在9800 WLC上配置RADIUS &； TACACS+ for GUI &； CLI身份验证

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 只读用户限制
- 为WLC配置RADIUS身份验证
- 为RADIUS配置ISE
- 配置TACACS+ WLC
- TACACS+ ISE配置

故障排除

- 故障排除WLC GUI或通过WLC CLI的CLI RADIUS/TACACS+访问
- 排除通过ISE GUI的WLC GUI或CLITACACS+访问故障

简介

本文档介绍如何为RADIUS或TACACS+外部身份验证配置Catalyst 9800。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst Wireless 9800配置型号
- AAA、RADIUS和TACACS+概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C9800-CL v17.9.2
- ISE 3.2.0

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。

背景信息

当用户尝试访问CLI或WLC的GUI时，系统会提示他们输入用户名和密码。默认情况下，这些凭证会与设备自身中存在的本地用户数据库进行比较。或者，可以指示WLC将输入凭证与远程AAA服务器进行比较：WLC可以使用RADIUS或TACACS+与服务器通信。

配置

在本示例中，在AAA服务器(ISE)上分别配置了adminuser和helpdeskuser两种类型的用户。这些用户分别是admin-group和helpdesk-group组的一部分。 用户adminuser(admin-group的一部分)应被授予对WLC的完全访问权限。另一方面，helpdesk-group的helpdeskuser部分旨在仅向WLC授予监控器权限。因此，没有配置访问权限。

本文先配置WLC和ISE进行RADIUS身份验证，然后对TACACS+执行相同操作。

只读用户限制

当TACACS+或RADIUS用于9800 WebUI身份验证时，存在以下限制：

- 权限级别为0的用户存在，但无权访问GUI
- 权限级别为1到14的用户只能查看Monitor选项卡（这相当于本地身份验证的只读用户的权限级别）
- 权限级别为15的用户具有完全访问权限
- 不支持权限级别为15的用户以及仅允许特定命令的命令集。用户仍然可以通过WebUI执行配置更改

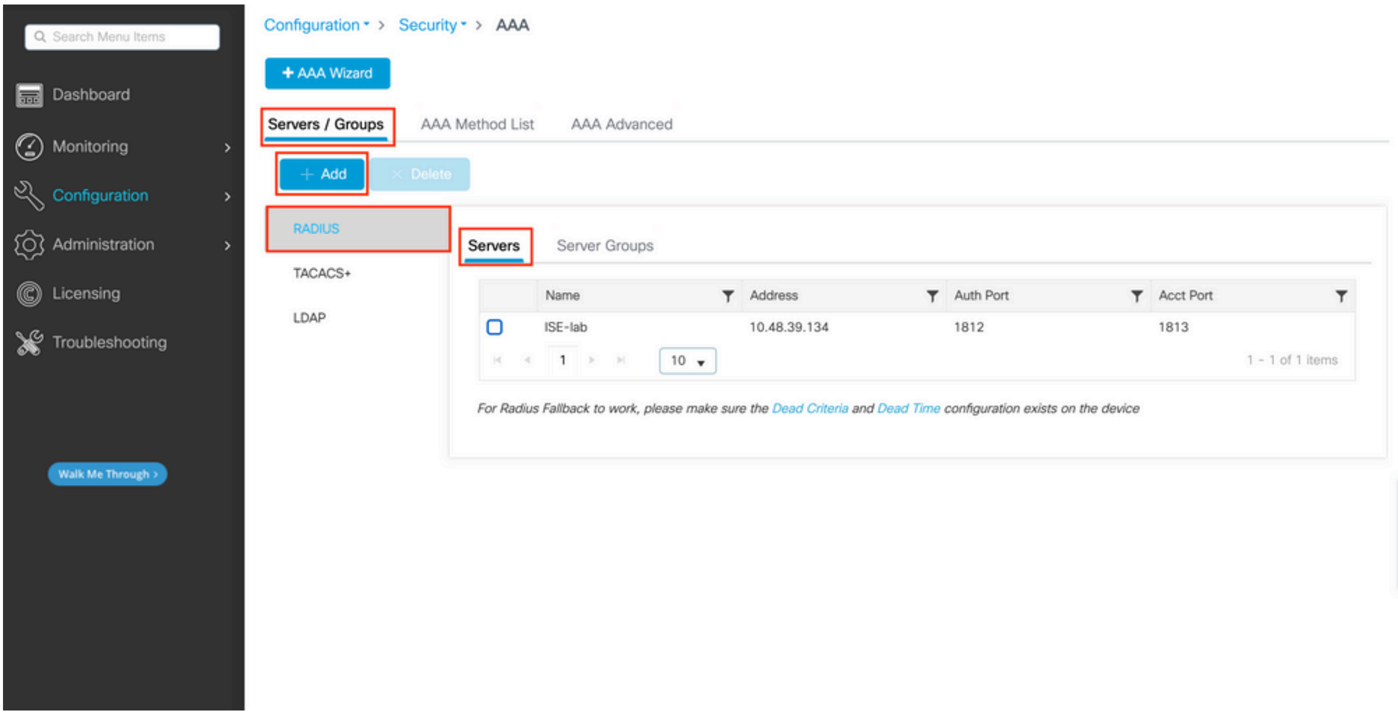
不能更改或修改这些注意事项。

为WLC配置RADIUS身份验证

步骤1:声明RADIUS服务器。

在GUI中：

首先，在WLC上创建ISE RADIUS服务器。 这可以在GUI WLC页面的选项卡Servers/Groups > RADIUS > Servers中完成(用https://<WLC-IP>/webui/#/aaa访问)，或者导航到Configuration > Security > AAA(如下图所示)。

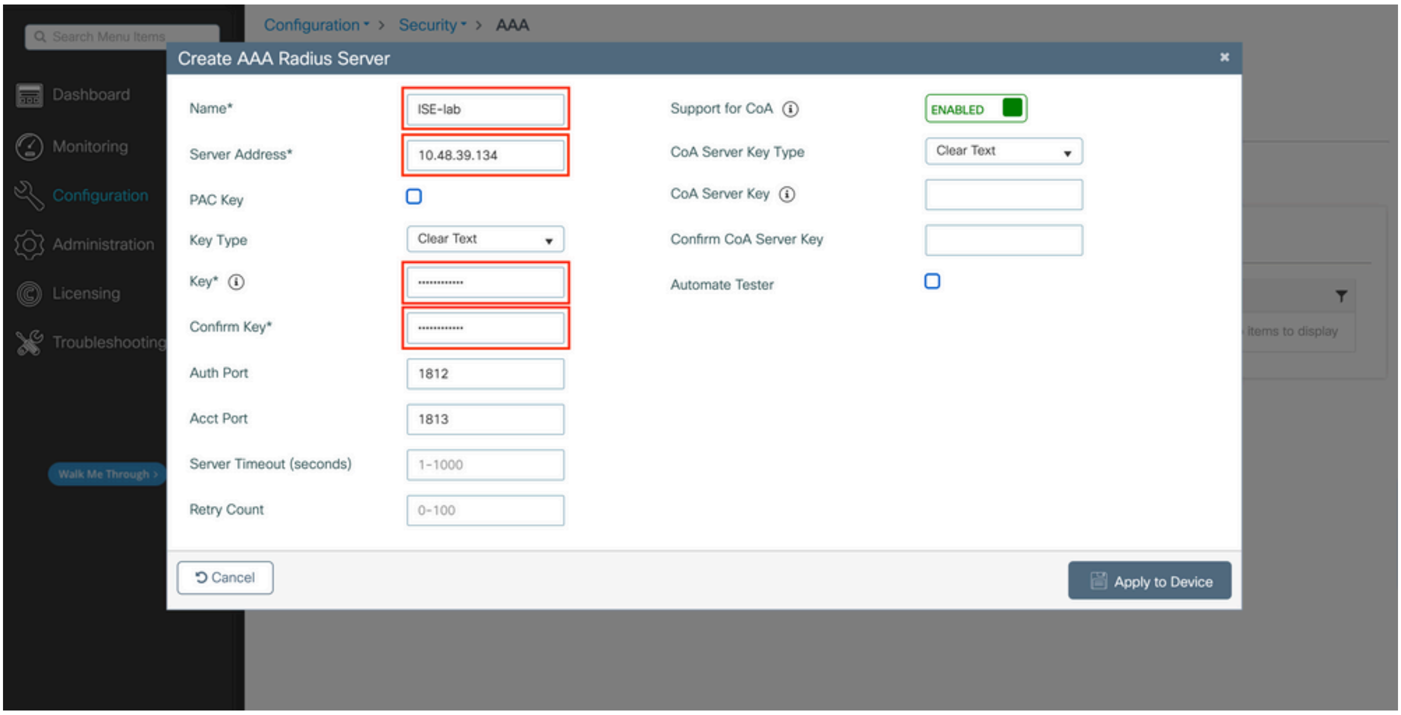


	Name	Address	Auth Port	Acct Port
□	ISE-lab	10.48.39.134	1812	1813

1 - 1 of 1 items

For Radius Fallback to work, please make sure the Dead Criteria and Dead Time configuration exists on the device

要在WLC上添加RADIUS服务器，请单击映像中以红色框显示的Add按钮。这将打开屏幕截图中所示的弹出窗口。



Name*	ISE-lab	Support for CoA	ENABLED
Server Address*	10.48.39.134	CoA Server Key Type	Clear Text
PAC Key	□	CoA Server Key	
Key Type	Clear Text	Confirm CoA Server Key	
Key*	············	Automate Tester	□
Confirm Key*	············		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

在此弹出窗口中，必须提供：

- 服务器名称（请注意，不必与ISE系统名称匹配）
- 服务器IP地址
- WLC和RADIUS服务器之间的共享密钥

可以配置其他参数，例如用于身份验证和记账的端口，但这些不是必需的，保留为本文档的默认设置。

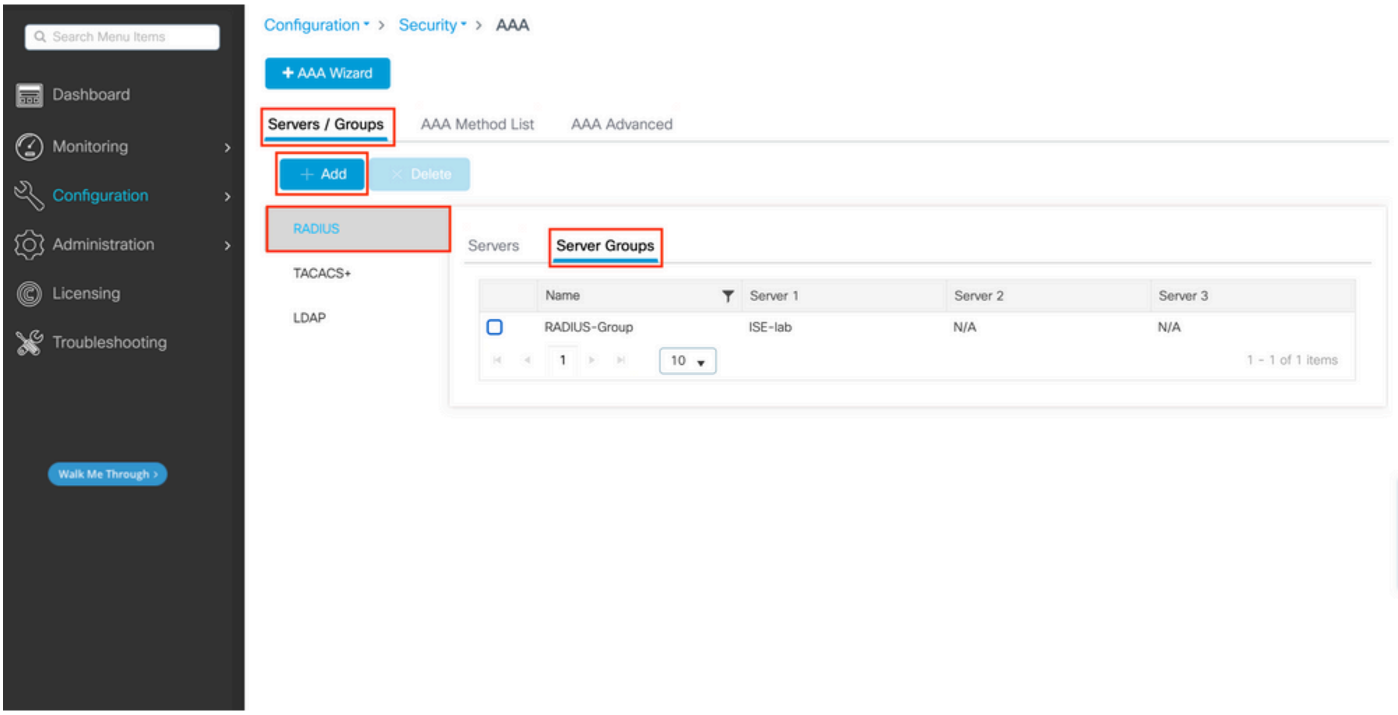
从CLI：

```
<#root>

WLC-9800(config)#radius server

ISE-lab

 WLC-9800(config-radius-server)#address ipv4

10.48.39.134

auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Cisco123
```

第二步：将RADIUS服务器映射到服务器组。

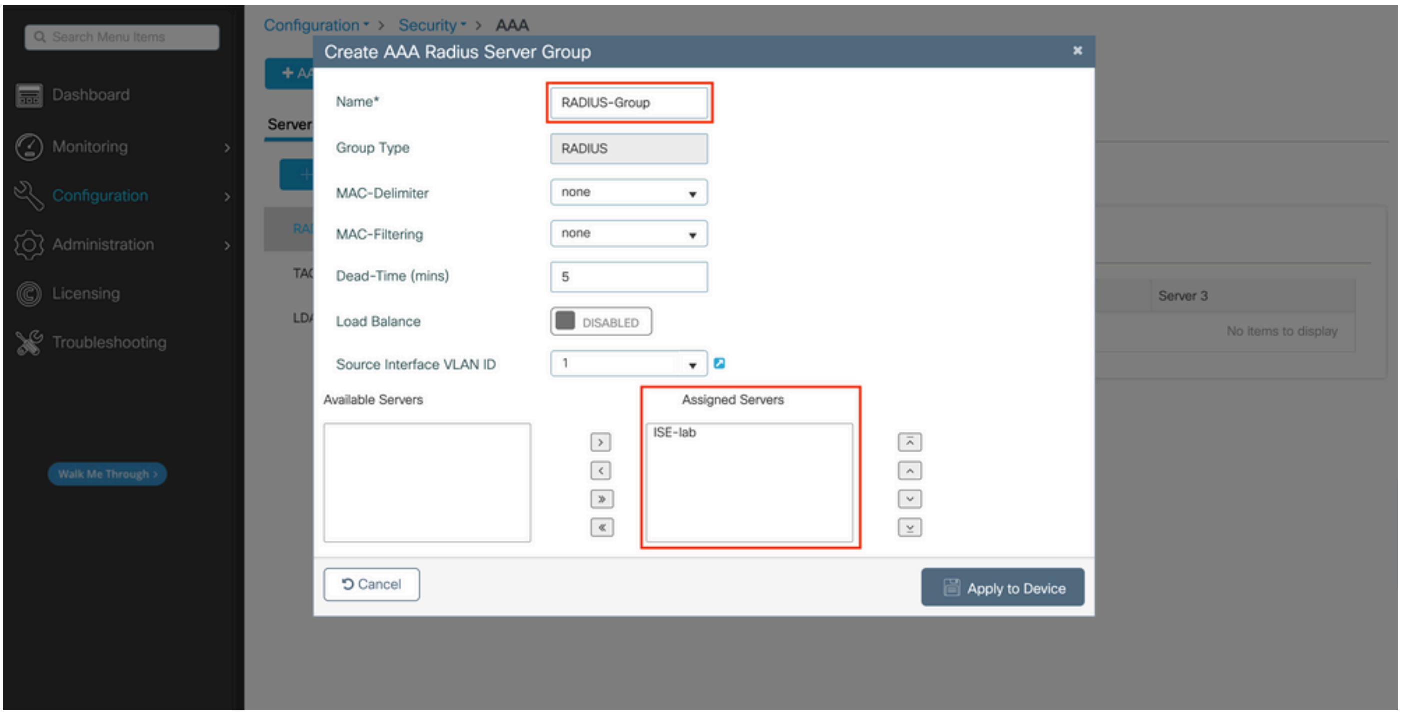
在GUI中：

如果您有多个可用于身份验证的RADIUS服务器，建议将这些服务器映射到同一服务器组。WLC负责对服务器组中的服务器之间的不同身份验证进行负载均衡。RADIUS服务器组在Servers/Groups > RADIUS > Server Groups选项卡的GUI页面上配置，与步骤1中提到的相同，如图所示。



	Name	Server 1	Server 2	Server 3
□	RADIUS-Group	ISE-lab	N/A	N/A

对于服务器的创建，当您点击Add按钮（框定在上一个图像中）时，会出现一个弹出窗口，如下图所示。



Create AAA Radius Server Group

Name* RADIUS-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 5

Load Balance DISABLED

Source Interface VLAN ID 1

Available Servers

Assigned Servers: ISE-lab

Cancel

Apply to Device

在弹出窗口中，为组提供一个名称，并将所需服务器移至Assigned Servers列表。

从CLI：

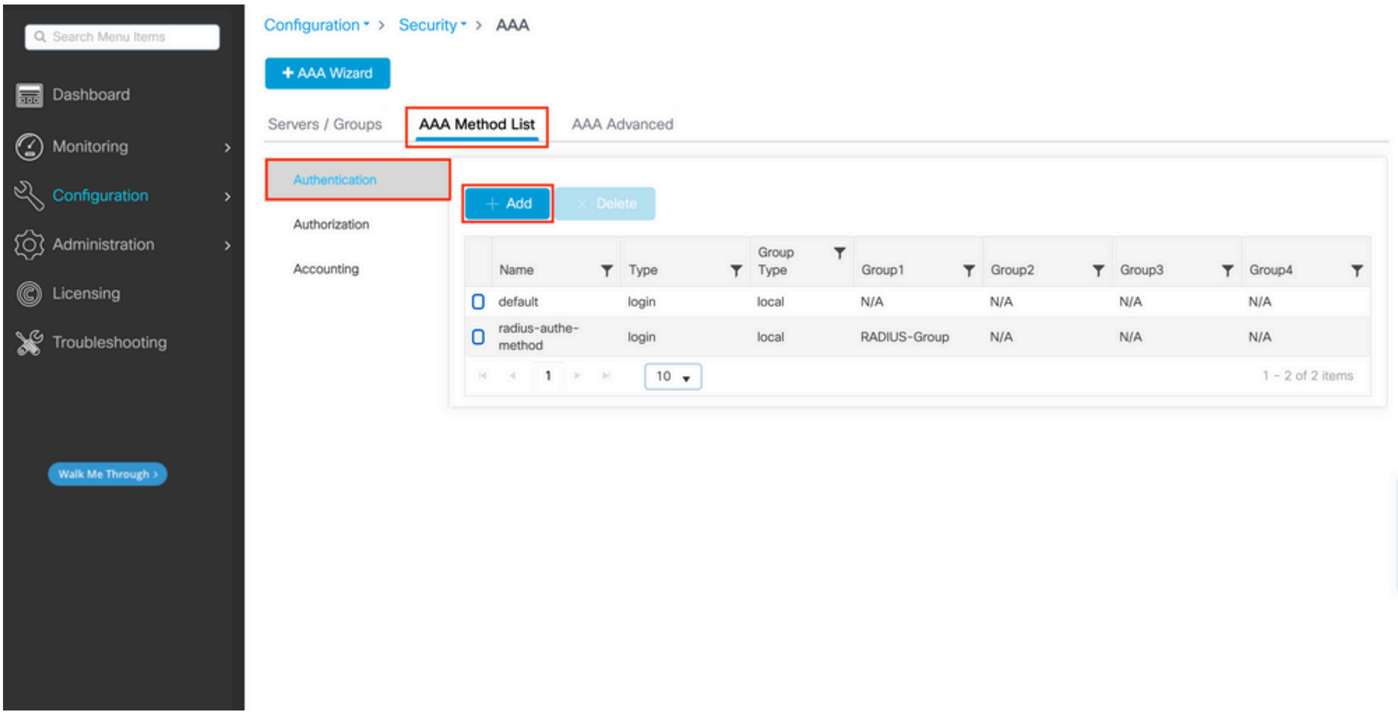
```
<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

WLC-9800(config-sg-radius)# server name

ISE-lab
```

