

# Flex 7500 ワイヤレス ブランチ コントローラ 導入ガイド

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[製品概要](#)

[製品仕様](#)

[データ シート](#)

[プラットフォーム機能](#)

[Flex 7500 の起動](#)

[Flex 7500 のライセンス](#)

[AP ベース カウント ライセンス](#)

[AP アップグレード ライセンス](#)

[ソフトウェア リリース サポート](#)

[サポートされるアクセス ポイント](#)

[FlexConnect のアーキテクチャ](#)

[アクセス ポイント制御トラフィックを集中化する利点](#)

[クライアント データ トラフィックを分散する利点](#)

[FlexConnect の動作モード](#)

[WAN 要件](#)

[ワイヤレス ブランチ ネットワーク設計](#)

[主な設計要件](#)

[概要](#)

[長所](#)

[ブランチ ネットワーク設計に対処する機能](#)

[IPv6 サポート一覧](#)

[機能マトリクス](#)

[AP グループ](#)

[WLC からの設定](#)

[要約](#)

[FlexConnect グループ](#)

[FlexConnect グループの主な目的](#)

[WLC からの FlexConnect グループの設定](#)

[CLI を使用した確認](#)

[FlexConnect VLAN オーバーライド](#)

[要約](#)

[手順](#)

[制限](#)

[FlexConnect VLAN に基づく中央スイッチング](#)

[要約](#)

[手順](#)

[制限](#)

[FlexConnect ACL](#)

[要約](#)

[手順](#)

[制限](#)

[FlexConnect スプリット トンネリング](#)

[要約](#)

[手順](#)

[制限](#)

[耐障害性](#)

[要約](#)

[制限](#)

[WLAN ごとのクライアント制限](#)

[主な目的](#)

[制限](#)

[WLC の設定](#)

[NCS の設定](#)

[ピアツーピア ブロッキング](#)

[要約](#)

[手順](#)

[制限](#)

[AP 事前イメージのダウンロード](#)

[要約](#)

[手順](#)

[制限](#)

[FlexConnect スマート AP イメージ アップグレード](#)

[要約](#)

[手順](#)

[制限](#)

[FlexConnect モードでの自動変換 AP](#)

[手動モード](#)

[自動変換モード](#)

[ローカル スwitching WLAN のための FlexConnect WGB/uWGB サポート](#)

[要約](#)

[手順](#)

[制限](#)

[Radius サーバ数の増加のサポート](#)

[要約](#)

[手順](#)

[制限](#)

[拡張ローカル モード \( ELM \)](#)  
[Flex 7500 のゲスト アクセス サポート](#)  
[NCS からの WLC 7500 の管理](#)  
[FAQ](#)  
[関連情報](#)

## 概要

このドキュメントでは、Cisco Flex 7500 ワイヤレス ブランチ コントローラを導入する方法について説明しています。このドキュメントでは、次のことを目的としています。

- FlexConnect ソリューションのさまざまなネットワーク要素と、その通信フローについて説明する。
- Cisco FlexConnect ワイヤレス ブランチ ソリューションを設計するための、一般的な導入ガイドラインを提供する。
- 製品に関する情報ベースを支える、7.2.103.0 コード リリースのソフトウェア機能について説明する。

注：7.2より前のFlexConnectはHybrid REAP(HREAP)と呼ばれていました。現在は FlexConnect と呼ばれています。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

### 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## 製品概要

図 1 : Cisco Flex 7500



Cisco Flex 7500 シリーズ Cloud Controller は、複数のサイトでの[ワイヤレス](#)の導入に適した、スケーラビリティの高いブランチ オフィス用コントローラです。Cisco Flex 7500 シリーズのコン

トローラをプライベートクラウドに導入すれば、分散しているブランチ オフィスにワイヤレスサービスを拡大し、集中管理できるので、総運用コストが削減されます。

Cisco Flex 7500 シリーズ ( 図 1 ) によって、最大 500 カ所のブランチ オフィスのワイヤレス [アクセスポイント](#) を管理でき、IT 管理者は、最大 3000 台のアクセスポイント ( AP ) と 30,000 のクライアントの設定、管理、およびトラブルシューティングをデータセンターから行うことができます。Cisco Flex 7500 シリーズのコントローラは、セキュアなゲスト アクセス、Payment Card Industry ( PCI ) 基準に準拠した不正検出、ブランチ ( ローカルでスイッチングが行われる ) オフィスでの Wi-Fi による音声およびビデオに対応しています。

この表は、Flex 7500、WiSM2、WLC 5500 コントローラの拡張性の違いを示しています。

拡張性	Flex 7500	WiSM2	WLC 5500
アクセスポイントの総数	6,000	1,000	500
クライアントの総数	64,000	15,000	7,000
最大 FlexConnect グループ	2000	100	100
FlexConnect グループあたりの最大 AP 数	100	25	25
最大 AP グループ数	6000	1,000	500

## 製品仕様

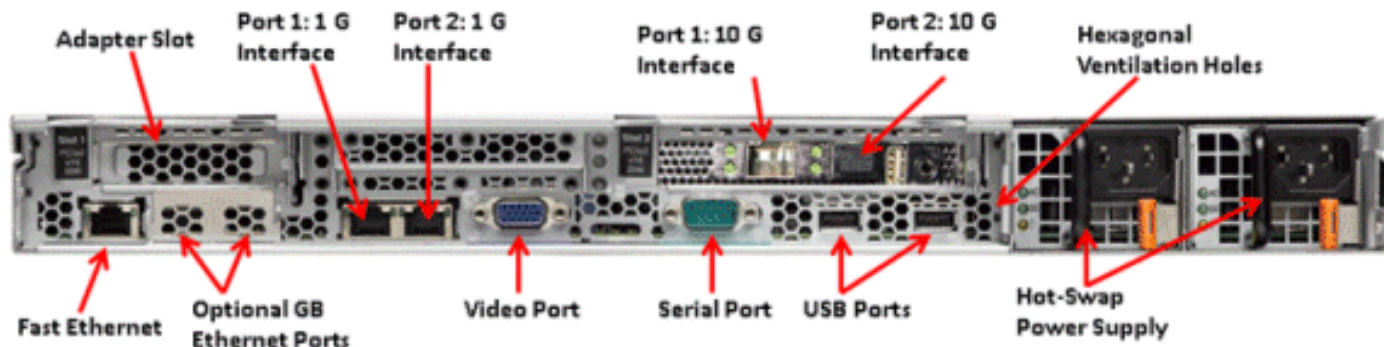
### データシート

[http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data\\_sheet\\_c78-650053.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html) を参照してください。

### プラットフォーム機能

図 2 : Flex 7500 の背面図

#### Rear View



### ネットワーク インターフェイスポート

インターフェイスポート	用途
ファストイーサネット	統合管理モジュール ( IMM )

ポート 1 : 1G	WLC サービス ポート
ポート 2 : 1G	WLC リダンダンシー ポート ( RP )
ポート 1 : 10G	WLC 管理インターフェイス
ポート 2 : 10G	WLC バックアップ管理インターフェイス ポート ( ポート障害 )
オプションの Gb イーサネット ポート	N/A

注 :

- 2x10Gインターフェイスに対するLAGサポートにより、高速フェールオーバーリンク冗長性を備えたアクティブ-アクティブリンク動作が可能になります。LAGを備えた追加のアクティブな10Gリンクは、コントローラのワイヤレススループットを変更しません。
- 2x10G インターフェイス
- 2x10G インターフェイスは、SFP 製品番号 SFP-10G-SR の光ファイバケーブルのみをサポートしています。
- スイッチ側 SFP 製品番号 X2-10GB-SR

## システム MAC アドレス

ポート 1 : 10G ( 管理インターフェイス )	システムまたはベース MAC アドレス
ポート 2 : 10G ( バックアップ管理インターフェイス )	ベース MAC アドレス + 5
ポート 1 : 1G ( サービス ポート )	ベース MAC アドレス + 1
ポート 2 : 1G ( リダンダンシー ポート )	ベース MAC アドレス + 3

## シリアル コンソール リダイレクト

WLC 7500 では、デフォルトでポーレート 9600 でのコンソールのリダイレクトが可能になっており、フロー制御なしの Vt100 端末をシミュレートします。

## インベントリ情報

図 3 : WLC 7500 コンソール

```
(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
```

デスクトップ管理インターフェイス ( DMI ) テーブルには、サーバハードウェアと BIOS の情報が格納されています。

WLC 7500 は、BIOS のバージョン、PID と VID、およびシリアル番号をインベントリの一部として表示します。

## Flex 7500 の起動

ソフトウェア メンテナンス用のシスコ ブート ロード オプションは、シスコの既存のコントローラプラットフォームと同じです。

図 4 : 起動順序

```
Cisco Bootloader (Version          )

                .o88b. d8888888b .d8888.  .o88b.  .d88b.
                d8P  Y8  `88'  88'  YP d8P  Y8  .8P  Y8.
                8P      88  `8bo.  8P      88  88
                8b      88      `Y8b. 8b      88  88
                Y8b d8  .88.  db  8D Y8b d8  `8b d8'
                `Y88P' Y888888P `8888Y' `Y88P' `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
```

図 5 : WLC 設定ウィザード

```
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 Port Num [1 to 2]: 1 ← 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
```

注：Flex 7500のブートアップシーケンスは同等であり、既存のコントローラプラットフォームと一貫性があります。最初の起動には、ウィザードを使用した WLC の設定が必要です。

## [Flex 7500 のライセンス](#)

### [AP ベース カウント ライセンス](#)

AP ベース カウント SKU
300

500
1,000
2000
3,000
6000

## [AP アップグレード ライセンス](#)

AP アップグレード SKU
100
250
500
1,000

ベース カウントとアップグレード カウントを除き、注文、インストール、表示を含むライセンス取得手順全体は、シスコの既存の WLC 5508 と同じです。

ライセンス取得手順全体を網羅している [WLC 7.3 コンフィギュレーション ガイド](#)を参照してください。

## [ソフトウェア リリース サポート](#)

Flex 7500 は、WLC コード バージョン 7.0.116.x 以降のみをサポートしています。

## [サポートされるアクセス ポイント](#)

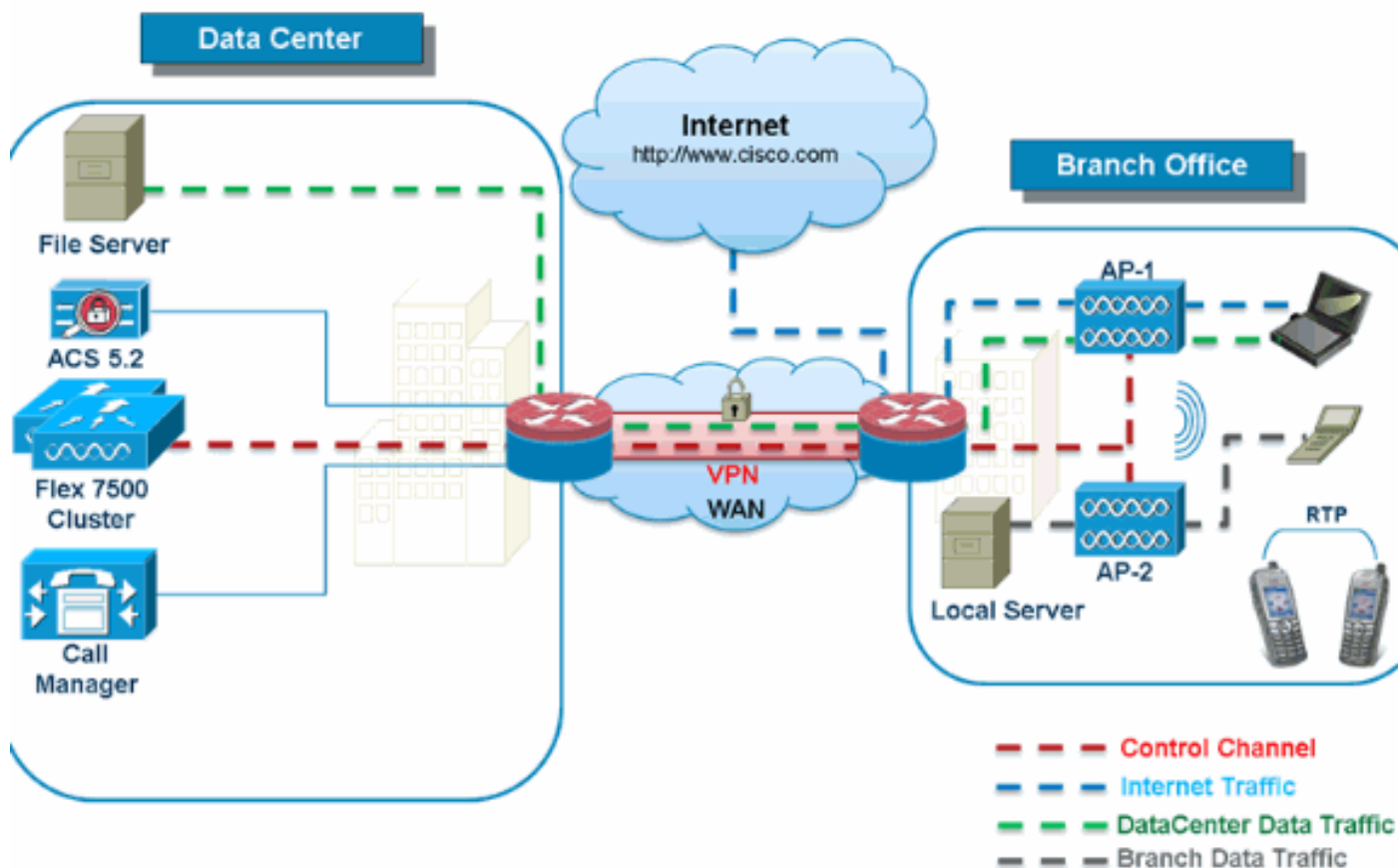
アクセス ポイント 1040、1130、1140、1550、3500、3600、2600、1250、1260、1240、OEAP 600、ISR 891、および ISR 881 が Flex 7500 でサポートされます。

## [FlexConnect のアーキテクチャ](#)

図 6 : 一般的なワイヤレス ブランチ トポロジ



# FlexConnect Architecture



FlexConnect は、ブランチ オフィスおよびリモート オフィスでの導入に向けた無線ソリューションです。Hybrid REAP ソリューションとも呼びますが、このドキュメントでは FlexConnect と呼びます。

FlexConnect ソリューションを使用すると、お客様は次のことが可能になります。

- データセンターからの AP のトラフィックの制御と管理を集中化する。制御トラフィックを [図 6](#) の赤い破線で示します。
- 各ブランチ オフィスでクライアント データトラフィックを分散させる。データトラフィックを [図 6](#) の青、緑、紫の破線で示します。各トラフィック フローは、最も効率の良い方法で最終的な宛先に向かいます。

## アクセス ポイント制御トラフィックを集中化する利点

- 1 カ所からの監視とトラブルシューティング
- 管理が容易
- データセンター リソースへのセキュアでシームレスなモバイル アクセス
- ブランチ設置プランにおける削減
- 運用費用のさらなる節約

## クライアント データトラフィックを分散する利点

- WAN リンクの完全な障害やコントローラの使用不能による運用上のダウンタイムなし ( 持続性 )
- WAN リンク障害時のブランチ内でのモビリティの復元力

- ・ブランチの拡張性の向上。最大 100 AP および 250,000 平方フィート ( AP あたり 5000 平方フィート ) まで拡張可能な規模のブランチをサポートします。

Cisco FlexConnect ソリューションは、セントラル クライアント データ トラフィックもサポートしていますが、ゲスト データ トラフィックのみに限定することを推奨します。次の表では、データ トラフィックが中央のデータセンターでもスイッチングされる非ゲスト クライアントのみについで、WLAN L2 セキュリティ タイプに対する制限事項を示します。

### 中央でスイッチングされる非ゲスト ユーザに対する L2 セキュリティのサポート

WLAN L2 セキュリティ	Type	結果
なし	N/A	許可
WPA + WPA2	802.1x	許可
	CCKM	許可
	802.1x + CCKM	許可
	PSK	許可
802.1x	WEP	許可
スタティック WEP	WEP	許可
WEP + 802.1x	WEP	許可
CKIP		許可

注：これらの認証制限は、データ トラフィックがブランチに分散されているクライアントには適用されません。

### 中央およびローカルでスイッチングされるユーザに対する L3 セキュリティのサポート

WLAN L3 セキュリティ	Type	結果
Web 認証	内部	許可
	外部	許可
	カスタマイズ	許可
Web パススルー	内部	許可
	外部	許可
	カスタマイズ	許可
条件付き Web リダイレクト	外部	許可
スプラッシュ ページ Web リダイレクト	外部	許可

FlexConnect 外部 Webauth の導入の詳細については、『[FlexConnect 外部 WebAuth 導入ガイド](#)』を参照してください。

HREAP/FlexConnect AP の状態とデータ トラフィック スイッチング オプションの詳細については、『[FlexConnect の設定](#)』を参照してください。

### FlexConnect の動作モード

FlexConnect のモード	説明

ド	
接続中	FlexConnect は、コントローラの背後にある CAPWAP コントロール プレーンが稼働しているとき、つまり WAN リンクが停止していないときに接続モードになります。
スタン ドアロ ン	これに対して、スタンドアロン モードとは、FlexConnect がコントローラに接続されずに稼働しているときの状態です。スタンドアロン モードの FlexConnect AP は、停電や WLC または WAN の障害が発生した場合でも、直近の設定で機能し続けます。

FlexConnect の動作原理の詳細については、『[H-Reap / FlexConnect 設計および導入ガイド](#)』を参照してください。

## WAN 要件

FlexConnect AP はブランチ サイトに導入され、WAN リンクを介してデータセンターから管理されます。最小帯域幅制限である AP あたり 12.8 kbps を満たし、ラウンドトリップ遅延が、データ用の導入の場合は 300 ms を超えず、データと音声の導入の場合は 100 ms を超えないようにすることを強く推奨します。最大伝送単位 (MTU) は、500 バイト以上であることが必要です。

導入タイプ	WAN 帯域幅 (最小)	WAN RTT 遅延 (最大)	ブランチあたりの最大 AP 数	ブランチあたりの最大クライアント数
Data	64 Kbps	300 ms	5	25
データ + 音声	128 kbps	100 ms	5	25
モニタ	64 Kbps	2 秒	5	N/A
Data	640 Kbps	300 ms	50	1,000
データ + 音声	1.44 Mbps	100 ms	50	1,000
モニタ	640 Kbps	2 秒	50	N/A

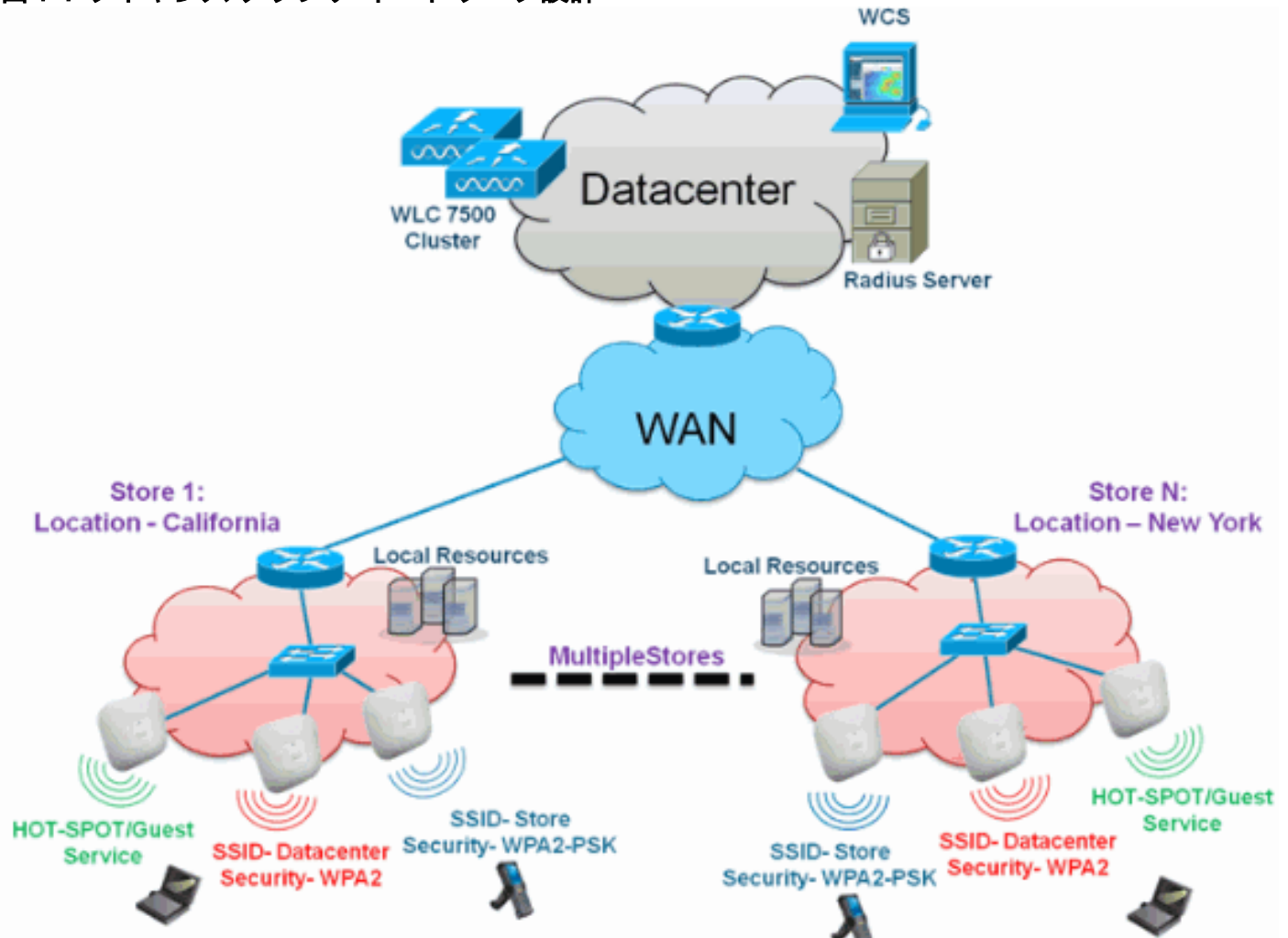
## ワイヤレス ブランチ ネットワーク設計

このドキュメントの残りの部分では、セキュアな分散ブランチ ネットワークを実装するためのガイドラインとベスト プラクティスについて説明します。FlexConnect アーキテクチャは、次の設計要件を満たすワイヤレス ブランチ ネットワークに推奨します。

### 主な設計要件

- 最大 100 AP および 250,000 平方フィート ( AP あたり 5000平方フィート ) まで拡張可能な規模のブランチ
- 中央での管理とトラブルシューティング
- 運用上のダウンタイムなし
- クライアントベースのトラフィック セグメンテーション
- 企業リソースに対するシームレスでセキュアなワイヤレス接続
- PCI 準拠
- ゲストのサポート

