ISE를 DNAC GUI용 외부 인증으로 구성

목차
<u>소개</u>
사전 요구 사항
요구 사항
사용되는 구성 요소
<u>시작하기 전에</u>
<u>구성</u>
<u>(옵션1) RADIUS를 사용하여 DNAC 외부 인증 구성</u>
<u>(옵션1) RADIUS를 위한 ISE 구성</u>
<u>(옵션2) TACACS+를 사용하여 DNAC 외부 인증 구성</u>
<u>(옵션2) TACACS+용 ISE 구성</u>
<u>다음을 확인합니다.</u>
RADIUS 컨피그레이션 확인
<u>TACACS+ 컨피그레이션 확인</u>
문제 해결
<u>참조</u>

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 거 부하는 경우 Cisco DNA Center가 로컬 사용자에게 돌아가지 않습니다. 외부 인증 폴백이 활 성화된 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 있습니 다. 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.

2

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)	_

Exit

DevOps 역할 이름

b. 액세스 권한을 정의합니다.

⊟ Cisc	o DNA Center				Create a User Role	Q @ @ \$
	Define the	e Acce	SS			
	These perm permissions	issions enabl allow. Click	e different o here to Lear	apabilities in Ci n More.	cco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these 🛛 🗙	
	Define the DevO a role is configur	ps-Role role ed with Den 1	e. Custom y permissio	roles permit or on, all related o	restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If ontent for that capability is removed from the GUI.	
	Access +	Permission			Description	
	> Assurance	O Deny	⊖ Read	() Write	Assure consistent service levels with complete visibility across all aspects of your network.	
	> Network Analytics	O Deny	O Read	O Write	Access to Network Analytics related components.	
	> Network Design	O Deny	O Read	O 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	O Deny	⊖ Read	O Write	Configure, upgrade, provision and manage your network devices.	
	> Network Services	O Deny	O Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.	
	> Platform	O Deny	Read	O Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
	> Security	O Deny	O Read	O Write	Manage and control secure access to the network.	
						2
Exit					Review Back	Next

DevOps 역할 액세스

c. 새 역할을 생성합니다.

■ Cisco DNA Center	Create a User Role	Q @ C A
Summary Review the DevOps-Role role. Make su	are 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	
v 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	Derv	
- Exit	(Back Create Role

DevOps 역할 요약

■ Cisco DNA Center		Create a User Role	Q @ & \$
Network De	vice Deliy		
Port Manag	ement Deny		
Topology	Deny		
License	Deny		
Network Telen	betry Deny		
PnP	Deny		
Provision	Deny		
NETWORK SERV	CES		
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Write		
Events	Write		
Reports	Write	J	
SECURITY			
Group-Based	Policy Deny		
IP Based Acce	ss Control Deny		
Security Advis	pries Deny		
SYSTEM			
Machine Reas	uning Deny		1
Custom Manag	nennet Daeu		
Exit		Back	Create Role

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) 확 인란을 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 확 인합니다.

■ Cisco DNA Center	System / Users & Roles	Q @ @ 4
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 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 or	Cisco DNA Center is the on Cisco DNA Center.
a b	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 attricon configuration profile would bok like "cisco-av-pairs Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the AAA attribute configuration in the case of manually defining the case of manually defining the case of manually defining the case of	ibutes list. A sample
С	Reset to Default Update AAA Server(s) Primary AAA Server P Adoress ISE Server 1 IP ISE Server 2 IP Shared Secret Shared Secret Shared Secret TACACS RADIUS TACACS RADIUS TACACS Authentication Port B12 B12 Primary AAA Server	

(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(네트워 크 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 정의 합니다.

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.

$\equiv \frac{\mathrm{dede}}{\mathrm{dec}}$ Identity Services	Engine	Policy / Policy Elements	A & @ 0 A
J Bookmarks	Dictionaries Conditions	Results	
Dashboard	Authentication \sim	Authorization Profiles 3: New Authorization Profile	
10 Context Visibility	Allowed Protocols	Authorization Profile a	
N Operations	Authorization V	* Name DevOps-Profile	
Policy	Downloadable ACLs	Description	
2. Administration	Prefiling		
H Work Centers	Posture	* Access Type ACCESS_ACCEPT V	
	Client Provisioning	Network Device Profile micro v 0	
(2) Interactive Help		Service Template	
		Track Movement	
		Passive Identity Tracking 🗋 🕜	
		> Common Tasks	
		Advanced Attributes Settings b	
		E <u>Casexcises-ex-pair</u> × <u>ROLE-DevOps-Role</u> +	
		C	
		V Attributes Details Access Type = ACCESS ACCEPT Once are grain = RGLF-toochope Raise	
		(Cancel

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.

