使用外部身份验证配置本地Web身份验证

目录

简介

本文档介绍如何在9800无线局域网控制器(WLC)上配置本地网络身份验证和本地身份验证。

先决条件

Cisco建议您了解9800 WLC配置模型。

要求

Cisco 建议您了解以下主题：

- Cisco WLC 9800系列。
- 全面的Web身份验证知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-CL WLC Cisco IOS® XE版本17.12.5
- 思科接入点C9117AXI。

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

本地Web身份验证(LWA)是可在WLC上配置的无线局域网(WLAN)身份验证方法。当用户从可用网络列表中选择WLAN时，会将其重定向到Web门户。在此门户中，根据配置的不同，可能会提示用户输入用户名和密码、接受可接受使用策略(AUP)或结合使用这两种操作以最终完成其连接。

有关登录过程中出现的四种Web身份验证页的信息，请参阅配置本地Web身份验证指南，并查看Web身份验证类型的可用选项。您还可以参考Types of Authentication部分下的Configure Local Web Authentication with External Authentication指南。

参数映射

参数映射是WLC上启用Web身份验证的基本配置元素。它包含一组设置，用于管理Web身份验证过程的各个方面，包括身份验证类型、重定向URL、附加参数、超时和自定义Web页。要激活和管理特定SSID的基于Web的身份验证，此映射必须链接到WLAN配置文件。

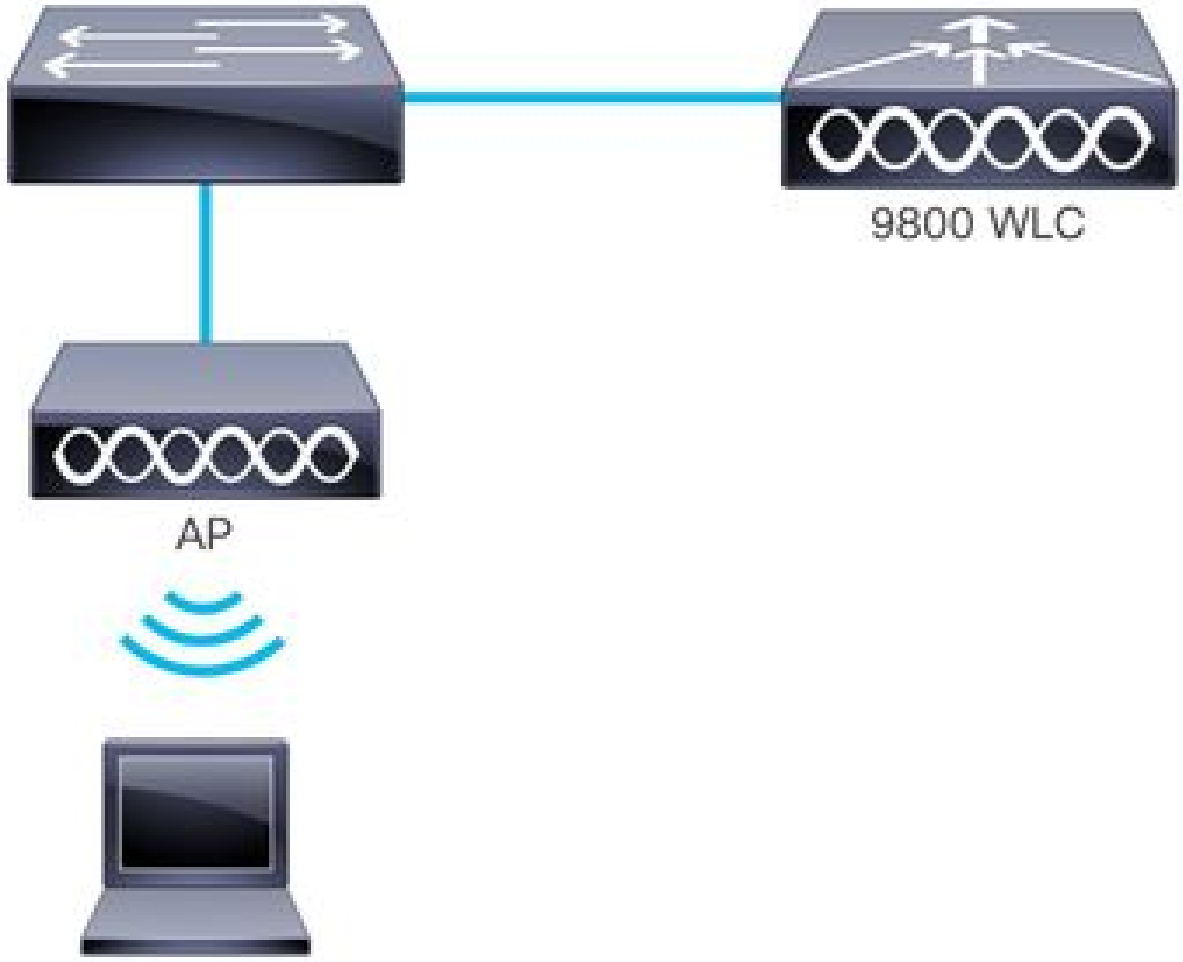
无线LAN控制器随附默认全局参数映射，但管理员可以选择创建自定义参数映射，以便根据特定需求自定义Web身份验证行为。

用于身份验证的数据库

如果参数映射配置为使用用户名和密码，则必须定义身份验证凭证，这些凭证存储在WLC本地。通过GUI创建访客用户帐户时，可以设置每个访客帐户允许的最大同时登录数。有效值范围为0至64，其中0表示该访客用户允许无限制的同时登录。

LWA主要用于小型部署。它支持与其他身份验证方法的集成，您可以查看客户端支持的身份验证组合以获取详细信息。

该图像表示LWA的通用拓扑：



具有本地身份验证的LWA的通用拓扑

LWA网络拓扑中的设备：

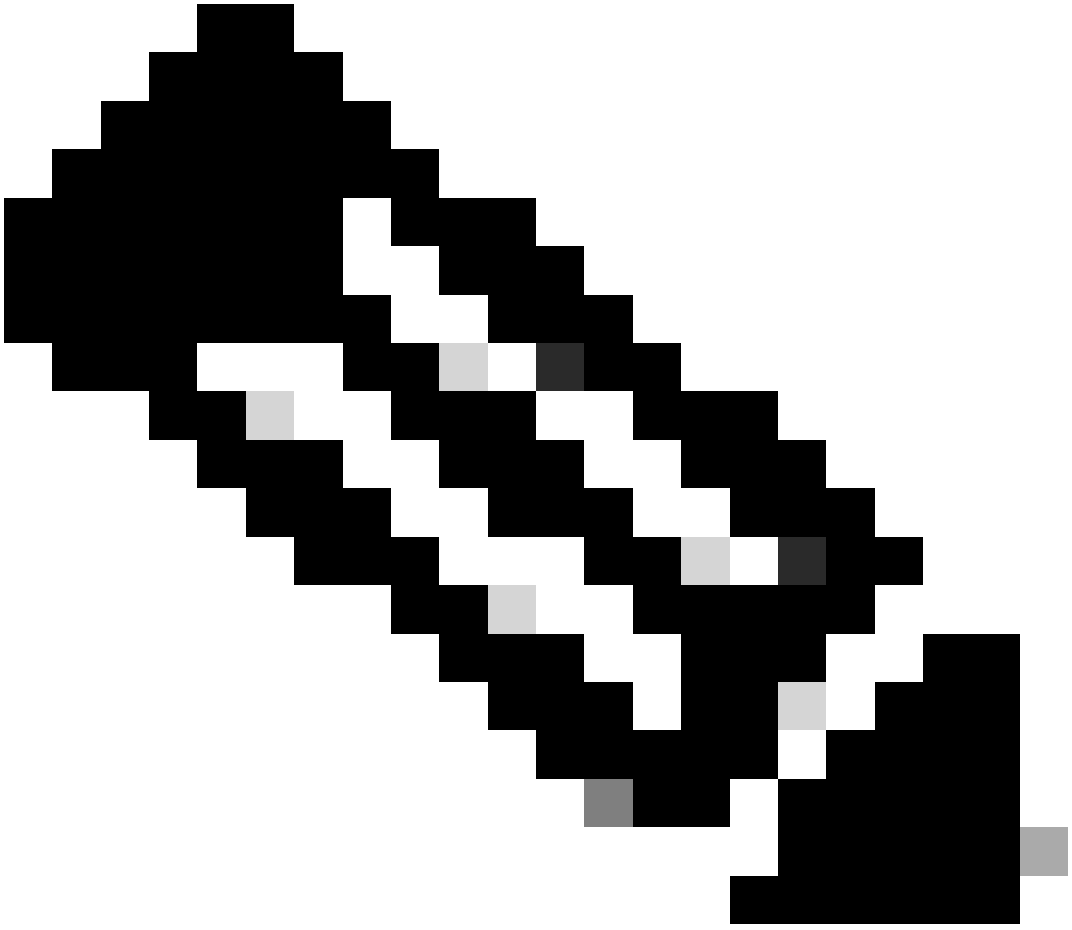
- 客户端/请求方：向WLAN发起连接请求，稍后向DHCP和DNS服务器发起连接请求，并响应来自WLC的通信。
- 接入点：连接到交换机，它会广播访客WLAN并为访客设备提供无线连接。在访客用户完成身份验证之前，它通过输入有效凭证、接受AUP或两者组合来允许DHCP和DNS流量。
- WLC/身份验证器：管理AP和客户端设备。WLC托管重定向URL并实施访问控制列表(ACL)，在配置参数映射时管理流量以及默认创建的流量。它拦截来自访客用户的HTTP请求，并将它们重定向到Web门户（登录页面），用户必须在该门户中进行身份验证。WLC捕获用户凭证，对访客进行身份验证，并检查本地数据库以验证凭证有效性。
- 身份验证服务器：在此场景中，WLC用作身份验证服务器。它会验证访客用户凭证，并相应地授予或拒绝网络访问。

配置

在CLI上使用本地身份验证进行本地Web身份验证

本地身份验证的方法列表

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



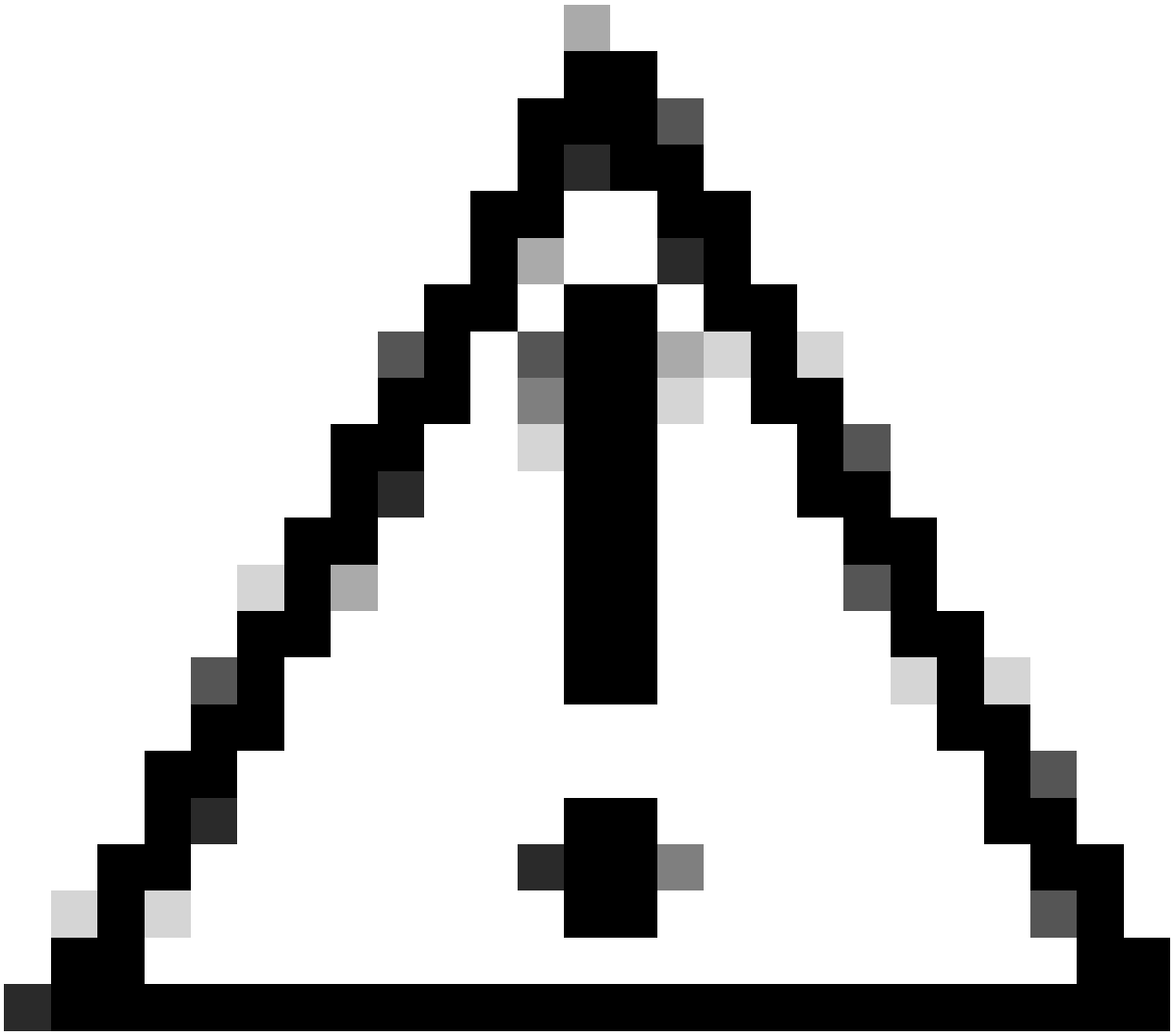
注意：要使Local Login Method List正常工作，请确保WLC上存在配置aaa authorization network default local。当WLC授权用户进入网络时，这是必要的。

