Configurazione dell'autenticazione TACACS+ su CIMC con ISE Server

Sommario

Introduzione

Questo documento descrive la configurazione dell'autenticazione Access-Control System Plus (TACACS+) di Terminal Access Controller su Cisco Integrated Management Controller (CIMC).

TACACS+ viene comunemente utilizzato per autenticare i dispositivi di rete con un server centrale. Dalla versione 4.1(3b), Cisco IMC supporta l'autenticazione TACACS+. Il supporto TACACS+ su CIMC semplifica la gestione di più account utente che hanno accesso al dispositivo. Questa funzionalità consente di modificare periodicamente le credenziali dell'utente e di gestire gli account utente in remoto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Management Controller (CIMC)
- Access-Control System Plus di Terminal Access Controller (TACACS+)

Componenti usati

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

- UCS-C220-M4S

- Versione CIMC: 4.1, paragrafo 3 ter
- Cisco Identity Services Engine (ISE) versione 3.0.0.458

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

Configurazione lato server TACACS+ per l'associazione dei privilegi

Il livello di privilegio dell'utente viene calcolato in base al valore **cisco-av-**pair configurato per tale utente. È necessario creare una **coppia cisco-av** sul server TACACS+ e gli utenti non possono usare alcun attributo TACACS+ predefinito. Per l'attributo **cisco-av-pair** sono supportate le tre sintassi seguenti

Per il privilegio **admin**:

```
cisco-av-pair=shell:roles="admin"
```

Per il privilegio **utente**:

```
cisco-av-pair=shell:roles="user"
```

Per il privilegio **di sola lettura**:

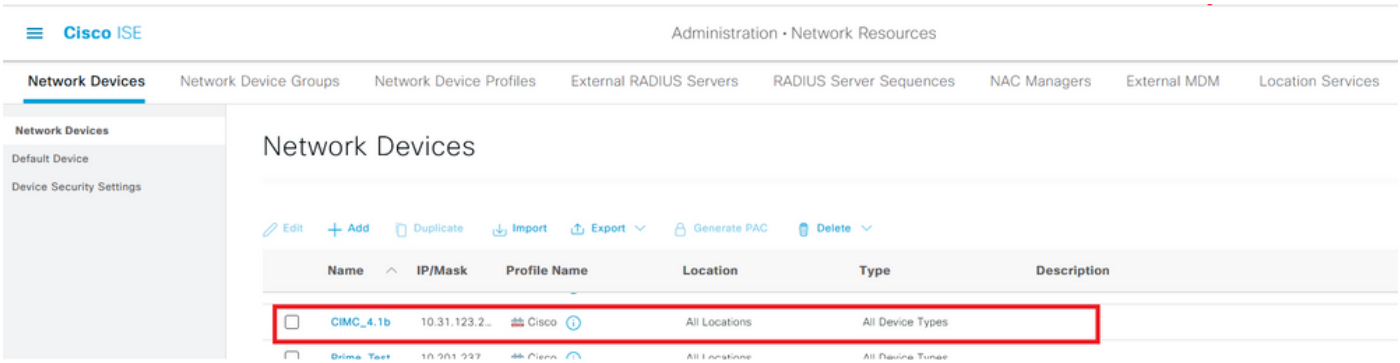
```
cisco-av-pair=shell:roles="read-only"
```

Per supportare altri dispositivi, se è necessario aggiungere altri ruoli, è possibile aggiungerli con una virgola come separatore. Ad esempio, UCSM supporta **aaa**, quindi è possibile configurare **shell:roles="admin,aaa"** e CIMC accetta questo formato.