図 7: ワイヤレス ブランチ ネットワーク設計



## 概要

ブランチ ユーザが、豊富な機能を備え、拡張性が高くセキュアなネットワーク サービスを、地理的に離れた複数の場所にまたがって提供するの、ますます困難かつ高価になっています。お客様を支援するため、シスコは、Flex 7500 を導入することでこれらの課題に対処します。

Flex 7500 ソリューションは、複雑なセキュリティ、管理、設定、トラブルシューティング作業をデータセンター内に仮想化し、それらのサービスを各ブランチに透過的に拡張します。Flex 7500 を使用した導入では、IT 担当者が容易に設定、管理でき、最も重要なことに、容易に拡張できます。

## 長所

- 6000 台の AP のサポートによる高い拡張性

- FlexConnect Fault Tolerance を使用した高い復元力
- FlexConnect ( 中央およびローカル スイッチング ) を使用したトラフィックのセグメンテーションの促進
- AP グループと FlexConnect グループを使用した店舗設計の複製による容易な管理。

## ブランチ ネットワーク設計に対処する機能

このガイドの残りのセクションでは、[図 7](#) に示すネットワーク設計を実現するための機能の使用と推奨事項について説明します。

### 機能

主な機能	ハイライト
AP グループ	複数のブランチ サイトを扱うときに、運用と管理が容易になります。また、似たブランチ サイトについて設定を柔軟に複製できます。
FlexConnect グループ	FlexConnect グループは、ローカル バックアップ Radius、CCKM/OKC 高速ローミング、ローカル認証の機能を提供します。
耐障害性	ワイヤレス ブランチの復元力を高め、運用上のダウンタイムをなくします。
ELM ( Adaptive wIPS 用の拡張ローカルモード )	クライアントにサービスを提供するときに、クライアントのパフォーマンスに影響を与えることなく、Adaptive wIPS 機能を提供します。
WLAN ごとのクライアント制限	ブランチ ネットワーク上のゲスト クライアントの総数を制限します。
AP 事前イメージのダウンロード	ブランチをアップグレードするときのダウンタイムを削減します。
FlexConnect における AP の自動変換	ブランチの FlexConnect の AP を自動的に変換するための機能。
ゲスト アクセス	シスコの既存のゲスト アクセス アーキテクチャを FlexConnect で引き続き使用できます。

## IPv6 サポート一覧

機能	中央スイッチング		ローカルスイッチング	
	5500	Flex	5500 /	Flex

	/ WiSM-2	7500	WiSM-2	7500
IPv6 (クライアントモビリティ)	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 RA ガード	サポート対象	サポート対象	サポート対象	サポート対象
IPv6 DHCP ガード	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 ソース ガード	サポート対象	Not Supported	Not Supported	Not Supported
RA スロットリングとレート制限	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 ACL	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 クライアント可視性	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 ネイバー探索キャッシング	サポート対象	Not Supported	Not Supported	Not Supported
IPv6 ブリッジング	サポート対象	Not Supported	サポート対象	サポート対象

## 機能マトリクス

FlexConnect の機能マトリクスについては、『[FlexConnect 機能マトリクス](#)』を参照してください。

## AP グループ

コントローラで WLAN を作成した後、アクセス ポイント グループを使用して WLAN を別々のアクセス ポイントに選択的に公開し、ワイヤレス ネットワークをより効率的に管理できます。一般的な導入では、WLAN 上のすべてのユーザはコントローラ上の 1 個のインターフェイスにマッピングされます。したがって、その WLAN にアソシエーションされたすべてのユーザは、同じサブネットまたは VLAN 上にあります。ただし、複数のインターフェイス間で負荷を分散したり、アクセス ポイント グループを作成して、個々の部門 (たとえばマーケティング部門、技術部門、運用部門) などの特定の条件に基づいてユーザ グループに負荷を分散できます。さらに、ネットワーク管理を簡素化するために、これらのアクセス ポイント グループを別個の VLAN で設定できます。

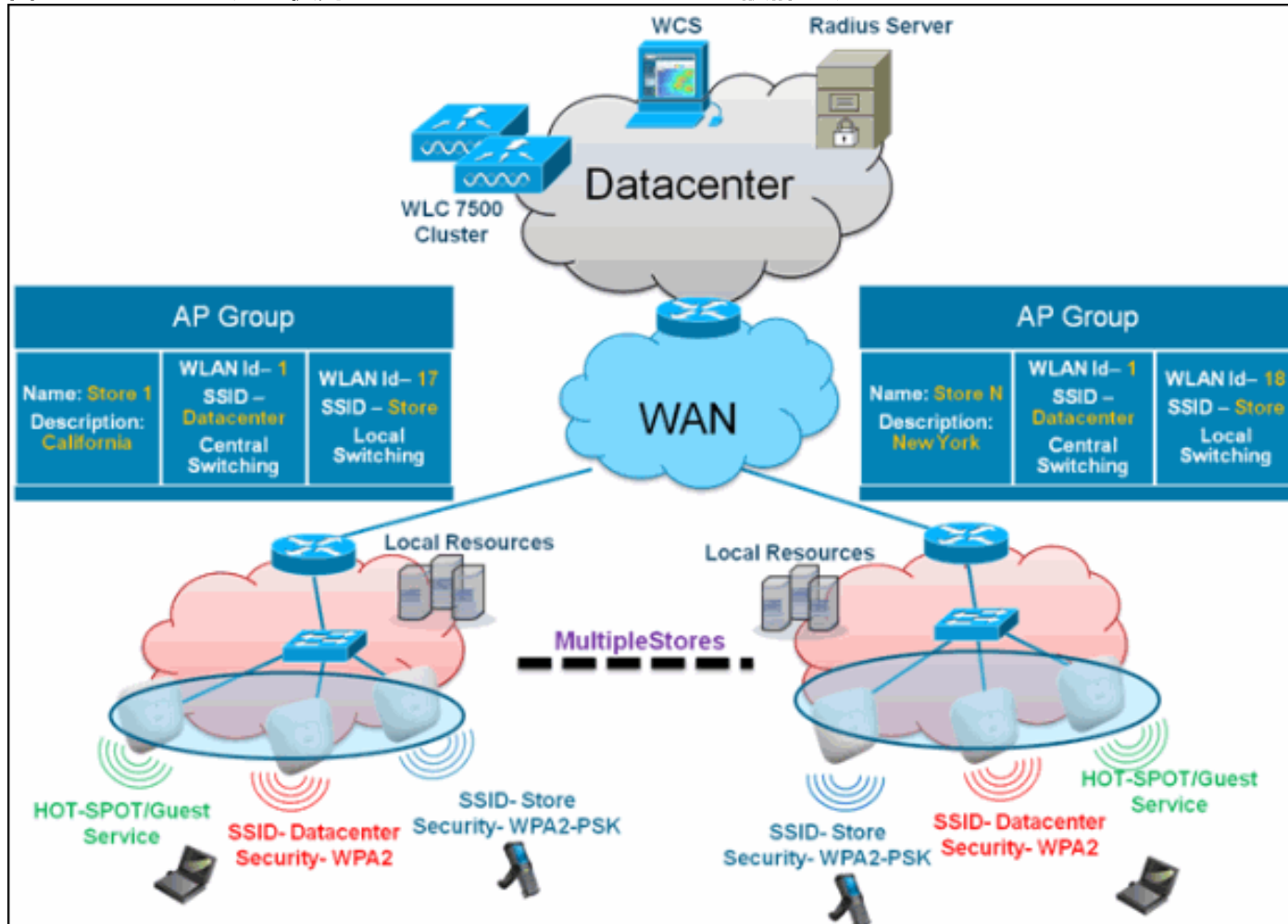
このドキュメントでは、地理的に離れた場所にまたがる複数の店舗を管理するときに、複数の



APグループを使用してネットワーク管理を単純化します。運用を容易にするために、このドキュメントでは、店舗ごとに1つのAPグループを作成して、次の要件を満たします。

- ローカル店舗責任者の管理アクセスのための、全店舗にまたがる、中央でスイッチングされる SSID Datacenter。
- ハンドヘルドスキャナ用の、全店舗にまたがる、異なる WPA2-PSK キーを持つ、ローカルでスイッチングされる SSID Store。

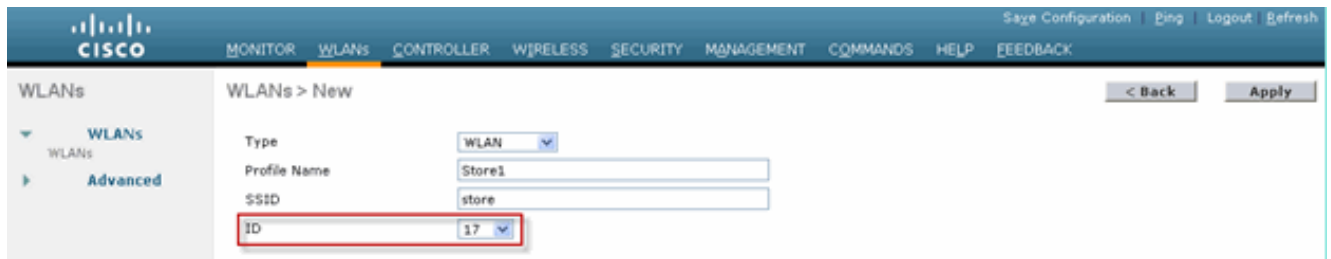
図 8 : APグループを使用したワイヤレス ネットワーク設計リファレンス



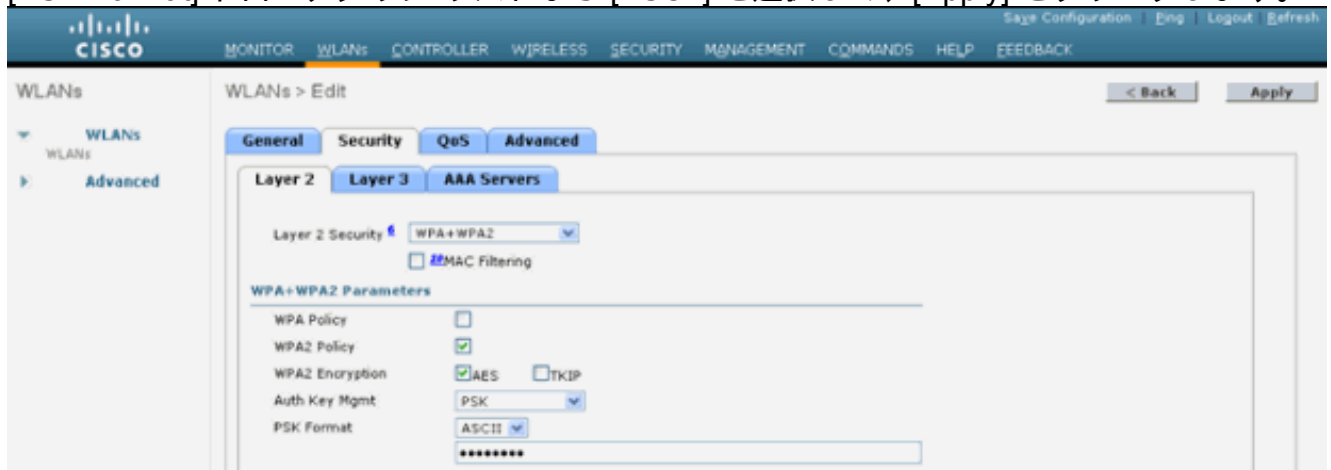
## WLC からの設定

次のステップを実行します。

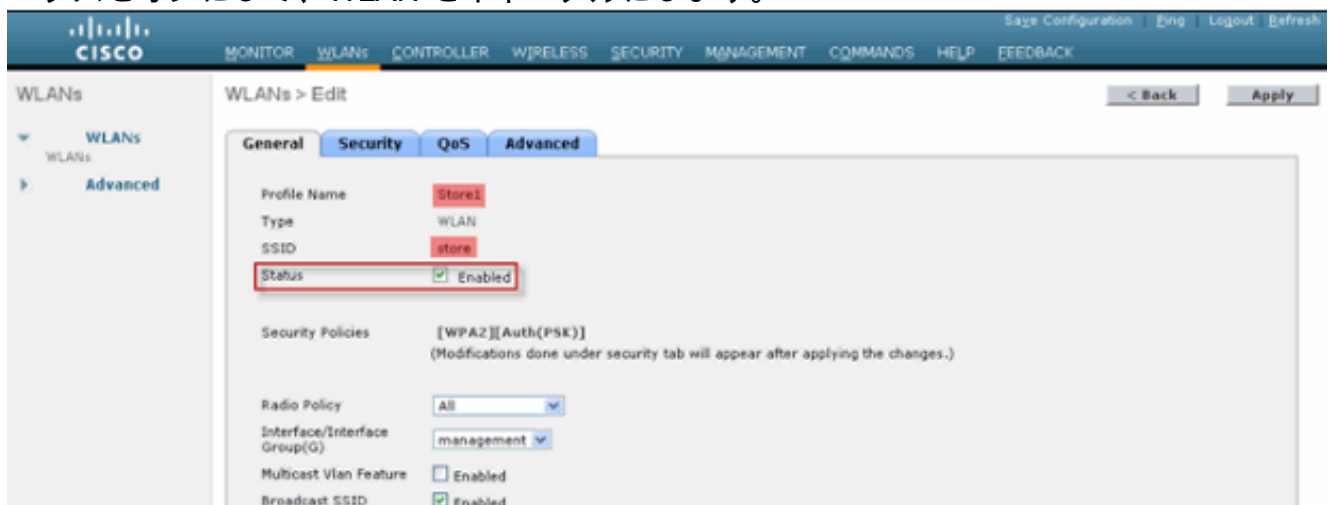
1. [WLANs] > [New] ページで、[Profile Name] フィールドに **Store1** と入力し、[SSID] フィールドに **store** と入力し、[ID] ドロップダウン リストから [17] を選択します。注：WLAN ID 1 ~ 16はデフォルトグループの一部であり、削除できません。異なる WPA2-PSK を使用した店舗ごとに同じ SSID store を使用するという要件を満たすために、WLAN ID 17 以降を使用する必要があります。というのは、これらはデフォルトグループに属しておらず、各店舗に制限できるからです。



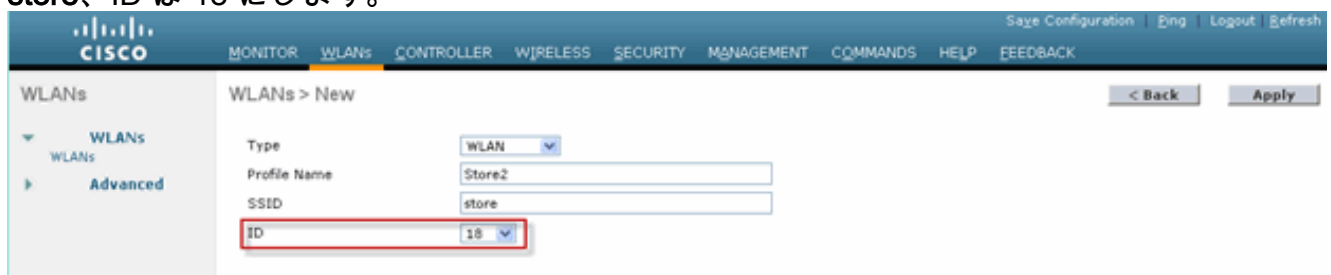
2. [WLAN] > [Security] で、[Auth Key Mgmt] ドロップダウン リストから [PSK] を選択し、[PSK Format] ドロップダウン リストから [ASCII] を選択して、[Apply] をクリックします。



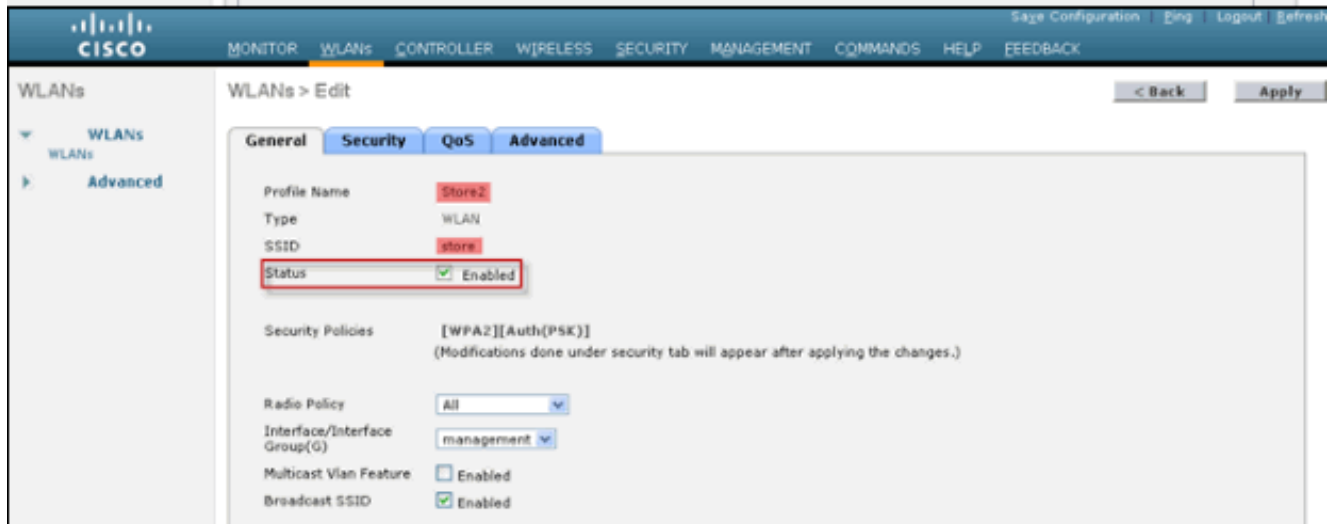
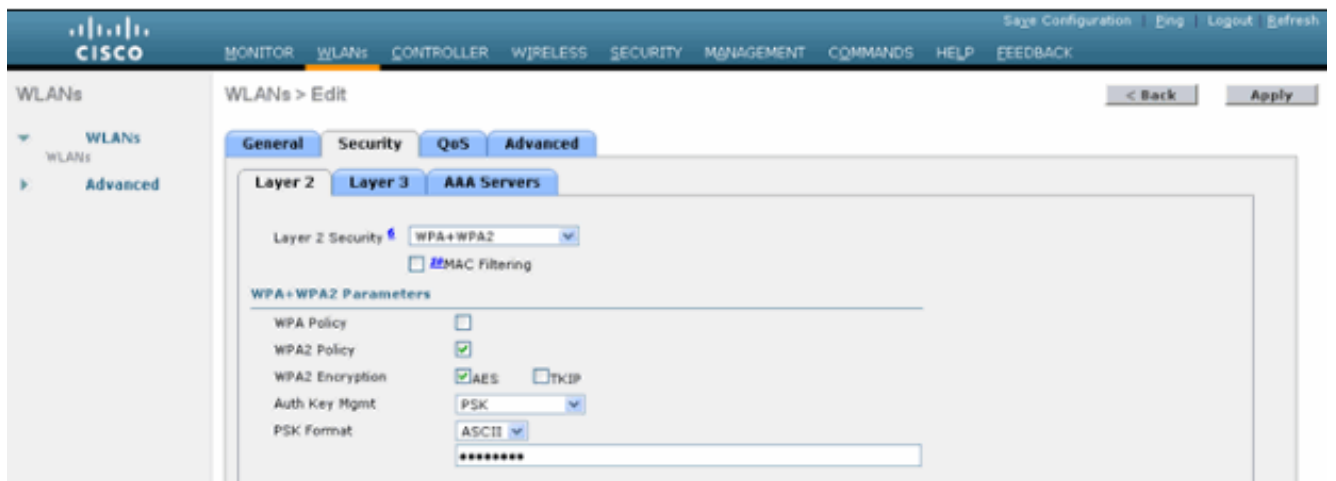
3. [WLAN] > [General] をクリックし、セキュリティ ポリシーの変更内容を確認し、[Status] ボックスをオンにして、WLAN をイネーブルにします。



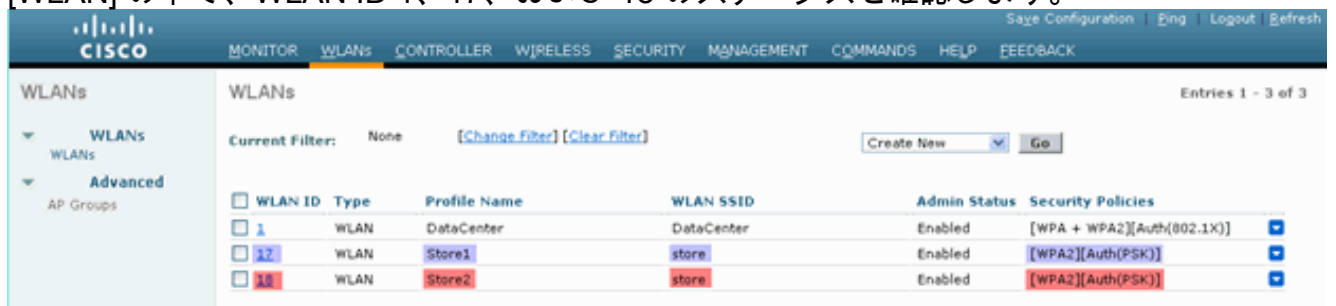
4. 新しい WLAN プロファイル Store2 についてステップ 1、2、3 を繰り返します。SSID は store、ID は 18 にします。



