設定Mac過濾器失敗時的Web Auth驗證和疑難排解

目錄

簡介

本文檔介紹如何使用ISE進行外部身份驗證配置、排除和驗證「Mac過濾器故障」功能上的本地Web身份驗證。

必要條件

配置ISE進行MAC身份驗證

在ISE/Active Directory上配置的有效使用者憑據

需求

思科建議您瞭解以下主題：

基本瞭解如何在控制器Web UI中導航

策略、WLAN配置檔案和策略標籤配置

ISE上的服務策略配置

採用元件

9800 WLC版本17.12.2

C9120 AXI AP

9300交換器

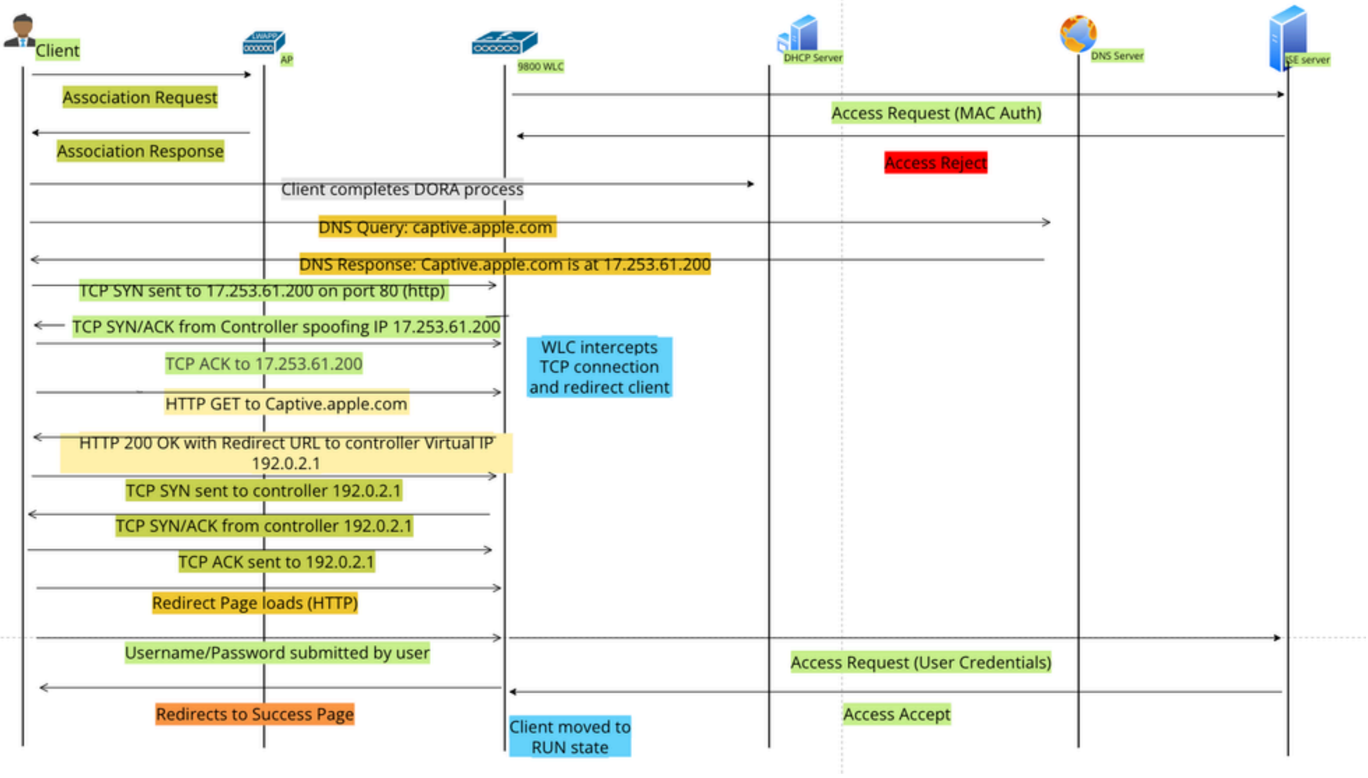
ISE版本3.1.0.518

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

Web Auth「On Mac Failure Filter」功能在同時使用MAC驗證和Web驗證的WLAN環境中充當後援機制。

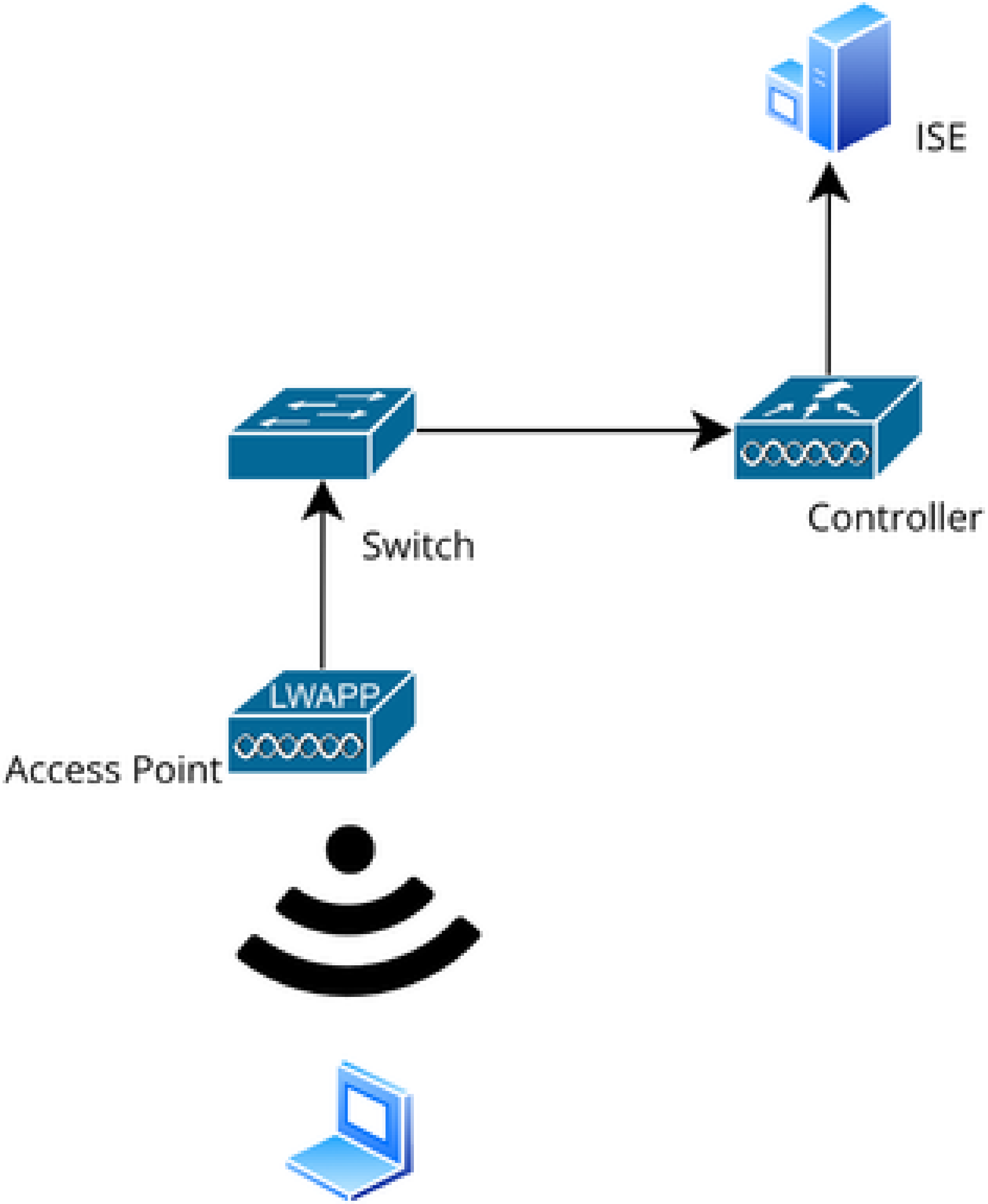
- 後退機制：當客戶端嘗試透過外部RADIUS伺服器(ISE)或本地伺服器使用MAC過濾器連線到WLAN且未能進行身份驗證時，此功能會自動啟動第3層Web身份驗證。
- 身份驗證成功：如果客戶端透過MAC過濾器成功進行身份驗證，則會繞過Web身份驗證，從而允許客戶端直接連線到WLAN。
- 避免取消關聯：此功能有助於防止因MAC過濾器身份驗證失敗而導致取消關聯。


Client
LWAPP
AP
9800 WLC
DHCP Server
DNS Server
ISE server
Association Request
Association Response
Access Request (MAC Auth)
Access Reject
Client completes DORA process
DNS Query: captive.apple.com
DNS Response: Captive.apple.com is at 17.253.61.200
TCP SYN sent to 17.253.61.200 on port 80 (http)
TCP SYN/ACK from Controller spoofing IP 17.253.61.200
WLC intercepts TCP connection and redirect client
TCP ACK to 17.253.61.200
HTTP GET to Captive.apple.com
HTTP 200 OK with Redirect URL to controller Virtual IP 192.0.2.1
TCP SYN sent to controller 192.0.2.1
TCP SYN/ACK from controller 192.0.2.1
TCP ACK sent to 192.0.2.1
Redirect Page loads (HTTP)
Username/Password submitted by user
Access Request (User Credentials)
Redirects to Success Page
Access Accept
Client moved to RUN state

Web身份驗證流程

設定

網路圖表



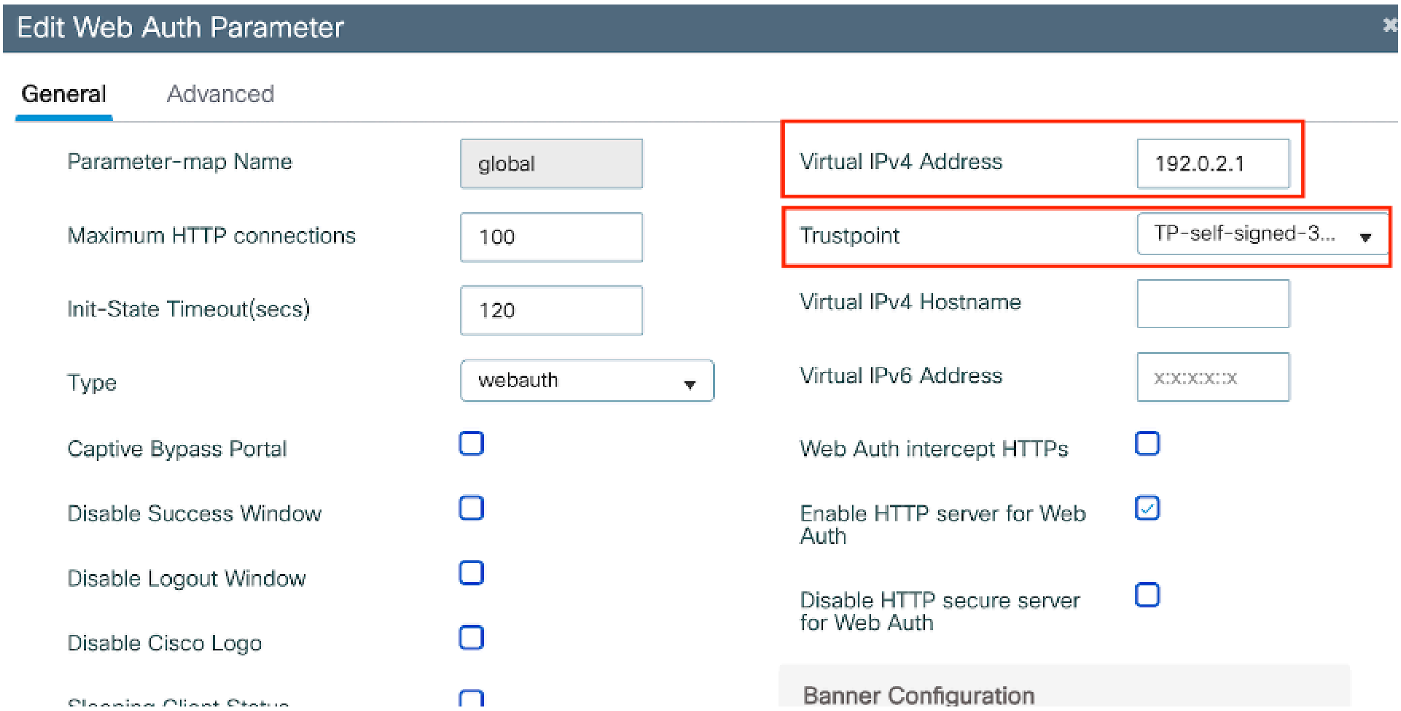
網路拓撲

組態

設定Web引數

導覽至Configuration > Security > Web Auth，然後選擇Global parameter map

從全局引數對映驗證虛擬IP和信任點配置。所有自定義Web Auth引數配置檔案從全局引數對映繼承虛擬IP和信任點配置。



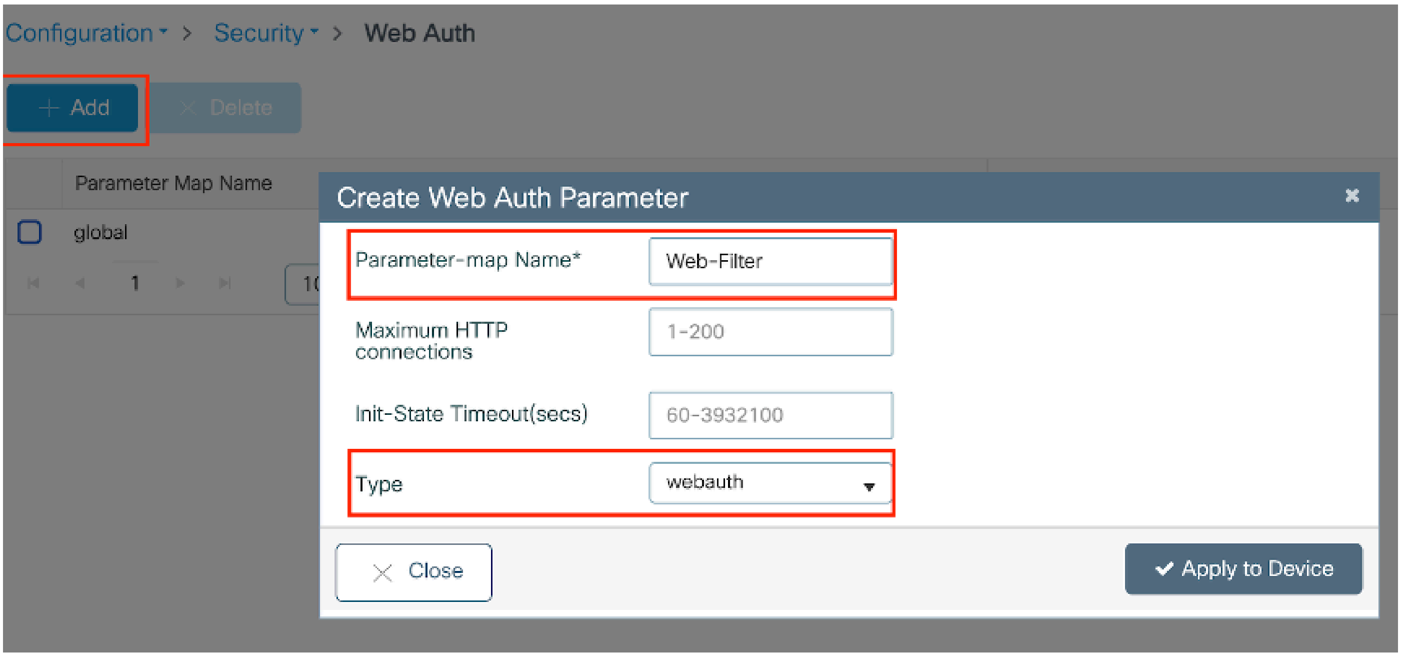
Edit Web Auth Parameter

General | Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	X:X:X:X::X
Captive Bypass Portal	□	Web Auth intercept HTTPs	□
Disable Success Window	□	Enable HTTP server for Web Auth	☑
Disable Logout Window	□	Disable HTTP secure server for Web Auth	□
Disable Cisco Logo	□	Banner Configuration	
Sleeping Client Status	□		

