# Guide de déploiement du contrôleur de filiale sans fil Flex 7500

# Contenu

Introduction Conditions préalables **Conditions requises** Components Used Conventions Présentation du produit Spécifications du produit **Fiche technique** Fonctionnalité de la plate-forme Démarrage du Flex 7500 Licence Flex 7500 Licence de nombre de base AP Licence de mise à niveau AP Prise en charge des versions logicielles Points d'accès pris en charge Architecture FlexConnect Avantages de la centralisation du trafic de contrôle des points d'accès Avantages de la distribution du trafic de données client Modes de fonctionnement FlexConnect **Configuration WAN requise** Conception de réseau de filiale sans fil Exigences de conception principales Apercu **Avantages** Fonctionnalités d'adressage Conception de réseau de filiale Matrice de prise en charge IPv6 Matrice de fonctions **Groupes AP** Configurations à partir du WLC Résumé **Groupes FlexConnect** Objectifs principaux des groupes FlexConnect Configuration du groupe FlexConnect à partir du WLC Vérification à l'aide de CLI Remplacement du VLAN FlexConnect Résumé

Procédure Limites Commutation centrale basée sur VLAN FlexConnect Résumé Procédure Limites ACL FlexConnect Résumé Procédure Limites **Tunnellisation fractionnée FlexConnect** Résumé Procédure Limites Tolérance aux pannes Résumé Limites Limite client par WLAN **Objectif principal** Limites **Configuration WLC Configuration NCS** Blocage peer-to-peer Résumé **Procédure** Limites Téléchargement de préimage AP Résumé Procédure Limites Mise à niveau d'image FlexConnect Smart AP Résumé Procédure Limites Convertir automatiquement les points d'accès en mode FlexConnect Mode manuel Mode de conversion automatique Prise en charge FlexConnect WGB/uWGB pour les WLAN de commutation locale Résumé Procédure Limites Prise en charge d'un nombre accru de serveurs Radius Résumé Procédure Limites

Mode local amélioré (ELM) Prise en charge de l'accès invité dans Flex 7500 Gestion du WLC 7500 à partir de NCS Forum aux questions Informations connexes

# **Introduction**

Ce document décrit comment déployer le contrôleur de branchement sans-fil de la gamme Cisco Flex 7500. Le présent document a pour objet :

- Expliquer les différents éléments réseau de la solution Cisco FlexConnect, ainsi que leur flux de communication.
- Fournir des directives générales de déploiement pour la conception de la solution de filiale sans fil Cisco FlexConnect.
- Expliquer les fonctions logicielles de la version de code 7.2.103.0 qui renforcent la base d'informations sur le produit.

**Remarque :** Avant la version 7.2, FlexConnect s'appelait Hybrid REAP (HREAP). Maintenant on l'appelle FlexConnect.

# **Conditions préalables**

## **Conditions requises**

Aucune spécification déterminée n'est requise pour ce document.

## **Components Used**

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

## **Conventions**

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

# Présentation du produit

#### Figure 1 : Cisco Flex 7500



Le contrôleur cloud Cisco Flex 7500 est un contrôleur de filiale hautement évolutif pour les déploiements <u>sans fil</u> multisites. Déployé dans le cloud privé, le contrôleur Cisco Flex 7500 étend

les services sans fil aux filiales distribuées avec un contrôle centralisé qui réduit le coût total d'exploitation.

La gamme Cisco Flex 7500 (Figure 1) peut gérer <u>des points d'accès</u> sans fil dans 500 filiales au maximum et permet aux responsables informatiques de configurer, gérer et dépanner jusqu'à 3 000 points d'accès (AP) et 30 000 clients du data center. Le contrôleur de la gamme Cisco Flex 7500 prend en charge l'accès invité sécurisé, la détection des pirates pour la conformité PCI (Payment Card Industry) et la voix et la vidéo Wi-Fi dans les filiales (commutées localement).

Ce tableau met en évidence les différences d'évolutivité entre les contrôleurs Flex 7500, WiSM2 et WLC 5500 :

Évolutivité	Flex 7500	WiSM2	WLC 5500
Nombre total de points d'accès	6,000	1000	500
Nombre total de clients	64,000	15,000	7,000
Groupes FlexConnect max	2000	100	100
Nombre max. de points d'accès par groupe FlexConnect	100	25	25
Groupes d'AP max.	6000	1000	500

# Spécifications du produit

## Fiche technique

#### Reportez-vous à

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data\_sheet\_c78-650053.html

## Fonctionnalité de la plate-forme

# Figure 2 : Vue arrière du Flex 7500



Ports d'interface réseau

Ports d'interface	Utilisation

Fast Ethernet	Module de gestion intégrée (IMM)
Port 1 : 1G	Port de service WLC
Port 2 : 1G	Port redondant WLC (RP)
Port 1 : 10 G	Interface de gestion WLC
Port 2 : 10 G	Port d'interface de gestion de sauvegarde WLC (défaillance de port)
Ports Gigabit Ethernet en option	S/O

#### Note:

- La prise en charge LAG pour les interfaces 2x10G permet le fonctionnement de la liaison active-active avec une redondance de liaison de basculement rapide. Une liaison 10G active supplémentaire avec LAG ne modifie pas le débit sans fil du contrôleur.
- 2 interfaces 10 G
- Les interfaces 2x10G prennent uniquement en charge les câbles optiques avec le produit SFP n° SFP-10G-SR.
- Produit SFP côté commutateur X2-10GB-SR

#### Adresses MAC système

Port 1 : 10G (interface de gestion)	Adresse MAC système/base
Port 2 : 10G(Interface de gestion des sauvegardes)	Adresse MAC de base + 5
Port 1 : 1G (port de service)	Adresse MAC de base + 1
Port 2 : 1G (port redondant)	Adresse MAC de base + 3

#### Redirection de console série

Le WLC 7500 permet la redirection de console par défaut au débit de 9600 bauds, simulant le terminal Vt100 sans contrôle de flux.

Informations de stock

Figure 3 : Console WLC 7500

(Cisco Controller) >**show inventory** 

Burned-in MAC Address...... E4:1F:13:65:DB:6C Maximum number of APs supported..... 2000 NAME: "Chassis" , DESCR: "Cisco Wireless Controller" PID: AIR-CT7510-K9, VID: V01, SN: KQZZXWL

La table Desktop Management Interface (DMI) contient les informations sur le matériel et le BIOS du serveur.

Le WLC 7500 affiche la version du BIOS, le PID/VID et le numéro de série dans l'inventaire.

# Démarrage du Flex 7500

Les options du chargeur de démarrage Cisco pour la maintenance logicielle sont identiques aux plates-formes de contrôleur existantes de Cisco.

#### Figure 4 : Commande de démarrage

```
Cisco Bootloader (Version
                      .d88b. d88888b. d8888b. d8888b. d8888b.
                                       88' YP d8P
                     d8P
                          ¥8
                                `88'
                                                    Y8 .8P
                                                             Y8.
                     8P
                                88
                                               8P
                                                       88
                                                             88
                                       `8bo.
                     d8
                                88
                                         `Y8b. 8b
                                                       88
                                                             88
                     Y8b
                          d8
                                .88.
                                            8D Y8b
                                                    d8 ^ 8b
                                                            d8'
                                       db
                      ,A88b, A88888b, S888A, JA86b,
                                                        `Y88P'
Booting Primary Image...
Press <ESC> now for additional boot options...
    Boot Options
Please choose an option from below:
 1. Run primary image (Version
                                            (default)
2. Run backup image
                      (Version
3. Manually upgrade primary image
 4. Change active boot image
 5. Clear Configuration
```

Figure 5 : Assistant Configuration WLC

Would you like to terminate autoinstall? [yes]: System Name [Cisco\_65:db:6c] (31 characters max): AUTO-INSTALL: process terminated -- no configuration loaded Enter Administrative User Name (24 characters max): admin Default values (admin or Cisco or its variants) in password is not allowed. Enter Administrative Password (24 characters max): \* \* \* \*\*\*\*\*\* Re-enter Administrative Password Management Interface IP Address: 172.20.227.174 Management Interface Netmask: 255.255.255.224 Management Interface Default Router: 172.20.227.161 Management Interface VLAN Identifier (0 = untagged): Management Interface VLAN Identifier (1 = untagged): Management Port 1: 10G Management Interface DHCP Server IP Address: 172.20.227.161 Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: mobility Network Name (SSID): DataCenter Configure DHCP Bridging Mode [yes][NO]: NO Allow Static IP Addresses [YES][no]: Yes Configure a RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter Country Code list (enter 'help' for a list of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configure a NTP server now? [YES][no]: no Configure the system time now? [YES][no]: yes Enter the date in MM/DD/YY format: 09/02/10 Enter the time in HH:MM:SS format: 11:50:00 Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

**Remarque :** La séquence de démarrage Flex 7500 est équivalente et cohérente avec les platesformes de contrôleur existantes. Le démarrage initial nécessite une configuration WLC à l'aide de l'Assistant.

## Licence Flex 7500

Licence de nombre de base AP

Références du nombre de points d'accès

300	
500	
1000	
2000	
3000	
6000	

## Licence de mise à niveau AP

Références de mise à niveau AP
100
250
500
1000

Àl'exception du nombre de base et de mise à niveau, la procédure de licence complète qui couvre la commande, l'installation et l'affichage est similaire au WLC 5508 existant de Cisco.

Reportez-vous au <u>guide de configuration WLC 7.3</u>, qui couvre l'ensemble de la procédure de licence.

# Prise en charge des versions logicielles

Le Flex 7500 prend en charge le code WLC version 7.0.116.x et ultérieure uniquement.

# Points d'accès pris en charge

Points d'accès 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 et R 881 est pris en charge avec Flex 7500.

# Architecture FlexConnect

Figure 6 : Topologie type de filiale sans fil

# FlexConnect Architecture



FlexConnect est une solution sans fil pour les déploiements de filiales et de bureaux distants. Il est également appelé solution hybride REAP, mais ce document l'appellera FlexConnect.

La solution FlexConnect permet au client de :

- Centraliser le trafic de contrôle et de gestion des points d'accès à partir du data center.Le trafic de contrôle est marqué par des tirets rouges dans la <u>figure 6</u>.
- Distribuer le trafic de données client à chaque succursale.Le trafic de données est marqué par des tirets bleus, verts et violets dans la <u>Figure 6</u>.Chaque flux de trafic se dirige vers sa destination finale de la manière la plus efficace.

## Avantages de la centralisation du trafic de contrôle des points d'accès

- Volet unique de surveillance et de dépannage
- Facilité de gestion
- Accès mobile sécurisé et transparent aux ressources du data center
- Réduction de l'encombrement des filiales
- Augmentation des économies opérationnelles

## Avantages de la distribution du trafic de données client

- Pas de temps d'arrêt opérationnel (capacité de survie) contre les pannes de liaison WAN complètes ou l'indisponibilité du contrôleur
- Résilience de la mobilité au sein des filiales lors de pannes de liaison WAN
- Augmentation de l'évolutivité des filiales. Prend en charge la taille des filiales pouvant évoluer

jusqu'à 100 points d'accès et 250 000 pieds carrés (5 000 pieds carrés). pieds par point d'accès).

La solution Cisco FlexConnect prend également en charge le trafic de données client central, mais elle doit être limitée au trafic de données invité uniquement. Ce tableau suivant décrit les restrictions sur les types de sécurité WLAN de couche 2 uniquement pour les clients non invités dont le trafic de données est également commuté de manière centralisée au niveau du data center.

Sécurité WLAN L2	Туре	Résultat	
Aucune	S/O	Autorisé	
	802.1x	Autorisé	
	ССКМ	Autorisé	
	802.1x + CCKM	Autorisé	
	PSK	Autorisé	
802.1x	WEP Autori		
WEP statique	WEP	Autorisé	
WEP + 802.1x	WEP	Autorisé	
CKIP		Autorisé	

Prise en charge de la sécurité de couche 2 pour les utilisateurs non invités à commutation centralisée

**Remarque :** Ces restrictions d'authentification ne s'appliquent pas aux clients dont le trafic de données est distribué dans la succursale.

Prise en charge de la sécurité de couche 3 pour les utilisateurs à commutation centrale et locale

Sécurité WLAN L3	Туре	Résultat
	Interne	Autorisé
Authentification Web	Externe	Autorisé
	Personnalisé	Autorisé
	Interne	Autorisé
Accès Web	Externe	Autorisé
	Personnalisé	Autorisé
Redirection Web conditionnelle	Externe	Autorisé
Redirection Web de la page de démarrage	Externe	Autorisé

Pour plus d'informations sur le déploiement de Flexconnect WebAuth externe, reportez-vous au <u>Guide de déploiement de Flexconnect WebAuth externe</u>

Pour plus d'informations sur les états des points d'accès HREAP/FlexConnect et les options de commutation de trafic de données, référez-vous à <u>Configuration de FlexConnect</u>.

Modes de fonctionnement FlexConnect

-	
Mode	Description
FlexC	Description

onnec t	
conne cted	Un FlexConnect est dit être en mode connecté lorsque son plan de contrôle CAPWAP de retour au contrôleur est actif et opérationnel, ce qui signifie que la liaison WAN n'est pas désactivée.
Auton ome	Le mode autonome est spécifié comme état de fonctionnement entré par FlexConnect lorsqu'il n'a plus la connectivité au contrôleur. Les points d'accès FlexConnect en mode autonome continueront à fonctionner avec la dernière configuration connue, même en cas de panne d'alimentation et de défaillance WLC ou WAN.

Pour plus d'informations sur la théorie des opérations FlexConnect, reportez-vous au <u>Guide de</u> <u>conception et de déploiement H-Reap / FlexConnect</u>.

## **Configuration WAN requise**

Les points d'accès FlexConnect sont déployés sur le site de la filiale et gérés à partir du data center via une liaison WAN. Il est fortement recommandé que la restriction de bande passante minimale reste de 12,8 kbits/s par point d'accès, la latence aller-retour ne dépassant pas 300 ms pour les déploiements de données et 100 ms pour les déploiements de données + voix. L'unité de transmission maximale (MTU) doit être d'au moins 500 octets.

Type de déploie ment	Bande passante WAN (min.)	Latence RTT WAN (max.)	Nombre max. de points d'accès par filiale	Nombre maximal de clients par filiale
Donné es	64 kbps	300 ms	5	25
Donné es + voix	128 kbps	100 ms	5	25
Monitor	64 kbps	2 sec	5	S/O
Donné es	640 kbps	300 ms	50	1000
Donné es + voix	1.44 Mbits/s	100 ms	50	1000
Monitor	640 kbps	2 sec	50	S/O

# Conception de réseau de filiale sans fil

Le reste de ce document présente les directives et décrit les meilleures pratiques pour la mise en oeuvre de réseaux de filiales distribués sécurisés. L'architecture FlexConnect est recommandée pour les réseaux de filiales sans fil répondant à ces exigences de conception.

## Exigences de conception principales

- Taille de filiale pouvant évoluer jusqu'à 100 points d'accès et 250 000 pieds carrés (5 000 pieds carrés). pieds par point d'accès)
- Gestion centrale et dépannage
- Pas d'interruption opérationnelle
- Segmentation du trafic basée sur le client
- Une connectivité sans fil transparente et sécurisée aux ressources de l'entreprise
- Compatible PCI
- Assistance aux invités

#### Figure 7 : Conception de réseau de filiale sans fil



#### **Aperçu**

Les clients des filiales éprouvent de plus en plus de difficultés et de coûts à fournir des services réseau complets, évolutifs et sécurisés sur des sites géographiques. Pour aider les clients, Cisco répond à ces défis en introduisant le Flex 7500.

