



# Flex 7500 Wireless Branch Controller Deployment Guide

Last Updated: 04/28/2015

## Introduction

This document describes how to deploy a Cisco Flex 7500 wireless branch controller. The purpose of this document is to:

- Explain various network elements of the Cisco FlexConnect solution, along with their communication flow.
- Provide general deployment guidelines for designing the Cisco FlexConnect wireless branch solution.

**Note:** Prior to release 7.2, FlexConnect was called Hybrid REAP (HREAP). Now it is called FlexConnect.

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

This document is not restricted to specific software and hardware versions.

## Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Product Overview

**Figure 1** Cisco Flex 7500



The Cisco Flex 7500 Series Cloud Controller is a highly scalable branch controller for multi-site [wireless](#) deployments. Deployed in the private cloud, the Cisco Flex 7500 series controller extends wireless services to distributed branch offices with centralized control that lowers total cost of operations.

## Product Specifications

The Cisco Flex 7500 series (Figure 1 on page 1) can manage wireless access points in up to 2000 branch locations and allows IT managers to configure, manage, and troubleshoot up to 6000 access points (APs) and 64,000 clients from the data center. The Cisco Flex 7500 series controller supports secure guest access, rogue detection for Payment Card Industry (PCI) compliance, and in-branch (locally switched) Wi-Fi voice and video.

The following table highlights the scalability differences between the Flex 7500, 8500, WiSM2 and WLC 5500 controller:

Scalability	Flex 7500/8500	WiSM2	WLC 5500
Total Access Points	6,000	1000	500
Total Clients	64,000	15,000	7,000
Max FlexConnect Groups	2000	100	100
Max APs per FlexConnect Group	100	25	25
Max AP Groups	6000	1000	500

**Note:** Flex 7500 only operates in FlexConnect mode. Additional modes are supported in WiSM2, 5500, and 8500 series controllers.

**Note:** DTLS license is required for Office Extend AP support.

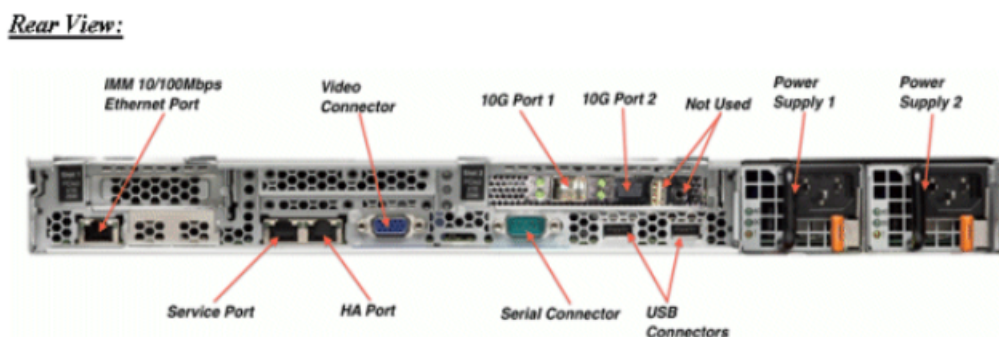
## Product Specifications

## Data Sheet

Refer to Cisco Flex 7500 Series Cloud Controller Data Sheet:  
[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)

## Platform Feature

**Figure 2 Flex 7500 Rear View**



## Network Interface Ports

Interface Ports	Usage
Fast Ethernet	Integrated Management Module (IMM)
Port 1: 1G	WLC Service Port
Port 2: 1G	WLC Redundant Port (RP)
Port 1: 10G	WLC Management Interface
Port 2: 10G	WLC Backup Management Interface Port (Port Failure)

**Note:** LAG support for 2x10G interfaces allows active-active link operation with fast failover link redundancy. An additional active 10G link with LAG does not change the controller wireless throughput.

- 2x10G interfaces.
- 2x10G interfaces support optic cable with SFP product # SFP-10G-SR and SFP-10G-LR.
- Switch side SFP or X2 product should be of the same type SR or LR.

## System MAC Addresses

Port 1: 10G (Management Interface)	System/Base MAC address
Port 2: 10G (Backup Management Interface)	Base MAC address+5
Port 1: 1G (Service Port)	Base MAC address+1
Port 2: 1G (Redundant Port)	Base MAC address+3

## Serial Console Redirect

The WLC 7500 enables console redirect by default at the baud rate of 9600, simulating Vt100 terminal with no flow control.

## Inventory Information

**The following is the WLC 7500 Console:**

(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

The Desktop Management Interface (DMI) table contains server hardware and BIOS information. The WLC 7500 displays BIOS version, PID/VID and Serial Number as part of inventory.

**Note:** Flex 7500 is currently shipped with VID=V02.

## Flex 7500 Boot Up

Cisco boot loader options for software maintenance are identical to Cisco's existing controller platforms.

**Figure 3** Boot-Up Order

```
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
```

950444



**Figure 4 WLC Configuration Wizard**

```

Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:d8:6c] (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
    
```

**Note:** The Flex 7500 boot up sequence is equivalent and consistent with existing controller platforms. Initial boot up requires WLC configuration using the Wizard.

## Flex 7500 Licensing

### AP Base Count Licensing

AP Base Count SKUs
300
500
1000
2000
3000
6000

## AP Upgrade Licensing

AP Upgrade SKUs
100
250
500
1000

Except for the base and upgrade counts, the entire licensing procedure that covers ordering, installation, and viewing is similar to Cisco's existing WLC 5508.

Refer to the [WLC 7.3 configuration guide](#), which covers the entire licensing procedure.

## Software Release Support

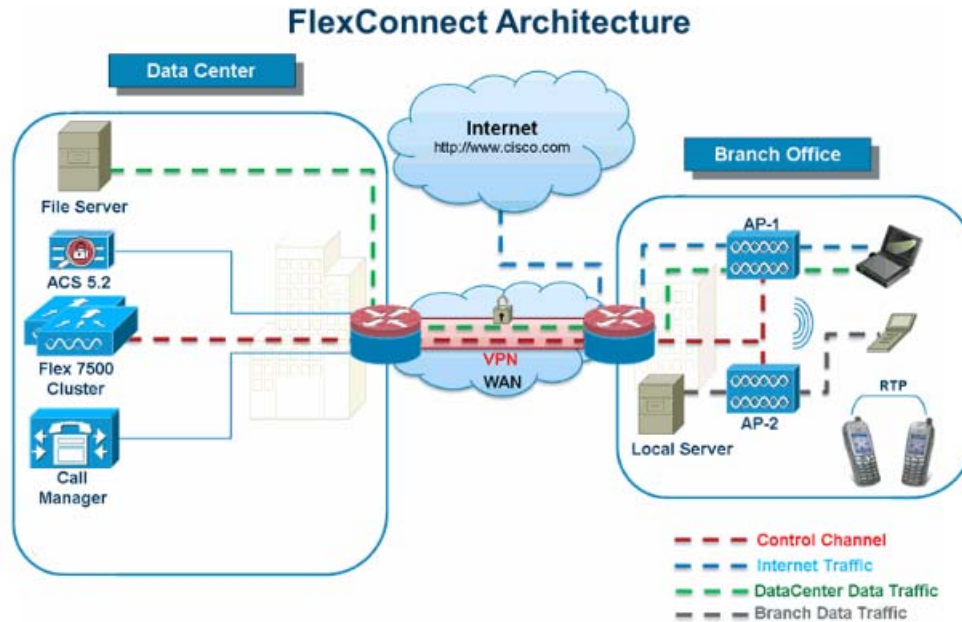
The Flex 7500 supports WLC code version 7.0.116.x and later only.

## Supported Access Points

Access Points 3600, 3500, 2600, 1600, 1550, 1260, 1240, 1140, 1130, 1040, 700, and 600 series, Cisco 891 Series Integrated Services Router and Cisco 881 Series Integrated Services Router.

## FlexConnect Architecture

**Figure 5 Typical Wireless Branch Topology**



350446

FlexConnect is a wireless solution for branch office and remote office deployments.

The FlexConnect solution enables the customer to:

- Centralize control and manage traffic of APs from the Data Center.
  - Control traffic is marked by red dashes in [Figure 5 on page 7](#).
- Distribute the client data traffic at each Branch Office.
  - Data traffic is marked by blue, green, and purple dashes in [Figure 5 on page 7](#).
  - Each traffic flow is going to its final destination in the most efficient manner.

### Advantages of Centralizing Access Point Control Traffic

- Single pane of monitoring and troubleshooting.
- Ease of management.
- Secured and seamless mobile access to Data Center resources.
- Reduction in branch footprint.
- Increase in operational savings.

## Advantages of Distributing Client Data Traffic

- No operational downtime (survivability) against complete WAN link failures or controller unavailability.
- Mobility resiliency within branch during WAN link failures.
- Increase in branch scalability. Supports branch size that can scale up to 100 APs and 250,000 square feet (5000 sq. feet per AP).

The Cisco FlexConnect solution also supports Central Client Data Traffic, but it is limited to Guest data traffic only. This next table describes the restrictions on WLAN L2 security types only for non-guest clients whose data traffic is also switched centrally at the Data Center.

**Table 1 L2 Security Support for Centrally Switched Non-Guest Users**

WLAN L2 Security	Type	Result
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	CCKM	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed
CKIP	-	Allowed

**Note:** These authentication restrictions do not apply to clients whose data traffic is distributed at the branch.

**Table 2 L3 Security Support for Centrally and Locally Switched Users**

WLAN L3 Security	Type	Result
Web Authentication	Internal	Allowed
	External	Allowed
	Customized	Allowed
Web Pass-Through	Internal	Allowed
	External	Allowed
	Customized	Allowed
Conditional Web Redirect	External	Allowed
Splash Page Web Redirect	External	Allowed

For more information on Flexconnect external webauth deployment, please refer to [Flexconnect External WebAuth Deployment Guide](#)

For more information on HREAP/FlexConnect AP states and data traffic switching options, refer to [Configuring FlexConnect](#).

## FlexConnect Modes of Operation

FlexConnect Mode	Description
Connected	A FlexConnect is said to be in Connected Mode when its CAPWAP control plane back to the controller is up and operational, meaning the WAN link is not down.
Standalone	Standalone mode is specified as the operational state the FlexConnect enters when it no longer has the connectivity back to the controller. FlexConnect APs in Standalone mode will continue to function with last known configuration, even in the event of power failure and WLC or WAN failure.

For more information on FlexConnect Theory of Operations, refer to the [H-Reap/FlexConnect Design and Deployment Guide](#).

## WAN Requirements

FlexConnect APs are deployed at the Branch site and managed from the Data Center over a WAN link. The maximum transmission unit (MTU) must be at least 500 bytes.

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	64 Kbps	300 ms	5	25
Data	640 Kbps	300 ms	50	1000
Data	1.44Mbps	1 sec	50	1000
Data + Voice	128 Kbps	100 ms	5	25
Data + Voice	1.44Mbps	100 ms	50	1000
Data + Flex AVC	75 Kbps	300 msec	5	25
Monitor	64 Kbps	2 sec	5	N/A
Monitor	640 Kbps	2 sec	50	N/A

**Note:** It is highly recommended that the minimum bandwidth restriction remains 12.8 Kbps per AP with the round trip latency no greater than 300 ms for data deployments and 100 ms for data + voice deployments.

For large deployments with scale for max APs per branch = 100 and max clients per branch = 2000.

### Key Features

Adaptive WIPS, Context Aware (RFIDs), Rogue Detection, Clients with central 802.1X auth and CleanAir.

### Test Results

For 100 APs, 2000 Clients, 1000 RFIDs, 500 Rogue APs, and 2500 Rogue Clients (Features above turned on):

Recommended BW = 1.54 Mbps

Recommended RTT latency = 400 ms

**Test Results**

For 100 APs, 2000 Clients, no rogue, and no RFIDs. (Features above turned off).

Recommended BW = 1.024 Mbps

Recommended Latency = 300 ms

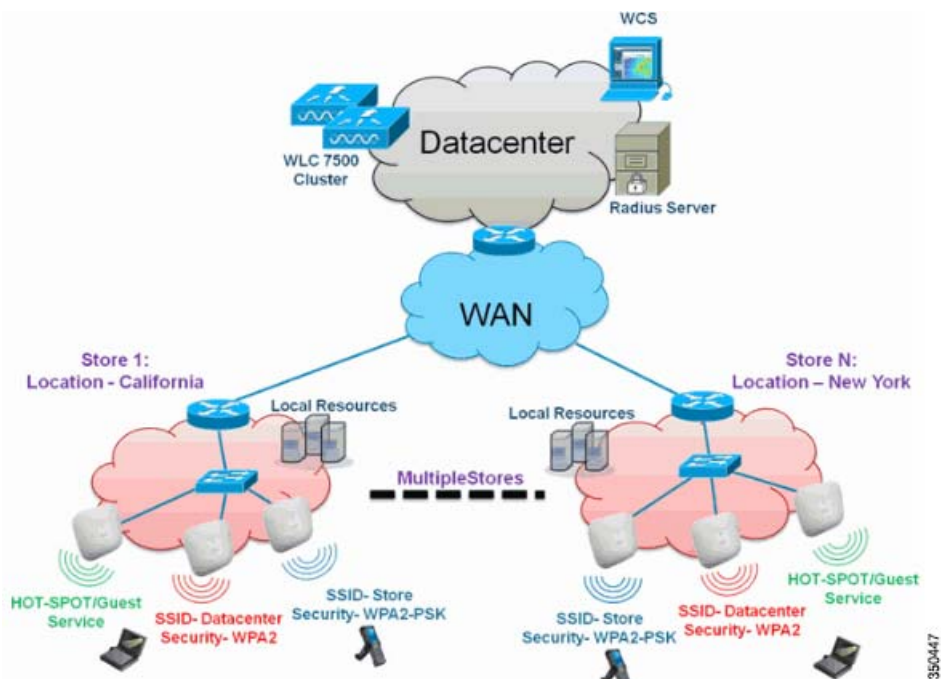
## Wireless Branch Network Design

The rest of this document highlights the guidelines and describes the best practices for implementing secured distributed branch networks. FlexConnect architecture is recommended for wireless branch networks that meet these design requirements.

### Primary Design Requirements

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 sq. feet per AP)
- Central management and troubleshooting
- No operational downtime
- Client-based traffic segmentation
- Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests

**Figure 6 Wireless Branch Network Design**



## Overview

Branch customers find it increasingly difficult and expensive to deliver full-featured scalable and secure network services across geographic locations. In order to support customers, Cisco is addressing these challenges by introducing the Flex 7500.

The Flex 7500 solution virtualizes the complex security, management, configuration, and troubleshooting operations within the data center and then transparently extends those services to each branch. Deployments using Flex 7500 are easier for IT to set up, manage and, most importantly, scale.

## Advantages

- Increase scalability with 6000 AP support.
- Increased resiliency using FlexConnect Fault Tolerance.
- Increase segmentation of traffic using FlexConnect (Central and Local Switching).
- Ease of management by replicating store designs using AP groups and FlexConnect Groups.

## Features Addressing Branch Network Design

The rest of the sections in the guide captures feature usage and recommendations to realize the network design shown in [Figure 6 on page 10](#).

**Table 3 Features**

Primary Features	Highlights
AP Groups	Provides operational/management ease when handling multiple branch sites. Also, gives the flexibility of replicating configurations for similar branch sites.
FlexConnect Groups	FlexConnect Groups provide the functionality of Local Backup Radius, CCKM/OKC fast roaming, and Local Authentication.
Fault Tolerance	Improves the wireless branch resiliency and provides no operational downtime.
ELM (Enhanced Local Mode for Adaptive WIPS)	Provide Adaptive WIPS functionality when serving clients without any impact to client performance.
Client Limit per WLAN	Limiting total guest clients on branch network.
AP Pre-image Download	Reduces downtime when upgrading your branch.
Auto-convert APs in FlexConnect	Functionality to automatically convert APs in FlexConnect for your branch.
Guest Access	Continue existing Cisco's Guest Access Architecture with FlexConnect.

**Note:** Flexconnect APs implemented with WIPS mode can increase bandwidth utilization significantly based on the activity being detected by the APs. If the rules have forensics enabled, the link utilization can go up by almost 100 Kbps on an average.

## IPv6 Support Matrix

Features	Centrally Switched		Locally Switched	
	5500/ WiSM-2/8500	Flex 7500	5500 / WiSM-2/8500	Flex 7500
IPv6 (Client Mobility)	Supported	Not Supported	Not Supported	Not Supported
IPv6 RA guard	Supported	Supported	Supported	Supported
IPv6 DHCP guard	Supported	Not Supported	Not Supported	Not Supported
IPv6 Source guard	Supported	Not Supported	Not Supported	Not Supported
RA throttling/ Rate limit	Supported	Not Supported	Not Supported	Not Supported
IPv6 ACL	Supported	Not Supported	Not Supported	Not Supported
IPv6 Client Visibility	Supported	Not Supported	Not Supported	Not Supported
IPv6 Neighbor discovery caching	Supported	Not Supported	Not Supported	Not Supported
IPv6 Bridging	Supported	Not Supported	Supported	Supported

## Feature Matrix

Refer to [FlexConnect Feature Matrix](#) for a feature matrix for the FlexConnect feature.

## Infrastructure Multicast

It is not possible to configure the AP multicast mode for Cisco Flex 7500 series controllers because only unicast is supported.

Also, it is not possible to configure Global multicast mode for Cisco Flex 7500 series controllers.

## AP Groups

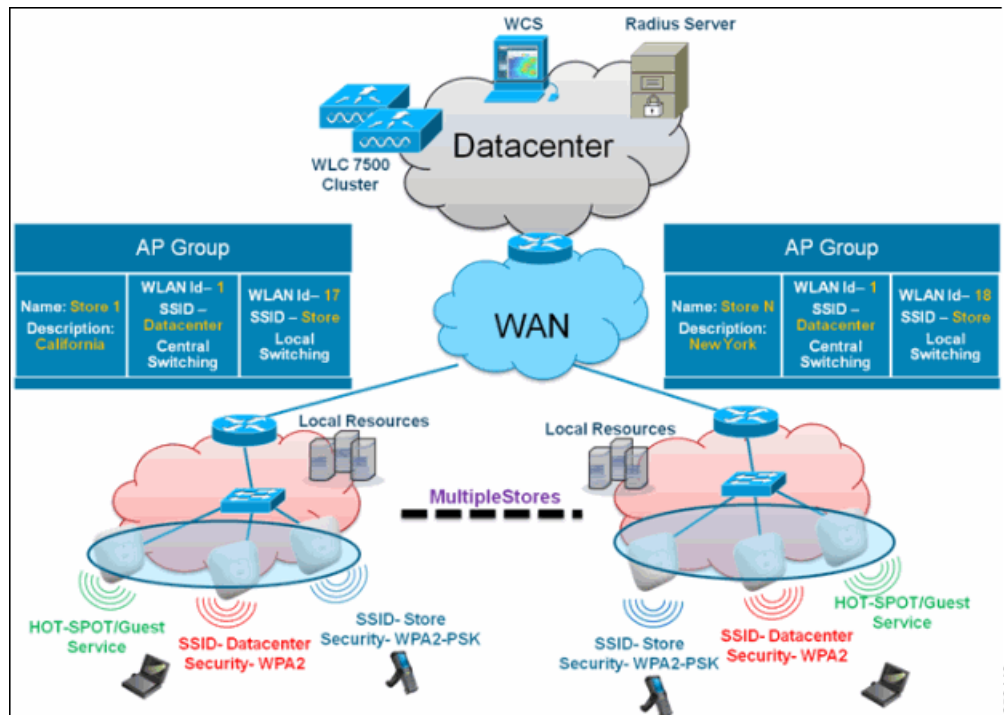
After creating WLANs on the controller, you can selectively publish them (using access point groups) to different access points in order to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing, Engineering or Operations) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

This document uses AP groups to simplify network administration when managing multiple stores across geographic locations. For operational ease, the document creates one AP-group per store to satisfy these requirements:

- Centrally Switched SSID Data center across all stores for Local Store Manager administrative access.
- Locally Switched SSID Store with different WPA2-PSK keys across all stores for hand-held scanners.



**Figure 7 Wireless Network Design Reference Using AP Groups**



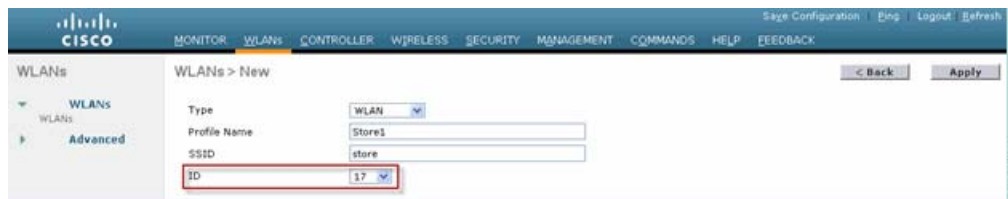
350448

Configurations from WLC

Complete the following steps:

1. On the **WLANs > New** page, enter **Store1** in the **Profile Name** field, enter **store** in the **SSID** field, and choose **17** from the **ID** drop-down list.

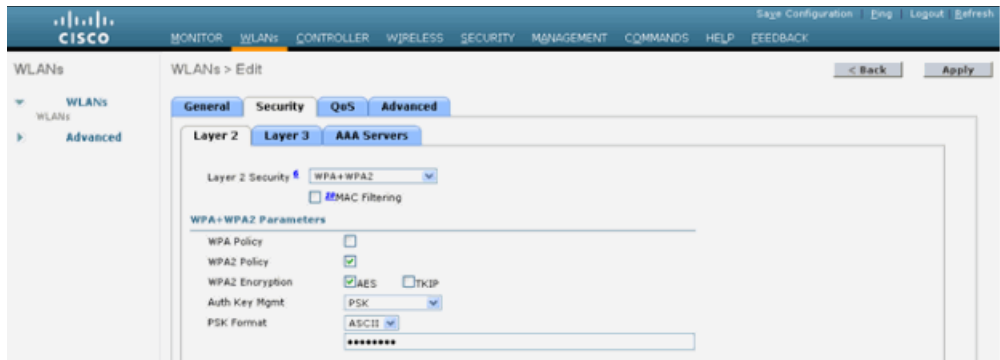
**Note:** WLAN IDs 1-16 are part of the default group and cannot be deleted. In order to satisfy our requirement of using same SSID store per store with a different WPA2-PSK, you need to use WLAN ID 17 and beyond because these are not part of the default group and can be limited to each store.



350448

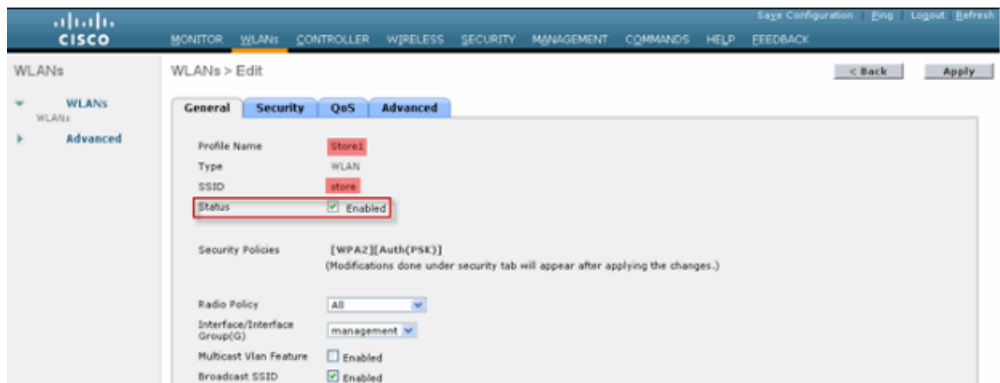
2. Under **WLANs > Security**, choose **PSK** from the **Auth Key Mgmt** drop-down list, choose **ASCII** from the **PSK Format** drop-down list, and then click **Apply**.

AP Groups



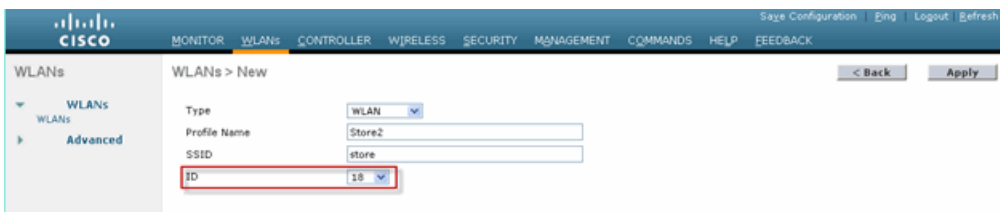
350450

3. Click **WLANs > General**, verify the Security Policies change, and check the **Status** box to enable the WLAN.

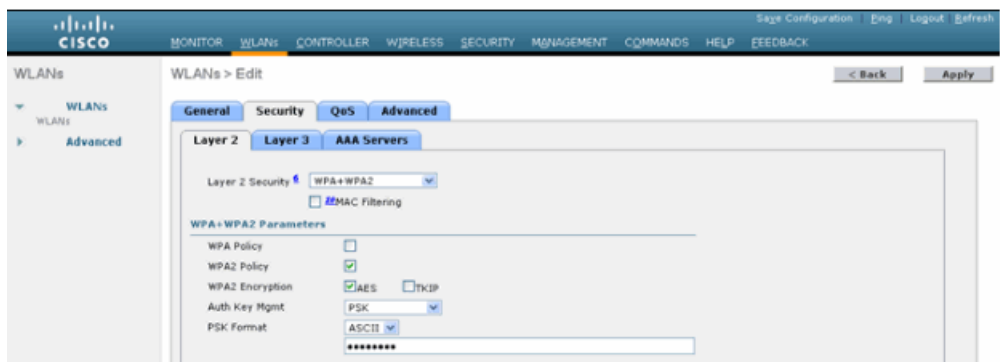


350451

4. Repeat steps 1, 2 and 3 for new WLAN profile **Store2**, with SSID as **store** and ID as **18**.

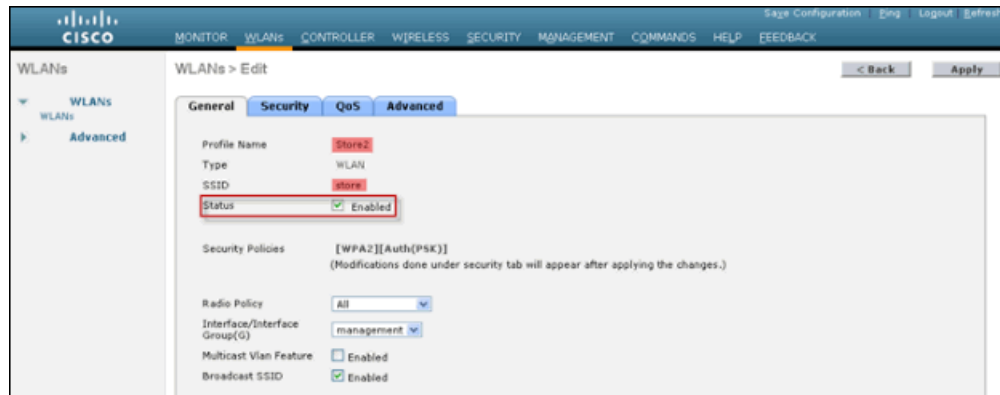


350452



350453

AP Groups



350454

5. Create and enable the WLAN profile with Profile Name **DataCenter**, SSID **DataCenter** and ID **1**.

**Note:** On creation, WLAN IDs from 1–16 are automatically part of the default-ap-group.

6. Under **WLANs**, verify the status of WLAN IDs 1, 17 and 18.

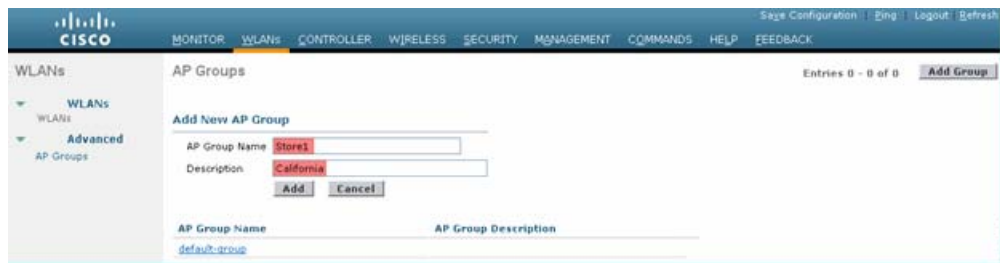


350455

7. Click **WLANs > Advanced > AP group > Add Group**.

8. Add AP Group Name as **Store1**, same as WLAN profile **Store1**, and Description as the Location of the Store. In this example, California is used as the location of the store.

9. Click **Add** when done.

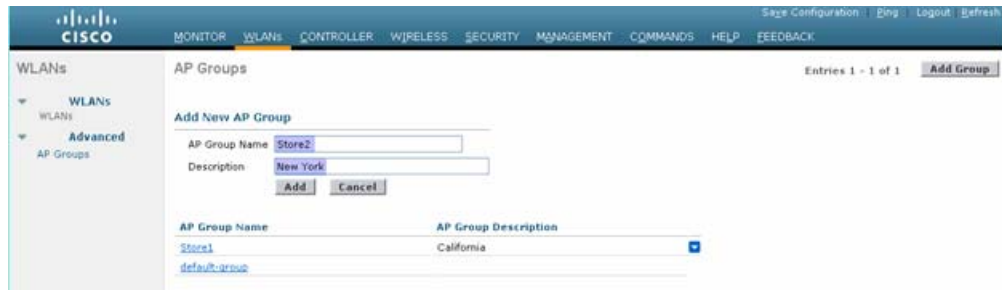


350456

10. Click **Add Group** and create the AP Group Name as **Store2** and the description as New York.

11. Click **Add**.

## AP Groups



350457

12. Verify the group creation by navigating to **WLANs > Advanced > AP Groups**.



350458

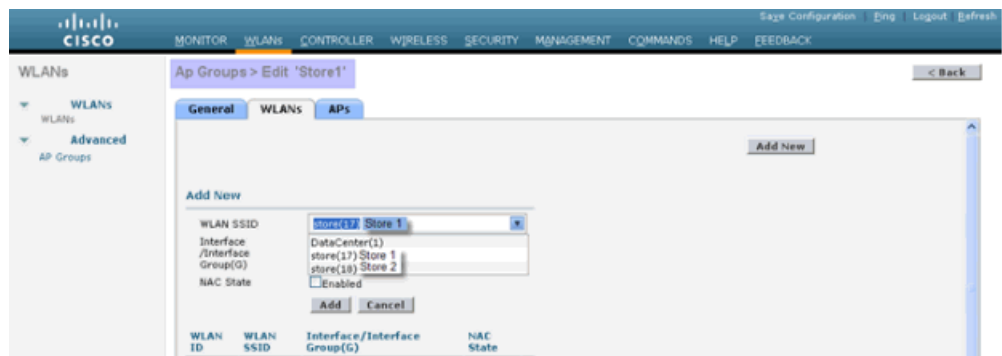
13. Click AP Group Name **Store1** to add or edit the WLAN.

14. Click **Add New** to select the WLAN.

15. Under **WLANs**, from the **WLAN SSID** drop-down, choose **WLAN ID 17 store(17)**.

16. Click **Add** after WLAN ID 17 is selected.

17. Repeat steps (14 -16) for WLAN ID 1 DataCenter(1). This step is optional and needed only if you want to allow Remote Resource access.



350459

18. Go back to the **WLANs > Advanced > AP Groups**.

19. Click AP Group Name **Store2** to add or edit WLAN.

20. Click **Add New** to select the WLAN.

21. Under **WLANs**, from **WLAN SSID** drop-down, choose **WLAN ID 18 store(18)**.

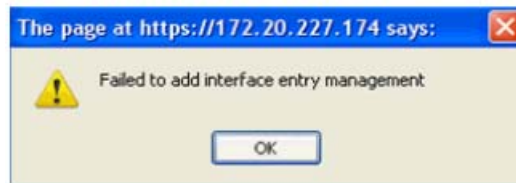
22. Click **Add** after WLAN ID 18 is selected.

23. Repeat steps 14 -16 for WLAN ID 1 DataCenter(1).

## AP Groups



**Note:** Adding multiple WLAN profiles with the same SSID under a single AP group is not permitted.



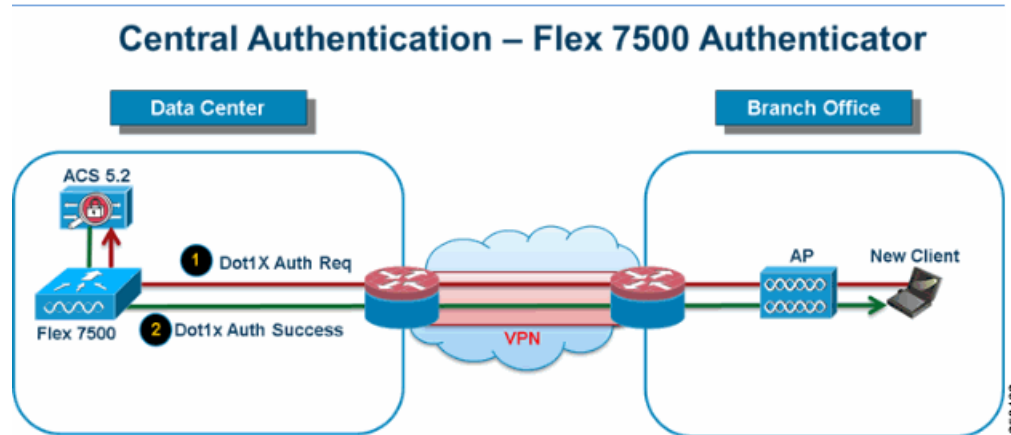
**Note:** Adding APs to the AP group is not captured in this document, but it is needed for clients to access network services.

## Summary

- AP groups simplify network administration.
- Troubleshooting ease with per branch granularity
- Increased flexibility

## FlexConnect Groups

**Figure 8 Central Dot1X Authentication (Flex 7500 Acting as Authenticator)**



In most typical branch deployments, it is easy to foresee that client 802.1X authentication takes place centrally at the Data Center as shown in [Figure 8 on page 18](#). Because the above scenario is perfectly valid, it raises these concerns:

- How can wireless clients perform 802.1X authentication and access Data Center services if Flex 7500 fails?
- How can wireless clients perform 802.1X authentication if WAN link between Branch and Data Center fails?
- Is there any impact on branch mobility during WAN failures?
- Does the FlexConnect Solution provide no operational branch downtime?

FlexConnect Group is primarily designed and should be created to address these challenges. In addition, it eases organizing each branch site, because all the FlexConnect access points of each branch site are part of a single FlexConnect Group.

**Note:** FlexConnect Groups are not analogous to AP Groups.

## Primary Objectives of FlexConnect Groups

### Backup RADIUS Server Failover

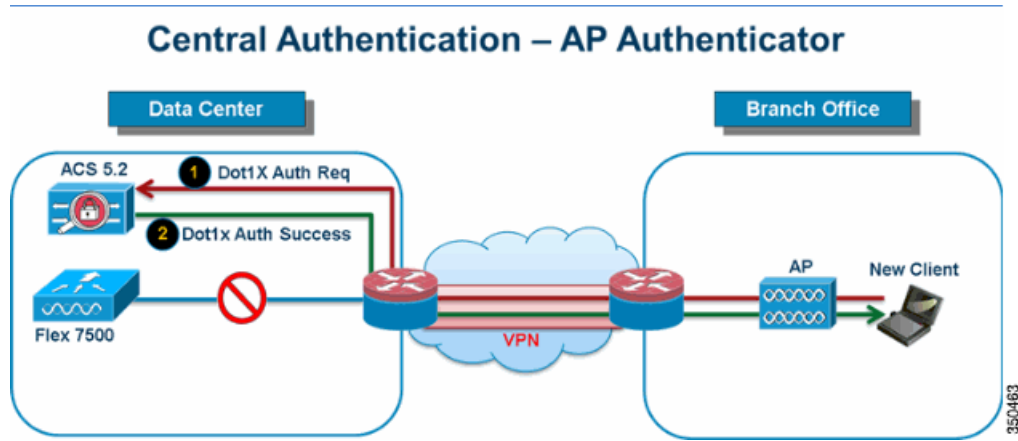
You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. In order to increase the resiliency of the branch, administrators can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers are used only when the FlexConnect access point is not connected to the controller.

**Note:** Backup RADIUS accounting is not supported.

### Local Authentication

Before the 7.0.98.0 code release, local authentication was supported only when FlexConnect is in Standalone Mode to ensure client connectivity is not affected during WAN link failure. With the 7.0.116.0 release, this feature is now supported even when FlexConnect access points are in Connected Mode.

Figure 9 Central Dot1X Authentication (FlexConnect APs Acting as Authenticator)

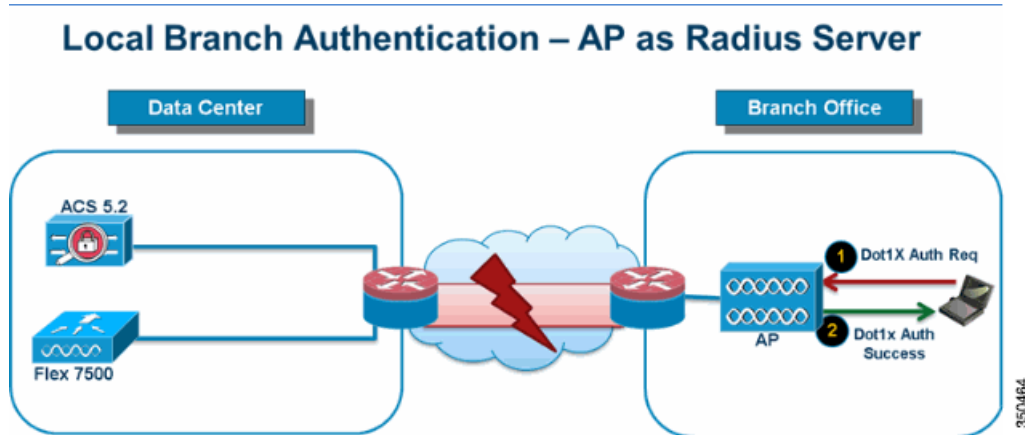


As shown in [Figure 9 on page 19](#), branch clients can continue to perform 802.1X authentication when the FlexConnect Branch APs lose connectivity with Flex 7500. As long as the RADIUS/ACS server is reachable from the Branch site, wireless clients will continue to authenticate and access wireless services. In other words, if the RADIUS/ACS is located inside the Branch, then clients will authenticate and access wireless services even during a WAN outage.

**Note:** This feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect Group is configured with both backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the Local EAP Server on FlexConnect access point itself (if the primary and secondary are not reachable).

Local EAP (Local Authentication Continuation)

Figure 10 Dot1X Authentication (FlexConnect APs Acting as Local-EAP Server)



- You can configure the controller to allow a FlexConnect AP in standalone or connected mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the static list of user names and passwords to each FlexConnect access point of that particular FlexConnect Group when it joins the controller. Each access point in the group authenticates only its own associated clients.

## FlexConnect Groups

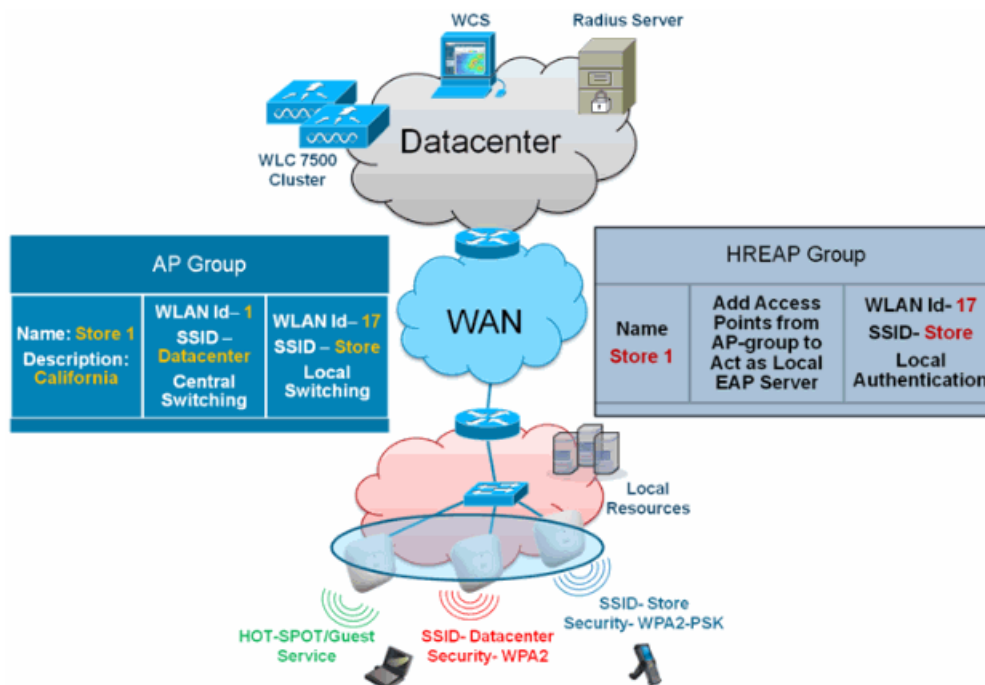
- This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database, or adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.
- As shown in [Figure 10 on page 19](#), if the RADIUS/ACS server inside the Data Center is not reachable, then FlexConnect APs automatically acts as a Local-EAP Server to perform Dot1X authentication for wireless branch clients.

## CCKM/OKC Fast Roaming

- FlexConnect Groups are required for CCKM/OKC fast roaming to work with FlexConnect access points. Fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM/OKC cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM/OKC cache for all 100 clients is not practical. If you create a FlexConnect Group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM/OKC cache is distributed among those four access points only when the clients associate to one of them.
- This feature along with Backup Radius and Local Authentication (Local-EAP) ensures **no operational downtime** for your branch sites.

**Note:** CCKM/OKC fast roaming among FlexConnect and non-FlexConnect access points is not supported.

**Figure 11 Wireless Network Design Reference Using FlexConnect Groups**



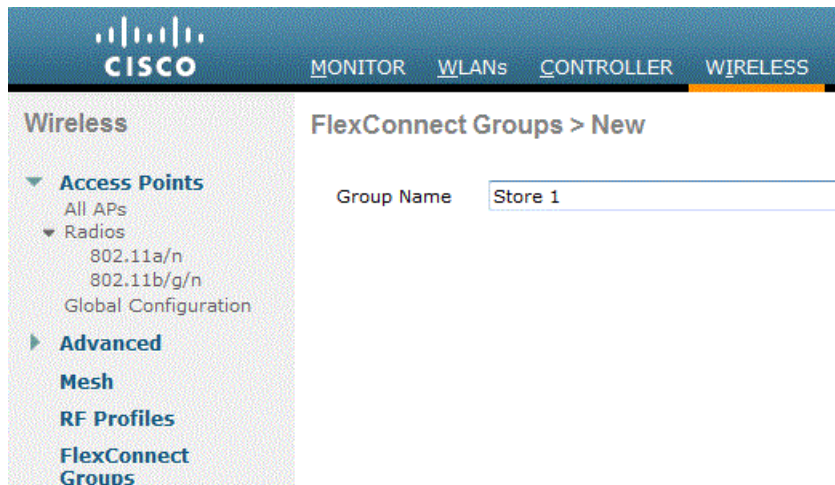
350465



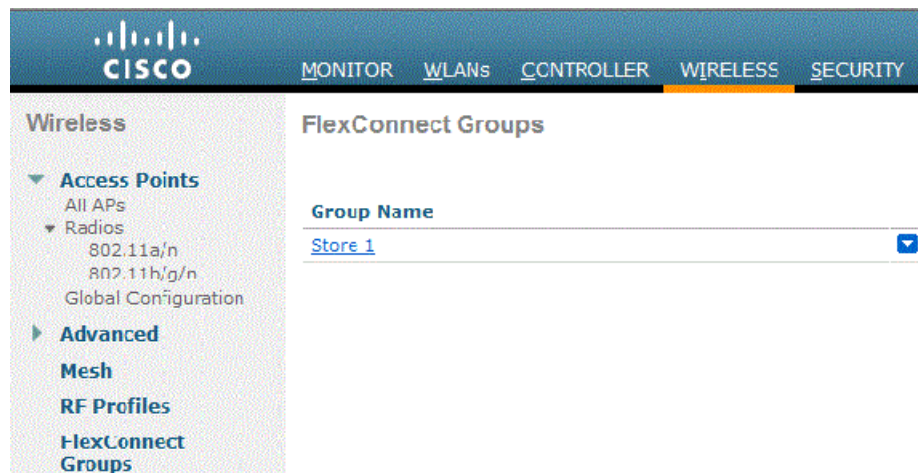
## FlexConnect Group Configuration from WLC

Complete the steps in this section in order to configure FlexConnect Groups to support Local Authentication using LEAP, when FlexConnect is either in Connected or Standalone mode. The configuration sample in [Figure 11 on page 20](#) illustrates the objective differences and 1:1 mapping between the AP Group and FlexConnect Group.

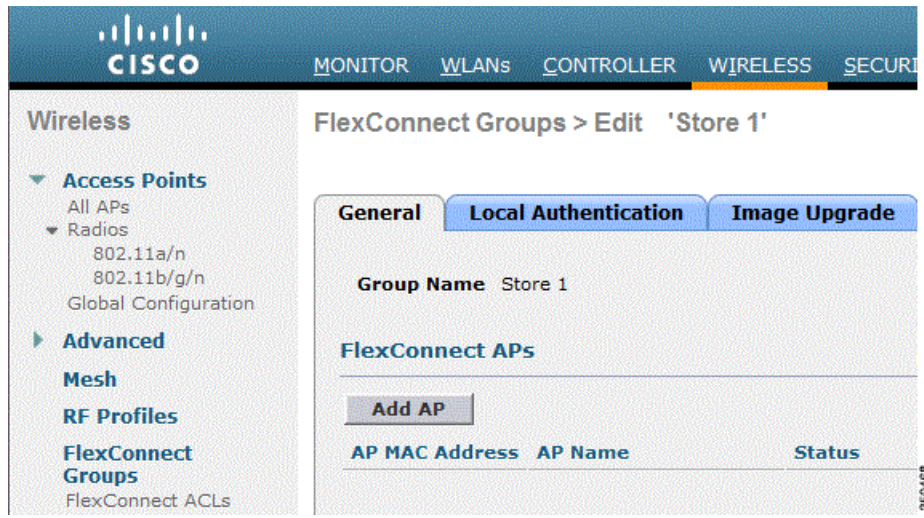
1. Click **New** under **Wireless > FlexConnect Groups**.
2. Assign Group Name **Store 1**, similar to the sample configuration as shown in [Figure 11 on page 20](#).
3. Click **Apply** when the Group Name is set.



4. Click the Group Name **Store 1** that you just created for further configuration.



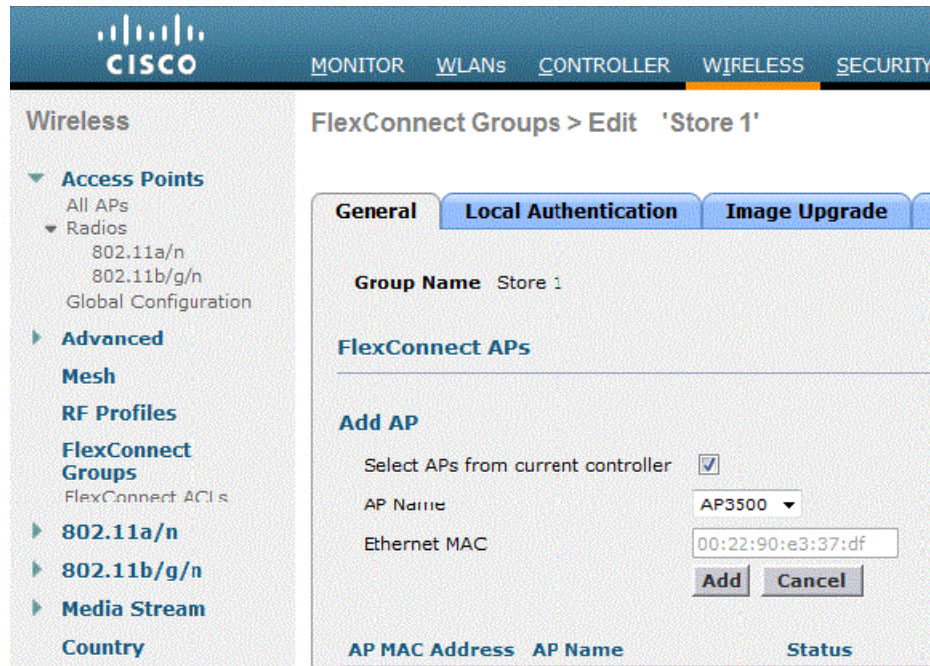
5. Click **Add AP**.



