

Configure ISE as an External Authentication for DNAC GUI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Before you begin](#)

[Configure](#)

[\(Option1\) Configure DNAC External Authentication Using RADIUS](#)

[\(Option1\) Configure ISE for RADIUS](#)

[\(Option2\) Configure DNAC External Authentication Using TACACS+](#)

[\(Option2\) Configure ISE for TACACS+](#)

[Verify](#)

[Verify RADIUS Configuraiton](#)

[Verify TACACS+ Configuration](#)

[References](#)

Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) as an external authentication for Cisco DNA Center GUI administration.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- TACACS+ and RADIUS protocols.
- Cisco ISE Integration with Cisco DNA Center.
- Cisco ISE Policy Evaluation.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE) Version 3.4 Patch1.
- Cisco DNA Center Version-2.3.5.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before you begin

- Ensure you have at least one **RADIUS** authentication server configured on **System > Settings > External Services > Authentication and Policy Servers**.
- Only a user with **SUPER-ADMIN-ROLE** permissions on DNAC can perform this procedure.
- Enable external authentication fallback.

Note,

In releases earlier than 2.1.x, when external authentication is enabled, Cisco DNA Center falls back to local users if the AAA server is unreachable or the AAA server rejects an unknown username. In the current release, Cisco DNA Center does not fall back to local users if the AAA server is unreachable or the AAA server rejects an unknown username.

When external authentication fallback is enabled, external users and local admins can log in to Cisco DNA Center.

To enable external authentication fallback, SSH to the Cisco DNA Center instance and enter the this CLI command (*magctl rbac external_auth_fallback enable*).

Configure

(Option1) Configure DNAC External Authentication Using RADIUS

Step 1. (Optional) Define a Custom Roles.

Configure your custom roles that fulfils your requirement, instead, you can use the default User Roles. This can be done from the tab **System > Users & Roles > Role Based Access Control**.

Procedure

a. Create a New Role

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.

Role Name*
DevOps-Role

Describe the role (optional)

2

Exit

Next

b. Define the Access

Define the Access

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.

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.

Exit Review Back **Next**

c. Create the New 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 [Edit](#)

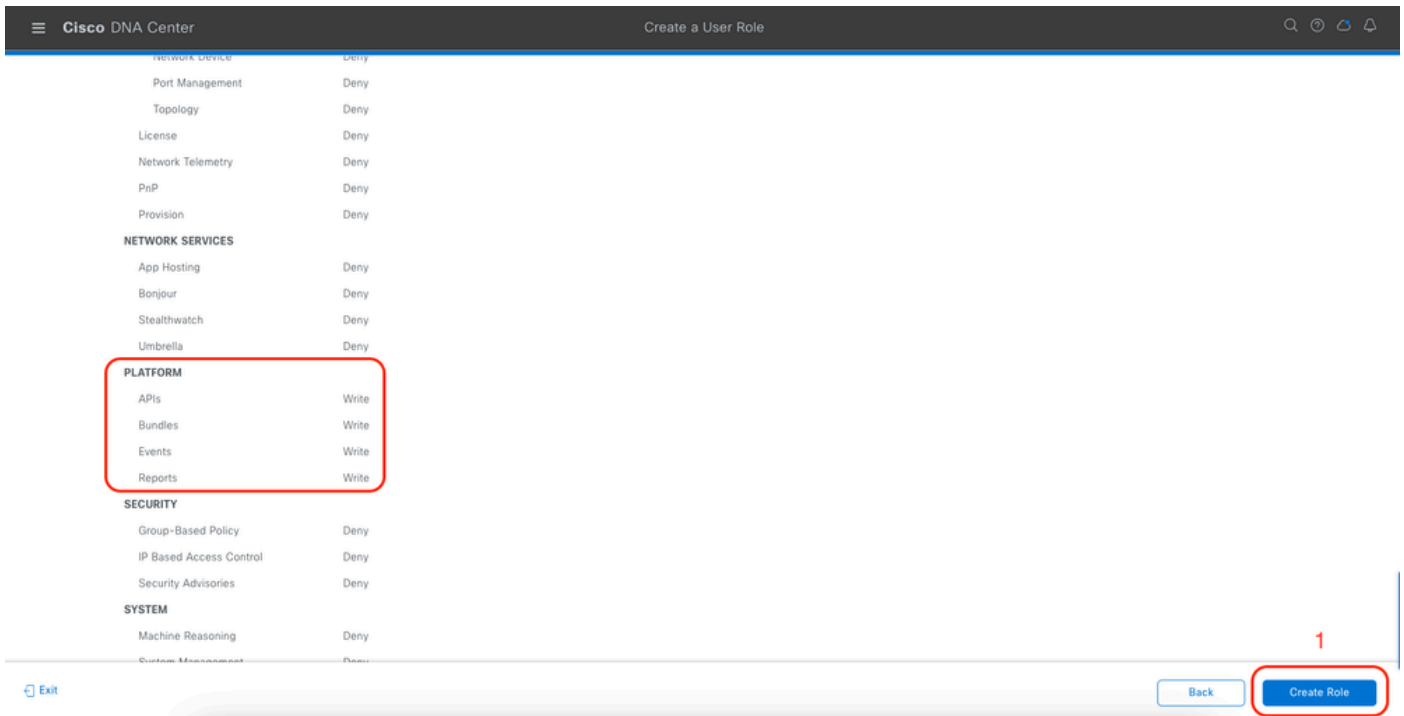
Role Name DevOps-Role

Role Description

Role Capability [Edit](#)

Capability	Permission
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**



Review and Create DevOps Role

Step 2. Configure External Authentication Using RADIUS

This can be done from the tab **System > Users & Roles > External Authentication**.

Procedure

- To enable external authentication in Cisco DNA Center, check the **Enable External User** check box.
- Set the **AAA attributes**.

Enter **Cisco-AVPair** in the **AAA attributes** field.

- (Optional) Configure Primary and Secondary AAA Server.

Ensure **RADIUS** protocol is enabled on **Primary AAA Server** at least, or on both Primary and Secondary server.

System / Users & Roles

External Authentication

Enable External User

AAA Attribute: Cisco-AVPair

Reset to Default Update

Primary AAA Server	Secondary AAA Server
IP Address: ISE Server 1 IP	IP Address: ISE Server 2 IP
Shared Secret: *****	Shared Secret: *****
<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS
Authentication Port: 1812	Authentication Port: 1812

(RADIUS) External Authentication Configuration Steps

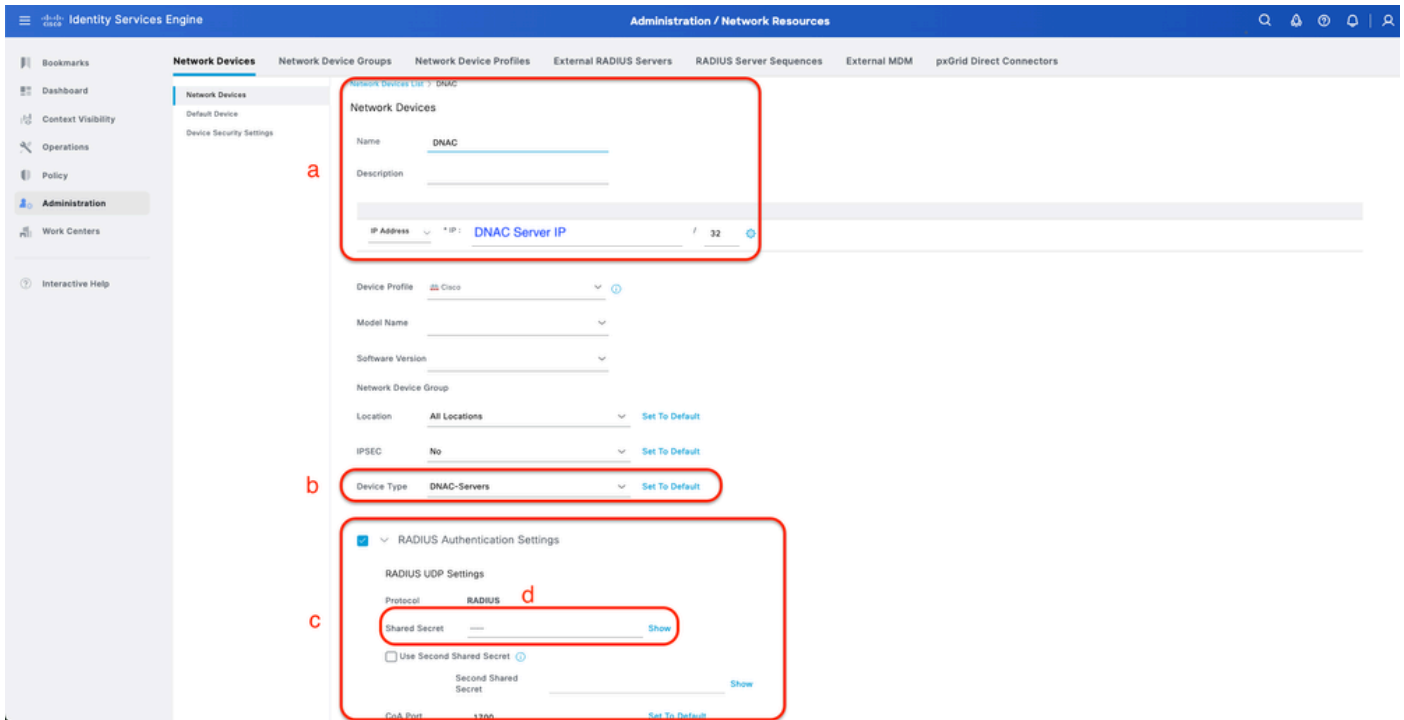
(Option1) Configure ISE for RADIUS

Step 1. Add DNAC server as a Network Device on ISE

This can be done from the tab **Administration > Network Resources > Network Devices**.

