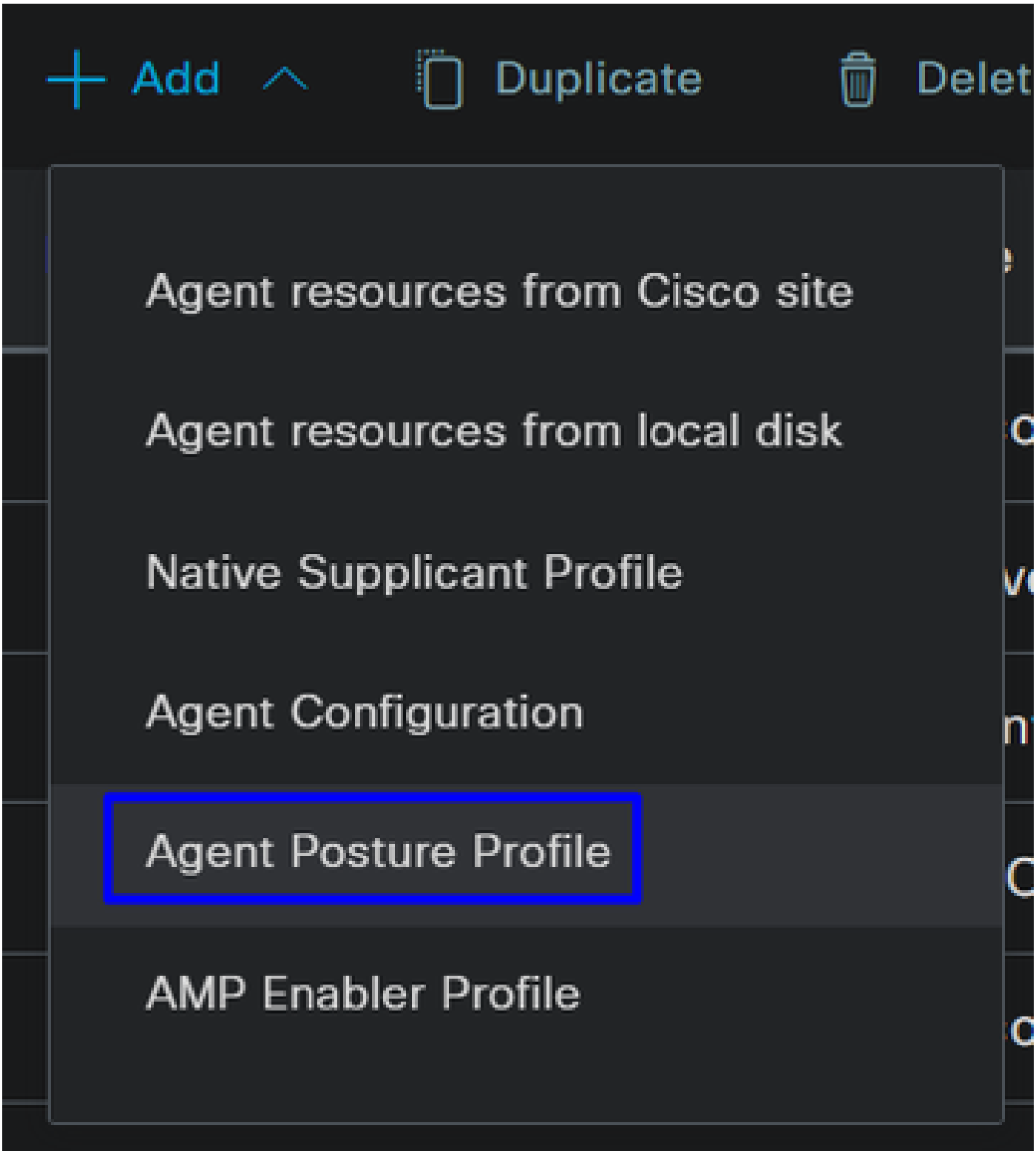


- Selezionare la casella di controllo per ogni modulo di conformità necessario e fare clic su **Save**

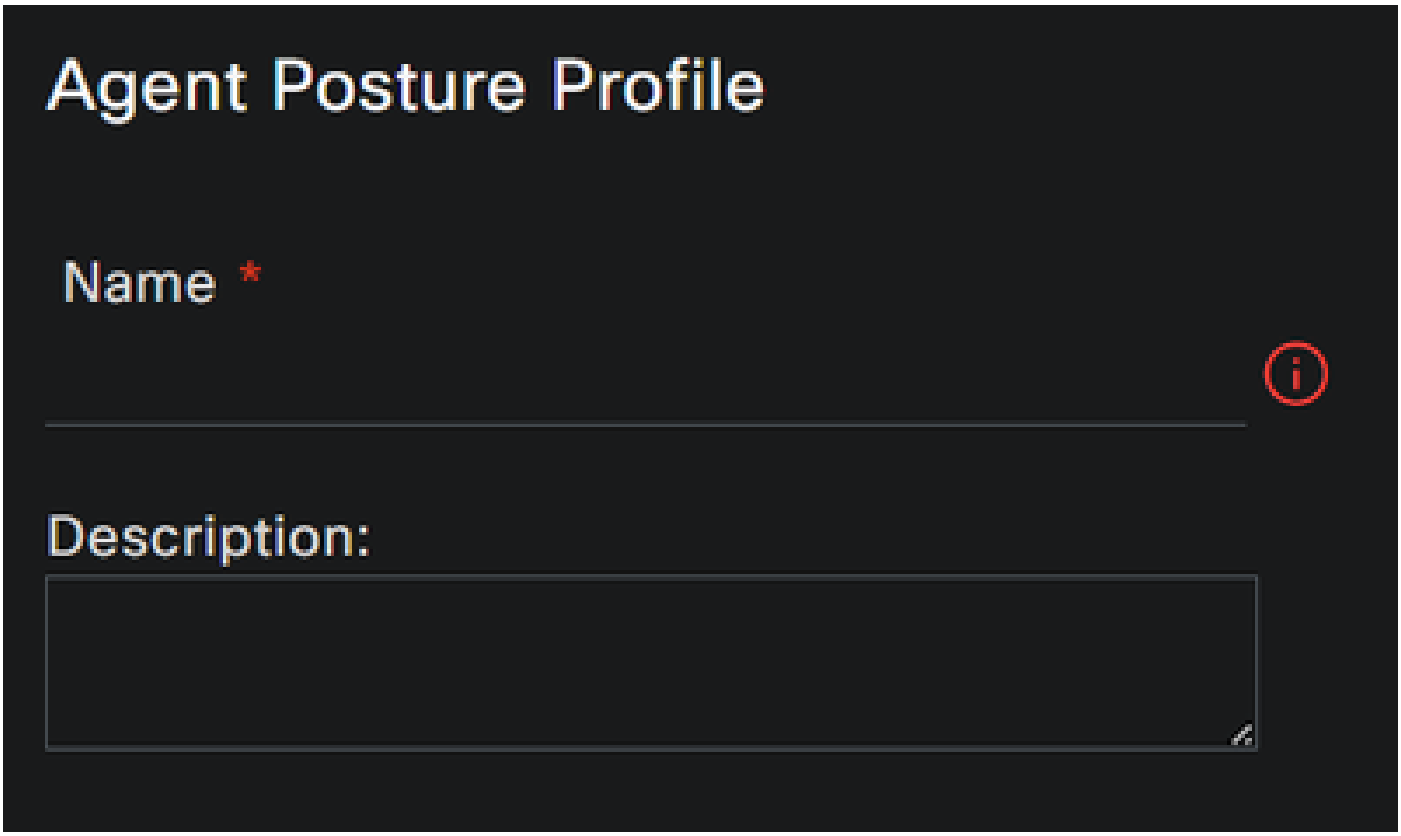


Step 3Configurare il profilo agente

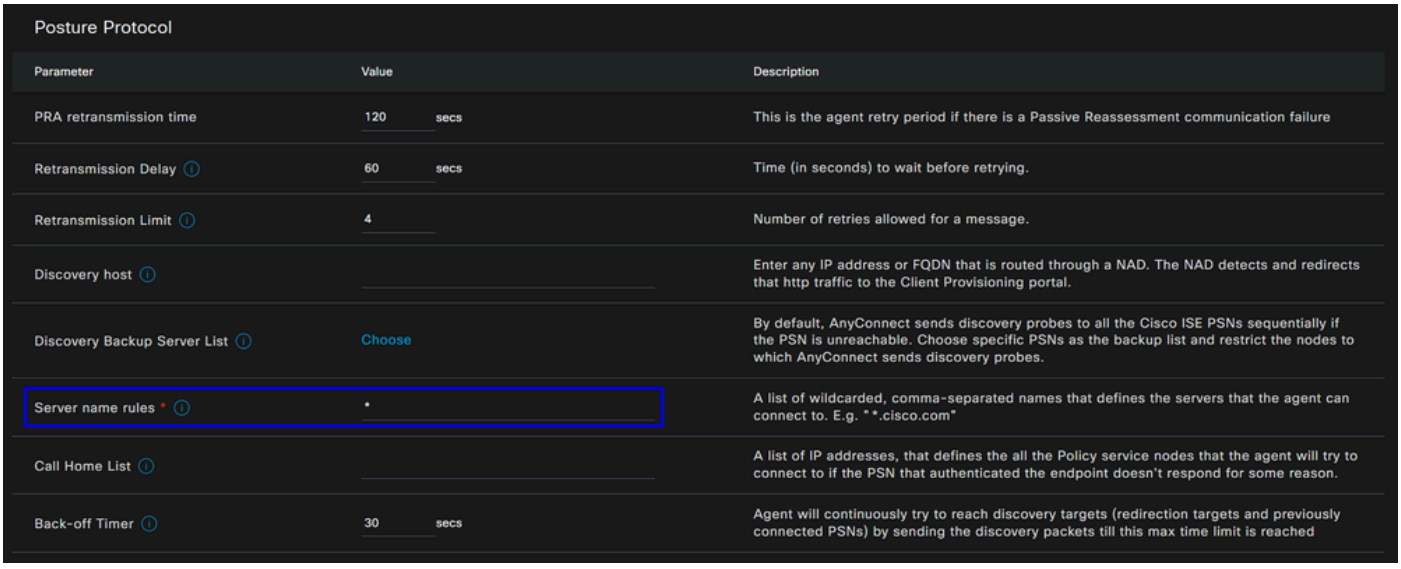
- Fare clic su + Add > Agent Posture Profile



- Creare un **Name** file per **Posture Profile**

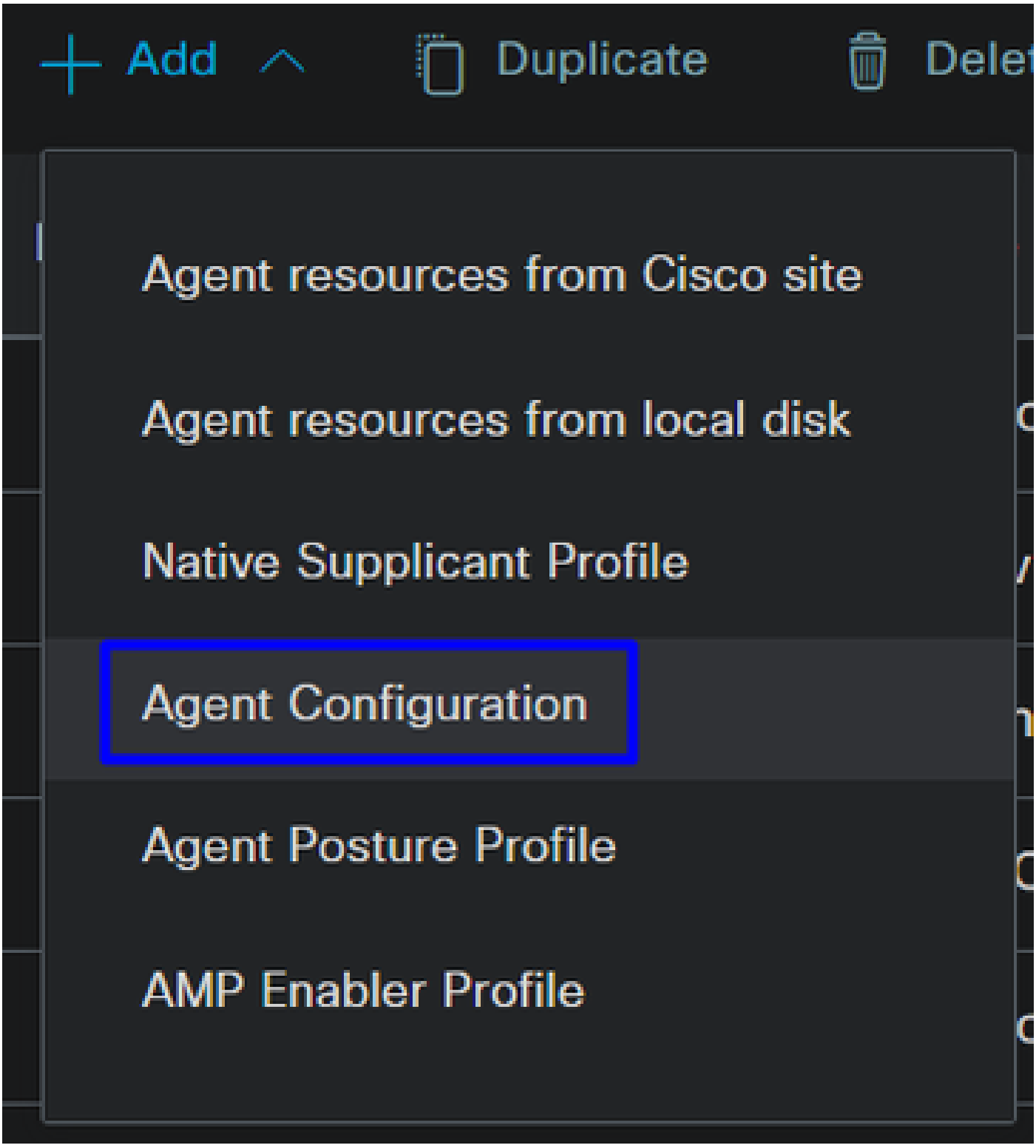


- In Regole nome server inserire un nome ***** e fare clic **Save** dopo

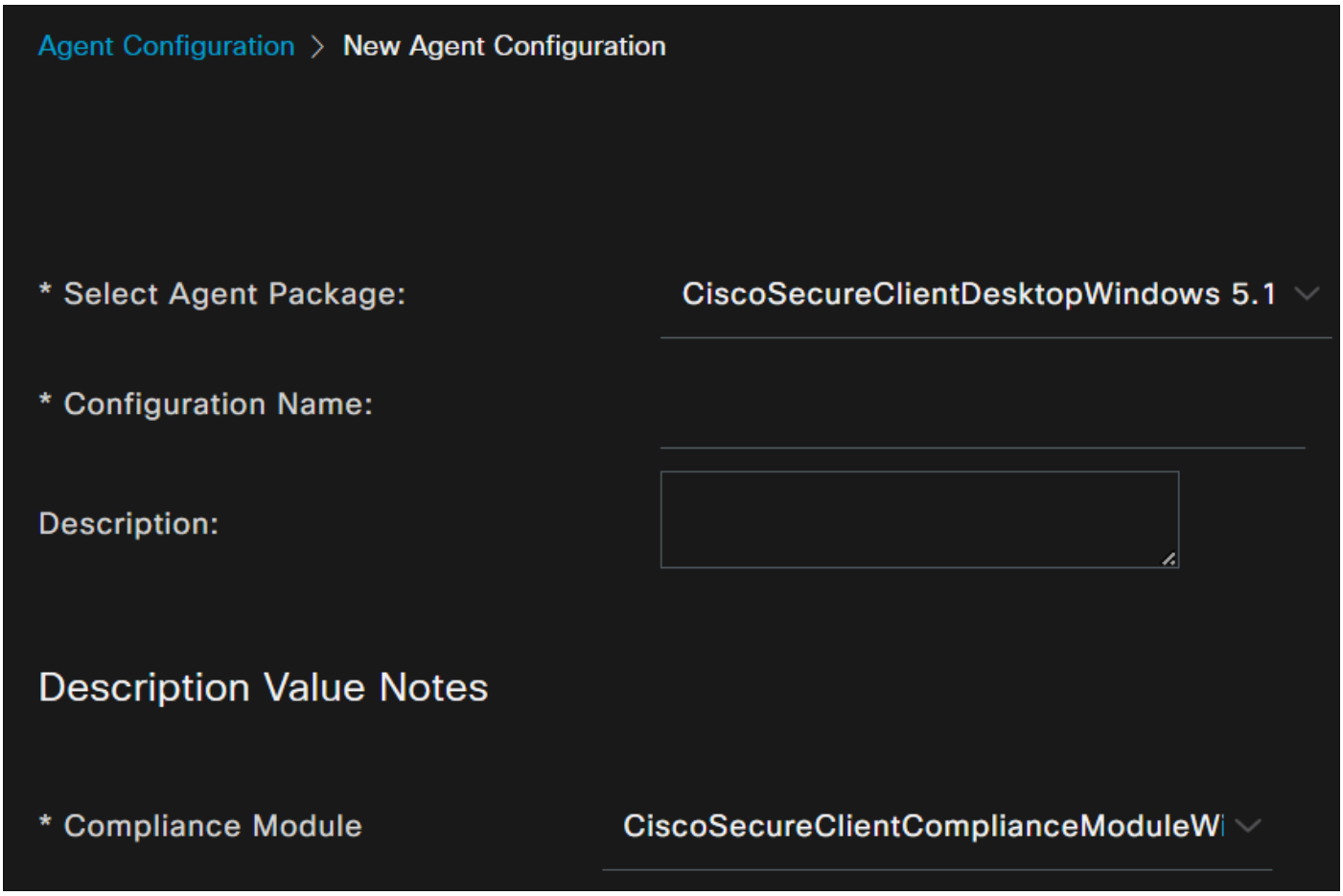


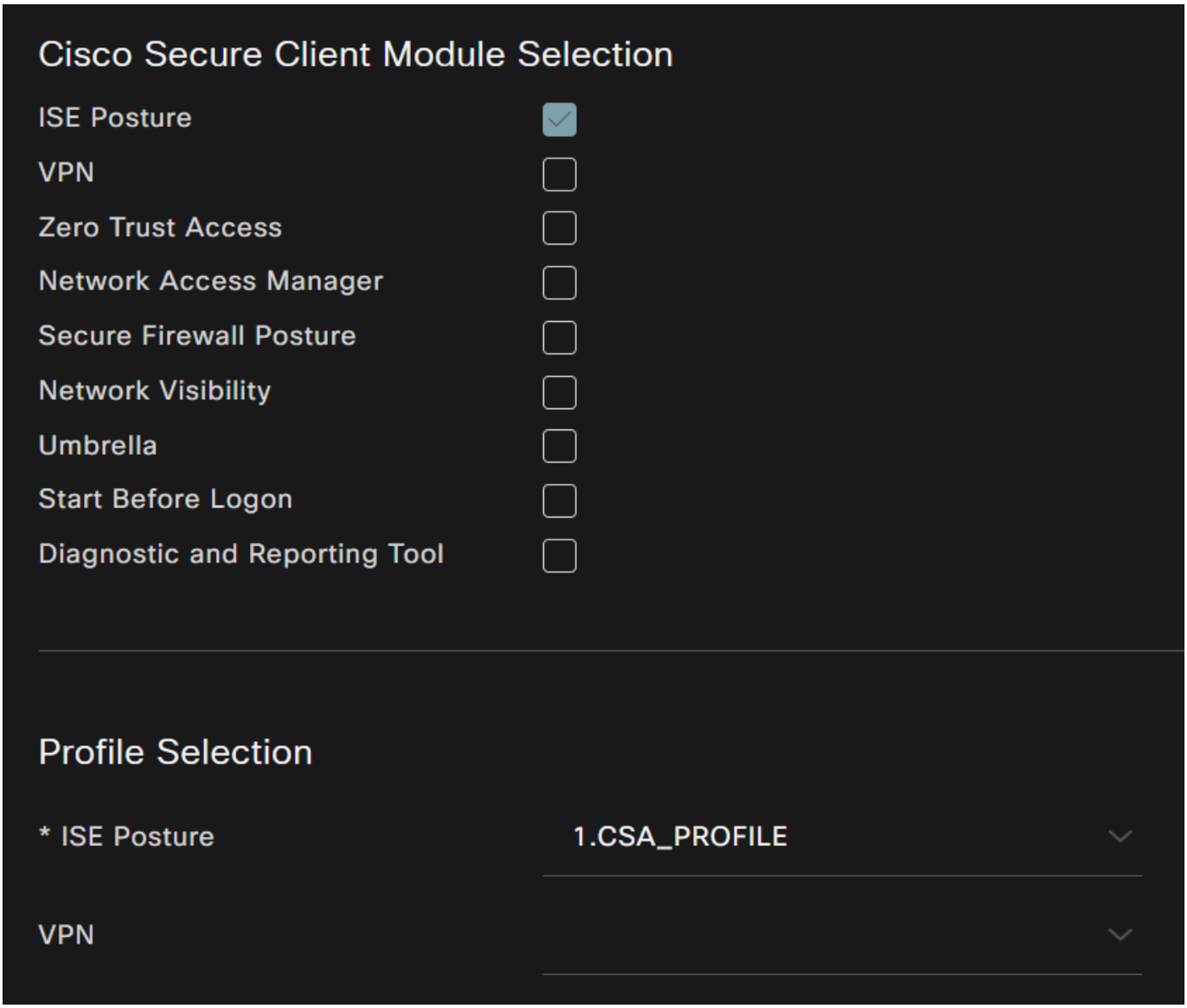
Step 4 Configurazione dell'agente

- Fare clic su + Add > Agent Configuration



- Quindi, configurare i parametri successivi:

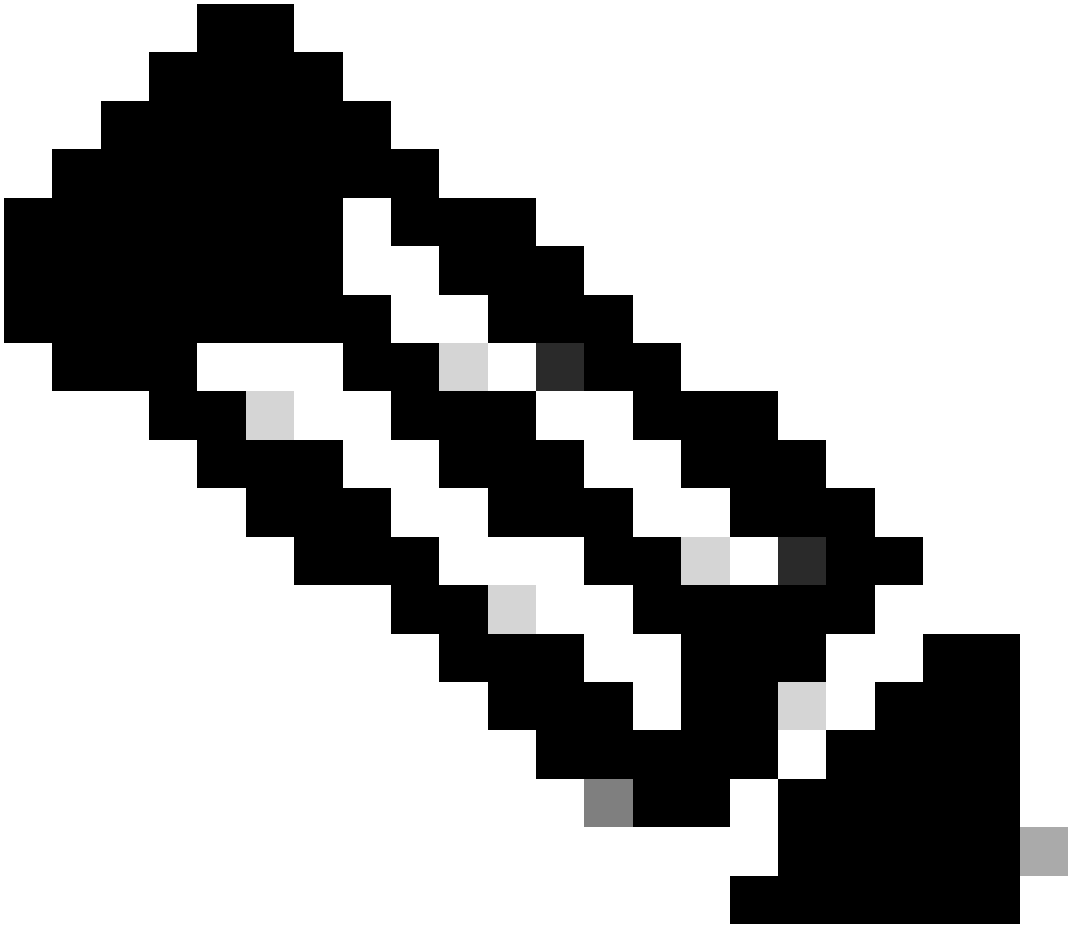

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package : scegliere il pacchetto caricato in Step1 Download and Upload Agent Resources.
- **Configuration Name**: scegliere un nome per riconoscere **Agent Configuration**
- **Compliance Module**: scegliere il Modulo di conformità scaricato nella Fase 2 Scaricare il modulo di conformità
- Cisco Secure Client Module Selection
  - **ISE Posture**: selezionare la casella di controllo
- **Profile Selection**

- **ISE Posture**: scegliere il profilo ISE configurato nel passo 3 Configurazione del profilo dell'agente

- Fare clic su **Save**

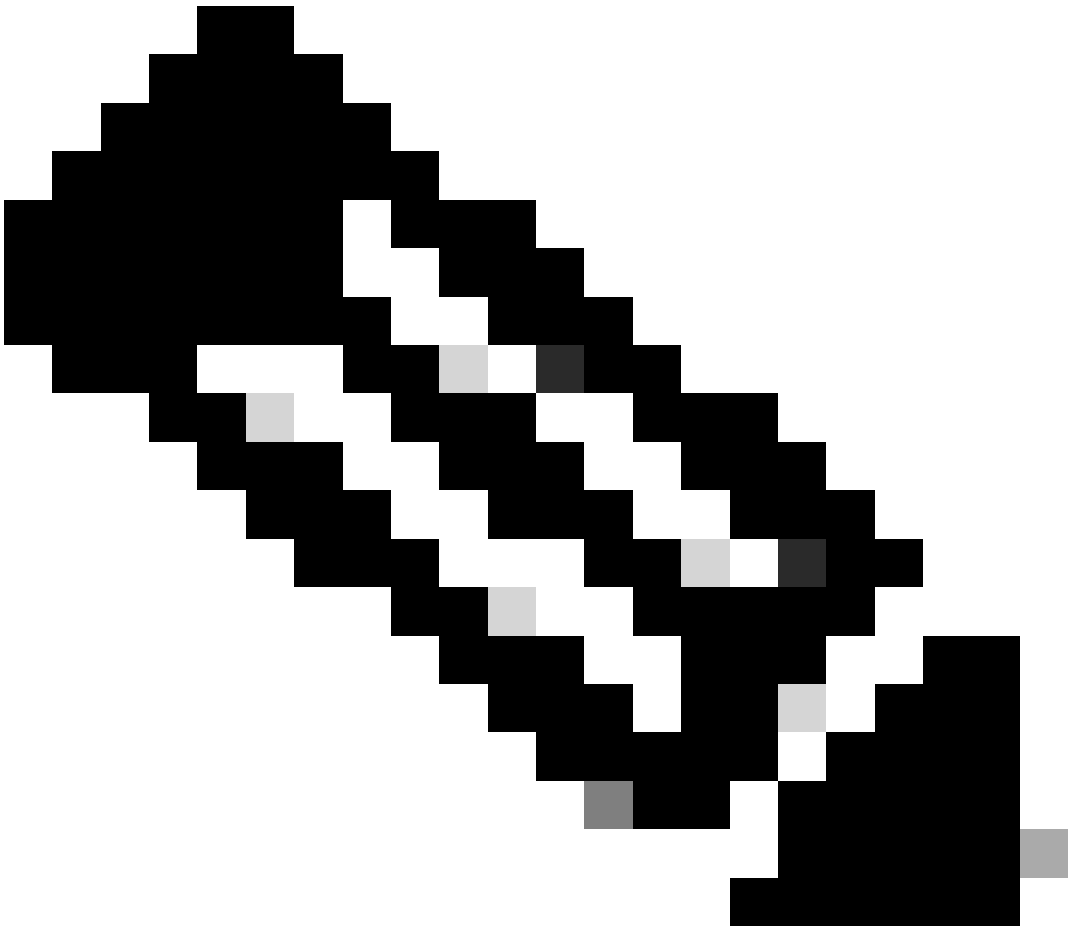


Nota: si consiglia che ogni sistema operativo, Windows, Mac OS o Linux, disponga di una configurazione client indipendente.

