

Configuration de l'intégration WLC du 9800 avec Aruba ClearPass - Déploiement de Dot1x & FlexConnect pour les filiales

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Flux de trafic](#)

[Diagramme du réseau](#)

[Configuration du contrôleur sans fil Catalyst 9800](#)

[C9800 - Configuration des paramètres AAA pour dot1x](#)

[C9800 - Configuration du profil WLAN « Corp »](#)

[C9800 - Configuration du profil de stratégie](#)

[C9800 - Configurer la balise de stratégie](#)

[C9800 - AP JoinProfile](#)

[C9800 - FlexProfile](#)

[C9800 - Étiquette de site](#)

[C9800 - Étiquette RF](#)

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

[Configurer Aruba CPPM](#)

[Configuration initiale du serveur Aruba ClearPass Policy Manager](#)

[Appliquer les licences](#)

[Ajout du contrôleur sans fil C9800 en tant que périphérique réseau](#)

[Configurer CPPM pour utiliser Windows AD comme source d'authentification](#)

[Configuration du service d'authentification Dot1X CPPM](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit l'intégration du contrôleur sans fil Catalyst 9800 avec Aruba ClearPass Policy Manager.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de ces rubriques et qu'elles aient été configurées et vérifiées :

- Contrôleur sans fil Catalyst 9800
- Serveur Aruba ClearPass (nécessite une licence de plate-forme, une licence d'accès, une licence embarquée)
- Windows AD opérationnel
- Autorité de certification (CA) facultative
- Serveur DHCP opérationnel
- Serveur DNS opérationnel (requis pour la validation de la liste de révocation de certificats)
- ESXi
- Tous les composants pertinents sont synchronisés sur NTP et vérifiés pour avoir l'heure correcte (requis pour la validation du certificat)
- Connaissance des sujets :
 - Déploiement du C9800 et nouveau modèle de configuration
 - Fonctionnement de FlexConnect sur C9800
 - Authentification Dot1x

Composants utilisés

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

- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 points d'accès
- Aruba ClearPass, correctif 6-8-0-109592 et 6.8-3
- Serveur MS Windows
 - Active Directory (GP configuré pour l'émission automatique de certificats basés sur une machine vers les terminaux gérés)
 - Serveur DHCP avec option 43 et option 60
 - Serveur DNS
 - Serveur NTP pour synchroniser tous les composants
 - AC