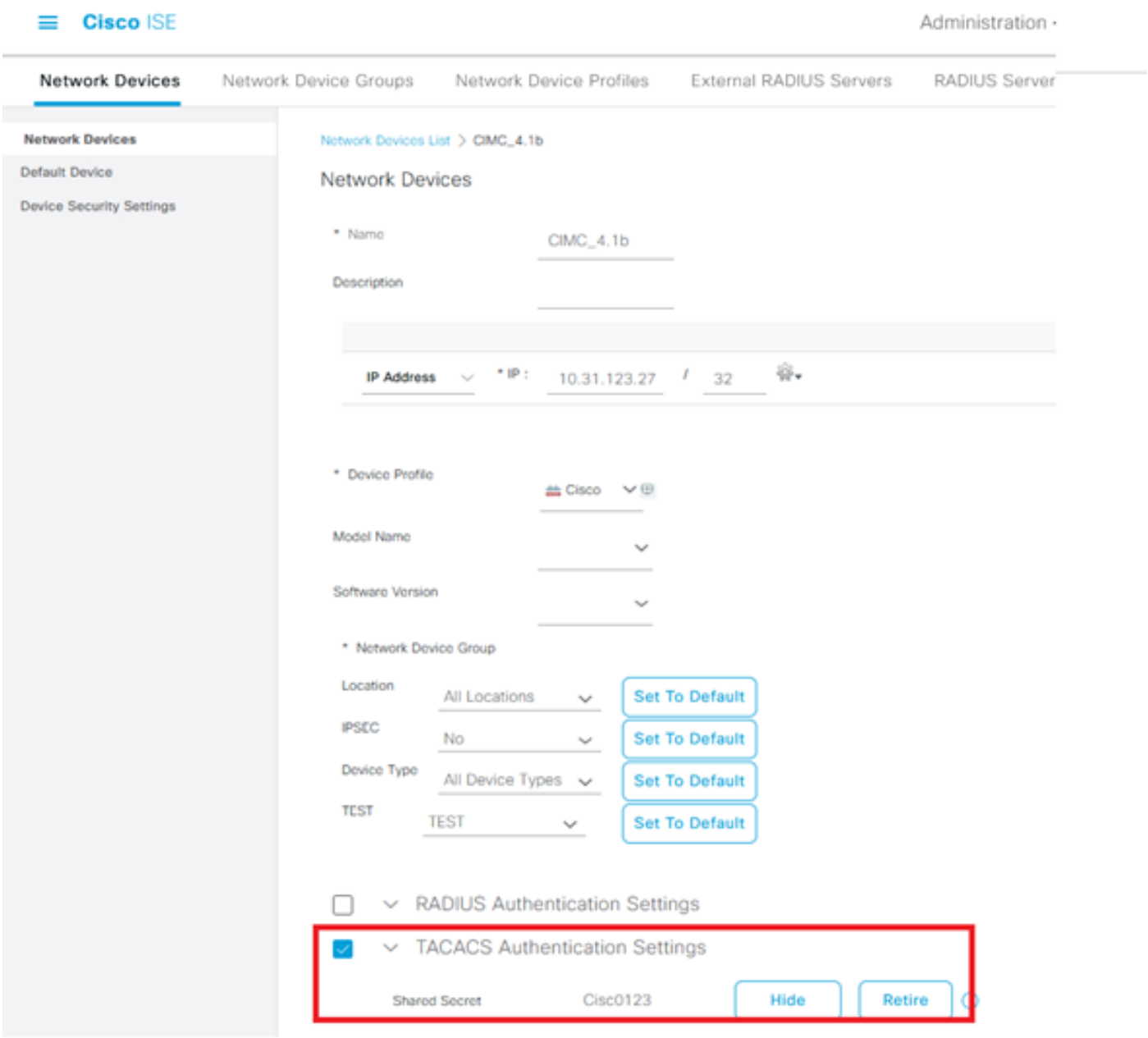
> **Nota:** se **cisco-av-pair** non è configurato sul server TACACS+, un utente con quel server ha un privilegio di **sola lettura**.