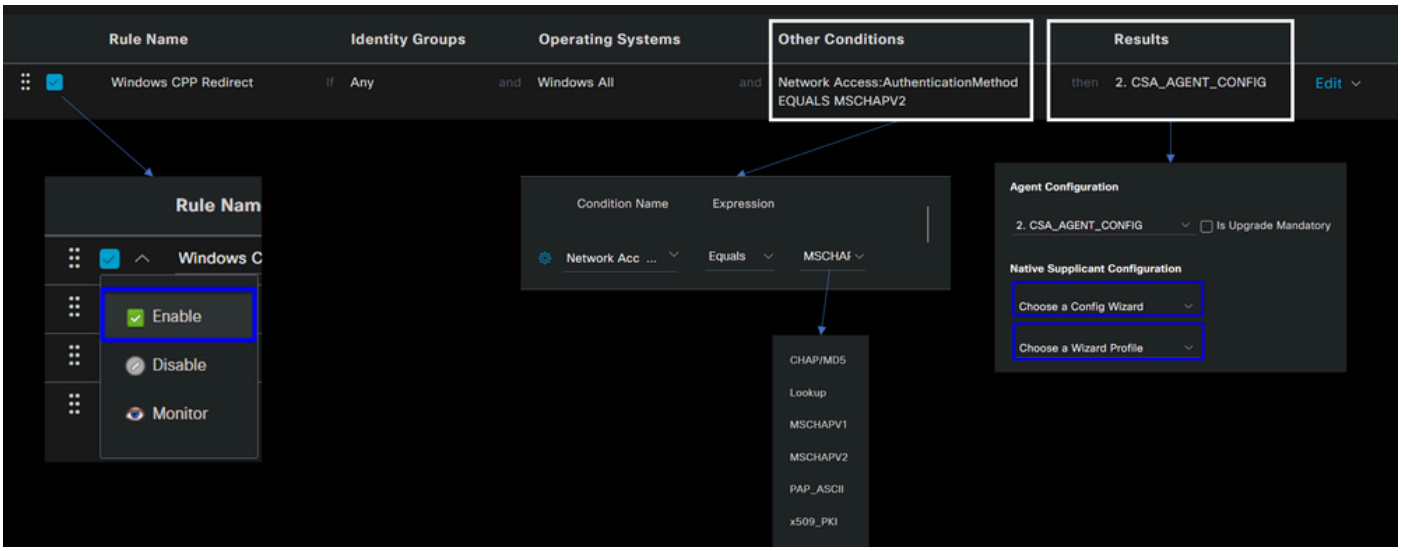
Configura criterio di provisioning client

Per abilitare il provisioning della postura ISE e dei moduli configurati nell'ultimo passaggio, è necessario configurare una policy per eseguire il provisioning.

- Passa al dashboard ISE
- Fare clic su **Work Center > Client Provisioning**



Nota: si consiglia che ogni sistema operativo, Windows, Mac OS o Linux, disponga di un criterio di configurazione client.



- **Rule Name**: configurare il nome del criterio in base al tipo di dispositivo e alla selezione del gruppo di identità in modo da semplificare l'identificazione di ogni criterio
- **Identity Groups**: scegliere le identità da valutare in base ai criteri
- **Operating Systems**: scegliere il sistema operativo in base al pacchetto dell'agente selezionato nella fase Select Agent Package.
- **Other Condition**: scegliere in **Network Access** base al**Authentication Method**EQUALS metodo configurato nella fase, Aggiungi gruppo RADIUS o lasciare vuoto
- **Result**: scegliere la configurazione dell'agente configurata nel passo 4 Configurare la configurazione dell'agente
    - **Native Supplicant Configuration**: Scegli Config Wizarde Wizard Profile
- Contrassegnare il criterio come abilitato se non è elencato come abilitato nella casella di controllo.

Creare i profili di autorizzazione

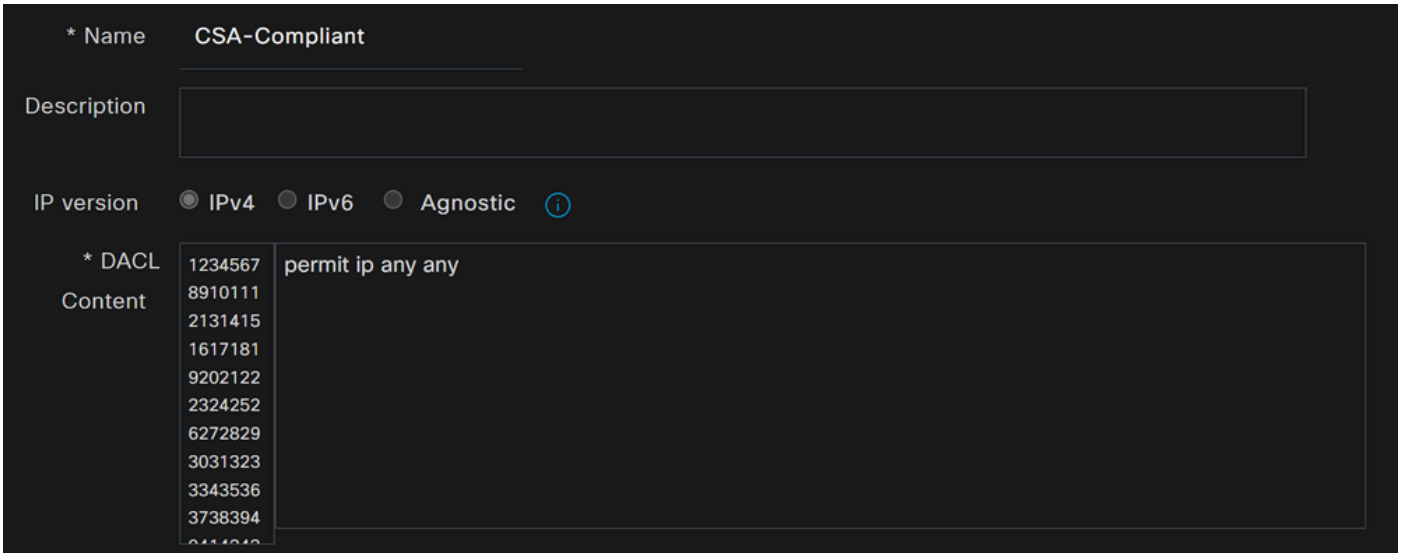
Il profilo di autorizzazione limita l'accesso alle risorse a seconda della postura dell'utente dopo il passaggio di autenticazione. È necessario verificare l'autorizzazione per determinare a quali risorse l'utente può accedere in base alla postura.

Profilo di autorizzazione	Descrizione
Conforme	Conforme utente - Agente installato - Postura verificata

Conforme sconosciuto	Utente non conforme - Reindirizza per installare l'agente - Postura in sospeso da verificare
NegaAccesso	Utente non conforme - Nega accesso

Per configurare il DACL, passare al dashboard ISE:

- Fare clic su **Work Centers > Policy Elements > Downloadable ACLs**
- Fare clic su **+Add**
- Creare la **Compliant DACL**



- **Name**: consente di aggiungere un nome che fa riferimento alla conformità DACL
- **IP version**: Scegli **IPv4**
- DACL Content: crea un elenco di controllo di accesso scaricabile (DACL, Downloadable Access Control List) che consente di accedere a tutte le risorse della rete

<#root>

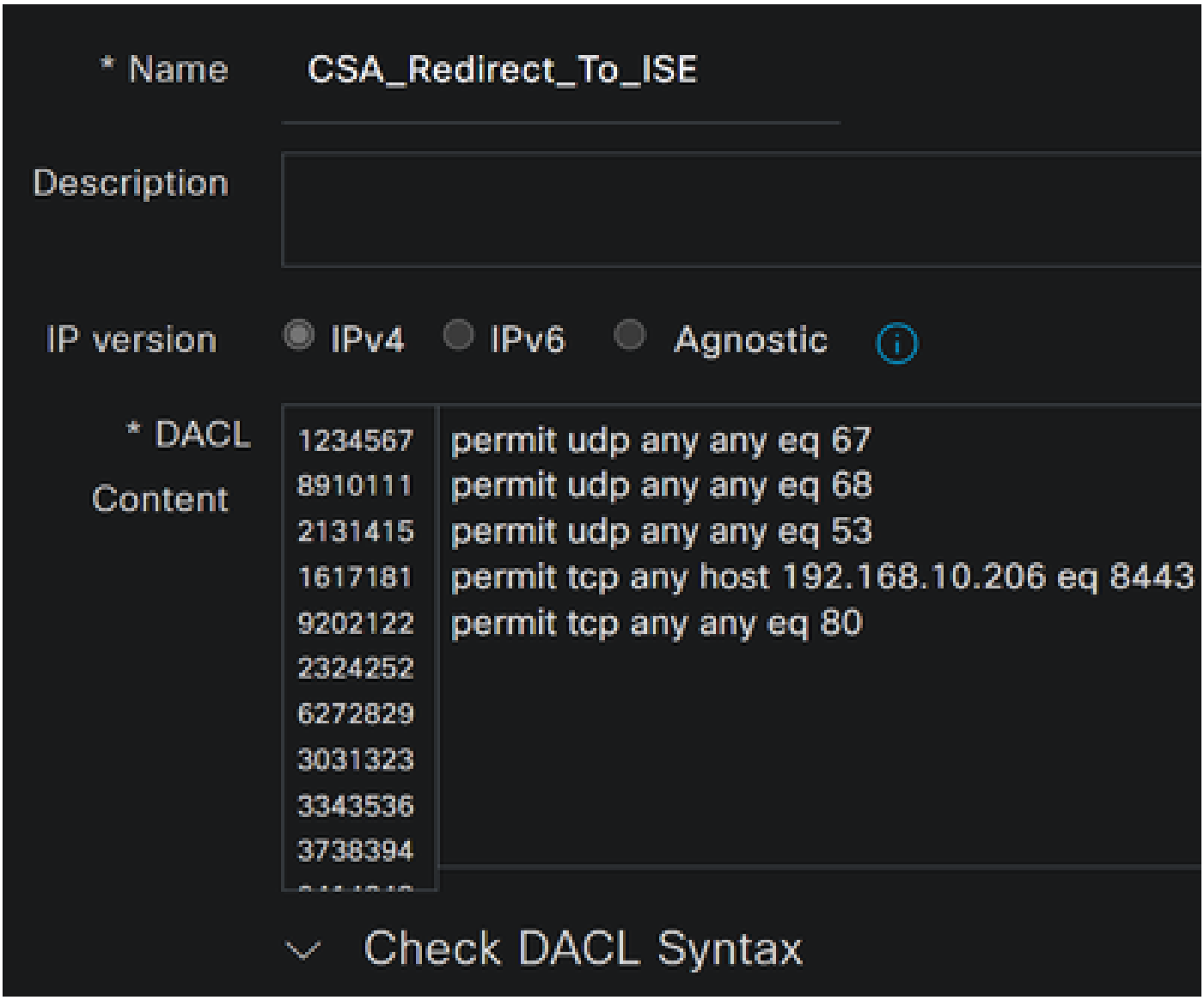
```
permit ip any any
```

Fare clic su **Save** e creare l'elenco DACL di conformità sconosciuto

- Fare clic su **Work Centers > Policy Elements > Downloadable ACLs**

- Fare clic su **+Add**

- Creare la **Unknown Compliant DACL**



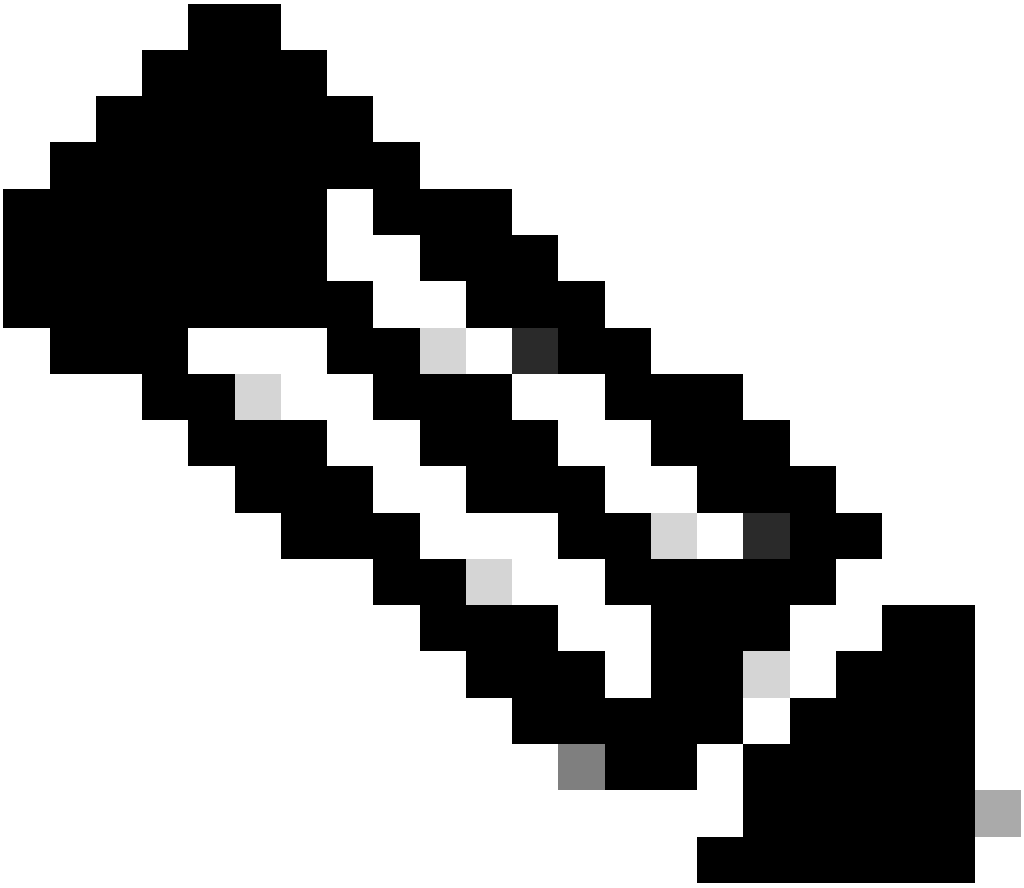
- **Name**: consente di aggiungere un nome che fa riferimento all'elenco DACL-Unknown-Compliant

