· I | I · I | I · I CISCO

Flex 7500 Wireless Branch Controller Deployment Guide

Last Updated: 04/28/2015

Introduction

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

- Explain various network elements of the Cisco FlexConnect solution, along with their communication flow.
- Provide general deployment guidelines for designing the Cisco FlexConnect wireless branch solution.
 Note: Prior to release 7.2, FlexConnect was called Hybrid REAP (HREAP). Now it is called FlexConnect.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Product Overview

Figure 1 Cisco Flex 7500



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

Product Specifications

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

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

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

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

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

Product Specifications

Data Sheet

Refer to Cisco Flex 7500 Series Cloud Controller Data Sheet: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ ps11635/data_sheet_c78-650053.html

Platform Feature

Figure 2 Flex 7500 Rear View

Rear View:



Product Specifications

Network Interface Ports

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

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

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

System MAC Addresses

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

Serial Console Redirect

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

Inventory Information

The following is the WLC 7500 Console:

(Cisco Controller) >show inventory

Burned-in MAC Address..... E4:1F:13:65:DB:6C

Maximum number of APs supported...... 2000

NAME: "Chassis", DESCR: "Cisco Wireless Controller"

PID: AIR-CT7510-K9, VID: V01, SN: KQZZXWL

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

Flex 7500 Boot Up

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

Flex 7500 Boot Up

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

Figure 3 Boot-Up Order

| Cisco Bootloader | (Versio | n |) | | |
|-----------------------------|-----------|------------|---------|---------|---------|
| | | | | | |
| | | | | | |
| | .088b. | d888888b | .d8888. | .088b. | .d88b. |
| | d8P Y8 | `88' | 88' YP | d8P Y8 | .8P Y8. |
| | 8P | 88 | .od8′ | 8P | 88 88 |
| | d8 | 88 | `Y8b. | 8b | 88 88 |
| | YSb d8 | .88. | db 8D | YSb dS | '8b d8' |
| | `Y88P' | Y888888P | ,8888Å, | `Y88P' | `Y88P' |
| | | | | | |
| | | | | | |
| Booting Primary Image | · · · · | | | | |
| Press <esc> now for a</esc> | addition | al boot op | ptions | | |
| | | | | | |
| Boot Options | | | | | |
| | | | | | |
| Please choose an opti | ion from | below: | | | |
| | | | | | |
| 1. Run primary image | e (Versio | on | . (d | efault) | |
| 2. Run backup image | (Versi | on | | | |
| 3. Manually upgrade | primary | image | | | |
| 4. Change active boo | ot image | | | | _ |
| 5. Clear Configuration | ion | | | | DM44 |
| | | | | | 95 |

Flex 7500 Licensing

Figure 4 WLC Configuration Wizard

| Would you like to terminate autoinstall? [yes]: |
|---|
| System Name [Cisco_65:db:6c] (31 characters max): AUTO-INSTALL: process terminated no configuration loaded |
| Enter Administrative User Name (24 characters max): admin Default values (admin or Cisco or its variants) in password is not allowed. Enter Administrative Password (24 characters max): ******* Re-enter Administrative Password : ******* |
| Management Interface IP Address: 172.20.227.174 Management Interface Netmask: 255.255.255.224 Management Interface Default Router: 172.20.227.161 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num [1 to 2]: 1 Management Interface DHCP Server IP Address: 172.20.227.161 |
| Virtual Gateway IP Address: 1.1.1.1 |
| Mobility/RF Group Name: mobility |
| Network Name (SSID): DataCenter |
| Configure DHCP Bridging Mode [yes][NO]: NO |
| Allow Static IP Addresses [YES][no]: Yes |
| Configure a RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details. |
| Enter Country Code list (enter 'help' for a list of countries) [US]: |
| Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes |
| Configure a NTP server now? [YES][no]: no Configure the system time now? [YES][no]: yes Enter the date in MM/DD/YY format: 09/02/10 Enter the time in HH:MM:SS format: 11:50:00 |
| Configuration correct? If yes, system will save it and reset. [yes] [NO]: yes |

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

Flex 7500 Licensing

AP Base Count Licensing

| AP Base Count SKUs |
|--------------------|
| 300 |
| 500 |
| 1000 |
| 2000 |
| 3000 |
| 6000 |
| |

Software Release Support

AP Upgrade Licensing

| AP Upgrade SKUs |
|-----------------|
| 100 |
| 250 |
| 500 |
| 1000 |

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

Refer to the WLC 7.3 configuration guide, which covers the entire licensing procedure.

Software Release Support

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

Supported Access Points

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

FlexConnect Architecture

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 on page 7.
- Distribute the client data traffic at each Branch Office.
 - Data traffic is marked by blue, green, and purple dashes in Figure 5 on page 7.
 - Each traffic flow is going to its final destination in the most efficient manner.

Advantages of Centralizing Access Point Control Traffic

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

FlexConnect Architecture

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.

| 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 |

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

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

For more information on HREAP/FlexConnect AP states and data traffic switching options, refer to Configuring FlexConnect.

FlexConnect Architecture

FlexConnect Modes of Operation

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

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

WAN Requirements

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

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

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

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

Key Features

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

Test Results

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

Recommended BW = 1.54 Mbps

Recommended RTT latency = 400 ms

Wireless Branch Network Design

Test Results

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

Recommended BW = 1.024 Mbps

Recommended Latency = 300 ms

Wireless Branch Network Design

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

Primary Design Requirements

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

Figure 6 Wireless Branch Network Design



Features Addressing Branch Network Design

Overview

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

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

Advantages

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

Features Addressing Branch Network Design

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

| Table 3Features | |
|-----------------|--|
|-----------------|--|

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

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

IPv6 Support Matrix

IPv6 Support Matrix

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

Feature Matrix

Refer to FlexConnect Feature Matrix for a feature matrix for the FlexConnect feature.

Infrastructure Multicast

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

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

AP Groups

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

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

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



Figure 7 Wireless Network Design Reference Using AP Groups

Configurations from WLC

Complete the following steps:

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

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

| cisco | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | Sage Config EEEDBACK | uration Bing- | Logout Eefresh |
|----------|-----------|--------|------------|----------|----------|------------|----------|------|-------------------------|-----------------|------------------|
| WLANs | WLANs> | New | | | | | | | | < Back | Apply |
| WLANS | Type | | WLAN | M | | | | | | | |
| Advanced | Profile N | errive | Store | 1 | | | | | | | |
| | SSID | | store | | | | | | | | |
| | ID | | 17 (| ×. | | | | | | | |

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

| uluulu cisco | MONITOR WLANS CONTROLLER WIREL | ESS SECURITY MANAGEMENT | COMMANDS HELP | Sa <u>v</u> e Configuration Bing EEEDBACK | Logout <u>B</u> efresh |
|-----------------|--------------------------------|-------------------------|---------------|--|------------------------|
| WLANs | WLANs > Edit | | | < Back | Apply |
| WLANS | General Security QuS Advan | ed | | | |
| Advanced | Layer 2 Layer 3 AAA Servers | | | | |
| | Layer 2 Security 6 WPA+WPA2 | × | | | |
| | WPA+WPA2 Parameters | | | | |
| | WPA Policy | | | | |
| | WPA2 Policy | | | | |
| | WPA2 Encryption PAES | KIP | | | |
| | Auth Key Mgmt PSK | ~ | | | |
| | PSK Format ASCII M | | | | |
| | •••••• | | | | |

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

| cısco | MONITOR WLANS CONTROLLER WIRELESS | SECURITY MANAGEMENT | COMMANDS HELP | Sage Configuration Eing Logout Befresh |
|-------------|-------------------------------------|---------------------------------------|---------------------|--|
| WLANs | WLANs > Edit | | | < Back Apply |
| WLANS WLANS | General Security QoS Advanced | | | |
| Advanced | Profile Name Store1 | | | |
| | Type WLAN | | | |
| | SSID store | | | |
| | Status Enabled | | | |
| | Security Policies [WPA2][Auth(P5K)] | | | |
| | (Modifications done under | r security tab will appear after appl | lying the changes.) | |
| | Radio Policy All | | | |
| | Interface/Interface management v | | | |
| | Multicast Vian Feature 🔲 Enabled | | | |
| | Broadcast SSID Enabled | | | |

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

| uluilu cisco | MONITOR WLANS CONTROLL | ER WIRELESS SECURIT | Y MANAGEMENT COMMANDS | Saye S HELP EEEOB | Configuration Eing I ACK | Logout <u>R</u> efresh |
|--|--|----------------------------------|-----------------------|----------------------|-----------------------------|--------------------------|
| WLANs | WLANs > New | | | | < Back | Apply |
| ₩LANS WLANS Advanced | Type Stopped S | ILAN V tore2 8 V | | | | 350452 |
| սիսիս cisco | MONITOR WLANS CONTROLL | R WIRELESS SECURIT | Y MANAGEMENT COMMANDS | Sage C | onfiguration Eng L | agout Befresh |
| WLANs | WLANs > Edit | | | | < Back | Αρρίγ |
| WLANS | General Security QoS | Advanced | | | | |
| ➤ Advanced | Layer 2 Layer 3 AAJ Layer 2 Security 6 WFA+W 2 Max WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Dolcy WPA2 Encryption Auth Key Mgmt PSK Format 4 | AES There AES There CELL V | | - | | 350453 |

| uluulu cisco | MONITOR WLANS CO | VTROLLER WIRELESS S | ECURITY MANAGEMENT | COMMANDS HELP | Sage Configuration Bing EEEDBACK | Logout Befres |
|-----------------|---------------------------------|------------------------------|---------------------------------|----------------------|-------------------------------------|---------------|
| WLANs | WLANs > Edit | | | | < Back | Apply |
| WLANS WLANS | General Security | QoS Advanced | | | | |
| Advanced | Profile Name | Store2 | | | | |
| | Туре | WLAN | | | | |
| | SSID | store | | | | |
| | Status | Enabled | | | | |
| | | | | | | |
| | Security Policies | [WPA2][Auth(PSK)] | | | | |
| | | (Modifications done under si | county tab will appear after ap | plying the changes.) | | |
| | Radio Policy | All | | | | |
| | Interface/Interface Group(G) | management 💌 | | | | |
| | Multicast Vian Feature | Enabled | | | | |
| | Broadcast SSID | Enabled | | | | |

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

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

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

| cisco | MONITOR | WLANS | | WIRELESS SEC | CURITY MANAGEMEN | | S HELP EE | a <u>v</u> e Configuration EDBACK | Ping Logou | <u>R</u> efrest |
|-------------|---------------|------------------------------|---|-----------------------|---|--------|---|--|-------------|-----------------|
| WLANs | WLANs | | | | | | | | Entries 1 | -3 of 3 |
| WLANS WLANS | Current Filte | r: None | [Change | Filter] [Clear Filter | a | Create | New 💌 | Go | | |
| Advanced | | | | | | | | | | |
| AP Groups | WLAN ID | Туре | Profile Name | e | WLAN SSID | | Admin Status | Security Policies | | |
| AP Groups | WLAN ID | Type WLAN | Profile Nam DataCenter | e | WLAN SSID DataCenter | | Admin Status Enabled | Security Policies [WPA + WPA2][Aut | \$(802.1X)] | |
| AP Groups | WLAN ID | WLAN WLAN | Profile Nam DataCenter Store1 | e | WLAN SSID DataCenter store | | Admin Status Enabled Enabled | Security Policies [WPA + WPA2][Aut [WPA2][Auth(PSK) | th(802.1X)] | 0 |
| AP Groups | WLAN ID | Type WLAN WLAN WLAN | Profile Nam DataCenter Store1 Store2 | e | WLAN SSID DataCenter store store | | Admin Status Enabled Enabled Enabled | Security Policies [WPA + WPA2][Auth [WPA2][Auth(PSK) [WPA2][Auth(PSK) | f*(802.1X)] | 0 |

- 7. Click WLANs > Advanced > AP group > Add Group.
- 8. Add AP Group Name as **Store1**, same as WLAN profile **Store1**, and Description as the Location of the Store. In this example, California is used as the location of the store.
- 9. Click Add when done.

| cisco | Say Monitor Wlans controller wireless security monagement commands help see | e Configuration <u>P</u> ing Logaut <u>B</u> efresh JBACK |
|---|--|--|
| WLANS WLANS WLANS WLANS WLANS WLANS AP Groups | AP Groups Add New AP Group AP Group Name Stores Description Cafemia | Entries 0 - 0 of 0 Add Group |
| | AP Group Name AP Group Description | |

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

| cisco | MONITOR WLAN | | WIRELESS SECUR | ITY MANAGEMENT | COMMANDS | HELP | Sage Configuration Ping EEEOBACK | Logout Befresh |
|---|--|--------------------------|---------------------------|----------------|----------|------|-------------------------------------|----------------|
| WLANS WLANS WLANS WLANS Advanced AP Groups | AP Groups Add Nevy AP Gro AP Group Name Description | up Store2 New York | | | | | Entries 1 - 1 of 1 | Add Group |
| | AP Group Name Store1 default-group | | AP Group De California | escription | ٥ | | | |

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

| | MONITOR WLANS Q | ONTROLLER WIRELESS | SECURITY MANAGEMENT | COMMANDS HELP | Save Configuration Ping EEEDBACK | Logout <u>R</u> efresh |
|------------|-------------------------|--------------------|---------------------|---------------|---------------------------------------|------------------------|
| WLANs | AP Groups | | | | Entries 1 - 2 of 2 | Add Group |
| WLANS | AP Group Name | AP G | roup Description | | | |
| * Advanced | Storel | Califo | omia | | | |
| AP Groups | Store2 default-group | New | York | | | 100 |
| | | | | | | 251 |

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

| .ı ı.ı ı. cısco | Sage Configuration Eng Lego MONITOR <u>WLANS C</u> ONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK | ut Befresh |
|--------------------|--|--------------|
| WLANs | Ap Groups > Edit 'Store1' | Back |
| WLANS WLANS | General WLANS APS | ^ |
| AP Groups | Add New | |
| | Interface DataCenter(1) /Interface stare(1)/Store 1 Group(0) stare(1)/Store 2 NAC State Enabled | |
| | Add Cancel WLAN Interface/Interface NAC ID \$\$SID Group(G) \$tate | |

- 18. Go back to the WLANs > Advanced > AP Groups.
- 19. Click AP Group Name Store2 to add or edit WLAN.
- 20. Click Add New to select the WLAN.
- 21. Under WLANs, from WLAN SSID drop-down, choose WLAN ID 18 store(18).
- 22. Click Add after WLAN ID 18 is selected.
- 23. Repeat steps 14 16 for WLAN ID 1 DataCenter(1).

| ı. cısco | Saye Configuration _ Eng MONITORCONTROLLER WIRELESS _ECURITY MANAGEMENT COMMANDS HELP _EEEBBACK | Logout Eefres |
|------------------------|--|---------------|
| WLANs | Ap Groups > Edit 'Store2' | < Back |
| WLANS | General WLANS APs | |
| Advanced AP Groups | Add New | Î |
| | Add New | |
| | WLAN SSID STOCOFUL Store 2 | |
| | Interside descentrals Group(G) store(1) Store 1 Group(G) store(10) Store 2 | |
| | Add Cancel | |
| | WLAN WLAN Interface/Interface NAC ID \$510 Group(G) State | |

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

| The pa | ge at https://172.20.227.174 says: | X |
|--------|--|---|
| 1 | Failed to add interface entry management | |
| | ОК | |

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

Summary

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

FlexConnect Groups



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 on page 18. Because the above scenario is perfectly valid, it raises these concerns:

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

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

Note: FlexConnect Groups are not analogous to AP Groups.

Primary Objectives of FlexConnect Groups

Backup RADIUS Server Failover

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

Note: Backup RADIUS accounting is not supported.

Local Authentication

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



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

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

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

Local EAP (Local Authentication Continuation)





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.

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

CCKM/OKC Fast Roaming

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

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



Figure 11 Wireless Network Design Reference Using FlexConnect Groups

FlexConnect Group Configuration from WLC

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

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

| ،،۱۱،،۱۱،، cısco | MONITOR | <u>W</u> LANs | CONTROLLER | WIRELESS |
|---|-----------|---------------|------------|----------|
| Wireless | FlexConn | ect Gro | ups > New | |
| Access Points All APs Radios | Group Nar | ne Sto | re 1 | |
| Advanced | | | | |
| Mesh | | | | |
| RF Profiles | | | | |
| FlexConnect Groups | | | | 350.466 |

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



5. Click Add AP.

| ဂျက်က cisco | MONITOR | WLANS | <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 | Local | Authentication | Image U | pgrade |
| Advanced Mesh RF Profiles FlexConnect Groups ElexConnect ACLs | FlexCor Add A AP MAC | Address | S AP Name | Sta | itus |

 Check the Enable AP Local Authentication check box to enable Local Authentication when the AP is in Standalone Mode.

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

- 7. Check the Select APs from current controller check box to enable the AP Name drop-down menu.
- 8. Choose the AP from the drop-down that needs to be part of this FlexConnect Group.
- 9. Click Add after the AP is chosen from the drop-down.
- Repeat steps 7 and 8 to add all the APs to this FlexConnect Group that are also part of AP-Group Store 1. See Figure 11 on page 20 to understand the 1:1 mapping between the AP-Group and FlexConnect Group.

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

| cisco | Monitor <u>W</u> lans <u>C</u> ontroller | WIRELESS <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 | P3500 - |
| 802.11a/n 802.11b/g/n Media Stream | Ethernet MAC | 00:22:90:e3:37:df |
| Country | AP MAC Address AP Name | Status |

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

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

| neral Local Authentication | Image Upgrade VLAN-ACL mapping |
|---|----------------------------------|
| ocal Users Protocols | |
| ЕАР | |
| Enable LEAP Authentication ² | |
| EAP Fast | |
| Enable EAP Fast Authentication ² | |
| Server Key (in hex) | Enable Auto key generation |
| | ••••• |
| | •••••• |
| Authority ID (in hex) | 436973636f0000000000000000000000 |
| Authority Info | Cisco A_ID |
| PAC Timeout (2 to 4095 days) | |

13. Under Local Authentication, click Local Users.

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

| Contractor of the local sector of the local se | 1000000000000 | uon | mage opgrade | VLAN-ACL Indpping |
|--|---------------|-----|------------------------------|-------------------|
| ocal Users | Protocols | | | |
| No of Users | | 0 | Add User | |
| lser Name | | | Upload CSV file ¹ | |
| | | | File Name | |
| | | | UserName | cisco |
| | | | | |

- 17. From the top pane, click WLANs.
- 18. Click WLAN ID 17. This was created during the AP Group creation. See Figure 7 on page 13.

| cisco | | WLANS C | CNTROLLER | WIRELESS | SECURITY | MANAGEI |
|----------|--------------|-----------|-----------|-----------------|------------|----------|
| WLANs | WLANs | | | | | |
| WI ANS | Current Filt | ter: None | [Cha | nge Elter] [Cle | ar Filter] | |
| Advanced | | ID Type | Profile N | ame | W | LAN SSID |
| | □ 2 | WEAN | Guest | | G | uest g |
| | □ <u>17</u> | WLAN | Store-1 | | S | tore |

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

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

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

| WLANs > | Edit | 'Store-1' |
|---------|------|-----------|
|---------|------|-----------|

| General Security | Qo | S Advanc | ced |
|------------------------------------|--------------------|------------|----------------------------|
| P2P Blocking Action | | Disabled | - |
| Client Exclusion 3 | | Enabled | 60 Timeout Value (secs) |
| Maximum Allowed Cl | ients 🖁 | 0 | |
| Static IP Tunneling | 1 | Enabled | |
| Wi-Fi Direct Clients P | olicy | Disabled 👻 | 1 |
| Maximum Allowed Cl Per AP Radio | ients | 200 | |
| Off Channel Scanning | Defer | | |
| Scan Defer Priority | 0 3 | L 2 3 4 | 5 6 7 V V |
| Scan Defer Time (msecs) | 100 | | |
| FlexConnect | | | |
| FlexConnect Local Sv 2 | vitching | Enabled | |
| FlexConnect Local Au | uth 💶 | Enabled | |
| Learn Client IP Addre | ess <mark>5</mark> | Enabled | |

