

Configurar 9800 WLC e Aruba ClearPass - Acesso de convidado e FlexConnect

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Fluxo de tráfego para a implantação corporativa de convidados do CWA](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configurar parâmetros C9800 de acesso sem fio de convidado](#)

[C9800 - Configuração AAA para convidado](#)

[C9800 - Configurar ACL de redirecionamento](#)

[C9800 - Configuração de perfil de WLAN de convidado](#)

[C9800 - Definição de perfil de política de convidado](#)

[C9800 - Marca de política](#)

[C9800 - Perfil de junção de AP](#)

[C9800 - Perfil Flex](#)

[C9800 - Marca do local](#)

[C9800 - Perfil de RF](#)

[C9800 - Atribuir tags ao AP](#)

[Configurar a instância Aruba CPPM](#)

[Configuração inicial do Aruba ClearPass Server](#)

[Inscreva-se para obter licenças](#)

[Nome de host do servidor](#)

[Gerar Certificado de Servidor Web CPPM \(HTTPS\)](#)

[Definir a WLC C9800 como um dispositivo de rede](#)

[Página do Portal do Convidado e Temporizadores de CoA](#)

[ClearPass - Configuração do CWA para Convidados](#)

[Atributo de Metadados de Ponto de Extremidade ClearPass: Allow-Guest-Internet](#)

[Configuração de Política de Imposição de Reautenticação ClearPass](#)

[Configuração do Perfil de Imposição de Redirecionamento do Portal de Convidado ClearPass](#)

[Configuração do Perfil de Imposição de Metadados ClearPass](#)

[Configuração da Política de Imposição de Acesso à Internet de Convidado ClearPass](#)

[Configuração da Política de Imposição Pós-AUP de Convidado ClearPass](#)

[Configuração do Serviço de Autenticação MAB ClearPass](#)

[Configuração do Serviço de Webauth ClearPass](#)

[ClearPass - Logon na Web](#)

[Verificação - Autorização do CWA convidado](#)

[Appendix](#)

Introduction

Este documento descreve a integração do Catalyst 9800 Wireless LAN Controller (WLC) com o Aruba ClearPass para fornecer o Guest Wireless Service Set Identifier (SSID) que aproveita a Central Web Authentication (CWA) para clientes sem fio em um modo Flexconnect de implantação de Ponto de Acesso (AP).

A autenticação sem fio de convidados é suportada pelo Portal de Convidados com uma página de política de usuário aceitável (AUP) anônima, hospedada no Aruba Clearpass em um segmento de zona desmilitarizada (DMZ) segura.

Prerequisites

Este guia supõe que estes componentes foram configurados e verificados:

- Todos os componentes pertinentes são sincronizados com o Network Time Protocol (NTP) e verificados para ter a hora correta (necessária para a validação do certificado)
- Servidor DNS operacional (necessário para fluxos de tráfego de convidado, validação da lista de revogação de certificados (CRL))
- Servidor DHCP operacional
- Uma autoridade de certificação (CA) opcional (necessária para assinar o Portal do Convidado hospedado no CPPM)
- WLC Catalyst 9800
- Aruba ClearPass Server (requer licença de plataforma, licença de acesso, licença integrada)
- Vmware ESXi

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Implantação do C9800 e novo modelo de configuração
- Switching Flexconnect no C9800
- Autenticação 9800 CWA (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

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst C9800-L-C com 17.3.4c
- Cisco Catalyst C9130AX
- Aruba ClearPass, patch 6-8-0-109592 e 6.8-3
- Servidor MS Windows Ative Directory (GP configurado para emissão automática de certificado baseada em computador para pontos de extremidade gerenciados) Servidor DHCP com opção 43 e opção 60 Servidor DNSServidor NTP para sincronizar com o tempo todos os

componentes O CA

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O diagrama transmite os detalhes das trocas de acesso WiFi Guest antes que o usuário convidado tenha permissão para entrar na rede:

1. O usuário convidado associa-se com o Guest Wifi em um escritório remoto.
2. A solicitação de acesso inicial ao RADIUS é enviada por proxy pelo C9800 para o servidor RADIUS.
3. O servidor procura o endereço MAC convidado fornecido no Banco de Dados de Ponto de Extremidade MAC local.
Se o endereço MAC não for encontrado, o servidor responde com um perfil MAC Authentication Bypass (MAB). Essa resposta RADIUS inclui:
 - Lista de Controle de Acesso (ACL) de Redirecionamento de URL
 - Redirecionamento de URL
4. O cliente passa pelo processo de aprendizado de IP, no qual recebe um endereço IP.
5. O C9800 faz a transição do cliente convidado (identificado por seu endereço MAC) para o estado 'Autenticação da Web Pendente'.
6. A maioria dos sistemas operacionais de dispositivos modernos, em associação com as WLANs de convidados, executam algum tipo de detecção de portal cativo.
O mecanismo exato de detecção depende da implementação específica do SO. O SO cliente abre uma caixa de diálogo pop-up (pseudo-navegador) com uma página redirecionada pelo C9800 para a URL do portal do convidado hospedada pelo servidor RADIUS fornecido como parte da resposta RADIUS Access-Accept.
7. O Usuário Convidado aceita os Termos e Condições no pop-up apresentado O ClearPass define uma flag para o endereço MAC do cliente em seu Banco de Dados de Ponto Final (DB) para indicar que o cliente concluiu uma autenticação e inicia uma Alteração de Autorização (CoA) RADIUS, pela seleção de uma interface com base na tabela de roteamento (se houver várias interfaces presentes no ClearPass).
8. A WLC faz a transição do Cliente Convidado para o Estado 'Run' e o usuário recebe acesso à Internet sem mais redirecionamentos.

Note: Para o fluxograma de estado do Cisco 9800 Foreign, Anchor Wireless Controller com RADIUS e Portal de convidado hospedado externamente, consulte a seção Apêndice neste artigo.