Requisiti di configurazione ISE

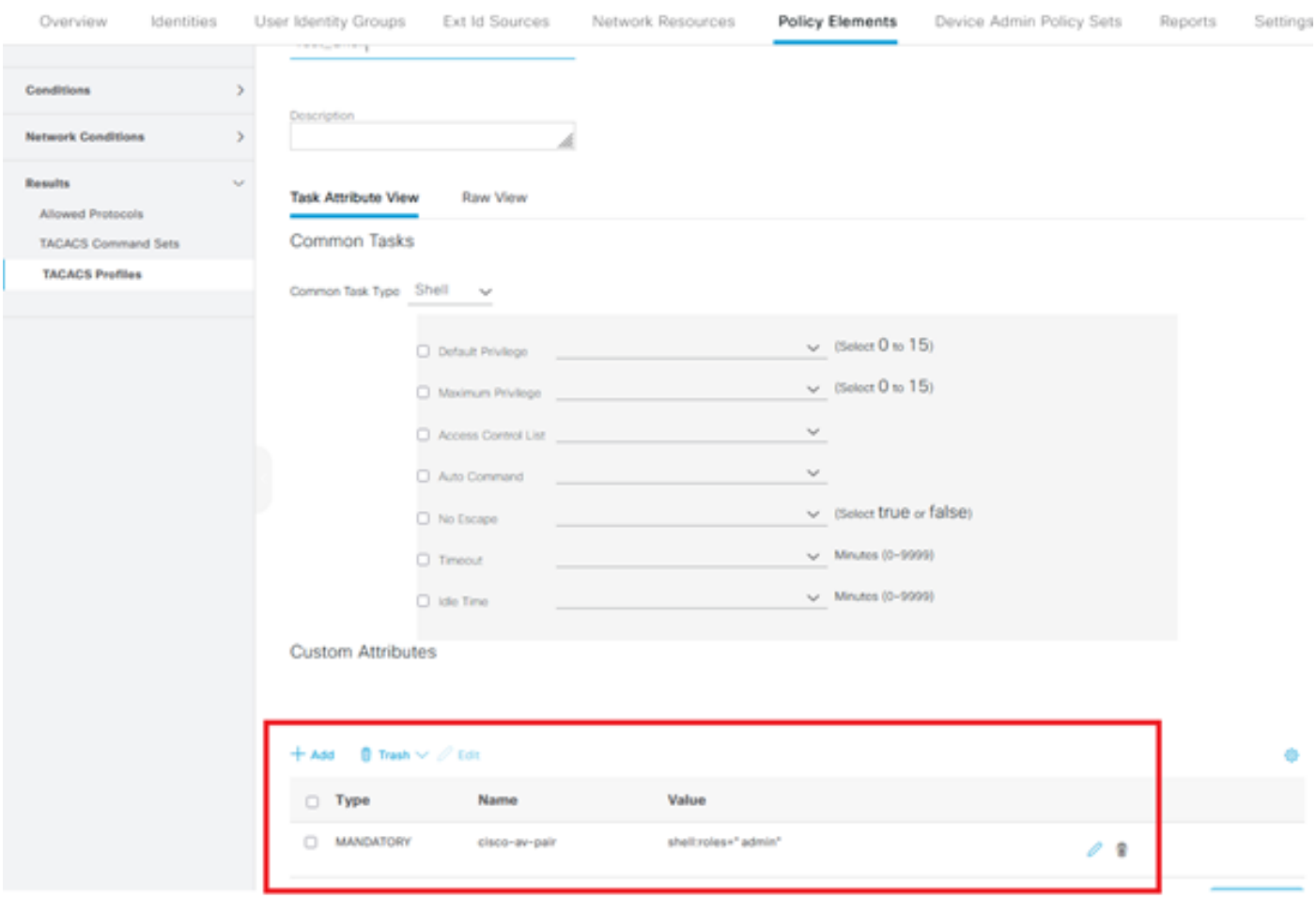
L'IP di gestione del server deve essere consentito sui dispositivi di rete ISE.



Password segreta condivisa da immettere in CIMC.



Shell Profile con attributo **cisco-av-pair** con autorizzazioni di amministratore.

