

FlexConnect Wireless Branch Controller Deployment Guide

Last Updated: December, 2017

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.



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.

The Cisco Flex 7500 series (Figure 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.



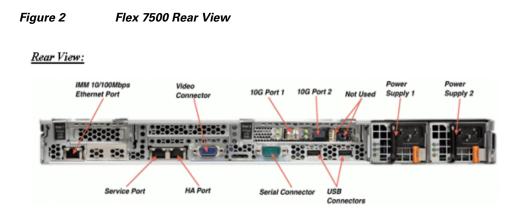
DTLS license is required for Office Extend AP support.

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

Platform Feature



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)	



ſ

- 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.



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.

50MAA

Cisco Bootloader	(Versio)	n)			
	.088b.	d888888b	.d8888.	.088b.	.d8	8b.
	d8P Y8	`88'	88' YP	d8P Y8	.8P	Y8.
	8P	88	`8bo.	8P	88	88
	d8			8b		88
		.88.			d8′	
	. A88b.	Y888888P	.8888A.	. A88b.	` ¥8	8P'
Booting Primary Image						
Press <esc> now for a</esc>		al boot op	ptions			
Boot Options						
Please choose an opti	lon from	below:				
1. Run primary image	Werei	~ n	· (d)	efault)		
				eraure)		
3. Manually upgrade						
4. Change active boo	t image					
5. Clear Configurati						
4. Change active boo	primary t image		·			

Figure 3 Boot-Up Order

I

Γ

Figure 4 WLC Configuration Wizard

```
Jould you like to terminate autoinstall? [yes]:
System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded
Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password
Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface VLAN Identifier (0 = untagged):
Management Port 1: 10G
Management Interface Port Num [1 to 2]: 1 🔶
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
```

<u>Note</u>

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.

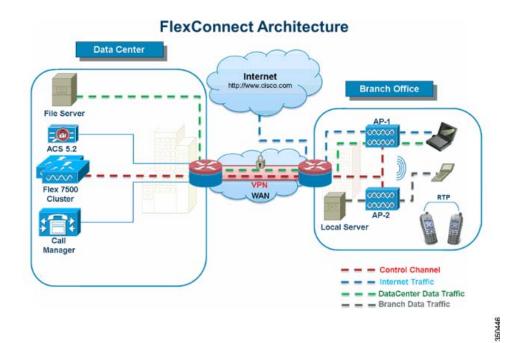
Supported Access Points

I

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



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.
- Distribute the client data traffic at each Branch Office.
 - Data traffic is marked by blue, green, and purple dashes in Figure 5.
 - Each traffic flow is going to its final destination in the most efficient manner.

1

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	Туре	Result
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	ССКМ	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed
CKIP	-	Allowed

I

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	Туре	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

1

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 Mod 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
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

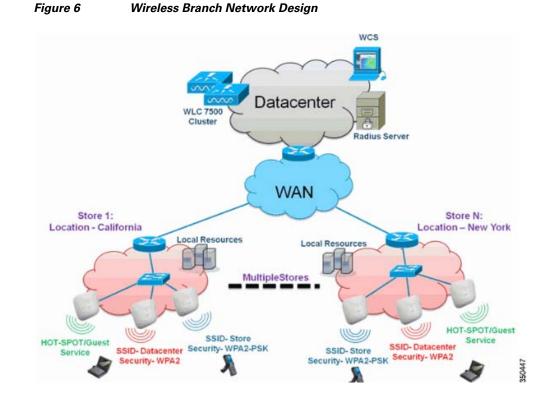
Recommended Latency = 300 ms

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



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.

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.		

Table 3Features

Note

Γ

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 Switcl	ned	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.

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.

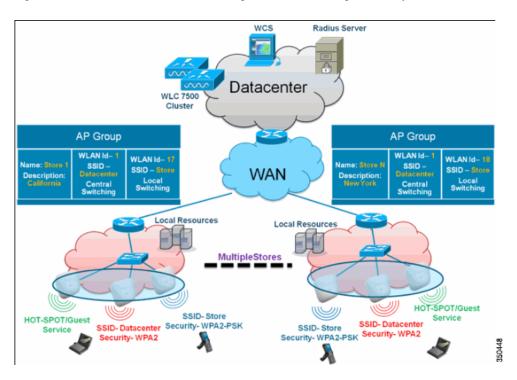


Figure 7 Wireless Network Design Reference Using AP Groups

Configurations from WLC

ſ

Complete the following steps:

Step 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.

<u>Note</u>

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.



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



1

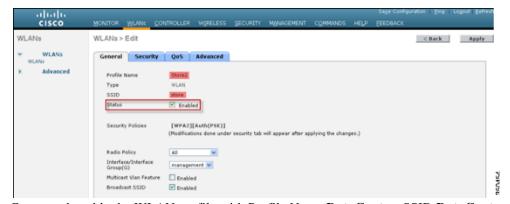
Step 3 Click **WLAN > General**, verify the Security Policies change, and check the **Status** box to enable the WLAN.

ahaha									Saye Corfig	uration Eing L	ogout Befresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		
WLANs	WLANs > I	Edit								< Back	Apply
WLANS WLANS	General	Secur	ity QoS	Advanced							
Advanced	Profile N	larne	Storel								
	Type		WLAN								
	SSID		store								
	Status		🗹 Enabi	ed.							
	Security	Policies		Auth(PSK)]	e en eurite tab	will appear after as	solution the share				
			(Houmeau	ons cone unce	r security tab	nni appear anter aj	sprying the trian	pes-)			
	Radio Po	olicy	All								
	Interfac Group(C	e/Interfaci 3)	manager	nent 🛩							7
	Multices	t Vlan Feat	ure 🗌 Enable	d							SEOAE4
	Broadca	st SSID	🗹 Enable	d							2

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

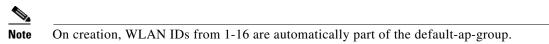
cisco	MONITOR WLAP	IS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	Sage Configuration Eing I	Logout <u>R</u> efresh
WLANS WLANS WLANS Advanced	WLANs > New Type Profile Name SSID ID	WLAT Store store 18	2					< Back	Apply
									2







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



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

 cisco		<u>W</u> LANS 1	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS		Sa <u>v</u> e Configuration EEDBACK	Eing	Logout	Befrest
WLANs	WLANs									En	tries 1 - 3	3 of 3
* WLANs	Current Filte	None	[Change	e Filter] [Clear	Filter]		Create N	iana 📈	Go			
WLANs Advanced												
 Advanced AP Groups 	WLAN ID	Туре	Profile Nam	ie.	WL	AN SSID			s Security Policie	5		
 Advanced 	WLAN ID	Type	Profile Nam DataCenter	ne		AN SSID					.1×)]	
 Advanced 				ie		taCenter	A E	dmin Statu	is Security Policie	uth(802		0

- Step 7 Click WLAN > Advanced > AP group > Add Group.
- **Step 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.
- Step 9 Click Add when done.

ululu cisco	MONITOR WLANS CONTROLL	R WIRELESS SECURITY	MENAGEMENT COMMANDS	нецр	Sage Configuration Ping EEEDBACK	Logout <u>R</u> efres
WLANS WLANS WLANS	AP Groups				Entries 0 - 0 of 0	Add Group
 Advanced AP Groups 	AP Group Name Stores Description Caldomia Add Can					
	AP Group Name	AP Group Descri	ption			
	default-group					

- Step 10 Click Add Group and create the AP Group Name as Store2 and the description as New York.
- Step 11 Click Add.

I

cisco	MONITOR WLA	NS CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMM	ANDS HELF	Saye Configuration Eing FEEDBACK	Logout <u>B</u> efresh
WLANs	AP Groups					Entries 1 - 1 of 1	Add Group
* WLANS	Add New AP Gr	нир					
 Advanced AP Groups 	AP Group Name	Store2					
AL GLOOPS	Description	New York					
		Add Cancel					
	AP Group Name		AP Group Desc				
	Storel		California				
	default-group						

Step 12 Verify the group creation by navigating to WLAN > Advanced > AP Groups.

.ı ı.ı ı. cısco	MONITOR WLANS	CONTROLLER	WIRELESS S	ECURITY	MANAGEMENT	COMMANDS	нецр	Sage Configuration Ping	Logout <u>R</u> efrest
WLANs	AP Groups							Entries 1 - 2 of 2	Add Group
WLANS	AP Group Name		AP Gro	oup Descri	ption				
Advanced AP Groups	Store1		Californ New Yo						
per croops	Store2 default-group		New To	A.K.					

- **Step 13** Click AP Group Name **Store1** to add or edit the WLAN.
- Step 14 Click Add New to select the WLAN.
- Step 15 Under WLAN, from the WLAN SSID drop-down, choose WLAN ID 17 store(17).
- **Step 16** Click **Add** after WLAN ID 17 is selected.
- Step 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.

MONITOR MU		WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	Sage Configuration Bing EEEDBACK	Logout Befre
Ap Groups > I	Edit 'Store1'						< Back
General	VLANS APS						
						Add New	î
Add New							
WLAN SSID Interface /Interface Group(G) NAC State	DataCenter(1) store(17) Store						
WLAN WLA ID SSII	IN Interface/Inte						
	Ap Groups > 1 General V Add New WLAN SSID Interface Group(G) NAC State	Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID DataCenter(1) Group(G) Group(G) NAC State Lenabled Add Came WLAN WLAN Interface/Liste	Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID DotaCenter(1) Interface there(10) Store 1 Group(0) NAC State Enabled Add Cancel WLAN WLAN Interface/Interface NAC	Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID Det&Center(1) Interface starc(10) TStore 1 Group(0) Add Centel WLAN WLAN Interface/Interface NAC	Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID DataCenter(1) Anterface stare(10) Store 1 Group(0) stare(10) Store 1 Group(0) stare(10) Store 1 Group(0) stare(10) Store 1 Add Cencel WLAN WLAN Interface/Interface NAC	Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID DOWNCHER Blore 1 K Interface Downcher(1) Group(0) ptore(1)) Store 1 Group(0) ptore(1) Store 1 Add Cancel WLAN WLAN Interface/Interface NAC	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK Ap Groups > Edit 'Store1' General WLANS APS Add New WLAN SSID DataCenter(1) Therface Store(1) Sto

- **Step 19** Click AP Group Name **Store2** to add or edit WLAN.
- Step 20 Click Add New to select the WLAN.

Step 18

- Step 21 Under WLAN, from WLAN SSID drop-down, choose WLAN ID 18 store(18).
- Step 22 Click Add after WLAN ID 18 is selected.
- **Step 23** Repeat steps 14 -16 for WLAN ID 1 DataCenter(1).

 cısco	MONITOR WLANS		S SECURITY MANAGEMENT	COMMANDS HELP	Sage Configuration Ping) Logout <u>B</u> efre:
WLANs	Ap Groups > Edit	"Store2"				< Back
WLANS	General WLAN	Ns APs				
Advanced AP Groups					Add New	î
	Add New					
	WLAN SSID Interface	DataCenter(1)				
	/Interface Group(G) NAC State	store(17) Store 1 store(18) Store 2 Enabled				
		Add Cancel				
	WLAN WLAN ID SSID	Interface/Interface Group(G)	NAC State			



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

The pag	ge at https://172.20.227.174 says:	×
1	Failed to add interface entry management	
	ОК	
	dding APs to the AP group is not captured ccess network services.	in this

Summary

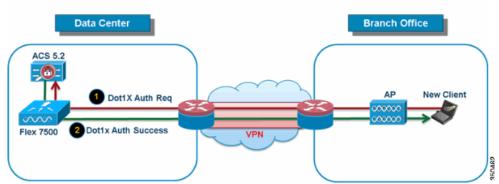
Γ

- 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)

Central Authentication – Flex 7500 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. 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.



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.

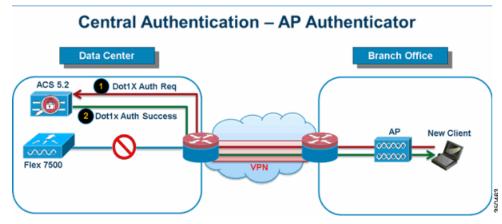


Backup RADIUS accounting is not supported.

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, 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.



With Local Authentication turned on, the AP will always authenticate the clients locally, even when it is in connected mode. When Local Authentication is disabled, the controller will authenticate clients to the Central RADIUS server when the FlexConnect AP is in connected mode. When the AP is in Standalone mode, the AP will authenticate clients to the Local RADIUS / Local EAP on AP configured on the FlexConnect Group.



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) Local Branch Authentication – AP as Radius Server Data Center Branch Office Dot1X Auth Req Do

• 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.

Success

350464

- 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, 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.



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

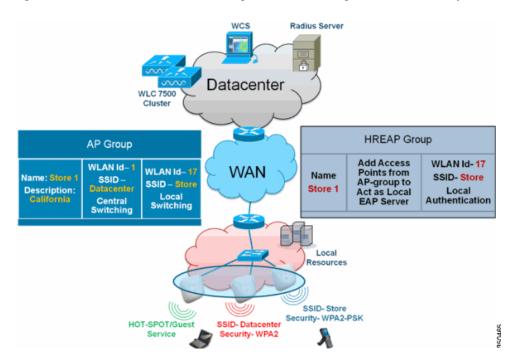


Figure 11 Wireless Network Design Reference Using FlexConnect Groups

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 illustrates the objective differences and 1:1 mapping between the AP Group and FlexConnect group.