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

| Properties | WLAN Configuration Details : 1 |
|----------------------|--------------------------------------|
| System | |
| WLANs | General Security QoS Advanced |
| H WLAN Configuration | |
| AP Groups | HexConnect Local Switching 🗹 Enable |
| FlexConnect | FlexConnect Local Auth 🔍 🔣 Enable |
| Security | Learn Client IP Address 🛛 Enable |
| Access Points | Session Timeout |
| 802.11 | Coverage Hole Detection V Enable |
| 802.11a/n | IPv6 2 Enable |
| 802.11b/g/n | Diagnostic Channel 2 📃 Enable |
| Mesh | Override Interface ACL IPv4 NONE |
| Ports | Peer to Peer Blocking (1) Disable |
| Management | Wi-Fi Direct Clients Policy Disabled |
| Location | Timeout Value 60 (secs) |

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

| •• ci | Lilin Lisco Erime SCO Network C | ontrol Systen | n • Services | ▼ Reports | Adı | nnistation | • |
|--------------|------------------------------------|---------------|-----------------|---------------|----------|------------|------------------|
| cillei Se | nts and Users | • 🗶 Luseble | | More 💌 😨 Irad | k (Ten K | Gidenni | y Hoknown Hisers |
| | MAC Address | IP Address | IP lype | User Name | Type | Vendor | Device Name |
| 0 | 00:22:90:1b:17:42 | | ₽v1 | Unknown | S | Cisco | WCS_SW 0.1.0.22 |
| 0 | 1c:df:0f:66:86:58 | | ₽v4 | Unknown | 5 | Cisco | WC5_SW-9.1.0.22 |
| 0 | 00:21:6a:97:9b:bc | | ₽v4 | host/vikatta | | Intel | oeap-Laiwar-2 |
| 0 | 00:22:90:15:96:48 | | IPv4 | Unknown | | Lisco | WCS_SW-9.1.0.2 |
| 0 | 00:22:90:1b:17:8c | | ₽v1 | Unknown | - | Cisco | WCS_SW 0.1.0.22 |
| Q | 00:25:0b:4d:77:c4 | | ₽v4 | Unknown | 6 | Cisco | WCS_SW-9.1.0.2 |
| 0 | c4:7d:4f:3a:c5:d5 | | TPv4 | Unknown | | CISCO | WC5_SW-9.1.0.2 |
| 0 | 00:21:a0:d5:03:c4 | | ₽v4 | Unknown | | Cisco | WCS_SW-9.1.0.23 |
| 0 | f3:66:f2:67:7f:60 | | ₽v4 | Unknown | 5 | Cisco | WC5_5W-9.1.0.2 |
| 0 | 00:1f:ca:b0:01:b4 | | ₽v4 | Unknown | 6 | Ciscu | WCS_SW-9.1.0.22 |
| 0 | 88:43:e1:d1:df:02 | | ₽v4 | Unknown | | Cisco | WCS_SW-9.1.0.2 |
| 0 | 00:22:bd:1b:c2:b5 | | ₽v1 | Unknown | | Cisco | WCS_SW 0.1.0.2 |
| 0 | f3:66:f2:ab:1e:69 | | ₽v4 | Unknown | 5 | Cisco | WC5_SW-9.1.0.2 |
| 0 | 00:11:58:JUL4:4e | | ₽v4 | Unknown | 8 | Ciscu | WCS_SW-9.1.0.2 |
| 0 | 00:1e:/atbb:21:8d | | ₽v4 | ssimm | | Cisco | oeap-ta war-2 |

| Virtual Domain: RO | OT-DOMAIN | root 👻 Log Ou | ıt 🔎 | • |
|--------------------|-----------|---------------|-----------|---------------------------------------|
| | | | | |
| | | | | Total 299 🛛 😵 🏰 🗸 |
| | | | Show | Associated Clients 🔹 🍸 |
| Location | VLAN | Status | Interface | Quick Filter |
| Unknown | 109 | Associated | Gi1/0/34 | Advanced Filter |
| Unknown | 109 | Associated | Gi1/0/26 | All |
| Root Area | 310 | Associated | data | Manage Preset Filters |
| Unknown | 109 | Associated | Gi1/0/36 | 2.4GHz Clients |
| Unknown | 109 | Associated | Gi1/0/32 | SGHZ Clients |
| Unknown | 109 | Associated | Gi1/0/30 | |
| Unknown | 109 | Associated | Gi1/0/13 | All Wired Clients |
| Unknown | 109 | Associated | Gi1/0/27 | Associated Clients |
| Unknown | 109 | Associated | Gi1/0/12 | Clients known by ISE |
| Unknown | 109 | Associated | Gi1/0/15 | Clients detected by MSE |
| Unknown | 109 | Associated | Gi1/0/28 | Clients detected in the last 24 hours |
| Unknown | 109 | Associated | Gi1/0/14 | Clients with Problems |
| Unknown | 109 | Associated | Gi1/0/9 | Excluded Clients |
| Unknown | 109 | Associated | Gi1/0/29 | FlexConnect Locally Authenticated |
| Root Area | 311 | Associated | voice | New clients detected in last 24 hours |

Verification Using CLI

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

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

FlexConnect VLAN Override

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

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



Summary

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

Procedure

Complete these steps:

1. Create a WLAN for 802.1x authentication.

| seneral | Security | QoS Adv | anced |
|---------------------------------------|--|----------------------------|-------|
| Layer 2 | Layer 3 | AAA Server | |
| Layer 2 | Security ⁶ | VPA+WPA2 2MAC Filtering | × |
| | | | |
| WPA+WPA | 12 Parameter | s | |
| WPA+WPA WPA Po WPA2 P | 12 Parameter licy olicy | s | |
| WPA+WPA WPA Po WPA2 P WPA2 E | A2 Parameter licy olicy ncryption | s V Aes | Пткір |

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

| General Security | QoS | Advance | d | | | | |
|-------------------------|-----------|------------|-----------------|--------|---------------------------------|--------|--------|
| Allow AAA Override | 🗹 E | inabled | | | DHCP | | |
| Coverage Hole Detect | on 🗹 E | inabled | | | DHCP Server | verrid | |
| Enable Session Timeor | A 1800 | nion Times | nut (ence) | | DHC2 Adds Assistment | | |
| Aironet IE | E E | sabled | Jor (secs) | | | equire | |
| Diagnostic Channel | | abled | | | Hanagement Frame Protection | (HEP) | 2 |
| Override Interface AC | IPv4 | | | 1Pv6 | MFP Client Protection 4 Option | nal 👻 | |
| | None | | ~ | None 💌 | DTIM Period (in beacon interval | 5) | |
| P2P Blocking Action | Disa | bled | ~ | | | | - |
| Client Exclusion 2 | E 6 | nabled 6 | 0 | | 802.11a/n (1 - 255) 1 | | |
| Marine Allered Clark | | т | imeout Value (s | ecs) | 802.11b/g/n (1 - 255) 1 | | |
| Maximum Allowed Clie | nts = 0 | | | | NAC | | |
| Static IP Tunneling | LE | nabled | | | NAC State None | | |
| Wi-Fi Direct Clients Po | licy Disa | bled M | | | Load Balancing and Band Select | | |
| Per AP Radio | nts 200 | | | | Client Load Balancing | - | _ |
| ff Channel Scanning I | ofer | | | | Cieffic Coad deterioing | - | |
| Case Defections | 0 1 2 | | 6 6 7 | | Client Band Select Z | | |
| Scan Deter Priority | | | | | Passive Client | | |
| | | | | | Passive Client | | |
| Scan Defer Time | 100 | | | | Voice | | |
| (msecs) | 10000 | | | | Media Session Snooping | | Enable |
| lexConnect | | | | | Re-anchor Roamed Voice Clients | | Enable |
| FlexConnect Local | Er Er | abled | | | KTS based CAC Policy | | Enable |

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

| 🕈 AAA General | Server Index | 1 |
|-----------------------------------|-----------------------|---|
| Authentication | Server Address | |
| Accounting | Shared Secret Format | ASCII 🛩 |
| Falback TACACS+ | Shared Secret | *** |
| LDAP Local Net Lines | Confirm Shared Secret | ••• |
| MAC Filtering Disabled Clients | Key Wrap | (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |
| User Login 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 |

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.

| eneral | Credentials | Interfaces | High Availability | Inventory | Advanced | |
|-----------|---------------|------------------|-------------------|-----------------|-------------------|-----------------------|
| eneral | | | | Versions | | |
| AP Name | - A | P3500 | | Primary Soft | ware Version | 7.2.1.69 |
| Location | de | fault location | | Backup Soft | vare Version | 7.2.1.72 |
| AP MAC | Address co | :ef:48:c2:35:57 | | Predownload | Status | None |
| Base Ra | fio MAC 20 | ::3f:38:f6:98:b0 | | Predownload | ed Version | None |
| Admin S | tatus E | nable 💌 | | Predownload | Next Retry Time | NA |
| AP Mode | 6 | exConnect 🛛 👻 | | Predownload | Retry Count | NA |
| AP Sub M | tode N | one 💌 | | Boot Version | | 12.4.23.0 |
| Operatio | nal Status Ri | G | | IOS Version | | 12.4(20111122:141426) |
| Port Num | iber 1 | | | Mini IOS Ver | sion | 7.0.112.74 |
| Venue G | roup U | nspecified | * | IP Config | | |
| Venue T | vpe U | nspecified 💌 | | IP Address | | 10.10.10.132 |
| Venue N | ame | | | Static IP | | |
| Languag | • | | | | | |
| Network | Spectrum 00 | 045BA896226F411 | 7D98BA920FBA8A16 | Time Statistics | | |
| Interroce | ney | | | UP Time | | 0 d, 00 h 01 m 14 s |
| | | | | Controller As | sociated Time | 0 d, 00 h 00 m 14 s |
| | | | | Controller As | sociation Latency | 0 d, 00 h 00 m 59 s |

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

| eneral | Local Authentication | Image Upgrade | VLAN-ACL mapping | | |
|------------------------------|----------------------------|---------------|--|-------------------------|---|
| Group N exCon | ame Store 1 nect APs | | AAA Primary Radius Server | None | ~ |
| | | | | | |
| dd AP | Ps from current controller | | Secondary Radius Server | None | × |
| Add AP Select A AP Nam | Ps from current controller | AP3500 | Secondary Radius Server Enable AP Local Authentic | None ation ² | * |

7. 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 | 1 |
| switchport mode trunk | 1000 |

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

- 8. 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.
- 9. Navigate to WLAN GUI > Wireless > All APs, click the specific AP > FlexConnect tab, and click VLAN Mapping.

| AP Na | me | AP3500 | |
|------------|----------|-------------------|------|
| Base F | adio MAC | 2c:3f:38:f6:98:b0 | |
| WLAN Id | SSID | | VLAN |
| 1 | Store 1 | | 109 |

10. 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 | |
| IETF 64 | Tunnel-Type | Tagged Enum | [T:1] VLAN | |
| IETF 81 | Tunnel-Private-Group-ID | Tagged String | [T:1] 3 | 0485 |

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

| LAN ACL M | apping | |
|-----------|--------|--|
| Vlan Id | 3 | |

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

Limitations

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

FlexConnect VLAN Based Central Switching

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

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



Summary

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

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

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

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

Procedure

Complete these steps:

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

| General Security | QoS Advanced |
|---|------------------------------------|
| Allow AAA Override | Enabled |
| Coverage Hole Detection | Enabled |
| Enable Session Timeout | 1800 Session Timeout (secs) |
| Aironet IE | Enabled |
| Diagnostic Channel | |
| Override Interface ACL | IPv4 None 💌 IPv6 None 💌 |
| 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 |
| FlexConnect | |

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

| General Security | QoS Advanced |
|---|------------------------------------|
| Allow AAA Override | Fnabled |
| Coverage Hole Detection | |
| Enable Session Timeout | ¥ 1800 Session Timeout (secs) |
| Aironet IE | ✓Enabled |
| Diagnostic Channel | Enabled |
| Override Interface ACL | IPv4 None V IPv6 None |
| 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 | Enabled |
| Learn Client IP Address S | Enabled |

3. Set AP Mode to FlexConnect.

All APs > Details for AP_3500E



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.

| cisco | | <u>W</u> LANs | | WIRELESS | SECURITY | |
|---|--|---------------|--------------------------|-------------|------------|--|
| Wireless | All APs > A | P_3500E | E > VLAN Ma | ppings | | |
| Access Points All APs Radios 802.11a/n | AP Name Base Radio | AP | _3500E 7d:4f:53:24:e0 | | | |
| 802.11b/g/n Global Configuration | WLAN Id St | SID | | аны е 32.25 | VLAN ID | |
| ▶ Advanced | 1 'S | lore 1' : | | | 63 | |
| Mesh RF Profiles | Centrally s | vitched M | lans | | | |
| FlexConnect Groups FlexConnect ACLs | WLAN Id | income a re | SSID | VLAN ID | | |
| 802.11a/n | AP level VL | AN ACL M | apping | | | |
| 802.11b/g/n | Vlan Id | Ingree | SS ACL | Egress A | CL | |
| Media Stream | 63 | none | ~ | none 💌 | | |
| Country Timers | Group level VLAN ACL Mapping Vian Id Ingress ACL Egress ACL | | | | | |

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).

| uluulu cisco | MONITOR WLA | NS <u>C</u> ONTROLLE | R WIRELESS | SECURITY | MANAGEMENT COM | MMANDS HELP | EEEDBACK |
|----------------------|----------------|----------------------|-----------------|------------|----------------|----------------|------------|
| Controller | Interfaces | | | | | | |
| General Inventory | Interface Name | | YLAN Identifier | IP Address | Interface Type | e Dynamic AP M | fanagement |
| Interfaces | dyn | | 62 | 9.6.62.10 | Dynamic | Disabled | |
| Interface Groups | management | | 61 | 9.6.61.2 | Static | Enabled | |

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.
FlexConnect VLAN Based Central Switching

| Monitor Summary Access Points Cisco CleanAir | Clients > Detail | | AP Properties | |
|---|---|---------------------------------|--|---|
| Statistics CDP Rogues Redundancy | MAC Address IPv4 Address IPv6 Address | 00:40:96:58:64:5e 9.6.62.100 | AP Address AP Name AP Type WLAN Profile | o4:7d:4f:53:24:e0 AP_3500E 802.11e *Store 1* |
| Multicast | | | Data Switching 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 |

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

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.

FlexConnect VLAN Based Central Switching

| lient Properties | | AP Properties | |
|------------------|-------------------|------------------------------------|-------------------|
| MAC Address | 00:40:96:b8:d4:be | AP Address | o4:7d:4f:53:24:e0 |
| IPv4 Address | 9.6.61.100 | AP Name | AP_3500E |
| IPv6 Address | | AP Type | 802.11a |
| | | WLAN Profile "St Data Switching | Central |
| | | Authentication | Central |
| | | Status | Associated |
| | | Association ID | 1 |
| | | 802.11 Authentication | Open System |
| | | Reason Code | з |
| | | Status Code | 0 |
| Client Type | Regular | CF Pollable | Not Implemented |
| User Name | betauser2 | CF Poll Request | Not Implemented |
| Port Number | 1 | Short Preamble | Not Implemented |
| Interface | management | PBCC | Not Implemented |
| UI AN 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.

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:et |
| IPv4 Address | 9.6.63.100 | AP Name | AP_3500E |
| IPv6 Address | | AP Type | 802.11a |
| | | WLAN Profile | 'Store 1' |
| | | Data Switching | Local |
| | | Authentication | Central |

Limitations

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

FlexConnect ACL

FlexConnect ACL

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



Summary

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

Procedure

Complete these steps:

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

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

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

FlexConnect ACL

| Access Control Lists > New | < Back Apply | 1 |
|---|--------------|--------|
| Access Control List Name Flex-ACL-Ingress | | |
| | | |
| | | 150408 |

- 4. Click Apply.
- 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 | e ral s List Nam | e Flex-ACL- | Ingress | | | | | | |
| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | | |
| | | | | | | | | | |

6. Click Add New Rule.

| Access Control Lis | sts > Rules > New | | | < Back | Apply |
|--------------------|-------------------|-----------------------|--------------------|--------|--------|
| Sequence | 1 | 10 4 4 4 4 4 4 | Nataral | | |
| Source | IP Address 💌 | 0.0.0.0 | 0.0.0.0 | | |
| Destination | IP Address 💌 | IP Address 0.0.0.0 | Netmask 0.0.0.0 | | |
| Protocol | Any 💌 | | | | |
| DSCP | Any 💌 | | | | |
| Action | Deny 💌 | | | | 350500 |

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

- 7. Once the FlexConnect ACLs are created, it can be mapped for WLAN-VLAN mapping under individual FlexConnect AP or can be applied on VLAN-ACL mapping on the FlexConnect Group.
- 8. Map FlexConnect ACL configured above at AP level for individual VLANs under VLAN mappings for individual FlexConnect AP. Navigate to WLC GUI > Wireless > All AP, click the specific AP > FlexConnect tab > VLAN Mapping.

FlexConnect ACL

| AP Name | | AP3500 | | |
|--|---------------------------------------|------------------------|----------|----------------|
| Base Rad | lio MAC | 2c:3f:38:f6:98 | ::60 | |
| WLAN Id | SSID | | | VLAN ID |
| 1 | Store 1 | | | 109 |
| | | | | |
| entrally VLAN Id | switche SSID | ed Wlans | | VLAN ID |
| entrally WLAN Id 2 | switche SSID Store 3 | ed Wlans | | VLAN ID N/A |
| entrally WLAN Id 2 P level | Switche SSID Store 3 | ed Wlans CL Mapping | | VLAN ID N/A |
| Centrally WLAN Id 2 \P level Vlan Id | Switche SSID Store 3 VLAN AC | ed Wlans CL Mapping | Egress / | VLAN IE N/A |

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.

| General | Local Authentication | Image Upgrade | VLAN-ACL mapping | |
|-----------|----------------------|---------------|------------------|--|
| LAN ACL | Mapping | | | |
| Vlan Id | 0 | | | |
| Ingress A | CL Flex-ACL-Egress |] | | |
| Egress AG | CL 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:

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

| General Se | urity | QoS | Advanced | 1 | |
|---------------------------------------|-------------------|--------------|-------------------|----------------|---------|
| Allow AAA Ove Coverage Hole | rride Detectio | Enal | bled | | |
| Enable Session | n Timeout | ✓ 180 Ses | 0 sion Timeout | (secs) | |
| Aironet IE | | Enab | led | | |
| Diagnostic Cha | annel | Enab | led | | |
| Override Inter | face ACL | IPv4 N | one 💌 | IPve | None 💌 |
| P2P Blocking A | ction | Disable | ed | ~ | |
| Client Exclusio | n <u>3</u> | Enab | led 60 Timeou | t Value (secs) | |
| Maximum Allos Clients ² | ved | 0 |] | | |
| Static IP Tunne | ling 💶 | Enab | led | | |
| Wi-Fi Direct Cl Policy | ients | Disabl | ed 💌 | Flaw Logal C | |
| Maximum Allo Clients Per AP | ved Radio | 200 |] | should not be | enabled |
| FlexConnect | | | | / | |

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

| eneral Security | QoS Advanced | | | |
|-------------------------|------------------------|-------------|-----------------------|---------------|
| Allow AAA Override | Denna | | DUCT | |
| Allow ARA Overhoe | | | DHCP | — |
| Coverage Hole Detection | M Enabled | | DHCP Server | U Overnde |
| Enable Session Timeout | Session Timeout (secs) | | DHCP Addr. Assignment | Required |
| Aironet IE | Enabled | | Nanagement Frame Prot | ection (MEP) |
| Diagnostic Channel | Enabled | | | cease (energy |
| Override Interface ACL | IPv4 None V | IPv6 None 💌 | MFP Client Protection | Optional V |

3. Set AP Mode to FlexConnect.

All APs > Details for AP_3500E

| General | Credenti | als Inter | faces | High Availability |
|----------|------------|--------------------|---------|-------------------|
| eneral | | | | |
| AP Name | C. | AP_3500E | | |
| Location | | | | |
| AP MAC | Address | o4:7d:4f:3a | a:07:74 | |
| Base Rad | dio MAC | o4:7d:4f:53 | 3:24:e0 | |
| Admin St | atus | Enable 💌 |] | |
| AP Mode | | FlexConne | ct 💌 | |
| AP Sub N | 1ode | local FlexConne | et | - |
| Operatio | nal Status | monitor | | |
| Port Num | ber | Sniffer | ector | |
| Venue G | roup | SE-Connec | t l | ~ |

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.

| llı. cısco | Move | TOR W | LANS CONTROLLS | ER WIJRELESS | SECORITY | MANAGEMENT | COMMANDS | HELP | EEEOBACX |
|---|-------|------------|-----------------------------|------------------------------|----------|-------------|-----------|------|----------|
| Wireless | Acce | ess Con | trol Lists > Edit | | | | | | |
| Access Points All APs | Gene | iral | | | | | | | |
| # #40005 602.116/5 802.116/s/s | Acces | s List Nam | ie Flex- | ACL | | | | | |
| Global Configuration | Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | |
| Mesh | 1 | Permit | 9.6.61.0 / 255.255.255.0 | 9.1.0.150 255.255.255.255 | ICMP | Any | Any | Any | ۰ |
| RF Profiles FlexConnect Groups FlexConnect ACLs | | | | | | | | | |

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



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

| AP Name | AP_3500E | |
|-----------------|-------------------|--|
| Base Radio MAC | c4:7d:4f:53:24:e0 | |
| WLAN ACL Map | oing | Enter WLAN ID on which Split Tunnel should be enabled |
| WLAN Id | 1 | |
| Local-Split ACL | Flex-ACL | Click Add after |

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

| AP Na | me | AP_3500E | |
|--------|-------------|-------------------|-----------------|
| Base P | Radio MAC | o4:7d:4f:53:24:e0 | |
| WLAN | ACL Mapp | ping | |
| WLA | N Id | 0 | |
| Loca | I-Split ACL | Flex-ACL 💌 | |
| | | Add | |
| WLAN | | | |
| Id | WLAN P | rofile Name | Local-Split ACL |
| | | | |

- 7. 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 Radios | General Local Authentical | tion Image Upgrade | AAA YLAN-ACL mepping | WLAN-ACL mapping | WebPalicies |
| 002-11b/g/h 002-11b/g/h Global Configuration • Advanced | Web Auth ACL Mapping | | Local Split ACL Map | ping Enter WLA Tunnel sho | N ID on which Split uid be enabled |
| Mesh RF Profiles FlexConnect Groups | WebAuth ACL Flex-ACL | × | Local Spit ACL | Fitx-ACL | after selecting Flex |
| PlexConnect ACLs > 802.11a/n | WLAN Id WLAN Profile N | ame WebAuth ACI | WLAN Ed WLAN | reafile Name Loca | displit ACL |

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

| Wireless | FlexConnect Groups > Edit Flex-Group' |
|---|--|
| Access Points All APs Radies B02.11a/h | General Local Authentication Image Upgrade AAA VLAN-ACL mapping WLAN-ACL mapping WebPolicies |
| 802.11b/g/n Global Cenfiguration Advanced | Web Auth ACL Mapping Local Split ACL Mapping |
| Mesh RF Profiles | WLAN Id 0 WLAN Id 0 WLAN Id 0 WLAN Id 0 United Split ACL Play-ACL M |
| FlexConnect Groups FlexConnect ACLs 802.11e/n | Add |
| > 802.11b/g/n | 1 "Store 1" Flex-4CL 🛩 🖬 |

Limitations

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

Fault Tolerance

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

Fault Tolerance

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

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

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

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

Summary

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

Limitations

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

Client Limit per WLAN

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

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

Client Limit per WLAN

Primary Objective

- Set limits on maximum clients
- Operational ease

Note: This is not a form of QoS.

