ACL scaricabile negli switch Catalyst 1300

Obiettivo

L'obiettivo di questo articolo è dimostrare il funzionamento del DACL (Access Control List) scaricabile sugli switch Cisco Catalyst 1300 con Cisco Identity Service Engine (ISE).

Dispositivi interessati | Versione software

- Catalyst serie 1300 |4.1.6.54

Introduzione

Gli ACL dinamici sono ACL assegnati a una porta dello switch in base a una policy o a criteri quali l'appartenenza al gruppo di account utente, l'ora del giorno e così via. Potrebbero essere ACL locali specificati da filter-ID o ACL scaricabili (DACL).

Gli ACL scaricabili sono ACL dinamici creati e scaricati dal server Cisco ISE. Applicano in modo dinamico le regole di controllo dell'accesso in base all'identità dell'utente e al tipo di dispositivo. DACL offre il vantaggio di disporre di un repository centrale per gli ACL, in modo che non sia necessario crearli manualmente su ciascuno switch. Quando un utente si connette a uno switch, deve solo autenticarsi e lo switch scarica gli ACL applicabili dal server Cisco ISE.

Casi di utilizzo di ACL scaricabili

1. Utenti diversi riceveranno ACL diversi quando si collegano a uno switch (Utenti ISE locali).
2. Gli utenti con connettività di rete limitata possono accedere a un portale Web centrale per l'accesso completo alla rete (autenticazione Web centrale).
3. Avanzate - uso del MAB (MAC Authentication Bypass) per consentire la comunicazione con Windows Active Directory (AD) e alcuni servizi correlati durante la connessione del server ISE ad AD e il monitoraggio dell'autenticazione utente. Prima dell'accesso ad Active Directory di Windows, la rete consentirà l'accesso solo a risorse molto limitate, ma l'autenticazione AD scaricherà ACL diversi in base ai gruppi Windows e consentirà l'accesso completo alla rete.
4. Avanzate: gli utenti ricevono ACL diversi a seconda del giorno della settimana, dell'ora del giorno o di altri fattori, a causa delle policy sul server ISE.

In questo articolo, il primo caso di utilizzo sarà discusso in dettaglio.

Sommario

- Configura client RADIUS
- Configura autenticazione 802.1x
- Configurazione server Cisco ISE per ACL scaricabili
- Configurazioni client
- Verifica DACL

Prerequisiti

- Accertarsi che lo switch Catalyst 1300 sia aggiornato al firmware più recente (il firmware dello switch deve essere 4.1.6 o superiore).
- Assegnare un indirizzo IP statico allo switch a scopo di gestione.

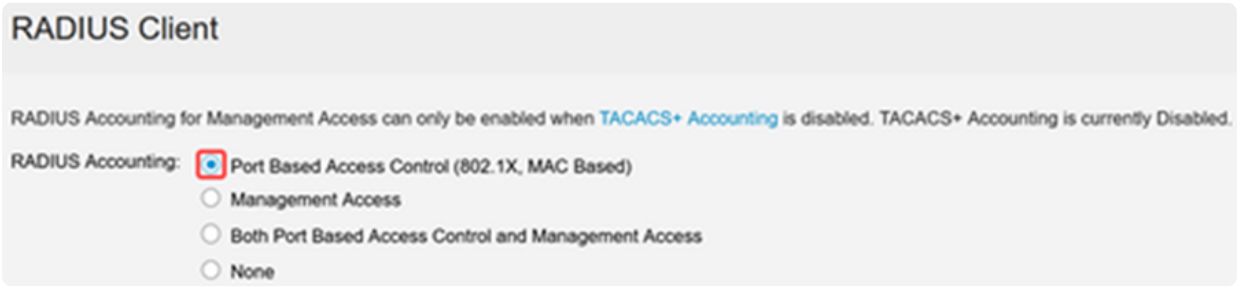
Configura client RADIUS

Passaggio 1

Accedere allo switch Catalyst 1300 e selezionare Security > RADIUS Client menu.

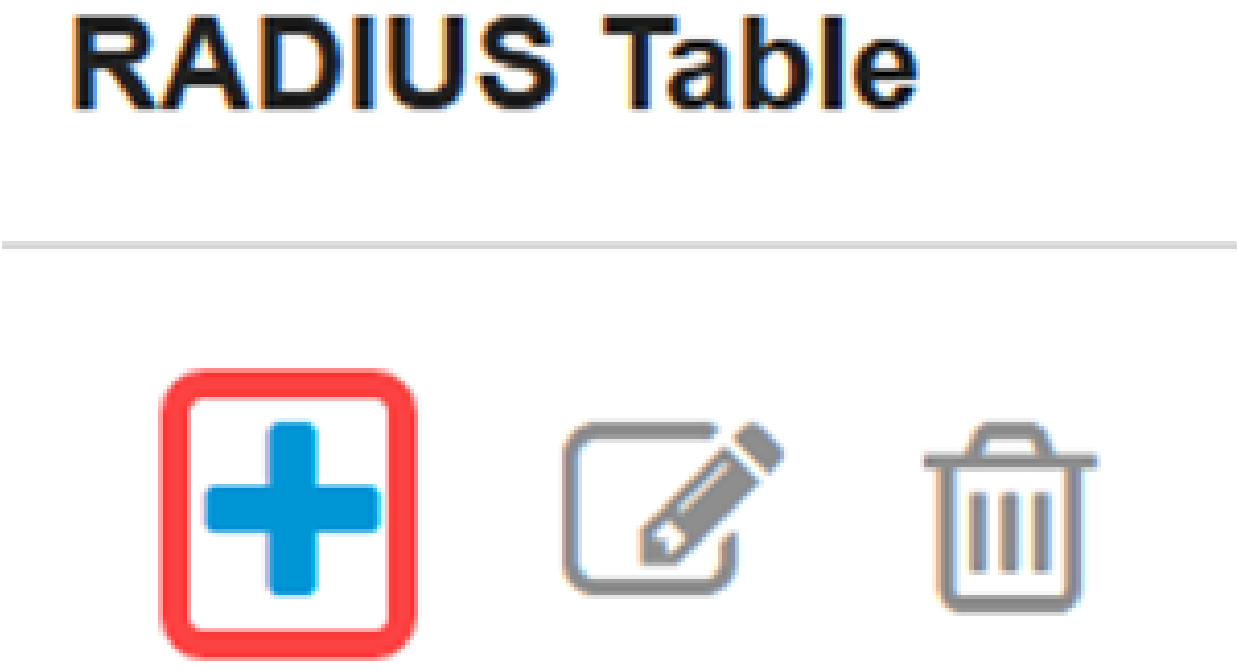
Passaggio 2

Per Accounting RADIUS, selezionare l'opzione Controllo di accesso basato sulla porta.



Passaggio 3

In Tabella RADIUS, fare clic sull'icona più per aggiungere Cisco ISE Server.



Passaggio 4

Immettere i dettagli di Cisco ISE Server e fare clic su Apply (Applica).

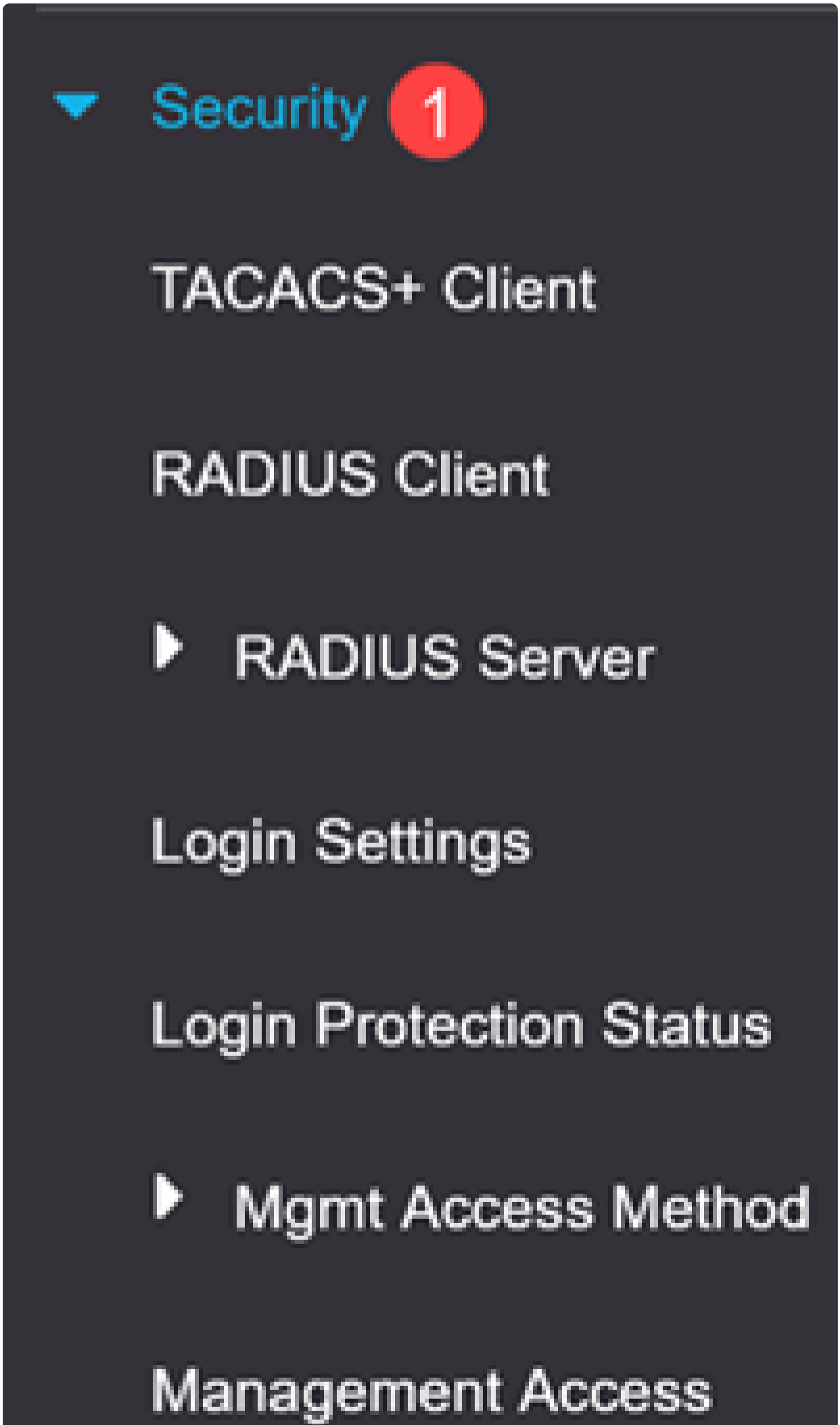
Note:

Il tipo di utilizzo deve essere selezionato come 802.1x.

Configura autenticazione 802.1x

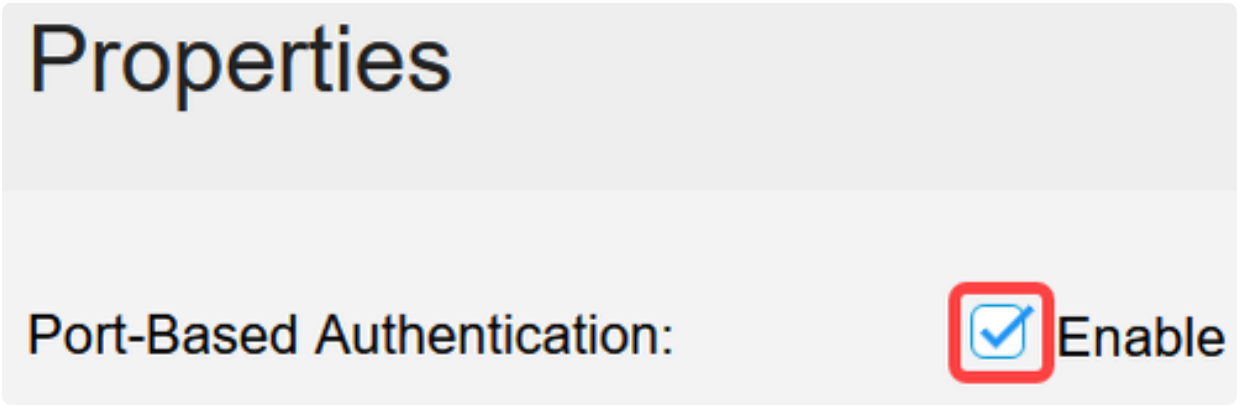
Passaggio 1

Selezionare Protezione > Autenticazione 802.1X > Menu Proprietà.


