Configurazione di ISE come autenticazione esterna per l'interfaccia grafica DNAC

Sommario

Introduzione

Questo documento descrive come configurare Cisco Identity Services Engine (ISE) come autenticazione esterna per l'amministrazione della GUI di Cisco DNA Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- protocolli TACACS+ e RADIUS.
- CISCO ISE Integration con Cisco DNA Center.
- Cisco ISE Policy Evaluation.

Componenti usati

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

- Cisco Identity Services Engine (ISE) versione 3.4 Patch1.

- Cisco DNA Center versione 2.3.5.5.

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.

Operazioni preliminari

- Verificare che almeno un server di autenticazione RADIUS sia configurato in System > Settings > External Services > Authentication and Policy Server.
- Questa procedura può essere eseguita solo da un utente con autorizzazioni SUPER-ADMIN-ROLE su DNAC.
- Abilita fallback autenticazione esterna.

⚠ Attenzione: Nelle versioni precedenti alla 2.1.x, quando l'autenticazione esterna è abilitata, Cisco DNA Center restituisce il server agli utenti locali se il server AAA non è raggiungibile o se il server AAA rifiuta un nome utente sconosciuto. Nella versione corrente, Cisco DNA Center non esegue il fallback agli utenti locali se il server AAA non è raggiungibile o se il server AAA rifiuta un nome utente sconosciuto. Quando il fallback dell'autenticazione esterna è abilitato, gli utenti esterni e gli amministratori locali possono accedere a Cisco DNA Center.

Per abilitare il fallback dell'autenticazione esterna, SSH sull'istanza di Cisco DNA Center e immettere il comando this CLI (magctl rbac external_auth_fallback enable).

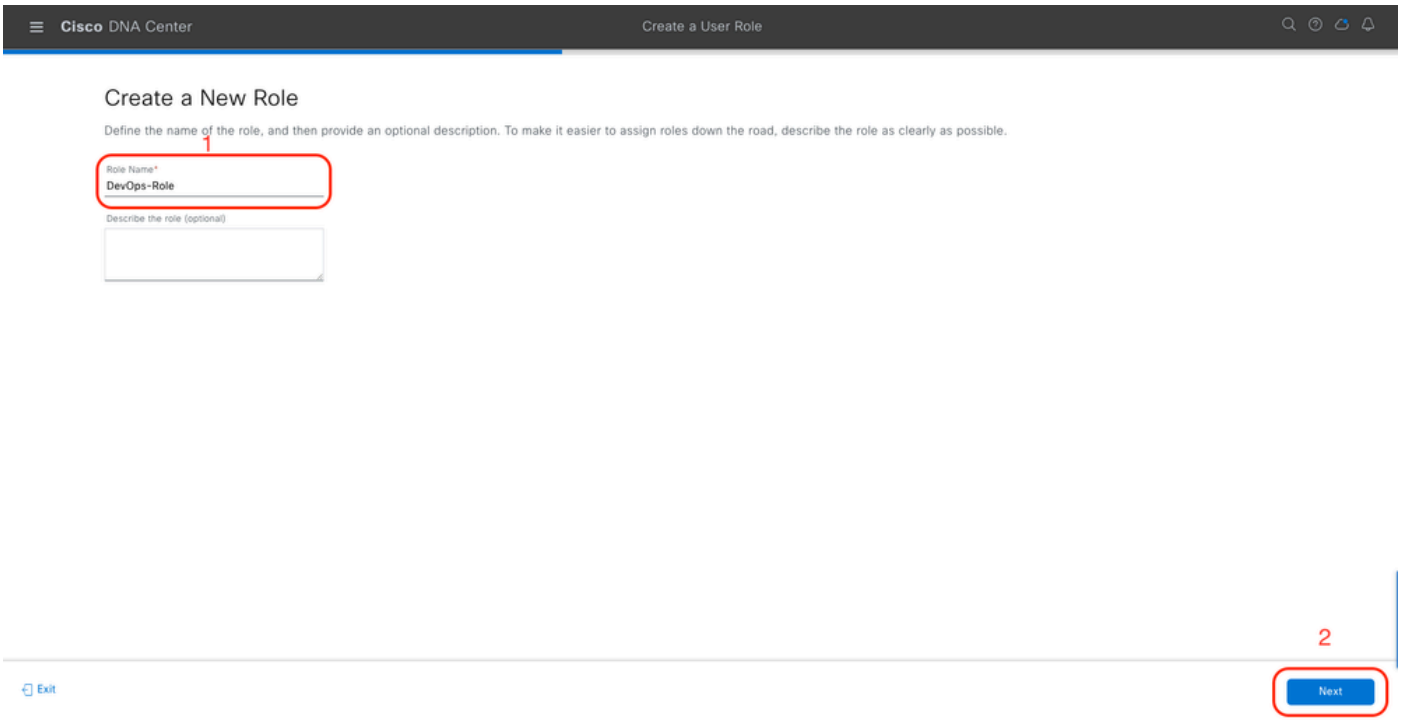
Configurazione

(Opzione1) Configurazione dell'autenticazione esterna DNAC tramite RADIUS

Passaggio 1. (Facoltativo) Definire un ruolo personalizzato.
Configurare i ruoli personalizzati che soddisfano i requisiti, è possibile utilizzare i ruoli utente predefiniti. A tale scopo, è possibile utilizzare la scheda Sistema > Utenti e ruoli > Controllo di accesso basato su ruoli.

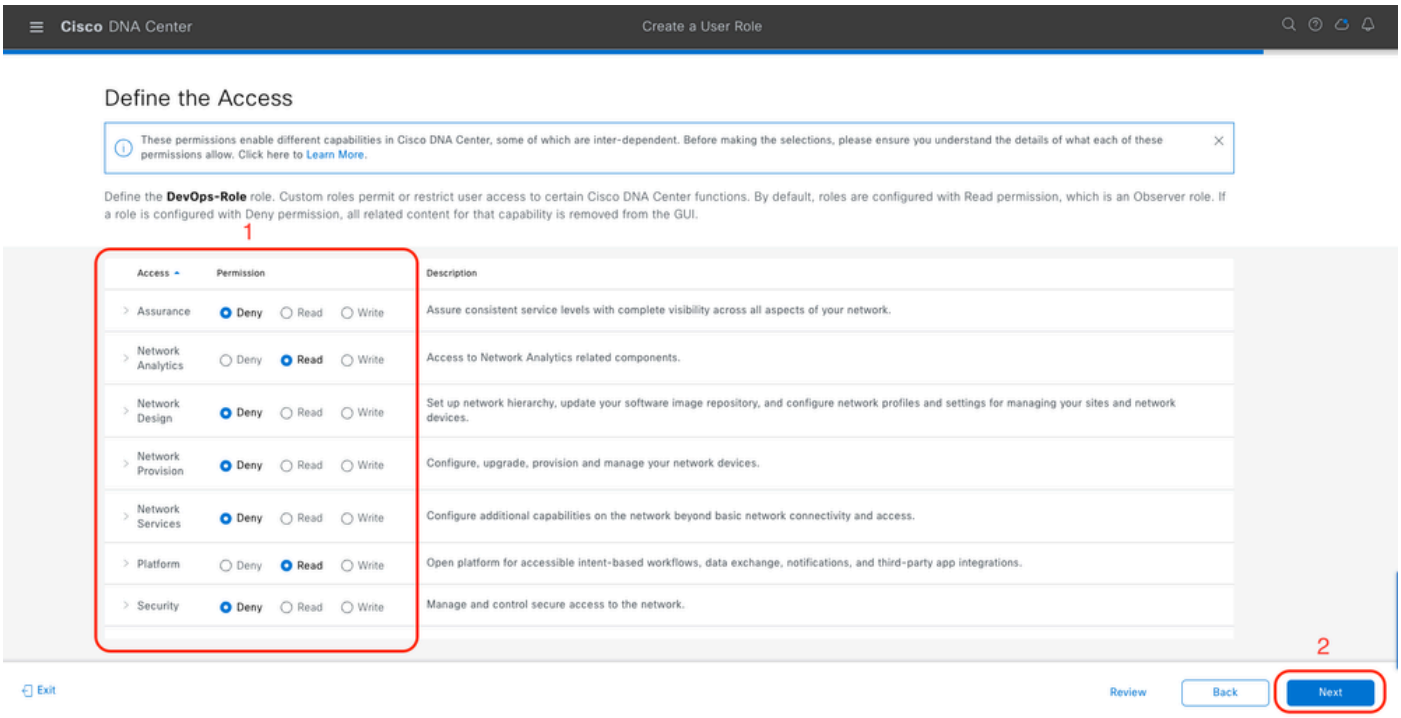
Procedura

r. Creare un nuovo ruolo.



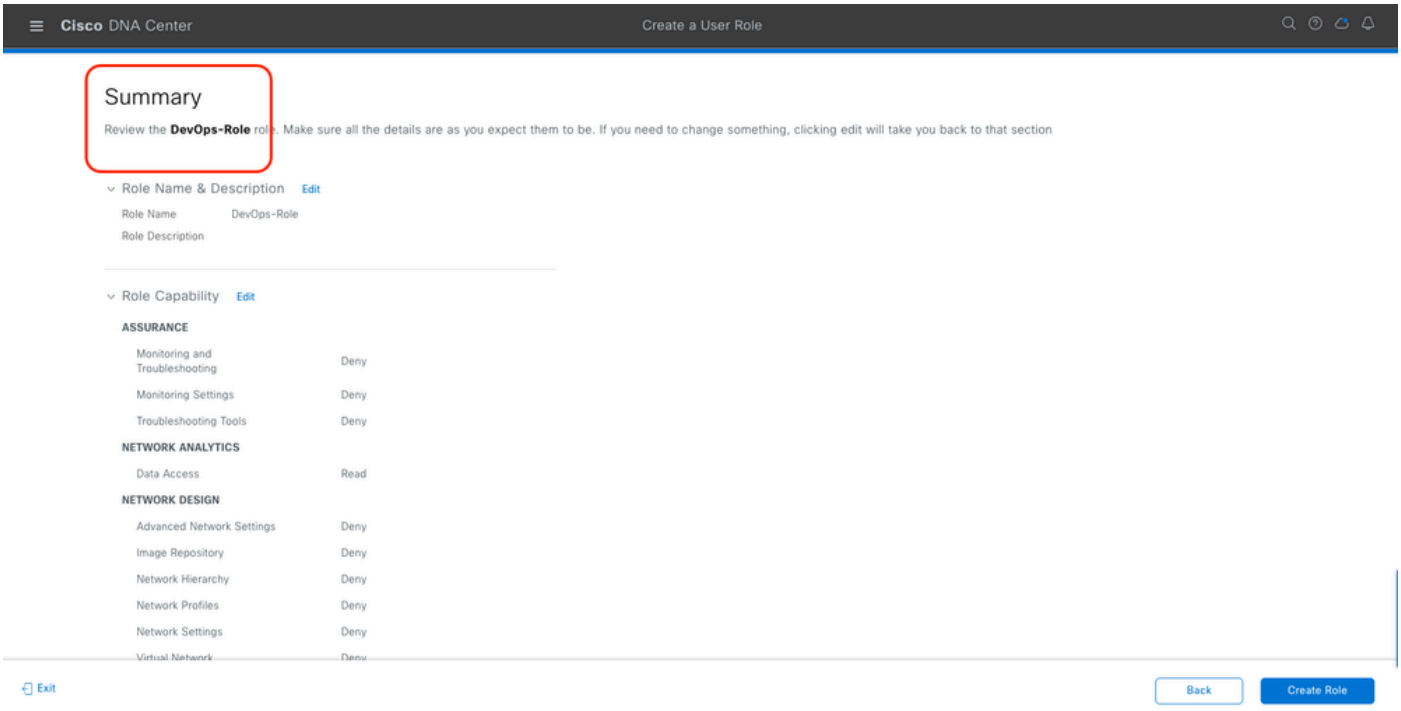
Nome ruolo DevOps

b. Definire l'accesso.

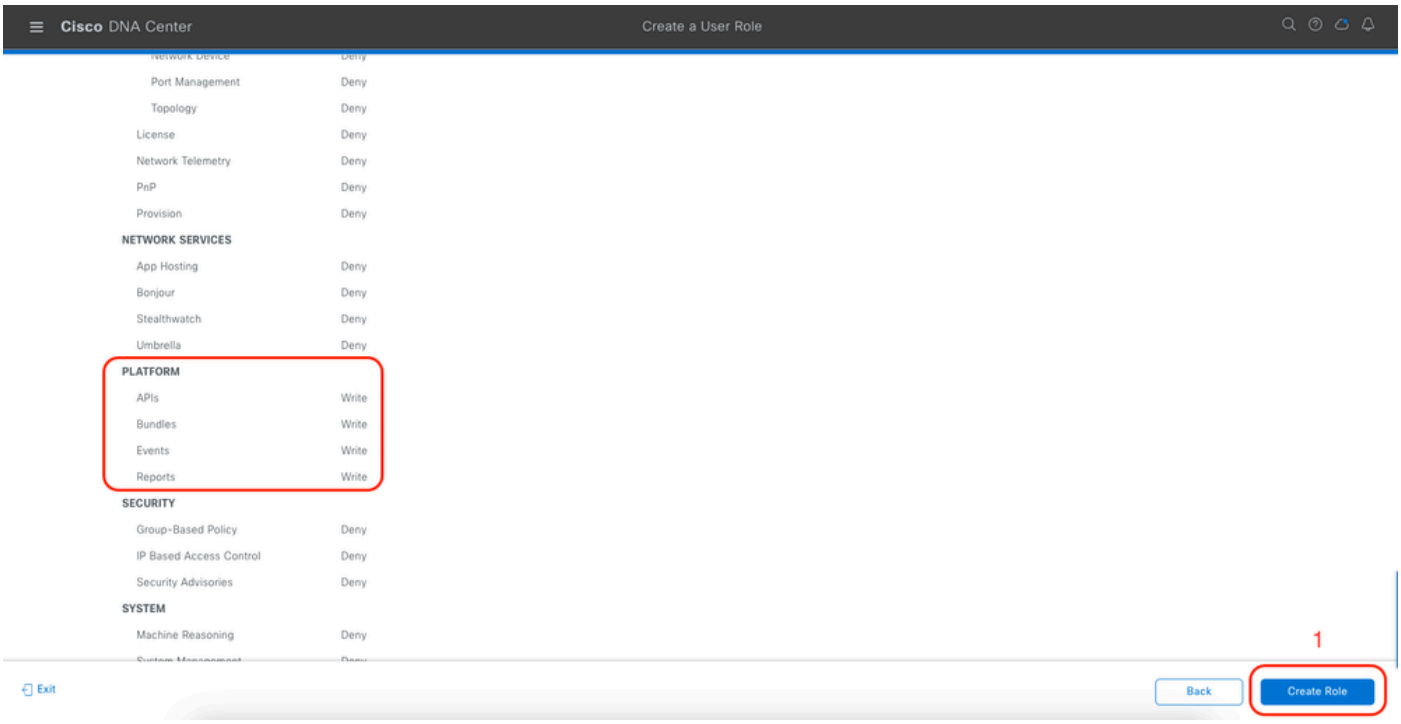


Accesso al ruolo DevOps

c. Creare il nuovo ruolo.



Riepilogo ruolo DevOps



Verifica e crea ruolo DevOps

Passaggio 2. Configurare l'autenticazione esterna utilizzando RADIUS.
A tale scopo, è possibile selezionare la scheda Sistema > Utenti e ruoli > Autenticazione esterna.

