将ISE配置为DNAC GUI的外部身份验证

目录

简介

本文档介绍如何将思科身份服务引擎(ISE)配置为思科DNA中心GUI管理的外部身份验证。

先决条件

要求

思科建议您了解以下主题：

- TACACS+和RADIUS协议。
- 思科ISE与思科DNA中心集成。
- 思科ISE策略评估。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)版本3.4补丁1。
- 思科DNA中心版本2.3.5.5。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

- 确保您在System > Settings > External Services > Authentication and Policy Servers上配置了至少一个RADIUS身份验证服务器。
- 只有对DNAC具有超级管理员角色权限的用户才能执行此过程。
- 启用外部身份验证回退。

⚠ 警告：在早于2.1.x的版本中，当启用外部身份验证时，如果AAA服务器无法访问或AAA服务器拒绝未知用户名，则Cisco DNA Center将回退到本地用户。在当前版本中，如果AAA服务器无法访问或AAA服务器拒绝未知用户名，Cisco DNA Center不会回退到本地用户。启用外部身份验证回退后，外部用户和本地管理员可以登录到Cisco DNA Center。

要启用外部身份验证回退，请通过SSH连接到Cisco DNA Center实例并输入此CLI命令(magctl rbac external_auth_fallback enable)。

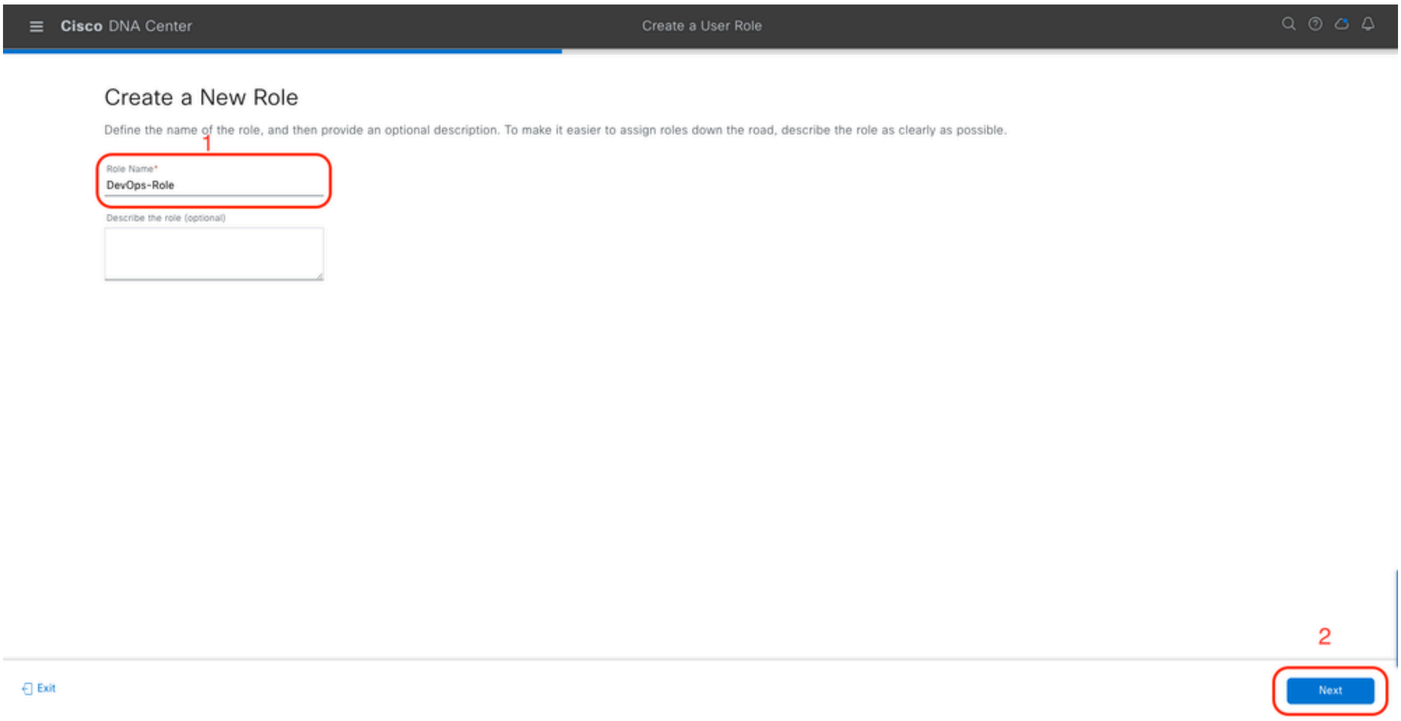
配置

（选项1）使用RADIUS配置DNAC外部身份验证

步骤1.（可选）定义自定义角色。
配置满足要求的自定义角色，您可以使用默认用户角色。这可以通过System > Users & Roles > Role Based Access Control选项卡完成。

步骤

a.创建新角色。



Create a New Role

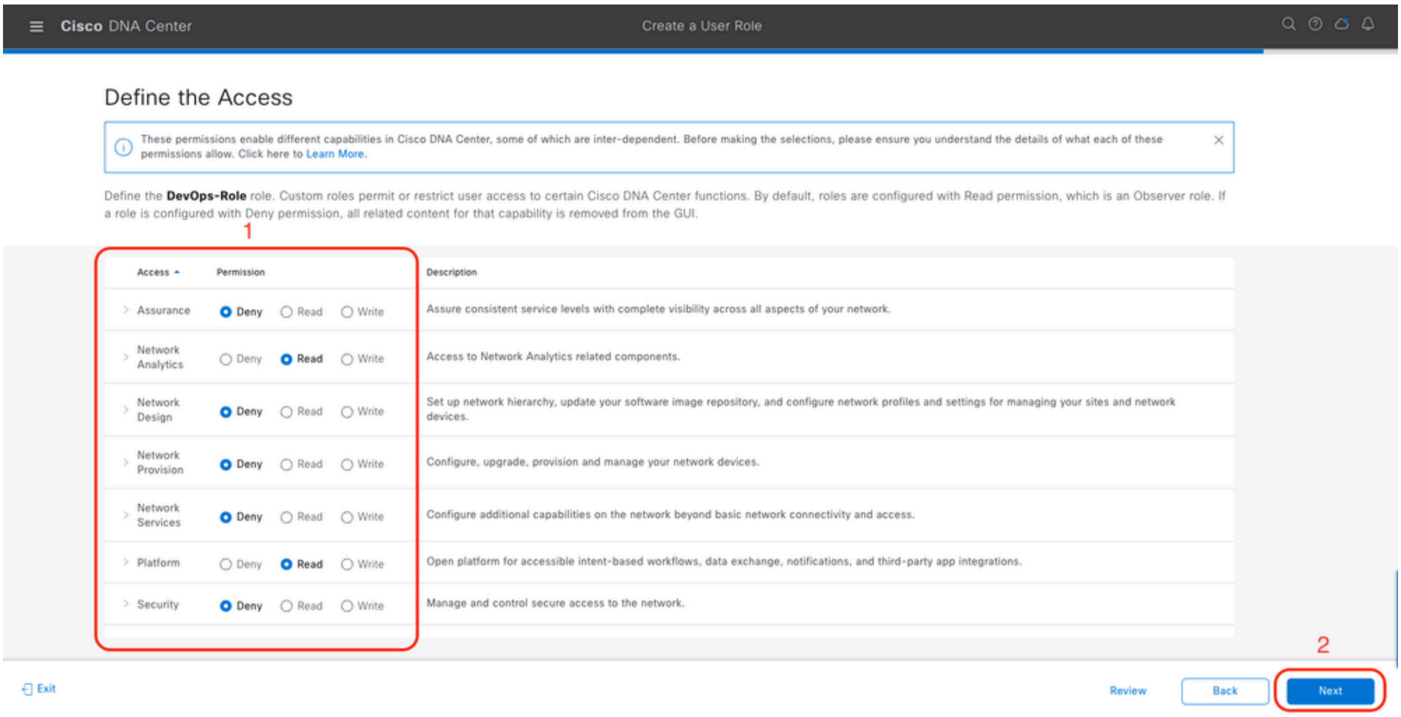
Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name*: DevOps-Role

Describe the role (optional)

DevOps角色名称

b.定义访问。



Define the Access

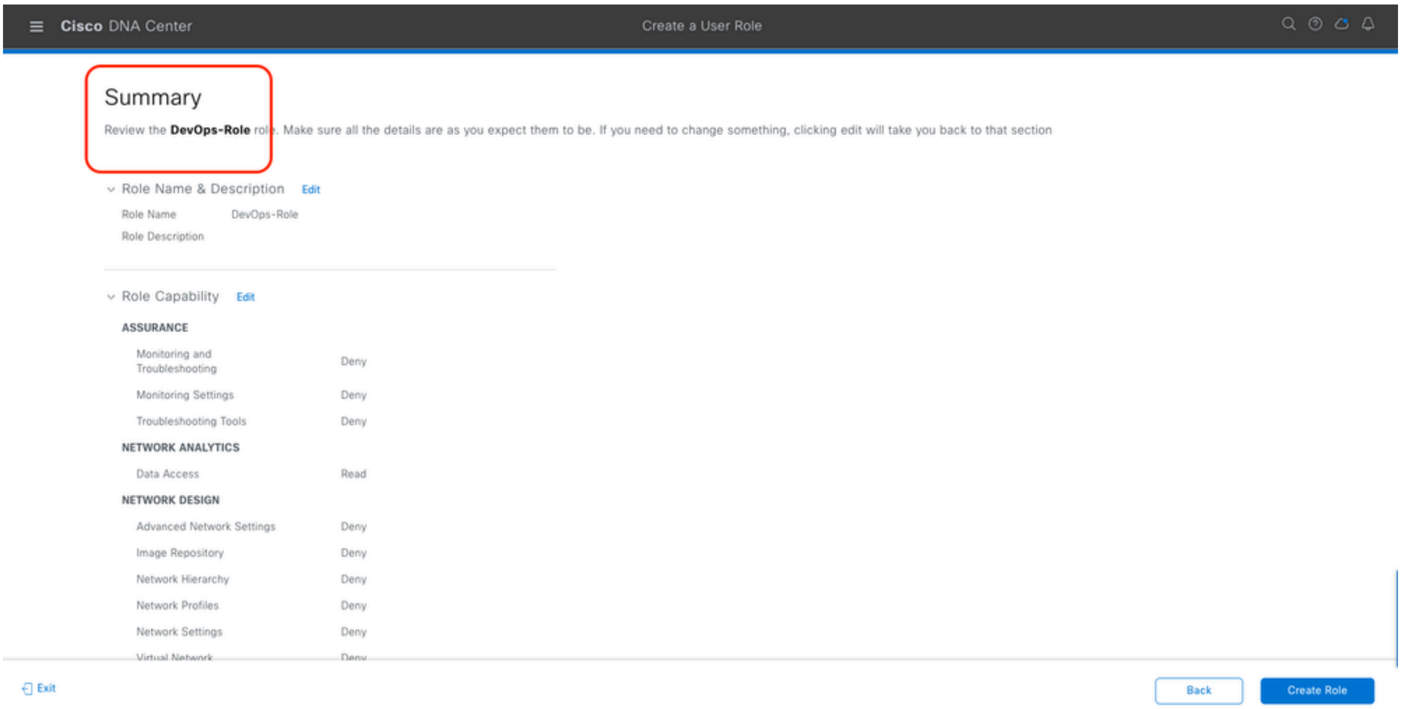
These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to Learn More.

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	● Deny ○ Read ○ Write	Assure consistent service levels with complete visibility across all aspects of your network.
Network Analytics	○ Deny ● Read ○ Write	Access to Network Analytics related components.
Network Design	● Deny ○ Read ○ 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	● Deny ○ Read ○ Write	Configure, upgrade, provision and manage your network devices.
Network Services	● Deny ○ Read ○ Write	Configure additional capabilities on the network beyond basic network connectivity and access.
Platform	○ Deny ● Read ○ Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
Security	● Deny ○ Read ○ Write	Manage and control secure access to the network.

DevOps角色访问

c.创建新角色。



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

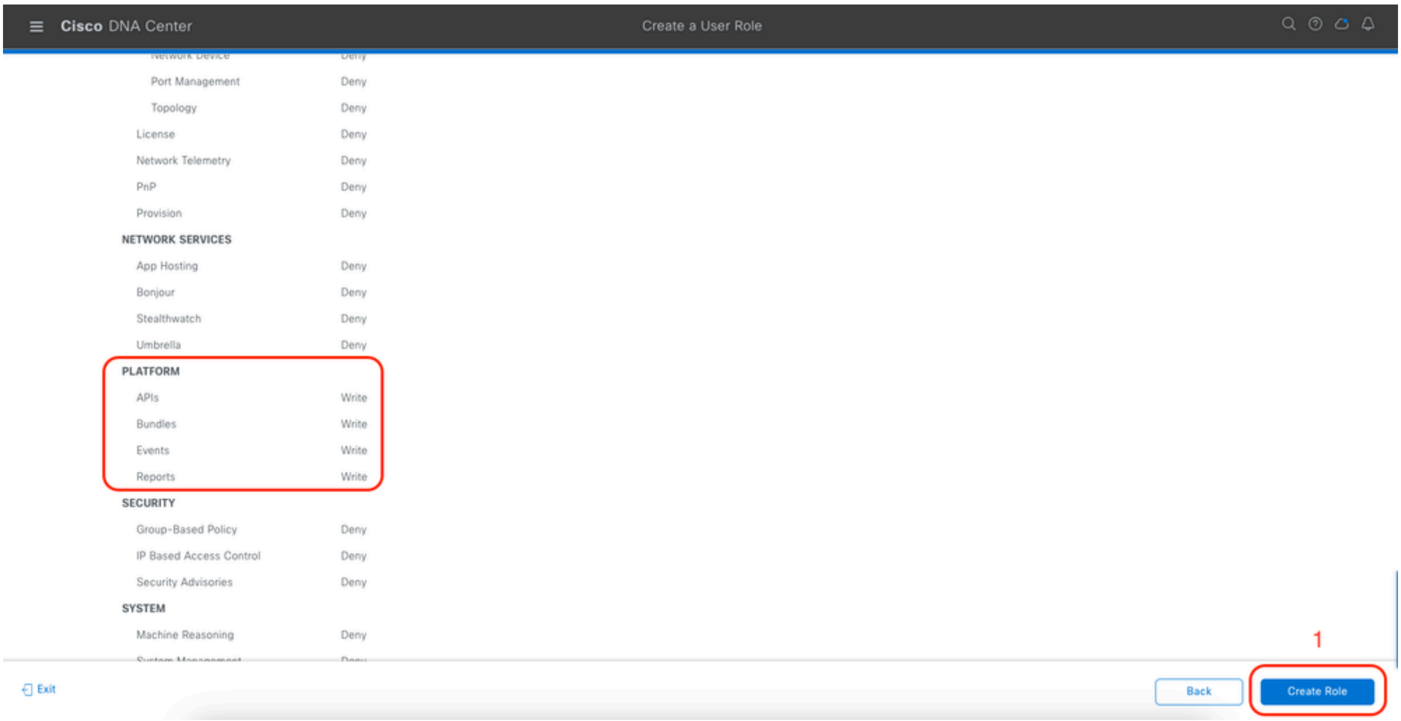
Role Name & Description Edit

Role Name	DevOps-Role
Role Description	

Role Capability Edit

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

DevOps角色摘要



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

审核并创建DevOps角色

步骤2.使用RADIUS配置外部身份验证。
这可以通过System > Users & Roles > External Authentication选项卡完成。

