

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione Duo](#)

[Configurazione accesso sicuro](#)

[Configurazione del gruppo Radius sui pool IP](#)

[Configurazione del profilo VPN per l'uso di ISE](#)

[Impostazioni generali](#)

[Autenticazione, autorizzazione e accounting](#)

[Traffic Steering](#)

[Cisco Secure Client Configuration](#)

[Configurazioni ISE](#)

[Configura elenco dispositivi di rete](#)

[Configurare un gruppo](#)

[Configura utente locale](#)

[Configura set di criteri](#)

[Configura autorizzazione set di criteri](#)

[Configura utenti locali o di Active Directory Radius](#)

[Configurazione della postura ISE](#)

[Configura condizioni di postura](#)

[Configura requisiti postura](#)

[Configura criterio postura](#)

[Configura provisioning client](#)

[Configura criterio di provisioning client](#)

[Creare i profili di autorizzazione](#)

[Configura set di criteri di postura](#)

[Verifica](#)

[Convalida postura](#)

[Connessione nel computer](#)

[Come verificare i log in ISE](#)

[Conformità](#)

[Non conformità](#)

[Primi passi verso un accesso sicuro e l'integrazione con ISE](#)

[Risoluzione dei problemi](#)

[Come scaricare i log di debug di ISE Posture](#)

[Verifica dei registri di accesso remoto per l'accesso protetto](#)

[Genera pacchetto DART su client protetto](#)

[Informazioni correlate](#)

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

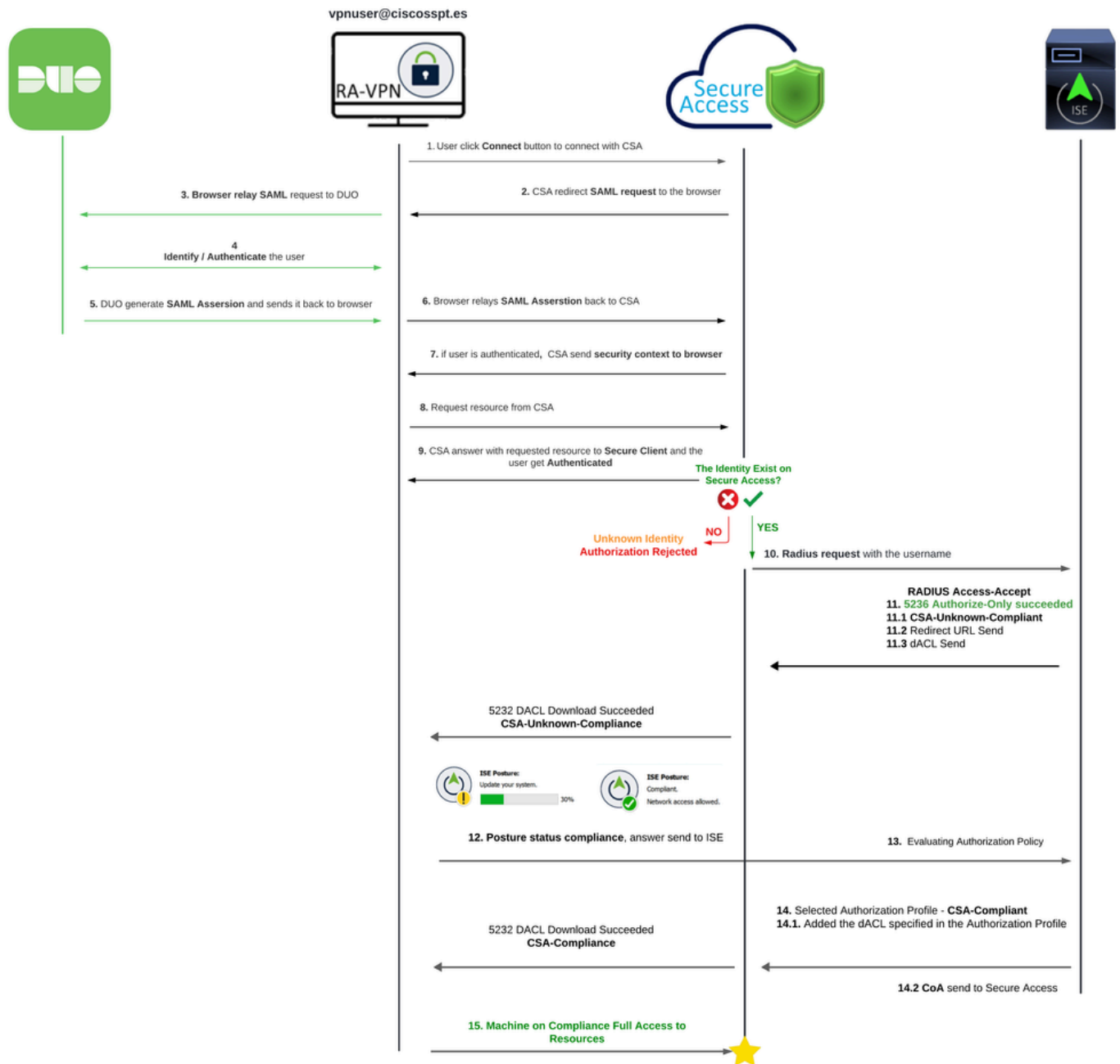
Componenti usati

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



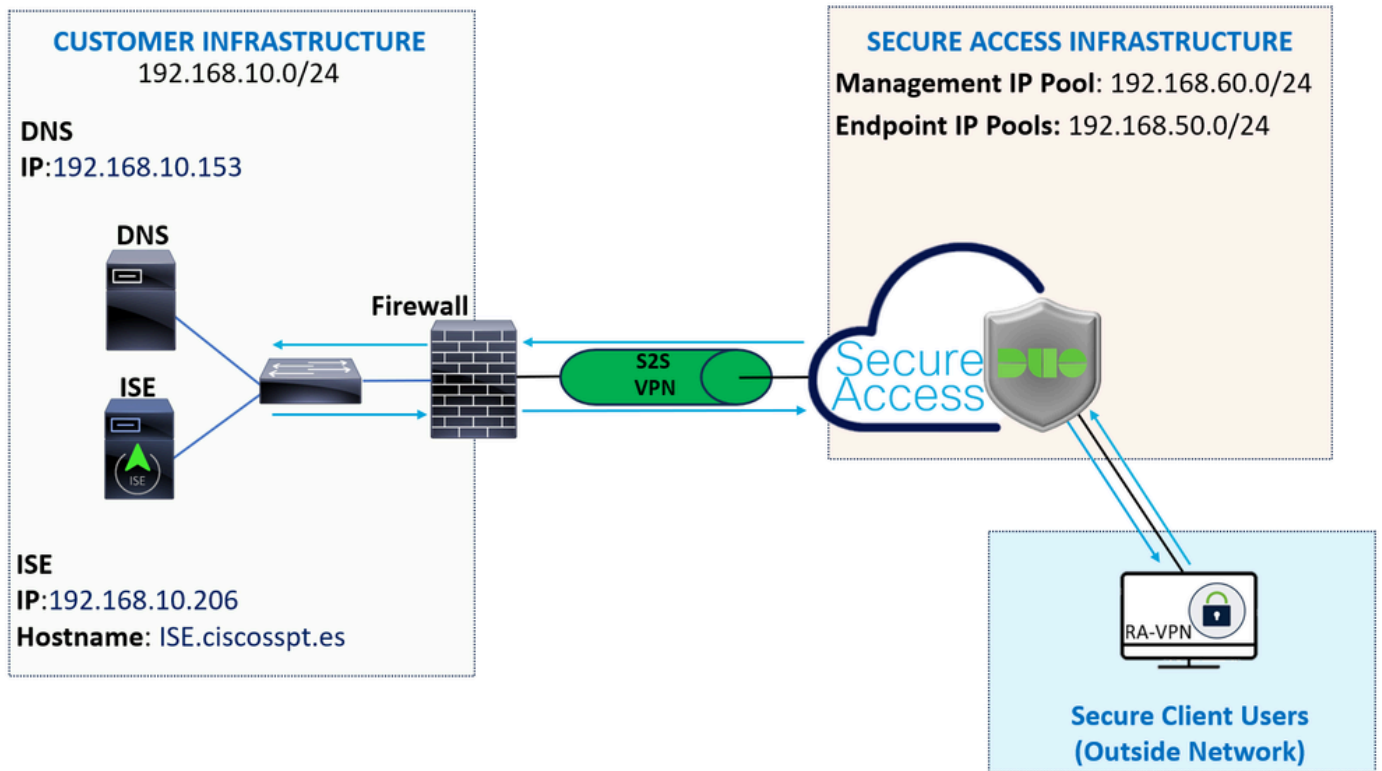
L'integrazione di Duo SAML con Cisco Identity Services Engine (ISE) migliora il processo di autenticazione e aggiunge un altro livello di sicurezza alle soluzioni Cisco Secure Access. Duo SAML fornisce una funzionalità Single Sign-On (SSO) che semplifica il processo di accesso dell'utente garantendo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

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

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



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

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

Generic SAML Service Provider - Single Sign-On

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

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

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy

Certificate Fingerprints

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

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 su **Manage**

Manage IP Pools

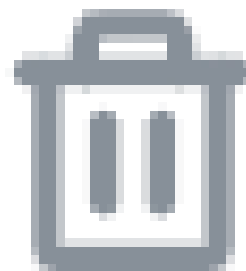
Manage

2 Regions mapped

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

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

- 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

RADIUS Groups (optional)

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



No RADIUS groups created

Add RADIUS Group

← Edit RADIUS Group



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

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings



RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×



+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

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

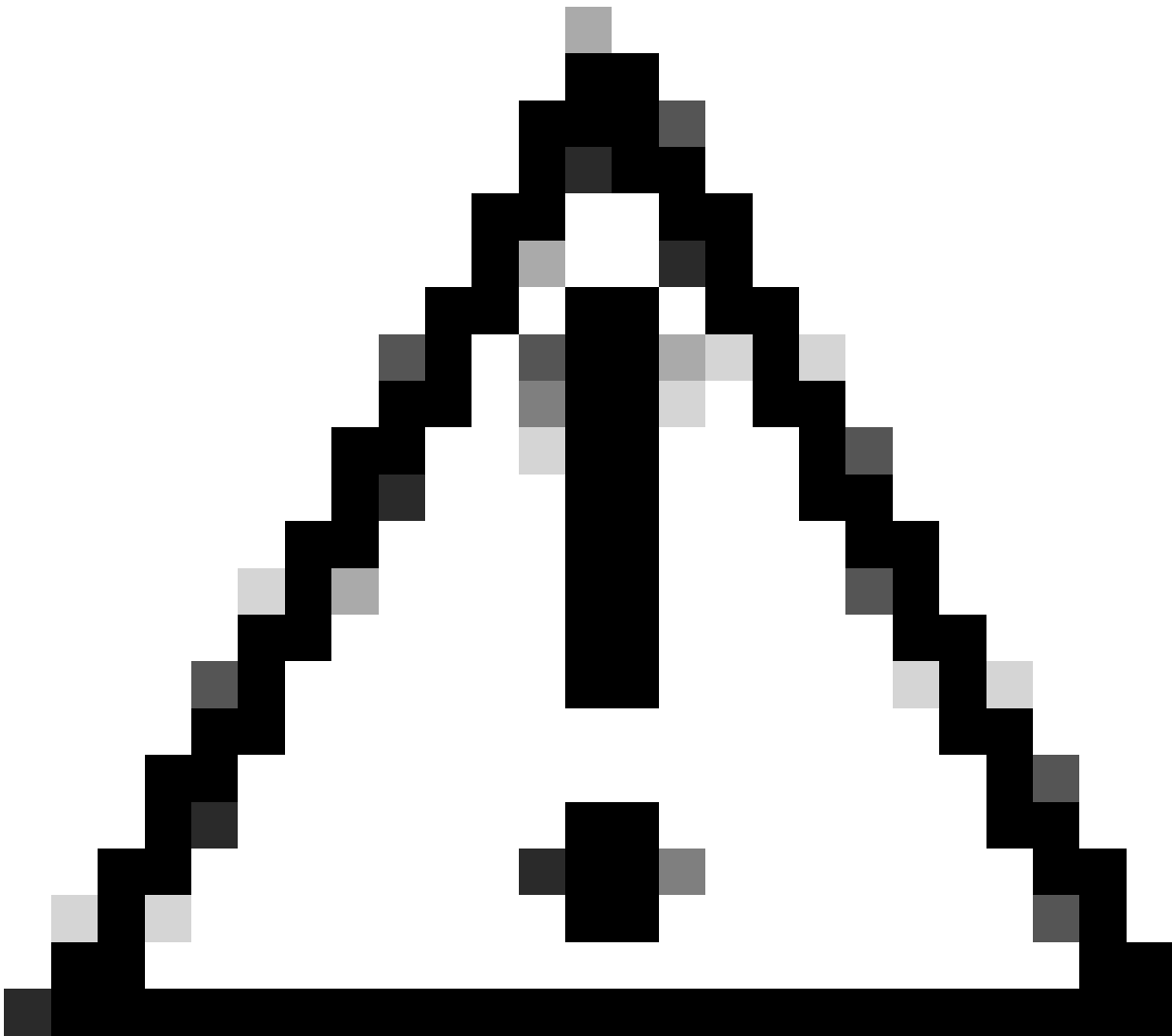
- **Authorization:** selezionare la casella di controllo per Authorization e selezionare la porta, per impostazione predefinita, 1812

- 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

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

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

- Quindi, configurare le opzioni successive:

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Password

Cancel

Save & Add server

Save

- **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'opzione Assign Server e selezionare il server ISE:

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- 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

Settings

Type Generic SAML Service Provider - Single Sign-On

Name

ISE - SAML

Duo Push users will see this when approving transactions.

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

ISE - SAML

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

Metadata

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

Certificate Fingerprints

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

Downloads

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

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

VPN Profile name

ISE_CSA_SAML

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


Authenticate with CA certificates
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

SAML Metadata XML Configuration

 **1. Download Service Provider XML file**
This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

 **2. Generate IdP Security Metadata XML File**
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

 **3. Upload IdP security metadata XML file**

✓ File 'ISE - SAML - IDP Metadata.xml' uploaded. [Replace](#) [Delete](#)

Manual Configuration



Cancel

Back

Next

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

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

Authentication, Authorization, and Accounting

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

Authentication **Authorization** Accounting

Enable Radius Authorization

Use defaults or customize groups to map to regions

Select one group for all regions

[+ Group](#)

ISE_CSA

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



Cancel

Back

Next

- **Authorization**

- **Enable Radius Authorization:** 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.

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

Authentication, Authorization, and Accounting

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

Authentication Authorization Accounting

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

Select one group for all regions + Group

ISE_CSA ▼

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



Cancel

Back

Next

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

- Fare clic su **Next**

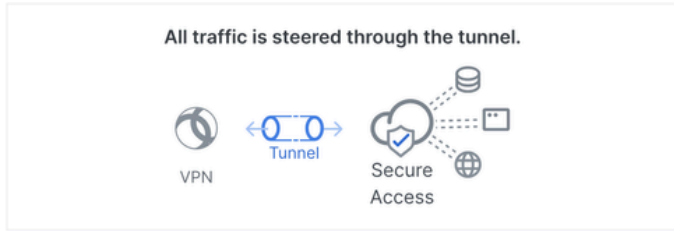
After you have done configured the Authentication, Authorization and Accounting continuare con Traffic Steering.

Traffic Steering

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

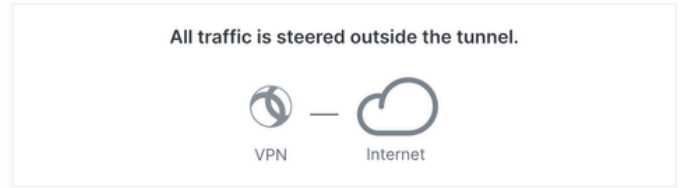
Tunnel Mode

Connect to Secure Access



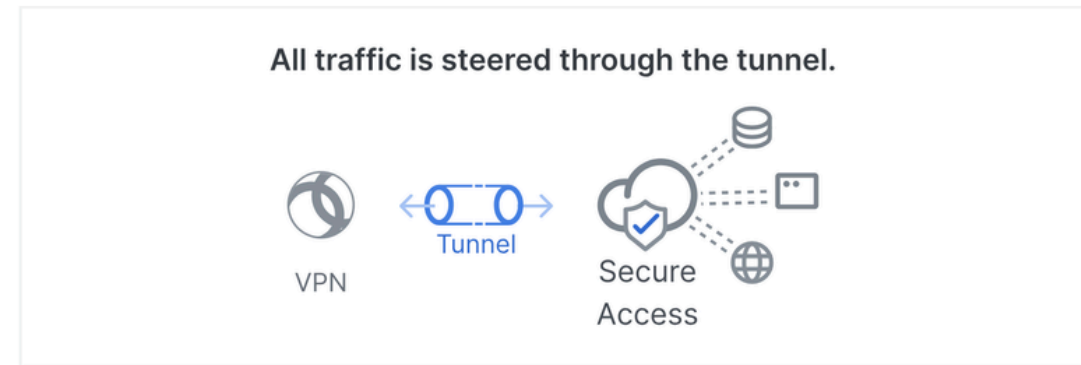
Tunnel Mode

Bypass Secure Access



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

Connect to Secure Access



Add Exceptions

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

+ Add

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

Cancel

Back **Next**

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 attraverso Secure Access (nessuna protezione Internet)

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

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

[+ Add](#)

Destinations

Exclude Destinations

Actions



No matches found

[Cancel](#)

[Back](#)

[Next](#)



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

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

Banner Message
Require user to accept a banner message post authentication

Session Timeout
 days

Session Timeout Alert
 minutes before

Maximum Transmission Unit ⓘ

[Cancel](#) [Back](#) [Save](#)

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

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 valore Management 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 Name per il gruppo e fare clic su **Submit**

The screenshot shows the Administration interface with the following structure:

- Administration**
 - System
 - Deployment
 - Licensing
 - Certificates
 - Logging
 - Maintenance
 - Upgrade
- Network Resources**
 - Network Devices
 - Network Device Groups
 - Network Device Profiles
 - External RADIUS Servers
 - RADIUS Server Sequences
 - NAC Managers
- Identity Management**
 - Identities
 - Groups** (highlighted with a red box)
 - External Identity So
 - Identity Source Seq
 - Settings

Identity Groups

- Endpoint Identity Groups
- User Identity Groups** (highlighted with a red box)

User Identity Groups

User Identity Group

* Name **5** **CSA-ISE**

Description

6 **Submit**

Name
<input type="checkbox"/> ALL_ACCOUNTS (default)
<input type="checkbox"/> CSA-ISE → GROUP CREATED
<input type="checkbox"/> Employee

Configura utente locale

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

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

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

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

▼ User Groups

⋮ ▼

- **Username:** 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.

