

使用ISE和Catalyst 9800無線LAN控制器配置動態VLAN分配

目錄

[簡介](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[使用RADIUS伺服器進行動態VLAN指派](#)

[設定](#)

[網路圖表](#)

[配置步驟](#)

[Cisco ISE配置](#)

[步驟1.將Catalyst WLC配置為Cisco ISE伺服器上的AAA客戶端](#)

[步驟2.在Cisco ISE上配置內部使用者](#)

[步驟3.設定用於動態VLAN分配的RADIUS\(IETF\)屬性](#)

[為多個VLAN配置交換機](#)

[Catalyst 9800 WLC組態](#)

[步驟1.使用驗證伺服器的詳細資訊設定WLC](#)

[步驟2.配置VLAN](#)

[步驟3.配置WLAN\(SSID\)](#)

[步驟4.配置策略配置檔案](#)

[步驟5.配置策略標籤](#)

[步驟6.為AP分配策略標籤](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹動態VLAN分配的概念，以及如何設定Catalyst 9800無線LAN控制器(WLC)和思科身分識別服務引擎(ISE)以分配無線LAN(WLAN)，以便為無線使用者端完成此操作。

需求

思科建議您瞭解以下主題：

- 具有WLC和輕量型存取點(LAP)的基本知識。
- 具有AAA伺服器的功能知識，例如ISE。
- 全面瞭解無線網路和無線安全問題。
- 具有動態VLAN分配方面的功能知識。
- 具備無線接入點(CAPWAP)的控制和調配基礎知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體版本16.12.4a的Cisco Catalyst 9800 WLC(Catalyst 9800-CL)。
- 本地模式下的Cisco 2800系列LAP。
- 本機Windows 10請求方。
- 思科身分識別服務引擎(ISE)，執行版本2.7。
- Cisco 3850系列交換器 (執行韌體版本16.9.6)。

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

使用RADIUS伺服器進行動態VLAN指派

在大多數無線區域網路(WLAN)系統中，每個WLAN都有一個靜態原則，適用於與服務組識別碼(SSID)相關聯的所有使用者端。此方法雖然功能強大，但也有侷限性，因為它要求客戶端與不同的SSID關聯以繼承不同的QoS和安全策略。

但是，Cisco WLAN解決方案支援身份網路。這允許網路通告單個SSID並允許特定使用者基於使用者憑證繼承不同的QoS或安全策略。

動態VLAN分配是一種功能，可根據使用者提供的憑證將無線使用者置於特定VLAN中。將使用者分配到特定VLAN的任務由RADIUS身份驗證伺服器 (例如Cisco ISE) 處理。例如，這可用於允許無線主機在園區網路中移動時保持在同一個VLAN上。

因此，當使用者端嘗試與在控制器上註冊的LAP相關聯時，WLC會將使用者的憑證傳遞到RADIUS伺服器以進行驗證。驗證成功後，RADIUS伺服器會將某些Internet工程工作小組(IETF)屬性傳遞給使用者。這些RADIUS屬性決定必須分配給無線客戶端的VLAN ID。客戶端的SSID並不重要，因為系統始終為使用者分配此預先確定的VLAN ID。

用於VLAN ID分配的RADIUS使用者屬性包括：

- IETF 64 (隧道型別) — 將其設定為VLAN。
- IETF 65 (隧道介質型別) — 將其設定為802。
- IETF 81 (隧道專用組ID) — 將其設定為VLAN ID。

