

在Catalyst 9800 WLC和ISE上配置集中网络身份验证(CWA)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[9800 WLC 上的 AAA 配置](#)

[WLAN 配置](#)

[策略配置文件配置](#)

[策略标签配置](#)

[策略标签分配](#)

[重定向 ACL 配置](#)

[为HTTP或HTTPS启用重定向](#)

[ISE 配置](#)

[将 9800 WLC 添加到 ISE](#)

[在 ISE 上创建新用户](#)

[创建授权配置文件](#)

[配置身份验证规则](#)

[配置授权规则](#)

[仅限 FlexConnect 本地交换无线接入点](#)

[证书](#)

[验证](#)

[故障排除](#)

[核对清单](#)

[RADIUS的服务端口支持](#)

[收集调试信息](#)

[Examples](#)

简介

本文档介绍如何在Catalyst 9800 WLC和ISE上配置CWA无线LAN。

先决条件

要求

Cisco建议您了解9800无线局域网控制器(WLC)的配置。

使用的组件

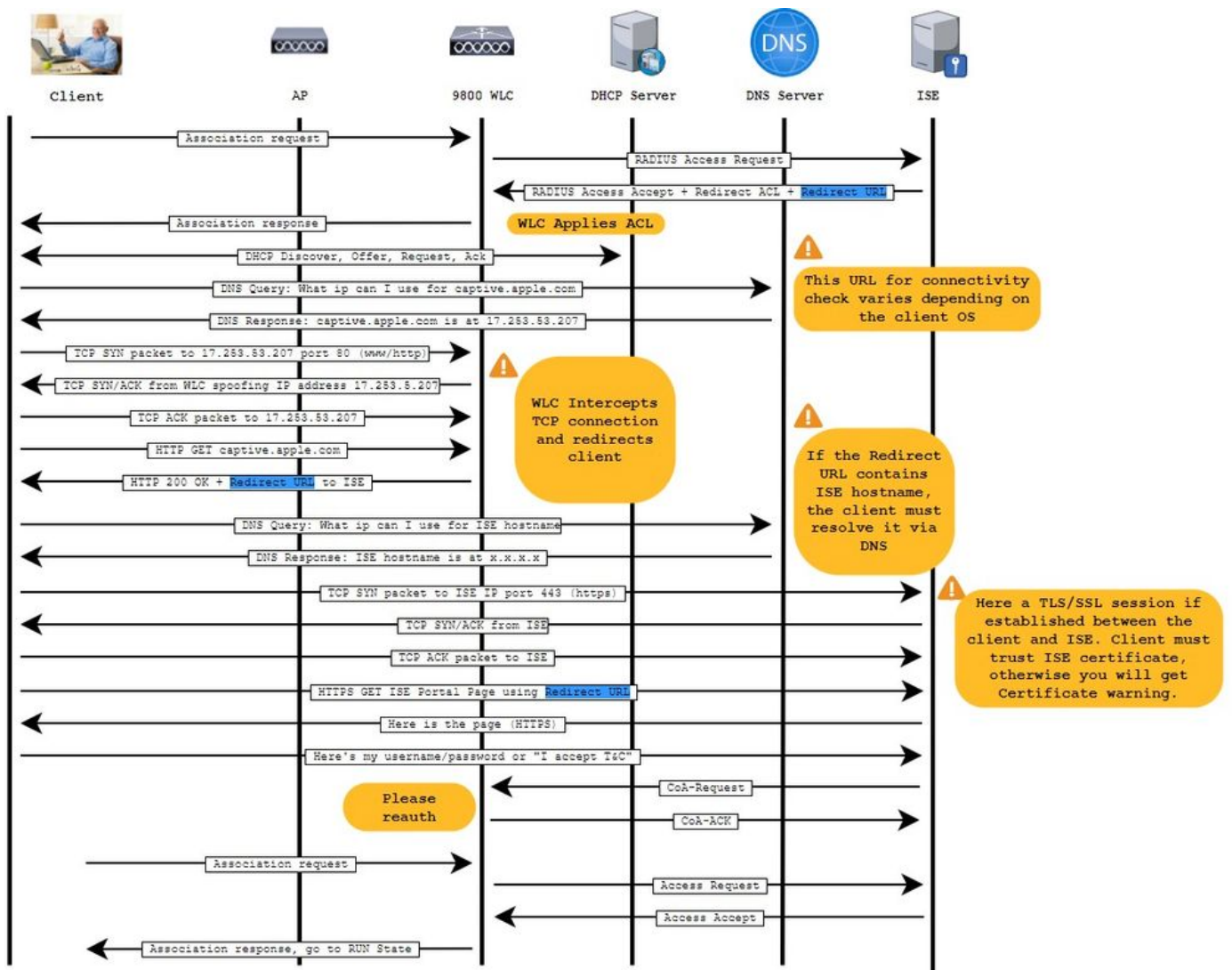
本文档中的信息基于以下软件和硬件版本：

- 9800 WLC Cisco IOS® XE直布罗陀v17.6.x
- 身份服务引擎(ISE) v3.0

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。

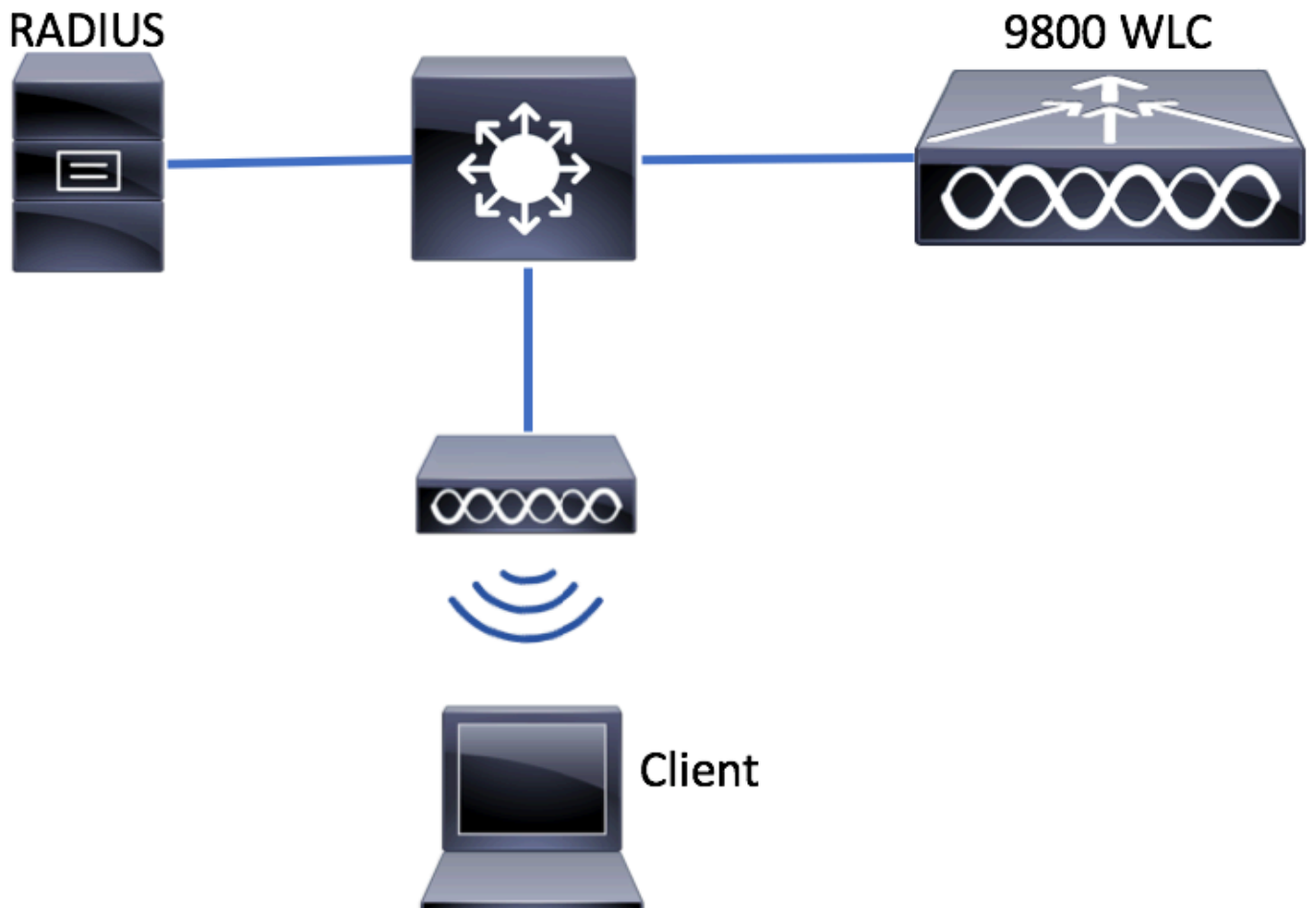
背景信息

此处显示了CWA流程，您可以在这里看到Apple设备的CWA流程示例：



配置

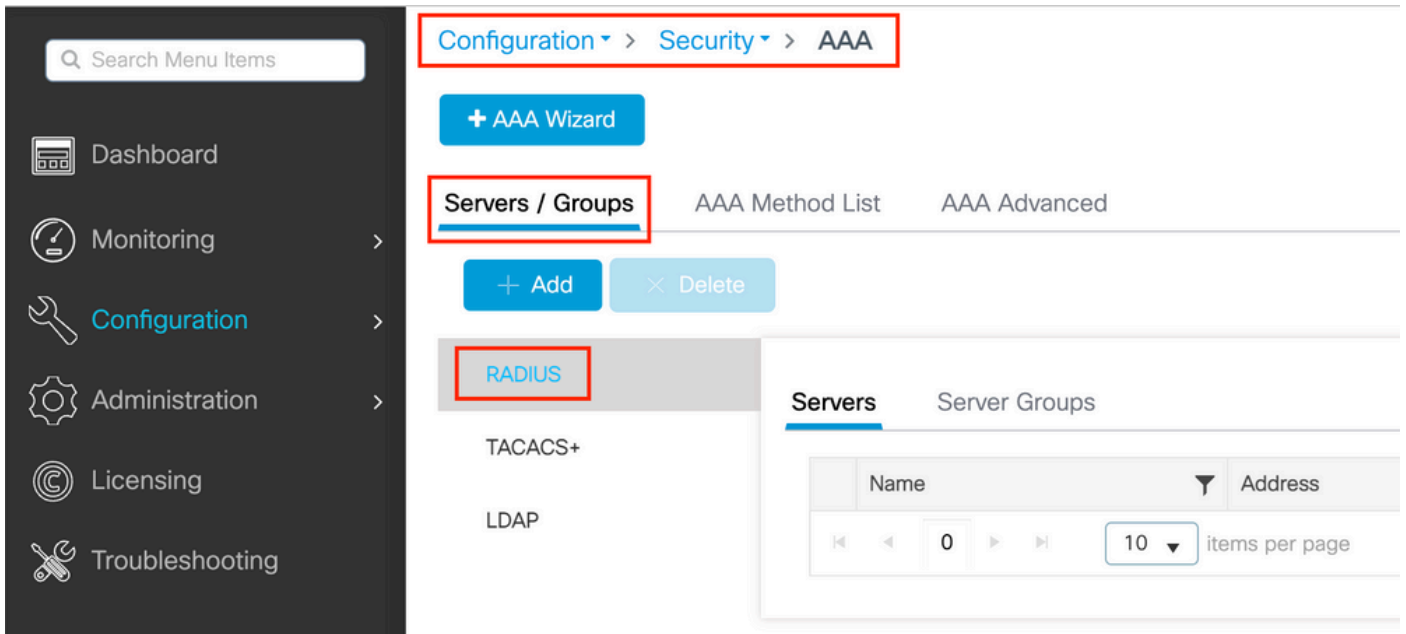
网络图



9800 WLC 上的 AAA 配置

步骤1:将ISE服务器添加到9800 WLC配置。

导航到Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add 并输入RADIUS服务器信息，如图所示。



如果您计划将来使用中央 Web 身份验证（或任何一种需要 CoA 的安全措施），请确保已启用对 CoA 的支持。

The 'Create AAA Radius Server' configuration window contains the following fields and options:

- Name*: ISE-server
- Server Address*: [Redacted]
- PAC Key:
- Key Type: Clear Text
- Key*: [Redacted]
- Confirm Key*: [Redacted]
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA: ENABLED
- CoA Server Key Type: Clear Text
- CoA Server Key: [Redacted]
- Confirm CoA Server Key: [Redacted]
- Automate Tester:

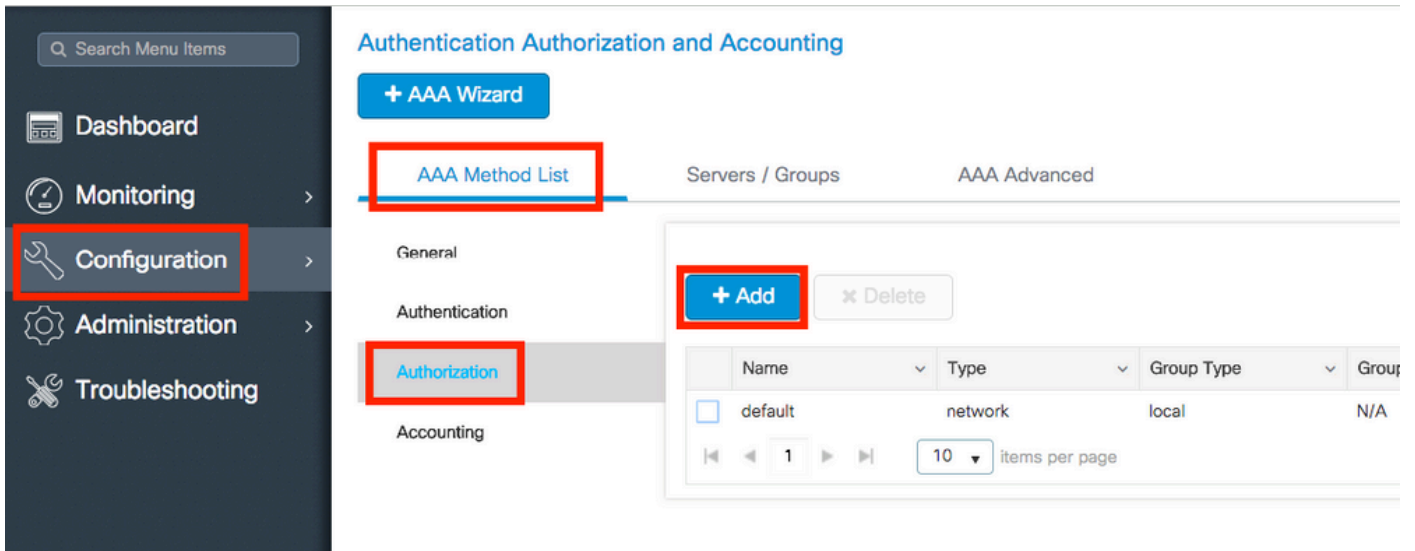
Buttons: Cancel, Apply to Device



