

在Catalyst 9800上使用锚点配置中央Web身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置锚定到另一个Catalyst 9800的Catalyst 9800](#)

[网络图](#)

[在两台9800上配置AAA](#)

[在WLC上配置WLAN](#)

[在外部WLC上创建策略配置文件和策略标记](#)

[在锚点WLC上创建策略配置文件](#)

[在两个9800上重定向ACL配置](#)

[配置ISE](#)

[配置锚定到AireOS WLC的Catalyst 9800](#)

[Catalyst 9800外部配置](#)

[锚点AireOS WLC上的AAA配置](#)

[AireOS WLC上的WLAN配置](#)

[在AireOS WLC上重定向ACL](#)

[配置ISE](#)

[当AireOS WLC是外部WLC，而Catalyst 9800是锚时，配置的差异](#)

[验证](#)

[故障排除](#)

[Catalyst 9800故障排除信息](#)

[客户端详细信息](#)

[嵌入式数据包捕获](#)

[RadioActive跟踪](#)

[AireOS故障排除信息](#)

[客户端详细信息](#)

[从CLI调试](#)

[参考](#)

简介

本文档介绍如何在Catalyst 9800上配置并排除中心Web身份验证(CWA)的故障，该CWA指向另一个无线LAN控制器(WLC)作为移动锚点，使用AireOS或另一个9800 WLC覆盖目标。

先决条件

要求

建议您对9800 WLC、AireOS WLC和思科ISE有基本了解。假设在启动CWA锚点配置之前，您已在两个WLC之间建立移动隧道。这不在此配置示例的范围内。如果您需要帮助，请参阅标题为“[在Catalyst 9800控制器上构建移动隧道](#)”的文档。

使用的组件

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。

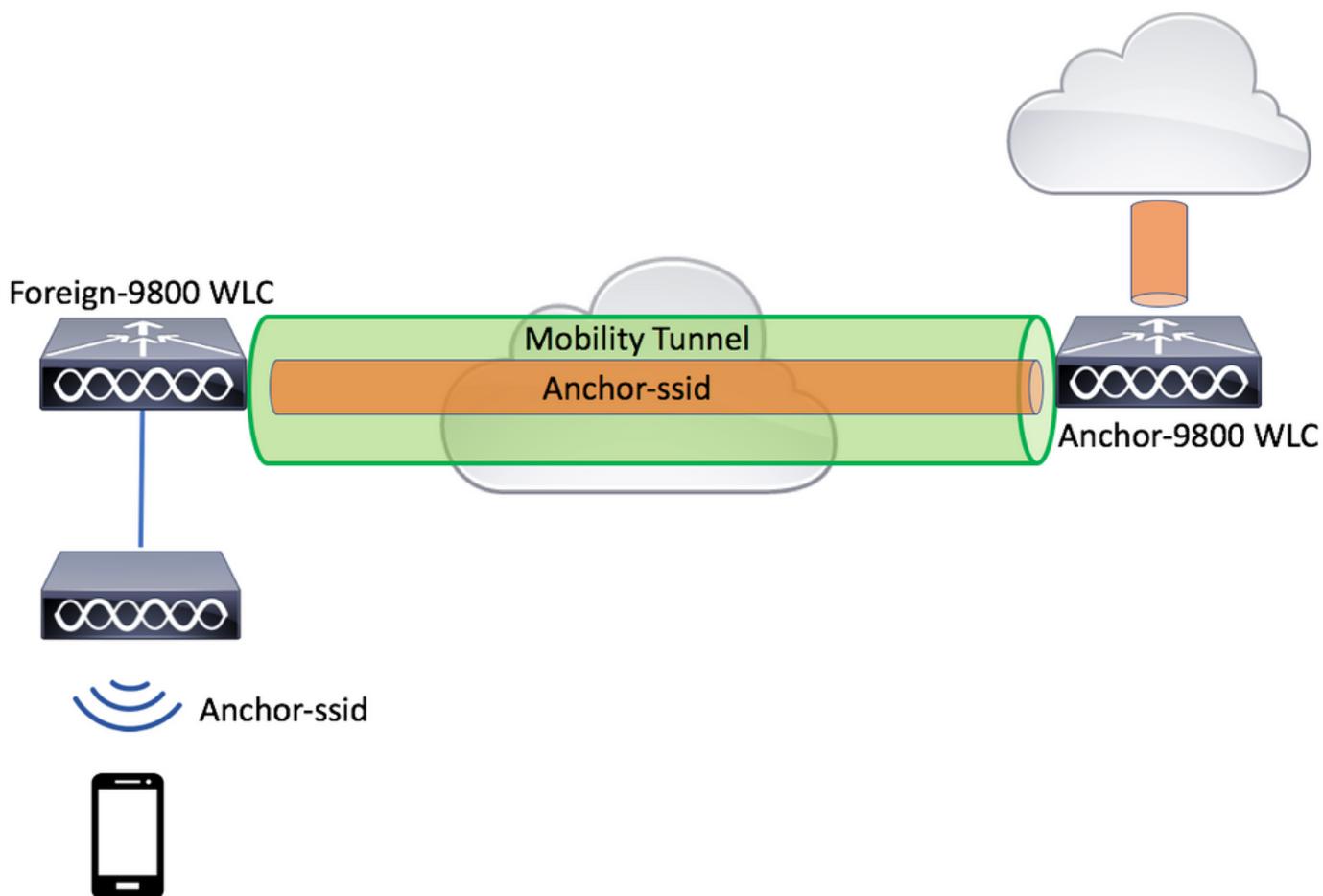
9800 17.2.1

5520 8.5.164 IRCM映像

ISE 2.4

配置锚定到另一个Catalyst 9800的Catalyst 9800

网络图



在两台9800上配置AAA

在锚点和外部，您需要先添加RADIUS服务器并确保已启用CoA。这可以在菜单中完成 Configuration>Security>AAA>Servers/Groups>Servers>单击Add按钮。

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Welcome admin
Last login Fri, May 15 2020 16:56:51 ...

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

+ Add Delete

RADIUS Servers

TACACS+ Server Groups

LDAP

Create AAA Radius Server

Name*	CLUS-Server
Server Address*	X.X.X.X
PAC Key	<input type="checkbox"/>
Key Type	Clear Text
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

Cancel Apply to Device

您现在需要创建一个服务器组，并将刚配置的服务器放入该组。此操作在此处完成
Configuration>Security>AAA>Servers/Groups>Server Groups>+Add。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS Servers Server Groups

TACACS+

LDAP

Create AAA Radius Server Group

Name* CLUS-Server-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers Assigned Servers

CLUS-Server

Cancel Apply to Device

现在，创建一个**授权方法列表**（CWA不需要身份验证方法列表），其中类型为network，组类型为group。将上一操作中的服务器组添加到此方法列表。

此配置在此处完成**Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top is **Configuration > Security > AAA**. The left sidebar shows the navigation menu with **Configuration** selected. The main content area is titled **AAA Method List** and includes a **+ Add** button. Below this, the **Authorization** tab is active. A **Quick Setup: AAA Authorization** dialog box is open, showing the following configuration details:

- Method List Name***: CLUS-AuthZ-Meth-List
- Type***: network
- Group Type**: group
- Fallback to local**:
- Authenticated**:
- Available Server Groups**: radius, ldap, tacacs+, ISE1
- Assigned Server Groups**: CLUS-Server-Group

At the bottom of the dialog, there are **Cancel** and **Apply to Device** buttons.

(可选) 使用与授权方法列表相同的服务器组创建记帐方法列表。可以在此处创建记帐列表
Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar contains menu items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled "AAA Method List" and includes tabs for "Servers / Groups", "AAA Method List", and "AAA Advanced". Under the "AAA Method List" tab, there are sections for "Authentication", "Authorization", and "Accounting". The "Accounting" section is highlighted, and a "+ Add" button is visible. A modal window titled "Quick Setup: AAA Accounting" is open, showing the following configuration details:

- Method List Name*: CLUS-Acct-Meth-List
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for "Cancel" and "Apply to Device" are located at the bottom of the modal.

