

配置9800 WLC與Aruba ClearPass - Dot1x &適用於分支機構部署的FlexConnect

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[流量](#)

[網路圖表](#)

[設定Catalyst 9800無線控制器](#)

[C9800 — 為dot1x配置AAA引數](#)

[C9800 — 配置「公司」WLAN配置檔案](#)

[C9800 — 配置策略配置檔案](#)

[C9800 — 配置策略標籤](#)

[C9800 - AP加入配置檔案](#)

[C9800 - Flex設定檔](#)

[C9800 — 站點標籤](#)

[C9800 - RF標籤](#)

[C9800 — 為AP分配標籤](#)

[配置Aruba CPPM](#)

[Aruba ClearPass策略管理器伺服器初始配置](#)

[應用許可證](#)

[新增C9800無線控制器作為網路裝置](#)

[配置CPPM以使用Windows AD作為身份驗證源](#)

[配置CPPM Dot1X身份驗證服務](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹Catalyst 9800無線控制器與Aruba ClearPass策略管理器(CPPM)和Microsoft Active Directory(AD)的整合，以在Flexconnect部署中向無線客戶端提供dot1x身份驗證。

必要條件

需求

思科建議您瞭解以下主題，並且這些主題已經過配置和驗證：

- Catalyst 9800無線控制器
- Aruba ClearPass Server (需要平台許可證、訪問許可證、板載許可證)
- 可運行的Windows AD
- 可選證書頒發機構(CA)
- 可操作的DHCP伺服器
- 可操作的DNS伺服器 (證書CRL驗證所必需的)
- ESXi
- 所有相關元件均同步到NTP並驗證其時間是否正確 (驗證證書時需要)
- 主題知識： C9800部署和新配置模型C9800上的FlexConnect操作 Dot1x驗證

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

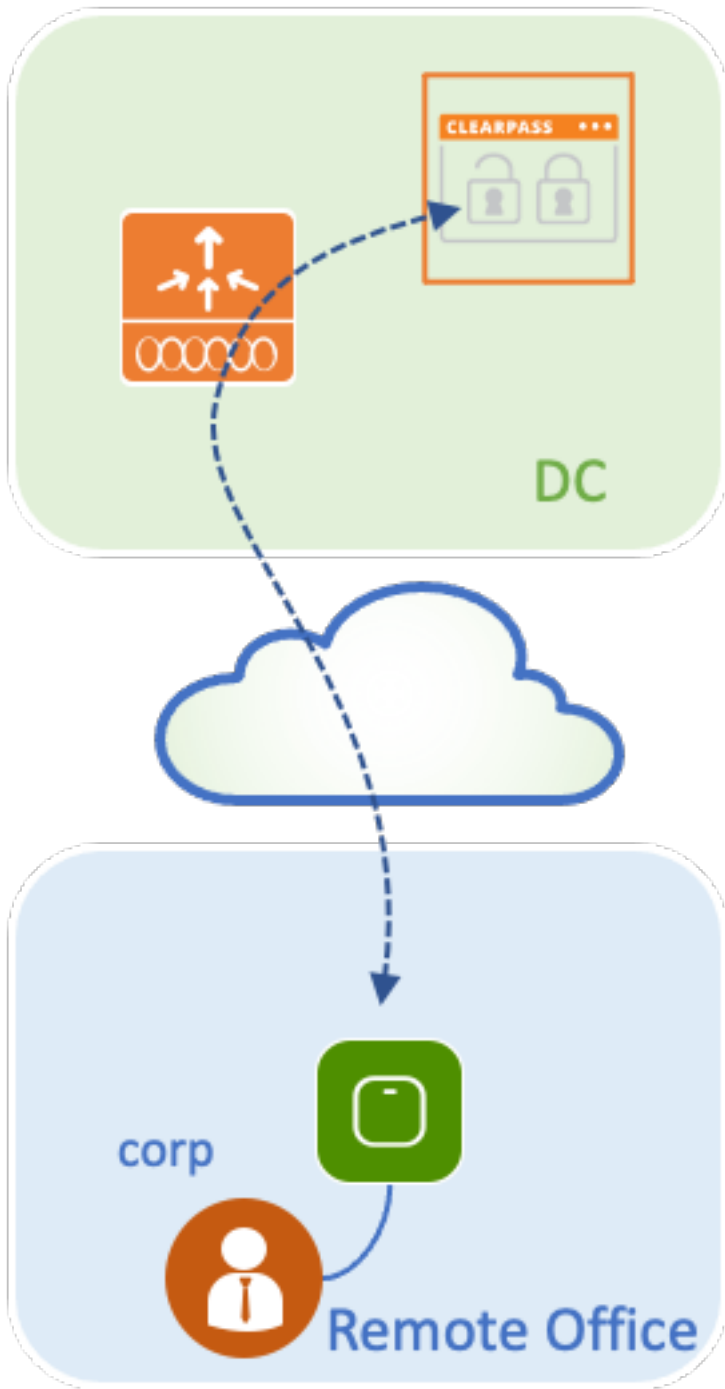
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX、4800 AP
- Aruba ClearPass , 6-8-0-109592和6.8-3修補程式
- MS Windows伺服器 Active Directory (GP配置為向託管端點自動發出基於電腦的證書) 帶有選項43和選項60的DHCP伺服器DNS伺服器NTP伺服器可對所有元件進行時間同步CA

