

# Configurazione dell'integrazione WLC 9800 con Aruba ClearPass - Dot1x & Installazione di FlexConnect per filiali

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso traffico](#)

[Esempio di rete](#)

[Configurazione del controller wireless Catalyst 9800](#)

[C9800 - Configurazione dei parametri AAA per dot1x](#)

[C9800 - Configurazione del profilo WLAN aziendale](#)

[C9800 - Configura profilo criteri](#)

[C9800 - Configura tag criteri](#)

[C9800 - Profilo di join AP](#)

[C9800 - Flex Profile](#)

[C9800 - Tag sito](#)

[C9800 - Tag RF](#)

[C9800 - Assegna tag all'access point](#)

[Configurazione di Aruba CPPM](#)

[Configurazione iniziale del server Aruba ClearPass Policy Manager](#)

[Applica licenze](#)

[Aggiunta del controller wireless C9800 come dispositivo di rete](#)

[Configurare CPPM per l'utilizzo di Windows AD come origine di autenticazione](#)

[Configura servizio di autenticazione CPPM Dot1X](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritta l'integrazione del controller wireless Catalyst 9800 con Aruba ClearPass Policy Manager (CPPM) e Microsoft Active Directory (AD) per fornire l'autenticazione dot1x ai client wireless in un'implementazione di Flexconnect.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti, che sono stati configurati e verificati:

- Catalyst 9800 Wireless Controller
- Aruba ClearPass Server (richiede licenza della piattaforma, licenza di accesso, licenza integrata)
- AD Windows operativo
- CA (Certification Authority) opzionale
- Server DHCP operativo
- Server DNS operativo (necessario per la convalida CRL certificato)
- ESXi
- Tutti i componenti pertinenti vengono sincronizzati con NTP e verificati per verificare che abbiano l'ora corretta (necessaria per la convalida del certificato)
- Conoscenza degli argomenti: Distribuzione C9800 e nuovo modello di configurazione  
Funzionamento di FlexConnect su C9800 Autenticazione Dot1x

## Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

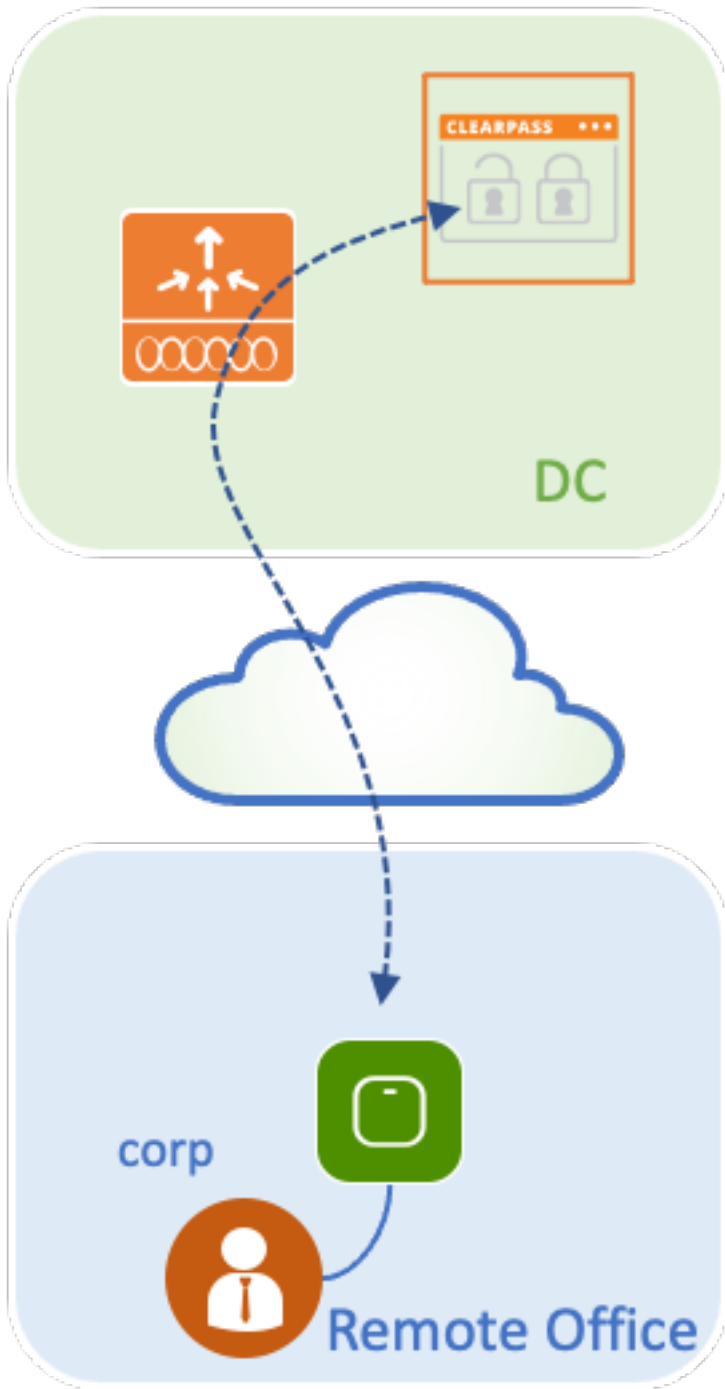
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 AP
- Aruba ClearPass, patch 6-8-0-109592 e 6.8-3
- Server MS Windows Active Directory (Criteri di gruppo configurati per il rilascio automatico di certificati basati su computer agli endpoint gestiti) Server DHCP con opzione 43 e opzione 60 Server DNS Server NTP per sincronizzare l'ora di tutti i componenti CA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

