

Configuración de la integración de 9800 WLC con Aruba ClearPass - Dot1x & Implementación de FlexConnect para sucursales

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de tráfico](#)

[Diagrama de la red](#)

[Configuración del controlador inalámbrico Catalyst 9800](#)

[C9800 - Configuración de parámetros AAA para dot1x](#)

[C9800 - Configuración del perfil WLAN "corporativo"](#)

[C9800 - Configurar perfil de política](#)

[C9800 - Configurar etiqueta de directiva](#)

[C9800 - Perfil de unión a PA](#)

[C9800: perfil flexible](#)

[C9800: etiqueta del sitio](#)

[C9800: etiqueta RF](#)

[C9800 - Asignación de etiquetas a AP](#)

[Configuración de Aruba CPPM](#)

[Configuración inicial del servidor de Aruba ClearPass Policy Manager](#)

[Aplicar licencias](#)

[Agregar el controlador inalámbrico C9800 como dispositivo de red](#)

[Configurar CPPM para usar Windows AD como origen de autenticación](#)

[Configurar el servicio de autenticación Dot1X de CPPM](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la integración del controlador inalámbrico Catalyst 9800 con Aruba ClearPass Policy Manager (CPPM) y Microsoft Active Directory (AD) para ofrecer autenticación dot1x a clientes inalámbricos en una implementación Flexconnect.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de estos temas y que se hayan configurado y verificado:

- Controlador inalámbrico Catalyst 9800
- Servidor Aruba ClearPass (requiere licencia de plataforma, licencia de acceso y licencia integrada)
- Windows AD operativo
- Autoridad de certificación opcional (CA)
- Servidor DHCP operativo
- Servidor DNS operativo (necesario para la validación de CRL de certificados)
- ESXi
- Todos los componentes pertinentes se sincronizan con NTP y se verifica que tengan la hora correcta (necesario para la validación del certificado)
- Conocimiento de temas: Implementación de C9800 y nuevo modelo de configuraciónFuncionamiento de FlexConnect en C9800 Autenticación Dot1x

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 AP
- parche de Aruba ClearPass, 6-8-0-109592 y 6.8-3
- Servidor MS Windows Active Directory (GP configurado para la emisión automatizada de certificados basada en equipo a terminales administrados)Servidor DHCP con opción 43 y opción 60Servidor DNSServidor NTP para sincronizar la hora de todos los componentesCA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Flujo de tráfico

En una implementación empresarial típica con varias sucursales, cada sucursal está configurada para proporcionar acceso dot1x a los empleados corporativos. En este ejemplo de configuración, PEAP se utiliza para proporcionar acceso dot1x a usuarios corporativos a través de una instancia ClearPass implementada en el Data Center central (DC). Los certificados de equipo se utilizan junto con la verificación de las credenciales de los empleados en un servidor de Microsoft AD.

