

# 在DNA Center和ISE 3.1上配置RADIUS外部身份验证

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[更多角色](#)

---

## 简介

本文档介绍如何使用运行3.1版本的Cisco ISE服务器在Cisco DNA中心配置RADIUS外部身份验证。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科DNA中心和思科ISE已集成，并且集成处于活动状态。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco DNA Center 2.3.5.x版本。
- 思科ISE 3.1版本。

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。

## 配置

步骤1: 登录到Cisco DNA Center GUI，然后导航到System > Settings > Authentication and Policy Servers。

验证是否已配置RADIUS协议以及ISE类型服务器的ISE状态是否为活动。

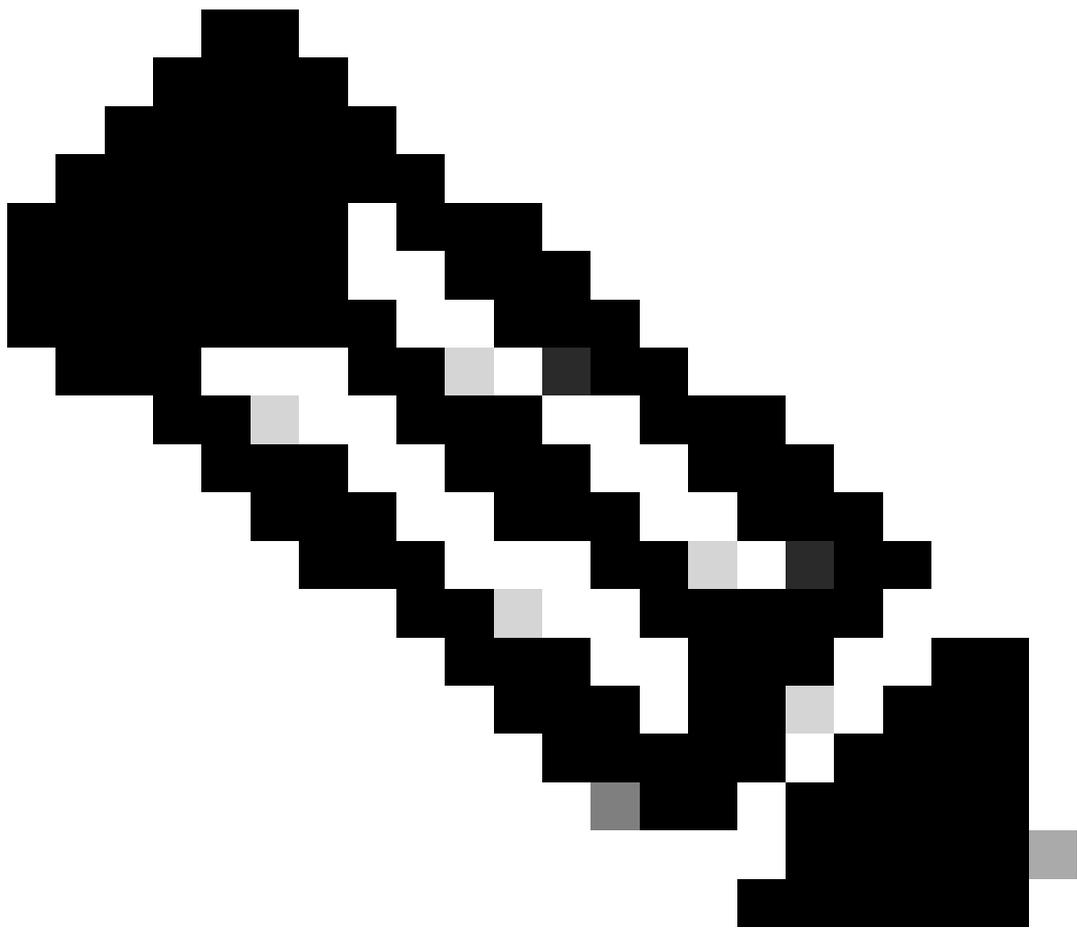
## Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	<b>RADIUS</b>	<b>ISE</b>	<b>ACTIVE</b>	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