- **IP version**: Scegli **IPv4**

- **DACL Content**: Creare un DACL che offra accesso limitato alla rete, a DHCP, DNS, HTTP e al portale di provisioning sulla porta 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
```

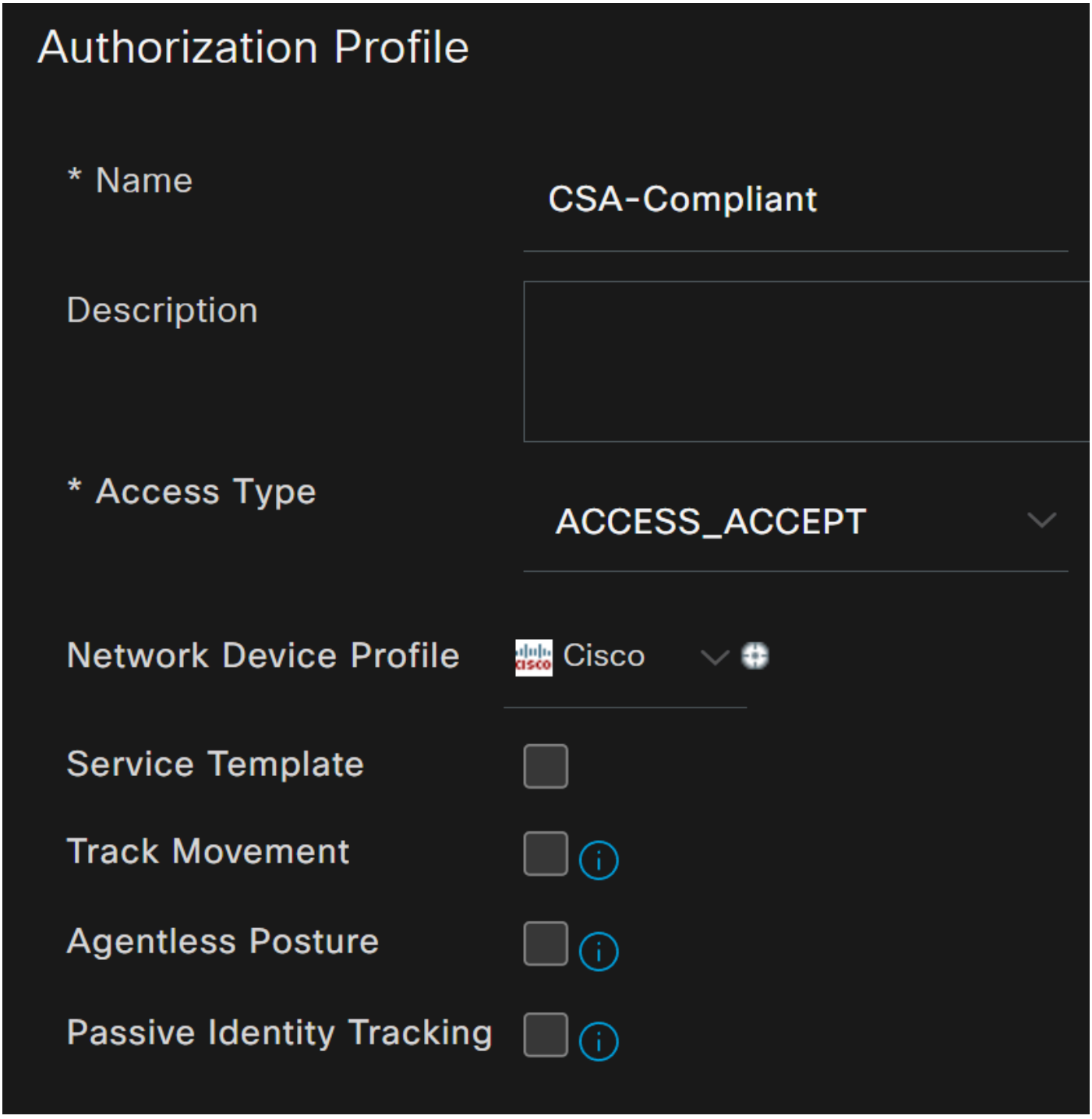


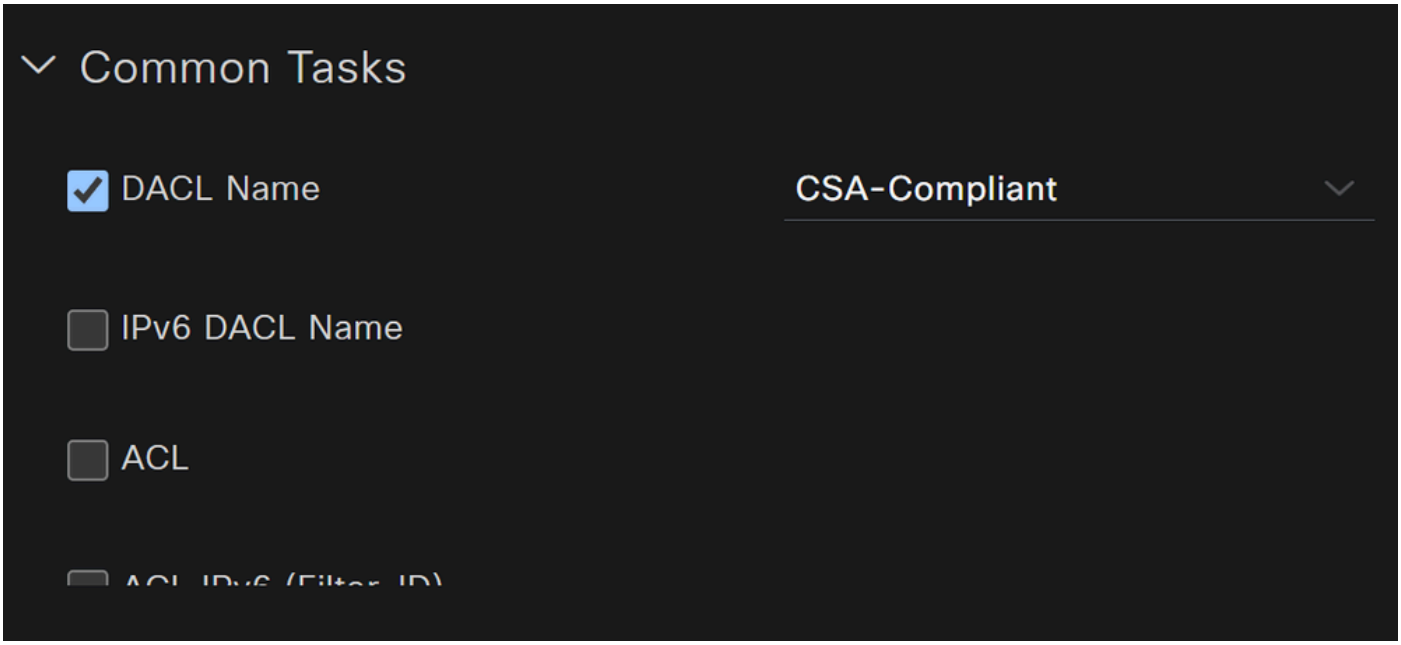
Nota: in questo scenario, l'indirizzo IP 192.168.10.206 corrisponde al server Cisco Identity Services Engine (ISE) e la porta 8443 è stata designata per il portale di provisioning. Ciò significa che è consentito il traffico TCP verso l'indirizzo IP 192.168.10.206 tramite la porta 8443, facilitando l'accesso al portale di provisioning.

A questo punto, si dispone dell'elenco DACL richiesto per creare i profili di autorizzazione.

Per configurare i profili di autorizzazione, passare al dashboard ISE:

- Fare clic su **Work Centers > Policy Elements > Authorization Profiles**
  - Fare clic su **+Add**
  - Creare la **Compliant Authorization Profile**





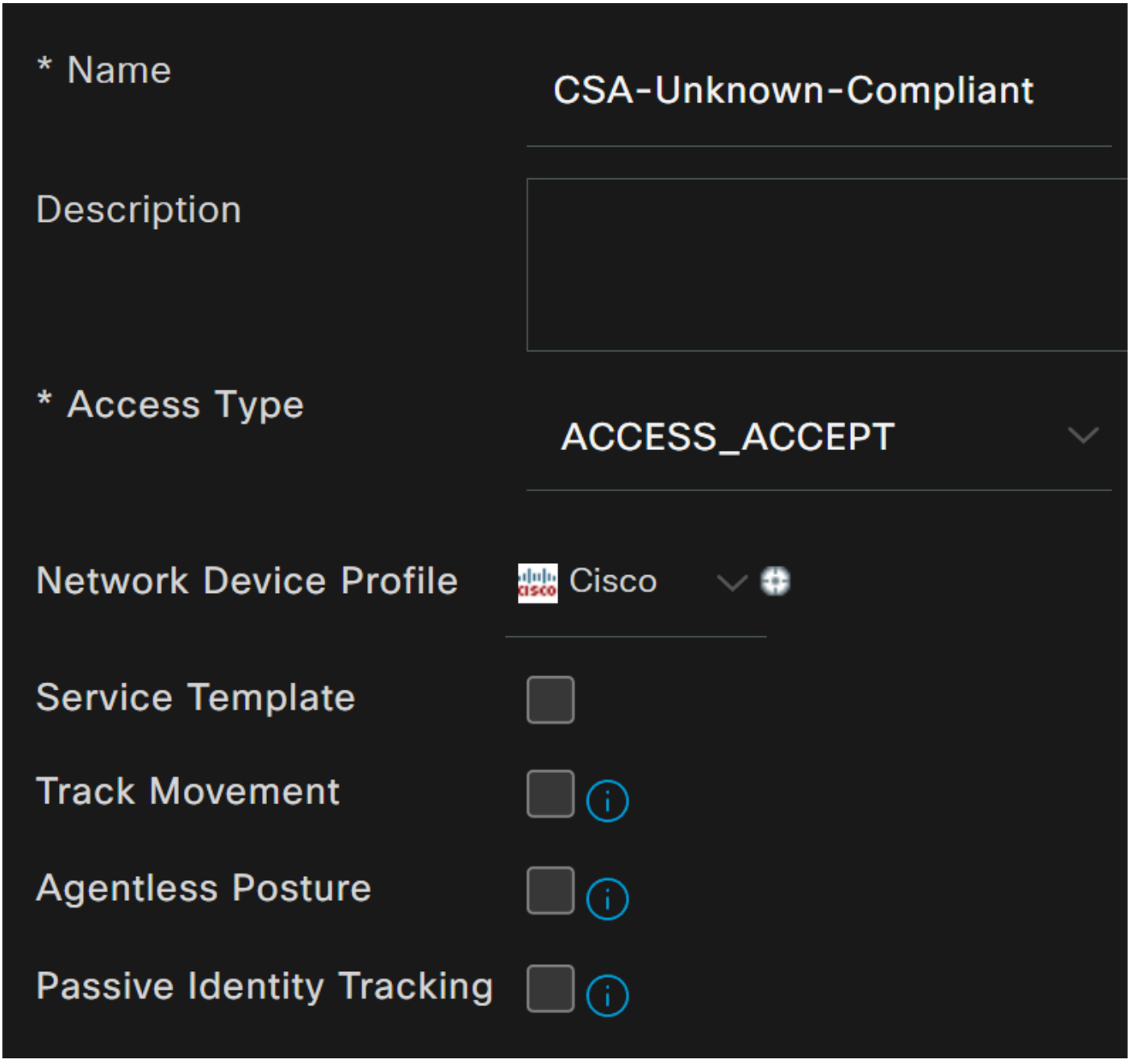
- **Name**: crea un nome che fa riferimento al profilo di autorizzazione conforme
- Access Type: Scegli **ACCESS_ACCEPT**

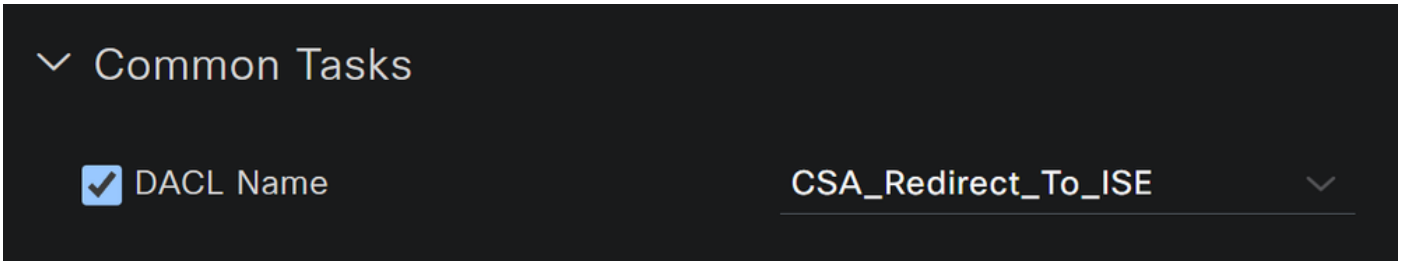
- **Common Tasks**
  - **DACL NAME**: scegliere il DACL configurato nel passo DACL conforme

Fate clic su **Save** e create la Unknown Authorization Profile

- Fare clic su **Work Centers > Policy Elements > Authorization Profiles**
- Fare clic su **+Add**

- Creare la **Uknown Compliant Authorization Profile**

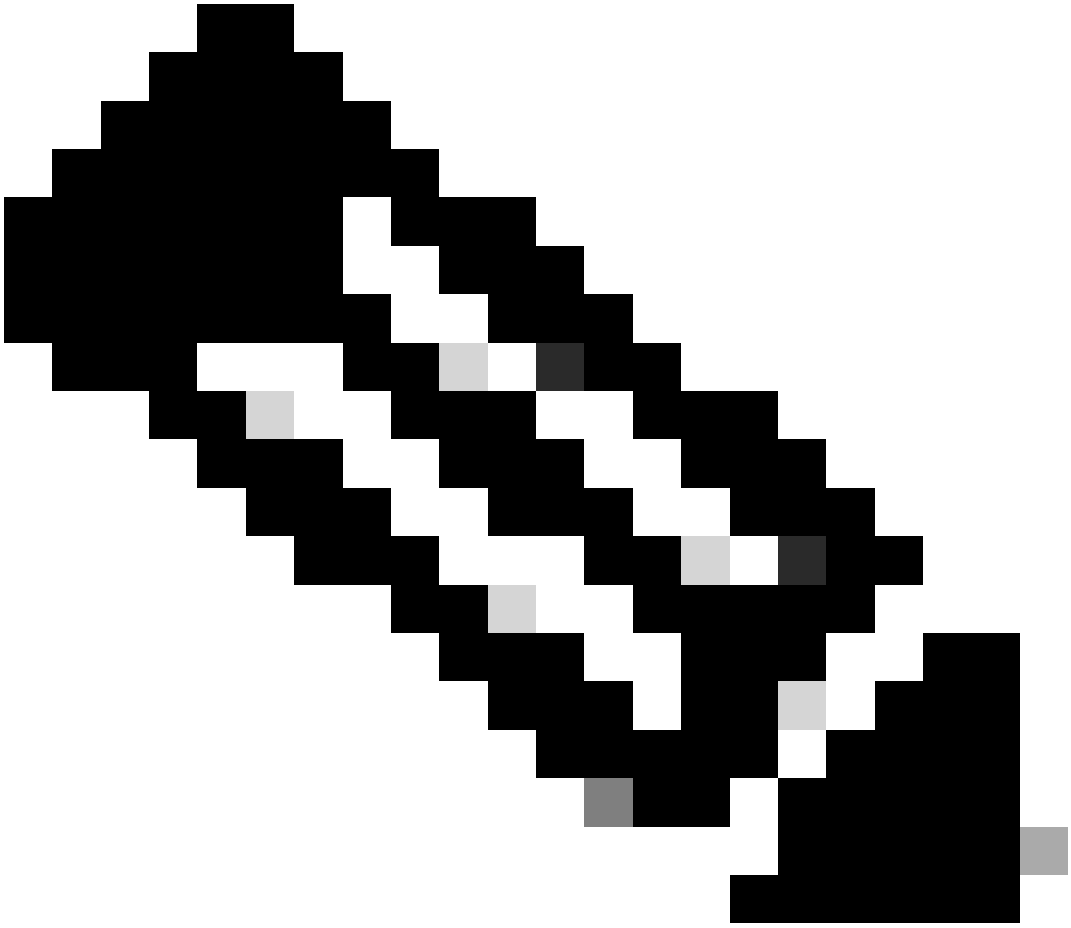




- **Name**: crea un nome che fa riferimento al profilo di autorizzazione conforme sconosciuto
- Access Type: Scegli **ACCESS_ACCEPT**

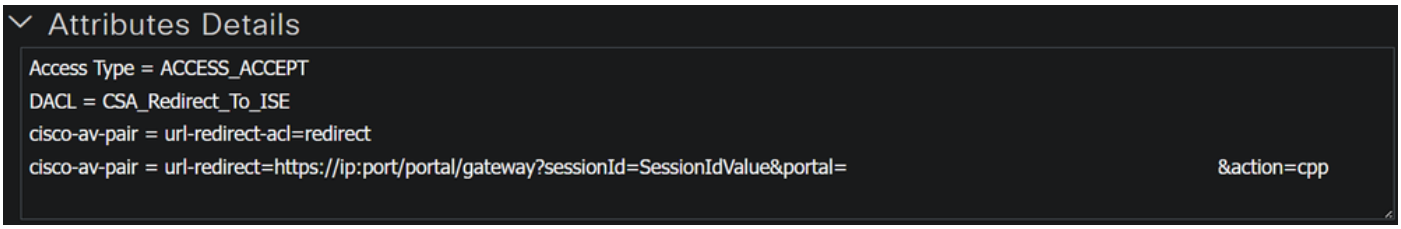
- **Common Tasks**
    - **DACL NAME**: scegliere l'elenco DACL configurato nella fase DACL conforme sconosciuto
        - **Web Redirection (CWA,MDM,NSP,CPP)**
            - Scegli **Client Provisioning (Posture)**
                - **ACL**: deve essere redirect
                - **Value**: scegliere il portale di provisioning predefinito oppure, se ne è stato definito un altro, sceglierlo

---



Nota: il nome dell'ACL di reindirizzamento sull'accesso sicuro per tutte le distribuzioni è **redirect**.

Dopo aver definito tutti questi valori, è necessario disporre di qualcosa di simile in Attributes Details.



Fare clic **Save** per terminare la configurazione e continuare con il passaggio successivo.

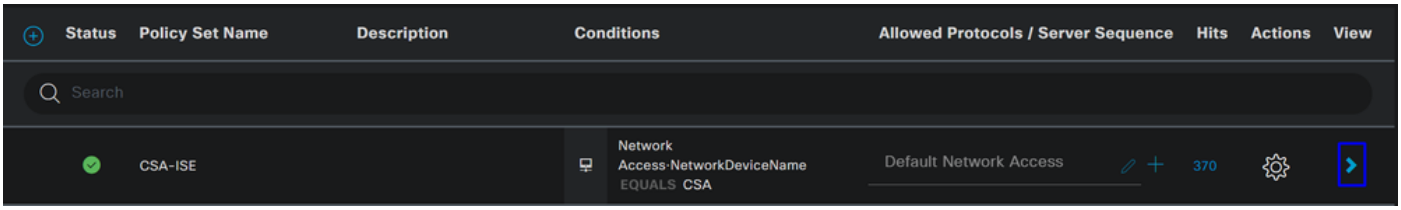
Configura set di criteri di postura

I tre criteri creati si basano sui profili di autorizzazione configurati, ad esempio **DenyAccess**non è necessario crearne un altro.

