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

Table des matières

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 (requise 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 (requise 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.

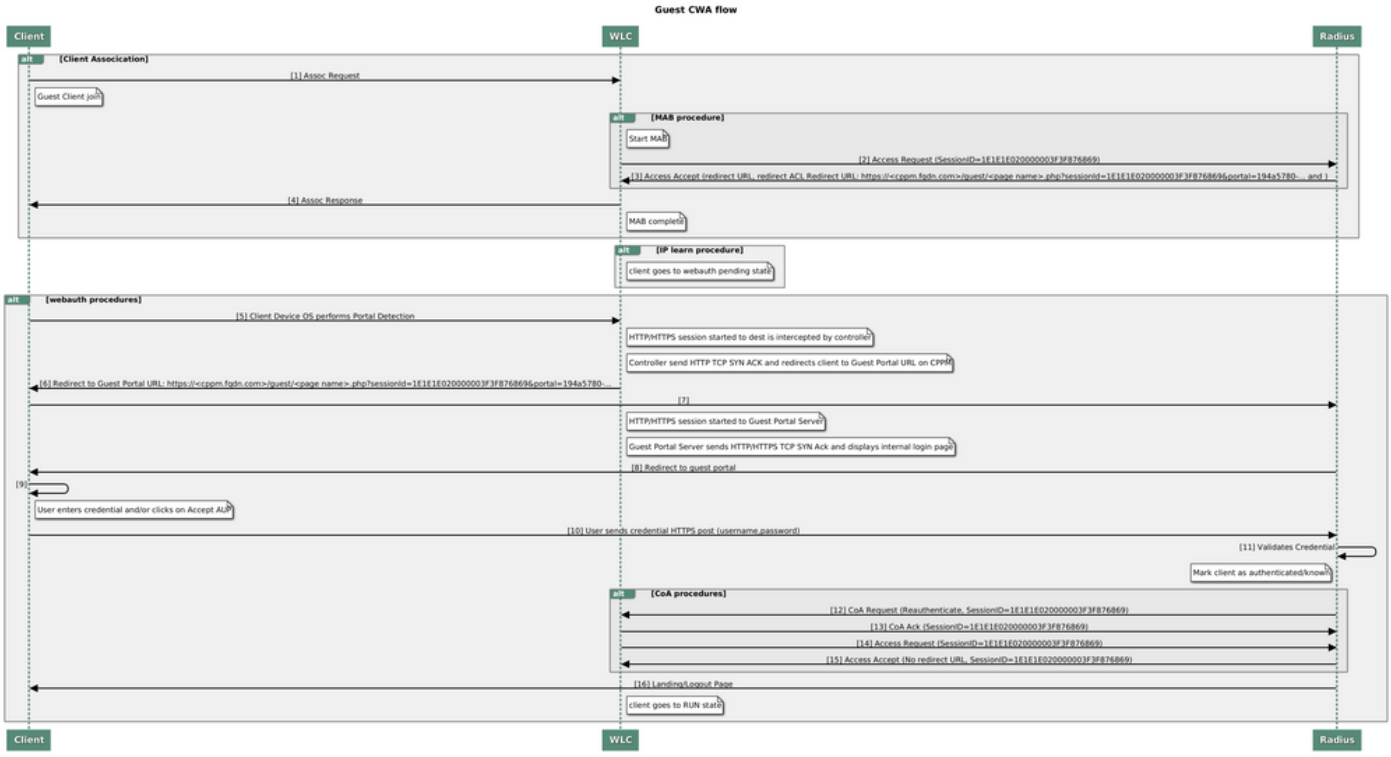


Diagramme d'état d'authentification Web de Guest Central (CWA)

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

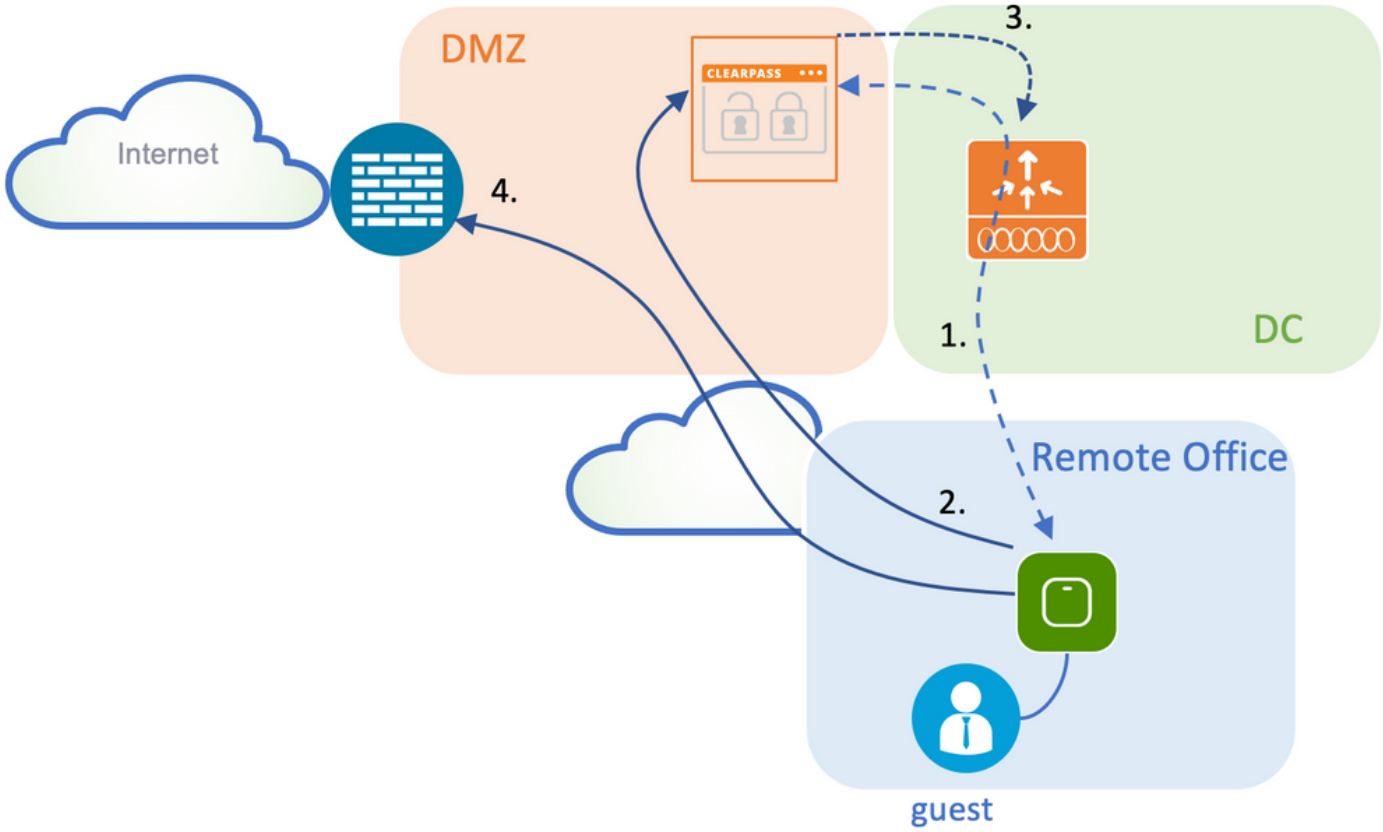
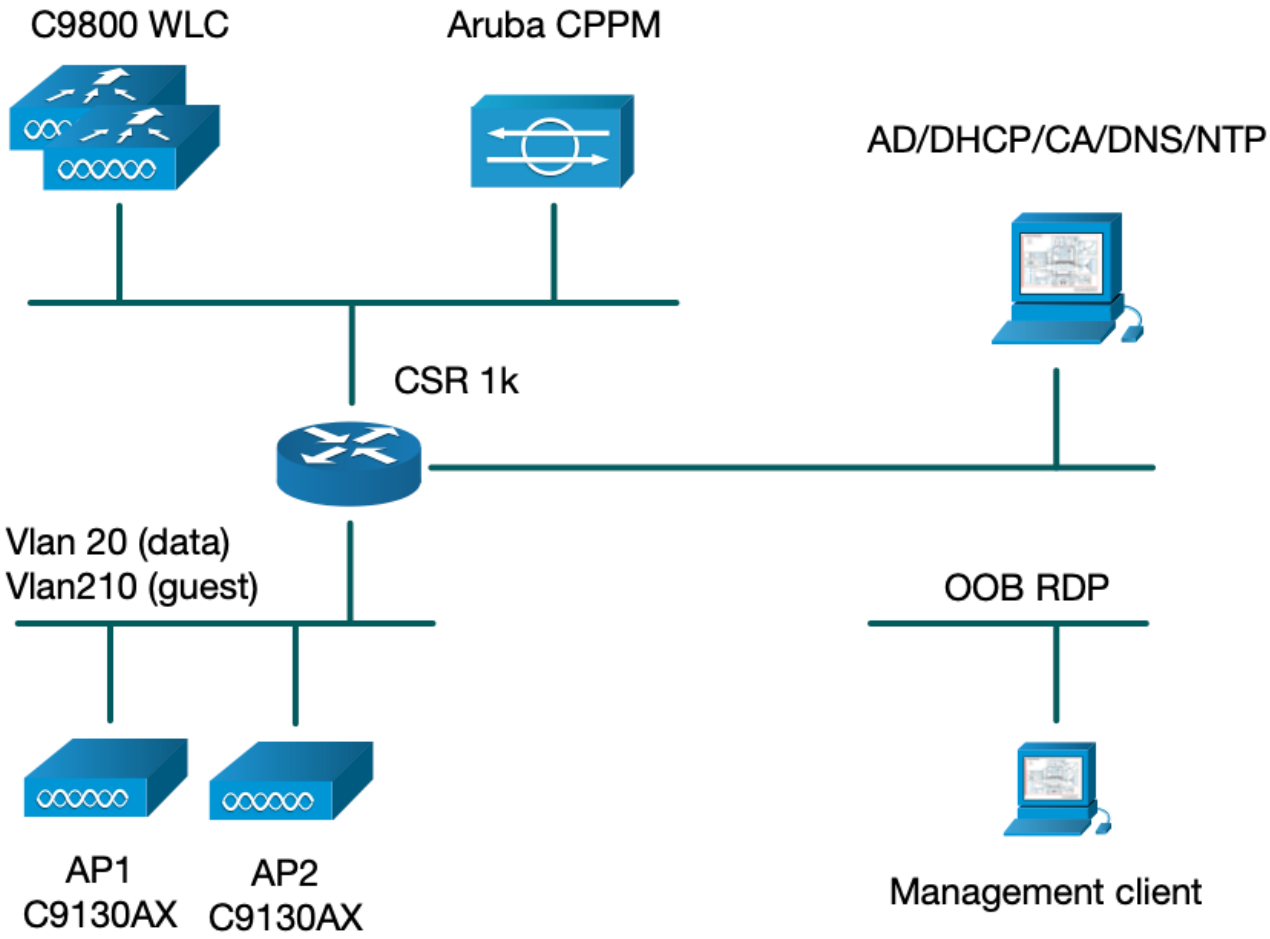


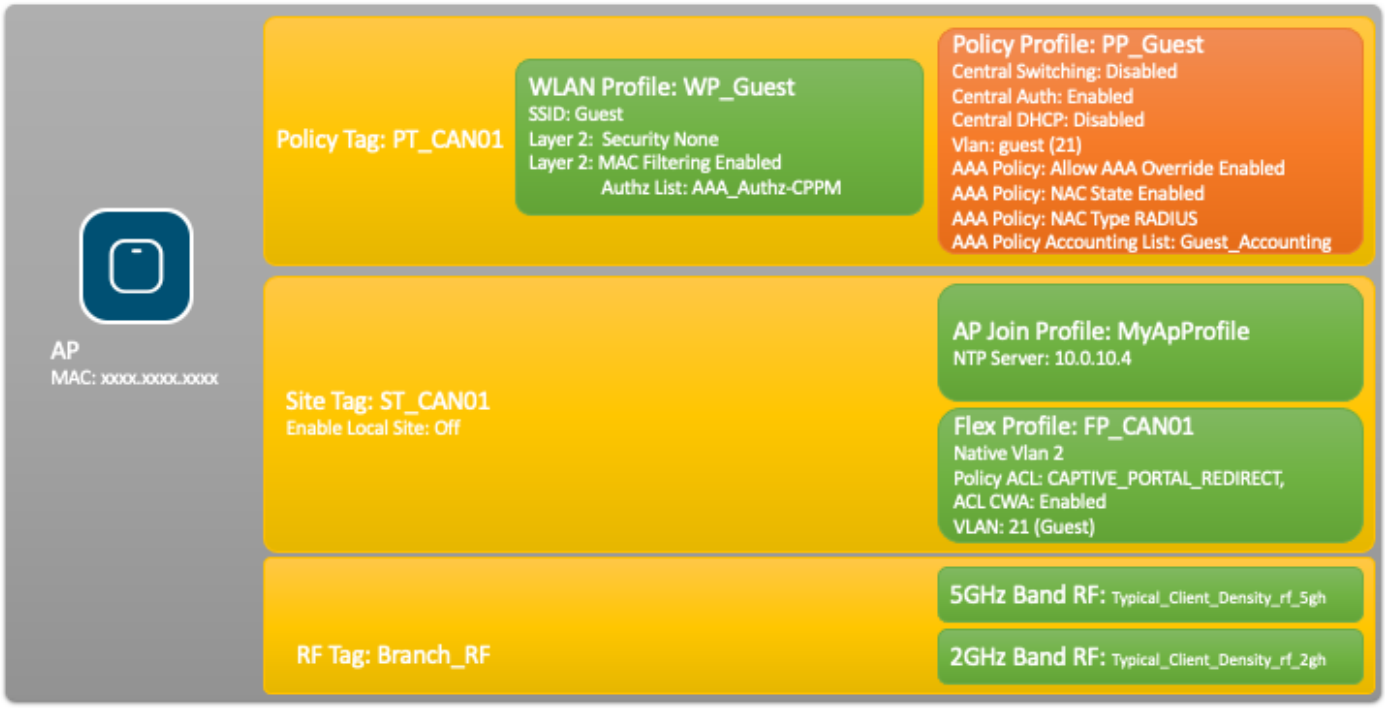
Diagramme du réseau

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 :

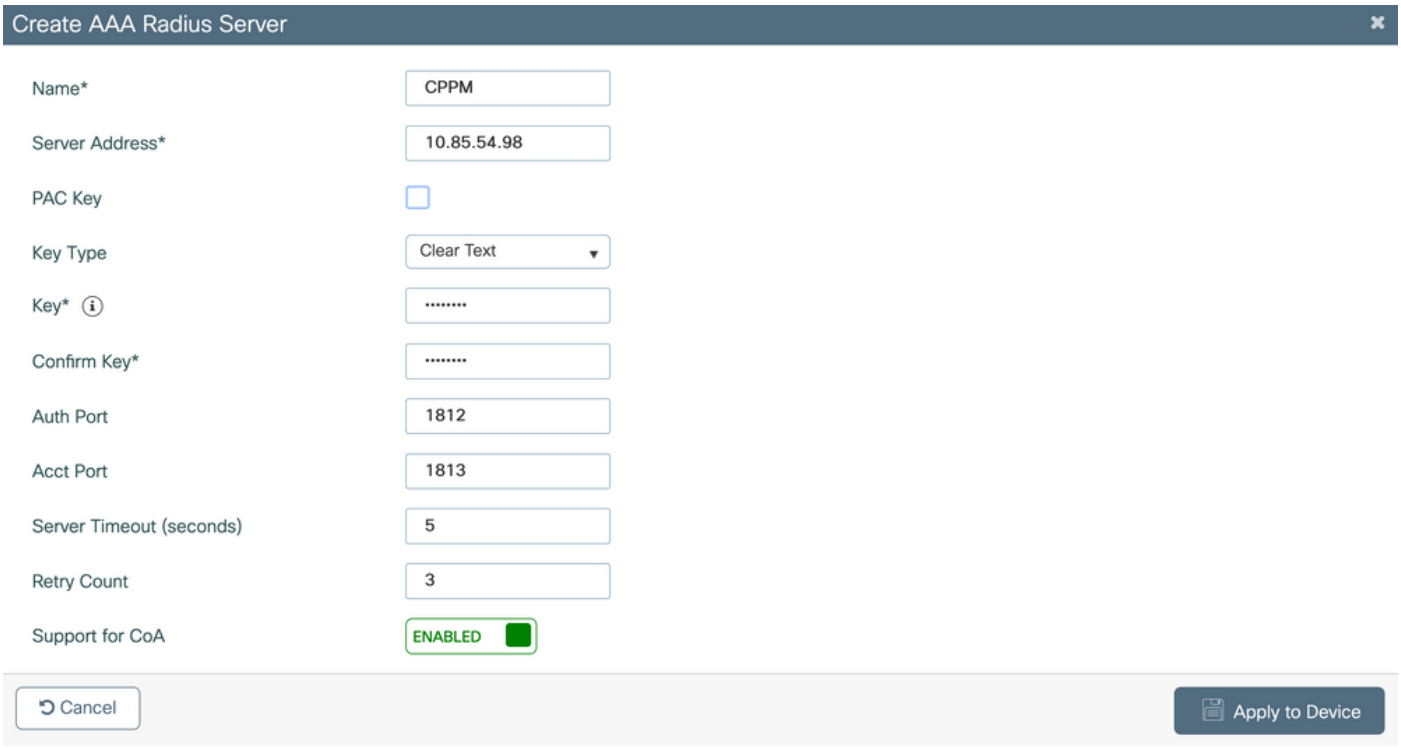


Configuration des paramètres de l'accès sans fil invité C9800

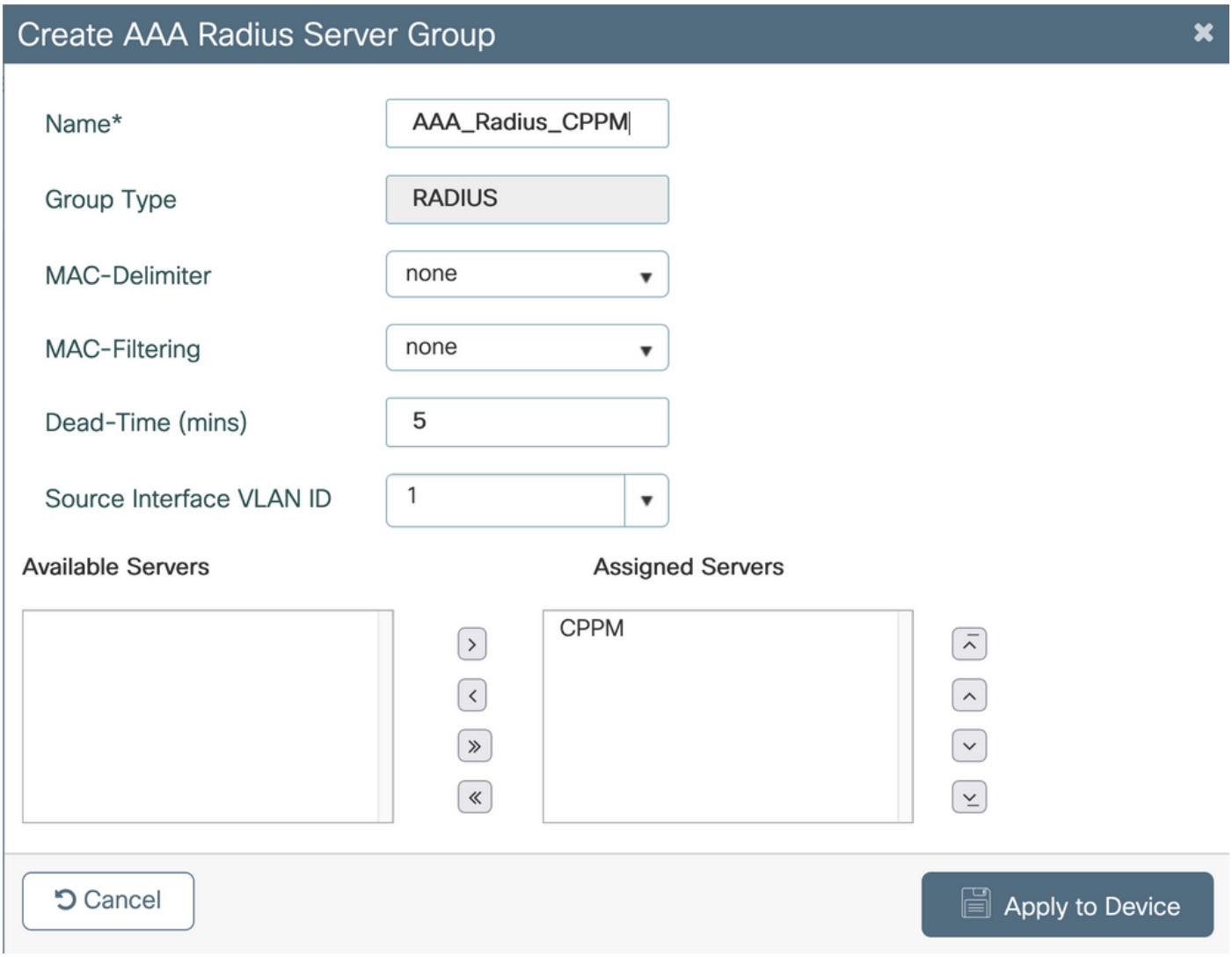
C9800 - Configuration AAA pour invité

Remarque : à propos de l'ID de bogue Cisco CSCvh03827, 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.