-

第三步：创建指向RADIUS服务器组的AAA身份验证登录方法。

在GUI中：

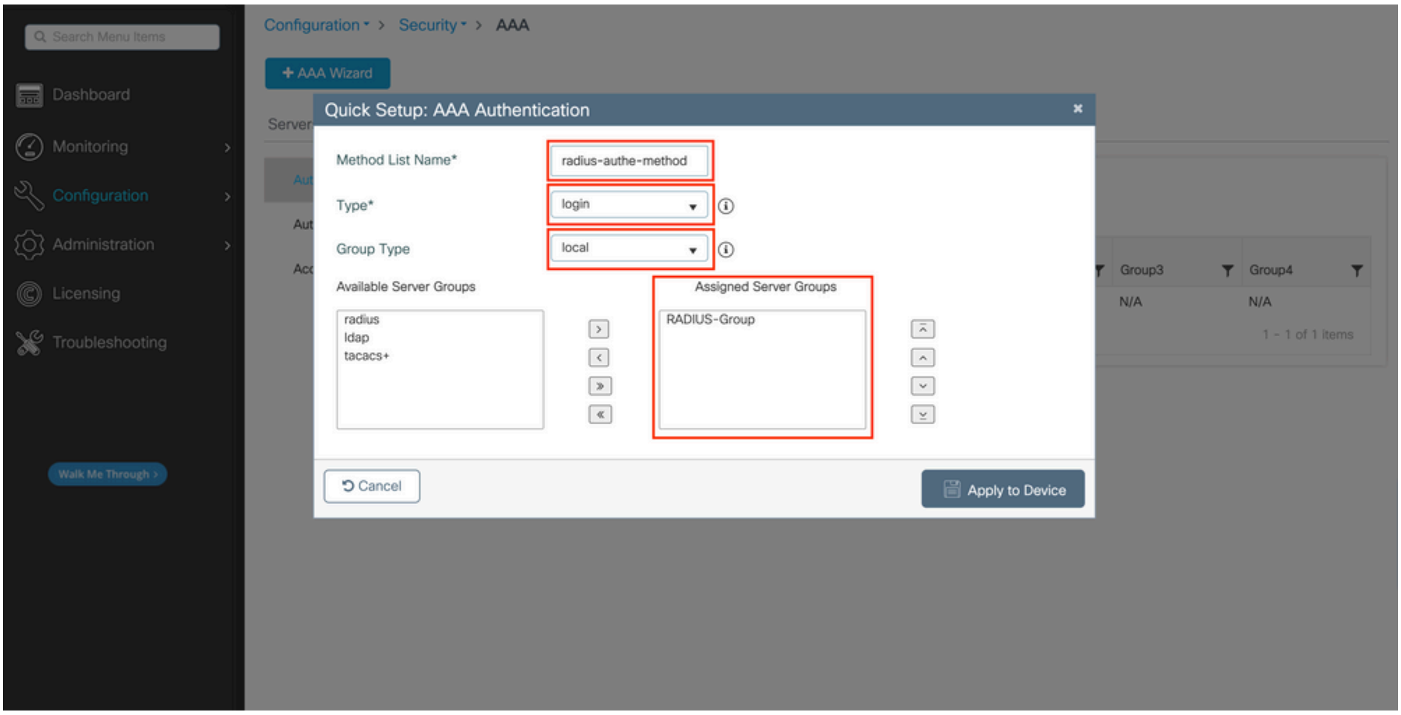
仍在GUI页面上https://<WLC-IP>/webui/#/aaa，导航至AAA Method List > Authentication选项卡，然后创建身份验证方法，如此图中所示。



	Name	Type	Group Type	Group1	Group2	Group3	Group4
○	default	login	local	N/A	N/A	N/A	N/A
○	radius-authe-method	login	local	RADIUS-Group	N/A	N/A	N/A

1 - 2 of 2 items

与往常一样，使用Add按钮创建身份验证方法时，系统会显示配置弹出窗口，类似于下图中所示的窗口。



Method List Name* radius-authe-method

Type* login

Group Type local

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: RADIUS-Group

在此弹出窗口中，为方法提供一个名称。选择Type(作为登录)，将在上一步中创建的组服务器添加到Assigned Server Groups列表中。对于Group Type字段，可以进行几种配置。

- 如果您选择Group Type作为local，则WLC首先检查用户凭证是否存在于本地，然后回退到服务器组。

- 如果您选择Group Type作为组并且不选中Fall back to local选项，则WLC仅检查服务器组的用户凭证。

- 如果您选择Group Type作为组并选中Fallback to local选项，则WLC将根据服务器组检查用户凭证，并且仅在服务器未响应时查询本地数据库。如果服务器发送reject消息，则将对用户进行身份验证，即使它可能存在于本地数据库中。

从CLI：

如果您希望只有在首先在本地未找到用户凭证的情况下才使用服务器组检查用户凭证，请使用：

```
<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

 local group

RADIUS-Group
```

如果您希望仅对服务器组检查用户凭证，请使用：

```
<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method
```

```
 group
```

RADIUS-Group

如果要对服务器组检查用户凭证，并且最后不响应本地条目，请使用：

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

```
 group
```

RADIUS-Group

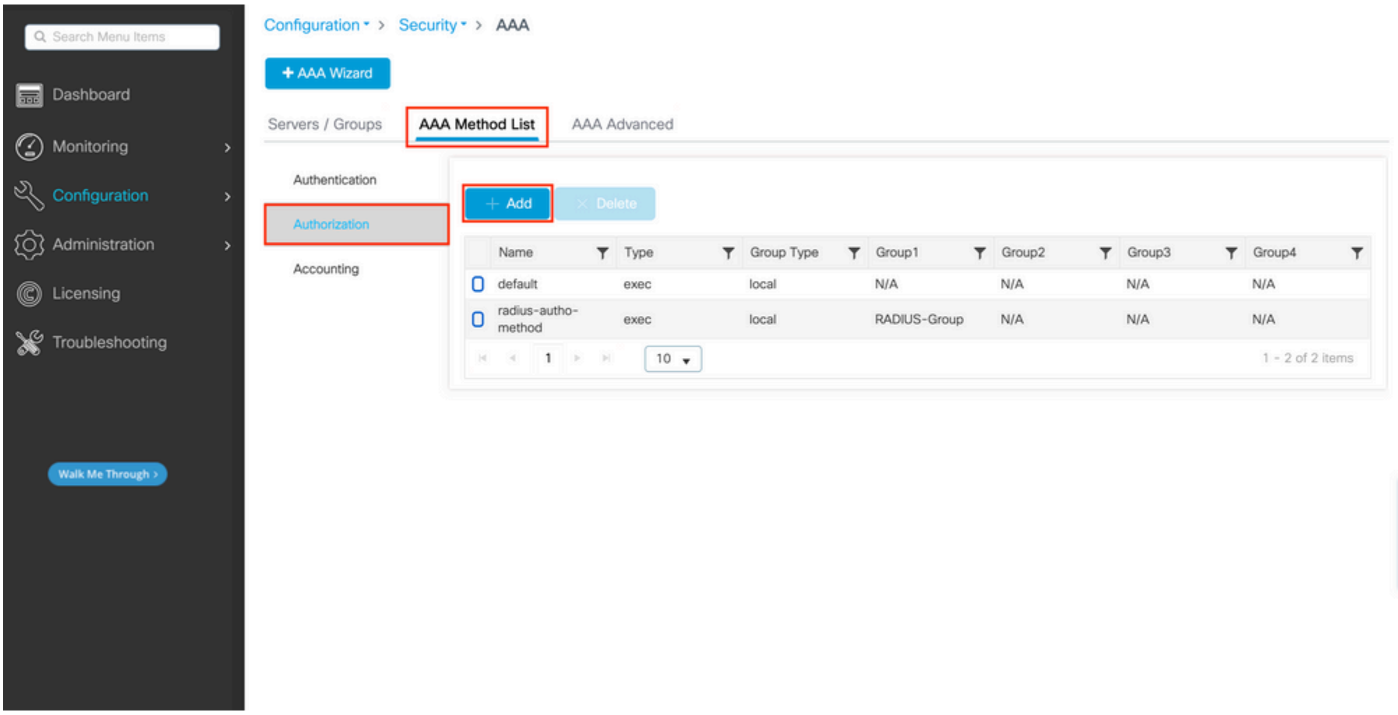
```
 local
```

在此示例设置中，有些用户仅在本机创建，而有些用户仅在ISE服务器上创建，因此，请使用第一个选项。

第四步：创建指向RADIUS服务器组的AAA授权exec方法。

在GUI中：

用户还必须获得授权才能获得访问权限。仍然可以从GUI Page Configuration > Security > AAA中，导航到AAA Method List > Authorization选项卡，然后创建授权方法，如此图中所示。

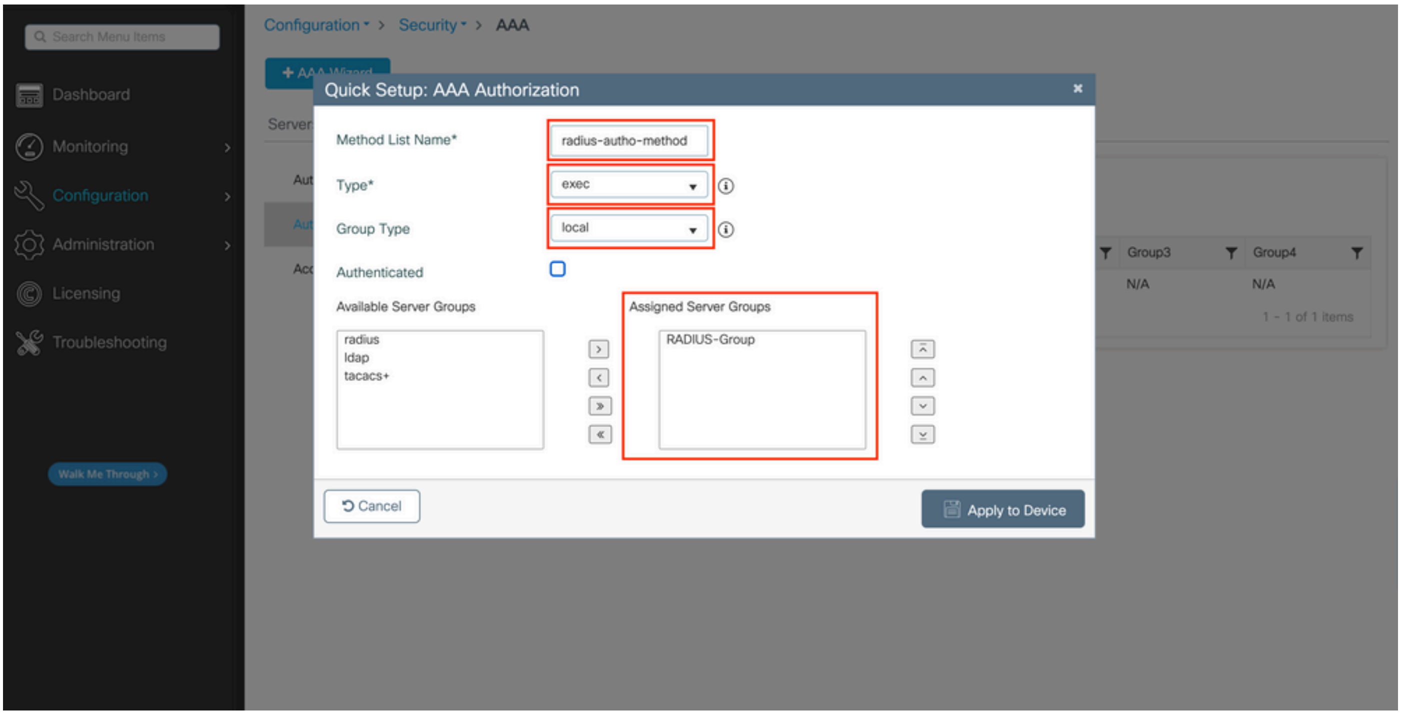


	Name	Type	Group Type	Group1	Group2	Group3	Group4
☐	default	exec	local	N/A	N/A	N/A	N/A
☐	radius-autho-method	exec	local	RADIUS-Group	N/A	N/A	N/A

1 - 2 of 2 items

授权方法创建

当您使用Add按钮添加新授权方法时，会显示与所描述授权方法配置类似的弹出窗口。



Quick Setup: AAA Authorization

Method List Name* radius-autho-method

Type* exec

Group Type local

Authenticated ☐

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: RADIUS-Group

在此配置弹出窗口中，为授权方法提供一个名称，选择Type作为exec，并使用与步骤3中用于身份验证方法的组类型顺序相同的组类型。

从CLI：

对于身份验证方法，首先分配授权以根据本地条目检查用户，然后根据服务器组中的条目检查用户。

<#root>

```
WLC-9800(config)#aaa authorization exec
```

```
radius-autho-method
```

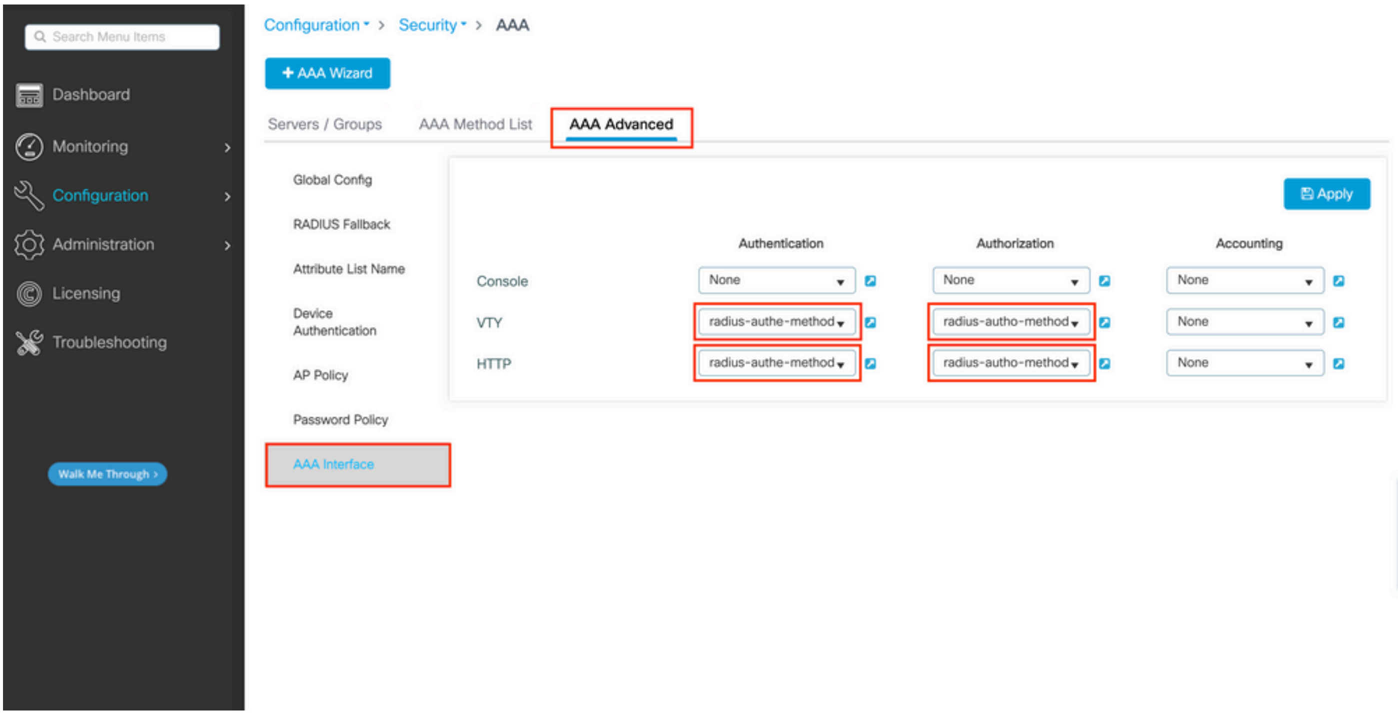
```
 local group
```

```
RADIUS-Group
```

第五步：将方法分配给HTTP配置和用于Telnet/SSH的VTY线路。

在GUI中：

创建的身份验证和授权方法可用于HTTP和/或Telnet/SSH用户连接，从AAA Advanced > AAA Interface选项卡可以配置该连接，但该选项卡仍可从GUI WLC页(可在https://<WLC-IP>/webui/#/aaa中访问)访问，如下图所示：



	Authentication	Authorization	Accounting
Console	None	None	None
VTY	radius-authe-method	radius-autho-method	None
HTTP	radius-authe-method	radius-autho-method	None

用于GUI身份验证的CLI：

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

radius-autho-method

Telnet/SSH身份验证的CLI：

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

```
WLC-9800(config-line)#authorization exec
```

radius-autho-method

请注意，当对HTTP配置执行更改时，最好重新启动HTTP和HTTPS服务。可以使用以下命令实现此目的：

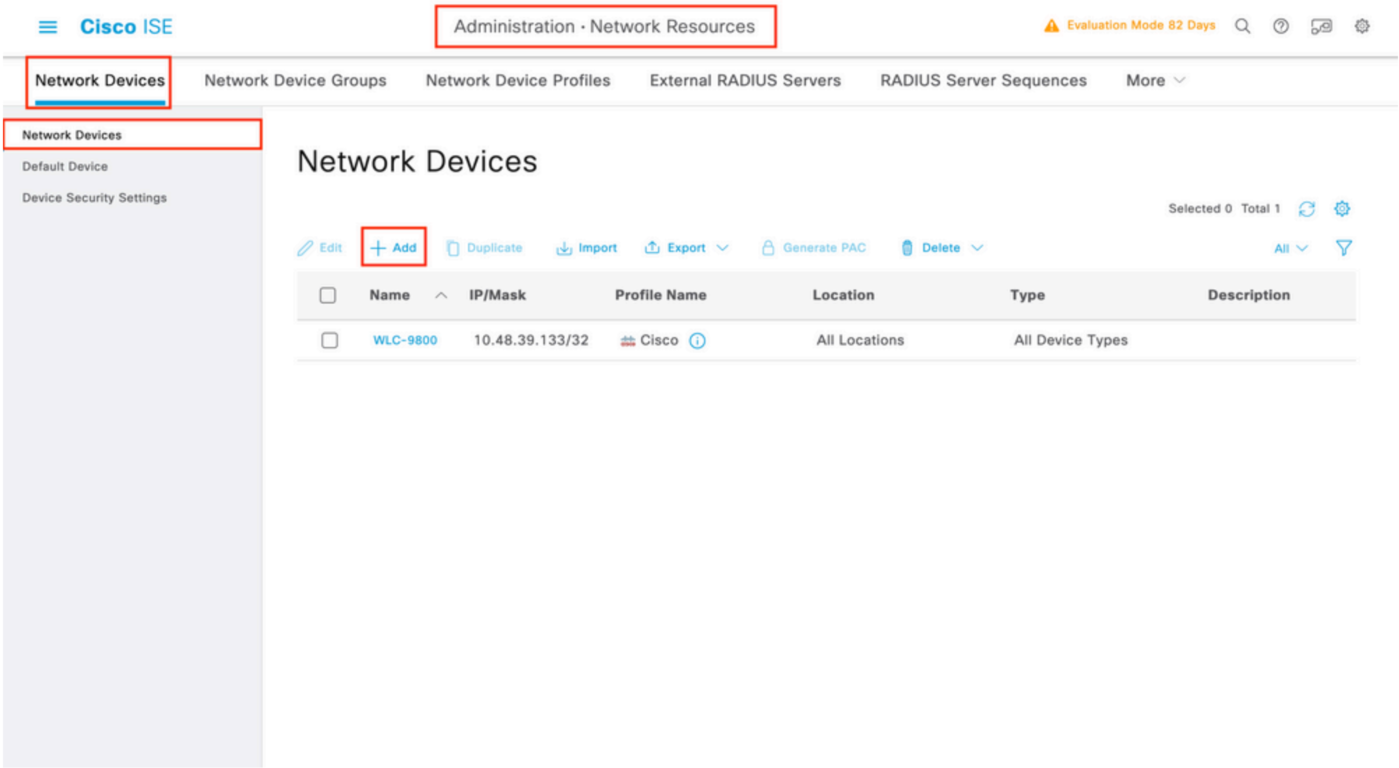
```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-serv
```

