使用本地身份驗證配置本地Web身份驗證

目錄

簡介

本檔案介紹如何在9800無線LAN控制器(WLC)上使用本機驗證設定本地Web驗證。

必要條件

思科建議您瞭解9800 WLC組態型號。

需求

思科建議您瞭解以下主題：

- Cisco WLC 9800系列。
- Web驗證的全面知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800-CL WLC Cisco IOS® XE版本17.12.5
- 思科存取點C9117AXI。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本地Web驗證(LWA)是一種可在WLC上設定的無線區域網路(WLAN)驗證方法。使用者從可用網路清單選擇WLAN時，會將其重新導向到Web輸入網站。在此門戶中，根據配置的不同，可能會提示使用者輸入使用者名稱和密碼、接受可接受使用策略(AUP)或同時執行上述兩項操作以最終確定連線。

有關登入過程中顯示的四種Web身份驗證頁的資訊，請參閱配置本地Web身份驗證指南，並檢視Web身份驗證型別的可用選項。您也可以參閱「Types of Authentication」部分下的Configure Local Web Authentication with External Authentication指南。

引數對映

引數對映是WLC上啟用Web驗證的基本配置元素。它由一組設定組成，用於管理Web身份驗證過程的各個方面，包括身份驗證型別、重定向URL、附加的引數、超時和自定義Web頁。要啟用和管理特定SSID的基於Web的身份驗證，此對映必須連結到WLAN配置檔案。

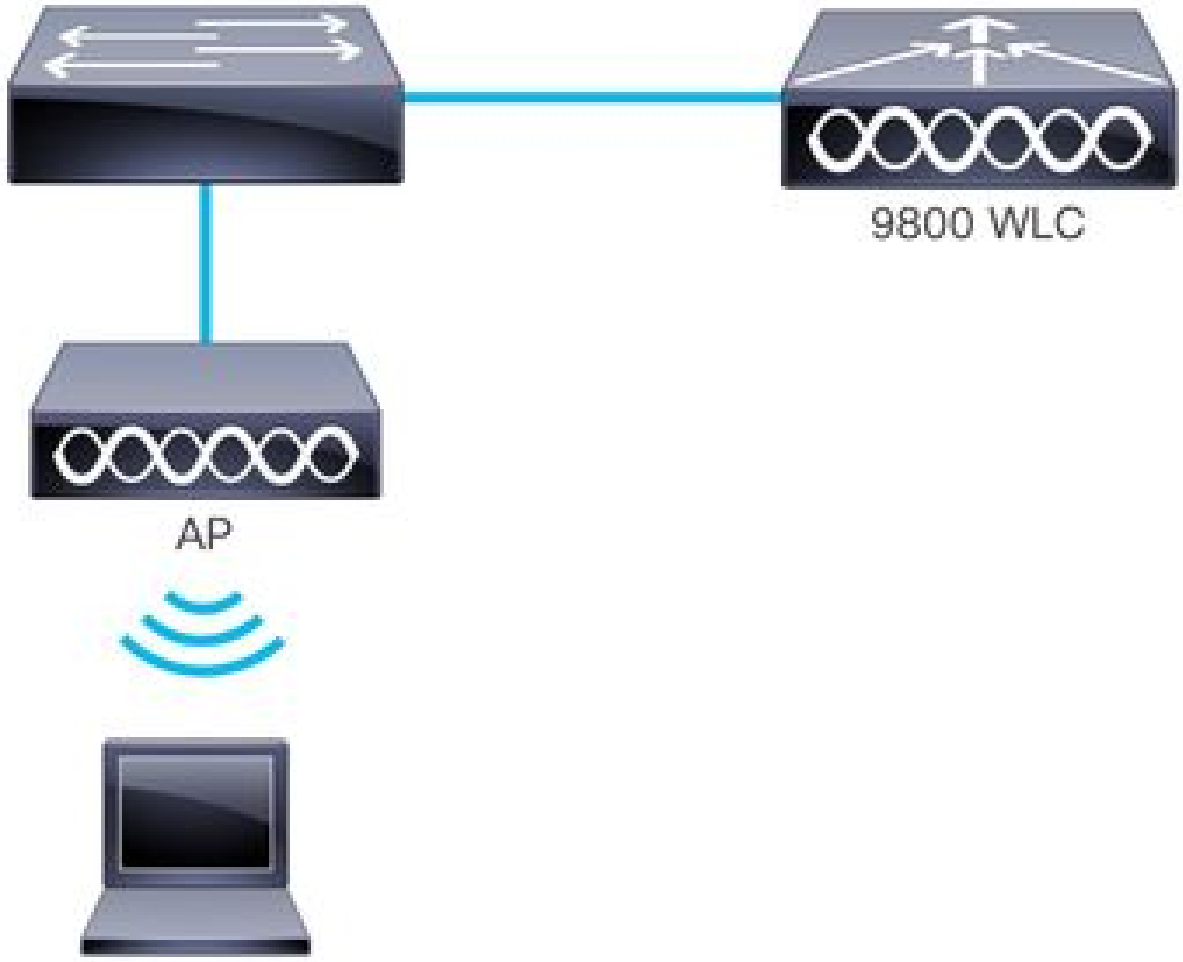
無線LAN控制器附帶一個預設全域引數映像，但管理員可選擇建立自訂引數映像，以根據特定需求自訂Web驗證行為。

用於身份驗證的資料庫

如果將引數對映配置為使用使用者名稱和密碼，則必須定義身份驗證憑據，這些憑據儲存在WLC本地。通過GUI建立訪客使用者帳戶時，可以設定每個訪客帳戶允許的最大同時登入數。有效值範圍為0到64，其中0表示該訪客使用者允許無限制的同時登入。

LWA主要用於小型部署。它支援與其他身份驗證方法整合，您可以檢查客戶端支援的身份驗證組合以瞭解詳細資訊。

該圖表示LWA的通用拓撲：



具有本地身份驗證的LWA的通用拓撲

LWA網路拓撲中的裝置：

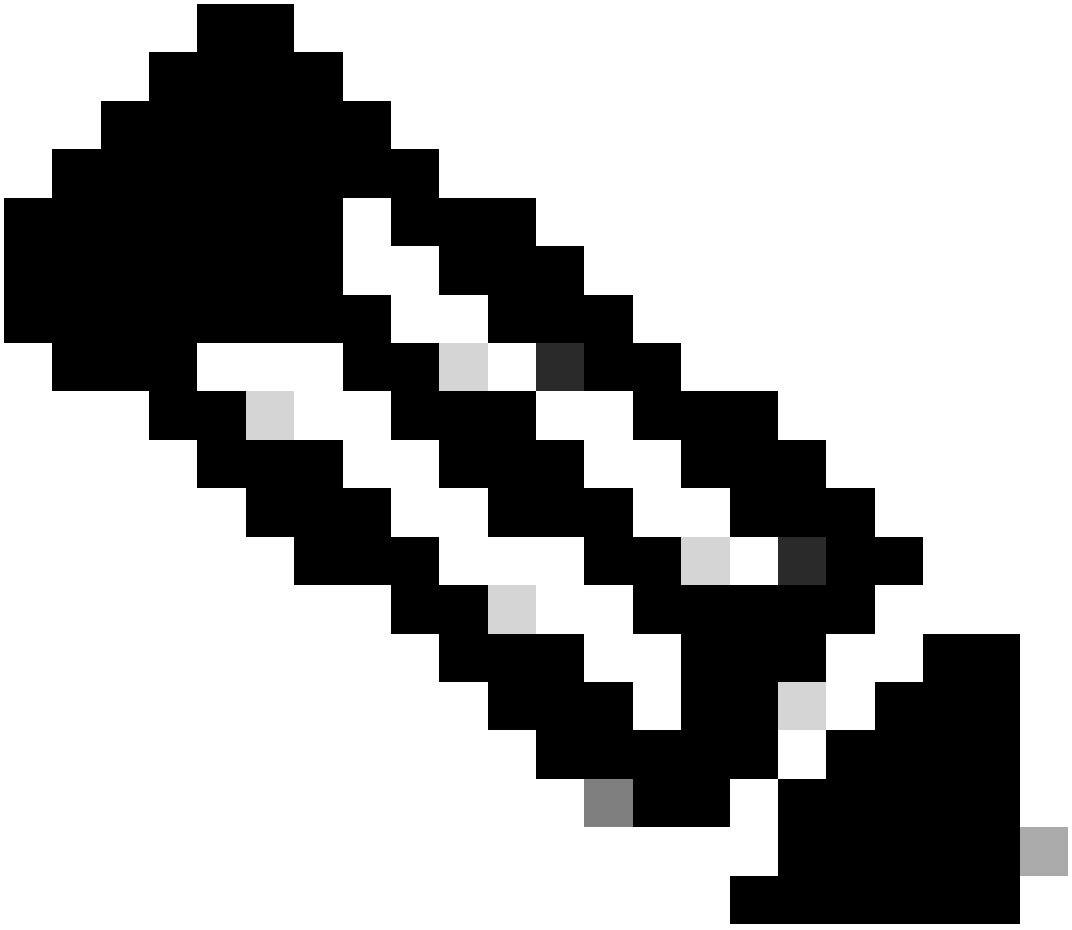
- 客戶端/請求方：向WLAN發起連線請求，稍後向DHCP和DNS伺服器發起連線請求，並響應來自WLC的通訊。
- 接入點：連接到交換機後，它會廣播訪客WLAN並為訪客裝置提供無線連線。它通過在訪客使用者完成身份驗證之前輸入有效憑證、接受AUP或兩者組合來允許DHCP和DNS流量。
- WLC/驗證器：管理AP和客戶端裝置。WLC託管重新導向URL，並在設定引數對映時強制實施管理流量及預設建立流量的存取控制清單(ACL)。擷取訪客使用者的HTTP要求，並將其重新導向到使用者必須進行驗證的Web輸入網站（登入頁面）。WLC會擷取使用者認證、驗證訪客，並檢查本機資料庫以驗證憑證有效性。
- 驗證伺服器：在此案例中，WLC相當於驗證伺服器。它驗證訪客使用者憑證，並相應地授予或拒絕網路訪問。