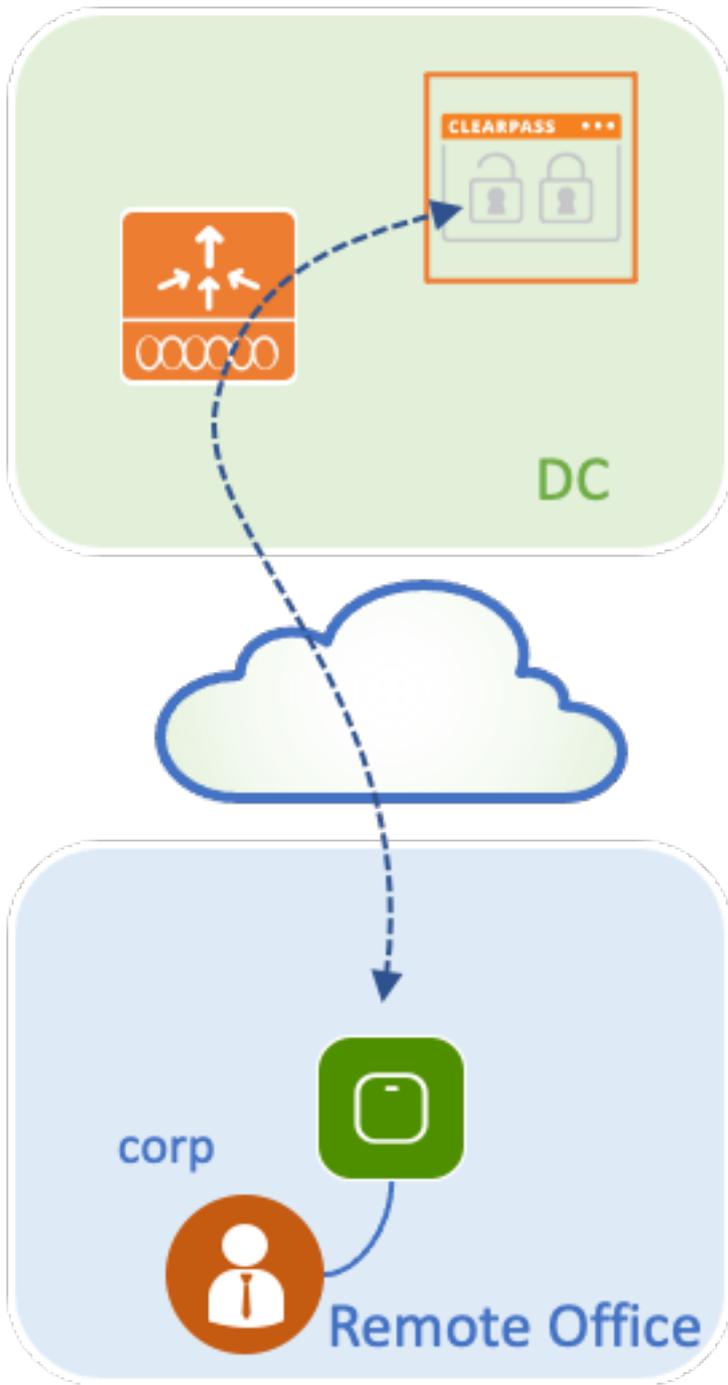
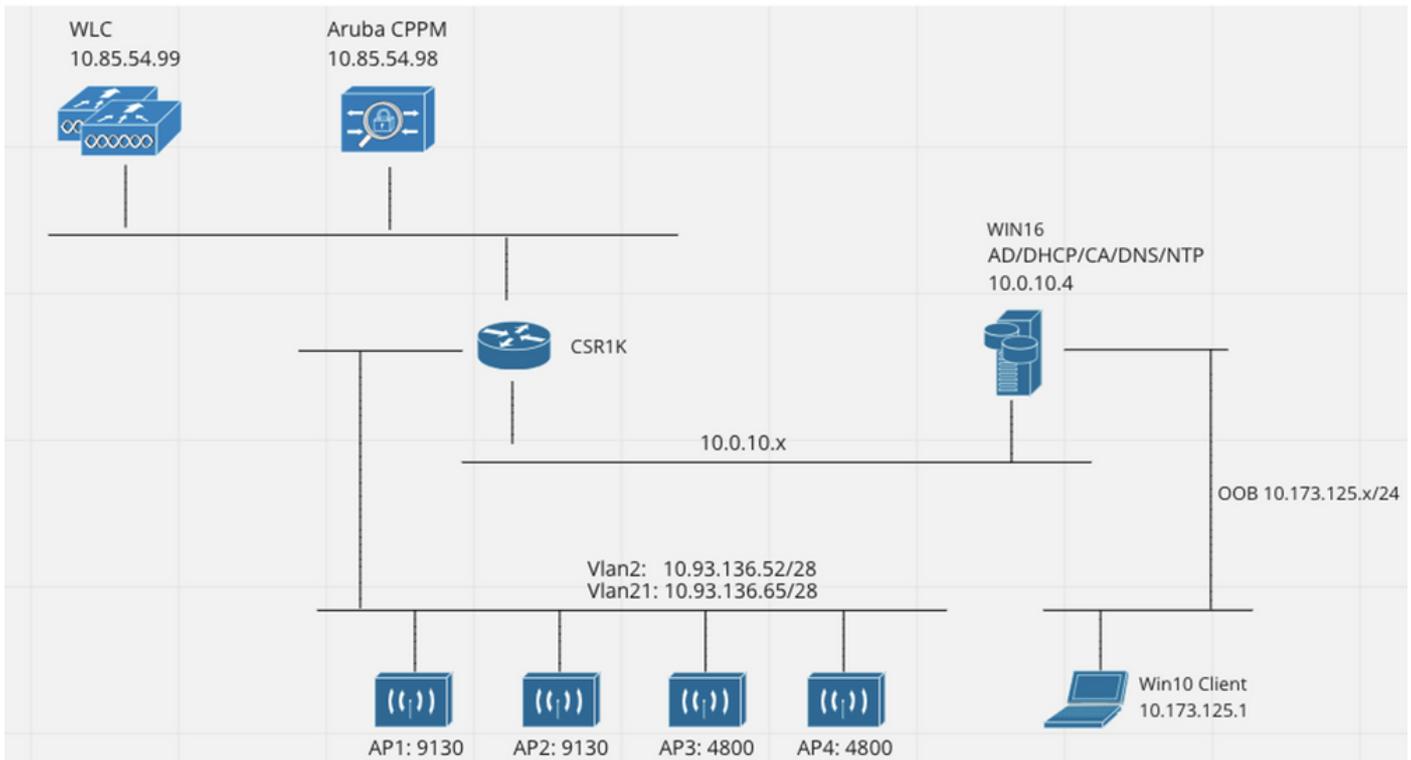