- Step 1 Click New under Wireless > FlexConnect Groups.
- **Step 2** Assign Group Name Store 1, similar to the sample configuration as shown in Figure 11.
- **Step 3** Click **Apply** when the Group Name is set.

ſ

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS
Wireless	FlexConr	nect Gro	ups > New	
 Access Points All APs Radios	Group Na	me Sto	ore 1	
Advanced				
Mesh				
RF Profiles				
FlexConnect Groups				

1



Step 5

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

 cısco	MONITOR	<u>W</u> LANs	<u>C</u> CNTROLLER	WIRELESS	<u>S</u> ECURITY	
Wireless	FlexConn	ect Gro	ups			
 Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration 	Group Nan Store 1	ne			۵	
Advanced						
Mesh						
RF Profiles						
HexConnect Groups						350467
Click Add AP.						

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecuri
Wireless	FlexConn	ect Gro	ups > Edit 'S	tore 1'	
 Access Points All APs Radios	General Group I	Local	Authentication	Image U	pgrade
 Advanced Mesh RF Profiles FlexConnect Groups FlexConnect ACLs 	Add A		S AP Name	Sta	itus

Step 6 Check the **Enable AP Local Authentication** box in order to enable Local Authentication when the AP is in Standalone Mode.



Step 20 shows how to enable Local Authentication for Connected Mode AP.

- Step 7 Check the Select APs from current controller box in order to enable the AP Name drop-down menu.
- **Step 8** Choose the AP from the drop-down that needs to be part of this FlexConnect Group.
- **Step 9** Click **Add** after the AP is chosen from the drop-down.
- **Step 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 to understand the 1:1 mapping between the AP-Group and FlexConnect group.

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

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER	W <u>I</u> RELESS <u>S</u> ECURITY
Wireless	FlexConnect Groups > Edit 'S	store 1'
 Access Points All APs Radios	General Local Authentication Group Name Store 1	Image Upgrade
Advanced Mesh	FlexConnect APs	
RF Profiles FlexConnect Groups FlexConnect ACLs	Add AP Select APs from current controller	✓
 802.11a/n 802.11b/g/n Media Stream 	Ethernet MAC	00:22:90:e3:37:df Add Cancel
Country	AP MAC Address AP Name	Status

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

Step 12 Click **Apply** after the check box is set.

Note

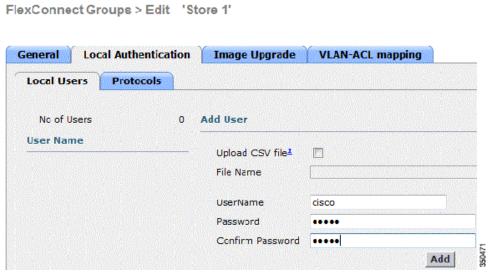
If you have a backup controller, make sure the FlexConnect groups are identical and AP MAC address entries are included per FlexConnect group.

ed.

1

neral Local Authentication	Image Upgrade VLAN-ACL mapping
ocal Users Protocols	
АР	
Enable LEAP Authentication ² AP Fast	
Enable EAP Fast Authentication ²	
Server Key (in hex)	Enable Auto key generation
	·····
Authority ID (in hex)	436973636f0000000000000000000000
Authority Info	Cisco A_ID

- Step 13 Under Local Authentication, click Local Users.
- **Step 14** Set the UserName, Password and Confirm Password fields, then click **Add** in order to create user entry in the Local EAP server residing on the AP.
- **Step 15** Repeat step 13 until your local user name list is exhausted. You cannot configure or add more than 100 users.
- Step 16 Click Apply after step 14 is completed and the No of Users count is verified.

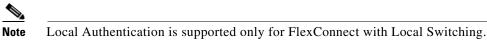


Step 17 From the top pane, click WLANs.

Step 18 Click WLAN ID 17. This was created during the AP Group creation. See Figure 7.

ahala					
CISCO	MONITOR	WLANS C	CONTROLLER W	IRELESS <u>S</u> ECURII	IY MANAGEI
WLANs	WLANs				
WI ANS	Current Fil	ter: None	[Change F	Elter] [Clear Eilter]	
Advanced		ID Type	Profile Name	:	WLAN SSID
	□ 2	WEAN	Guest		Guest
	□ <u>17</u>	WLAN	Store-1		Store 2

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





I

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

WLANs > Edit 'Store-1'

General	Security	QoS	A	dvan	ced]	1203
P2P Bloc	king Action	ſ	Disabl	ed		•	
Client Ex	clusion ³		Z Ena	bled	60 Tim	eout	Value (secs)
Maximun	n Allowed Clien	ts 🚨 🛛 🖸					
Static IP	Tunneling 💶	[🛛 Ena	bled			
Wi-Fi Dir	ect Clients Poli	cy [Disabl	ed 👻]		
Maximun Per AP R	n Allowed Clien adio	ts 2	00				
Off Channe	l Scanning De	fer					
Scan Del	fer Priority	0 1	2	3 4	5	6 V	7
Scan Del (msecs)	fer Time	100					
FlexConne	t						
FlexConr 2	nect Local Swite	hing	Z Er	nabled			
FlexConr	nect Local Auth	12	Z Er	nabled			
Learn Cli	ent IP Address	5 [Er	nabled			-

1

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

Properties	>	Configure > Controllers >			a wation
System	>		> 00L7	ans > wear com	juracion .
WLANs	~	General Security C	QoS	Advanced	
 WLAN Configuration AP Groups 		HexConnect Local Switching		⊢nable	
FlexConnect	>	FlexConnect Local Auth		Enable	
Security	>	Learn Client IP Address	的建筑的	Enable	
Access Points	>	Session Timeout Coverage Hole Detection		Enable Enable	
802.11	>	Aironet IE		Enable	
802.11a/n	>	IPv6 2		Enable	
802.11b/g/n	>	Diagnostic Channel 🙎	I	Enable	
Mesh	>	Override Interface ACL	IPv4	NONE	Seconder
Ports	~ >	Peer to Peer Blocking 🔍	Disa	able	-
Management	>	Wi-Fi Direct Clients Policy	Self-	abled	
Location	>	Client Exclusion 4 Timeout Value		Enable (secs)	

Γ

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

(Ilome Mci	nitor 🔻	Configure	✓ Service	s v Rep	orts 🔻	Adı	nnistration	
Tlents and Users									
~	Irribeshoot	🍐 lest	• 🛣 Lusable	Remove .	💿 Vinre 🔹	😨 Irad	(lens	Sidenti ^a	y Linknown Lisers
	MAC Address		IP Address	IV Lype	User N	ame	Type	Vendor	Device Name
0	00:22:90:1b:	17:42		IPv4	Unkno	wn	-	Cisco	WCS_SW 0.1.0.23
0	1c:df:0f:66:8	6:58		IPv4	Unknor	wn	5	Cisco	WC5_SW-9.1.0.2
0	00:21:6a:97:	9b:bc		₽v4	host/vi	ikalla		Intel	oeap-Laiwar-2
0	UU:22:90:1b:	96:48		1Pv4	Unkno	wn	-	LISCO	WCS_SW-9.1.0.2
0	00:22:90:1b:	17:8c		₽v1	Unkno	wn	-	Cisco	WCS_SW 0.1.0.2
0	00:25:0b:4d:	77:c4		₽v4	Unkno	wn	5	Cisco	WCS_SW-9.1.0.2
0	c4:7d:4f:3a:c	5:d5		TPv4	Unkno	wn	-	CISCO	WCS_SW-9.1.0.2
0	00:21:a0:d6:	03:c4		IPv4	Unkno	wn		Cisco	WCS_SW-9.1.0.2
υ	f3:66:f2:67:7	f:60		₽v4	Unkno	wn	5	Cisco	WCS_SW-9.1.0.2
0	CC:1f:caibd:b	1:64		I₽v4	Unknor	WII	2	Ciscu	WCS_SW-9.1.0.2
0	88:43:e1:d1:	df:02		IPv4	Unkno	wn	5	Cisco	WCS_SW-9.1.0.2
0	00:22:bd:1b:	c2:b5		₽v1	Unkno	wn	-	Cisco	WCS_SW 0.1.0.2
0	f3:66:f2:ab:1	e:69		₽v4	Unkno	wn	5	Cisco	WCS_SW-9.1.0.2
0	00:10:58:Jul	.4:4e		₽v4	Unknor	WI]	8	Ciscu	WCS_SW-9.1.0.2
\cap	UU:1e:/atbb:	21:8d			ssimm			Cisco	oeap-tawar-2

Virtual Domain: RC	OT-DOMAIN	root 👻 Log Ou	ut 🔎	→
				😵 🖾 🕗
				Total 299 😽 🎰 🎡 🕯
			Show	Associated Clients 🔹 🏹
Location	VLAN	Status	Interface	
Unknown	109	Associated	Gi1/0/34	Advanced Filter
Unknown	109	Associated	Gi1/0/26	
Root Area	310	Associated	data	Manage Preset Filters
Unknown	109	Associated	Gi1/0/36	2.4GHz Clients
Unknown	109	Associated	Gi1/0/32	5GHz Clients All Lightweight Clients
Unknown	109	Associated	Gi1/0/30	All Autonomous Clients
Unknown	109	Associated	Gi1/0/13	
Unknown	109	Associated	Gi1/0/27	Associated Clients
Unknown	109	Associated	Gi1/0/12	Clients known by ISE
Unknown	109	Associated	Gi1/0/15	Clients detected by MSE
Unknown	109	Associated	Gi1/0/28	Clients detected in the last 24 hours
Unknown	109	Associated	Gi1/0/14	Clients with Problems
Unknown	109	Associated	Gi1/0/9	Excluded Clients
Unknown	109	Associated	Gi1/0/29	
Root Area	311	Associated	voice	New clients detected in last 24 hours

1

Verification Using CLI

I

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

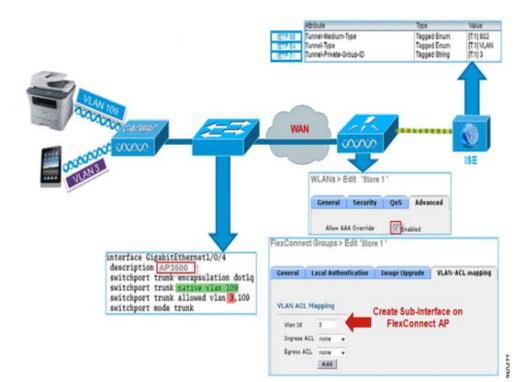
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c

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.

1

- 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:

Step 1 Create a WLAN for 802.1x authentication.

1010 Decimentaria	Security	QoS Advanced	
Layer 2	Layer 3	AAA Servers	
	Security ⁶	2MAC Filtering	
WPA Po			
-	olicy	\checkmark	
WPA2 P			
	ncryption	AES TKIP	

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

Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection Enable Session Timeout Aironet IE Diagnostic Channel	Enabled Enabled Session Timeout (secs) Enabled Enabled	DHCP Server	erride quired 1FP)
Override Interface ACL P2P Blocking Action	Disabled V	MFP Client Protection 4 Optiona DTIM Period (in beacon intervals)	
Client Exclusion 2 Maximum Allowed Clients Static IP Tunneling 4	Enabled 60 Timeout Value (secs)	802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC	
Wi-Fi Direct Clients Policy Maximum Allowed Clients	Disabled 💌	NAC State None S	
Per AP Radio Dff Channel Scanning Def		Client Load Balancing Client Band Select 2	
	0 1 2 3 4 5 6 7	Passive Client Passive Client	
Scan Defer Time (msecs)	100	Voice Media Session Snooping Re-anchor Roamed Voice Clients	Enable

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

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

Step 4 The AP is in local mode by default, so covert 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.

Γ

General	Credentials	Interfaces	High Availability	Inventory	Advanced	
ieneral				Versions		
AP Name	- A	P3500		Primary Soft	ware Version	7.2.1.69
Location	de	fault location		Backup Soft	ware Version	7.2.1.72
AP MAC	Address co	:ef:48:c2:35:57		Predownload	l Status	None
Base Ra	dio MAC 20	::3f:38:f6:98:b0		Predownload	led Version	None
Admin S	tatus E	nable 💌		Predownload	Next Retry Time	NA
AP Mode	E	exConnect 👻		Predownload	Retry Count	NA
AP Sub M	tode N	one 💌		Boot Version	1	12.4.23.0
Operatio	nal Status Ri	EG		IOS Version		12.4(20111122:141426)
Port Num	nber 1			Mini IOS Ver	sion	7.0.112.74
Venue G	roup U	nspecified	*	IP Config		
Venue Tr	vpe U	nspecified 🐱		IP Address		10.10.10.132
Venue N	ame			Static IP		
Languag	e 🗌					
Network Interface	Spectrum 00	045BA896226F411	7D98BA920FBA8A16	Time Statistic	s	
Incertace	ney			UP Time		0 d, 00 h 01 m 14 s
				Controller As	ssociated Time	0 d, 00 h 00 m 14 s
				Controller As	ssociation Latency	0 d, 00 h 00 m 59 s

1

Step 5 Add the FlexConnect APs to the FlexConnect group.