Procedura

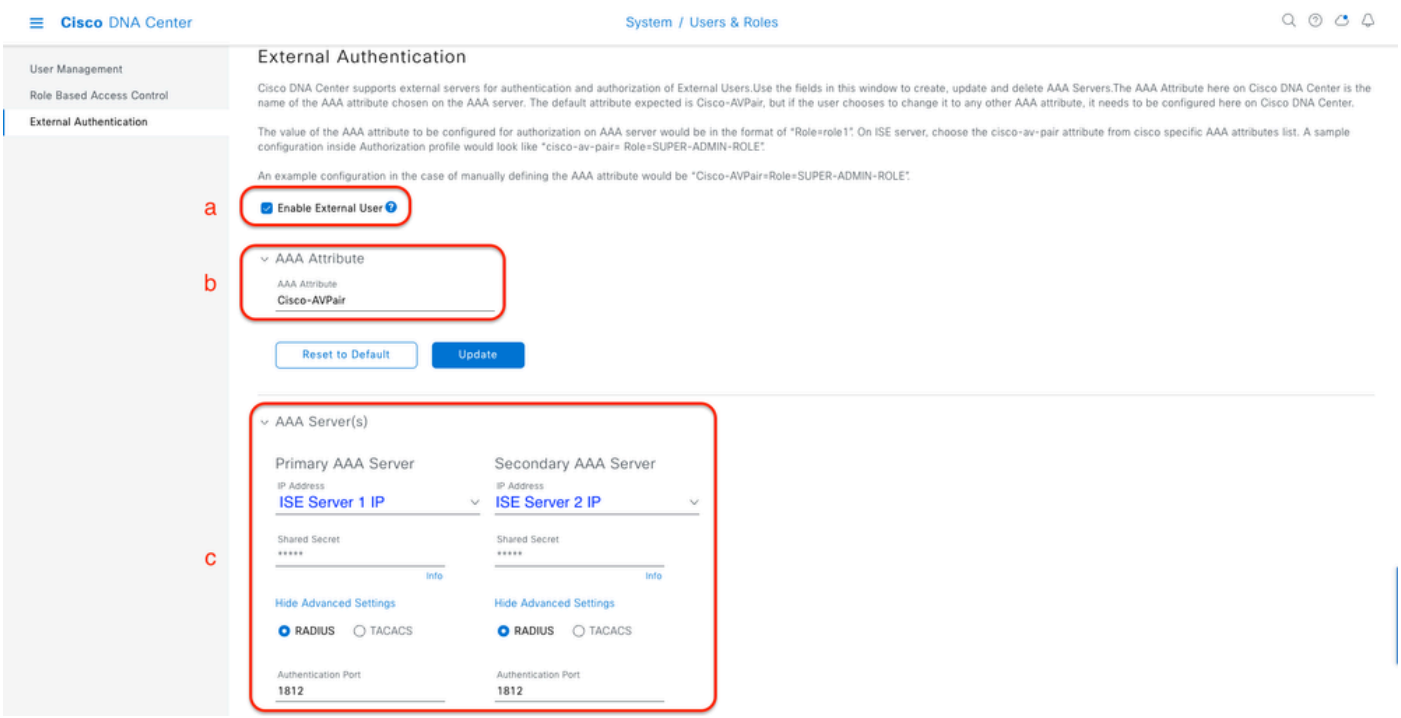
r. Per abilitare l'autenticazione esterna in Cisco DNA Center, selezionare la casella di controllo Abilita utente esterno.

b. Impostare gli attributi AAA.

Immettere Cisco-AVPair nel campo AAA Attributes (Attributi AAA).

c. (Facoltativo) Configurare il server AAA primario e secondario.

Verificare che il protocollo RADIUS sia abilitato sul server AAA primario o almeno sul server primario e secondario.



(RADIUS) Procedura di configurazione dell'autenticazione esterna

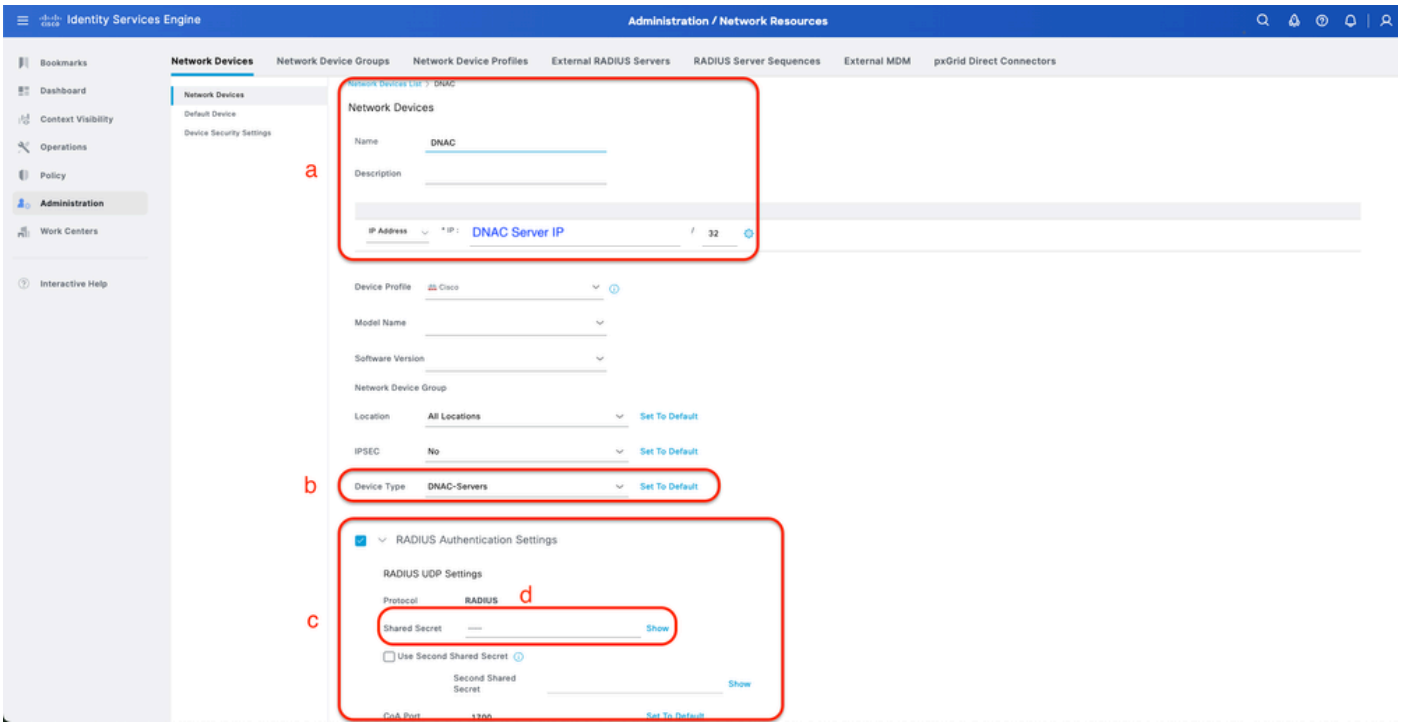
(Opzione 1) Configurare ISE per RADIUS

Passaggio 1. Aggiungere un server DNAC come dispositivo di rete su ISE.

A tale scopo, selezionare la scheda Amministrazione > Risorse di rete > Dispositivi di rete.

Procedura

r. Definire il nome e l'indirizzo IP del dispositivo di rete (DNAC).
b. (Facoltativo) Classificare il tipo di dispositivo per la condizione Set di criteri.
c. Abilitare le impostazioni di autenticazione RADIUS.
d. Imposta il segreto condiviso RADIUS.



ISE Network Device (DNAC) per RADIUS

Passaggio 2. Creare profili di autorizzazione RADIUS.

Questa operazione può essere eseguita dalla scheda Criterio > Elementi della policy > Risultati > Autorizzazione > Profili di autorizzazione.

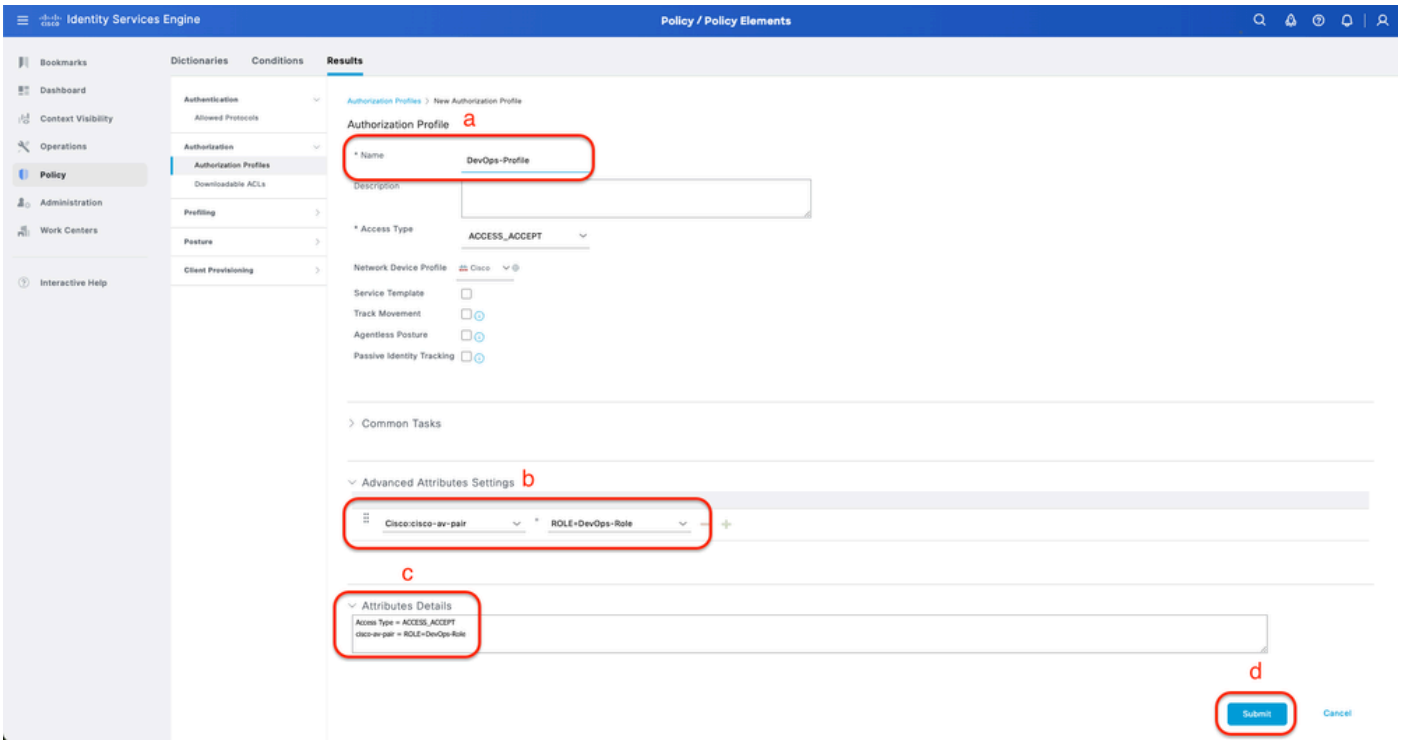
Nota: Creare 3 profili di autorizzazione RADIUS, uno per ogni ruolo utente.

Procedura
a. Fare clic su Aggiungi e definire il nome del profilo di autorizzazione RADIUS.

b. Immettere Cisco:cisco-av-pair nelle impostazioni avanzate degli attributi e specificare il ruolo utente corretto.

- Per il ruolo utente (DecOps-Role), immettere ROLE=DevOps-Role.
- Per il ruolo utente (NETWORK-ADMIN-ROLE), immettere ROLE=NETWORK-ADMIN-ROLE.
- Per il ruolo utente (SUPER-ADMIN-ROLE), immettere ROLE=SUPER-ADMIN-ROLE.

c. Esaminare i dettagli dell'attributo.
d. Fare clic su Save (Salva).



Creazione del profilo di autorizzazione

Passaggio 3. Creazione del gruppo di utenti.

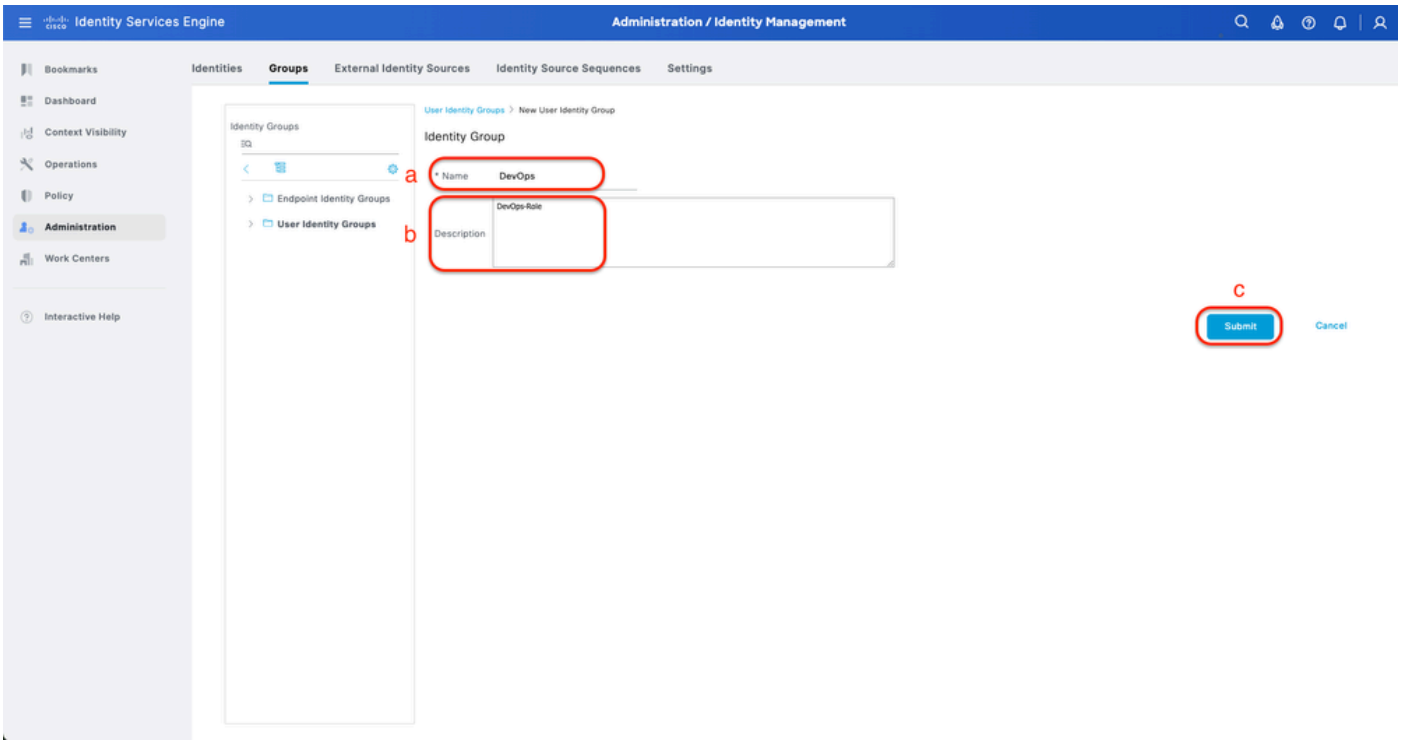
A tale scopo, è possibile utilizzare la scheda Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente.

Procedura

r. Fare clic su Aggiungi e definire il nome del gruppo di identità

b. (Facoltativo) Definire la descrizione.

c. Fare clic su Sottometti.



Crea gruppo di identità utente

Passaggio 4. Creazione dell'utente locale.

A tale scopo, è possibile utilizzare la scheda Amministrazione > Gestione delle identità > Identità > Utenti.

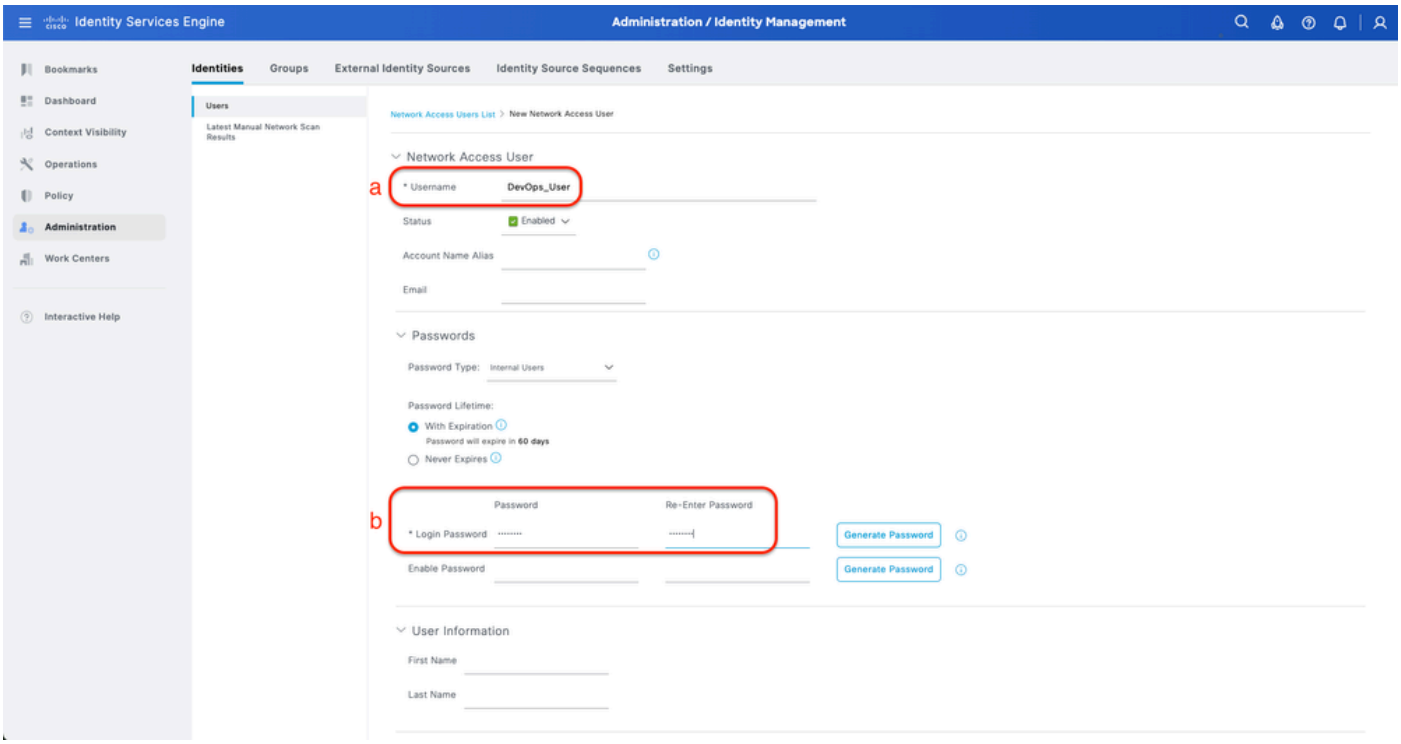
Procedura

r. Fare clic su Add (Aggiungi) e definire il nome utente.