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

Passaggio 2

Fare clic sulla casella di controllo per abilitare l'autenticazione basata sulla porta.

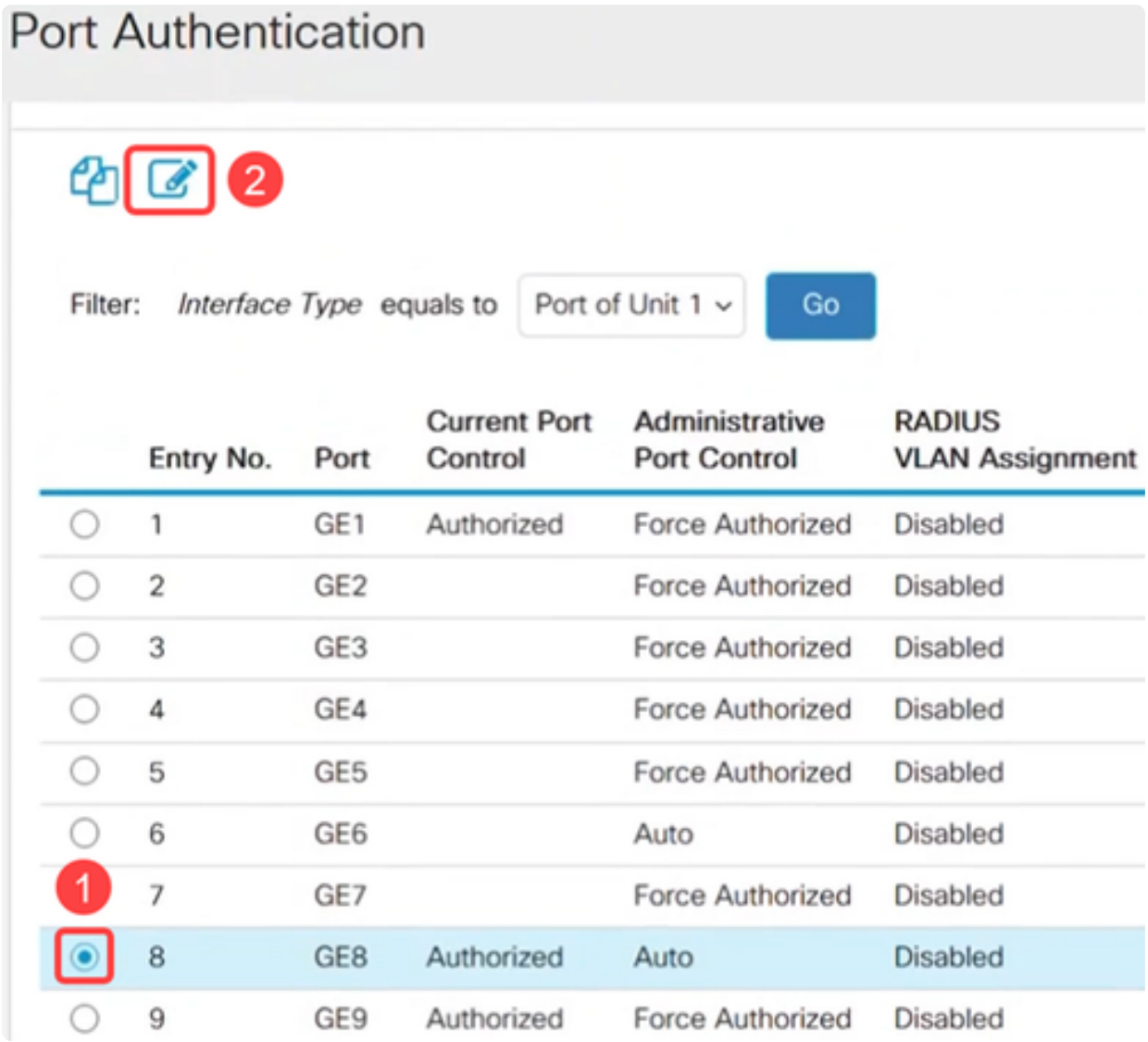


Passaggio 3

In Metodo di autenticazione, selezionare RADIUS e fare clic su Applica.

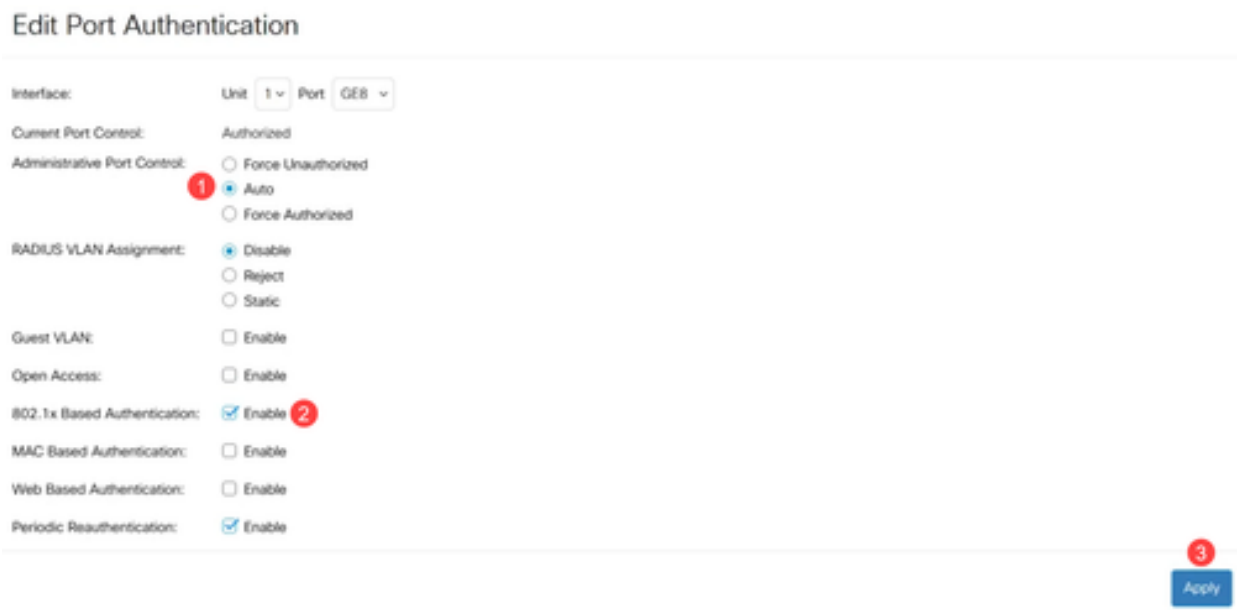
Passaggio 4

Andare al menu Security > 802.1X Authentication > Port Authentication (Sicurezza > Autenticazione 802.1X> Autenticazione porta). Selezionare la porta a cui è collegato il portatile e fare clic sull'icona Modifica. Nell'esempio è selezionato GE8.



Passaggio 5

Selezionare Administrative Port Control come Auto e abilitare l'autenticazione basata su 802.1x. Fare clic su Apply (Applica).



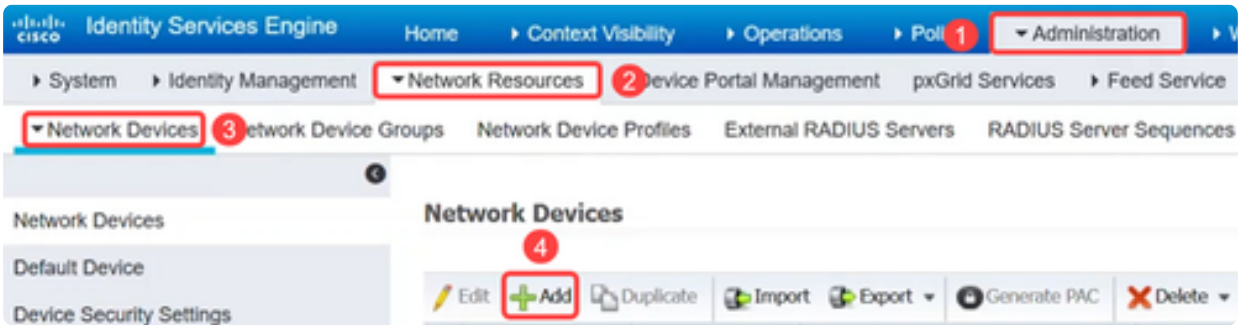
Configurazione server Cisco ISE per ACL scaricabili

> **Note:**
> La configurazione ISE non rientra nell'ambito del supporto Cisco Business. Per ulteriori informazioni, consultare la guida per l'amministratore di ISE.

Le configurazioni mostrate in questo articolo sono un esempio di ACL scaricabili per usare gli switch Cisco Catalyst serie 1300.

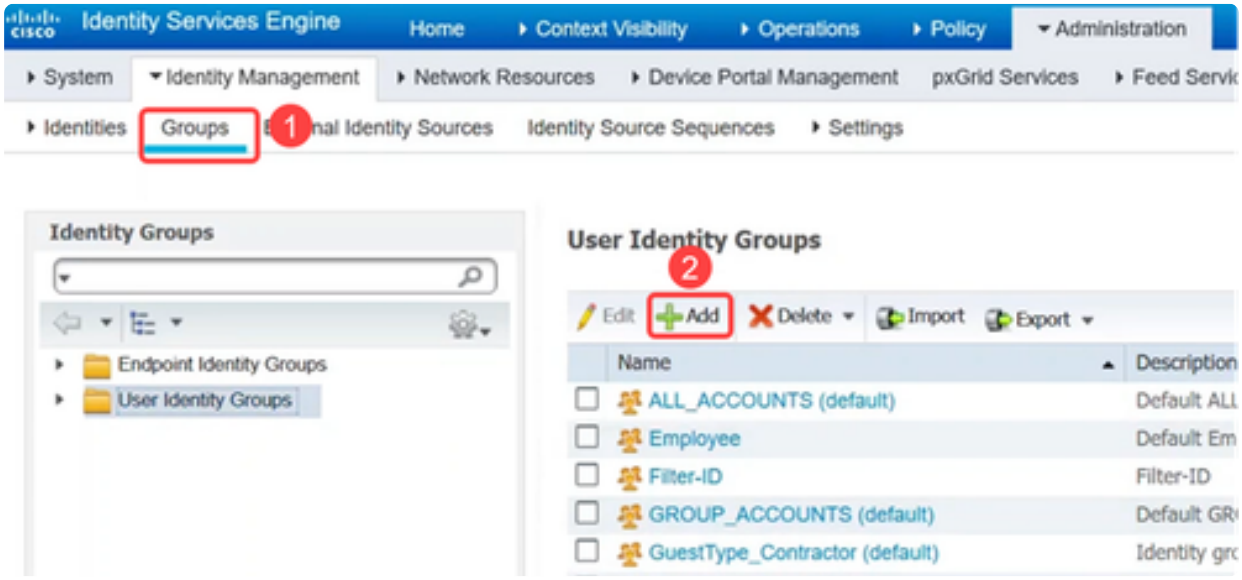
Passaggio 1

Accedere al server Cisco ISE e selezionare Amministrazione > Risorse di rete > Dispositivi di rete, quindi aggiungere il dispositivo dello switch Catalyst.