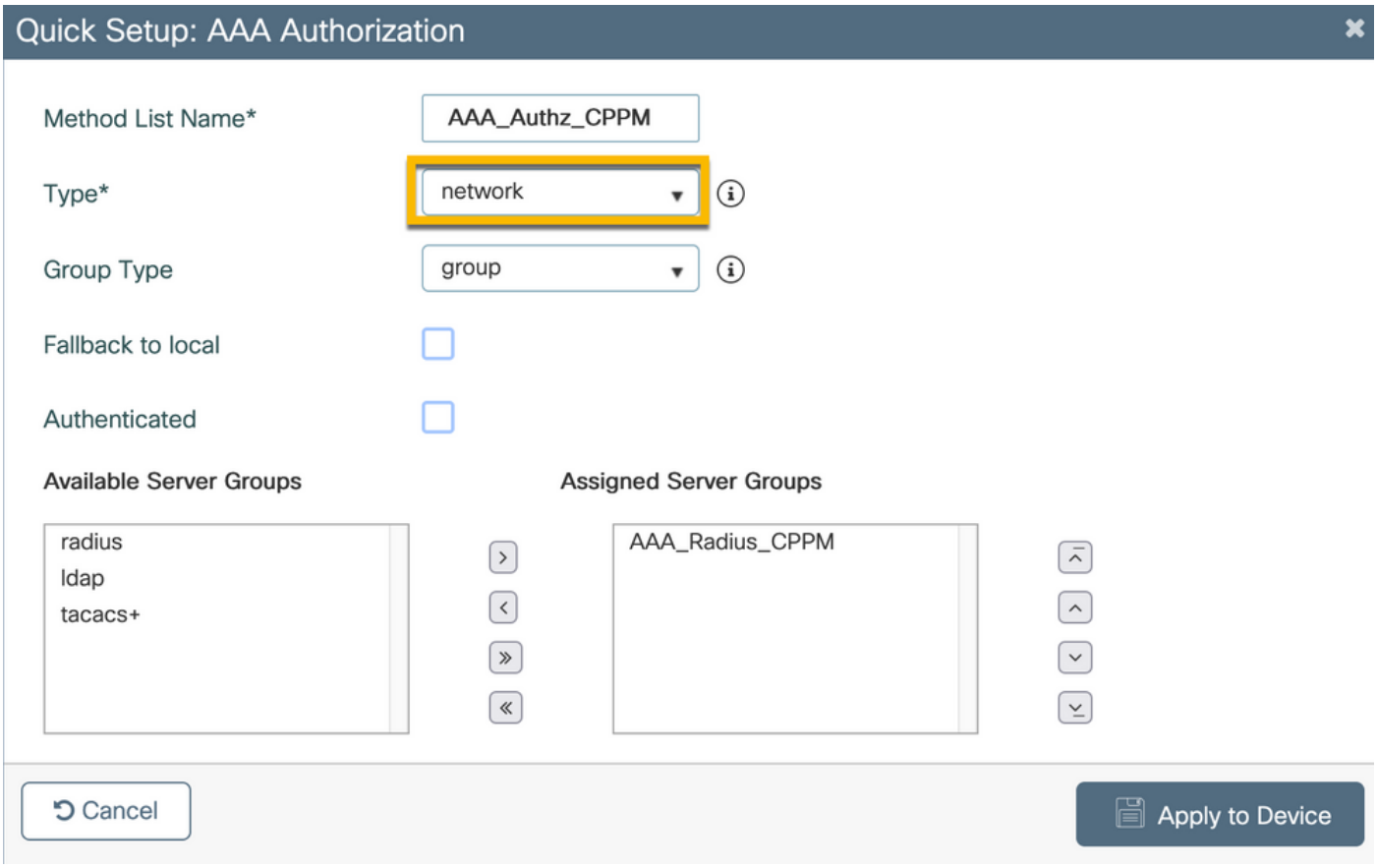
Étape 1. Ajoutez le ou les serveurs DMZ Aruba ClearPass à la configuration du WLC 9800 et créez une liste de méthodes d'authentification. Naviguez jusqu'àConfiguration > Security > AAA > Servers/Groups > RADIUS > Servers > +Addet saisissez les informations relatives au serveur RADIUS.



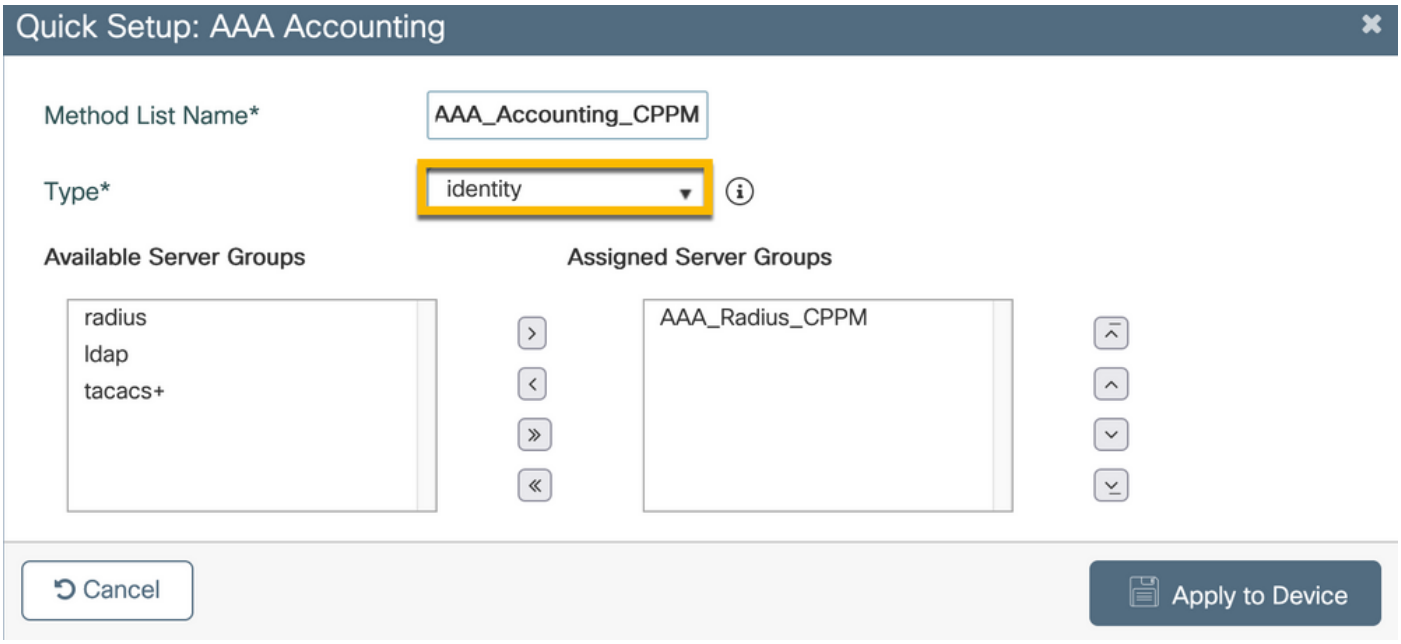
Étape 2. Définissez un groupe de serveurs AAA pour les invités et affectez le serveur configuré à l'étape 1 à ce groupe de serveurs. Accédez àConfiguration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add.



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 àConfiguration > Security > AAA > AAA Method List > Authorization > +Add. SélectionnezType Network, puisAAA Server Groupconfigurez à l'étape 2.



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 àConfiguration > Security > AAA > AAA Method List > Accounting > +Add. ChoisissezType Identitydans le menu déroulant, puis configurezAAA Server Groupà l'étape 2.



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.

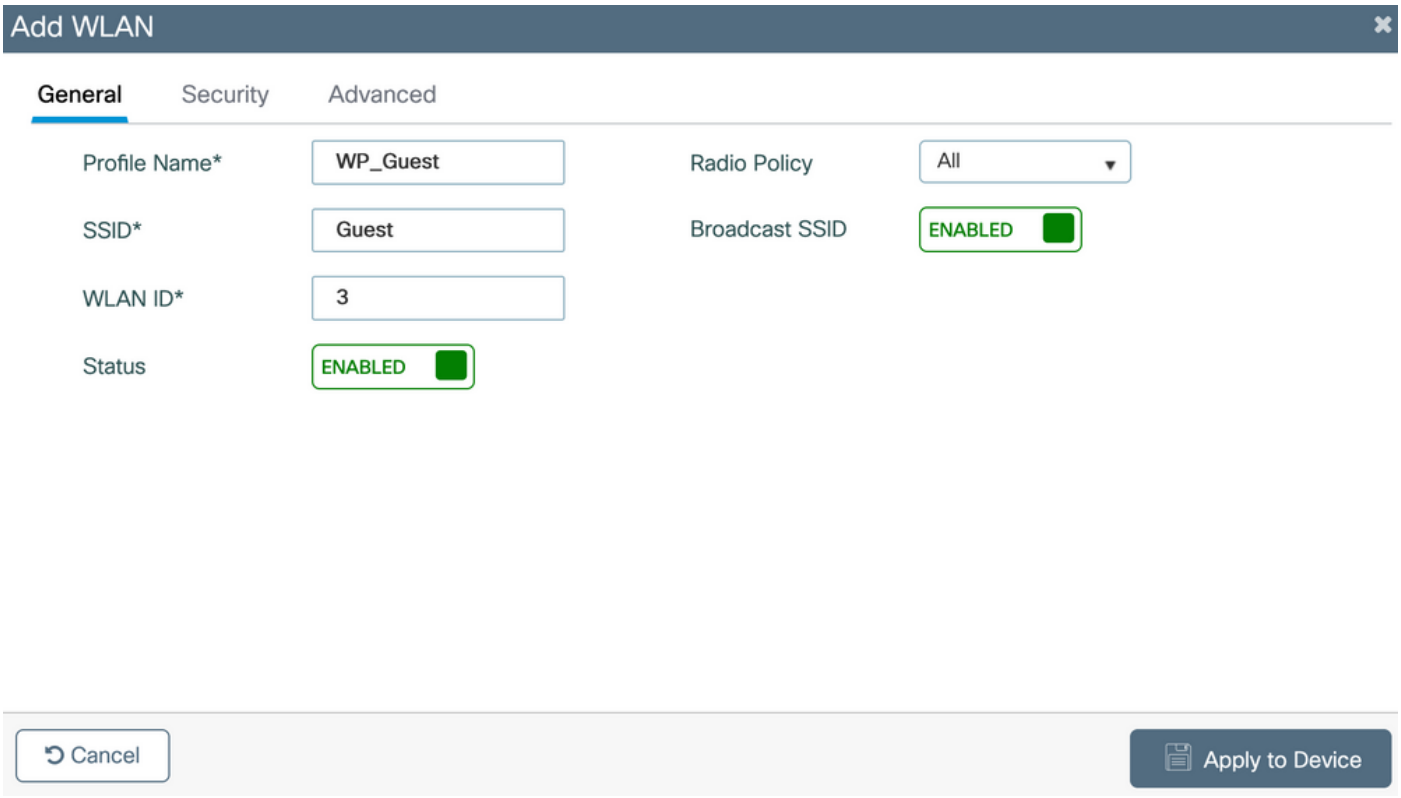
Accédez àConfiguration > Security > ACLet définissez une nouvelle liste de contrôle d'accès nomméeCAPTIVE_PORTAL_REDIRECT. Configurez la liste de contrôle d'accès avec ces ACE :

- 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 àConfiguration > Tags & Profiles > Wireless > +Add. Créez un nouveau profil SSID WP_Guest, avec la diffusion du SSID « Guest » auquel les clients invités s'associent.

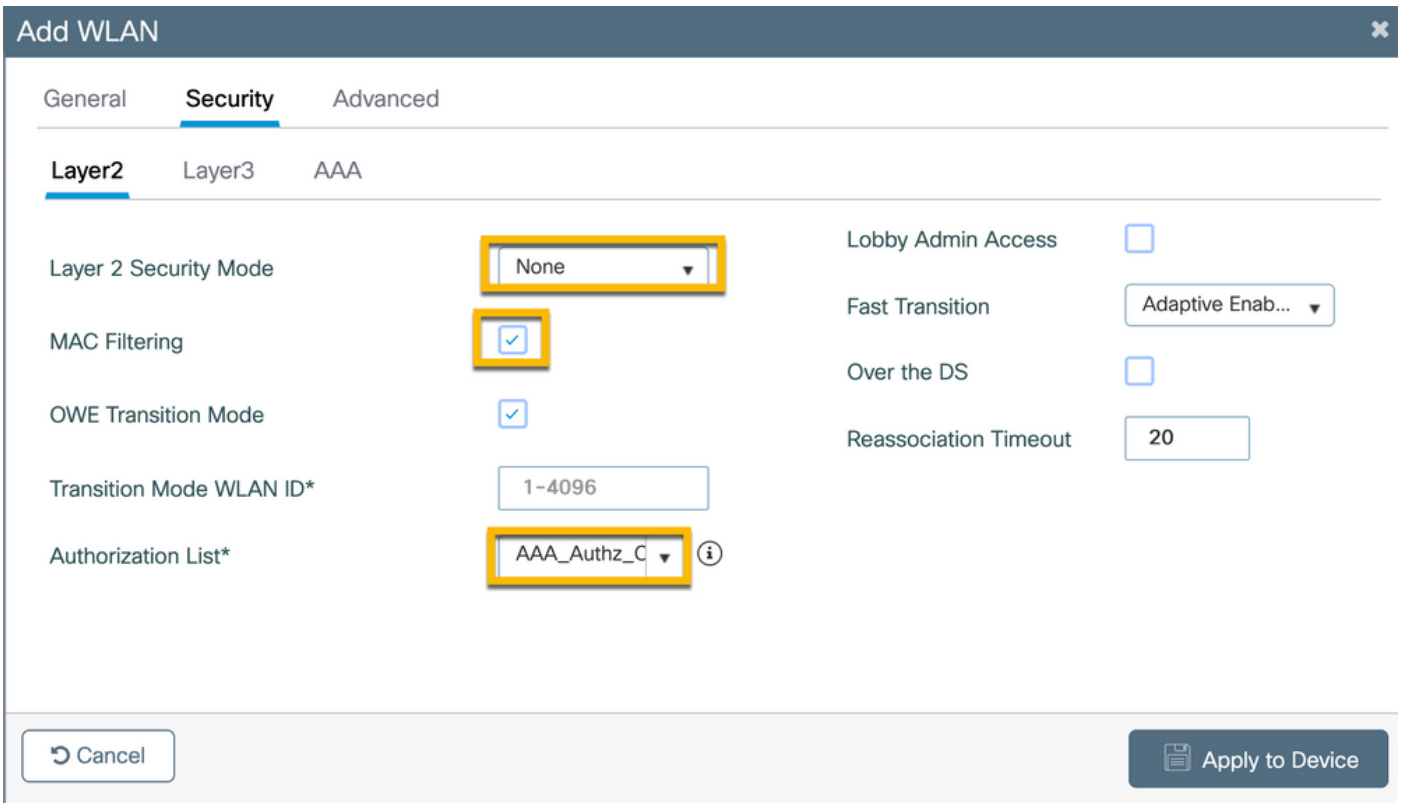


Dans la même boîte de dialogueAdd WLAN, accédez à l'Security > Layer 2onglet.

- 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)