設定

在CLI上使用用本地身份驗證的本地Web身份驗證

用於本地身份驗證的方法清單

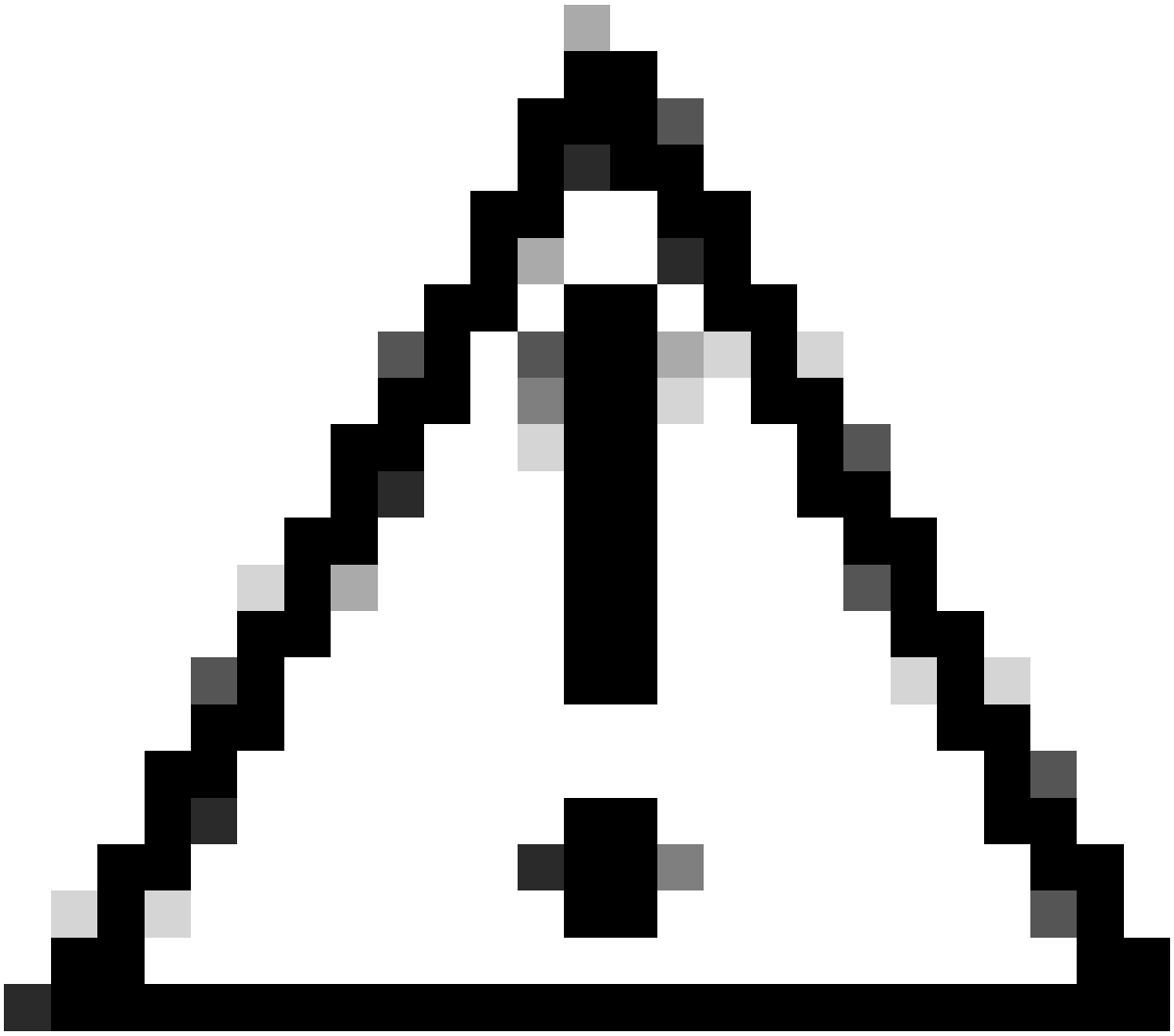
```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



附註：若要使Local Login Method List正常運作，請確保WLC上存在配置aaa authorization network default local。這是必要的，因為WLC會授權使用者進入網路。

引數對映

```
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
```



注意：虛擬IP必須是RFC 5737中建議的不可路由地址。預設情況下，IP 192.0.2.1已設定。有關虛擬IP地址的詳細資訊，請參閱Cisco Catalyst 9800系列配置最佳實踐。在AireOs上，大多數時候使用的IP是1.1.1.1。由於它已成為公共IP，因此不再建議使用。

建立多個引數對映的功能可實現定製的流程：以及每個WLAN的特定演示引數。全域引數對映決定信任點，進而決定WLC在重新導向入口上呈現給使用者端的憑證。此外，它還控制截獲的客戶端流量的型別，例如重定向門戶的HTTP/HTTPS、虛擬IP地址的域或主機名解析。這種分離使全域性對映能夠處理總體設定（如證書呈現和流量攔截），而使用者定義的引數對映則提供每個WLAN的精細體驗。

WLAN安全引數

```
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
```

建立策略配置檔案

```
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
```

建立策略標籤

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

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

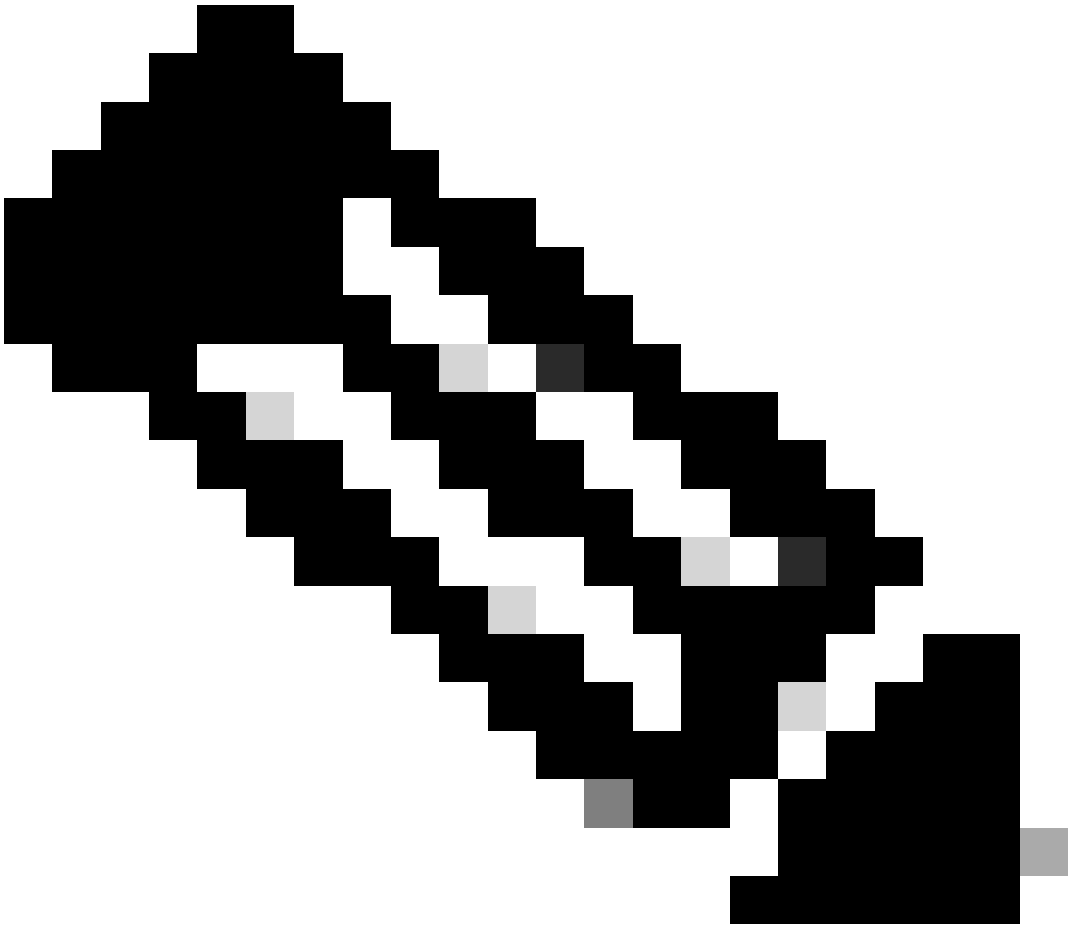
```
9800WLC(config-policy-tag)# end
```

為AP分配策略標籤

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


       >


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


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

建立訪客使用者名稱