步骤

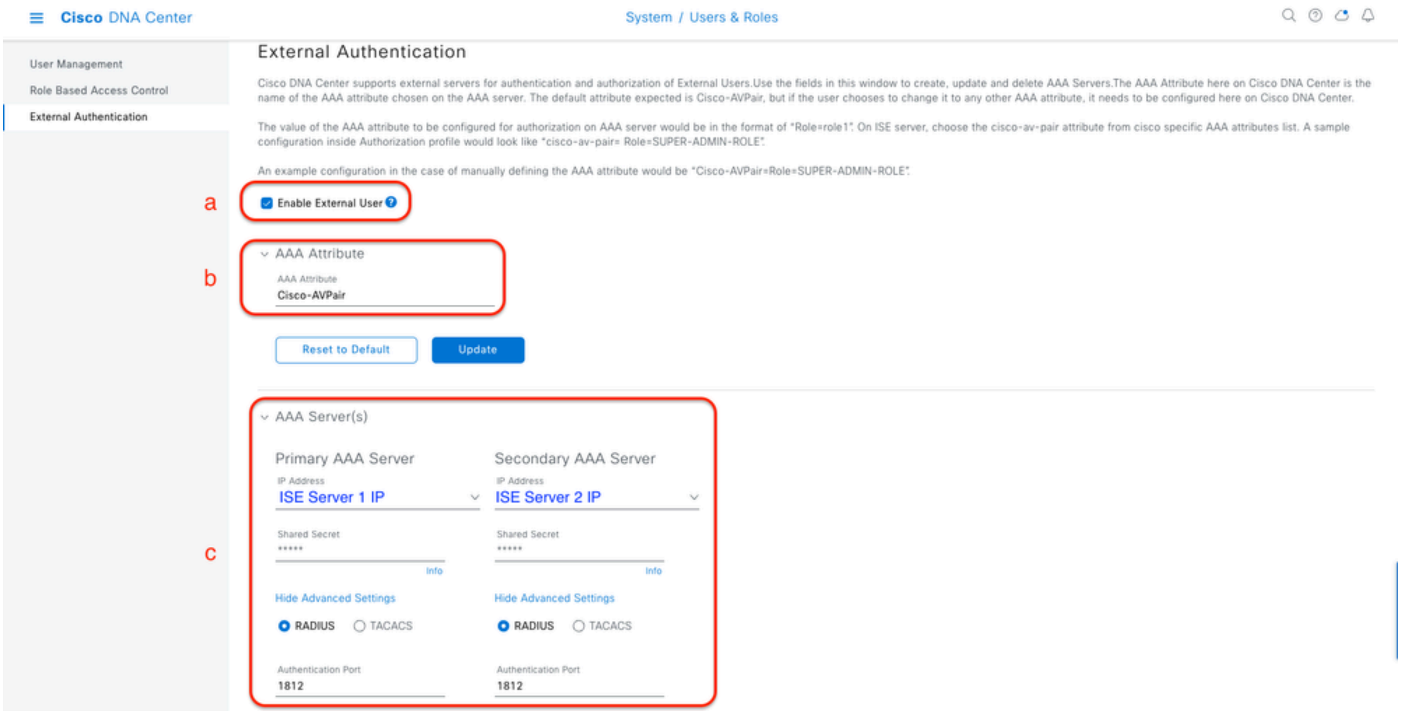
a.要在Cisco DNA Center中启用外部身份验证，请选中启用外部用户复选框。

b.设置AAA属性。

在AAA attributes字段中输入Cisco-AVPair。

c.（ 可选 ）配置主要和辅助AAA服务器。

确保主AAA服务器上或主服务器和辅助服务器上都启用了RADIUS协议。



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

AAA Server(s)

Primary AAA Server
IP Address: ISE Server 1 IP
Shared Secret: *****
● RADIUS ○ TACACS
Authentication Port: 1812

Secondary AAA Server
IP Address: ISE Server 2 IP
Shared Secret: *****
● RADIUS ○ TACACS
Authentication Port: 1812

(RADIUS)外部身份验证配置步骤

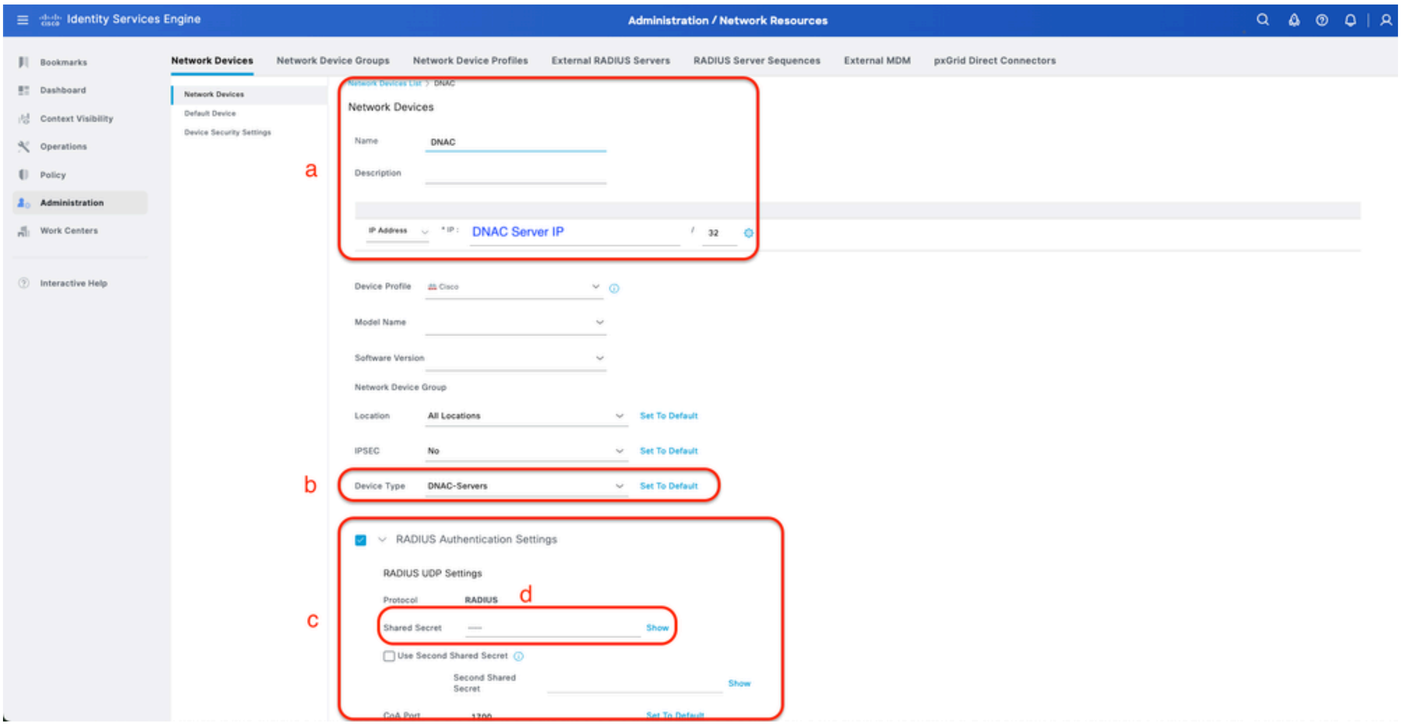
（选项1）为RADIUS配置ISE

步骤1.将DNAC服务器添加为ISE上的网络设备。

这可以通过管理>网络资源>网络设备选项卡完成。

步骤

a.定义(DNAC)网络设备名称和IP。
b.（可选）为策略集条件对设备类型进行分类。
c.启用RADIUS身份验证设置。
d.设置RADIUS共享密钥。



Network Devices

Name: DNAC

Description:

IP Address * IP : DNAC Server IP / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: DNAC-Servers — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ---- Show

□ Use Second Shared Secret

Second Shared Secret: Show

CoA Port: 1700 — Set To Default

用于RADIUS的ISE网络设备(DNAC)

步骤2.创建RADIUS授权配置文件。

这可以通过选项卡完成 Policy > Policy Elements > Results > Authorization > 授权配置文件。

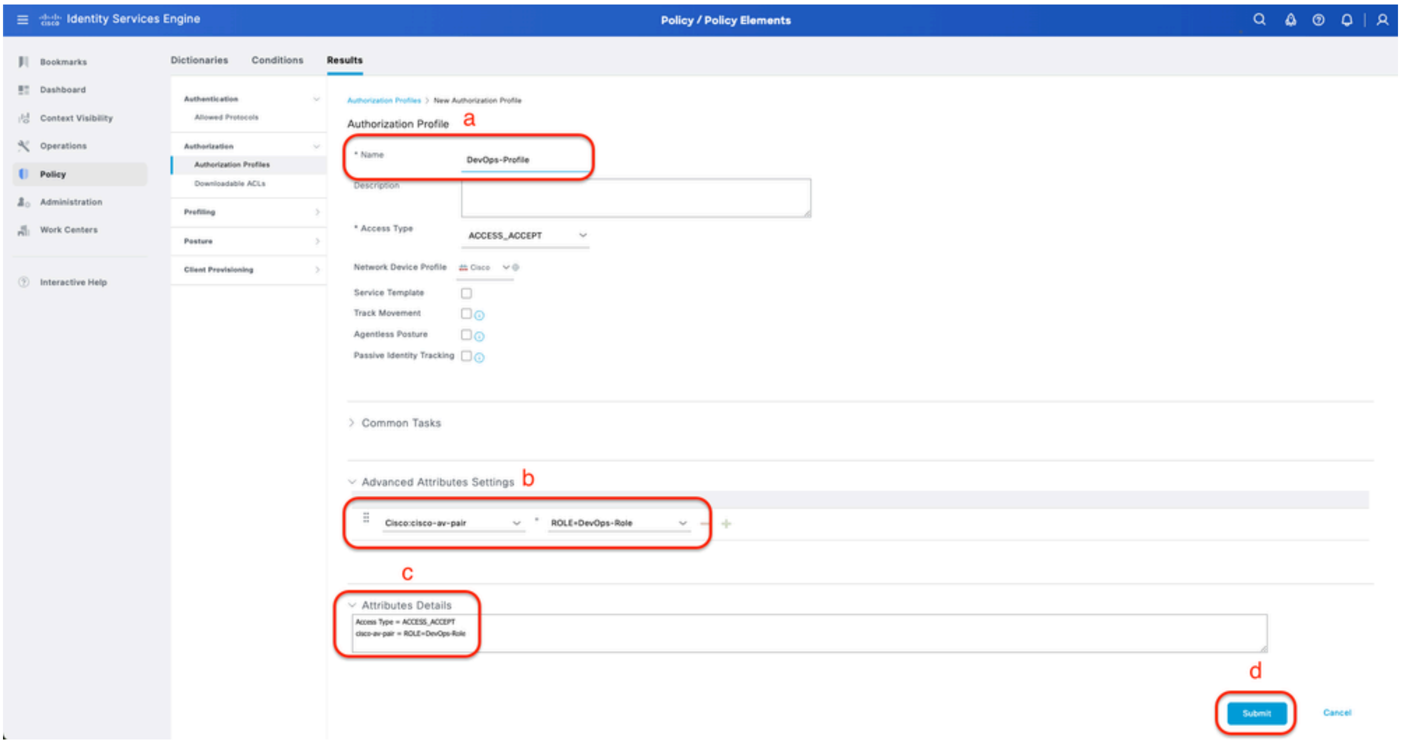
注意：创建3个RADIUS授权配置文件，每个用户角色一个。

步骤
a.单击Add并定义RADIUS授权配置文件名称。

b.在Advanced Attributes Settings中输入Cisco:cisco-av-pair，并填充正确的User角色。

- 对于(DecOps-Role)用户角色，请输入ROLE=DevOps-Role。
- 对于(NETWORK-ADMIN-ROLE)用户角色，请输入ROLE=NETWORK-ADMIN-ROLE。
- 对于(SUPER-ADMIN-ROLE)用户角色，请输入ROLE=SUPER-ADMIN-ROLE。

c.查看属性详细信息。
d.Click Save.



Authorization Profile

* Name DevOps-Profile

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Advanced Attributes Settings

Cisco:cisco-av-pair = ROLE=DevOps-Role

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = ROLE=DevOps-Role

创建授权配置文件

步骤3.创建用户组。

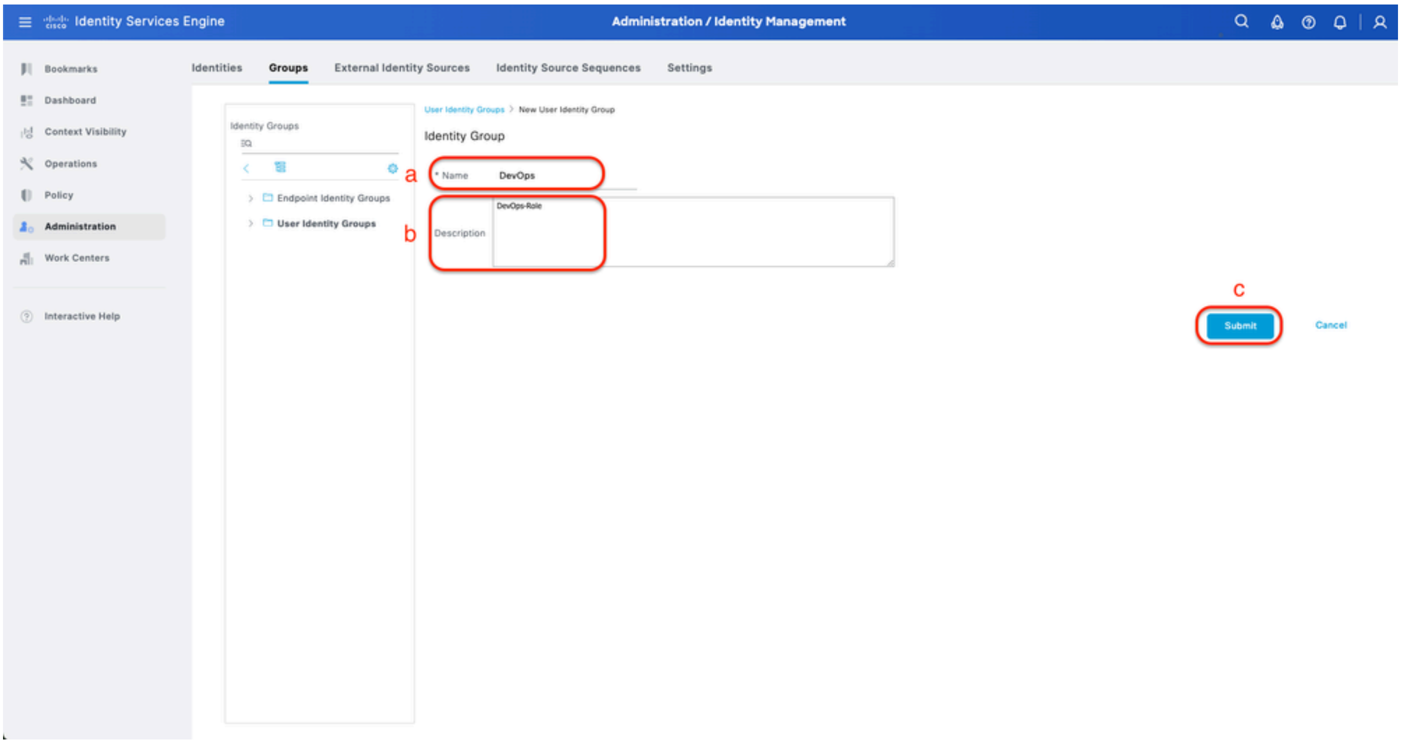
这可以通过Administration > Identity Management > Groups > User Identity Groups选项卡完成。

步骤

a.单击Add并定义身份组名称

b.（可选）定义说明。

c.单击Submit。



* Name: DevOps

Description: DevOps-Role

创建用户身份组

步骤4.创建本地用户。

这可以通过管理>身份管理>身份>用户选项卡完成。

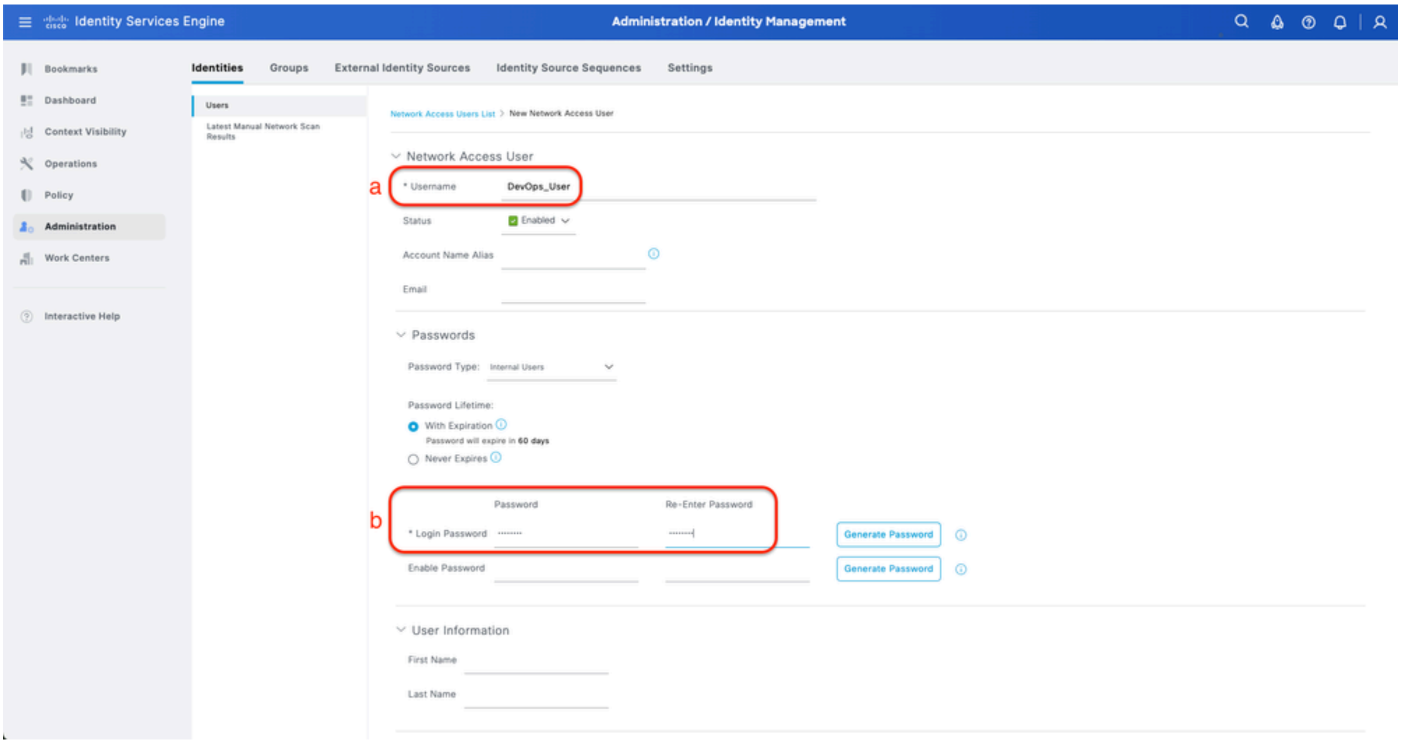
步骤

a.单击Add并定义用户名。

b.设置登录密码。

c.将用户添加到相关用户组。

d.单击 submit。



Network Access User

- * Username: DevOps_User
- Status: ☑ Enabled
- Account Name Alias:
- Email:

Passwords

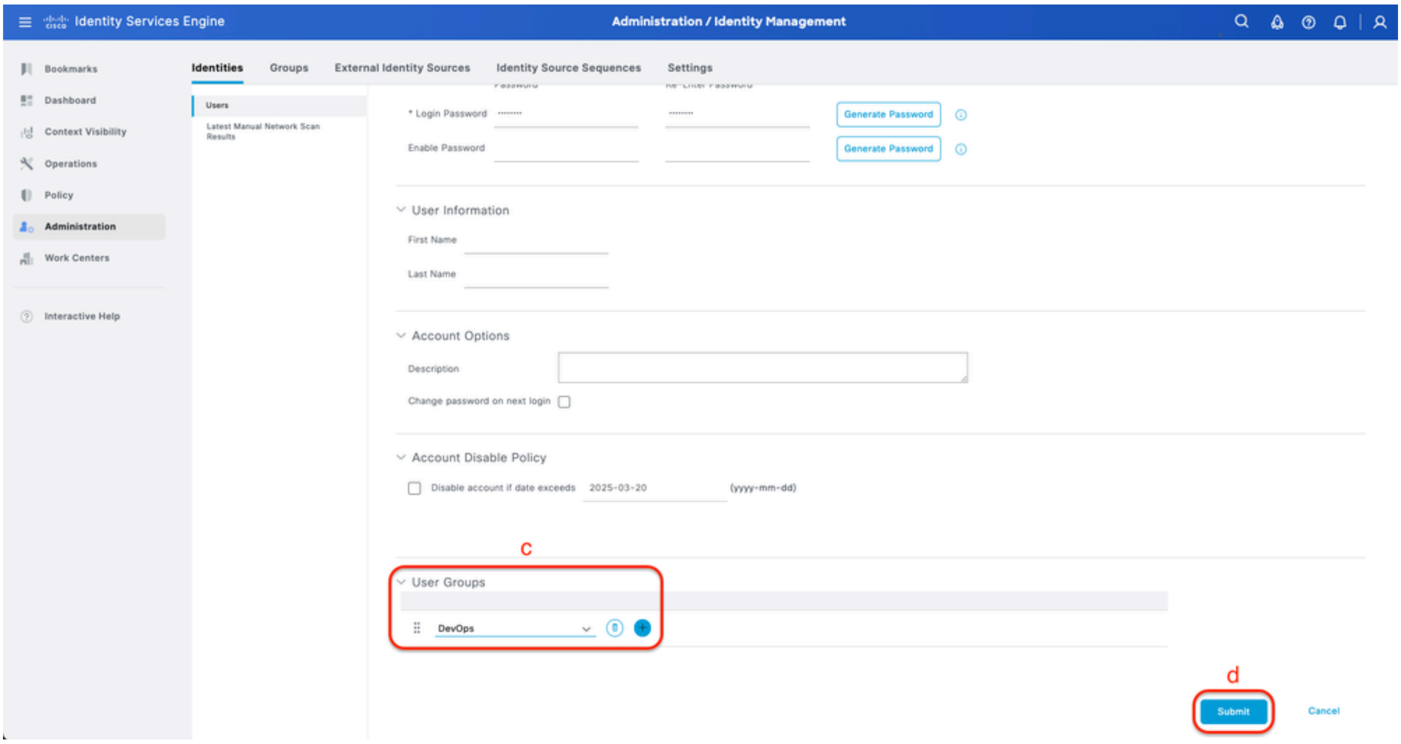
- Password Type: Internal Users
- Password Lifetime:
  - ● With Expiration
    Password will expire in 60 days
  - ○ Never Expires

	Password	Re-Enter Password
* Login Password	········	········
Enable Password		

User Information

- First Name:
- Last Name:

创建本地用户1-2



	Password	Re-Enter Password
* Login Password	········	········
Enable 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)

User Groups

- DevOps

创建本地用户2-2

步骤5.（可选）添加RADIUS策略集。

这可以在Policy > Policy Sets选项卡中完成。

步骤

a.单击Actions并选择(上面插入新行)。

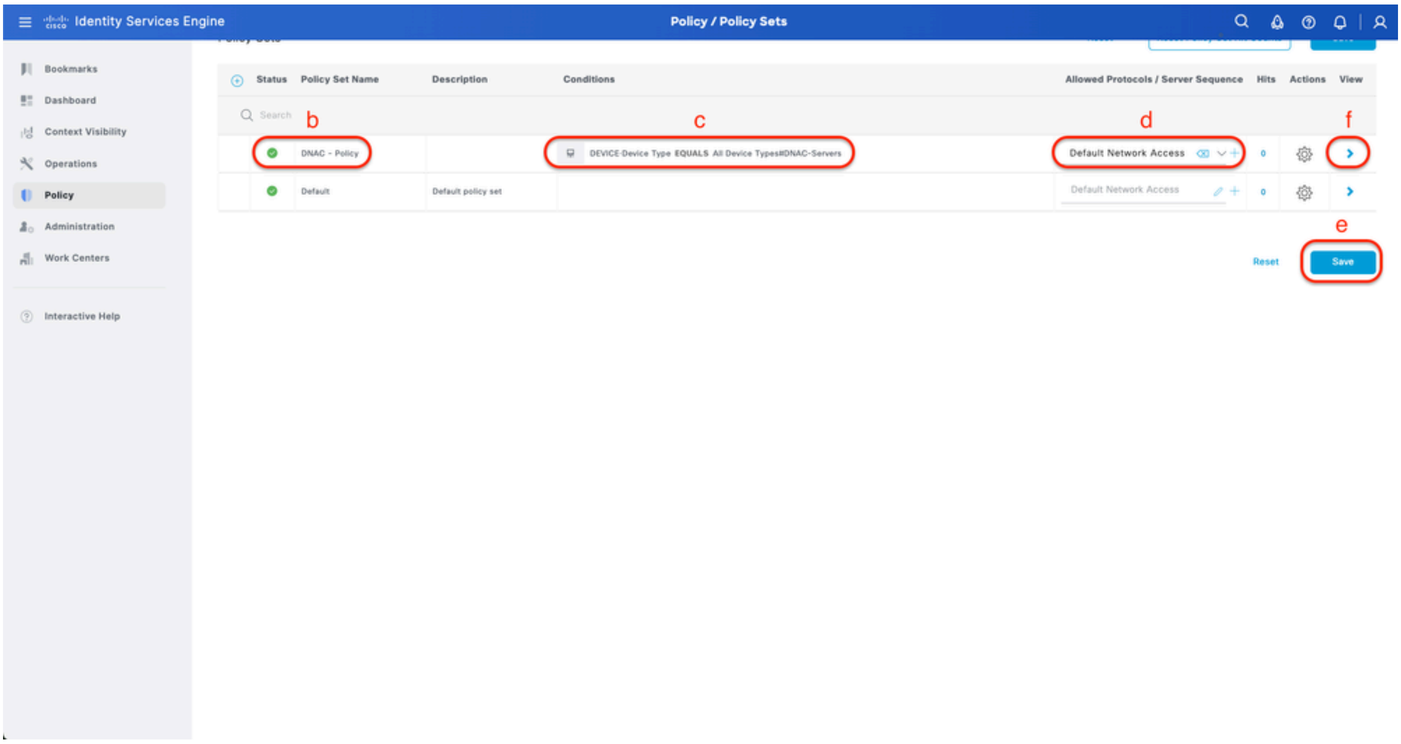
b.定义策略集名称。

c.将Policy Set Condition设置为Select Device Type you previous created on(Step1 > b)。

d.设置Allowed协议。

e.Click Save.

f.点击(>)Policy Set View配置身份验证和授权规则。



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	⚙	>

添加RADIUS策略集

步骤6.配置RADIUS身份验证策略。

这可以通过Policy > Policy Sets >单击(>)选项卡完成。

步骤

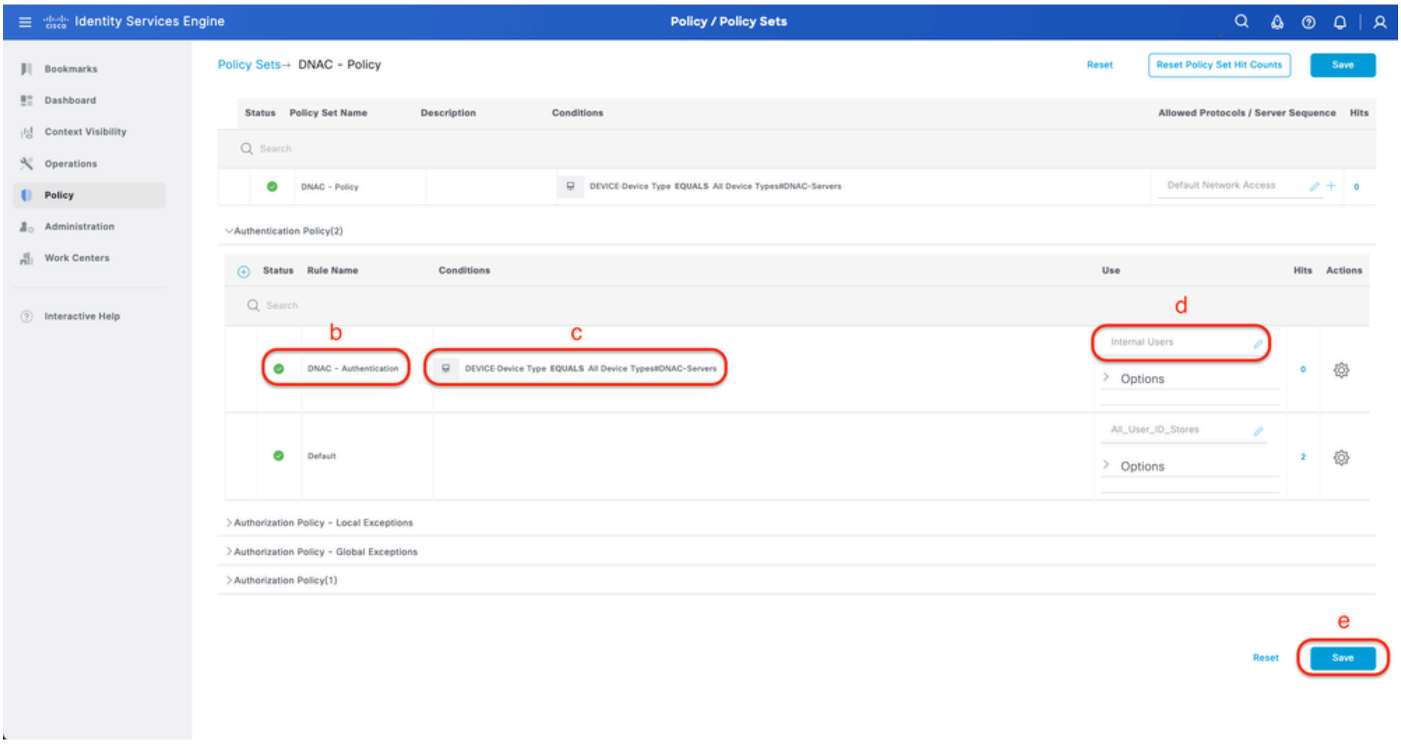
a.单击Actions并选择(上面插入新行)。

b.定义身份验证策略名称。

c.设置先前在上创建的Authentication Policy Condition和Select Device Type（步骤1 > b）。

d.为身份源设置Authentication Policy Use。

e.Click Save.



添加RADIUS身份验证策略

步骤7.配置RADIUS授权策略。

这可以通过Policy > Policy Sets>Click(>)选项卡完成。

此步骤用于为每个用户角色创建授权策略：

- 超级管理员角色
- NETWORK-ADMIN-ROLE
- DevOps — 角色

步骤

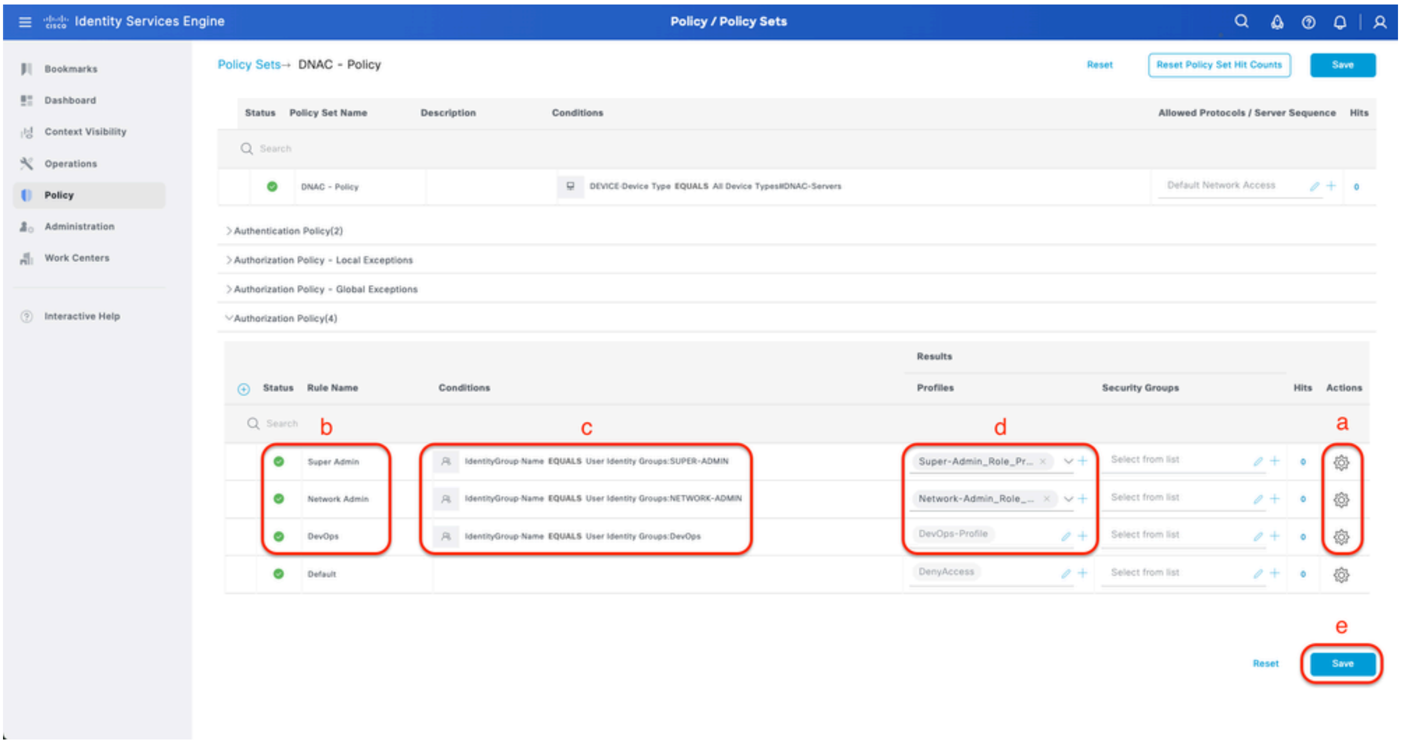
a.单击Actions并选择(上面插入新行)。

b.定义授权策略名称。

c.设置授权策略条件并选择您在中创建的用户组（第3步）。

d.设置授权策略结果/配置文件和选择您在中创建的授权配置文件(Step2)。

e.Click Save.