为RADIUS配置ISE

步骤1:将WLC配置为RADIUS的网络设备。

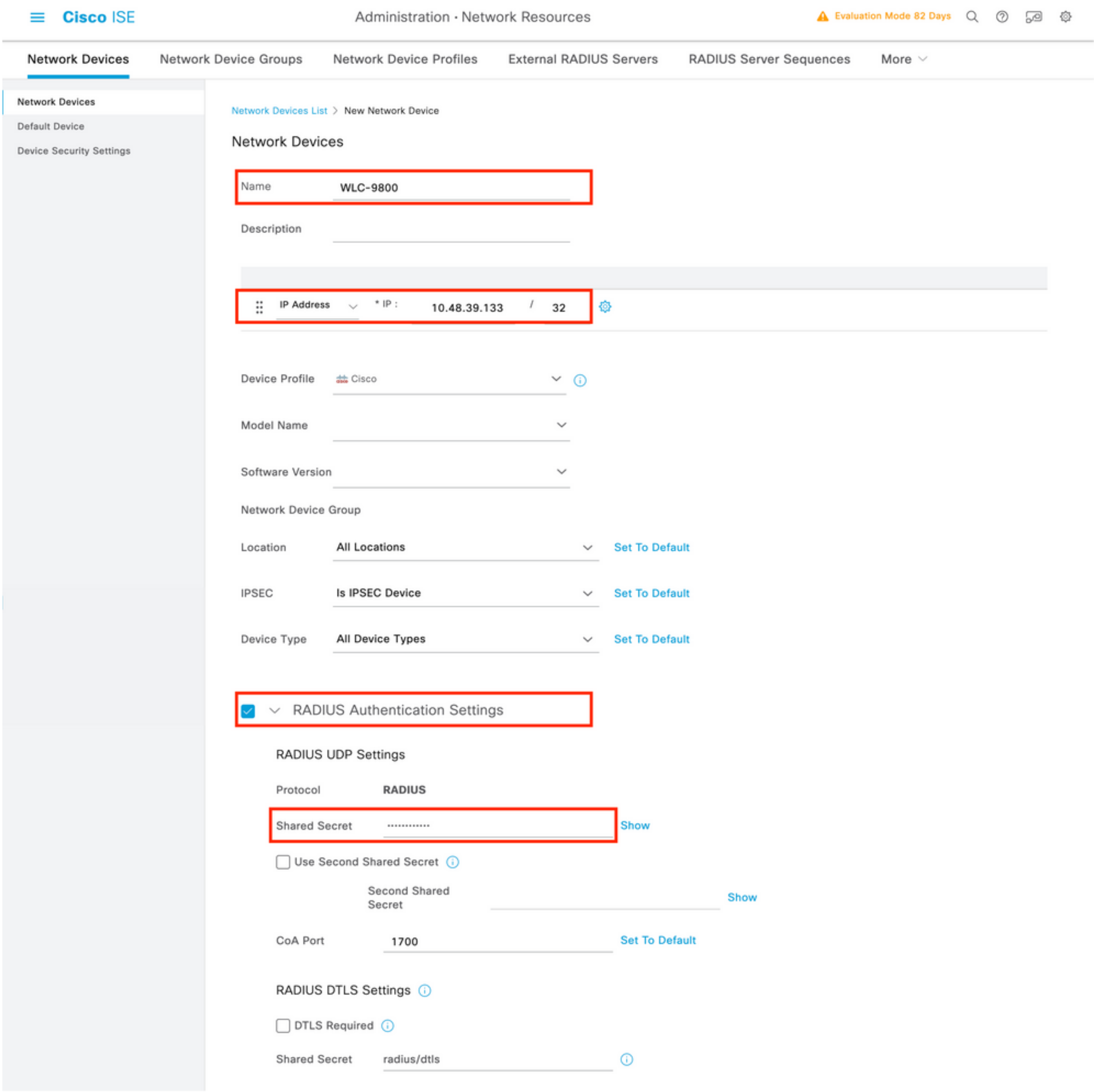
在GUI中：

要声明上一节中使用的WLC是ISE中的RADIUS网络设备，请导航到Administration > Network Ressources > Network Devices(默认)并打开Network devices（网络设备）选项卡，如下一图所示。



☐	Name	IP/Mask	Profile Name	Location	Type	Description
☐	WLC-9800	10.48.39.133/32	Cisco	All Locations	All Device Types	

要添加网络设备，请使用Add按钮，该按钮将打开新的网络设备配置表。



Network Devices

Name: WLC-9800

Description:

IP Address * IP : 10.48.39.133 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ············

□ Use Second Shared Secret

Second Shared Secret:

CoA Port: 1700

RADIUS DTLS Settings

□ DTLS Required

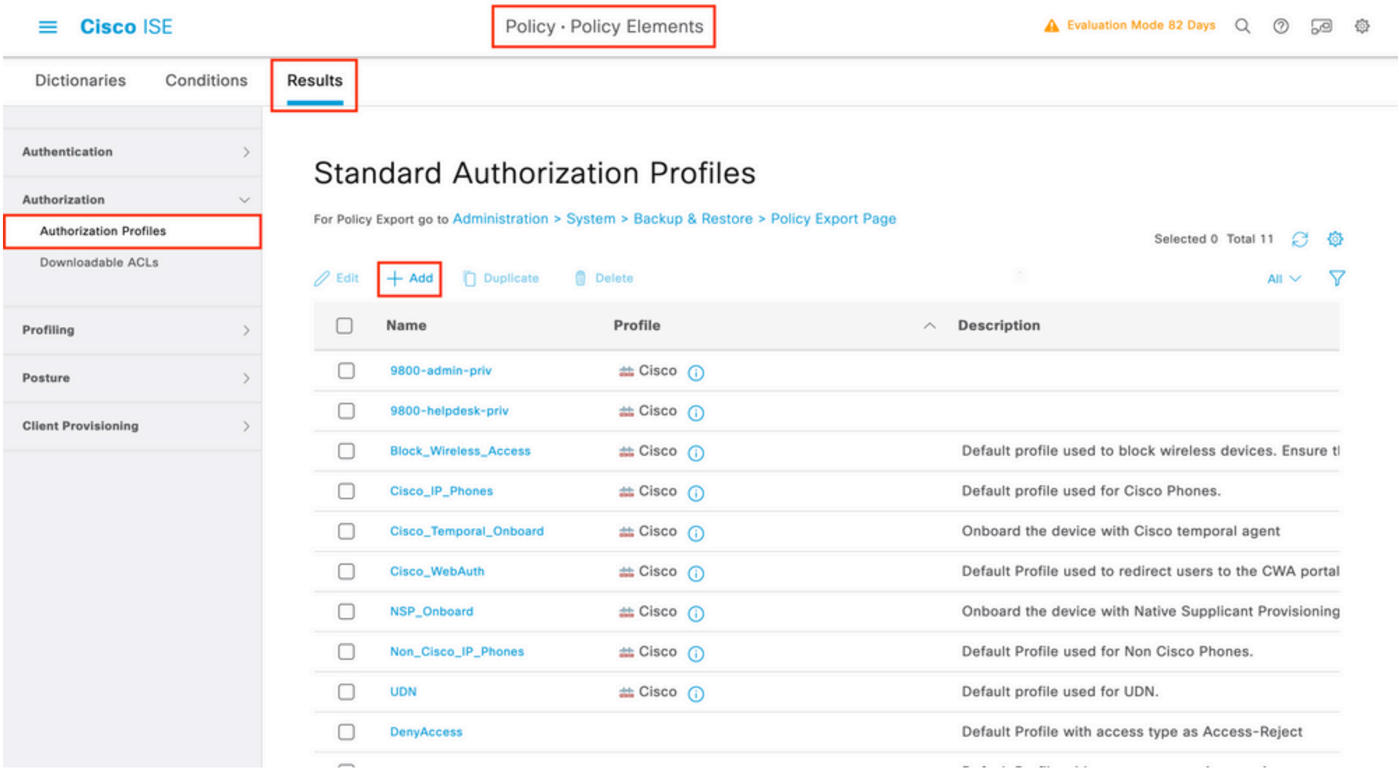
Shared Secret: radius/dtls

在新窗口中，为网络设备提供一个名称，并添加其IP地址。选择RADIUS身份验证设置并配置与WLC上使用的RADIUS共享密钥相同的RADIUS共享密钥。

第二步：创建授权结果，以返回权限。

在GUI中：

要获得管理员访问权限，adminuser的权限级别必须为15，以允许访问exec提示外壳。另一方面，helpdeskuser则不需要exec提示符外壳访问，因此可以分配权限级别低于15。要为用户分配适当的权限级别，可以使用授权配置文件。这些可以从ISE GUI Page Policy > Policy Elements > Results选项卡下的Authorization > Authorization Profiles配置（如下图所示）。



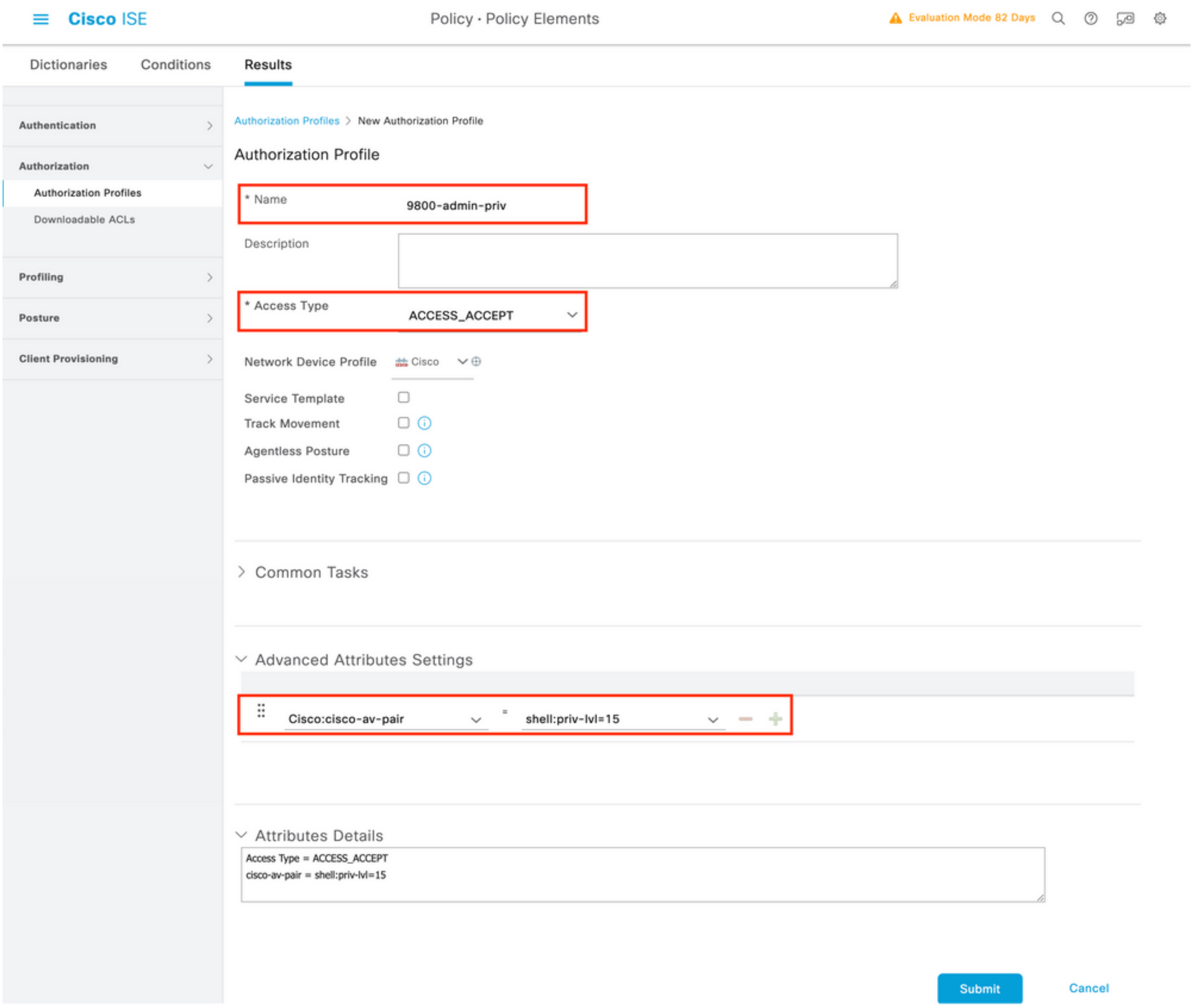
Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 11

	Name	Profile	Description
□	9800-admin-priv	Cisco	
□	9800-helpdesk-priv	Cisco	
□	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure tl
□	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
□	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
□	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
□	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
□	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
□	UDN	Cisco	Default profile used for UDN.
□	DenyAccess		Default Profile with access type as Access-Reject

要配置新的授权配置文件，请使用Add按钮，这将打开新的授权配置文件配置表。要配置分配给adminuser的配置文件，此表单必须尤其如下所示。



Authorization Profile

* Name 9800-admin-priv

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Cisco:cisco-av-pair = shell:priv-lvl=15

