

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Operazioni preliminari](#)

[Configurazione](#)

[\(Opzione1\) Configurazione dell'autenticazione esterna DNAC tramite RADIUS](#)

[\(Opzione 1\) Configurare ISE per RADIUS](#)

[\(Opzione 2\) Configurazione dell'autenticazione esterna DNAC con TACACS+](#)

[\(Opzione 2\) Configurare ISE per TACACS+](#)

[Verifica](#)

[Verifica configurazione RADIUS](#)

[Verifica configurazione TACACS+](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

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.

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name*
DevOps-Role

Describe the role (optional)

Nome ruolo DevOps

b. Definire l'accesso.

Define the Access

1

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

1

Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

Accesso al ruolo DevOps

c. Creare il nuovo ruolo.

Cisco DNA Center Create a User Role

Summary
Review the **DevOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section

Role Name & Description **DevOps-Role** Edit

Role Description

Role Capability Edit

ASSURANCE

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

NETWORK ANALYTICS

Data Access	Read
-------------	------

NETWORK DESIGN

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

Exit Back Create Role

Riepilogo ruolo DevOps

Cisco DNA Center Create a User Role

Network Device	Deny
Port Management	Deny
Topology	Deny
License	Deny
Network Telemetry	Deny
PnP	Deny
Provision	Deny

NETWORK SERVICES

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

PLATFORM

APIs	Write
Bundles	Write
Events	Write
Reports	Write

SECURITY

Group-Based Policy	Deny
IP Based Access Control	Deny
Security Advisories	Deny

SYSTEM

Machine Reasoning	Deny
System Management	Deny

Exit Back Create Role

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.

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and contains the following configuration options:

- Enable External User:** A checkbox that is checked, highlighted with a red box and labeled 'a'.
- AAA Attribute:** A dropdown menu with 'Cisco-AVPair' selected, highlighted with a red box and labeled 'b'.
- AAA Server(s):** A section with two columns for 'Primary AAA Server' and 'Secondary AAA Server', highlighted with a red box and labeled 'c'. Each column contains:
 - IP Address: 'ISE Server 1 IP' and 'ISE Server 2 IP'.
 - Shared Secret: Masked with '*****'.
 - Protocol: 'RADIUS' selected (radio button checked), 'TACACS' unselected.
 - Authentication Port: '1812'.

(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.

