Configure ISE as an External Authentication for DNAC GUI

Contents

Introduction							
<u>Prerequisites</u>							
Requirements							
Components Used							
Before you begin							
Configure							
(Option1) Configure DNAC External Authentication Using RADIUS							
(Option1) Configure ISE for RADIUS							
(Option2) Configure DNAC External Authentication Using TACACS+							
(Option2) Configure ISE for TACACS+							
Verify							
Verify RADIUS Configuration							
Verify TACACS+ Configuration							
<u>References</u>							

Introduction

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

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

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

Components Used

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

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

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

Before you begin

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

Note,

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

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

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

Configure

(Option1) Configure DNAC External Authentication Using RADIUS

Step 1. (Optional) Define a Custom Roles.

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

Procedure

a. Create a New Role



b. Define the Access

⊟ Cisc	o DNA Center				Create a User Role	Q @ & \$
	Define the These permi- permissions Define the DevO a role is configure	e Acce issions enabl allow. Click I ps-Role role ed with Den 1	e different c here to Lear e. Custom r y permissio	apabilities in Cis n More. roles permit or on, all related c	co DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these 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 - > Assurance > Network Analytics	Permission Deny Deny	ReadRead	O Write	Description Assure consistent service levels with complete visibility across all aspects of your network. Access to Network Analytics related components.	
	> Network Design	O Deny	O 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	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	() Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
	> Security	O Deny	() Read	O Write	Manage and control secure access to the network.	
€ Exit					Review Back	2 Next

DevOps Role Access

c. Create the New Role

■ Cisco DNA Center	Create a User Role	Q @ @ \$
Summary Review the DevOps-Role role. A ~ Role Name & Description Role Name DevOps-Re	Aake 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 Edit	
Role Description		
v 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	Denv	
- Exit	Back	Create Role

DevOps Role Summary

≡ Cisco	DNA Center		Create a User Role	Q @ & 4
	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		1
	Custom Management	Danu		
Exit				Back Create Role

Review and Create DevOps Role

Step 2. Configure External Authentication Using RADIUS This can be done from the tab **System > Users & Roles > External Authentication**.

Procedure

a. To enable external authentication in Cisco DNA Center, check the Enable External User check box.

b. Set the AAA attributes.

Enter Cisco-AVPair in the AAA attributes field.

c. (Optional) Configure Primary and Secondary AAA Server.

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

≡ Cisco DNA Center	System / Users & Roles	Q @ C 4				
User Management	External Authentication					
Role Based Access Control	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 Cis name of the AAA attribute chosen on the AAA attribute, it needs to be configured here on it of the AAA attribute chosen on the AAA attribute. 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 it of the AAA attribute chosen on the AAA attribute.	.co DNA Center is the Cisco DNA Center.				
External Authentication	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 attribute	tes list. A sample				
	configuration inside Authorization profile would look like "cisco-av-pair≋ Role=SUPER-ADMIN-ROLE".					
а						
b AAA Attribute AAA Attribute Cisco-AVPair						
	Reset to Default Update					
c						

(RADIUS) External Authentication Configuration Steps

(Option1) Configure ISE for RADIUS

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

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

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



ISE Network Device (DNAC) for RADIUS

Step 2. Create RADIUS Authorization Profiles

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

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

Procedure

a. Click Add and define the RADIUS Authorization Profile name

b. Enter the Cisco:cisco-av-pair in the Advanced Attributes Settings and fill the correct User role

- For the (DecOps-Role) user role, enter **ROLE=DevOps-Role**
- For the (NETWORK-ADMIN-ROLE) user role, enter **ROLE=NETWORK-ADMIN-ROLE**
- For the(SUPER-ADMIN-ROLE) user role, enter **ROLE=SUPER-ADMIN-ROLE**
- c. Review the Attribute Details
- d. Click Save