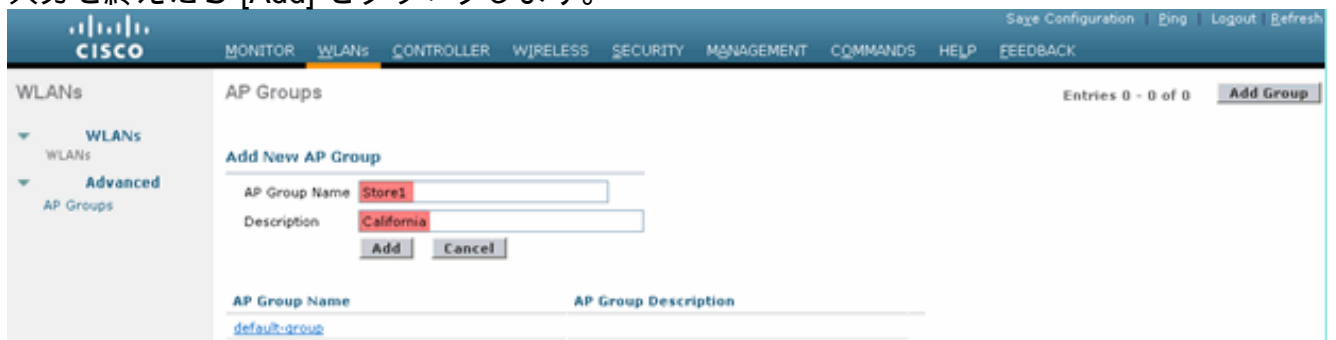




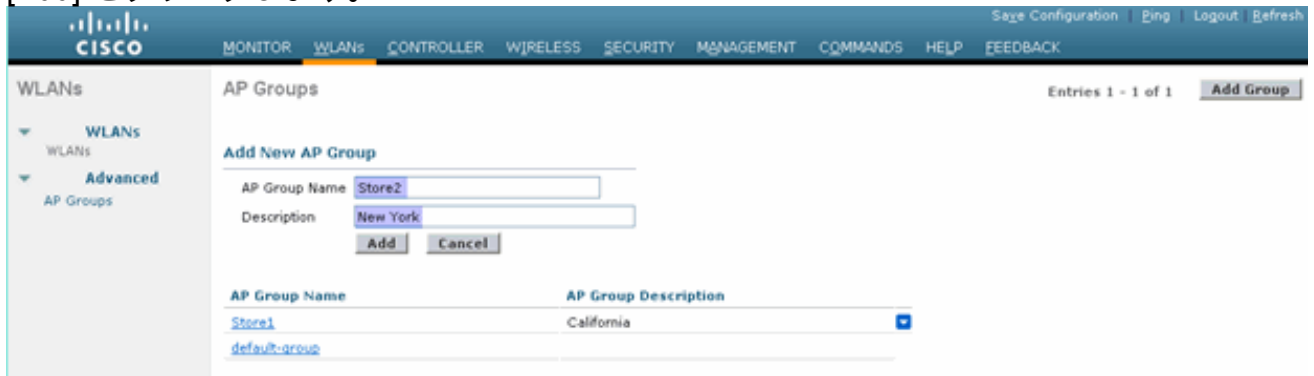
5. [Profile Name] を **DataCenter**、SSID を **DataCenter**、ID を 1 にして WLAN プロファイルを作成し、イネーブルにします。注：作成時に、1 ~ 16のWLAN IDは自動的にdefault-ap-groupの一部になります。
6. [WLAN] の下で、WLAN ID 1、17、および 18 のステータスを確認します。



7. [WLAN] > [Advanced] > [AP group] > [Add Group] の順にクリックします。
8. AP グループ名 **Store1** を追加します。これは、WLAN プロファイル **Store1** と同じ名前です。[Description] は店舗の場所にします。この例では、店舗の場所として California を使用しています。
9. 入力を終わったら [Add] をクリックします。



10. [Add Group] をクリックし、[AP Group Name] に **Store2**、[Description] に New York と入力してグループを作成します。
11. [Add] をクリックします。



12. [WLAN] > [Advanced] > [AP Groups] の順にクリックしてグループが作成されたことを確認します。



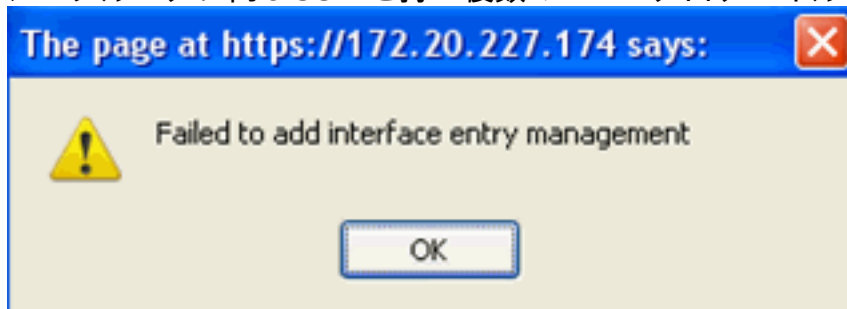
13. AP グループ名 **Store1** をクリックして、WLAN を追加または編集します。
14. [Add New] をクリックし、WLAN を選択します。
15. [WLAN] の下で、[WLAN SSID] ドロップダウンから [WLAN ID 17 store(17)] を選択します。
16. WLAN ID 17 を選択した後で [Add] をクリックします。
17. WLAN ID 1 DataCenter(1) について、ステップ 14 ~ 16 を繰り返します。このステップはオプションであり、リモート リソース アクセスを許可する場合のみ必要です。



18. [WLAN] > [Advanced] > [AP Groups] 画面に戻ります。
19. AP グループ名 **Store2** をクリックして、WLAN を追加または編集します。
20. [Add New] をクリックし、WLAN を選択します。
21. [WLAN] の下で、[WLAN SSID] ドロップダウンから [WLAN ID 18 store(18)] を選択します。
22. WLAN ID 18 を選択した後で [Add] をクリックします。
23. WLAN ID 1 DataCenter(1) について、ステップ 14 ~ 16 を繰り返します。



注：1つのAPグループに同じSSIDを持つ複数のWLANプロファイルを追加することはでき



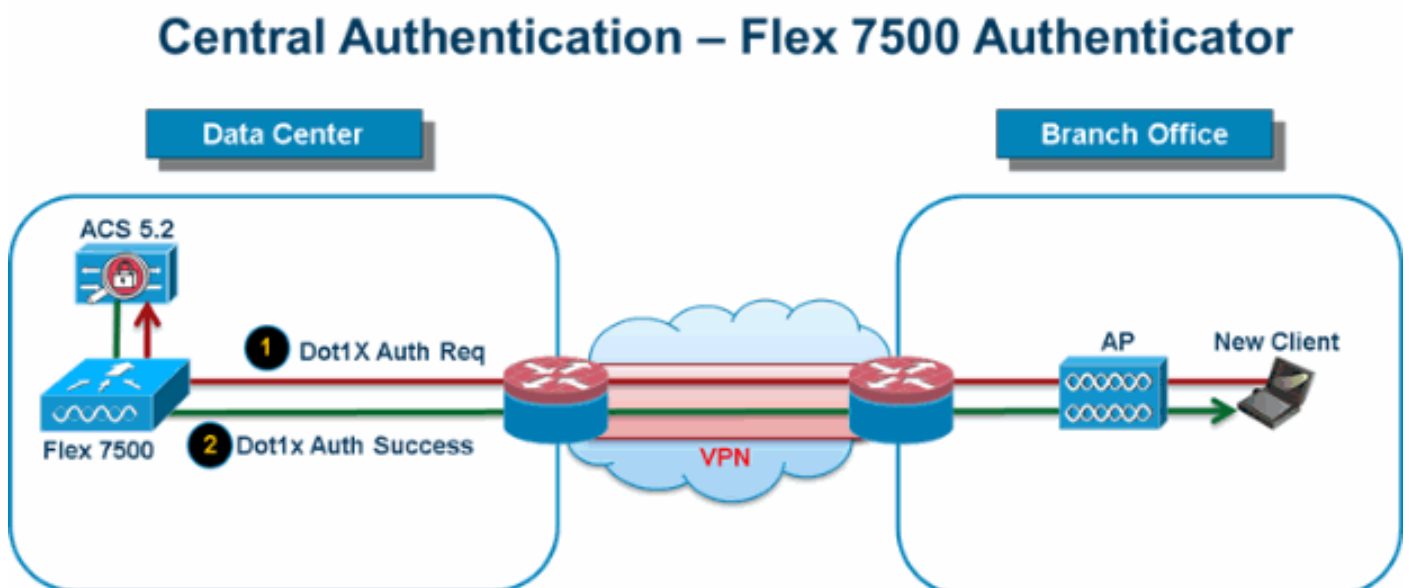
ません。注：APグループへのAPの追加は、このドキュメントでは取り上げませんが、クライアントがネットワークサービスにアクセスするために必要です。

## 要約

- APグループによりネットワーク管理が簡単になります。
- ブランチごとの粒度による容易なトラブルシューティング
- 柔軟性の向上

## FlexConnect グループ

図 9：中央の Dot1X 認証 (Flex 7500 がオーセンティケーターとして動作)



ほとんどの一般的なブランチ展開では、[図9](#)に示すように、クライアント802.1X認証がデータセ

ンターで中央で行われることが容易に予測できます。上記のシナリオは完全に有効であるため、次の問題が発生します。

- Flex 7500 が障害になった場合、クライアントはどのようにして 802.1X 認証を行いデータセンターのサービスにアクセスすれば良いのか。
- ブランチとデータセンターの間の WAN リンクが障害になった場合、ワイヤレス クライアントは 802.1X 認証をどのようにして行えば良いのか。
- WAN 障害の際にブランチのモビリティに影響があるか。
- FlexConnect ソリューションではブランチの運用上のダウンタイムがなくなるのか。

FlexConnect グループは、これらの課題に対処することを主な目的としており、そのために作成する必要があります。また、各ブランチ サイトを容易に整理できるようになります。これは、各ブランチ サイトのすべての FlexConnect アクセス ポイントが 1 つの FlexConnect グループに属するためです。

注：FlexConnectグループは、APグループに類似していません。

## FlexConnect グループの主な目的

### バックアップ RADIUS サーバのフェールオーバー

- スタンドアロン モードの FlexConnect アクセス ポイントがバックアップ RADIUS サーバに対して完全な 802.1X 認証を実行できるように、コントローラを設定することができます。管理者は、ブランチの復元力を高めるために、プライマリ バックアップ RADIUS サーバか、プライマリとセカンダリの両方のバックアップ RADIUS サーバを構成できます。このバックアップサーバが使用されるのは、FlexConnect アクセス ポイントがコントローラに接続されていないときだけです。

注：バックアップRADIUSアカウントリングはサポートされていません。

### ローカル認証

- 7.0.98.0 コード リリースの前は、WAN リンクの障害時にクライアントの接続が影響を受けないように、ローカル認証は FlexConnect がスタンドアロン モードの場合のみサポートされていました。7.0.116.0 リリースにより、FlexConnect アクセス ポイントが接続モードの場合においても、この機能がサポートされるようになりました。図 10：中央の Dot1X 認証 (FlexConnect AP がオーセンティケータとして動作)

## Central Authentication – AP Authenticator

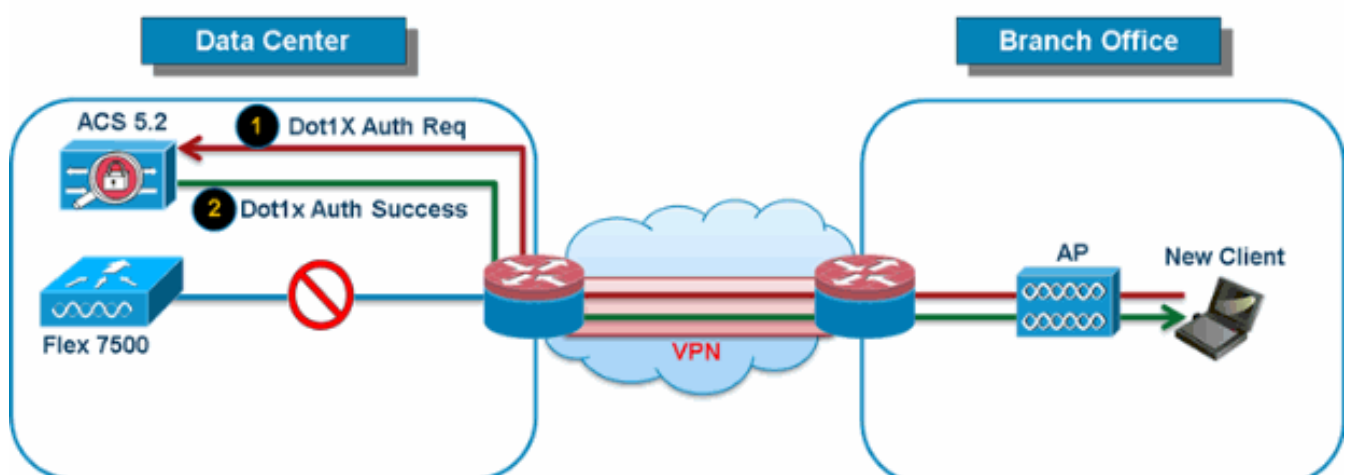
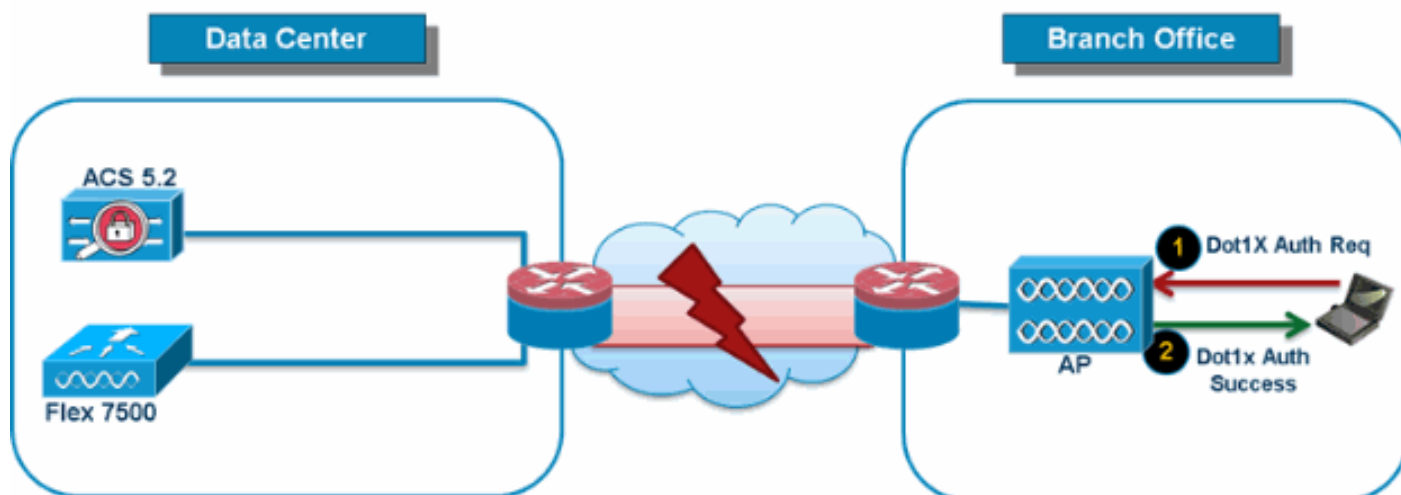


図 10 に示すように、FlexConnect ブランチ AP が Flex 7500 に接続できない場合でも、ブランチ クライアントは引き続き 802.1X 認証を実行できます。RADIUS/ACS サーバにブランチ サイトから到達可能な限り、ワイヤレス クライアントは、引き続き認証とワイヤレス サービスへのアクセスを行います。言い換えれば、RADIUS/ACS がブランチの中にある場合、クライアントは WAN が停止している間でも認証とワイヤレス サービスへのアクセスを行います。注：この機能は、FlexConnect/バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect アクセス ポイントは、まずプライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバを試行し (プライマリに接続できない場合)、最後に FlexConnect アクセス ポイント自身のローカルな EAP サーバを試行します (プライマリとセカンダリの両方に接続できない場合)。

ローカル EAP (ローカルでの認証の継続)

図 11 : Dot1X 認証 ( FlexConnect AP がローカルな EAP サーバとして動作 )

## Local Branch Authentication – AP as Radius Server



- スタンドアロン モードまたは接続モードの FlexConnect AP が最大 100 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるように、コントローラを設定できます。コントローラは、それぞれの FlexConnect アクセス ポイントがコントローラに加入すると、ユーザ名とパスワードのスタティック リストをその特定の FlexConnect グループの FlexConnect アクセス ポイントに送信します。グループ内の各アクセス ポイントは、そのアクセス ポイントにアソシエートされたクライアントのみを認証します。
- この機能が適しているのは、企業が自律アクセス ポイント ネットワークから軽量な FlexConnect アクセス ポイント ネットワークに移行するときに、大きなユーザ データベースを保持したくない場合や、自律アクセス ポイントの持つ RADIUS サーバ機能の代わりとなる別のハードウェア デバイスを追加したくない場合です。
- 図 11 に示すように、データセンターの RADIUS/ACS サーバが到達不能な場合、FlexConnect AP は自動的にローカル EAP サーバとして振る舞い、ワイヤレス ブランチ クライアントの Dot1X 認証を行います。

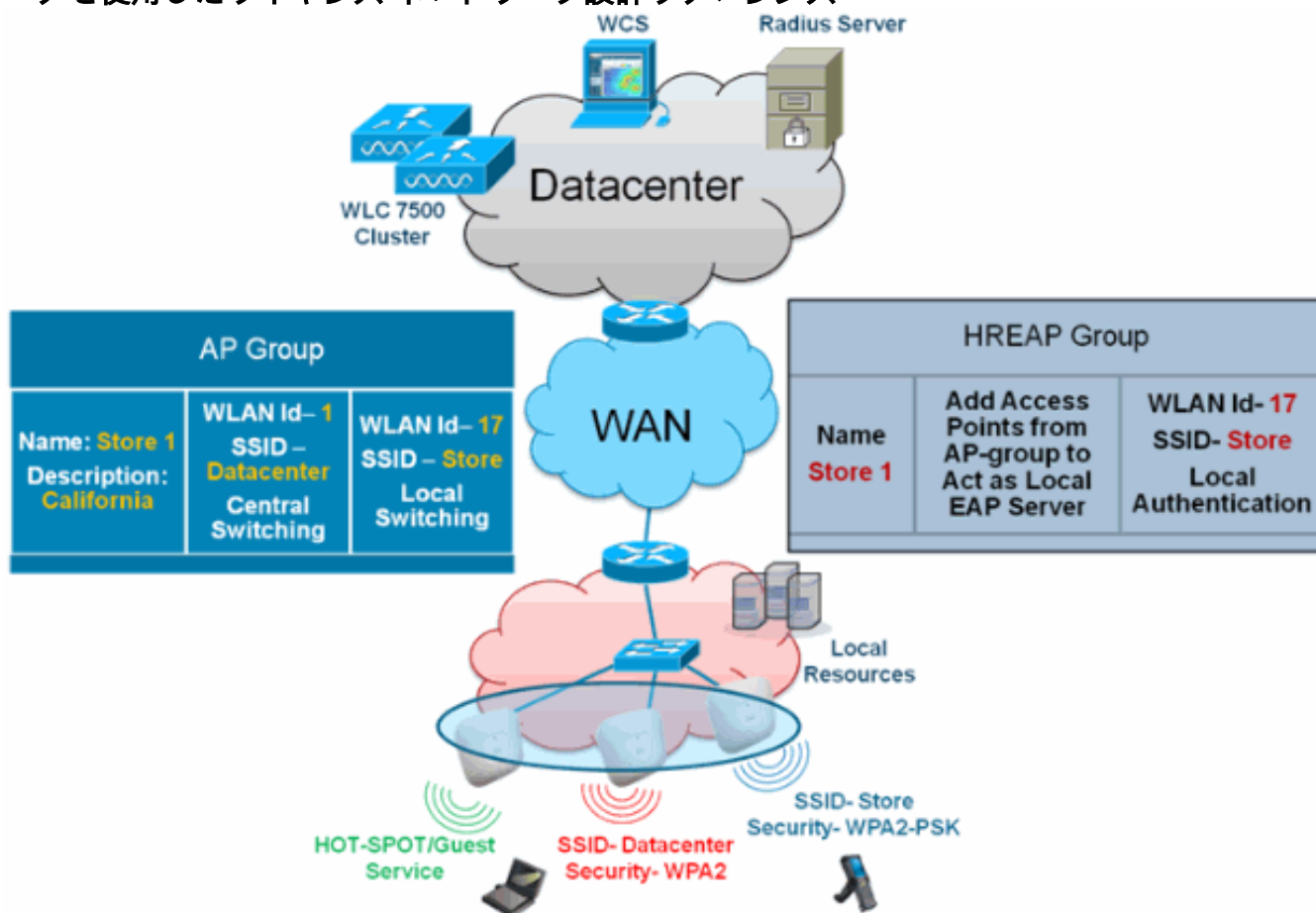
### CCKM/OKC 高速ローミング

- FlexConnect グループは、FlexConnect アクセス ポイントと共に使用する CCKM/OKC 高速ローミングが必要となります。高速ローミングは、無線クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行され



たマスター キーの派生キーをキャッシュすることにより実現します。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。たとえば、300 個のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM/OKC キャッシュを送信することは現実的ではありません。限定されたいくつかのアクセス ポイントからなる FlexConnect グループを作成すれば（たとえば、同じリモート オフィス内の 4 個のアクセス ポイントのグループを作成）、クライアントはその 4 個のアクセス ポイント間でのみローミングします。CCKM/OKC キャッシュがその 4 個のアクセス ポイント間で配布されるのは、クライアントが 1 個のアクセス ポイントにアソシエートするときだけとなります。

- この機能とバックアップ Radius およびローカル認証（ローカル EAP）により、ブランチ サイトの運用上のダウンタイムがなくなります。注：FlexConnectと非FlexConnectアクセスポイント間のCCKM/OKC高速ローミングはサポートされていません。図 12：FlexConnect グループを使用したワイヤレス ネットワーク設計リファレンス