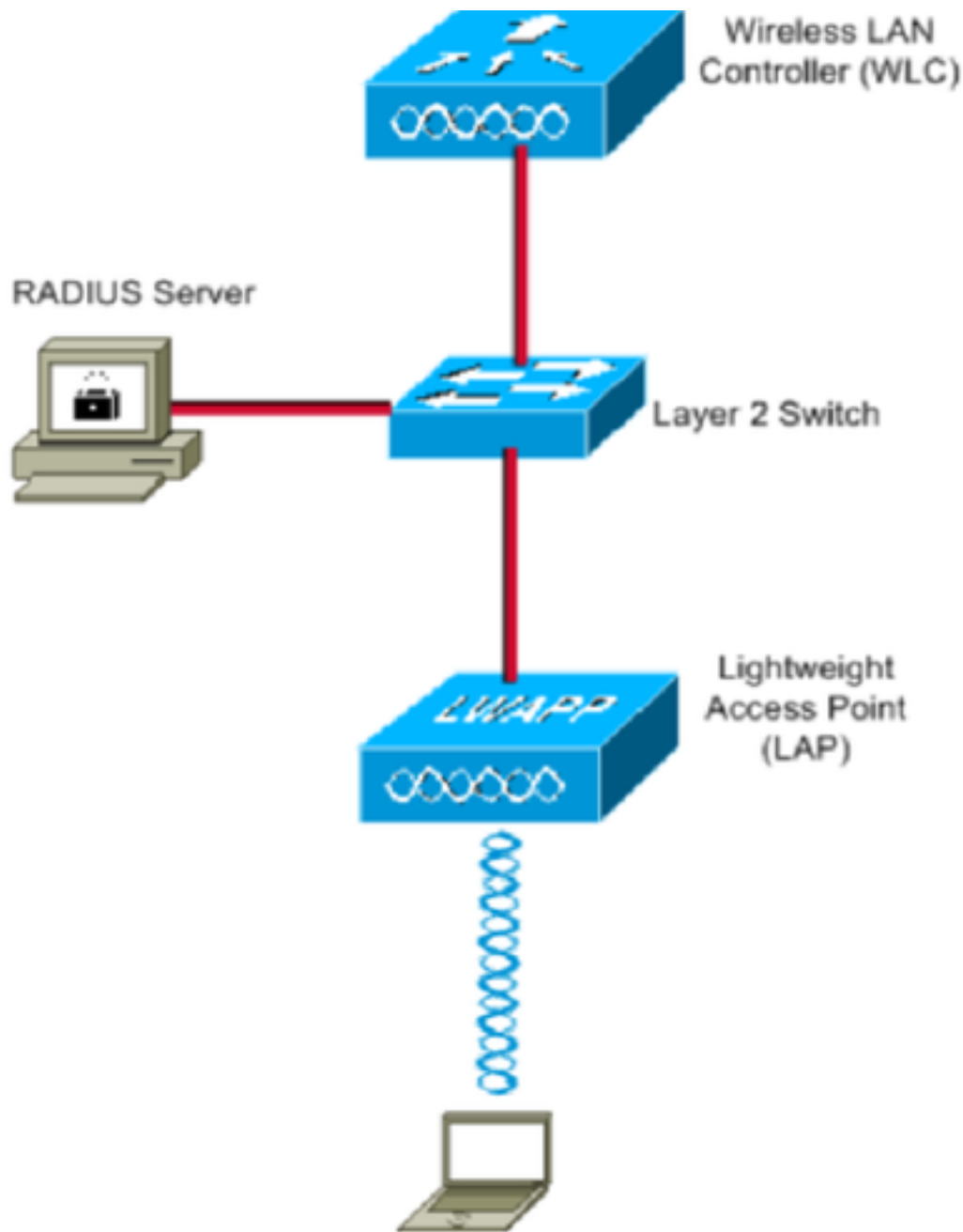
VLAN ID為12位，取值範圍為1到4094 (含1和4094)。由於Tunnel-Private-Group-ID屬於字串型別 (如[RFC2868](#)中定義用於IEEE 802.1X)，因此VLAN ID整數值被編碼為字串。傳送這些隧道屬性時，需要在Tag欄位中輸入它們。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



以下是此圖中所用元件的配置詳細資訊：

- 思科ISE(RADIUS)伺服器的IP地址為10.10.1.24。
- WLC的管理介面地址為10.10.1.17。
- 控制器上的內部DHCP伺服器用於將IP地址分配給無線客戶端。
- 本文使用搭載PEAP的802.1x作為安全機制。
- 整個配置中都使用VLAN102。使用者名稱jonathga-102配置為由RADIUS伺服器置於VLAN102中。

配置步驟

此配置分為三類：

- Cisco ISE配置。
- 為交換機配置多個VLAN。
- Catalyst 9800 WLC組態。

Cisco ISE配置

此配置需要執行以下步驟：

- 將Catalyst WLC配置為Cisco ISE伺服器上的AAA客戶端。
- 在Cisco ISE上配置內部使用者。
- 配置用於思科ISE上的動態VLAN分配的RADIUS(IETF)屬性。

步驟1.將Catalyst WLC配置為Cisco ISE伺服器上的AAA客戶端

以下過程說明如何將WLC新增為ISE伺服器上的AAA客戶端，以便WLC可以將使用者憑證傳遞到ISE。

請完成以下步驟：

1. 從ISE GUI導航至 **Administration > Network Resources > Network Devices**並選擇 **Add**。
2. 使用WLC管理IP地址和WLC與ISE之間的RADIUS共用金鑰完成配置，如下圖所示：