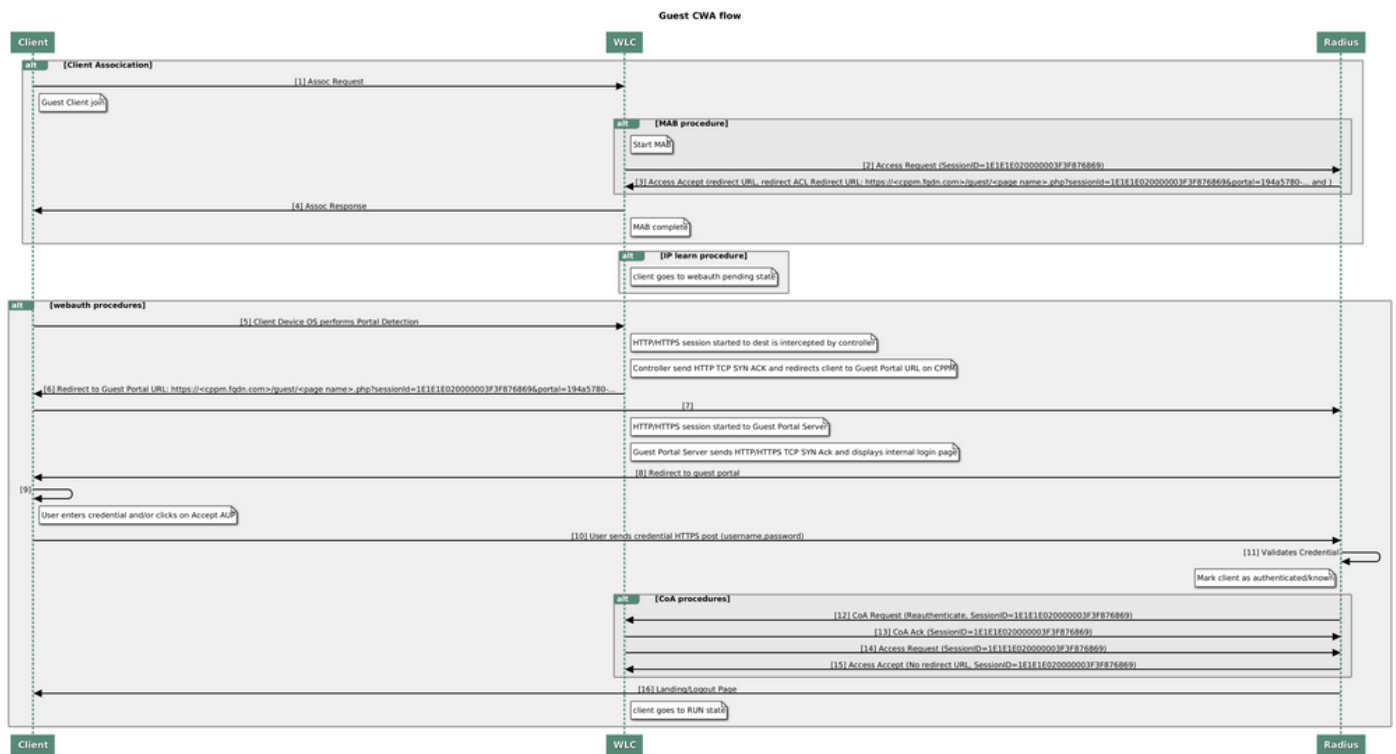


Diagrama de Estado da Autenticação da Web Central de Convidados (CWA)

Fluxo de tráfego para a implantação corporativa de convidados do CWA

Em uma implantação empresarial típica com várias filiais, cada filial é configurada para fornecer acesso segmentado e seguro aos convidados por meio de um Portal do Convidado assim que o convidado aceita o EULA.

Neste exemplo de configuração, o CWA 9800 é usado para acesso de convidado por meio da integração a uma instância separada do ClearPass implantada exclusivamente para usuários convidados no DMZ seguro da rede.

Os convidados devem aceitar os termos e condições estabelecidos no portal pop-up de consentimento da Web fornecido pelo servidor DMZ ClearPass. Este exemplo de configuração se concentra no método de Acesso de convidado anônimo (ou seja, nenhum nome de usuário/senha de convidado é necessário para autenticar no Portal de convidado).

O fluxo de tráfego que corresponde a essa implantação é mostrado na imagem:

1. RADIUS - Fase MAB
2. URL do Cliente Convidado redirecionar para o Portal Convidado
3. Após o convidado aceitar o EULA no Portal do Convidado, o RADIUS CoA Reauthenticate é emitido do CPPM para o 9800 WLC
4. O convidado pode acessar a Internet

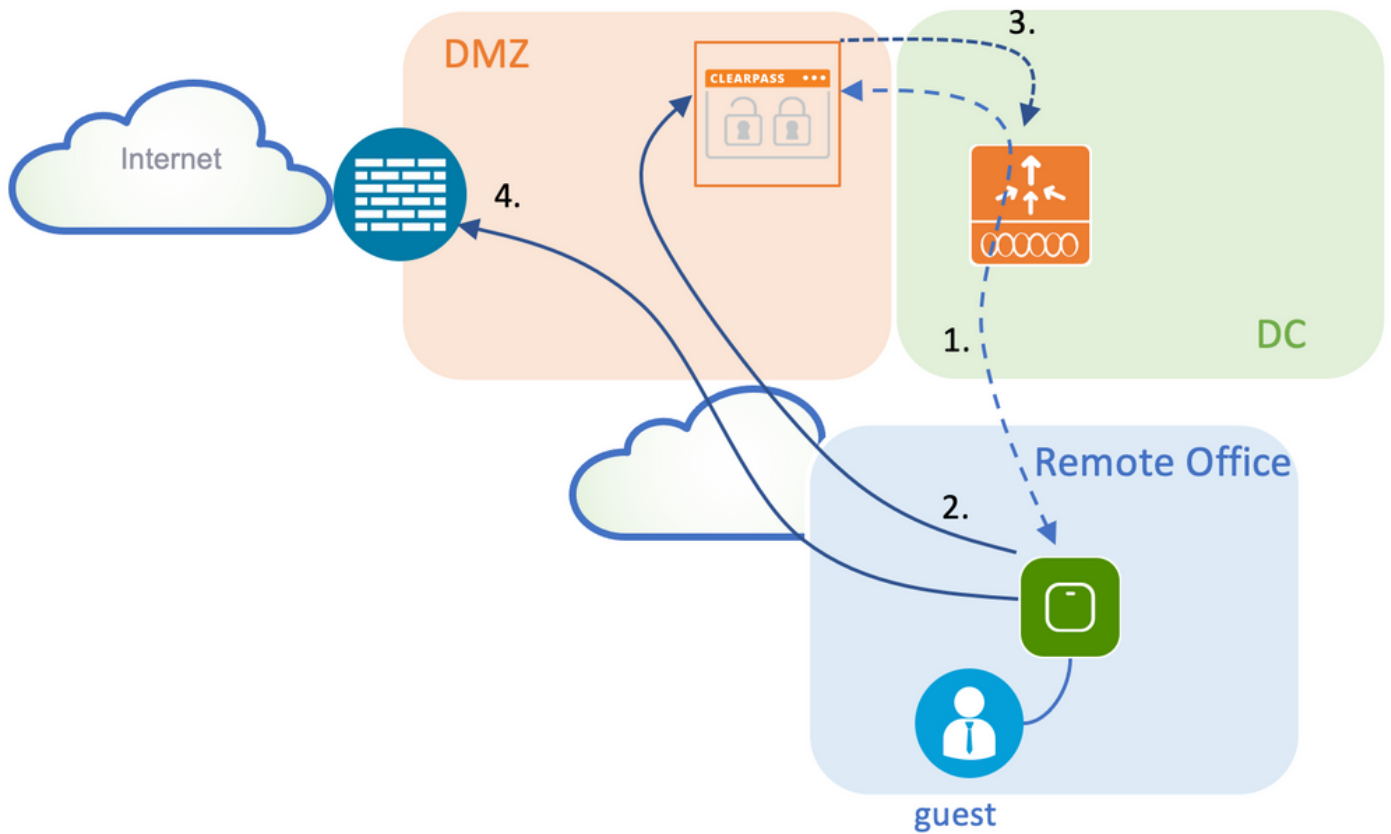
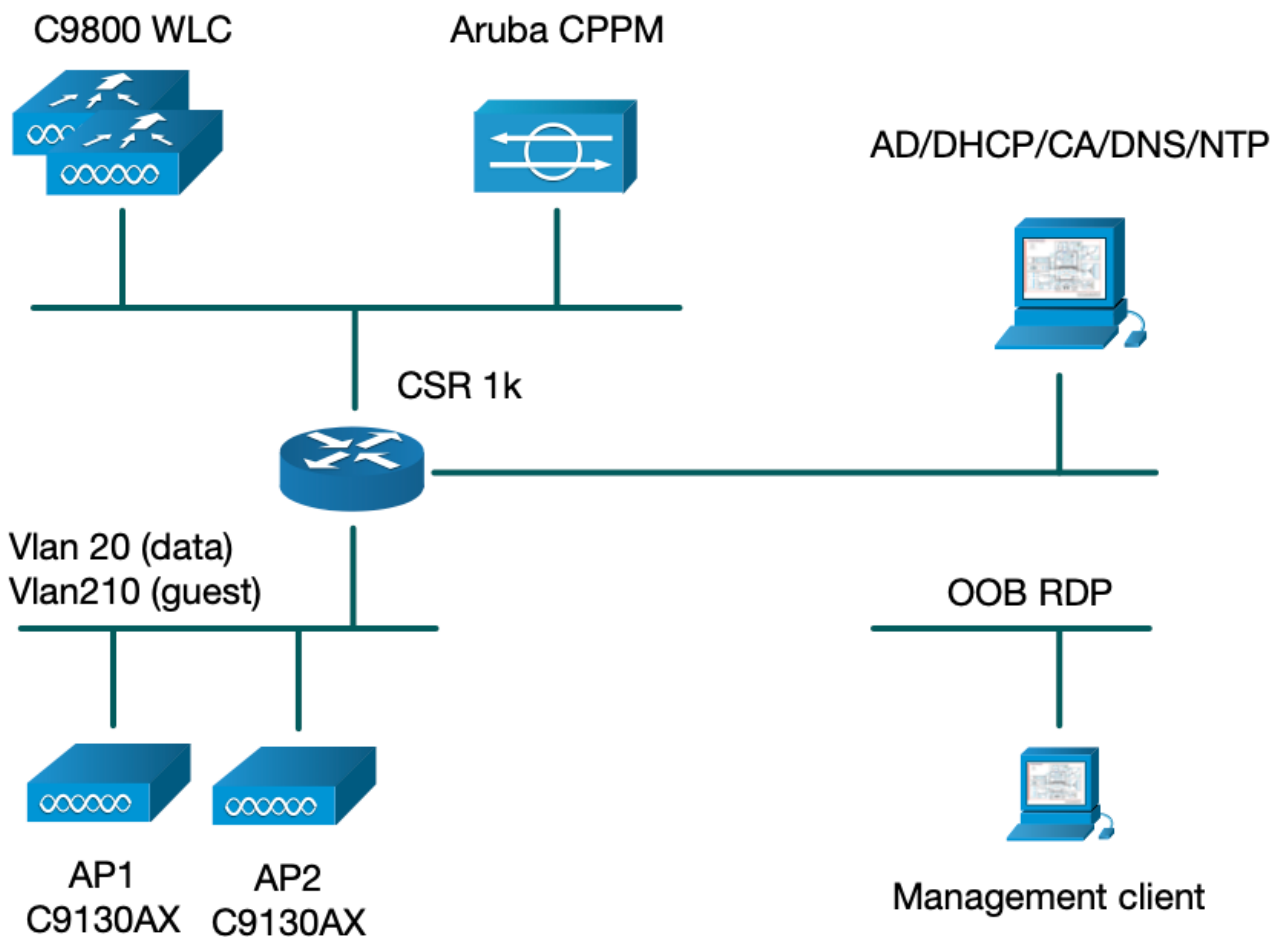