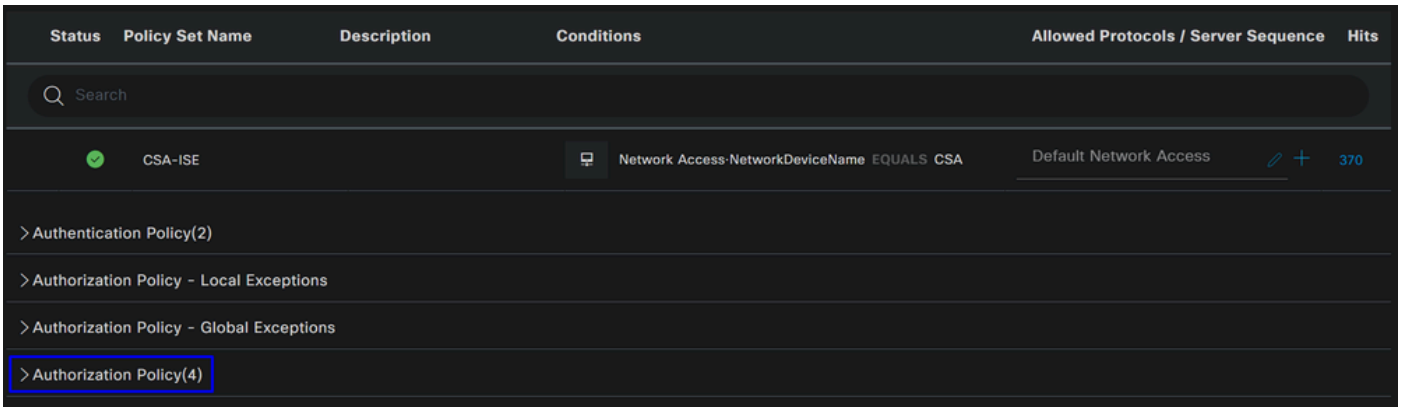
Set di criteri - Autorizzazione	Profilo di autorizzazione
Conforme	Profilo autorizzazione - Conforme
Conforme sconosciuto	Profilo di autorizzazione - Conforme sconosciuto
Non conforme	NegaAccesso

Passa al dashboard ISE

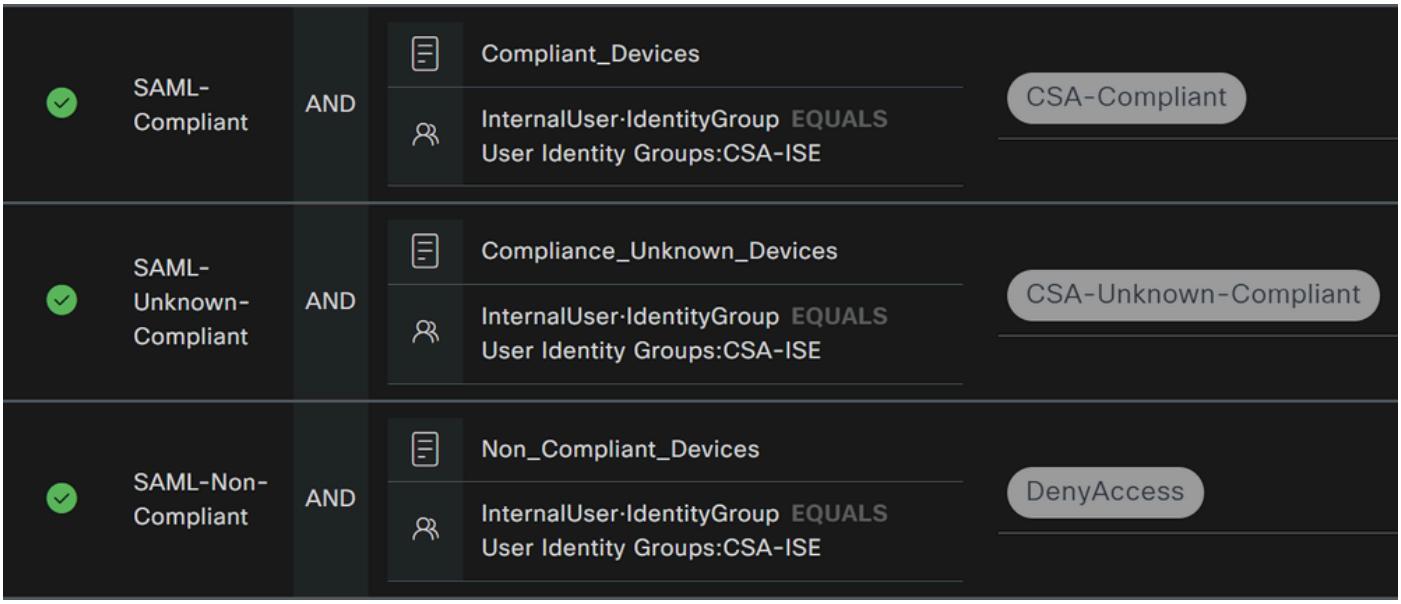
- Fare clic su **Work Center > Policy Sets**
- Fare clic su per accedere > al criterio creato



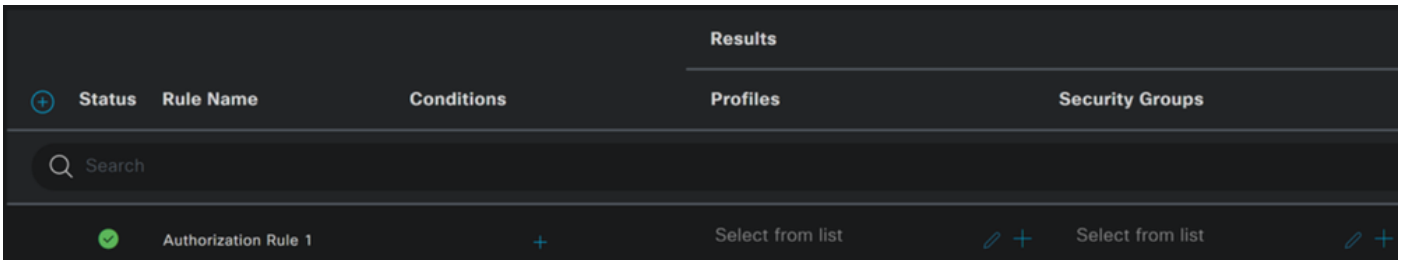
- Fare clic sul pulsante Authorization Policy



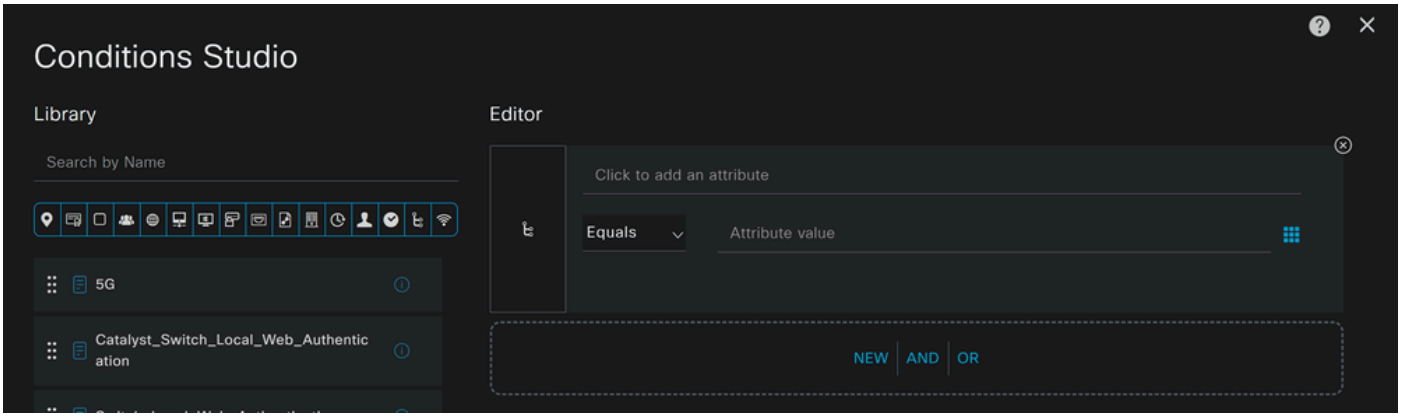
- Creare i tre criteri successivi nell'ordine seguente:



- Fare clic per definire + il **CSA-Compliance** criterio:

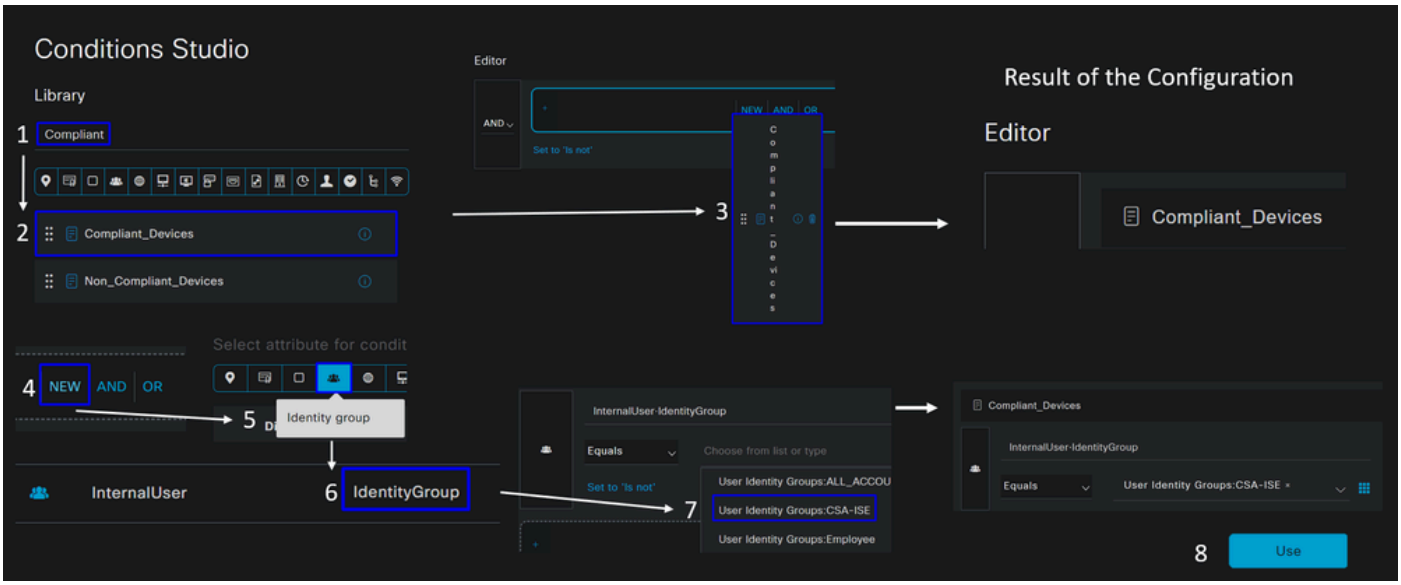


- Per il passo successivo, modificare le Rule Name, Conditionse Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:

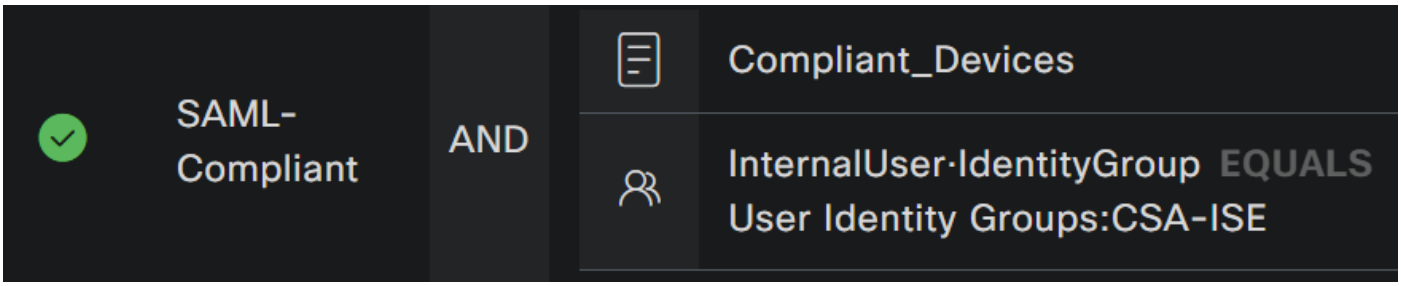


- Per creare la condizione, cercare **compliant**
- È necessario aver visualizzato Compliant_Devices
- Trascinare e rilasciare sotto **Editor**

- Fare clic sotto la casella Editor in **New**
- Fare clic sull'**Identity Group** icona
- Scegli **Internal User Identity Group**
- In **Equals**, scegliere il **User Identity Group** tipo di corrispondenza
- Fare clic su **Use**

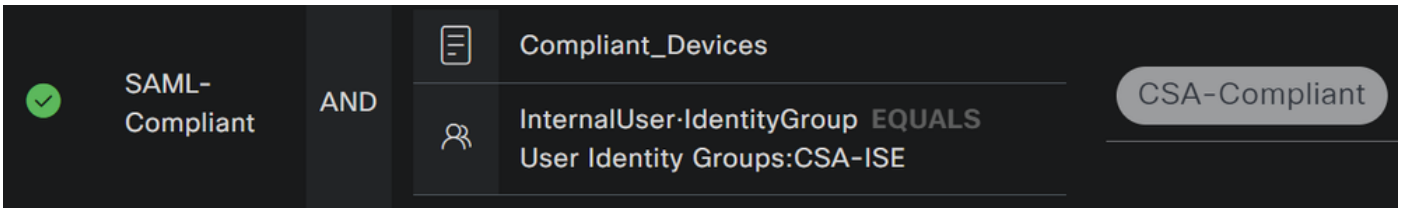


- Di conseguenza, si otterrà l'immagine successiva



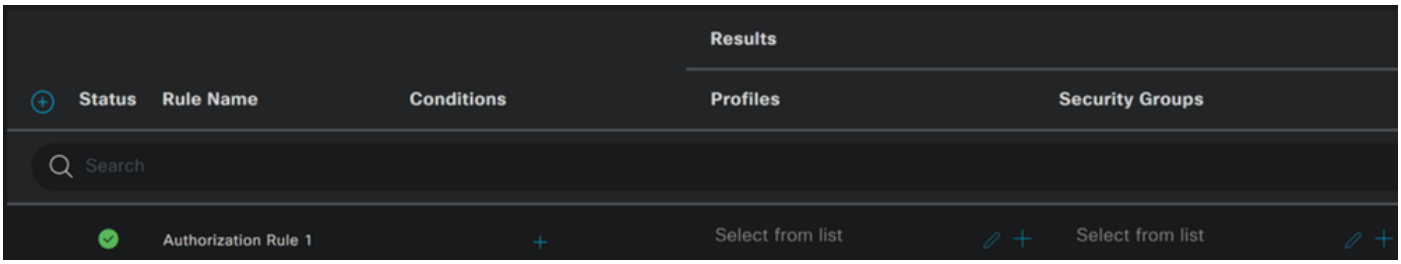
- In fare **Profile** clic sotto il pulsante a discesa e scegliere il profilo autorizzazione reclamo configurato nella fase, Profilo

autorizzazione conforme

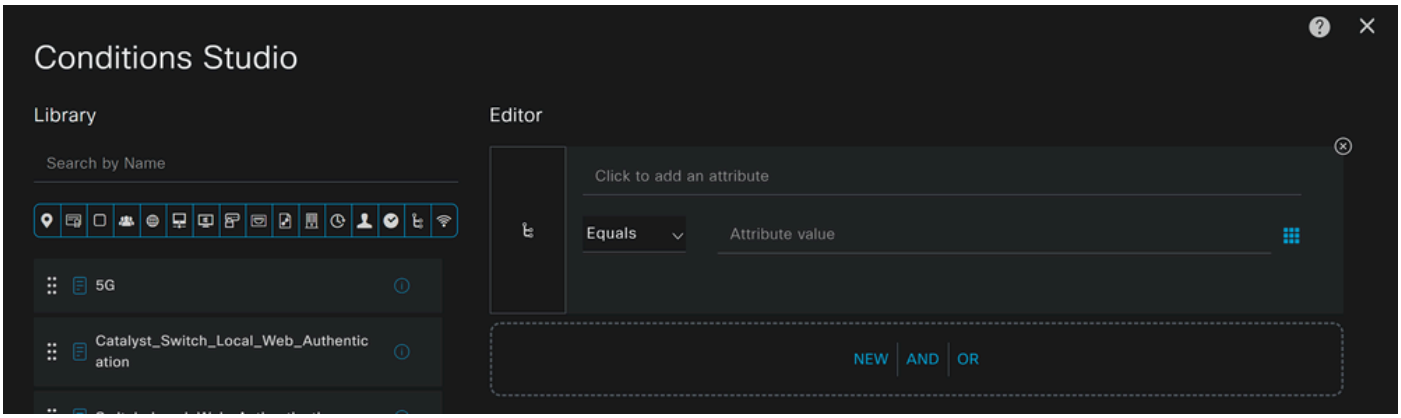


A questo punto è stato configurato il **Compliance Policy Set**router.

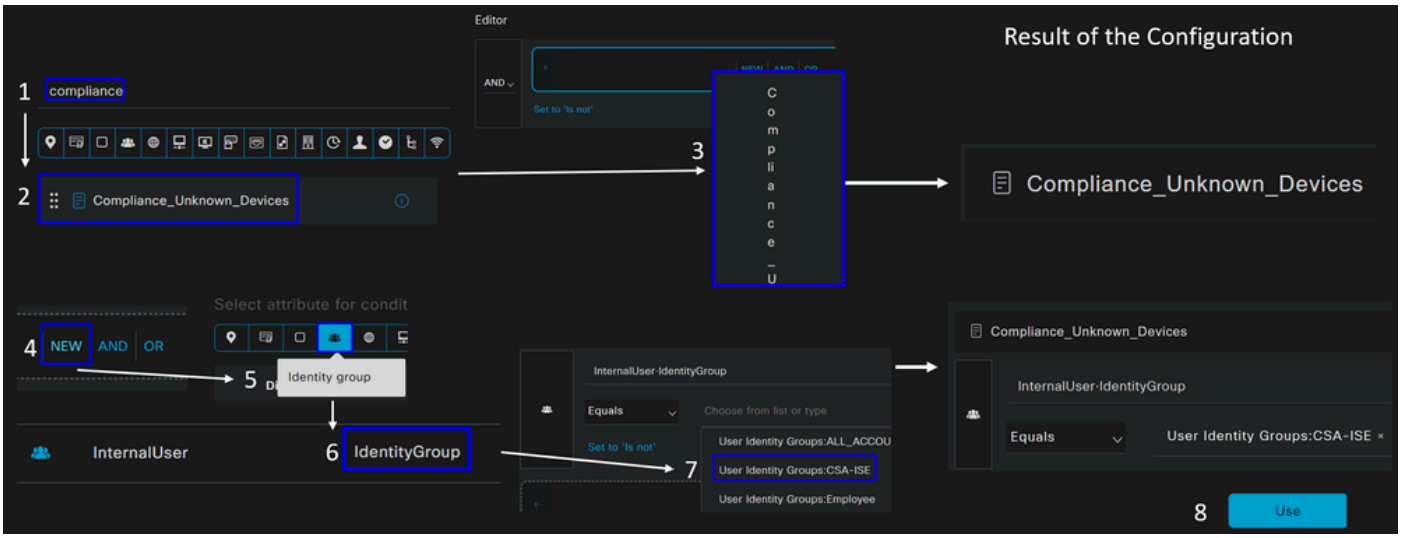
- Fare clic per definire + il **CSA-Unknown-Compliance** criterio:



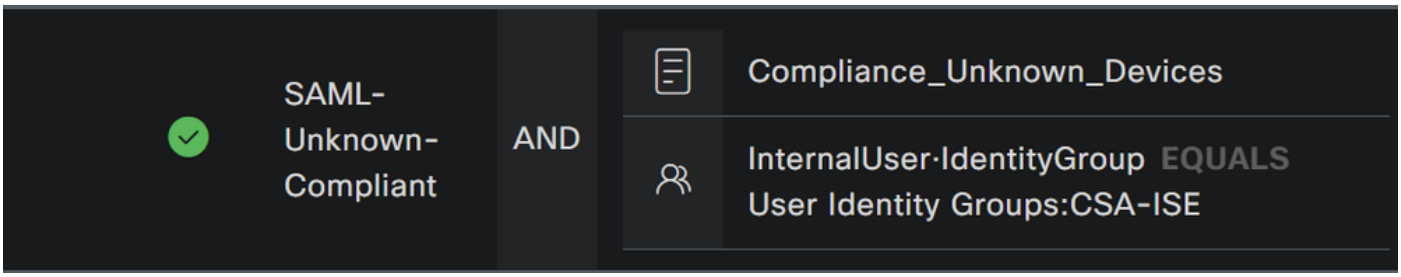
- Per il passo successivo, modificare le Rule Name, Conditionse Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Unknown-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:



- Per creare la condizione, cercare **compliance**
- È necessario aver visualizzato Compliant_Unknown_Devices
- Trascinare e rilasciare sotto **Editor**
- Fare clic sotto la casella Editor in **New**
- Fare clic sull'**Identity Group** icona
- Scegli **Internal User Identity Group**
- In **Equals**, scegliere il **User Identity Group** tipo di corrispondenza
- Fare clic su **Use**

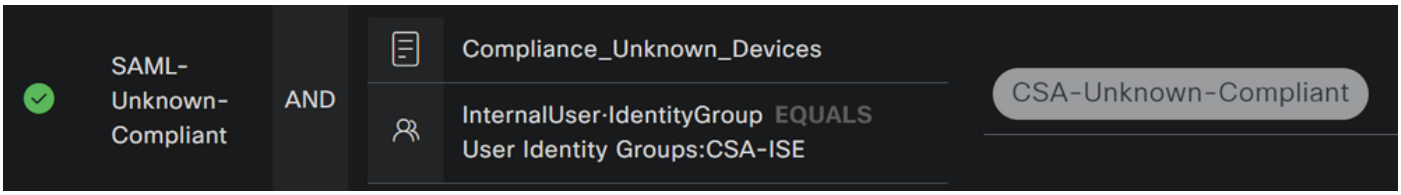


- Di conseguenza, si otterrà l'immagine successiva



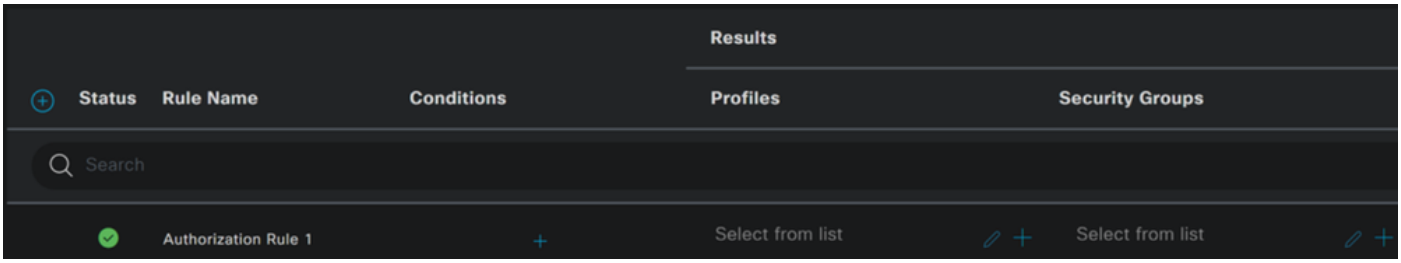
- In fare **Profile** clic sotto il pulsante a discesa e scegliere il profilo autorizzazione reclamo configurato nella fase, Profilo

autorizzazione conforme sconosciuto

