

Configuración de 9800 WLC y Aruba ClearPass: acceso de invitado & FlexConnect

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de tráfico para la implementación empresarial de invitados de CWA](#)

[Diagrama de la red](#)

[Configurar](#)

[Configuración de los parámetros del acceso inalámbrico de invitado C9800](#)

[C9800 - Configuración AAA para invitado](#)

[C9800 - Configurar ACL de redirección](#)

[C9800: configuración del perfil WLAN de invitado](#)

[C9800: definición de perfil de política de invitado](#)

[C9800: etiqueta de política](#)

[C9800 - Perfil de unión a PA](#)

[C9800: perfil flexible](#)

[C9800: etiqueta del sitio](#)

[C9800: perfil de RF](#)

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

[Configurar instancia de Aruba CPPM](#)

[Configuración inicial del servidor Aruba ClearPass](#)

[Solicitar licencias](#)

[Hostname del servidor](#)

[Generar certificado de servidor web CPPM \(HTTPS\)](#)

[Definir C9800 WLC como un dispositivo de red](#)

[Temporizadores de CoA y página del portal de invitados](#)

[ClearPass: configuración de CWA de invitado](#)

[Atributo de metadatos del terminal ClearPass: Allow-Guest-Internet](#)

[Configuración de directiva de aplicación de reautenticación ClearPass](#)

[Configuración del perfil de aplicación de redirección del portal de invitados ClearPass](#)

[Configuración del perfil de aplicación de metadatos ClearPass](#)

[Configuración de la política de aplicación de acceso a Internet de invitado ClearPass](#)

[Configuración de la política de aplicación posterior a AUP de invitado ClearPass](#)

[Configuración del servicio de autenticación MAB ClearPass](#)

[Configuración del servicio ClearPass Webauth](#)

[ClearPass: inicio de sesión web](#)

[Verificación - Autorización de CWA de invitado](#)

[Appendix](#)

[Información Relacionada](#)

Introducción

Este documento describe la integración del controlador de LAN inalámbrica (WLC) Catalyst 9800 con Aruba ClearPass para proporcionar un identificador de conjunto de servicios inalámbricos de invitado (SSID).

Prerequisites

Esta guía asume que estos componentes se han configurado y verificado:

- Todos los componentes pertinentes se sincronizan con el protocolo de tiempo de la red (NTP) y se comprueba que tienen la hora correcta (necesario para la validación del certificado)
- Servidor DNS operativo (necesario para los flujos de tráfico de invitados y la validación de la lista de revocación de certificados (CRL))
- Servidor DHCP operativo
- Una autoridad de certificación (CA) opcional (necesaria para firmar el portal de invitados alojado CPPM)
- WLC Catalyst 9800
- Servidor Aruba ClearPass (requiere licencia de plataforma, licencia de acceso y licencia integrada)
- Vmware ESXi

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementación de C9800 y nuevo modelo de configuración
- Switching Flexconnect en C9800
- Autenticación CWA 9800 (consulte <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

Componentes Utilizados

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

- Cisco Catalyst C9800-L-C que ejecuta 17.3.4c
- Cisco Catalyst C9130AX
- 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 60
 - Servidor DNS

- Servidor NTP para sincronizar la hora de todos los componentes
- La CA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La integración de la implementación del WLC Catalyst 9800 utiliza la autenticación web central (CWA) para clientes inalámbricos en una implementación de punto de acceso (AP) en modo Flexconnect.

El portal de invitados admite la autenticación inalámbrica de invitados con una página de política de usuario aceptable (AUP) anónima, alojada en Aruba Clearpass en un segmento de zona desmilitarizada segura (DMZ).

El diagrama transmite los detalles de los intercambios de acceso Wifi de invitado antes de que se permita al usuario invitado acceder a la red:

1. El usuario invitado se asocia con el Wifi invitado en una oficina remota.
2. El C9800 convierte en proxy la solicitud de acceso RADIUS inicial al servidor RADIUS.
3. El servidor busca la dirección MAC de invitado proporcionada en la base de datos de terminales MAC local.
Si no se encuentra la dirección MAC, el servidor responde con un perfil de omisión de autenticación MAC (MAB). Esta respuesta RADIUS incluye:
 - Lista de control de acceso (ACL) de redirección de URL
 - Redirección de URL
4. El cliente pasa por el proceso de aprendizaje de IP donde se le asigna una dirección IP.
5. C9800 pasa el cliente invitado (identificado por su dirección MAC) al estado 'Pendiente de autenticación web'.


6. La mayoría de los sistemas operativos de dispositivos modernos en asociación con las WLAN de invitados realizan algún tipo de detección de portal cautivo.

El mecanismo de detección exacto depende de la implementación específica del sistema operativo. El sistema operativo del cliente abre un cuadro de diálogo emergente (pseudonavegador) con una página redirigida por C9800 a la URL del portal de invitados alojada en el servidor RADIUS proporcionado como parte de la respuesta de aceptación de acceso de RADIUS.

7. El Usuario invitado acepta los Términos y condiciones en la ventana emergente ClearPass establece un indicador para la dirección MAC del cliente en su Base de datos de terminales (DB)

para indicar que el cliente ha completado una autenticación e inicia un Cambio de autorización (CoA) RADIUS, mediante la selección de una interfaz basada en la tabla de routing (si hay varias interfaces presentes en ClearPass).

8. El WLC pasa el cliente invitado al estado "Run" y el usuario tiene acceso a Internet sin más redireccionamientos.

 Nota: Para ver el diagrama de flujo de estado del controlador inalámbrico de anclaje externo Cisco 9800 con RADIUS y el portal de invitados alojado externamente, consulte la sección Apéndice de este artículo.

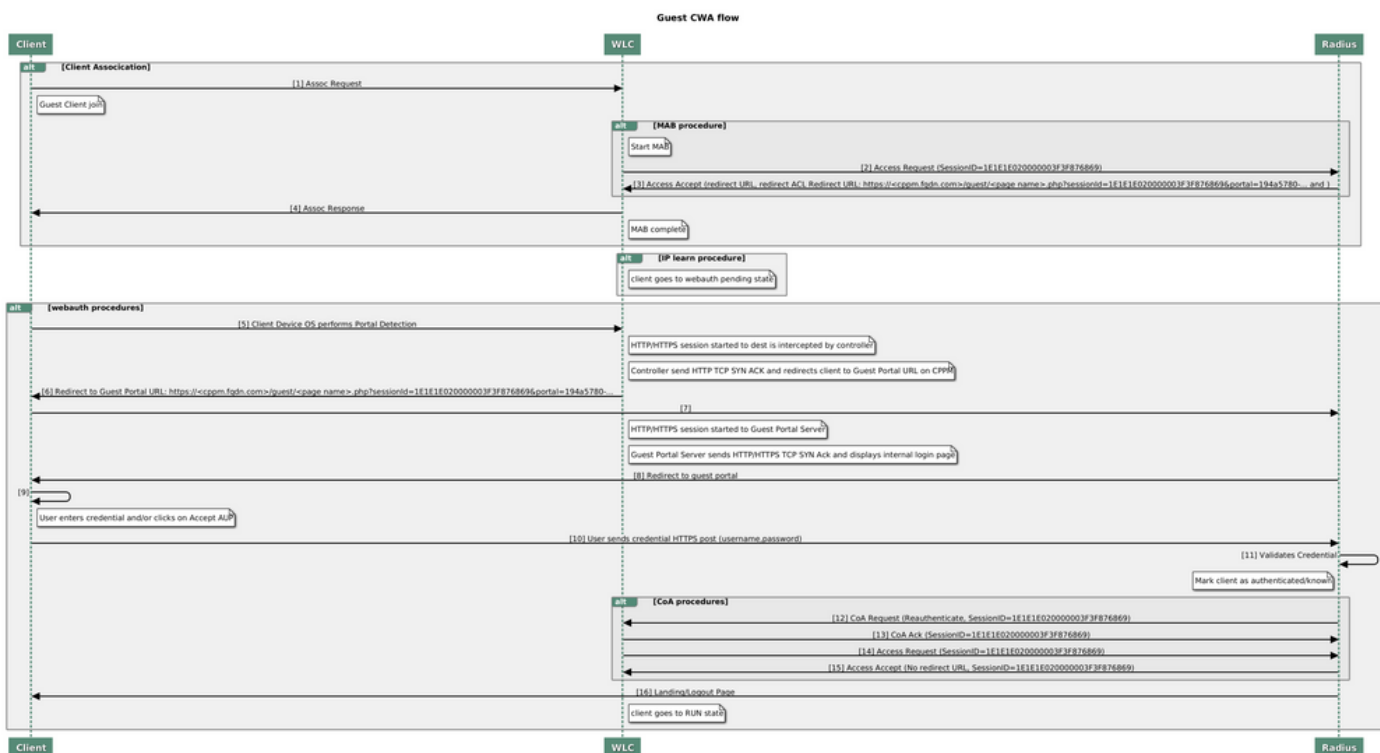


Diagrama de estado de la autenticación web central para invitados (CWA)

Flujo de tráfico para la implementación empresarial de invitados de CWA

En una implementación empresarial típica con varias sucursales, cada sucursal se configura para proporcionar acceso seguro y segmentado a los invitados a través de un portal de invitados una vez que el invitado acepta el EULA.