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15
```

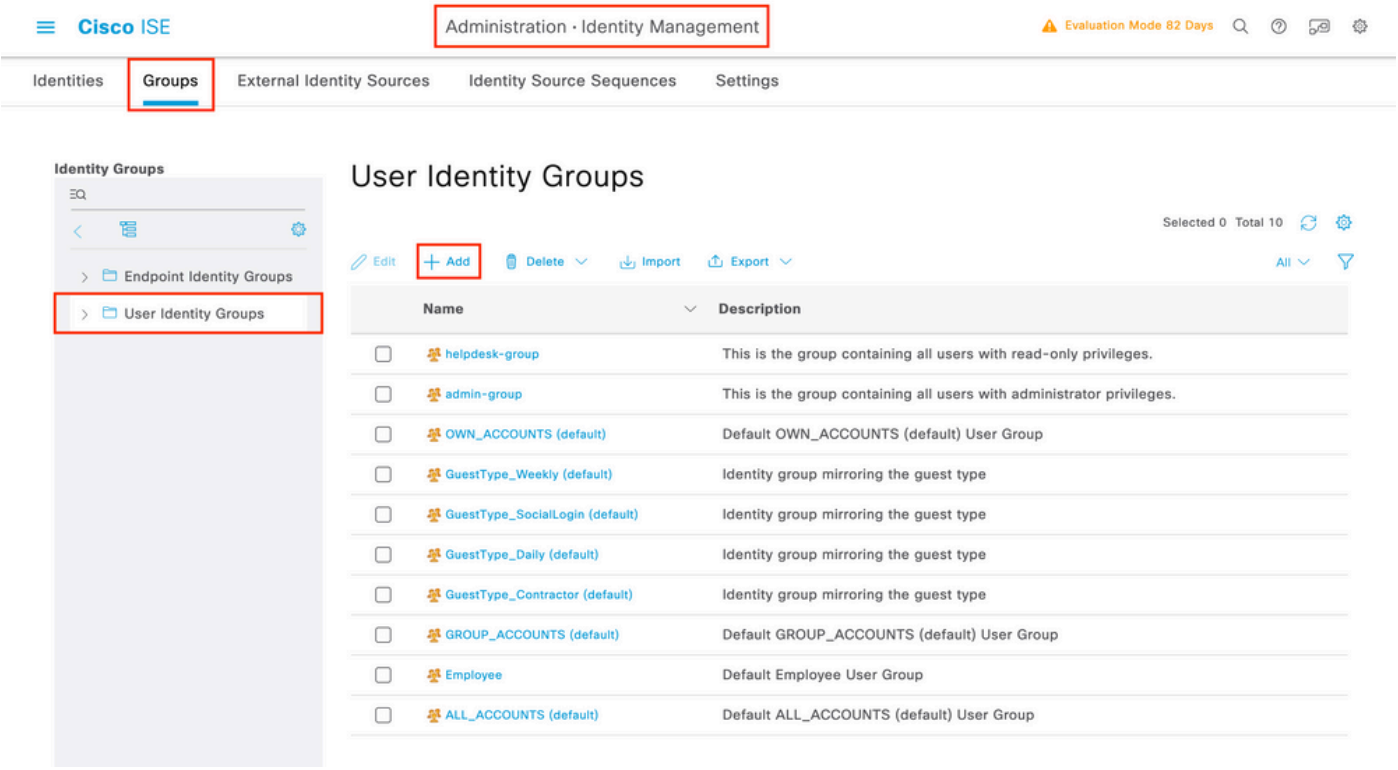
显示的配置将权限级别15授予与其关联的任何用户。如前所述，这是在下一步中创建的adminuser的预期行为。但是，helpdeskuser的权限级别必须较低，因此必须创建第二个策略元素。

helpdeskuser的策略元素与上面创建的策略元素相似，不同之处在于字符串必shell:priv-lvl=15 须更改为shell:priv-lvl=X，并将X替换为所需的权限级别。在本例中，使用1。

第三步：在ISE上创建用户组。

从 GUI：

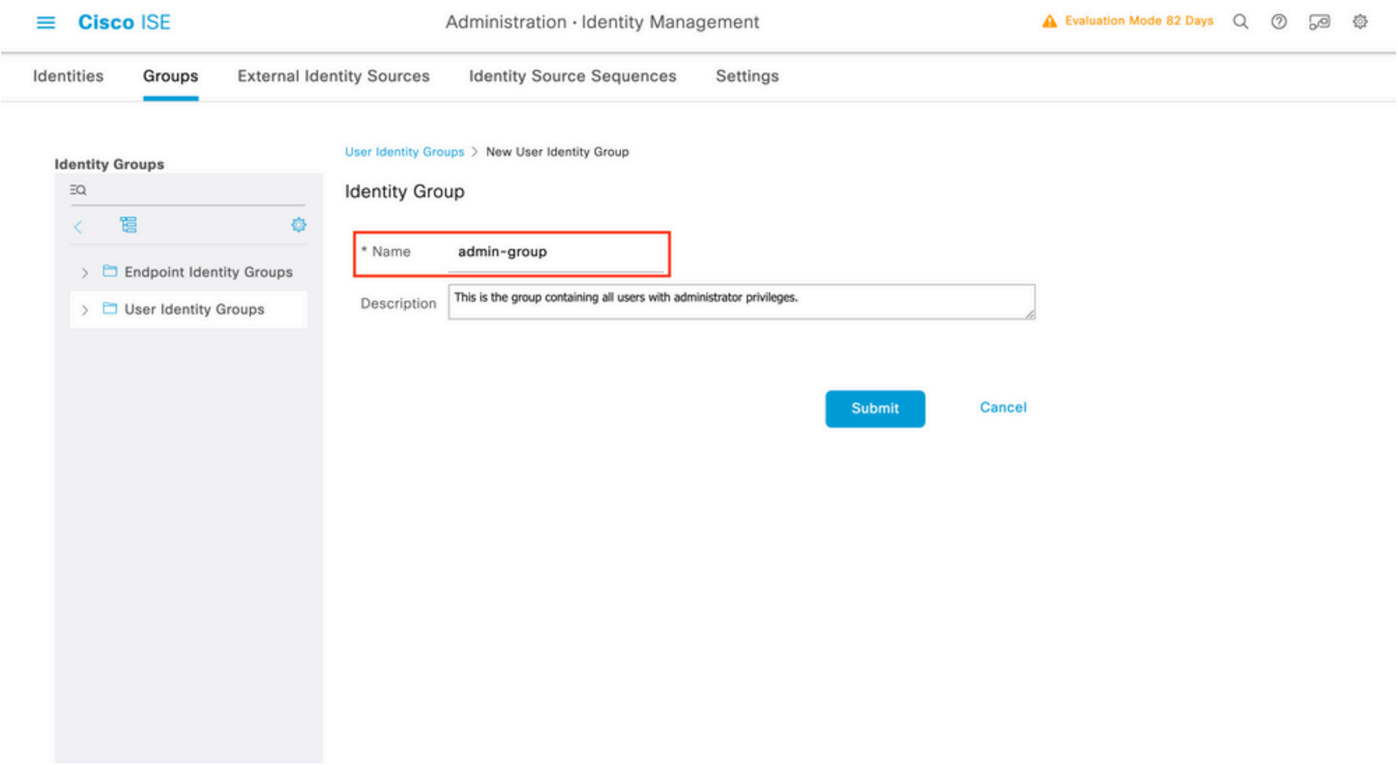
通过Administration > Identity Management > Groups GUI Page的User Identity Groups选项卡创建ISE用户组，如屏幕截图所示。



User Identity Groups

	Name	Description
□	helpdesk-group	This is the group containing all users with read-only privileges.
□	admin-group	This is the group containing all users with administrator privileges.
□	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
□	GuestType_Weekly (default)	Identity group mirroring the guest type
□	GuestType_SocialLogin (default)	Identity group mirroring the guest type
□	GuestType_Daily (default)	Identity group mirroring the guest type
□	GuestType_Contractor (default)	Identity group mirroring the guest type
□	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
□	Employee	Default Employee User Group
□	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

要创建新用户，请使用Add按钮，该按钮将打开新的用户身份组配置表单，如下所示。


Cisco ISE
Administration · Identity Management
Evaluation Mode 82 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > New User Identity Group
Submit
Cancel

Identity Group

* Name: admin-group

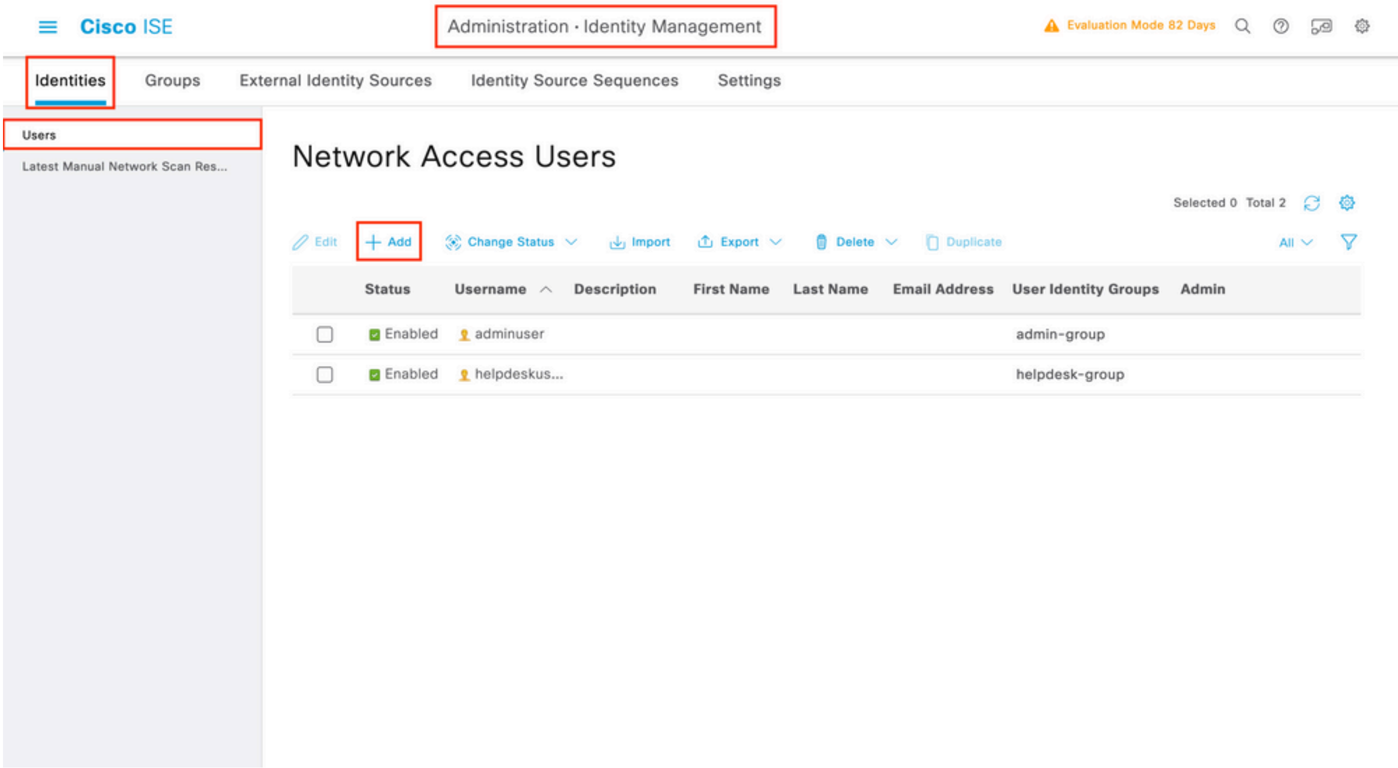
Description: This is the group containing all users with administrator privileges.

提供创建的组的名称。创建上面讨论的两个用户组，即admin-group 和helpdesk-group。

第四步：在ISE上创建用户。

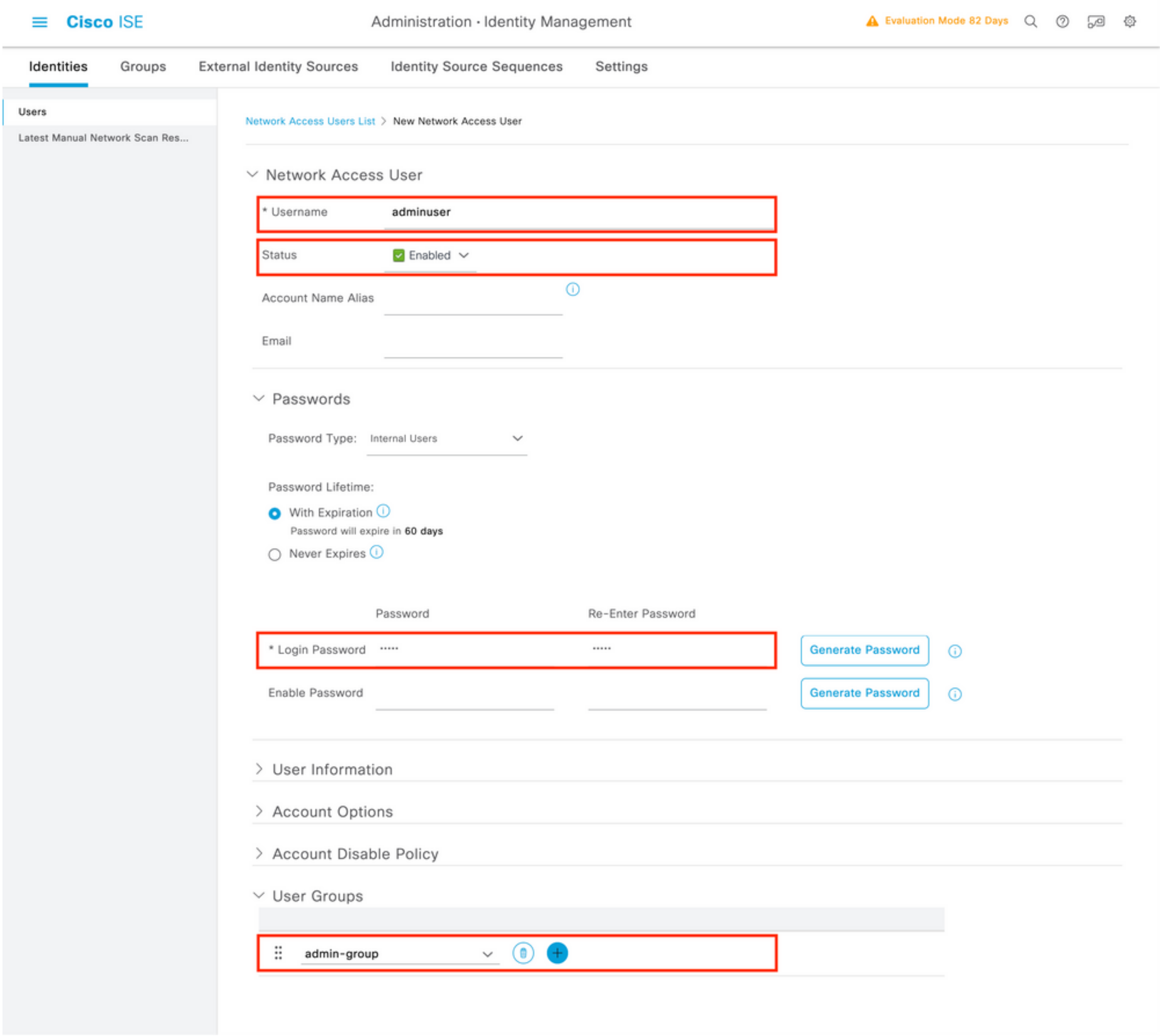
从 GUI：

ISE用户通过Administration > Identity Management > Identities GUI Page的用户选项卡创建，如屏幕截图所示。



	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	adminuser					admin-group	
□	Enabled	helpdeskus...					helpdesk-group	

要创建新用户，请使用Add按钮打开新的网络访问用户配置表，如下所示。



* Username adminuser

Status ☑ Enabled

Account Name Alias

Email

Password Type: Internal Users

Password Lifetime:

● With Expiration
Password will expire in **60 days**

○ Never Expires

	Password	Re-Enter Password
* Login Password	•••••	•••••
Enable Password		

admin-group

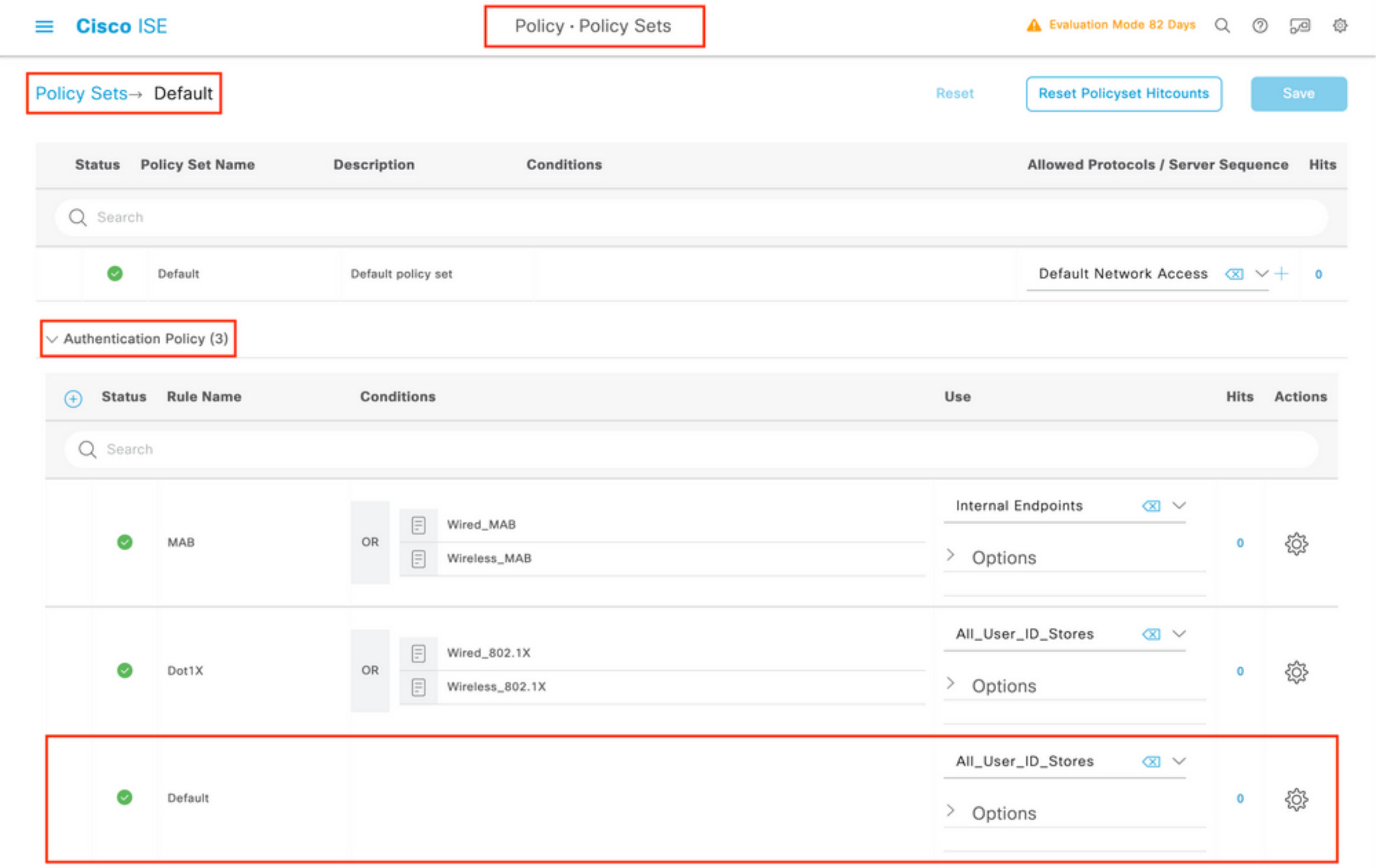
向用户提供凭证，即用于在WLC上进行身份验证的用户名和密码。并且，确保用户的状态为Enabled。最后，在表单末尾的User Groups下拉菜单中，将用户添加到其相关组(已在步骤4.中创建)。

创建上面讨论的两个用户，即adminuser和helpdeskuser。

第五步：对用户进行身份验证。

在GUI中：

在此场景中，ISE的默认策略集的身份验证策略（已预配置）允许默认网络访问。此策略设置可在ISE GUI页面的Policy > Policy Sets中查看，如下图所示。因此，没有必要对其进行更改。



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

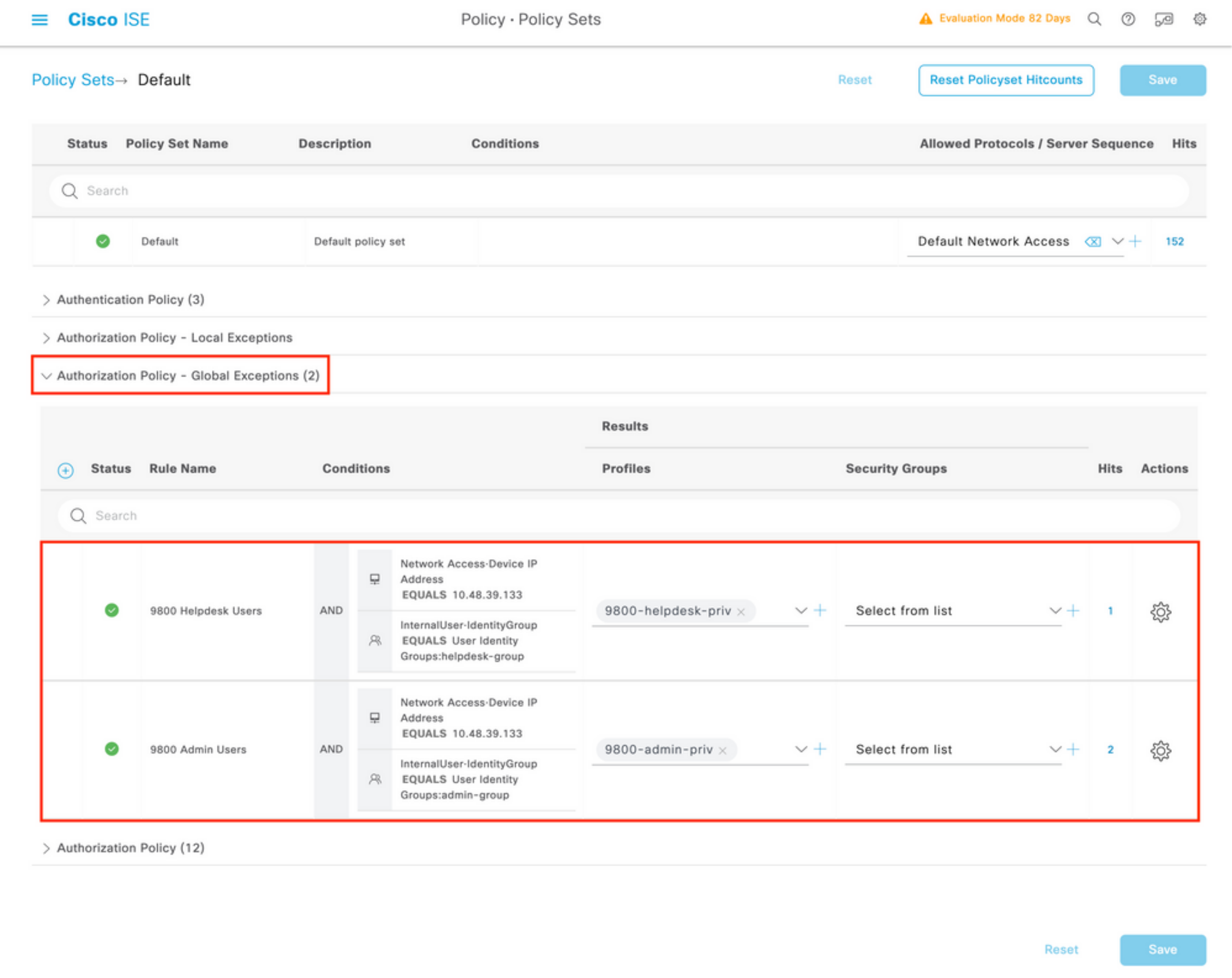
Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options	0	⚙
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	0	⚙
✓	Default		All_User_ID_Stores Options	0	⚙

第六步：授权用户。

在GUI中：

登录尝试通过身份验证策略后，需要对其进行授权，并且ISE需要返回之前创建的授权配置文件（允许接受，以及权限级别）。

在本示例中，根据设备IP地址（即WLC IP地址）过滤登录尝试，并根据用户所属的组区分要授予的权限级别。另一个有效的方法是根据用户的用户名过滤用户，因为在本例中，每个组仅包含一个用户。



Cisco ISE — Policy · Policy Sets

Evaluation Mode 82 Days

Policy Sets→ Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

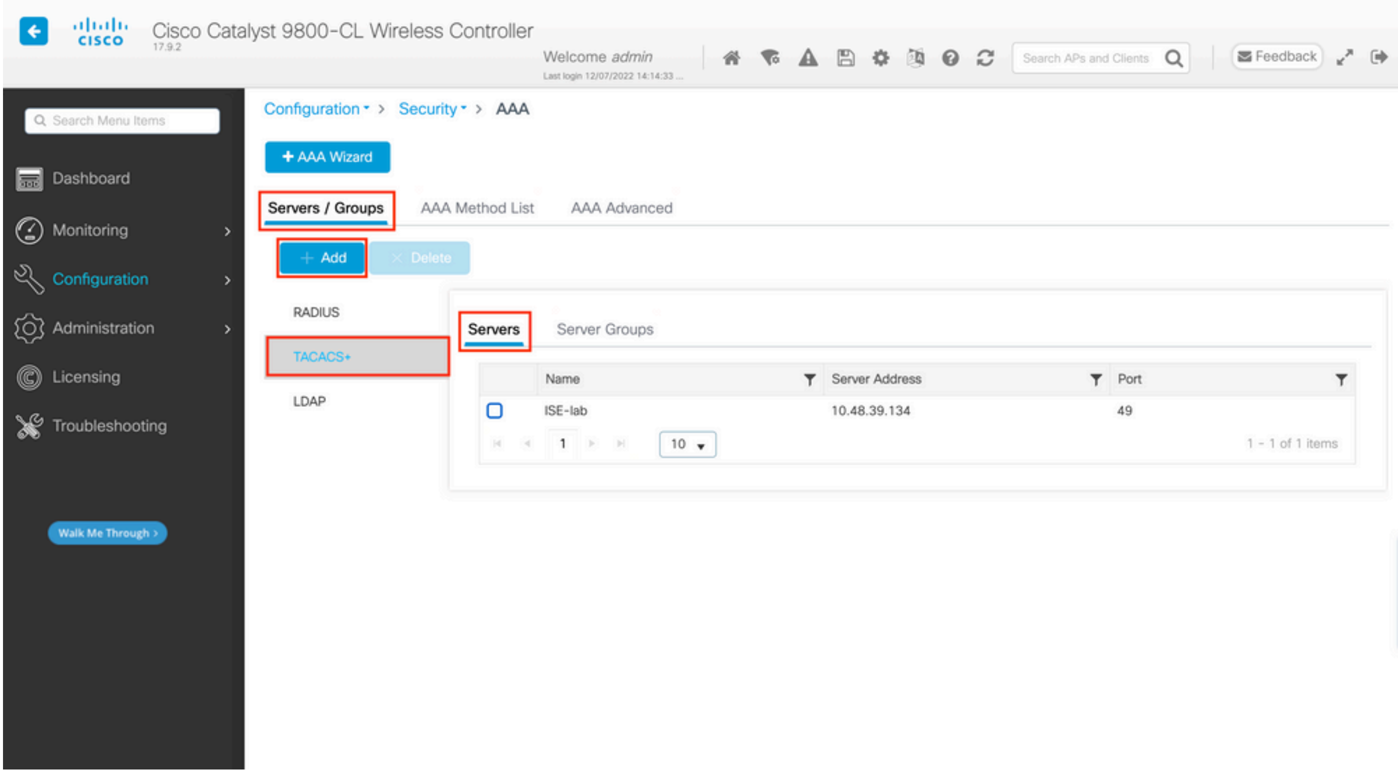
∨ Authorization Policy - Global Exceptions (2)

				Results			
Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
✓	9800 Helpdesk Users	AND	Network Access·Device IP Address EQUALS 10.48.39.133 InternalUser·IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙
✓	9800 Admin Users	AND	Network Access·Device IP Address EQUALS 10.48.39.133 InternalUser·IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙

> Authorization Policy (12)

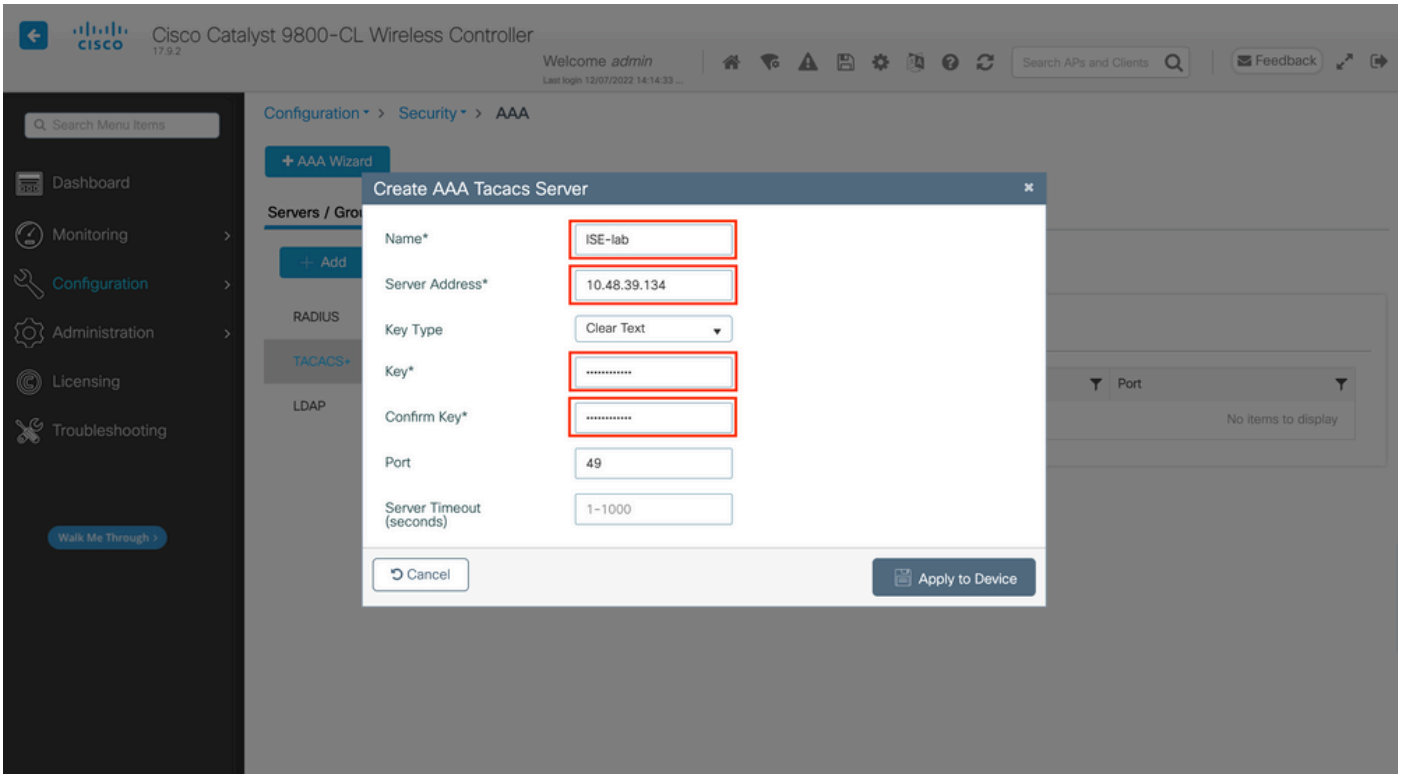
完成此步骤后，为adminuser 和helpdesk用户配置的凭证可用于在WLC中通过GUI或通过Telnet/SSH进行身份验证。

配置TACACS+ WLC
步骤1:声明TACACS+服务器。
在GUI中：
首先，在WLC上创建Tacacs+服务器ISE。 可以在https://<WLC-IP>/webui/#/aaa中访问的GUI WLC页面的选项卡Servers/Groups > TACACS+ > Servers中完成此操作，或者导航到Configuration > Security > AAA(如下图所示)。



Name	Server Address	Port
ISE-lab	10.48.39.134	49

要在WLC上添加TACACS服务器，请点击上图中的红色帧的Add按钮。这将打开所描述的弹出窗口。



Name*: ISE-lab

Server Address*: 10.48.39.134

Key Type: Clear Text

Key*: ••••••••••••

Confirm Key*: ••••••••••••

Port: 49

Server Timeout (seconds): 1-1000

弹出窗口打开时，请提供服务器名称（不必与ISE系统名称匹配）、IP地址、共享密钥、使用的端口和超时。

在此弹出窗口中，必须提供：

- 服务器名称（请注意，不必与ISE系统名称匹配）
-

服务器IP地址

- WLC和TACACS+服务器之间的共享密钥

可以配置其他参数，例如用于身份验证和记账的端口，但这些不是强制性的，保留为本文档的默认设置。

从CLI：

<#root>

WLC-9800(config)#tacacs server

ISE-lab