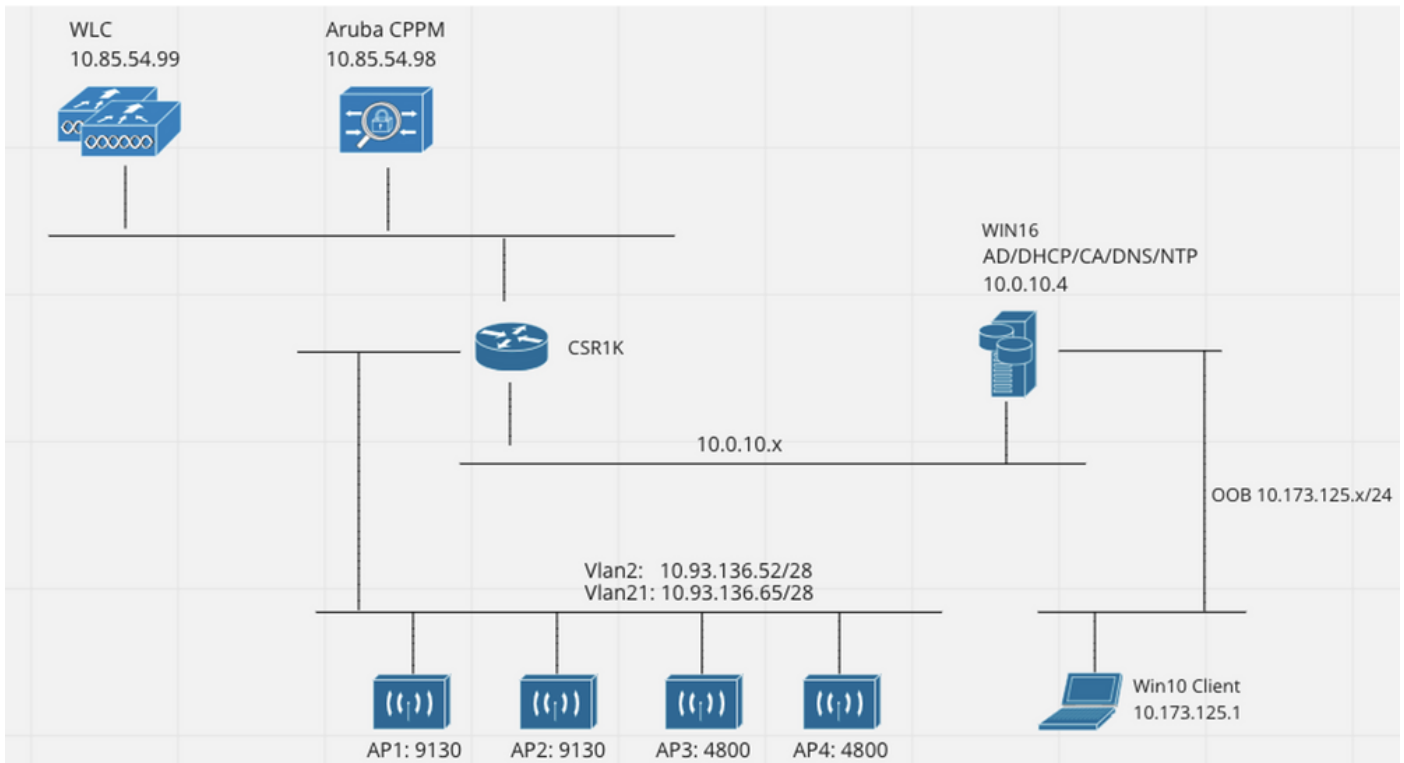
## Premesse

### Flusso traffico

In una tipica implementazione aziendale con più filiali, ogni filiale è configurata per fornire accesso dot1x ai dipendenti aziendali. In questo esempio di configurazione, PEAP viene utilizzato per fornire accesso dot1x agli utenti aziendali tramite un'istanza ClearPass implementata nel centro dati centrale (DC). I certificati del computer vengono utilizzati insieme alla verifica delle credenziali dei dipendenti in un server AD Microsoft.

