# 将ISE配置为DNAC GUI的外部身份验证

目录
先决条件
使用的组件
开始使用前
<u>(选项1)使用RADIUS配置DNAC外部身份验证</u>
<u>(选项1)为RADIUS配置ISE</u>
<u>(选项2)使用TACACS+配置DNAC外部身份验证</u>
<u>(选项2)为TACACS+配置ISE</u>
<u>验证</u>
检验RADIUS配置
检验TACACS+配置
<u>故障排除</u>
<u>参考</u>

# 简介

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

## 先决条件

要求

思科建议您了解以下主题:

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

### 使用的组件

本文档中的信息基于以下软件和硬件版本:

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

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

- 确保您在System > Settings > External Services > Authentication and Policy Servers上配置了 至少一个RADIUS身份验证服务器。
- 只有对DNAC具有超级管理员角色权限的用户才能执行此过程。
- 启用外部身份验证回退。
- ⚠ 警告:在早于2.1.x的版本中,当启用外部身份验证时,如果AAA服务器无法访问或AAA服务器拒绝未知用户名,则Cisco DNA Center将回退到本地用户。在当前版本中,如果AAA服务器无法访问或AAA服务器拒绝未知用户名,Cisco DNA Center不会回退到本地用户。启用外部身份验证回退后,外部用户和本地管理员可以登录到Cisco DNA Center。

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

### 配置

(选项1)使用RADIUS配置DNAC外部身份验证

步骤1.(可选)定义自定义角色。

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

#### 步骤

a.创建新角色。

Ξ	Cisco DNA Center	Create a User Role	Q @ 🛎 🗘
	Create a New Role Define the name of the role, and then p Role Name* DevOps-Role Describe the role (optional)	provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.	

### b.定义访问。

≡ Cisco DNA	Center			Create a User Role	Q @ @ \$					
Defi	ne the Acce	ess								
() <sup>T</sup>	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 a role is	the <b>DevOps-Role</b> ro s configured with De 1	le. Custom ny permissi	roles permit or on, all related c	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.						
A	ccess • Permissio	1		Description						
> A	ssurance O Deny	O Read	O Write	Assure consistent service levels with complete visibility across all aspects of your network.						
> N	etwork O Deny	<ul> <li>Read</li> </ul>	O Write	Access to Network Analytics related components.						
> N	etwork 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.						
> N	etwork rovision O Deny	O Read	O Write	Configure, upgrade, provision and manage your network devices.						
> N S	etwork ervices O Deny	O Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.						
> P	latform O Deny	Read	O Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.						
> s	ecurity O Deny	O Read	O Write	Manage and control secure access to the network.						
					2					
€ Exit				Review Back	Next					

DevOps角色访问

### c.创建新角色。

■ Cisco DNA Center		Create a User Role	Q @ <b>4</b> 4
Summary Review the DevOps-Role role. Make :	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	
<ul> <li>Role Name &amp; Description</li> <li>Edit</li> </ul>			
Role Name DevOps-Role			
Role Description			
<ul> <li>Role Capability Edit</li> </ul>			
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角色摘要

≡ Cisco	DNA Center		Create a User Role			Q @ 6
	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
	Cuntom Management	Donu				<u> </u>
Exit					Back	Create Rol

审核并创建DevOps角色

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

步骤

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

b.设置AAA属性。

在AAA attributes字段中输入Cisco-AVPair。

c.(可选)配置主要和辅助AAA服务器。

确保主AAA服务器上或主服务器和辅助服务器上都启用了RADIUS协议。

#### ■ Cisco DNA Center

System / Users & Roles

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 Cisco DNA Center is the name of the AAA attribute chosen on the AAA attribute, it needs to be configured here on 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 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".
a	Enable External User
b	AAA Attribute AAA Attribute Cisco-AVPair
	Reset to Default Update
С	AAA Server(s)       Primary AAA Server     Secondary AAA Server       IP Address     IP Address       ISE Server 1 IP     ISE Server 2 IP       shared Secret     Shared Secret       Imme     Imme       Imme     Imme       Hide Advanced Settings     Hide Advanced Settings       O RADIUS O TACACS     O RADIUS O TACACS       Authentication Port     Authentication Port       1812     1812