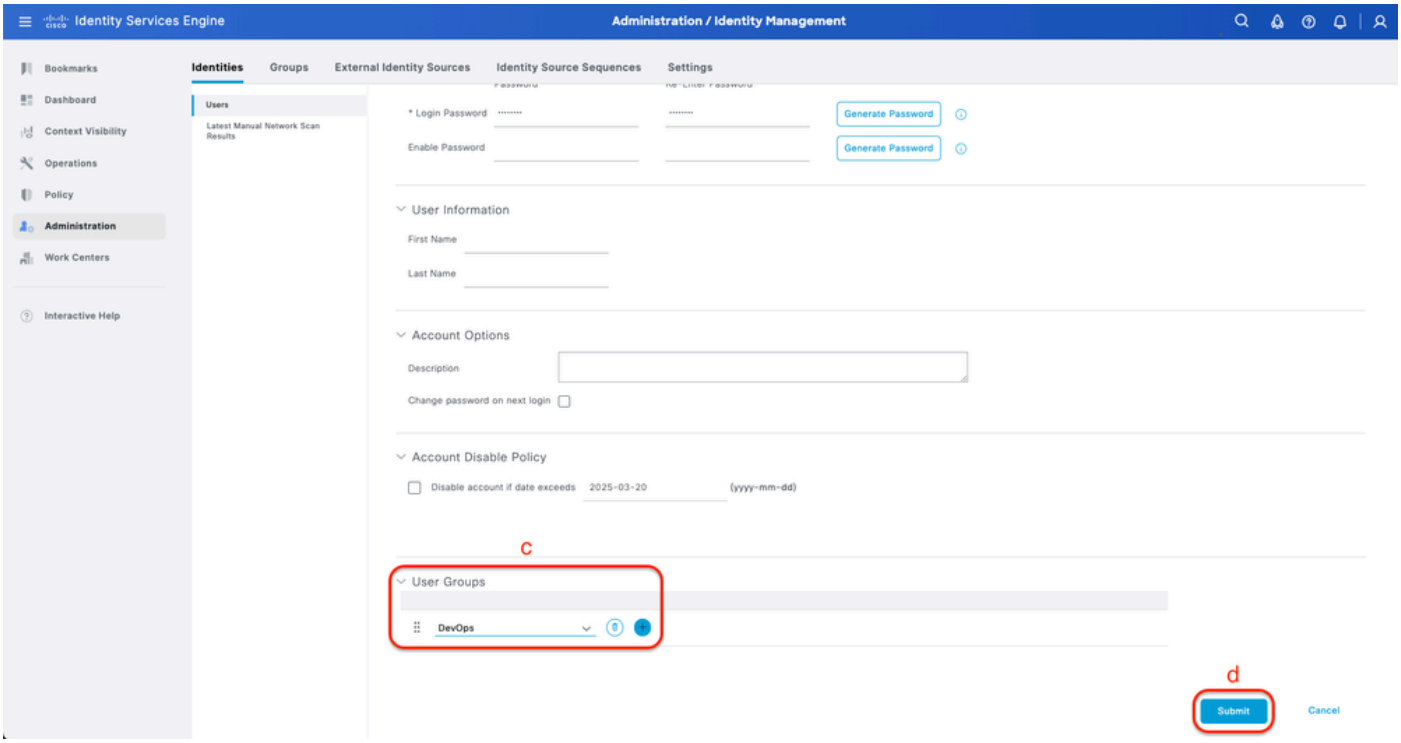
b. Impostare la password di accesso.

c. Aggiungere l'utente al gruppo di utenti correlato.

d. Fare clic su Invia.



Crea utente locale 1-2



Crea utente locale 2-2

Passaggio 5. (Facoltativo) Aggiungere il set di criteri RADIUS.

A tale scopo, è possibile utilizzare la scheda Criteri > Set di criteri.

Procedura

r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

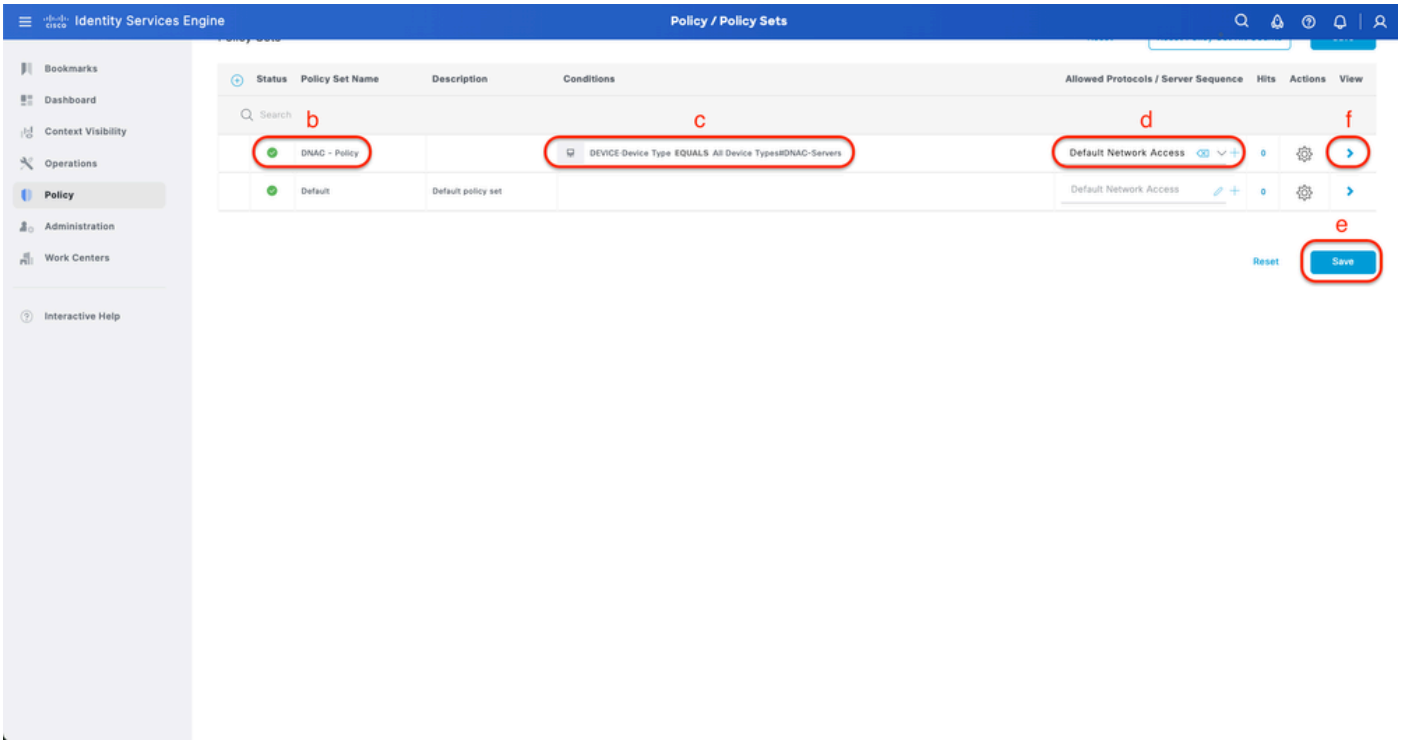
b. Definire il nome del set di criteri.

c. Impostare Policy Set Condition (Condizione di impostazione criteri) su Select Device Type (Seleziona tipo di dispositivo) creato in precedenza (Step1 > b).

d. Impostare i protocolli consentiti.

e. Fare clic su Save (Salva).

f. Fare clic su (>) Visualizzazione set di criteri per configurare le regole di autenticazione e autorizzazione.



Aggiungi set di criteri RADIUS

Passaggio 6. Configurare i criteri di autenticazione RADIUS.

A tale scopo, è possibile utilizzare la scheda Criteri > Set di criteri > Fare clic su (>).

Procedura

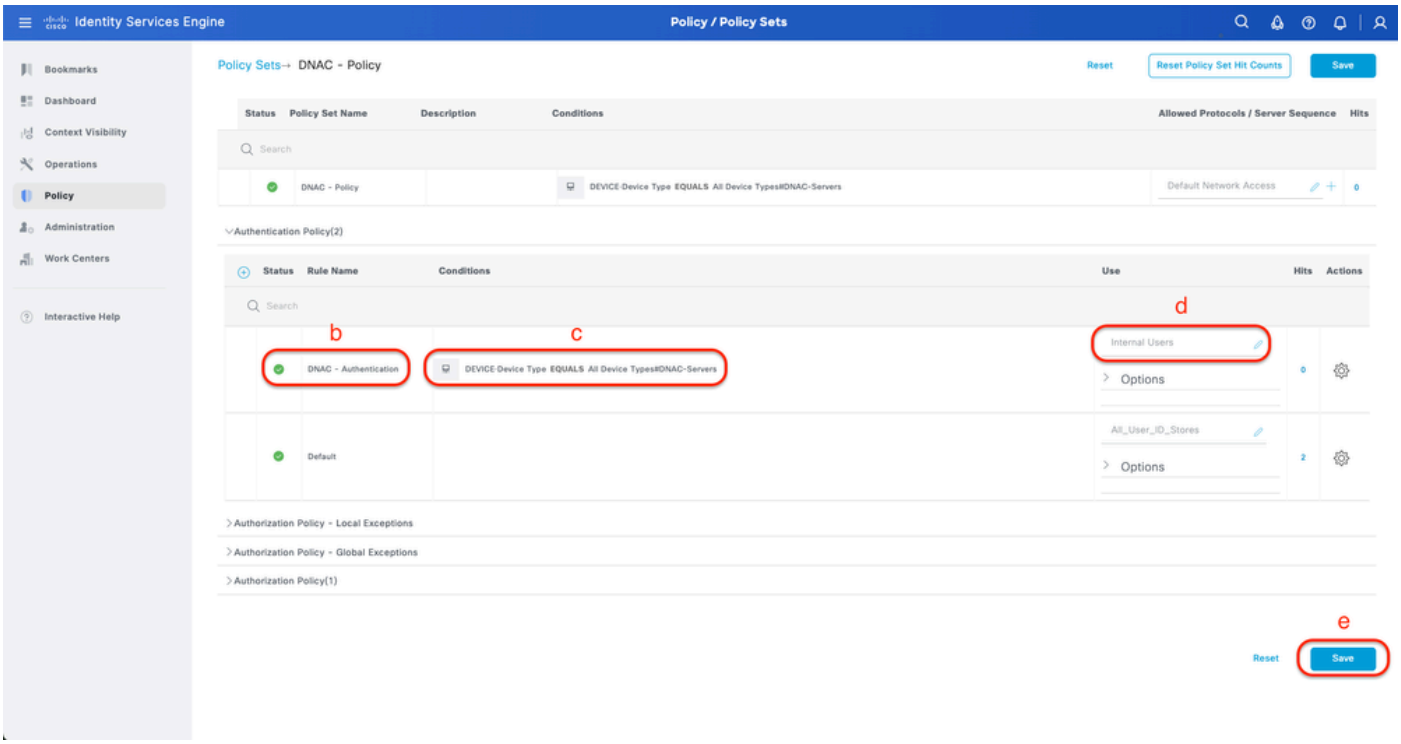
r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

b. Definire il nome del criterio di autenticazione.

c. Impostare la condizione del criterio di autenticazione e selezionare il tipo di dispositivo creato in precedenza (passo 1 > b).

d. Impostare l'utilizzo dei criteri di autenticazione per l'origine identità.

e. Fare clic su Save (Salva).



Aggiungi criterio di autenticazione RADIUS

Passaggio 7. Configurare i criteri di autorizzazione RADIUS.

A tale scopo, è possibile utilizzare la scheda Criteri > Set di criteri > Fare clic su (>).

Questo passaggio consente di creare criteri di autorizzazione per ogni ruolo utente:

- RUOLO DI AMMINISTRATORE PRIVILEGIATO
- RUOLO-AMMINISTRATORE-RETE
- DevOps-Role

Procedura

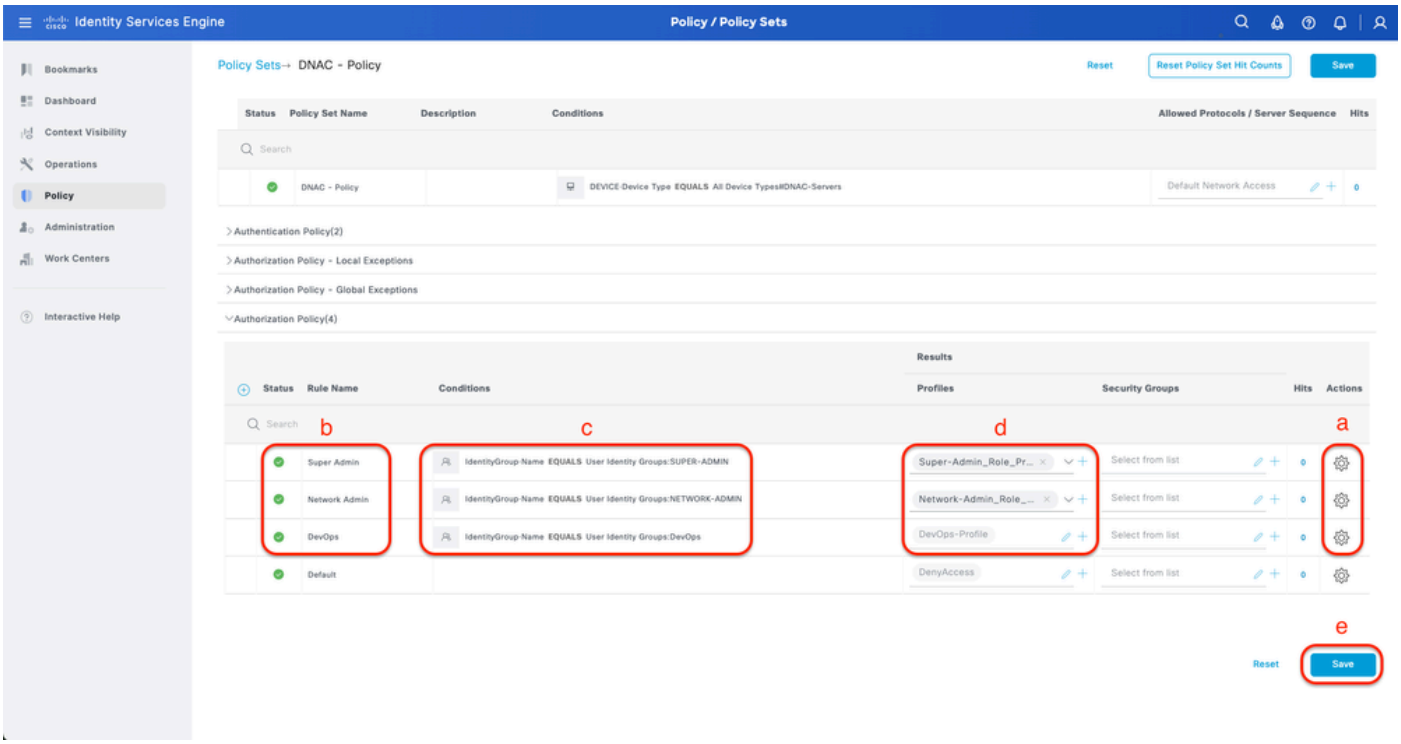
r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

b. Definire il nome del criterio di autorizzazione.

c. Impostare la condizione del criterio di autorizzazione e selezionare il gruppo di utenti creato in (passo 3).

d. Impostare i profili/risultati dei criteri di autorizzazione e selezionare il profilo di autorizzazione creato in (Fase 2).

e. Fare clic su Save (Salva).