Diagrama de Rede

Note: Para fins de demonstração em laboratório, uma instância única/combinação do Aruba CPPM Server é usada para atender às funções Guest e Corp SSID Network Access Server (NAS). A implementação de práticas recomendadas sugere instâncias NAS independentes.



Configurar

Neste exemplo de configuração, um novo modelo de configuração no C9800 é utilizado para criar os perfis e tags necessários para fornecer acesso corporativo dot1x e acesso de convidado CWA à filial da empresa. A configuração resultante é resumida nesta imagem:

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

Configurar parâmetros C9800 de acesso sem fio de convidado

C9800 - Configuração AAA para convidado

Note: Sobre o bug da Cisco ID [CSCvh03827](#), certifique-se de que os servidores de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization, and Accounting) definidos não tenham balanceamento de carga, já que o mecanismo depende da persistência SessionID na WLC para trocas ClearPass RADIUS.

Etapa 1. Adicione o(s) servidor(es) DMZ Aruba ClearPass à configuração da WLC 9800 e crie uma lista de métodos de autenticação. Navegue para **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add** e insira as informações dos servidores 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* (i)	<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

Etapa 2. Defina o grupo de servidores AAA para convidados e atribua o servidor configurado na Etapa 1 a esse grupo de servidores. Navegue até **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add**.

Create AAA Radius Server Group ✕

Name*	<input type="text" value="AAA_Radius_CPPM "/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="5"/>
Source Interface VLAN ID	<input type="text" value="1"/>

Available Servers

Assigned Servers



CPPM



Etapa 3. Defina uma lista de métodos de autorização para acesso de convidado e mapeie o grupo de servidores criado na Etapa 2. Navegue para **Configuration > Security > AAA > AAA Method List > Authorization > +Add**. Escolha **Type Network** e depois **AAA Server Group** configurado na Etapa 2.

Quick Setup: AAA Authorization ✕

Method List Name*

Type* network (i)

Group Type (i)

Fallback to local

Authenticated

Available Server Groups Assigned Server Groups

<ul style="list-style-type: none">radiusldaptacacs+	> < >> <<	<ul style="list-style-type: none">AAA_Radius_CPPM	^ ^ v v
---	--------------------	---	------------------

Etapa 4. Crie uma lista de métodos de Contabilidade para acesso de convidado e mapeie o grupo de servidores criado na Etapa 2. Navegue para **Configuration > Security > AAA > AAA Method List > Accounting > +Add**. Escolha **Type Identity** no menu suspenso e depois **AAA Server Group** configurado na Etapa 2.

Quick Setup: AAA Accounting ✕

Method List Name*

Type* identity (i)

Available Server Groups Assigned Server Groups

<ul style="list-style-type: none">radiusldaptacacs+	> < >> <<	<ul style="list-style-type: none">AAA_Radius_CPPM	^ ^ v v
---	--------------------	---	------------------

A ACL de redirecionamento define qual tráfego deve ser redirecionado para o Portal do Convidado em vez de ter permissão para passar sem redirecionamento. Aqui, a ACL deny implica ignorar redirecionamento ou passar, enquanto permit implica redirecionar para o portal. Para cada classe de tráfego, você precisa considerar a direção do tráfego ao criar entradas de controle de acesso (ACEs) e criar ACEs que correspondam ao tráfego de entrada e saída.

Navegue até **Configuration > Security > ACL** e defina uma nova ACL chamada **CAPTIVE_PORTAL_REDIRECT**. Configure a ACL com estas ACEs:

- ACE1: Permite que o tráfego ICMP (Internet Control Message Protocol) bidirecional ignore o redirecionamento e é usado principalmente para verificar a acessibilidade.
- ACE10, ACE30: Permite o fluxo de tráfego DNS bidirecional para o servidor DNS 10.0.10.4 e não pode ser redirecionado para o portal. Uma busca e interceptação de DNS para resposta são necessárias para disparar o fluxo de convidados.
- ACE70, ACE80, ACE110, ACE120: Permite acesso HTTP e HTTPS ao portal cativo de convidado para que o usuário seja apresentado ao portal.
- ACE150: Todo o tráfego HTTP (porta UDP 80) é redirecionado.

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 - Configuração de perfil de WLAN de convidado

Etapa 1. Navegue até **Configuration > Tags & Profiles > Wireless > +Add**. Crie um novo perfil SSID WP_Guest, com a transmissão de SSID 'Guest' ao qual os clientes convidados se associam.

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	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="3"/>		
Status	ENABLED <input checked="" type="checkbox"/>		

↶ Cancel

📄
Apply to Device

Na mesma caixa de diálogo **Add WLAN**, navegue até a guia **Security > Layer 2**.

- Modo de segurança da camada 2: Nenhum

- Filtragem MAC: Habilitado

- Lista de autorização: AAA_Authz_CPPM no menu suspenso (configurado na Etapa 3. como parte da configuração 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 - Definição de perfil de política de convidado

Na GUI da WLC C9800, navegue para **Configuration > Tags & Profiles > Policy > +Add**.

Nome: PP_Guest

Status: Habilitado

Switching central: Desabilitado

Autenticação Central: Habilitado

DHCP central: Desabilitado

Associação Central: Desabilitado

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*

PP_Guest

Description

Policy Profile for Guest

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED


Central Association

DISABLED

Flex NAT/PAT

DISABLED

 Cancel

 Apply to Device

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	
Description	Profile for Branch Guest	WLAN Switching Policy
Status	<input type="checkbox"/> DISABLED	Central Switching <input type="checkbox"/> DISABLED
Passive Client	<input type="checkbox"/> DISABLED	Central Authentication ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central DHCP <input type="checkbox"/> DISABLED
CTS Policy		Central Association <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>	Flex NAT/PAT <input type="checkbox"/> DISABLED
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

↶ Cancel 📄 Apply to Device

Navegue até a guia **Access Policies** na mesma caixa de diálogo **Add Policy Profile**.