(RADIUS)外部身份验证配置步骤

(选项1)为RADIUS配置ISE

步骤1.将DNAC服务器添加为ISE上的网络设备。

这可以通过管理>网络资源>网络设备选项卡完成。

#### 步骤

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

=	dentity Services E	Engine				Administr	ration / Network Resources			٩	۵	0	4   ۵
н	Bookmarks	Network Devices	Network Dev	vice Groups Ne	etwork Device Profiles	External RADIUS Servers	RADIUS Server Sequences	External MDM	pxGrid Direct Connectors				
11日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日	Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Network Device Default Device Device Security Settings	а	Network Device Network Device Name Description IP Address Device Profile Model Name Software Version	> DNAC           es:           pNAC          *™:           DNAC Serve           #2: Cisco	r IP	· <u>' 32</u> Ø						
			b c	Network Device 1 Location IPSEC Device Type RADIUS Protocol Shared St Use St	All Locations All Locations No DNAC-Servers US Authentication Settil UDP Settings RADRUS Cd Second Shared Secret Second Shared Secret 1000	Set To De     Set To De	fault fault fault Show						

用于RADIUS的ISE网络设备(DNAC)

步骤2.创建RADIUS授权配置文件。

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

注意:创建3个RADIUS授权配置文件,每个用户角色一个。

#### 步骤

a.单击Add并定义RADIUS授权配置文件名称。

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

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

c.查看属性详细信息。 d.Click Save.

≡ deale Identity Servic	ces Engine	Policy / Policy Elements	Q & @ Q   A
JII Bookmarks	Dictionaries Conditions	esults	
<ul> <li>Bashboard</li> <li>Context Visibility</li> <li>Operations</li> <li>Policy</li> <li>Administration</li> <li>Work Centers</li> <li>Interactive Help</li> </ul>	Asthentication v Athentication Profiles v Asthenication Profiles v Downloadsbin ACLa v Profiling 2 Postare 2 Client Provisioning 2	Authorization Profile a Authorization Profile a * Name pevOgs-Prefile Description * Access Type ACCESS_ACCEPT ~ Network Device Profile © Course ~ © Service Template □ Track Movement □ © Agentiess Posture □	
		Advanced Attributes Settings b  C  Attributes Details  Attributes Details  Reserver R02-bedgesite	d Cancel

创建授权配置文件

步骤3.创建用户组。

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

步骤

a.单击Add并定义身份组名称

b.(可选)定义说明。

c.单击Submit。



创建用户身份组

步骤4.创建本地用户。

这可以通过管理>身份管理>身份>用户选项卡完成。

步骤

a.单击Add并定义用户名。

b.设置登录密码。

c.将用户添加到相关用户组。

d.单击 submit。

$\equiv$ $\frac{1}{1000}$ Identity Services Eng	jine	Administration / Identity Management	0000	9   A
I Bookmarks Id	entities Groups External Id	entity Sources Identity Source Sequences Settings		
년 Context Visibility 왓 Operations	Latest Manual Network Scan Results	Verwork Access User		
Policy     Administration	a	* Username DevOps_User Status Enabled V		
Work Centers		Account Name Alias O Email		
Interactive Help		Password Type: Internal Users     Password Lifetime:     With Expiration ①     Password will expire in 60 days     Never Expires ①		
	b	Password     Re-Enter Password       * Login Password		