```
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
```

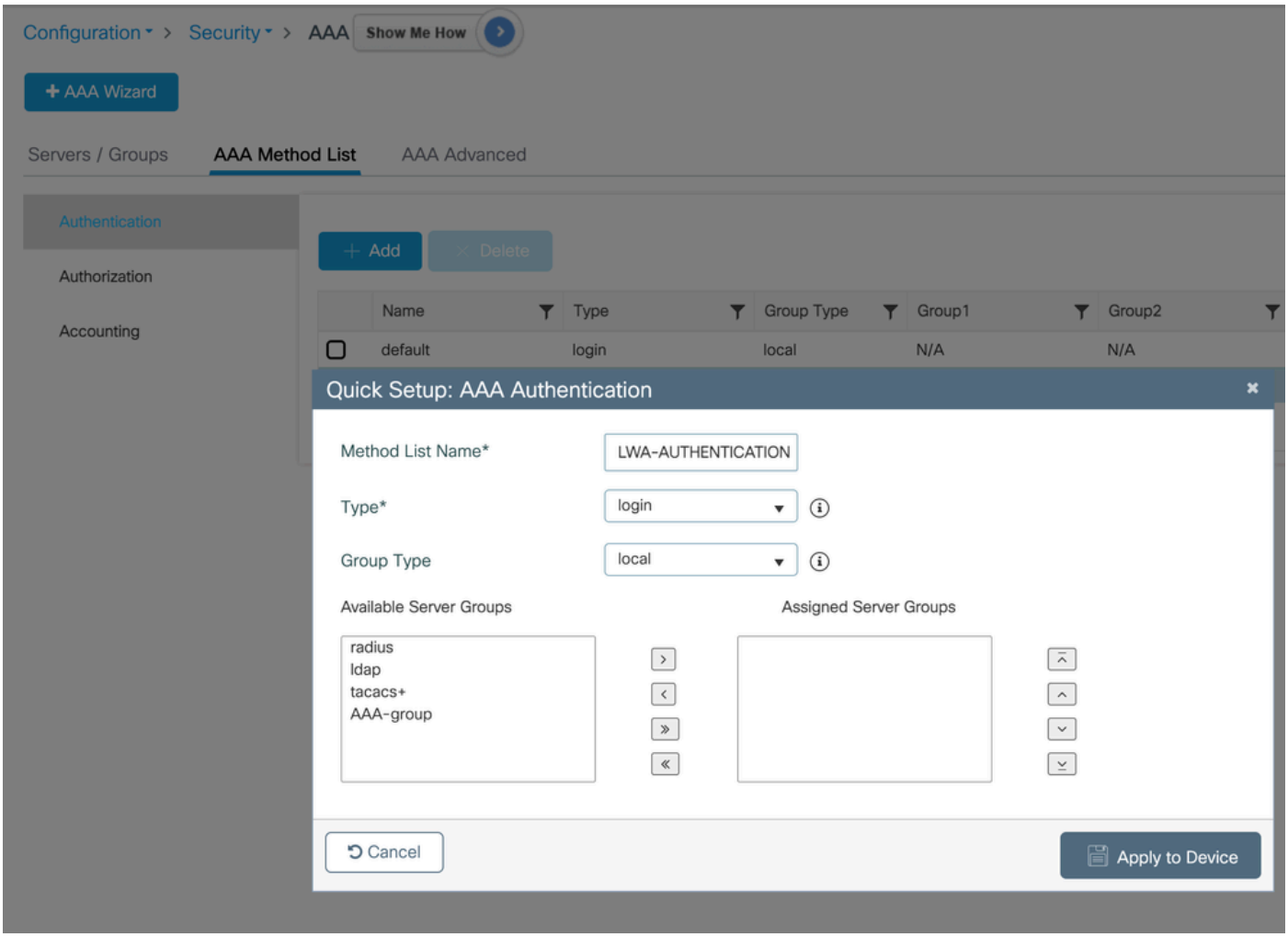


附註：在為訪客使用者設定生存期時，如果年份設定為1，則不能指定後續引數，即月、日、小時和分鐘，因為最大生存期為1年。

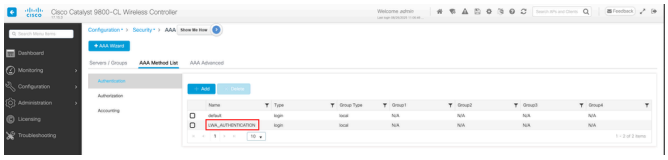
本地Web驗證與通過WebUI的本地驗證

用於本地身份驗證的方法清單

導覽至Configuration > Security > AAA > AAA Method List > Authentication > Add，以稍後在WLAN配置中使用的方法清單。

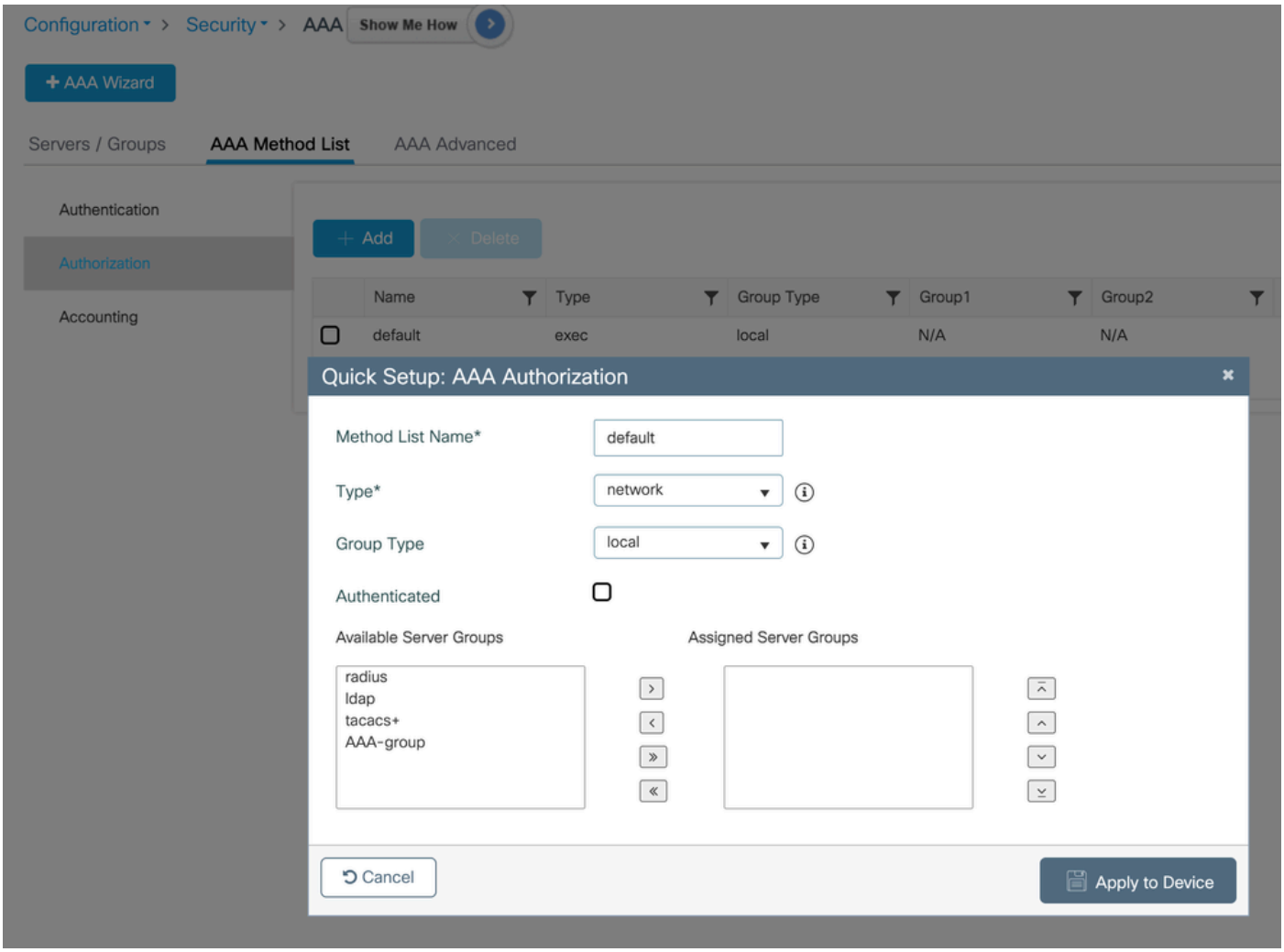


按一下Apply to Device後，確認建立AAA方法清單：

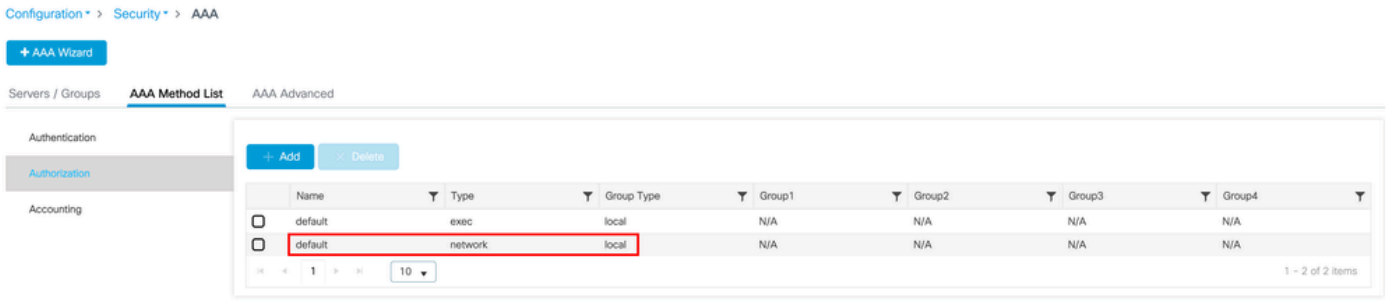


確儲存在本地授權方法清單，這是為工作而建立的本地登入方法清單的要求。

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

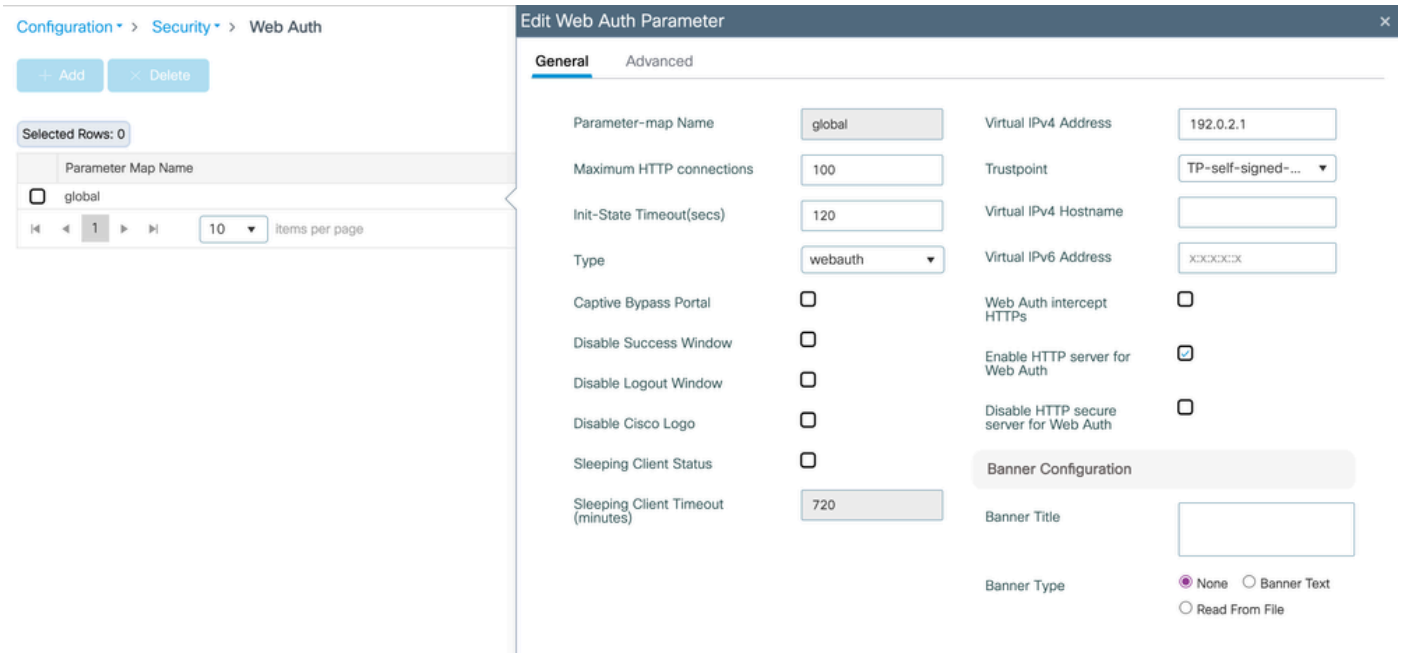


按一下Apply to Device後，確認建立AAA方法清單：