- Criação de perfis RADIUS: Habilitado
- Grupo VLAN/VLAN: 210 (ou seja, a VLAN 210 é a VLAN local do convidado em cada filial)

Note: A VLAN de convidado para Flex não deve ser definida na WLC 9800 em VLANs, no VLAN/VLAN Group type VLAN number.

Defeito conhecido: o bug da Cisco ID [CSCvn48234](#) faz com que o SSID não seja transmitido se a mesma VLAN de convidado Flex for definida no WLC e no 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

Na mesma caixa de diálogo **Add Policy Profile**, navegue até a guia **Advanced**.

- Permitir substituição de AAA: Habilitado

- Estado NAC: Habilitado

- Tipo de NAC: RADIUS

- Lista de contabilidade: AAA_Accounting_CPPM (definido na Etapa 4. como parte da configuração AAA)

⚠ 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

Note: 'Network Admission Control (NAC) State - Enable' é necessário para permitir que a WLC C9800 aceite mensagens RADIUS CoA.

C9800 - Marca de política

Na GUI do C9800, navegue para **Configuration > Tags & Profiles > Tags > Policy > +Add**.

-Nome: PT_CAN01

-Descrição: Marca de política para o site da filial CAN01

Na mesma caixa de diálogo **Add Policy Tag**, em **WLAN-POLICY MAPS**, clique em **+Add** e mapeie o Perfil de WLAN criado anteriormente para o Perfil de política:

- Perfil de WLAN: WP_Guest

- Perfil da política: PP_Guest

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

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

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

C9800 - Perfil de junção de AP

Na GUI da WLC C9800, navegue para **Configuration > Tags & Profiles > AP Join > +Add**.

-Nome: Branch_AP_Profile

- Servidor NTP: 10.0.10.4 (consulte o diagrama de topologia do laboratório). Este é o servidor NTP usado pelos APs na Filial para sincronização.

Add AP Join Profile ✕

General Client CAPWAP AP Management Security ICap QoS

Name*

Description

LED State

LAG Mode

NTP Server

GAS AP Rate Limit

Apphost


OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

 Cancel

 Apply to Device

C9800 - Perfil Flex

Os perfis e marcas são modulares e podem ser reutilizados para vários sites.

No caso da implantação do FlexConnect, se as mesmas IDs de VLAN forem usadas em todos os locais da filial, você poderá reutilizar o mesmo perfil flex.

Etapa 1. Em uma GUI do C9800 WLC, navegue para **Configuration > Tags & Profiles > Flex > +Add**.

-Nome: FP_Branch

- ID da VLAN nativa: 10 (obrigatório apenas se você tiver uma VLAN nativa não padrão onde deseja ter uma interface de gerenciamento 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

Na mesma caixa de diálogo **Add Flex Profile**, navegue até a guia **Policy ACL** e clique em **+Add**.

- Nome da ACL: `CATIVE_PORTAL_REDIRECT`

- Autenticação da Web Central: Habilitado

Em uma implantação do Flexconnect, espera-se que cada AP gerenciado faça download da ACL de redirecionamento localmente, pois o redirecionamento acontece no AP e não no C9800.

Add Flex Profile ✕

General Local Authentication **Policy ACL** VLAN Umbrella

ACL Name	Central Web Auth	Pre Auth URL Filter
0	10	No items to display

10 items per page

ACL Name*

Central Web Auth

Pre Auth URL Filter

Na mesma caixa de diálogo **Add Flex Profile**, navegue até a guia **VLAN** e clique em **+Add** (consulte o diagrama de topologia do laboratório).

- Nome da VLAN: convidado

-ID da 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 - Marca do local

Na GUI da WLC 9800, navegue para **Configuration > Tags & Profiles > Tags > Site > Add**.

Note: Crie uma Tag de Site exclusiva para cada Site Remoto que precise suportar os dois SSIDs sem fio, conforme descrito.

Há um mapeamento 1-1 entre uma localização geográfica, a marca do site e uma configuração do perfil Flex.

Um site de conexão flexível deve ter um perfil de conexão flexível associado a ele. Você pode ter no máximo 100 pontos de acesso para cada site de conexão flexível.

-Nome: ST_CAN01

- Perfil de ingresso no AP: Branch_AP_Profile

- Perfil Flex: FP_Branch

- Habilitar Site Local: Desabilitado

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

Na GUI da WLC 9800, navegue para **Configuration > Tags & Profiles > Tags > RF > Add**.

-Nome: Filial_RF

- Perfil de radiofrequência (RF) da banda de 5 GHz: Typical_Client_Density_5gh (opção definida pelo sistema)

- Perfil de RF de banda de 2,4 GHz: Typical_Client_Density_2gh (opção definida pelo sistema)

The screenshot shows the 'Add RF Tag' configuration window. The fields are as follows:

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

Buttons: Cancel, Apply to Device

C9800 - Atribuir tags ao AP

Há duas opções disponíveis para atribuir tags definidas a APs individuais na implantação:

- Atribuição baseada em nome de AP, que aproveita regras regex que correspondem a padrões no campo Nome de AP (**Configurar > Tags e perfis > Tags > AP > Filtro**)

- Atribuição baseada em endereço MAC Ethernet do AP (**Configurar > Tags e perfis > Tags > AP > Estático**)

Na implantação da produção com o DNA Center, é altamente recomendável usar o DNAC e o fluxo de trabalho PNP do AP ou usar um método de carregamento em massa CSV (Comma-Separated Values, valores separados por vírgula) disponível no 9800 para evitar a atribuição manual por AP. Navegue até **Configure > Tags & Profiles > Tags > AP > Static > Add** (Observe a opção **Upload File**).

- Endereço MAC do AP: <AP_ETHERNET_MAC>

- Nome da tag de política: PT_CAN01

- Nome da tag do site: ST_CAN01

- Nome da etiqueta RF: Filial_RF

Note: A partir do Cisco IOS®-XE 17.3.4c, há um máximo de 1.000 regras regex por limitação de controlador. Se o número de locais na implantação exceder esse número, a atribuição estática por MAC deverá ser aproveitada.

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

Note: Como alternativa, para aproveitar o método de atribuição de tag baseado em regex do nome do AP, navegue para **Configurar > Tags e perfis > Tags > AP > Filtro > Adicionar**.

-Nome: BR_CAN01

- Regex do nome do AP: BR-CAN01-.(7) (Esta regra corresponde à convenção de nome AP adotada dentro da organização. Neste exemplo, as tags são atribuídas aos APs que têm um campo AP Name que contém 'BR_CAN01-' seguido por sete caracteres.)

-Prioridade: 1

- Nome da tag de política: PT_CAN01 (conforme definido)

- Nome da tag do site: ST_CAN01

- Nome da etiqueta RF: Filial_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
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01
Active	YES	RF Tag Name	Branch_RF
Priority*	1		

Cancel

Apply to Device

Configurar a instância Aruba CPPM

Para configuração de CPPM Aruba baseada em práticas recomendadas/de produção, entre em

contato com o recurso HPE Aruba SE local.

Configuração inicial do Aruba ClearPass Server

O Aruba ClearPass é implantado com o uso do modelo OVF (Open Virtualization Format) no servidor ESXi <> que aloca os seguintes recursos:

- Duas CPUs virtuais reservadas
- 6 GB de RAM
- Disco de 80 GB (deve ser adicionado manualmente após a implantação inicial da VM antes que a máquina seja ligada)

Inscreeva-se para obter licenças

Aplice a licença da plataforma via: **Administração > Gerenciador de servidores > Licenciamento**. Adicione licenças de plataforma, acesso e onboard.