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is **Administration > Network Resources > Network Devices**. The page title is **Network Devices List > New Network Device**. The configuration form includes the following fields and settings:

- Name:** WLC-C9800-CL (highlighted with a red box)
- Description:** vWLC-9800
- IP Address:** 10.10.1.17 (highlighted with a red box)
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
 - Location:** All Locations
 - IPSEC:** No
 - Device Type:** WLC
- RADIUS Authentication Settings:**
 - Protocol:** RADIUS (highlighted with a red box)
 - Shared Secret:** (masked with dots, highlighted with a red box)
 - Use Second Shared Secret:** (unchecked)
 - CoA Port:** 1700

步驟2.在Cisco ISE上配置內部使用者

此過程說明如何在Cisco ISE的內部使用者資料庫上新增使用者。

請完成以下步驟：

1. 從ISE GUI導航至 **Administration > Identity Management > Identities** 並選擇 **Add**.
2. 使用使用者名稱、密碼和使用者組完成配置，如下圖所示：

The screenshot shows the Cisco Identity Services Engine (ISE) GUI for configuring a new Network Access User. The breadcrumb navigation is Administration > Identity Management > Identities > New Network Access User. The configuration form includes the following sections:

- Network Access User:** Name (jonathga-102), Status (Enabled), Email.
- Passwords:** Password Type (Internal Users), Login Password, Re-Enter Password, Enable Password.
- User Information:** First Name, Last Name.
- Account Options:** Description, Change password on next login (checkbox).
- Account Disable Policy:** Disable account if date exceeds (2021-05-18).
- User Groups:** VLAN102.

步驟3.設定用於動態VLAN分配的RADIUS(IETF)屬性

以下步驟說明如何為無線使用者建立授權配置檔案和身份驗證策略。

請完成以下步驟：

1. 從ISE GUI導航至 **Policy > Policy Elements > Results > Authorization > Authorization profiles** 並選擇 **Add** 建立新配置檔案。
2. 使用相應組的VLAN資訊完成授權配置檔案配置。此圖顯示 **jonathga-VLAN-102** 組配置設定。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > jonathga-VLAN-102

Authorization Profile

* Name

Description

Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID ID/Name

Advanced Attributes Settings

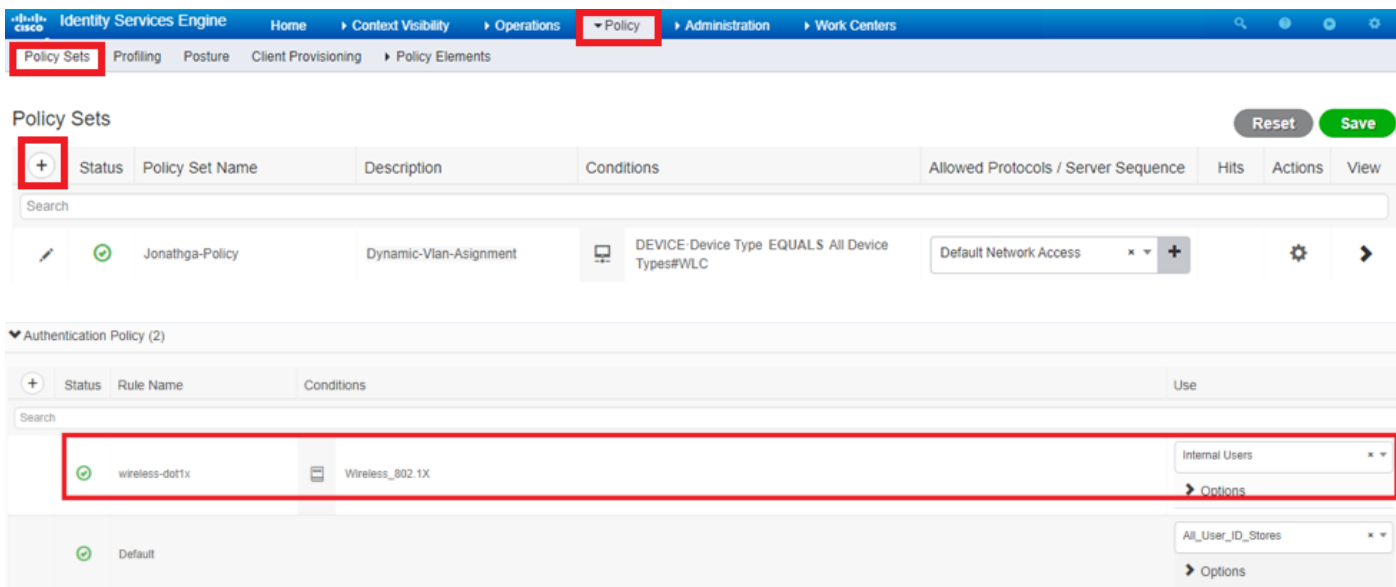
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:102
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