C9800 - Définition du profil de politique d'invité

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

Nom : PP_Guest

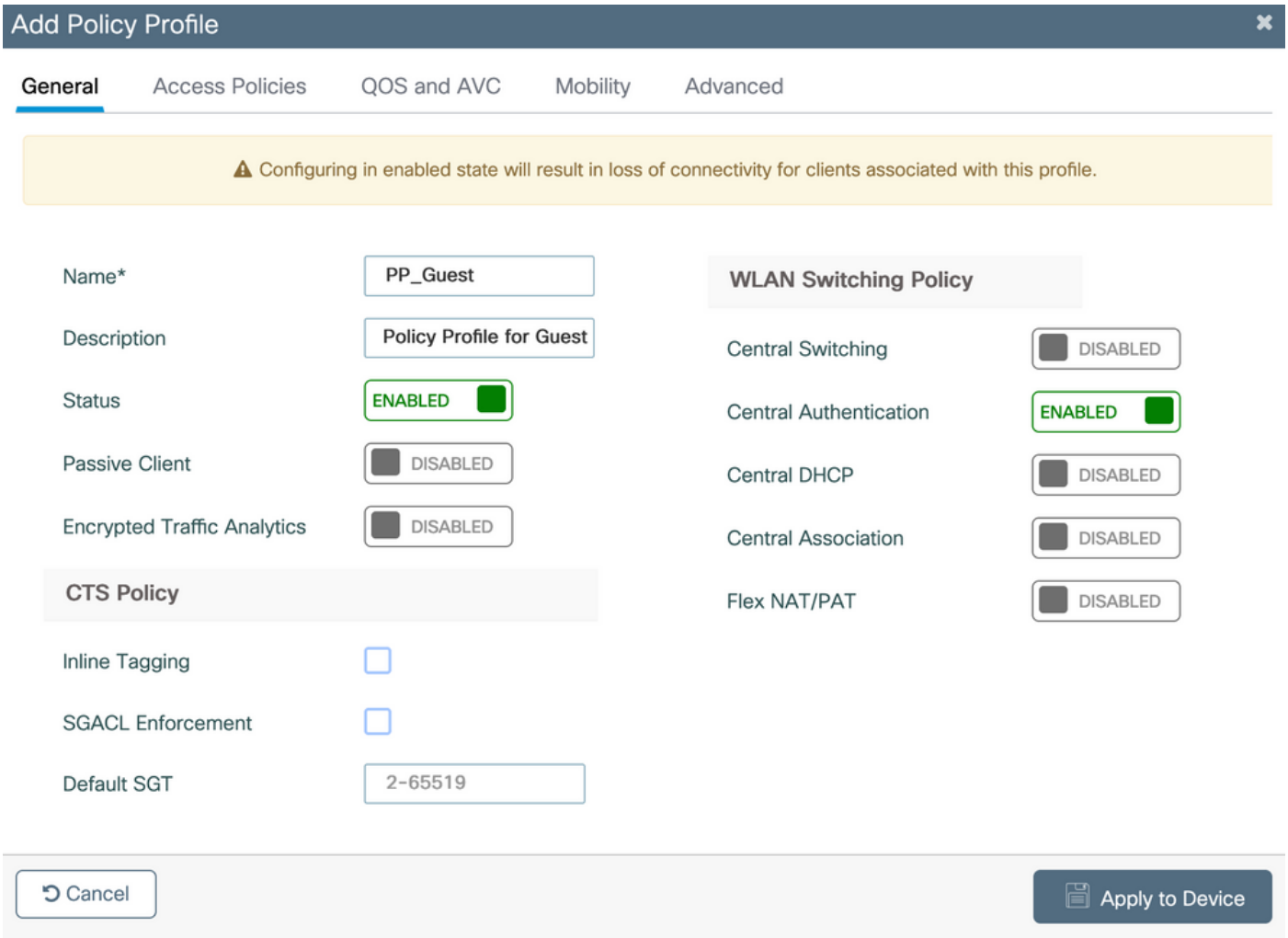
État : Activé

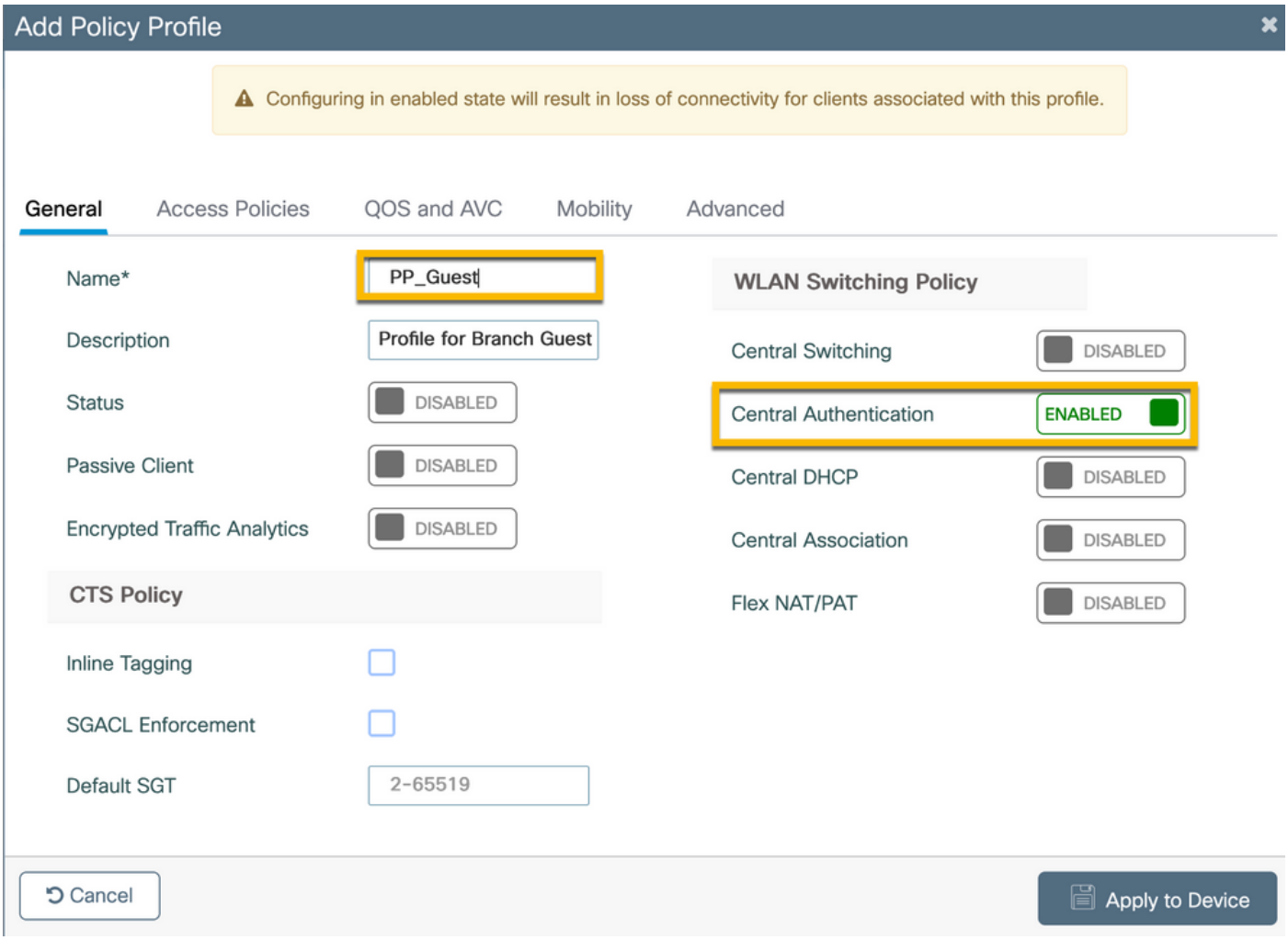
Commutation centrale : désactivée

Authentification centrale : activée

DHCP central : désactivé

Association centrale : Désactivé





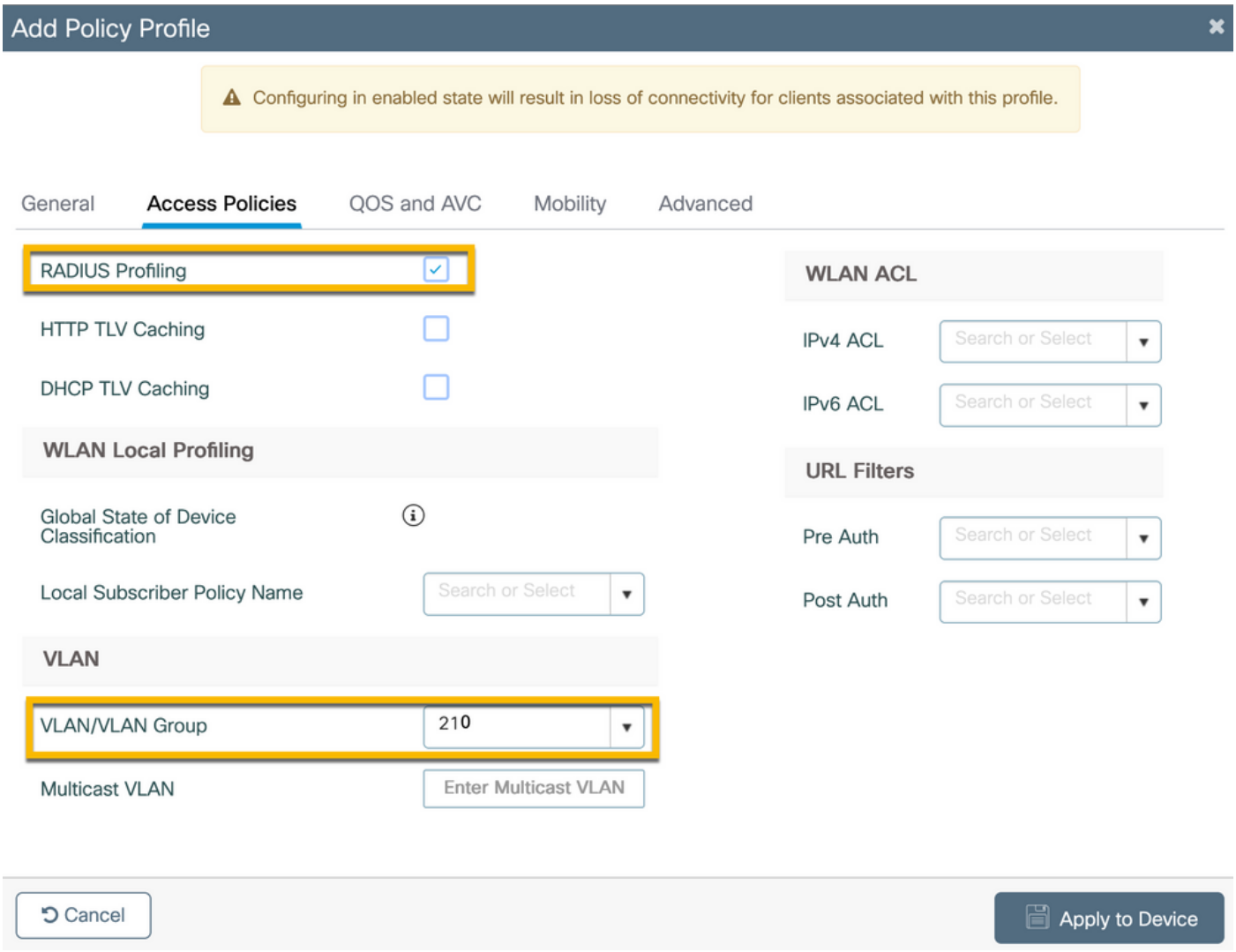
Accédez à l'ongletAccess Policiesdans la mêmeAdd Policy Profileboîte de dialogue.

- 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.



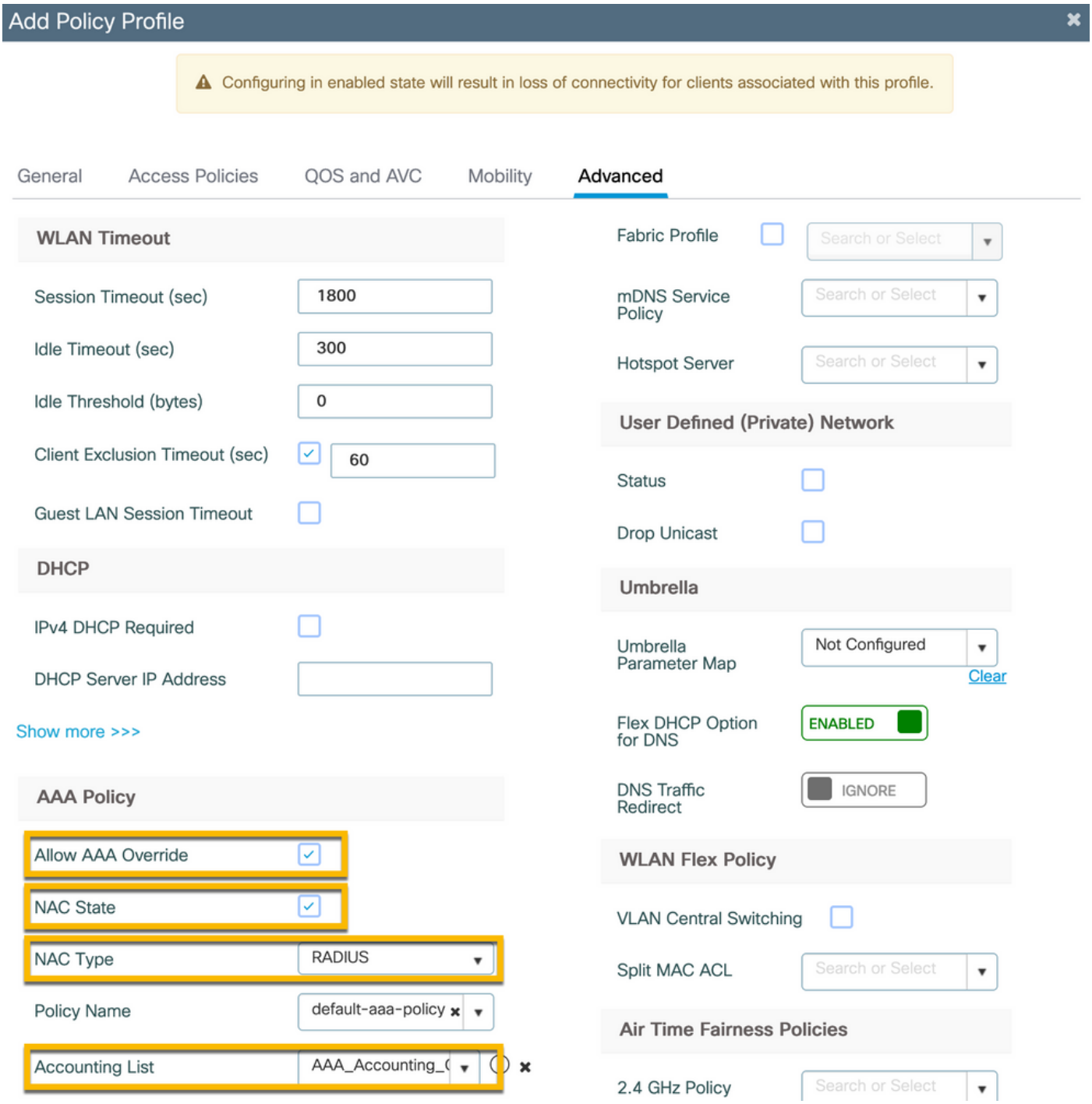
Dans la mêmeAdd Policy Profileboîte de dialogue, accédez à l'Advancedonglet.

- 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)



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 àConfiguration > Tags & Profiles > Tags > Policy > +Add.

- Nom : PT_CAN01

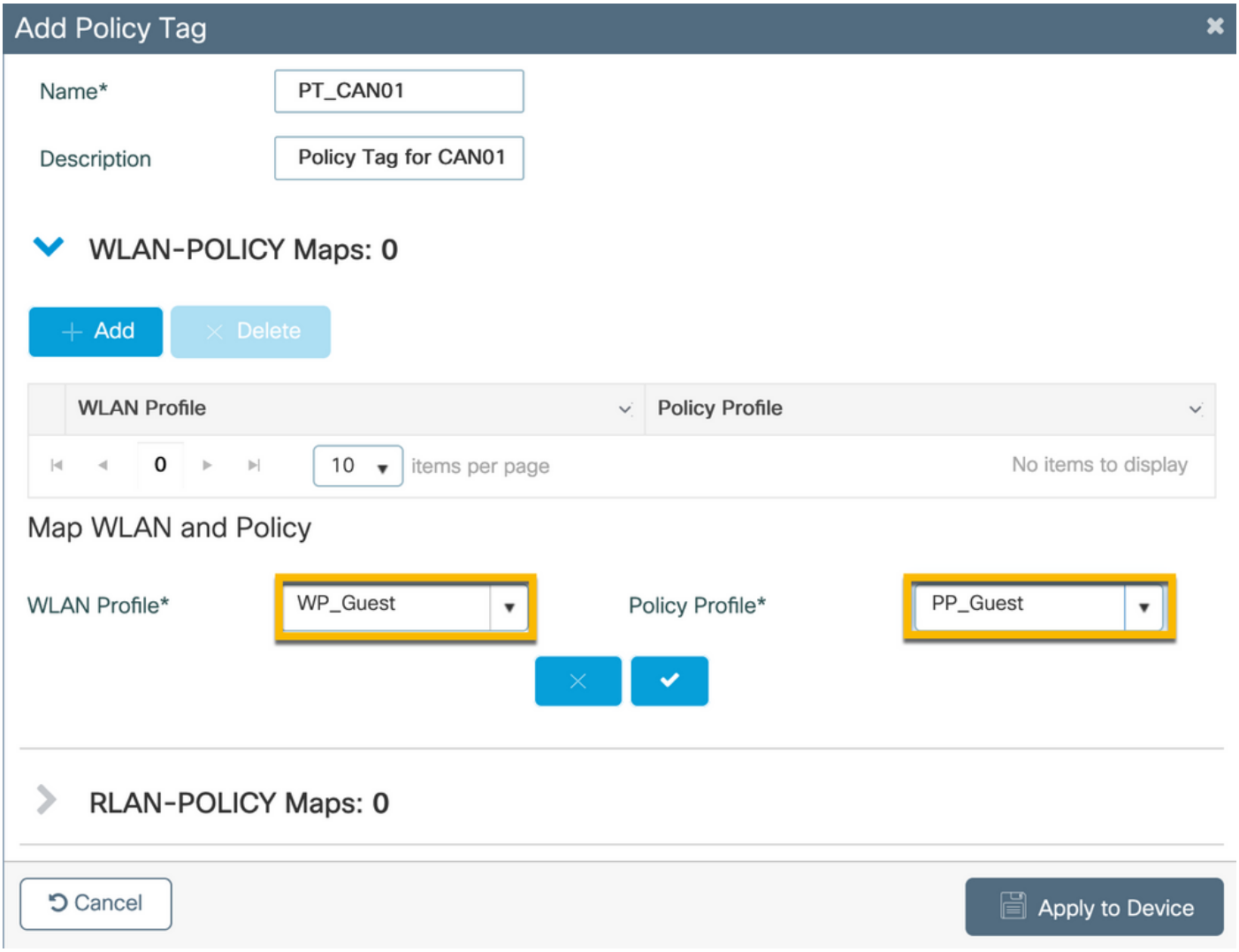
- Description : Étiquette de politique pour le site de la succursale CAN01

Dans la même boîte de dialogue,Add Policy TagsousWLAN-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

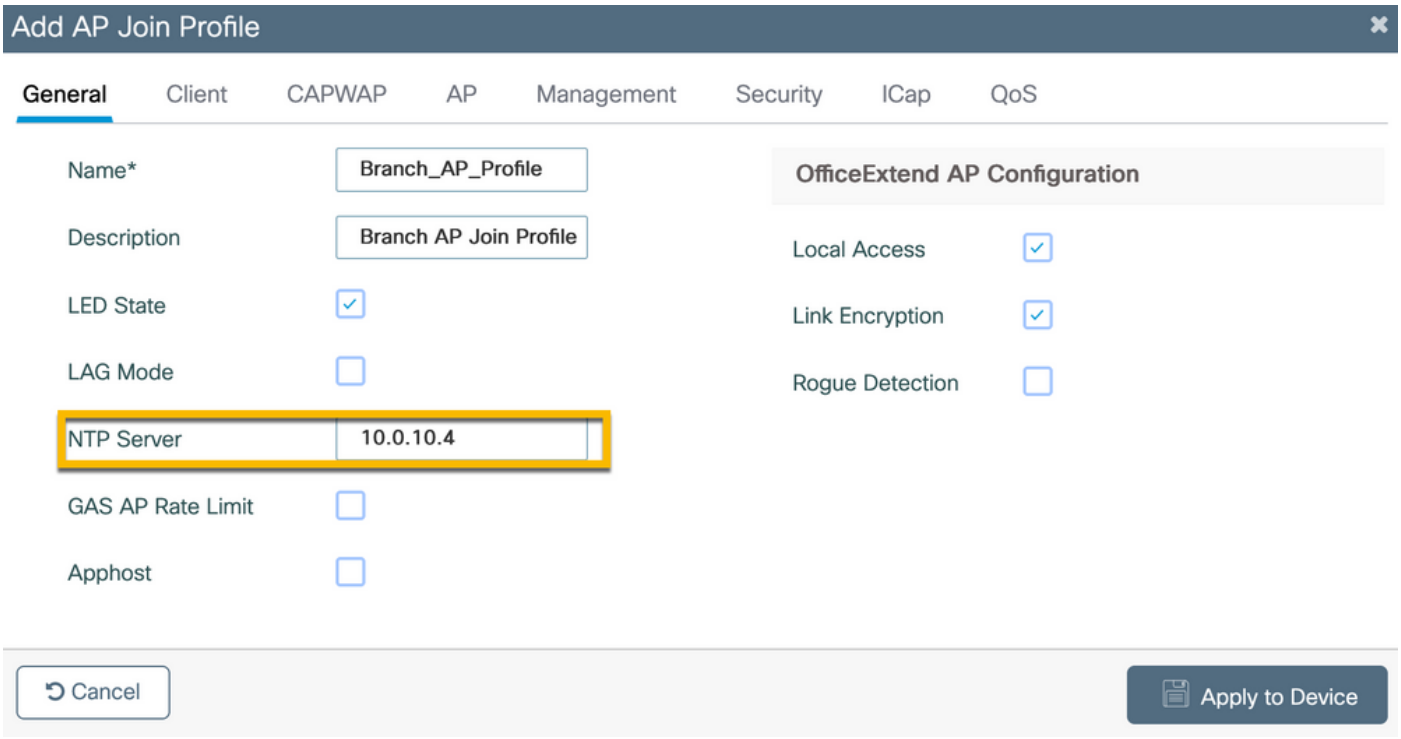


C9800 - Profil de jonction AP

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.



C9800 - Profil flexible

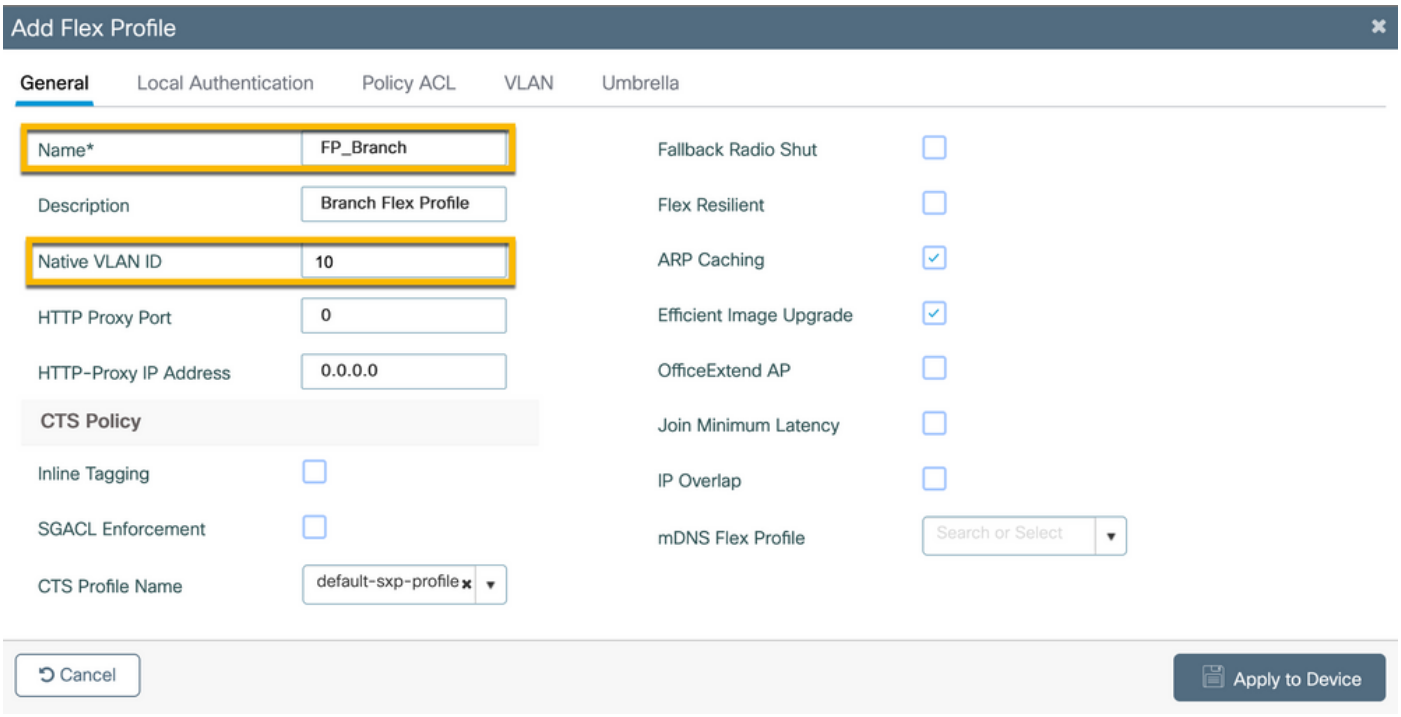
Les profils et les étiquettes sont modulaires et peuvent être réutilisés pour plusieurs sites.