Nome de host do servidor

Navegue para **Administration > Server Manager > Server Configuration** e escolha o servidor CPPM provisionado recentemente.

-Hostname: Cppm

- FQDN: cppm.example.com

- Verifique o endereçamento IP e o DNS da porta de gerenciamento

Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

The screenshot shows the 'Server Configuration' page for a CPPM server. The 'System' tab is active, and the 'Network' sub-tab is selected. The 'Management Port' configuration is highlighted with a yellow box. The 'DNS Settings' section is also visible, with the 'Primary' IP address highlighted.

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			

Gerar Certificado de Servidor Web CPPM (HTTPS)

Este certificado é usado quando a página ClearPass Guest Portal é apresentada via HTTPS aos clientes convidados que se conectam ao Guest Wifi na Filial.

Etapa 1. Carregar o certificado da cadeia de publicação da CA.

Navegue até **Administração > Certificados > Lista confiável > Adicionar.**

-Uso: Habilitar outros

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**

Etapa 2. Criar Solicitação de Assinatura de Certificado.

Navegue até **Administração > Certificados > Armazenamento de certificados > Certificados do servidor > Uso: Certificado de servidor HTTPS.**

- Clique na opção **Criar** solicitação de assinatura de certificado

- Denominação comum: CPPM

- Organização: **cppm.example.com**

Certifique-se de preencher o campo SAN (um nome comum deve estar presente na SAN, bem

como no IP e em outros FQDNs, conforme necessário). O formato é DNS: <fqdn1>,DNS:<fqdn2>,IP<ip1>.

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
Submit Cancel	

Etapa 3. Em sua CA de escolha, assine o CSR do serviço HTTPS do CPPM recém-gerado.

Etapa 4. Navegue até **Modelo de certificado > Servidor Web > Importar certificado**.

- Tipo de certificado: Server Certificate

-Uso: Certificado do servidor HTTP

- Arquivo de certificado: Procure e selecione o certificado de serviço CPPM HTTPS assinado pela CA

Import Certificate	
Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	<input type="button" value="Browse..."/> No file selected.
Import Cancel	

Definir a WLC C9800 como um dispositivo de rede

Navegue até **Configuration > Network > Devices > Add**.

-Nome: WLC_9800_Branch

- Endereço IP ou de sub-rede: 10.85.54.99 (consulte o diagrama de topologia do laboratório)

- Cisco RADIUS compartilhada: <senha RADIUS da WLC>

- Nome do fornecedor: Cisco

- Habilitar Autorização Dinâmica 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**

Página do Portal do Convidado e Temporizadores de CoA

É muito importante definir os valores corretos do temporizador em toda a configuração. Se os temporizadores não estiverem ajustados, você provavelmente encontrará um redirecionamento de Portal da Web cíclico com o cliente fora do 'Estado de Execução'.

Temporizadores para prestar atenção a:

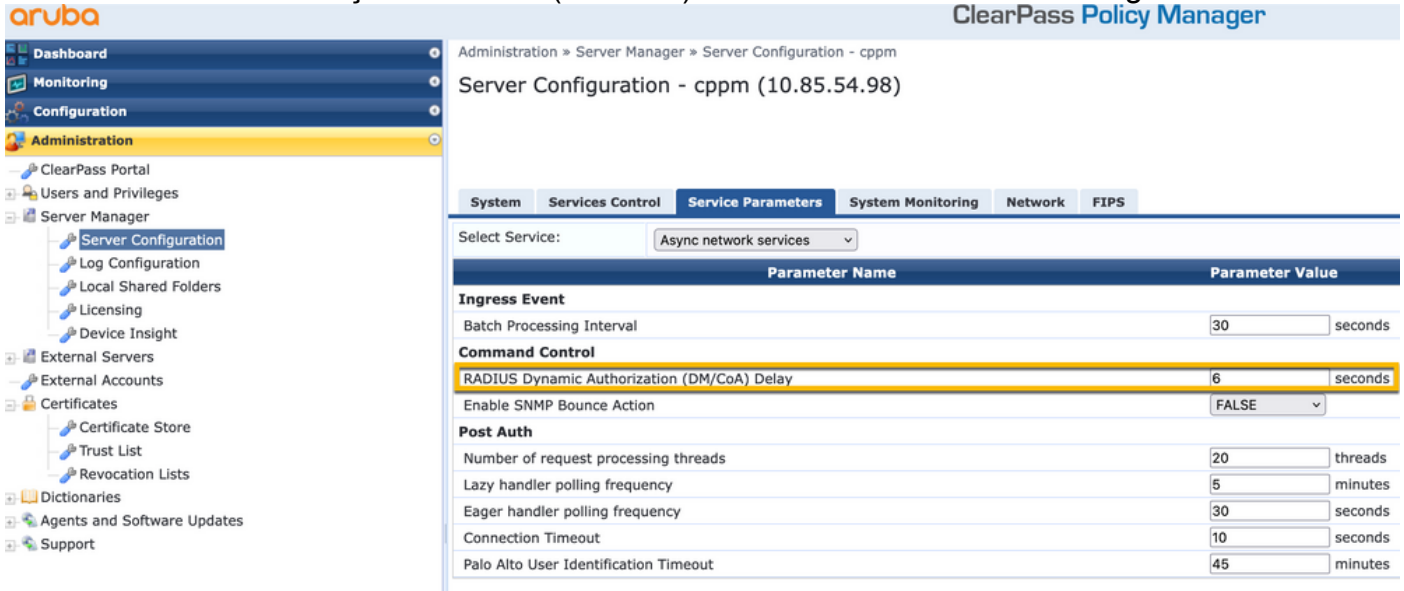
- Temporizador de logon no portal da Web: este temporizador atrasa sua página de redirecionamento antes que ela permita acesso à página do portal convidado para notificar o serviço CPPM sobre a transição de estado, registrar o valor de atributo personalizado 'Allow-Guest-Internet' do ponto de extremidade e disparar o processo de CoA de CPPM para WLC. Navegue até **Guest > Configuration > Pages > Web Logins**.
 - Escolher Nome do Portal de Convidado: Lab Anonymous Guest Registration (esta configuração da página do Portal do convidado é detalhada como mostrado)
 - Clique em **Editar**
 - Atraso de login: 6 segundos

* Login Delay: 6
The time in seconds to delay while displaying the login message.

- Temporizador de atraso de CoA ClearPass: Isso atrasa a origem das mensagens de CoA do ClearPass para a WLC. Isso é necessário para que o CPPM faça a transição do estado do

Ponto de Extremidade do Cliente internamente antes que a Confirmação de CoA (ACK) volte do WLC. Os testes de laboratório mostram os tempos de resposta em menos de milissegundos da WLC e, se o CPPM não tiver terminado de atualizar os atributos do endpoint, a nova sessão RADIUS da WLC será correspondida à política de imposição do serviço MAB não autenticado e o cliente receberá uma página de redirecionamento novamente. Navegue para **CPPM > Administration > Server Manager > Server Configuration** e escolha **CPPM Server > Service Parameters**.