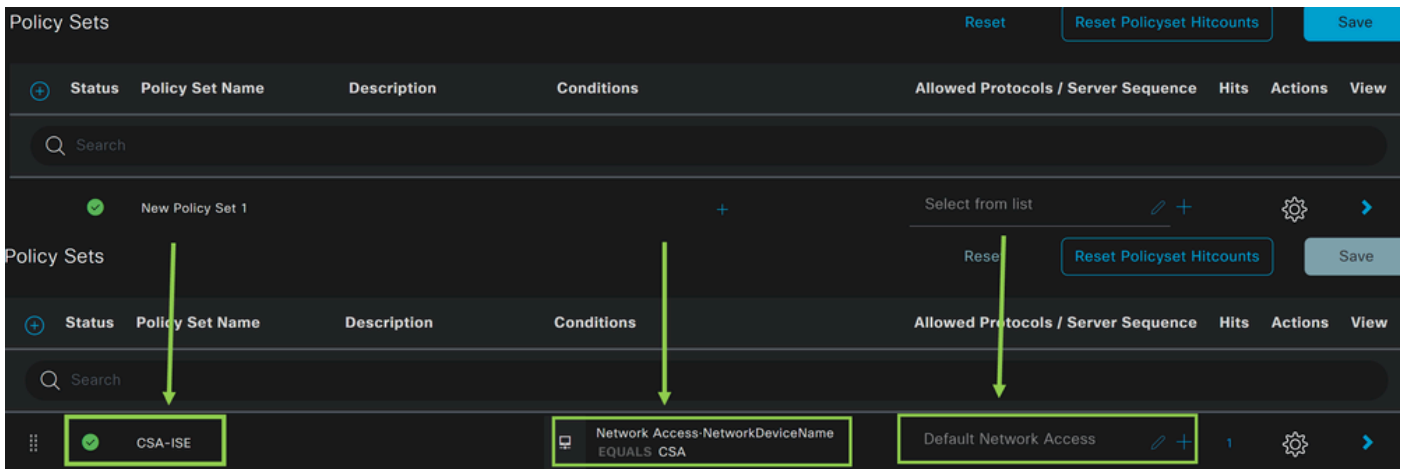
Quindi, è possibile eseguire **Save** la configurazione e continuare con il passaggio **Configure Policy Set**.

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:

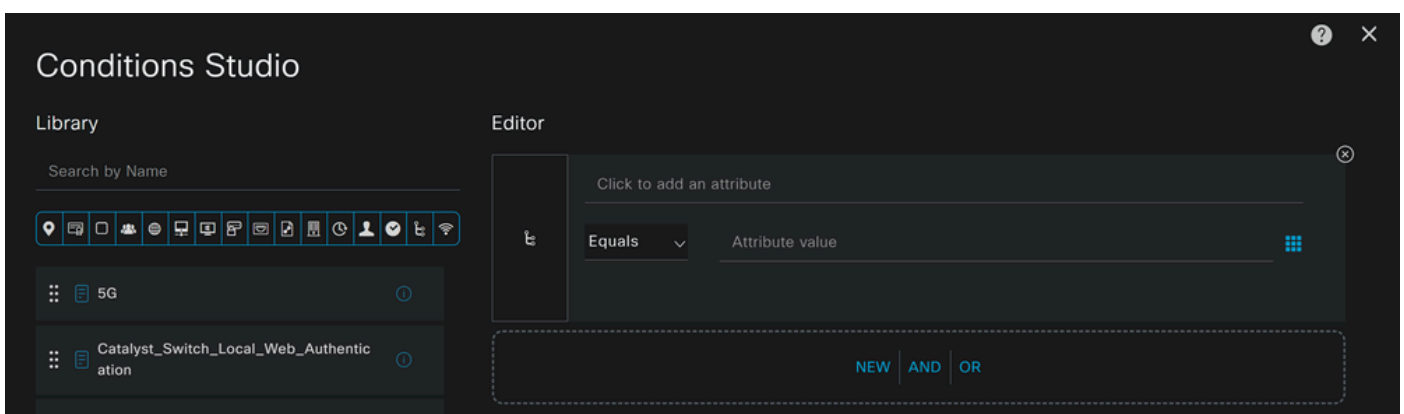
- Fare clic su Policy > Policy Sets
- Fare clic per + aggiungere un nuovo set di criteri



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**.

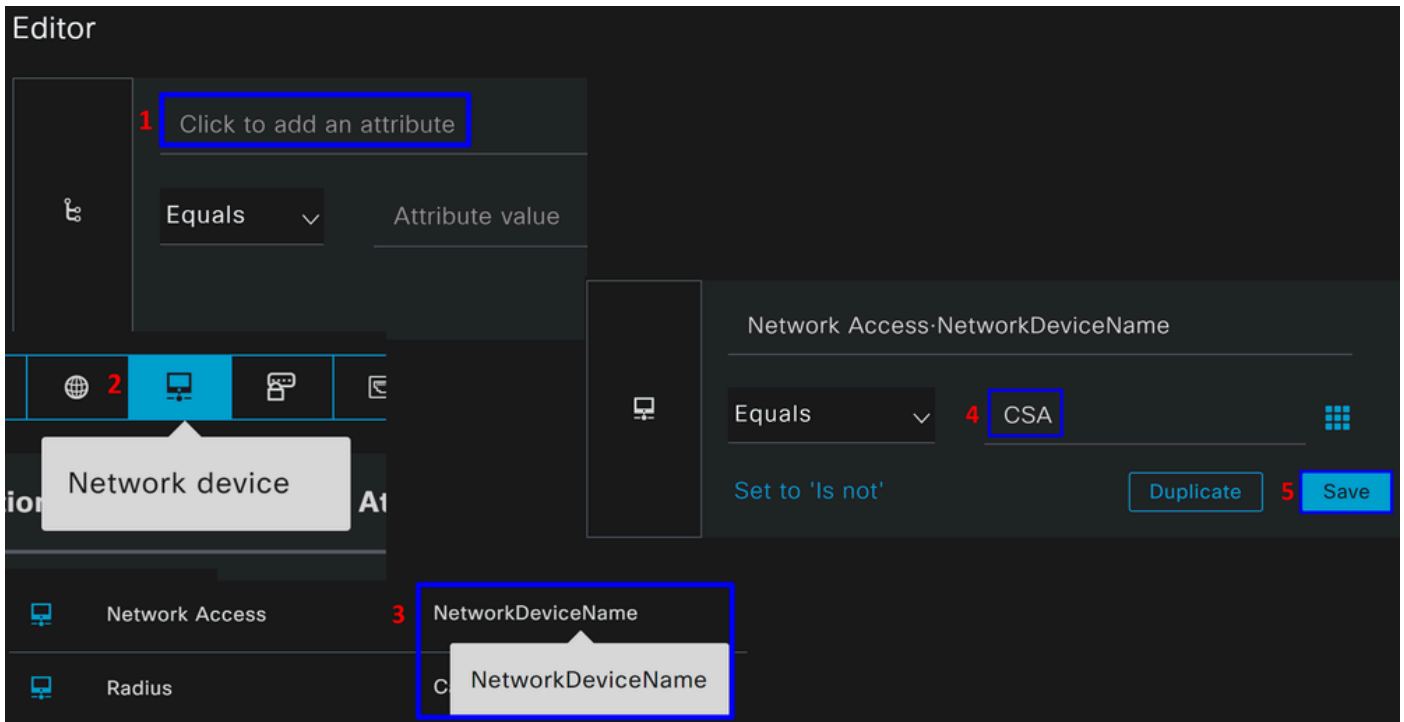
Per creare l'oggetto **condition** che corrisponde al set di criteri, procedere con le istruzioni seguenti:

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



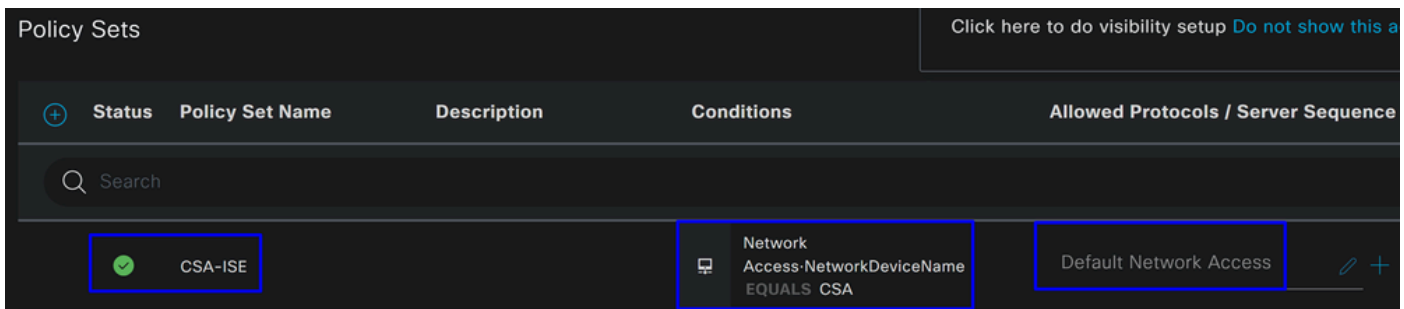
- Per creare le Condizioni, fare clic su Click to add an attribute
- Fare clic sul **Network Device** pulsante
- Sotto le opzioni sottostanti, fare clic su **Network Access - Network Device Name** opzione
- Sotto l'opzione Equals, scrivere il nome del **Network Device** sotto il passaggio [Configure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

- Fare clic su **Save**



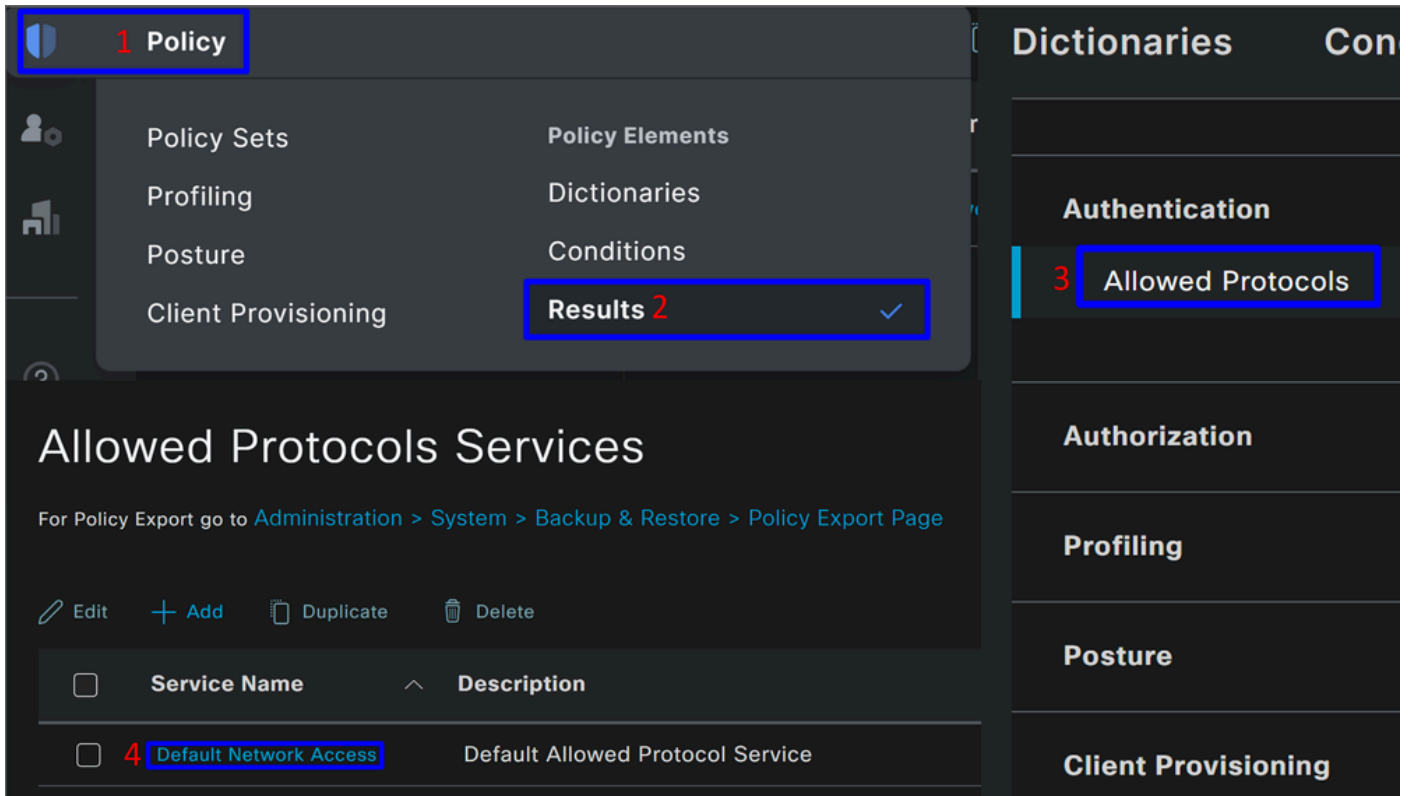
Questo criterio approva solo la richiesta dell'origine CSA di continuare l'installazione **Authentication** e la **Authorization** configurazione in base al set di criteri **CSA-ISE** e verifica i protocolli consentiti in base al **Default Network Access** per i protocolli consentiti.

Il risultato del criterio definito deve essere:



- Per verificare il **Default Network Access Protocols** permesso, procedere con le istruzioni seguenti:

- Fare clic su Policy > Results
 - Fare clic su **Allowed Protocols**
 - Fare clic su **Default Network Access**

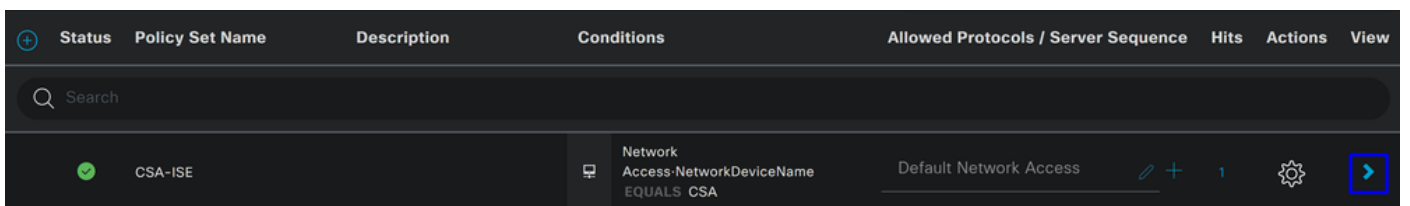


- Quindi, vengono visualizzati tutti i protocolli consentiti su **Default Network Access**

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:

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

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

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:

Authorization Policy(2)

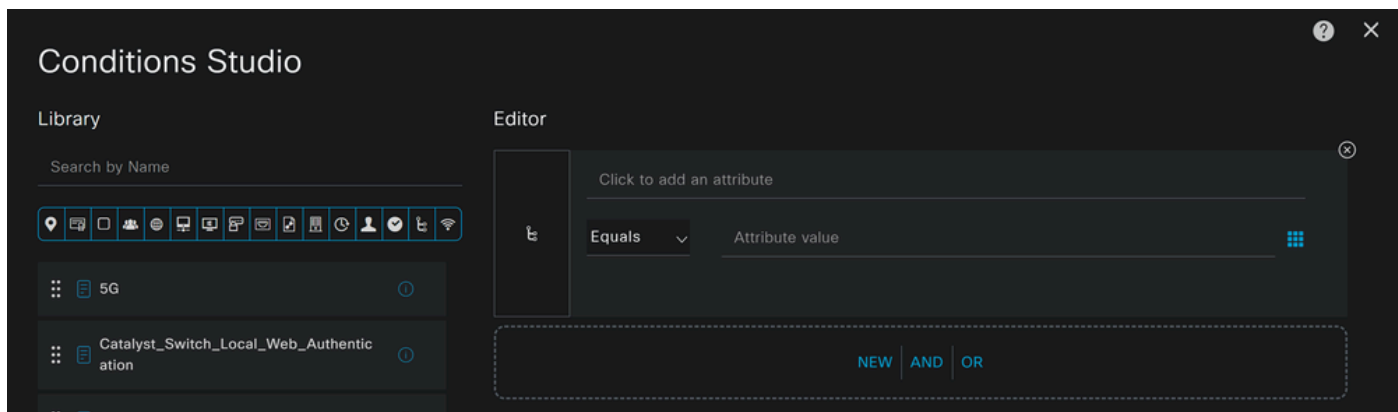
			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Rule 1		Select from list	Select from list
+					
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