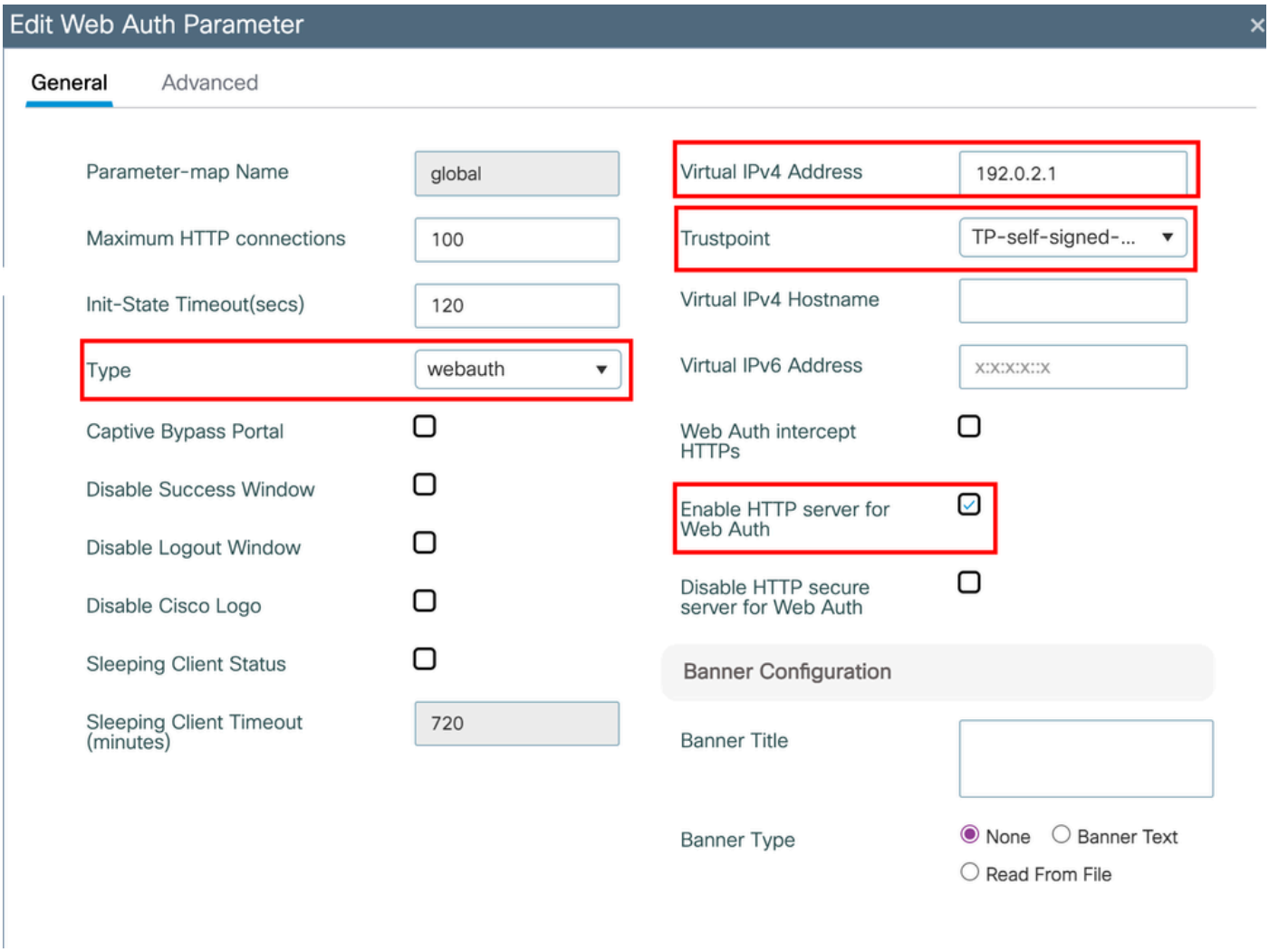


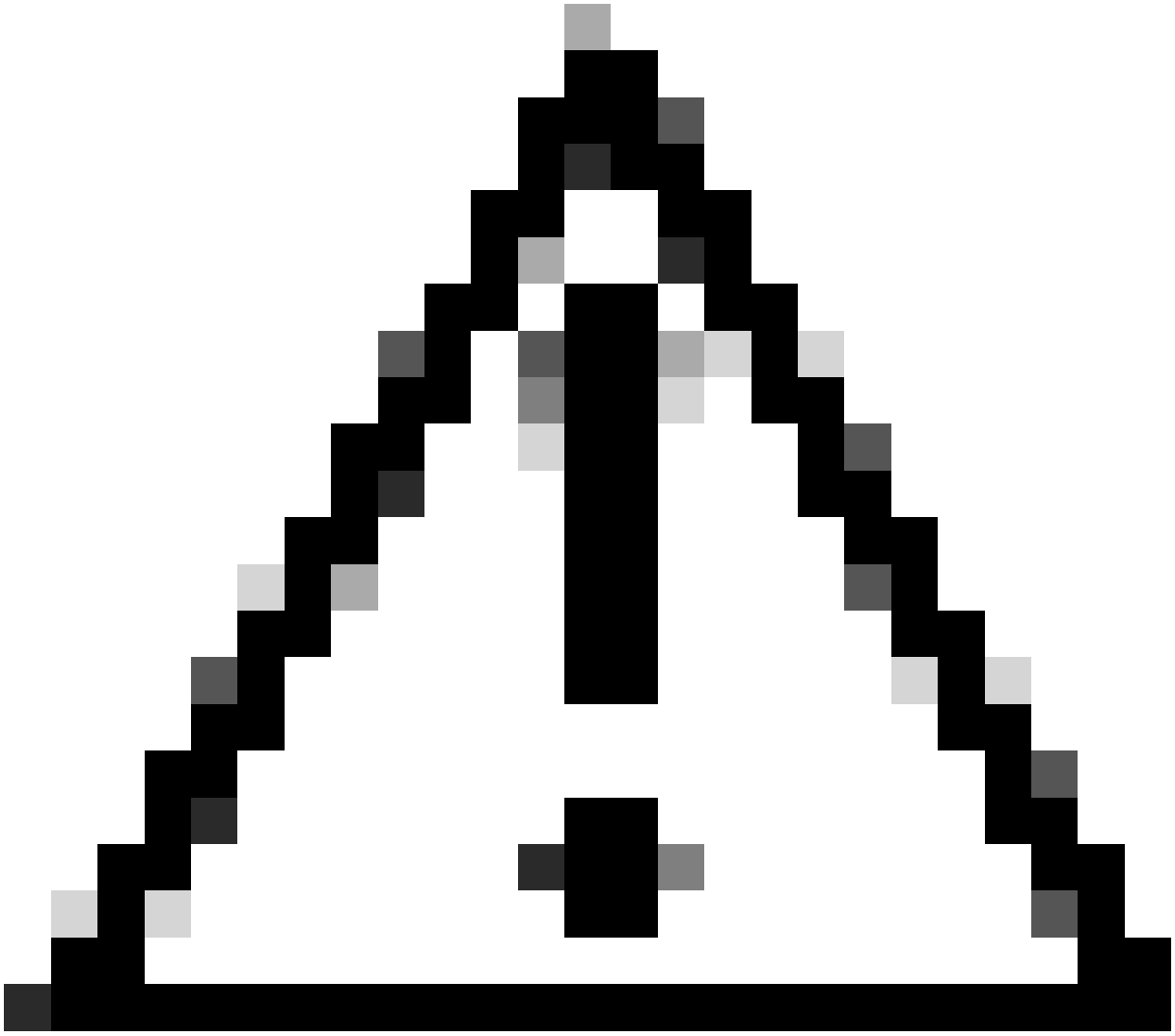
引數對映

Configuration > Security > Web Auth時編輯全域性引數對映



選擇要使用的Web驗證型別、虛擬IP和WLC在Web入口上顯示的信任點。在本例中，自簽名證書處於選中狀態，並且可能會導致「您的連線不是專用網路：:ERR_CERT_AUTHORITY_INVALID」型別的免責宣告，因為這是一個本地重要證書(LSC)，並且不是由Internet上的可識別CA簽名的。若要修改此項，請使用第三方簽名的證書。詳細資訊請參閱在Catalyst 9800 WLC上產生和下載CSR憑證，或是提供視訊選項，說明在Cisco 9800 WLC上上傳和建立Truspoint以更新WebAuth和WebAdmin的憑證 |安全無線LAN控制器設定。

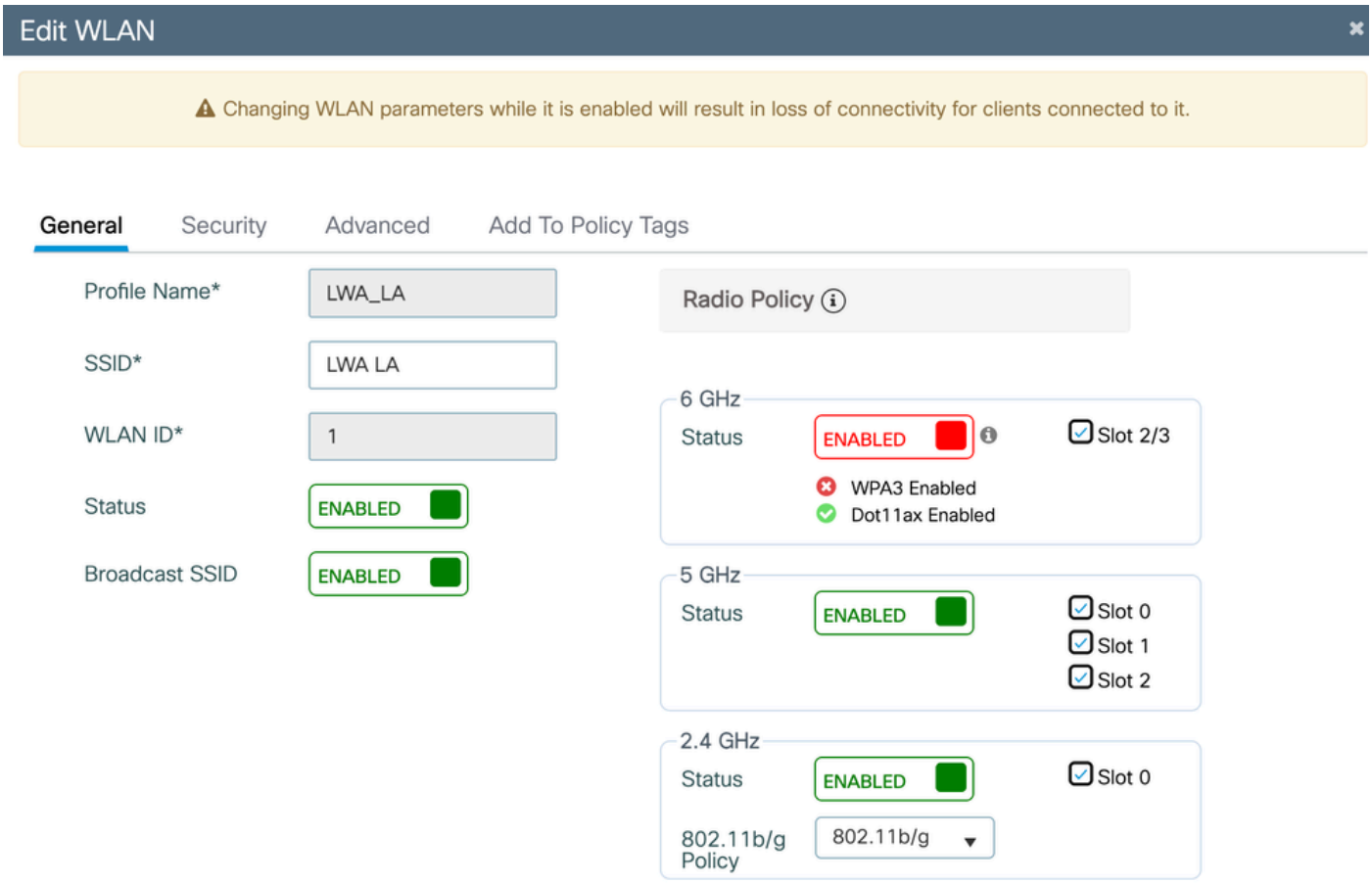

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
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



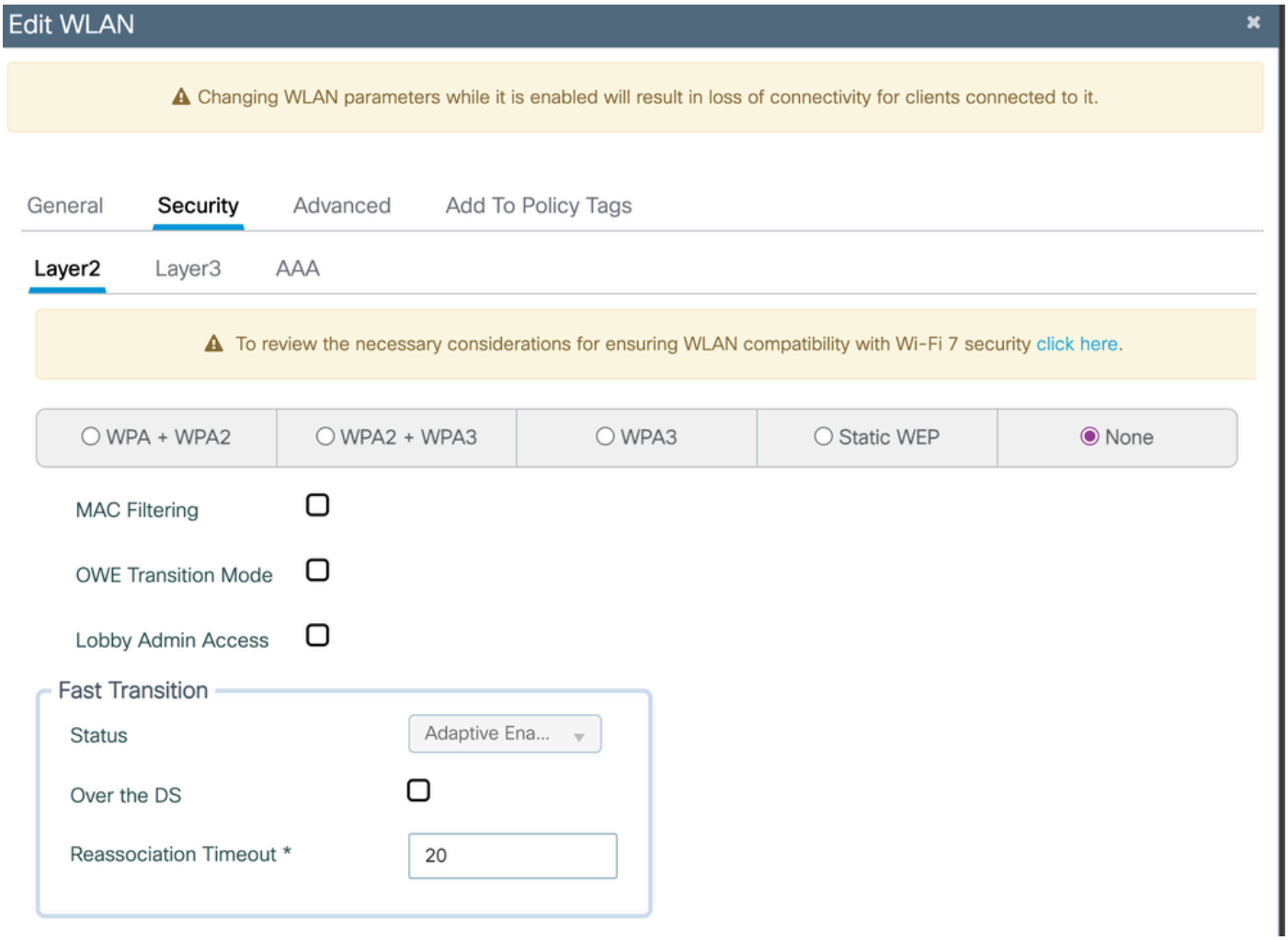