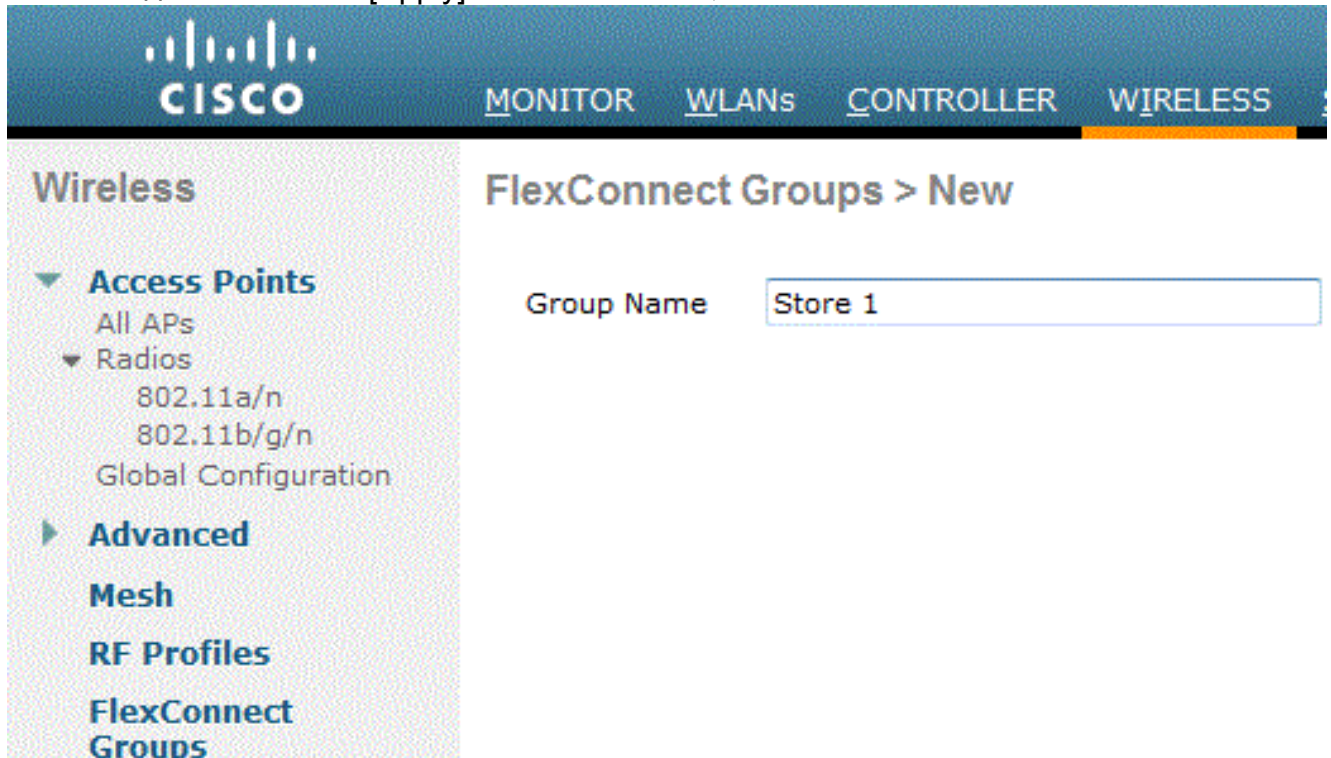


## WLC からの FlexConnect グループの設定

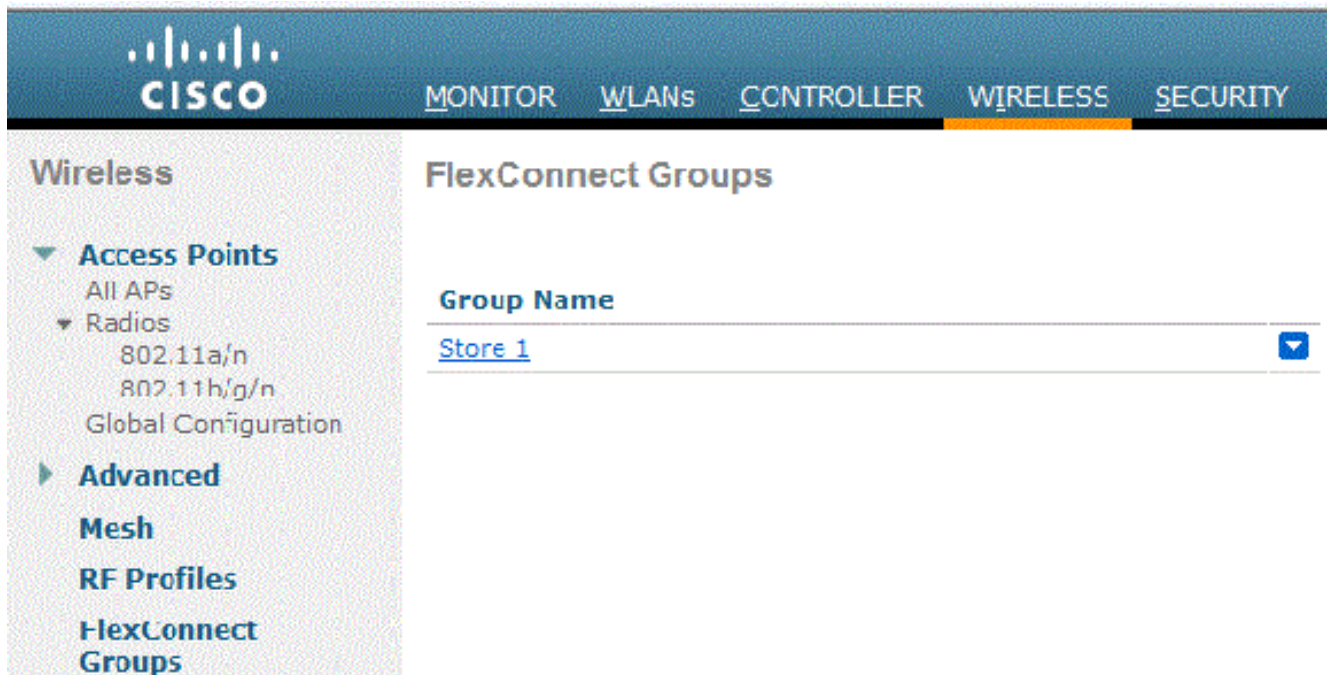
FlexConnect が接続モードまたはスタンドアロン モードのときに、LEAP を使用したローカル認証をサポートするように FlexConnect グループを設定するには、このセクションの手順を実行します。図 12 の設定例は、AP グループと FlexConnect グループの客観的な違いと 1 対 1 マッピングを示しています。

1. [Wireless] > [FlexConnect Groups] の下の [New] をクリックします。

2. [図 12](#) に示す設定例と同様に、グループ名 Store 1 を割り当てます。
3. グループ名を設定したら [Apply] をクリックします。



4. 作成したグループ名 Store 1 をクリックし、さらに設定します。



5. [Add AP] をクリックします。



The screenshot shows the Cisco FlexConnect Groups configuration interface. The left sidebar contains a navigation menu with the following items: Wireless, Access Points (All APs, Radios (802.11a/n, 802.11b/g/n, Global Configuration)), Advanced, Mesh, RF Profiles, FlexConnect Groups (selected), and FlexConnect ACLs. The main content area is titled 'FlexConnect Groups > Edit 'Store 1''. It features three tabs: 'General', 'Local Authentication', and 'Image Upgrade'. The 'Local Authentication' tab is active. Under this tab, the 'Group Name' is set to 'Store 1'. Below this is a section titled 'FlexConnect APs' with an 'Add AP' button. At the bottom, there is a table with columns 'AP MAC Address', 'AP Name', and 'Status'.

6. AP がスタンドアロン モードのときにローカル認証をイネーブルにするには、[Enable AP Local Authentication] ボックスをオンにします。注：ステップ20は、接続モードAPのローカル認証を有効にする方法を示しています。
7. [AP Name] ドロップダウン メニューを有効にするには、[Select APs from current controller] ボックスをオンにします。
8. この FlexConnect グループに含める必要がある AP をドロップダウンから選択します。
9. AP をドロップダウンから選択した後、[Add] をクリックします。
10. 手順7と8を繰り返して、APグループストア1にも含まれるこのFlexConnectグループにすべてのAPを追加します。APグループとFlexConnectグループの1:1マッピングについて [図 12](#)を参照してください。店舗ごとに AP グループを作成した場合は ([図 8](#))、その AP グループのすべての AP がこの FlexConnect グループに属するのが理想です ([図 12](#))。AP グループと FlexConnect グループの比率を 1 対 1 に保つことにより、ネットワーク管理が簡単になります。



The screenshot shows the Cisco FlexConnect Groups configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Wireless' and contains a tree view with categories like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', '802.11a/n', '802.11b/g/n', 'Media Stream', and 'Country'. The main content area is titled 'FlexConnect Groups > Edit 'Store 1'' and has three tabs: 'General', 'Local Authentication', and 'Image Upgrade'. The 'Local Authentication' tab is active. Under the 'FlexConnect APs' section, there is an 'Add AP' form with the following fields: 'Select APs from current controller' (checked), 'AP Name' (dropdown menu showing 'AP3500'), and 'Ethernet MAC' (text input showing '00:22:90:e3:37:df'). There are 'Add' and 'Cancel' buttons below the form. At the bottom, a table header is visible with columns for 'AP MAC Address', 'AP Name', and 'Status'.

11. [Local Authentication] > [Protocols] をクリックし、[Enable LEAP Authentication] ボックスをオンにします。
12. チェックボックスを設定した後、[Apply] をクリックします。注：バックアップコントローラがある場合は、FlexConnectグループが同一で、AP MACアドレスエントリがFlexConnectグループごとに含まれていることを確認してください。



General Local Authentication Image Upgrade VLAN-ACL mapping

Local Users Protocols

LEAP

Enable LEAP Authentication

EAP Fast

Enable EAP Fast Authentication

Server Key (in hex)  Enable Auto key generation

Authority ID (in hex) 436973636f00000000000000000000000000000000

Authority Info Cisco\_A\_ID

PAC Timeout (2 to 4095 days)

13. [Local Authentication] の [Local Users] をクリックします。
14. AP 上にあるローカル EAP サーバ内にユーザ エントリを作成するには、[Username]、[Password]、および [Confirm Password] フィールドを設定し、[Add] をクリックします。
15. ローカル ユーザ名リストがなくなるまでステップ 13 を繰り返します。100 人を超えるユーザの設定や追加はできません。
16. ステップ 14 が完了したら [Apply] をクリックし、[No of Users] の数を確認します。

General Local Authentication Image Upgrade VLAN-ACL mapping

Local Users Protocols

No of Users 0 Add User

User Name

Upload CSV file

File Name

UserName cisco

Password

Confirm Password

Add

17. 上部のペインで [WLANs] をクリックします。
18. [WLAN ID 17] をクリックします。これは AP グループの作成時に作成されたものです。 [図 8](#)

を参照してください。

The screenshot shows the Cisco WLANs configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows a tree view with 'WLANs' expanded, containing 'WLANs' and 'Advanced'. The main content area is titled 'WLANs' and shows a table of WLANs. The table has columns for 'WLAN ID', 'Type', 'Profile Name', and 'WLAN SSID'. Two WLANs are listed: ID 2 (Type: WLAN, Profile Name: Guest, WLAN SSID: Guest) and ID 17 (Type: WLAN, Profile Name: Store-1, WLAN SSID: Store). The 'Current Filter' is set to 'None'.

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID
<input type="checkbox"/>	2	WLAN	Guest	Guest
<input type="checkbox"/>	17	WLAN	Store-1	Store

19. [WLAN] > [Edit for WLAN ID 17] の下で、[Advanced] をクリックします。

20. 接続モードでローカル認証をイネーブルにするには、[FlexConnect Local Auth] ボックスをオンにします。注：ローカル認証は、ローカルスイッチングを使用するFlexConnectでのみサポートされます。注：WLANでローカル認証を有効にする前に、必ずFlexConnectグループを作成してください。



## WLANs > Edit 'Store-1'

General	Security	QoS	Advanced
P2P Blocking Action			Disabled
Client Exclusion <a href="#">3</a>	<input checked="" type="checkbox"/> Enabled		60 Timeout Value (secs)
Maximum Allowed Clients <a href="#">8</a>		0	
Static IP Tunneling <a href="#">11</a>	<input type="checkbox"/> Enabled		
Wi-Fi Direct Clients Policy			Disabled
Maximum Allowed Clients Per AP Radio		200	
<b>Off Channel Scanning Defer</b>			
Scan Defer Priority		<b>0</b>	<b>1</b>
		<input type="checkbox"/>	<input type="checkbox"/>
		<b>2</b>	<b>3</b>
		<input type="checkbox"/>	<input type="checkbox"/>
		<b>4</b>	<b>5</b>
		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		<b>6</b>	<b>7</b>
		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan Defer Time (msecs)		100	
<b>FlexConnect</b>			
FlexConnect Local Switching <a href="#">2</a>	<input checked="" type="checkbox"/> Enabled		
FlexConnect Local Auth <a href="#">12</a>	<input checked="" type="checkbox"/> Enabled		
Learn Client IP Address <a href="#">5</a>	<input checked="" type="checkbox"/> Enabled		

NCS には

、次に示すように、接続モードでローカル認証をイネーブルにするための [FlexConnect Local Auth] チェックボックスもあります。



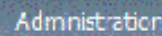
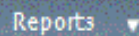
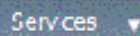
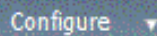
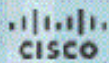
Properties > System > **WLANs** > WLAN Configuration

WLAN Configuration Details : 1  
 Configure > Controllers > [Controller Name] > WLANs > WLAN Configuration :

General Security QoS **Advanced**

HexConnect Local Switching	<input checked="" type="checkbox"/>	Enable
FlexConnect Local Auth ⓘ	<input checked="" type="checkbox"/>	Enable
Learn Client IP Address	<input checked="" type="checkbox"/>	Enable
Session Timeout	<input type="checkbox"/>	Enable
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enable
Aironet IE	<input checked="" type="checkbox"/>	Enable
IPv6 ⓘ	<input type="checkbox"/>	Enable
Diagnostic Channel ⓘ	<input type="checkbox"/>	Enable
Override Interface ACL	IPv4	NONE
Peer to Peer Blocking ⓘ		Disable
Wi-Fi Direct Clients Policy		Disabled
Client Exclusion ⓘ	<input checked="" type="checkbox"/>	Enable
Timeout Value		60 (secs)

NCS は、次に示すように、FlexConnect でローカルに認証されたクライアントをフィルタおよびモニタするための機能も備えています。



## Clients and Users



Refresh



Test



Useful



Remove



More



Track Clients



Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name
<input type="radio"/>	00:22:90:1b:17:42		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	1c:df:0f:66:86:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:6e:97:9b:bc		IPv4	husl/vikal... 	Intel	oeap-ta-war-2	
<input type="radio"/>	00:22:90:1b:96:48		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:90:1b:17:8c		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	00:25:0b:4d:77:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	c4:7d:4f:3a:c5:d5		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:a0:d5:03:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	f3:66:f2:67:7f:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:17:ca:bc:01:b4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	88:43:e1:d1:df:02		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:bd:1b:e2:b5		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	f3:66:f2:ab:1e:69		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1c:58:dc:b4:4e		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1e:7a:0b:21:8d		IPv4	ssimm		Cisco	oeap-ta-war-2



Virtual Domain: ROOT-DOMAIN    root ▼    Log Out    🔍

Total 299

Location	VLAN	Status	Interface
Unknown	109	Associated	Gi1/0/34
Unknown	109	Associated	Gi1/0/26
Root Area	310	Associated	data
Unknown	109	Associated	Gi1/0/36
Unknown	109	Associated	Gi1/0/32
Unknown	109	Associated	Gi1/0/30
Unknown	109	Associated	Gi1/0/13
Unknown	109	Associated	Gi1/0/27
Unknown	109	Associated	Gi1/0/12
Unknown	109	Associated	Gi1/0/15
Unknown	109	Associated	Gi1/0/28
Unknown	109	Associated	Gi1/0/14
Unknown	109	Associated	Gi1/0/9
Unknown	109	Associated	Gi1/0/29
Root Area	311	Associated	voice

Associated Clients

- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- 2.4GHz Clients
- 5GHz Clients
- All Lightweight Clients
- All Autonomous Clients
- All Wired Clients
- Associated Clients
- Clients known by ISE
- Clients detected by MSE
- Clients detected in the last 24 hours
- Clients with Problems
- Excluded Clients
- FlexConnect Locally Authenticated
- New clients detected in last 24 hours
- On Network Clients

## CLI を使用した確認

クライアント認証状態とスイッチング モードは、WLC 上で次の CLI を使用してすばやく確認できます。

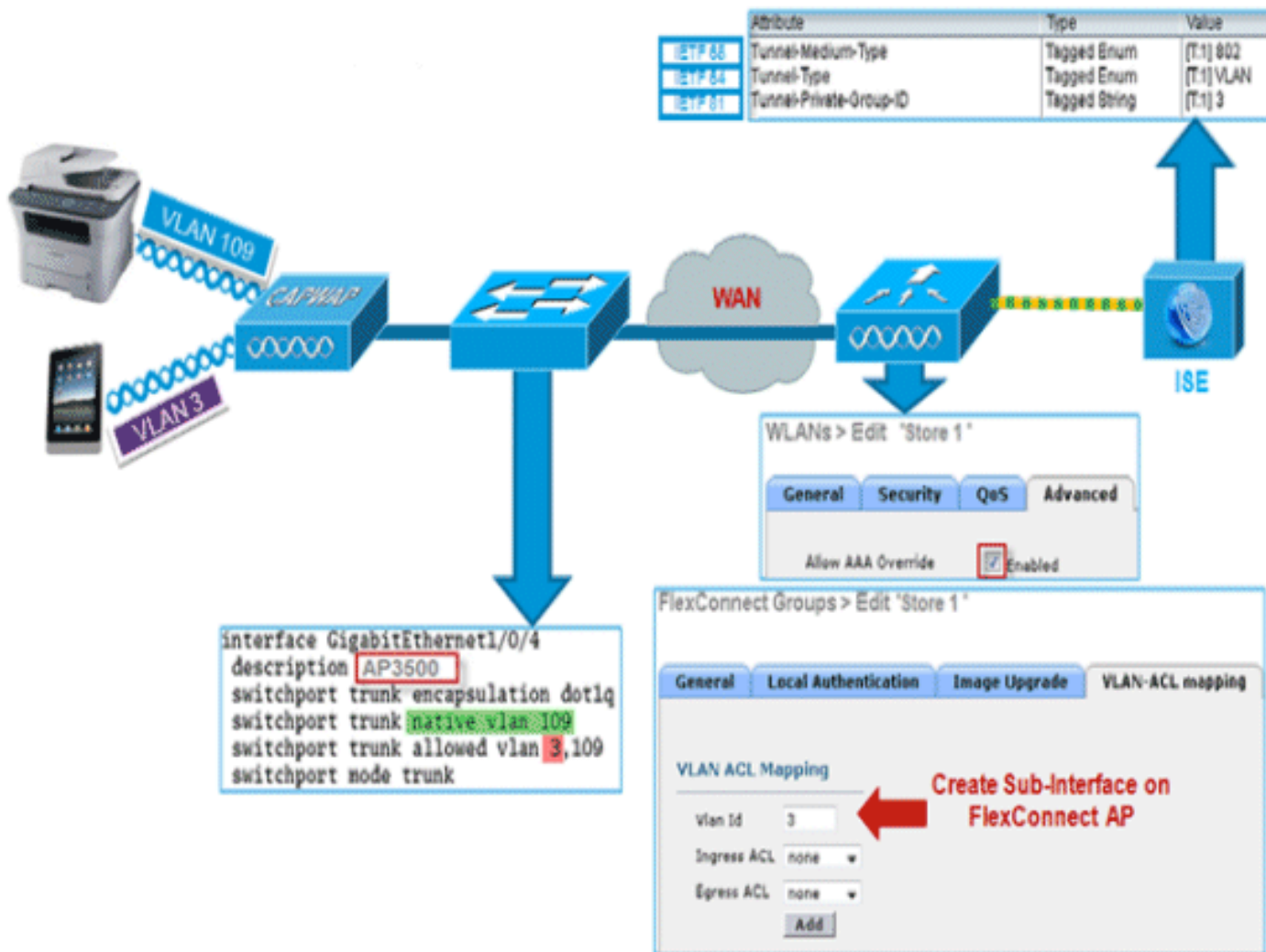
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address..... 00:24:d7:2b:7c:0c
Client Username ..... N/A
AP MAC Address..... d0:57:4c:08:e6:70
Client State..... Associated
H-REAP Data Switching..... Local
H-REAP Authentication..... Local
```

## FlexConnect VLAN オーバーライド

現在の FlexConnect アーキテクチャでは、WLAN から VLAN への厳密なマッピングがあるため、FlexConnect AP 上で特定の WLAN にアソシエーションされたクライアントは、それにマッピン

グされる VLAN に従う必要があります。この方式は、異なる VLAN ベースのポリシーを継承するために各クライアントを異なる SSID にアソシエーションする必要があるため、さまざまな制約があります。

7.2 リリースより、ローカル スイッチングが設定された個々の WLAN に対する、VLAN の AAA オーバーライドがサポートされています。AP には、動的に VLAN を割り当てるために、個別の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、FlexConnect グループの ACL-VLAN マッピングを使用した設定に基づいて事前に作成された、VLAN 用のインターフェイスがあります。WLC は、AP でサブインターフェイスを事前作成するために使用されます。



## 要約

- AAA VLAN オーバーライドは、中央およびローカル認証モードでローカル スイッチングが設定された WLAN について、リリース 7.2 からサポートされています。
- AAA オーバーライドは、ローカル スイッチングが設定された WLAN 上でイネーブルにする必要があります。
- FlexConnect AP には、ダイナミック VLAN 割り当て用に、WLC から VLAN が事前に作成されている必要があります。
- AAA オーバーライドから返された VLAN が AP クライアント上にない場合は、VLAN の IP は AP のデフォルト VLAN インターフェイスから取得されます。

## 手順



次のステップを実行します。

1. 802.1x 認証用の WLAN を作成します。

The screenshot shows the 'WLANs > Edit 'Store 1'' configuration page. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. Below it, the 'WPA+WPA2 Parameters' section is visible, with a red box highlighting the following settings: 'WPA2 Policy' (checked), 'WPA2 Encryption' (checked) with 'AES' selected and 'TKIP' unselected, and 'Auth Key Mgmt' (dropdown) set to '802.1X'. Other settings include 'WPA Policy' (unchecked) and 'WPA gtk-randomize State' (dropdown) set to 'Disable'.

2. WLC 上のローカル スイッチング WLAN 用に AAA オーバーライドのサポートをイネーブルにします。[WLAN GUI] > [WLAN] > [WLAN ID] > [Advance] タブに移動します。

The screenshot shows the 'WLANs > Edit 'Store 1'' configuration page, with the 'Advanced' tab selected. A red box highlights the 'Allow AAA Override' checkbox, which is checked and labeled 'Enabled'. Another red box highlights the 'FlexConnect Local Switching' checkbox, also checked and labeled 'Enabled'. The page contains various other configuration options such as 'Coverage Hole Detection', 'Session Timeout', 'Aironet IE', 'Diagnostic Channel', 'Override Interface ACL', 'P2P Blocking Action', 'Client Exclusion', 'Maximum Allowed Clients', 'Static IP Tunneling', 'Wi-Fi Direct Clients Policy', 'Off Channel Scanning Defer', 'DHCP', 'Management Frame Protection (MFP)', 'DTIM Period', 'NAC', 'Load Balancing and Band Select', 'Passive Client', and 'Voice'.

3. 802.1x 認証用に AAA サーバの詳細をコントローラに追加します。AAA サーバを追加するためには、[WLC GUI] > [Security] > [AAA] > [Radius] > [Authentication] > [New] に移動します。

**Security**

- AAA
  - General
  - RADIUS
    - Authentication**
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies

**RADIUS Authentication Servers > Edit**

Server Index: 1

Server Address: [Redacted]

Shared Secret Format: ASCII

Shared Secret: [Masked]

Confirm Shared Secret: [Masked]

Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User:  Enable

Management:  Enable

IPSec:  Enable

4. AP はデフォルトでローカル モードになっているため、モードを FlexConnect モードに変換します。[Wireless] > [All APs] を選択し、[Individual AP] をクリックすることで、ローカルモードの AP を FlexConnect モードに変換できます。

**All APs > Details for AP3500**

General | **Credentials** | Interfaces | High Availability | Inventory | Advanced

**General**

AP Name: AP3500

Location: default location

AP MAC Address: cc:ef:48:c2:35:57

Base Radio MAC: 2c:3f:38:f6:98:b0

Admin Status: Enable

AP Mode: FlexConnect

AP Sub Mode: None

Operational Status: REG

Port Number: 1

Venue Group: Unspecified

Venue Type: Unspecified

Venue Name: [Empty]

Language: [Empty]

Network Spectrum Interface Key: 0D45BA896226F4117D98BA920FBA8A16

**Versions**

Primary Software Version: 7.2.1.69

Backup Software Version: 7.2.1.72

Predownload Status: None

Predownloaded Version: None

Predownload Next Retry Time: NA

Predownload Retry Count: NA

Boot Version: 12.4.23.0

IOS Version: 12.4(20111122:141426)\$

Mini IOS Version: 7.0.112.74

**IP Config**

IP Address: 10.10.10.132

Static IP:

**Time Statistics**

UP Time: 0 d, 00 h 01 m 14 s

Controller Associated Time: 0 d, 00 h 00 m 14 s

Controller Association Latency: 0 d, 00 h 00 m 59 s

5. FlexConnect AP を FlexConnect グループに追加します。[WLC GUI] > [Wireless] > [FlexConnect Groups] > FlexConnect グループを選択 > [General] タブ > [Add AP] に移動します。

The screenshot shows the 'FlexConnect Groups > Edit 'Store 1'' configuration page. The 'General' tab is active. Under 'FlexConnect APs', the 'Add AP' section is highlighted with a red box. It includes a checked checkbox for 'Select APs from current controller', a dropdown for 'AP Name' set to 'AP3500', and a text field for 'Ethernet MAC' set to 'cc:ef:48:c2:35:57'. There are 'Add' and 'Cancel' buttons below. To the right, the 'AAA' section shows 'Primary Radius Server' and 'Secondary Radius Server' both set to 'None', and 'Enable AP Local Authentication' is unchecked.

6. FlexConnect AP は、トランク ポート上で接続され、WLAN にマッピングされた VLAN と AAA オーバーライドされた VLAN がトランク ポート上で許可されている必要があります。