Navigate under WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General tab > Add AP.

eneral Local Authenticati	on Image Upgrade VLA	N-ACL mapping		
Group Name Store 1		AAA		
		Primary Radius Server	None	*
	er 🖌	Primary Radius Server Secondary Radius Server	None	v
	er 🕑 AP3500 💌		None	100
Add AP Select APs from current controlle		Secondary Radius Server	None	100

Step 6 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 dotlq	
switchport trunk native vlan 109	
switchport trunk allowed vlan 3,109	2
switchport mode trunk	350483

- Note In this configuration, VLAN 109 is used for WLAN VLAN mapping and VLAN 3 is used for AAA override.
- Step 7 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.

AP Na	ne	AP3500	
Base R	adio MAC	2c:3f:38:f6:98:b0	
WLAN Id	SSID		D
1	Store 1	1	109

Step 8 Create a user in the AAA server and configure the user to return VLAN ID in IETF Radius attribute.

	Attribute	Туре	Value	
IETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802	٦.
IETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN	
IETF 81	Tunnel-Private-Group-ID	Tagged String	[T:1] 3	0485

Step 9 In order 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.

In order 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.

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping
	to and the second s		
LAN ACL M	Mapping		
Vlan Id	3		

- **Step 10** Associate a client on this WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN.
- **Step 11** The client should receive an IP address from the dynamic VLAN returned via the AAA server.
- Step 12 In order to verify, click WLC GUI > Monitor > Client, click the specific client MAC address in order to check the client details.

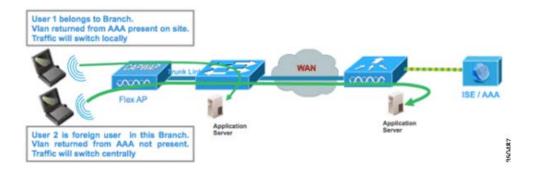
Limitations

- 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:

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

eneral Security	QoS Advanced	_
Allow AAA Override	🗹 Enabled	
Coverage Hole Detection	Enabled	
Enable Session Timeout	Session Timeout (secs)	
Aironet IE	Enabled	
Diagnostic Channel	Enabled	
Override Interface ACL	IPv4 None 💌 IPv6 None	2
P2P Blocking Action	Disabled	
Client Exclusion ³	Enabled 60 Timeout Value (secs)	
Maximum Allowed Clients ^g	0	
Static IP Tunneling 💶	Enabled	
Wi-Fi Direct Clients Policy	Disabled 💌	
Maximum Allowed Clients Per AP Radio	200	
lexConnect		

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

General Security	QoS Advanced
Allow AAA Override	✓ Enabled
Coverage Hole Detection	Enabled
Enable Session Timeout	I800 Session Timeout (secs)
Aironet IE	Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None V IPv6 None V
P2P Blocking Action	Disabled 💌
Client Exclusion 3	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients ^g	0
Static IP Tunneling 💶	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
lexConnect	
FlexConnect Local Switching ²	Enabled
FlexConnect Local Auth 担	Enabled
Learn Client IP Address 5	Enabled

1

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

General	Credentia	als Interfaces	High Availability
ieneral			
AP Name	6	AP_3500E	
Location			
AP MAC	Address	o4:7d:4f:3a:07:74	
Base Rad	lio MAC	o4:7d:4f:53:24:e0)
Admin St	atus	Enable 💌	
AP Mode		FlexConnect	·
AP Sub N	lode	local FlexConnect	
Operation	nal Status	monitor Rogue Detector	
Port Num	ber	Sniffer	
Venue G	roup	Bridge SE-Connect	~

All APs > Details for AP_3500E

Step 4 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.

ဂျကျက cisco		WLANS		WIRELESS	SECURITY
Wireless	All APs > A	AP_3500	DE > VLAN Ma	ppings	
Access Points All APs	AP Name	4	P_3500E		
♥ Radios 802.11a/n	Base Radio	MAC d	4:7d:4f:53:24:e0		
802.11b/g/n Global Configuration	WLAN Id S	SID			VLAN ID
Advanced	1 'S	tore 1' :			63
Mesh					Lawrence
RF Profiles	Centrally s	witched	Mans		
FlexConnect Groups FlexConnect ACLs	WLAN Id	HIGH G	SSID	VLAN ID	
▶ 802.11a/n	AP level VL	AN ACL	Mapping		
▶ 802.11b/g/n	Vlan Id		ess ACL	Egress A	CL
Media Stream	63	none	×	none 💌	
Country Timers	Group leve	I VLAN A	CL Mapping		
▶ QoS	Vlan Id	Ingr	ess ACL	Egress A	CL

Step 5 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).

ſ

uluulu cisco	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT COM	IMANDS HELP	<u>F</u> EEDBACK
Controller	Interfaces						
General Inventory	Interface Name		YLAN Identifier	IP Address	Interface Type	Dynamic AP M	anagement
Interfaces	dyn		62	9.6.62.10	Dynamic	Disabled	
Interface Crouns	management		61	9.6.61.2	Static	Enabled	

Step 6

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.

Summary				
Access Points				
Cisco CleanAir	Client Properties		AP Properties	
 Statistics CDP 	MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
Rogues	IPv4 Address	9.6.62.100	AP Name	AP_3500E
Redundancy	IPv6 Address		AP Type	802.11a
Clients			WLAN Profile	'Store 1'
Multicast			Data Switching	Central
			Authentication	Central
			Status	Associated
			Association ID	1
			802.11 Authentication	Open System
			Reason Code	3
			Status Code	0
	Client Type	Regular	CF Pollable	Not Implemented
	User Name	betauser	CF Poll Request	Not Implemented
	Port Number	1	Short Preamble	Not Implemented
	Interface	dyn	PBCC	Not Implemented
	VLAN ID	62	Channel Agility	Not Implemented

<u>Note</u>

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).

Step 7 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.

ent Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e
Pv4 Address	9.6.61.100	AP Name	AP_3500E
Pv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentic	cation Open System
		Reason Code	3
		: Status Code	0
lient Type	Regular	CF Pollable	Not Implemented
lser Name	betauser2	CF Poll Request	Not Implemented
Port Number	1	Short Preamble	Not Implemented
interface	management	PBCC	Not Implemented
VLAN ID	61	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.

Step 8 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	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

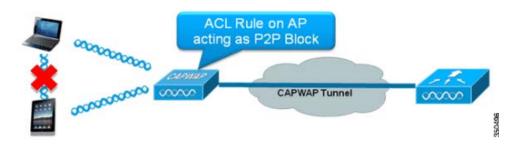
Limitations

I

- 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.

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:

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

FlexConnect Access Control Lists	Entries 0 - 0 of 0	New
Acl Name		
11' 1 TT		

1

Step 2 Click New.

Step 3 Configure the ACL Name.

Access Control Lists > No	9W	< Back	Apply
Access Control List Name	Flex-ACL-Ingress]	

Step 4 Click Apply.

Step 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.

Acce	ess Con	trol Lists > Edit						< Back	Add New Rule
Gene Acces	e ral s List Nam	e Flex-ACL-	Ingress						
	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP		

Step 6 Click Add New Rule.

I

Access Contro	ol Lists > Rules > New			< Back	Apply
Sequence	1				
Source	IP Address 👻	IP Address 0.0.0.0	Netmask 0.0.0.0		
Destination	IP Address 👻	IP Address 0.0.0.0	Netmask 0.0.0.0		
Protocol	Any 💌				
DSCP	Any 💌				
Action	Deny 💌				350500
					8
	~				

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.

- **Step 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.
- Step 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.

AP Name	8	AP3500		
Base Ra	dio MAC	2c:3f:38:f6:98:	ЬО	
WLAN Id	SSID			VLAN ID
1	Store 1			109
entrally	switche	d Wlans		
(1)	-	d Wlans		VLAN ID
WLAN Id	-	d Wlans		VLAN ID N/A
WLAN Id 2	SSID Store 3	ed Wlans CL Mapping		0.00055100
WLAN Id 2	SSID Store 3	L Mapping	Egress A	N/A

1

Step 9 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.

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping	
LAN ACL M	lapping			
Vlan Id	0			
Ingress AC	Flex-ACL-Egress 💌			
Egress ACL	Flex-ACL-Egress			
	Add			

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:

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

1

General	Security	QoS	Advanced		
Coveraç	A Override le Hole Detectio cession Timeout	✓ 18 Se	abled 00 ession Timeout	(secs)	
	tic Channel	Ena Ena			
Override	Interface ACL	IPv4	None 💌		IPv6 None N
P2P Bloc	king Action	Disat	oled	~	
Client E	clusion ¹	Ena	bled 60 Timeou	It Value (secs)	
Maximur Clients	n Allowed	0			
Static IP	Tunneling 💶	Ena	bled		
Wi-Fi Dir Policy	ect Clients	Disab	oled 💌		
	n Allowed Per AP Radio	200			I Switching be enabled
lexConne	ct			/	

Step 2 Set DHCP Address Assignment to **Required.**

eneral Security	QoS Advanced			
Allow AAA Override	Enabled		DHCP	
Coverage Hole Detection	Enabled		DHCP Server	Override
Enable Session Timeout	Session Timeout (secs)		DHCP Addr. Assignment	Required
Aironet IE	Enabled		Management Frame Prot	ection (MFP)
Diagnostic Channel	Enabled			
Override Interface ACL	IPv4 None M	IPv6 None V	MFP Client Protection	Optional V

Step 3 Set AP Mode to FlexConnect.

General	Credentia	als Interface	s High Ava	ailability
ieneral				
AP Name		AP_3500E		
Location				
AP MAC A	ddress	o4:7d:4f:3a:07:3	74	
Base Radi	o MAC	o4:7d:4f:53:24:6	e0	
Admin Sta	atus	Enable 💌		
AP Mode		FlexConnect	~	
AP Sub M	ode	local FlexConnect		È.
Operation	al Status	monitor		
Port Numb	ber	Rogue Detector Sniffer		
Venue Gr	oup	Bridge SE-Connect	~	

All APs > Details for AP_3500E

Step 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.

ıılııılı. cısco	Mont	TOR	<u>w</u> lans		ER WIJRELESS	2	ECURITY	MANAGEMENT	COMMANDS	неџр	EEEDBACK
Wireless	Acce	ess Co	ontrol L	ists > Edit							
Access Points All APs	Gene	eral									
 Radios 802.11a/n 802.11b/g/n 	Acces	s List Na	ame	Flex-	ACL						
Global Configuration	Seq	Actio	n Sour	ce IP/Mask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	
 Advanced Mesh 	1	Permit	9.6.6	1.0 /	9.1.0.150 255.255.255.255	1	ICMP	Any	Any	Any	
RF Profiles FlexConnect Groups	-										
FlexConnect ACLs											

Step 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.

Complete these steps in order to push Flex ACL as a Local Split ACL to individual Flex AP:

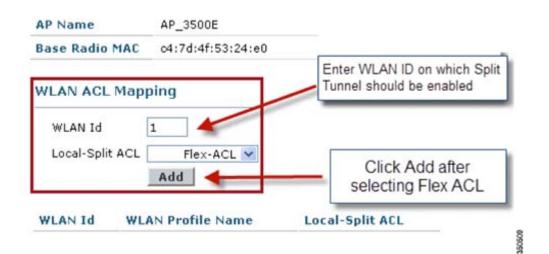
a. Click Local Split ACLs.