Procedure

- Define (DNAC) Network Device name and IP
- (Optional) Classify Device Type for Policy Set condition
- Enable RADIUS Authentication Settings
- Set RADIUS Shared Secret



ISE Network Device (DNAC) for RADIUS

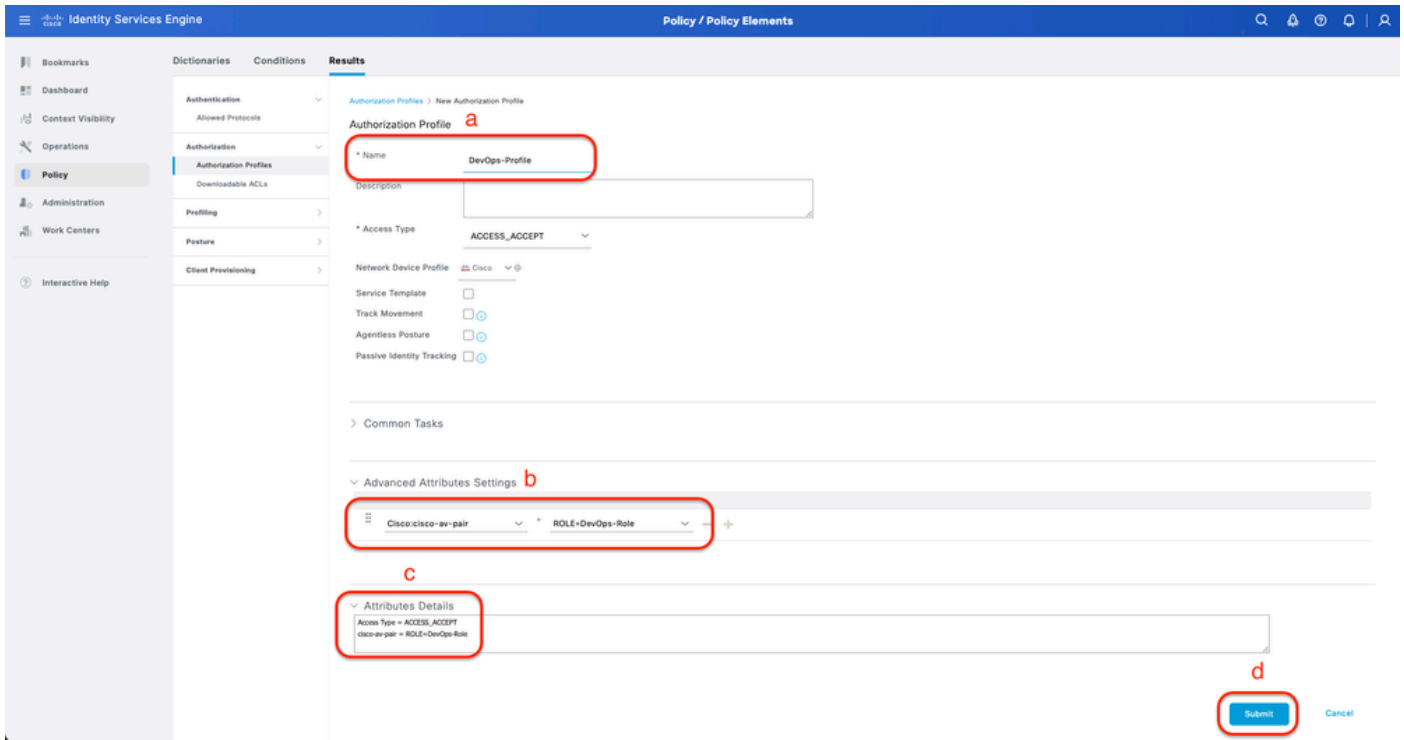
Step 2. Create RADIUS Authorization Profiles

This can be done from the tab **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Note, create 3x RADIUS Authorization Profiles, one for each User Role.

Procedure

- a. Click **Add** and define the RADIUS Authorization Profile name
- b. Enter the **Cisco:cisco-av-pair** in the Advanced **Attributes Settings** and fill the correct User role
 - For the (DecOps-Role) user role, enter **ROLE=DevOps-Role**
 - For the (NETWORK-ADMIN-ROLE) user role, enter **ROLE=NETWORK-ADMIN-ROLE**
 - For the(SUPER-ADMIN-ROLE) user role, enter **ROLE=SUPER-ADMIN-ROLE**
- c. Review the **Attribute Details**
- d. Click **Save**



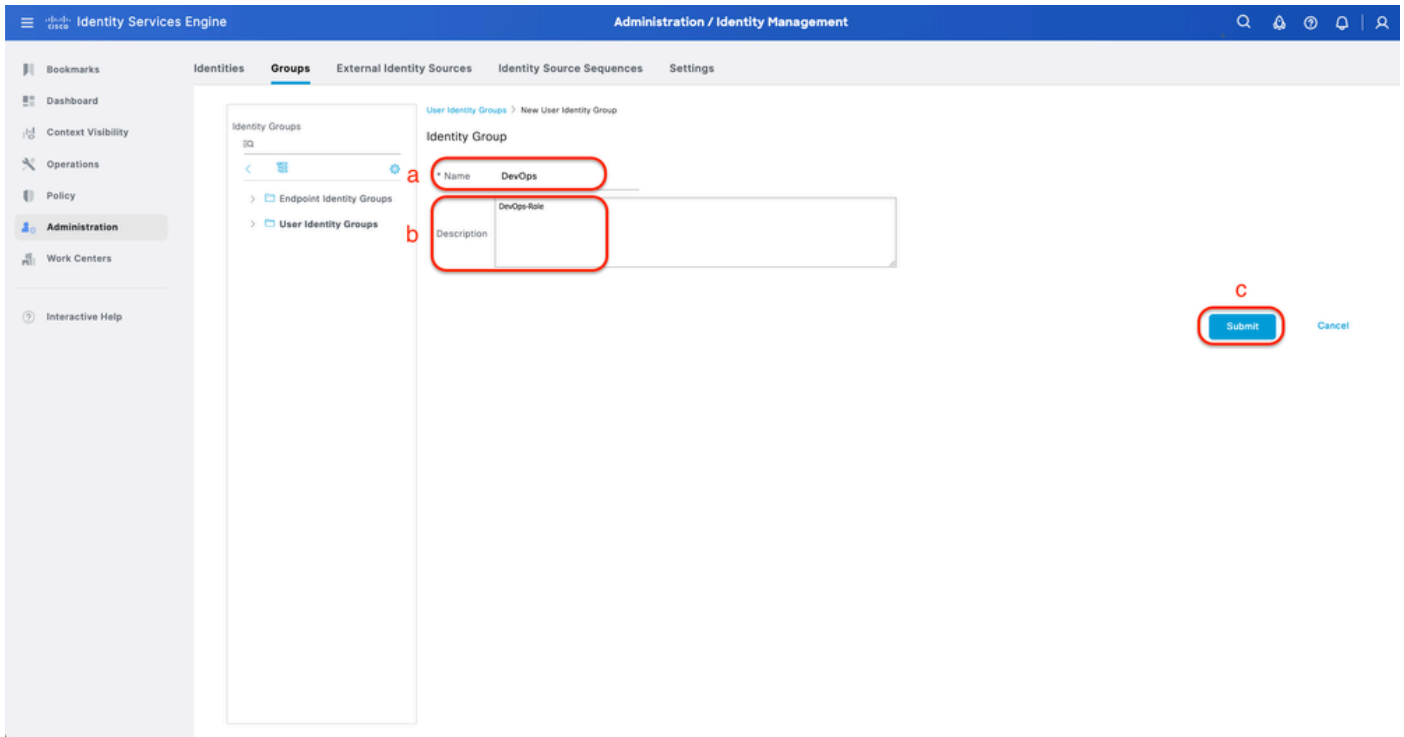
Create Authorization Profile

Step 3. Create User Group

This can be done from the tab **Administration > Identity Management > Groups > User Identity Groups**.