6. Check the **Enable AP Local Authentication** check box to enable Local Authentication when the AP is in Standalone Mode.
- Note:** Step 20 shows how to enable Local Authentication for Connected Mode AP.
7. Check the **Select APs from current controller** check box to enable the **AP Name** drop-down menu.
8. Choose the AP from the drop-down that needs to be part of this FlexConnect Group.
9. Click **Add** after the AP is chosen from the drop-down.
10. Repeat steps 7 and 8 to add all the APs to this FlexConnect Group that are also part of AP-Group Store 1. See [Figure 11 on page 20](#) to understand the 1:1 mapping between the AP-Group and FlexConnect Group.

If you have created an AP-Group per Store ([Figure 7 on page 13](#)), then ideally all the APs of that AP-Group should be part of this FlexConnect Group ([Figure 11 on page 20](#)). Maintaining 1:1 ratio between the AP-Group and FlexConnect Group simplifies network management.

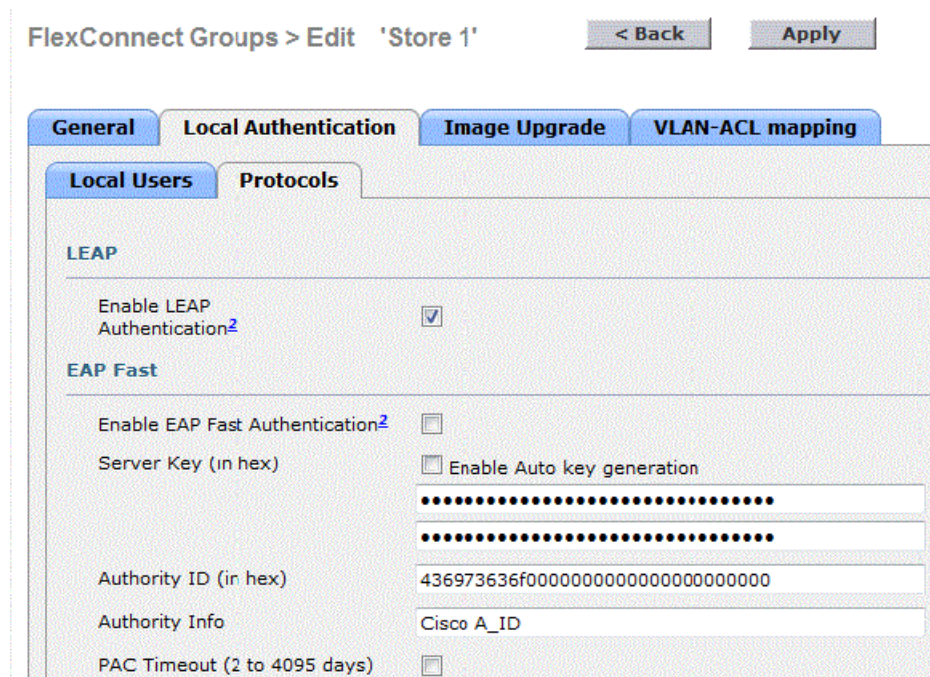




11. Click **Local Authentication > Protocols** and check the **Enable LEAP Authentication** check box.

12. Click **Apply**.

**Note:** If you have a backup controller, make sure the FlexConnect Groups are identical and AP MAC address entries are included per FlexConnect Group.



## FlexConnect Groups

13. Under **Local Authentication**, click **Local Users**.
14. Set the **UserName**, **Password** and **Confirm Password** fields, then click **Add** to create user entry in the Local EAP server residing on the AP.
15. Repeat step 13 until your local user name list is exhausted. You cannot configure or add more than 100 users.
16. Click **Apply** after step 14 is completed and the Number of users count is verified.

FlexConnect Groups > Edit 'Store 1'

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

**Local Users** **Protocols**

Nc of Users: 0 **Add User**

**User Name**

Upload CSV file:

File Name:

UserName:

Password:

Confirm Password:

**Add**

350471

17. From the top pane, click **WLANs**.
18. Click **WLAN ID 17**. This was created during the AP Group creation. See [Figure 7 on page 13](#).

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGER

WLANs

WLANs

Advanced

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

<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

350472

19. Under **WLANs > Edit** for WLAN ID 17, click **Advanced**.
20. Check the **FlexConnect Local Auth** check box to enable Local Authentication in Connected Mode.
 

**Note:** Local Authentication is supported only for FlexConnect with Local Switching.

**Note:** Always make sure to create the FlexConnect Group before enabling Local Authentication under WLAN.



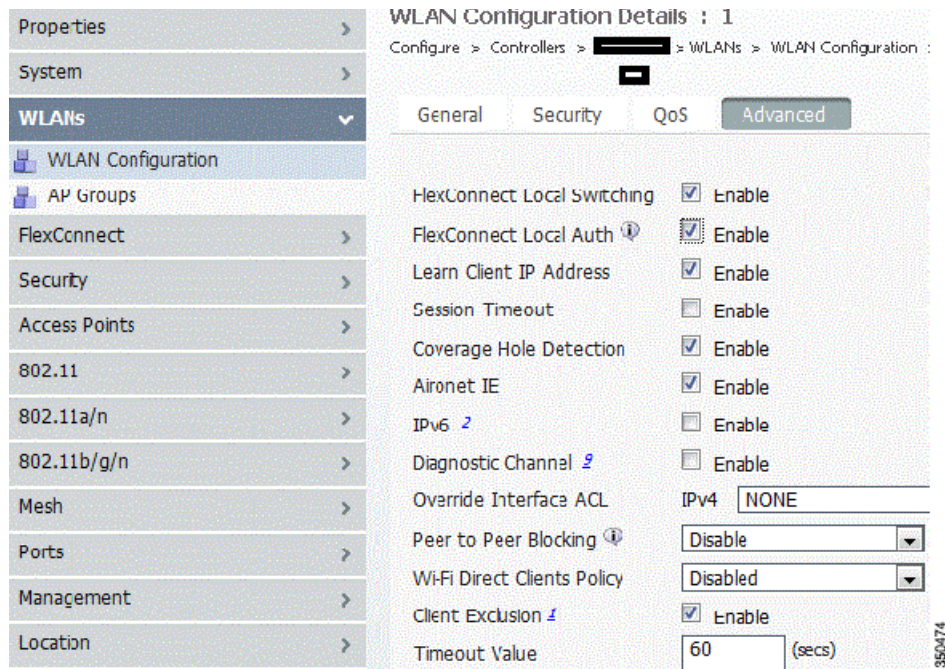
WLANs > Edit 'Store-1'

The screenshot shows the 'Advanced' tab of the WLAN configuration for 'Store-1'. The configuration is as follows:

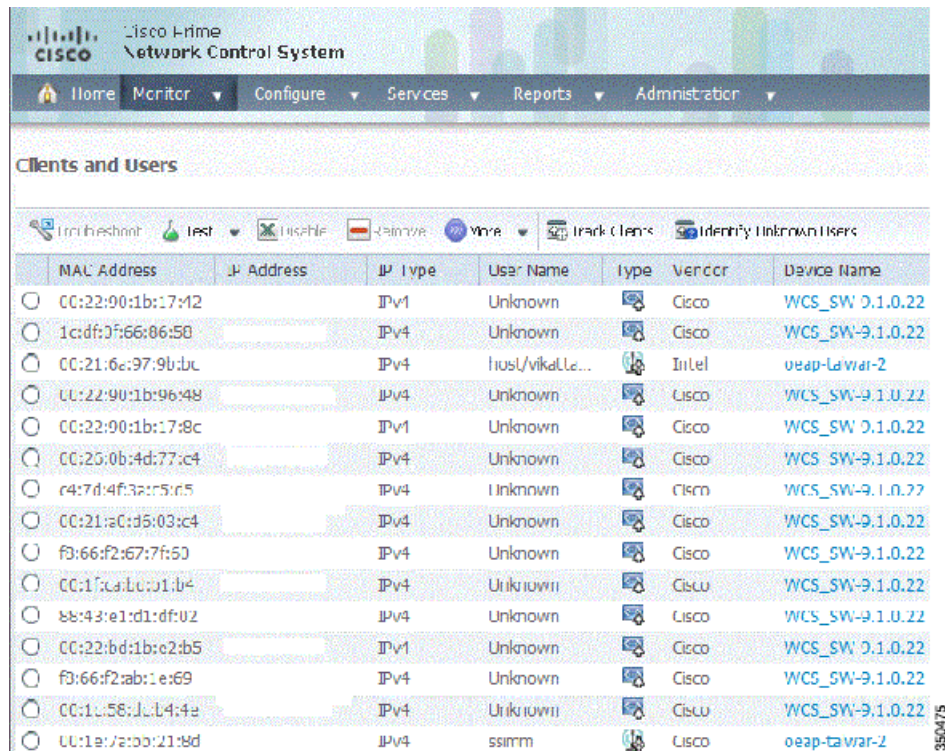
Setting	Value
P2P Blocking Action	Disabled
Client Exclusion	Enabled (Timeout Value: 60 secs)
Maximum Allowed Clients	0
Static IP Tunneling	Enabled
Wi-Fi Direct Clients Policy	Disabled
Maximum Allowed Clients Per AP Radio	200
<b>Off Channel Scanning Defer</b>	
Scan Defer Priority	0: <input type="checkbox"/>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

NCS and Cisco Prime also provides the FlexConnect Local Auth check box in order to enable Local Authentication in Connected Mode as shown here:

FlexConnect Groups



NCS and Cisco Prime also provides facility to filter and monitor FlexConnect Locally Authenticated clients as shown here:





The screenshot shows a web interface for managing FlexConnect Groups. At the top, it displays 'Virtual Domain: ROOT-DOMAIN' and 'root' with a 'Log Out' button. Below this is a search bar and navigation icons. A table lists associated clients with columns for Location, VLAN, Status, and Interface. A 'Show' dropdown menu is open, displaying various filter options such as 'All', '2.4GHz Clients', '5GHz Clients', and 'Associated Clients'. The table contains 15 rows of data, and the filter menu lists 15 options. A vertical ID '350478' is visible on the right side of the interface.

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

### Verification Using CLI

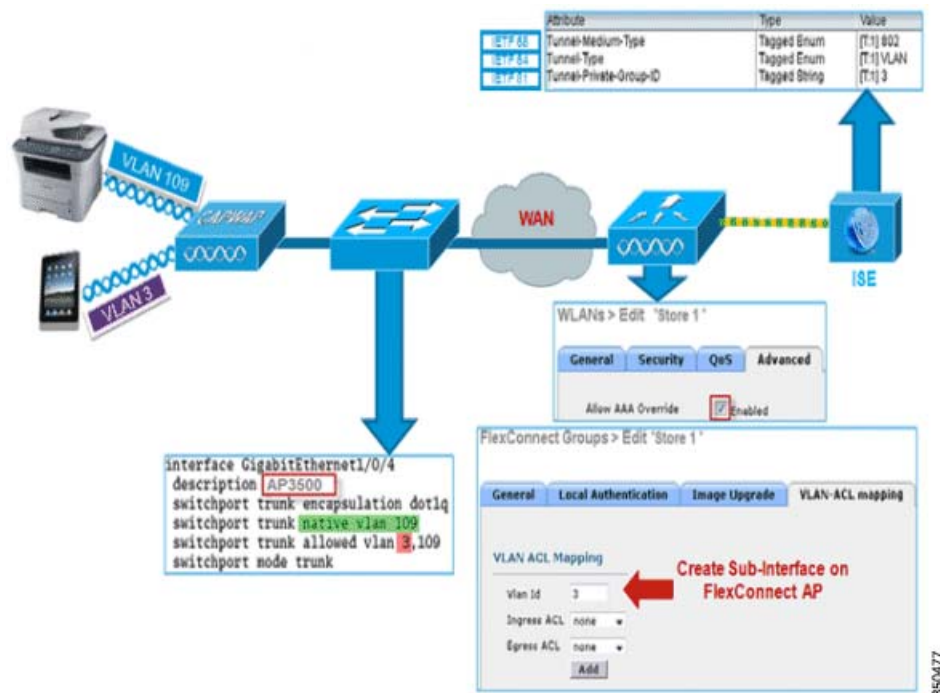
Client authentication state and switching mode can quickly be verified using this CLI on the WLC:

```
(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
```

## FlexConnect VLAN Override

In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, and thus the client getting associated on a particular WLAN on FlexConnect AP has to abide by a VLAN which is mapped to it. This method has limitations, because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

From 7.2 release onwards, AAA override of VLAN on individual WLAN configured for local switching is supported. In order to have dynamic VLAN assignment, AP would have the interfaces for the VLAN pre-created based on a configuration using existing WLAN-VLAN Mapping for individual FlexConnect AP or using ACL-VLAN mapping on a FlexConnect Group. The WLC is used to pre-create the sub-interfaces at the AP.



## Summary

- AAA VLAN override is supported from release 7.2 for WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on WLAN configured for local switching.
- The FlexConnect AP should have VLAN pre-created from WLC for dynamic VLAN assignment.
- If VLANs returned by AAA override are not present on AP client, they will get an IP from the default VLAN interface of the AP.

## Procedure

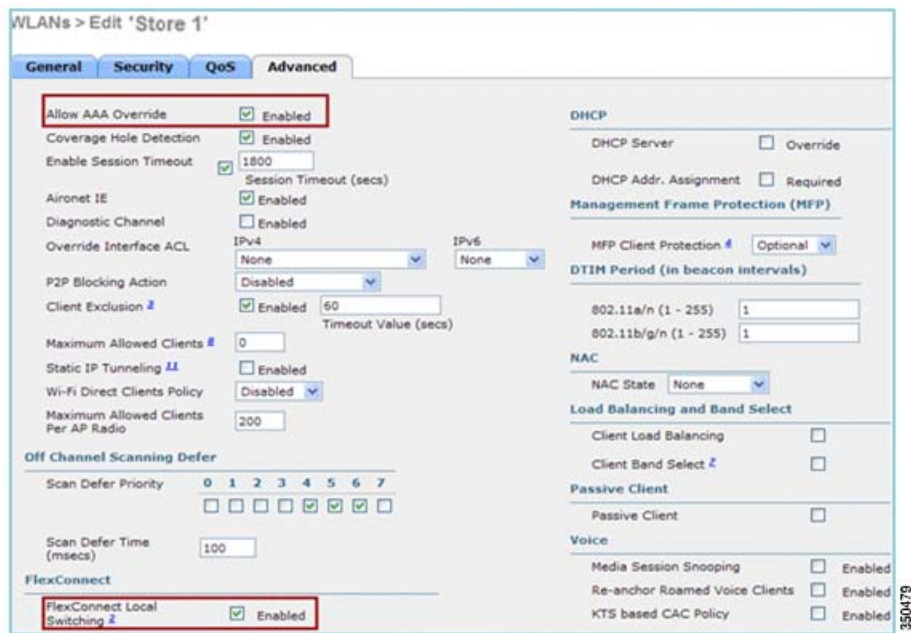
Complete these steps:

1. Create a WLAN for 802.1x authentication.





2. Enable AAA override support for local switching WLAN on the WLC. Navigate to **WLAN GUI > WLAN > WLAN ID > Advanced** tab.



3. Add the AAA server details on the controller for 802.1x authentication. To add the AAA server, navigate to **WLC GUI > Security > AAA > Radius > Authentication > New**.

Security

RADIUS Authentication Servers > Edit

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

Server Index: 1

Server Address: [Redacted]

Shared Secret Format: ASCII

Shared Secret: [Redacted]

Confirm Shared Secret: [Redacted]

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

350480

4. The AP is in local mode by default, so convert the mode to FlexConnect mode. Local mode APs can be converted to FlexConnect mode by going to **Wireless > All APs**, and click the Individual AP.

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)S

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

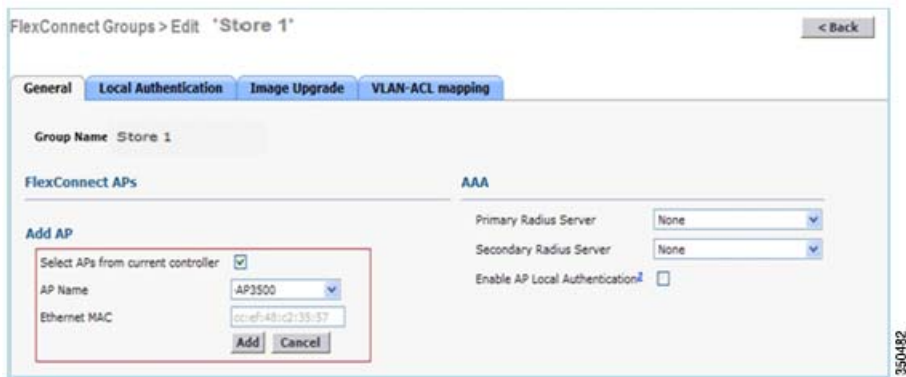
Controller Associated Time: 0 d, 00 h 00 m 14 s

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

350481

5. Add the FlexConnect APs to the FlexConnect Group.
6. Navigate under **WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General tab > Add AP**.

FlexConnect VLAN Override

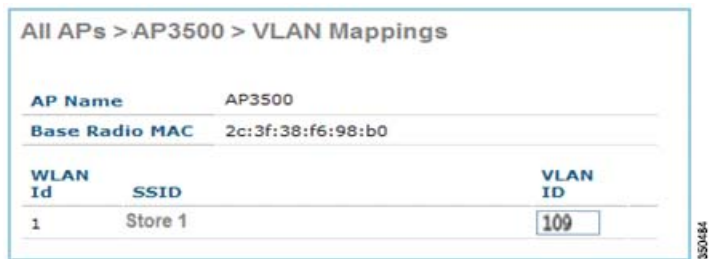


- The FlexConnect AP should be connected on a trunk port and WLAN mapped VLAN and AAA overridden VLAN should be allowed on the trunk port.

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

**Note:** In this configuration, VLAN 109 is used for WLAN VLAN mapping and VLAN 3 is used for AAA override.

- Configure WLAN to VLAN Mapping for the FlexConnect AP. Based on this configuration, the AP would have the interfaces for the VLAN. When the AP receives the VLAN configuration, corresponding dot11 and Ethernet sub-interfaces are created and added to a bridge-group. Associate a client on this WLAN and when the client associates, its VLAN (default, based on the WLAN-VLAN mapping) is assigned.
- Navigate to **WLAN GUI > Wireless > All APs**, click the specific **AP > FlexConnect** tab, and click **VLAN Mapping**.

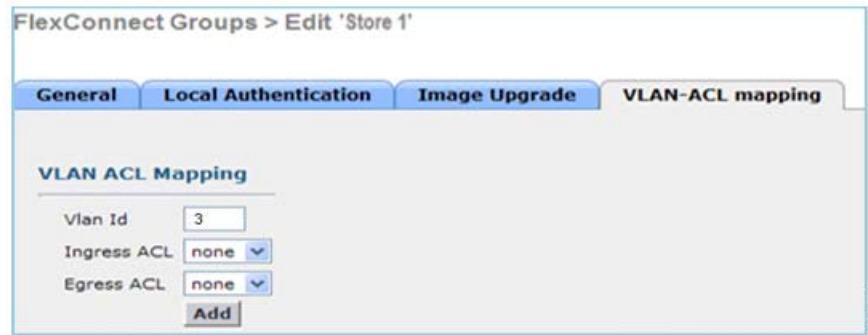


- Create a user in the AAA server and configure the user to return VLAN ID in IETF Radius attribute.

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

## FlexConnect VLAN Based Central Switching

11. To have dynamic VLAN assignment, the AP would have the interfaces for the dynamic VLAN pre-created based on the configuration using existing WLAN-VLAN Mapping for the individual FlexConnect AP or using ACL-VLAN mapping on FlexConnect Group.
12. To configure AAA VLAN on the FlexConnect AP, navigate to **WLC GUI > Wireless > FlexConnect Group**, click the specific **FlexConnect group > VLAN-ACL mapping**, and enter VLAN in the **Vlan ID** field.



13. Associate a client on this WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN.
14. The client should receive an IP address from the dynamic VLAN returned via the AAA server.
15. To verify, click **WLC GUI > Monitor > Client**, click the specific client MAC address in order to check the client details.

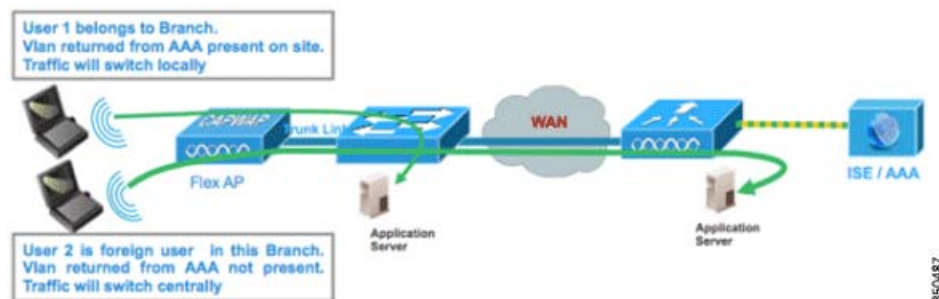
## Limitations

- Cisco AireSpace-specific attributes will not be supported and IETF attribute VLAN ID will only be supported.
- A maximum of 16 VLANs can be configured in per-AP configuration either via WLAN-VLAN Mapping for individual FlexConnect AP or using ACL-VLAN mapping on the FlexConnect Group.

## FlexConnect VLAN Based Central Switching

In controller software releases 7.2, AAA override of VLAN (Dynamic VLAN assignment) for locally switched WLANs will put wireless clients to the VLAN provided by the AAA server. If the VLAN provided by the AAA server is not present at the AP, the client is put to a WLAN mapped VLAN on that AP and traffic will switch locally on that VLAN. Further, prior to release 7.3, traffic for a particular WLAN from FlexConnect APs can be switched Centrally or Locally depending on the WLAN configuration.

From release 7.3 onwards, traffic from FlexConnect APs can be switched Centrally or Locally depending on the presence of a VLAN on a FlexConnect AP.



## Summary

Traffic flow on WLANs configured for Local Switching when Flex APs are in Connected Mode:

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the Flex AP database, traffic will switch centrally and the client will be assigned this VLAN/Interface returned from the AAA server provided that the VLAN exists on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the Flex AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be assigned a VLAN/Interface mapped to a WLAN on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client will be assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

Traffic flow on WLANs configured for Local Switching when Flex APs are in Standalone Mode:

- If the VLAN returned by an AAA server is not present in the Flex AP database, the client will be put to default VLAN (that is, a WLAN mapped VLAN on Flex AP). When the AP connects back, this client will be de-authenticated and will switch traffic centrally.
- If the VLAN returned by an AAA server is present in the Flex AP database, the client will be put into a returned VLAN and traffic will switch locally.
- If the VLAN is not returned from an AAA server, the client will be assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

## Procedure

Complete these steps:

1. Configure a WLAN for Local Switching and enable AAA override.

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	<input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)
Maximum Allowed Clients	0
Static IP Tunneling	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	Disabled
Maximum Allowed Clients Per AP Radio	200

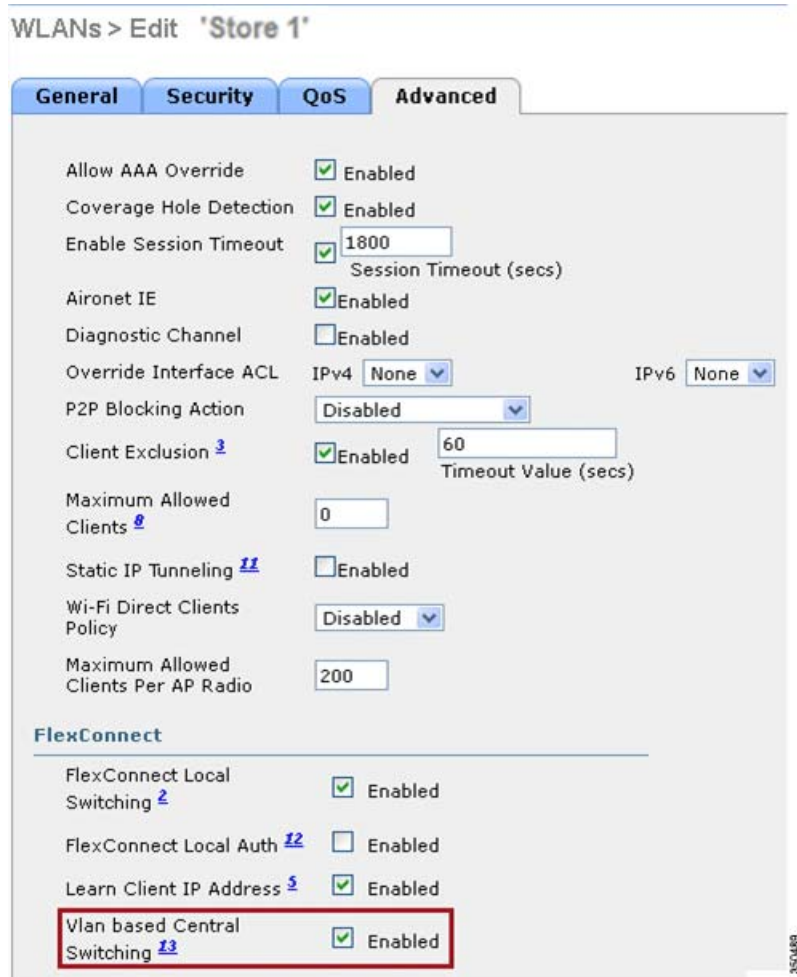
**FlexConnect**

FlexConnect Local Switching	<input checked="" type="checkbox"/> Enabled
-----------------------------	---

3550488

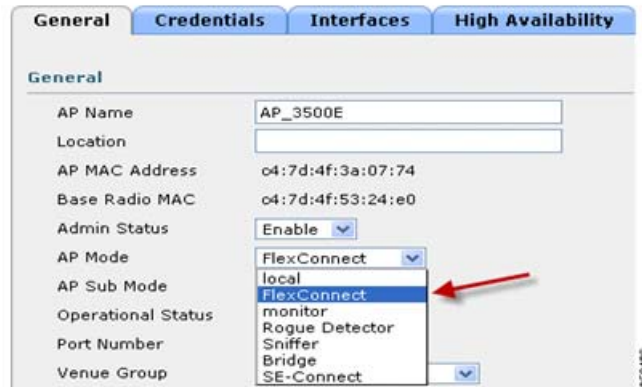
2. Enable **Vlan based Central Switching** on the newly created WLAN.

FlexConnect VLAN Based Central Switching



3. Set AP Mode to FlexConnect.

All APs > Details for AP\_3500E





- Make sure that the FlexConnect AP has some sub-interface present in its database, either via WLAN-VLAN Mapping on a particular Flex AP or via configuring VLAN from a Flex group. In this example, VLAN 63 is configured in WLAN-VLAN mapping on Flex AP.

The screenshot shows the Cisco FlexConnect AP configuration page for AP\_3500E. The page is titled "All APs > AP\_3500E > VLAN Mappings". The left sidebar shows the navigation menu with "Wireless" selected. The main content area shows the following configuration:

AP Name: AP\_3500E  
Base Radio MAC: 04:7d:4f:53:24:e0

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

Below this table, there are sections for "Centrally switched Wlans", "AP level VLAN ACL Mapping", and "Group level VLAN ACL Mapping". The "AP level VLAN ACL Mapping" section shows a table with columns for "Vlan Id", "Ingress ACL", and "Egress ACL". The row for Vlan Id 63 shows "none" for both Ingress and Egress ACLs.

- In this example, VLAN 62 is configured on WLC as one of the dynamic interfaces and is not mapped to the WLAN on the WLC. The WLAN on the WLC is mapped to Management VLAN (that is, VLAN 61).

The screenshot shows the Cisco FlexConnect WLC configuration page for the Controller. The page is titled "Controller > Interfaces". The left sidebar shows the navigation menu with "Controller" selected. The main content area shows the following configuration:

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

- Associate a client to the WLAN configured in Step 1 on this Flex AP and return VLAN 62 from the AAA server. VLAN 62 is not present on this Flex AP, but it is present on the WLC as a dynamic interface so traffic will switch centrally and the client will be assigned VLAN 62 on the WLC. In the output captured here, the client has been assigned VLAN 62 and Data Switching and Authentication are set to Central.



**Monitor**

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Redundancy
- Clients
- Multicast

**Clients > Detail**

Client Properties		AP Properties	
MAC Address	00:40:96:b0: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
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		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

Client Type	Regular
User Name	betausar
Port Number	1
Interface	dyn
VLAN ID	62

**Note:** Observe that although WLAN is configured for Local Switching, the Data Switching field for this client is Central based on the presence of a VLAN (that is, VLAN 62, which is returned from the AAA server, is not present in the AP Database).

- If another user associates to the same AP on this created WLAN and some VLAN is returned from the AAA server which is not present on the AP as well as the WLC, traffic will switch centrally and the client will be assigned the WLAN mapped interface on the WLC (that is, VLAN 61 in this example setup), because the WLAN is mapped to the Management interface which is configured for VLAN 61.

Clients > Detail

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
		Status	Associated
Client Type	Regular	Association ID	1
User Name	betouser2	802.11 Authentication	Open System
Port Number	1	Reason Code	3
Interface	management	Status Code	0
VLAN ID	61	CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

**Note:** Observe that although WLAN is configured for Local Switching, the Data Switching field for this client is Central based on the presence of a VLAN. That is, VLAN 61, which is returned from the AAA server, is not present in the AP Database but is also not present in the WLC database. As a result, the client is assigned a default interface VLAN/Interface which is mapped to the WLAN. In this example, the WLAN is mapped to a management interface (that is, VLAN 61) and so the client has received an IP address from VLAN 61.

- If another user associates to it on this created WLAN and VLAN 63 is returned from the AAA server (which is present on this Flex AP), the client will be assigned VLAN 63 and traffic will switch locally.

Clients > Detail

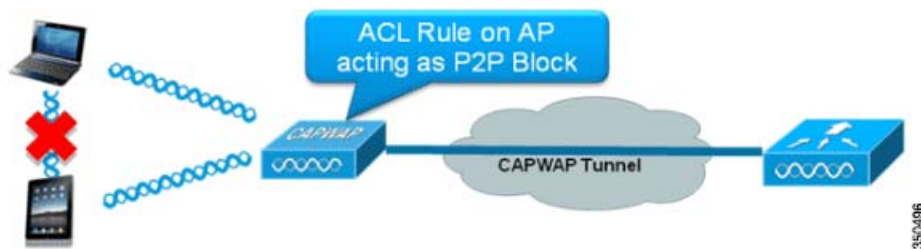
Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

## Limitations

- VLAN Based Central Switching is only supported on WLANs configured for Central Authentication and Local Switching.
- The AP sub-interface (that is, VLAN Mapping) should be configured on the FlexConnect AP.
- RADIUS NAC is not supported when VLAN based central switching feature is turned on.

## FlexConnect ACL

With the introduction of ACLs on FlexConnect, there is a mechanism to cater to the need of access control at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. FlexConnect ACLs are created on the WLC and should then be configured with the VLAN present on the FlexConnect AP or FlexConnect Group using VLAN-ACL mapping which will be for AAA override VLANs. These are then pushed to the AP.



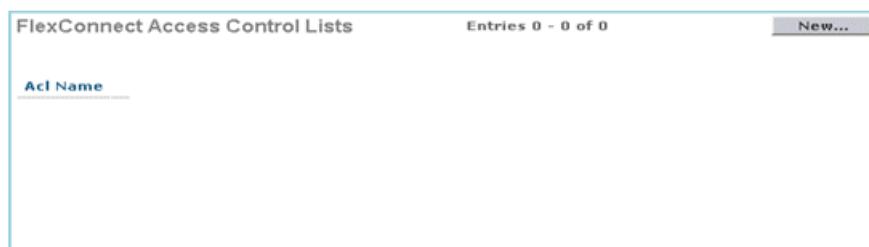
## Summary

- Create FlexConnect ACL on the controller.
- Apply the same on a VLAN present on FlexConnect AP under AP Level VLAN ACL mapping.
- Can be applied on a VLAN present in FlexConnect Group under VLAN-ACL mapping (generally done for AAA overridden VLANs).
- While applying ACL on VLAN, select the direction to be applied which will be “ingress”, “egress” or “ingress and egress”.

## Procedure

Complete these steps:

1. Create a FlexConnect ACL on the WLC. Navigate to **WLC GUI > Security > Access Control List > FlexConnect ACLs**.



2. Click **New**.
3. Configure the ACL Name.

Access Control Lists > New

< Back Apply

Access Control List Name Flex-ACL-Ingress

350498

4. Click **Apply**.

5. Create rules for each ACL. In order to create rules, navigate to **WLC GUI > Security > Access Control List > FlexConnect ACLs**, and click the above created ACL.

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
-----	--------	----------------	---------------------	----------	-------------	-----------	------

350499

6. Click **Add New Rule**.

Access Control Lists > Rules > New

< Back Apply

Sequence 1

Source IP Address 0.0.0.0 Netmask 0.0.0.0

Destination IP Address 0.0.0.0 Netmask 0.0.0.0

Protocol Any

DSCP Any

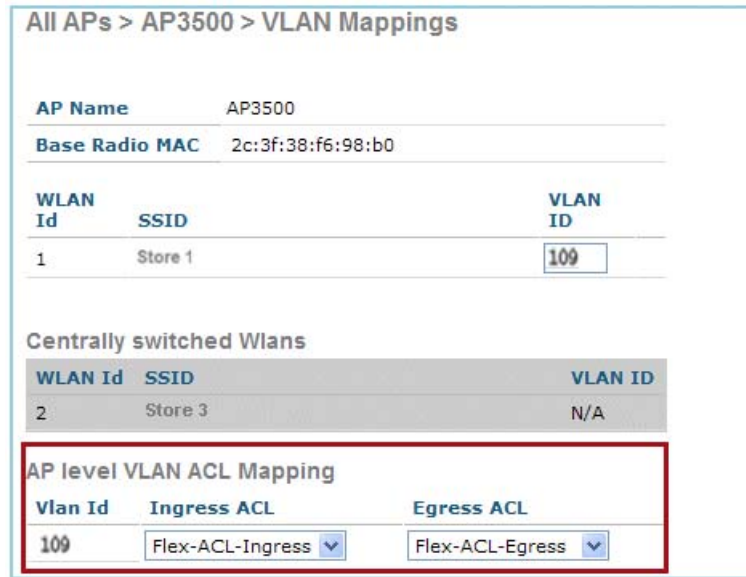
Action Deny

350500

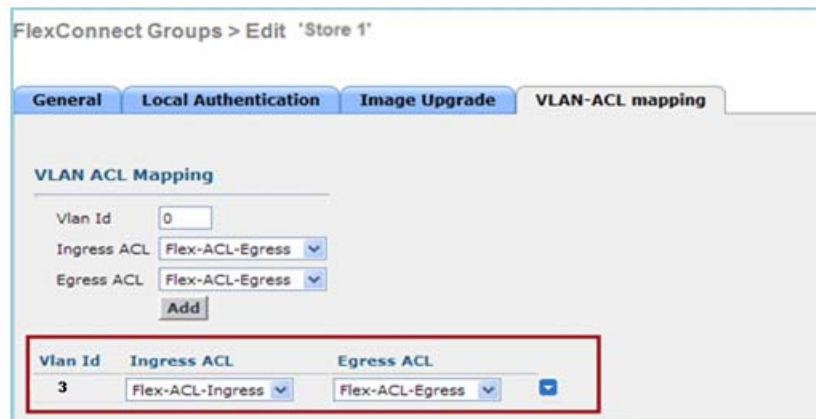
**Note:** Configure the rules as per the requirement. If the permit any rule is not configured at the end, there is an implicit deny which will block all traffic.

7. Once the FlexConnect ACLs are created, it can be mapped for WLAN-VLAN mapping under individual FlexConnect AP or can be applied on VLAN-ACL mapping on the FlexConnect Group.

8. Map FlexConnect ACL configured above at AP level for individual VLANs under VLAN mappings for individual FlexConnect AP. Navigate to **WLC GUI > Wireless > All AP**, click the specific **AP > FlexConnect tab > VLAN Mapping**.



- FlexConnect ACL can also be applied on VLAN-ACL mapping in the FlexConnect Group. VLANs created under VLAN-ACL mapping in FlexConnect Group are mainly used for dynamic VLAN override.



## Limitations

- A maximum of 512 FlexConnect ACLs can be configured on WLC.
- Each individual ACL can be configured with 64 rules.
- A maximum of 32 ACLs can be mapped per FlexConnect Group or per FlexConnect AP.
- At any given point in time, there is a maximum of 16 VLANs and 32 ACLs on the FlexConnect AP.

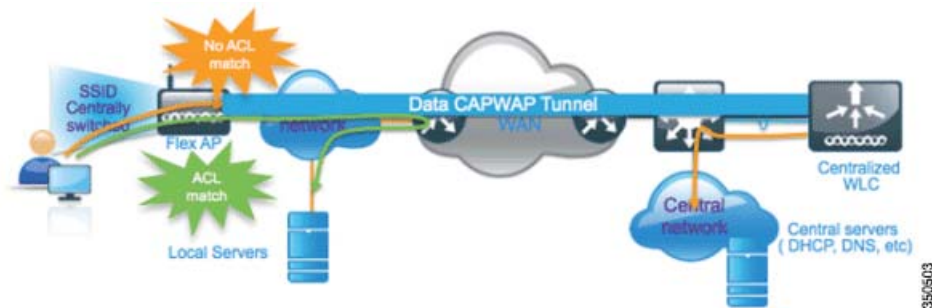
## FlexConnect Split Tunneling

In WLC releases prior to 7.3, if a client connecting on a FlexConnect AP associated with a centrally switched WLAN needs to send some traffic to a device present in the local site/network, they need to send traffic over CAPWAP to the WLC and then get the same traffic back to the local site over CAPWAP or using some off-band connectivity.

From release 7.3 onwards, **Split Tunneling** introduces a mechanism by which the traffic sent by the client will be classified based on packet contents **using Flex ACL**. Matching packets are switched locally from Flex AP and the rest of the packets are centrally switched over CAPWAP.

The Split Tunneling functionality is an added advantage for OEAP AP setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly without consuming WAN bandwidth by sending packets over CAPWAP. Split tunneling is not supported on OEAP 600 APs. Flex ACL can be created with rules in order to permit all the devices present at the local site/network. When packets from a wireless client on the Corporate SSID matches the rules in Flex ACL configured on OEAP AP, that traffic is switched locally and the rest of the traffic (that is, implicit deny traffic) will switch centrally over CAPWAP.

The Split Tunneling solution assumes that the subnet/VLAN associated with a client in the central site is not present in the local site (that is, traffic for clients which receive an IP address from the subnet present on the central site will not be able to switch locally). The Split Tunneling functionality is designed to switch traffic locally for subnets which belong to the local site in order to avoid WAN bandwidth consumption. Traffic which matches the Flex ACL rules are switched locally and NAT operation is performed changing the client's source IP address to the Flex AP's BVI interface IP address which is routable at the local site/network.



## Summary

- The Split Tunneling functionality is supported on WLANs configured for Central Switching advertised by Flex APs only.
- The DHCP required should be enabled on WLANs configured for Split Tunneling.
- The Split Tunneling configuration is applied per WLAN configured for central switching on per Flex AP or for all the Flex APs in a FlexConnect Group.

## Procedure

Complete these steps:

1. Configure a WLAN for Central Switching (that is, **Flex Local Switching** should not be enabled).



FlexConnect Split Tunneling



2. Set the **DHCP Addr. Assignment** field to **Required**.



3. Set **AP Mode** to **FlexConnect**.

All APs &gt; 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 FlexConnect

Operational Status

Port Number

Venue Group

4. Configure FlexConnect ACL with a permit rule for traffic which should be switched locally on the Central Switch WLAN. In this example, the FlexConnect ACL rule is configured so it will alert ICMP traffic from all the clients which are on the 9.6.61.0 subnet (that is, exist on the Central site) to 9.1.0.150 to be switched locally after the NAT operation is applied on Flex AP. The rest of the traffic will hit an implicit deny rule and be switched centrally over CAPWAP.

Wireless

Access Points

Radios

Global Configuration

Advanced

Mesh

RF Profiles

FlexConnect Groups

FlexConnect ACLs

Access Control Lists > Edit

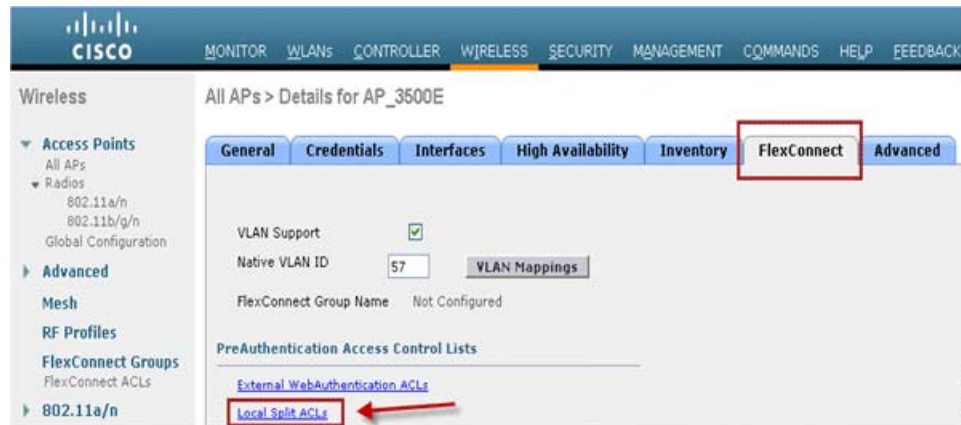
General

Access List Name Flex-ACL

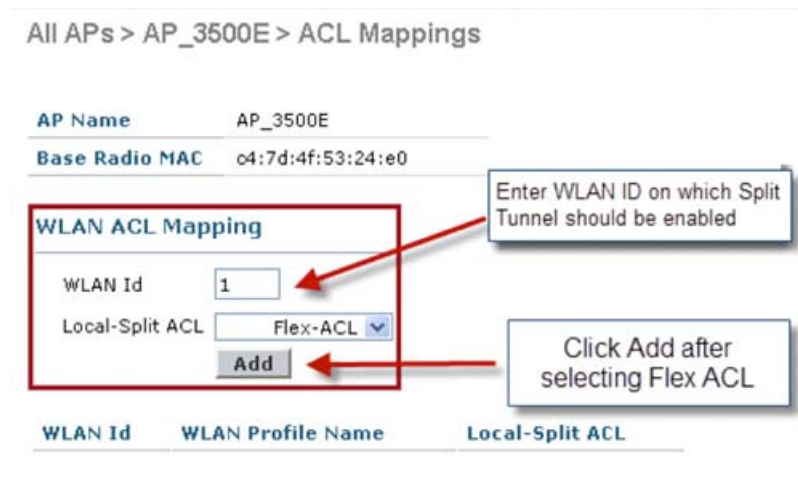
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	9.6.61.0 / 255.255.255.0	9.1.0.150 / 255.255.255.255	ICMP	Any	Any	Any

5. This created FlexConnect ACL can be pushed as a Split Tunnel ACL to individual Flex AP or can also be pushed to all the Flex APs in a Flex Connect group.
6. Complete these steps in order to push Flex ACL as a Local Split ACL to individual Flex AP:
  - a. Click **Local Split ACLs**.

FlexConnect Split Tunneling



- b. Select **WLAN Id** on which Split Tunnel feature should be enabled, choose **Flex-ACL**, and click **Add**.



- c. Flex-ACL is pushed as Local-Split ACL to the Flex AP.

## FlexConnect Split Tunneling

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

7. Complete these steps in order to push Flex ACL as Local Split ACL to a FlexConnect Group:

- Select the WLAN Id on which the Split Tunneling feature should be enabled. On the **WLAN-ACL mapping** tab, select FlexConnect ACL from the FlexConnect Group where particular Flex APs are added, and click **Add**.

Wireless FlexConnect Groups > Edit Flex-Group'

General Local Authentication Image Upgrade AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id

WebAuth ACL

Local Split 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	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL

- The Flex-ACL is pushed as LocalSplit ACL to Flex APs in that Flex group.

Wireless FlexConnect Groups > Edit Flex-Group'

General Local Authentication Image Upgrade AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id

WebAuth ACL

Local Split ACL Mapping

WLAN Id

Local Split ACL

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL
1	"Store 1"				Flex-ACL

## Limitations

- Flex ACL rules should not be configured with permit/deny statement with same subnet as source and destination.

## Fault Tolerance

- Traffic on a Centrally Switched WLAN configured for Split Tunneling can be switched locally only when a wireless client initiates traffic for a host present on the local site. If traffic is initiated by clients/host on a local site for wireless clients on these configured WLANs, it will not be able to reach the destination.
- Split Tunneling is not supported for Multicast/Broadcast traffic. Multicast/Broadcast traffic will switch centrally even if it matches the Flex ACL.

## Fault Tolerance

FlexConnect Fault Tolerance allows wireless access and services to branch clients when:

- FlexConnect Branch APs lose connectivity with the primary Flex 7500 controller.
- FlexConnect Branch APs are switching to the secondary Flex 7500 controller.
- FlexConnect Branch APs are re-establishing connection to the primary Flex 7500 controller.

FlexConnect Fault Tolerance, along with Local EAP as outlined above and PEAP/EAP-TLS authentication on FlexConnect AP with release 7.5, together provide zero branch downtime during a network outage. This feature is enabled by default and cannot be disabled. It requires no configuration on the controller or AP. However, to ensure Fault Tolerance works smoothly and is applicable, this criteria should be maintained:

- WLAN ordering and configurations have to be identical across the primary and backup Flex 7500 controllers.
- VLAN mapping has to be identical across the primary and backup Flex 7500 controllers.
- Mobility domain name has to be identical across the primary and backup Flex 7500 controllers.
- It is recommended to use Flex 7500 as both the primary and backup controllers.

## Summary

- FlexConnect will not disconnect clients when the AP is connecting back to the same controller provided there is no change in configuration on the controller.
- FlexConnect will not disconnect clients when connecting to the backup controller provided there is no change in configuration and the backup controller is identical to the primary controller.
- FlexConnect will not reset its radios on connecting back to the primary controller provided there is no change in configuration on the controller.

## Limitations

- Supported only for FlexConnect with Central/Local Authentication with Local Switching.
- Centrally authenticated clients require full re-authentication if the client session timer expires before the FlexConnect AP switches from Standalone to Connected mode.
- Flex 7500 primary and backup controllers must be in the same mobility domain.

## Client Limit per WLAN

Along with traffic segmentation, the need for restricting the total client accessing the wireless services arises. For example, limiting total Guest Clients from branch tunneling back to the Data Center.

In order to address this challenge, Cisco is introducing Client Limit per WLAN feature that can restrict the total clients allowed on a per WLAN basis.

## Primary Objective

- Set limits on maximum clients
- Operational ease

**Note:** This is not a form of QoS.

By default, the feature is disabled and does not force the limit.

## Limitations

This feature does not enforce client limit when the FlexConnect is in Standalone state of operation.

## WLC Configuration

Complete these steps:

1. Select the Centrally Switched WLAN ID 1 with SSID **DataCenter**. This WLAN was created during THE AP Group creation. See [Figure 7 on page 13](#).
2. Click the **Advanced** tab for WLAN ID 1.
3. Set the client limit value for the Maximum Allowed Clients text field.
4. Click **Apply** after the text field for Maximum Allowed Clients is set.

WLANs > Edit

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

IPv6 Enable

Override Interface ACL  None

P2P Blocking Action  Disabled

Client Exclusion  Enabled 60  
Timeout Value (secs)

**Maximum Allowed Clients 0**

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs) 100

DHCP

DHCP Server  Override

DHCP Addr. Assignment  Required

Management Frame Protection (MFP)

MFP Client Protection  Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC OOB State  Enabled

Posture State  Enabled

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Foot Notes

2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication

3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

4 Client MFP is not active unless WPA2 is configured

5 Learn Client IP is configurable only when H-REAP Local Switching is enabled

6 WMM and open or AES security should be enabled to support higher 11n rates

7 Multicast Should Be Enabled For IPv6.

8 Band Select is configurable only when Radio Policy is set to 'All'.

9 Value zero implies there is no restriction on maximum clients allowed.

10 MAC Filtering is not supported with H-REAP Local authentication

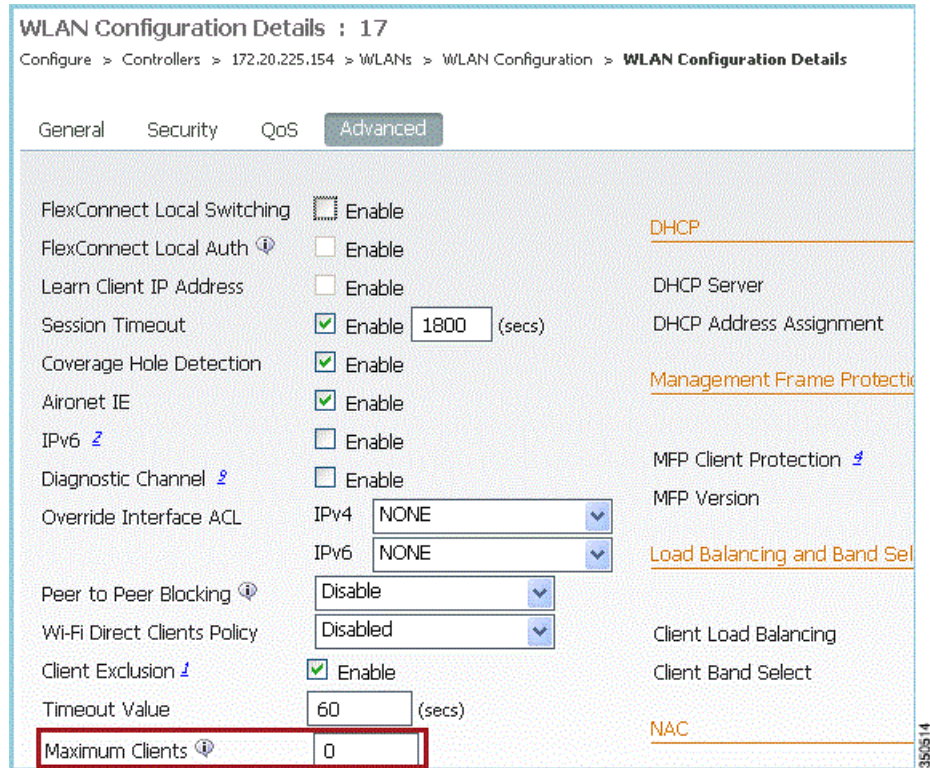
350513

Default for Maximum Allowed Clients is set to 0, which implies there is no restriction and the feature is disabled.



