

ISE를 DNAC GUI용 외부 인증으로 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[시작하기 전에](#)

[구성](#)

[\(옵션1\) RADIUS를 사용하여 DNAC 외부 인증 구성](#)

[\(옵션1\) RADIUS를 위한 ISE 구성](#)

[\(옵션2\) TACACS+를 사용하여 DNAC 외부 인증 구성](#)

[\(옵션2\) TACACS+용 ISE 구성](#)

[다음을 확인합니다.](#)

[RADIUS 컨피그레이션 확인](#)

[TACACS+ 컨피그레이션 확인](#)

[문제 해결](#)

[참조](#)

소개

이 문서에서는 Cisco DNA Center GUI 관리를 위한 외부 인증으로 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- TACACS+ 및 RADIUS 프로토콜.
- Cisco ISE와 Cisco DNA Center의 통합
- Cisco ISE 정책 평가.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.


- Cisco ISE(Identity Services Engine) 버전 3.4 패치 1.
- Cisco DNA Center 버전 2.3.5.5.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

시작하기 전에

- System(시스템) > Settings(설정) > External Services(외부 서비스) > Authentication and Policy Servers(인증 및 정책 서버)에서 적어도 하나 이상의 RADIUS 인증 서버를 구성했는지 확인합니다.
- DNAC에 대한 SUPER-ADMIN-ROLE 권한이 있는 사용자만 이 절차를 수행할 수 있습니다.
- 외부 인증 폴백을 활성화합니다.

 주의: 2.1.x 이전 릴리스에서 외부 인증이 활성화된 경우, AAA 서버에 연결할 수 없거나 AAA 서버가 알 수 없는 사용자 이름을 거부하면 Cisco DNA Center는 로컬 사용자에게 폴백됩니다. 현재 릴리스에서는 AAA 서버에 연결할 수 없거나 AAA 서버가 알 수 없는 사용자 이름을 거부하는 경우 Cisco DNA Center가 로컬 사용자에게 돌아가지 않습니다. 외부 인증 폴백이 활성화된 경우 외부 사용자 및 로컬 관리자가 Cisco DNA Center에 로그인할 수 있습니다.

외부 인증 폴백을 활성화하려면 Cisco DNA Center 인스턴스에 SSH를 적용하고 이 CLI 명령 (`magctl rbac external_auth_fallback enable`)을 입력합니다.

구성

(옵션1) RADIUS를 사용하여 DNAC 외부 인증 구성

단계 1. (선택 사항) 사용자 지정 역할을 정의합니다.

요구 사항을 충족하는 사용자 지정 역할을 구성합니다. 대신 기본 사용자 역할을 사용할 수 있습니다. 이 작업은 System(시스템) > Users & Roles(사용자 및 역할) > Role Based Access Control(역할 기반 액세스 제어) 탭에서 수행할 수 있습니다.

절차

a. 새 역할을 만듭니다.

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)

2

Next

DevOps 역할 이름

b. 액세스 권한을 정의합니다.

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.

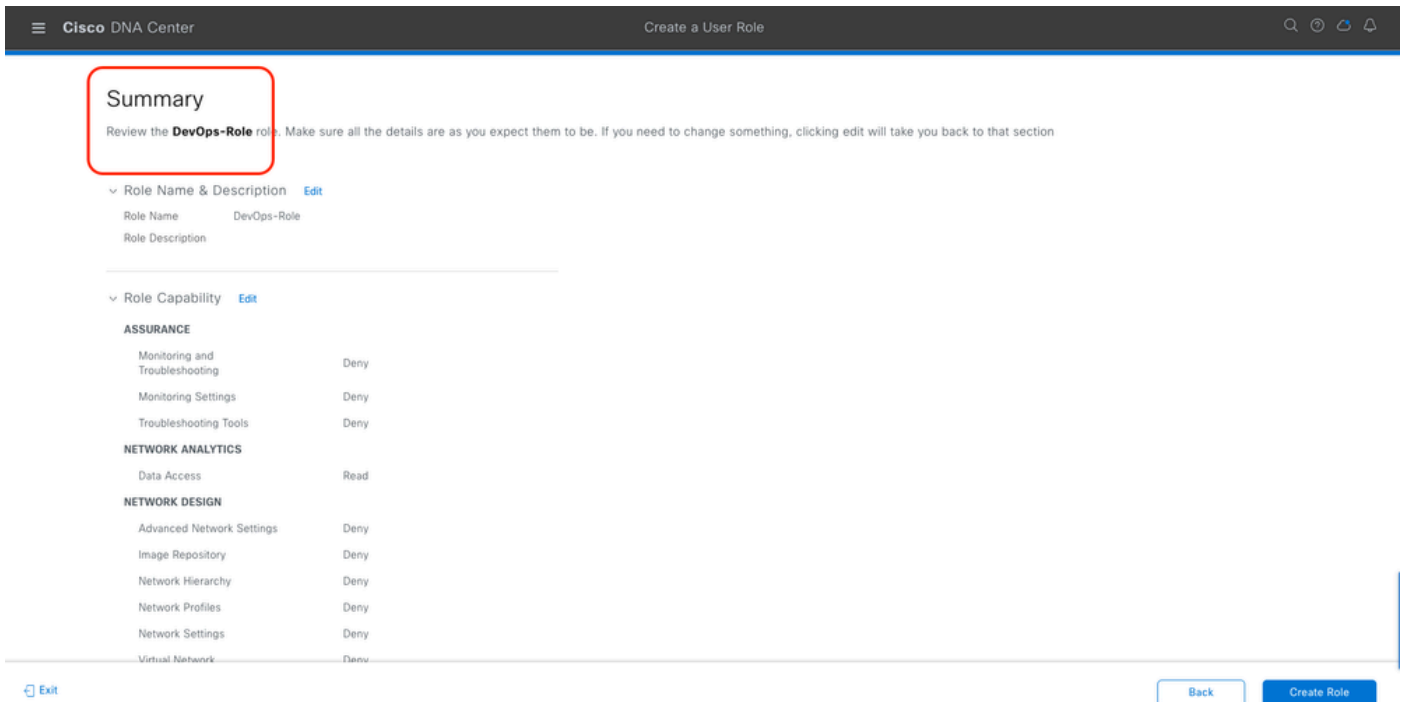
2

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.

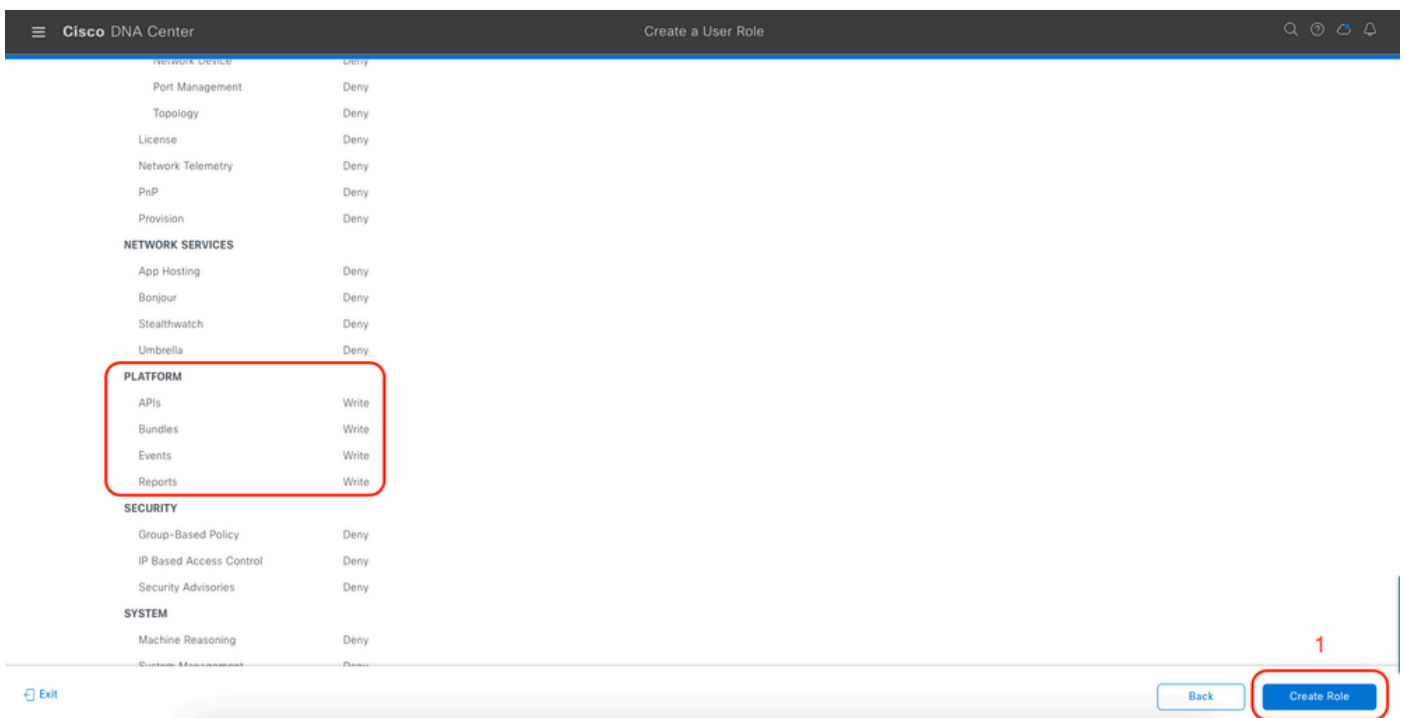
Next

DevOps 역할 액세스

c. 새 역할을 생성합니다.



DevOps 역할 요약



DevOps 역할 검토 및 생성

2단계. RADIUS를 사용하여 외부 인증을 구성합니다.

이 작업은 System(시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증) 탭에서 수행할 수 있습니다.

절차

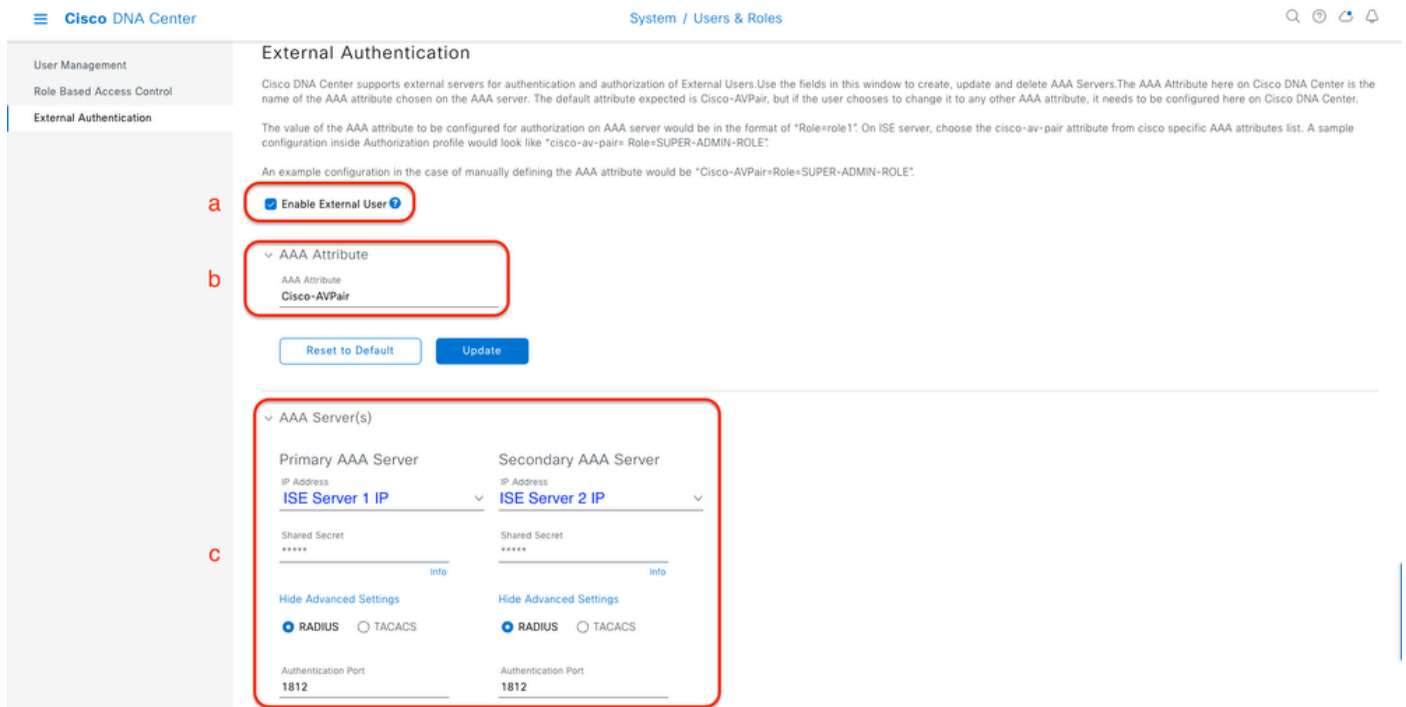
a. Cisco DNA Center에서 외부 인증을 활성화하려면 Enable External User(외부 사용자 활성화) 확인란을 선택합니다.

b. AAA 특성을 설정합니다.