Procedure

- a. Click **Add** and define the Identity Group name
- b. (Optional) Define the Description
- c. Click **Submit**



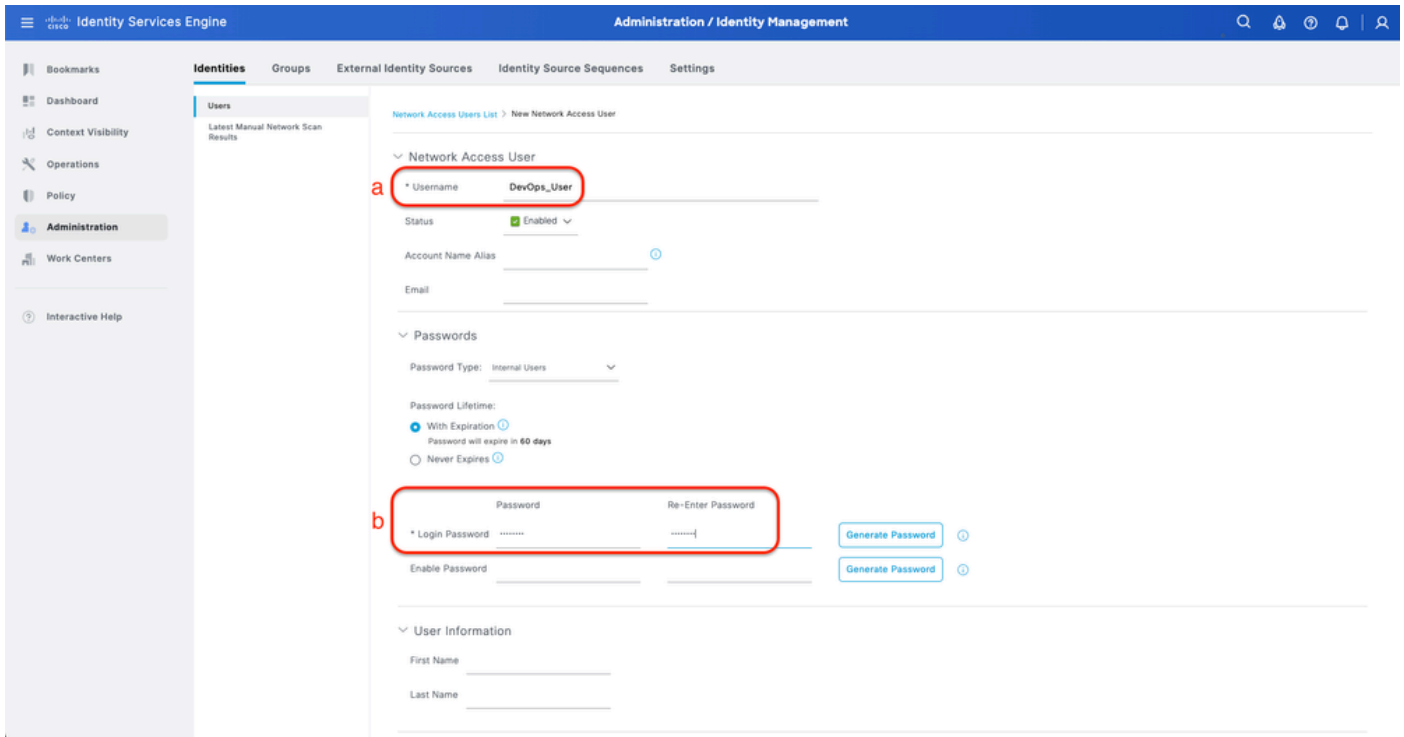
Create User Identity Group

Step 4. Create Local User

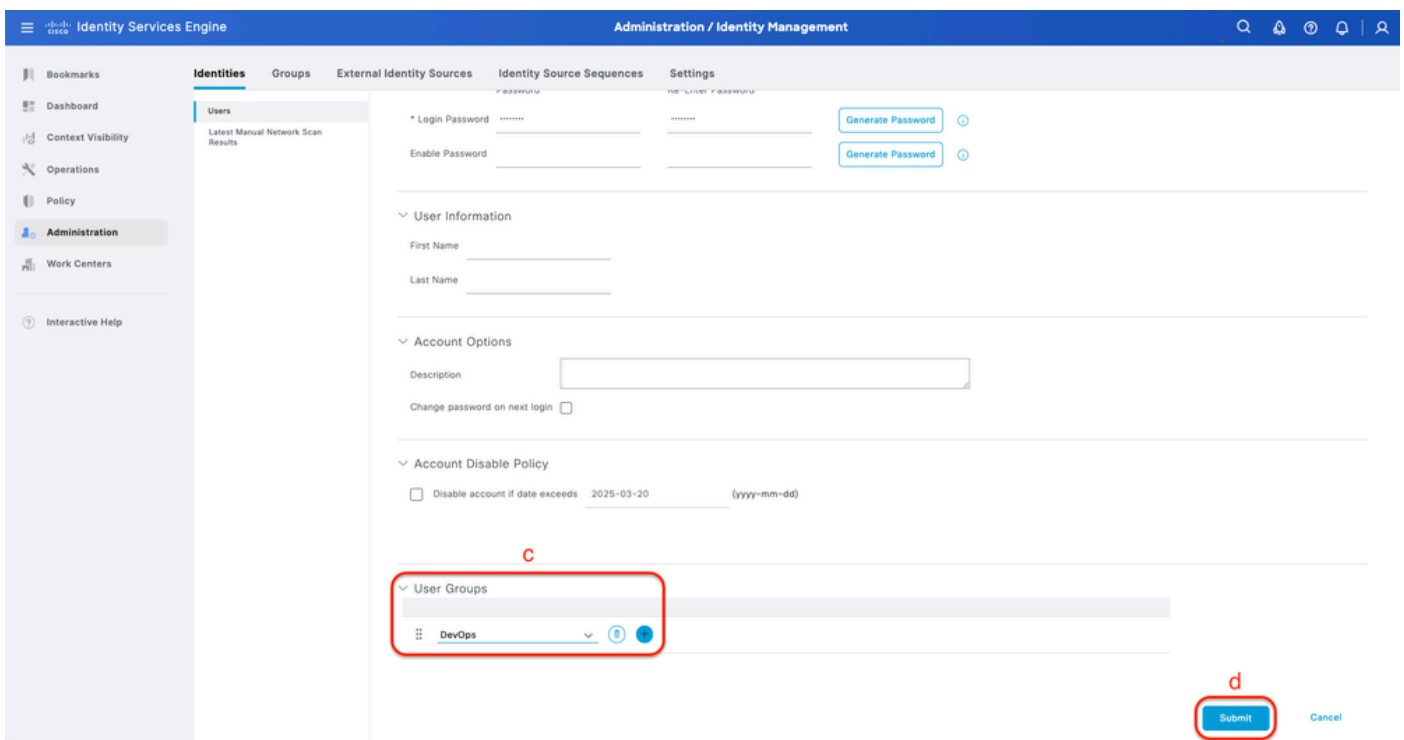
This can be done from the tab **Administration > Identity Management > Identities > Users**.

Procedure

- a. Click **Add** and define the Username
- b. Set the Login Password
- c. Add the user to the related user group.
- d. Click **Submit**