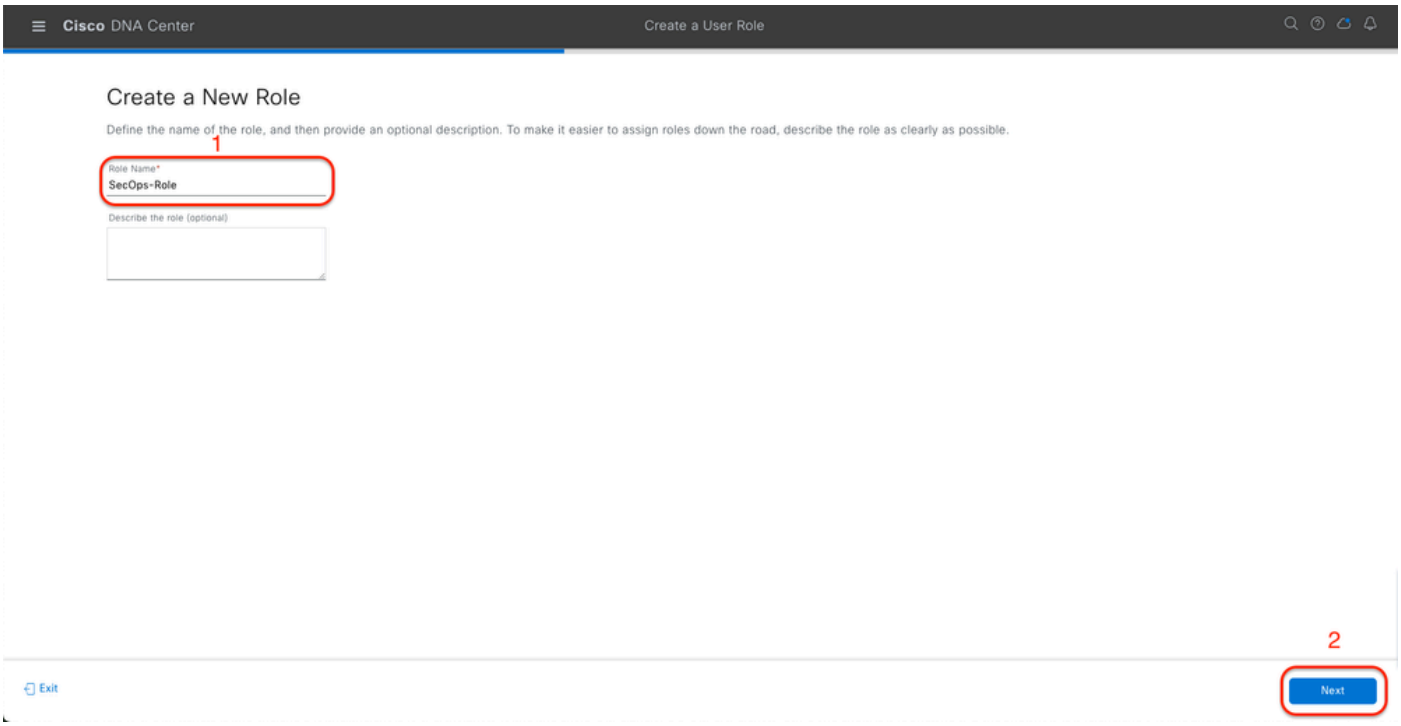
Aggiungi criterio di autorizzazione

(Opzione 2) Configurazione dell'autenticazione esterna DNAC con TACACS+

Passaggio 1. (Facoltativo) Definire un ruolo personalizzato.
Configurare i ruoli personalizzati che soddisfano i requisiti, è possibile utilizzare i ruoli utente predefiniti. A tale scopo, è possibile utilizzare la scheda Sistema > Utenti e ruoli > Controllo di accesso basato su ruoli.

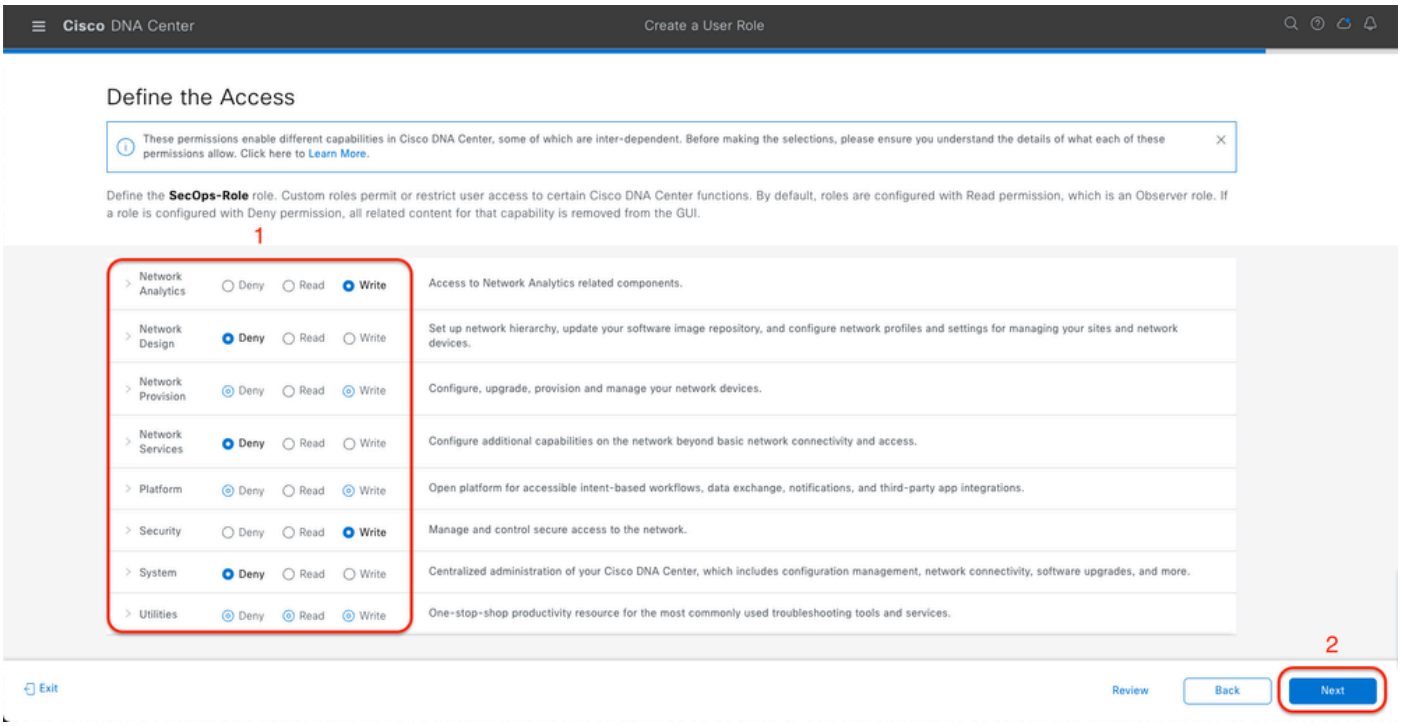
Procedura

r. Creare un nuovo ruolo.



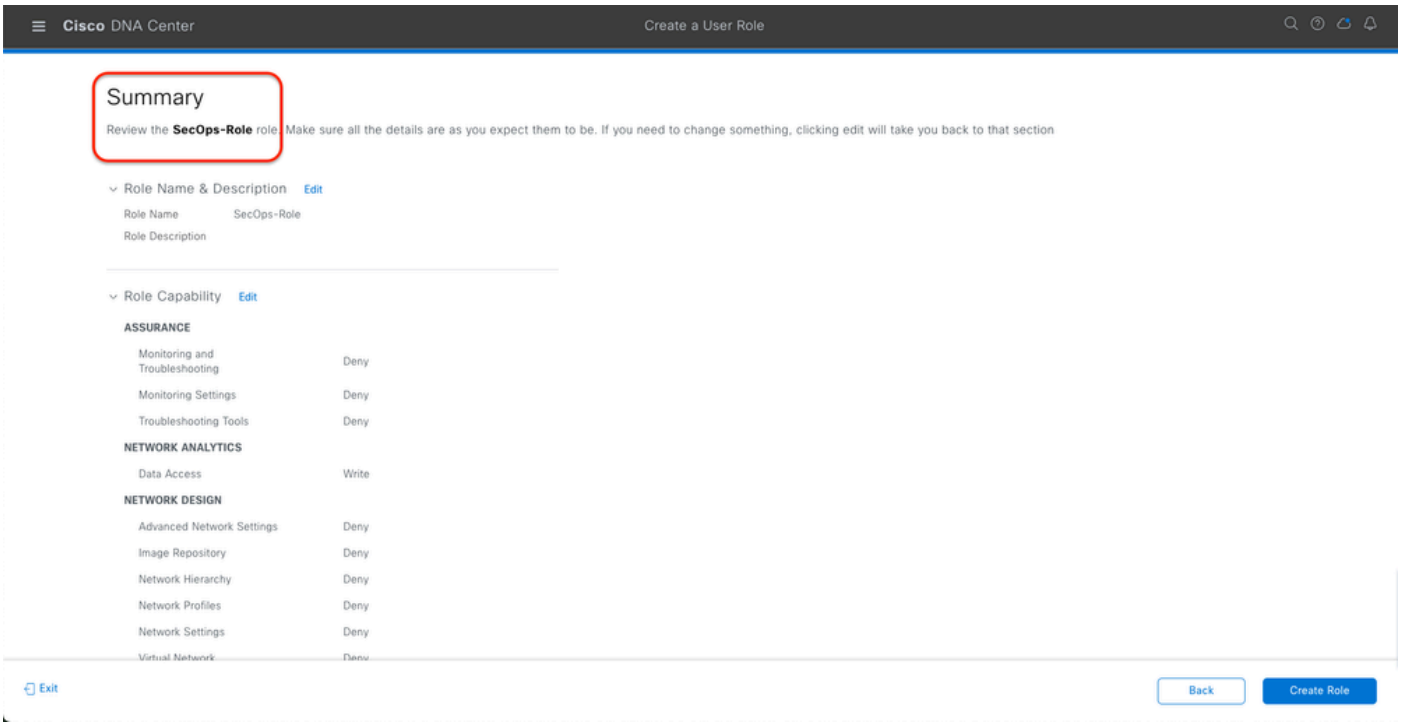
Nome ruolo SecOps

b. Definire l'accesso.

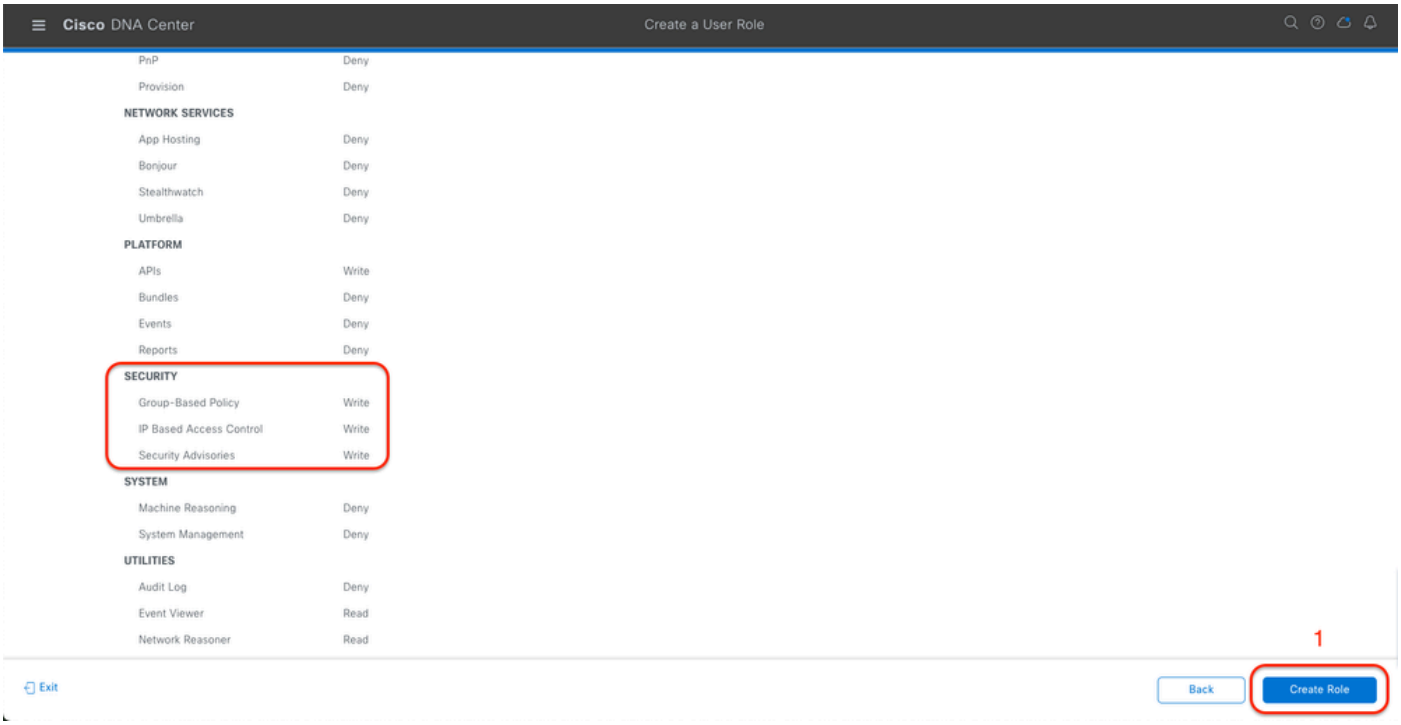


Accesso al ruolo SecOps

c. Creare il nuovo ruolo.



Riepilogo ruolo SecOps



Revisione e creazione ruolo SecOps

Passaggio 2. Configurare L'Autenticazione Esterna Tramite TACACS+.
A tale scopo, è possibile selezionare la scheda Sistema > Utenti e ruoli > Autenticazione esterna.

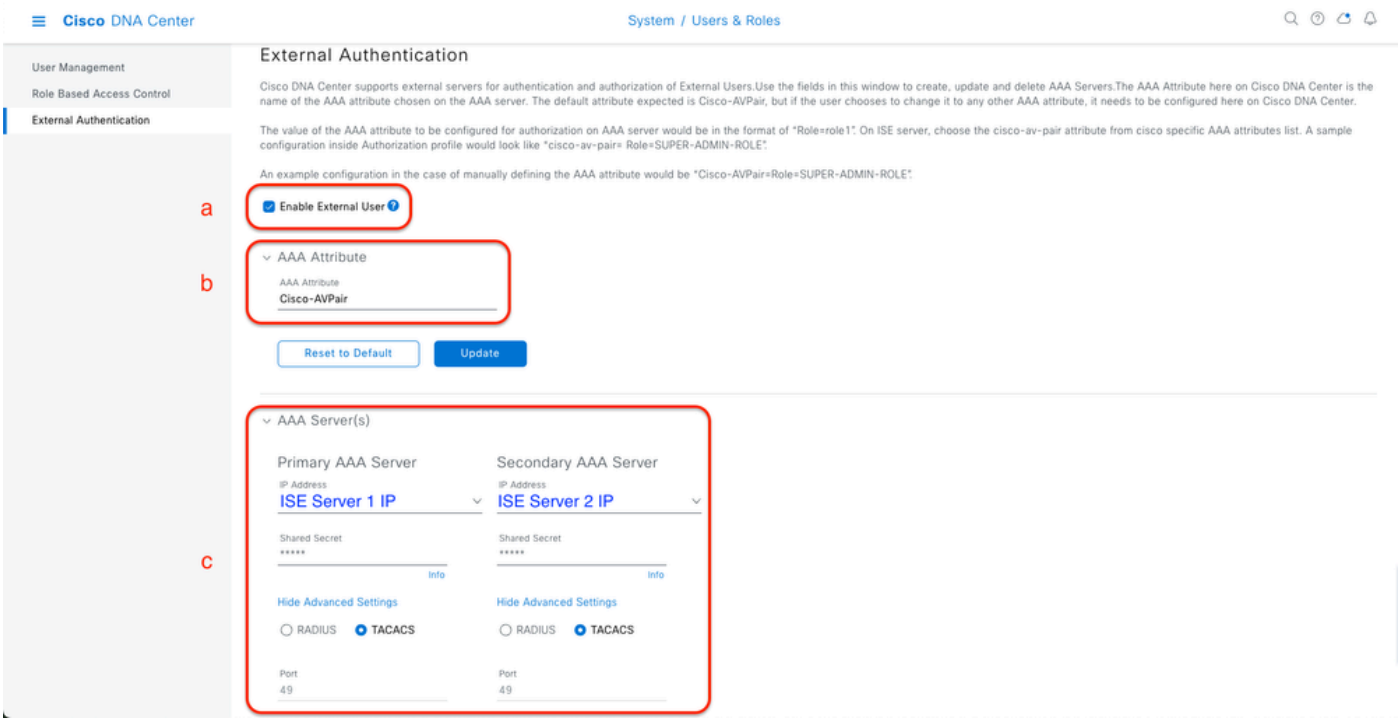
r. Per abilitare l'autenticazione esterna in Cisco DNA Center, selezionare la casella di controllo Abilita utente esterno.

b. Impostare gli attributi AAA.

Immettere Cisco-AVPair nel campo AAA Attributes (Attributi AAA).

c. (Facoltativo) Configurare il server AAA primario e secondario.