- Atraso de Autorização Dinâmica (DM/CoA) RADIUS - Definido como 6 segundos



ClearPass - Configuração do CWA para Convidados

A configuração do CWA do ClearPass é composta de (3) pontos de serviço/estágios:

Componente ClearPass	Tipo de serviço	Propósito
1. Gerente de políticas	Serviço: Autenticação Mac	Se o atributo personalizado Allow-Guest-Internet = TRUE, permite na rede. Caso contrário, aciona Redirect e COA: Reautenticar . Apresente a página AUP de login anônimo.
2. Convidado	Logins da Web	O atributo personalizado do conjunto de pós-autenticação Allow-Guest-Internet = TRUE. Atualizar Ponto de Extremidade para Conhecido
3. Gestor de políticas	Serviço: Autenticação baseada na Web	Defina o atributo personalizado Allow-Guest-Internet = TRUE COA: Reautenticar

Atributo de Metadados de Ponto de Extremidade ClearPass: Allow-Guest-Internet

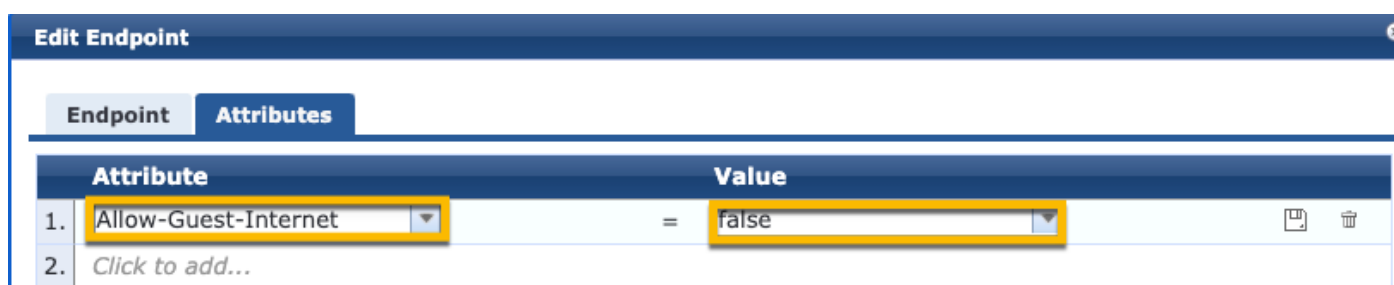
Crie um atributo de metadados do tipo Booleano para controlar o estado do Ponto de Extremidade Convidado à medida que o cliente faz a transição entre o estado 'Webauth Pendente' e 'Executar':

- Novos convidados que se conectam a WiFi têm um atributo de metadados padrão definido como Allow-Guest-Internet=false. Com base nesse atributo, a autenticação do cliente passa pelo serviço MAB



- O cliente convidado, quando você clica no botão AUP Accept, tem seu atributo de metadados atualizado para Allow-Guest-Internet=true. O MAB subsequente baseado nesse atributo definido como True permite acesso não redirecionado à Internet

Navegue para ClearPass > Configuration > Endpoints, selecione qualquer endpoint da lista, clique na guia **Attributes**, adicione Allow-Guest-Internet com o valor false e Save.

Note: Você também pode editar o mesmo ponto final e excluir esse atributo logo depois - essa etapa simplesmente cria um campo no BD de metadados de Pontos Finais que pode ser usado em políticas.



The screenshot shows the 'Edit Endpoint' window with the 'Attributes' tab selected. It displays a table with two columns: 'Attribute' and 'Value'. The first row contains 'Allow-Guest-Internet' in the 'Attribute' column and 'false' in the 'Value' column. The second row is a placeholder with the text 'Click to add...'. There are also icons for saving and deleting at the end of the first row.

	Attribute	Value	
1.	Allow-Guest-Internet	= false	 
2.	Click to add...		

Configuração de Política de Imposição de Reautenticação ClearPass

Crie um Perfil de Imposição atribuído ao cliente convidado imediatamente após o cliente aceitar AUP na página Portal do Convidado.

Navegue até **ClearPass > Configuration > Profiles > Add**.

- Modelo: Autorização dinâmica RADIUS

-Nome: 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:	<input type="text"/> --Select--	Remove View Details Modify

Radius:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station-Id}
Radius:Cisco	Cisco-AVPair	assinante:command=reauthen
Radius:Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-session}
Radius:Cisco	Cisco-AVPair	assinante:reauthenticate-type=type=last

Configuração do Perfil de Imposição de Redirecionamento do Portal de Convidado ClearPass

Crie um Perfil de Imposição que seja aplicado ao Convidado durante a fase MAB inicial, quando o endereço MAC não for encontrado no Banco de Dados de Ponto de Extremidade CPPM com 'Allow-Guest-Internet' definido como 'true'.

Isso faz com que a WLC 9800 redirecione o cliente convidado para o Portal de Convidado CPPM para autenticação externa.

Navegue até **ClearPass > Imposição > Perfis > Adicionar**.

-Nome: Cisco_Portal_Redirect

-Digite: RADIUS

-Ação: Aceitar

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:	<input type="text"/>	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>
	--Select--	

Perfil de Imposição de Redirecionamento ClearPass

Na mesma caixa de diálogo, na guia **Atributos**, configure dois Atributos de acordo com esta imagem:

Enforcement Profiles - Cisco_Portal_Redirect

Summary	Profile	Atributos
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/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

Atributos do perfil de redirecionamento ClearPass

O atributo **url-redirect-acl** é definido como **CAPTIVE-PORTAL-REDIRECT**, que é o nome da ACL criada no C9800.

Note: Somente a referência à ACL é passada na mensagem RADIUS, e não o conteúdo da ACL. É importante que o nome da ACL criada na WLC 9800 corresponda exatamente ao valor desse atributo RADIUS, como mostrado.

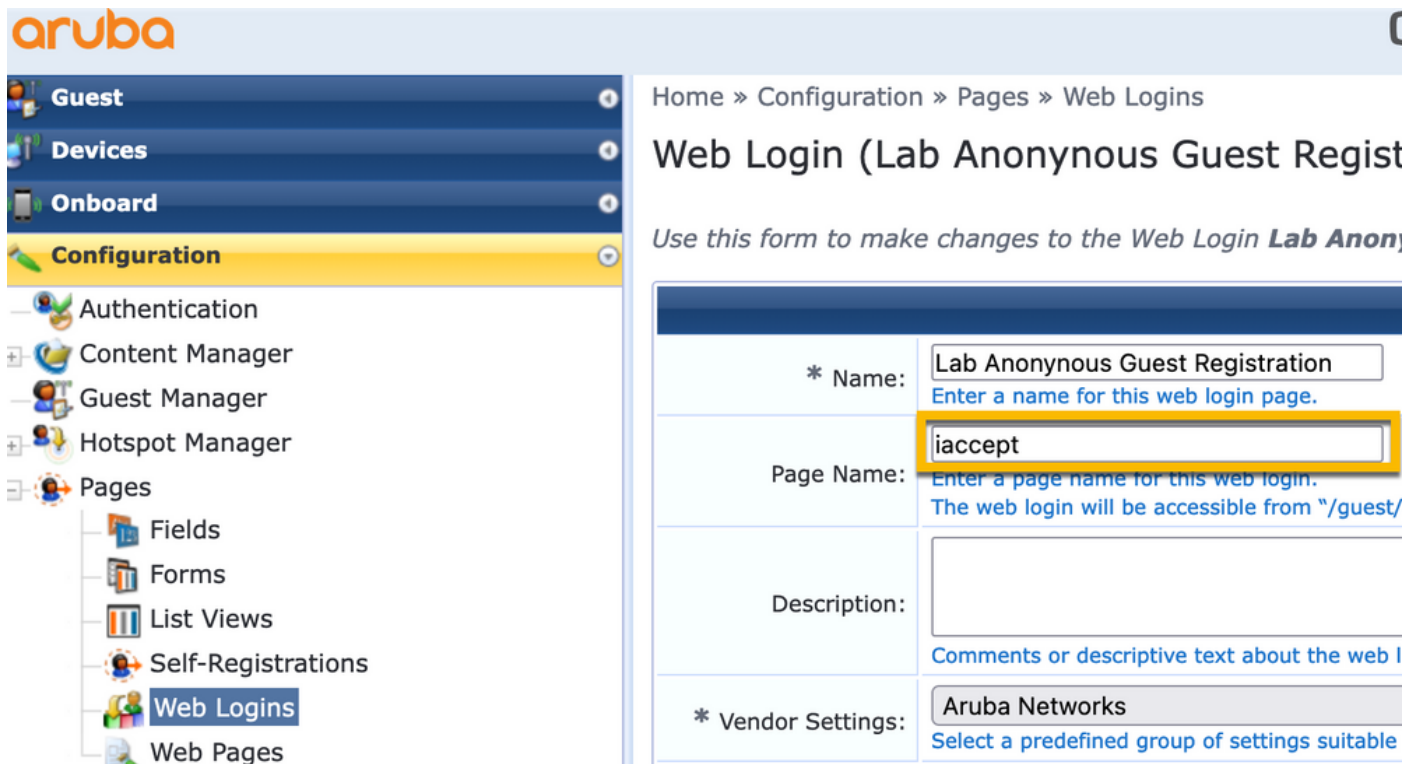
O atributo **url-redirect** é composto de vários parâmetros:

- A URL de destino onde o Portal do Convidado está hospedado, <https://cppm.example.com/guest/iaccept.php>
- **MAC de Cliente Convidado**, macro %{Connection:Client-Mac-Address-Hyphen}
- **Authenticator IP** (9800 WLC dispara o redirecionamento), macro %{Radius:IETF:NAS-IP-Address}
- ação **cmd-login**

A URL da Página de Logon da Web Convidado do ClearPass é vista quando você navega para **CPPM > Convidado > Configuração > Páginas > Logons da Web > Editar**.