ſ



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

All APs > AP_3500E > ACL Mappings



I

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

AP Nan	ne	AP_3500E	
Base R	adio MAC	o4:7d:4f:53:24:e0	
WLAN WLAN	ACL Mapp	oing 0	
Local	-Split ACL	Flex-ACL V	
WLAN			
Id	WLAN P	rofile Name	Local-Split ACL

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

a. 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'			
Access Points All AP1 Redioi	General Local Authentication	Image Upgrade	AAA YLAN-ACL mapping	WLAN-ACL mapping	WebPalicies
602.11a/h 602.11b/g/h Global Configuration F Advanced	Web Auth ACL Mepping		Local Split ACL Map		NID on which Split vid be enabled
Mesh RF Profiles FlexConnect Groups	WLAN 3d 0 WebAuth ACL Flex-ACL M Add		WLAN 1d 1 Local Spik ACL	Flex-ACL Click ADD	after selecting Flex
ResConnect ACLs 002.11a/n	WLAN Id WLAN Profile Name	WebAuth ACL	WLAN Ed WLAN F	rufile Name Loca	isplit ACL

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

Wi	ireless	FlexConne	ct Groups > Edit	Flex-Group*			
	Access Points All APy Radios 802.11a/h	General	Local Authentication	Image Upgrade	AAA VLAN-ACL mappi	WLAN-ACL mapping	WebPolicies
	802.11b/g/n Global Configuration	Web Aut	h ACL Mapping		Local Split ACL	Mapping	
٠	Advanced	WLAN IC			WLAN Id	0	
	Mesh						
	RF Profiles	WebAut			Local Split ACL	Flex-ACL M	
	FlexConnect Groups FlexConnect ACLs		Add			Add	
	802.11a/n	WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN IG WI	LAN Profile Name Lo	Per-ACL
	802.11b/g/n				1 '5	tore 1'	Flex-ACL 💌 🖬

ſ

Limitations

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

1

• 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



te 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. Any configuration mismatch across WLCs in any of below will result in radio reset at AP:

- 1. Flexconnect group (all possible configs)
- 2. WLAN to WLAN mapping per AP / AP Group / WLAN
- 3. Radio related configs (rates / power) etc.
- **4**. WLAN configurations

WLC Configuration

I

Complete these steps:

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

eneral Security	QoS Advanced		
Allow AAA Override Coverage Hole Detectio Enable Session Timeou Aironet IE Diagnostic Channel IPv6 Enable ² Override Interface ACL P2P Blocking Action Client Exclusion ³	t 1800 Session Timeout (secs) Enabled None Disabled Scabled	DHCP DHCP Server DHCP Addr. Assignment DHCP Addr. Assignment Required Management Frame Protection Optional DTIM Period (in beacon intervals) 002.11a/n (1 - 255) 1	
Maximum Allowed Clients ⁹ If Channel Scanning D Scan Defer Priority	0 1 2 3 4 5 6 7	802.11b/g/n (1 - 255) 1 NAC NAC OOB State Enabled Posture State Enabled	
Scan Defer Time(msecs)		Load Balancing and Band Select Client Load Balancing Client Band Select #	~
When client exclusion is Client MIP is not active u Learn Client IP is configu WMM and open or AES s Multicast Should Be Enab Band Select is configural Value zero implies there	nless WPA2 is configured rable only when HREAP Local Switching is en ecurity should be enabled to support higher 1	ity (will require administrative override to reset excluded clients) blied In rates	

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

1

NCS Configuration

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

WLAN Configuration Deta Configure > Controllers > 172.20.225	ils : 17 5.154 > WLANs > WLAN Configuration > W	/LAN Configuration Details
General Security QoS	Advanced	
FlexConnect Local Switching	Enable	DHCP
Learn Client IP Address	Enable	DHCP Server
Session Timeout	Enable 1800 (secs)	DHCP Address Assignment
Coverage Hole Detection	Enable	Management Frame Protectio
Aironet IE IPv6 2	Enable Enable	
Diagnostic Channel 2		MFP Client Protection 🖻
Override Interface ACL	IPv4 NONE	MFP Version
	IPv6 NONE	Load Balancing and Band Sel
Peer to Peer Blocking 🔍	Disable 🔽	
Wi-Fi Direct Clients Policy	Disabled 🔽	Client Load Balancing
Client Exclusion 4	🗹 Enable	Client Band Select
Timeout Value	60 (secs)	NAC
Maximum Clients 🔍	0	NAC

Configuration through Cisco Prime

ſ

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

cisco Infrastructure		🙆 Home	Moni	tor V Cor	figure *	Ser	vices *	Reports *	Adminis	stration 🛛 🔻	
Properties	>	General Security	Qc	IS Adv	anced	Но	tSpot	Policy Confi	guration	1	
System	>						FlexCor				
WLANs	~	Session Timeout		5707 C				nnect Local Swit	tching	Enable	
WLAN Configuration		Coverage Hole Detection Aironet IE					FlexCo	nnect Local Auth	D	Enable	
AP Groups		IPv6 2	E En				Learn	Client IP Address	5	C Enable	
Policy Configuration		Diagnostic Channel	□ En				VLAN I	Based Central Sw	vitching	🖸 Enable	
RexConnect	>	Override Interface ACL	IPv4	NONE		•	Centra	DHCP Processin	19	Enable	
Security	>	and the state free	IPv6	NONE		•		ie DNS		Enable	
Access Points	>	Peer to Peer Blocking 2	Disa	ble	•		NAT-P	AT		Enable	
802.11	>	Wi-Fi Direct Clients Policy	Dise	bled	•		DHCP	Server		Override	
802.11a/n	>	Client Exclusion	🕑 En	able				Address Assignm	ient	Required	
802.11b/g/n	>	Timeout Value	60	(secs)			Manage	ment Frame Pr	otection	n (MFP)	
Application Visibility And Control	>	Maximum Clients	0				MED C	lient Protection	2	Enabled	_
Netflow	>	Mobility Anchors	0				MEP V			1	
Mesh	>	Foreign Controller Mappings	0				Load Ba	alancing and Ba	nd Sele	ct	
Ports	>	Passive Client		able			Client	Load Balancing			
Management	>	Off Channel Scanning Defer						Band Select			
Location	>						NAC	NUMBER OF			
Router Advertisement	>	Scan Defer Priority		234567			NAC S	tate		None \$	
Redundancy	>	Scan Defer Time	10) (ms)			Voice				
PMIP		071M Period 2 802.11a/n (1-255)	1				Client P	Profiling		Enable	

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.

1



Summary

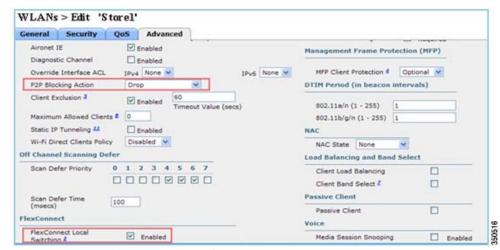
• Peer-to-peer Blocking is configured per WLAN

- 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:

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



Step 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

I

- 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:

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

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

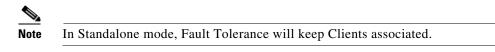
Download file to Controller	
File Type	Code
Transfer Mode	TFTP 💌
Server Details	
IP Address	
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_0_112_52.aes

- **Step 2** Save the configurations on the controllers, but do not reboot the controller.
- Step 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	Perform a backup image pre-download on this AP
Download Primary	Download Backup
Perform a interchange of both the images on this AP	
Interchange Image	8 5 30/34

```
*Sep
              903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image
              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:
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
                                                                   35051
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!
1111
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.
Reboot the controllers after all the AP images are downloaded.
```

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



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

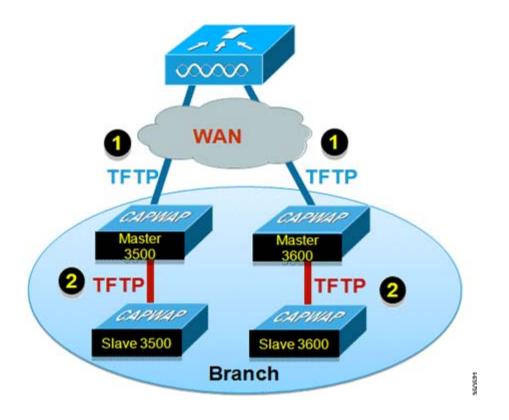
Step 4

• 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.



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:

Step 1Upgrade the image on the controller.Navigate to WLC GUI > Commands > Download File in order to begin the download.

1

SCH02

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

- **Step 2** Save the configurations on the controllers, but do not reboot the controller.
- **Step 3** Add the FlexConnect APs to FlexConnect group.

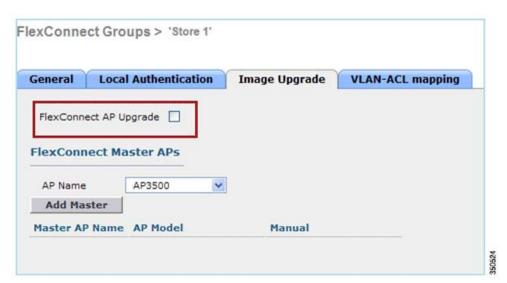
Γ

Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > General tab > Add AP.

350522

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping		
Group N	ame Store 1				
lexCon	nect APs		AAA		
dd AP			Primary Radius Server	None	~
	Ps from current controller	2	Secondary Radius Server	None	*
Select A		-	mail and a desired		
Select A		AR3500	Enable AP Local Authentication		

Step 4 Click the FlexConnect AP Upgrade check box in order to achieve efficient AP image upgrade.
 Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab.



- **Step 5** The Primary AP can be selected manually or automatically:
 - a. In order 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.

General	Local Authentica	tion Image Upgrade	VLAN-ACL mapping	
FlexConn	ect AP Upgrade 🔽			
Slave Ma	ximum Retry Count	44		
Upgrade	Image	Backup 💌	FlexConnect Upgrade	
FlexCon	nect Master APs			
AP Name	AR3500	~		
Add Ma	ster			
	P Name	AP Model	Manual	12000
Master A				

<u>Note</u>

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.

I

b. In order to automatically select Primary AP, navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab, and click FlexConnect Upgrade.

General	Local Authentica	tion Image	Upgrade V	LAN-ACL mapping	
FlexConn	ect AP Upgrade 🕑				
Slave Ma	ximum Retry Count	44			
Upgrade	Image	Backup 💌	Flex	Connect Upgrade	
AP Name	AP3500-1	~			
Add Ma	ster				
Master Al	P Name	AP Model	Ma	inual	
	500-1	c3500I	no		P3

Step 6 In order to start efficient AP image upgrade for all the APs under a specific FlexConnect group, click **FlexConnect Upgrade**.

If Primary AP is selected automatically, the Manual field will be updated as no.

Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect group > Image Upgrade tab and click FlexConnect Upgrade.

eral	Local Authentical	tion Image Upgrade	VLAN-ACL mapping
exConn	ect AP Upgrade 🗹		

Note

- **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.
- Step 7 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.

In order 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	

Step 8

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



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	redentials	Interfaces	High Availability		
General					
AP Name	AP3	500			
Location	defa	ault location			
AP MAC Add	ress 00:	00:22:90:e3:37:df			
Base Radio M	1AC 00:	00:22:bd:d1:71:30			
Admin Status	s Dis	able 👻			
AP Mode	loca	al 👻			
AP Sub Mode	loca	Connect			
Operational S	Status mor	nitor			
Port Number		ue Detector fer			
Venue Group	Brid SE-	lge Connect	•		

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

Auto Convert Mode

This mode is available only for the Flex 7500 Controller and is supported only using CLI. This mode triggers the change on all the connected APs. It is recommended that Flex 7500 is deployed in a different mobility domain than existing WLC campus controllers before you enable this CLI:

• This feature is also supported on the 8510, 5520 and 8540 controllers.

```
(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) >
```

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

(Cisco Controller) >show ap autoconvert

AP Autoconvert Disabled

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

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

This option is currently available only via CLIs.

These CLIs are available only on the WLC 7500.

Step 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) >

Step 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.



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

I

Complete these steps:

Step 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.

General	Security	QoS A	dvanced		
Coverag Enable S Aironet Diagnos Override P2P Bloc Client E: Maximu Clients Static IF Wi-Fi Dir Policy Maximu	tic Channel Interface ACL king Action colusion 3 n Allowed Tunneling 11 ect Clients n Allowed fer AP Radio stSpot ation	1800	d on Timeout (secs) d d e V f 60 Timeout Valu	IPv6	None 💌

1

Step 2 Set AP Mode to **FlexConnect.**

All APs > Details for AP_3500E

General 👔	Credentia	als In	terfaces	High Availabilit
eneral				
AP Name		AP_3500	E	
Location				
AP MAC A	ddress	o4:7d:4f	:3a:07:74	
Base Radi	o MAC	o4:7d:4f	:53:24:e0	
Admin Sta	tus	Enable	*	
AP Mode		FlexCon	nect 🔽	
AP Sub Me	ode	local FlexCon	nect	-
Operation	al Status	monitor	and the state of the	
Port Numb	er	Rogue D Sniffer	etector	
Venue Gro	pup	Bridge SE-Coni	nect	~

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

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEOBACK				
Clients											
Current Filter	None	Change Filter] [Clear Filter]								
Client MAC Addr	AP Name		WLAN	Profile	WLAN SSID		Protocol	Status	Auth	Fort	WG8
00:40:95-56:d4:be	AP_3500E		"Store	÷ 1'	"Store 1"		N/A	Associated	Yes	1	No
31. 19. 17 FR. 94. 81											
00:50:b6:09:e5:3b	AP_3500E		'Stor	e 1'	"Store 1"		N/A	Associated	Yes	1	No

Step 4

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

Clients > Detail							
Client Properties		AP	AP Properties				
MAC Address	o4:7d:4f:3a:08:10	4	AP Address	o4:7d:4f:53:24:e0			
IPv4 Address	9.6.63.102	A	AP Name	AP_3500E			
IPv6 Address		A	AP Type	802.11an			
		N N	VLAN Profile	'Store 1'			
		c	Data Switching	Local			
		A	Authentication	Central			
		s	Status	Associated			
		A	ssociation ID	1			
		8	02.11 Authentication	Open System			
		F	leason Code	1			
		, i s	itatus Code	0			
Client Type	WGB		CF Pollable	Not Implemented			
Number of Wired Cli	ient(s) 2	0	CF Poll Request	Not Implemented			

Step 5 In order to check the details of the wired/wireless clients behind WGB, go to **Monitor > Clients**, and select the client.

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

Clients > Detail

ſ

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

Step 1 Mode of configuration prior to release 7.4.