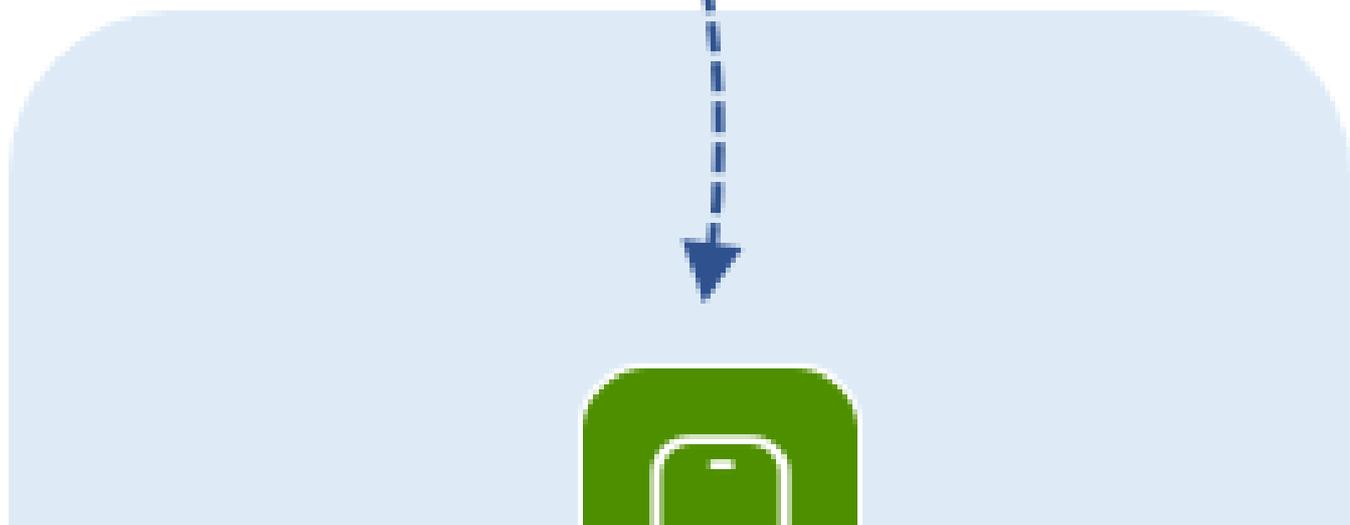
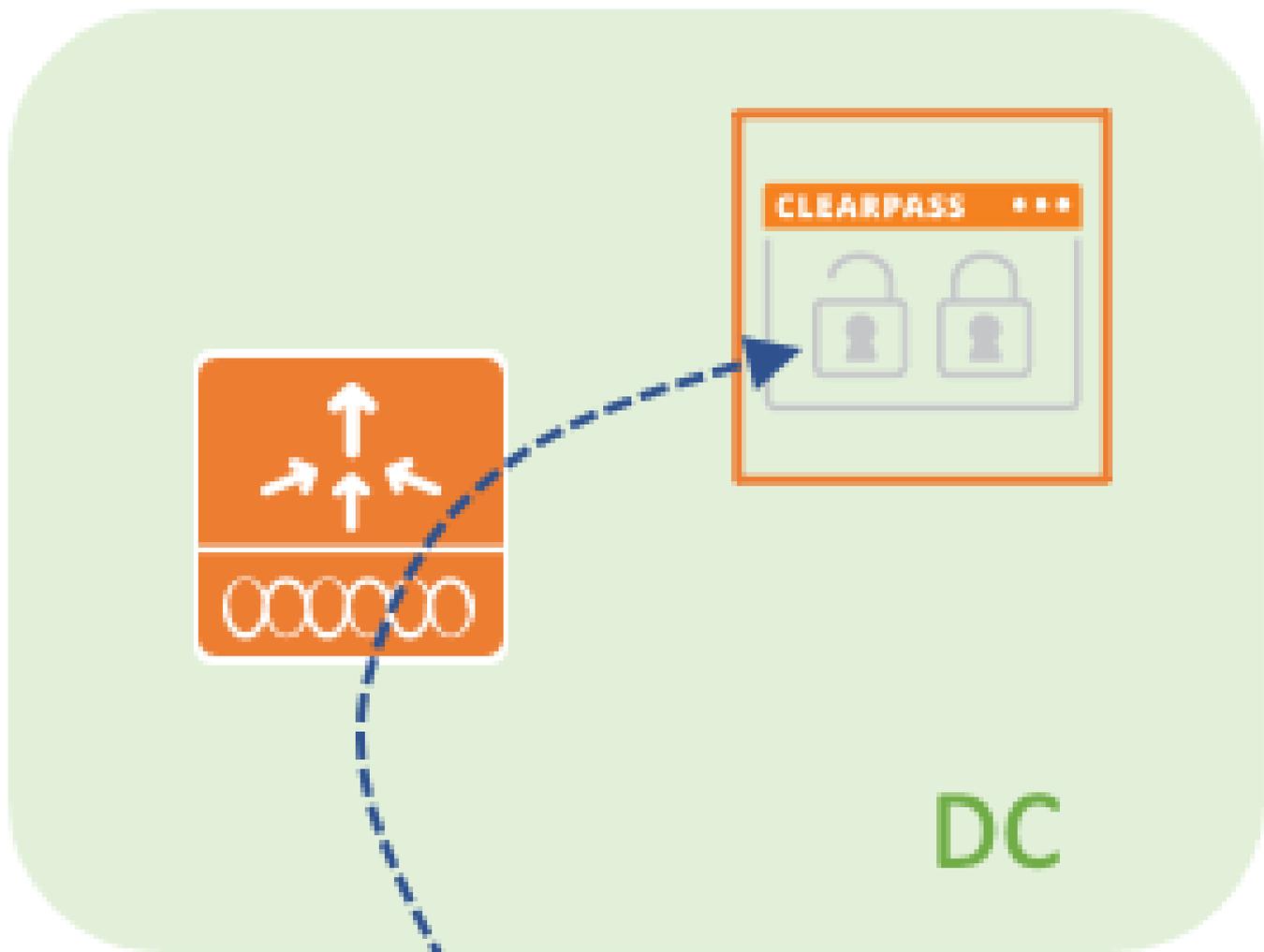
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Flux de trafic