Create Local User 1-2



Create Local User 2-2

Step 5. (Optional) Add RADIUS Policy Set

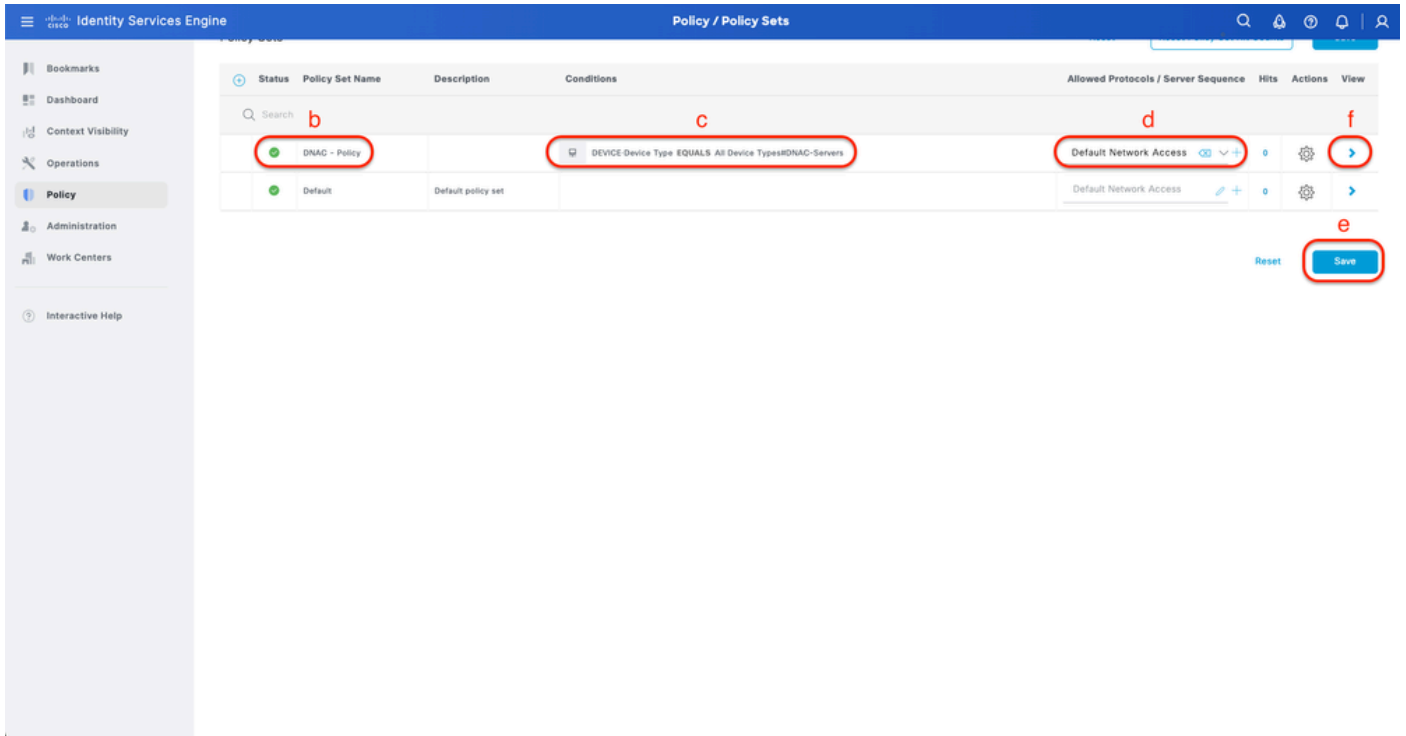
This can be done from the tab **Policy > Policy Sets**.

Procedure

a. Click **Actions** and choose (**Insert new row above**)

b. Define the Policy Set name

- c. Set the Policy Set **Condition** to **Select** Device Type you created previously on (Step1 > b)
- d. Set the Allowed protocols
- e. Click **Save**
- f. Click (>) Policy Set View to configure authentication and authorization rules



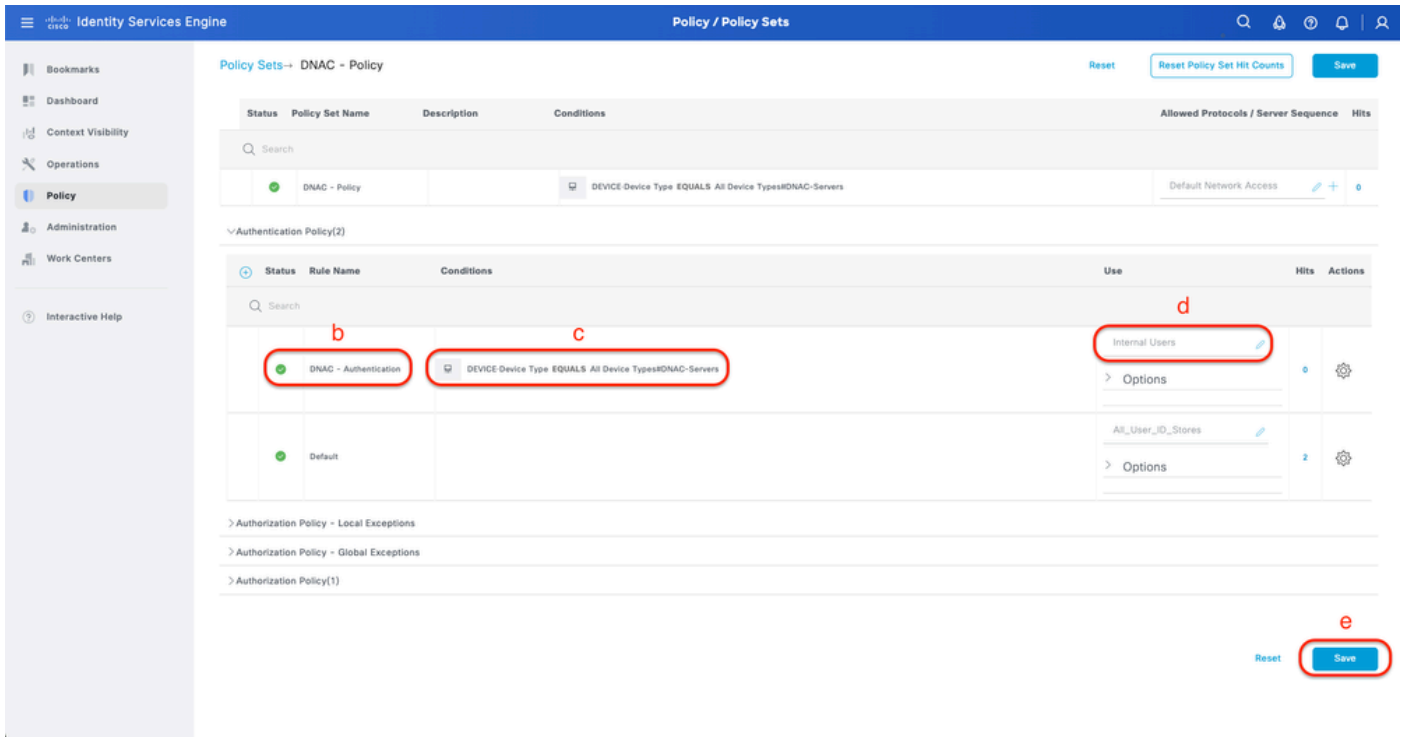
Add RADIUS Policy Set

Step 6. Configure RADIUS Authentication Policy

This can be done from the tab **Policy > Policy Sets > Click (>)**.

Procedure

- a. Click **Actions** and **choose (Insert new row above)**
- b. Define the Authentication Policy name
- c. Set the Authentication Policy **Condition** and **Select** Device Type you created previously on (Step1 > b)
- d. Set the Authentication Policy **Use** for Identity source
- e. Click **Save**



Add RADIUS Authentication Policy

Step 7. Configure RADIUS Authorization Policy

This can be done from the tab **Policy** > **Policy Sets**> **Click (>)**.

This step to create Authorization Policy for each User Role.

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- DevOps-Role

Procedure

- Click **Actions** and **choose (Insert new row above)**
- Define the Authorization Policy name
- Set the Authorization Policy **Condition** and **Select** User Group that you created in (Step3)
- Set the Authorization Policy **Results/Profiles** and **Select** Authorization Profile that you created in (Step2)
- Click **Save**

Add Authorization Policy

(Option2) Configure DNAC External Authentication Using TACACS+

Step 1. (Optional) Define a Custom Roles.

Configure your custom roles that fulfils your requirement, instead, you can use the default User Roles. This can be done from the tab **System > Users & Roles > Role Based Access Control**.

Procedure

a. Create a New Role

SecOps Role Name

b. Define the Access

Define the Access

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.