```
interface GigabitEthernet1/0/4
description AP3500
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk
```

注：この設定では、WLAN VLANマッピングに vlan 109が使用され、AAAオーバーライドにvlan 3が使用されます。

7. FlexConnect AP の WLAN から VLAN へのマッピングを設定します。この設定に基づき、AP に VLAN 用のインターフェイスが設定されます。AP が VLAN の設定を受信すると、対応する dot11 およびイーサネット サブインターフェイスが作成され、ブリッジグループに追加されます。この WLAN 上にクライアントをアソシエーションします。クライアントがアソシエーションされるときに、その VLAN ( デフォルト、WLAN-VLAN マッピングに基づきます ) が割り当てられます。[WLAN GUI] > [Wireless] > [All APs] > 特定の AP をクリック > [FlexConnect] タブに移動し、[VLAN Mapping] をクリックします。

The screenshot shows the 'All APs > AP3500 > VLAN Mappings' configuration page. It displays the AP details and a table of VLAN mappings.

All APs > AP3500 > VLAN Mappings		
<b>AP Name</b>		AP3500
<b>Base Radio MAC</b>		2c:3f:38:f6:98:b0
WLAN Id	SSID	VLAN ID
1	Store 1	109

8. AAA サーバでユーザを作成し、IETF Radius 属性の中で VLAN ID を返すようにユーザを設定します。

	Attribute	Type	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

9. AP には、動的に VLAN を割り当てるために、個別の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、FlexConnect グループの ACL-VLAN マッピングを使用した設定に基づいて事前に作成された、ダイナミック VLAN 用のインターフェイスがあります。FlexConnect AP 上で AAA VLAN を設定するために、[WLC GUI] > [Wireless] > [FlexConnect Group] > 特定の FlexConnect グループをクリック > [VLAN-ACL mapping] に移動し、[Vlan ID] フィールドに VLAN を入力します。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

**VLAN ACL Mapping**

Vlan Id

Ingress ACL

Egress ACL

10. AAA VLAN を返すために、この WLAN にクライアントをアソシエーションし、AAA サーバで設定したユーザ名を使用して認証します。
11. クライアントは、AAA サーバを通じて返されたダイナミック VLAN から IP アドレスを取得します。
12. 確認のため、[WLC GUI] > [Monitor] > [Client] > 特定のクライアントの MAC アドレスをクリックして、クライアントの詳細を確認します。

## 制限

- Cisco Airespace 固有の属性はサポートされず、IETF 属性 VLAN ID のみがサポートされます。
- 個別の FlexConnect AP の WLAN-VLAN マッピングを通じて、または FlexConnect グループの ACL-VLAN マッピングを使用して、AP 設定ごとに最大 16 個の VLAN を設定できます。

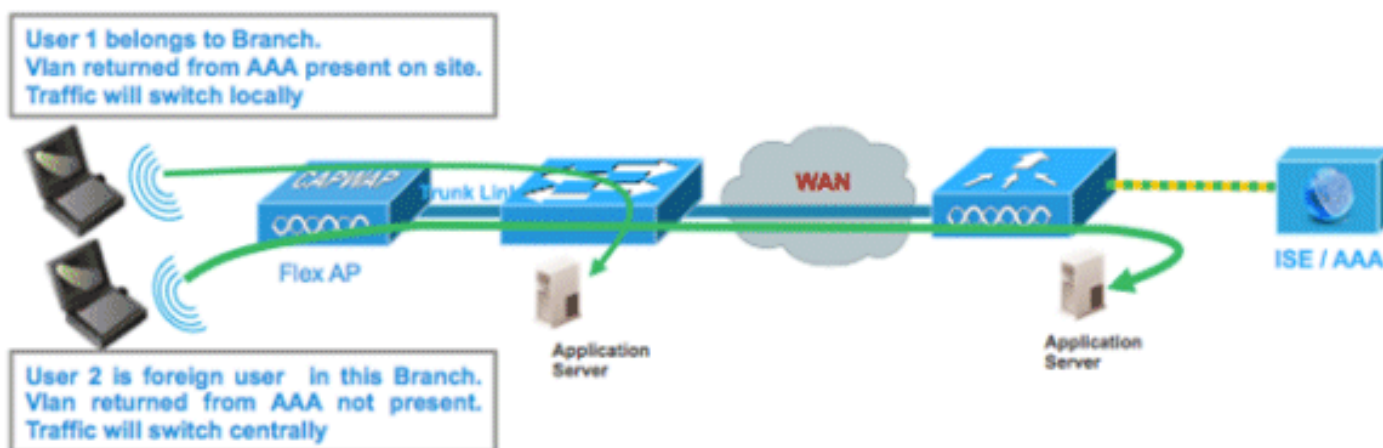
## FlexConnect VLAN に基づく中央スイッチング

コントローラ ソフトウェア リリース 7.2 では、ローカルにスイッチングされる WLAN に対する VLAN の AAA オーバーライド (ダイナミック VLAN 割り当て) により、ワイヤレスクライアントが AAA サーバで提供される VLAN に配置されます。AAA サーバから渡された VLAN が AP に存在しない場合、クライアントはその AP 上で WLAN からマッピングされた VLAN に配置され、トラフィックはその VLAN でローカルにスイッチングされます。さらに、7.3 よりも前のリリースでは、FlexConnect AP からの特定の WLAN のトラフィックは、WLAN の設定に応じて中央またはローカルでスイッチングされます。

リリース 7.3 から、FlexConnect AP からのトラフィックは、FlexConnect AP 上に VLAN が存在



するかどうかに応じて、中央またはローカルでスイッチングされます。



## 要約

Flex AP が接続モードの場合に、ローカルスイッチングが設定された WLAN 上のトラフィックフローは、次のようになります。

- VLAN が AAA 属性の 1 つとして返され、その VLAN が Flex AP データベースに存在しない場合、トラフィックは中央でスイッチングされ、VLAN が WLC 上に存在する限り、AAA サーバから返されたこの VLAN とインターフェイスがクライアントに割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が Flex AP データベースに存在しない場合、トラフィックは中央でスイッチングされます。その VLAN が WLC にも存在しない場合、クライアントには WLC 上で WLAN にマッピングされた VLAN とインターフェイスが割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在する場合、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

Flex AP がスタンドアロンモードの場合に、ローカルスイッチングが設定された WLAN 上のトラフィックフローは、次のようになります。

- AAA サーバによって返された VLAN が Flex AP データベースに存在しない場合、クライアントはデフォルト VLAN (つまり、Flex AP 上で WLAN にマッピングされた VLAN) に配置されます。AP が接続するとき、このクライアントは認証を解除され、トラフィックが中央でスイッチングされます。
- AAA サーバによって返された VLAN が Flex AP データベースに存在する場合、クライアントは返された VLAN に配置され、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

## 手順

次のステップを実行します。

1. WLAN でローカルスイッチングを設定し、AAA オーバーライドをイネーブルにします。

## WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
<b>Allow AAA Override</b>	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	<input type="text" value="1800"/>	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
Diagnostic Channel	<input type="checkbox"/>	Enabled	
Override Interface ACL		IPv4 <input type="text" value="None"/>	IPv6 <input type="text" value="None"/>
P2P Blocking Action		<input type="text" value="Disabled"/>	
Client Exclusion <sup>3</sup>	<input checked="" type="checkbox"/>	Enabled	<input type="text" value="60"/> Timeout Value (secs)
Maximum Allowed Clients <sup>6</sup>		<input type="text" value="0"/>	
Static IP Tunneling <sup>11</sup>	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		<input type="text" value="Disabled"/>	
Maximum Allowed Clients Per AP Radio		<input type="text" value="200"/>	
<b>FlexConnect</b>			
<b>FlexConnect Local Switching <sup>2</sup></b>	<input checked="" type="checkbox"/>	Enabled	

2. 新たに作成した WLAN に対して [Vlan based Central Switching] をイネーブルにします。

## WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
Diagnostic Channel	<input type="checkbox"/>	Enabled	
Override Interface ACL	IPv4	None	IPv6 None
P2P Blocking Action		Disabled	
Client Exclusion <sup>3</sup>	<input checked="" type="checkbox"/>	Enabled	60 Timeout Value (secs)
Maximum Allowed Clients <sup>8</sup>		0	
Static IP Tunneling <sup>11</sup>	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		Disabled	
Maximum Allowed Clients Per AP Radio		200	
<b>FlexConnect</b>			
FlexConnect Local Switching <sup>2</sup>	<input checked="" type="checkbox"/>	Enabled	
FlexConnect Local Auth <sup>12</sup>	<input type="checkbox"/>	Enabled	
Learn Client IP Address <sup>5</sup>	<input checked="" type="checkbox"/>	Enabled	
Vlan based Central Switching <sup>13</sup>	<input checked="" type="checkbox"/>	Enabled	

3. [AP Mode] を [FlexConnect] に設定します。

All APs > Details for AP\_3500E

General Credentials Interfaces High Availability

General

AP Name AP\_3500E

Location

AP MAC Address 04:7d:4f:3a:07:74

Base Radio MAC 04:7d:4f:53:24:e0

Admin Status Enable

AP Mode FlexConnect

AP Sub Mode

Operational Status

Port Number

Venue Group

local  
FlexConnect  
monitor  
Rogue Detector  
Sniffer  
Bridge  
SE-Connect

4. 特定の Flex AP 上の WLAN-VLAN マッピングが、Flex グループからの VLAN の設定を通じて、FlexConnect AP のデータベースにいくつかのサブインターフェイスがあることを確認します。この例で、VLAN 63 が Flex AP 上の WLAN-VLAN マッピングで設定されています

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY

Wireless

Access Points

Radios

Global Configuration

Advanced

Mesh

RF Profiles

FlexConnect Groups

FlexConnect ACLs

802.11a/n

802.11b/g/n

Media Stream

Country

Timers

QoS

All APs > AP\_3500E > VLAN Mappings

AP Name AP\_3500E

Base Radio MAC 04:7d:4f:53:24:e0

WLAN Id	SSID	VLAN ID
1	'Store 1' :	63

Centrally switched Wlans

WLAN Id	SSID	VLAN ID

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
63	none	none

Group level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL

5. この例で、VLAN 62 がダイナミック インターフェイスの 1 つとして WLC 上で設定されており、WLC 上で WLAN にマッピングされていません。WLC 上の WLAN は、管理 VLAN (つまり VLAN 61) にマッピングされています。



CISCO					
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK					
Controller	Interfaces				
General					
Inventory					
Interfaces					
Interface Groups					
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
dyn	62	9.6.62.10	Dynamic	Disabled	
management	61	9.6.61.2	Static	Enabled	

6. この Flex AP 上でステップ 1 で設定した WLAN にクライアントをアソシエーションし、AAA サーバから VLAN 62 を返します。VLAN 62 はこの Flex AP に存在しませんが、WLC 上にダイナミック インターフェイスとして存在するため、トラフィックは中央でスイッチングされ、クライアントには WLC 上の VLAN 62 が割り当てられます。次に示す出力で、クライアントには VLAN 62 が割り当てられ、[Data Switching] と [Authentication] は [Central] に設定されています。

Monitor		Clients > Detail	
Summary			
Access Points			
Cisco CleanAir			
Statistics			
CDP			
Rogues			
Redundancy			
Clients			
Multicast			
Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.62.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
Client Type	Regular	WLAN Profile	'Store 1'
User Name	betauser	Data Switching	Central
Port Number	1	Authentication	Central
Interface	dyn	Status	Associated
VLAN ID	62	Association ID	1
		802.11 Authentication	Open System
		Reason Code	3
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

注：WLANはローカルスイッチング用に設定されていますが、このクライアントの[Data Switching]フィールドはVLANの存在に基づいて中央に配置されています（つまり、AAAサーバから返されるVLAN 62はAPデータベースに存在しません）。

7. 別のユーザがこの作成した WLAN 上で同じ AP にアソシエーションされ、AP にも WLC にも存在しないいくつかの VLAN が AAA サーバから返された場合、トラフィックは中央でスイッチングされ、クライアントには WLC 上で WLAN にマッピングされたインターフェイスが割り当てられます（この例では VLAN 61）。これは、WLAN が、VLAN 61 が設定されている管理インターフェイスにマッピングされるためです。

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	*Store 1*
		Data Switching	Central
		Authentication	Central
Client Type	Regular	Status	Associated
User Name	betouser2	Association ID	1
Port Number	1	802.11 Authentication	Open System
Interface	management	Reason Code	3
VLAN ID	61	Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

注：WLANがローカルスイッチング用に設定されているが、このクライアントの[Data Switching]フィールドがVLANの存在に基づいて中央であることを確認します。つまり、AAAサーバから返されるVLAN 61がAPデータベースに存在しないものの、WLCデータベースにも存在しません。その結果、クライアントには、WLANにマッピングされているデフォルトインターフェイスのVLANとインターフェイスが割り当てられます。この例で、WLANは管理インターフェイス（つまりVLAN 61）にマッピングされているため、クライアントはVLAN 61からIPアドレスを取得しました。

8. 別のユーザがこの作成されたWLAN上でそれにアソシエーションされ、AAAサーバ（このFlex AP上に存在）からVLAN 63が返された場合、クライアントにはVLAN 63が割り当てられ、トラフィックはローカルにスイッチングされます。

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d: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

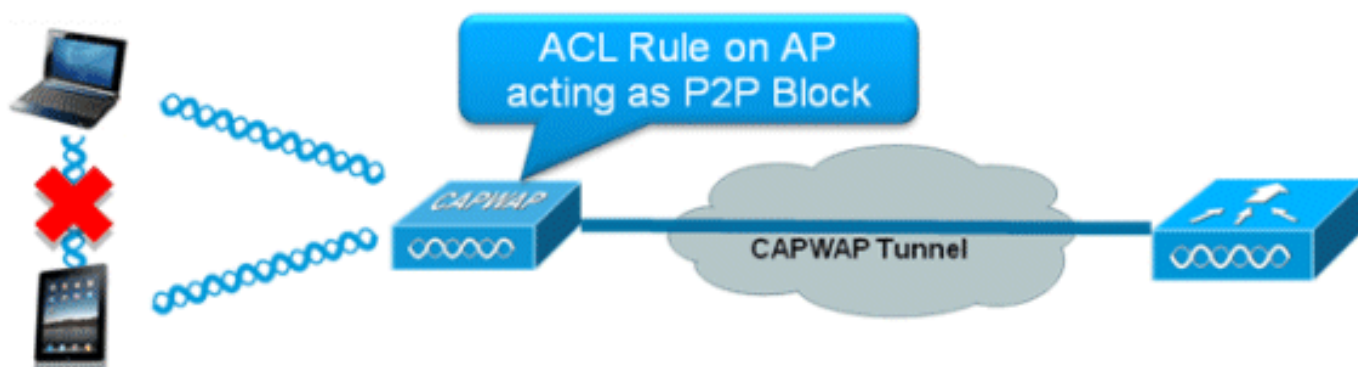
## 制限

- VLANベースの中央スイッチングは、中央認証とローカルスイッチングが設定されたWLANのみでサポートされています。
- APサブインターフェイス（つまりVLANマッピング）がFlexConnect AP上で設定されてい

る必要があります。

## FlexConnect ACL

FlexConnect 上での ACL の導入に伴い、AP からのローカルにスイッチングされるデータトラフィックの保護と整合性のために、FlexConnect AP でアクセスコントロールの必要性を満たすメカニズムがあります。FlexConnect ACL を WLC 上で作成し、FlexConnect AP が、AAA オーバーライド VLAN 用の VLAN-ACL マッピングを使用した FlexConnect グループ上に存在する VLAN を使用して設定する必要があります。これらの ACL は AP にプッシュされます。



### 要約

- コントローラで FlexConnect ACL を作成します。
- 同じことを、AP レベル VLAN ACL マッピングの下で、FlexConnect AP 上に存在する VLAN に適用します。
- VLAN-ACL マッピングの下で、FlexConnect グループに存在する VLAN に適用できます (一般に AAA オーバーライドされた VLAN に対して行います)。
- VLAN に対して ACL を適用する際に、適用する方向として「ingress」、「egress」、または「ingress and egress」を選択します。

### 手順

次のステップを実行します。

1. WLC 上で FlexConnect ACL を作成します。[WLC GUI] > [Security] > [Access Control List] > [FlexConnect ACLs] に移動します。



2. [New] をクリックします。
3. ACL 名を設定します。

Access Control Lists > New < Back    Apply

Access Control List Name

4. [Apply] をクリックします。
5. 各 ACL のルールを作成します。ルールを作成するには、[WLC GUI] > [Security] > [Access Control List] > [FlexConnect ACLs] に移動し、上で作成した ACL をクリックします。

Access Control Lists > Edit < Back    Add New Rule

**General**

Access List Name      Flex-ACL-Ingress

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP

6. [Add New Rule] をクリックします。

Access Control Lists > Rules > New < Back    Apply

Sequence     

Source            IP Address            Netmask     

Destination            IP Address            Netmask     

Protocol     

DSCP     

Action     

**注：要件に従ってルールを設定します。最後で permit any any ルールが設定されていない場合、すべてのトラフィックをブロックする暗黙的な拒否があります。**

7. FlexConnect ACL を作成すると、個別の FlexConnect AP の下で WLAN-VLAN マッピング用にマッピングしたり、FlexConnect グループに対する VLAN-ACL マッピングに適用できます。
8. 個々の FlexConnect AP に対し、VLAN マッピングの下の個々の VLAN について、上で設定した FlexConnect ACL を AP レベルでマッピングします。[WLC GUI] > [Wireless] > [All AP] > 特定の AP をクリック > [FlexConnect] タブ > [VLAN Mapping] に移動します。

## All APs > AP3500 > VLAN Mappings

AP Name AP3500

Base Radio MAC 2c:3f:38:f6:98:b0

WLAN Id	SSID	VLAN ID
1	Store 1	109

### Centrally switched Wlans

WLAN Id	SSID	VLAN ID
2	Store 3	N/A

### AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
109	Flex-ACL-Ingress	Flex-ACL-Egress

9. FlexConnect ACL は、FlexConnect グループ内の VLAN-ACL マッピングに適用することもできます。FlexConnect グループ内の VLAN-ACL マッピングの下で作成された VLAN は、主にダイナミック VLAN オーバーライドに使用されます。

## FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

### VLAN ACL Mapping

Vlan Id

Ingress ACL

Egress ACL

Vlan Id	Ingress ACL	Egress ACL
3	Flex-ACL-Ingress	Flex-ACL-Egress

## 制限

- 最大 512 個の FlexConnect ACL を WLC に対して設定できます。
- 個々の ACL には 64 個のルールを設定できます。
- FlexConnect グループまたは FlexConnect AP あたり最大 32 個の ACL をマッピングできま



す。

- 最大 16 個の VLAN と 32 個の ACL が FlexConnect AP 上に同時に存在できます。

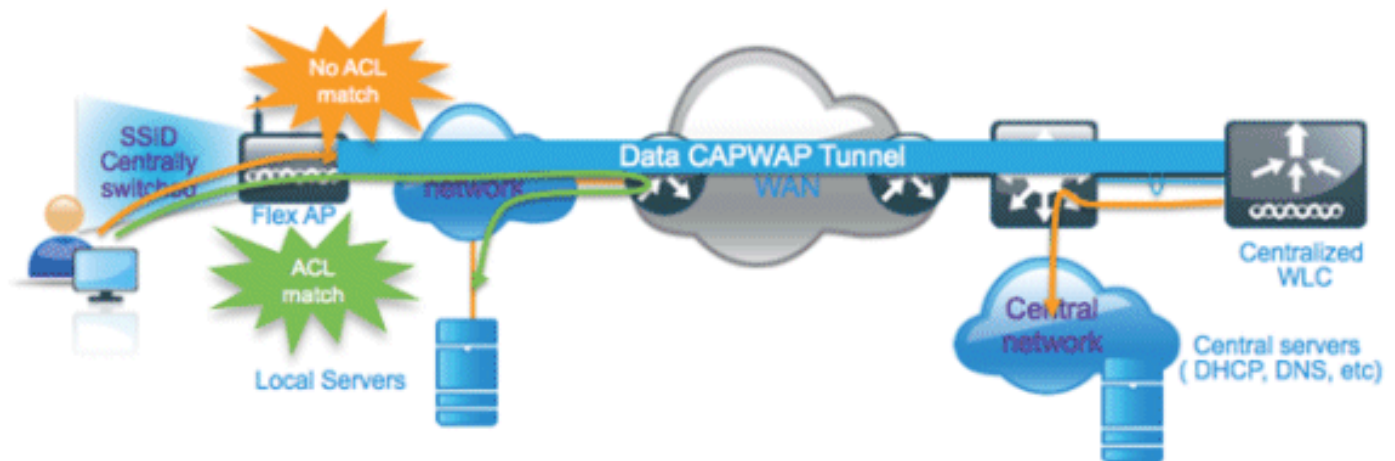
## FlexConnect スプリット トンネリング

7.3 よりも前の WLC リリースでは、中央でスイッチングされる WLAN にアソシエーションされている FlexConnect AP に接続しているクライアントが、ローカルなサイトまたはネットワークにあるデバイスに何らかのトラフィックを送信する必要がある場合、CAPWAP 経由で WLC にトラフィックを送信し、同じトラフィックを CAPWAP 経由かオフバンド接続を使用してローカルサイトに戻す必要がありました。

リリース 7.3 以降、スプリット トンネリングにより、クライアントによって送信されたトラフィックを、Flex ACL を使用し、パケットの内容に基づいて分類するメカニズムが導入されました。一致するパケットは Flex AP からローカルにスイッチングされ、残りのパケットは CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング機能には、会社の SSID 上のクライアントがローカル ネットワーク上のデバイス (プリンタ、リモート LAN ポート上の有線マシン、またはパーソナル SSID 上のワイヤレス デバイス) と直接通信でき、CAPWAP を介してパケットを送信することで WAN 帯域幅を消費することがないという、OEAP AP 構成に対するさらなるメリットがあります。スプリット トンネリングは OEAP 600 AP ではサポートされていません。Flex ACL は、ローカル サイトまたはネットワークに存在するすべてのデバイスを許可するために、ルールを使用して作成できます。会社の SSID 上のワイヤレス クライアントからのパケットが、OEAP AP 上で設定されている Flex ACL のルールに一致した場合、そのトラフィックはローカルにスイッチングされ、残りのトラフィック (つまり暗黙的に拒否されたトラフィック) は、CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング ソリューションでは、中央サイトのクライアントにアソシエーションされているサブネットまたは VLAN がローカル サイトにないことを前提としています (つまり、中央サイトにあるサブネットから IP アドレスを受け取るクライアントのトラフィックは、ローカルにスイッチングできません)。スプリット トンネリング機能は、WAN の帯域幅の使用を避けるために、ローカル サイトに属するサブネットについてトラフィックをローカルにスイッチングすることを目的としています。Flex ACL ルールに一致するトラフィックはローカルにスイッチングされ、NAT 操作が実行され、クライアントの送信元 IP アドレスが、ローカル サイトまたはネットワークでルーティング可能な Flex AP の BVI インターフェイス IP アドレスに変更されます。



## 要約

- スプリット トンネリング機能は、Flex AP のみによってアドバタイズされる、中央でのスイッチングが設定された WLAN 上でサポートされます。
- 必要な DHCP を、スプリット トンネリングが設定された WLAN 上でイネーブルにする必要があります。
- スプリット トンネリングの設定は、Flex AP ごとか、FlexConnect グループ内のすべての Flex AP に対して、中央のスイッチングが設定された WLAN ごとに適用されます。

## 手順

次のステップを実行します。

1. WLAN で中央でのスイッチングを設定します (つまり、[Flex Local Switching] をイネーブルにしません)。

WLANs > Edit 'Store 1'

General Security QoS Advanced

Allow AAA Override  Enabled

Coverage Hole Detection  Enabled

Enable Session Timeout  1800  
Session Timeout (secs)

Aironet IE  Enabled

Diagnostic Channel  Enabled

Override Interface ACL IPv4  IPv6

P2P Blocking Action

Client Exclusion  Enabled 60  
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling  Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

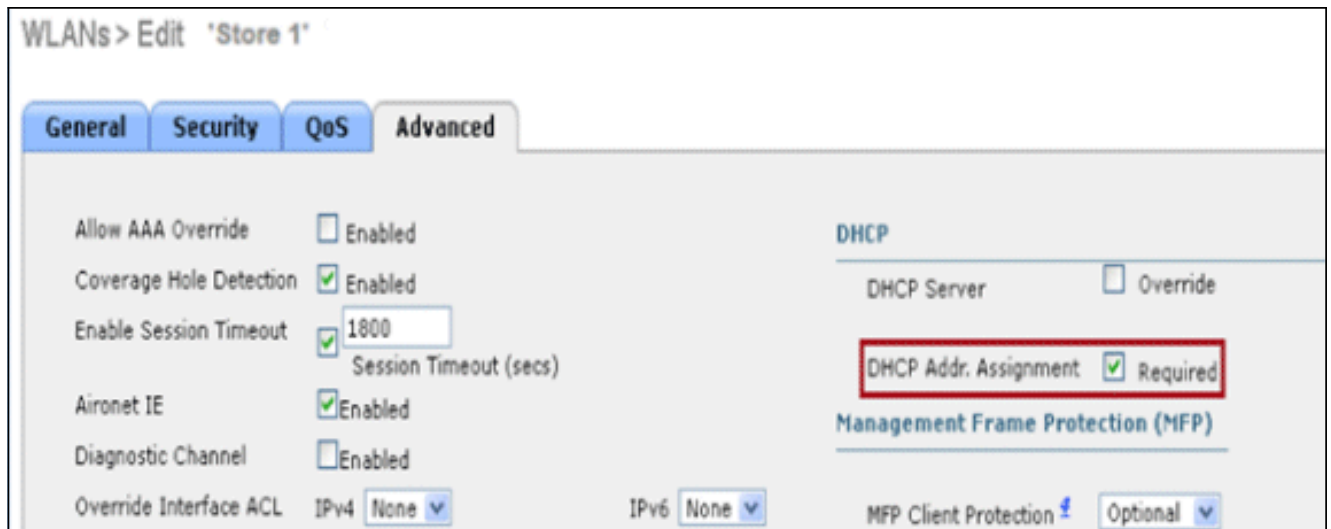
**FlexConnect**

**FlexConnect Local Switching**  Enabled

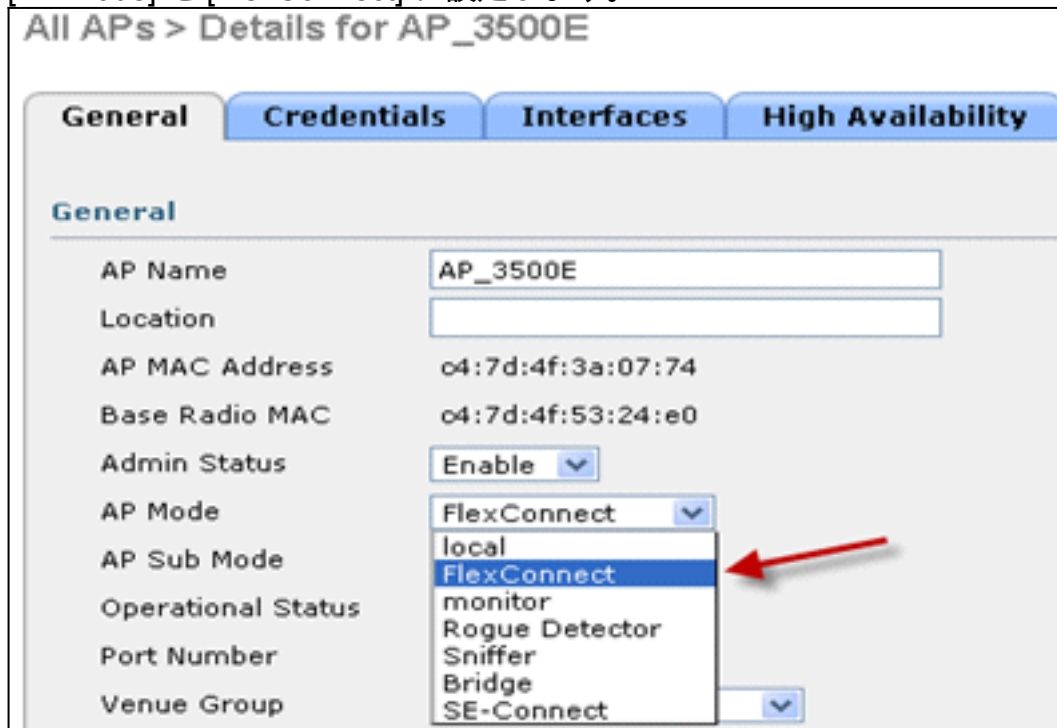
Flex Local Switching should not be enabled

2. [DHCP Address Assignment] を [Required] に設定します。





3. [AP Mode] を [FlexConnect] に設定します。



4. 中央でスイッチングされる WLAN 上でローカルにスイッチングする必要があるトラフィックに対し、許可ルールを使用して FlexConnect ACL を設定します。この例で、FlexConnect ACL ルールは、9.6.61.0 サブネット上にある（つまり中央のサイトに存在する）すべてのクライアントから、9.1.0.150 への ICMP トラフィックについて、Flex AP 上で NAT 操作を適用した後でローカルなスイッチングについてアラートを発行するよう設定されています。残りのトラフィックは暗黙的な拒否ルールに一致し、CAPWAP 経由で中央でスイッチングされます。

Wireless

Access Points

- All APs
- Radios
  - 802.11a/n
  - 802.11b/g/n
- Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Groups
  - FlexConnect ACLs

Access Control Lists > Edit

General

Access List Name: Flex-ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	9.6.61.0 / 255.255.255.0	9.1.0.150 / 255.255.255.255	ICMP	Any	Any	Any

5. この作成された FlexConnect ACL は、スプリット トンネル ACL として個々の Flex AP にプッシュするか、FlexConnect グループ内のすべての Flex AP にプッシュできます。Flex ACL をローカル スプリット ACL として個々の Flex AP にプッシュするには、次の手順を実行します。[Local Split ACLs] をクリックします。

Wireless

All APs > Details for AP\_3500E

General | Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced

VLAN Support

Native VLAN ID: 57 [VLAN Mappings](#)

FlexConnect Group Name: Not Configured

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

スプリット トンネリング機能をイネーブルにする WLAN Id を選択し、[Flex-ACL] を選択して [Add] をクリックします。

All APs > AP\_3500E > ACL Mappings

AP Name AP\_3500E

Base Radio MAC c4:7d:4f:53:24:e0

**WLAN ACL Mapping**

WLAN Id

Local-Split ACL

Enter WLAN ID on which Split Tunnel should be enabled

Click Add after selecting Flex ACL

WLAN Id	WLAN Profile Name	Local-Split ACL
---------	-------------------	-----------------

Flex-ACL は、ローカル スプリット ACL として Flex AP にプッシュされます。

All APs > AP\_3500E > ACL Mappings

AP Name AP\_3500E

Base Radio MAC c4:7d:4f:53:24:e0

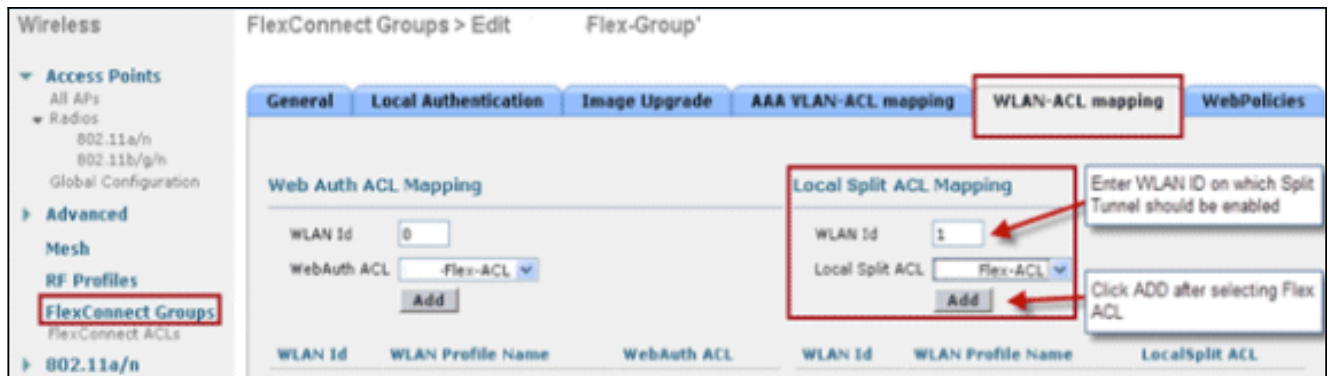
**WLAN ACL Mapping**

WLAN Id

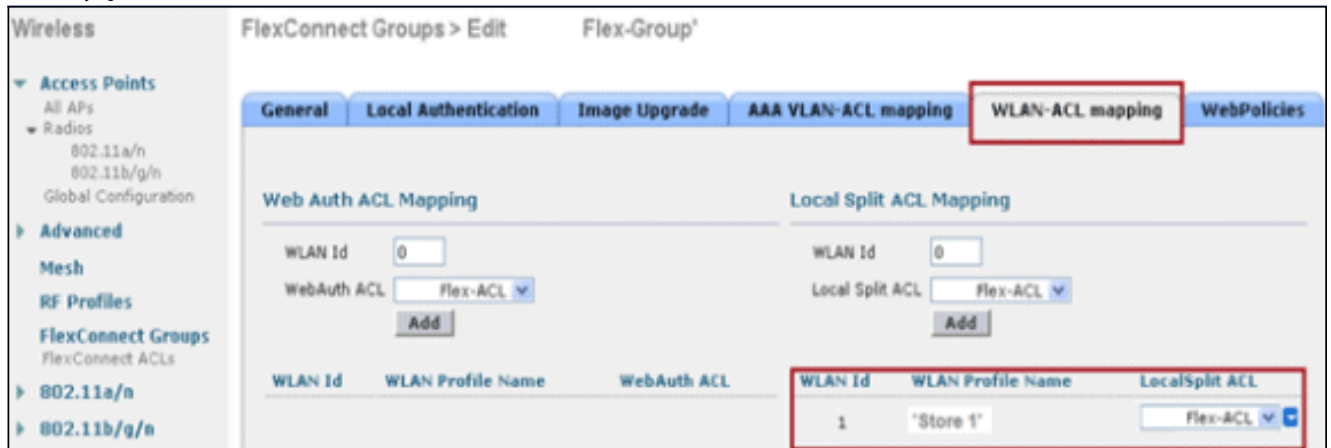
Local-Split ACL

WLAN Id	WLAN Profile Name	Local-Split ACL
1	*Store 1*	Flex-ACL <input type="button" value="v"/>

Flex ACL をローカル スプリット ACL として FlexConnect グループにプッシュするには、次の手順を実行します。スプリット トンネリング機能をイネーブルにする WLAN Id を選択します。[WLAN-ACL mapping] タブで、特定の Flex AP を追加する FlexConnect グループから FlexConnect ACL を選択し、[Add] をクリックします。



Flex-ACL がローカル スプリット ACL としてその Flex グループ内の Flex AP にプッシュされます。



## 制限

- Flex ACL ルールは、同じサブネットを送信元および宛先とする permit/deny 文を使用して設定できません。
- スプリット トンネリングが設定された、中央でスイッチングされる WLAN 上のトラフィックをローカルにスイッチングできるのは、ワイヤレス クライアントがローカル サイト上にあるホスト宛のトラフィックを送信した場合のみです。トラフィックが、ローカル サイト上のクライアントまたはホストにより、これらの設定された WLAN 上のワイヤレス クライアントに送信された場合、宛先に到達できません。
- マルチキャストまたはブロードキャストトラフィックについては、スプリット トンネリングはサポートされていません。マルチキャストまたはブロードキャストトラフィックは、Flex ACL に一致しても中央でスイッチングされます。

## 耐障害性

FlexConnect Fault Tolerance を使用すると、次の場合に、ブランチ クライアントに対するワイヤレス アクセスとサービスが可能です。

- FlexConnect Branch AP がプライマリ Flex 7500 コントローラへの接続を失った場合。
- FlexConnect Branch AP はセカンダリ Flex 7500 コントローラに切り換えます。
- FlexConnect Branch AP は、プライマリ Flex 7500 コントローラへの接続を再確立します。

FlexConnect Fault Tolerance は、上で説明したローカル EAP と共に、ネットワーク停止時のゼロ ブランチ ダウンタイムを提供します。この機能はデフォルトでイネーブルになっており、ディセーブルにできません。コントローラまたは AP での設定は不要です。ただし、Fault Tolerance が円滑に機能し適用可能であるためには、次の条件を満たす必要があります。

- WLAN の順序と設定は、プライマリとバックアップの Flex 7500 コントローラで同じであることが必要です。
- VLAN マッピングは、プライマリとバックアップの Flex 7500 コントローラで同じであることが必要です。
- モビリティドメイン名は、プライマリとバックアップの Flex 7500 コントローラで同じであることが必要です。
- Flex 7500 をプライマリとバックアップのコントローラとして使用することを推奨します。

## 要約

- FlexConnect は、コントローラの設定が変更されない限り、AP が同じコントローラに接続するときにクライアントを切断しません。
- FlexConnect は、設定に変更がなく、バックアップコントローラがプライマリコントローラと同じである限り、バックアップコントローラに接続するときにクライアントを切断しません。
- FlexConnect は、コントローラの設定に変更がない限り、元のプライマリコントローラに接続するときに、その無線をリセットしません。

## 制限

- ローカルスイッチングと、中央またはローカルの認証を使用した FlexConnect のみでサポートされます。
- FlexConnect AP がスタンドアロンモードから接続モードに切り換わる前にクライアントセッションタイマーが切れた場合、中央で認証されるクライアントの完全な再認証が必要です。
- Flex 7500 プライマリおよびバックアップコントローラは、同じモビリティドメインに属している必要があります。

## WLAN ごとのクライアント制限

トラフィックのセグメンテーションに加えて、ワイヤレスサービスにアクセスするクライアントの総数を制限する必要性が生じます。

例：ブランチトンネリングからデータセンターへのゲストクライアントの総数を制限する。

この課題に対処するため、シスコは WLAN ごとのクライアント制限機能を導入しています。この機能を使用すると、許可されるクライアントの総数を WLAN ごとに制限できます。

## 主な目的

- 最大クライアント数に対して制限を設定する
- 運用を容易にする

注：これは QoS の形式ではありません。

この機能はデフォルトでディセーブルになっており、制限は適用されません。

## 制限



FlexConnect がスタンドアロン動作状態の場合には、クライアントの上限が適用されません。

## WLC の設定

次のステップを実行します。

1. SSID が **DataCenter** の、中央でスイッチングされている WLAN ID 1 を選択します。この WLAN は、AP グループの作成時に作成したものです。図 8 を参照してください。
2. WLAN ID 1 の [Advanced] タブをクリックします。
3. [Maximum Allowed Clients] テキスト フィールドにクライアントの上限値を設定します。
4. [Maximum Allowed Clients] のテキスト フィールドに設定した後、[Apply] をクリックします

The screenshot shows the 'WLANs > Edit' configuration page for WLAN ID 1. The 'Advanced' tab is selected. The 'Maximum Allowed Clients' field is highlighted in red and contains the value '0'. Other settings include 'Allow AAA Override' (disabled), 'Coverage Hole Detection' (enabled), 'Enable Session Timeout' (1800 secs), 'Aironet IE' (enabled), 'Diagnostic Channel' (disabled), 'IPv6 Enable' (disabled), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (enabled, 60 secs), 'Off Channel Scanning Defer' (Scan Defer Priority 0-7, Scan Defer Time 100 msec), 'DHCP' (DHCP Server, DHCP Addr. Assignment), 'Management Frame Protection (MFP)' (MFP Client Protection Optional), 'DTIM Period (in beacon intervals)' (802.11a/n 1, 802.11b/g/n 1), 'NAC' (NAC OOB State, Posture State), and 'Load Balancing and Band Select' (Client Load Balancing, Client Band Select). The 'Foot Notes' section at the bottom contains 10 numbered notes, with note 9 highlighted in red: '9 Value zero implies there is no restriction on maximum clients allowed.'

[Maximum Allowed Clients] のデフォルトは 0 に設定されています。これは、制限がなく、機能がデisableになっていることを示します。

## NCS の設定

NCS からこの機能をイネーブルにするには、[Configure] > [Controllers] > [Controller IP] > [WLANs] > [WLAN Configuration] > [WLAN Configuration Details] に移動します。

## WLAN Configuration Details : 17

Configure > Controllers > 172.20.225.154 > WLANs > WLAN Configuration > **WLAN Configuration Details**

General Security QoS **Advanced**

FlexConnect Local Switching	<input type="checkbox"/> Enable	
FlexConnect Local Auth ⓘ	<input type="checkbox"/> Enable	
Learn Client IP Address	<input type="checkbox"/> Enable	
Session Timeout	<input checked="" type="checkbox"/> Enable	1800 (secs)
Coverage Hole Detection	<input checked="" type="checkbox"/> Enable	
Aironet IE	<input checked="" type="checkbox"/> Enable	
IPv6 ↗	<input type="checkbox"/> Enable	
Diagnostic Channel ↗	<input type="checkbox"/> Enable	
Override Interface ACL	IPv4	NONE
	IPv6	NONE
Peer to Peer Blocking ⓘ		Disable
Wi-Fi Direct Clients Policy		Disabled
Client Exclusion ↕	<input checked="" type="checkbox"/> Enable	
Timeout Value		60 (secs)
Maximum Clients ⓘ		0

**DHCP**

DHCP Server  
DHCP Address Assignment

**Management Frame Protection**

MFP Client Protection ↗  
MFP Version

**Load Balancing and Band Sel**

Client Load Balancing  
Client Band Select

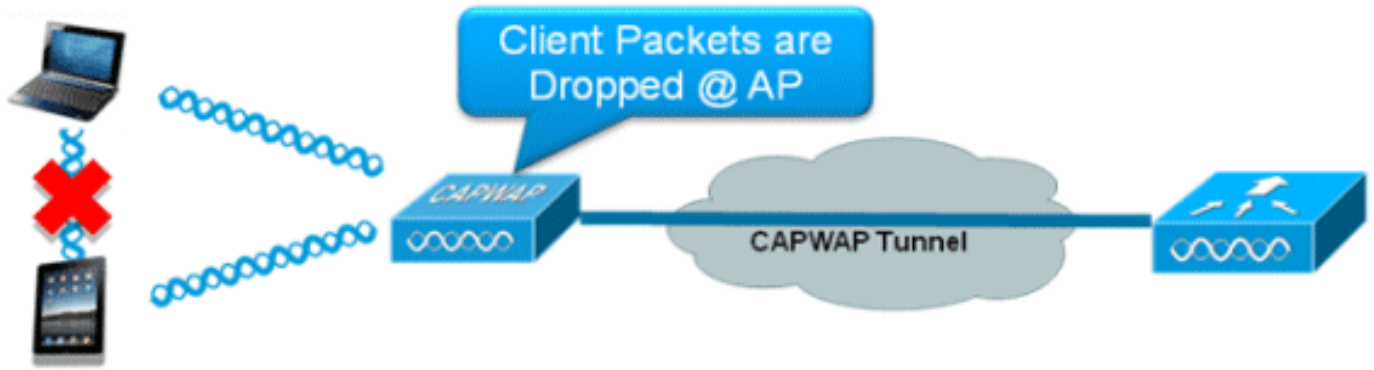
**NAC**

## ピアツーピア ブロッキング

7.2 よりも前のコントローラ ソフトウェア リリースでは、ピアツーピア ( P2P ) ブロッキングは中央でスイッチングされる WLAN に対してのみサポートされていました。ピアツーピア ブロッキングでは、WLAN に対して次の 3 つのいずれかの動作を設定できます。

- [Disabled] : ピアツーピア ブロッキングをディセーブルにし、同じサブネット内のクライアント宛のトラフィックをコントローラ内でローカルにブリッジします。これがデフォルト値です。
- [Drop] : コントローラは同じサブネット内のクライアント宛のパケットをドロップします。
- [Forward Up-Stream] : パケットはアップストリーム VLAN に転送されます。コントローラ上のデバイスは、パケットに関して実行すべきアクションを決定します。

リリース 7.2 より、ピアツーピア ブロッキングは、ローカル スイッチング WLAN にアソシエーションされたクライアントに対してサポートされています。WLAN ごとのピアツーピア設定は、コントローラによって FlexConnect AP にプッシュされます。



## 要約

- ピアツーピア ブロッキングは、WLAN ごとに設定します。
- WLAN ごとのピアツーピア ブロッキングの設定は、WLC によって FlexConnect AP にプッシュされます。
- WLAN 上でドロップまたはアップストリーム転送として設定されたピアツーピア ブロッキング アクションは、FlexConnect AP でイネーブルにされたピアツーピア ブロッキングとして扱われます。

## 手順

次のステップを実行します。

1. FlexConnect ローカル スイッチングが設定された WLAN 上で、ピアツーピア ブロッキング アクションを [Drop] としてイネーブルにします。

2. ローカル スイッチングが設定された WLAN で P2P ブロッキング アクションを [Drop] または [Forward-Upstream] として設定すると、WLC から FlexConnect AP にプッシュされます。FlexConnect AP はこの情報をフラッシュ内の REAP コンフィギュレーション ファイルに保存します。これにより、FlexConnect AP がスタンドアロン モードの場合でも、P2P 設定を対応するサブインターフェイスに適用できます。



## 制限

- FlexConnect では、ソリューション P2P ブロッキング設定を特定の FlexConnect AP または AP のサブセットのみに適用できません。SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチング クライアントのための統一ソリューションは、P2P アップストリーム転送をサポートしています。ただし、これは FlexConnect ソリューションでサポートされません。これは、P2P ドロップとして扱われ、クライアント パケットは、次のネットワーク ノードに転送されずにドロップされます。
- 中央スイッチング クライアント用の統一ソリューションは、異なる AP にアソシエーションされたクライアントに対する P2P ブロッキングをサポートしています。ただし、このソリューションは、同じ AP に接続されたクライアントのみを対象としています。FlexConnect ACL は、この制限の回避策として使用できます。

## AP 事前イメージのダウンロード

この機能を使用すると、AP は動作中にコードをダウンロードできます。AP 事前イメージのダウンロードは、ソフトウェアのメンテナンスやアップグレードの際のネットワークのダウンタイムを削減するうえできわめて有効です。

### 要約

- ソフトウェア管理の容易化
- 店舗アップグレードごとのスケジュール実現には NCS が必要
- ダウンタイムの削減

### 手順

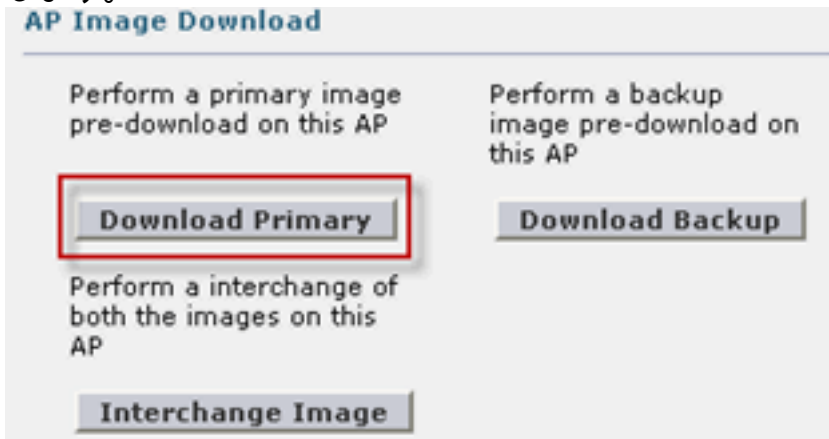
次のステップを実行します。

1. プライマリおよびバックアップ コントローラでイメージをアップグレードします。[WLC GUI] > [Commands] > [Download File] に移動し、ダウンロードを開始します。

Download file to Controller	
File Type	Code
Transfer Mode	TFTP
Server Details	
IP Address	[Redacted]
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_0_112_52.aes

2. コントローラに設定を保存しますが、コントローラをリポートしないでください。
3. プライマリ コントローラから AP 事前イメージ ダウンロード コマンドを実行します。[WLC GUI] > [Wireless] > [Access Points] > [All APs] に移動し、事前イメージのダウンロードを開始するアクセス ポイントを選択します。アクセス ポイントを選択したら、[Advanced] タブをクリックします。[Download Primary] をクリックして事前イメージのダウンロードを開始

します。