注意：RADIUS\_TACACS协议类型适用于本文档。



警告：如果ISE服务器未处于活动状态，则必须首先修复集成。

第二步：在ISE服务器上，导航到管理>网络资源>网络设备，点击过滤器图标，写入Cisco DNA中心IP地址，然后确认条目是否存在。如果是，请继续执行步骤3。

如果缺少相应条目，则必须看到无可用数据消息。

## Network Devices



在这种情况下，您必须为Cisco DNA Center创建一个网络设备，然后单击Add按钮。

## Network Devices

Selected 0 Total 0  

 Edit **+ Add**  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

从Cisco DNA Center配置Name、Description和IP Address ( 或Addresses ) , 所有其他设置均设置为默认值, 本文档不需要这些设置。

## Network Devices

\* Name

Description

	<input type="text" value="IP Address"/>		* IP :	<input type="text" value=""/>		<input type="text" value=""/>		<input type="text" value=""/>		<input type="text" value="32"/>	
---	---	---	--------	-------------------------------	---	-------------------------------	---	-------------------------------	--	---------------------------------	---

\* Device Profile

Model Name

Software Version

### \* Network Device Group

Location

[Set To Default](#)

IPSEC

[Set To Default](#)

Device Type

[Set To Default](#)

向下滚动并通过单击其复选框以启用RADIUS身份验证设置并配置共享密钥。



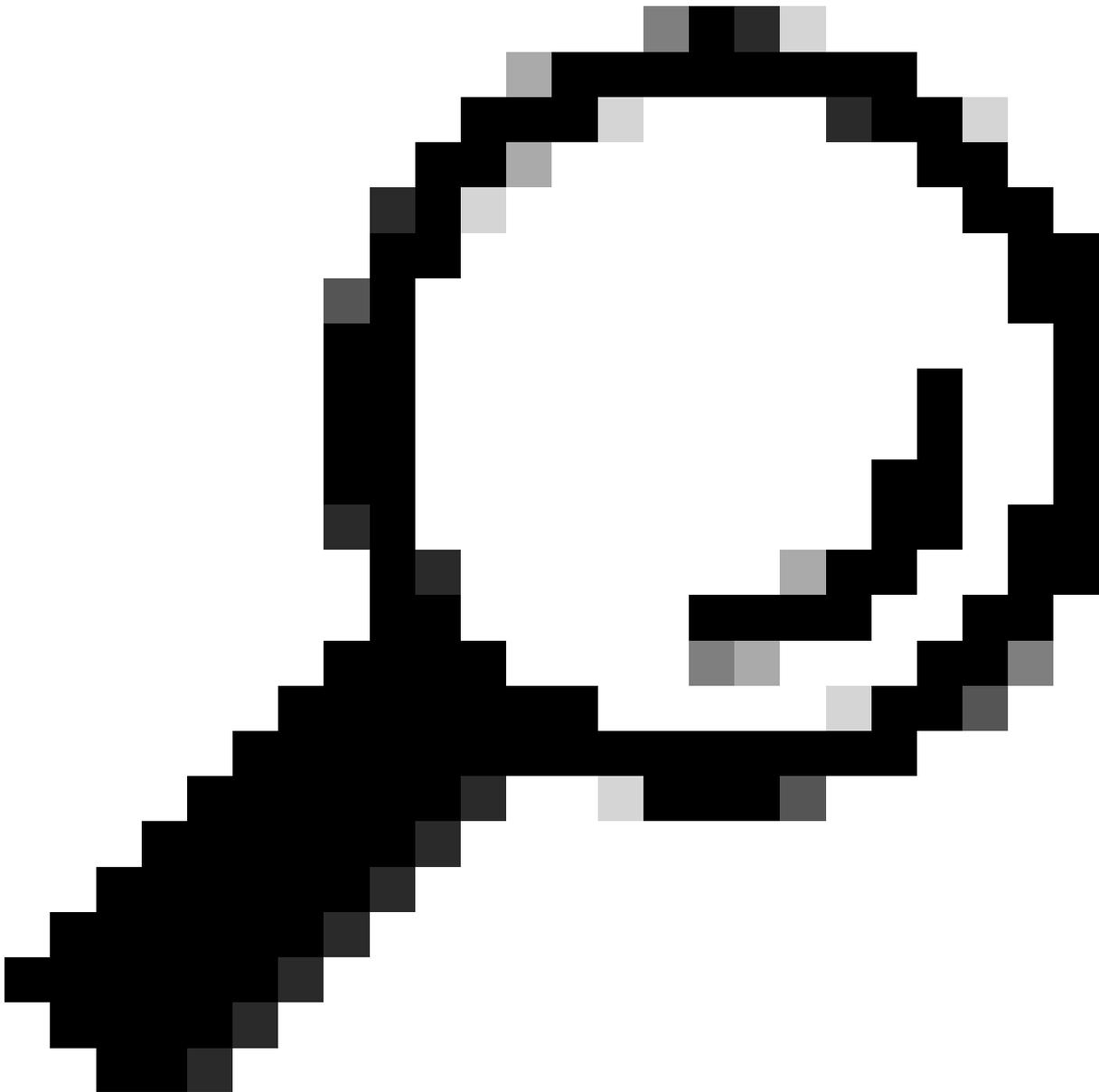
## ▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret .....