≡	dentity Services E	Engine	Administration / Identity Management	۹	\$ 0	¢	A
н	Bookmarks	Identities Groups	s External Identity Sources Identity Source Sequences Settings				
== -년	Context Visibility	Users Latest Manual Network Sca Results	Can				
×	Operations		V Network Access User				
0	Policy		a vusename Devops_user				
20	Administration		Status 🛛 Enabled 🗸				
di.	Work Centers		Account Name Alias				
(?)	Interactive Help		Email Passwords Password Type: Internal Users Password Lifetime:				
			With Explaint © Passord with Explaint 60 days Never Expires ©				
			b Password Re-Enter Password * Login Password				
			Enable Password Generate Password 🕢				
			V User Information				
			Last Name				

로컬 사용자 생성 1-2

=	deader Identity Services i	Engine				Ac	dminist	tration / Identity Manageme	ent		۹	۵	0	٥	A
р	Bookmarks	Identities	Groups	Externa	I Identity Sources	Identity Source Sequen	ces	Settings							
部 小 り り り り り り り い り や り り り り や り り り り り	Dashboard Context Visibility Operations Policy Administration Work Centers	Users Latest Manu Results	al Network Scan		* Login Password Enable Password ~ User Informat First Name Last Name ~ Account Optic Description				Generate Password	0					
					Change password Account Disal Disable account User Groups DevOps	on next login ble Policy wr if date exceeds2025-0 C ~())3-20	(yyyy-mm-dd)			d Submr.		Ca	ncel	

로컬 사용자 생성 2-2

5단계. (선택 사항) RADIUS 정책 집합을 추가합니다.

이 작업은 Policy(정책) > Policy Sets(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(1단계 > b).

d. Allowed 프로토콜을 설정합니다.

e. 저장을 클릭합니다.

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

≡ dentity Services Engine	Policy / Policy Sets	
JI Bookmarks Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
Context Visibility Q. Search b Vd Context Visibility Image: Context Visibility V Operations Image: Context Visibility	C DEVICE Device Type EQUALS All Device TypesHDNAC-Servers	d f Default Network Access ∞ ∨ → ◎ ⊗ →
Policy Default	Default policy set	Default Network Access 🥜 🕂 o 🏟 🗲
≜_ Administration		e
I Work Centers		Reset Save
Interactive Help		

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(디바이 스 유형)을 선택합니다(1단계 > b).

d. ID 소스에 대한 인증 정책 사용을 설정합니다.

e. 저장을 클릭합니다.

≡ death Identity Services En	jine Policy / Policy Sets		۵ ۵	0	0 A
JI Bookmarks	Policy Sets-+ DNAC - Policy	Reset	Reset Policy Set Hit Counts		Save
Dashboard	Status Policy Set Name Description Conditions		Allowed Protocols / Server	Seque	ice Hits
i명 Context Visibility	Q Search				
Operations	DNAC - Policy DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers		Default Network Access	1	+ 0
& Administration					
Work Centers	 ✓ Authenocation Poice(i(z)) 				
	Status Rule Name Conditions	Use		Hits	Actions
Interactive Help	Q. Search		d		
		Internal U	Users 🌒		
	DNAC - Authentication EVICE Device Type RQUALS As Device TypesRDNAC-Servers	> Optio	ns	۰	¢
		All_User	_ID_Stores		
	Default	> Optio	ns	2	Ô
	> Authorization Policy - Local Exceptions				
	> Authorization Policy - Global Exceptions				
	> Authorization Policy(1)				
					е
			Reset		Save

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.

- 수퍼 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.