注意：在版本17.4.X及更高版本中，请确保在配置RADIUS服务器时也配置CoA服务器密钥。使用与共享密钥相同的密钥（在ISE上默认情况下相同）。目的是为CoA配置不同于共享密钥的密钥（如果这是您的RADIUS服务器所配置的密钥）。在Cisco IOS XE 17.3中，Web UI仅使用与CoA密钥相同的共享密钥。

第二步：创建授权方法列表。

导航至Configuration > Security > AAA > AAA Method List > Authorization > + Add 如图所示。



Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Authenticated

Available Server Groups **Assigned Server Groups**

<input type="text" value="ldap"/> <input type="text" value="tacacs+"/>	<input type="button" value=">"/>	<input type="text" value="radius"/>	<input type="button" value="^"/>
	<input type="button" value="<"/>		<input type="button" value="^"/>
	<input type="button" value=">>"/>		<input type="button" value="v"/>
	<input type="button" value="<<"/>		<input type="button" value="v"/>

第3步：(可选) 创建会计方法列表，如图所示。

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

+ AAA Wizard

AAA Method List

Servers / Groups

General

Authentication

Authorization

Accounting

+ Add

x Delete

Name
0

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups

Assigned Server Groups

ldap
tacacs+

radius

Cancel

Apply to Device

注意：如果由于思科漏洞ID [CSCvh03827](#)而决定对（来自Cisco IOS XE CLI配置的）RADIUS服务器进行负载均衡，则CWA不起作用。外部负载均衡器的使用效果良好。但是，使用calling-station-id RADIUS属性确保您的负载均衡器按客户端运行。依赖UDP源端口不是平衡来自9800的RADIUS请求的受支持机制。

第4步：（可选）您可以定义AAA策略以将SSID名称作为被叫站ID属性发送，如果您希望稍后在ISE上利用此条件，此功能会非常有用。

导航到Configuration > Security > Wireless AAA Policy(AAA)并编辑默认AAA策略或创建一个新AAA策略。

- ☰ Dashboard
- 🕒 Monitoring >
- 🔧 **Configuration** >
- ⚙️ Administration >
- 🔧 Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪ ⏩ 1 ⏪ ⏩
10 items per page