La solution Flex 7500 virtualise les opérations complexes de sécurité, de gestion, de configuration et de dépannage au sein du data center, puis étend ces services de manière transparente à chaque filiale. Les déploiements utilisant Flex 7500 sont plus faciles à configurer, à gérer et, surtout, à faire évoluer.

## **Avantages**

- Augmenter l'évolutivité grâce à la prise en charge de 6 000 points d'accès
- Résilience accrue grâce à la tolérance aux pannes FlexConnect
- Augmenter la segmentation du trafic à l'aide de FlexConnect (Commutation centrale et locale)
- Facilité de gestion en répliquant les conceptions de magasin à l'aide des groupes AP et FlexConnect.

# Fonctionnalités d'adressage Conception de réseau de filiale

Les autres sections du guide décrivent l'utilisation des fonctionnalités et les recommandations pour réaliser la conception du réseau illustrée à la <u>Figure 7</u>.

#### Fonctionnalités :

Fonctions principales	Points saillants
Groupes AP	Facilité d'exploitation et de gestion lors de la gestion de plusieurs sites de filiales. Offre également la souplesse nécessaire à la réplication des configurations pour des sites de filiales similaires.
Groupes FlexConnect	Les groupes FlexConnect offrent les fonctionnalités de Local Backup Radius, CCKM/OKC Fast Roaming et Local Authentication.
Tolérance aux pannes	Améliore la résilience de la filiale sans fil et n'offre aucun temps d'arrêt opérationnel.
ELM (Enhanced Local Mode for Adaptive wIPS)	Fournir une fonctionnalité wIPS adaptative lorsque vous desservez des clients sans impact sur les performances des clients.
Limite client par WLAN	Limitation du nombre total de clients invités sur le réseau de filiale.
Téléchargem ent de préimage AP	Réduit les temps d'arrêt lors de la mise à niveau de votre filiale.
Convertir automatique ment les points d'accès dans FlexConnect	Fonctionnalité permettant de convertir automatiquement les points d'accès dans FlexConnect pour votre succursale.
Accès invité	Poursuivez l'architecture d'accès invité existante de Cisco avec FlexConnect.

# Matrice de prise en charge IPv6

Fonctionnal	Cc ce	ommutation ntralisée		Commuté localement	
ités		5500/WiS M-2	Flex 7500	5500/WiS M-2	Flex 7500
IPv6 (mobilité des clients)	Pr ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
Protection RA IPv6	Pr ch	is en arge	Pris en charge	Pris en charge	Pris en charge
Protection DHCP IPv6	Pri ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
Protection de source IPv6	Pri ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
Limite de débit/limite de débit	Pr ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
ACL IPv6	Pr ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
Visibilité du client IPv6	Pr ch	is en arge	Non pris en charge	Non pris en charge	Non pris en charge
Mise en cache de découverte de voisin IPv6	Pri ch	s en arge	Non pris en charge	Non pris en charge	Non pris en charge
Pontage IPv6	Pri ch	s en arge	Non pris en charge	Pris en charge	Pris en charge

# Matrice de fonctions

Référez-vous à <u>Matrice de fonctions FlexConnect</u> pour une matrice de fonctions pour la fonction FlexConnect.

# **Groupes AP**

Après avoir créé des WLAN sur le contrôleur, vous pouvez les publier de manière sélective (à l'aide de groupes de points d'accès) sur différents points d'accès afin de mieux gérer votre réseau sans fil. Dans un déploiement classique, tous les utilisateurs d'un WLAN sont mappés à une interface unique sur le contrôleur. Par conséquent, tous les utilisateurs associés à ce WLAN se trouvent sur le même sous-réseau ou VLAN. Cependant, vous pouvez choisir de répartir la charge entre plusieurs interfaces ou vers un groupe d'utilisateurs en fonction de critères spécifiques tels que les différents services (marketing, ingénierie ou opérations) en créant des groupes de points d'accès. En outre, ces groupes de points d'accès peuvent être configurés dans des VLAN distincts

pour simplifier l'administration du réseau.

Ce document utilise des groupes AP pour simplifier l'administration du réseau lors de la gestion de plusieurs magasins sur des sites géographiques. Pour faciliter le fonctionnement, le document crée un groupe AP par magasin pour répondre à ces exigences :

- Datacenter SSID à commutation centralisée dans tous les magasins pour l'accès administratif du Gestionnaire de magasins locaux.
- Magasin SSID commuté localement avec différentes clés WPA2-PSK dans tous les magasins pour les scanners portables.





## Configurations à partir du WLC

Procédez comme suit :

1. Sur la page WLANs > New, saisissez Store1 dans le champ Profile Name, saisissez store dans le champ SSID et choisissez 17 dans la liste déroulante ID.Remarque : les ID de réseau local sans fil 1 à 16 font partie du groupe par défaut et ne peuvent pas être supprimés. Afin de satisfaire à notre exigence d'utiliser le même SSID store par magasin avec un WPA2-PSK différent, vous devez utiliser l'ID WLAN 17 et au-delà, car ceux-ci ne font pas partie du groupe par défaut et peuvent être limités à chaque magasin.

ahaha				Sage Configuration   Ping   Logout Befresh
cisco	MONITOR WLANS CONTRI	ILLER WIJRELESS SECURITY M	NANAGEMENT COMMANDS HELP	EEEDBACK
WLANs	WLANs > New			< Back Apply
WLANS	Туре	WLAN 💌		
Advanced	Profile Name	Storel		
	SSID	store		
	ID	17 🛩		

2. Sous WLAN > Security, sélectionnez **PSK** dans la liste déroulante Auth Key Mgmt, choisissez **ASCII** dans la liste déroulante PSK Format, puis cliquez sur

Apply.									
cisco	MONITOR WLANS CONT	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sage Configu EEEDBACK	ration <u>P</u> ing	Logout <u>R</u> efresh
WLANs	WLANs > Edit							< Back	Αρρίγ
WLANS	General Security	QoS Advanced							
Advanced	Layer 2 Layer 3	AAA Servers							
	Layer 2 Security 4 WP	MAC Filtering							
	WPA+WPA2 Parameters								
	WPA Policy								
	WPA2 Policy								
	WPA2 Encryption	PAES DTKIP							
	Auth Key Mgmt	PSK 💌							
	PSK Format	ASCII 💌							
		•••••							

3. Cliquez sur WLAN > General, vérifiez les modifications apportées aux stratégies de sécurité et cochez la case Status pour activer le

situation English	would Befresh
CISCO MONITOR MLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	eToor Ferrers
WLANs WLANs > Edit cmack	Apply
WLANS General Security QoS Advanced	_
Advanced Profile Name Store1	
Type WLAN	
SSID store	
Status 💌 Enabled	
Security Policies [WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)	
Radio Policy All	
Interface/Interface management v	
Multicast Vlan Feature Enabled	
Broadcast SSID 🕑 Enabled	

4. Répétez les étapes 1, 2 et 3 pour le nouveau profil WLAN **Store2**, avec le **magasin** SSID et l'ID

$\mathbf{a}$	
×	
Ο.	
	8.

10.										
ahaha										Logout   Befresh
cisco	MONITOR	₩LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
WLANs	WLANs > 1	New							< Back	Apply
₩ WLANs     WLANs     Advanced	Type Profile Nam SSID ID	ie	WLAN Store 18	2						

CISCO       MONITOR       WILANS       CONTROLLER       WILENS       SECURITY       MANAGEMENT       COMMANDS       HELP       EEEDBACK         WLANS       WLANS       WLANS       Ceneral       Security       QoS       Advanced         WLANS       WLANS       General       Security       QoS       Advanced         WLANS       Hayer 2       Layer 3       AAA Servers       Layer 2       Layer 3       Layer 3       AAA Servers         Layer 2       Security       WPA+WPA2       V       MAAC Filtering       WPA-WPA2       V       V       MAAC Filtering       WPA Policy       V       MAA2 Encryption       Aats       ThCIP       Adth Key Mgmt       PSK       V       PSK Format       ASCII V       V <t< th=""></t<>
WLANs     WLANs       WLANs     General Security QoS Advanced       Layer 2 Layer 3 AAA Servers       Layer 2 Security WPA+WPA2 v       MMAAC Filtering       WPA+WPA2 Parameters       WPA Policy       WPA2 Policy       WPA2 Encryption       Addx C Mgmt       PSK Format
WLANS   WLANS   Ceneral   Security   QoS   Advanced     Layer 2   Layer 2   Layer 2   Layer 2   Layer 2   Layer 2   MMAC Filtering   WPA+WPA2 Parameters   WPA Policy   WPA2 Policy   WPA2 Encryption   Auth Key Mgmt   PSK Format   ASCIT V
Advanced       Layer 2       Layer 3       AAA Servers         Layer 2       Security *       WPA+WPA2       Image: Comparison of the c
Layer 2 Security WPA+WPA2 MMAC Filtering WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format ASCIT V 
Layer 2 Security WPA+WPA2 W MMAC Filtering WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format Ascrit
WPA+WPA2 Parameters         WPA Policy         WPA2 Policy         WPA2 Policy         WPA2 Encryption         Auth Key Mgmt         PSK Format         ASCI1
WPA-WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format ASCII
WPA Policy  WPA2 Policy  WPA2 Policy  WPA2 Encryption  Auth Key Mgmt  PSK  PSK Format  ASCII
WPA2 Encryption ALES TKIP Auth Key Mgmt PSK V PSK Format ASCII V
Auth Key Mgmt PSK V PSK Format ASCII V
PSK Format
•••••
Sage Configuration Bing Logout Befres
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs WLANs>Edit
WLANS General Security QoS Advanced
Advanced Profile Name Store2
Type WLAN
SSID store
Status 🗹 Enabled
Security Policies [WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
( in a second
Radio Policy All
Interface/Interface management ×
Multicast Vian Feature Enabled

- 5. Créez et activez le profil WLAN avec le nom de profil **DataCenter**, SSID **DataCenter** et ID 1.**Remarque :** Lors de la création, les ID de réseau local sans fil de 1 à 16 font automatiquement partie du groupe de points d'accès par défaut.
- 6. Sous WLAN, vérifiez l'état des ID de WLAN 1, 17 et

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS SECUE	TY MANAGEMENT	COMMANDS H	elp fee	EDBACK		
cisco										
LANS	WLANS								Entries 1	- 3
WLANS	Current Fill	Non	e [Change	Filter] [Clear Filter]						
WLANs	corrent rin					Create New	×	60		
WLANs Advanced AP Groups	WLAN II	D Туре	Profile Nam	e	WLAN SSID	Create New	nin Status	Go Security Policies		
WLANs Advanced AP Groups		D Type WLAN	Profile Nam DataCenter	e	WLAN SSID DataCenter	Adm Enal	nin Status	Security Policies [WPA + WPA2][At	s wh(802.1X)]	
WLANS Advanced AP Groups		D Type WLAN WLAN	Profile Nam DataCenter Store1	e	WLAN SSID DataCenter store	Adm Enal Enal	nin Status bled bled	Security Policies [WPA + WPA2][Auth(PSK	s vth(802.1X)]	0

- 7. Cliquez sur WLAN > Avancé > Groupe AP > Ajouter un groupe.
- 8. Ajoutez le nom du groupe AP **Store1**, identique au profil WLAN **Store1**, et la description comme emplacement du magasin. Dans cet exemple, la Californie est utilisée comme emplacement du magasin.
- 9. Cliquez sur **Ajouter** lorsque vous avez terminé.



- 10. Cliquez sur **Ajouter un groupe** et créez le **magasin** de noms de groupe AP et la description New York.
- 11. Cliquez sur

**O**------

Add.										
սիսիս								Sage Configuration		Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		
WLANs	AP Groups							Entries 1 -	1 of 1	Add Group
<ul> <li>WLANS WLANS</li> <li>Advanced AP Groups</li> </ul>	Add New AP Group AP Group Name Description AP Group Name Store1 default-group	w York w York dd Cancel	AP Cal	Group Descr	iption					

12. Vérifiez la création du groupe en cliquant sur WLAN > Advanced > AP

Groups.									
ahaha								Save Configuration   Ping	Logout   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
WLANs	AP Groups							Entries 1 - 2 of 2	Add Group
* WLANS	AB Crown Marrie			Deces	intian				
WLANS	AP Group Name		API	sroup Descr	iption				
<ul> <li>Advanced</li> </ul>	Store1		Cali	fornia					
AP Groups	Store2		New	York					
	default-group								

- 13. Cliquez sur AP Group Name Store1 pour ajouter ou modifier le WLAN.
- 14. Cliquez sur Add New pour sélectionner le WLAN.
- 15. Sous WLAN, dans la liste déroulante WLAN SSID, sélectionnez WLAN ID 17 store(17).
- 16. Cliquez sur Add après la sélection de l'ID WLAN 17.
- 17. Répétez les étapes 14 à 16 pour l'ID de réseau local sans fil 1 DataCenter(1). Cette étape est facultative et nécessaire uniquement si vous souhaitez autoriser l'accès aux ressources distantes.

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sage Configuration	Eng Logout Befres
WLANs	Ap Grou	ps > Edit	'Store1'							< Back
WLANS WLANS	General	WLA	Ns APs							
Advanced     AP Groups									Add New	Î
	Add Ne	w								
	WLAN	SSID	store (17) St	ore 1		ļ				
	/Interf Group	face (G)	store(17) Stor store(18) Stor	0 0 1 0 2						
	NAC S	tate	Add Ca	incel						
	WLAN ID	WLAN	Interface/In Group(G)	terface	NAC					
			are ablead							

18. Revenez à l'écran WLAN > Advanced > AP Groups.

- 19. Cliquez sur AP Group Name Store2 pour ajouter ou modifier un WLAN.
- 20. Cliquez sur Add New pour sélectionner le WLAN.
- 21. Sous WLAN, dans la liste déroulante WLAN SSID, sélectionnez WLAN ID 18 store(18).
- 22. Cliquez sur Add après la sélection de l'ID WLAN 18.
- 23. Répétez les étapes 14 à 16 pour l'ID de réseau local sans fil 1 DataCenter(1).

. cisco	Saya ( MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDB	Configuration <u>P</u> ing Logout <u>B</u> efres ACK
WLANs	Ap Groups > Edit 'Store2'	< Back
WLANs     WLANs     WLANs     Advanced     AP Groups	General WLANS APS	ew
	Add New       WLAN SSID       Interface       Jinterface       Jinterface       Josef (1)       Jinterface       store(12)       NAC State       Enabled       Add       Cancel       WLAN       WLAN       WLAN       Interface/Interface       NAC State	

Remarque : L'ajout de plusieurs profils WLAN avec le même SSID sous un seul groupe AP



l'ajout de points d'accès au groupe de points d'accès n'est pas capturé dans ce document, mais il est nécessaire que les clients accèdent aux services réseau.

## <u>Résumé</u>

- Les groupes AP simplifient l'administration du réseau.
- Dépannage aisé avec la granularité de chaque branche
- Flexibilité accrue

# **Groupes FlexConnect**

Figure 9 : Authentification Dot1X centrale (Flex 7500 agissant en tant qu'authentificateur)

# **Central Authentication – Flex 7500 Authenticator**



Dans la plupart des déploiements typiques de filiales, il est facile de prévoir que l'authentification 802.1X du client a lieu de manière centralisée au niveau du data center, comme illustré à la Figure 9. Comme le scénario ci-dessus est parfaitement valable, il soulève ces préoccupations :

- Comment les clients sans fil peuvent-ils effectuer l'authentification 802.1X et accéder aux services de data center en cas de défaillance de Flex 7500 ?
- Comment les clients sans fil peuvent-ils effectuer l'authentification 802.1X en cas de défaillance de la liaison WAN entre la filiale et le data center ?
- Y a-t-il un impact sur la mobilité des filiales lors de pannes de réseau étendu ?
- La solution FlexConnect n'offre-t-elle pas de temps d'arrêt opérationnel pour les filiales ?