全域Web驗證引數設定檔

第1步：選擇「增加」建立自定義Web身份驗證引數對映。輸入設定檔名稱，然後選擇「Webauth」作為「Type」。



Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth

Web Auth引數配置檔案

如果您的客戶端也獲得IPv6地址，您還必須在引數對映中增加虛擬IPv6地址。使用文檔範圍2001：db8：：/32中的IP

如果您的使用者端取得IPv6位址，他們很有可能會嘗試在V6而不是V4中取得HTTP Web驗證重新導向，因此您也需要設定虛擬IPv6。

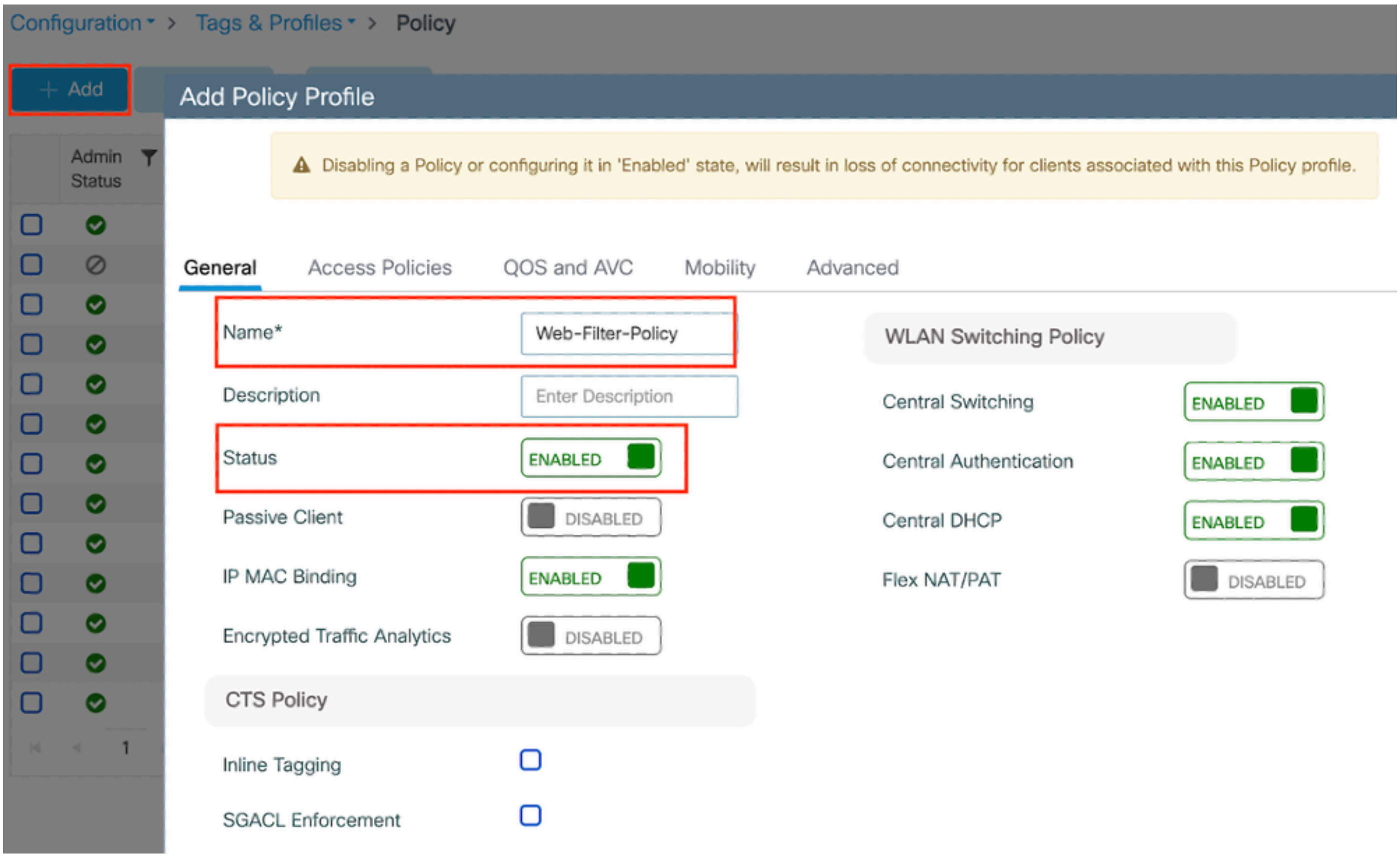
CLI配置：

```
parameter-map type webauth Web-Filter
 type webauth
```

配置策略配置檔案

第1步：建立策略配置檔案

導航到Configuration > Tags & Profiles > Policy。選取「新增」。在「一般」標籤中，指定設定檔名稱並啟用狀態切換。



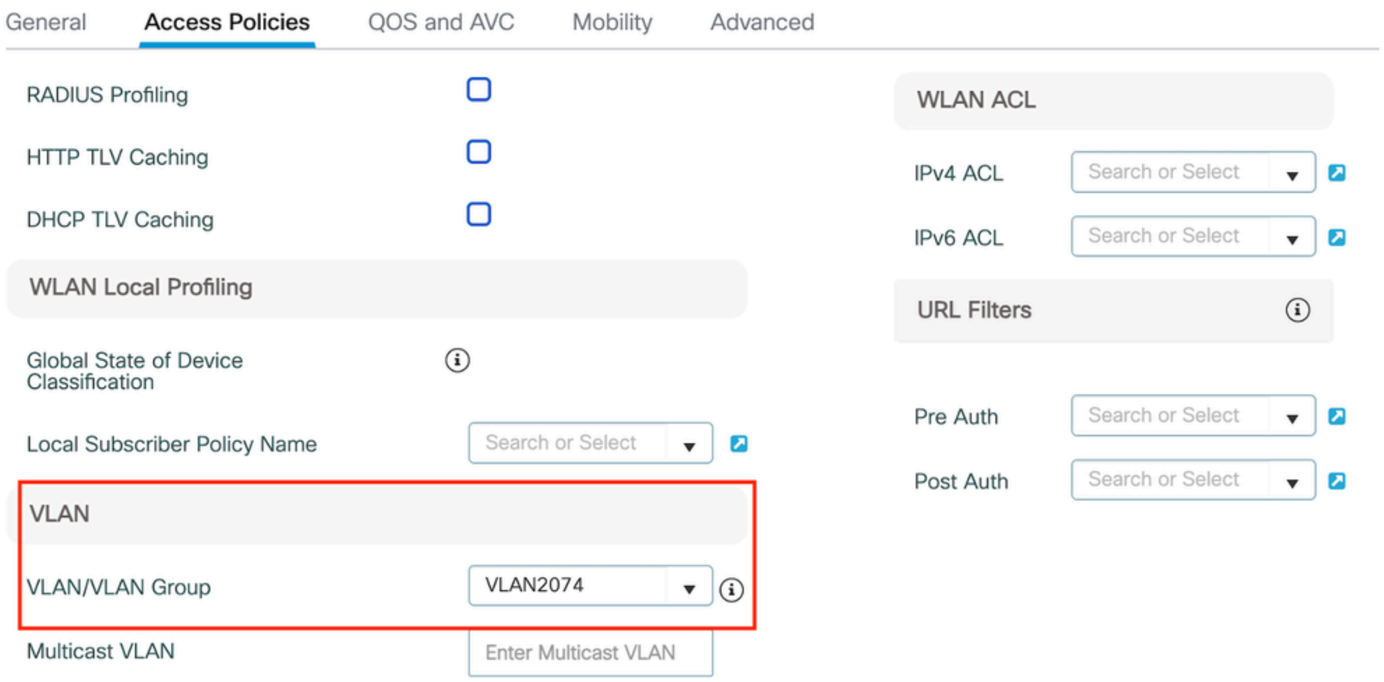
Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*	Web-Filter-Policy
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
IP MAC Binding	ENABLED
Encrypted Traffic Analytics	DISABLED
Inline Tagging	□
SGACL Enforcement	□
Central Switching	ENABLED
Central Authentication	ENABLED
Central DHCP	ENABLED
Flex NAT/PAT	DISABLED

策略配置檔案

步驟2：

在Access Policies頁籤下，從VLAN部分下拉選單中選擇客戶端VLAN。



RADIUS Profiling □

HTTP TLV Caching □

DHCP TLV Caching □

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: VLAN2074 ⓘ

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

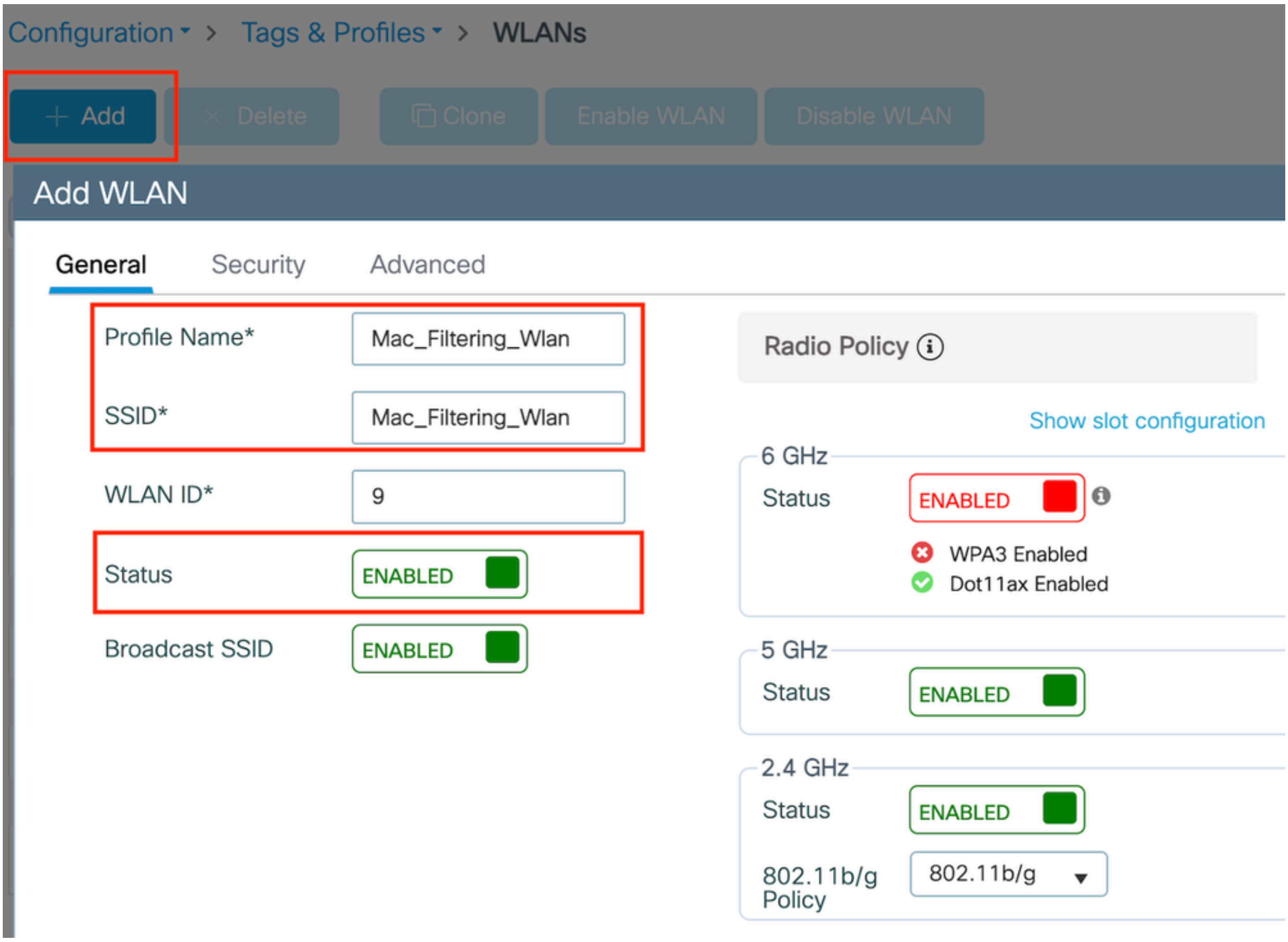
訪問策略頁籤

CLI配置：

```
wireless profile policy Web-Filter-Policy
 vlan VLAN2074
 no shutdown
```

配置WLAN配置檔案

第1步：導航到Configuration > Tags and Profiles > WLANs。選取「新增」以建立新設定檔。定義配置檔名稱和SSID名稱，並啟用狀態欄位。



Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status ENABLED

☒ WPA3 Enabled

✓ Dot11ax Enabled

5 GHz

Status ENABLED

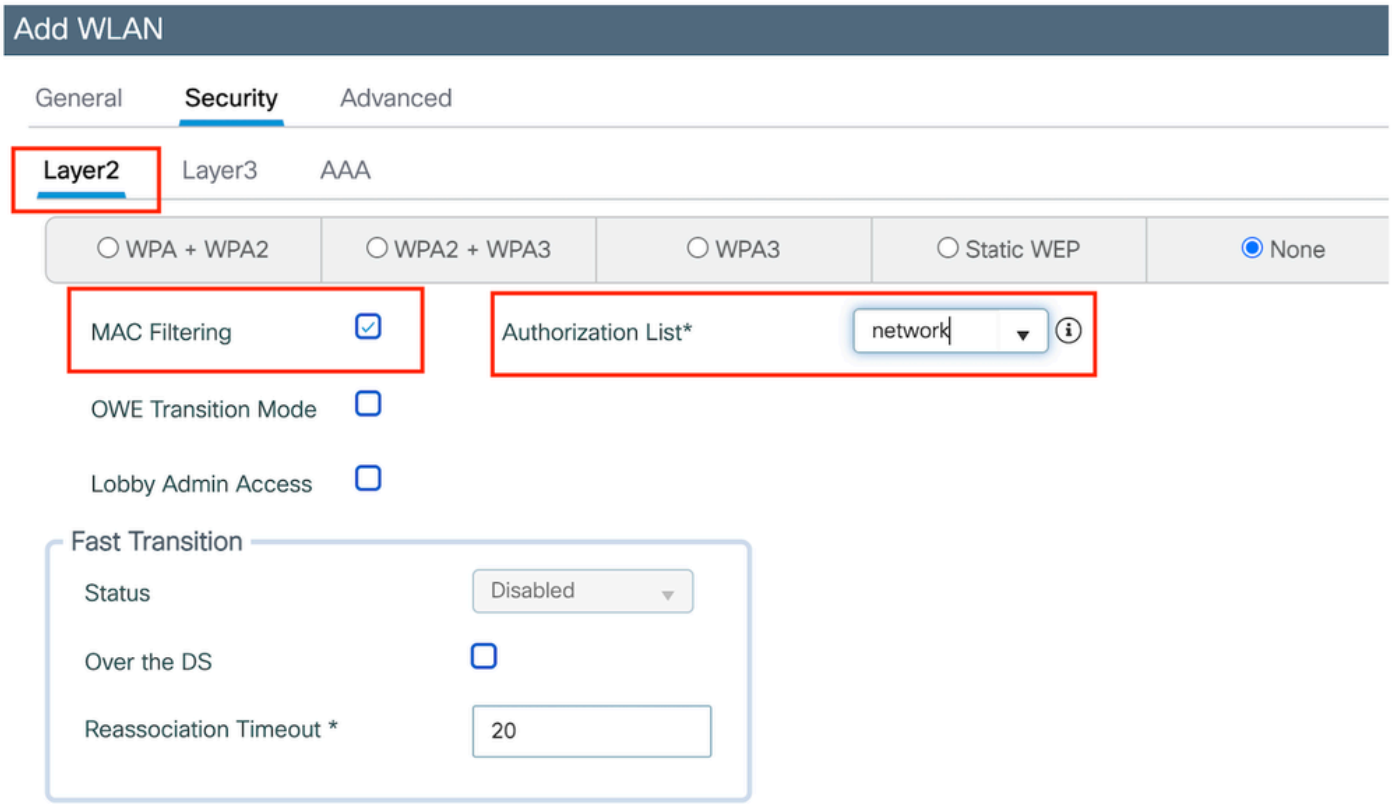
2.4 GHz

Status ENABLED

802.11b/g Policy 802.11b/g

WLAN配置檔案

第2步：在Security頁籤下，啟用「Mac Filtering」覈取方塊，並在授權清單中配置RADIUS伺服器（ISE或本地伺服器）。此設定使用ISE進行Mac身份驗證和Web身份驗證。



○ WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ● None

MAC Filtering ☑

Authorization List* network

OWE Transition Mode □

Lobby Admin Access □

Fast Transition

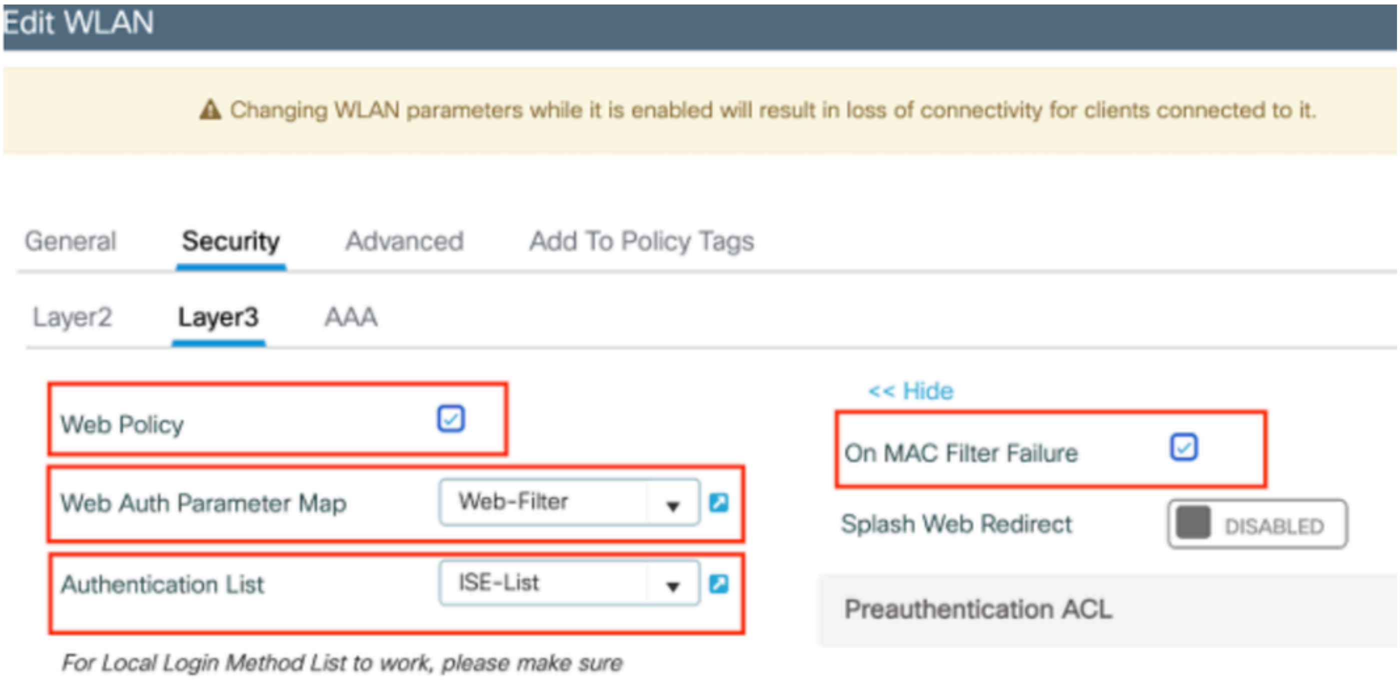
Status Disabled

Over the DS □

Reassociation Timeout * 20

WLAN第2層安全性

第3步：導航到安全>第3層。啟用Web策略並將其與Web身份驗證引數對映配置檔案關聯。選中「On Mac Filter Failure」覈取方塊，然後從Authentication清單中選擇RADIUS伺服器。



⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Web Policy ☑

Web Auth Parameter Map Web-Filter

Authentication List ISE-List

For Local Login Method List to work, please make sure

On MAC Filter Failure ☑

Splash Web Redirect DISABLED

Preauthentication ACL

WLAN Layer3 security頁籤

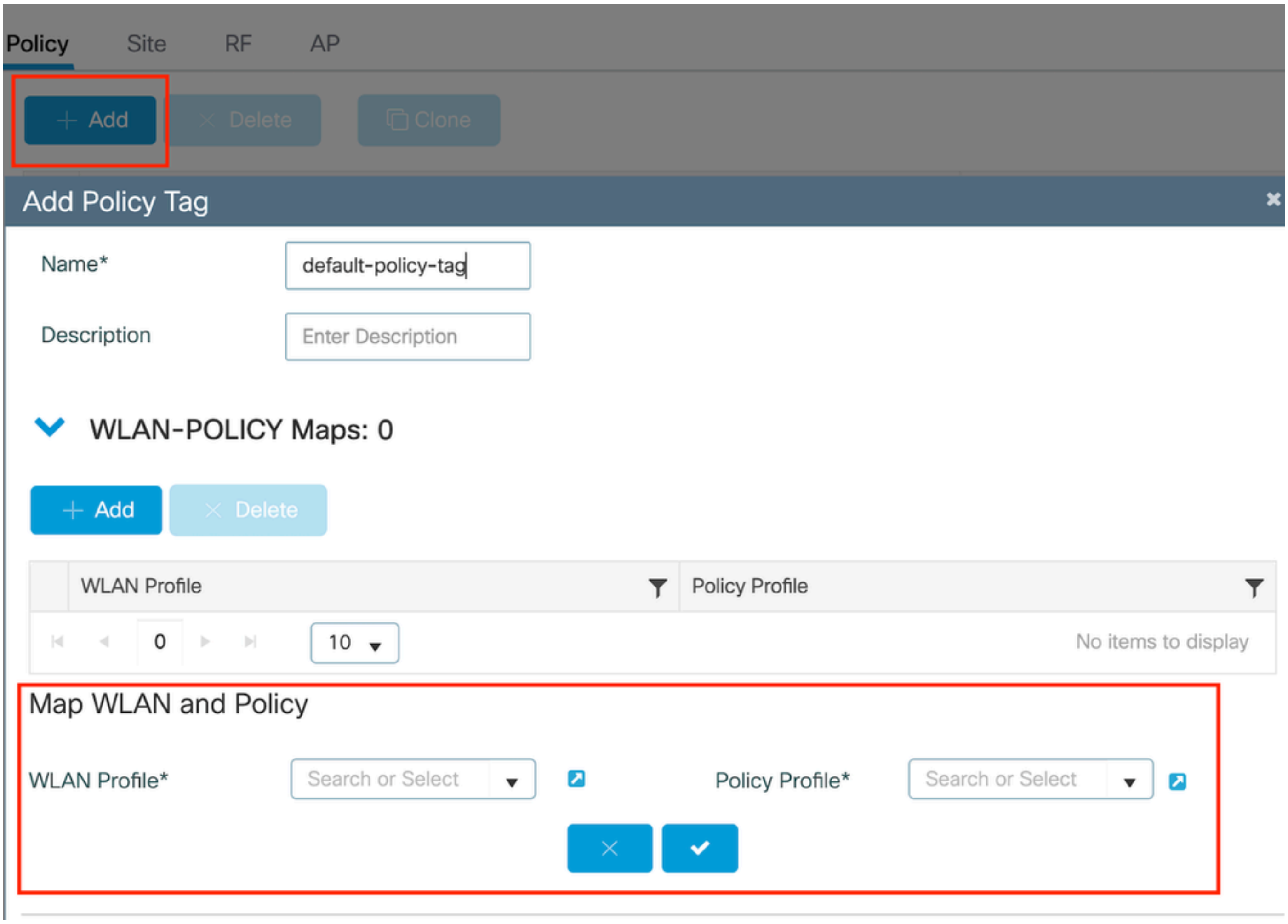
CLI配置

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
```

```
 mac-filtering network
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list ISE-List
 security web-auth on-macfilter-failure
 security web-auth parameter-map Web-Filter
 no shutdown
```

第4步：配置策略標籤、建立WLAN配置檔案和策略配置檔案對映

導航到Configuration > Tags & Profiles > Tags > Policy。按一下「增加」以定義策略標籤的名稱。在WLAN-Policy Maps下，選擇Add以對映之前建立的WLAN和策略配置檔案。



Name*: default-policy-tag

Description: Enter Description

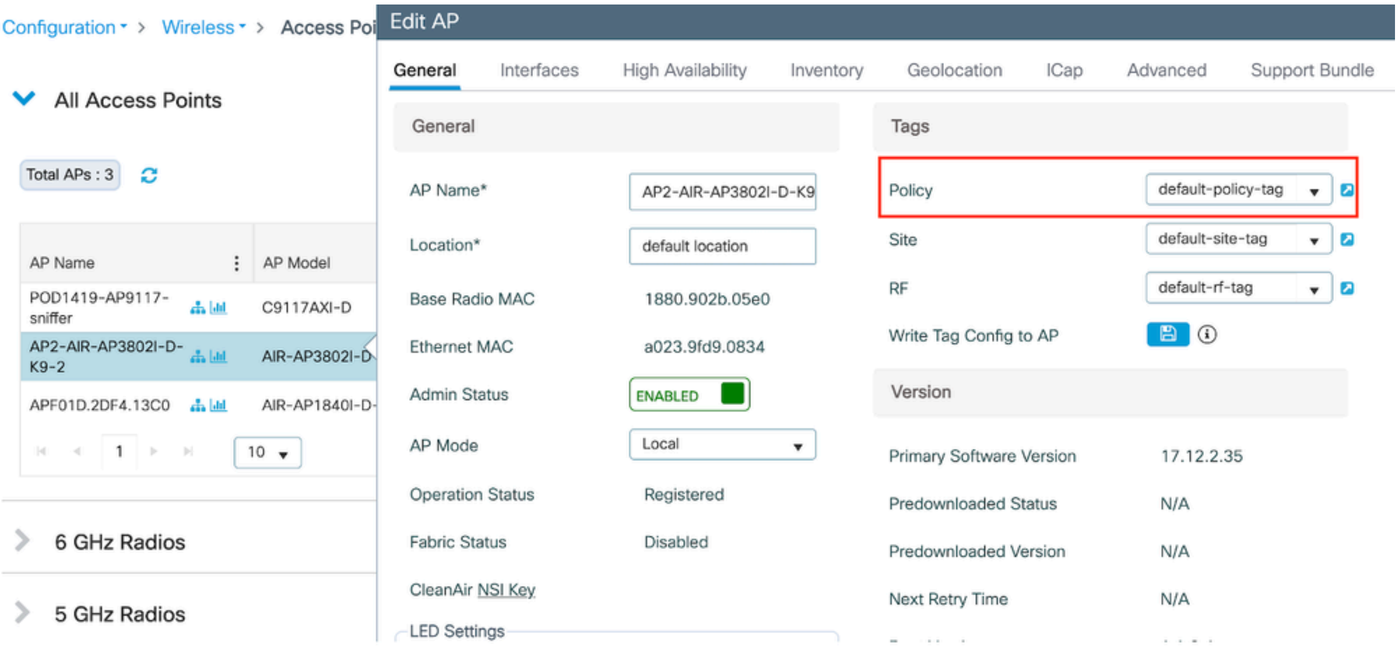
策略標籤對映

CLI配置：

```
wireless tag policy default-policy-tag
 description "default policy-tag"
```

```
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

第5步：導航到配置(Configuration) >無線(Wireless) >存取點(Access Point)。選擇負責廣播此SSID的存取點。在Edit AP選單中，分配建立的策略標籤。



Configuration > Wireless > Access Poi

All Access Points

Total APs : 3

AP Name		AP Model
POD1419-AP9117-sniffer		C9117AXI-D
AP2-AIR-AP3802I-D-K9-2		AIR-AP3802I-D
APF01D.2DF4.13C0		AIR-AP1840I-D-