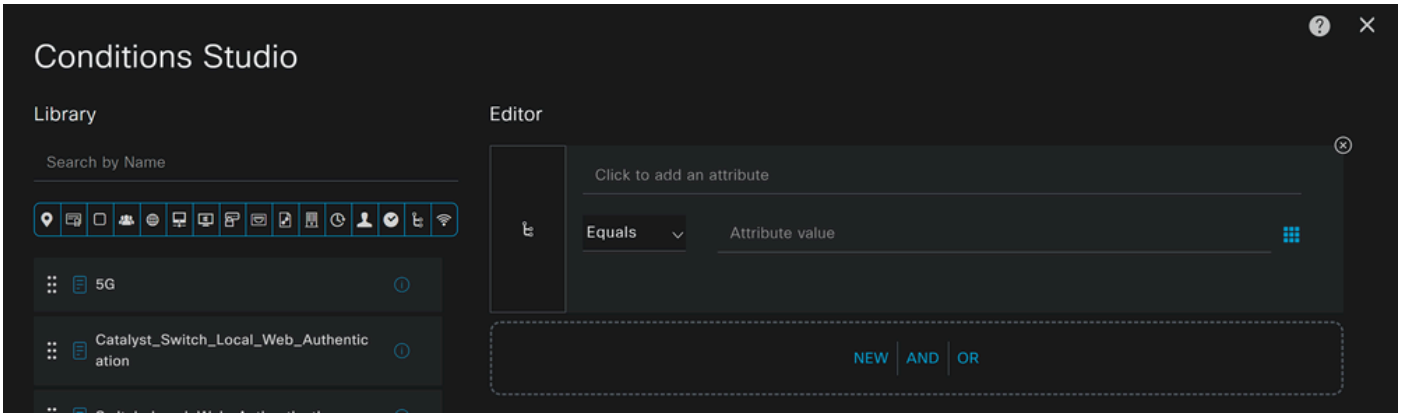


A questo punto è stato configurato il **Unknown Compliance Policy Set**router.

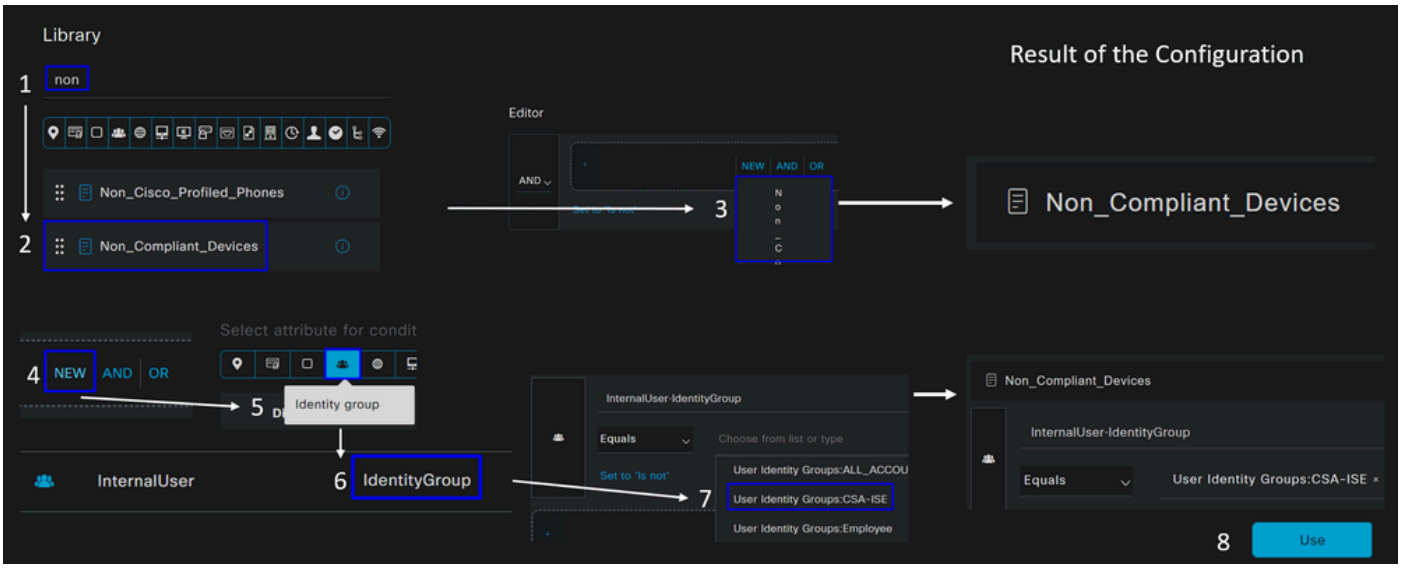
- Fare clic su **+** per definire la **CSA- Non-Compliant** policy:



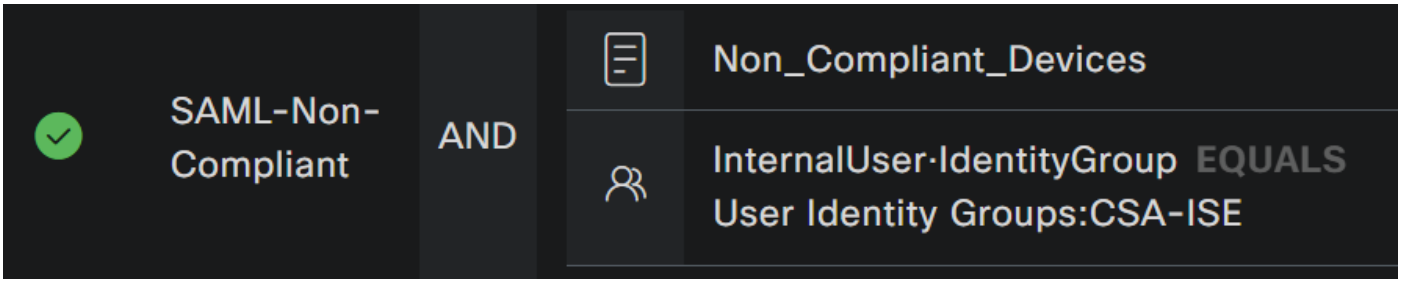
- Per il passo successivo, modificare le Rule Name, Conditionse Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Non-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:



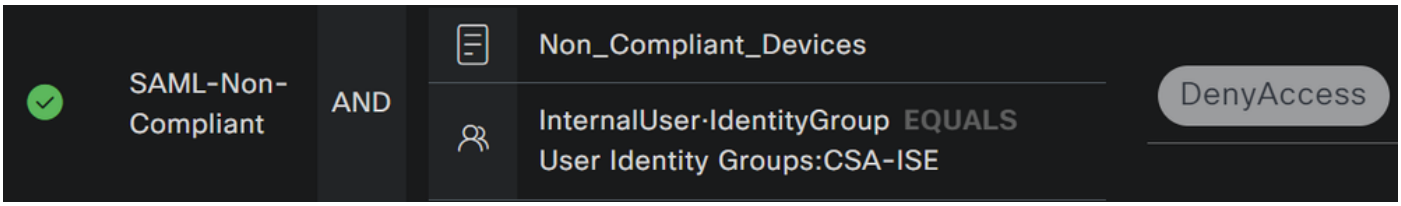
- Per creare la condizione, cercare **non**
- È necessario aver visualizzato Non_Compliant_Devices
- Trascinare e rilasciare sotto **Editor**
- Fare clic sotto la casella Editor in **New**
- Fare clic sull'**Identity Group** icona
- Scegli **Internal User Identity Group**
- In **Equals**, scegliere il **User Identity Group** tipo di corrispondenza
- Fare clic su **Use**



- Di conseguenza, si otterrà l'immagine successiva



- In **Profile** fare clic sotto il pulsante a discesa e scegliere il profilo autorizzazione reclamo **DenyAccess**



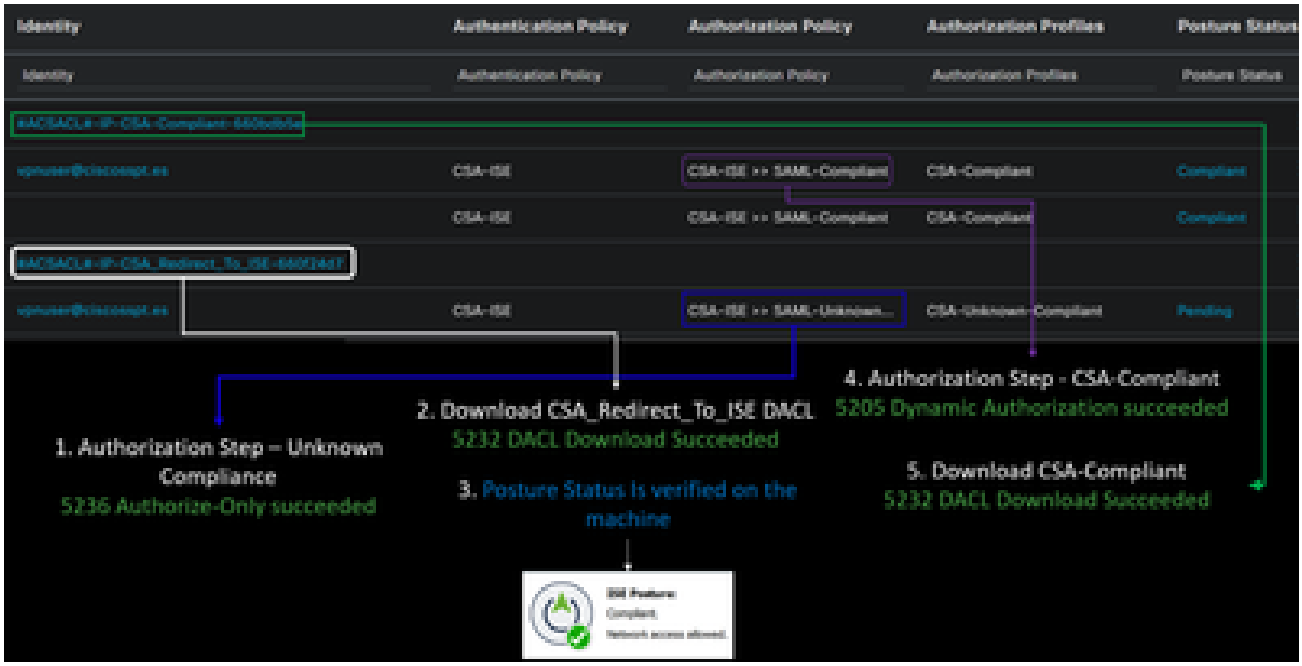
Una volta terminata la configurazione dei tre profili, è possibile testare l'integrazione con la postura.

Verifica

Convalida postura

Connessione nel computer

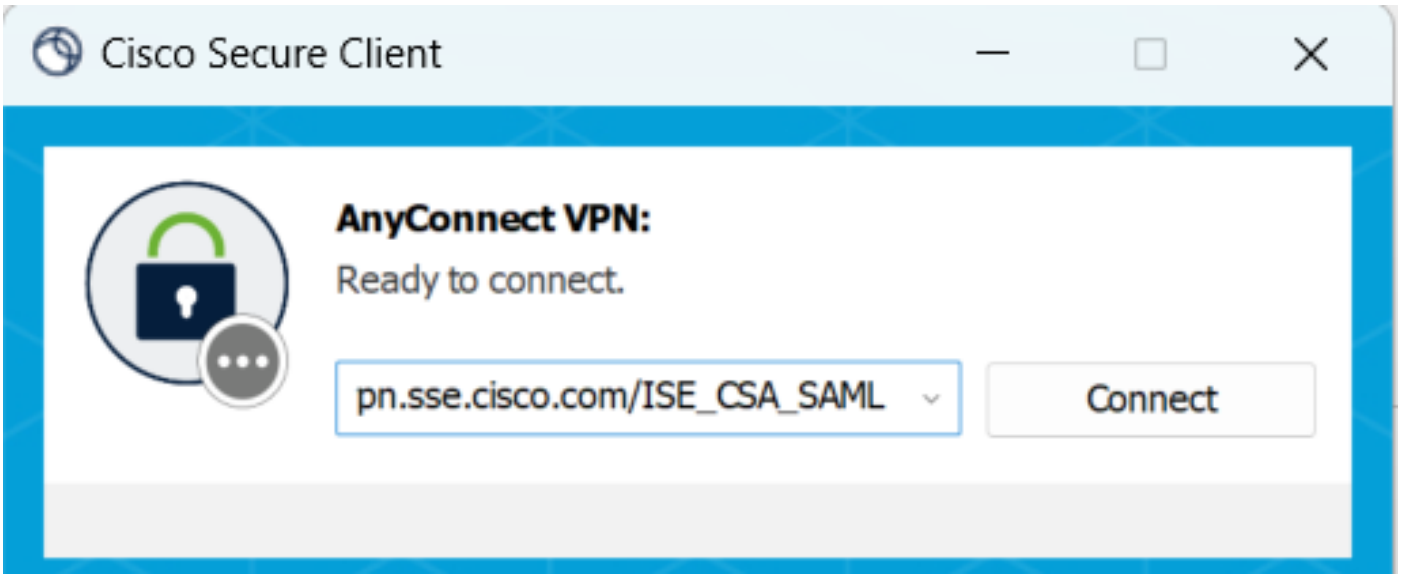
Connettersi al dominio FQDN RA-VPN fornito su Secure Access via Secure Client.



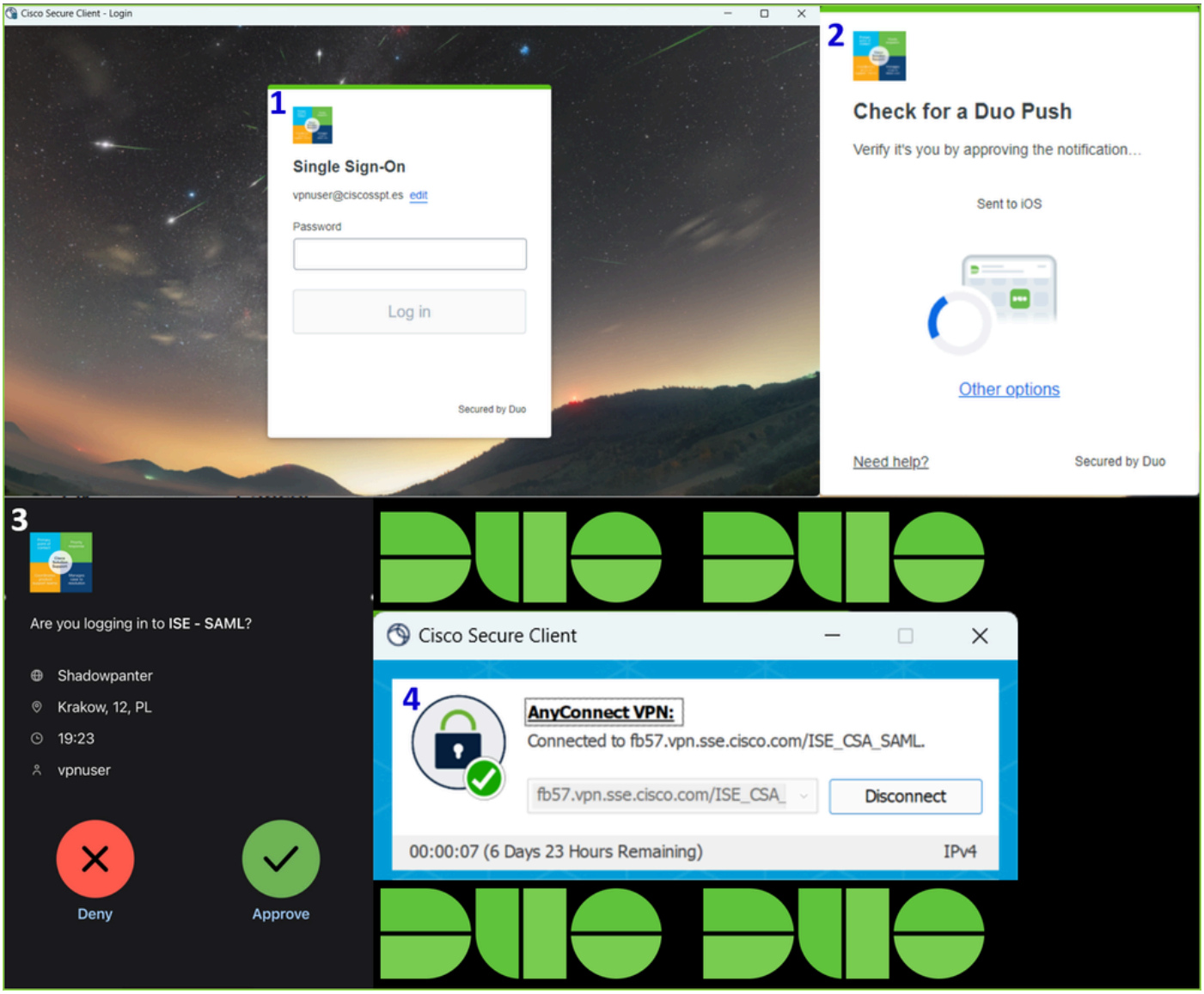
Nota: per questa fase non è necessario installare alcun modulo ISE.

---

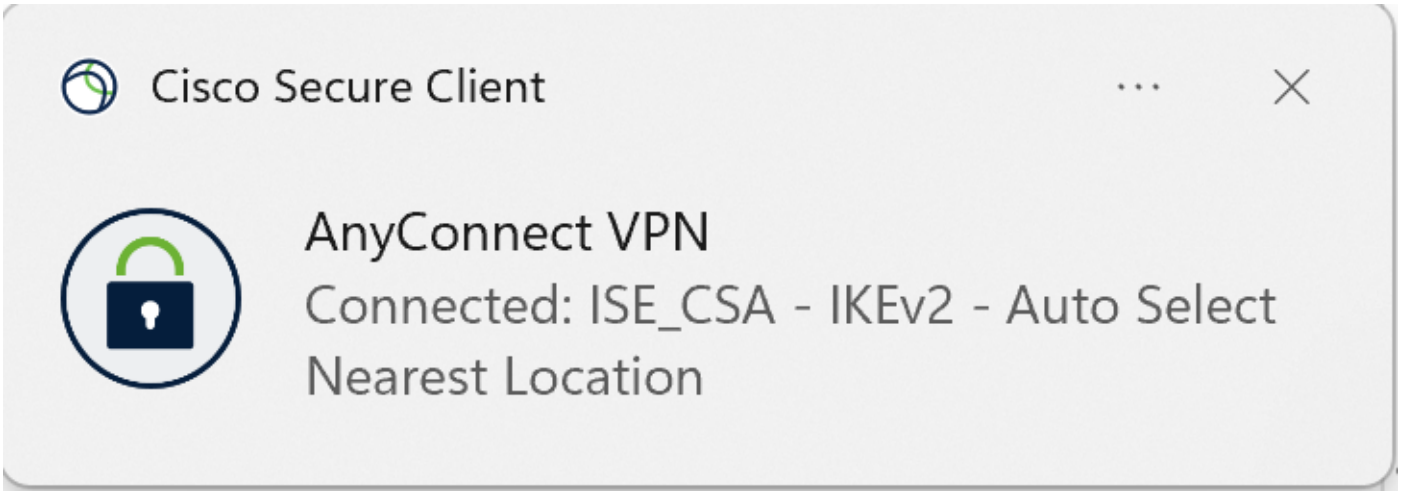
1. Connettersi utilizzando Secure Client.

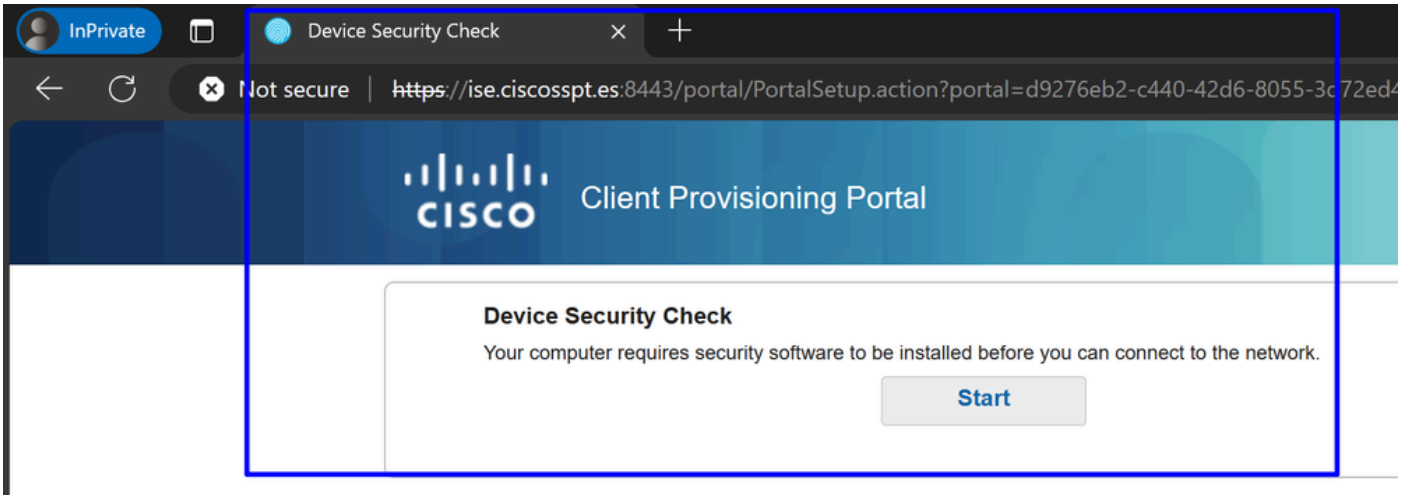


2. Fornire le credenziali per l'autenticazione tramite Duo.



3. A questo punto, ti colleghi alla VPN e, molto probabilmente, verrai reindirizzato ad ISE; in caso contrario, puoi provare a passare a **http:1.1.1.1**IOS.



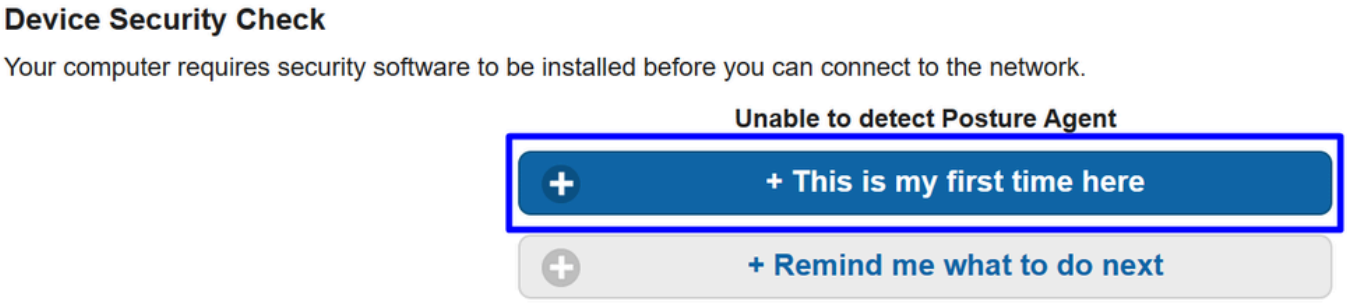


Nota: a questo punto, l'utente è soggetto al set di criteri Authorization - CSA-Unknown-Compliance perché sul computer non è installato ISE Posture Agent e viene reindirizzato al portale di provisioning ISE per installare l'agente.

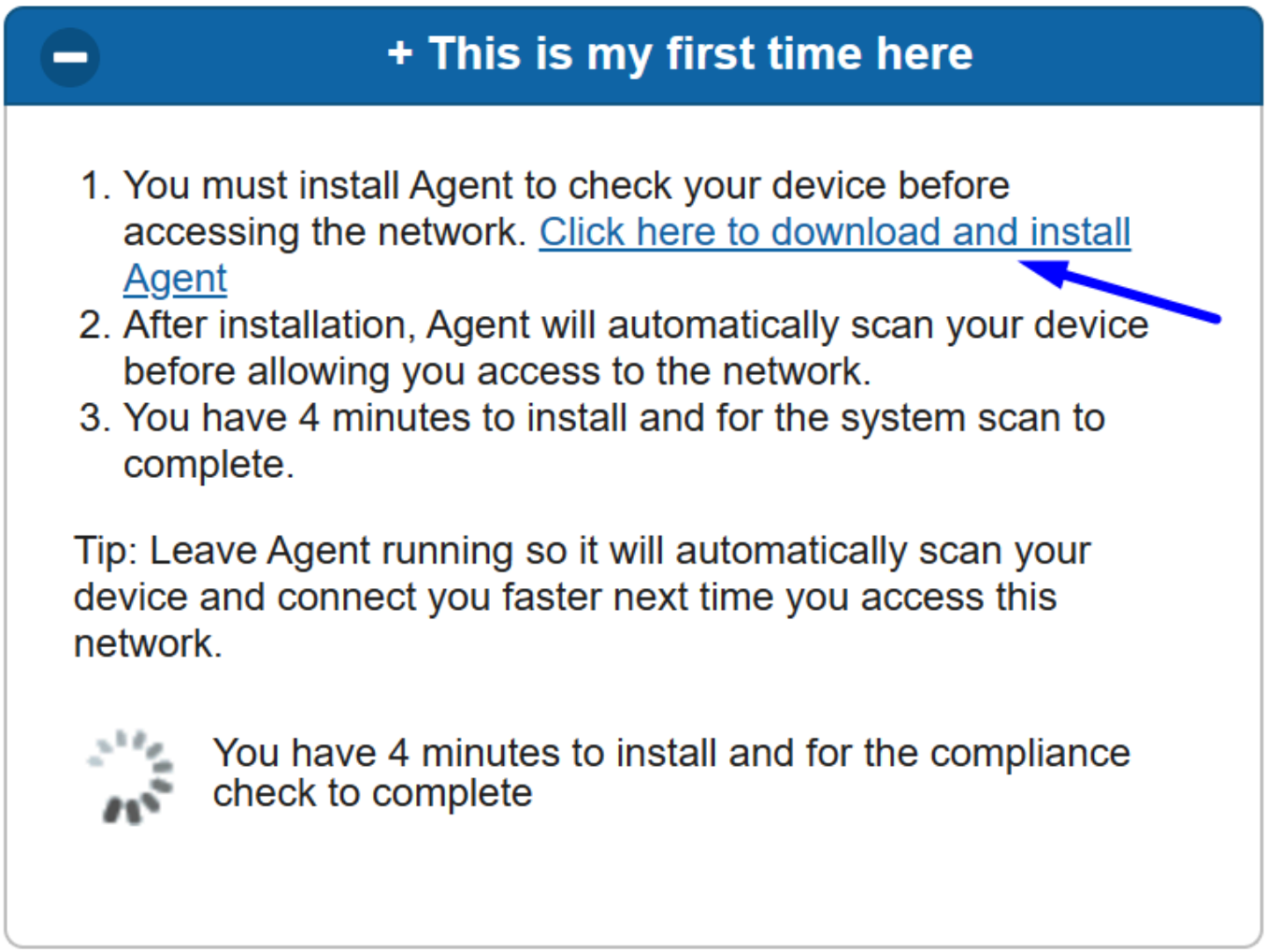
---

4. Fare clic su Avvia per procedere con il provisioning dell'agente.

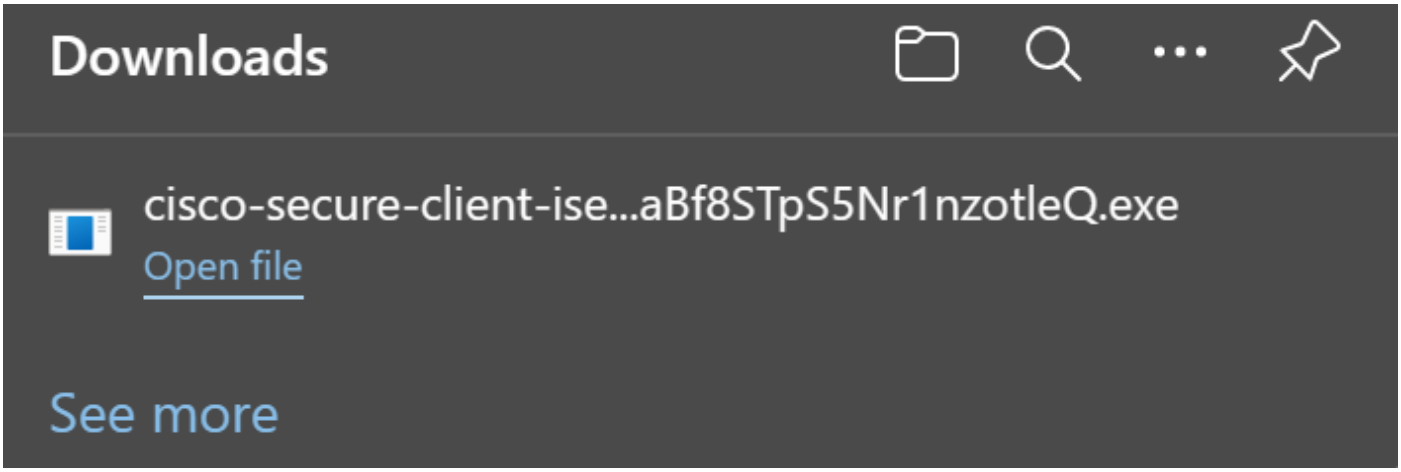
5. Fare clic su **+ This is my first time here**.

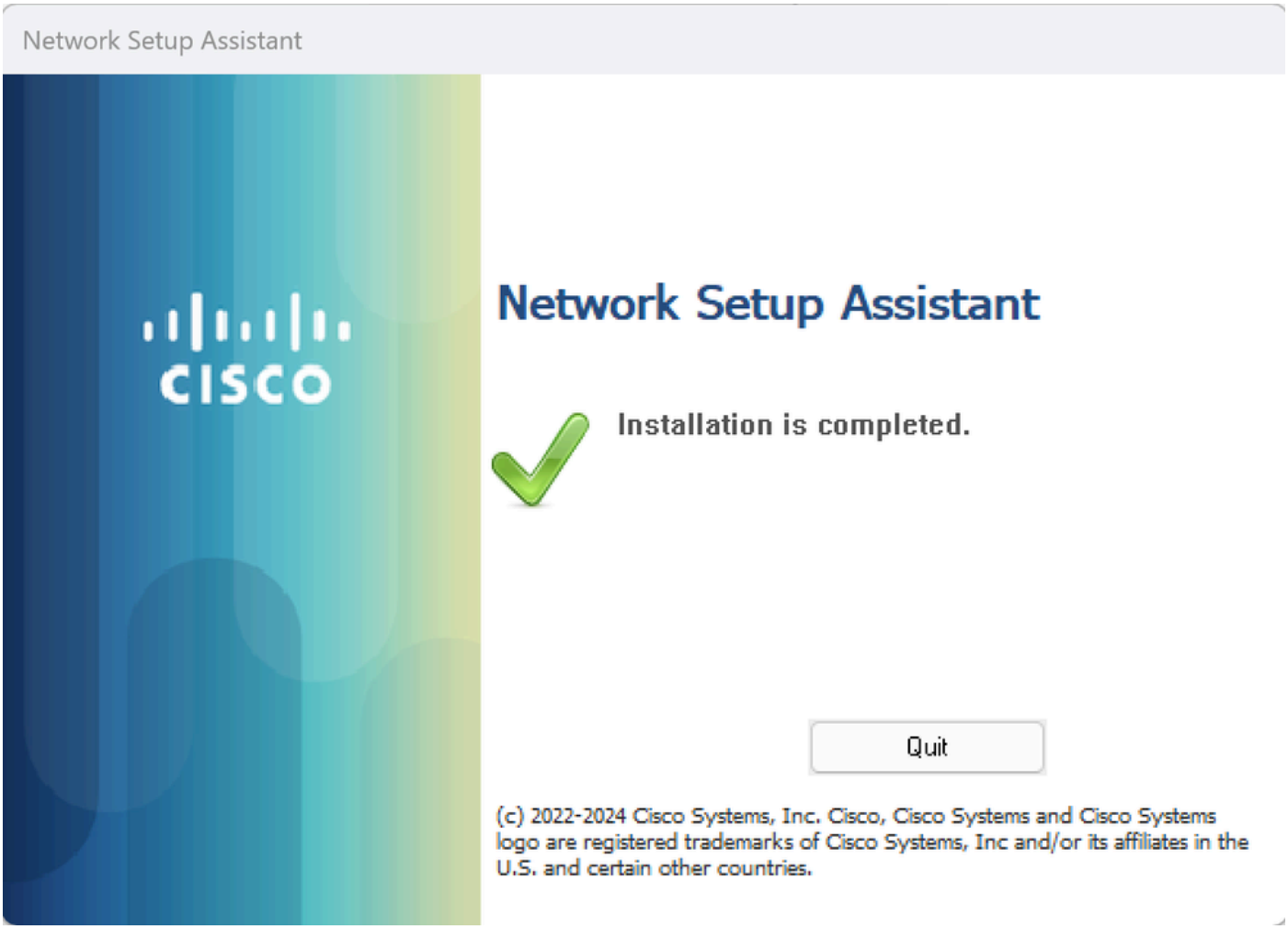


6. Fare clic su **Click here to download and install agent**

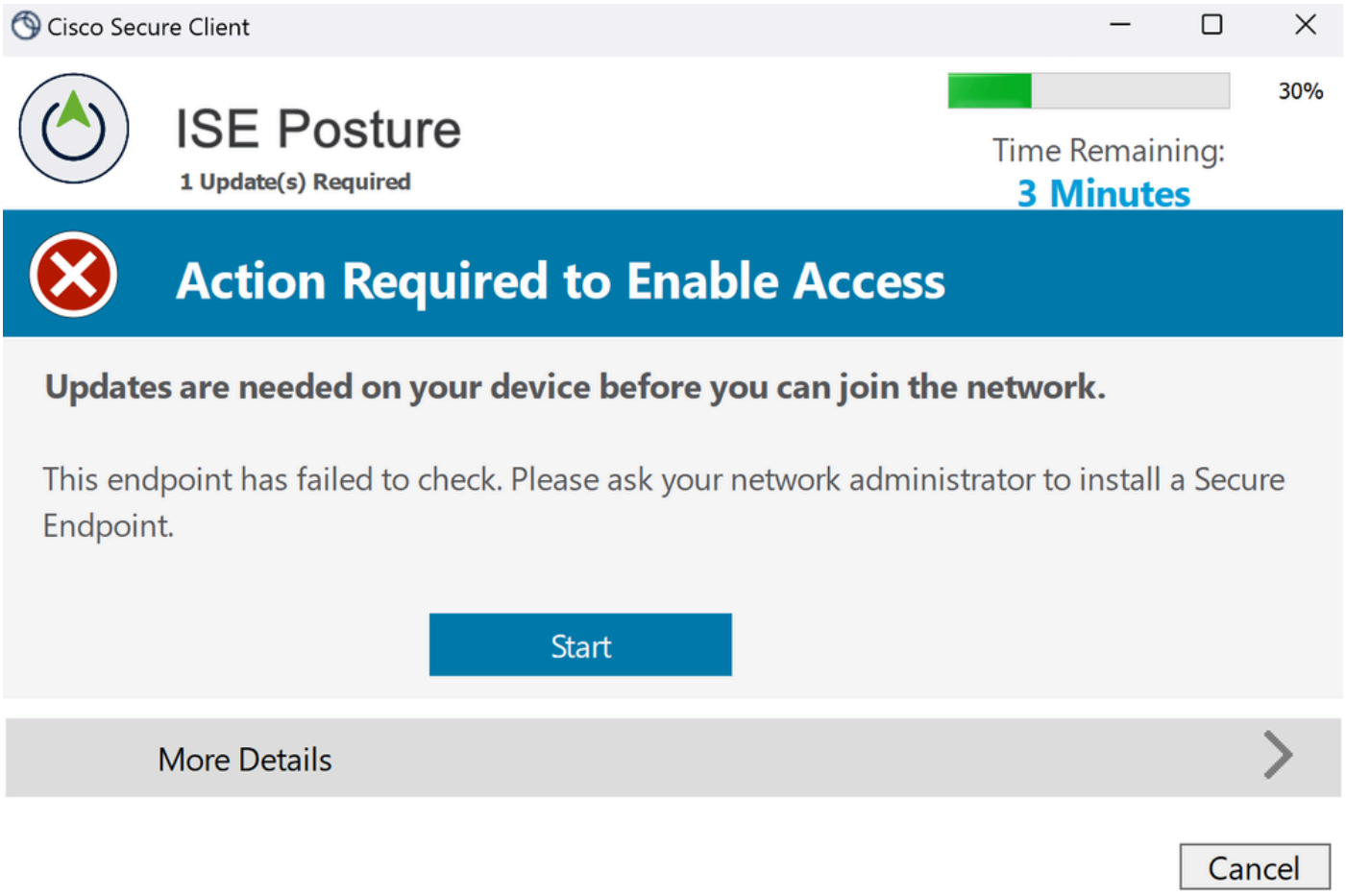


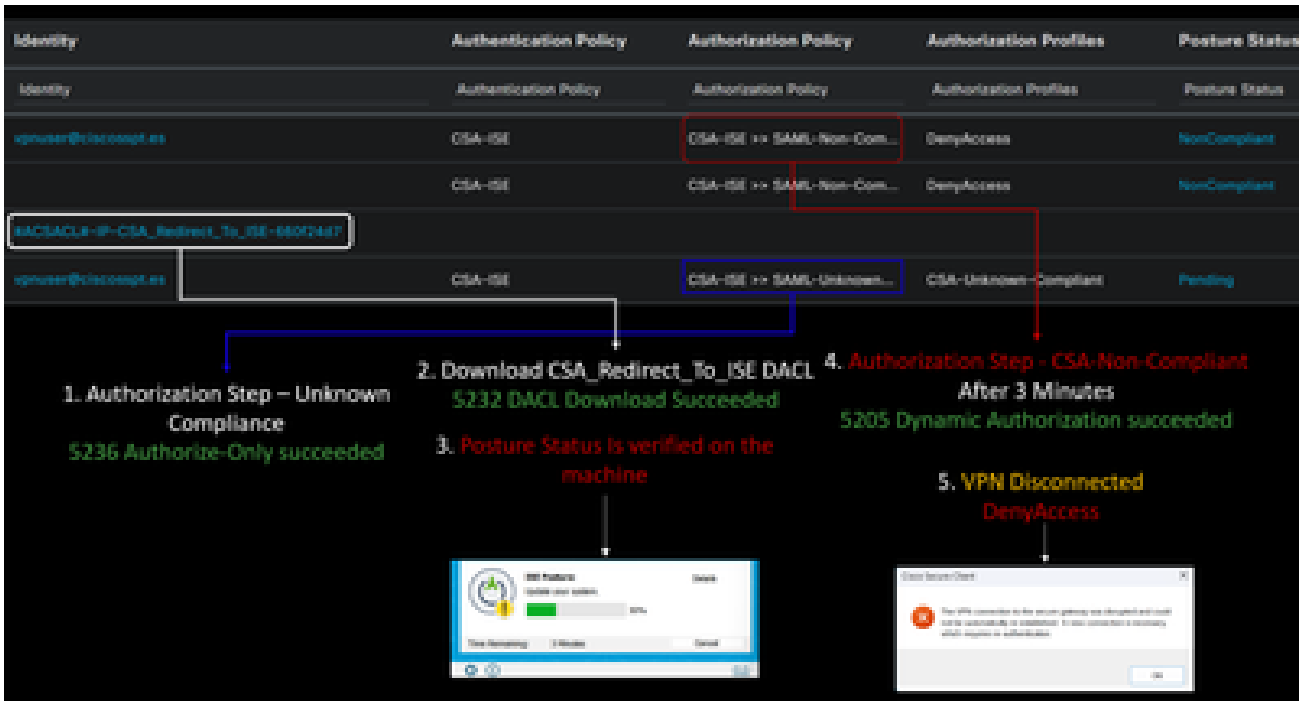
7. Installare l'agente





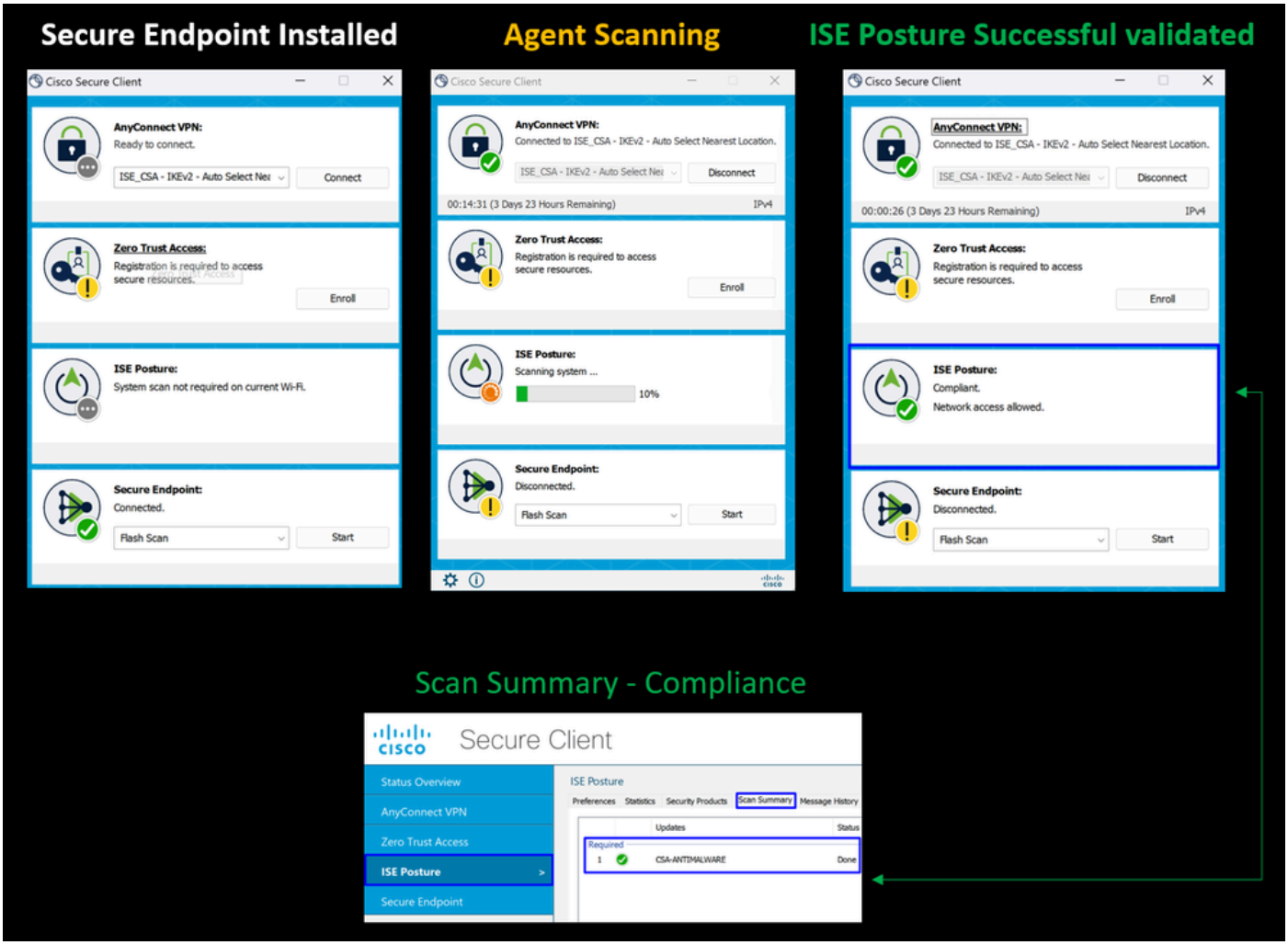