Show

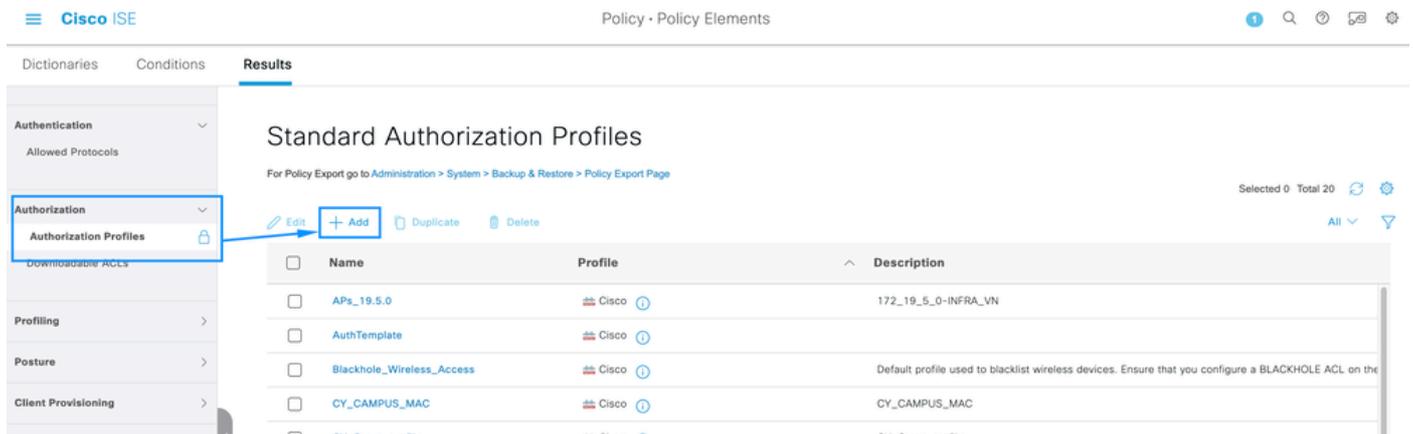


提示：此共享密钥将在以后需要，因此请将其保存到其他位置。

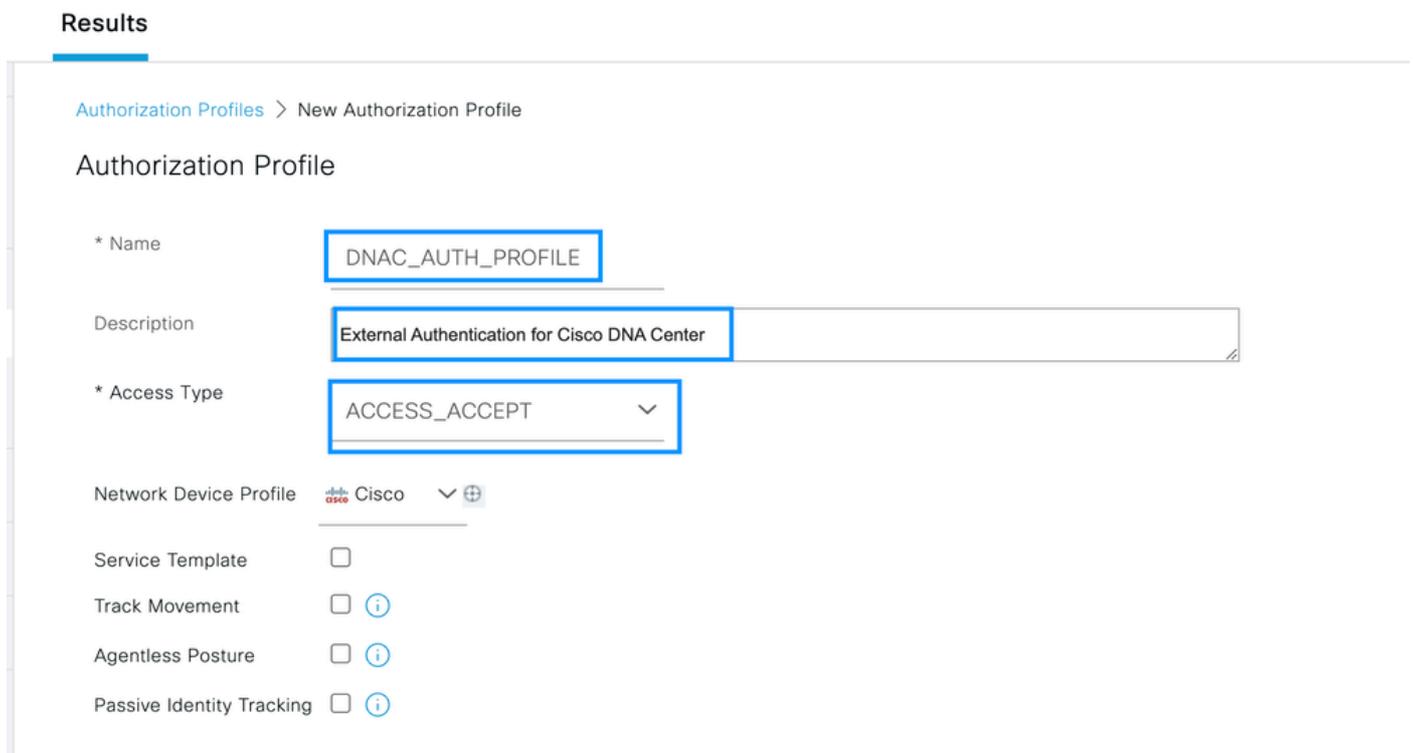
然后，单击Submit。

第三步：在ISE服务器上，导航到策略>策略元素>结果，创建授权配置文件。

确保您处于Authorization > Authorization Profiles下，然后选择Add选项。



配置名称，添加说明以记录新配置文件，并确保访问类型设置为ACCESSES\_ACCEPT。



向下滚动并配置Advanced Attributes Settings。

在左侧列中搜索cisco-av-pair选项并将其选中。

在右列手动键入Role=SUPER-ADMIN-ROLE。

一旦它看起来像以下图像，请单击Submit。

### Advanced Attributes Settings

⋮ Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE +

### Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = Role=SUPER-ADMIN-ROLE

第四步：在ISE服务器上，导航到工作中心(Work Centers) >分析器(Profiler) >策略集(Policy Sets)，配置身份验证和授权策略。

确定默认策略并单击蓝色箭头进行配置。

The screenshot shows the Cisco ISE Work Centers - Profiler interface. The 'Policy Sets' section is active, displaying a table of policy sets. The 'Default' policy set is highlighted with a blue box, and a blue arrow points to its configuration icon. The table has the following columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➔
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➔
✅	Default	Default policy set		Default Network Access	180517	⚙️	➔