$\equiv \frac{\mathrm{dede}}{\mathrm{dscs}}$ Identity Services	Engine	Policy / Policy Elements	
JI Bookmarks	Dictionaries Conditions	Results	
E Dashboard	Authentication	Authorization Profiles 3 New Authorization Profile	
10 Context Visibility	Allowed Protocols	Authorization Profile a	
N Operations	Authorization ~	* Name DevOps-Profile	
Policy	Downloadable ACLs	Description	
≜ _○ Administration	Profiling		
Work Centers	Pesture	* Access Type ACCESS_ACCEPT V	
8	Client Provisioning	Network Device Profile 🗰 Crace 🗸 🖗	
Tuteractive resp		Service Template Task Movement O Agentiess Posture O Passive Identity Tracking O F Common Tasks Advanced Attributes Settings	
			Cl Submit Cancel

Create Authorization Profile

Step 3. Create User Group

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

Procedure

a. Click Add and define the Identity Group name

b. (Optional) Define the Description

c. Click Submit



Create User Identity Group

Step 4. Create Local User

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

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

≡	dentity Services i	Engine		Administration / Identity Management	Q	۵ (စင	9 S
н	Bookmarks	Identities Groups	External Id	entity Sources Identity Source Sequences Settings				
15	Dashboard Context Visibility	Users Latest Manual Network Scan Results		Network Access Users List > New Network Access User				
*	Operations			V Network Access User				
0	Policy		a	Status Enabled V				
1	Work Centers			Account Name Alias				
(?)	Interactive Help			Email				
				Passwords Descent Time: Investigation				
				Password Lifelime:				
				With Expiration ① Passard will expire to 60 days New re Expires ③				
			. (Password Re-Enter Password				
			b	* Login Password				
				Enable Password Generate Password 💿				
				✓ User Information				
				First Name				
				Last name				

Create Local User 1-2

≡	official identity Services E	Engine				A	dministratie	on / Identity Mar	nageme	nt			E II.	۹	۵	0	¢	A
Л	Bookmarks	Identities	Groups	Extern	al Identity Sources	Identity Source Sequen	ices Sett	ings										
	Dashboard	Users Latest Mary	ual Network Scan		* Login Password					Generate Password	0							
*	Operations	Results			Enable Password					Generate Password	0							
0	Policy				✓ User Informat	ion												
80	Administration				First Name													
4	Work Centers				Last Name													
(?)	Interactive Help				 Account Option Change password 	ons												
					Account Disa Disable account	ble Policy unt if date exceeds 2025-0	03-20	(yyyy-mm-d	id)									
					 ✓ User Groups Ⅲ DevOps 	с (б												
														d Submit		Car	icel	

Create Local User 2-2

Step 5. (Optional) Add RADIUS Policy Set

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

- a. Click Actions and choose (Insert new row above)
- b. Define the Policy Set name

- c. Set the Policy Set **Condition** to **Select** Device Type you created previously on (Step1 > b)
- d. Set the Allowed protocols

e. Click Save

f. Click (>) Policy Set View to configure authentication and authorization rules

=	deale Identity Services Engine	ne	Policy / Policy Sets	Q & @ Q A
н	Bookmarks	Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
-id	Context Visibility	Q Search b	C DEVICE-Device Type EQUALS All Device TypesIIDIAAC-Servers	d f Default Network Access @ ∨+) ø ⊗ (♪)
*	Operations Policy	C Default	Default policy set	Default Network Access 🖉 + o 🎄 >
а. -П	Administration Work Centers			Reset
(?)	Interactive Help			_

Add RADIUS Policy Set

Step 6. Configure RADIUS Authentication Policy

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

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

≡	dentity Services Eng	ine Policy / Policy Sets		۵ ۵	0	Q	۹
н	Bookmarks	Policy Sets→ DNAC - Policy	Reset	Reset Policy Set Hit Counts		Save	
	Dashboard	Status Policy Set Name Description Conditions		Allowed Protocols / Serve	r Seque	nce Hit	5
명	Context Visibility	Q, Search					
~	Operations	DNAC - Pulicy DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers		Default Network Access		+ 0	
	Policy						
A.,	Administration	✓Authentication Policy(2)					
-file	Work Centers	Status Rule Name Conditions	Use		Hits	Actions	
?	Interactive Help	Q, Search		d			
		DNAC - Authentication C DEVICE Device Type EQUALS All Device TypesBONAC-Servers	> Opti	Users	۰	¢	
		Default	All_Use > Opti	r_JD_Stores /	2	ŵ	
		> Authorization Policy - Local Exceptions					
		>Authorization Policy - Global Exceptions					
		>Authorization Policy(1)					
				Reset	(e Save	D

Add RADIUS Authentication Policy

Step 7. Configure RADIUS Authorization Policy

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

This step to create Authorization Policy for each User Role.