≡ dedic Identity Services En	gine	Policy / Policy Sets		
JI Bookmarks	Policy Sets -> DNAC - Policy		Reset	Reset Policy Set Hit Counts Save
E Dashboard	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
Policy	ONAC - Policy	DEVICE-Device Type EQUALS All Device TypesIIDNAC-Servers		Default Network Access 🥒 + o
Administration	> Authentication Policy(2)			
베. Work Centers	> Authorization Policy - Local Exceptions			
Interactive Help	>Authorization Policy - Global Exception ~Authorization Policy(4)	1		
	🕂 Status Rule Name	Conditions	Results Profiles Security (Groups Hits Actions
	Q Search b	с	d	a
	Super Admin	A IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr_ × + Select f	rom list 🥒 🕂 🔹 🔞
	Network Admin	A IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	(Network-Admin_Role ×) v + Select f	rom list 🥒 🔶 🏠
	O DevOps	A IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile / + Select f	rom list 🥒 🔶 🔿
	O Default		DenyAccess / + Select f	rom list 🥒 🕂 🔹 🚳
				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 있습니 다. 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.

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* SecOps-Role		
Describe the role (optional)		
		<u> </u>
		×

보안 담당 중역 역할 이름

b. 액세스 권한을 정의합니다.

≡ Cisco DNA C	enter			Create a User Role	Q @ & \$
Defin	e the Acce	ess			
(i) The per	se permissions enab nissions allow. Click	le different o here to Lear	apabilities in C n More.	isco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these 🛛 🗙	
Define th a role is o	SecOps-Role rol onfigured with Der 1	le. Custom ny permissio	roles permit o on, all related	r restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If content for that capability is removed from the GUI.	
> Net Ana	rork vtics O Deny	O Read	O Write	Access to Network Analytics related components.	
> Net Des	ork gn Oeny	○ Read	O Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.	
> Net Prov	iork 🍥 Deny	⊖ Read	 Write 	Configure, upgrade, provision and manage your network devices.	
> Net Ser	ork O Deny	○ Read	⊖ Write	Configure additional capabilities on the network beyond basic network connectivity and access.	
> Plat	orm 🍥 Deny	() Read	 Write 	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
> Sec	rity 🔿 Deny	○ Read	O Write	Manage and control secure access to the network.	
> Sys	em 💿 Deny	○ Read	O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.	
> Utili	ies 💿 Deny	Read	Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.	
					2
⊖ Exit				Review Back	Next

SecOps 역할 액세스

c. 새 역할을 생성합니다.

■ 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	
V Role Name & Description Edit	R Construction of the second se	
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	Denv	
🕣 Exit		Back Create Role

SecOps 역할 요약

■ Cisco DNA Center		Create a User Role	Q @ 4
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		1
- Exit			Back Create Role

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) 확 인란을 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 확인 합니다.



(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.

=	dealer Identity Services	Engine						Administration	/ System				۹	۵ ه	<u>ه</u>	۱ A
н	Bookmarks	Deployment	Licensing	Certificate	s Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings					
	Dashboard															
15	Context Visibility				Adm	nistration										
×	Operations															
0	Policy				— × 1	Monitoring										
80	Administration				Ro	e Pi	RIMARY	Ŷ								
ń	Work Centers				Ot	her Monitoring Node										
٢	Interactive Help] Dedicated MnT 🕡										
						olicy Service										
					2 ~	Enable Session Se	rvices 🕕									
						Include Node in No	ode Group None		~ <u>0</u>							
						this Destring Consistent										
						able Proting Service	•									
					En En	able Threat Centric P	VAC Service 🕡									
						Enable SXP Service	• • •									
					1 💷	able Device Admin 5	Service ()									
					- E	able Passive Identity	y Service 🕕									
					— , ,	oxGrid 🕕										
					En En	able pxGrid Cloud 🤇)									
														2		
												Res	•	Sav	re	D

장치 관리 서비스 사용

2단계. ISE에서 DNAC 서버를 네트워크 디바이스로 추가합니다.

이 작업은 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워 크 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(정 책 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 일치 하는지 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.

≡	abala Identity Services	Engine		Work	Centers / Device Ad	ministration			٩	۵	0	Q	A
н	Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
50	Dashboard		User Identi	ty Groups > New User Iden	ntity Group								
명	Context Visibility	Identity Groups	Identity	Group									
~%	Operations	< 18	a CName	SecOps									
-0	Policy	> 🛅 Endpoint	dentity Groups	SecOps-Role	{ ──								
20	Administration	> 🗅 User Iden	tity Groups Descrip	tion									
đ	Work Centers)								
(7)	Interactive Help								C		c	incel	

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.