您可以选择SSID作为选项1。请注意，即使您仅选择SSID，被叫站ID仍会将AP MAC地址附加到SSID名称。

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

Option 1

SSID ▼

Option 2

Not Configured ▼

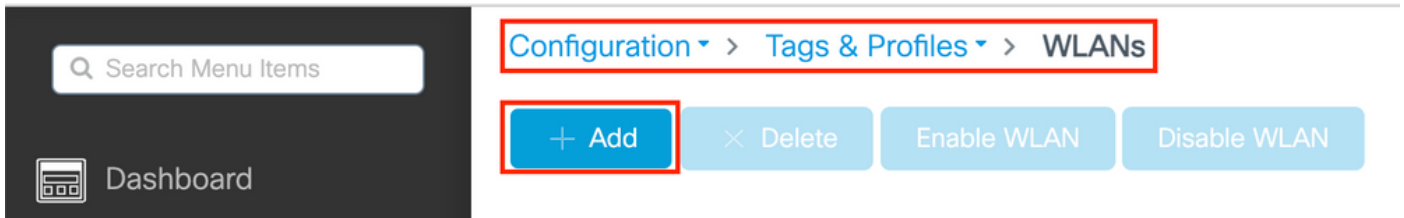
Option 3

Not Configured ▼

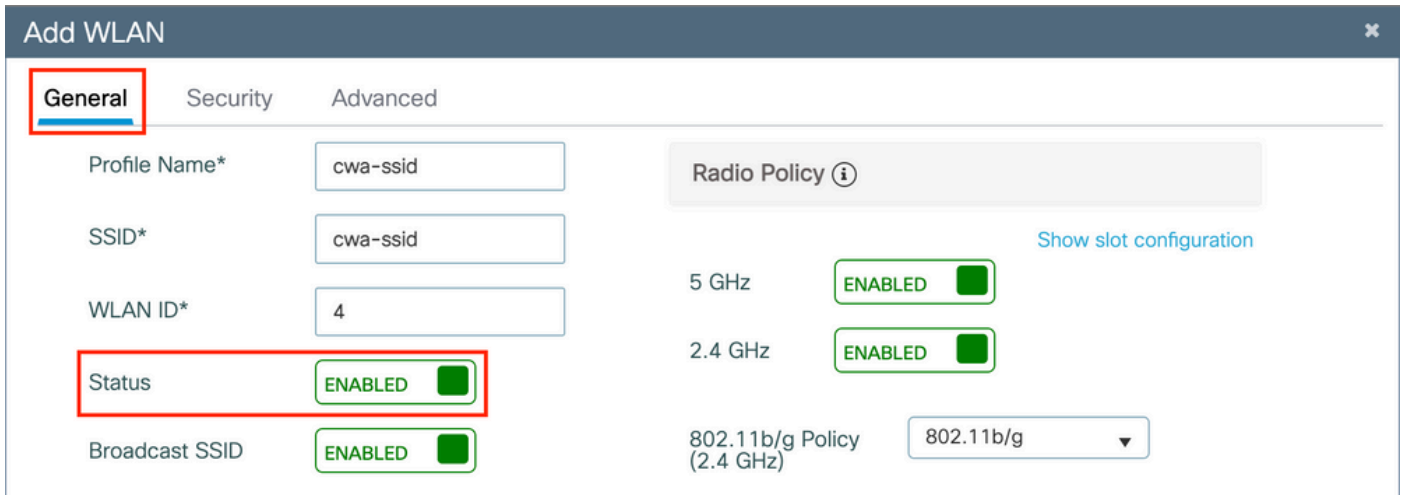
WLAN 配置

步骤1:创建WLAN。

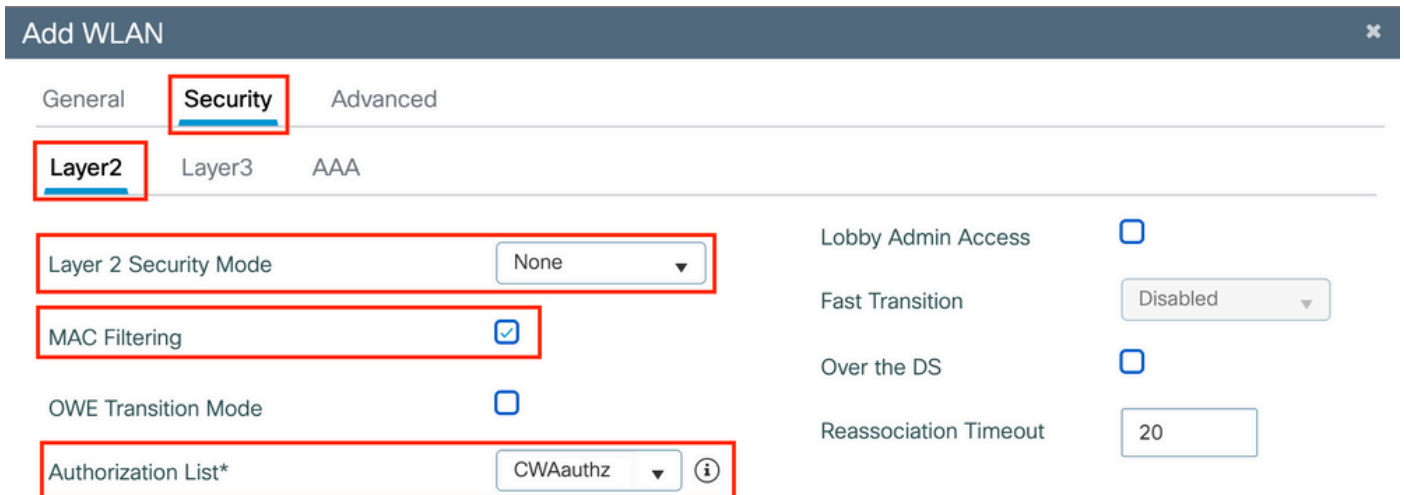
根据需要导航到Configuration > Tags & Profiles > WLANs > + Add 并配置网络。



第二步：输入WLAN常规信息。



第三步：导航到选Security 项卡，然后选择所需的安全方法。在这种情况下，只需要“MAC过滤”和AAA授权列表(在AAA Configuration 部分的步骤2中创建)。



CLI :

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

```
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

策略配置文件配置

在策略配置文件中，您可以决定将客户端分配到哪个VLAN，以及其他设置(例如访问控制列表(ACL)、服务质量(QoS)、移动锚点、计时器等)。

您可以使用默认策略配置文件，也可以新建策略配置文件。

GUI:

步骤1:新建Policy Profile。

导航到Configuration > Tags & Profiles > Policy 并配置default-policy-profile 或创建新配置。

The screenshot displays the 'Policy Profile' configuration interface. On the left is a dark sidebar with a search bar and menu items: 'Dashboard', 'Monitoring', 'Configuration' (highlighted), and 'Administration'. The main content area has a title 'Policy Profile' and two buttons: '+ Add' (highlighted with a red box) and 'x Delete'. Below these is a table with two columns: 'Policy Profile Name' and 'Description'. The table contains two entries: 'voice' and 'default-policy-profile' (highlighted with a red box). At the bottom of the table is a pagination control showing '1' items per page.

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

确保已启用配置文件。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

第二步：选择VLAN。

导航到Access Policies 选项卡，从下拉列表中选择VLAN名称或手动键入VLAN-ID。请勿在策略配置文件中配置 ACL。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

第三步：配置策略配置文件以接受ISE覆盖（允许AAA覆盖）和授权更改(CoA）（NAC状态）。您也可以选择指定审计方法。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="CWAacct"/> ⓘ ✕

WGB Parameters

Broadcast Tagging	<input type="checkbox"/>
WGB VLAN	<input type="checkbox"/>

Policy Proxy Settings

ARP Proxy	<input type="checkbox"/> DISABLED
IPv6 Proxy	<input type="text" value="None"/>

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles


Tunnel Profile

CLI :

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

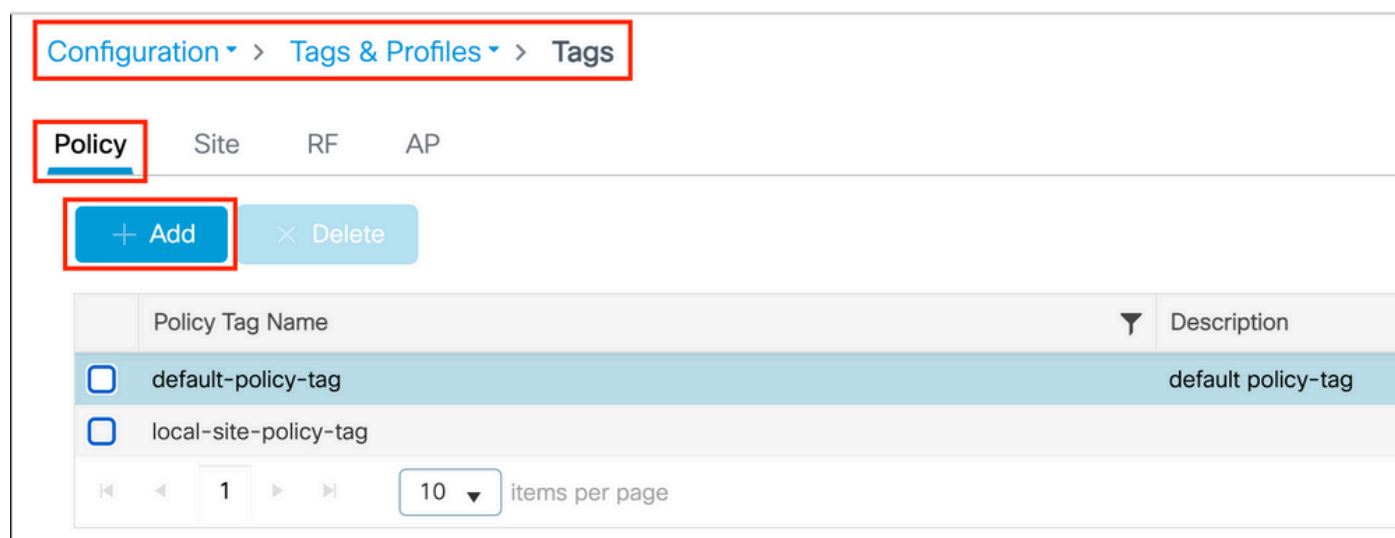
策略标签配置

在策略标签中，您可以将 SSID 与策略配置文件相关联。您可以新建策略标签，也可以使用 default-policy 标签。

 **注意：** default-policy 标记会自动将 WLAN ID 介于 1 到 16 之间的任何 SSID 映射到默认策略配置文件。不能修改或删除。如果有 ID 为 17 或更高的 WLAN，则不能使用 default-policy 标记。

GUI:

导航到 Configuration > Tags & Profiles > Tags > Policy 并根据需要添加新条目，如图所示。



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag
<input type="checkbox"/> local-site-policy-tag	

1 10 items per page

将 WLAN 配置文件关联到所需的策略配置文件。

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

↶ Cancel
📄 Apply to Device

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

策略标签分配

将策略标签分配给所需的 AP。


GUI:

要将标签分配给一个AP，请导航到Configuration > Wireless > Access Points > AP Name > General Tags，进行所需的分配，然后点击 Update & Apply to Device。

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.</p>
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

 **注意：** 请注意，更改AP上的策略标记后，它将失去与9800 WLC的关联，并在大约1分钟内重新加入。

要为多个AP分配相同的策略标记，请导航到Configuration > Wireless > Wireless Setup > Advanced > Start Now。

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



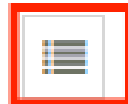
RF Tag



Apply

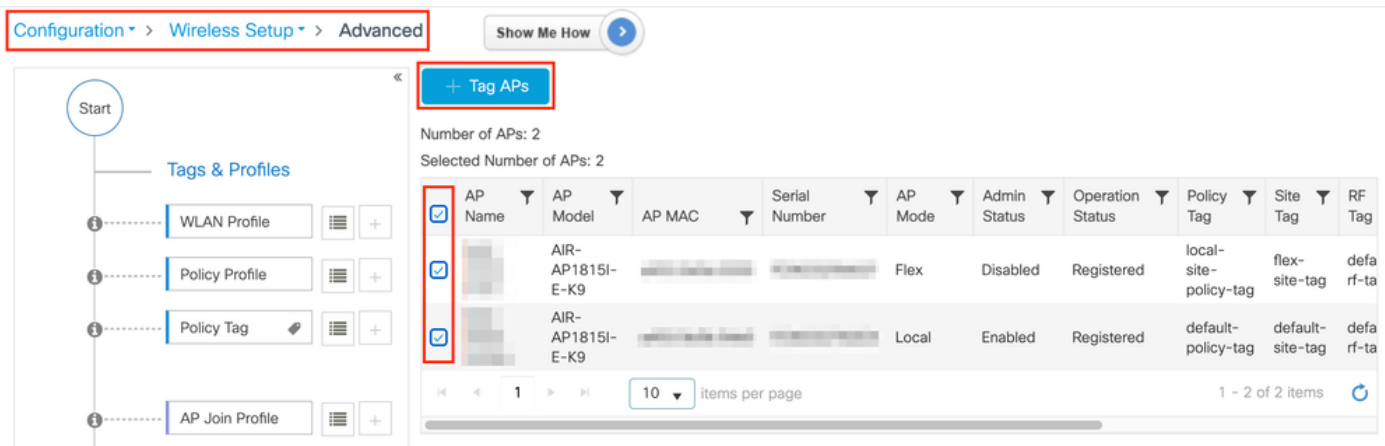


Tag APs

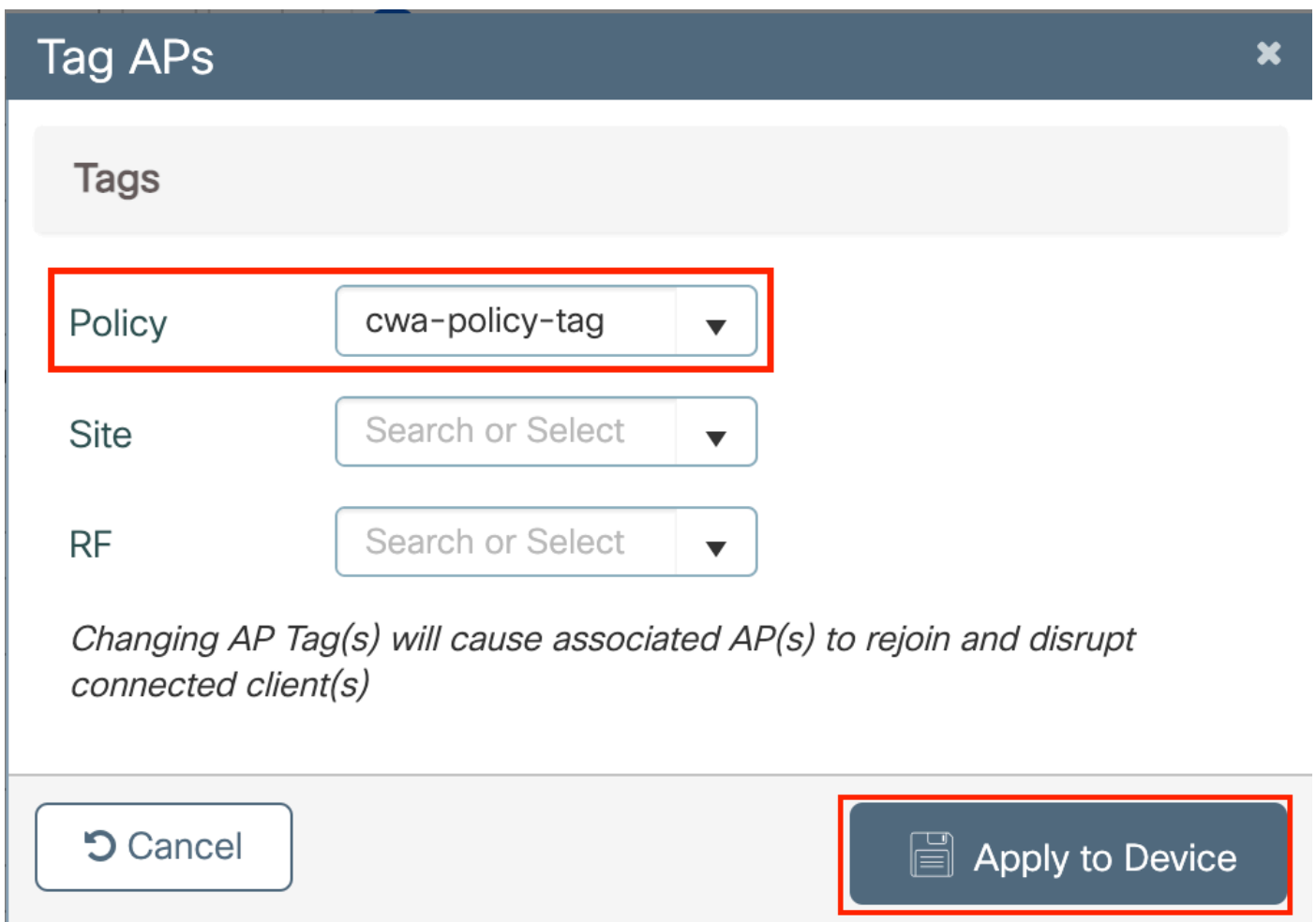


Start Now →

Done



选择所需的标记，然后单击Save & Apply to Device (如图所示)。



CLI :

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```

重定向 ACL 配置

步骤1:导航到Configuration > Security > ACL > + Add 以创建新的ACL。

为ACL选择一个名称，然后使其按照IPv4 Extended 顺序键入并添加每个规则，如图所示。

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type Host Name* ! This field is mandatory

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
0										


10 items per page No items to display

您需要拒绝流向 ISE PSN 节点的流量以及 DNS，同时允许所有其余流量。此重定向ACL不是安全ACL，而是传送ACL，它定义哪些流量进入CPU进行进一步处理（如重定向）以及哪些流量停留在数据平面（拒绝上）并避免重定向。

ACL必须如下所示（在本例中用您的ISE IP地址替换10.48.39.28）：


Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

1 items per page 1 - 5 of 5 items

 **注意：**对于重定向ACL，请将deny操作视为拒绝重定向（而不是拒绝流量），将permit操作视为允许重定向。WLC仅检查可重定向的流量（默认情况下为端口80和443）。

CLI :

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

 **注意：**如果使用permit ip any any结束ACL而不是侧重于端口80的permit，则WLC还会重定向HTTPS，这通常是多余的，因为它必须提供自己的证书，并始终会创建证书违规。上述语句的例外情况是，在CWA的情况下，您不需要在WLC上使用证书：如果您启用了HTTPS拦截，则需要一个证书，但无论如何它都不被视为有效。

您可以通过仅拒绝访客端口8443至ISE服务器的操作来改进ACL。

为HTTP或HTTPS启用重定向

Web管理员门户配置与Web身份验证门户配置绑定，它需要在端口80上侦听才能重定向。因此，必须启用HTTP才能使重定向正常工作。您可以选择全局启用它(使用命令ip http server)，或者可以仅为Web身份验证模块启用HTTP(使用参数映射下的命令webauth-http-enable)。



注意：HTTP流量的重定向在CAPWAP内部发生，即使在FlexConnect本地交换的情况下也是如此。由于是WLC执行侦听工作，因此AP在CAPWAP隧道内发送HTTP(S)数据包，并在CAPWAP中接收从WLC返回的重定向

如果您希望在尝试访问HTTPS URL时进行重定向，请在参数映射下添加命令intercept-https-enable，但请注意，此配置不是最佳配置，因为它仍然影响WLC CPU并生成证书错误：

<#root>