AAA 특성 필드에 Cisco-AVPair를 입력합니다.

c. (선택 사항) 기본 및 보조 AAA 서버를 구성합니다.

RADIUS 프로토콜이 주 AAA 서버 이상 또는 주 서버와 보조 서버 모두에서 활성화되어 있는지 확인합니다.



(RADIUS) 외부 인증 컨피그레이션 단계

(옵션1) RADIUS를 위한 ISE 구성

1단계. ISE에서 DNAC 서버를 네트워크 디바이스로 추가합니다.

이 작업은 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 탭에서 수행할 수 있습니다.

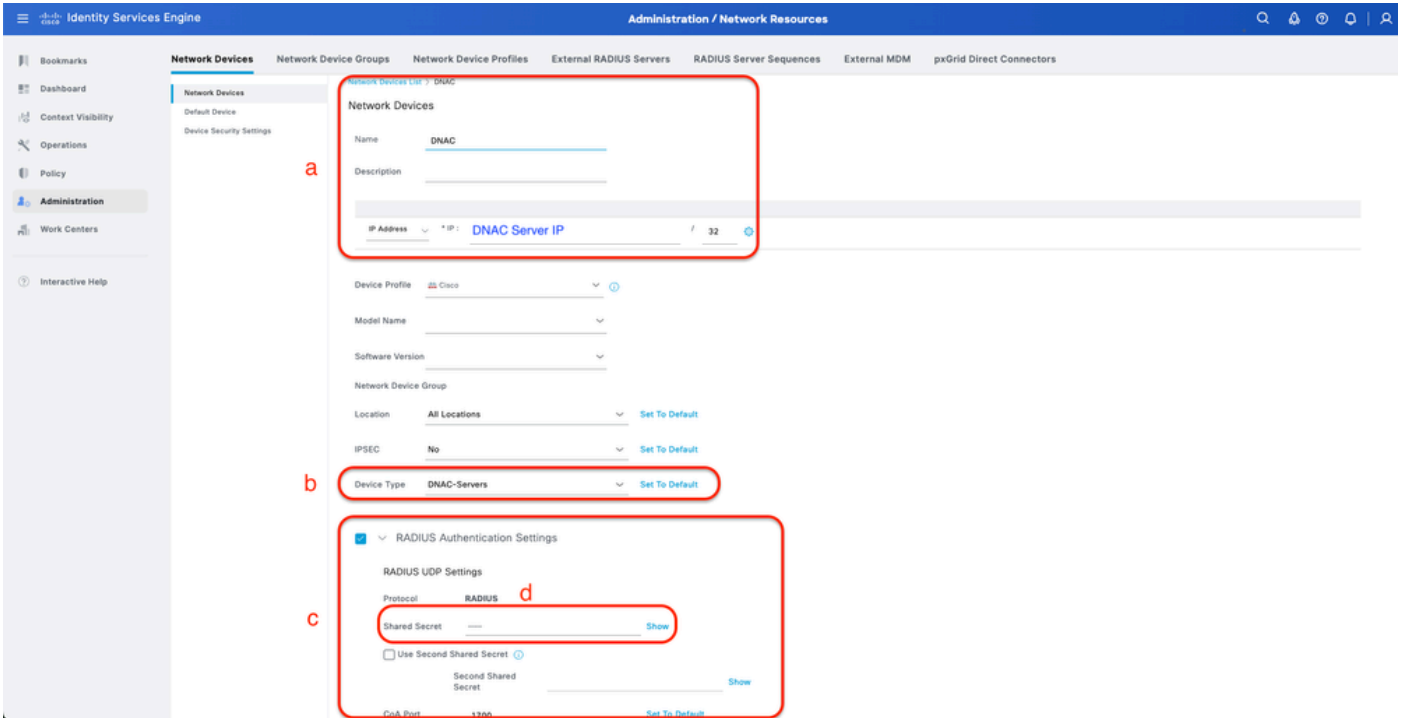
절차

a. (DNAC) 네트워크 디바이스 이름 및 IP를 정의합니다.

b. (선택 사항) 정책 집합 조건에 대한 디바이스 유형을 분류합니다.

c. RADIUS 인증 설정을 활성화합니다.

d. RADIUS 공유 암호를 설정합니다.



RADIUS용 ISE 네트워크 디바이스(DNAC)

2단계. RADIUS 권한 부여 프로파일을 생성합니다.

이 작업은 탭에서 수행할 수 있습니다. 정책 > 정책 구성 요소 > 결과 > 인증 > 권한 부여 프로파일.

 참고: 각 사용자 역할에 대해 하나씩 3x RADIUS 권한 부여 프로파일을 생성합니다.

절차

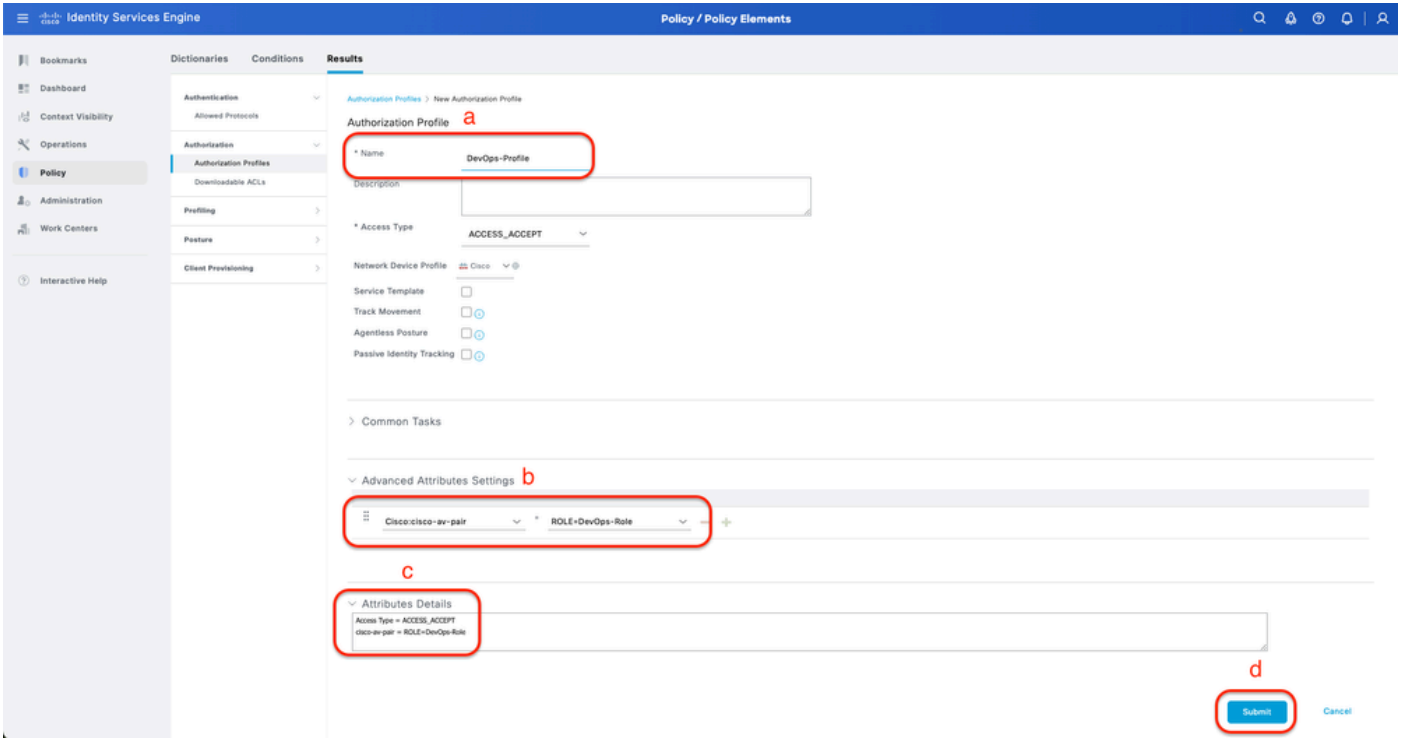
a. Add(추가)를 클릭하고 RADIUS Authorization Profile(RADIUS 권한 부여 프로파일) 이름을 정의합니다.

b. Advanced Attributes Settings(고급 특성 설정)에 Cisco:cisco-av-pair를 입력하고 올바른 사용자 역할을 채웁니다.

- (DecOps-Role) 사용자 역할에 ROLE=DevOps-Role을 입력합니다.
- (NETWORK-ADMIN-ROLE) 사용자 역할의 경우 ROLE =NETWORK-ADMIN-ROLE을 입력합니다.
- (SUPER-ADMIN-ROLE) 사용자 역할의 경우 ROLE =SUPER-ADMIN-ROLE을 입력합니다.

c. Attribute Details(특성 세부사항)를 검토합니다.

d. 저장을 클릭합니다.



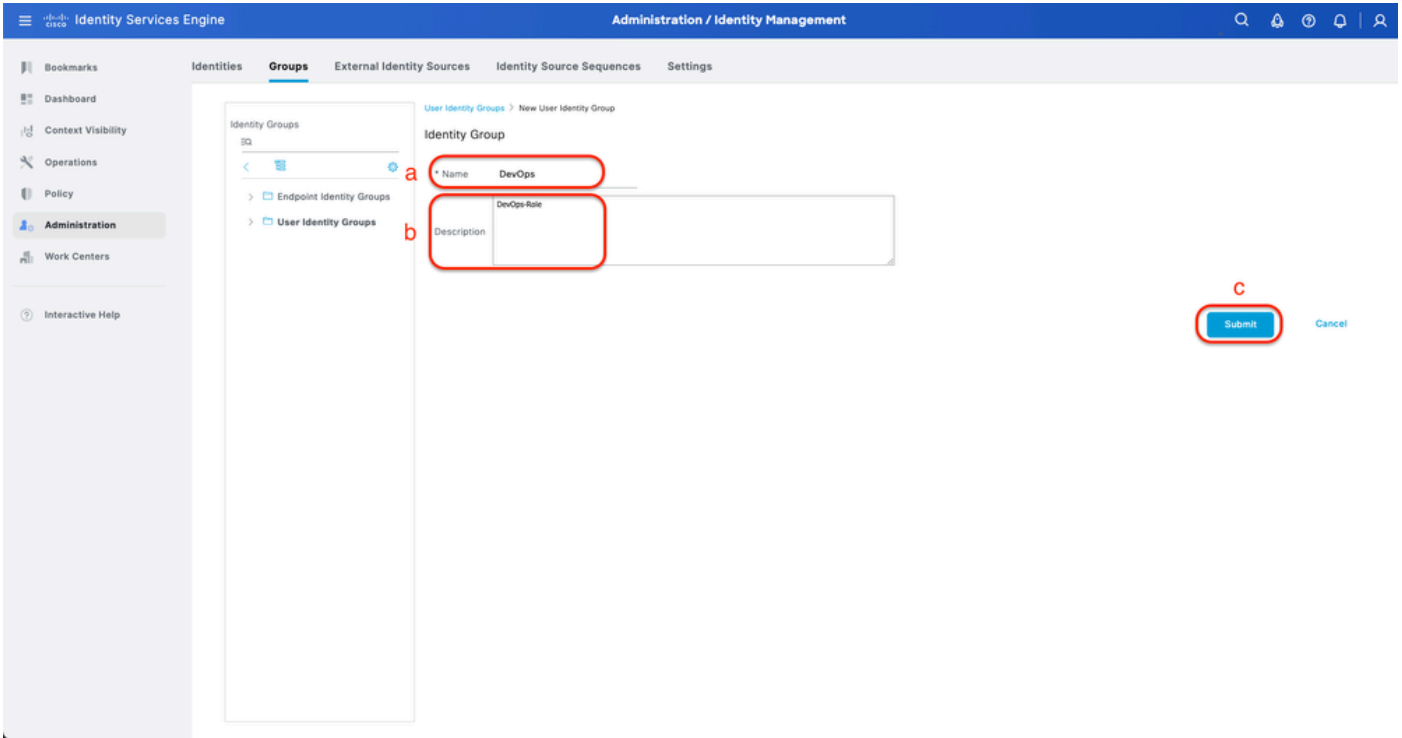
권한 부여 프로파일 생성

3단계. 사용자 그룹을 생성합니다.