Dans un déploiement d'entreprise type avec plusieurs filiales, chaque filiale est configurée pour fournir un accès point1x aux employés de l'entreprise. Dans cet exemple de configuration, PEAP

est utilisé pour fournir un accès dot1x aux utilisateurs de l'entreprise via une instance ClearPass déployée dans le data center central (DC). Les certificats d'ordinateur sont utilisés conjointement avec la vérification des informations d'identification des employés par rapport à un serveur Microsoft AD.



entrez le nom du groupe de serveurs RADIUS et attribuez les informations du serveur RADIUS. Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

Create AAA Radius Server Group [X]

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers: CPPM_Guest

Assigned Servers: CPPM_Corp

[Cancel] [Apply to Device]

Étape 3. Définissez la liste de méthodes d'authentification dot1x pour les utilisateurs d'entreprise. Accédez à Configuration > Security > AAA > AAA Method List > Authentication et cliquez sur +Add. Sélectionnez Type dot1x dans le menu déroulant. Cliquez sur le bouton Apply to Device comme illustré dans cette image.

Quick Setup: AAA Authentication

Method List Name*

Dot1X_Authentication

Type*

dot1x

Group Type

group

Fallback to local

Available Server Groups

radius
ldap
tacacs+
WLC_Tacacs_Servers
AAA_Group_Guest

Assigned Server Groups

AAA_Group_Corp

Cancel

Apply to Device

C9800 - Configuration du profil WLAN « Corp »

Étape 1. Accédez à Configuration > Tags & Profiles > Wireless et cliquez sur +Add. Entrez un nom de profil, le SSID « Corp » et un ID WLAN qui n'est pas déjà utilisé.

Add WLAN

General

Security

Advanced

Profile Name*

WP_Corp

Radio Policy

All

SSID*

Corp

Broadcast SSID

ENABLED

WLAN ID*

3

Status

ENABLED

Cancel

Apply to Device

Étape 2. Accédez à l'onglet Security et au sous-onglet Layer2. Il est inutile de modifier les paramètres par défaut de cet exemple de configuration.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Étape 3. Accédez au sous-onglet AAA et sélectionnez la liste de méthodes d'authentification configurée précédemment. Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List Dot1X_Authenticatio ⓘ

Local EAP Authentication

↶ Cancel Apply to Device

C9800 - Configuration du profil de stratégie

Étape 1. Accédez à Configuration > Tags & Profiles > Policy et cliquez sur +Add et entrez un nom et une description de profil de stratégie. Activez la stratégie et désactivez la commutation centrale, le protocole DHCP et l'association, car le trafic utilisateur de l'entreprise est commuté localement au niveau du point d'accès, comme illustré dans l'image.