Policy Sets→ DNAC - Policy

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

> Authentication Policy(2)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy(4)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	Super Admin	IdentityGroup·Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr...	Select from list	0	⚙
●	Network Admin	IdentityGroup·Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role_...	Select from list	0	⚙
●	DevOps	IdentityGroup·Name EQUALS User Identity Groups:DevOps	DevOps-Profile	Select from list	0	⚙
●	Default		DenyAccess	Select from list	0	⚙

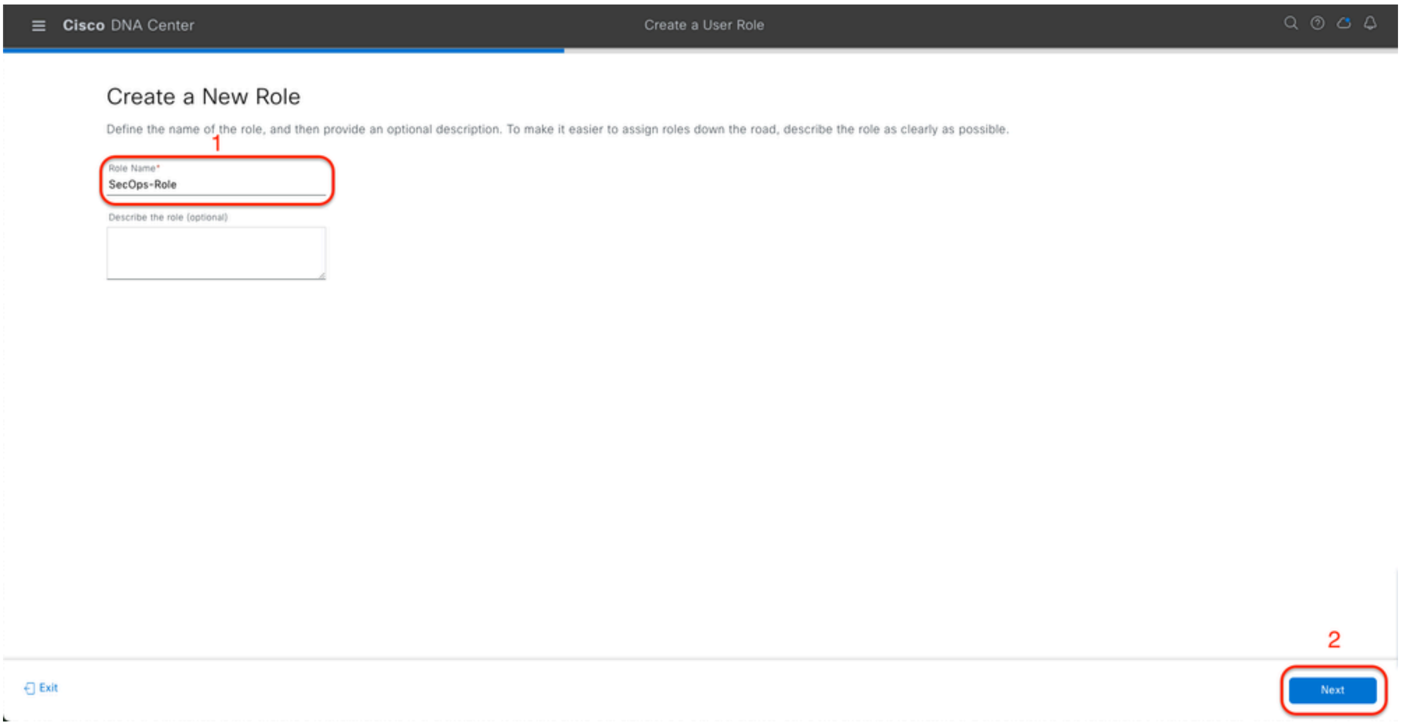
添加授权策略

（选项2）使用TACACS+配置DNAC外部身份验证

步骤1.（可选）定义自定义角色。
配置满足要求的自定义角色，您可以使用默认用户角色。这可以通过System > Users & Roles > Role Based Access Control选项卡完成。

步骤

a.创建新角色。



Create a New Role

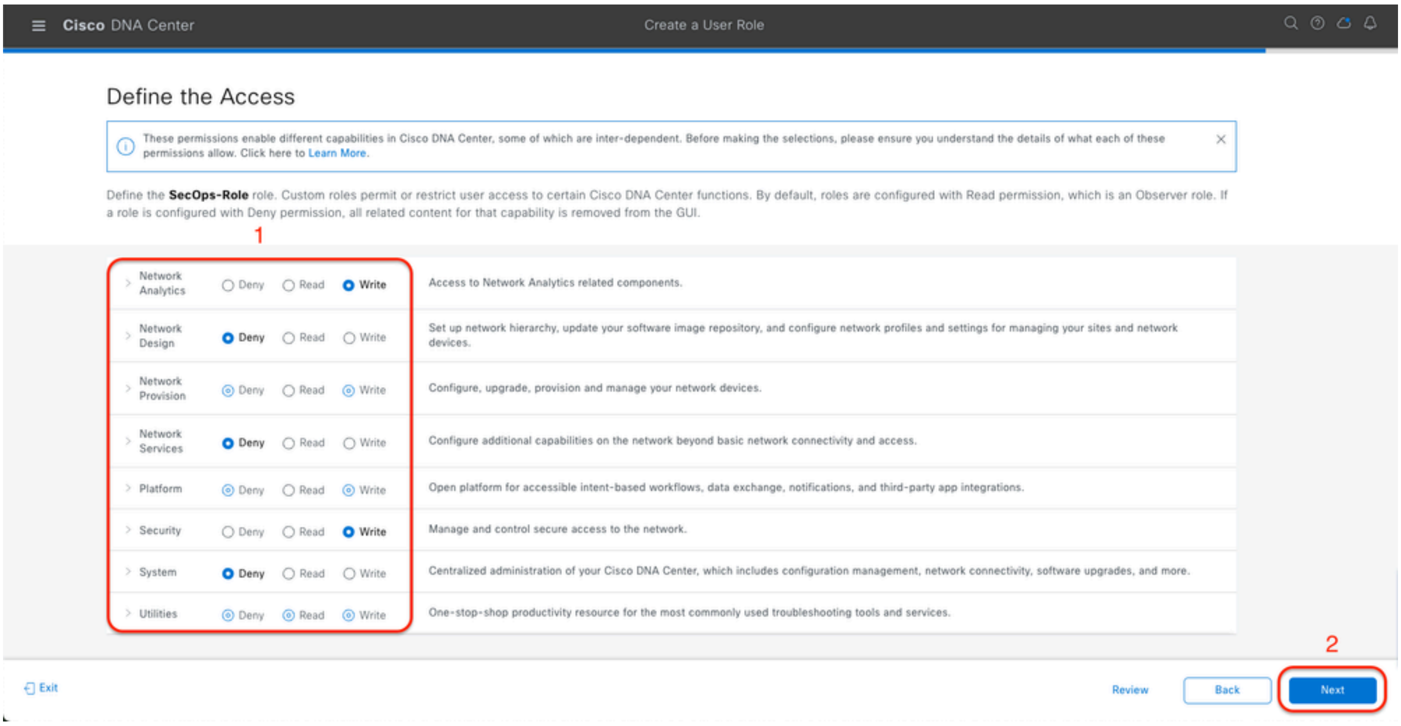
Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name*
SecOps-Role

Describe the role (optional)

SecOps角色名称

b.定义访问。



Define the Access

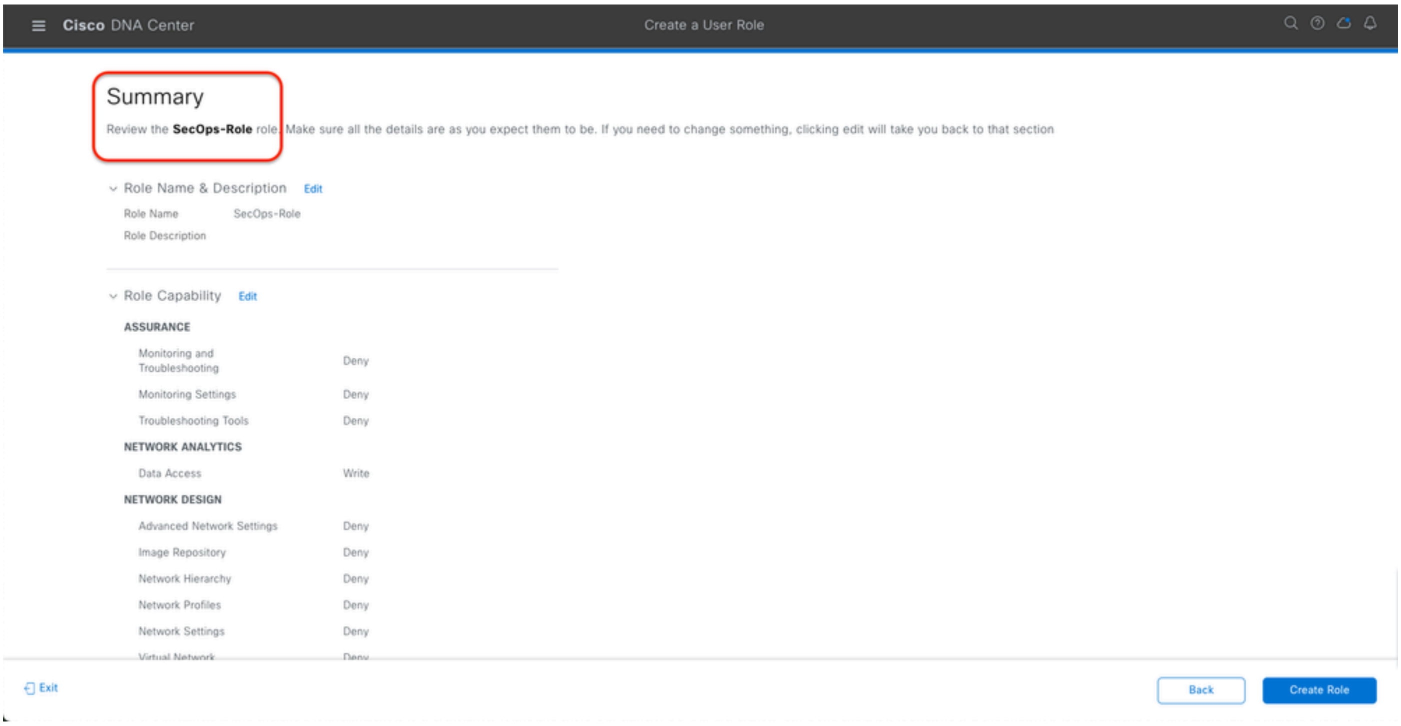
ⓘ These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to Learn More. ✕

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.

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

SecOps角色访问

c.创建新角色。



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

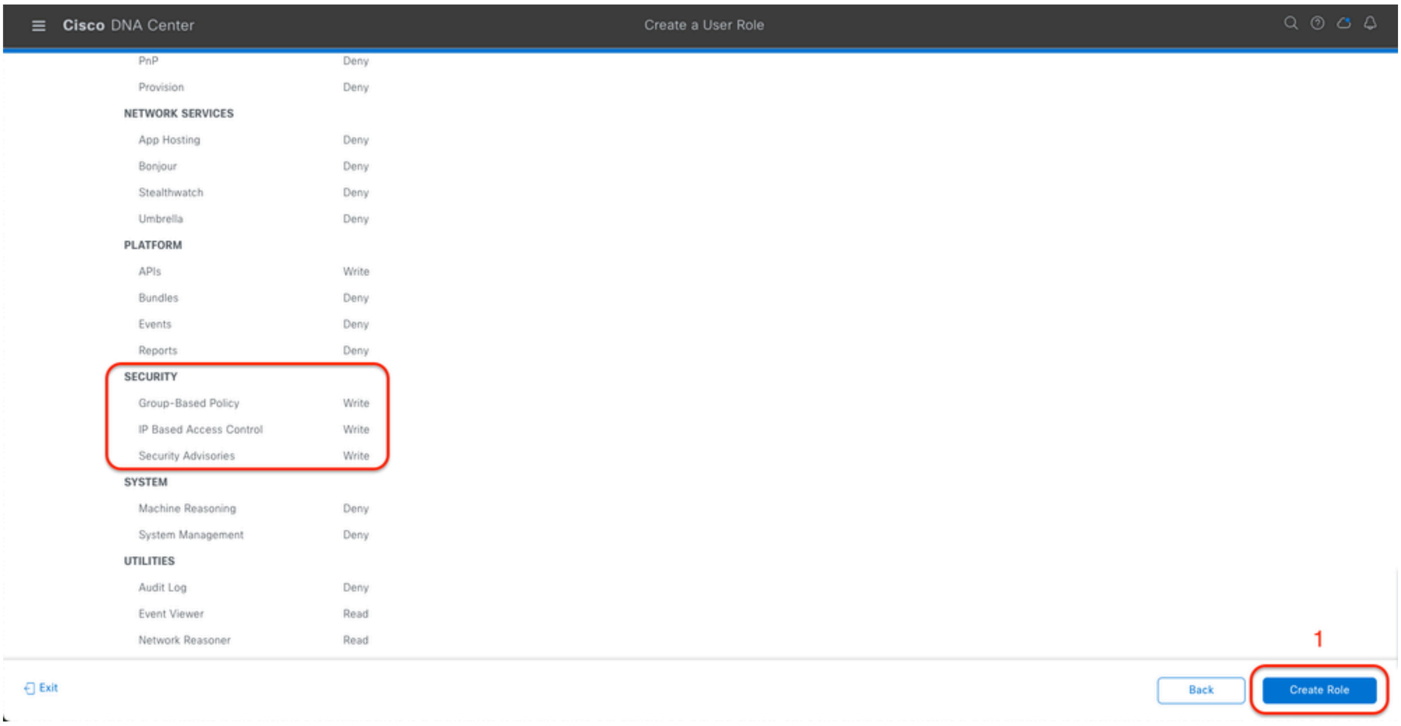
⌄ Role Name & Description Edit

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

SecOps角色摘要



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

审核并创建SecOps角色

步骤2.使用TACACS+配置外部身份验证。
这可以通过System > Users & Roles > External Authentication选项卡完成。

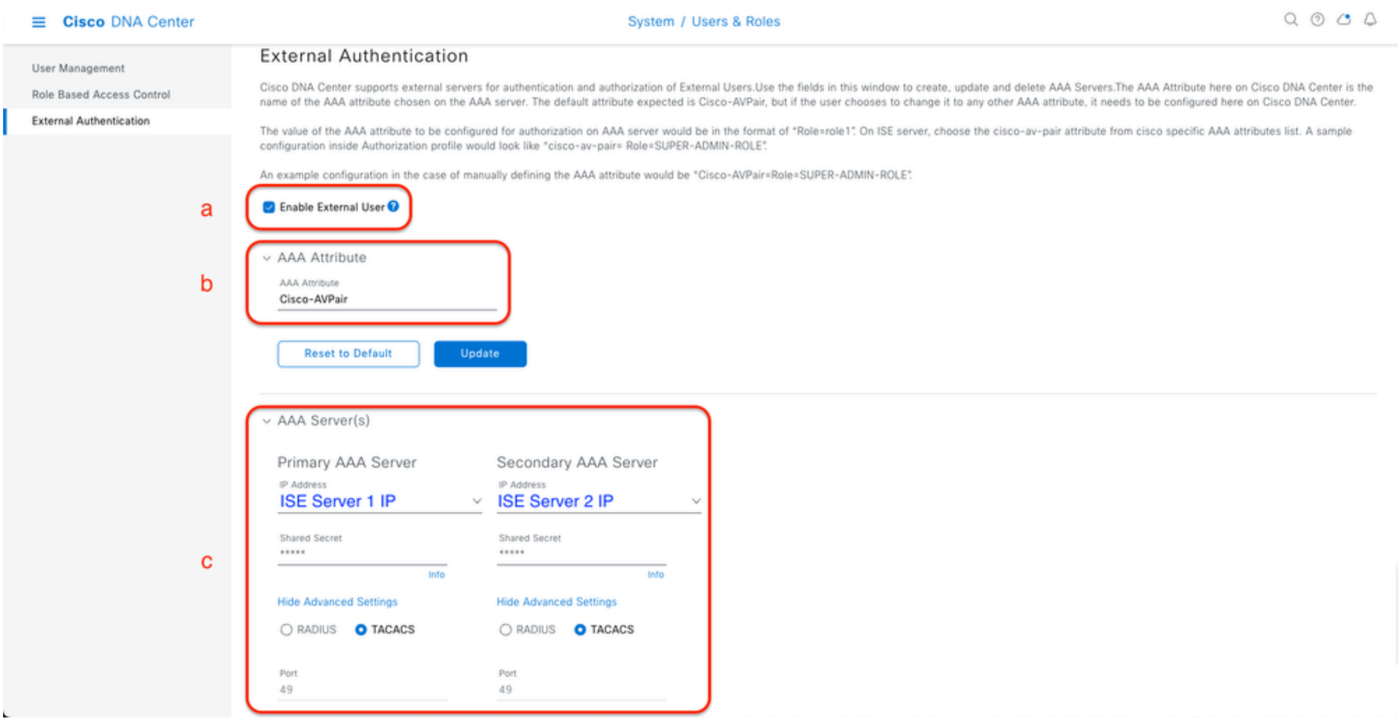
a.要在Cisco DNA Center中启用外部身份验证，请选中启用外部用户复选框。

b.设置AAA属性。

在AAA attributes字段中输入Cisco-AVPair。

c.（可选）配置主要和辅助AAA服务器。

确保主AAA服务器上或主服务器和辅助服务器上都启用了TACACS+。



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

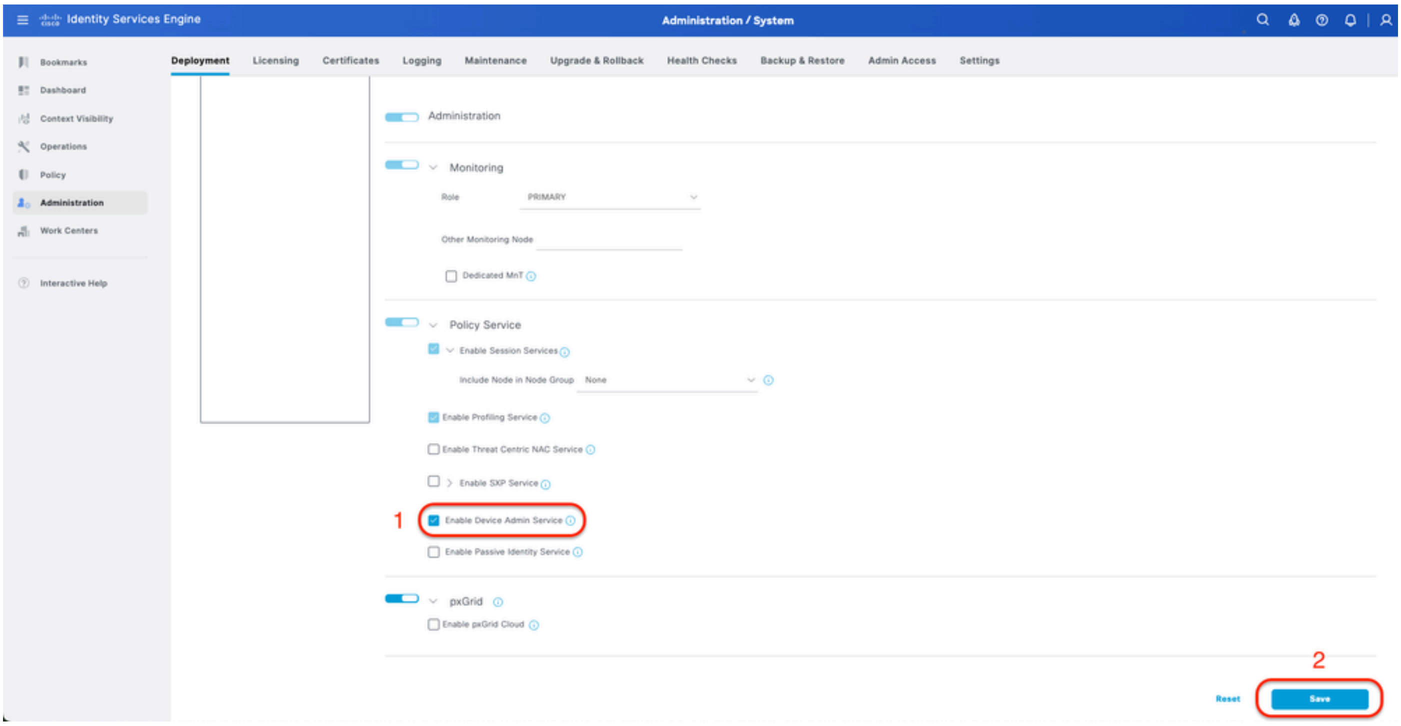
AAA Server(s)