配置授權配置檔案後，需要為無線使用者建立身份驗證策略。您可以使用新的 Custom 策略或修改 Default 策略集。在此示例中，建立自定義配置檔案。

3. 導航至 Policy > Policy Sets 並選擇 Add 如圖所示建立新策略：



現在，您需要為使用者建立授權策略，以便根據組成員資格分配各自的授權配置檔案。

5. 開啟 Authorization policy 分節並建立策略以滿足此要求，如下圖所示：



為多個VLAN配置交換機

若要允許多個VLAN通過交換器，需要發出以下命令，以設定連線到控制器的交換器連線埠：

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

附註：預設情況下，大多數交換機允許通過中繼埠在該交換機上建立所有VLAN。如果有線網路連線到交換器，則此相同組態會套用到連線網路的交換器連線埠。這樣可啟用有線和無線網路中相同VLAN之間的通訊。

Catalyst 9800 WLC組態

此配置需要執行以下步驟：

- 使用驗證伺服器的詳細資訊設定WLC。
- 配置VLAN。
- 配置WLAN(SSID)。
- 配置策略配置檔案。

- 配置策略標籤。
- 將策略標籤分配給AP。

步驟1.使用驗證伺服器的詳細資訊設定WLC

必須設定WLC，才能與RADIUS伺服器通訊以驗證使用者端。

請完成以下步驟：

1. 從控制器GUI導航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 並輸入RADIUS伺服器資訊，如下圖所示：

The screenshot shows the Cisco WLC GUI configuration page for AAA. The navigation path is Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add. The 'Servers / Groups' tab is selected, and the 'RADIUS' section is active. The 'Create AAA Radius Server' dialog is open, with the following fields and values:

Field	Value
Name*	Cisco-ISE
Server Address*	10.10.1.24
PAC Key	<input type="checkbox"/>
Key Type	Clear Text
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100

Additional settings on the right side of the dialog:

- Support for CoA: ENABLED
- CoA Server Key Type: Clear Text
- CoA Server Key:
- Confirm CoA Server Key:
- Automate Tester:

The 'Apply to Device' button is highlighted in red.

2. 若要將RADIUS伺服器新增到RADIUS群組，請導覽至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** 如下圖所示：

Create AAA Radius Server Group



Name*	ISE-SERVER
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Load Balance	<input type="checkbox"/> DISABLED
Source Interface VLAN ID	none

Available Servers

server-2019

Assigned Servers

Cisco-ISE

Cancel

Apply to Device

3. 要建立身份驗證方法清單，請導航至 Configuration > Security > AAA > AAA Method List > Authentication > + Add 如下圖所示：

The screenshot shows the network configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area is titled "Authentication Authorization and Accounting". It features a blue "+ AAA Wizard" button, a blue "AAA Method List" button (highlighted with a red box), and a "Servers / Groups" section. Under "General", the "Authentication" tab is selected (highlighted with a red box). In the "Servers / Groups" table, a blue "+ Add" button is highlighted with a red box. Below the table, a "Name" column header is visible.

Quick Setup: AAA Authentication

Method List Name* ISE-SERVER

Type* dot1x ⓘ

Group Type group ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- radgrp_SykesLab
- server2019
- tacacgrp_SykesLab

Assigned Server Groups

- ISE-SERVER

Cancel Apply to Device

步驟2.配置VLAN

以下程式介紹如何在Catalyst 9800 WLC上設定VLAN。如本檔案前面所述，WLC中還必須存在RADIUS伺服器的Tunnel-Private-Group ID屬性下指定的VLAN ID。

在本示例中，使用者jonathga-102是使用 Tunnel-Private-Group ID of 102 (VLAN =102) 在RADIUS伺服器上。

1. 導航至 Configuration > Layer2 > VLAN > VLAN > + Add 如下圖所示：

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

VLAN

SVI **VLAN** VLAN Group

+ Add × Delete

	VLAN ID	Name
<input type="checkbox"/>	1	defau
<input type="checkbox"/>	100	VLAN
<input type="checkbox"/>	210	VLAN
<input type="checkbox"/>	2602	VLAN