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

Exit Review Back **Next**

SecOps Role Access

c. Create the New 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](#)

Capability	Permission
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**

SecOps Role Summary

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

Review and Create SecOps Role

Step 2. Configure External Authentication Using TACACS+

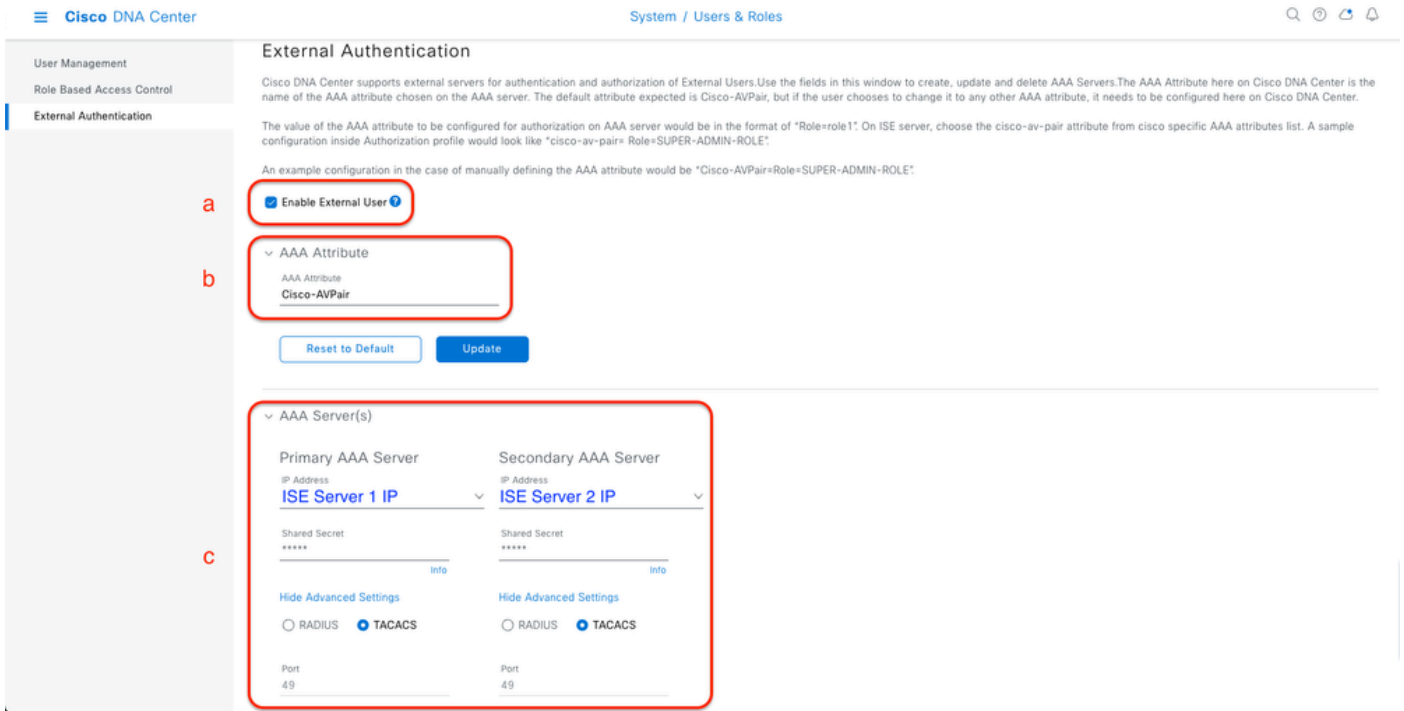
This can be done from the tab **System > Users & Roles > External Authentication**.

- To enable external authentication in Cisco DNA Center, check the **Enable External User** check box.
- Set the **AAA attributes**.

Enter **Cisco-AVPair** in the **AAA attributes** field.

- (Optional) Configure Primary and Secondary AAA Server.

Ensure **TACACS+** protocol is enabled on **Primary AAA Server** at least, or on both Primary and Secondary server.

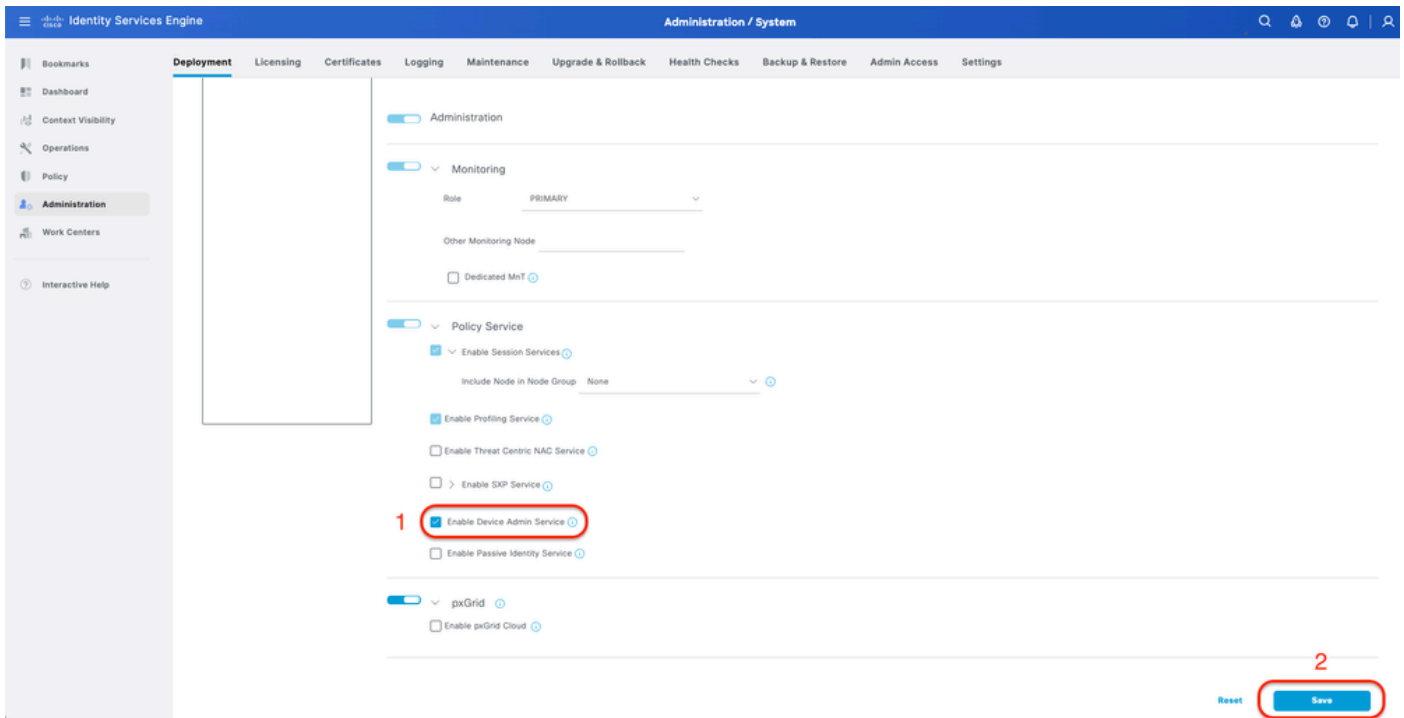


(TACACS+) External Authentication Configuration Steps

(Option2) Configure ISE for TACACS+

Step 1. Enable Device Admin Service

This can be done from the tab **Administration** > **System** > **Deployment** > **Edit (ISE PSN Node)** > **Check Enable Device Admin Service**.



Enable Device Admin Service

Step 2. Add DNAC server as a Network Device on ISE

This can be done from the tab **Administration** > **Network Resources** > **Network Devices**.

Procedure

- Define (DNAC) Network Device name and IP
- (Optional) Classify Device Type for Policy Set condition
- Enable TACACS+ authentication Settings
- Set TACACS+ Shared Secret

ISE Network Device (DNAC) for TACACS+

Step 3. Create TACACS+ Profiles for each DNAC role

This can be done from the tab **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

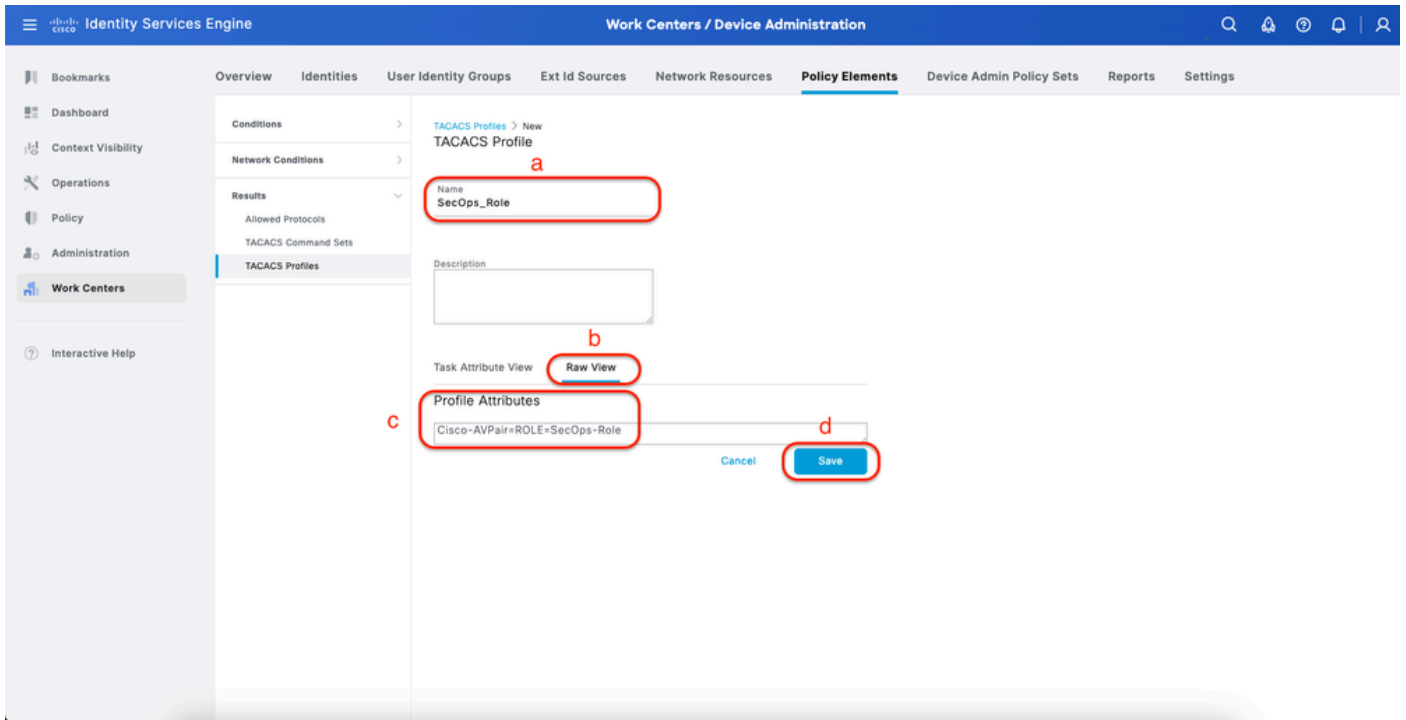
Note, create 3x TACACS+ Profiles, one for each User Role.