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

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

\equiv $\frac{\mathrm{obselv}}{\mathrm{cisco}}$ identity Servic	es Engine	Policy / Policy Sets		
J Bookmarks	Policy Sets -> DNAC - Policy		Reset	Reset Policy Set Hit Counts Save
E Dashboard Id Context Visibility	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
% OperationsPolicy	OnAC - Policy	DEVICE Device Type EQUALS AIL Device TypesHDNAC-S	ervers	Default Network Access 🥒 🕂 🗴
2. Administration	>Authentication Policy(2)			
Work Centers	> Authorization Policy - Local Exception:	1		
Interactive Help	>Authorization Policy - Global Exception	15		
			Results	
	🕒 Status Rule Name	Conditions	Profiles Secu	rity Groups Hits Actions
	Q Search b	С	d	а
	Super Admin	R IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr × V+ Sel	lect from list 🥒 🕂 🔹 🕼
	Network Admin	向。 identityGroup-Name EQUALS User identity Groups:NETWORK-ADMIN	Network-Admin_Role × + Set	lect from list 🥒 + 🔹 🚳
	DevOps	R IdentityGroup Name EQUALS User Identity Groups:DevOps	DevOps-Profile 0 + Set	lect from list 🥒 🔶
	O Default		DenyAccess 🥒 + Seb	lect from list 🥒 🕂 🔹 🚳
				е
				Reset

Add Authorization Policy

(Option2) Configure DNAC External Authentication Using TACACS+

Step 1. (Optional) Define a Custom Roles.

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

Procedure

a. Create a New Role

≡ Cisco DNA Center	Create a User Role	Q @ & A
Create a New Role Define the name of the role, and then provide an optional description. To make it	t easier to assign roles down the road, describe the role as clearly as possible.	2
⊖ Exit		Next

b. Define the Access

⊟ Cise	o DNA Center				Create a User Role	Q @ 4
	Define th	e Acce	SS			
	These perm permission	nissions enab s allow. Click	e different o here to Lear	apabilities in C m More.	is co DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these $ imes$	
	Define the SecO a role is configur	ps-Role role red with Den 1	e. Custom y 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.	
	> Network Analytics	O Deny	O Read	O Write	Access to Network Analytics related components.	
	> Network Design	O 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	O Deny	O Read	 Write 	Configure, upgrade, provision and manage your network devices.	
	> Network Services	O Deny	⊖ Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.	
	> Platform	O Deny	○ Read	 Write 	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
	> Security	O Deny	○ Read	O Write	Manage and control secure access to the network.	
	> System	O Deny	O Read	O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.	
	> Utilities	O Deny	Read	Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.	
						2
Exit					Review Back	Next

SecOps Role Access

c. Create the New Role

⊟ Cisc	o DNA Center		Create a User Role		Q @ @ \$
	Summary Review the SecOps-Role role Make s	ure 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	Denv			
Exit				Back	Create Role
L					

SecOps Role Summary

■ Cisco DNA Center		Create a User Role	Q @ C 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

Review and Create SecOps Role

Step 2. Configure External Authentication Using TACACS+ This can be done from the tab **System > Users & Roles > External Authentication**.

a. To enable external authentication in Cisco DNA Center, check the Enable External User check box.

b. Set the AAA attributes.

Enter Cisco-AVPair in the AAA attributes field.

c. (Optional) Configure Primary and Secondary AAA Server.