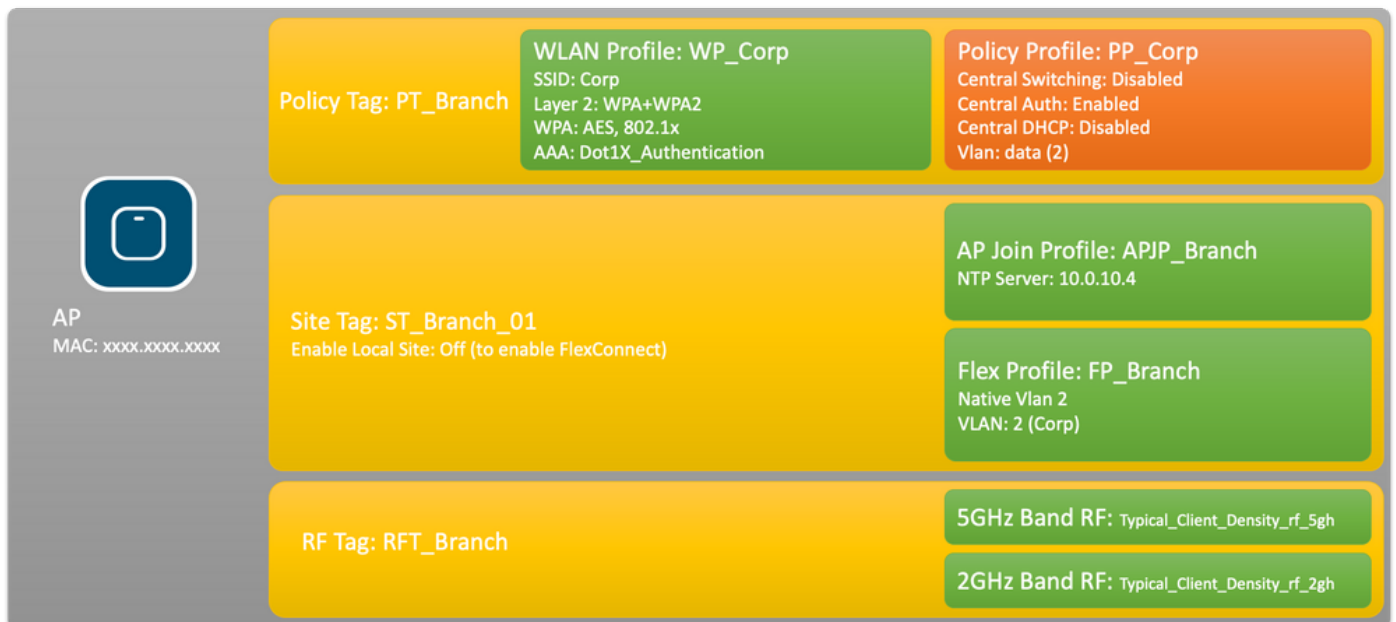


Esempio di rete



## Configurazione del controller wireless Catalyst 9800

In questo esempio di configurazione, il nuovo modello di configurazione su C9800 viene utilizzato per creare i profili e i tag necessari per fornire accesso aziendale dot1x alle filiali aziendali. La configurazione risultante viene riepilogata nel diagramma.



## C9800 - Configurazione dei parametri AAA per dot1x

Passaggio 1. Aggiungere il server 'Corp' di Aruba ClearPass Policy Manager alla configurazione WLC 9800. Passare a **Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server**. Fare clic su **+Aggiungi** e immettere le informazioni sul server RADIUS. Fare clic sul pulsante **Applica a dispositivo** come mostrato nell'immagine.

Name*	<input type="text" value="CPPM_Corp"/>
Server Address*	<input type="text" value="10.85.54.97"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key* ⓘ	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

Passaggio 2. Definire il gruppo di server AAA per gli utenti aziendali. Passare a **Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Gruppi** e fare clic su **+Aggiungi**, immettere il nome del gruppo di server RADIUS e assegnare le informazioni sul server RADIUS. Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

### Create AAA Radius Server Group ✕

Name*	AAA_Group_Corp
Group Type	RADIUS
MAC-Delimiter	none ▼
MAC-Filtering	none ▼
Dead-Time (mins)	5
Source Interface VLAN ID	none ▼

Available Servers		Assigned Servers
CPPM_Guest	>	CPPM_Corp
	<	
	>>	
	<<	

↶ Cancel 📄 Apply to Device