参数映射

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



警告：虚拟IP必须是RFC 5737中建议的不可路由地址。默认情况下，IP 192.0.2.1已设置。有关虚拟IP地址的详细信息，请参阅Cisco Catalyst 9800系列配置最佳实践。在AireOs上，大多数时候使用的IP是1.1.1.1。由于它已成为公共IP，因此不再建议使用。

创建多个参数映射的功能可实现定制流程：自定义网页和每个WLAN的特定演示参数。全局参数映射确定信任点，从而确定WLC在重定向门户上向客户端提供的证书。此外，它还控制拦截的客户端流量的类型，例如重定向门户的HTTP/HTTPS、虚拟IP地址的域或主机名解析。这种分离允许全局映射处理总体设置，例如证书表示和流量拦截，而用户定义的参数映射则提供每个WLAN的精细体验。

WLAN安全参数

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
```

```
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

创建策略配置文件

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

创建策略标记

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

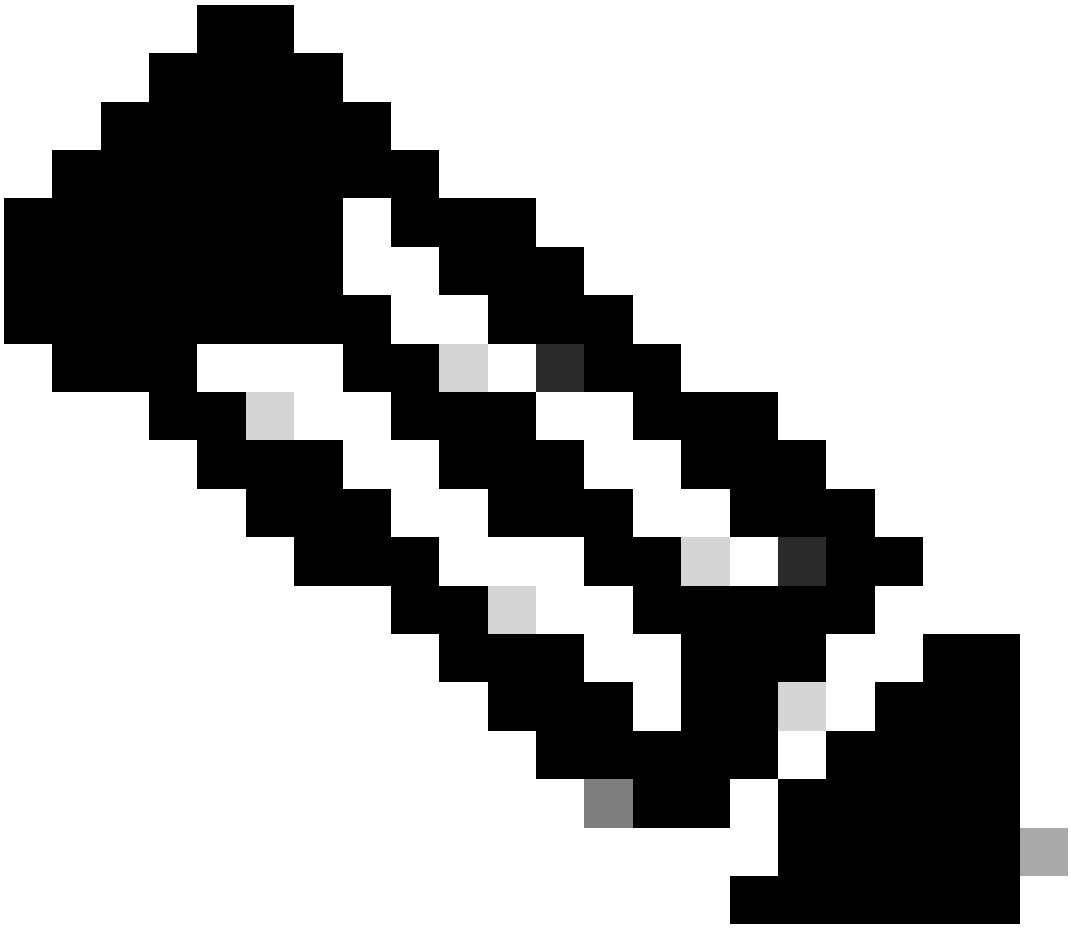
```
9800WLC(config-policy-tag)# end
```

为AP分配策略标记

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap


       >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

创建访客用户名

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description


        guest-user lifetime year 0 month 11 day 30 hour 23


9800WLC(config-user-name)#end
```