在WLC上配置WLAN

在两个WLC上创建和配置WLAN。两个WLAN上的WLAN应匹配。安全类型应为mac过滤，应应用上一步的授权方法列表。此配置在Configuration>Tags & Profiles>WLANs>+Add下完成

← Cisco 17.2.1 Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Profile Name* CLUS-WLAN-Name Radio Policy All

SSID* CLUS-SSID Broadcast SSID ENABLED

WLAN ID* 2

Status ENABLED

Cancel Apply to Device

← Cisco 17.2.1 Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None Lobby Admin Access

MAC Filtering Fast Transition Adaptive Enab...

OWE Transition Mode Over the DS

Authorization List* CLUS-AuthZ-Meth-l Reassociation Timeout 20

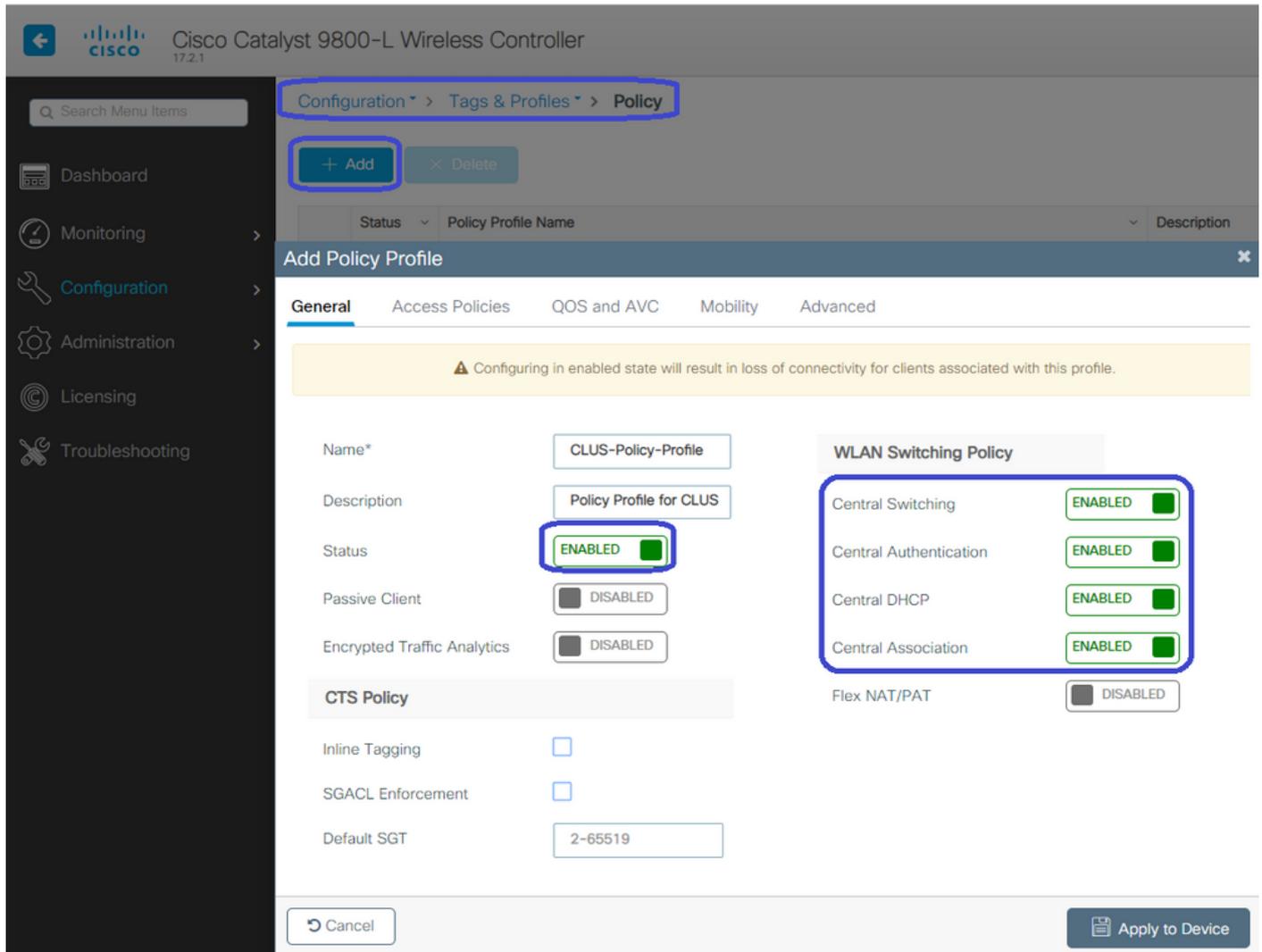
Cancel Apply to Device

在外部WLC上创建策略配置文件和策略标记

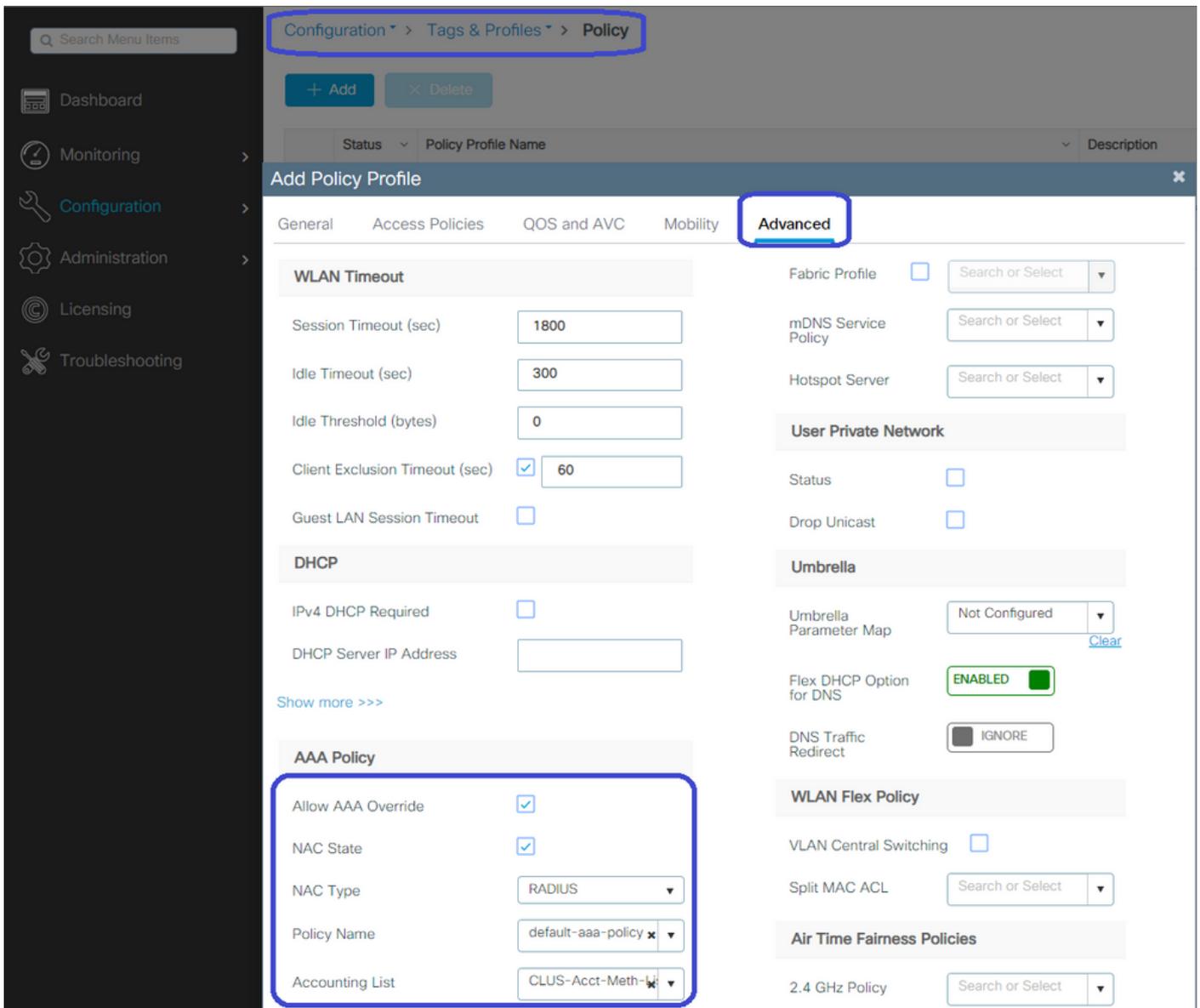
转到外部WLC Web UI。

要创建策略配置文件，请转到**Configuration>Tags & Profiles>Policy>+Add**

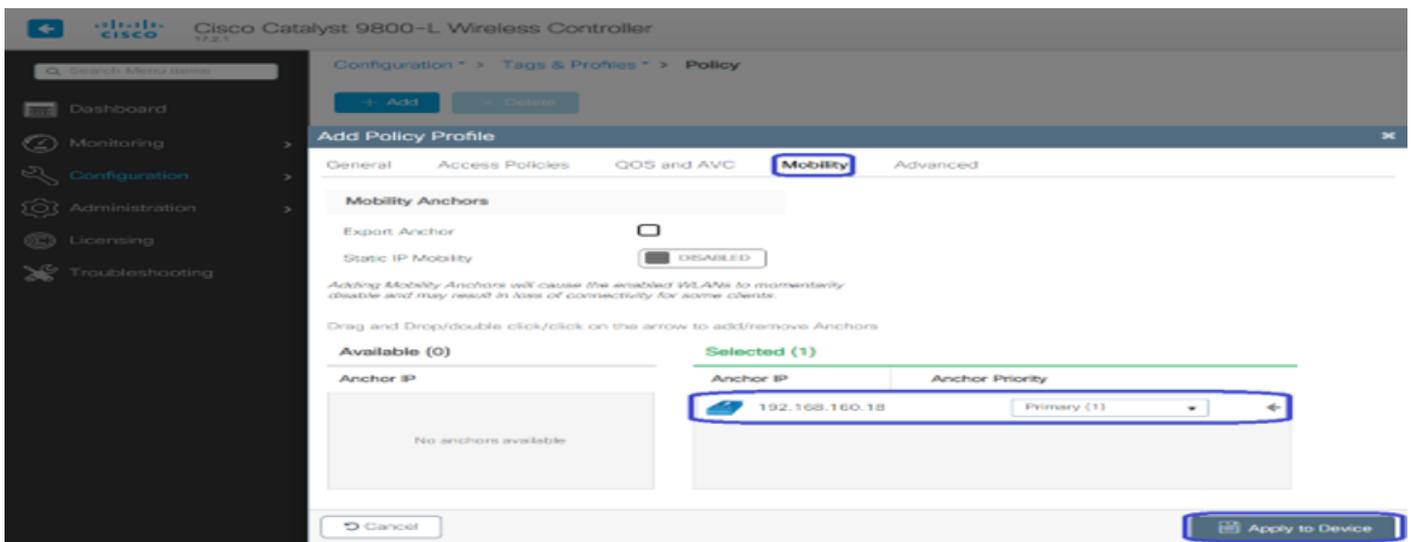
锚定时，必须使用中央交换。



在“高级”选项卡上，AAA覆盖和RADIUS NAC对于CWA是必需的。如果选择创建会计方法列表，您也可以在此处应用该会计方法列表。



在“移动”选项卡上，不选中“导出锚点”复选框，而是将锚点WLC添加到锚点列表。确保点击“应用到设备”。提醒一下，这假定您已在两个控制器之间建立移动隧道



要使AP使用此策略配置文件，您需要创建策略标记并将其应用到您希望使用的AP。

要创建策略标记，请转至Configuration>Tags & Profiles>Tags?Policy>+Add

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

Policy Tag Name

Add Policy Tag

Name* CLUS-Policy-Tag

Description Policy Tag for CLUS

WLAN-POLICY Maps: 0