Le groupe FlexConnect est principalement conçu et doit être créé pour relever ces défis. En outre, il facilite l'organisation de chaque site de filiale, car tous les points d'accès FlexConnect de chaque site de filiale font partie d'un seul groupe FlexConnect.

Remarque : les groupes FlexConnect ne sont pas analogues aux groupes AP.

#### Objectifs principaux des groupes FlexConnect

#### Basculement du serveur RADIUS de sauvegarde

 Vous pouvez configurer le contrôleur pour autoriser un point d'accès FlexConnect en mode autonome à effectuer une authentification 802.1X complète sur un serveur RADIUS de sauvegarde. Afin d'accroître la résilience de la filiale, les administrateurs peuvent configurer un serveur RADIUS de sauvegarde principal ou un serveur RADIUS de sauvegarde principal et secondaire. Ces serveurs sont utilisés uniquement lorsque le point d'accès FlexConnect n'est pas connecté au contrôleur.

**Remarque :** La sauvegarde de la comptabilité RADIUS n'est pas prise en charge.

#### Authentification locale

 Avant la publication du code 7.0.98.0, l'authentification locale n'était prise en charge que lorsque FlexConnect est en mode autonome pour s'assurer que la connectivité du client n'est pas affectée en cas de défaillance de liaison WAN. Avec la version 7.0.116.0, cette fonctionnalité est désormais prise en charge même lorsque les points d'accès FlexConnect sont en mode connecté. Figure 10 : Authentification Dot1X centrale (AP FlexConnect agissant en tant qu'authentificateur)



# **Central Authentication – AP Authenticator**

Comme l'illustre la Figure 10, les clients de filiale peuvent continuer à effectuer l'authentification 802.1X lorsque les points d'accès FlexConnect Branch perdent la connectivité avec Flex 7500. Tant que le serveur RADIUS/ACS est accessible depuis le site de la filiale, les clients sans fil continueront à s'authentifier et à accéder aux services sans fil. En d'autres termes, si RADIUS/ACS se trouve dans la succursale, les clients authentifient et accèdent aux services sans fil même en cas de panne du réseau étendu. **Remarque :** cette fonctionnalité peut être utilisée conjointement avec la fonctionnalité de serveur RADIUS de sauvegarde FlexConnect. Si un groupe FlexConnect est configuré avec le serveur RADIUS de sauvegarde et l'authentification locale, le point d'accès FlexConnect tente toujours d'authentifier les clients à l'aide du serveur RADIUS de sauvegarde principal, suivi du serveur RADIUS de sauvegarde secondaire (si le serveur principal n'est pas accessible) et enfin du serveur EAP local sur le point d'accès FlexConnect lui-même (si le serveur principal et secondaire ne sont pas accessibles).

EAP local (suite de l'authentification locale)

Figure 11 : Authentification Dot1X (AP FlexConnect agissant en tant que serveur EAP local)



# Local Branch Authentication – AP as Radius Server

• Vous pouvez configurer le contrôleur pour permettre à un AP FlexConnect en mode

autonome ou connecté d'exécuter l'authentification LEAP ou EAP-FAST pour un maximum de 100 utilisateurs configurés de manière statique. Le contrôleur envoie la liste statique des noms d'utilisateur et des mots de passe à chaque point d'accès FlexConnect de ce groupe FlexConnect particulier lorsqu'il rejoint le contrôleur. Chaque point d'accès du groupe authentifie uniquement ses propres clients associés.

- Cette fonctionnalité est idéale pour les clients qui migrent d'un réseau de point d'accès autonome vers un réseau de point d'accès léger FlexConnect et ne sont pas intéressés par la maintenance d'une base de données d'utilisateurs de grande taille ou par l'ajout d'un autre périphérique matériel pour remplacer la fonctionnalité de serveur RADIUS disponible dans le point d'accès autonome.
- Comme l'illustre la <u>Figure 11</u>, si le serveur RADIUS/ACS à l'intérieur du centre de données n'est pas accessible, les points d'accès FlexConnect agissent automatiquement en tant que serveur EAP local pour effectuer l'authentification Dot1X pour les clients des filiales sans fil.

#### Itinérance rapide CCKM/OKC

- Les groupes FlexConnect sont requis pour que l'itinérance rapide CCKM/OKC fonctionne avec les points d'accès FlexConnect. L'itinérance rapide est obtenue en mettant en cache un dérivé de la clé principale à partir d'une authentification EAP complète afin qu'un échange de clés simple et sécurisé puisse se produire lorsqu'un client sans fil se déplace vers un autre point d'accès. Cette fonctionnalité évite la nécessité d'effectuer une authentification RADIUS EAP complète lorsque le client se déplace d'un point d'accès à un autre. Les points d'accès FlexConnect doivent obtenir les informations de cache CCKM/OKC pour tous les clients qui pourraient s'associer afin qu'ils puissent les traiter rapidement au lieu de les renvoyer au contrôleur. Si, par exemple, vous avez un contrôleur avec 300 points d'accès et 100 clients qui peuvent s'associer, l'envoi du cache CCKM/OKC pour les 100 clients n'est pas pratique. Si vous créez un groupe FlexConnect comprenant un nombre limité de points d'accès (par exemple, vous créez un groupe pour quatre points d'accès dans un bureau distant), les clients ne circulent que parmi ces quatre points d'accès et le cache CCKM/OKC est distribué entre ces quatre points d'accès que lorsque les clients s'associent à l'un d'eux.
- Cette fonctionnalité, associée à Backup Radius et Local Authentication (Local-EAP), ne garantit aucun temps d'arrêt opérationnel pour vos sites de succursales.Remarque : l'itinérance rapide CCKM/OKC entre les points d'accès FlexConnect et non FlexConnect n'est pas prise en charge.Figure 12 : Référence de conception de réseau sans fil à l'aide des groupes FlexConnect



## Configuration du groupe FlexConnect à partir du WLC

Complétez les étapes de cette section afin de configurer les groupes FlexConnect pour prendre en charge l'authentification locale à l'aide de LEAP, lorsque FlexConnect est en mode Connecté ou Autonome. L'exemple de configuration de la <u>Figure 12</u> illustre les différences d'objectifs et le mappage 1:1 entre le groupe AP et le groupe FlexConnect.

- 1. Cliquez sur **Nouveau** sous Wireless > FlexConnect Groups.
- 2. Affectez le magasin de noms de groupe 1, similaire à l'exemple de configuration présenté à la <u>Figure 12</u>.
- 3. Cliquez sur **Apply** lorsque le nom du groupe est défini.

cisco	MONITOR	<u>W</u> LANs	CONT	ROLLER	W <u>I</u> RELESS
Wireless	FlexCon	nect Gro	oups >	New	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li></ul></li></ul>	Group Na	ime S	tore 1		
Advanced					
Mesh					
RF Profiles					
FlexConnect Groups			-		

4. Cliquez sur le **magasin** de noms de groupe **1** que vous venez de créer pour une configuration

ultérieure.

cisco	MONITOR	<u>w</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY
Wireless	FlexConr	nect Gro	ups		
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> <li>202112/2</li> </ul>	Group Nat	me			
802.114/n 802.11h/g/n Global Configuration					
Advanced					
Mesh					
RF Profiles					
FlexConnect Groups					
5. Cliquez sur <b>Add</b> <b>AP</b> .					

uluilu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecuri
Wireless	FlexConn	ect Gro	ups > Edit 'S	tore 1'	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Global Configuration</li> </ul> </li> </ul>	General Group	Local	Authentication	Image U	pgrade
<ul> <li>Advanced</li> <li>Mesh</li> <li>RF Profiles</li> <li>FlexConnect Groups</li> <li>FlexConnect ACLs</li> </ul>	FlexCon Add A AP MAC	Address	s AP Name	Sta	itus

- 6. Cochez la case **Enable AP Local Authentication** afin d'activer l'authentification locale lorsque l'AP est en mode autonome. **Remarque :** l'étape 20 montre comment activer l'authentification locale pour le point d'accès en mode connecté.
- 7. Cochez la case **Sélectionner les points d'accès à partir du contrôleur actuel** afin d'activer le menu déroulant Nom de point d'accès.
- 8. Choisissez l'AP dans la liste déroulante qui doit faire partie de ce groupe FlexConnect.
- 9. Cliquez sur Add après avoir choisi le point d'accès dans la liste déroulante.
- 10. Répétez les étapes 7 et 8 pour ajouter tous les points d'accès à ce groupe FlexConnect qui font également partie du magasin de groupe AP 1. Voir <u>Figure 12</u> pour comprendre le mappage 1:1 entre le groupe AP et le groupe FlexConnect.Si vous avez créé un AP-Group par Store (<u>Figure 8</u>), alors idéalement tous les AP de ce AP-Group devraient faire partie de ce FlexConnect Group (<u>Figure 12</u>). Le maintien d'un ratio 1/1 entre le groupe AP et le groupe FlexConnect simplifie la gestion du réseau.



- 11. Cliquez sur Local Authentication > Protocols et cochez la case Enable LEAP Authentication.
- 12. Cliquez sur Apply après avoir activé la case à cocher. Remarque : Si vous disposez d'un contrôleur de sauvegarde, assurez-vous que les groupes FlexConnect sont identiques et que les entrées d'adresse MAC AP sont incluses par groupe FlexConnect.

FlexConnect G	Sroups >	Edit	'Store 1	•
---------------	----------	------	----------	---

|--|

Apply

ieneral	Local Authenticatio	n Image Upgrade	VLAN-ACL mapping
Local Use	ers Protocols		
LEAP			
Enable Authent	LEAP ication <sup>2</sup>		
EAP Fast			
Enable	EAP Fast Authentication	2	
Server	Key (in hex)	🔲 Enable Auto key ge	neration
		•••••	
Authori	ty ID (in hex)	436973636f00000000	000000000000
Authori	ty Info	Cisco A_ID	
PAC Tir	neout (2 to 4095 days)		

- 13. Sous Authentification locale, cliquez sur **Utilisateurs locaux**.
- 14. Définissez les champs Username, Password et Confirm Password, puis cliquez sur **Add** afin de créer une entrée utilisateur dans le serveur EAP local résidant sur l'AP.
- 15. Répétez l'étape 13 jusqu'à épuisement de votre liste de noms d'utilisateur local. Vous ne pouvez pas configurer ou ajouter plus de 100 utilisateurs.
- 16. Cliquez sur **Apply** après avoir terminé l'étape 14 et vérifié le nombre d'utilisateurs.

ieneral Loc	al Authentication	n Image Upgrade	VLAN-ACL mapping
Local Users	Protocols		
Nc of Users	0	Add User	
User Name		Unload COV Shall	
		File Name	
		The Herite	
		UserName	cisco

17. Dans le volet supérieur, cliquez sur WLAN.

18. Cliquez sur **WLAN ID 17**. Ceci a été créé lors de la création du groupe AP. Voir la <u>figure</u> 8.

cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGE
WLANs	WLANs					
WI ANS WLANS	Current Fil	iter: No	ne [ <u>Cha</u>	inge Eilter] [Cle	ar Filter]	
Advanced	_					
		ID Type	Profile N	lame	v	VLAN SSID
	□ <u>2</u>	WEAN	Guest		G	uest
	□ <u>17</u>	WLAN	Store-1		S	tore

- 19. Sous WLAN > Edit for WLAN ID 17, cliquez sur **Advanced**.
- 20. Cochez la case **FlexConnect Local Auth** afin d'activer l'authentification locale en mode connecté. **Remarque :** l'authentification locale est prise en charge uniquement pour FlexConnect avec commutation locale. **Remarque :** Veillez toujours à créer le groupe FlexConnect avant d'activer l'authentification locale sous

```
WLANs > Edit 'Store-1'
```

General Security	Qo	s	Adv	anc	ed	]	
P2P Blocking Action		Disa	abled				
Client Exclusion <sup>2</sup>		🗹 Enabled			60 Timeout Value (se		
Maximum Allowed Clie	ents 🚨	0					
Static IP Tunneling 🎞		E 6	inable	ed			
Wi-Fi Direct Clients Po	licy	Dis	abled	-			
Maximum Allowed Clie Per AP Radio	ents	200					
Off Channel Scanning [	Defer						
Scan Defer Priority	0 1	L 2	3	4	5	6	7
Scan Defer Time (msecs)	100						
FlexConnect							
FlexConnect Local Swi 2	itching		Enab	led			
FlexConnect Local Aut	:h <del>12</del>		Enab	led			
Learn Client IP Addres	ss <mark>5</mark>		Enab	led			

## WLAN.

NCS fournit également la case à cocher FlexConnect Local Auth afin d'activer l'authentification locale en mode connecté, comme indiqué ici :

Properties	>	WLAN Configuration Det	ails : 1
System	>		
WLANs	~	General Security	QoS Advanced
Han Configuration			
🚪 AP Groups		HexConnect Local Switching	Enable
FlexConnect	>	FlexConnect Local Auth 🕸	🗹 Enable
Security	>	Learn Client IP Address	🗹 Enable
Access Points	>	Session Timeout	Enable
802.11	>	Coverage Hole Detection Aironet IE	Enable
802.11a/n	>	IPv6 <sup>2</sup>	Enable
802.11b/g/n	>	Diagnostic Channel 🙎	Enable
Mesh	>	Override Interface ACL	IPv4 NONE
Ports	,	Peer to Peer Blocking 🛈	Disable
Management	>	Wi-Fi Direct Clients Policy	Disabled
Location	>	Timeout Value	60 (secs)

Le système NCS offre également la possibilité de filtrer et de surveiller les clients authentifiés localement FlexConnect, comme illustré ici

:

•1  C	cisco Network Control System								
6	Ilome Monitor	Configure	▼ Services	<ul> <li>Reports</li> </ul>	▼ Adı	nnistration			
Clients and Users									
R	urcubeshoot 🍐 lest	• 🗶 usable	- Remove	More 💌 🚟 Irai	rk Clents	Soldenniy	Hoknown Hisers		
	MAC Address	IP Address	IP iype	User Name	lype	Vendor	Device Name		
0	00:22:90:1b:17:42		₽v1	Unknown		Cisco	WCS_SW 0.1.0.2		
0	1c:df:0f:66:86:58		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
0	00:21:6a:97:9b:bc		₽v4	host/vikatta		Intel	oeap-laiwar-2		
0	00:22:90:15:96:48		IPv4	Unknown	-	LISCO	WCS_SW-9.1.0.2		
0	00:22:90:1b:17:8c		₽v1	Unknown	<b></b>	Cisco	WCS_SW 0.1.0.2		
Q	00:25:0b:4d:77:c4		₽v4	Unknown	5	Cisco	WCS_SW-9.1.0.2		
0	c4:7d:4f:3a:c5:d5		IPv4	Unknown		CISCO	WCS_SW-9.1.0.2		
0	00:21:a0:d5:03:c4		IPv4	Unknown	<b></b>	Cisco	WCS_SW-9.1.0.2		
Û	f3:66:f2:67:7f:60		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
0	00:15ca:b0:01:b4		₽v4	Unknown	2	Cisco	WCS_SW-9.1.0.2		
0	88:43:e1:d1:df:02		IPv4	Unknown	<b></b>	LISCO	WCS_SW-9.1.0.2		
0	00:22:bd:1b:e2:b5		₽v1	Unknown	<b></b>	Cisco	WCS_SW 0.1.0.2		
0	f3:66:f2:ab:1e:69		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2		
Ō.	00:10:58:dc:b4:4e		₽v4	Unknown	8	Ciscu	WCS_SW-9.1.0.2		
$\cap$	00:1e:/a:bb:21:8d		IPv4	ssimm	618	CISCO	oean-ta viar-7		

Virtual Domain: ROOT-DOMAIN

root 🗸 Log Out

2+

1 0

			Show	Associated Clients *
Location	VLAN	Status	Interface	Quick Filter
Unknown	109	Associated	Gi1/0/34	Advanced Filter
Unknown	109	Associated	Gi1/0/26	All
Root Area	310	Associated	data	Manage Preset Filters
Unknown	109	Associated	Gi1/0/36	2.4GHz Clients
Unknown	109	Associated	Gi1/0/32	5GHz Clients
Unknown	109	Associated	Gi1/0/30	All Autopomous Clients
Unknown	109	Associated	Gi1/0/13	All Wired Clients
Unknown	109	Associated	Gi1/0/27	Associated Clients
Unknown	109	Associated	Gi1/0/12	Clients known by ISE
Unknown	109	Associated	Gi1/0/15	Clients detected by MSE
Unknown	109	Associated	Gi1/0/28	Clients detected in the last 24 hours
Unknown	109	Associated	Gi1/0/14	Clients with Problems
Unknown	109	Associated	Gi1/0/9	Excluded Clients
Unknown	109	Associated	Gi1/0/29	FlexConnect Locally Authenticated
Root Area	311	Associated	voice	New clients detected in last 24 hours

## Vérification à l'aide de CLI

L'état d'authentification du client et le mode de commutation peuvent être rapidement vérifiés à l'aide de cette CLI sur le WLC :

(Cisco	Controller) >show client detail 00:24:d7:2b	:7c:0c
Client	MAC Address	00:24:d7:2b:7c:0c
Client	Username	N/A
AP MAC	Address	d0:57:4c:08:e6:70
Client	State	Associated
H-REAP	Data Switching	Local
H-REAP	Authentication	Local

# Remplacement du VLAN FlexConnect

Dans l'architecture FlexConnect actuelle, il existe un mappage strict de WLAN vers VLAN, et par conséquent le client qui est associé à un WLAN particulier sur l'AP FlexConnect doit respecter un

VLAN qui lui est mappé. Cette méthode a des limites, car elle exige que les clients s'associent à différents SSID pour hériter de politiques différentes basées sur VLAN.