Passaggio 3. Definire l'elenco dei metodi di autenticazione dot1x per gli utenti aziendali. Selezionare **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione** e fare clic su **+Aggiungi**. Selezionare **Tipo dot1x** dal menu a discesa. Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

## Quick Setup: AAA Authentication



Method List Name\*

Dot1X\_Authentication

Type\*

dot1x



Group Type

group



Fallback to local

Available Server Groups

radius  
ldap  
tacacs+  
WLC\_Tacacs\_Servers  
AAA\_Group\_Guest



Assigned Server Groups

AAA\_Group\_Corp



Cancel



Apply to Device

## C9800 - Configurazione del profilo WLAN aziendale

Passaggio 1. Passare a **Configurazione > Tag e profili > Wireless** e fare clic su **+Aggiungi**. Immettere il nome di un profilo, il SSID 'Corp' e un ID WLAN non ancora in uso.

### Add WLAN



General

Security

Advanced

Profile Name\*

WP\_Corp

Radio Policy

All

SSID\*

Corp

Broadcast SSID

ENABLED



WLAN ID\*

3

Status

ENABLED



Cancel



Apply to Device

Passaggio 2. Passare alla scheda **Protezione** e alla scheda secondaria **Layer2**. Non è necessario modificare i parametri predefiniti di questo esempio di configurazione.

## Add WLAN

General **Security** Advanced

**Layer2** Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

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

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Passaggio 3. Passare alla scheda secondaria **AAA** e selezionare l'elenco dei metodi di autenticazione configurato in precedenza. Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.