+ Add × Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Map WLAN and Policy

WLAN Profile* CLUS-WLAN-Name Policy Profile* CLUS-Policy-Profile

× ✓

RLAN-POLICY Maps: 0

Cancel Apply to Device

要同时将其添加到多个AP，请转至**Configuration>Wireless Setup>Advanced>Start Now**。点击“标记AP”旁的项目符号栏，将标记添加到您选择的AP。

Configuration > Wireless Setup > Advanced

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

- Tag APs

Done

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

AP Name	AP Model	AP MAC	AP Mode
<input checked="" type="checkbox"/> Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local
<input checked="" type="checkbox"/> Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local
<input checked="" type="checkbox"/> AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local

1 10 items per page

Tag APs

Tags

Policy: CLUS-Policy-Tag

Site: Search or Select

RF: Search or Select

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

在锚点WLC上创建策略配置文件

转到锚点WLC Web UI。在锚点9800上的Policy Profile（策略配置文件）下**Configuration（配置）> Tags & Profiles（标记和配置文件）> Tags（标记）> Policy（策略）>+Add（添加）**。确保这与在外部创建的策略配置文件匹配，但移动选项卡和记帐列表除外。

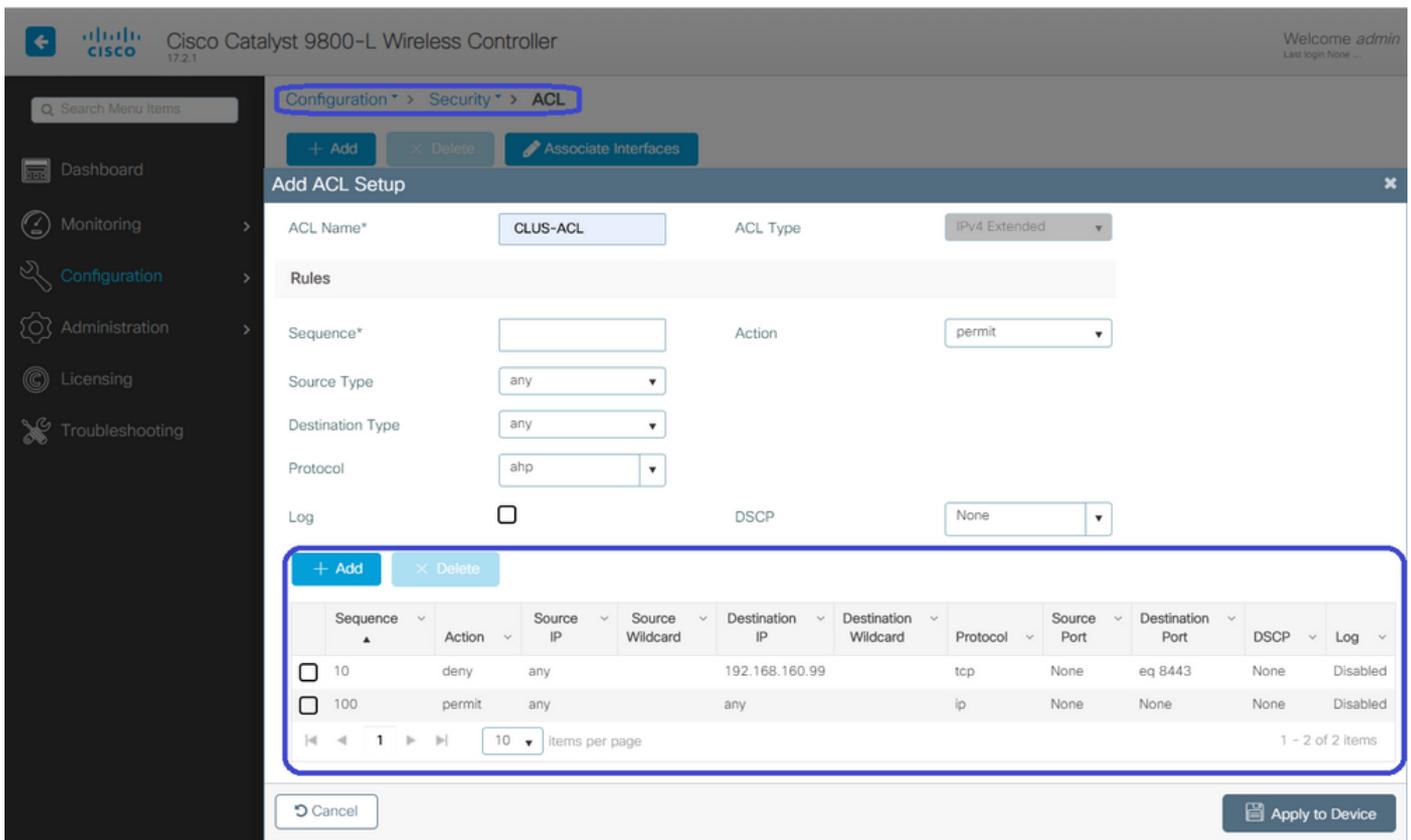
在此，您不添加锚点，但是您确实选中了“导出锚点”复选框。请勿在此处添加会计列表。提醒一下，这假定您已在两个控制器之间建立移动隧道