Àpartir de la version 7.2, le remplacement AAA du VLAN sur chaque WLAN configuré pour la commutation locale est pris en charge. Afin d'avoir une affectation VLAN dynamique, AP aurait les interfaces pour le VLAN précréé en fonction d'une configuration utilisant le mappage WLAN-VLAN existant pour chaque AP FlexConnect ou en utilisant le mappage ACL-VLAN sur un groupe FlexConnect. Le WLC est utilisé pour précréer les sous-interfaces au niveau de l'AP.



## Résumé

- La substitution de VLAN AAA est prise en charge à partir de la version 7.2 pour les WLAN configurés pour la commutation locale en mode d'authentification centrale et locale.
- Le remplacement AAA doit être activé sur le WLAN configuré pour la commutation locale.
- L'AP FlexConnect doit avoir un VLAN précréé à partir du WLC pour l'affectation dynamique de VLAN.
- Si les VLAN renvoyés par écrasement AAA ne sont pas présents sur le client AP, ils obtiendront une adresse IP de l'interface VLAN par défaut de l'AP.

## Procédure

Procédez comme suit :

1. Créez un WLAN pour l'authentification 802.1x.

ANs > E	dit 'Store 1'		
eneral	Security	QoS Adva	anced
Layer 2	Layer 3	AAA Servers	5
Layer 2	Security 🤷 🛛 🛛	VPA+WPA2 	~
WPA+WPA	2 Parameter	s	
WPA Po	licy		
WPA2 P	olicy	<b>V</b>	
WPA2 E	ncryption	AES	🗌 ТКІР
Auth Ke	y Mgmt	802.1X	~
WPA gtl State	-randomize	Disa	ole 💙

 Activez la prise en charge du remplacement AAA pour le WLAN de commutation locale sur le WLC. Accédez à WLAN GUI > WLAN > WLAN ID > Advance tab.

General Security Qo	S Advanced		
Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection	Enabled	DHCP Server	verride
Enable Session Timeout	1800 Session Timeout (secs)	DHCP Addr. Assignment	equired
Aironet IE	Enabled	Management Frame Protection (	MFP)
Diagnostic Channel	Enabled		
Override Interface ACL	IPv4 IPv6	MFP Client Protection 4 Option	al 🗸
P2P Blocking Action	Disabled	DTIM Period (in beacon intervals	.)
Client Exclusion 2	Enabled 60	802.11a/n (1 - 255) 1	
Maximum Allowed Clients	Timeout Value (secs)	802.11b/g/n (1 - 255) 1	
Static IP Tunneling	Enabled	NAC	
Wi-Fi Direct Clients Policy	Disabled M	NAC State None 💌	
Maximum Allowed Clients	200	Load Balancing and Band Select	
Per AP Radio		Client Load Balancing	
Off Channel Scanning Defer		Client Band Select Z	
Scan Defer Priority 0	1 2 3 4 5 6 7	Passive Client	
		Passive Client	
Scan Defer Time		Voice	
(msecs)		Media Session Snooping	Enal
lexConnect		Re-anchor Roamed Voice Clients	Enal
FlexConnect Local	V Saablad	KTS based CAC Policy	

 Ajoutez les détails du serveur AAA sur le contrôleur pour l'authentification 802.1x. Afin d'ajouter le serveur AAA, naviguez jusqu'à l'interface graphique du WLC > Security > AAA > Radius > Authentication > New.

Security	RADIUS Authentication S	ervers > Edit
T AAA General	Server Index	1
• RADIUS	Server Address	
Accounting	Shared Secret Format	ASCII 🗸
Fallback TACACS+	Shared Secret	***
LDAP Local Net Users	Confirm Shared Secret	•••
MAC Filtering Disabled Clients	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
User Login Policies AP Policies	Port Number	1812
Password Policies	Server Status	Enabled 💌
Local EAP	Support for RFC 3576	Enabled 💌
Priority Order	Server Timeout	2 seconds
Certificate	Network User	Enable
Access Control Lists	Management	Enable
Wireless Protection     Policies	IPSec	Enable Enable

4. Le point d'accès est en mode local par défaut, de sorte que le mode est couvert en mode FlexConnect. Les points d'accès en mode local peuvent être convertis en mode FlexConnect en accédant à Wireless > All APs, puis cliquez sur le point d'accès individuel.

I APs > De	etails for AP3	500					
General	Credentials	Interfaces	High Availa	bility	Inventory	Advanced	
General					Versions		
AP Name	A	P3500			Primary Soft	ware Version	7.2.1.69
Location	de	fault location			Backup Softw	vare Version	7.2.1.72
AP MAC A	ddress co	:ef:48:c2:35:57			Predownload	Status	None
Base Radi	o MAC 20	::3f:38:f6:98:b0			Predownload	ed Version	None
Admin Sta	tus Er	nable 💌			Predownload	Next Retry Time	NA
AP Mode	E	exConnect 🗸 🗸			Predownload	Retry Count	NA
AP Sub Mo	de N	one 💌			Boot Version		12.4.23.0
Operationa	al Status Ri	G			IOS Version		12.4(20111122:141426
Port Numb	er 1				Mini IOS Ver	sion	7.0.112.74
Venue Gro	up U	nspecified	~		IP Config		
Venue Typ	e U	nspecified 💌			IP Address		10.10.132
Venue Nar	me				Static IP		
Language							
Network S Interface H	pectrum 00 Key	045BA896226F411	7D98BA920FBA	8A16	Time Statistics		
					UP Time		0 d, 00 h 01 m 14 s
					Controller As	sociated Time	0 d, 00 h 00 m 14 s
					Controller As	sociation Latency	0 d, 00 h 00 m 59 s

 Ajoutez les points d'accès FlexConnect au groupe FlexConnect.Naviguez sous WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General tab > Add AP.

	on Image Upgrade VLA	N-ACL mapping		
Group Name Store 1				
exConnect APs		АЛА		
dd AP		Primary Radius Server	None	¥
Select APs from current controller	Secondary Radius Server	None	*	
		Enable AP Local Authentication <sup>2</sup>		
AP Name	AP3300			

6. L'AP FlexConnect doit être connecté sur un port d'agrégation et le VLAN mappé WLAN et le VLAN écrasé AAA doivent être autorisés sur le port
```
interface GigabitEthernet1/0/4
description AP3500
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk
```

d'agrégation.

Remarque : dans cette

configuration, le VLAN 109 est utilisé pour le mappage de VLAN WLAN et le VLAN 3 pour le remplacement AAA.

7. Configurez le mappage WLAN vers VLAN pour l'AP FlexConnect. En fonction de cette configuration, le point d'accès aurait les interfaces pour le VLAN. Lorsque le point d'accès reçoit la configuration VLAN, les sous-interfaces dot11 et Ethernet correspondantes sont créées et ajoutées à un groupe de ponts. Associez un client à ce WLAN et lorsque le client s'associe, son VLAN (par défaut, en fonction du mappage WLAN-VLAN) est attribué.Naviguez jusqu'à l'interface graphique WLAN > Wireless > All APs > cliquez sur l'onglet AP spécifique > FlexConnect, puis cliquez sur VLAN

AP Nan	ne	AP3500	
Base Radio MAC		2c:3f:38:f6:98:b0	
WLAN Id	SSID		VLAN ID
1	Store 1		109

#### Mapping.

8. Créez un utilisateur sur le serveur AAA et configurez l'utilisateur pour renvoyer l'ID de VLAN dans l'attribut Radius

	Attribute	Туре	Value
IETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802
IETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN
IETF 81	Tunnel-Private-Group-ID	Tagged String	[T:1] 3

IETF.

9. Afin d'avoir une affectation VLAN dynamique, l'AP aurait les interfaces pour le VLAN dynamique précréé en fonction de la configuration en utilisant le mappage WLAN-VLAN existant pour le point d'accès FlexConnect individuel ou en utilisant le mappage ACL-VLAN sur le groupe FlexConnect.Afin de configurer le VLAN AAA sur l'AP FlexConnect, accédez à l'interface utilisateur graphique du WLC > Wireless > FlexConnect Group > cliquez sur le groupe FlexConnect spécifique > VLAN-ACL mapping, et entrez VLAN dans le champ ID de VLAN.

exConnec	t Groups > Edit 'Store	1'	
General	Local Authentication	Image Upgrade	VLAN-ACL mapping
VLAN ACL	Mapping		
Ingress AG			
Egress AC	L none 💌		
	Add		

- 10. Associez un client sur ce WLAN et authentifiez-vous à l'aide du nom d'utilisateur configuré dans le serveur AAA afin de renvoyer le VLAN AAA.
- 11. Le client doit recevoir une adresse IP du VLAN dynamique retourné via le serveur AAA.
- 12. Afin de vérifier, cliquez sur WLC GUI > Monitor > Client > cliquez sur l'adresse MAC du client spécifique afin de vérifier les détails du client.

#### Limites

- Les attributs spécifiques à **Cisco Airespace** ne seront pas pris en charge et l'ID de VLAN d'attribut IETF sera uniquement pris en charge.
- Un maximum de 16 VLAN peuvent être configurés dans la configuration par point d'accès via le mappage WLAN-VLAN pour chaque point d'accès FlexConnect ou en utilisant le mappage ACL-VLAN sur le groupe FlexConnect.

## Commutation centrale basée sur VLAN FlexConnect

Dans les versions 7.2 du logiciel du contrôleur, la substitution AAA de VLAN (affectation de VLAN dynamique) pour les WLAN commutés localement placera les clients sans fil sur le VLAN fourni par le serveur AAA. Si le VLAN fourni par le serveur AAA n'est pas présent sur le point d'accès, le client est placé sur un VLAN WLAN mappé sur ce point d'accès et le trafic bascule localement sur ce VLAN. De plus, avant la version 7.3, le trafic d'un WLAN particulier à partir des points d'accès FlexConnect peut être commuté de manière centralisée ou locale en fonction de la configuration du WLAN.

Àpartir de la version 7.3, le trafic des points d'accès FlexConnect peut être commuté de manière centralisée ou locale en fonction de la présence d'un VLAN sur un point d'accès FlexConnect.



### <u>Résumé</u>

Flux de trafic sur les WLAN configurés pour la commutation locale lorsque les points d'accès flexibles sont en mode connecté :

- Si le VLAN est retourné en tant qu'un des attributs AAA et que le VLAN n'est pas présent dans la base de données Flex AP, le trafic bascule de façon centralisée et le client se verra attribuer ce VLAN/interface retourné par le serveur AAA, à condition que le VLAN existe sur le WLC.
- Si le VLAN est retourné comme l'un des attributs AAA et que le VLAN n'est pas présent dans la base de données Flex AP, le trafic bascule de façon centralisée. Si ce VLAN n'est pas non plus présent sur le WLC, un VLAN/interface mappé à un WLAN sur le WLC sera attribué au client.
- Si le VLAN est retourné en tant qu'un des attributs AAA et que le VLAN est présent dans la base de données des points d'accès FlexConnect, le trafic bascule localement.
- Si le VLAN n'est pas renvoyé par le serveur AAA, un VLAN mappé WLAN est attribué au client sur ce point d'accès FlexConnect et le trafic est commuté localement.

Flux de trafic sur les WLAN configurés pour la commutation locale lorsque les points d'accès flexibles sont en mode autonome :

- Si le VLAN retourné par un serveur AAA n'est pas présent dans la base de données Flex AP, le client sera mis au VLAN par défaut (c'est-à-dire un VLAN mappé WLAN sur Flex AP). Lorsque le point d'accès se connecte de nouveau, ce client sera déauthentifié et commutera le trafic de manière centralisée.
- Si le VLAN retourné par un serveur AAA est présent dans la base de données Flex AP, le client sera placé dans un VLAN retourné et le trafic sera commuté localement.
- Si le VLAN n'est pas renvoyé par un serveur AAA, un VLAN mappé WLAN est attribué au client sur ce point d'accès FlexConnect et le trafic est commuté localement.