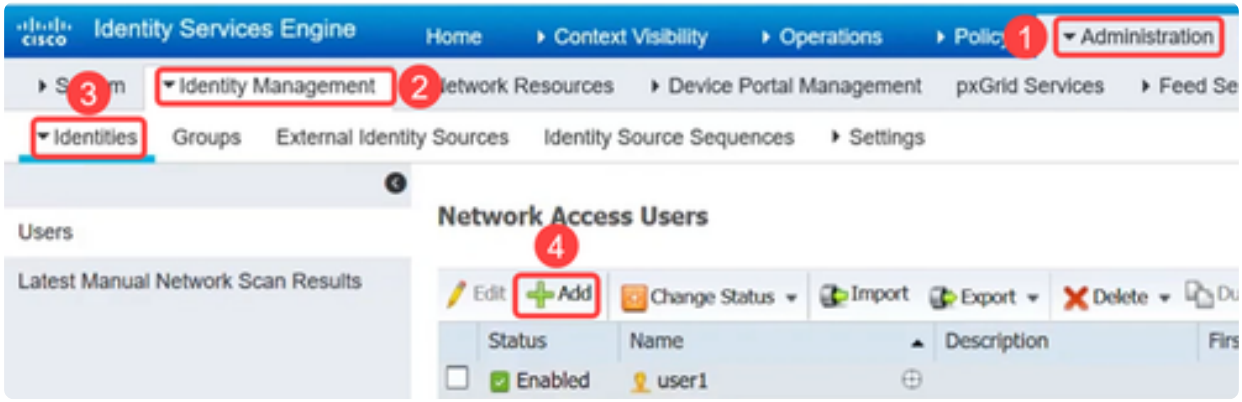
Passaggio 2

Per creare i gruppi di identità utente, passare alla scheda Gruppi e aggiungere i gruppi di identità utente.



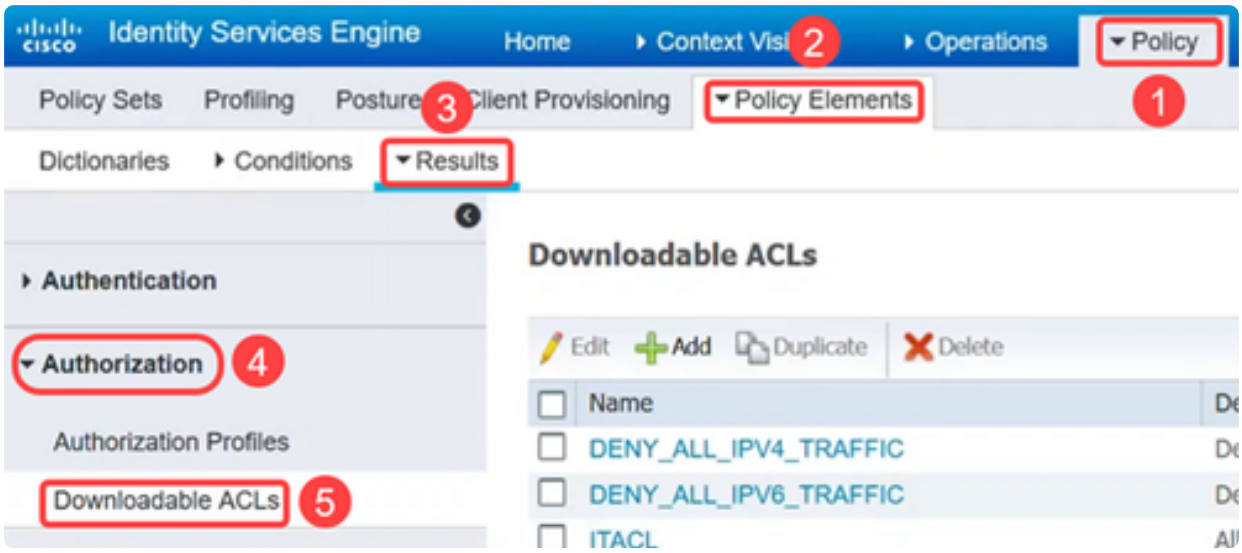
Passaggio 3

Andare al menu Amministrazione > Gestione delle identità > Identità per definire gli utenti e mappare gli utenti ai gruppi.



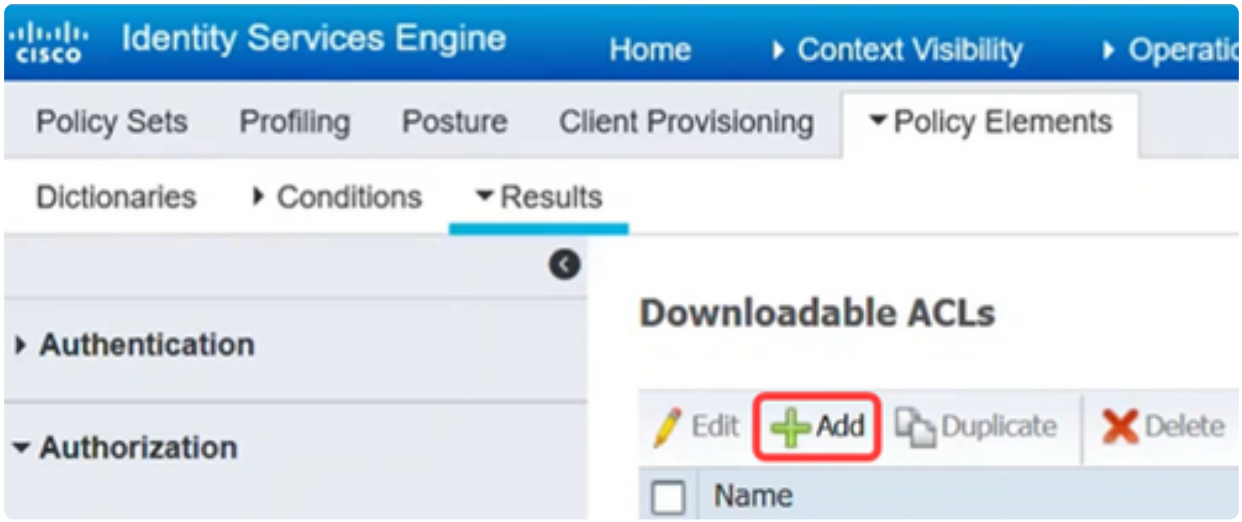
Passaggio 4

Passare a Criterio > Elementi criteri > menu Risultati. In Authorization (Autorizzazione), fare clic su Downloadable ACLs (ACL scaricabili).



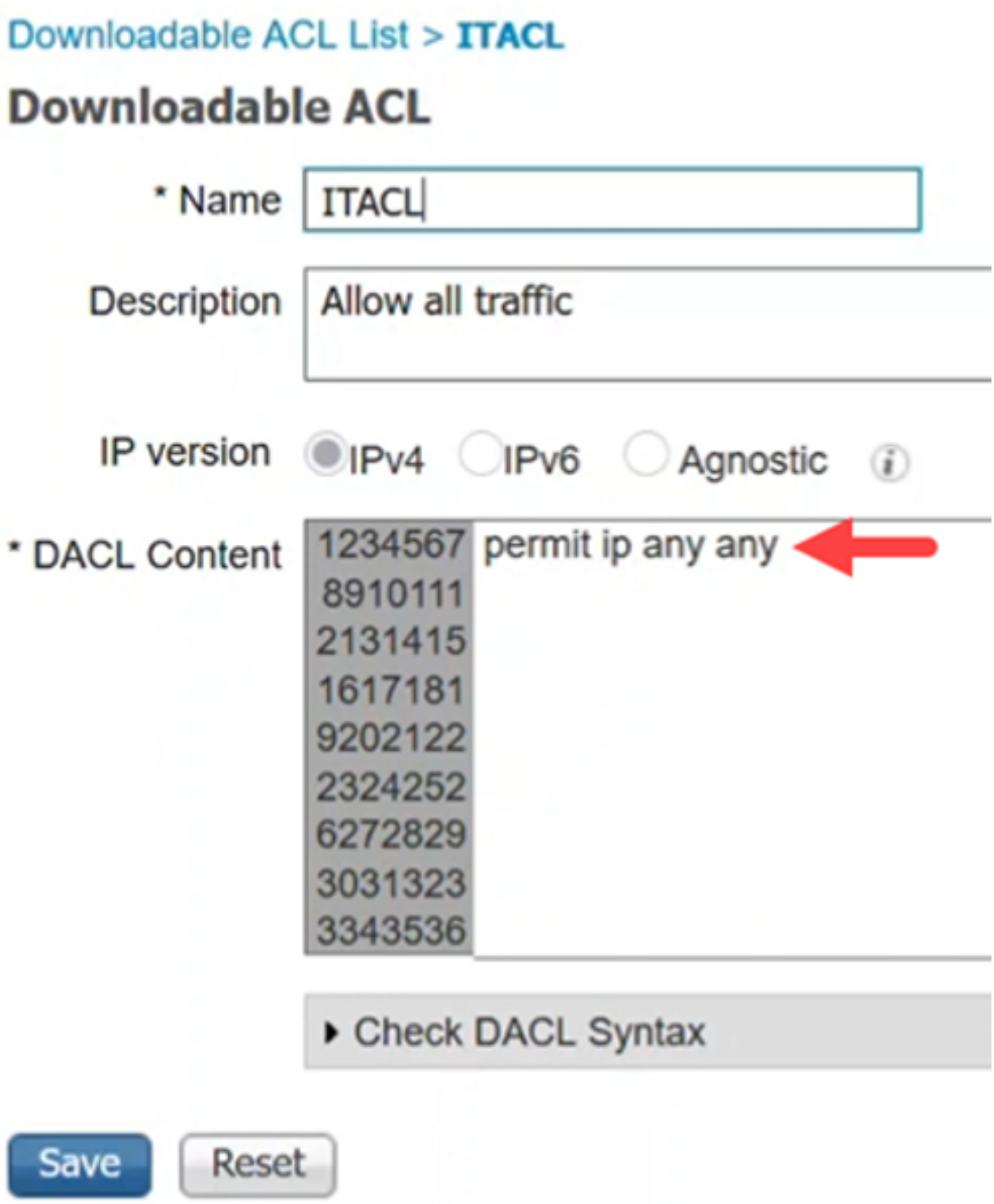
Passaggio 5

Fare clic sull'icona Add per creare l'ACL scaricabile.



Passaggio 6

Configurare il nome, la descrizione, selezionare la versione IP e immettere le voci di controllo di accesso (ACE) che costituiranno l'ACL scaricabile nel campo Contenuto DACL. Fare clic su Save (Salva).



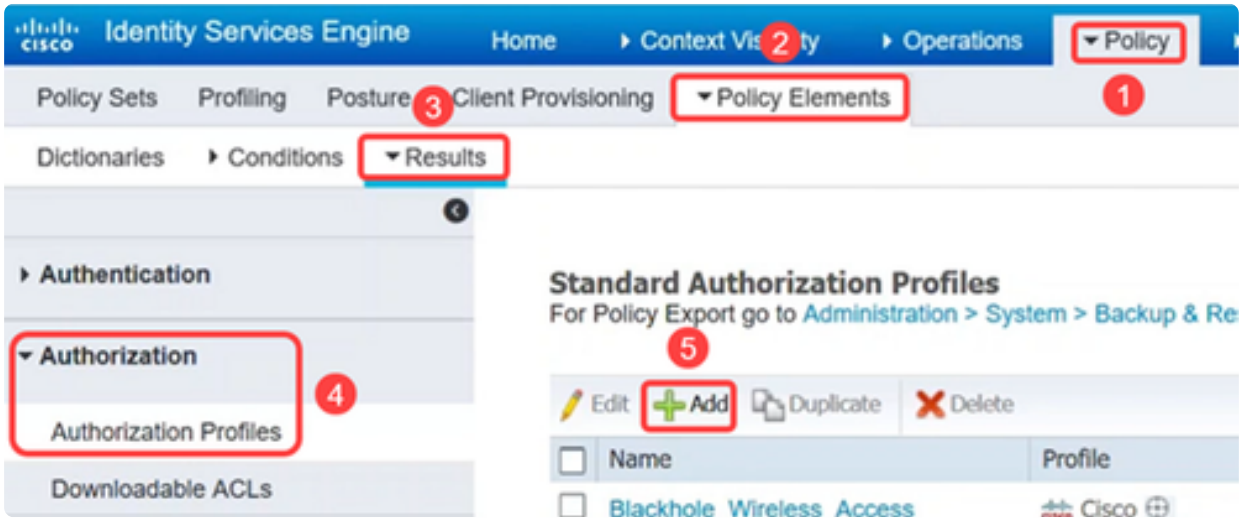
Note:

Sono supportati solo gli ACL IP e l'origine deve essere ANY (QUALSIASI). Per ACL su ISE, ora è supportato solo IPv4. Se un ACL viene immesso con un'altra origine, anche se la sintassi può essere corretta per quanto riguarda ISE, non riuscirà quando applicato allo switch.