注意：没有理由将此配置文件与策略标记中的WLAN关联。如果您这样做，会造成问题。如果要对此WLC上的AP使用相同的WLAN，请为其创建另一个策略配置文件。

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Policy. The 'Add Policy Profile' dialog is open, with the 'Mobility' tab selected. In the 'Mobility Anchors' section, the 'Export Anchor' checkbox is checked, and the 'Static IP Mobility' toggle is set to 'DISABLED'. A warning message states: 'Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.' Below this, there is a section for 'Available (1)' anchors, with one anchor IP '192.168.160.16' listed. The 'Selected (0)' section is currently empty, displaying 'Anchors not assigned'. At the bottom of the dialog, there are 'Cancel' and 'Apply to Device' buttons.

在两个9800上重定向ACL配置

接下来，您需要在两个9800上创建重定向ACL配置。外部上的条目无关紧要，因为它将是将ACL应用于流量的锚点WLC。唯一的要求是它在那里，并有一些入口。锚点上的条目必须“拒绝”访问端口8443上的ISE，并“允许”其他所有内容。此ACL仅应用于从客户端“传入”的流量，因此不需要返回流量的规则。DHCP和DNS将在ACL中没有条目时通过。

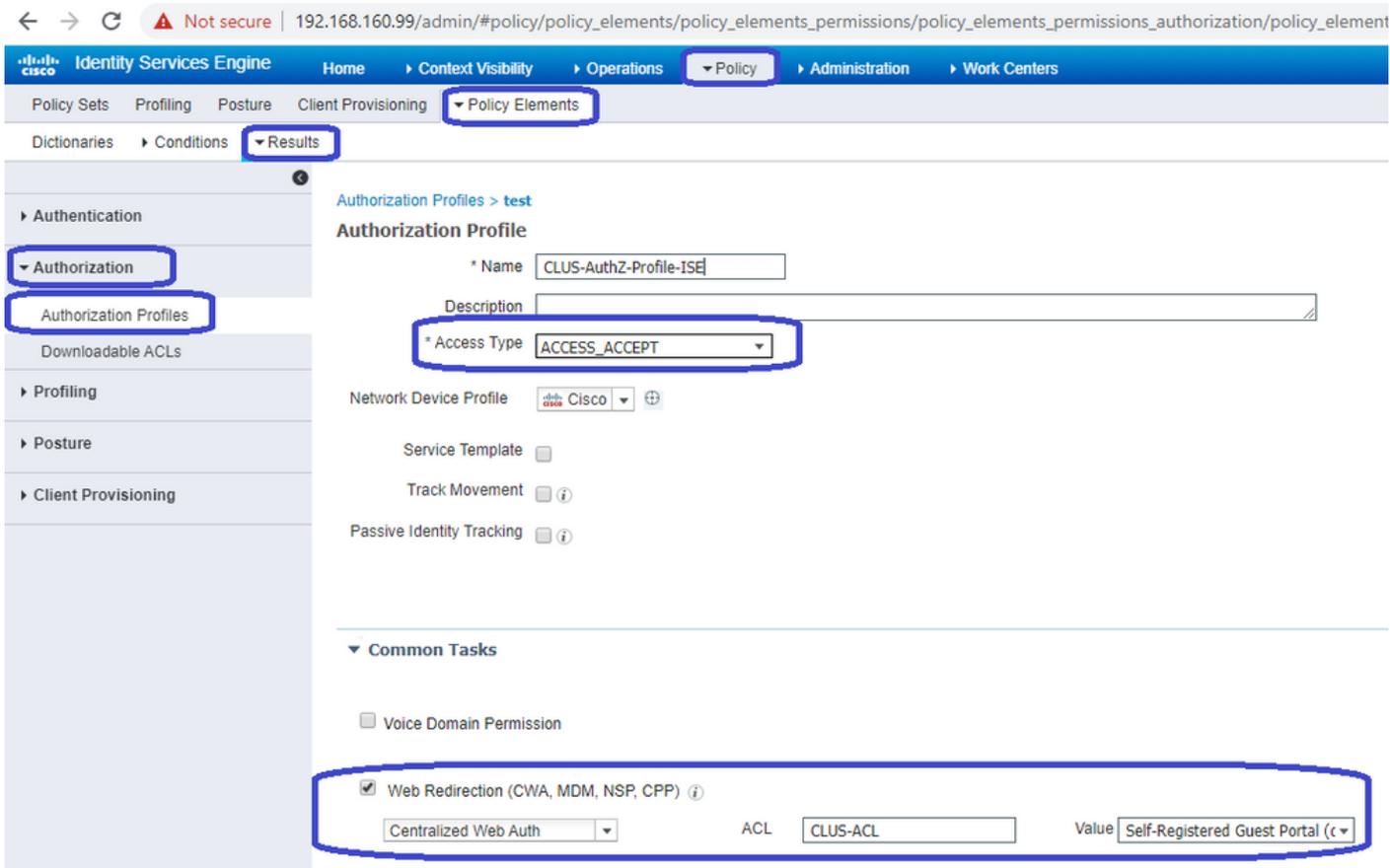


配置ISE

最后一步是为CWA配置ISE。此门户有大量选项，但此示例将坚持基本操作，并使用默认自注册访客门户。

在ISE上，您需要创建授权配置文件、使用身份验证策略设置的策略和使用授权配置文件的授权策略，将9800（外部）作为网络设备添加到ISE，并创建用户名和密码以登录网络。

要创建授权配置文件，请转到Policy>Policy Elements>Authorization>Results>Authorization Profiles>，然后单击Add。确保返回的访问类型为“access_accept”，然后设置要发回的AVP（属性一值对）。对于CWA，重定向ACL和重定向URL是必需的，但您也可以发送回VLAN ID和会话超时等内容。ACL名称必须与外部和锚点9800上重定向ACL的名称匹配。

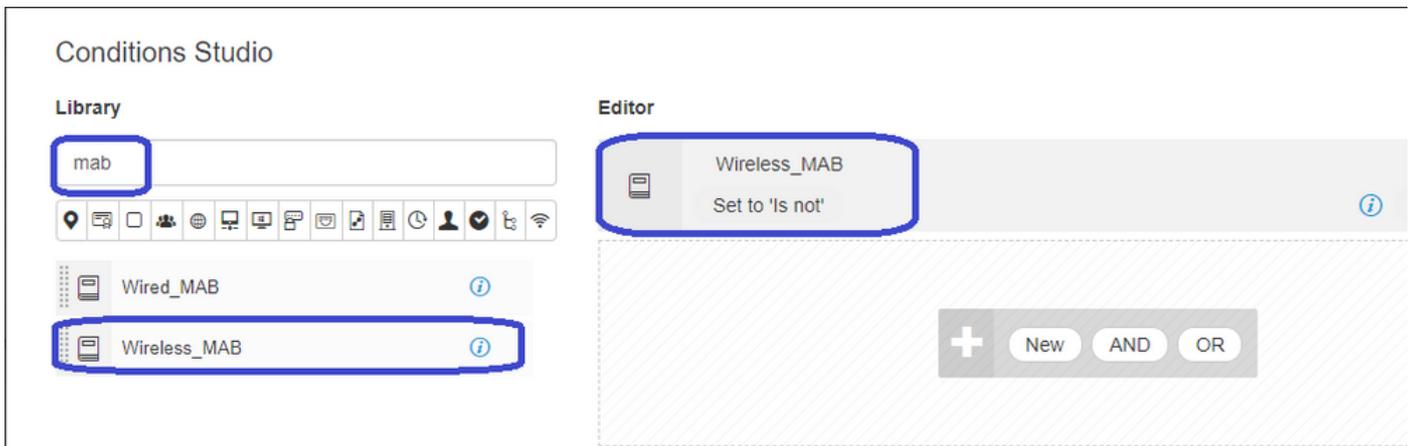


然后，您需要配置一种方法，将刚创建的授权配置文件应用到通过CWA的客户端。为此，一种方法是创建策略集，在使用MAB时绕过身份验证，并在使用在被叫站ID中发送的SSID时应用授权配置文件。同样，有很多方法可以做到这一点，所以如果你需要更具体或更安全的東西，那么，这只是最简单的方法。