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 àConfiguration > 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)

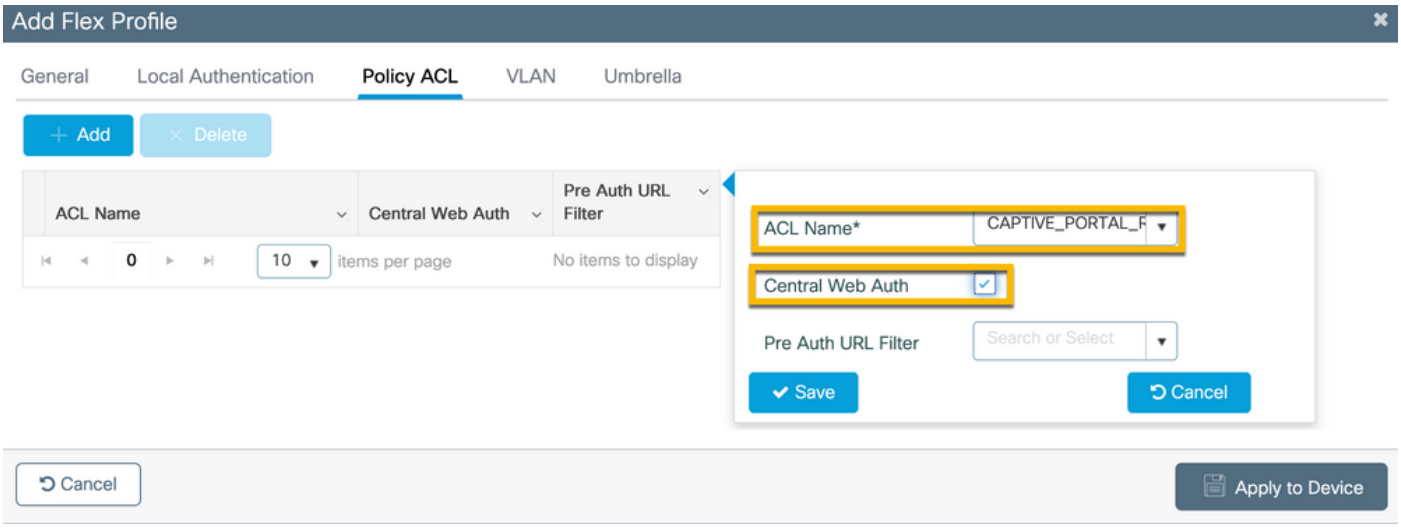


Dans la mêmeAdd Flex Profileboîte de dialogue, accédez à l'ongletPolicy ACLet cliquez sur+Add.

- Nom ACL : CAPTIVE_PORTAL_REDIRECT

- Authentification Web centrale : activée

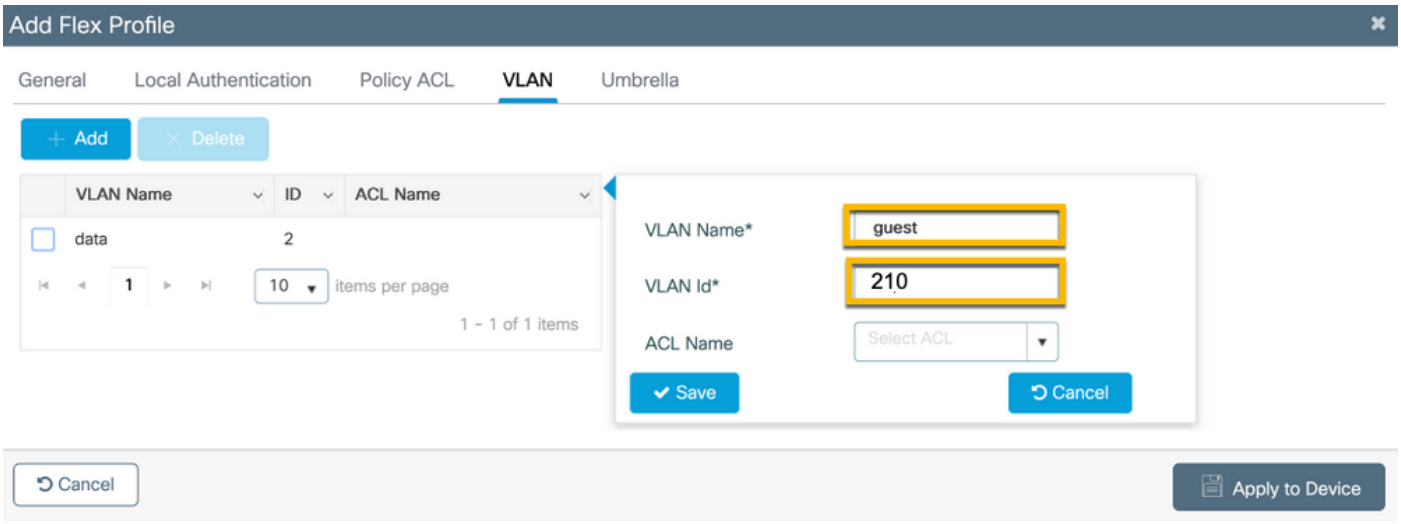
Sur un déploiement Flexconnect, chaque point d'accès géré est censé télécharger la liste de contrôle d'accès de redirection localement, car la redirection se produit au niveau du point d'accès et non sur le C9800.



Dans la mêmeAdd Flex Profileboîte de dialogue, accédez à l'VLANonglet et cliquez sur+Add(reportez-vous au schéma de topologie des travaux pratiques).

- Nom du VLAN : guest

- ID de VLAN : 210



C9800 - Étiquette de site

Sur l'interface utilisateur graphique du WLC 9800, accédez àConfiguration > 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.

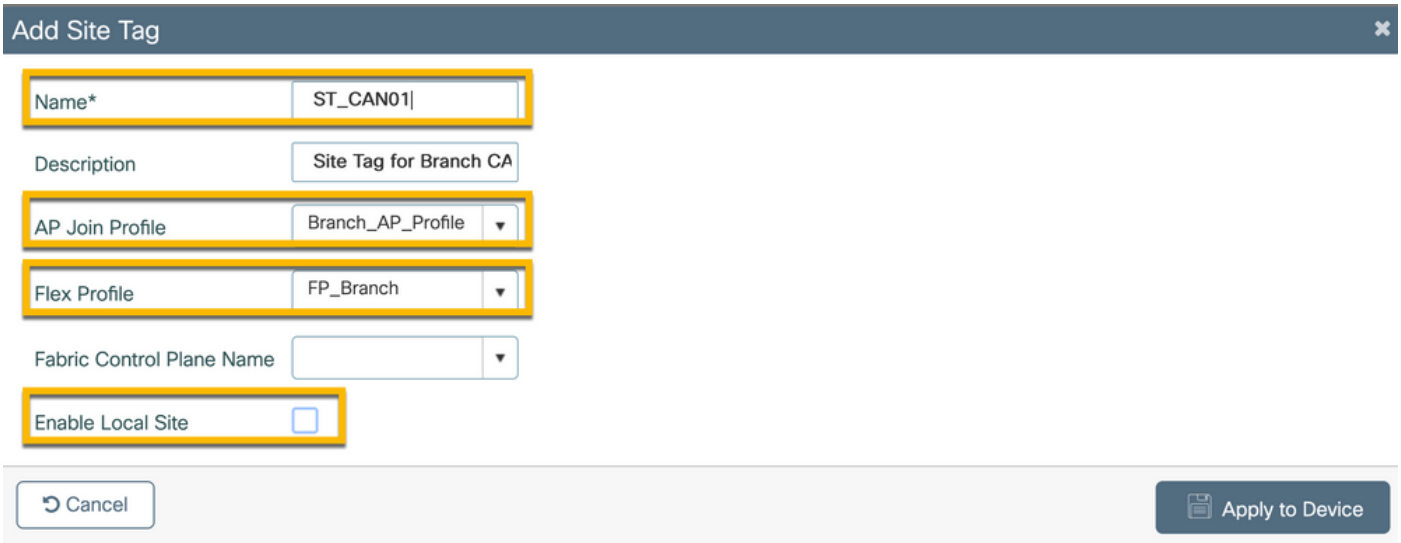
Un site de connexion flexible doit être associé à un profil de connexion flexible. Vous pouvez disposer d'un maximum de 100 points d'accès pour chaque site Flex Connect.

- Nom : ST_CAN01

- Profil de jointure AP : Branch_AP_Profile

- Profil flexible : FP_Branch

- Activer le site local : Désactivé



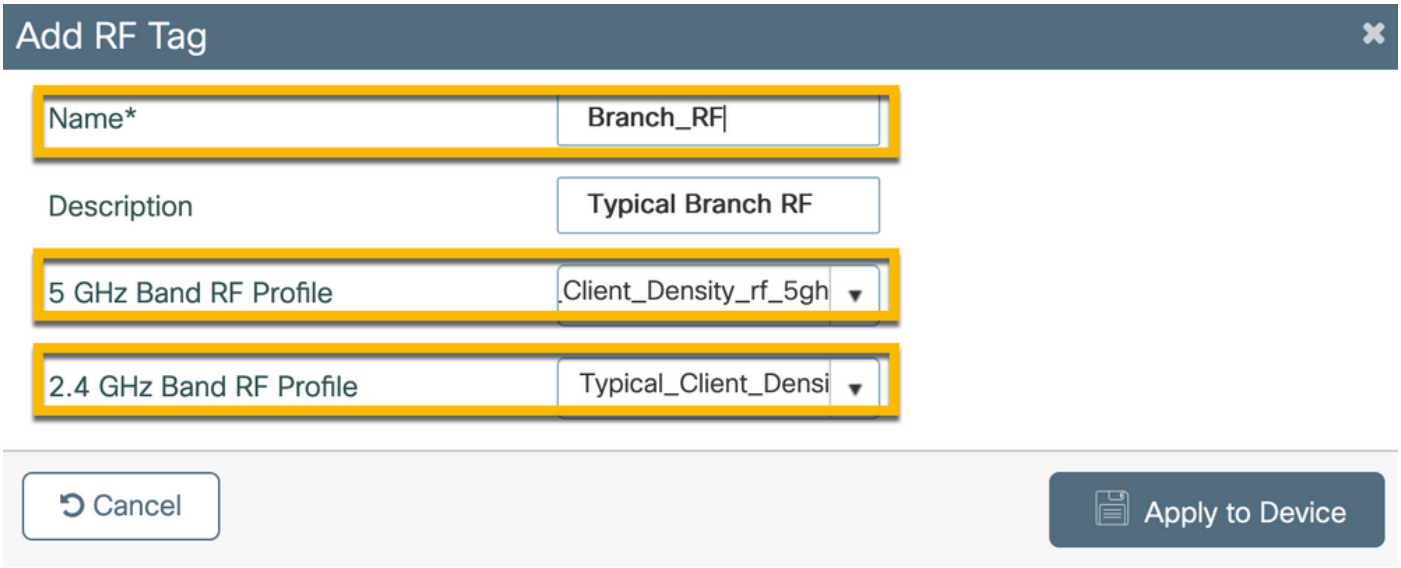
C9800 - Profil RF

Sur l'interface utilisateur graphique du WLC 9800, accédez àConfiguration > 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)



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 àConfigure > Tags & Profiles > Tags > AP > Static > Add(notez l'Upload Fileoption).

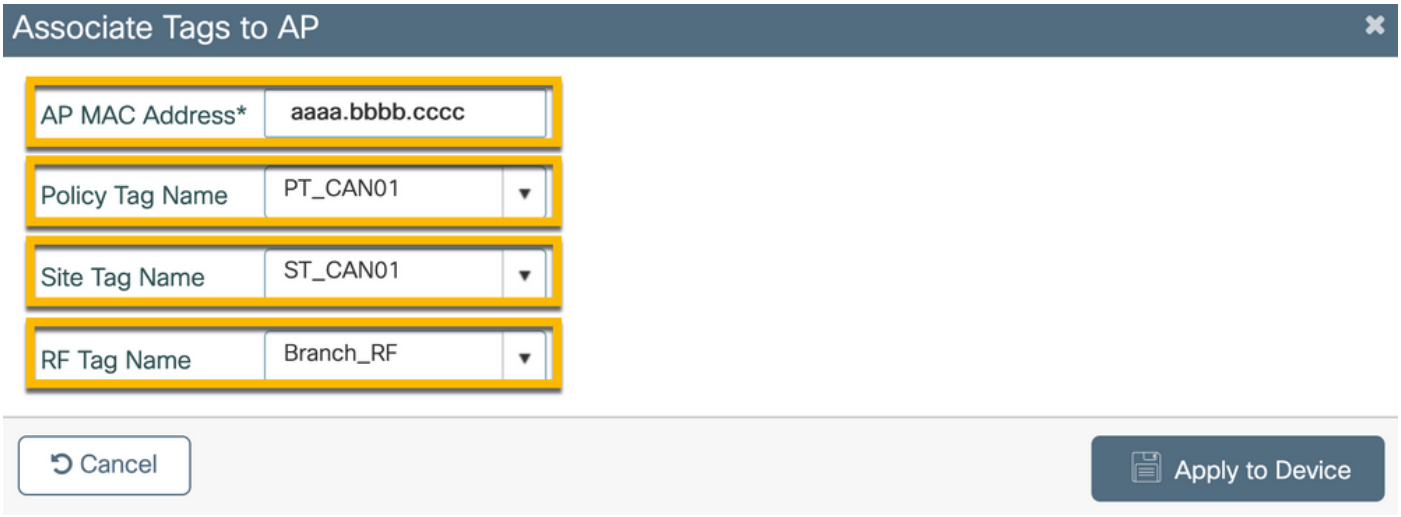
- Adresse MAC AP : <AP_ETHERNET_MAC>

- 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.



Remarque : vous pouvez également utiliser la méthode d'affectation de balise basée sur l'expression régulière AP-name en naviguant jusqu'àConfigure > Tags & Profiles > Tags > AP > Filter > Add.

- Nom : BR_CAN01

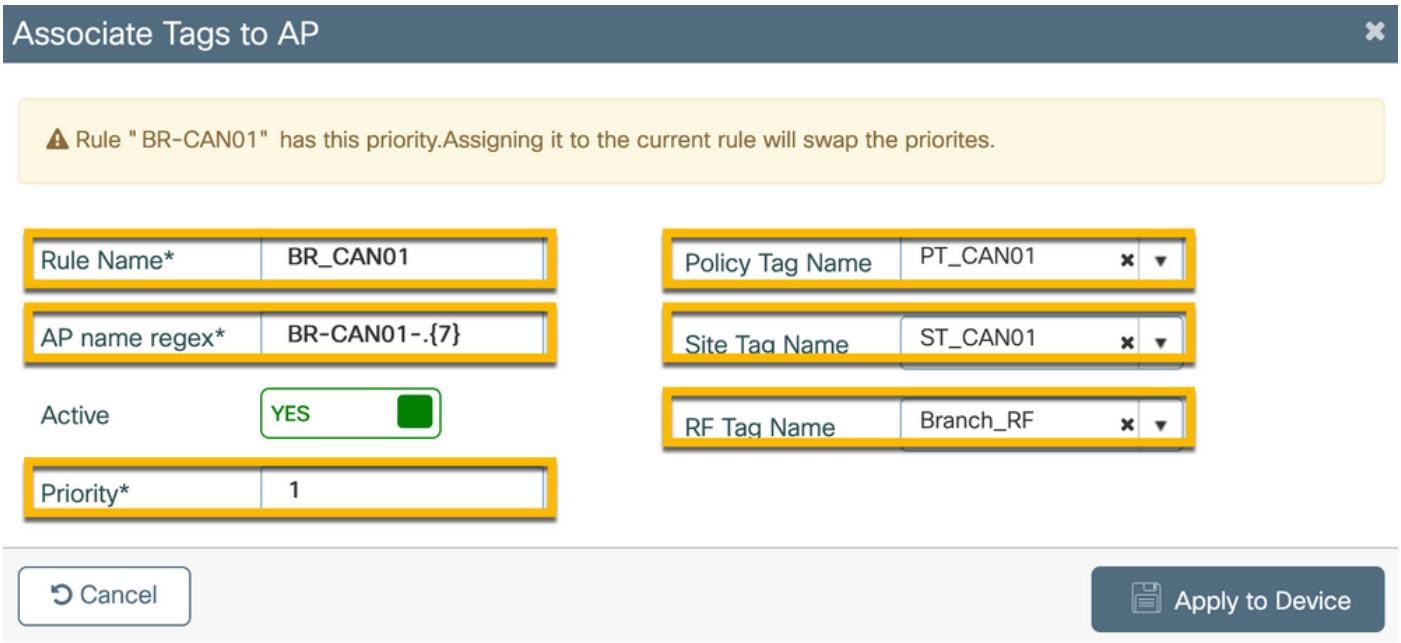
- Régex de nom d'AP : BR-CAN01-.(7) (Cette règle correspond à la convention de nom d'AP adoptée dans l'organisation. Dans cet exemple, les balises sont attribuées aux points d'accès qui ont un champ de nom de point d'accès qui contient 'BR_CAN01-' suivi de sept caractères.)

- 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



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 viaAdministration > Server Manager > Licensing. AjoutezPlatformAccess, etOnboard licenses.

Server Hostname

Accédez au serveur CPPM nouvellement provisionnéAdministration > Server Manager > Server Configurationet sélectionnez-le.

- Nom d'hôte : cppm

- FQDN : cppm.example.com

- Vérifier l'adressage IP et DNS du port de gestion

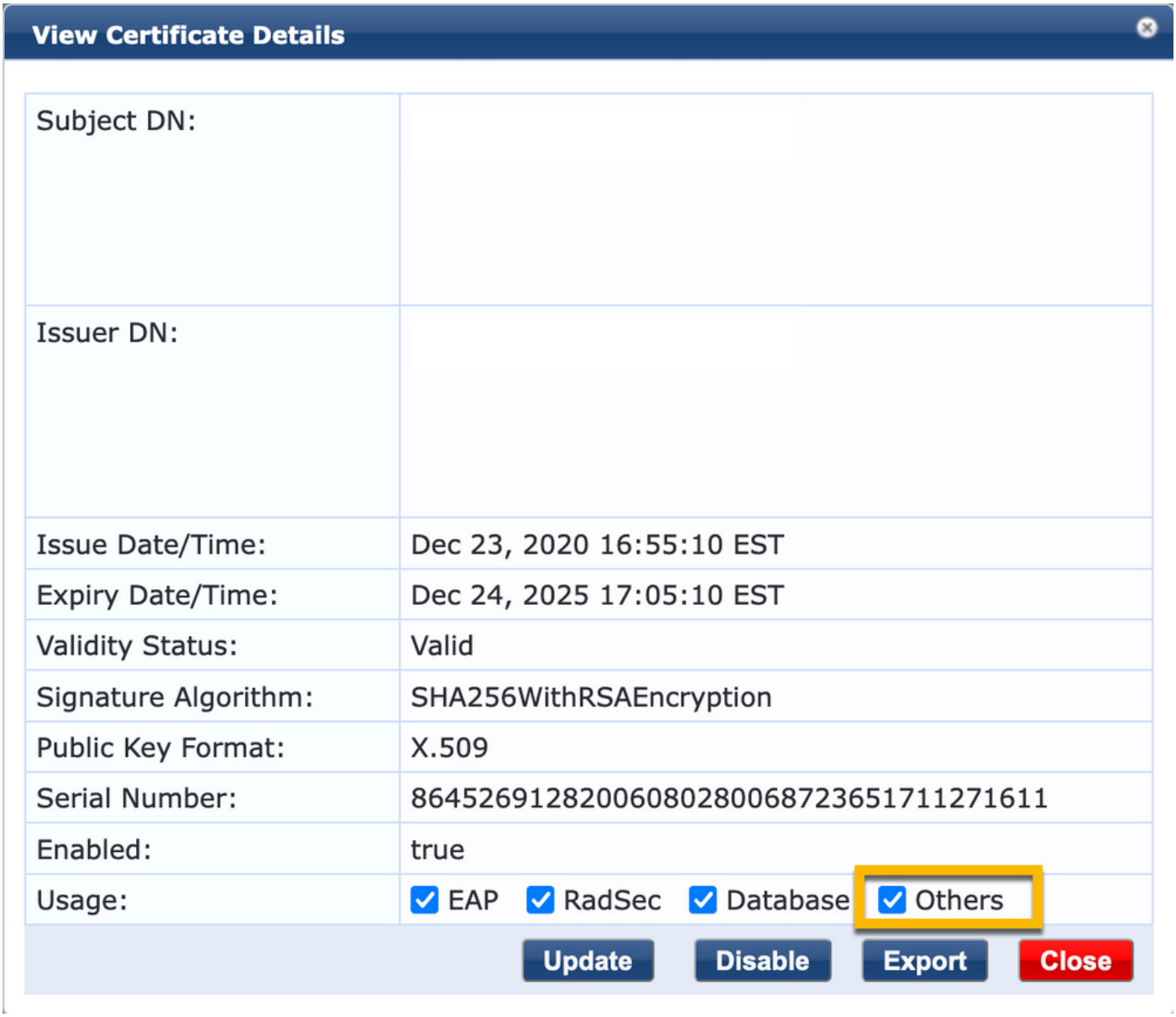
Générer un certificat de serveur Web CPPM (HTTPS)

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 àAdministration > Certificates > Trust List > Add.