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。

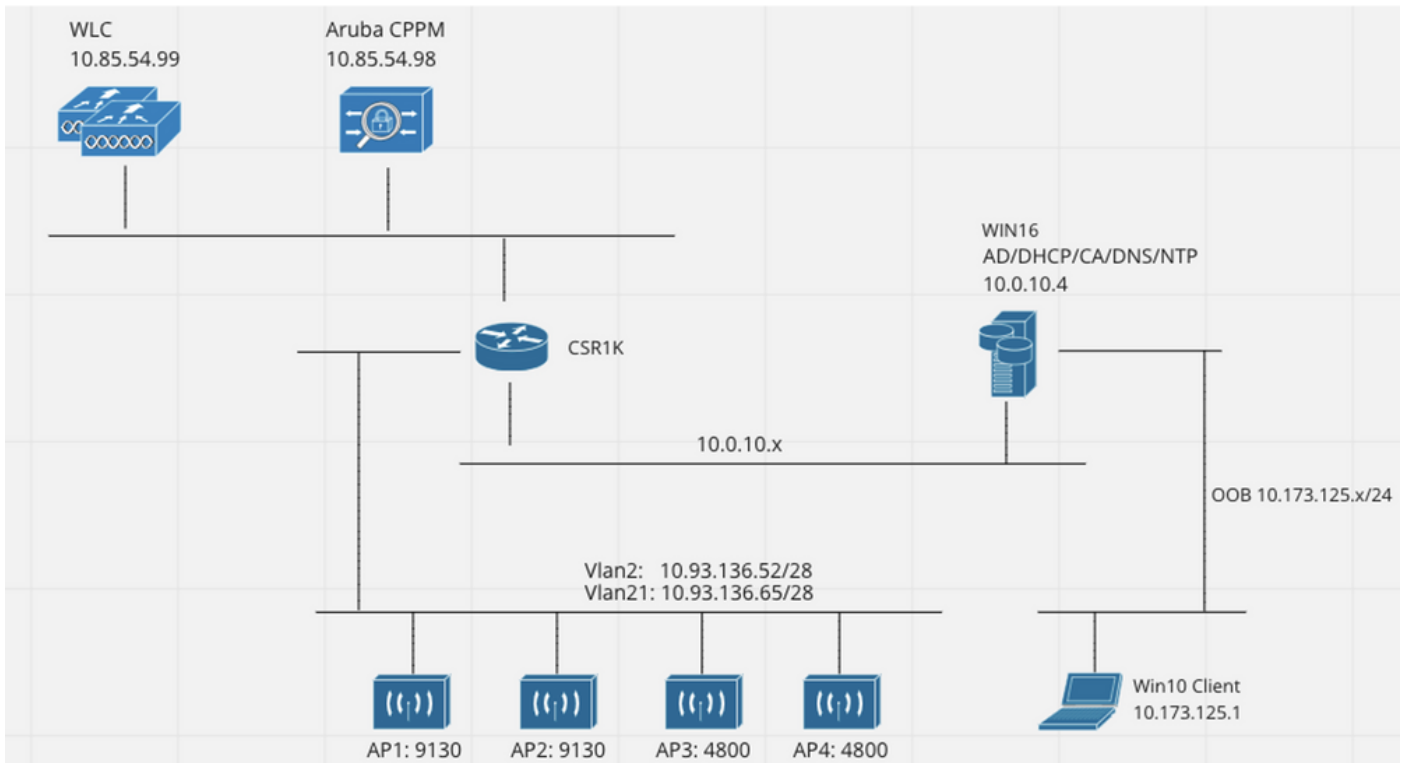
背景資訊

流量

在具有多個分支機構的典型企業部署中，每個分支機構都設定為向企業員工提供dot1x訪問許可權。在此配置示例中，PEAP用於通過部署在中央資料中心(DC)中的ClearPass例項為企業使用者提供dot1x訪問許可權。電腦證書與針對Microsoft AD伺服器的員工憑據驗證結合使用。

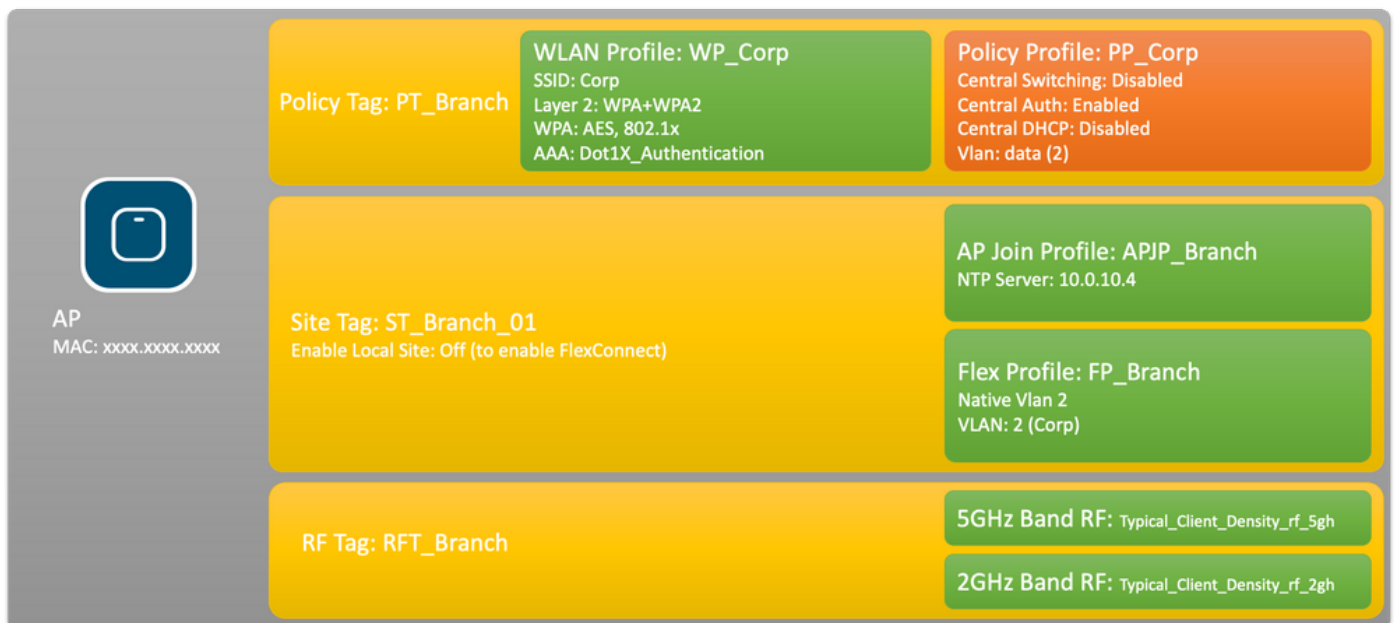


網路圖表



設定Catalyst 9800無線控制器

在此配置示例中，利用C9800上的新配置模型來建立必要的配置檔案和標籤，從而為企業分支機構提供dot1x企業訪問。結果配置總結在圖中。



C9800 — 為dot1x配置AAA引數

步驟1.將Aruba ClearPass Policy Manager 'Corp'伺服器新增到9800 WLC配置中。導覽至 **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers**。單擊**Add**並輸入RADIUS伺服器資訊。按一下**Apply to Device**按鈕，如下圖所示。

Create AAA Radius Server ✕

Name*

Server Address*

PAC Key

Key Type

Key*

Confirm Key*

Auth Port

Acct Port

Server Timeout (seconds)