```
WLC-9800(config-server-tacacs)#address ipv4
```

10.48.39.134

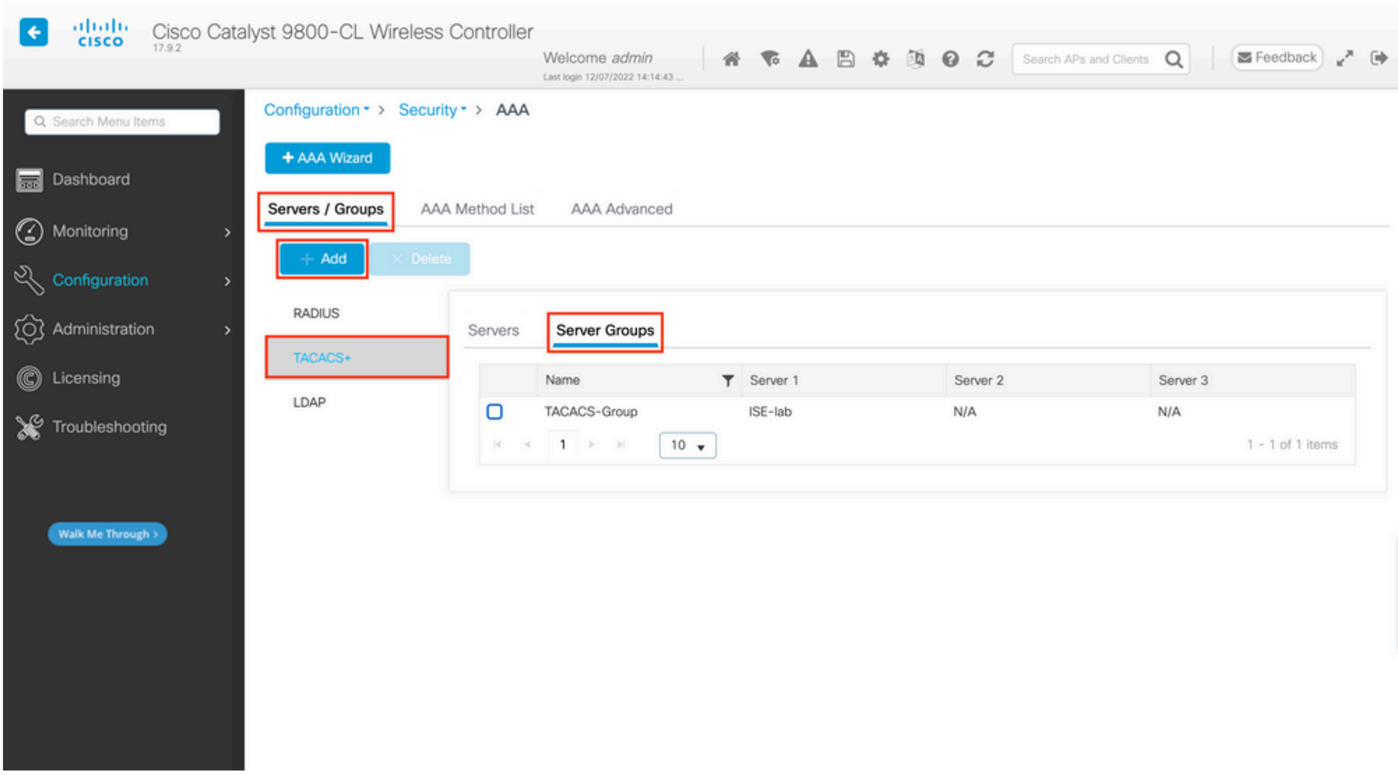
```
WLC-9800(config-server-tacacs)#key
```

Cisco123

第二步：将TACACS+服务器映射到服务器组。

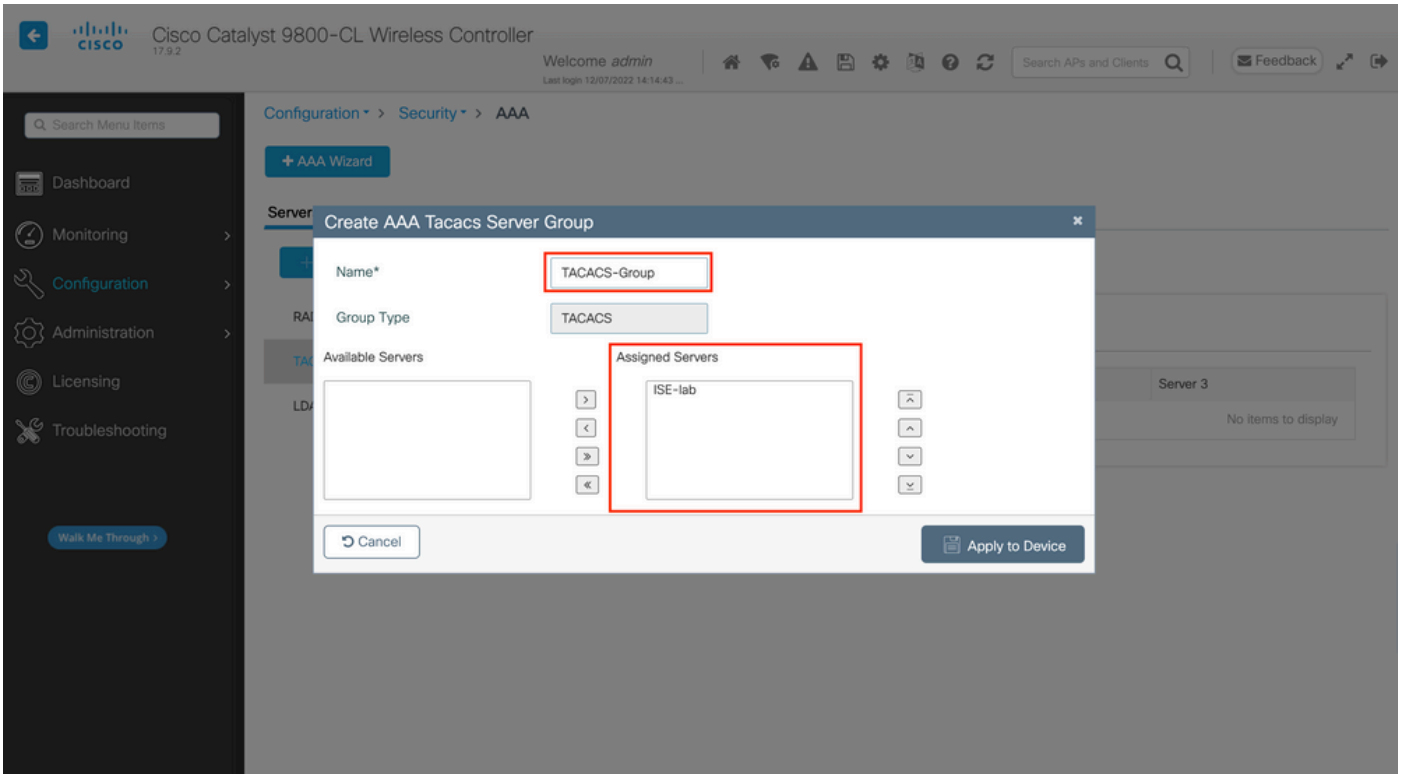
在GUI中：

如果您有多个可用于身份验证的TACACS+服务器，建议将这些服务器映射到同一服务器组。然后，WLC负责对服务器组中的服务器之间的不同身份验证进行负载均衡。TACACS+服务器组通过第1步中提到的GUI页面（如图所示）的Servers/Groups > TACACS > Server Groups选项卡配置。



	Name	Server 1	Server 2	Server 3
□	TACACS-Group	ISE-lab	N/A	N/A

对于服务器的创建，当您单击先前图像（如图所示）中的Add按钮时，会出现一个弹出窗口。



Name*: TACACS-Group

Group Type: TACACS

Assigned Servers: ISE-lab

在弹出窗口中，为组指定名称，并将所需服务器移至Assigned Servers列表。

从CLI：