이 작업은 Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹) 탭에서 수행할 수 있습니다.

절차

- a. Add(추가)를 클릭하고 ID 그룹 이름을 정의합니다
- b. (선택 사항) 설명을 정의합니다.
- c. 제출을 클릭합니다.



사용자 ID 그룹 생성

4단계. 로컬 사용자를 생성합니다.

이 작업은 Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) 탭에서 수행할 수 있습니다.

절차

- a. Add(추가)를 클릭하고 Username(사용자 이름)을 정의합니다.
- b. 로그인 비밀번호를 설정합니다.
- c. 관련 사용자 그룹에 사용자를 추가합니다.
- d. Submit(제출)을 클릭합니다.

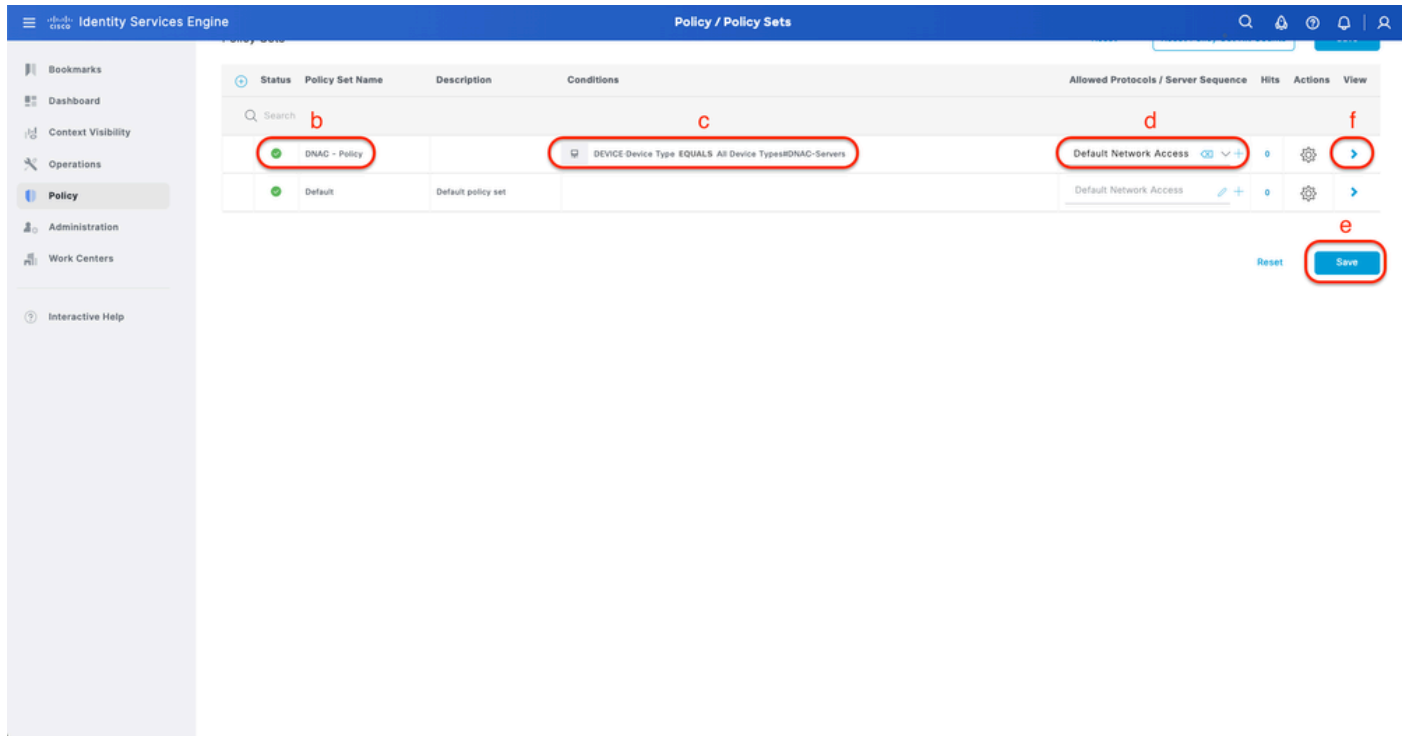
b. 정책 집합 이름을 정의합니다.

c. 이전에 생성한 Select Device Type(디바이스 유형 선택)으로 Policy Set Condition(정책 설정 조건)을 설정합니다(1단계 > b).

d. Allowed 프로토콜을 설정합니다.

e. 저장을 클릭합니다.

f. 인증 및 권한 부여 규칙을 구성하려면 (>) Policy Set View를 클릭합니다.



RADIUS 정책 집합 추가

6단계. RADIUS 인증 정책을 구성합니다.

이 작업은 Policy(정책) > Policy Sets(정책 집합) > Click(>) 탭에서 수행할 수 있습니다.

절차

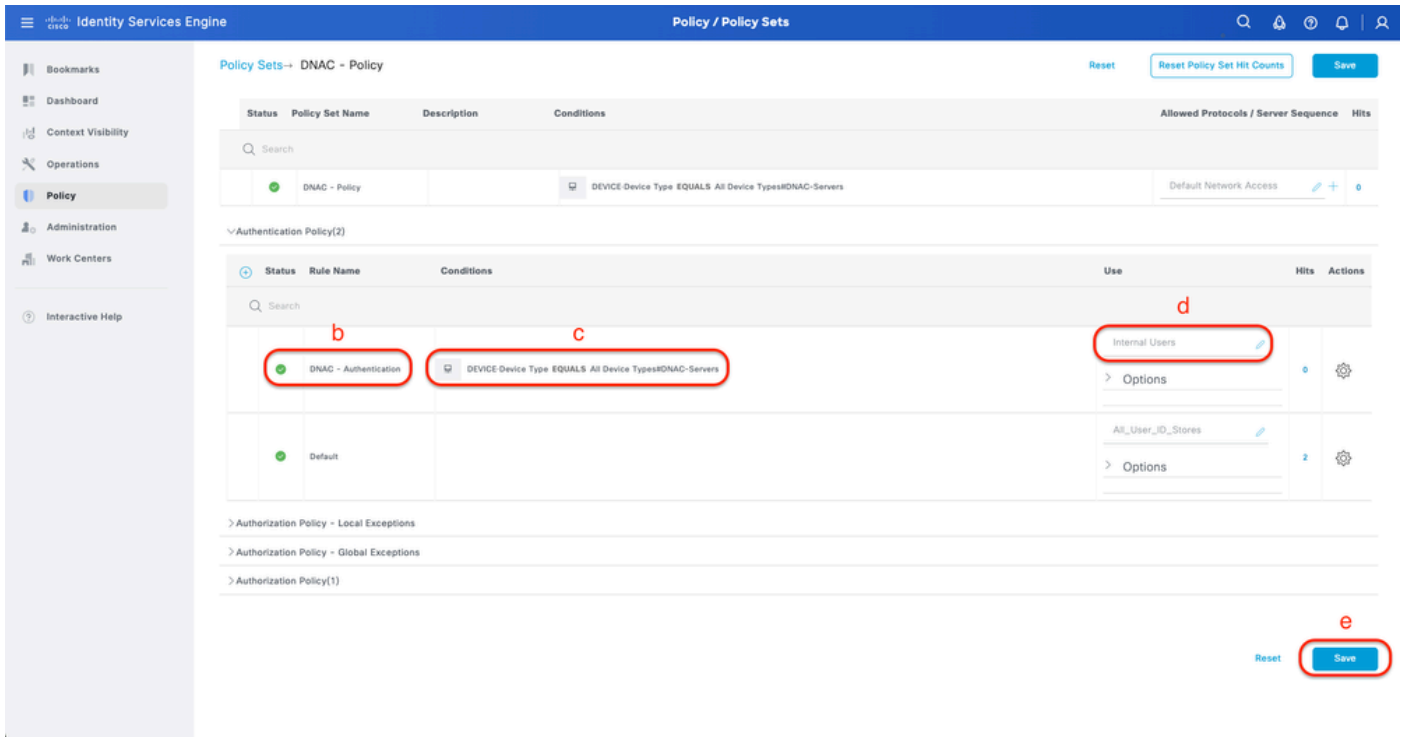
a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 인증 정책 이름을 정의 합니다.

c. Authentication Policy Condition(인증 정책 조건)을 설정하고 이전에 생성한 Device Type(디바이스 유형)을 선택합니다(1단계 > b).

d. ID 소스에 대한 인증 정책 사용을 설정합니다.

e. 저장을 클릭합니다.



RADIUS 인증 정책 추가

7단계. RADIUS 권한 부여 정책을 구성합니다.

이 작업은 Policy(정책) > Policy Sets(정책 집합) > Click(>) 탭에서 수행할 수 있습니다.

각 사용자 역할에 대한 권한 부여 정책을 생성하려면 다음 단계를 수행합니다.

- 슈퍼 관리자 역할
- 네트워크 관리자 역할
- DevOps 역할

절차

a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 권한 부여 정책 이름을 정의 합니다.

c. 권한 부여 정책 조건을 설정하고(3단계)에서 생성한 사용자 그룹을 선택합니다.

d. 권한 부여 정책 결과/프로파일을 설정하고 (2단계)에서 생성한 권한 부여 프로파일을 선택합니다

e. 저장을 클릭합니다.

Identity Services Engine Policy / Policy Sets

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	Profiles	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	⚙️

Reset Save

권한 부여 정책 추가

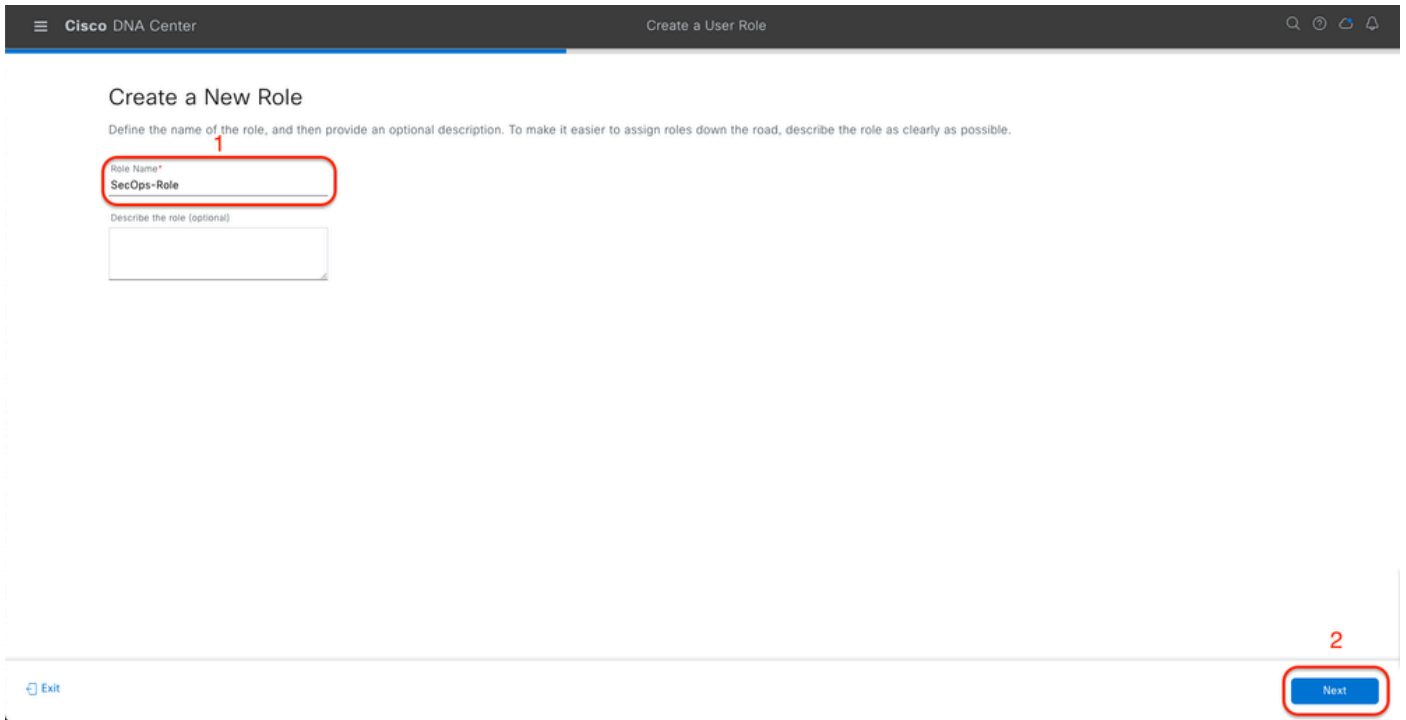
(옵션2) TACACS+를 사용하여 DNAC 외부 인증 구성

단계 1. (선택 사항) 사용자 지정 역할을 정의합니다.