Add WLAN ✕

General **Security** Advanced

---

Layer2 Layer3 **AAA**

---

Authentication List Dot1X\_Authenticatio ⓘ

Local EAP Authentication

---

↶ Cancel Apply to Device

## C9800 - Configura profilo criteri

Passaggio 1. Passare a **Configurazione > Tag e profili > Criterio** e fare clic su **+Aggiungi** e immettere un nome e una descrizione per il profilo del criterio. Abilitare il criterio e disabilitare la commutazione centrale, il protocollo DHCP e l'associazione, in quanto il traffico dell'utente aziendale viene commutato localmente nell'access point, come mostrato nell'immagine.

⚠ 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"/>			<b>WLAN Switching Policy</b>
Description	<input type="text" value="Policy Profile for Corp"/>			Central Switching <input type="checkbox"/> DISABLED
Status	<input checked="" 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
<b>CTS Policy</b>				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"/>			

Passaggio 2. Passare alla scheda **Access Policies** (Criteri di accesso) e immettere manualmente l'ID della VLAN da usare sulla filiale per il traffico dell'utente aziendale. Questa VLAN non deve essere configurata sul modello C9800. Deve essere configurato nel profilo Flex, come descritto più avanti. Non selezionare un nome VLAN dall'elenco a discesa (vedere Cisco bug ID [CSCvn48234](#)) per maggiori informazioni). Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

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

General	<b>Access Policies</b>	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
<b>WLAN Local Profiling</b>				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
<b>VLAN</b>				
VLAN/VLAN Group	<input type="text" value="2"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
				<b>WLAN ACL</b>
				IPv4 ACL <input type="text" value="Search or Select"/>
				IPv6 ACL <input type="text" value="Search or Select"/>
<b>URL Filters</b>				
				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 - Configura tag criteri

Dopo aver creato il profilo WLAN (WP\_Corp) e il profilo delle policy (PP\_Corp), è necessario creare un tag delle policy per associare questi profili WLAN e delle policy. Questo tag di criteri viene applicato ai punti di accesso. Assegnare questo tag ai punti di accesso per attivare la configurazione di questi punti per abilitare gli SSID selezionati.

Passaggio 1. Passare a **Configurazione > Tag e profili > Tag**, selezionare la scheda **Criterio** e fare clic su **+Aggiungi**. Immettere il nome e la descrizione del tag criteri. Fare clic su **+Add in WLAN-POLICY Maps**. Selezionare il profilo WLAN e il profilo criteri creati in precedenza, quindi fare clic sul pulsante con il segno di spunta, come mostrato nell'immagine.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

➤ RLAN-POLICY Maps: 0

Passaggio 2. Verificare e fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

Add Policy Tag ✕

Name\*

Description

**▼ WLAN-POLICY Maps: 1**

+ Add ✕ Delete

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**

↶ Cancel
📄 Apply to Device

## C9800 - Profilo di join AP

I profili di join AP e i profili Flex devono essere configurati e assegnati ai punti di accesso con tag del sito. È necessario utilizzare un tag del sito diverso per ogni succursale in modo da supportare la transizione rapida 802.11r (FT) all'interno di una succursale, ma limitare la distribuzione della chiave PMK del client solo tra i punti di accesso di tale succursale. È importante non riutilizzare lo stesso tag del sito in più succursali. Configurare un profilo di join AP. È possibile utilizzare un singolo profilo di join AP se tutte le diramazioni sono simili oppure creare più profili se alcuni dei parametri configurati devono essere diversi.

Passaggio 1. Passare a **Configurazione > Tag e profili > AP Join** e fare clic su **+Aggiungi**. Immettere il nome e la descrizione del profilo di AP Join. Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

**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 Profile

Configurare un profilo Flex. Anche in questo caso, è possibile usare un unico profilo per tutte le diramazioni, se sono simili e hanno la stessa mappatura VLAN/SSID. In alternativa, è possibile creare più profili se alcuni dei parametri configurati, ad esempio le assegnazioni della VLAN, sono diversi.