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

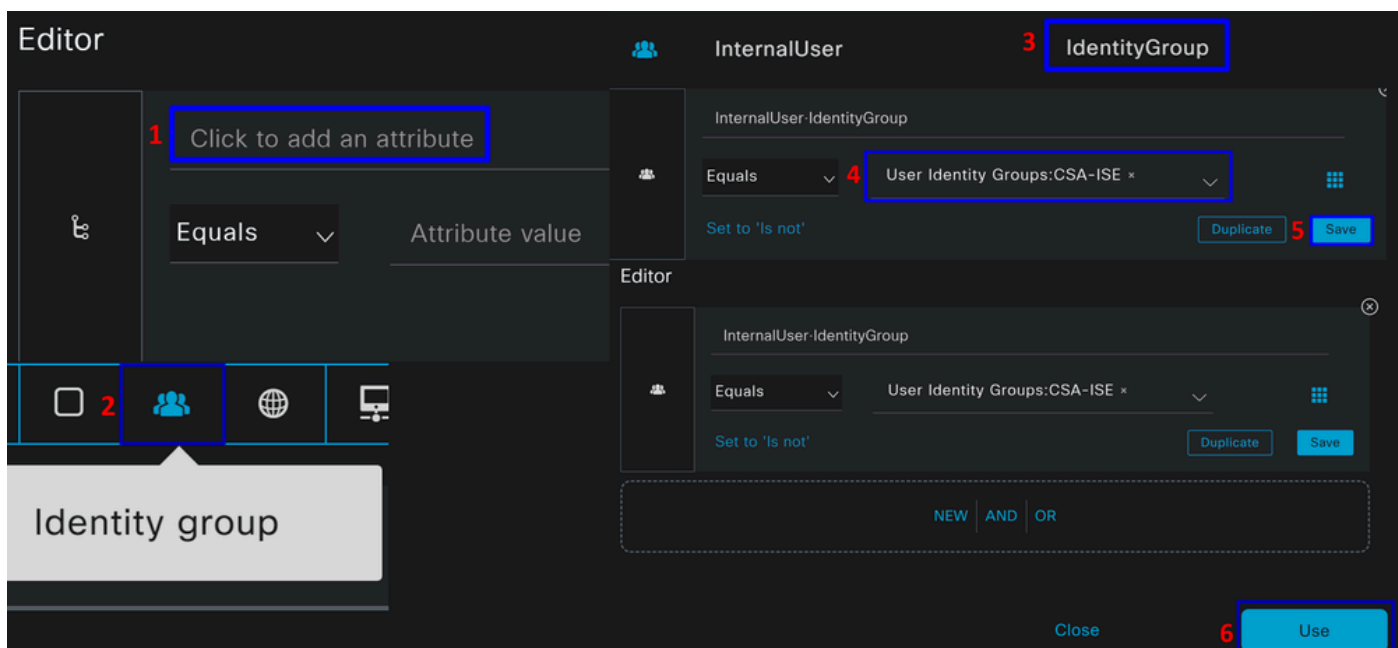
Authorization Policy(2)

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

- 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:

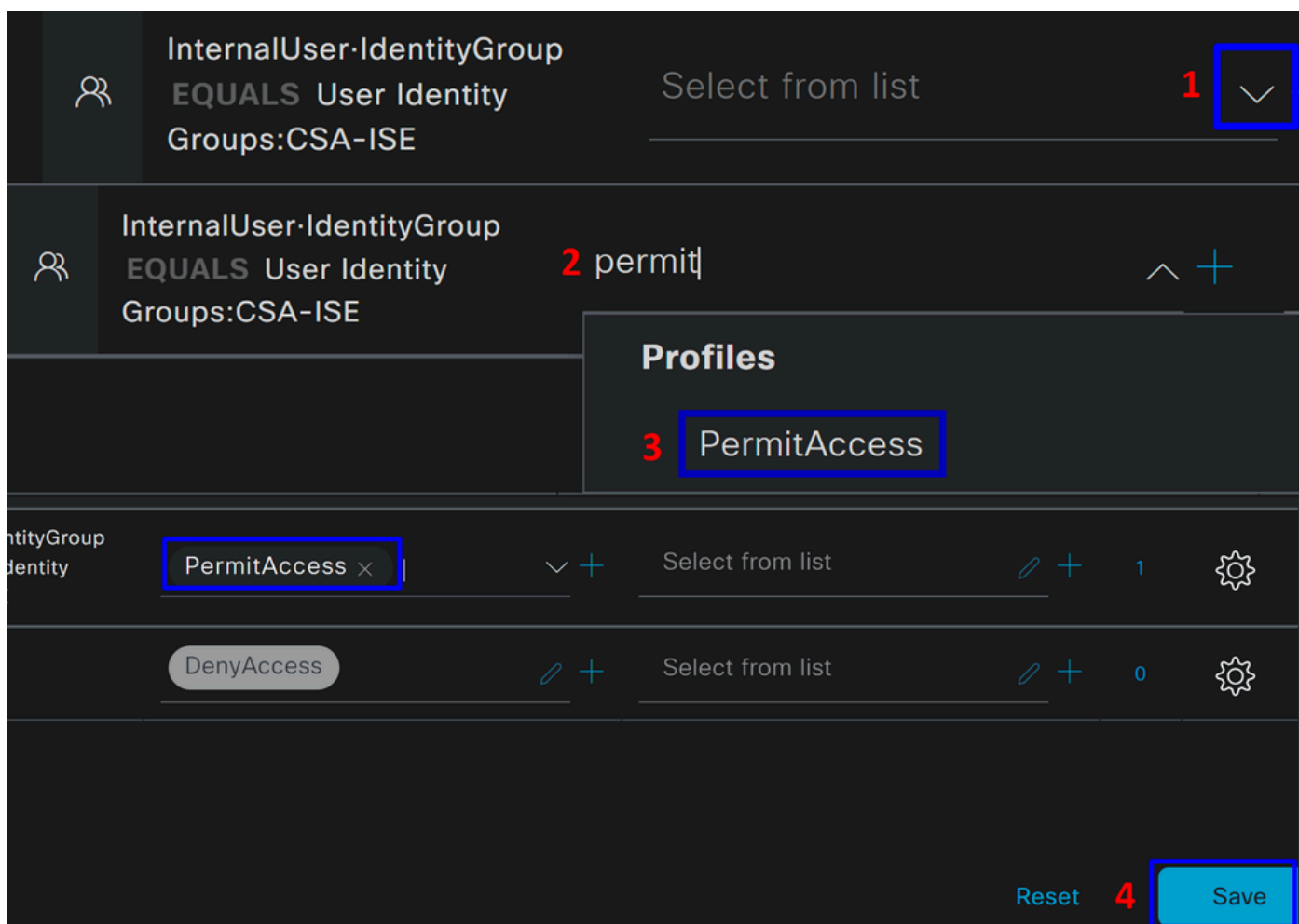


- Per creare le Condizioni, fare clic su Click to add an attribute
- Fare clic sul **Identity Group** pulsante
- Sotto le opzioni sottostanti, fare clic su **Internal User - IdentityGroup** option (Utente interno - opzione)
- Sotto l'**Equals** opzione, utilizzare l'elenco a discesa per trovare il **Group**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





28 Events

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

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

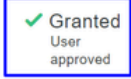
- Passare alla **Cisco ISE Dashboard**

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

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

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

- Passare al [Pannello Duo Admin](#)
- Fare clic su **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

Configura utenti locali o di Active Directory Radius

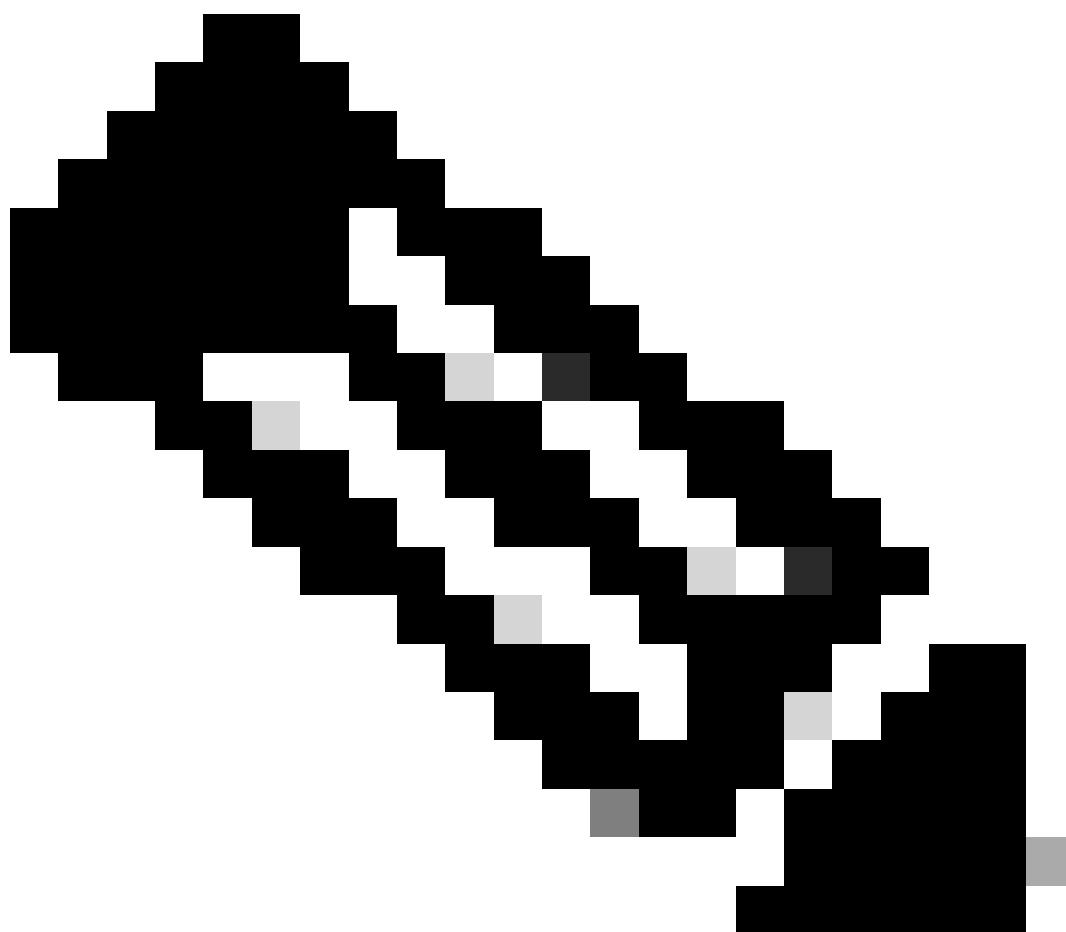
Configurazione della postura ISE

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.

The image shows two side-by-side screenshots of the 'Anti-Malware Condition' configuration interface. The left screenshot shows the default configuration: Name is empty, Description is empty, Compliance Module is '4.x or later', Operating System is 'Select Operating System', and Vendor is 'ANY'. The right screenshot shows a specific configuration: Name is 'CSA-Antimalware', Description is empty, Compliance Module is '4.x or later', Operating System is 'Windows All', and Vendor is 'Cisco Systems, Inc.'. Arrows indicate the mapping of fields between the two configurations. At the bottom of each configuration, there are radio buttons for 'Check Type', with 'Installation' selected in both.

- **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.

Baseline Condition Advanced Condition

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

2

	Product Name	Minimum Version	Maximum Version	Minimum Complia
<input type="checkbox"/>	ANY	ANY	ANY	N/A
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
<input type="checkbox"/>	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

3

Save Reset

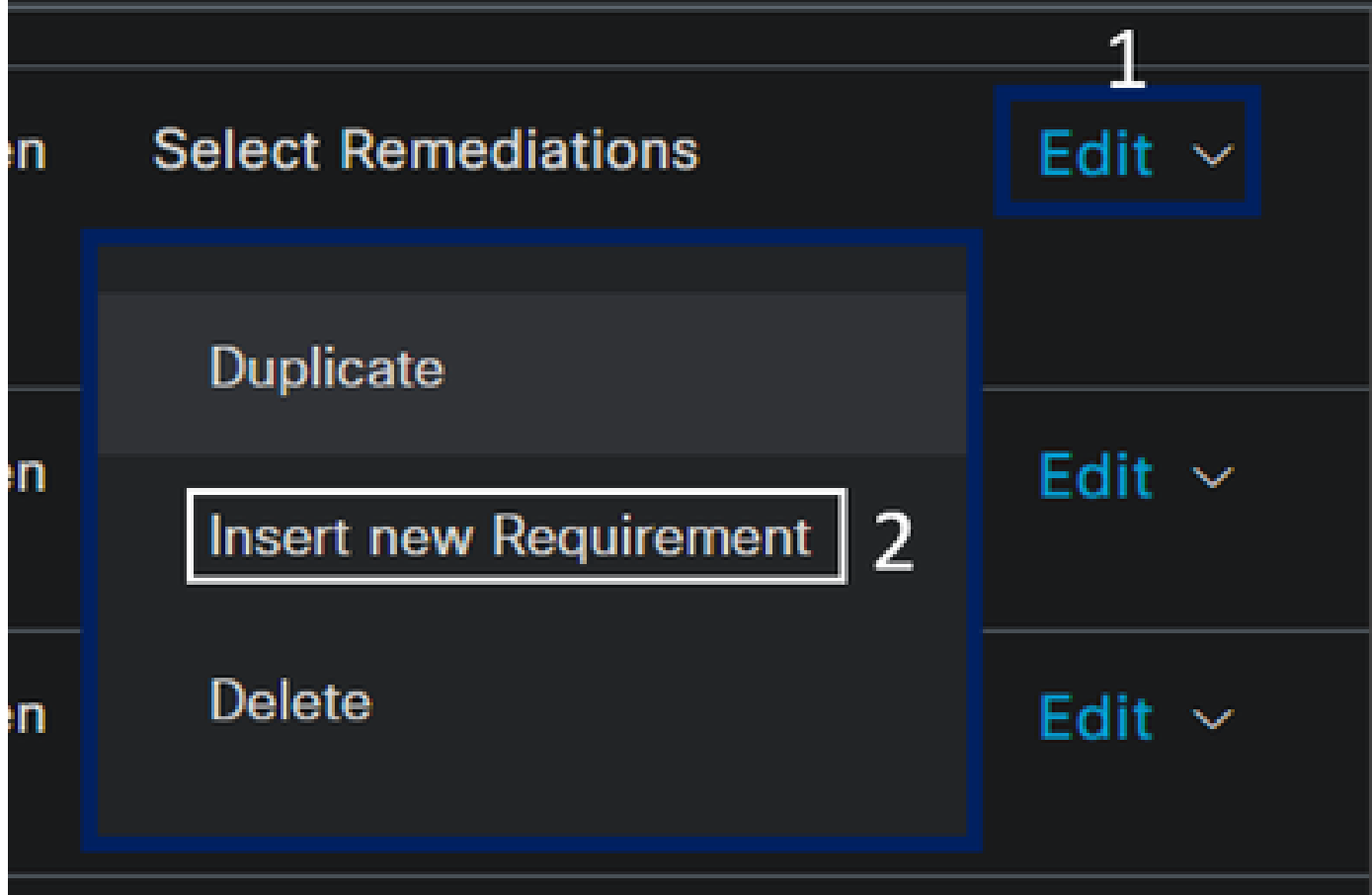
- Selezionare la casella di controllo relativa alle condizioni che si desidera valutare
- Configurare la versione minima da verificare
- Fare clic su Salva per continuare con il passaggio successivo