≡	diale Identity Services	Engine				Work	Centers / Dev	vice Administ	tration			Q	ۍ و	Q	
Л	Bookmarks	Overview	Identities	User Identit	y Groups	Ext Id Sources	Network Reso	ources Pol	icy Elements	Device Admin Policy	Sets Reports	Settings			
53	Dashboard	Users		Netw	ork Access Users	List > New Network Ac	cess User								
15	Context Visibility														
×	Operations				Network Acc	cess User									
-0	Policy			a	Username	SecOps_User	_								
8.	Administration			S	itatus	Enabled 🗸	_								
đ	Work Centers			A	ccount Name A	lias	0								
				E	mail										
?	Interactive Help														
				~	Passwords										
					Password Type:	Internal Users	~								
					Password Lifetir	me:									
					 With Expirat 	tion 🕕									
					 Never Expire 	es 🕕									
						Password		Re-Enter Passv	vord						
				D L	* Login Passwo	rd				Generate Password	0				
					Enable Passwor	ď				Generate Password	0				
				\sim	User Inform	nation									

로컬 사용자 생성 1-2

≡	abala Identity Services	Engine			Work	Centers / Device Ad	ministration			٩	۵	0	Q	<u>م</u>
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
	Dashboard	Users		✓ User Infor	mation									
명	Context Visibility			First Name										
*	Operations			Last Name										
- 0	Policy													
8.	Administration			✓ Account C	options									
đ	Work Centers			Description										
?	Interactive Help			Change passv	vord on next login									
				✓ Account D	isable Policy									
				Disable a	account if date exceed	s 2025-03-20	(yyyy-mm-dd)							
					С									
				✓ User Grou	ps									
				II SecOp	5	<u>∽</u> 0 ●								
										d				
										Submit		Canc	el	

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.

≡	dentity Services Er	ngine		Policy / Policy Sets	Q & @ Q A
Щ	Bookmarks	Policy Sets			Reset Reset Policy Set Hit Counts Save
	Dashboard	Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
망	Context Visibility	Q Search		6	d t
*	Operations	D			
0	Policy	DNAC - Policy		H DEVICE-Device Type EQUALS All Device Types#UNAC-Servers	
8.	Administration	😨 Default	Default policy set		Default Network Access 🖉 + 🔹 🍪 🕨
di.	Work Centers				e
					Reset Save
?	Interactive Help				

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(디바이 스 유형)을 선택합니다(2단계 > b).

d. ID 소스에 대한 인증 정책 사용을 설정합니다.

e. 저장을 클릭합니다.