6 GHz Radios

5 GHz Radios

Edit AP

General | Interfaces | High Availability | Inventory | Geolocation | ICap | Advanced | Support Bundle

General

AP Name*	AP2-AIR-AP3802I-D-K9
Location*	default location
Base Radio MAC	1880.902b.05e0
Ethernet MAC	a023.9fd9.0834
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
CleanAir NSI Key	

LED Settings

Tags

Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	

Version

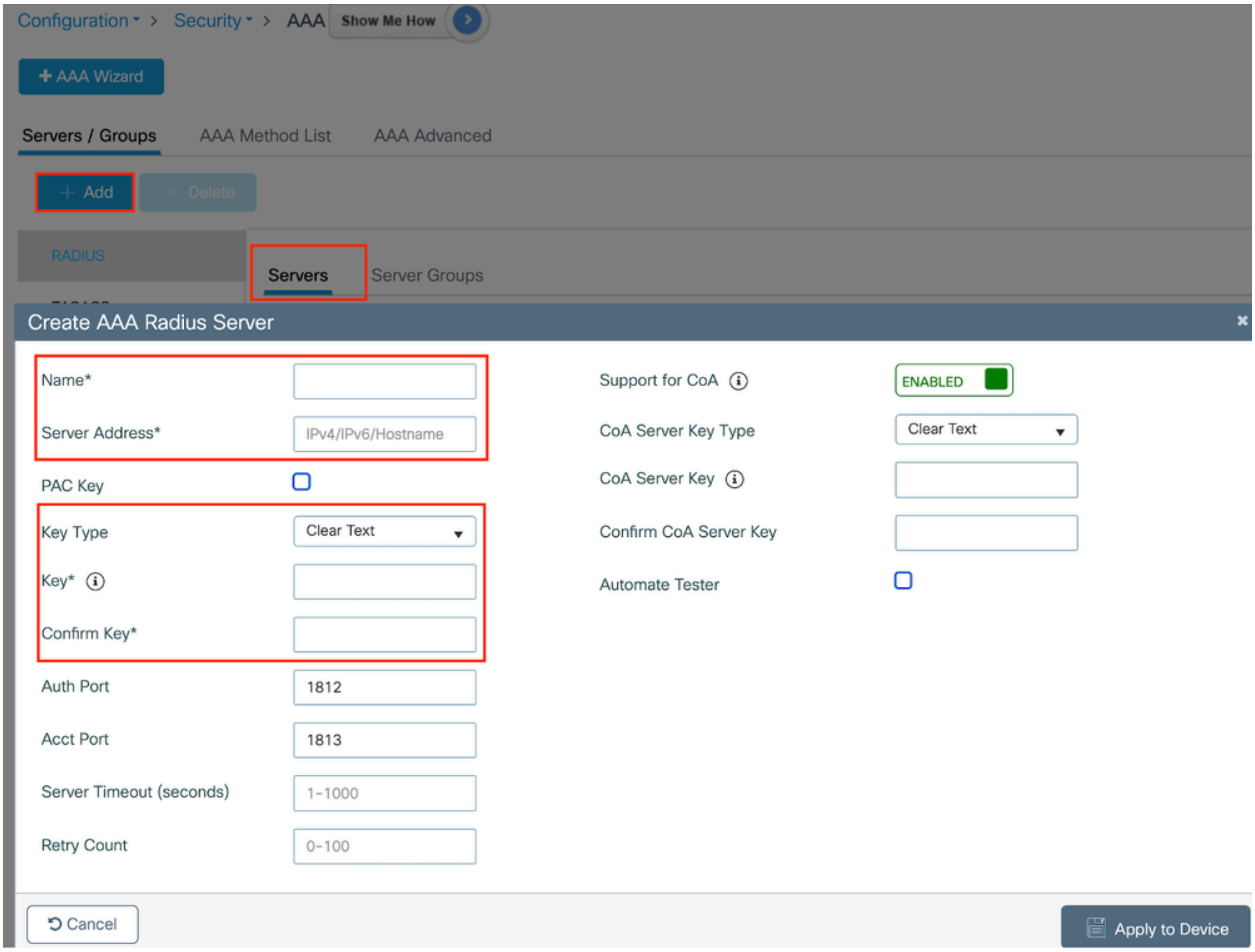
Primary Software Version	17.12.2.35
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A

將策略標籤對映到AP

配置AAA設定：

步驟1：建立Radius伺服器：

導航到Configuration > Security > AAA。按一下「伺服器/群組」段落下的「新增」選項。在「建立AAA Radius伺服器」頁上，輸入伺服器名稱、IP地址和共用金鑰。



Create AAA Radius Server

Name*

Server Address* IPv4/IPv6/Hostname

PAC Key □

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

CoA Server Key Type Clear Text

CoA Server Key

Confirm CoA Server Key

Automate Tester □

伺服器配置

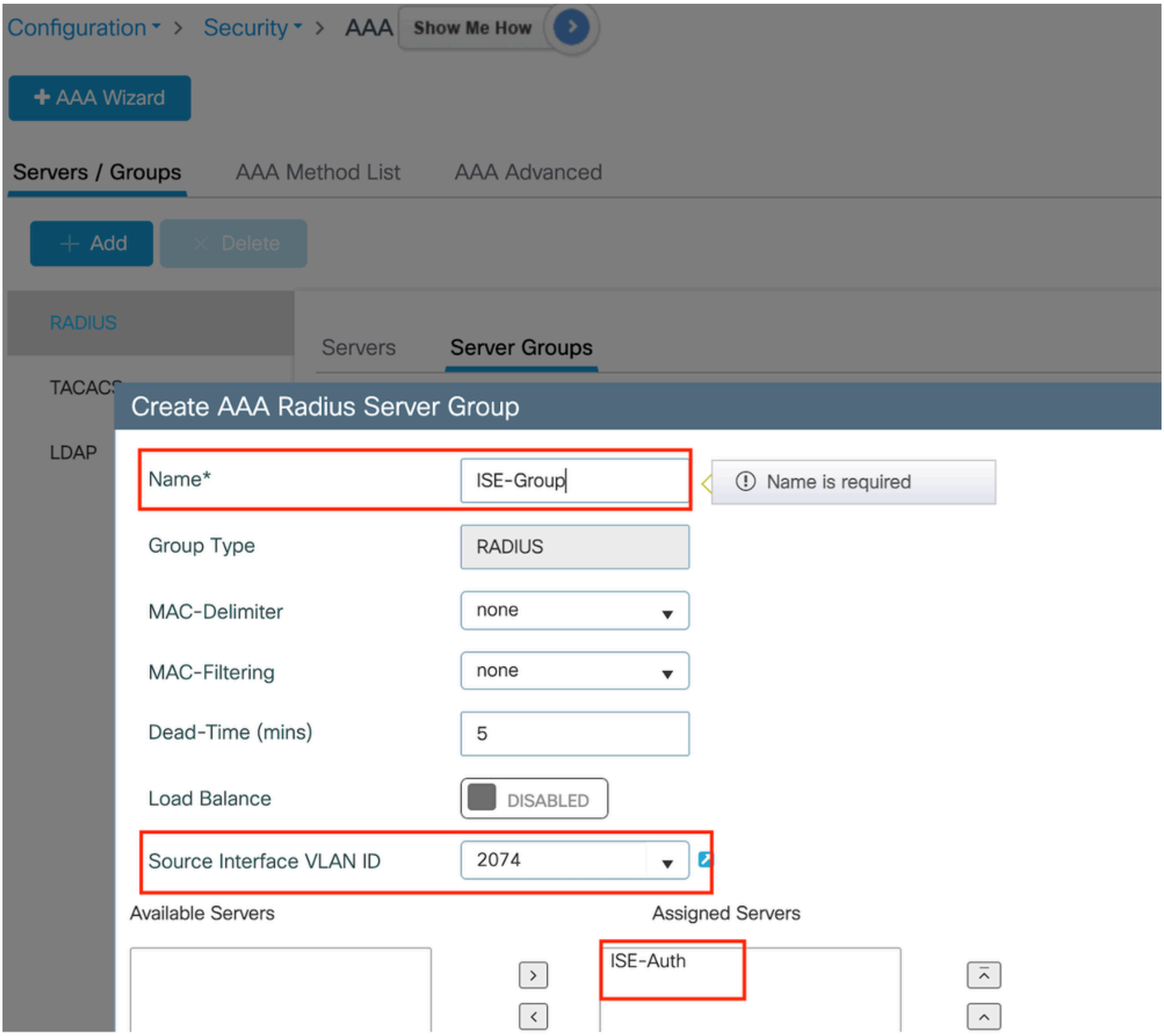
CLI配置

```
radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key *****
 server name ISE-Auth
```

步驟2：建立Radius伺服器群組：

選取「伺服器群組」段落底下的「新增」選項，以定義伺服器群組。切換要包含在相同群組組態中的伺服器。

無需設定源介面。預設情況下，9800使用其路由表來確定用於連線RADIUS伺服器的介面，並且通常使用預設網關。



Create AAA Radius Server Group

Name*	ISE-Group
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Load Balance	DISABLED
Source Interface VLAN ID	2074