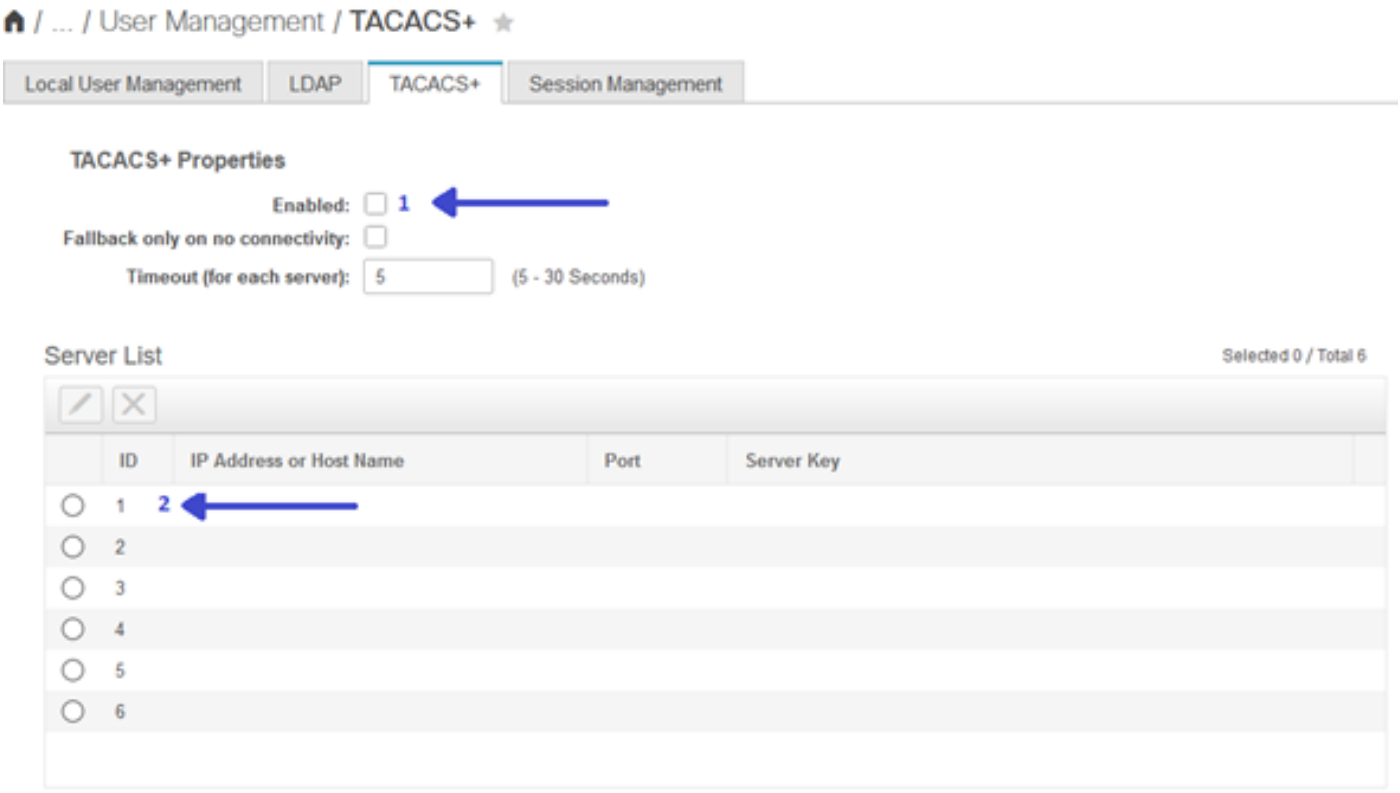


Configurazione TACACS+ su CIMC

Passaggio 1. Selezionare **Admin > User Management > TACACS+**

Passaggio 2. Selezionare la casella di controllo per abilitare **TACACS+**

Passaggio 3. È possibile aggiungere un nuovo server in una delle 6 righe specificate nella tabella. Fate clic sulla riga o selezionatela e fate clic sul pulsante **Modifica** sopra la tabella, come mostrato nell'immagine.