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

■ Cisco DNA Center	System / Users & Roles	Q @ @ \$
User Management Role Based Access Control	External Authentication Gisco 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 is needs to be con-	ribute here on Cisco DNA Center is the
External Authentication a b	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 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". C AAA Attribute C AAA Attribute C AAA Attribute C AAA Attribute C AAA Attribute C AAA Attribute C Astribute C AAA Attribute C AAAA Attribute C AAA Attribute C AAAA Attribute C AAAAA Attribute C AAAAAATTRIBUTE C AAAAAATTRIBUTE C AAAAAATTRIBUTE C AAAAATTRIBUTE C AAAATTRIBUTE C AAAATTRIBUTE C AAAATTRIBUTE C AAAATTRIBUTE C AAAAATTRIBUTE C AAAATTRIBUTE C AAAAATTRIBUTE C AAAAATTRIBUTE C AAAATTRIBUTE C AA	nfigured here on Cisco DNA Center. ecific AAA attributes list. A sample
С	~ AAA Server(s) Primary AAA Server P Address ISE Server 1 IP Shared Secret Info Shared Secret Info Hide Advanced Settings RADIUS O TACACS Port 49	

(TACACS+) External Authentication Configuration Steps

(Option2) Configure ISE for TACACS+

Step 1. Enable Device Admin Service

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

Ξ	dealer Identity Services	Engine						Administration	/ System				۹	\$ 0	Q	۹
н	Bookmarks	Deployme	nt Licensing	Certificate	ts Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings					
	Dashboard				Adm	eletration										
18	Context Visibility				Adm	matration										
	Bolicy				— • 1	Monitoring										
	Administration				Ro	le P	RIMARY	v								
-	Work Centers															
					Ot	her Monitoring Node										
٢	Interactive Help				C	Dedicated MnT (
						Policy Service										
					2 ×	Enable Session Se	rvices 🕡									
						Include Node in No	ode Group None		~ 0							
					E Fr	able Profiling Service										
					0.5	ship Threat Contrict	VAC Service O									
						Enable SXP Servic	•0									
					1 💷	nable Device Admin :	Service 🕕									
					- E	nable Passive Identit	y Service 🕕									
						w Grid O										
					- EF	able pxGrid Cloud (
														2		
															_	
												Reset	L	Save)

Enable Device Admin Service

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

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

Procedure

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

≡ dealer Identity Services Engine Administration / Network Resources	Q & @ Q A
JI Bookmarks Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors	
E Dashboard Vetwork Devices Vision (in), Prior	
hig Context Visibility Defeet Notions to Device Notions to Device	
Overations Device Security Sec	
Name DRAC	
a Description	
A ANIMALIZION	
Work Centers PAtters PAtters (32 0)	
© Interactive Help Device Profile ₫0.0xo ∨ ○	
Model Name V	
Software Version	
Network Device Group	
Location All Locations V Set To Default	
IPSEC No Set To Default	
D Orvice Type DNAC-Servers 🗠 Set To Default	
RADIUS Authentication Settings	
TACACS Authentication Settings	
C d Shared Secret Show Retire C	
Chable Single Connect Mode	
Legary Cisco Device	
○ TACACS Draft Compliance Single Connect Support	
SIMP Settings	

ISE Network Device (DNAC) for TACACS+

Step 3. Create TACACS+ Profiles for each DNAC role

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

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

Procedure

- a. Click Add and define the TACACS Profile name
- b. Click the Raw View tab

c. Enter the Cisco-AVPair=ROLE= and fill the correct User role

- For the (SecOps-Role) user role, enter Cisco-AVPair=ROLE=SecOps-Role
- For the (NETWORK-ADMIN-ROLE) user role, enter Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE
- For the(SUPER-ADMIN-ROLE) user role, enter Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE

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

d. Click Save

≡	dentity Services I	Engine				Work	Centers / Device Ad	ministration			٩	۵	0	۵	R
Д	Bookmarks	Overview	Identities	Use	r Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
5	Dashboard	Conditions		>	TACACS Profiles >	New									
망	Context Visibility	Network Co	anditions	>	TACACS Profi	a									
*	Operations	Results		÷	Name SecOps_Role										
. U.	Administration	TACACS	Protocols Command Sets												
1	Work Centers	TACACS	Profiles		Description										
a l	Interactive Help			С	Task Attribute Vie Profile Attribu Cisco-AVPair=R	b Raw View tes IOLE=SecOps-Role	Cancel	d Save							