En este ejemplo de configuración, 9800 CWA se utiliza para el acceso de invitados mediante la integración a una instancia ClearPass independiente implementada exclusivamente para usuarios invitados en la DMZ segura de la red.

Los invitados deben aceptar los términos y condiciones establecidos en el portal emergente de consentimiento web proporcionado por el servidor DMZ ClearPass. Este ejemplo de configuración se centra en el método Anonymous Guest Access (es decir, no se requiere ningún nombre de usuario/contraseña de invitado para autenticarse en el portal de invitados).

El flujo de tráfico que corresponde a esta implementación se muestra en la imagen:

1. RADIUS - fase MAB
2. Redirección de URL de cliente invitado al portal de invitados
3. Después de la aceptación de invitado de EULA en el portal de invitados, RADIUS CoA Reauthenticate se emite desde CPPM a 9800 WLC
4. El huésped tiene acceso a Internet

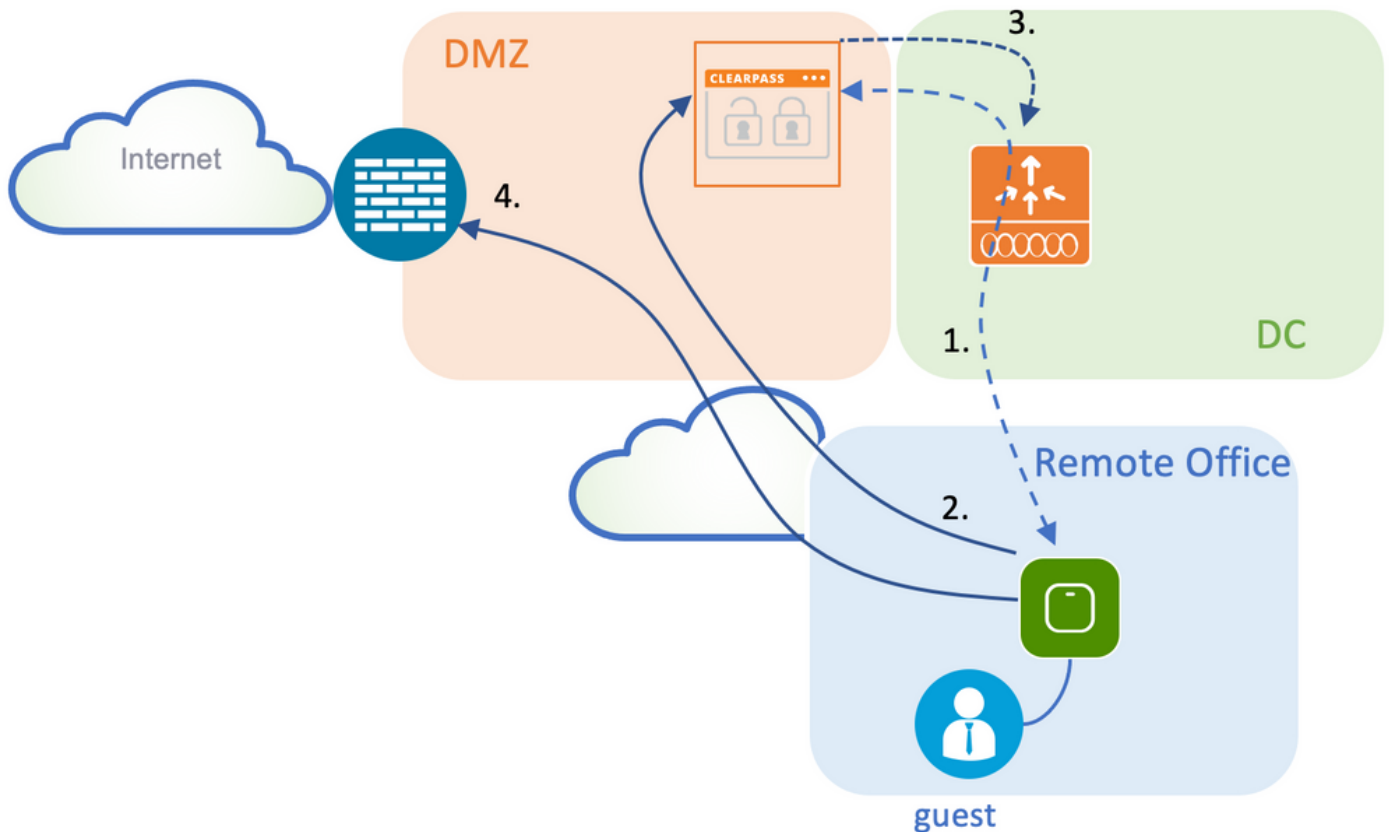

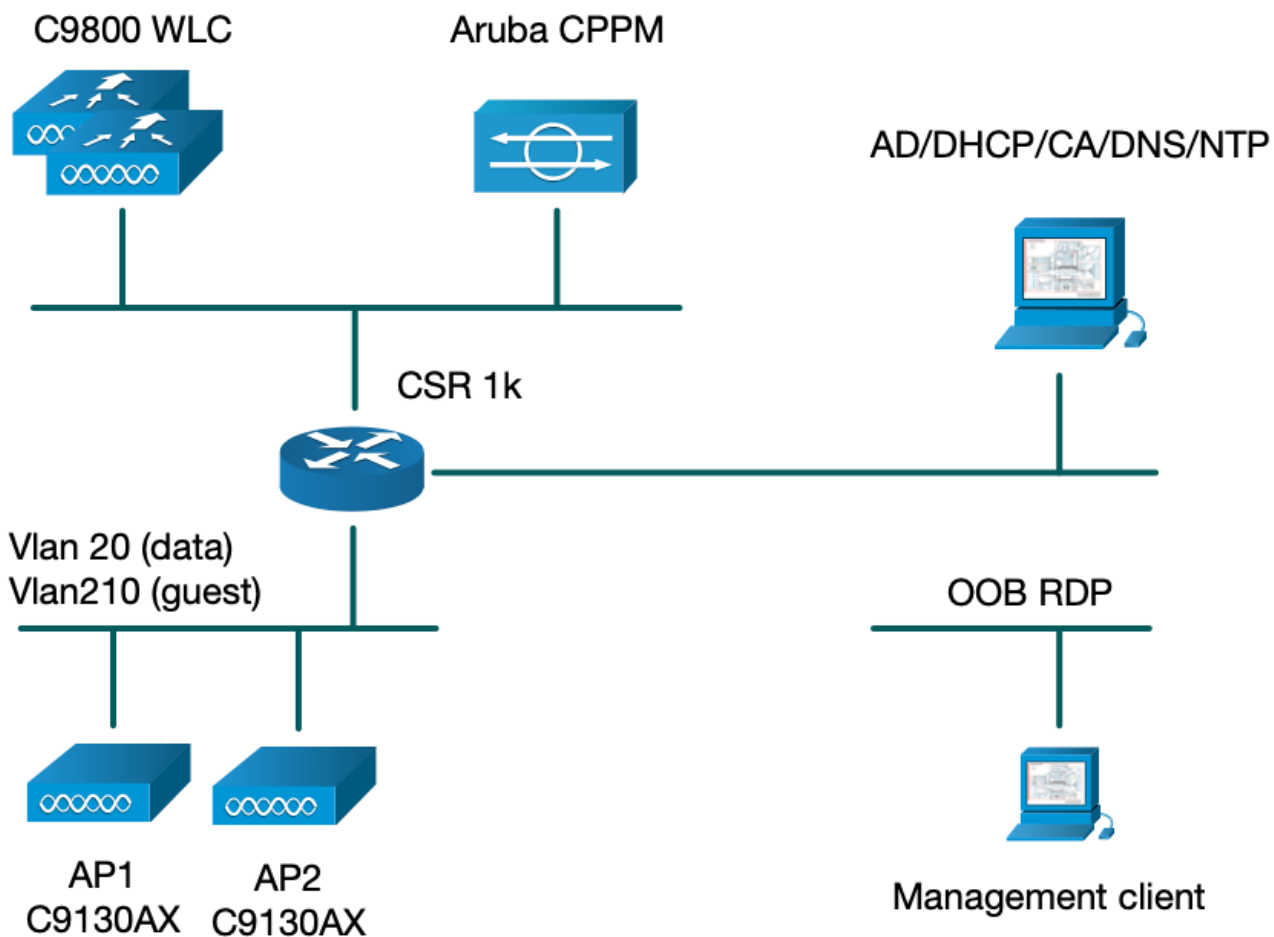


Diagrama de la red

 Nota: para fines de demostración de laboratorio, se utiliza una instancia de servidor CPPM de Aruba única/combinada para servir a las funciones de servidor de acceso a la red (NAS) SSID de invitado y de cuerpo. La implementación de prácticas recomendadas sugiere instancias de NAS independientes.