```
*Sep 13 21:21:14.903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [REDACTED] not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
  Version Suffix: k9w8-.wnbu_j_mr.201009101910
  Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Ios Image Size: 5530112
  Total Image Size: 5550592
  Image Feature: WIRELESS LAN|LWAPP
  Image Family: C1250
  Wireless Switch Management Version: [REDACTED]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre [REDACTED]..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.█
```

- すべての AP イメージをダウンロードした後、コントローラをリブートします。コントローラがリブートするまで、AP はスタンドアロン モードにフォールバックします。注：スタンドアロンモードでは、耐障害性によってクライアントが関連付けられたままになります。コントローラが起動すると、AP は事前にダウンロードされたイメージで自動的にリブートします。リブート後、AP はプライマリ コントローラに接続し、クライアントのサービスを再開します。



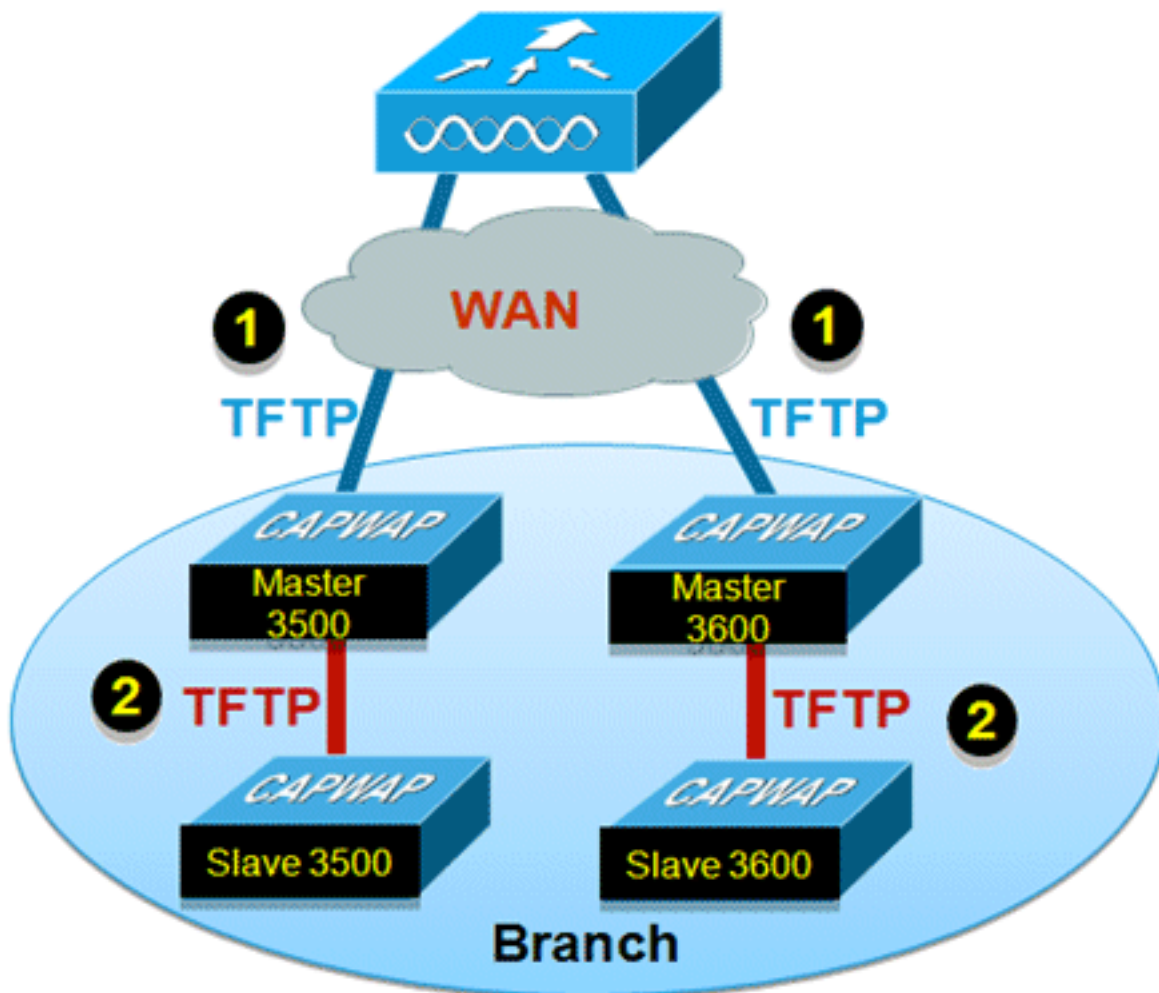
## 制限

- CAPWAP AP のみで動作します。

## FlexConnect スマート AP イメージ アップグレード

事前のイメージダウンロード機能により、ダウンタイムがある程度短縮されますが、すべての FlexConnect AP が、それぞれの AP イメージを、WAN リンクを介し高い遅延で事前にダウンロードする必要があります。

Efficient AP Image Upgrade は、各 FlexConnect AP のダウンタイムを短縮します。基本的な考え方は、AP モデルごとに 1 台の AP のみがコントローラからイメージをダウンロードし、マスターまたはサーバとして振る舞い、同じモデルの残りの AP はスレーブまたはクライアントとして動作し、マスターから AP イメージを事前にダウンロードします。サーバからクライアントへの AP イメージの配布はローカル ネットワーク上で行われ、WAN リンクのような遅延が発生しません。その結果、処理が高速になります。



## 要約

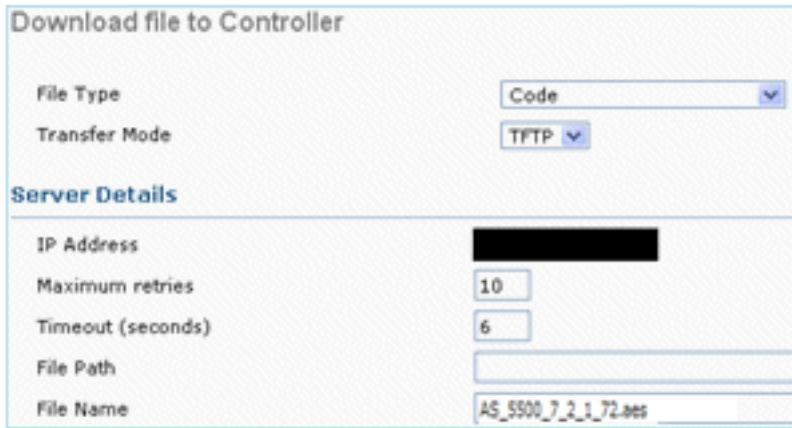
- マスターとスレーブの AP を、FlexConnect グループごとに各 AP モデルに対して選択します。
- マスターが WLC からイメージをダウンロードします。
- スレーブがマスター AP からイメージをダウンロードします。

- ・ダウンタイムを削減し WAN の帯域幅を節約します。

## 手順

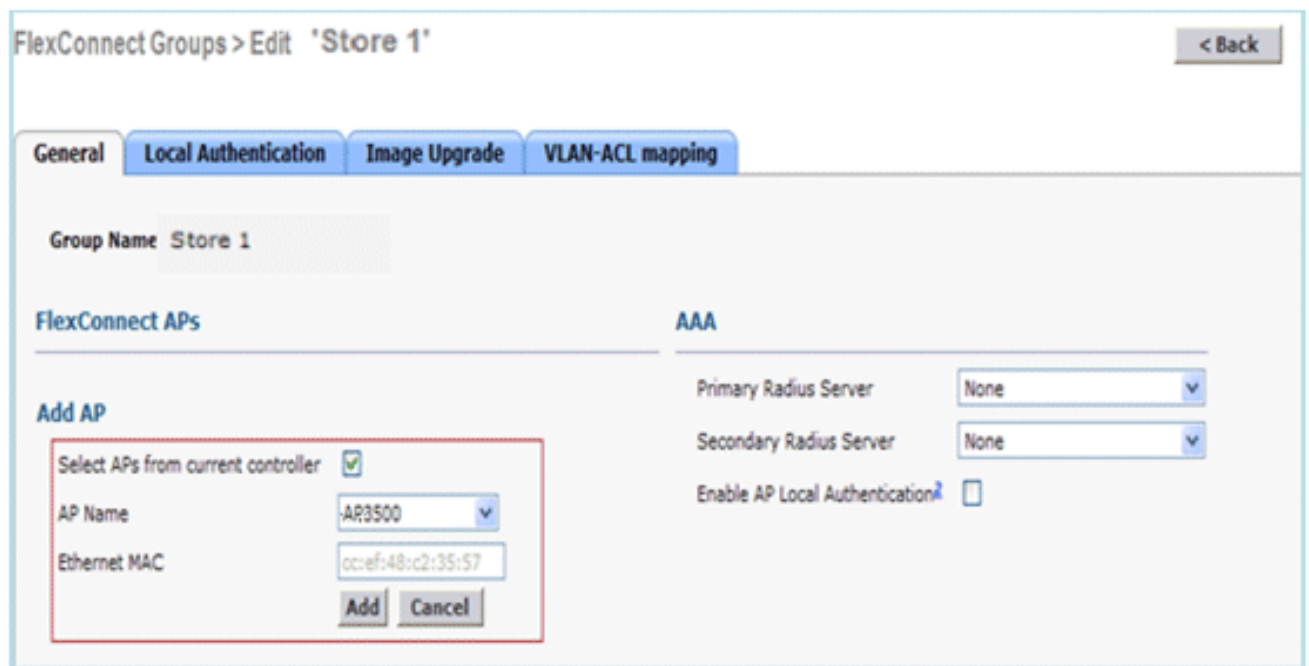
次のステップを実行します。

1. コントローラでイメージをアップグレードします。ダウンロードを開始するため、[WLC GUI] > [Commands] > [Download File] に移動します。



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

2. コントローラに設定を保存しますが、コントローラをリブートしないでください。
3. FlexConnect AP を FlexConnect グループに追加します。[WLC GUI] > [Wireless] > [FlexConnect Groups] > FlexConnect グループを選択 > [General] タブ > [Add AP] に移動します。



FlexConnect Groups > Edit 'Store 1'	
General   Local Authentication   Image Upgrade   VLAN-ACL mapping	
Group Name Store 1	
FlexConnect APs	
Add AP	
Select APs from current controller	<input checked="" type="checkbox"/>
AP Name	AR3500
Ethernet MAC	cc:ef:48:c2:35:57
Add Cancel	
AAA	
Primary Radius Server	None
Secondary Radius Server	None
Enable AP Local Authentication	<input type="checkbox"/>

4. 効率的な AP イメージのアップグレードを実現するには、[FlexConnect AP Upgrade] チェックボックスをオンにします。[WLC GUI] > [Wireless] > [FlexConnect Groups] > FlexConnect グループを選択 > [Image Upgrade] タブに移動します。

FlexConnect Groups > 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

FlexConnect AP Upgrade

**FlexConnect Master APs**

AP Name AP3500

Add Master

Master AP Name	AP Model	Manual

5. マスター AP は手動または自動で選択できます。マスター AP を手動で選択するには、[WLC GUI] > [Wireless] > [FlexConnect Groups] > [FlexConnect Group] > [Image Upgrade] タブ > [FlexConnect Master APs] に移動し、ドロップダウン リストから AP を選択し、[Add Master] をクリックします。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

FlexConnect AP Upgrade

Slave Maximum Retry Count 44

Upgrade Image Backup FlexConnect Upgrade

**FlexConnect Master APs**

AP Name AP3500

Add Master

Master AP Name	AP Model	Manual
AP3500	c3500I	yes

注：マスター AP として設定できるのは、モデルごとに1つの AP だけです。マスター AP を手動で設定した場合、[Manual] フィールドが [yes] になります。マスター AP を自動で選択するには、[WLC GUI] > [Wireless] > [FlexConnect Groups] > [FlexConnect Group] > [Image Upgrade] タブを選択し、[FlexConnect Upgrade] をクリックします。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

注：[マスタAP]が自動的に選択されている場合、[Manual]フィールドは[no]に更新されます。

6. 特定の FlexConnect グループに属するすべての AP について効率的な AP イメージのアップグレードを開始するには、[FlexConnect Upgrade] をクリックします。[WLC GUI] > [Wireless] > [FlexConnect Groups] > FlexConnect グループを選択 > [Image Upgrade] タブに移動し、[FlexConnect Upgrade] をクリックします。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

注：Slave Maximum Retry Countは、マスターAPからイメージをダウンロードするためにスレーブAPが実行する試行回数（デフォルトでは44）です。この試行回数を超えると、スレーブAPはWLCからイメージをダウンロードします。新しいイメージをダウンロードするために WLC に対して 20 回試行します。20 回を超えた場合、管理者はダウンロードプロセスを再度開始する必要があります。

7. FlexConnect アップグレードを開始すると、マスター AP のみが WLC からイメージをダウンロードします。[All AP] ページで、[Upgrade Role] は [Master/Central] として更新されます。これは、マスター AP が中央にある WLC からイメージをダウンロードしたことを意味します。スレーブ AP はローカル サイトにあるマスター AP からイメージをダウンロードします。[All AP] ページの [Upgrade Role] が [Slave/Local] に更新されるのはこのためです。これを確認するには、[WLC GUI] > [Wireless] に移動します。



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

8. すべての AP イメージをダウンロードした後、コントローラをリブートします。コントローラがリブートするまで、AP はスタンダオン モードにフォールバックします。注：スタンダオンモードでは、耐障害性によってクライアントが関連付けられたままになります。コントローラが起動すると、AP は事前にダウンロードされたイメージで自動的にリブートします。リブート後、AP はプライマリ コントローラに接続し、クライアントのサービスを再開します。

## 制限

- マスター AP の選択は、FlexConnect グループごと、各グループの AP モデルごとに行われます。
- 同じモデルの 3 台のスレーブ AP のみとそのマスター AP から同時にアップグレードでき、残りのスレーブ AP は、AP イメージをダウンロードするためにランダムなバックオフ タイマーを使用してマスター AP に再試行します。
- スレーブ AP が何らかの理由でマスター AP からイメージをダウンロードできない場合、WLC から新しいイメージを取得します。
- この機能は、CAPWAP AP のみで動作します。

## FlexConnect モードでの自動変換 AP

Flex 7500 には、AP モードを FlexConnect に変換するための次の 2 つのオプションがあります。

- 手動モード
- 自動変換モード

### 手動モード

このモードは、すべてのプラットフォームで使用でき、AP ごとにのみ変更を行うことができます。

1. [WLC GUI] > [Wireless] > [All APs] に移動し、AP を選択します。
2. [AP Mode] で [FlexConnect] を選択し、[Apply] をクリックします。
3. AP モードを変更すると AP がリブートします。

## All APs > Details for AP3500

General	Credentials	Interfaces	High Availability
<b>General</b>			
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 FlexConnect monitor Rogue Detector Sniffer Bridge SE-Connect		
Operational Status			
Port Number			
Venue Group	▾		

このオプションは、現在のすべての WLC プラットフォームでも使用できます。

### 自動変換モード

このモードは Flex 7500 コントローラのみで使用でき、CLI の使用のみがサポートされています。このモードでは、接続されているすべての AP で変更が起動されます。この CLI をイネーブルにする前に、既存の WLC キャンパス コントローラとは異なるモビリティドメインに Flex 7500 を導入することを推奨します。