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**

Remediations Actions



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

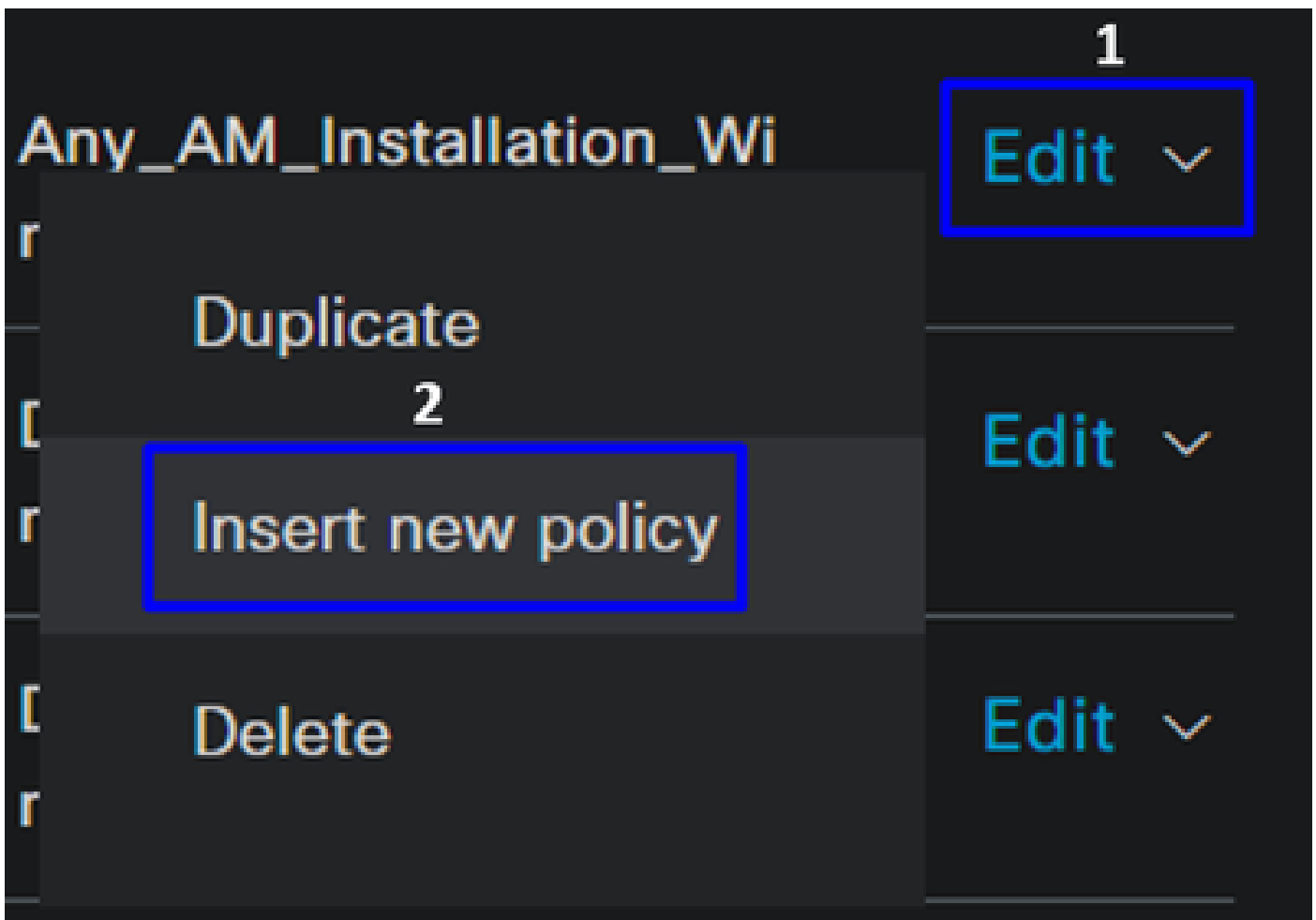
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
CSA-ANTIMALWARE	for Windows All	using 4.x or later	using Agent	met if CSA-Antimalware then	Message Text Only Edit ▾

- **Name:** 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	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	CSA-Windows-Posture	If Any	and Windows All	and 4.x or later	and Agent	and	then CSA-ANTIMALWARE

- **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:

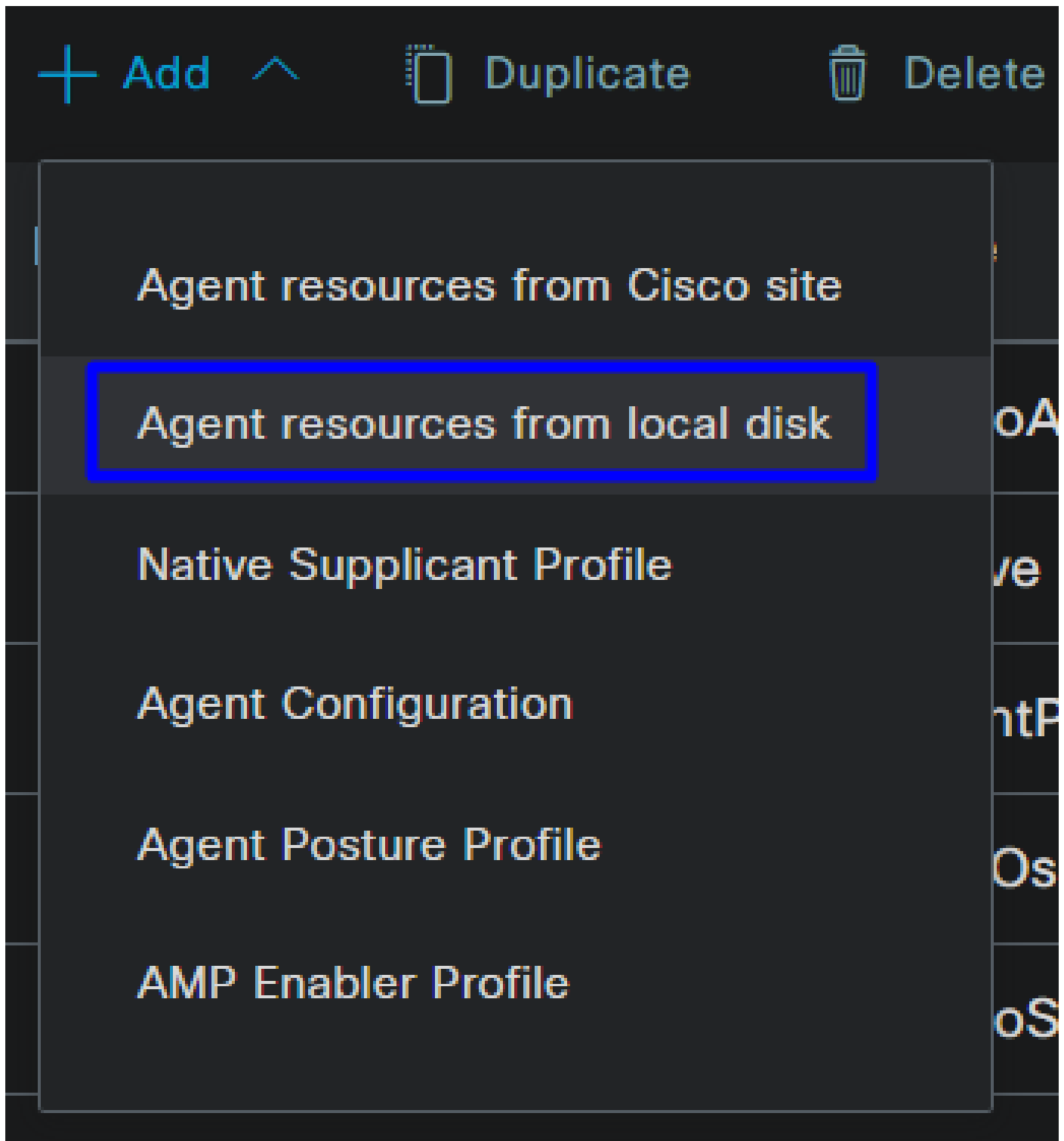
Risorse da configurare	Descrizione
1. Agent Resources	Pacchetto di provisioning Web client sicuro.
2. Compliance Module	Cisco ISE Compliance Module
3. Agent Profile	Controllo del profilo di provisioning.
3. Agent Configuration	Definire i moduli di cui eseguire il provisioning impostando il portale di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

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

- 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

+ Add ^ Duplicate Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

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

Download Remote Resources

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

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

Cancel

Save

Step 3 Configurare il profilo agente

- Fare clic su + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

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

Agent Posture Profile

Name *



Description:

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

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 Configurazione dell'agente

- Fare clic su + Add > Agent Configuration

+ Add ^

📱 Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- Quindi, configurare i parametri successivi:

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

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

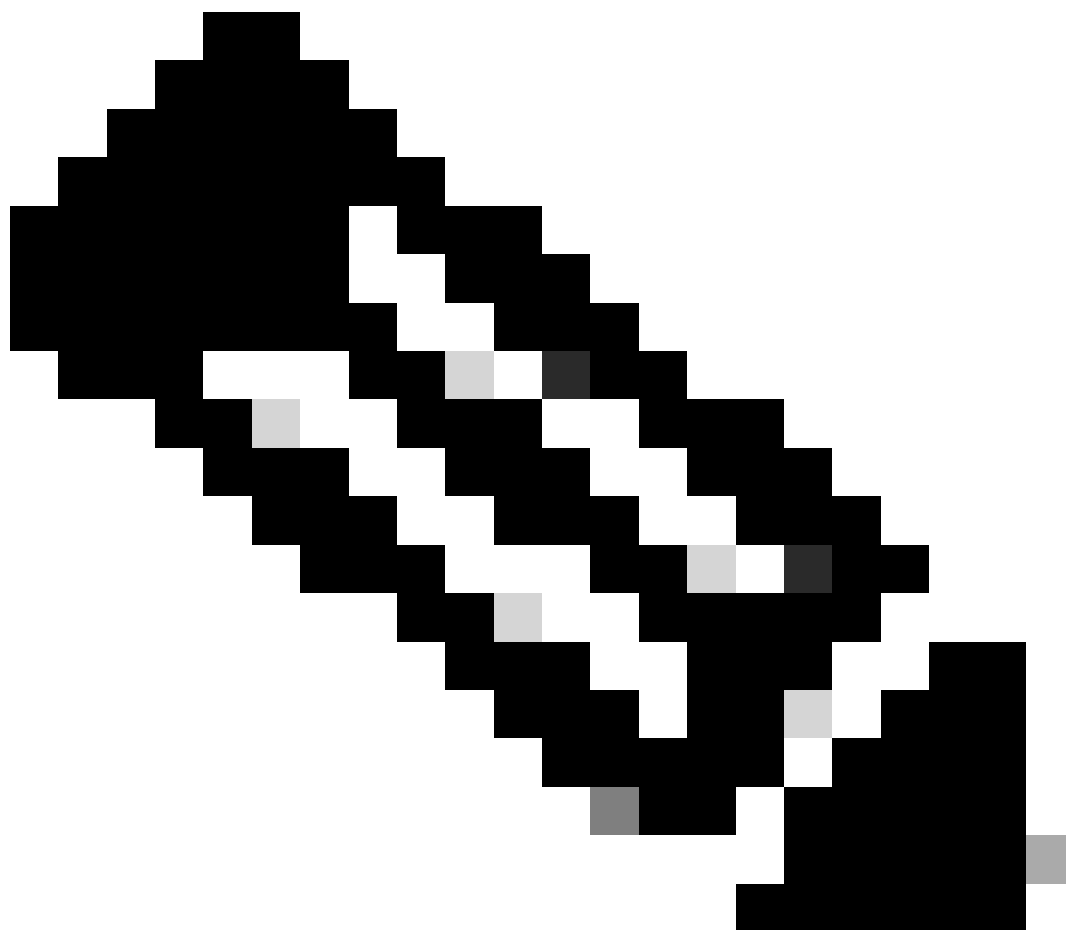
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- Select Agent Package : 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](#)

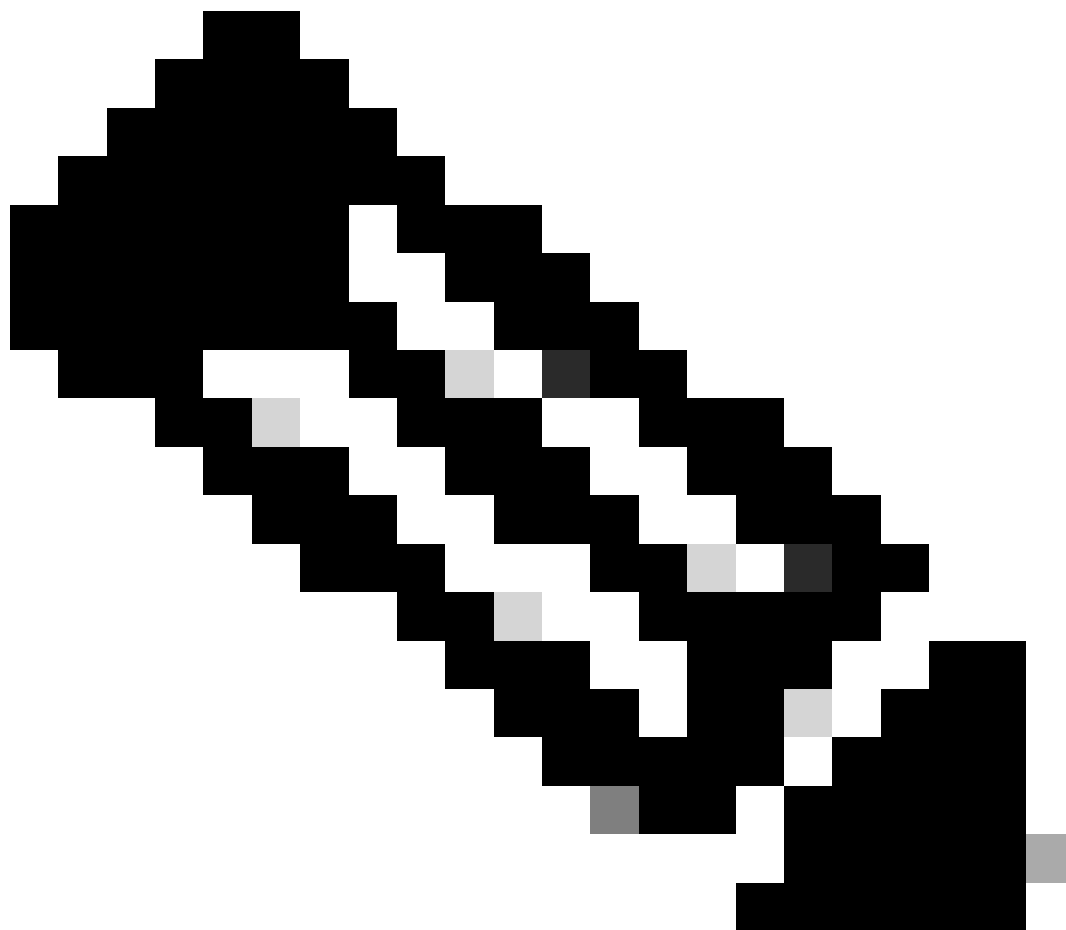
- Fare clic su **Save**



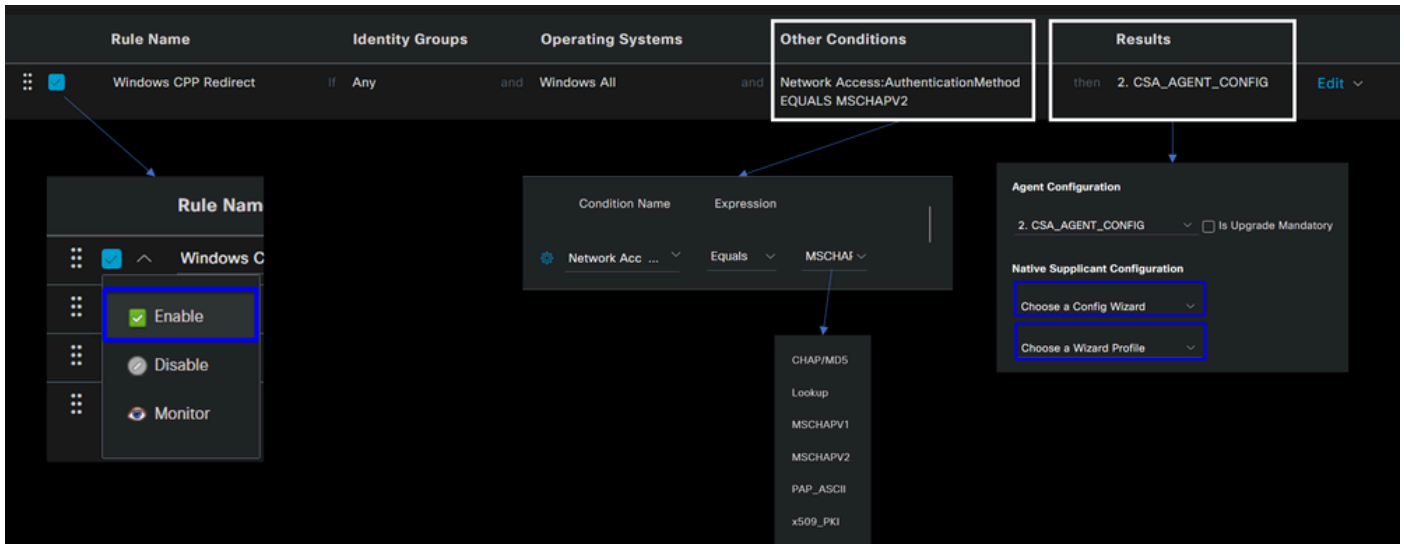
Nota: si consiglia che ogni sistema operativo, Windows, Mac OS o Linux, disponga di una configurazione client indipendente.