在默认策略集中，展开身份验证策略，在默认部分下，展开选项，并确保它们与以下配置匹配。

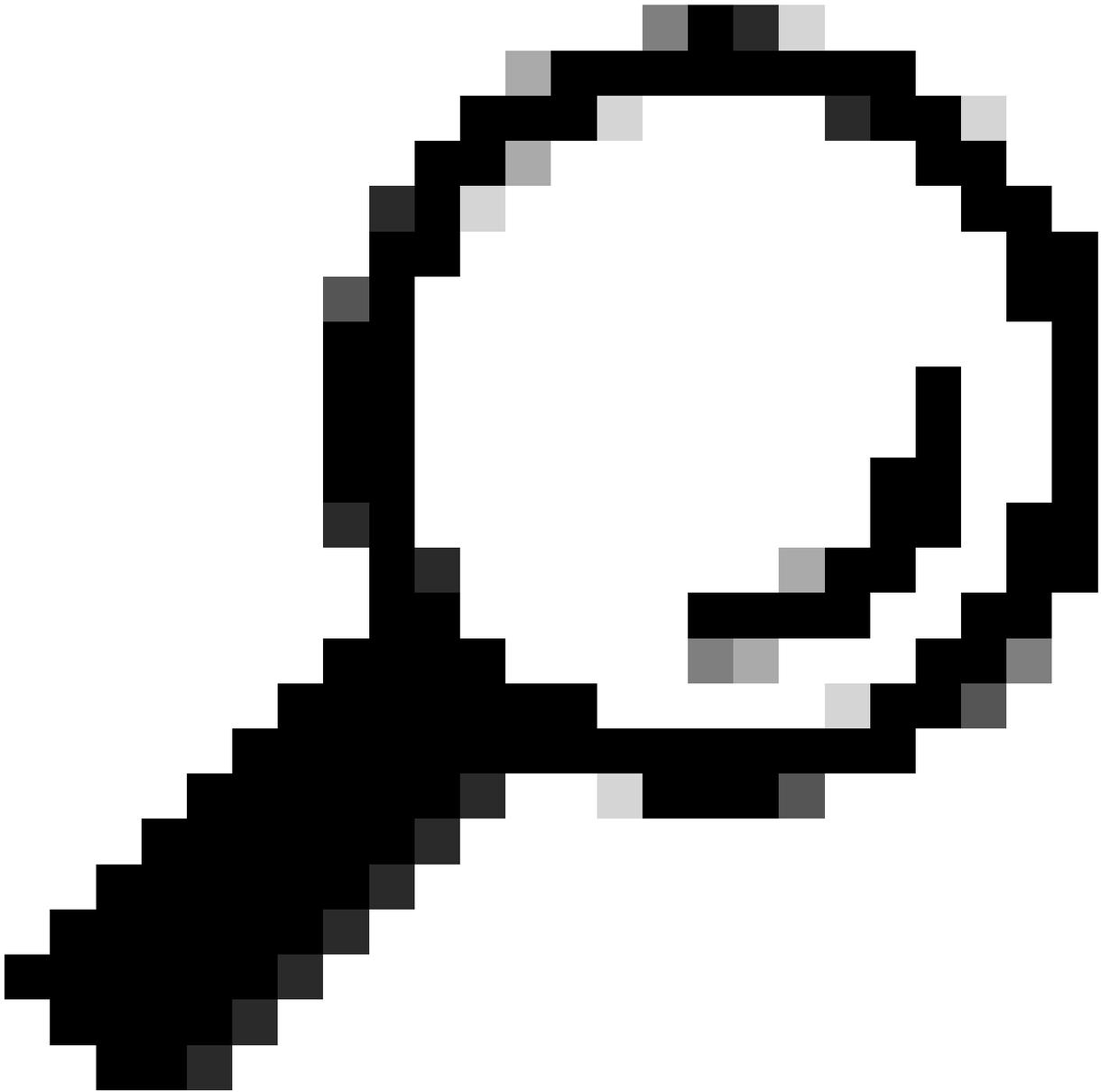
Policy Sets -> Default

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access [ ] [ ] +	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints [ ] [ ] > Options	4556	[ ]
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores [ ] [ ] > Options	0	[ ]
✓	Default		All_User_ID_Stores [ ] [ ] Options [ ] If Auth fail REJECT [ ] [ ] If User not found REJECT [ ] [ ] If Process fail DROP [ ] [ ]	62816	[ ]



提示：在3个选项上配置的“拒绝”功能也有效

---

在默认策略集中，展开授权策略并选择添加图标以创建新的授权条件。

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<span>+</span>	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (25)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
<span>+</span>						

配置规则名称，并点击添加图标以配置条件。

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<span>+</span>	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (26)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
<span>+</span>	DNAC-SUPER-ADMIN-ROLE					

作为情况的一部分，请将其关联到步骤2中配置的网络设备IP地址。

# Conditions Studio

## Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- CY\_Campus
- CY\_CAMPUS\_MAC
- CY\_Campus\_voice
- CY\_Guest
- EAP-MSCHAPv2

## Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

点击保存。

将其另存为新的库条件，并根据需要为其命名，本例中将其命名为DNAC。

# Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list

Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

最后，配置在步骤3中创建的配置文件。

The screenshot shows the Cisco ISE Work Centers - Profiler interface. The top navigation bar includes 'Overview', 'Ext Id Sources', 'Network Devices', 'Endpoint Classification', 'Node Config', 'Feeds', 'Manual Scans', 'Policy Elements', 'Profiling Policies', and 'More'. The main content area is titled 'Policy Sets -> Default' and features a table with columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', and 'Hits'. A search bar is present above the table. The table lists a 'Default' policy set with a status of 'On' and 180617 hits. Below the table, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (25)'. The 'Authorization Policy (25)' section is expanded, showing a table with columns for 'Status', 'Rule Name', 'Conditions', 'Profiles', 'Security Groups', 'Hits', and 'Actions'. A search bar is also present above this table. The first row in this table shows a rule named 'DNAC-SUPER-ADMIN-ROLE' with conditions 'DNAC' and a profile 'DNAC\_AUTH\_PROFILE'. The 'Update' button is highlighted with a red box.

单击Save。

第五步：登录Cisco DNA Center GUI并导航到System > Users & Roles > External Authentication。

单击Enable External User选项，并将AAA Attribute设置为Cisco-AVPair。

The screenshot shows the Cisco DNA Center System / Users & Roles External Authentication configuration page. The left sidebar contains 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and contains the following text: 'Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo it needs to be configured here on Cisco DNA Center.' Below this text, there are two paragraphs of explanatory text. The first paragraph states: '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 cist attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".' The second paragraph states: 'An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".' Below the text, there is a checkbox labeled 'Enable External User' which is checked. Below this, there is a section titled 'AAA Attribute' with a dropdown menu showing 'Cisco-AVPair'. At the bottom, there are two buttons: 'Reset to Default' and 'Update'. The 'Update' button is highlighted with a red box.



注意：ISE服务器在后端使用属性Cisco-AVPair，因此第3步上的配置有效。

---

向下滚动以查看AAA服务器配置部分。在第1步中配置ISE服务器的IP地址并在第3步中配置共享密钥。

然后单击View Advanced Settings。

∨ AAA Server(s)

### Primary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

[View Advanced Settings](#)

Update

### Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

[View Advanced Settings](#)

Update

确认已选中RADIUS选项，并在两台服务器上单击Update按钮。

∨ AAA Server(s)

### Primary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS  TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

### Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS  TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

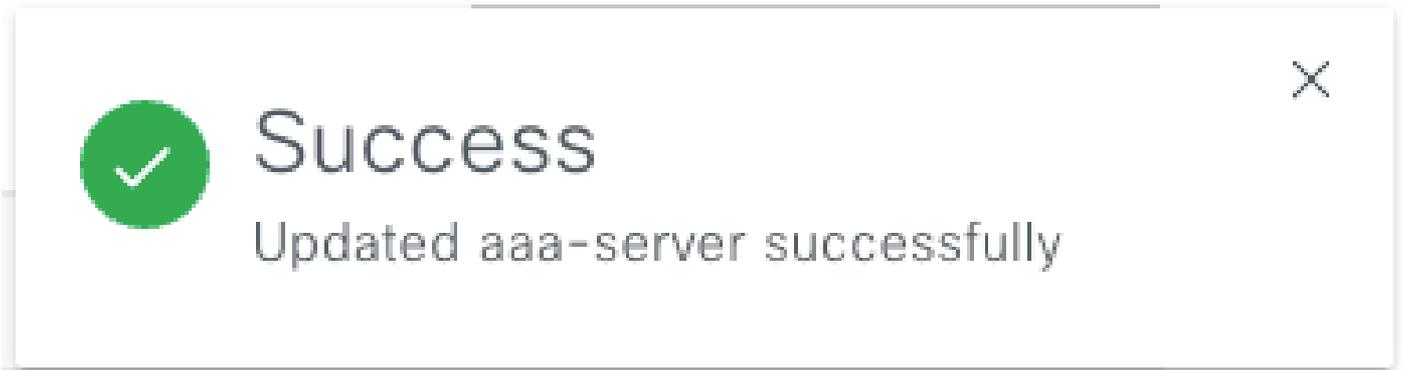
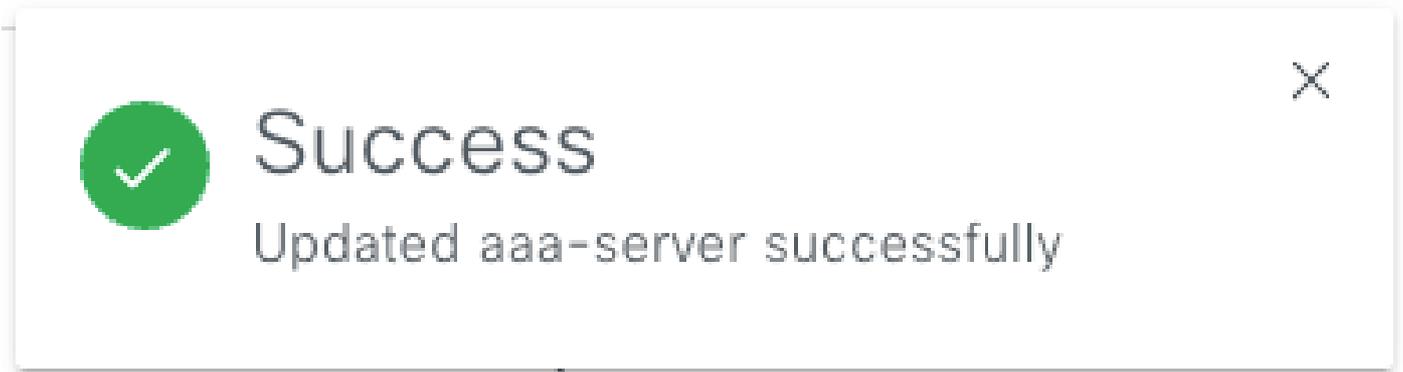
Timeout (seconds)