创建本地用户1-2

≡	dentity Services E	Engine					Admi	inistration /	/ Identity Ma	anageme	nt			5.13 2.13		Q	۵	0	۹ ا	A
月 王 志 父 し ふ る 。 ③	Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers	Identities Users Latest Manuel Results	Groups	Extern	al Identity Sources  * Login Password Enable Password  V User Informa First Name Last Name V Account Opt Description	Identity Sou	rce Sequences	setting	5 7 0339000 V		Generate Password Generate Password	) ©								
					<ul> <li>Account Dis:</li> <li>Disable account</li> <li>User Groups</li> <li>User Groups</li> </ul>	ble Policy unit if date exce C	- 2025-03-20	0	(yyy>mm	-dd)					Sut	mit		Ganc	cel	

创建本地用户2-2

步骤5.(可选)添加RADIUS策略集。

这可以在Policy > Policy Sets选项卡中完成。

步骤

a.单击Actions并选择(上面插入新行)。

b.定义策略集名称。

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

d.设置Allowed协议。

e.Click Save.

f.点击(>)Policy Set View配置身份验证和授权规则。

≡ dentity Serv	rices Engine	Policy / Policy Sets	
Bookmarks	<ul> <li>Status Policy Set Name</li> </ul>	Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
Dashboard	Q Search b	C	
ℜ Operations	DNAG - PORCY	M DEVICE-Device Type #QUALS All Device Type#RDAAC-Servers	Default Network Access (2) 0 (2) (3)
Policy     Administration	Uniot	versuit poixy set	
HIII Work Centers			Reset
Interactive Help			

添加RADIUS策略集

步骤6.配置RADIUS身份验证策略。

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

步骤

a.单击Actions并选择(上面插入新行)。

b.定义身份验证策略名称。

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

d.为身份源设置Authentication Policy Use。

e.Click Save.

≡ dentity Services En	gine Policy / Policy Sets		Q & @	0 Q   A
JI Bookmarks	Policy Sets-+ DNAC - Policy	Reset Reset Policy Se	t Hit Counts	Save
Dashboard	Status Policy Set Name Description Conditions	Allowed Proto	cols / Server Sequ	ence Hits
No Constantions	Q Search			
Policy	DNAC - Pelicy           DIAAC - Pelicy         DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers	Default Netwo	ork Access	9 + o
Administration	V Authentication Policy(2)			
Work Centers				
	Status Rule name     Conditions	d	Prics	Actions
Interactive Help	Burkon     C     BUNAC - Authentication     DEVICE Device Type EQUALS All Device TypestiDNAC-Servers     Default     Default	Internal Users     Options     All_User_IO_Stores     Options	· ·	\$ \$
	> Authorization Policy - Local Exceptions			
	> Authorization Policy - Global Exceptions			
	> Authorization Policy(1)			
			Reset	e Save

添加RADIUS身份验证策略

步骤7.配置RADIUS授权策略。

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

此步骤用于为每个用户角色创建授权策略:

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

#### 步骤

a.单击Actions并选择(上面插入新行)。

b.定义授权策略名称。

c.设置授权策略条件并选择您在中创建的用户组(第3步)。

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

e.Click Save.

$\equiv$ $\frac{1}{1000}$ Identity Services Eng	jine	Policy / Policy Sets		Q & Ø Q
Bookmarks	Policy Sets -> DNAC - Policy	Reset	Reset Policy Set Hit Counts Save	
id Context Visibility	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
Operations     Policy	ONAC - Policy	DEVICE Device Type EQUALS AI Device TypesIIDNAC-Servers		Default Network Access 🥒 🔶
Administration	>Authentication Policy(2)			
HIII Work Centers	> Authorization Policy - Local Exceptions			
Interactive Help	>Authorization Policy - Global Exception	5		
			Results	
	+ Status Rule Name	Conditions	Profiles Security	y Groups Hits Actions
	Q Search b	С	d	a
	Super Admin	R IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr × V + Select	t from list 🖉 + 🔹 🚳
	Network Admin	R IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role × v + Select	t from list 🥒 + 🔹 🚳
	DevOps	R IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile 0 + Select	t from list 🥒 🕂 🔹 🚳
	Oefault		DenyAccess 0 + Select	t from list 🥒 + 🔹 🏠
				е
				Reset