Configurar

En este ejemplo de configuración, se aprovecha un nuevo modelo de configuración en C9800 para crear los perfiles y etiquetas necesarios para proporcionar acceso corporativo dot1x y acceso de invitado CWA a la sucursal empresarial. La configuración resultante se resume en esta imagen:

AP
MAC: xxxxx.xxxxx.xxxx

Policy Tag: PT_CAN01

WLAN Profile: WP_Guest
SSID: Guest
Layer 2: Security None
Layer 2: MAC Filtering Enabled
Authz List: AAA_Authz-CPPM

Policy Profile: PP_Guest
Central Switching: Disabled
Central Auth: Enabled
Central DHCP: Disabled
Vlan: guest (21)
AAA Policy: Allow AAA Override Enabled
AAA Policy: NAC State Enabled
AAA Policy: NAC Type RADIUS
AAA Policy Accounting List: Guest_Accounting

Site Tag: ST_CAN01
Enable Local Site: Off

AP Join Profile: MyApProfile
NTP Server: 10.0.10.4

Flex Profile: FP_CAN01
Native Vlan 2
Policy ACL: CAPTIVE_PORTAL_REDIRECT,
ACL CWA: Enabled
VLAN: 21 (Guest)


RF Tag: Branch_RF

5GHz Band RF: Typical_Client_Density_rf_5gh

2GHz Band RF: Typical_Client_Density_rf_2gh

Configuración de los parámetros del acceso inalámbrico de invitado C9800

C9800 - Configuración AAA para invitado

 Nota: Acerca del Id. de bug Cisco [CSCvh03827](https://www.cisco.com/cisco/webbugtool/bugdetails.do?bugid=CSCvh03827), asegúrese de que los servidores de Autenticación, Autorización y Contabilización (AAA) definidos no estén balanceados por carga, ya que el mecanismo depende de la persistencia de Id. de sesión en los intercambios WLC a ClearPass RADIUS.

Paso 1. Agregue los servidores DMZ Aruba ClearPass a la configuración del WLC 9800 y cree una lista de métodos de autenticación. Desplácese hasta `Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add` e introduzca la información del servidor RADIUS.

Create AAA Radius Server



Name*	<input type="text" value="CPPM"/>
Server Address*	<input type="text" value="10.85.54.98"/>
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

Cancel

Apply to Device

Paso 2. Defina el grupo de servidores AAA para invitados y asigne el servidor configurado en el paso 1 a este grupo de servidores. Desplácese hasta [Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add](#).

Create AAA Radius Server Group



Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers

Assigned Servers



Cancel

Apply to Device

Paso 3. Defina una lista de métodos de autorización para el acceso de invitado y asigne el grupo de servidores creado en el paso 2. Desplácese hasta [Configuration > Security > AAA > AAA Method List > Authorization > +Add](#). Elija [Type Networky configure AAA Server Group](#) en el paso 2.

Quick Setup: AAA Authorization



Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Authenticated

Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

AAA_Radius_CPPM



Cancel

Apply to Device

Paso 4. Cree una lista de métodos de contabilidad para el acceso de invitado y asigne el grupo de servidores creado en el paso 2. Desplácese hasta **Configuration > Security > AAA > AAA Method List > Accounting > +Add**. Elija **Type Identity** en el menú desplegable y, a continuación, **AAA Server Group** configure en el paso 2.

Quick Setup: AAA Accounting



Method List Name*

Type* ⓘ

Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

AAA_Radius_CPPM



Cancel

Apply to Device

C9800 - Configurar ACL de redirección

La ACL de redirección define qué tráfico debe redirigirse al portal de invitados en lugar de permitir que pase sin redirección. En este caso, la negación de ACL implica la omisión de la redirección o

el paso a través, mientras que permit implica la redirección al portal. Para cada clase de tráfico, debe tener en cuenta la dirección del tráfico al crear entradas de control de acceso (ACE) y ACE que coincidan con el tráfico de entrada y de salida.

Desplácese hasta **Configuration > Security > ACL** y defina una nueva ACL denominada **CAPTIVE_PORTAL_REDIRECT**. Configure la ACL con estas ACE:

- ACE1: permite que el tráfico ICMP (protocolo de mensajes de control de Internet) bidireccional omita la redirección y se utiliza principalmente para verificar la disponibilidad.
- ACE10, ACE30: permite el flujo de tráfico DNS bidireccional al servidor DNS 10.0.10.4 y no se puede redirigir al portal. Se requiere una búsqueda de DNS y una interceptación de respuesta para activar el flujo de invitados.
- ACE70, ACE80, ACE110, ACE120: permite el acceso HTTP y HTTPS al portal cautivo de invitados para que el usuario pueda ver el portal.
- ACE150: se redirige todo el tráfico HTTP (puerto UDP 80).

Sequence ▲	Action ▼	Source IP ▼	Source Wildcard ▼	Destination IP ▼	Destination Wildcard ▼	Protocol ▼	Source Port ▼	Destination Port ▼
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800: configuración del perfil WLAN de invitado

Paso 1. Desplácese hasta **Configuration > Tags & Profiles > Wireless > +Add**. Cree un nuevo perfil de SSID **WP_Guest**, con la difusión de SSID 'Guest' con el que los clientes invitados se asocian.

Add WLAN ✕

General Security Advanced

Profile Name*	<input type="text" value="WP_Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Cancel

Apply to Device

En el mismo Add WLAN cuadro de diálogo, vaya a la Security > Layer 2 Ficha.

- Modo de seguridad de capa 2: Ninguno

- Filtrado de MAC: activado

- Lista de autorización: AAA_Authz_CPPM en el menú desplegable (configurado en el paso 3 como parte de la configuración AAA)

Add WLAN ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
OWE Transition Mode	<input checked="" type="checkbox"/>	Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	<input type="text" value="1-4096"/>	Reassociation Timeout	<input type="text" value="20"/>
Authorization List*	<input type="text" value="AAA_Authz_C"/>		

Cancel

Apply to Device

C9800: definición de perfil de política de invitado

En C9800 WLC GUI, navegue hasta `Configuration > Tags & Profiles > Policy > +Add`.

Nombre: PP_Invitado

Estado: habilitado

Switching central: desactivado

Autenticación central: habilitada

DHCP central: desactivado

Asociación central: Desactivada

Add 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*	<input type="text" value="PP_Guest"/>	WLAN Switching Policy
Description	<input type="text" value="Policy Profile for Guest"/>	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"/>	

Add Policy Profile ✕

⚠ 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*	PP_Guest	WLAN Switching Policy
Description	Profile for Branch Guest	Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> DISABLED	Central Authentication ENABLED <input checked="" type="checkbox"/>
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	2-65519	

Navegue hasta la **Access Policies** pestaña en el mismo **Add Policy Profile** diálogo.

- Perfiles RADIUS: Habilitado

- Grupo VLAN/VLAN: 210 (es decir, VLAN 210 es la VLAN local de invitado en cada sucursal)

✎ Nota: La VLAN de invitado para Flex no debe definirse en el WLC 9800 en VLAN, en el número de VLAN del tipo VLAN del grupo VLAN/VLAN.

Defecto conocido: el ID de bug Cisco [CSCvn48234](#) hace que el SSID no se transmita si la misma VLAN de invitado Flex se define en el WLC y en el perfil Flex.

⚠ 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

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Cancel

Apply to Device

En el mismo Add Policy Profile cuadro de diálogo, desplácese a la Advanced ficha.

- Permitir anulación de AAA: habilitado
- Estado de NAC: habilitado
- Tipo de NAC: RADIUS
- Lista de Contabilidad: AAA_Accounting_CPPM (definida en el paso 4 como parte de la configuración de AAA)

Add Policy Profile



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

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

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="AAA_Accounting_"/>

Fabric Profile

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

✎ Nota: se requiere 'Network Admission Control (NAC) State - Enable' para habilitar el WLC C9800 para aceptar los mensajes CoA de RADIUS.

C9800: etiqueta de política

En la GUI de C9800, vaya a **Configuration > Tags & Profiles > Tags > Policy > +Add**.

- Nombre: PT_CAN01

- Descripción: Etiqueta de política para la sucursal CAN01

En el mismo cuadro de diálogo **Add Policy Tag**, en **WLAN-POLICY MAPS**, haga clic en **+Add** y asigne el perfil

WLAN creado anteriormente al perfil de política:

- Perfil WLAN: WP_Guest

- Perfil de política: PP_Guest

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

C9800 - Perfil de unión a PA

En C9800 WLC GUI, navegue hasta `Configuration > Tags & Profiles > AP Join > +Add`.

- Nombre: Branch_AP_Profile

- Servidor NTP: 10.0.10.4 (consulte el diagrama de topología de laboratorio). Este es el servidor NTP que utilizan los AP en la sucursal para sincronizar.

Add AP Join Profile

General	Client	CAPWAP	AP	Management	Security	ICap	QoS
Name*	Branch_AP_Profile		OfficeExtend AP Configuration				
Description	Branch AP Join Profile		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	10.0.10.4						
GAS AP Rate Limit	<input type="checkbox"/>						
Apphost	<input type="checkbox"/>						
<input type="button" value="Cancel"/>			<input type="button" value="Apply to Device"/>				

C9800: perfil flexible

Los perfiles y las etiquetas son modulares y se pueden reutilizar para varios sitios.

En el caso de la implementación de FlexConnect, si se utilizan los mismos ID de VLAN en todas las sucursales, puede volver a utilizar el mismo perfil flexible.

