

# Configurer le WLC 9800 et Aruba ClearPass - Guest Access & FlexConnect

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Flux de trafic pour le déploiement CWA Guest Enterprise](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configuration des paramètres de l'accès sans fil invité C9800](#)

[C9800 - Configuration AAA pour invité](#)

[C9800 - Configurer la liste de contrôle d'accès Redirection](#)

[C9800 - Configuration du profil WLAN invité](#)

[C9800 - Définition du profil de politique d'invité](#)

[C9800 - Balise de stratégie](#)

[C9800 - Profil de jonction AP](#)

[C9800 - Profil flexible](#)

[C9800 - Étiquette de site](#)

[C9800 - Profil RF](#)

[C9800 - Attribuer des balises au point d'accès](#)

[Configurer l'instance Aruba CPPM](#)

[Configuration initiale du serveur Aruba ClearPass](#)

[Demander des licences](#)

[Server Hostname](#)

[Générer un certificat de serveur Web CPPM \(HTTPS\)](#)

[Définir le WLC C9800 comme périphérique réseau](#)

[Page Guest Portal et minuteurs CoA](#)

[ClearPass - Configuration CWA invité](#)

[Attribut de métadonnées du point de terminaison ClearPass : Allow-Guest-Internet](#)

[Configuration de la stratégie de réauthentification ClearPass](#)

[Configuration du profil de redirection du portail invité ClearPass](#)

[Configuration du profil d'application des métadonnées ClearPass](#)

[Configuration de la stratégie d'application ClearPass Guest Internet Access](#)

[Configuration de la stratégie d'application ClearPass Guest Post-AUP](#)

[Configuration du service d'authentification MAB ClearPass](#)

[Configuration du service ClearPass Webauth](#)

[ClearPass - Connexion Web](#)

[Vérification - Autorisation CWA invité](#)

[Annexe](#)

[Informations connexes](#)

---

# Introduction

Ce document décrit l'intégration du contrôleur LAN sans fil (WLC) Catalyst 9800 avec Aruba ClearPass pour fournir un SSID (Guest Wireless Service Set Identifier).

## Conditions préalables

Ce guide suppose que ces composants ont été configurés et vérifiés :

- Tous les composants pertinents sont synchronisés sur le protocole NTP (Network Time Protocol) et vérifiés pour avoir l'heure correcte (requis pour la validation du certificat)
- Serveur DNS opérationnel (requis pour les flux de trafic invité, la validation de la liste de révocation de certificats)
- Serveur DHCP opérationnel
- Une autorité de certification (CA) facultative (requis pour signer le portail invité hébergé par CPPM)
- WLC Catalyst 9800
- Serveur Aruba ClearPass (nécessite une licence de plate-forme, une licence d'accès, une licence embarquée)
- VMware ESXi

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiement du C9800 et nouveau modèle de configuration
- Commutation Flexconnect sur C9800
- Authentification CWA 9800 (reportez-vous à la page <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst C9800-L-C qui exécute 17.3.4c
- Cisco Catalyst C9130AX
- Aruba ClearPass, correctif 6-8-0-109592 et 6.8-3
- Serveur MS Windows
  - Active Directory (GP configuré pour l'émission automatisée de certificats basés sur des ordinateurs vers des points de terminaison gérés)
  - Serveur DHCP avec option 43 et option 60
  - Serveur DNS
  - Serveur NTP pour synchroniser tous les composants
  - L'AC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

L'intégration de la mise en oeuvre du WLC du Catalyst 9800 utilise l'authentification Web centrale (CWA) pour les clients sans fil dans un déploiement de point d'accès (AP) en mode Flexconnect.

L'authentification sans fil des invités est prise en charge par Guest Portal avec une page de stratégie utilisateur acceptable (AUP) anonyme, hébergée sur Aruba Clearpass dans un segment de zone démilitarisée sécurisée (DMZ).

Le schéma présente les détails des échanges d'accès Wi-Fi invité avant que l'utilisateur invité ne soit autorisé à accéder au réseau :

1. L'utilisateur invité s'associe au Wi-Fi invité dans un bureau distant.
2. La demande d'accès RADIUS initiale est envoyée par proxy par C9800 au serveur RADIUS.
3. Le serveur recherche l'adresse MAC d'invité fournie dans la base de données MAC locale des points de terminaison.  
Si l'adresse MAC est introuvable, le serveur répond avec un profil MAC Authentication Bypass (MAB). Cette réponse RADIUS inclut :
  - Liste de contrôle d'accès de redirection d'URL
  - Redirection d'URL
4. Le client passe par le processus d'apprentissage IP où une adresse IP lui est attribuée.
5. C9800 fait passer le client invité (identifié par son adresse MAC) à l'état « Web Auth Pending ».
6. La plupart des systèmes d'exploitation de périphériques modernes associés aux WLAN invités effectuent une sorte de détection de portail captif.  
Le mécanisme de détection exact dépend de l'implémentation spécifique du système d'exploitation. Le système d'exploitation client ouvre une boîte de dialogue contextuelle (pseudo-navigateur) avec une page redirigée par C9800 vers l'URL du portail invité hébergée par le serveur RADIUS fournie dans le cadre de la réponse d'acceptation d'accès RADIUS.
7. L'utilisateur invité accepte les conditions générales de la fenêtre contextuelle ClearPass présentée. Il définit un indicateur pour l'adresse MAC du client dans sa base de données de terminaux (DB) afin d'indiquer que le client a terminé une authentification et initie une modification d'autorisation RADIUS (CoA), en sélectionnant une interface basée sur la table de routage (si plusieurs interfaces sont présentes sur ClearPass).
8. Le WLC fait passer le client invité à l'état « Exécuter » et l'utilisateur se voit accorder l'accès à Internet sans autre redirection.

 Remarque : pour le diagramme de flux d'état du contrôleur sans fil d'ancrage étranger Cisco 9800 avec RADIUS et le portail invité hébergé en externe, reportez-vous à la section Annexe de cet article.