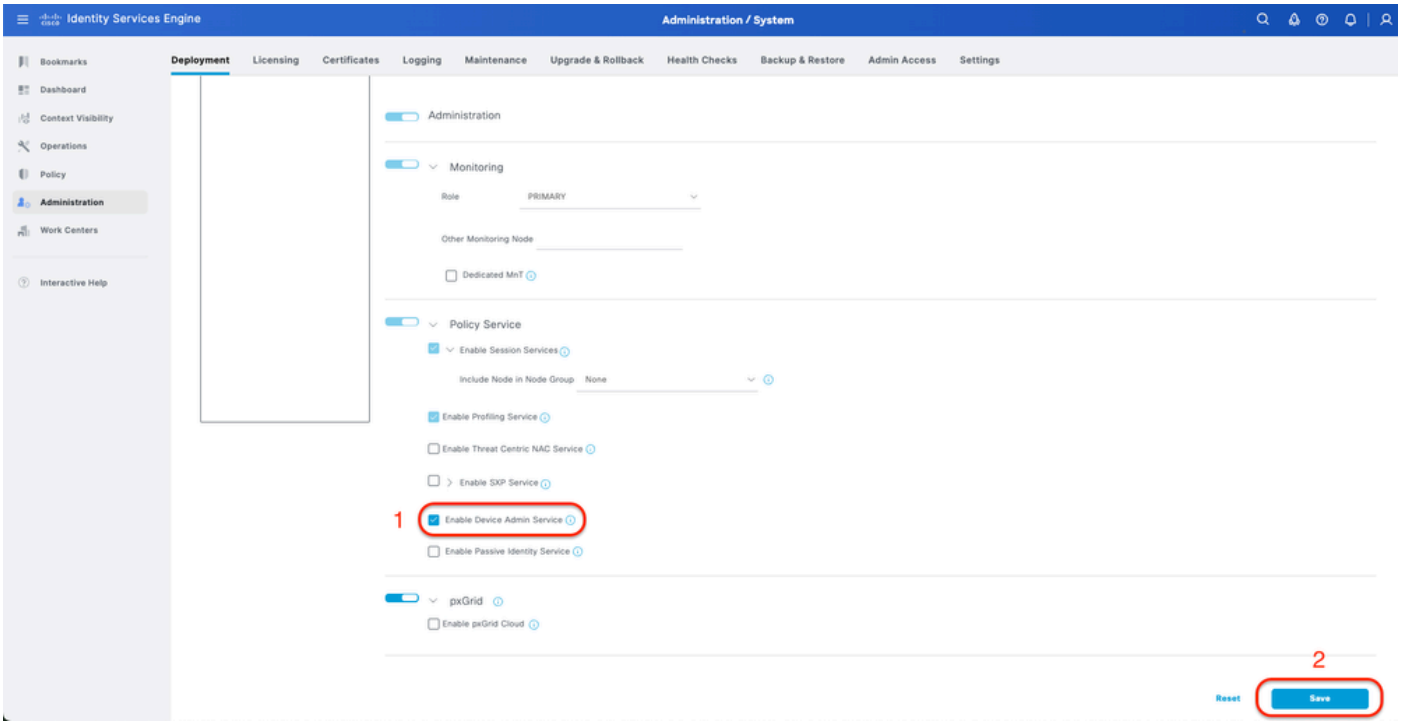
Verificare che il protocollo TACACS+ sia abilitato sul server AAA primario o almeno sul server primario e secondario.



Passaggi della configurazione dell'autenticazione esterna (TACACS+)

(Opzione 2) Configurare ISE per TACACS+

Passaggio 1. Abilitare il servizio Amministrazione dispositivi.
A tale scopo, selezionare la scheda Amministrazione > Sistema > Distribuzione > Modifica (ISE PSN Node) > Selezionare Abilita servizio di amministrazione dispositivi.



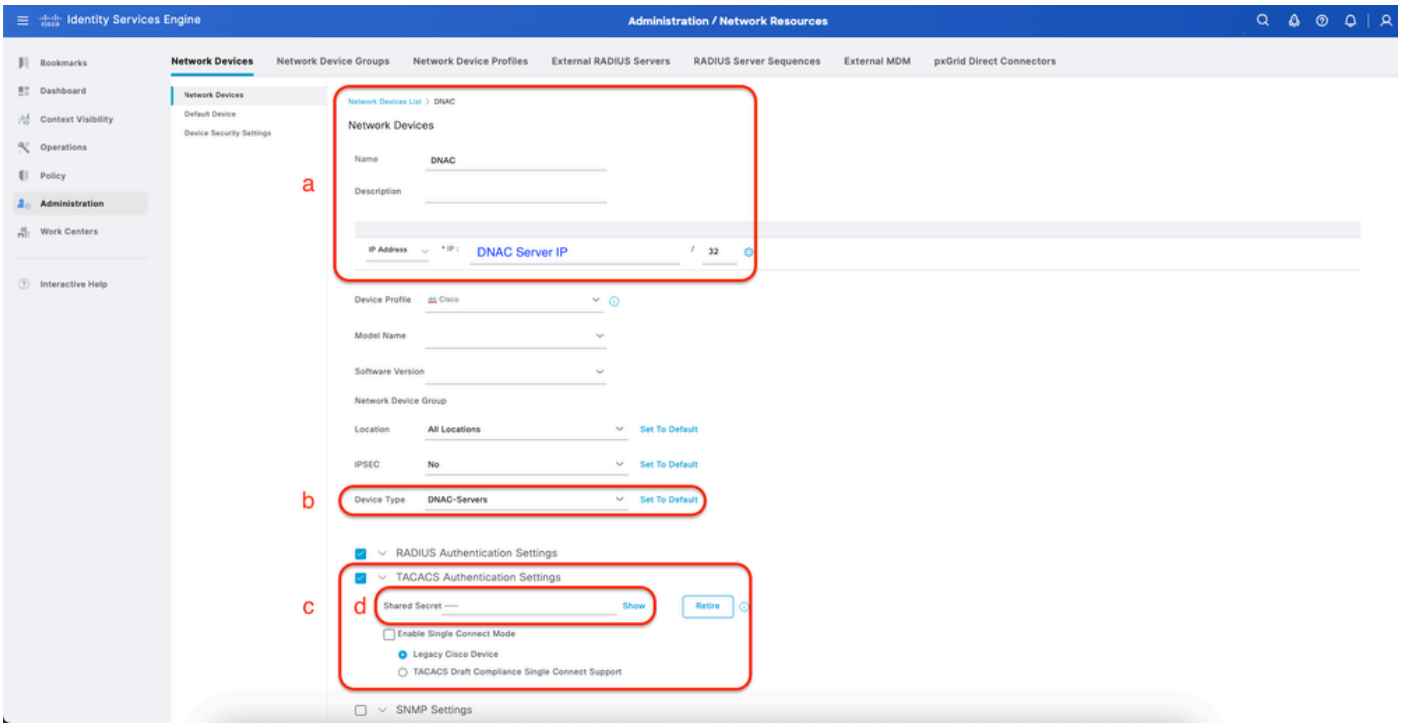
Abilita servizio di amministrazione dispositivi

Passaggio 2. Aggiungere un server DNAC come dispositivo di rete su ISE.

A tale scopo, selezionare la scheda Amministrazione > Risorse di rete > Dispositivi di rete.

Procedura

r. Definire il nome e l'indirizzo IP del dispositivo di rete (DNAC).
b. (Facoltativo) Classificare il tipo di dispositivo per la condizione Set di criteri.
c. Abilitare le impostazioni di autenticazione TACACS+.
d. Impostare TACACS+ Shared Secret.



ISE Network Device (DNAC) per TACACS+

Passaggio 3. Creare profili TACACS+ per ogni ruolo DNAC.

A tale scopo, selezionare la scheda Work Center > Device Administration > Policy Elements > Results > TACACS Profiles.

Nota: Creare 3 profili TACACS+, uno per ogni ruolo utente.

Procedura

r. Fare clic su Add (Aggiungi) e definire il nome del profilo TACACS.

b. Fate clic sulla scheda Vista grezza (Raw View).

c. Immettere il valore Cisco-AVPair=ROLE= e specificare il ruolo utente corretto.

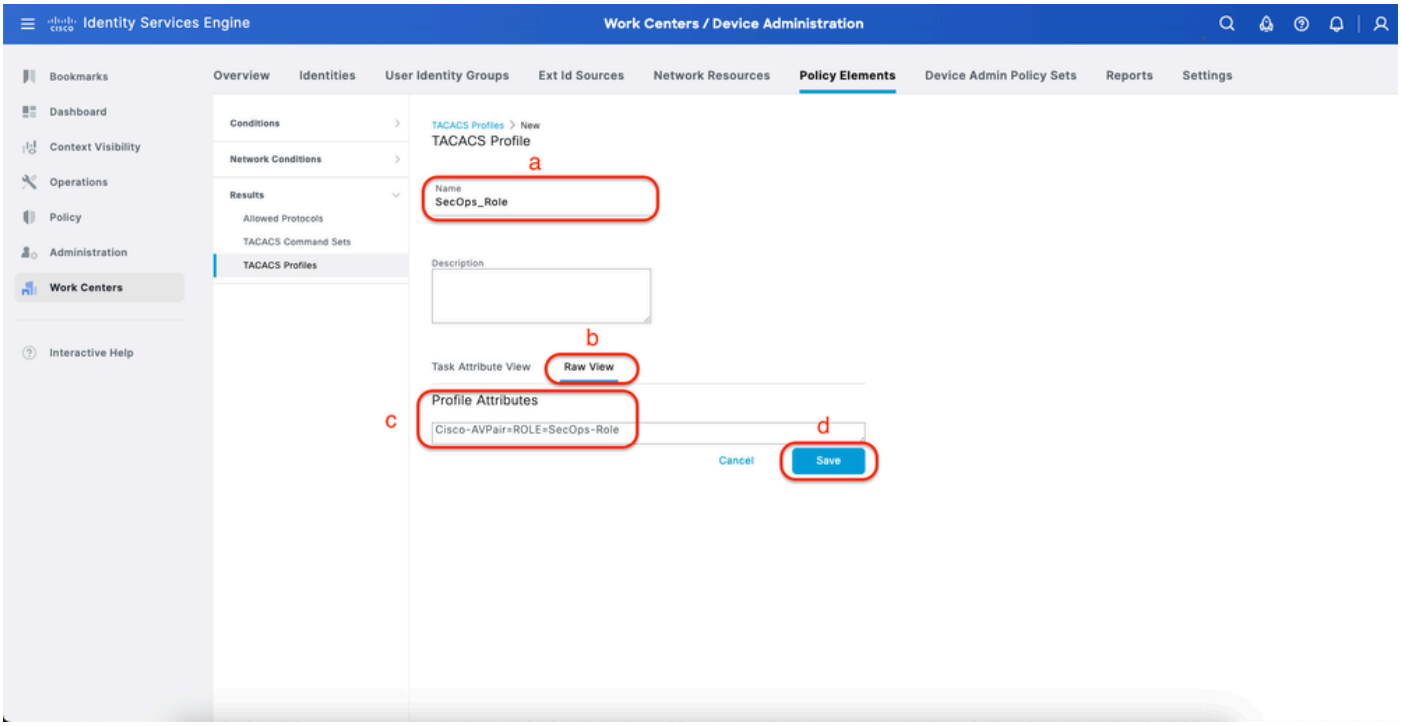
- Per il ruolo utente (SecOps-Role), immettere Cisco-AVPair=ROLE=SecOps-Role.

- Per il ruolo utente (NETWORK-ADMIN-ROLE), immettere Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE.
- Per il ruolo utente (SUPER-ADMIN-ROLE), immettere Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE.

Nota: Il valore di AVPair (Cisco-AVPair=ROLE=) fa distinzione tra maiuscole e minuscole e garantisce che corrisponda al ruolo utente DNAC.

---

d. Fare clic su Save (Salva).



Crea profilo TACACS (SecOps_Role)

Passaggio 4. Creazione del gruppo di utenti.

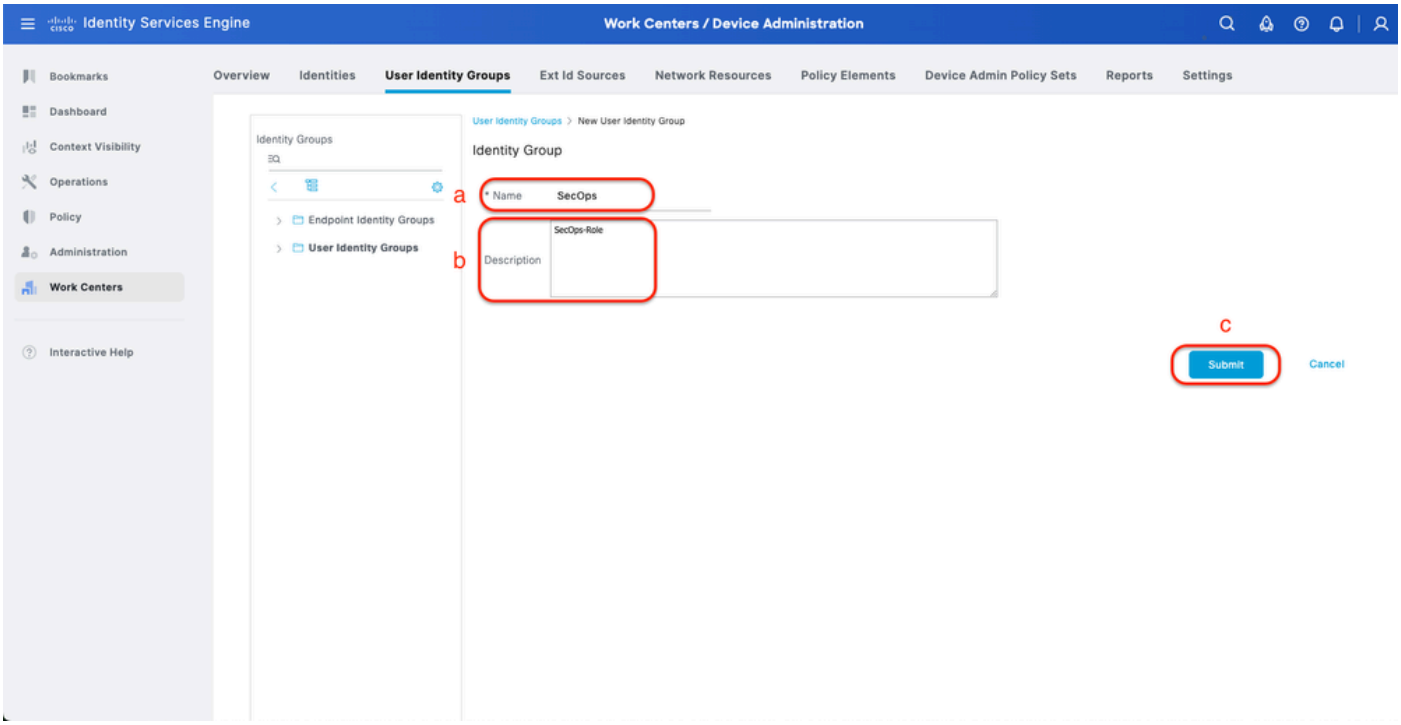
A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Gruppi di identità utente.

Procedura

r. Fare clic su Aggiungi e definire il nome del gruppo di identità.

b. (Facoltativo) Definire la descrizione.

c. Fare clic su Sottometti.



Crea gruppo di identità utente

Passaggio 5. Creare un utente locale.

A tale scopo, è possibile selezionare la scheda Centri di lavoro > Amministrazione dispositivi > Identità > Utenti.

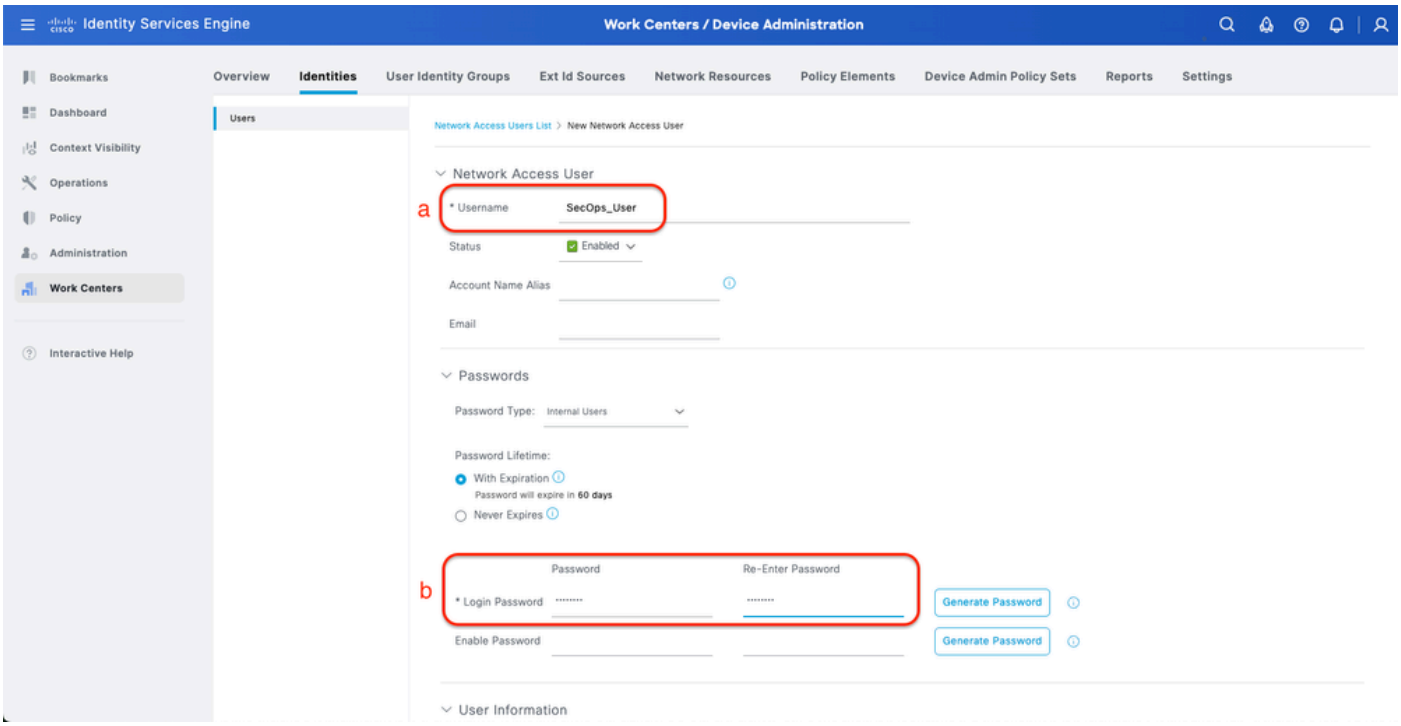
Procedura

r. Fare clic su Add (Aggiungi) e definire il nome utente.