#### **Procédure**

Procédez comme suit :

1. Configurez un WLAN pour la commutation locale et activez la substitution AAA.

WLANs > Edit 'Store 1	,
General Security	QoS Advanced
Allow AAA Override	▼ Epabled
Coverage Hole Detection	✓ Enabled
Enable Session Timeout	Session Timeout (secs)
Aironet IE	Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None 💙 IPv6 None 💙
P2P Blocking Action	Disabled
Client Exclusion <sup>3</sup>	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients <sup>g</sup>	0
Static IP Tunneling 💶	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
FlexConnect	
FlexConnect Local Switching <sup>2</sup>	✓ Enabled

2. Activez la commutation centralisée basée sur Vlan sur le WLAN nouvellement créé.

WLANs > Edit 'Store 1	*
General Security	QoS Advanced
Allow AAA Override	Enabled
Coverage Hole Detection	Enabled
Enable Session Timeout	Session Timeout (secs)
Aironet IE	✓Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None 💌 IPv6 None 💌
P2P Blocking Action	Disabled 💌
Client Exclusion <sup>3</sup>	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients <sup>g</sup>	0
Static IP Tunneling 🎞	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
FlexConnect	
FlexConnect Local Switching <mark>2</mark>	Enabled
FlexConnect Local Auth 💶	Enabled
Learn Client IP Address 5	Enabled
Vlan based Central Switching <sup><u>13</u></sup>	Enabled

3. Définissez le mode AP sur

All APs > De	All APs > Details for AP_3500E						
General	Credentials	Interfaces	High Availa	bility			
General							
AP Name	AP.	_3500E					
Location							
AP MAC A	ddress o4:	7d:4f:3a:07:74					
Base Radi	o MAC o4:	7d:4f:53:24:e0					
Admin Sta	tus En	able 💌					
AP Mode	Fle	xConnect 🔽					
AP Sub Mo	ode loc	al ×Connect	and the second se				
Operation	al Status mo	nitor					
Port Numb	er Sn	gue Detector iffer					
Venue Gro	oup SE	dge -Connect	~				

4. Assurez-vous que le point d'accès FlexConnect comporte une sous-interface dans sa base de données, soit via le mappage WLAN-VLAN sur un point d'accès Flex particulier, soit via la configuration du VLAN à partir d'un groupe Flex. Dans cet exemple, le VLAN 63 est configuré dans le mappage WLAN-VLAN sur le point d'accès

uluilu cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY
Wireless	All APs >	AP_3500	DE > VLAN Ma	ppings	
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> <li>802.11a/n</li> </ul>	AP Name Base Radi	o MAC o	AP_3500E x4:7d:4f:53:24:e0		
802.11b/g/n Global Configuration	WLAN Id	SSID			VLAN ID
Advanced	1	Store 1' :			63
Mesh					
RF Profiles	Centrally	switched	Wlans		
FlexConnect Groups FlexConnect ACLs	WLAN Id		SSID	VLAN ID	
▶ 802.11a/n	AP level V	LAN ACL	Mapping		
▶ 802.11b/g/n	Vlan Id	Ingr	ess ACL	Egress A	CL
Media Stream	63	none	• •	none 💌	
Country					
Timers	Group lev	el VLAN A	ACL Mapping		
▶ QoS	¥lan Id	Ingr	ess ACL	Egress A	CL

5. Dans cet exemple, le VLAN 62 est configuré sur le WLC comme une des interfaces dynamiques et n'est pas mappé au WLAN sur le WLC. Le WLAN sur le WLC est mappé au VLAN de gestion (c'est-à-dire au VLAN 61).

ululu cisco	Monitor <u>w</u> lai	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT COM	MMANDS HELP	FEEDBACK
Controller	Interfaces						
General Inventory	Interface Name		LAN Identifier	IP Address	Interface Type	Dynamic AP Ma	inagement
Interfaces	<u>ayn</u> management		52	9.6.62.10	Static	Enabled	<b>M</b>

6. Associez un client au WLAN configuré à l'étape 1 sur ce point d'accès Flex et renvoyez le VLAN 62 à partir du serveur AAA. Le VLAN 62 n'est pas présent sur ce point d'accès flexible, mais il est présent sur le WLC en tant qu'interface dynamique, de sorte que le trafic se commute de façon centralisée et que le client se voit attribuer le VLAN 62 sur le WLC. Dans le résultat capturé ici, le VLAN 62 a été attribué au client et la commutation et l'authentification des données sont définies sur

Central.				
Monitor Summary > Access Points > Cisco CleanAir > Statistics > CDP > Rogues > Redundancy Clients Multicast	Clients > Detail Client Properties MAC Address IPv4 Address IPv6 Address	00:40:96:b0:d4:be 9.6.62.100	AP Properties AP Address AP Name AP Type WLAN Profile Data Switching Authentication Status Association ID 802.11 Authentication	o4:7d:4f:53:24:e0 AP_3500E 802:11a Store 1* Central Central Associated 1 Onen System
			802.11 Authentication	Open System
			Reason Code	3
		i.	Status Code	0
	Client Type	Regular	CF Pollable	Not Implemented
	User Name	betauser	CF Poll Request	Not Implemented
	Port Number	1	Short Preamble	Not Implemented
	Interface	dyn	PBCC	Not Implemented
	VLAN ID	62	Channel Agility	Not Implemented

**Remarque :** observez que bien que le WLAN soit configuré pour la commutation locale, le champ de commutation de données de ce client est Central en fonction de la présence d'un VLAN (c'est-à-dire, VLAN 62, qui est renvoyé du serveur AAA, n'est pas présent dans la base de données AP).

7. Si un autre utilisateur s'associe au même point d'accès sur ce WLAN créé et qu'un certain VLAN est retourné par le serveur AAA qui n'est pas présent sur le point d'accès ainsi que sur le WLC, le trafic bascule de façon centralisée et le client se verra attribuer l'interface mappée WLAN sur le WLC (c'est-à-dire VLAN 61 dans cet exemple de configuration), car le WLAN est mappé à l'interface de gestion configurée pour VLAN 61

Clients > Detail				
Client Properties		AP Pro	perties	
MAC Address	00:40:96:b8:d4:be	AP Ad	Idress	o4:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Na	ime	AP_3500E
IPv6 Address		AP Ty	pe	802.11a
		WLAN	Profile 'Sto	ore 1'
		Data	Switching	Central
		Authe	ntication	Central
		Status	5	Associated
		Assoc	iation ID	1
		802.1	1 Authentication	Open System
		Reaso	on Code	3
	.i	Status	s Code	0
Client Type	Regular	CF Po	llable	Not Implemented
User Name	betauser2	CF Po	ll Request	Not Implemented
Port Number	1	Short	Preamble	Not Implemented
Interface	management	PBCC		Not Implemented
VLAN ID	61	Chanr	nel Agility	Not Implemented

**Remarque :** Notez que bien que le WLAN soit configuré pour la commutation locale, le champ Commutation de données de ce client est Central en fonction de la présence d'un VLAN. Autrement dit, le VLAN 61, qui est retourné par le serveur AAA, n'est pas présent dans la base de données AP mais n'est pas non plus présent dans la base de données WLC. Par conséquent, une interface VLAN/interface par défaut est attribuée au client, qui est mappé au WLAN. Dans cet exemple, le WLAN est mappé à une interface de gestion (c'est-à-dire VLAN 61) et le client a donc reçu une adresse IP du VLAN 61.

8. Si un autre utilisateur s'y associe sur ce WLAN créé et le VLAN 63 est retourné par le serveur AAA (qui est présent sur ce point d'accès flexible), le VLAN 63 sera attribué au client et le trafic sera commuté

#### localement.

Clients > Detail			
<b>Client Properties</b>		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

#### **Limites**

• La commutation centralisée basée sur VLAN est uniquement prise en charge sur les WLAN configurés pour l'authentification centrale et la commutation locale.

 La sous-interface AP (c'est-à-dire, le mappage VLAN) doit être configurée sur l'AP FlexConnect.

# ACL FlexConnect

Avec l'introduction des listes de contrôle d'accès sur FlexConnect, il existe un mécanisme pour répondre au besoin de contrôle d'accès au niveau du point d'accès FlexConnect pour la protection et l'intégrité du trafic de données commutées localement à partir du point d'accès. Les listes de contrôle d'accès FlexConnect sont créées sur le WLC et doivent ensuite être configurées avec le VLAN présent sur le groupe FlexConnect AP ou FlexConnect à l'aide du mappage VLAN-ACL qui sera pour les VLAN de remplacement AAA. Ils sont ensuite repoussés vers le point d'accès.



### Résumé

- Créez une liste de contrôle d'accès FlexConnect sur le contrôleur.
- Appliquez la même chose sur un VLAN présent sur le point d'accès FlexConnect sous le mappage de la liste de contrôle d'accès VLAN au niveau du point d'accès.
- Peut être appliqué sur un VLAN présent dans le groupe FlexConnect sous le mappage VLAN-ACL (généralement fait pour les VLAN écrasés AAA).
- Lors de l'application de la liste de contrôle d'accès sur le VLAN, sélectionnez la direction à appliquer qui sera " " d'entrée, " " de sortie ou " " d'entrée et de sortie.

#### Procédure

Procédez comme suit :

 Créez une liste de contrôle d'accès FlexConnect sur le WLC. Accédez à WLC GUI > Security > Access Control List > FlexConnect ACL.

FlexConnect Access Control Lists	Entries 0 - 0 of 0	New
Acl Name		

- 2. Cliquez sur New.
- 3. Configurez le nom de la liste de contrôle d'accès.

Access Control Lists > N	ew	< Bac	k Apply
Access Control List Name	Flex-ACL-Ingress	]	

- 4. Cliquez sur Apply.
- Créez des règles pour chaque liste de contrôle d'accès. Afin de créer des règles, accédez à WLC GUI > Security > Access Control List > FlexConnect ACL, puis cliquez sur la liste de contrôle d'accès créée cidessus.

Acce	ss Con	trol Lists > Edit						< Back	Add New Rule
Gene Acces	ral s List Name	e Flex-ACL-	Ingress						
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP		
Jeq	HCubii	555172 11 711 12		Trococor					

6. Cliquez sur **Ajouter une nouvelle** règle.

Access Control List	s > Rules > New			< Back	Apply
Sequence	1	10 Address	Nature a de		
Source	IP Address 💌	0.0.0.0	0.0.0.0		
Destination	IP Address 💌	IP Address 0.0.0.0	Netmask 0.0.0.0		
Protocol	Any 💌				
DSCP	Any 💌				
Action	Deny 💌				

**Remarque :** configurez les règles conformément à la condition requise. Si la règle permit any n'est pas configurée à la fin, il y a un refus implicite qui bloquera tout le trafic.

- 7. Une fois les listes de contrôle d'accès FlexConnect créées, elles peuvent être mappées pour le mappage WLAN-VLAN sous un point d'accès FlexConnect individuel ou appliquées sur le mappage VLAN-ACL sur le groupe FlexConnect.
- 8. Mapper la liste de contrôle d'accès FlexConnect configurée ci-dessus au niveau du point d'accès pour les VLAN individuels sous les mappages VLAN pour chaque point d'accès FlexConnect. Naviguez jusqu'à l'interface graphique du WLC > Wireless > All AP > cliquez sur l'AP spécifique > onglet FlexConnect > VLAN Mapping

AP Name		AP3500					
Base Rad	lio MAC	2c:3f:38:f6:98:	Ь0				
WLAN Id	SSID			VLAN ID			
1	Store 1			109			
Centrally	switche	d wians					
Centrally WLAN Id	switche SSID	d Wians		VLAN ID			
Centrally WLAN Id 2	SSID Store 3	d Wians		VLAN ID N/A			
Centrally WLAN Id 2 AP level	SSID Store 3	L Mapping		VLAN ID N/A			
Centrally WLAN Id 2 AP level Vlan Id	SSID Store 3 VLAN AC	L Mapping	Egress ACL	VLAN ID N/A			

9. La liste de contrôle d'accès FlexConnect peut également être appliquée au mappage VLAN-ACL dans le groupe FlexConnect. Les VLAN créés sous le mappage VLAN-ACL dans le groupe FlexConnect sont principalement utilisés pour la substitution VLAN dynamique.

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping
VLAN ACL	Mapping	-	
Vlan Id	0		
Vlan Id Ingress A	ACL Flex-ACL-Egress	]	
Vlan Id Ingress / Egress A	CL Flex-ACL-Egress V		

#### Limites

- Un maximum de 512 listes de contrôle d'accès FlexConnect peut être configuré sur le WLC.
- Chaque liste de contrôle d'accès peut être configurée avec 64 règles.
- Un maximum de 32 listes de contrôle d'accès peut être mappé par groupe FlexConnect ou par point d'accès FlexConnect.
- Àtout moment donné, il y a un maximum de 16 VLAN et 32 ACL sur le point d'accès FlexConnect.

# Tunnellisation fractionnée FlexConnect

Dans les versions de WLC antérieures à la version 7.3, si un client se connectant sur un point d'accès FlexConnect associé à un WLAN à commutation centralisée doit envoyer du trafic à un périphérique présent dans le site/réseau local, il doit envoyer du trafic via CAPWAP au WLC et ensuite récupérer le même trafic vers le site local via CAPWAP ou en utilisant une connectivité hors bande.

Àpartir de la version 7.3, la **tunnellisation fractionnée** introduit un mécanisme par lequel le trafic envoyé par le client sera classifié en fonction du contenu des paquets **utilisant la liste de contrôle d'accès Flex**. Les paquets correspondants sont commutés localement à partir de Flex AP et les autres paquets sont commutés de manière centralisée via CAPWAP.

La fonctionnalité de fractionnement en canaux est un avantage supplémentaire pour la configuration du point d'accès OEAP où les clients sur un SSID d'entreprise peuvent communiquer directement avec des périphériques sur un réseau local (imprimantes, machine filaire sur un port LAN distant ou périphériques sans fil sur un SSID personnel) sans consommer de bande passante WAN en envoyant des paquets sur CAPWAP. La transmission tunnel partagée n'est pas prise en charge sur les points d'accès OEAP 600. Une liste de contrôle d'accès flexible peut être créée avec des règles afin d'autoriser tous les périphériques présents sur le site/réseau local. Lorsque les paquets provenant d'un client sans fil sur le SSID d'entreprise

correspondent aux règles de la liste de contrôle d'accès flexible configurée sur le point d'accès OEAP, ce trafic est commuté localement et le reste du trafic (c'est-à-dire le trafic implicite de refus) passe de manière centralisée sur CAPWAP.

La solution de fractionnement en canaux suppose que le sous-réseau/VLAN associé à un client sur le site central n'est pas présent sur le site local (c'est-à-dire que le trafic des clients qui reçoivent une adresse IP du sous-réseau présent sur le site central ne pourra pas basculer localement). La fonctionnalité de fractionnement en canaux est conçue pour commuter le trafic localement pour les sous-réseaux appartenant au site local afin d'éviter la consommation de bande passante WAN. Le trafic qui correspond aux règles de la liste de contrôle d'accès Flex est commuté localement et le fonctionnement de la NAT est effectué en changeant l'adresse IP source du client en adresse IP d'interface BVI du point d'accès Flex, qui est routable sur le site/réseau local.



### <u>Résumé</u>

- La fonctionnalité de fractionnement en canaux est prise en charge sur les WLAN configurés pour la commutation centrale annoncée par les points d'accès flexibles uniquement.
- Le DHCP requis doit être activé sur les WLAN configurés pour la transmission tunnel partagée.
- La configuration de fractionnement en canaux est appliquée par WLAN configuré pour la commutation centralisée sur chaque point d'accès Flex ou pour tous les points d'accès Flex dans un groupe FlexConnect.

#### **Procédure**

Procédez comme suit :

 Configurez un WLAN pour la commutation centrale (c'est-à-dire que la commutation locale flexible ne doit pas être activée).