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

Limitations

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

WLC Configuration

Complete these steps:

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

| seneral Securi | y Qo5 Advanced | | • |
|---|---|---|---|
| Allow AAA Overrid Coverage Hole De Enable Session Tin Aironet IE Diagnostic Channe IPv6 Enable Z Override Interface P2P Blocking Actio Client Exclusion 2 | e Enabled section V Enabled section V Enabled V Enabled ACL None V Disabled V VEnabled C Timeout Value (secs) | DHCP DHCP Server Override DHCP Addr. Assignment Required Management Frame Protection (MFP) MFP Client Protection f Optional DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1 | Â |
| Clients 2 | 0 | NAC OOB State C sould | |
| ff Channel Scannin Scan Defer Priority | 0 1 2 3 4 5 6 7 | Posture State Enabled | |
| Scan Defer Time(msecs) | 100 | Client Load Balancing Client Band Select | ~ |
| | | a | > |
| 2 H-REAP Local Switch 3 When client exclusion 4 Client MFP is not act 5 Learn Client IP is co 5 WMM and open or A 5 WMM and open or A 1 Multicast Should Be 1 Band Select is confi | ing is not supported with IPsec, CRANITE auther n is enabled, a Timeout Value of zero means int ive unless WPA2 is configured infigurable only when HREAP Local Switching is e ES security should be enabled to support higher Enabled For IPH6. wrable only when Radio Policy is set to 'All'. | tication nity (will require administrative override to reset excluded clients) vabled 11n rates | |

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

Client Limit per WLAN

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 | ails : 17 5.154 > WiLANS > WiLAN Coofiguration > 1 | NI AN Configuration Details |
|-------------------------------------|---|-----------------------------|
| configure y controllery y Deleoide. | | |
| General Security QoS | Advanced | |
| | | |
| FlexConnect Local Switching | Enable | DUCD |
| FlexConnect Local Auth 🔍 | Enable | |
| Learn Client IP Address | Enable | DHCP Server |
| Session Timeout | Enable 1800 (secs) | DHCP Address Assignment |
| Coverage Hole Detection | 🗹 Enable | Management Eramo Protoct |
| Aironet IE | 🗹 Enable | Management Frame Protect |
| IPv6 <u>∠</u> | 🗖 Enable | treach the truth of |
| Diagnostic Channel 2 | 🗖 Enable | MFP Client Protection 2 |
| Override Interface ACL | IPv4 NONE | MFP Version |
| | IPv6 NONE | Load Balancing and Band Se |
| Peer to Peer Blocking 🔍 | Disable | |
| Wi-Fi Direct Clients Policy | Disabled 🗸 | Client Load Balancing |
| Client Exclusion 1 | 🗹 Enable | Client Band Select |
| Timeout Value | 60 (secs) | |
| Maximum Clients 🔍 | | NAC |

Configuration through Cisco Prime

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

Peer-to-Peer Blocking

| | | Home | Monit | tor | Configure | Ser | vices * | Reports * | Adminis | tration 💌 | | |
|------------------------------------|---|-----------------------------|-------|------|-----------|-------------------------|----------|-----------------|------------|-----------|------|---|
| Properties | × | General Security | Qo | s 🔳 | Advanced | Ho | tSpot | Policy Cor | figuration | | | |
| System | > | | | | | | Elector | tion | | | | |
| WLANs | ~ | Session Timeout | | able | | | FlexCo | onnect Local Sv | vitching | Enable | | |
| WLAN Configuration | | Aironet IF | e En | able | | | FlexCo | onnect Local Au | th 2 | Enable | | |
| AP Groups | | TPu6 2 | C En | able | | | Learn | Client IP Addre | \$5 | Enable | E. | |
| Policy Configuration | | Dissportic Channel (2) | O Fo | able | | | VLAN | Based Central S | witching | 🗇 Enable | 6 | |
| FlexConnect | > | Override Interface ACL | IPv4 | NONE | | • | Centra | I DHCP Proces | sing | 🗆 Enable | t i | |
| Security | > | -0 | IPv6 | NONE | | • | Overri | de DNS | | Enable | | |
| Access Points | > | Peer to Peer Blocking 2 | Disa | ble | • | | NAT-P | TA | | Enable | ÉS. | |
| 802.11 | > | Wi-Fi Direct Clients Policy | Disa | bled | • | | DHCP | Server | | Overrid | le | |
| 802.11a/n | > | Client Exclusion | 🗹 En | able | | | DHCP | Address Assign | ment | Requir | ed | |
| 802.11b/g/n | 5 | Timeout Value | 60 | (se | cs) | | Manag | ement Frame | Protection | (MFP) | 2047 | |
| Application Visibility And Control | > | Maximum Clients | 0 | | | | MED C | Next Destaction | 0 1 | Enabled | | - |
| Netflow | > | | | _ | | | MED V | Ment Protection | | Linebrow | | - |
| Mesh | > | Mobility Anchors | 0 | | | | Load B | alancing and B | and Selec | t | | |
| Ports | > | Passive Client | O Fo | able | | | | | | | | |
| Management | > | OF Channel Scanning Defer | - | | | | Client | Load Balancing | | Enable | | |
| Location | > | on ordering beier | | | | | NAC | Dent Select | 1 | | | |
| Router Advertisement | > | Scan Defer Priority | 01 | 2345 | 67 | | NAC S | tate | 1 | None | • | |
| Redundancy | 5 | Scan Defer Time | 100 |) (m | s) | | Voice | | | | | |
| | - | DTIM Period | | | | | Client F | Profiling | | | | |

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.



Peer-to-Peer Blocking

Summary

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

Procedure

Complete these steps:

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

| General Security | QoS Advanced | | |
|--|----------------------------------|--|------------|
| Aironet IE | Enabled | Management Frame Protec | tion (MFP) |
| Diagnostic Channel Override Interface AC P2P Blocking Action | L IPv4 None V | IPv6 None MFP Client Protection f | Optional |
| Client Exclusion 3 Maximum Allowed Clie Static IP Tunneling 44 | Enabled 60 Timeout Value (sec | s) 802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC | |
| Wi-Fi Direct Clients Po Off Channel Scanning C | licy Disabled M Defer | NAC State None Store None | elect |
| Scan Defer Priority | 0 1 2 3 4 5 6 7 | Client Load Balancing Client Band Select Z | |
| Scan Defer Time (msecs) FlexConnect | 100 | Passive Client Voice | |
| FlexConnect Local | Enabled | Media Session Snooping | Ecoled |

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

Limitations

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

AP Pre-Image Download

AP Pre-Image Download

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

Summary

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

Procedure

Complete these steps:

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

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

| Download file to Controller | | L |
|-----------------------------|------------------------|------|
| File Type Transfer Mode | Code v | |
| Server Details | | |
| IP Address | | |
| Maximum retries | 10 | |
| Timeout (seconds) | 6 | |
| File Path | | 5 |
| File Name | AS_5500_7_0_112_52.aes | 2000 |

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

| P 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 | |

```
903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Sep
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)!!!!!!
                                                                    350519
*Sep 13 21:25:43.747: Loading file /c1250-pre
                                                                  *
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds
New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.
```

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

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

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

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

Limitations

Works only with CAPWAP APs.

FlexConnect Smart AP Image Upgrade

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

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



Summary

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

Procedure

Complete these steps:

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

| Download file to Controller | | |
|-----------------------------|----------------------|--|
| File Type | Code | |
| Transfer Mode | TFTP 💌 | |
| Server Details | | |
| IP Address | | |
| Maximum retries | 10 | |
| Timeout (seconds) | 6 | |
| File Path | | |
| File Name | AS_5500_7_2_1_72.8es | |

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

| eneral | Local Authentication | Image Upgrade | VLAN-ACL mapping | | |
|------------------------------------|----------------------|--|-----------------------|------|---|
| Group N lexConi | ame Store 1 | | AAA | | |
| dd AP | | | Primary Radius Server | None | ~ |
| Select APs from current controller | | Secondary Radius Server Enable AP Local Authenticat | None | * | |

6. Check the FlexConnect AP Upgrade check box in order to achieve efficient AP image upgrade.

7. Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab.

| | Authentication | Image Upgrade | VLAN-ACL mapping |
|------------------|----------------|---------------|------------------|
| FlexConnect AP U | Jpgrade 🗌 | | |
| FlexConnect M | aster APs | | |
| AP Name | AP3500 | | |
| Add Master | | 10000 | |

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

| reneral | Local Authentica | tion Image Upgra | ade VLAN-ACL mapping | |
|---------------------|------------------|------------------------------|----------------------|--|
| FlexConnec | t AP Upgrade 🗹 | | | |
| Slave Maxi | mum Retry Count | 44 | | |
| Upgrade In | nage | Backup 😪 FlexConnect Upgrade | | |
| FlexConne | ct Master APs | | | |
| | | | | |
| AP Name Add Mast | AR3500 | M | | |
| AP Name Add Mast | AR3500 | Model | Manual | |

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

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

| Seneral Loc | al Authentica | tion Ima | e Upgrade | VLAN-ACL mapping | 0 |
|---------------------------------|--------------------------|----------|-----------|---------------------|---|
| FlexConnect AP Slave Maximum | Upgrade 🔽 Retry Count | 44 | | | |
| Upgrade Image | | Backup 💌 | | FlexConnect Upgrade | |
| AP Name | AP3500-1 | ~ | | | |
| Add Master | | | | | |
| Master AP Name | e | AP Model | | Manual | |
| | | c35001 | | 00 | 0 |

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

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

| eneral | Local Authenticat | tion Image (| Upgrade | VLAN-ACL mapping |
|------------------------|-------------------|--------------|---------|------------------|
| | | | | |
| FlexConne Slave Ma: | act AP Upgrade 🕑 | 44 | | |

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

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

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

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

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

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

Limitations

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

Auto Convert APs in FlexConnect Mode

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 Credent | ials Interfaces | High Availability |
|--------------------|----------------------|-------------------|
| ieneral | | |
| AP Name | AP3500 | |
| Location | default location | |
| AP MAC Address | 00:22:90:e3:37:df | |
| Base Radio MAC | 00:22:bd:d1:71:30 | |
| Admin Status | Disable 👻 | |
| AP Mode | local 👻 | |
| AP Sub Mode | local ElexConnect | |
| Operational Status | monitor | |
| Port Number | Sniffer | |
| Venue Group | Bridge SE-Connect | - |

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

Auto Convert Mode

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

(Cisco Controller) > config ap autoconvert ?

disable.....Disables auto conversion of unsupported mode APs to supported modes when AP joins

flexconnect......Converts unsupported mode APs to flexconnect mode when AP joins monitor.....Converts unsupported mode APs to monitor mode when AP joins

(Cisco Controller) >

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

(Cisco Controller) > show ap autoconvert

FlexConnect WGB/uWGB Support for Local Switching WLANs

AP Autoconvert Disabled

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

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

This option is currently available only via CLIs.

These CLIs are available only on the WLC 7500.

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

(Cisco Controller) >config ap autoconvert flexconnect

(Cisco Controller) > show ap autoconvert

AP Autoconvert FlexConnect

(Cisco Controller) >

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

(Cisco Controller >config ap autoconvert monitor

(Cisco Controller) > show ap autoconvert

AP Autoconvert Monitor

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

FlexConnect WGB/uWGB Support for Local Switching WLANs

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

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

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

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

FlexConnect WGB/uWGB Support for Local Switching WLANs



Summary

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

Procedure

Complete these steps:

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

| General | Security | QoS | Advanced | |
|---|---|--|---|--------------------------------|
| Allow A4 Coverage Enable S Aironet Diagnos Override P2P Bloc Client E: Maximu Clients S Static IP Wi-Fi Dir Policy Maximu Clients F Clear Hu | AA Override ge Hole Detectio Session Timeout IE tic Channel e Interface ACL cking Action xclusion ² m Allowed trunneling ²¹ rect Clients m Allowed Per AP Radio otSpot | □ Enai □ Enai □ 180 Ses □ Enab □ Enab □ Disabl □ Enab □ Disabl □ Disabl □ Disabl □ Disabl | bled bled o ssion Timeout (secs bled lone ed filed filed bled ed v bled | s) IPv6 None s ue (secs) |

FlexConnect WGB/uWGB Support for Local Switching WLANs

2. Set AP Mode to FlexConnect.

| General | Credentials | Interfaces | High Availability |
|-----------|-------------|---------------------------|-------------------|
| General | | | |
| AP Name | | AP_3500E | |
| Location | [| | |
| AP MAC | Address | o4:7d:4f:3a:07:74 | |
| Base Rad | io MAC | o4:7d:4f:53:24:e0 | |
| Admin St | atus | Enable 💌 | |
| AP Mode | | FlexConnect 🔽 | |
| AP Sub M | ode | local | |
| Operation | al Status | monitor | |
| Port Num | ber | Rogue Detector Sniffer | |
| Venue Gr | quo | Bridge SE-Connect | ~ |

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

| MONITOR WLA | NS CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | | | | |
|-------------------|---------------|---------------|----------------|------------|-----------|------|----------|------------|------|------|-----|
| Clients | | | | | | | | | | | |
| Current Filter | None | Change Filter | [Clear Filter] | | | | | | | | |
| Client MAC Addr | AP Name | | WLAN | Profile | WLAN SSID | | Protocol | Status | Auth | Fort | WGB |
| 00:40:96-58:d4:5 | AP_3500E | | "Store | 1 | "Store 1" | | N/A | Associated | Yes | 1 | No |
| 00:50:b6:09:e5:3 | AP_3500E | | 'Store | e 1' | "Store 1" | | N/A | Associated | Yes | 1 | No |
| 04:7d:4f:3a:68:10 | AP 3500E | | "Store | e 1° | "Store 1" | | 802.11an | Associated | Yes | 1 | Yes |

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

Clients > Detail

FlexConnect WGB/uWGB Support for Local Switching WLANs

| Clients > Detail | | | |
|--------------------|-------------------|-----------------------|-------------------|
| Client Properties | | AP Properties | |
| MAC Address | o4:7d:4f:3a:08:10 | AP Address | o4:7d:4f:53:24:e0 |
| IPv4 Address | 9.6.63.102 | AP Name | AP_3500E |
| IPv6 Address | | AP Type | 802.11an |
| | | WLAN Profile | 'Store 1' |
| | | Data Switching | Local |
| | | Authentication | Central |
| | | Status | Associated |
| | | Association ID | 1 |
| | | 802.11 Authentication | Open System |
| | | Reason Code | 1 |
| | | Status Code | 0 |
| Client Type | WG8 | CF Pollable | Not Implemented |
| Number of Wired Cl | ient(s) 2 | CF Poll Request | Not Implemented |

5. 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 Authentication | Open System |
| | | Reason Code | 1 |
| | | Status Code | 0 |
| Client Type | WGB Client | CF Pollable | Not Implemented |
| WGB MAC Address | o4:7d:4f:3a:08:10 | CF Poll Request | Not Implemented |

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

Support for an Increased Number of Radius Servers

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

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

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

Summary

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

Procedure

1. Mode of configuration prior to release 7.4.

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

| cisco | MONITOR MLANS | CONTROLLE | wyneless yn | URITY MAN | AGEMENT COMMAN | | | Sea Configuration (Bris) Legisl |
|---|---|--------------|---|------------------|------------------------|--------------|---|-----------------------------------|
| Becurity | RADIUS Authenti | cation Serv | ers | | | | | Apply New- |
| • AAA General • 842035 ActiveChalten Accounting Fallback | Call Station 30 Type Use AES Ray Waap MAC Delimiter | I Deipe | HAC Address II d for FIPS customers at | d requires a key | y why compliant RAD1.4 | i amver) | | |
| + TALACS+ LDAP | Natwork Managers | Sarear Index | Sareer Address | Part | 1Pfeet | Admin Status | | |
| Local Net Lisars MAC Educine | M M | 1 | 1234 | 1812 | Disabled | Enabled | | |
| Disabled Gierts | M M | 2 | 1.2.3.4 | 2 | District | Enabled | 0 | |
| Giver Legie Policies | M M | 3 | 1234 | 3 | Disabled | Enabled | | |
| AP Peterse Respond Policies | 66 M | 1 | 1.2.3.4 | | Disabled | Enabled | | |
| Toront Page | M M | 5 | 1.2.3.4 | 8 | Disabled | Enabled | | |
| LOCALEAP | H H | 6 | 1.2.3.4 | 6 | Disabled | Evabled | | |
| Priority Order | H H | 1 | 1.2.3.4 | 7 | Disabled | Enabled | | |
| Certificate | H H | | 1.2.3.4 | | Disabled | Enabled | | |
| Access Centrel Lists | 8 8 | | 1.2.3.4 | | Disabled | Enabled | | |
| Wireless Protection | 12 H | 22 | 1.2.3.4 | 10 | Disabled | Enabled | | |
| Pulicies | 8 H | 22 | 1.2.3.4 | 11 | Disabled | Enabled | | |
| Web Auth | 8 8 | | 5.2.3.4 | 12 | Disabled | Enabled | • | |
| Trustfor SXP | 8 8 | 13 | 1.2.3.4 | 13 | Disabled | Enabled | | |
| Trustsec SUP | 8 6 | 38 | 1.2.3.4 | 14 | Disabled | Enabled | | |
| | 8 8 | .13 | 1.2.3.4 | 15 | Disabled | Enabled | | |
| | 8 8 | | 1.2.3.4 | 36 | Disabled | Enabled | | |
| | H H | 11 | 1.2.3.4 | 17 | Disabled | Enabled | | |

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

Enhanced Local Mode (ELM)

| Wireless | FlasConnect Groups > Edit 'abc' | | e Back Apply |
|---|---|--|--------------|
| Al Ahy • Balliss 822,114/s 922,113/g/n Distal Configuration | General Local Authentication Druger Upgrade AAA VLAN-ACL of | napping WLAN-ACL mapping WebPolicies Central SmC7 | |
| Anan Maah SF Proclamat Groups Parclamat Acta 9 802.11a/n 9 802.11a/n 9 802.11a/n 9 802.11a/n 9 802.11b/a/n 9 802.1 | AP NAC Adress AP Nove Blaks | Image National Source [25] 3.2.4.5mc/17 [3] water Affects Source [25] 3.2.4.5mc/17 [3] water Affects Source [25] 3.2.4.5mc/17 [3] water Affects Source [25] 3.2.4.5mc/17 [3] [26] 3.2.5.5.6mc/2 [26] 3.2.5.6mc/2 [26] 3.2.5.6mc/2 [26] 1.2.3.5.6mc/2 [26] 3.2.5.6mc/2 [26] 3.2.5.6mc/2 [26] 1.2.3.5.6mc/2 [26] 3.2.5.6mc/2 [26] 3.2.5.6mc/2 [26] 1.2.5.6.7mc/2 [26] 3.2.5.7.6mc/2 [26] 3.2.6.7.6mc/2 [26] 1.2.5.7.6mc/2 [26] 3.2.6.7.6mc/2 [26] 3.2.6.7.6mc/2 | |

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

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

| cisco | BONITOR MLANS CONTROLLER WIRELESS SECURITY HANAGE | IMENT COMMANDS HELP FRED | **** | Sage Collipsetter Brig Linguit Ball |
|---|--|--|--|-------------------------------------|
| Winsiess * Access Points Al Afty * Raise 002.11a/1 Cod Red Raise | FlexConnect Groups > Edit 'abc' General Catal Authentication Triage Upgrade ACL Has Group Rame exc | ping Castral CHCP | • | chox Any |
| Einhel Configuration Advanced Neah RF Profiles PlexConnect Groups PrecConnect Gr | FrexCannect APs AP NAC Address AP Name Status | AAA Server IP Address Berver Type Uhered Berver Carling Shared Servet Part Number Batt | 1.2.3.4 Secondary (2) Teams 4 | |
| Application Visibility And Control Country Timers NetSlove QuS | - | Barver Type Address Anary £23.4 UnConfigured Unconfigured | Part 3 D 8 D | |

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

Guest Access Support in Flex 7500

Figure 12 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.

