

# Configurazione di APIC per l'amministrazione dei dispositivi con ISE e TACACS+

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Procedura di autenticazione](#)

[Configurazione APIC](#)

[Configurazione di ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

In questo documento viene descritta la procedura per integrare APIC con ISE per l'autenticazione degli utenti amministratore con il protocollo TACACS+.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- Protocollo TACACS

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- APIC versione 4.2(7u)
- Patch 1 per ISE versione 3.2

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.

## Configurazione

### Esempio di rete



Diagramma integrazione

### Procedura di autenticazione

Passaggio 1. Accedere all'applicazione APIC con le credenziali utente di amministratore.

Passaggio 2. Il processo di autenticazione attiva e ISE convalida le credenziali localmente o tramite Active Directory.

Passaggio 3. Una volta completata l'autenticazione, ISE invia un pacchetto di autorizzazioni per autorizzare l'accesso all'APIC.

Passaggio 4. ISE mostra un log live di autenticazione completato.

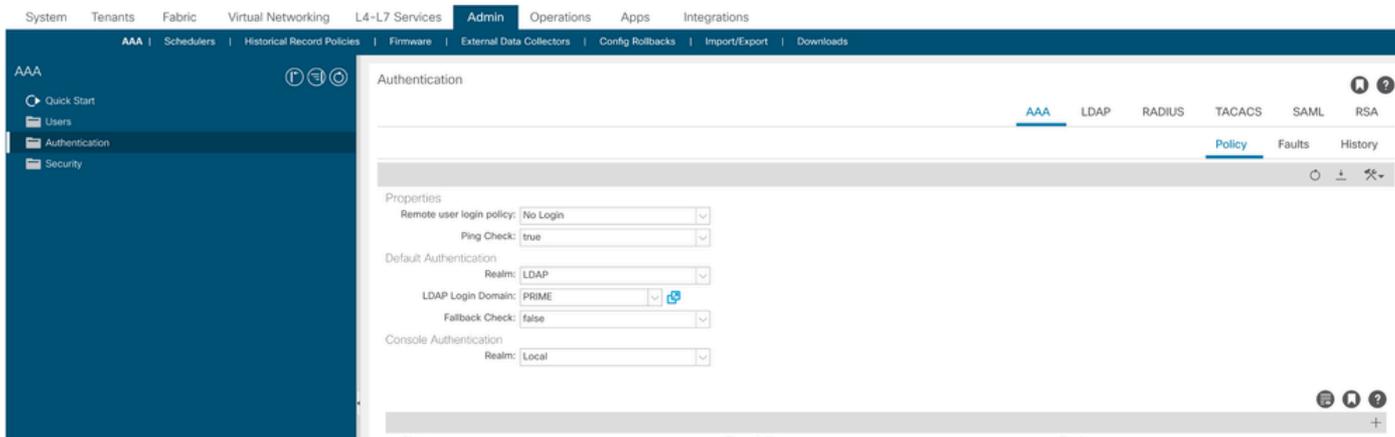
---

 Nota: APIC replica la configurazione TACACS+ sugli switch foglia che fanno parte della struttura.

---

### Configurazione APIC

Passaggio 1. Per creare un nuovo dominio di accesso, passare all'Admin > AAA > Authentication > AAA' icona e scegliere tale icona.



Configurazione dell'amministratore dell'accesso APIC

Passaggio 2. Definire un nome e un realm per il nuovo dominio di accesso e fare clic su **+** in Provider per creare un nuovo provider.

## Create Login Domain

Name:

Realm:

Description:

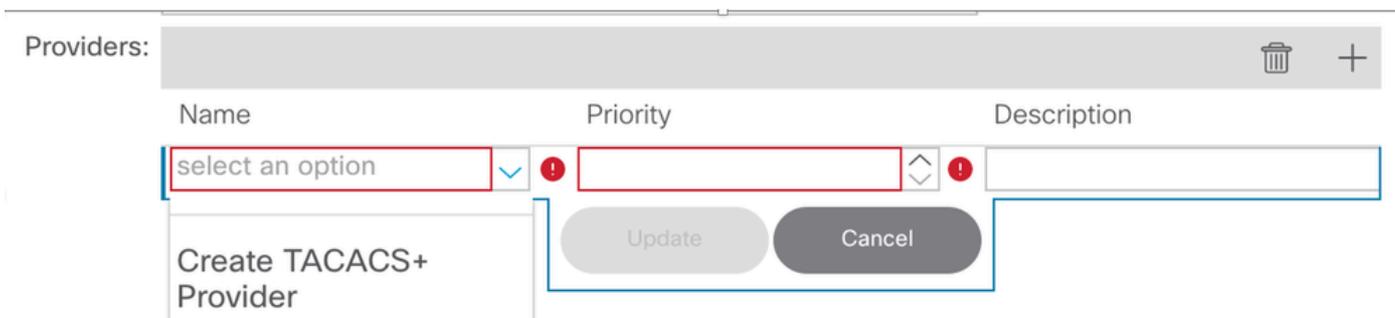
Providers: 🗑️ +

| Name | Priority | Description |
|------|----------|-------------|
|      |          |             |

Cancel

Submit

Amministratore accesso APIC



Provider TACACS APIC

Passaggio 3. Definire l'indirizzo IP o il nome host ISE, definire un segreto condiviso e scegliere il

gruppo di criteri endpoint di gestione (EPG). Fare clic **Submit** per aggiungere il provider TACACS+ all'account admin.

## Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol:

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring:

**Cancel** **Submit**

Impostazioni provider TACACS APIC

## Create Login Domain



Name:

Realm:

Description:

Providers:

| Name     | Priority | Description |
|----------|----------|-------------|
| 52.13.89 | 1        |             |

**Cancel** **Submit**

| Host Name | Description | Port | Timeout (sec) | Retries |
|-----------|-------------|------|---------------|---------|
| .52.13.89 |             | 49   | 5             | 1       |

Visualizzazione provider TACACS

## Configurazione di ISE

Passaggio 1. Passare a purtroppo>Amministrazione > Risorse di rete > Gruppi di dispositivi di rete. Creare un gruppo di dispositivi di rete in Tutti i tipi di dispositivi.

### ☰ Cisco ISE

Network Devices **Network Device Groups** Network Device Profiles External

## Network Device Groups

All Groups

Choose group ▾

↻ **Add** Duplicate Edit 🗑️ Trash 👁️ Show group members 📄 Import 📤 Export ▾ ☰

| <input type="checkbox"/> Name               | Description      |
|---|------------------|
| <input type="checkbox"/> ▾ All Device Types | All Device Types |
| <input type="checkbox"/> APIC               |                  |

ISE Network Device Group

Passaggio 2. Passare a Administration > Network Resources > Network Devices. Selezionare Adddefine APIC Name and IP address, scegliere APIC in Device Type and TACACS+ checkbox, quindi definire la password da usare nella configurazione del provider TACACS+ per APIC. Fare clic su .Submit

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

Network Devices

Name

Description

IP Address  \* IP :

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location   [Set To Default](#)

IPSEC   [Set To Default](#)

Device Type   [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret  [Show](#)

[Retire](#)

Ripetere i passaggi 1 e 2 per gli switch foglia.

Passaggio 3. Per integrare ISE con Active Directory, seguire le istruzioni riportate sul collegamento;

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>.



Nota: In questo documento sono inclusi sia gli utenti interni che i gruppi degli amministratori di Active Directory come origini di identità. Tuttavia, il test viene eseguito con l'origine di identità degli utenti interni. Il risultato è lo stesso per i gruppi AD.

---

Passaggio 4. (Facoltativo) Navigare su Outlook > Administration > Identity Management > Groups. Selezionate **User Identity Groups** e fate clic su **Add**. Creare un gruppo per gli utenti Admin di sola lettura e gli utenti Admin.

Identity Groups

EQ

< [List Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

# User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

| Name  | Description       |
|---|-------------------|
| <input type="checkbox"/> ALL_ACCOUNTS (default) | Default ALL_      |
| <input type="checkbox"/> APIC_RO                | <a href="#">i</a> |
| <input type="checkbox"/> APIC_RW                |                   |

Gruppo di identità

Passaggio 5. (Facoltativo) Passare a >OutlookAdministration > Identity Management > Identity. Fare clicAdd creare unRead Only Adminutente e unAdminutente. Assegnare ogni utente a ogni gruppo creato nel passaggio 4.

Users

Latest Manual Network Scan Res...

# Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

| Status                   | Username | Description | First Name | Last Name | Email Address | User Identity Groups |
|--------------------------|----------|-------------|------------|-----------|---------------|----------------------|
| <input type="checkbox"/> | Enabled  | APIC_ROUser |            |           |               | APIC_RO              |
| <input type="checkbox"/> | Enabled  | APIC_RWUser |            |           |               | APIC_RW              |

Passaggio 6. Navigare fino a Android>Administration > Identity Management > Identity Source Sequence. ScegliereAddDefinisci nome, quindi scegliereAD Join PointsInternal UsersOrigine identità dall'elenco. SelezionareTreat as if the user was not found and proceed to the next store in the sequence sottoAdvanced Search List Settings e fare clic suSave.

∨ Identity Source Sequence

\* Name

Description

∨ Certificate Based Authentication

Select Certificate Authentication Profile

∨ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

| Available          |  | Selected       |
|--------------------|--|----------------|
| Internal Endpoints |  | iselab         |
| Guest Users        |  | Internal Users |
| All_AD_Join_Points |  |                |

Navigation buttons: > < >> << (between columns) and ^ > < > (within Selected column)

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Sequenza origine identità

7. Passare a ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Selezionare

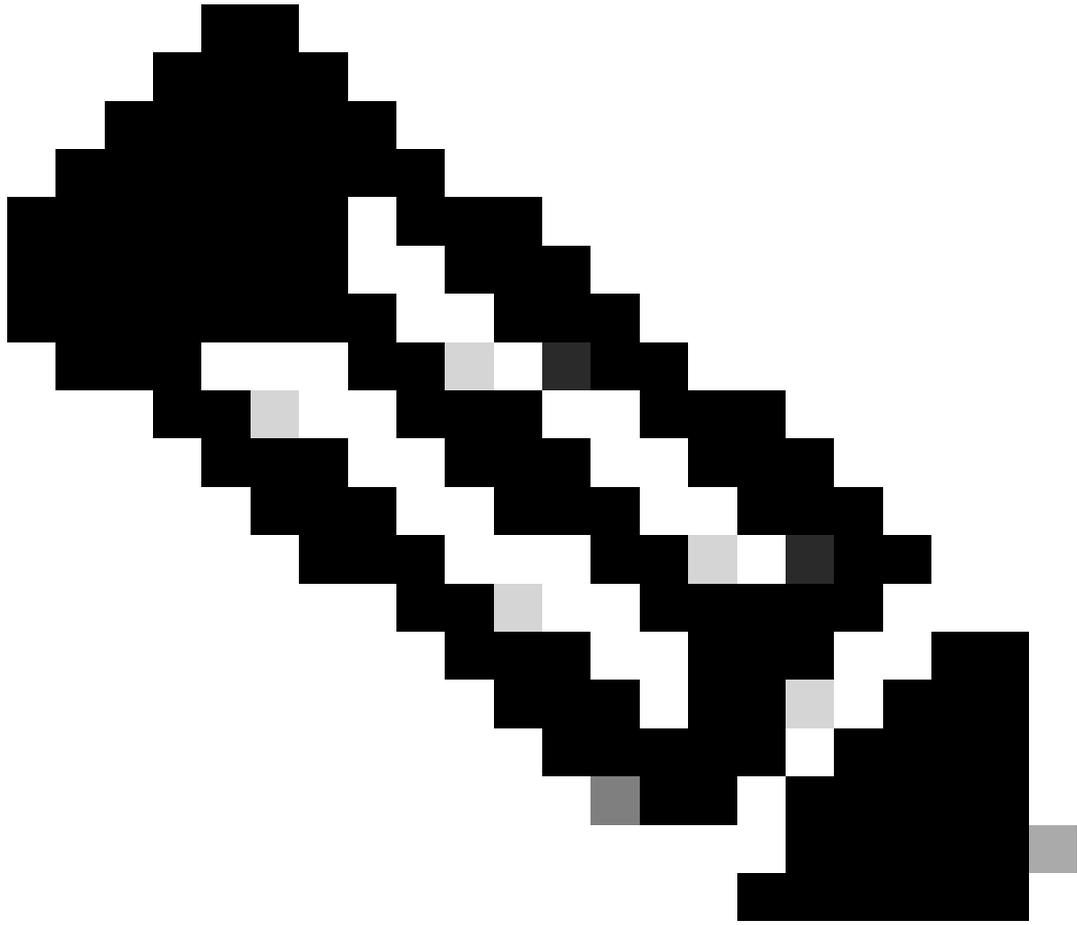
Aggiungi, definire un nome e deselezionare Consenti CHAP e Consenti MS-CHAPv1 dall'elenco dei protocolli di autenticazione. Selezionare Salva.