WLANs > E	dit 'Store	ə 1'					
General	Security	QoS	Advan	ced			
Allow AA Coverag Enable S Aironet I Diagnost Override P2P Bloc Client Ex Maximur Clients	A Override le Hole Detectio Session Timeout IE tic Channel Interface ACL king Action colusion <sup>2</sup> m Allowed	Disab	abled abled 00 sssion Time bled bled bled bled fied bled	eout (s	ecs) Value (sec	IPv6 None	~
Wi-Fi Dir Policy	ect Clients	Disab	led 💌				
Maximur Clients P	n Allowed Per AP Radio	200		:	Flex Loo should no	cal Switching ot be enable	g ed
FlexConne	ct			~			
FlexCon Switchin	nect Local g ²		Enabled				

2. Définissez l'attribution d'adresse DHCP sur

### Obligatoire.

Obligatoli C.				
WLANs > Edit 'Store 1	* (			
Court Courts	A.C. Marriel			
General Security	QoS Advanced			
Allow AAA Override	E contrat		DUCD.	
Allow AAA OTCITIGE			DHCP	
Coverage Hole Detection	🗹 Enabled		DHCP Server	Override
Enable Session Timeout	1800			
	Session Timeout (secs)		DHCP Addr. Assignment	V Required
Aircrat IE			errer rieurrizzigniteit.	C Required
Alloliet IC	Enabled		Management Frame Prote	ction (MFP)
Diagnostic Channel	Enabled			
Override Interface ACL	IPv4 None 💌	IPv6 None 💌	MFP Client Protection 🔮	Optional 💌

3. Définissez le mode AP sur

All APs > De	tails for AP_3	3500E		
General	Credentials	Interfaces	High Availa	bility
General				
AP Name	AP.	_3500E		
Location				
AP MAC A	ddress o4:	7d:4f:3a:07:74		
Base Radio	MAC 04:	7d:4f:53:24:e0		
Admin Sta	tus En	able 💌		
AP Mode	Fle	xConnect 🔽		
AP Sub Mo	de loc	al ×Connect	and the second se	
Operationa	al Status mo	nitor		
Port Numb	er Sn	gue Detector iffer		
Venue Gro	up SE	age -Connect	~	

4. Configurez la liste de contrôle d'accès FlexConnect avec une règle d'autorisation pour le trafic qui doit être commuté localement sur le WLAN du commutateur central. Dans cet exemple, la règle de liste de contrôle d'accès FlexConnect est configurée de sorte qu'elle avertit le trafic ICMP de tous les clients qui se trouvent sur le sous-réseau 9.6.61.0 (c'est-à-dire qui existent sur le site central) vers 9.1.0.150 pour qu'il soit commuté localement après l'application de l'opération NAT sur le point d'accès Flex. Le reste du trafic va atteindre une règle implicite de refus et être commuté de manière centralisée via CAPWAP.

cisco	MONI	TOR	<u>W</u> LANs		LER	WIRELESS	şe	CURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Wireless	Acce	ess Co	ntrol Li	ists > Edit								
Access Points     All APs     Radios	Gene	eral										
802.11a/n 802.11b/g/n	Acces	s List Na	me	Fle	x-AC	L						
Global Configuration	Seq	Action	Sour	ce IP/Masi	D I	estination P/Mask	1	Protocol	Source Port	Dest Port	DSCP	
Mesh	1	Permit	9.6.6 255.2	1.0	/ 9	.1.0.150 55.255.255	1	ICMP	Any	Any	Any	
RF Profiles FlexConnect Groups FlexConnect ACLs												

5. Cette liste de contrôle d'accès FlexConnect créée peut être poussée en tant que liste de contrôle d'accès à tunnel partagé vers un point d'accès Flex individuel ou peut également être poussée vers tous les points d'accès Flex dans un groupe Flex Connect.Complétez ces étapes afin de pousser la liste de contrôle d'accès flexible en tant que liste de contrôle d'accès partagée locale vers chaque point d'accès flexible :Cliquez sur Listes de contrôle d'accès divisées locales.



Sélectionnez WLAN Id sur lequel la fonction Split Tunnel doit être activée, choisissez Flex-ACL, puis cliquez sur

All APs > AP_3500E > ACL Mapp	ings
AP Name AP_3500E	
Base Radio MAC 04:7d:4f:53:24:e0	
WLAN ACL Mapping	Enter WLAN ID on which Split Tunnel should be enabled
WLAN Id 1	
Local-Split ACL Flex-ACL S	Click Add after selecting Flex ACL
WLAN Id WLAN Profile Name	Local-Split ACL

Flex-ACL est envoyé en tant que Local-Split ACL au point d'accès

AP Name		AP_3500E	
Base Rad	io MAC	o4:7d:4f:53:24:e0	D
WLAN I Local-Si	d [ plit ACL [	0 Flex-ACL 💌	
	1	Add	
WLAN Id		Add rofile Name	Local-Split AC

Complétez ces étapes afin de pousser la liste de contrôle d'accès flexible en tant que liste de contrôle d'accès partagée locale vers un groupe FlexConnect :Sélectionnez l'ID WLAN sur lequel la fonction de fractionnement en canaux doit être activée. Dans l'onglet **WLAN-ACL mapping**, sélectionnez FlexConnect ACL dans le groupe FlexConnect où des points d'accès Flex particuliers sont ajoutés, puis cliquez sur

Add.						
Wireless	FlexConnect Groups > Edit	Flex-Group'				
Access Points     All APs     Pador	General Local Authentication	Image Upgrade	AAA YLAN-ACL mapping	WLAN-ACL	mapping V	VebPolicies
802.11a/n 802.11b/g/n Global Configuration	Web Auth ACL Mapping		Local Split ACL Map	ping	Enter WLAN ID	on which Split
Advanced				-	Tunnel should be	e enabled
Mesh	WLAN IG 0		WLAN 10 1			
RF Profiles FlexConnect Groups	Add		Local Spirt ACL	Hex-ACL	Click ADD after ACL	selecting Flex
▶ 802.11a/n	WLAN Id WLAN Profile Name	WebAuth ACL	WLAN Id WLAN I	rofile Name	LocalSpl	IR ACL

La Flex-ACL est envoyée en tant que LocalSplit ACL aux AP Flex dans ce groupe Flex.

Wireless	FlexConnect Groups > Edit	Flex-Group'			
Access Points     All APs     Radios	General Local Authentication	Image Upgrade	AAA VLAN-ACL mapping	WLAN-ACL mapping	WebPolicies
802.114/n 802.11b/g/n Global Configuration	Web Auth ACL Mapping		Local Split ACL Map	ping	
Mesh RF Profiles	WLAN ID 0 WebAuth ACL Plex-ACL V		WLAN Id 0 Local Split ACL	Flex-ACL M	
FlexConnect Groups FlexConnect ACLs	Add		Ad	4	
▶ 802.11a/n ▶ 802.11b/g/n	WLAN Id WLAN Profile Name	WebAuth ACL	1 Store	Profile Name Local	Flex-ACL V

### **Limites**

- Les règles de liste de contrôle d'accès flexible ne doivent pas être configurées avec l'instruction permit/deny avec le même sous-réseau que la source et la destination.
- Le trafic sur un WLAN à commutation centralisée configuré pour la transmission tunnel partagée ne peut être commuté localement que lorsqu'un client sans fil initie le trafic pour un hôte présent sur le site local. Si le trafic est initié par des clients/hôtes sur un site local pour des clients sans fil sur ces WLAN configurés, il ne pourra pas atteindre la destination.
- La transmission tunnel partagée n'est pas prise en charge pour le trafic multidiffusion/diffusion. Le trafic multidiffusion/diffusion bascule de manière centralisée même s'il correspond à la liste de contrôle d'accès Flex.

## Tolérance aux pannes

La tolérance aux pannes FlexConnect permet l'accès sans fil et les services aux clients des filiales lorsque :

- Les points d'accès FlexConnect Branch perdent la connectivité avec le contrôleur Flex 7500 principal.
- Les points d'accès FlexConnect Branch passent au contrôleur Flex 7500 secondaire.
- Les points d'accès FlexConnect Branch rétablissent la connexion au contrôleur Flex 7500 principal.

La tolérance aux pannes FlexConnect, ainsi que le protocole EAP local, comme indiqué ci-dessus, garantissent un temps d'arrêt zéro pour les filiales lors d'une panne de réseau. Cette fonctionnalité est activée par défaut et ne peut pas être désactivée. Il ne nécessite aucune configuration sur le contrôleur ou le point d'accès. Toutefois, pour garantir que la tolérance aux pannes fonctionne correctement et est applicable, il convient de maintenir ces critères :

- Les commandes et les configurations WLAN doivent être identiques sur les contrôleurs Flex 7500 principal et de secours.
- Le mappage VLAN doit être identique sur les contrôleurs Flex 7500 principal et de secours.
- Le nom de domaine de mobilité doit être identique sur les contrôleurs Flex 7500 principal et de secours.
- Il est recommandé d'utiliser Flex 7500 comme contrôleurs principal et de secours.

### <u>Résumé</u>

- FlexConnect ne déconnecte pas les clients lorsque le point d'accès se connecte de nouveau au même contrôleur, à condition qu'il n'y ait aucun changement de configuration sur le contrôleur.
- FlexConnect ne déconnecte pas les clients lors de la connexion au contrôleur de sauvegarde, à condition qu'il n'y ait aucune modification dans la configuration et que le contrôleur de sauvegarde soit identique au contrôleur principal.
- FlexConnect ne réinitialisera pas ses radios lors de la connexion au contrôleur principal, à condition qu'il n'y ait aucun changement dans la configuration du contrôleur.

### **Limites**

- Pris en charge uniquement pour FlexConnect avec authentification centrale/locale avec commutation locale.
- Les clients authentifiés de manière centralisée nécessitent une réauthentification complète si le minuteur de session client expire avant que l'AP FlexConnect passe du mode autonome au mode connecté.
- Les contrôleurs principaux et de sauvegarde Flex 7500 doivent se trouver dans le même domaine de mobilité.

# Limite client par WLAN

Parallèlement à la segmentation du trafic, il est nécessaire de restreindre l'accès total des clients aux services sans fil.

**Exemple :** Limitation du nombre total de clients invités à partir de la tunnellisation des filiales vers le data center.

Pour relever ce défi, Cisco introduit une fonctionnalité Client Limit par WLAN qui peut limiter le nombre total de clients autorisés par WLAN.

#### **Objectif principal**

- Définir des limites sur le nombre maximal de clients
- Facilité opérationnelle

Remarque : il ne s'agit pas d'une forme de QoS.

Par défaut, la fonction est désactivée et ne force pas la limite.

#### **Limites**

Cette fonctionnalité n'applique pas de limite de client lorsque FlexConnect est en état de fonctionnement autonome.

### Configuration WLC

Procédez comme suit :

1. Sélectionnez l'ID WLAN à commutation centralisée 1 avec SSID DataCenter. Ce WLAN a

été créé lors de la création du groupe AP. Voir la figure 8.

- 2. Cliquez sur l'onglet Avancé pour WLAN ID 1.
- 3. Définissez la valeur limite du client pour le champ de texte Maximum Allowed Clients.
- 4. Cliquez sur Apply après avoir défini le champ de texte pour Maximum Allowed

#### Clients.

Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection	Enabled	DHCP Server Override	-
Enable Session Timeout Aironet IE Diagnostic Channel	Session Timeout (secs)	DHCP Addr. Assignment  Required Nanagement Frame Protection (MFP)	
IPv6 Enable 2		MFP Client Protection 💈 Optional 💌	
Override Interface ACL	None 💌	DTIM Period (in beacon intervals)	
P2P Blocking Action	Disabled 💌		
Client Exclusion 2	Enabled 60 Timeout Value (secs)	802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1	
Maximum Allowed Clients <sup>9</sup>	0	NAC	
ff Channel Scanning Defe	or	NAC OOB State Enabled	
Scan Defer Priority	0 1 2 3 4 5 6 7	Posture State Enabled	
L		Client Load Balancing	
Scan Defer Time(msecs)	100	Client Band Select <sup>g</sup>	
			>

La valeur par défaut pour Maximum Allowed Clients est 0, ce qui signifie qu'il n'y a aucune restriction et que la fonctionnalité est désactivée.

#### **Configuration NCS**

Afin d'activer cette fonctionnalité à partir de NCS, accédez à Configurer > Contrôleurs > IP du contrôleur > WLAN > Configuration WLAN > Détails de configuration WLAN.

WLAN Configuration Deta	ils : 17	
Configure > Controllers > 172.20.225	5.154 > WLANs > WLAN Configuration > 🛚	ILAN Configuration Details
General Security QoS	Advanced	
FlexConnect Local Switching	Enable	DHCP
FlexConnect Local Auth 🔍	Enable	<u></u>
Learn Client IP Address	🗌 Enable	DHCP Server
Session Timeout	Enable 1800 (secs)	DHCP Address Assignment
Coverage Hole Detection	🗹 Enable	Management Frame Protecti
Aironet IE	🗹 Enable	management rame rrotecti
IPv6 ∠	🔲 Enable	MED Client Distantion of
Diagnostic Channel 🙎	🔲 Enable	MFP Client Protection 2
Override Interface ACL	IPv4 NONE	MFP Version
	IPv6 NONE	Load Balancing and Band Se
Peer to Peer Blocking 🔍	Disable	
Wi-Fi Direct Clients Policy	Disabled 🗸	Client Load Balancing
Client Exclusion 🕹	🗹 Enable	Client Band Select
Timeout Value	60 (secs)	
Maximum Clients 🔍	0	NAC

## Blocage peer-to-peer

Dans les versions logicielles du contrôleur antérieures à la version 7.2, le blocage P2P (peer-topeer) n'était pris en charge que pour les WLAN de commutation centrale. Le blocage peer-to-peer peut être configuré sur un WLAN avec l'une des trois actions suivantes :

- Désactivé Désactive le blocage peer-to-peer et le trafic ponté localement au sein du contrôleur pour les clients du même sous-réseau. C'est la valeur par défaut.
- Drop : entraîne le contrôleur à rejeter les paquets pour les clients du même sous-réseau.
- Forward Up-Stream Entraîne le transfert du paquet sur le VLAN en amont. Les périphériques situés au-dessus du contrôleur décident des actions à entreprendre concernant le paquet.

Àpartir de la version 7.2, le blocage peer-to-peer est pris en charge pour les clients associés au WLAN de commutation locale. Par WLAN, la configuration peer-to-peer est poussée par le contrôleur vers l'AP FlexConnect.



### Résumé

- Le blocage peer-to-peer est configuré par WLAN
- Par WLAN, la configuration de blocage peer to peer est poussée par le WLC vers les points d'accès FlexConnect.
- L'action de blocage peer-to-peer configurée en tant que drop ou amont-forward sur le WLAN est traitée comme un blocage peer-to-peer activé sur l'AP FlexConnect.

### Procédure

Procédez comme suit :

1. Activez l'action de blocage peer-to-peer comme **Drop** sur le WLAN configuré pour la commutation locale

F	lexC	20	onr	ne	ct.
					-

WLANs > Edit 'Storel'	
General Security QoS Advanced	
Aironet IE Enabled	Management Frame Protection (MFP)
Diagnostic Channel Enabled Override Interface ACL IPv4 None  IPv6	MFP Client Protection & Optional
Client Exclusion 2 Client Enabled 60 Timeout Value (secs)	802.11a/n (1 - 255) 1
Static IP Tunneling 44 Enabled	802.11b/g/n (1 - 255) 1 NAC
Wi-Fi Direct Clients Policy Disabled M Off Channel Scanning Defer	NAC State None V Load Balancing and Band Select
Scan Defer Priority 0 1 2 3 4 5 6 7	Client Load Balancing Client Band Select Z
Scan Defer Time 100	Passive Client
lexConnect	Voice
FlexConnect Local Switching 2 Enabled	Media Session Snooping Enabled

2. Une fois que l'action de blocage P2P est configurée comme Drop ou Forward-Upstream sur le WLAN configuré pour la commutation locale, elle est poussée du WLC vers l'AP FlexConnect. Les points d'accès FlexConnect stockeront ces informations dans le fichier de configuration de la mémoire flash. Avec cela, même lorsque l'AP FlexConnect est en mode autonome, il peut appliquer la configuration P2P sur les sous-interfaces correspondantes.

### Limites

- Dans FlexConnect, la configuration de blocage P2P de la solution ne peut pas être appliquée uniquement à un point d'accès FlexConnect ou à un sous-ensemble d'AP particulier. Il est appliqué à tous les AP FlexConnect qui diffusent le SSID.
- La solution unifiée pour les clients de commutation centralisée prend en charge P2P amontaval. Cependant, cela ne sera pas pris en charge dans la solution FlexConnect. Ceci est traité comme une perte P2P et les paquets client sont abandonnés au lieu d'être transférés au noeud réseau suivant.
- La solution unifiée pour les clients de commutation centralisée prend en charge le blocage P2P pour les clients associés à différents points d'accès. Cependant, cette solution cible uniquement les clients connectés au même point d'accès. Les listes de contrôle d'accès FlexConnect peuvent être utilisées comme solution de contournement pour cette limitation.