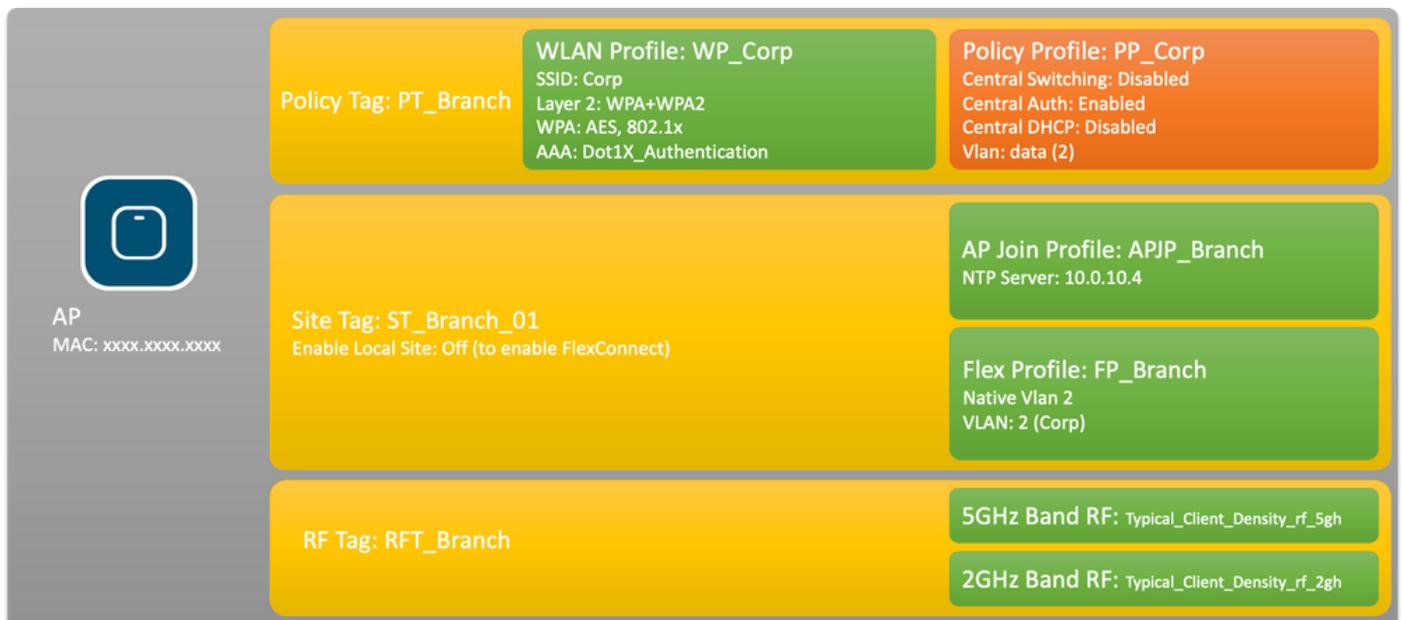