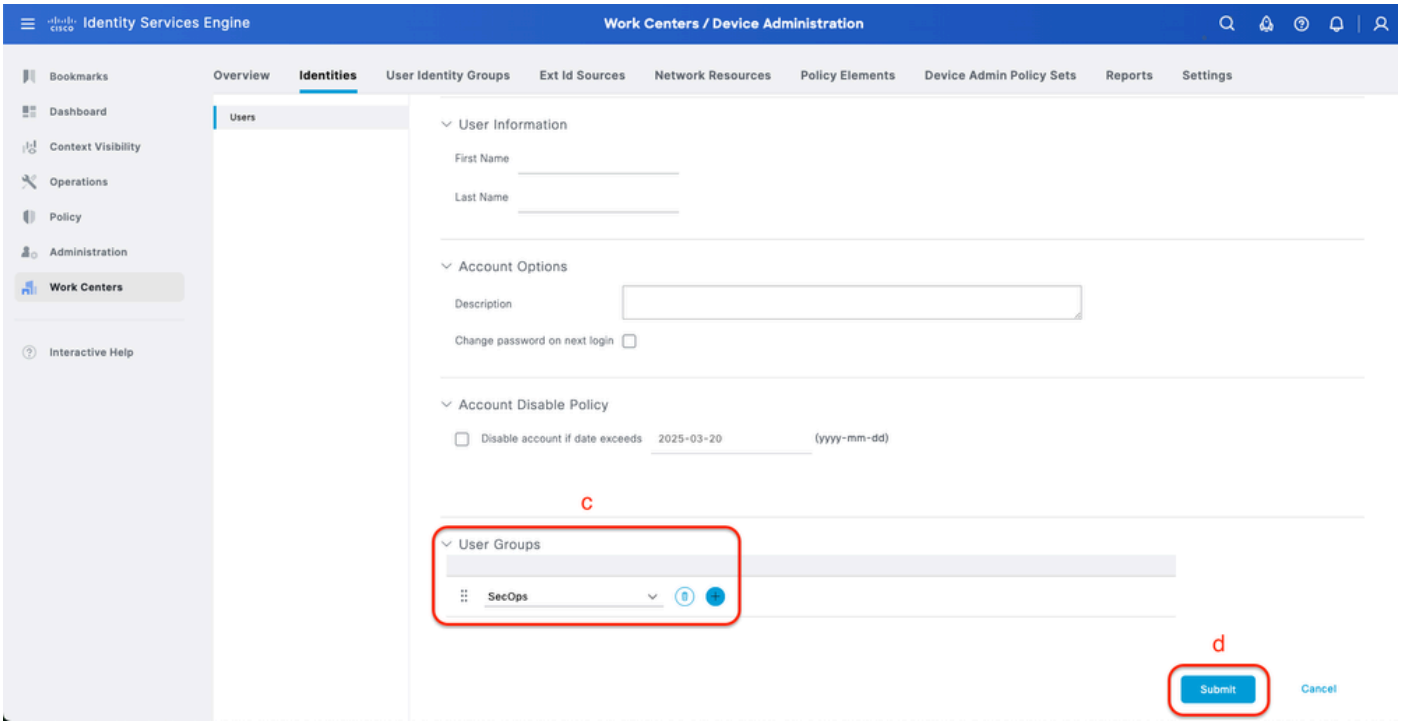
b. Impostare la password di accesso.

c. Aggiungere l'utente al gruppo di utenti correlato.

d. Fare clic su Invia.



Crea utente locale 1-2



Crea utente locale 2-2

Passaggio 6. (Facoltativo) Aggiungere il set di criteri TACACS+.

A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.

Procedura

r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

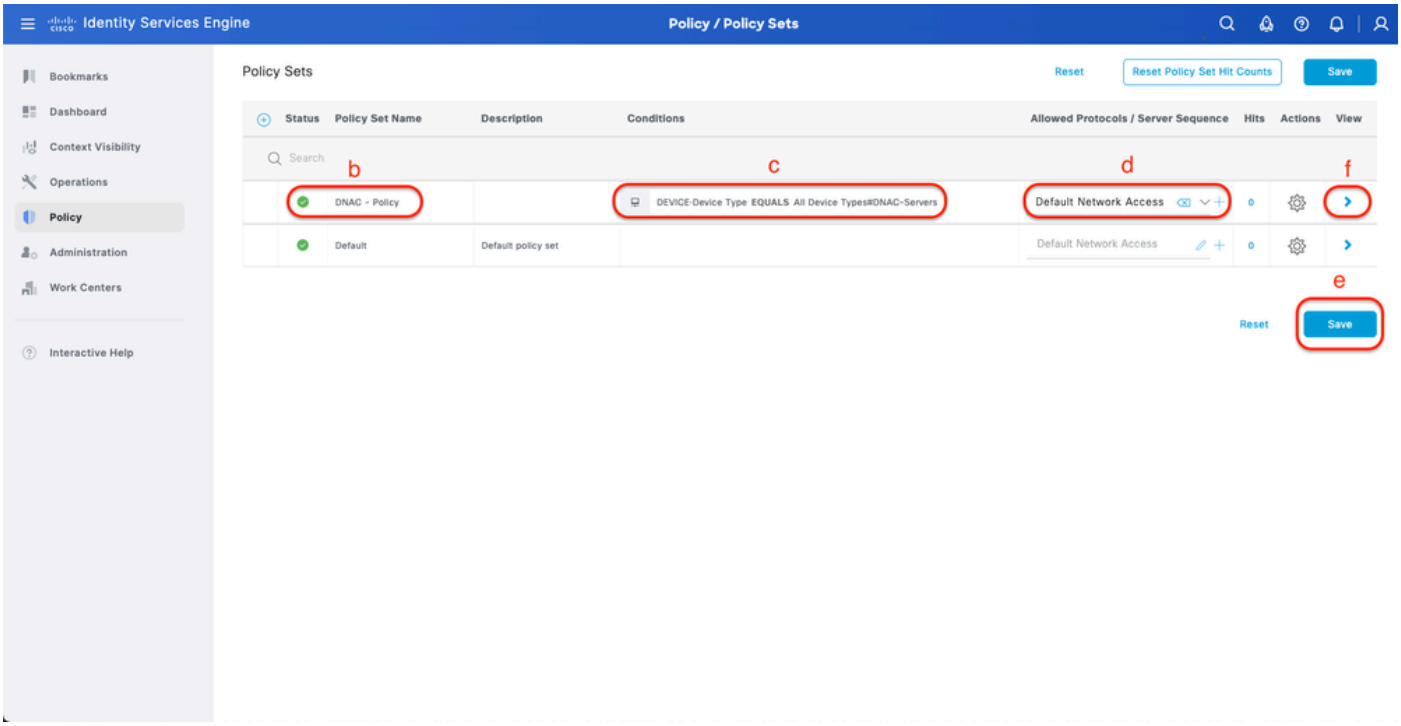
b. Definire il nome del set di criteri.

c. Impostare Policy Set Condition (Condizione di impostazione criteri) su Select Device Type (Seleziona tipo di dispositivo) creato in precedenza (Step2 > b).

d. Impostare i protocolli consentiti.

e. Fare clic su Save (Salva).

f. Fare clic su (>) Visualizzazione set di criteri per configurare le regole di autenticazione e autorizzazione.



Aggiungi set di criteri TACACS+

Passaggio 7. Configurare il criterio di autenticazione TACACS+.

A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > Fare clic su (>).

Procedura

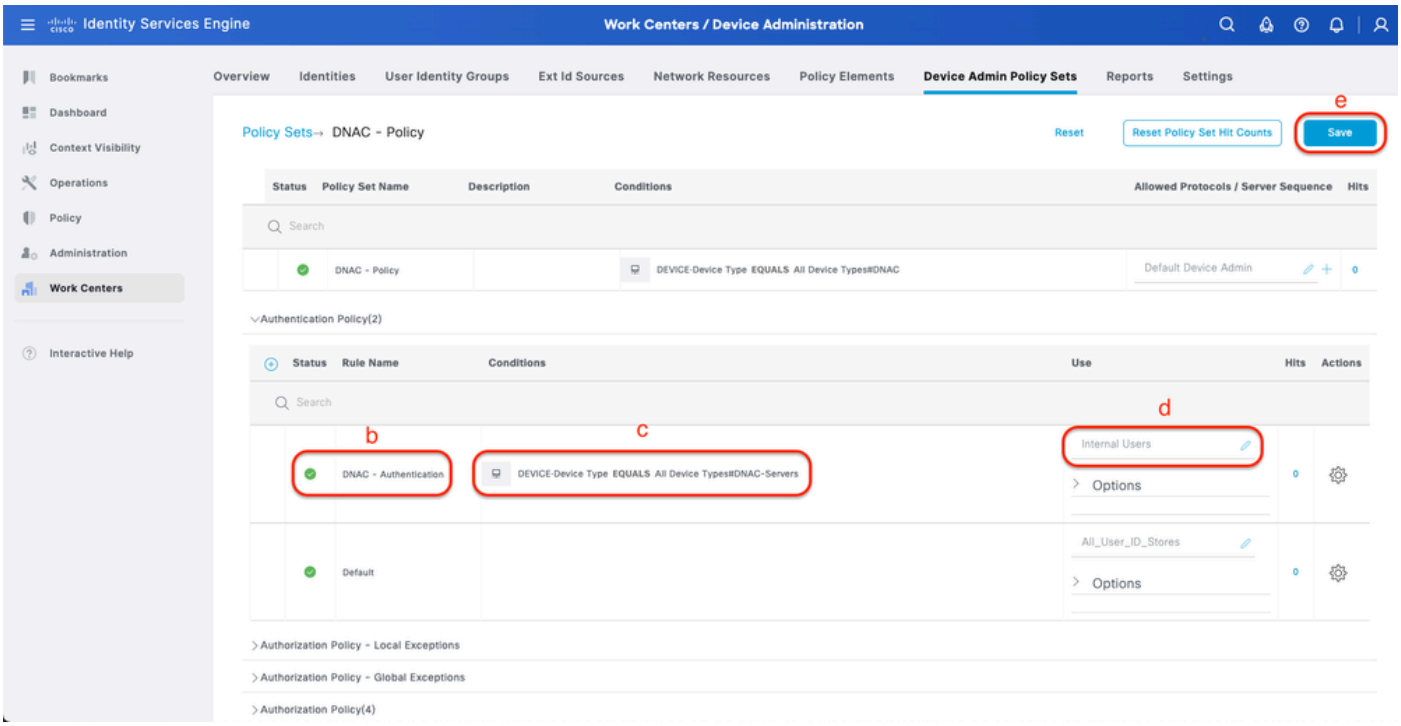
r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

b. Definire il nome del criterio di autenticazione.

c. Impostare la condizione del criterio di autenticazione e selezionare il tipo di dispositivo creato in precedenza (passo 2 > b).

d. Impostare l'utilizzo dei criteri di autenticazione per l'origine identità.

e. Fare clic su Save (Salva).



Aggiungi criterio di autenticazione TACACS+

Passaggio 8. Configurare i criteri di autorizzazione TACACS+.

A tale scopo, selezionare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > Fare clic su (>).

Questo passaggio consente di creare criteri di autorizzazione per ogni ruolo utente:

- RUOLO DI AMMINISTRATORE PRIVILEGIATO
- RUOLO-AMMINISTRATORE-RETE
- Ruolo SecOps

Procedura

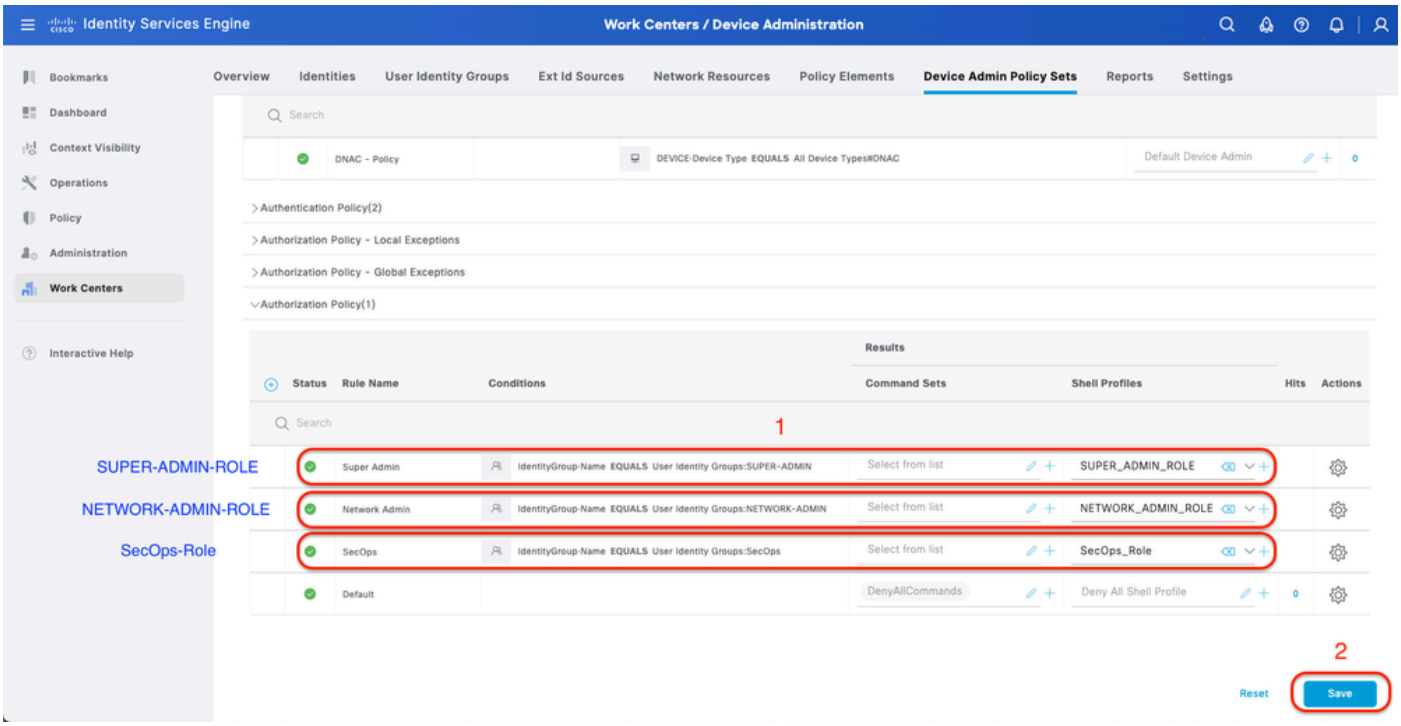
r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

b. Definire il nome del criterio di autorizzazione.

c. Impostare la condizione del criterio di autorizzazione e selezionare il gruppo di utenti creato in (passo 4).

d. Impostare i profili di shell dei criteri di autorizzazione e selezionare il profilo TACACS creato in (Passaggio 3).

e. Fare clic su Save (Salva).