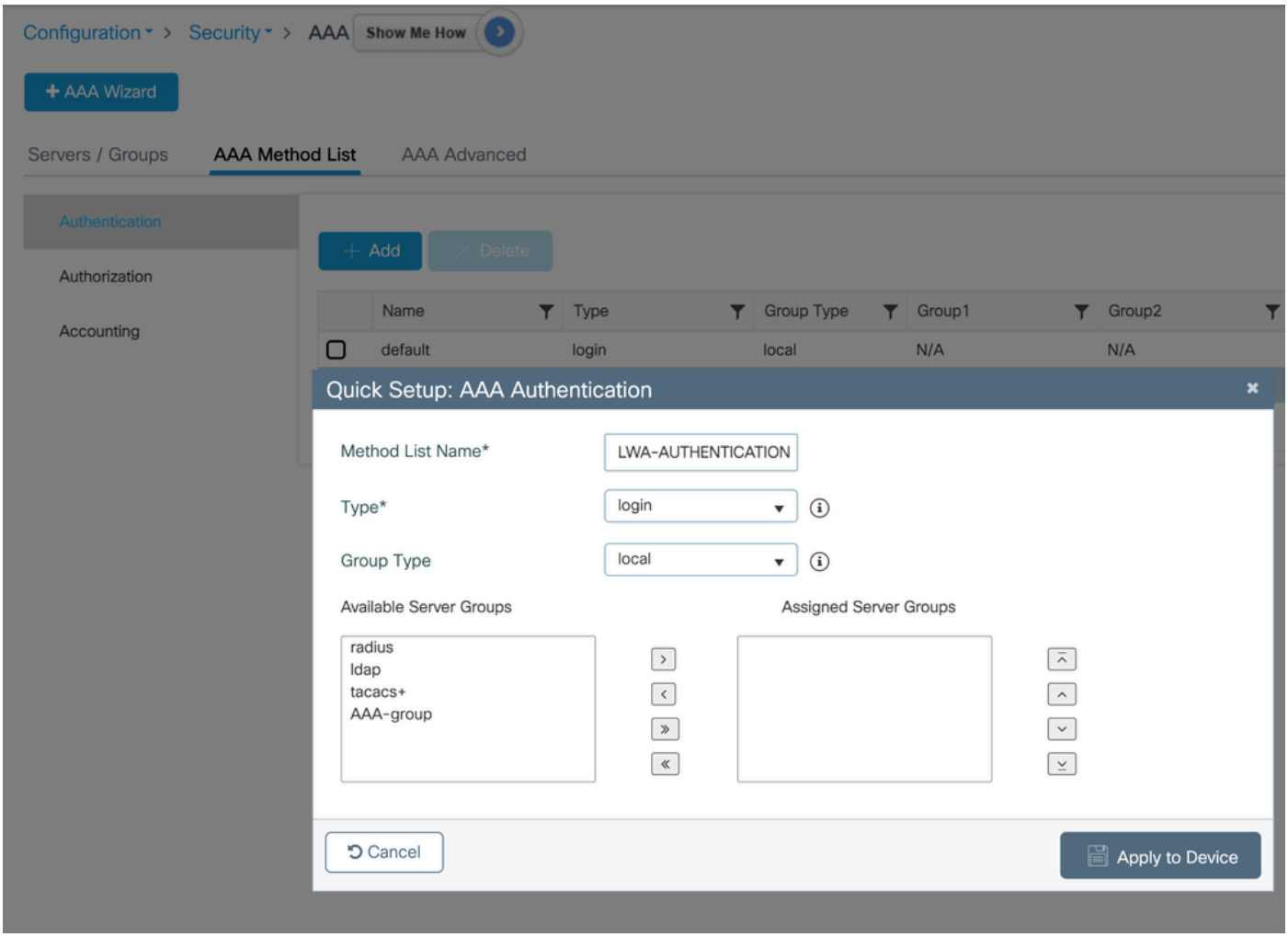


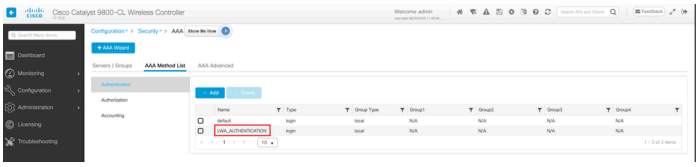
注意：在为访客用户设置生存期时，如果年份设置为1，则不能指定后续参数，即月、日、小时和分钟，因为最大生存期为1年。

通过WebUI使用本地身份验证的本地Web身份验证

本地身份验证的方法列表

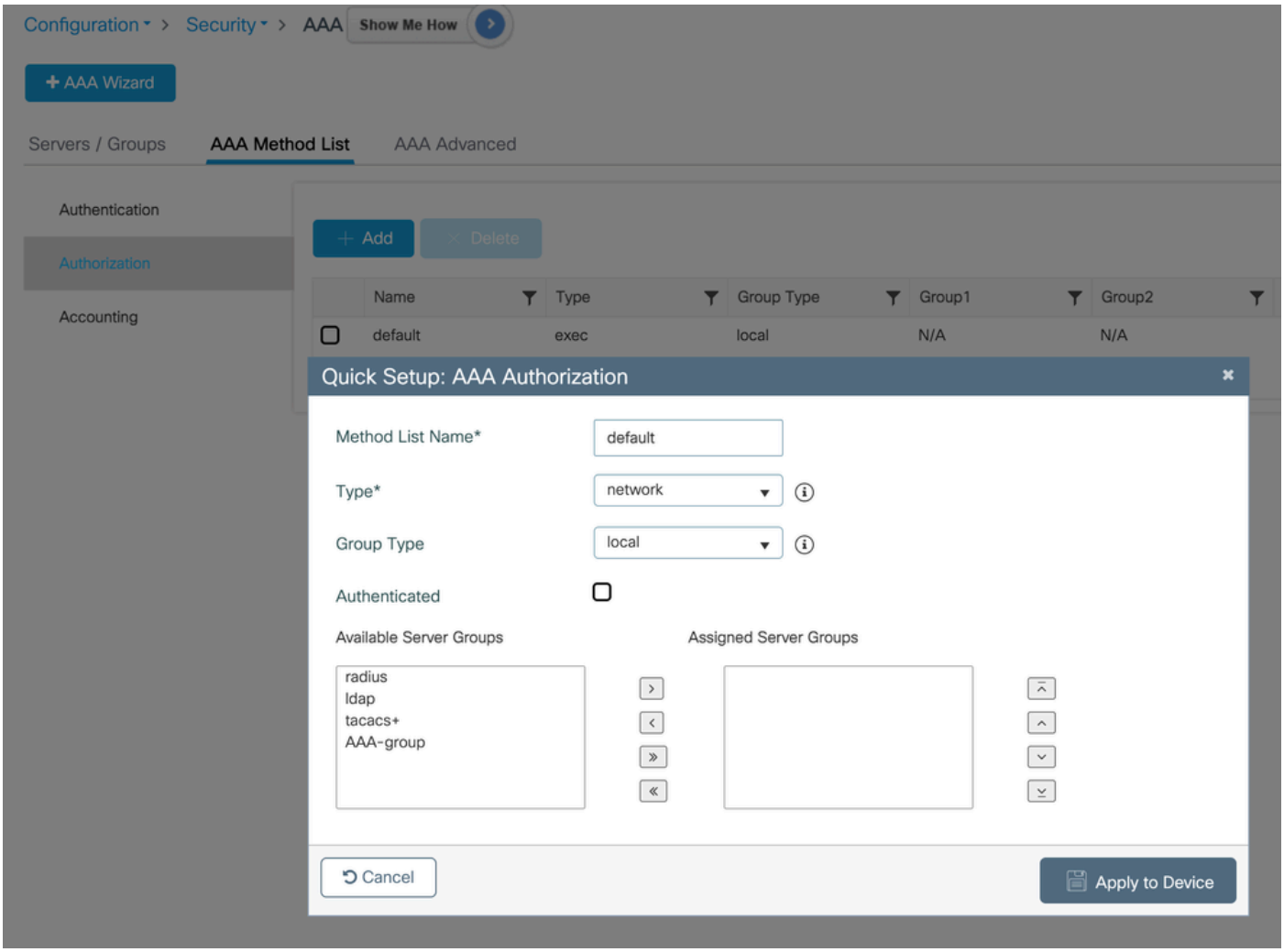
导航到Configuration > Security > AAA > AAA Method List > Authentication > Add以创建稍后用于WLAN配置的方法列表。



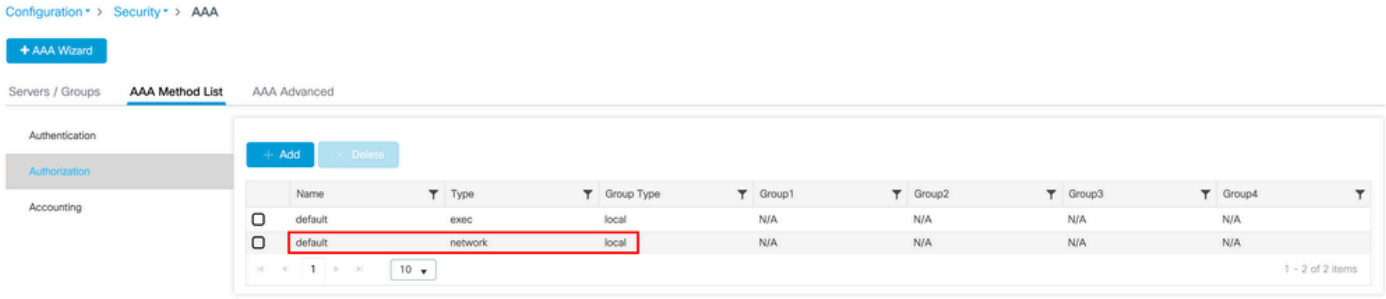
单击Apply to Device后，确认创建AAA方法列表： 

确保存在本地授权方法列表，这是为工作而创建的本地登录方法列表的要求。

Configuration > Security > AAA > AAA Method List > Authorization > Add

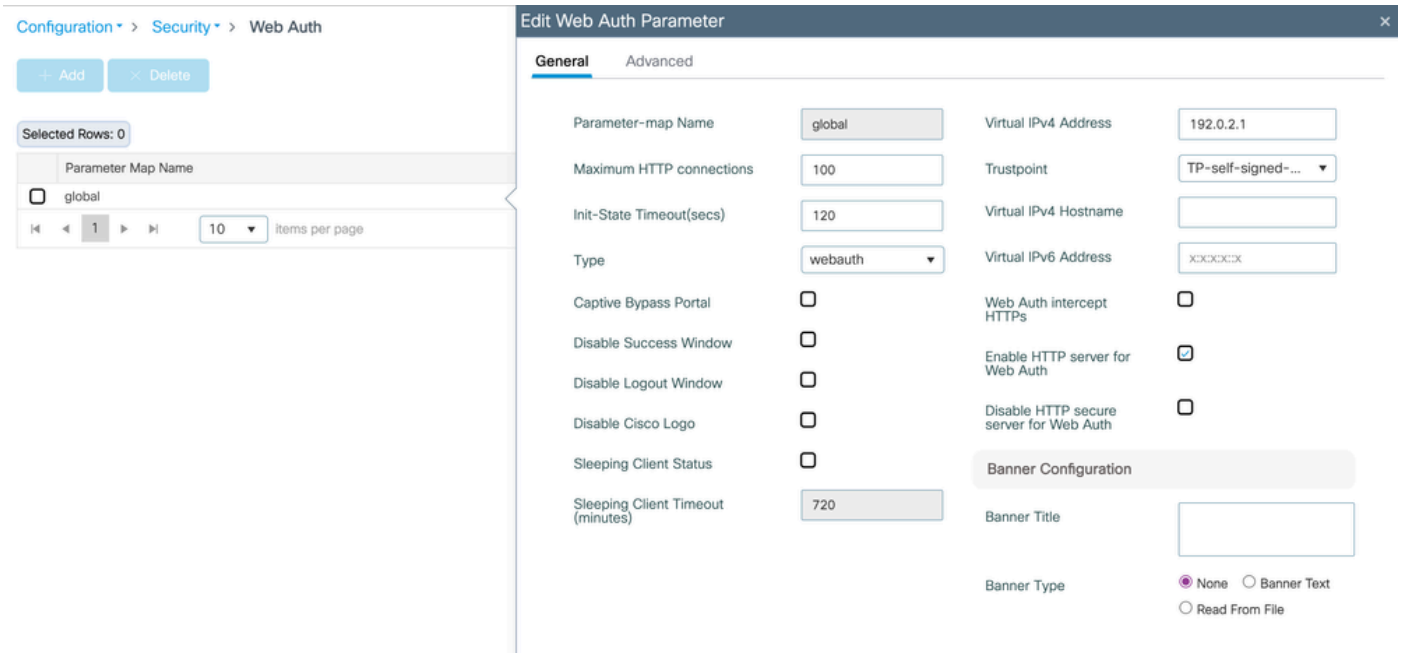


单击Apply to Device后，确认创建AAA方法列表：

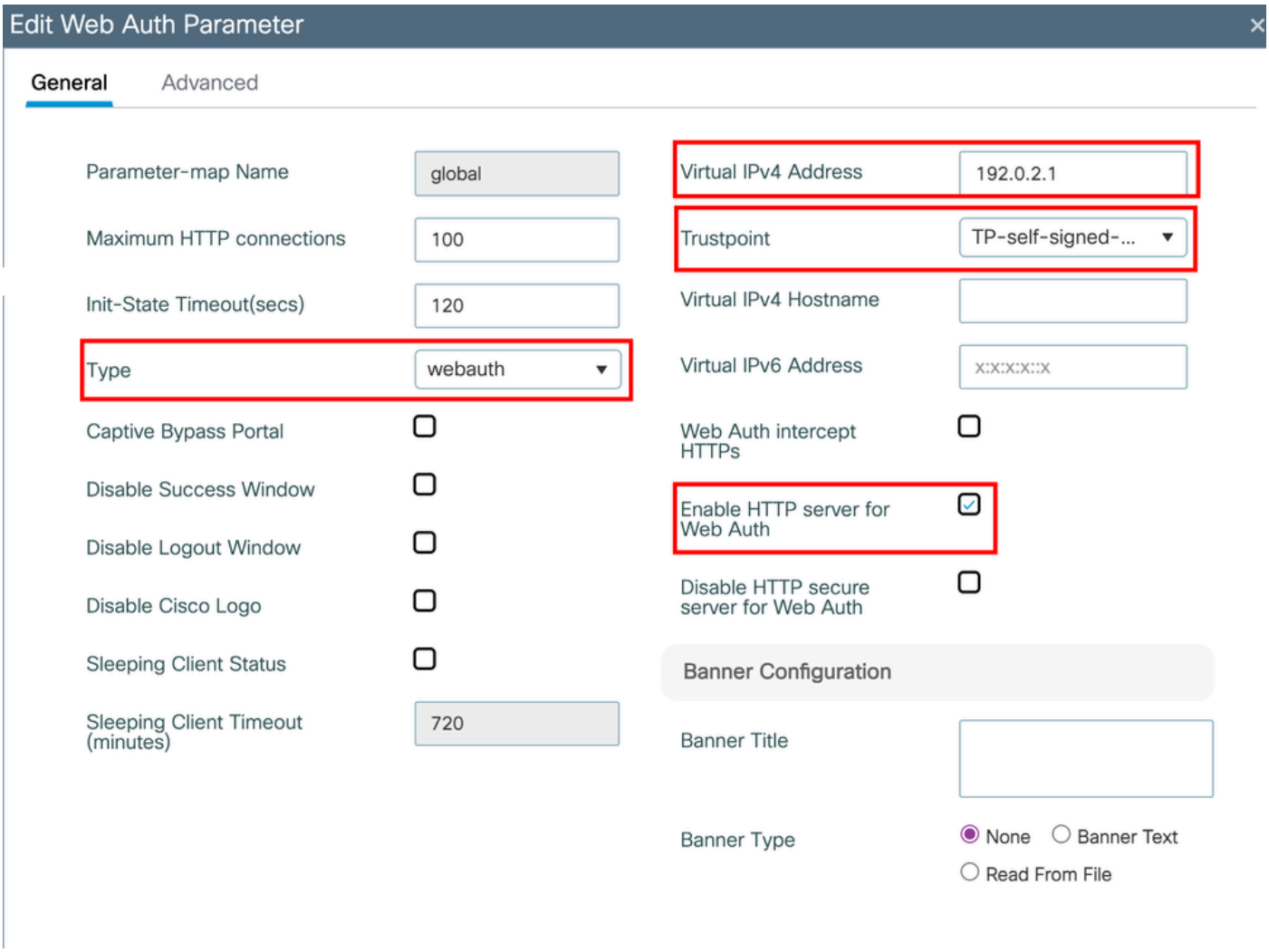


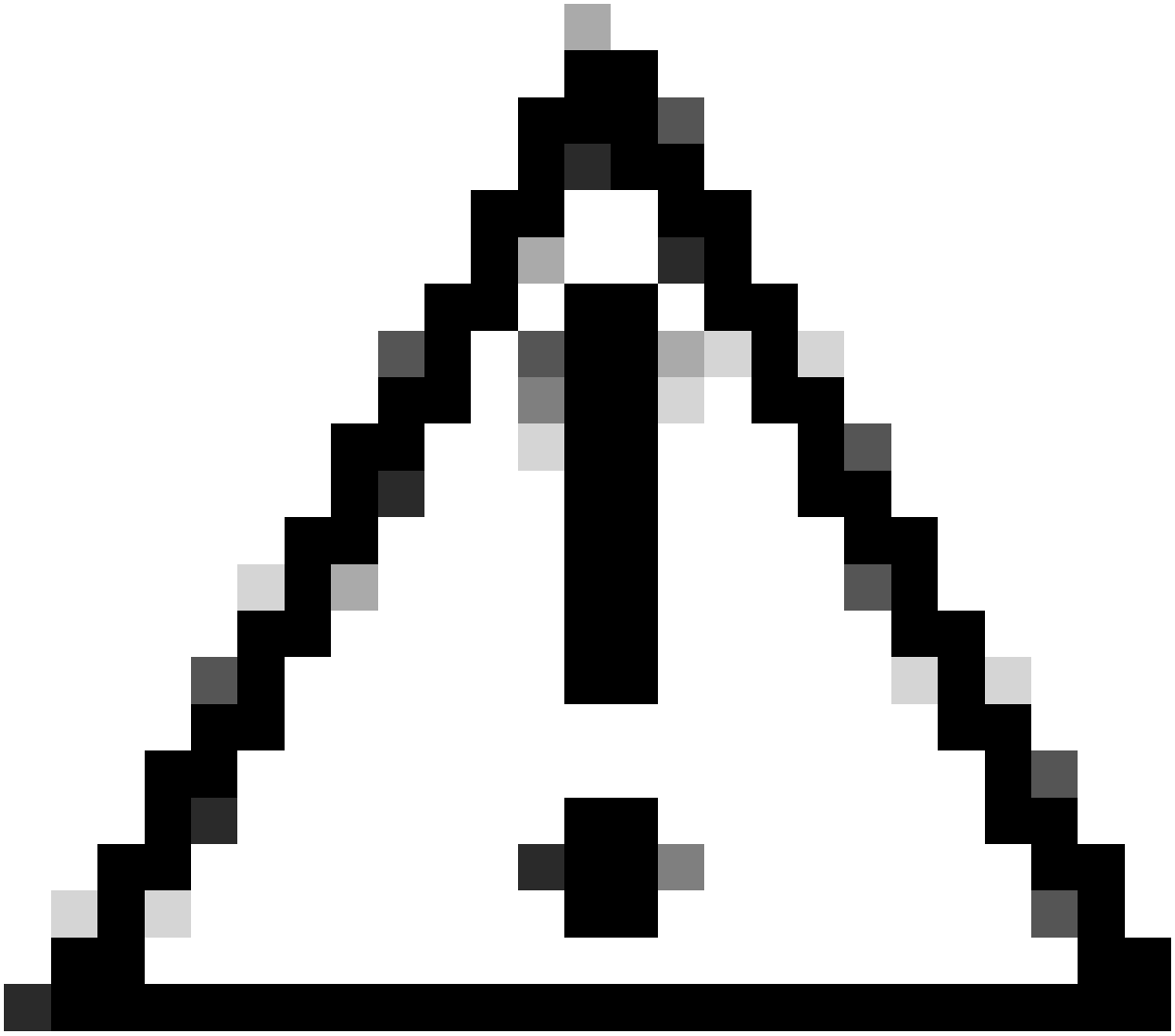
参数映射

在Configuration > Security > Web Auth中编辑全局参数映射



选择要使用的Web身份验证类型、虚拟IP和WLC在Web门户上显示的信任点。在这种情况下，选择自签名证书，并且可能会导致“您的连接不是私有网络：:ERR_CERT_AUTHORITY_INVALID”类型的免责声明，因为这是本地重要证书(LSC)，并且不是由互联网上可识别的CA签名。要修改此内容，请使用第三方签名证书。有关详细信息，请参阅在Catalyst 9800 WLC上生成和下载CSR证书，或者有一个视频选项说明在Cisco 9800 WLC上为WebAuth和WebAdmin上传和Truspoint创建续订证书 |安全无线局域网控制器设置。

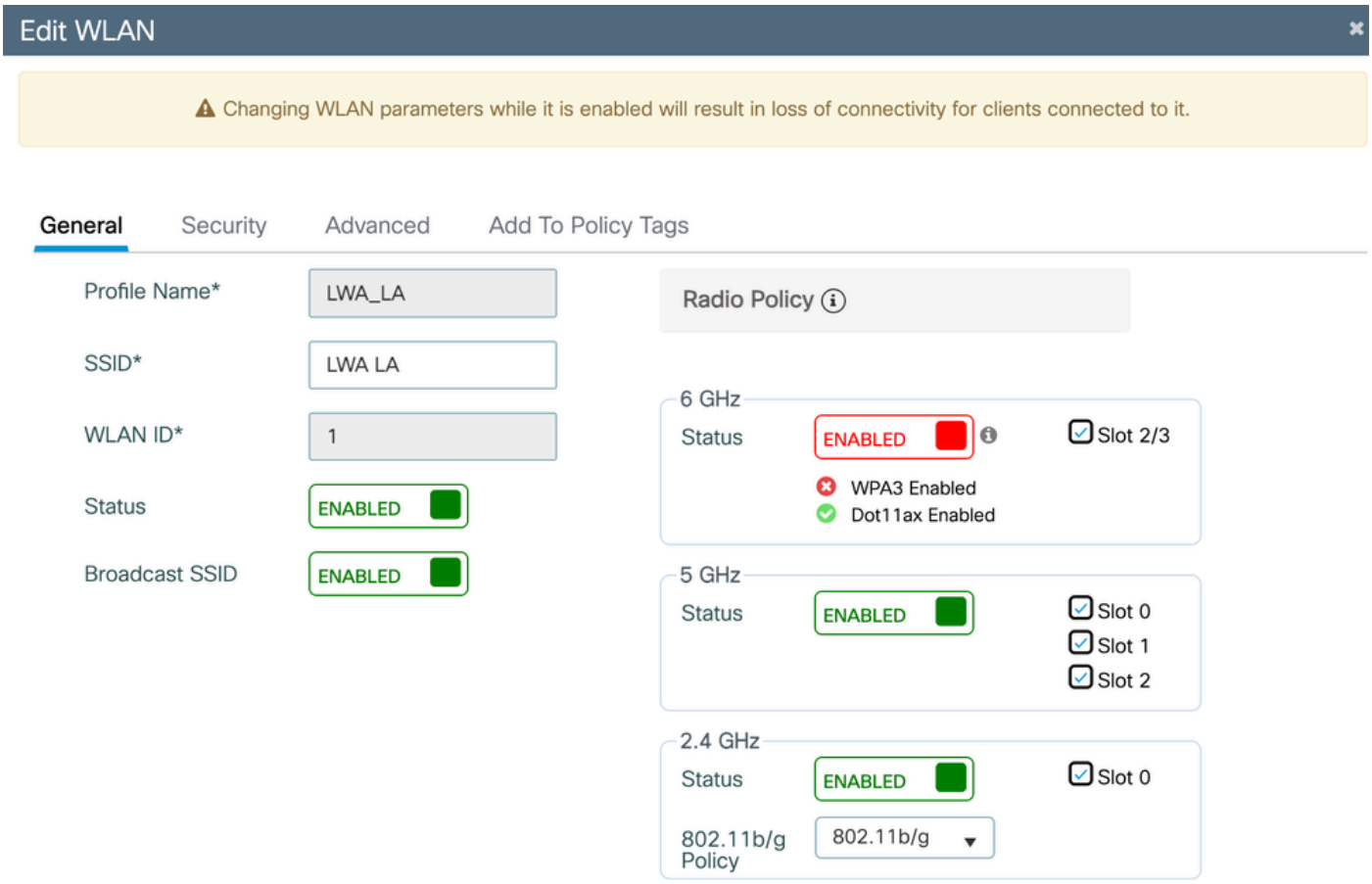