Diagrama de la red



Configuración del controlador inalámbrico Catalyst 9800

En este ejemplo de configuración, se aprovecha el nuevo modelo de configuración de C9800 para crear los perfiles y las etiquetas necesarios para proporcionar acceso corporativo dot1x a las sucursales empresariales. La configuración resultante se resume en el diagrama.



C9800 - Configuración de parámetros AAA para dot1x

Paso 1. Agregue el servidor 'Corp' del administrador de políticas de Aruba ClearPass a la configuración del WLC 9800. Navegue hasta **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers**. Haga clic en **+Add** e ingrese la información del servidor RADIUS. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

Create AAA Radius Server ✕

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

Paso 2. Defina el Grupo de Servidores AAA para los usuarios corporativos. Navegue hasta **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups** y haga clic en **+Add**, ingrese el nombre del grupo de servidores RADIUS y asigne la información del servidor RADIUS. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

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

Paso 3. Defina la lista de métodos de autenticación dot1x para usuarios corporativos. Navegue hasta **Configuration > Security > AAA > AAA Method List > Authentication** y haga clic en **+Add**. Seleccione **Type dot1x** en el menú desplegable. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

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 - Configuración del perfil WLAN "corporativo"

Paso 1. Navegue hasta **Configuration > Tags & Profiles > Wireless** y haga clic en **+Add**. Introduzca un nombre de perfil, el SSID 'Corp' y una ID de WLAN que no esté en 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

Paso 2. Navegue hasta la pestaña **Seguridad** y la subpestaña **Capa 2**. No es necesario cambiar ninguno de los parámetros predeterminados para este ejemplo de configuración.

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

Paso 3. Navegue hasta el subseparador **AAA** y seleccione la Lista de Métodos de Autenticación configurada anteriormente. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ⓘ

Local EAP Authentication

↶ Cancel Apply to Device

C9800 - Configurar perfil de política

Paso 1. Navegue hasta **Configuration > Tags & Profiles > Policy** y haga clic en **+Add** e ingrese un nombre y descripción del perfil de política. Habilite la política y deshabilite el switching central, DHCP y la asociación, ya que el tráfico de usuario corporativo se conmuta localmente en el AP como se muestra en la imagen.

⚠ 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 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
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"/>			

Paso 2. Navegue hasta la pestaña **Políticas de acceso** e ingrese manualmente el ID de la VLAN que se utilizará en la sucursal para el tráfico de usuarios corporativo. No es necesario configurar esta VLAN en el propio C9800. Se debe configurar en el perfil de Flex, como se detalla más adelante. No seleccione un nombre de VLAN en la lista desplegable (consulte Cisco bug ID [CSCvn48234](#) para obtener más información). Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

⚠ 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 - Configurar etiqueta de directiva

Una vez creados el perfil WLAN (WP_Corp) y el perfil de política (PP_Corp), se debe crear una etiqueta de política para enlazar estos perfiles de WLAN y de política. Esta etiqueta de directiva se aplica a los puntos de acceso. Asigne esta etiqueta de directiva a los puntos de acceso para activar la configuración de estos para activar los SSID seleccionados en ellos.

Paso 1. Navegue hasta **Configuración > Etiquetas y perfiles > Etiquetas**, seleccione la pestaña **Política** y haga clic en **+Agregar**. Introduzca el nombre y la descripción de la etiqueta de directiva. Haga clic en **+Add** bajo **WLAN-POLICY Maps**. Seleccione el perfil WLAN y el perfil de política creados anteriormente y, a continuación, haga clic en el botón de marca de verificación como se muestra en esta imagen.

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**

Paso 2. Verifique y haga clic en el botón **Apply to Device** como se muestra en esta imagen.