注意：如果您在9800上全域性停用HTTP，請確認您已選中「Enable HTTP server for Web Auth」，因為Cisco已分隔這些進程的依存關係。客戶端或Supplicant客戶端將啟動HTTP連線進程，並且控制器會攔截該會話以顯示Web門戶。因此，除非絕對需要，否則建議不要啟用Web Auth Intercept HTTPS，因為此設定對大多數部署來說是不必要的，而且可能會提高控制器CPU利用率，從而影響效能。

WLAN安全引數

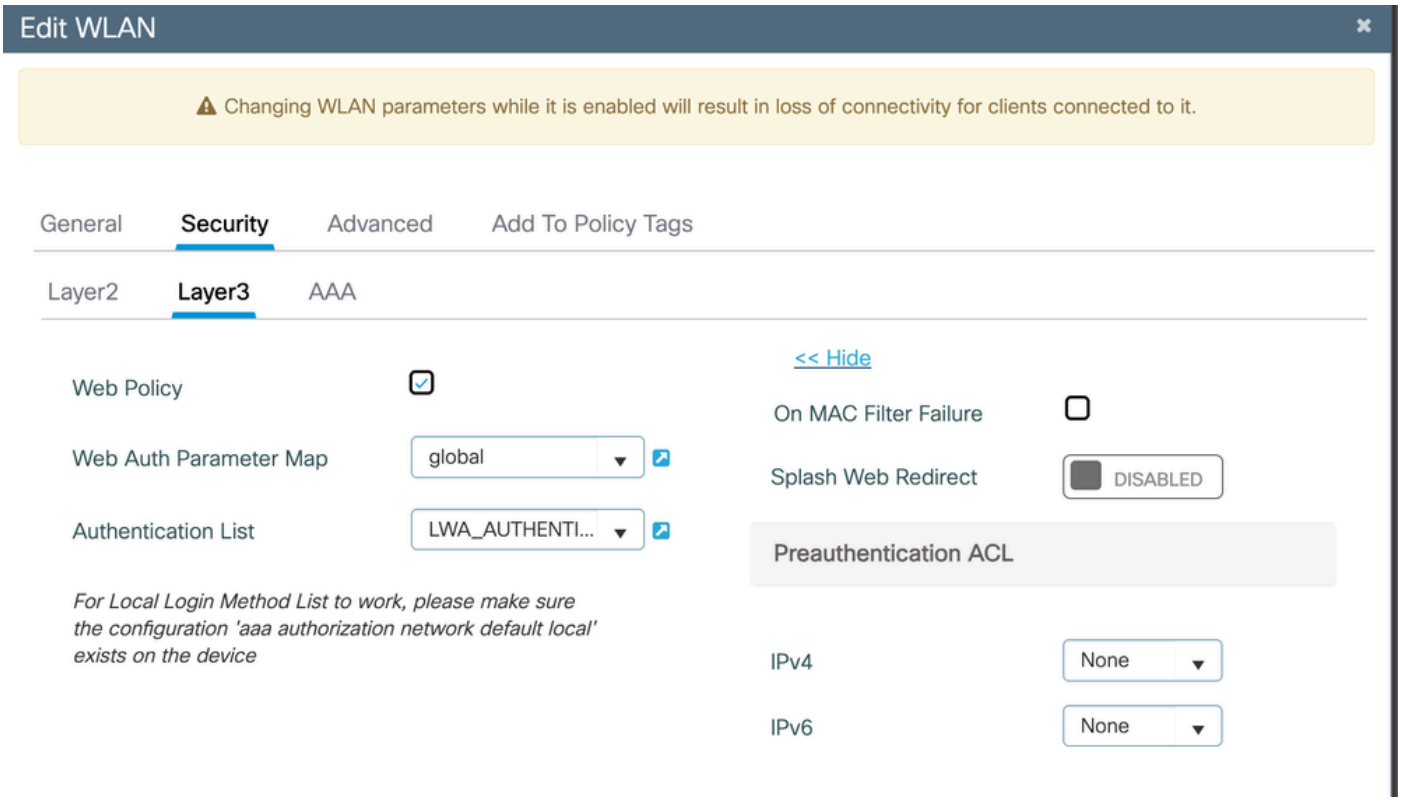
導覽至Configuration > Tags & Profiles > WLANs，然後按一下Add。



在Security頁籤上，為Layer2選擇None。

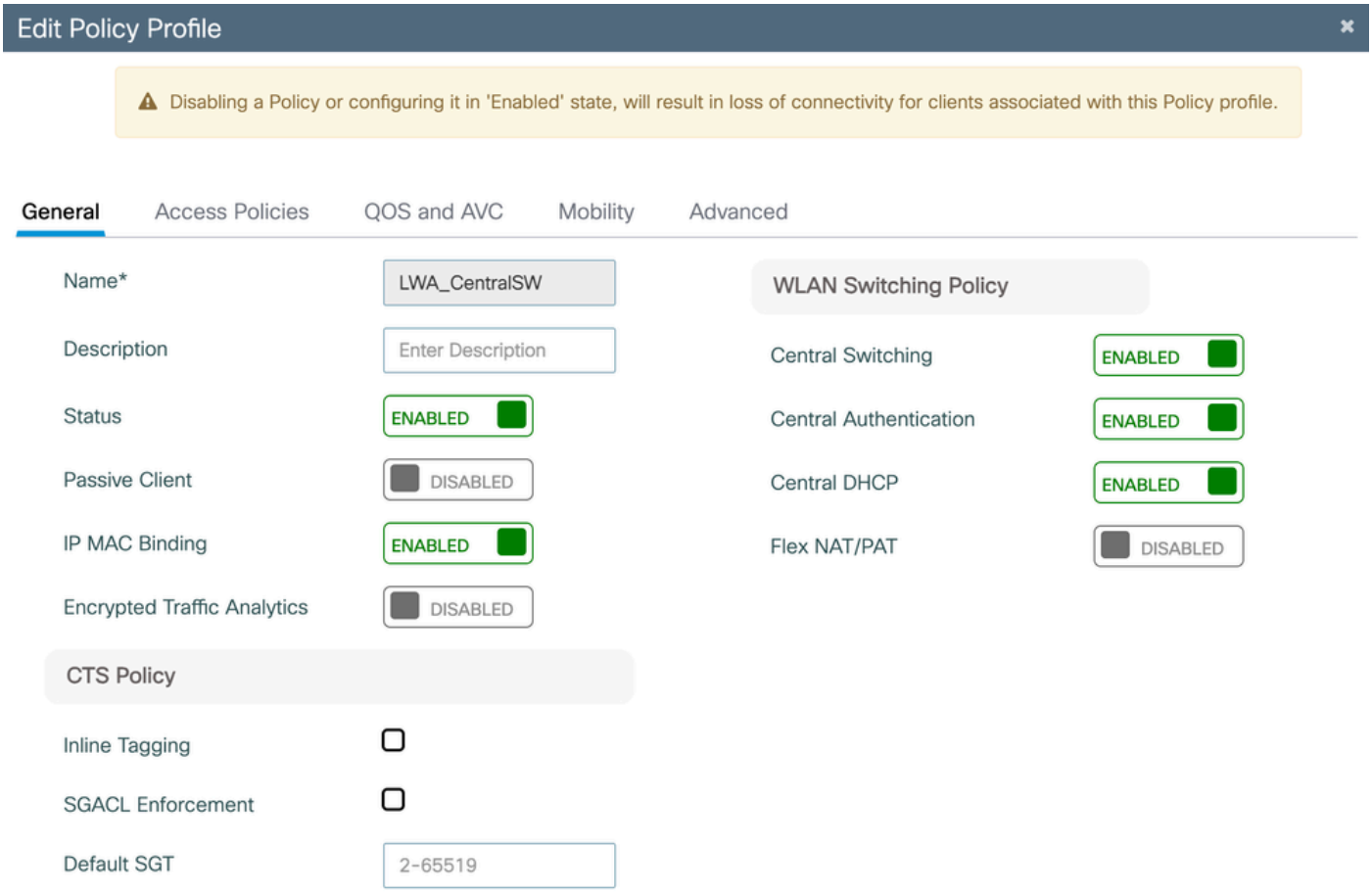


在Security頁籤上，對於Layer3，選中Web Policy框，從下拉選單和Authentication List中選擇以前配置的引數對映。

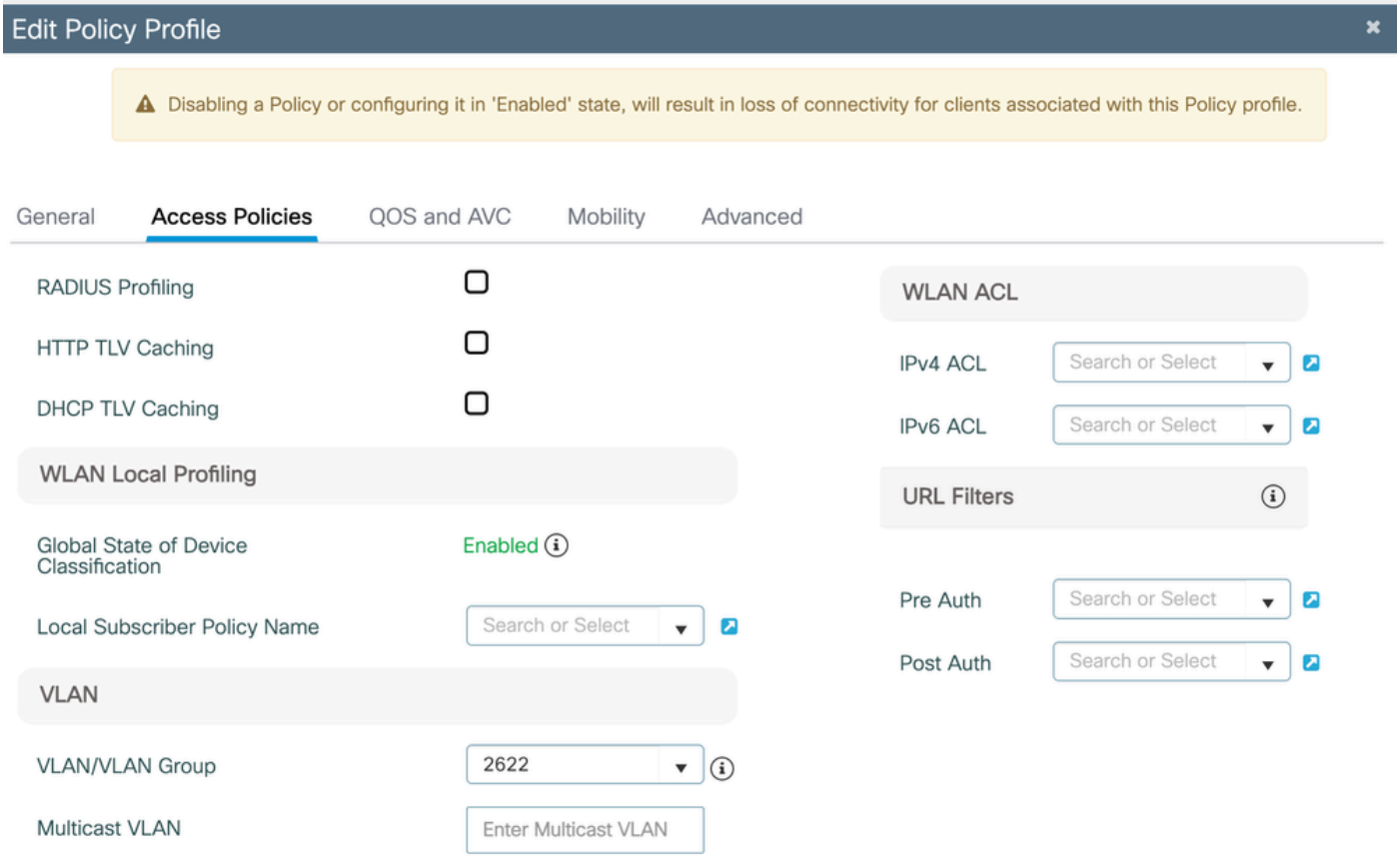


建立策略配置檔案

要建立連結到WLAN配置檔案的策略配置檔案，請導航到Configuration > Tags & Profiles > Policy。

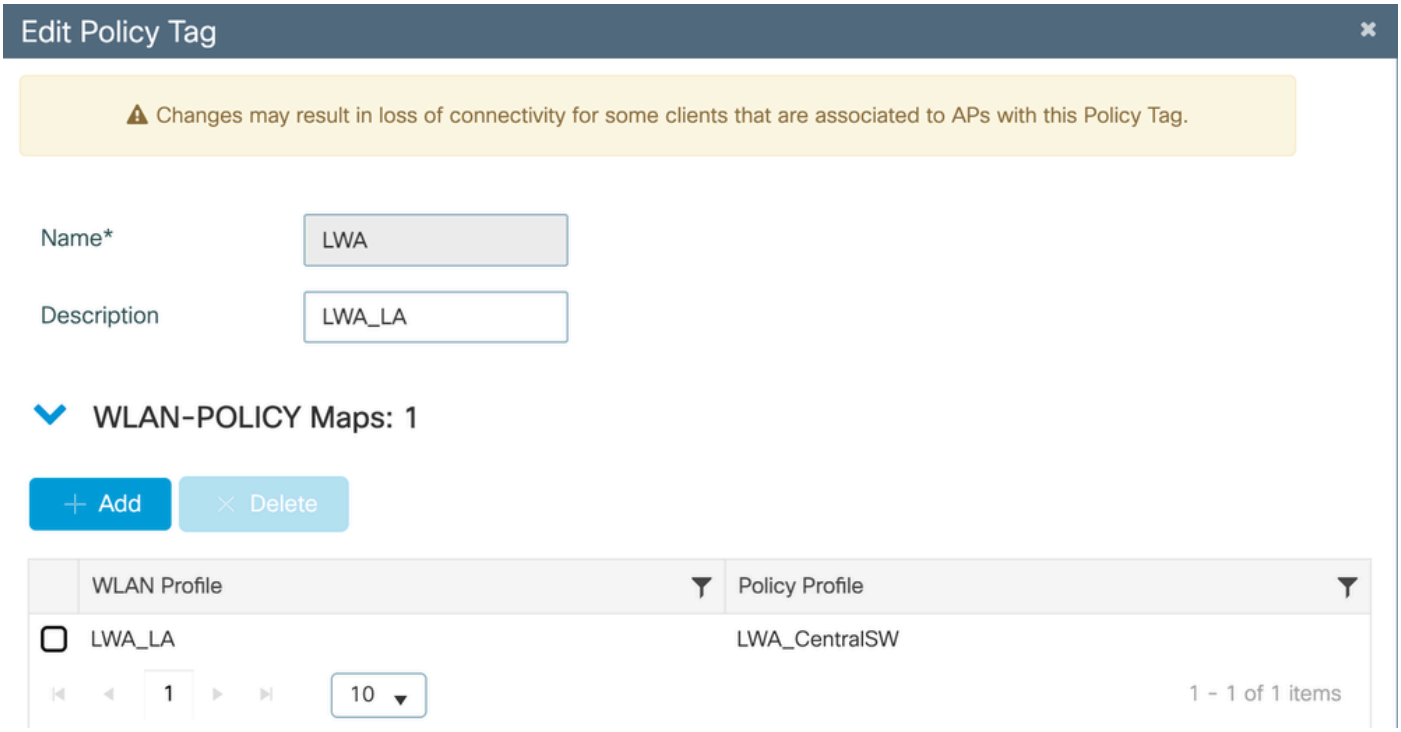


在Access Policies頁籤上，選擇客戶端/請求方從中請求IP的VLAN。