2. 輸入所需的資訊，如下圖所示：

Create VLAN ✕

Create a single VLAN

VLAN ID*

Name

State **ACTIVATED**

IGMP Snooping DISABLED

ARP Broadcast DISABLED

Port Members

Available (2)

- Gi1 ➔
- Gi2 ➔

Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range* - (Ex:5-7)

附註： 如果不指定名稱，VLAN會自動分配名稱VLANXXXX，其中XXXX是VLAN ID。

對所有需要的VLAN重複步驟1和2，完成後可以繼續步驟3。

3. 驗證資料介面中是否允許VLAN。 如果正在使用埠通道，請導航至 **Configuration > Interface > Logical > PortChannel name > General**. 如果您看到它配置為 **Allowed VLAN = All** 配置完畢。 如果您看到 **Allowed VLAN = VLANs IDs** 新增所需的VLAN，並在之後選擇 **Update & Apply to Device**. 如果沒有使用埠通道，請導航至 **Configuration > Interface > Ethernet > Interface Name > General**. 如果您看到它配置為 **Allowed VLAN = All** 配置完畢。 如果您看到 **Allowed VLAN = VLANs IDs** 新增所需的VLAN，並在之後選擇 **Update & Apply to Device**.

如果您使用全部或特定VLAN ID，此映像將顯示與介面設定相關的組態。

General

Advanced

Interface

GigabitEthernet3

Description

(1-200 Characters)

Admin Status

UP 

Port Fast

disable ▼

Enable Layer 3 Address

DISABLED

Switchport Mode

trunk ▼

Allowed Vlan


All Vlan IDs

Native Vlan

▼

General

Advanced

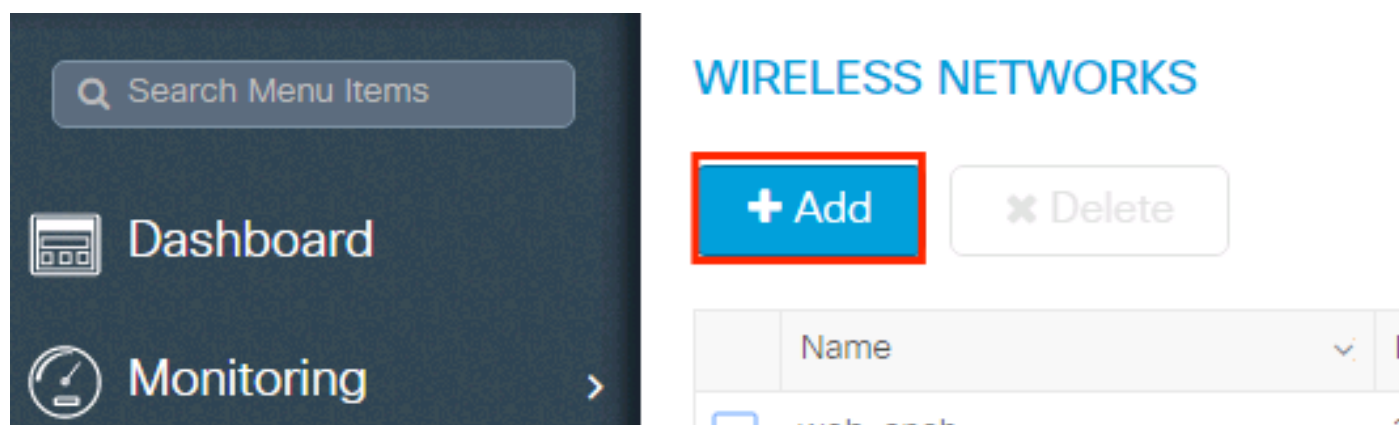
Interface	GigabitEthernet1	
Description	<input type="text"/>	(1-200 Characters)
Speed	1000	▼
Admin Status	UP 	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	trunk ▼	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	551,102,105	(e.g. 1,2,4,6-10)
Native Vlan	551 ▼	

步驟3.配置WLAN(SSID)

以下程式說明如何在WLC中設定WLAN。

請完成以下步驟：

1. 以便建立WLAN。導航至 **Configuration > Wireless > WLANs > + Add** 並根據需要配置網路，如下圖所示：



2. 輸入WLAN資訊，如下圖所示：

Add WLAN ✕

General Security Advanced

Profile Name* Dinamyc-VLAN

SSID* Dinamyc-VLAN

WLAN ID* 6

Status **ENABLED**

Radio Policy All

Broadcast SSID **ENABLED**

3. 導航至 **Security** 頁籤並選擇所需的安全方法。在此例中，WPA2 + 802.1x (如圖所示) :

Add WLAN ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode **WPA + WPA2**

MAC Filtering

Protected Management Frame

PMF Disabled

WPA Parameters

WPA Policy

Fast Transition Adaptive Enab...