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
192.0.2.1
Trustpoint
TP-self-signed-...
Virtual IPv4 Hostname
Virtual IPv6 Address
x:x:x:x::x
Web Auth intercept HTTPs
Enable HTTP server for Web Auth
Disable HTTP secure server for Web Auth
Banner Configuration
Banner Title
Banner Type
None
Banner Text
Read From File



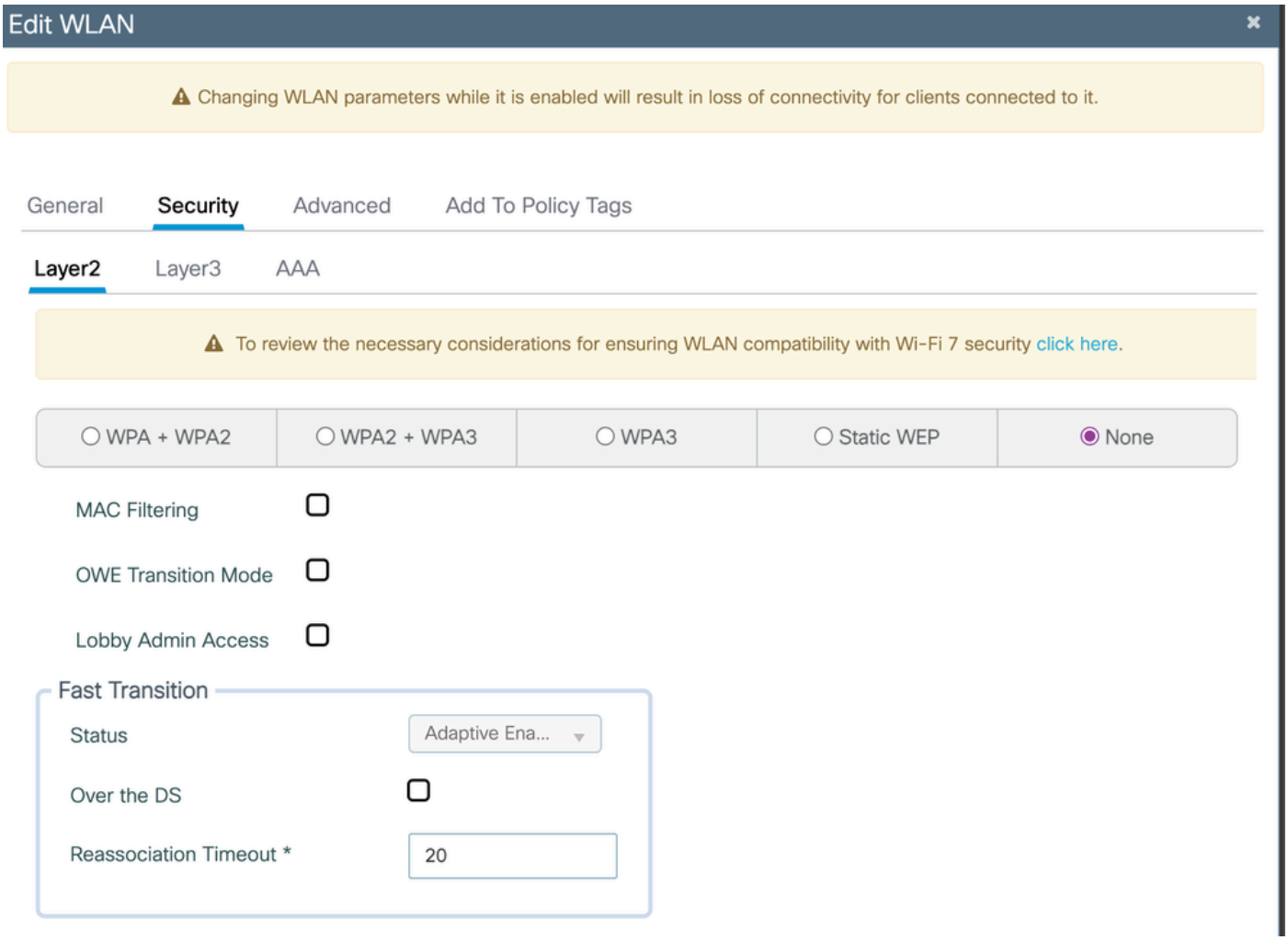
警告：如果在9800上全局禁用了HTTP，请确保选中Enable HTTP server for Web Auth，因为思科将这些进程的依赖关系分隔开。客户端或Supplicant客户端将启动HTTP连接进程，并且控制器会拦截该会话以显示Web门户。因此，除非绝对需要，否则不建议启用Web Auth Intercept HTTPS，因为此设置对大多数部署来说是不必要的，并且可能会增加控制器CPU利用率，从而影响性能。

WLAN安全参数

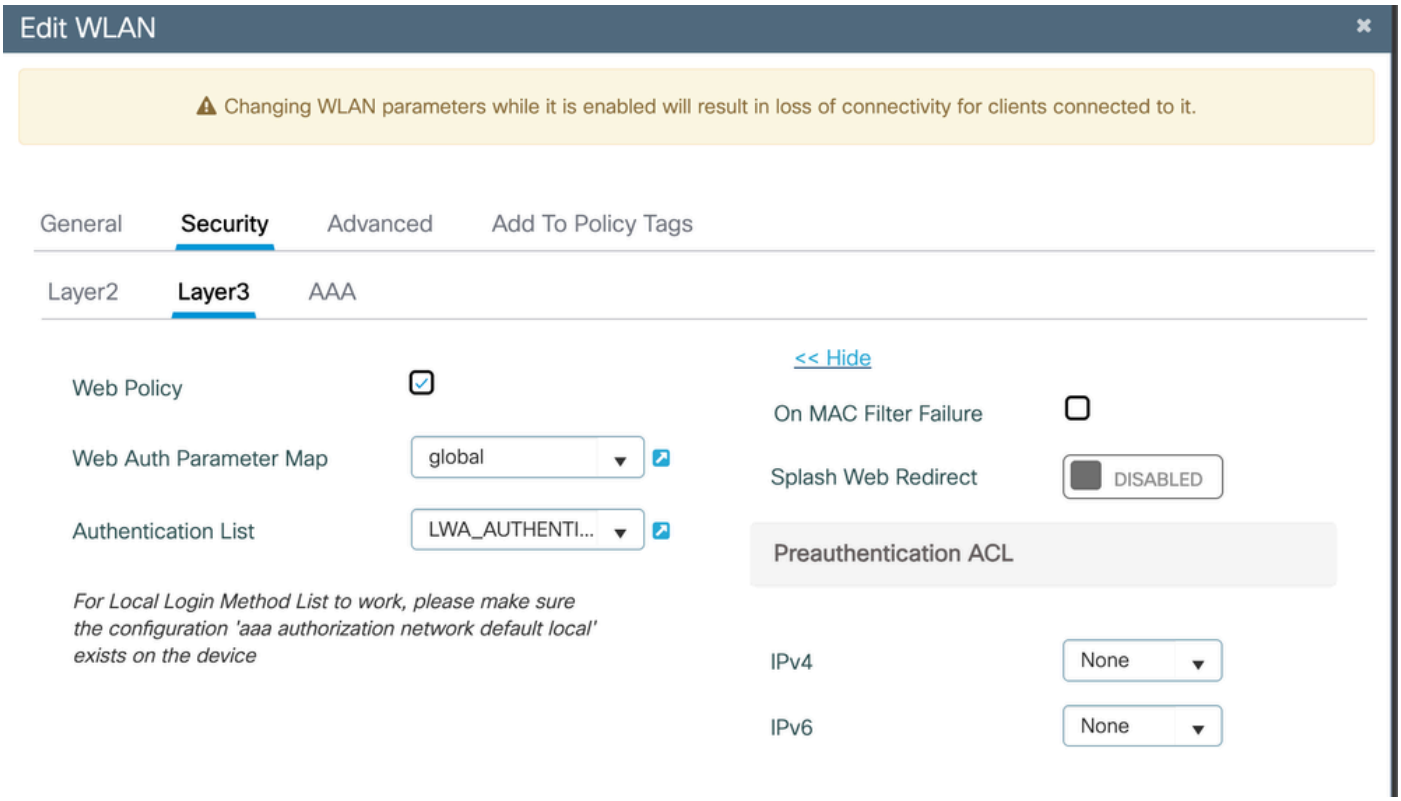
导航到Configuration > Tags & Profiles > WLANs，单击Add。



在Security选项卡上，对于Layer2，选择None。

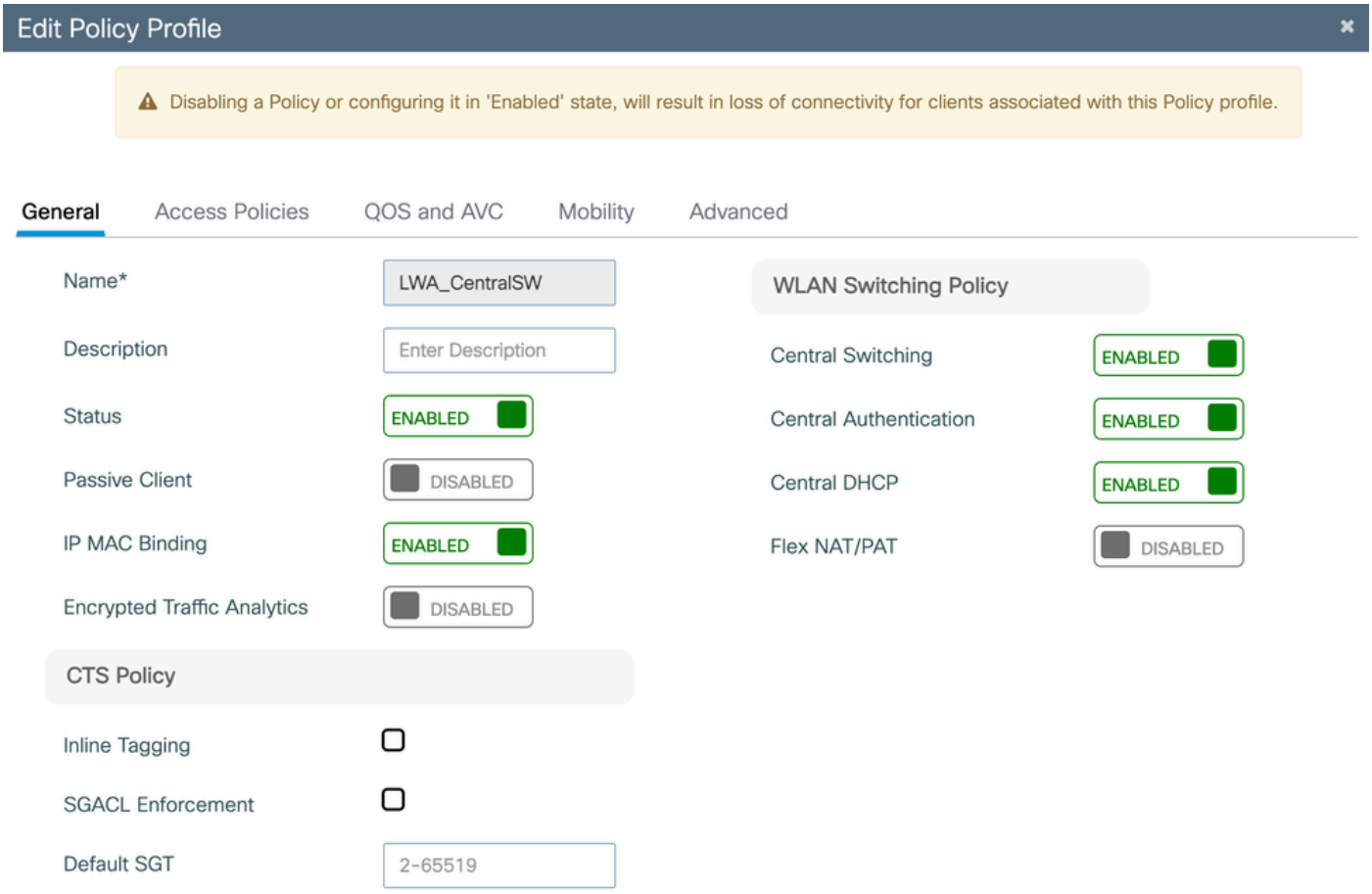


在Security选项卡上，对于Layer3，选中Web Policy框，从下拉菜单和Authentication List中选择以前配置的参数映射。

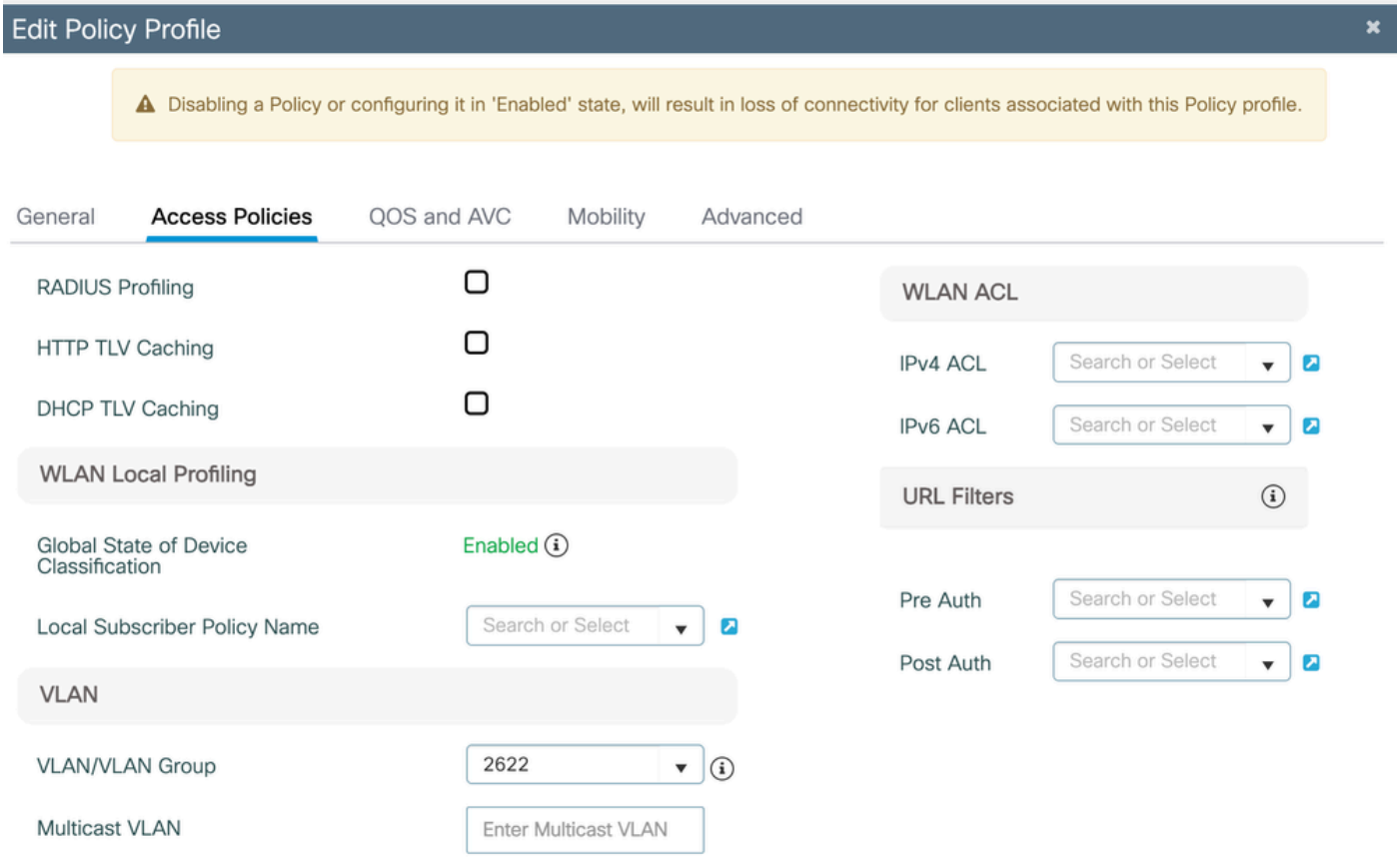


创建策略配置文件

要创建要链接到WLAN配置文件的策略配置文件，请导航到配置>标记和配置文件>策略。

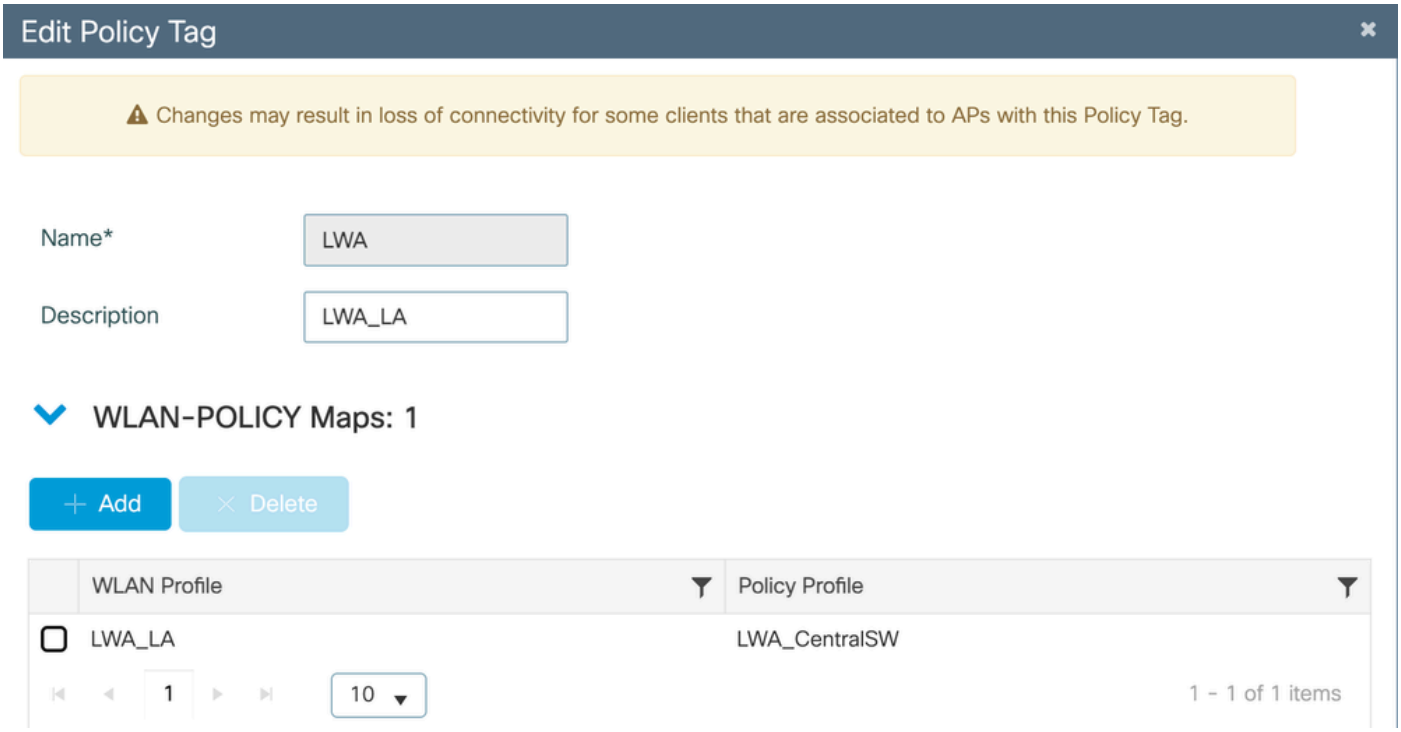


在Access Policies选项卡上，选择Clients/Supplicant客户端从中请求IP的VLAN。



创建策略标记

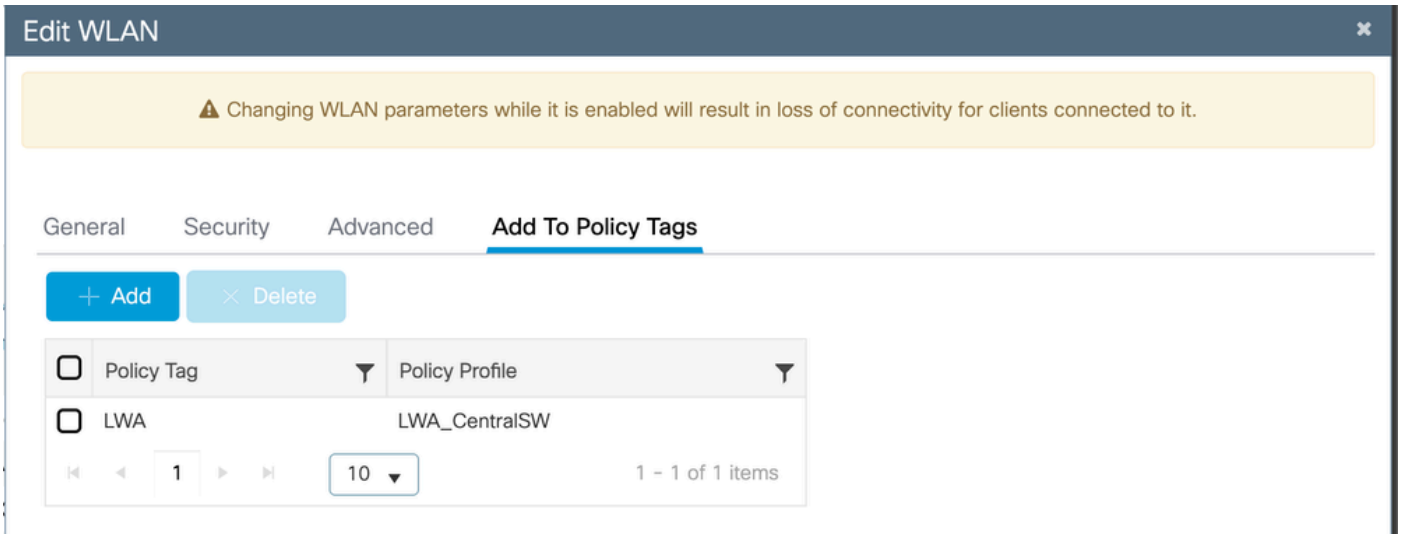