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 Wizard e 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 **CSA-Compliant**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0444040	

- **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**

Description

IP version IPv4 IPv6 Agnostic (i)

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

- **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

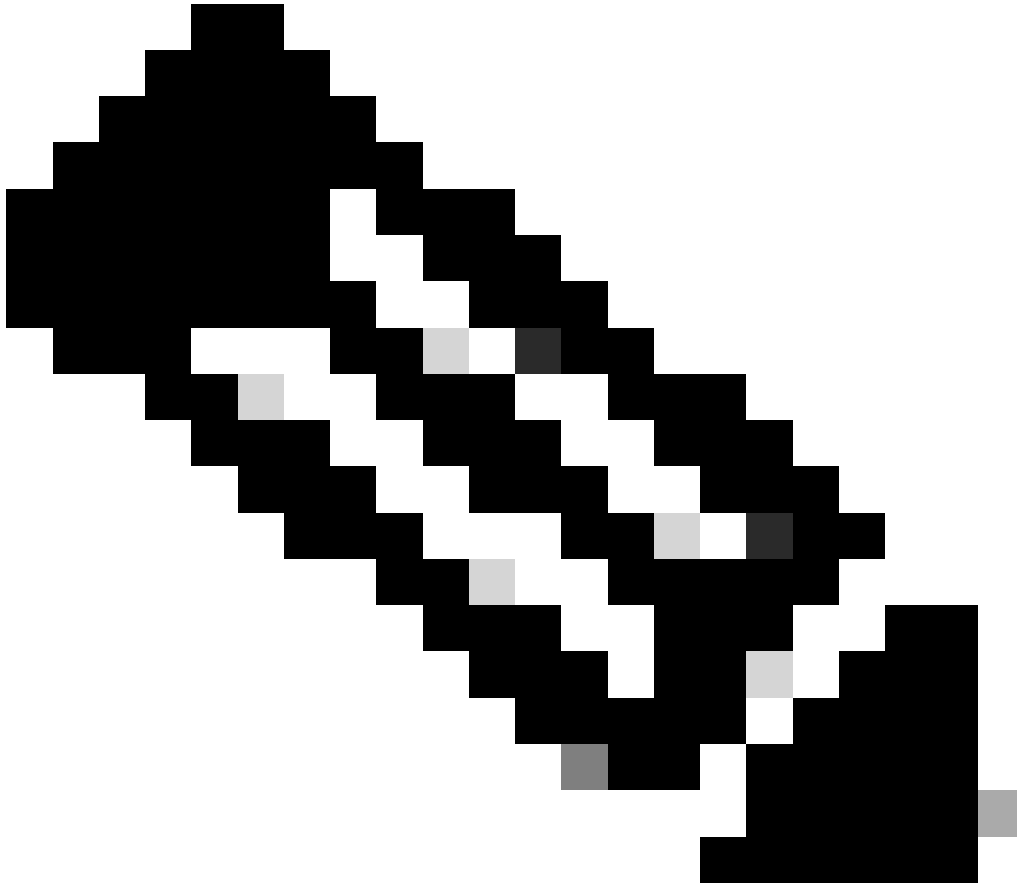
```

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**

Authorization Profile

* Name

CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile



Cisco



Service Template

Track Movement



Agentless Posture



Passive Identity Tracking



✓ Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL ID (Filter ID)

- **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** 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:** 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.

Attributes Details

Access Type = ACCESS_ACCEPT

DAACL = CSA_Redirect_To_ISE

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=

&action=cpp

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

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

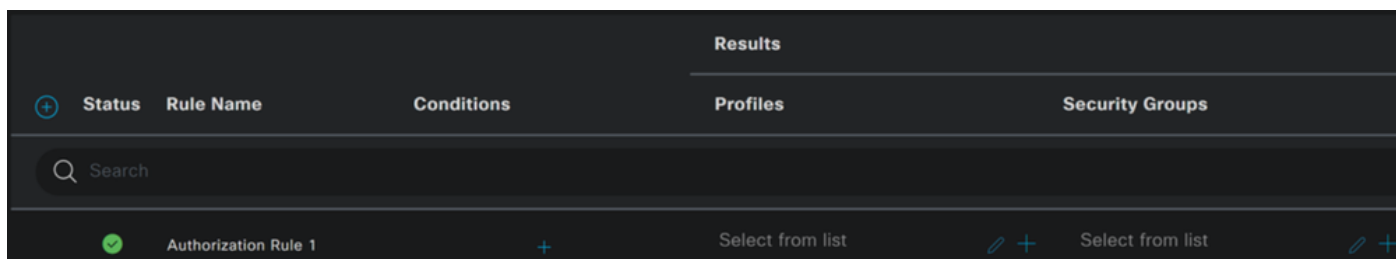
- Fare clic sul pulsante Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🟢	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370
<ul style="list-style-type: none"> > Authentication Policy(2) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions > Authorization Policy(4) 					

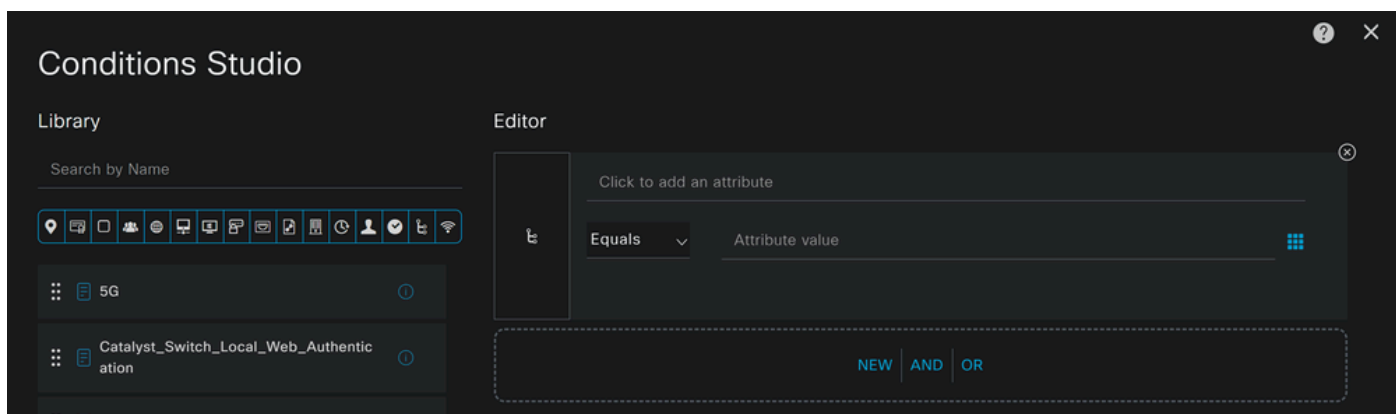
- Creare i tre criteri successivi nell'ordine seguente:

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

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

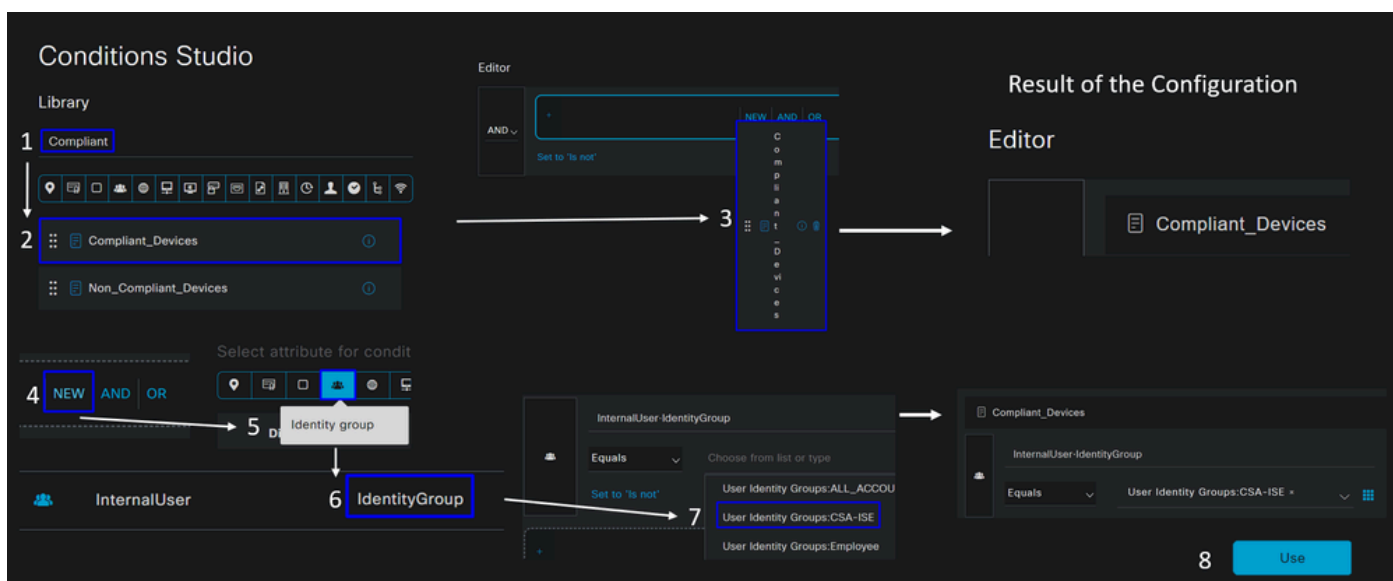


- Per il passo successivo, modificare le Rule Name, Conditionse Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:

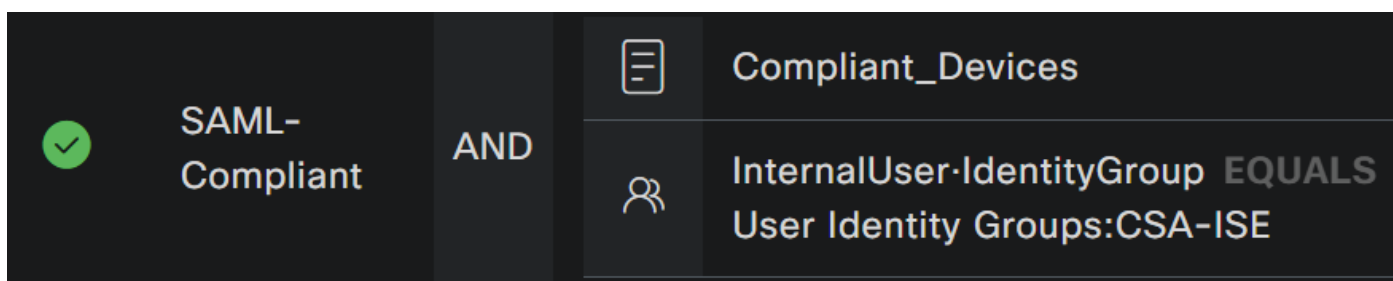


- Per creare la condizione, cercare **compliant**
- È necessario aver visualizzato **Compliant_Devices**
- Trascinare e rilasciare sotto **Editor**

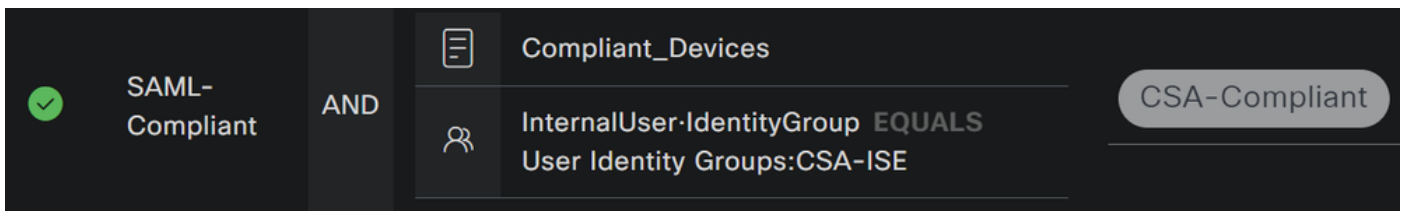
- Fare clic sotto la casella Editor in **New**
- Fare clic sull'**Identity Group** icona
- Scegli **Internal User Identity Group**
- In **Equals**, scegliere il **User Identity Group** tipo di corrispondenza
- Fare clic su **Use**



- Di conseguenza, si otterrà l'immagine successiva

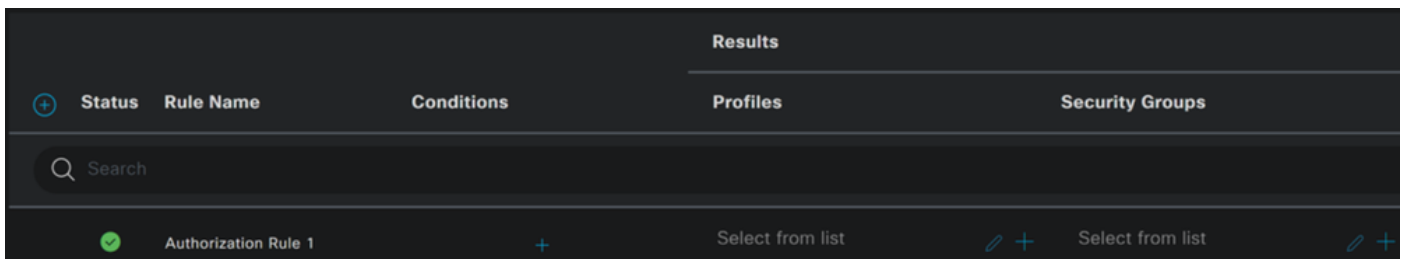