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 - Perfil de unión a PA

Los perfiles de unión a PA y los perfiles flexibles deben configurarse y asignarse a puntos de acceso con etiquetas de sitio. Se debe utilizar una etiqueta de sitio diferente para cada sucursal a fin de admitir 802.11r Fast Transition (FT) dentro de una sucursal, pero limitar la distribución del PMK del cliente solo entre los AP de esa sucursal. Es importante no volver a utilizar la misma etiqueta de sitio en varias sucursales. Configure un perfil de unión a AP. Puede utilizar un único perfil de unión de AP si todas las sucursales son similares, o crear varios perfiles si algunos de los parámetros configurados deben ser diferentes.

Paso 1. Navegue hasta **Configuration > Tags & Profiles > AP Join** y haga clic en **+Add**. Ingrese el nombre y la descripción del perfil de unión de AP. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

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: perfil flexible

Ahora configure un perfil flexible. De nuevo, puede utilizar un único perfil para todas las sucursales si son similares y tienen la misma asignación VLAN/SSID. O bien, puede crear varios perfiles si algunos de los parámetros configurados, como las asignaciones de VLAN, son diferentes.

Paso 1. Navegue hasta **Configuration > Tags & Profiles > Flex** y haga clic en **+Add**. Ingrese el nombre y la descripción del perfil de Flex.

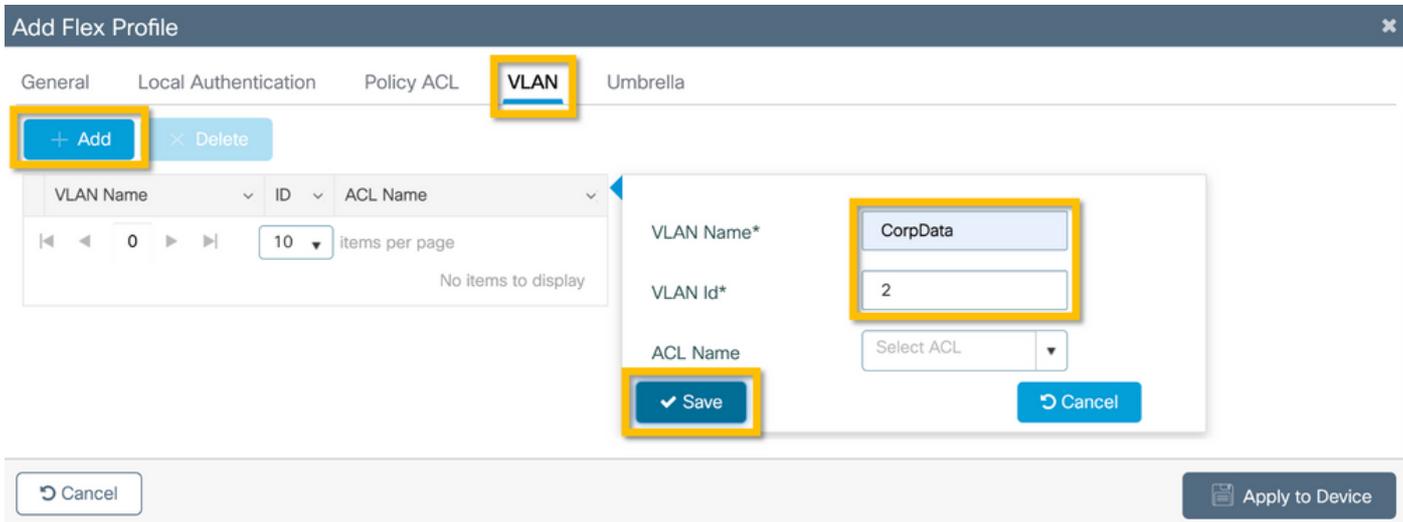
Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