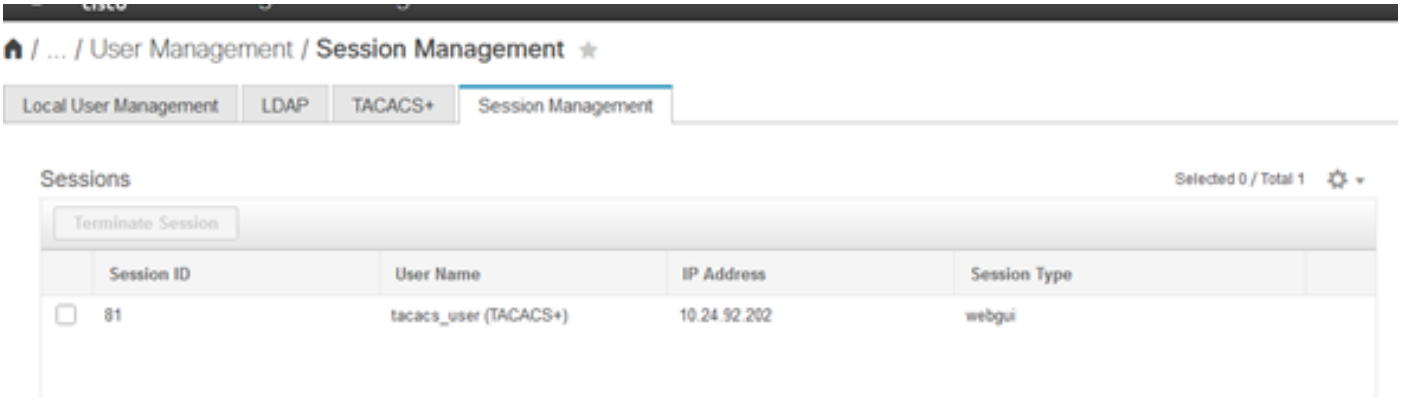


Nota: Nel caso in cui un utente abbia abilitato il fallback di TACACS+ su nessuna opzione di connettività, CIMC applica che la priorità della prima autenticazione deve sempre essere impostata su TACACS+ altrimenti la configurazione del fallback potrebbe diventare irrilevante.

Passaggio 4. Inserire l'indirizzo IP o il nome host, la porta e la chiave del server/il segreto condiviso e **salvare** la configurazione.

Cisco IMC supporta fino a sei server remoti TACACS+. Una volta completata l'autenticazione, al nome utente viene aggiunto (TACACS+).

Questa condizione viene visualizzata anche in Gestione sessioni



Verifica

- Èpossibile configurare un massimo di 6 server TACACS+ sul CIMC.
- La lunghezza massima della chiave segreta associata al server è 64 caratteri.
- Il timeout può essere configurato tra 5 e 30 secondi (il che corrisponde al massimo a 180 secondi per essere in linea con LDAP).
- Se un server TACACS+ deve usare il nome del servizio per creare **cisco-av-pair**, gli utenti devono usare **Log in** come nome del servizio.
- Nessun supporto per lo scorfano per modificare le configurazioni.

Verifica della configurazione dalla CLI in CIMC

- Verificare se TACACS+ è abilitato.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- Verificare i dettagli di configurazione per server.