Name is required

Available Servers

Assigned Servers

ISE-Auth

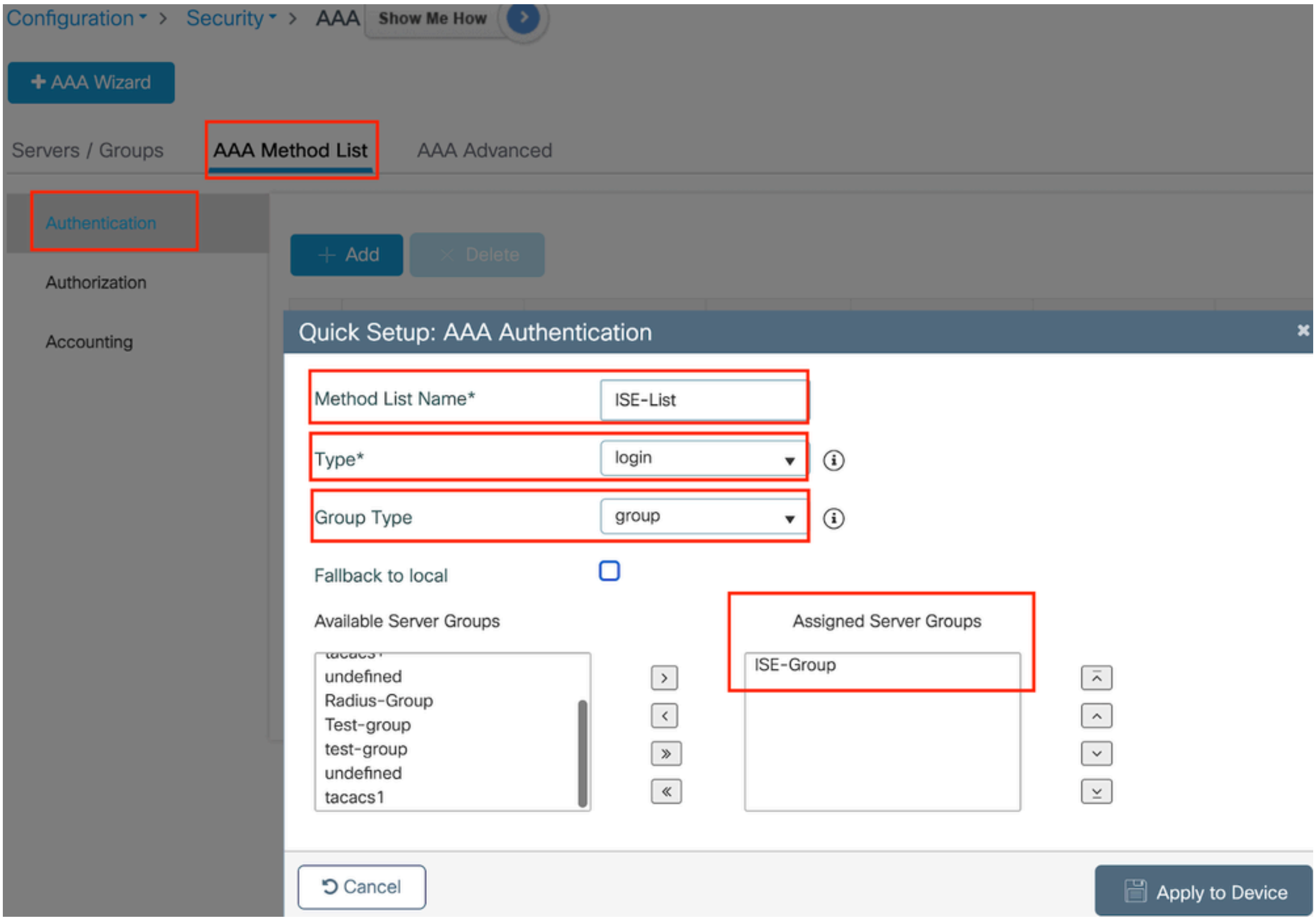
伺服器組

CLI配置

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2074
 deadtime 5
```

第3步：配置AAA方法清單：

導航到AAA Method List頁籤。在「身份驗證」下，按一下「增加」。定義方法清單名稱，將「型別」定義為「登入」，將「群組」型別定義為「群組」。在Assigned Server Group部分下對映配置的身份驗證伺服器組。



Method List Name* ISE-List

Type* login

Group Type group

Fallback to local □

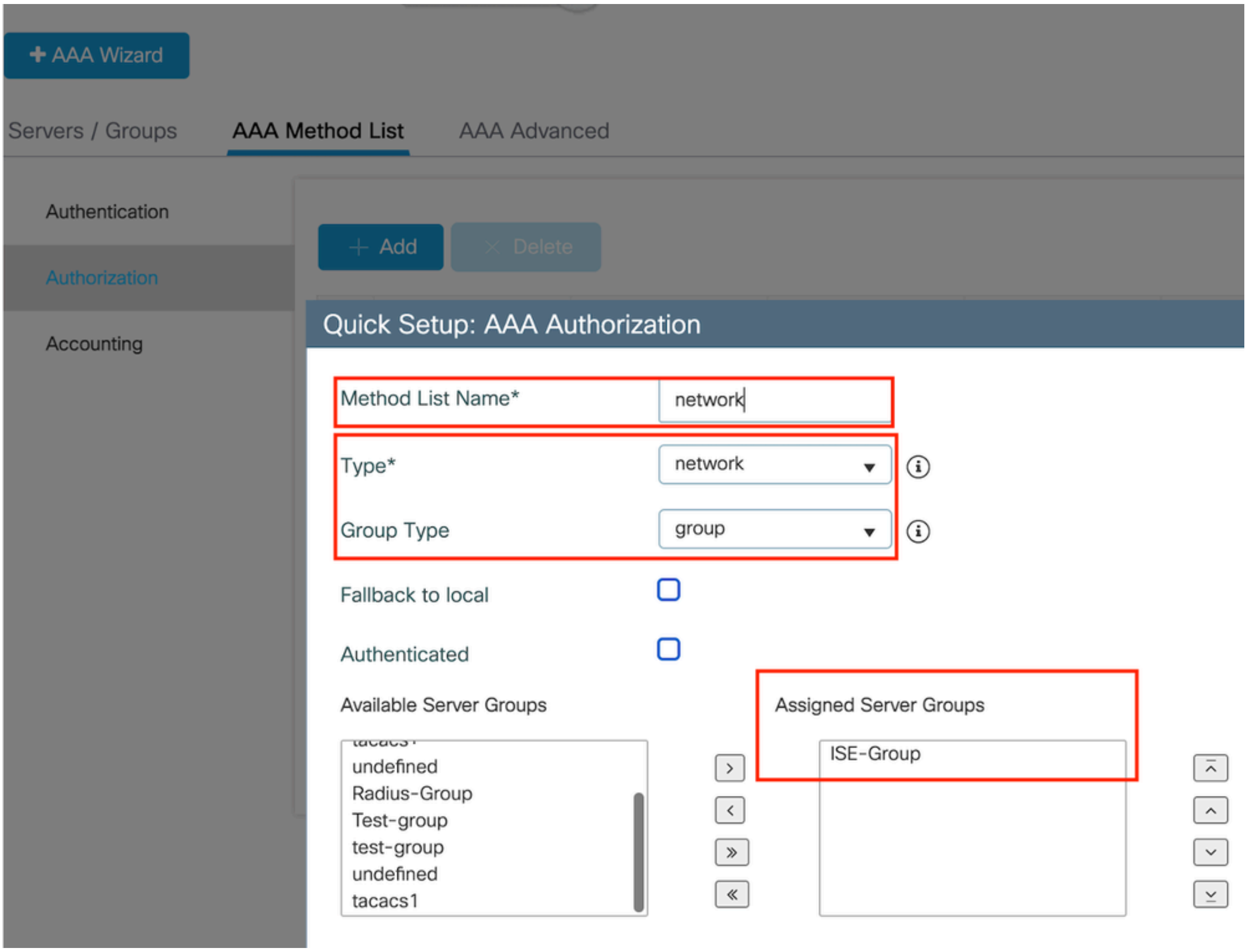
Assigned Server Groups: ISE-Group

驗證方法清單

CLI配置

```
aaa authentication login ISE-List group ISE-Group
```

導航到Authorization Method List部分，然後點選Add。定義方法清單名稱，並將型別設定為「網路」，將群組型別設定為「群組」。將配置的RADIUS伺服器切換到Assigned Server Groups部分。



Method List Name* network

Type* network

Group Type group

Fallback to local □

Authenticated □

Available Server Groups: tacacs+, undefined, Radius-Group, Test-group, test-group, undefined, tacacs1

Assigned Server Groups: ISE-Group

授權方法清單

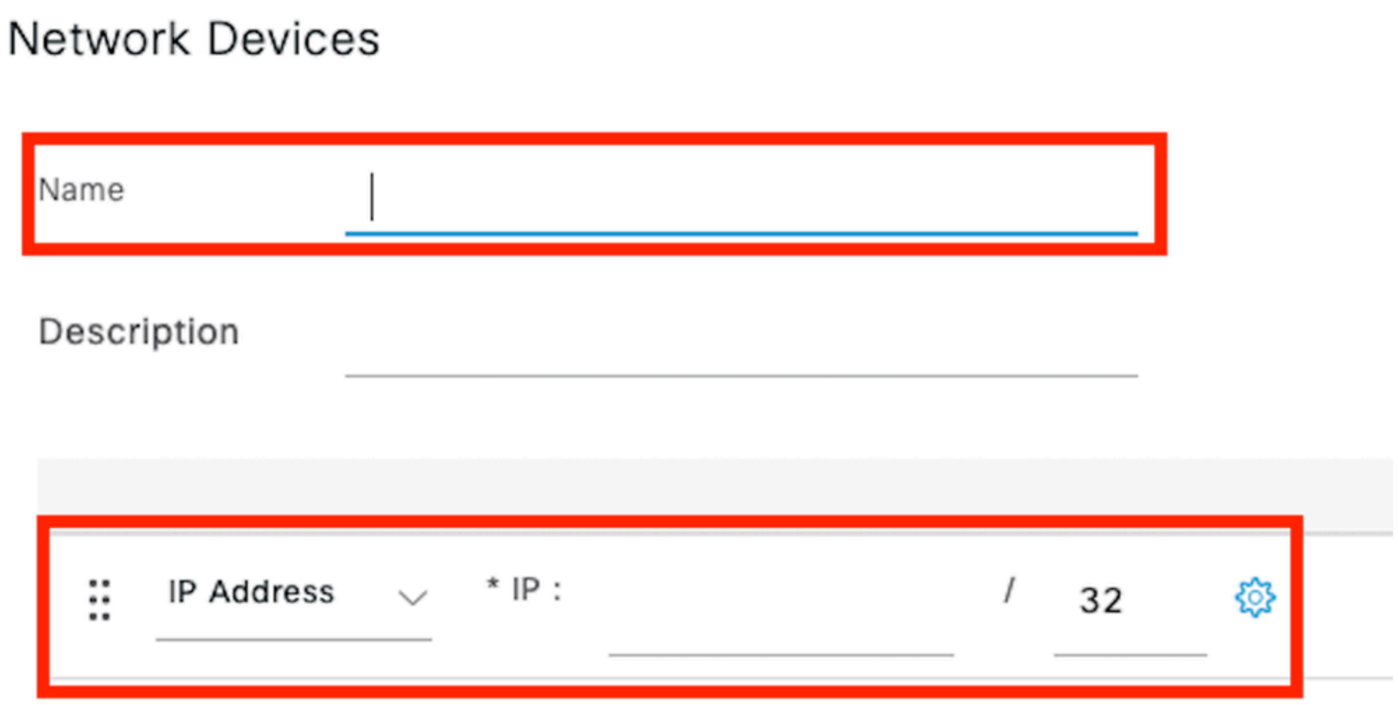
CLI配置

```
aaa authorization network network group ISE-Group
```

ISE 組態:

在ISE上增加WLC作為網路裝置

第1步：導航到管理(Administration) >網路裝置(Network Devices)，然後點選增加(Add)。在Radius Authentication Settings下輸入控制器IP地址、主機名和共用金鑰



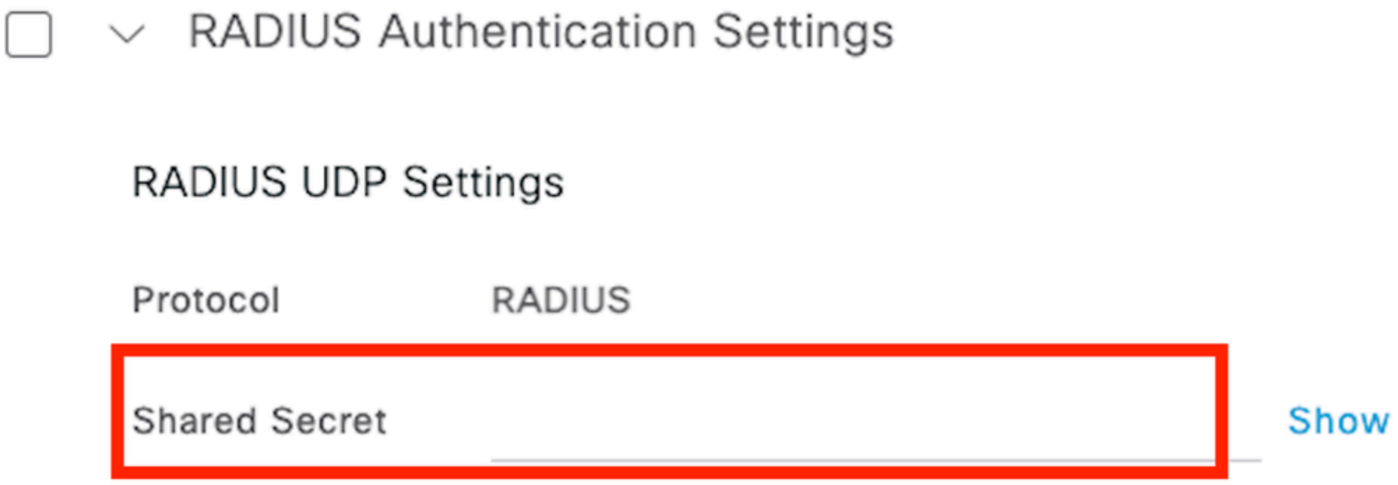
Network Devices

Name

Description

IP Address * IP : / 32

增加網路裝置



☐ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

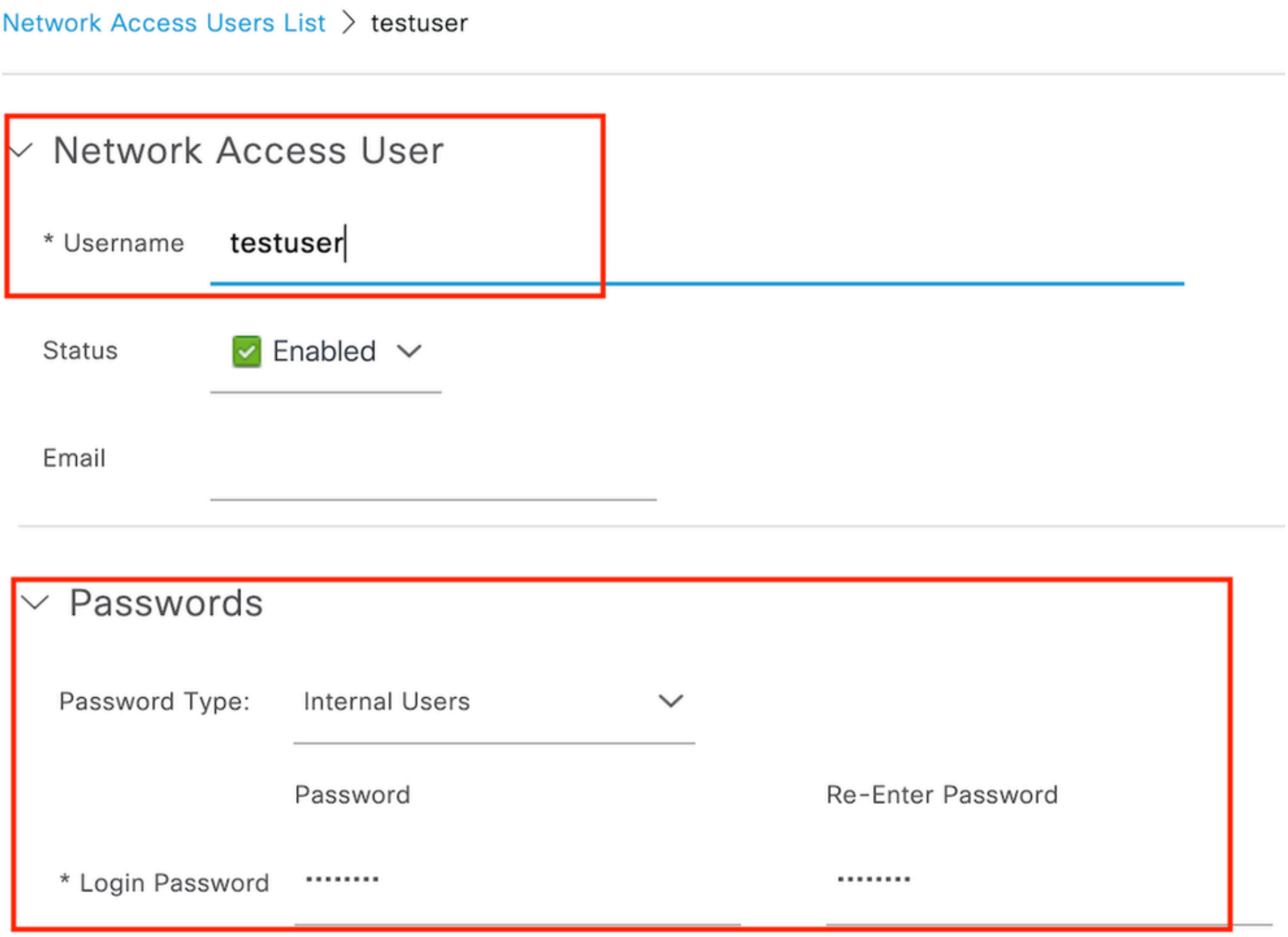
Shared Secret

共用金鑰

步驟2：建立使用者專案

在Identity Management > Identities下，選擇Add選項。

配置客戶端必須用於Web身份驗證的使用者名稱和口令



Network Access Users List > testuser

Network Access User

* Username testuser

Status ☑ Enabled

Email

Passwords

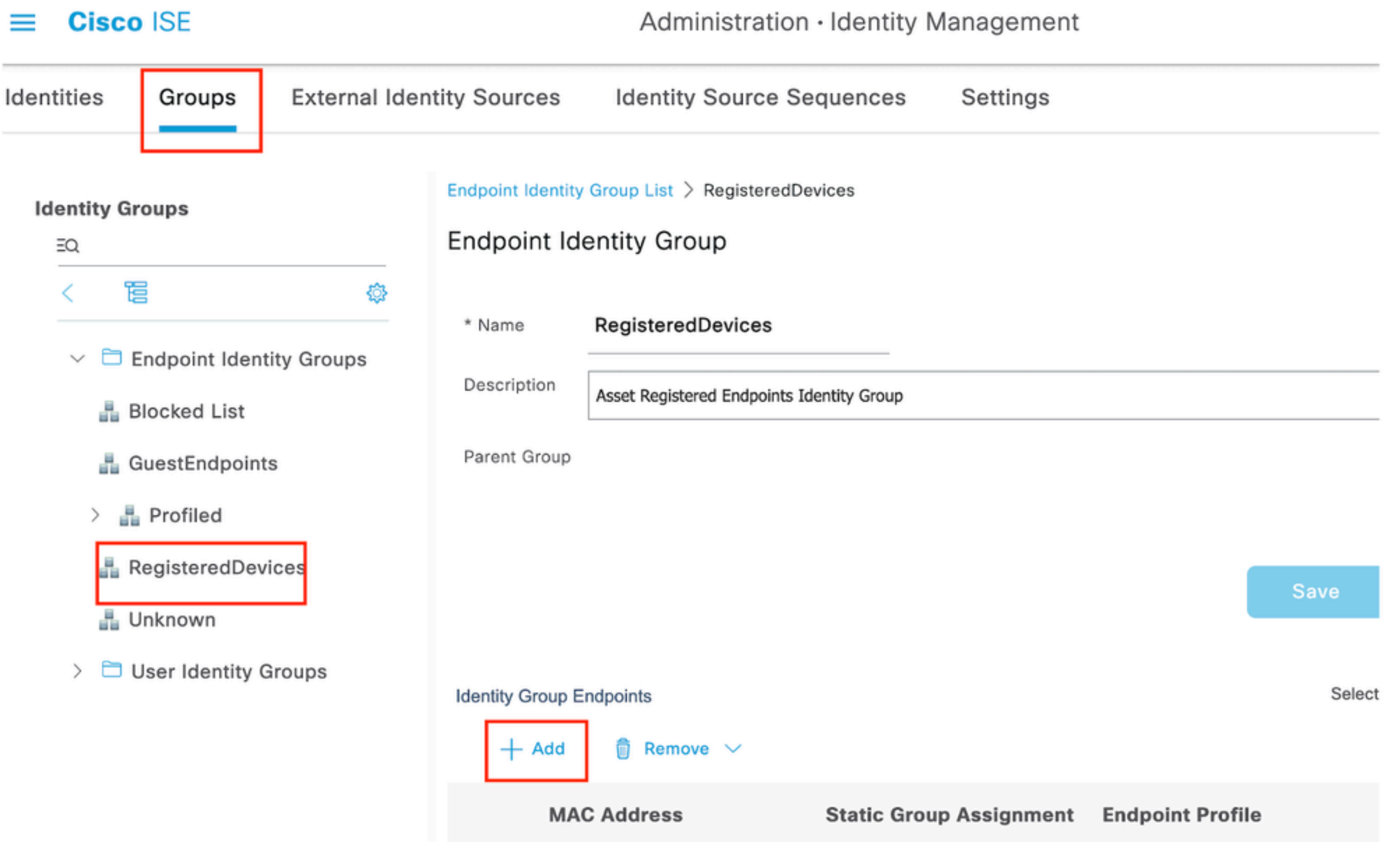
Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	·········	·········

增加使用者憑據

第3步：導航到管理(Administration) >身份管理(Identity Management) >組(Groups) >已註冊裝置(Registered Devices)，然後點選增加(Add)。

輸入裝置mac地址以在伺服器上建立條目。



* Name: RegisteredDevices

Description: Asset Registered Endpoints Identity Group

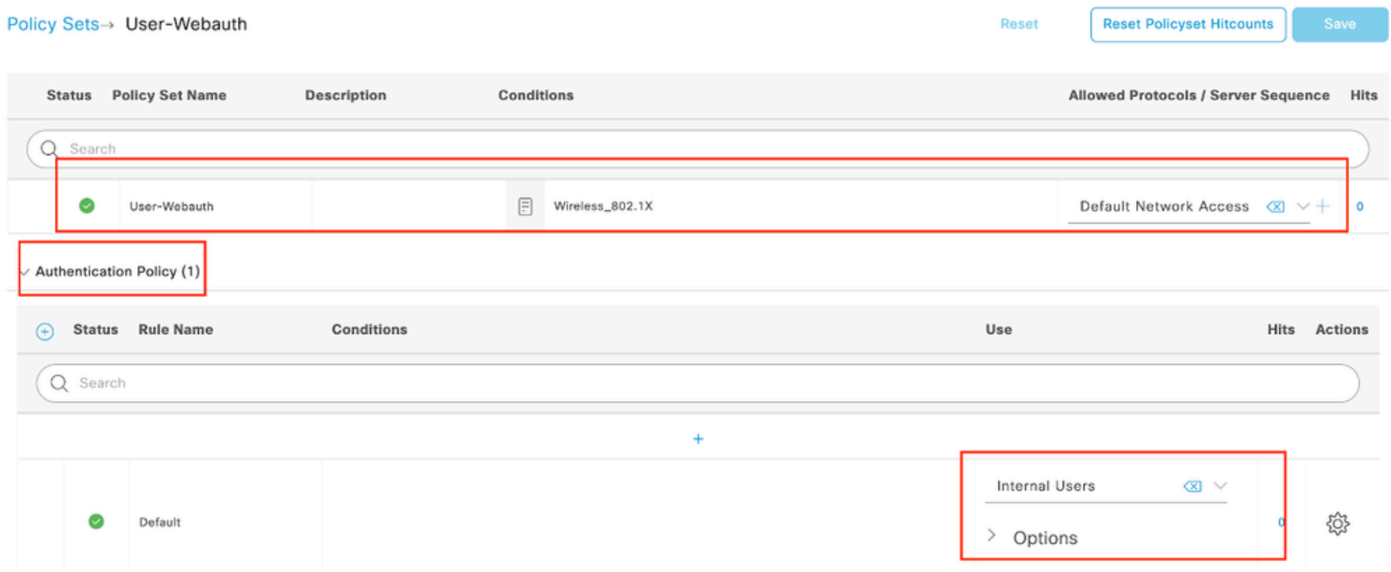
Parent Group

增加裝置MAC地址

第4步：建立服務策略

導航到Policy > Policy sets，然後選擇「+」號建立新策略集

此策略集用於使用者Web身份驗證，其中客戶端的使用者名稱和密碼在「身份管理」中建立

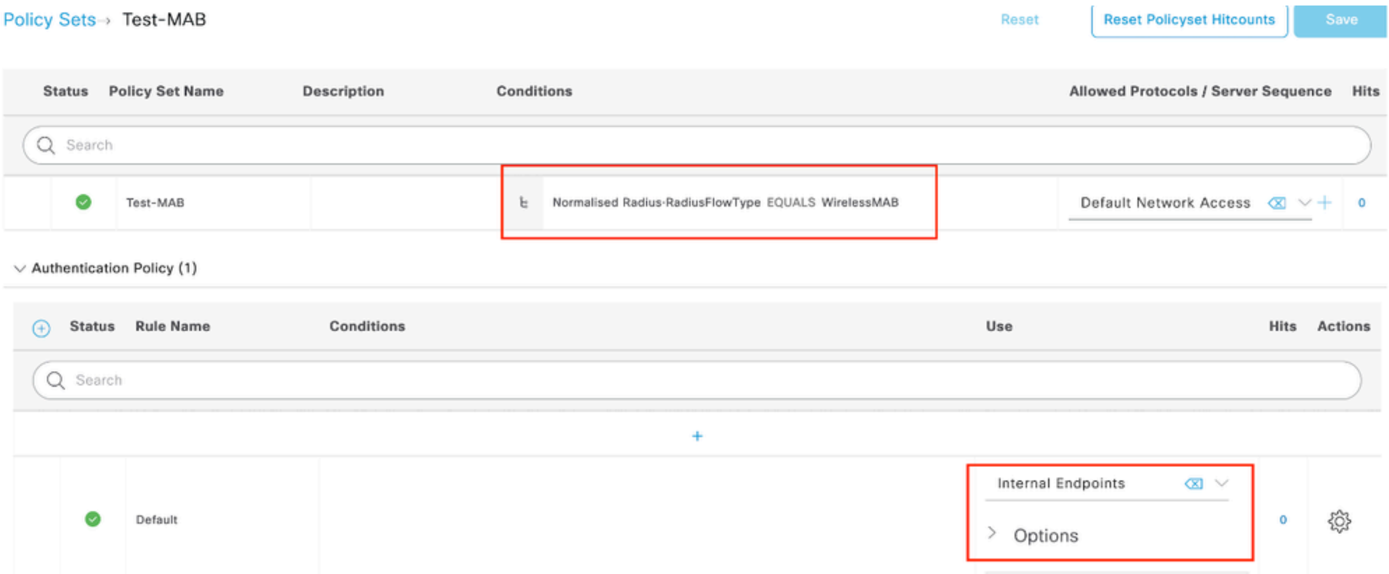

Policy Sets→ User-Webauth
Reset
Reset Policyset Hitcounts
Save
Search
Authentication Policy (1)
Search
+
Options

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	0	⚙

Web身份驗證服務策略

同樣，建立MAB服務策略並在身份驗證策略下對映內部終端。



Policy Sets → Test-MAB

Reset | Reset Policyset Hitcounts | Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Test-MAB		Normalised Radius·RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)

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

MAB身份驗證服務策略

驗證

控制器配置

<#root>