Paso 1. En una GUI de C9800 WLC, navegue hasta `Configuration > Tags & Profiles > Flex > +Add`.

- Nombre: FP_Branch

- ID de VLAN nativa: 10 (solo se requiere si tiene una VLAN nativa no predeterminada en la que desea tener una interfaz de administración de AP)

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name* Fallback Radio Shut

Description Flex Resilient

Native VLAN ID ARP Caching

HTTP Proxy Port Efficient Image Upgrade

HTTP-Proxy IP Address OfficeExtend AP

CTS Policy Join Minimum Latency

Inline Tagging IP Overlap

SGACL Enforcement mDNS Flex Profile

CTS Profile Name

En el mismo Add Flex Profile cuadro de diálogo, desplácese a la Policy ACL ficha y haga clic en +Add.

- Nombre de ACL: CAPTIVE_PORTAL_REDIRECT
- Autenticación web central: habilitada

En una implementación de Flexconnect, se espera que cada AP administrado descargue la ACL de redirección localmente ya que la redirección ocurre en el AP y no en el C9800.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

ACL Name	Central Web Auth	Pre Auth URL Filter
0	<input checked="" type="checkbox"/>	

10 items per page No items to display

ACL Name*

Central Web Auth

Pre Auth URL Filter

En el mismo Add Flex Profile cuadro de diálogo, vaya a la VLAN ficha y haga clic en +Add (consulte el diagrama de topología de laboratorio).

- Nombre de VLAN: invitado
- ID de VLAN: 210

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

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

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

VLAN Name*

VLAN Id*


ACL Name

✓ Save ↶ Cancel

↶ Cancel Apply to Device

C9800: etiqueta del sitio

En la GUI del 9800 WLC, navegue hasta `Configuration > Tags & Profiles > Tags > Site > Add`.

 **Nota:** cree una etiqueta de sitio única para cada sitio remoto que admita los dos SSID inalámbricos, tal como se describe a continuación.

Existe una asignación 1-1 entre una ubicación geográfica, una etiqueta de sitio y una configuración de perfil flexible.

Un sitio de conexión flexible debe tener un perfil de conexión flexible asociado. Puede disponer de un máximo de 100 puntos de acceso para cada sitio de Flex Connect.

- Nombre: ST_CAN01
- Perfil de unión a PA: Branch_AP_Profile
- Perfil flexible: FP_Branch
- Activar sitio local: desactivado

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

C9800: perfil de RF

En la GUI del 9800 WLC, navegue hasta [Configuration > Tags & Profiles > Tags > RF > Add](#).

- Nombre: Branch_RF
- Perfil de radiofrecuencia (RF) de banda de 5 GHz: Typical_Client_Density_5gh (opción definida por el sistema)
- Perfil de RF de banda de 2,4 GHz: Typical_Client_Density_2gh (opción definida por el sistema)

Add RF Tag ✕

Name*	Branch_RF
Description	Typical Branch RF
5 GHz Band RF Profile	Client_Density_rf_5gh ▼
2.4 GHz Band RF Profile	Typical_Client_Densi ▼

↶ Cancel 📄 Apply to Device


C9800 - Asignación de etiquetas a AP

Hay dos opciones disponibles para asignar etiquetas definidas a AP individuales en la implementación:

- Asignación basada en nombre de AP, que aprovecha las reglas de regex que coinciden con los patrones del campo Nombre de AP ([Configure > Tags & Profiles > Tags > AP > Filter](#))
- Asignación basada en direcciones MAC Ethernet del punto de acceso ([Configure > Tags & Profiles > Tags > AP > Static](#))

En la implementación de producción con Cisco DNA Center, se recomienda encarecidamente utilizar DNAC y AP PNP Workflow o utilizar un método de carga masivo estático de valores separados por comas (CSV) disponible en 9800 para evitar la asignación manual por AP. Desplácese hasta [Configure > Tags & Profiles > Tags > AP > Static > Add](#) (observe la [Upload File](#) opción).


- Dirección MAC del punto de acceso: <AP_ETHERNET_MAC>
- Nombre de etiqueta de directiva: PT_CAN01
- Nombre de la etiqueta del sitio: ST_CAN01
- Nombre de la etiqueta RF: Branch_RF

 Nota: A partir de Cisco IOS® XE 17.3.4c, hay un máximo de 1000 reglas regex por limitación de controlador. Si el número de sitios de la implementación supera este número, se debe aprovechar la asignación estática por MAC.

Associate Tags to AP ✕

AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01 ▼
Site Tag Name	ST_CAN01 ▼
RF Tag Name	Branch_RF ▼

 Cancel

 Apply to Device

 Nota: como alternativa, para aprovechar el método de asignación de etiquetas basado en regex de nombre de AP, vaya a [Configure > Tags & Profiles > Tags > AP > Filter > Add](#).

- Nombre: BR_CAN01
- Regex de nombre de AP: BR-CAN01-(7) (Esta regla coincide con la convención de nombre de AP adoptada dentro de la organización. En este ejemplo, las etiquetas se asignan a los AP que tienen un campo AP Name que contiene 'BR_CAN01-' seguido de siete caracteres cualesquiera.)
- Prioridad: 1
- Nombre de etiqueta de directiva: PT_CAN01 (según se define)
- Nombre de la etiqueta del sitio: ST_CAN01
- Nombre de la etiqueta RF: Branch_RF

Associate Tags to AP



⚠ Rule " BR-CAN01 " has this priority. Assigning it to the current rule will swap the priorities.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01	x	▼
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01	x	▼
Active	YES	RF Tag Name	Branch_RF	x	▼
Priority*	1				

Configurar instancia de Aruba CPPM

Para conocer las prácticas recomendadas y de producción basadas en la configuración de Aruba CPPM, póngase en contacto con su recurso local de HPE Aruba SE.

Configuración inicial del servidor Aruba ClearPass

Aruba ClearPass se implementa mediante la plantilla Open Virtualization Format (OVF) en el servidor ESXi <> que asigna estos recursos:

- Dos 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)

Solicitar licencias

Solicite una licencia de plataforma a través de [Administration > Server Manager > Licensing](#). **Agregar** PlatformAccess, y Onboard licenses.

Hostname del servidor

Desplácese hasta [Administration > Server Manager > Server Configuration](#) el servidor CPPM recién provisionado y selecciónelo.

- Nombre de host: cppm
- FQDN: cppm.example.com
- Verifique el direccionamiento IP y DNS del puerto de administración

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm				
FQDN:	cppm.example.com				
Policy Manager Zone:	default				Manage F
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:cppm(10.85.54.98)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	Primary master				
Span Port:	-- None --				
		IPv4		IPv6	Action
Management Port	IP Address	10.85.54.98			Configure
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
Data/External Port	IP Address				Configure
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	10.85.54.122			Configure
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

Generar certificado de servidor web CPPM (HTTPS)

Este certificado se utiliza cuando la página ClearPass Guest Portal se presenta a través de HTTPS a los clientes invitados que se conectan a la red Wi-Fi de invitados en la sucursal.

Paso 1. Cargue el certificado de la cadena de publicaciones de la CA.

Desplácese hasta Administration > Certificates > Trust List > Add.

- Uso: Habilitar otros

View Certificate Details

Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	<input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others

Update **Disable** **Export** **Close**

Paso 2. Crear solicitud de firma de certificado.

Desplácese hasta Administration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS Server Certificate.

- Haga clic en el Create Certificate Signing Request

- Nombre común: CPPM

- Organización: cppm.example.com

Asegúrese de rellenar el campo SAN (debe haber un nombre común en SAN, así como IP y otros FQDN, según sea necesario). El formato es DNS

,DNS:

,IP

Create Certificate Signing Request

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:
Verify Private Key Password:
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

Paso 3. En la CA que elija, firme la CSR del servicio HTTPS de CPPM recién generado.

Paso 4. Desplácese hasta Certificate Template > Web Server > Import Certificate.

- Tipo de certificado: Certificado de servidor

- Uso: certificado de servidor HTTP

- Archivo de certificado: Examine y elija el certificado de servicio HTTPS de CPPM firmado por la CA

Import Certificate

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

Definir C9800 WLC como un dispositivo de red

Desplácese hasta [Configuration > Network > Devices > Add](#).