```
parameter-map type webauth global
type webauth
```

intercept-https-enable

trustpoint xxxxx

您还可以通过GUI执行此操作，在参数映射(Configuration > Security > Web Auth)中选中选项“Web Auth intercept HTTPS”。

The screenshot displays the configuration interface for Web Auth. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth' and includes '+ Add' and '× Delete' buttons. Below these is a table with the following structure:

Parameter Map Name
<input type="checkbox"/> global

Below the table is a pagination control showing '1' and '10 items per page'. On the right side, the 'Edit Web Auth Parameter' panel is visible, containing the following settings:

- Maximum HTTP connections: 100
- Init-State Timeout(secs): 120
- Type: webauth
- Virtual IPv4 Address: (empty)
- Trustpoint: --- Select ---
- Virtual IPv6 Address: :::::XX
- Web Auth intercept HTTPS:** (highlighted with a red box)
- Captive Bypass Portal:

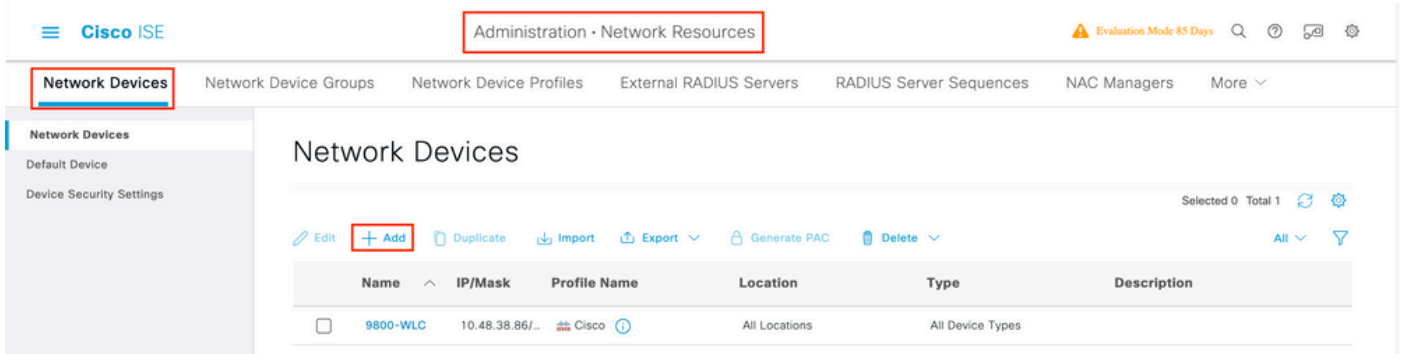


注意：默认情况下，浏览器使用HTTP网站启动重定向过程，如果需要HTTPS重定向，则必须选中Web Auth intercept HTTPS；但是，不建议使用此配置，因为它会增加CPU使用率。

ISE 配置

将 9800 WLC 添加到 ISE

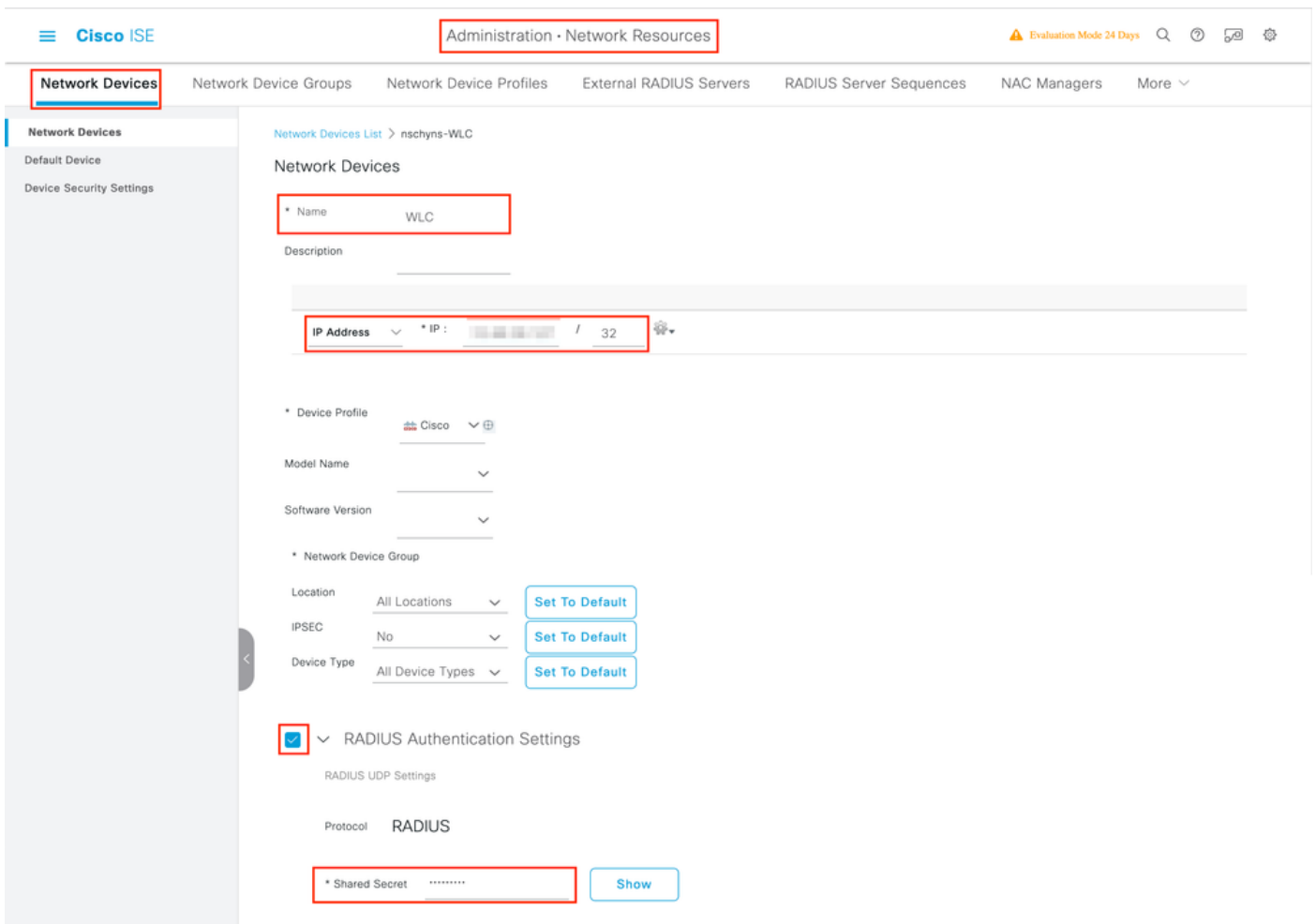
步骤1: 打开ISE控制台并导航至Administration > Network Resources > Network Devices > Add (如图所示)。



第二步：配置网络设备。

或者，它可以是指定的型号名称、软件版本和说明，并根据设备类型、位置或WLC分配网络设备组。