- Utilisation : Activer les autres



Étape 2. Créer une demande de signature de certificat.

Accédez àAdministration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS Server Certificate.

- Cliquez sur le bouton Create Certificate Signing Request

- Nom commun : CPPM

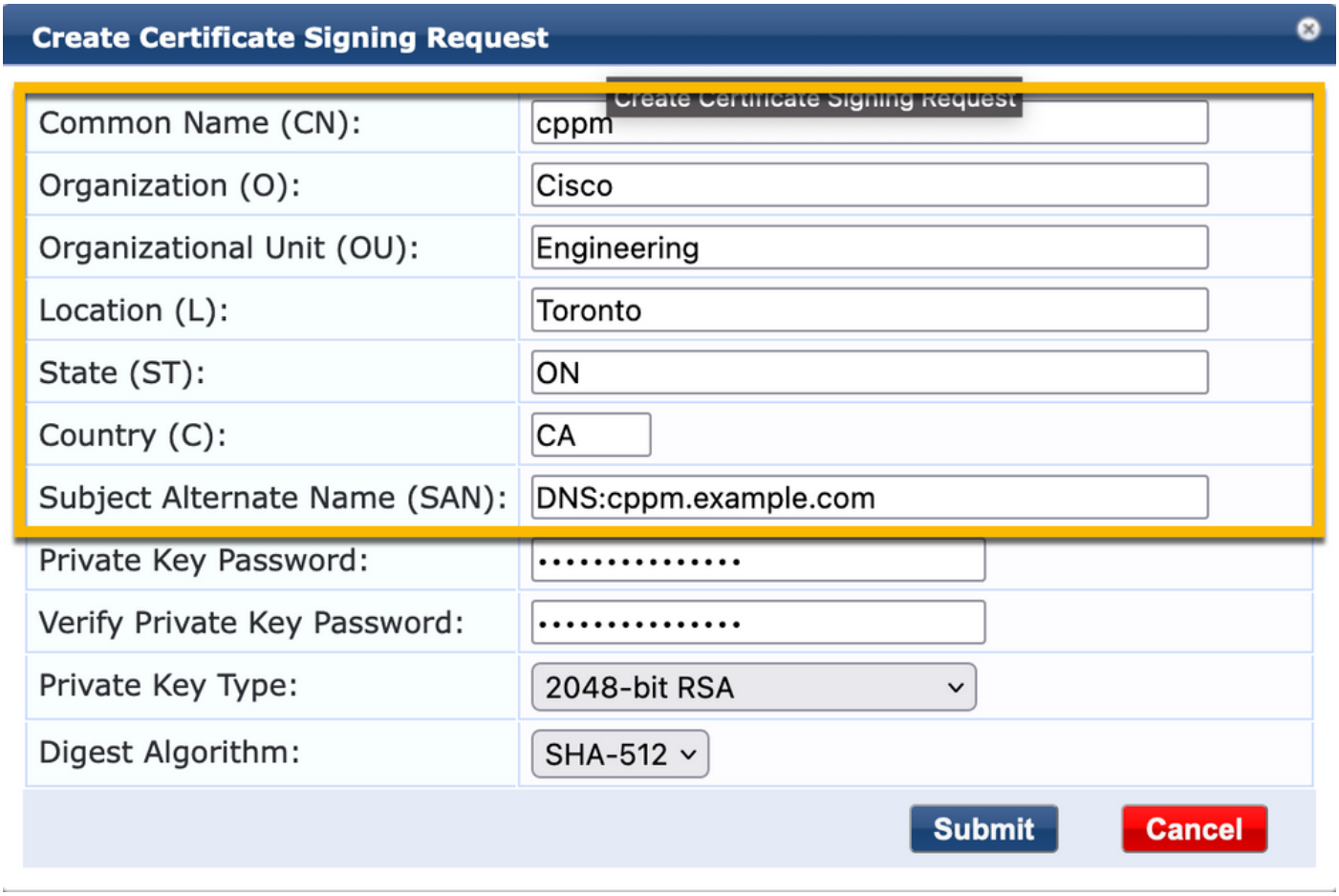
- Organisation : cppm.example.com

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

.



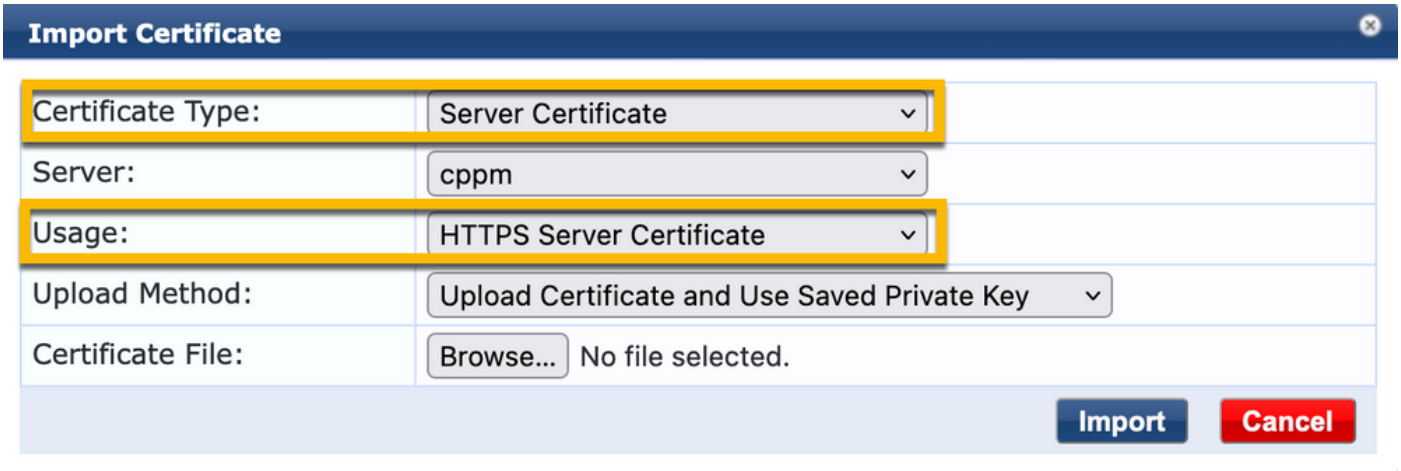
Étape 3. Dans l'autorité de certification de votre choix, signez le CSR du service HTTPS CPPM nouvellement généré.

Étape 4. Accédez àCertificate 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



Définir le WLC C9800 comme périphérique réseau

Accédez àConfiguration > Network > Devices > Add.

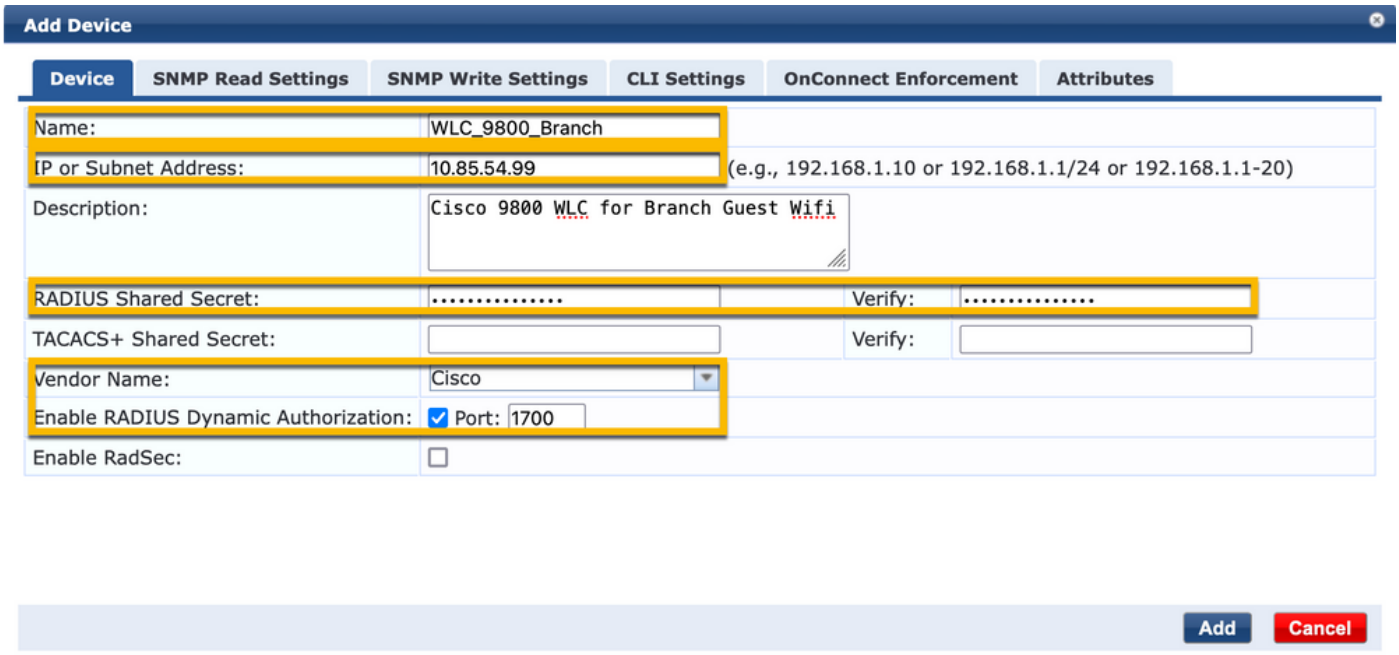
- Nom : WLC_9800_Branch

- 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

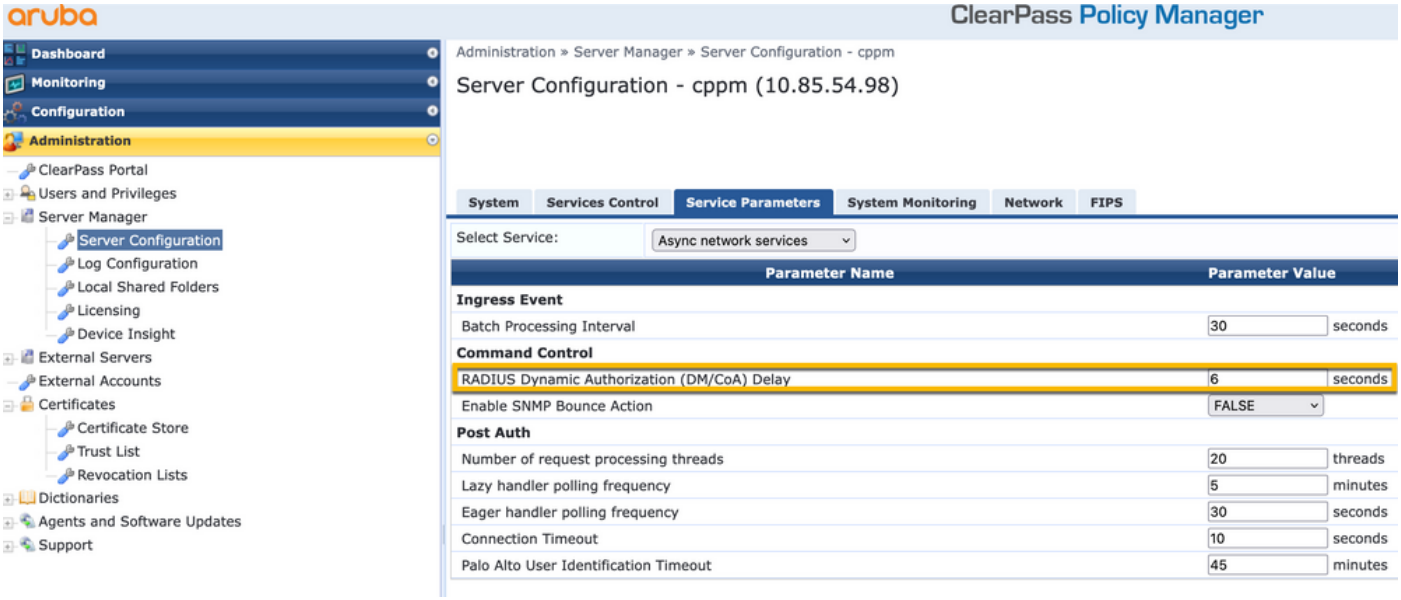


Page Guest Portal et minuteurs CoA

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 àGuest > 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

- 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 àCPPM > Administration > Server Manager > Server Configurationet sélectionnezCPPM Server > Service Parameters.
  - Délai d'autorisation dynamique (DM/CoA) RADIUS - défini sur six secondes



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 personnaliséAllow-Guest-Internet= TRUE, autorisez-le sur le réseau. Sinon, déclenchezRedirectetCOA: Reauthenticate.
2. Invité	Connexions Web	Présenter la page AUP de connexion anonyme. Post-auth définit un attribut personnaliséAllow-Guest-Internet=

		TRUE.
3. Gestionnaire des politiques	Service : authentification basée sur le Web	Mettre à jour le terminal Known Définir l'attribut personnaliséAllow-Guest-Internet= VRAI 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'àClearPass > Configuration > Endpoints, choisissez un point de terminaison dans la liste, cliquez sur l'Attributesonglet, ajoutezAllow-Guest-Internetavec la valeurfalseetSave.

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.

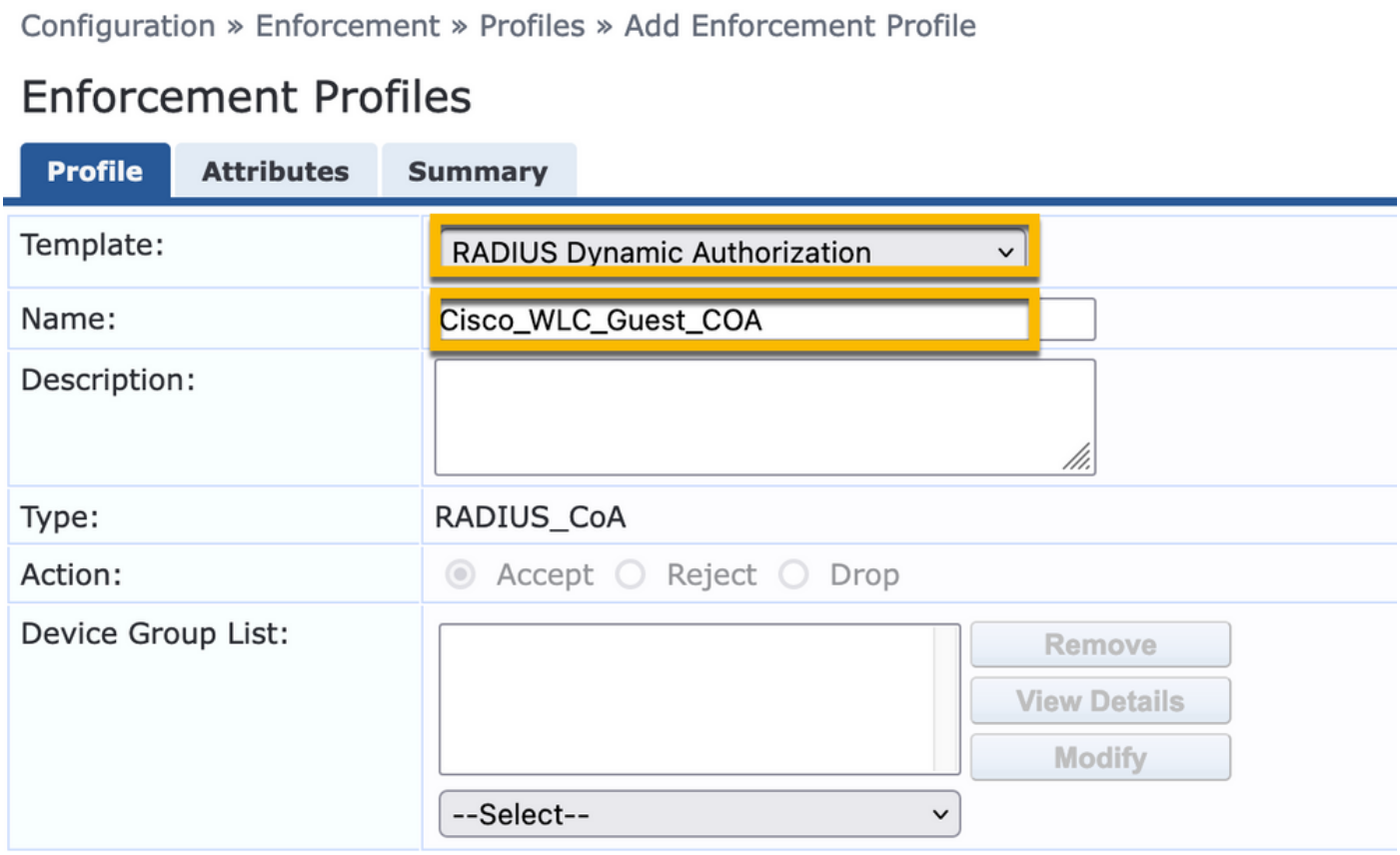
Configuration de la stratégie de réauthentification ClearPass

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 àClearPass > Configuration > Profiles > Add.

- Modèle : RADIUS Dynamic Authorization

- Nom : Cisco_WLC_Guest_COA



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 ».

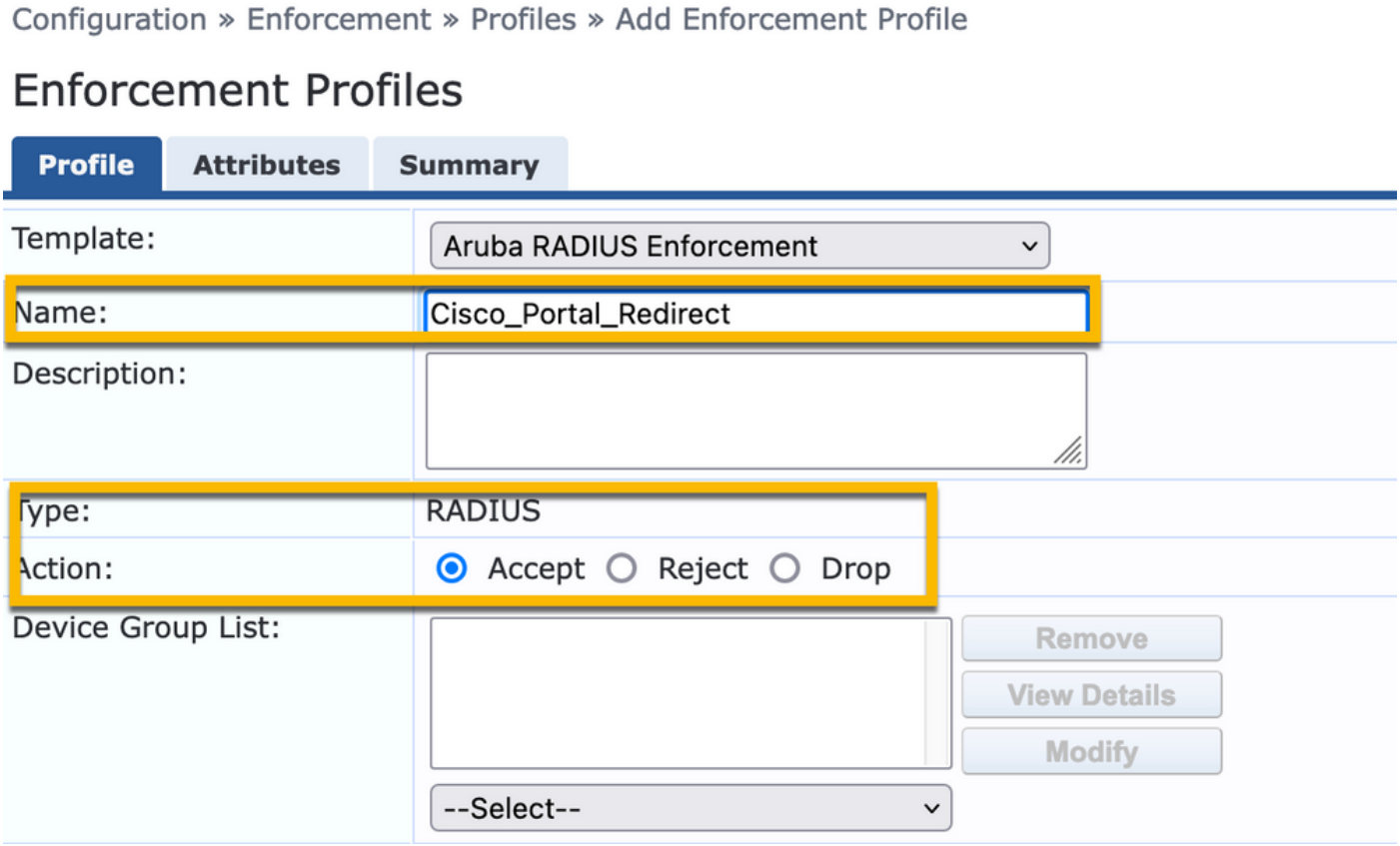
Le WLC 9800 redirige alors le client invité vers le portail invité CPPM pour l'authentification externe.