添加授权策略

### (选项2)使用TACACS+配置DNAC外部身份验证

步骤1.(可选)定义自定义角色。

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

#### 步骤

a.创建新角色。

≡ 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. Role Nume*	To make it easier to assign roles down the road, describe the role as clearly as possible.	
SecOps-Role Describe the role (optional)		
		2
€ Exit		Next

### b.定义访问。

■ Cisco DNA Center	Create a User Role	Q @ 4								
Define the Access	Define the Access									
These permissions enable different capabilities in Ci- permissions allow. Click here to Learn More.	sco 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 SecOps-Role role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.										
> Network Analytics 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	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	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.									
> 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	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.									
		2								
€ Exit	Review Back	Next								

SecOps角色访问

### c.创建新角色。

■ Cisco DNA Center		Create a User Role	
Summary Review the SecOps-F	ole role Make sure all the details are as you expect the	em to be. If you need to change something, clicking edit will take you back to that section	
<ul> <li>Role Name &amp; De Role Name Role Description</li> </ul>	scription Edit SecOps-Role		
<ul> <li>Role Capability</li> <li>ASSURANCE</li> </ul>	Edit		
Monitoring and Troubleshooting	Deny		
Monitoring Setting	s Deny		
Troubleshooting To	ols Deny		
NETWORK ANALYTIC	\$		
Data Access	Write		
NETWORK DESIGN			
Advanced Network	Settings Deny		
Image Repository	Deny		
Network Profiles	Deny		
Network Settings	Denv		
Virtual Network	Denv		
- Exit			Back Create Role

SecOps角色摘要

■ Cisco DNA Center		Create a User Role	Q @ 🛎 🗘
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

审核并创建SecOps角色

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

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

b.设置AAA属性。

在AAA attributes字段中输入Cisco-AVPair。

c.(可选)配置主要和辅助AAA服务器。

确保主AAA服务器上或主服务器和辅助服务器上都启用了TACACS+。

■ Cisco DNA Center	System / Users & Roles	Q @ C 4	ł.
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 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 config The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Rofe=role1". On ISE server, choose the cisco-av-pair attribute from cisco specie configuration inside Authorization profile would look 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".  The value <b>Super External User</b>	ute here on Cisco DNA Center is the gured here on Cisco DNA Center. Jfic AAA attributes list. A sample	
b	AAA Attribute     AAA Attribute     Cisco-AVPair      Reset to Default     Update		
С	∼ AAA Server(s)             Primary AAA Server             P Address             P Address             ISE Server 1 IP             Shared Secret             Info             Shared Secret             Info             Hide Advanced Settings             Hide Advanced Settings             Port             Port            Port             Port             Port		

(TACACS+)外部身份验证配置步骤

### (选项2)为TACACS+配置ISE

#### 步骤1.启用设备管理服务。

这可以通过Administration > System > Deployment > Edit(ISE PSN Node)> Check Enable Device Admin Service选项卡完成。

≡ dade Identity Services Engine	Administration / System	۹	۵ ۵	ÐÇ	ء   د
I Bookmarks Deployment Licensing	Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings				
E: Dashboard					
10 Context Visibility	Administration				
≪ Operations					
Policy	Monitoring				
2. Administration	Role PRIMARY V				
HI Work Centers	Other Monitoring Node				
③ Interactive Help	Dedicated MNT ()				
	Policy Service     Craste Session Service;     Include Node in Node Group: None     Craste Profiling Service;     Craste Profiling Service;     Craste Profiling Service;     Craste StAP Service;     Craste StAP Service;     Craste StaP Service;     Craste StaP Service;     Craste Prostice Admin Service;     Craste Prostice A				
	v pxGrid () Enable pxGrid Cloud ()				
	Reset		Sa	**	