建立策略標籤

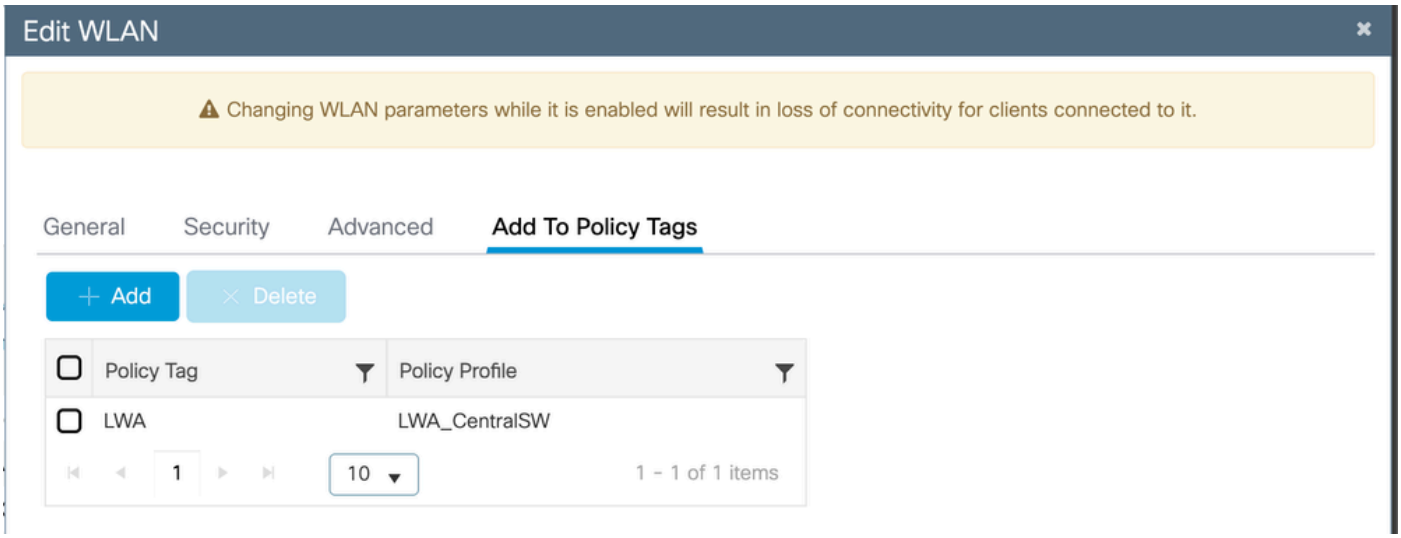
在本配置指南中，我們建立了名為LWA的自定義策略標籤。



關聯WLAN和策略配置檔案

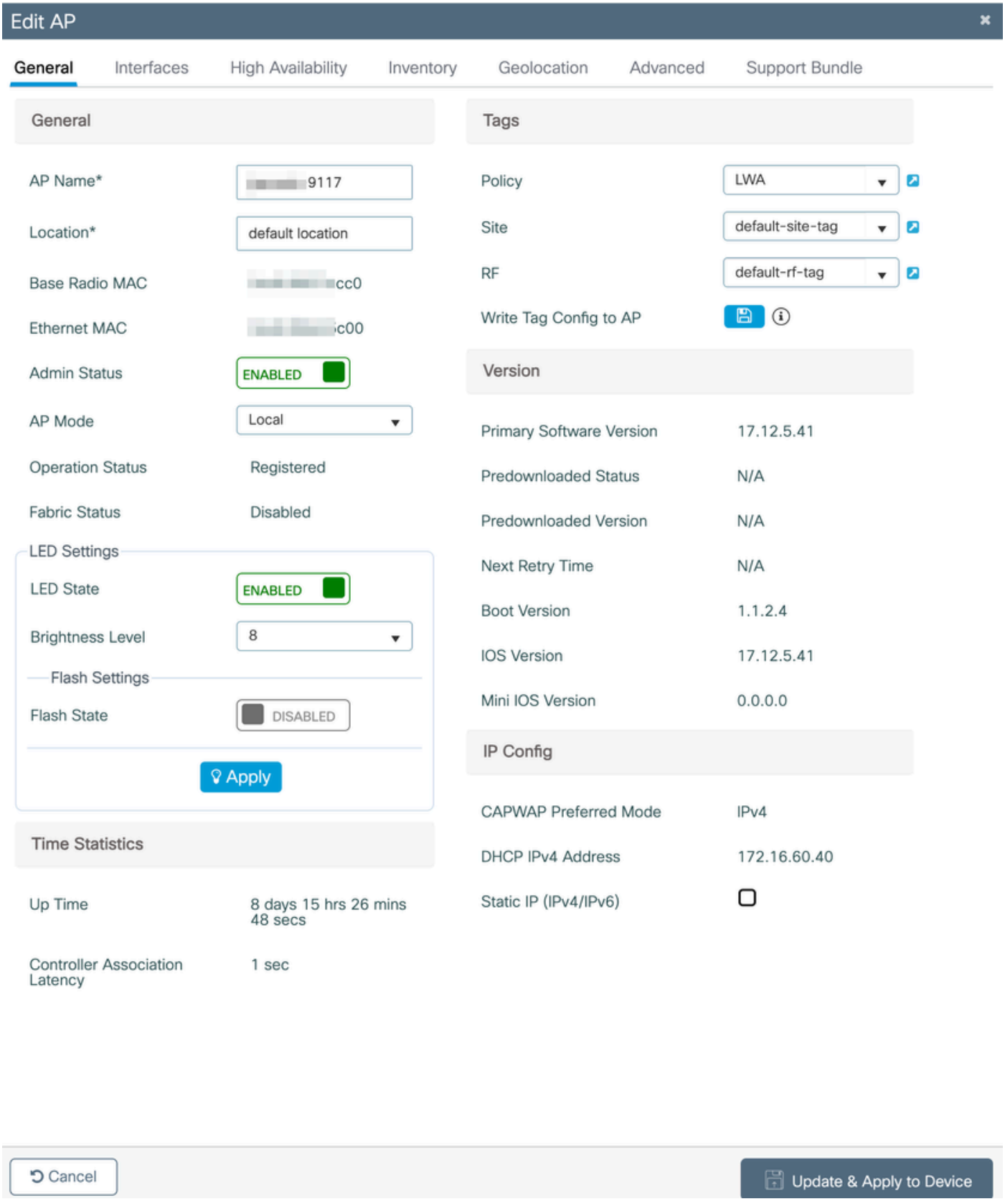
若要將交換原則從原則設定檔和WLAN連結，請導覽至Configuration > Tags & Profiles >

WLANs，選擇WLAN Profile，然後按一下Add to Policy Tags。



為AP分配策略標籤

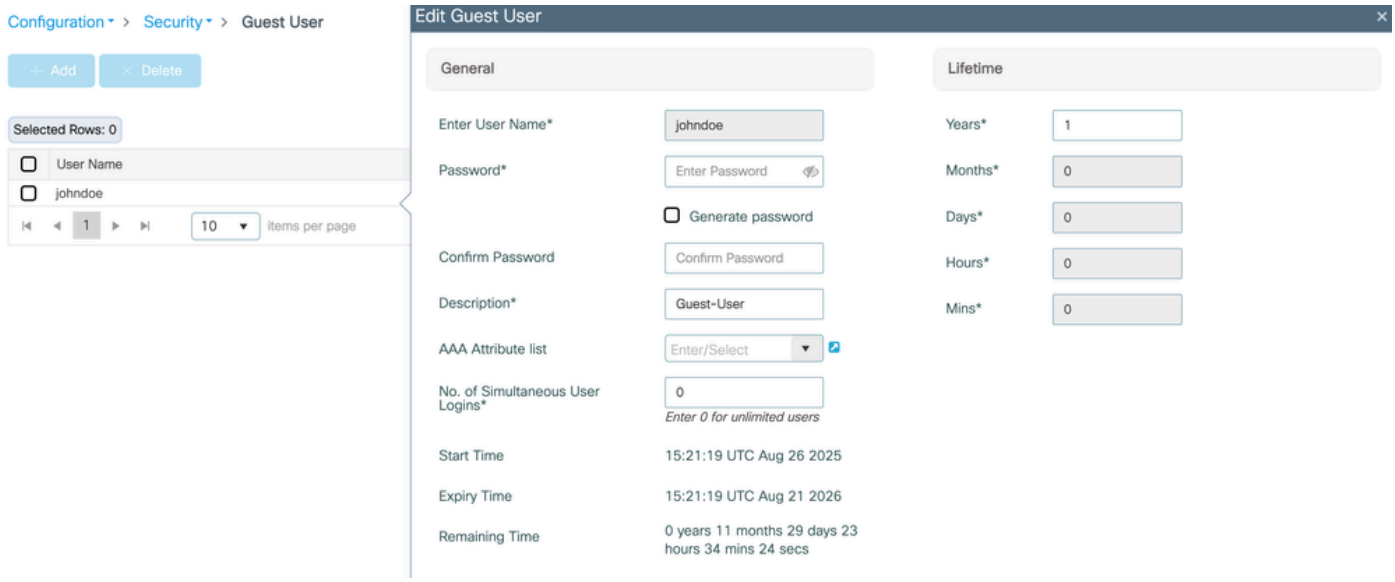
若要使用已建立的策略標籤來標籤AP，請導航到Configuration > Wireless > Access Points，選擇該AP，在General頁籤的右側是AP使用的標籤。



建立訪客使用者名稱

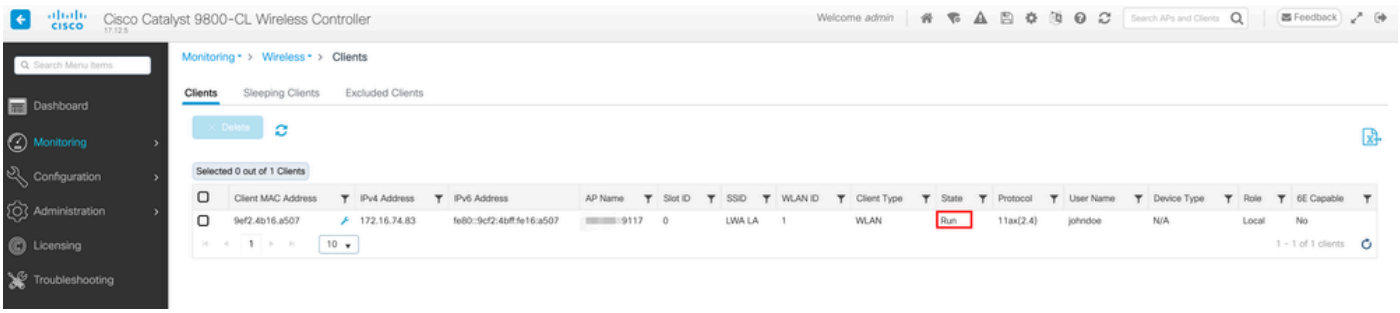
如果您在引數對映上選擇了webauth型別，則需要使用Guest User-Name，要建立它，請導航到Configuration > Security > Guest User。

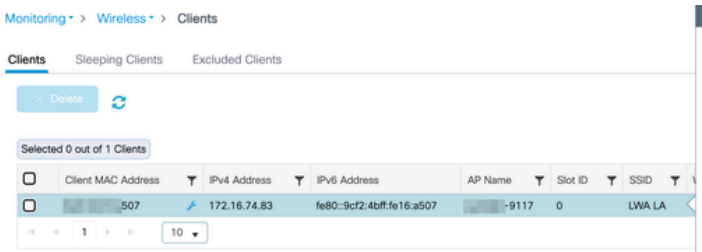
使用者的最大生存時間為1年。您可以使用可用選項指定其他。

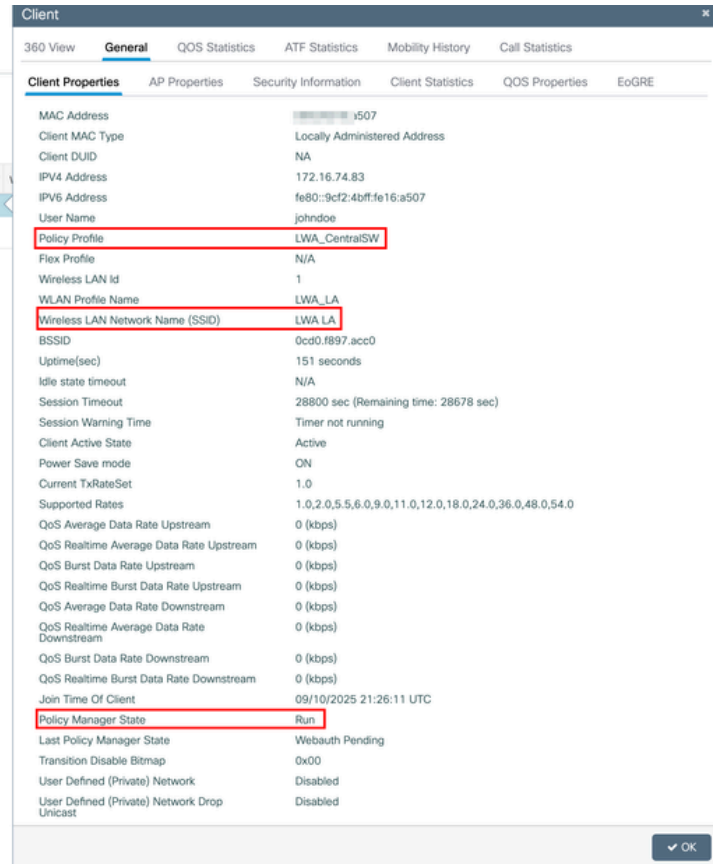