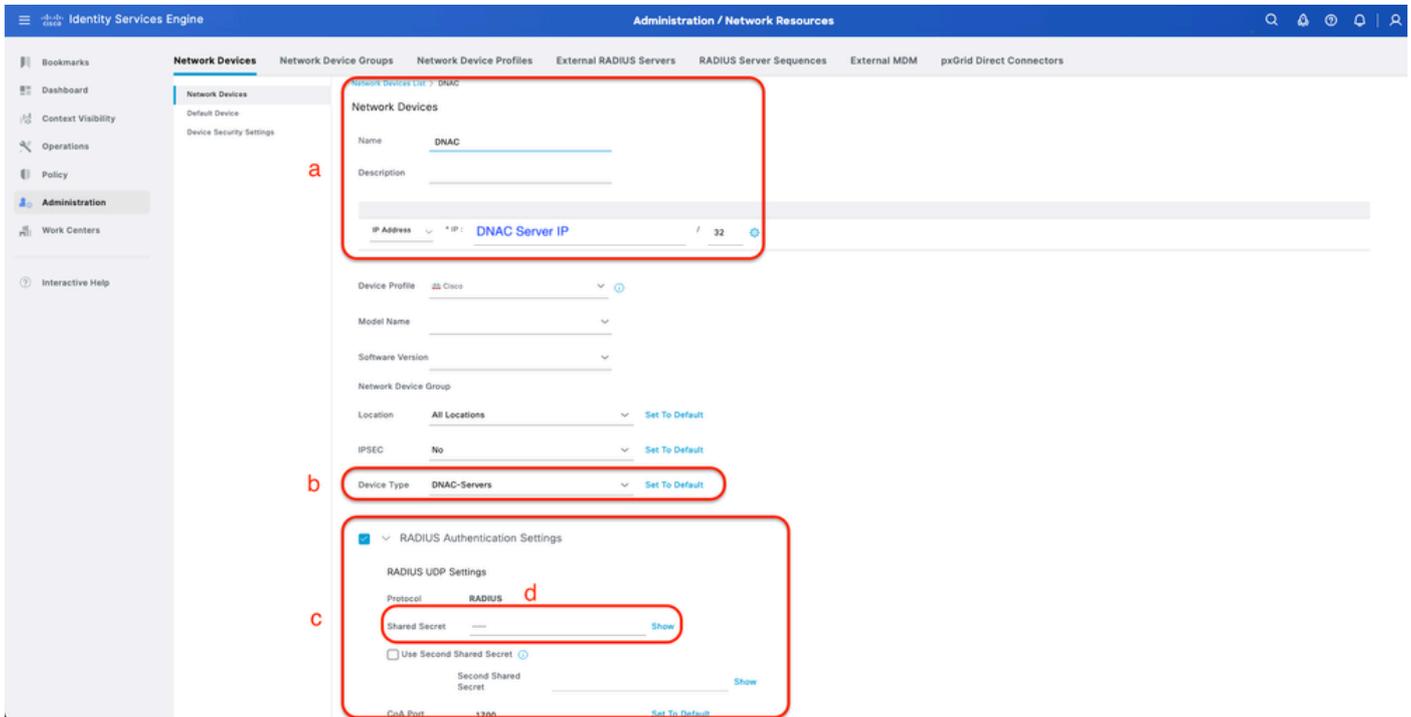
Procedura

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

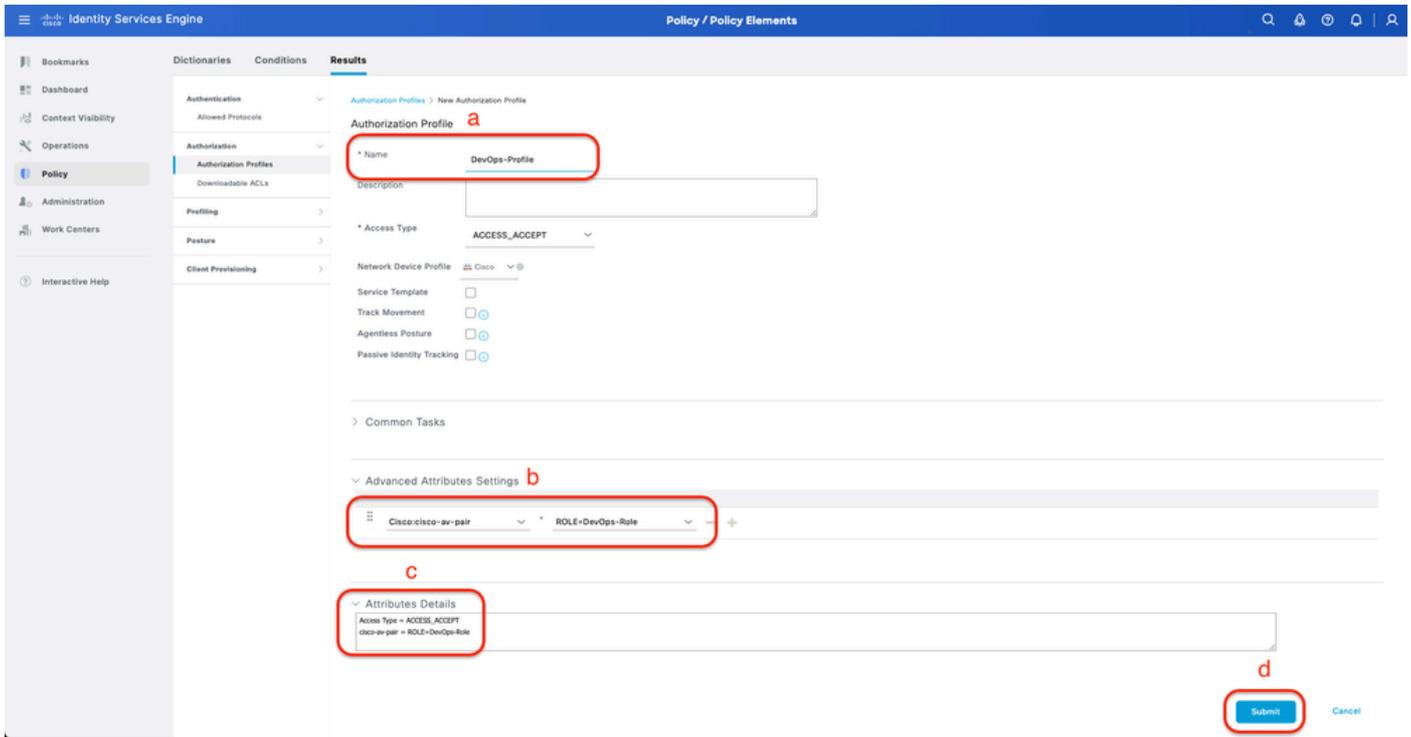
a. Fare clic su Aggiungi e definire il nome del profilo di autorizzazione RADIUS.

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).



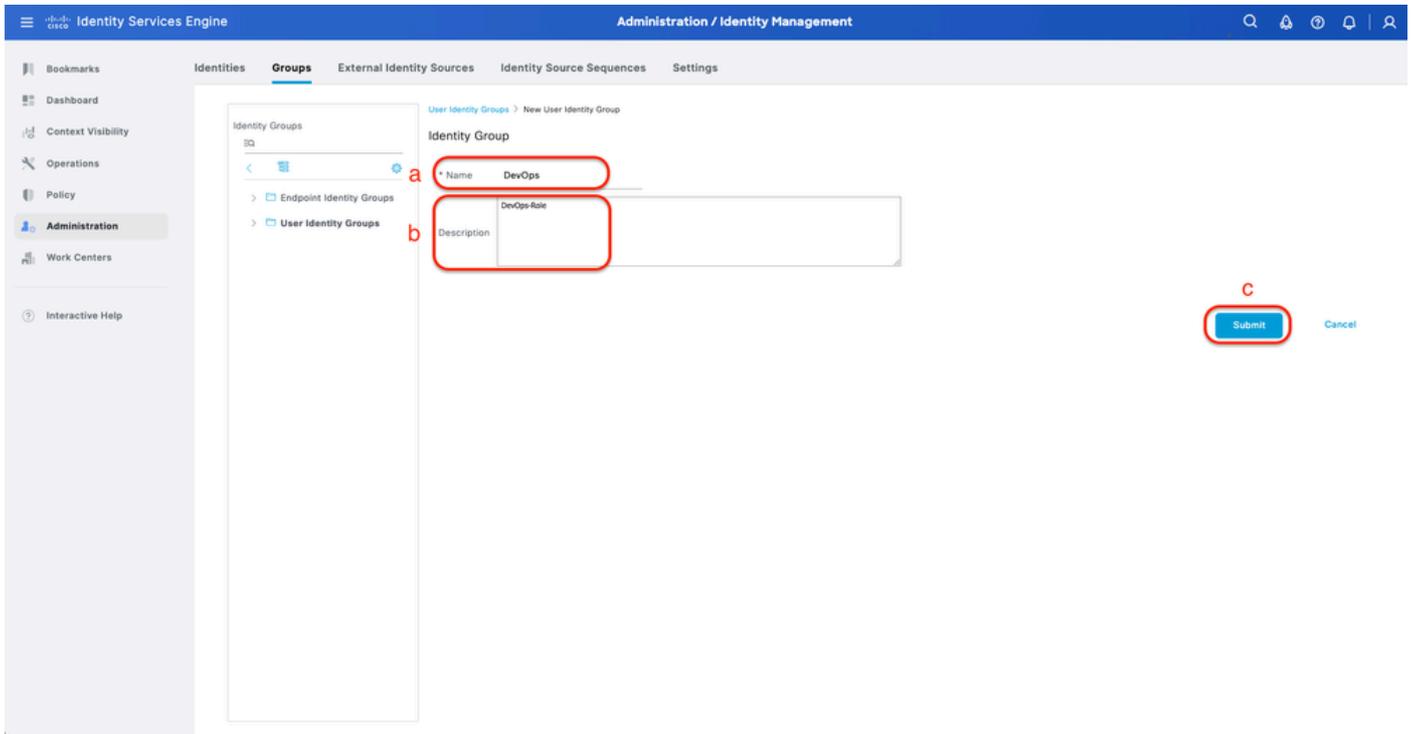
Creazione del profilo di autorizzazione

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.

Identity Services Engine Administration / Identity Management

Network Access Users List > New Network Access User

a * Username **DevOps_User**

Status Enabled

Account Name Alias

Email

b Password Re-Enter Password

* Login Password Re-Enter Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Crea utente locale 1-2

Identity Services Engine Administration / Identity Management

* Login Password Re-Enter Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 2025-03-20 (yyyy-mm-dd)

c User Groups

DevOps

d Submit Cancel

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).