启用设备管理服务

步骤2.将DNAC服务器添加为ISE上的网络设备。

#### 步骤

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

≡ dealer Identity Services	Engine	Administration / Network Resources	္ရန္စစ္န	9   A
JI Bookmarks	Network Devices Network D	evice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors		
Bookmarks     Dashboard     Dashboard     Ontext Visibility     Operations     Policy     Policy     Nork Centers     Interactive Help	Network Device Device Security Settings: A	Process     Partice Profile     Comparison     Partice Profile     Comparison       Passes     *****     ******     ******     ************************************		
	b c	Software Version		

用于TACACS+的ISE网络设备(DNAC)

步骤3.为每个DNAC角色创建TACACS+配置文件。

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

注意:创建3个TACACS+配置文件,每个用户角色一个。

步骤

a.单击Add并定义TACACS Profile名称。

b.单击Raw View选项卡。

c.输入Cisco-AVPair=ROLE=并填写正确的用户角色。

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

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

### d.Click Save.

≡ deale Identity Ser	vices Engine		Work Centers / Device Administration						۵	@ (	2   S
I Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
Dashboard	Conditions	> TACACS Profiles >	New								
I Context Visibility	Network Conditions	TACACS Profi	a								
Operations     Policy	Results Allowed Protocols	Vame SecOps_Role		$\supset$							
Administration	TACACS Command Sets	Description									
Work Centers	TALACS Promes										
Interactive Help		C Profile Attribute VM C Cisco-AVPair=R	B Raw View Ites ROLE=SecOps-Role	Cancel	d Save						

创建TACACS配置文件(SecOps\_Role)

步骤4.创建用户组。

这可以通过工作中心>设备管理>用户身份组选项卡完成。

步骤

a.单击Add并定义身份组名称。

b.(可选)定义说明。

c.单击Submit。

$\equiv \frac{1}{1000}$ Identity Services	Engine		Work Centers / Dev	vice Administration			Q &	ତ ଦ   ୧
JU Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources Network Reso	ources Policy Elements	Device Admin Policy Sets	Reports	Settings	
Image: Second system     Image: Second system       Image: Second system     Operations       Image: Second system     Policy       Image: Second system     Administration       Image: Second system     Work Centers	Identity Groups SQ C SC C C C C C C C C C C C C C C C C	antity Groups b	y Groups > New User Mentity Group Group SecOps SecOps-Role				C	Cancel

创建用户身份组

步骤5.创建本地用户。

这可以通过工作中心>设备管理>身份>用户选项卡完成。

步骤

a.单击Add并定义用户名。

b.设置登录密码。

c.将用户添加到相关用户组。

d.单击 submit。

≡	■ shorth Identity Services Engine				Work Centers / Device Administration							٩	۵ و	0 Q   A
Щ	Bookmarks	Overview	Identities	User Ident	tity Groups	Ext Id Sources	Network Reso	urces Po	licy Elements	Device Admin Policy S	Sets Reports	Settings		
5	Dashboard	Users		Ne	twork Access User	s List > New Network Ac	cess User							
망	Context Visibility													
*	Operations			Ĭ	Network Ac	cess User	~							
0	Policy			a	* Username	SecOps_User	J							
8.	Administration				Status	Z Enabled 🗸								
đ	Work Centers				Account Name	Alias	0							
					Email									
?	Interactive Help													
				`	<ul> <li>Passwords</li> </ul>									
					Password Type	6: Internal Users	~							
					Password Lifet	time:								
					<ul> <li>With Expira</li> </ul>	ation 🕕								
					Password w	ill expire in 60 days								
					O Wever Expi	103 🕖								
				(		Password		Re-Enter Pass	word	)				
				b	* Login Passw	ord				Generate Password	0			
				· ·	Enable Passwo	ord				Generate Password	0			
											~			
					. Une led									
					<ul> <li>User Inform</li> </ul>	nation								