Primary AAA Server	Secondary AAA Server
IP Address: ISE Server 1 IP	IP Address: ISE Server 2 IP
Shared Secret: *****	Shared Secret: *****
Hide Advanced Settings	Hide Advanced Settings
○ RADIUS ● TACACS	○ RADIUS ● TACACS
Port: 49	Port: 49

(TACACS+)外部身份验证配置步骤

（选项2）为TACACS+配置ISE

步骤1.启用设备管理服务。
这可以通过Administration > System > Deployment > Edit(ISE PSN Node)> Check Enable Device Admin Service选项卡完成。



Administration

Monitoring
Role: PRIMARY
Other Monitoring Node
□ Dedicated MnT

Policy Service
☑ Enable Session Services
Include Node in Node Group: None
☑ Enable Profiling Service
□ Enable Threat Centric NAC Service
□ Enable SXP Service
☑ Enable Device Admin Service
□ Enable Passive Identity Service

pxGrid
□ Enable pxGrid Cloud

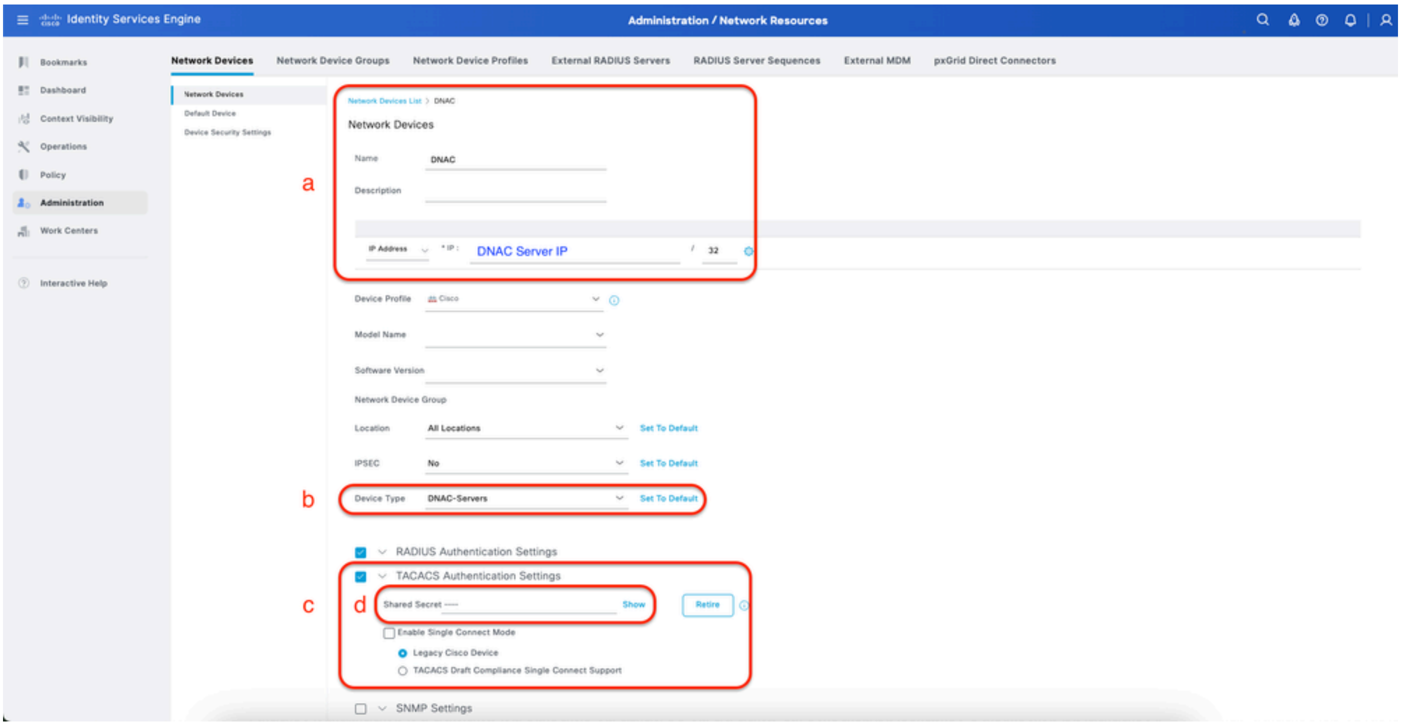
启用设备管理服务

步骤2.将DNAC服务器添加为ISE上的网络设备。

这可以通过管理>网络资源>网络设备选项卡完成。

步骤

a.定义(DNAC)网络设备名称和IP。
b.（可选）为策略集条件对设备类型进行分类。
c.启用TACACS+身份验证设置。
d.设置TACACS+共享密钥。



Network Devices

Name: DNAC

Description:

IP Address * IP : DNAC Server IP / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

IPSEC: No

Device Type: DNAC-Servers

☑ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret -----

□ Enable Single Connect Mode

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

□ SNMP Settings

用于TACACS+的ISE网络设备(DNAC)

步骤3.为每个DNAC角色创建TACACS+配置文件。

这可以从工作中心>设备管理>策略元素>结果> TACACS配置文件选项卡完成。

注意：创建3个TACACS+配置文件，每个用户角色一个。

步骤

a.单击Add并定义TACACS Profile名称。

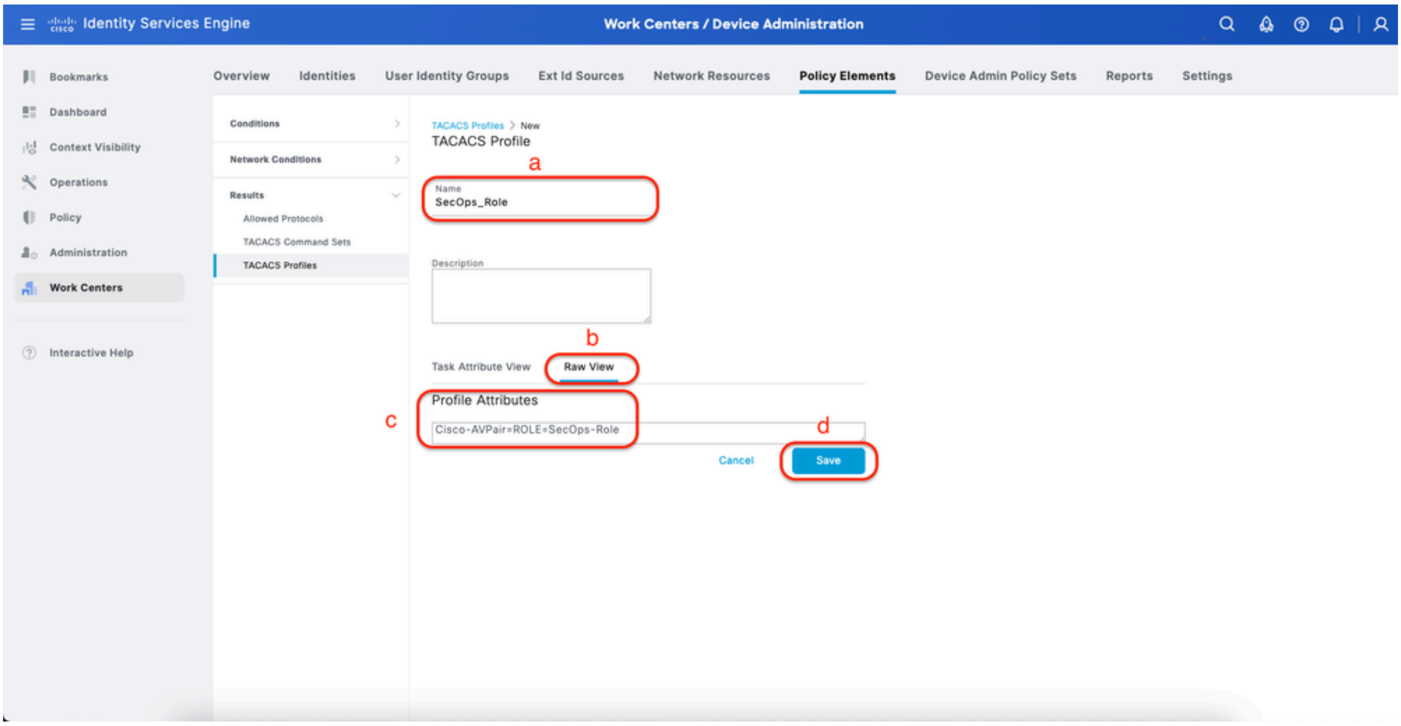
b.单击Raw View选项卡。

c.输入Cisco-AVPair=ROLE=并填写正确的用户角色。

- 对于(SecOps-Role)用户角色，请输入Cisco-AVPair=ROLE=SecOps-Role。
- 对于(NETWORK-ADMIN-ROLE)用户角色，请输入Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE。
- 对于(SUPER-ADMIN-ROLE)用户角色，请输入Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE。

注意：请记住，AVPair值(Cisco-AVPair=ROLE=)区分大小写，并确保其与DNAC用户角色匹配。

d.Click Save.



TACACS Profile

Name
SecOps_Role

Description

Profile Attributes
Cisco-AVPair=ROLE=SecOps-Role

创建TACACS配置文件(SecOps_Role)