요구 사항을 충족하는 사용자 지정 역할을 구성합니다. 대신 기본 사용자 역할을 사용할 수 있습니다. 이 작업은 System(시스템) > Users & Roles(사용자 및 역할) > Role Based Access Control(역할 기반 액세스 제어) 탭에서 수행할 수 있습니다.

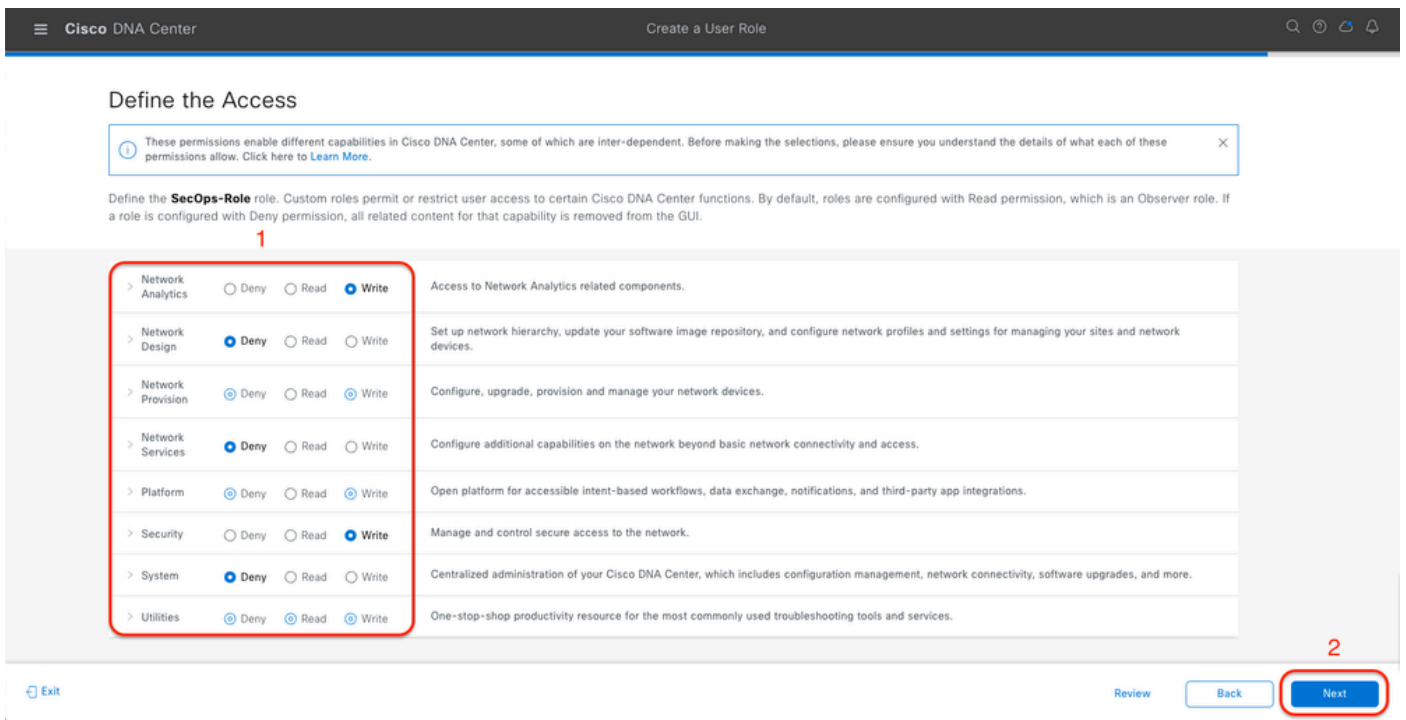
절차

a. 새 역할을 만듭니다.



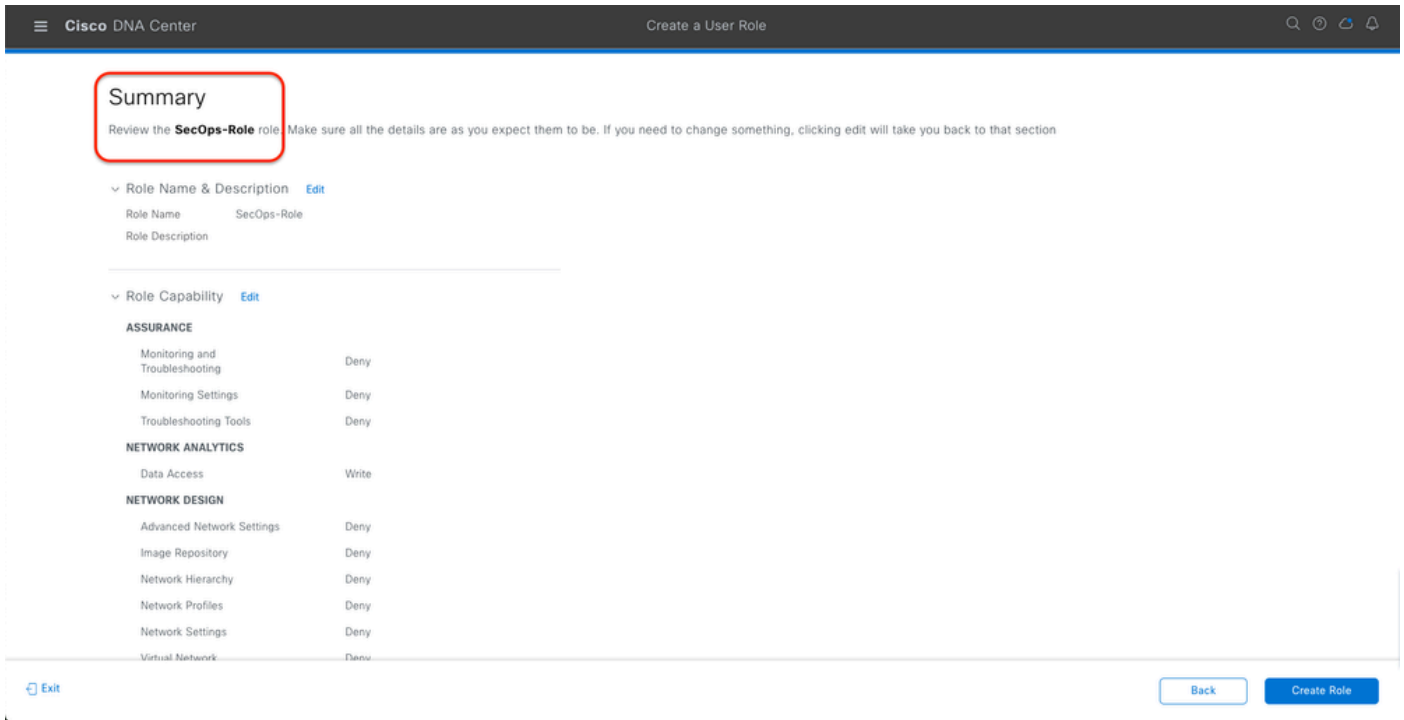
보안 담당 중역 역할 이름

b. 액세스 권한을 정의합니다.

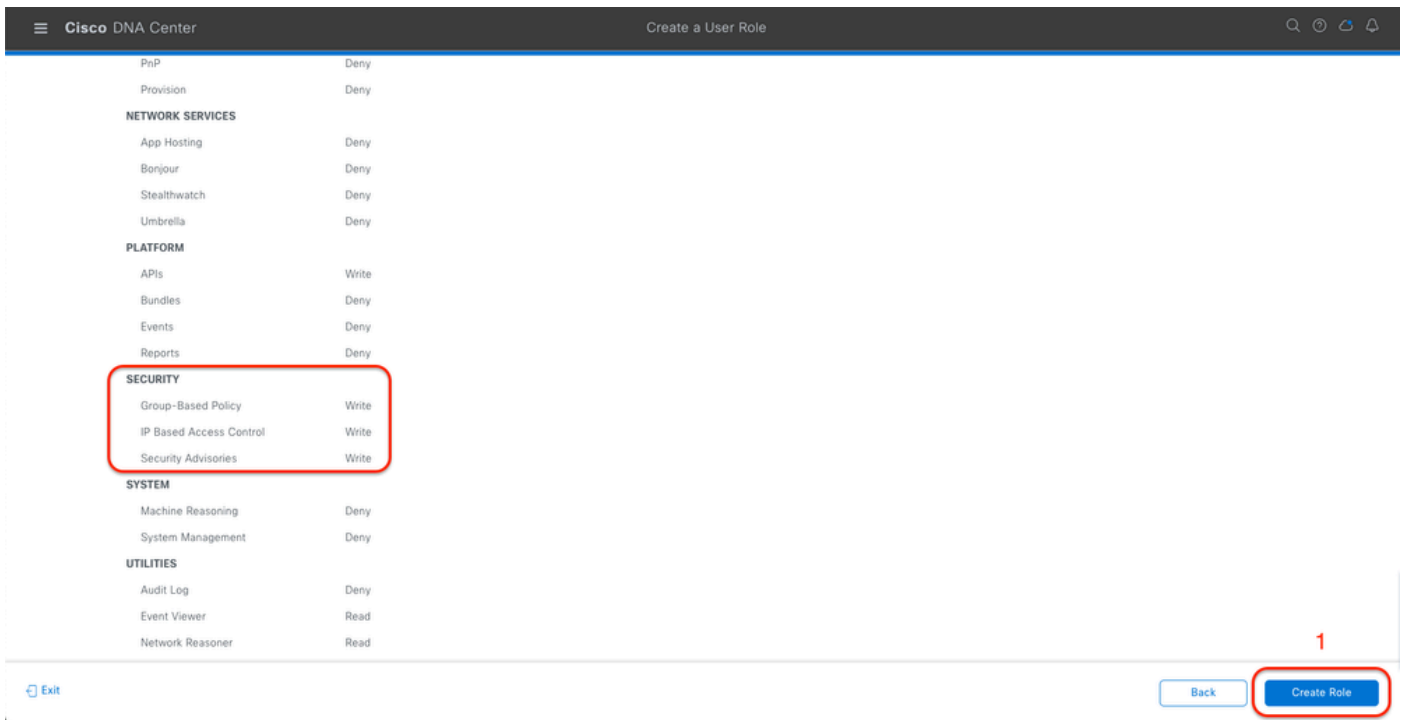


SecOps 역할 액세스

c. 새 역할을 생성합니다.



SecOps 역할 요약



SecOps 역할 검토 및 생성

2단계. TACACS+를 사용하여 외부 인증을 구성합니다.

이 작업은 System(시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증) 탭에서 수행할 수 있습니다.

