

在Catalyst 9800無線控制器系列上配置802.1X認證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[WLC配置](#)

[9800 WLC上的AAA配置](#)

[WLAN配置檔案配置](#)

[原則設定檔組態](#)

[原則標籤組態](#)

[原則標籤指定](#)

[ISE 組態](#)

[宣告WLC on ISE](#)

[在ISE上建立新使用者](#)

[建立授權設定檔](#)

[建立策略集](#)

[建立身份驗證策略](#)

[建立授權策略](#)

[驗證](#)

[疑難排解](#)

[對WLC進行故障排除](#)

[在ISE上進行故障排除](#)

簡介

本文說明如何在Cisco Catalyst 9800系列無線控制器上設定具有802.1X安全性的WLAN。

必要條件

需求

思科建議您瞭解以下主題：

- 802.1X

採用元件

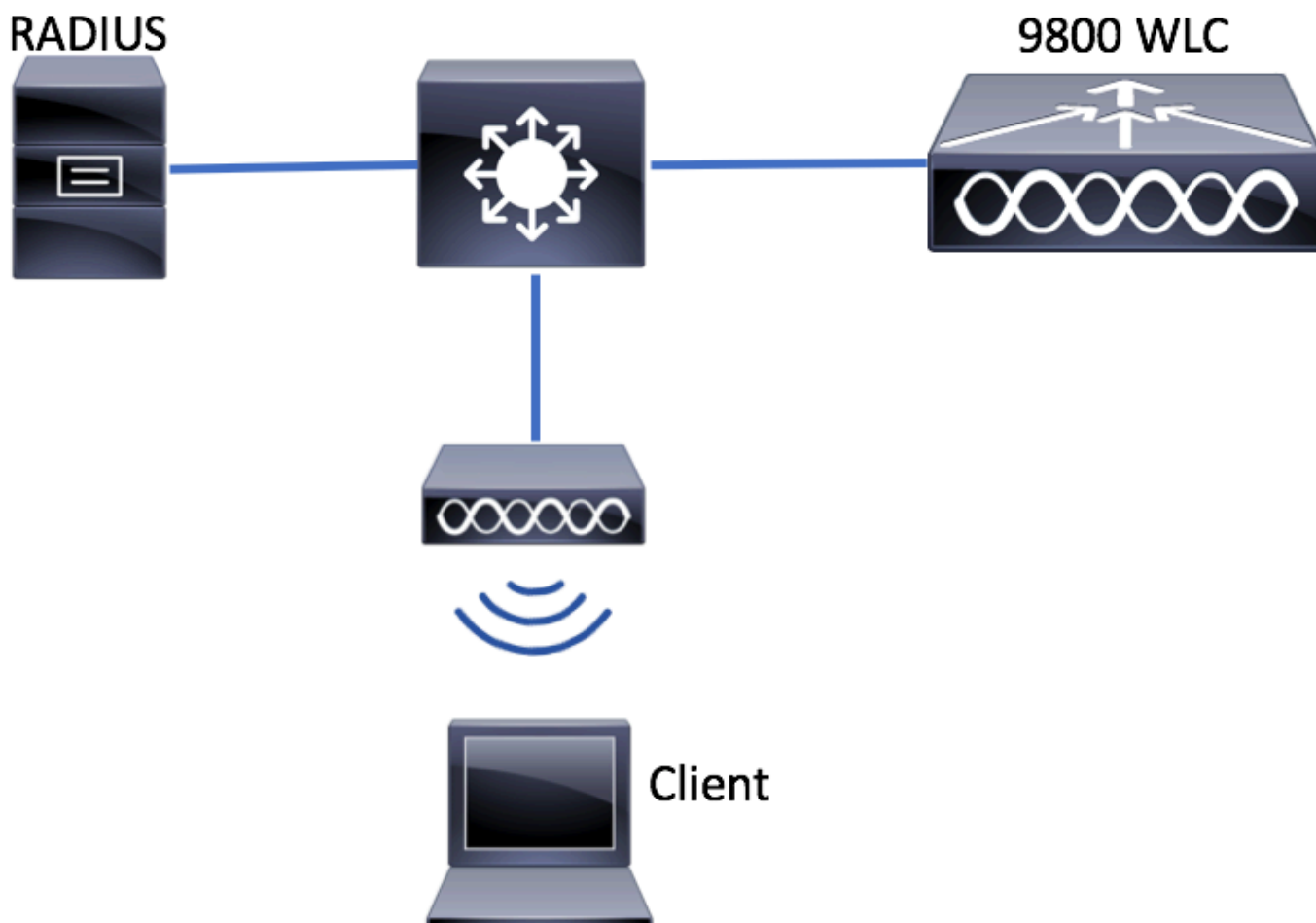
本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800無線控制器系列(Catalyst 9800-CL)
- Cisco IOS® XE直布羅陀版17.3.x
- Cisco ISE 3.0