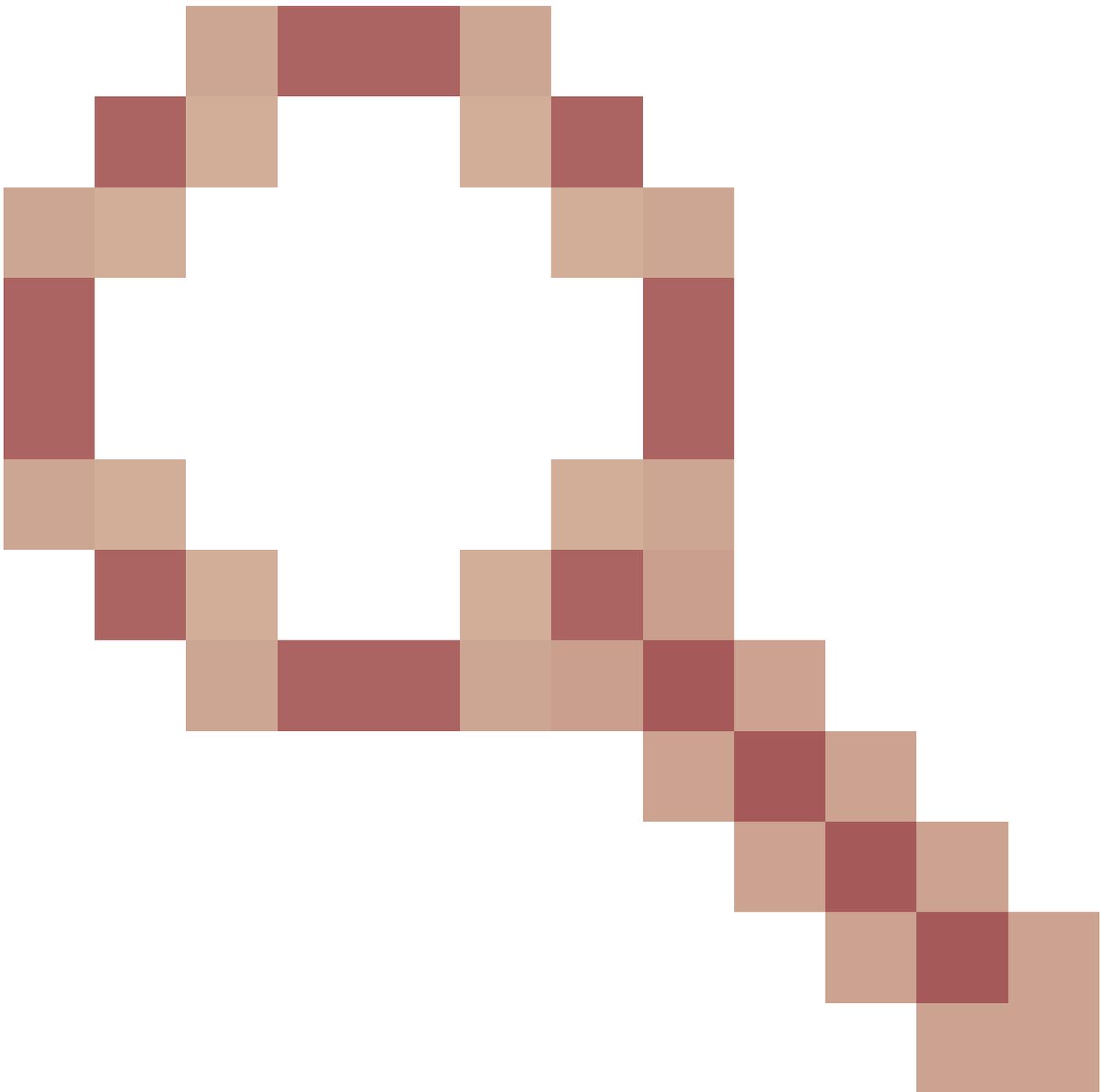
Add Policy Profile



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

Étape 2. Accédez à l'onglet Access Policies et saisissez manuellement l'ID du VLAN à utiliser au niveau de la filiale pour le trafic utilisateur de l'entreprise. Ce VLAN n'a pas besoin d'être configuré sur le C9800 lui-même. Il doit être configuré dans le profil flexible, comme détaillé plus loin. Ne sélectionnez pas de nom de VLAN dans la liste déroulante (consultez l'ID de bogue Cisco [CSCvn48234](https://www.cisco.com/c/en_US/bugtools/bugsearch.html?bugid=CSCvn48234))



pour plus d'informations). Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Cancel

Apply to Device

C9800 - Configurer la balise de stratégie

Une fois le profil WLAN (WP_Corp) et le profil de stratégie (PP_Corp) créés, une balise de stratégie doit à son tour être créée pour lier ces profils WLAN et de stratégie. Cette balise de stratégie est appliquée aux points d'accès. Attribuez cette balise de stratégie aux points d'accès pour déclencher la configuration de ceux-ci afin d'activer les SSID sélectionnés sur ceux-ci.

Étape 1. Accédez à Configuration > Tags & Profiles > Tags, sélectionnez l'onglet Policy et cliquez sur +Add. Saisissez le nom et la description de la balise de stratégie. Cliquez sur +Add sous WLAN-POLICY Maps. Sélectionnez le profil WLAN et le profil de stratégie créés précédemment, puis cliquez sur le bouton de coche comme illustré dans cette image.

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 0**

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile*

Policy Profile*

➤ **RLAN-POLICY Maps: 0**

Étape 2. Vérifiez et cliquez sur le bouton Apply to Device comme illustré dans cette image.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WP_Corp	PP_Corp

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

➤ RLAN-POLICY Maps: 0

C9800 - Profil de jonction AP

Les profils de jointure AP et les profils flexibles doivent être configurés et attribués aux points d'accès avec des balises de site. Une balise de site différente doit être utilisée pour chaque branche afin de prendre en charge la transition rapide 802.11r (FT) au sein d'une branche, tout en limitant la distribution de la PMK client parmi les AP de cette branche uniquement. Il est important de ne pas réutiliser la même balise de site dans plusieurs filiales. Configurez un profil de jonction AP. Vous pouvez utiliser un seul profil de jointure AP si toutes les branches sont similaires, ou créer plusieurs profils si certains des paramètres configurés doivent être différents.