The screenshot shows the Cisco ISE configuration page for the TACACS Protocol. The left sidebar contains a navigation menu with the following items: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Conditions, Network Conditions, Results, Allowed Protocols, TACACS Command Sets, and TACACS Profiles. The main content area is titled 'Allowed Protocols Services List > TACACS Protocol' and 'Allowed Protocols'. It features a form with the following fields: 'Name' (TACACS Protocol), 'Description' (empty text box), and a section titled 'Allowed Protocols' containing 'Authentication Protocols'. Under 'Authentication Protocols', there is a note: 'Only Authentication Protocols relevant to TACACS are displayed.' Below the note are three checkboxes: 'Allow PAP/ASCII' (checked), 'Allow CHAP' (unchecked), and 'Allow MS-CHAPv1' (unchecked).

TACACS - Consenti protocollo

8. Navigare fino a **Aeroporto di Atlanta** Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Fare clic su **+** adde creare due profili in base agli attributi presenti nell'elenco in Raw View. Fare clic su **Save**.

- Utente amministratore: `cisco-av-pair=shell:domains=all/admin/`
- Utente amministratore di sola lettura: `cisco-av-pair=shell:domains=all/read-all`



Nota: In caso di spazio o caratteri aggiuntivi, la fase di autorizzazione ha esito negativo.

---

Conditions >

Network Conditions >

Results ▾

- Allowed Protocols
- TACACS Command Sets
- TACACS Profiles**

[TACACS Profiles](#) > APIC ReadWrite Profile

### TACACS Profile

Name  
**APIC ReadWrite Profile**

---

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel
Save

Profilo TACACS

Overview

Identities

User Identity Groups

Ext Id Sources

**Network Resources**

Conditions >

Network Conditions >

Results ▾

- Allowed Protocols
- TACACS Command Sets
- TACACS Profiles**

## TACACS Profiles

↻
Add
Duplicate
Trash ▾
Edit

|                          | Name                   | Type  | Description |
|--------------------------|------------------------|-------|-------------|
| <input type="checkbox"/> | APIC ReadOnly Profile  | Shell |             |
| <input type="checkbox"/> | APIC ReadWrite Profile | Shell |             |

Profili Amministratore TACACS e Amministratore di sola lettura

Passaggio 9. Navigare fino a recentemente > Work Centers > Device Administration > Device Admin Policy Set. Creare un nuovo set di criteri, definire un nome e scegliere il tipo di dispositivo APIC creato nel passaggio 1. Scegliere TACACS Protocol creato nel passaggio 7. come protocollo consentito, quindi fare clic su Save.

Policy Sets Reset [Reset Policyset Hitcounts](#) [Save](#)

| Status                               | Policy Set Name | Description | Conditions                                      | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------------------------------------|-----------------|-------------|---|-------------------------------------|------|---------|------|
| <span style="color: green;">●</span> | APIC            |             | DEVICE-Device Type EQUALS All Device Types#APIC | TACACS Protocol                     | 55   |         |      |