8. Dopo aver installato l'agente, ISE Posture inizia a verificare la postura corrente delle macchine. Se i requisiti della politica non vengono soddisfatti, viene visualizzata una schermata di popup che guida l'utente verso la conformità.


Cisco Secure Client
ISE Posture
1 Update(s) Required
30%
Time Remaining:
3 Minutes
Action Required to Enable Access
Updates are needed on your device before you can join the network.
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.
Start
More Details
Cancel

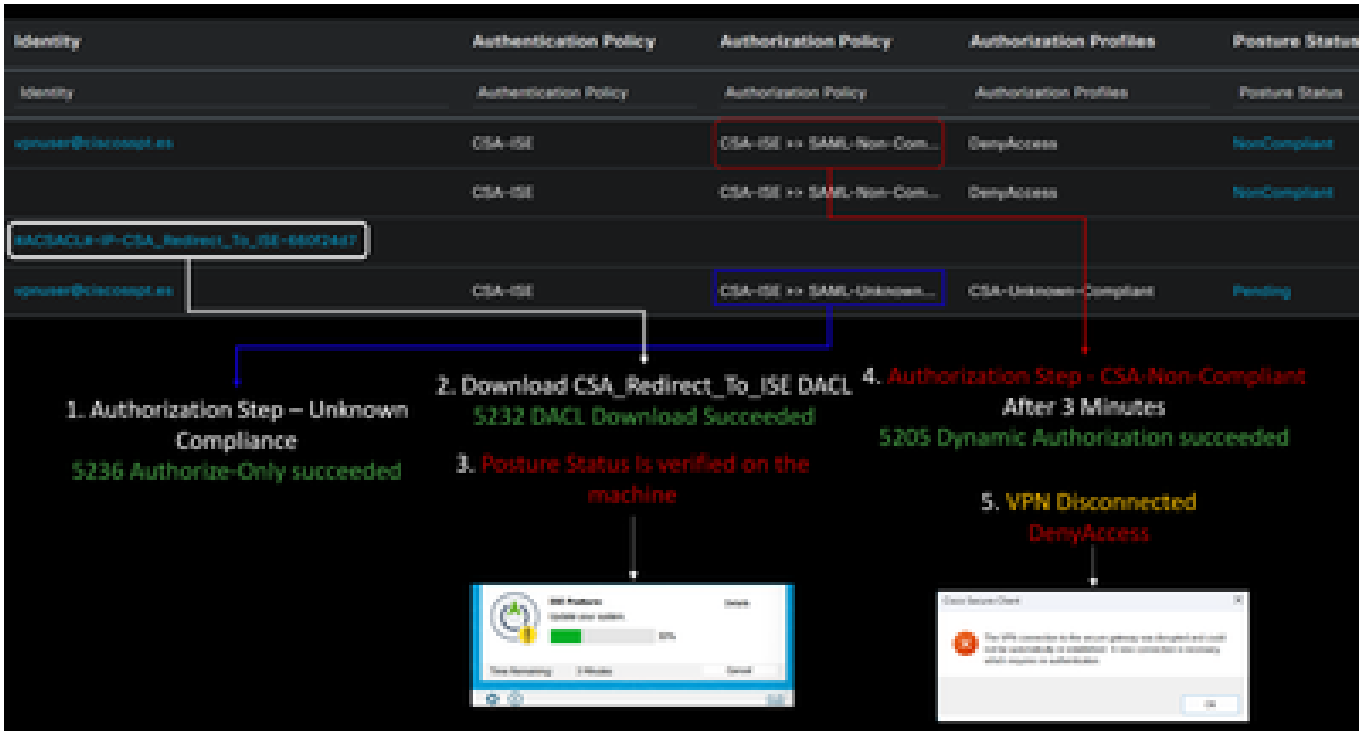

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status is verified on the machine
4. Authorization Step - CSA-Non-Compliant
After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected
DenyAccess

Nota: se Cancel o il tempo rimanente termina, l'utente diventa automaticamente non conforme, rientra nei criteri di autorizzazione impostati CSA-Non-Compliance e viene immediatamente disconnesso dalla VPN.

9. Installare l'agente endpoint sicuro e riconnettersi alla VPN.



10. Dopo che l'agente ha verificato la conformità della macchina, la postura cambia per essere in reclamo e dare accesso a tutte le risorse sulla rete.

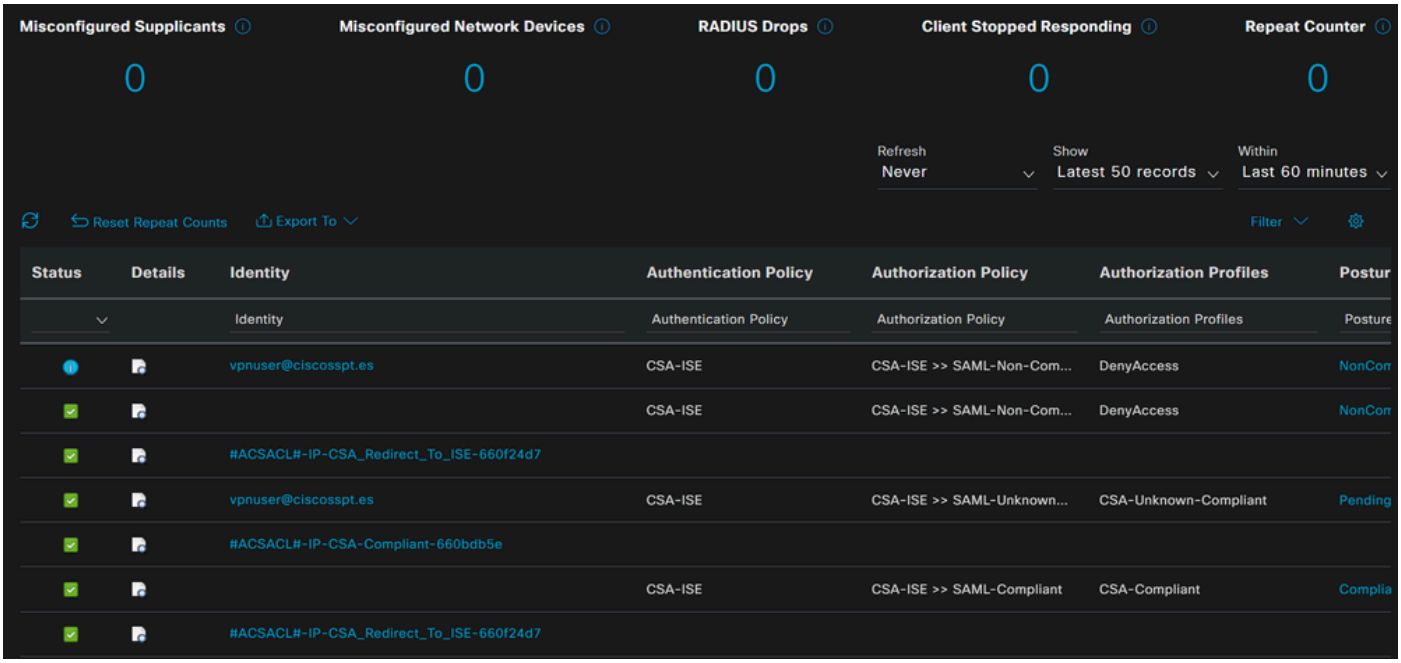


Nota: una volta ottenuta la conformità, si rientra nel set di criteri di autorizzazione CSA-Conformità e si ha immediatamente accesso a tutte le risorse di rete.

Come verificare i log in ISE

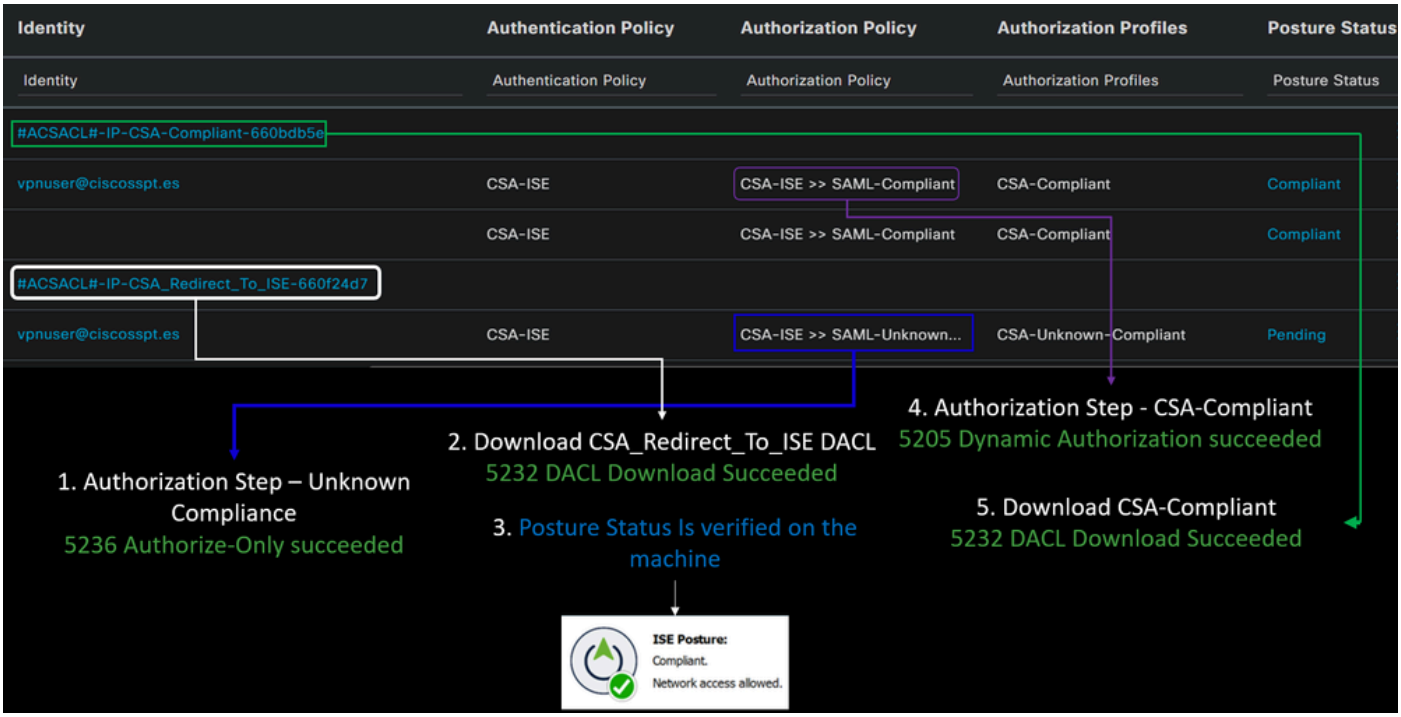
Per verificare il risultato dell'autenticazione per un utente, sono disponibili due esempi di conformità e non conformità. Per esaminarlo ad ISE, attenersi alle seguenti istruzioni:

- Passa al dashboard ISE
- Fare clic su Operations > Live Logs

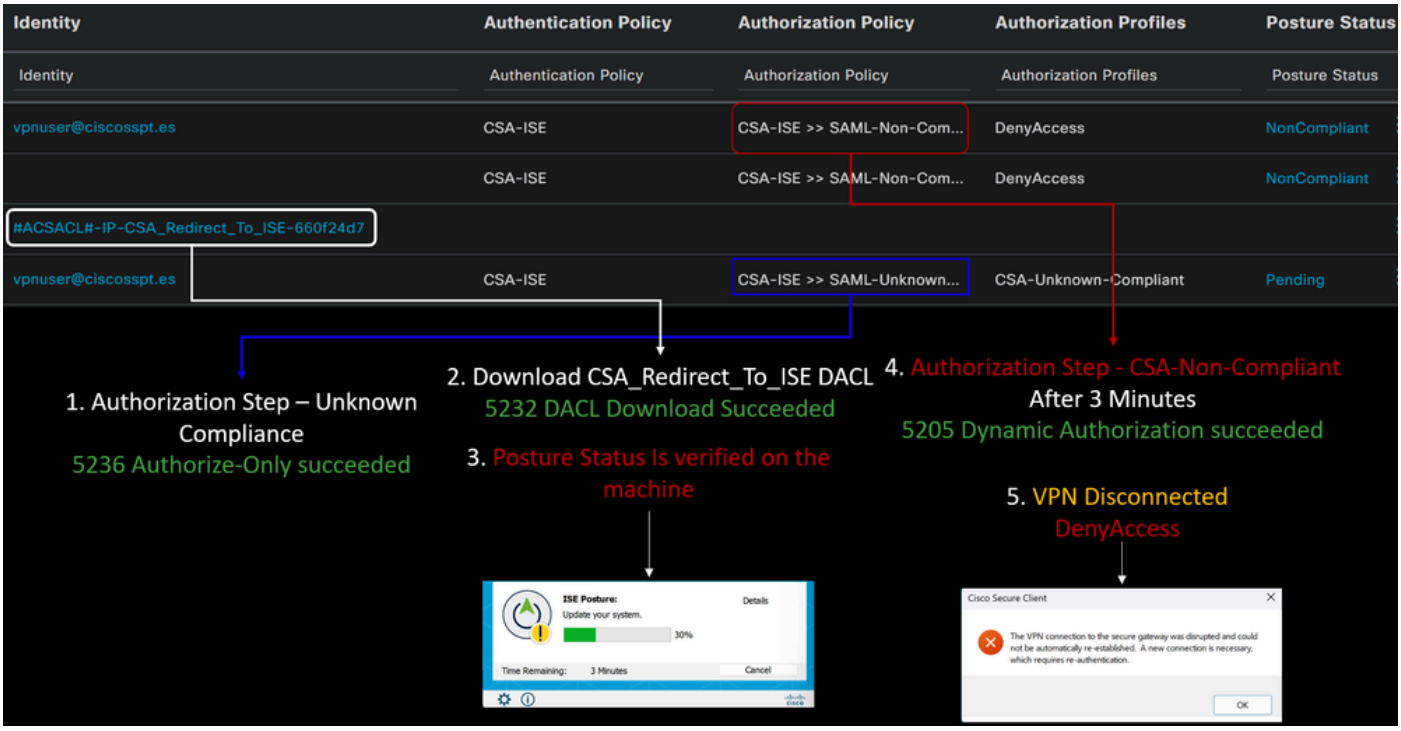


Lo scenario successivo mostra come gli eventi di conformità e non conformità vengono visualizzati in **Live Logs**:

Conformità



Non conformità



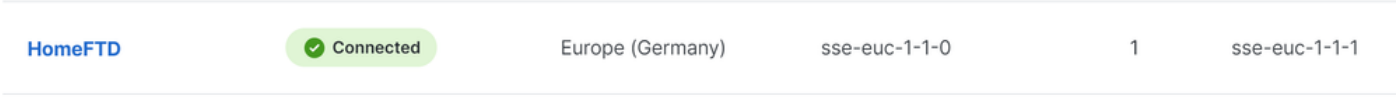
Primi passi verso un accesso sicuro e l'integrazione con ISE

Nell'esempio successivo, Cisco ISE si trova nella rete 192.168.10.0/24, e la configurazione delle reti raggiungibili tramite il tunnel deve essere aggiunta alla configurazione del tunnel.

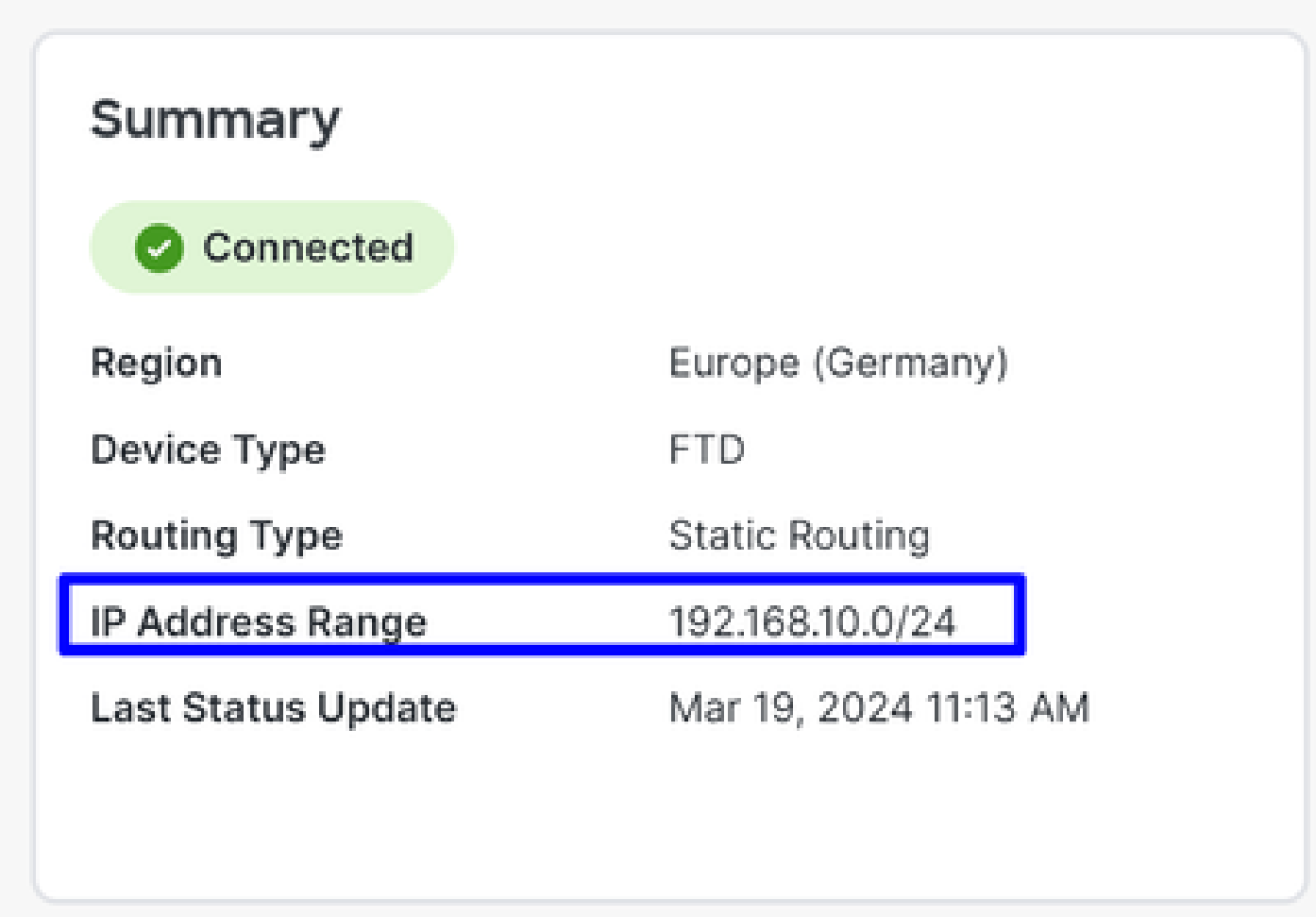
Step 1: verifica della configurazione del tunnel:

Per verificare questa condizione, passare al Dashboard di accesso protetto.

- Fare clic su **Connect > Network Connections**
- Fare clic su **Network Tunnel Groups** > Tunnel



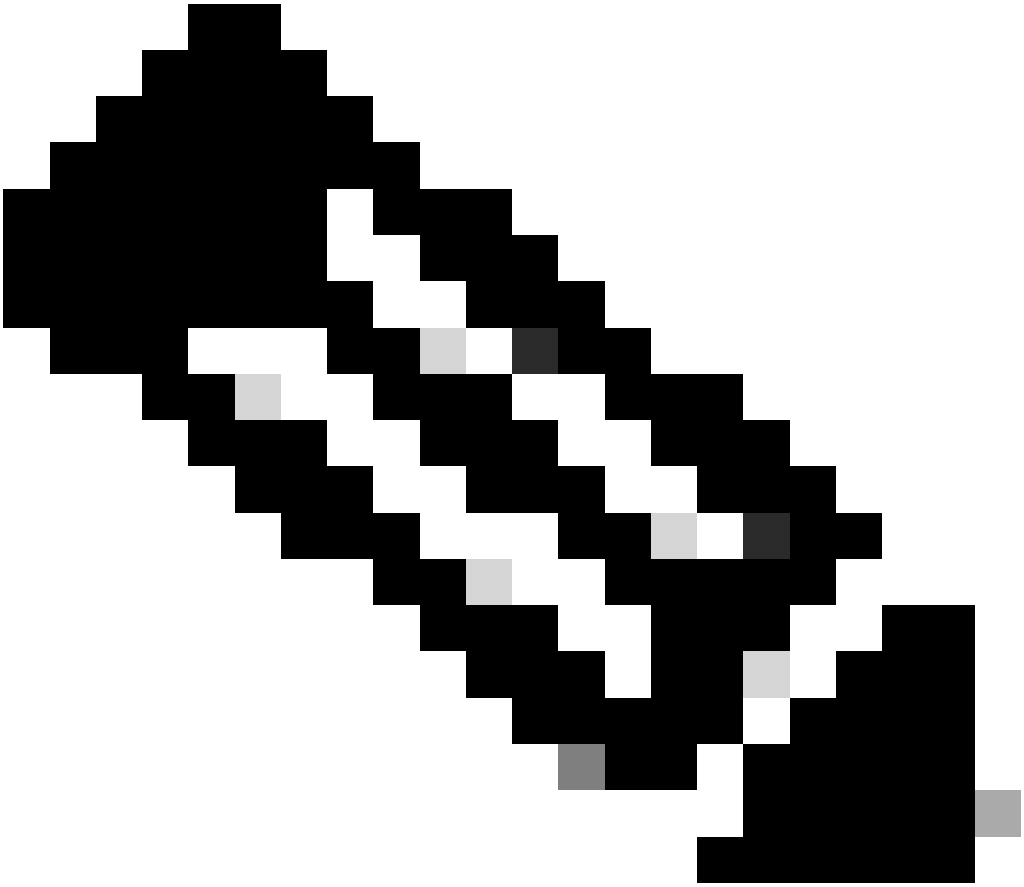
- In riepilogo, verificare che il tunnel abbia configurato lo spazio di indirizzi in cui si trova Cisco ISE:



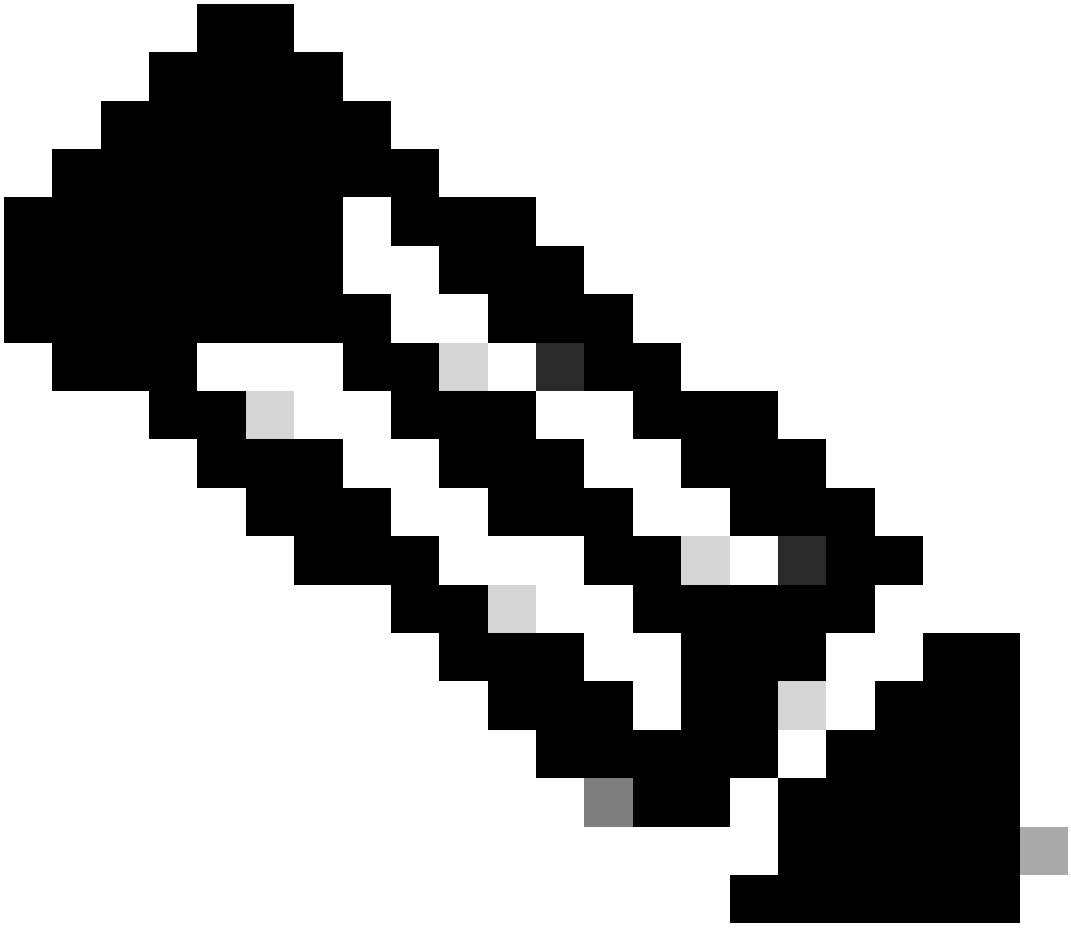
Step 2: Autorizza il traffico sul firewall.