```
(Cisco Controller) >config ap autoconvert ?
```

```
disable          Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect      Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins
```

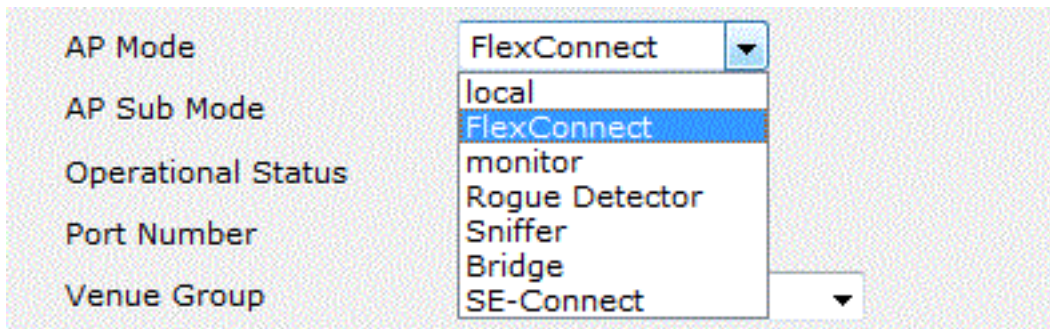
```
(Cisco Controller) >
```

1. 自動変換機能はデフォルトでディセーブルになっており、次の show コマンドで確認できません。

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

```
AP Autoconvert ..... Disabled
```

サポートされない AP モードは、Local Mode、Sniffer、Rogue Detector、および Bridge で



す。このオプションは、現在 CLI のみで使用できます。これらの CLI は、WLC 7500 のみで使用できます。

2. `config ap autoconvert flexconnect` CLI を実行すると、ネットワーク内のサポートされない AP モードのすべての AP が FlexConnect モードに変換されます。すでに FlexConnect または Monitor モードになっている AP は影響を受けません。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

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

```
AP Autoconvert ..... FlexConnect
```

```
(Cisco Controller) >
```

3. `config ap autoconvert monitor` CLI を実行すると、ネットワーク内のサポートされない AP モードのすべての AP が Monitor モードに変換されます。すでに FlexConnect または Monitor モードになっている AP は影響を受けません。

```
(Cisco Controller) >config ap autoconvert monitor
```

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