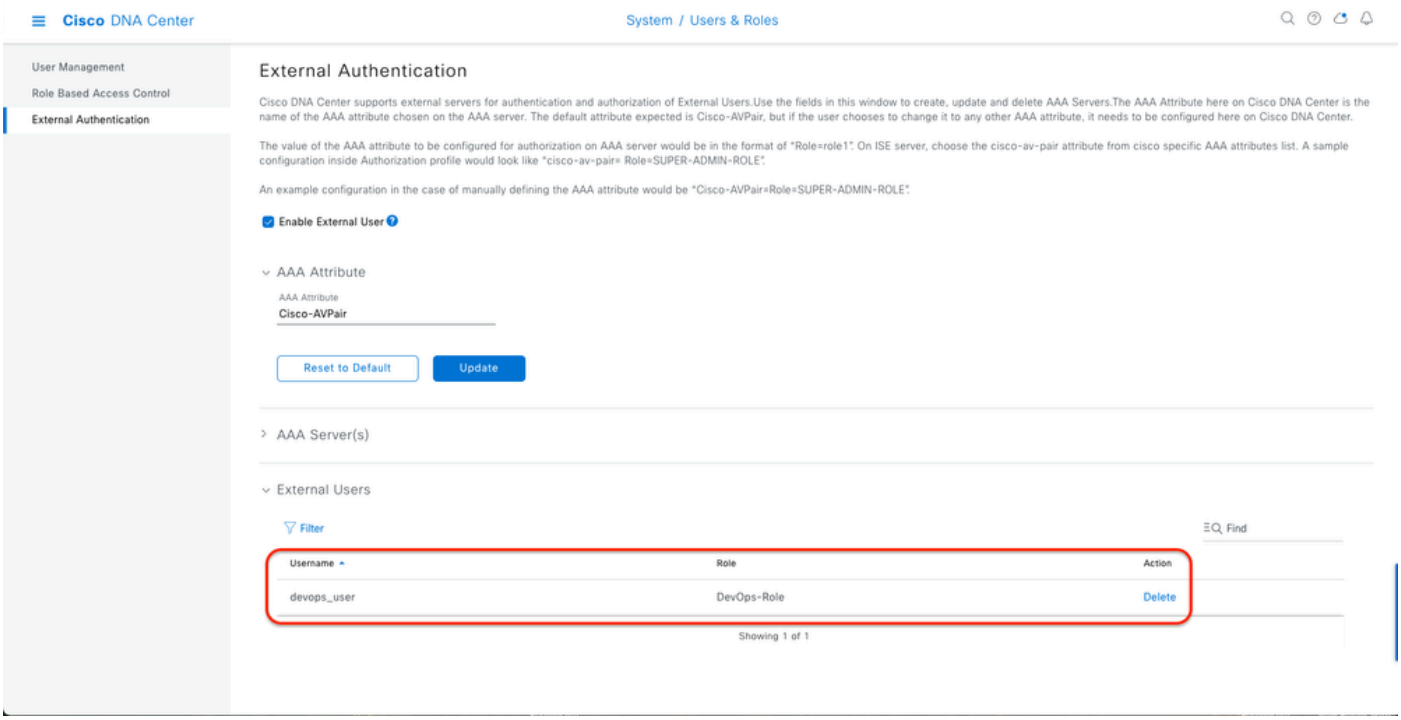


Aggiungi criterio di autorizzazione

Verifica

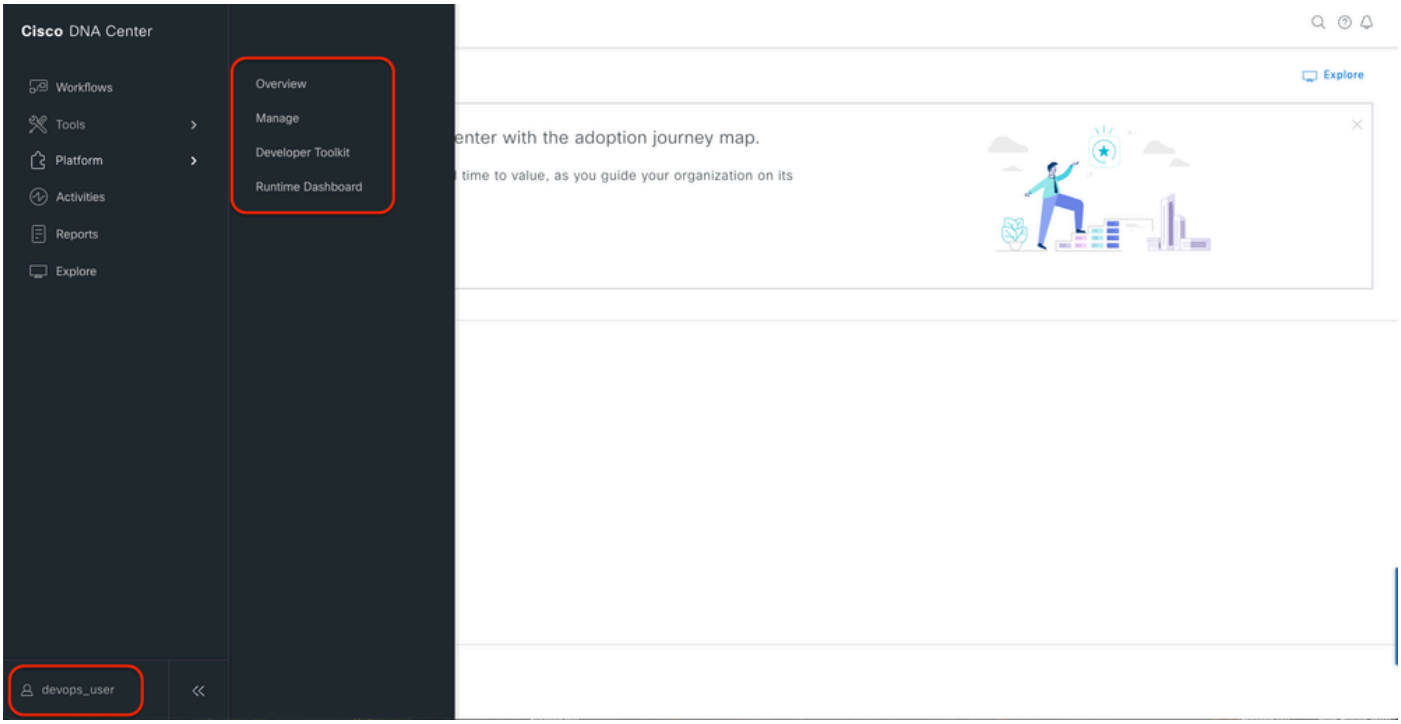
Verifica configurazione RADIUS

1- DNAC - Display External Users System > Utenti e ruoli > Autenticazione esterna > Utenti esterni.
È possibile visualizzare l'elenco degli utenti esterni che hanno eseguito il login tramite RADIUS per la prima volta. Le informazioni visualizzate includono i relativi nomi utente e ruoli.



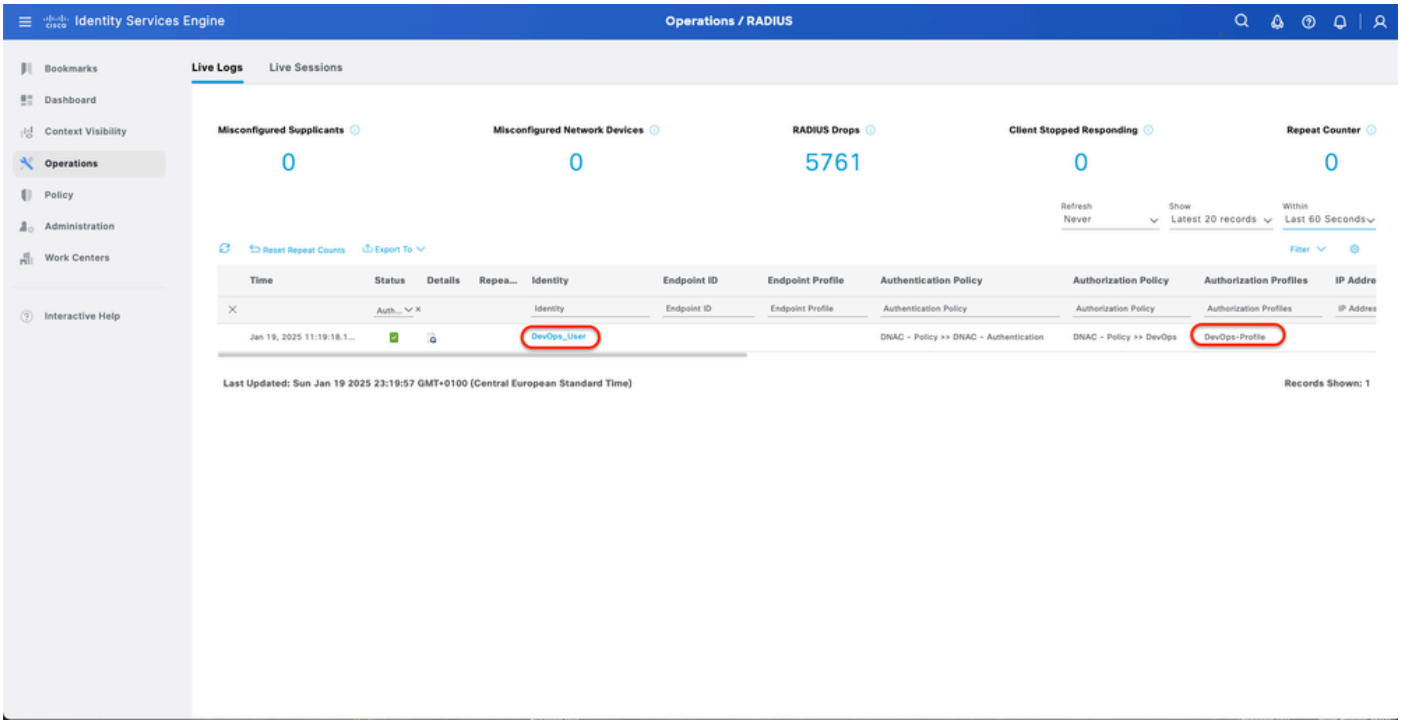
Utenti esterni

2. DNAC - Conferma accesso utente.



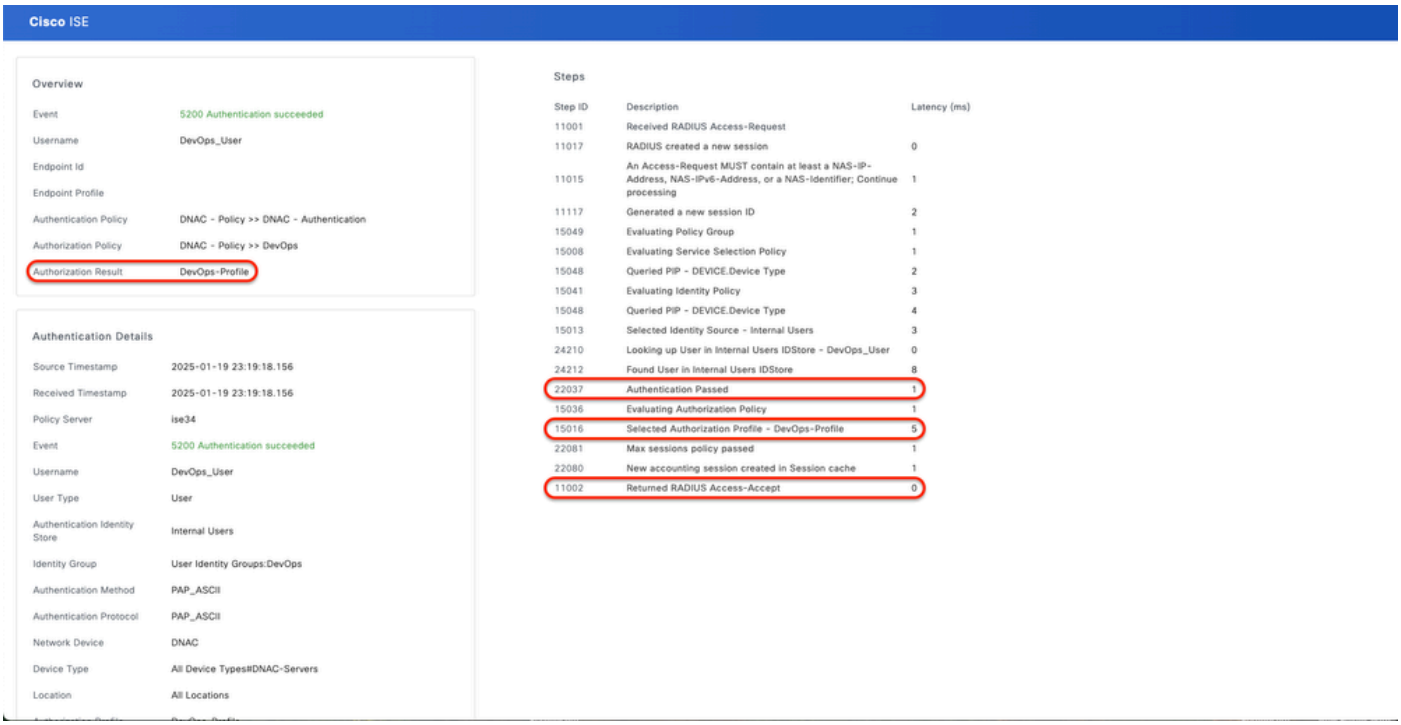
Accesso utente limitato

3.a ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs.

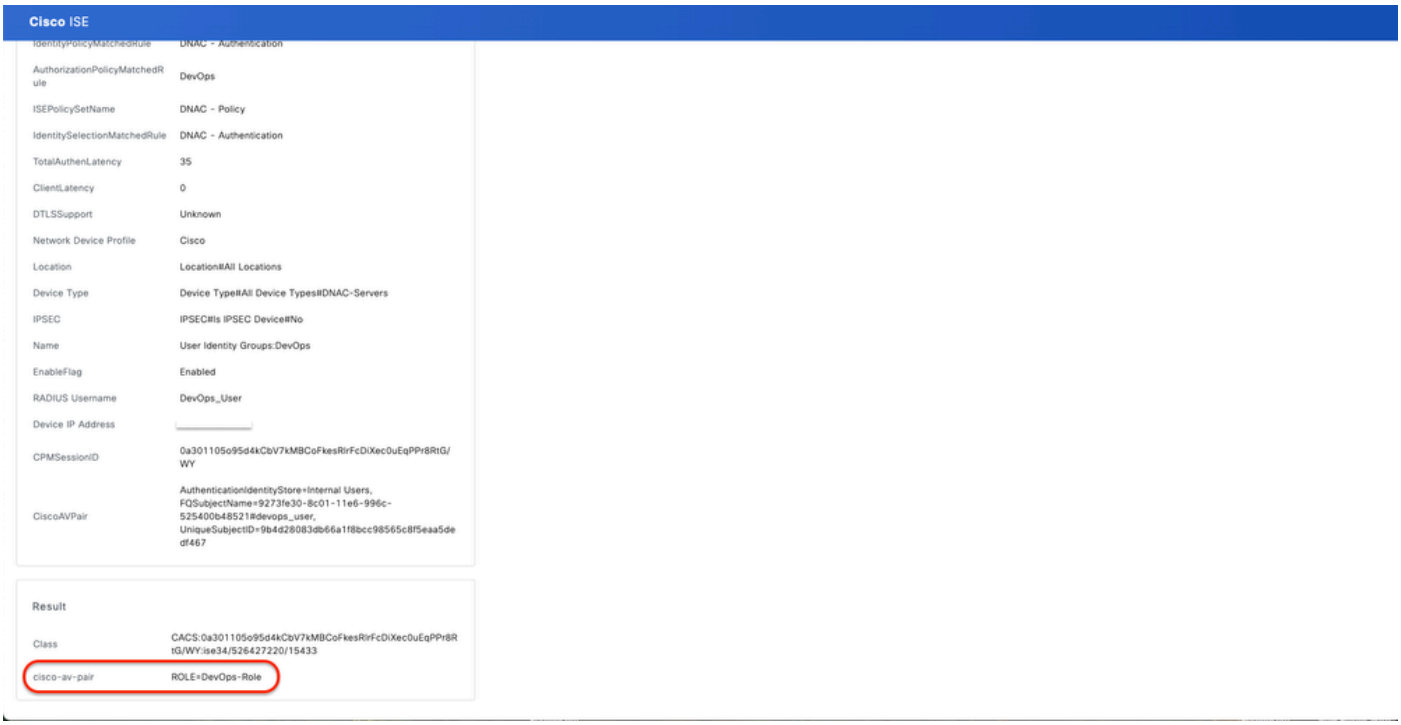


Registri dinamici RADIUS

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Fare clic su (Dettagli) per visualizzare il log di autorizzazione.