步骤4.创建用户组。

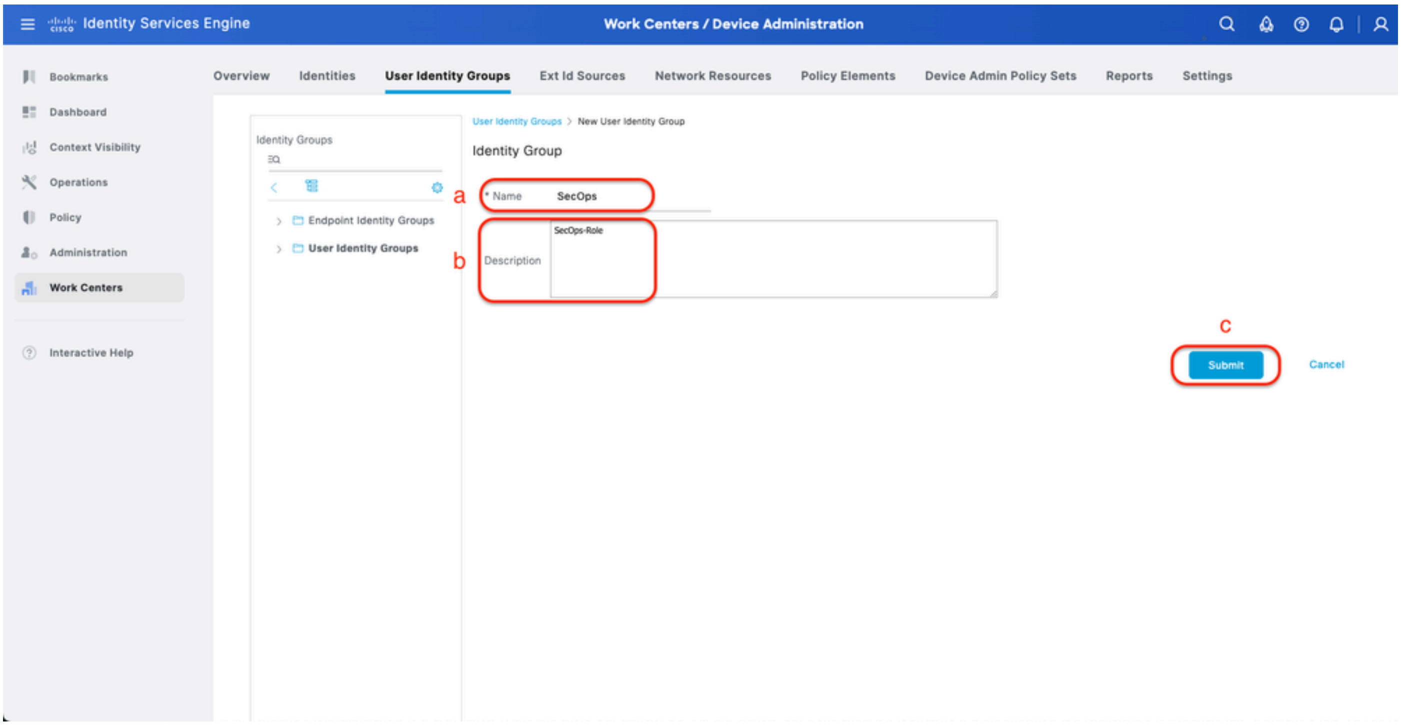
这可以通过工作中心>设备管理>用户身份组选项卡完成。

步骤

a.单击Add并定义身份组名称。

b.（可选）定义说明。

c.单击Submit。



* Name SecOps

Description SecOps-Role

创建用户身份组

步骤5.创建本地用户。

这可以通过工作中心>设备管理>身份>用户选项卡完成。

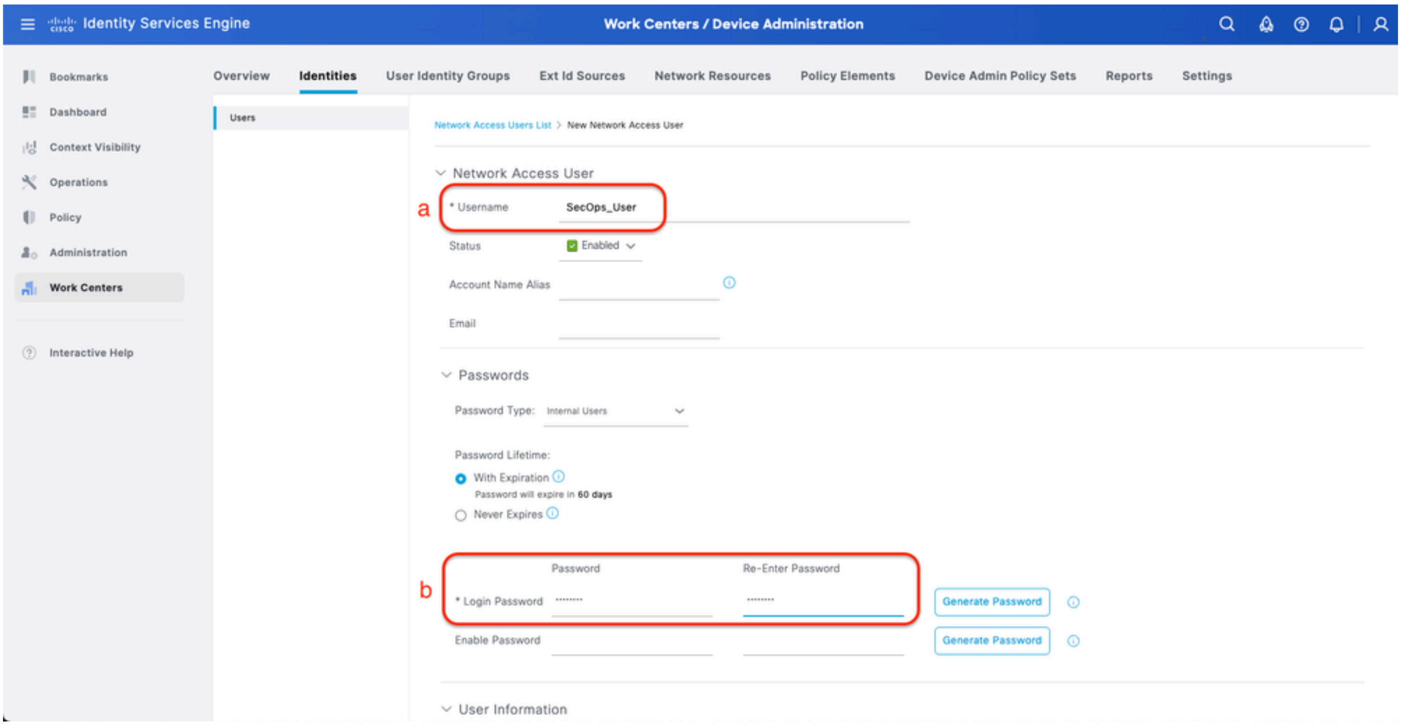
步骤

a.单击Add并定义用户名。

b.设置登录密码。

c.将用户添加到相关用户组。

d.单击 submit。



Network Access Users List > New Network Access User

Network Access User

* Username SecOps_User

Status ☑ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

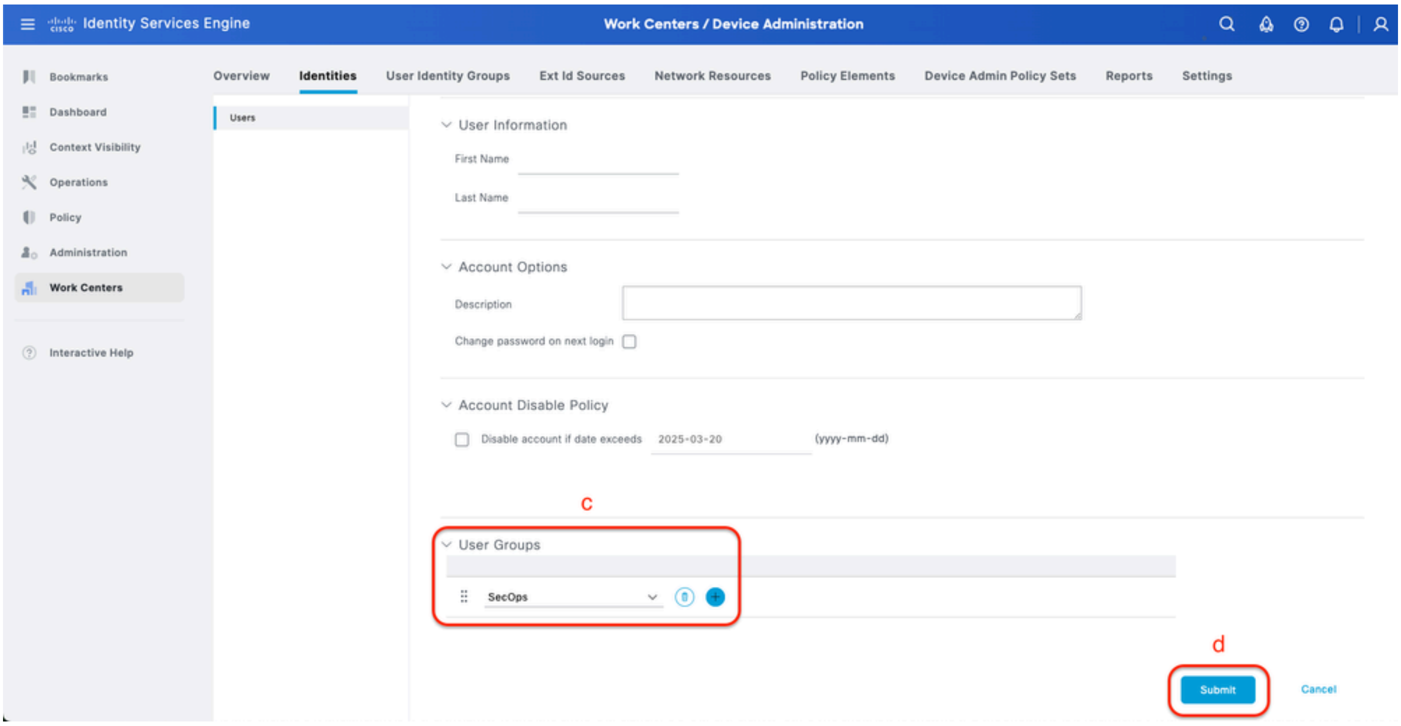
● With Expiration
Password will expire in 60 days

○ Never Expires

	Password	Re-Enter Password
* Login Password	········	········
Enable Password		

User Information

创建本地用户1-2



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)

User Groups

SecOps

创建本地用户2-2

步骤6.（可选）添加TACACS+策略集。

这可以通过工作中心>设备管理>设备管理策略集选项卡完成。

步骤

a.单击Actions并选择(上面插入新行)。

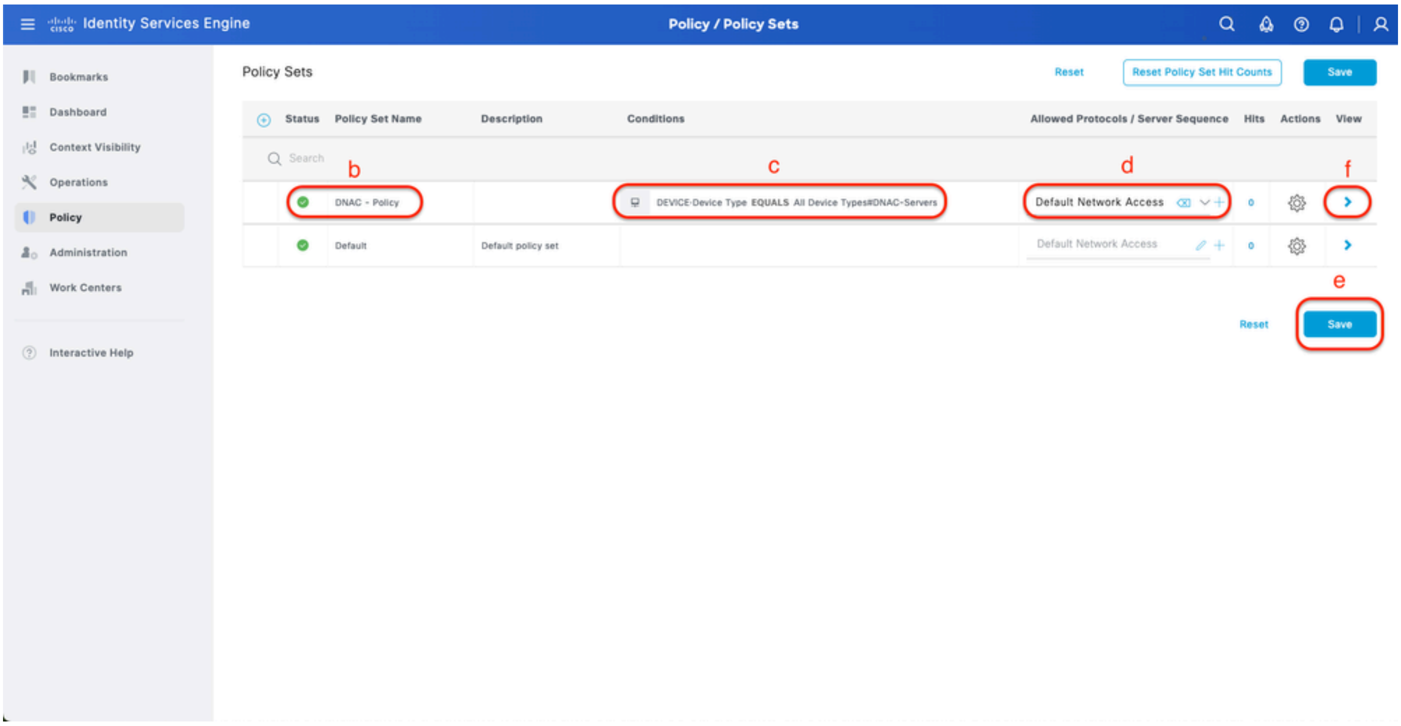
b.定义策略集名称。

c.将Policy Set Condition设置为Select Device Type you previous created on(Step2 > b)。

d.设置Allowed协议。

e.Click Save.

f.点击(>)Policy Set View配置身份验证和授权规则。



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	⚙	>

添加TACACS+策略集

步骤7.配置TACACS+身份验证策略。

这可以从工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)>点击(>)完成。

步骤

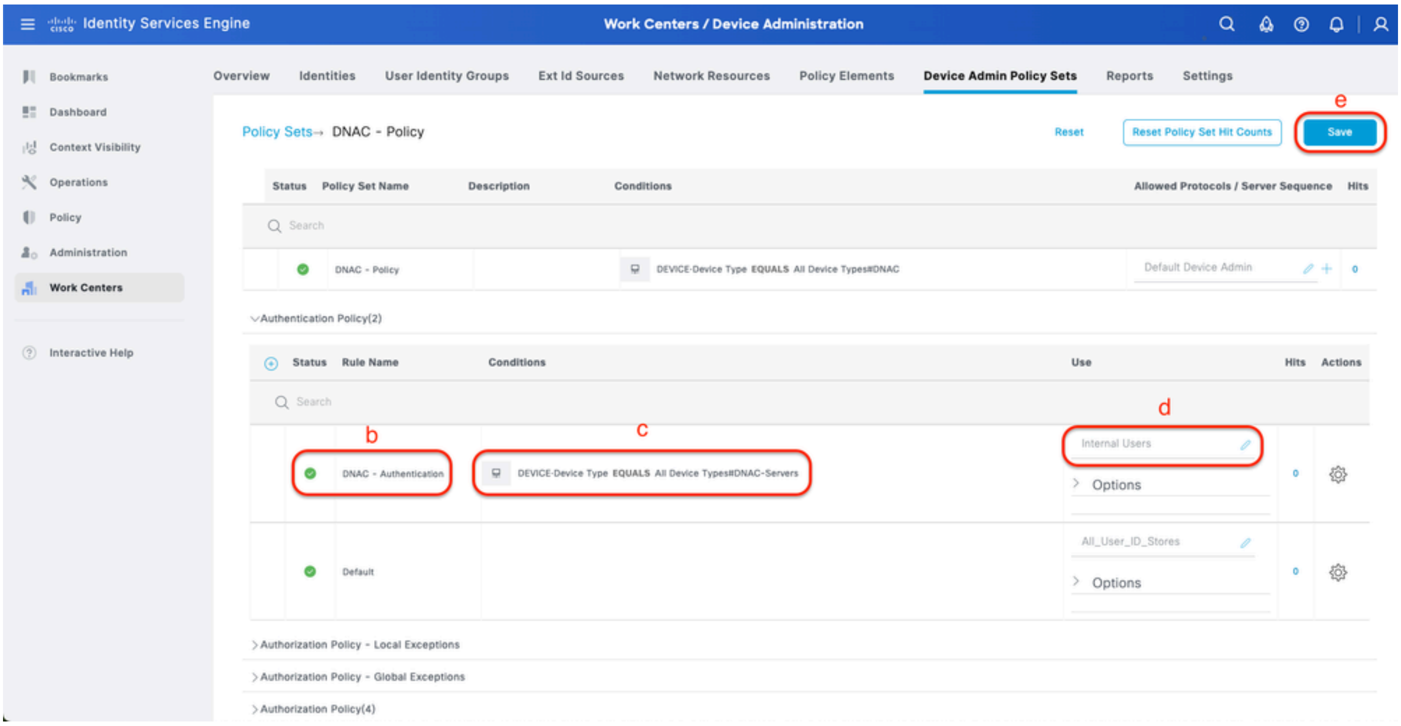
a.单击Actions并选择(上面插入新行)。

b.定义身份验证策略名称。

c.设置先前在上创建的Authentication Policy Condition和Select Device Type（步骤2 > b）。

d.为身份源设置Authentication Policy Use。

e.Click Save.



Policy Sets→ DNAC - Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	DNAC - Policy		DEVICE·Device Type EQUALS All Device Types#DNAC	Default Device Admin	0

∨Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	DNAC - Authentication	DEVICE·Device Type EQUALS All Device Types#DNAC-Servers	Internal Users Options	0	⚙
✓	Default		All_User_ID_Stores Options	0	⚙

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

> Authorization Policy(4)

添加TACACS+身份验证策略

步骤8.配置TACACS+授权策略。

这可以从工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)>点击(>)中完成。

此步骤用于为每个用户角色创建授权策略：

- 超级管理员角色
- NETWORK-ADMIN-ROLE
- SecOps角色

步骤

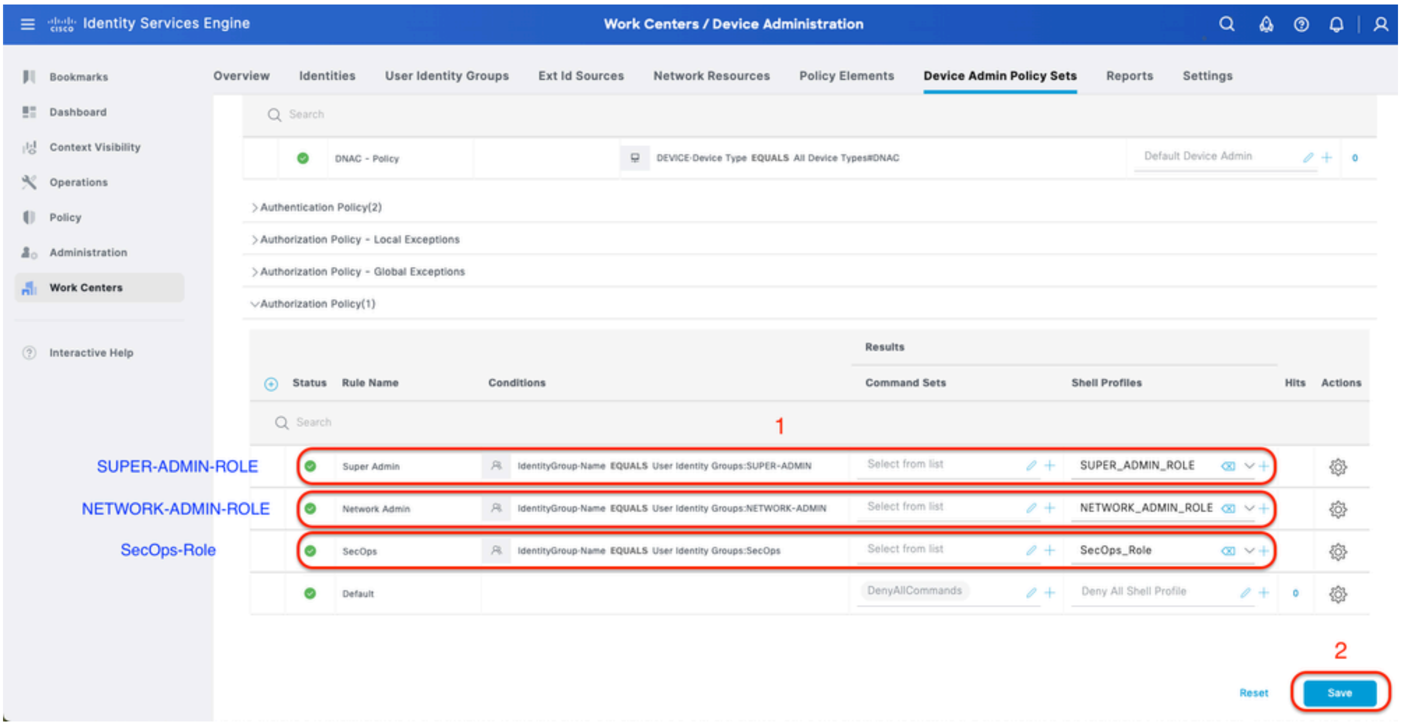
a.单击Actions并选择(上面插入新行)。

b.定义授权策略名称。

c.设置授权策略条件并选择您在中创建的用户组（第4步）。

d.设置授权策略外壳配置文件和选择您在中创建的TACACS配置文件（步骤3）。

e.Click Save.