Create TACACS Profile (SecOps_Role)

Step 4. Create User Group

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

- a. Click \boldsymbol{Add} and define the Identity Group name
- b. (Optional) Define the Description
- c. Click Submit

≡	dentity Services	Engine		Work	Centers / Device Adr	ministration		Ē	٩	۵	0	φI	8
Л	Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
51	Dashboard		User Identi	ty Groups > New User Ide	ntity Group								
1d	Context Visibility	Identity Groups	Identity	Group									
×	Operations	< 1	a Name	SecOps									
0	Policy	> 🛅 Endpoint	Identity Groups	SecOps-Role	<──								
20	Administration	> 🛅 User Ider	tity Groups b Descrip	ation									
đ	Work Centers				J								
•	Interactive Help								C		Can	cel	

Step 5. Create Local User

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

Procedure

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

d. Click Submit

≡	dentity Services	Engine				Work	Centers / De	evice Adm	inistration				٩	۵	0	۵	۹
Л	Bookmarks	Overview	Identities	User Iden	tity Groups	Ext Id Sources	Network Res	sources	Policy Elements	Device A	dmin Policy Se	ts Reports	Settings				
5	Dashboard	Users		N	etwork Access User	s List > New Network Ac	cess User										
명	Context Visibility																
- %	Operations				Network Ac	cess User											
-0	Policy			a	* Username	SecOps_User	J										
8.	Administration				Status	Z Enabled 🗸											
đ	Work Centers				Account Name	Alias	0	0									
?	Interactive Help				Email												
					 Passwords Password Type 	: Internal Users	~										
					Password Lifet	ime:											
					 With Expiration Password w 	ition ① Ill expire in 60 days											
					O Never Expl	res 🛈											
				b		Password		Re-Enter I	Password								
				~	* Login Passw	ord				Genera	te Password	0					
					Enable Passwo	rd				Genera	ate Password	0					
					∨ User Inforr	nation											

Create Local User 1-2

≡	dentity Services	Engine			Work	Centers / Device Adr	ministration			٩	۵	0	Q 2
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
5	Dashboard	Users		✓ User Information	nation								
망	Context Visibility			First Name									
~%	Operations			Last Name									
-0	Policy			-									
8.	Administration			✓ Account C	ptions								
đ	Work Centers			Description	Γ								
?	Interactive Help			Change passv	rord on next login								
				✓ Account D	isable Policy								
				Disable a	ccount if date exceed	s 2025=03=20	(yyyy-mm-dd)						
					с								
				✓ User Grou	ps								
						<u>~</u> 0 🖲							
										d			
										Submit		Canc	el

```
Create Local User 2-2
```

Step 6. (Optional) Add TACACS+ Policy Set

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

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



Add TACACS+ Policy Set

Step 7. Configure TACACS+ Authentication Policy

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

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

≡	dentity Services E	Engine Work Centers / Device Administration		۵ ۵	0	Q	۹
н	Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Adm	nin Policy Sets Repor	rts Settings			
	Dashboard	Deliny Sets - DNAC - Deliny	Peret P	acat Ballou Sat Mit Causta		e	ה
1d	Context Visibility	Policy Sets - Divac - Policy	Reset	eset Policy Set Hit Counts	C	Save	J
*	Operations	Status Policy Set Name Description Conditions	A	llowed Protocols / Server S	Sequen	ce Hitr	
-0	Policy	Q Search					
8.	Administration	DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC		Default Device Admin	0	+ 0	
កា	Work Centers						
		VAuthentication Policy(2)					
(?)	Interactive Help	• Status Rule Name Conditions	Use		Hits	Actions	
		Q Search		d			
		b C	Internal Use	rs a			
		DNAC - Authentication DEVICE-Device Type EQUALS All Device TypesIIDNAC-Servers	> Options	;	0		
			All_User_ID	_Stores			
		O Default	> Options	3	0	曫	
		> Authorization Policy - Local Exceptions					
		>Authorization Policy - Global Exceptions					
		> Authorization Policy(4)					

Add TACACS+ Authentication Policy

Step 8. Configure TACACS+ Authorization Policy

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

This step to create Authorization Policy for each User Role.