Accédez àClearPass > Enforcement > Profiles > Add.

- Nom : Cisco_Portal_Redirect

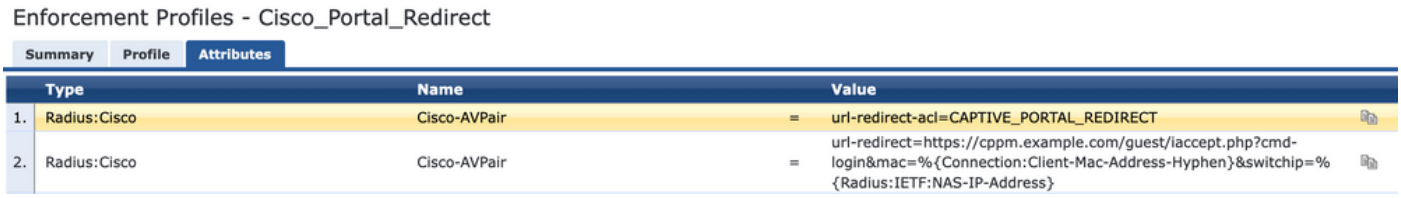
- Type : RADIUS

- Action : accepter



ClearPass Redirect Enforcement Profile

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



Attributs de profil de redirection ClearPass

L'attribut esturl-redirect-acldéfini surCAPTIVE-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.

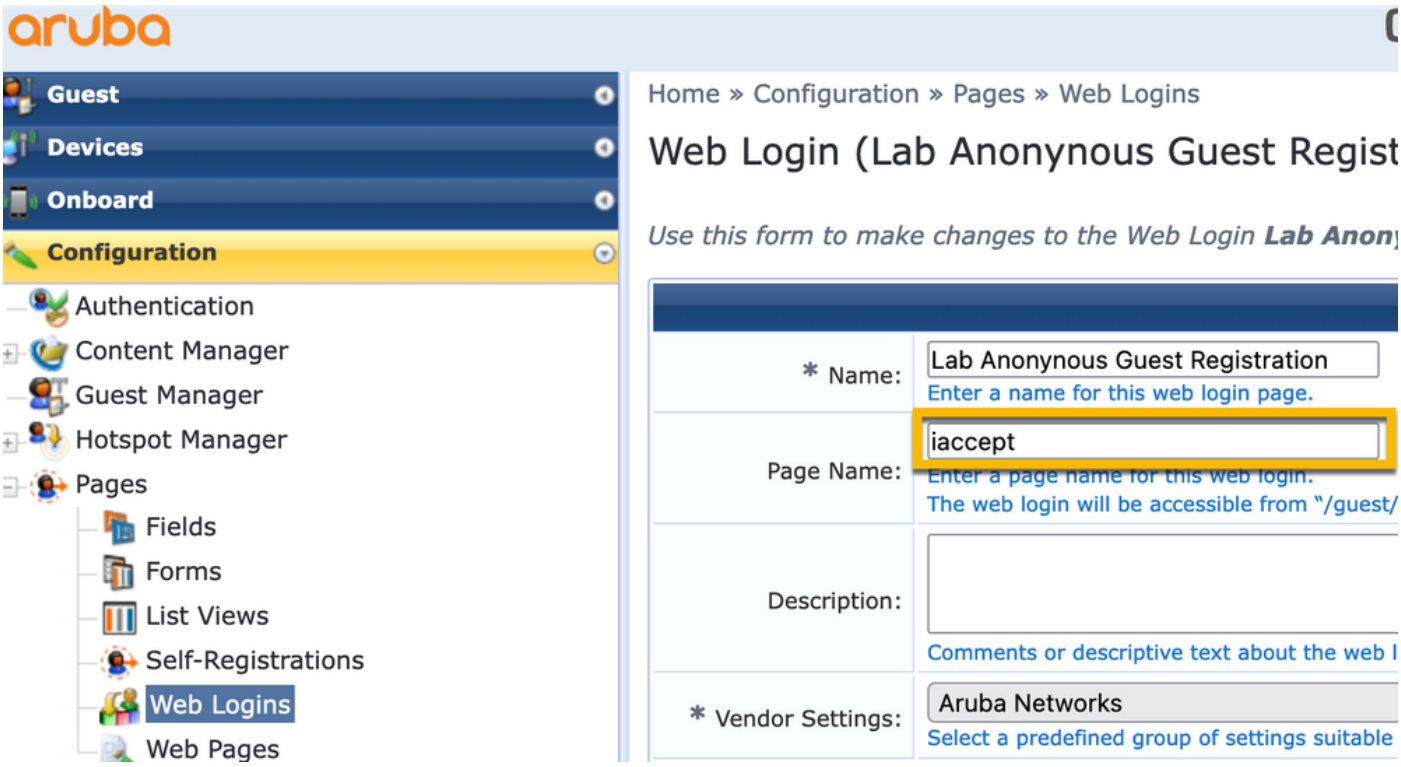
L'attributurl-redirectest composé de plusieurs paramètres :

- 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 àCPPM > Guest > Configuration > Pages > Web Logins > Edit.

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

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



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

Configuration du profil d'application des métadonnées ClearPass

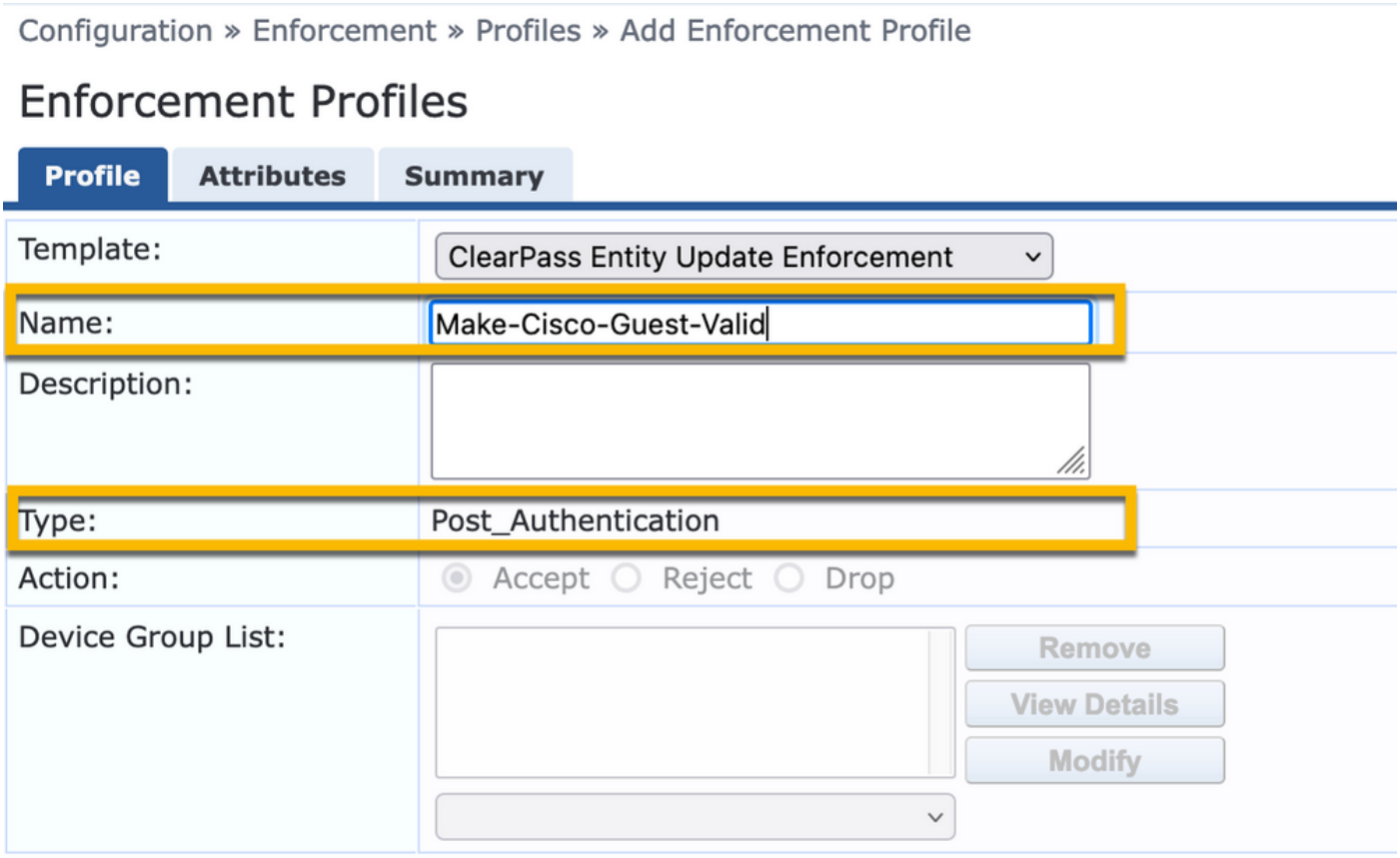
Configurez le profil d'application afin de mettre à jour l'attribut de métadonnées Endpoint qui est utilisé pour le suivi de la transition d'état par CPPM.

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 àClearPass > Enforcement > Profiles > Add.

- Modèle : Mise à jour des entités ClearPass

- Type : Post_Authentication



Dans la même boîte de dialogue, cliquez surAttributesl'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

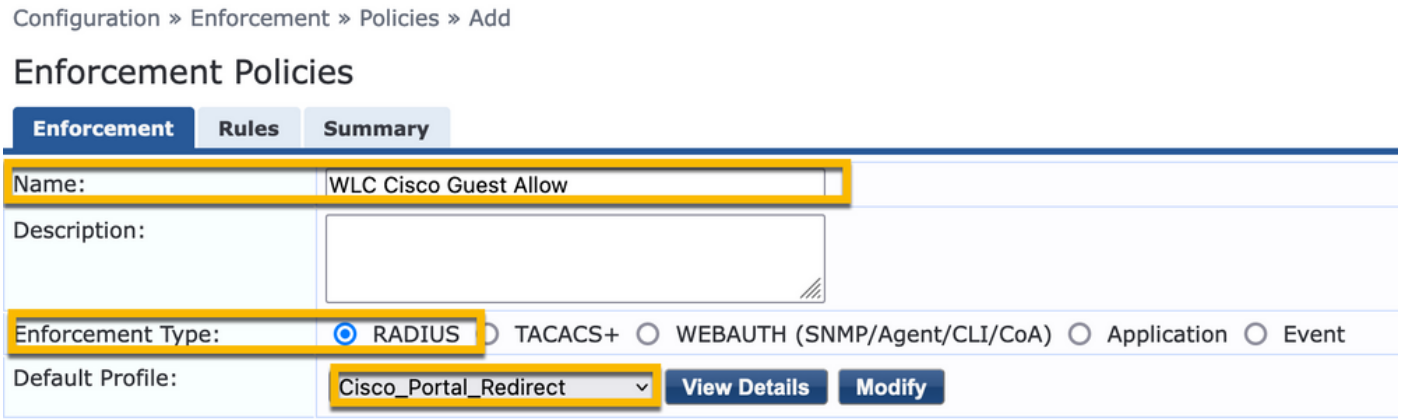
Configuration de la stratégie d'application ClearPass Guest Internet Access

Accédez àClearPass > Enforcement > Policies > Add.

- Nom : WLC Cisco Guest Allow

- Type d'application : RADIUS

- Profil par défaut : Cisco_Portal_Redirect



Dans la même boîte de dialogue, accédez à l'ongletRuleset cliquez surAdd Rule.

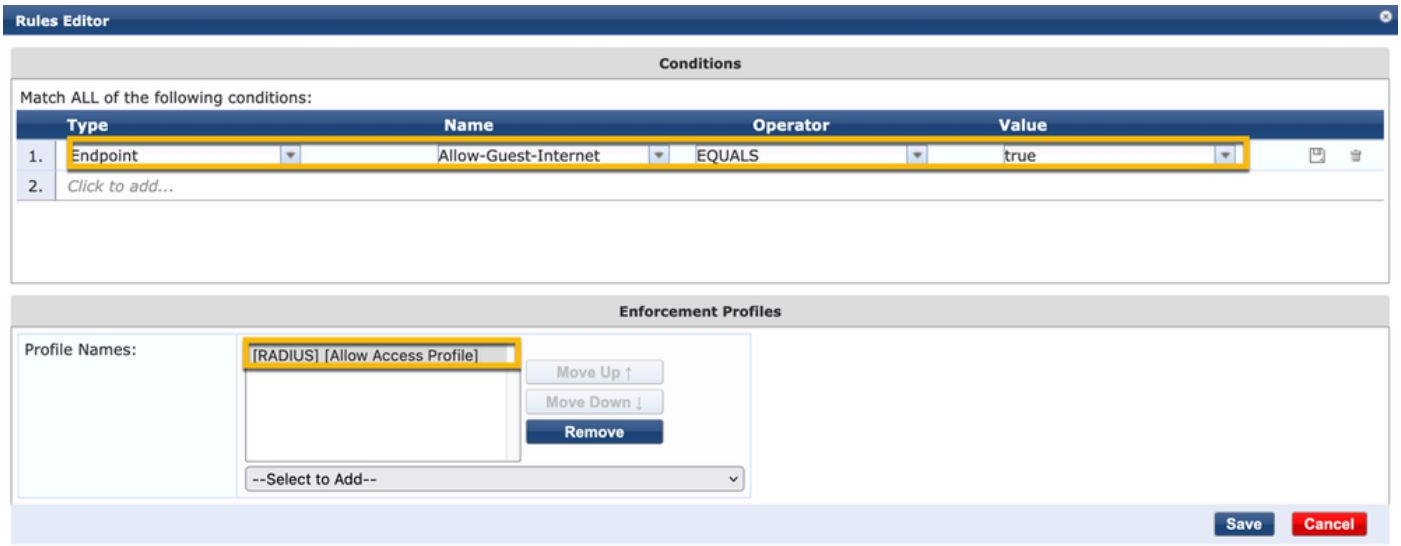
- Type : terminal

- Nom : Allow-Guest-Internet

- Opérateur : EQUALS

- Valeur Vrai

- Noms de profil / Choisir d'ajouter : [RADIUS] [Autoriser le profil d'accès]



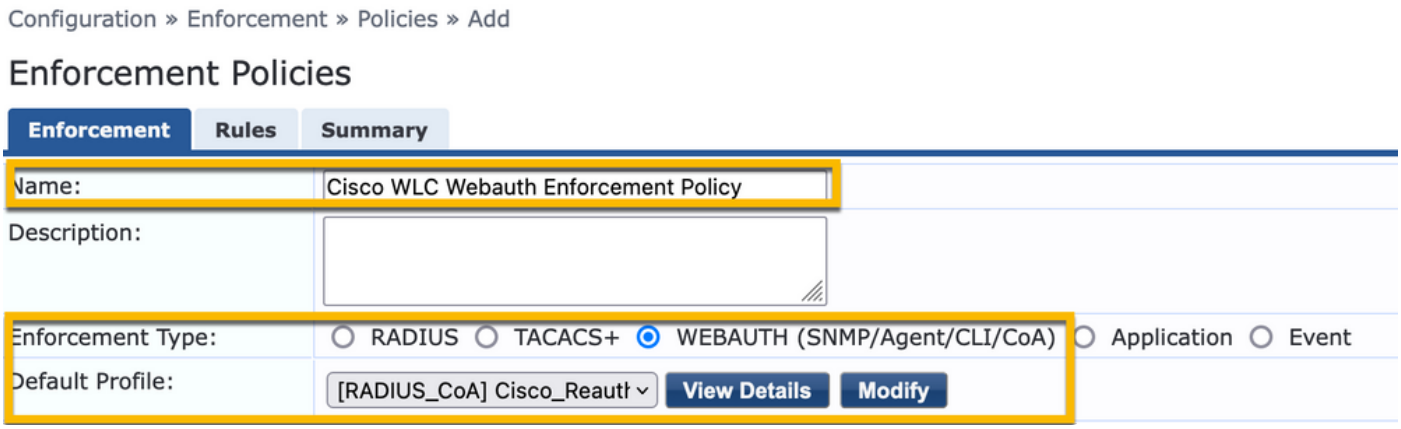
Configuration de la stratégie d'application ClearPass Guest Post-AUP

Accédez àClearPass > Enforcement > Policies > 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



Dans la même boîte de dialogue, accédez àRules > Add.

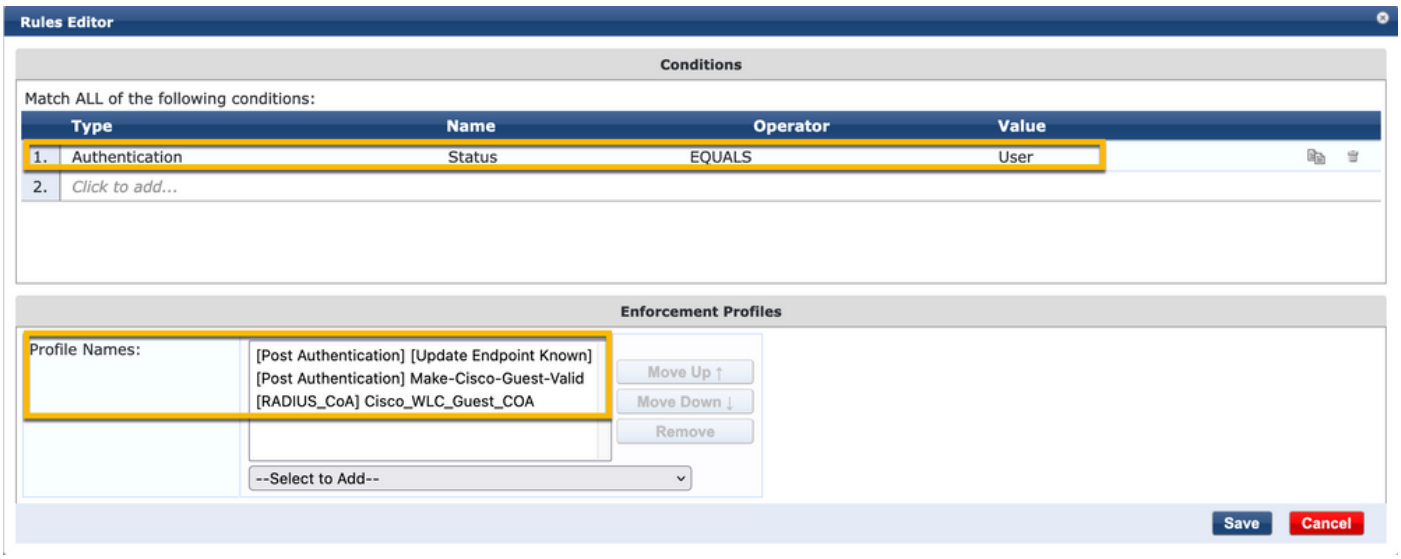
- Conditions : authentification

- 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]



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 àCPPM > Monitoring > Live Monitoring > Access Trackeret assurez-vous que l'entrée du journal RADIUS contient les détails de la société RADIUS.