## NCS Configuration

In order to enable this feature from the NCS, go to **Configure > Controllers > Controller IP > WLANs > WLAN Configuration > WLAN Configuration Details**.



## Configuration through Cisco Prime

In order to enable this feature from the Cisco Prime, go to **Configure > Controllers > Controller IP > WLANs > WLAN Configuration > WLAN Configuration Details**.

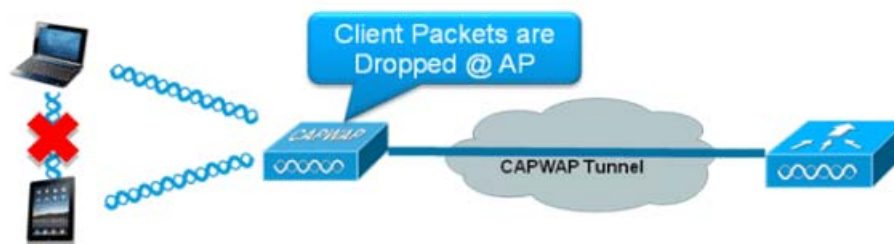
The screenshot shows the Cisco Prime Infrastructure configuration interface for WLANs. The 'Advanced' tab is active, displaying various configuration options. The 'Peer to Peer Blocking' option is set to 'Disable'. The 'Maximum Clients' field is highlighted with a red box and set to '0'. Other options include Session Timeout, Coverage Hole Detection, Aironet IE, IPv6, Diagnostic Channel, Override Interface ACL, Wi-Fi Direct Clients Policy, Client Exclusion, Timeout Value, Mobility Anchors, Foreign Controller Mappings, Passive Client, Off Channel Scanning Defer, Scan Defer Priority, Scan Defer Time, DTIM Period, FlexConnect, DHCP, MFP, Load Balancing and Band Select, NAC, and Voice.

## Peer-to-Peer Blocking

In controller software releases prior to 7.2, peer-to-peer (P2P) blocking was only supported for central switching WLANs. Peer-to-peer blocking can be configured on WLAN with any of these three actions:

- Disabled - Disables peer-to-peer blocking and bridged traffic locally within the controller for clients in the same subnet. This is the default value.
- Drop - Causes the controller to discard packets for clients in the same subnet.
- Forward Up-Stream - Causes the packet to be forwarded on the upstream VLAN. The devices above the controller decide what action to take regarding the packet.

From release 7.2 onwards, peer-to-peer blocking is supported for clients associated on local switching WLAN. Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP.



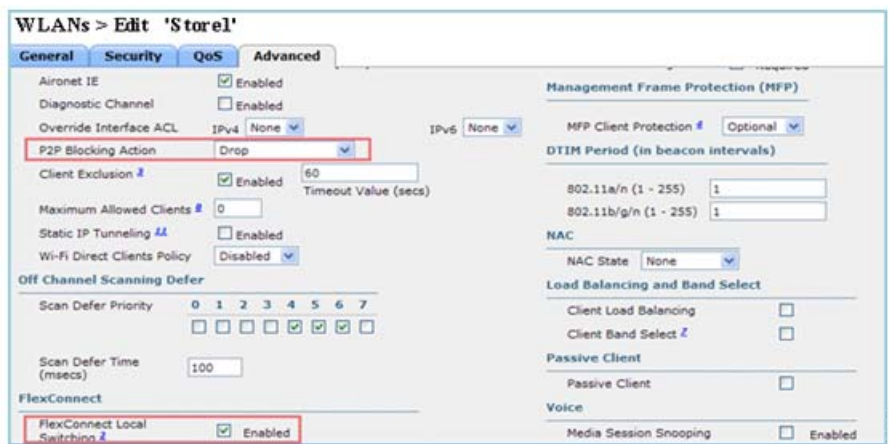
## Summary

- Peer-to-peer Blocking is configured per WLAN
- Per WLAN, peer-to-peer blocking configuration is pushed by WLC to FlexConnect APs.
- Peer-to-peer blocking action configured as drop or upstream-forward on WLAN is treated as peer-to-peer blocking enabled on FlexConnect AP.

## Procedure

Complete these steps:

1. Enable peer-to-peer blocking action as **Drop** on WLAN configured for FlexConnect Local Switching.



2. Once the P2P Blocking action is configured as **Drop** or **Forward-Upstream** on WLAN configured for local switching, it is pushed from the WLC to the FlexConnect AP. The FlexConnect APs will store this information in the reap config file in flash. With this, even when FlexConnect AP is in standalone mode, it can apply the P2P configuration on the corresponding sub-interfaces.

## Limitations

- In FlexConnect, solution P2P blocking configuration cannot be applied only to a particular FlexConnect AP or sub-set of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports P2P upstream-forward. However, this will not be supported in the FlexConnect solution. This is treated as P2P drop and client packets are dropped instead of forwarded to the next network node.
- Unified solution for central switching clients supports P2P blocking for clients associated to different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

## AP Pre-Image Download

This feature allows the AP to download code while it is operational. The AP pre-image download is extremely useful in reducing the network downtime during software maintenance or upgrades.

### Summary

- Ease of software management
- Schedule per store upgrades: NCS or Cisco Prime is needed to accomplish this.
- Reduces downtime

### Procedure

Complete these steps:

1. Upgrade the image on the primary and backup controllers.

Navigate under **WLC GUI > Commands > Download File** to start the download.

Download file to Controller

File Type: Code

Transfer Mode: TFTP

**Server Details**

IP Address: [Redacted]

Maximum retries: 10

Timeout (seconds): 6

File Path: [Redacted]

File Name: AS\_5500\_7\_0\_112\_52.aes

2. Save the configurations on the controllers, but do not reboot the controller.
3. Issue the AP pre-image download command from the primary controller.
  - a. Navigate to **WLC GUI > Wireless > Access Points > All APs** and choose the access point to start pre-image download.
  - b. Once the access point is chosen, click the **Advanced** tab.
  - c. Click **Download Primary** to initiate pre-image download.

**AP Image Download**

Perform a primary image pre-download on this AP

**Download Primary**

Perform a backup image pre-download on this AP

**Download Backup**

Perform a interchange of both the images on this AP

**Interchange Image**

## FlexConnect Smart AP Image Upgrade

```

*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.

```

4. Reboot the controllers after all the AP images are downloaded.

The APs now fall back to Standalone mode until the controllers are rebooting.

**Note:** In Standalone mode, Fault Tolerance will keep Clients associated.

Once the controller is back, the APs automatically reboot with the pre-downloaded image. After rebooting, the APs re-join the primary controller and resume client's services.

## Limitations

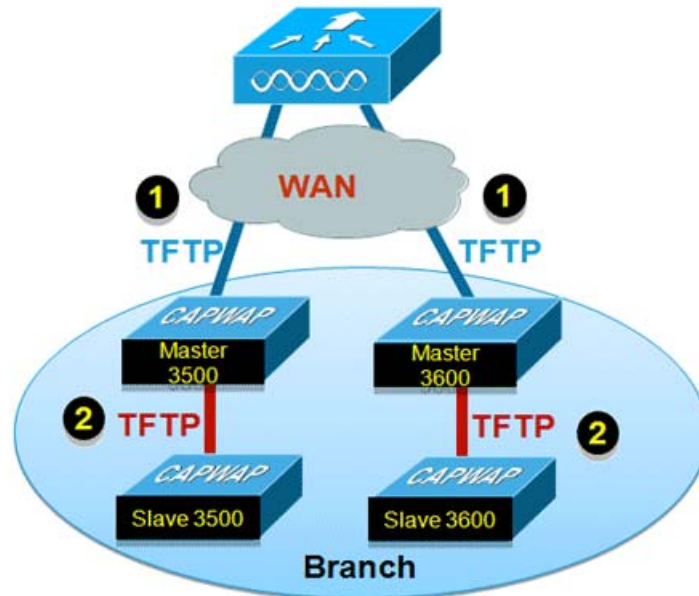
- Works only with CAPWAP APs.

## FlexConnect Smart AP Image Upgrade

The pre-image download feature reduces the downtime duration to a certain extent, but still all the FlexConnect APs have to pre-download the respective AP images over the WAN link with higher latency.



Efficient AP Image Upgrade will reduce the downtime for each FlexConnect AP. The basic idea is only one AP of each AP model will download the image from the controller and will act as Primary/Server, and the rest of the APs of the same model will work as Subordinate/Client and will pre-download the AP image from the primary. The distribution of AP image from the server to the client will be on a local network and will not experience the latency of the WAN link. As a result, the process will be faster.



360021

## Summary

- Primary and Subordinate APs are selected for each AP Model per FlexConnect Group
- Primary downloads image from WLC
- Subordinate downloads image from Primary AP
- Reduces downtime and saves WAN bandwidth

## Procedure

Complete these steps:

1. Upgrade the image on the controller.
2. Navigate to **WLC GUI > Commands > Download File** to begin the download.

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

360022



3. Save the configurations on the controllers, but do not reboot the controller.
4. Add the FlexConnect APs to FlexConnect Group.
5. Navigate to **WLC GUI > Wireless > FlexConnect Groups**, select **FlexConnect Group > General tab > Add AP**.

FlexConnect Groups > Edit 'Store 1' < Back

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

Group Name Store 1

FlexConnect APs AAA

Add AP

Select APs from current controller

AP Name AR3500

Ethernet MAC cc:ef:48:c2:35:57

Add Cancel

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication

350523

6. Check the **FlexConnect AP Upgrade** check box in order to achieve efficient AP image upgrade.
7. Navigate to **WLC GUI > Wireless > FlexConnect Groups**, select **FlexConnect Group > Image Upgrade** tab.

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

350524

8. The primary AP can be selected manually or automatically:
  - a. To manually select the primary AP, navigate to **WLC GUI > Wireless > FlexConnect Groups**, select **FlexConnect Group > Image Upgrade tab > FlexConnect Master APs**, and select **AP** from the drop-down list, and click **Add Master**.

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	c3500I	yes

350525

**Note:** Only one AP per model can be configured as primary AP. If primary AP is configured manually, the Manual field will be updated as yes.

- b. To automatically select primary AP, navigate to **WLC GUI > Wireless > FlexConnect Groups**, select **FlexConnect Group > Image Upgrade** tab, and click **FlexConnect Upgrade**.

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**

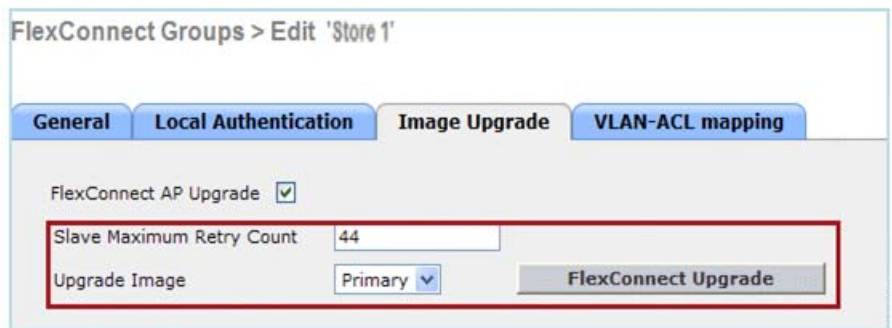
AP Name

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

350526

**Note:** If primary AP is selected automatically, the Manual field will be updated as no.

9. To start efficient AP image upgrade for all the APs under a specific FlexConnect Group, click **FlexConnect Upgrade**.
10. Navigate to **WLC GUI > Wireless > FlexConnect Groups**, select **FlexConnect group > Image Upgrade** tab and then click **FlexConnect Upgrade**.



**Note:** Subordinate Maximum Retry Count is the number of attempts (44 by default) in which the subordinate AP will make in order to download an image from the primary AP, after which it will fall back to download the image from the WLC. It will make 20 attempts against WLC in order to download a new image after which the administrator has to re-initiate the download process.

11. Once FlexConnect Upgrade is initiated, only the primary AP will download the image from the WLC. Under All AP page, **Upgrade Role** will be updated as **Master/Central** which means primary AP has downloaded the image from the WLC which is at the central location. The subordinate AP will download the image from the primary AP which is at the local site and is the reason under All AP page **Upgrade Role** will be updated as **Slave/Local**.
12. To verify this, navigate to **WLC GUI > Wireless**.

AP Name	AP Model	AP MAC	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

13. Reboot the controllers after all the AP images are downloaded. The APs now fall back to Standalone mode until the controllers are rebooting.

**Note:** In Standalone mode, Fault Tolerance will keep Clients associated.

Once the controller is back, the APs automatically reboot with the pre-downloaded image. After rebooting, the APs re-join the primary controller and resume the client's services.

## Limitations

- Primary AP selection is per FlexConnect Group and per AP model in each group.
- Only 3 subordinate APs of same model can upgrade simultaneously from their primary AP and rest of the subordinate APs will use the random back-off timer to retry for the primary AP in order to download the AP image.
- In the instance that the subordinate AP fails to download the image from the primary AP for some reason, it will go to the WLC in order to fetch the new image.
- This works only with CAPWAP APs.
- Smart AP image upgrade does not work when the primary AP is connected over CAPWAPv6.

## Auto Convert APs in FlexConnect Mode

The Flex 7500 provides these two options to convert the AP mode to FlexConnect:

- Manual mode
- Auto convert mode

### Manual Mode

This mode is available on all the platforms and allows the change to take place only on per AP basis.

1. Navigate to **WLC GUI > Wireless > All APs** and choose the AP.
2. Select **FlexConnect** as the AP Mode, then click **Apply**.
3. Changing the AP mode causes the AP to reboot.

#### 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	FlexConnect			
Operational Status	monitor			
Port Number	Rogue Detector			
Venue Group	Sniffer			
	Bridge			
	SE-Connect			

This option is also available on all the current WLC platforms.

### Auto Convert Mode

- This feature is supported in Flex 7500, 8510, 8540 and 5520 controller.

(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) >

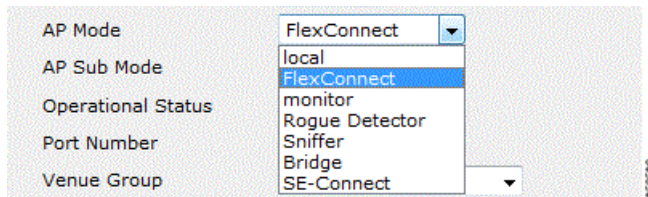
1. The Auto-conversion feature is disabled by default, which can be verified by using this **show** command:

(Cisco Controller) >show ap autoconvert

FlexConnect WGB/uWGB Support for Local Switching WLANs

AP Autoconvert ..... Disabled

Non-supported AP modes = Local Mode, Sniffer, Rogue Detector and Bridge.



This option is currently available only via CLIs.

These CLIs are available only on the WLC 7500.

- 2. Performing **config ap autoconvert flexconnect** CLI converts all the APs in the network with non-supported AP mode to FlexConnect mode. Any APs that are already in FlexConnect or Monitor Mode are not affected.

(Cisco Controller) >config ap autoconvert flexconnect

(Cisco Controller) >show ap autoconvert

AP Autoconvert ..... FlexConnect

(Cisco Controller) >

- 3. Performing **config ap autoconvert monitor** CLI converts all the APs in the network with non-supported AP mode to Monitor mode. Any APs that are already in FlexConnect or Monitor mode are not affected.

(Cisco Controller) >config ap autoconvert monitor

(Cisco Controller) >show ap autoconvert

AP Autoconvert ..... Monitor

There is no option to perform both **config ap autoconvert flexconnect** and **config ap autoconvert monitor** at the same time.

## FlexConnect WGB/uWGB Support for Local Switching WLANs

From release 7.3 onwards, WGB/uWGB and wired/wireless clients behind WGBs are supported and will work as normal clients on WLANs configured for local switching.

After association, WGB sends the IAPP messages for each of its wired/wireless clients, and Flex AP will behave as follows:

- When Flex AP is in connected mode, it forwards all the IAPP messages to the controller and the controller will process the IAPP messages the same as Local mode AP. Traffic for wired/wireless clients will be switched locally from Flex APs.
- When AP is in standalone mode, it processes the IAPP messages, wired/wireless clients on the WGB must be able to register and de-register. Upon transition to connected mode, Flex AP will send the information of wired clients back to the controller. WGB will send registration messages three times when Flex AP transitions from Standalone to Connected mode.

Wired/Wireless clients will inherit WGB's configuration, which means no separate configuration like AAA authentication, AAA override, and FlexConnect ACL is required for clients behind WGB.



35/0531

## Summary

- No special configuration is required on WLC in order to support WGB on Flex AP.
- Fault Tolerance is supported for WGB and clients behind WGB.
- WGB is supported on an IOS AP: 1240, 1130, 1140, 1260, 1600, 1250, 2600, and 3600.

## Procedure

Complete these steps:

1. No special configuration is needed in order to enable WGB/uWGB support on FlexConnect APs for WLANs configured for local switching as WGB. Also, clients behind WGB are treated as normal clients on local switching configured WLANs by Flex APs. Enable **FlexConnect Local Switching** on a WLAN.

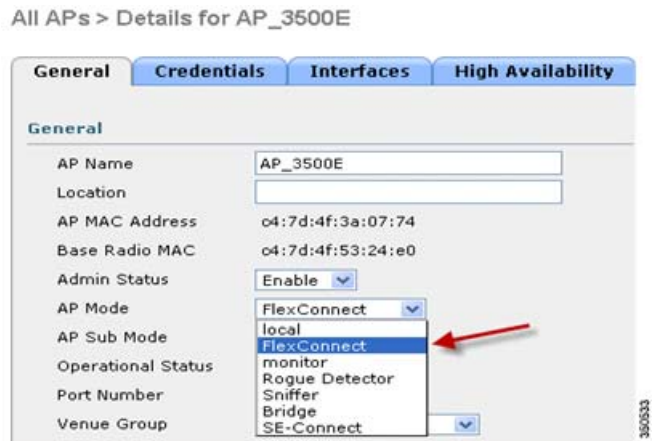
WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
Allow AAA Override	<input 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	<input checked="" type="checkbox"/>	60	Timeout Value (secs)
Maximum Allowed Clients		0	
Static IP Tunneling	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		Disabled	
Maximum Allowed Clients Per AP Radio		200	
Clear HotSpot Configuration	<input type="checkbox"/>	Enabled	
<b>FlexConnect</b>			
FlexConnect Local Switching	<input checked="" type="checkbox"/>	Enabled	

35/0532



2. Set AP Mode to FlexConnect.



3. Associate WGB with wired clients behind this configured WLAN.

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
00:40:96:30:d4:b4	AP_3500E	"Store 1"	"Store 1"	N/A	Associated	Yes	1	No
00:50:b6:09:e5:38	AP_3500E	"Store 1"	"Store 1"	N/A	Associated	Yes	1	No
04:7d:4f:3a:08:10	AP_3500E	"Store 1"	"Store 1"	802.11an	Associated	Yes	1	Yes

4. To check the details for WGB, go to Monitor > Clients, and select WGB from the list of clients.

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. To check the details of the wired/wireless clients behind WGB, go to **Monitor > Clients**, and select the client.

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		

## Limitations

- Wired clients behind WGB will always be on the same VLAN as WGN itself. Multiple VLAN support for clients behind WGB is not supported on Flex AP for WLANs configured for Local Switching.
- A maximum of 20 clients (wired/wireless) are supported behind WGB when associated to Flex AP on WLAN configured for local switching. This number is the same as what we have today for WGB support on Local mode AP.
- Web Auth is not supported for clients behind WGB associated on WLANs configured for local switching.

## Support for an Increased Number of Radius Servers

Prior to release 7.4, the configuration of RADIUS servers at the FlexConnect Group was done from a global list of RADIUS servers on the controller. The maximum number of RADIUS servers, which can be configured in this global list, is 17. With an increasing number of branch offices, it is a requirement to be able to configure a RADIUS server per branch site. In release 7.4 onwards, it will be possible to configure Primary and Backup RADIUS servers per FlexConnect Group which may or may not be part of the global list of 17 RADIUS authentication servers configured on the controller.

An AP specific configuration for the RADIUS servers will also be supported. The AP specific configuration will have greater priority than the FlexConnect Group configuration.

The existing configuration command at the FlexConnect Group, which needs the index of the RADIUS server in the global RADIUS server list on the controller, will be deprecated and replaced with a configuration command, which configures a RADIUS server at the Flexconnect Group using the IP address of the server and shared secret.

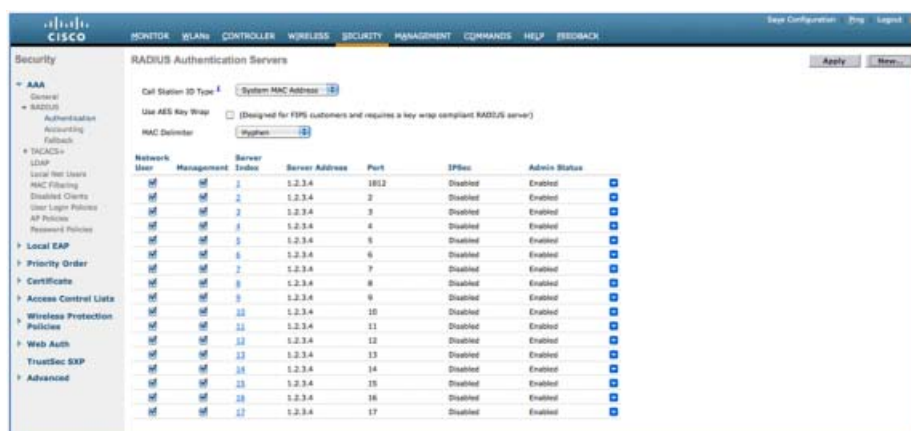
### Summary

- Support for configuration of Primary and Backup RADIUS servers per FlexConnect Group, which may or may not be present in the global list of RADIUS authentication servers.
- The maximum number of unique RADIUS servers that can be added on a WLC is the number of FlexConnect Groups that can be configured on a given platform times two. An example is one primary and one secondary RADIUS server per FlexConnect Group.
- Software upgrade from a previous release to release 7.4 will not cause any RADIUS configuration loss.
- The deletion of the primary RADIUS server is allowed without having to deleting the secondary RADIUS server. This is consistent with the present FlexConnect Group configuration for the RADIUS server.

### Procedure

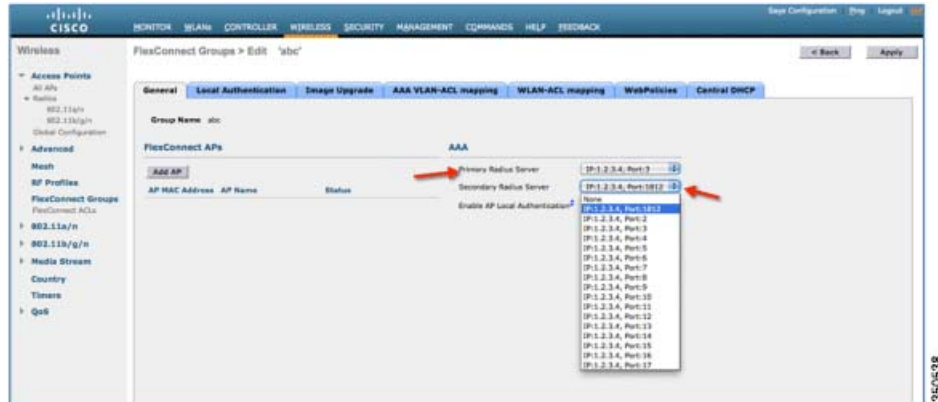
1. Mode of configuration prior to release 7.4.

A maximum of 17 RADIUS servers can be configured under the AAA Authentication configuration.



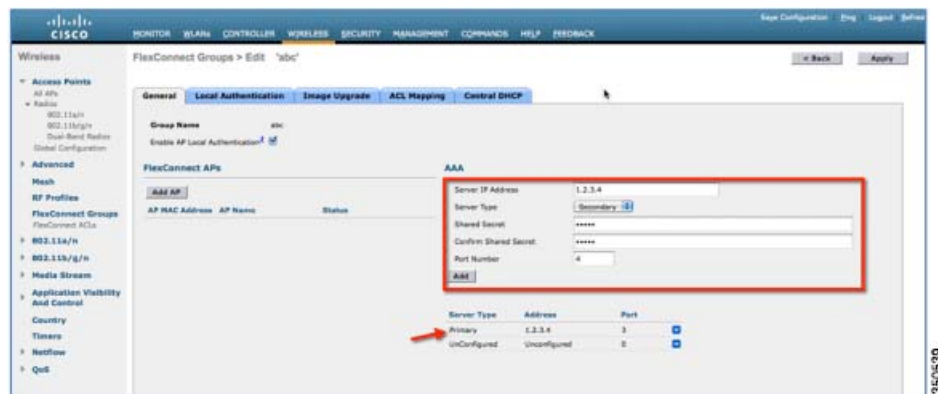
2. Primary and Secondary RADIUS servers can be associated with a FlexConnect Group using a drop-down list comprising of RADIUS servers configured on the AAA Authentication page.

## Enhanced Local Mode (ELM)



### 3. Mode of configuration at FlexConnect Group in release 7.4.

Primary and Secondary RADIUS servers can be configured under the FlexConnect Group using an IP address, port number and Shared Secret.



## Limitations

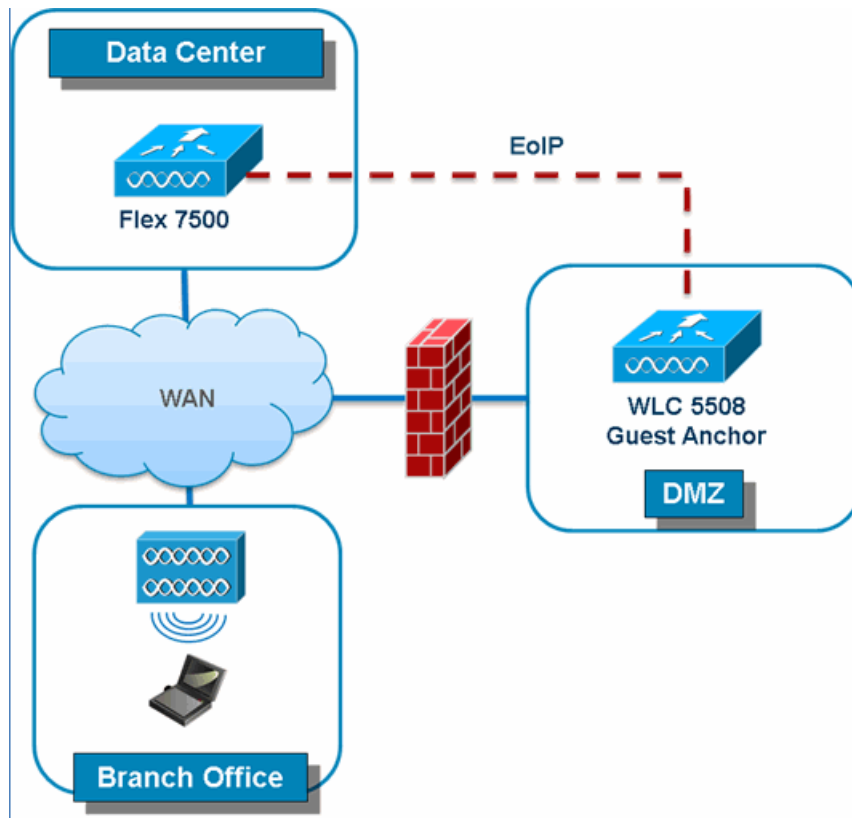
- Software downgrade from release 7.4 to a previous release will retain the configuration but with some limitations.
- Configuring a primary/secondary RADIUS server when a previous one is configured will cause the older entry to be replaced by the new one.

## Enhanced Local Mode (ELM)

ELM is supported on the FlexConnect solution. Refer to the best practices guide on ELM for more information.

## Guest Access Support in Flex 7500

Figure 12 Guest Access Support in Flex 7500



3570540

Flex 7500 will allow and continue to support creation of EoIP tunnel to your guest anchor controller in DMZ. For best practices on the wireless guest access solution, refer to the Guest Deployment Guide.

## Managing WLC 7500 with NCS

The management of the WLC 7500 from NCS is identical to Cisco's existing WLCs.

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

350541

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		7.0.112.6Z	mobility	Reachable	Identical
<input type="checkbox"/>	172.20.227.172	5508-Primary	5500		7.0.112.5Z	mobility	Reachable	Identical

For more information on managing WLC and discovering templates, refer to the [Cisco Wireless Control System Configuration Guide, Release 7.0.172.0](#).

## Managing WLC 7500 with Cisco Prime

The management of the WLC 7500 from Cisco Prime is identical to Cisco's existing WLCs.



The screenshot shows the 'Add Controllers' configuration page in Cisco Prime Infrastructure. The page is titled 'Add Controllers' and has a breadcrumb trail 'Configure > Controllers > Add Controllers'. The page is divided into three main sections: General Parameters, SNMP Parameters, and Telnet/SSH Parameters. In the General Parameters section, the 'Add Format Type' is set to 'Device Info'. The 'IP Addresses' field contains the text 'WLC 7500 IP Address' and is highlighted with a red box. The 'Wism Auto Add' checkbox is unchecked. In the SNMP Parameters section, the 'Version' is set to 'v2c', 'Retries' is '2', and 'SNMP Timeout' is '10'. In the Telnet/SSH Parameters section, the 'Protocol' is set to 'Telnet', 'Username' is 'admin', and 'Telnet Timeout' is '60'. There are 'Add' and 'Cancel' buttons at the bottom left.

## Support for PEAP and EAP-TLS Authentication

FlexConnect AP can be configured as a RADIUS server for LEAP and EAP-FAST client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will do dot1x authentication on the AP itself using the local radius. With controller release 7.5, PEAP and EAP-TLS EAP methods are also supported.

## EAP-TLS

### Certificate Generation for EAP-TLS

The following steps are needed on the WLC and the client in order to authenticate the client to the FlexConnect AP using EAP-TLS authentication.

On WLC:

1. Generate device certificate for the WLC.
2. Get device certificate signed by CA server.
3. Generate CA certificate from the CA server.
4. Import device and CA certificate into the WLC in .pem format.

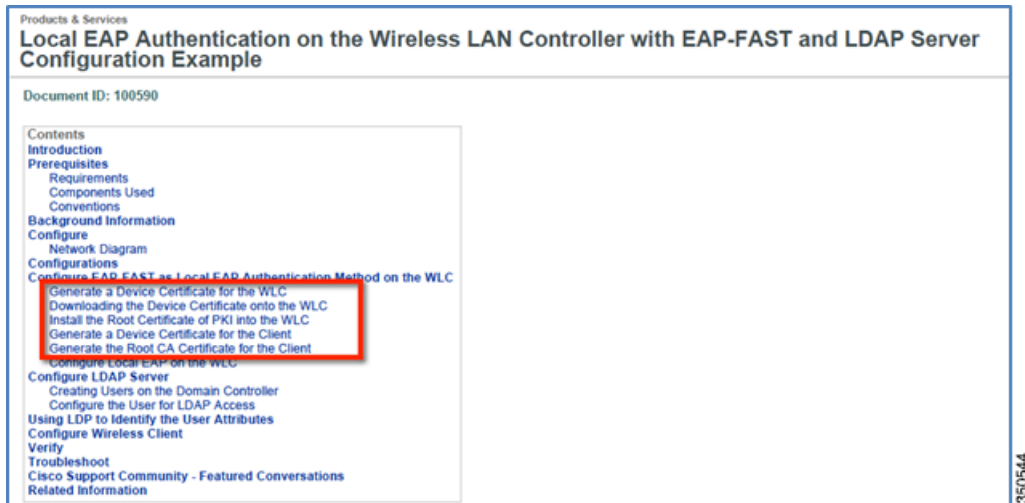
On Client:

1. Generate client certificate.

2. Get client certificate signed by CA server.
3. Generate CA certificate from the CA server.
4. Install client and CA certificate on the client.

Detailed steps on how to accomplish the above steps are listed in Document-100590 ([http://www.cisco.com/en/US/products/ps6366/products\\_configuration\\_example09186a008093f1b9.shtml](http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008093f1b9.shtml))

Figure 13 Document 100590

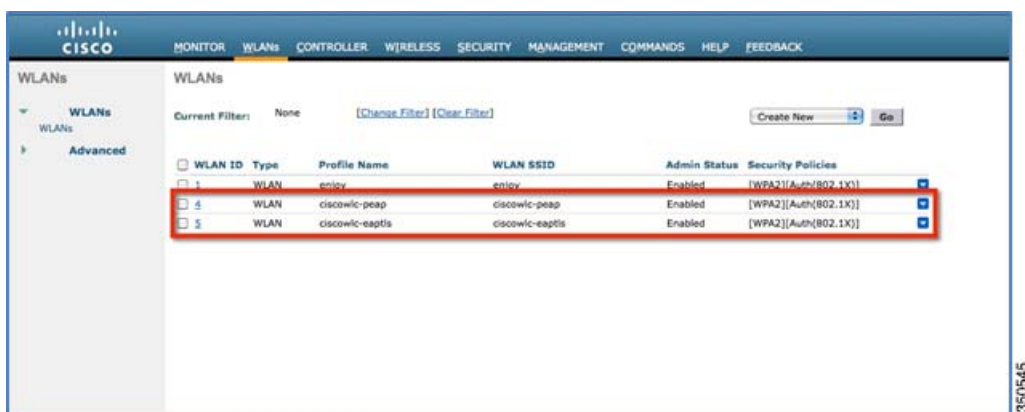


## Configuration of EAP-TLS on FlexConnect AP

1. Create WLAN for Local Switching and Local Authentication.

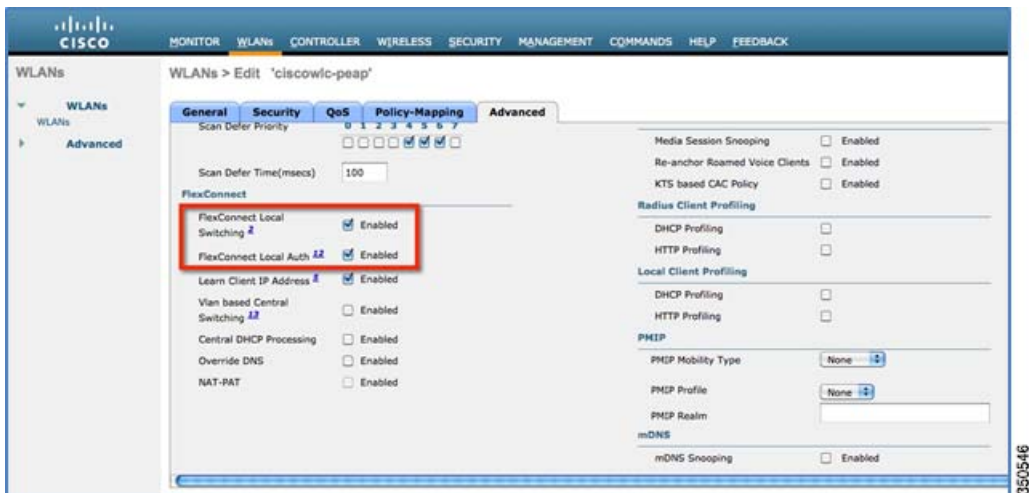
In the example below, two WLANs have been created, one for EAP-TLS and the other for PEAP authentication.

Figure 14 WLAN Configuration for PEAP and EAP-TLS



2. Enable **FlexConnect Local Switching** and **FlexConnect Local Auth**.

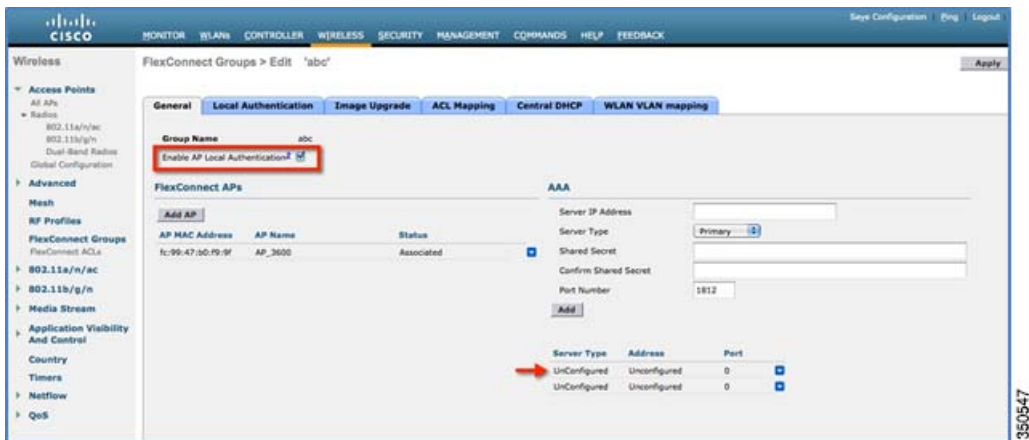
Figure 15 WLANs for Local Switching and Local Authentication



3. Enable AP Local Authentication.

Check the **Enable AP Local Authentication** check box on the FlexConnect Groups edit page. Radius Servers on the FlexConnect Group must be 'Unconfigured'. If any RADIUS servers are configured on the FlexConnect Group, the AP tries to authenticate the wireless clients using the RADIUS servers first. AP Local Authentication is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

Figure 16 FlexConnect Group Configuration for AP Local Authentication



4. Selecting EAP methods will now have two more options, PEAP and EAP-TLS under the FlexConnect Group with the existing LEAP and EAP-FAST options.

- a. Current controller release supports downloading of EAP device and root (CA) certificates to the controller and the same is stored in PEM format on the flash.

Figure 17 Downloading Vendor Device Certificate

The screenshot shows the Cisco Flex 7500 controller web interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar lists various commands: Download File, Upload File, Reboot, Config Boot, Scheduled Reboot, Reset to Factory Default, Set Time, and Login Banner. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type:** Vendor Device Certificate (highlighted with a red box)
- Certificate Password:** \*\*\*\*
- Transfer Mode:** TFTP
- Server Details:**
  - IP Address:** [Empty field]
  - Maximum retries:** 10
  - Timeout (seconds):** 6
  - File Path:** /
  - File Name:** ciscowldev.pem

350548

Figure 18 Downloading Vendor CA Certificate

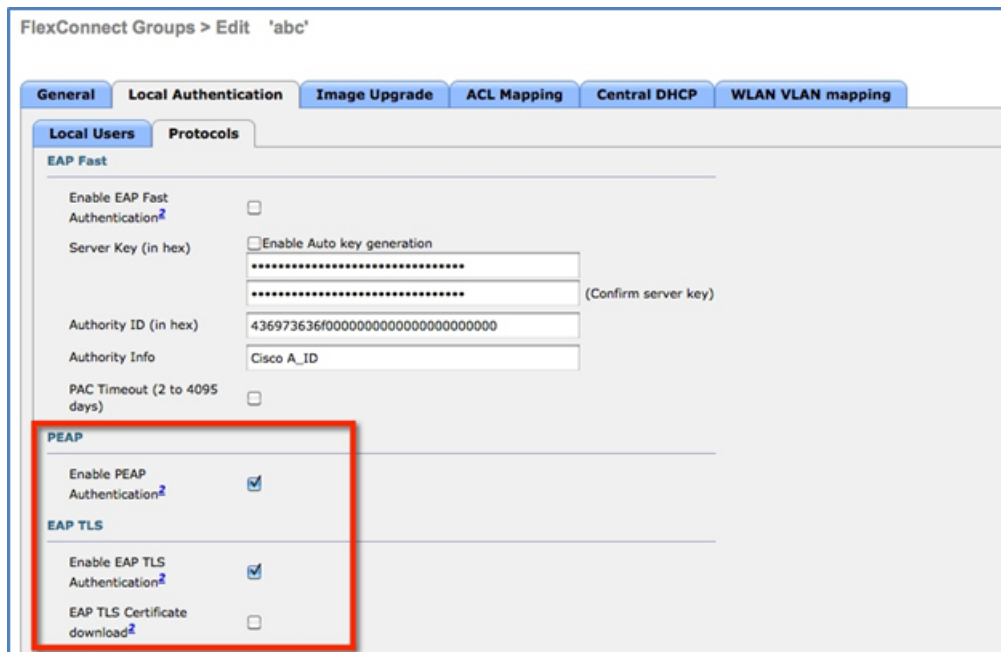
The screenshot shows the Cisco Flex 7500 controller web interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar lists various commands: Download File, Upload File, Reboot, Config Boot, Scheduled Reboot, Reset to Factory Default, Set Time, and Login Banner. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type:** Vendor CA Certificate (highlighted with a red box)
- Transfer Mode:** TFTP
- Server Details:**
  - IP Address:** [Empty field]
  - Maximum retries:** 10
  - Timeout (seconds):** 6
  - File Path:** /
  - File Name:** ciscowlcca.pem

350549

- b. With release 7.5, these certificates will be used for authenticating clients using EAP-TLS. Both the device and root certificates will be downloaded to all the FlexConnect APs in the FlexConnect Group if the EAP-TLS method is enabled, and the same is used at the AP to authenticate the clients.
- c. When a new AP joins the group, certificates will be pushed to the AP along with other configurations. The user has to download the EAP device and Root certificates to controller prior to enabling EAP-TLS on the FlexConnect Group.
- d. Upon receiving a certificate message from the controller, the AP will import these certificates, store them in memory and use them for authenticating clients.
- e. **EAP TLS Certificate Download** option is provided to push any updated certificates to the AP.

**Figure 19 Enabling PEAP and EAP TLS on AP Local Authentication under FlexConnect Group**

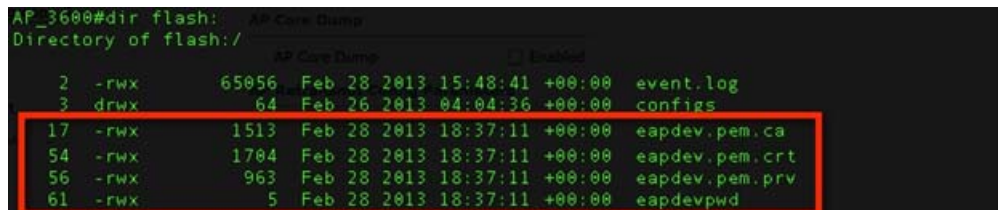


### Certificate Files on AP

Four files are downloaded to the AP, when EAP-TLS is enabled.

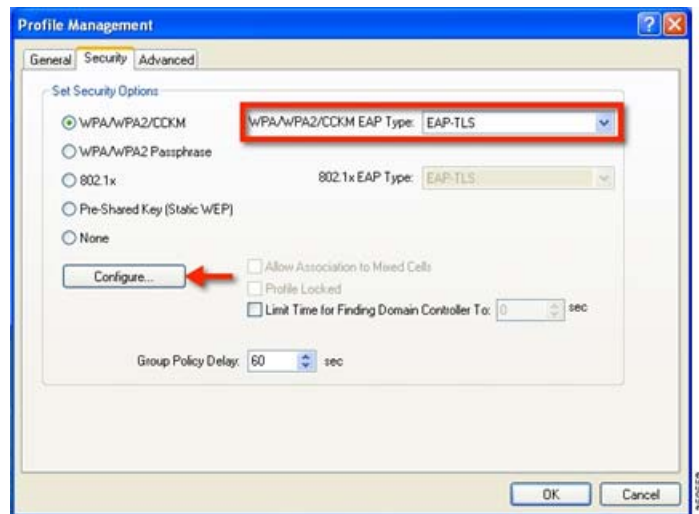
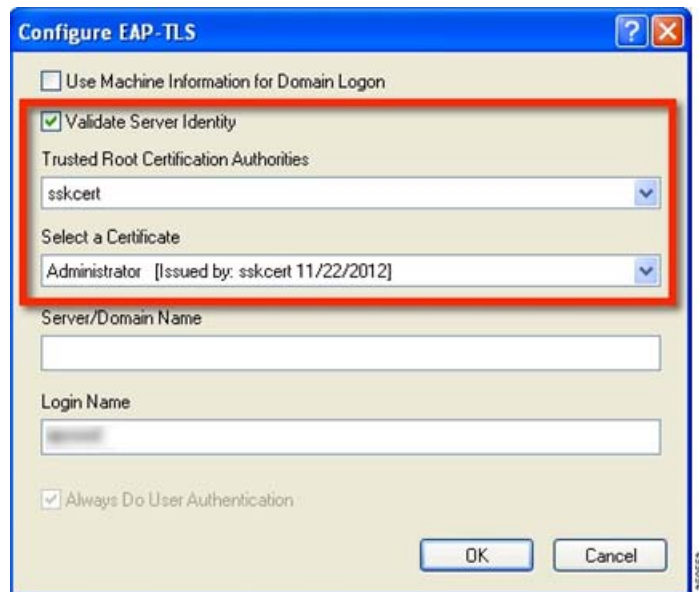
- eapdev.pem.ca - This is the CA (root) certificate.
- eapdev.pem.crt -This is the public certificate of the device.
- eapdev.pem.prv -This is the RSA private key of the device.
- eapdevpwd - This is the password file to protect the private key.

**Figure 20 Files Stored in the Flash on AP**



### Client Configuration

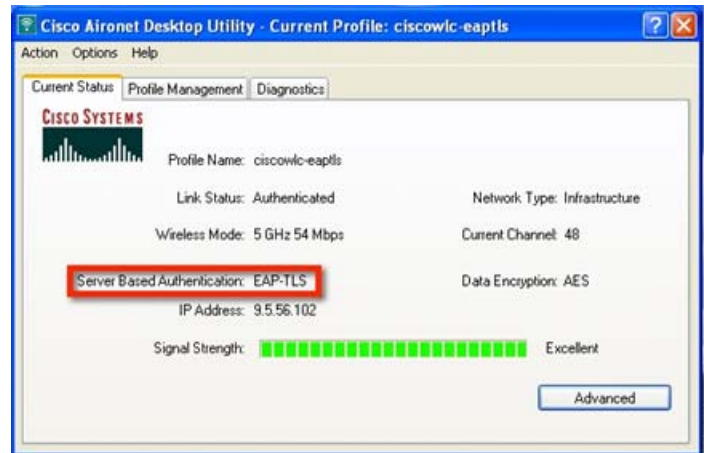
Configure the wireless profile for EAP-TLS by selecting EAP Type **EAP-TLS** and specifying the Trusted Root certificate Authorities and the client certificate.

**Figure 21 Wireless Profile for EAP-TLS****Figure 22 Validate Server Identity**

Once the client is connected, Server Based Authentication will reflect EAP-TLS.



