

# 在Catalyst 9800無線控制器系列上配置802.1X身份驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[WLC組態](#)

[9800 WLC上的AAA組態](#)

[WLAN配置檔案配置](#)

[原則設定檔組態](#)

[原則標籤組態](#)

[策略標籤分配](#)

[ISE 組態](#)

[宣告ISE上的WLC](#)

[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](#)

[WLC上的疑難排解](#)

[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

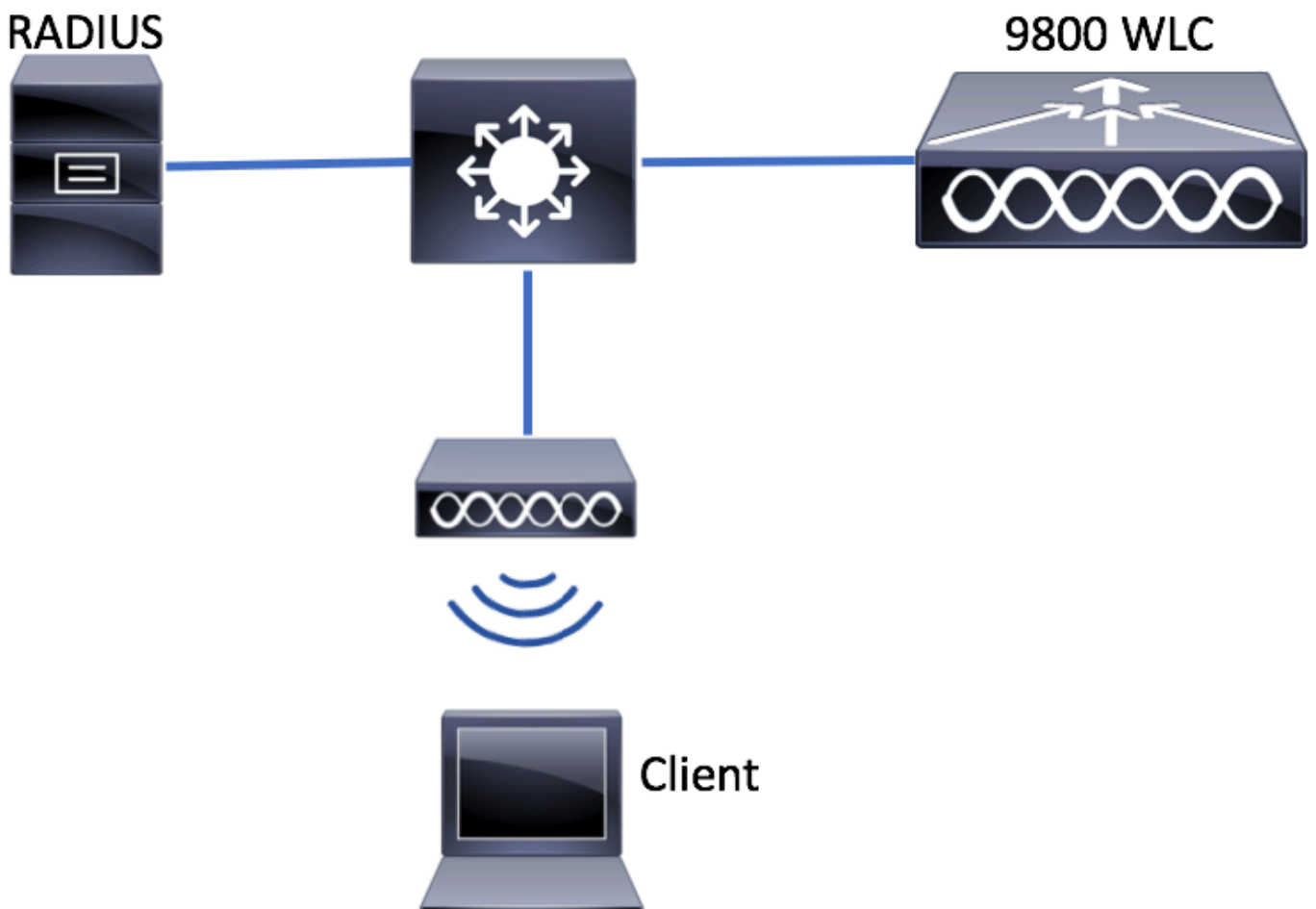
本文中的資訊係根據以下軟體和硬體版本：

- 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組態

#### 9800 WLC上的AAA組態

GUI:

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

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List **Servers / Groups** AAA Advanced

+ Add Delete

**RADIUS** TACACS+ LDAP

Servers Server Groups

Name	Address
------	---------

如果您計畫將來使用中央Web驗證（或任何需要授權變更[CoA]的安全型別），請確保支援CoA。

Create AAA Radius Server

Name\* ISE-kcg Clear PAC Key

IPv4/IPv6 Server Address\* 172.16.0.11 Set New PAC Key

Shared Secret\* .....

Confirm Shared Secret\* .....

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

Cancel Save & Apply to Device

步驟2.將RADIUS伺服器新增到RADIUS組。導航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. 為您的組指定一個名稱，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. 建立身份驗證方法清單。導航至 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**

Authorization

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
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

### 關於AAA失效伺服器檢測的註釋

設定RADIUS伺服器後，您就可以檢查它是否被認為是「ALIVE」：

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC
(2) : current UP Platform State from WNCDC (3) : current UP Platform State from WNCDC (4) :
current UP ...
```

您可以配置 **dead criteria**，以及 **deadtime** 多台RADIUS伺服器時，尤應如此。

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

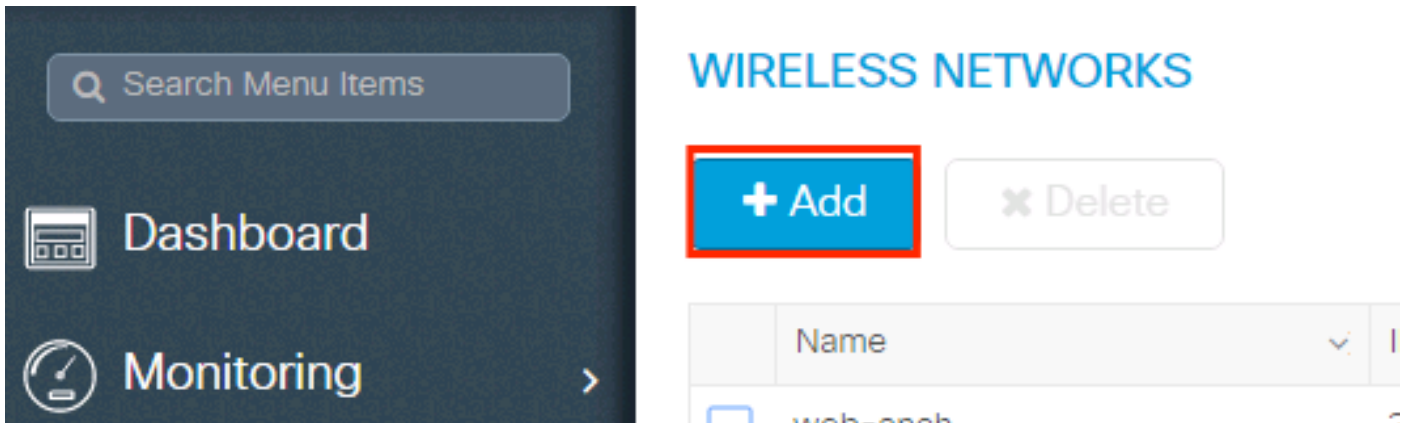
**註：** **dead criteria** 是用來標籤RADIUS伺服器為宕機的條件。它包括：1. 超時（以秒為單位），表示從控制器上次從RADIUS伺服器收到有效封包時間起至伺服器標籤為停用的時間長度。2. 一個計數器，表示RADIUS伺服器標籤為失效之前，控制器上必須發生的連續超時數。

**註:** **deadtime** 指定在死條件將其標籤為死後，伺服器保持死狀態的時間（以分鐘為單位）。一旦死區期滿，控制器會將伺服器標籤為UP(ALIVE)，並通知已註冊的客戶端狀態變化。如果在狀態標籤為UP後伺服器仍然無法訪問，並且滿足dead條件，則在死時間間隔內，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Configuration > Wireless > WLANs > + Add，然後根據需要配置網路。



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. 導航至 **Security** 選項卡，並選擇所需的安全方法。在本例中WPA2 + 802.1x。

**Add WLAN** [Close]

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** [Close]

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配置部分選擇在步驟3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:

導覽至 **Configuration > Tags & Profiles > Policy Profile**，然後設定 **default-policy-profile** 或建立一個新配置檔案。

**Policy Profile**

**+ Add**      ✕ Delete

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

1      10 items per page



確認設定檔已啟用。

此外，如果您的存取點(AP)處於本機模式，請確保原則設定檔已啟用中央交換和中央驗證。

### 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	<b>WLAN Switching Policy</b> 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	
<b>CTS Policy</b>		
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

<b>WLAN Local Profiling</b>		<b>WLAN ACL</b>	
HTTP TLV Caching	<input type="checkbox"/>	IPv4 ACL	Search or Select ▼
RADIUS Profiling	<input type="checkbox"/>	IPv6 ACL	Search or Select ▼
DHCP TLV Caching	<input type="checkbox"/>	<b>URL Filters</b>	