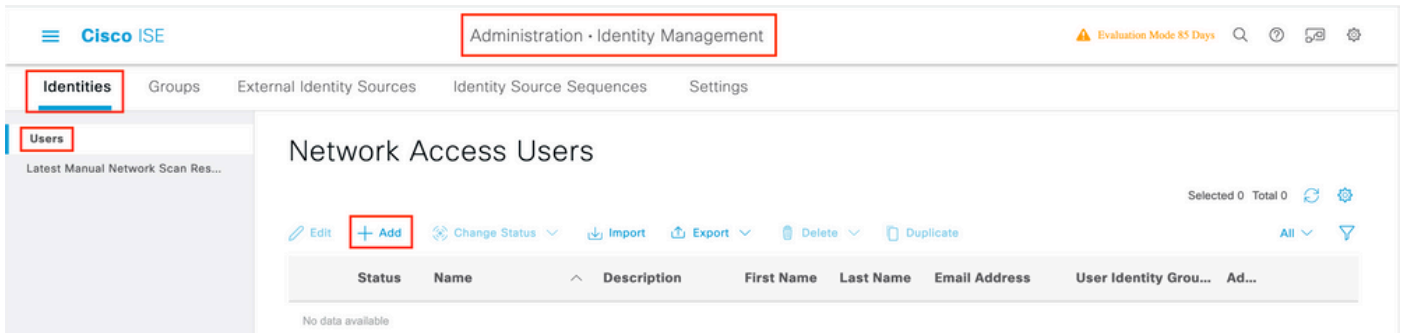
此处的IP地址与发送身份验证请求的WLC接口对应。默认情况下，它是管理接口，如图所示：



有关网络设备组的详细信息，请参阅ISE管理员指南章节：管理网络设备：[ISE_网络设备组](#)。

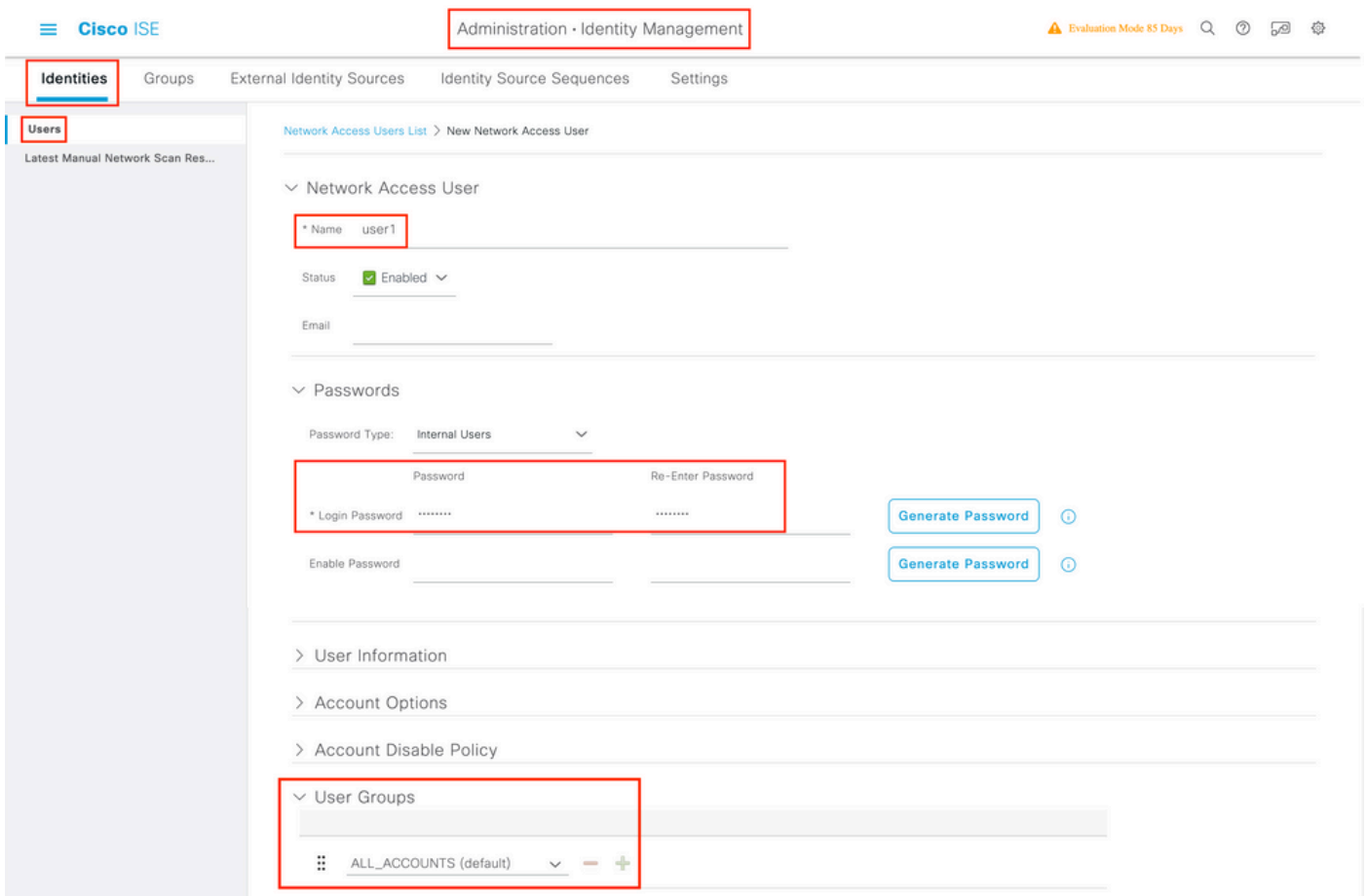
在 ISE 上创建新用户

步骤1:导航至Administration > Identity Management > Identities > Users > Add 如图所示。



第二步：输入相关信息。

在本示例中，此用户属于名为ALL_ACCOUNTS的组，但可以根据需要进行调整，如图所示。

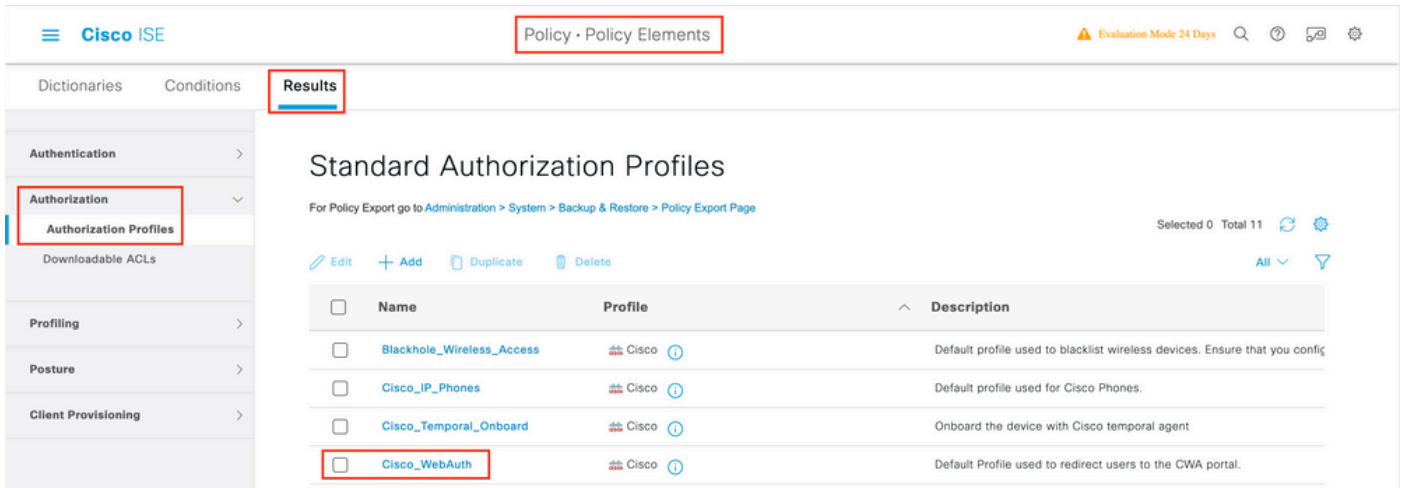


创建授权配置文件

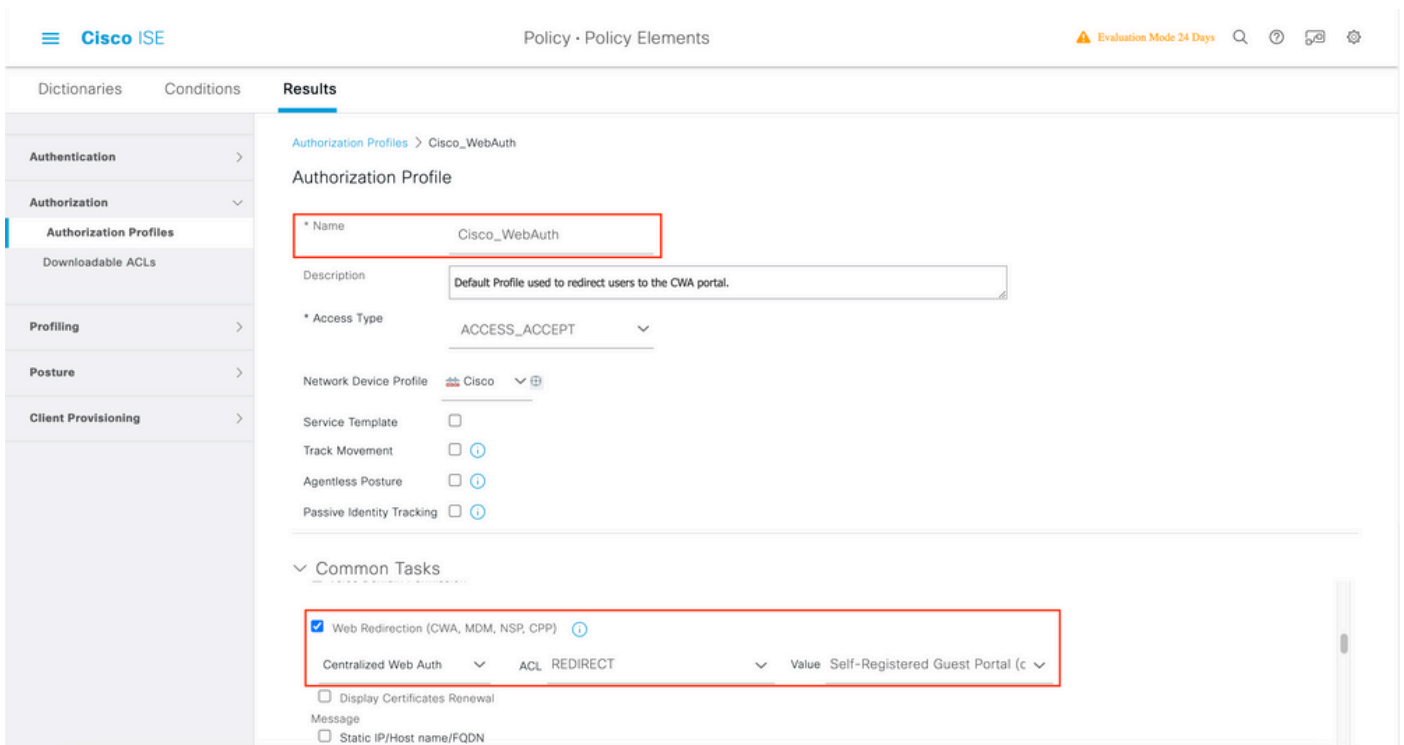
策略配置文件是根据客户端参数（例如mac地址、凭证、使用的WLAN等）分配给客户端的结果。它可以分配特定设置，如虚拟局域网(VLAN)、访问控制列表(ACL)、统一资源定位器(URL)重定向等。

请注意，在最新版本的 ISE 中，已存在 Cisco_Webauth 授权结果。您可以对其进行编辑以修改重定向 ACL 名称，从而与 WLC 上配置的名称相一致。

步骤1:导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。单击add以创建您自己的结果或编辑 Cisco_Webauth默认结果。

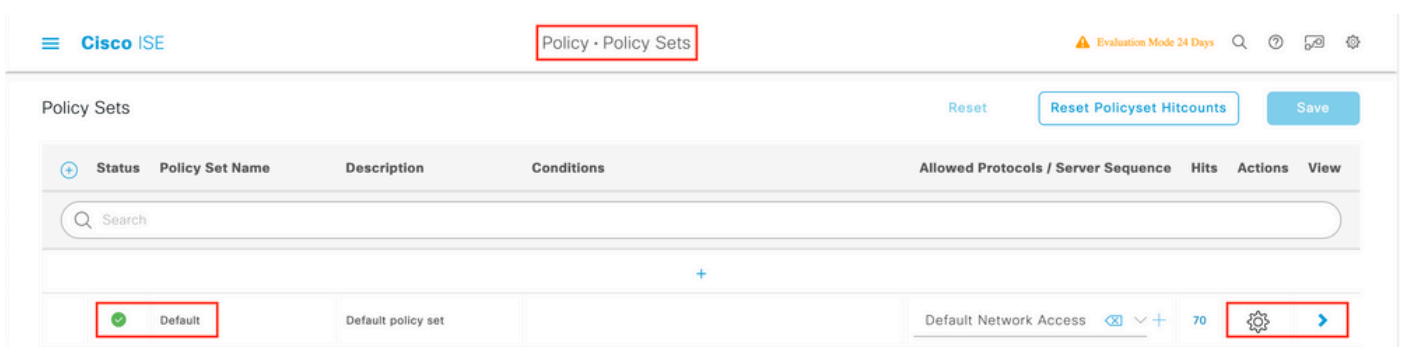


第二步：输入重定向信息。确保ACL名称与9800 WLC上配置的ACL名称相同。

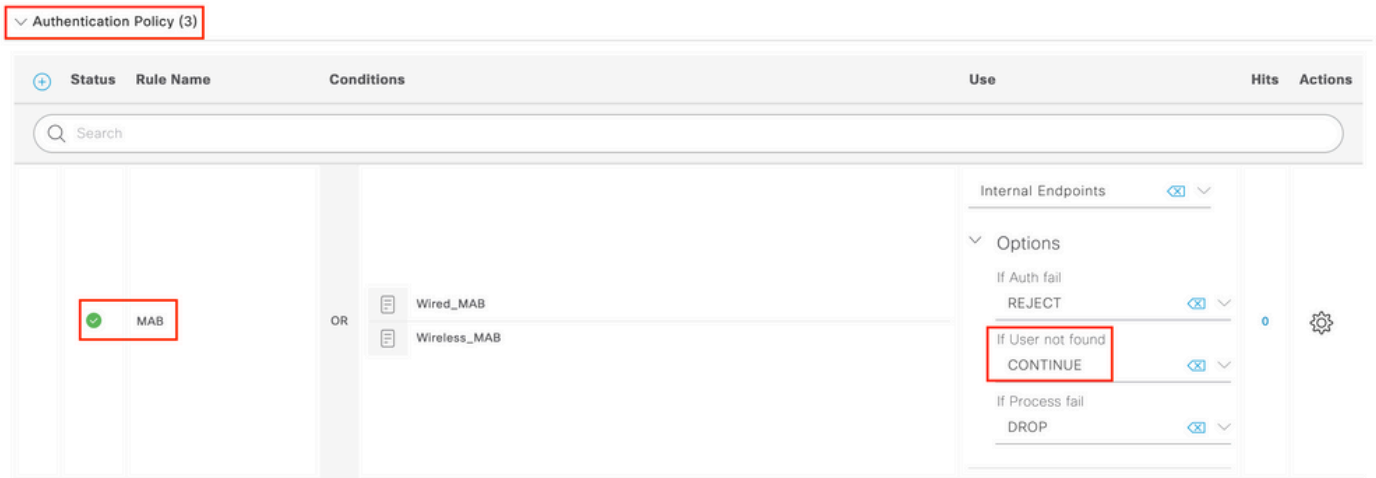


配置身份验证规则

步骤1: 策略集定义身份验证和授权规则的集合。要创建策略集，请导航至Policy > Policy Sets，点击列表中第一个策略集的齿轮，然后选Insert new row 择或点击右侧的蓝色箭头以选择默认策略集。



第二步：展开Authentication policy。对于MAB规则（匹配有线或无线MAB），展开Options，然后选择CONTINUE选项，以防您看到“If User not found”。



第三步：单击Save 以保存更改。

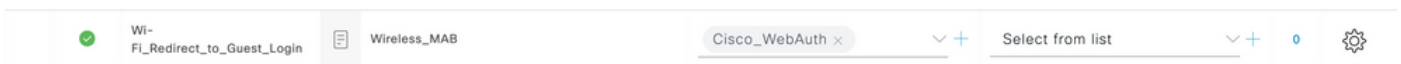
配置授权规则

授权规则负责确定将哪些权限（哪个授权配置文件）结果应用于客户端。

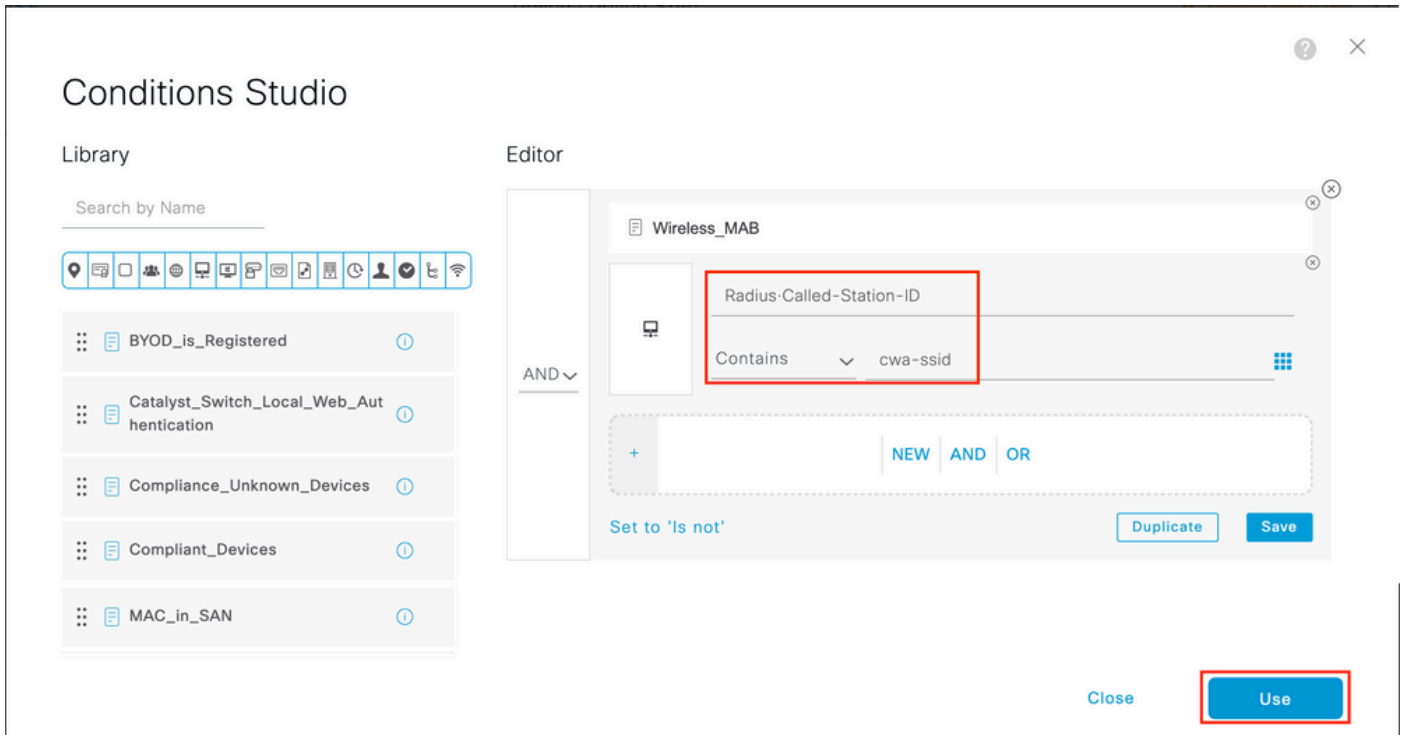