- In fare **Profile** clic sotto il pulsante a discesa e scegliere il profilo autorizzazione reclamo configurato nella fase, [Profilo](#)

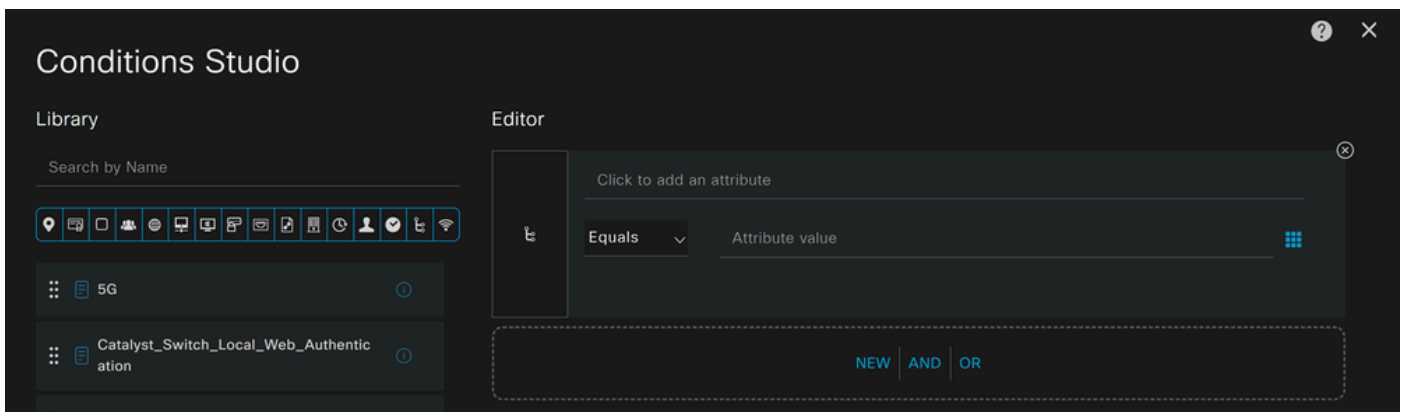


A questo punto è stato configurato il **Compliance Policy Setrouter**.

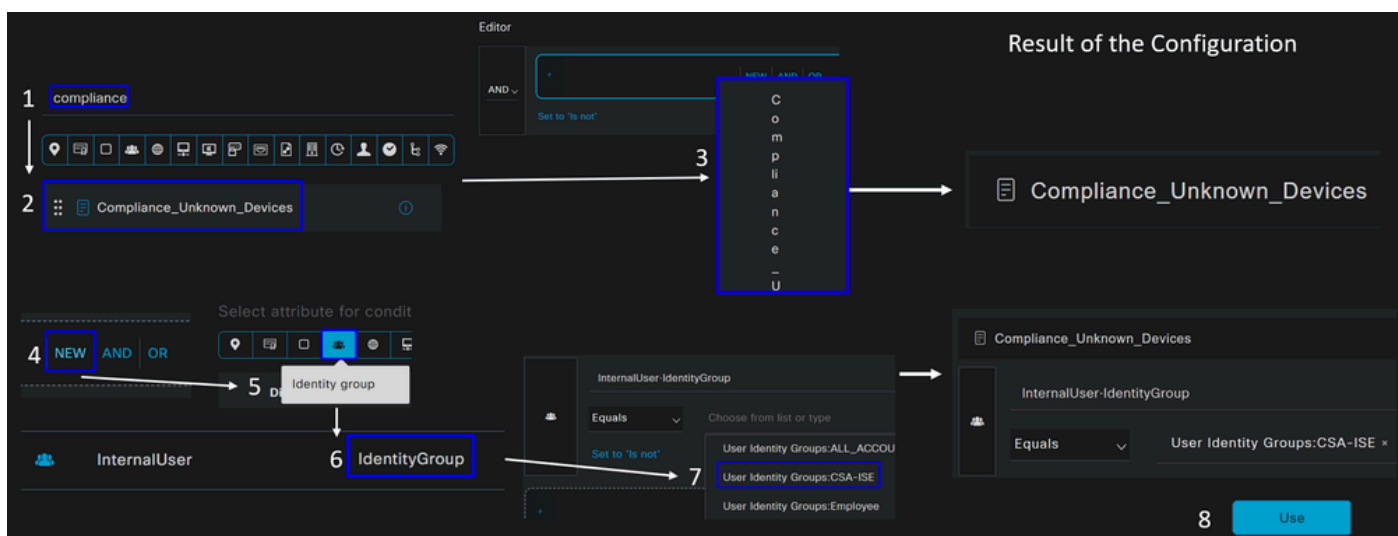
- Fare clic per definire + il **CSA-Unknown-Compliance** criterio:



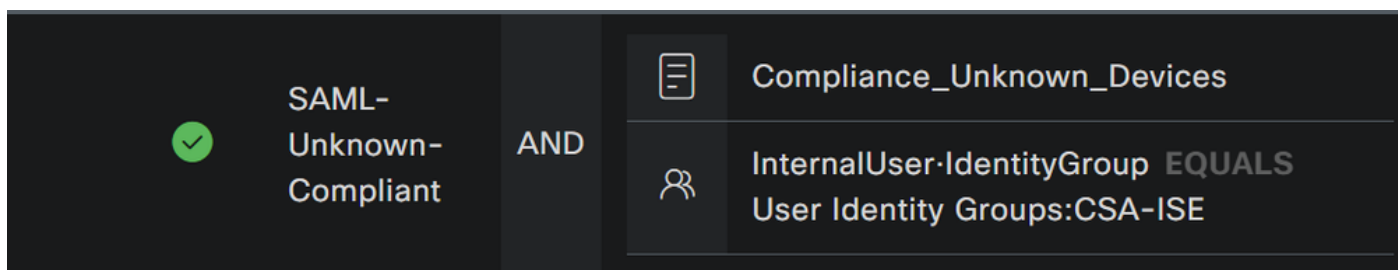
- Per il passo successivo, modificare le Rule Name, Conditionse Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Unknown-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:



- 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**

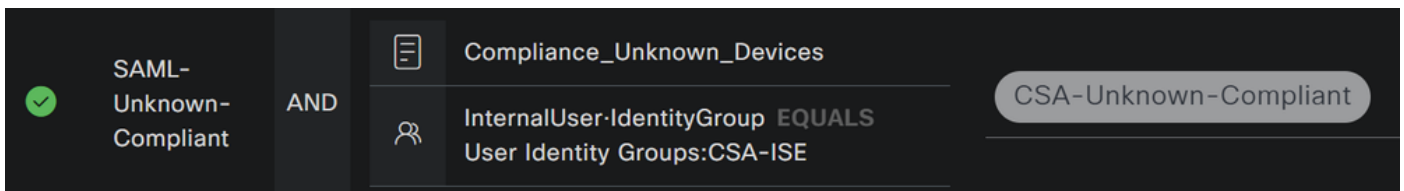


- Di conseguenza, si otterrà l'immagine successiva



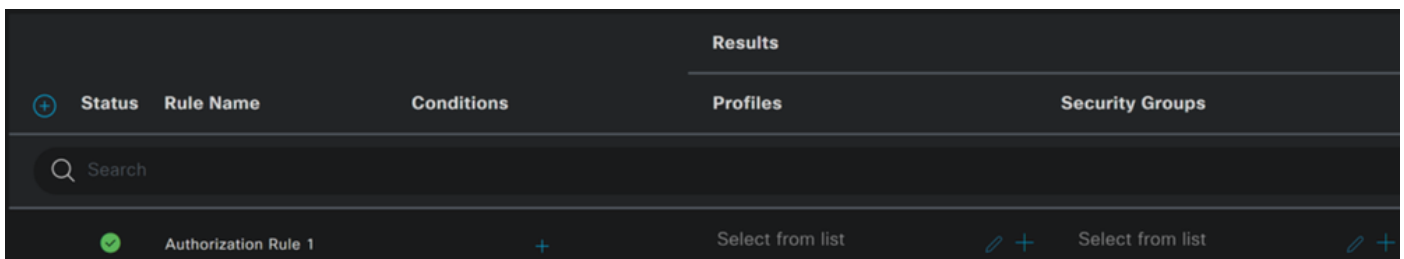
- In fare **Profile** clic sotto il pulsante a discesa e scegliere il profilo autorizzazione reclamo configurato nella fase, [Profilo](#)

[autorizzazione conforme sconosciuto](#)

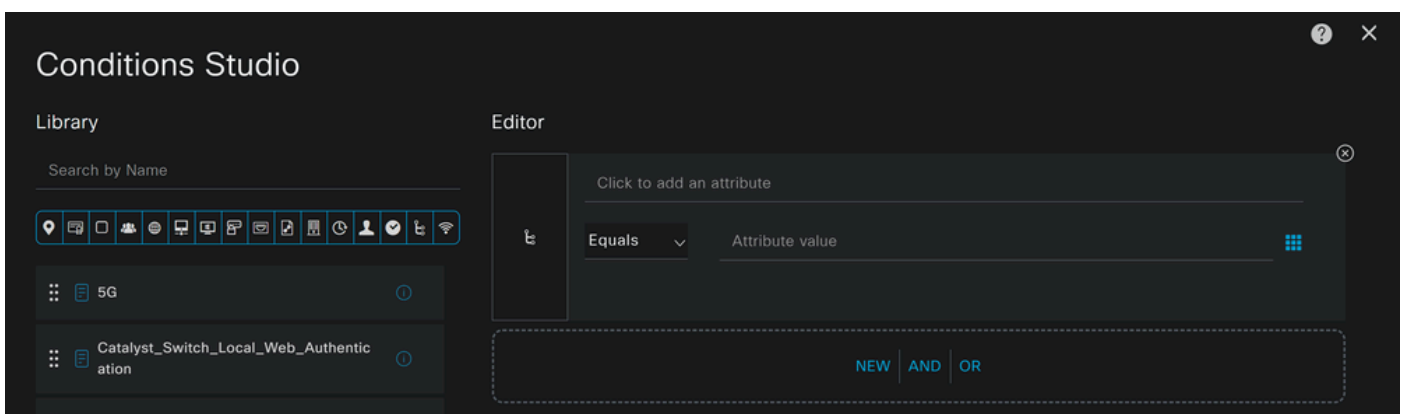


A questo punto è stato configurato il **Unknown Compliance Policy Setrouter**.

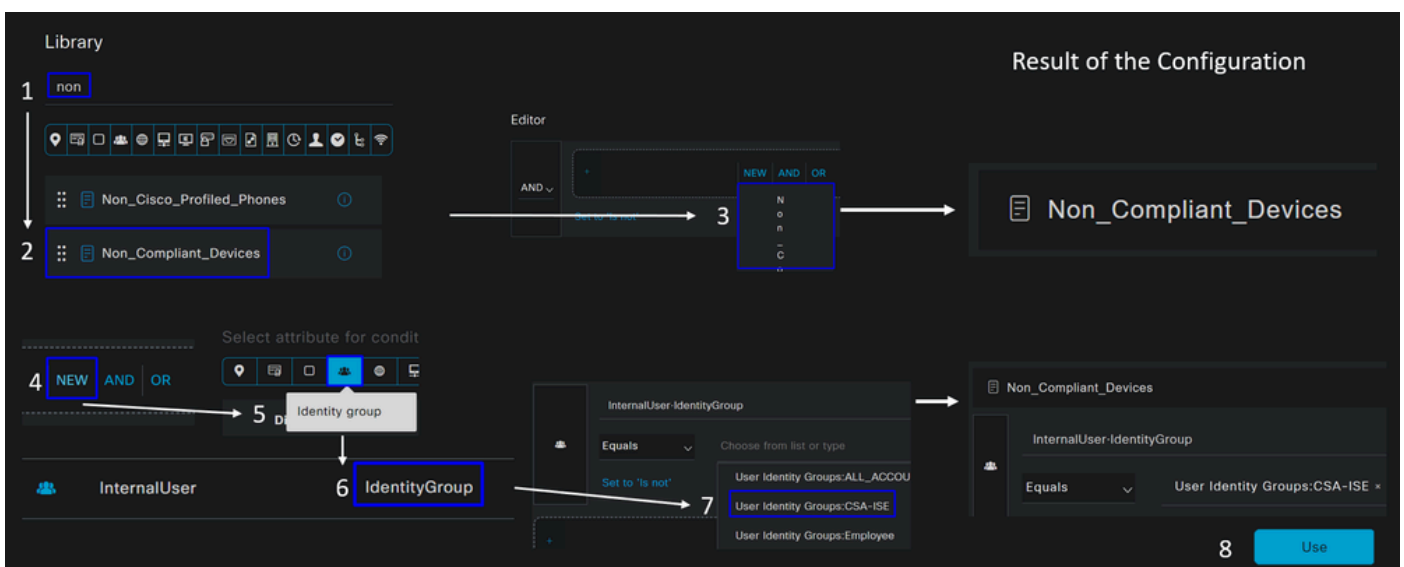
- Fare clic su + per definire la **CSA- Non-Compliant** policy:



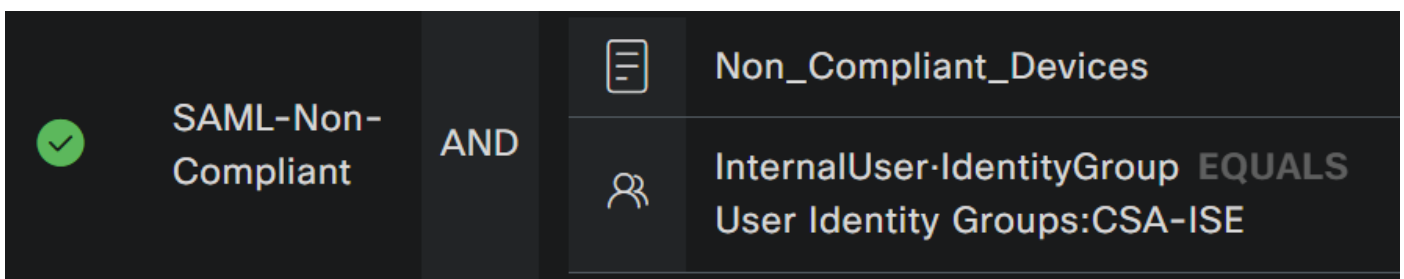
- Per il passo successivo, modificare le Rule Name, Conditione Profiles
- Quando si imposta **Name** Configura un nome su **CSA-Non-Compliance**
- Per configurare la **Condition**funzione, fare clic sul pulsante +
- In **Condition Studio**, sono disponibili le informazioni seguenti:



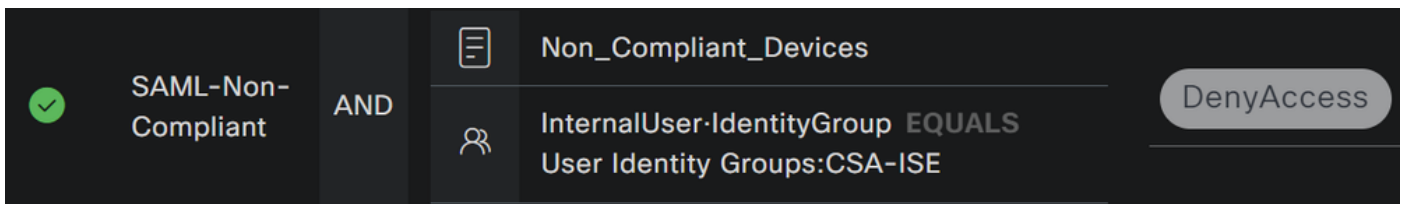
- Per creare la condizione, cercare **non**
- È necessario aver visualizzato Non_Compliant_Devices
- Trascinare e rilasciare sotto **Editor**
- Fare clic sotto la casella Editor in **New**
- Fare clic sull'**Identity Group** icona
- Scegli **Internal User Identity Group**
- In **Equals**, scegliere il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



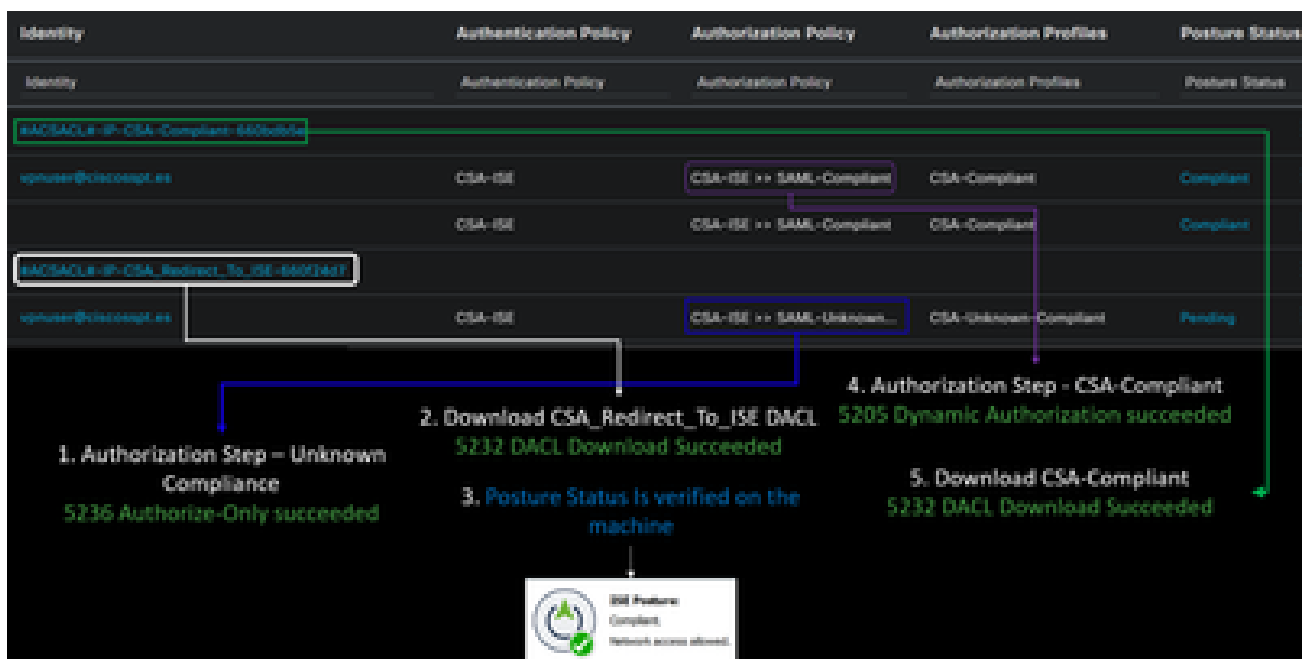
Una volta terminata la configurazione dei tre profili, è possibile testare l'integrazione con la postura.

Verifica

Convalida postura

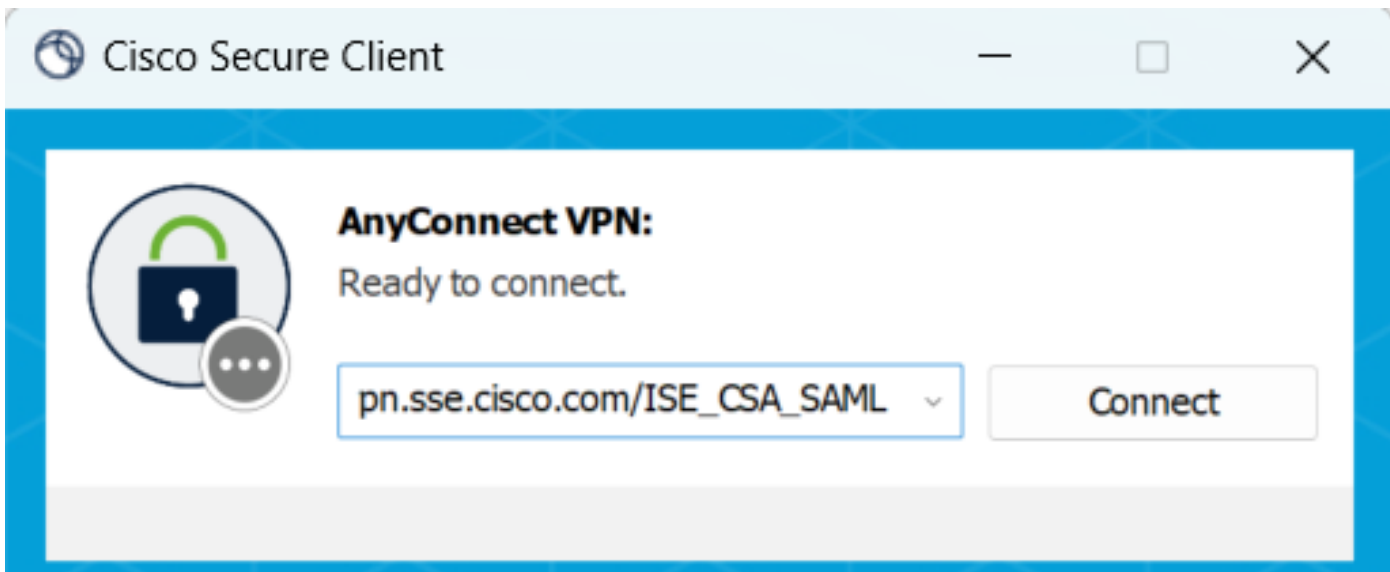
Connessione nel computer

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

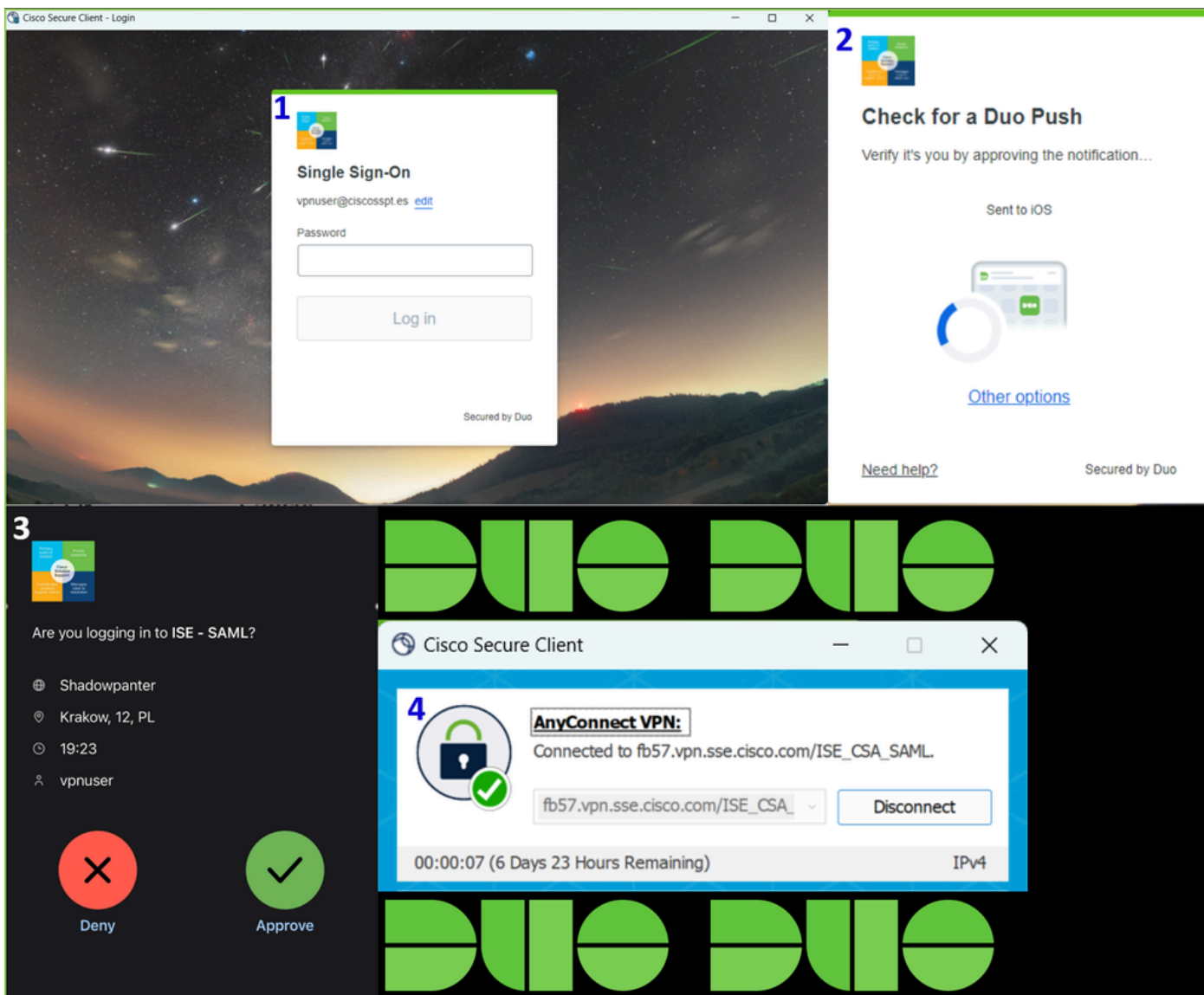


Nota: per questa fase non è necessario installare alcun modulo ISE.

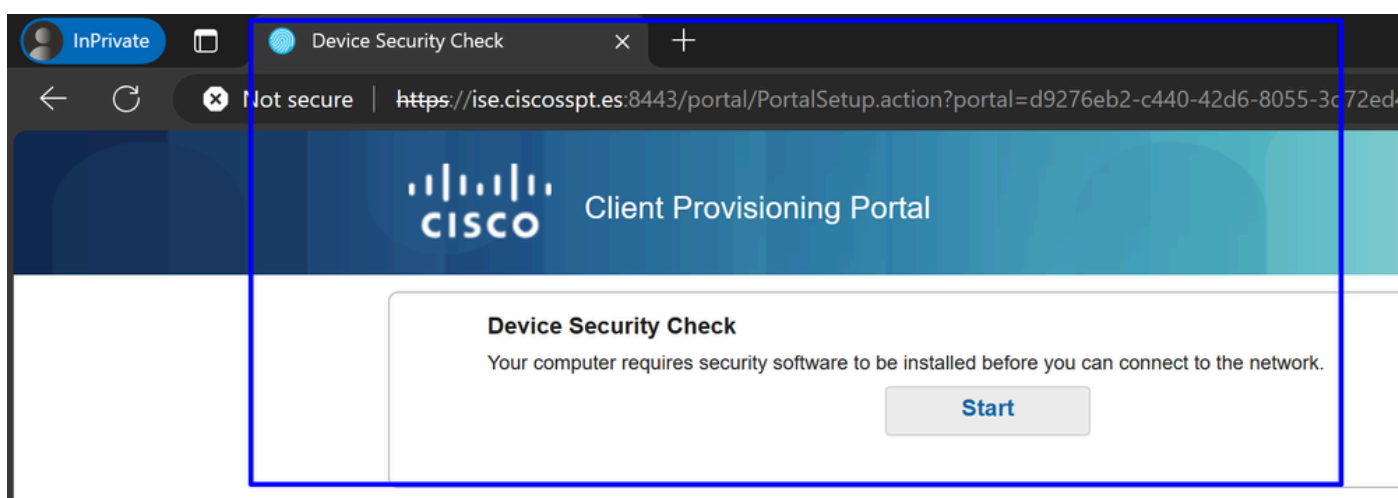
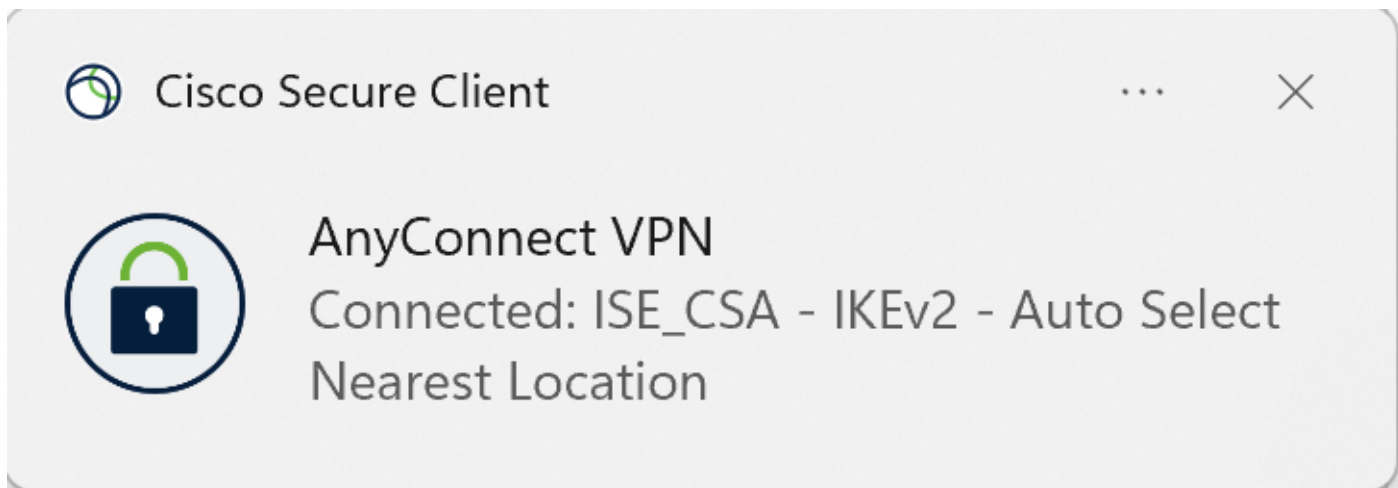
1. Connettersi utilizzando Secure Client.