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。

設定

網路圖表



WLC配置

9800 WLC上的AAA配置

GUI：

步驟 1.宣告RADIUS伺服器。導航到 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 並輸入RADIUS伺服器資訊。

如果您計畫將來使用中央Web身份驗證（或任何需要授權更改[CoA]的安全型別），請確保啟用對CoA的支援。

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

步驟 2.將RADIUS伺服器增加到RADIUS組。導航到 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. 為組指定名稱，並移動之前在清單中建立的伺服器 Assigned Servers.

Create AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

步驟 3. 建立驗證方法清單。導覽至 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**。

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration

Authentication Authorization and Accounting

AAA Method List Servers / Groups

General

Authentication

Name

輸入以下資訊：

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

CLI :

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 3
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```


有關AAA Dead-Server檢測的注意事項


設定RADIUS伺服器後，您就可以檢查它是否視為「ALIVE」：


```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

可以在WLC上配置 **dead criteria**, 和 **deadtime** ，特別是在使用多個RADIUS伺服器的情況下。

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

 **注意：** **dead criteria** 是用來將RADIUS伺服器標籤為停機的標準。它包括：1.逾時（秒），代表從控制器上次從RADIUS伺服器收到有效封包的時到伺服器標示為停機的時間，所必須經過的時間。2.一個計數器，代表在RADIUS伺服器被標籤為失效之前必須在控制器上發生的連續超時次數。

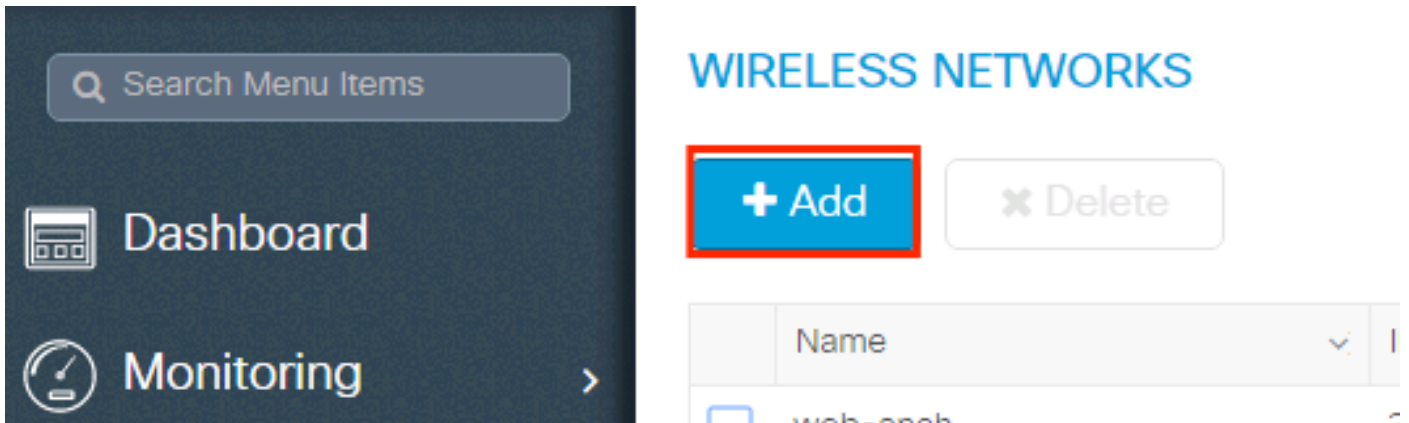
 **注意：** **deadtime**指定在停頓條件將其標籤為停頓後，伺服器保持停頓狀態的時間（以分鐘為單位）。一旦死期過期，控制器

 將伺服器標籤為UP (ALIVE)，並通知已註冊的客戶端有關狀態更改的資訊。如果狀態標籤為UP後仍無法訪問伺服器，並且滿足dead條件，則在死區時間間隔內伺服器將再次標籤為dead。

WLAN配置檔案配置

GUI：

步驟 1. 建立WLAN。導覽至「組態」>「無線」>「WLAN」>「+ 新增」，並依需要設定網路。



步驟 2. 輸入無線區域網資訊

Add WLAN

General Security Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

步驟 3. 導航到安全性頁籤，然後選擇所需的安全方法。在本示例中，WPA2 + 802.1x。

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

Fast Transition Adaptive Enab... ▼

Over the DS

Reassociation Timeout 20

PMF Disabled ▼

WPA Parameters

WPA Policy

Add WLAN ✕

PMF Disabled ▼

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x ▼

步驟 4. 從 Security > AAA 頁籤中，從9800 WLC上的AAA配置部分選擇第3步中建立的身份驗證方法。

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List list-name

Local EAP Authentication

Cancel Save & Apply to Device