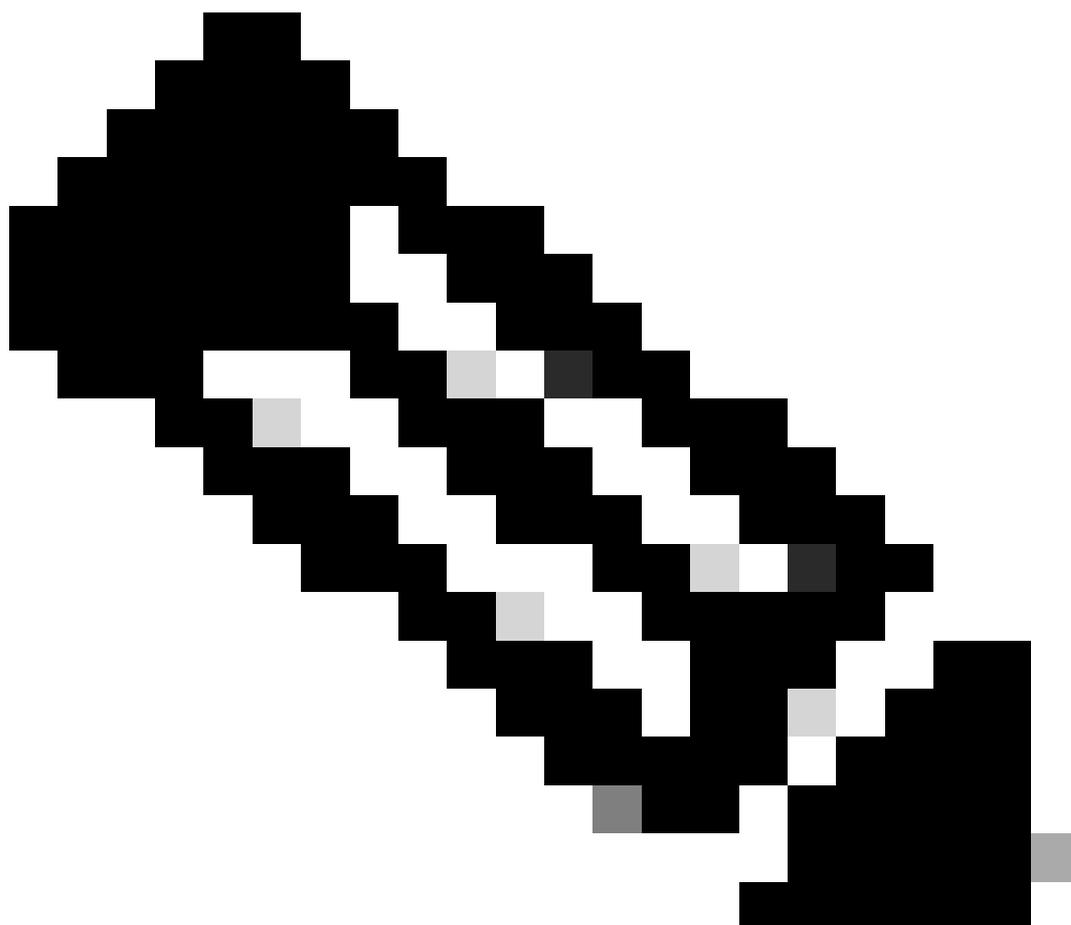
### Set di criteri TACACS

Passaggio 10. In Nuovo Policy Set fare clic sulla freccia destra > e creare un criterio di autenticazione. Definite un nome e scegliete l'indirizzo IP del dispositivo come condizione. Scegliere quindi la sequenza di origine delle identità creata al passo 6.

Authentication Policy (2)

| Status                               | Rule Name                  | Conditions                                     | Use      | Hits | Actions |
|--------------------------------------|----------------------------|--|----------|------|---------|
| <span style="color: green;">●</span> | APIC Authentication Policy | Network Access Device IP Address EQUALS 188.21 | APIC_ISS | 55   | Options |

### Criterio di autenticazione



Nota: La posizione o altri attributi possono essere utilizzati come condizione di autenticazione.

Passaggio 11. Creare un profilo di autorizzazione per ogni tipo di utente Amministratore, definire un nome e scegliere un utente interno e/o un gruppo di utenti AD come condizione. È possibile utilizzare condizioni aggiuntive, ad esempio APIC. Scegliere il profilo della shell appropriato in ogni criterio di autorizzazione e fare clic su Save.

Authorization Policy (3)

| Status | Rule Name       | Conditions   | Results | Command Sets    | Shell Profiles         | Hits | Actions |
|--------|-----------------|--|---------|-----------------|------------------------|------|---------|
| ON     | APIC Admin RO   | AND<br>Network Access Device IP Address EQUALS .188.21<br>IdentityGroup-Name EQUALS User Identity Groups:APIC_RO   |         |                 | APIC ReadOnly Profile  | 34   |         |
| ON     | APIC Admin User | AND<br>Network Access Device IP Address EQUALS .188.21<br>OR<br>IdentityGroup-Name EQUALS User Identity Groups:APIC_RW<br>IsExternalGroups EQUALS cisco:lab/Bullfin/Administrators |         |                 | APIC ReadWrite Profile | 16   |         |
| ON     | Default         |  |         | DenyAllCommands | Deny All Shell Profile | 0    |         |

Profilo di autorizzazione TACACS

## Verifica

Passaggio 1. Accedere all'interfaccia utente APIC con le credenziali User Admin. Selezionare l'opzione TACACS dall'elenco.

APIC  
Version 4.2(7u)  
CISCO

User ID  
APIC\_ROUser

Password  
.....