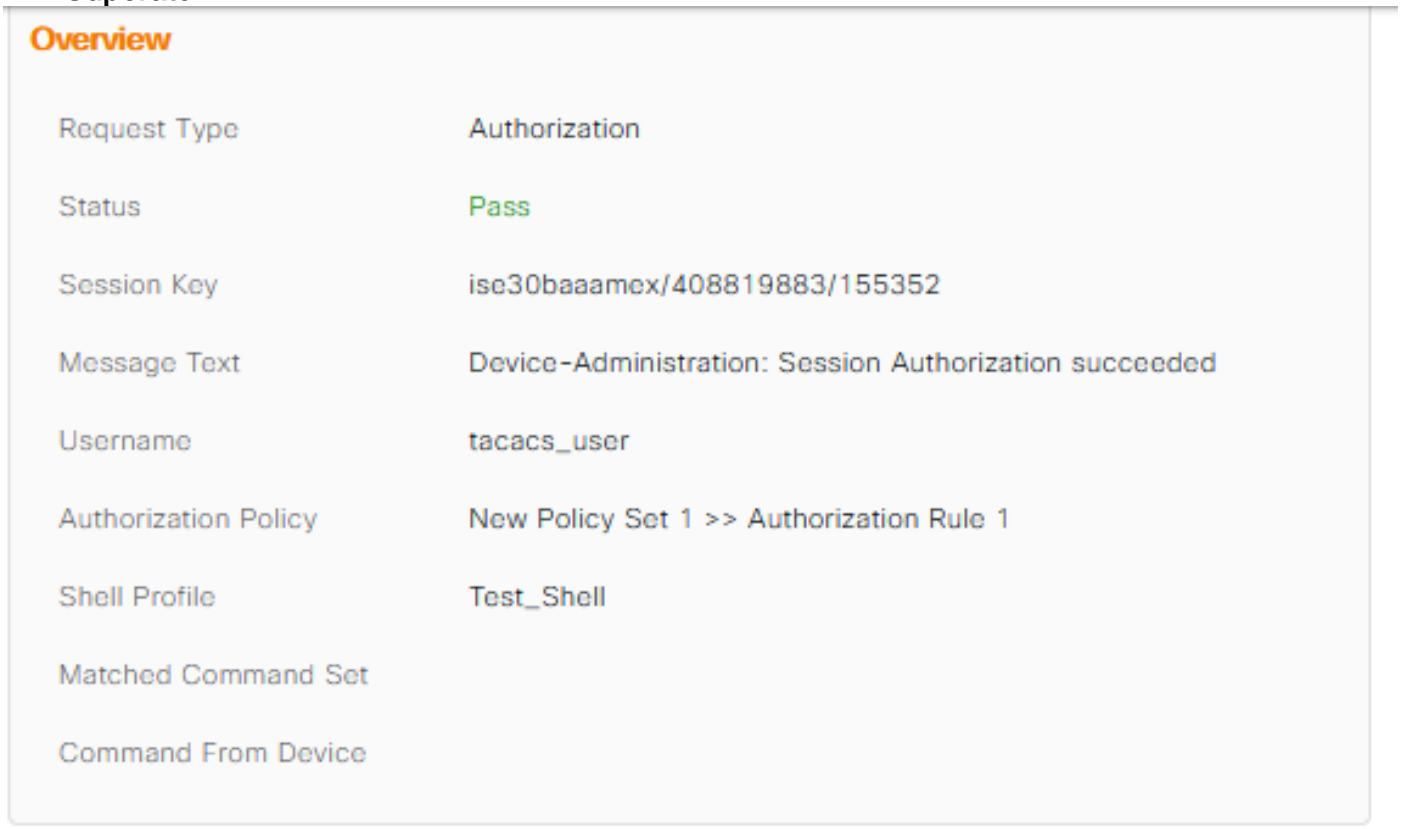
```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: ******
Server Port: 49
```