Figure 23 Client Authentication using EAP-TLS



### Client Certificates

The Trusted Root and Client Certificates can be viewed as follows (These are the certificates as generated earlier)

Figure 24 Certificates on Client



Figure 25 Trusted Root (CA) Certificate on Client

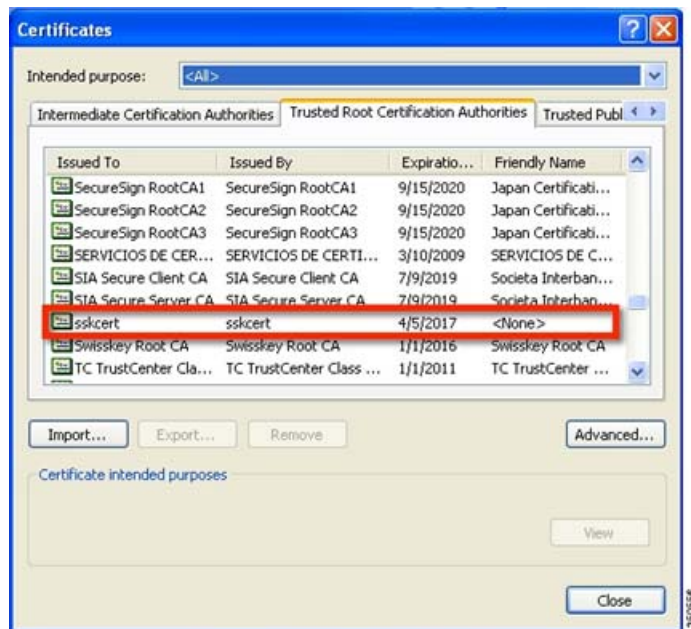
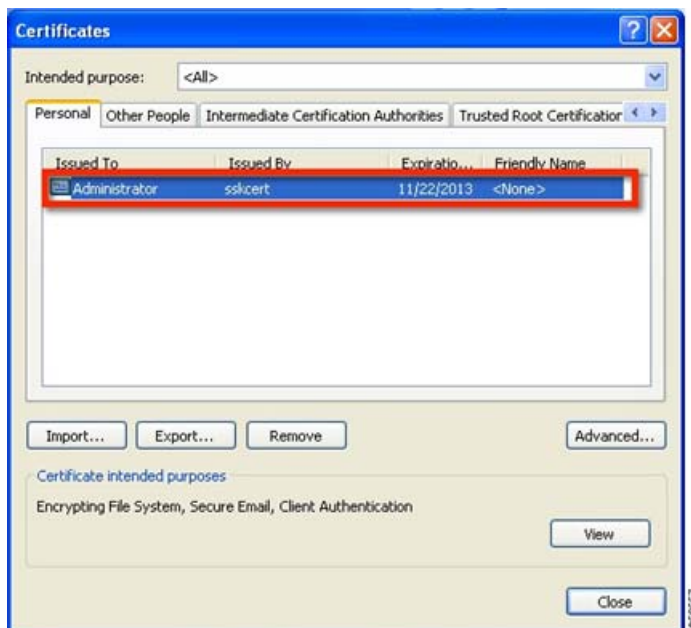


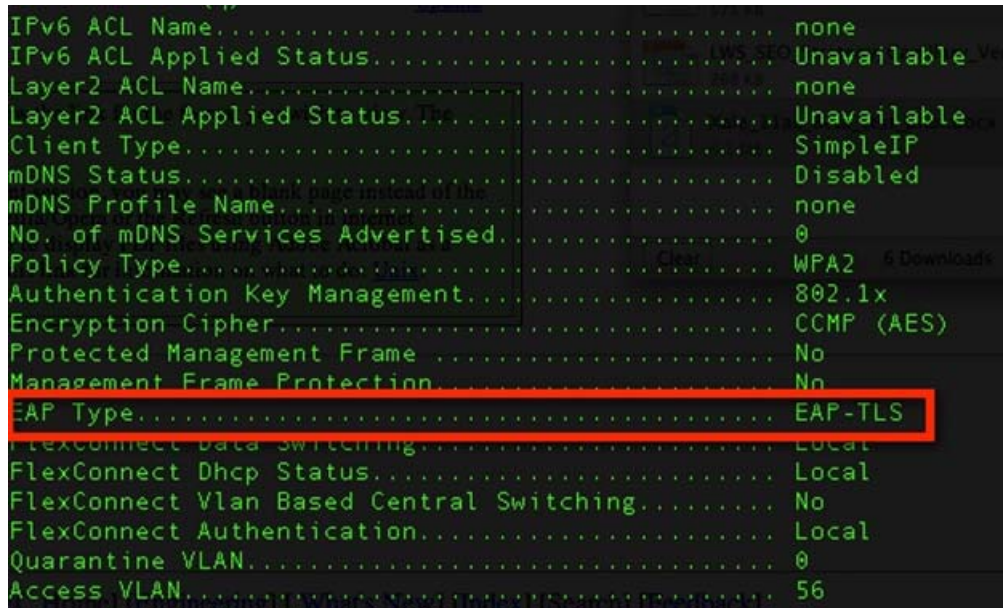
Figure 26 Trusted Client Certificate



## Show Commands

The EAP type of the client will be reflected on the WLC and can be seen in the output of **show client detail**.

Figure 27 EAP Type for Client Authenticated using EAP-TLS

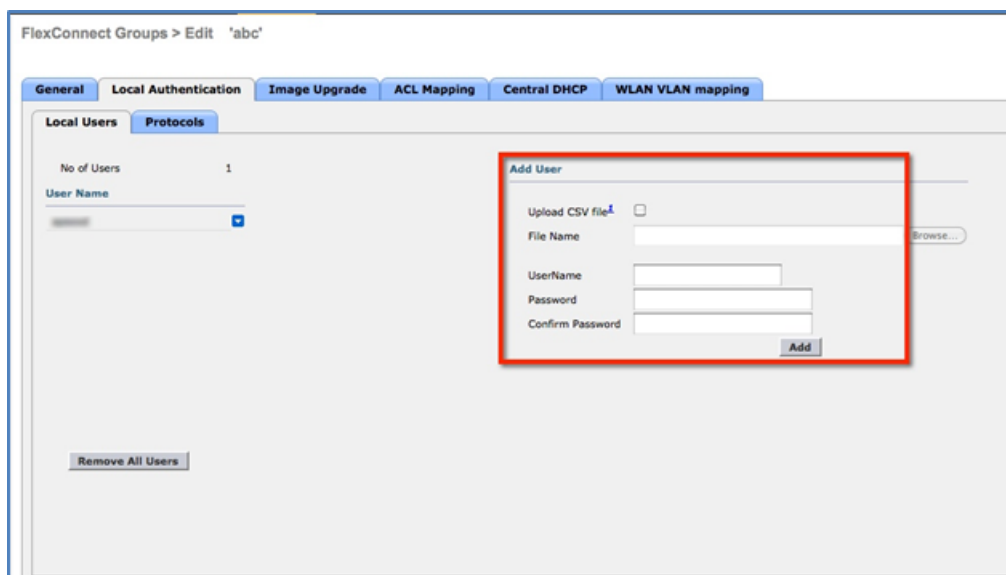


## EAP-PEAP

PEAP (EAP-MSCHAPv2 and EAP-GTC) EAP Type is supported with release 7.5 and Users need to be added on the WLC as shown below. A maximum of 100 users can be added per FlexConnect Group.

## User Creation

Figure 28 User Addition for Local Authentication



## Client Configuration

Selecting EAP Type EAP-MSCHAPv2 or GTC can configure the wireless profile for EAP-PEAP.

**Figure 29 Wireless Profile for EAP-PEAP (EAP-MSCHAPv2)**



Users created on the controller need to be configured on the client.

**Figure 30 User Name and Password for PEAP**

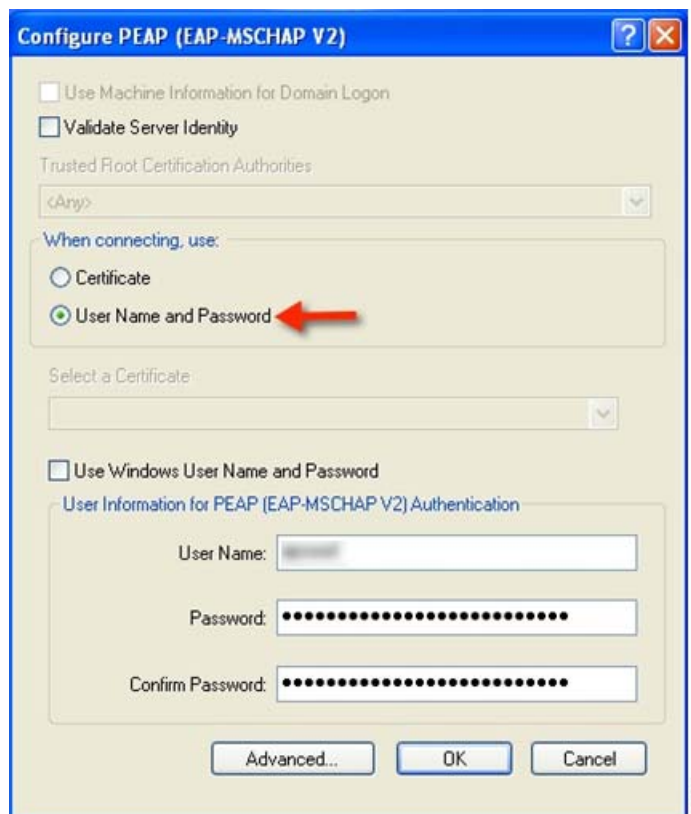
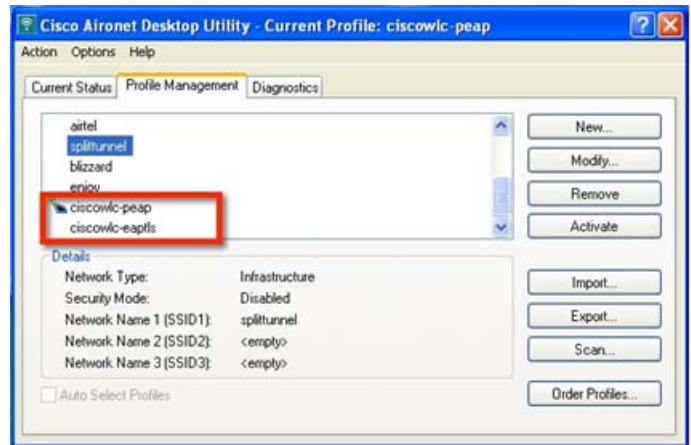
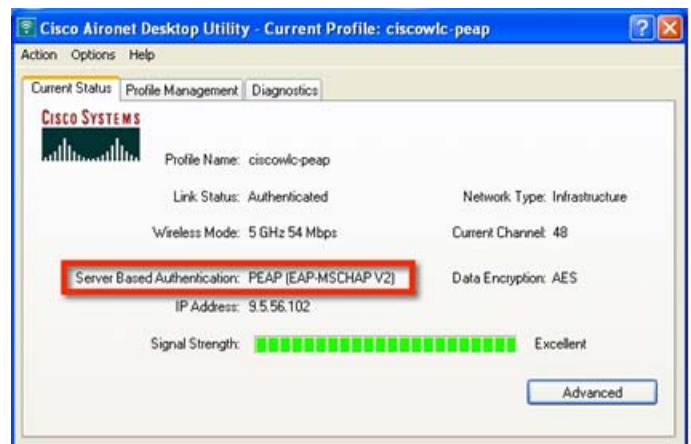


Figure 31 Cisco Aironet Desktop Utility Profile Management



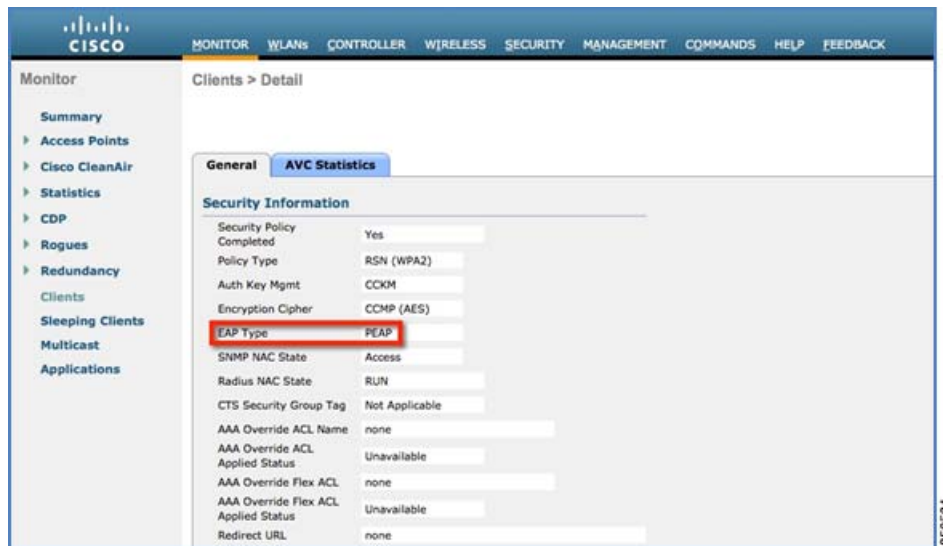
Once the client is connected, Server Based Authentication will reflect PEAP(EAP-MSCHAPv2).

Figure 32 Client Authentication using PEAP(EAP-MSCHAPv2)



Once the client is authenticated, the EAP Type can be seen under the Client Detail page.

Figure 33 Web GUI Client Details



## Show Commands

The EAP type of the client will be reflected on the WLC and can be seen in the output of **show client detail**.

Figure 34 EAP Type of Client Authenticated using PEAP

```

IPv6 ACL Applied Status..... Unavailable
Layer2 ACL Name..... none
Layer2 ACL Applied Status..... Unavailable
Client Type..... SimpleIP
mDNS Status..... Disabled
mDNS Profile Name..... none
No. of mDNS Services Advertised..... 0
Policy Type..... WPA2
Authentication Key Management..... 802.1x
Encryption Cipher..... CCMP (AES)
Protected Management Frame..... No
Management Frame Protection..... No
EAP Type..... PEAP
FlexConnect Data Switching..... Local
FlexConnect Dhcp Status..... Local
FlexConnect Vlan Based Central Switching..... No
FlexConnect Authentication..... Local
Quarantine VLAN..... 0
Access VLAN..... 56

```

## CLI Support for PEAP and EAP-TLS on FlexConnect APs

Two new CLIs have been added to configure PEAP and EAP-TLS from the controller.

```
config flexconnect group <groupName> radius ap peap <enable | disable>
```

```
config flexconnect group <groupName> radius ap eap-tls <enable | disable>
```

A CLI for certificate download has been added as well.

```
config flexconnect group <groupName> radius ap eap-cert download
```



## WLAN-VLAN mapping at FlexConnect Group Level

```

(Cisco Controller) >config flexconnect group abc radius ap peap ?
disable      Disables PEAP authentication
enable      Enables PEAP authentication
(Cisco Controller) >config flexconnect group abc radius ap eap-tls ?
disable      Disables EAP-TLS authentication
enable      Enables EAP-TLS authentication
(Cisco Controller) >config flexconnect group abc radius ap eap-cert ?
download     download eap Root and Device certificate to AP
(Cisco Controller) >config flexconnect group abc radius ap eap-cert download

```

Configurations at the AP can be seen from the console.

**Figure 35 CLI Commands on AP Console**

```

AP-368R#show running-config brief | s eap
aaa local authentication reap_eap_methods authorization reap_eap_methods
aaa authentication dot1x reap_eap_methods group radius local
aaa authorization network reap_eap_methods local
aaa authorization credential-download reap_eap_methods local
dot1x ssid ciscowlc-eap-tls 3
dot1x ssid ciscowlc-peap 4
eap_profile lwapp_eap_profile
method tls
method peap

```

The following commands can be used to troubleshoot this feature:

```

debug eap all
debug aaa authentication
debug dot11 aaa authenticator all
debug aaa api
debug aaa subsystem
debug dot11 aaa dispatcher
debug aaa protocol local
debug radius
debug aaa dead-criteria transaction

```

## Guidelines

- FlexConnect AP should be in standalone mode or configured for Local authentication.
- Certificates must be present on the AP for EAP-TLS to work.

## WLAN-VLAN mapping at FlexConnect Group Level

Prior to release 7.5, WLAN to VLAN mapping was done on a per AP basis.

With increasing number of APs in a deployment, there is a need to provide the capability of adding WLAN to VLAN maps from the FlexConnect Group. This will be supported in release 7.5.

## WLAN-VLAN mapping at FlexConnect Group Level

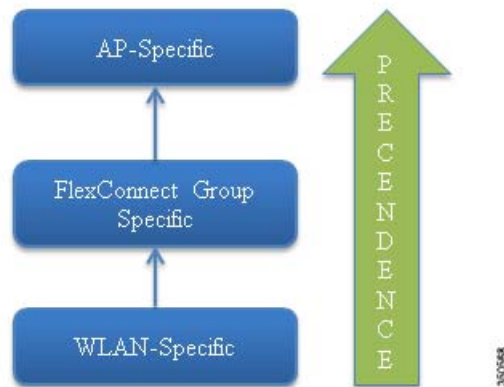
This will push the WLAN to VLAN mapping to all the APs present in the FlexConnect Group. The FlexConnect level configuration will have a higher precedence compared to the WLAN-VLAN mapping configured on the WLAN.

## WLAN-VLAN Mapping Inheritance

- WLAN level WLAN-VLAN mapping has the lowest precedence.
- Higher precedence mapping will override the mapping of lower precedence
- AP level WLAN-VLAN mapping has the highest precedence
- On deletion of a higher precedence mapping, the next highest precedence mapping will take effect.

The following figure depicts the order of precedence as it refers to WLAN-VLAN mapping at the WLAN, FlexConnect Group and at the AP.

**Figure 36 Flow of Inheritance**



## GUI Configuration

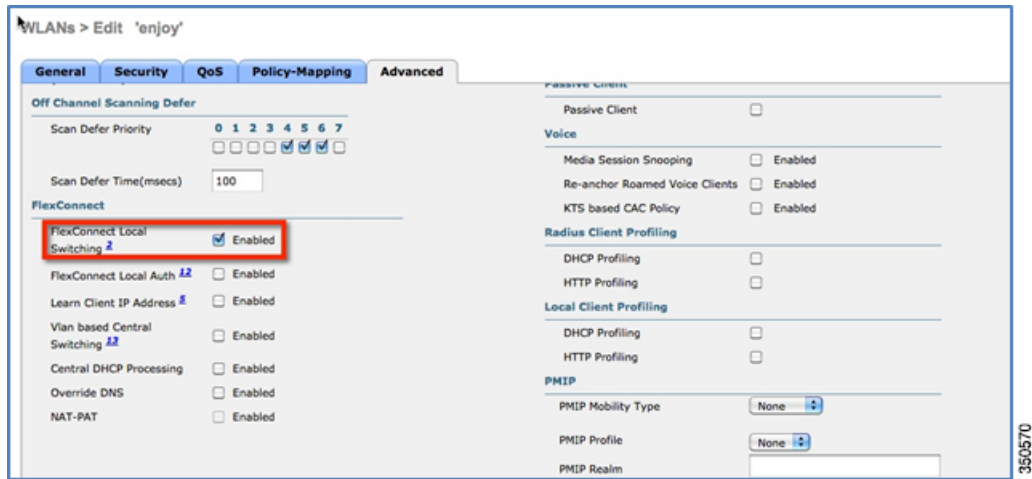
1. Create WLAN for Local Switching

**Figure 37 WLAN for Local Switching**

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	ciscover-peap	ciscover-peap	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	ciscover-eaptls	ciscover-eaptls	Enabled	[WPA2][Auth(802.1X)]

WLAN-VLAN mapping at FlexConnect Group Level

Figure 38 FlexConnect Local Switching



The WLAN is mapped to the management VLAN 56.

Figure 39 WLAN Mapped to VLAN 56 Management Interface

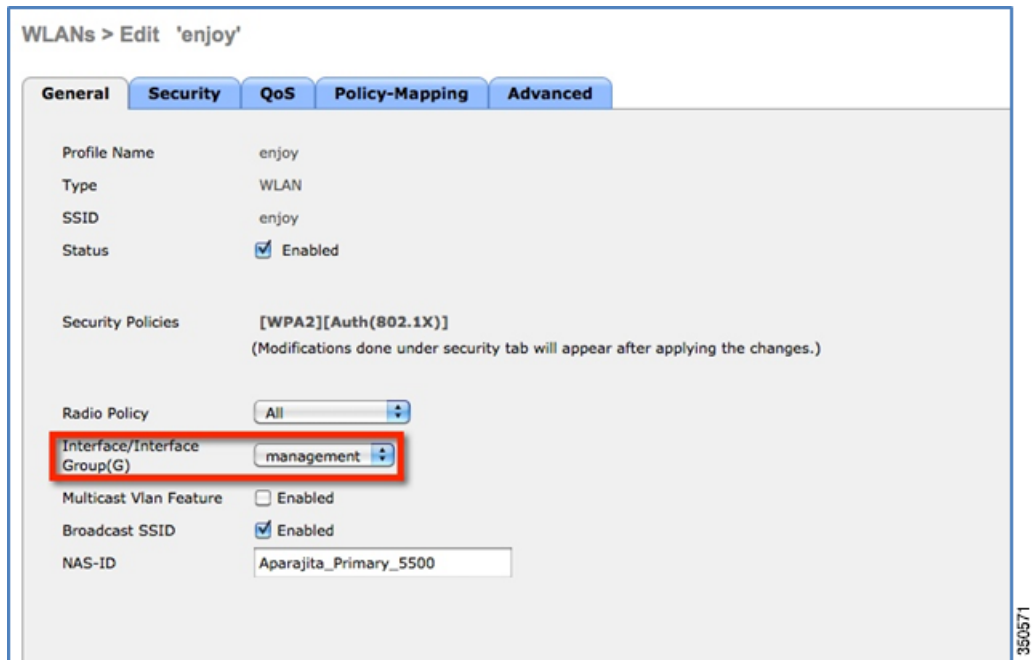
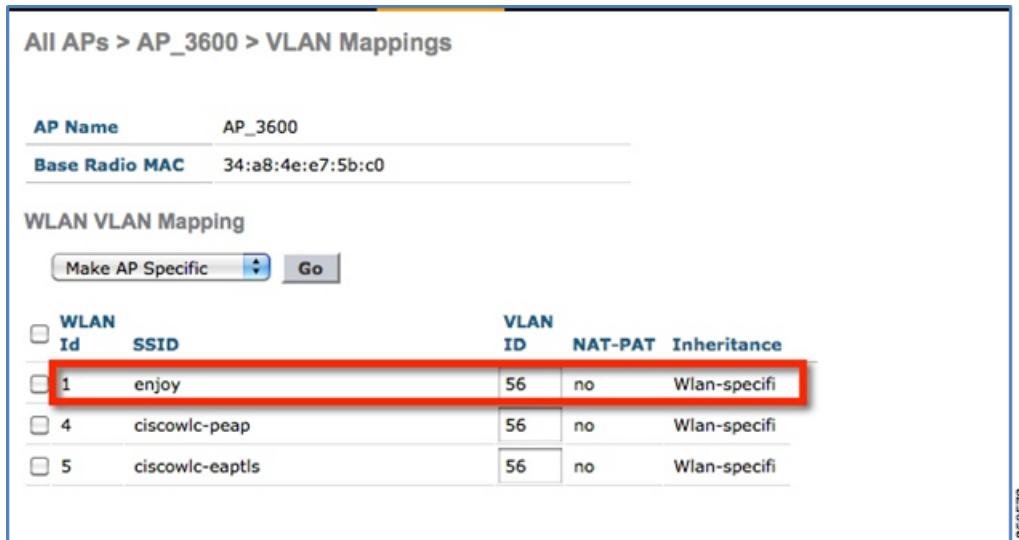


Figure 40 WLAN Mapped to VLAN 56 as Per WLAN-Specific Mapping



All APs > AP\_3600 > VLAN Mappings

AP Name AP\_3600

Base Radio MAC 34:a8:4e:e7:5b:c0

WLAN VLAN Mapping

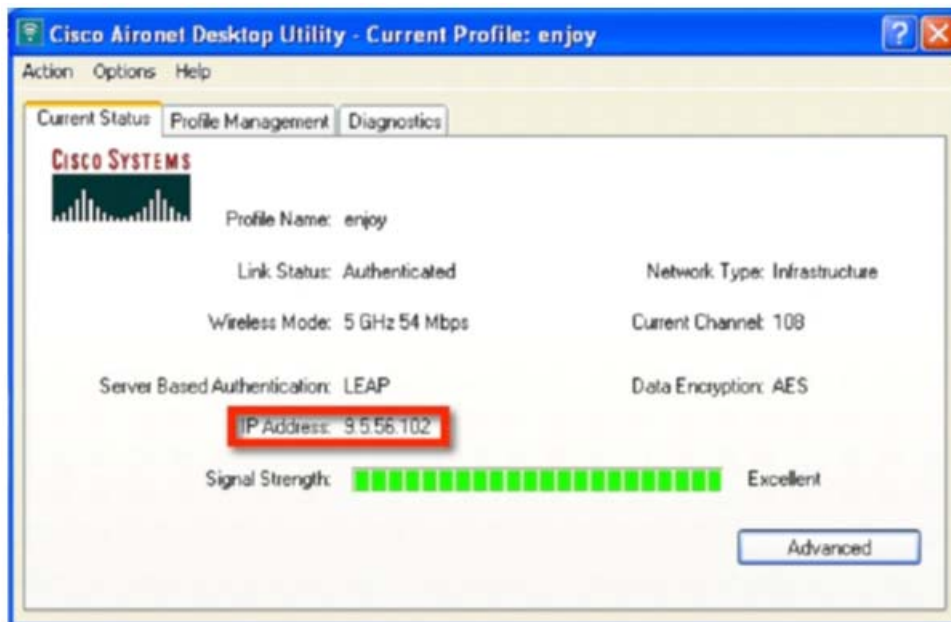
Make AP Specific Go

WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
1	enjoy	56	no	Wlan-specifi
4	ciscowlc-peap	56	no	Wlan-specifi
5	ciscowlc-eaptls	56	no	Wlan-specifi

350572

When a client connects to this WLAN, it will get an IP in VLAN 56.

Figure 41 Client in VLAN 56



Cisco Aironet Desktop Utility - Current Profile: enjoy

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

Profile Name: enjoy

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 108

Server Based Authentication: LEAP Data Encryption: AES

IP Address: 95.56.102

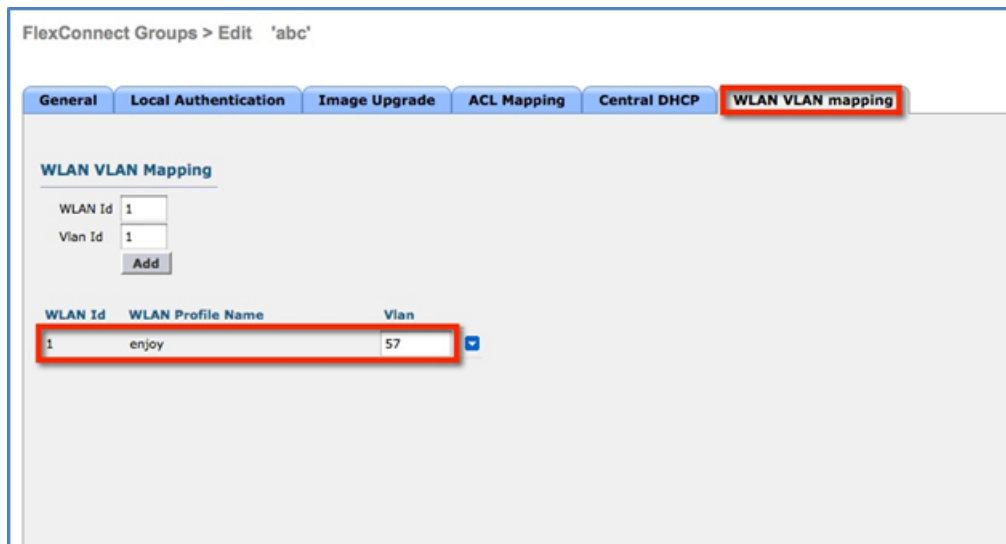
Signal Strength: Excellent

Advanced

2. Create WLAN-VLAN mapping under FlexConnect Groups. This capability is the new feature in release 7.5.

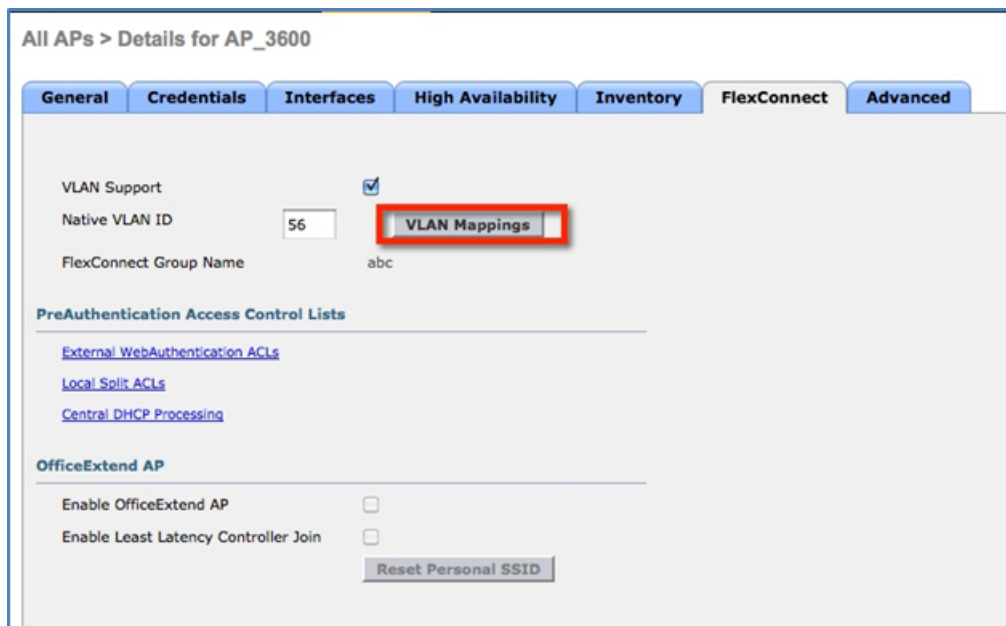
WLAN-VLAN mapping at FlexConnect Group Level

Figure 42 WLAN Mapped to VLAN 57 under FlexConnect Group



WLAN-VLAN mappings can be viewed per AP from the VLAN Mappings page.

Figure 43 VLAN Mappings at AP



In this example, the WLAN is mapped to VLAN 57 on the FlexConnect Group, since the Group-specific mappings take precedence over WLAN-specific mappings.

**Figure 44** WLAN 1 Mapped to VLAN 57 as Per Group-Specific Configuration Inheritance

All APs > AP\_3600 > VLAN Mappings

AP Name: AP\_3600  
Base Radio MAC: 34:a8:4e:e7:5b:c0

WLAN VLAN Mapping

Make AP Specific [Go]

WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
<input type="checkbox"/> 1	enjoy	57	no	Group-speci
<input type="checkbox"/> 4	ciscowlc-peap	56	no	Wlan-specifi
<input type="checkbox"/> 5	ciscowlc-eaptls	56	no	Wlan-specifi

350576

The client is assigned an IP address in VLAN 57.

**Figure 45** Client in VLAN 57

Cisco Aironet Desktop Utility - Current Profile: enjoy

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

Profile Name: enjoy

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 108

Server Based Authentication: LEAP Data Encryption: AES

IP Address: 9.5.57.100

Signal Strength: [Signal strength bar] Excellent

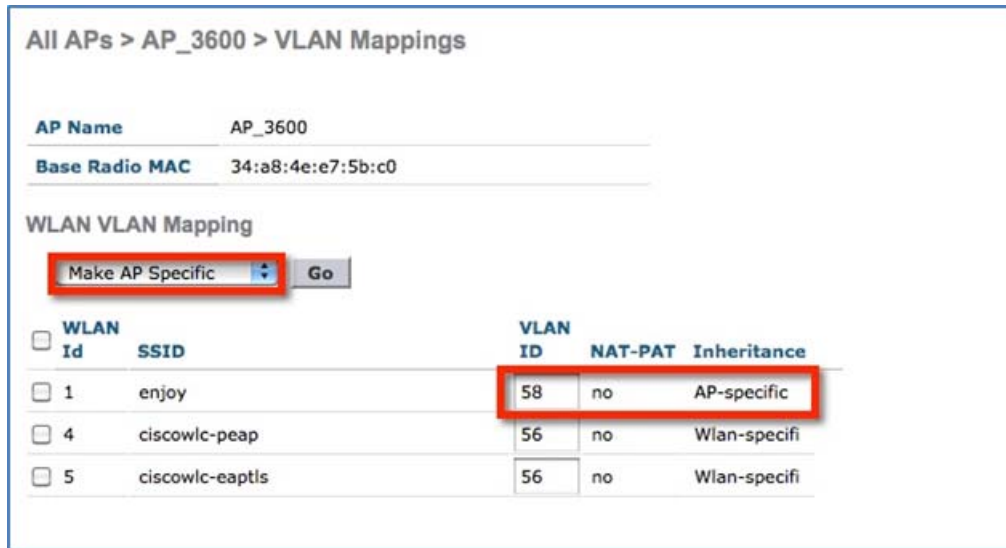
Advanced

3. To create a WLAN-VLAN mapping at the AP, select **Make AP Specific** under **VLAN Mappings**.

Once this is done, the WLAN is mapped to VLAN 58 since AP-specific mappings take precedence over Group-specific and WLAN-specific mappings.

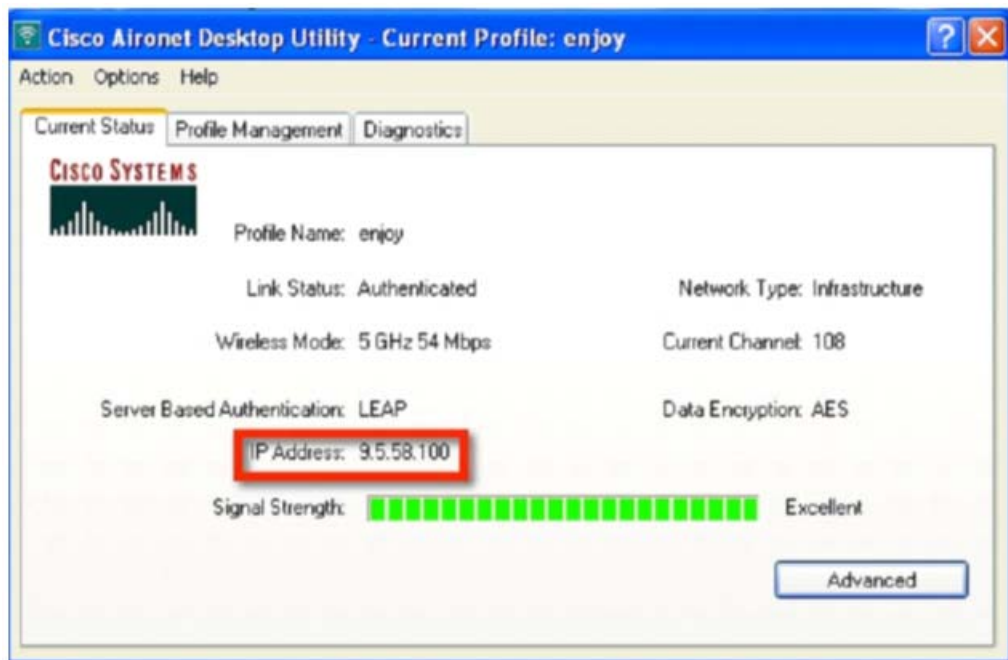


Figure 46 WLAN Mapped to VLAN 58 as Per AP-Specific Mapping Inheritance



The client is assigned an IP address in VLAN 58.

Figure 47 Client in VLAN 58



## CLI Configuration

The following CLIs have been added as part of this feature:

- `config flexconnect group <group> wlan-vlan wlan <wlan-id> add vlan <vlan-id>`

## WLAN-VLAN mapping at FlexConnect Group Level

- `config flexconnect group <group> wlan-vlan wlan <wlan-id> delete`
- `config ap flexconnect vlan remove wlan <wlan_id> <ap_name>`

Figure 48 WLAN-VLAN Configuration at FlexConnect Group from CLI

```
(Cisco Controller) >config flexconnect group abc wlan-vlan wlan 1 ?
add          Add Wlan-Vlan mapping on the wlanId at flexgroup level
delete       Delete Wlan-Vlan mapping for the wlanId at flexgroup level
(Cisco Controller) >config flexconnect group abc wlan-vlan wlan 1 add ?
vlan         Config Vlan for the Wlan-Vlan mapping for wlanId at flexconnect group level
(Cisco Controller) >config flexconnect group abc wlan-vlan wlan 1 add vlan ?
<Vlan ID>    Config vlanId for the wlan-vlan mapping for wlanId at flexGroup
```

The command `show flexconnect group detail` can be used to see the WLAN-VLAN mapping for the FlexConnect Group

Figure 49 `show flexconnect group detail` Output

```
(Cisco Controller) >show flexconnect group detail abc
Number of AP's in Group: 1
fc:99:47:b0:f9:9f AP_3600
Efficient AP Image Upgrade ..... Disabled
Master-AP-Mac      Master-AP-Name
Group Radius Servers Settings:
Type              Server Address      Port
-----
Primary          Unconfigured        Unconfigured
Secondary        Unconfigured        Unconfigured
Group Radius AP Settings:
AP RADIUS server..... Enabled
EAP-FAST Auth..... Disabled
LEAP Auth..... Enabled
EAP-TLS Auth..... Enabled
EAP-TLS CERT Download..... Enabled
PEAP Auth..... Enabled
--More-- or (q)uit
Server Key Auto Generated... No
Server Key..... <hidden>
Authority ID..... 436973636f0000000000000000000000
Authority Info..... Cisco_A_ID
PAC Timeout..... 0
Multicast on Overridden interface config: Disabled
Number of User's in Group: 1
Group-Specific FlexConnect Wlan-Vlan Mapping:
WLAN ID      Vlan ID
-----
1            57
WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat
```

The command `show ap config general <AP name>` can be used to view the WLAN-VLAN mappings per AP.

**Figure 50** show ap config general Output

```

FlexConnect Vlan mode :..... Enabled
Native ID :..... 56
WLAN 1 :..... 57 (Group-Specific)
WLAN 4 :..... 56 (Wlan-Specific)
WLAN 5 :..... 56 (Wlan-Specific)
FlexConnect VLAN ACL Mappings
FlexConnect Group..... abc 56 (Group-Specific)
Group VLAN ACL Mappings
                    56 (Group-Specific)
                    56 (Group-Specific)
AP-Specific FlexConnect Policy ACLs :
L2Acl Configuration ..... Not Available
FlexConnect Local-Split ACLs :
                    57 (Wlan-Specific)

```

WLAN ID	PROFILE NAME	ACL	TYPE
57			Group-Specific
56			Wlan-Specific
56			Wlan-Specific

```

Flexconnect Central-Dhcp Values :

```

The following commands can be used to troubleshoot this feature:

On WLC:

- `debug flexconnect wlan-vlan <enable | disable>`

On AP:

- `debug capwap flexconnect wlan-vlan`

## Guidelines

- The WLAN should be locally switched.
- The configuration will be pushed to the AP only if the WLAN is broadcasted on that AP.

## VLAN Name Override for FlexConnect

This section provides information about the VLAN Name Override feature for FlexConnect introduced in release 8.1. This section also explains the functionality and configuration, and provides deployment scenario examples of the new feature on the FlexConnect APs and the controller.

## Dynamic VLAN Assignment with RADIUS Server

In most WLAN systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID), or WLAN in the controller terminology. Although powerful, this method has limitations, because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco WLAN solution supports identity networking. This allows the network to advertise a single SSID, but allows specific users to inherit different QoS or security policies based on the user credential.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. A RADIUS authentication server, such as CiscoSecure ACS or ISE, handles this task of assigning users to a specific VLAN.

Dynamic VLAN Assignment is possible with FlexConnect branch deployments based on VLAN ID or VLAN Name for central switching and based on VLAN ID only, for local switching WLANs prior to this release. This release introduces the feature that allows VLAN Name Override for FlexConnect Local Switching WLANs as well.

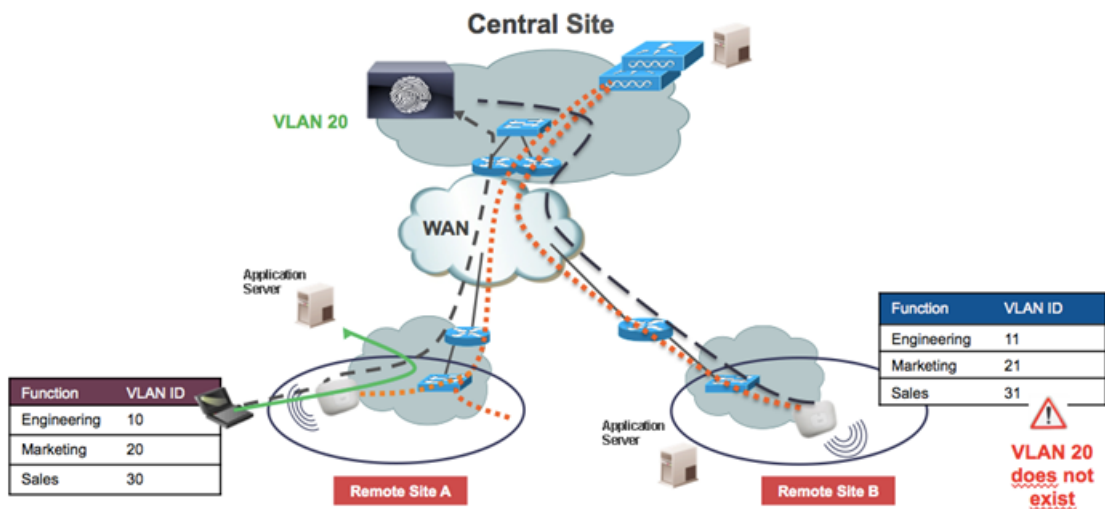
## VLAN Name Override Overview

The VLAN Name Override feature is useful in deployments that have a single central radius authenticating multiple branches. With hundreds of different branches, it becomes very difficult to standardize VLAN IDs across all sites and requires a configuration that provides a unique VLAN Name mapped locally to a VLAN ID that can be different across different branch locations.

This design involving different VLAN IDs across different sites is also useful from the sizing and scaling perspective to limit the number of clients per Layer 2 broadcast domain.

## Use Case Definition

To explain further the use case that this feature addresses, consider the following example.



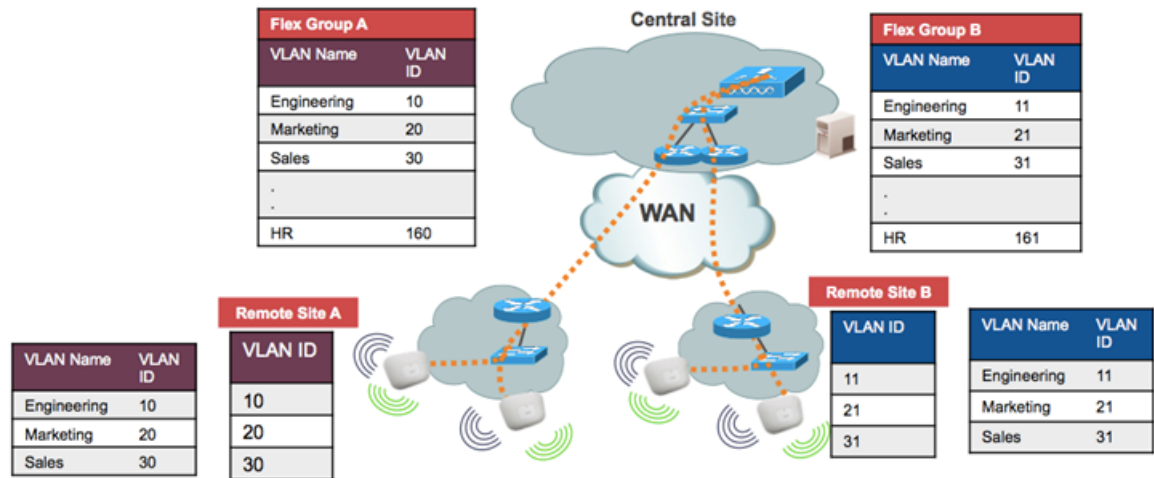
Remote Site A has three categories of users in the departments such as Engineering, Marketing, and Sales that need to be mapped to different VLAN IDs. Engineering needs to be mapped to VLAN ID 10, marketing to 20, and Sales to 30. Similarly, on Remote Site B, the same category of users needs to be mapped to VLAN ID 11, 21, and 31 respectively. All client authentications happen centrally with the RADIUS server shared across all sites. Using AAA Override of VLAN ID does not satisfy the requirement since a different set of VLAN IDs are present in each branch. For example, the RADIUS server is configured to return VLAN ID 20 for marketing. When a marketing employee authenticates in Remote Site B, VLAN 20 is not present in that branch and the user will be defaulted to the WLAN mapped VLAN ID for the FlexConnect Group at that branch, thus breaking the requirement.

## VLAN Mapping Design

VLAN Name to VLAN ID mappings allow the VLAN ID details to be abstracted out in the form of VLAN Name templates that are applied to FlexConnect Groups. Each VLAN Name template contains up to 16 VLAN Name to VLAN ID mappings. VLAN Name to ID mappings are pushed to the FlexConnect APs that are part of the FlexConnect Group, as long as the corresponding VLAN ID is present on the FlexConnect Group, via a WLAN-VLAN or VLAN-ACL Mapping. Multiple VLAN Names mapped to a single VLAN ID is possible, and the VLAN Name can have a maximum of 32 ASCII characters.

In the example considered in this section, VLAN Name to VLAN ID mapping template 'Remote Site A' is created and applied to FlexConnect Group A. Similarly, VLAN Name to VLAN ID mapping template 'Remote Site B' is created and applied to FlexConnect Group B. The mapping is pushed to the individual APs that are part of the FlexConnect Group.

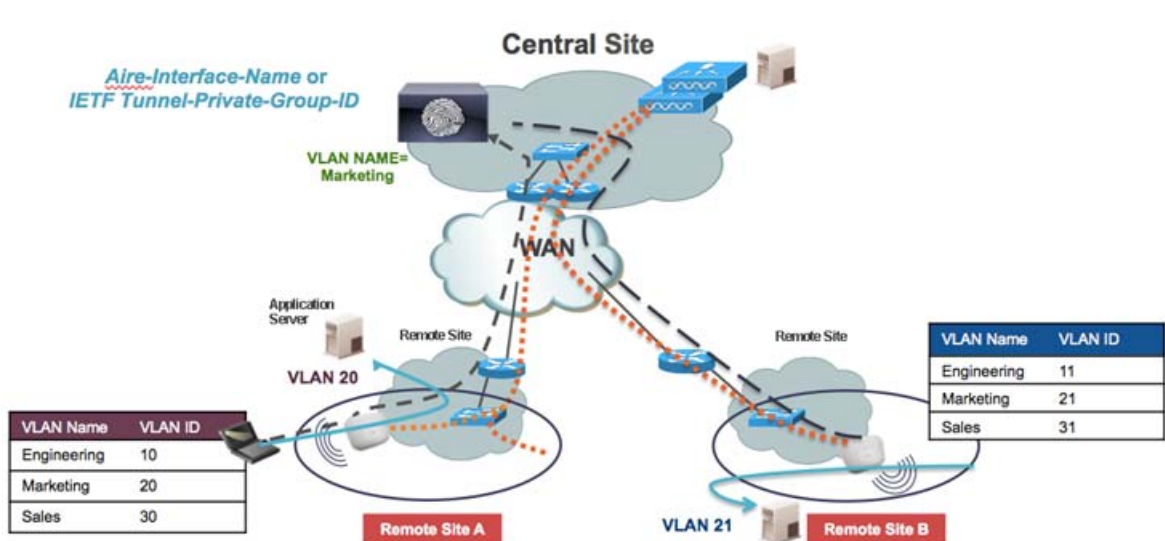
VLAN Name Override for FlexConnect



Solution – AAA Override of VLAN Name

The RADIUS Server is configured with the Airespace Attributes Aire-Interface-Name or IETF Attribute Tunnel-Private-Group-ID to return a VLAN Name, instead of a VLAN ID.

For example, when VLAN Name “marketing” is returned to an AP in Remote Site A, a VLAN Name to VLAN ID mapping lookup is done and the client is assigned to the corresponding VLAN ID. In Remote Site A, the client is assigned VLAN ID 20, and in Remote Site B, the client is assigned VLAN ID 21 as shown in the following figure.



The benefit of using this approach is that the RADIUS Server only needs to be aware of the user function and logical categorization of that user, and can be kept independent of the specifics of VLAN design within the branch itself.

- This feature supports both Central and Local Authentication with local switching VLANs.
- If the AAA server returns multiple VLAN attributes, preference is given to the VLAN Name attribute.

## VLAN Name Override for FlexConnect

- In the event that Aire-Interface-Name and Tunnel-Private-Group-ID are both returned, the Tunnel-Private-Group-ID attribute is given preference.
- If AAA server returns an unknown VLAN name attribute, the client is defaulted to the WLAN-VLAN ID mapping present on the AP.
- This feature is also supported in the standalone mode.

## Feature Configuration

This section provides step-by-step information on how to configure the features described in the following section.

### Configuring Features

To configure the features, perform these steps:

1. From the controller GUI, choose **WLANs > New** to create a new WLAN. The **New WLANs** window is displayed. Enter the WLAN ID and WLAN SSID information. You can enter any name to be the WLAN SSID. Click **Apply** to go to the **Edit** window of the WLAN.
2. Configure the WLAN for WPA2 Layer 2 Security and AAA Server information. It is the job of the RADIUS server to assign a wireless client to a specific VLAN Name upon successful authentication.

The screenshot shows the 'WLANs > Edit 'jk-aaa-ca'' configuration window. The 'AAA Servers' tab is selected, showing options for Radius Servers, Authentication Servers, Accounting Servers, EAP Parameters, Radius Server Accounting, and LDAP Servers.