Configuration > Security > Guest User
Add
Delete
Selected Rows: 0
User Name
johndoe
1
10
items per page
Edit Guest User
General
Enter User Name*
johndoe
Password*
Enter Password
Generate password
Confirm Password
Confirm Password
Description*
Guest-User
AAA Attribute list
Enter/Select
No. of Simultaneous 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

驗證

通過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
10
1 - 1 of 1 clients





通過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

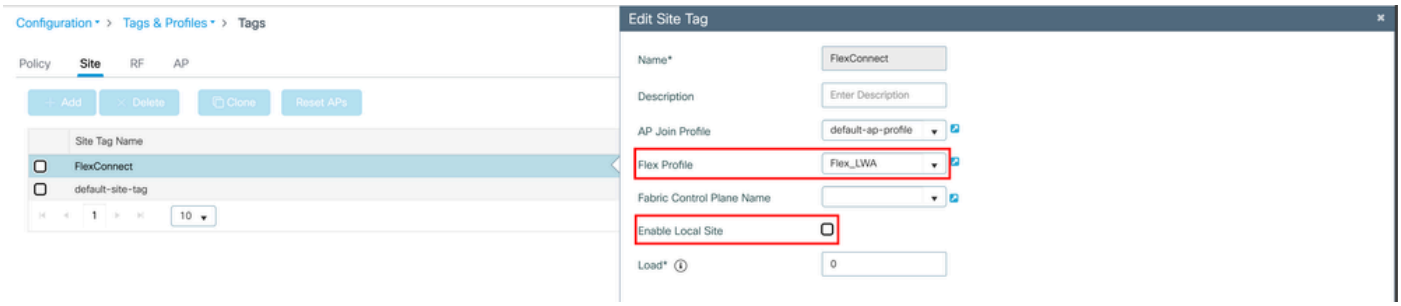
Signal to Noise Ratio : 4 dB

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
```