Passaggio 7

Creare profili di autorizzazione che verranno utilizzati per associare logicamente il DACL e altri criteri all'interno dei set di criteri ISE.

A tale scopo, selezionare Policy > Policy Elements > Results > Authorization > Authorization Profiles (Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione) e fare clic su Add (Aggiungi).

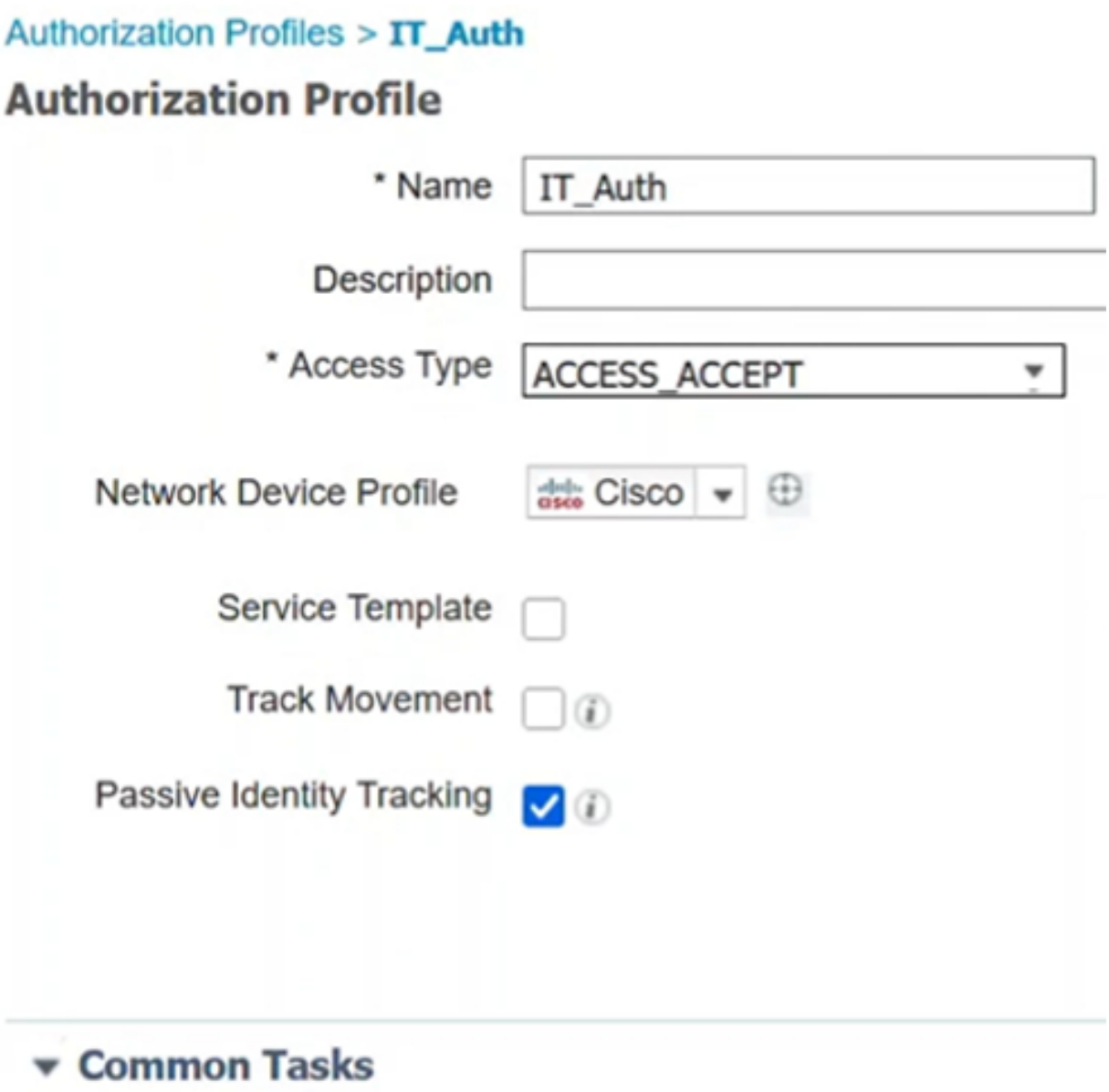


Passaggio 8

Nella pagina Profilo di autorizzazione, configurare quanto segue:

- Nome
- Descrizione
- Tipo di accesso: deve essere impostato su ACCESS_ACCEPT. Se impostato su ACCESS_REJECT, l'autenticazione verrà rifiutata.
- Network Device Profile: da selezionare come Cisco.
- Tracciamento passivo delle identità: potrebbe essere necessario abilitarlo per alcuni scenari di autenticazione. È necessaria per gli scenari EasyConnect_PassiveID collegati ad AD.
- Attività comuni - Questa sezione dispone di molte opzioni. Per questo esempio, è configurato DACL Name (Nome DACL).

Fare clic su Save (Salva).



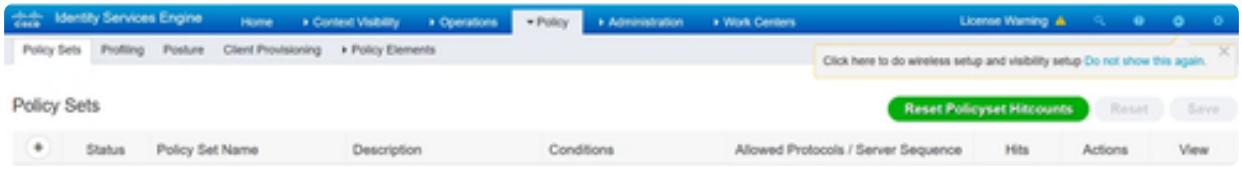
Passaggio 9

Per configurare i set di criteri che sono raggruppamenti logici di criteri di autenticazione e autorizzazione, scegliere Criterio > Set di criteri dal menu.

Quando si esamina un elenco di set di criteri, è possibile visualizzare quanto segue:

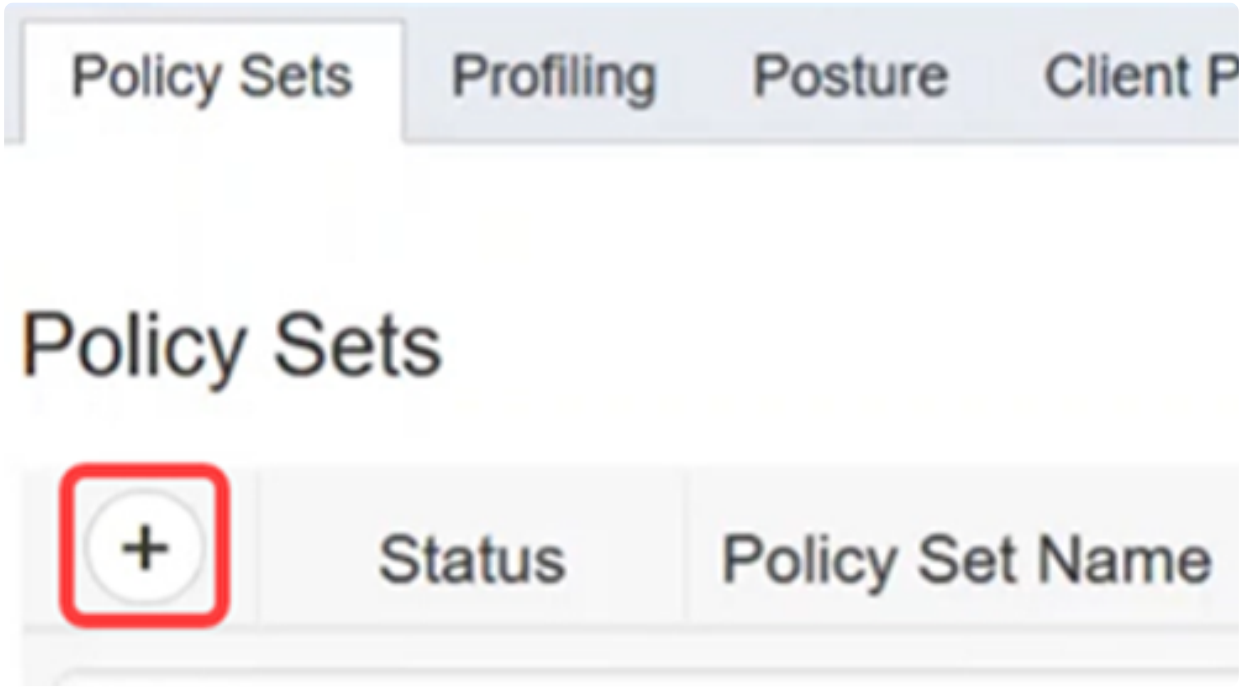
- Stato: un segno di spunta verde indica attivato, un cerchio bianco vuoto indica disattivato e un'icona a forma di occhio è solo per la configurazione di un monitor.
- Nome e descrizione set di criteri - sono di immediata comprensione
- Condizioni: definire dove viene applicato il set di criteri.
- Protocolli consentiti/sequenza server: imposta controlli più avanzati.
- Accessi: visualizza il numero di accessi al set di criteri.
- Azioni: consente di modificare l'ordine in cui è possibile applicare i set di criteri, copiare un set di criteri esistente o eliminare un set di criteri esistente.

- Visualizza: consente di modificare i dettagli del set di criteri.



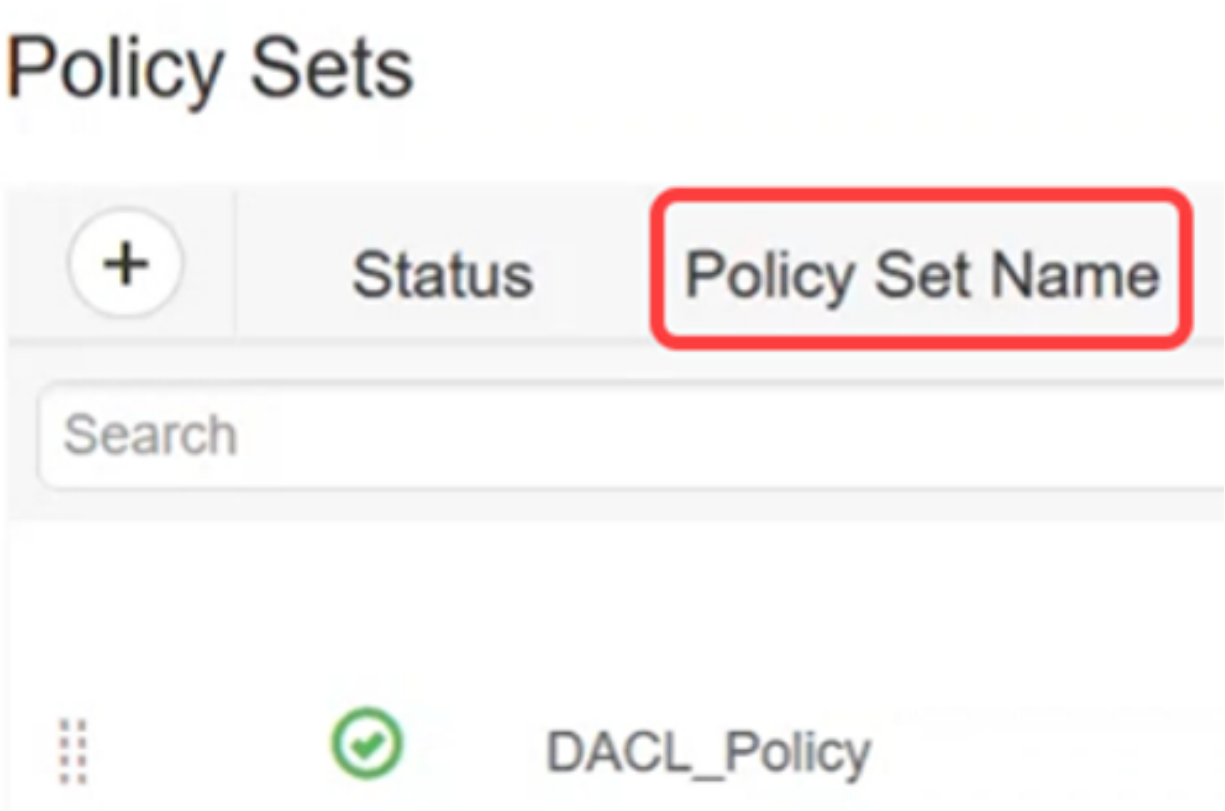
Passaggio 10

Per creare un set di criteri, fare clic sul pulsante Aggiungi.