Domain  
S\_TACACS

Login

Log in APIC

Passaggio 2. Verificare l'accesso sull'interfaccia utente APIC e l'applicazione dei criteri appropriati ai log TACACS Live.

# Welcome to APIC

What's new in version 4.2(7u)



## New Features

- Floating L3out
  - Docker EE (Kubernetes) container integration
  - L4-L7 Services support in vPod
  - Backup PBR destination
  - Support for 64 Remote Leaf pairs
- UI Enhancements:
    - User-defined UI banner
    - First Time Setup wizard
    - Simplified L3Out creation
    - EPG to leafs deployment view

[View Release Notes](#)

### Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

### Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

### Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

messaggio di benvenuto APIC

Ripetere i passaggi 1 e 2 per gli utenti Amministratore di sola lettura.

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

| Logged Time                | Status | Details | Identity    | Type          | Authentication Policy             | Authorization Policy  | Ise Node | Network Devic...    |
|----------------------------|--------|---------|-------------|---------------|-----------------------------------|-----------------------|----------|---------------------|
| ×                          | ▼      |         | Identity    | ▼             | Authentication Policy             | Authorization Policy  | Ise Node | Network Device N... |
| Apr 20, 2023 10:14:42.4... | ✓      | 🔒       | APIC_ROUser | Authorizat... |                                   | APIC >> APIC Admin RO | PAN32    | APIC-LAB            |
| Apr 20, 2023 10:14:42.2... | ✓      | 🔒       | APIC_ROUser | Authentic...  | APIC >> APIC Authentication Po... |                       | PAN32    | APIC-LAB            |

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

Log TACACS+ Live

## Risoluzione dei problemi

Passaggio 1. Navigare fino a Android > Operations > Troubleshoot > Debug Wizard. Selezionare TACACS e fare clic su Debug Nodes.

# Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

| <input type="checkbox"/>            | Name                      | Description               | Status   |
|-------------------------------------|---------------------------|---------------------------|----------|
| <input type="checkbox"/>            | 802.1X/MAB                | 802.1X/MAB                | DISABLED |
| <input type="checkbox"/>            | Active Directory          | Active Directory          | DISABLED |
| <input type="checkbox"/>            | Application Server Issues | Application Server Issues | DISABLED |
| <input type="checkbox"/>            | BYOD portal/Onboarding    | BYOD portal/Onboarding    | DISABLED |
| <input type="checkbox"/>            | Context Visibility        | Context Visibility        | DISABLED |
| <input type="checkbox"/>            | Guest portal              | Guest portal              | DISABLED |
| <input type="checkbox"/>            | Licensing                 | Licensing                 | DISABLED |
| <input type="checkbox"/>            | MnT                       | MnT                       | DISABLED |
| <input type="checkbox"/>            | Posture                   | Posture                   | DISABLED |
| <input type="checkbox"/>            | Profiling                 | Profiling                 | DISABLED |
| <input type="checkbox"/>            | Replication               | Replication               | DISABLED |
| <input checked="" type="checkbox"/> | TACACS                    | TACACS                    | DISABLED |

Configurazione profilo di debug

Passaggio 2. Scegliere il nodo che riceve il traffico e fare clic su **Save**.

Diagnostic Tools   Download Logs   **Debug Wizard**

Debug Profile Configuration  
Debug Log Configuration

Debug Profile Configuration > Debug Nodes

## Debug Nodes

Selected profile **TACACS**

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

 Filter  

| <input type="checkbox"/>            | Host Name           | Persona   | Role           |
|-------------------------------------|---------------------|---|----------------|
| <input checked="" type="checkbox"/> | PAN32.ciscoise.lab  | Administration, Monitoring, Policy Service      | PRI(A), PRI(M) |
| <input type="checkbox"/>            | SPAN32.ciscoise.lab | Administration, Monitoring, Policy Service, ... | SEC(A), SEC(M) |

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

Selezione nodi di debug

Passaggio 3. Eseguire un nuovo test e scaricare i log in **Operations > Troubleshoot > Download logs** come mostrato:

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cab7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

Se nei debug non vengono visualizzate le informazioni di autenticazione e autorizzazione, verificare quanto segue:

1. Il servizio Amministrazione dispositivi è abilitato sul nodo ISE.
2. L'indirizzo IP ISE corretto è stato aggiunto alla configurazione APIC.
3. Se al centro si trova un firewall, verificare che la porta 49 (TACACS) sia autorizzata.

## 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).