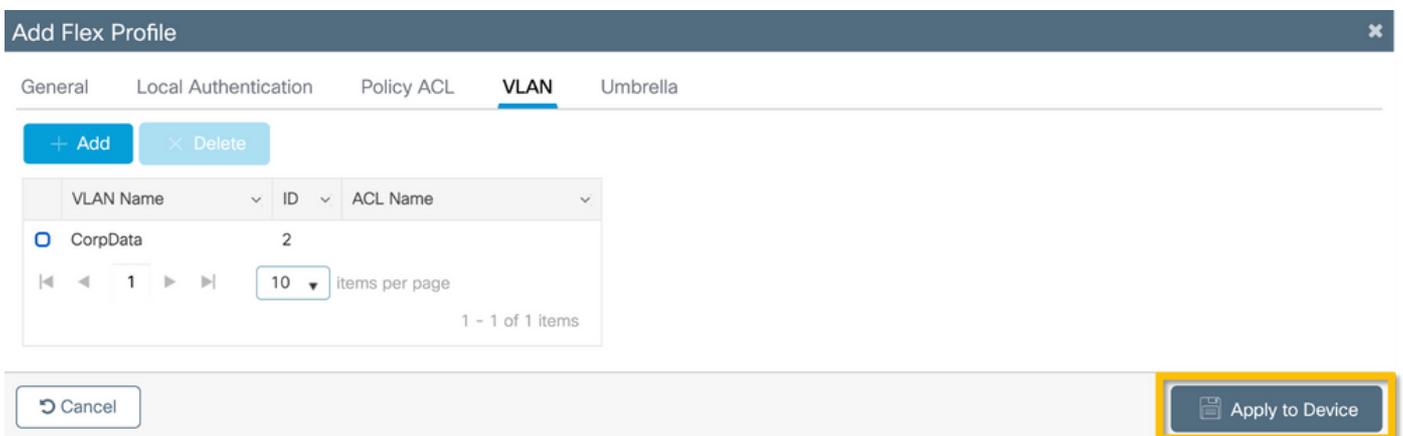
Name*	FP_Branch	Fallback Radio Shut	<input type="checkbox"/>
Description	Flex Profile for branches	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	1	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	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

Paso 2. Navegue hasta la pestaña **VLAN** y haga clic en **+Add**. Ingrese el nombre de VLAN y el ID de la VLAN local en la sucursal que el AP debe utilizar para conmutar localmente el tráfico de usuario corporativo. Haga clic en el botón **Save** como se muestra en esta imagen.



Paso 3. Verifique y haga clic en el botón **Apply to Device** como se muestra en esta imagen.



C9800: etiqueta del sitio

Las etiquetas de sitio se utilizan para asignar perfiles de unión y perfiles flexibles a los puntos de acceso. Como se ha mencionado anteriormente, se debe utilizar una etiqueta de sitio diferente para cada sucursal con el fin de admitir 802.11r Fast Transition (FT) dentro de una sucursal, pero limitar la distribución del PMK del cliente solo entre los AP de esa sucursal. Es importante no volver a utilizar la misma etiqueta de sitio en varias sucursales.

Paso 1. Navegue hasta **Configuración > Etiquetas y perfiles > Etiquetas**, seleccione la pestaña **Sitio** y haga clic en **+Agregar**. Introduzca un nombre y una descripción de la etiqueta del sitio, seleccione el perfil de unión a PA creado, desactive la casilla **Enable Local Site** y, por último, seleccione el perfil flexible creado anteriormente. Desmarque la casilla **Enable Local Site** para cambiar el punto de acceso de **Local Mode** a **FlexConnect**. Finalmente, haga clic en el botón **Apply to Device** como se muestra en esta imagen.

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

C9800: etiqueta RF

Paso 1. Navegue hasta **Configuration > Tags & Profiles > Tags**, seleccione la pestaña **RF** y haga clic en **+Add**. Ingrese un nombre y una descripción para la etiqueta RF. Seleccione los **perfiles RF definidos por el sistema** del menú desplegable. Haga clic en el botón **Apply to Device** como se muestra en esta imagen.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

C9800 - Asignación de etiquetas a AP

Ahora que se han creado las etiquetas que incluyen las diversas políticas y perfiles necesarios para configurar los puntos de acceso, debemos asignarlos a los puntos de acceso. Esta sección muestra cómo realizar manualmente una etiqueta estática asignada a un punto de acceso, basada en su dirección MAC Ethernet. Para entornos de producción de productos, se recomienda utilizar el flujo de trabajo Cisco DNA Center AP PNP o un método de carga CSV masivo y estático disponible en 9800.