- Nombre: WLC_9800_Branch
- Dirección IP o de subred: 10.85.54.99 (consulte el diagrama de topología de laboratorio)
- RADIUS Shared Cisco: <contraseña RADIUS WLC>
- Nombre del proveedor: Cisco
- Activar la autorización dinámica de RADIUS: 1700

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	WLC_9800_Branch				
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:	Cisco 9800 WLC for Branch Guest Wifi				
RADIUS Shared Secret:		Verify:	
TACACS+ Shared Secret:			Verify:		
Vendor Name:	Cisco				
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: 1700				
Enable RadSec:	<input type="checkbox"/>				

[Add](#) [Cancel](#)

Temporizadores de CoA y página del portal de invitados

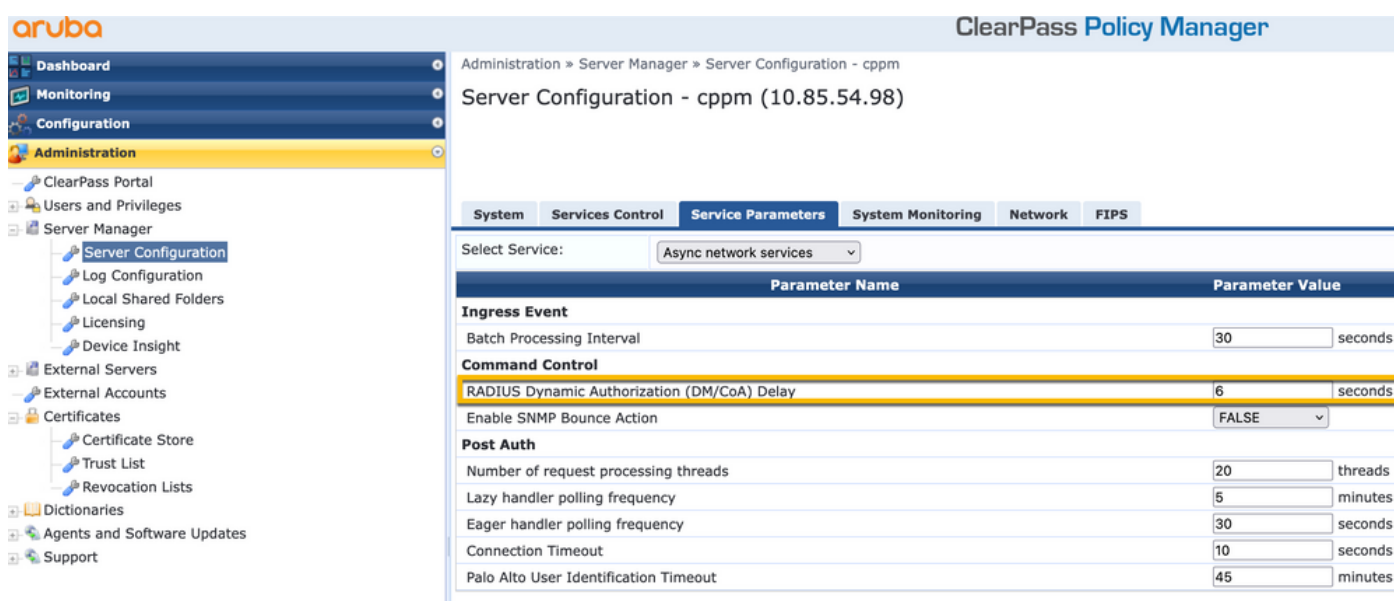
Es muy importante establecer los valores de temporizador correctos en toda la configuración. Si los temporizadores no están ajustados, es probable que se encuentre con una redirección del portal web en ciclo con el cliente, no en 'Estado de ejecución'.

Temporizadores a los que prestar atención:

- Temporizador de inicio de sesión web en el portal: este temporizador retrasa la página de redirección antes de permitir el acceso a la página del portal de invitados para notificar al servicio CPPM la transición de estado, registrar el valor del atributo personalizado de terminal 'Allow-Guest-Internet' y activar el proceso CoA de CPPM a WLC. Desplácese hasta [Guest > Configuration > Pages > Web Logins](#).
 - Seleccione Guest Portal Name (Nombre del portal de invitados): Lab Anonymous Guest Registration (esta configuración de la página del portal de invitados se detalla como se muestra)
 - Haga clic en [Edit](#)
 - Retraso en el inicio de sesión: 6 segundos

* Login Delay: The time in seconds to delay while displaying the login message.

- Temporizador de retraso CoA ClearPass: Esto retrasa el origen de los mensajes CoA de ClearPass al WLC. Esto es necesario para que CPPM realice correctamente la transición del estado del punto final del cliente internamente antes de que el reconocimiento de CoA (ACK) regrese del WLC. Las pruebas de laboratorio muestran los tiempos de respuesta en submilisegundos del WLC y, si el CPPM no ha terminado de actualizar los atributos de los terminales, la nueva sesión RADIUS del WLC coincide con la política de aplicación del servicio MAB no autenticado y se vuelve a dar al cliente una página de redirección. Desplácese hasta CPPM > Administration > Server Manager > Server Configuration y seleccione CPPM Server > Service Parameters.
 - Retraso de la autorización dinámica (DM/CoA) de RADIUS: establecido en seis segundos



ClearPass: configuración de CWA de invitado

La configuración de CWA de ClearPass-side se compone de (3) puntos de servicio/fases:

Componente ClearPass	Tipo de servicio	Propósito
1. Gestor de políticas	Servicio: autenticación Mac	Si el atributo personalizado Allow-Guest-Internet= TRUE, déjelo en la red. De lo contrario, gatillo RedirectyCOA: Reauthenticate.
2. Invitado	Inicios de sesión web	Presente la página AUP de inicio de sesión anónimo. Post-auth establece un atributo personalizado Allow-Guest-Internet= TRUE.

3. Gestor de políticas	Servicio: autenticación basada en Web	Actualizar terminal a Known Establecer atributo personalizado Allow-Guest-Internet=TRUE COA: Reauthenticate
------------------------	---------------------------------------	---


Atributo de metadatos del terminal ClearPass: Allow-Guest-Internet

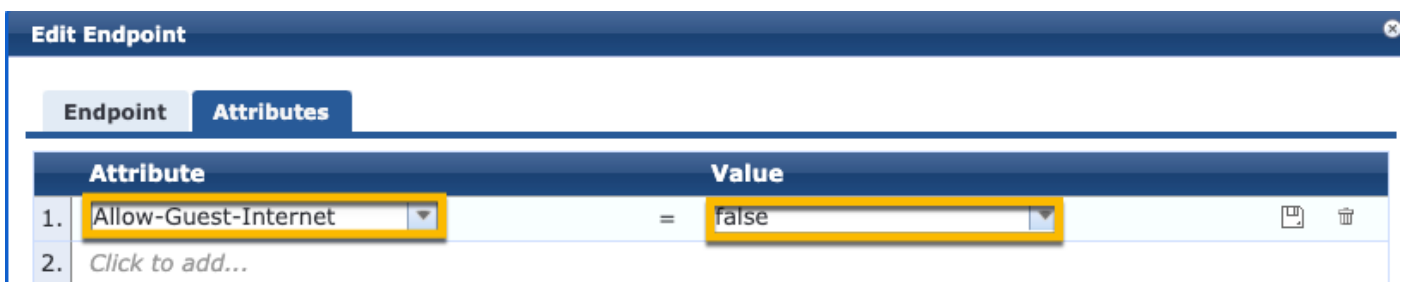
Cree un atributo de metadatos de tipo Booleano para realizar un seguimiento del estado del punto final de invitado mientras el cliente realiza transiciones entre los estados 'Webauth pendiente' y 'Run':

- Los nuevos invitados que se conectan a Wifi tienen un atributo de metadatos predeterminado establecido en Allow-Guest-Internet=false. Según este atributo, la autenticación del cliente pasa a través del servicio MAB

- Cliente invitado cuando hace clic en el botón Aceptar AUP, tiene su atributo de metadatos actualizado para Permitir-Invitado-Internet=true. El MAB posterior basado en este atributo establecido en True permite el acceso no redirigido a Internet

Desplácese hasta ClearPass > Configuration > Endpoints, seleccione cualquier extremo de la lista, haga clic en la Attributes ficha, agregue Allow-Guest-Internet con el valor false y Save.

 Nota: También puede editar el mismo terminal y eliminar este atributo inmediatamente después; este paso simplemente crea un campo en la base de datos de metadatos de terminales que se puede utilizar en políticas.



Configuración de directiva de aplicación de reautenticación ClearPass

Cree un perfil de aplicación que se asigne al cliente invitado inmediatamente después de que el cliente acepte la AUP en la página Portal de invitados.

Desplácese hasta ClearPass > Configuration > Profiles > Add.

- Plantilla: Autorización dinámica de RADIUS

- Nombre: Cisco_WLC_Guest_COA

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Dynamic Authorization	
Name:	Cisco_WLC_Guest_COA	
Description:		
Type:	RADIUS_CoA	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; width: 300px; height: 40px; margin-right: 10px;"></div> <div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">Modify</div> </div> </div> <div style="margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0; display: inline-block;">--Select--</div> </div>	

Radio:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station-Id}
Radio:Cisco	Cisco-AVPair	subscriber:command=volver a autenticar
Radio:Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-session-id}
Radio:Cisco	Cisco-AVPair	subscriber:reauthenticate-type=last-type=last

Configuración del perfil de aplicación de redirección del portal de invitados ClearPass

Cree un perfil de aplicación que se aplique al invitado durante la fase MAB inicial, cuando la dirección MAC no se encuentre en la base de datos de terminales CPPM con 'Allow-Guest-Internet' establecido en 'true'.

Esto hace que el WLC 9800 redirija al cliente invitado al portal de invitados CPPM para la autenticación externa.

Desplácese hasta ClearPass > Enforcement > Profiles > Add.