## Téléchargement de préimage AP

Cette fonctionnalité permet au point d'accès de télécharger du code pendant qu'il est opérationnel. Le téléchargement pré-image AP est extrêmement utile pour réduire les temps d'indisponibilité du réseau lors de la maintenance ou des mises à niveau logicielles.

### <u>Résumé</u>

- Facilité de gestion logicielle
- Planifier les mises à niveau par magasin : Le NCS est nécessaire à cette fin
- Réduction des temps d'arrêt

#### **Procédure**

Procédez comme suit :

1. Mettez à niveau l'image sur les contrôleurs principal et de sauvegarde.Naviguez sous Interface graphique utilisateur du WLC > Commandes > Download File pour démarrer le Download file to Controller

	File Type	Code
	Server Details	TFTP M
	IP Address	
	Maximum retries	10
	Timeout (seconds)	6
	File Path	
téléchargement.	File Name	AS_\$\$00_7_0_112_\$2.aes

- 2. Enregistrez les configurations sur les contrôleurs, mais ne redémarrez pas le contrôleur.
- 3. Émettez la commande de téléchargement pré-image AP à partir du contrôleur principal.Accédez à WLC GUI > Wireless > Access Points > All APs et choisissez le point d'accès pour démarrer le téléchargement pré-image.Une fois le point d'accès choisi, cliquez sur l'onglet Avancé.Cliquez sur Télécharger principal pour lancer le téléchargement pré-



4. Redémarrez les contrôleurs une fois toutes les images AP téléchargées.Les points d'accès repassent en mode autonome jusqu'à ce que les contrôleurs redémarrent. Remarque : En mode autonome, la tolérance aux pannes conservera l'association des clients.Une fois le contrôleur de retour, les points d'accès redémarrent automatiquement avec l'image prétéléchargée.Après le redémarrage, les points d'accès rejoignent le contrôleur principal et reprennent les services du client.

#### **Limites**

• Fonctionne uniquement avec les AP CAPWAP.

## Mise à niveau d'image FlexConnect Smart AP

La fonctionnalité de prétéléchargement d'image réduit la durée d'indisponibilité dans une certaine mesure, mais tous les points d'accès FlexConnect doivent encore prétélécharger les images AP respectives sur la liaison WAN avec une latence plus élevée.

La mise à niveau efficace des images AP réduira les temps d'arrêt pour chaque AP FlexConnect. L'idée de base est qu'un seul point d'accès de chaque modèle AP téléchargera l'image à partir du contrôleur et agira comme maître/serveur, et le reste des points d'accès du même modèle fonctionnera comme esclave/client et prétéléchargera l'image AP à partir du maître. La distribution de l'image AP du serveur au client se fera sur un réseau local et ne connaîtra pas la latence de la liaison WAN. En conséquence, le processus sera plus rapide.



#### Résumé

- Les points d'accès maître et esclave sont sélectionnés pour chaque modèle de point d'accès par groupe FlexConnect
- Image de téléchargement maître à partir du WLC
- Image de téléchargement d'esclave à partir du point d'accès maître
- Réduit les temps d'arrêt et économise la bande passante WAN

### Procédure

Procédez comme suit :

1. Mettez à niveau l'image sur le contrôleur.Accédez à WLC GUI > Commandes > Download File afin de commencer le

Download file to Controller	
File Type	Code 💌
Transfer Mode	TFTP 🗸
Server Details	
IP Address	
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_2_1_72.aes

téléchargement.

- 2. Enregistrez les configurations sur les contrôleurs, mais ne redémarrez pas le contrôleur.
- Ajoutez les points d'accès FlexConnect au groupe FlexConnect.Naviguez jusqu'à l'interface graphique du WLC > Wireless > FlexConnect Groups > sélectionnez FlexConnect Group > General tab > Add

AP.

enerai	Local Authentication	Image Upgrade	VLAN-ACL mapping	
Group N	ame Store 1			
lexCon	nect APs		АЛА	
dd AP			Primary Radius Server None	*
Select A	Ps from current controller	2	Secondary Radius Server None	*
			Enable AP Local Authentication 2	
AP Nam	e	AR3500		

 4. Cliquez sur la case FlexConnect AP Upgrade afin d'obtenir une mise à niveau efficace de l'image AP.Naviguez jusqu'à l'interface graphique du WLC > Wireless > FlexConnect Groups > sélectionnez FlexConnect Group > Image Upgrade.

FlexConnect G	roups > 'Store 1'		
General Lo	cal Authentication	Image Upgrade	VLAN-ACL mapping
FlexConnect Al	P Upgrade		
AP Name	AP3500	•	
Add Master Master AP Nar	ne AP Model	Manual	

5. Le point d'accès maître peut être sélectionné manuellement ou automatiquement :Afin de sélectionner manuellement le point d'accès maître, naviguez jusqu'à l'interface utilisateur graphique du WLC > Wireless > FlexConnect Groups > sélectionnez FlexConnect Group > Image Upgrade tab > FlexConnect Master APs, sélectionnez AP dans la liste déroulante, puis cliquez sur Add

Master.

eneral	Local Authentica	tion Image Upgr	ade VLAN-ACL mappin	g
lexConnec	AP Upgrade			
Slave Maxir	num Retry Count	44		
Uporade Im	ace	Backup 💌	FlexConnect Upgrade	
exConne	ct Master APs			
exConne	AR3500	×		
AP Name Add Mast	AR3500	~		
AP Name Add Mast	er lame	AP Model	Manual	

**Remarque :** un seul AP par modèle peut être configuré en tant qu'AP maître. Si l'AP maître est configuré manuellement, le champ Manual sera mis à jour comme **yes**. Afin de sélectionner automatiquement le point d'accès maître, naviguez jusqu'à l'interface utilisateur graphique du WLC > Wireless > FlexConnect Groups > sélectionnez **FlexConnect Group > Image Upgrade** tab, puis cliquez sur **FlexConnect Upgrade**.

Local Addientic	ation Image Upg	rade VLAN-ACL mapping	
FlexConnect AP Upgrade Slave Maximum Retry Count Upgrade Image	44 Backup 💌	FlexConnect Upgrade	
	~		
AP Name AP3500-1 Add Master			
AP Name AP3500-1 Add Master Master AP Name	AP Model	Manual	

**Remarque :** si l'AP maître est sélectionné automatiquement, le champ Manual sera mis à jour comme **non**.

6. Afin de démarrer une mise à niveau efficace de l'image AP pour tous les AP sous un groupe FlexConnect spécifique, cliquez sur Mise à niveau FlexConnect.Naviguez jusqu'à l'interface graphique du WLC > Wireless > FlexConnect Groups > sélectionnez FlexConnect group > Image Upgrade tab, puis cliquez sur FlexConnect Upgrade.

xConne	ct Groups > Edit	'Store '	1'			
eneral	Local Authentica	tion	Image Upg	rade	VLAN-ACL mapping	
FlexConne	ect AP Upgrade 🕑					
Slave Ma	ximum Retry Count	44				
				1000000	class can a dura a da	- 1

**Note :** Nombre maximal de tentatives d'esclave est le nombre de tentatives (44 par défaut) dans lesquelles l'AP esclave fera afin de télécharger une image à partir de l'AP maître, après quoi il retombera pour télécharger l'image à partir du WLC. Il fera 20 tentatives contre le WLC afin de télécharger une nouvelle image après quoi l'administrateur doit relancer le processus de téléchargement.

7. Une fois la mise à niveau FlexConnect lancée, seul le point d'accès maître téléchargera l'image à partir du WLC. Sous la page Tous les points d'accès, " rôle de mise à niveau " sera mis à jour en tant que maître/central, ce qui signifie que le point d'accès maître a téléchargé l'image à partir du WLC qui se trouve à l'emplacement central. Le point d'accès esclave téléchargera l'image à partir du point d'accès maître qui se trouve sur le site local et est la raison sous All AP page " Upgrade Role " sera mise à jour en tant que Esclave/Local.Afin de vérifier cela, accédez à WLC GUI > Wireless.

AP Name	AP Model	АР МАС	Download Status	Upgrade Role (Master/Slave)
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

8. Redémarrez les contrôleurs une fois toutes les images AP téléchargées. Les points d'accès repassent en mode autonome jusqu'à ce que les contrôleurs redémarrent. Remarque : En mode autonome, la tolérance aux pannes conservera l'association des clients. Une fois le contrôleur de retour, les points d'accès redémarrent automatiquement avec l'image prétéléchargée. Après le redémarrage, les points d'accès rejoignent le contrôleur principal et reprennent les services du client.

### Limites

- La sélection du point d'accès principal est par groupe FlexConnect et par modèle AP dans chaque groupe.
- Seuls 3 points d'accès esclaves du même modèle peuvent effectuer une mise à niveau simultanée à partir de leur point d'accès maître et les autres points d'accès esclaves utiliseront le compteur de temporisation aléatoire pour réessayer pour le point d'accès maître afin de télécharger l'image du point d'accès.
- Dans le cas où l'AP esclave ne parvient pas à télécharger l'image à partir de l'AP maître pour une raison quelconque, il ira au WLC afin de récupérer la nouvelle image.
- Cela fonctionne uniquement avec les AP CAPWAP.

# Convertir automatiquement les points d'accès en mode FlexConnect

Le Flex 7500 fournit les deux options suivantes pour convertir le mode AP en FlexConnect :

- Mode manuel
- Mode de conversion automatique

### Mode manuel

Ce mode est disponible sur toutes les plates-formes et permet la modification uniquement sur la base de chaque point d'accès.

- 1. Accédez à WLC GUI > Wireless > All APs et choisissez AP.
- 2. Sélectionnez FlexConnect comme mode AP, puis cliquez sur Apply.
- 3. La modification du mode AP entraîne le redémarrage de

### All APs > Details for AP3500

anaral		
eneral		
AP Name	AP3500	
Location	default location	
AP MAC Address	00:22:90:e3:37:df	
Base Radio MAC	00:22:bd:d1:71:30	
Admin Status	Disable 👻	
AP Mode	local 👻	
AP Sub Mode	local	
Operational Status	monitor Reque Detector	
Port Number	Sniffer	
	Bridge	

option est également disponible sur toutes les plates-formes WLC actuelles.

#### Mode de conversion automatique

Ce mode n'est disponible que pour le contrôleur Flex 7500 et n'est pris en charge qu'à l'aide de l'interface de ligne de commande. Ce mode déclenche la modification sur tous les AP connectés. Il est recommandé que Flex 7500 soit déployé dans un domaine de mobilité différent de celui des contrôleurs de campus WLC existants avant d'activer cette CLI :

(Cisco Controller) >config ap autoconvert ?						
disable	Disables auto conversion of unsupported mode APs to supported modes when AP joins					
flexconnect monitor	Converts unsupported mode APs to flexconnect mode when AP joins Converts unsupported mode APs to monitor mode when AP joins					

(Cisco Controller) >

1. La fonction de conversion automatique est désactivée par défaut, qui peut être vérifiée à l'aide de cette commande **show** :

(Cisco Controller) >**show ap autoconvert** 

AP Autoconvert ..... Disabled Modes AP non pris en charge = Local Mode, Sniffer, Rogue Detector et

AP Mode	FlexConnect
AP Sub Mode	local
Operational Status	monitor
Operational Status	Rogue Detector
Port Number	Sniffer
Venue Group	SE-Connect

#### Bridge.

option est actuellement disponible uniquement via les CLI.Ces CLI sont disponibles uniquement sur le WLC 7500.

2. En exécutant **config ap autoconvert flexconnect** CLI, tous les points d'accès du réseau sont convertis en mode FlexConnect en mode AP non pris en charge. Les points d'accès qui sont déjà en mode FlexConnect ou Monitor ne sont pas affectés. (Cisco Controller) >config ap autoconvert flexconnect

(Cisco Controller) >**show ap autoconvert** AP Autoconvert ...... FlexConnect

(Cisco Controller) >

3. L'exécution de **config ap autoconvert monitor** CLI convertit tous les points d'accès du réseau avec le mode AP non pris en charge en mode Surveillance. Les points d'accès qui sont déjà en mode FlexConnect ou Monitor ne sont pas affectés. (Cisco Controller >config ap autoconvert monitor

(Cisco Controller) >**show ap autoconvert** 

AP Autoconvert ..... Monitor

Il n'existe aucune option permettant d'exécuter à la fois **config ap autoconvertflexconnect** et **config ap autoconvert monitor** en même temps.

## Prise en charge FlexConnect WGB/uWGB pour les WLAN de commutation locale

Àpartir de la version 7.3, les clients WGB/uWGB et filaires/sans fil derrière les WGB sont pris en charge et fonctionneront comme des clients normaux sur les WLAN configurés pour la commutation locale.

Après association, WGB envoie des messages IAPP pour chacun de ses clients filaires/sans fil, et Flex AP se comporte comme suit :

- Lorsque le point d'accès flexible est en mode connecté, il transfère tous les messages IAPP au contrôleur et le contrôleur traite les messages IAPP de la même manière que le point d'accès en mode local. Le trafic des clients filaires/sans fil sera commuté localement à partir des points d'accès Flex.
- Lorsque le point d'accès est en mode autonome, il traite les messages IAPP, les clients filaires/sans fil du WGB doivent pouvoir s'enregistrer et se désinscrire. Lors de la transition vers le mode connecté, Flex AP renvoie les informations des clients filaires au contrôleur.
   WGB enverra des messages d'enregistrement trois fois lorsque Flex AP passe du mode

autonome au mode connecté.

Les clients filaires/sans fil hériteront de la configuration de WGB, ce qui signifie qu'aucune configuration distincte comme l'authentification AAA, le remplacement AAA et la liste de contrôle d'accès FlexConnect n'est requise pour les clients derrière WGB.



### <u>Résumé</u>

- Aucune configuration spéciale n'est requise sur le WLC afin de prendre en charge le WGB sur l'AP Flex.
- La tolérance aux pannes est prise en charge pour WGB et les clients derrière WGB.
- WGB est pris en charge sur un AP IOS : 1240, 1130, 1140, 1260 et 1250.

#### **Procédure**

Procédez comme suit :

 Aucune configuration spéciale n'est nécessaire pour activer la prise en charge WGB/uWGB sur les points d'accès FlexConnect pour les WLAN configurés pour la commutation locale en tant que WGB. En outre, les clients derrière WGB sont traités comme des clients normaux sur les WLAN configurés par commutation locale par les points d'accès Flex. Activez la commutation locale FlexConnect sur un WLAN.