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

Procedure

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

- b. Define the Authorization Policy name
- c. Set the Authorization Policy Condition and Select User Group that you created in (Step4)
- d. Set the Authorization Policy Shell Profiles and Select TACACS Profile that you created in (Step3)
- e. Click Save

≡	deale Identity Services I	Engine					w	ork C	enters / Device Adm	inistratio	n				Q	۵ ۵) Ç	9 S
Щ	Bookmarks	Overv	iew Id	entities	User Identity	Groups	Ext Id Source	s I	Network Resources	Policy Ele	ements Device	Admin Policy Se	ts Rep	orts Se	ttings			
	Dashboard		Q Sea	ch														
ь	Context Visibility			DNAG	- Policy			Ģ	DEVICE-Device Type EQUALS	All Device Typ	pes#DNAC			Default Der	vice Admin		0+	0
*	Operations																	
-0	Policy		> Authentic	tion Polic	:y(2)													
8.	Administration		> Authoriza	ion Policy	r - Local Exceptions													
ភា	Work Centers		> Authoriza	ion Policy	 Global Exceptions 													
			VAutooriza	ion Policy	(1)													
?	Interactive Help										Results							
			🕑 Sta	tus Rul	e Name	Cond	litions				Command Sets		Shell Profil	es		Hits	Act	ions
			Q Se	arch					1									
	SUPER-ADMIN	I-ROLI	⊧ (Sup	er Admin	8	IdentityGroup-Name E	QUALS (User Identity Groups:SUPER-AC	DMIN	Select from list	ℓ +	SUPER_A	DMIN_ROLE	∞ ∨	•	\$\$	3
	NETWORK-ADM	IN-RO	LE (Net	work Admin	8	identityGroup-Name E	QUALS (User Identity Groups:NETWORK	-ADMIN	Select from list	0 +	NETWOR	K_ADMIN_RO)LE 🤕 🗸	•	£0	3
	SecOps-Rol	е	(Sec	Ops	8	IdentityGroup-Name E	QUALS (User Identity Groups:SecOps		Select from list	0 +	SecOps_	Role	∞ ~	+	<i>{</i> \$	3
				Def	ault						DenyAllCommands	0 +	Deny All S	Shell Profile	0	+ 0	<i>{</i> \$	}
															Re	set	Sa	we

Add Authorization Policy

Verify

Verify RADIUS Configuration

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

	■ Cisco DNA Center	System / Users & Roles	Q @ @ Q
	User Management Role Based Access Control	External Authentication	
Ē	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 Attr 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 spe configuration inside Authorization profile would look like "cisco-av-pairs 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".	
		🖉 Enable External User 🕗	
		 AAA Attribute AAA Attribute Cisco-AVPair Reset to Default Update AAA Server(s) External Users 	
		∑ Filter	EQ, Find
		Username Action Action)
		devops_user DevOps-Role Delete	
		Showing 1 of 1	

External Users

2. DNAC - Confirm user access



```
Limited User Access
```

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

=	dentity Services	Engine		Operations / RADIUS		Q & @ Q A
J	Bookmarks	Live Logs Live Sessions				
23	Dashboard					
16	Context Visibility	Misconfigured Supplicants ()	Misconfigured Network Devices 0	RADIUS Drops 🕕	Client Stopped Responding 🕕	Repeat Counter 🕕
*	Operations	0	0	5761	0	0
- 0	Policy				Refresh Sho	w Within
8.	Administration				Never 🗸 La	test 20 records v Last 60 Secondsv
ň	Work Centers	ට් 💭 Reset Repeat Counts 🖞 Export 1	° ~			Filter 🗸 🔘
		Time Status	Details Repea Identity	Endpoint ID Endpoint Profile	Authentication Policy Authorization Policy	Authorization Profiles IP Addre
?	Interactive Help	X Auth	× Identity	Endpoint ID Endpoint Profile	Authentication Policy Authorization Policy	Authorization Profiles IP Addres
		Jan 19, 2025 11:19:18.1 🥑	.a DevOps_User		DNAC - Policy >> DNAC - Authentication DNAC - Policy >> DevOps	DevOps-Profile
		Last Updated: Sun Jan 19 2025 23:19:	7 GMT+0100 (Central European Standard Time)			Records Shown: 1