```
show wireless tag policy detailed

default-policy-tag

Policy Tag Name : default-policy-tag
Description     : default policy-tag
Number of WLAN-POLICY maps: 1
WLAN Profile Name                  Policy Name
------------------------------------------------------------------------

Mac_Filtering_Wlan


Web-Filter-Policy
```

<#root>

```
show wireless profile policy detailed

Web-Filter-Policy


Policy Profile Name                 :

Web-Filter-Policy

Description                         :
```

```
Status                              :
```

ENABLED

```
VLAN                                :
```

2074

```
Multicast VLAN                      : 0
```

<#root>

```
show wlan name
```

Mac_Filtering_Wlan

```
WLAN Profile Name     :
```

Mac_Filtering_Wlan

```
================================================
Identifier                                     : 9
Description                                    :
Network Name (SSID)                            :
```

Mac_Filtering_Wlan

```
Status                                         :
```

Enabled

```
Broadcast SSID                                 :
```

Enabled

```
Mac Filter Authorization list name             :
```

network

```
Webauth On-mac-filter Failure              :
```

Enabled

```
    Webauth Authentication List Name           :
```

ISE-List

```
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      :
```

Web-Filter

<#root>

```
show parameter-map type webauth name Web-Filter
Parameter Map Name                :
```

Web-Filter

```
  Type                            :
```

webauth

```
  Auth-proxy Init State time     : 120 sec
  Webauth max-http connection    : 100
  Webauth logout-window          :
```

Enabled

```
  Webauth success-window         :
```

Enabled

```
  Consent Email                  : Disabled
  Activation Mode                : Replace
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```

<#root>

```
show ip http server status

HTTP server status:
```

Enabled

```
HTTP server port:
```

80

```
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:
```

Enabled

```
HTTP secure server port:
```

443

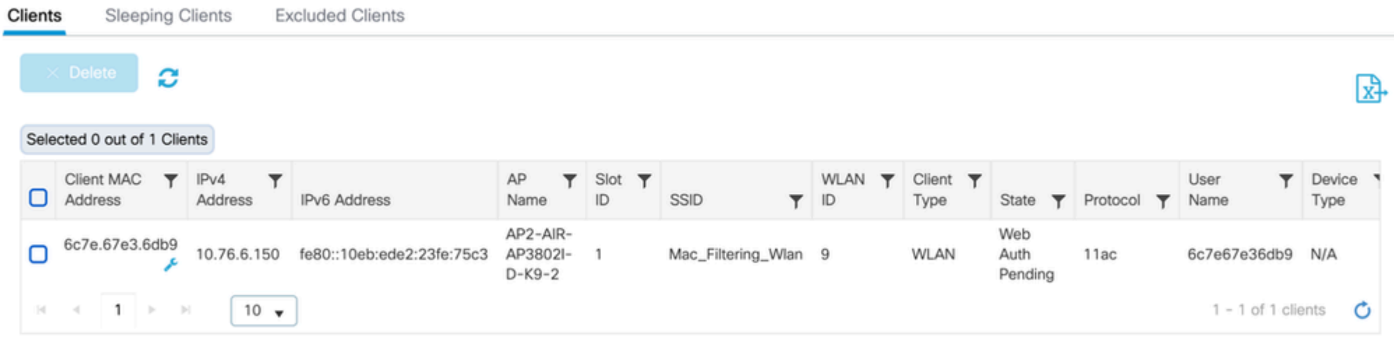
```
show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping
------------------
```

```
WLAN Profile Name                 Policy Name                       VLAN                              Flex
-------------------------------------------------------------------------------------------------------------
Mac_Filtering_Wlan                Web-Filter-Policy                 2074                              ENAB
```

控制器上的客戶端策略狀態

導航到Dashboard > Clients部分以確認連線的客戶端的狀態。
客戶端當前處於Web身份驗證掛起狀態



Clients Sleeping Clients Excluded Clients

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
□	6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

客戶端詳細資訊

```
show wireless client summary
Number of Clients: 1
MAC Address    AP Name                                      Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------------
6c7e.67e3.6db9 AP2-AIR-AP3802I-D-K9-2                       WLAN 9    Webauth Pending   11ac     Web 
```

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail
Client MAC Address :
```

6c7e.67e3.6db9

```
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.76.6.150

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
Client Username :
```

6c7e67e36db9

```
AP MAC Address : 1880.902b.05e0
AP Name: AP2-AIR-AP3802I-D-K9-2
AP slot : 1
Client State : Associated
Policy Profile :
```

Web-Filter-Policy

```
Flex Profile : N/A
```

```
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List
        Method : Web Auth
                Webauth State    :

Get Redirect

                Webauth Method   :

Webauth
```

在成功進行Web身份驗證後，客戶端策略管理器狀態將轉換為RUN

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A
```