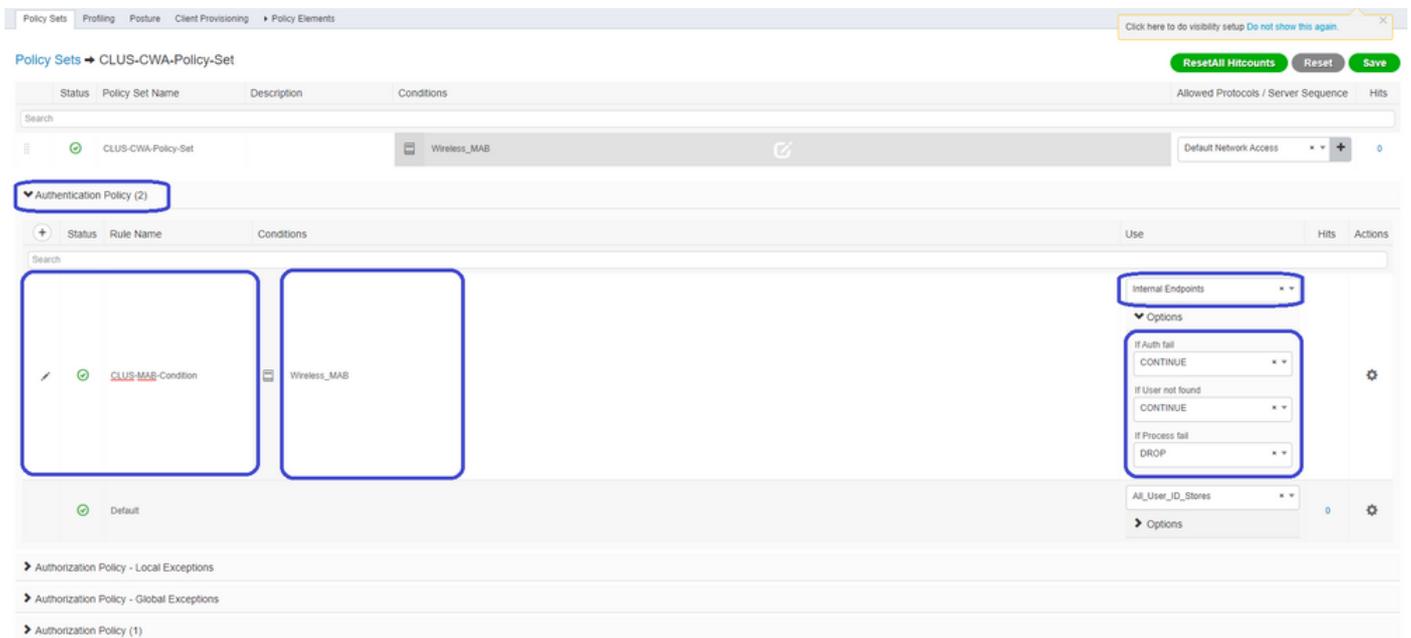
要创建策略集，请转至**Policy>Policy Sets**，然后按屏幕左侧的+按钮。将新策略集命名，并确保其设置为“默认网络访问”或允许MAB的“处理主机查找”的任何允许的协议列表（以检查允许的协议列表，请转至**Policy>Policy Elements>Results>Authentication>Allowed Protocols**）。现在，在您创建的新策略集中间点击该+号。



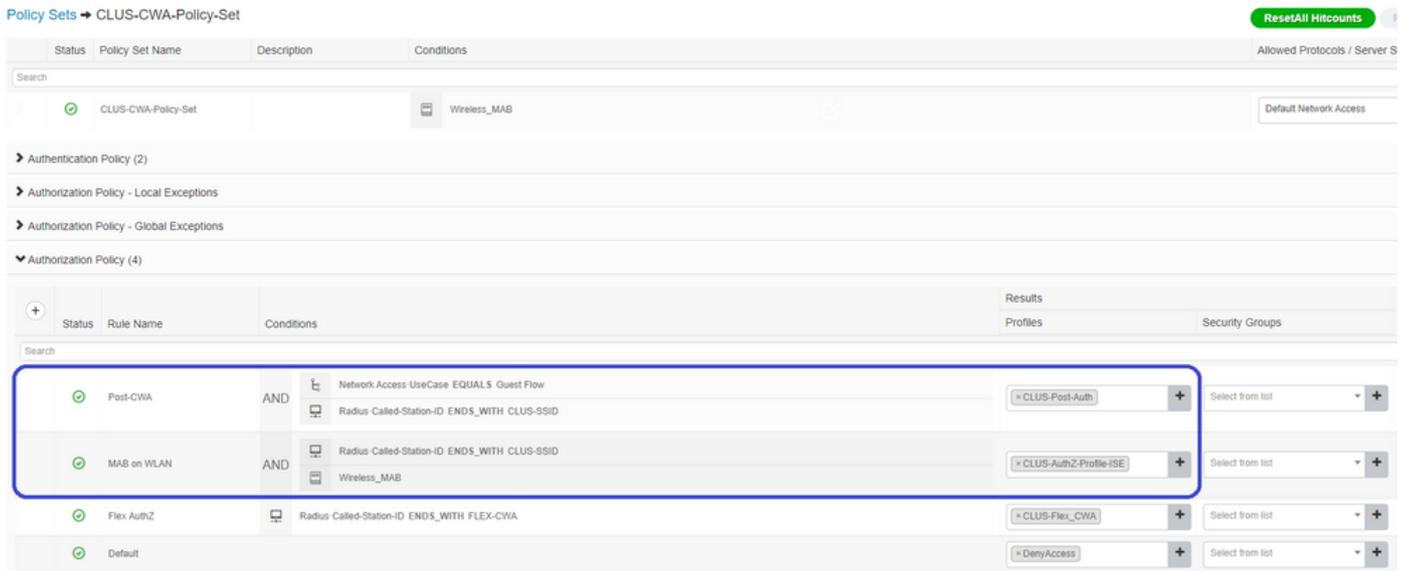
对于每次在ISE中使用MAB时的此策略集，它将通过此策略集。之后，您可以对被叫站ID制定匹配的授权策略，以便根据所使用的WLAN应用不同的结果。此流程可以定制，您可以进行许多匹配。