**WLANs > Edit 'jk-aaa-ca'**

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

**Radius Servers**

Radius Server Overwrite interface  Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

Server 1 IP: 9.1.0.101, Port: 1812

**Radius Server Accounting**

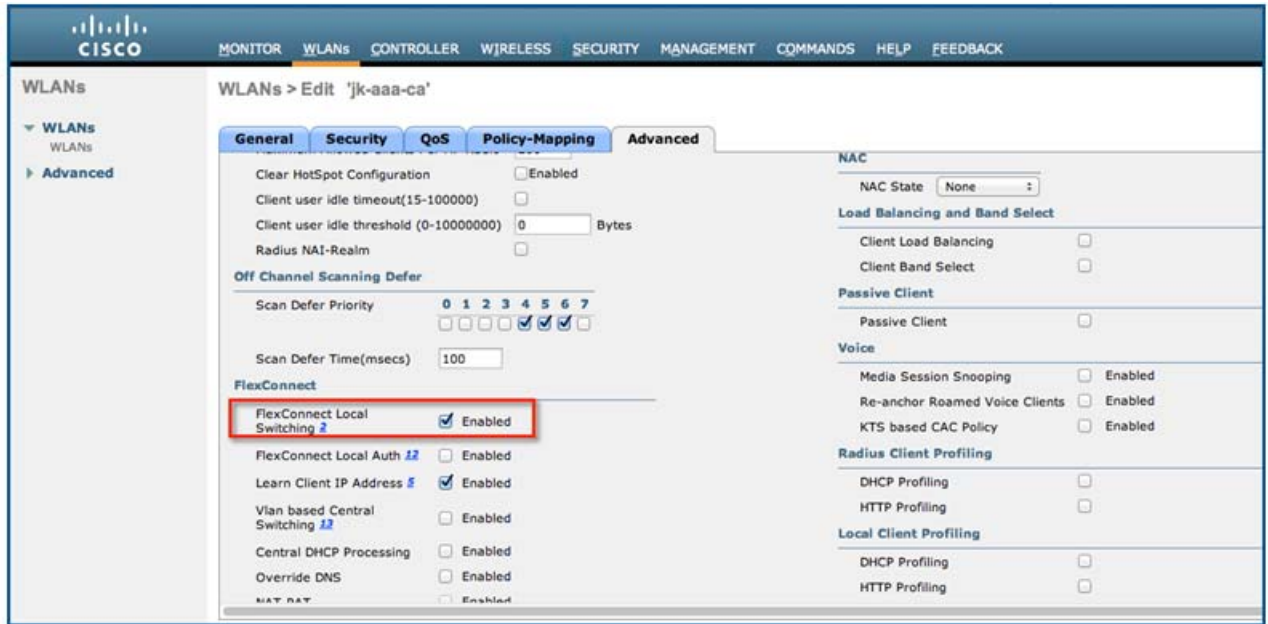
Interim Update

**LDAP Servers**

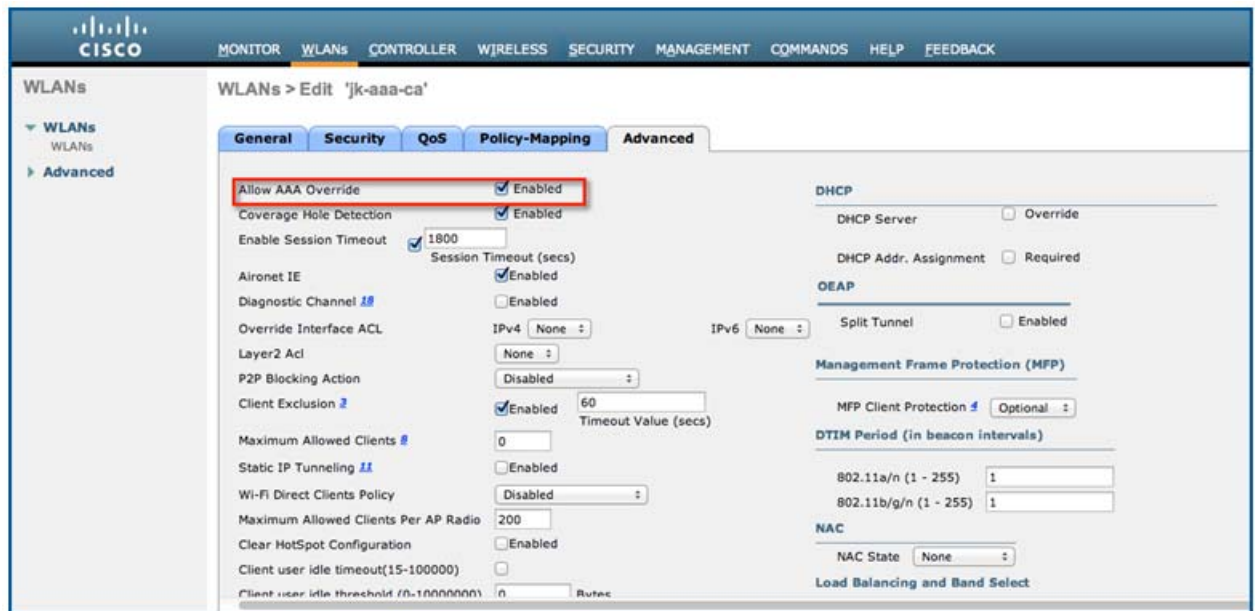
3. Configure the WLAN for **FlexConnect Local Switching** in the **Advanced** tab.



VLAN Name Override for FlexConnect

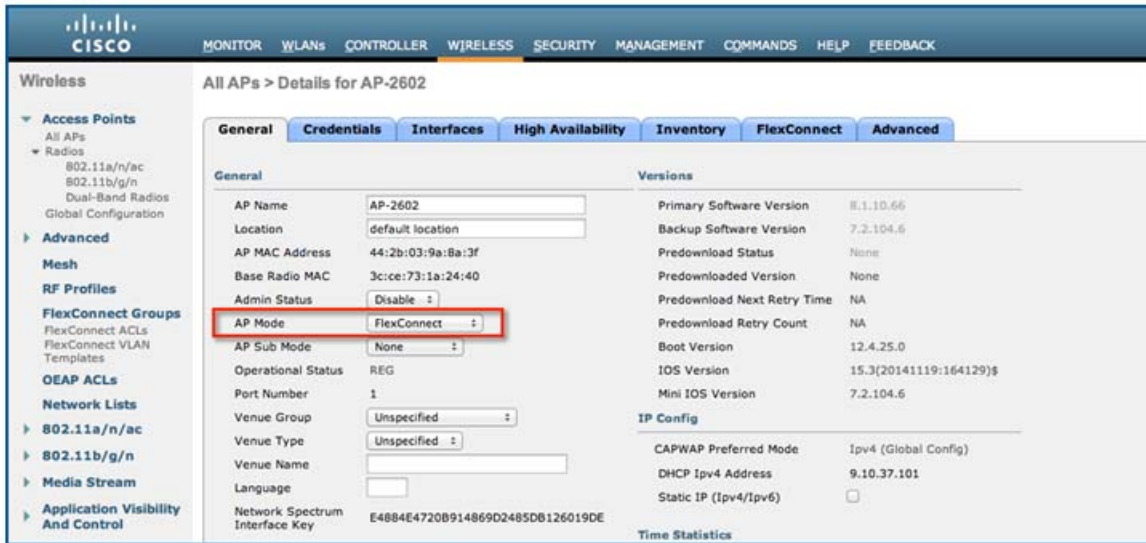
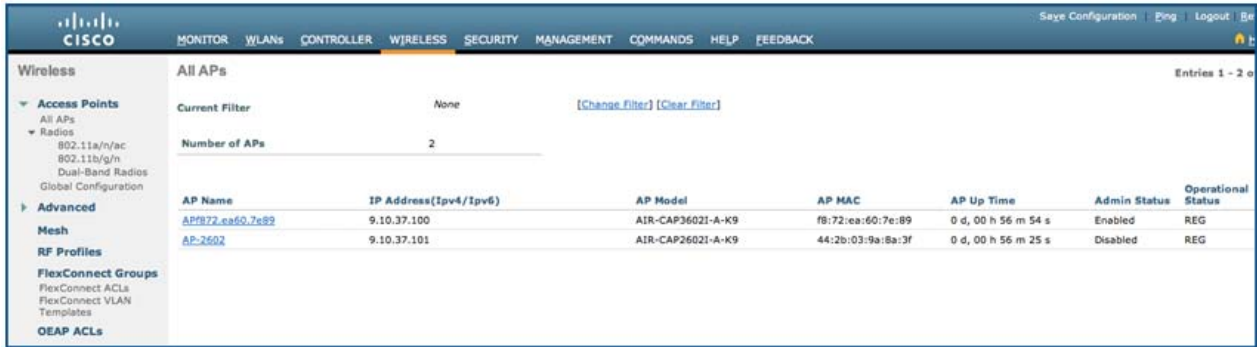


4. Check the **Allow AAA Override** check box to override the WLC and FlexConnect Group configurations by the RADIUS server.

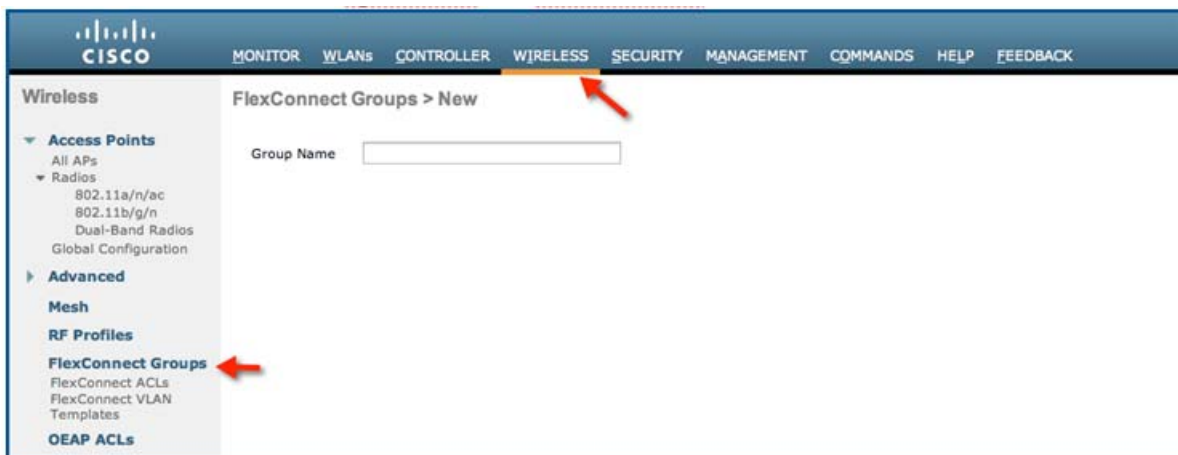


5. Click **Apply**.
6. Connect two access points to the WLC and convert them to FlexConnect mode.

VLAN Name Override for FlexConnect



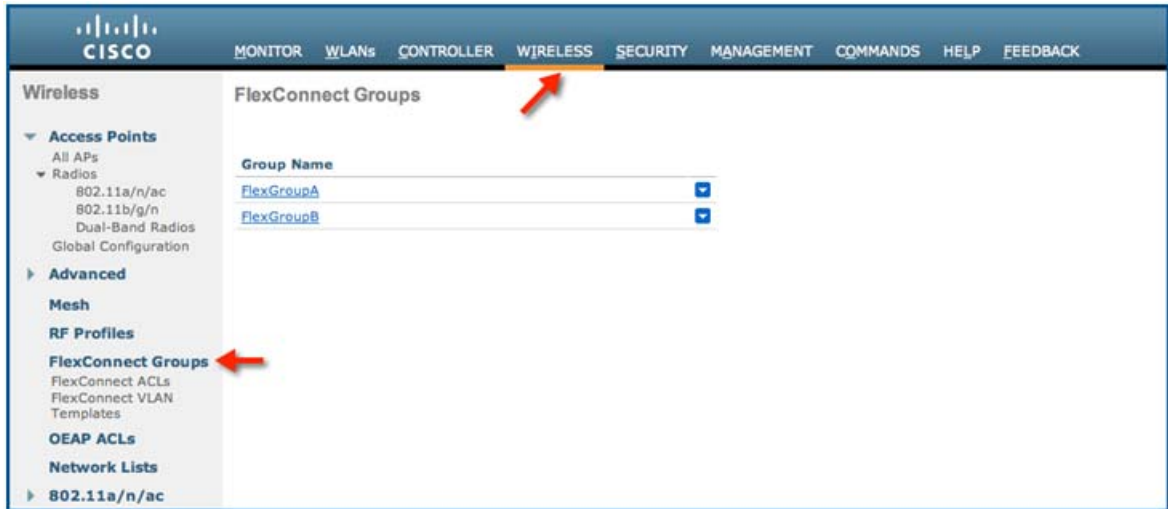
7. Create two FlexConnect Groups under **Wireless > FlexConnect Groups > New**.



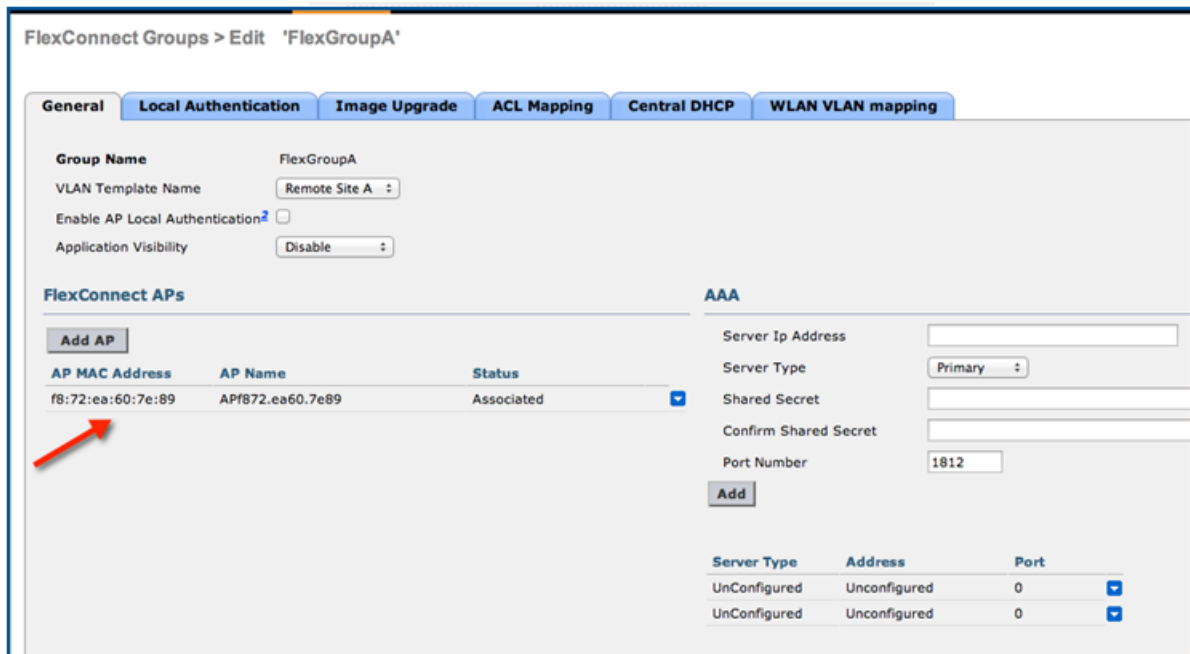
8. Click **Apply**.

VLAN Name Override for FlexConnect

In this example, **FlexGroupA** and **FlexGroupB** have been created for the Remote Sites A and B as explained in the use case study.



9. Click the FlexConnect Group name to edit. Assign one AP each to the FlexConnect Groups under **FlexConnect Groups > Edit FlexConnect Group Name > General**.



## VLAN Name Override for FlexConnect

FlexConnect Groups > Edit 'FlexGroupB'

General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping

Group Name FlexGroupB  
 VLAN Template Name Remote Site B  
 Enable AP Local Authentication   
 Application Visibility Disable

FlexConnect APs

Add AP

AP MAC Address	AP Name	Status
44:2b:03:9a:8a:3f	AP-2602	Associated

AAA

Server Ip Address  
 Server Type Primary  
 Shared Secret  
 Confirm Shared Secret  
 Port Number 1812

Add

Server Type	Address	Port
UnConfigured	Unconfigured	0
UnConfigured	Unconfigured	0

10. Click **Apply**.

11. Assign VLANs specific to each site on the FlexConnect Groups under **FlexConnect Groups > Edit FlexConnect Group Name > ACL Mapping > AAA VLAN-ACL mapping**.

In this example VLAN 37, 38 are assigned to Remote Site A and VLAN 37, 39 are assigned to Remote Site B.

FlexConnect Groups > Edit 'FlexGroupA'

General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping Policies

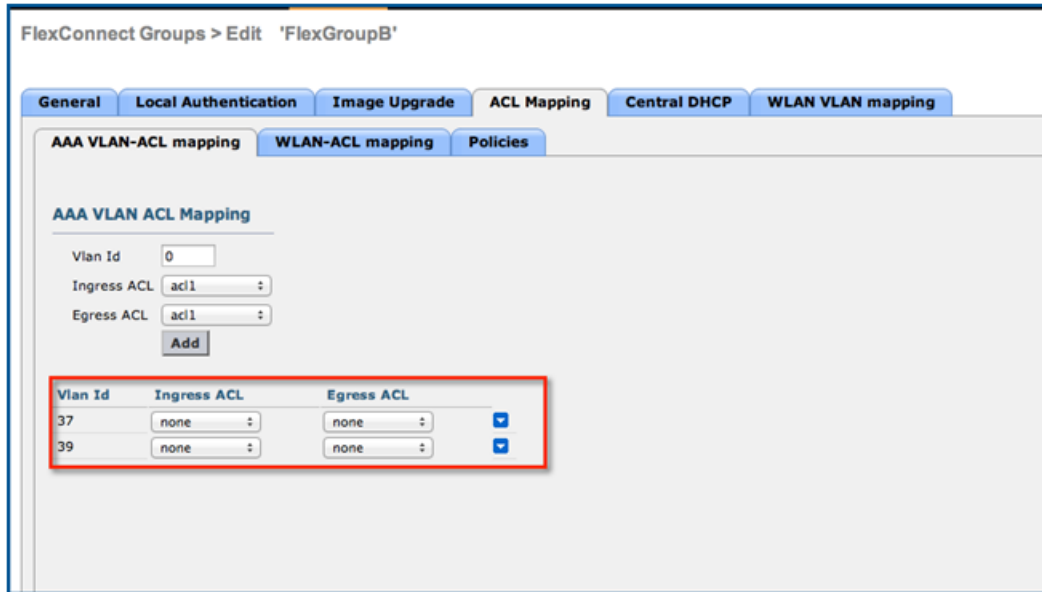
AAA VLAN ACL Mapping

Vlan Id 0  
 Ingress ACL none  
 Egress ACL none

Add

Vlan Id	Ingress ACL	Egress ACL
37	none	none
38	none	none

VLAN Name Override for FlexConnect

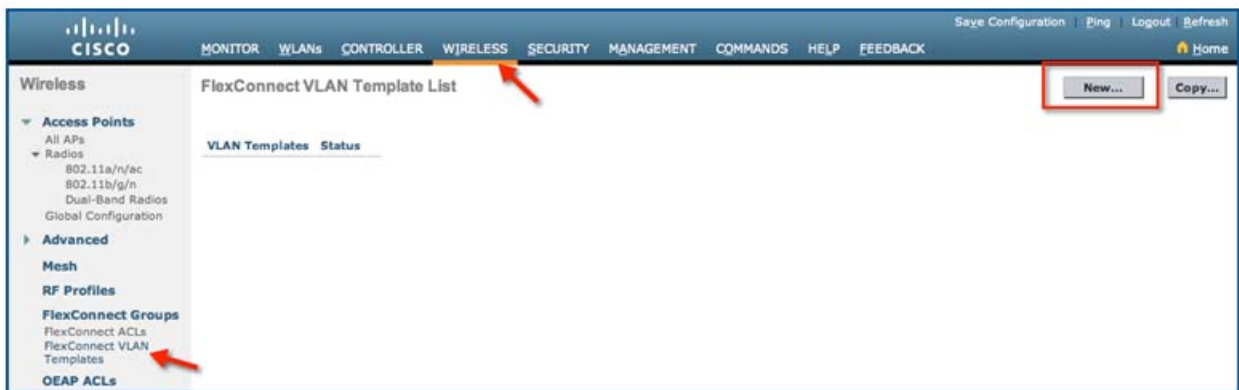


12. Click **Apply**.

VLAN Name Mapping

Creating VLAN Name Template

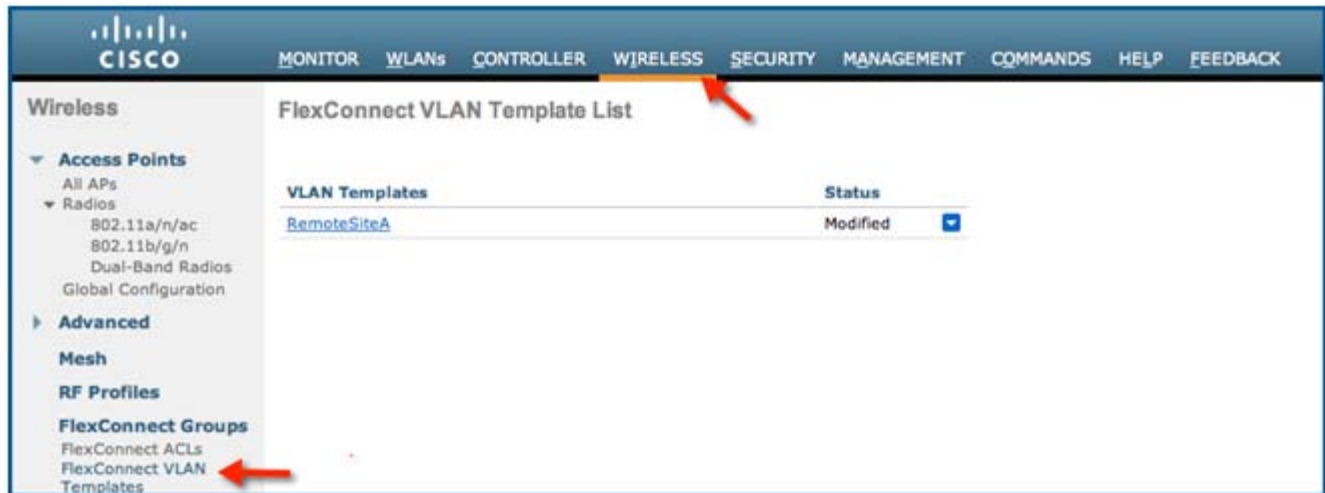
13. Create a VLAN Name template under **Wireless > FlexConnect Groups > FlexConnect VLAN Templates > New**.



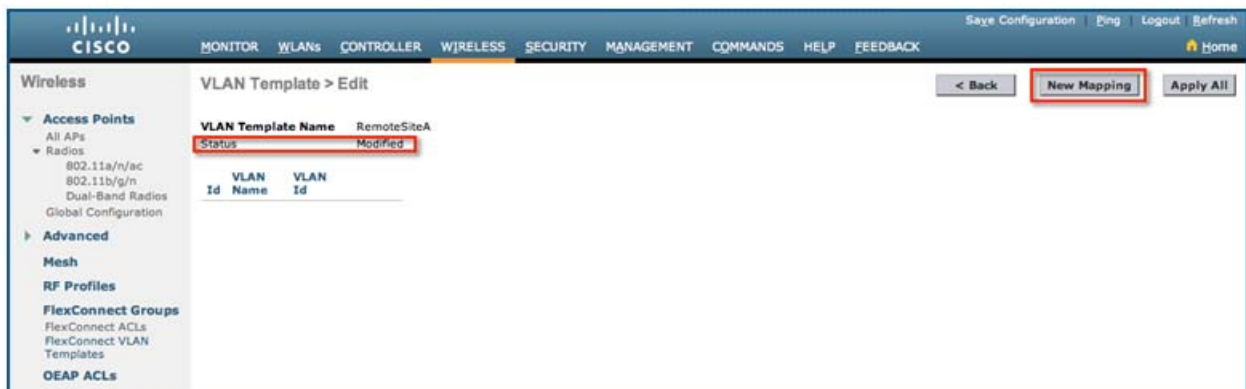
14. Click **Apply**.

In this example, the template is called **Remote Site A**. Observe that the status of the template is **Modified**.

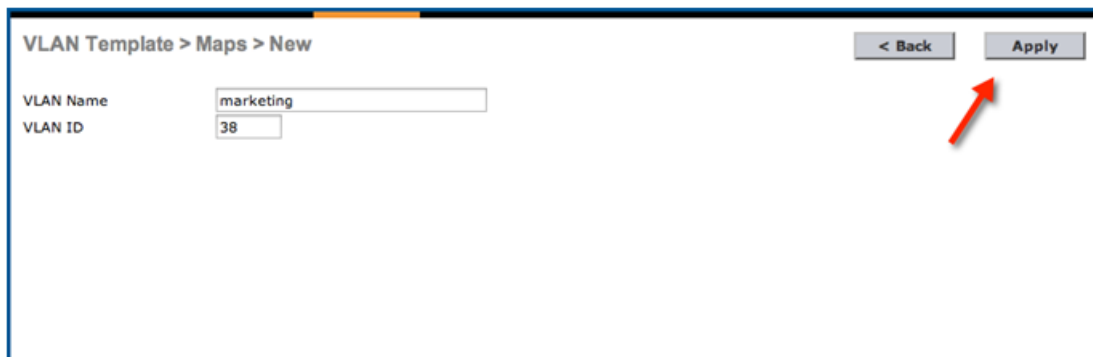
## VLAN Name Override for FlexConnect



15. Click the template to edit it and then click the **New Mapping** button to add the VLAN Name to VLAN ID mappings.



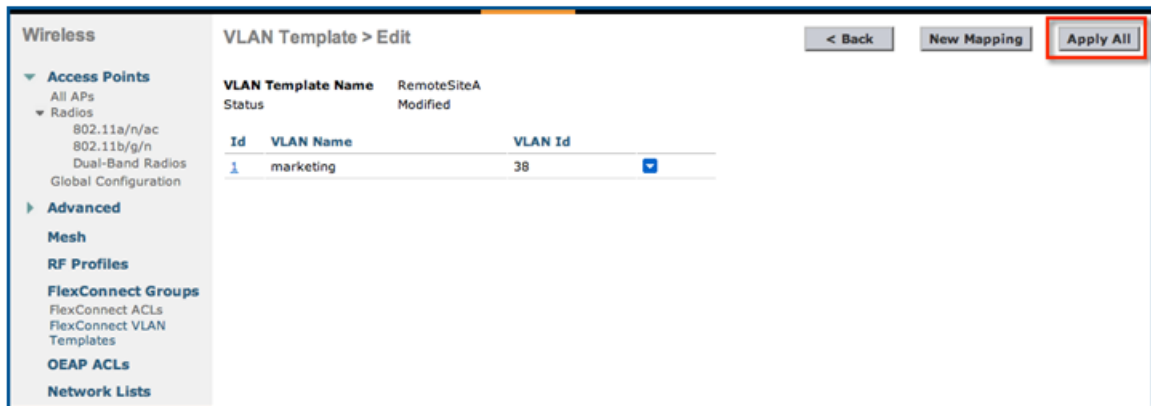
16. Add the VLAN Name to VLAN ID Mapping and click **Apply**. In this example, VLAN Name **marketing** is mapped to VLAN ID 38.



17. On the **VLAN Template > Edit** page, click **Apply All**.

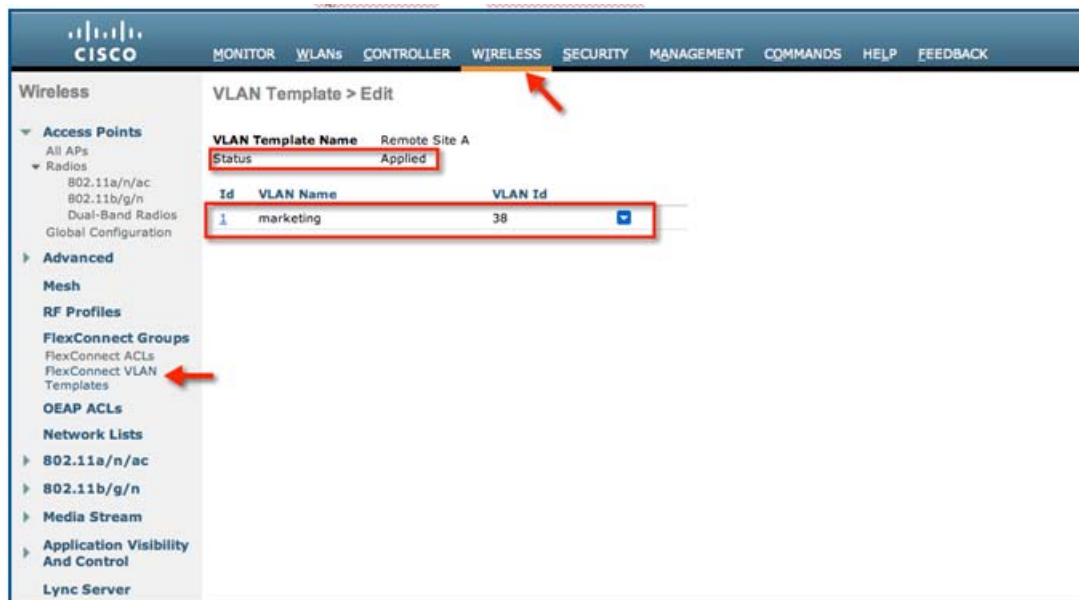


## VLAN Name Override for FlexConnect



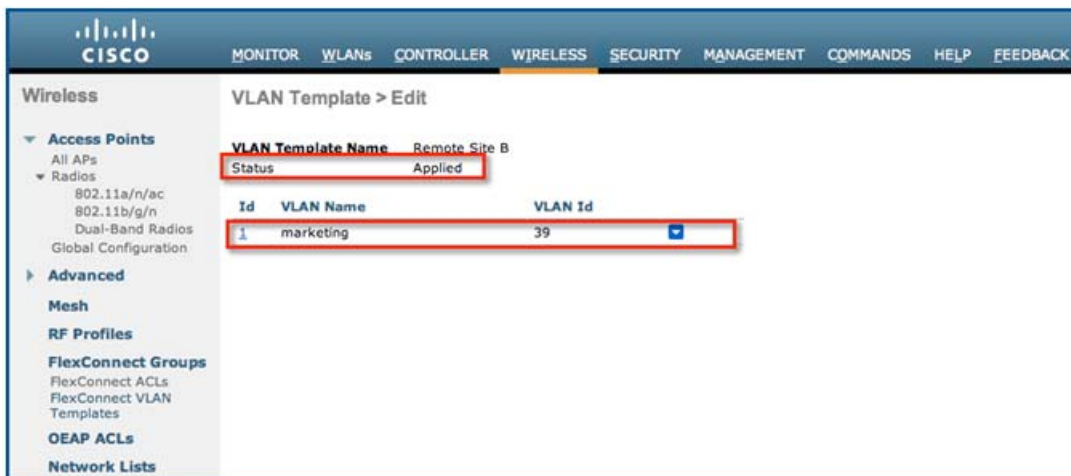
The status of the template changes to **Applied**.

**Note:** In order for the mapping to be pushed to the FlexConnect APs, the state of the template should be **Applied**. If the state is **Modified**, changes can be made to the template but they will not be pushed to the FlexConnect APs.

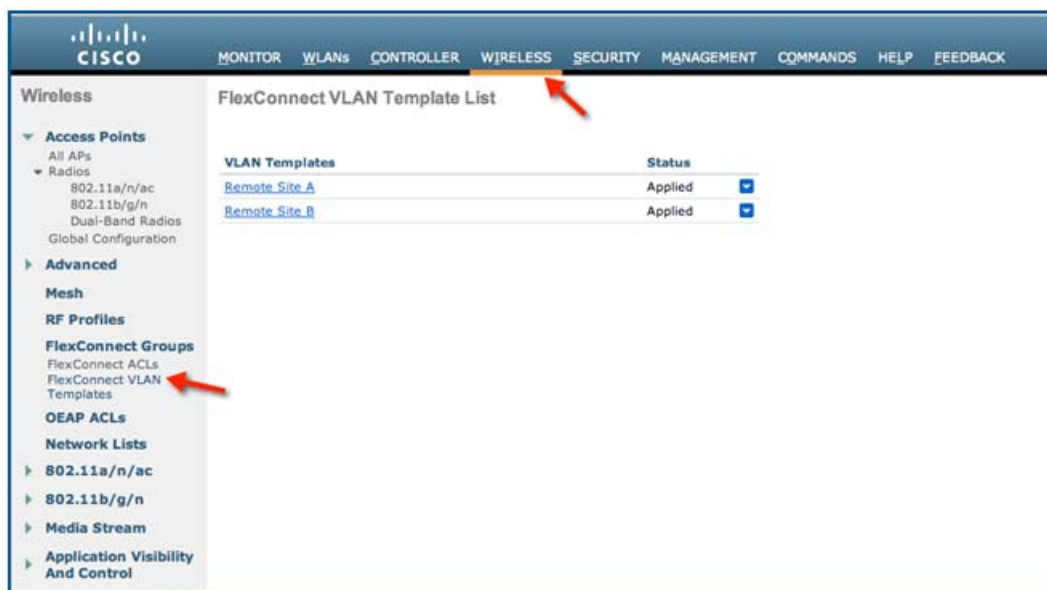


18. Similarly, create a VLAN Template for Remote Site B with VLAN Name **marketing** mapped to VLAN ID 39.

## VLAN Name Override for FlexConnect



19. Make sure that both the templates are created and the status is **Applied**.

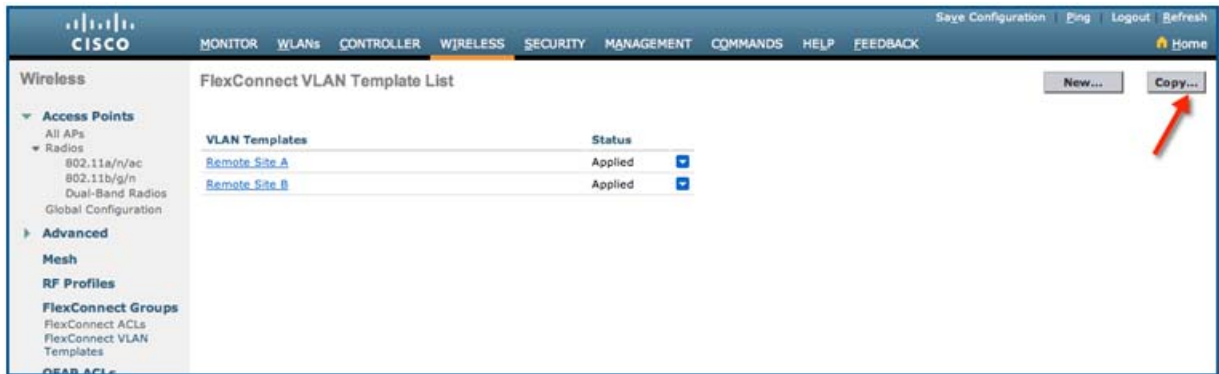


## Copying VLAN Name Template (Optional)

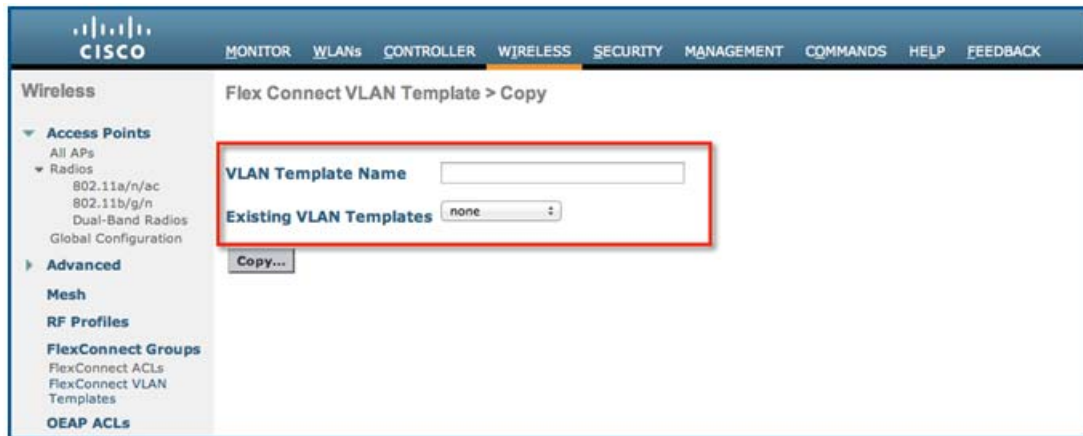
You can copy the VLAN Name templates to create a duplicate template. To copy the template, perform these steps:

20. Click the **Copy** button under **Wireless > FlexConnect Groups > FlexConnect VLAN Templates**.

VLAN Name Override for FlexConnect



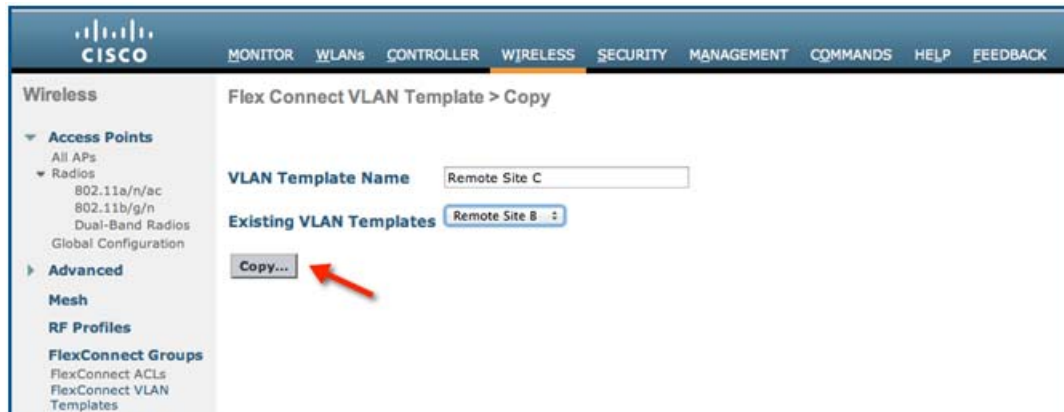
21. In the **VLAN Template Name** field, enter the destination template name. From the **Existing VLAN Template** drop-down menu, select the source template name.



22. Click **Copy**.

In this example, **Remote Site B** template is copied to **Remote Site C** since the sites B and C have the same VLAN Name to VLAN ID mapping requirements.

## VLAN Name Override for FlexConnect



The screenshot shows the FlexConnect VLAN Template List table. The table has two columns: "VLAN Templates" and "Status". The "Status" column has a dropdown menu for each row. A red arrow points to the dropdown menu for the "Remote Site C" row.

VLAN Templates	Status
<a href="#">Remote Site A</a>	Applied <input type="checkbox"/>
<a href="#">Remote Site B</a>	Applied <input type="checkbox"/>
<a href="#">Remote Site C</a>	Modified <input type="checkbox"/>

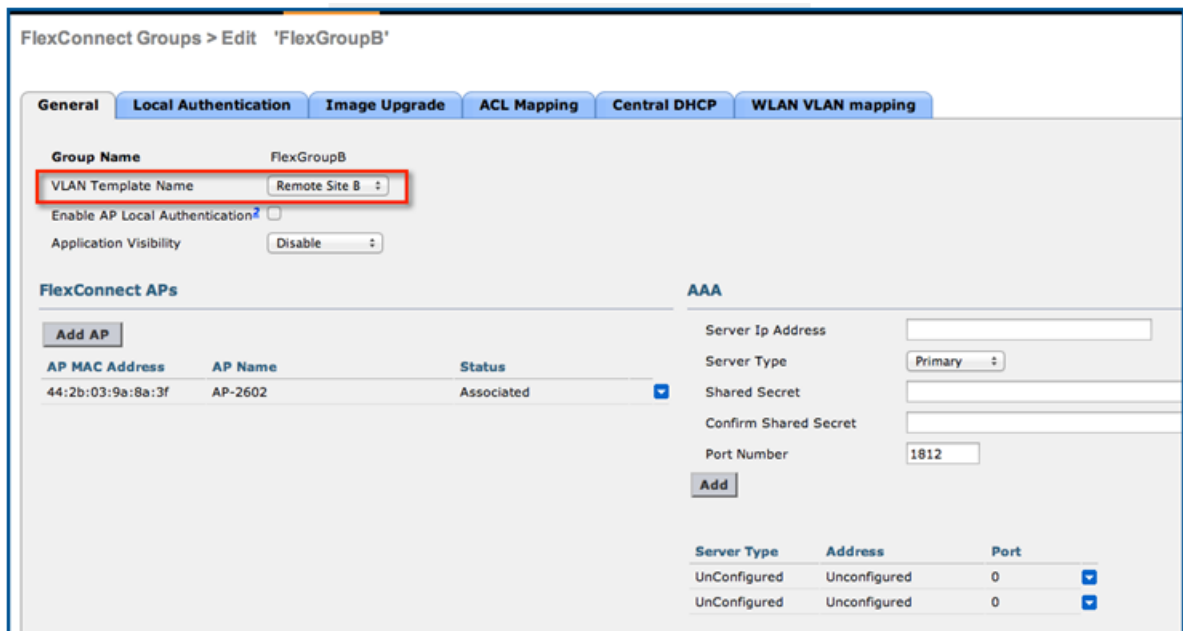
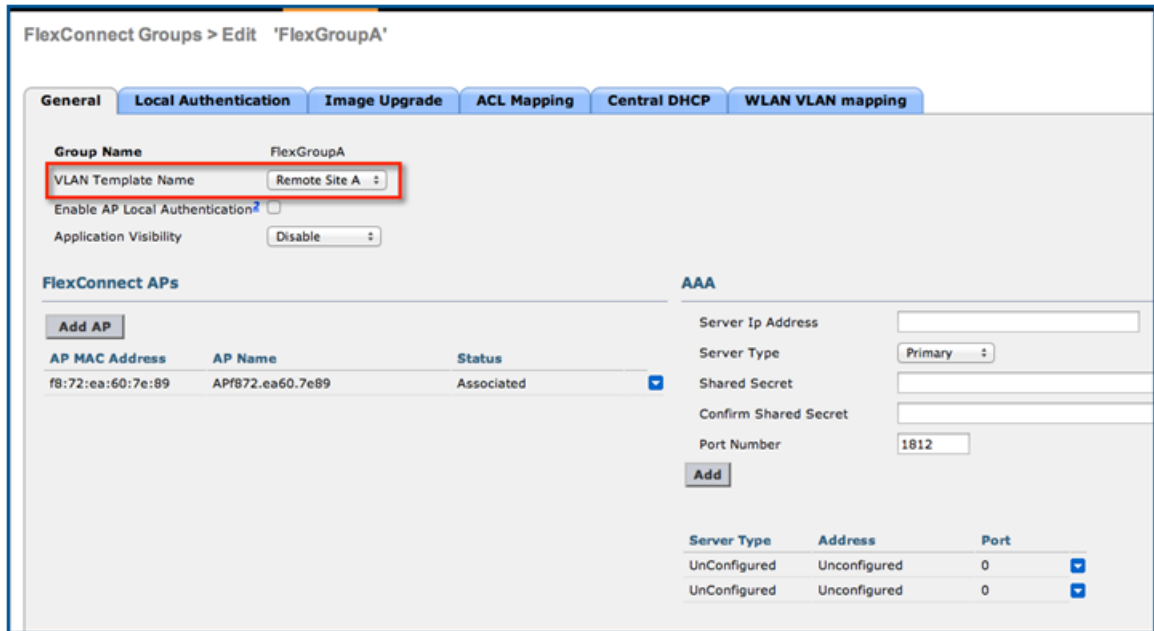
## Assigning VLAN Name Template

The VLAN Templates created must be applied to the respective FlexConnect Groups. To do this, perform these steps:

23. Under **FlexConnect Groups > Edit FlexConnect Group Name > General**, assign **VLAN Template Name** from the drop-down menu.

In this example, Template Remote Site A is assigned to FlexGroupA and Template Remote Site B is assigned to FlexGroupB.

VLAN Name Override for FlexConnect



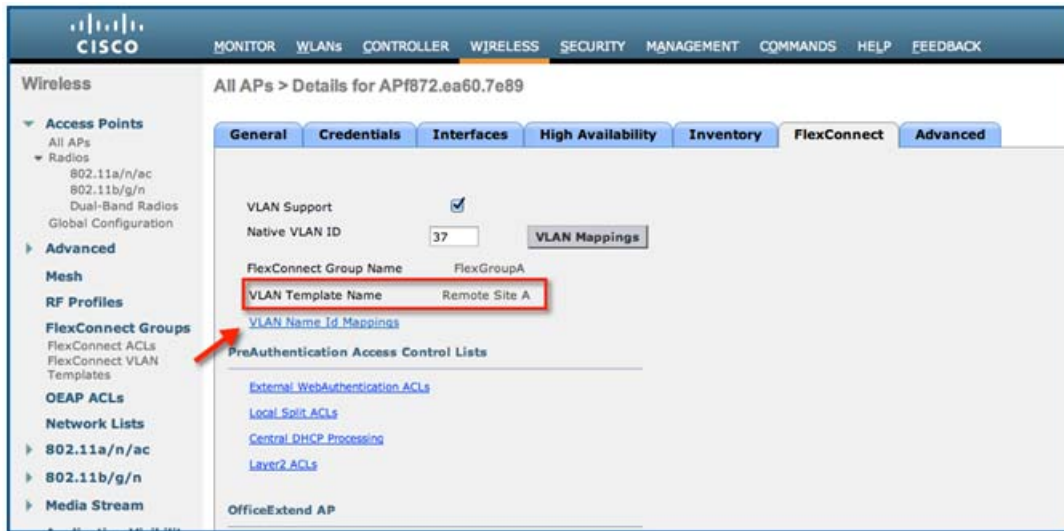
24. Click **Apply**.