DNAC - Policy — DEVICE·Device Type EQUALS All Device Types#DNAC — Default Device Admin — 0

> Authentication Policy(2)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy(1)

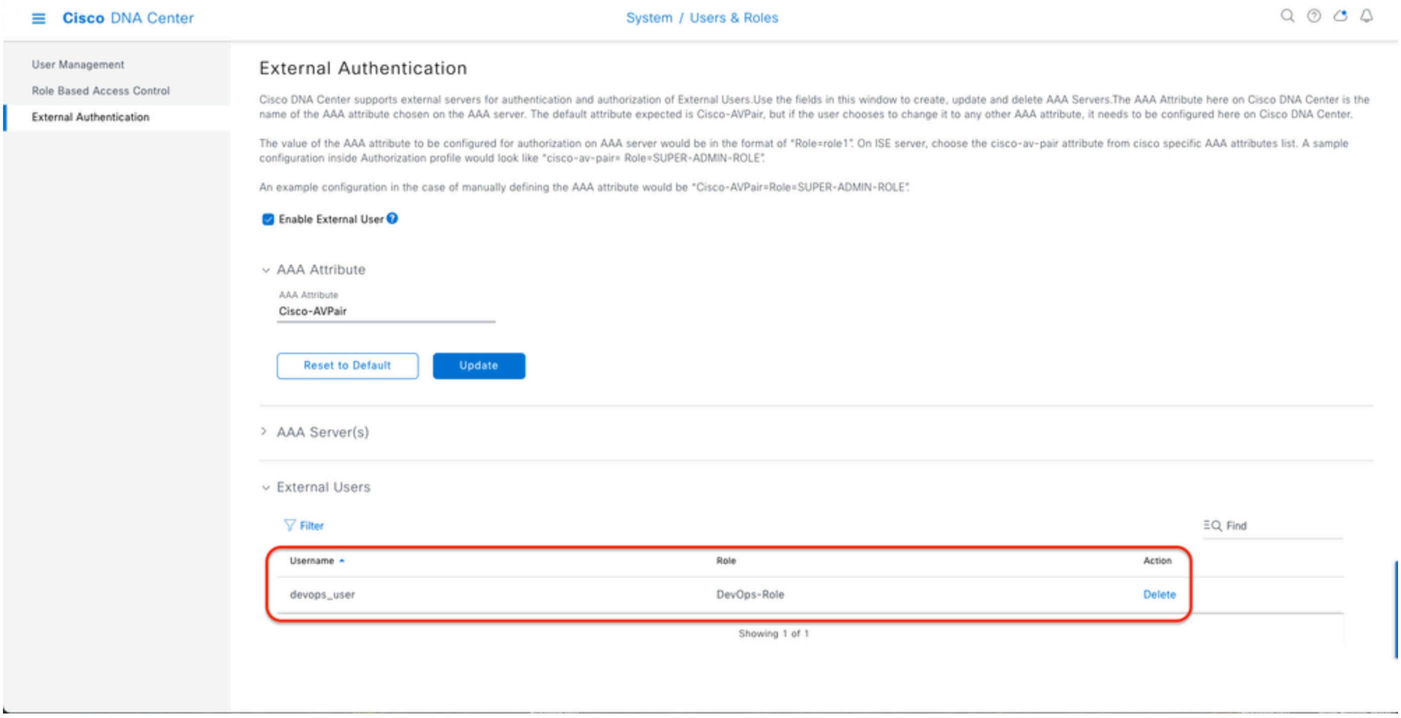
Status	Rule Name	Conditions	Results: Command Sets	Results: Shell Profiles	Hits	Actions
✓	Super Admin	IdentityGroup·Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE		⚙
✓	Network Admin	IdentityGroup·Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE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

添加授权策略

验证

检验RADIUS配置

1- DNAC — 显示外部用户系统>用户和角色>外部身份验证>外部用户。
您可以查看首次通过RADIUS登录的外部用户的列表。显示的信息包括他们的用户名和角色。



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

> AAA Server(s)

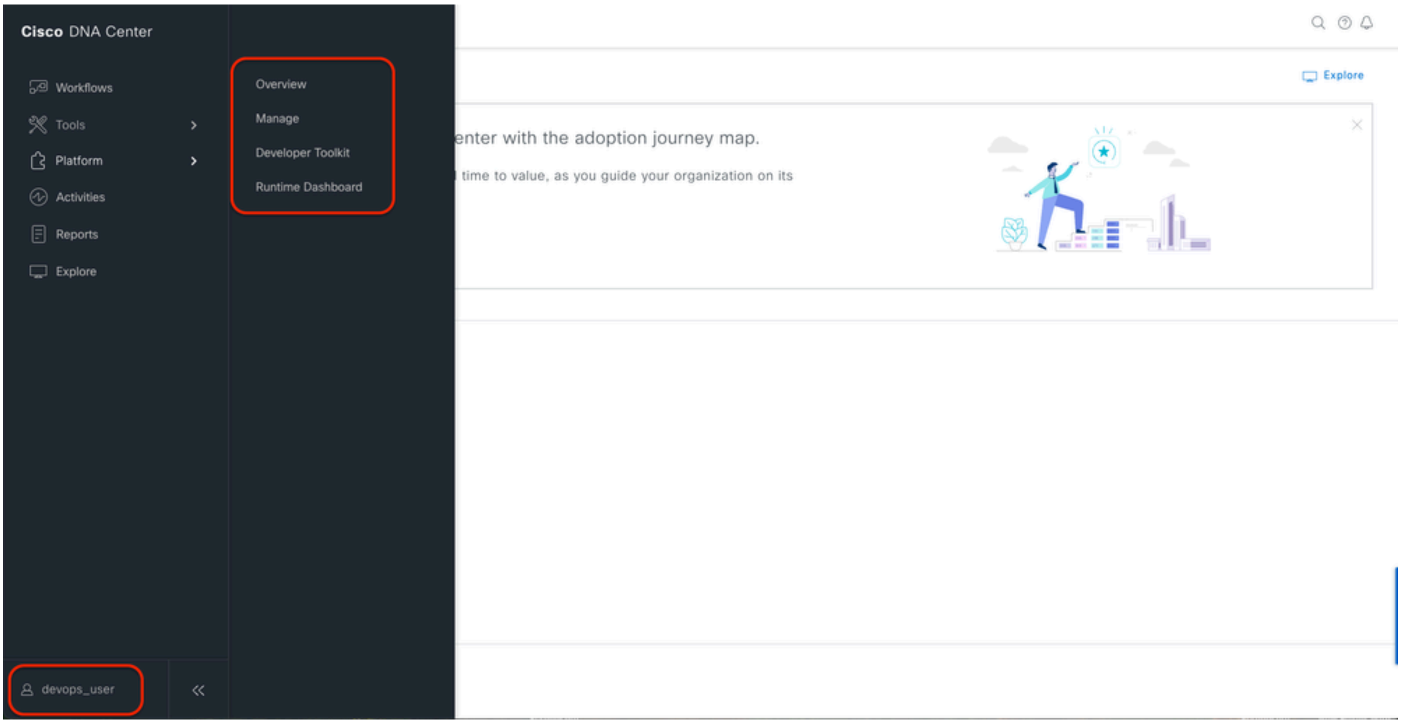
∨ External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

外部用户

2. DNAC — 确认用户访问权限。

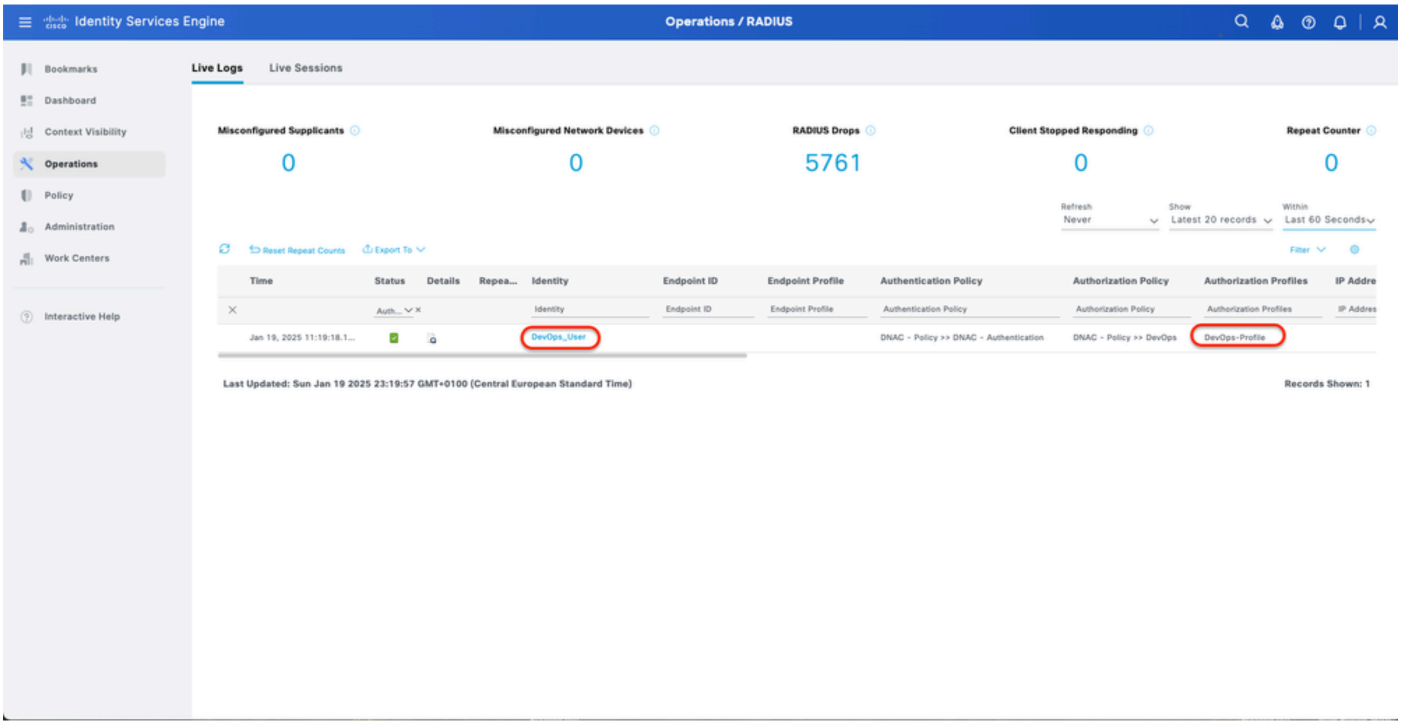


enter with the adoption journey map.

time to value, as you guide your organization on its

有限的用户访问

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



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	5761	0	0

Refresh: Never
Show: Latest 20 records
Within: Last 60 Seconds

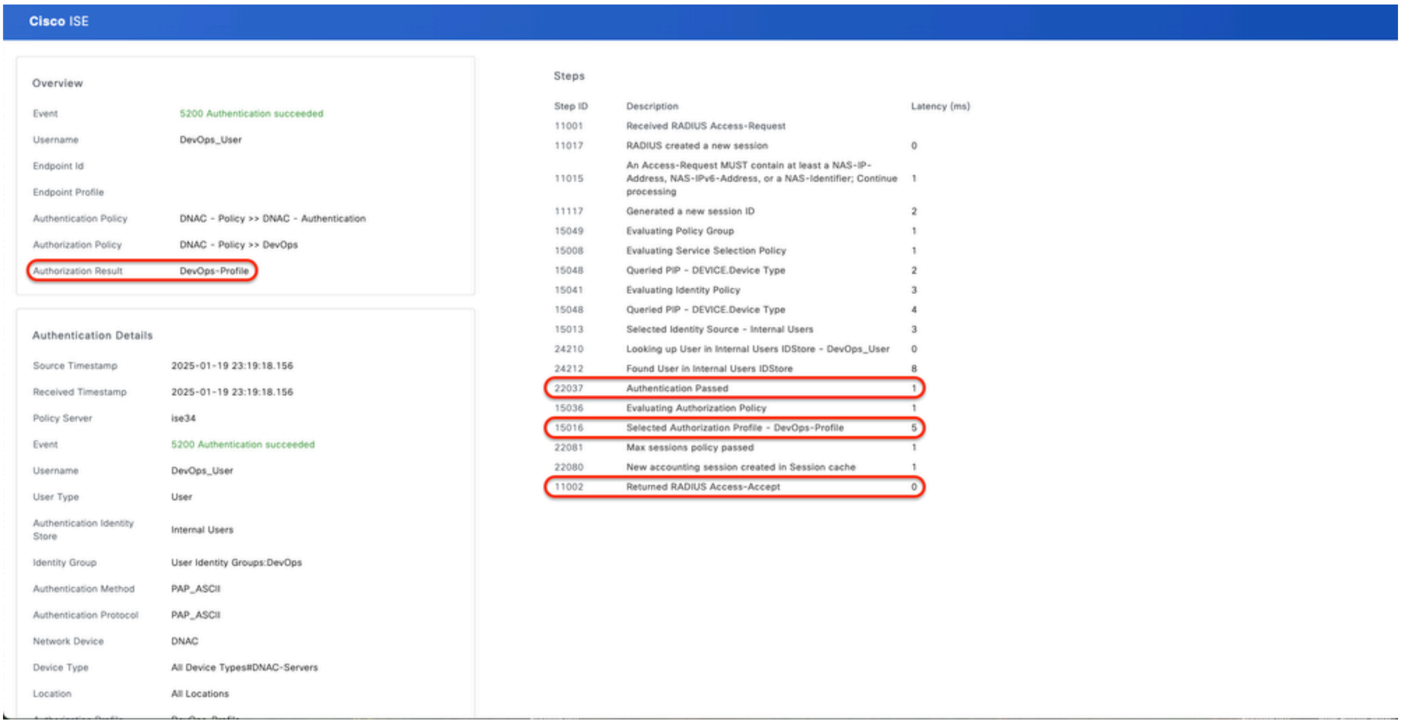
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Addre
Jan 19, 2025 11:19:18.1...	✓			DevOps_User			DNAC - Policy >> DNAC - Authentication	DNAC - Policy >> DevOps	DevOps-Profile	

Last Updated: Sun Jan 19 2025 23:19:57 GMT+0100 (Central European Standard Time)

Records Shown: 1

RADIUS实时日志

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



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

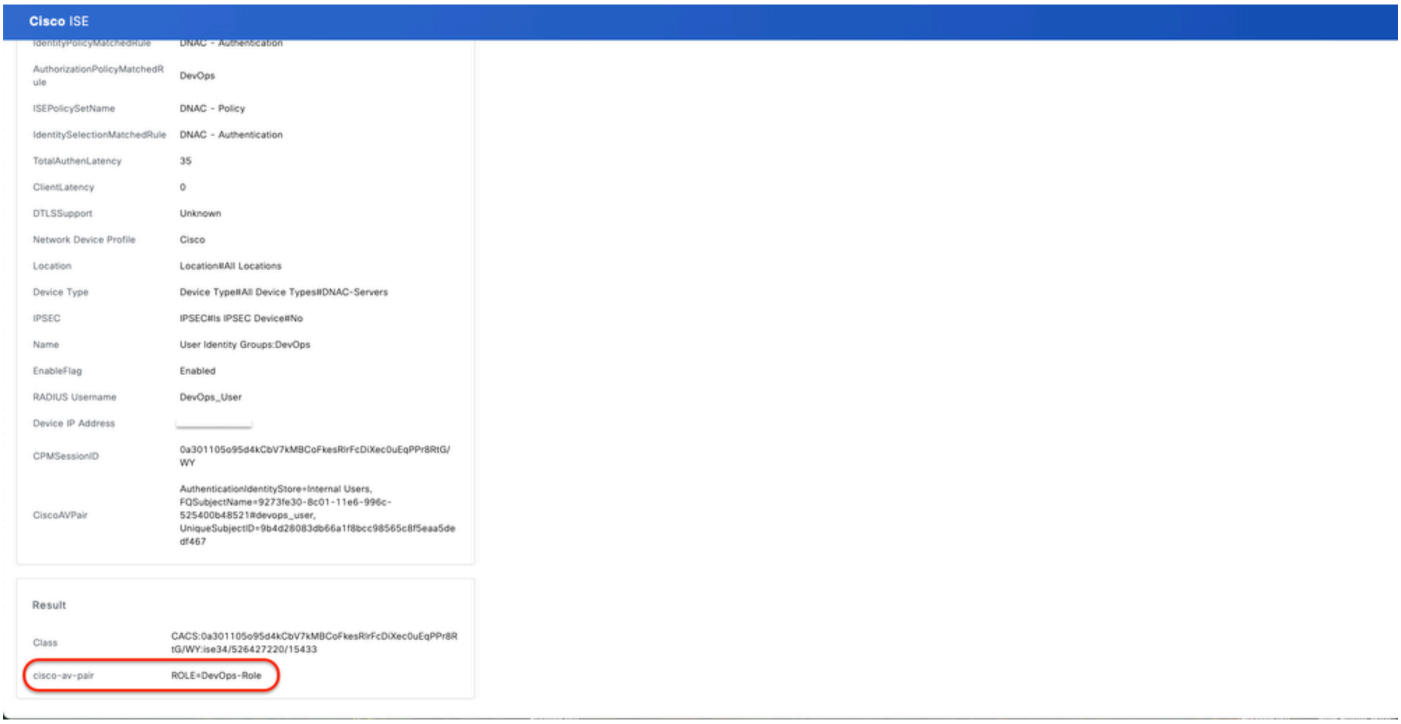
Authentication Details

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
Authorization Profile	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

RADIUS详细实时日志1-2



IdentityPolicyMatchedRule	DNAC - Authentication
AuthorizationPolicyMatchedRule	DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedRule	DNAC - Authentication
TotalAuthenLatency	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	[redacted]
CPMSessionID	0a301105o95d4kCbV7kMBCoFkesRlrFcDiXecOuEqPPr8RtG/WY
CiscoAVPair	AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5dedf467