```
<#root>

WLC-9800(config)#aaa group server tacacs+
```

TACACS-Group

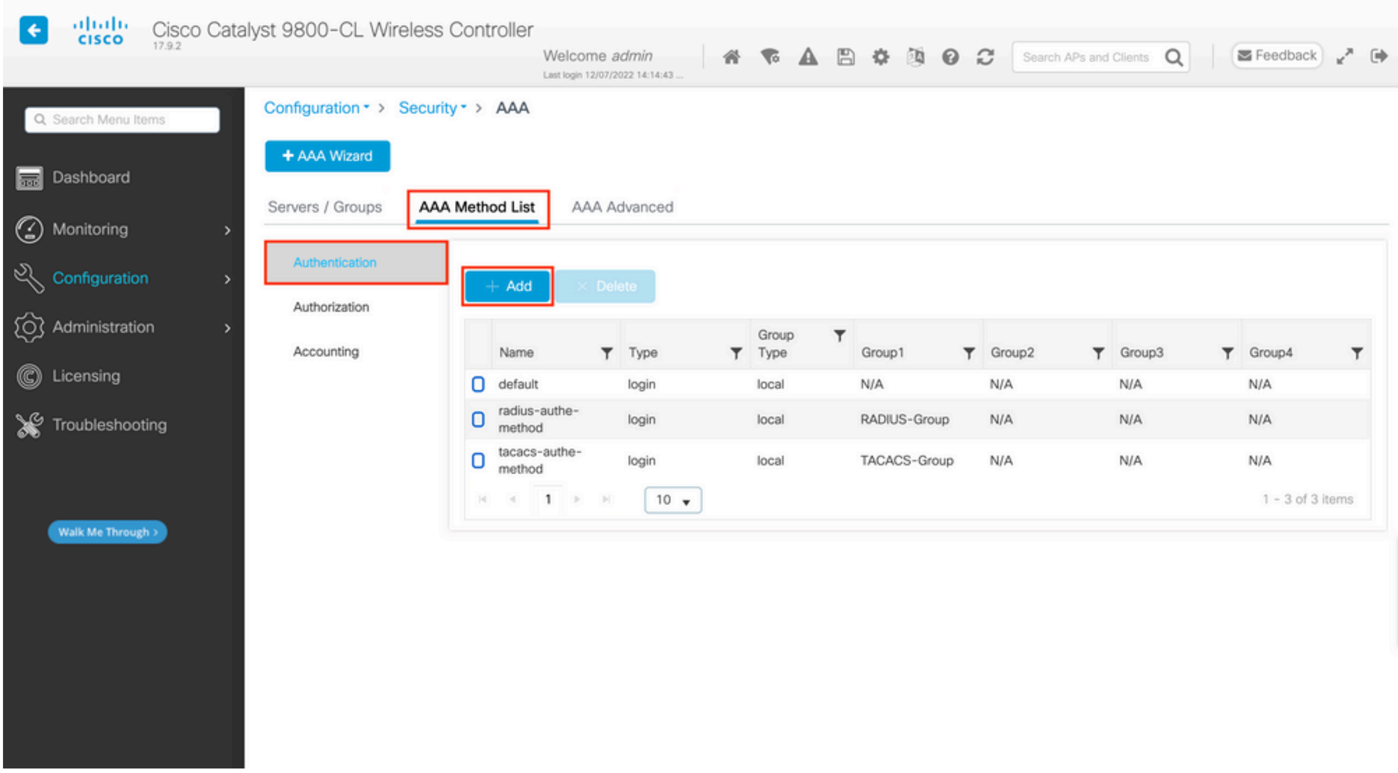
```
WLC-9800(config-sg-tacacs+)#server name
```

ISE-lab

第三步：创建指向TACACS+服务器组的AAA身份验证登录方法。

<u>在GUI中：</u>

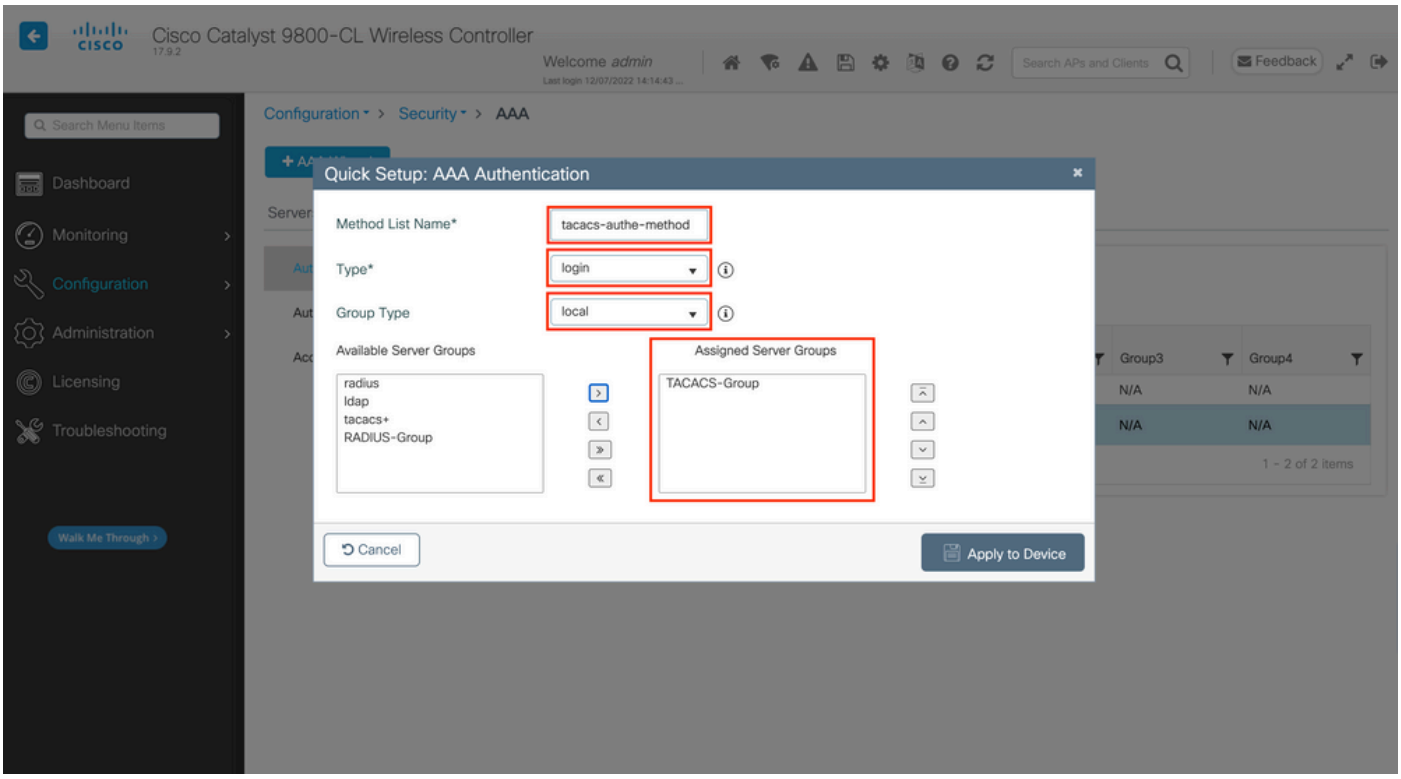
仍在GUI页面上https://<WLC-IP>/webui/#/aaa，导航至AAA Method List > Authentication选项卡，然后创建身份验证方法（如图所示）。



Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
radius-authe-method	login	local	RADIUS-Group	N/A	N/A	N/A
tacacs-authe-method	login	local	TACACS-Group	N/A	N/A	N/A

1 - 3 of 3 items

与往常一样，使用Add按钮创建身份验证方法时，系统会显示配置弹出窗口，类似于下图中所示的窗口。



Quick Setup: AAA Authentication

Method List Name*: tacacs-authe-method

Type*: login

Group Type: local

Available Server Groups: radius, ldap, tacacs+, RADIUS-Group

Assigned Server Groups: TACACS-Group

在此弹出窗口中，为方法提供一个名称，选择Type作为login，并将上一步中创建的组服务器添加到Assigned Server Groups列表。对于Group Type字段，可以进行几种配置。

- 如果您选择Group Type作为local，则WLC首先检查用户凭证是否存在于本地，然后回退到服务器组。
- 如果您选择Group Type作为组并且不选中Fall back to local选项，则WLC仅检查服务器组的用户凭证。
- 如果您选择Group Type作为组并选中Fallback to local选项，则WLC将根据服务器组检查用户凭证，并且仅在服务器未响应时查询本地数据库。如果服务器发送reject消息，则将对用户进行身份验证，即使它可能存在于本地数据库中。

从CLI：

如果您希望只有在首先在本地未找到用户凭证的情况下才使用服务器组检查用户凭证，请使用：

<#root>

WLC-9800(config)#aaa authentication login

`tacacs-authe-method`

```
 local group
```

TACACS-Group

如果您希望仅对服务器组检查用户凭据，请使用：

<#root>

```
WLC-9800(config)#aaa authentication login
```

tacacs-authe-method

```
 group
```

TACACS-Group

如果要对服务器组检查用户凭证，并且如果最后未使用本地条目进行响应，请使用：

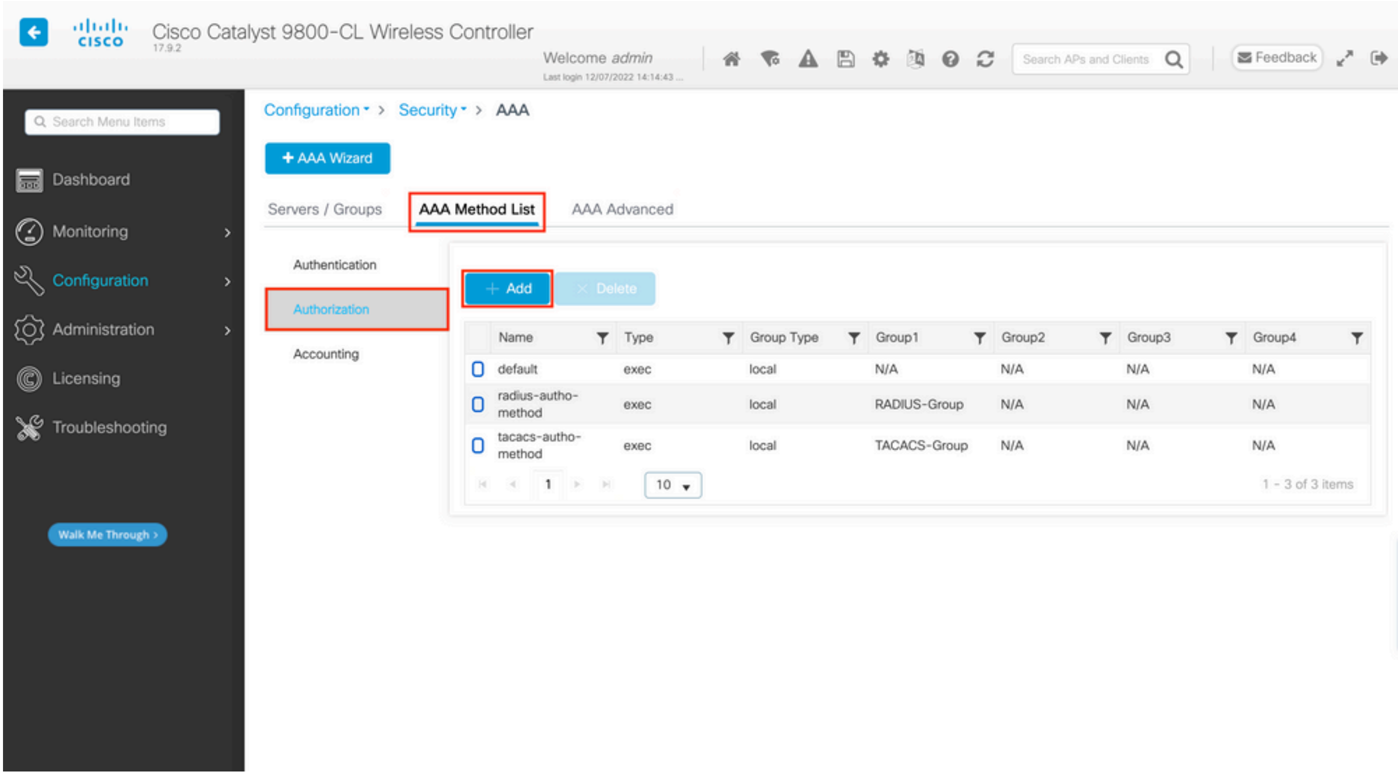
<#root>

```
WLC-9800(config)#aaa authentication login
```

```
tacacs-authe-method

 group

TACACS-Group

local
```

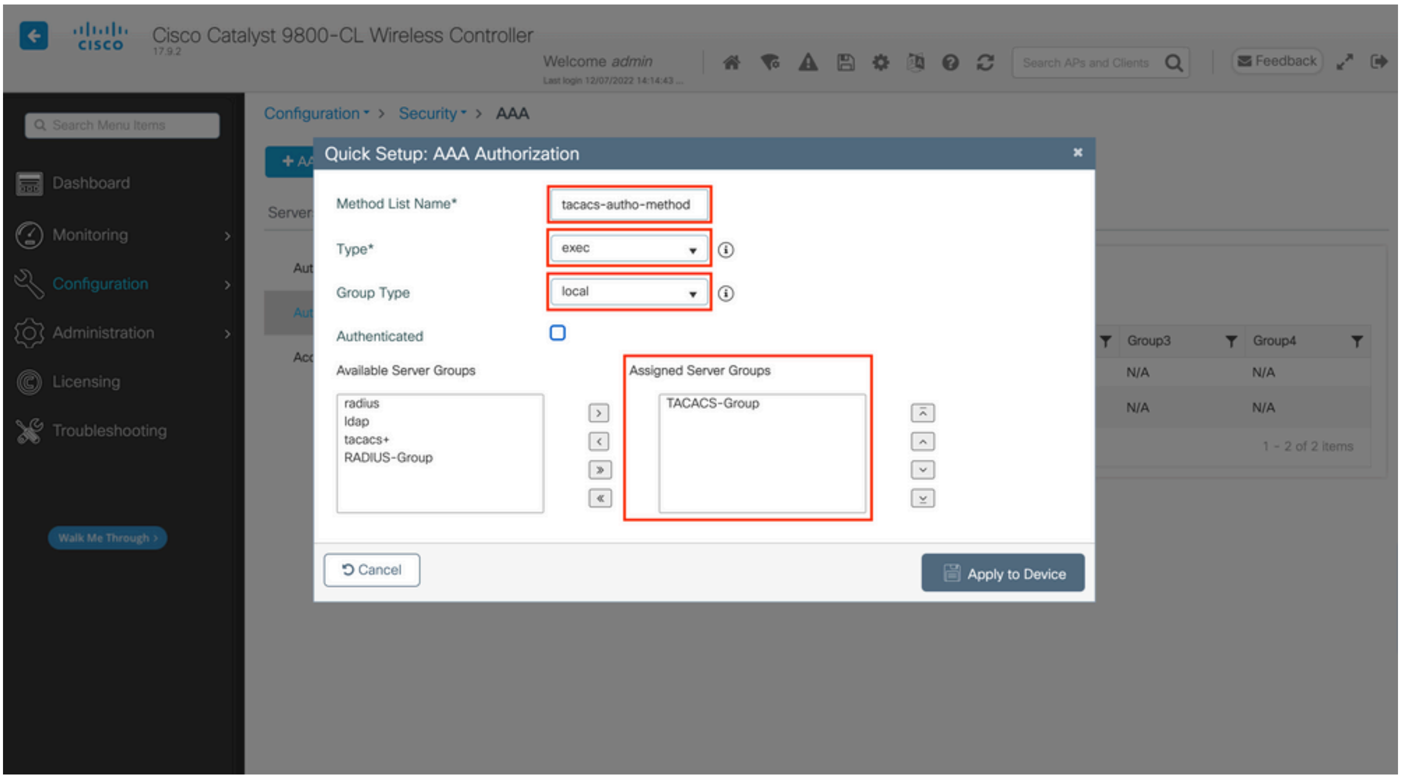
在此示例设置中，有些用户仅在本机创建，而有些用户仅在ISE服务器上创建，因此使用第一个选项。

第四步：创建指向TACACS+服务器组的AAA授权exec方法。
在GUI中：
用户还必须获得授权才能获得访问权限。 Configuration > Security > AAA 仍在GUI页面上，导航至AAA Method List > Authorization选项卡，然后创建授权方法（如图所示）。



Name	Type	Group Type	Group1	Group2	Group3	Group4
default	exec	local	N/A	N/A	N/A	N/A
radius-autho-method	exec	local	RADIUS-Group	N/A	N/A	N/A
tacacs-autho-method	exec	local	TACACS-Group	N/A	N/A	N/A

当您使用Add按钮添加新授权方法时，会显示与所描述授权方法配置类似的弹出窗口。



Quick Setup: AAA Authorization

Method List Name* tacacs-autho-method

Type* exec

Group Type local

Authenticated □

Available Server Groups
radius
ldap
tacacs+
RADIUS-Group

Assigned Server Groups
TACACS-Group

Cancel

Apply to Device

在此配置弹出窗口中，为授权方法提供一个名称，选择Type作为exec，并使用与上一步中用于身份验证方法的组类型顺序相同的组类型顺序。

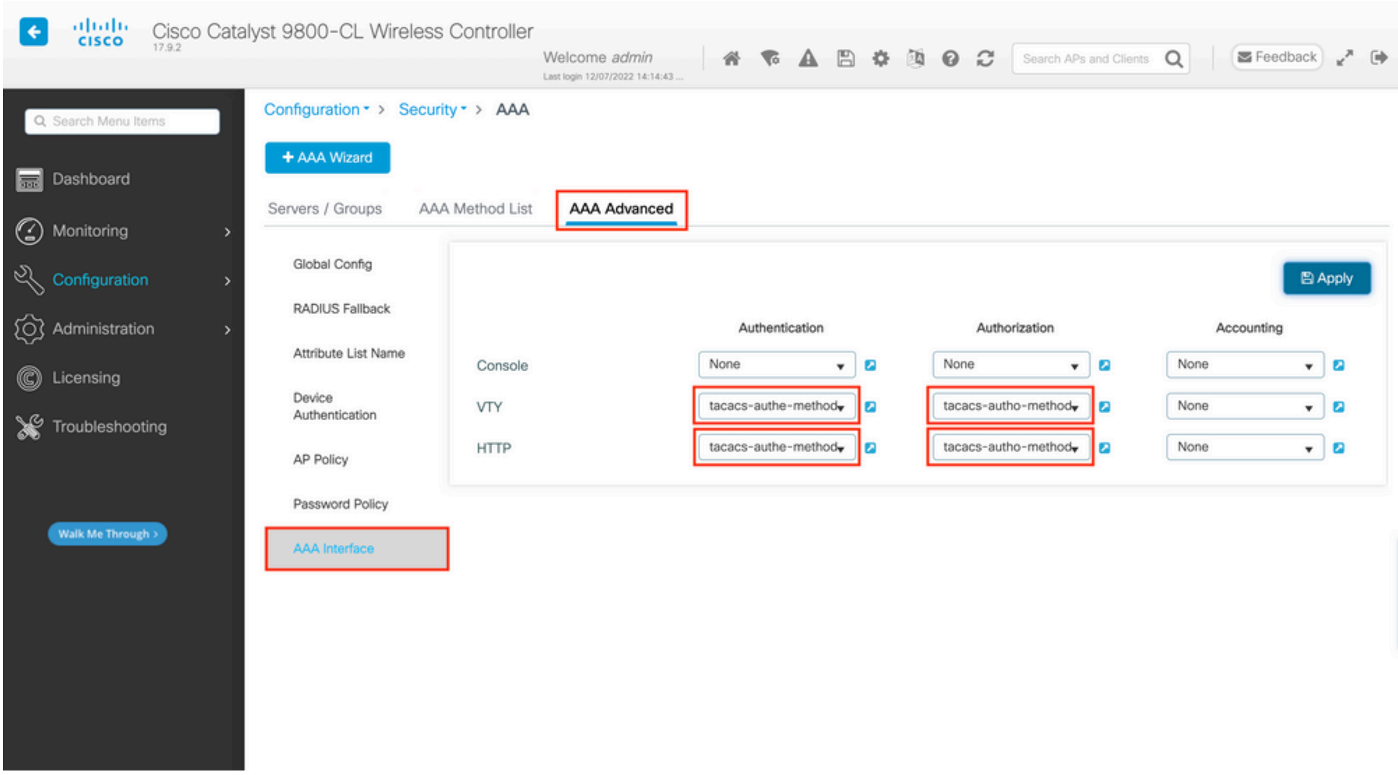
从CLI：

```
<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

 local group

TACACS-Group
```

第五步：将方法分配给HTTP配置和用于Telnet/SSH的VTY线路。

在GUI中：

创建的身份验证和授权方法可用于HTTP和/或Telnet/SSH用户连接，该连接可在AAA Advanced > AAA Interface选项卡上配置的，仍可从GUI WLC页(可在https://<WLC-IP>/webui/#/aaa中访问)访问，如图所示。



	Authentication	Authorization	Accounting
Console	None	None	None
VTY	tacacs-authe-method	tacacs-autho-method	None
HTTP	tacacs-authe-method	tacacs-autho-method	None

从CLI：

对于GUI身份验证：

```
<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

tacacs-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

tacacs-autho-method
```

对于Telnet/SSH身份验证：

<#root>

```
WLC-9800(config)#line vty 0 15
WLC-9800(config-line)#login authentication
```

tacacs-authe-method

```
WLC-9800(config-line)#authorization exec
```

tacacs-autho-method

请注意，当对HTTP配置执行更改时，最好重新启动HTTP和HTTPS服务。这可以通过这些命令来实现。

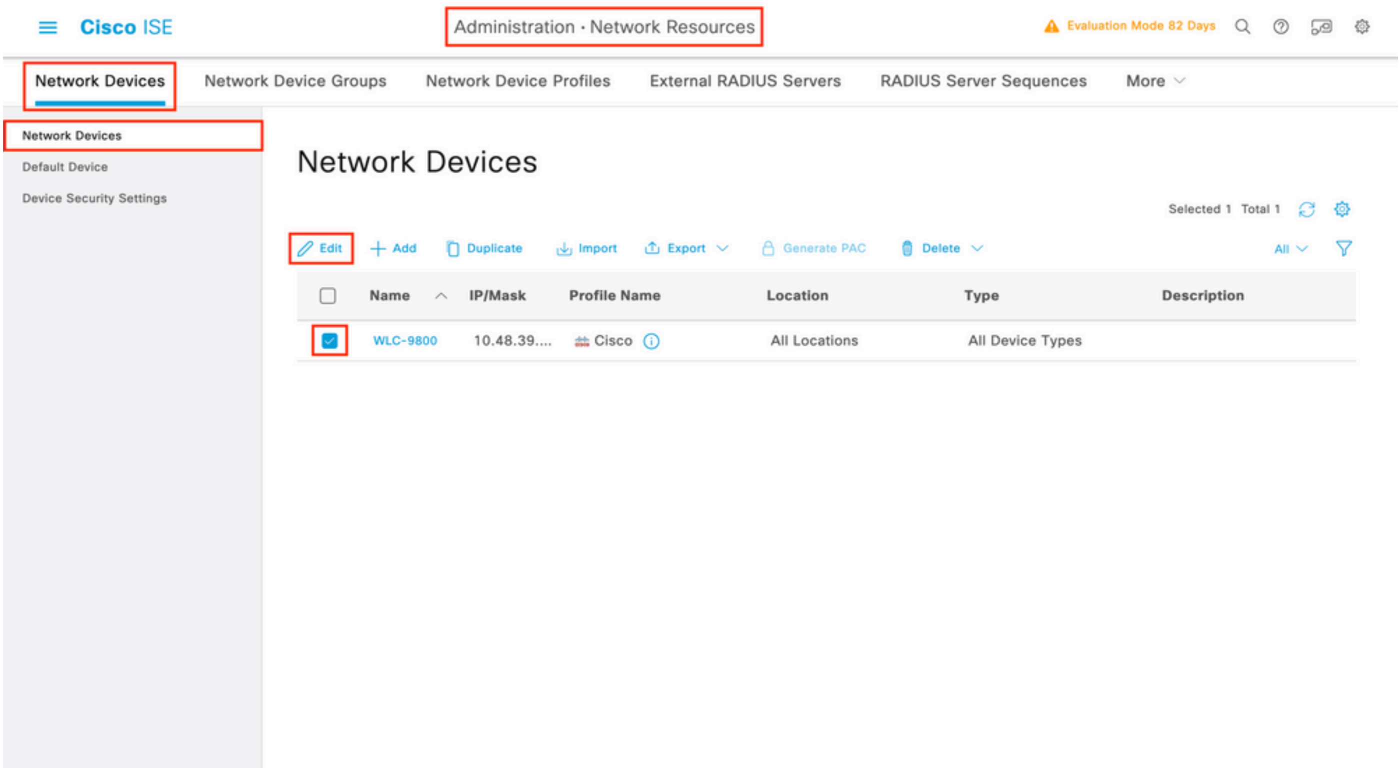
```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