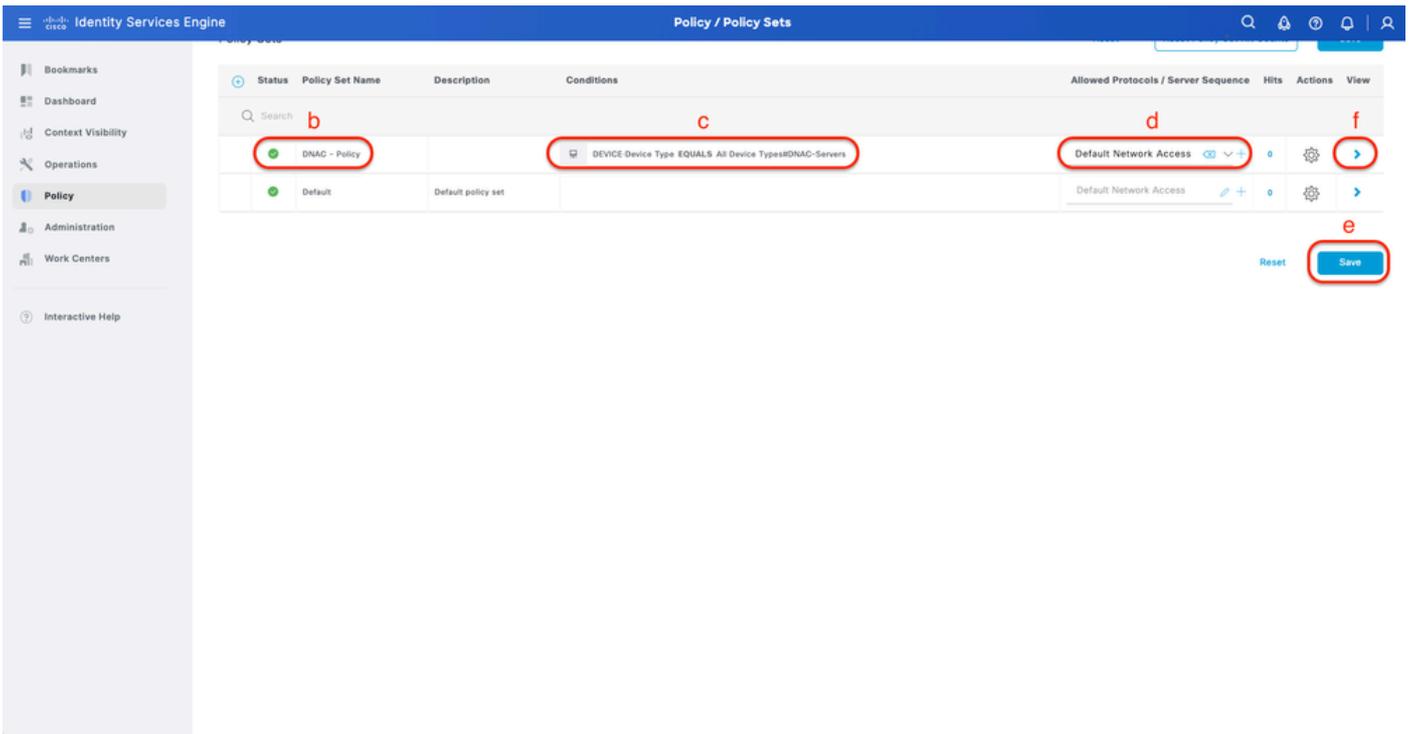
b. Definire il nome del set di criteri.

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).

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main area shows a table of Policy Sets under the 'Authentication Policy(2)' section. The first row is 'DNAC - Authentication' with a condition 'DEVICE Device Type EQUALS All Device Types#DNAC-Servers'. The 'Use' column for this row shows 'Internal Users'. The 'Save' button at the bottom right is highlighted with a red circle labeled 'e'. Other elements are labeled with red letters: 'b' for the rule name, 'c' for the condition, and 'd' for the user group selection.

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).

The screenshot displays the 'Policy / Policy Sets' configuration interface. At the top, there are navigation tabs for 'Policy Sets' and 'Policy'. Below this, a table lists policy sets with columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', and 'Hits'. A search bar is present above the table.

Below the table, there are expandable sections for 'Authentication Policy(2)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy(4)'. The 'Authorization Policy(4)' section is expanded, showing a detailed view of a policy rule.

The detailed view includes a table with columns for 'Status', 'Rule Name', 'Conditions', 'Profiles', 'Security Groups', 'Hits', and 'Actions'. The 'Rule Name' column contains 'Super Admin', 'Network Admin', 'DevOps', and 'Default'. The 'Conditions' column contains 'IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN', 'IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN', and 'IdentityGroup-Name EQUALS User Identity Groups:DevOps'. The 'Profiles' column contains 'Super-Admin_Role_Pr...', 'Network-Admin_Role_...', and 'DevOps-Profile'. The 'Security Groups' column contains 'Select from list'. The 'Hits' column contains '0'. The 'Actions' column contains a gear icon (labeled 'a') and a plus icon.

Red boxes and letters highlight specific elements: 'b' highlights the 'Rule Name' column; 'c' highlights the 'Conditions' column; 'd' highlights the 'Profiles' column; 'a' highlights the gear icon in the 'Actions' column; and 'e' highlights the 'Save' button at the bottom right.

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.

Cisco DNA Center Create a User Role

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name*

Describe the role (optional)

2

[Exit](#) [Next](#)

Nome ruolo SecOps

b. Definire l'accesso.

Cisco DNA Center Create a User Role

Define the Access

1

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

Define the **SecOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

> Network Analytics	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Manage and control secure access to the network.
> System	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
> Utilities	<input checked="" type="radio"/> Deny <input checked="" type="radio"/> Read <input checked="" type="radio"/> Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.

2

[Exit](#) [Review](#) [Back](#) [Next](#)

Accesso al ruolo SecOps

c. Creare il nuovo ruolo.

Cisco DNA Center Create a User Role

Summary
Review the **SecOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section.

Role Name & Description [Edit](#)

Role Name	SecOps-Role
Role Description	

Role Capability [Edit](#)

ASSURANCE

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

NETWORK ANALYTICS

Data Access	Write
-------------	-------

NETWORK DESIGN

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

[Exit](#) [Back](#) [Create Role](#)

Riepilogo ruolo SecOps

Cisco DNA Center Create a User Role

PnP	Deny
Provision	Deny

NETWORK SERVICES

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

PLATFORM

APIs	Write
Bundles	Deny
Events	Deny
Reports	Deny

SECURITY

Group-Based Policy	Write
IP Based Access Control	Write
Security Advisories	Write

SYSTEM

Machine Reasoning	Deny
System Management	Deny

UTILITIES

Audit Log	Deny
Event Viewer	Read
Network Reasoner	Read

[Exit](#) [Back](#) [Create Role](#) ¹

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.