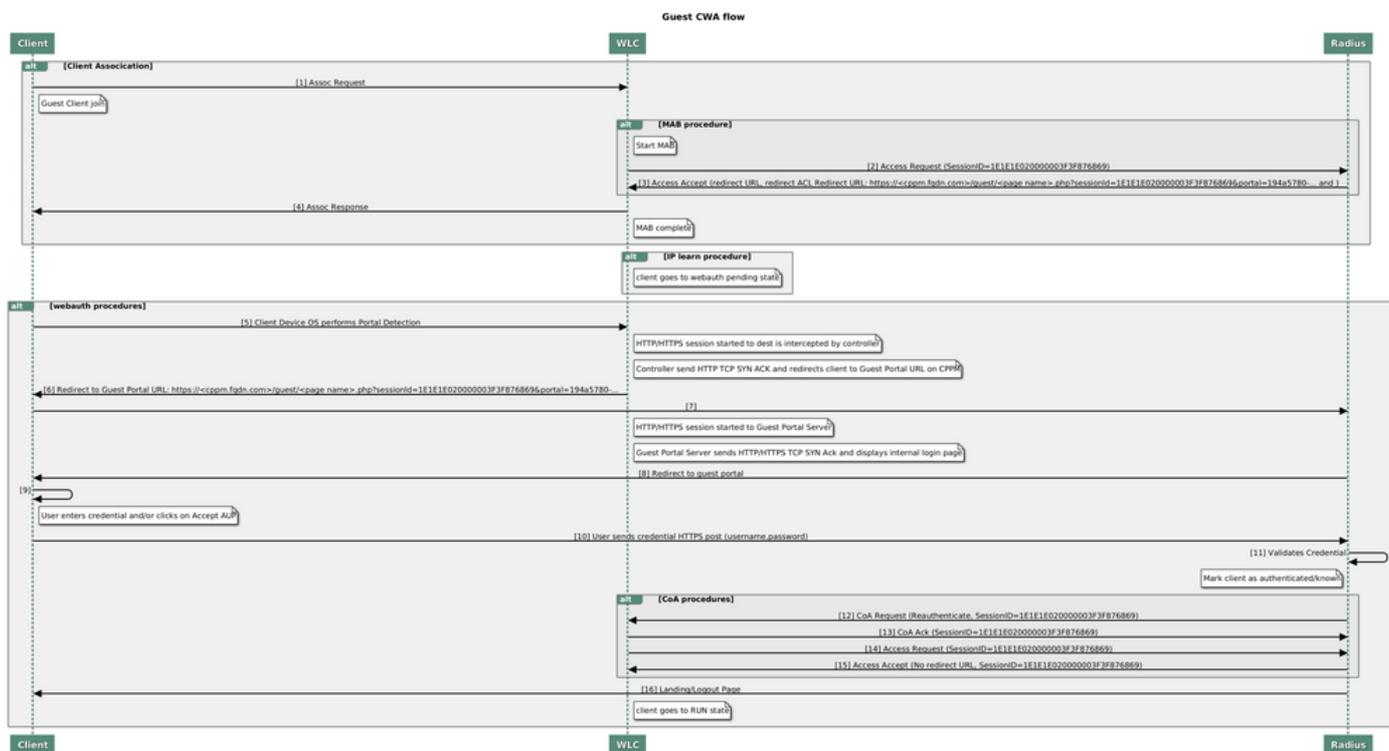


Diagramme d'état d'authentification Web de Guest Central (CWA)

## Flux de trafic pour le déploiement CWA Guest Enterprise

Dans un déploiement d'entreprise type avec plusieurs filiales, chaque filiale est configurée pour fournir un accès sécurisé et segmenté aux invités via un portail invité une fois que le client accepte le CLUF.

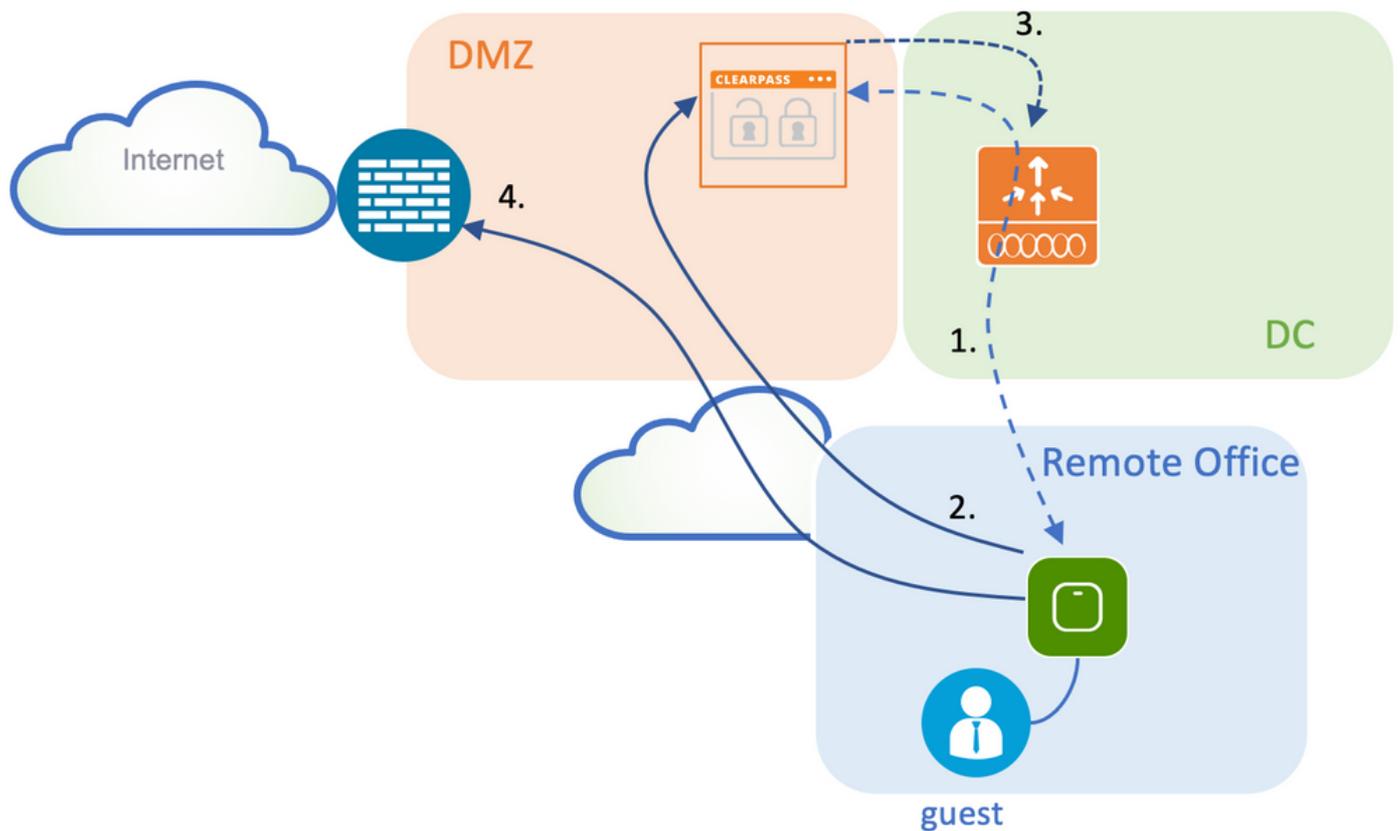
Dans cet exemple de configuration, 9800 CWA est utilisé pour l'accès invité via l'intégration à une instance ClearPass distincte déployée exclusivement pour les utilisateurs invités dans la DMZ sécurisée du réseau.

Les invités doivent accepter les conditions générales définies dans le portail contextuel de consentement Web fourni par le serveur ClearPass DMZ. Cet exemple de configuration se concentre sur la méthode d'accès invité anonyme (c'est-à-dire qu'aucun nom d'utilisateur/mot de passe invité n'est requis pour s'authentifier sur le portail invité).

Le flux de trafic correspondant à ce déploiement est illustré dans l'image :