- Sous9800 WLC, accédez àTroubleshooting > 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 àClearPass > 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 :

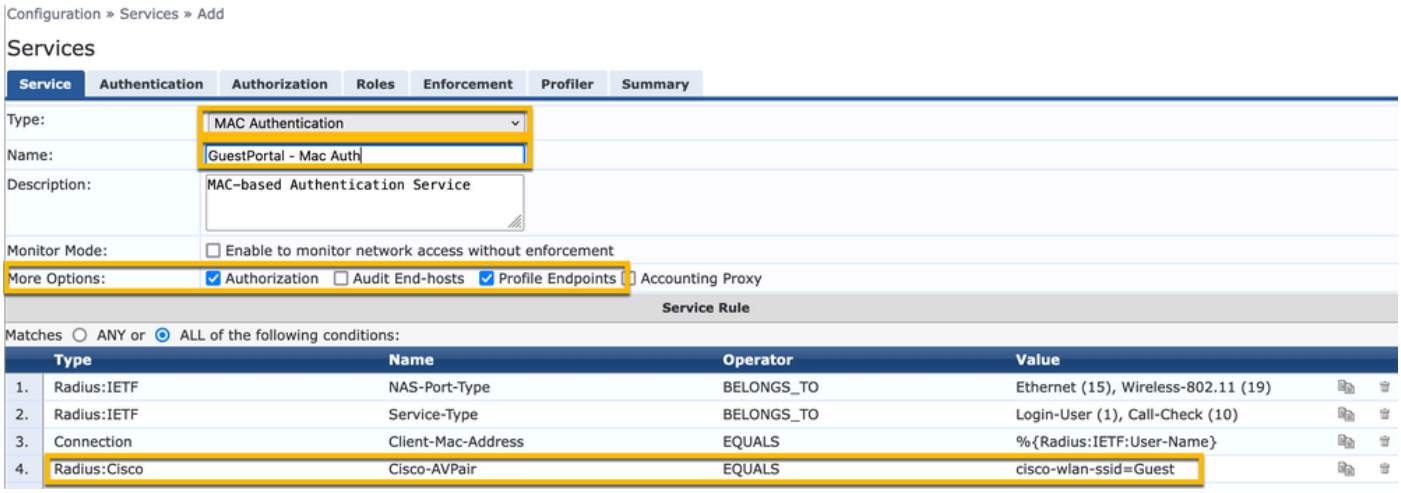
- Type : Rayon : Cisco

- Nom : Cisco-AVPair

- Opérateur : EQUALS

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

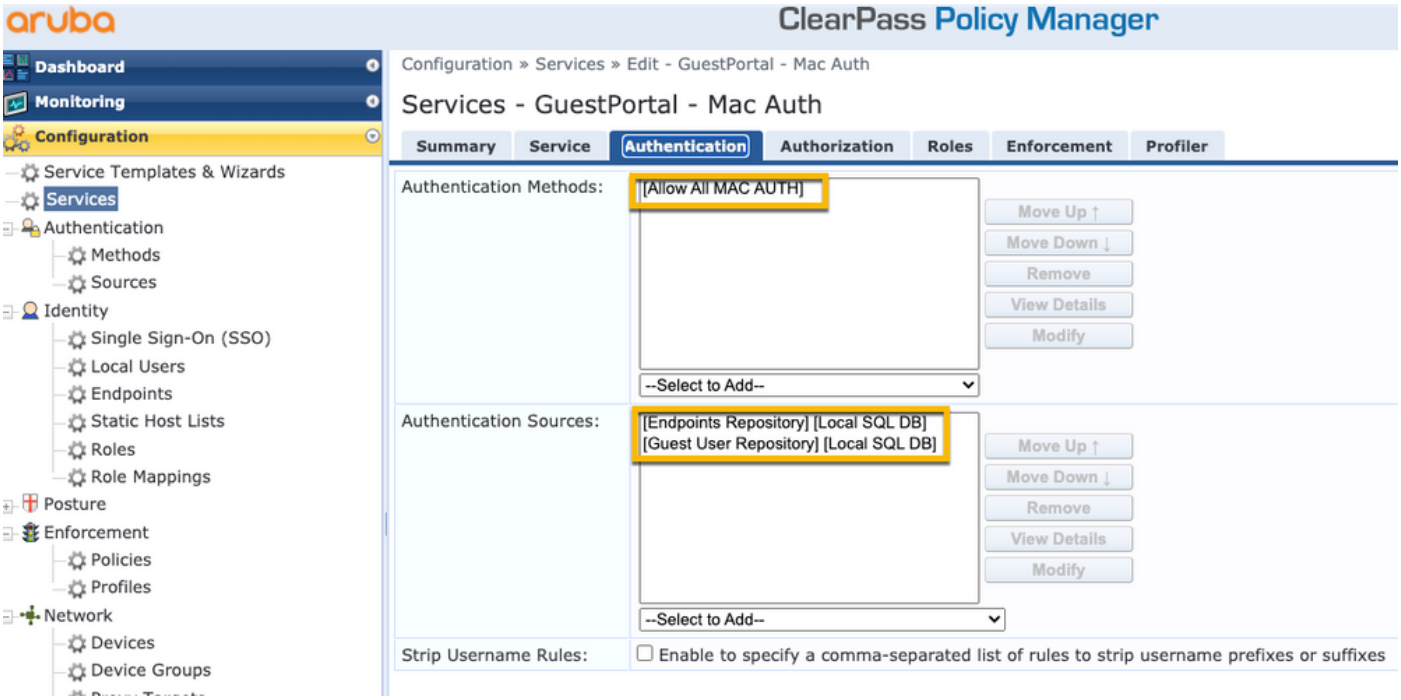
Remarque : « Guest » est le nom du SSID invité diffusé par le WLC 9800.



Dans la même boîte de dialogue, sélectionnez l'Authenticationonglet.

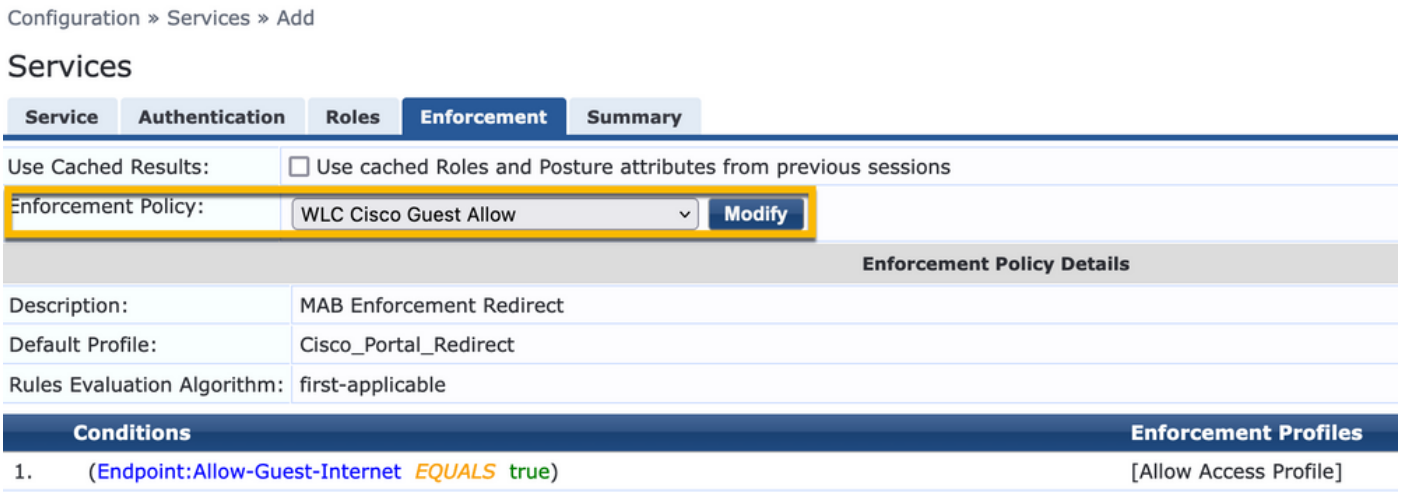
- Méthodes d'authentification : Remove [MAC AUTH], Add [Allow All MAC AUTH]

- Sources d'authentification : [Référentiel des points de terminaison][Base de données SQL locale], [Référentiel utilisateur invité][Base de données SQL locale]

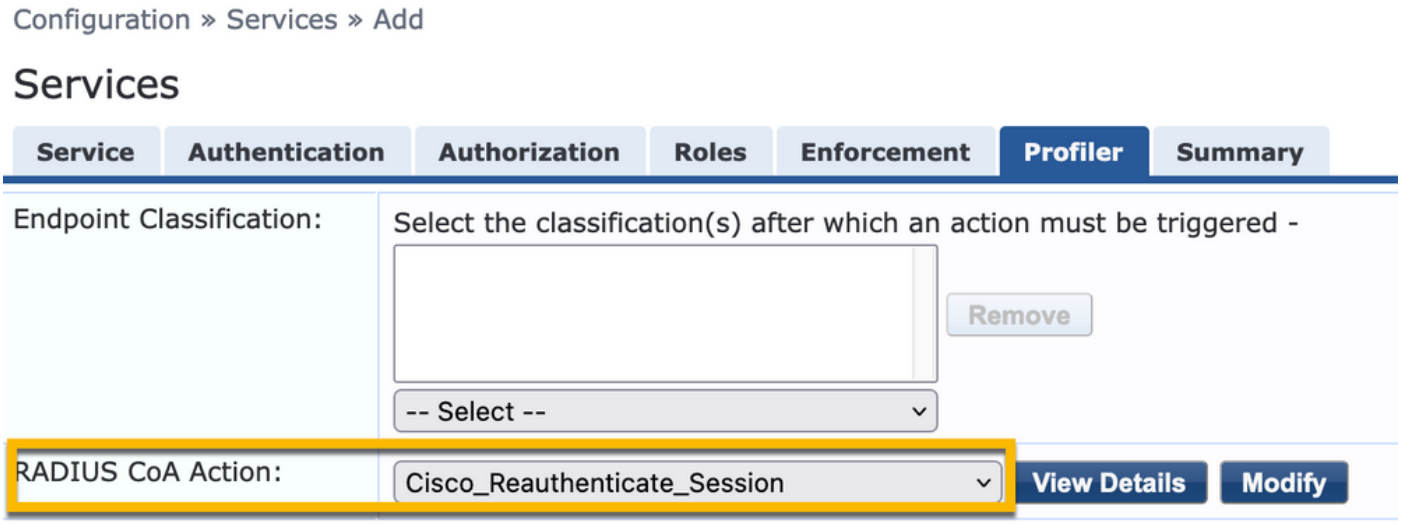


Dans la même boîte de dialogue, sélectionnez l'Enforcementonglet.

- Politique d'application : WLC Cisco Guest Allow



Dans la même boîte de dialogue, sélectionnez l'Enforcementonglet.

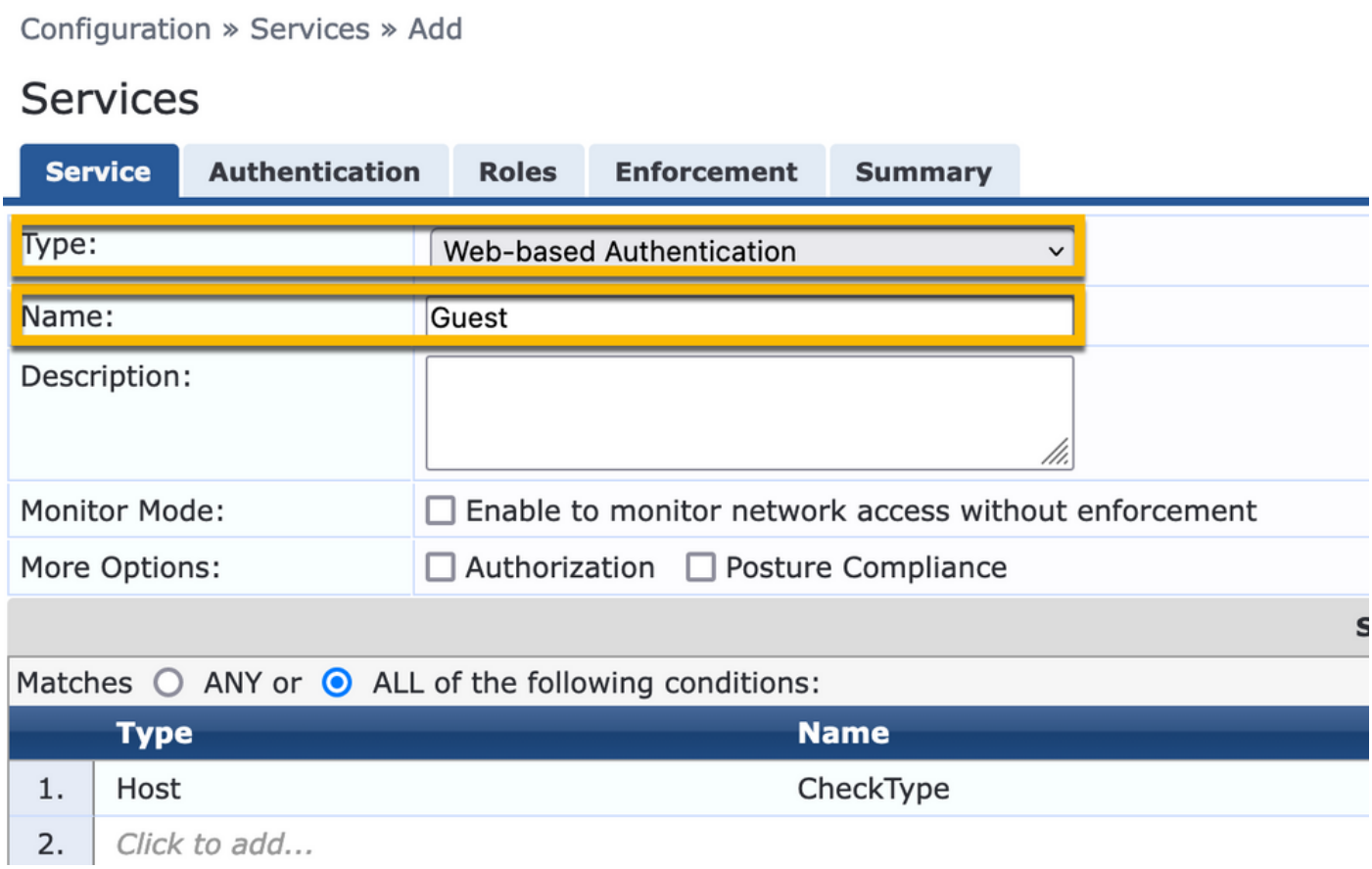


Configuration du service ClearPass Webauth

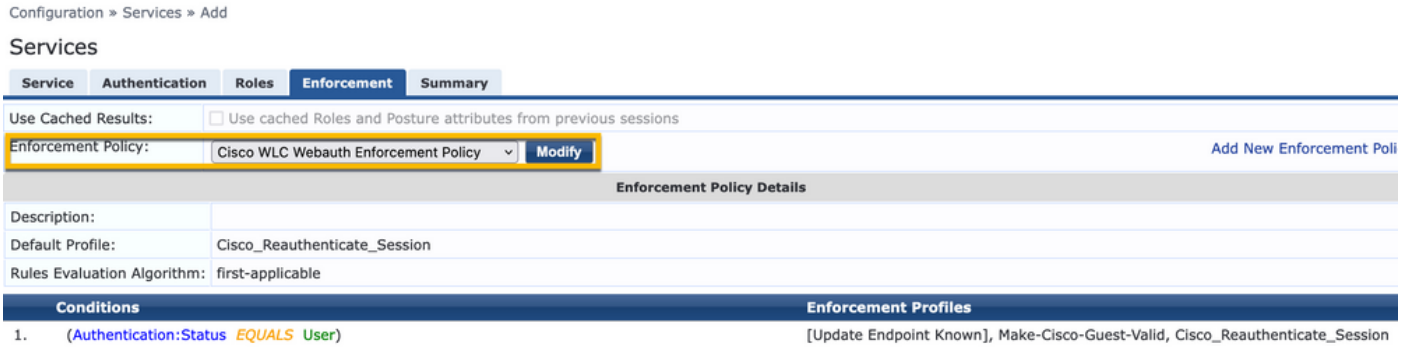
Accédez àClearPass > Enforcement > Policies > Add.

- Nom : Guest_Portal_Webauth

- Type : authentification basée sur le Web



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



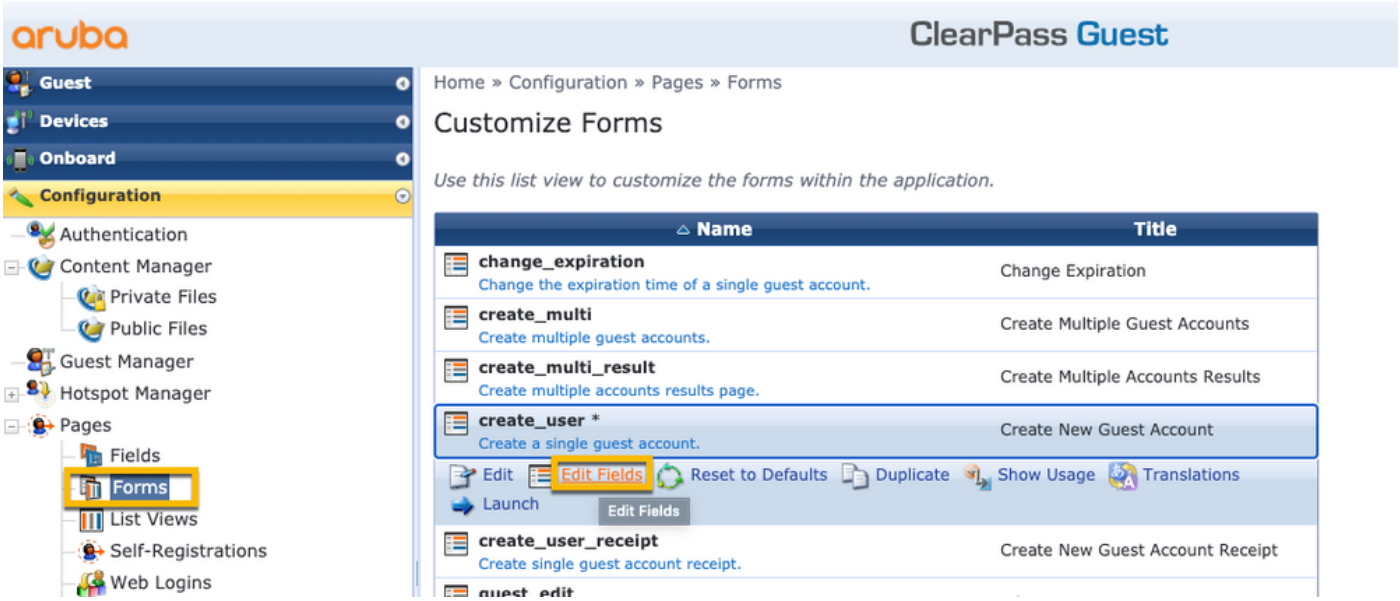
ClearPass - Connexion Web

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

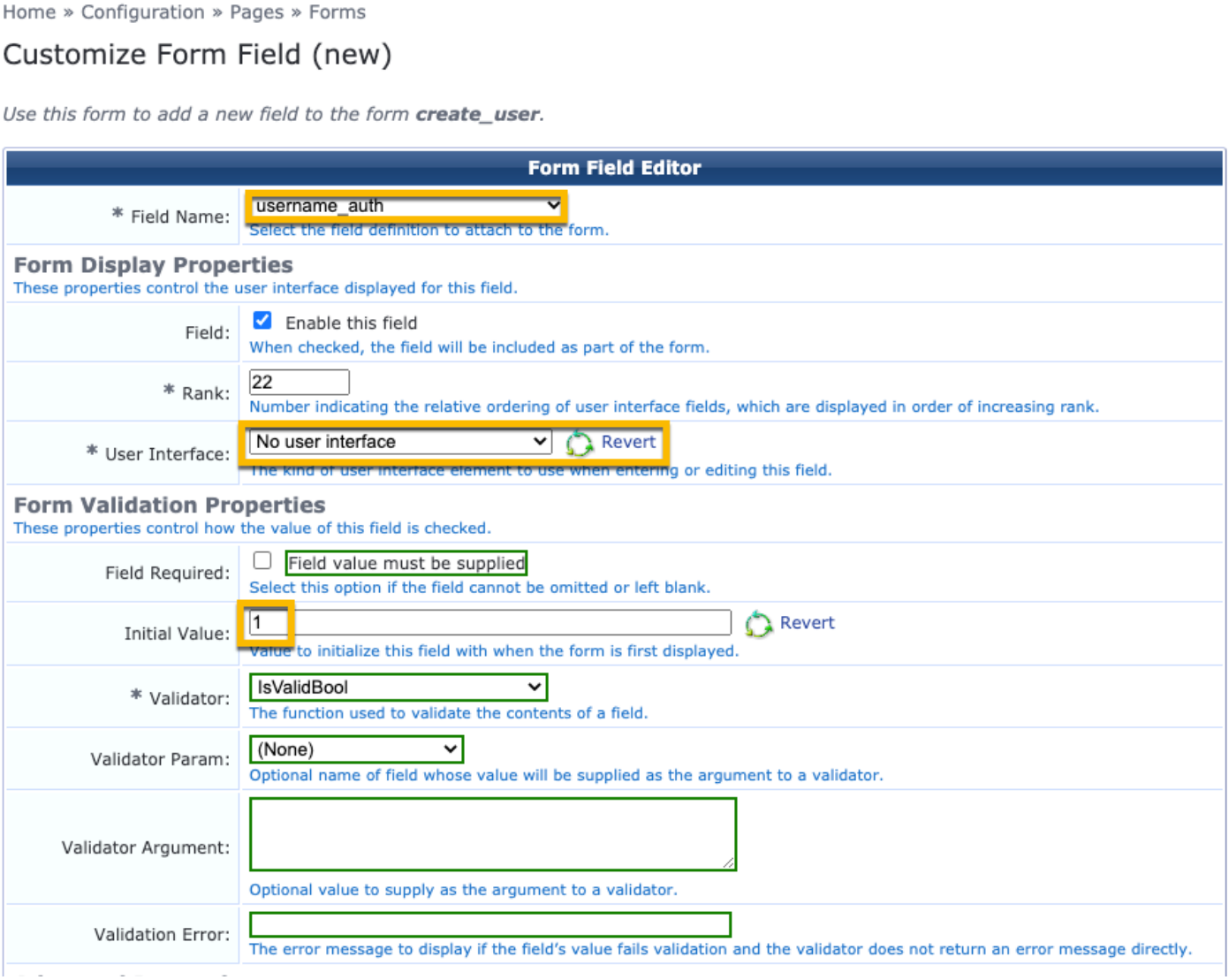
Les champs suivants doivent être définis/définis pour le nom d'utilisateur utilisé :

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 àClearPass > Guest > Configuration > Pages > Forms, puis sélectionnezcreate_userFormulaire.