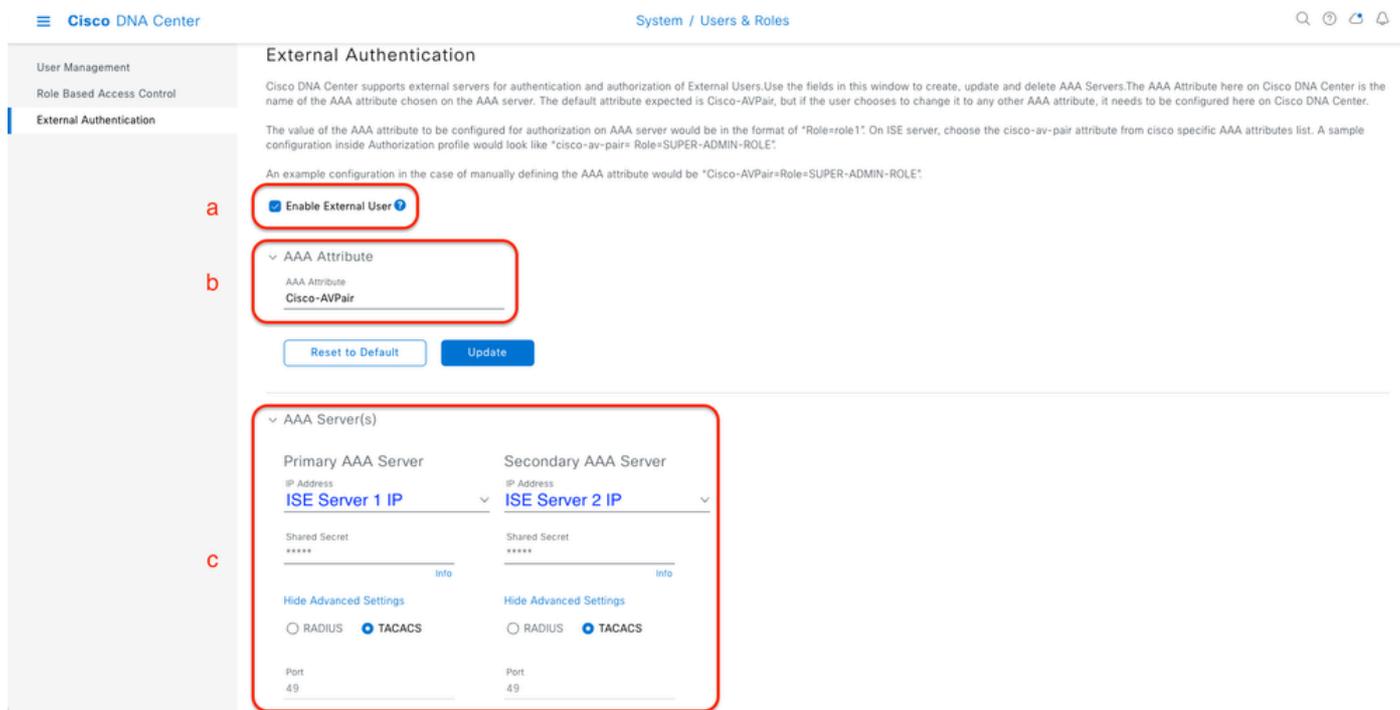
r. Per abilitare l'autenticazione esterna in Cisco DNA Center, selezionare la casella di controllo Abilita utente esterno.

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.

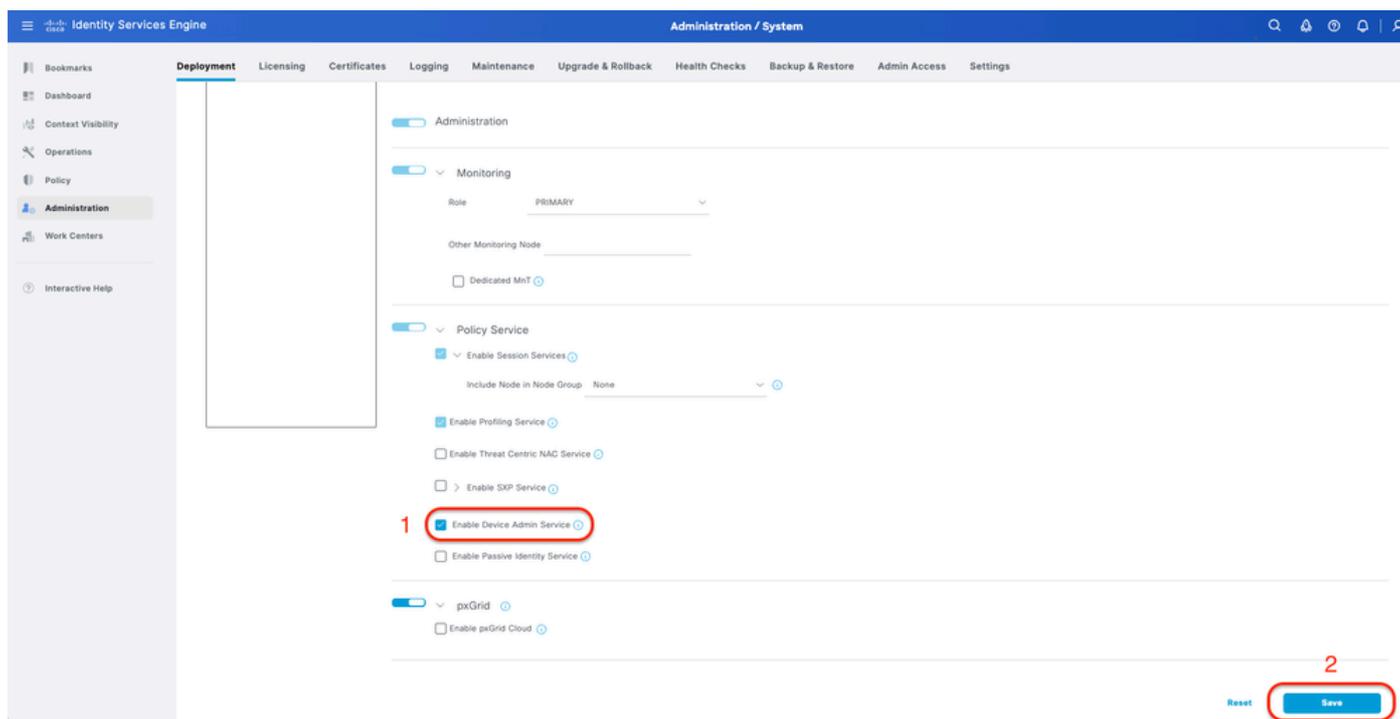


Passaggi della configurazione dell'autenticazione esterna (TACACS+)

(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.