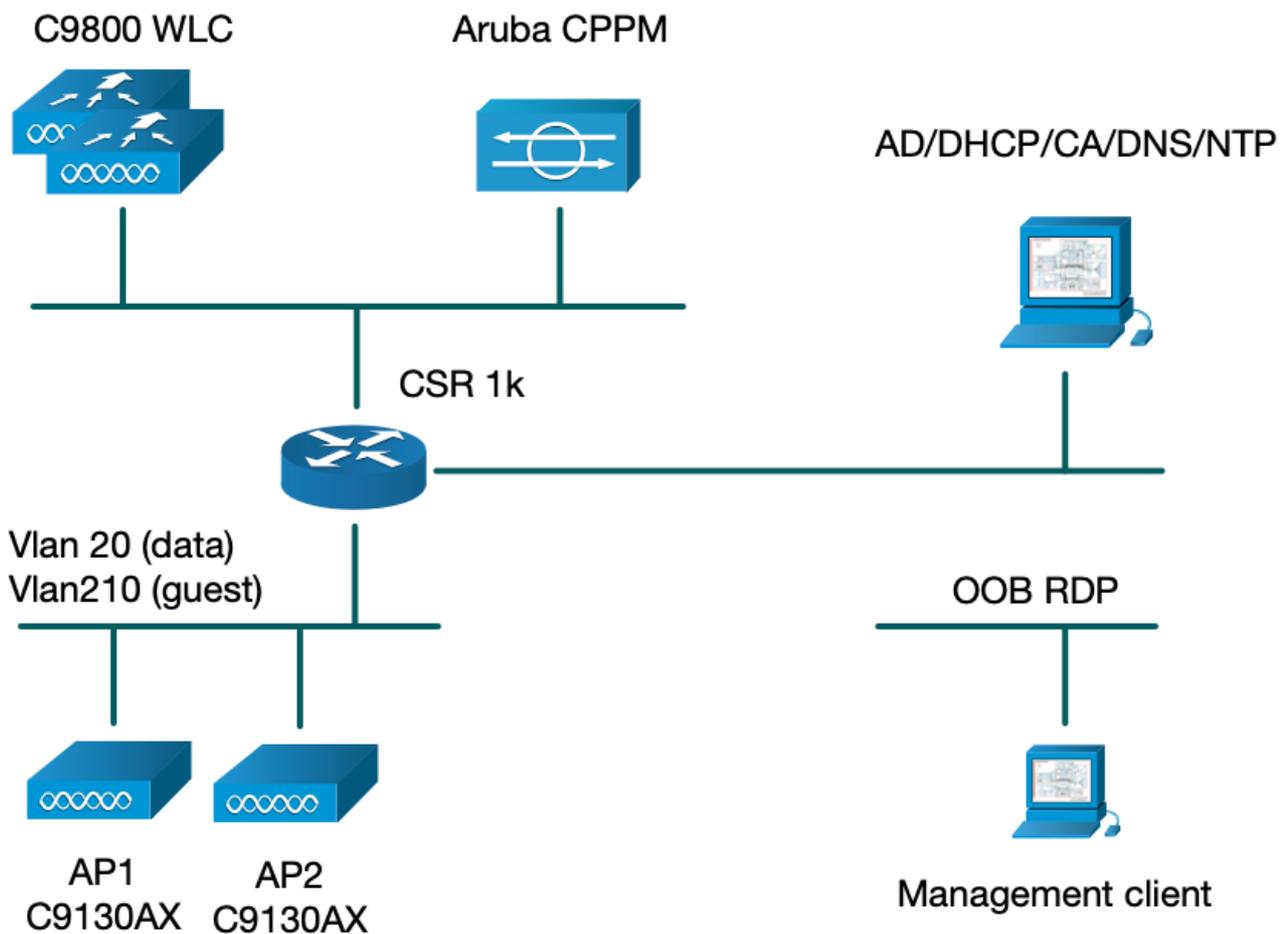
1. RADIUS - phase MAB
2. Redirection de l'URL du client invité vers le portail invité
3. Après l'acceptation du CLUF par l'invité sur le portail invité, la réauthentification RADIUS CoA est délivrée de CPPM à 9800 WLC

#### 4. L'invité est autorisé à accéder à Internet



#### Diagramme du réseau

 Remarque : pour les démonstrations de travaux pratiques, une seule instance de serveur Aruba CPPM est utilisée afin de servir les fonctions de serveur d'accès réseau (NAS) SSID invité et entreprise. La mise en oeuvre des meilleures pratiques suggère des instances NAS indépendantes.



## Configurer

Dans cet exemple de configuration, un nouveau modèle de configuration sur C9800 est utilisé afin de créer les profils et balises nécessaires pour fournir dot1x Corporate Access et CWA guest Access à la filiale de l'entreprise. La configuration résultante est résumée dans cette image :

AP  
MAC: XXXX.XXXX.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

## Configuration des paramètres de l'accès sans fil invité C9800

### C9800 - Configuration AAA pour invité

 Remarque : à propos de l'ID de bogue Cisco [CSCvh03827](https://cisco.com/cisco/webbugtool/bugdetails?bug=CSCvh03827), assurez-vous que les serveurs AAA (Authentication, Authorization, and Accounting) définis ne sont pas équilibrés en charge, car le mécanisme repose sur la persistance de l'ID de session dans les échanges WLC à ClearPass RADIUS.

Étape 1. Ajoutez le ou les serveurs DMZ Aruba ClearPass à la configuration du WLC 9800 et créez une liste de méthodes d'authentification. Naviguez jusqu'à Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add et saisissez les informations relatives au serveur 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

Étape 2. Définissez un groupe de serveurs AAA pour les invités et affectez le serveur configuré à l'étape 1 à ce groupe de serveurs. Accédez à Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add.

## Create AAA Radius Server Group



Name\*

AAA\_Radius\_CPPM|

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Source Interface VLAN ID

1

Available Servers

Assigned Servers



CPPM



Cancel



Apply to Device

Étape 3. Définissez une liste de méthodes d'autorisation pour l'accès invité et mappez le groupe de serveurs créé à l'étape 2. Accédez à Configuration > Security > AAA > AAA Method List > Authorization > +Add. Sélectionnez Type Network, puis AAA Server Group configurez à l'étape 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

Étape 4. Créez une liste de méthodes de comptabilisation pour l'accès invité et mappez le groupe de serveurs créé à l'étape 2. Accédez à Configuration > Security > AAA > AAA Method List > Accounting > +Add. Choisissez Type Identity dans le menu déroulant, puis configurez AAA Server Group à l'étape 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 - Configurer la liste de contrôle d'accès Redirection

La liste de contrôle d'accès de redirection définit le trafic qui doit être redirigé vers le portail invité par rapport au trafic autorisé sans redirection. Ici, le refus de la liste de contrôle d'accès implique

le contournement de la redirection ou du passage, tandis que le permis implique la redirection vers le portail. Pour chaque classe de trafic, vous devez tenir compte de la direction du trafic lorsque vous créez des entrées de contrôle d'accès (ACE) et des entrées de contrôle d'accès qui correspondent au trafic entrant et sortant.

Accédez à Configuration > Security > ACL et définissez une nouvelle liste de contrôle d'accès nommée CAPTIVE\_PORTAL\_REDIRECT. Configurez la liste de contrôle d'accès avec ces ACE :

- ACE1 : permet au trafic ICMP (Internet Control Message Protocol) bidirectionnel de contourner la redirection et est principalement utilisé pour vérifier l'accessibilité.
- ACE10, ACE30 : autorise le flux de trafic DNS bidirectionnel vers le serveur DNS 10.0.10.4 et ne peut pas être redirigé vers le portail. Une recherche et une interception DNS pour la réponse sont nécessaires pour déclencher le flux invité.
- ACE70, ACE80, ACE110, ACE120 : autorise l'accès HTTP et HTTPS au portail captif invité pour que l'utilisateur puisse accéder au portail.
- ACE150 : tout le trafic HTTP (port UDP 80) est redirigé.

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 - Configuration du profil WLAN invité

Étape 1. Accédez à Configuration > Tags & Profiles > Wireless > +Add. Créez un nouveau profil SSID WP\_Guest, avec la diffusion du SSID « Guest » auquel les clients invités s'associent.

## 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		

Dans la même boîte de dialogue Add WLAN, accédez à l'onglet Security > Layer 2.

- Mode de sécurité de couche 2 : Aucun

- Filtrage MAC : activé

- Liste d'autorisations : AAA\_Authz\_CPPM dans le menu déroulant (configuré à l'étape 3. dans le cadre de la configuration 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"/>		

## C9800 - Définition du profil de politique d'invité

Sur l'interface graphique utilisateur du WLC C9800, accédez à Configuration > Tags & Profiles > Policy > +Add.