Risoluzione dei problemi

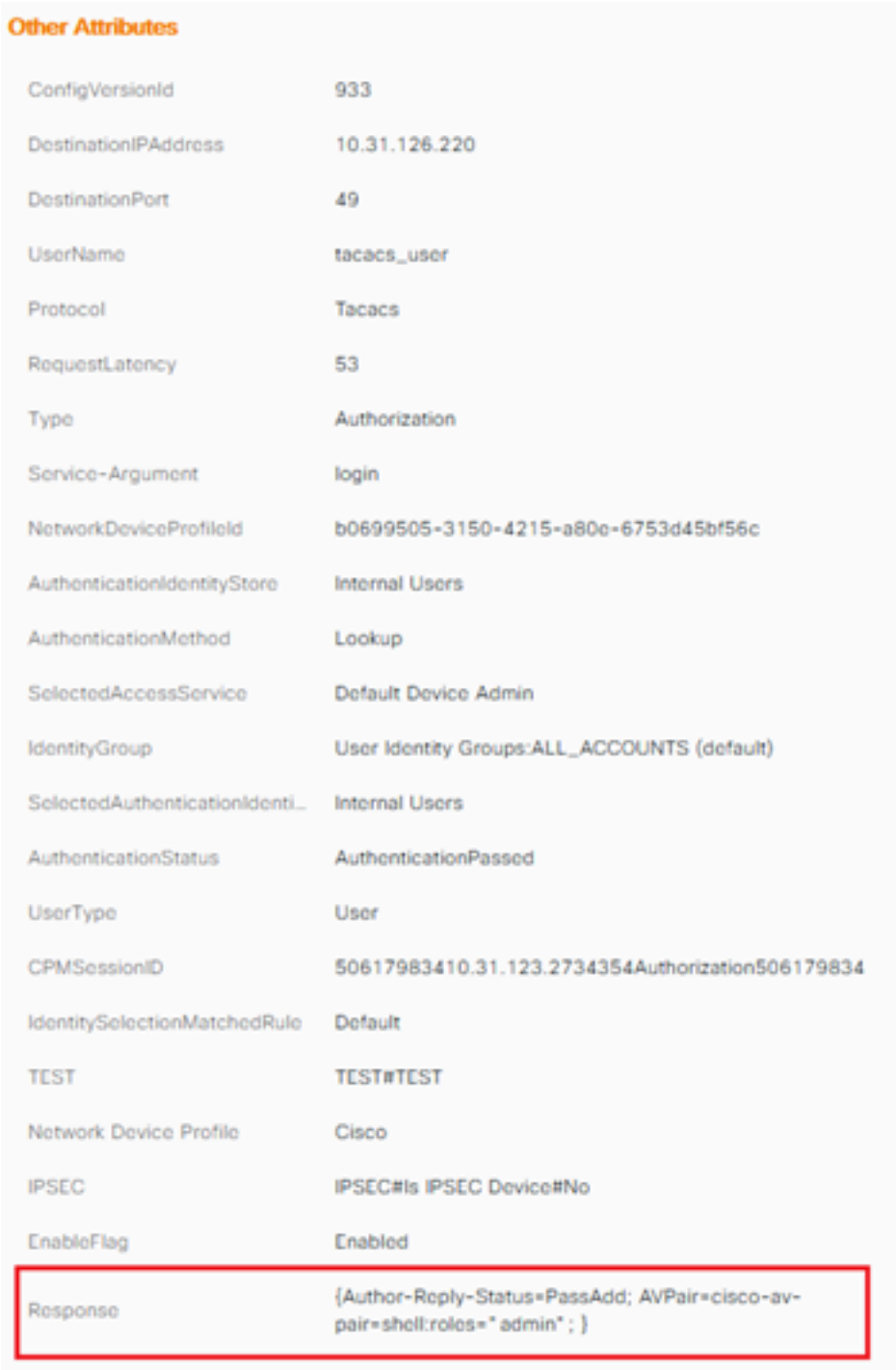
- Verificare che TACACS+ Server IP sia raggiungibile dal CIMC e che la porta sia configurata correttamente.
- Verificare che la **coppia cisco-av** sia configurata correttamente sul server TACACS+.
- Verificare che il server TACACS+ sia raggiungibile (IP e porta).
- Verificare che la chiave segreta o le credenziali corrispondano a quelle configurate sul server TACACS+.
- Se è possibile accedere con TACACS+ ma si hanno solo autorizzazioni di **sola lettura**, verificare se cisco-av-pair ha la sintassi corretta sul server TACACS+.

Risoluzione dei problemi ISE

- Verificare i registri Tacacs Live per uno dei tentativi di autenticazione. Lo stato deve essere **Superato**.



- Verificare che per la risposta sia configurato l'attributo **cisco-av-pair** corretto.



Informazioni correlate

- Autenticazione TACACS+ Cisco UCS-C
- Documentazione e supporto tecnico – Cisco Systems
- Configurare ISE 2.0: Autenticazione e autorizzazione dei comandi IOS TACACS+ in base all'appartenenza al gruppo AD