TACACS+ ISE配置

步骤1:将WLC配置为TACACS+的网络设备。

在GUI中：

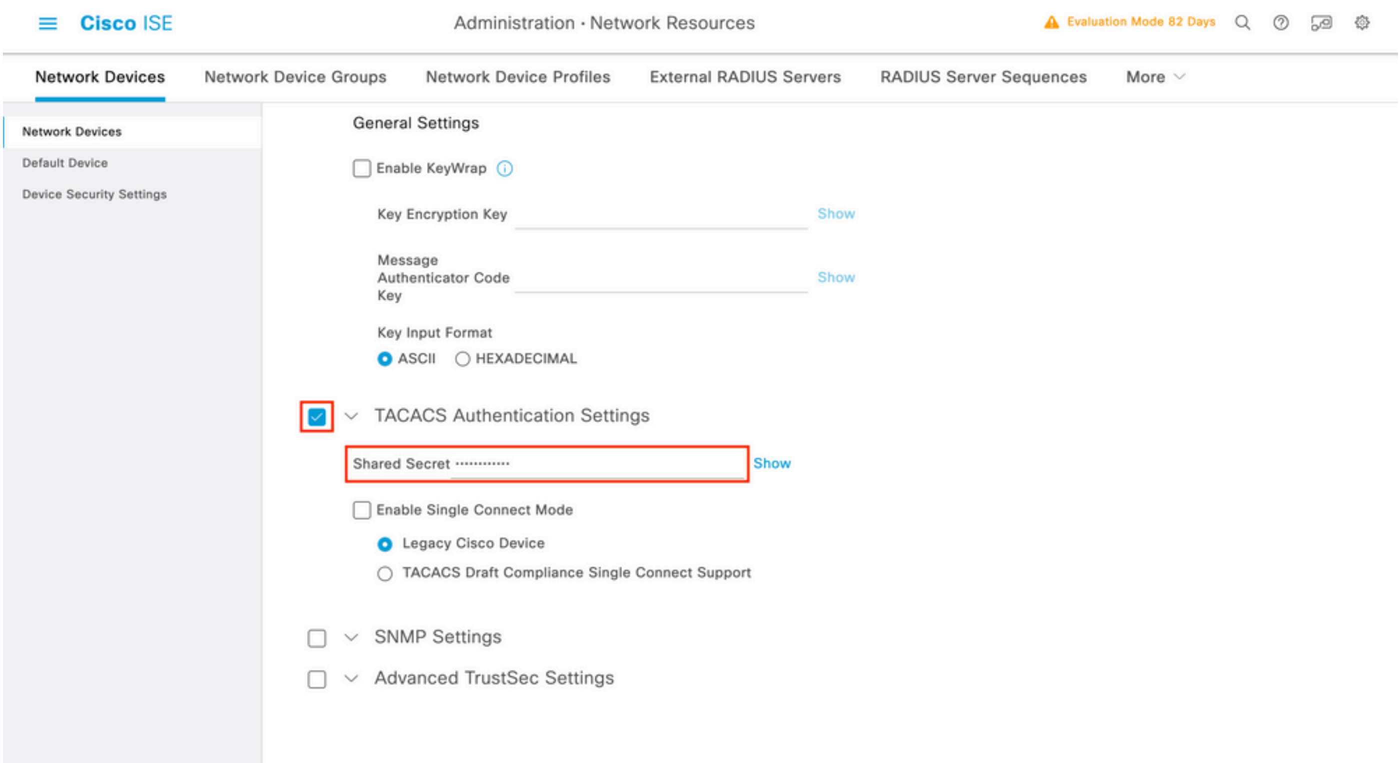
要声明上一节中使用的WLC是ISE中的RADIUS网络设备，请导航到Administration > Network Resources > Network Devices，然后打开"网络设备"选项卡，如此图中所示。



Network Devices

☐	Name	IP/Mask	Profile Name	Location	Type	Description
☑	WLC-9800	10.48.39....	Cisco	All Locations	All Device Types	

在本示例中，已为RADIUS身份验证添加了WLC(请参阅配置RADIUS ISE部分的步骤1)。因此，只需修改其配置即可配置TACACS身份验证，当您在网络设备列表中选择WLC并点击Edit按钮即可完成此任务。此时会打开网络设备配置表，如下图所示。



General Settings

☐ Enable KeyWrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

● ASCII ○ HEXADECIMAL

☑ TACACS Authentication Settings

Shared Secret ·············

☐ Enable Single Connect Mode

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

☐ SNMP Settings

☐ Advanced TrustSec Settings

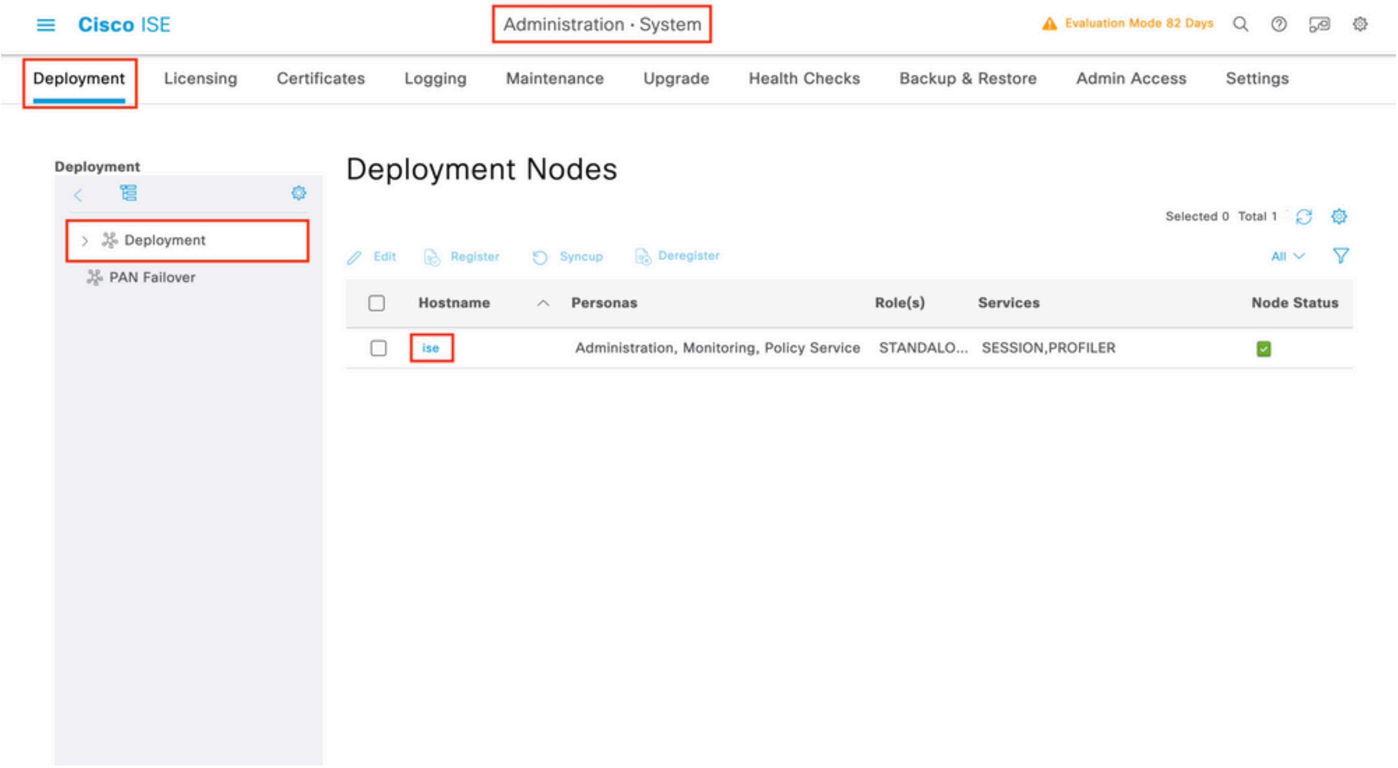
打开新窗口后，向下滚动到TACACS Authentication Settings部分，启用这些设置，并添加在Configure TACACS+ WLC部分的步骤1中输入的共享密钥。

第二步：启用节点的设备管理功能。

注意：要将ISE用作TACACS+服务器，您必须具有设备管理许可证包以及基础许可证或移动许可证。

在GUI中：

安装设备管理许可证后，必须启用节点的设备管理功能，才能将ISE用作TACACS+服务器。为此，请编辑所用ISE部署节点的配置(可在Administrator > Deployment下找到)，然后单击其名称或借助Edit按钮执行此操作。

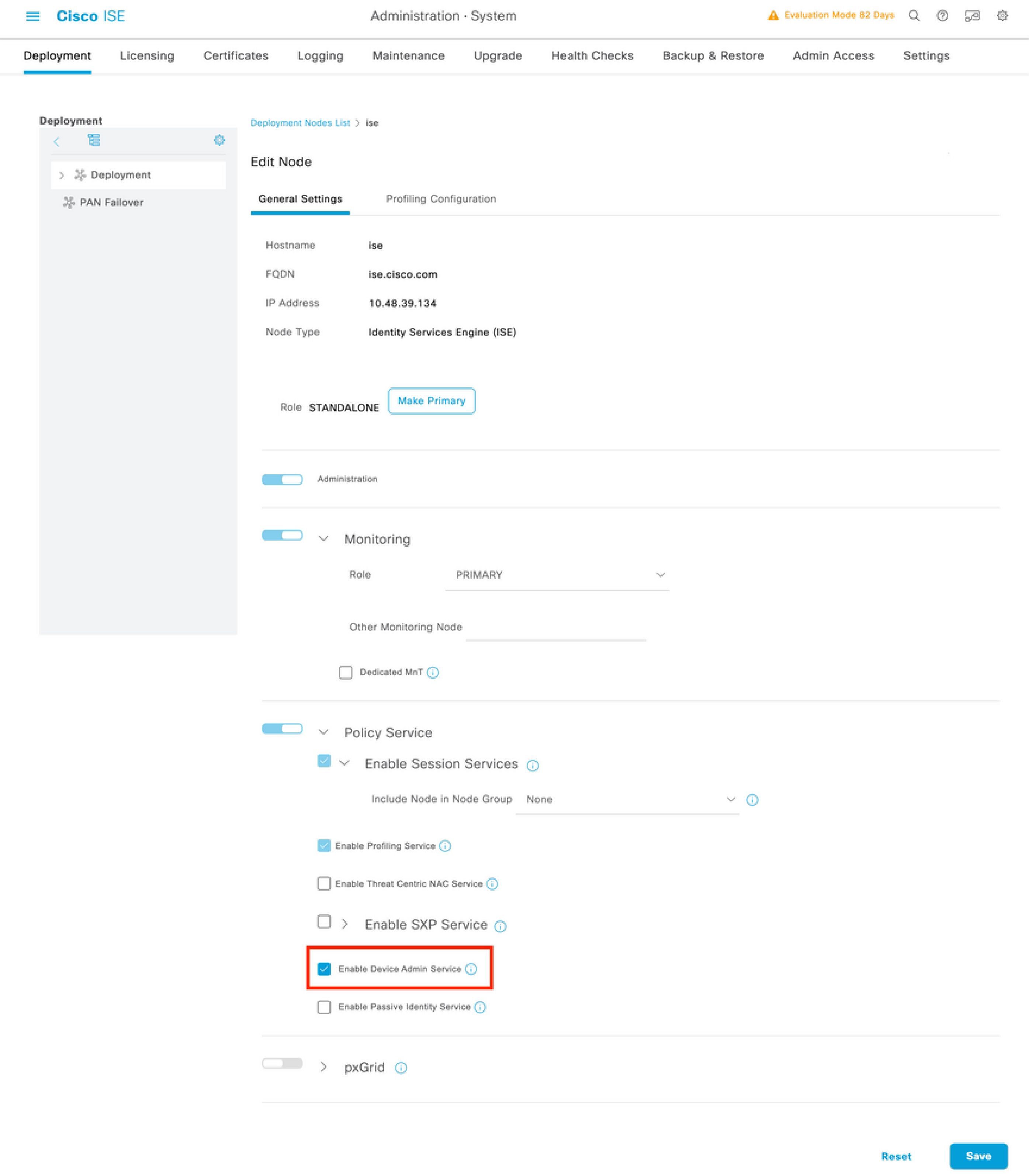


Deployment Nodes

Selected 0 Total 1

	Hostname	Personas	Role(s)	Services	Node Status
□	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	✓

打开节点配置窗口后，选中Policy Service部分下的Enable Device Admin Service选项，如此图中所示。



Edit Node

Hostname ise

FQDN ise.cisco.com

IP Address 10.48.39.134

Node Type Identity Services Engine (ISE)

Role STANDALONE

Administration

Monitoring

Role PRIMARY

Other Monitoring Node

□ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

☑ Enable Device Admin Service

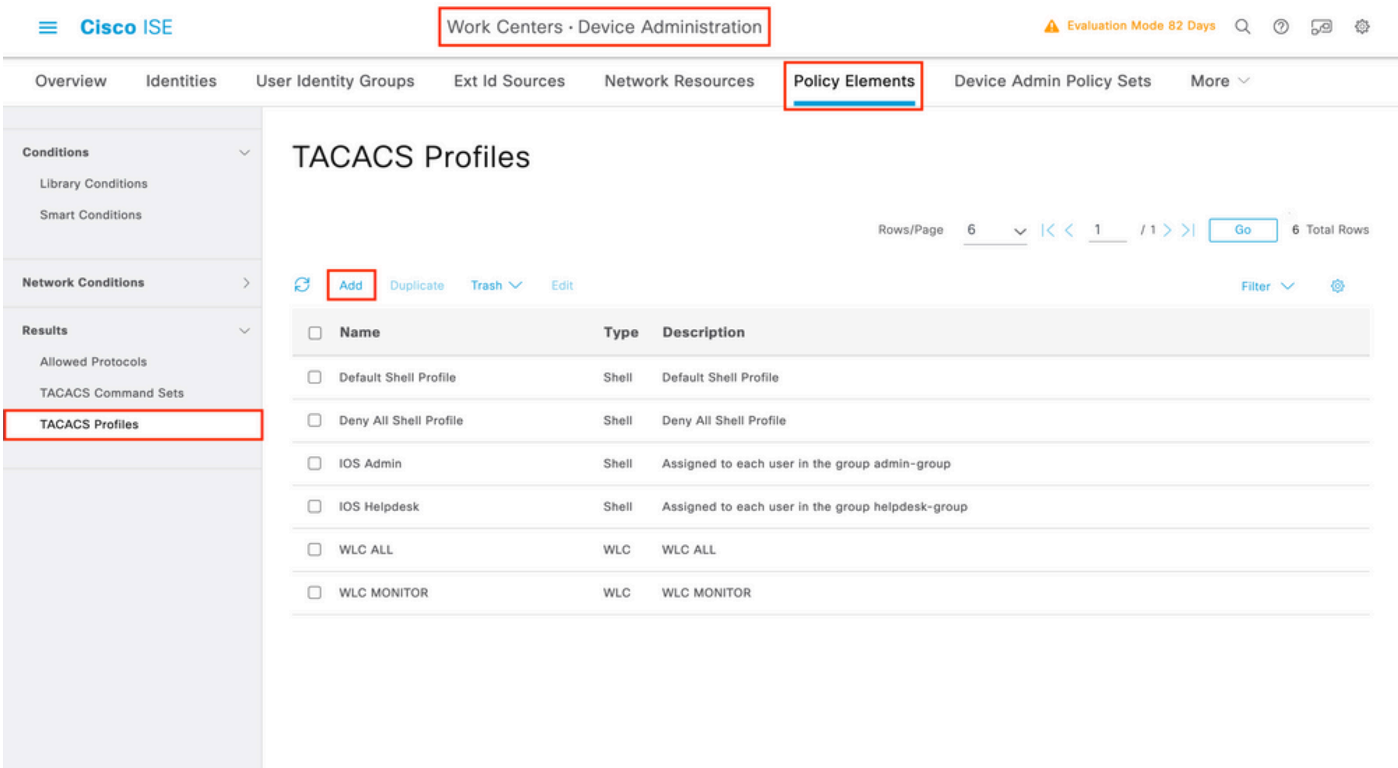
□ Enable Passive Identity Service

pxGrid

第三步：创建TACACS配置文件，以返回权限。

在GUI中：

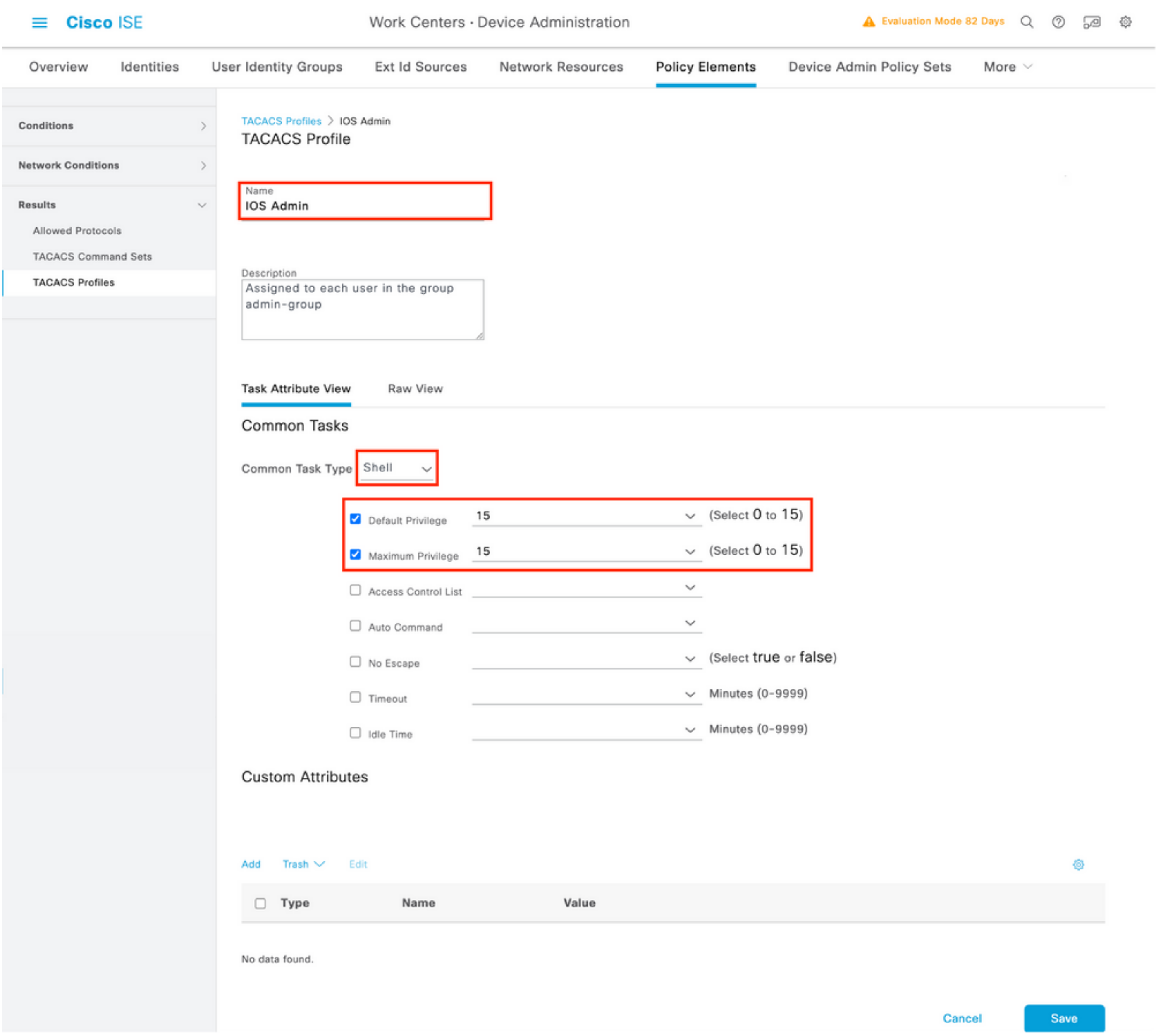
要获得管理员访问权限，adminuser的权限级别必须为15，以允许访问exec提示外壳。另一方面，helpdeskuser则不需要exec提示符外壳访问，因此可以分配权限级别低于15。要为用户分配适当的权限级别，可以使用授权配置文件。可以从ISE GUI页面Work Centers > Device Administration > Policy Elements在Results > TACACS Profiles选项卡下配置，如下图所示。



TACACS Profiles

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
IOS Admin	Shell	Assigned to each user in the group admin-group
IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

要配置新的TACACS配置文件，请使用Add按钮，该按钮会打开新的配置文件配置表，类似于图中所示的表单。要配置分配给adminuser(即，外壳权限级别为15)的配置文件，此表单尤其必须如下所示。



TACACS Profile

Name: IOS Admin

Description: Assigned to each user in the group admin-group

Common Tasks

Common Task Type: Shell

- ☑ Default Privilege: 15 (Select 0 to 15)
- ☑ Maximum Privilege: 15 (Select 0 to 15)
- □ Access Control List
- □ Auto Command
- □ No Escape (Select true or false)
- □ Timeout Minutes (0-9999)
- □ Idle Time Minutes (0-9999)

Custom Attributes

□ Type	Name	Value

No data found.