疑難排解

MAC失敗時的Web身份驗證功能的功能依賴於控制器功能在MAB失敗時觸發Web身份驗證。我們的主要目標是從控制器中有效地收集RA跟蹤以進行故障排除和分析。

收集放射性痕跡

啟用無線電活動跟蹤以在CLI中為指定的MAC地址生成客戶端調試跟蹤。

啟用放射性追蹤的步驟：

確定所有條件式偵錯都已停用

```
clear platform condition all
```

為指定的MAC地址啟用調試

```
debug wireless mac <H.H.H> monitor-time <Time is seconds>
```

重現問題後，請停用調試以停止RA跟蹤收集。

```
no debug wireless mac <H.H.H>
```

一旦RA跟蹤停止，調試檔案將在控制器bootflash中生成。

```
show bootflash: | include ra_trace
2728        179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

將檔案複製到外部伺服器。

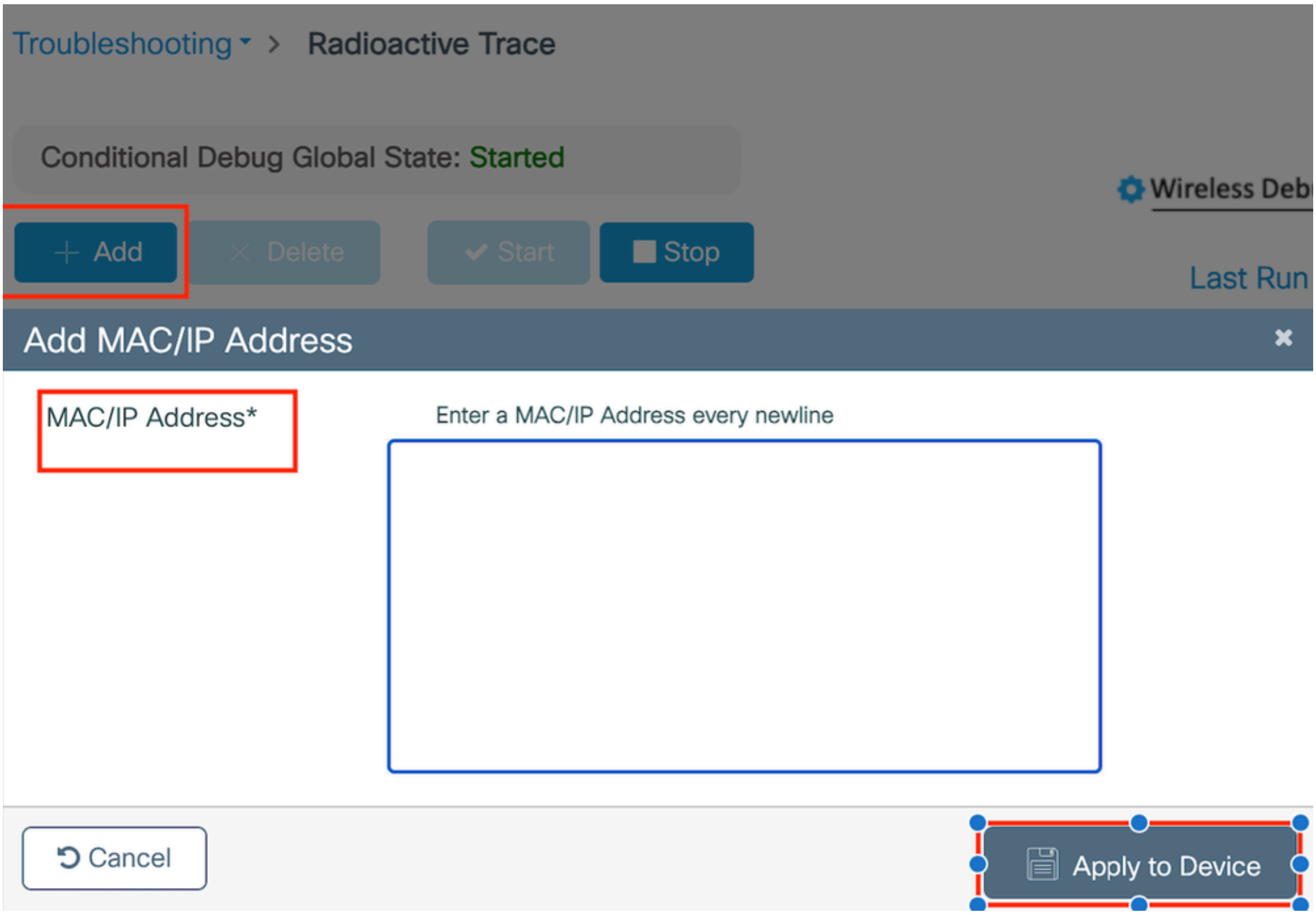
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addr
```

顯示調試日誌：

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

在GUI中啟用RA跟蹤，

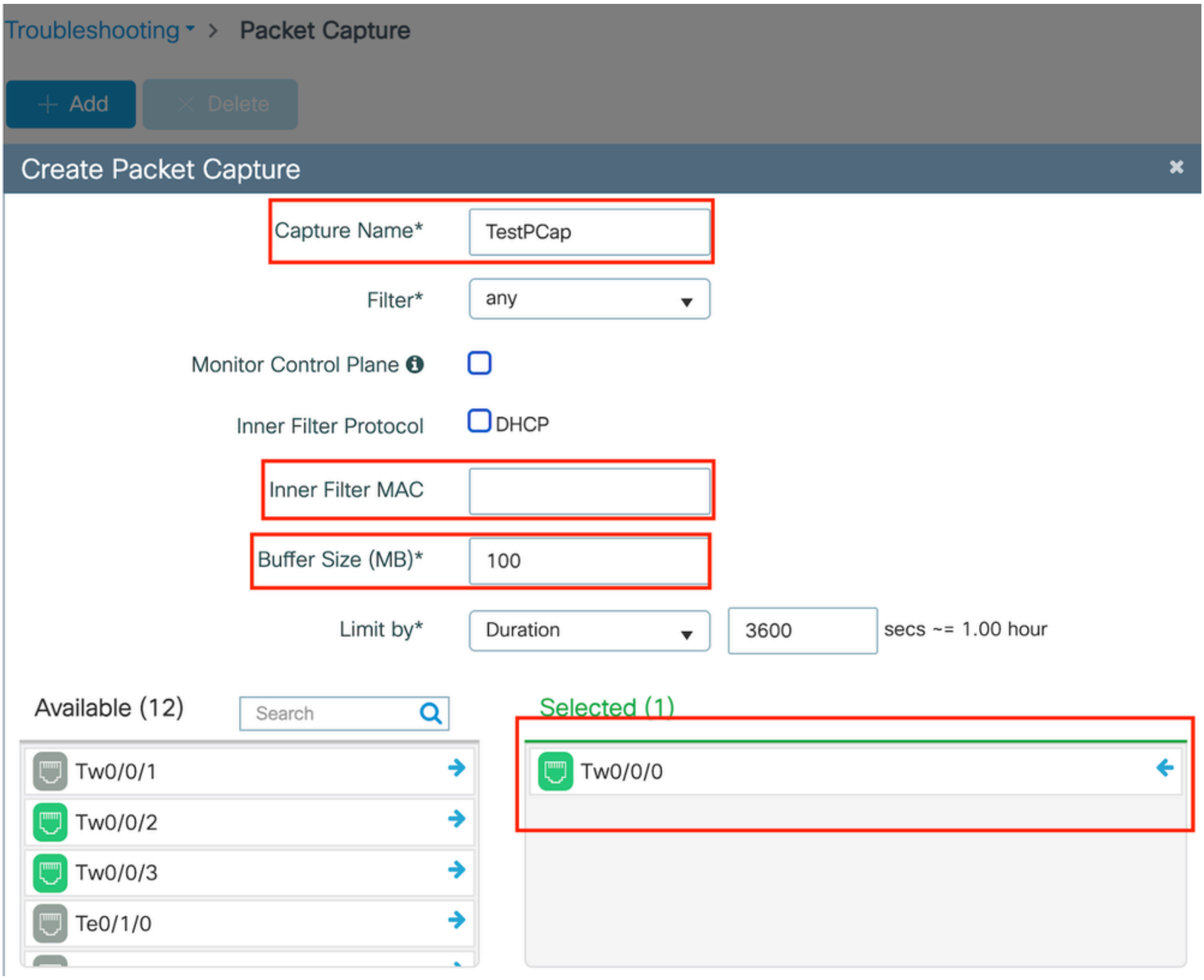
第1步：導航到故障排除>放射性跟蹤。選擇增加新條目的選項，然後在指定的增加MAC/IP地址頁籤中輸入客戶端MAC地址。


Troubleshooting > Radioactive Trace
Conditional Debug Global State: Started
Wireless Debi
+ Add
× Delete
✔ Start
■ Stop
Last Run
Add MAC/IP Address
MAC/IP Address*
Enter a MAC/IP Address every newline
Cancel
Apply to Device

無線電主動式追蹤

內嵌封包擷取：

導航至Troubleshooting > Packet Capture。輸入捕獲名稱並指定客戶端MAC地址作為內部過濾器MAC。將緩衝區大小設定為100，並選擇上行鏈路介面來監控傳入和傳出的資料包。



Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane □

Inner Filter Protocol □ DHCP

Inner Filter MAC

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ~= 1.00 hour

Available (12)

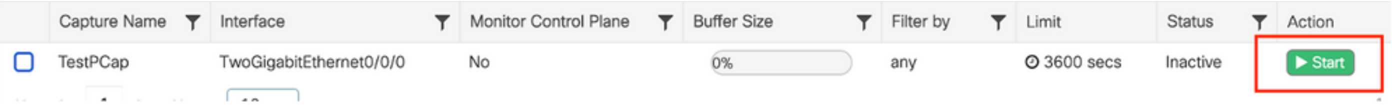
Selected (1)

Tw0/0/0

嵌入式資料包捕獲

注意：選擇「監控控制流量」選項以檢視重定向到系統CPU並重新注入資料平面的流量。

選擇Start捕獲資料包



	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
□	TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

開始捕獲

CLI配置

```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start

<Reporduce the issue>
```

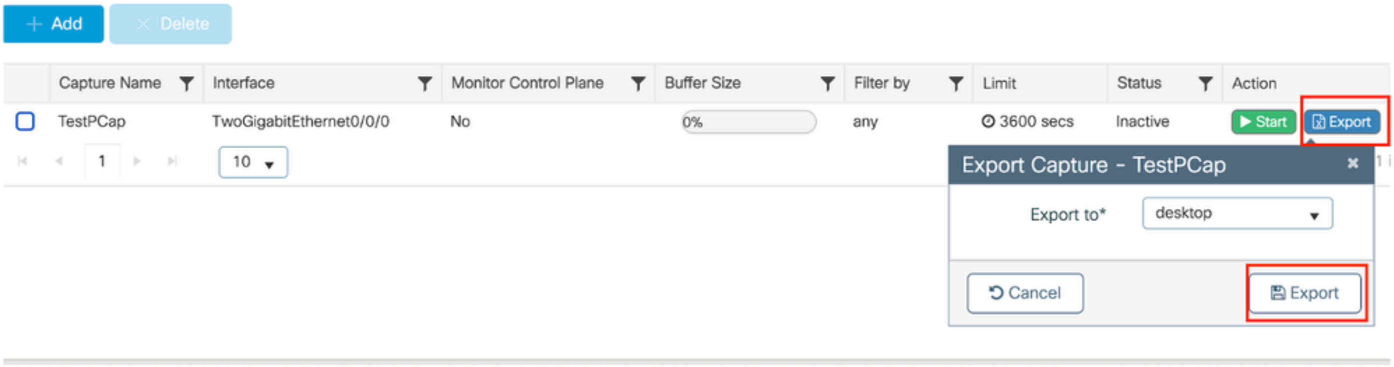
```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap

Status Information for Capture TestPCap
  Target Type:
 Interface: TwoGigabitEthernet0/0/0, Direction: BOTH
  Status : Inactive
  Filter Details:
  Capture all packets
  Inner Filter Details:
  Mac: 6c7e.67e3.6db9
  Continuous capture: disabled
  Buffer Details:
  Buffer Type: LINEAR (default)
  Buffer Size (in MB): 100
  Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 3600
  Packet Size to capture: 0 (no limit)
  Maximum number of packets to capture per second: 1000
  Packet sampling rate: 0 (no sampling)
```

將資料包捕獲導出到外部TFTP伺服器

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```



	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
□	TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start Export

Export Capture - TestPCap

Export to* desktop

導出資料包捕獲

示例場景在成功MAC身份驗證期間，客戶端裝置連線到網路，其MAC地址由RADIUS伺服器透過配置的策略進行驗證，在驗證後，網路接入裝置會授予訪問許可權，從而允許網路連線。

客戶端關聯後，控制器向ISE伺服器傳送訪問請求，

使用者名稱是客戶端的mac地址，因為這是MAB身份驗證

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
```

```
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
```

ISE傳送Access-Accept，因為我們有有效的使用者條目

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

客戶端策略狀態轉換到Mac Auth已完成

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29  Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

在成功MAB身份驗證後，客戶端處於IP learn狀態

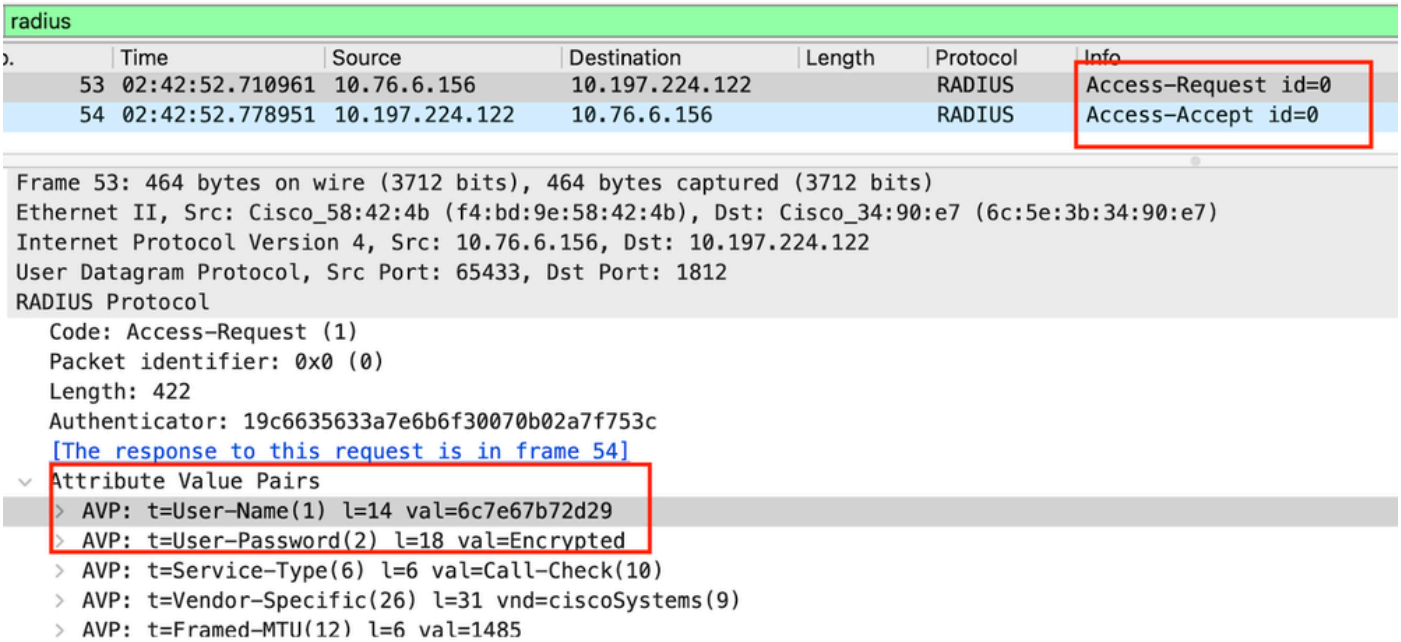
```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d2
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

客戶端策略管理器狀態更新為RUN，對於完成MAB身份驗證的客戶端，將跳過Web身份驗證

```
2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
```

使用嵌入式資料包捕獲進行驗證



```
radius
o.      Time              Source          Destination      Length   Protocol   Info
    53  02:42:52.710961  10.76.6.156     10.197.224.122             RADIUS     Access-Request id=0
    54  02:42:52.778951  10.197.224.122  10.76.6.156                RADIUS     Access-Accept id=0

 Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
 Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
 Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
 User Datagram Protocol, Src Port: 65433, Dst Port: 1812
 RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 422
    Authenticator: 19c6635633a7e6b6f30070b02a7f753c
    [The response to this request is in frame 54]
  ⌄ Attribute Value Pairs
    › AVP: t=User-Name(1) l=14 val=6c7e67b72d29
    › AVP: t=User-Password(2) l=18 val=Encrypted
    › AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    › AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    › AVP: t=Framed-MTU(12) l=6 val=1485
```