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

I

CISCO	MONETON			WIRELESS STC	and the second se	GEMENT COMMAND	S HELP PERIODAC		
Security	RADIUS	5 Authenticat	tion Serv	ers					Apply New-
AAA General - RADDUS Authentication		atien 30 Type ⁴ S Ray Way		NAC Address	d requires a key	who compliant RADI2/5	aarver)		
Adducting	MAC D	wimber	Hyphet	(8)					
TAEACS+ LOAP Local Ret Linese	Natwork	Hanaperson	Server Index	Server Address	Part	1Ples	Admin Status		
MAC Fibeling	H		1	1234	1812	Disabled	Enabled		
Disabled Ownes Uner Logie Policies AP Policies Personnel Policies	10	6	2	1.2.3.4	2	District	Enabled		
	M	6	3	12.24		Disabled	Enabled		
	68	68	4	1.2.3.4	4	Disabled	Enabled		
Local EAP	H	-	5	1.2.3.4	8	Disabled	Enabled		
	H	8	6	1.2.3.4	6	Disabled	Evabled		
Priority Order	18	95	1	1.2.3.4	7	Disabled	Enabled		
Certificate	M	ef		1234		Disabled	Enabled		
Access Centrel Lists	8	ef -		1.2.3.4	*	Disabled	Enabled		
Wireless Protection	M		22	1234	10	Disabled	Enabled		
Policies	10		22	1.2.3.4	11	Disabled	Enabled		
Web Auth	18	8	.12	5.2.3.4	12	Disabled	Enabled	•	
Trustlec SXP	1		13	1.2.3.4	13	Disabled	Enabled		
Advanced	8	6	38	1.2.3.4	14	Disabled	Enabled		
	- 10	*	.13	1.2.3.4	18	Disabled	Enabled	0	
	H			1.2.3.4	36	Disabled	Enabled		
	10	6	42	1.2.3.4	17	Disabled	Enabled		

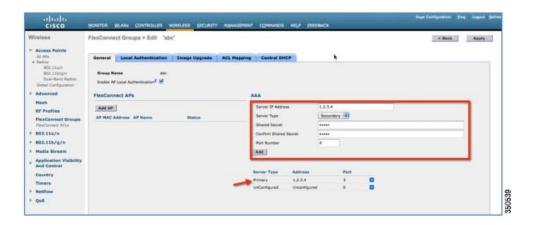
Step 2 Primary and Secondary RADIUS servers can be associated with a FlexConnect Group using a drop-down list comprising of RADIUS servers configured on the AAA Authentication page.

Virsiess	FleaConnect Groups > Edit 'abc'				e Back	Appiny
Access Prints All Alls Balling BE2.134(g) BE2.134(g) BE2.134(g) Below Defension Advanced Below Profiles PrecEntrect Groups PrecEntrect Groups Dist.134/n B02.134/n Mudia Stream	General Local Authentication In Group Name do PieseConnect APs Add AP AF NAC Address AF Name	ARA VLAN-ACL mapping AAA AAA Status Badus Brate AF La	tion Server al Authon Ecology (1971-2-3) (19	2, Port3 4, Port3 4, Port5 4, Port5 4, Port5		
Country Timers QoS			19:1.3,3 19:1.2,3 19:1.2,3 19:1.2,3 19:1.2,3 19:1.2,3			

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

ſ

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



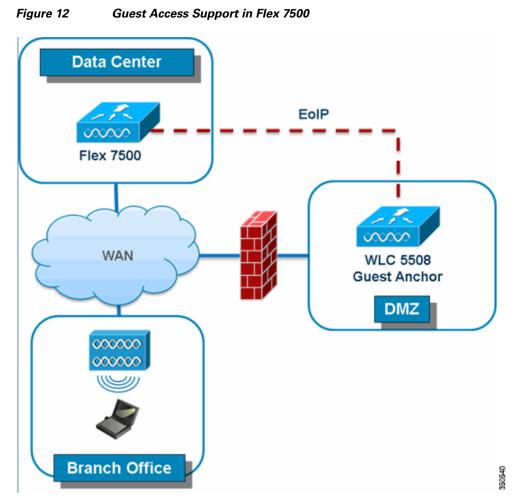
Limitations

- 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



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.

mmang	
	<u>Ent</u> ((-)
Reachability Status	Audit S
	Identic
	nmand ↔ Reachability Status Reachable

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

ſ

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

dd Controllers		
onfigure > Controllers > /	Add Controllers	
ieneral Parameters		
Add Format Type	Device Info	•
IP Addresses	WLC 7500 IP Address	(comma-separated IP Addresses)
Wism Auto Add (1)	WILL 7500 IP Address	
NMP Parameters ①		
Version	v2c	•
Retries	2	
SNMP Timeout	10	(secs)
Community		
Contraction of the second second	(h)	
einet/SSH Parameters		
Protocol	Teinet	0
Username	admin	
Password		
Confirm Password		
oonnin raconora		(secs)

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.sh tml)

Figure 13 Document 100590

Document ID: 100590	
Contents	
Introduction Prerequisites	
Requirements	
Components Used	
Conventions	
Background Information	
Configure Network Diagram	
Configurations	
Configure EAD EAST as Local EAD Authentication Method on the WLC	
Generate a Device Certificate for the WLC	
Downloading the Device Certificate onto the WLC	
Install the Root Certificate of PKI into the WLC Generate a Device Certificate for the Client	
Generate the Root CA Certificate for the Client	
Configure Local EAP on the WEC	
Configure LDAP Server	
Creating Users on the Domain Controller	
Configure the User for LDAP Access Using LDP to Identify the User Attributes	
Configure Wireless Client	
Verify	
Troubleshoot	
Cisco Support Community - Featured Conversations	
Related Information	

Configuration of EAP-TLS on FlexConnect AP

I

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

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT CO	MMANDS HELP	FEEDBACK	
VLANs .	WLANs					
WLANS	Current Filter: No	ne (Change Filter) (I	Dear Filter)		Create New Go	
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
	I WLAN	enloy	eniov	Enabled	[WPA21(Auth/802.1X1)	
	2 4 WLAN	ciscowic-peap	ciscowic-peap	Enabled	[WPA2][Auth(802.1X)]	
	S WLAN	ciscowic-eaptis	ciscowic-eaptis	Enabled	[WPA2][Auth(802.1X)]	

2. Enable FlexConnect Local Switching and FlexConnect Local Auth

cisco	MONITOR WLANS CONTRO	OLLER WIRELESS SECU	IRITY MANAGEMENT	COMMANDS HELP EEEDBACK	
/LANs	WLANs > Edit 'ciscowic	-peap*			
WLANS WLANS	General Security C	Policy-Mapping	Advanced		
Advanced				Media Session Snooping	Enabled
	Scan Defer Time(msecs)	100		Re-anchor Roamed Voice Clients	Enabled
	FlexConnect			KTS based CAC Policy	Enabled
	FlexConnect Local	_		Radius Client Profiling	
	Switching 2	Enabled		DHCP Profiling	0
	FlexConnect Local Auth	Enabled		HTTP Profiling	0
	Learn Client IP Address	Enabled		Local Client Profiling	
	Van based Central	E Linkowa		DHCP Profiling	0
	Switching 12	Enabled		HTTP Profiling	
	Central DHCP Processing	Enabled		PHIP	
	Override DNS	Enabled		PHIP Mobility Type	None 1
	NAT-PAT	C Enabled		PMIP Profile	
					None 1
				PMSP Realm	
				mDNS	
				mDNS Snooping	Enabled

Figure 15 WLANs for Local Switching and Local Authentication

3. Enable AP Local Authentication.

Enable 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

cisco	MONITOR WLANS CONTROLLER W	RELESS SECURITY HUMAGEMENT	соння	WIDS HELP	FEEDBACK			i (Ing Legout
Wireless * Access Points Al Ah * Bades 802.11A/n/Ac 802.11A/n/Ac 802.11A/n/Ac 802.11A/n/Ac	FlexConnect Groups > Edit 'abo General Local Authentication Group Name abo Enable Al Local Authentication	Image Upgrade ACL Mapping	Centr	at DHCP W	LAN VLAN map	ping		Apply
Elutel Configuration Advanced	FlexConnect APs			AAA				
Hesh RF Profiles FlexConnect Groups Deconnect Alls	Add AP AP MAC Address AP Name (c-99-47:50-79-91 AP 3600	Status Associated		Server IP Add Server Type Shared Secret		Primary	9	_
 802.11a/n/ac 802.11b/g/n Media Stream 				Confirm Share Port Number	id Secret	1812		
 Application Visibility And Control Country Timers Netflow 			-	Server Type UnConfigured UnConfigured	Address Unconfigured Unconfigured	Part D D	0	
> QoS								

- **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.

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	COMMANDS	HELP FEEDBACK
Commands Download File Upload File Reboot Config Boot	Download file to Controller File Type Certificate Password Transfer Mode Server Details	Vendor Device Certificate	1	
 Scheduled Reboot Reset to Factory Default Set Time Login Banner 	IP Address Maximum retries Timeout (seconds) File Path	10 6 /		
	File Name	ciscowlcdev.pem		

Figure 17 Downloading Vendor Device Certificate



Downloading Vendor CA Certificate

uluilu cisco	MONITOR WLANS CONTROLLER W	RELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Commands Download File Upload File Reboot Config Boot	Download file to Controller File Type Transfer Mode Server Details	Vendor CA Certificate	
 Scheduled Reboot Reset to Factory Default Set Time Login Banner 	IP Address Maximum retries Timeout (seconds) File Path File Name	10 6 / ciscowicca.pem	

- **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.

Local Users Protoc EAP Fast Enable EAP Fast Authentication ² Server Key (in hex)	Enable	s Auto key generation			
Enable EAP Fast Authentication ²	Enable				
Authentication ²	Enable				
	Enable				
Server Key (in hex)					
			•••	1	
				(Confirm server key)	
Authority ID (in hex)	4369736	436973636f00000000000000000000000]	
Authority Info	Cisco A_	,ID		1	
PAC Timeout (2 to 4099 days)					
PEAP					
Enable PEAP Authentication ²	۷				
EAP TLS					
Enable EAP TLS	M				

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

		lash:/					
2 3	-rwx drwx				15:48:41 04:04:36		event.log configs
17	-rwx	1513	Feb 28	2013	18:37:11	+00:00	eapdev.pem.ca
54	-rwx	1704	Feb 28	2013	18:37:11	+00:00	eapdev.pem.crt
56	- rwx	963	Feb 28	2013	18:37:11	+00:00	eapdev.pem.prv
61	-rwx		Feb 28	2013	18:37:11	+00:00	eapdevpwd

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.

neral Security Advanced			
⊚ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	EAP-TLS	~
O WPA/WPA2 Passphrase			
○ 802.1x	802.1x EAP Type:	EAP-TLS	15
Pre-Shared Key (Static WEP) None			
Configure	Allow Association to Mered Cr Profile Locked		
	Limit Time for Finding Domain	Controller To:	\$ S
Group Policy Delay.	60 😂 sec		

Figure 21 Wireless Profile for EAP-TLS

Figure 22 Validate Server Identity

ſ

Validate Server Identity	
Trusted Root Certification Authorities	~
Select a Certificate	
Administrator [Issued by: sskcert 11/22/2	012]
Server/Domain Name	
.ogin Name	
access of the second se	
accel.	

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

on Options	Help		
urrent Status	Profile Management	Diagnostics	
CISCO SYSTI		ciscowic-eapils	
		Authenticated	Network Type: Infrastructure
Wireless Mode.		5 GHz 54 Mbps	Current Channel: 48
Server	Based Authentication:	EAP-TLS	Data Encryption: AES
_	IP Address:	9.5.56.102	
	Signal Strength:		Excellent
			Advanced

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)

1

General	Security	Privacy	Content	Connections	Programs	Advanced
Conte	ent Advisor				-	
3	Ratings viewed	s help you on this co	mputer.	Enable	ent that can l	
Certifi	cates					
		rtificates to ies, and p		identify yourse	lf, certification	on
	Clea	r SSL Stat		ertificates	Publishe	rs
Perso	nal informa	ition				
			ores previo tches for y		AutoComp	lete
		oft Profile A al informat	Assistant sl ion.	tores your	My Profi	le
C						

Figure 24 Certificates on Client

Γ

Issued To	Issued By	Expiratio	Friendly Name	^
SecureSign RootCA1	SecureSign RootCA1	9/15/2020	Japan Certificati Japan Certificati	
SecureSign RootCA2	SecureSign RootCA2	9/15/2020		
SecureSign RootCA3		9/15/2020	Japan Certificati	
SERVICIOS DE CER	SERVICIOS DE CERTI	3/10/2009	SERVICIOS DE C	
SIA Secure Client CA	SIA Secure Client CA	7/9/2019	Societa Interban	
STA Secure Server CA	STA Secure Server CA	7/9/2019	Societa Interhan	12
🗄 sskcert	sskcert	4/5/2017	<none></none>	
Swisskey Root CA		1/1/2016	Swisskey Root CA	٦.
TC TrustCenter Cla	TC TrustCenter Class	1/1/2011	TC TrustCenter	Y
Export	Remove		Advanc	ced
tificate intended purpos	es			