Nom : PP\_Guest

État : Activé

Commutation centrale : désactivée

Authentification centrale : activée

DHCP central : désactivé

Association centrale : Désactivé

### 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"/>	<b>WLAN Switching Policy</b>	
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
<b>CTS Policy</b>		Flex NAT/PAT	<input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

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	<b>WLAN Switching Policy</b>
Description	Profile for Branch Guest	Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> DISABLED	Central Authentication <b>ENABLED</b> <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
<b>CTS Policy</b>		Flex NAT/PAT <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

↶ Cancel
📄 Apply to Device

Accédez à l'onglet **Access Policies** dans la même **Add Policy Profile** boîte de dialogue.

- Profilage RADIUS : activé

- VLAN/groupe de VLAN : 210 (c'est-à-dire que le VLAN 210 est le VLAN local invité sur chaque emplacement de filiale)

Remarque : le VLAN invité pour Flex ne doit pas être défini sur le WLC 9800 sous VLAN, dans le numéro VLAN de type VLAN/VLAN Group.

Défaut connu : le bogue Cisco ayant l'ID [CSCvn48234](#) empêche la diffusion du SSID si le même VLAN invité Flex est défini sous WLC et dans le profil 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

Dans la même Add Policy Profile boîte de dialogue, accédez à l'Advanced onglet.

- Autoriser le remplacement AAA : activé
- État NAC : activé
- Type NAC : RADIUS
- Liste de comptabilisation : AAA\_Accounting\_CPPM (définie à l'étape 4. dans le cadre de la configuration 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

✎ Remarque : l'état NAC (Network Admission Control) - Enable est requis pour permettre au WLC C9800 d'accepter les messages RADIUS CoA.

## C9800 - Balise de stratégie

Sur l'interface graphique du C9800, accédez à Configuration > Tags & Profiles > Tags > Policy > +Add.

- Nom : PT\_CAN01

- Description : Étiquette de politique pour le site de la succursale CAN01

Dans la même boîte de dialogue, Add Policy Tag sous WLAN-POLICY MAPS, cliquez sur +Add, et mappez le

profil WLAN précédemment créé au profil de stratégie :

- Profil WLAN : WP\_Guest

- Profil de stratégie : PP\_Guest

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page <span>No items to display</span>	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

---

➤ RLAN-POLICY Maps: 0

## C9800 - Profil de jonction AP

Sur l'interface graphique utilisateur du WLC C9800, accédez à Configuration > Tags & Profiles > AP Join > +Add.

- Nom : Branch\_AP\_Profile

- Serveur NTP : 10.0.10.4 (reportez-vous au schéma de topologie des travaux pratiques). Il s'agit du serveur NTP utilisé par les points d'accès de Branch pour la synchronisation.

## Add AP Join Profile

General	Client	CAPWAP	AP	Management	Security	ICap	QoS
Name*	Branch_AP_Profile			<b>OfficeExtend AP Configuration</b>			
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"/>						

### C9800 - Profil flexible

Les profils et les étiquettes sont modulaires et peuvent être réutilisés pour plusieurs sites.

Dans le cas d'un déploiement FlexConnect, si les mêmes ID de VLAN sont utilisés sur tous les sites des filiales, vous pouvez réutiliser le même profil Flex.

Étape 1. Sur une interface graphique utilisateur WLC C9800, accédez à Configuration > Tags & Profiles > Flex > +Add.

- Nom : FP\_Branch

- ID de VLAN natif : 10 (requis uniquement si vous avez un VLAN natif non par défaut où vous voulez avoir une interface de gestion 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

Dans la même Add Flex Profile boîte de dialogue, accédez à l'onglet Policy ACL et cliquez sur +Add.

- Nom ACL : CAPTIVE\_PORTAL\_REDIRECT
- Authentification Web centrale : activée

Sur un déploiement Flexconnect, chaque point d'accès géré est censé télécharger la liste de contrôle d'accès de redirection localement, car la redirection se produit au niveau du point d'accès et non sur le 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

Dans la même Add Flex Profile boîte de dialogue, accédez à l'onglet VLAN et cliquez sur +Add (reportez-vous au schéma de topologie des travaux pratiques).

- Nom du VLAN : guest
- 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 - Étiquette de site

Sur l'interface utilisateur graphique du WLC 9800, accédez à Configuration > Tags & Profiles > Tags > Site > Add.

 Remarque : créez une balise de site unique pour chaque site distant qui doit prendre en charge les deux SSID sans fil comme décrit.

Il existe un mappage 1-1 entre un emplacement géographique, une balise de site et une configuration de profil paramétrable.

Un site de connexion flexible doit être associé à un profil de connexion flexible. Vous pouvez disposer d'un maximum de 100 points d'accès pour chaque site Flex Connect.

- Nom : ST\_CAN01
- Profil de jointure AP : Branch\_AP\_Profile
- Profil flexible : FP\_Branch
- Activer le site local : Désactivé

**Add Site Tag** ✕

Name\*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

## C9800 - Profil RF

Sur l'interface utilisateur graphique du WLC 9800, accédez à Configuration > Tags & Profiles > Tags > RF > Add.

- Nom : Branch\_RF

- Profil de fréquence radio (RF) de la bande 5 GHz : Typical\_Client\_Density\_5gh (option définie par le système)

- Profil RF de la bande 2,4 GHz : Typical\_Client\_Density\_2gh (option définie par le système)

### 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 - Attribuer des balises au point d'accès

Deux options sont disponibles afin d'attribuer des balises définies à des points d'accès individuels dans le déploiement :

- Affectation basée sur le nom de l'AP, qui exploite les règles d'expression régulière qui correspondent aux modèles dans le champ Nom de l'AP (Configure > Tags & Profiles > Tags > AP > Filter)

- Affectation basée sur l'adresse MAC Ethernet (Configure > Tags & Profiles > Tags > AP > StaticAP)

Lors d'un déploiement en production avec Cisco DNA Center, il est fortement recommandé d'utiliser DNAC et AP PNP Workflow ou d'utiliser une méthode de chargement CSV (Comma-Separated Values) statique disponible dans le 9800 afin d'éviter l'attribution manuelle par AP. Accédez à Configure > Tags & Profiles > Tags > AP > Static > Add (notez l'Upload File option).

- Adresse MAC AP : <AP\_ETHERNET\_MAC>

- Nom de la balise de stratégie : PT\_CAN01

- Nom de la balise de site : ST\_CAN01

- Nom de la balise RF : Branch\_RF

 Remarque : à partir de la version 17.3.4c de la plate-forme logicielle Cisco IOS® XE, il existe un maximum de 1 000 règles regex par limite de contrôleur. Si le nombre de sites dans le déploiement dépasse ce nombre, l'affectation statique par MAC doit être exploitée.

### 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

 Remarque : vous pouvez également utiliser la méthode d'affectation de balise basée sur l'expression régulière AP-name en naviguant jusqu'à [Configure > Tags & Profiles > Tags > AP > Filter > Add.](#)

- Nom : BR\_CAN01

- Régex de nom d'AP : BR-CAN01-(7) (Cette règle correspond à la convention de nom d'AP adoptée dans l'organisation. Dans cet exemple, les balises sont attribuées aux points d'accès qui ont un champ de nom de point d'accès qui contient 'BR\_CAN01-' suivi de sept caractères.)