Passaggio 1. Passare a **Configurazione > Tag e profili > Flex** e fare clic su **+Aggiungi**. Immettere il nome e la descrizione del profilo Flex.

**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

Passaggio 2. Passare alla scheda **VLAN** e fare clic su **+Add**. Immettere il nome e l'ID della VLAN locale alla filiale che l'access point deve utilizzare per commutare localmente il traffico dell'utente aziendale. Fare clic sul pulsante **Save** (Salva), come mostrato nell'immagine.

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

**+ Add** ✕ Delete

VLAN Name	ID	ACL Name
No items to display		

10 items per page

VLAN Name\*

VLAN Id\*

ACL Name

**✓ Save** ↻ Cancel

↻ Cancel Apply to Device

Passaggio 3. Verificare e fare clic sul pulsante **Applica a dispositivo**, come mostrato nell'immagine.

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

**+ Add** ✕ Delete

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

10 items per page

1 - 1 of 1 items

↻ Cancel **Apply to Device**

## C9800 - Tag sito

I tag del sito vengono utilizzati per assegnare profili di join e profili Flex ai punti di accesso. Come accennato in precedenza, è necessario utilizzare un tag del sito diverso per ogni filiale per supportare la transizione rapida 802.11r (FT) all'interno di una filiale, ma limitare la distribuzione della chiave PMK del client solo tra gli access point della filiale. È importante non riutilizzare lo stesso tag del sito tra più filiali.

Passaggio 1. Passare a **Configurazione > Tag e profili > Tag**, selezionare la scheda **Sito** e fare clic su **+Aggiungi**. Immettere un nome e una descrizione per il tag del sito, selezionare il profilo di aggiunta AP creato, deselegionare la casella **Abilita sito locale** e infine selezionare il profilo Flex creato in precedenza. Deselegionare la casella **Attiva sito locale** per modificare il punto di accesso da **Modalità locale** a **FlexConnect**. Infine, fare clic sul pulsante **Applica al dispositivo** come mostrato nell'immagine.

**Add Site Tag** ✕

Name\*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

## C9800 - Tag RF

Passaggio 1. Passare a **Configurazione > Tag e profili > Tag**, selezionare la scheda **RF** e fare clic su **+Aggiungi**. Immettere un nome e una descrizione per il tag RF. Selezionare i **profili RF definiti dal sistema dal menu a discesa**. Fare clic sul pulsante **Applica alla periferica** come mostrato nell'immagine.

**Add RF Tag** ✕

Name\*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

## C9800 - Assegna tag all'access point

Ora che sono stati creati i tag che includono le varie policy e i profili richiesti per configurare i punti di accesso, è necessario assegnarli ai punti di accesso. Questa sezione illustra come eseguire manualmente un tag statico assegnato a un punto di accesso in base al relativo indirizzo MAC Ethernet. Per gli ambienti di produzione, si consiglia di utilizzare il flusso di lavoro PNP di Cisco DNA Center AP o un metodo di caricamento statico in blocchi CSV disponibile in 9800.

Passaggio 1. Passare a **Configura > Tag e profili > Tag**, selezionare la scheda **AP**, quindi la **scheda Static**. Fare clic su **+Aggiungi** e immettere l'indirizzo MAC AP, quindi selezionare il tag criteri, il tag sito e il tag RF definiti in precedenza. Fare clic sul pulsante **Applica a dispositivo** come mostrato nell'immagine.