#### 创建本地用户1-2

≡	abala Identity Services	Engine			Work Centers / Device Administration					٩	<b>\$</b> @	¢	A
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
	Dashboard	Users		✓ User Information	mation								
명	Context Visibility			First Name									
*	Operations			Last Name									
-0	Policy												
8.	Administration			✓ Account C	otions								
đ	Work Centers			Description	Γ								
?	Interactive Help			Change passv	vord on next login								
				✓ Account D									
				Disable a	account if date exceed	s 2025=03=20	(yyyy-mm-dd)						
					С								
				✓ User Grou	ps								
				: SecOp	5	<u>~</u> 0 😁							
										d			
			Description Change password on next login ~ Account Disable Policy: Disable account if date exceeds 2025-03-20 (yyyy-mm-dd) C V User Groups :: SecOps ~ (i)							Submit		ancel	

创建本地用户2-2

步骤6.(可选)添加TACACS+策略集。

这可以通过工作中心>设备管理>设备管理策略集选项卡完成。

#### 步骤

a.单击Actions并选择(上面插入新行)。

b.定义策略集名称。

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

d.设置Allowed协议。

e.Click Save.

f.点击(>)Policy Set View配置身份验证和授权规则。

=	dentity Services E	ngine		Policy / Policy Sets	
н	Bookmarks	Policy Sets			Reset Reset Policy Set Hit Counts Save
- 22	Dashboard	💿 Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
ьß	Context Visibility	Q Search		2	d (
*	Operations				
0	Policy	UNAC - Policy			Default Network Access 🐼 🗸 🛉
8.	Administration	C Default	Default policy set		Default Network Access 🖉 + o
di.	Work Centers				e
					Reset Save
?	Interactive Help				

添加TACACS+策略集

步骤7.配置TACACS+身份验证策略。

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

步骤

a.单击Actions并选择(上面插入新行)。

b.定义身份验证策略名称。

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

d.为身份源设置Authentication Policy Use。

e.Click Save.

≡ dentity Services	Engine Work Centers / Device Administration	Q &	⊕
Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements	Device Admin Policy Sets Reports Settings	
Dashboard	Policy Sets→ DNAC - Policy	Reset Reset Policy Set Hit Counts	e Save
명 Context Visibility 옷 Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Server	r Sequence Hits
Dolicy	Q Search		
Administration	DNAG - Policy     DVIGE-Device Type EQUALS All Device TypestDNAG	Default Device Admin	
Work Centers	✓Authentication Policy(2)		
Interactive Help	Status Rule Name Conditions	Use	Hits Actions
	Q Search	d	
	b C DNAC - Authentication C Device Type EQUALS All Device TypesHDNAC-Servers	Internal Users	o (ô)
		> Options	121
		All_User_ID_Stores	~
	Default	> Options	• (Ç)
	>Authorization Policy - Local Exceptions		
	>Authorization Policy - Global Exceptions		
	> Authorization Policy(4)		

添加TACACS+身份验证策略

#### 步骤8.配置TACACS+授权策略。

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

此步骤用于为每个用户角色创建授权策略:

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

#### 步骤

a.单击Actions并选择(上面插入新行)。

b.定义授权策略名称。

c.设置授权策略条件并选择您在中创建的用户组(第4步)。

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

e.Click Save.