- Priorité : 1

- Nom de la balise de stratégie : PT\_CAN01 (tel que défini)

- Nom de la balise de site : ST\_CAN01

- Nom de la balise 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				

↶ Cancel 📄 Apply to Device

## Configurer l'instance Aruba CPPM

Pour connaître les meilleures pratiques de production basées sur la configuration Aruba CPPM, contactez votre ressource HPE Aruba SE locale.

### Configuration initiale du serveur Aruba ClearPass

Aruba ClearPass est déployé avec l'utilisation du modèle Open Virtualization Format (OVF) sur le serveur ESXi <> qui alloue ces ressources :

- Deux processeurs virtuels réservés
- 6 Go de RAM
- Disque de 80 Go (doit être ajouté manuellement après le déploiement initial de la machine virtuelle avant la mise sous tension de la machine)

### Demander des licences

Demandez une licence de plate-forme via Administration > Server Manager > Licensing. Ajoutez PlatformAccess, et Onboard licenses.

### Server Hostname

Accédez au serveur CPPM nouvellement provisionné Administration > Server Manager > Server Configuration et sélectionnez-le.

- Nom d'hôte : cppm
- FQDN : cppm.example.com
- Vérifier l'adressage IP et DNS du port de gestion

## 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
<b>Management Port</b>	IP Address	10.85.54.98			<a href="#">Configure</a>
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
<b>Data/External Port</b>	IP Address				<a href="#">Configure</a>
	Subnet Mask				
	Default Gateway				
<b>DNS Settings</b>	Primary	10.85.54.122			<a href="#">Configure</a>
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

## Générer un certificat de serveur Web CPPM (HTTPS)

Ce certificat est utilisé lorsque la page ClearPass Guest Portal est présentée via HTTPS aux clients invités qui se connectent au Wi-Fi invité dans la filiale.

Étape 1. Téléchargez le certificat CA pub chain.

Accédez à Administration > Certificates > Trust List > Add.

- Utilisation : Activer les autres

### 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**

Étape 2. Créer une demande de signature de certificat.

Accédez à Administration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS Server Certificate.

- Cliquez sur le bouton Create Certificate Signing Request

- Nom commun : CPPM

- Organisation : cppm.example.com

Veillez à renseigner le champ SAN (un nom commun doit être présent dans SAN, ainsi que dans IP et d'autres noms de domaine complets, le cas échéant). Le format est 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

Étape 3. Dans l'autorité de certification de votre choix, signez le CSR du service HTTPS CPPM nouvellement généré.

Étape 4. Accédez à [Certificate Template > Web Server > Import Certificate](#).

- Type de certificat : certificat de serveur
- Utilisation : certificat de serveur HTTP
- Fichier de certificat : parcourez et sélectionnez le certificat de service HTTPS CPPM signé par l'autorité de certification

### 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.

## Définir le WLC C9800 comme périphérique réseau

Accédez à Configuration > Network > Devices > Add.

- Nom : WLC\_9800\_Branch
- Adresse IP ou de sous-réseau : 10.85.54.99 (reportez-vous au schéma de topologie des travaux pratiques)
- RADIUS Shared Cisco : <mot de passe RADIUS WLC>
- Nom du fournisseur : Cisco
- Activer l'autorisation dynamique 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**

## Page Guest Portal et minuteurs CoA

Il est très important de définir les valeurs de minuteur correctes tout au long de la configuration. Si les minuteurs ne sont pas réglés, vous risquez de vous retrouver dans une redirection de portail Web en cours de cycle avec le client, et non dans l'état d'exécution.

Minuteurs à prendre en compte :

- Portal Web Login timer : ce minuteur retarde votre page de redirection avant d'autoriser l'accès à la page du portail invité pour notifier le service CPPM de la transition d'état, enregistrer la valeur de l'attribut personnalisé « Allow-Guest-Internet » du terminal et déclencher le processus CoA de CPPM vers WLC. Accédez à Guest > Configuration > Pages > Web Logins.
  - Choisissez le nom du portail invité : Lab Anonymous Guest Registration (cette configuration de page du portail invité est détaillée comme indiqué)
  - Cliquez sur Edit
  - Délai de connexion : 6 secondes

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

- ClearPass CoA delay timer : Ceci retarde l'émission des messages CoA de ClearPass à WLC. Cela est nécessaire pour que CPPM puisse effectuer la transition de l'état du terminal client en interne avant que l'accusé de réception CoA (ACK) ne revienne du WLC. Les tests en laboratoire montrent les temps de réponse de moins d'une milliseconde à partir du WLC, et si CPPM n'a pas terminé la mise à jour des attributs de point de terminaison, la nouvelle session RADIUS à partir du WLC est mise en correspondance avec la stratégie d'application de service MAB non authentifié, et le client reçoit à nouveau une page de redirection.

Accédez à CPPM > Administration > Server Manager > Server Configuration et sélectionnez CPPM Server > Service Parameters.

- Délai d'autorisation dynamique (DM/CoA) RADIUS - défini sur six secondes

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Administration » Server Manager » Server Configuration - cppm' and 'Server Configuration - cppm (10.85.54.98)'. The 'Service Parameters' tab is active, showing a list of parameters for 'Async network services'. The 'Command Control' section is highlighted, and the 'RADIUS Dynamic Authorization (DM/CoA) Delay' parameter is set to 6 seconds.

Parameter Name	Parameter Value
<b>Ingress Event</b>	
Batch Processing Interval	30 seconds
<b>Command Control</b>	
<b>RADIUS Dynamic Authorization (DM/CoA) Delay</b>	6 seconds
Enable SNMP Bounce Action	FALSE
<b>Post Auth</b>	
Number of request processing threads	20 threads
Lazy handler polling frequency	5 minutes
Eager handler polling frequency	30 seconds
Connection Timeout	10 seconds
Palo Alto User Identification Timeout	45 minutes

## ClearPass - Configuration CWA invité

La configuration CWA côté ClearPass se compose de (3) points/étapes de service :

Composant ClearPass	Type de service	Objectif
1. Gestionnaire des politiques	Service : authentification Mac	Si l'attribut personnalisé Allow-Guest-Internet= TRUE, autorisez-le sur le réseau. Sinon, déclenchez Redirect et Reauthenticate.
2. Invité	Connexions Web	Présenter la page AUP de connexion anonyme. Post-auth définit un attribut personnalisé Allow-Guest-Internet=

		TRUE.
3. Gestionnaire des politiques	Service : authentification basée sur le Web	Mettre à jour le terminal <small>Known</small> Définir l'attribut personnalisé <code>Allow-Guest-Internet=VRAI</code> COA: Reauthenticate

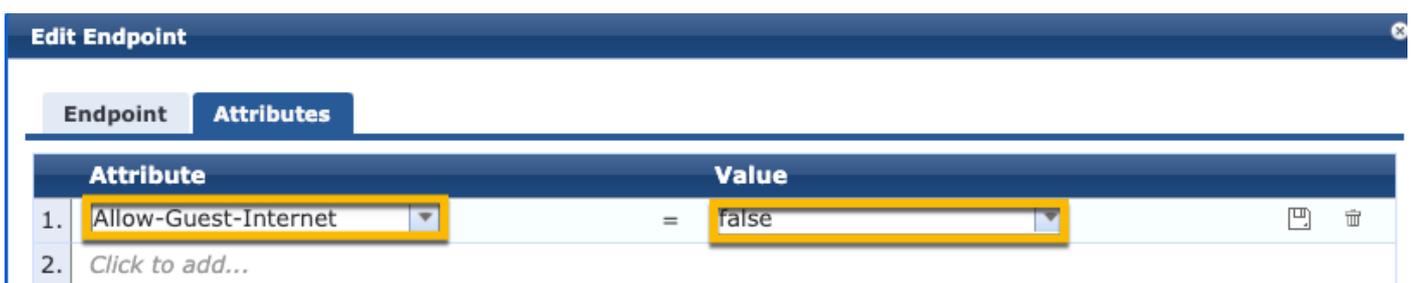
Attribut de métadonnées du point de terminaison ClearPass : Allow-Guest-Internet