步骤1:在同一策略集页上，关闭Authentication Policy，然后展开Authorziation Policy，如图所示。



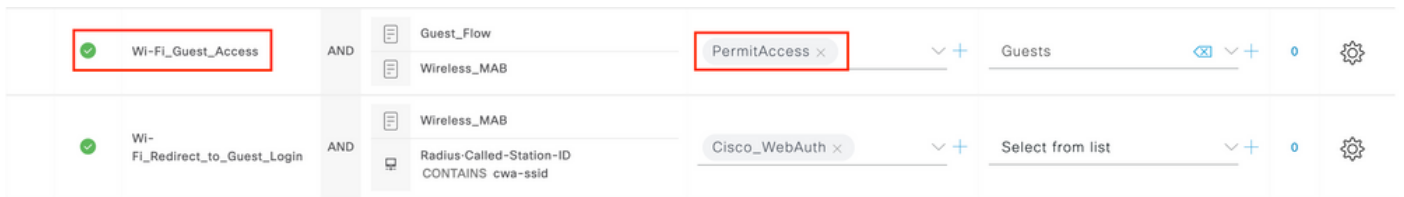
第二步：最近的ISE版本以名为Wifi_Redirect_to_Guest_Login的预创建规则开头，它最符合我们的需求。将左边的灰色符号转为enable。



第三步：该规则仅匹配Wireless_MAB并返回CWA重定向属性。现在，您可以选择添加一些小扭曲，使其仅与特定SSID匹配。选择条件(Wireless_MAB as of now)以显示条件工作室。在右侧添加条件，然后选择具有Called-Station-ID属性的Radius词典。使其与 SSID 名称匹配。使用屏幕底部的Use验证（如图所示）。



第四步：Guest Flow 现在，您需要与该条件匹配的第二个规则(以更高优先级定义)，以便在用户在门户上进行身份验证后返回网络访问详细信息。您可以使用Wifi Guest Access规则，该规则在默认情况下ISE最新版本上也是预先创建的。然后，只需启用左侧带有绿色标记的规则，您可以返回默认PermitAccess或配置更精确的访问列表限制。



第五步：保存规则。

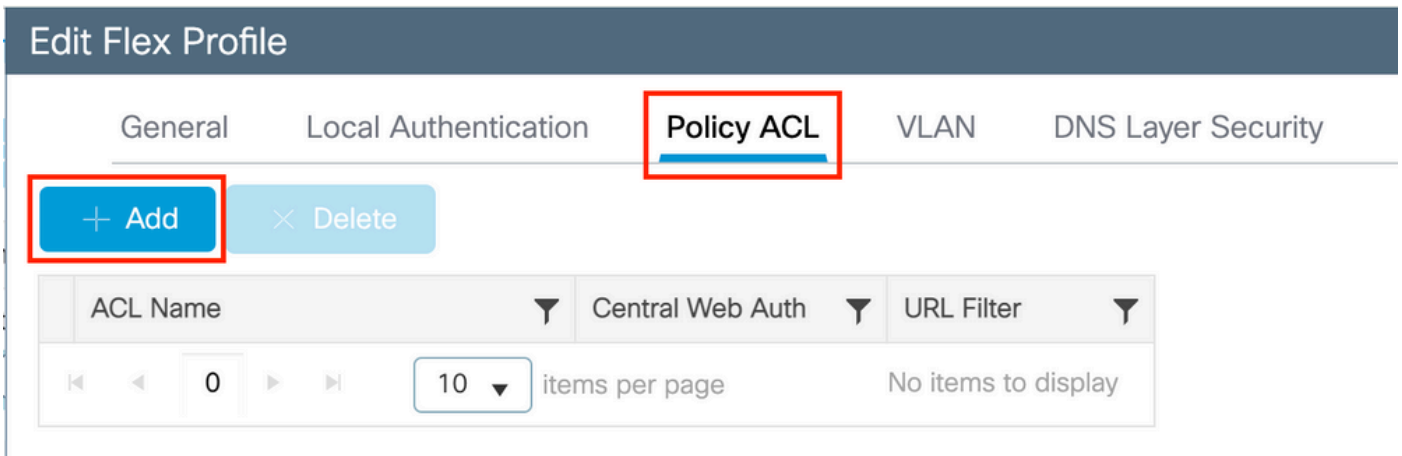
单击规则底部的Save。

仅限 FlexConnect 本地交换无线接入点

如果有 FlexConnect 本地交换无线接入点和 WLAN，该如何操作？前述部分仍然适用。但是，您需要执行额外的步骤，以便提前将重定向ACL推送到AP。

导航至Configuration > Tags & Profiles > Flex(可选)并选择您的Flex配置文件。然后，导航到Policy ACL选项卡。

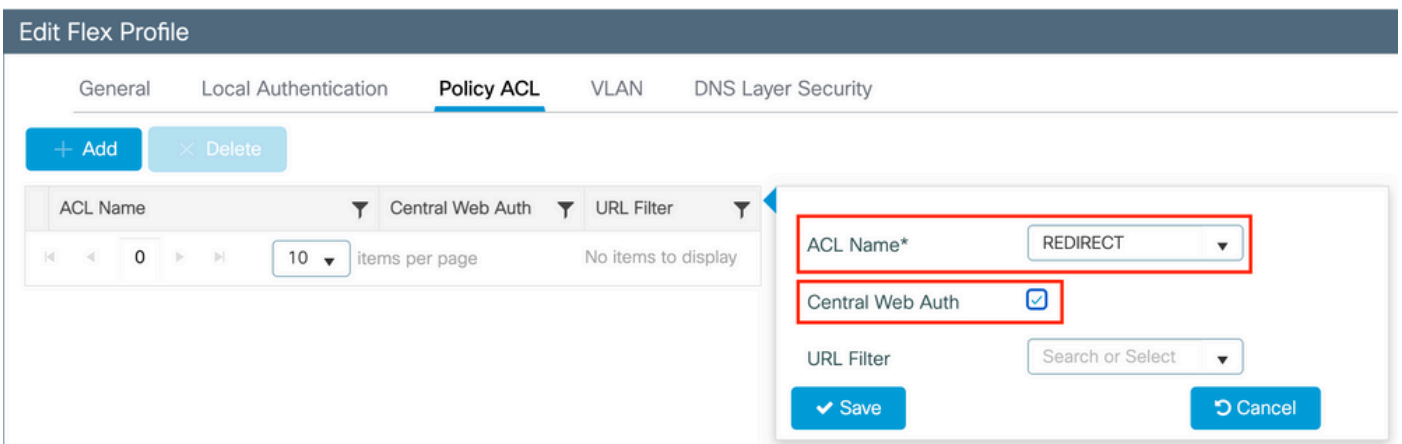
点击Add（如图所示）。



选择您的重定向ACL名称并启用集中Web身份验证。此复选框会自动反转AP自身上的ACL（这是因为“deny”语句表示Cisco IOS XE中WLC上的“不重定向到此IP”）。但是，在AP上，“deny”语句的含义相反。因此，该复选框会自动交换所有许可，并在推送到AP时拒绝这些许可。您可以通过AP CLI中的show ip access list命令验证这一点。

注意：在Flexconnect本地交换方案中，ACL必须特别提及返回语句（在本地模式下不一定需要），因此请确保所有ACL规则涵盖两种流量方式（例如，传入/传出ISE）。

不要忘记先按Save，然后再按Update and apply to the device。



证书

要使客户端信任Web身份验证证书，无需在WLC上安装任何证书，因为提供的唯一证书是ISE证书（必须受客户端信任）。

验证

您可以使用下列命令验证当前配置。

<#root>