Verifying VLAN Name Mappings on FlexConnect AP

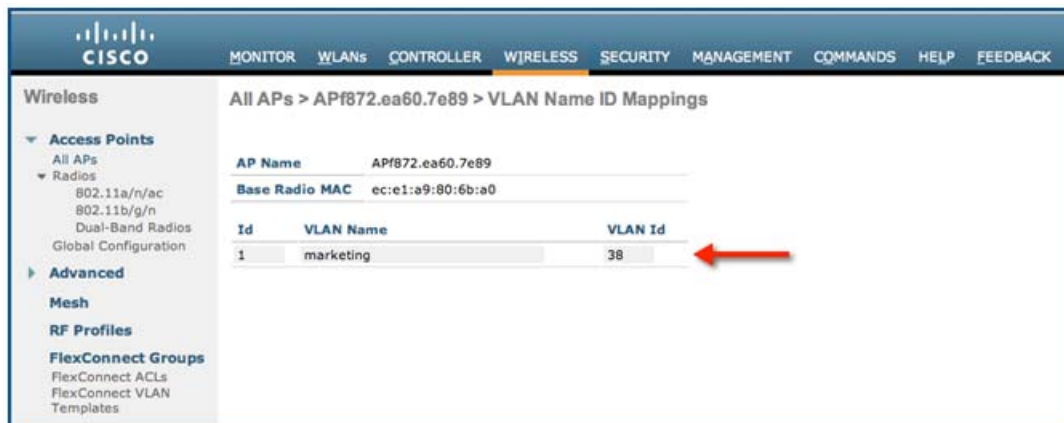
To verify that the VLAN Mappings are pushed to the FlexConnect APs, perform these steps:

25. Check the **VLAN Template Name** under **Wireless > All APs > Details > FlexConnect**.

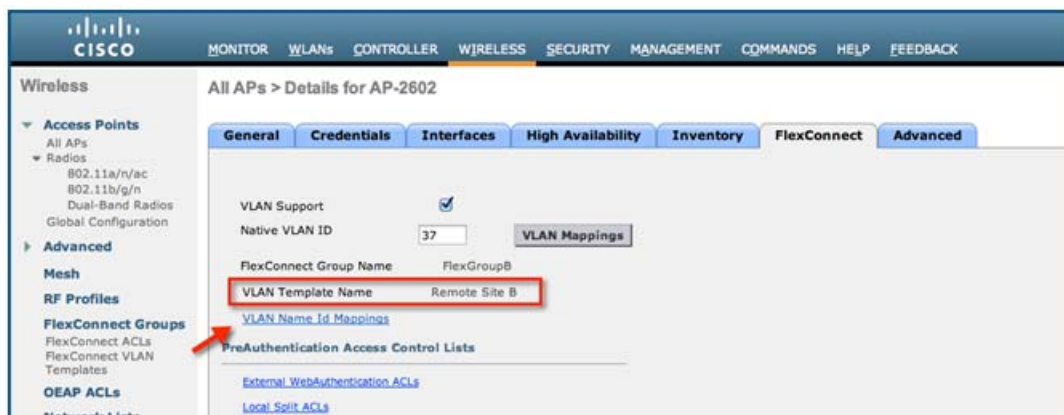
## VLAN Name Override for FlexConnect



26. Click the **VLAN Name Id Mappings** link to verify the individual mappings.

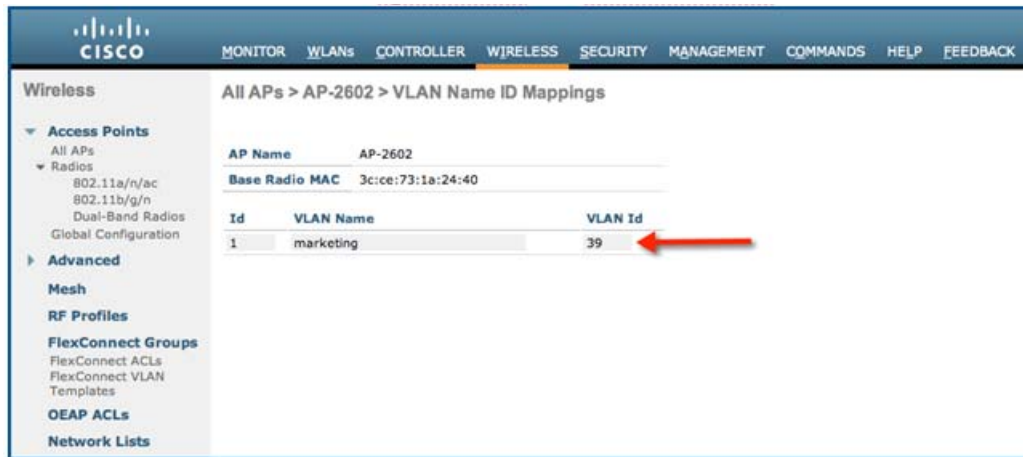


27. Similarly, verify the mappings for the other FlexConnect AP in FlexGroupB.





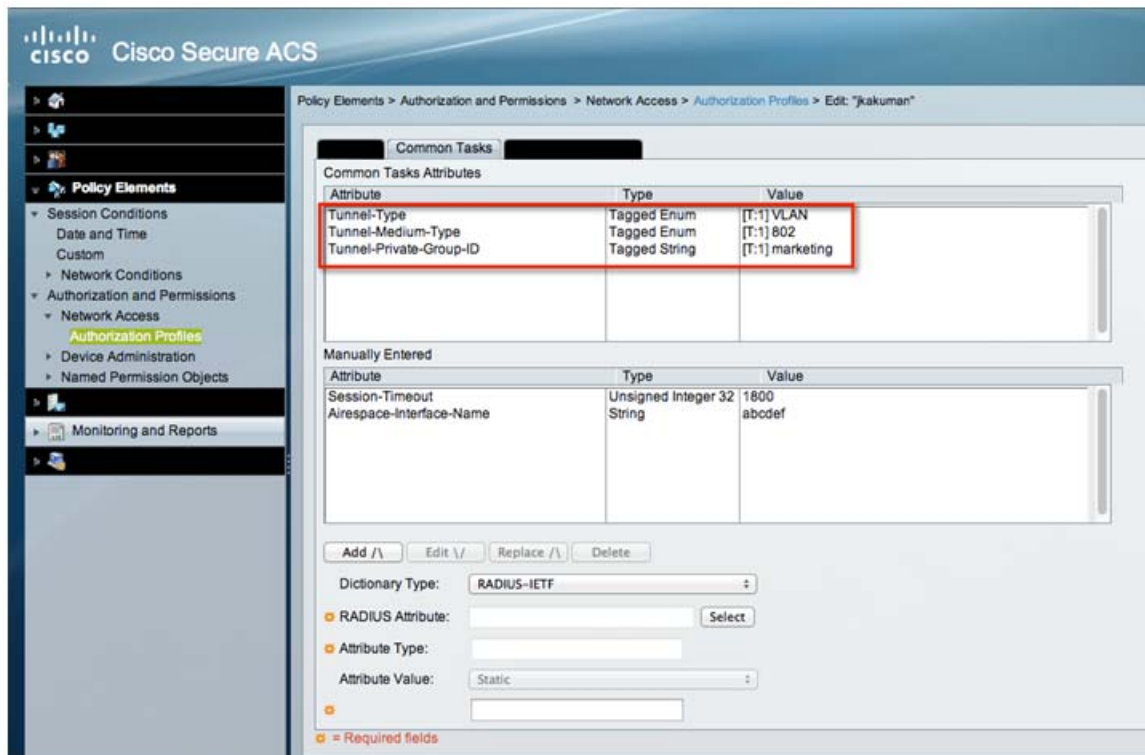
VLAN Name Override for FlexConnect



Thus, VLAN Name **marketing** is mapped to VLAN ID 38 in Remote Site A and to VLAN ID 39 in Remote Site B.

### RADIUS Server Configuration

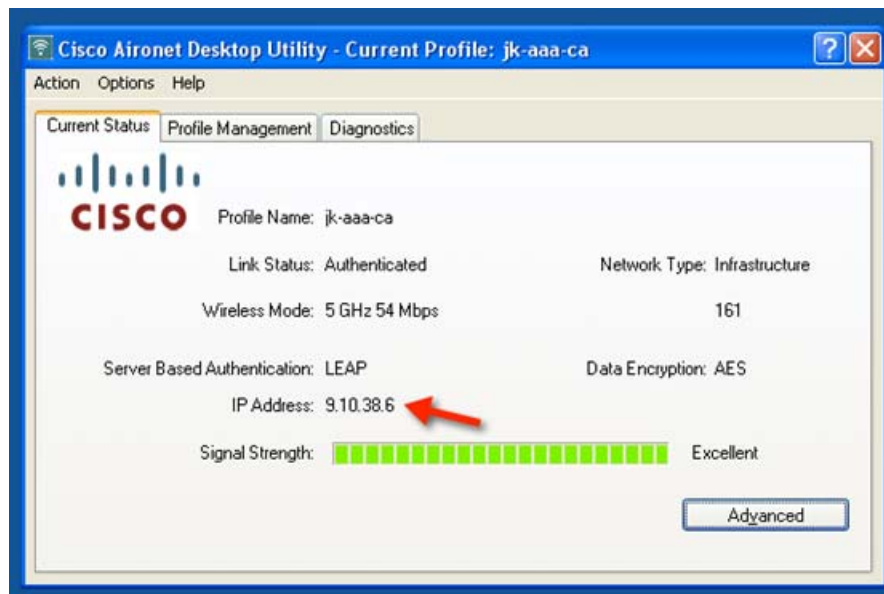
The following screenshot is from Cisco ACS 5.3. Cisco ACS or Cisco ISE can be used as the AAA RADIUS Server. Configure the user details under **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and add **Tunnel-Private-Group-ID** or **Aire-Interface-Name** attribute to reflect VLAN Name **marketing**.



## Verifying AAA Override

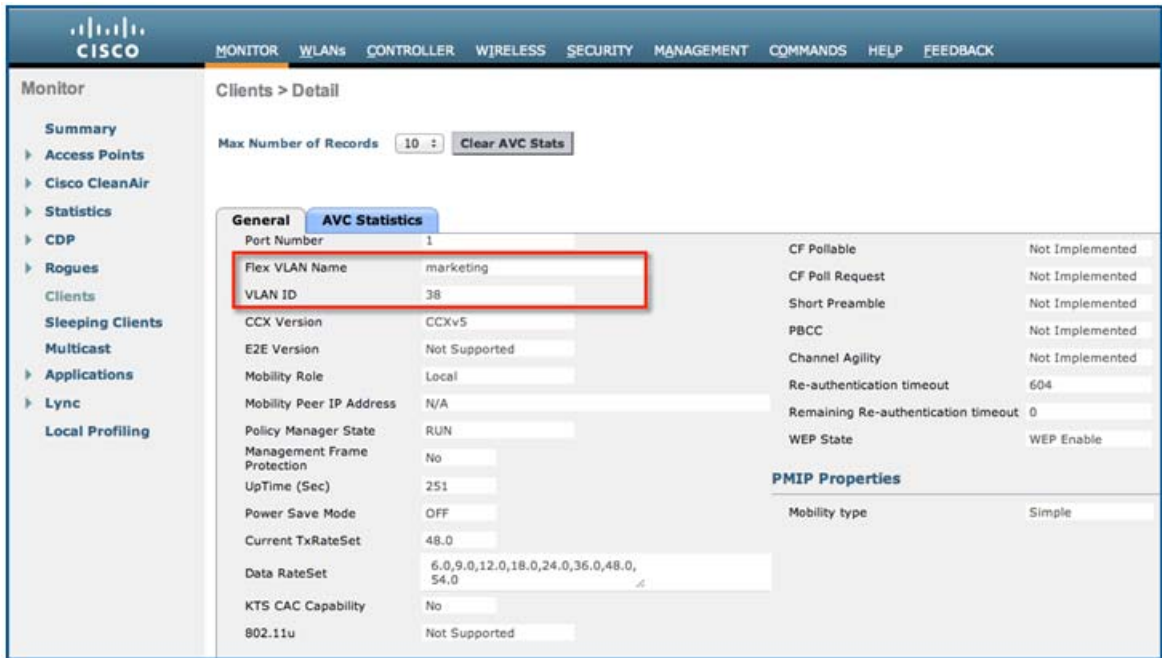
To verify AAA override, perform these steps:

28. Connect a client to AP in Remote Site A and upon successful authentication, verify that it has an IP address in the VLAN mapped to VLAN Name **marketing** in that site. In this example **marketing** is mapped to VLAN 38 in Remote Site A.



29. The VLAN Name for the client can also be verified on the client details page under **Monitor > Clients > Detail** by clicking the MAC address of the client.

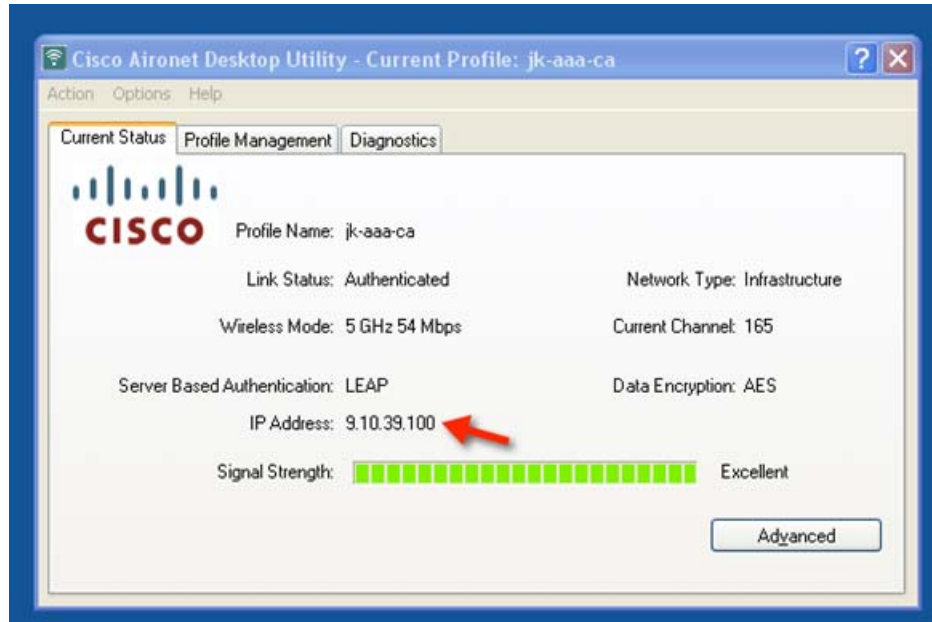
VLAN Name Override for FlexConnect



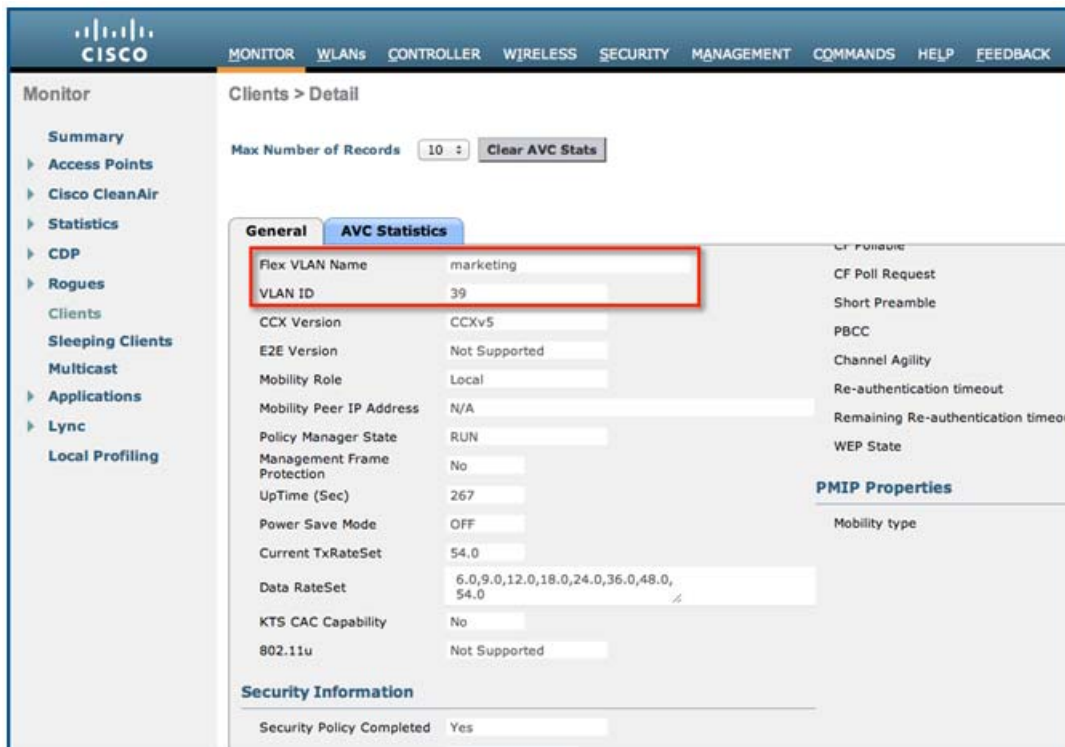
- Associate the client to the other FlexConnect AP and the same WLAN and upon successful authentication, verify that it has an IP address in the VLAN mapped to VLAN name **marketing** in that site. In this example, **marketing** is mapped to VLAN 39 in Remote Site B.



VLAN Name Override for FlexConnect



31. Make sure that the **Flex VLAN Name** field in the client details page reflects the correct Flex VLAN name and VLAN ID.



## Client ACL Support

Prior to release 7.5, we support FlexConnect ACLs on the VLAN. We also support AAA override of VLANs. If a client gets an AAA override of VLAN, it is placed on the overridden VLAN and the ACL on the VLAN applies for the client. If an ACL is received from the AAA for locally switched clients, we ignore the same. With release 7.5, we address this limitation and provide support for client based ACLs for locally switched WLANs.

### Client ACL Overview

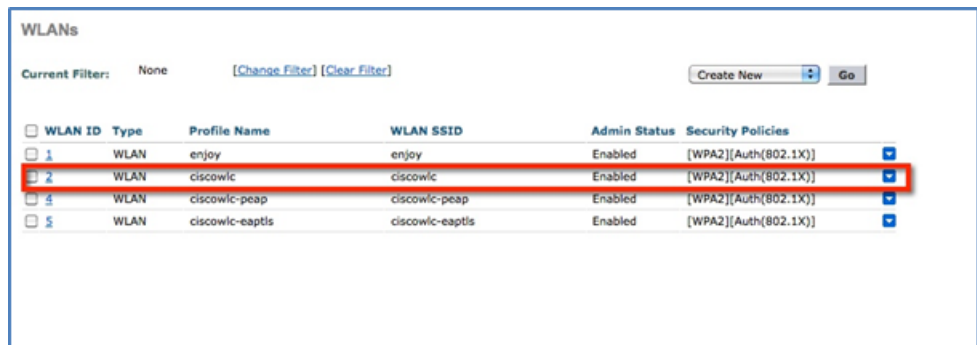
- a. This feature allows application of Per-Client ACL for locally switching WLANs.
- b. Client ACL is returned from the AAA server on successful Client L2 Authentication/Web Auth as part of Airespace Radius Attributes.
- c. The controller will be used to pre-create the ACLs at the AP. When the AP receives the ACL configuration, it will create the corresponding IOS ACL. Once, AAA server provides the ACL, the client structure will be updated with this information.
- d. There will be configuration per FlexConnect Group as well as per AP. A maximum of 16 ACLs can be created for a FlexConnect Group and a maximum of 16 ACLs can be configured per-AP.
- e. In order to support fast roaming (CCKM/PMK) for the AAA overridden clients, the controller will maintain these ACL in the cache and push them to all APs which are part of the FlexConnect Group.
- f. In the case of central authentication, when the controller receives the ACL from the AAA server, it will send the ACL name to the AP for the client. For locally authenticated clients, the ACL will be sent from the AP to the controller as part of CCKM/PMK cache, which will then be distributed to all APs belonging to the FlexConnect-group.
- g. Maximum of 16 Client ACLs per FlexConnect Group, maximum of 16 Client ACLs per-AP
- h. Total of 96 ACLs can be configured on the AP (32 VLAN-ACL, 16 WLAN-ACL, 16 Split tunnel, 16 FlexConnect Client ACL, 16 AP Client ACL), each ACL with 64 rules.
- i. The ACL will be applied on the dot11 side for the client in question. This ACL will be applied in addition to the VLAN ACL, which is applied on the VLAN of the Ethernet interface of the AP.
- j. Client ACL applied in addition to VLAN-ACL, both can exist simultaneously and are applied serially.



### Configuring Client ACL

1. Create a Local Switching WLAN, which is either centrally switched or locally switched.

Figure 51 Create Local Switching WLAN

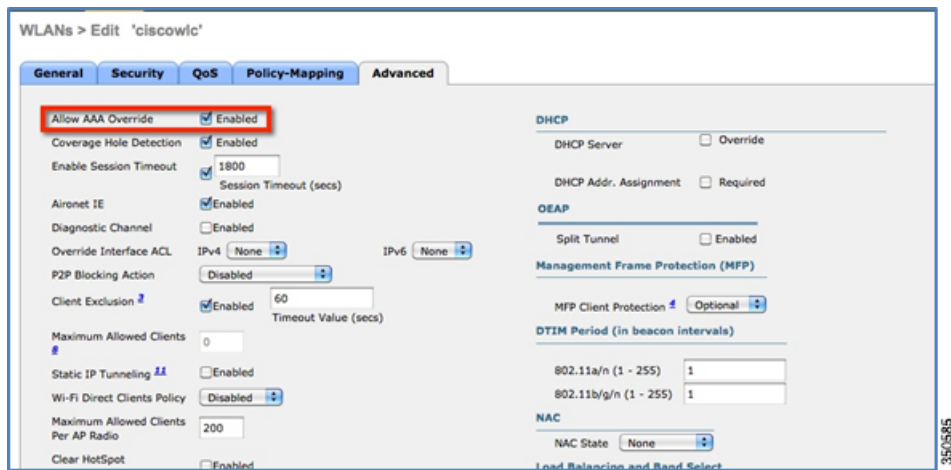


WLANs

Current Filter: None [Change Filter] [Clear Filter] [Create New] [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	ciscowic	ciscowic	Enabled	[WPA2][Auth(802.1X)]
3	WLAN	ciscowic-peap	ciscowic-peap	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	ciscowic-eaptls	ciscowic-eaptls	Enabled	[WPA2][Auth(802.1X)]

- Turn on AAA override for the WLAN by checking the **Allow AAA Override** check box.



WLANs > Edit 'ciscowic'

General Security QoS Policy-Mapping 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  None IPv6  None

P2P Blocking Action  Disabled

Client Exclusion  Enabled 60  
Timeout Value (secs)

Maximum Allowed Clients 0

Static IP Tunneling  Enabled

Wi-Fi Direct Clients Policy  Disabled

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot  Enabled

DHCP

DHCP Server  Override

DHCP Addr. Assignment  Required

OEAP

Split Tunnel  Enabled

Management Frame Protection (MFP)

MFP Client Protection  Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State  None

- Create a FlexConnect ACL.

FlexConnect ACL can be configured from the Security page as well as from the Wireless page.



Figure 52 Configure FlexConnect ACL

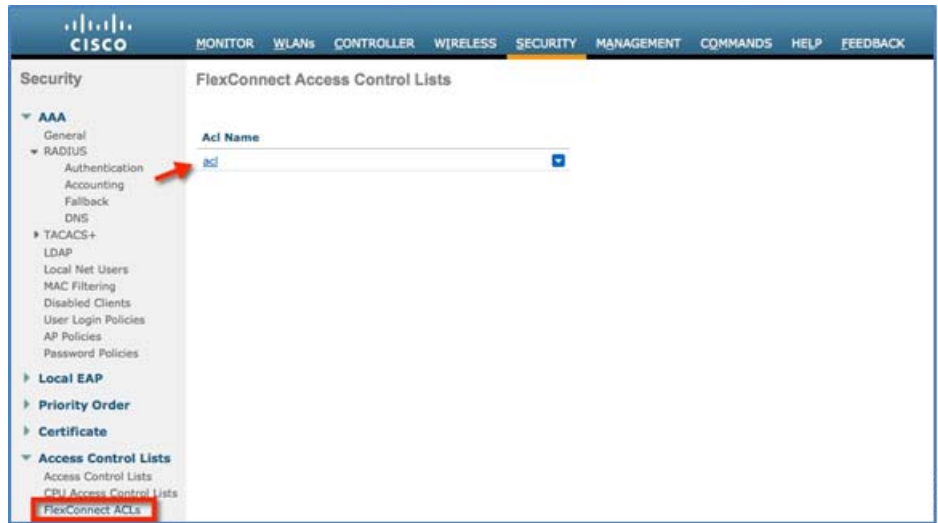
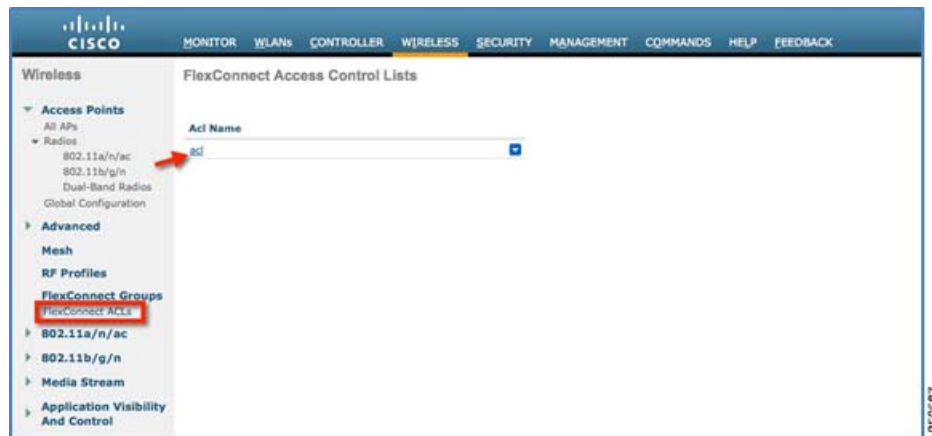


Figure 53 Configure FlexConnect ACL



4. Assign the FlexConnect ACL to the FlexConnect Group or to the AP.

Figure 54 ACL Mapping on FlexConnect Group

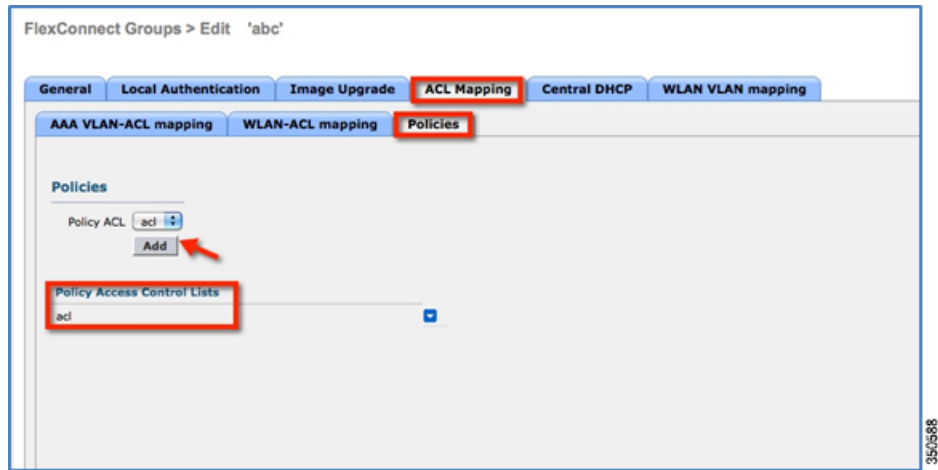
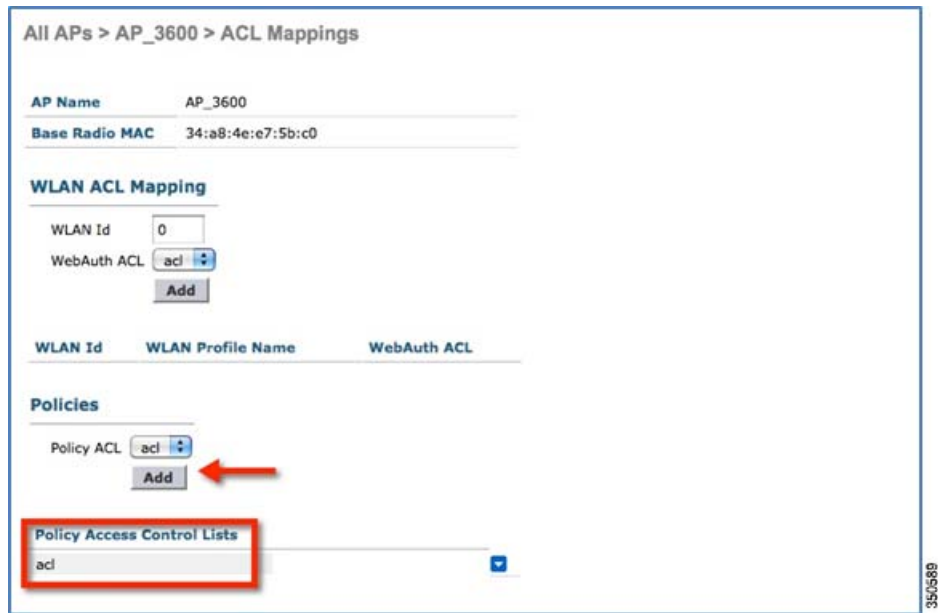


Figure 55 ACL Mapping on AP



5. Configure the Airespace attribute on the Radius/Cisco ACS server/ISE.

Figure 56 Aire-Acl-Name on Cisco ACS Server

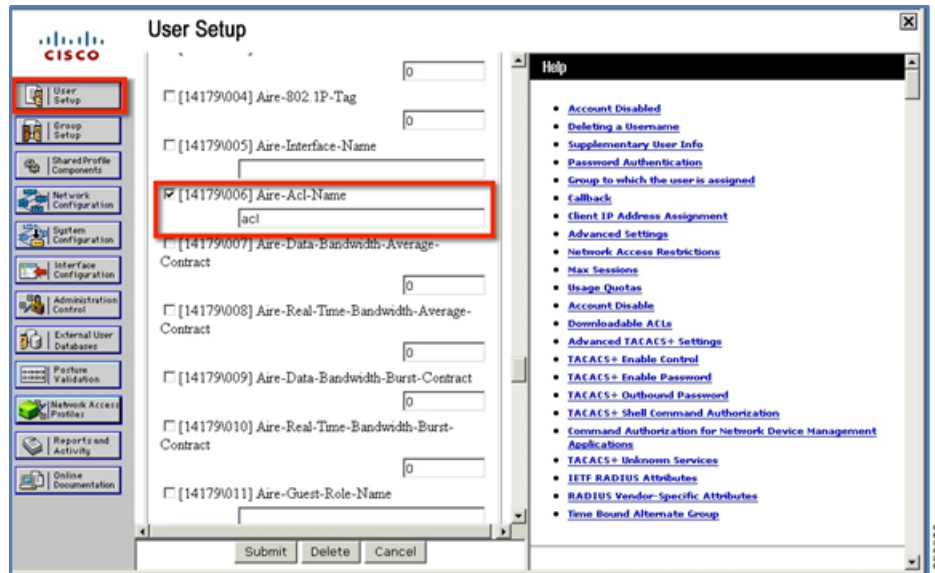
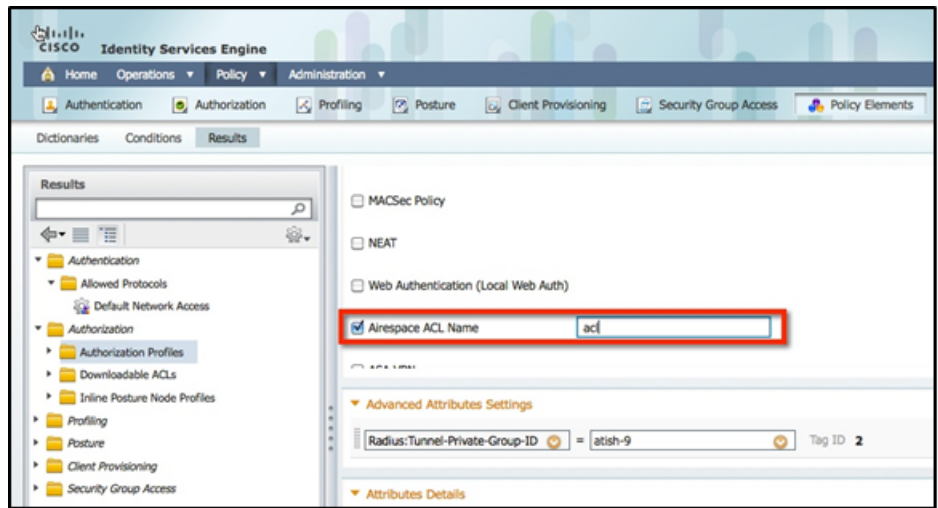
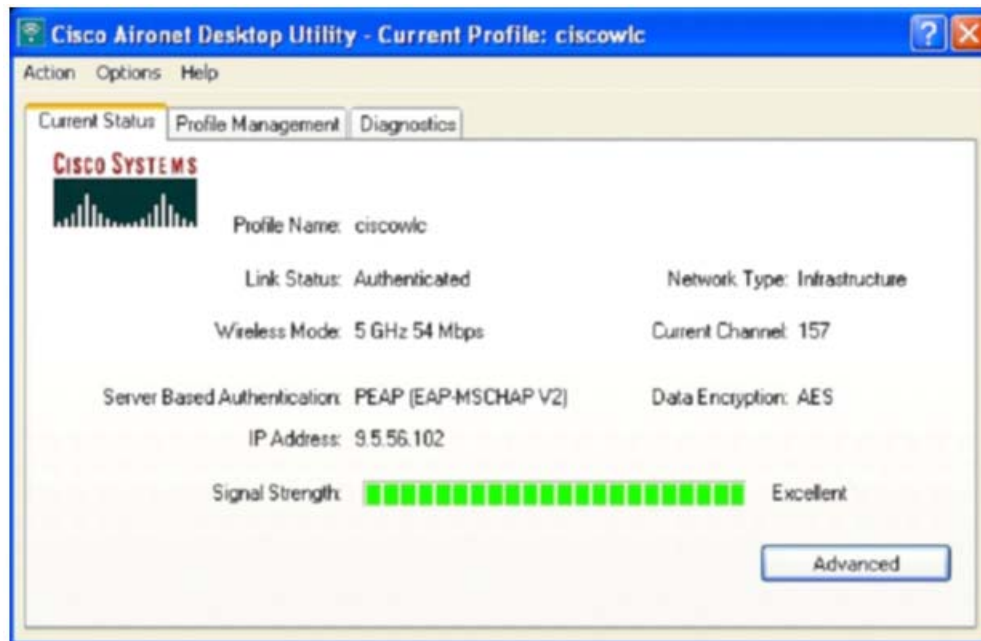


Figure 57 Airespace ACL Name on ISE



6. Authenticate the client.



## CLI Configuration

The Client ACL can be seen on the AP using the commands **show access-list** and **show controllers dot11Radio**

**Figure 58** show access-lists Output

```
AP_3600#show access-lists
Extended IP access list acl
 10 deny icmp any any (10 matches)
 20 permit ip any any (328 matches)
AP_3600#
```

**Figure 59** Client ACL on AP

```
AP_3600#show controllers dot11Radio 1 | b -cli
--Clients # AID VLAN Status S/I/B/A Age Tx0-R(A) Mode Enc Key Rate Mask Tx Rx BVI Split-ACL Client-ACL L2-ACL
7cd1 c386.7edc 2 5 3A 40294 000 1FE 300 0-0 (0) 3280 600 1-10 00FFFFFFF 0217 00C acl
0040.96b8.d4be 1 2 30 40244 000 1F2 300 0-0 (0) 0188 200 0-10 00FF00000 0060 060
(Client) MaxFrt DefUniFrt DefMultFrt WiredProt
7cd1 c386.7edc 3 3 3 0
0040.96b8.d4be 3 3 3 0
Agr TxLk PkL MaxL AC counts
7cd1 c386.7edc 10 30 0 65460 0 (0,0) 0 (0,0) 0 (0,0) 0 (0,0)
0040.96b8.d4be 10 15 0 0 0 (0,0) 0 (0,0) 0 (0,0) 0 (0,0)
RxPkts KBytes Dup Dec Mic TxPkts KBytes Retry RSSI SNR
7cd1 c386.7edc 150 12 20 0 0 64 2 6 38 53
```

<http://www.cisco.com/c/en/us/support/wireless/flex-7500-series-wireless-controllers/tsd-products-support-series-home.html>

## Guidelines

- Prior to AAA sending the client ACL, the ACL should be pre-created on the group or AP. The ACL will not be dynamically downloaded to the AP at the time of client join.
- A maximum of 96 ACLs can be configured on the AP.

## Client ACL Support

- Each ACL will have a maximum of 64 rules.
- If client is already authenticated, and ACL name is changed on the radius, then client will have to do a full authentication again to get the correct client ACL.
- Since ACL not saved in cache at the controller, if the AP reboots/crashes, its cache will not be updated and the client will have to do full authentication for correct client ACL to be applied.
- If an ACL is returned from the AAA server but the corresponding ACL is not present on the AP, the client will be de-authenticated. A log message will be generated at the AP and WLC console.

On AP:

```
*Mar 4 09:20:43.255: %LWAPP-3-CLIENT_ACL_ENTRY_NOT_EXIST: Deleting Mobile for 0040.96b8.d4be: CLIENT ACL not exist on AP
```

On WLC:

```
*spamApTask7: Mar 04 14:51:03.989: #HREAP-3-CLIENT_ACL_ENTRY_NOT_EXIST: spam_irad.c:36670 The client 00:40:96:b8:d4:be could not join AP : 34:a8:4e:e7:5b:c0 for slot 1, Reason: acl returned from RADIUS/local policy not present at AP
```

The various scenarios are listed in the table below:

ACL present on AP	ACL returned from AAA	Behavior
No	No	N/A
No	Yes	Client will be de-authenticated
Yes	No	Normal L2 authentication. No ACL will be applied.
Yes	Yes	L2 Authentication with client ACL being applied.

## VideoStream for FlexConnect Local Switching

### Introduction

Cisco Unified Wireless Network (CUWN) release 8.0 introduces a new feature—VideoStream for Local Switching, for branch office deployments. This feature enables the wireless architecture to deploy multicast video streaming across the branches, just like it is currently possible for enterprise deployments. This feature recompensates the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

### Components Used

VideoStream feature for Local Switching is available in CUWN software version 8.0. This feature is supported on all wireless LAN controllers (WLANs) and newer generation indoor access points (APs). This feature is unavailable on autonomous access points.

## Supported Wireless Hardware and Software

VideoStream is supported on all the following Cisco Wireless LAN controllers:

- Cisco 5500 Controller
- Cisco 7510 Controller
- Cisco 8510 Controller
- Cisco WiSM-2 Controller
- Cisco 2504 Controller
- vWLC

IGMPv2 is the supported version on all of the controllers.

VideoStream is supported on 802.11n models of APs consisting of Cisco Aironet 1140, 1250, 1260, 1520, 1530, 1550, 1600, 2600, 3500, 3600 series APs and 802.11ac models 3700 and 2700 series APs.

## Theory of Operation

Before going into details about the VideoStream feature, you should understand some of the shortfalls in Wi-Fi multicast. 802.11n is a prominently discussed wireless technology for indoor wireless deployments. Equally prominent requirement is seen in multimedia service on an enterprise and branch network, in particular, video. Multicast does not provide any MAC layer recovery on multicast and broadcast frames. Multicast and broadcast packets do not have an Acknowledgement (ACK), and all packet delivery is best effort. Multicast over wireless with 802.11a/b/g/n does not provide any mechanism for reliable transmission.

Wireless deployments are prone to interference, high channel utilization, and low SNR at the edge of the cell. There are also many clients sharing the same channel but have different channel conditions, power limitations, and client processing capabilities. Therefore, multicast is not a reliable transmission protocol to all the clients in the same channel because each client has different channel conditions.

Wireless multicast does not prioritize the video traffic even though it is marked as Differentiated Service Code Point (DSCP) by the video server. The application will see a loss of packets with no ACK, and retries to the delivery will be bad. In order to provide reliable transmissions of multicast packet, it is necessary that the network classify queues and provisions using Quality of Service (QoS). This virtually removes the issue of unreliability by eliminating dropped packets and delay of the packets to the host by marking the packets and sorting them to the appropriate queue.

Even though the 802.11n, and now 802.11ac, adaptation has gained momentum both with the network and clients, wireless multicast has not been able to use the 802.11n and 802.11ac data rates. This has also been one of the factors for an alternate mechanism for wireless multicast propagation.

## VideoStream

VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP regardless if there is a client joined to a multicast group. In order to get around this limitation, the AP has to send multicast traffic to the host using Unicast forwarding, only on the WLAN that the client is joined and at the data rate the client is joined at.

VideoStream can be enabled globally on the controller. The feature can also be enabled at the WLAN level, and provides more control to the administrator to identify specific video streams for Multicast Direct functionality.



## Stream Admission

As mentioned earlier, while video is an efficient, high-impact means of communication, it is also very bandwidth intensive, and as is seen, not all video content is prioritized the same. From earlier discussion it is clear that organizations investing in video cannot afford to have network bandwidth consumed without any prioritization of business-critical media.

## Multicast to Unicast

By enabling 802.11n data rates and providing packet error correction, multicast-to-unicast capabilities of Cisco VideoStream enhances reliability of delivering streaming video over Wi-Fi beyond best-effort features of traditional wireless networks.

A wireless client application subscribes to an IP multicast stream by sending an IGMP join message. With reliable multicast, this request is snooped by the infrastructure, which collects data from the IGMP messages. The AP checks the stream subscription and configuration. A response is sent to the wireless client attached to the AP in order to initiate reliable multicast once the stream arrives. When the multicast packet arrives, the AP replicates the multicast frame and converts it to 802.11 unicast frames. Finally, a reliable multicast service delivers the video stream as unicast directly to the client.

## Higher Video Scaling on Clients

With Cisco VideoStream technology, all of the replication is done at the edge (on the AP), thus utilizing the overall network efficiently. At any point in time, there is only the configured media stream traversing the network, because the video stream is converted to unicast at the APs based on the IGMP requests initiated by the clients. Some other vendor implementations do a similar conversion of multicast to unicast, but do it inefficiently as evidenced by the load put on the wired network to support the stream.

## Switch Configuration

VideoStream can be deployed on an existing branch wide wired and wireless network. The overall implementation and maintenance costs of a video over wireless network are greatly reduced. The assumption is that the wired network is multicast enabled. In order to verify that the access switch is part of the layer 3 network, connect a client machine to the switchport and verify if the client machine is able to join a multicast feed.

`show run | include multicast` displays if multicast is enabled on the layer 3 switch else if not enabled for multicast, you can enable multicast by executing the following command on the switch:

```
L3_Switch#show run | include multicast
```

```
ip multicast-routing distributed
```

Depending on the type of Protocol Independent Routing (PIM) configuration on the wired network, the layer 3 switch is configured either in PIM Sparse mode or in PIM dense mode. There is also a hybrid mode, PIM sparse-dense mode which is widely used.

```
interface Vlan56
```

```
ip address 9.5.56.1 255.255.255.0
```

```
ip helper-address 9.1.0.100
```

```
ip pim sparse-dense-mode
```

end

**show ip igmp interfaces** display the SVI interfaces that are participating in the IGMP membership. This command displays the version of IGMP configured on the switch or the router. The IGMP activity on the interface can also be verified in the form of IGMP join and leave messages by the clients.

```
L3_Switch#show ip igmp interface
```

```
Vlan56 is up, line protocol is up
```

```
Internet address is 9.5.56.1/24
```

```
IGMP is enabled on interface
```

```
Current IGMP host version is 2
```

```
Current IGMP router version is 2
```

```
IGMP query interval is 60 seconds
```

```
IGMP configured query interval is 60 seconds
```

```
IGMP querier timeout is 120 seconds
```

```
IGMP configured querier timeout is 120 seconds
```

```
IGMP max query response time is 10 seconds
```

```
Last member query count is 2
```

```
Last member query response interval is 1000 ms
```

```
Inbound IGMP access group is not set
```

```
IGMP activity: 6 joins, 3 leaves
```

```
Multicast routing is enabled on interface
```

```
Multicast TTL threshold is 0
```

```
Multicast designated router (DR) is 9.5.56.1 (this system)
```

```
IGMP querying router is 9.5.56.1 (this system)
```

```
Multicast groups joined by this system (number of users):
```

```
224.0.1.40(1)
```

The above configuration can be verified by running the **show ip mroute** command on the layer 3 switch. The above configuration has certain entries that need to be looked into. The special notation of (Source, Group), pronounced “S, G” where the source “S” is the source IP address of the multicast server and “G” is the Multicast Group Address that a client has requested to join. If the network has many sources, you will see on the routers an (S,G) for each of the source IP address and Multicast Group addresses. This output displayed below also has information of outgoing and incoming interfaces.

```
L3_Switch#show ip mroute
```

```
IP Multicast Routing Table
```

## Client ACL Support

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

L - Local, P - Pruned, R - RP-bit set, F - Register flag,

T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,

X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,

U - URD, I - Received Source Specific Host Report,

Z - Multicast Tunnel, z - MDT-data group sender,

Y - Joined MDT-data group, y - Sending to MDT-data group,

V - RD & Vector, v - Vector

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(\* , 239.255.255.250), 4d20h/00:02:35, RP 0.0.0.0, flags: DC

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan56, Forward/Sparse-Dense, 4d20h/stopped

(\* , 229.77.77.28), 4d15h/00:02:36, RP 0.0.0.0, flags: DC

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan56, Forward/Sparse-Dense, 00:24:34/stopped

(\* , 224.0.1.40), 5d17h/00:02:41, RP 0.0.0.0, flags: DCL

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

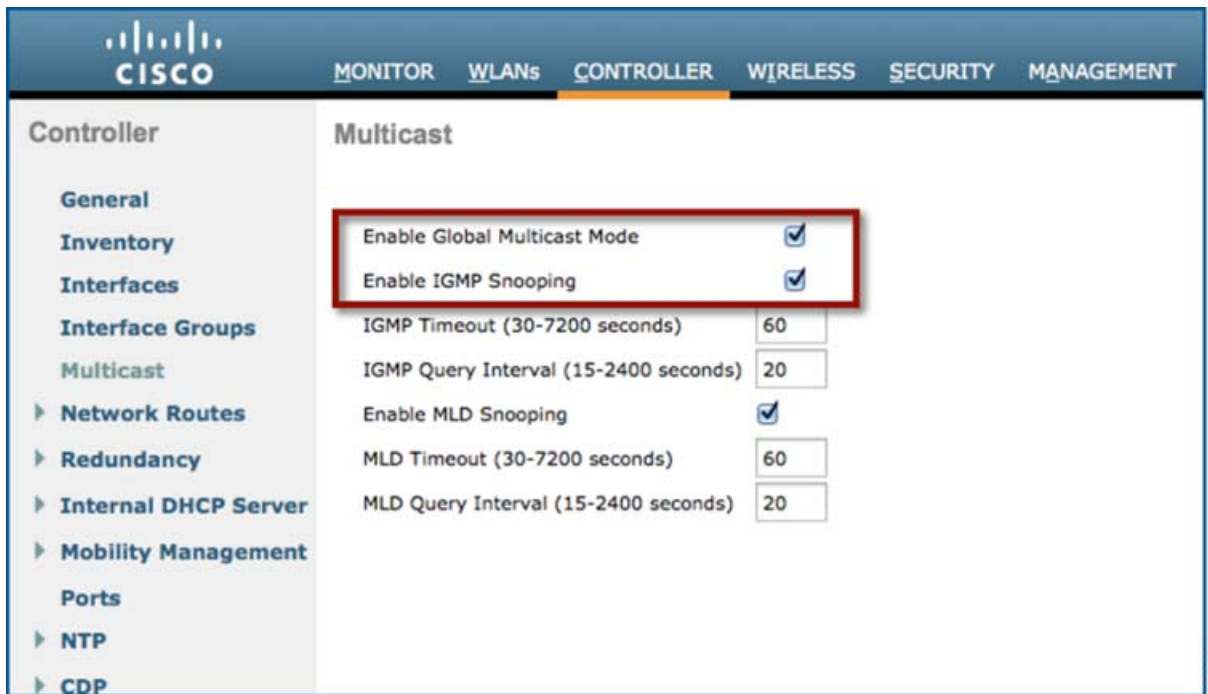
Vlan56, Forward/Sparse-Dense, 5d17h/stopped

## Controller Configuration

Enabling VideoStream-Global

Enable Global Multicast Mode and IGMP snooping on the controller as shown below:

Figure 60 WLC Configuration

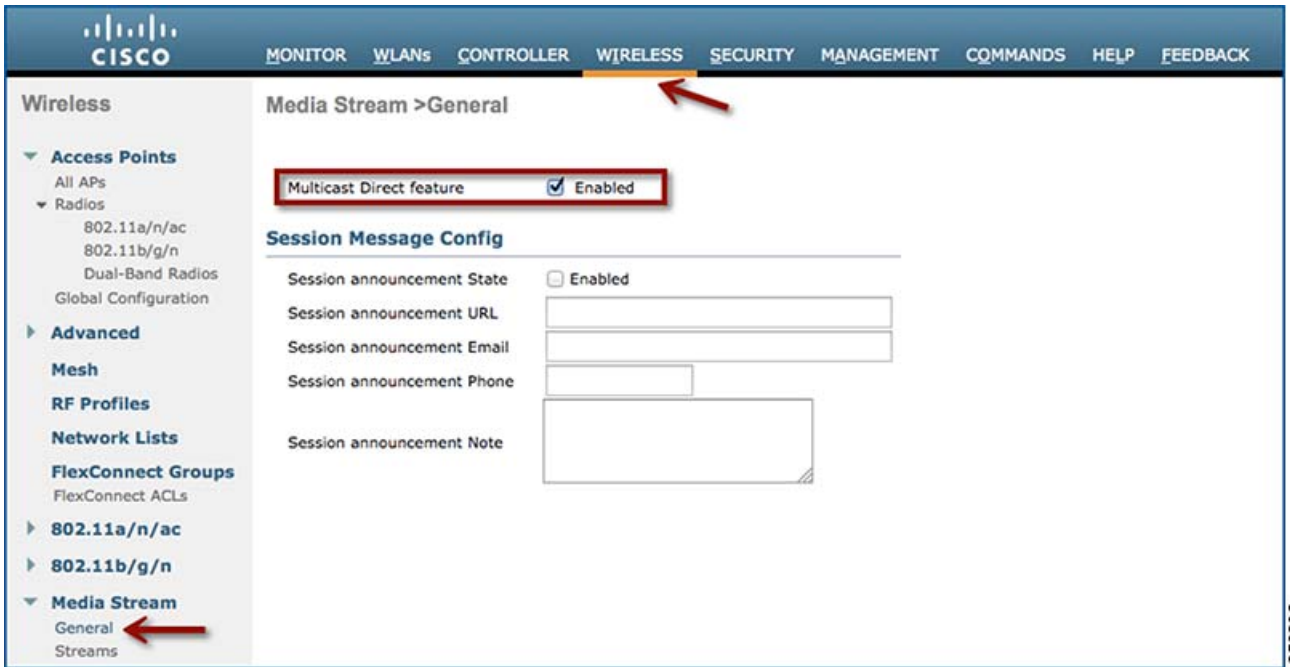


```
(Cisco Controller) >config network multicast global enable
```

```
(Cisco Controller) >config network multicast igmp snooping enable
```

To enable the VideoStream feature globally on the controller, navigate to **Wireless > Media Stream > General** and check the **Multicast Direct Feature** check box. Enabling the feature here populates some of the configuration parameters on the controller for VideoStream.