Paso 1. Navegue hasta **Configure > Tags & Profiles > Tags**, seleccione la pestaña **AP** y luego la pestaña **Static**. Haga clic en **+Agregar** e ingrese la dirección MAC del AP, y seleccione la etiqueta de política, la etiqueta del sitio y la etiqueta RF definidas previamente. Haga clic en el botón **Aplicar al dispositivo** como se muestra en esta imagen.

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"/> ▼

Configuración de Aruba CPPM

Configuración inicial del servidor de Aruba ClearPass Policy Manager

Aruba clearpass se implementa mediante una plantilla OVF en el servidor ESXi con estos recursos:

- 2 CPU virtuales reservadas
- 6 GB de RAM
- Disco de 80 GB (se debe agregar manualmente después de la implementación inicial de la máquina virtual antes de encender la máquina)

Aplicar licencias

Aplice la licencia de plataforma mediante: **Administration > Server Manager > Licensing**. Agregar acceso e incorporación

Agregar el controlador inalámbrico C9800 como dispositivo de red

Vaya a **Configuration > Network > Devices > Add** como se muestra en esta imagen.

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

Configurar CPPM para usar Windows AD como origen de autenticación

Vaya a **Configuration > Authentication > Sources > Add**. Seleccione Tipo: Active Directory en el menú desplegable como se muestra en esta imagen.

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 Move Up Move Down Remove

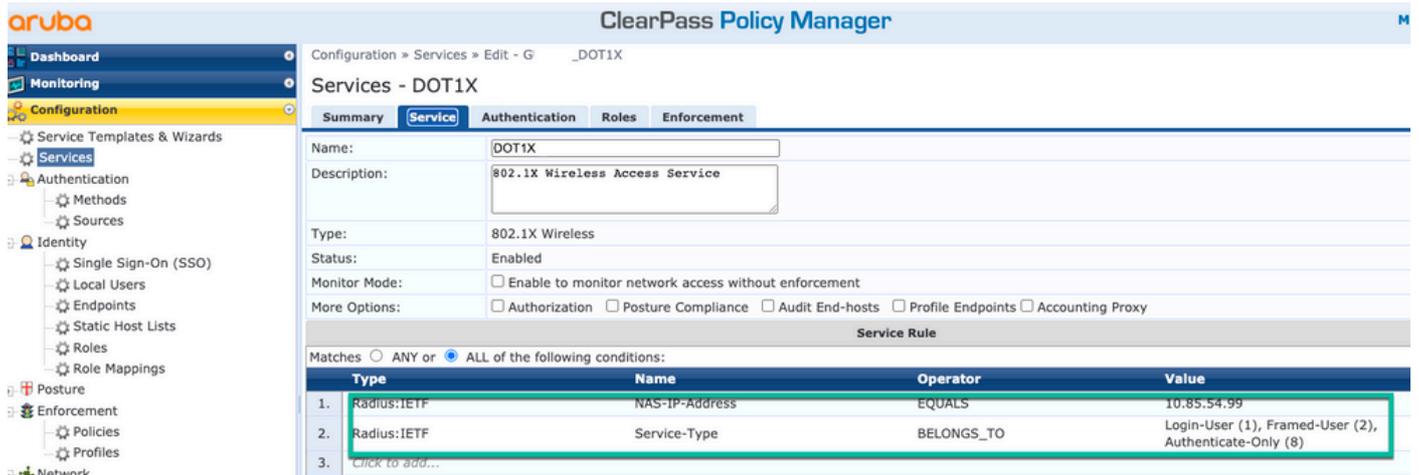
Configurar CPPM Servicio de autenticación Dot1X

Paso 1. Cree un 'servicio' que coincida en varios atributos RADIUS:

- Radio:IETF | Nombre: NAS-IP-Address | IGUAL A | <IP ADDR>
- Radio:IETF | Nombre: Tipo de servicio | IGUAL A |1,2,8

Paso 2. Para la producción, se recomienda hacer coincidir el nombre SSID en lugar de 'NAS-IP-

Address' para que una condición sea suficiente en una implementación de varios 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