≡	dialic Identity Services E	Engin	e				Wa	ork Centers / Device Ad	ministratio	n			٩	۵ ۵	) G	א   א
н	Bookmarks	Over	view	Ident	ties User Ide	ntity Groups	Ext Id Sources	s Network Resources	Policy Ele	ements Device Adr	min Policy Set	s Reports	Settings			
51	Dashboard		Q	Search												
명	Context Visibility			0	DNAC - Policy			DEVICE-Device Type EQUAL	S All Device Typ	pes#DNAC		Defa	ult Device Admi	n ,	0+	0
×	Operations															
0	Policy		> Authe	ntication	Policy(2)											
20	Administration		> Autho	rization	Policy - Local Except	lions										
đ	Work Centers		> Autho	rization	Policy - Global Excep	tions										
			~Autho	rization	Policy(1)											
?	Interactive Help									Results						
			۲	Status	Rule Name	Condi	tions			Command Sets	1	Shell Profiles		Hits	Act	lons
			Q	Search				1								
	SUPER-ADMIN	-ROI	E	•	Super Admin	8	identityGroup-Name EQ	QUALS User Identity Groups:SUPER-	ADMIN	Select from list	0+	SUPER_ADMIN_	ROLE 🐼 🤉	<u>_</u> +	< <u>\$</u>	>
	NETWORK-ADMI	N-RO	DLE	0	Network Admin	R	identityGroup-Name EQ	QUALS User Identity Groups:NETWO	RK-ADMIN	Select from list	0 +	NETWORK_ADM	N_ROLE 🚾	-	<i>{</i> 2	3
	SecOps-Role	е		0	SecOps	8	identityGroup-Name EQ	QUALS User Identity Groups:SecOps		Select from list	0 +	SecOps_Role	<b>(3</b> )	-	<i>{</i> \$	2
				٥	Default					DenyAllCommands	0 +	Deny All Shell Pro	file d	+ 0	< <u>\$</u>	>
															:	2
													R	pset	Sa	

添加授权策略

# 验证

### 检验RADIUS配置

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

	■ Cisco DNA Center	System / Users & Roles	Q @ @ Q
	User Management Role Based Access Control	External Authentication	
Г	External Authentication	Cisco DNA Center supports external servers for authentication and authorization of External Sers. Use the heids 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 conf	igured here on Cisco DNA Center is the
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 spec configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".	tific 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 🕖	
		<ul> <li>AAA Attribute</li> <li>AAA Attribute</li> <li>Cisco-AVPair</li> <li>Reset to Default</li> <li>Update</li> <li>AAA Server(s)</li> <li>External Users</li> </ul>	
			EQ, Find
		Username * Role Action	)
		devops_user DevOps-Role Delete	
		Showing 1 of 1	, ,

外部用户



```
有限的用户访问
```

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

=	death Identity Services	Engine	Opera	tions / RADIUS	<u>ବ ଜ ଜ</u> ଜ   ନ
н	Bookmarks	Live Logs Live Sessions			
10	Dashboard Context Visibility	Misconfigured Supplicants ()	Misconfigured Network Devices 🕕	RADIUS Drops 🕕	Client Stopped Responding 💿 Repeat Counter 💿
*	Operations	0	0	5761	0 0
0	Policy				Refresh Show Within
8.	Administration	0. http://www.akauto.com			Never v Latest 20 records v Last 60 Seconds v
ñ	Work Centers	Time Status	Details Repea Identity Endpoint	ID Endpoint Profile Authentication Policy	Authorization Policy Authorization Profiles IP Addre
(?)	Interactive Help	X <u>Authv</u> X	Identity Endpoint	D Endpoint Profile Authentication Policy	Authorization Policy Authorization Profiles IP Addres
		Jan 19, 2025 11:19:18.1 🕑	.o DevOps_User	DNAC - Policy >> DNAC - Author	stication DNAC - Policy >> DevOps DevOps-Profile
		Last Updated: Sun Jan 19 2025 23:19:57 G	MT+0100 (Central European Standard Time)		Records Shown: 1

RADIUS实时日志

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click(Details)for Authorization  $\log_{\circ}$ 

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 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	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

RADIUS详细实时日志1-2

	Cisco ISE	
	IdentityPolicyMatchedHule	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	
	CPMSessionID	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
	CiscoAVPair	AuthenticationidentityStore-Internal Users, FQSubjectName 92731630-801-1166-998c- 525400648521646vogs_user, UniqueSubjectD+984d28083db66a1f8bcc98565c8f5eaa5de df467
	Result	
	Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R tG/WY:ise34/526427220/15433
1	cisco-av-pair	ROLE=DevOps-Role
Ľ		