Procedure

- Click **Add** and define the **TACACS Profile** name
- Click the **Raw View** tab
- Enter the **Cisco-AVPair=ROLE=** and fill the correct User role
 - For the (SecOps-Role) user role, enter **Cisco-AVPair=ROLE=SecOps-Role**
 - For the (NETWORK-ADMIN-ROLE) user role, enter **Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE**
 - For the(SUPER-ADMIN-ROLE) user role, enter **Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE**

Note, remember AVPair value (**Cisco-AVPair=ROLE=<User Role>**) is a case-sensitive and ensure it is matching to the DNAC User Role.

- Click **Save**



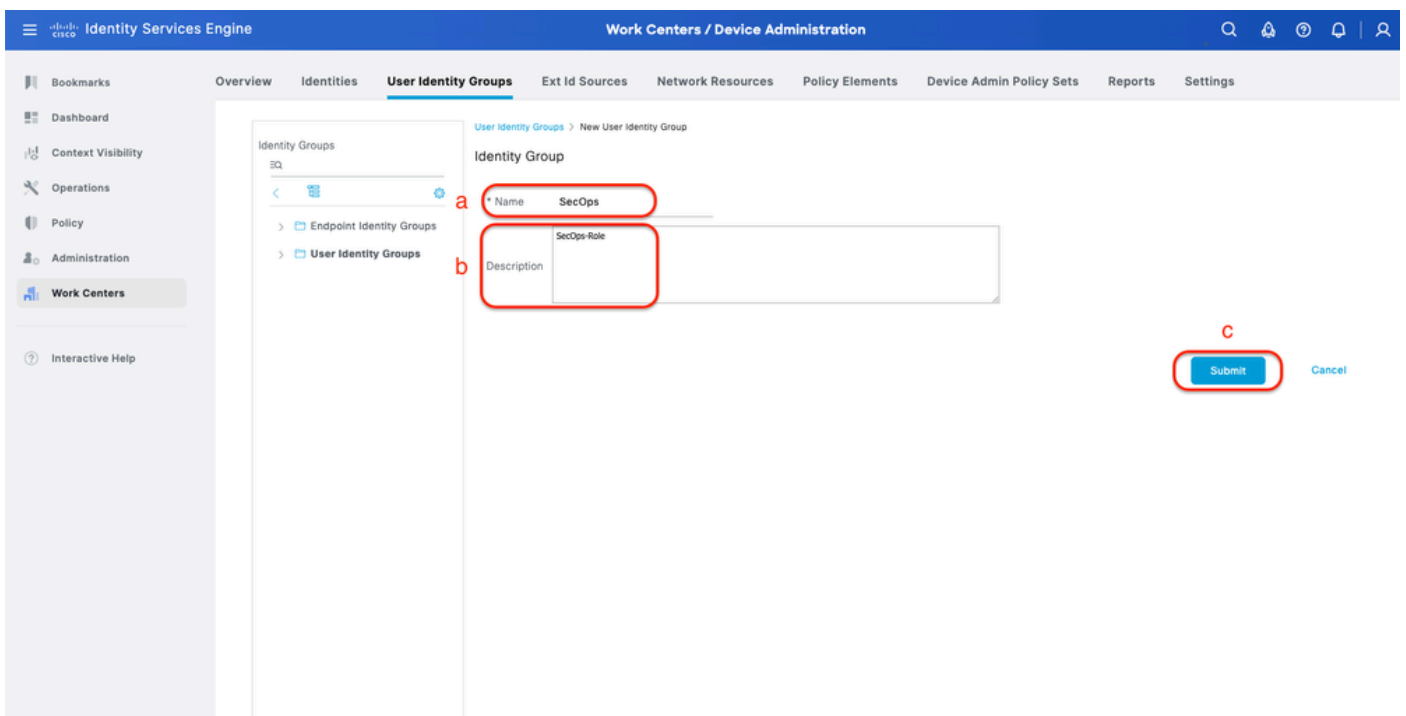
Create TACACS Profile (SecOps_Role)

Step 4. Create User Group

This can be done from the tab **Work Centers > Device Administration > User Identity Groups**.

Procedure

- a. Click **Add** and define the Identity Group name
- b. (Optional) Define the Description
- c. Click **Submit**



Create User Identity Group

Step 5. Create Local User

This can be done from the tab **Work Centers > Device Administration > Identities > Users**.

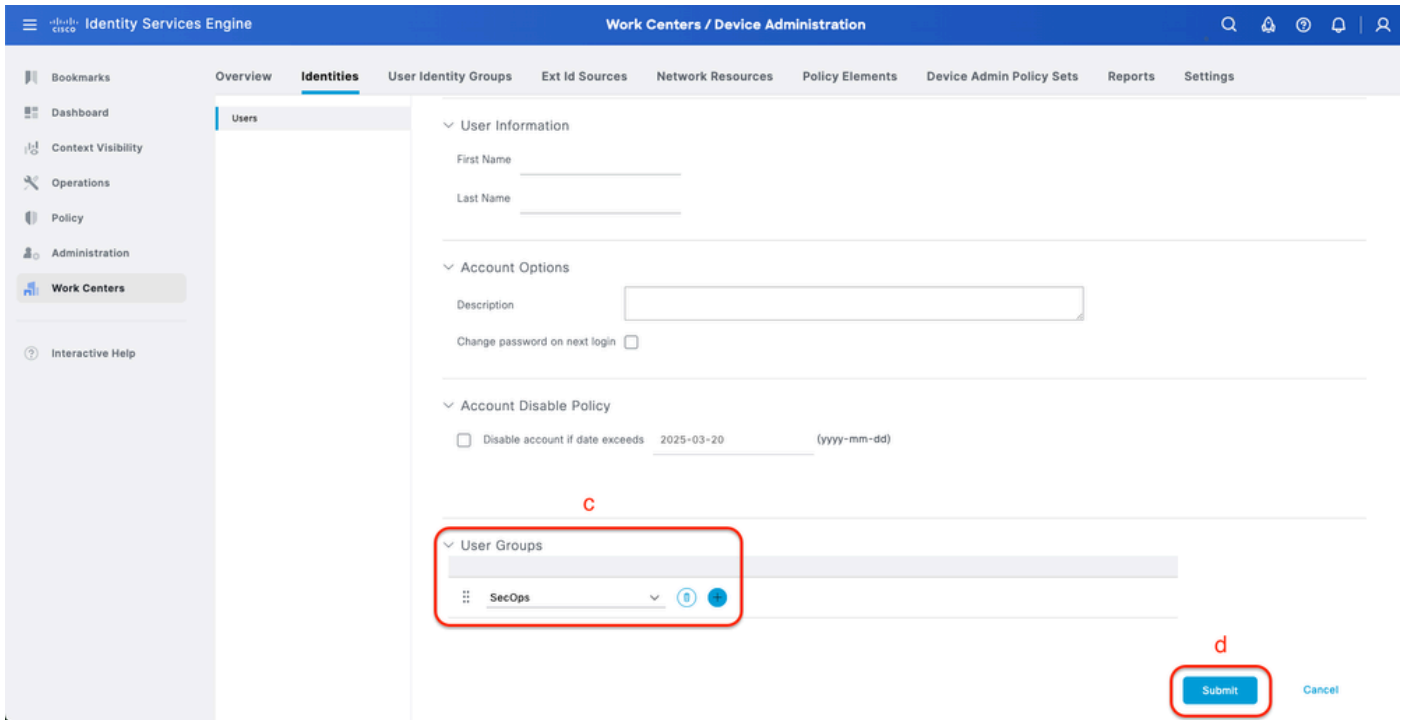
Procedure

- Click **Add** and define the Username
- Set the Login Password
- Add the user to the related user group.
- Click **Submit**