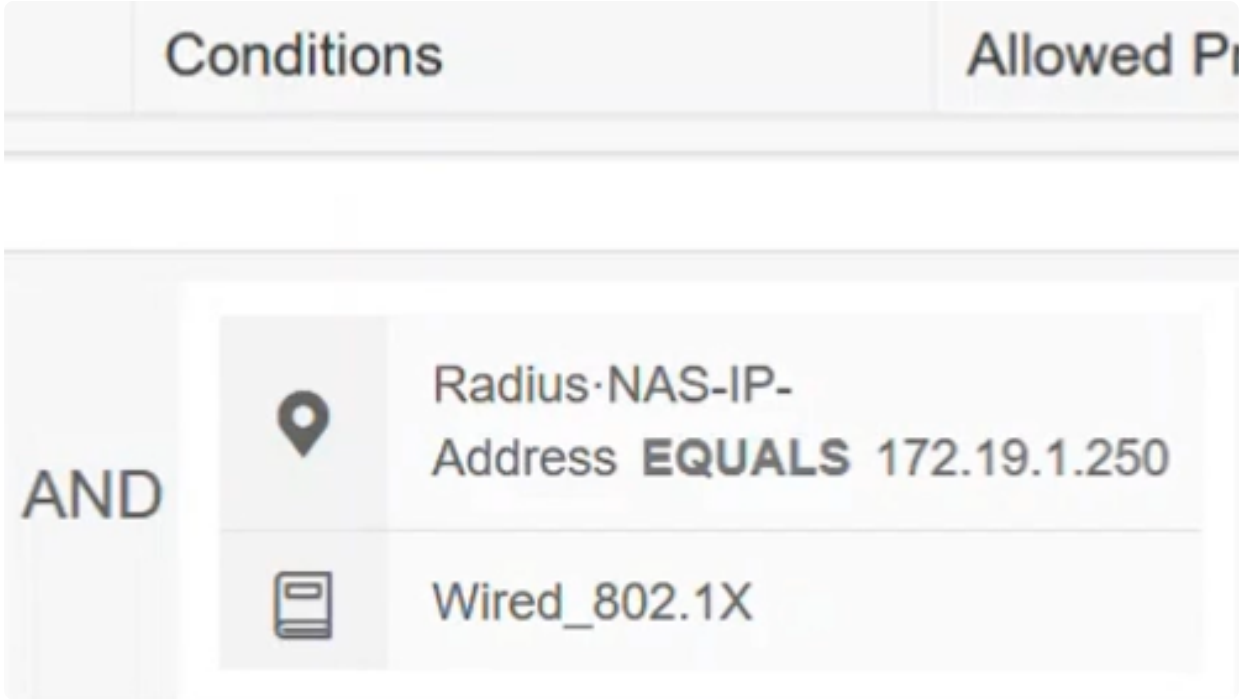
Passaggio 11

Definire un nome per il set di criteri.



Passaggio 12

In Condizioni fare clic sul pulsante Aggiungi. Verrà aperto Conditions Studio in cui è possibile definire dove verrà utilizzato questo profilo di autenticazione. Nell'esempio, è stato applicato all'indirizzo Radius-NAS-IP-Address (lo switch), ossia al traffico 172.19.1.250 e wired_802.1x.

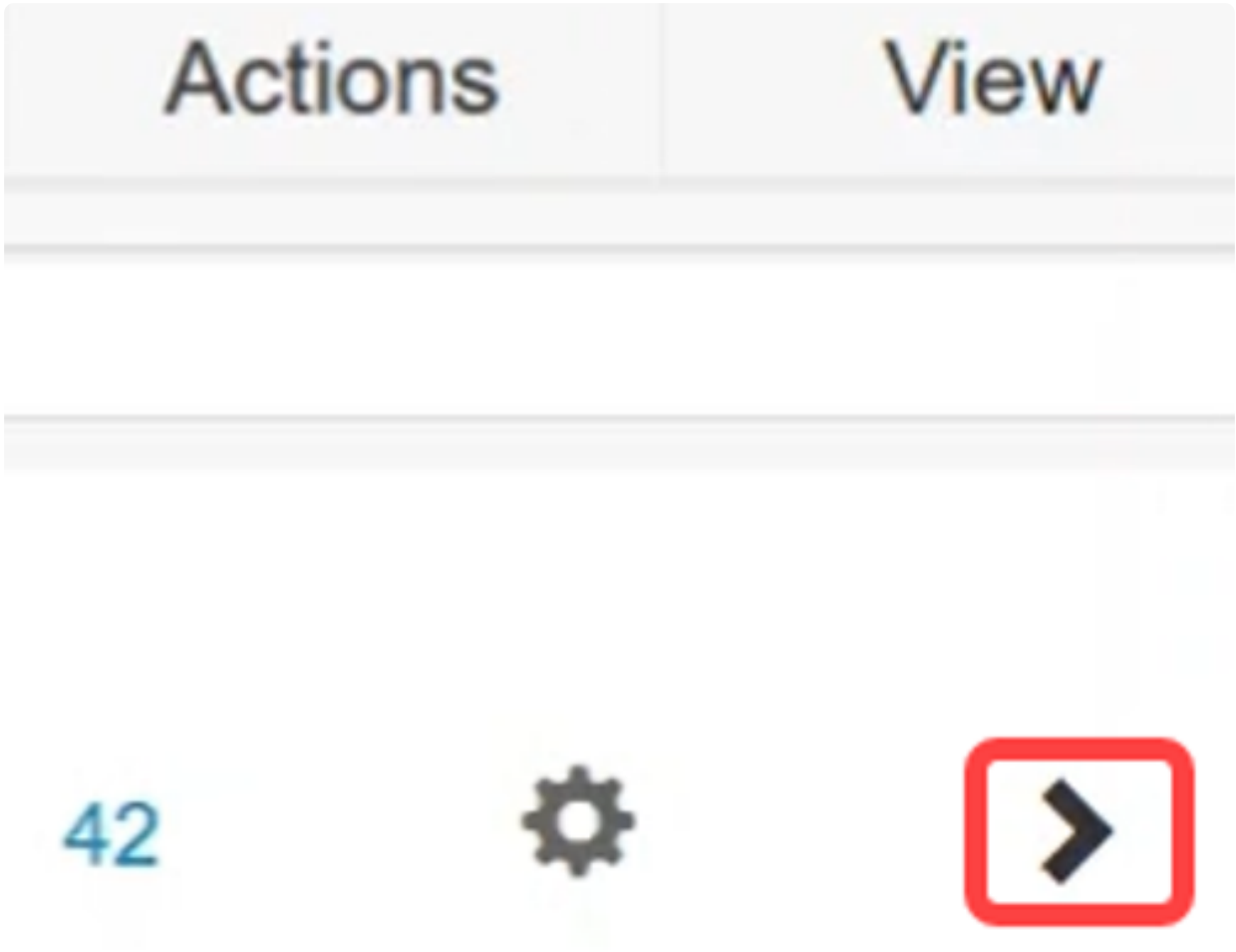


Passaggio 13

Configurare i Protocolli consentiti in Accesso di rete predefinito e fare clic su Salva.

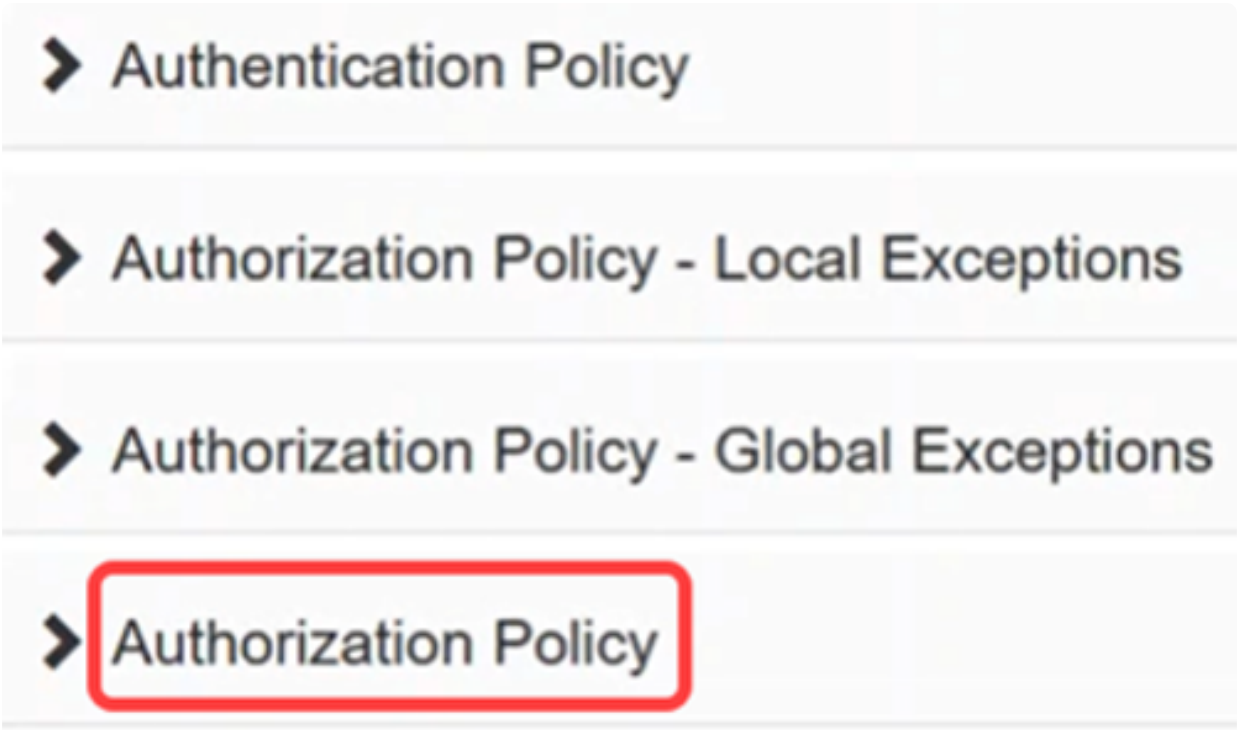
Passaggio 14

In Visualizza fare clic sull'icona a forma di freccia per configurare i criteri di autenticazione e autorizzazione in base alla configurazione della rete e ai requisiti oppure scegliere le impostazioni predefinite. In questo esempio fare clic su Criteri di autorizzazione.