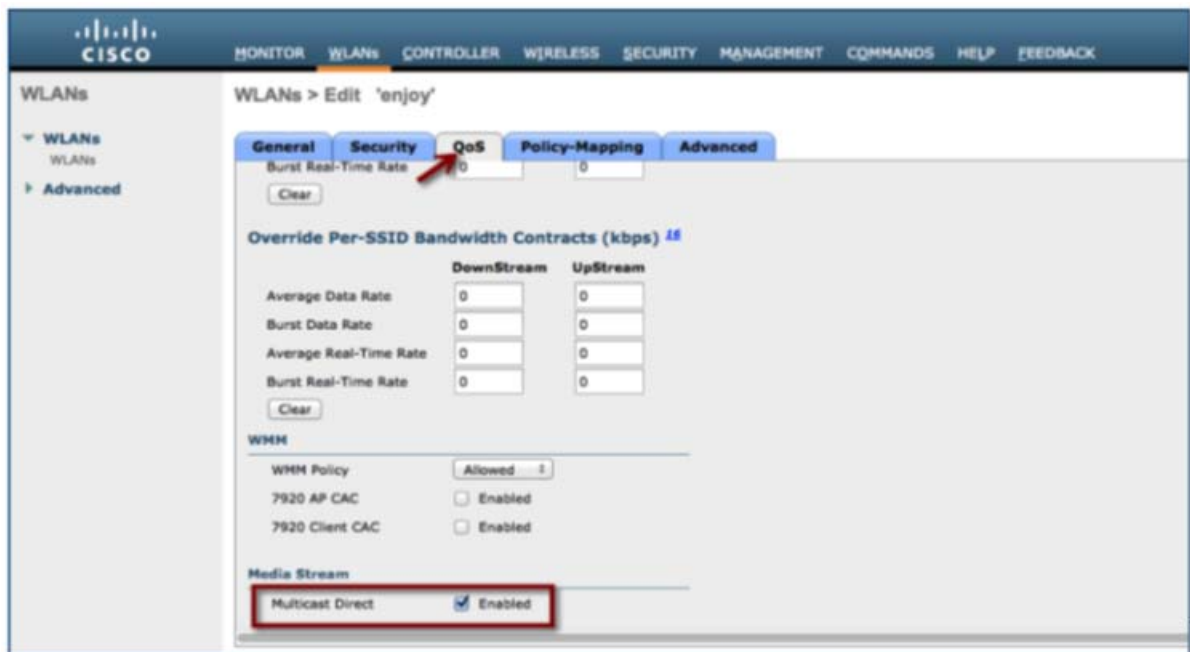
Figure 61 Enable VideoStream - Global



(Cisco Controller) >config media-stream multicast-direct ?

- enable      Enable Global Multicast to Unicast Conversion
- disable     Disable Global Multicast to Unicast Conversion

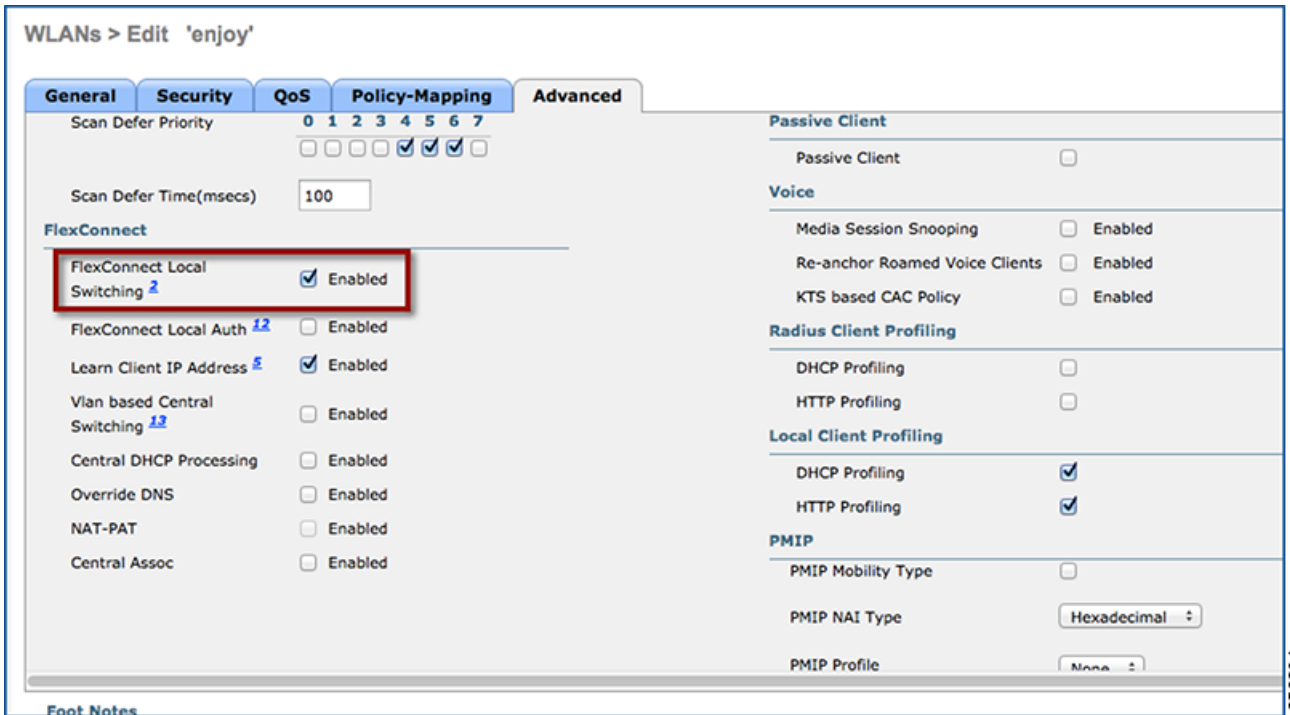
The multicast direct button under **WLAN > QoS** appears on if the feature is enabled globally.



This provides the flexibility to enable VideoStream feature per SSID and is described later in this document.

Turn on Local Switching under **WLAN > Advanced** and ensure that the APs in the setup are in FlexConnect mode.

Figure 62 Enable Local Switching on WLAN



352804



Figure 63 Change AP Mode to FlexConnect

All APs > Details for AP\_1600

General Credentials Interfaces High Availability Inventory FlexConnect Advanced

**General**

AP Name	AP_1600	Primary Software Version	8.0.72.114
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	6c:20:56:13:f6:23	Predownload Status	None
Base Radio MAC	68:86:a7:cb:c0:d0	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
<b>AP Mode</b>	<b>FlexConnect</b>	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	15.2.2.0
Operational Status	REG	IOS Version	15.3(20140203:113124)\$
Port Number	1	Mini IOS Version	7.4.1.37
Venue Group	Unspecified	<b>IP Config</b>	
Venue Type	Unspecified	IP Address	9.5.56.105
Venue Name		IPv6 Address	
Language		Static IP	<input type="checkbox"/>
Network Spectrum	731759626C780B4A4A128E3F1D98F252	Static IPv6	<input type="checkbox"/>
Interface Key			

352805

## Add Media Stream Configuration

To add a multicast stream to the controller, navigate to **Wireless > Media Stream > Streams** and click **Add New**.

Figure 64 Media Stream Configuration

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Site Configuration Ping Logout Refresh

Wireless

Media Stream > New

< Back Apply

Stream Name	Media2
Multicast Destination Start IP Address(ipv4/ipv6)	229.77.77.28
Multicast Destination End IP Address(ipv4/ipv6)	229.77.77.28
Maximum Expected Bandwidth(1 to 35000 Kbps)	500

**Resource Reservation Control(RRC) Parameters**

Select from predefined templates	Select
Average Packet Size (100-1500 bytes)	1200
RRC Periodic update	<input checked="" type="checkbox"/>
RRC Priority (1-8)	1
Traffic Profile Violation	best-effort

352806

For configuration using CLI use:

```
configure media-stream add multicast-direct <media-stream-name> <start-IP> <end-IP> [template | detail
<bandwidth> <packet-size> <Re-evaluation> video <priority> <drop|fallback>]
```

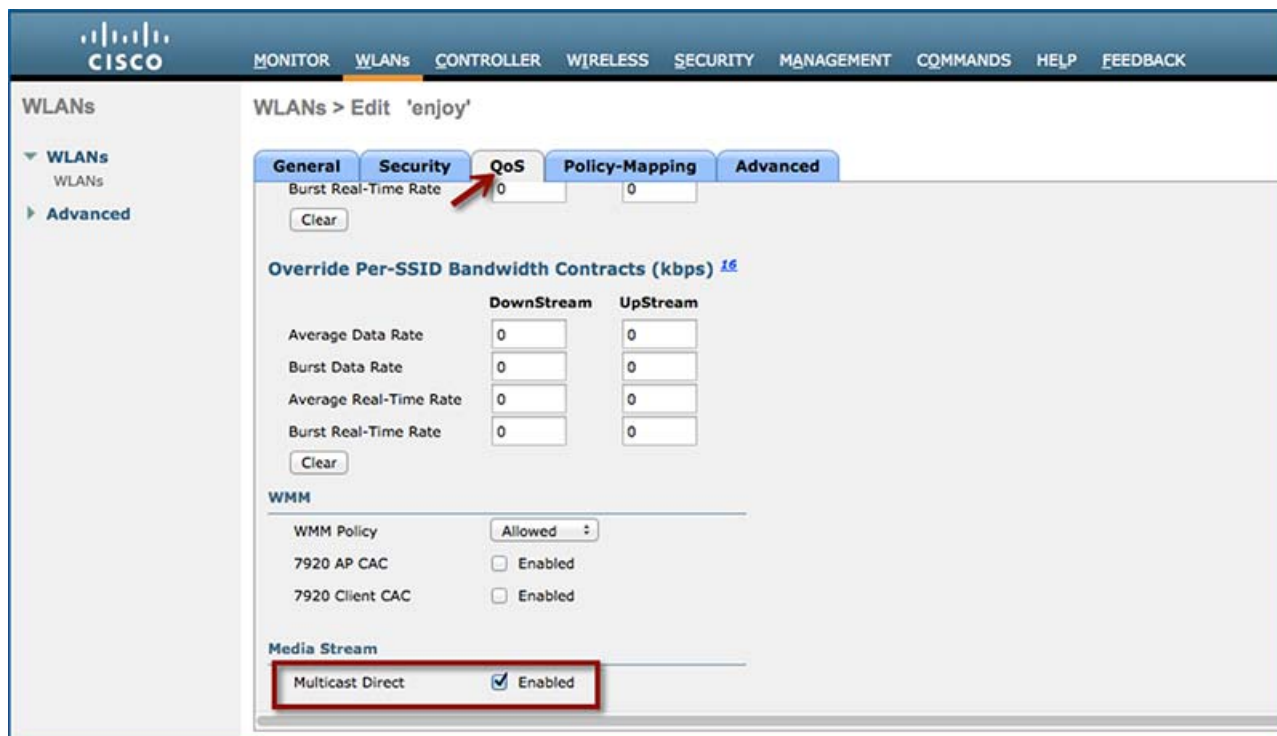
As mentioned it is necessary that the administrator is aware of the video characteristic streaming through a controller. A true balance must be drawn when the streams configuration are added. For example, if the stream bit rate varies between 1200 Kbps and 1500 Kbps the stream must be configured for a bandwidth of 1500 Kbps. If the stream is configured for 3000 Kbps then you will have lesser video client serviced by the AP. Similarly, configuring for 1000 Kbps will cause pixelization, bad audio, and bad user experience.

The multicast destination start IP address and end IP address can be the same address as shown in [Figure 64 on page 122](#). You can also configure a range of multicast address on the controller. There is a limitation of 100 on the number of multicast addresses entries or the number of stream entries that will be pushed to the APs.

## Enabling VideoStream - WLAN

One or all WLANs/SSIDs configured can be enabled for streaming video with VideoStream. This is another configuration step that can control the enabling of the VideoStream feature. Enabling or disabling the VideoStream feature is non-disruptive. Click **WLAN > <WLAN ID> > QoS**.

**Figure 65 Enable VideoStream - WLAN**



Configure the Quality of Service (QoS) to Gold (video) to stream video to wireless client at a QoS value of gold (4). This will only enable video quality of service to wireless clients joined to a configured stream on the controller. The rest of the clients will be enabled for appropriate QoS. To enable Multicast Direct on the WLAN, check the **Multicast Direct** check box as shown in [Figure 65 on page 123](#). This will enable the WLAN to service wireless clients with the VideoStream feature.

(Cisco Controller) > **config wlan media-stream multicast-direct 1 ?**

enable Enables Multicast-direct on the WLAN

disable Disables Multicast-direct on the WLAN.

All wireless clients requesting to join a stream will be assigned video QoS priority on admission. Wireless client streaming video prior to enabling the feature on the WLAN will be streaming using normal multicast. Enabling the feature switch the clients to multicast-direct automatically on the next IGMP snooping interval. Legacy multicast can be enabled on the WLAN by not checking the Multicast Direct feature. This will show that wireless clients streaming video are in Normal Multicast mode.

## Verifying VideoStream Functionality

Make sure the wireless clients are associated to the access point(s), and are configured for a correct interface. As seen in the [Figure 66 on page 124](#), there are three clients associated to one AP. All three clients have an IP address from VLAN 56 (SSID name—enjoy). The associated clients have an IP address and good uplink connectivity to the AP.

**Figure 66 Client Summary**

Client MAC Addr	IP Address	AP Name	WLAN Profile	WLAN SSID	User Name
7c:d1:c3:86:7e:dc	9.5.56.100	AP_1600	enjoy	enjoy	Unknown
88:cb:87:bd:0c:ab	9.5.56.113	AP_1600	enjoy	enjoy	Unknown
d8:96:95:02:7e:b4	9.5.56.108	AP_1600	enjoy	enjoy	Unknown

Enable streaming on the wired side by connecting a video server with a configured multicast address 229.77.77.28. Refer the following link to know how to stream from a Video Server:

[https://wiki.videolan.org/Documentation:Streaming\\_HowTo\\_New/#Streaming\\_using\\_the\\_GUI](https://wiki.videolan.org/Documentation:Streaming_HowTo_New/#Streaming_using_the_GUI)

Complete the steps:

1. Join wireless clients to the multicast streaming video.

**Note:** Use VLC player to stream and watch video.

2. Double click on the VLC icon on your desktop. Click **Media > Open Network stream**. Choose Protocol = UDP, Address = 229.77.77.28, Port = 1234 in the format **udp://@229.77.77.28:1234**.
3. Click **Play**.

L3\_Switch#**show ip mroute**

IP Multicast Routing Table

Client ACL Support

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

L - Local, P - Pruned, R - RP-bit set, F - Register flag,

T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,

X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,

U - URD, I - Received Source Specific Host Report,

Z - Multicast Tunnel, z - MDT-data group sender,

Y - Joined MDT-data group, y - Sending to MDT-data group,

V - RD & Vector, v - Vector

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(\* , 239.255.255.250), 4d20h/00:02:47, RP 0.0.0.0, flags: DC

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan56, Forward/Sparse-Dense, 4d19h/stopped

(\* , 229.77.77.28), 4d15h/00:02:44, RP 0.0.0.0, flags: DC

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan56, Forward/Sparse-Dense, 00:17:24/stopped

(\* , 224.0.1.40), 5d17h/00:02:53, RP 0.0.0.0, flags: DCL

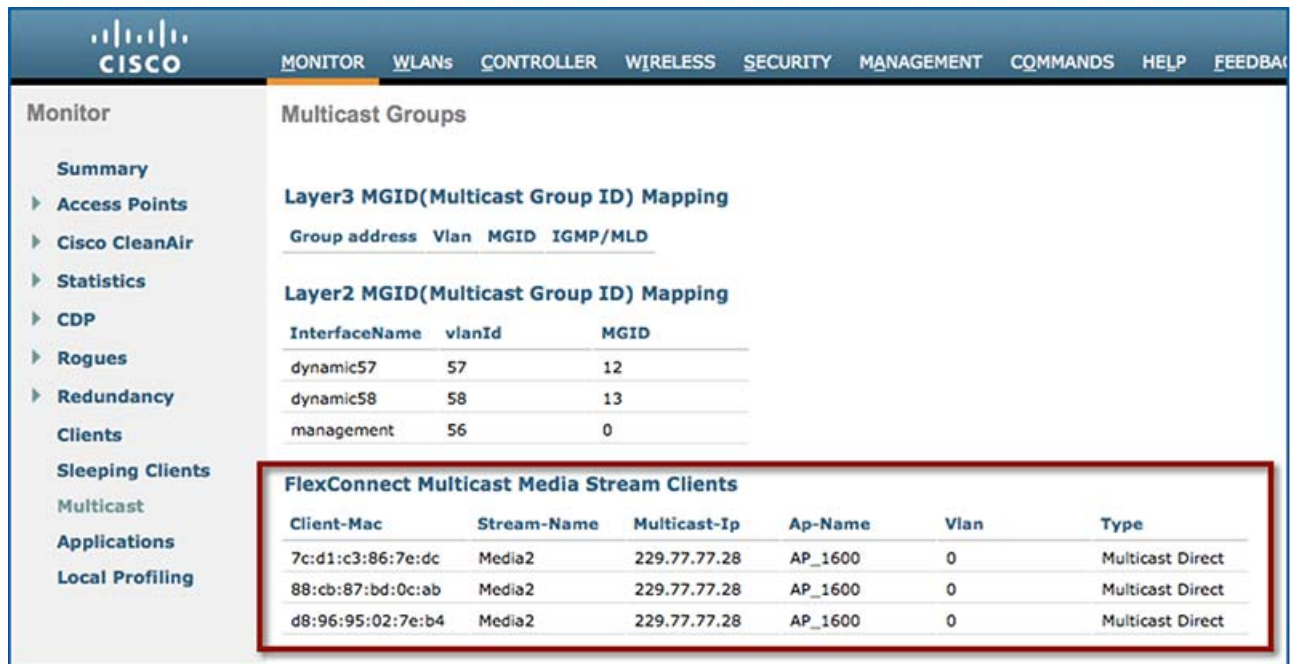
Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan56, Forward/Sparse-Dense, 5d17h/stopped

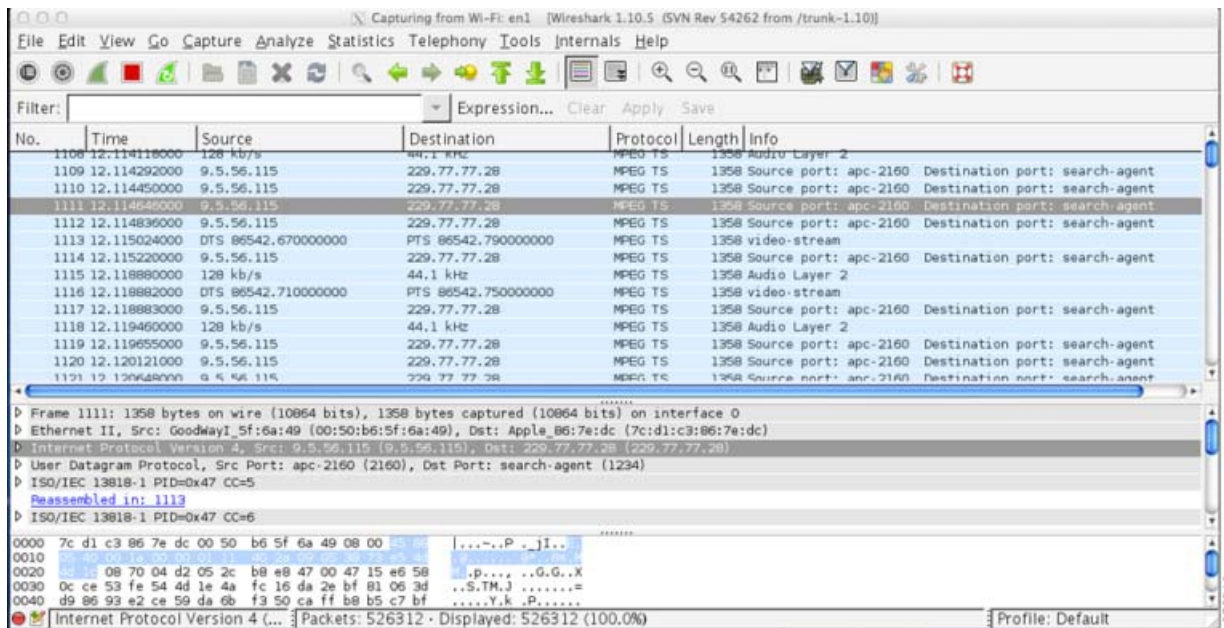
It is observed that the MAC address of the wireless clients is in a Multicast-Direct Allowed State.

Figure 67 FlexConnect VideoStream Clients



The Wireshark capture on the client shows the Multicast to Unicast Video Stream. The Ethernet header contains the MAC address of the client as the Destination MAC address, for example, 7c:d1:c3:86:7e:dc.

Figure 68 Wireshark Capture Depicting mc2uc



## Limitations

The limitations to this feature scope include:

1. There is no admission control for local switched clients' multicast video requests, which means always admit the configured video stream subscriptions as mc2uc.
2. Due to the limit of CAPWAP payload length, only the first 100 media-streams will be pushed from the controller to the AP in this release. For example, `config media-stream add multicast-direct stream1 225.0.0.1 225.0.0.10 template coarse`, is considered as one entry.
3. Roaming support is limited to adding mobile payload. Whenever the client roams to another AP, the WLC will add the entry for the client in the mc2uc table. This means that roaming in standalone mode of FlexConnect AP will not be supported for this feature.
4. Currently this feature only has IPv4 support.

## Show Commands – Controller

Some of the show commands are documented earlier in this document. The following section is only for your reference:

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

```
Number of APs..... 5
Global AP User Name..... Not Configured
Global AP Dot1x User Name..... Not Configured
```

AP Name	Slots	AP Model	Ethernet MAC	Location	Country	IP Address	Clients	DSE Location
AP1142	2	AIR-LAP1142N-A-K9	f0:f7:55:f1:75:20	default location IN		9.5.56.109	0	[0 ,0 ,0 ]
AP_2600	2	AIR-CAP2602E-N-K9	fc:99:47:d9:86:90	default location IN		9.5.56.110	0	[0 ,0 ,0 ]
AP3700	2	AIR-CAP3702E-N-K9	7c:ad:74:ff:6b:46	default location IN		9.5.56.116	0	[0 ,0 ,0 ]
AP_3600-2	2	AIR-CAP3602I-N-K9	a4:4c:11:f0:e9:dc	default location IN		9.5.56.111	0	[0 ,0 ,0 ]
AP_1600	2	AIR-CAP1602I-N-K9	6c:20:56:13:f6:23	default location IN		9.5.56.105	2	[0 ,0 ,0 ]

(Cisco Controller) **>show client summary**

```
Number of Clients..... 2
Number of PMIPv6 Clients..... 0
```

GLAN/

RLAN/



## Client ACL Support

MAC Address	AP Name	Slot	Status	WLAN	Auth Protocol	Port	Wired	PMIPv6	Role
88:cb:87:bd:0c:ab	AP_1600	1	Associated	1	Yes 802.11a	1	No	No	Local
d8:96:95:02:7e:b4	AP_1600	1	Associated	1	Yes 802.11a	1	No	No	Local

(Cisco Controller) >**show media-stream multicast-direct state**

Multicast-direct State..... enable

Allowed WLANs..... 1

(Cisco Controller) >**show media-stream group summary**

Stream Name	Start IP	End IP	Operation Status
Media1	239.1.1.1	239.2.2.2	Multicast-direct
Media2	229.77.77.28	229.77.77.28	Multicast-direct

(Cisco Controller) >**show media-stream group detail Media2**

Media Stream Name..... Media2

Start IP Address..... 229.77.77.28

End IP Address..... 229.77.77.28

RRC Parmmeters

Avg Packet Size(Bytes)..... 1200

Expected Bandwidth(Kbps)..... 500

Policy..... Admit

RRC re-evaluation..... periodic

QoS..... Video

Status..... Multicast-direct

Usage Priority..... 1

Violation..... fallback

(Cisco Controller) >**show flexconnect media-stream client summary**

Client Mac	Stream Name	Multicast IP	AP-Name	VLAN	Type
------------	-------------	--------------	---------	------	------



## Client ACL Support

```
-----
7c:d1:c3:86:7e:dc Media2      229.77.77.28  AP_1600      0  Multicast Direct
88:cb:87:bd:0c:ab Media2      229.77.77.28  AP_1600      0  Multicast Direct
d8:96:95:02:7e:b4 Media2      229.77.77.28  AP_1600      0  Multicast Direct
```

(Cisco Controller) >**show flexconnect media-stream client Media2**

```
Media Stream Name..... Media2
IP Multicast Destination Address (start)..... 229.77.77.28
IP Multicast Destination Address (end)..... 229.77.77.28
```

Client Mac	Multicast IP	AP-Name	VLAN	Type
7c:d1:c3:86:7e:dc	229.77.77.28	AP_1600	0	Multicast Direct
88:cb:87:bd:0c:ab	229.77.77.28	AP_1600	0	Multicast Direct
d8:96:95:02:7e:b4	229.77.77.28	AP_1600	0	Multicast Direct

## Show and Debug Commands – AP

- Debug ip igmp snooping group
- Debug capw mcast
- Show capwap mcast flexconnect clients
- Show capwap mcast flexconnect groups

AP\_1600#**show capwap mcast flexconnect clients**

=====

Bridge Group: 1

=====

Multicast Group Address 229.77.77.28::

MCUC List:

Number of MCUC Client: 3

88cb.87bd.0cab(Bridge Group = 1 Vlan = 0)

7cd1.c386.7edc(Bridge Group = 1 Vlan = 0)

d896.9502.7eb4(Bridge Group = 1 Vlan = 0)

-----

MC Only List:

Number of MC Only Client: 0

-----

AP\_1600#**show capwap mcast flexconnect groups**

WLAN mc2uc configuration:

WLAN ID 1 , Enabled State 1

WLAN ID 2 , Enabled State 0

WLAN ID 3 , Enabled State 0

WLAN ID 4 , Enabled State 0

WLAN ID 5 , Enabled State 0

WLAN ID 6 , Enabled State 0

WLAN ID 7 , Enabled State 0

WLAN ID 8 , Enabled State 0

WLAN ID 9 , Enabled State 0

WLAN ID 10, Enabled State 0

WLAN ID 11, Enabled State 0

WLAN ID 12, Enabled State 0

WLAN ID 13, Enabled State 0

WLAN ID 14, Enabled State 0

WLAN ID 15, Enabled State 0

WLAN ID 16, Enabled State 0

Video Group Configuration:

Group startIp 239.1.1.1 endIp 239.2.2.2

Group startIp 229.77.77.28 endIp 229.77.77.28

## FlexConnect Faster Time to Deploy

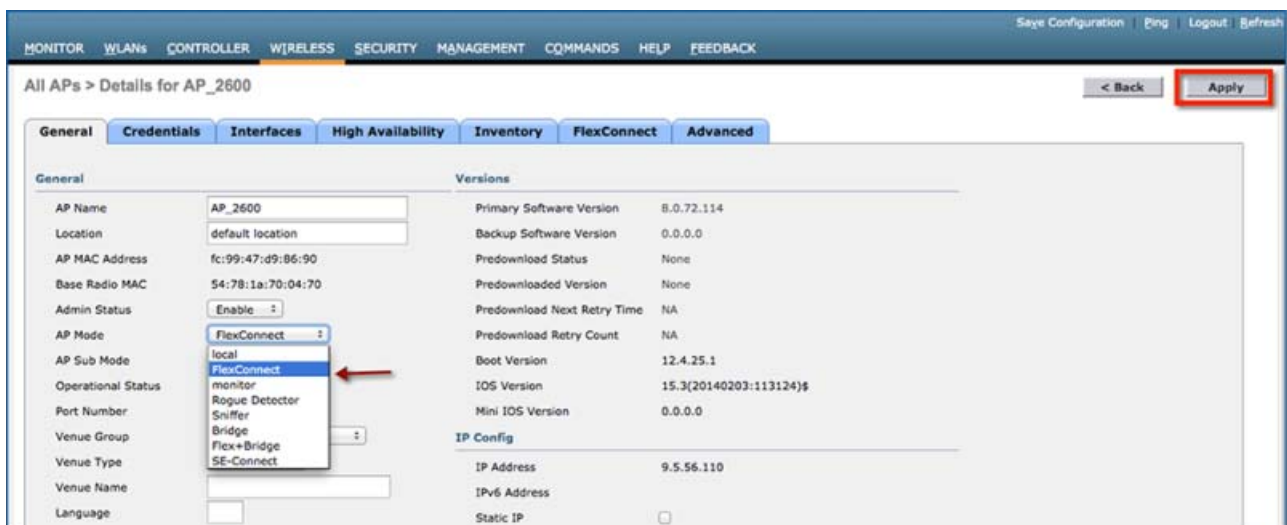
The existing system requires an AP reboot when converted from Local mode to FlexConnect mode. Once the AP boots up, it joins back the controller and subsequently all the FlexConnect configuration is pushed down to the AP. This process increases the total time to deploy a FlexConnect solution in a branch. Time to deployment is a critical differentiator for any branch deployment.

## FlexConnect Plus Bridge Mode

This feature in release 8.0 eliminates the need to reboot when the AP is converted to FlexConnect mode. When the controller sends the AP a mode change message, the AP will get converted to FlexConnect mode without requiring a reload. The AP sub mode will also be configured if the AP receives the AP sub mode payload information from the controller. With this approach, the AP entry will be maintained at the controller and there will not be any AP disassociation.

Only Local mode to Flexconnect mode conversion is supported, any other mode change will cause an AP reboot. Similarly, changing of the AP sub mode to WIPS does not need reboot, but the rest of the sub mode configuration requires AP reboot.

**Figure 69 Conversion to FlexConnect - No Reboot Required**



## FlexConnect Plus Bridge Mode

From release 8.0 onward, FlexConnect + Bridge mode allows the Flexconnect functionality across mesh APs. Flex + Bridge mode is used to enable Flexconnect capabilities on Mesh (Bridge mode) APs. Refer to the [Information about FlexConnect plus Bridge Mode](#) section in Cisco Wireless LAN Controller Configuration Guide, Release 8.0 for more details.

## Application Visibility and Control for FlexConnect

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and WLC platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following components:

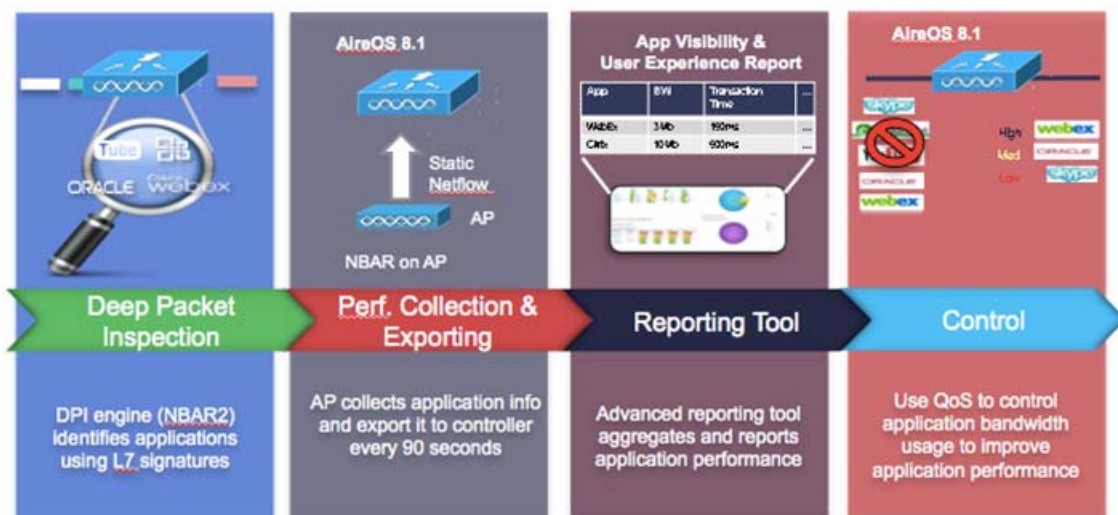
- Next-generation Deep Packet Inspection (DPI) technology, called as Network Based Application Recognition (NBAR2), allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which supports stateful L4 - L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a common flow table for all IOS features that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS), and Access Control List (ACL), which can take action based on this classification.

- Ability to Apply Mark using QoS, Drop and Rate-limit applications.

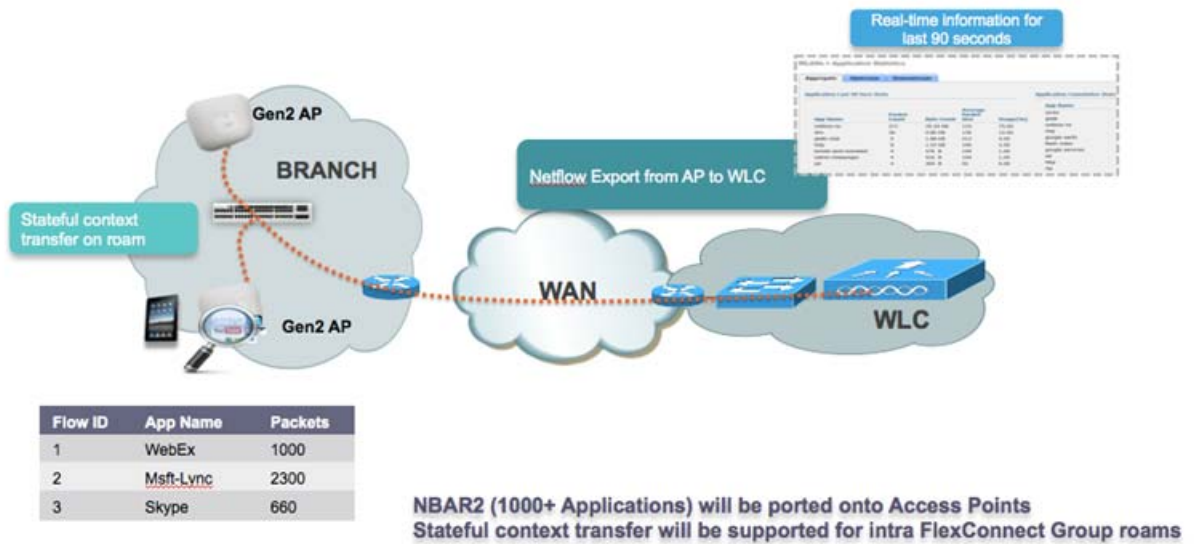
The key use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

AVC is supported on the 5520, 8540, 2500, 5508, 7500, 8500, and WiSM2 controllers on Local and FlexConnect modes (for WLANs configured for central switching only) since release 7.4. Release 8.1 introduces support for Application Visibility and Control for locally switched WLANs on FlexConnect APs on 5508, 7500, 75100, WiSM2, and vWLC.

## How AVC Works



- NBAR2 engine runs on the FlexConnect AP.
- Classification of applications happens at the access point using the DPI engine (NBAR2) to identify applications using L7 signatures.
- AP collects application information and exports it to controller every 90 seconds.
- Real-time applications are monitored on the controller user interface.
- Ability to take actions, drop, mark or rate-limit, is possible on any classified application on the FlexConnect access point.



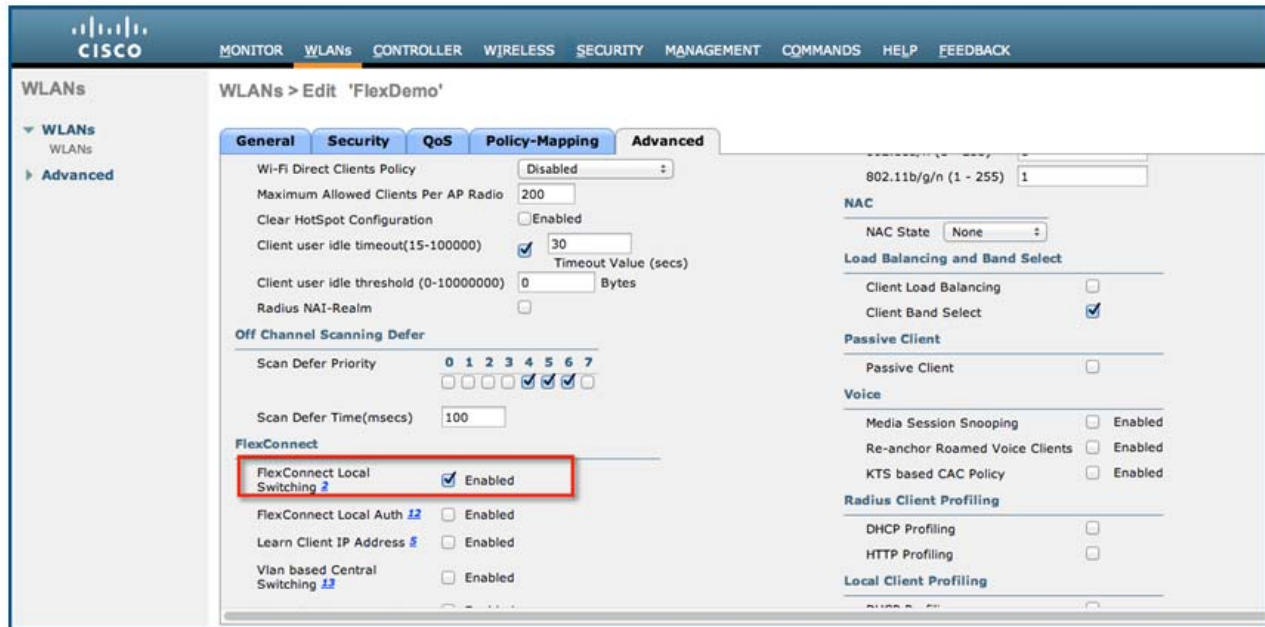
## AVC Facts and Limitations

- AVC on the FlexConnect AP can classify and take action on 1000+ different applications.
- The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- Intra FlexConnect Group roaming support.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- Multicast traffic is not supported by AVC application.
- Netflow export for FlexConnect AVC is not supported in 8.1.

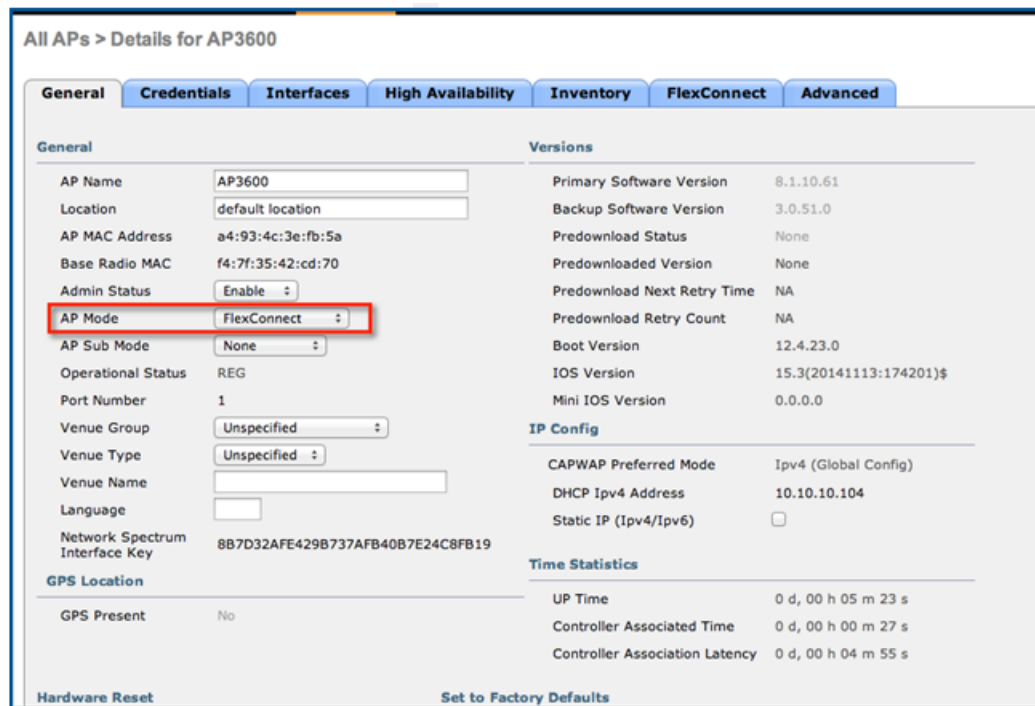
## Configuring Application Visibility

To configure the application visibility, perform these steps:

1. Open a web browser on the wired laptop, and then enter your WLC IP Address.
2. Create an OPEN WLAN with naming convention, for example, "FlexDemo".
3. Enable **FlexConnect Local Switching** on the WLAN and then click **Apply**.

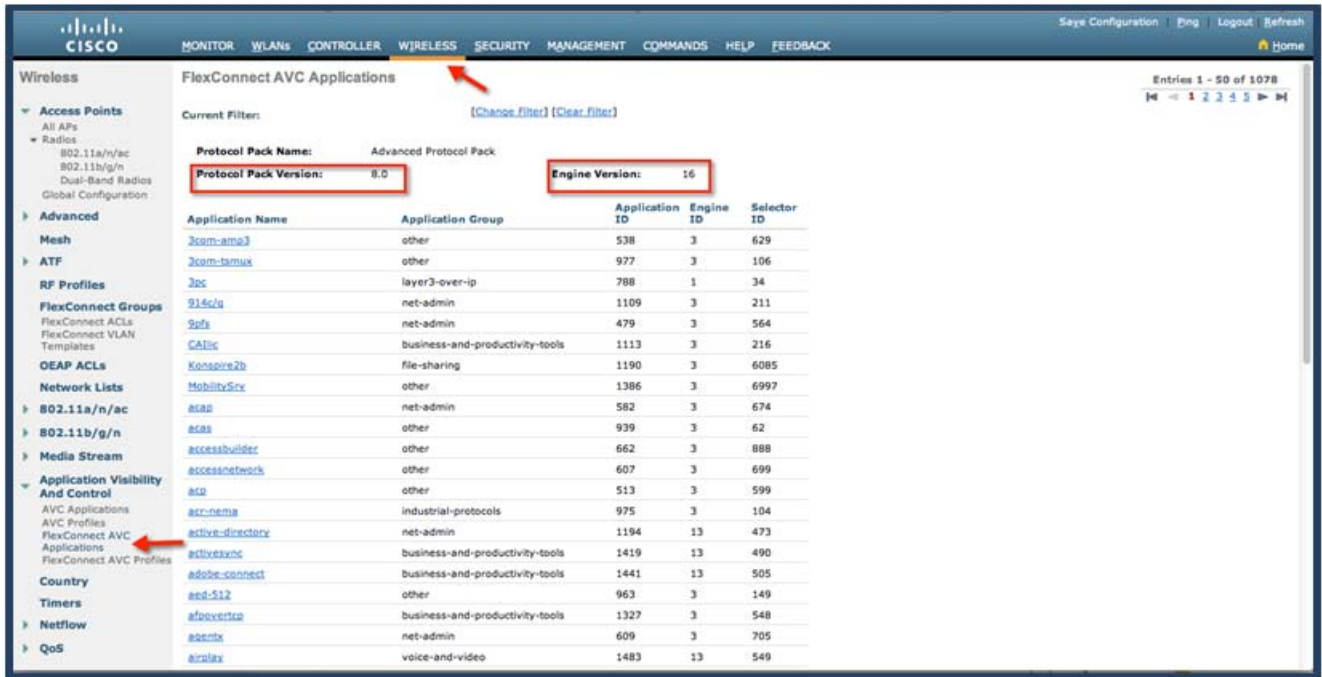


4. Make sure that the APs connected to this WLAN are among the list of supported access points for this feature.
5. Convert the AP to FlexConnect mode by selecting **FlexConnect** in the **AP Mode** drop-down menu, and then click **Apply**. The mode changes to FlexConnect without a reboot.

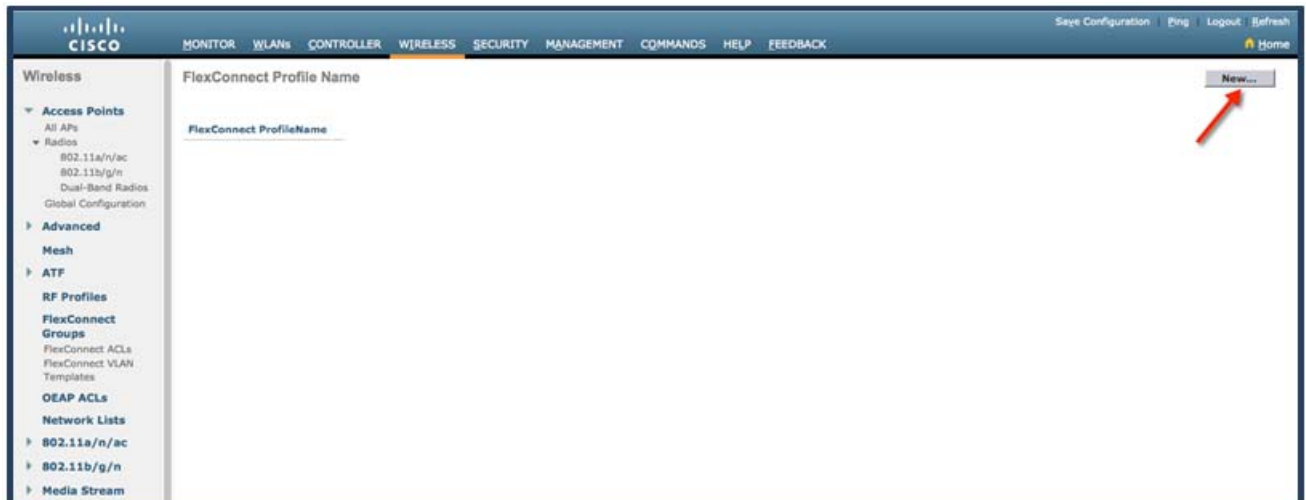


6. Create a FlexConnect Group and add the AP to the FlexConnect Group. In the following example, "FlexGroup" is the FlexConnect Group and the access point AP3600 is added to it.

7. Applications that can be identified, classified, and controlled are listed under **Wireless > Application Visibility and Control > FlexConnect AVC Applications**. The access points support Protocol Pack version 8.0 and NBAR engine version 16.

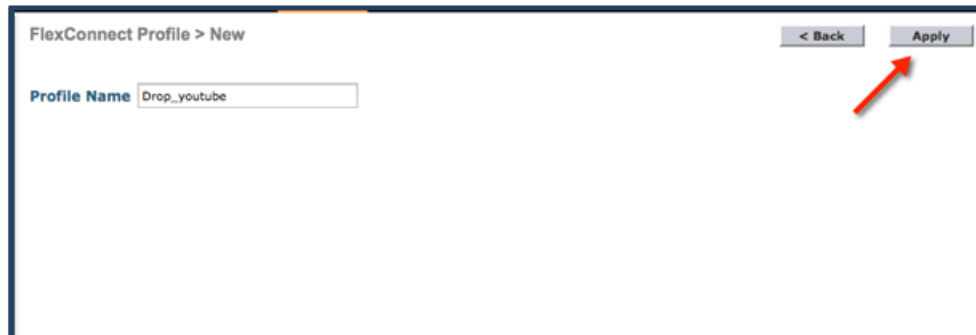


8. Create an AVC profile under **Wireless > Application Visibility and Control > FlexConnect AVC Profiles > New** with name "Drop\_youtube".



9. Click **Apply**.



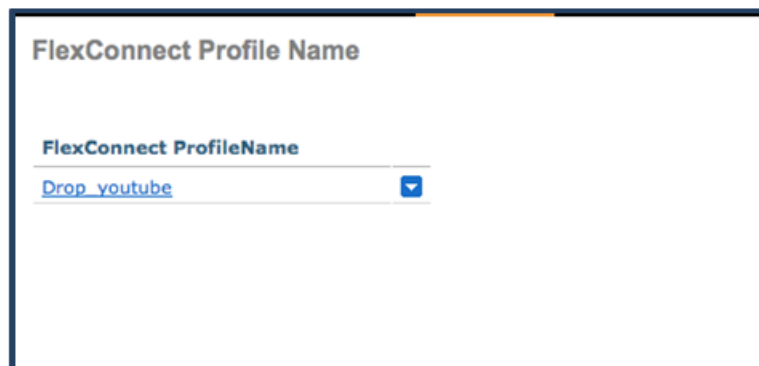


FlexConnect Profile > New

< Back Apply

Profile Name Drop\_youtube

The AVC profile is created with the new name “Drop\_youtube”.

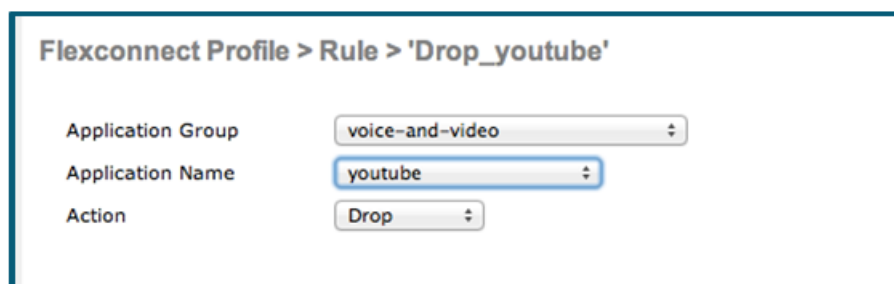


FlexConnect Profile Name

FlexConnect ProfileName

Drop\_youtube

10. Click the Profile name and then click **Add New Rule**. Select the **Application Group**, **Application Name**, and **Action**, and then click **Apply**.