### 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"/> ▼

## Configurazione di Aruba CPPM

### Configurazione iniziale del server Aruba ClearPass Policy Manager

Aruba clearpass viene implementato tramite il modello OVF sul server ESXi con le seguenti risorse:

- 2 CPU virtuali riservate
- 6 GB di RAM
- Disco da 80 GB (deve essere aggiunto manualmente dopo la distribuzione iniziale della VM prima che la macchina venga accesa)

### Applica licenze

Applicare la licenza della piattaforma tramite: **Amministrazione > Server Manager > Licenze**.  
Aggiungi **accesso e onboard**

### Aggiunta del controller wireless C9800 come dispositivo di rete

Selezionare **Configurazione > Rete > Dispositivi > Aggiungi**, come mostrato nell'immagine.

**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

## Configurare CPPM per l'utilizzo di Windows AD come origine di autenticazione

Passare a **Configurazione > Autenticazione > Origini > Aggiungi**. Seleziona tipo: Active Directory dal menu a discesa come illustrato nell'immagine.

**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: Move Up ↑ Move Down ↓ Add Backup Remove

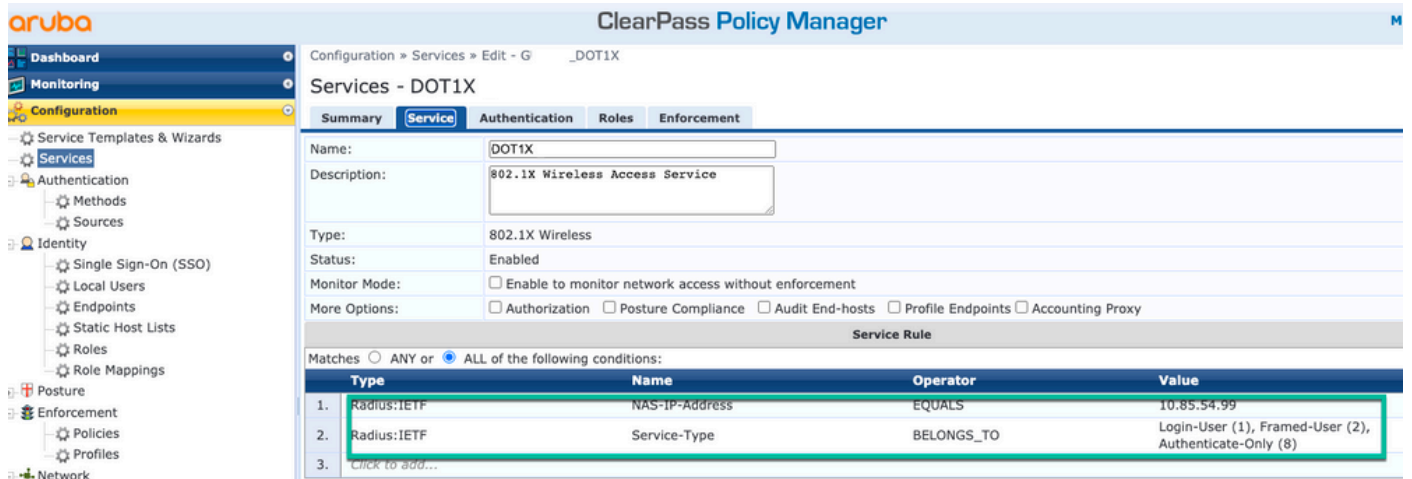
## Configura CPPM Servizio di autenticazione Dot1X

Passaggio 1. Creare un "servizio" corrispondente a diversi attributi RADIUS:

- Raggio:IETF | Nome: Indirizzo IP-NAS | UGUALE A | <INDIRIZZO IP>
- Raggio:IETF | Nome: Service-Type | UGUALE A | 1,2,8

Passaggio 2. Per la produzione, si consiglia di utilizzare il nome SSID anziché 'NAS-IP-Address' in

modo che una condizione sia sufficiente in una distribuzione multi-WLC. 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