在本配置指南中，我们创建了名为LWA的自定义策略标记。



关联WLAN和策略配置文件

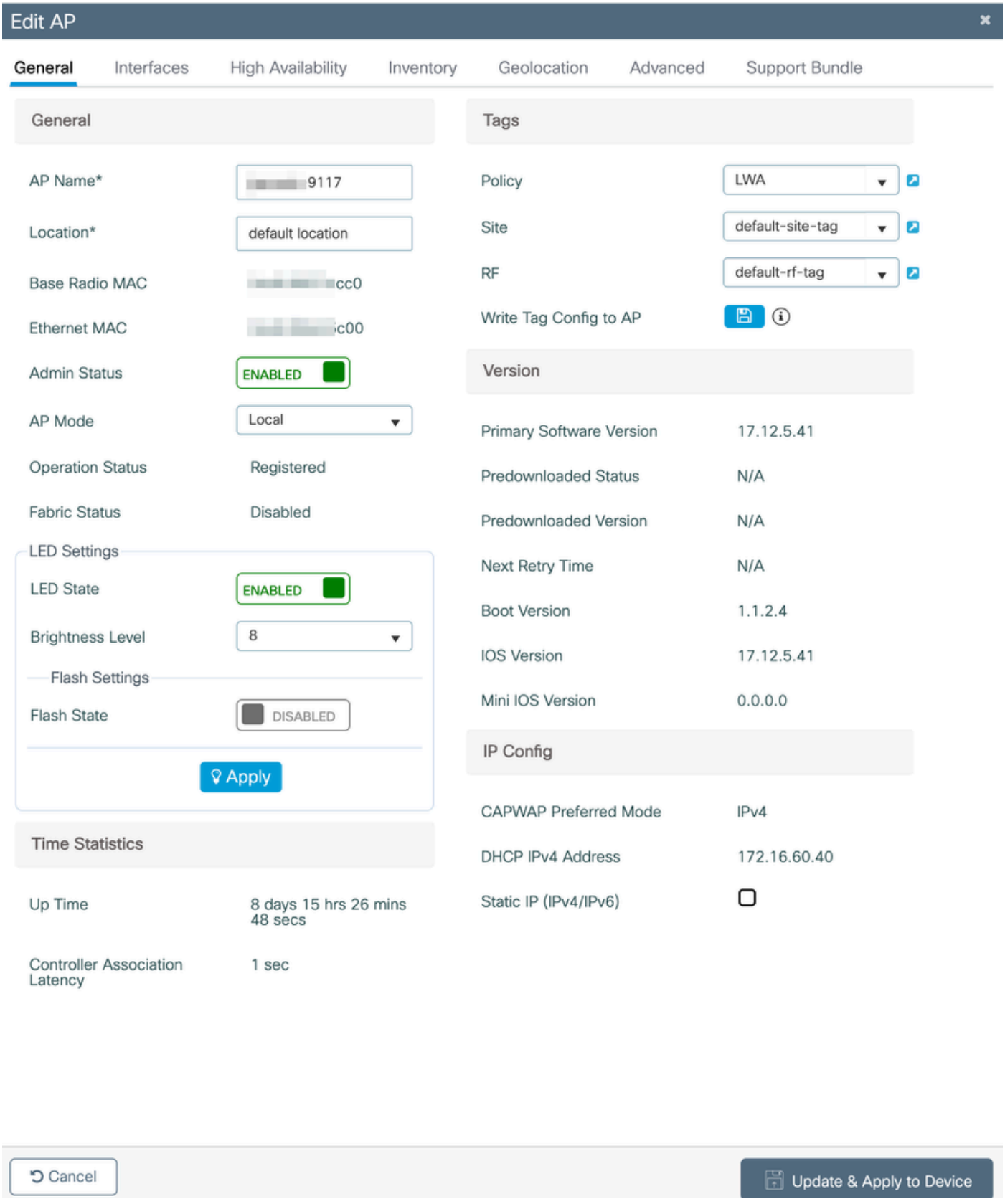
要将Policy Profile和WLAN中的交换策略链接，请导航到Configuration > Tags & Profiles >

WLANs，选择WLAN Profile，然后点击Add to Policy Tags。



为AP分配策略标记

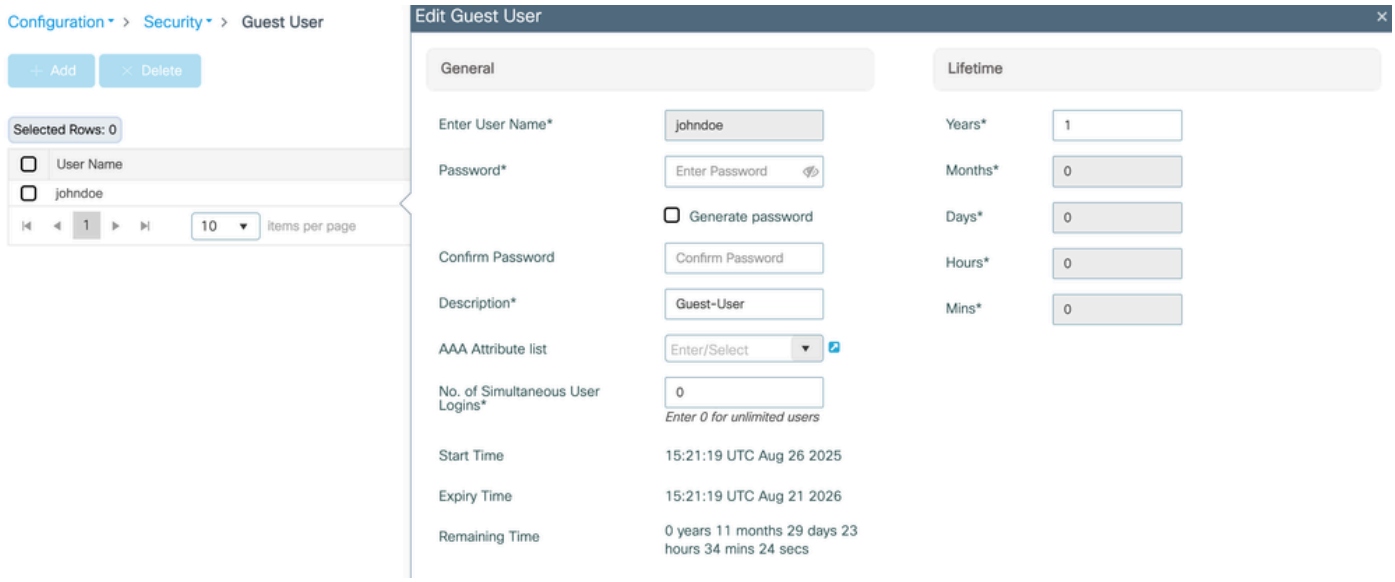
要使用已创建的策略标记对AP进行标记，请导航到Configuration > Wireless > Access Points，选择AP，在General选项卡上，右侧是AP使用的标记。



创建访客用户名

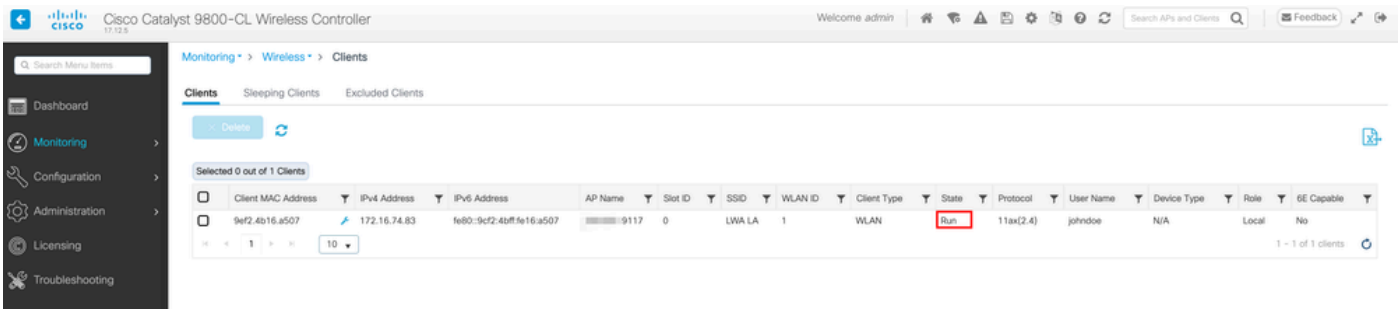
如果您在参数映射中选择了webauth类型，则需要访客用户名，要创建它，请导航到配置>安全>访客用户。

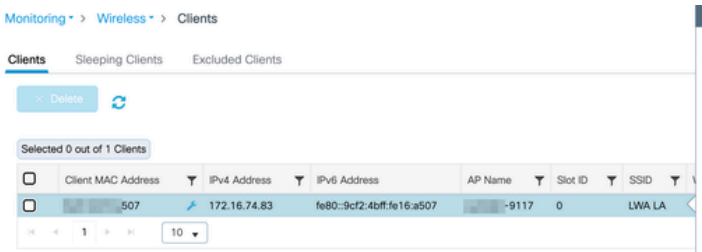
用户的最大生存时间为1年。您可以使用可用选项指定其他选项。

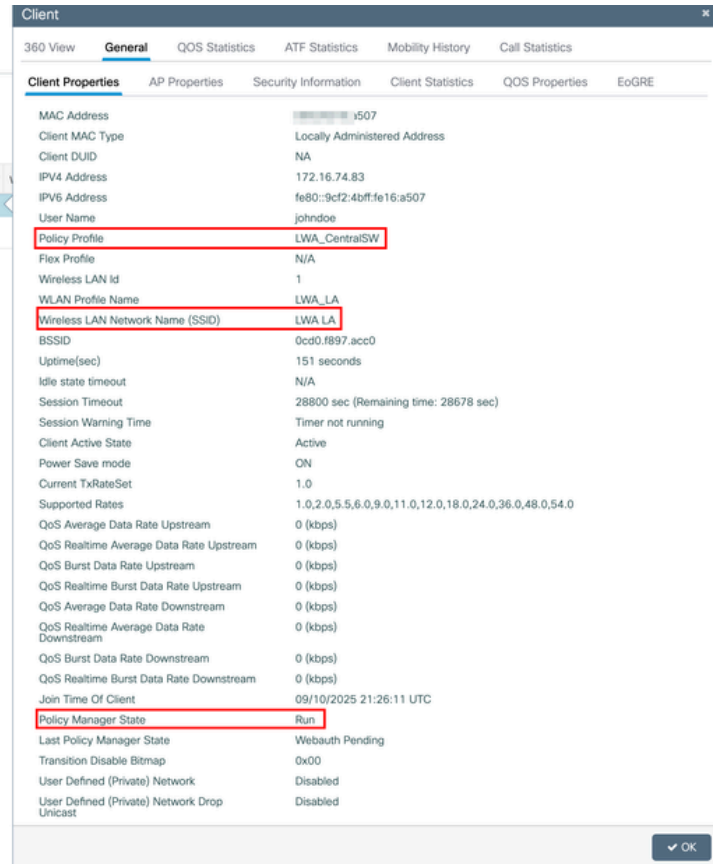

Configuration > Security > Guest User
Add
Delete
Selected Rows: 0
User Name
johndoe
1
10
items per page
Edit Guest User
General
Enter User Name*
johndoe
Password*
Enter Password
Generate password
Confirm Password
Confirm Password
Description*
Guest-User
AAA Attribute list
Enter/Select
No. of Simultaneous User Logins*
0
Enter 0 for unlimited users
Start Time
15:21:19 UTC Aug 26 2025
Expiry Time
15:21:19 UTC Aug 21 2026
Remaining Time
0 years 11 months 29 days 23 hours 34 mins 24 secs
Lifetime
Years*
1
Months*
0
Days*
0
Hours*
0
Mins*
0

验证

通过GUI


Cisco Catalyst 9800-CL Wireless Controller
Welcome admin
Search APs and Clients
Feedback
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
AP Name
Slot ID
SSID
WLAN ID
Client Type
State
Protocol
User Name
Device Type
Role
6E Capable
9ef2.4b16.a507
172.16.74.83
fe80::9cf2:4bff:fe16:a507
9117
0
LWA LA
1
WLAN
Run
11ax(2.4)
johndoe
N/A
Local
No
1 - 1 of 1 clients





通过CLI

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name       Type ID State Protocol  Method    Role
-------------------------------------------------------------------------------------------------------------
9ef2.4b16.a507   xxxxx-9117 WLAN 1  Run   11ax(2.4) Web Auth  Local
9800WLC#show wireless client mac-address


       detail


Client MAC Address : 9ef2.4b16.a507


Client MAC Type : Locally Administered Address


Client DUID: NA


Client IPv4 Address : 172.16.74.83


Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507


Client Username : johndoe
```