The screenshot displays the 'New Network Access User' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Work Centers / Device Administration' and shows the 'Users' section under 'Identities'. The configuration form includes the following fields and options:

- Username:** * Username (highlighted with a red box labeled 'a')
- Status:** Enabled Disabled
- Account Name Alias:**
- Email:**
- Passwords:**
 - Password Type:** Internal Users
 - Password Lifetime:**
 - With Expiration (Password will expire in 60 days)
 - Never Expires
 - Password:** (highlighted with a red box labeled 'b')
 - Re-Enter Password:** (highlighted with a red box labeled 'b')
 - Generate Password:**
 - Enable Password:**
- User Information:**

Create Local User 1-2



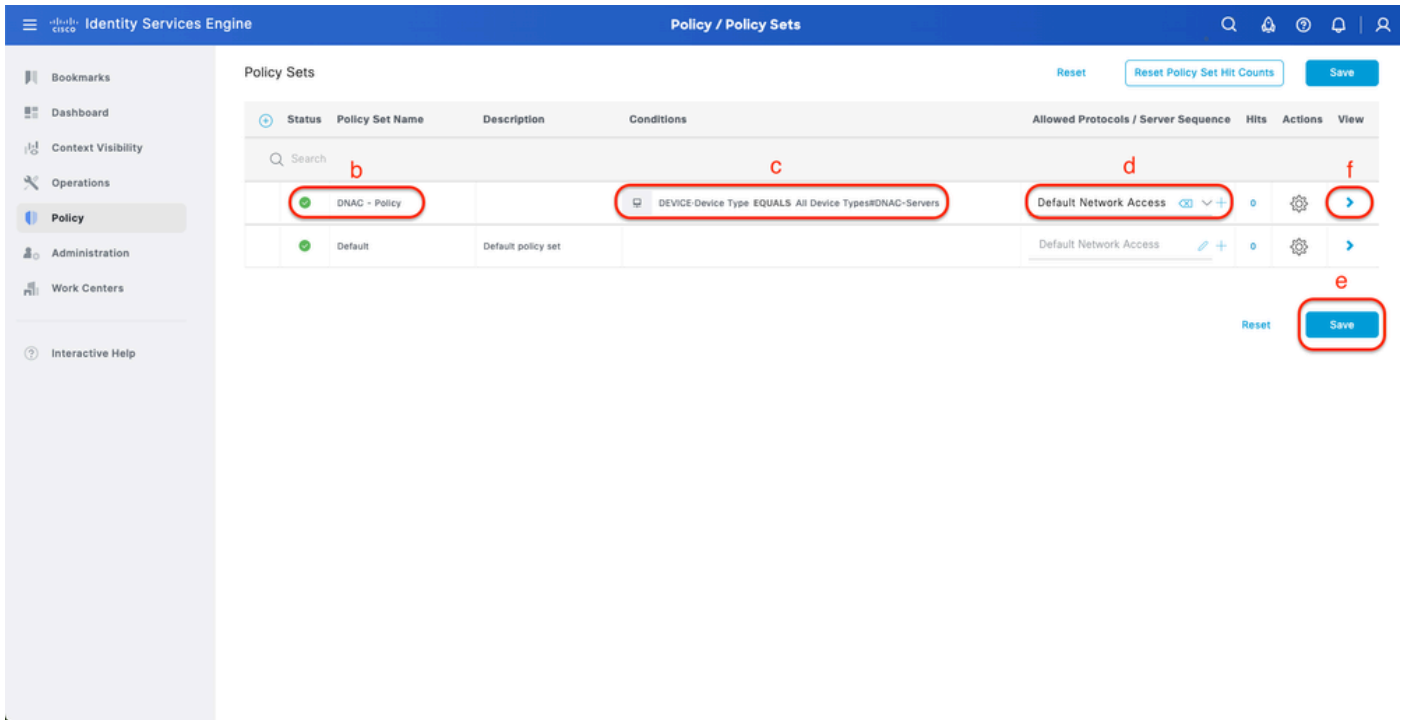
Create Local User 2-2

Step 6. (Optional) Add TACACS+ Policy Set

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets**.

Procedure

- a. Click **Actions** and **choose (Insert new row above)**
- b. Define the Policy Set name
- c. Set the Policy Set **Condition** to **Select Device Type** you created previously on (Step2 > b)
- d. Set the Allowed protocols
- e. Click **Save**
- f. Click (>) Policy Set View to configure authentication and authorization rules



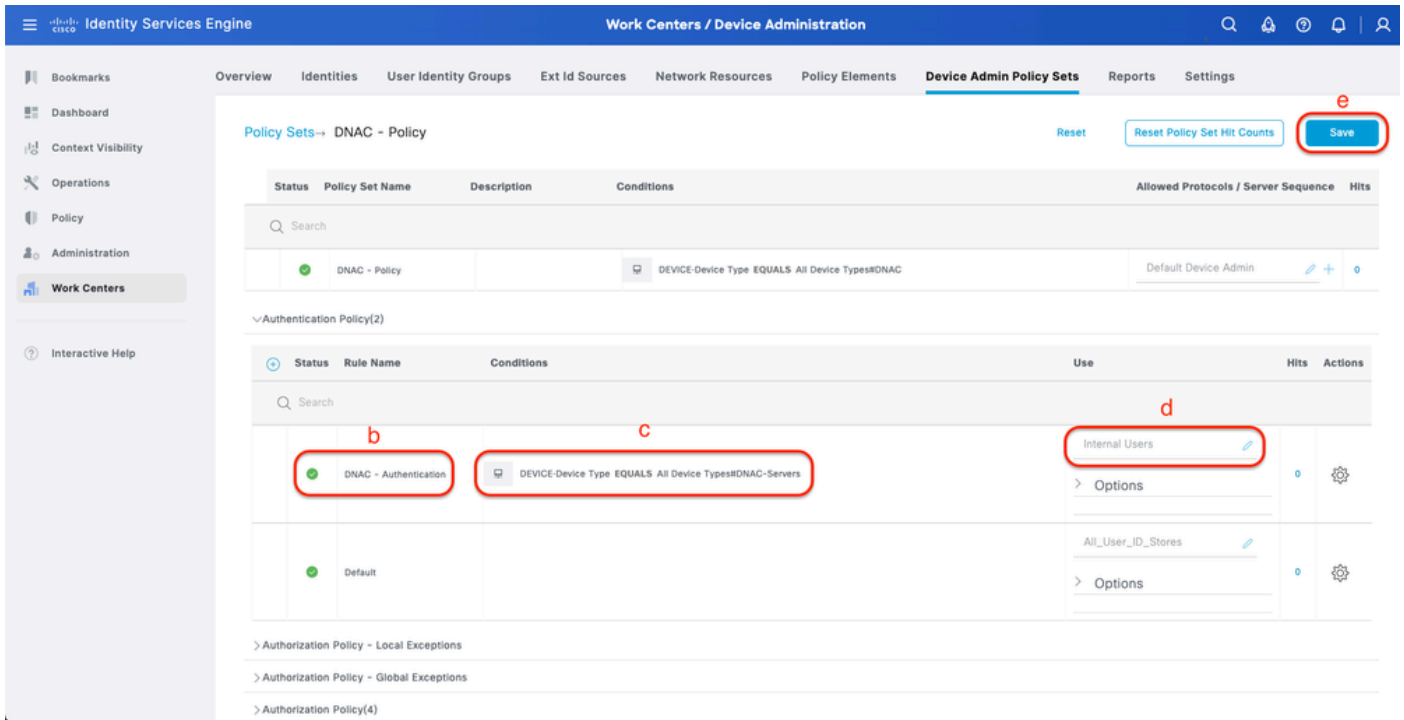
Add TACACS+ Policy Set

Step 7. Configure TACACS+ Authentication Policy

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>)**.

Procedure

- Click **Actions** and **choose (Insert new row above)**
- Define the Authentication Policy name
- Set the Authentication Policy **Condition** and **Select** Device Type you created previously on (Step2 > b)
- Set the Authentication Policy **Use** for Identity source
- Click **Save**



Add TACACS+ Authentication Policy

Step 8. Configure TACACS+ Authorization Policy

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>)**.

This step to create Authorization Policy for each User Role.