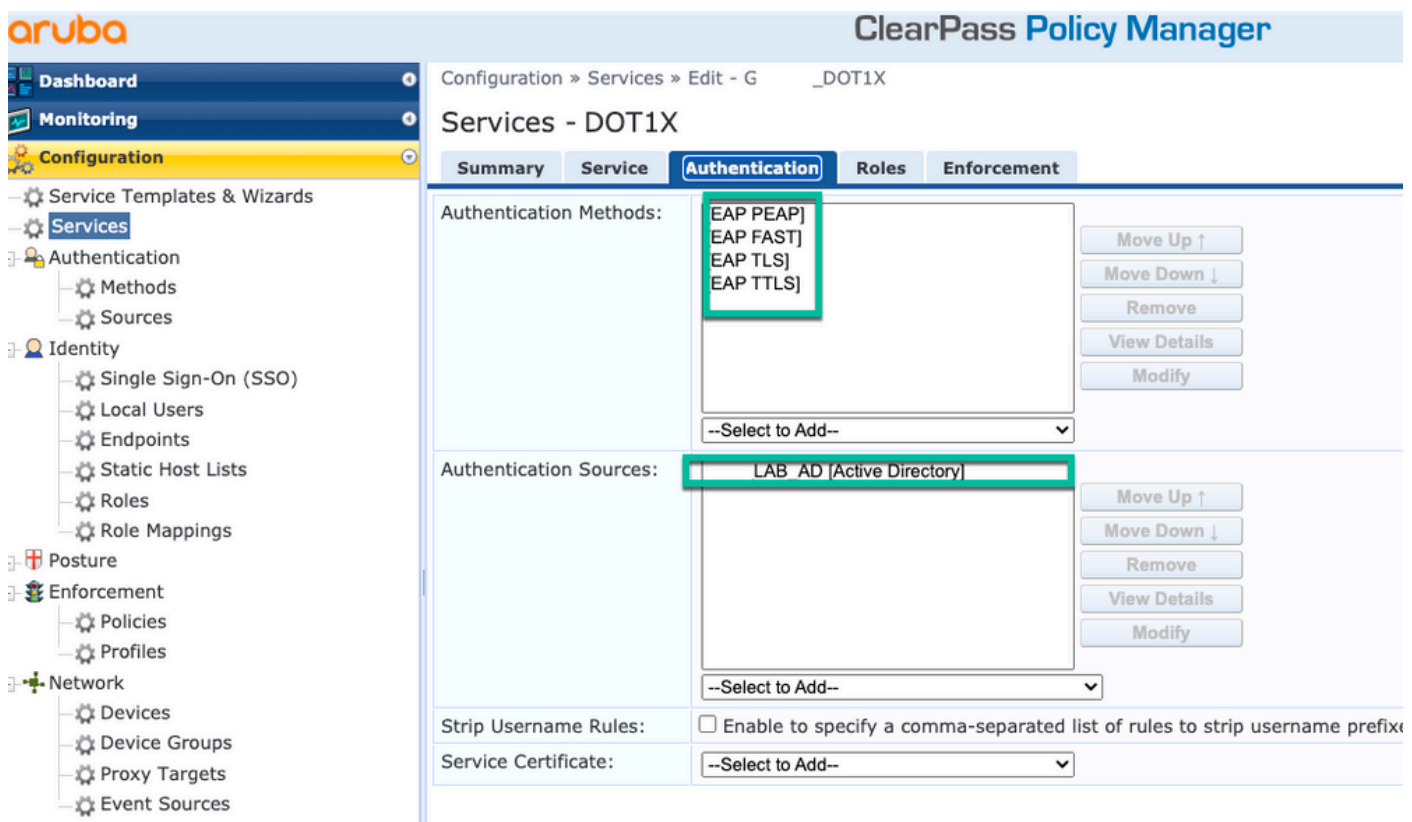
Status: Enabled

Monitor Mode:  Enable to monitor network access without enforcement

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

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)



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--

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Informazioni correlate

- [Guida alle best practice per l'installazione di Cisco 9800](#)

- [Informazioni sul modello di configurazione dei controller wireless Catalyst 9800](#)
- [Informazioni su FlexConnect su Catalyst 9800 Wireless Controller](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).