Managing WLC 7500 with Cisco Prime

| onfigure > <u>Controllers</u> > A | dd Controllers | |
|---|-------------------------------------|-----------|
| eneral Parameters | | |
| Add Format Type | Device Info | ~ |
| IP Addresses | WLC 7500 I | P Address |
| Network Mask | 255.255.255.0 | |
| NMP Parameters 🏵 | | |
| Version | v2c | ~ |
| Retries | 2 | |
| Timeout | 10 | (secs) |
| | | |
| Community | private | |
| Community eInet/SSH Paramete | private | |
| Community elnet/SSH Paramete User Name | private | |
| Community eInet/SSH Paramete User Name Password | private ITS ④ admin ++++++ | |
| Community eInet/SSH Paramete User Name Password Confirm Password | private ITS admin | |
| Community eInet/SSH Paramete User Name Password Confirm Password Retries | private | |

| Cont | ntrollers ig.rs > Controllers | | | | | Select a | command | |
|------|----------------------------------|-----------------|------|----------|------------------|---------------------|---------------------|--------------|
| | | | | | | | | Entries 1 |
| | P.Address | Controller Name | Tape | Location | Software Version | Mobility Group Name | Reachability Status | Audit Status |
| | 172.20.227.174 | Ambassador | 7500 | | 7.0.112.62 | mobility | Reachable | Identical |
| | 172.20.227.172 | 5508-Primary | 5500 | | 7.0.112.52 | mobility | Reachable | Identical |

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

Managing WLC 7500 with Cisco Prime

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

| | | (a) nome monitor V configure V Services V Reports V Administration V |
|---|----------------------|--|
| Add Controllers Configure > Controlers > A | Add Controllers | |
| Seneral Parameters | | |
| Add Format Type | Device Info | • |
| IP Addresses | WIC 7500 IP Address | (comma-separated IP Addresses) |
| 🗆 Wism Auto Add 🕖 🖣 | Wite 7500 IF Address | |
| Childe Descenters (1) | | |
| Version | (v2c | |
| Detailer | | |
| Retries | 2 | |
| SNMP Timeout | 10 | (secs) |
| Community | | |
| Telnet/SSH Parameters | Ð | |
| Protocol | Telnet | • |
| Username | admin | |
| Password | | |
| Confirm Password | | |
| Telnet Timeout | 60 | (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.shtml)

Figure 13 Document 100590

| Document ID: 100590 | |
|--|--|
| Contents Introduction Prerequisites Requirements Components Used Conventions Background Information Configure ADD EAST as Local EAD Authentication Method on the WLC Onfigure ADD EAST as Local EAD Authentication Method on the WLC Downloading the Device Certificate for the VHLC Install the Root Certificate of PKI into the WLC Generate a Device Certificate of the Client Configure LOCAL EAPT on the VNLC Configure LOCAL EAPT on th | |
| Configure Wireless Client Verify Troubleshoot Cisco Support Community - Featured Conversations Related Information | |

Configuration of EAP-TLS on FlexConnect AP

1. Create WLAN for Local Switching and Local Authentication.

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

Figure 14 WLAN Configuration for PEAP and EAP-TLS

| uluilu cisco | | VLANS (| CONTROLLER WIRELESS | S SECURITY MANAGEMENT | COMMANDS HELP | FEEDBACK | |
|-----------------|-------------------------|------------------------------|---|--|---|---|--|
| WLANS WLANS | WLANs Current Filter | , None | (Charge Filter) (| Quar Filter] | | Create New 🕄 Ga | |
| Advanced | UNLAN 10 | Type WLAN WLAN WLAN | Profile Name oniev ciscowic-peap ciscowic-eaptis | WLAN SSID eniox ciscowic-peap ciscowic-eaptis | Admin Status Enabled Enabled Enabled | Security Policies (WPA21(Auth/802.1X)) (WPA2](Auth/802.1X)] (WPA2](Auth/802.1X)] | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

2. Enable FlexConnect Local Switching and FlexConnect Local Auth.



| cisco | MONITOR WLANS CONTRO | ALLER WIRELESS SEA | DURITY MANAGEMENT | COMMANDS HELP FEEDBACK | |
|----------------|---|--------------------|-------------------|--------------------------------|-------------|
| LANs | WLANs > Edit 'ciscowic | -peap' | | | |
| WLANS WLANS | General Security C Scan Defer Priority | Policy-Mapping | Advanced | Martin Canadan Connelan | Enabled |
| Advanced | | | | Be anther Reamed Voice Clients | Enabled |
| | Scan Defer Time(msecs) | 100 | | KTS based CAC Policy | Enabled |
| | FlexConnect | | | Radius Client Profiling | |
| | FlexConnect Local | Enabled | | DHCP Profiling | 0 |
| | Enderson Land Land H | Enabled | | HTTP Profiling | D |
| | Prexconnect cocal Auton | E Coubled | | Local Client Profiling | |
| | Learn Client IP Address * | E Eneoleo | | DHCP Profiling | 0 |
| | Switching 12 | C Enabled | | HTTP Profiling | 0 |
| | Central DHCP Processing | Enabled | | PHIP | |
| | Override DNS | Enabled | | PHIP Mobility Type | None 1 |
| | NAT-PAT | Enabled | | PMIP Profile | (Burne 14) |
| | | | | | |
| | | | | mDNS | |
| | | | | mDNS Secondar | C Enabled |

3. Enable AP Local Authentication.

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

Figure 16 FlexConnect Group Configuration for AP Local Authentication

| Wireless | FlexConnect Gro | ups > Edit 'abc | 1 | | | | | | | Appl |
|--|---|--|--------------|----------------|-----------|---|---|----------------|---|------|
| Access Points Al APs Radios 802.11a/n/ac 902.11b/g/n Dual Band Radios | General Local Group Name Enable AF Local As | Authentication abc thertication ² | Image Upgrad | e 🛛 ACL Mappin | ng Centro | I DHCP W | LAN VLAN map | ping | | |
| Advanced | FlexConnect AP | | | | | AAA | | | | |
| Hesh RF Profiles FlexConnect Groups | Add AP | AP Name | | tatus | | Server IP Add Server Type | ress | Primary 4 | 9 | |
| 802.11a/n/ac 802.11b/g/n Media Stream Application Visibility | ACTIVE AT DULTETH | W, 344 | | | J | Confirm Share Port Number | od Secret | 1812 | | |
| And Control Country Timers Netflow | | | | | - | Server Type UnConfigured UnConfigured | Address Unconfigured Unconfigured | Pert 0 0 | 8 | |

- 4. Selecting EAP methods will now have two more options, PEAP and EAP-TLS under the FlexConnect Group with the existing LEAP and EAP-FAST options.
 - a. Current controller release supports downloading of EAP device and root (CA) certificates to the controller and the same is stored in PEM format on the flash.

Figure 17 Downloading Vendor Device Certificate

| Commands | Download file to C | ontroller | | | | | |
|---|--|-----------|-----------------------|----------------------------------|-------------|---|--|
| Download File Upload File Reboot Config Boot | File Type Certificate Password Transfer Mode Server Details | | • | Vendor Device (••• IFTP : | Certificate | 1 | |
| Reset to Factory Default Set Time Login Banner | IP Address Maximum retries Timeout (seconds) File Path File Name | | 10 6 / cisco | wicdev.pem | | | |

Figure 18 Downloading Vendor CA Certificate

| Commands | Download file to Controller | * |
|---|---|-----------------------|
| Download File Upload File Reboot Config Boot | File Type Transfer Mode Server Details | Vendor CA Certificate |
| Scheduled Reboot Reset to Factory Default Set Time | IP Address Maximum retries Timeout (seconds) File Path | 10 6 / |
| Login Banner | File Name | 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.

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

| | ication In | nage Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping |
|---|--------------------------------|------------------|----------------------|--------------|-------------------|
| ocal Users Protocol | s | | | | |
| Enable EAP Fast Authentication ² Server Key (in hex) | Enable Aut | o key generation | | 1 | |
| | ••••• | | (Confirm server key) | | |
| Authority ID (in hex) | 436973636f00000000000000000000 | | | | |
| Authority Info | Cisco A_ID | | | | |
| PAC Timeout (2 to 4095 days) | | | | | |
| EAP | | | | | |
| Enable PEAP Authentication ² | M | | | | |
| AP TLS | | | | | |

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

| 2 3 | - rwx drwx | 65056 64 | Feb Feb | 28 281 | 15:48:41 | +00:00 | event.log configs |
|--------|---------------|-------------|------------|---------|----------|--------|----------------------|
| | -rwx | 1513 | Feb | 28 2013 | 18:37:11 | +00:00 | eapdev.pem.ca |
| 4 | -rwx | 1704 | Feb | 28 2013 | 18:37:11 | +00:00 | eapdev.pem.crt |
| 6 | -rwx | 963 | Feb | 28 2013 | 18:37:11 | +00:00 | eapdev.pem.prv |
| | -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.

Figure 21 Wireless Profile for EAP-TLS



Figure 22 Validate Server Identity

| onfigure EAP-TLS | ? 🛛 |
|---|-----------|
| Use Machine Information for Domain Logon | |
| ✓ Validate Server Identity Trusted Root Certification Authorities | |
| sskcert | ~ |
| Select a Certificate | |
| Administrator [Issued by: sskcert 11/22/2012] | × |
| Server/Domain Name |] |
| and in the second se | |
| Always Do User Authentication | OK Cancel |

Once the client is connected, Server Based Authentication will reflect EAP-TLS.
Figure 23 Client Authentication using EAP-TLS

| and Chabas | | (maximum) | |
|-------------|-----------------------------------|-----------------|------------------------------|
| tent Status | rotile Management | Diagnostics | |
| ISCO SYSTEM | S | | |
| ահ. ահ. | | | |
| | Profile Name: | ciscowic-eaplis | |
| | Link Status: | Authenticated | Network Type: Infrastructure |
| | Marian Made | E GUa Ed Mhoa | Convert Channel 49 |
| | witeless mode. | 5 GHz 54 Mbps | Current Charmet 46 |
| Server Ba | sed Authentication. | EAP-TLS | Data Encryption: AES |
| _ | IP Address | 9556102 | |
| | | | |
| | Signal Strength: | | Excelent |
| | | | |

Client Certificates

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

Figure 24 Certificates on Client



Figure 25 Trusted Root (CA) Certificate on Client

| Issued To | Issued By | Expiratio | Friendly Name | ^ |
|---------------------------|----------------------|-----------|-------------------|-----|
| SecureSign RootCA1 | SecureSign RootCA1 | 9/15/2020 | Japan Certificati | 1 |
| SecureSign RootCA2 | SecureSign RootCA2 | 9/15/2020 | Japan Certificati | |
| SecureSign RootCA3 | 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 |
| Esskcert | sskcert | 4/5/2017 | <none></none> | |
| Swisskey Root CA | Swisskey Root CA | 1/1/2016 | Swisskey Root CA | ١. |
| TC TrustCenter Cla | TC TrustCenter Class | 1/1/2011 | TC TrustCenter | ~ |
| Export | Remove | | Advanc | ed. |
| | | | Lindian | |
| tificate intended purpose | 15 | | | |

Figure 26 Trusted Client Certificate

| ertificates | | | | | ? |
|-------------------|---------------------|-------------------------|-------------------|-------------------------|---------|
| intended purpose | . < | All> | | | ~ |
| Personal Othe | r People | Intermediate Certifica | ation Authorities | Trusted Root Certificat | ior < > |
| Issued To | | Issued By | Expirati | Friendly Name | |
| 🔤 Administra | kor | sskcert | 11/22/2 |)13 <none></none> | |
| Import | Export ided purp | Remove |] | Adva | nced |
| | | | | | |
| Encrypting File S | 5ystem, S | ecure Email, Client Aut | hentication | Viev | ~ |

Show Commands

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

Figure 27 EAP Type for Client Authenticated using EAP-TLS

| IPv6 ACL Name | none |
|--|------------------|
| IPv6 ACL Applied Status | Unavailable |
| Layer2 ACL Name | none |
| Layer2 ACL Applied Status. Tr | Unavailable |
| Client Type | SimpleIP |
| 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 |
| EAP Type | EAP-TLS |
| r texconnect, baca, switching and a second second second | LUCAL |
| FlexConnect Dhcp Status | Local |
| FlexConnect Vlan Based Central Switching | No |
| FlexConnect Authentication | Local |
| Quarantine VLAN | Θ |
| Access VLAN. | 56 |

EAP-PEAP

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

User Creation

Figure 28 User Addition for Local Authentication

| Local Add | ientication | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping | | |
|------------------|-------------|---------------|-------------|-----------------|-------------------|-----|--------|
| ocal Users Prote | ocols | | | | | | |
| No of Users | 1 | | | Add User | | | |
| ser Name | | | | Upload CSV file | | | |
| | | | | File Name | | | Browse |
| | | | | UserName | | | |
| | | | | Password | | | |
| | | | | Confirm Passwor | 4 | Add | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Remove All User | | | | | | | |

Client Configuration

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

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

| WPA/WPA2/CCKM | WPA/WPA2/CCKM EAP Type: | PEAP (EAP-MSCHAP V2) | ~ |
|-----------------------------|-------------------------------|------------------------|---|
|) WPA/WPA2 Passphrase | | | |
|) 802.1x | 802.1x EAP Type: | PEAP (EAP MSCHAP V2) | ~ |
| Pre-Shared Key (Static WEP) | | | |
|) None | | | |
| Continue | Allow Association to Maxed Co | sta | |
| Congre | Profile Locked | Constant In the second | |
| | Limit Time for Finding Doman | Controller To: 0 and | |
| Group Policy Delay: | 60 🔹 sec | | |
| | | | |

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

Figure 30 User Name and Password for PEAP

| | ion for Domain Logon |
|---|---|
| Validate Server Identit | у |
| rusted Floot Certification | Authorities |
| (Any> | × |
| When connecting, use: | |
| Certificate | |
| User Name and Pass | sword |
| Use Windows User N User Information for PE | Name and Password EAP (EAP-MSCHAP V2) Authentication |
| User N | ame: |
| | word |
| Pass | |

Figure 31 Cisco Aironet Desktop Utility Profile Management

| Options Help | | |
|---|-----------------|--------------|
| nt Status Profile Manager | Diagnostics | |
| aitel | | New |
| blizzard | | Modify |
| eniov | | Remove |
| ciscowic-eaptis | | Activate |
|)etals | | |
| Network Type: | Infrastructure | Import |
| Security Mode: Network Name 1 (SSID1): | Disabled | Export |
| Network Name 2 (SSID2): | <empty></empty> | Scan |
| Network Name 3 (SSID3): | <empty></empty> | Joan |
| Auto Calcul Durlles | | Order ProBet |

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

Figure 32 Client Authentication using PEAP(EAP-MSCHAPv2)

| rent Status | Profile Management | Diagnostice | |
|-------------|----------------------|----------------------|------------------------------|
| | M S Profile Name: | ciscowlc-peap | |
| | Link Status: | Authenticated | Network Type: Infrastructure |
| | Wireless Mode: | 5 GHz 54 Mbps | Current Channel: 48 |
| Server B | ased Authentication: | PEAP (EAP-MSCHAP V2) | Data Encryption: AES |
| _ | IP Address: | 9.5.56.102 | |
| | Signal Strength: | | Excellent |

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

Figure 33 Web GUI Client Details

| cisco | | MLANS (| CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|--|---|---|----------------------------|----------|------------|----------|------|----------|
| Monitor Summary Access Points Cisco CleanAir | Clients > D | etail AVC St | atistics | | | | | | |
| Statistics | Security I | nformati | ion | | | | | | |
| CDP Rogues Redundancy Clients Sleeping Clients Multicast Applications | Security P Completed Policy Type Auth Key I Encryption EAP Type SNMP NAC Radius NA CTS Secur AAA Overr AAA Overr AAA Overr AAA Overr | olicy 5 6 Mgmt 1 Cipher 2 State C State 1ty Group T ride ACL Na atus 1tide Flex AC atus 1tide Flex AC | Yes RSN (WP CCKM CCMP (A) PEAP Access RUN fag Not Appl ime none Unavailai CL none CL Unavailai | A2) ES) cable ble | | | | | |

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

| IFv6 ACL Applied Status. Layer2 ACL Name. Layer2 ACL Applied Status. Client Type. mDNS Status. mDNS Profile Name. No. of mDNS Services Advertised. Policy Type. Authentication Key Management. Encryption Cipher. Protected Management Frame. | Unavailable none Unavailable SimpleIP Disabled none 8 WFA2 882.1x CCMP (AES) No |
|---|---|
| EAP Type | PEAP |
| FlexConnect Data Switching. FlexConnect Dhcp Status. FlexConnect Vlan Based Central Switching FlexConnect Authentication Quarantine VLAN. Access VLAN. | Local No Local 0 9 9 56 99 |

CLI Support for PEAP and EAP-TLS on FlexConnect APs

| Two new CLIs have been added to configure PEAP | and EAP-T | LS from the controller. | | | | | |
|--|------------|-----------------------------------|--|--|--|--|--|
| config flexconnect group <groupname> radius ap</groupname> | реар | <enable disable="" =""></enable> | | | | | |
| config flexconnect group <groupname> radius ap</groupname> | eap-tls | <enable disable="" =""></enable> | | | | | |
| A CLI for certificate download has been added as well. | | | | | | | |
| config flexconnect group <groupname> radius ap</groupname> | eap-cert c | lownload | | | | | |



Configurations at the AP can be seen from the console.