Neste exemplo, o nome da página do Portal do Convidado no CPPM é definido como **iaccept**.

Note: As etapas de configuração para a página Portal do convidado são as descritas.



The screenshot displays the Aruba configuration interface. On the left, a navigation menu is visible with the following items: Guest, Devices, Onboard, Configuration (highlighted), Authentication, Content Manager, Guest Manager, Hotspot Manager, and Pages. Under 'Pages', there are sub-items: Fields, Forms, List Views, Self-Registrations, Web Logins (selected), and Web Pages. The main content area shows the breadcrumb 'Home » Configuration » Pages » Web Logins' and the title 'Web Login (Lab Anonymus Guest Regist'. Below the title, there is a note: 'Use this form to make changes to the Web Login Lab Anonymus Guest Registration'. The configuration form contains the following fields: '* Name:' with the value 'Lab Anonymus Guest Registration'; 'Page Name:' with the value 'iaccept' (highlighted in yellow); 'Description:' which is empty; and '* Vendor Settings:' with the value 'Aruba Networks'. There are also blue links for help text: 'Enter a name for this web login page.', 'Enter a page name for this web login. The web login will be accessible from "/guest/', and 'Comments or descriptive text about the web login page'.

Note: Para dispositivos Cisco, **audit_session_id** seria normalmente usado, mas não é suportado por outros fornecedores.

Configuração do Perfil de Imposição de Metadados ClearPass

Configure o Perfil de Imposição para atualizar o atributo de metadados de Ponto de Extremidade usado para o rastreamento de transição de estado pelo CPPM.

Este perfil é aplicado à entrada de Endereço MAC do Cliente Convidado no banco de dados de Ponto de Extremidade e define o argumento '**Allow-Guest-Internet**' como '**true**'.

Navegue até **ClearPass > Imposição > Perfis > Adicionar**.

- Modelo: Imposição de Atualização de Entidade ClearPass

- Digite: Pós-autenticação

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="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="display: flex; justify-content: flex-end; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Modify</div> </div>	

No mesmo diálogo, a guia **Atributos**.

-Digite: Endpoint

-Nome: Allow-Guest-Internet

Note: Para que esse nome apareça no menu suspenso, você precisa definir manualmente esse campo para pelo menos um ponto final, conforme descrito nas Etapas.

-Valor: verdadeiro

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Endpoint	Allow-Guest-Internet	= true
2. <i>Click to add...</i>		

Configuração da Política de Imposição de Acesso à Internet de Convidado ClearPass

Navegue até **ClearPass > Aplicação > Políticas > Adicionar**.

-Nome: Permissão de Convidado Cisco da WLC

- Tipo de aplicação: RADIUS

- Perfil padrão: Cisco_Portal_Redirect

Enforcement Policies

Enforcement Rules Summary

Name: WLC Cisco Guest Allow

Description:

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

Default Profile: Cisco_Portal_Redirect **View Details** **Modify**

Na mesma caixa de diálogo, navegue até a guia **Regras** e clique em **Adicionar regra**.

-Digite: Endpoint

-Nome: Allow-Guest-Internet

- Operador: IGUAL A

- Valor Verdadeiro

- Nomes de perfil / Selecione para adicionar: [RADIUS] [Permitir Perfil de Acesso]

Rules Editor

Conditions

Match ALL of the following conditions:

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

Enforcement Profiles

Profile Names: [RADIUS] [Allow Access Profile]

Move Up ↑
Move Down ↓
Remove

--Select to Add--

Save **Cancel**

Configuração da Política de Imposição Pós-AUP de Convidado ClearPass

Navegue até **ClearPass > Aplicação > Políticas > Adicionar**.

-Nome: Política de aplicação de Webauth do Cisco WLC

- Tipo de aplicação: WEBAUTH (SNMP/Agente/CLI/CoA)

- Perfil padrão: [RADIUS_CoA] Cisco_Reauthenticate_Session

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_Reauth **View Details** **Modify**

Na mesma caixa de diálogo, navegue até **Regras > Adicionar**.

-Condições: Autenticação

-Nome: Status

- Operador: IGUAL A

-Valor: Usuário

- Nomes de perfil: <adicionar cada>:

- [Pós-autenticação] [Atualizar endpoint conhecido]

- [Pós-autenticação] [Tornar-Cisco-Convidado-Válido]

- [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**

Note: Se você encontrar um cenário com um pop-up contínuo do pseudonavegador de redirecionamento do Portal do Convidado, isso indica que os Temporizadores CPPM exigem ajustes ou que as mensagens RADIUS CoA não são trocadas adequadamente entre CPPM e 9800 WLC. Verifique esses sites.

Navegue até **CPPM > Monitoring > Live Monitoring > Access Tracker** e verifique se a entrada do log do RADIUS contém detalhes do RADIUS CoA.

Em **9800 WLC**, navegue para **Troubleshooting > Packet Capture**, ative o pcap na interface em que a chegada dos pacotes RADIUS CoA é esperada e verifique se as mensagens RADIUS CoA

são recebidas do CPPM.

Configuração do Serviço de Autenticação MAB ClearPass

O serviço é correspondido no par de Atributos Valor (AV) Raio: Cisco | CiscoAVPair | cisco-wlan-ssid

Navegue até **ClearPass > Configuration > Services > Add**.

Guia **Serviço**:

-Nome: GuestPortal - Autenticação Mac

-Digite: Autenticação MAC

- Mais opções: Selecionar Autorização, Pontos de Extremidade de Perfil

Adicionar regra de correspondência:

-Digite: Radius: Cisco

-Nome: Cisco-AVPair

- Operador: IGUAL A

-Valor: cisco-wlan-ssid=Convidado (corresponde ao seu nome SSID de Convidado configurado)

Note: 'Convidado' é o nome do SSID Convidado transmitido pela WLC 9800.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type: **MAC Authentication**

Name: **GuestPortal - Mac Auth**

Description: **MAC-based Authentication Service**

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		

No mesmo diálogo, escolha a guia **Autenticação**.

- Métodos de autenticação: Remova [MAC AUTH], adicione [Allow All MAC AUTH]

- Fontes de autenticação: [Repositório de Pontos de Extremidade][BD SQL Local], [Repositório de Usuário Convidado][BD SQL Local]

aruba ClearPass Policy Manager

Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]

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

No mesmo diálogo, escolha a guia **Aplicação**.

- Política de aplicação: Permissão de Convidado Cisco da WLC

Configuration » Services » Add

Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results: 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]

No mesmo diálogo, escolha a guia **Aplicação**.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

RADIUS CoA Action: Cisco_Reauthenticate_Session **View Details** **Modify**

Configuração do Serviço de Webauth ClearPass

Navegue até **ClearPass > Aplicação > Políticas > Adicionar**.