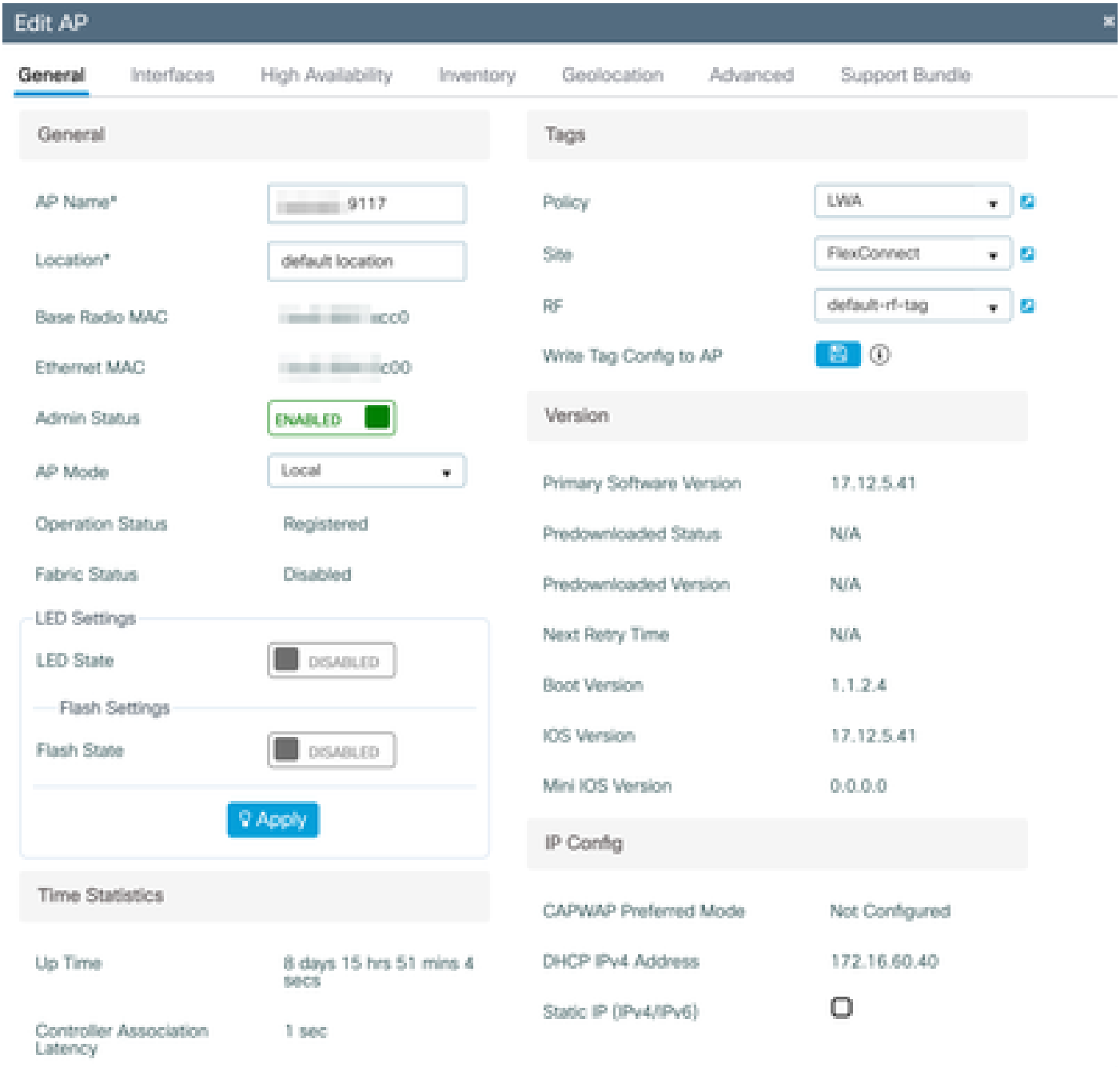
FlexConnect本地交換上的本地Web驗證

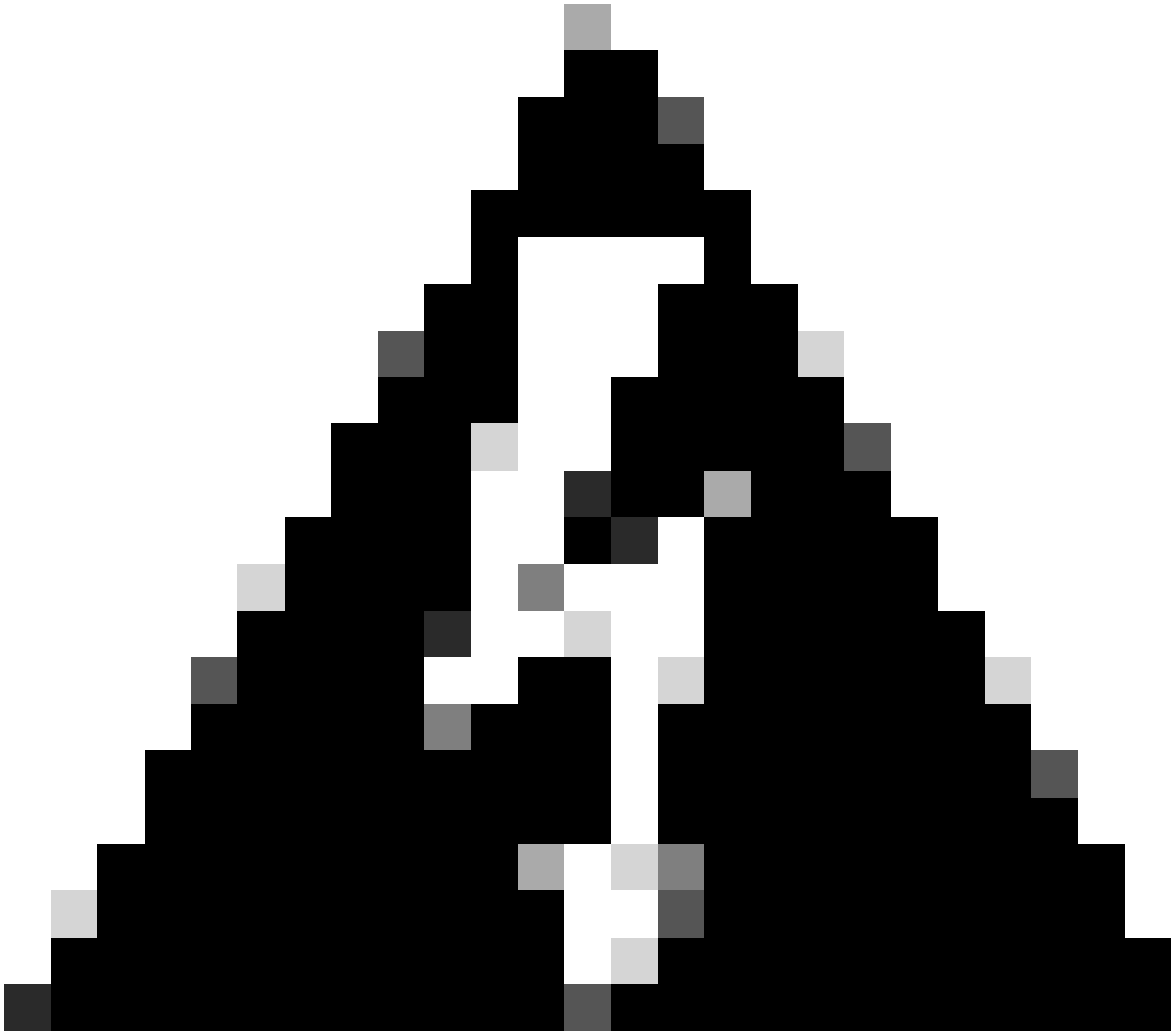
在此案例中，假設AP處於FlexConnect模式。要使AP處於FlexConnect模式，您需要在SiteTag上關聯一個Flex配置檔案，其中「啟用本地站點」覈取方塊處於禁用狀態。此站點標籤使用預設的ap-join和自定義的彈性配置檔名稱Flex_LWA:



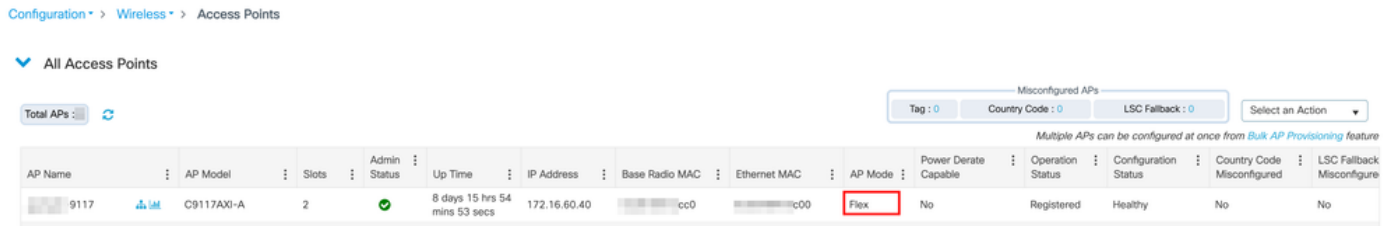
為AP分配策略標籤

導航到Configuration > Wireless > Access Points，選擇AP，在General頁籤的右側是AP使用的標籤。

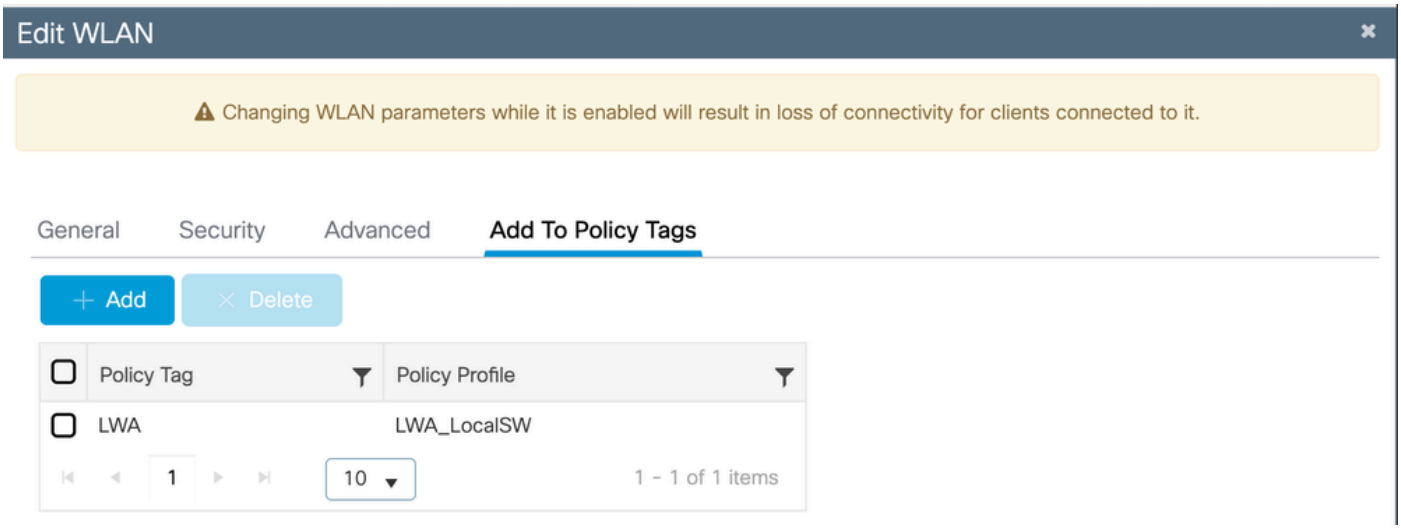


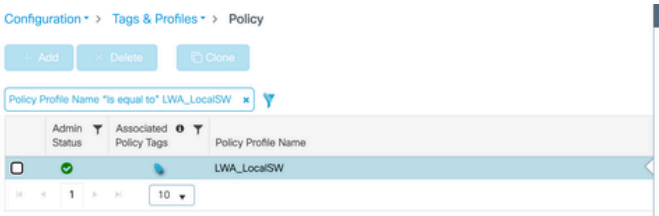


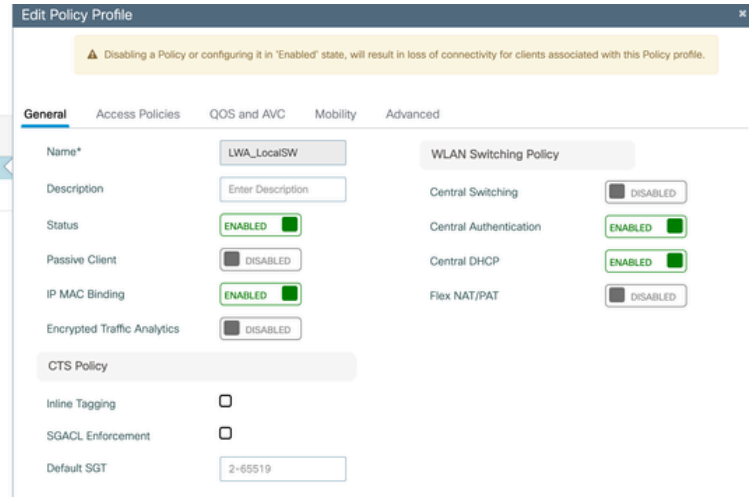
警告：更改標籤會導致AP退出WLC。



與WLAN關聯的策略配置檔案是本地交換







驗證

```
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)

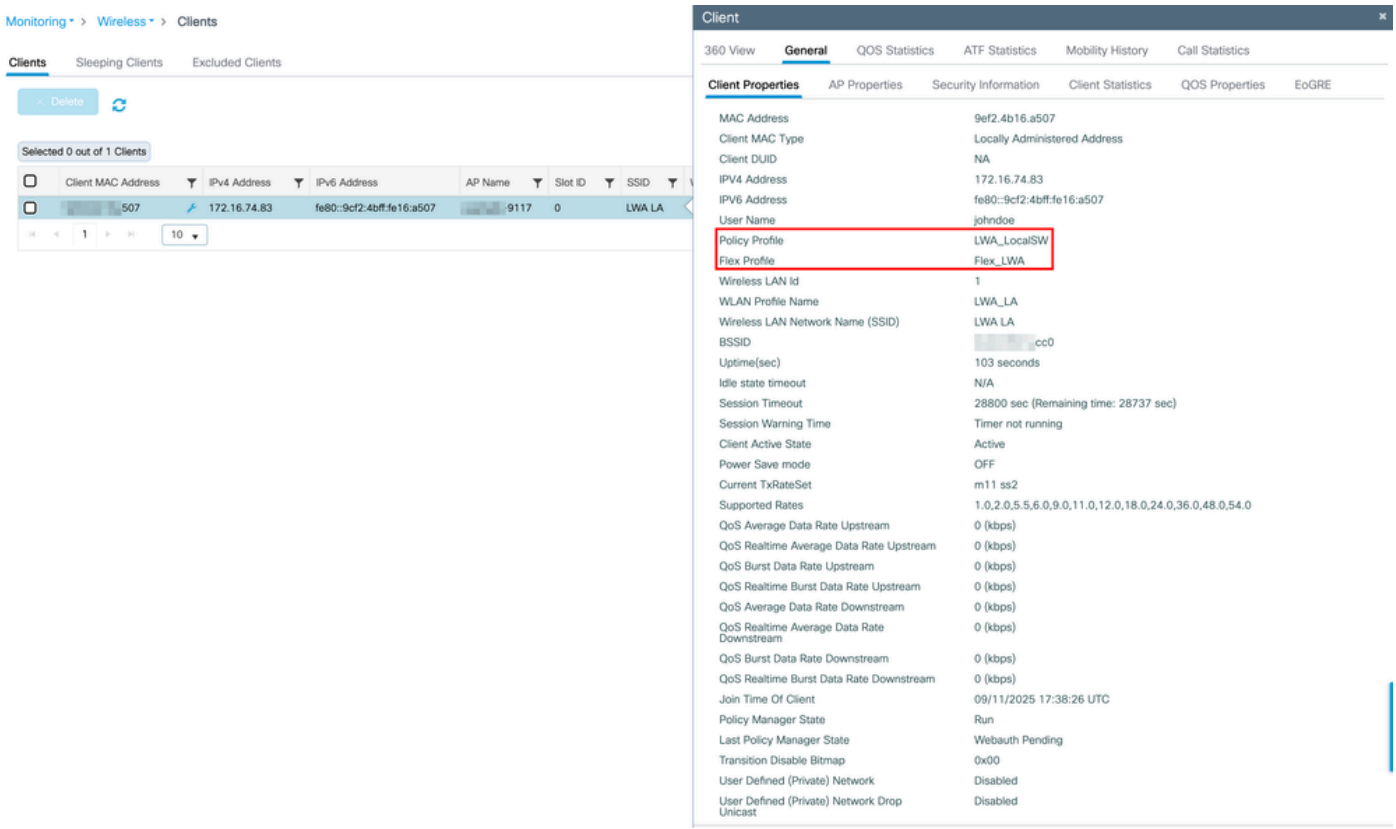
WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED



疑難排解

「Web Auth Pending」狀態表示使用者端已與存取點建立關聯，但尚未完成Web驗證程式。在此狀態期間，控制器會攔截使用者端HTTP流量，並將其重新導向到Web驗證入口網站，以便使用者登入或接受條款。在成功完成Web身份驗證之前，客戶端將保持此狀態，之後客戶端策略管理器狀態將轉換為「運行」並授予完整網路訪問許可權。

為了直觀地看到客戶端連線的流，請驗證使用外部身份驗證配置本地Web身份驗證中的LWA流。

排解9800 WLC上的LWA的常見問題描述了客戶端從客戶端角度所經歷的各個階段。

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。