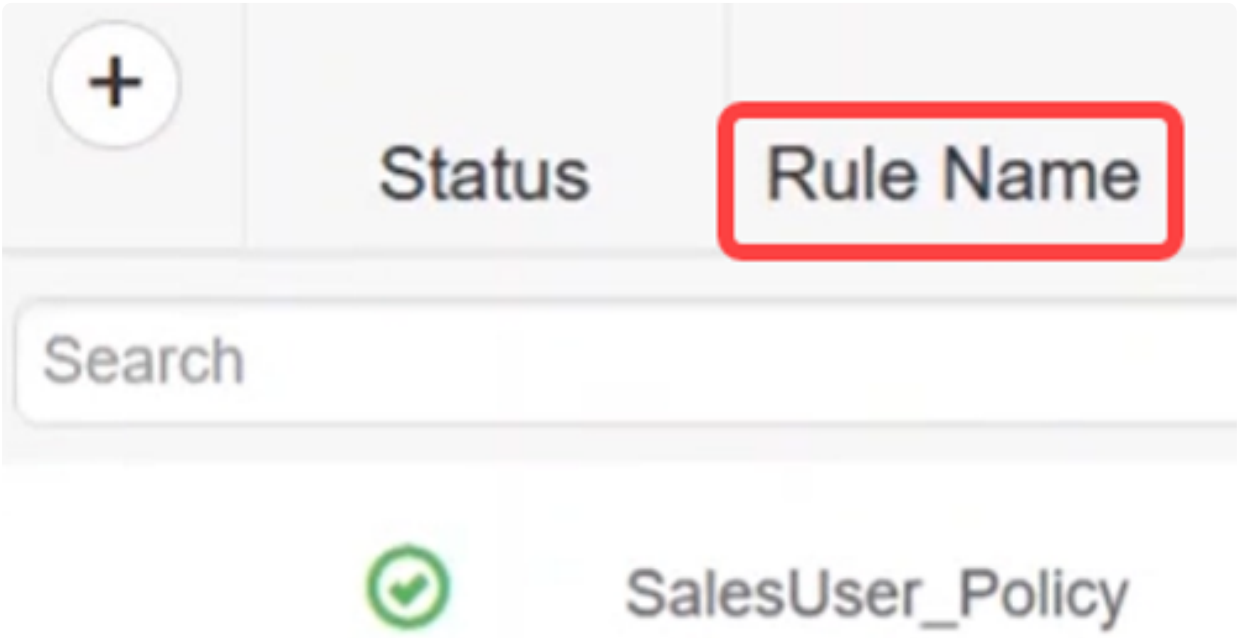
Passaggio 15

Fare clic sull'icona più per aggiungere un criterio.



Passaggio 16

Immettere il nome della regola.



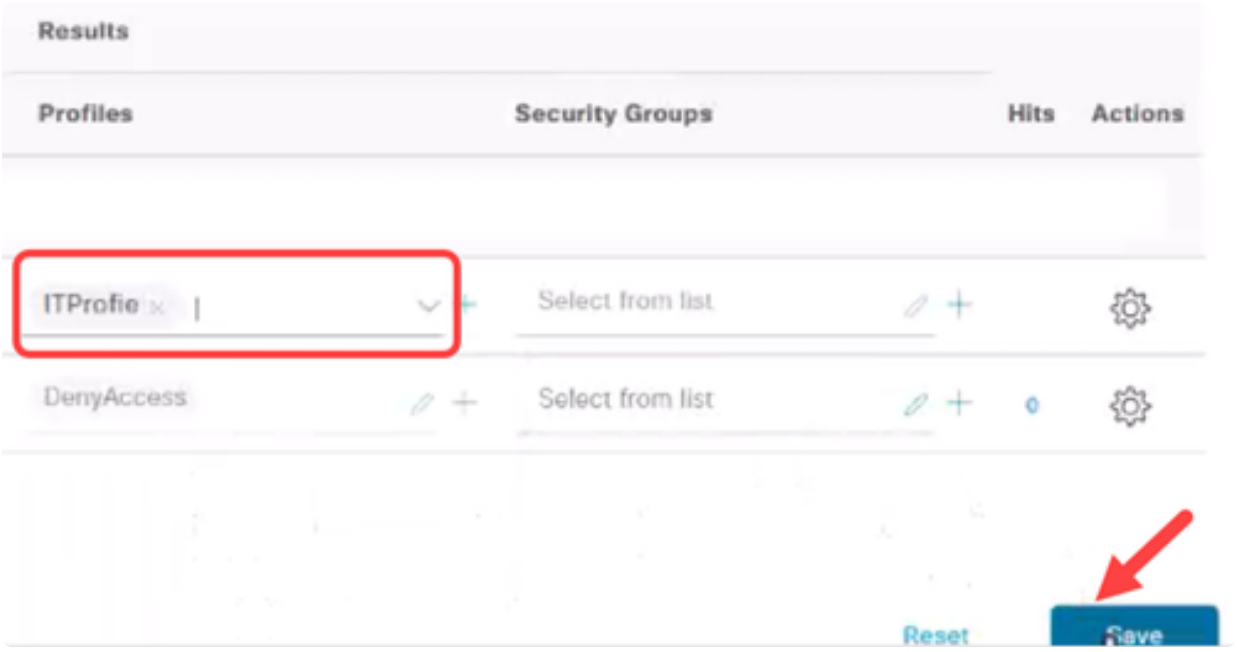
Passaggio 17

In Condizioni, fare clic sull'icona più e selezionare il gruppo di identità. Fare clic su

Usa.

Passaggio 18

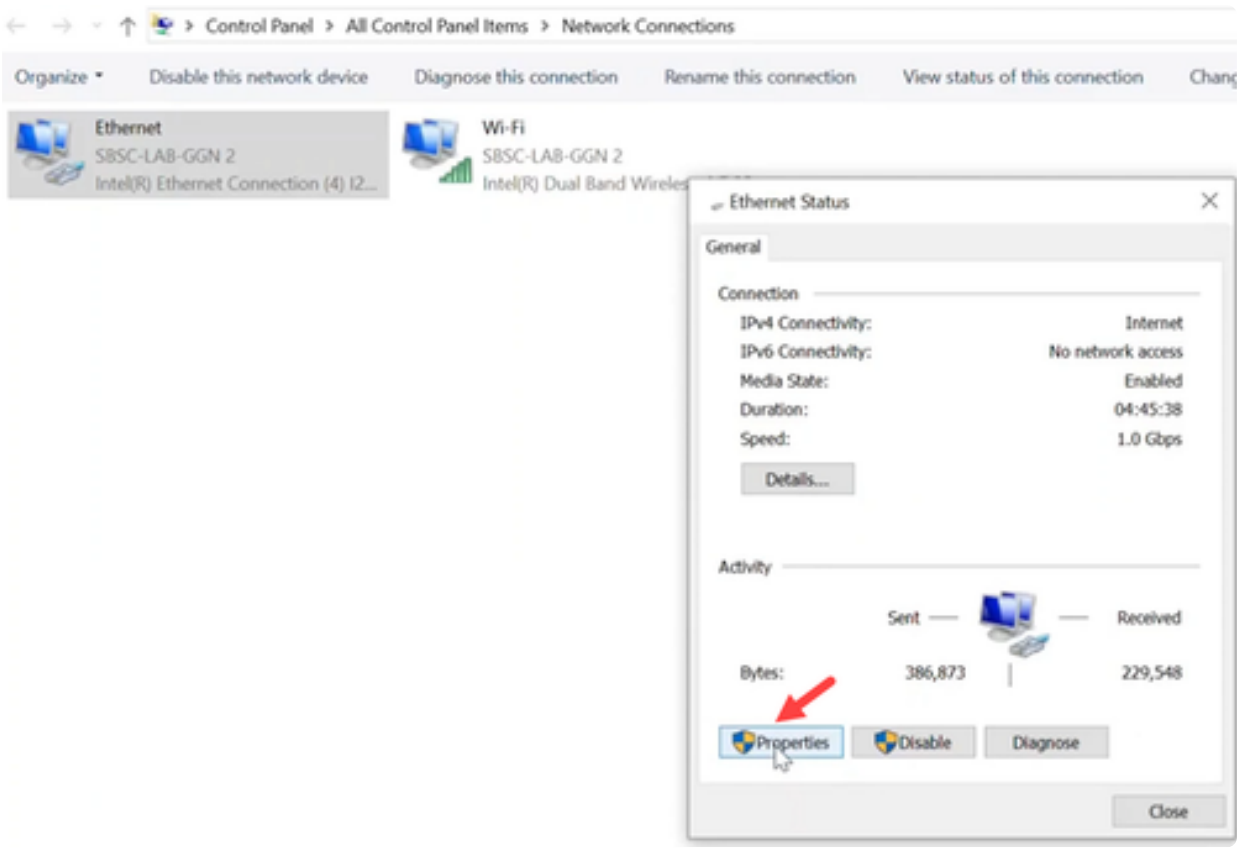
Applicate il profilo richiesto e fate clic su Salva (Save).



Configurazioni client

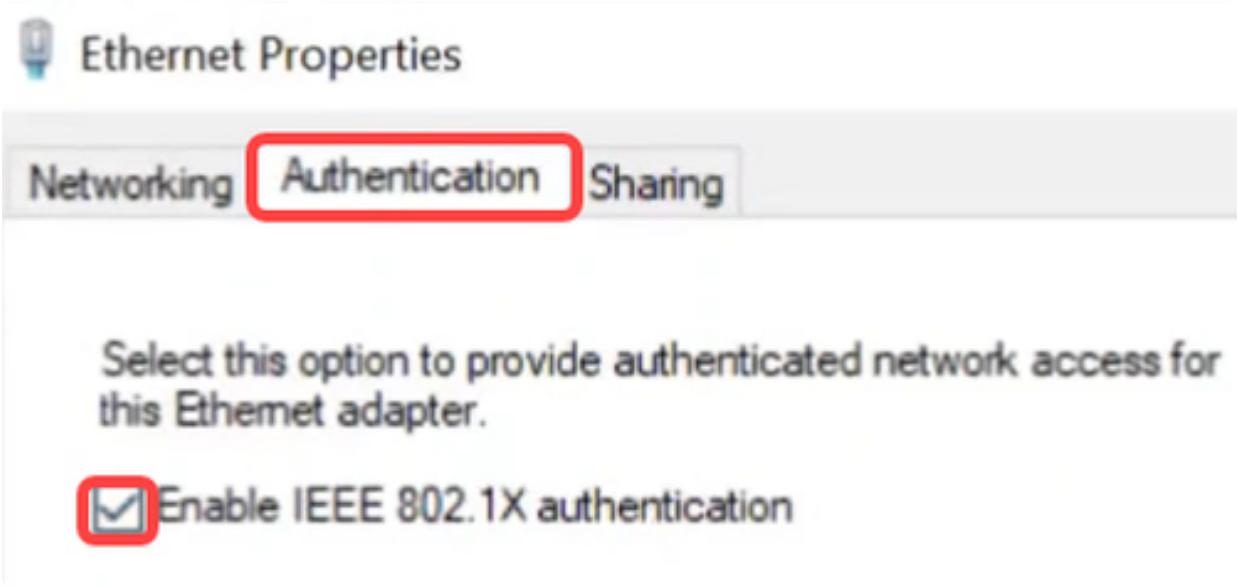
Passaggio 1

Sul laptop client, selezionare Connessioni di rete > Ethernet e fare clic su Proprietà.