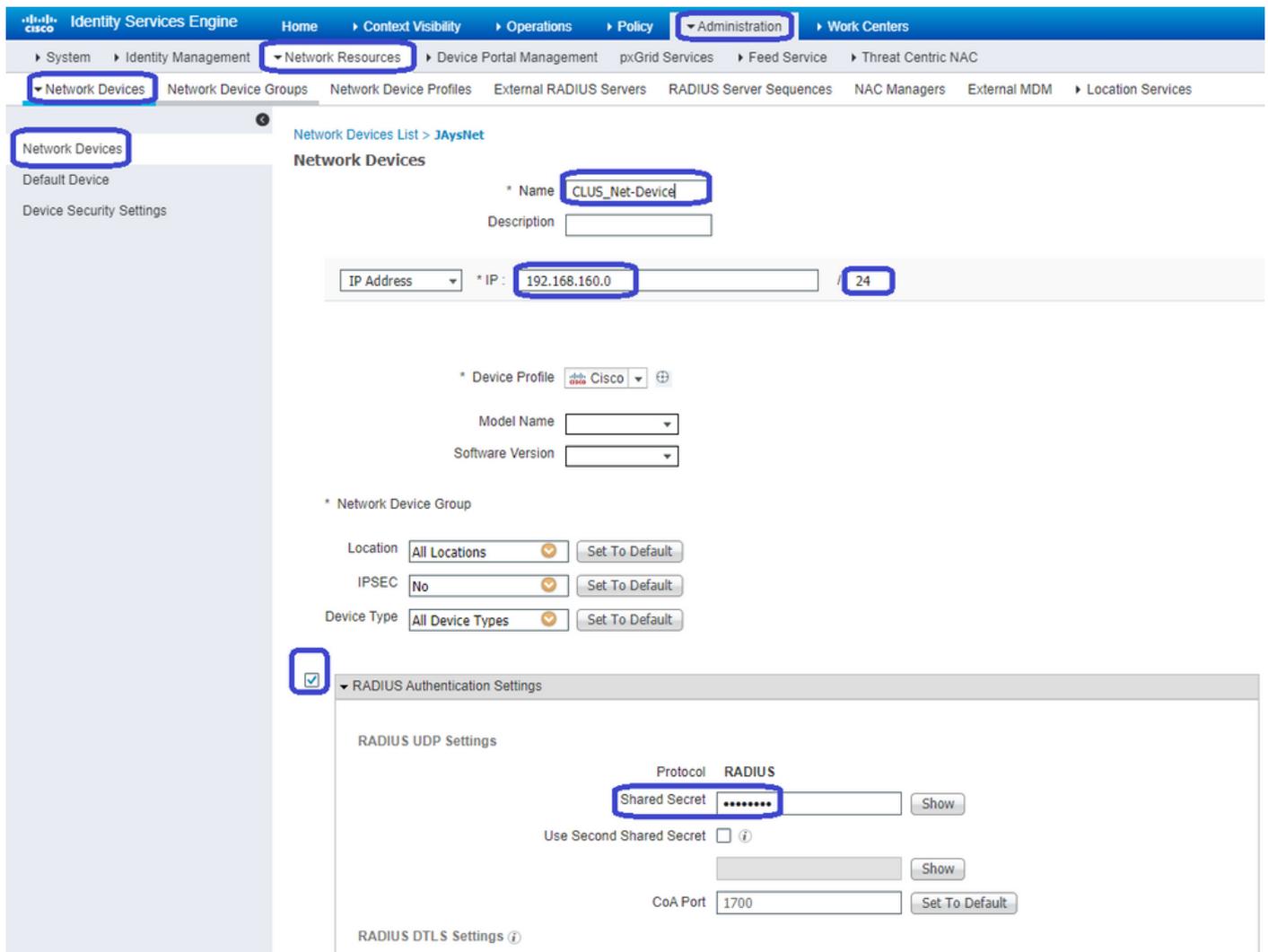
在策略集内，创建策略。身份验证策略在MAB上可以再次匹配，但您需要更改ID存储以使用“内部终端”，并需要更改选项以继续进行身份验证失败和找不到用户。



设置身份验证策略后，您需要在授权策略中创建两个规则。此策略读起来像ACL，因此顺序需要在顶部设置身份验证后规则，在底部设置身份验证前规则。后身份验证规则将匹配已通过访客流的用户。也就是说，如果他们已经登录，他们会遵守这条规则，然后停止。如果他们尚未登录，则继续从列表中按下预身份验证规则获取重定向。最好将授权策略规则与以SSID结尾的被叫站点ID进行匹配，以便仅命中配置为这样做的WLAN。



配置策略集后，您需要向ISE告知9800（外部），以便ISE信任它作为身份验证器。这可以在Admin>Network Resources>Network Device>+中完成。您需要为其命名，设置IP地址（在本例中为整个管理子网），启用RADIUS，并设置共享密钥。ISE上的共享密钥必须与9800上的共享密钥匹配，否则此过程将失败。添加配置后，按“提交”按钮保存配置。



最后，您需要将客户端将要输入的用户名和密码添加到登录页面，以验证他们应该具有网络访问权限。这在Admin>Identity Management>Identity>Users>+Add下完成，并确保在添加后点击提交。与ISE的其他所有功能一样，这是可定制的，不必是本地存储的用户，但是，这是最简单的配置。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

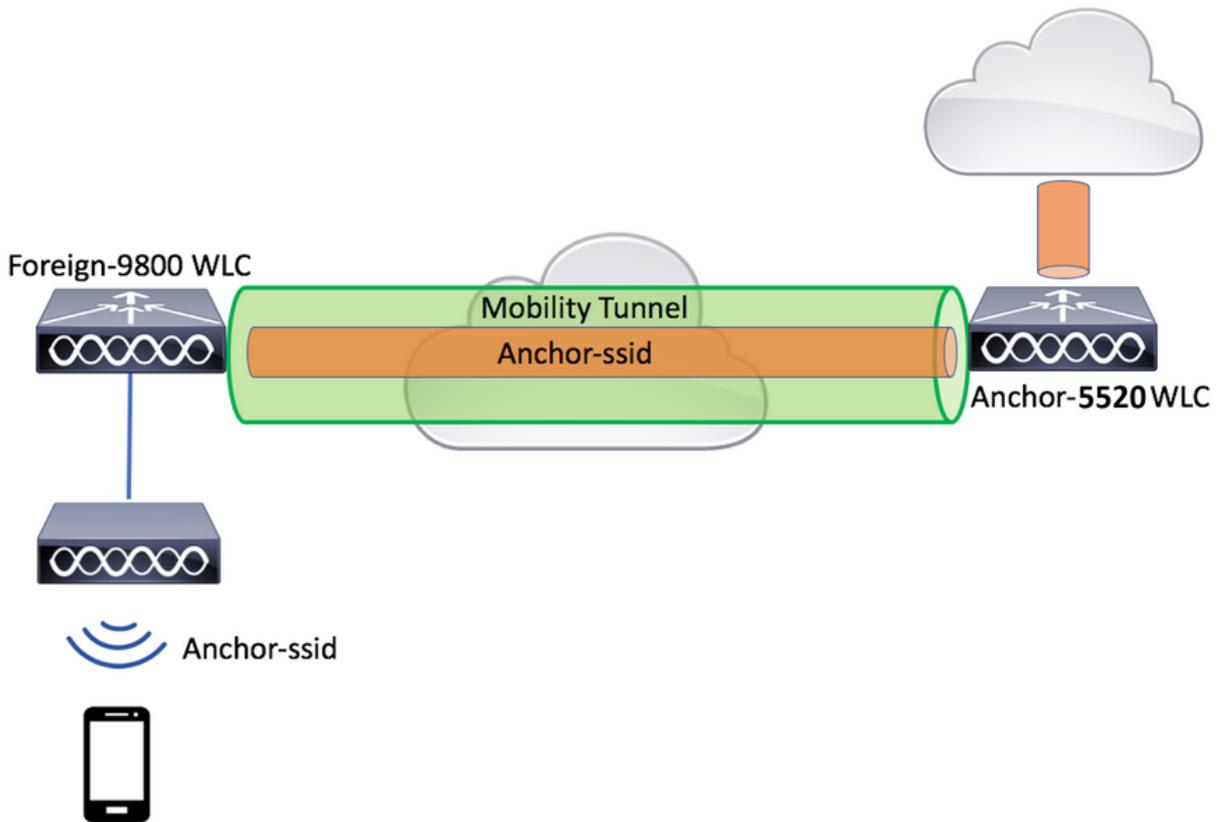
Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

配置锚定到AireOS WLC的Catalyst 9800



Catalyst 9800外部配置

按照与前面讨论的步骤操作，跳过“在锚点WLC上创建策略配置文件”部分。

锚点AireOS WLC上的AAA配置

通过转到Security>AAA>RADIUS>Authentication>New，将服务器添加到WLC中。添加服务器IP地址、共享密钥和CoA支持。

The first screenshot shows the 'RADIUS Authentication Servers' configuration page. The 'Auth Called Station ID Type' is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen'. The 'Framed MTU' is set to '1300'. The 'Network User' table is empty.