Figure 35 CLI Commands on AP Console

| P 3600#show running-config brief s eap |
|---|
| aa local authentication reap_eap_methods authorization reap_eap_methods |
| aa authentication dotlx reap_eap_methods group radius local |
| aa authorization network reap_eap_methods local |
| waa authorization credential-download reap_eap_methods local |
| otii silu ciscowic-eaplis o |
| otl1 ssid ciscowlc-peap 4 |
| ap profile lwapp eap profile |
| method lis |
| method peap |

The following commands can be used to troubleshoot this feature:

debug eap all

debug aaa authentication

debug dot11 aaa authenticator all

debug aaa api

debug aaa 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

Figure 37 WLAN for Local Switching

| WLANS WLANS | WLANs Current Filter | n None | (Change Filter) (C | lear Filter) | | Create New Go | |
|----------------|-------------------------|--------|--------------------|-----------------|--------------|----------------------|--|
| Advanced | WLAN ID | Туре | Profile Name | WLAN SSID | Admin Status | Security Policies | |
| | 01 | WLAN | enjoy | enjoy | Enabled | [WPA2][Auth(802.1X)] | |
| | 01 | WLAN | ciscowic-peap | ciscowic-peap | Enabled | [WPA2][Auth(802.1X)] | |
| | 0 5 | WLAN | ciscowic-eaptis | ciscowic-eaptis | Enabled | [WPA2][Auth(802.1X)] | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

00

Figure 38 FlexConnect Local Switching

| eneral Security | QoS Policy-Mapping | Advanced | PASSING CITER | | |
|---------------------------|--------------------|----------|--------------------------------|---------|--|
| 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 | |
| lexConnect | | | KTS based CAC Policy | Enabled | |
| FlexConnect Local | Enabled | | Radius Client Profiling | | |
| Switching 4 | | | DHCP Profiling | 0 | |
| FlexConnect Local Auth | Enabled | | HTTP Profiling | | |
| Learn Client IP Address | Enabled | | Local Client Profiling | | |
| Vian based Central | Enabled | | DHCP Profiling | | |
| Switching ** | C Faibled | | HTTP Profiling | | |
| Central DHCP Processing | | | PMIP | | |
| Overnde DNS | Enabled | | PMIP Mobility Type | None | |

The WLAN is mapped to the management VLAN 56.

Figure 39 WLAN Mapped to VLAN 56 Management Interface

| eneral | Security | QoS | Policy-Mapping | Advanced | |
|------------------------|--------------|--------------------|--|--------------------|------------------------------|
| Profile Na | ime | enjoy | | | |
| Туре | | WLAN | | | |
| SSID | | enjoy | | | |
| Status | | 🗹 Enab | led | | |
| Security I | Policies | [WPA2 (Modifica |][Auth(802.1X)] tions done under securi | ty tab will appear | after applying the changes.) |
| Radio Pol | icy | All | \$ | | |
| Interface, Group(G) | /Interface | manag | ement 💼 | | |
| Multicast | Vlan Feature | Enabl | ed | | |
| Broadcas | SSID | 🗹 Enabl | ed | | |
| | | Anarailt | a Primary 5500 | | |

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

| P Name | AP_3600 | | | |
|---|-------------------|------------------------|---------------------|--|
| ase Radio MAC | 34:a8:4e:e7:5b:c0 | | | |
| AN VLAN Map | ping | | | |
| Make AP Specif | ic 🗧 Go | | | |
| Make AP Specif WLAN Id SSID | ic 🗘 Go | VLAN ID | NAT-PAT | Inheritance |
| Make AP Specif WLAN Id SSID 1 enjoy | ic 🗘 Go | VLAN ID 56 | NAT-PAT | Inheritance Wlan-specifi |
| Make AP Specif WLAN Id SSID 1 enjoy 4 ciscowi | -peap | VLAN ID 56 56 | NAT-PAT no no | Inheritance Wlan-specifi Wlan-specifi |

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

Figure 41 Client in VLAN 56

| rrent Status Profile Management | Diagnostics | |
|--|---------------|------------------------------|
| IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII | enijoy | |
| 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 |
| | | |

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

| 1 | FlexConne | ct Groups > Edit 'abo | 5' | | | | |
|---|-------------------------------|-----------------------|---------------|-------------|--------------|-------------------|--|
| | General | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping | |
| | WLAN VL WLAN Id Vian Id | AN Mapping | | | | | |
| | WLAN Id | WLAN Profile Name | Vian 57 | 1. | | | |
| | <u> </u> | cijey | 57 | | | | |
| | | | | | | | |
| | | | | | | | |

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

Figure 43 VLAN Mappings at AP

| eneral Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced |
|--|------------|-------------------|-----------|-------------|----------|
| VLAN Support Native VLAN ID | 56 | VLAN Mappings | | | |
| FlexConnect Group Name | abc | | | | |
| | | | | | |
| Authentication Access Cont | rol Lists | | | | |
| eAuthentication Access Cont | rol Lists | | | | |
| Authentication Access Cont External WebAuthentication ACLs Local Split ACLs | rol Lists | | | | |
| eAuthentication Access Cont External WebAuthentication ACLs Local Split ACLs Central DHCP Processing | rol Lists | | | | |
| eAuthentication Access Cont External WebAuthentication ACLs Local Split ACLs Central DHCP Processing | rol Lists | | | | |
| eAuthentication Access Cont External WebAuthentication ACLs Local Split ACLs Central DHCP Processing FiceExtend AP Enable OfficeExtend AP | trol Lists | | | | |

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 | | | |
| | | | | |
| Make AP Specifi WLAN Id SSID | c 🔹 Go | VLAN ID | NAT-PAT | Inheritance |
| Make AP Specifi WLAN Id SSID | c 🔹 Go | VLAN ID 57 | NAT-PAT | Inheritance Group-speci |
| Make AP Specifi WLAN Id SSID 1 enjoy 4 ciscowlo | c 🔹 Go | VLAN ID 57 56 | NAT-PAT no no | Inheritance Group-speci Wlan-specifi |

The client is assigned an IP address in VLAN 57.

Figure 45 Client in VLAN 57

| 🗑 Cisco Aironet Desktop Utili | ty - Current Profile: enjoy | ? |
|-----------------------------------|-----------------------------|------------------------------|
| Action Options Help | | |
| Current Status Profile Management | Diagnostics | |
| CISCO SYSTEMS | | |
| ntilitrantilitra Profile Name | : enjoy | |
| Link Status | : Authenticated | Network Type: Infrastructure |
| Wireless Mode | 5 GHz 54 Mbps | Current Channel: 108 |
| Server Based Authentication | LEAP | Data Encryption: AES |
| IP Address | 9.5.57.100 | |
| Signal Strength | | Excellent |
| | | Advanced |
| | | Adranced |
| | | Advanced |

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

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

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

| AP Name | | AP_3600 | | | |
|---------------------------|---|-------------------|------------------------|---------------------|--|
| Base Radi | io MAC | 34:a8:4e:e7:5b:c0 | | | |
| | | | | | |
| WLAN Id | AP Specific | Go | VLAN | NAT-PAT | Inheritance |
| Make / WLAN Id 1 | AP Specific SSID enjoy | Go | VLAN ID | NAT-PAT | Inheritance AP-specific |
| Make / Id 1 | AP Specific SSID enjoy ciscowlc- | ·peap | VLAN ID 58 56 | NAT-PAT no no | Inheritance AP-specific Wlan-specifi |

The client is assigned an IP address in VLAN 58.

Figure 47 Client in VLAN 58

| ent Status | Profile Management Diagnostics | |
|------------|--------------------------------|------------------------------|
| CO SYSTEM | 5 | |
| lluumillu | Profile Name: enjoy | |
| | Link Status: Authenticated | Network Type: Infrastructure |
| | Wireless Mode: 5 GHz 54 Mbps | Current Channet: 108 |
| Server Ba | sed Authentication: LEAP | Data Encryption: AES |
| | IP Address: 9.5.58.100 | |
| | Signal Strength: | Excellent |
| | Signal Strength: | Excellent |

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

Figure 49 show flexconnect group detail Output

| (Cisco Control | ler) >show flexcor | nnect group | detail abc | | |
|--|------------------------------------|---|----------------------------|--------------|------------------------|
| Number of AP's | in Group: 1 | | | | |
| fc:99:47:60:f9 | 9f AP_3600 | Joined | | | |
| Efficient AP I | mage Upgrade | Disabled | | | |
| Master-AP-Mac | Master-AP-Name | | Polis Navel - Mor | del Manual | |
| Group Radius S | ervers Settings: | | | | Ndisini Type Intachian |
| Туре | Server Address | Port | | | Current Channel 112 |
| Primary Secondary | Unconfigured Unconfigured | Unconfigu Unconfigu | ired ired modern LEAP | | O Min Encoppion: AEG |
| Anna Alternation | P CONTRACTOR | | | | |
| LEAP Auth EAP-TLS Auth EAP-TLS CERT D PEAP Auth | ownload. En | abled abled abled abled | | | Attiving |
| More or (q Server Key Aut Server Key Authority ID. Authority Info PAC Timeout Multicast on O Number of User |) uit o Generated No 43: | <hidden> 6973636f006 sco A_ID ce config:</hidden> | 00000000000000 Disabled | 960000 | |
| Group-Specific | FlexConnect Wlan | -Vlan Mappi | ng: | | |
| WLAN ID VI | an ID | | | | |
| 1 57 | | | | | |
| WLAN ID SSID | | | Central-Dhcp | Dns-Override | Nat-Pat |

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

Figure 50 show ap config general Output

| FlexConnect Vlan mode : | Enabled | |
|--|--|------|
| NativesID2banusst | | |
| WLAN 1 : | 57 (Group-Specific) 🤜 | |
| WLAN 4 | | |
| WEAN 5 Page 1 March 1 Street Street | (Wlan-Specific) | |
| FlexConnect VLAN ACL Mappings | | |
| FlexConnect Group | ensweren weren abc St (Group-Specific) | |
| Group VLAN ACL Mappings | | |
| | | |
| AP-Specific FlexConnect Policy ACLs | | |
| L2Acl Configuration | Not Available | |
| FlexConnect Local-Split ACLs : | | |
| WLAN ID PROFILE NAME | ACL | TYPE |
| | | |
| The second s | | |
| Flexconnect Central-Dhcp Values : | | |

The following commands can be used to troubleshoot this feature:

On WLC:

debug flexconnect wlan-vlan <enable | disable>

On AP:

debug capwap flexconnect wlan-vlan

Guidelines

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

VLAN Name Override for FlexConnect

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

Dynamic VLAN Assignment with RADIUS Server

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

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

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

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

VLAN Name Override Overview

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

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

Use Case Definition

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



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

VLAN Mapping Design

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

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



Solution - AAA Override of VLAN Name

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

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



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

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

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

Feature Configuration

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

Configuring Features

To configure the features, perform these steps:

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

| | Security QoS Po | licy-Mapping Adva | nced |
|---|---|--|----------------|
| Layer 2 | Layer 3 AAA Serve | rs | |
| Select AAA s Radius Serve Radius Se | ervers below to override errs rver Overwrite interface (Authentication Servers () Enabled | Use of default servers of Enabled Accounting Servers | EAP Parameters |
| Server 1 | IP:9.1.0.101, Port:1812 ‡ | None ‡ | Enable |
| Server 2 | None ÷ | None + | |
| Server 3 | None ‡ | None + | |
| | None ‡ | None ‡ | |
| Server 4 | | None | |
| Server 4 Server 5 | None \$ | None + | |
| Server 4 Server 5 Server 6 | None ÷ | None + | |

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

| li.ili. cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT CO | MMANDS HELP <u>f</u> eedback |
|------------------|--|--|
| WLANs | WLANs > Edit 'jk-aaa-ca' | |
| WLANS | General Security QoS Policy-Mapping Advanced | |
| Advanced | Clear HotSpot Configuration | NAC |
| | Client user idle timeout(15-100000) | NAC State None : |
| | Client user idle threshold (0-10000000) 0 Bytes | Load Balancing and Band Select |
| | Radius NAI-Realm | Client Load Balancing |
| | Off Channel Scanning Defer | Client Band Select |
| | Scan Defer Principy 0 1 2 3 4 5 6 7 | Passive Client |
| | | Passive Client |
| | Econ Defec Time(mases) 100 | Voice |
| | Electonnect | Media Session Snooping 🔲 Enabled |
| | | Re-anchor Roamed Voice Clients 🔲 Enabled |
| | Switching 2 Enabled | KTS based CAC Policy Enabled |
| | FlexConnect Local Auth 12 Enabled | Radius Client Profiling |
| | Learn Client IP Address 💈 🥑 Enabled | DHCP Profiling |
| | Vian based Central | HTTP Profiling |
| | Switching 12 | Local Client Profiling |
| | Central DHCP Processing Enabled | DHCP Profiling |
| | Override DNS | HTTP Profiling |
| | NAT DAT Enshied | |

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

| li.ili. cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK |
|-------------------------------------|--|
| WLANS WLANS WLANS Advanced | WLANs > Edit 'jk-aaa-ca' General Security QoS Policy-Mapping Advanced Allow AAA Override Enabled Coverage Hole Detection Enabled Enable Session Timeout 1800 Session Timeout (secs) DHCP Server Aironet IE Ørabled Diagnostic Channel 18 Enabled Override Interface ACL IPv4 None 2 IPv6 None 2 Split Tunnel P2P Blocking Action Diabled 2 Client Exclusion 2 O Maximum Allowed Clients 8 0 Static IP Tunneling 11 Enabled Wi-Fi Direct Clients Policy Disabled 2 Wi-Fi Direct Clients Policy Disabled 2 Wi-Fi Direct Clients Policy Disabled 2 Maximum Allowed Clients Per AP Radio 200 Clear HotSpot Configuration Enabled |
| | Client user idle timeout(15-100000) Client user idle timeout(15-1000000) Rutes Load Balancing and Band Select |

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

| | MONITOR WLANS | CONTROLLER WIRELESS SECURITY | MANAGEMENT COMMANDS HELP | FEEDBACK | Sa <u>v</u> e (| Configuration Eing | y Logout Be A t |
|---|------------------|------------------------------|--------------------------------|-------------------|---------------------|--------------------|------------------------|
| Wireless | All APs | | | | | | Entries 1 - 2 o |
| Access Points All APs Radios 802.11a/n/ac 802.11b/q/n | Current Filter | None 2 | [Change Filter] [Clear Filter] | | | | |
| Dual-Band Radios Global Configuration | AP Name | IP Address(Ipv4/Ipv6) | AP Model | AP MAC | AP Up Time | Admin Status | Operational Status |
| PAdvanced | AP/872.ea60.7e89 | 9.10.37.100 | AIR-CAP36021-A-K9 | f8:72:ea:60:7e:89 | 0 d, 00 h 56 m 54 s | Enabled | REG |
| Mesn | AP-2602 | 9.10.37.101 | AIR-CAP2602I-A-K9 | 44:2b:03:9a:8a:3f | 0 d, 00 h 56 m 25 s | Disabled | REG |
| Provines FlexConnect Groups PlexConnect ACLs PlexConnect VLAN Templates OEAP ACLs | | | | | | | |

| uluilu cisco | MONITOR WLANS C | ONTROLLER WIRELESS SECURITY | MANAGEMENT COMMANDS HE | P EEEDBACK |
|---|--|--|--|---|
| Wireless All APs Radios 802.11a/n/ac | All APs > Details for General Creden | r AP-2602 tials Interfaces High Availabilit | y Inventory FlexConnec | Advanced |
| S02.11b/g/n Dual-Band Radios Global Configuration Advanced Mesh RF Profiles | General AP Name Location AP MAC Address Base Radio MAC Admin Status | AP-2602 default location 44:2b:03:9a:8a:3f 3c:ce:73:1a:24:40 Disable = | Versions Primary Software Version Backup Software Version Predownload Status Predownloaded Version Predownloaded Version Predownload Mext Retry Time | 8.1.10.66 7.2.104.6 None NA |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates OEAP ACLs Network Lists 802.11a/n/ac | AP Mode AP Sub Mode Operational Status Port Number Venue Group | FlexConnect None 2 REG 1 Unspecified | Predownload Retry Count Boot Version IOS Version Mini IOS Version IP Config | NA 12.4.25.0 15.3(20141119:164129)\$ 7.2.104.6 |
| B02.11b/g/n Media Stream Application Visibility And Control | Venue Type Venue Name Language Network Spectrum Interface Key | Unspecified : E4884E4720B914869D2485DB126019DE | CAPWAP Preferred Mode DHCP Ipv4 Address Static IP (Ipv4/Ipv6) Time Statistics | Ipv4 (Global Config) 9.10.37.101 |

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

| ululu cisco | | <u>w</u> lans | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|----------|---------------|------------|----------|----------|------------|----------|------|----------|
| Wireless | FlexCon | nect Gro | ups > New | | 1 | | | | |
| Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | Group Na | ame | | | | | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | + | | | | | | | | |
| OEAP ACLS | | | | | | | | | |

8. Click Apply.

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

| cisco | MONITOR | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | нецр | FEEDBACK |
|---|------------|---------------|------------|----------|----------|------------|----------|------|----------|
| Wireless | FlexCon | nect Gro | ups | 1 | | | | | |
| Access Points All APs Padios | Group Nar | ne | | ÷ | | | | | |
| 802.11a/n/ac | FlexGroup/ | 5 · | | | | | | | |
| 802.11b/g/n Dual-Band Radios Global Configuration | FlexGroupE | 2 | | | | | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | + | | | | | | | | |
| OEAP ACLS | | | | | | | | | |
| Network Lists | | | | | | | | | |
| ▶ 802.11a/n/ac | | | | | | | | | |

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

| FlexConne | ct Groups | >Edit 'Flex | (GroupA' | | | | | | | |
|--|---|------------------------|------------------------------|-------------|-----------|---------------|-------------|---------|------|--|
| General | Local Au | thentication | Image Upgrade | ACL Mapping | Central D | HCP WLAN | VLAN mappin | 9 | | |
| Group Na VLAN Tem Enable AP Application | nplate Name Local Auther n Visibility | FlexG Remo Disab | roupA te Site A : le : | | | | | | | |
| FlexConn | ect APs | | | | | AAA | | | | |
| Add AP | 1 | | | | | Server Ip Add | ress | | | |
| АР МАС А | ddress | AP Name | | Status | | Server Type | | Primary | • | |
| f8:72:ea:6 | 0:7e:89 | APf872.ea60.7 | e89 | Associated | | Shared Secret | | | | |
| | | | | | | Confirm Share | d Secret | | | |
| | | | | | | Port Number | | 1812 |] | |
| | | | | | | Add | | | | |
| | | | | | | Server Type | Address | | Port | |
| | | | | | | UnConfigured | Unconfigure | d | 0 | |
| | | | | | | UnConfigured | Unconfigure | d | 0 | |
| | | | | | | | | | | |

| FlexConne | ct Groups | >Edit 'Flex | (GroupB' | | | | | | | |
|-------------|--------------|------------------------|---------------|-------------|-----------|---------------|-------------|---------|------|--|
| | | | | | | | | | | |
| | | | | | | | | _ | | |
| General | Local Aut | thentication | Image Upgrade | ACL Mapping | Central I | HCP WLAN | VLAN mappir | ng | | |
| | | | | | | | | | | |
| Group Na | me | FlexG | roupB | | | | | | | |
| VLAN Tem | plate Name | Remo | te Site B 💠 | | | | | | | |
| Enable AP | Local Auther | ntication ² | | | | | | | | |
| Application | n Visibility | Disab | le 0 | | | | | | | |
| | | | | | | | | | | |
| FlexConne | ect APs | | | | | AAA | | | | |
| | 1 | | | | | Server In Add | | _ | | |
| Add AP | 1 | | | | | Server ip nou | | | | |
| AP MAC A | ddress | AP Name | | Status | | Server Type | | Primary | + | |
| 44:2b:03:9 | a:8a:3f | AP-2602 | | Associated | | Shared Secret | | | | |
| | | | | | | Confirm Share | d Secret | | | |
| | | | | | | Port Number | | 1812 | 1 | |
| - | | | | | | Port Number | | 1016 | | |
| | | | | | | Add | | | | |
| | | | | | | | | | | |
| | | | | | | Server Type | Address | | Port | |
| | | | | | | UnConfigured | Unconfigure | -d | 0 | |
| | | | | | | UnConfigured | Unconfigure | ad a | 0 | |
| | | | | | | enconinger cu | onconigure | | 3 | |