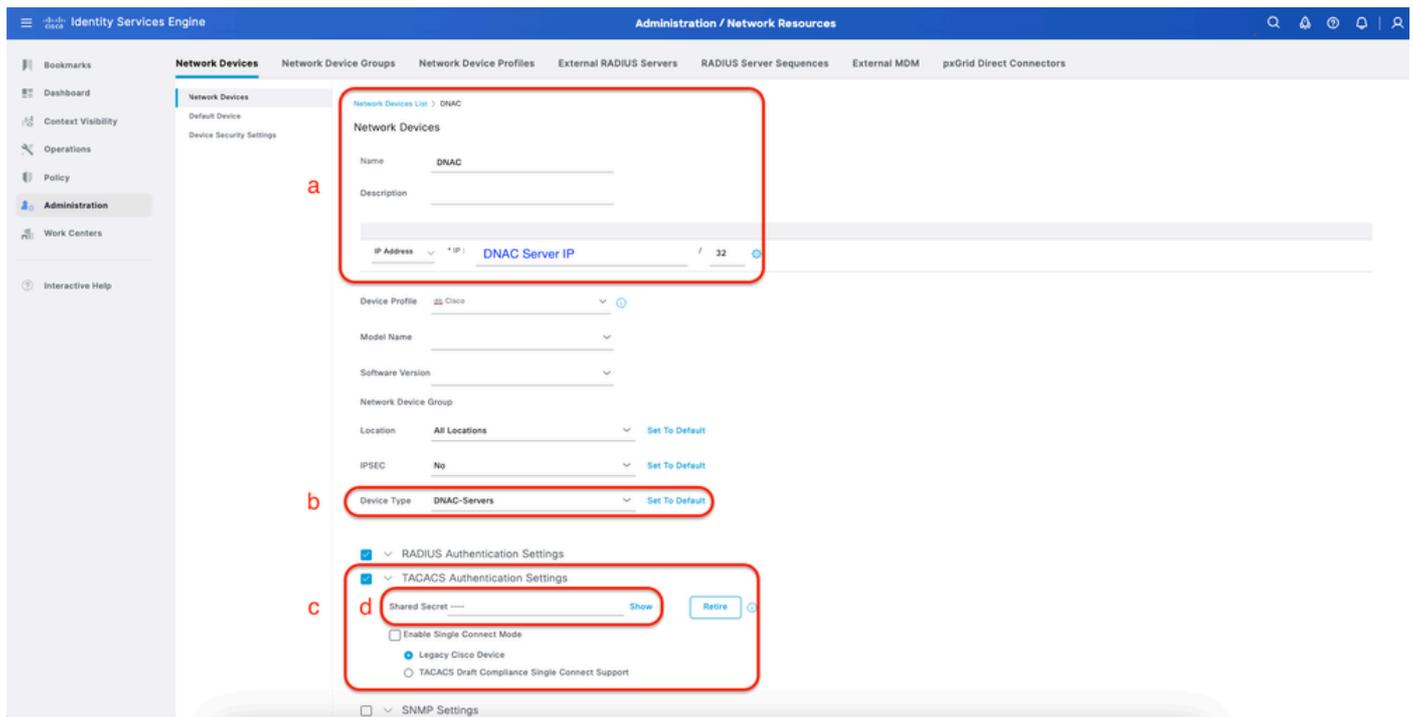
Abilita servizio di amministrazione dispositivi

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.

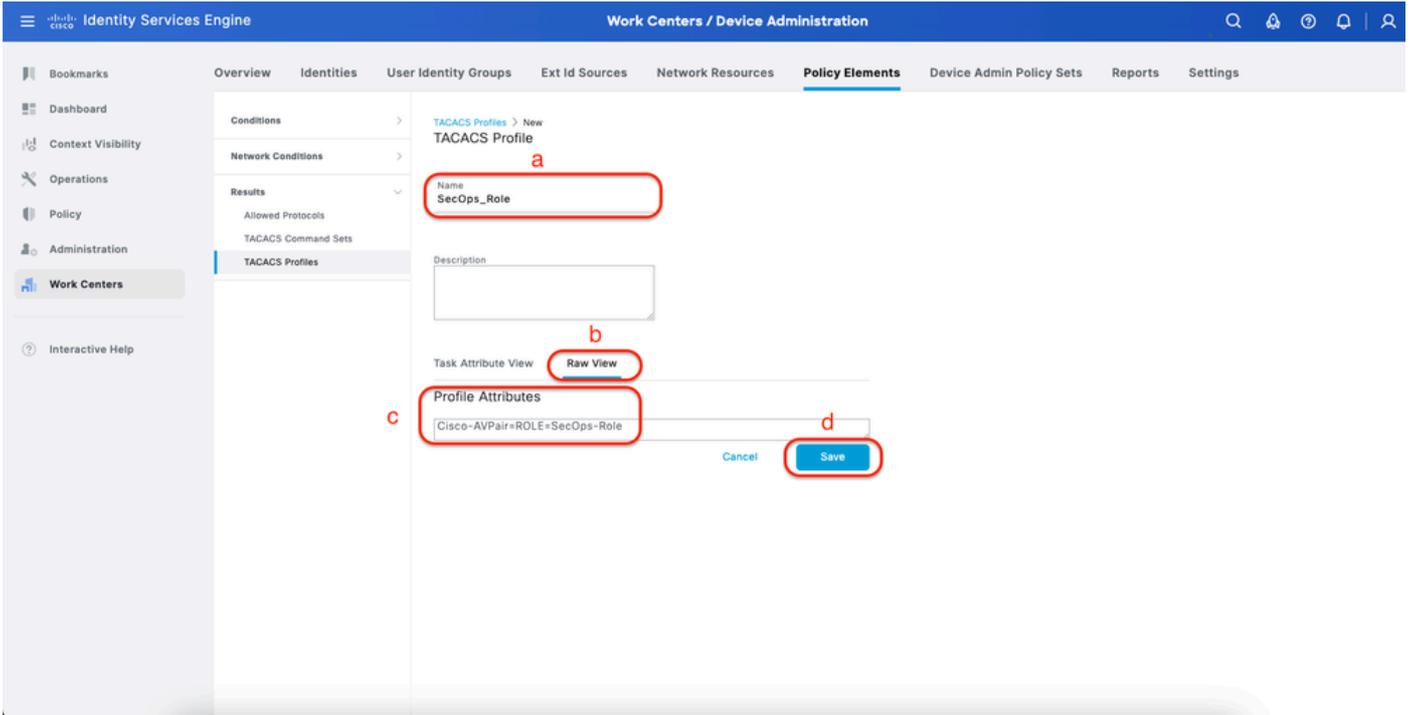
Procedura

- 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).