Étape 1. Accédez à Configuration > Tags & Profiles > AP Join et cliquez sur +Add. Saisissez le nom et la description du profil de connexion AP. Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

Add AP Join Profile ✕

General Client CAPWAP AP Management Security ICap QoS

Name*	<input type="text" value="APJP_Branch"/>	OfficeExtend AP Configuration	
Description	<input type="text" value="Profiles for branches"/>	Local Access	<input checked="" type="checkbox"/>
LED State	<input checked="" type="checkbox"/>	Link Encryption	<input checked="" type="checkbox"/>
LAG Mode	<input type="checkbox"/>	Rogue Detection	<input type="checkbox"/>
NTP Server	<input type="text" value="0.0.0.0"/>		
GAS AP Rate Limit	<input type="checkbox"/>		
Apphost	<input type="checkbox"/>		

C9800 - Profil flexible

Configurez maintenant un profil flexible. Là encore, vous pouvez utiliser un profil unique pour toutes les branches si celles-ci sont similaires et ont le même mappage VLAN/SSID. Vous pouvez également créer plusieurs profils si certains des paramètres configurés, tels que les affectations de VLAN, sont différents.

Étape 1. Accédez à Configuration > Tags & Profiles > Flex et cliquez sur +Add. Saisissez le nom et la description du profil paramétrable.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name*	<input type="text" value="FP_Branch"/>	Fallback Radio Shut	<input type="checkbox"/>
Description	<input type="text" value="Flex Profile for branches"/>	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	<input type="text" value="1"/>	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	<input type="text" value="0"/>	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	<input type="text" value="0.0.0.0"/>	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	<input type="text" value="Search or Select"/>
CTS Profile Name	<input type="text" value="default-sxp-profile ✕"/>		

Étape 2. Accédez à l'onglet VLAN et cliquez sur +Add. Entrez le nom et l'ID du VLAN local au niveau de la branche que le point d'accès doit utiliser pour commuter localement le trafic utilisateur de l'entreprise. Cliquez sur le bouton Save comme illustré dans cette image.

The screenshot shows the 'Add Flex Profile' dialog box with the 'VLAN' tab selected. The 'Add' button is highlighted. A form is open with the following fields: 'VLAN Name*' containing 'CorpData', 'VLAN Id*' containing '2', and 'ACL Name' set to 'Select ACL'. The 'Save' button is highlighted.

Étape 3. Vérifiez et cliquez sur le bouton Apply to Device comme illustré dans cette image.

The screenshot shows the 'Add Flex Profile' dialog box with the 'VLAN' tab selected. The 'Add' button is highlighted. A table lists the VLAN configuration:

VLAN Name	ID	ACL Name
CorpData	2	

The 'Apply to Device' button is highlighted.

C9800 - Étiquette de site

Les balises de site permettent d'attribuer des profils de jointure et des profils flexibles aux points d'accès. Comme mentionné précédemment, une balise de site différente doit être utilisée pour chaque branche afin de prendre en charge la transition rapide 802.11r (FT) au sein d'une branche, tout en limitant la distribution du PMK client parmi les AP de cette branche uniquement. Il est important de ne pas réutiliser la même balise de site dans plusieurs filiales.

Étape 1. Accédez à Configuration > Tags & Profiles > Tags, sélectionnez l'onglet Site et cliquez sur +Add. Entrez un nom et une description de balise de site, sélectionnez le profil de connexion AP créé, décochez la case Enable Local Site, et enfin sélectionnez le profil flexible créé précédemment. Décochez la case Enable Local Site pour changer le point d'accès de Local Mode à FlexConnect. Enfin, cliquez sur le bouton Apply to Device comme illustré dans cette image.