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- SecOps-Role

Procedure

- Click **Actions** and choose (**Insert new row above**)
- Define the Authorization Policy name
- Set the Authorization Policy **Condition** and **Select** User Group that you created in (Step4)
- Set the Authorization Policy **Shell Profiles** and **Select** TACACS Profile that you created in (Step3)
- Click **Save**

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

< 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

Add Authorization Policy

Verify

Verify RADIUS Configuraiton

1- DNAC - Display External Users **System > Users & Roles > External Authentication > External Users**. You can view the list of external users who have logged in through RADIUS for the first time. The information that is displayed includes their usernames and roles.

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

AAA Attribute

Cisco-AVPair

Reset to Default Update

AAA Server(s)

External Users

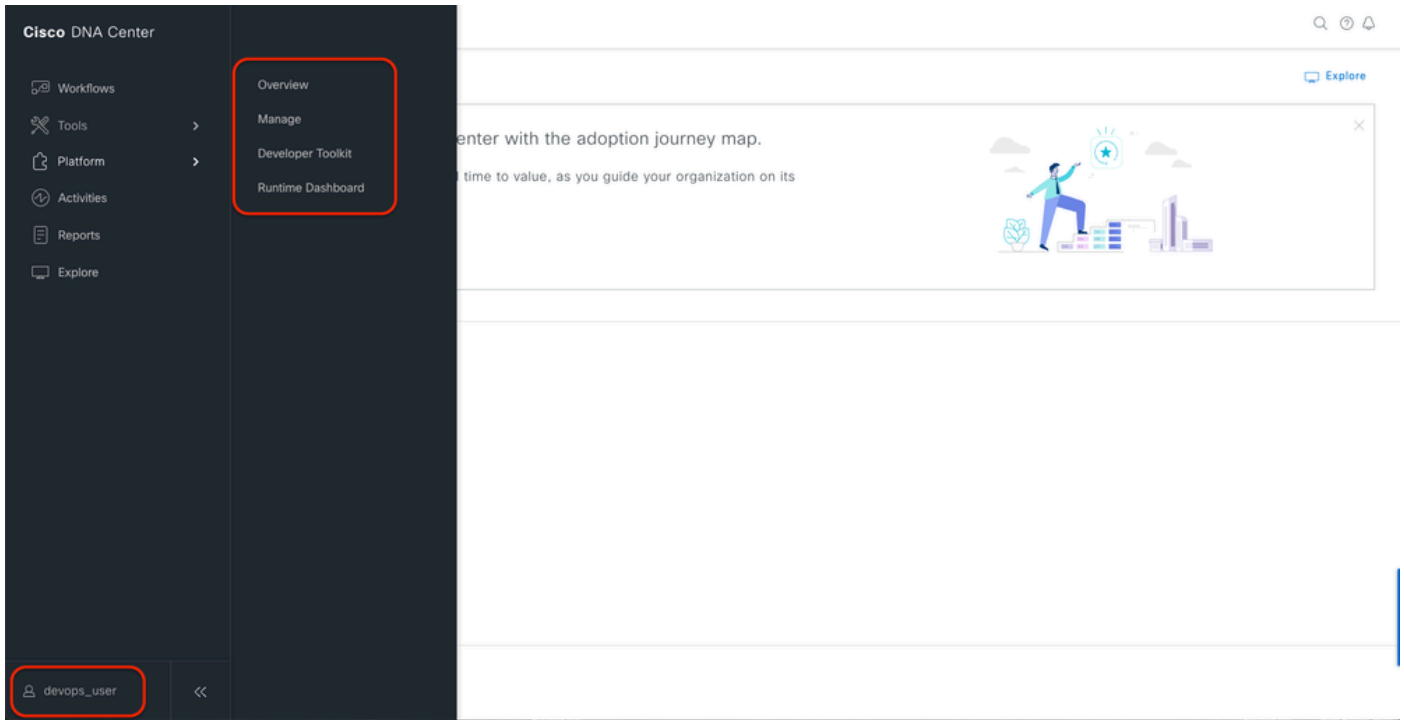
Filter

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

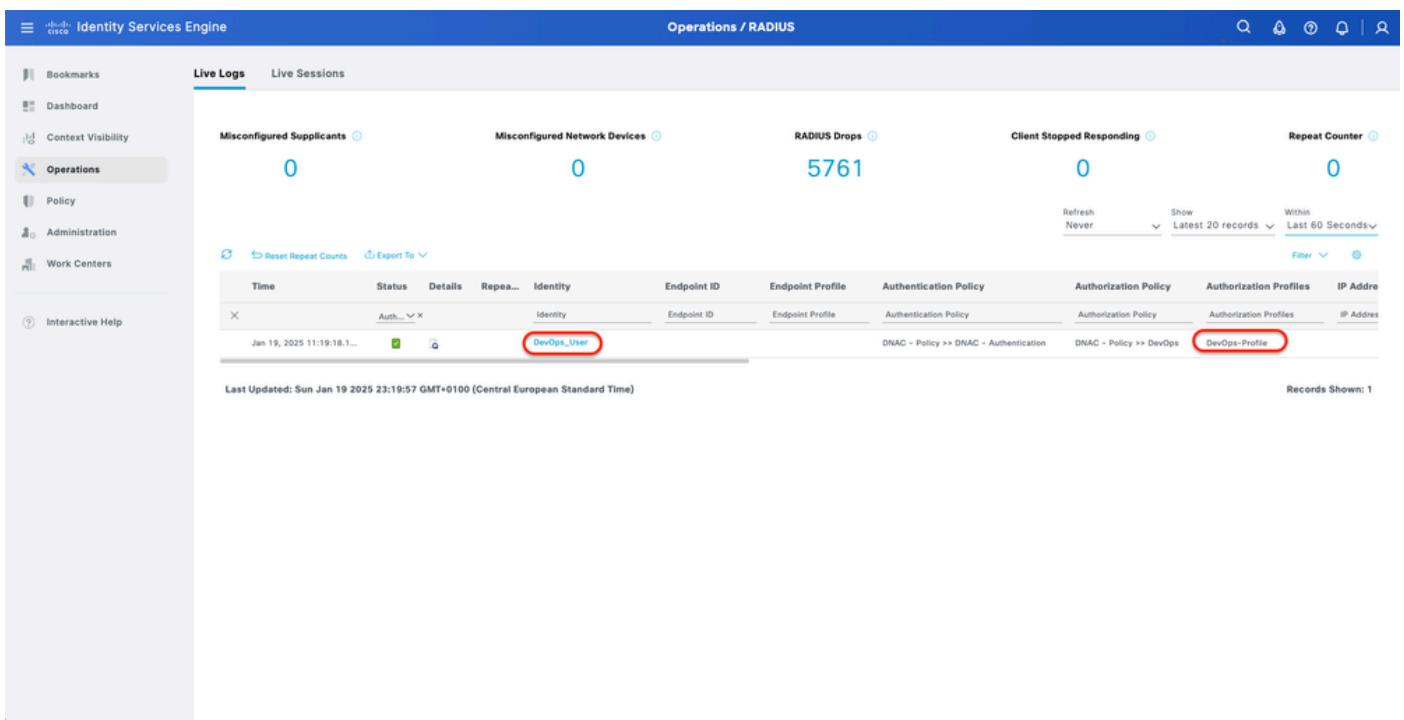
External Users

2. DNAC - Confirm user access



Limited User Access

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



RADIUS Live-Logs

3.b ISE - RADIUS Live-Logs **Operations > RADIUS > Live-Logs > Click (Details) for Authorization log.**

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

RADIUS Detailed Live-Logs 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: 0a301105o95d4kCvV7kMBCoFkesRrFcdXec0uEqPP8RIG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5de4f467

Result

Class: CACS:0a301105o95d4kCvV7kMBCoFkesRrFcdXec0uEqPP8RIG/WY:ise34/528427220/15433

cisco-av-pair ROLE=DevOps-Role

RADIUS Detailed Live-Logs 2-2

Verify TACACS+ Configuration

1- DNAC - Display External Users **System > Users & Roles > External Authentication > External Users**. You can view the list of external users who have logged in through TACACS+ for the first time. The information that is displayed includes their usernames and roles.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

AAA Attribute
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

External Users

2. DNAC - Confirm user access

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

Limited User Access

3.a ISE - TACACS+ Live-Logs Work Centers > Device Administration > Overview > 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#A# Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#A# Device Types#DNAC...	Lo

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

TACACS Live-Logs

3.b ISE - detailed TACACS+ Live-Logs **Work Centers > Device Administration > Overview > TACACS Livelog > Click (Details)** for Authorization log.

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

TACACS+ Detailed Live-Logs 1-2

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; }

TACACS+ Detailed Live-Logs 2-2

References

[Cisco Identity Services Engine Administrator Guide, Release 3.4 > Device Administration](#)

[Cisco DNA Center Administrator Guide, Release 2.3.5](#)

[Cisco DNA Center: Role Based Access Control with External Authentication](#)