Créez un attribut de métadonnées de type Boolean afin de suivre l'état du point de terminaison invité lorsque le client passe de l'état 'Webauth Pending' à l'état 'Run' :

- Les nouveaux invités qui se connectent au Wi-Fi ont un attribut de métadonnées par défaut défini afin de `Allow-Guest-Internet=false`. Sur la base de cet attribut, l'authentification du client passe par le service MAB
- Client invité lorsque vous cliquez sur le bouton d'acceptation AUP, a son attribut de métadonnées mis à jour afin de `Allow-Guest-Internet=true`. Le MAB suivant basé sur cet attribut défini sur True permet un accès non redirigé à Internet

Naviguez jusqu'à `ClearPass > Configuration > Endpoints`, choisissez un point de terminaison dans la liste, cliquez sur l'Attributes onglet, ajoutez `Allow-Guest-Internet` avec la valeur `false` et Save.

 Remarque : vous pouvez également modifier le même point de terminaison et supprimer cet attribut juste après. Cette étape crée simplement un champ dans la base de données de métadonnées Endpoints qui peut être utilisé dans les stratégies.



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

Configuration de la stratégie de réauthentification ClearPass

Créez un profil d'application affecté au client invité immédiatement après que le client a accepté le protocole AUP sur la page Guest Portal.

Accédez à `ClearPass > Configuration > Profiles > Add`.

- Modèle : RADIUS Dynamic Authorization
- Nom : 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"/> <input type="text"/> --Select--	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>

Rayon:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station-Id}
Rayon:Cisco	Cisco-AVPair	abonné:commande=réauthentifier
Rayon:Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-session-id}
Rayon:Cisco	Cisco-AVPair	abonné:reauthenticate-type=last-type=last

### Configuration du profil de redirection du portail invité ClearPass

Créez un profil d'application appliqué à l'invité au cours de la phase MAB initiale, lorsque l'adresse MAC est introuvable dans la base de données de point de terminaison CPPM avec « Allow-Guest-Internet » défini sur « true ».

Le WLC 9800 redirige alors le client invité vers le portail invité CPPM pour l'authentification externe.

Accédez à [ClearPass > Enforcement > Profiles > Add.](#)

- Nom : Cisco\_Portal\_Redirect

- Type : RADIUS

- Action : accepter

Configuration » Enforcement » Profiles » Add Enforcement Profile

## Enforcement Profiles

**Profile** | Attributes | Summary

Template: Aruba RADIUS Enforcement

Name: Cisco\_Portal\_Redirect

Description:

Type: RADIUS

Action:  Accept  Reject  Drop

Device Group List:

Remove  
View Details  
Modify

--Select--

ClearPass Redirect Enforcement Profile

Dans la même boîte de dialogue, sous l'onglet, **Attributes** configurez deux Attributs selon cette image :

Enforcement Profiles - Cisco\_Portal\_Redirect

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

Attributs de profil de redirection ClearPass

L'attribut `url-redirect-acl` défini sur `CAPTIVE-PORTAL-REDIRECT`, qui est le nom de la liste de contrôle d'accès créée sur C9800.

 Remarque : seule la référence à la liste de contrôle d'accès est transmise dans le message RADIUS, et non le contenu de la liste. Il est important que le nom de la liste de contrôle d'accès créée sur le WLC 9800 corresponde exactement à la valeur de cet attribut RADIUS comme indiqué.

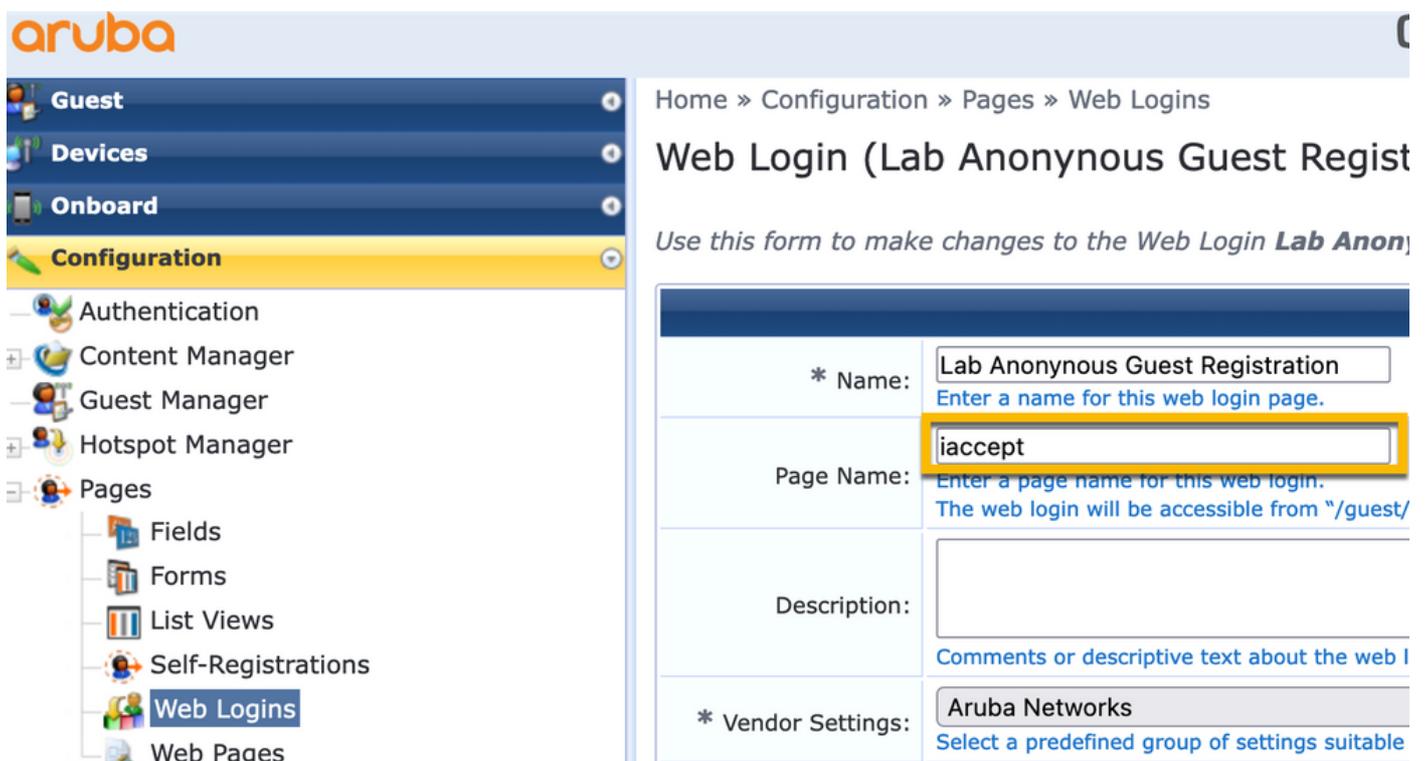
L'attribut `url-redirect` est composé de plusieurs paramètres :

- URL cible où le portail invité est hébergé : <https://cppm.example.com/guest/iaccept.php>
- Adresse MAC du client invité, macro %{Connection:Client-Mac-Address-Hyphen}
- Authenticator IP (9800 WLC déclenche la redirection), macro %{Radius:IETF:NAS-IP-Address}
- action cmd-login

L'URL de la page ClearPass Guest Web Login s'affiche lorsque vous accédez à CPPM > Guest > Configuration > Pages > Web Logins > Edit.