The second screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The 'Server Index (Priority)' is set to '1'. The 'Server IP Address(Ipv4/Ipv6)' is '192.168.160.99'. The 'Shared Secret Format' is 'ASCII'. The 'Shared Secret' and 'Confirm Shared Secret' fields are filled with asterisks. The 'Apply Cisco ISE Default settings' checkbox is checked. The 'Key Wrap' checkbox is unchecked. The 'Port Number' is '1812'. The 'Server Status' is 'Enabled'. The 'Support for CoA' dropdown is set to 'Enabled'. The 'Server Timeout' is '5' seconds. The 'Network User' checkbox is checked. The 'Management' checkbox is checked. The 'Management Retransmit Timeout' is '5' seconds. The 'Tunnel Proxy' checkbox is unchecked. The 'PAC Provisioning' checkbox is unchecked. The 'IPsec' checkbox is unchecked.

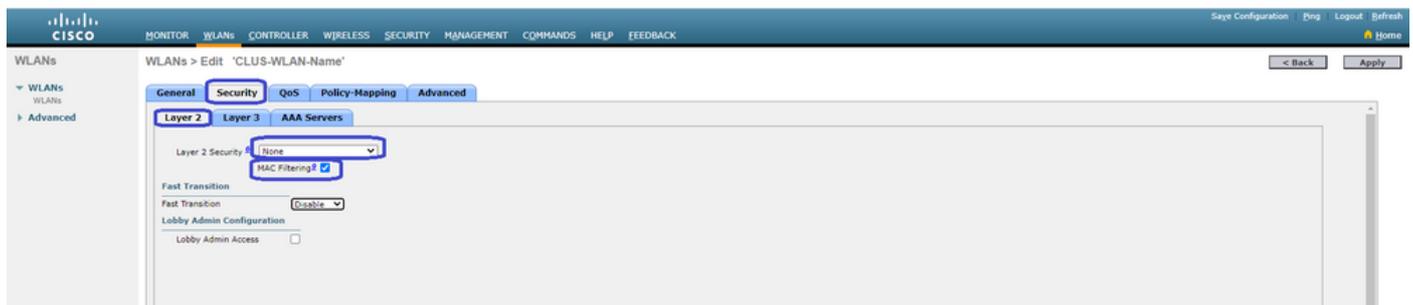
AireOS WLC上的WLAN配置

要创建WLAN，请转至WLANs>Create New>Go。

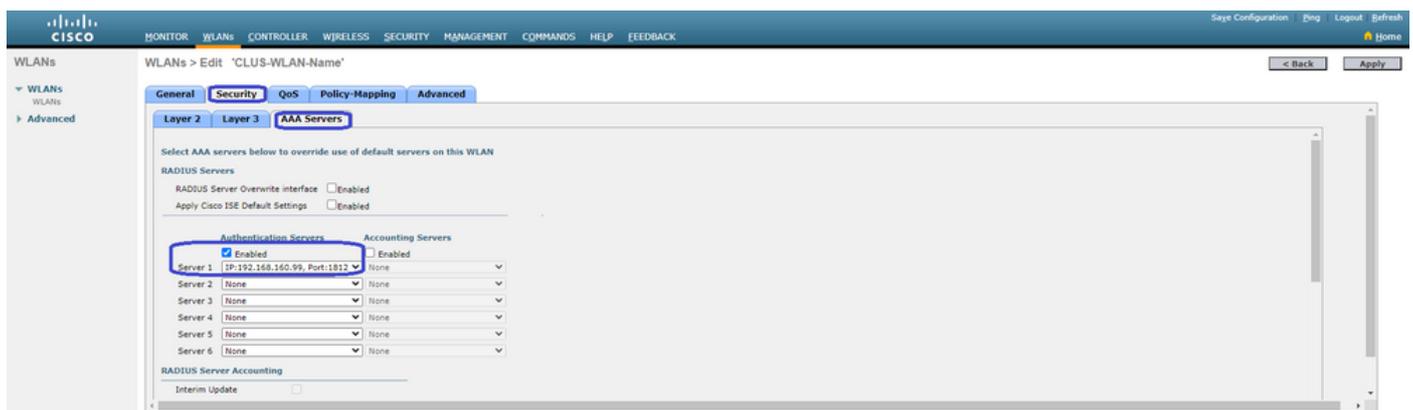
配置配置文件名称、WLAN ID和SSID，然后点击“应用”。



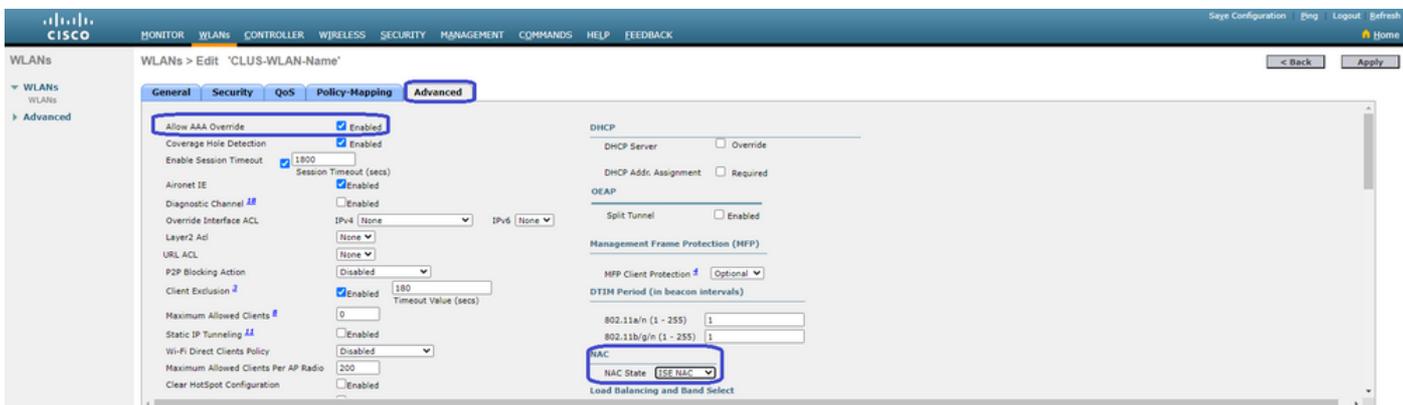
这会将您带到WLAN配置。在“常规”选项卡上，如果您不打算将ISE配置为在AVP中发送接口，您可以添加希望客户端使用的接口。然后转到Security>Layer2选项卡，匹配您在9800上使用的“Layer 2 Security”配置并启用“MAC Filtering”。



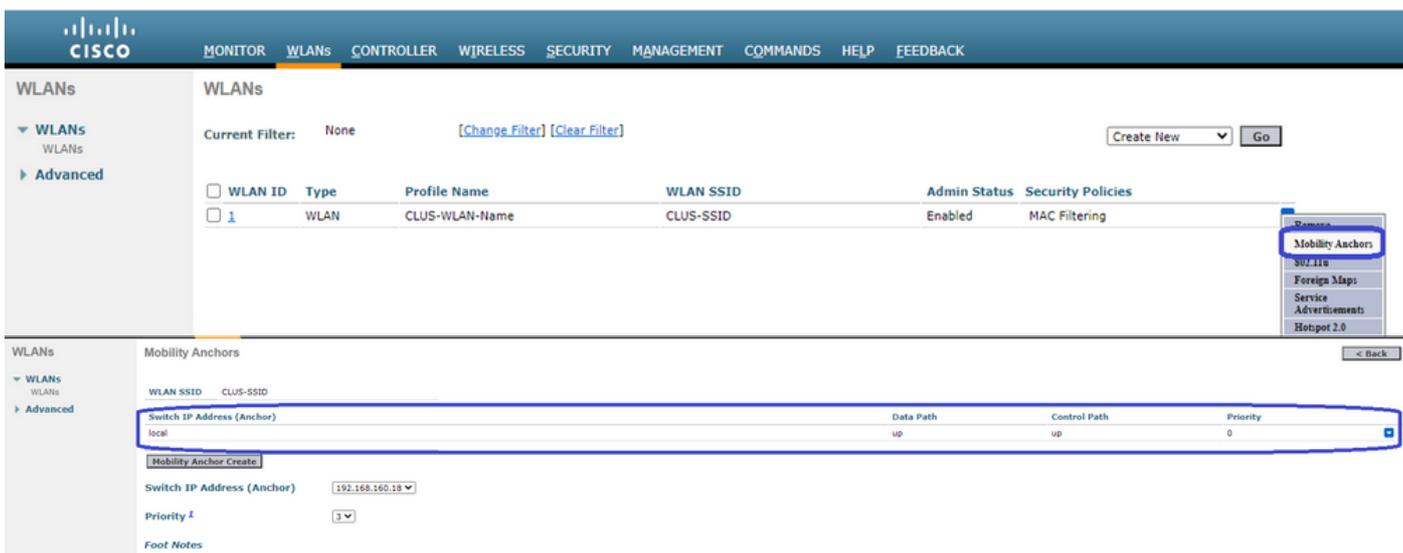
现在转到Security>AAA Servers选项卡，将ISE服务器设置为“Authentication Servers”。请勿为“记帐服务器”设置任何内容。取消选中“启用”(Enable)复选框以进行记账。