4

Update

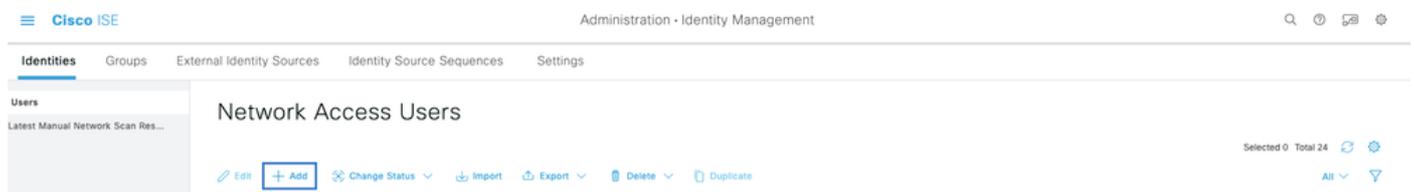
Update

您必须看到每个成功消息。



现在您可以使用在ISE菜单>管理>身份管理>身份>用户下创建的任何ISE身份登录。

如果您没有创建任何应用，请登录ISE，导航到上面的路径，然后添加新的网络访问用户。



## 验证

加载Cisco DNA Center GUI 并使用来自ISE身份的用户登录。



# Cisco DNA Center

The bridge to possible

✓ Success!