Retry Count

Support for CoA ENABLED

步驟2.為企業使用者定義AAA伺服器組。導航到Configuration > Security > AAA > Servers/Groups > RADIUS > Groups，然後單擊+Add，輸入RADIUS伺服器組名並分配RADIUS伺服器資訊。按一下「Apply to Device」按鈕，如下圖所示。

Create AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers

- CPPM_Guest

Assigned Servers

- CPPM_Corp

步驟3.為公司使用者定義dot1x身份驗證方法清單。導覽至Configuration > Security > AAA > AAA Method List > Authentication，然後單擊+Add。從下拉選單中選擇型別dot1x。按一下應用到裝置按鈕，如下圖所示。

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- WLC_Tacacs_Servers
- AAA_Group_Guest

Assigned Server Groups

- AAA_Group_Corp

C9800 — 配置「公司」WLAN配置檔案

步驟1.導覽至Configuration > Tags & Profiles > Wireless，然後單擊+Add。輸入配置檔名稱、SSID 'Corp'和尚未使用的WLAN ID。

Add WLAN

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID

WLAN ID*

Status

步驟2.導覽至Security索引標籤和Layer2子標籤。無需更改此配置示例的任何預設引數。

The screenshot shows the 'Add WLAN' configuration interface with the 'Security' tab selected. The 'Layer2' sub-tab is also selected. The configuration includes the following settings:

- Layer 2 Security Mode: WPA + WPA2
- MAC Filtering:
- Protected Management Frame:
- PMF: Disabled
- WPA Parameters:
- WPA Policy:
- WPA2 Policy:
- GTK Randomize:
- OSEN Policy:
- WPA2 Encryption: AES(CCMP128), CCMP256, GCMP128, GCMP256
- Auth Key Mgmt: 802.1x, PSK, CCKM, FT + 802.1x, FT + PSK, 802.1x-SHA256, PSK-SHA256
- Lobby Admin Access:
- Fast Transition: Adaptive Enab...
- Over the DS:
- Reassociation Timeout: 20
- MPSK Configuration:

At the bottom of the page, there is a 'Cancel' button on the left and an 'Apply to Device' button on the right.

步驟3.導航到AAA子頁籤，然後選擇之前配置的身份驗證方法清單。按一下「Apply to Device」按鈕，如下圖所示。

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ▼ ⓘ

Local EAP Authentication

↶ Cancel Apply to Device

C9800 — 配置策略配置檔案

步驟1。導覽至Configuration > Tags & Profiles > Policy，然後按一下+Add，並輸入策略配置檔名稱和說明。啟用策略，並禁用集中交換、DHCP和關聯，因為公司使用者流量在AP進行本地交換，如下圖所示。

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

General	Access Policies	QOS and AVC	Mobility	Advanced
Name*	<input type="text" value="PP_Corp"/>			WLAN Switching Policy
Description	<input type="text" value="Policy Profile for Corp"/>			Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> ENABLED			Central Authentication <input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED			Central DHCP <input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED			Central Association <input type="checkbox"/> DISABLED
CTS Policy				Flex NAT/PAT <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>			
SGACL Enforcement	<input type="checkbox"/>			
Default SGT	<input type="text" value="2-65519"/>			

步驟2. 導航到訪問策略頁籤，然後手動輸入要在分支機構用於企業使用者流量的VLAN的ID。此VLAN無需在C9800上配置。必須在彈性配置檔案中對其進行配置，詳見。請勿從下拉選單中選擇VLAN名稱(請參閱思科錯誤ID [CSCvn48234](#) 瞭解更多資訊)。按一下「Apply to Device」按鈕，如下圖所示。

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

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
WLAN Local Profiling				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="2"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
				WLAN ACL
				IPv4 ACL <input type="text" value="Search or Select"/>
				IPv6 ACL <input type="text" value="Search or Select"/>
URL Filters				
				Pre Auth <input type="text" value="Search or Select"/>
				Post Auth <input type="text" value="Search or Select"/>
<input type="button" value="Cancel"/>				<input type="button" value="Apply to Device"/>

C9800 — 配置策略標籤

建立WLAN配置檔案(WP_Corp)和策略配置檔案(PP_Corp)後，必須依次建立策略標籤以將這些WLAN和策略配置檔案繫結在一起。此策略標籤應用於接入點。將此策略標籤分配給接入點，以觸發這些接入點的配置，從而在其上啟用選定的SSID。