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

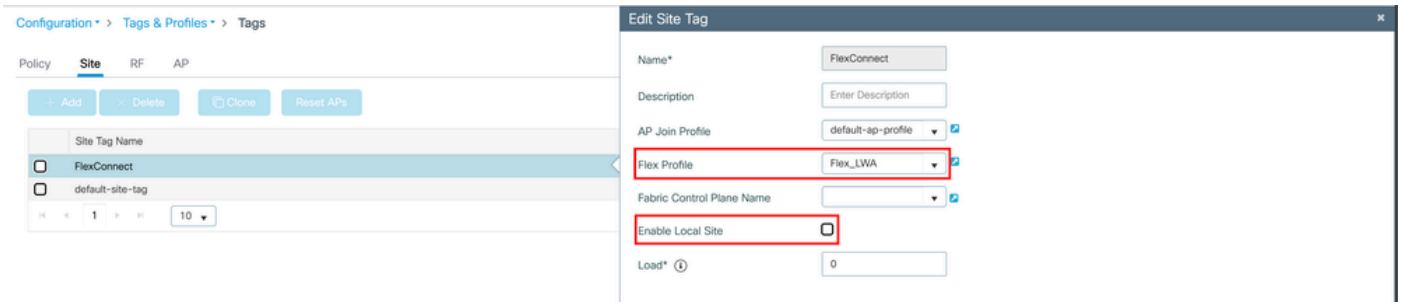
Signal to Noise Ratio : 4 dB

Fabric status : Disabled

```
Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED
```