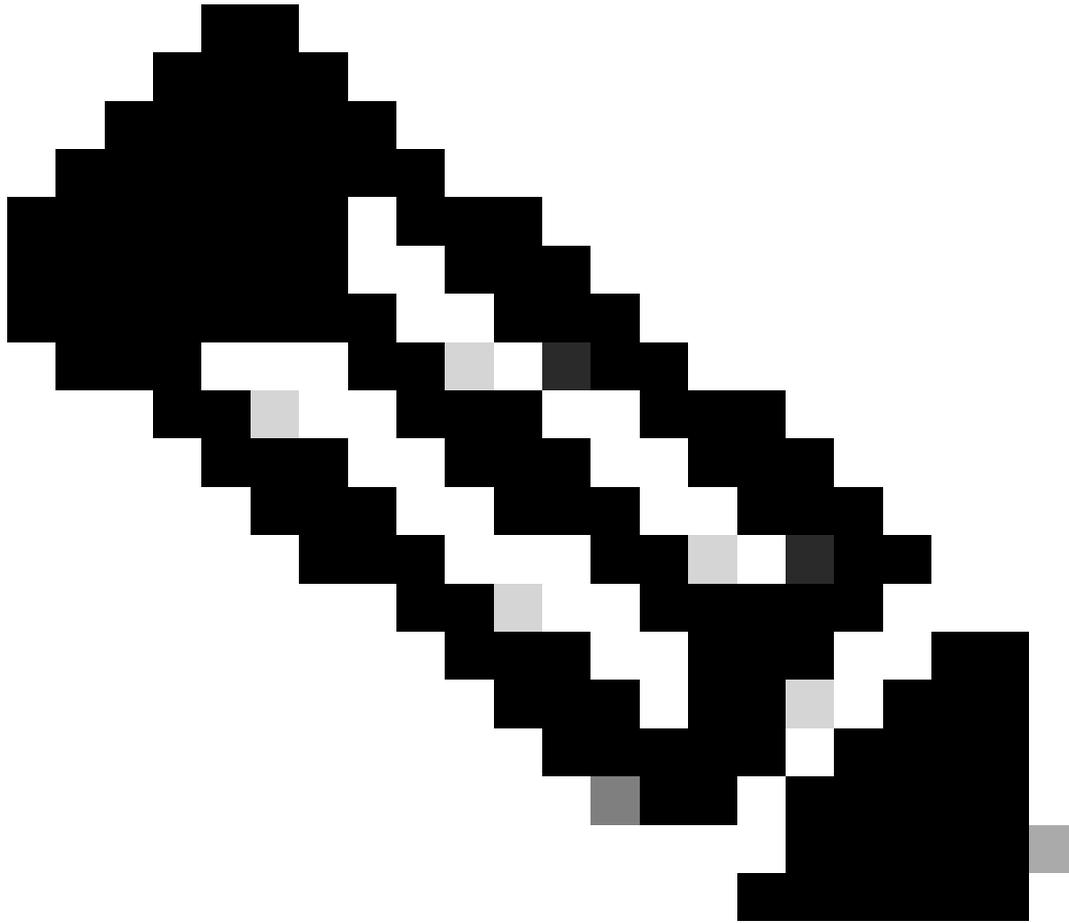
Username

test

Password

.....

Log In



注意：ISE身份上的任何用户现在都可以登录。您可以向ISE服务器上的身份验证规则添加更精细的粒度。

---

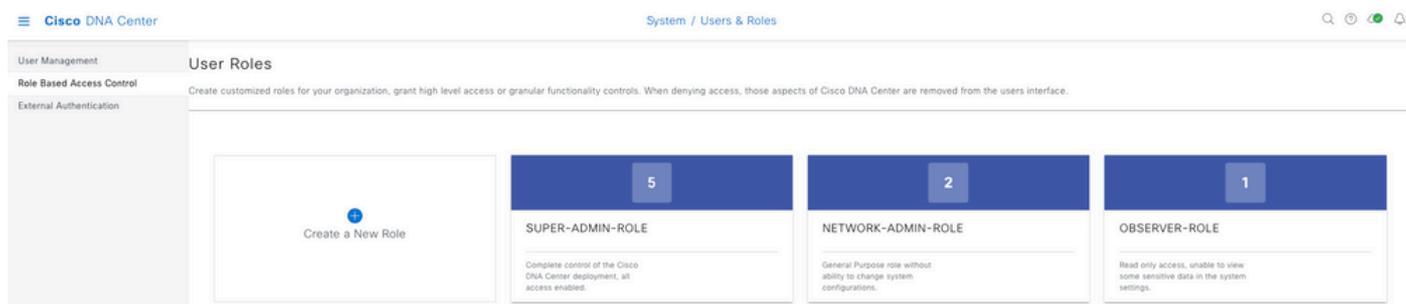
登录成功后，用户名会显示在Cisco DNA Center GUI上

## Welcome, test

欢迎屏幕

### 更多角色

您可以对Cisco DNA Center上的每个角色重复这些步骤，因为我们默认拥有：SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE和OBSERVER-ROLE。



在本文档中，我们使用SUPER-ADMIN-ROLE角色示例，但您可以在ISE上为Cisco DNA Center中的每个角色配置一个授权配置文件，唯一的考虑事项是在第3步配置的角色需要与Cisco DNA Center上的角色名称完全匹配（区分大小写）。

## 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）。