1

Figure 25 Trusted Root (CA) Certificate on Client

itended p	urpose:	<4	4)>							~
Personal	Other Peo	ople	Interm	ediate Ce	ertification	h Authorities	Trus	ted Root	Certificatio	< >
Issued	To		Iss	ued By		Expira	tio	Friendly	Name	
🖻 Adm	ninistrator		ssko	ert		11/22/	2013	<none></none>		
Import		port		Remo	ve				Advan	ced
	E) (E)	-		Remo	ve				Advan	ced
Certificate		purp	oses			tication			Advan	ced

Figure 26 Trusted Client Certificate

Show Commands

Γ

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

IPv6 ACL Name	none
IPv6 ACL Applied Status	
Layer2 ACL Name	
Layer2 ACL Applied Status. The	
Client Type	
mDNS Status	Disabled
mDNS Profile Name	none
No. of mDNS Services Advertised	Θ
Policy Type	WPA2 6 Downloads
Authentication Key Management	802.1x
Encryption Cipher	CCMP (AES)
Protected Management Frame	No
Management Frame Protection	No
АР Туре	EAP-TLS
rexconnect bata switching	
FlexConnect Dhcp Status	
FlexConnect Vlan Based Central Switching	
FlexConnect Authentication	
Quarantine VLAN	
Access VLAN	56

1

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

neral Local	Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping		
ocal Users	Protocols						
No of Users	1			Add User			٦.
amost .	۰			Upload CSV file	4 D		Browse)
				UserName		_	
				Password Confirm Passw	ord		
						Add	
Remove All L	leave						
Remove All	Jsers						

Figure 28 User Addition for Local Authentication

Client Configuration

ſ

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

● WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	PEAP (EAP-MSCHAP V2)	~
WPA/WPA2 Passphrase 802.1x Pre-Shared Key (Static WEP)	802.1x EAP Type:	PEAP (EAP MSCHAP V2)	-
O None	Allow Association to Maxed Co Profile Locked		c
Group Policy Delay	r 60 🗢 sec		

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

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

	r Domain Logon
Validate Server Identity	
rusted Floot Certification Auth	oribes
(Any>	
When connecting, use:	
Certificate	
User Name and Password	
Use Windows User Name	and Password EAP-MSCHAP V2) Authentication
User Name:	
User Name: Password:	••••••
	••••••

1

Figure 30 User Name and Password for PEAP

Options Help		
ent Status Profile Managem	ent Diagnostics	
airtel	^	New
splittunnel blizzard		Modify
criov ciscowic-peap		Remove
ciscowic-peap ciscowic-eaptis	~	Activate
Details		
Network Type:	Infrastructure Disabled	Import
Security Mode: Network Name 1 (SSID1):	spiltunnel	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

Figure 31 Cisco Aironet Desktop Utility Profile Management

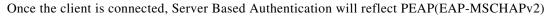


Figure 32 Client Authentication using PEAP(EAP-MSCHAPv2)

ment Status	Profile Management	Diagnostics	
CISCO SYST	EMS		
սՈւսուս	Profile Name:	ciscowlc-peap	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 48
Server	Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES
_	IP Address:	9.5.56.102	
	Signal Strength:		Excellent

ſ

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

igure 33	Web GUI Clier	nt Details			
uluilu cisco	MONITOR WLANS COM	VTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	FEEDBACK
Monitor Summary Access Points Cisco CleanAir Statistics CDP Rogues Redundancy Clients Sieeping Clients Multicast Applications	Clients > Detail General AVC Statis Security Information Security Policy Completed Policy Type Auth Key Mgmt Encryption Cipher EAP Type SNMP NAC State Radius NAC State CTS Security Group Tag AAA Override ACL Name AAA Override ACL Name	Yes RSN (WPA2) CCKM CCMP (AES) PEAP Access RUN Not Applicable			
	Applied Status AAA Override Flex ACL AAA Override Flex ACL Applied Status	Unavailable none Unavailable			
	Redirect URL	none			

+ c

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**

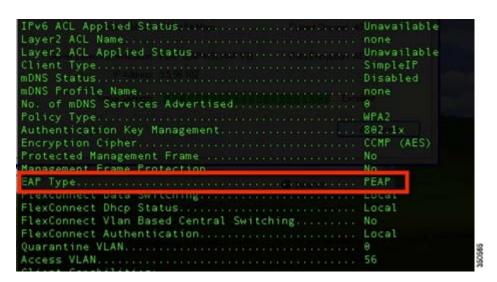


Figure 34 EAP Type of Client Authenticated using PEAP

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></groupname>	radius	ap	peap	<enable th="" <=""><th>disable></th></enable>	disable>
config flexconnect	group	<groupname></groupname>	radius	ap	eap-tls	<enable td="" <=""><td>disable></td></enable>	disable>

A CLI for certificate download has been added as well.

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



Configurations at the AP can be seen from the console.

Figure 35 CLI Commands on AP Console



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 subsys
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.

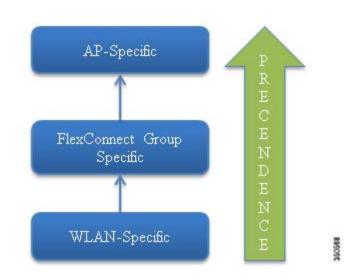
This will push the WLAN to VLAN mapping to all the APs present in the FlexConnect group. The FlexConnect level configuration will have a higher precedence compared to the WLAN-VLAN mapping configured on the WLAN.

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

DENEON

WLANs					
	(Change Filter) (C	Sear Filter)		Create New Co	
WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
C 2 WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]	0
					-
	Current Filter: No	WLAN ID Type Profile Name U WLAN enjoy U WLAN elicowic-peap	Current Filter: None Chance Filter: Clear Filter: WLAN ID Type Profile Name WLAN SSID ULAN SSID WLAN enjoy enjoy WLAN ciscowic-peap ciscowic-peap	Current Filter: None [Chance_Filter]	Current Filter: None (Change Filter) Create New 15 Ga WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies WLAN enjoy enjoy Enabled (WRA2[Aub(102.1X)] WLAN ciscowic-peap Enabled (WRA2[Aub(102.1X)]

Figure 37 WLAN for Local Switching



eneral Security	QoS Policy-Mapping	Advanced	Passive Chem		
ff Channel Scanning Defer			Passive Client	0	
Scan Defer Priority	0 1 2 3 4 5 6 7		Voice		
			Media Session Snooping	Enabled	
Scan Defer Time(msecs)	100		Re-anchor Roamed Voice Clients	Enabled	
exConnect			KTS based CAC Policy	Enabled	
FlexConnect Local Switching 2	C Enabled		Radius Client Profiling		
			DHCP Profiling		
FlexConnect Local Auth	Enabled		HTTP Profiling		
Learn Client IP Address	Enabled		Local Client Profiling		
Vian based Central Switching 12	Enabled		DHCP Profiling	0	
Central DHCP Processing	Enabled		HTTP Profiling		
Override DNS	Enabled		PMIP		
NAT-PAT	Enabled		PMIP Mobility Type	None	

The WLAN is mapped to the management VLAN 56.

Γ

eneral	Security	QoS	Policy-Mapping	Advanced	
Profile Na	ame	enjoy			
Туре		WLAN			
SSID		enjoy			
Status		🗹 Enat	oled		
Radio Pol	licy	All	•		
	/Interface		ement 😜		
Multicast	Vlan Feature	🗌 Enab	led		
Broadcas	t SSID	🗹 Enab	led		
NAS-ID		Aparajit	a_Primary_5500		

1

Figure 39 WLAN Mapped to VLAN 56 Management Interface

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

AP Name	AP_3600			
Base Radio MAC	34:a8:4e:e7:5b:c0			
Make AP Specif	ic 🗘 Go	VLAN ID	NAT-PAT	Inheritance
WLAN	ic 🗘 Go		NAT-PAT	Inheritance Wlan-specifi
WLAN Id SSID		ID		

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

🖻 Cisco Aironet Desktop Utility	y - 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:	9.5.56.102		
Signal Strength:		Excellent	
		Advanced	

Figure 41 Client in VLAN 56

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

Figure 42 WLAN Mapped to VLAN 57 under FlexConnect Group

	Local Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping	
	AN Mapping					
WLAN Id						
Vlan Id	1 Add					
LAN Id	WLAN Profile Name	Vian 57	1.			

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

ſ

All APs > Details for AP_3600 General Credentials Interfaces High Availability Inventory FlexConnect Advanced VLAN Support ً VLAN Mappings Native VLAN ID 56 FlexConnect Group Name abc **PreAuthentication Access Control Lists** External WebAuthentication ACLs Local Split ACLs Central DHCP Processing OfficeExtend AP Enable OfficeExtend AP Enable Least Latency Controller Join Reset Personal SSID 350575

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

AP Name	AP_3600			
Base Radio MAC	34:a8:4e:e7:5b:c0			
VLAN VLAN Map				
Make AP Specifi		VLAN ID	NAT-PAT	Inheritance
Make AP Specifi			NAT-PAT	Inheritance Group-speci
Make AP Specifi WLAN Id SSID	Go	ID		_

The client is assigned an IP address in VLAN 57.

😤 Cisco Aironet Desktop Utility	y - Current Profile: enjoy	?
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS	enjoy	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 108
Server Based Authentication:		Data Encryption: AES
Signal Strength:		Excellent
		Advanced

Figure 45 Client in VLAN 57

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

AP	Name		AP_3600			
Ba	se Radi	o MAC	34:a8:4e:e7:5b:c0			
1	Make A	P Specific	Go			
- A -	Make A WLAN Id	SSID	Go	VLAN ID	NAT-PAT	Inheritance
-	WLAN Id		Go		NAT-PAT	Inheritance AP-specific
	WLAN Id	SSID		ID		

The client is assigned an IP address in VLAN 58.

Γ

Figure 47

😤 Cisco Aironet Desktop Utilit	y - Current Profile: enjoy		?×
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utiliutiliu. Profile Name:	enjoy		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 108	
Server Based Authentication:		Data Encryption: AES	
IP Address:	9.5.58.100		
Signal Strength:		Excellent	
		Advanced	

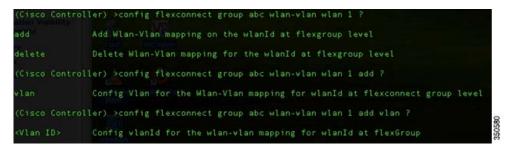
Client in VLAN 58

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>
- 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



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

(Cisco Control	ler) >show flexco	nnect grou	up detail abc		
Number of AP's	in Group: 1				
fc:99:47:60:f9	:91 AP_3600	Joined			
Efficient AP I	mage Upgrade	Disabled	i		
Master-AP-Mac	Master-AP-Nam		Profile Name" • Mo	del Manua	
Group Radius S Type	ervers Settings: Server Address	Port			
Primary Secondary	Unconfigured Unconfigured	Unconfig Unconfig			
EAP-FAST Auth. LEAP Auth EAP-TLS Auth EAP-TLS CERT D	er. En Di En en ownload. En En	sabled abled abled			
Server Key Authority ID Authority Info)uit o Generated No 431 Ci 0	6973636f00		****	
	verridden interfa 's in Group: 1 apsond	ce config:	Disabled		
Group-Specific	FlexConnect Wlan	-Vlan Mapp	oing:		
ULAN ID VI	an ID				
WLAN ID SSID			Central-Dhcp	Dns-Override	Nat-Pat

Figure 49 show flexconnect group detail Output

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

FlexConn FlexConn	Native ID Language WLAN 1 WLAN 4 WLAN 5 ect VLAN ACL Mappings ect Group AN ACL Mappings	57 56 56 56 56	(Group-Specific) (Wlan-Specific) (Wlan-Specific) (CompSpecific)	
L2Acl Co	fic FlexConnect Policy ACI nfiguration ect Local-Split ACLs :			
WLAN ID	PROFILE NAME	ACL		TYPE
Flexcon	nect Central-Dhcp Values			

The following commands can be used to troubleshoot this feature:

On WLC:

• debug flexconnect wlan-vlan <enable | disable>

On AP:

ſ

• 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.

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.
- Client ACL applied in addition to VLAN-ACL, both can exist simultaneously and are applied serially.