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://1.1.1.1IOS>.





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.

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. Fare clic su + **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

+ + This is my first time here


+ + Remind me what to do next

6. Fare clic su [Click here to download and install agent](#)

+ This is my first time here

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

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

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

7. Installare l'agente

Downloads



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

[Open file](#)

[See more](#)

Network Setup Assistant



Network Setup Assistant



Installation is completed.

Quit

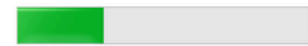
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. 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.



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.

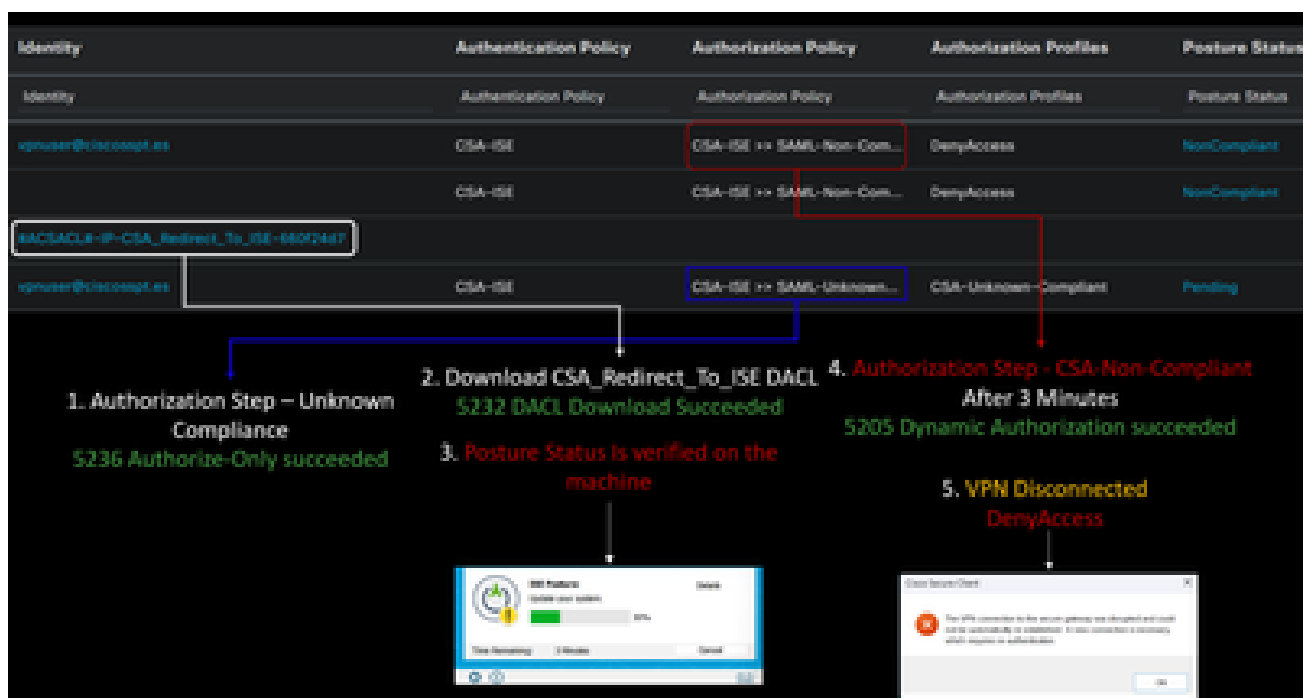
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details

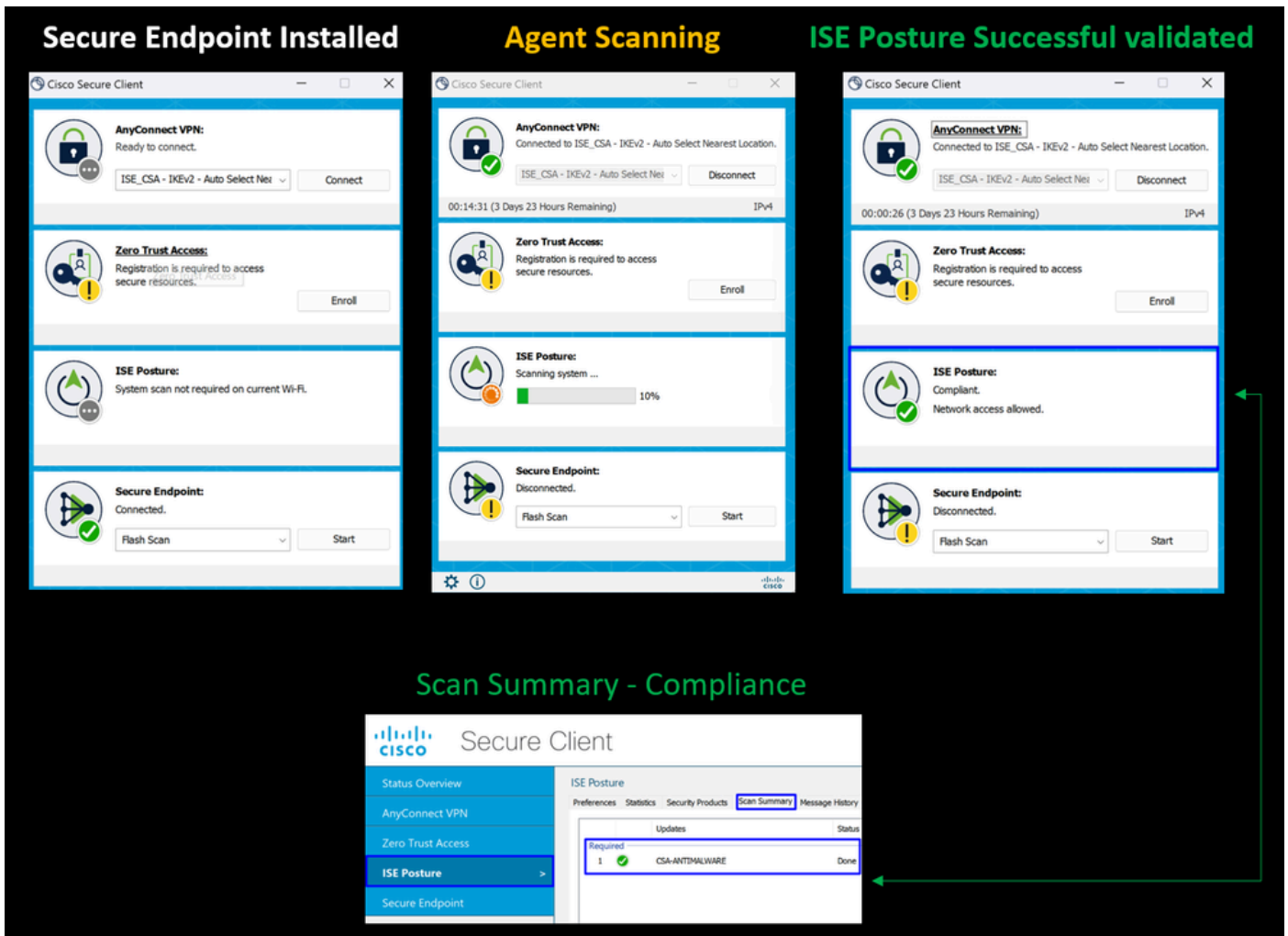


Cancel

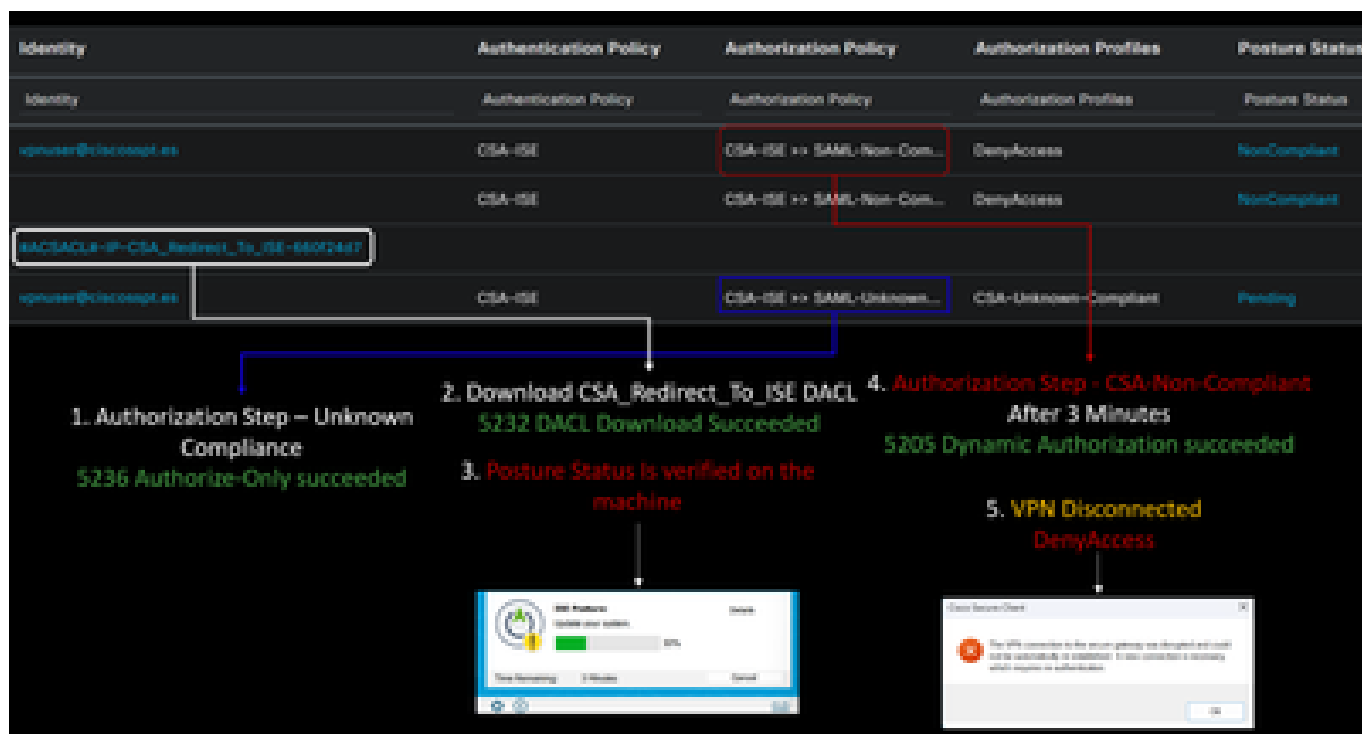


Nota: se Cancel o il tempo rimanente termina, l'utente diventa automaticamente non conforme, rientra nei criteri di autorizzazione impostati [CSA-Non-Compliance](#) e viene immediatamente disconnesso dalla VPN.

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:

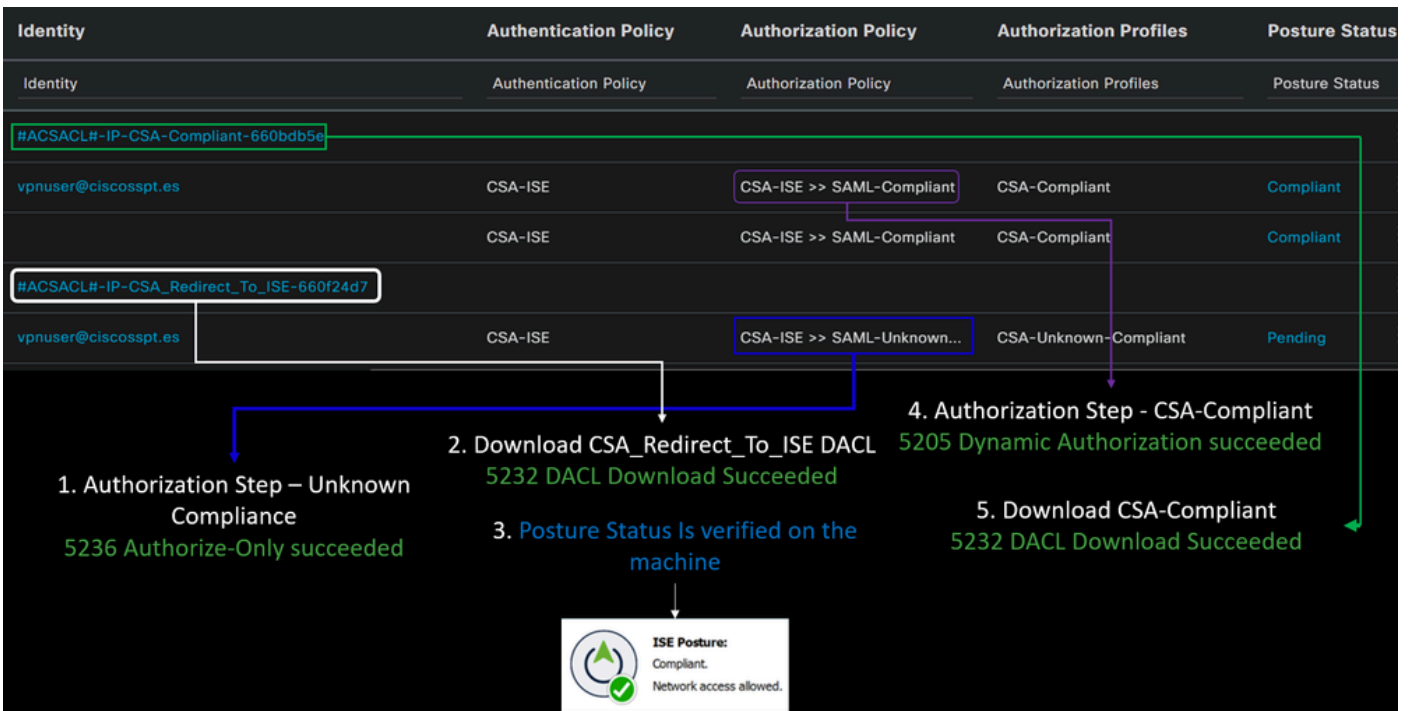
- Passa al dashboard ISE
- Fare clic su Operations > Live Logs

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

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
		#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCon
		vpnuser@ciscospt.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	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia

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

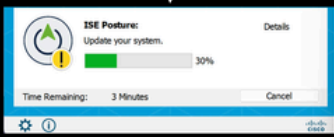

Conformità



Non conformità

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

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**

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

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

Summary



Connected

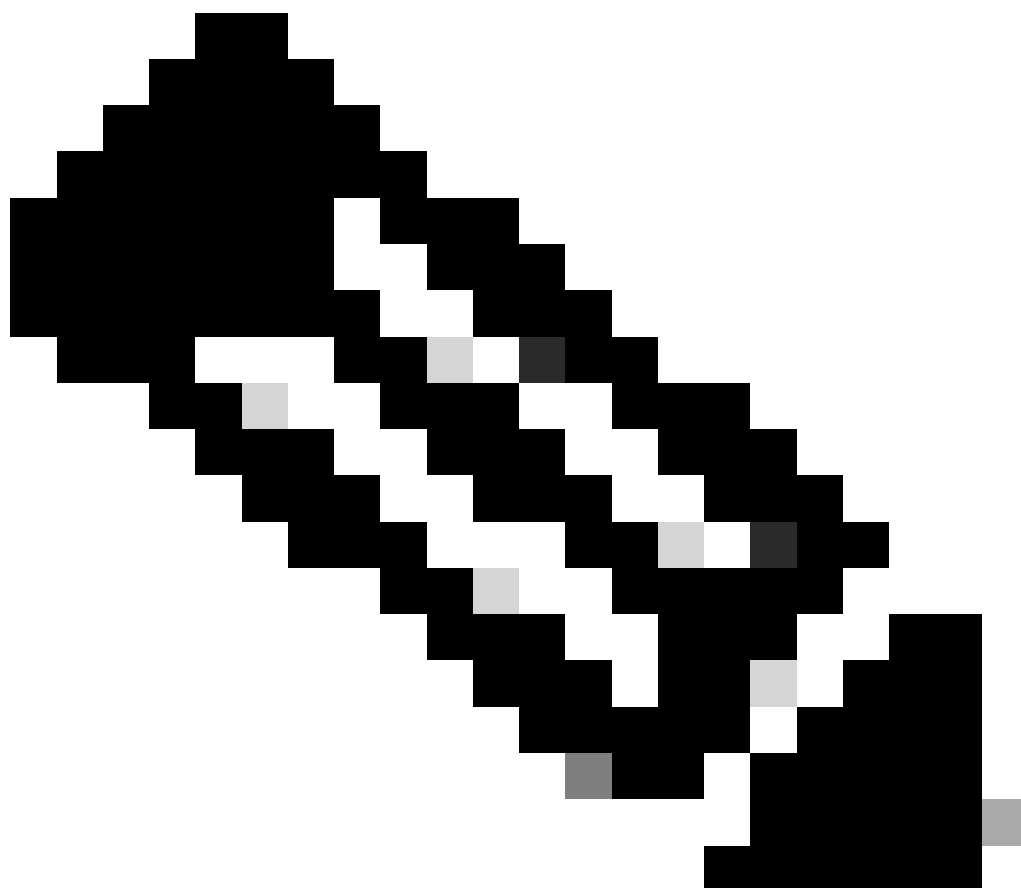
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2: 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.ciscoppt.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**

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	 