Per consentire a Secure Access di utilizzare il dispositivo ISE per l'autenticazione Radius, è necessario aver configurato una regola da Secure Access alla rete con le porte Radius richieste:

Regola	Origine	Destinazione	Porta di destinazione
ISE - Accesso sicuro **Pool di gestione**	Server_ISE	Pool di gestione IP (RA-VPN)	**CACAO** UDP 1700 (porta predefinita)
Secure Access Management: IP Pool per ISE	Pool IP di gestione	Server_ISE	**Autenticazione, autorizzazione** UDP 1812 (porta predefinita) **Contabilità** UDP 1813 (porta predefinita)
Secure Access Endpoint IP Pool a ISE	Pool IP endpoint	Server_ISE	**Portale di provisioning** TCP 8443 (porta predefinita)
Pool IP endpoint di accesso sicuro nel SERVER DNS	Pool IP endpoint	Server DNS	**DNS** UDP e TCP 53



Nota: per ulteriori informazioni sulle porte correlate ad ISE, consultare il Manuale dell'utente - Riferimento porta.



Nota: se l'ISE è stata configurata per l'individuazione tramite un nome, ad esempio ise.ciscosppt.es, è necessaria una regola DNS

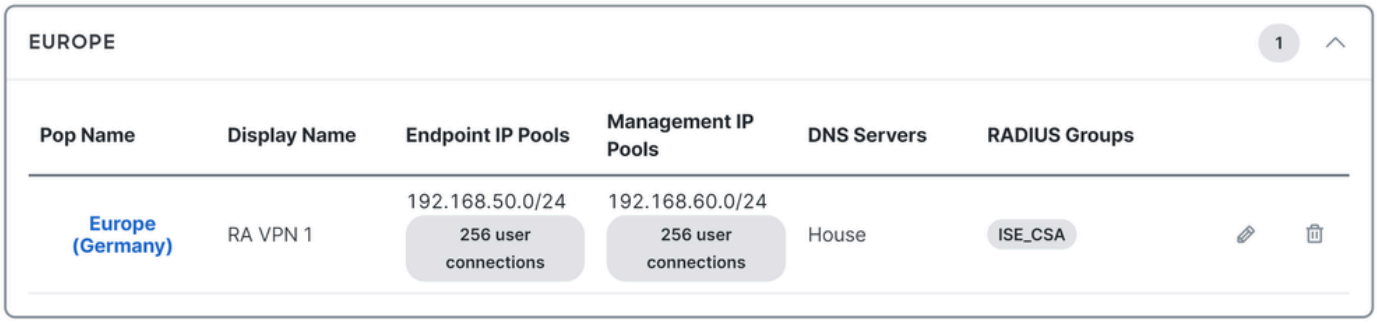
Pool di gestione e pool IP degli endpoint

Per verificare il pool IP di gestione e endpoint, passare al dashboard di accesso sicuro:

- Fare clic su **Connect > End User Connectivity**
- Fare clic su Virtual Private Network

- Inferiore **Manage IP Pools**

- Fare clic su **Manage**



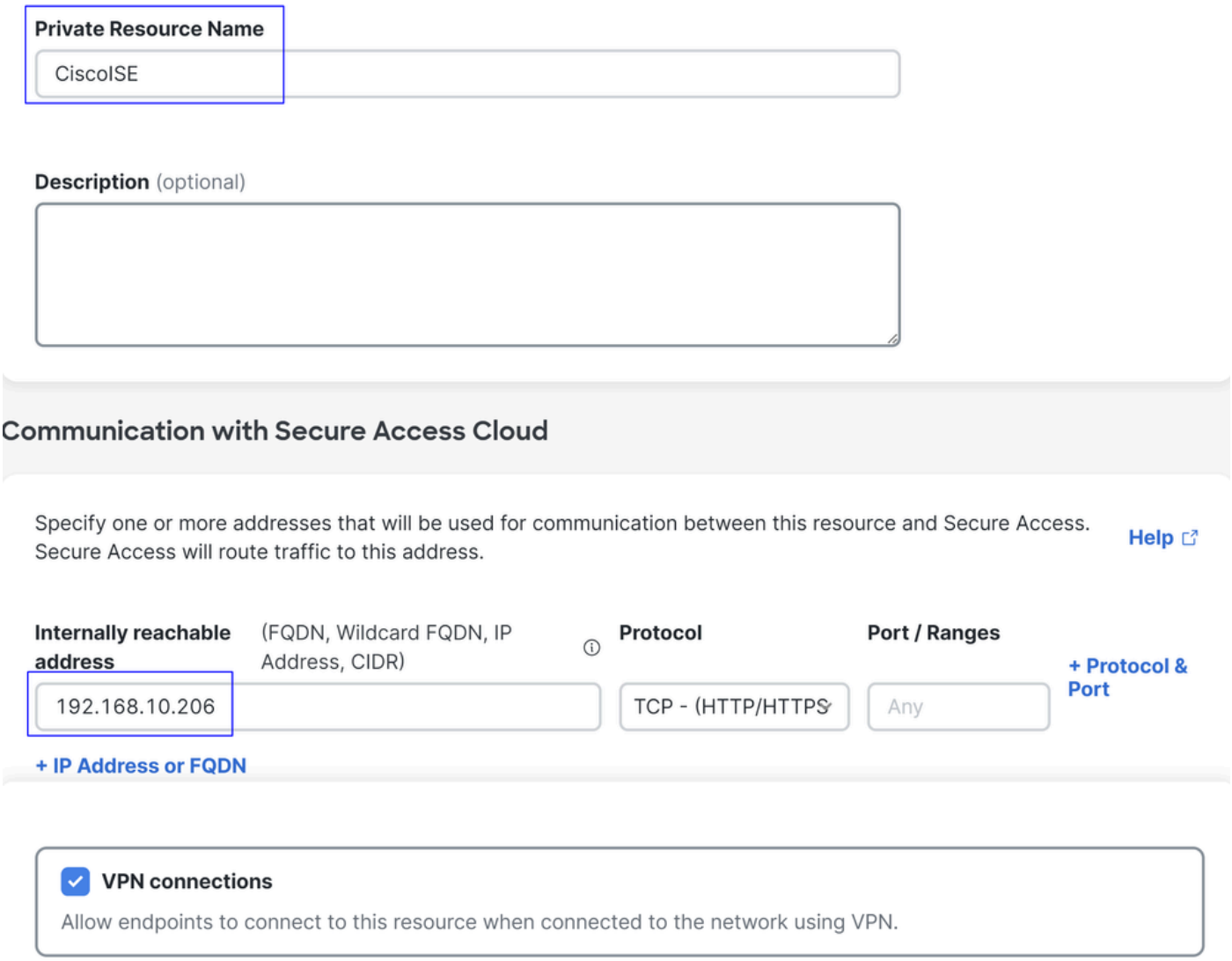
Fase 3: verificare che l'ISE sia configurata in Private Resources

Per consentire agli utenti connessi tramite la VPN di passare a **ISE Provisioning Portal**, è necessario accertarsi di aver configurato il dispositivo come risorsa privata per consentire l'accesso, che viene utilizzata per consentire il provisioning automatico della ISE Posture Module rete tramite la VPN.

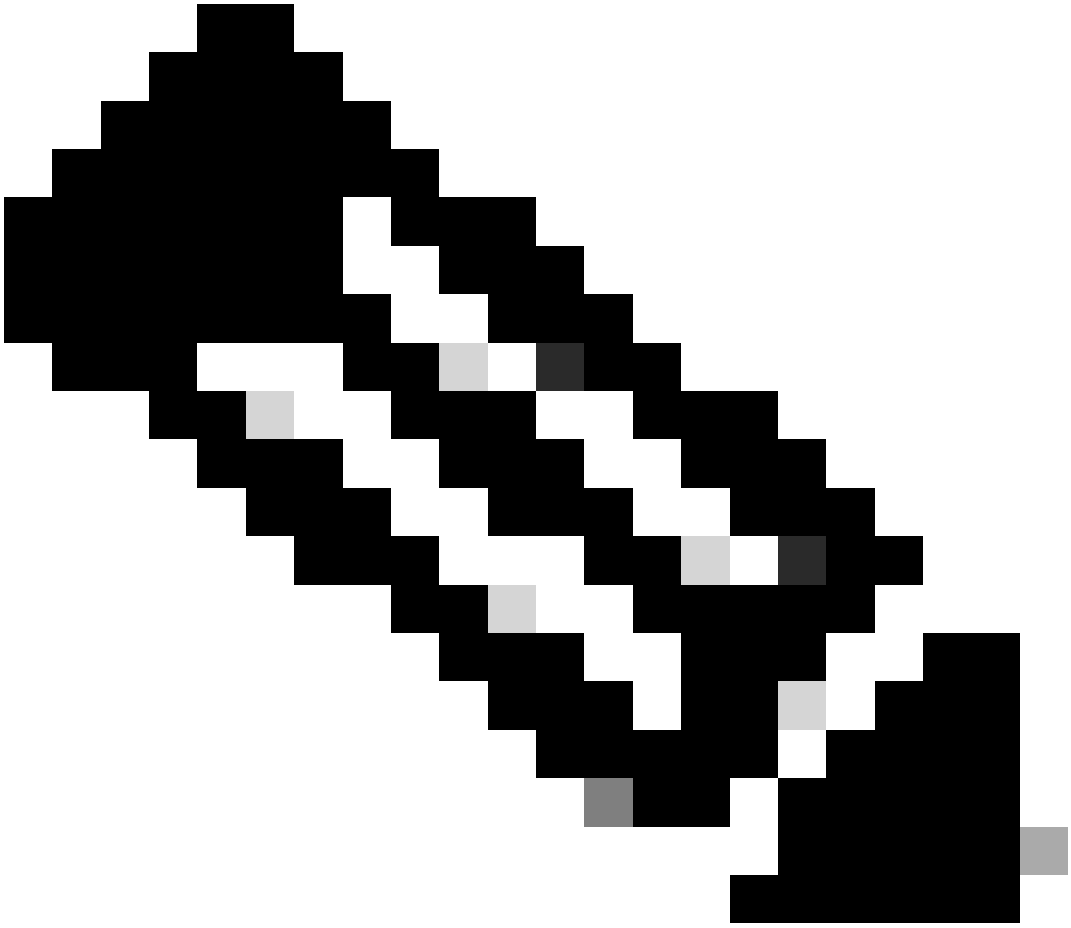
Per verificare di aver configurato correttamente ISE, passare al Dashboard di accesso sicuro:

- Fare clic su **Resources > Private Resources**

- Fare clic sulla risorsa ISE



Se necessario, è possibile limitare la regola alla porta del portale di provisioning (8443).



Nota: assicurarsi di aver selezionato la casella di controllo per le connessioni VPN.

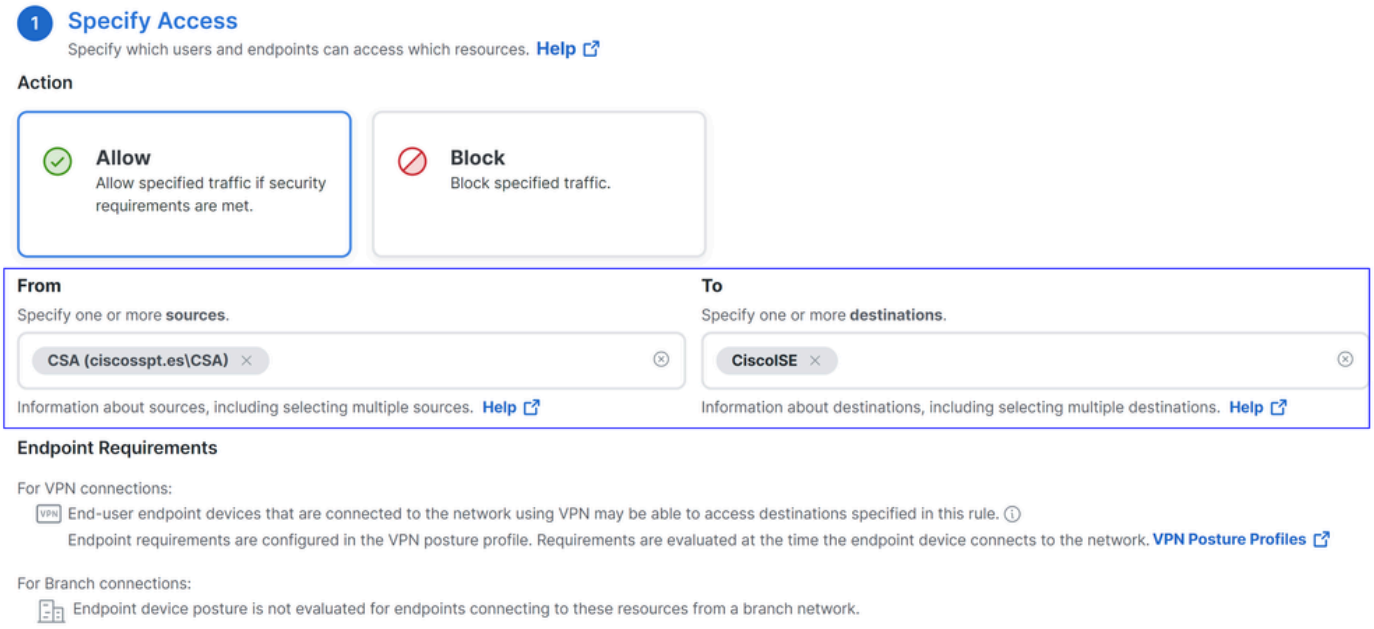
Fase 4: Autorizzare l'accesso ad ISE in base alla policy di accesso

Per consentire agli utenti connessi tramite la VPN di passare a **ISE Provisioning Portal**, è necessario verificare di aver configurato e **Access Policy** di consentire agli utenti configurati in base a tale regola di accedere alla risorsa privata configurata in Step3.

Per verificare di aver configurato correttamente ISE, passare al Dashboard di accesso sicuro:

- Fare clic su **Secure > Access Policy**