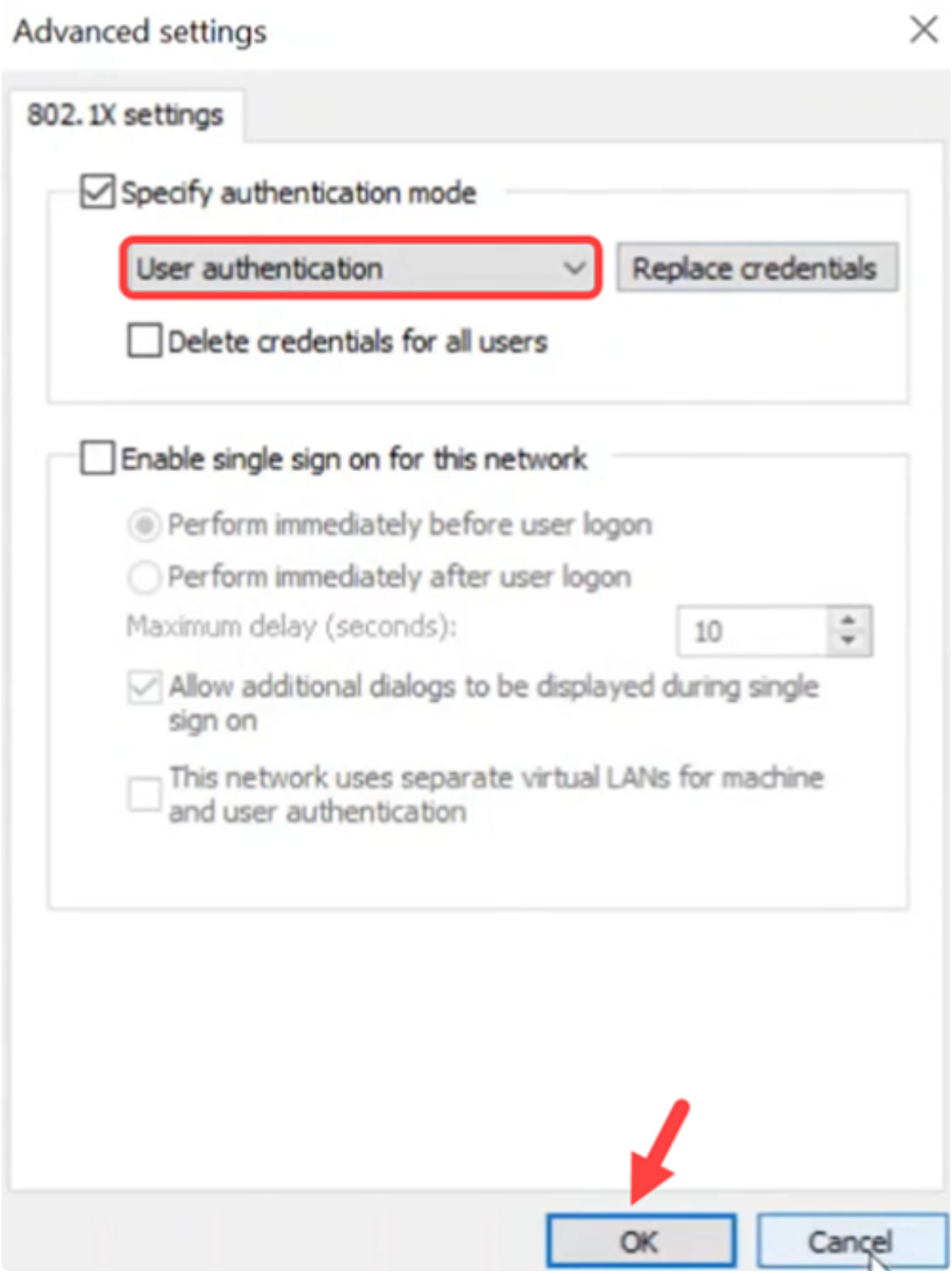
Passaggio 2

Fare clic sulla scheda Authentication (Autenticazione) e verificare che l'autenticazione 802.1X sia abilitata.



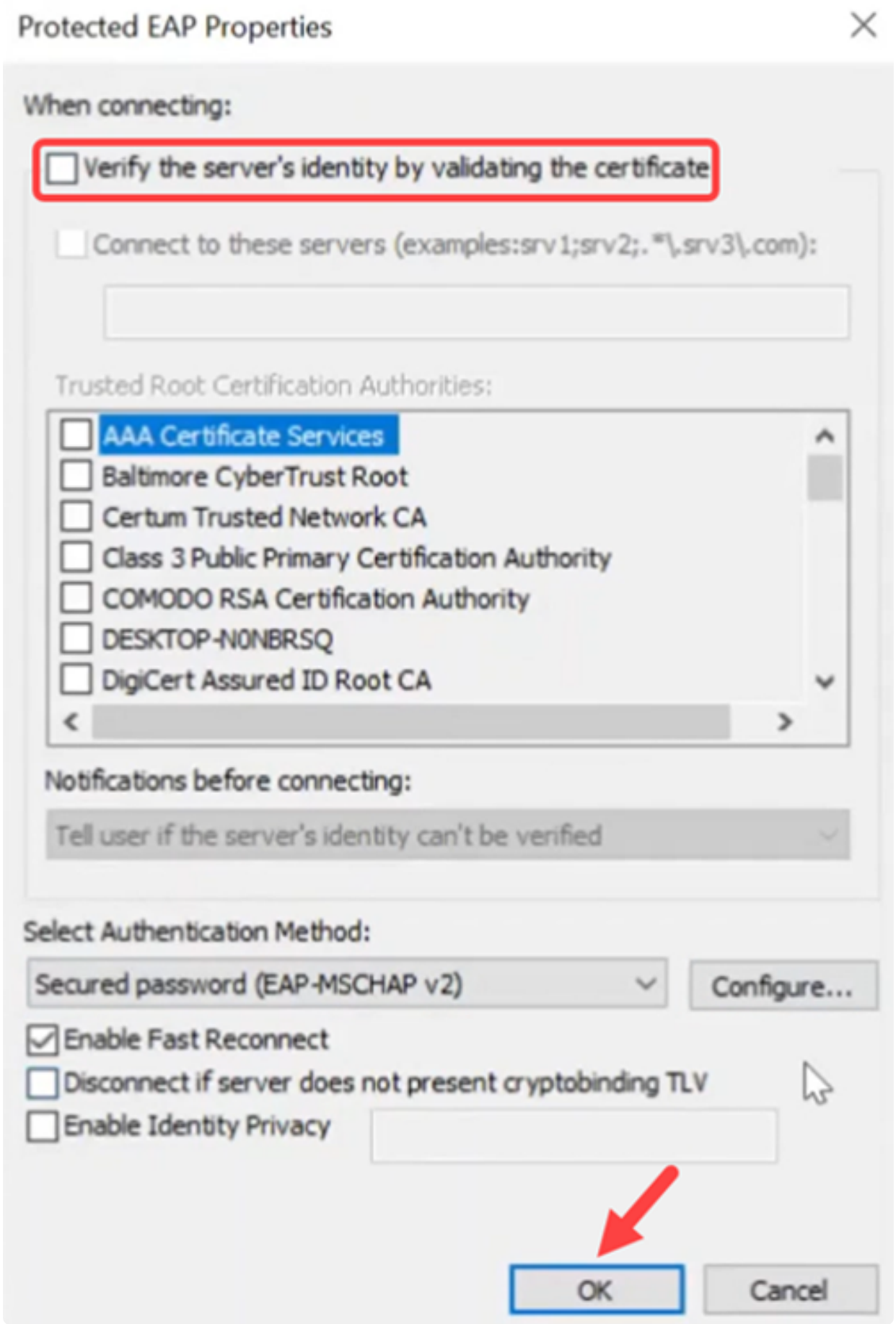
Passaggio 3

In Impostazioni aggiuntive, selezionare Autenticazione utente come modalità di autenticazione. Fare clic su Salva credenziali e quindi su OK.



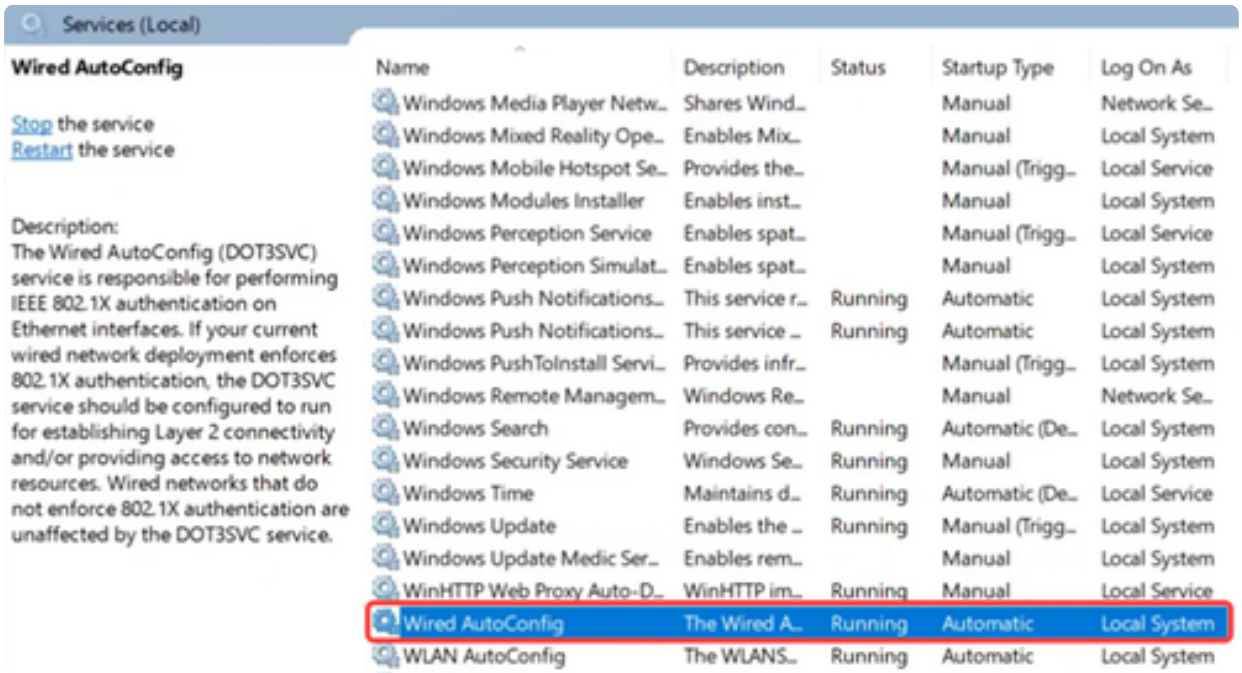
Passaggio 4

Fare clic su Settings (Impostazioni) e assicurarsi che la casella accanto a Verify the server’s identity by validating the certificate (Verifica dell’identità del server tramite la convalida del certificato) sia deselezionata. Fare clic su OK.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

Passaggio 5

In Servizi, abilitare le impostazioni di configurazione automatica per reti cablate.

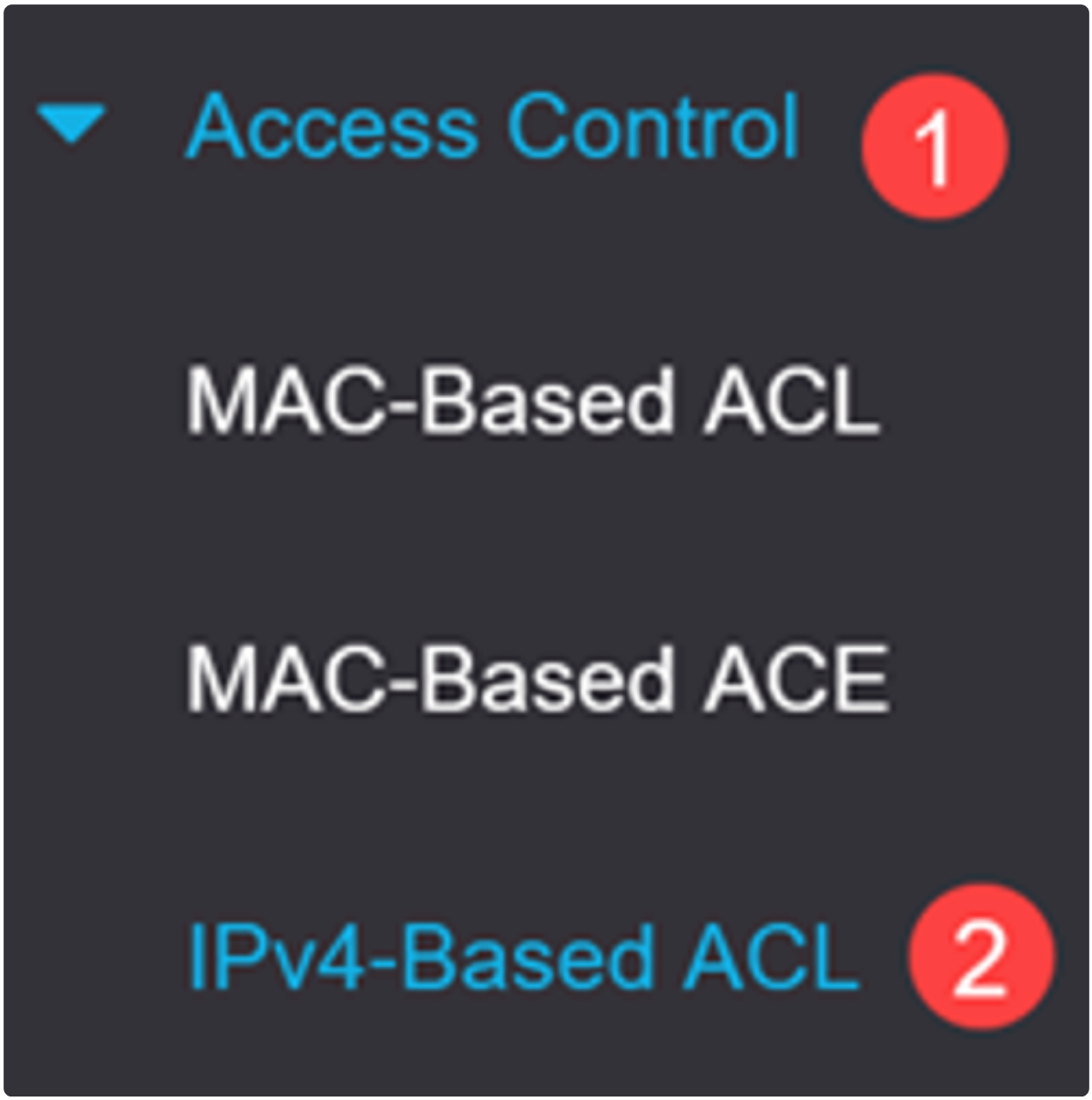


Verifica DACL

Dopo aver autenticato l'utente, è possibile verificare l'ACL scaricabile.