Steps to Configure Client ACL

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

Figure 51 Create Local Switching WLAN

rrent Filter	. None	[Change Filter] [0	lear Filter]		Create New Go	
WLAN ID	Туре	Profile Name	WLAN SSID	Admin Status	Security Policies	
	WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]	
2	WLAN	ciscowic	ciscowlc	Enabled	[WPA2][Auth(802.1X)]	
4	WLAN	ciscowlc-peap	ciscowlc-peap	Enabled	[WPA2][Auth(802.1X)]	
2 5	WLAN	ciscowlc-eaptls	ciscowlc-eaptls	Enabled	[WPA2][Auth(802.1X)]	

2. Turn on AAA override for the WLAN

Enable AAA override

neral Security	QoS Policy-Mapping Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	C Enabled	DHCP Server Override
Enable Session Timeout	Session Timeout (secs)	DHCP Addr. Assignment 🛛 Required
Aironet IE	✓Enabled	OEAP
Diagnostic Channel	Enabled	Split Tunnel Enabled
Override Interface ACL	IPv4 None IPv6 None IPv6	
P2P Blocking Action	Disabled	Management Frame Protection (MFP)
Client Exclusion 2	Enabled 60 Timeout Value (secs)	MFP Client Protection 1 Optional
Maximum Allowed Clients	0	DTIM Period (in beacon intervals)
Static IP Tunneling	Enabled	802.11a/n (1 - 255) 1
Wi-Fi Direct Clients Policy	Disabled	802.11b/g/n (1 - 255) 1
Maximum Allowed Clients		NAC

3. Create a FlexConnect ACL

I

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

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Wireless	FlexConn	ect Acc	ess Control L	.ists						
Access Points All APs * Radios	Acl Name									
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration										
Advanced										
Mesh										
RF Profiles										
FlexConnect Groups										
802.11a/n/ac										
802.11b/g/n										
Media Stream										
Application Visibility And Control										

1

Figure 52 Configure FlexConnect ACL

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

Figure 53 ACL Mapping on FlexConnect Group

FlexCo	nnect Groups > Edit	'abc'				
Gener	al Local Authentica	ation Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping	
AAA	VLAN-ACL mapping	WLAN-ACL mapping	Policies			
Pc	cies blicy ACL act a Add]	۰			

AP Name	AP_3600	
Base Radio MAC	34:a8:4e:e7:5b:c0	
WLAN ACL Map	ping	
WLAN Id 0		
WebAuth ACL	aci 🔹	
	Add	
-	Add AN Profile Name WebAuth ACL	
WLAN Id WL		
-	AN Profile Name WebAuth ACL	
WLAN Id WL	AN Profile Name WebAuth ACL	
WLAN Id WL Policies Policy ACL acl	AN Profile Name WebAuth ACL	

Figure 54 ACL Mapping on AP

I

Γ

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



abab	User Setup	×
cisco	o Help	F
Setup	[14179\004] Aire-802.1P-Tag O Account Disabled Deleting a Username	-
(Broup Setup	[14179/005] Aire-Interface-Name [14179/005] Aire-Interface-Name Password Authentication	
Network Configuration	Group to which the user is assigned Group to which the user is assigned Callback	
System	acl Client IP Address Assignment Advanced Settings	
Interface Configuration	Contract 0 Nature Access Restrictions	
Administration Control	Contract	
Databases	0 Advanced TACACS+ Settings	
Posture Validation	[14179/009] Aire-Data-Bandwidth-Burst-Contract TACACS+ Enable Password TACACS+ Outbound Password TACACS+ Outbound Password	
Profiles	TACACS+ Shell Command Authorization TACACS+ Shell Command Authorization TacAcS+ Shell Command Authorization for Network Device Management Applications TacAcS+ Shell Command Authorization TacAcS+ Shell Command Authorization TacAcS+ Shell Command Authorization	
Documentation	TACAC5+ Unknown Survices Inter RADUS At Works Survices Inter RADUS At Works RADUS Vender Survices RADUS Vender Survices	
	EADIUS Vender-Specific Attributes Time Bound Alternate Group	
[Submit Delete Cancel	

A Home Operations Policy A	dministr	ation 🔻
🚑 Authentication 💿 Authorization	🛃 Prof	filing 🔗 Posture 👸 Client Provisioning 🚊 Security Group Access 🦺 Policy Elements
Dictionaries Conditions Results		
Results		
	P	MACSec Policy
◆• ■/=	2.	I NEAT
Authentication		
* 🧰 Allowed Protocols	- 11	Web Authentication (Local Web Auth)
a Default Network Access		
* 🧰 Authorization		Airespace ACL Name acl
Authorization Profiles	- 16	0.101100
Downloadable ACLs	- 11	
Inline Posture Node Profiles		 Advanced Attributes Settings
Profiling Posture		Radius:Tunnel-Private-Group-ID 😳 = atish-9 📀 Tag ID 2

1

Figure 56 Airespace ACL Name on ISE

6. Authenticate the client.

🖻 Cisco Aironet Desktop Utilit	y - Current Profile: ciscowlo		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	ciscowlc		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 157	
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES	
IP Address:	9.5.56.102		
Signal Strength:		Excellent	
		Advanced	

CLI Configuration

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



Figure 57 show access-lists Output

Figure 58 Client ACL on AP

									Split-ACL	Client-ACL	L2-AC
				8-8 (8) 3388					Charles of the second	and the recessions	
040.96b8.d4be		30 40244	888 1F2 38	0-0 (0) 0188	208 8-18	66FF666668	0868	868		act	
	(Client) M	axfri Def	UniPri Defi	ultfri Wiredfr	ot						
cd1.c386.7edc											
40.96b8.d4be											
	Agr TxLt Pi	kL MaxL		AC counts							
d1.c386.7edc	18 38 8 6!	5468									
40.96b8.d4be	10 15 0 0			0 (0,0)	8 (8,8						
				TxPkts KByte							

http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

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.
- 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_lrad.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 recompenses 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.

1

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 9.5.56.1 255.255.0
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
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

ſ

Enabling VideoStream—Global

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

Figure 59 WLC Configuration

uluili. cisco	MONITOR	<u>w</u> lans	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Controller	Multicast					
General Inventory Interfaces		obal Multic		8 8		
Interface Groups	IGMP Tim	eout (30-7	200 seconds)	60		
Multicast	IGMP Que	ery Interval	(15-2400 seconds) 20		
Network Routes	Enable MI	LD Snoopin	9	2		
Redundancy	MLD Time	out (30-72	200 seconds)	60		
Internal DHCP Server	MLD Que	ry Interval	(15-2400 seconds)	20		
Mobility Management						
Ports						
▶ NTP						
► CDP						

(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.

cisco	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Wireless Access Points 	Media Stream >Genera	1 🔨					
All APs	Multicast Direct feature	S Enabled					
✓ Radios 802.11a/n/ac 802.11b/g/n	Session Message Config	1					
Dual-Band Radios Global Configuration	Session announcement Stat	e 🔄 Enabled					
Advanced	Session announcement URL						
	Session announcement Ema	ill	-				
Mesh	Session announcement Pho	ne					
RF Profiles							
Network Lists	Session announcement Note						
FlexConnect Groups				a			
▶ 802.11a/n/ac							
▶ 802.11b/g/n							
 Media Stream General Streams 							

Figure 60 Enable VideoStream - Global

(Cisco Controller) >config media-stream multicast-direct ?enableEnable Global Multicast to Unicast ConversiondisableDisable Global Multicast to Unicast Conversion

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

1

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs WLANs > Edit 'enjoy' WLANs General Security Cos Policy-Mapping Advanced Burst Real-Time Rate 0 0 Clear Override Per-SSID Bandwidth Contracts (kbps) 15 DownStream UpStream Average Data Rate 0 0 Burst Real-Time Rate 0 0 Use Real-Time Rate 0 0 Burst Real-Time Rate 0 0 UNMM WIM Policy Allowed 2 Type O AP CAC Enabled Multicast Direct Enabled	

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.

eneral Security (QoS Policy-Mapping	Advanced		
Scan Defer Priority	0 1 2 3 4 5 6 7		Passive Client	
			Passive Client	
Scan Defer Time(msecs)	100		Voice	
exConnect			Media Session Snooping	Enabled
FlexConnect Local	C Enabled		Re-anchor Roamed Voice Clients	Enabled
Switching ²	Chooled		KTS based CAC Policy	Enabled
FlexConnect Local Auth	Enabled		Radius Client Profiling	
Learn Client IP Address 5	Enabled		DHCP Profiling	
Vian based Central	Enabled		HTTP Profiling	
Switching 13			Local Client Profiling	
Central DHCP Processing	Enabled		DHCP Profiling	I
Override DNS	Enabled		HTTP Profiling	I
NAT-PAT	Enabled		PMIP	
Central Assoc	Enabled		PMIP Mobility Type	0
			PMIP NAI Type	Hexadecimal +
			PMIP Profile	Nona 1

Figure 61 Enable Local Switching on WLAN



ſ

General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
eneral				Versions		
AP Name		AP_1600		Primary Softwa	are Version	8.0.72.114
Location		default location		Backup Softwa	re Version	0.0.0
AP MAC A	Address	5c:20:56:13:f6:23		Predownload S	tatus	None
Base Rad	io MAC	58:86:a7:cb:c0:d0		Predownloaded	Version	None
Admin St	atus	Enable +		Predownload N	ext Retry Time	NA
AP Mode		FlexConnect	:	Predownload R	etry Count	NA
AP Sub M	lode 🗌	None ÷		Boot Version		15.2.2.0
Operation	nal Status	REG		IOS Version		15.3(20140203:113124)\$
Port Num	ber	L		Mini IOS Versio	on	7.4.1.37
Venue Gr	oup	Unspecified	•	IP Config		
Venue Ty	pe (Unspecified +		IP Address		9.5.56.105
Venue Na	ime			IPv6 Address		
Language				Static IP	(7
Network	Spectrum .	21750626078084	A4A128E3F1D98F252	Static IPv6	(

Add Media Stream Configuration

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

1

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP	Saye Configuration Ping Logout Befresh FEEDBACK
Wireless	Media Stream > New	K	< Back Apply
 Access Points All APs Radios 802.11a/n/ac B02.11b/g/n Dual-Band Radios 	Stream Name Multicest Destination Start IP Address(ipv4/ipv6) Multicest Destination End IP Address(ipv4/ipv6) Maximum Expected Bandwidth(1 to 35000 Kbps)	Media2 229,77.77.28 229,77.77.28 500	
Global Configuration Advanced Mesh RF Profiles Network Lists FlexConnect Groups FlexConnect ACLs B02.11a/n/ac B02.11b/g/n Media Stream	Resource Reservation Control(RRC) Parar Select from predefined templates Average Packet Size (100-1500 bytes) RRC Periodic update RRC Priority (1-8) Traffic Profile Violation	Select : 1200 1 best-effort :	

Figure 63 Media Stream Configuration

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 63. 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.

CISCO	MONITOR WLANS CONT		LLSS SECOR	TT MANAGEMENT	COMMONDS HELF	TECOBACK
LANs	WLANs > Edit 'enjoy'					
WLANS	General Security		y-Mapping	Advanced		
		0	0			
Advanced	Clear					
	Override Per-SSID Ba	ndwidth Contr	acts (kbps)	ē.		
		DownStream	UpStream			
	Average Data Rate	0	0			
	Burst Data Rate	0	0			
	Average Real-Time Rate	0	0			
	Burst Real-Time Rate	0	0			
	Clear					
	WMM					
	WMM Policy	Allowed :				
	7920 AP CAC	Enabled				
	7920 Client CAC	Enabled				
	and the second second second					
	Media Stream					

Figure 64 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 64. 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 65, 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.

uluilu cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY M	ANAGEMENT	COMMANDS	HELP EEE	DBACK	
Ionitor	Clients	Markadan 1	verti di scatta a						
Summary Access Points	Current Filter	None	[Change Filter	[Clear Filter]					
Cisco CleanAir	Client MAC Addr	P Address	AP Name		- r	WLAN Profile	WLAN	SSID	User Name
Statistics	7c:d1:c3:86:7e:dc	9.5.56.100	AP_1600			enjoy	enjoy		Unknown
CDP	88:cb:87:bd:0c:ab	9.5.56.113	AP_1600			enjoy	enjoy		Unknown
Rogues	d8:96:95:02:7e:b4	9.5.56.108	AP_1600			enjoy	enjoy		Unknown
Redundancy Clients Sleeping Clients Multicast Applications Local Profiling									

Figure 65 Client Summary

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 Sever: https://wiki.videolan.org/Documentation:Streaming_HowTo_New/#Streaming_using_the_GUI

Complete the steps:

L

Γ

Join w	vireless clients to the multicast streaming video.
<u>Note</u>	Use VLC player to stream and watch video.
	e click on the VLC icon on your desktop. Click Media > Open Network stream . Choos col = UDP, Address = 229.77.77.28, Port = 1234 in the format udp://@229.77.77.28:123
Click	Play.
L3	B_Switch#show ip mroute
II	P Multicast Routing Table
Fl	ags: 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
Οι	atgoing interface flags: H - Hardware switched, A - Assert winner
1	Timers: Uptime/Expires
]	Interface state: Interface, Next-Hop or VCD, State/Mode
(*	s, 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
(*	s, 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
(*	r, 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.