Dans cet exemple, le nom de la page Guest Portal dans CPPM est défini comme `iaccept`.

 Remarque : les étapes de configuration de la page Guest Portal sont décrites ci-dessous.



The screenshot shows the Aruba CPPM configuration interface. On the left is a navigation menu with categories: Guest, Devices, Onboard, Configuration (highlighted), Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages (expanded to show Fields, Forms, List Views, Self-Registrations, Web Logins, and Web Pages), and Web Pages. The main content area shows the configuration for a 'Web Login (Lab Anonymous Guest Registration)'. The breadcrumb trail is 'Home » Configuration » Pages » Web Logins'. The page title is 'Web Login (Lab Anonymous Guest Registration)'. Below the title is the instruction: 'Use this form to make changes to the Web Login Lab Anonym...'. The form contains the following fields:

- \* Name:** Lab Anonymous Guest Registration (with a sub-note: 'Enter a name for this web login page.')
- Page Name:** iaccept (highlighted with a yellow box, with a sub-note: 'Enter a page name for this web login. The web login will be accessible from "/>

 Remarque : pour les périphériques Cisco, est normalement `audit_session_id` utilisé, mais ce n'est pas pris en charge par d'autres fournisseurs.

## Configuration du profil d'application des métadonnées ClearPass

Configurez le profil d'application afin de mettre à jour l'attribut de métadonnées Endpoint qui est utilisé pour le suivi de la transition d'état par CPPM.

Ce profil est appliqué à l'entrée d'adresse MAC du client invité dans la base de données de point de terminaison et définit l'`Allow-Guest-Internet` argument sur 'true'.

Accédez à ClearPass > Enforcement > Profiles > Add.

- Modèle : Mise à jour des entités ClearPass

- Type : 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="border: 1px solid #ccc; height: 40px;"></div>	<div style="text-align: right;"><button>Remove</button> <button>View Details</button> <button>Modify</button></div>

Dans la même boîte de dialogue, cliquez sur **Attributes** l'onglet.

- Type : terminal

- Nom : Allow-Guest-Internet

 Remarque : pour que ce nom apparaisse dans le menu déroulant, vous devez définir manuellement ce champ pour au moins un point de terminaison, comme décrit dans les étapes.

- Valeur : true

Configuration » Enforcement » Profiles » Add Enforcement Profile

## Enforcement Profiles

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

Configuration de la stratégie d'application ClearPass Guest Internet Access

Accédez à ClearPass > Enforcement > Policies > Add.

- Nom : WLC Cisco Guest Allow
- Type d'application : RADIUS
- Profil par défaut : Cisco\_Portal\_Redirect

Configuration » Enforcement » Politiques » Add

## 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**

Dans la même boîte de dialogue, accédez à l'onglet **Rules** et cliquez sur **Add Rule**.

- Type : terminal
- Nom : Allow-Guest-Internet
- Opérateur : EQUALS
- Valeur Vrai
- Noms de profil / Choisir d'ajouter : [RADIUS] [Autoriser le profil d'accès]

**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**

## Configuration de la stratégie d'application ClearPass Guest Post-AUP

Accédez à ClearPass > Enforcement > Politiques > Add.

- Nom : Politique d'application Webauth de Cisco WLC

- Type d'application : WEBAUTH (SNMP/Agent/CLI/CoA)
- Profil par défaut : [RADIUS\_CoA] Cisco\_Reauthenticate\_Session

Configuration » Enforcement » Policies » Add

## Enforcement Policies

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

Dans la même boîte de dialogue, accédez à Rules > Add.

- Conditions : authentification
- Nom : État
- Opérateur : EQUALS
- Valeur : Utilisateur
- Noms des profils : <ajouter chaque profil> :
- [Post-authentification] [Point de terminaison de mise à jour connu]
- [Post-authentification] [Make-Cisco-Guest-Valid]
- [RADIUS\_CoA] [Cisco\_WLC\_Guest\_COA]

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
	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>
	--Select to Add--

 Remarque : si vous vous trouvez dans un scénario avec une fenêtre contextuelle de pseudo-navigateur de redirection Guest Portal continue, cela indique que les minuteurs CPPM nécessitent des ajustements ou que les messages RADIUS CoA ne sont pas échangés correctement entre CPPM et le WLC 9800. Vérifiez ces sites.

- Accédez à CPPM > Monitoring > Live Monitoring > Access Tracker et assurez-vous que l'entrée du journal RADIUS contient les détails de la société RADIUS.

- Sous 9800 WLC, accédez à Troubleshooting > Packet Capture, activez PCAP sur l'interface où l'arrivée des paquets RADIUS CoA est attendue, et vérifiez que les messages RADIUS CoA sont reçus du CPPM.

## Configuration du service d'authentification MAB ClearPass

Le service est associé à la paire de valeurs d'attribut (AV) Radius : Cisco | CiscoAVPair | cisco-wlan-ssid

Accédez à ClearPass > Configuration > Services > Add.

Onglet Service :

- Nom : GuestPortal - Mac Auth

- Type : authentification MAC

- Plus d'options : sélectionnez Autorisation, Points de terminaison de profil

Ajouter une règle de correspondance :

- Type : Rayon : Cisco

- Nom : Cisco-AVPair

- Opérateur : EQUALS

- Valeur : cisco-wlan-ssid=Invité (correspond à votre nom SSID d'invité configuré)



Remarque : « Guest » est le nom du SSID invité diffusé par le 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		

Dans la même boîte de dialogue, sélectionnez l'Authentication onglet.

- Méthodes d'authentification : Remove [MAC AUTH], Add [Allow All MAC AUTH]
- Sources d'authentification : [Référentiel des points de terminaison][Base de données SQL locale], [Référentiel utilisateur invité][Base de données SQL locale]

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

Dans la même boîte de dialogue, sélectionnez l'Enforcement onglet.

- Politique d'application : WLC Cisco Guest Allow

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]

Dans la même boîte de dialogue, sélectionnez l'Enforcement onglet.

## 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>					<a href="#">Remove</a>
	-- Select --					▼
RADIUS CoA Action:	Cisco_Reauthenticate_Session				▼	<a href="#">View Details</a> <a href="#">Modify</a>

### Configuration du service ClearPass Webauth

Accédez à ClearPass > Enforcement > Policies > Add.

- Nom : Guest\_Portal\_Webauth

- Type : authentification basée sur le 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>			

Dans la même boîte de dialogue, sous l'onglet Enforcement, la politique d'application : Politique d'application Webauth de Cisco WLC.

## 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	<a href="#">Modify</a>	<a href="#">Add New Enforcement Poli</a>
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 - Connexion Web

Pour la page Anonymous AUP Guest Portal, utilisez un seul nom d'utilisateur sans champ de mot de passe.

Les champs suivants doivent être définis/définis pour le nom d'utilisateur utilisé :

nom\_utilisateur\_auth | Authentification par nom d'utilisateur : | 1

Afin de définir le champ 'username\_auth' pour un utilisateur, ce champ doit d'abord être exposé dans le formulaire 'edit user'. Accédez à ClearPass > Guest > Configuration > Pages > Forms, puis sélectionnez create\_user Formulaire.