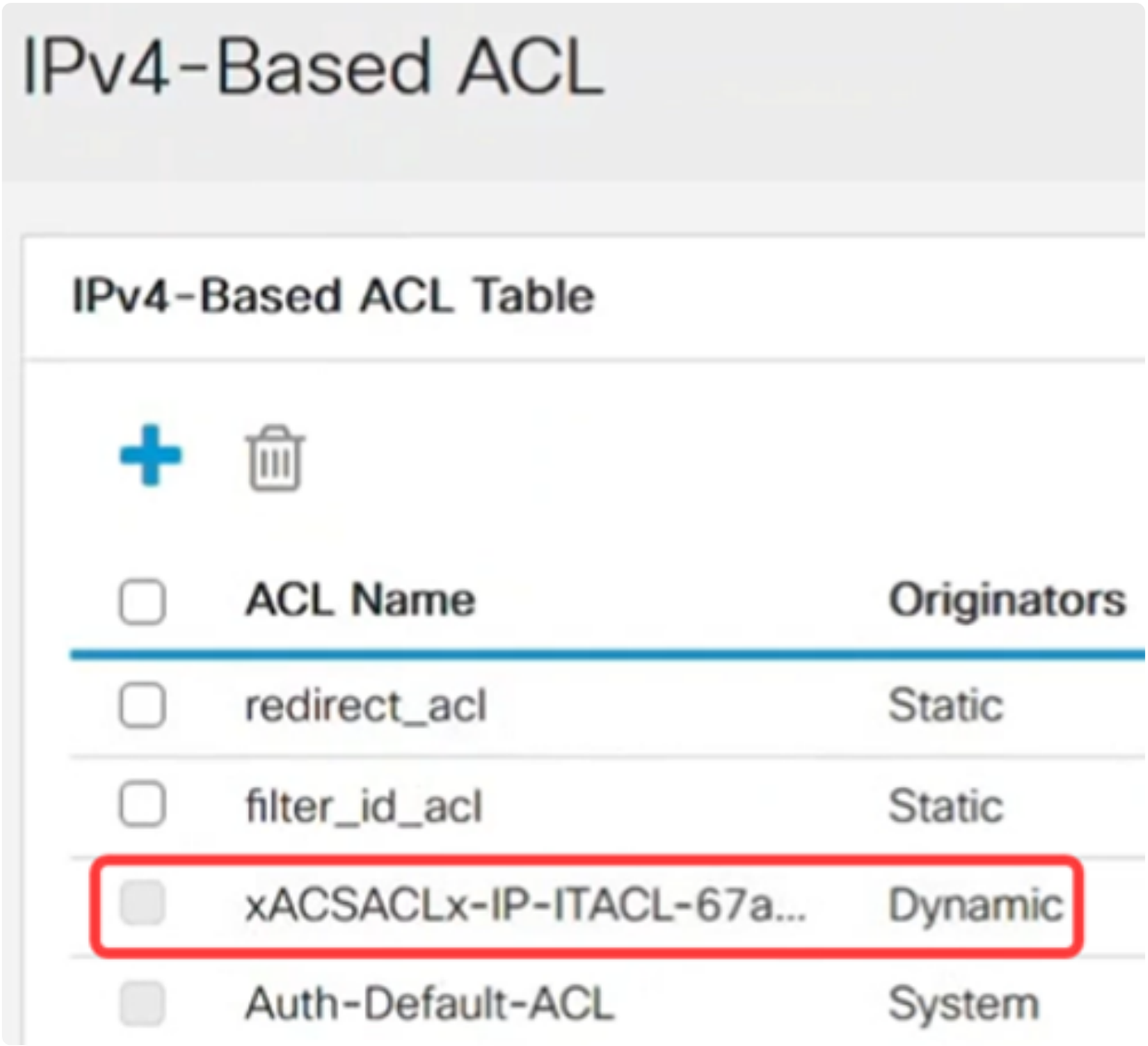
Passaggio 1

Accedere allo switch Catalyst 1300 e selezionare Access Control > IPv4-Based ACL menu.



Passaggio 2

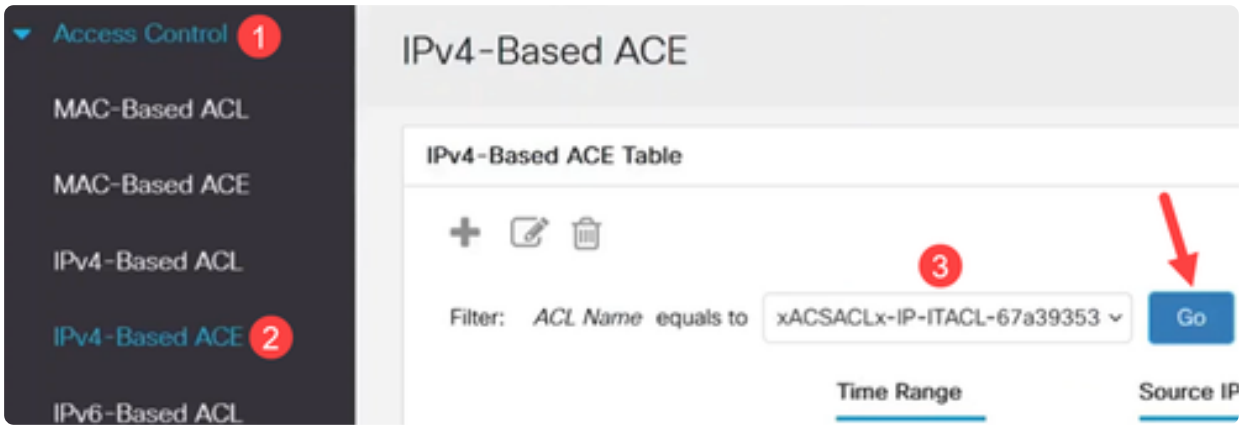
La tabella ACL basata su IPv4 visualizzerà l'ACL scaricato.



Note:
Non è possibile modificare gli ACL scaricabili.

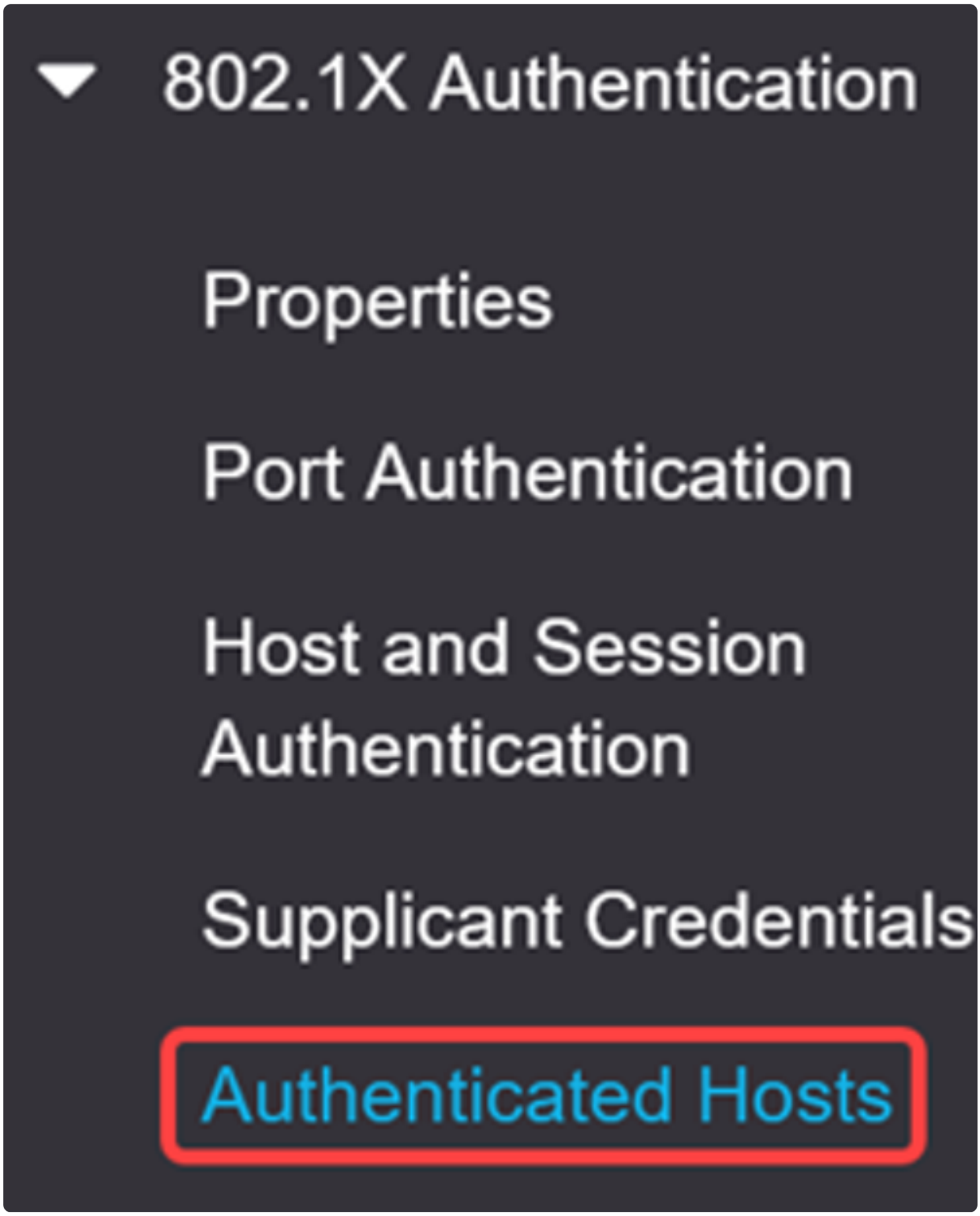
Passaggio 3

Un altro modo per verificare è individuare l'ACL basato su IPv4, selezionare l'ACL scaricabile dal menu a discesa Nome ACL e fare clic su Vai. Verranno visualizzate le regole configurate in ISE.



Passaggio 4

Passare a Protezione > Autenticazione 802.1 > Menu Host autenticati. È possibile verificare gli utenti autenticati. Per ulteriori informazioni, fare clic su Authenticated Sessions.



Passaggio 5

Dalla CLI, eseguire il comando show ip access-lists interface seguito dall'ID dell'interfaccia.

Nell'esempio, è possibile visualizzare gli ACL e gli ACE applicati alla rete Gigabit Ethernet 3.

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

Passaggio 6

Per visualizzare le impostazioni relative alla connessione ISE e ai download degli ACL, usare il comando

show dot1x session interface <ID> in dettaglio. È possibile visualizzare lo stato, lo stato di autenticazione 802.1x e gli ACL scaricati.

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:           :31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
     Oper host mode: multi-host
    Session timeout: N/A
     Session Uptime: 196 sec
  Common Session ID: 14FBA8C00500032222C35D9E
    Acct Session ID: 0x05000322
 Server Policies:
            ACS ACL: xACSACLx-IP-SalesACL-6760399d

 Method status list:
    Method                  State
    802.1x                  Authentication success
```

Conclusioni

Ecco qua! Ora sapete come funziona il download dell'ACL sugli switch Cisco Catalyst 1300 con Cisco ISE.

Per ulteriori informazioni, consultare la Guida all'amministrazione di Catalyst 1300 e la pagina di supporto di Cisco Catalyst serie 1300.

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).