≡	dentity Services E	Engine Work Centers / Device Administration			٩	۵ ۵) (A A
н	Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy S	Sets	Reports	Settings			
	Dashboard		_	((<u> </u>
망	Context Visibility	Policy Sets - DINAG - Policy	Reset	Reset P	olicy Set Hit G	ounts	5:	Me
~%	Operations	Status Policy Set Name Description Conditions		Allowe	d Protocols / S	ierver Seq	ence	Hits
-0	Policy	Q Search						
8.	Administration	DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC		Defau	It Device Admi	n	0 +	0
-file	Work Centers							
		✓Authentication Policy(2)						
(?)	Interactive Help	• Status Rule Name Conditions	Use			Hit	Act	lons
		Q Search		d				
		b c	Inter	mal Users	b)		
		DNAC - Authentication DEVICE-Device Type EQUALS All Device TypesIDNAC-Servers	> 0	ptions		•	141	3
			AILU	User_ID_Store	is d			
		Default	> 0	ptions		0	44	2
		> Authorization Policy - Local Exceptions						
		> Authorization Policy - Global Exceptions						
		> Authorization Policy(4)						

```
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.

- 수퍼 관리자 역할
- 네트워크 관리자 역할
- 보안 담당 중역

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 셸 프로파일을 설정하고 3단계에서 생성한 TACACS 프로파일을 선택합니다.

e. 저장을 클릭합니다.

≡	deale Identity Services E	Engin	e				We	ork Centers / Device Ad	ministratio	n			٩	۵	0	Q A
Л	Bookmarks	Over	view	Identit	ties User Identit	y Groups	Ext Id Sources	s Network Resources	Policy Ele	ements Device Ad	min Policy Set	Reports	Settings			
	Dashboard		Q s	earch												
dia la construction de la constr	Context Visibility			0	DNAC - Policy			DEVICE-Device Type EQUAL	S All Device Typ	pes#DNAC		De	fault Device Ad	min	0	+ 0
×	Operations															
0	Policy		> Auther	tication	Policy(2)											
80	Administration		> Author	ization P	Policy - Local Exception	8										
đ	Work Centers		> Author	ization P	olicy - Global Exception	15										
			~Author	ization P	folicy(1)											
?	Interactive Help									Results						
			۲	Status	Rule Name	Condit	tions			Command Sets		Shell Profiles			Hits	Actions
			Q	Search				1								
	SUPER-ADMIN	I-ROL	.Е	•	Super Admin	8 1	dentityGroup-Name EQ	QUALS User Identity Groups:SUPER-	ADMIN	Select from list	0 +	SUPER_ADMIN	_ROLE 🛛 🐼	~+		(\$)
	NETWORK-ADMI	IN-RC	DLE	•	Network Admin	8.0	dentityGroup-Name EQ	QUALS User Identity Groups:NETWO	RK-ADMIN	Select from list	<i>e</i> +	NETWORK_AD	MIN_ROLE 🖾	<u>~</u> +		(2)
	SecOps-Rol	е		•	SecOps	8 1	dentityGroup-Name EQ	QUALS User Identity Groups:SecOps		Select from list	0 +	SecOps_Role	8	~+)		(2)
				٢	Default					DenyAllCommands	0 +	Deny All Shell P	rofile	1 +	0	{ô}
																2
														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 역 할) > External Authentication(외부 인증) > External Users(외부 사용자). RADIUS를 통해 처음 로그인한 외부 사용자 목록을 볼 수 있습니다. 표시되는 정보에는 사용자 이 름 및 역할이 포함됩니다.

	■ Cisco DNA Center	System / Users & Roles	Q @ & \$
	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 Attri 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 con	ibute here on Cisco DNA Center is the figured here on Cisco DNA Center.
1		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 speconfiguration inside Authorization profile would look like "cisco-av-paire Role=SUPER-ADMIN-ROLE".	cific AAA attributes list. A sample
		An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE:	
		 AAA Attribute AAA Attribute Cisco-AVPair 	
		Reset to Default Update	
		> AAA Server(s)	
		✓ External Users	EQ. Find
		Username • Role Action	
		devops_user DevOps-Role Delete	
		Showing 1 of 1	

2. DNAC - 사용자 액세스를 확인합니다.

Cisco DNA Center			Q ⊚ Q
Cisco DNA Center	Overview Manage Developer Toolkit Runtime Dashboard	enter with the adoption journey map. time to value, as you guide your organization on its	Q () A
요 devops_user 《			

제한된 사용자 액세스

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

≡	dentity Services	Engine		Operations / RADIUS		Q & @ Q A
н	Bookmarks	Live Logs Live Sessions				
53	Dashboard					
цы	Context Visibility	Misconfigured Supplicants 🕕	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter ()
*	Operations	0	0	5761	0	0
-0	Policy				Refresh Sh	ow Within
8.	Administration				Never 🗸 L	atest 20 records 🗸 Last 60 Seconds
đ	Work Centers	Ø ⇔Reset Repeat Counts ⊕Export To ∨				Filter 🗸 🔘
		Time Status D	Details Repea Identity	Endpoint ID Endpoint Profile	Authentication Policy Authorization Policy	Authorization Profiles IP Addre
?	Interactive Help	X AuthX	Identity	Endpoint ID Endpoint Profile	Authentication Policy Authorization Policy	Authorization Profiles IP Addres
		Jan 19, 2025 11:19:10.1 🗹 💡	a bevops_user		DNAG - Policy >> DNAG - Authentication DNAG - Policy >> DevOps	DevOps-Profile
		Last Updated: Sun Jan 19 2025 23:19:57 GM	IT+0100 (Central European Standard Time)			Records Shown: 1

RADIUS 라이브 로그