The screenshot shows the Aruba ClearPass Guest interface. On the left, a navigation sidebar has 'Forms' highlighted under the 'Configuration' section. The main area is titled 'Customize Forms' and contains a table of forms. The 'create\_user\*' form is selected, and its 'Edit Fields' button is highlighted with an orange box.

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
<b>create_user*</b> Create a single guest account.	<b>Create New Guest Account</b>
create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt
guest_edit	

Choisissez visitor\_name (ligne 20), puis cliquez sur 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	<b>visitor_name</b>	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: 1 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.

Maintenant, créez le nom d'utilisateur afin de l'utiliser derrière la page du portail d'invité AUP.

Accédez à **àCPPM > Guest > Guest > Manage Accounts > Create**.

- Nom d'invité : GuestWiFi

- Nom de la société : Cisco
- Adresse électronique : guest@example.com
- Authentification de nom d'utilisateur : autoriser l'accès invité avec l'utilisation de son nom d'utilisateur uniquement : activé
- Activation du compte : maintenant
- Expiration du compte : le compte n'expire pas
- Conditions d'utilisation : Je suis le sponsor : Activé

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>v</small> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input type="text" value="Account will not expire"/> <small>v</small> <small>Select an option for changing the expiration time of this account.</small>
* Account Role:	<input type="text" value="[Guest]"/> <small>v</small> <small>Role to assign to this account.</small>
Password:	<b>281355</b>
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the <a href="#">terms of use</a>
<input type="button" value="Create"/>	

Créer un formulaire de connexion Web. Accédez à CPPM > Guest > Configuration > Web Logins.

Nom : Lab Anonymous Guest Portal

Nom de la page : iaccept

Paramètres du fournisseur : Aruba Networks

Méthode de connexion : déclenchée par le serveur - Modification de l'autorisation (RFC 3576) envoyée au contrôleur

Authentification : anonyme - ne nécessite pas de nom d'utilisateur ou de mot de passe

Utilisateur anonyme : GuestWifi

Termes : vous devez confirmer les termes et conditions

Étiquette de connexion : accepter et se connecter

URL par défaut : [www.example.com](http://www.example.com)

Délai de connexion : 6

Update Endpoint : marque l'adresse MAC de l'utilisateur comme point d'extrémité connu

Avancé : personnalisez les attributs stockés avec le point de terminaison, les attributs de point de terminaison dans la section post-auth :

nom d'utilisateur | Nom d'utilisateur

nom\_visiteur | Nom du visiteur

cn | Nom du visiteur

téléphone\_visiteur | Téléphone du visiteur

email (courrier électronique) | Courriel

poste | Courriel

nom\_sponsor | Nom du sponsor

e-mail\_sponsor | E-mail du sponsor

Allow-Guest-Internet | vrai

## Vérification - Autorisation CWA invité

Dans le CPPM, accédez à [Live Monitoring > Access Tracker](#).

Le nouvel utilisateur invité se connecte et déclenche le service MAB.

Onglet Résumé :

**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

Dans la même boîte de dialogue, accédez à l'Inputonglet.

**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

Dans la même boîte de dialogue, accédez à l'Outputonglet.

## 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

## Annexe

À titre de référence, un diagramme de flux d'état est présenté ici pour les interactions entre le contrôleur d'ancrage, le contrôleur étranger Cisco 9800 et le serveur RADIUS et le portail invité hébergé en externe.

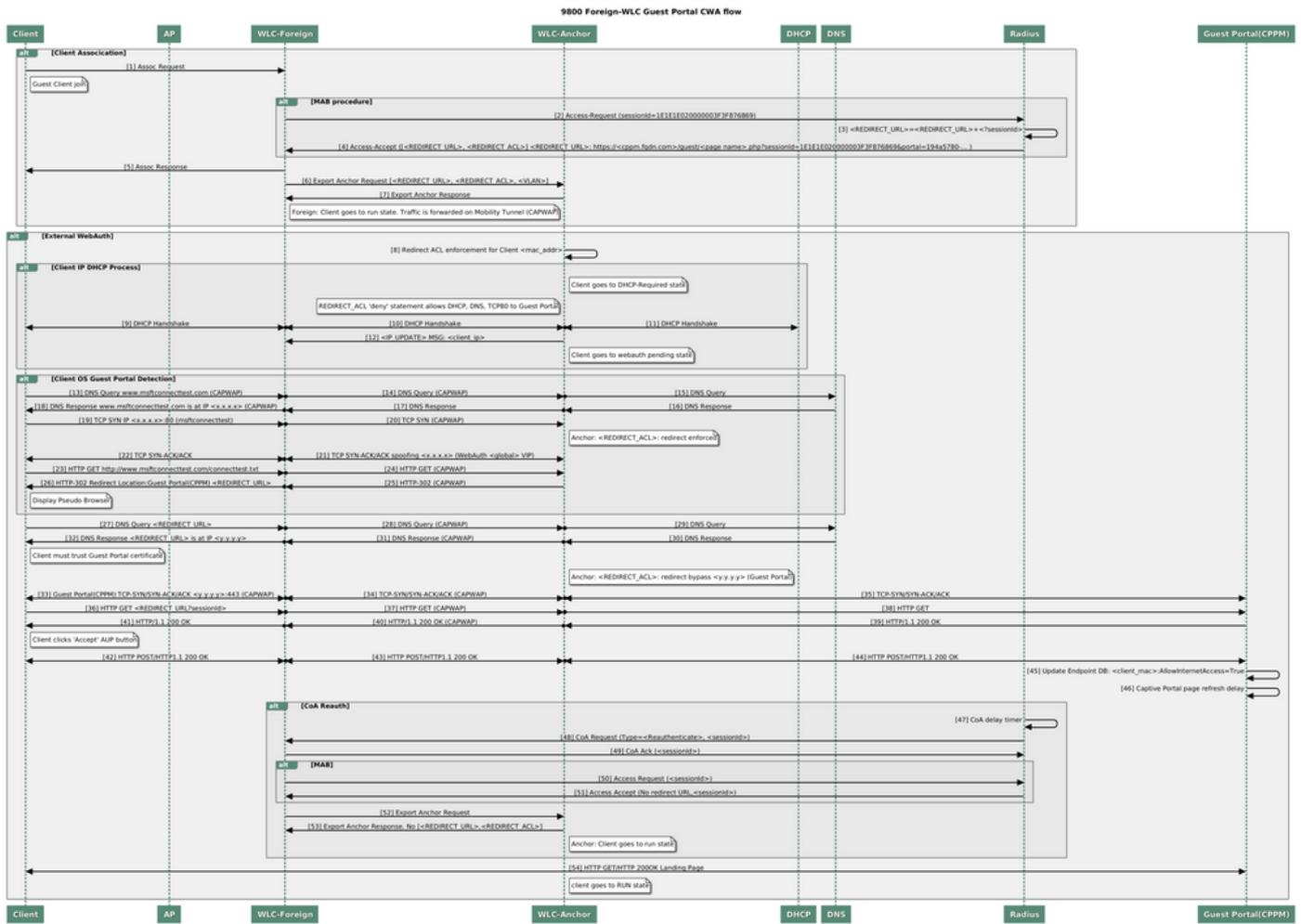


Diagramme d'état d'authentification Web Guest Central avec WLC d'ancrage

## Informations connexes

- [Guide des meilleures pratiques de déploiement du Cisco 9800](#)
- [Comprendre le modèle de configuration des contrôleurs sans fil Catalyst 9800](#)
- [Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.