```
# show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
# show ap tag summary
```

```
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

以下是与本示例相对应的WLC配置的相关部分：

<#root>

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

故障排除

核对清单

- 确保客户端连接并获得有效的IP地址。
- 如果重定向不是自动的，请打开浏览器并尝试使用随机IP地址。例如，10.0.0.1。如果重定向有效，则可能存在DNS解析问题。确认您拥有通过DHCP提供的有效DNS服务器，并且该服务器可以解析主机名。
- 确保您配置了命令ip http server，以使HTTP上的重定向正常运行。Web管理员门户配置与Web身份验证门户配置绑定，需要将其列在端口80上才能重定向。您可以选择全局启用它(使用命令ip http server)，或者可以仅为Web身份验证模块启用HTTP(使用参数映射下的命令webauth-http-enable)。
- 如果在尝试访问HTTPS URL时未重定向且这是必需的，请验证是否在参数映射下使用命令intercept-https-enable：

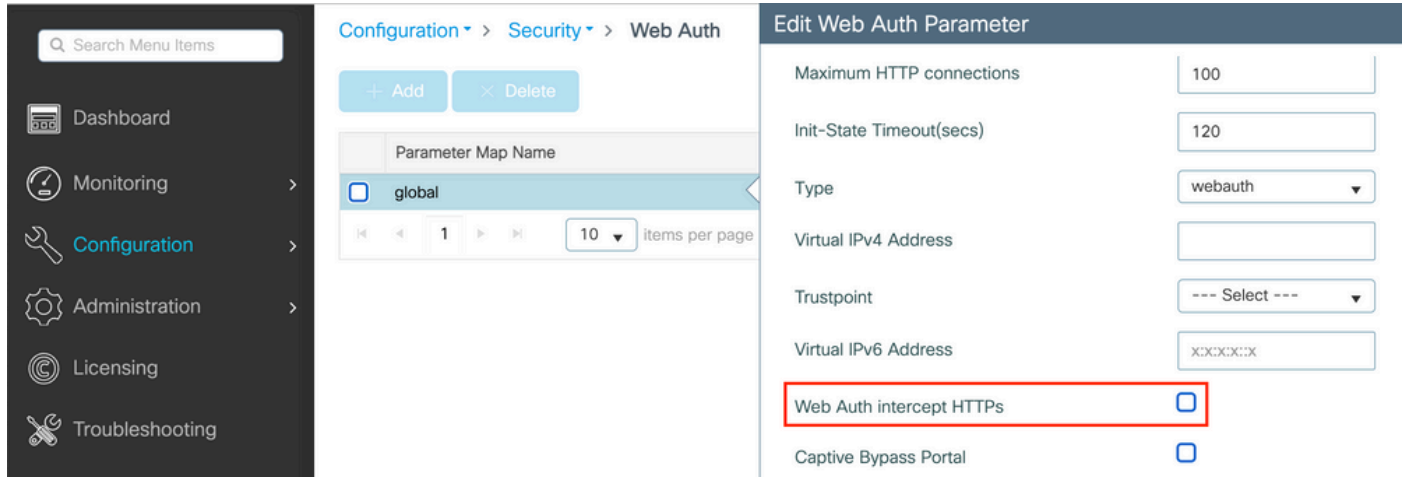
<#root>

```
parameter-map type webauth global
type webauth
```

`intercept-https-enable`

`trustpoint xxxxx`

您还可以通过GUI检查是否在参数映射中选中了Web Auth intercept HTTPS选项：



RADIUS的服务端口支持

Cisco Catalyst 9800系列无线控制器的服务端口称为GigabitEthernet 0端口。从版本17.6.1开始，此端口支持RADIUS（包括CoA）。

如果要将服务端口用于RADIUS，则需要以下配置：

```
<#root>
```

```
aaa server radius dynamic-author
client 10.48.39.28
```

```
vrf Mgmt-intf
```

```
server-key cisco123
```

```
interface GigabitEthernet0
```

```
vrf forwarding Mgmt-intf
```

```
ip address x.x.x.x x.x.x.x
```

```
!if using aaa group server:
```

```
aaa group server radius group-name
server name nicoISE
```

```
ip vrf forwarding Mgmt-intf
```

```
ip radius source-interface GigabitEthernet0
```

收集调试信息

WLC 9800 提供无间断跟踪功能。这样可以确保始终记录所有客户端连接相关的错误、警告和通知级别消息，并且可以在发生事故或故障情况后查看日志。



注意：您可以在日志中返回几小时到几天，但取决于生成的日志量。

要查看9800 WLC在默认情况下收集的跟踪，可以通过SSH/Telnet连接到9800 WLC并执行以下步骤（确保将会话记录到文本文件）。

步骤1:检查WLC当前时间，以便您可以在问题发生之前跟踪登录时间。

```
<#root>
```

```
# show clock
```

第二步：根据系统配置的指示，从WLC缓冲区或外部系统日志收集系统日志。这样可以快速查看系统的运行状况和错误（如果有）。

```
<#root>
```

```
# show logging
```

第三步：验证是否启用了任何调试条件。

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```



注意：如果看到列出了任何条件，则意味着遇到已启用条件（mac地址、IP地址等）的所有进程的跟踪都会记录到调试级别。这会增加日志量。因此，建议在不主动调试时清除所有条件。

第四步：假设测试中的mac地址未列为步骤3中的条件，收集特定mac地址的“永远在线”通知级别跟踪。

```
<#root>
```

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

您可以显示会话内容，也可以将文件复制到外部 TFTP 服务器。

```
<#root>
```

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件调试和无线电主动跟踪

如果永远在线跟踪不能为您提供足够的信息来确定所调查问题的触发因素，您可以启用条件调试并捕获无线活动(RA)跟踪，从而为与指定条件（本例中为客户端MAC地址）交互的所有进程提供调试级别跟踪。要启用条件调试，请继续执行以下步骤。

第五步：确保没有启用调试条件。

```
<#root>
```


```
# clear platform condition all
```


第六步：启用要监控的无线客户端mac地址的调试条件。

这些命令用于开始监控所提供的 MAC 地址，持续 30 分钟（1800 秒）。您可以选择延长监控时间，最多监控 2085978494 秒。

```
<#root>
```

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 注意：要同时监控多个客户端，请对每个mac地址运行debug wireless mac<aaaa.bbbb.cccc>命令。

 注意：您不会在终端会话中看到客户端活动的输出，因为所有内容都在内部缓冲，供以后查看。

步骤7'。重现要监控的问题或行为。

步骤 8如果在默认或配置的监控时间开启之前重现问题，请停止调试。

<#root>

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

一旦监控时间过去或调试无线停止，9800 WLC将生成一个本地文件，其名称为：

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤9.收集MAC地址活动的文件。您可以将ra trace .log复制到外部服务器或直接在屏幕上显示输出。

检查 RA 跟踪文件的名称。

<#root>

```
# dir bootflash: | inc ra_trace
```

将文件复制到外部服务器：

<#root>

```
# copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

显示内容：

```
<#root>
```

```
# more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤 10如果根本原因仍不明显，请收集内部日志，这些日志是调试级别日志的更详细视图。您无需再次调试客户端，因为我们只需进一步详细查看已收集和内部存储的调试日志。

```
<#root>
```

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```



注意：此命令输出返回所有进程的所有日志级别的跟踪，而且非常大。让Cisco TAC帮助分析这些跟踪。

您可以将ra-internal-FILENAME.txt复制到外部服务器或直接在屏幕上显示输出。

将文件复制到外部服务器：

```
<#root>
```

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

显示内容：

```
<#root>
```

```
# more bootflash:ra-internal-<FILENAME>.txt
```

步骤 11删除调试条件。

```
<#root>
```

```
# clear platform condition all
```



注意：请确保在故障排除会话之后始终删除调试条件。

Examples

如果身份验证结果不是您预期的结果，请务必导航到ISEOperations > Live logs页面并获取身份验证结果的详细信息。

系统将显示失败原因（如果出现故障）以及ISE接收的所有RADIUS属性。

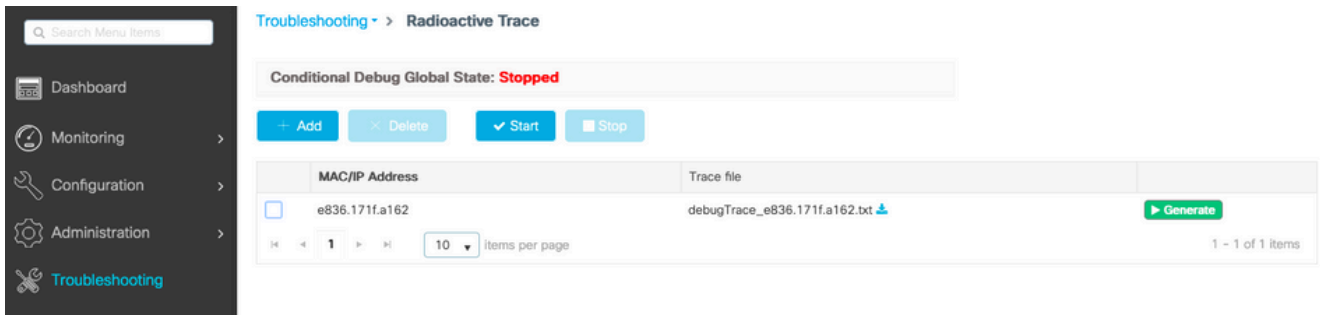
在下一个示例中，ISE 拒绝身份验证，原因在于没有匹配的授权规则。这是因为，您会看到Called-station-ID属性作为SSID名称附加到 AP mac地址，而授权与SSID名称完全匹配。当该规则更改为“包含”而非“等于”时，该规则会得到修复。

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1ype
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid



在这种情况下，问题出在您在创建ACL名称时输入了拼写错误，但该名称与ISE返回的ACL名称不匹配，或者WLC抱怨没有像ISE请求的ACL那样的ACL：

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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）。