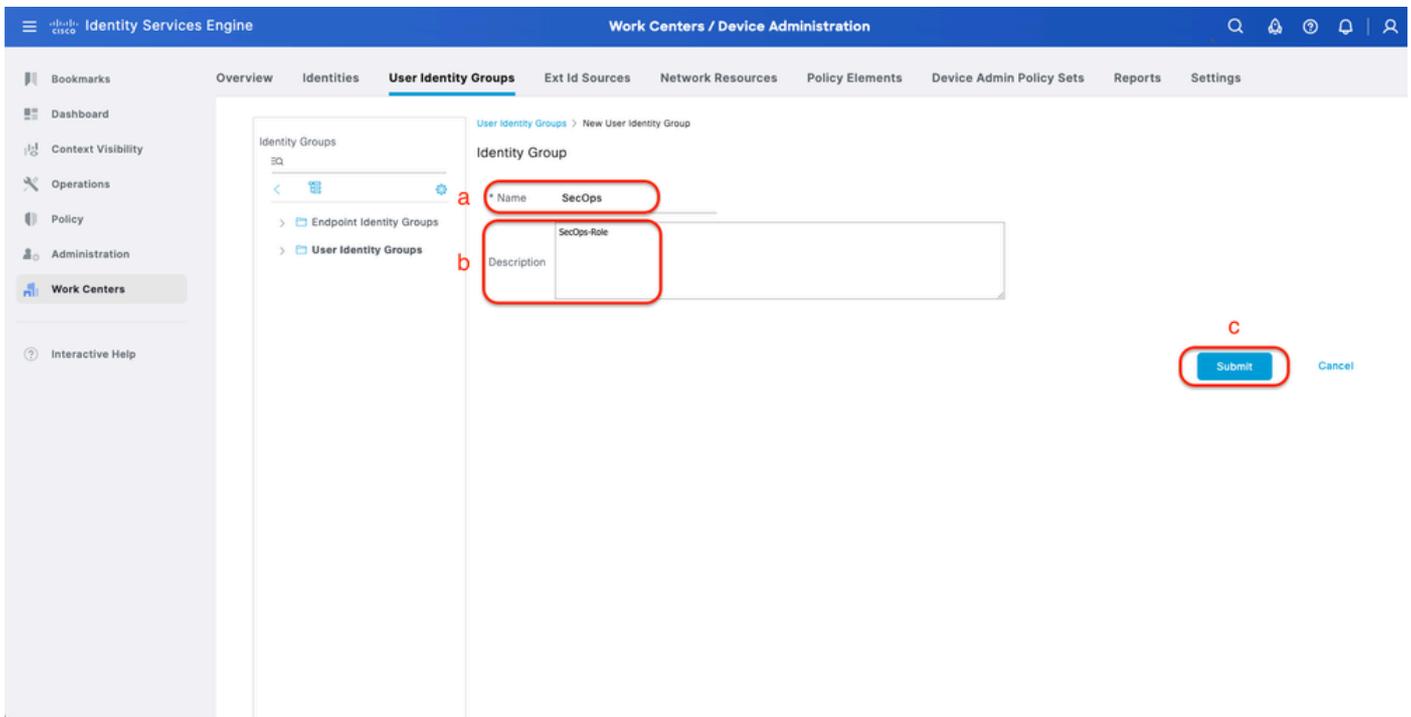
Crea profilo TACACS (SecOps_Role)

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

- Fare clic su Aggiungi e definire il nome del gruppo di identità.
- (Facoltativo) Definire la descrizione.
- Fare clic su Sottometti.



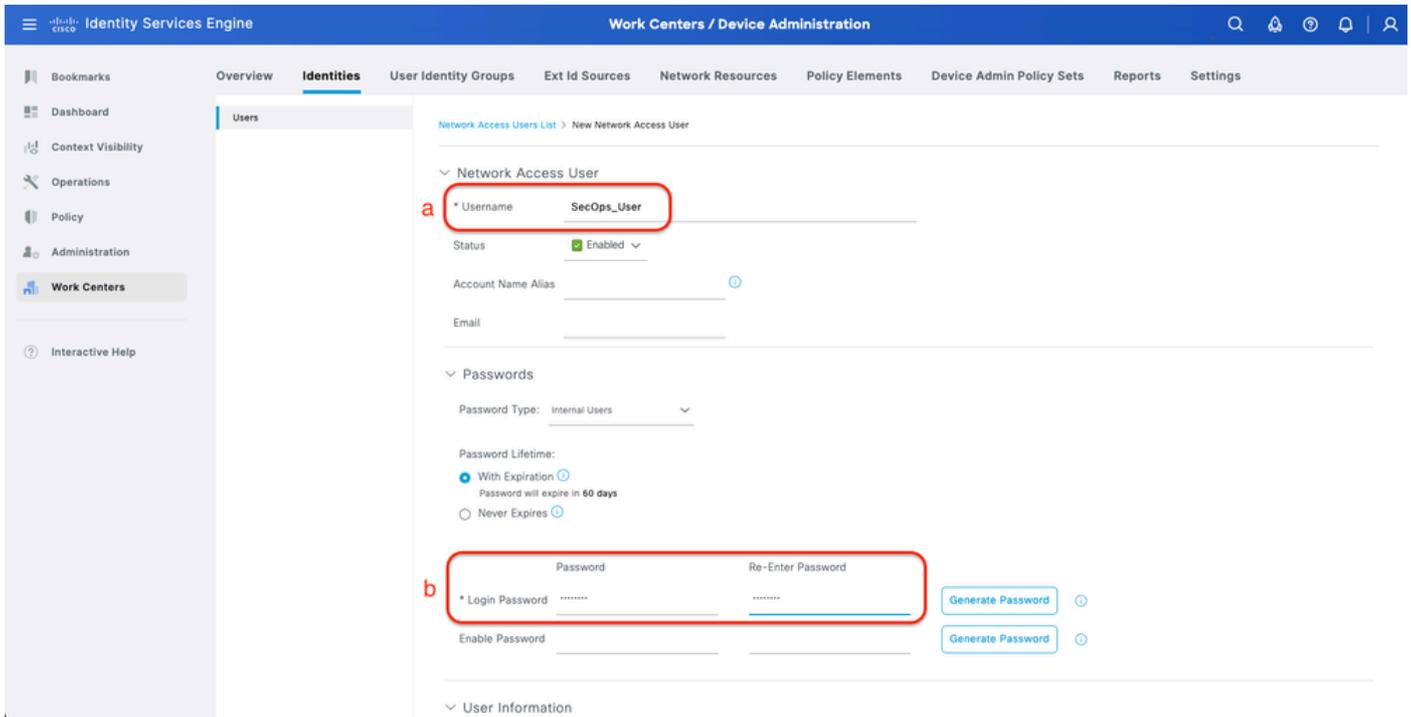
Crea gruppo di identità utente

Passaggio 5. Creare un utente locale.