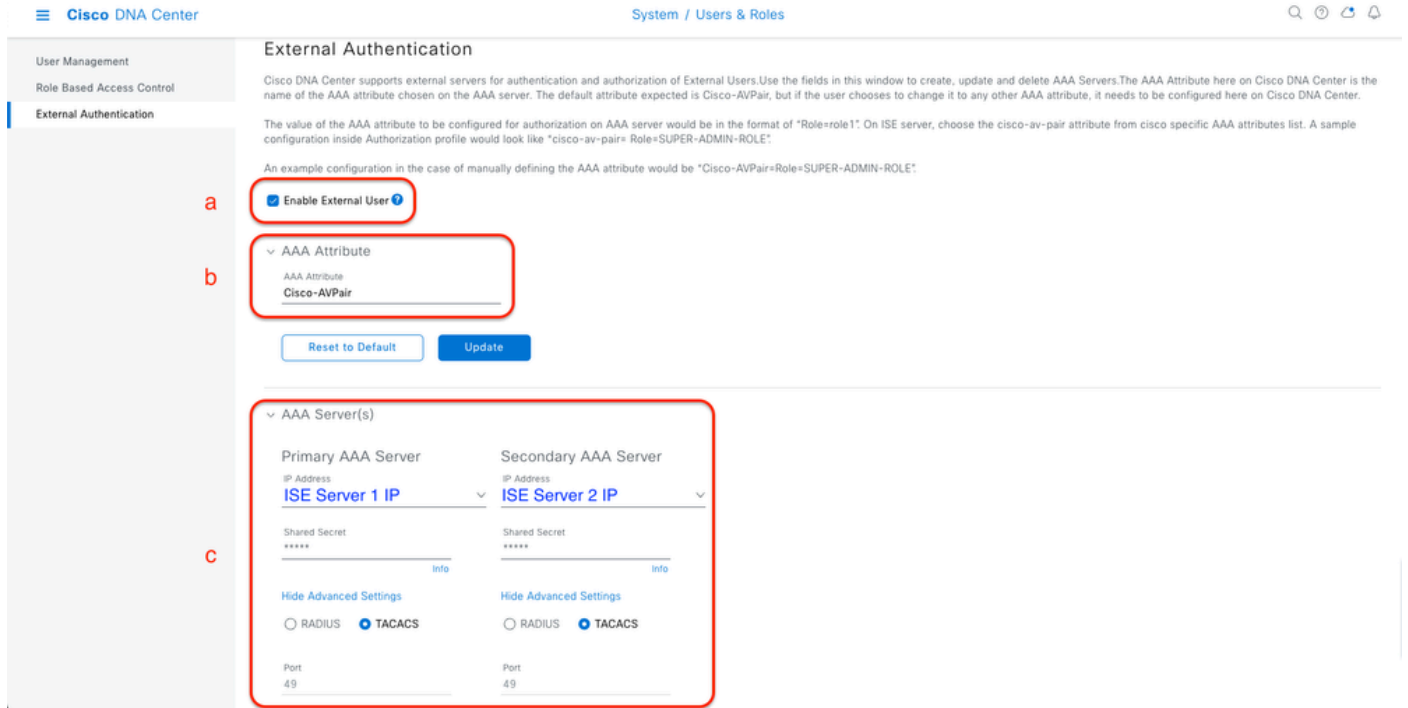
a. Cisco DNA Center에서 외부 인증을 활성화하려면 Enable External User(외부 사용자 활성화) 확인란을 선택합니다.

b. AAA 특성을 설정합니다.

AAA 특성 필드에 Cisco-AVPair를 입력합니다.

c. (선택 사항) 기본 및 보조 AAA 서버를 구성합니다.

TACACS+ 프로토콜이 주 AAA 서버 이상 또는 주 서버와 보조 서버 모두에서 활성화되었는지 확인합니다.

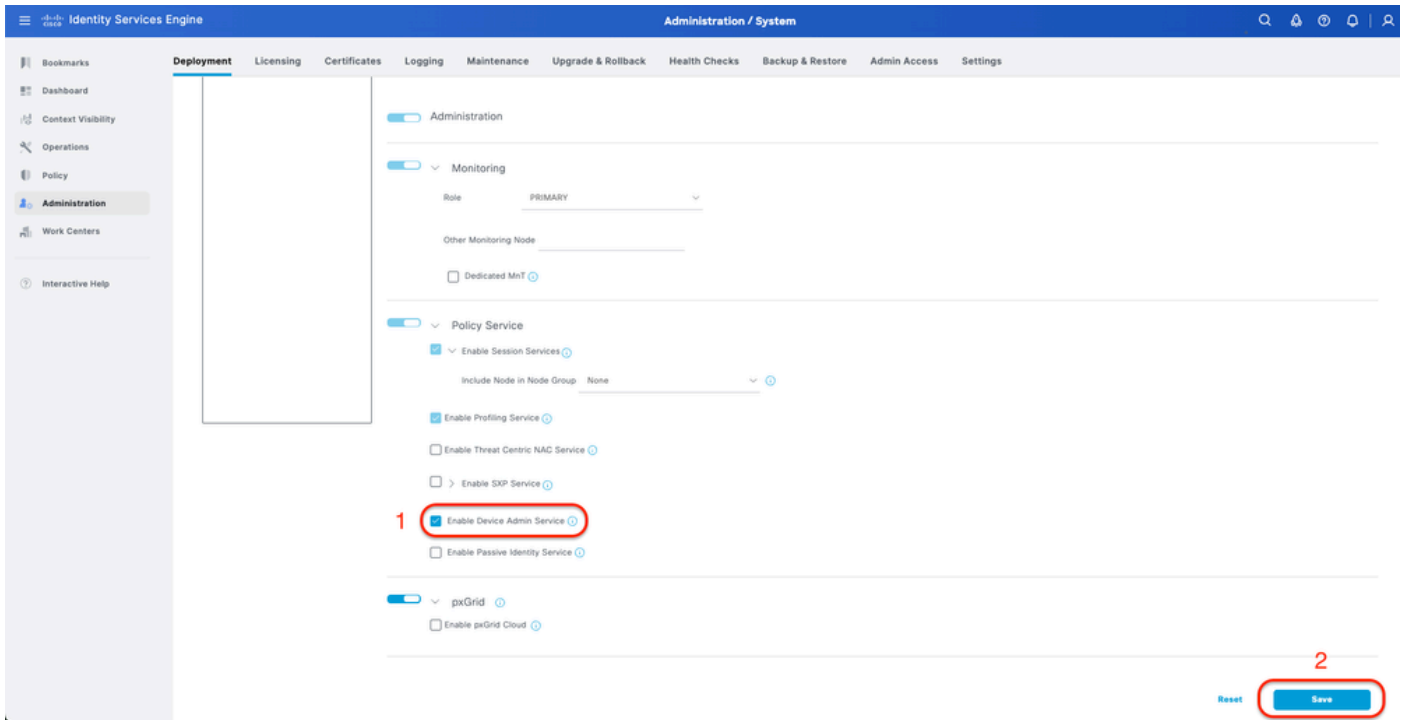


(TACACS+) 외부 인증 컨피그레이션 단계

(옵션2) TACACS+용 ISE 구성

1단계. Device Admin Service를 활성화합니다.

이 작업은 Administration(관리) > System(시스템) > Deployment(구축) > Edit (ISE PSN Node)(편집 (ISE PSN 노드)) > Enable Device Admin Service(디바이스 관리 서비스 활성화) 탭에서 수행할 수 있습니다.



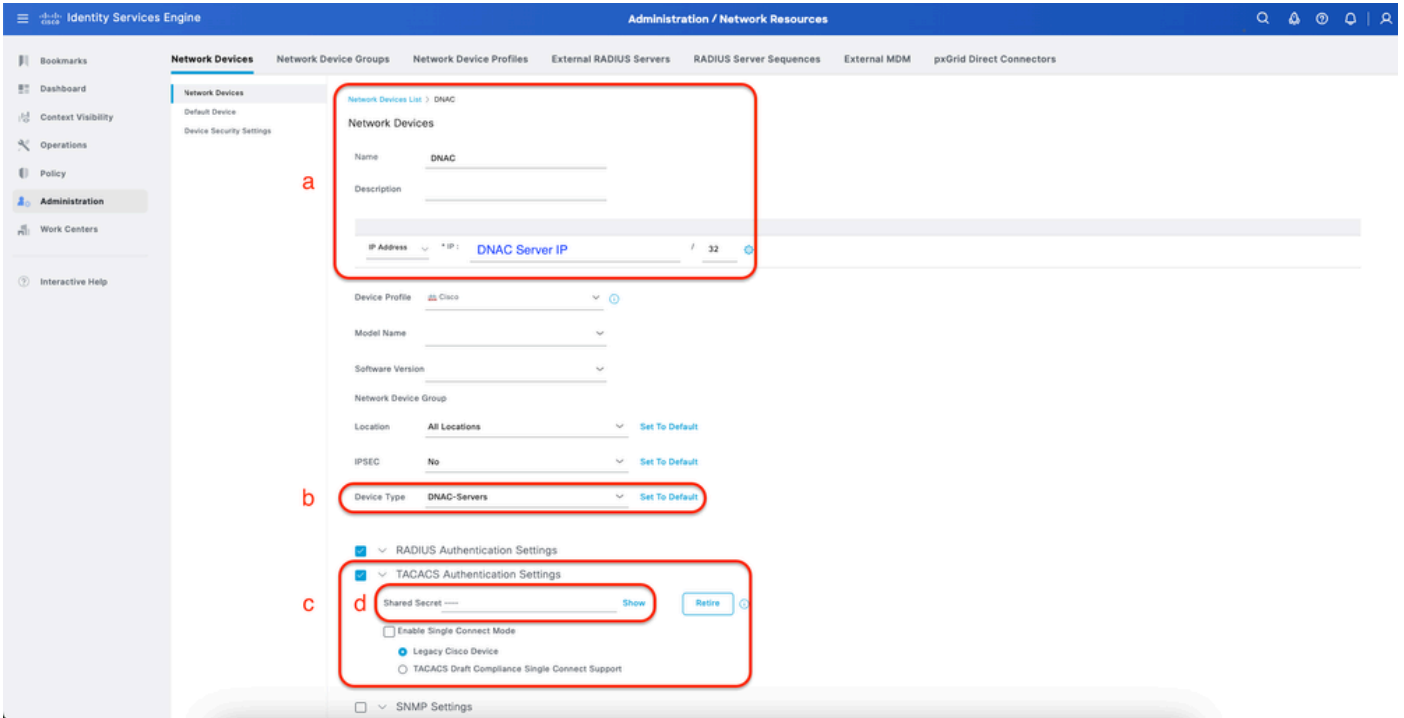
장치 관리 서비스 사용

2단계. ISE에서 DNAC 서버를 네트워크 디바이스로 추가합니다.

이 작업은 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 탭에서 수행할 수 있습니다.

절차


- a. (DNAC) 네트워크 디바이스 이름 및 IP를 정의합니다.
- b. (선택 사항) 정책 집합 조건에 대한 디바이스 유형을 분류합니다.
- c. TACACS+ 인증 설정을 활성화합니다.
- d. TACACS+ 공유 암호를 설정합니다.



TACACS+용 ISE 네트워크 디바이스(DNAC)

3단계. 각 DNAC 역할에 대한 TACACS+ 프로필을 생성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필) 탭에서 수행할 수 있습니다.

 참고: 각 사용자 역할에 하나씩 3x TACACS+ 프로필을 생성합니다.


절차

a. Add(추가)를 클릭하고 TACACS 프로필 이름을 정의합니다.