Flexconnect Profile > Rule > 'Drop\_youtube'

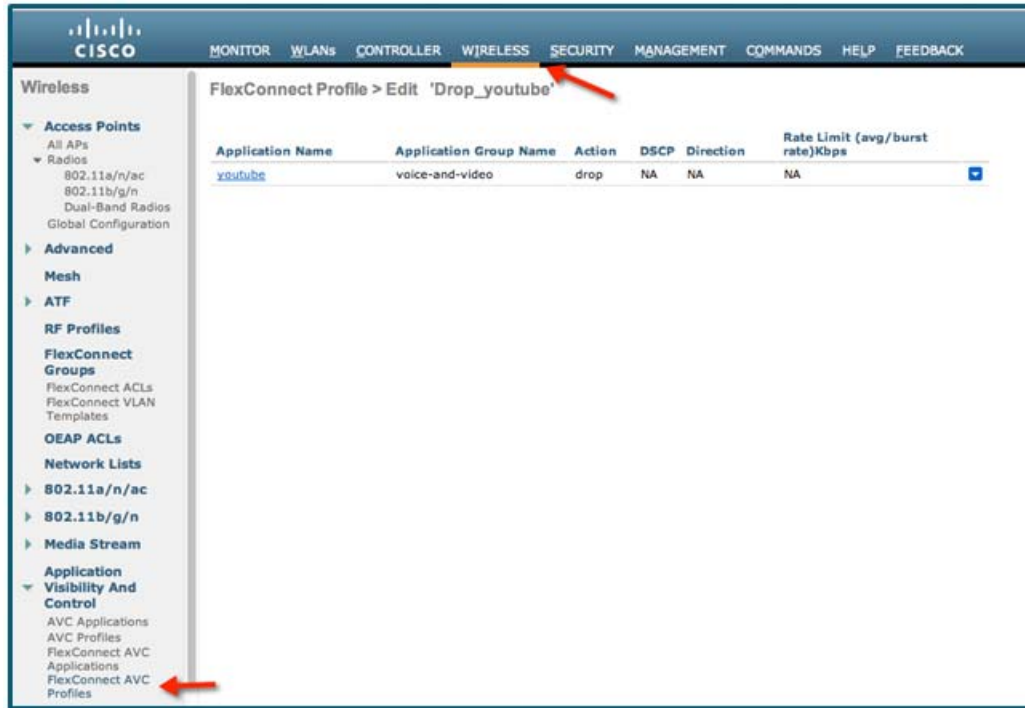
Application Group voice-and-video

Application Name youtube

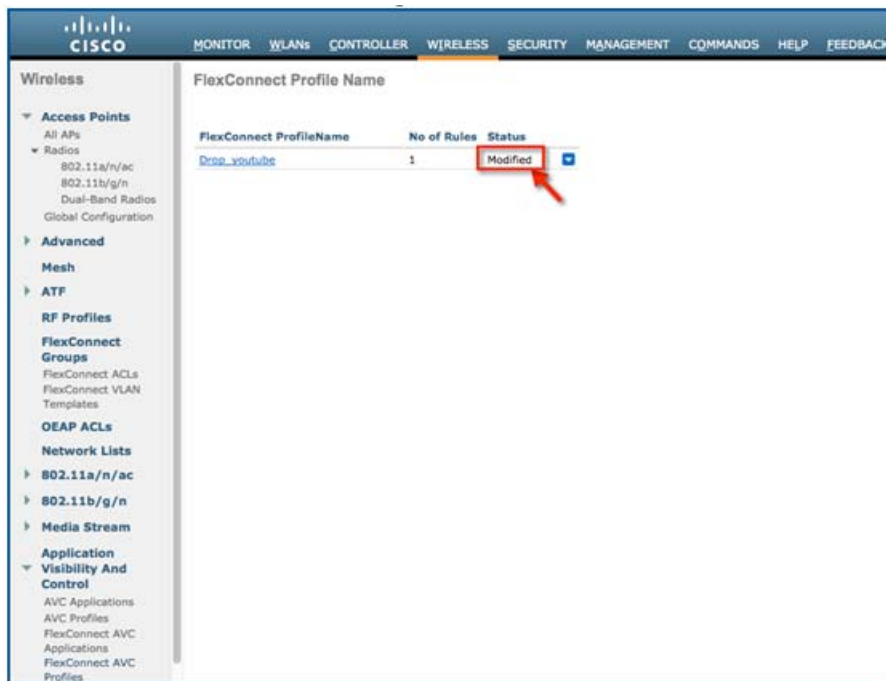
Action Drop

11. Verify that the rule is added as shown in the following figure.

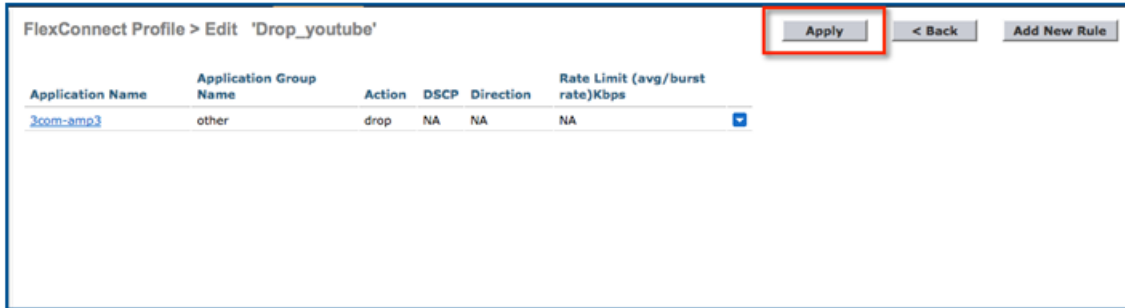
Application Visibility and Control for FlexConnect



The status of the FlexConnect AVC profile at this point is **Modified**.



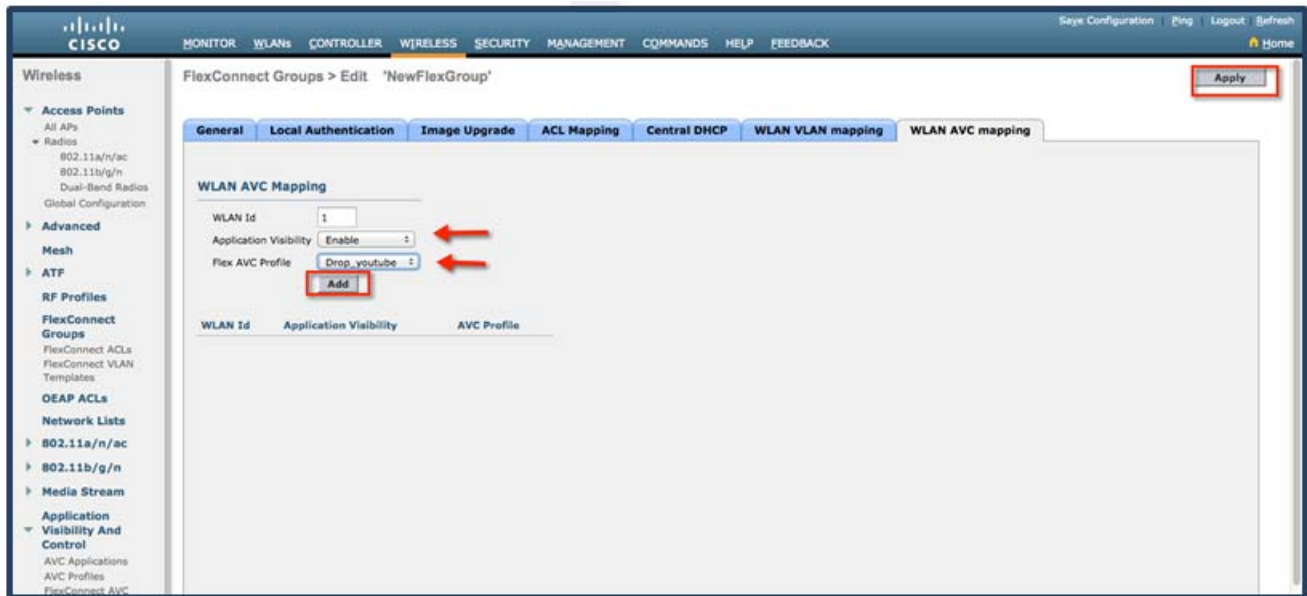
12. Select the profile and click **Apply** for the profile to be applied and to take effect.



The status of the FlexConnect AVC profile is changed to **Applied**.



13. Enable **Application Visibility** on the FlexConnect group under **Wireless > FlexConnect Group > FlexConnect Group name > WLAN AVC Mapping** by selecting the WLAN ID and choosing **Enable** from the drop-down menu.
14. Apply the FlexConnect AVC profile by selecting the profile created in the previous set from the **Flex AVC Profile** drop-down menu. Click **Add** and then click **Apply**.

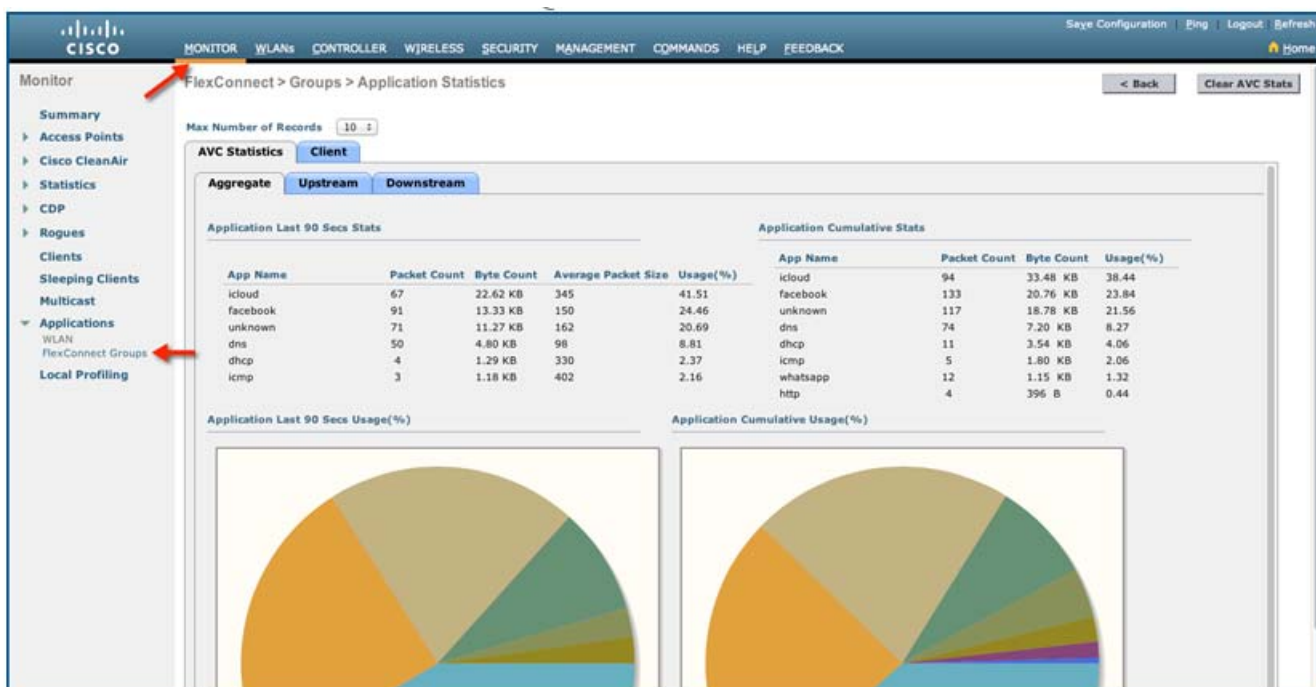


- Once AVC is enabled on the FlexConnect Group, from the associated wireless client, start different types of traffic using the applications (already installed) such as Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, Ping, Trace route, and so on.

Once traffic is initiated from the wireless client, visibility of different traffic can be observed on a per FlexConnect Group and per client basis. This provides the administrator a good overview of the network bandwidth utilization and type of traffic in the network per client and per branch site

- To check the visibility globally for all WLANs on a FlexConnect Group, click **Monitor > Applications > FlexConnect > FlexConnect Groups** and then select the FlexConnect group created earlier.

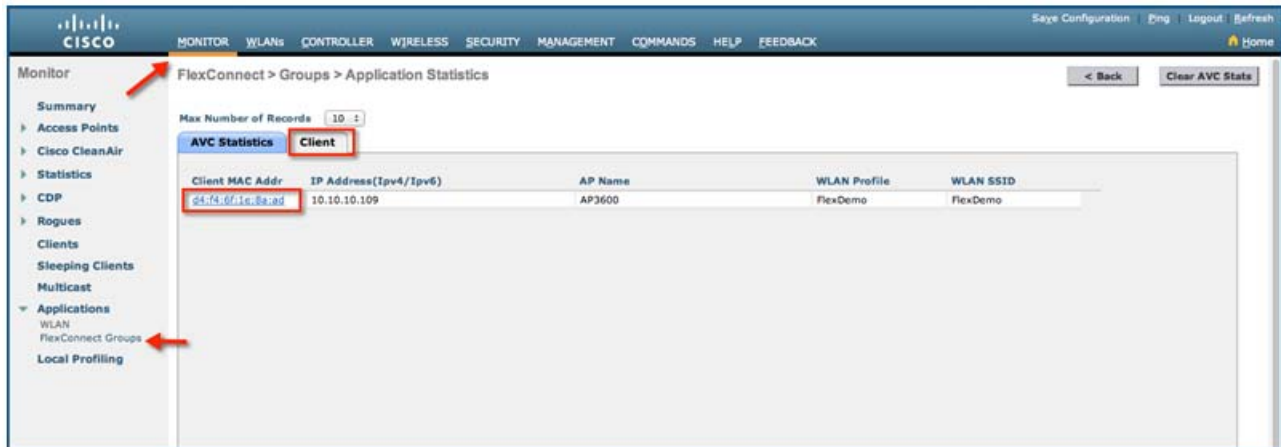
The following screen is visible which lists aggregate data for the top 10 applications running on that particular FlexConnect group.



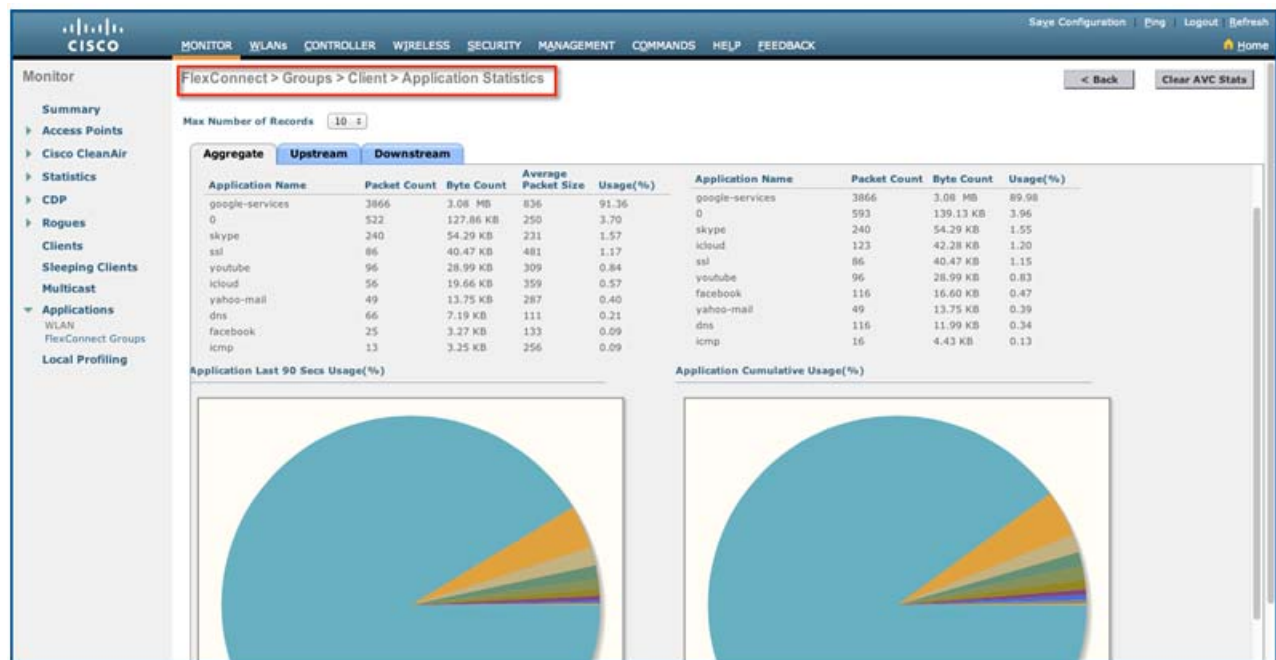
This page provides more granular visibility per FlexConnect Group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect Group from the same page by clicking the **Upstream** and **Downstream** tabs.

**Note:** The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the **Max Number of Records** field on this page. The default value is 10.

- To have more granular visibility of the top 10 applications per client on a particular locally switched WLAN where AVC visibility is enabled, click **Monitor > Applications > FlexConnect Group > FlexConnect Group name > Clients**. Then, click any individual client MAC entry listed on that page.



After clicking on an individual client MAC entry, the client details page appears.



This page provides further granular stats per client associated on locally switched WLANs, where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group as in this example. The page lists the top 10 applications in last the 90 seconds as well as cumulative stats for top 10 applications.

18. You can view upstream and downstream stats individually per client from the same page by clicking the **Upstream** and **Downstream** tabs.

**Note:** The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the **Max Number of Records Field** on this page. The default value is 10.

19. You can clear the AVC stats for the particular client by clicking the **Clear AVC Stats** button.

Now, if you open [YouTube](#), from wireless clients, you will observe that client cannot play any YouTube videos. Also, if applicable, open your Facebook account and try to open any YouTube video. You will observe YouTube videos cannot be played. Because YouTube is blocked in the FlexConnect AVC profile, and AVC profile is mapped to WLAN on the FlexConnect Group. You cannot access YouTube videos via browser, or even via YouTube application or from any other website.

**Note:** If your browser was already open with [YouTube](#), refresh the browser for the AVC profile to take effect.

## VLAN Support / Native VLAN on FlexConnect Group

### Feature Introduction

Prior to release 8.1, VLAN support and Native VLAN ID configuration is available on a per FlexConnect AP basis.

To consolidate the configurations for all the FlexConnect APs at each branch, ease the process of configuration and management, as well as to bring about consistency of configuration within a given branch, this configuration is provided at the FlexConnect Group starting release 8.1.

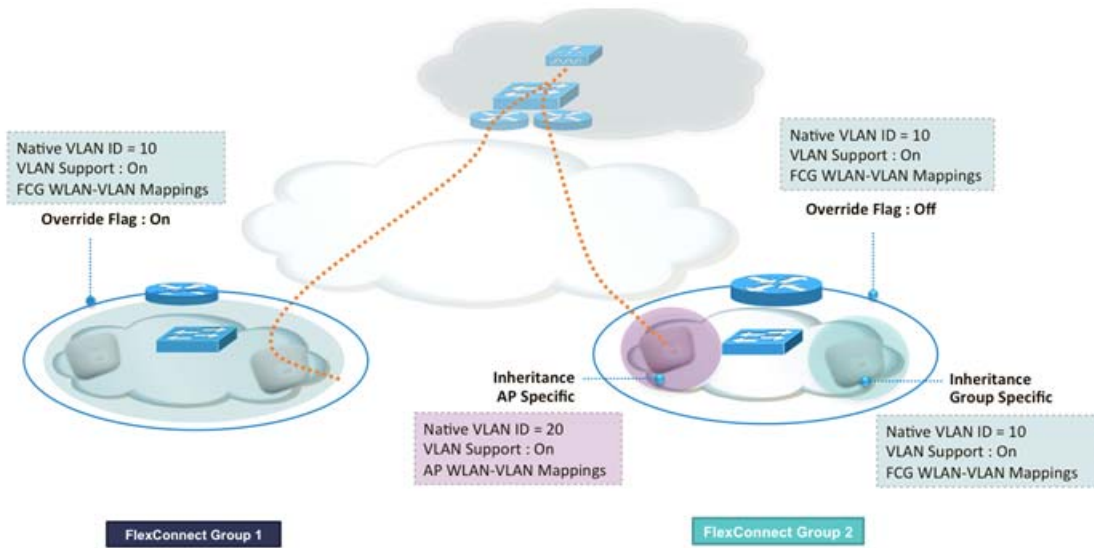
This feature is supported on all WLCs and APs supporting FlexConnect mode in release 8.1.

### VLAN Support/ Native VLAN on FlexConnect Group

- This feature provides the ability to configure VLAN Support and Native VLAN ID on a FlexConnect group.
- Additionally, an override option is also provided at the group.
- The override option overrides the VLAN Support and Native VLAN ID parameters previously configured on the access points, changes the inheritance level at the AP to “Group-specific”, removes AP specific WLAN-VLAN mappings, and pushes the group-specific configuration including WLAN-VLAN mapping configured on the group to all the APs in that group.
- When the override flag is set at the FlexConnect group, modification of VLAN Support, Native VLAN ID, WLAN-VLAN Mappings, and Inheritance-Level at the AP is not allowed.
- In addition to the above-mentioned configurations, an additional Inheritance-Level configuration is provided at the FlexConnect AP. This needs to be set to “Make VLAN AP specific” to configure any AP-Specific VLAN Support, Native VLAN ID, and VLAN-WLAN mappings on the AP. Note that the user can modify this knob only when the override flag at the group is disabled.

In the following example, two FlexConnect groups have been configured. FlexConnect group 1 has the override flag enabled. As a result, all the APs in this group inherit the VLAN configuration from the group including the VLAN Support, Native VLAN, and WLAN-VLAN mappings. FlexConnect group 2 has the override flag disabled. Thus, the APs in this group will follow the inheritance based on the AP and group specific configuration and inheritance order. An AP that has inheritance set to AP-Specific will have the AP-specific parameters in action. An AP that has inheritance set to Group-specific will inherit the configuration from the group.

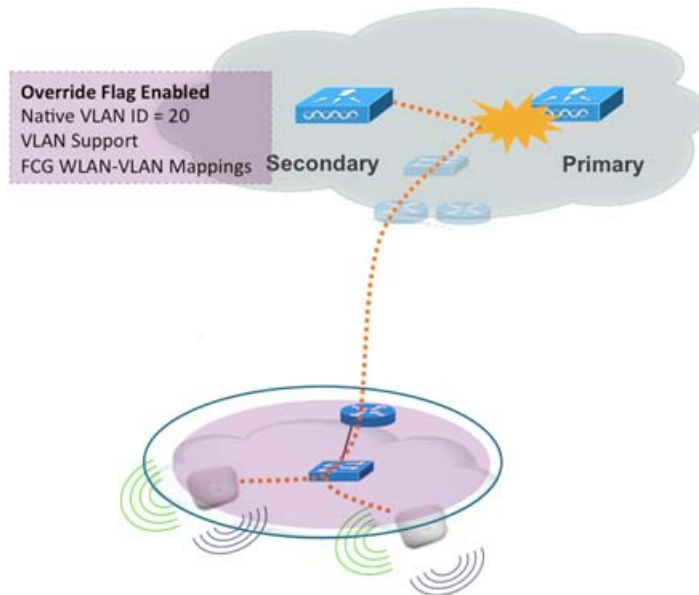
VLAN Support / Native VLAN on FlexConnect Group



AP Fallback Behavior

With Override Flag Enabled on Secondary Controller

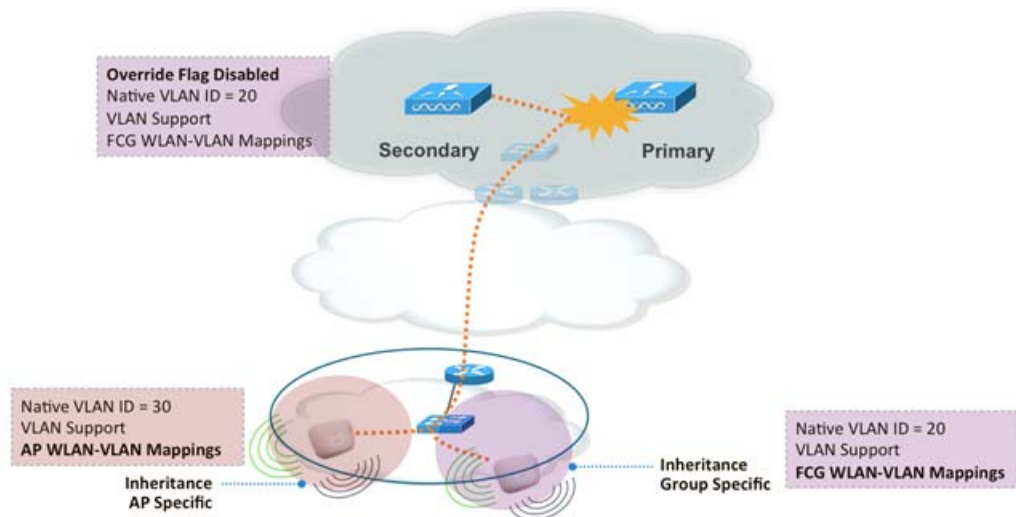
When the override flag is enabled on the secondary controller, the APs inherit the configuration from the secondary controller irrespective of the configuration on the primary controller and the APs.





## With Override Flag Disabled on Secondary Controller

With the override flag disabled on the secondary controller, the APs that were configured with AP-specific parameters retain their AP specific configuration unless specifically changed on the secondary controller on a per AP basis. The APs, which inherit their configuration from the FlexConnect group on the primary, will inherit their configuration from the FlexConnect group on the secondary controller based on the configuration of the secondary FlexConnect group. Note that the FlexConnect group override flag configuration is not stored on the AP.



## Upgrade and Downgrade Considerations

When upgrading to release 8.1, the existing FlexConnect group configuration follows the following rules:

- Native VLAN ID on the FlexConnect group is set to 1
- VLAN support on the FlexConnect group is disabled
- Override flag on the FlexConnect group is disabled

When downgrading from release 8.1:

- VLAN Support and Native VLAN ID is on a per AP basis
- WLAN-VLAN mappings follow the previous inheritance model

## Configuring VLAN Support / Native VLAN Using Web UI

To configure VLAN Support/ Native VLAN from the GUI, perform these steps:

1. Go to **Wireless > FlexConnect Groups > 'FlexConnect Group Name' > WLAN VLAN Mapping**.
2. Check the **VLAN Support** check box, enter a **Native VLAN ID** in the box provided, and check the **Enable Override Native VLAN on AP** check box as shown in the following figure.

The knob for **Override Native VLAN on AP** does the following:

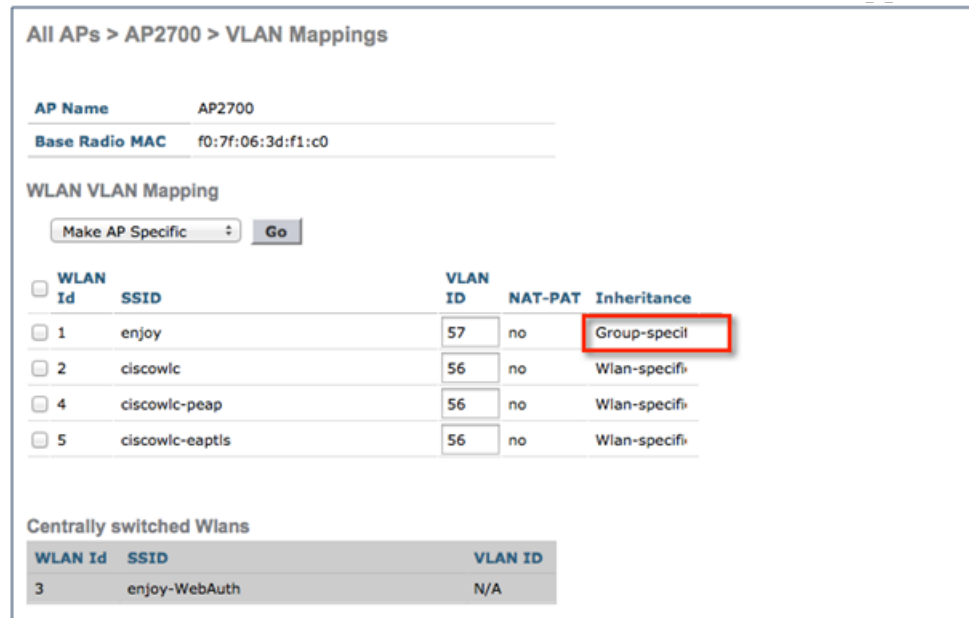
- Overrides the **VLAN Support** and **Native VLAN ID** parameters previously configured on the access points.

The screenshot shows the Cisco FlexConnect Groups configuration interface. The 'WLAN VLAN mapping' tab is active, and a red box highlights the 'VLAN Support' and 'Override Native VLAN on AP' options, both checked. The 'Native VLAN ID' is set to 10. Below, the 'WLAN VLAN Mapping' section shows a table with one entry: WLAN Id 1, FlexDemo, and Vlan 11.

- Changes the **Inheritance Level** at the AP to “Group-specific”.

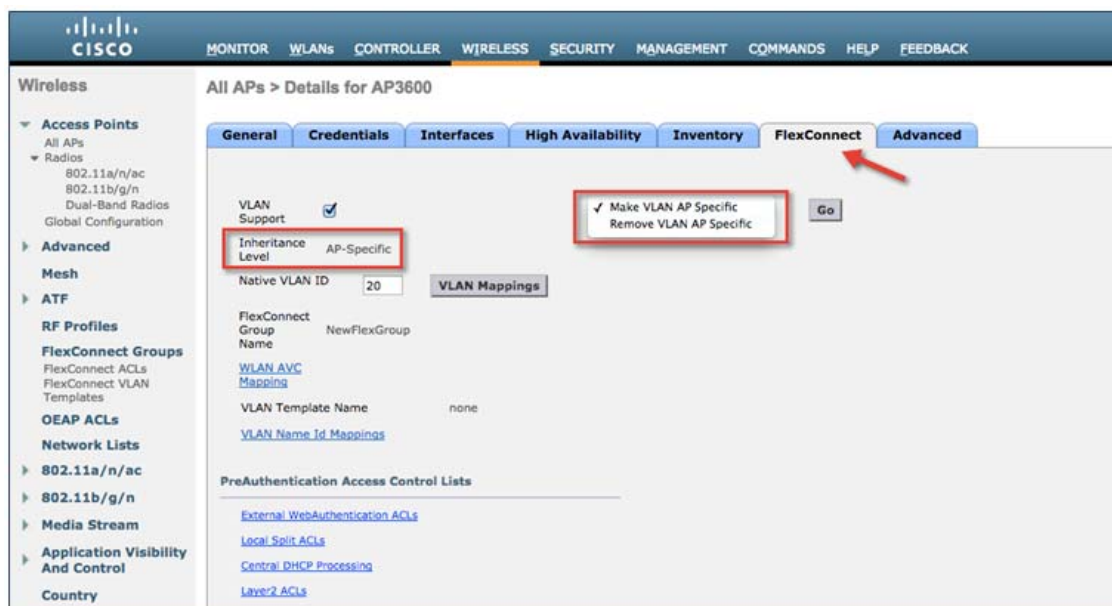
The screenshot shows the Cisco FlexConnect configuration interface for 'All APs > Details for AP2700'. The 'Advanced' tab is active, and a red box highlights the 'Inheritance Level' dropdown menu, which is set to 'Group-Specific'. Other options include 'VLAN Support' checked, 'Native VLAN ID', and 'VLAN Mappings'.

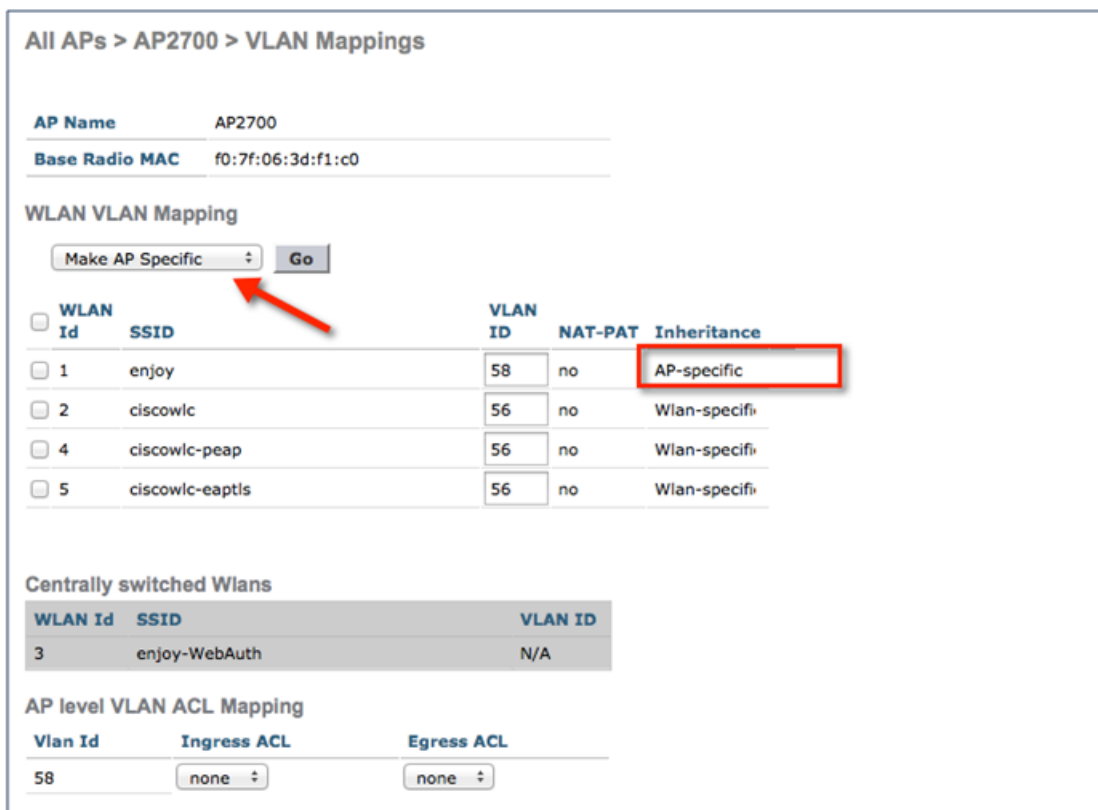
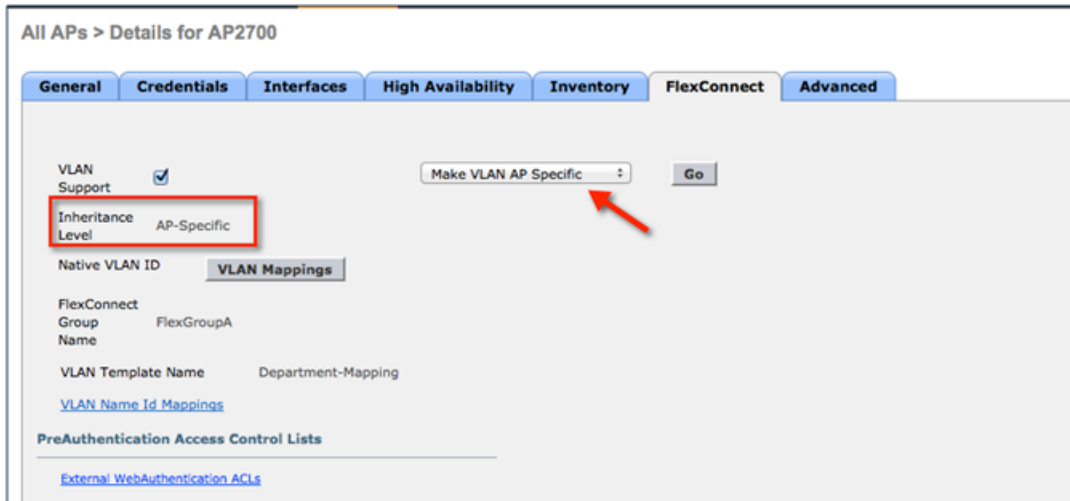
- Removes AP Specific WLAN-VLAN Mappings.
- Pushes the group-specific configuration including WLAN-VLAN Mapping configured on the group to all the APs in that group.



**Note:** When the override flag is set at the FlexConnect Group, modification of VLAN Support, Native VLAN ID, WLAN-VLAN Mappings, and Inheritance-Level at the AP is not allowed.

3. In addition to the above-mentioned configurations, an additional Inheritance-Level configuration is provided at the FlexConnect AP. Set this to **Make VLAN AP specific** to configure any AP-Specific VLAN Support, Native VLAN ID, and VLAN-WLAN mappings on the AP. Note that the user can modify this knob only when the override flag at the group is disabled.





## Configuring VLAN Support / Native VLAN Using CLI

To configure FlexConnect Group-Specific VLAN Support, Native VLAN ID, and Override flag, the following CLIs can be used:

- Enable or disable VLAN Support at the FlexConnect Group

## FlexConnect Client Troubleshooting

- ```
config flexconnect group <groupName> vlan <enable / disable>
```

  - Configure Native VLAN ID at the FlexConnect Group
- ```
config flexconnect group <groupName> vlan native <vlan_id>
```

  - Configure Override flag at the FlexConnect Group
- ```
config flexconnect group <groupName> vlan override-native-ap <enable / disable>
```

To configure the AP-specific configuration, the following CLIs can be used:

- Existing CLI to Configure VLAN Support at FlexConnect AP
- ```
config ap flexconnect vlan <enable/disable> <AP Name>
```

  - Existing CLI to Configure Native VLAN ID at FlexConnect AP
- ```
config ap flexconnect vlan native <vlan-ID>
```

  - New CLI to Remove Native VLAN ID configuration at FlexConnect AP
- ```
config ap flexconnect vlan native remove <AP Name>
```

The following show commands can be used to view the VLAN Support, Native VLAN ID and Override flag configuration at the FlexConnect Group:

(Cisco Controller) **>show flexconnect group detail NewFlexGroup**

```
Number of AP's in Group: 1
a4:93:4c:3e:fb:5a      AP3600      Joined      Flexconnect
<snip>
Group-Specific Vlan Config:
Vlan Mode..... Enabled
Native Vlan..... 10
Override AP Config..... Disabled
<snip>
```

The following show commands can be used to view the Inheritance level, VLAN Support, and Native VLAN ID configuration at the FlexConnect AP:

(Cisco Controller) **>show ap config general AP3600**

```
<snip>
Native Vlan Inheritance: ..... AP
FlexConnect Vlan mode :..... Enabled
  Native ID :..... 10
  WLAN 1 :..... 11 (Group-Specific)
FlexConnect VLAN ACL Mappings
FlexConnect Group..... NewFlexGroup
Group VLAN ACL Mappings
<snip>
```

## FlexConnect Client Troubleshooting

In 8.1, you can debug the client connectivity issue on the access point (AP) by entering a particular MAC address of a client from the controller console. Also, you can debug the client connectivity issue across the branch site without entering debug commands on multiple APs or enabling multiple debugs. A single debug command should enable this functionality.

### Key Enhancements

- Ability to track a given client in a branch

## FlexConnect Client Troubleshooting

- Central and local authentication support
- Provide AP and group level client troubleshooting
- Complete client life cycle support
- Maximum four clients per FlexConnect AP or FlexConnect group
- Support for debugging in roaming scenarios within FlexConnect group

## Debug per AP

From the WLC CLI, run the following command to enable the debug per AP:

```
debug flexconnect client ap <AP-Name>add <MAC addr1>
```

```
(POD6-WLC) >debug flexconnect client ap POD6-AP3600 ?
add          Configures the client mac addresses on AP for debug
delete       Deletes the client mac addresses on AP
syslog       Configures syslog server for debug logging

(POD6-WLC) >debug flexconnect client ap POD6-AP3600 add aa:bb:cc:dd:ee:ff
```

## Debug per FlexConnect Group (FCG)

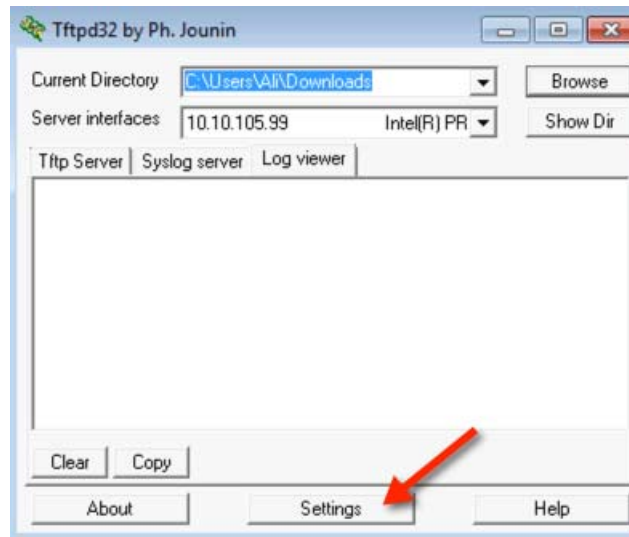
From the WLC CLI, run the following command to enable the debug per FCG:

```
debug flexconnect client group <group-name> add/delete <addr1> { <addr2> | <addr3> | <addr4>}
```

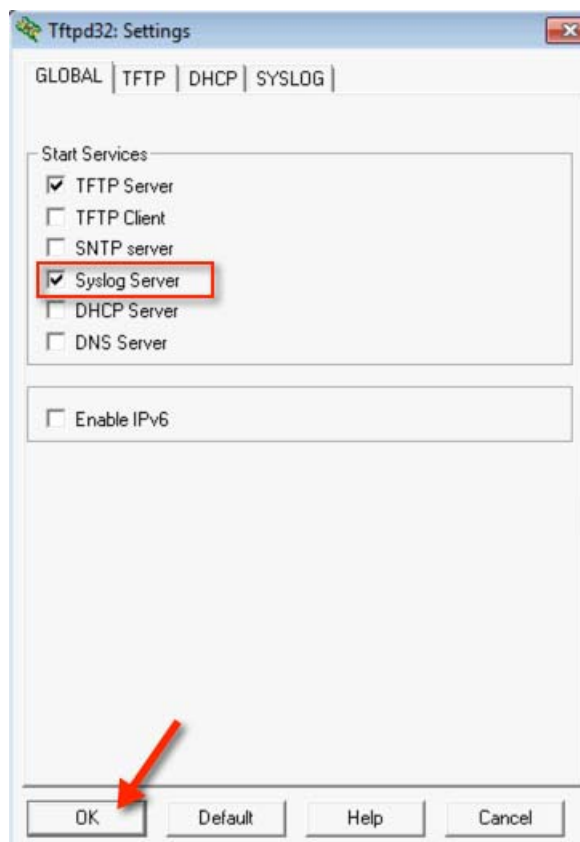
```
(POD6-WLC) >debug flexconnect client group pod6-flex add aa:bb:cc:dd:ee:ff
```

## Enabling Syslog on FlexConnect AP and FlexConnect Group

1. Open the tftp32 application  installed on your PC.
2. Click **Settings**.



3. Check the **Syslog Server** check box to enable the application as a syslog server and then click **OK**.



4. Go to the WLC CLI and set the syslog server for the debugs by running the following commands:



## Web Links

## Syslog Per FlexAP

```
(POD6-WLC) >debug flexconnect client ap POD6-AP3600 syslog 10.10.60.YYY
```

## Syslog Per FlexConnect Group

```
(POD6-WLC) >debug flexconnect client group pod6-flex syslog 10.10.60.YYY
```

The **show debug** command on WLC CLI verifies that the syslog is configured.

```
(POD6-WLC) >show debug
MAC debugging ..... disabled
Debug Flags Enabled:

Flex-AP Client Debugging ..... enabled

-----
AP Name                               Syslog IP Address           Mac Addresses
-----
POD6-AP3600                           10.10.60.51                aa:bb:cc:ff:ee:10
                                      aa:bb:cc:dd:ee:ff

Flex-Group Client Debugging ..... enabled

-----
Group Name                             Syslog IP Address           Mac Addresses
-----
pod6-flex                               10.10.60.51                aa:bb:cc:dd:ee:ff
```

The debug logs can be viewed on the syslog server file and on the AP console.

## Web Links

- Cisco WLAN Controller Information:  
<http://www.cisco.com/c/en/us/products/wireless/4400-series-wireless-lan-controllers/index.html>  
<http://www.cisco.com/c/en/us/products/wireless/2000-series-wireless-lan-controllers/index.html>
- Cisco NCS Management Software Information:  
<http://www.cisco.com/c/en/us/products/wireless/prime-network-control-system-series-appliances/index.html>
- Cisco MSE Information: <http://www.cisco.com/c/en/us/products/wireless/mobility-services-engine/index.html>
- Cisco LAP Documentation: <http://www.cisco.com/c/en/us/products/wireless/aironet-3500-series/index.html>

## Terminology

- APM—AP Manager Interface
- Dyn—Dynamic Interface
- Management—Management Interface
- Port—Physical Gbps port
- WiSM-2—Wireless Service Module
- AP—Access Point
- LAG—Link Aggregation
- SPAN—Switch Port Analyzer

## FAQ

- RSPAN—Remote SPAN
- VACL—VLAN Access Control List
- DEC—Distributed Etherchannel
- DFC—Distributed Forwarding Card
- OIR—Online Insertion and Removal
- VSL—Virtual Switch Link
- ISSU—In Service Software Upgrade
- MEC—Multichassis Ether Channel
- VSS—Virtual Switch System
- WCS—Wireless Control System
- NAM—Network Analysis Module
- IDSM—Intrusion Detection Service Module
- FWSM—Firewall Service Module
- STP—Spanning Tree Protocol
- VLAN—Virtual LAN
- SSO—Stateful Switchover
- WCP—Wireless Control Protocol
- WiSM-2—Wireless Service Module-2

## FAQ

Q. If I configure LAPs at a remote location as FlexConnect, can I give those LAPs a primary and secondary controller?

Example: There is a primary controller at site A and a secondary controller at site B. If the controller at site A fails, the LAP does failover to the controller at site B. If both controllers are unavailable does the LAP fall into FlexConnect standalone mode?

A. Yes. First the LAP fails over to its secondary. All WLANs that are locally switched have no changes, and all that are centrally switched just have the traffic go to the new controller. And, if the secondary fails, all WLANs that are marked for local switching (and open/pre-shared key authentication/you are doing AP authenticator) remain up.

Q. How do access points configured in Local mode deal with WLANs configured with FlexConnect Local Switching?

A. Local mode access points treat these WLANs as normal WLANs. Authentication and data traffic are tunneled back to the WLC. During a WAN link failure this WLAN is completely down and no clients are active on this WLAN until the connection to the WLC is restored.

Q. Can I do web authentication with Local switching?

A. Yes, you can have an SSID with web-authentication enabled and drop the traffic locally after web-authentication. Web-authentication with Local switching works fine.

Q. Can I use my Guest-Portal on the Controller for an SSID, which is handled locally by the H REAP? If yes, what happens if I lose connectivity to the controller? Do current clients drop immediately?

A. Yes. Since this WLAN is locally switched, the WLAN is available but no new clients are able to authenticate as the web page is not available. But, the existing clients are not dropped off.

Q. Can FlexConnect certify PCI compliance?

A. Yes. FlexConnect solution supports rogue detection to satisfy PCI compliance.

## Cisco Support Community - Featured Conversations

[Cisco Support Community](#) is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Below are just some of the most recent and relevant conversations happening right now.



The screenshot displays the Cisco Support Community interface. At the top, it features the Cisco logo and the text "Discussions Happening Now in The Cisco Support Community". Below this, a call to action says "Want to see more? Join us by clicking [here](#)". A list of featured discussions follows, each with a right-pointing arrow, the topic title, the author's name, the number of replies, and the time since the post was made. The discussions listed are: "WLAN design guide for branch office" by gariup.guido (12 Replies, 10 months, 1 week ago); "Flex 7500 supported RADIUS Servers" by jburk at pmm-i.com (2 Replies, 9 months, 2 weeks ago); "Cisco Flex 7500 Series Wireless..." by dvaggalis (3 Replies, 1 year, 1 month ago); "ASK THE EXPERTS:Branch Office Wireless..." by ciscomoderator (25 Replies, 1 year, 5 months ago); and "HREAP Scalability - Clients" by wirelessdeploy (2 Replies, 1 year, 1 month ago). At the bottom of the list are two buttons: "Start A New Discussion" and "Subscribe" with a RSS icon. A vertical ID number "350543" is visible on the right side of the screenshot.

## Related Information

- [HREAP Design and Deployment Guide](#)
- [Cisco 4400 Series Wireless LAN Controllers](#)
- [Cisco 2000 Series Wireless LAN Controllers](#)
- [Cisco Wireless Control System](#)
- [Cisco 3300 Series Mobility Services Engine](#)
- [Cisco Aironet 3500 Series](#)
- [Cisco Secure Access Control System](#)
- [Technical Support & Documentation - Cisco Systems](#)