CLI :

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

原則設定檔組態

在策略配置檔案中，您可以決定要將客戶端分配到哪個VLAN，以及其他設定（如訪問控制清單[ACL]、服務品質[QoS]、移動錨點、計時器等）。

您可以使用預設策略配置檔案，也可以建立新配置檔案。

GUI :

導航到配置 > 標籤和配置檔案 > 策略配置檔案，配置您的預設策略配置檔案或建立新配置檔案。

Policy Profile

+ Add ✕ Delete

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

1 items per page

確認設定檔已啟用。

此外，如果您的存取點(AP)處於本地模式，請確保策略配置檔案已啟用集中交換和集中身份驗證。

Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile	WLAN Switching Policy Central Switching <input checked="" type="checkbox"/> Central Authentication <input checked="" type="checkbox"/> Central DHCP <input checked="" type="checkbox"/> Central Association Enable <input checked="" type="checkbox"/> Flex NAT/PAT <input type="checkbox"/>
Description	default policy profile	
Status	ENABLED <input checked="" type="checkbox"/>	
Passive Client	<input type="checkbox"/> DISABLED	
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	
CTS Policy		
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

在Access Policies頁籤中選擇需要分配客戶端的VLAN。

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



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



如果您計畫在Access-Accept like VLAN分配中包含ISE返回屬性，請在 **Advanced** 頁籤中啟用AAA覆蓋：

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)	<input style="width: 80%;" type="text" value="1800"/>
Idle Timeout (sec)	<input style="width: 80%;" type="text" value="300"/>
Idle Threshold (bytes)	<input style="width: 80%;" type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input style="width: 80%;" type="text" value="60"/>

DHCP

IPv4 DHCP Required	<input checked="" type="checkbox"/>
DHCP Server IP Address	<input style="width: 80%;" type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input style="width: 80%;" type="text" value="default-aaa-policy"/> ✕ ▼

Fabric Profile	<input type="checkbox"/> <input style="width: 80%;" type="text" value="Search or Select"/> ▼
Umbrella Parameter Map	<input style="width: 80%;" type="text" value="Not Configured"/> ▼
mDNS Service Policy	<input style="width: 80%;" type="text" value="default-mdns-service"/> ▼ Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input style="width: 80%;" type="text" value="Search or Select"/> ▼