RADIUS Live-Logs

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 ise34 Policy Server Event 5200 Authenti cation 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 All Locations Location

Cisco ISE

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 Detailed Live-Logs 1-2

Cisco ISE		
IdentityPolicyMatc	mediture t	UNAC - Authentication
AuthorizationPolic ule	yMatchedR (DevOps
ISEPolicySetName		DNAC - Policy
IdentitySelectionN	fatchedRule (DNAC - Authentication
TotalAuthenLatenc	ty 3	35
ClientLatency	0	0
DTLSSupport		Unknown
Network Device P	rofile (Cisco
Location	L	Location#All Locations
Device Type	1	Device Type#All Device Types#DNAC-Servers
IPSEC		PSEC#Is IPSEC Device#No
Name		User Identity Groups:DevOps
EnableFlag	E	Enabled
RADIUS Username		DevOps_User
Device IP Address	- L	
CPMSessionID	0	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
CiscoAVPair		AuthenticationidentityStore +internal Users, CGSubjectName+9273fe30-8c01 - 1 te6-996c- 555400e48521 te6vops_uter, IniqueSubjectID=984d28083d866a118bcc98565c8f5eaa5de gr467
Result		
Class	CA tG	CS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R /WY:ise34/526427220/15433
cisco-av-pair	RC	DLE=DevOps-Role
-		

RADIUS Detailed Live-Logs 2-2

Verify TACACS+ Configuration

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

■ Cisco DNA Center	System / Users & Roles	Q @ @ 4
User Management Role Based Access Control External Authentication	 AAA Attribute AAA Attribute Cisco-AVPair Reset to Default Update 	
	 AAA Server(s) Primary AAA Server Secondary AAA Server IP Address IP Address	
	✓ External Users	EQ, Find
	Username + Role Action secops_user SecOps-Role Delete	
	Showing 1 of 1	

External Users

2. DNAC - Confirm user access

Cisco DNA Center			Q (0)
T Policy >	Group-Based Access Control		💭 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			
A secops_user ≪		Detwork Bug Identifier Identify bugs in the network	

Limited User Access

3.a ISE - TACACS+ Live-Logs Work Centers > Device Administration > Overview > TACACS Livelog.



TACACS Live-Logs

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

test Cisco ISE					
Overview		Steps			
Request Type	Authorization	Step ID	Description	Latency (ms)	
Status	Pace	13005	Received TACACS+ Authorization Request		
5		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	
Authorization Delicu	DNAC - Deline >> SecOne	15013	Selected Identity Source - Internal Users	5	
Authorization Policy	Divid - Policy >> accops	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		
Command From Device		15036	Evaluating Authorization Policy	8	
		15048	Queried PIP - Network Access.UserName	10	
		15048	Queried PIP - IdentityGroup.Name	2	
Authorization Details		22001	Selected Shell Profile		
Autionzation Details		22081	New accounting session created in Session cache		
Generated Time	2025-01-19 17:12:43.368 +1:00	13034	Returned TACACS+ Authorization Denly		
Logged Time	2025-01-19 17:12:43.368	15054	Received 190903* Paciforization Repry		
Epoch Time (eac)	1737303163				
chocu unite (sec)	1737303103				
ISE Node	ise34				
Message Text	Device-Administration: Session Authorization succeeded				
Failure Reason					
Resolution					
Root Cause					
Username	SecOps_User				
Network Device Name	DNAC				

TACACS+ Detailed Live-Logs 1-2



TACACS+ Detailed Live-Logs 2-2

References

Cisco Identity Services Engine Administrator Guide, Release 3.4 > Device Administration

Cisco DNA Center Administrator Guide, Release 2.3.5

Cisco DNA Center: Role Based Access Control with External Authentication