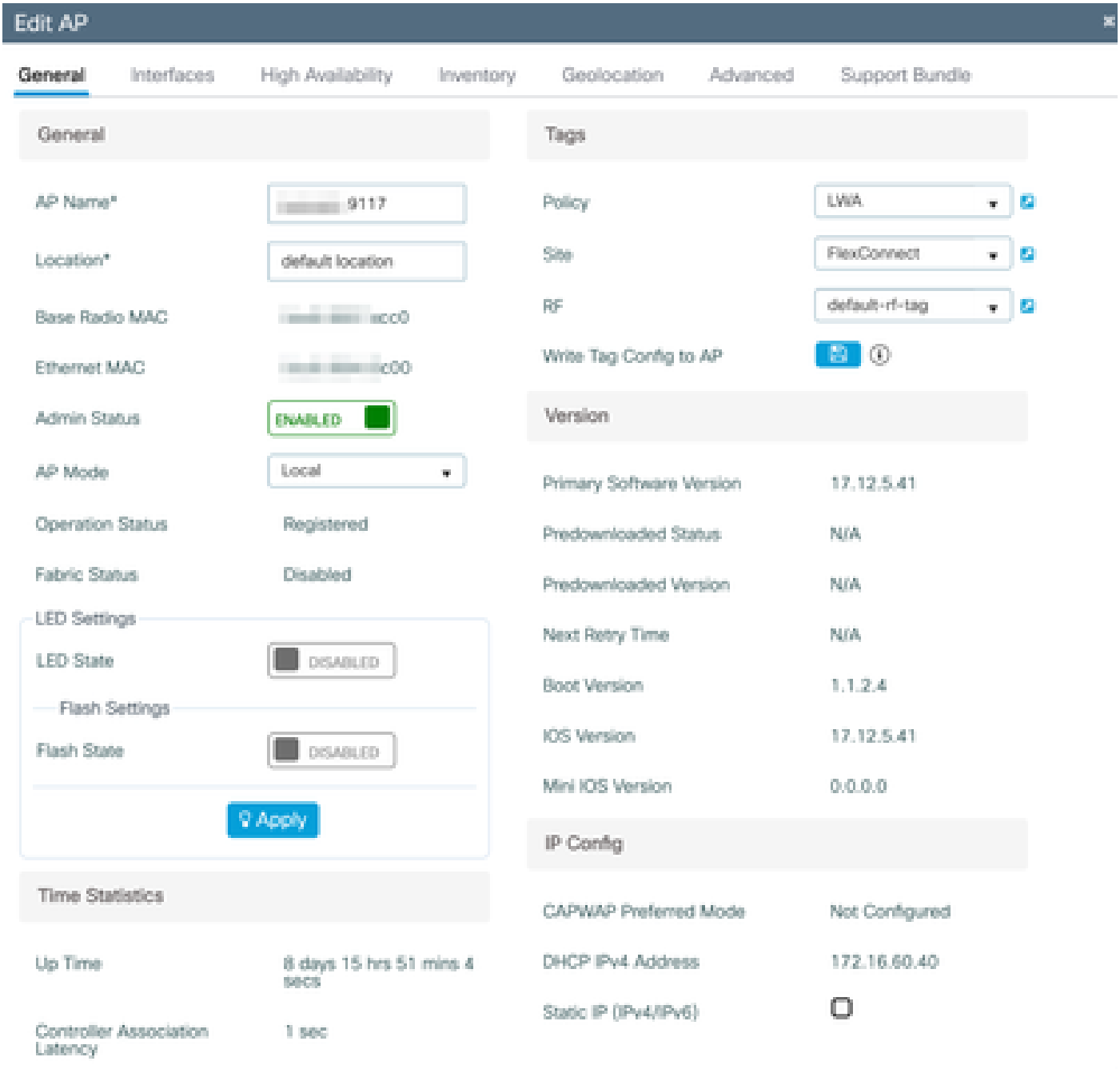
FlexConnect本地交换上的本地Web身份验证

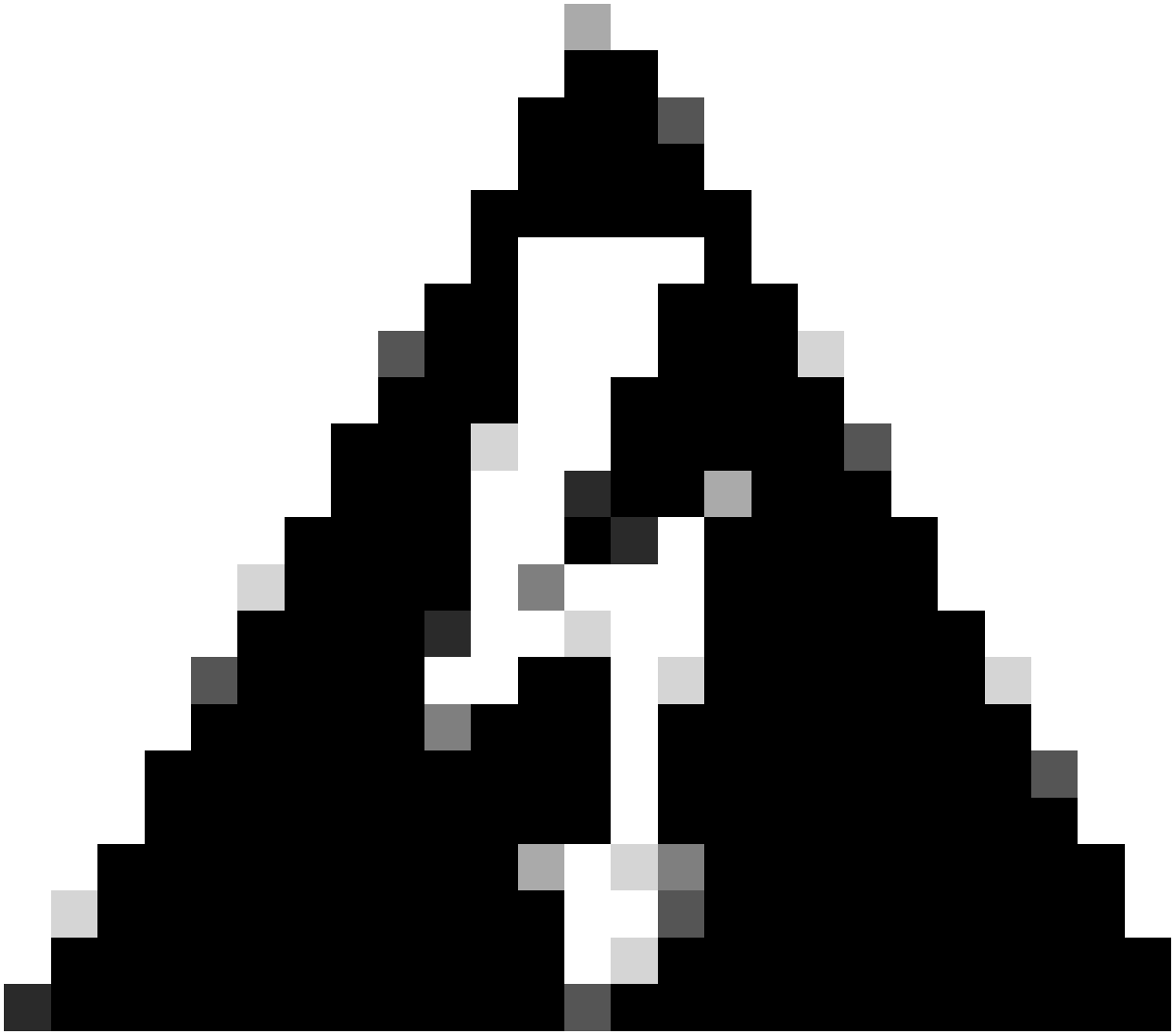
对于此场景，假设AP处于FlexConnect模式。对于处于FlexConnect模式的AP，您需要在SiteTag上关联一个Flex配置文件，其中Enable Local Site复选框处于禁用状态。此站点标签使用默认的ap-join和自定义的弹性配置文件名称Flex_LWA:



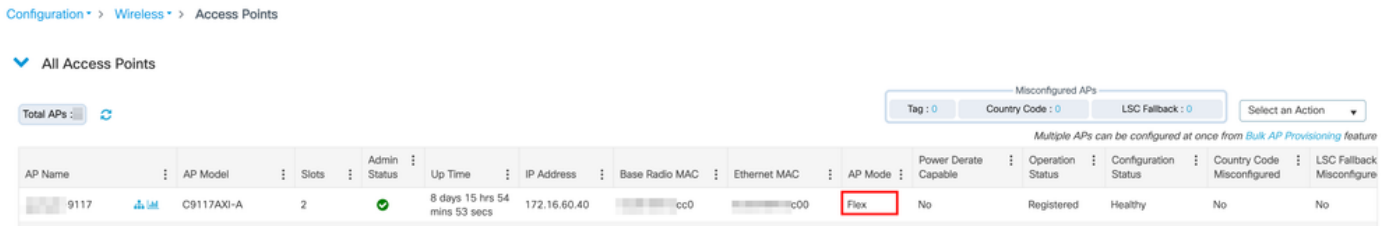
为AP分配策略标记

导航到Configuration > Wireless > Access Points，选择AP，在General选项卡的右侧是AP使用的标记。

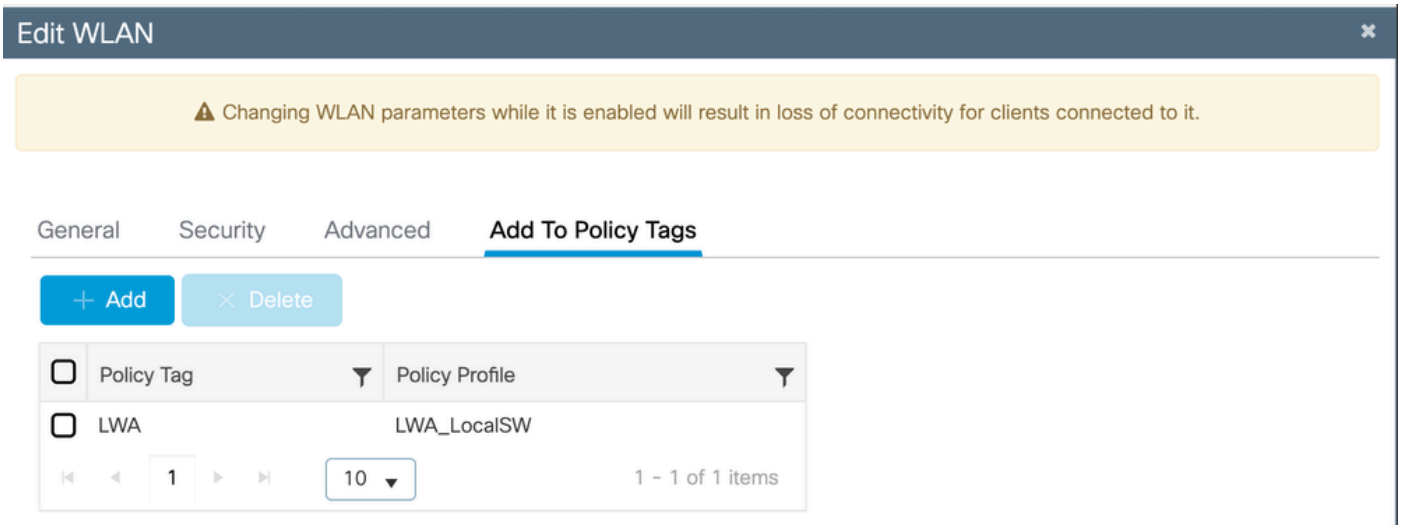


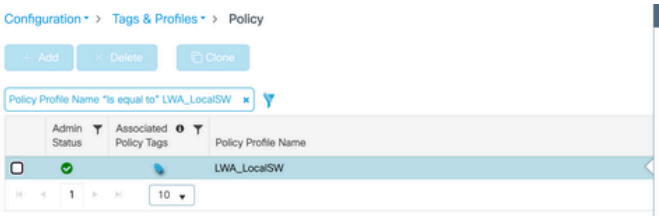


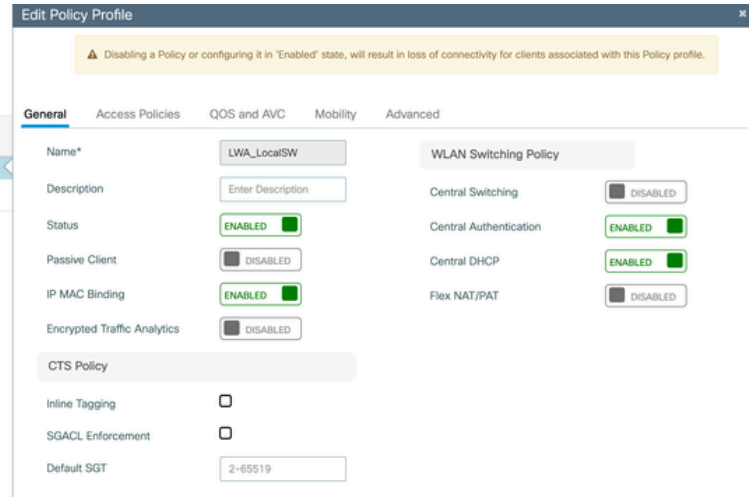
警告：更改标记会导致AP断开WLC连接。



与WLAN关联的策略配置文件是本地交换







验证

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name        Type ID  State Protocol  Method    Role
---------------------------------------------------------------------------------------------
9ef2.4b16.a507 xxxxx-9117 WLAN 1 Run 11ax(2.4) Web Auth Local

9800WLC#show wireless client mac-address


        detail


Client MAC Address :



Client MAC Type : Locally Administered Address


Client DUID: NA
```

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

```
Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0
```

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

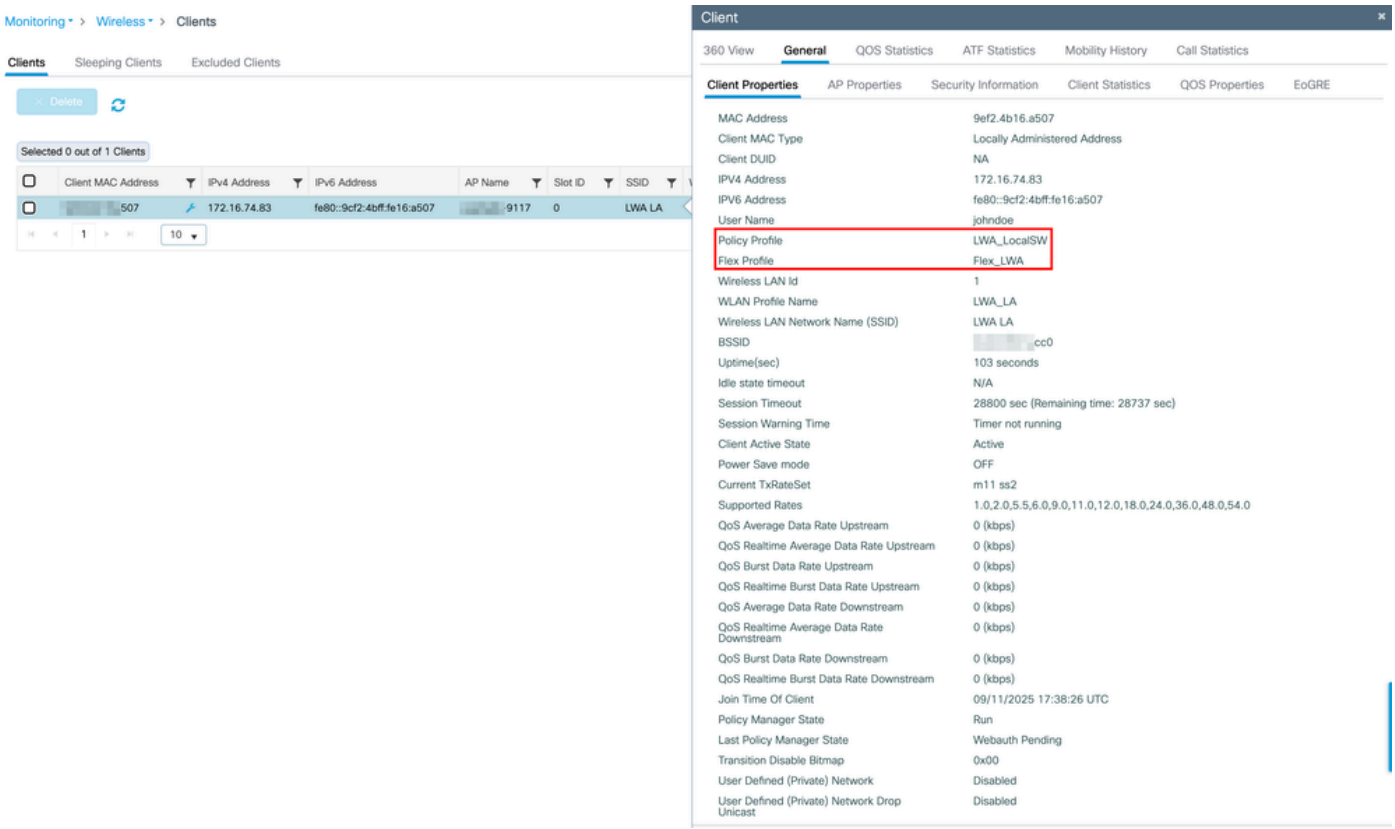
WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED



故障排除

“Web Auth Pending”状态表示客户端已与接入点关联，但尚未完成Web身份验证过程。在此状态下，控制器会拦截客户端HTTP流量并将其重定向到Web身份验证门户，以便用户登录或接受条款。客户端将保持此状态，直到成功完成Web身份验证，然后客户端策略管理器状态转换为“运行”并授予完整网络访问权限。

为了直观地查看客户端连接的流，请从使用外部身份验证配置本地Web身份验证验证LWA流。

在排除9800 WLC上LWA的常见问题中，从客户端角度描述了客户端所经历的各个阶段。

- 技术支持和文档 - Cisco Systems

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）。