-Nome: Guest_Portal_Webauth

-Digite: Autenticação baseada na Web

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Type:	Web-based Authentication			
Name:	Guest			
Description:				
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>			

Enquanto estiver no mesmo diálogo, na guia **Aplicação**, a Política de aplicação: Política de aplicação de Webauth do Cisco WLC.

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:	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 - Logon na Web

Para a página Portal de convidado AUP anônimo, use um único nome de usuário sem campo de senha.

O nome de usuário usado deve ter estes campos definidos/definidos:

username_auth | Autenticação de nome de usuário: | 1

Para definir o campo 'username_auth' para um usuário, esse campo deve ser exposto primeiro no formulário 'edit user'. Navegue para **ClearPass > Guest > Configuration > Pages > Forms** e escolha o formulário **create_user**.

aruba ClearPass Guest

Home » Configuration » Pages » Forms

Customize Forms

Use this list view to customize the forms within the application.

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	

Selecione **visitor_name** (linha 20) e clique em **Inserir depois**.

Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

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

Quick Help Preview Form

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:	<input type="text" value="username_auth"/> <small>Select the field definition to attach to the form.</small>
Form Display Properties <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	<input type="text" value="22"/> <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	<input type="text" value="No user interface"/> <input type="button" value="Revert"/> <small>The kind of user interface element to use when entering or editing this field.</small>
Form Validation Properties <small>These properties control how the value of this field is checked.</small>	
Field Required:	<input type="checkbox"/> Field value must be supplied <small>Select this option if the field cannot be omitted or left blank.</small>
Initial Value:	<input type="text" value="1"/> <input type="button" value="Revert"/> <small>Value to initialize this field with when the form is first displayed.</small>
* Validator:	<input type="text" value="IsValidBool"/> <small>The function used to validate the contents of a field.</small>
Validator Param:	<input type="text" value="(None)"/> <small>Optional name of field whose value will be supplied as the argument to a validator.</small>
Validator Argument:	<input type="text"/> <small>Optional value to supply as the argument to a validator.</small>
Validation Error:	<input type="text"/> <small>The error message to display if the field's value fails validation and the validator does not return an error message directly.</small>

Agora, crie o nome de usuário a ser usado atrás da página do Portal de Convidado AUP.

Navegue até **CPPM > Convidado > Convidado > Gerenciar contas > Criar**.

- Nome do convidado: WiFi de convidado
- Nome da empresa: Cisco
- Endereço de e-mail: guest@example.com
- Autenticação de nome de usuário: Permitir acesso de convidado com o uso apenas do nome de usuário: Habilitado
- Ativação da conta: Agora
- Vencimento da conta: A conta não expira
- Termos de uso: Sou o patrocinador: Habilitado

Create Guest Account

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

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

Criar Formulário de Logon na Web. Navegue até **CPPM > Convidado > Configuração > Logins da Web**.

Os atributos de ponto final na seção de pós-autenticação:

nome do usuário | Nome de usuário

nome_visitante | Nome do visitante

cn | Nome do visitante

visitor_phone | Telefone do visitante

e-mail | E-mail

correio | E-mail

nome_do_patrocinador | Nome do patrocinador

e-mail_do_patrocinador | E-mail do patrocinador

Allow-Guest-Internet | verdadeiro

No CPPM, navegue para **Monitoramento em tempo real > Controlador de acesso**.

O novo usuário convidado que conecta e aciona o serviço MAB.

Guia **Resumo**:

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**

Na mesma caixa de diálogo, navegue até a guia **Entrada**.

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**

Na mesma caixa de diálogo, navegue até a guia **Saída**.

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

Para fins de referência, um fluxograma de estado é apresentado aqui para as interações do

controlador Âncora, Externo Cisco 9800 com o servidor RADIUS e o Guest Portal hospedado externamente.

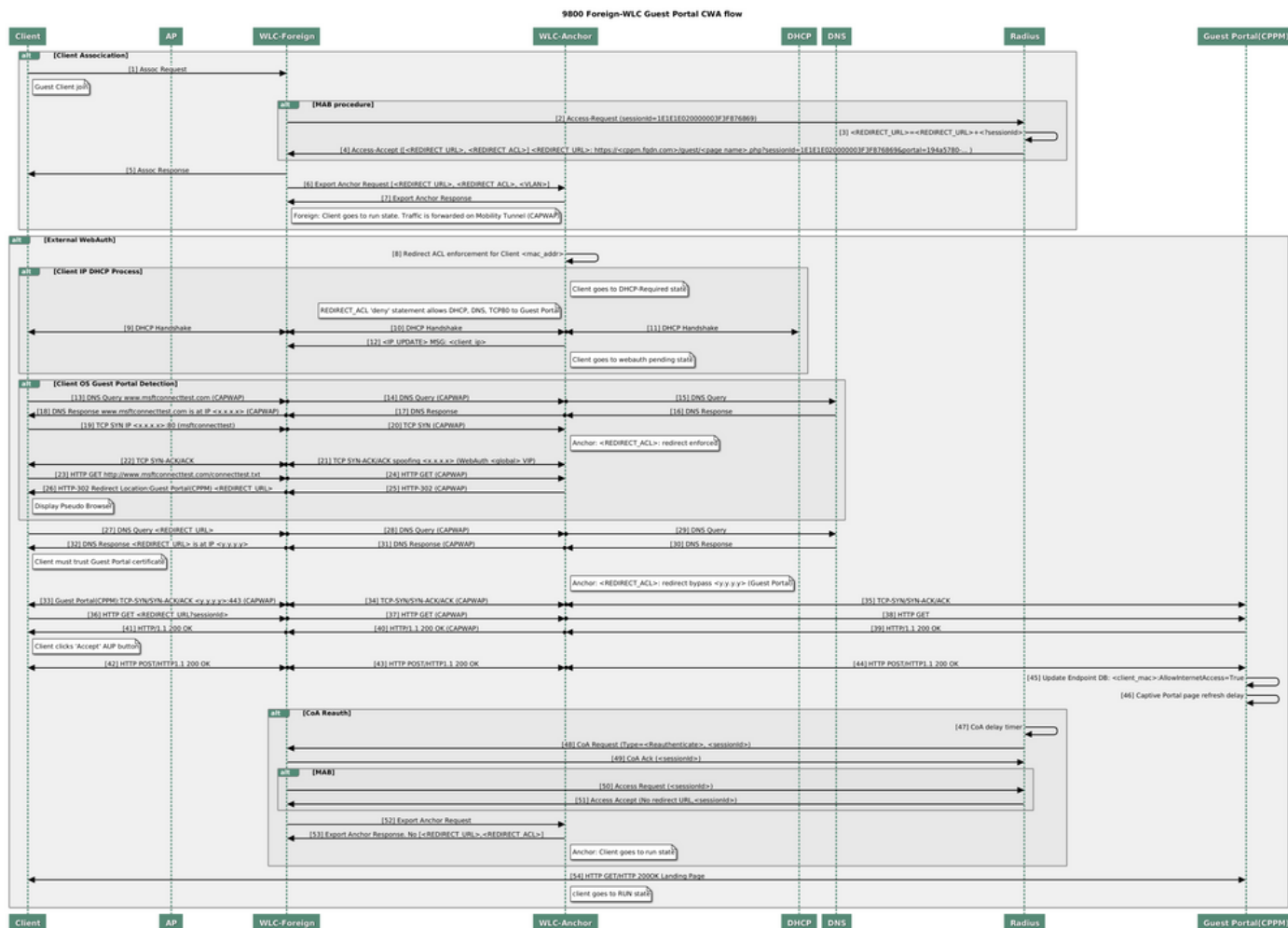


Diagrama de Estado de Autenticação da Web Central de Convidados com WLC de Âncora

Informações Relacionadas

- [Guia de práticas recomendadas de implantação do Cisco 9800](#)
- [Compreender o Modelo de Configuração dos Catalyst 9800 Wireless Controllers](#)
- [Entender o FlexConnect no Catalyst 9800 Wireless Controller](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.