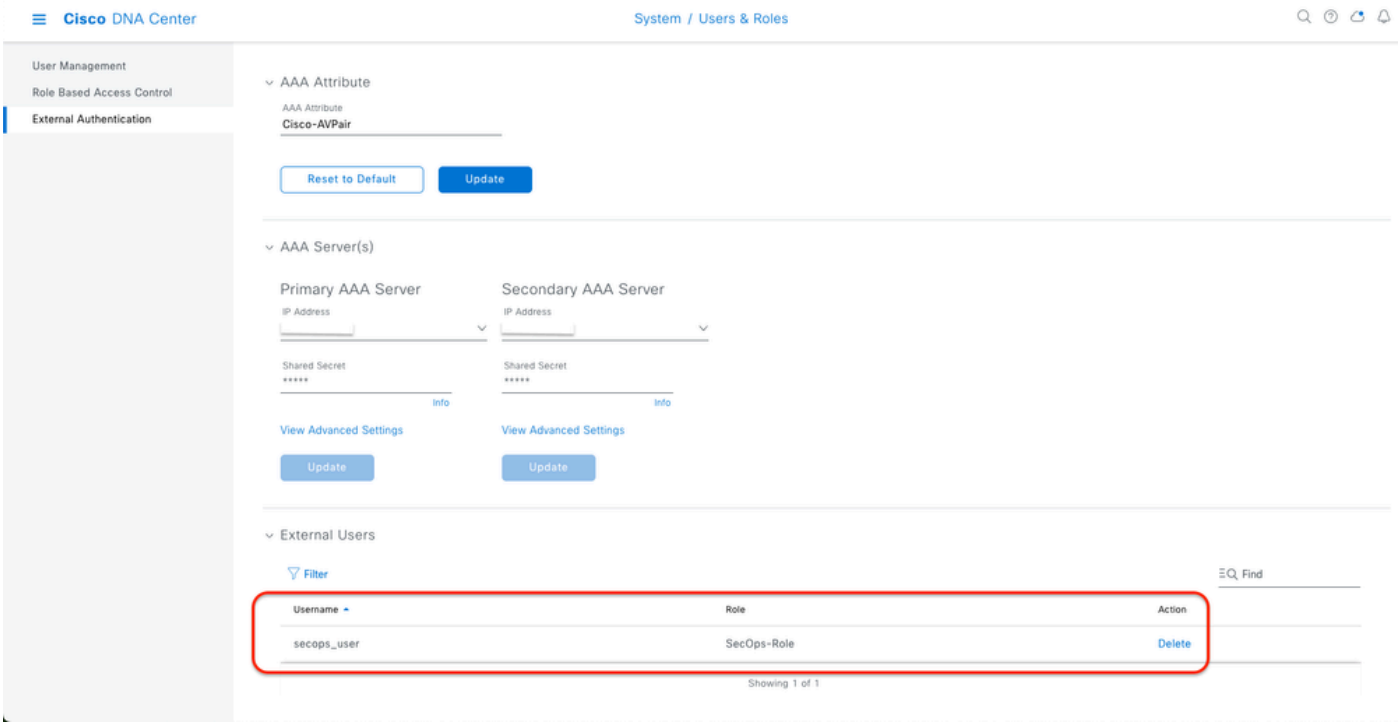
Live log dettagliati RADIUS 1-2



Registri dinamici dettagliati RADIUS 2-2

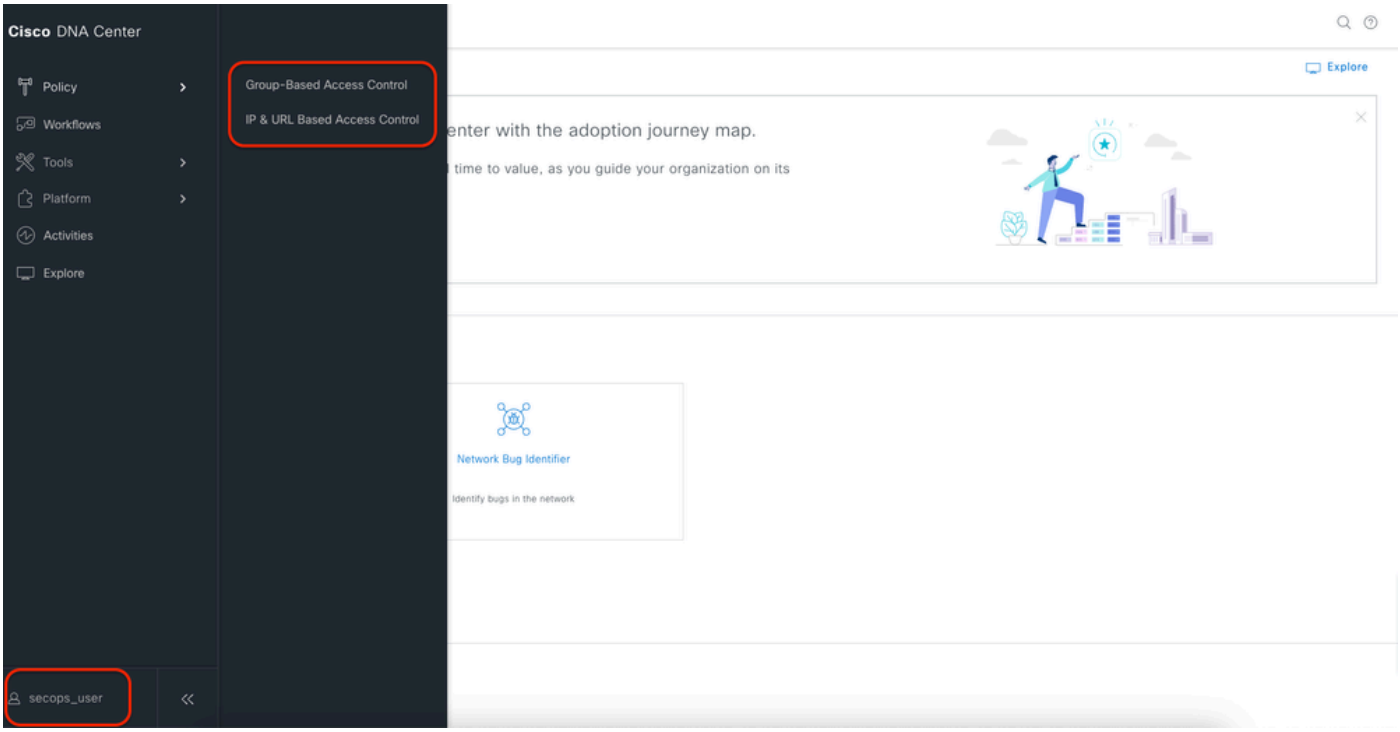
Verifica configurazione TACACS+

1- DNAC - Display External Users System > Utenti e ruoli > Autenticazione esterna > Utenti esterni.
È possibile visualizzare l'elenco degli utenti esterni che hanno effettuato il login tramite TACACS+ per la prima volta. Le informazioni visualizzate includono i relativi nomi utente e ruoli.



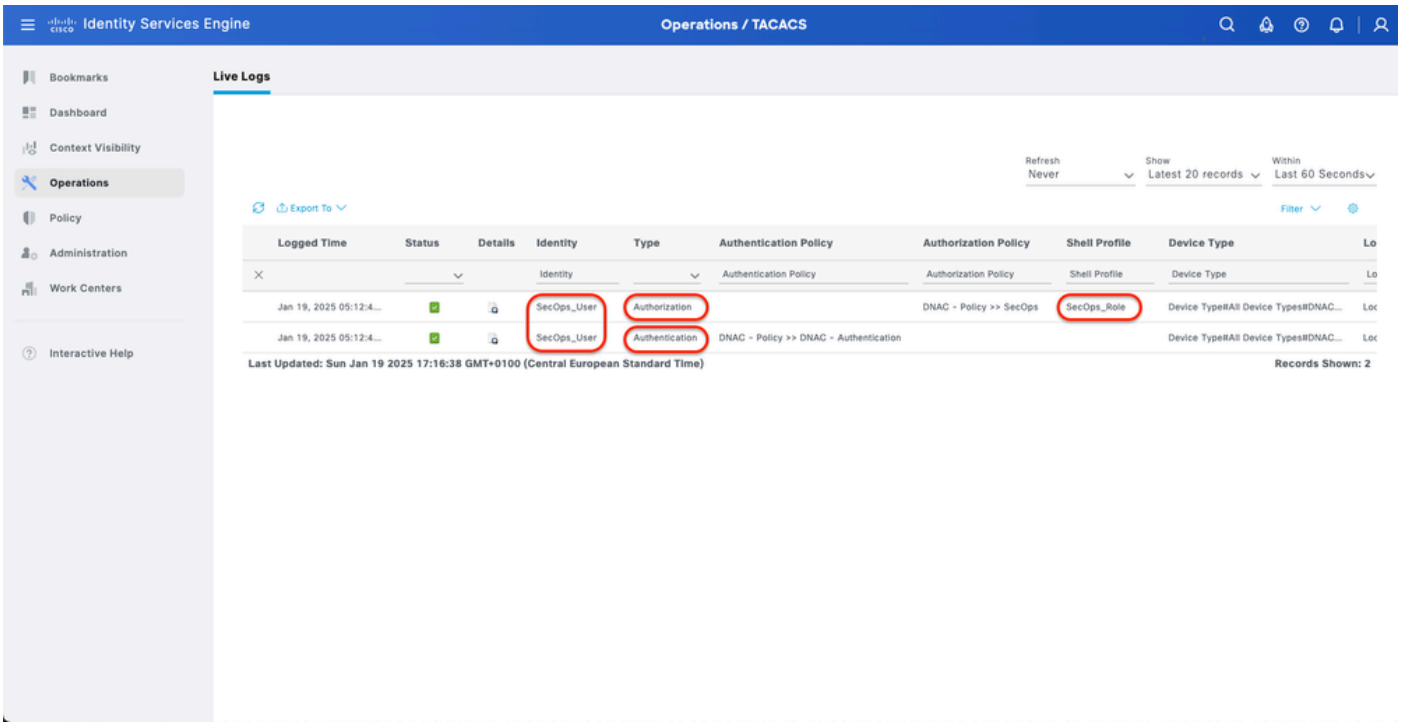
Utenti esterni

2. DNAC - Conferma accesso utente.



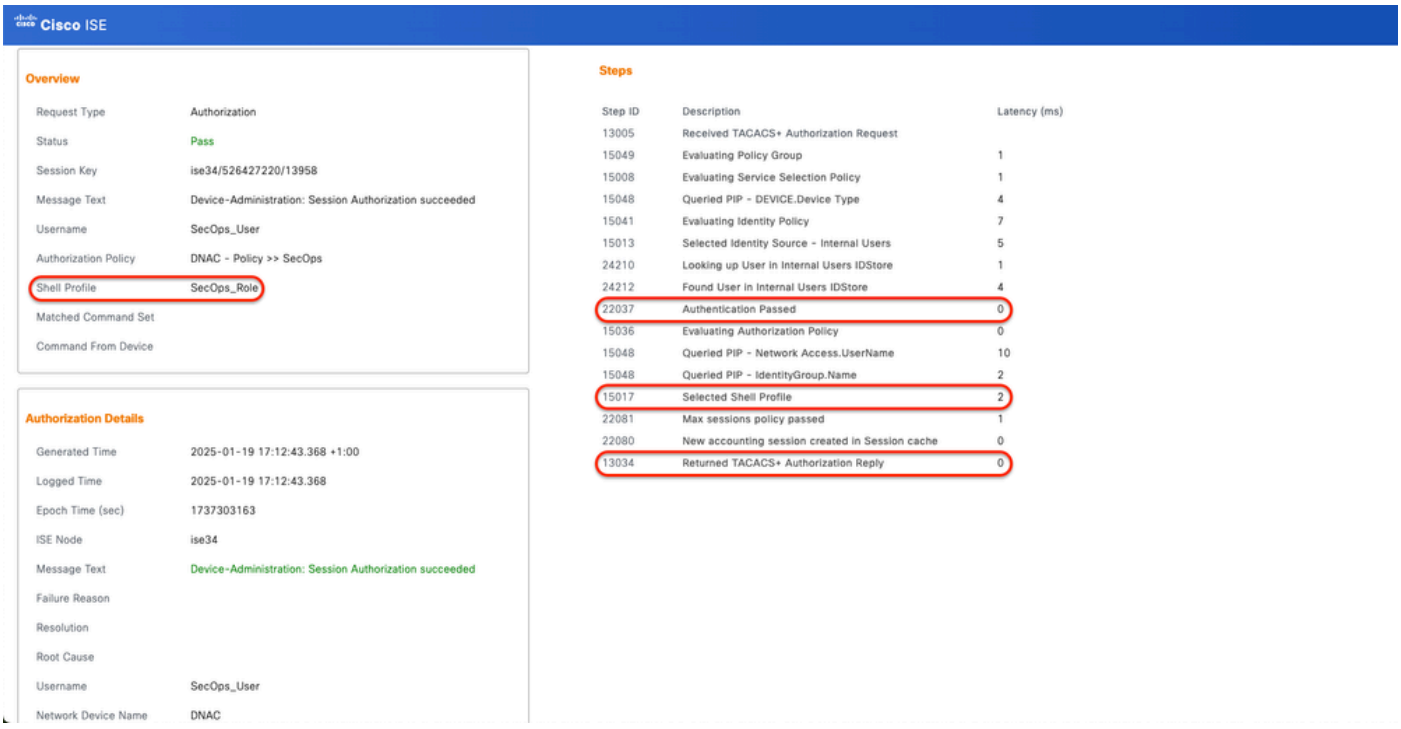
Accesso utente limitato

3.a ISE - TACACS+ Live-Logs Centri di lavoro > Amministrazione dispositivi > Panoramica > TACACS Livelog.

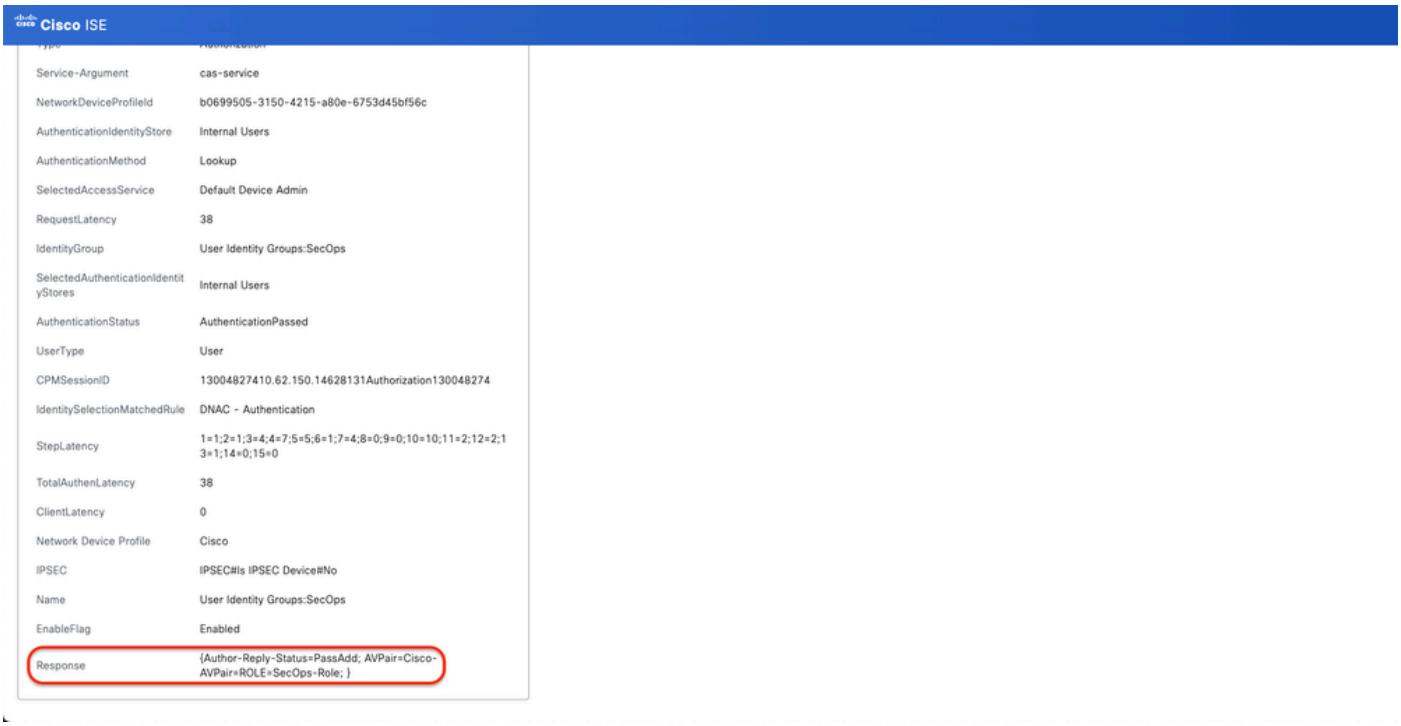


Live log TACACS

3.b ISE - dettagliato TACACS+ Live-Logs Centri di lavoro > Amministrazione dispositivi > Panoramica > TACACS Livelog > Fare clic (Dettagli) per visualizzare il log di autorizzazione.



Registri dettagliati TACACS+ 1-2



Registri attivi dettagliati TACACS+ 2-2

Risoluzione dei problemi

Non sono attualmente disponibili informazioni di diagnostica specifiche per questa configurazione.

Riferimenti

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.4 > Amministrazione dispositivi
- Cisco DNA Center Administrator Guide, versione 2.3.5
- Cisco DNA Center: Controllo degli accessi basato sui ruoli con autenticazione esterna

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).