Over the DS

Reassociation Timeout 20

Add WLAN

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

自 **Security > AAA** 頁籤，從中選擇在步驟3中建立的身份驗證方法 **Configure the WLC with the Details of the Authentication Server** 一節，如下圖所示：

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication

Cancel Apply to Device

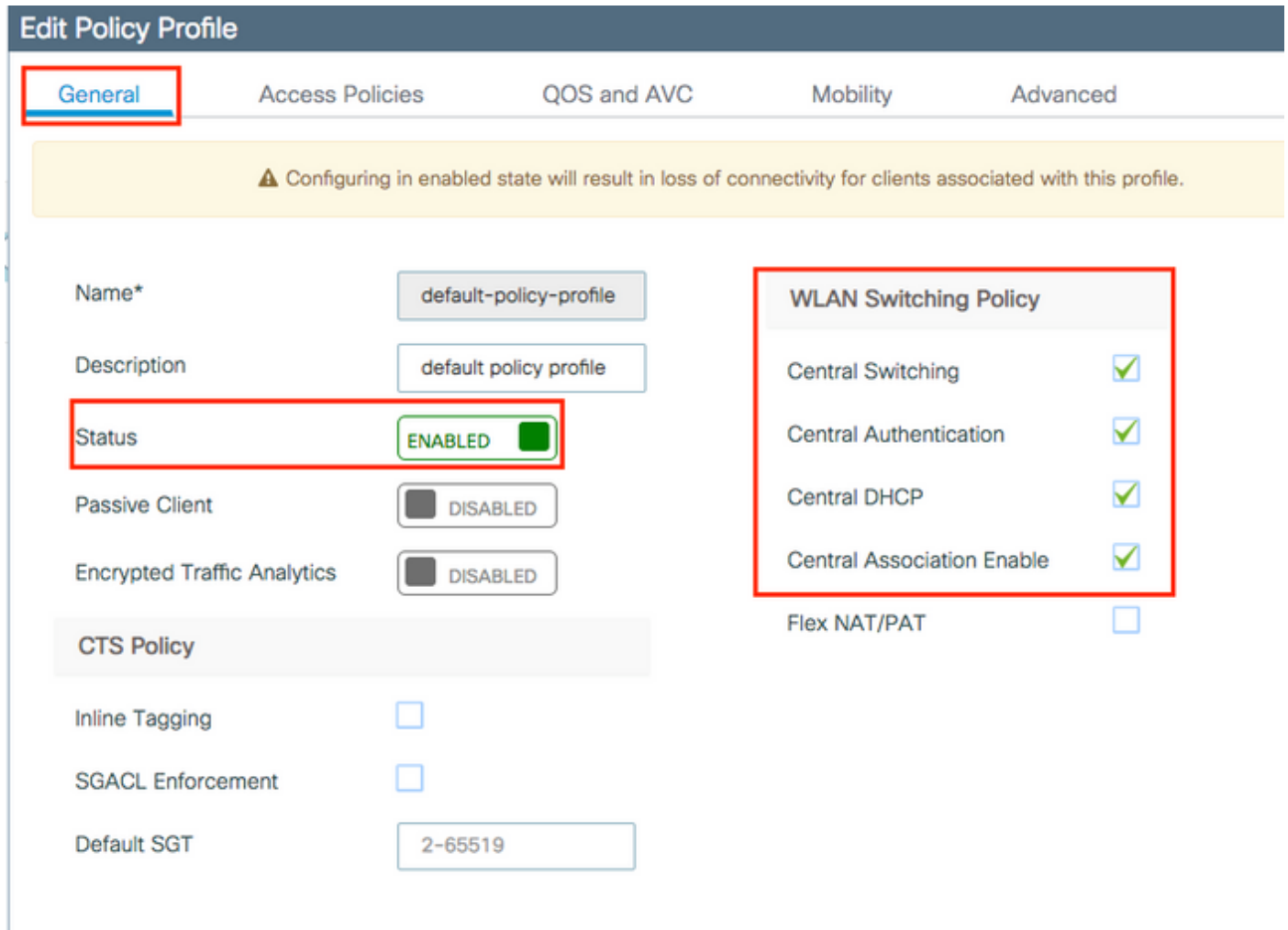
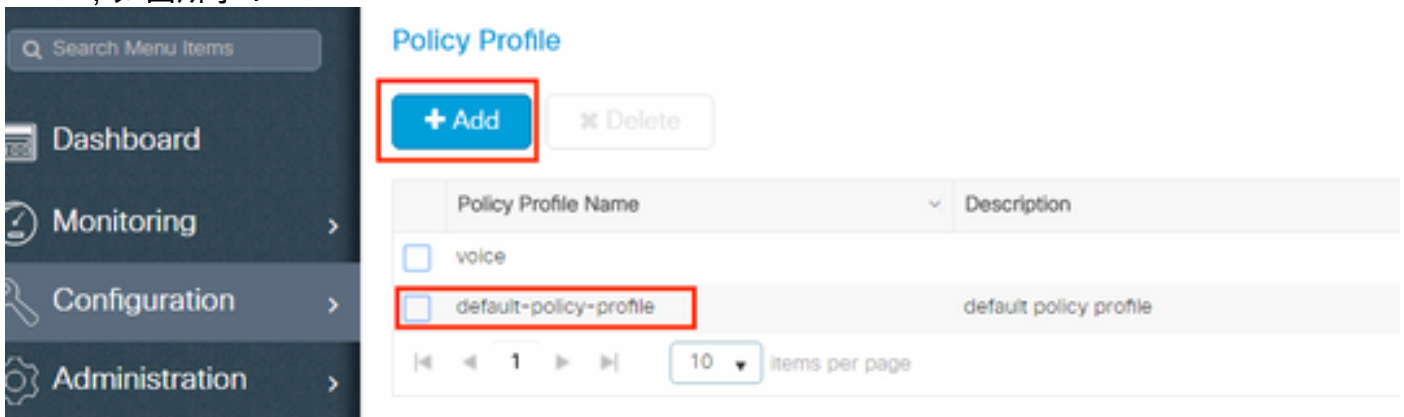
步驟4.配置策略配置檔案