RADIUS详细实时日志2-2

### 检验TACACS+配置

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

	■ Cisco DNA Center		System / Users & Roles		Q @ C 4
I	User Management Role Based Access Control External Authentication	<ul> <li>AAA Attribute</li> <li>AAA Attribute</li> <li>Cisco-AVPair</li> <li>Reset to Default</li> <li>Update</li> </ul>			
		<ul> <li>AAA Server(s)</li> <li>Primary AAA Server</li> <li>P Address</li> <li>Shared Secret</li> <li>*****</li> <li>Info</li> <li>View Advanced Settings</li> <li>Update</li> </ul>	Secondary AAA Server IP Address Shared Secret territe Info View Advanced Settings Update		
		<ul> <li>✓ External Users</li> <li></li></ul>			EQ, Find
		Username 🝝	Role	Action	
		secops_user	SecOps-Role	Delete	
			Showing 1 of 1		

#### 外部用户

### 2. DNAC — 确认用户访问权限。

Cisco DNA Center			Q (0)
<sup>8</sup> T <sup>0</sup> Policy	Group-Based Access Control		C Explore
5 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			
		9-0 <sup>0</sup>	
		Network Bug Identifier	
		Identify bugs in the network	
$\frown$			
요 secops_user			

有限的用户访问

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

≡	dentity Services I	Engine					Operat	ions / TACACS			q	۵ ۵	Ð	۹
н	Bookmarks	Live Log	js											
55	Dashboard		-											
망	Context Visibility								Refre	<i>b</i>	Show	Within		
*	Operations								Neve	r v	Latest 20 records	Last 6	) Second	sv
0	Policy	6	う 🍈 Export To 🗸									Filter	~ •	
80	Administration		Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
di.	Work Centers	>	<	Y		Identity		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#I	NAC	Loc
(?)	Interactive Help	10	Jan 19, 2025 05:12:4 st Undated: Sun Jan 19 2	025 17:16:38	GMT+0100	SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All De	Record	NAC	Loc
			st opusted. Sun san 192	025 17.10.30	GMTFOTO	(central curope	an otanuaru rimey					Record	s Shown	-

TACACS实时日志

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

Cisco ISE	이 특별 이 이 이 분들한 수 있습			
erview		Steps		
Request Type	Authorization	Step ID	Description	Latency (ms)
Status	Pass	13005	Received TACACS+ Authorization Request	
Passian Key		15049	Evaluating Policy Group	1
session key	15034/520427220/13356	15008	Evaluating Service Selection Policy	1
Message Text	Device-Administration: Session Authorization succeeded	15048	Queried PIP - DEVICE.Device Type	4
Jsername	SecOps_User	15041	Evaluating Identity Policy	7
Authorization Policy	DNAC - Policy >> SecOps	15013	Selected Identity Source - Internal Users	5
		24210	Looking up User in Internal Users IDStore	
Shell Profile	SecUps_Role	24212	Authentication Record	4
Matched Command Set		15036	Evaluating Authorization Dollary	
Command From Device		15048	Queried PIP - Network Access UserName	10
		15048	Oueried PIP - IdentityGroup.Name	2
		15017	Selected Shell Profile	2
uthorization Details		22081	Max sessions policy passed	1
		22080	New accounting session created in Session cache	0
Jenerated Time	2025-01-19 17:12:43.368 +1:00	13034	Returned TACACS+ Authorization Reply	0
ogged Time	2025-01-19 17:12:43.368			
poch Time (sec)	1737303163			
SE Node	ise34			
Message Text	Device-Administration: Session Authorization succeeded			
ailure Reason				
resolution				
Root Cause				
lisoname	SecOns User			
vac nellig	naroha"naai			
Network Device Name	DNAC			

TACACS+详细实时日志1-2

Cisco ISE	
. 100	riterione before
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+详细实时日志2-2

# 故障排除

当前没有可用于此配置的特定诊断信息。

# 参考

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

#### 关于此翻译

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

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

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