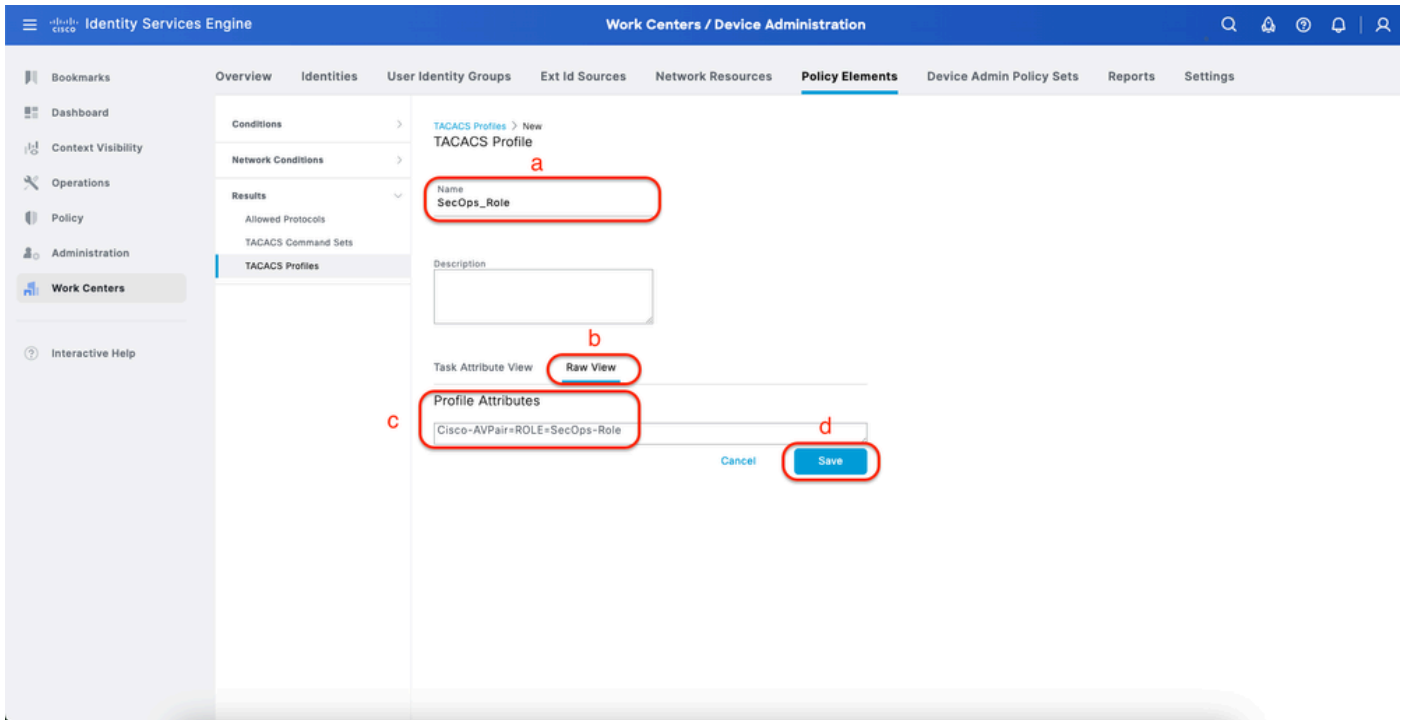
b. Raw View(원시 뷰) 탭을 클릭합니다.

c. Cisco-AVPair=ROLE=를 입력하고 올바른 사용자 역할을 입력합니다.

- (SecOps-Role) 사용자 역할에 Cisco-AVPair=ROLE=SecOps-Role을 입력합니다.
- (NETWORK-ADMIN-ROLE) 사용자 역할에 Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE을 입력합니다.
- (SUPER-ADMIN-ROLE) 사용자 역할의 경우 Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE을 입력합니다.

 참고: AVPair 값(Cisco-AVPair=ROLE=)은 대/소문자를 구분하며 DNAC 사용자 역할과 일치하는지 확인합니다.

d. 저장을 클릭합니다.



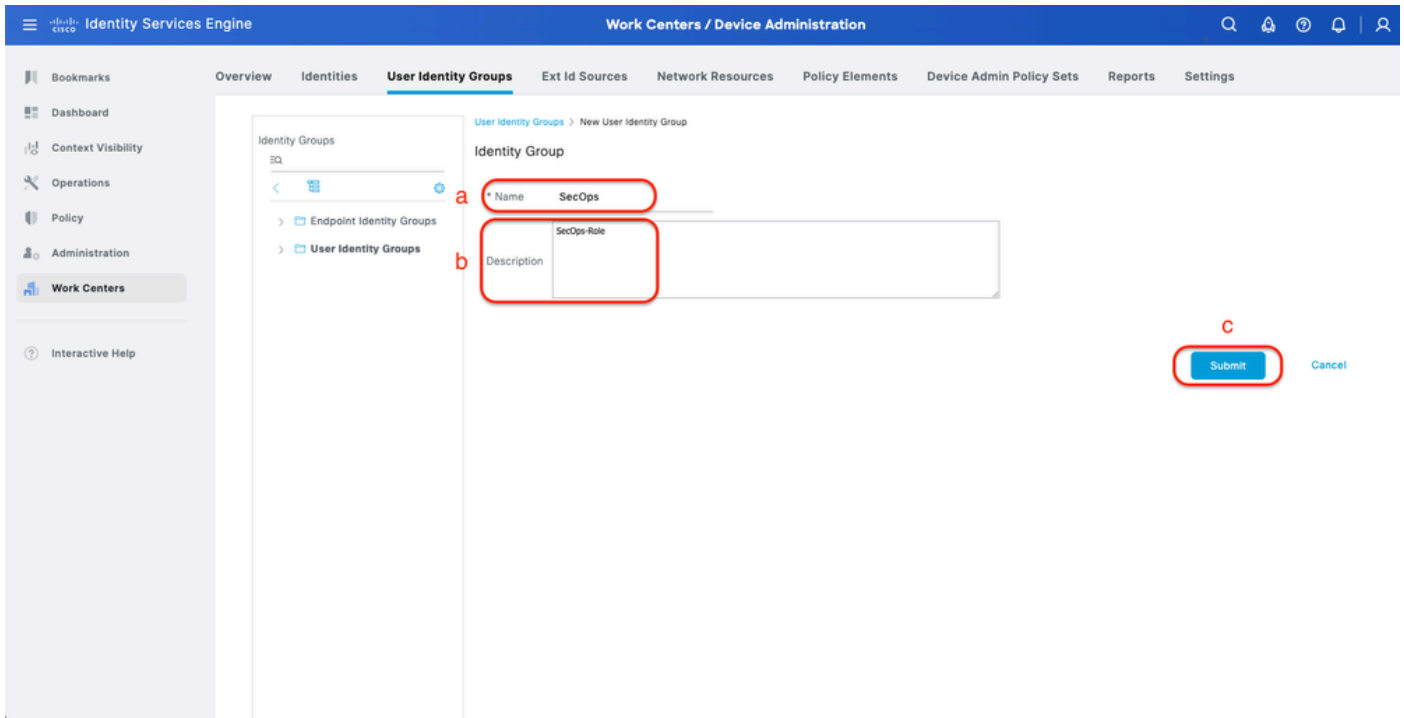
TACACS 프로파일 생성(SecOps_Role)

4단계. 사용자 그룹을 생성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > User Identity Groups(사용자 ID 그룹) 탭에서 수행할 수 있습니다.

절차

- a. Add(추가)를 클릭하고 ID 그룹 이름을 정의합니다.
- b. (선택 사항) 설명을 정의합니다.
- c. 제출을 클릭합니다.



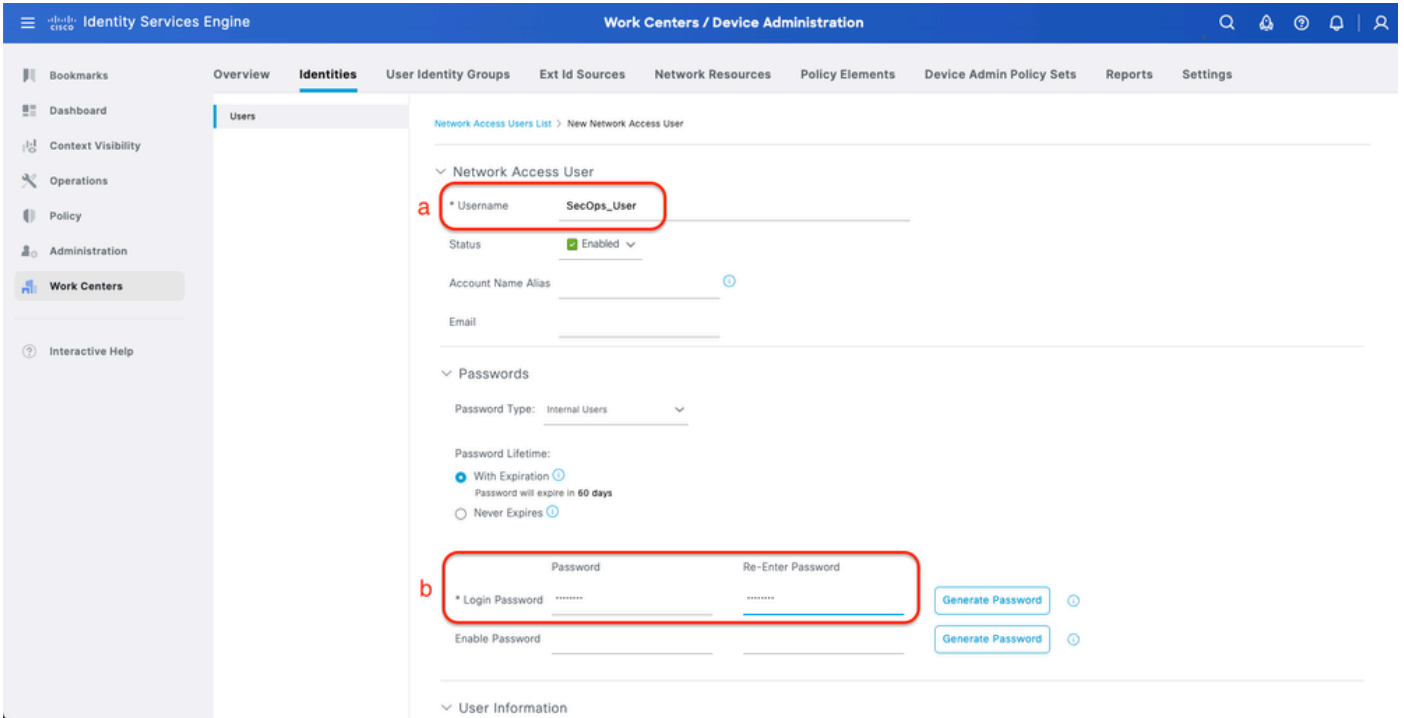
사용자 ID 그룹 생성

5단계. 로컬 사용자를 생성합니다.

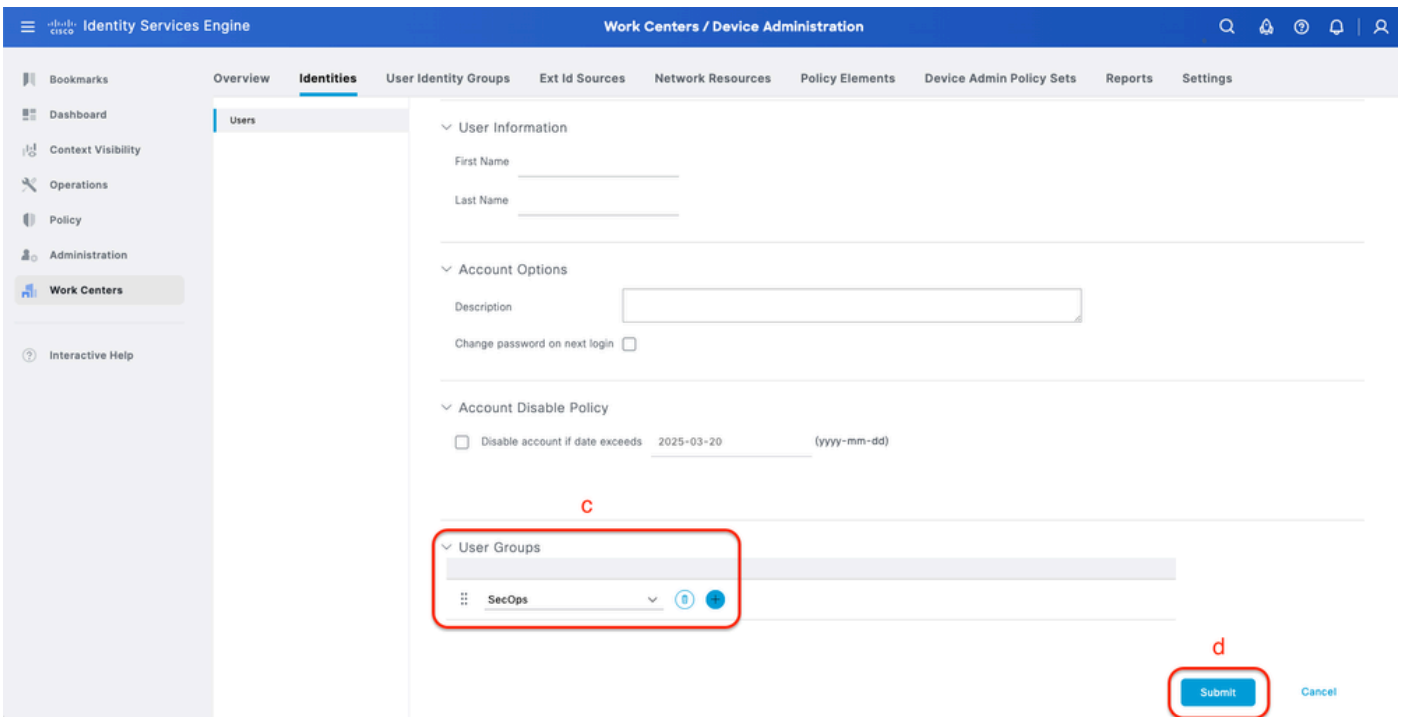
이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Identities(ID) > Users(사용자) 탭에서 수행할 수 있습니다.