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

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

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

[Help](#)

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

[+ Protocol & Port](#)

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ IP Address or FQDN](#)

VPN connections

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

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

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

Endpoint Requirements

For VPN connections:

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

For Branch connections:

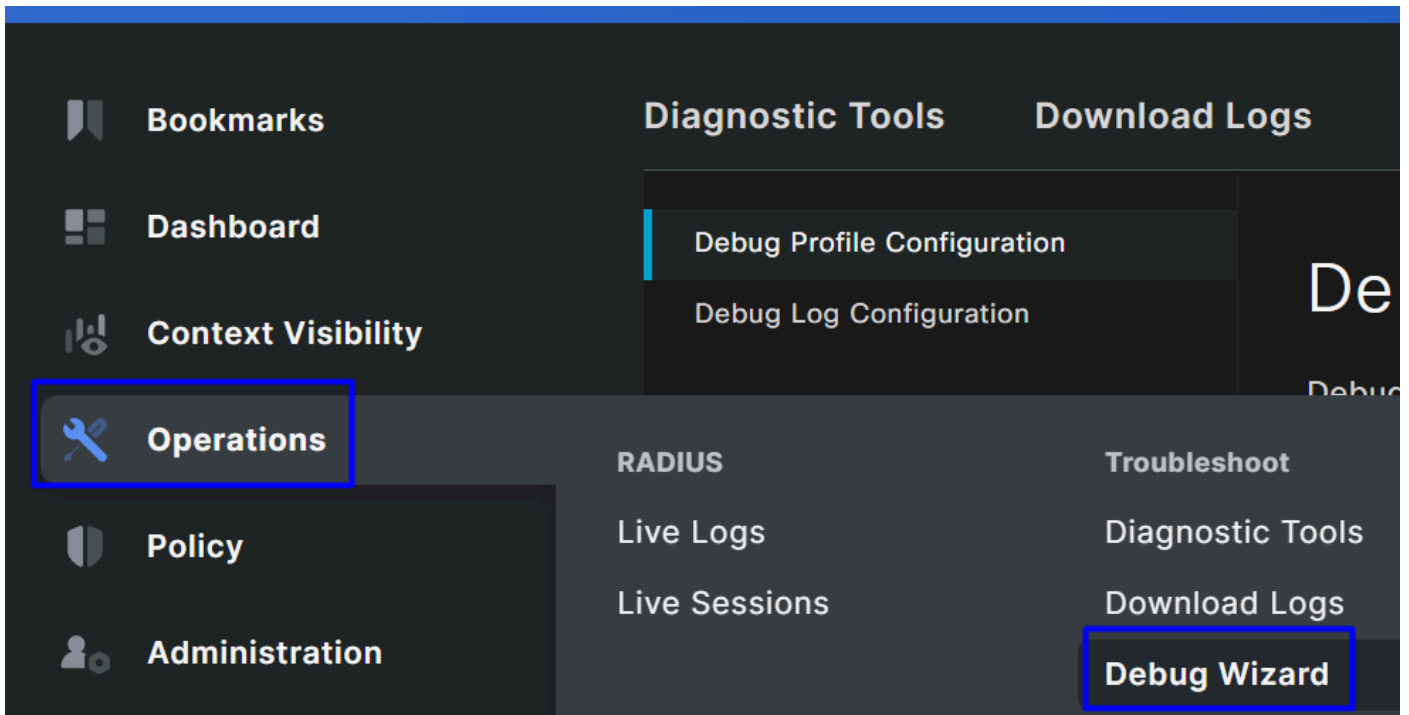
-  Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Risoluzione dei problemi

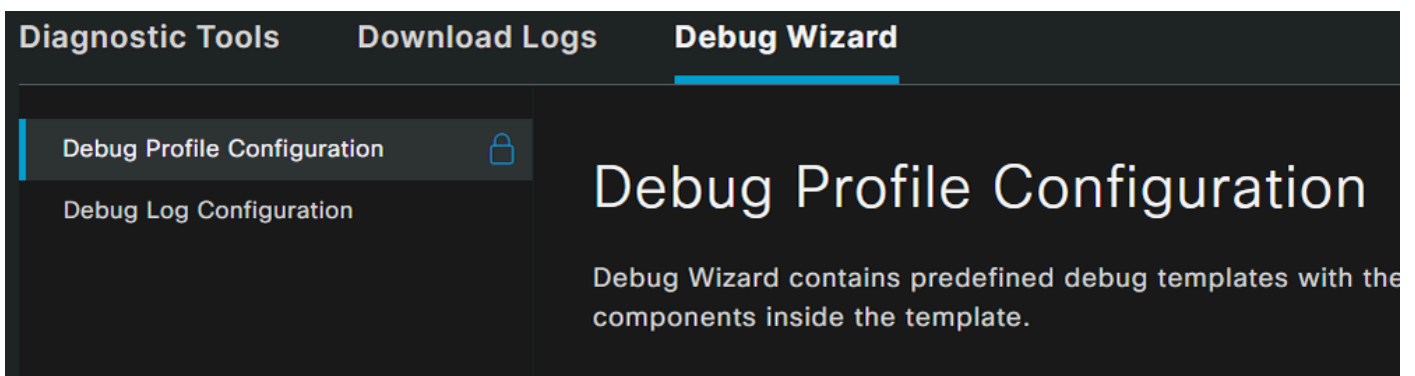
Come scaricare i log di debug di ISE Posture

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

Pos

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

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

Background interface elements include:

- Section header: "Debug V"
- Section header: "Debug Profile Con"
- Section header: "Debug I"
- Text: "Selected profile"
- Text: "Choose on which ISE nodes you want to enable this profile."
- Refresh icon (circular arrow)
- Table with columns "Host Name" and "Persona":

Host Name	Persona
<input checked="" type="checkbox"/> ISE.ciscosspt.es	Administration, Monitoring, Policy Serv

- Fare clic su Save

Debug Nodes

Selected profile Posture

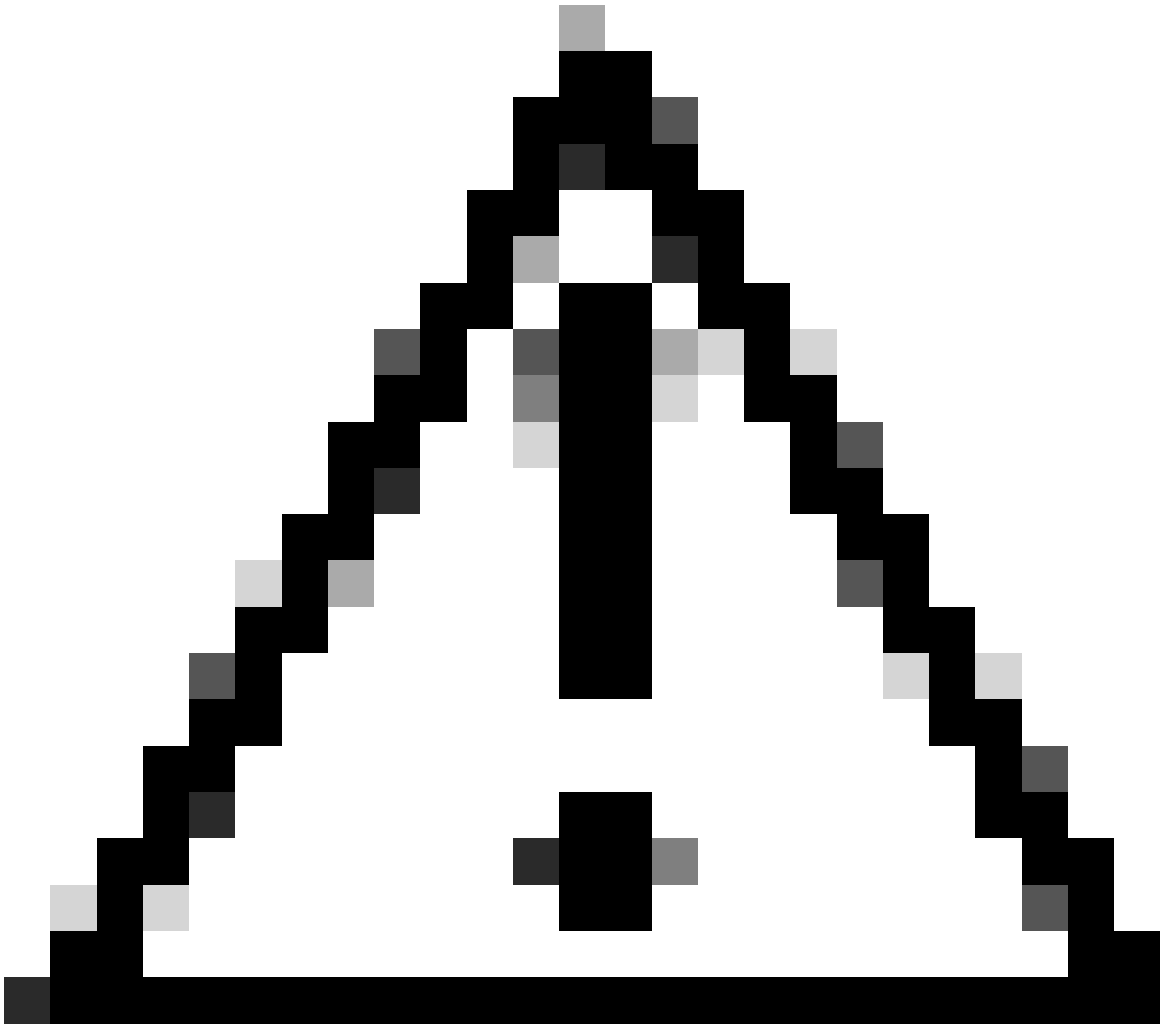
Choose on which ISE nodes you want to enable this profile.

 Filter  

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

Cancel

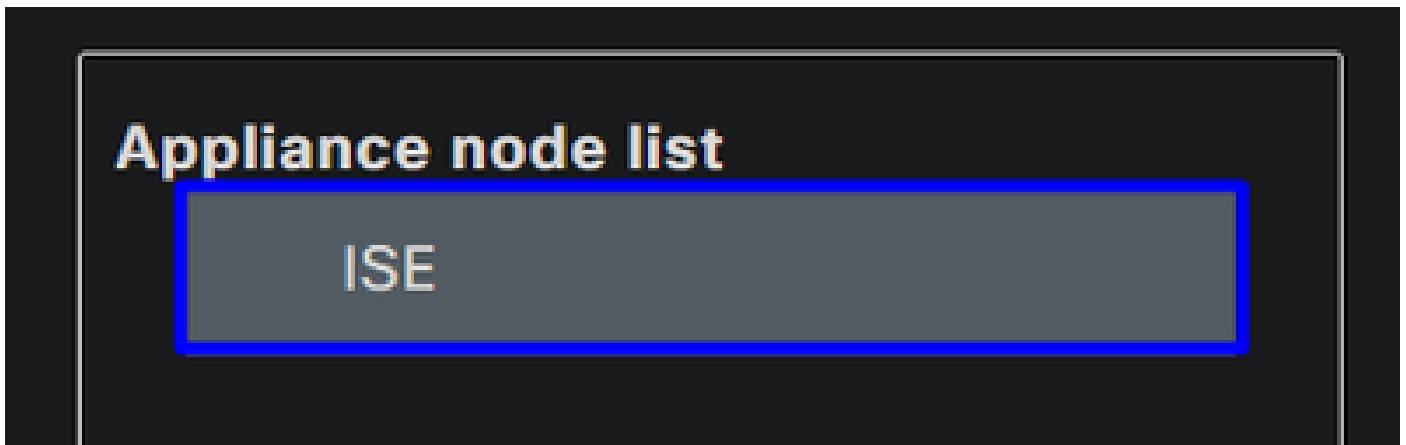
Save



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:

Support Bundle

Debug Logs

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

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

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

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- 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**

Support Bundle - Last Generated

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

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

Size(KB): 52165.0

Download

Delete


















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

100 Events

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

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).