- Nombre: Cisco_Portal_Redirect

- Tipo: RADIUS

- Acción: Aceptar

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Cisco_Portal_Redirect	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:		<div style="text-align: right;"><button>Remove</button> <button>View Details</button> <button>Modify</button></div>
		--Select--

Perfil de aplicación de redirección de ClearPass


En el mismo cuadro de diálogo, en la Attributes ficha, configure dos Atributos según esta imagen:

Enforcement Profiles - Cisco_Portal_Redirect

Summary	Profile	Attributes
Type	Name	Value
1. Radius: Cisco	Cisco-AVPair	= url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2. Radius: Cisco	Cisco-AVPair	= url-redirect=https://cppm.example.com/guest/laccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

Atributos de perfil de redirección ClearPass

El url-redirect-acl atributo se establece en CAPTIVE-PORTAL-REDIRECT, que es el nombre de la ACL creada en C9800.


 Nota: Sólo la referencia a la ACL se pasa en el mensaje RADIUS, y no el contenido de la ACL. Es importante que el nombre de la ACL creada en el WLC 9800 coincida exactamente con el valor de este atributo RADIUS como se muestra.

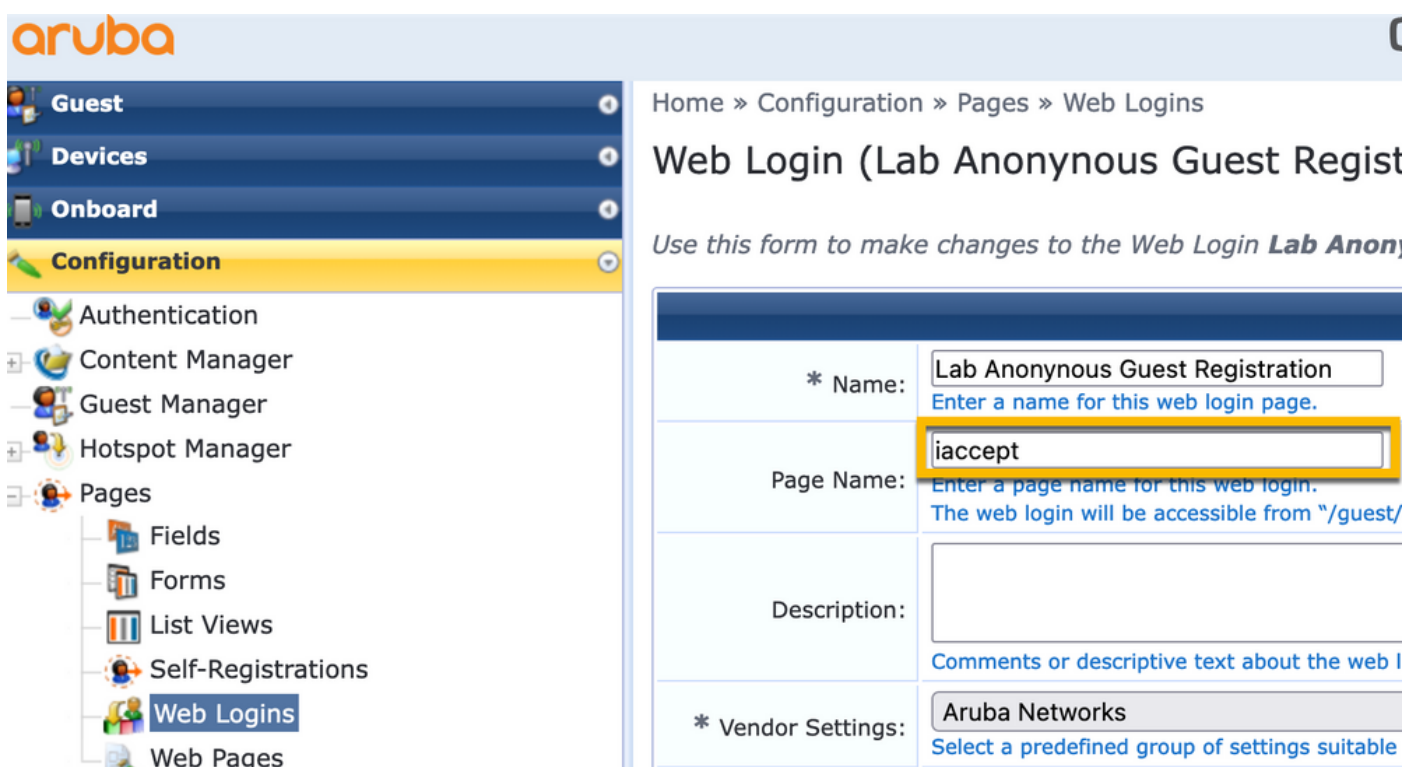
El url-redirect atributo se compone de varios parámetros:

- La URL de destino donde se aloja el portal de invitados, <https://cppm.example.com/guest/iaccept.php>
- MAC de cliente invitado, macro `%{Connection:Client-Mac-Address-Hyphen}`
- IP del autenticador (el WLC 9800 activa la redirección), macro `%{Radius:IETF:NAS-IP-Address}`
- `cmd-login action`

La URL de la página de inicio de sesión web de invitado ClearPass se muestra al desplazarse `aCPPM > Guest > Configuration > Pages > Web Logins > Edit`.


En este ejemplo, el nombre de la página Portal de invitados en CPPM se define como `iaccept`.

 Nota: los pasos de configuración de la página Portal de invitados son los descritos.



The screenshot shows the Aruba configuration interface. On the left is a navigation menu with categories like Guest, Devices, Onboard, Configuration, Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages, and Web Pages. The 'Pages' section is expanded, showing 'Web Logins' selected. The main content area shows the configuration for 'Web Login (Lab Anonymous Guest Registration)'. The breadcrumb path is 'Home » Configuration » Pages » Web Logins'. The form fields are:

- * Name: Lab Anonymous Guest Registration (with a tooltip: 'Enter a name for this web login page.')
- Page Name: **iaccept** (highlighted with a yellow box, with a tooltip: 'Enter a page name for this web login. The web login will be accessible from "/guest/')
- Description: (empty text area, with a tooltip: 'Comments or descriptive text about the web login.')
- * Vendor Settings: Aruba Networks (with a tooltip: 'Select a predefined group of settings suitable')

 Nota: para los dispositivos de Cisco, normalmente `audit_session_id` se utiliza, pero no es compatible con otros proveedores.

Configuración del perfil de aplicación de metadatos ClearPass

Configure el perfil de aplicación para actualizar el atributo de metadatos de punto final que se utiliza para el seguimiento de transición de estado por CPPM.

Este perfil se aplica a la entrada de dirección MAC del cliente invitado en la base de datos de terminales y establece el `Allow-Guest-Internet` argumento en 'true'.

Desplácese hasta `ClearPass > Enforcement > Profiles > Add`.

- Plantilla: Aplicación de actualización de entidad ClearPass

- Tipo: Post_Authentication

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile

Attributes


Summary

Template:	ClearPass Entity Update Enforcement
Name:	Make-Cisco-Guest-Valid
Description:	
Type:	Post_Authentication
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop
Device Group List:	<div style="display: flex; align-items: center;"><div style="flex-grow: 1;"><div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div><div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div></div><div style="margin-left: 10px;"><div style="border: 1px solid #ccc; padding: 2px; width: 60px; text-align: center;">Remove</div><div style="border: 1px solid #ccc; padding: 2px; width: 60px; text-align: center;">View Details</div><div style="border: 1px solid #ccc; padding: 2px; width: 60px; text-align: center;">Modify</div></div></div>

En el mismo cuadro de diálogo, la **Attributes** ficha.

- Tipo: terminal

- Nombre: Allow-Guest-Internet

 Nota: Para que este nombre aparezca en el menú desplegable, debe definir manualmente este campo para al menos un terminal, como se describe en los pasos.

- Valor: true

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile

Attributes

Summary

	Type	Name	Value
1.	Endpoint	Allow-Guest-Internet	= true
2.	Click to add...		

Configuración de la política de aplicación de acceso a Internet de invitado ClearPass

Desplácese hasta **ClearPass > Enforcement > Políticas > Add.**

- Nombre: WLC Cisco Guest Allow
- Tipo de aplicación: RADIUS
- Perfil predeterminado: Cisco_Portal_Redirect

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	WLC Cisco Guest Allow	
Description:		
Enforcement Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	Cisco_Portal_Redirect	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

En el mismo cuadro de diálogo, desplácese a la **Rules** ficha y haga clic en **Add Rule**.

- Tipo: terminal
- Nombre: Allow-Guest-Internet
- Operador: EQUALS
- Valor verdadero
- Nombres de perfil / Agregar: [RADIUS] [Permitir perfil de acceso]

Rules Editor				
Conditions				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Endpoint	Allow-Guest-Internet	EQUALS	true	<input type="button" value="Add"/> <input type="button" value="Remove"/>
2.	Click to add...			
Enforcement Profiles				
Profile Names:	[RADIUS] [Allow Access Profile]	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>		
--Select to Add--				
				<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Configuración de la política de aplicación posterior a AUP de invitado ClearPass

Desplácese hasta **ClearPass > Enforcement > Policies > Add**.