- Fare clic sulla regola configurata per consentire l'accesso degli utenti VPN ad ISE

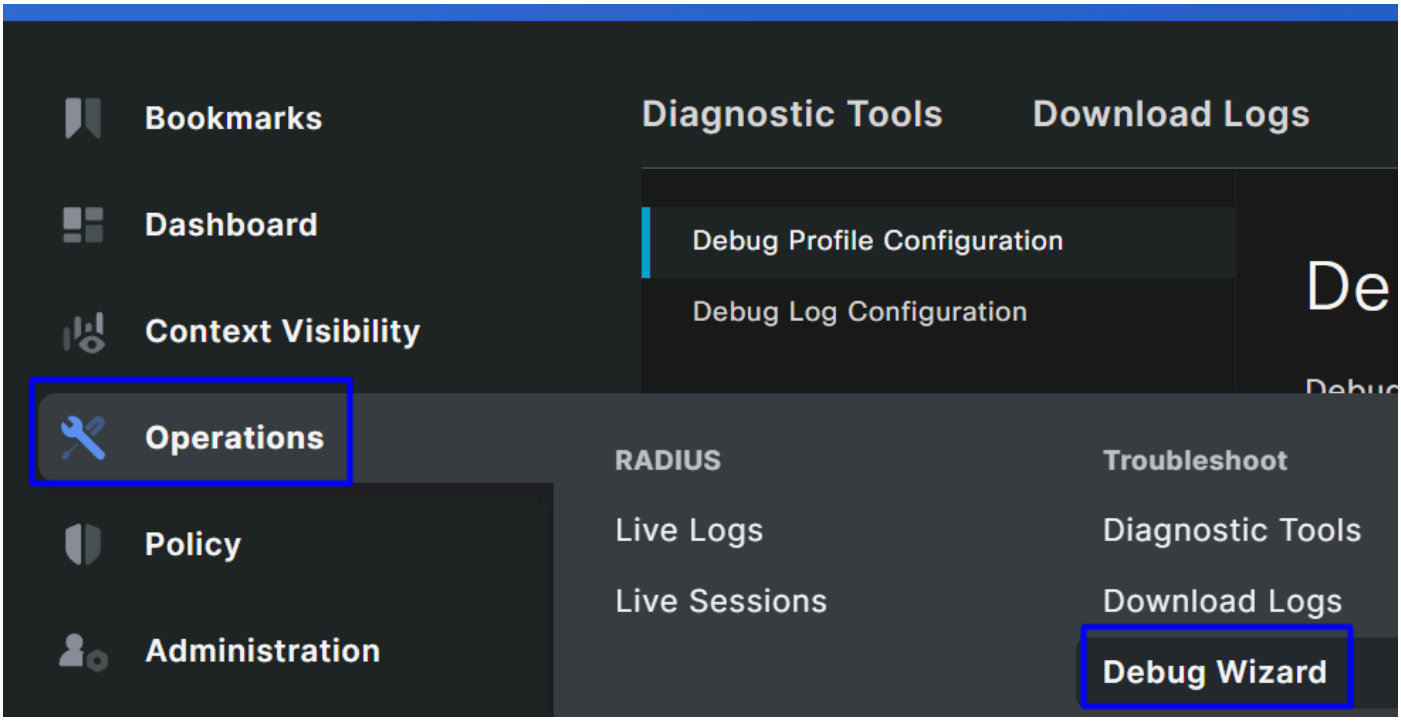


Risoluzione dei problemi

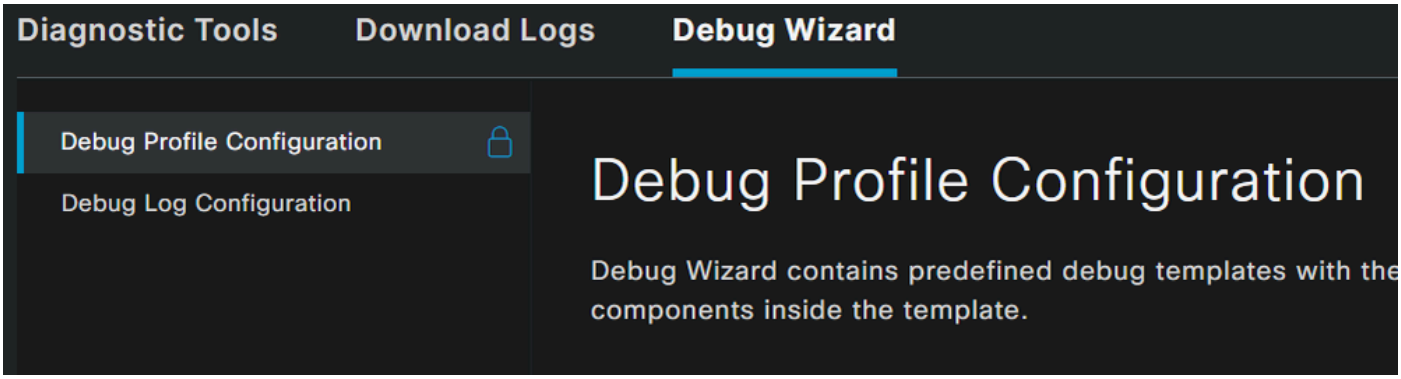
Come scaricare i log di debug di ISE Posture

Per scaricare i log ISE per verificare un problema relativo alla postura, procedere come segue:

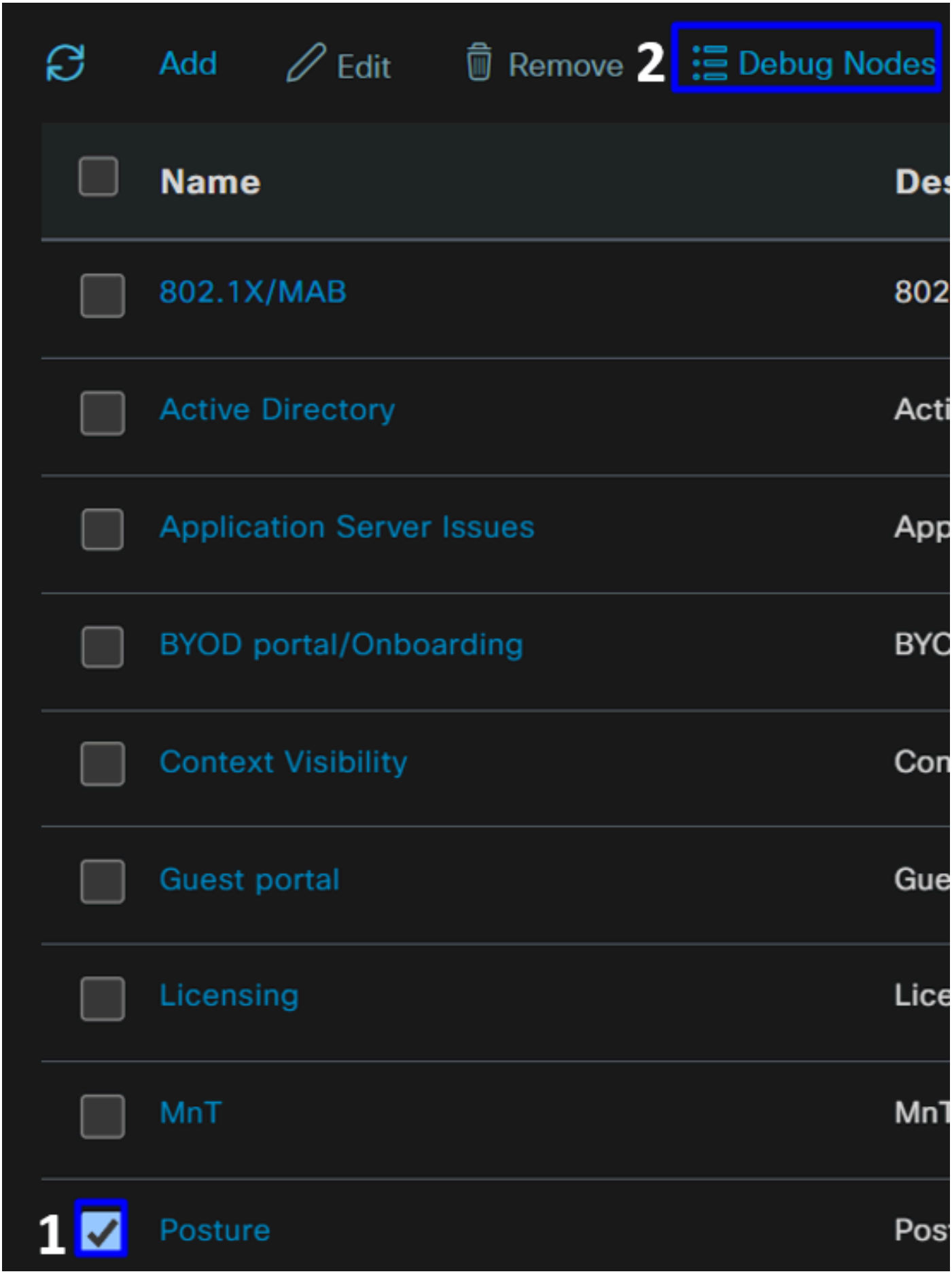
- Passa al dashboard ISE
- Fare clic su Operations > Troubleshoot > Debug Wizard



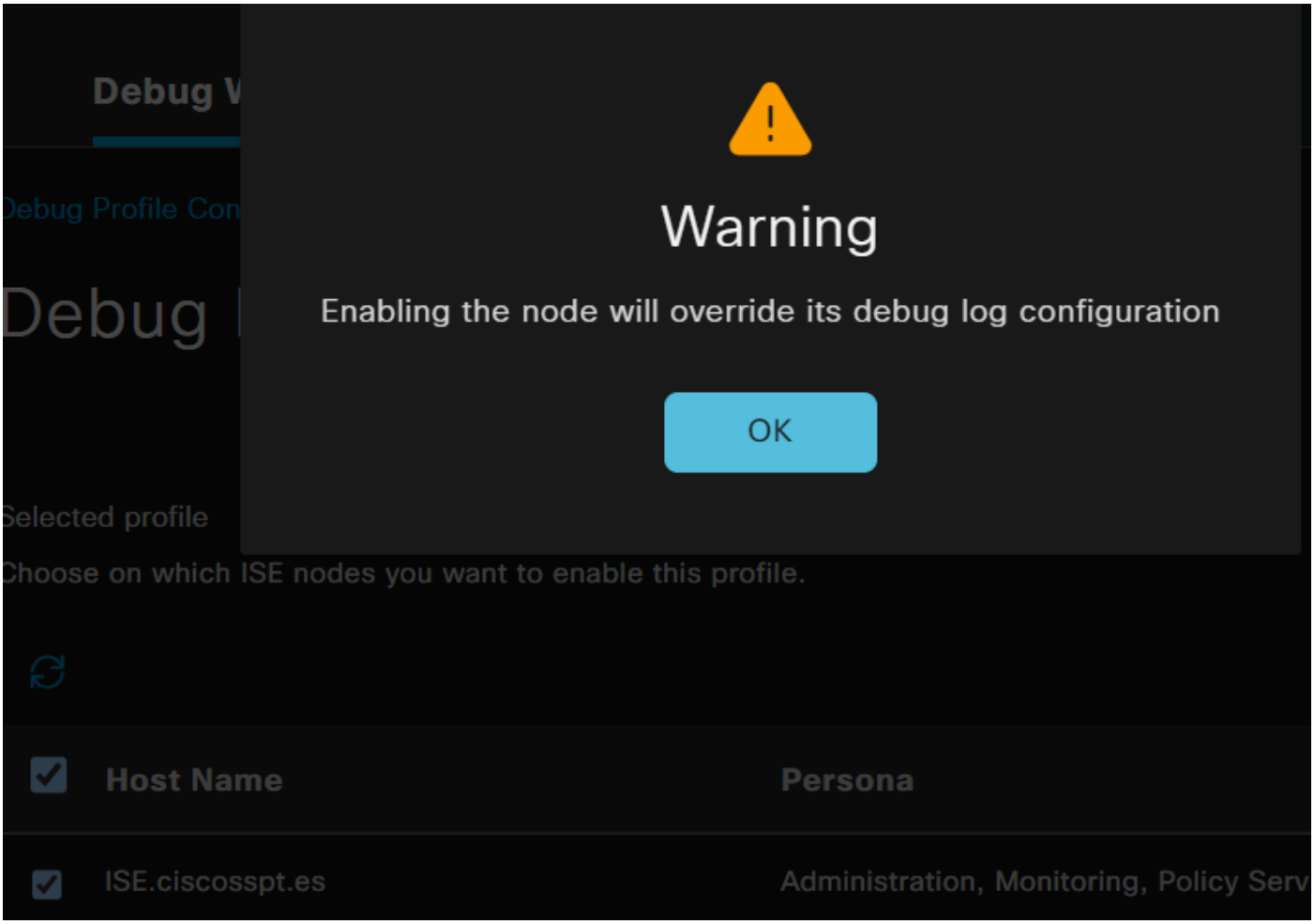
- Fare clic su Debug Profile Configuration



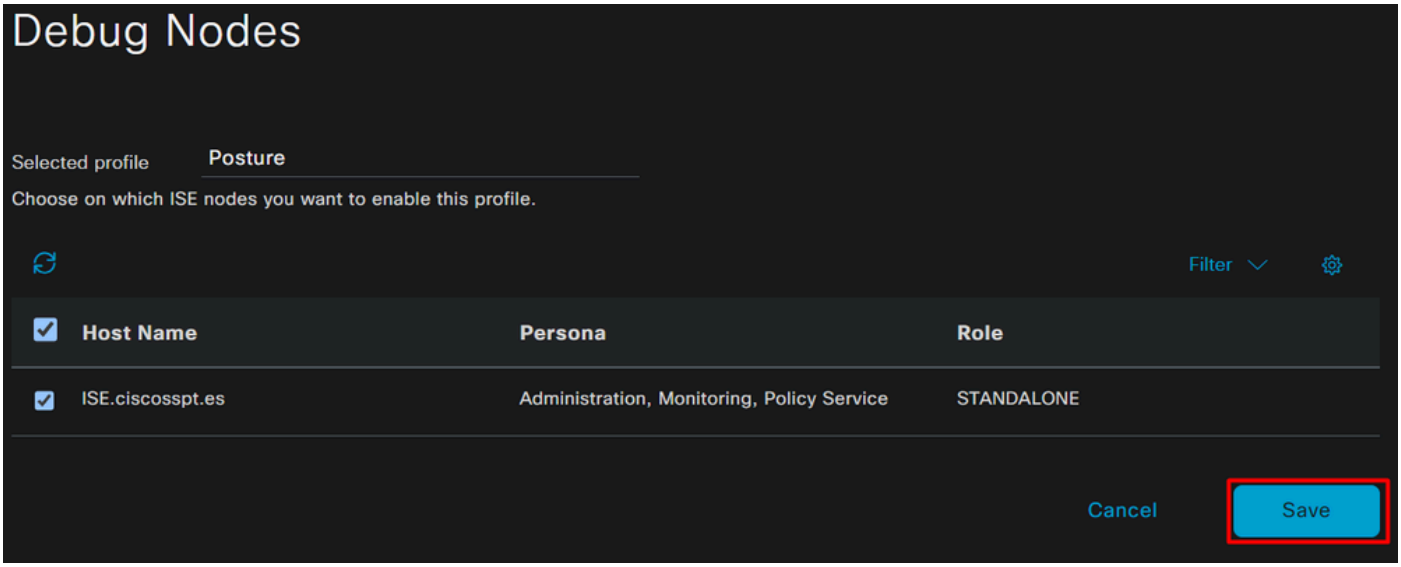
- Selezionare la casella di controllo **Posture > Debug Nodes**

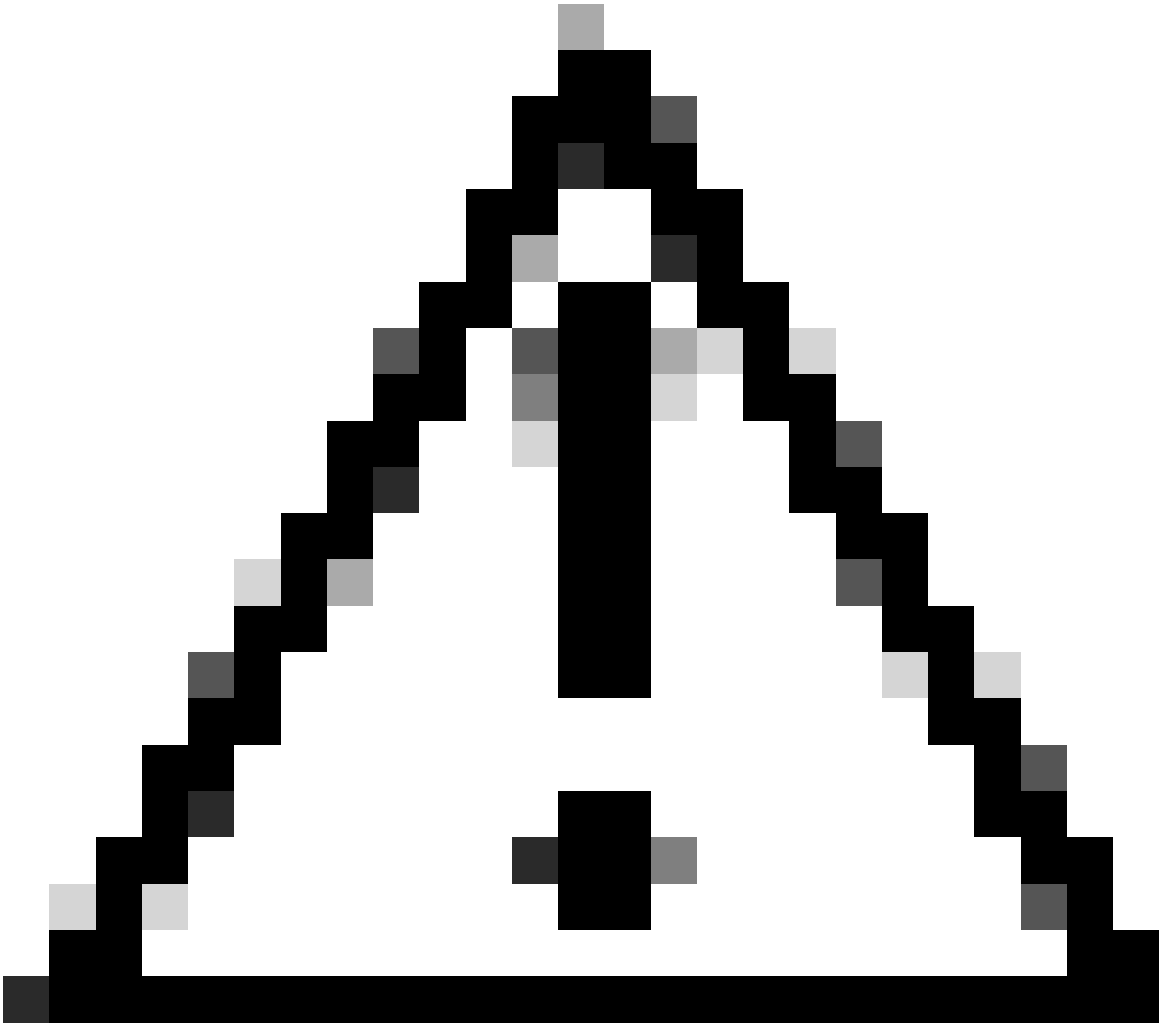

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- Selezionare la casella di controllo relativa ai nodi ISE su cui si desidera abilitare la modalità di debug per risolvere il problema



- Fare clic su Save

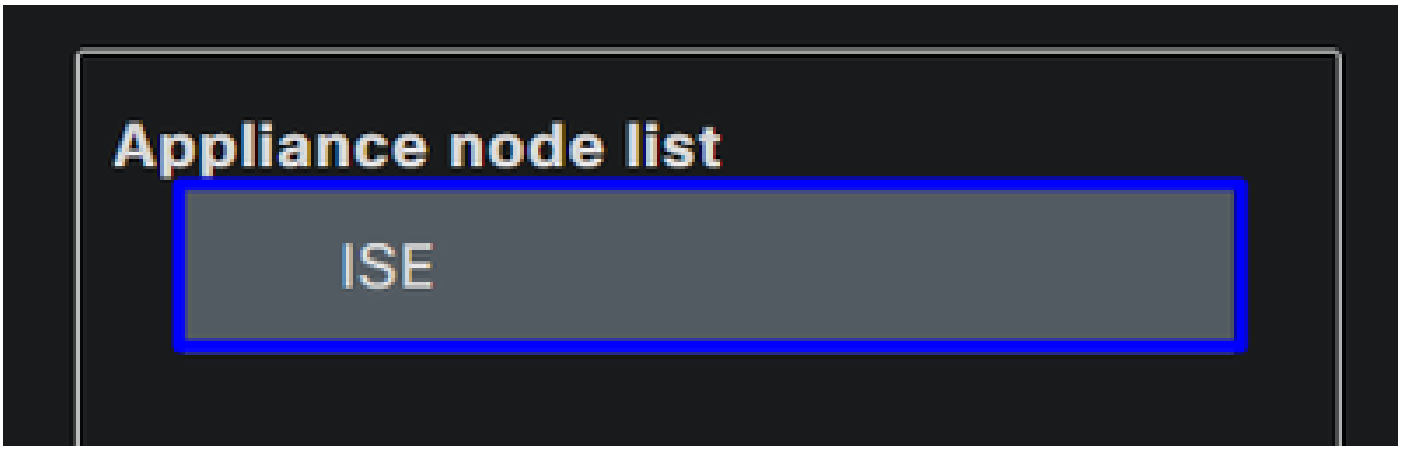

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



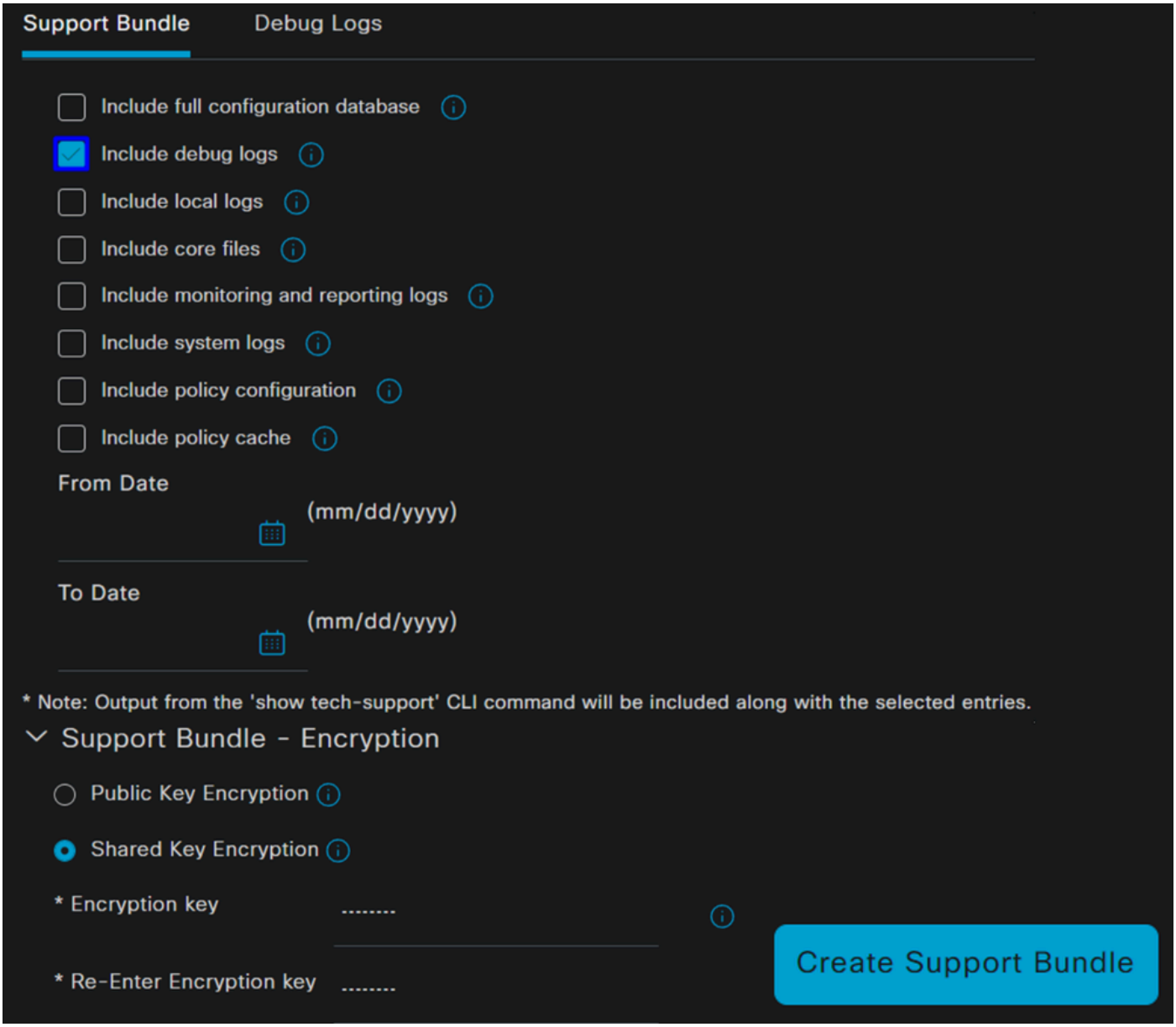
Attenzione: dopo questo punto, è necessario iniziare a riprodurre il problema; **the debug logs can affect the performance of your device**.

Dopo aver riprodotto il problema, procedere con i passi successivi:

- Fare clic su Operations > Download Logs
- Scegliere il nodo da cui estrarre i registri

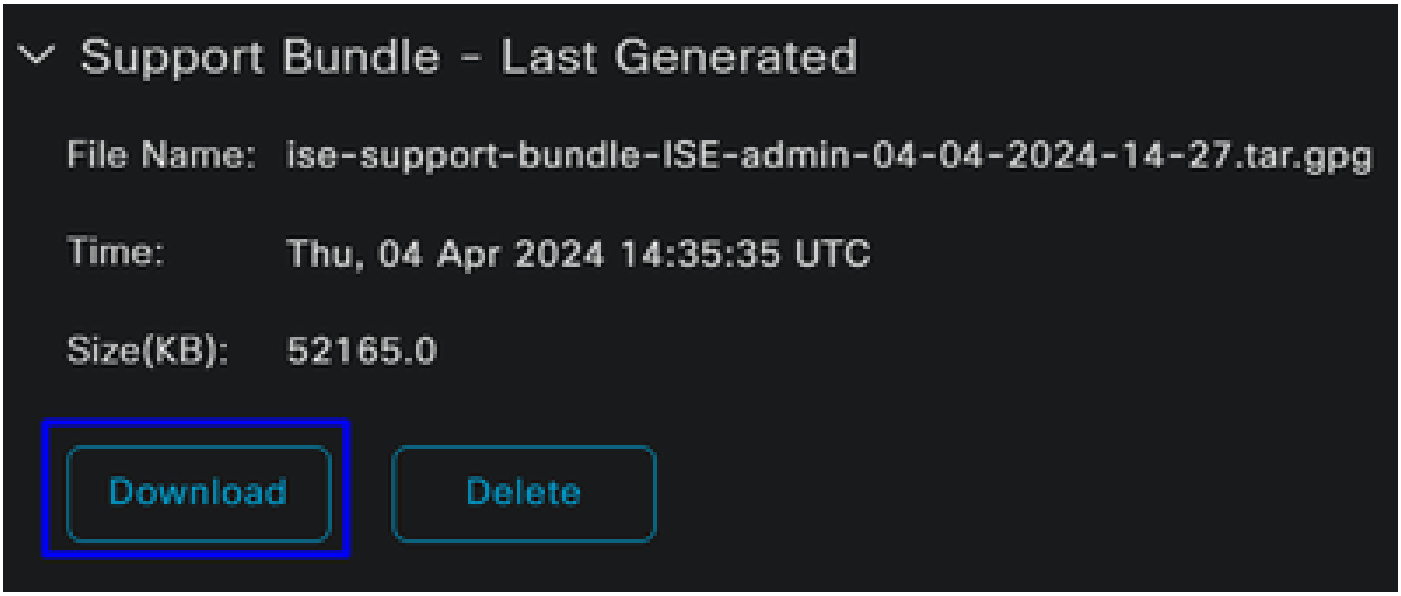


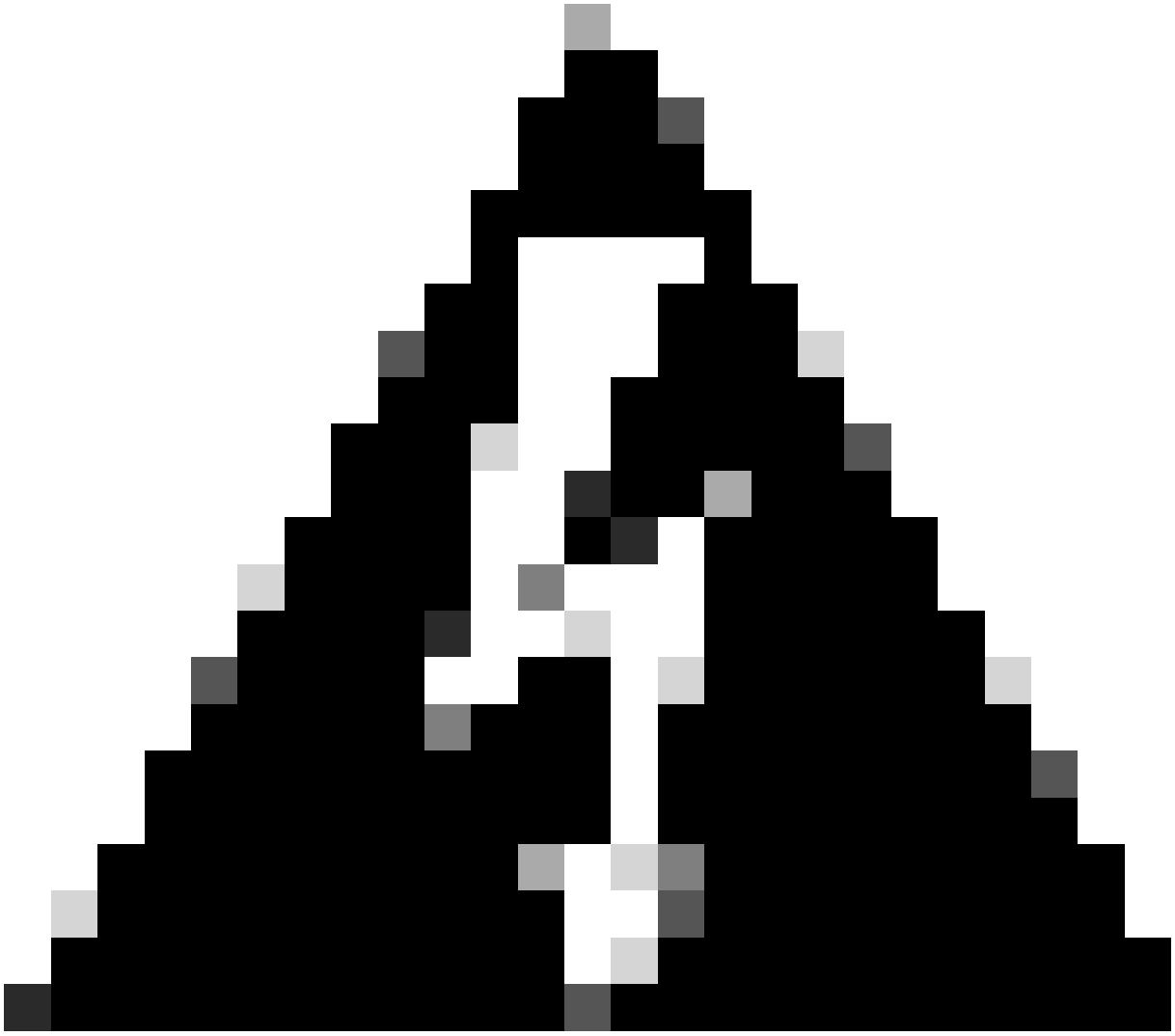
- In **Support Bundle**, scegliere le opzioni seguenti:



- Include debug logs
- Inferiore **Support Bundle Encryption**
  - **Shared Key Encryption**
    - Riempi **Encryption key** e **Re-Enter Encryption key**

- Fare clic su **Create Support Bundle**
- Fare clic su **Download**





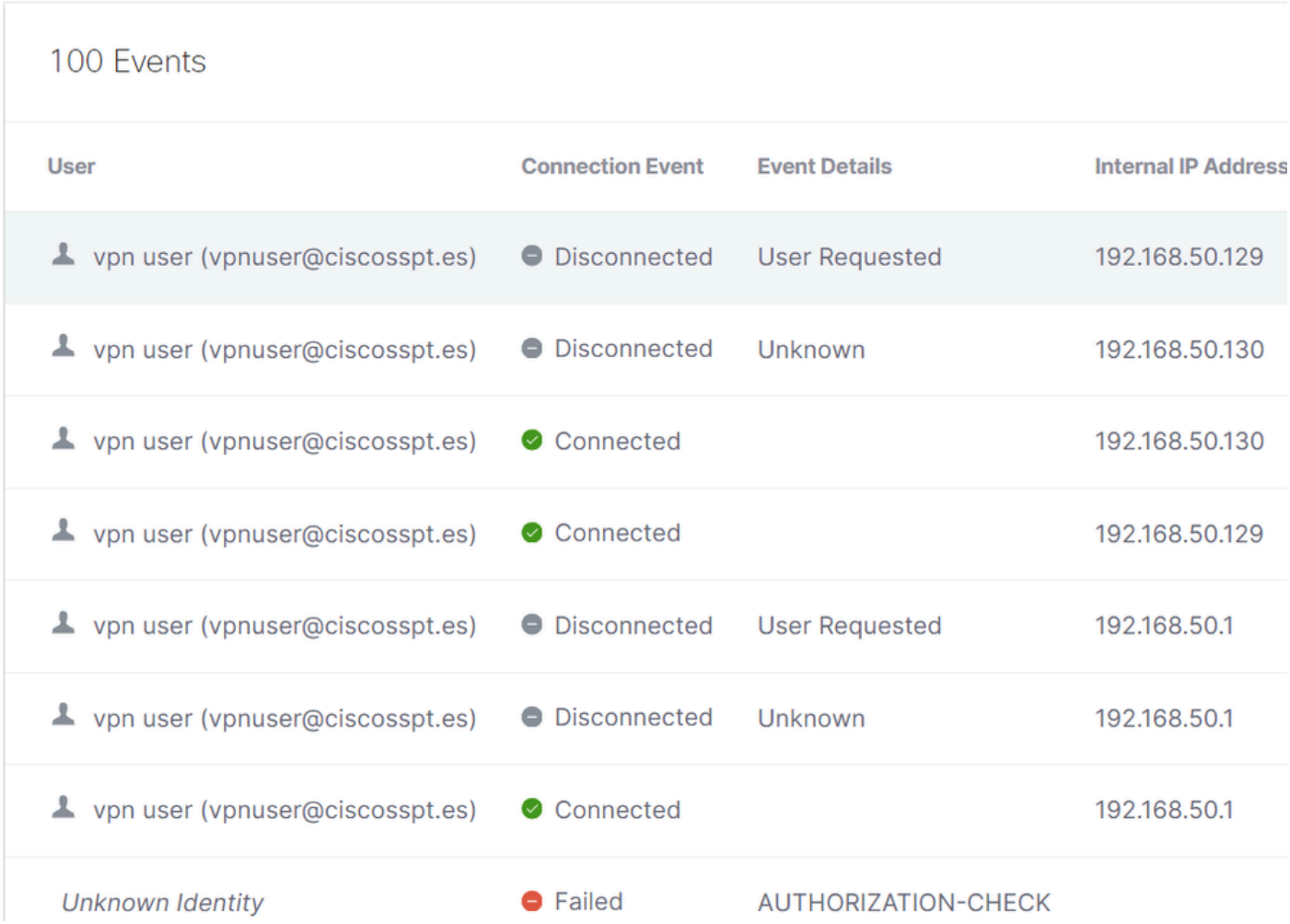
Avviso: disabilitare la modalità di debug abilitata nella fase Debug Profile Configuration

---

Verifica dei registri di accesso remoto per l'accesso protetto

Accedere al Dashboard di accesso protetto:

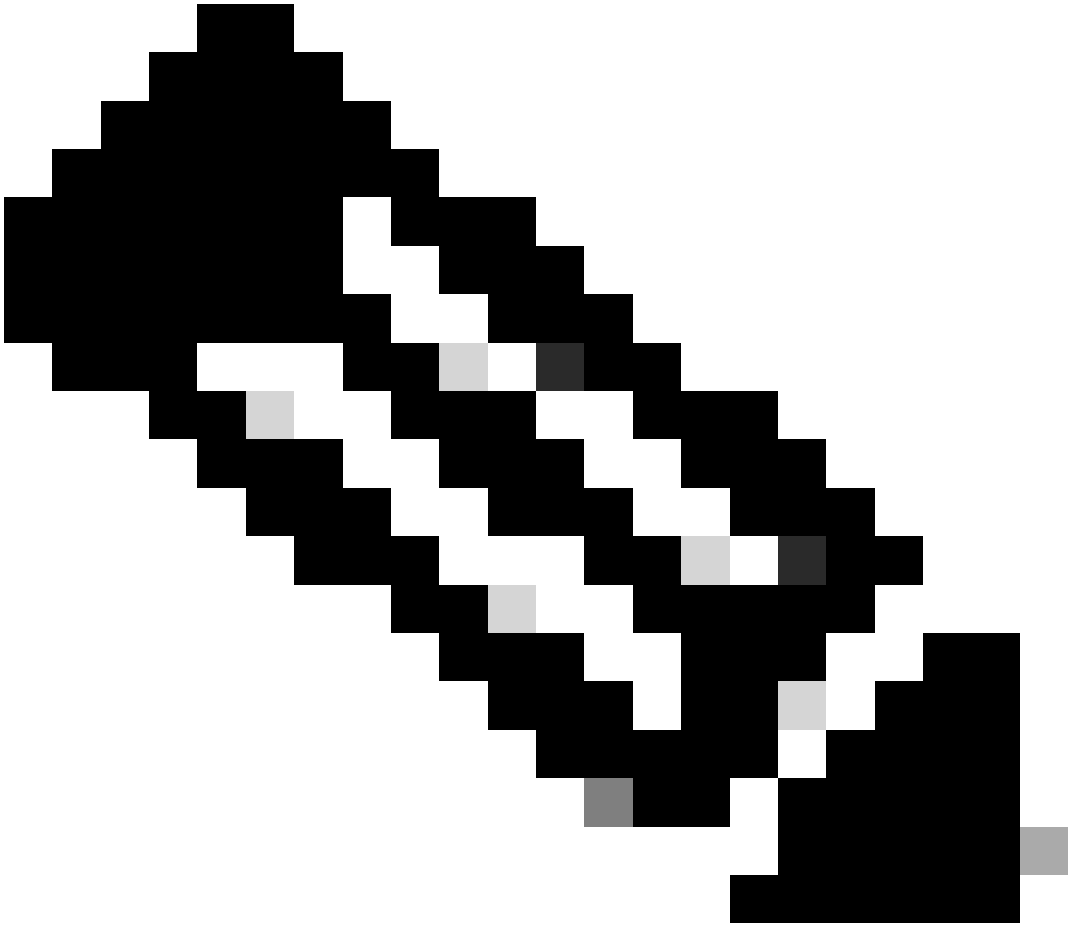
- Fare clic su Monitor > Remote Access Logs



Genera pacchetto DART su client protetto

Per generare il pacchetto DART sul computer, verificare l'articolo successivo:

Strumento di diagnostica e reporting (DART) Cisco Secure Client



Nota: dopo aver raccolto i log indicati nella sezione Risoluzione dei problemi, aprire una richiesta con **TAC** cui procedere all'analisi delle informazioni.

Informazioni correlate

- **Supporto tecnico Cisco e download**
- **Documentazione e guida per l'utente di Secure Access**

- **Download del software Cisco Secure Client**
- **Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).