Add Site Tag ✕

Name*

Description

AP Join Profile ▼

Flex Profile ▼

Fabric Control Plane Name

Enable Local Site

C9800 - Étiquette RF

Étape 1. Accédez à Configuration > Tags & Profiles > Tags, sélectionnez l'onglet RF et cliquez sur +Add. Entrez un nom et une description pour l'étiquette RF. Sélectionnez les profils RF définis par le système dans le menu déroulant. Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile ▼

2.4 GHz Band RF Profile ▼

C9800 - Attribuer des balises au point d'accès

Maintenant que les balises sont créées et incluent les différentes stratégies et profils requis pour configurer les points d'accès, nous devons les attribuer aux points d'accès. Cette section explique comment exécuter manuellement une balise statique attribuée à un point d'accès, en fonction de son adresse MAC Ethernet. Pour les environnements de production de produits, il est recommandé d'utiliser le workflow Cisco DNA Center AP PNP ou d'utiliser une méthode de téléchargement CSV statique en masse disponible dans le modèle 9800.

Étape 1. Accédez à Configure > Tags & Profiles > Tags, sélectionnez l'onglet AP, puis l'onglet Static. Cliquez sur +Add et entrez l'adresse MAC du point d'accès, puis sélectionnez la balise de

stratégie, la balise de site et la balise RF précédemment définies. Cliquez sur le bouton Apply to Device (Appliquer au périphérique) comme illustré dans cette image.

Associate Tags to AP

AP MAC Address* 380e.4dbf.589a

Policy Tag Name PT_Branch

Site Tag Name ST_Branch_01

RF Tag Name RFT_Branch

Cancel

Apply to Device

Configurer Aruba CPPM

Configuration initiale du serveur Aruba ClearPass Policy Manager

Aruba clearpass est déployé via le modèle OVF sur le serveur ESXi avec ces ressources :

- 2 CPU 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)

Appliquer les licences

Appliquez la licence de la plate-forme via : Administration > Server Manager > Licensing. Ajout d'accès et intégration

Ajout du contrôleur sans fil C9800 en tant que périphérique réseau

Accédez à Configuration > Network > Devices > Add comme indiqué dans cette image.

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: >WLC-10.85.54.99

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: LAB WLC 9800

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

Enable RADIUS Dynamic Authorization: Port: 1700

Enable RadSec:

Copy Save Cancel

Configurer CPPM pour utiliser Windows AD comme source d'authentification

Accédez à Configuration > Authentication > Sources > Add. Sélectionnez Type : Active Directory dans le menu déroulant comme illustré dans cette image.

aruba ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General | Primary | Attributes | Summary

Name: LAB_AD

Description:

Type: Active Directory

Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources:

-- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority:

Add Backup Remove

Configurer le service d'authentification CPPM Dot1X

Étape 1. Créez un « service » correspondant à plusieurs attributs RADIUS :

- Rayon: IETF | Nom : NAS-IP-Address | ÉGAL | <ADRESSE IP>

- Rayon:IETF | Nom : Service-Type | ÉGAL | 1,2,8

Étape 2. Pour la production, il est recommandé de faire correspondre un nom SSID au lieu de 'NAS-IP-Address' afin qu'une condition suffise dans un déploiement multi-WLC. Rayon:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID

The screenshot shows the 'Services - DOT1X' configuration page in the 'Service' tab. The 'Name' is 'DOT1X' and the 'Description' is '802.1X Wireless Access Service'. The 'Type' is '802.1X Wireless' and the 'Status' is 'Enabled'. The 'Monitor Mode' is set to 'None'. The 'Service Rule' section is expanded to show 'Matches' set to 'ALL of the following conditions':

Type	Name	Operator	Value
Radius:IETF	NAS-IP-Address	EQUALS	10.85.54.99
Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Click to add...			

The screenshot shows the 'Services - DOT1X' configuration page in the 'Authentication' tab. The 'Authentication Methods' list includes EAP PEAP, EAP FAST, EAP TLS, and EAP TTLS. The 'Authentication Sources' list includes LAB_AD [Active Directory]. The 'Strip Username Rules' checkbox is unchecked, and the 'Service Certificate' dropdown is set to '--Select to Add--'.

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il est important de noter que le WLC 9800 n'utilise pas de manière fiable le même port source

UDP pour une transaction RADIUS de client sans fil donnée. C'est quelque chose ClearPass peut être sensible. Il est également important de baser tout équilibrage de charge RADIUS sur le client calling-station-id et de ne pas essayer de s'appuyer sur le port source UDP du côté du WLC.

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.