对helpdesk配置文件重复此操作。最后，Default Privilege和Maximum Privilege均设置为1。

第四步：在ISE上创建用户组。

这类似于本文档配置RADIUS ISE部分的步骤3。

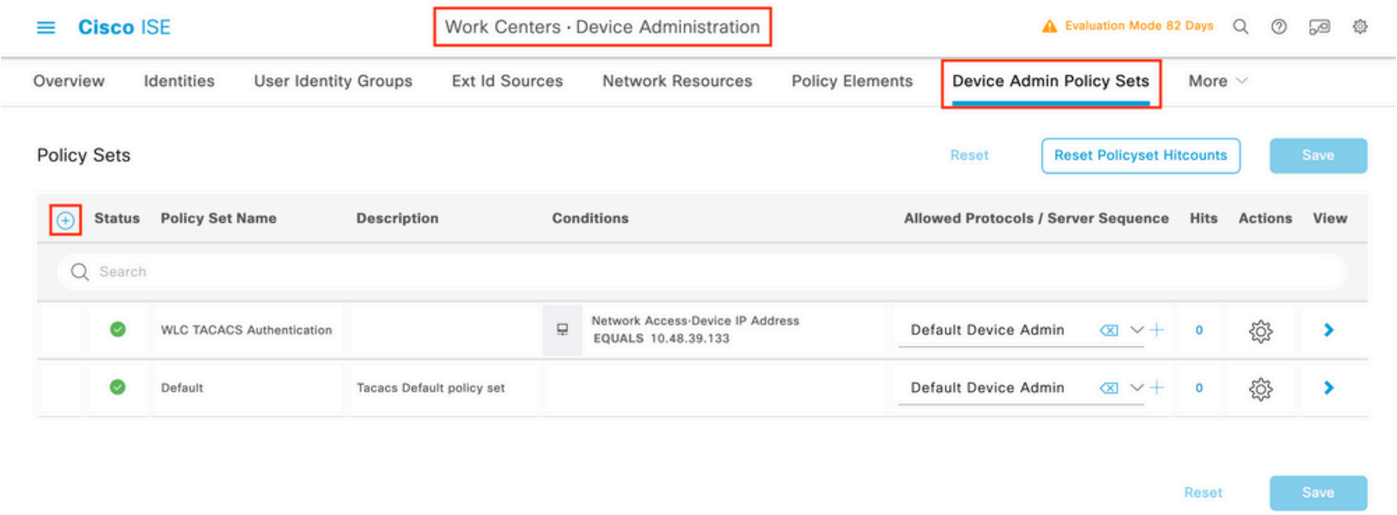
第五步：在ISE上创建用户。

这类似于本文档配置RADIUS ISE部分的步骤4。

第六步：创建设备管理策略集。

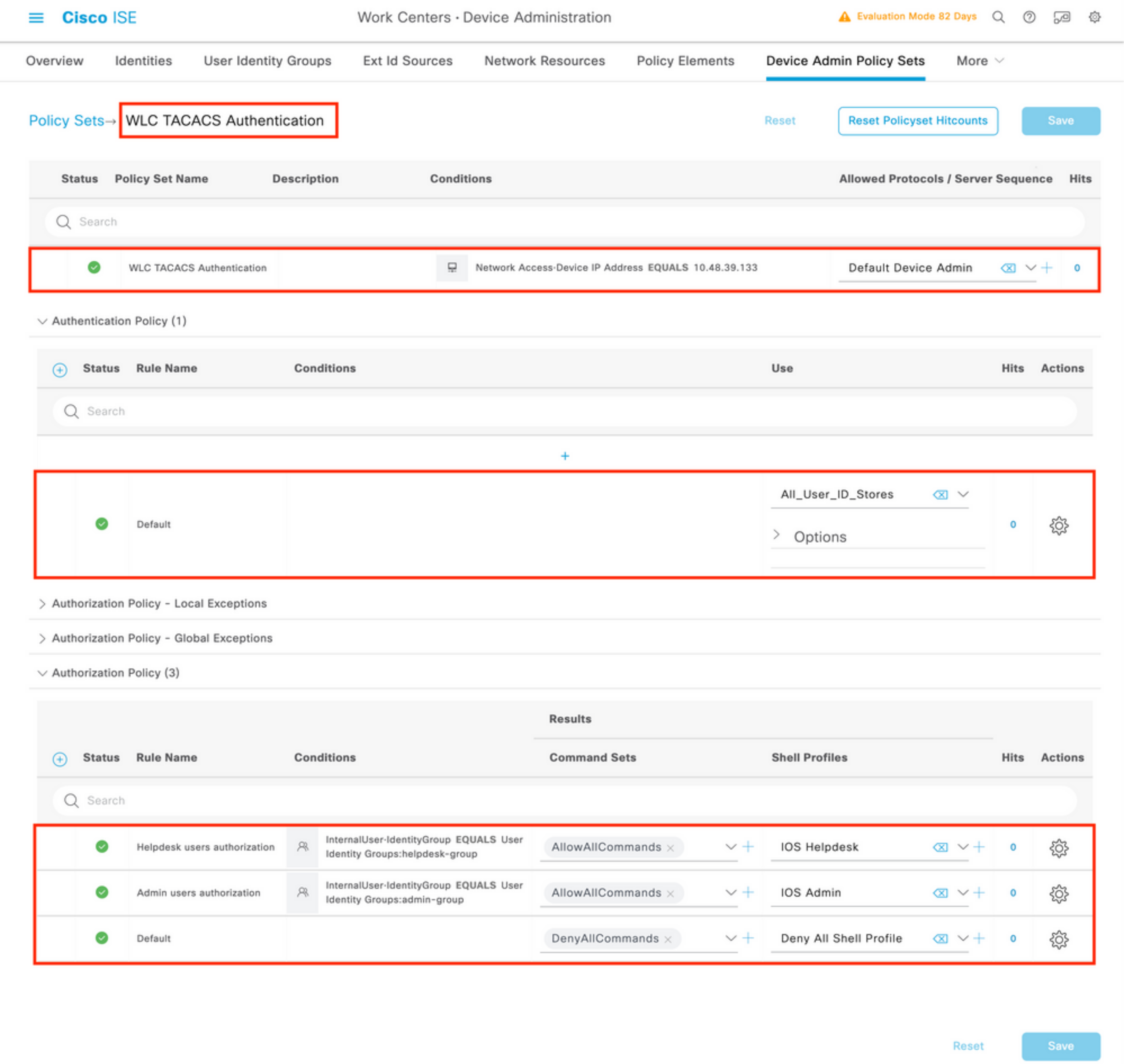
在GUI中：

对于RADIUS访问，用户创建后，仍需要在ISE上定义其身份验证和授权策略，以便授予他们适当的访问权限。TACACS身份验证使用设备管理策略集实现这一目的，可以通过Work Centers > Device Administration > Device Admin Policy Sets GUI Page进行配置，如下所示。



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	WLC TACACS Authentication		Network Access·Device IP Address EQUALS 10.48.39.133	Default Device Admin	0	⚙	›
✓	Default	Tacacs Default policy set		Default Device Admin	0	⚙	›

要创建设备管理策略集，请使用上一映像中以红色框框显示的添加按钮，这会将项目添加到策略集列表。为新创建的组提供一个名称、必须应用该名称的条件以及允许的协议/服务器序列(此处，Default Device Admin足够)。使用Save按钮完成策略集的添加，并使用其右侧的箭头访问其配置页（如图所示）。



Policy Sets→ WLC TACACS Authentication

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	WLC TACACS Authentication		Network Access·Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		All_User_ID_Stores Options	0	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

			Results			
Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
✓	Helpdesk users authorization	InternalUser·IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0	⚙
✓	Admin users authorization	InternalUser·IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0	⚙
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙

此示例中的特定策略集“WLC TACACS Authentication”过滤IP地址与示例C9800 WLC IP地址相等的请求。

作为身份验证策略，Default Rule已保留，因为它满足使用案例的需要。已设置两个授权规则：

- 当用户属于已定义的组admin-group时，将触发第一个值。它允许所有命令(通过默认Permit_all规则)并分配权限15(通过定义的IOS_Admin TACACS配置文件)。

- 当用户属于定义的组helpdesk-group时，触发第二个。 它允许所有命令(通过默认规Permit_all 则)并分配权限1(通过定义的IOS_HelpdeskTACACS配置文件)。

完成此步骤后，为adminuser和helpdesk用户配置的凭证可用于在WLC中通过GUI或Telnet/SSH进行身份验证。

故障排除

如果您的RADIUS服务器期望发送服务类型RADIUS属性，则可以在WLC上添加：

```
radius-server attribute 6 on-for-login-auth
```

通过WLC CLI排除WLC GUI或CLI RADIUS/TACACS+访问故障

为了对通过TACACS+访问WLC GUI或CLI进行故障排除，请发出debug tacacs命令以及terminal monitor one，并在尝试登录后查看实时输出。

例如，成功登录后注销adminuser用户将生成以下输出。

```
    <#root>

WLC-9800#

terminal monitor

WLC-9800#

debug tacacs

TACACS access control debugging is on
WLC-9800#
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

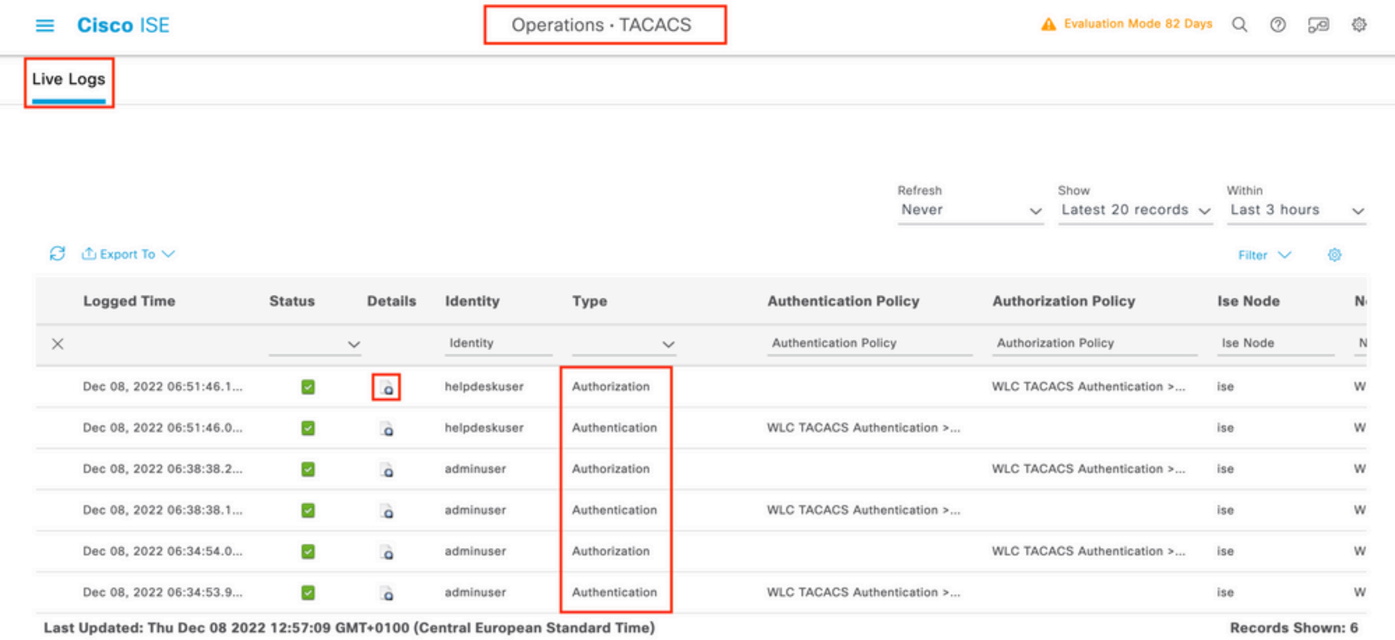
从这些日志中可以看到，TACACS+服务器返回了正确的权限(即AV priv-lvl=15)。

当您执行RADIUS身份验证时，显示与RADIUS流量相关的类似调试输出。

相反，命令debug aaa authentication和debug aaa authorization将显示WLC在用户尝试登录时选择的方法列表。

通过ISE GUI排除WLC GUI或CLI TACACS+访问故障

从第Operations > TACACS > Live Logs页起，可以查看通过TACACS+进行的直到最近24小时内的每个用户身份验证。要展开TACACS+授权或身份验证的详细信息，请使用与此事件相关的Details按钮。



Refresh: Never

Show: Latest 20 records

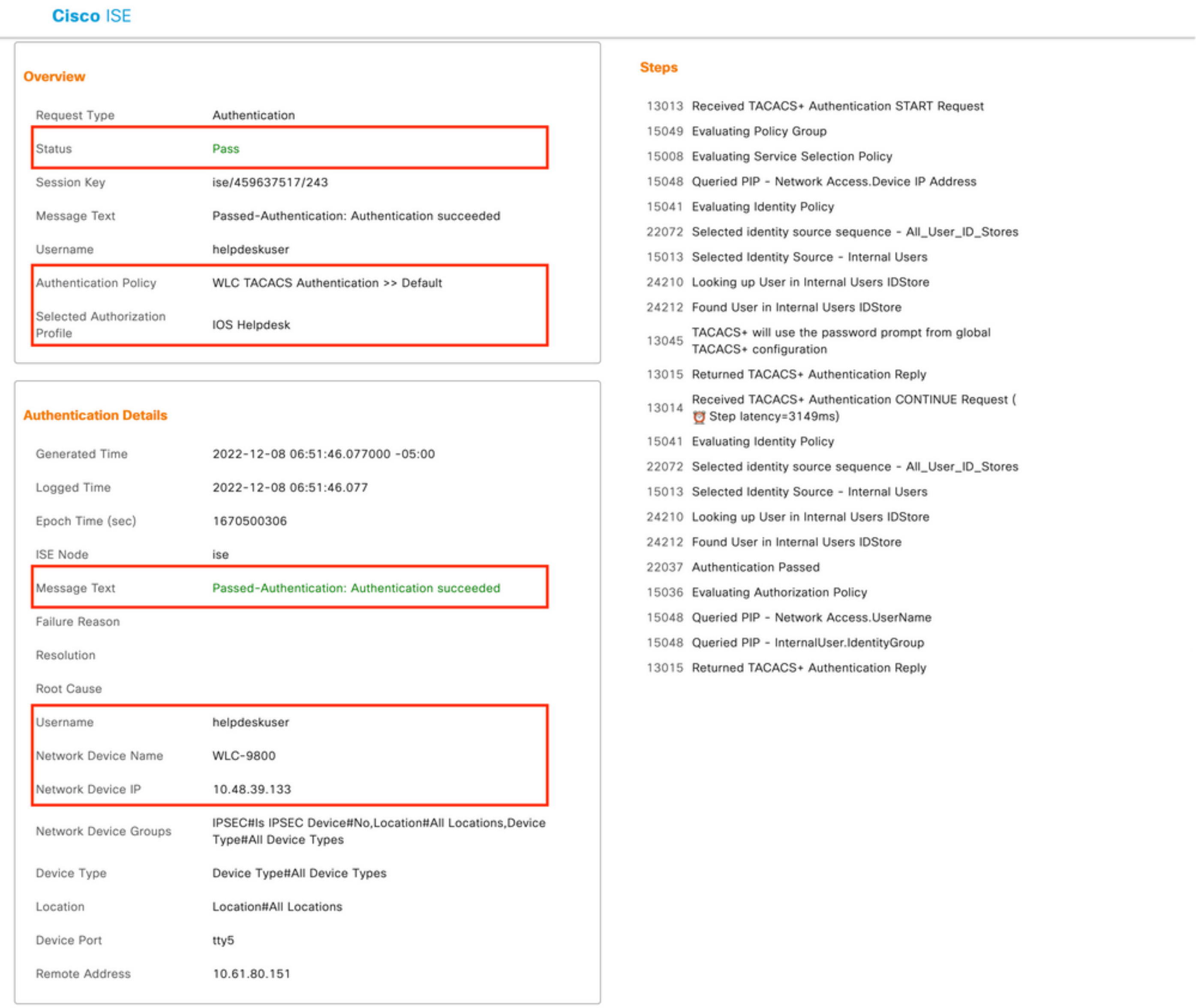
Within: Last 3 hours

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	✓	🔍	helpdeskuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	✓	🔍	helpdeskuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:38:38.2...	✓	🔍	adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	✓	🔍	adminuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:34:54.0...	✓	🔍	adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	✓	🔍	adminuser	Authentication	WLC TACACS Authentication >...		ise	W

Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)

Records Shown: 6

展开时，helpdeskuser的身份验证成功尝试如下所示：



Cisco ISE

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Device IP Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
13045	TACACS+ will use the password prompt from global TACACS+ configuration
13015	Returned TACACS+ Authentication Reply
13014	Received TACACS+ Authentication CONTINUE Request (⏰ Step latency=3149ms)
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.IdentityGroup
13015	Returned TACACS+ Authentication Reply

从这里，您可以看到用户helpdeskuser已借助身份验证策略成功通过身份验证WLC-9800到网络设备WLC TACACS Authentication > Default。此外，授权配置文件IOS Helpdesk已分配给此用户，并已授予权限级别1。

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）。