```
AP Autoconvert ..... Monitor
```

`config ap autoconvert flexconnect` と `config ap autoconvert monitor` を同時に実行するオプションはありません。

## ローカル スイッチング WLAN のための FlexConnect WGB/uWGB サポート

リリース 7.3 から、WGB/uWGB および WGB の背後にある有線またはワイヤレス クライアントがサポートされ、ローカル スイッチングが設定された WLAN 上の通常のクライアントとして動作します。

アソシエーションの後、WGB はその各有線またはワイヤレス クライアントについて IAPP メッセージを送信し、Flex AP は次のように振る舞います。

- Flex AP が接続モードの場合、すべての IAPP メッセージをコントローラに転送し、コントローラはローカル モード AP と同様に IAPP メッセージを処理します。有線またはワイヤレス クライアント宛のトラフィックは、Flex AP からローカルにスイッチングされます。
- AP がスタンドアロン モードの場合、AP が IAPP メッセージを処理し、WGB 上の有線またはワイヤレス クライアントは登録と登録解除を行うことができます必要があります。Flex AP は、接続モードに遷移するとき、有線クライアントの情報をコントローラに送信します。Flex AP がスタンドアロン モードから接続モードに遷移するとき、WGB は登録メッセージを 3 回送信します。

有線またはワイヤレス クライアントは WGB の設定を引き継ぎます。つまり、AAA 認証、AAA

オーバーライド、FlexConnect ACL などの個別の設定は、WGB の背後にあるクライアントについては不要です。



## 要約

- Flex AP 上で WGB をサポートするために、WLC 上で特別な設定は不要です。
- Fault Tolerance は、WGB および WGB の背後にあるクライアントに対してサポートされています。
- WGB がサポートされている IOS AP は、1240、1130、1140、1260、1250 です。

## 手順

次のステップを実行します。

1. WGB としてローカル スイッチングが設定された WLAN について、FlexConnect AP 上で WGB または uWGB のサポートをイネーブルにするために、特別な設定は不要です。また、WGB の背後にあるクライアントは、Flex AP により、ローカル スイッチングが設定された WLAN 上の通常のクライアントとして扱われます。WLAN で [FlexConnect Local Switching] をイネーブルにします。



## 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  IPv6

P2P Blocking Action

Client Exclusion  Enabled   
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling  Enabled

Wi-Fi Direct Clients Policy

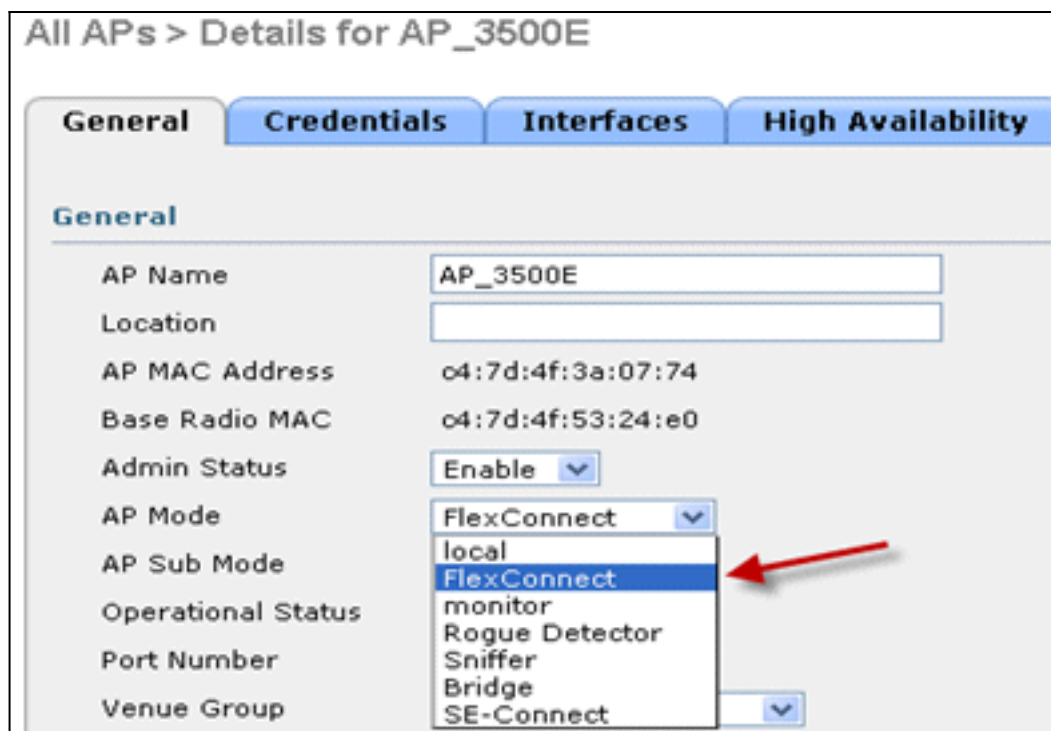
Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration  Enabled

### FlexConnect

FlexConnect Local Switching  Enabled

2. [AP Mode] を [FlexConnect] に設定します。



3. WGB を、この設定された WLAN の背後にある有線クライアントにアソシエーションします

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
<a href="#">00:40:96:b8:d4:be</a>	AP_3500E	"Store 1"	"Store 1"	N/A	Associated	Yes	1	No
<a href="#">00:50:b6:09:e5:3b</a>	AP_3500E	"Store 1"	"Store 1"	N/A	Associated	Yes	1	No
<a href="#">04:7d:4f:3a:08:10</a>	AP_3500E	"Store 1"	"Store 1"	802.11an	Associated	Yes	1	Yes

4. WGB の詳細を確認するには、[Monitor] > [Clients] に移動し、クライアントのリストから [WGB] を選択します。

Clients > Detail

Client Properties		AP Properties	
MAC Address	04:7d:4f:3a:08:10	AP Address	04:7d: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 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB		
Number of Wired Client(s)	2		

5. WGB の背後にある有線またはワイヤレス クライアントの詳細を確認するには、[Monitor] > [Clients] に移動し、クライアントを選択します。

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	04:7d: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
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB Client		
WGB MAC Address	04:7d:4f:3a:08:10		

## 制限

- WGB の背後にある有線クライアントは、常に WGN 自体と同じ VLAN にあります。WGB の背後にあるクライアントに対する複数 VLAN のサポートは、ローカル スイッチングが設定された WLAN について、Flex AP 上でサポートされていません。
- ローカル スイッチングが設定された WLAN 上の Flex AP にアソシエーションされている場合、WGB の背後では、最大 20 台のクライアント (有線またはワイヤレス) がサポートされています。この数は、現在のローカル モード AP での WGB のサポートと同じです。
- ローカル スイッチングが設定された WLAN にアソシエーションされている WGB の背後にあ

るクライアントについては、Web Auth はサポートされません。

## Radiusサーバ数の増加のサポート

リリース7.4より前では、FlexConnectグループでのRADIUSサーバの設定は、コントローラ上のRADIUSサーバのグローバルリストから行われました。このグローバルリストで設定できるRADIUSサーバの最大数は17です。ブランチオフィスが増えるにつれて、ブランチサイトごとにRADIUSサーバを設定することが必要になります。リリース7.4以降では、FlexConnectグループごとにプライマリおよびバックアップRADIUSサーバを設定できます。コントローラで設定された17台のRADIUS認証サーバのグローバルリストに含まれる場合とそうでない場合があります。

RADIUSサーバのAP固有の設定もサポートされます。AP固有の設定は、FlexConnectグループ設定よりも優先度が高くなります。

コントローラのグローバルRADIUSサーバリストにRADIUSサーバのインデックスが必要なFlexConnectグループの既存の設定コマンドは廃止され、サーバのIPアドレスと共有秘密を使用してFlexconnectグループのRADIUSサーバを設定する設定コマンドに置き置ききき換えます。

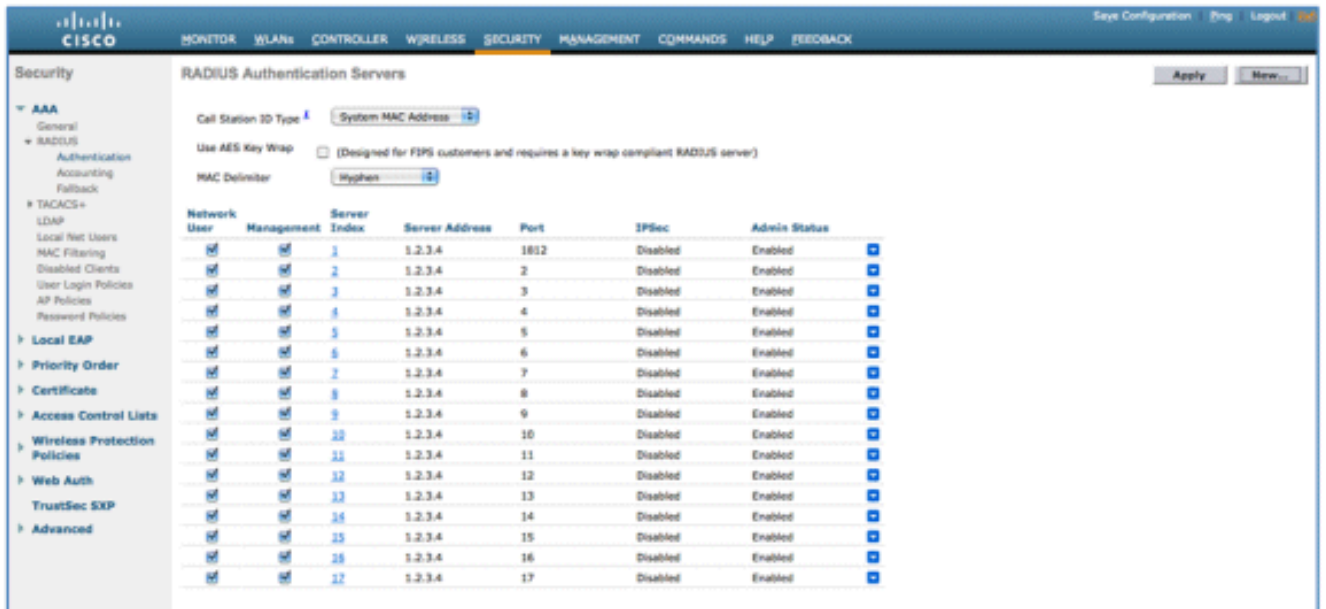
### 要約

- FlexConnectグループごとのプライマリおよびバックアップRADIUSサーバの設定のサポート。RADIUS認証サーバのグローバルリストに含まれる場合と含まれない場合があります。
- WLCに追加できる一意のRADIUSサーバの最大数は、特定のプラットフォームで設定できるFlexConnectグループの数を2倍にします。たとえば、FlexConnectグループごとに1つのプライマリRADIUSサーバと1つのセカンダリRADIUSサーバがあります。
- 以前のリリースからリリース7.4へのソフトウェアアップグレードでは、RADIUS設定が失われることはありません。
- プライマリRADIUSサーバの削除は、セカンダリRADIUSサーバを削除しなくても許可されます。これは、RADIUSサーバの現在のFlexConnectグループ設定と一致します。

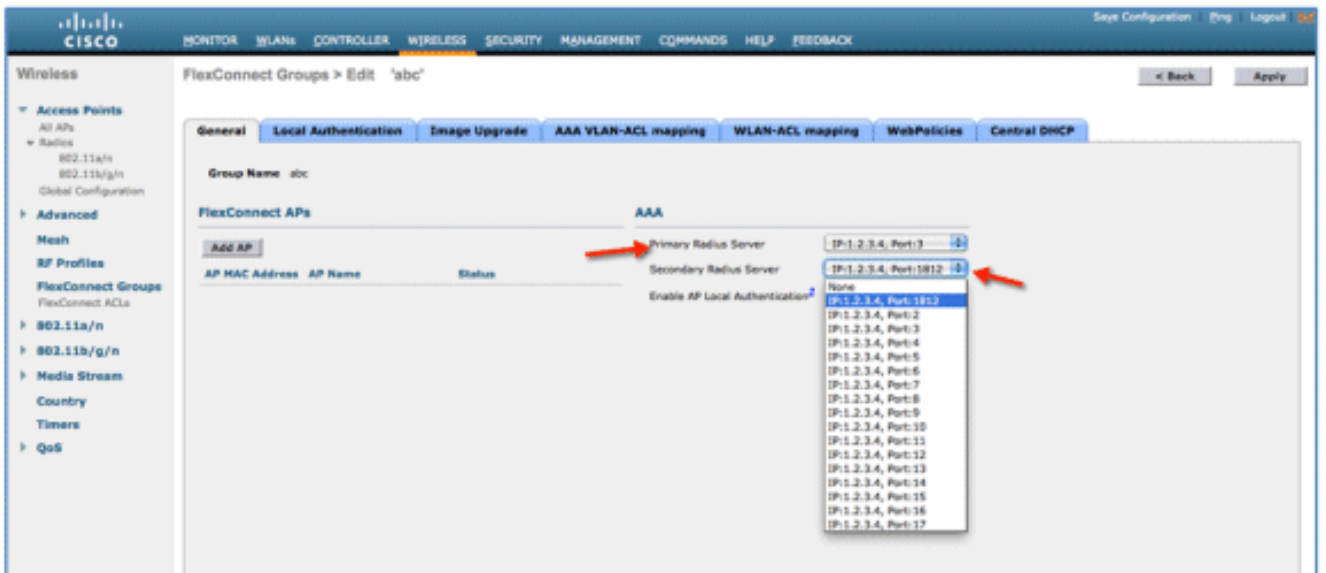
### 手順

1. リリース7.4より前の設定モード。AAA認証設定では、最大17台のRADIUSサーバを設定できます。

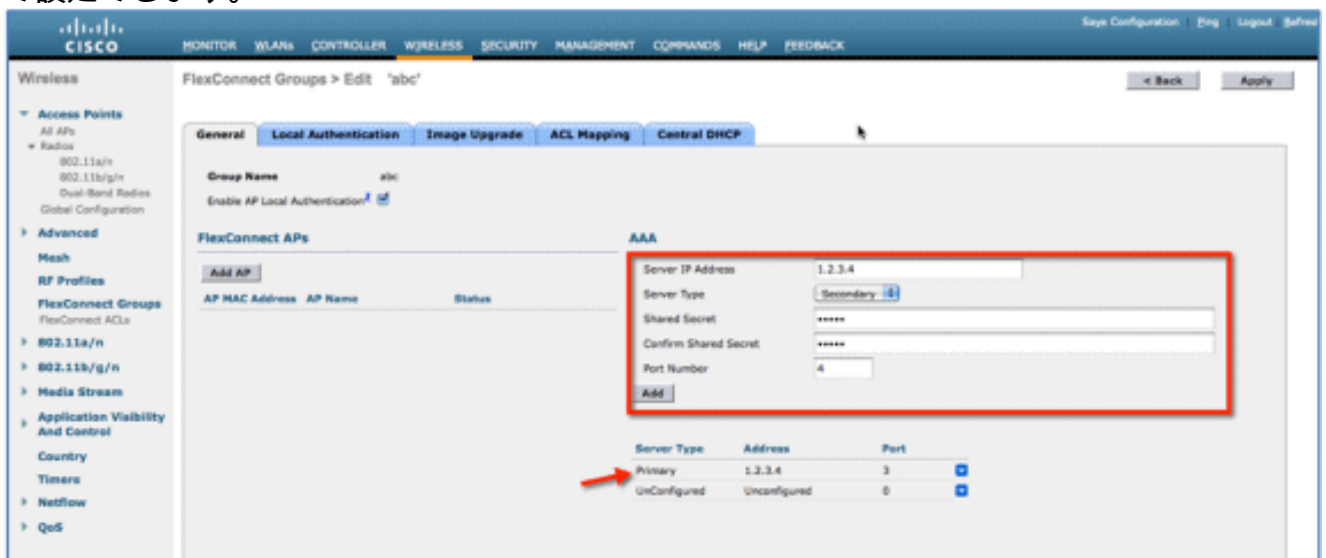




2. プライマリおよびセカンダリRADIUSサーバは、[AAA Authentication]ページで設定されたRADIUSサーバで構成されるドロップダウンリストを使用して、FlexConnectグループに関連付けることができます。



3. リリース7.4のFlexConnectグループの設定モード。プライマリおよびセカンダリRADIUSサーバは、IPアドレス、ポート番号、および共有秘密を使用して、FlexConnectグループの下で設定できます。



## 制限

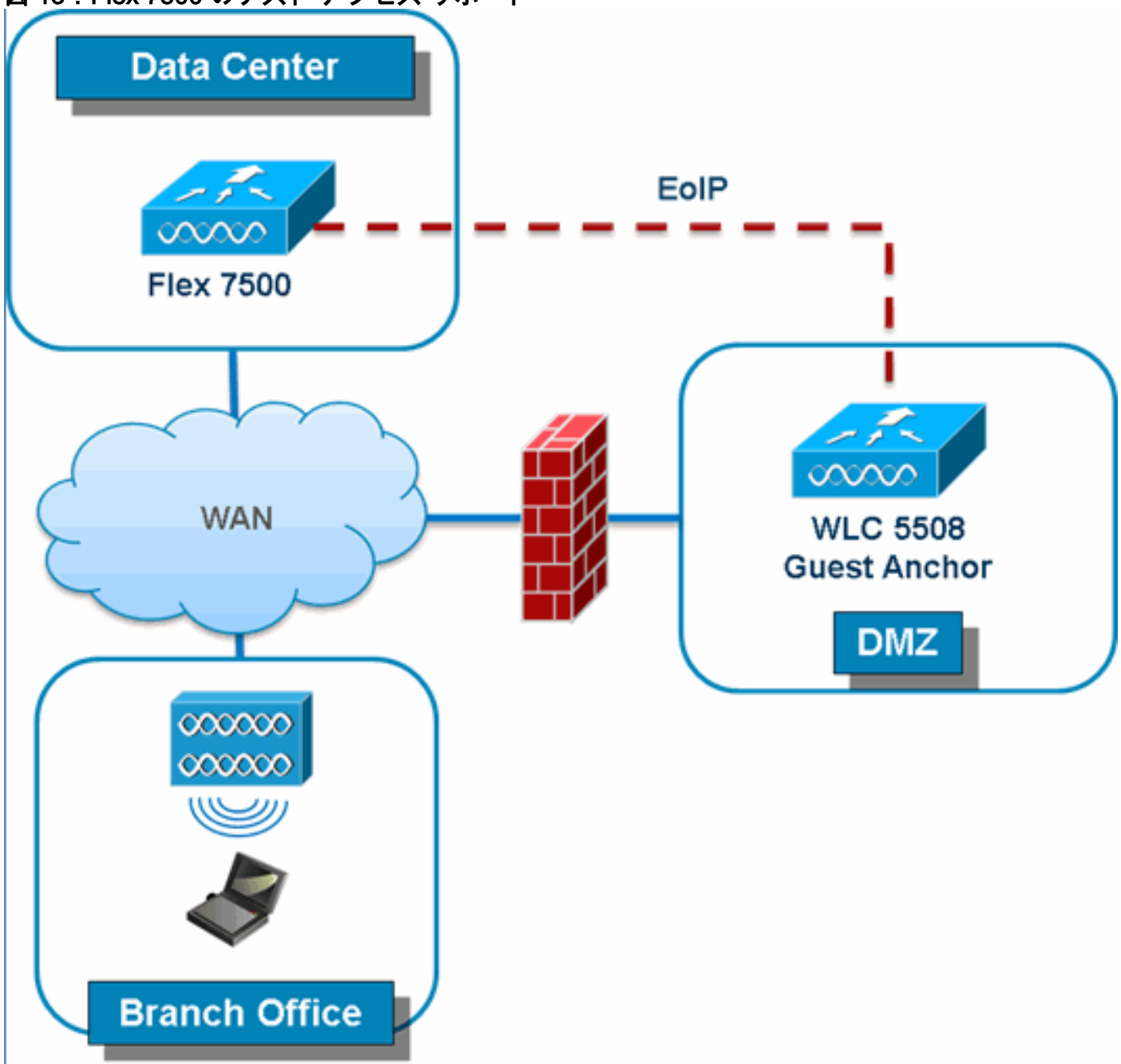
- リリース7.4から以前のリリースへのソフトウェアダウングレードでは、設定は保持されますが、いくつかの制限があります。
- 以前のRADIUSサーバを設定すると、古いエントリが新しいエントリに置き換えられます。

## 拡張ローカル モード ( ELM )

FlexConnect ソリューションでは ELM がサポートされています。詳細については、ELM に関するベスト プラクティス ガイドを参照してください。

## Flex 7500 のゲスト アクセス サポート

図 13 : Flex 7500 のゲスト アクセス サポート



Flex 7500 では、DMZ にあるゲスト アンカー コントローラへの EoIP トンネルを使用でき、その

作成が引き続きサポートされています。ワイヤレスゲストアクセスソリューションのベストプラクティスについては、『ゲスト導入ガイド』を参照してください。

## NCS からの WLC 7500 の管理

NCS からの WLC 7500 の管理は、シスコの既存の WLC と同じです。

Monitor ▾ Reports ▾ Configure ▾ Services ▾

### Add Controllers

Configure > Controllers > Add Controllers

#### General Parameters

Add Format Type: Device Info ▾

IP Addresses: **WLC 7500 IP Address**

Network Mask: 255.255.255.0

Verify Telnet/SSH Capabilities ⓘ

#### SNMP Parameters ⓘ

Version: v2c ▾

Retries: 2

Timeout: 10 (secs)

Community: private

#### Telnet/SSH Parameters ⓘ

User Name: admin

Password: ●●●●●●

Confirm Password: ●●●●●●

Retries: 3

Timeout: 60 (secs)

OK Cancel

Controllers

Configure > Controllers

-- Select a command --

<input type="checkbox"/>	IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
<input type="checkbox"/>	172.20.227.174 ⓘ	Ambassador	7500		7.0.112.62	mobility	Reachable	Identical
<input type="checkbox"/>	172.20.227.177 ⓘ	5508-Primary	5500		7.0.112.52	mobility	Reachable	Identical

WLC の管理とテンプレートの検出の詳細については、『[Cisco Wireless Control System コンフィギュレーションガイド、リリース 7.0.172.0](#)』を参照してください。

## FAQ

Q. FlexConnect のようにリモートの場所に LAP を設定する場合、その LAP にプライマリ コントローラやセカンダリ コントローラを提供できますか。

例：サイトAにプライマリコントローラがあり、サイトBにセカンダリコントローラがあります。サイトAのコントローラに障害が発生すると、LAPはサイトBのコントローラにフェールオーバーします。両方のコントローラが使用できない場合、LAPはFlexConnectスタンドアロンモードになりますか。

A.はい。まず、LAPは、そのセカンダリにフェールオーバーします。ローカルでスイッチングされるすべてのWLANに変更はなく、中央でスイッチングされるすべてのWLANはトラフィックを新しいコントローラに送信します。また、セカンダリに障害が発生した場合、ローカルスイッチング用とマークされたすべてのWLAN（およびオープン/事前共有鍵認証/ユーザがAPオーセンティケータである）はアップ状態のままです。

Q. ローカルモードで設定されているアクセスポイントは、FlexConnect ローカルスイッチングで設定されたWLANをどのように扱うのですか。

A.ローカルモードアクセスポイントはこれらのWLANを通常のWLANとして扱います。認証とデータトラフィックはWLCにトンネリングして戻されます。WANリンクの障害が発生しているとき、このWLANは完全にダウンしており、WLCへの接続が回復するまでこのWLANのクライアントはアクティブになりません。

Q. ローカルスイッチングでWeb認証を実行できますか。

A.はい。Web認証が有効なSSIDを持ち、Web認証後にローカルでトラフィックをドロップできます。ローカルスイッチングを伴うWeb認証は問題なく動作します。

Q. HREAPによってローカルで処理されるSSID用にコントローラで自分のゲストポータルを使用できますか。使用できる場合、コントローラへの接続が失われたときにはどうなりますか。現在のクライアントは即座にドロップしますか。

A.はい。このWLANはローカルでスイッチングされるため、WLANは利用可能ですが、Webページは利用可能ではないため新しいクライアントは認証できません。しかし、既存のクライアントはドロップされません。

Q. FlexConnectはPCIコンプライアンスを保証できますか。

A.はい。FlexConnectソリューションは、PCIコンプライアンスを満たすために不正検出をサポートしています。

## [関連情報](#)

- [HREAP の設計および導入ガイド](#)
- [Cisco 4400 シリーズ ワイヤレス LAN コントローラ](#)
- [Cisco 2000 シリーズ ワイヤレス LAN コントローラ](#)
- [Cisco Wireless Control System](#)
- [Cisco 3300 シリーズ モビリティ サービス エンジン](#)
- [Cisco Aironet 3500 シリーズ](#)
- [Cisco Secure Access Control System](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)