- Nombre: Política de aplicación de Cisco WLC Webauth

- Tipo de aplicación: WEBAUTH (SNMP/Agent/CLI/CoA)

- Perfil predeterminado: [RADIUS_CoA] Cisco_Reauthenticate_Session

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement Rules Summary

Name: Cisco WLC Webauth Enforcement Policy

Description:

Enforcement Type: RADIUS TACACS+ WEBAUTH (SNMP/Agent/CLI/CoA) Application Event

Default Profile: [RADIUS_CoA] Cisco_Reautht **View Details** **Modify**

En el mismo cuadro de diálogo, desplácese hasta Rules > Add.

- Condiciones: Autenticación

- Nombre: Estado

- Operador: EQUALS

- Valor: Usuario

- Nombres de perfil: <add each>:

- [Autenticación posterior] [Actualización de terminal conocida]

- [Autenticación posterior] [Make-Cisco-Guest-Valid]

- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	User
2.	Click to add...		

Enforcement Profiles

Profile Names: [Post Authentication] [Update Endpoint Known]
[Post Authentication] Make-Cisco-Guest-Valid
[RADIUS_CoA] Cisco_WLC_Guest_COA

Move Up ↑
Move Down ↓
Remove

--Select to Add--

Save Cancel



Nota: Si se encuentra con un escenario con una ventana emergente continua del pseudonavegador de redirección del portal de invitados, es indicativo de que los temporizadores CPPM requieren ajustes o que los mensajes RADIUS CoA no se intercambian correctamente entre CPPM y 9800 WLC. Verifique estos sitios.

- Desplácese hasta CPPM > Monitoring > Live Monitoring > Access Tracker y asegúrese de que la entrada del registro RADIUS contenga los detalles de RADIUS CoA.

- En 9800 WLC, navegue hasta Troubleshooting > Packet Capture, habilite PCAP en la interfaz donde se espera la llegada de los paquetes CoA de RADIUS y verifique que los mensajes CoA de RADIUS se reciban del CPPM.

Configuración del servicio de autenticación MAB ClearPass

El servicio coincide en el par Valor de atributo (AV) Radius: Cisco | CiscoAVPair | cisco-wlan-ssid

Desplácese hasta ClearPass > Configuration > Services > Add.

Ficha Servicio:

- Nombre: GuestPortal - Mac Auth

- Tipo: autenticación MAC

- Más opciones: seleccione Autorización, terminales de perfil

Agregar regla de coincidencia:

- Tipo: Radio: Cisco

- Nombre: Cisco-AVPair

- Operador: EQUALS

- Valor: cisco-wlan-ssid=Invitado (coincida con el nombre SSID de invitado configurado)



Nota: 'Invitado' es el nombre del SSID de invitado transmitido por el WLC 9800.

Configuration > Services > Add

Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type:

Name:

Description:

Monitor Mode: Enable to monitor network access without enforcement

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

Service Rule

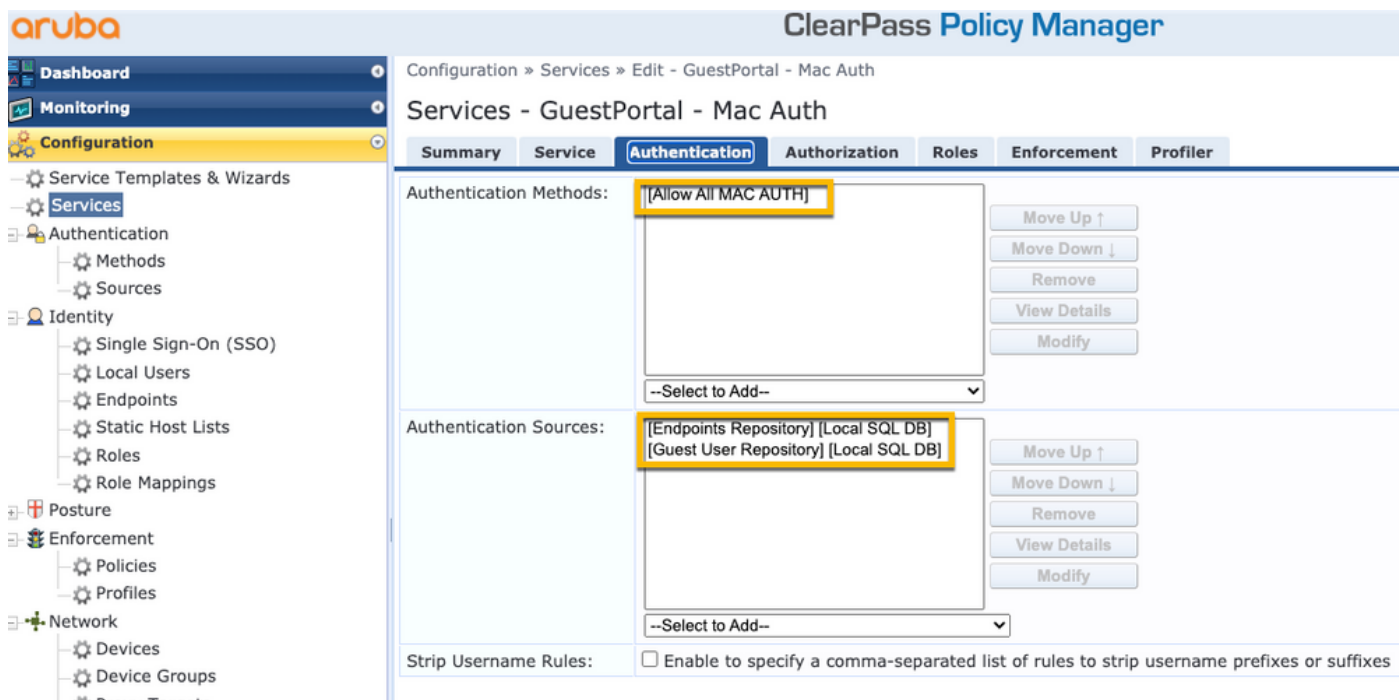
Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS %{Radius:IETF:User-Name}
4.	Radius:Cisco	Cisco-AVPair	EQUALS cisco-wlan-ssid=Guest

En el mismo cuadro de diálogo, elija la Authentication ficha.

- Métodos de autenticación: Remove [MAC AUTH], Add [Allow All MAC AUTH]

- Orígenes de autenticación: [Repositorio de terminales][Base de datos SQL local], [Repositorio de usuarios invitados][Base de datos SQL local]



En el mismo cuadro de diálogo, elija la **Enforcement** ficha.

- Política de aplicación: WLC Cisco Guest Allow

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:		WLC Cisco Guest Allow		Modify
Enforcement Policy Details				
Description:	MAB Enforcement Redirect			
Default Profile:	Cisco_Portal_Redirect			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]			

En el mismo cuadro de diálogo, elija la **Enforcement** ficha.

Services

Service	Authentication	Authorization	Roles	Enforcement	Profiler	Summary
Endpoint Classification:	Select the classification(s) after which an action must be triggered -					
	<div style="border: 1px solid #ccc; height: 40px;"></div>					<button>Remove</button>
	-- Select --					▼
RADIUS CoA Action:	Cisco_Reauthenticate_Session				▼	<button>View Details</button> <button>Modify</button>

Configuración del servicio ClearPass Webauth

Desplácese hasta ClearPass > Enforcement > Policies > Add.

- Nombre: Guest_Portal_Webauth

- Tipo: autenticación basada en Web

Services

Service	Authentication	Roles	Enforcement	Summary	
Type:	Web-based Authentication				▼
Name:	Guest				
Description:	<div style="border: 1px solid #ccc; height: 40px;"></div>				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name				
1.	Host	CheckType			
2.	<i>Click to add...</i>				

Mientras que en el mismo diálogo, en la Enforcement pestaña, la Política de aplicación: Cisco WLC Webauth Política de aplicación.

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	Cisco WLC Webauth Enforcement Policy Modify			Add New Enforcement Poli
Enforcement Policy Details				
Description:				
Default Profile:	Cisco_Reauthenticate_Session			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Status EQUALS User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

ClearPass: inicio de sesión web

Para la página Portal de invitados de AUP anónima, utilice un único nombre de usuario sin campo de contraseña.

El nombre de usuario que se utiliza debe tener estos campos definidos/definidos:

username_auth | Autenticación de nombre de usuario: | 1

Para establecer el campo 'username_auth' para un usuario, ese campo debe exponerse primero en el formulario 'edit user'. Desplácese hasta ClearPass > Guest > Configuration > Pages > Forms y elija create_user formulario.

The screenshot shows the Aruba ClearPass Guest configuration interface. The left sidebar has a 'Forms' menu item highlighted. The main content area is titled 'Customize Forms' and contains a table of forms. The 'create_user*' form is selected, and its 'Edit Fields' button is highlighted.

Name	Title
change_expiration Change the expiration time of a single guest account.	Change Expiration
create_multi Create multiple guest accounts.	Create Multiple Guest Accounts
create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results
create_user* Create a single guest account.	Create New Guest Account
create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt
guest_edit	

Elija visitor_name (fila 20) y haga clic en Insert After.

Customize Form Fields (create_user)

Use this list view to modify the fields of the form **create_user**.

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Guest's Name:	Name of the guest.

Edit
 Edit Base Field
 Remove
 Insert Before
 Insert After
 Disable Field

Customize Form Field (new)

Use this form to add a new field to the form **create_user**.