3.b ISE - RADIUS Live-Logs Operations(RADIUS 라이브 로그 작업) > RADIUS > Live-Logs(라이 브 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
Authentication Details	8
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

Steps		
Step ID	Description	Latency
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	
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 상세 라이브 로그 1-2

Cisco ISE	
IdentityPolicyMatchedRule	DNAC - Authentication
AuthorizationPolicyMatchedR ule	DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedRule	DNAC - Authentication
TotalAuthenLatency	35
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device TypeIIAII Device TypesIIDNAC-Servers
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:DevOps
EnableFlag	Enabled
RADIUS Username	DevOps_User
Device IP Address	
CPMSession/D	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
CiscoAVPair	AuthenticationidentityStore=Internal Users, FQS-bigetName=9273403-Rc01-11e6-996c- 52540044851946wops_user, UniqueSubjectID=9b4d28083db66a118bcc98565c8f5eaa5de df467
Result	
Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R t6/WY:ise34/526427220/15433
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 역 할) > External Authentication(외부 인증) > External Users(외부 사용자). TACACS+를 통해 처음 로그인한 외부 사용자 목록을 볼 수 있습니다. 표시되는 정보에는 사용자 이 름 및 역할이 포함됩니다.

■ Cisco DNA Center		System / Users & Roles		Q @ 🛎 Q
User Management Role Based Access Control External Authentication	 AAA Attribute AAA Attribute Cisco-AVPair Reset to Default Update 			
	AAA Server(s) Primary AAA Server PAdress PAdress Shared Secret Shared Secret Info View Advanced Settings Vie Update	address		
	 ✓ External Users ✓ Filter Username - secops_user 	Role SecOps-Role	Action Delete	Q Find
		Showing 1 or 1		

외부 사용자

2. DNAC - 사용자 액세스를 확인합니다.

Cisco DNA Center			Q (0)
⁸ ∰ Policy	Group-Based Access Control		C Explore
- Workflows	IP & URL Based Access Control	enter with the adoption journey map.	×
🕺 Tools		time to value, as you guide your organization on its	
Platform			
Activities			
Explore			
		Retwork Bug Identifier Identify bugs in the network	
요 secops_user			

제한된 사용자 액세스

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

≡	abalic Identity Services	Engine					Operat	ions / TACACS			Q	۵ 🕼	¢	A
Л	Bookmarks	Live Lo	js											
	Dashboard													
pla o	Context Visibility								Refres	h	Show	Within		
*	Operations								Neve	r v	Latest 20 records	/ Last 60	Second	ds√
0	Policy	-	う 🍈 Export To 🗸									Filter	~ 4	5
8.	Administration		Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
đ	Work Centers	>	<	×		Identity	Š	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
			Jan 19, 2025 05:12:4		0	SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All De	vice Types#C	NAC	Loc
(?)	Interactive Help	1	Jan 19, 2025 05:12:4	25 17:16:38 (Q	SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All De	vice TypesIIC Record	NAC	Loc
			st opdated. Suit Sait 192	25 17.10.30	am 1+0100	(central curoper	in Standard Time)					Record	s onown	

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		Steps		
Request Type	Authorization	Step ID	Description	Latency (ms)
Statue	Date	13005	Received TACACS+ Authorization Request	
010103		15049	Evaluating Policy Group	1
Session Key	ise34/526427220/13958	15008	Evaluating Service Selection Policy	1
Message Text	Device-Administration: Session Authorization succeeded	15048	Queried PIP - DEVICE.Device Type	4
Username	SecOps User	15041	Evaluating Identity Policy	7
		15013	Selected Identity Source - Internal Users	5
Authorization Policy	DNAC - Policy >> SecOps	24210	Looking up User in Internal Users IDStore	1
Shell Profile	SecOps_Role	24212	Found User in Internal Users IDStore	4
Matched Command Set		22037	Authentication Passed	0
		15036	Evaluating Authorization Policy	0
Command From Device		15048	Queried PIP - Network Access.UserName	10
		15048	Queried PIP - IdentityGroup.Name	2
		15017	Selected Shell Profile	2
uthorization Details		22081	Max sessions policy passed	1
Generated Time	2025-01-19 17:12:43 368 +1:00	22080	New accounting session created in Session cache	0
		13034	Returned TACACS+ Authorization Reply	•
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

Cisco ISE	
1350	riteriorization
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
SelectedAuthenticationIdentit yStores	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 3=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+ 상세 라이브 로그 2-2

문제 해결

현재 이 구성에 사용할 수 있는 특정 진단 정보가 없습니다.

참조

- <u>Cisco Identity Services Engine 관리자 가이드, 릴리스 3.4 > 장치 관리</u>
- <u>Cisco DNA Center 관리자 가이드, 릴리스 2.3.5</u>
- <u>Cisco DNA Center: 외부 인증을 통한 역할 기반 액세스 제어</u>

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 번 역 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.