在WLAN配置中，切换到“高级”选项卡并启用“允许AAA覆盖”，并将“NAC状态”更改为“ISE NAC”



最后一件事就是把它固定在自己身上。为此，请返回WLANs页面，将鼠标悬停在WLAN>Mobility Anchors右侧的蓝色框上。将“交换机IP地址（锚点）”设置为本地，然后按“移动锚点创建”按钮。然后，它应显示优先级为0的本地锚点。



在AireOS WLC上重定向ACL

这是AireOS WLC上需要的最终配置。要创建重定向ACL，请转到**Security>Access Control Lists>Access Control Lists>New**。输入ACL名称（这必须与AVP中发送的内容匹配）并点击“应用”。



现在，单击您刚创建的ACL的名称。单击“添加新规则”按钮。与9800控制器不同，在AireOS WLC上，您为允许到达ISE的流量配置允许语句，而无需重定向。默认情况下允许DHCP和DNS。

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists**
 - Access Control Lists
 - CPU Access Control

Access Control Lists > Edit

General

Access List Name: CLUS-ACL

Deny Counters: 5

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

配置ISE

CWAISE

ISE9800ISE

Policy>Policy Elements>Authorization>Results>Authorization Profiles>+Add“access_accept”AVP — CWAACLURLVLAN ID ACLWLCACL

← → ↻ Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > test

Authorization Profile

* Name: CLUS-AuthZ-Profile-ISE

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL: CLUS-ACL Value: Self-Registered Guest Portal

CWAMABIDSSID

Policy>Policy Set+“MAB”Policy>Policy Elements>Results>Authentication>Allowed Protocols +

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Click here to do visibility setup Do not show this again.

Policy Sets

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	CLUS-CWA-Policy-Set			Default Network Access			
	Default	Default policy set		Default Network Access	0		

Reset Save

ISEMABIDWLAN

Conditions Studio

Library

mab

Wired_MAB

Wireless_MAB

Editor

Wireless_MAB

Set to 'Is not'

New AND OR

MABID"

Policy Sets Profiling Posture Client Provisioning Policy Elements

Click here to do visibility setup Do not show this again.

Policy Sets → CLUS-CWA-Policy-Set

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access	0

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
	CLUS-MAB-Condition	Wireless_MAB	Internal Endpoints		
	Default		All_User_ID_Stores	0	

Options

- If Auth fail: CONTINUE
- If User not found: CONTINUE
- If Process fail: DROP

All_User_ID_Stores

Options

- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (1)

ACLSSIDWLAN

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)						
Authorization Policy - Local Exceptions						
Authorization Policy - Global Exceptions						
Authorization Policy (4)						
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups
+	✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth		Select from list
+	✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE		Select from list
+	✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA		Select from list
+	✓	Default		DenyAccess		Select from list

ISE9800ISEAdmin>Network Resources>Network Device>+.IPRADIUSISE9800"

Identity Services Engine Administration

Network Resources > Network Device

Network Devices List > JaysNet

Network Devices

* Name: CLUS_Net-Device

Description: []

IP Address: * IP: 192.168.160.0 / 24

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: No [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: [] [Show]

Use Second Shared Secret: [] [Show]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings []

Admin>Identity Management>Identity>Users>+Add ISE

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Administration, and Work Centers. The 'Identities' section is expanded, showing Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'Users' section is selected, and the 'New Network Access User' form is displayed. The form includes fields for Name (CLUS-User), Status (Enabled), Email, Password Type (Internal Users), Login Password (*****), Re-Enter Password (*****), User Information (First Name, Last Name), Account Options (Description, Change password on next login), Account Disable Policy (Disable account if date exceeds 2020-07-17), and User Groups (Select an item). The 'Submit' button is highlighted with a red box.

当AireOS WLC是外部WLC，而Catalyst 9800是锚时，配置的差异

如果希望AireOs WLC成为外部控制器，则配置与之前相同，只有两个差异。

1. AAA记帐从不在锚点上完成，因此9800将没有记帐方法列表，并且AireOS WLC将启用记帐并指向ISE。
2. AireOS需要定位于9800，而不是自身。在策略配置文件中，9800不会选择锚点，但会选中“导出锚点”框。
3. 请注意，当AireOS WLC将客户端导出到9800时，它只发送WLAN配置文件名称(WLAN Profile Name)。因此，9800将将从AireOS发送的WLAN配置文件名称应用到WLAN配置文件名称和策略配置文件名称。也就是说，当从AireOS WLC锚定到9800 WLC时，两个WLC上的WLAN配置文件名称和9800上的策略配置文件名称必须全部匹配。

验证

要验证9800 WLC上的配置，请运行以下命令

- AAA

Show Run | section aaa|radius

- WLAN

Show wlan id <wlan id>

- 策略配置文件

Show wireless profile policy detailed <profile name>

- 策略标记

Show wireless tag policy detailed <policy tag name>

- ACL

Show IP access-list <ACL name>

- 验证移动是否与锚点一起启用

Show wireless mobility summary

要验证AireOS WLC上的配置，请运行以下命令

- AAA

Show radius summary

注意：RFC3576是CoA配置

- WLAN

Show WLAN <wlan id>

- ACL

Show acl detailed <acl name>

- 验证移动性是否与外部

Show mobility summary

故障排除

根据客户端在进程中停止的点，故障排除看起来有所不同。例如，如果WLC从ISE在MAB上未收到响应，则客户端将停滞在“Policy Manager State:关联”，不会导出到锚点。在这种情况下，您只能对外部进行故障排除，并可以收集RA跟踪和WLC和ISE之间流量的数据包捕获。另一个示例是MAB已成功通过，但客户端未收到重定向。在这种情况下，您需要确保外国用户在AVP中收到重定向并将其应用到客户端。您还需要检查锚点，以确保客户端具有正确的ACL。此故障排除范围不在此技术文档的设计范围内（查看有关通用客户端故障排除指南的参考信息）。

有关9800 WLC上CWA故障排除的更多帮助，请参阅Cisco Live!演示DGTL-TSENT-404

Catalyst 9800故障排除信息

客户端详细信息

show wireless client mac-address

您应查看“策略管理器状态”、“会话管理器>身份验证方法”、“移动角色”。

您还可以在GUI中的Monitoring>Clients下找到此信息

嵌入式数据包捕获

命令从CLI启动 *#monitor capture <capture name>* ,然后在此之后显示选项。

在GUI中，转到Troubleshoot>Packet Capture>+Add

RadioActive跟踪

从CLI

debug wireless mac/ip

使用命令的no形式将其停止。这将记录到名为“ra_trace”的bootflash中的文件，然后记录客户端的MAC或IP地址以及日期和时间。

在GUI中，转到Troubleshoot>Radio Trace>+Add。添加客户端的mac或ip地址，点击apply，然后点击start。在您完成该过程几次后，停止跟踪，生成日志并将其下载到您的设备。

AireOS故障排除信息

客户端详细信息

在CLI中显示客户端详细信息

从GUI Monitor>Clients

从CLI调试

Debug client

Debug mobility handoff

Debug mobility config

参考

[使用9800控制器构建移动隧道](#)

[9800上的无线调试和日志收集](#)