Choisissezvisitor_name(ligne 20), puis cliquez surInsert After.



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

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

- Nom d'invité : GuestWiFi

- Nom de la société : Cisco

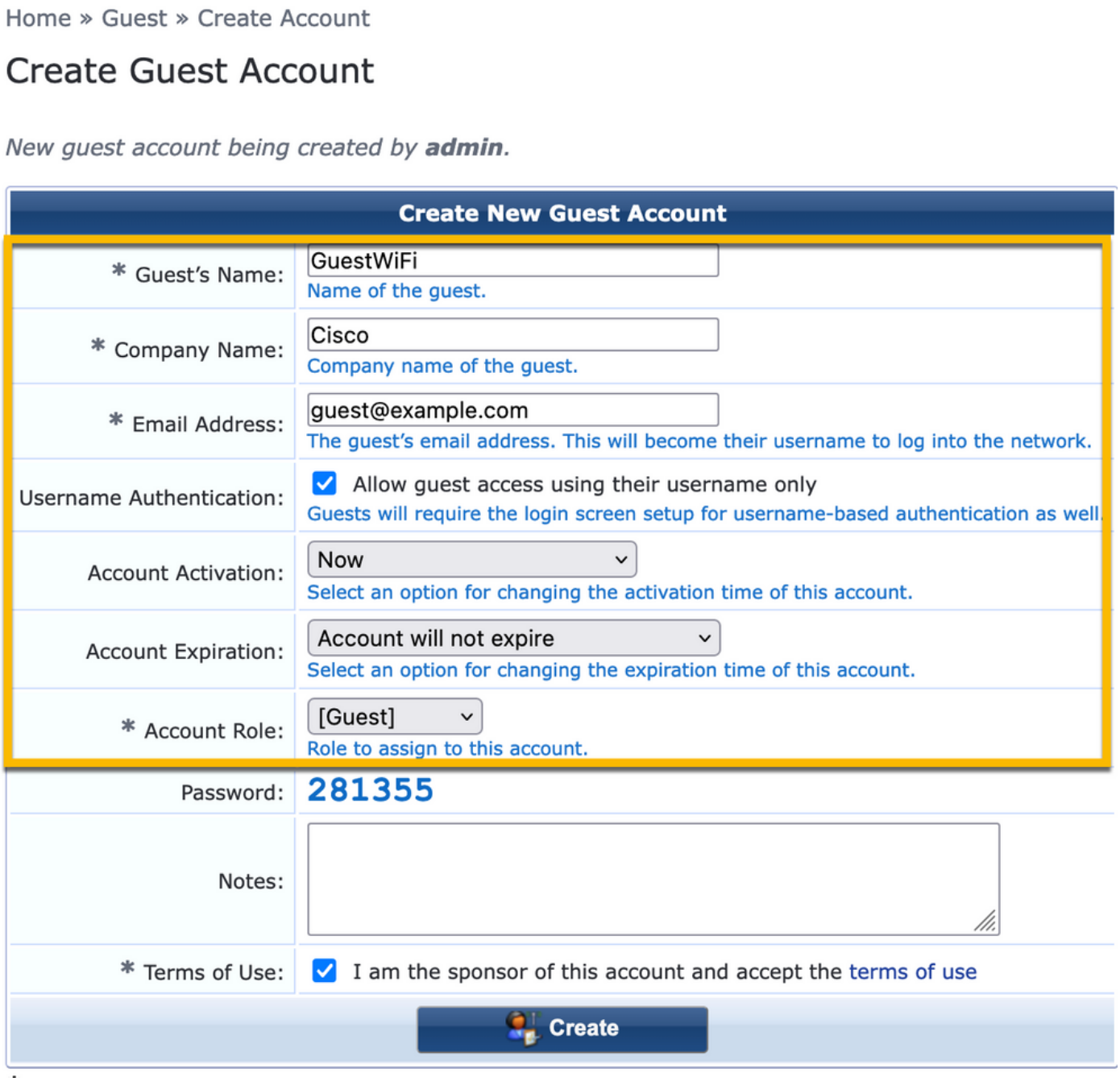
- Adresse électronique : guest@example.com

- 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



Créer un formulaire de connexion Web. Accédez àCPPM > 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
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 :

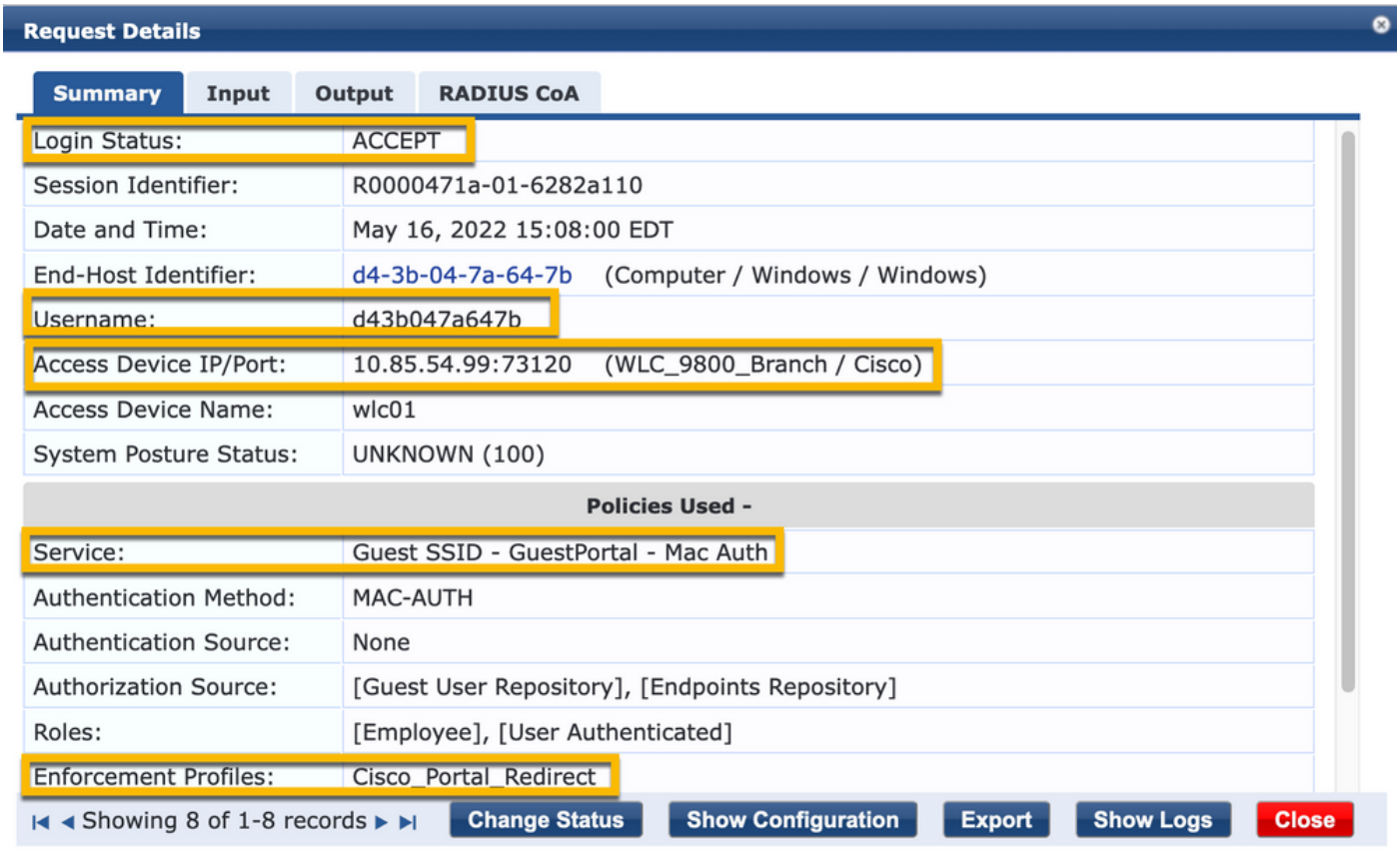
nom d'utilisateur | Nom d'utilisateur
nom_visiteur | Nom du visiteur
cn | Nom du visiteur
téléphone_visiteur | Téléphone du visiteur
email (courrier électronique) | Courriel
poste | Courriel
nom_sponsor | Nom du sponsor
e-mail_sponsor | E-mail du sponsor
Allow-Guest-Internet | vrai

Vérification - Autorisation CWA invité

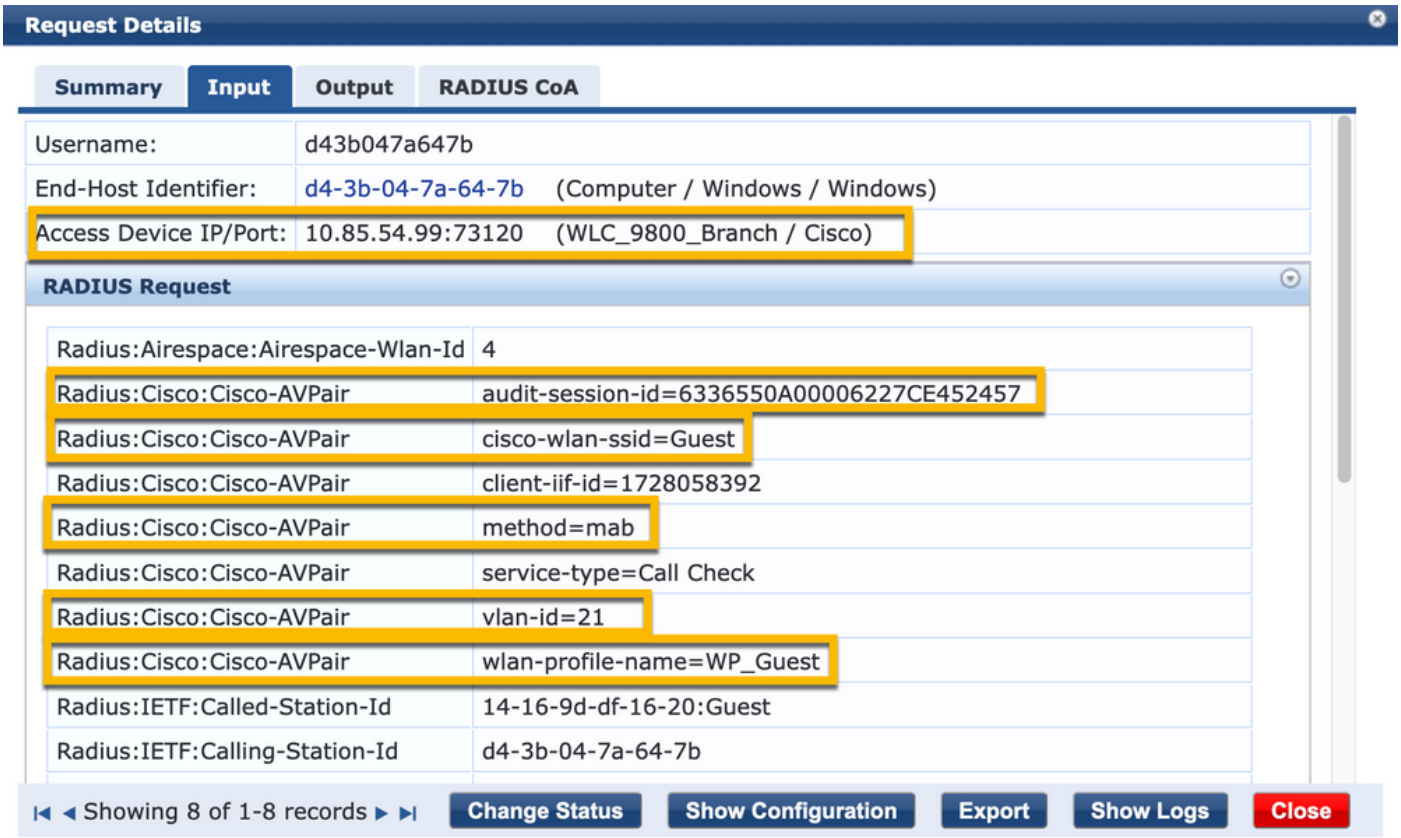
Dans le CPPM, accédez àLive Monitoring > Access Tracker.

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

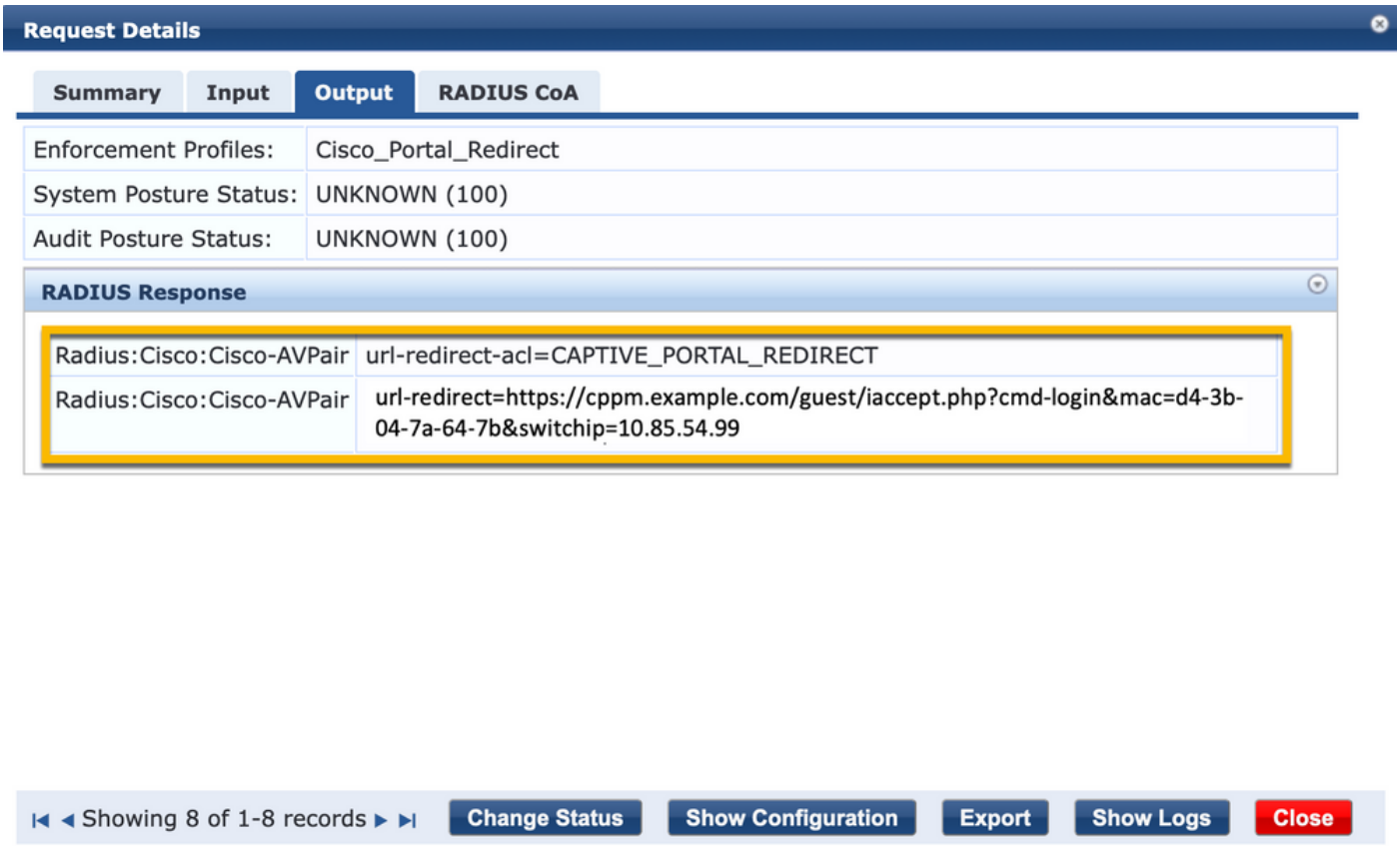
Onglet Résumé :



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



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



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.

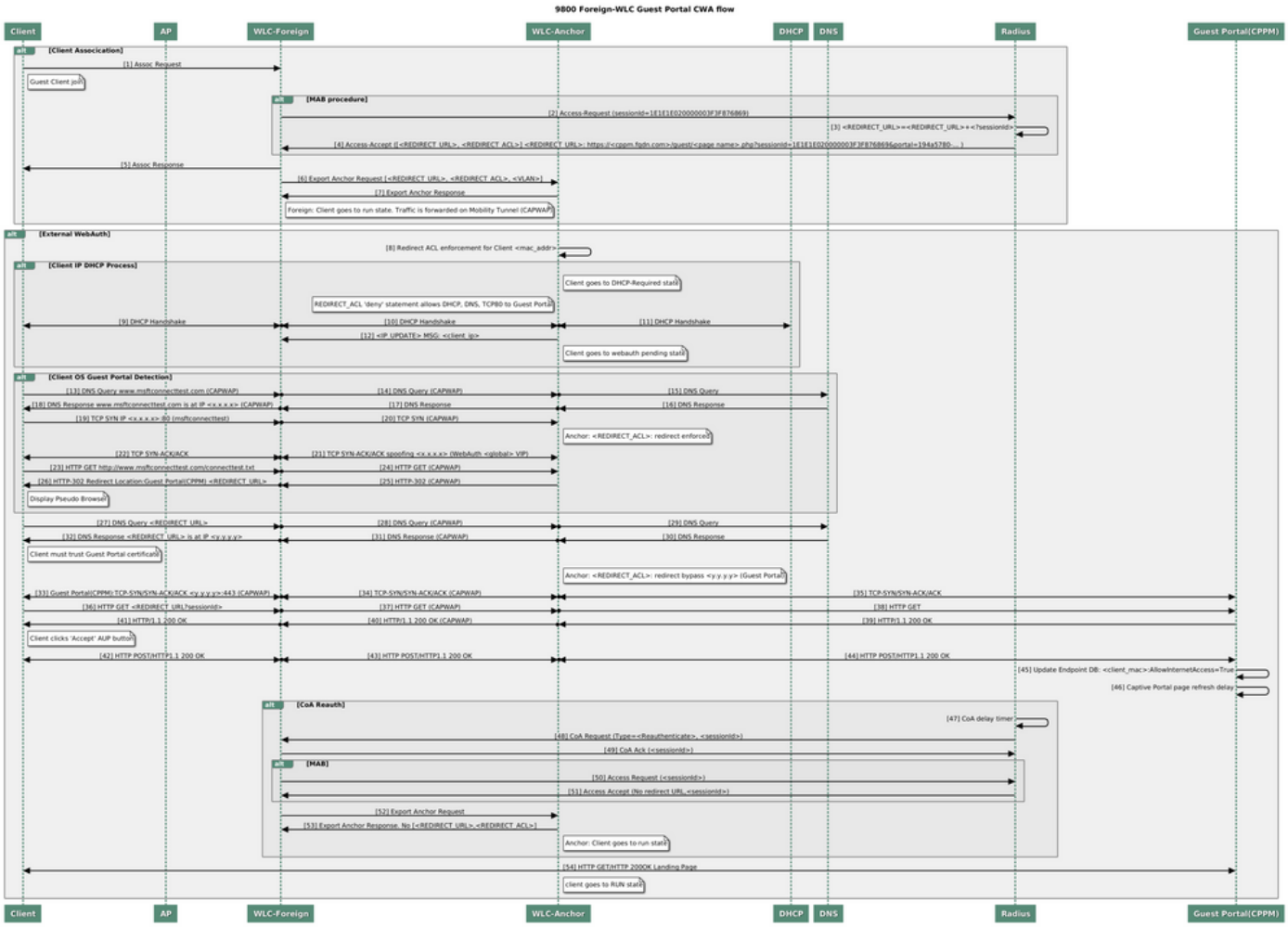


Diagramme d'état d'authentification Web Guest Central avec WLC d'ancrage

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.