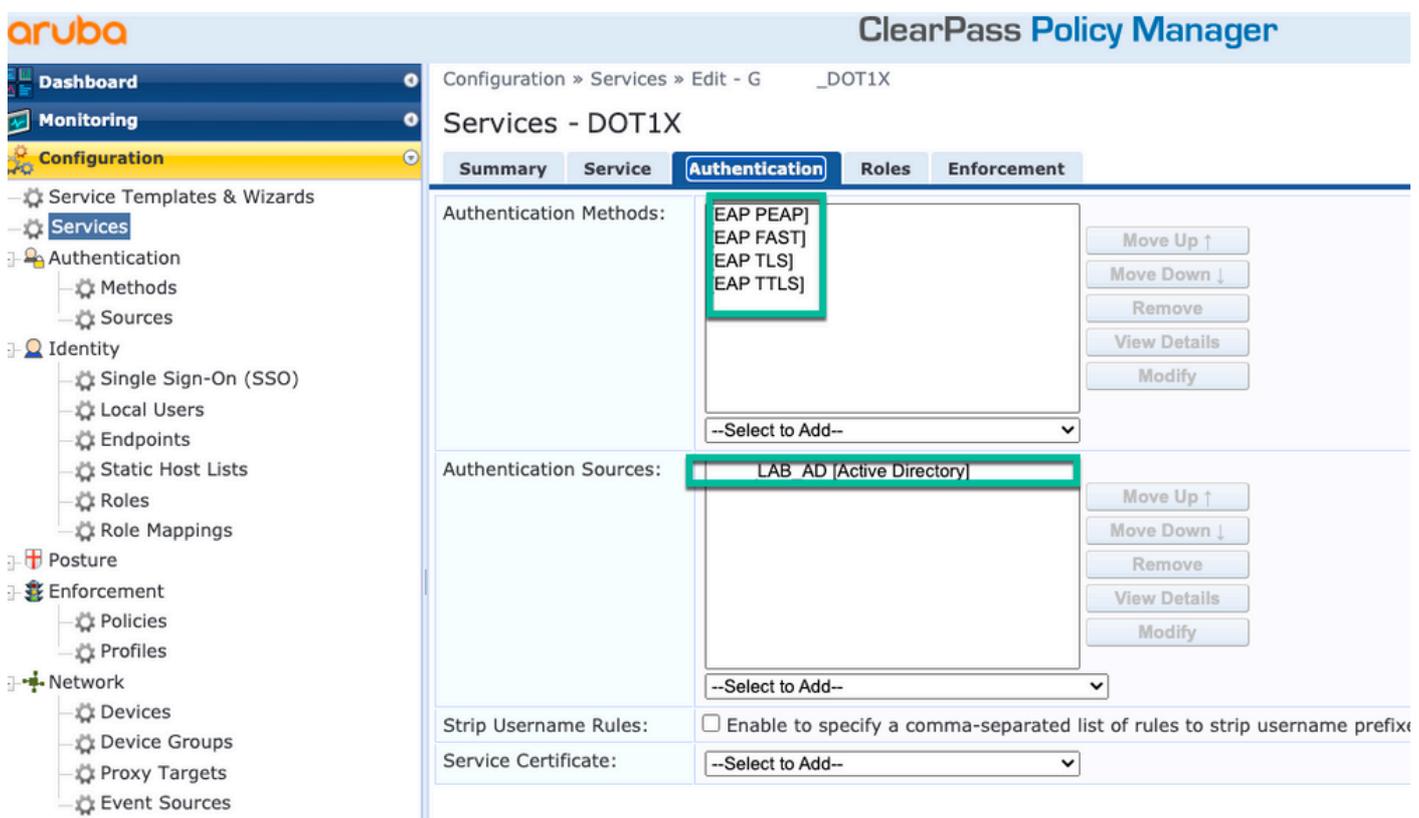
Monitor Mode: Enable to monitor network access without enforcement

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

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)



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--

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Guía de prácticas recomendadas de implementación de Cisco 9800](#)

- [Comprensión del modelo de configuración de controladores inalámbricos Catalyst 9800](#)
- [Información sobre FlexConnect en el controlador inalámbrico Catalyst 9800](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).