以下程式說明如何在WLC中設定原則設定檔。

請完成以下步驟：

1. 導航至 **Configuration > Tags & Profiles > Policy Profile** 配置您的 **default-policy-profile** 或建立一個新檔案

, 如圖所示 :



2. 從 **Access Policies** 頁籤指定無線客戶端在預設情況下連線到此WLAN時分配到的VLAN , 如下圖所示 :

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

附註：在提供的示例中，RADIUS伺服器的任務是在身份驗證成功時將無線客戶端分配給特定VLAN，因此策略配置檔案中配置的VLAN可以是黑洞VLAN，RADIUS伺服器會覆蓋此對映並將通過該WLAN的使用者分配到RADIUS伺服器中user Tunnel-Group-Private-ID欄位中指定的VLAN。

3. 從 **Advance** 頁籤，啟用 **Allow AAA Override** 覈取方塊，以在RADIUS伺服器傳回將使用者端放在正確的VLAN上所需的屬性時覆寫WLC組態，如下圖所示：

Edit Policy Profile

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile Search or Select

Umbrella Parameter Map Not Configured

mDNS Service Policy default-mdns-servic [Clear](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

5 GHz Policy Search or Select

Cancel Update & Apply to Device

步驟5.配置策略標籤

以下步驟說明如何在WLC中設定原則標籤。

請完成以下步驟：

1. 導航至 Configuration > Tags & Profiles > Tags > Policy 並在需要時新增一個，如下圖所示：

Manage Tags

Policy Site RF AP

+ Add x Delete

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

10 items per page

2. 向策略標籤新增名稱並選擇 +Add，如下圖所示：

Add Policy Tag

Name* Dynamic-VLAN

Description Enter Description

WLAN-POLICY Maps: 0

+ Add x Delete

WLAN Profile	Policy Profile
0 items per page No items to display	

3. 將您的WLAN配置檔案連結到所需的策略配置檔案，如下圖所示：

Add Policy Tag

Name* Dynamic-VLAN

Description Enter Description

WLAN-POLICY Maps: 0

+ Add x Delete

WLAN Profile	Policy Profile
0 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Dinamyc-VLAN

Policy Profile* default-policy-profil

x ✓

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> Dinamyc-VLAN	default-policy-profile