Air Time Fairness Policies

2.4 GHz Policy	<input style="width: 80%;" type="text" value="Search or Select"/> ▼
5 GHz Policy	<input style="width: 80%;" type="text" value="Search or Select"/> ▼

CLI :

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

原則標籤組態

策略標籤用於將SSID與策略配置檔案連結。您可以建立新的原則標籤，或使用 default-policy-tag。

注意： default-policy-tag會自動將WLAN ID介於1和16之間的任何SSID對映到預設策略配置檔案。無法修改或刪除。如果您的WLAN的ID為17或更高，則不能使用default-policy-tag。

GUI :

如果需要，請導航到 **Configuration > Tags & Profiles > Tags > Policy** 並增加新的日誌。

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Manage Tags

Policy Site RF AP

+ Add **✕ Delete**

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

1 10 items per page

將 WLAN 設定檔連結至想要的原則設定檔。

Add Policy Tag

Name*

Description

+ Add **✕ Delete**

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel **Save & Apply to Device**

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile*

Policy Profile*

✕
✓

↶ Cancel
Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile

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

↶ Cancel
Save & Apply to Device

CLI :

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

原則標籤指定

指派原則標籤至需要的 AP。


GUI :

要將標籤分配給一個AP，請導航至 **Configuration > Wireless > Access Points > AP Name > General Tags**, 分配相關策略標籤，然後按一下 **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration window with the following details:

- General Tab:** AP Name* (AP3802-02-WS), Location* (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled).
- Version Tab:** Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.52), Mini IOS Version (0.0.0.0).
- IP Config Tab:** IP Address (172.16.0.207), Static IP (unchecked).
- Time Statistics Tab:** Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), Controller Association Latency (8 days 21 hrs 50 mins 33 secs).
- Tags Section:** Policy (default-policy-tag), Site (default-site-tag), RF (default-rf-tag).

Buttons: Cancel, Update & Apply to Device.

 注意：請注意，當AP上的策略標籤發生更改時，它將斷開與9800 WLC的關聯，並在稍後重新加入。

要將同一策略標籤分配給多個AP，請導航至 **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



Tag APs

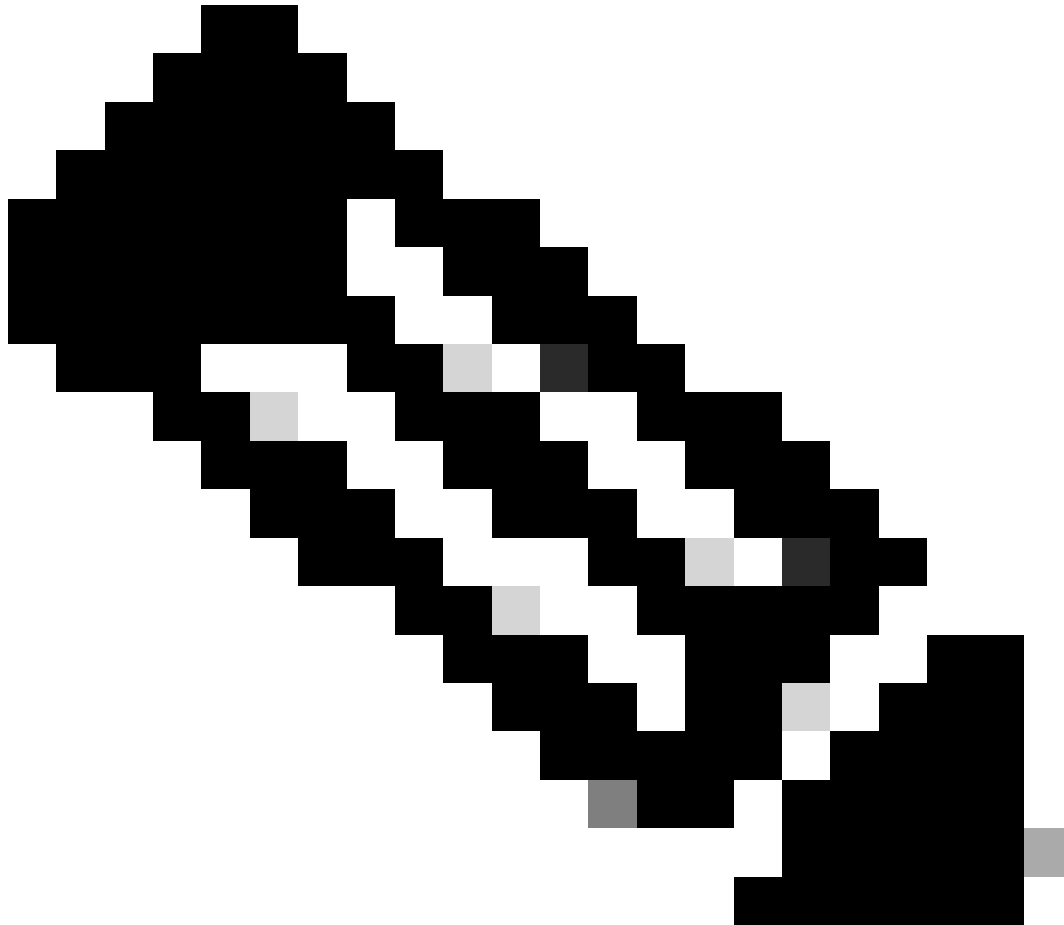


Done

Start Now →