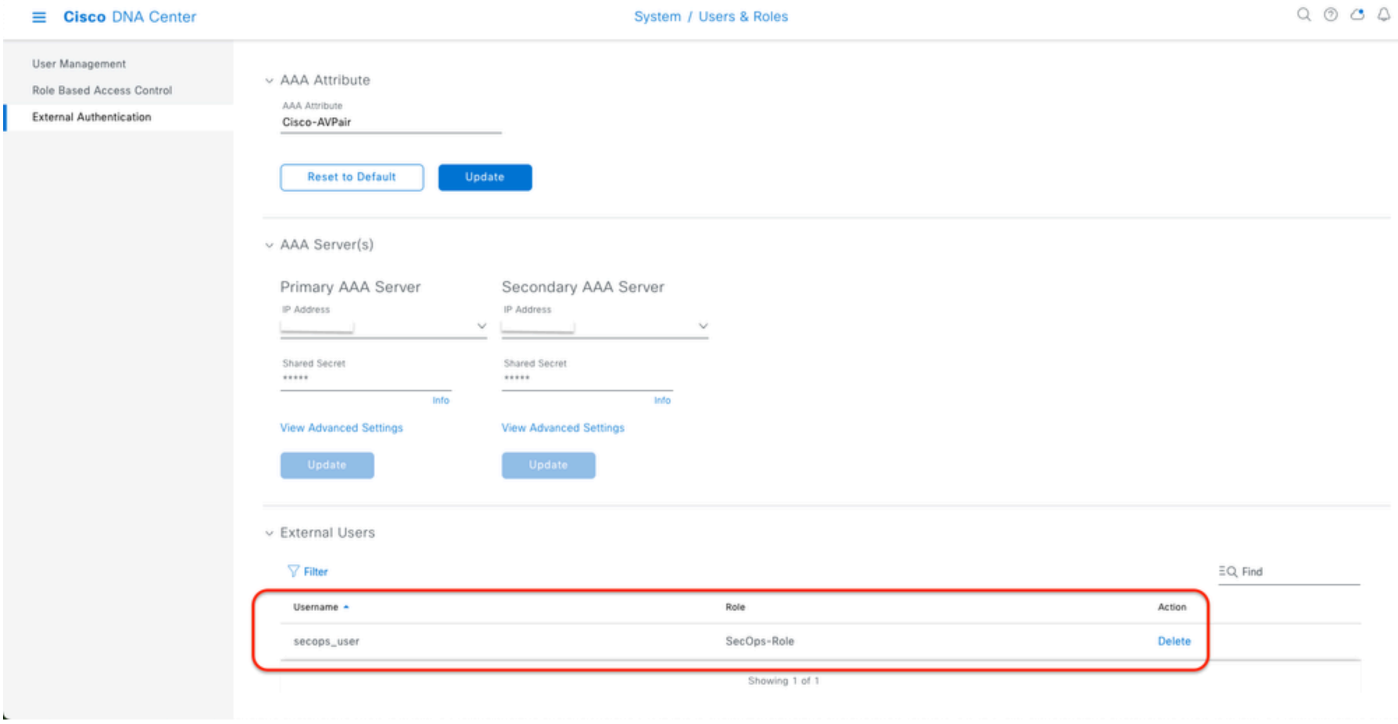
Result

Class	CACS:0a301105o95d4kCbV7kMBCoFkesRlrFcDiXecOuEqPPr8RtG/WY:ise34/526427220/15433
cisco-av-pair	ROLE=DevOps-Role

RADIUS详细实时日志2-2

检验TACACS+配置

1- DNAC — 显示外部用户系统>用户和角色>外部身份验证>外部用户。
您可以查看首次通过TACACS+登录的外部用户的列表。显示的信息包括他们的用户名和角色。

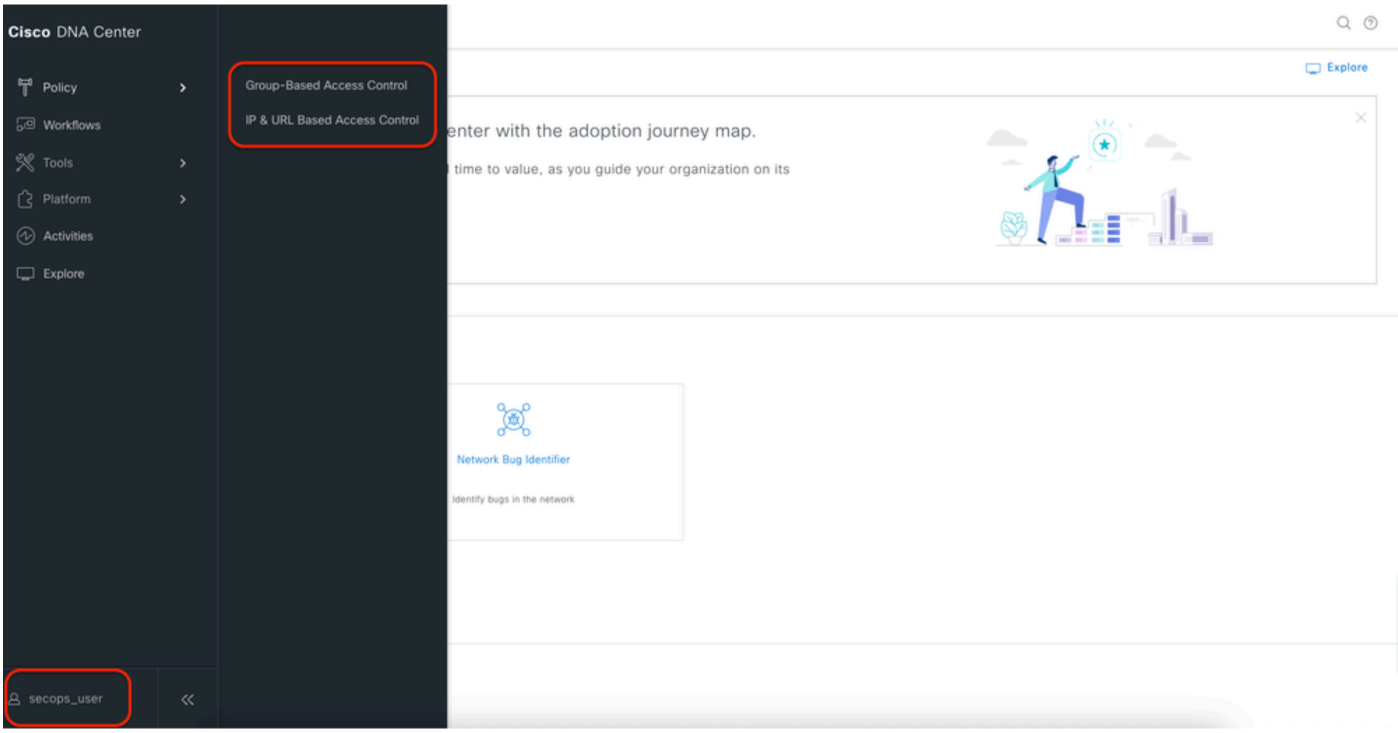


Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

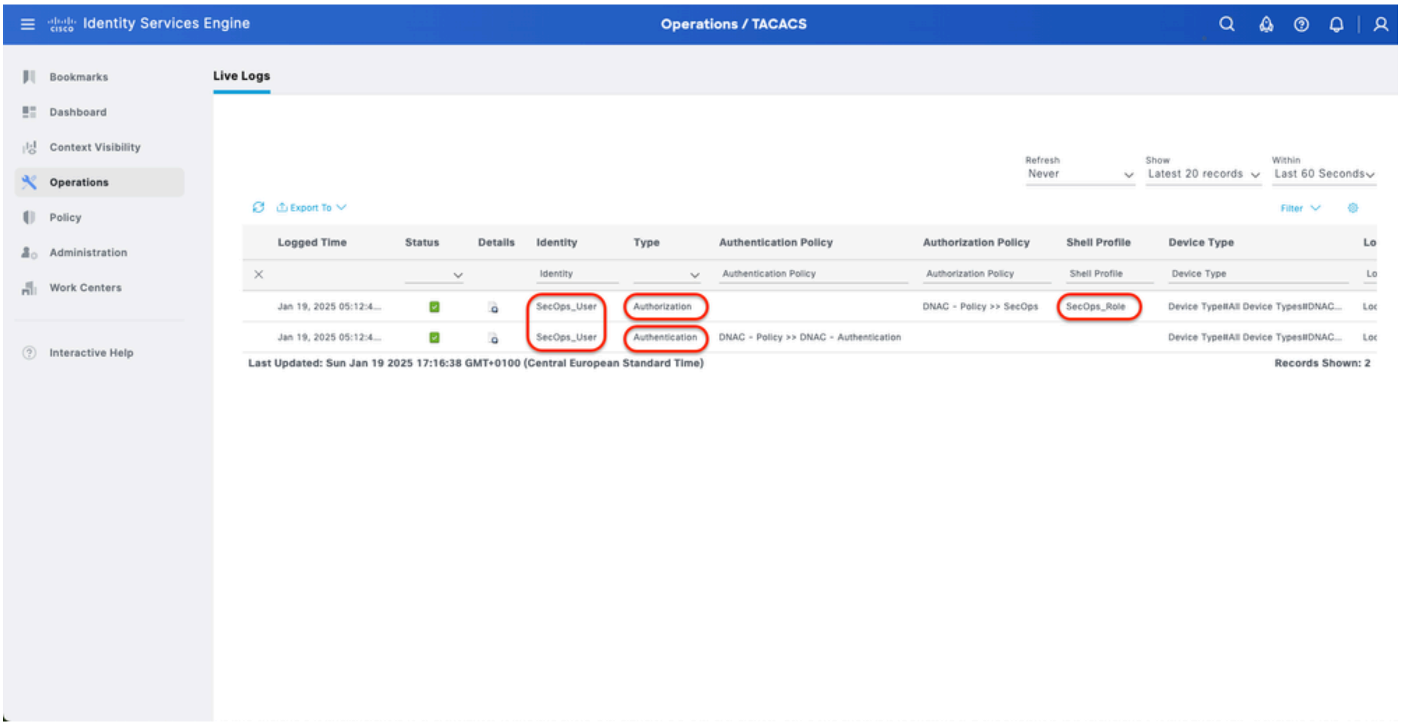
外部用户

2. DNAC — 确认用户访问权限。


Cisco DNA Center
Policy
Workflows
Tools
Platform
Activities
Explore
Group-Based Access Control
IP & URL Based Access Control
Explore
enter 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

有限的用户访问

3.a ISE - TACACS+实时日志工作中心(Work Centers)>设备管理(Device Administration)>概述(Overview)> TACACS实时日志(TACACS Livelog)。



Refresh: Never
Show: Latest 20 records
Within: Last 60 Seconds

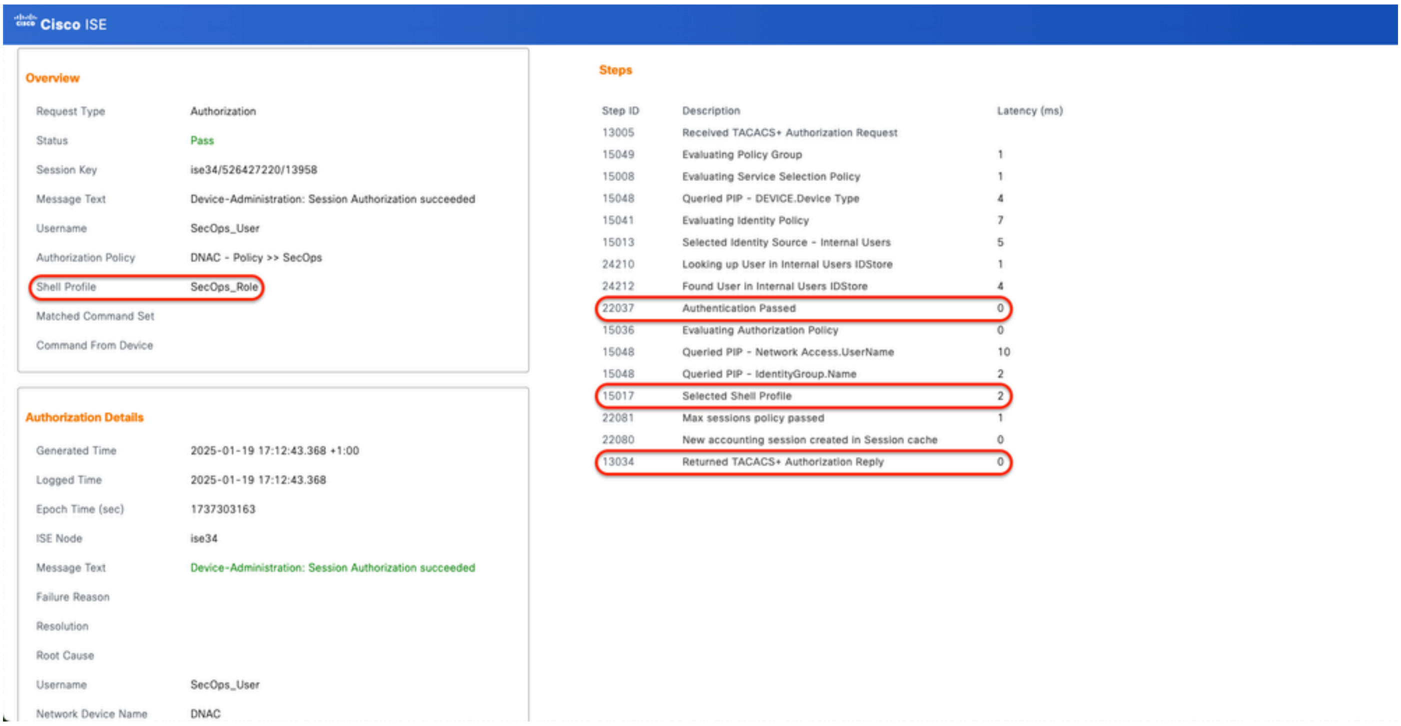
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All Device Types#DNAC...	Loc
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC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

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

Records Shown: 2

TACACS实时日志

3.b ISE — 详细的TACACS+实时日志工作中心(Work Centers)>设备管理(Device Administration)>概述(Overview)> TACACS实时日志(TACACS Livelog)>点击（ 详细信息）(Click(Details))获取授权日志。



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	

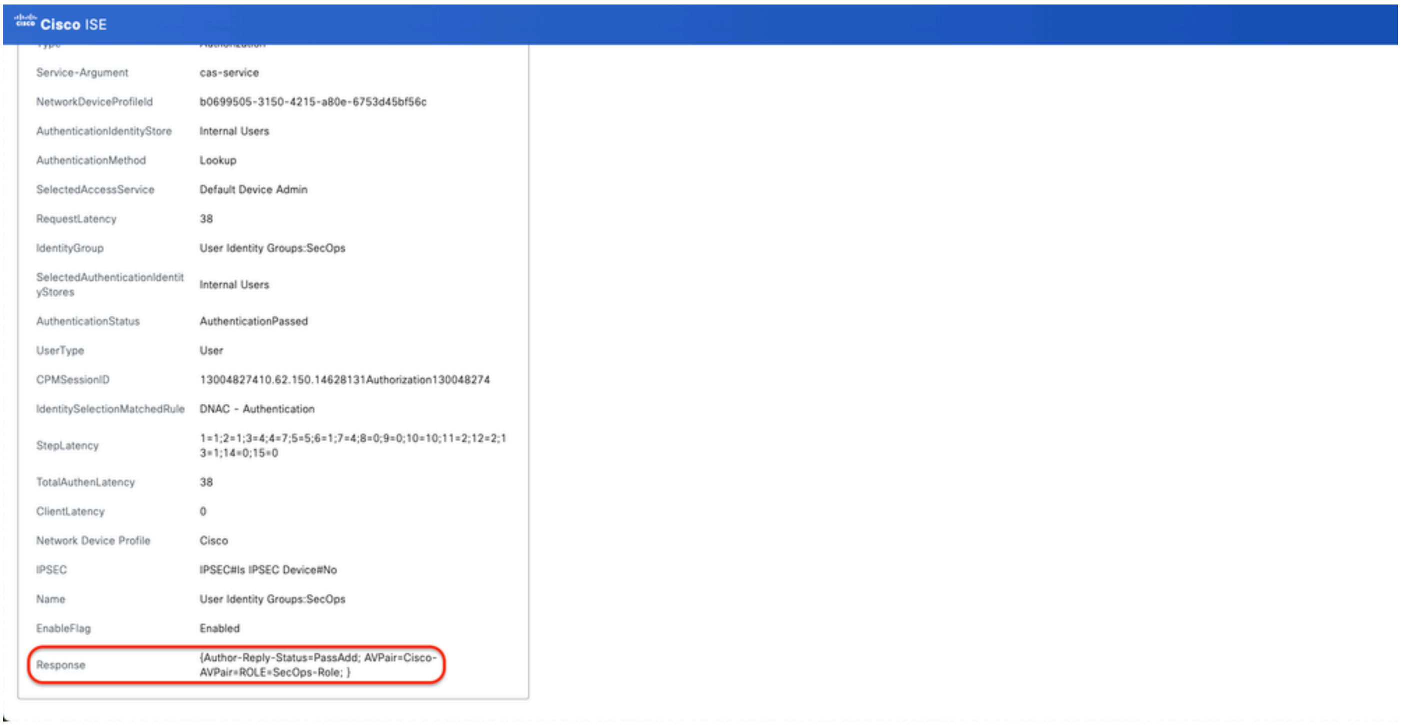
Authorization Details

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+详细实时日志1-2



Cisco ISE

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
TotalAuthenLatency	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+详细实时日志2-2

故障排除

当前没有可用于此配置的特定诊断信息。

参考

- 思科身份服务引擎管理员指南，版本3.4 >设备管理
- Cisco DNA Center管理员指南，版本2.3.5
- Cisco DNA Center：使用外部身份验证的基于角色的访问控制

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。