Radius封包

客戶端裝置的MAC身份驗證失敗的示例

在成功關聯後為客戶端啟動MAC身份驗證

```
2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Succes
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
```

ISE將傳送Access-Reject，因為ISE中沒有此裝置條目

```
2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000
```

對客戶端裝置啟動Web-Auth作為MAB失敗

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
```

一旦客戶端發起HTTP GET請求，重定向URL會被推送到客戶端裝置，因為相應的TCP會話被控制器偽裝。

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

使用者端啟動HTTP Get以進入重新導向URL，網頁載入後，就會送出登入認證。

控制器向ISE傳送訪問請求

這是一個Web驗證，因為在Access-Accept資料包中觀察到有效的使用者名稱

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
```

從ISE接收的Access-Accept

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

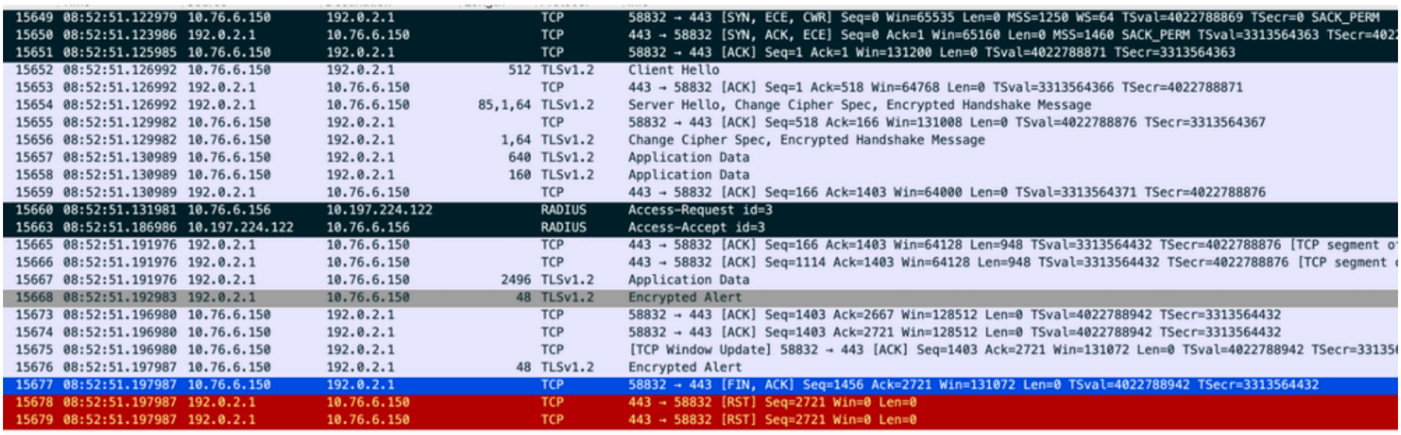
Web身份驗證成功，並且客戶端狀態轉換為RUN狀態

```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

透過EPC捕獲進行驗證

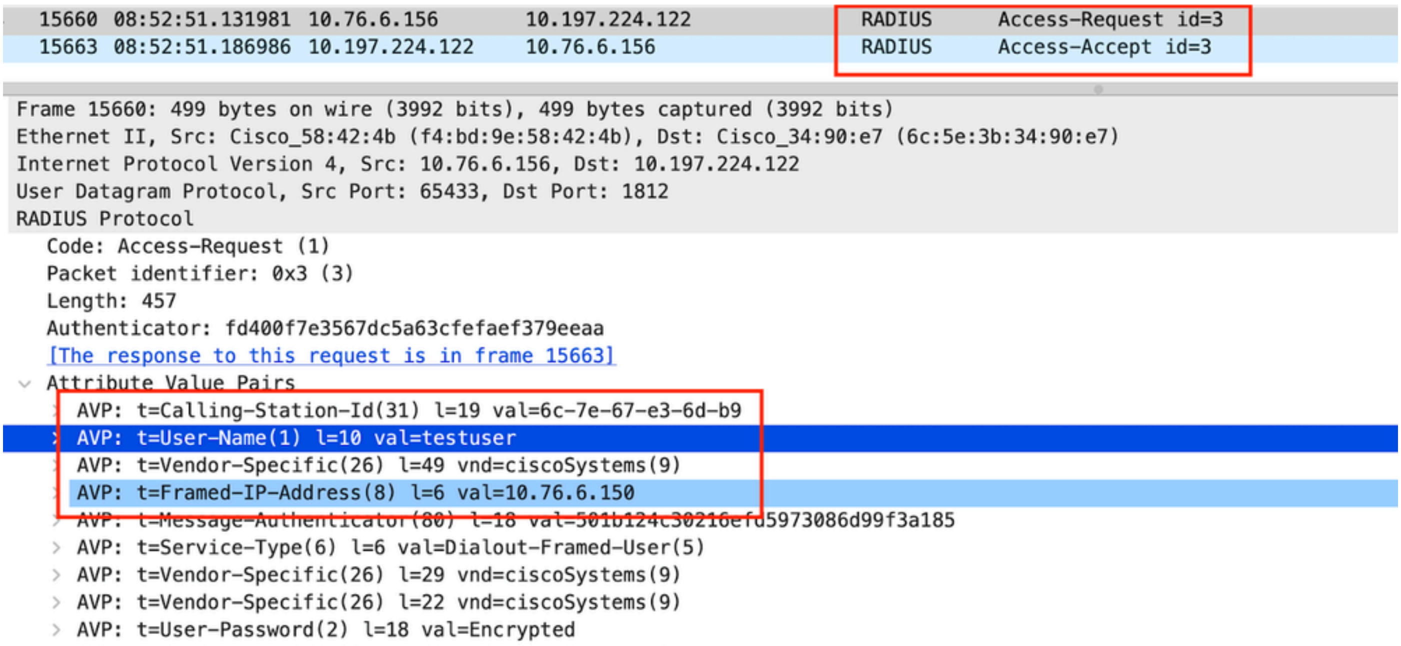
客戶端完成與控制器虛擬IP地址的TCP握手，客戶端載入重定向門戶頁。使用者提交使用者名稱和密碼後，我們可以觀察來自控制器管理IP位址的radius存取要求。

在身份驗證成功後，客戶端TCP會話關閉，並且客戶端在控制器上轉換到RUN狀態。



```
15649 08:52:51.122979 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650 08:52:51.123986 192.0.2.1       10.76.6.150                TCP      443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=402
15651 08:52:51.125985 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652 08:52:51.126992 10.76.6.150     192.0.2.1             512  TLSv1.2  Client Hello
15653 08:52:51.126992 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654 08:52:51.126992 192.0.2.1       10.76.6.150       85,1,64  TLSv1.2  Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655 08:52:51.129982 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656 08:52:51.129982 10.76.6.150     192.0.2.1            1,64  TLSv1.2  Change Cipher Spec, Encrypted Handshake Message
15657 08:52:51.130989 10.76.6.150     192.0.2.1             640  TLSv1.2  Application Data
15658 08:52:51.130989 10.76.6.150     192.0.2.1             160  TLSv1.2  Application Data
15659 08:52:51.130989 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660 08:52:51.131981 10.76.6.156     10.197.224.122             RADIUS   Access-Request id=3
15663 08:52:51.186986 10.197.224.122  10.76.6.156                RADIUS   Access-Accept id=3
15665 08:52:51.191976 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666 08:52:51.191976 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment
15667 08:52:51.191976 192.0.2.1       10.76.6.150          2496  TLSv1.2  Application Data
15668 08:52:51.192983 192.0.2.1       10.76.6.150            48  TLSv1.2  Encrypted Alert
15673 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      [TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=33135
15676 08:52:51.197987 10.76.6.150     192.0.2.1              48  TLSv1.2  Encrypted Alert
15677 08:52:51.197987 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678 08:52:51.197987 192.0.2.1       10.76.6.150                TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679 08:52:51.197987 192.0.2.1       10.76.6.150                TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
```

具有RADIUS資料包的TCP流

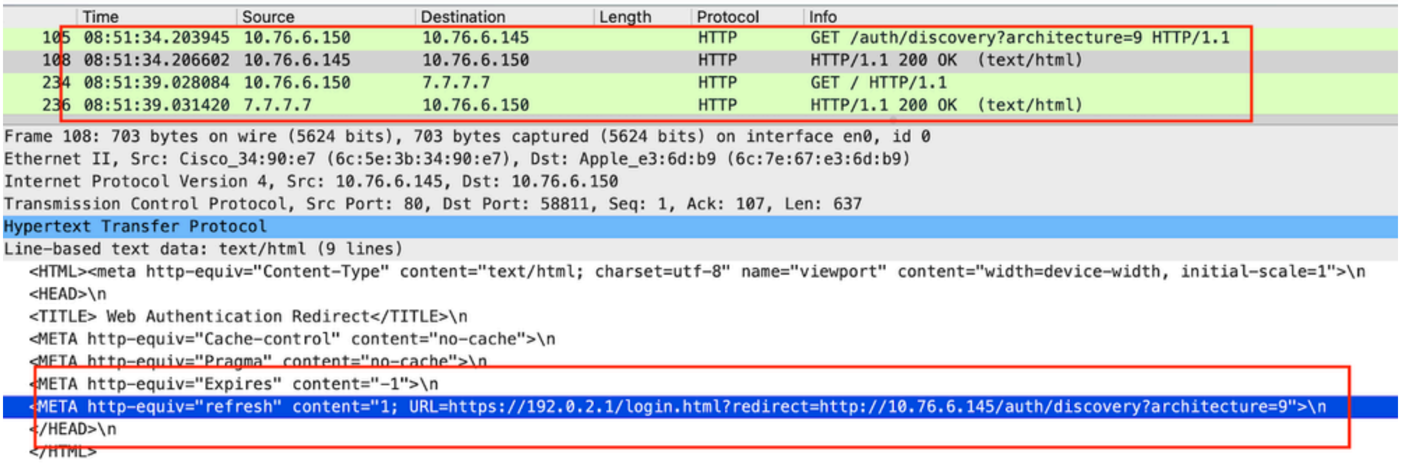


```
15660 08:52:51.131981 10.76.6.156     10.197.224.122    RADIUS    Access-Request id=3
15663 08:52:51.186986 10.197.224.122  10.76.6.156       RADIUS    Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x3 (3)
    Length: 457
    Authenticator: fd400f7e3567dc5a63cfefaef379eeaa
    [The response to this request is in frame 15663]
    Attribute Value Pairs
        AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
        AVP: t=User-Name(1) l=10 val=testuser
        AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
        AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
        AVP: t=Message-Authenticator(80) l=18 val=501b124c30216efd5973086d99f3a185
        AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)
        AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
        AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
        AVP: t=User-Password(2) l=18 val=Encrypted
```

使用使用者憑證傳送到ISE的RADIUS資料包

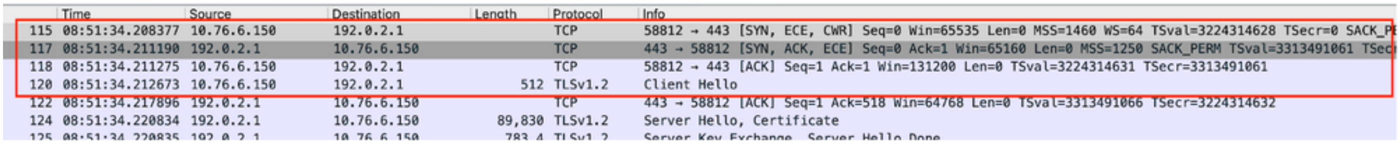
用於驗證客戶端流量的客戶端Wireshark捕獲重定向到門戶頁面並驗證到控制器虛擬IP地址/Web伺服器的TCP握手



```
     Time             Source       Destination   Length  Protocol  Info
105  08:51:34.203945  10.76.6.150  10.76.6.145           HTTP      GET /auth/discovery?architecture=9 HTTP/1.1
108  08:51:34.206602  10.76.6.145  10.76.6.150           HTTP      HTTP/1.1 200 OK  (text/html)
234  08:51:39.028084  10.76.6.150  7.7.7.7               HTTP      GET / HTTP/1.1
236  08:51:39.031420  7.7.7.7      10.76.6.150           HTTP      HTTP/1.1 200 OK  (text/html)
Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637
Hypertext Transfer Protocol
Line-based text data: text/html (9 lines)
   <HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
   <HEAD>\n
   <TITLE> Web Authentication Redirect</TITLE>\n
   <META http-equiv="Cache-control" content="no-cache">\n
   <META http-equiv="Pragma" content="no-cache">\n
   <META http-equiv="Expires" content="-1">\n
   <META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
   </HEAD>\n
   </HTML>
```

客戶端捕獲以驗證重定向url

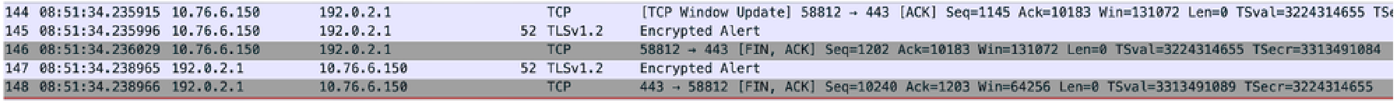
客戶端與控制器的虛擬IP地址建立TCP握手



```
    Time             Source         Destination      Length  Protocol  Info
115 08:51:34.208377  10.76.6.150    192.0.2.1                TCP       58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PE
117 08:51:34.211190  192.0.2.1      10.76.6.150              TCP       443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSec
118 08:51:34.211275  10.76.6.150    192.0.2.1                TCP       58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120 08:51:34.212673  10.76.6.150    192.0.2.1           512  TLSv1.2   Client Hello
122 08:51:34.217896  192.0.2.1      10.76.6.150              TCP       443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124 08:51:34.220834  192.0.2.1      10.76.6.150      89,830  TLSv1.2   Server Hello, Certificate
125 08:51:34.220835  192.0.2.1      10.76.6.150       783,4  TLSv1.2   Server Key Exchange, Server Hello Done
```

客戶端和Web伺服器之間的TCP握手

在成功Web身份驗證後關閉會話，



```
144 08:51:34.235915  10.76.6.150    192.0.2.1              TCP      [TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSe
145 08:51:34.235996  10.76.6.150    192.0.2.1          52  TLSv1.2  Encrypted Alert
146 08:51:34.236029  10.76.6.150    192.0.2.1              TCP      58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147 08:51:34.238965  192.0.2.1      10.76.6.150        52  TLSv1.2  Encrypted Alert
148 08:51:34.238966  192.0.2.1      10.76.6.150            TCP      443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655
```

客戶端完成Web身份驗證後關閉TCP會話

相關文章

瞭解 Catalyst 9800 無線 LAN 控制器的無線偵錯和記錄收集作業

9800上的Web型驗證

在9800上配置本地Web身份驗證

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）。