```
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

疑難排解



註：外部負載均衡器的用途良好。但是，透過使用calling-station-id RADIUS屬性，確保負載均衡器針對每個客戶端運行。依賴UDP源埠不是用於平衡來自9800的RADIUS請求的受支援機制。

對WLC進行故障排除

WLC 9800提供永遠開啟追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別消息持續記錄，並且您可以在事件發生後檢視事件或故障條件的日誌。

這取決於生成的日誌量，但通常，您可以返回幾小時到幾天。

為了檢視9800 WLC預設收集的跟蹤，您可以透過SSH/Telnet連線到9800 WLC並執行以下步驟：（確保將會話記錄到文本檔案中）。

步驟 1.檢查WLC目前時間，以便您可以追蹤問題發生時的記錄。


```
# show clock
```

步驟 2.根據系統配置的指示，從WLC緩衝區或外部系統日誌收集系統日誌。如此可快速檢視系統健全狀況和錯誤（如有）。

```
# show logging
```

步驟 3.驗證是否啟用了任何調試條件。

```
# show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Ad
```

 **注意：**如果發現列出任何條件，則意味著所有遇到啟用條件（mac地址、ip地址等）的進程的跟蹤將記錄到調試級別。這將增加日誌的量。因此，建議在不主動調試時清除所有條件。

步驟 4.假設測試的mac地址未列為步驟3中的條件，收集特定mac地址的always-on通知級別跟蹤：

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

您可以顯示作業階段上的內容，也可以將檔案複製到外部TFTP伺服器：

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

條件式偵錯和無線電主動式追蹤

如果永遠線上的追蹤無法提供足夠資訊來判斷觸發調查中問題的原因，您可以啟用條件式偵錯並擷取「無線電作用中(RA)」追蹤，此追蹤會為與指定條件（此案例為使用者端mac位址）互動的所有處理作業提供偵錯層級追蹤。您可以透過GUI或CLI執行此操作。

CLI：

要啟用條件調試，請執行以下步驟：

步驟 5.確保未啟用調試條件。

```
# clear platform condition all
```

步驟 6.為要監控的無線客戶端MAC地址啟用調試條件。

此指令會開始監控提供的mac位址長達30分鐘（1800秒）。您可以選擇將此時間增加至2085978494秒。

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



附註：若要同時監控多個用戶端，請針對每個 MAC 位址執行 debug wireless mac <aaaa.bbbb.cccc> 指令。



注意：您不會在終端會話中看到客戶端活動的輸出，因為所有內容都在內部進行緩衝以便以後檢視。

步驟 7.重現您要監控的問題或行為。

步驟 8.如果在預設或配置的監控時間過去之前重現問題，則停止調試。

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

當監控時間結束或偵錯無線停止後，9800 WLC 會產生本機檔案，名稱如下：

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟 9. 收集 MAC 位址活動的檔案。 您可以將ra trace.log複製到外部伺服器，或直接在螢幕上顯示輸出。