步驟1. 導航到Configuration > Tags & Profiles > Tags，選擇Policy頁籤並按一下+Add。輸入策略標籤名稱和說明。在WLAN-POLICY Maps下按一下+Add。選擇之前建立的WLAN配置檔案和策略配置檔案，然後按一下複選標籤按鈕，如下圖所示。

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

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

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

步驟2. 驗證並點選Apply to Device按鈕，如下圖所示。

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WP_Corp	PP_Corp

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

➤ RLAN-POLICY Maps: 0

C9800 - AP加入配置檔案

需要配置接入點加入配置檔案和彈性配置檔案，並將其分配到具有站點標籤的接入點。對於每個分支，必須使用不同的站點標籤，才能支援分支內的802.11r快速過渡(FT)，同時限制客戶端PMK僅在該分支的AP之間的分配。在多個分支之間重複使用相同的站點標籤非常重要。配置AP加入配置檔案。如果所有分支都類似，則可以使用單個AP連線配置檔案；如果某些配置的引數必須不同，則可以使用多個配置檔案。

步驟1. 導航到**配置>標籤和配置檔案> AP加入**，然後按一下**+Add**。輸入AP加入配置檔名稱和說明。按一下「**Apply to Device**」按鈕，如下圖所示。

Add AP Join Profile ✕

General Client CAPWAP AP Management Security ICap QoS

Name*	APJP_Branch	OfficeExtend AP Configuration	
Description	Profiles for branches	Local Access	<input checked="" type="checkbox"/>
LED State	<input checked="" type="checkbox"/>	Link Encryption	<input checked="" type="checkbox"/>
LAG Mode	<input type="checkbox"/>	Rogue Detection	<input type="checkbox"/>
NTP Server	0.0.0.0		
GAS AP Rate Limit	<input type="checkbox"/>		
Apphost	<input type="checkbox"/>		

↶ Cancel **Apply to Device**

C9800 - Flex設定檔

現在配置Flex配置檔案。同樣地，如果所有分支類似，並且具有相同的VLAN/SSID對映，則可以使用單個配置檔案。或者，如果某些配置的引數（如VLAN分配）不同，則可以建立多個配置檔案。

步驟1. 導覽至Configuration > Tags & Profiles > Flex，然後單擊+Add。輸入Flex配置檔名稱和說明。

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name*	FP_Branch	Fallback Radio Shut	<input type="checkbox"/>
Description	Flex Profile for branches	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	1	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	Search or Select ▼
CTS Profile Name	default-sxp-profile ✕ ▼		

↶ Cancel **Apply to Device**

步驟2. 導覽至VLAN索引標籤，然後按一下+Add。輸入位於分支的本地VLAN的VLAN名稱和ID，AP必須使用該資訊在本地交換企業使用者流量。按一下「Save」按鈕，如下圖所示。

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
◀ ◀ 0 ▶ ▶	10	items per page

No items to display

VLAN Name*

VLAN Id*

ACL Name

✓ Save ↻ Cancel

↻ Cancel 📄 Apply to Device

步驟3.驗證並點選Apply to Device按鈕，如下圖所示。

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input checked="" type="checkbox"/> CorpData	2	

◀ ◀ 1 ▶ ▶ items per page

1 - 1 of 1 items

↻ Cancel **📄 Apply to Device**

C9800 — 站點標籤

站點標籤用於將加入配置檔案和Flex配置檔案分配給接入點。如前所述，每個分支必須使用不同的站點標籤，以支援分支內的802.11r快速過渡(FT)，但僅限制客戶端PMK在該分支的AP之間的分配。在多個分支之間不要重複使用相同的站點標籤。

步驟1.導航到**Configuration > Tags & Profiles > Tags**，選擇**Site**頁籤，然後按一下**+Add**。輸入站點標籤名稱和說明，選擇建立的AP加入配置檔案，取消選中**Enable Local Site**框，最後選擇先前建立的Flex配置檔案。取消選中**Enable Local Site**框，將接入點從**Local Mode**更改為**FlexConnect**。最後，按一下**Apply to Device**按鈕，如下圖所示。