Form Field Editor

* Field Name: username_auth Select the field definition to attach to the form.

Form Display Properties
These properties control the user interface displayed for this field.

Field: Enable this field
When checked, the field will be included as part of the form.

* Rank:
Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.

* User Interface: No user interface Revert
The kind of user interface element to use when entering or editing this field.

Form Validation Properties
These properties control how the value of this field is checked.

Field Required: Field value must be supplied
Select this option if the field cannot be omitted or left blank.

Initial Value: Revert
Value to initialize this field with when the form is first displayed.

* Validator: IsValidBool
The function used to validate the contents of a field.

Validator Param: (None)
Optional name of field whose value will be supplied as the argument to a validator.

Validator Argument:
Optional value to supply as the argument to a validator.

Validation Error:
The error message to display if the field's value fails validation and the validator does not return an error message directly.

Ahora cree el nombre de usuario para utilizarlo detrás de la página del portal de invitados de AUP.

Desplácese hasta CPM > Guest > Guest > Manage Accounts > Create.

- Nombre del invitado: GuestWiFi

- Nombre de la empresa: Cisco
- Correo electrónico: guest@example.com
- Autenticación de nombre de usuario: permitir el acceso de invitado con el uso de su nombre de usuario solamente: Habilitado
- Activación de la cuenta: ahora
- Vencimiento de la cuenta: la cuenta no caduca
- Términos de uso: Soy el patrocinador: Habilitado

Home » Guest » Create Account

Create Guest Account

*New guest account being created by **admin**.*

Create New Guest Account	
* Guest's Name:	<input type="text" value="GuestWiFi"/> <small>Name of the guest.</small>
* Company Name:	<input type="text" value="Cisco"/> <small>Company name of the guest.</small>
* Email Address:	<input type="text" value="guest@example.com"/> <small>The guest's email address. This will become their username to log into the network.</small>
Username Authentication:	<input checked="" type="checkbox"/> Allow guest access using their username only <small>Guests will require the login screen setup for username-based authentication as well</small>
Account Activation:	<input type="text" value="Now"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input type="text" value="Account will not expire"/> <small>Select an option for changing the expiration time of this account.</small>
* Account Role:	<input type="text" value="[Guest]"/> <small>Role to assign to this account.</small>
Password:	281355
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
<input type="button" value="Create"/>	

Cree un formulario de inicio de sesión web. Desplácese hasta CPPM > Guest > Configuration > Web Logins.

Nombre: Lab Anonymous Guest Portal

Nombre de página: iaccept

Configuración del proveedor: Aruba Networks

Método de inicio de sesión: iniciado por el servidor: cambio de autorización (RFC 3576) enviado al controlador

Autenticación: anónima: no requiere nombre de usuario ni contraseña

Usuario anónimo: GuestWifi

Términos: requiere una confirmación de los Términos y condiciones

Etiqueta de inicio de sesión: aceptar y conectar

URL predeterminada: www.example.com

Retraso de inicio de sesión: 6

Actualizar extremo: marque la dirección MAC del usuario como un extremo conocido

Avanzado: personalice los atributos almacenados con el terminal, los atributos del terminal en la sección posterior a la autenticación:

Nombre de usuario | Nombre de usuario

visitor_name | Nombre del visitante

cn | Nombre del visitante

visitor_phone | Teléfono del visitante

Correo electrónico | Correo electrónico

correo | Correo electrónico

nombre_patrocinador | Nombre del patrocinador

correo_electrónico_patrocinador | Correo electrónico del patrocinador

Allow-Guest-Internet | verdadero

Verificación - Autorización de CWA de invitado

En el CPPM, vaya a [Live Monitoring > Access Tracker](#).

El nuevo usuario invitado se conecta y activa el servicio MAB.

Ficha Resumen:

Request Details

Summary Input Output RADIUS CoA

Login Status:	ACCEPT
Session Identifier:	R0000471a-01-6282a110
Date and Time:	May 16, 2022 15:08:00 EDT
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Username:	d43b047a647b
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)
Access Device Name:	wlc01
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Guest SSID - GuestPortal - Mac Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Cisco Portal Redirect

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

En el mismo cuadro de diálogo, vaya a la Input Ficha.

Request Details

Summary Input Output RADIUS CoA

Username:	d43b047a647b
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)

RADIUS Request

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

En el mismo cuadro de diálogo, vaya a la Output Ficha.

Request Details

Summary	Input	Output	RADIUS CoA
Enforcement Profiles:		Cisco_Portal_Redirect	
System Posture Status:		UNKNOWN (100)	
Audit Posture Status:		UNKNOWN (100)	
RADIUS Response			
Radius: Cisco: Cisco-AVPair		url-redirect-acl=CAPTIVE_PORTAL_REDIRECT	
Radius: Cisco: Cisco-AVPair		url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99	

◀ ◀ Showing 8 of 1-8 records ▶ ▶

Change Status

Show Configuration

Export

Show Logs

Close

Appendix

A modo de referencia, aquí se presenta un diagrama de flujo de estado para las interacciones de controlador de anclaje externo de Cisco 9800 con el servidor RADIUS y el portal de invitados alojado externamente.

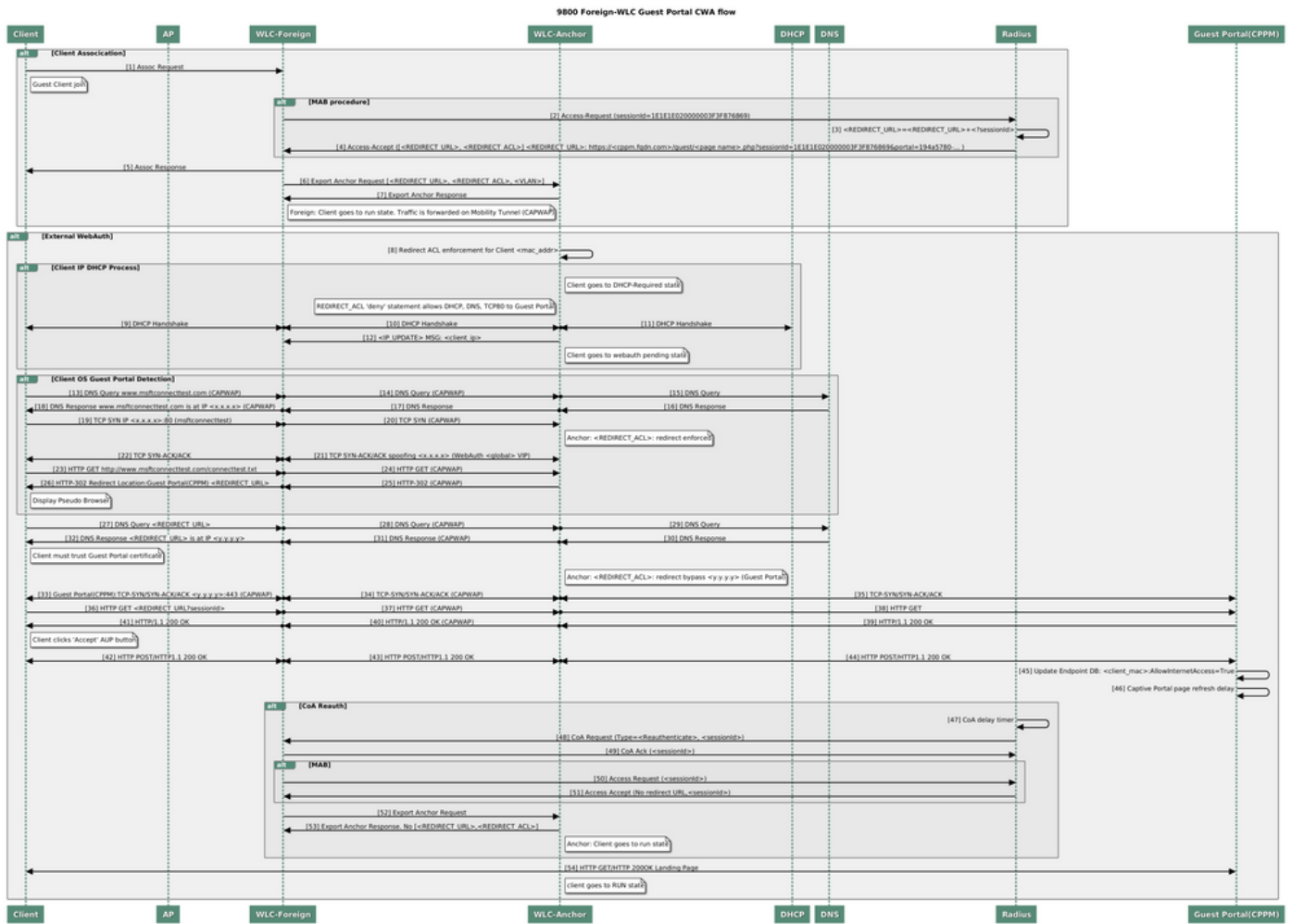


Diagrama de estado de autenticación web central de invitados con WLC de anclaje

Información Relacionada

- [Guía de prácticas recomendadas de implementación de Cisco 9800](#)
- [Comprenda el modelo de configuración de los controladores inalámbricos Catalyst 9800](#)
- [Comprensión de 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).