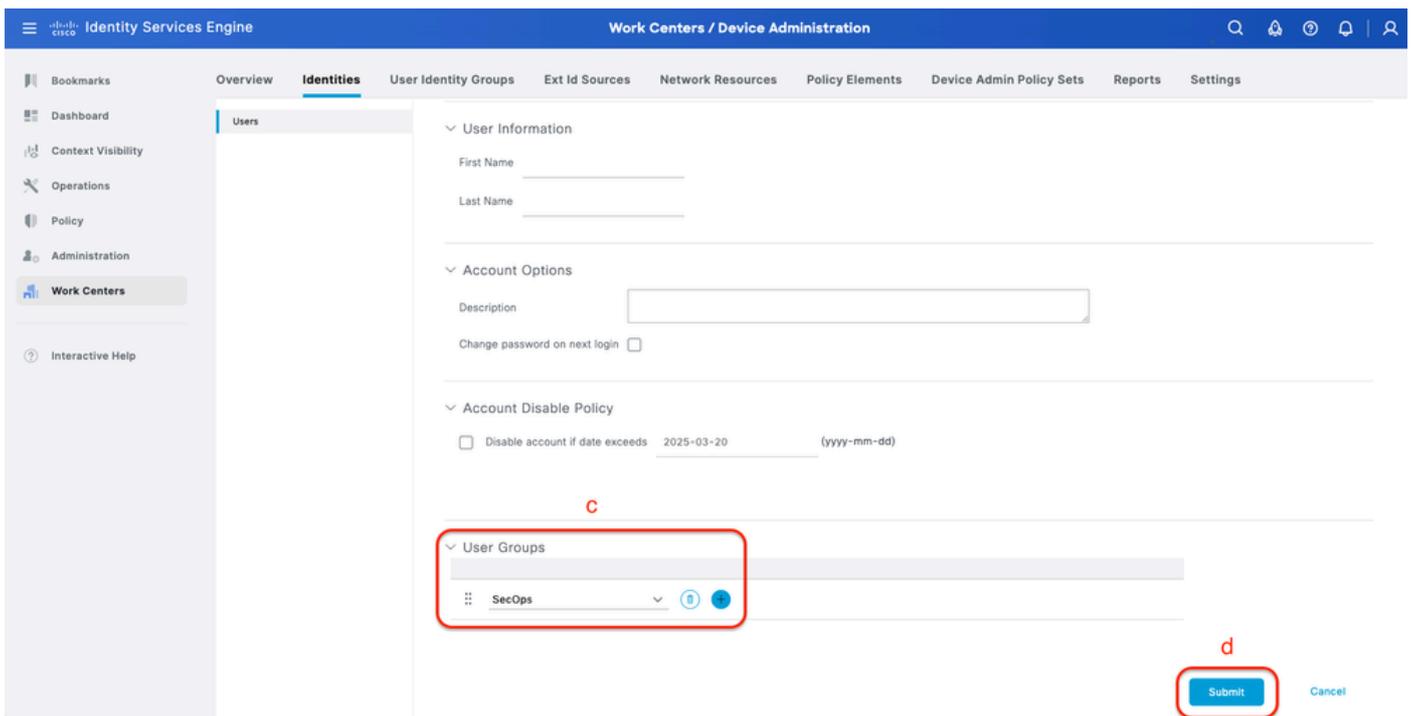
A tale scopo, è possibile selezionare la scheda Centri di lavoro > Amministrazione dispositivi > Identità > Utenti.

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.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	DNAC - Policy		DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0		>
●	Default	Default policy set		Default Network Access	0		>

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).

The screenshot displays the Cisco ISE Work Centers / Device Administration interface. The main content area is titled 'Policy Sets -> DNAC - Policy'. It features a table with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A 'Save' button is circled in red and labeled 'e'. Below this, the 'Authentication Policy(2)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The first row in this table has 'DNAC - Authentication' in the Rule Name column, 'DEVICE-Device Type EQUALS All Device Types#DNAC-Servers' in the Conditions column (labeled 'c'), and 'Internal Users' in the Use column (labeled 'd'). The 'Status' column for this row is circled in red and labeled 'b'.

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).

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
✓	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	⚙️
✓	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	⚙️
✓	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	⚙️
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️

Reset Save

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.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

Enable External User

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

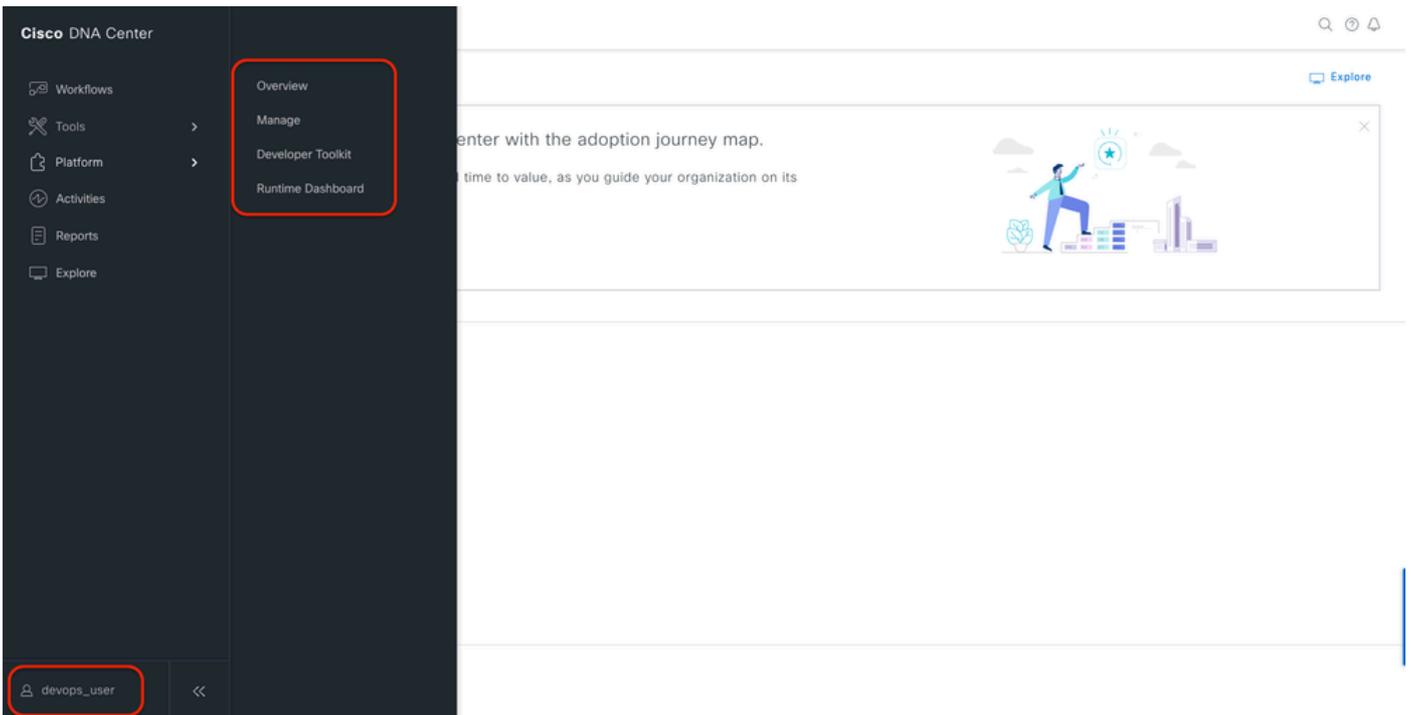
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