檢查 RA 追蹤檔案的名稱：

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

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://a.b.c.d/ra-FILENAME.txt
```

顯示內容：

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

步驟 10. 如果根本原因仍不明顯，請收集內部日誌，這是調試級別日誌的更詳細檢視。我們進一步詳細檢視已收集並內部儲存的調試日誌，因此您無需再次調試客戶端。

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



注意：此命令輸出返回所有進程的所有日誌級別的跟蹤，而且數量非常大。請聯絡 Cisco TAC 協助剖析此類追蹤。

您可將 ra-internal-FILENAME.txt 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

將檔案複製到外部伺服器：

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

顯示內容：

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

步驟 11. 移除偵錯條件。

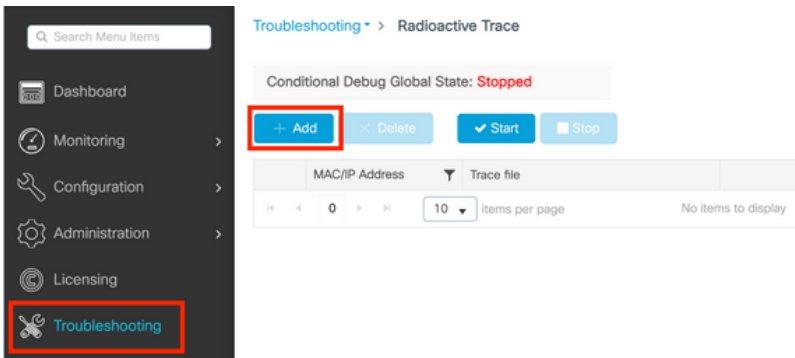
clear platform condition all



注意：請確保在排除會話故障後始終刪除調試條件。

GUI：

步驟 1. 轉到 **Troubleshooting > Radioactive Trace > + Add** 並指定要進行故障排除的客戶端的MAC/IP地址。

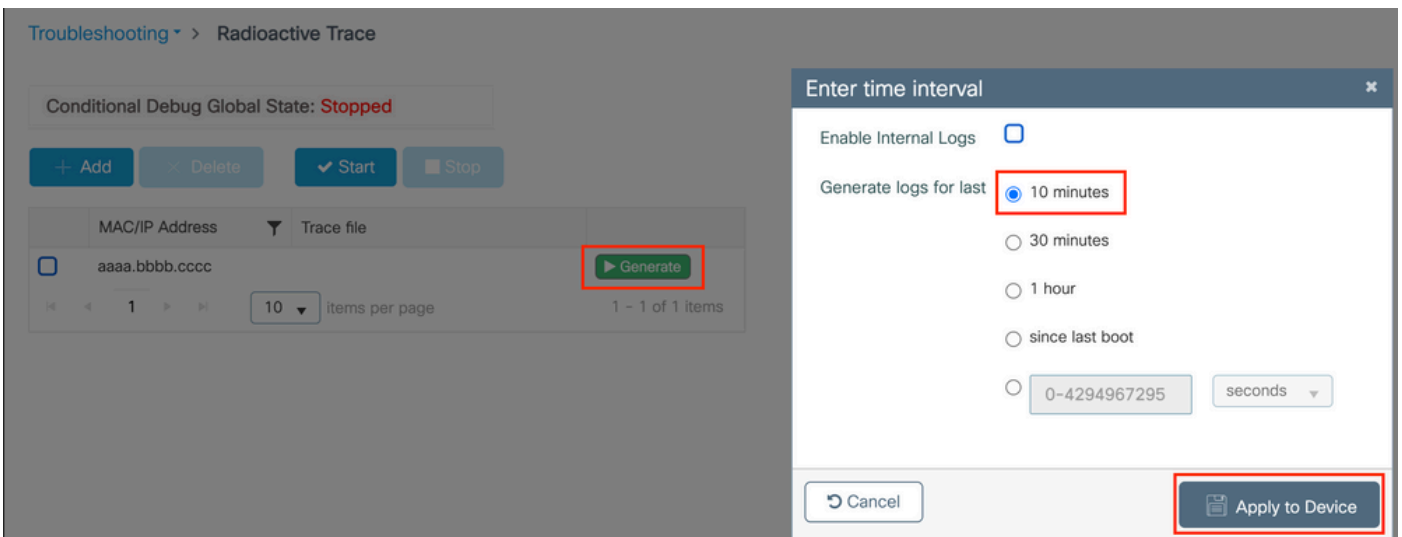


步驟 2. 按一下 **Start**。

步驟 3. 重現問題。

步驟 4. 按一下 **停止**。

步驟 5. 按一下 **Generate** 按鈕，選擇要獲取日誌的時間間隔，然後按一下 **Apply to Device**。In this example, the logs for the last 10 minutes are requested.



步驟 6. 將放射性跟蹤下載到您的電腦上，然後按一下「下載」按鈕並進行檢查。

Conditional Debug Global State: **Stopped**

[+ Add](#)
[x Delete](#)
[✓ Start](#)
[■ Stop](#)

MAC/IP Address	Trace file	
aaaa.bbbb.cccc	debugTrace_aaaa.bbbb.cccc.txt	Download Generate

10 items per page 1 - 1 of 1 items

Last Run Result

✓ State: Successful [See Details](#)
 MAC/IP Address: aaaa.bbbb.cccc
 Start Time: 08/24/2022 08:46:49
 End Time: 08/24/2022 08:47:00
 Trace file: debugTrace_aaaa.bbbb.cccc.txt [Download](#)

在ISE上進行故障排除

如果遇到客戶端身份驗證問題，您可以驗證ISE伺服器上的日誌。轉到 **Operations > RADIUS > Live Logs** 並看到身份驗證請求清單、匹配的策略集、每個請求的結果等。按一下每行 **Details** 頁籤下的放大鏡，可以獲得更多詳細資訊，如圖所示：

Cisco ISE Operations · RADIUS Evaluation Mode 85 Days

Live Logs Live Sessions

Misconfigured Suppliants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 2

Repeat Counter 0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Netwo
Aug 23, 2022 06:18:42.5...	●	Details	0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...	●	Details		user1	BC:D0:74:2B:6D:...						9800-W

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）。