WLANs > E	dit 'Store	1'					
General	Security	QoS	Advan	ced			
Allow AA Coverag Enable S Aironet I Diagnost Override	A Override e Hole Detectio ession Timeout E ic Channel Interface ACL	□ Ena □ Ena □ 180 Se □ Ena IPv4 □ Dicob	abled abled oo ssion Tim bled bled None 💌	eout (se	ecs)	IPv6	None 💌
Client Ex Maximun Clients <sup>g</sup>	clusion <sup>3</sup> n Allowed	✓Ena 0	bled 60 Ti	) meout V	alue (secs	)	
Static IP Wi-Fi Din Policy Maximum	Tunneling 👭 ect Clients	Disab	bled led 💌				
Clients P Clear Ho Configure FlexConne	er AP Radio tSpot ation ct	200	bled				
FlexConr Switching	nect Local		Enabled				

2. Définissez le mode AP sur

All APs > D	All APs > Details for AP_3500E									
General	Credentials	Interfaces	High Availa	bility						
General										
AP Name	AP	_3500E								
Location										
AP MAC	Address o4	:7d:4f:3a:07:74								
Base Ra	dio MAC o4	:7d:4f:53:24:e0								
Admin S	tatus En	able 💌								
AP Mode	Fle	xConnect 🔽								
AP Sub N	1ode loc	cal exConnect	and the second se							
Operatio	nal Status m	onitor								
Port Num	nber Sr	iffer								
Venue G	roup Br	idge -Connect	~							

3. Associez le WGB aux clients filaires derrière ce WLAN configuré.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK				
Clients												
Current Fil	lter	None	[Change Filte	r] [Clear Filter	]							
Client MA	C Addr	AP Name		WLAN	Profile	WLAN SSID		Protocol	Status	Auth	Port	WGB
00:40:96:	8:d4:be	AP_3500E		*Stor	e 1'	'Store 1'		N/A	Associated	Yes	1	No
00:50:b6:0	19:e5:3b	AP_3500E		"Stor	re 1"	"Store 1"		N/A	Associated	Yes	1	No
o4:7d:4f:3	ia:08:10	AP 3500E		*Stor	re 1'	'Store 1'		802.11an	Associated	Yes	1	Yes

 Afin de vérifier les détails de WGB, accédez à Monitor > Clients, et sélectionnez WGB dans la liste des clients.

Clients > Detail			
Client Properties		AP Properties	
MAC Address	o4:7d:4f:3a:08:10	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.102	AP Name	AP_3500E
IPv6 Address		AP Type	802.11an
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authenticatio	n Open System
		Reason Code	1
		: Status Code	0
Client Type	WGB	CF Pollable	Not Implemented
Number of Wired Cli	ent(s) 2	CF Poll Request	Not Implemented

 Afin de vérifier les détails des clients filaires/sans fil derrière WGB, accédez à Monitor > Clients, et sélectionnez le

client.			
Clients > Detail			
Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	0
		802.11 Authentication	Open System
		Reason Code	1
		: Status Code	0
Client Type	WGB Client	CF Pollable	Not Implemented
WGB MAC Address	o4:7d:4f:3a:08:10	CF Poll Request	Not Implemented

#### **Limites**

- Les clients filaires derrière WGB seront toujours sur le même VLAN que WGN lui-même. La prise en charge de plusieurs VLAN pour les clients derrière WGB n'est pas prise en charge sur Flex AP pour les WLAN configurés pour la commutation locale.
- Un maximum de 20 clients (filaires/sans fil) sont pris en charge derrière WGB lorsqu'ils sont associés à Flex AP sur WLAN configuré pour la commutation locale. Ce nombre est identique à ce que nous avons aujourd'hui pour la prise en charge de WGB sur le point d'accès en

mode local.

• L'authentification Web n'est pas prise en charge pour les clients derrière le WGB associés aux WLAN configurés pour la commutation locale.

## Prise en charge d'un nombre accru de serveurs Radius

Avant la version 7.4, la configuration des serveurs RADIUS au niveau du groupe FlexConnect était effectuée à partir d'une liste globale de serveurs RADIUS sur le contrôleur. Le nombre maximal de serveurs RADIUS pouvant être configurés dans cette liste globale est de 17. Avec un nombre croissant de filiales, il est nécessaire de pouvoir configurer un serveur RADIUS par site de filiale. À partir de la version 7.4, il sera possible de configurer les serveurs RADIUS principal et de sauvegarde par groupe FlexConnect qui peuvent ou non faire partie de la liste globale de 17 serveurs d'authentification RADIUS configurés sur le contrôleur.

Une configuration spécifique à un point d'accès pour les serveurs RADIUS sera également prise en charge. La configuration spécifique au point d'accès aura une priorité plus grande que la configuration du groupe FlexConnect.

La commande de configuration existante au niveau du groupe FlexConnect, qui nécessite l'index du serveur RADIUS dans la liste de serveurs RADIUS globaux sur le contrôleur, sera désapprouvée et remplacée par une commande de configuration, qui configure un serveur RADIUS au niveau du groupe Flexconnect en utilisant l'adresse IP du serveur et le secret partagé.

#### <u>Résumé</u>

- Prise en charge de la configuration des serveurs RADIUS principal et de sauvegarde par groupe FlexConnect, qui peuvent ou non figurer dans la liste globale des serveurs d'authentification RADIUS.
- Le nombre maximal de serveurs RADIUS uniques pouvant être ajoutés sur un WLC est le nombre de groupes FlexConnect pouvant être configurés sur une plate-forme donnée multiplié par deux. Un exemple est un serveur RADIUS principal et un serveur RADIUS secondaire par groupe FlexConnect.
- La mise à niveau logicielle d'une version précédente vers la version 7.4 ne provoquera aucune perte de configuration RADIUS.
- La suppression du serveur RADIUS principal est autorisée sans avoir à supprimer le serveur RADIUS secondaire. Ceci est cohérent avec la configuration actuelle du groupe FlexConnect pour le serveur RADIUS.

#### **Procédure**

1. Mode de configuration avant la version 7.4.Un maximum de 17 serveurs RADIUS peuvent être configurés dans la configuration AAA Authentication.
| uluili.<br>cisco                         | MONETOR         |               | ONTROLLER       | WIRELESS 2         | RCURITY MAY       | AGEMENT COMMANDS           | HELP EEEOBACK |   | u (sitt filiger) |  |
|--|-----------------|---------------|-----------------|--------------------|-------------------|----------------------------|---------------|---|------------------|--|
| Security                                 | RADIUS          | Authentical   | tion Serve      | irs                |                   |                            |               |   |                  |  |
| General<br>+ BADUS                       | Cell Stat       | ion ID Type I | System H        | IAC Address        |                   |                            |               |   |                  |  |
| Authentication<br>Accounting<br>Fallback | MAC Del         | initer (      | Hyphen          | for FDPS customers | and requires a lo | y wrap compliant RADIUS of | (ver)         |   |                  |  |
| # TACACS+<br>LDAP                        | Network<br>User | Management    | Server<br>Index | Server Address     | Port              | 1Pliec                     | Admin Status  |   |                  |  |
| NAC Filtering                            | 2               |               | 1               | 1.2.3.4            | 1812              | Disabled                   | Enabled       |   |                  |  |
| sabled Clients                           | 2               | 6             | 2               | 1.2.3.4            | 2                 | Disabled                   | Enabled       |   |                  |  |
| r Lagin Policies                         | 8               |               | 3               | 1.2.3.4            | 3                 | Disabled                   | Enabled       |   |                  |  |
| word Policies                            | 8               |               | 4               | 1.2.3.4            | 4                 | Disabled                   | Enabled       |   |                  |  |
| I EAP                                    | 8               | 5             | 5               | 1.2.3.4            | 5                 | Disabled                   | Enabled       |   |                  |  |
|  | 8               | 6             | 5               | 1.2.3.4            | 6                 | Disabled                   | Enabled       |   |                  |  |
| ity Order                                | 1               | 6             | 2               | 1.2.3.4            | 7                 | Disabled                   | Enabled       |   |                  |  |
| ificate                                  | M               | <b>e</b>      | 8               | 1.2.3.4            |                   | Disabled                   | Enabled       |   |                  |  |
| se Control Lists                         | 2               | <b>e</b>      | 2               | 1.2.3.4            | 9                 | Disabled                   | Enabled       |   |                  |  |
| reless Protection                        | M               | <b>e</b>      | 22              | 1.2.3.4            | 10                | Disabled                   | Enabled       |   |                  |  |
| icies                                    | 2               |               | 22              | 1.2.3.4            | 11                | Disabled                   | Enabled       |   |                  |  |
| eb Auth                                  | 2               |               | 32              | 1.2.3.4            | 12                | Disabled                   | Enabled       |   |                  |  |
| and an even                              | 2               | 8             | 33              | 1.2.3.4            | 13                | Disabled                   | Enabled       |   |                  |  |
| ustsec sxp                               | 2               | 6             | 35              | 1.2.3.4            | 14                | Disabled                   | Enabled       |   |                  |  |
| vanced                                   | 1               | 8             | 15              | 1.2.3.4            | 15                | Disabled                   | Enabled       | • |                  |  |
|  | 2               | 6             | 15              | 1.2.3.4            | 16                | Disabled                   | Enabled       |   |                  |  |
|  | M               |               | 12              | 1.2.3.4            | 17                | Disabled                   | Enabled       |   |                  |  |

 Les serveurs RADIUS principal et secondaire peuvent être associés à un groupe FlexConnect à l'aide d'une liste déroulante comprenant des serveurs RADIUS configurés sur la page AAA Authentication.

iliilii cisco	HONITOR WLANI CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP FEEDBACK	Saya Configuration 2 (5	ing   Logouit   🔮
Wireless	FlexConnect Groups > Edit 'abc'         General Local Authentication Image Upgrade AAA YLAN-ACL mapping WLAN-ACL mapping WebPolicies Central DMCP         Group Name six         FlexConnect APs       AAA         Made Adf       Primary Relius Server       [P1:2:3.4, Rev1:3]         P MAC Address AP Name       Batus       Scondary Relius Server       [P1:2:3.4, Rev1:3]         P MAC Address AP Name       Batus       Scondary Relius Server       [P1:2:3.4, Rev1:3]         P 1.2:3.4, Rev1:3]       P1:3:3.4, Rev1:3]       P1:3:3.4, Rev1:3]         P 1.2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]         P 1.2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]         P 1:2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]       P1:2:3.4, Rev1:3]	< Back	Appir

 Mode de configuration du groupe FlexConnect dans la version 7.4.Les serveurs RADIUS principal et secondaire peuvent être configurés sous le groupe FlexConnect à l'aide d'une adresse IP, d'un numéro de port et d'un secret partagé.

 cisco	Saya Configuration (Eng. 1) Honitor Wlans Controller Wireless Security Management Commands Help Feedback	Logout Befree
Wireless * Access Points Al APs * Rados 802.11a/n 802.11b/p/n Dual-Band Radios	FlexConnect Groups > Edit 'abc'        General     Local Authentication       Trace     Name       Stratic AP Local Authentication*	Apply
Advanced     Mesh     RF Profiles     FlexConnect Groups     FlexConnect ACLs     B02.11a/n     B02.11b/g/n     Media Stream     Asolinstice Visibility	FlexConnect APs     AAA       Aad AP     Server IP Address     1.2.3.4       AP MAC Address AP Name     Status     Server Type     Secondary (4)       Shared Servet     Stared Servet     Stared Servet     Stared Servet       Carlinn Shared Servet	
<ul> <li>And Centrel Country Timers</li> <li>Netflow</li> <li>QoS</li> </ul>	Server Type         Address         Part           Primary         1.3.3.4         3         3           UnConfigured         Unconfigured         0         3	

### **Limites**

- La mise à niveau logicielle de la version 7.4 vers une version précédente conserve la configuration mais avec certaines limitations.
- La configuration d'un serveur RADIUS principal/secondaire lors de la configuration d'un serveur précédent entraîne le remplacement de l'ancienne entrée par la nouvelle.

## Mode local amélioré (ELM)

ELM est pris en charge par la solution FlexConnect. Reportez-vous au guide des meilleures pratiques sur la gestion ELM pour plus d'informations.

## Prise en charge de l'accès invité dans Flex 7500

Figure 13 : Prise en charge de l'accès invité dans Flex 7500



Flex 7500 permettra et continuera à prendre en charge la création d'un tunnel EoIP vers votre contrôleur d'ancrage invité dans la zone DMZ. Pour connaître les meilleures pratiques concernant la solution d'accès invité sans fil, reportez-vous au Guide de déploiement des invités.

## Gestion du WLC 7500 à partir de NCS

La gestion du WLC 7500 à partir du NCS est identique aux WLC existants de Cisco.

<u>ث</u>	Monitor 🔻	<u>R</u> eports	<ul> <li><u>C</u>onfigure</li> </ul>	• • 3	Services 🔻	
Add	Add Controllers					
configure > <u>controllers</u> > Add Controllers						
Gen	eral Param	eters				
A	dd Format Ty	pe	Device Info		~	
IF	Addresses		WLC 7500 IP Address			
N	etwork Mask		255.255.255.0			
[	Verify Tel	net/SSH C	apabilities ᡇ			
SNN	IP Paramet	ers 🔍				
v	ersion		v2c		*	
R	etries		2			
Т	imeout		10		(secs)	
					-	
C	ommunity		private			
Teln	et/SSH Par	ameters	Ф			
U	ser Name		admin			
P	assword		•••••			
С	onfirm Passw	rord	•••••			
R	etries		3			
Т	imeout		60		(secs)	
OK	Cancel					
Control Configure >	lers Controllers					
			-			

Audit Status **Reachability Sta** P Address Type 172.20.227.174 @ Ambassador 7500 7.0.112.62 mobility Reachable Identical 172.20.227.177 @ 5508-Primary 5500 7.0.112.52 mobility Reachable Identical

-- Select a command --

Entries 1

Pour plus d'informations sur la gestion du WLC et la découverte de modèles, reportez-vous au <u>Guide de configuration du système de contrôle sans fil Cisco, version 7.0.172.0</u>.

## Forum aux questions

# Q. Si je configure des LAP sur un site distant en tant que FlexConnect, puis-je attribuer à ces LAP un contrôleur principal et secondaire ?

**Exemple :** Il y a un contrôleur principal sur le site A et un contrôleur secondaire sur le site B. Si le contrôleur du site A tombe en panne, le LAP bascule sur le contrôleur du site B. Si les deux contrôleurs ne sont pas disponibles, le LAP passe-t-il en mode autonome FlexConnect ?

**A.** Oui. Tout d'abord, le LAP bascule sur son secondaire. Tous les WLAN commutés localement n'ont pas de modifications, et tous ceux qui sont commutés centralement ont simplement le trafic dirigé vers le nouveau contrôleur. Et, si le secondaire échoue, tous les WLAN marqués pour la

commutation locale (et l'authentification de clé ouverte/pré-partagée/vous faites l'authentification AP) restent actifs.

# Q. Comment les points d'accès configurés en mode local traitent-ils les WLAN configurés avec la commutation locale FlexConnect ?

A. Les points d'accès en mode local traitent ces WLAN comme des WLAN normaux. L'authentification et le trafic de données sont réacheminés par tunnel vers le WLC. Lors d'une défaillance de liaison WAN, ce WLAN est complètement désactivé et aucun client n'est actif sur ce WLAN jusqu'à ce que la connexion au WLC soit rétablie.

#### Q. Puis-je effectuer une authentification Web avec la commutation locale ?

**A.** Oui, vous pouvez avoir un SSID avec l'authentification Web activée et abandonner le trafic localement après l'authentification Web. L'authentification Web avec commutation locale fonctionne correctement.

Q. Puis-je utiliser mon Guest-Portal sur le contrôleur pour un SSID, qui est géré localement par le protocole H REAP ? Si oui, que se passe-t-il si je perds la connectivité au contrôleur ? Les clients actuels sont-ils immédiatement abandonnés ?

**A.** Oui. Puisque ce WLAN est commuté localement, le WLAN est disponible mais aucun nouveau client ne peut s'authentifier car la page Web n'est pas disponible. Mais les clients existants ne sont pas abandonnés.

#### Q. FlexConnect peut-il certifier la conformité PCI ?

**A.** Oui. La solution FlexConnect prend en charge la détection des pirates pour garantir la conformité PCI.

### Informations connexes

- Guide de conception et de déploiement HREAP
- <u>Contrôleurs de réseau LAN fil de la gamme Cisco 4400</u>
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- <u>Système de contrôle sans fil Cisco</u>
- Moteur de services de mobilité de la gamme Cisco 3300
- Gamme Cisco Aironet 3500
- Système de contrôle d'accès sécurisé (ACS) de Cisco
- Support et documentation techniques Cisco Systems