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

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

| AAA VLAN | ACL mapping | LAN-ACL mapping | Policies | |
|-----------|-------------|-----------------|----------|--|
| | | | | |
| AAA VLAN | ACL Mapping | | | |
| Vlan Id | 0 | | | |
| Ingress / | CL none ÷ | | | |
| Egress A | CL none ÷ | | | |
| | Add | | | |
| Vian Id | Tooress ACI | Earnes ACI | | |
| 37 | none + | none ÷ | | |
| | none ÷ | none + | | |
| 38 | | | | |

| | ~ | 1 | | Central Driver | |
|-----------|-----------------|----------------|----------|----------------|--|
| AAA VLAN | -ACL mapping WL | AN-ACL mapping | Policies | | |
| | | | | | |
| | N ACL Mapping | | | | |
| | | | | | |
| Vian Id | 0 | | | | |
| Ingress / | ACL acl1 ÷ | | | | |
| Egress A | CL acl1 ÷ | | | | |
| | Add | | | | |
| Vian Id | Ingress ACL | Foress ACL | | | |
| 37 | none ÷ | none + | | | |
| | | none ÷ | | | |
| 39 | none + | | | | |

12. Click Apply.

VLAN Name Mapping

Creating VLAN Name Template

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

| uluulu cisco | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | EEEDBACK | Save Configuration | n <u> P</u> ing Logo | ut <u>B</u> efresh A <u>H</u> ome |
|---|----------|-----------|-------------|----------|----------|------------|----------|------|----------|--------------------|-------------------------|--------------------------------------|
| Wireless | FlexConr | plates SI | AN Template | List | | | | | | C | New | Серу |
| 802.11b/g/n Dual-Band Radios Global Configuration | | | | | | | | | | | | |
| Advanced | | | | | | | | | | | | |
| Mesh | | | | | | | | | | | | |
| RF Profiles | | | | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | | | | |
| OEAP ACLs | | | | | | | | | | | | |

14. Click Apply.

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

| cisco | MONITOR WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGE | MENT | COMMANDS | HELP | FEEDBACK |
|---|-----------------|---------------|----------|----------|----------|------|----------|------|----------|
| Wireless | FlexConnect VL/ | AN Template I | List | | | | | | |
| | VLAN Templates | | | | Status | - | | | |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | BemoteSiteA | | | | Modified | | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN | | | | | | | | | |

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

| ahaha | | | | | | | | | | | Saye Cor | figuration <u>P</u> ing L | ogout <u>R</u> efresh |
|---|-----|--------------|------------|-------------------------|----------|----------|------------|----------|------|----------|----------|---------------------------|-------------------------|
| CISCO | MON | ITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | | | 🔐 Home |
| Wireless | VLA | AN Ter | nplate > | Edit | | | | | | | < Back | New Mapping | Apply All |
| * Access Points All APs | VLA | N Templ | late Name | RemoteSiteA Modified | | | | | | | | | |
| Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | Id | VLAN Name | VLAN Id | | | | | | | | | | |
| Advanced | | | | | | | | | | | | | |
| Mesh | | | | | | | | | | | | | |
| RF Profiles | | | | | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | | | | | |
| OEAP ACLS | | | | | | | | | | | | | |

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

| VLAN Template | > Maps > New | < Back Apply |
|----------------------|-----------------|--------------|
| VLAN Name VLAN ID | marketing 38 | 1 |
| | | |
| | | |
| | | |

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

| Wireless | VLA | N Template > E | dit | | < Ba | ick | New Mapping | Арр |
|---|----------------|----------------------|-------------------------|---------|------|-----|-------------|-----|
| Access Points All APs Radios | VLAN Statu: | l Template Name s | RemoteSiteA Modified | | | | | |
| 802.11a/n/ac 802.11b/g/n | Id | VLAN Name | | VLAN Id | | | | |
| Dual-Band Radios Global Configuration | 1 | marketing | | 38 | | | | |
| Advanced | | | | | | | | |
| Mesh | | | | | | | | |
| RF Profiles | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | |
| OEAP ACLs | | | | | | | | |
| Network Lists | | | | | | | | |

The status of the template changes to Applied.

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

| | ဂျားပျား cisco | MONI | TOR | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|---|--------|------|---------------|--------------------------|----------|----------|------------|----------|------|----------|
| W | ireless | VLA | N Te | mplate > | > Edit | | | | | | |
| + | Access Points All APs Radios | Status | Temp | late Nam | e Remote Site Applied | A | | | | | |
| | 802.11a/n/ac 802.11b/n/n | Id | VLA | N Name | | VLAN Id | | | | | |
| | Dual-Band Radios Global Configuration | 1 | mark | ceting | | 38 | | | | | |
| • | Advanced | | | | | | | | | | |
| | Mesh | | | | | | | | | | |
| | RF Profiles | | | | | | | | | | |
| | FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | | |
| | OEAP ACLS | | | | | | | | | | |
| | Network Lists | | | | | | | | | | |
| • | 802.11a/n/ac | | | | | | | | | | |
| * | 802.11b/g/n | | | | | | | | | | |
| | Media Stream | | | | | | | | | | |
| * | Application Visibility And Control | | | | | | | | | | |
| | Lync Server | | | | | | | | | | |

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

| ာါာာါာ cisco | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|--------------------|-----------|--------------------------|----------|----------|------------|----------|------|----------|
| Wireless | VLAN T | emplate : | > Edit | | | | | | |
| Access Points All APs Radios | VLAN Tem Status | plate Nam | e Remote Site Applied | в | | | | | |
| 802.11a/n/ac 802.11b/g/n | Id VL | N Name | | VLAN Id | | | | | |
| Dual-Band Radios Global Configuration | 1 ma | rketing | | 39 | ۵ | | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | |
| OEAP ACLS | | | | | | | | | |
| Network Lists | | | | | | | | | |

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

| | cisco | | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAG | EMENT | COMMANDS | HELP | FEEDBACK |
|---|--|------------|----------|-------------|----------|----------|---------|-------|----------|------|----------|
| W | ireless | FlexCon | nect VL/ | AN Template | List | - | | | | | |
| * | Access Points All APs | VLAN Tem | plates | | | | Status | | | | |
| 8 | 802.11a/n/ac | Remote Sit | A at | | | | Applied | | | | |
| | 802.11b/g/n Dual-Band Radios | Remote Sit | 8.0 | | | | Applied | | | | |
| | Global Configuration | | | | | | | | | | |
| ۲ | Advanced | | | | | | | | | | |
| | Mesh | | | | | | | | | | |
| | RF Profiles | | | | | | | | | | |
| | FlexConnect Groups FlexConnect ACLs FlexConnect VLAN | | | | | | | | | | |
| | OEAP ACLS | | | | | | | | | | |
| | Network Lists | | | | | | | | | | |
| Þ | 802.11a/n/ac | | | | | | | | | | |
| Þ | 802.11b/g/n | | | | | | | | | | |
| ۲ | Media Stream | | | | | | | | | | |
| + | Application Visibility And Control | | | | | | | | | | |

Copying VLAN Name Template (Optional)

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

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

| iliilii cisco | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGE | MENT | COMMANDS | HELP | FEEDBACK | Sa <u>v</u> e Configuration | Eing | Logou | Befresh |
|---|------------|----------|-------------|----------|----------|---------|------|----------|------|----------|-----------------------------|------|-------|---------|
| Wireless | FlexConr | nect VLA | AN Template | List | | | | | | | 1 | New | | Сору |
| Access Points All APs Padios | VLAN Tem | plates | | | | Status | | | | | | | | 1 |
| 802.11a/n/ac | Remote Sit | te A | | | | Applied | | | | | | | | • |
| 802.11b/g/n Dual-Band Radios | Remote Sit | te B | | | | Applied | | | | | | | | |
| Global Configuration | | | | | | | | | | | | | | |
| Advanced | | | | | | | | | | | | | | |
| Mesh | | | | | | | | | | | | | | |
| RF Profiles | | | | | | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | | | | | | |
| OFAD ACLE | | | | | | | | | | | | | | |

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

| ւվովը cisco | MONITOR | <u>W</u> LANs | | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|------------------------|----------------------|-------------|----------|----------|------------|----------|------|----------|
| Wireless | Flex Con | nect VL | AN Template | > Copy | | | | | |
| ▼ Access Points All APs ▼ Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | VLAN Ten Existing V | nplate N /LAN Ter | ame | • | | | | | |
| Advanced Mesh | Сору | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | |
| OEAP ACLs | | | | | | | | | |

22. Click Copy.

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

| | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK |
|---|--|
| Wireless | Flex Connect VLAN Template > Copy |
| ▼ Access Points All APs ▼ Radios 802.11a/n/ac 802.11bg/n Dual-Band Radios Global Configuration | VLAN Template Name Remote Site C Existing VLAN Templates Remote Site 8 ÷ |
| Advanced | Сору |
| Mesh | |
| RF Profiles | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | |

| Texconnect VLAN Template List | |
|-------------------------------|--------------|
| VLAN Templates | Status |
| Remote Site A | Applied 🔽 |
| Remote Site B | Applied 🔽 |
| Remote Site C | Modified 🔽 🔫 |

Assigning VLAN Name Template

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

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

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

| FlexC | onnec | t Groups | >Edit 'Flex | GroupA' | | | | | | | |
|--------------------------|----------------------|--|--|---------------|-------------|-----------|-----------------|-------------|---------|------|--|
| Gene | eral | Local Aut | hentication | Image Upgrade | ACL Mapping | Central D | HCP WLAN V | /LAN mappin | g | | |
| Gro VLA Ena App | AN Temp able AP L | ie late Name ocal Auther Visibility | FlexGr Remote Re | e = = | | | | | | | |
| Flex | Conne | ct APs | | | | | AAA | | | | |
| Ad | Id AP | dress | AP Name | | Status | | Server Ip Addre | 155 | Primary | \$ | |
| f8:7 | 2:ea:60 | :7e:89 | APf872.ea60.7e | 89 | Associated | | Shared Secret | | | | |
| | | | | | | | Confirm Shared | Secret | | | |
| | | | | | | | Port Number | | 1812 |] | |
| | | | | | | | Server Type | Address | | Port | |
| | | | | | | | UnConfigured | Unconfigure | d | 0 | |
| | | | | | | | UnConfigured | Unconfigure | d | 0 | |

| xConnect G | roups > Edit 'Fle | xGroupB' | | | | | | |
|------------------------------------|----------------------------------|------------------------|-------------|------------|-----------------|--------------|----------|-----|
| Seneral Lo | cal Authentication | Image Upgrade | ACL Mapping | Central Di | ICP WLAN V | LAN mapping | | |
| Group Name | Flex0 Name Rem | GroupB ote Site B 💠 | | | | | | |
| Enable AP Loca Application Visi | Authentication ² Disa | ble ÷ | | | | | | |
| lexConnect | Ps | | | | AAA | | | |
| Add AP | | | | | Server Ip Addre | ess | | |
| AP MAC Addre | s AP Name | | Status | | Server Type | P | rimary ÷ | |
| 44:2b:03:9a:8a | 3f AP-2602 | | Associated | | Shared Secret | | | |
| | | | | | Confirm Shared | Secret | | |
| | | | | | Port Number | 16 | 12 | |
| | | | | | Add | | | |
| | | | | | Server Type | Address | Po | ort |
| | | | | | UnConfigured | Unconfigured | 0 | |
| | | | | | UnConfigured | Unconfigured | 0 | |

24. Click Apply.

Verifying VLAN Name Mappings on FlexConnect AP

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

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

| cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK |
|---|---|
| Wireless | All APs > Details for APf872.ea60.7e89 |
| Access Points All APs Radios | General Credentials Interfaces High Availability Inventory FlexConnect Advanced |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | VLAN Support |
| Advanced | FlexConnect Group Name FlexGroupA |
| RF Profiles | VLAN Template Name Remote Site A |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | VLAN Name Id Mappings PreAuthentication Access Control Lists |
| OEAP ACLs Network Lists | Extensi WebAuthentication ACLs Local Spirt ACLs |
| 802.11a/n/ac 802.11b/g/n | Central DHCP Processing Laver2.ACLs |
| Media Stream | OfficeExtend AP |

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

| ululu cisco | MONITOR | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | нецр | FEEDBACK |
|---|---------|---------------|-------------------|----------|-------------|------------|----------|------|----------|
| Wireless | All APs | > APf87 | 2.ea60.7e89 > 1 | VLAN Nam | e ID Mappir | ngs | | | |
| Access Points All APs | AP Nam | e | AP(872.ea60.7e89 | | | | | | |
| ▼ Radios 802.11a/n/ac | Base Ra | dio MAC | ec:e1:a9:80:6b:a0 | 0 | | | | | |
| 802.11b/g/n Dual-Band Radios | Id | VLAN Na | me | | VLAN Id | | | | |
| Global Configuration | 1 | marketing | 1 | | 38 | - | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups | | | | | | | | | |
| FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | |

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

| cisco | | WLANS CONTRO | LLER WIRELE | SS SECURITY MA | NAGEMENT CC | MMANDS HELP | FEEDBACK | |
|---|--------------------------------|-------------------------------------|--------------|-------------------|-------------|-------------|----------|--|
| Wireless | All APs > D | etails for AP- | 2602 | | | | | |
| Access Points All APs Radios | General | Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced | |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | VLAN Support Native VLAN ID | | 37 | VIAN Maggings | | | | |
| Advanced Mesh | FlexConn | nect Group Name | FlexGroup8 | | | | | |
| RF Profiles | VLAN Te | mplate Name | Remote Site | в | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | VIAN Ne PreAuthent | me Id Mappings tication Access C | ontrol Lists | | | | | |
| OEAP ACLS | External 3 Local Spli | VebAuthentication A | | | | | | |

| | cısco | MONITOR | <u>W</u> LANs | | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | EEEDBACK |
|---|---|----------|---------------|-------------------|------------|----------|------------|----------|------|----------|
| W | ireless | All APs | > AP-260 | 2 > VLAN Nar | ne ID Mapp | ings | | | | |
| | Access Points All APs | AP Name | | AP-2602 | | | | | | |
| | 802.11a/n/ac | Base Rad | io MAC | 3c:ce:73:1a:24:40 |) | | | | | |
| | 802.11b/g/n Dual-Band Radios | Id | VLAN Nam | e | | VLAN Id | | | | |
| | Global Configuration | 1 | marketing | | | 39 ┥ | | | | |
| | Advanced | | | | | 17 | | | | |
| | Mesh | | | | | | | | | |
| | RF Profiles | | | | | | | | | |
| | FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | | | |
| | OEAP ACLs | | | | | | | | | |
| | Network Lists | | | | | | | | | |

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

RADIUS Server Configuration

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

| | | | Policy Elements > Autorizatio |
|----------------------------------|---|--|--|
| | | | |
| | | in Tasks | Common T |
| Males | - | ibutes | Common Tasks Attribu |
| Value | Topped Enum | | Attribute |
| [T:1] 802 | Tagged Enum | pe | Tunnel-Medium-Type |
| [T:1] marketing | Tagged String | up-ID | Tunnel-Private-Group |
| | | | - |
| | | | |
| | | | |
| | | | Manually Entered |
| Value | Type | | Attribute |
| 2 1800 | Unsigned Integer 32 | Session-Timeout | |
| abcdef | String | e-Name | Airespace-Interface-N |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | CHINA CHINA |
| | Delete | t \/ Replace /\ | Add /\ Edit \ |
| * | | RADIUS-IETF | Dictionary Type: |
| ect | Sele | ĸ | o RADIUS Attribute: |
| manual | - Contraction | | · Andreite Tennet |
| | | | Attribute Type: |
| + | | Static | Attribute Value: |
| | | Static | Attribute value: |
| Value 2 1800 abcdef ect | Type Unsigned Integer 32 String Delete | e-Name t \/ Replace /\ RADIUS-IETF :: Static | Manually Entered Attribute Session-Timeout Alrespace-Interface-N Add /\ Edit \ Dictionary Type: RADIUS Attribute: Attribute Type: Attribute Value: |

Verifying AAA Override

To verify AAA override, perform these steps:

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

| ululu cisco | • | | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | |
|---------------------------------------|------|------------------------|---------------|---------------|----------|-----------------|----------------|----------|------|--------------|-----------|
| Monitor Summary F Access Point | 1 | Clients Current Fil | ter Nor | 16 | | (Change Filter) | [Clear Filter] | | | | |
| Cisco Clean | lir | Client MA | C Addr | IP Address(Ip | v4/Ipv6) | | AP Name | | | WLAN Profile | WLAN SSID |
| Statistics | | 00:40:95: | 4:59:93 | 9.10.38.6 | | | APf872.ea | 60.7e89 | | jk-aaa-ca | jk-aaa-ca |
| > CDP | | | | | | | | | | | |
| Rogues | | | | | | | | | | | |
| Clients Sleeping Clie Multicast | ints | | | | | | | | | | |

| rrent Status Profile Management | Diagnostics | |
|---------------------------------|---------------|------------------------------|
| 1111111 | | |
| CISCO Profile Name: | jk-aaa-ca | |
| Link Status: | Authenticated | Network Type: Infrastructure |
| Wireless Mode: | 5 GHz 54 Mbps | 161 |
| Server Based Authentication: | LEAP | Data Encryption: AES |
| IP Address: | 9.10.38.6 | |
| Signal Strength: | | Excellent |
| | | (|

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

| ululu cisco | MONITOR WLANS CONTR | COLLER WIRELESS SECURITY MA | NAGEMENT COMMANDS HELP FEEDBACK | |
|---|---|---|-------------------------------------|-----------------|
| Monitor Summary Access Points Cisco CleanAir Statistics | Clients > Detail Max Number of Records | 0 : Clear AVC Stats | | |
| > CDP | Port Number | 1 | CF Pollable | Not Implemented |
| Rogues | Flex VLAN Name | marketing | CF Poll Request | Not Implemented |
| Clients | VLAN ID | 38 | Short Preamble | Not Implemented |
| Sleeping Clients | CCX Version | CCXv5 | PBCC | Not Implemented |
| Multicast | E2E Version | Not Supported | Channel Agility | Not Implemented |
| Applications | Mobility Role | Local | Re-authentication timeout | 604 |
| > Lync | Mobility Peer IP Address | N/A | Remaining Re-authentication timeout | 0 |
| Local Profiling | Policy Manager State | RUN | WEP State | WEP Foable |
| | Management Frame Protection | No | | THE LEADER |
| | UpTime (Sec) | 251 | PMIP Properties | |
| | Power Save Mode | OFF | Mobility type | Simple |
| | Current TxRateSet | 48.0 | | |
| | Data RateSet | 6.0,9.0,12.0,18.0,24.0,36.0,48.0, 54.0 | | |
| | KTS CAC Capability | No | | |
| | 802.11u | Not Supported | | |

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

| cisco | MONITOR WLANS CONTRO | LLER WIRELESS | SECURITY MANAGEMEN | r commands | HELP | FEEDBACK | | Sage Configuration |
|-----------------------|----------------------------|----------------|--------------------------------|------------|------|--------------|-----------|--------------------|
| Monitor 🥖 | Clients | | | | | | | |
| Summary Access Points | Current Filter None | | (Change Filter) [Clear Filter] | | | | | |
| Cisco CleanAir | Client MAC Addr IP Addr | ess(Ipv4/Ipv6) | AP Nar | e | | WLAN Profile | WLAN SSID | User Name |
| Statistics | 00:40:96:64:59:93 9.10.39. | 00 | AP-260 | | | jk-aaa-ca | jk-aaa-ca | jkakuman |
| > CDP | - | | | | | | | |
| Rogues | | | | | | | | |
| Clients | | | | | | | | |
| Sleeping Clients | | | | | | | | |
| Multicast | | | | | | | | |
| Applications | | | | | | | | |
| > Lync | | | | | | | | |
| Local Profiling | | | | | | | | |

| n Options | Help | | | |
|---|--------------------|---------------|---------------------|-------------|
| rrent Status | Profile Management | Diagnostics | | |
| dual | Li. | | | |
| cisc | O Profile Name: | įk-aaa-ca | | |
| | Link Status; | Authenticated | Network Type: Inf | rastructure |
| | Wireless Mode: | 5 GHz 54 Mbps | Current Channel: 16 | 5 |
| Server Based Authentication: IP Address: | | LEAP | Data Encryption: AE | s |
| | | 9.10.39.100 | | |
| | Signal Strength: | | Excel | ent |
| | | | | dyanced |

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

| ll cisco | MONITOR WLANS CONTRO | DLLER WIRELESS SECURITY M | ANAGEMENT COMMANDS HELP FEEDBACK |
|--|---|--|----------------------------------|
| CISCO Monitor Summary Access Points Cisco CleanAir Statistics CDP Rogues Clients Sleeping Clients Multicast Applications Local Profiling | MONITOR WLANS CONTRO Clients > Detail Max Number of Records I General AVC Statistic Flex VLAN Name VLAN ID CCX Version E2E Version Mobility Role Mobility Role Mobility Peer IP Address Policy Manager State Management Frame Protection UpTime (Sec) Power Save Mode Current TxRateSet Data RateSet | CCXv5 Not Supported Local N/A RIN No 267 OFF 54.0 6.0,9.0,12.0,18.0,24.0,36.0,48.0, | ANAGEMENT COMMANDS HELP FEEDBACK |
| | KTS CAC Capability 802.11u Security Information | No Not Supported | |
| | Security Policy Completed | Yes | |