절차

- a. Add(추가)를 클릭하고 Username(사용자 이름)을 정의합니다.
- b. 로그인 비밀번호를 설정합니다.
- c. 관련 사용자 그룹에 사용자를 추가합니다.
- d. Submit(제출)을 클릭합니다.



로컬 사용자 생성 1-2



로컬 사용자 생성 2-2

6단계. (선택 사항) TACACS+ 정책 집합을 추가합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) 탭에서 수행할 수 있습니다.

절차

a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

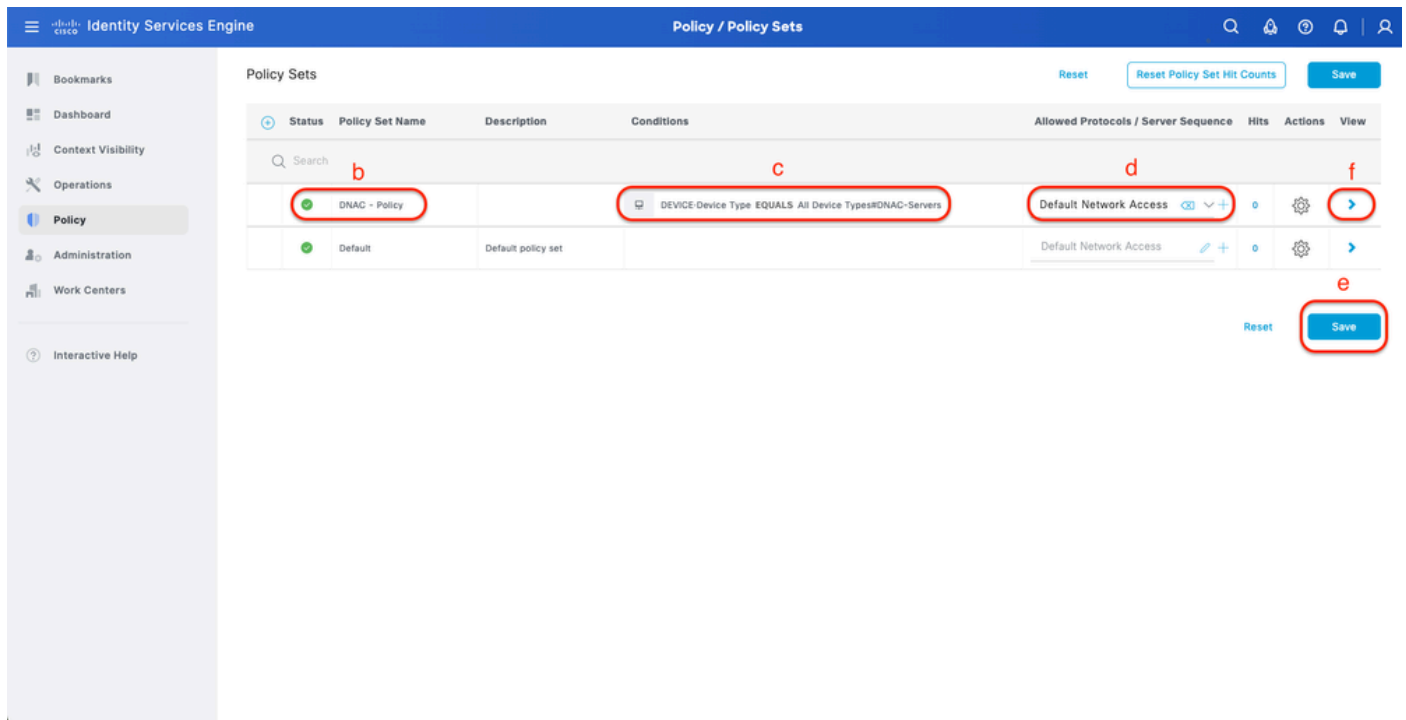
b. 정책 집합 이름을 정의합니다.

c. 이전에 생성한 Select Device Type(디바이스 유형 선택)으로 Policy Set Condition(정책 설정 조건)을 설정합니다(2단계 > b).

d. Allowed 프로토콜을 설정합니다.

e. 저장을 클릭합니다.

f. 인증 및 권한 부여 규칙을 구성하려면 (>) Policy Set View를 클릭합니다.



TACACS+ 정책 집합 추가

7단계. TACACS+ 인증 정책을 구성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) > Click(>) 탭에서 수행할 수 있습니다.

절차

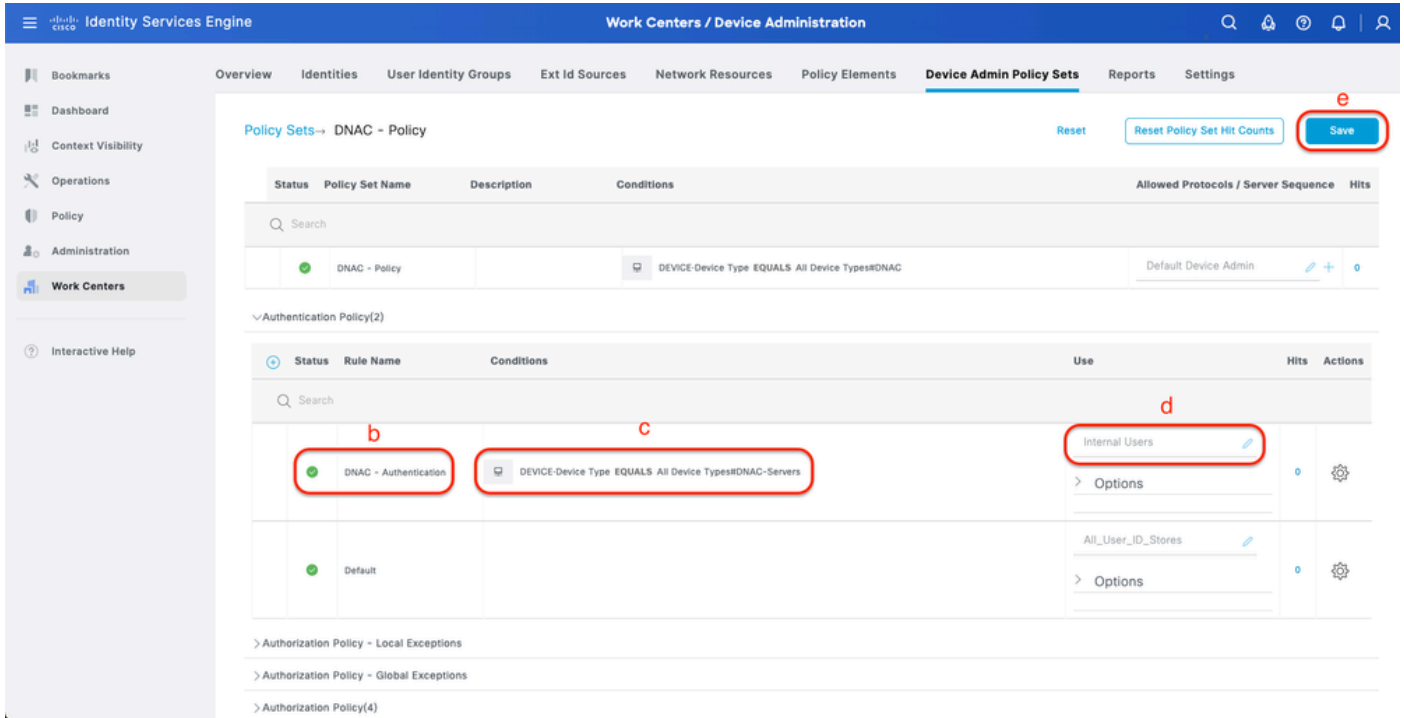
a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 인증 정책 이름을 정의 합니다.

c. Authentication Policy Condition(인증 정책 조건)을 설정하고 이전에 생성한 Device Type(디바이스 유형)을 선택합니다(2단계 > b).

d. ID 소스에 대한 인증 정책 사용을 설정합니다.

e. 저장을 클릭합니다.



TACACS+ 인증 정책 추가

8단계. TACACS+ 권한 부여 정책을 구성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) > Click (>)(클릭) 탭에서 수행할 수 있습니다.

각 사용자 역할에 대한 권한 부여 정책을 생성하려면 다음 단계를 수행합니다.

- 슈퍼 관리자 역할
- 네트워크 관리자 역할
- 보안 담당 종역

절차

a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 권한 부여 정책 이름을 정의 합니다.

c. 권한 부여 정책 조건을 설정하고(4단계)에서 생성한 사용자 그룹을 선택합니다.

d. 권한 부여 정책 셀 프로파일을 설정하고 3단계에서 생성한 TACACS 프로파일을 선택합니다.

e. 저장을 클릭합니다.

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

권한 부여 정책 추가

다음을 확인합니다.

RADIUS 컨피그레이션 확인

1- DNAC - Display External Users System(외부 사용자 표시 시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증) > External Users(외부 사용자).

RADIUS를 통해 처음 로그인한 외부 사용자 목록을 볼 수 있습니다. 표시되는 정보에는 사용자 이름 및 역할이 포함됩니다.

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)

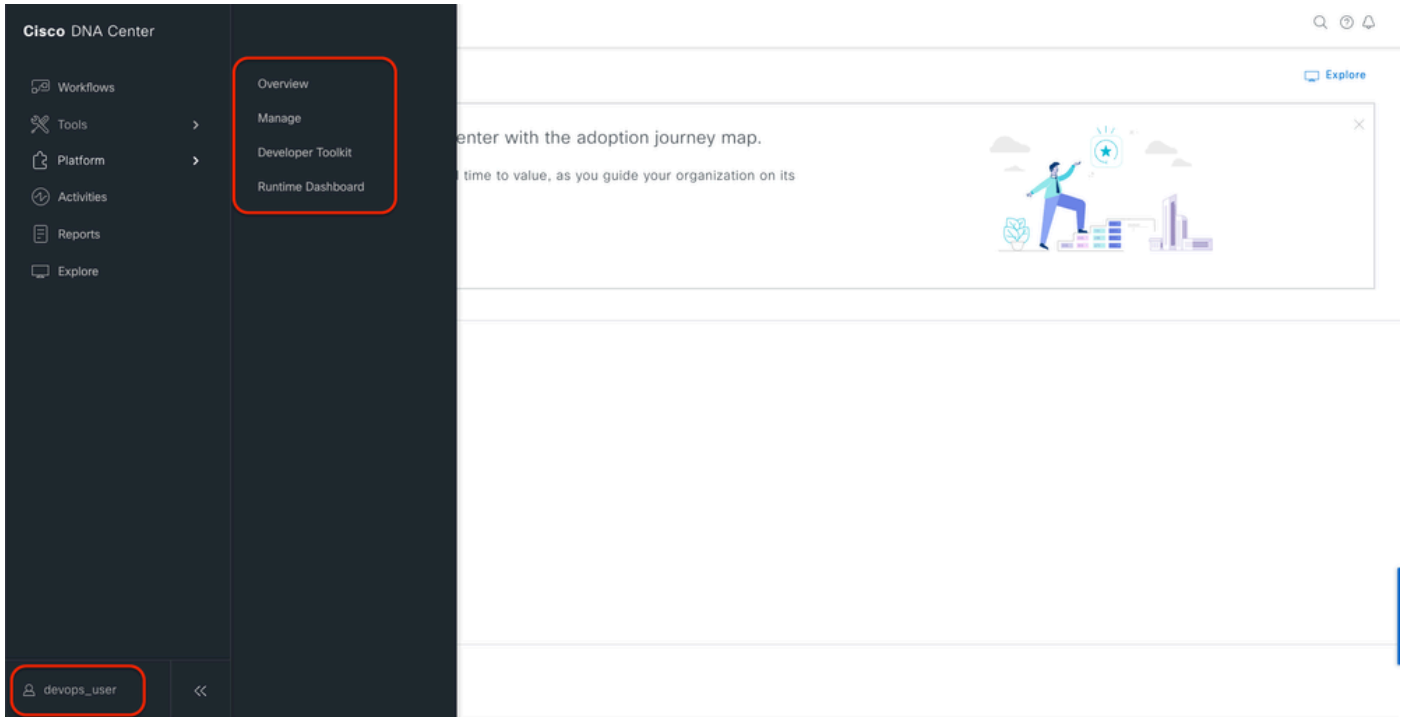
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