Add Site Tag✕

Name*	<input type="text" value="ST_Branch_01"/>
Description	<input type="text" value="Site Tag for Branch 01"/>
AP Join Profile	<input type="text" value="APJP_Branch"/> ▼
Flex Profile	<input type="text" value="FP_Branch"/> ▼
Fabric Control Plane Name	<input type="text"/> ▼
Enable Local Site	<input checked="" type="checkbox"/>

↶ Cancel

📄 Apply to Device

C9800 - RF標籤

步驟1. 導覽至Configuration > Tags & Profiles > Tags，選擇RF頁籤，然後按一下+Add。為RF標籤輸入名稱和說明。從下拉選單中選擇系統定義的RF配置檔案。按一下「Apply to Device」按鈕，如下圖所示。

Add RF Tag✕

Name*	<input type="text" value="RFT_Branch"/>
Description	<input type="text" value="RF in Typical Branch"/>
5 GHz Band RF Profile	<input type="text" value="Typical_Client_Densi"/> ▼
2.4 GHz Band RF Profile	<input type="text" value="Typical_Client_Densi"/> ▼

↶ Cancel

📄 Apply to Device

C9800 — 為AP分配標籤

現在，已經建立了包括配置接入點所需的各種策略和配置檔案的標籤，我們必須將它們分配給接入點。本節介紹如何根據接入點的乙太網MAC地址手動執行分配給該接入點的靜態標籤。對於產品生產環境，建議使用Cisco DNA Center AP PNP工作流，或使用9800中提供的靜態批次CSV上傳方法。

步驟1. 導航到配置>標籤和配置檔案>標籤，選擇AP頁籤，然後選擇Static頁籤。按一下+Add並輸入AP MAC地址，然後選擇先前定義的策略標籤、站點標籤和RF標籤。按一下Apply to Device按鈕，如下圖所示。

Associate Tags to AP ✕

AP MAC Address*	<input type="text" value="380e.4dbf.589a"/>
Policy Tag Name	<input type="text" value="PT_Branch"/>
Site Tag Name	<input type="text" value="ST_Branch_01"/>
RF Tag Name	<input type="text" value="RFT_Branch"/>

配置Aruba CPPM

Aruba ClearPass策略管理器伺服器初始配置

Aruba clearpass通過OVF模板在ESXi伺服器上部署，具有以下資源：

- 2個保留的虛擬CPU
- 6 GB RAM
- 80 GB磁碟（必須在初始虛擬機器部署後手動新增，然後才能開啟電腦）

應用許可證

通過以下方式應用平台許可證：**管理>伺服器管理器>許可**。新增訪問和板載

新增C9800無線控制器作為網路裝置

導覽至**Configuration > Network > Devices > Add**，如下圖所示。

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: >WLC-10.85.54.99

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: LAB WLC 9800

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

Enable RADIUS Dynamic Authorization: Port: 1700

Enable RadSec:

Copy Save Cancel

配置CPPM以使用Windows AD作為身份驗證源

導覽至Configuration > Authentication > Sources > Add。選擇型別：下拉菜單中的Active Directory，如下圖所示。

aruba ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Name: LAB_AD

Description:

Type: Active Directory

Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: -- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: Add Backup Remove

配置CPPM Dot1X驗證服務

步驟1。建立與多個RADIUS屬性相符的「服務」：

- Radius:IETF |名稱：NAS-IP-Address |等於 | <IP地址>
- Radius:IETF |名稱：Service-Type |等於 | 1、2、8

步驟2.對於生產環境，建議匹配SSID名稱而不是「NAS-IP-Address」，以便多WLC部署滿足一個

條件。Radius: Cisco: Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID

ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Name: DOT1X

Description: 802.1X Wireless Access Service

Type: 802.1X Wireless

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-IP-Address	EQUALS	10.85.54.99
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...		

ClearPass Policy Manager

Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Summary Service Authentication Roles Enforcement

Authentication Methods:

- EAP PEAP]
- EAP FAST]
- EAP TLS]
- EAP TTLS]

--Select to Add--

Authentication Sources:

- LAB AD (Active Directory]

--Select to Add--

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefix

Service Certificate: --Select to Add--

驗證

目前沒有適用於此組態的驗證程序。

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

- [思科9800部署最佳實踐指南](#)
- [瞭解Catalyst 9800無線控制器組態型號](#)

- [瞭解Catalyst 9800無線控制器上的FlexConnect](#)
- [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）。