Client ACL Support

Client ACL Support

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

Client ACL Overview

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



Configuring Client ACL

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

Client ACL Support

Figure 51 Create Local Switching WLAN

| WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN enjoy enjoy Enabled [WPA2](Auth(802.1X)) 2 WLAN ciscowic ciscowic Enabled [WPA2](Auth(802.1X)) | | | | | | |
|--|----------------------|---------|-----------------|-----------------|------|---------|
| 1 WLAN enjoy Enabled [WPA2](Auth(802.1X)] 2 WLAN ciscowic Enabled [WPA2](Auth(802.1X)] | Security Policies | Admin S | WLAN SSID | Profile Name | Туре | WLAN ID |
| 2 WLAN ciscowic ciscowic Enabled [WPA2][Auth(802.1X)] | [WPA2][Auth(802.1X)] | Enabled | enjoy | enjoy | WLAN | 1 |
| | [WPA2][Auth(802.1X)] | Enabled | ciscowic | ciscowlc | WLAN | 2 |
| 4 WLAN ciscowic-peap ciscowic-peap Enabled [WPA2][Auth(802.1X)] | [WPA2][Auth(802.1X)] | Enabled | ciscowlc-peap | ciscowlc-peap | WLAN | 4 |
| 5 WLAN ciscowic-eaptis ciscowic-eaptis Enabled [WPA2][Auth(802.1X)] | [WPA2][Auth(802.1X)] | Enabled | ciscowlc-eaptIs | ciscowlc-eaptls | WLAN | 5 |

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

| WLANs > Edit 'ciscowl | c' | |
|---|------------------------------------|-----------------------------------|
| General Security | QoS Policy-Mapping Advanced | |
| Allow AAA Override | Enabled | DHCP |
| Coverage Hole Detection | Enabled | DHCP Server Override |
| Enable Session Timeout | 1800 Session Timeout (secs) | DHCP Addr. Assignment 📃 Required |
| Aironet IE | Enabled | OEAP |
| Diagnostic Channel | Enabled | Solit Tunnel |
| Override Interface ACL | IPv4 None PV6 None | |
| P2P Blocking Action | Disabled | Management Frame Protection (MFP) |
| Client Exclusion 2 | Enabled 60 Timeout Value (secs) | MFP Client Protection 4 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 Per AP Radio | 200 | NAC State None |
| Clear HotSpot | Foabled | Load Balancing and Band Select |

3. Create a FlexConnect ACL.

FlexConnect ACL can be configured from the Security page as well as from the Wireless page.
Figure 52 Configure FlexConnect ACL

| cisco | | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|---|----------|----------|---------------|----------|----------|------------|----------|------|----------|
| Security | FlexConr | nect Acc | ess Control L | ists | | | | | |
| AAA General | Acl Name | | | | | | | | |
| AdDIUS Authentication Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies | <u>8</u> | | | | ٥ | | | | |
| Local EAP | | | | | | | | | |
| Priority Order | | | | | | | | | |
| Certificate | | | | | | | | | |
| Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs | | | | | | | | | |

Figure 53 Configure FlexConnect ACL

| cisco | MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | |
|--|----------|----------|---------------|----------|----------|------------|----------|------|----------|--|
| Wireless | FlexCon | nect Acc | ess Control L | ists | | | | | | |
| Access Points All APs Radios B02.11a/n/ac B02.11b/g/n Dual-Band Badios | Aci Name | | | | 0 | | | | | |
| Global Configuration Advanced | | | | | | | | | | |
| Mesh RF Profiles FlexConnect Groups | | | | | | | | | | |
| B02.11a/n/ac B02.11b/n/ac | | | | | | | | | | |
| Media Stream Application Visibility And Control | | | | | | | | | | |

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

Figure 54 ACL Mapping on FlexConnect Group

| | Local Hathenere | acion | Image Upgrade | ACL Mapping | Central DHCP | WLAN VLAN mapping | |
|-----------|------------------------|-------|---------------|-------------|--------------|-------------------|--|
| AA VLAN | -ACL mapping | WLAN | -ACL mapping | Policies | | | |
| | | | | | | | |
| olicies | | | | | | | |
| Policy AC | L ad | | | | | | |
| | | | | | | | |
| | Add 🔨 | | | | | | |
| | Add | | | | | | |
| olicy Acc | Add tess Control Lists | 1 | | | | | |
| olicy Acc | Add tess Control Lists | 1 | | • | | | |
| icy Acc | Add tess Control Lists | 1 | | • | | | |
| licy Acc | Add tess Control Lists | 1 | | | | | |

Figure 55 ACL Mapping on AP

| AP Name | AP_3600 | | | |
|---|---------------------------------|-------------|----------|--|
| Base Radio MA | C 34:a8:4e:e7:5b:c0 | | | |
| VLAN ACL M | apping | | | |
| WLAN Id | 0 | | | |
| | | | | |
| WebAuth ACL | ad | | | |
| WebAuth ACL | Add | | | |
| WebAuth ACL | Add WLAN Profile Name | WebAuth ACL | | |
| WebAuth ACL | Add Add WLAN Profile Name | WebAuth ACL | | |
| WebAuth ACL WLAN Id Policies Policy ACL | Add WLAN Profile Name | WebAuth ACL | | |
| WebAuth ACL WLAN Id Policies | Add WLAN Profile Name | WebAuth ACL | <u>.</u> | |

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

Figure 56 Aire-Acl-Name on Cisco ACS Server

| abab | User Setup | × |
|--|---|---|
| CISCO | 0 H2D [14179/004] Aire-802.1P-Tag • Account Disabled 0 • Deleting a Username 1[14179/005] Aire-Interface-Name • Supplementary User Info • Password Authentication • Supplementary User Info | - |
| Network Configuration System Configuration | Contract | |
| Administration Control Deternal User Databases Validation | 0 9 14179/008] Aire-Real-Time-Bandwidth-Average- Contract 0 14179/009] Aire-Data-Bandwidth-Burst-Contract • 14179/009] Aire-Data-Bandwidth-Burst-Contract • | |
| Network Access Pooffler Reports and Activity Online Decomentation | Interference of the second descent for the second descent descent descent descent desc | |
| | Submit Delete Cancel | _ |

Figure 57 Airespace ACL Name on ISE

| A Home Operations & Policy & Admi | iditation . | |
|--|---|-----------------|
| Authentication Authorization Conditions Results | honition 🖉 Posture 😡 Client Provisioning 🚍 Security Group Access | Policy Elements |
| Results | MACSec Policy NEAT Web Authentication (Local Web Auth) | |
| Authorization Authorization Profiles Downloadable ACLs Mode Bushlese Recting | C Arespace ACL Name acl | |
| imme roscure wood Profiles Profiling Assure Client Provisioning | Advanced Attributes Settings Radius:Tunnel-Private-Group-ID = atish-9 | Tag ID 2 |

6. Authenticate the client.

| , |
|---|
| |
| |
| |
| |
| |
| |
| |

CLI Configuration

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

Figure 58 show access-lists Output

| AP_3688#show | access-l | lists |
|--------------|----------|-------------------|
| Extended IP | | |
| 10 deny | icmp any | any (10 matches) |
| 28 permi | | any (328 matches) |
| AP 3688# | | |

Figure 59 Client ACL on AP

| Clients 8 A | ID VLAN | Status:S/I/ | B/A Age Txl | -R(A) Mode Enc | Key Rate | Mask Tx | Rx BVI | Split-ACL C | Lient-ACL L2-AC |
|----------------|----------|-------------|-------------|-----------------|------------|-----------|----------|-----------------------|-------------------------|
| 7cd1.c386.7edc | | 5 3A 48284 | 888 1FE 38 | 8 8-8 (8) 3388 | 688 1-18 8 | BEFFFFFFF | 0217 00C | and the second second | Characteristics and the |
| 9848.9658.d4be | | 2 38 48244 | 888 1F2 380 | 8 8-8 (8) 8188 | | OFF000008 | 8868 868 | a | ct: |
| | (Client) | Maxfri Def | UniPri Deff | fultfri Wiredfr | ot | | | | |
| cd1.c386.7edc | | | | | | | | | |
| 949.96b8.d4be | | | | | | | | | |
| | Agr TxLt | PkL MaxL | | | | | | | |
| cd1.c386.7edc | 18 38 8 | 65468 | | | | | | | |
| 040.96b8.d4be | 10 15 0 | | | | 8 (8,8) | | | | |
| | RxFkts | KBytes Du | p Dec Mic | TxPkts KByte | s Retry RS | SI SNR | | | |
| | | | | | | | | | |

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

Guidelines

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

- 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.

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

L3_Switch#show run | include multicast

ip multicast-routing distributed

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

interface Vlan56

ip address 9.5.56.1 255.255.255.0

ip helper-address 9.1.0.100

ip pim sparse-dense-mode

end

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

L3_Switch#show ip igmp interface

Vlan56 is up, line protocol is up

Internet address is 9.5.56.1/24

IGMP is enabled on interface

Current IGMP host version is 2

Current IGMP router version is 2

IGMP query interval is 60 seconds

IGMP configured query interval is 60 seconds

IGMP querier timeout is 120 seconds

IGMP configured querier timeout is 120 seconds

IGMP max query response time is 10 seconds

Last member query count is 2

Last member query response interval is 1000 ms

Inbound IGMP access group is not set

IGMP activity: 6 joins, 3 leaves

Multicast routing is enabled on interface

Multicast TTL threshold is 0

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

IGMP querying router is 9.5.56.1 (this system)

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

224.0.1.40(1)

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

Enabling VideoStream–Global

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

Figure 60 WLC Configuration

| ululu cisco | MONITOR WLA | Ns <u>C</u> ONTROLLER | WIRELESS | SECURITY | MANAGEMENT |
|----------------------|-----------------|------------------------|----------|----------|------------|
| Controller | Multicast | | | | |
| General | | | | | |
| Inventory | Enable Global M | ulticast Mode | Ø | | |
| Interfaces | Enable IGMP Sn | ooping | | | |
| Interface Groups | IGMP Timeout (| 30-7200 seconds) | 60 | | |
| Multicast | IGMP Query Inte | erval (15-2400 seconds | s) 20 | | |
| Network Routes | Enable MLD Sno | oping | 2 | | |
| Redundancy | MLD Timeout (3 | 0-7200 seconds) | 60 | | |
| Internal DHCP Server | MLD Query Inte | val (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.

Figure 61 Enable VideoStream - Global

| uluilu cisco | MONITOR WLANS CONTROL | LLER WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|--|---|---------------|----------|------------|----------|------|----------|
| Wireless All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios | Media Stream >General Multicast Direct feature Session Message Config Session announcement State | Enabled | | | | | |
| Global Configuration Advanced Mesh RF Profiles Network Lists | Session announcement URL Session announcement Email Session announcement Phone Session announcement Note | | | | | | |
| FlexConnect Groups FlexConnect ACLs | | | | | | | |

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

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

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

| cisco | HONITOR WLANS CONT | ROLLER WIRI | n.ess secu | RITY MANAGEMENT | COMMANDS | HELP | FEEDBACK | | |
|----------------|--|---------------|--------------|-----------------|----------|------|----------|--|--|
| WLANs | WLANs > Edit 'enjoy' | | | | | | | | |
| WLANS WLANS | General Security Burst Real-Time Rate | QoS Polic | 0 O | Advanced | | | | | |
| Autonceu | Override Per-SSID Bar | ndwidth Contr | racts (kbps) | 16 | | | | | |
| | | DownStream | UpStream | | | | | | |
| | Average Data Rate | 0 | 0 | | | | | | |
| | Burst Data Rate | 0 | 0 | | | | | | |
| | Average Real-Time Rate | 0 | 0 | | | | | | |
| | Burst Real-Time Rate | 0 | 0 | | | | | | |
| | Cear | | | | | | | | |
| | WHM | | | | | | | | |
| | WHM Policy | Allowed 1 | | | | | | | |
| | 7920 AF CAC | C Enabled | | | | | | | |
| | 7920 Client CAC | Enabled | | | | | | | |
| | Media Stream | | | | | | | | |
| | Multicast Direct | Z 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 C | 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 | |
| xConnect | | | Media Session Snooping | Enabled |
| FlexConnect Local | Enabled | | Re-anchor Roamed Voice Clients | Enabled |
| Switching ² | Chabled | | KTS based CAC Policy | Enabled |
| FlexConnect Local Auth 12 | Enabled | | Radius Client Profiling | |
| Learn Client IP Address 5 | Enabled | | DHCP Profiling | 0 |
| Vian based Central | Enabled | | HTTP Profiling | 0 |
| Switching 13 | | | Local Client Profiling | |
| Central DHCP Processing | Enabled | | DHCP Profiling | I |
| Override DNS | Enabled | | HTTP Profiling | |
| NAT-PAT | Enabled | | PMIP | |
| Central Assoc | Enabled | | PMIP Mobility Type | |
| | | | PMIP NAI Type | Hexadecimal + |
| | | | DMID Brofile | |

Figure 63 Change AP Mode to FlexConnect

| ieneral | Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced | |
|----------------------------------|---------------------------|--------------------|-------------------|-----------------|----------------|-------------------------|--|
| eneral | | | | Versions | | | |
| AP Name | | AP_1600 | | Primary Softwa | are Version | 8.0.72.114 | |
| Location | Location default location | | | Backup Softwa | re Version | 0.0.0.0 | |
| AP MAC Address 6c:20:56:13:f6:23 | | Predownload Status | | None | | | |
| Base Radio MAC 68:86:a7:cb:c0:d0 | | Predownloaded | Version | None | | | |
| Admin Stat | tus (| Enable + | | Predownload N | ext Retry Time | NA | |
| AP Mode | | FlexConnect | • | Predownload R | etry Count | NA | |
| AP Sub Mo | de | None : | _ | Boot Version | | 15.2.2.0 | |
| Operationa | al Status | REG | | IOS Version | | 15.3(20140203:113124)\$ | |
| Port Numb | er | 1 | | Mini IOS Versio | on | 7.4.1.37 | |
| Venue Gro | up (| Unspecified | • | IP Config | | | |
| Venue Typ | e (| Unspecified + | | IP Address | 0 | 9.5.56.105 | |
| Venue Nan | ne | | | IPv6 Address | | | |
| Language | | | | Static IP | (| 2 | |
| Network S | pectrum | 221750626078084 | 44412952510095252 | Static IPv6 | (| | |

Add Media Stream Configuration

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



| | MONITOR WLANS CONTROLLER WIRELES | 5 SECURITY MANAGEMENT COMMANDS | HELP FEEDBACK | Saye Configuration Ping Logout Befresh |
|---|--|---|---------------|--|
| Wireless | Media Stream > New | K | | < Back Apply |
| Access Points All APs Radies 802.11a/n/ac 802.11b/g/n Dual-Band Radies | Stream Name Multicast Destination Start IP Address(ipv4/ipv6) Multicast Destination End IP Address(ipv4/ipv6) Maximum Expected Bandwidth(1 to 35000 Kbps) | Modia2 229.77.77.28 229.77.77.28 500 | | 1 |
| Global Configuration Advanced Mesh RF Profiles Network Lists FlexConnect Groups FlexConnect ACLs B02.11a/n/ac | Resource Reservation Control(RRC) Para Select from predefined templates Average Packet Size (100-1500 bytes) RRC Periodic update RRC Priority (1-8) Traffic Profile Violation | Select 2 200 201 best-effort 2 | | |
| B02.11b/g/n Media Stream General Streams | | | | |

For configuration using CLI use:

configure media-stream add multicast-direct <media-stream-name> <start-IP> <end-IP> [template | detail

bandwidth> <packet-size> <Re-evaluation> video <priority> <drop|fallback>]

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

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

Enabling VideoStream - WLAN

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

| LANs | WLANs > Edit 'enjoy' | 5 | | | | | | |
|----------------|---|-----------|----------------|----------|--|--|--|--|
| WLANS WLANS | General Security Burst Real-Time Rate | QoS Polic | y-Mapping 0 | Advanced | | | | |
| | Override Per-SSID Bandwidth Contracts (kbps) 16 | | | | | | | |
| | 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 | | | | | | |
| | Media Stream | | | | | | | |
| | | | | | | | | |

Figure 65 Enable VideoStream - WLAN

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

| Cisco Controlle |) >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

Figure 66 Client Summarv

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

| _ | | - | |
|---|--|---|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| cisco | MONITOR WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | неџр | FEEDBACK | |
|--|---------------------------|------------|----------------|------------------|------------|--------------|------|-----------|-----------|
| Monitor Summary Access Points | Clients Current Filter | None | [Change Filter |] [Clear Filter] | | | | | |
| Cisco CleanAir | Client MAC Addr | IP Address | AP Name | | | 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 | | | | | | | | | |

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:

1. Join wireless clients to the multicast streaming video.

Note: Use VLC player to stream and watch video.

- Double click on the VLC icon on your desktop. Click Media > Open Network stream. Choose Protocol = UDP, Address = 229.77.77.28, Port = 1234 in the format udp://@229.77.77.28:1234.
- 3. Click Play.
 - L3_Switch#show ip mroute
 - IP Multicast Routing Table

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

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

- T SPT-bit set, J Join SPT, M MSDP created entry, E Extranet,
- X Proxy Join Timer Running, A Candidate for MSDP Advertisement,
- U URD, I Received Source Specific Host Report,
- Z Multicast Tunnel, z MDT-data group sender,
- Y Joined MDT-data group, y Sending to MDT-data group,
- V RD & Vector, v Vector

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

Timers: Uptime/Expires

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

(*, 239.255.255.250), 4d20h/00:02:47, RP 0.0.0.0, flags: DC Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Vlan56, Forward/Sparse-Dense, 4d19h/stopped

(*, 229.77.77.28), 4d15h/00:02:44, RP 0.0.0.0, flags: DC Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Vlan56, Forward/Sparse-Dense, 00:17:24/stopped

(*, 224.0.1.40), 5d17h/00:02:53, RP 0.0.0.0, flags: DCL Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Vlan56, Forward/Sparse-Dense, 5d17h/stopped

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

Figure 67 FlexConnect VideoStream Clients

| uluilu cisco | MONITOR WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | C <u>O</u> MMANDS | HELP | FEEDBA |
|--|---|---|--|---|---------------------------------|-----------------------|--|-------------------|
| Monitor | Multicast Group | s | | | | | | |
| Summary Access Points Cisco CleanAir Statistics CDP Rogues Redundancy Clients | Layer3 MGID(Mi Group address VI Layer2 MGID(Mi InterfaceName of dynamic57 dynamic58 dynamic58 dynamic58 | ulticast Group I an MGID IGMP/ ulticast Group I vlanId P 57 2 58 2 56 0 | D) Mapping MLD D) Mapping 4GID 22 13 | | | | | |
| Sleeping Clients Multicast Applications Local Profiling | FlexConnect Mu Client-Mac 7c:d1:c3:86:7e:dc 88:cb:87:bd:0c:ab d8:96:95:02:7e:b4 | ticast Media St Stream-Name Media2 Media2 Media2 | ream Clients Multicast-Ip 229.77.77.20 229.77.77.20 229.77.77.20 | Ap-Na Ap-160 AP_160 AP_160 AP_160 | me Vlan 00 0 00 0 00 0 | Tyj Mu Mu Mu | e Iticast Dir Iticast Dir Iticast Dir | ect ect ect |