1

1

սիսիս cisco	MONITOR WLA		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDB
lonitor	Multicast Gro	lps						
Summary Access Points Cisco CleanAir Statistics CDP	Group address	Multicast Group Vlan MGID IGMI Multicast Group vlanId	P/MLD					
Rogues	dynamic57	57	12					
Redundancy	dynamic58	58	13					
Clients	management	56	0					
Sleeping Clients Multicast	FlexConnect M Client-Mac	ulticast Media S Stream-Name		2 22 2249	ne Vlan	ту	pe	
Applications	7c:d1:c3:86:7e:d	c Media2	229.77.77.2	8 AP_160	0 0	Mu	Iticast Dire	ect
Local Profiling	88:cb:87:bd:0c:a	b Media2	229.77.77.2	B AP_160	0 0	Mu	Iticast Dire	ect
	d8:96:95:02:7e:t	4 Media2	229.77.77.2	8 AP 160	0 0	Mu	Iticast Dire	ect

Figure 66 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 67 Wireshark Capture Depicting mc2uc

ter:			Expression Clea	ar Apply S	ave				
	Time	Source	Destination		Length Info				
	108 12,114118000	128 kb/s	44.1 892	MPEO TS	1358 Audro La	A 211 17			_
	109 12,114292000	9.5.56.115	229.77.77.28	MPEG TS			Destination port:		
	110 12.114450000	9.5.56.115	229.77.77.28	MPEG TS			Destination port:		_
	111 12.114646000		229.77.77.28	MPEG TS			Destination port:		
	112 12,114836000	9.5.56.115	229.77.77.28	MPEG TS			Destination port:	search-agent	
	113 12,115024000	DTS 86542.670000000	PTS 86542.790000000	MPEG TS	1358 video-st				
		9.5.56.115	229.77.77.28	MPEG TS			Destination port:	search-agent	
	115 12.118880000	128 kb/s	44.1 kHz	MPEG TS	1358 Audio La				
	116 12.118882000	DTS 86542.710000000	PTS 86542.750000000	MPEG TS	1358 video.st		-		
		9.5.56.115	229.77.77.28	MPEG TS			Destination port:	search-agent	
	118 12.119460000	128 kb/s	44.1 kHz	MPEG TS	1350 Audio La		Sec. 19.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	119 12.119655000	9.5.56.115	229.77.77.28	MPEG TS			Destination port:		
	120 12.120121000	9.5.56.115	229.77.77.28	MPEG TS			Destination port:		
-1	101 10 100649000	Q 5 56 115	229 77 77 28	MDEG TS	1358 Source n	nrt: anr. 2160	Destination nort:	search anent	in the second
			mente l'annue de la companya de la	man					
			1358 bytes captured (10864 b) 5f:6a:49), Dst: Apple 86:7e						
			(9.5.25.115), 051: 229.77.77						-
			(60), Dst Port: search-agent		(f x #331)				
	IEC 13818-1 PID=0		ioo/, bac Porct search-agenc	(12.34)					
	sembled in: 1113	1447 66-5							
	IEC 13818-1 PID=0	XA7 CC-6							
	7c d1 c3 86 7e dc	00 50 b6 5f 6a 49 08 00	PjI						
	08 70 04 d2	01 11 40 24 09 05 38 73							
0									
0	Oc ce 53 fe 54 4d	le 4a fc 16 da 2e bf 81 da 6b f3 50 ca ff b8 b5							

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.
- 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 Controlle	er) > show ap summar y	Y		
Number of APs				
Global AP User N	Vame	Not	Configured	
Global AP Dot1x	User Name	Not	Configured	
AP Name	Slots AP Model	Ethernet MA	C Location	Country
IP Address Cli	ients DSE Location	n		
AP1142 9.5.56.109	2 AIR-LAP1142 0 [0,0	N-A-K9 f0:f7:55:	f1:75:20 default	location IN
AP 2600		,ој Е-N-К9 fc:99:47:	d0.96.00 dofoult	logation IN
9.5.56.110	0 [0,0		d9:00:90 delault	, IOCALION IN
AP3700	2 AIR-CAP3702	E-N-K9 7c:ad:74:	ff:6b:46 default	location IN
9.5.56.116	0 [0,0]	,0]		
AP_3600-2	2 AIR-CAP3602	I-N-K9 a4:4c:11:	f0:e9:dc default	location IN
9.5.56.111	0 [0,0]	,0]		
AP_1600	2 AIR-CAP1602		13:f6:23 default	location IN
9.5.56.105	2 [0,0]	,0]		
	er) > show client su	-		
Number of Client	s	2		
Number of PMIPV6	5 Clients	0		
			GLAN/	
			RLAN/	
MAC Address Wired PMIPV6 Rc		Slot Status	WLAN Auth Prot	ocol Port

88:cb:87:bd:0c	·ab AP 1600	1 Associated	1 Voc	802 11a	1	No
No Local	.ab Ar_1000	i ASSOCIATED	1 165	002.114	± .	110
d8:96:95:02:7e No Local	:b4 AP_1600	1 Associated	1 Yes	802.11a	1	No
		stream multicast-dire				
		en	able			
Allowed WLANs.		1				
(Cisco Control	ler) >show media-:	stream group summary				
Stream Name S Status		End I			Opera	ation
	39.1.1.1	23	39.2.2.2			
Media2 2 Multicast-dire	29.77.77.28 ct	22	29.77.77.28			
(Cisco Control	ler) > show media- :	stream group detail M	Iedia2			
Media Stream N	ame	Ме	edia2			
Start IP Addre	ss	22	9.77.77.28			
End IP Address RRC Parmmeter		22	9.77.77.28			
Avg Packet Si	ze(Bytes)	12	00			
Expected Band	width(Kbps)	50	00			
Policy		Ad	lmit			
RRC re-evalua	tion	pe	eriodic			
QoS	• • • • • • • • • • • • • • • • • • • •	Vi	deo			
Status		Μυ	lticast-di	rect		
-	-	1				
Violation		fa	llback			
		nnect media-stream cl		ry		
		Multicast IP			VLAN	
						-
7c:d1:c3:86:7e Multicast Dire		229.77.77.28	AP_160	0	0	
88:cb:87:bd:0c Multicast Dire		229.77.77.28	AP_160	0	0	
		229.77.77.28	AP_160	0	0	
d8:96:95:02:7e Multicast Dire	CL					
Multicast Dire		nnect media-stream cl	ient Media.	2		

1

IP Multicast Destination Address (end)..... 229.77.77.28

Client Mac	Multicast IP	AP-Name	VLAN	Туре
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
======
Multcast 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 5 , Enabled State 0
WLAN ID 7 , 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 12, 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.

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.

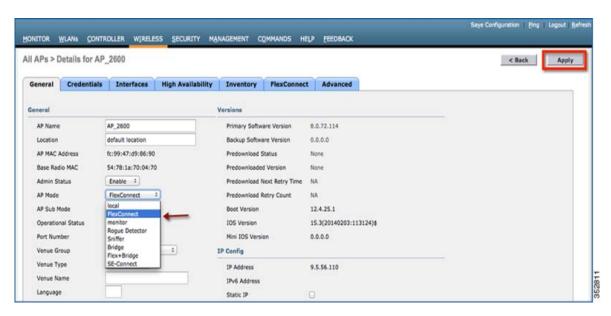


Figure 68 Conversion to FlexConnect - No Reboot Required

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.

Default FlexConnect Group

Introduction

During the initial deployment, the customer configures all access points from a staging controller. Prior to 8.3, day 0 configuration for FlexConnect access points is missing. Therefore the user has to create FlexConnect groups, create policies for remote sites and manually place APs under each group. VLAN support and native VLAN setting is disabled by default on a newly created FlexConnect group, which implies that remote client traffic is placed in an AP VLAN and can access internal, secure resources. There is also a limitation on the number of APs supported within a group that prevents the creation of a generic catch all FlexConnect group for initial deployment.

To overcome these challenges and to make the Day 0 branch setup easier and faster, the concept of a Default FlexConnect group has been introduced in release 8.3.

When the controller boots up, the "default-flex-group" is created by default. This group cannot be deleted or added manually. Similarly access points cannot be manually added to or deleted from the default-flex-group.

The group has default configuration for the FlexConnect group parameters upon creation and has no maximum limit on the number of APs that can be part of it. Any change in configuration gets propagated to all the APs that are part of this group and the configuration of the group is retained across resets.

When an AP in FlexConnect mode, which is not part of any admin-configured FlexConnect group, joins the controller, it becomes part of the default-flex-group and gets the configuration from this group.

In controllers such as Cisco Flex 7500 Series Controller, when the autoconvert mode is set to "flexconnect", during AP join, the AP gets converted to flexconnect mode and inherit config from default-flex-group thus supporting zero touch configuration.

Similarly when an admin configured FlexConnect group gets deleted or the AP is manually removed from such a group, the AP becomes part of the default-flex-group and inherits the config from this default group.

Features supported on Default FlexConnect Group

- VLAN support, Native VLAN, WLAN-VLAN mappings
- VLAN ACL mappings
- Webauth, Webpolicy, local split ACL
- Local authentication users
- RADIUS authentication
- Central DHCP/NAT-PAT

- Flex AVC
- VLAN name ID mappings
- Multicast override

Features Not Supported on Default FlexConnect Group

- Efficient image upgrade
- PMK cache distribution

Default FlexConnect Group with PnP

As a part of the zero-touch deployment, PnP server pushes configuration information to the AP. As of 8.2 the configuration contains WLC IPs, WLC names, AP mode and AP group name. This configuration has been extended to include the FlexConnect Group name starting release 8.3.

The feature is supported on the following APs that have PnP enabled:

AP 700,1600,1700,2600,2700,3600,3700, 1832,1852, 2802,3802,1810

When the AP joins the WLC it presents this FlexConnect group name to the WLC. The WLC then places the AP into an appropriate group after comparing pre-existing configurations and AP count on the FlexConnect Groups. There are various scenarios involved in deciding the FlexConnect group the AP will be placed in. The following specifically refer to scenarios where the AP will be placed as part of the default-flex-group.

Day 0 Setup Scenario

- 1. AP boots up and contacts the PnP server. PnP server does not have FlexConnect group configuration as part of the configured attributes. Also, the AP is not configured as part of any FlexConnect Group on the WLC. In this case, the AP is placed into the default-flex-group.
- 2. AP boots up and contacts the PnP server. PnP server returns a FlexConnect group configuration. The FlexConnect Group exists on the WLC but has reached the maximum capacity in terms of AP count. In this case, the AP is placed into the default-flex-group.

Day 1 Join Scenario

- 1. AP Joins WLC and does not have an AP to FlexConnect Group Mapping on the WLC
- 2. AP Joins WLC. AP has FlexConnect Group configuration present, but the FlexConnect group not configured on the WLC
- **3.** AP has FlexConnect Group configuration present, but FlexConnect group has reached its limit in terms of number of APs

Default FlexConnect Group Web UI

Step 1 To view the default FlexConnect Group choose WIRELESS > FlexConnect Groups > default-flex-group

Apply

	WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS HELP EEE
Mesh ATF	FlexConnect Groups	Entries 1 - 3 of 3 New
RF Profiles	Group Name	Number of APs
FlexConnect Groups	SiteA	0
MEACONNECCACES	SiteB	0
FlexConnect VLAN Templates	default-flex-group	1

Step 2

Γ

To view APs that are a part of the default-flex-group click on the FlexConnect AP link in the General tab

FlexConnect Groups > Edit 'default-flex-group'

eneral Local Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping
LAN AVC mapping				
Group Name defaul	t-flex-group			
/LAN Template Name none				
Enable AP Local Authentication ²				
exConnect AP				

Step 3 APs from default-flex-group can be moved to an admin configured FlexConnect group. Select the Group from "New Group Name" drop down menu and select the AP from the list and then click 'Move'

FlexConnect Group AP List

New Group Name	None 🗘	
Move	pod1-flex	
lexConnect APs		
	AP Name	Status

Upgrade or Downgrade behavior

Upon downgrading from release 8.3 to a lower version, the controller will retain the default-flex-group configuration. This group will be treated as any other admin-configurable FlexConnect group, i.e deletion and addition is possible, APs can be manually added or deleted from the group and the maximum limit on number of APs is applicable. Since the support for default-flex-group feature does not exist in earlier releases, FlexConnect APs will not join this group by default.

Upon upgrade to release 8.3 any FlexConnect AP that is not part of a FlexConnect group will join the default-flex-group and get the related default configuration. The rules of inheritance will continue to apply and therefore any AP specific FlexConnect Configuration will not be overwrited by the default FlexConnect group config.

CLI Commands

• The existing show command would display the configuration of the default-flex-group and the APs that are part of it.

show flexconnect group detail default-flex-group

• For all the APs that are part of this default group, the "show ap config general <apname>" command would reflect the default FlexConnect Group as shown below

FlexConnect Group..... default-flex-group

• A new cli command as below is introduced to display only the APs that are part of a specific group.

(Cisco Controller) >show flexconnect group detail default-flex-group aps

Number of APs in Group: 1

AP Ethernet MAC	Name	Status	Mode	Туре	Conflict with PnP

7c:0e:ce:f5:b2:a4 AP7c0e.cef5.b2a4 Joined Flexconnect Manual No

• A new cli command as below is introduced to allow copying of configuration from existing flexconnect group during creation of new groups. – VERIFY ?

config flexconnect group newGrpname add copy oldGrpName

• The default-flex-group cannot be created or deleted manually. Similarly APs cannot be added or deleted manually to the default-flex-group. So the following commands will throw an error upon execution:

(Cisco Controller) >config flexconnect group default-flex-group add Group default-flex-group has already been configured (Cisco Controller) >config flexconnect group default-flex-group delete Group default-flex-group cannot be deleted manually (Cisco Controller) >config flexconnect group default-flex-group ap add 23:2f:d2:ff:12:7d AP cannot be manually added to the default-flex-group. (Cisco Controller) >config flexconnect group default-flex-group ap delete 23:2f:d2:ff:12:7d AP cannot be manually deleted from the default-flex-group.

SNMP

The existing tables cLReapGroupConfigTable and cLReapGroupApConfigTable in CISCO-LWAPP-REAP_MIB would return the configuration of the default-flex-group and the joined APs respectively

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/i ndex.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
- 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.



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