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

> RLAN-POLICY Maps: 0

步驟6.為AP分配策略標籤

以下步驟說明如何在WLC中設定原則標籤。

請完成以下步驟：

1. 導航至 **Configuration > Wireless > Access Points > AP Name > General Tags** 並分配相關的策略標籤，然後選擇 **Update & Apply to Device** 如下圖所示：

Edit AP
✕

General
Interfaces
High Availability
Inventory
ICap
Advanced

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Tags

Policy

Site

Version

Primary Software Version

Predownloaded Status

Predownloaded Version

Next Retry Time

Boot Version

IOS Version

Mini IOS Version

IP Config

CAPWAP Preferred Mode

DHCP IPv4 Address

Static IP (IPv4/IPv6)

Time Statistics

Up Time

Controller Association Latency

↶ Cancel

注意：請注意，當AP上的策略標籤發生更改時，它會丟棄與WLC的關聯並連線回來。

驗證

使用本節內容，確認您的組態是否正常運作。

測試與Windows 10和本地請求方的連線，在提示您輸入使用者名稱和密碼後，輸入對映到ISE上VLAN的使用者資訊。

在上一個示例中，請注意jonathga-102已分配給RADIUS伺服器中指定的VLAN102。此範例使用此使用者名稱來接收驗證，並由RADIUS伺服器指派給VLAN:

完成驗證後，您需要確認您的使用者端是否根據傳送的RADIUS屬性分配到適當的VLAN。完成以下步驟即可完成此任務：

1. 從控制器GUI導航至 **Monitoring > Wireless > Clients > Select the client MAC address > General > Security**

Information 並尋找VLAN欄位，如下圖所示：

The screenshot shows the Cisco Catalyst GUI for monitoring wireless clients. On the left, a table lists the client details: Client MAC Address (b88a.6010.3c60), IPv4 Address (10.10.102.121), and IPv6 Address (fe80::d8a2:dc93:3758:6...). On the right, the 'Client' configuration page is shown, with the 'General' tab selected. The 'Security Information' section is highlighted with a red box, showing 'VLAN' set to '102'. The 'Server Policies' section is also highlighted with a red box, showing 'VLAN' set to '102' and 'Resultant Policies' showing 'VLAN Name' as 'VLAN0102' and 'VLAN' as '102'.

在此視窗中，您可以看到此使用者端是按照RADIUS伺服器上設定的RADIUS屬性指派給VLAN102。您可以在CLI中使用 `show wireless client summary detail` 如圖所示檢視相同資訊：

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
-----
MAC Address      SSID          AP Name      State  IP Address      Device-type  VLAN
BSSID           Auth Method  Created     Connected Protocol Channel Width SGI NSS Rate CAP Username
-----
[REDACTED] 10.3c60 [Dinamyc-VLAN] AIR-AP2802I-A-R9 Run 10.10.105.200 Intel-Device 105
[REDACTED] 44.4000 [802.1X] 05 06 11n(2.4) 1 20/20 Y/Y 1/1 24.0 E jonathga-105

Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
-----
MAC Address      SSID          AP Name      State  IP Address      Device-type  VLAN
BSSID           Auth Method  Created     Connected Protocol Channel Width SGI NSS Rate CAP Username
-----
[REDACTED] 10.3c60 [Dinamyc-VLAN] AIR-AP2802I-A-R9 Run 10.10.102.121 Intel-Device 102
[REDACTED] 44.4000 [802.1X] 54 55 11n(2.4) 1 20/20 Y/Y 1/1 m5 E jonathga-102
```

2. 可以啟用 **Radioactive traces** 以確保RADIUS屬性成功傳輸到WLC。為此，請執行以下步驟：從控制器GUI導航至 **Troubleshooting > Radioactive Trace > +Add**.輸入無線客戶端的Mac地址。選擇 **Start**.將使用者端連線到WLAN。導航至 **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

此部分的追蹤輸出可確保成功傳輸RADIUS屬性：

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: User-Name
[1] 13 "jonathga-102"
```

```

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: State
[24] 40 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class
[25] 54 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type
[64] 6 VLAN [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type
[65] 6 ALL_802 [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message
[79] 6 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-
Authenticator[80] 18 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-
Group-Id[81] 6 "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name
[102] 67 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key
[16] 52 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key
[17] 52 *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: username 0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: class 0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30 ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: tunnel-type 1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type 1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id 1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: timeout 0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile

```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [最終使用手冊](#)