Local Subscriber Policy Name	Search or Select ▼	Pre Auth	Search or Select ▼
<b>VLAN</b>		Post Auth	Search or Select ▼
VLAN/VLAN Group	VLAN2602 ▼		
Multicast VLAN	Enter Multicast VLAN		

如果您計畫在訪問接受類似於VLAN分配中擁有ISE返回屬性，請在 **Advanced** 頁籤：

The screenshot shows the 'Edit Policy Profile' window with the 'Advanced' tab selected. The 'AAA Policy' section is highlighted with a red box. The 'Allow AAA Override' checkbox is checked. Other sections include 'WLAN Timeout' with fields for Session Timeout (1800), Idle Timeout (300), Idle Threshold (0), and Client Exclusion Timeout (60). The 'DHCP' section has 'IPv4 DHCP Required' checked. The 'WLAN Flex Policy' section has 'VLAN Central Switching' unchecked. The 'Air Time Fairness Policies' section has '2.4 GHz Policy' and '5 GHz Policy' dropdowns. The 'Update & Apply to Device' button is visible at the bottom right.

## 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 之間的所有 SSID 對映到 default-policy-profile。不能修改或刪除。如果您的 WLAN 的 ID 為 17 或更高，則不能使用 default-policy-tag。

## GUI:

導航至 **Configuation > Tags & Profiles > Tags > Policy** 如果需要，可以新增新的。

Search Menu Items

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

### Manage Tags

Policy Site RF AP

**+ Add**

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**

WLAN Profile	Policy Profile
No items to display	

0 10 items per page

**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>
```

**策略標籤分配**

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**，分配相關的策略標籤，然後按一下 **Update & Apply to Device**。

The screenshot shows the 'Edit AP' configuration page with the 'General' tab selected. The 'General' section includes fields for 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), and Fabric Status (Disabled). The 'Tags' section has dropdown menus for Policy (default-policy-tag), Site (default-site-tag), and RF (default-rf-tag). The 'Version' section shows software and IOS versions. The 'IP Config' section shows IP Address (172.16.0.207) and a checkbox for Static IP. The 'Time Statistics' section shows Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), and Controller Association Latency (8 days 21 hrs 50 mins 33 secs). The 'Update & Apply to Device' button is highlighted with a red box.

Field	Value
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
Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
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	10.0.200.02
Mini IOS Version	0.0.0.0
IP Address	172.16.0.207
Static IP	<input type="checkbox"/>
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

註意：請注意，當AP上的策略標籤更改時，它會丟棄與9800 WLC的關聯，並在稍後重新連線。

要將相同的策略標籤分配給多個AP，請導航至 **Configuration > Wireless Setup > Advanced > Start Now > Apply**。



## 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）。