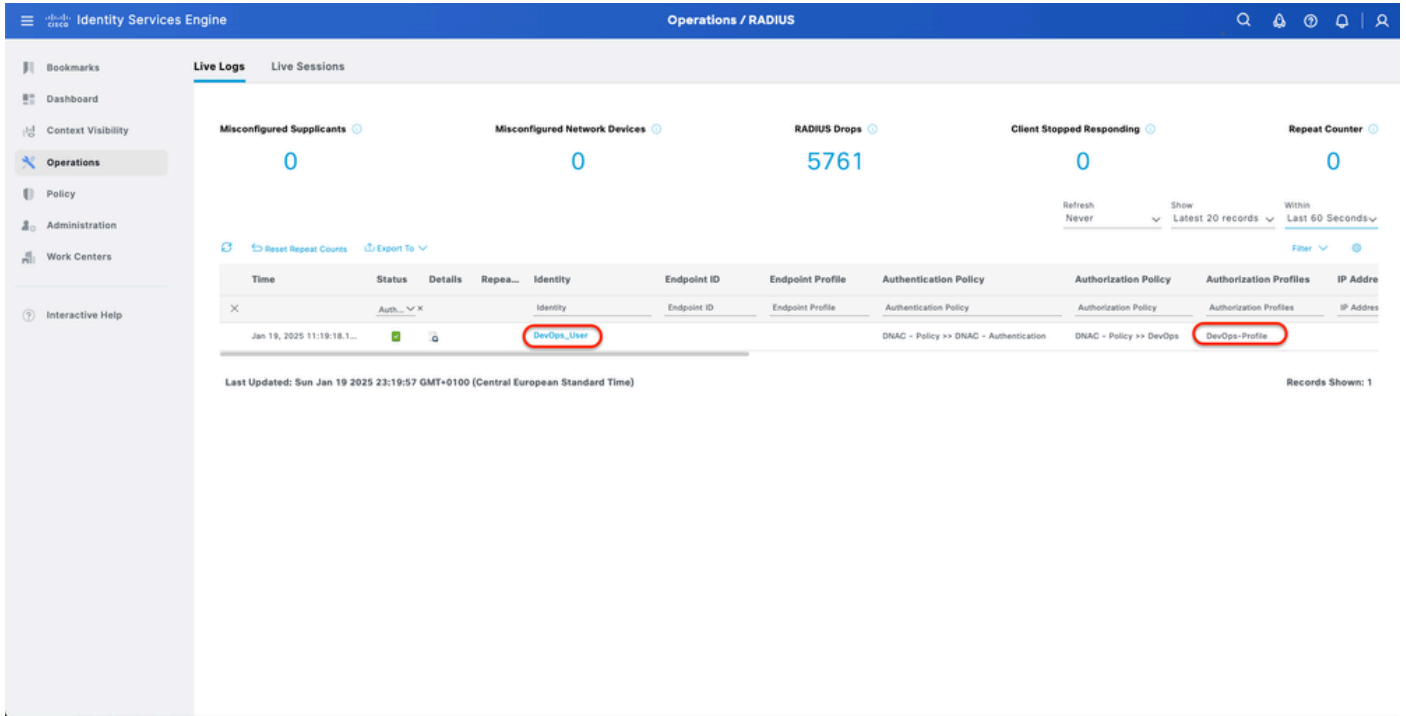
외부 사용자

2. DNAC - 사용자 액세스를 확인합니다.



제한된 사용자 액세스

3.a ISE - RADIUS Live-Logs Operations(RADIUS 라이브 로그 작업) > RADIUS > Live-Logs(라이브 로그).



RADIUS 라이브 로그

3.b ISE - RADIUS Live-Logs Operations(RADIUS 라이브 로그 작업) > RADIUS > Live-Logs(라이브 로그) > Click (Details) for Authorization log(권한 부여 로그를 클릭).

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 상세 라이브 로그 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=9b4d28083db66a1f8bcc98565c8f5ea5dedf467

Result

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

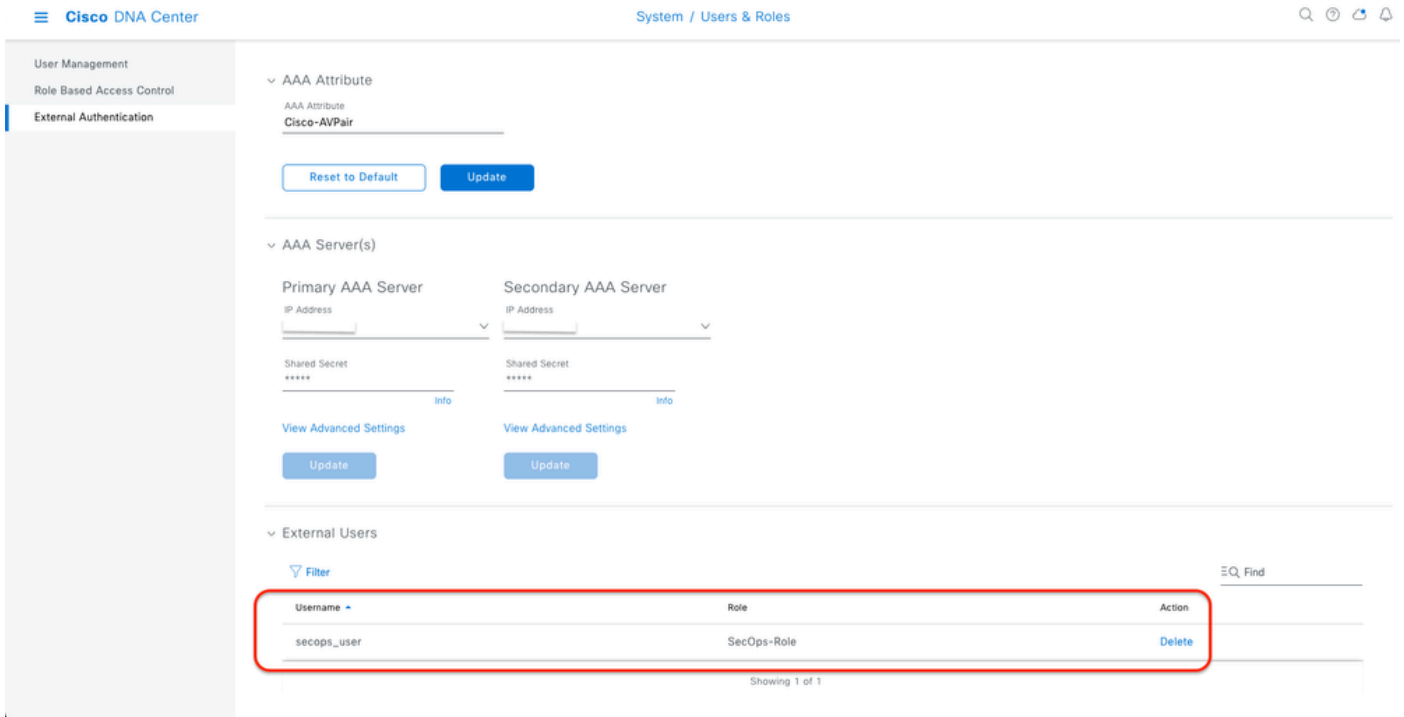
cisco-av-pair: ROLE=DevOps-Role

RADIUS 상세 라이브 로그 2-2

TACACS+ 컨피그레이션 확인

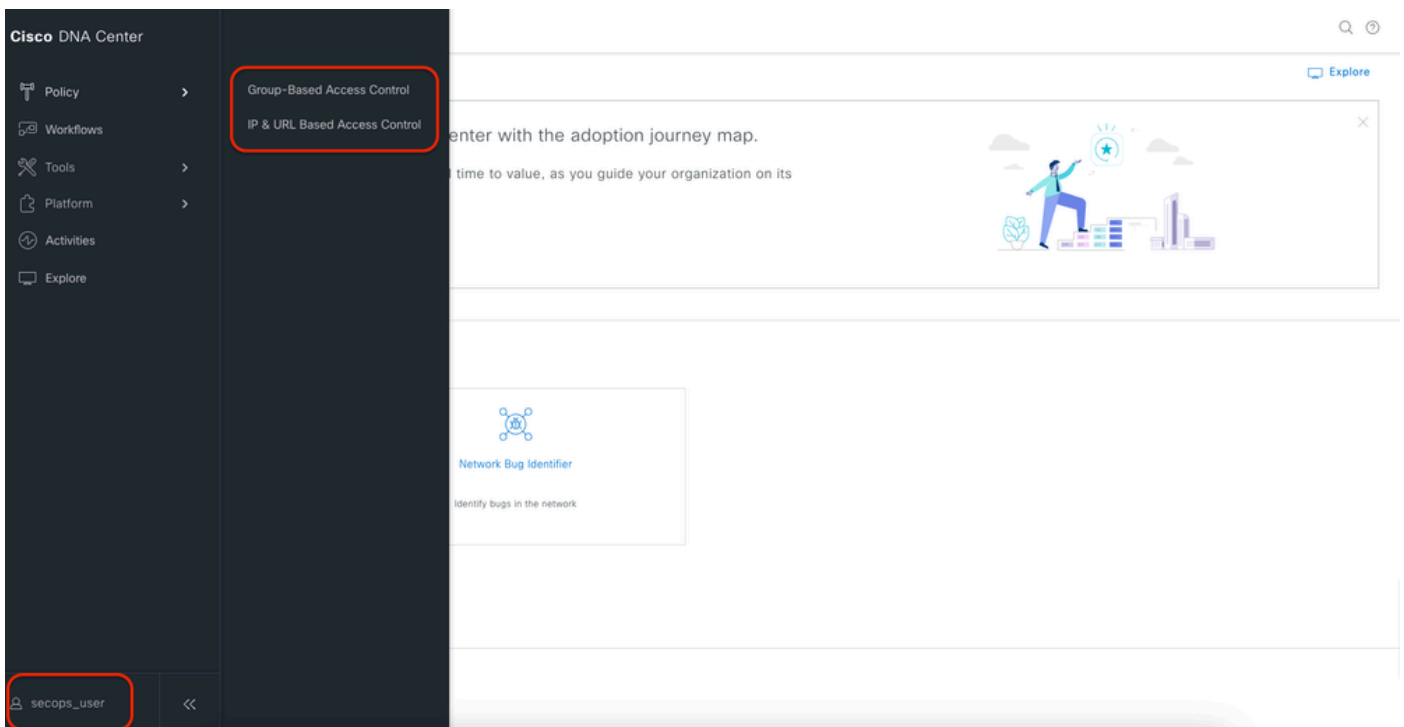
1- DNAC - Display External Users System(외부 사용자 표시 시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증) > External Users(외부 사용자).

TACACS+를 통해 처음 로그인한 외부 사용자 목록을 볼 수 있습니다. 표시되는 정보에는 사용자 이름 및 역할이 포함됩니다.



외부 사용자

2. DNAC - 사용자 액세스를 확인합니다.



제한된 사용자 액세스

3.a ISE - TACACS+ Live-Logs Work Centers(작업 센터) > Device Administration(디바이스 관리) > Overview(개요) > TACACS LiveLog(TACACS 라이브 로그).

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#All Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All Device Types#DNAC...	Lo

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

TACACS 라이브 로그

3.b ISE - 자세한 TACACS+ Live-Logs Work Centers(작업 센터) > Device Administration(디바이스 관리) > Overview(개요) > TACACS Livelog(TACACS 라이브 로그) > Click (Details) for Authorization log(권한 부여 로그 클릭)

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

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 sessions policy created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

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

TACACS+ 상세 라이브 로그 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+ 상세 라이브 로그 2-2

문제 해결

현재 이 구성에 사용할 수 있는 특정 진단 정보가 없습니다.

참조

- [Cisco Identity Services Engine 관리자 가이드, 릴리스 3.4 > 장치 관리](#)
- [Cisco DNA Center 관리자 가이드, 릴리스 2.3.5](#)
- [Cisco DNA Center: 외부 인증을 통한 역할 기반 액세스 제어](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.