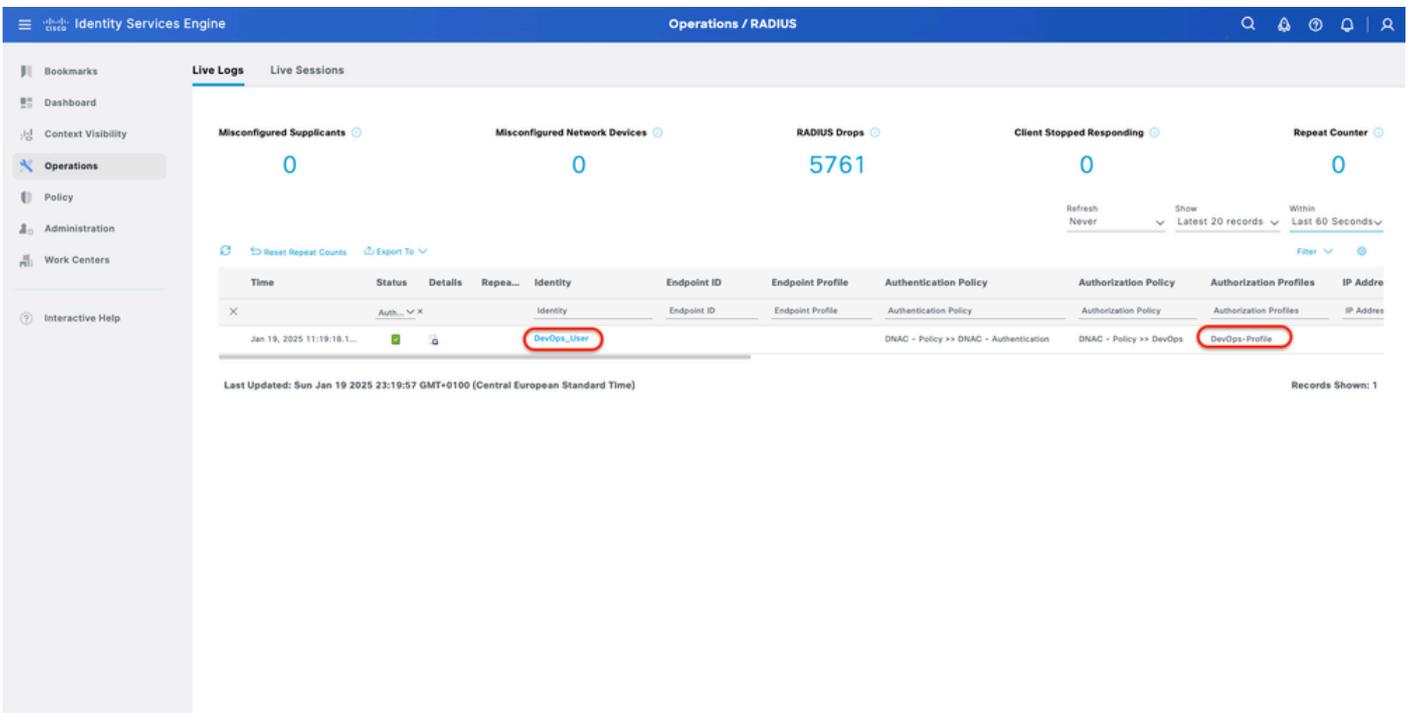
Utenti esterni

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.

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: DevOps_User

Endpoint Id:

Endpoint Profile:

Authentication Policy: DNAC - Policy >> DNAC - Authentication

Authorization Policy: DNAC - Policy >> DevOps

Authorization Result: DevOps-Profile

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

Authentication Details

Source Timestamp: 2025-01-19 23:19:18.156

Received Timestamp: 2025-01-19 23:19:18.156

Policy Server: ise34

Event: 5200 Authentication succeeded

Username: DevOps_User

User Type: User

Authentication Identity Store: Internal Users

Identity Group: User Identity Groups:DevOps

Authentication Method: PAP_ASCII

Authentication Protocol: PAP_ASCII

Network Device: DNAC

Device Type: All Device Types#DNAC-Servers

Location: All Locations

Live log dettagliati RADIUS 1-2

Cisco ISE

IdentityPolicyMatchedRule: DNAC - Authentication

AuthorizationPolicyMatchedRule: DevOps

ISEPolicySetName: DNAC - Policy

IdentitySelectionMatchedRule: DNAC - Authentication

TotalAuthnLatency: 35

ClientLatency: 0

DTLSSupport: Unknown

Network Device Profile: Cisco

Location: Location#All Locations

Device Type: Device Type#All Device Types#DNAC-Servers

IPSEC: IPSEC#Is IPSEC Device#No

Name: User Identity Groups:DevOps

EnableFlag: Enabled

RADIUS Username: DevOps_User

Device IP Address:

CPMSessionID: 0a301105o95d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=92731e30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5dedf467

Result

Class: CACS:0a301105o95d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY:ise34/528427220/15433

cisco-av-pair ROLE=DevOps-Role

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.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

Primary AAA Server Secondary AAA Server

IP Address IP Address

Shared Secret Shared Secret

View Advanced Settings View Advanced Settings

Update Update

External Users

Filter EQ Find

Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

Utenti esterni

2. DNAC - Conferma accesso utente.

Cisco DNA Center

Policy > Workflows > Tools > Platform > Activities > Explore

Group-Based Access Control
IP & URL Based Access Control

center with the adoption journey map.

time to value, as you guide your organization on its

Network Bug Identifier
Identify bugs in the network

secops_user

Accesso utente limitato

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

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#AII Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#AII Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

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.

Cisco ISE

Overview

Request Type: Authorization
 Status: Pass
 Session Key: ise34/526427220/13958
 Message Text: Device-Administration: Session Authorization succeeded
 Username: SecOps_User
 Authorization Policy: DNAC - Policy >> SecOps
 Shell Profile: SecOps_Role
 Matched Command Set
 Command From Device

Authorization Details

Generated Time: 2025-01-19 17:12:43.368 +1:00
 Logged Time: 2025-01-19 17:12:43.368
 Epoch Time (sec): 1737303163
 ISE Node: ise34
 Message Text: Device-Administration: Session Authorization succeeded
 Failure Reason
 Resolution
 Root Cause
 Username: SecOps_User
 Network Device Name: DNAC

Steps

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15017	Selected Shell Profile	2
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

Registri dettagliati TACACS+ 1-2

Type	Value
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;13=1;14=0;15=0
TotalAuthnLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=ROLE+SecOps-Role; }

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).