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

Figure 68 Wireshark Capture Depicting mc2uc

| - | Time | 121000 | Expression | | | | | | |
|-------------------|----------------|---------------------------------|------------------------------|---------------|-----------------|--------------|-------------------|----------------------|---|
| - 1108 1109 | Time | | 1 | a mppy - | ave | | | | |
| 1109 | | Source | Destination | Protocol | Length Info | | | | |
| 88.00 | 12.114292000 | 0.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source nor | tr anc. 2160 | Destination ports | search-agent | |
| 1110 | 12,114450000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | |
| | 12.114646000 | 9.5.56.115 | 229,77.77.28 | MPEG TS | 1358 Source per | t: apc-2100 | Destination port: | search-agent | |
| 1112 | 12.114836000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | _ |
| 1113 | 12,115024000 | DTS 86542.670000000 | PTS 86542.790000000 | MPEG TS | 1358 video-stre | am | | reasonand the second | |
| 1114 | 12.115220000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | |
| 1115 | 12.118880000 | 128 kb/s | 44.1 kHz | MPEG TS | 1358 Audio Laye | 17 2 | | | |
| 1116 | 12.118882000 | DTS 86542.710000000 | PTS 86542.750000000 | MPEG TS | 1358 video-stre | am | | | |
| 1117 | 12.118883000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | |
| 1118 | 12.119460000 | 128 kb/s | 44.1 kHz | MPEG TS | 1358 Audio Laye | r 2 | | | |
| 1119 | 12.119655000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | |
| 1120 | 12.120121000 | 9.5.56.115 | 229.77.77.28 | MPEG TS | 1358 Source por | t: apc-2160 | Destination port: | search-agent | |
| 1121 | 12 120649000 | Q 5 56 115 | 229 77 77 28 | MDEG TS | 1358 Source nor | t+ anr. 2168 | Destination nort: | search-anent | - |
| | | The second states in the second | | man | 1000 Inc. | | | | |
| ame 1 | 111: 1358 byte | s on wire (10854 bits), | .358 bytes captured (10864 b | its) on inter | Tace O | | | | |
| therne | t 11, 5rc: 000 | dway1_51:6a:49 (00:50:66 | 51:6a:49), Dst: Apple_86:7e | :dc (/c:d1:c. | 1:86:/e:dc) | | | | - |
| ner De | tagram Brotoco | 1 Sec Dort: and 2160 /2 | (63) Det Dortt search anant | (1224) | (/ v #351 /) | | | | |
| SO/TEC | 13010.1 DTD-0 | 47 CC-5 | bor, bac Porce search-agene | (1234) | | | | | |
| Duriec | blad in: 1113 | x47 00-3 | | | | | | | |
| SO/TEC | 13818.1 PTD=0 | x47 CC=6 | | | | | | | |
| | | | | ******* | | | | | |
| 0 7c d | il c3 86 7e dc | 00 50 b6 5f 6a 49 08 00 | PjI | | | | | | |
| | | | | | | | | | |

Limitations

The limitations to this feature scope include:

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

Show Commands - Controller

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

| AP Name | Slot | s AP Model | Ethernet MAC | Location | Country | IP Address | Clients | DSE | Location |
|-----------|------|------------------|---------------|----------------|----------------|-----------------|---------|-----|------------|
| | | · | | | | | | | |
| AP1142 | 2 | AIR-LAP1142N-A- | K9 f0:f7:55:f | 1:75:20 defaul | t location IN | 9.5.56 . | 109 | 0 | [0,0,0] |
| AP_2600 | 2 | AIR-CAP2602E-N- | K9 fc:99:47:c | 19:86:90 defau | ult location I | N 9.5.56. | 110 | 0 | [0,0,0] |
| AP3700 | 2 | AIR-CAP3702E-N- | K9 7c:ad:74: | ff:6b:46 defau | It location I | N 9.5.56. | 116 | 0 | [0,0,0] |
| AP_3600-2 | 2 | AIR-CAP3602I-N- | K9 a4:4c:11: | f0:e9:dc defau | ult location | N 9.5.56 | .111 | 0 | [0,0,0] |
| AP_1600 | 2 | AIR-CAP1602I-N-I | <9 6c:20:56: | 13:f6:23 defau | It location I | N 9.5.56. | 105 | 2 | [0, 0, 0] |

(Cisco Controller) >show client summary

Number of Clients..... 2

Number of PMIPV6 Clients...... 0

GLAN/ RLAN/

| MAC Address | AP Name | Slo | t Status | WLAI | N Aut | th Protocol | P | ort Wi | red PN | /IPV6 Role |
|------------------------------|--|-------|-------------|---------|-------|-------------|------------------|---------|--------|------------|
| | | | | | | | | | | |
| 88:cb:87:bd:0c:a | ab AP_1600 | 1 | Associated | 1 1 | Yes | 802.11a | 1 | No | No | Local |
| d8:96:95:02:7e: | o4 AP_1600 | 1 | Associated | d 1 | Yes | 802.11a | 1 | No | No | Local |
| | | | | | | | | | | |
| (Cisco Controller | (Cisco Controller) >show media-stream multicast-direct state | | | | | | | | | |
| Multicast-direct | State | | . enable | | | | | | | |
| Allowed WLANs. | | | 1 | | | | | | | |
| | | | | | | | | | | |
| (Cisco Controller |) >show media- | strea | im group su | ımmaı | У | | | | | |
| Stream Name S | Start IP | | End IP | | | Operat | tion | Statu | s | |
| | | | | | | | | | | |
| Media1 239 | .1.1.1 | | 239.2.2 | .2 | | Mul | ticas | st-dire | ect | |
| Media2 229 | .77.77.28 | | 229.7 | 7.77.2 | 8 | | Multicast-direct | | | |
| | | | | | | | | | | |
| (Cisco Controller |) >show media- | strea | ım group de | etail M | edia2 | 2 | | | | |
| Media Stream Na | ame | | Media2 | | | | | | | |
| Start IP Address. | | | 229.77.77.2 | 28 | | | | | | |
| End IP Address | | | 229.77.77.2 | 28 | | | | | | |
| RRC Parmmeter | s | | | | | | | | | |
| Avg Packet Size | (Bytes) | | 1200 | | | | | | | |
| Expected Bandwidth(Kbps) 500 | | | | | | | | | | |
| Policy Admit | | | | | | | | | | |
| RRC re-evaluation periodic | | | | | | | | | | |
| QoS | | . Vid | eo | | | | | | | |
| Status Multicast-direct | | | | | | | | | | |
| Usage Priority | | 1 | | | | | | | | |
| Violation | | fall | back | | | | | | | |
| | | | | | | | | | | |

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

| Client Mac | Stream Name | Multicast IP | AP-Name | VLAN | Туре |
|------------|-------------|--------------|---------|------|------|

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

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

| Media Stream Name | Media2 |
|--|--------------|
| IP Multicast Destination Address (start) | 229.77.77.28 |
| IP Multicast Destination Address (end) | 229.77.77.28 |

 Client Mac
 Multicast IP
 AP-Name
 VLAN
 Type

 7c:d1:c3:86:7e:dc
 229.77.77.28
 AP_1600
 0
 Multicast Direct

 88:cb:87:bd:0c:ab
 229.77.77.28
 AP_1600
 0
 Multicast Direct

 d8:96:95:02:7e:b4
 229.77.77.28
 AP_1600
 0
 Multicast Direct

Show and Debug Commands - AP

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

AP_1600#show capwap mcast flexconnect clients

```
======
Bridge Group: 1
=======
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

WLAN mc2uc configuration: WLAN ID 1 , Enabled State 1 WLAN ID 2 , Enabled State 0 WLAN ID 3 , Enabled State 0 WLAN ID 4 , Enabled State 0 WLAN ID 5 , Enabled State 0 WLAN ID 6 , Enabled State 0 WLAN ID 7 , Enabled State 0 WLAN ID 8 , Enabled State 0 WLAN ID 9 , Enabled State 0 WLAN ID 9 , Enabled State 0

AP_1600#show capwap mcast flexconnect groups

- WLAN ID 11, Enabled State 0
- WLAN ID 12, Enabled State 0
- WLAN ID 13, Enabled State 0
- WLAN ID 14, Enabled State 0
- WLAN ID 15, Enabled State 0
- WLAN ID 16, Enabled State 0
- Video Group Configuration:
- Group startlp 239.1.1.1 endlp 239.2.2.2
- Group startlp 229.77.77.28 endlp 229.77.77.28

FlexConnect Faster Time to Deploy

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

FlexConnect Plus Bridge Mode

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

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

Figure 69 Conversion to FlexConnect - No Reboot Required

| ONITOR WLANS COM | TROLLER WIRELE | SS SECURITY MA | NAGEMENT C | OMMANDS HEL | P FEEDBACK | Saye Configuration Bing Logout Be |
|------------------------|-----------------------|-------------------|------------------|-----------------|-------------------------|---------------------------------------|
| II APs > Details for A | AP_2600 | | | | | < Back Apply |
| General Credentia | Is Interfaces | High Availability | Inventory | FlexConnect | Advanced | |
| Ieneral | | | Versions | | | |
| AP Name | AP_2600 | | Primary Softw | are Version | 8.0.72.114 | |
| Location | default location | | Backup Softw | are Version | 0.0.0.0 | |
| AP MAC Address | fc:99:47:d9:86:90 | | Predownload ! | Status | None | |
| Base Radio MAC | 54:78:1a:70:04:70 | E. | Predownloade | d Version | None | |
| Admin Status | Enable : | | Predownload I | Next Retry Time | NA | |
| AP Mode | FlexConnect | 2 | Predownload I | Retry Count | NA | |
| AP Sub Mode | local FlexConnect | | Boot Version | | 12.4.25.1 | |
| Operational Status | monitor | | IOS Version | | 15.3(20140203:113124)\$ | |
| Port Number | Sniffer | | Mini IOS Version | | 0.0.0.0 | |
| Venue Group | Bridge Flex+Bridge | | IP Config | | | |
| Venue Type | SE-Connect | | IP Address | | 9.5.56.110 | |
| Venue Name | | | IPv6 Address | | | |
| Language | | | Static IP | | | |

FlexConnect Plus Bridge Mode

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

Application Visibility and Control for FlexConnect

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

AVC has the following components:

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

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

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

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

How AVC Works



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



AVC Facts and Limitations

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

Configuring Application Visibility

To configure the application visibility, perform these steps:

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

| ululu cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT | COMMANDS HELP FEEDBACK |
|-------------------------|--|--|
| WLANS WLANS WLANS | WLANs > Edit 'FlexDemo' General Security QoS Policy-Mapping Advanced Wi-Fi Direct Clients Policy Disabled ‡ Maximum Allowed Clients Per AP Radio 200 Clear HotSpot Configuration Enabled Client user idle timeout(15-100000) Ø 0 Timeout Value (secs) Client user idle threshold (0-10000000) Ø bytes Radius NAI-Realm Off Channel Scanning Defer Scan Defer Priority 0 1 2 3 4 5 6 7 Scan Defer Time(msecs) 100 FlexConnect Enabled FlexConnect Local Enabled Learn Client IP Address \$ Enabled Vian based Central Enabled | 802.11b/g/n (1 - 255) 1 NAC NAC NAC State None Load Balancing and Band Select Image: Client Collect Client Load Balancing Image: Client Collect Passive Client Image: Client Collect Passive Client Image: Client Collect Media Session Snooping Enabled Re-anchor Roamed Voice Clients Enabled KTS based CAC Policy Enabled Radius Client Profiling Image: Client Profiling DHCP Profiling Image: Client Profiling Local Client Profiling Image: Client Profiling |
| | | |

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

| eneral Cred | entials | Interfaces | High Avail | ability | Inventory | FlexConnect | Advanced |
|-------------------|---------|-------------------|--------------|---------|-----------------|------------------|-------------------------|
| neral | | | | | Versions | | |
| AP Name | AP3 | 600 | | | Primary Softw | are Version | 8.1.10.61 |
| Location | defa | ult location | | | Backup Softwa | are Version | 3.0.51.0 |
| AP MAC Address | a4:9 | 93:4c:3e:fb:5a | | | Predownload S | Status | None |
| Base Radio MAC | f4:7 | f4:7f:35:42:cd:70 | | | Predownloade | d Version | None |
| Admin Status | Ena | | | | Predownload N | Next Retry Time | NA |
| AP Mode | Flex | FlexConnect + | | | Predownload R | Retry Count | NA |
| AP Sub Mode | Nor | ne ¢ | | | Boot Version | | 12.4.23.0 |
| Operational Statu | s REG | REG | | | IOS Version | | 15.3(20141113:174201)\$ |
| Port Number | 1 | 1 | | | Mini IOS Versi | on | 0.0.0.0 |
| Venue Group | Uns | pecified | • | | IP Config | | |
| Venue Type | Uns | pecified \$ | | | CAPWAP Prefer | rred Mode | Ipv4 (Global Config) |
| Venue Name | | | | | DHCP Ipv4 Ad | dress | 10.10.10.104 |
| Language | | | | | Static IP (Ipv4 | /Ipv6) | |
| Network Spectrue | n 887 | D32AFE429B737A | FB40B7E24C8F | B19 | | | |
| PS Location | | | | | Time Statistics | | |
| | | | | | UP Time | | 0 d, 00 h 05 m 23 s |
| GPS Present | No | | | | Controller Ass | ociated Time | 0 d, 00 h 00 m 27 s |
| | | | | | Controller Ass | ociation Latency | 0 d, 00 h 04 m 55 s |

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

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

| uluili. cisco | MONITOR WLANS CONTRO | LLER WIRELESS SECURITY MANAG | EMENT COMM | NDS HE | LP FEEDBACK | Saye Configuration Eng Logout Hefresh A Home |
|---|--|---|-----------------------|--------|-------------|---|
| Wireless | FlexConnect AVC Applic | ations 🔨 | | | | Entries 1 - 50 of 1078 |
| Access Points All APs Radios B02.11a/n/ac B02.11b/g/n Dual-Band Badies Global Configuration | Current Filter: Protocol Pack Name: Protocol Pack Version: | (Change Filter) (Clear) Advanced Protocol Pack 8.0 Engine | filter) • Version: | 16 | | M - 7 7 7 7 9 P M |
| Advanced | Application Name | Application Group | Application ID | Engine | Selector | |
| Mesh | 3com-amo3 | other | 538 | 3 | 629 | |
| > ATF | Jcom-tamux | other | 977 | 3 | 106 | |
| RF Profiles | 200 | layer3-over-ip | 788 | 1 | 34 | |
| FlexConnect Groups | 914c/g | net-admin | 1109 | 3 | 211 | |
| RexConnect ACLs | 9pfs | net-admin | 479 | 3 | 564 | |
| Templates | CAlls | business-and-productivity-tools | 1113 | 3 | 216 | |
| OEAP ACLS | Konspire2b | file-sharing | 1190 | 3 | 6085 | |
| Network Lists | MobilitySrx | other | 1386 | 3 | 6997 | |
| ▶ 802.11a/n/ac | ecap | net-admin | 582 | 3 | 674 | |
| > 802.11b/g/n | ecos | other | 939 | 3 | 62 | |
| > Media Stream | accessbuilder | other | 662 | 3 | 888 | |
| Application Visibility | accessnetwork | ather | 607 | 3 | 699 | |
| * And Control | 802 | other | 513 | 3 | 599 | |
| AVC Applications | acrinema | industrial-protocols | 975 | 3 | 104 | |
| FlexConnect AVC | active-directory | net-admin | 1194 | 13 | 473 | |
| Applications FlexConnect AVC Profiles | activesyos | business-and-productivity-tools | 1419 | 13 | 490 | |
| Country | adobe-connect | business-and-productivity-tools | 1441 | 13 | 505 | |
| Timers | acd-512 | other | 963 | 3 | 149 | |
| > Netflow | afpoyerico | business-and-productivity-tools | 1327 | 3 | 548 | |
| 1.005 | strage | net-admin | 609 | 3 | 705 | |
| 1 400 | airplax | voice-and-video | 1483 | 13 | 549 | |

8. Create an AVC profile under Wireless > Application Visibility and Control > FlexConnect AVC Profiles > New with name "Drop_youtube".

| altalta | | | SECURITY | MANAGEMENT | COMMANDS | | FEDRACY | Save Configuration Ping | Logout Befresh |
|--|--------------------------|-----------|----------|------------|----------|------|----------|---------------------------|----------------|
| Wireless | ElexConnect Profile Name | WINESSO S | Tecourt | PERMOLINI | COMPANY | negr | Treparen | | |
| THICIDOS | Plexconnect Prome Rame | | | | | | | 54 | New |
| * Access Points | | | | | | | | | |
| All APs * Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | FlexConnect ProfileName | | | | | | | | |
| Advanced | | | | | | | | | |
| Mesh | | | | | | | | | |
| ▶ ATF | | | | | | | | | |
| RF Profiles | | | | | | | | | |
| FlexConnect Groups PierConnect ACLs PierConnect VLAN Templates | | | | | | | | | |
| OEAP ACLs | | | | | | | | | |
| Network Lists | | | | | | | | | |
| ▶ 802.11a/n/ac | | | | | | | | | |
| ¥ 802.11b/g/n | | | | | | | | | |
| + Media Stream | | | | | | | | | |

9. Click Apply.

| FlexConnect Profile > New | < Back Apply |
|---------------------------|--------------|
| Profile Name Drop_youtube | |
| | |
| | |
| | |
| | |

The AVC profile is created with the new name "Drop_youtube".

| FlexConnect Profile Name | |
|--------------------------|--|
| FlexConnect ProfileName | |
| Drop_youtube | |
| | |
| | |
| | |

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

| Flexconnect Profile > Rule > 'Drop_youtube' | | | | | |
|---|--------------------|--|--|--|--|
| Application Group | voice-and-video \$ | | | | |
| Application Name | youtube ‡ | | | | |
| Action | Drop ‡ | | | | |
| | | | | | |
| | | | | | |

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

| Wireless | FlexConnect Profile | e > Edit 'Drop_youtube' | 1 | | | | |
|--|---------------------|-------------------------|--------|------|-----------|-------------------------------|--------|
| Access Points | Application Name | Application Group Name | Action | DSCP | Direction | Rate Limit (avg) rate)Kbps | /burst |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | voutube | voice-and-video | drop | NA | NA | NA | |
| Advanced | | | | | | | |
| Mesh | | | | | | | |
| ATF | | | | | | | |
| RF Profiles | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | | | | | | | |
| OEAP ACLS | | | | | | | |
| Network Lists | | | | | | | |
| > 802.11a/n/ac | | | | | | | |
| > 802.11b/g/n | | | | | | | |
| Media Stream | | | | | | | |
| Application Visibility And Control AVC Applications AVC Profiles FlexConnect AVC Applications FlexConnect AVC | | | | | | | |

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



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

| FlexConnect Pro | ofile > Edit 'Drop_yout | ube' | | | | Apply | < Back | Add New Rule |
|------------------|---------------------------|--------|------|-----------|------------------------------------|-------|--------|--------------|
| Application Name | Application Group Name | Action | DSCP | Direction | Rate Limit (avg/burst rate)Kbps | | | |
| 3com-amp3 | other | drop | NA | NA | NA | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

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

| lexConnect ProfileName | No of Rules Status |
|------------------------|--------------------|
| Drop_youtube | 1 Applied |
| | |

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

| | MONITOR WLANS CONTROLLER | WIRELESS SECURITY | MANAGEMENT | COMMANDS H | LP FEEDBACK | | Says Configuration | Eing Logout Befresh |
|--|---|---|-------------|------------|-------------------|------------------|--------------------|-----------------------|
| Hirsting Cisco Wireless * Access Points Al An * Radius 002.113/n/ac 802.113/n/ac 802.113/n/ac Advanced Mesh ATF RF Profiles FlexConnect Groups PleaCannect VLAN Templates OEAP ACLs Network Lists # 802.113/n/ac # 802.113/n/ac # 802.113/n/ac | MONITOR WLANS CONTROLLER Flex.Connect Groups > Edit 'Ni General Local Authentication WLAN AVC Mapping WLAN Id Application Visibility Enable Piex AVC Profile Model Addition WLAN Id Application Visibility Addition WLAN Id | WIRELESS SECURITY WIRELESS SECURITY Timage Upgrade 2 3 AVC Profile | ACL Mapping | CQMMANDS H | WLAN VLAN mapping | WLAN AVC mapping | | |
| Application Visibility And Control AVC Applications AVC Profiles FlexConnect AVC | | | | | | | | |

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

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

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

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



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

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

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

| . cisco | MONITOR WLANS O | ONTROLLER WIRELESS | SECURITY MANAGEMENT | COMMANDS HELP | FEEDBACK | 1 | lage Configuration 👔 | Eng Logout Befresh |
|---|---|---|---|---------------|--------------------------------------|-----------------------|----------------------|----------------------|
| CISCO Monitor Summary Access Points Cisco CleanAir Statistics Clients Statistics Clients Steeping Clients Multicast * Applications WLAN | MONITOR WLANS OF FlexConnect > Grou Max Number of Records AVC Statistics C Client MAC Addr Cd:r410f11c.8a:ad | ONTROLLER WIRELESS IPS > Application Stat IIIent IP Address(Tpv4/Tpv6) 10.10.10.109 | SECURITY MANAGEMENT Istics AP Nam AP3600 | | EEEDBACK WLAN Profile FlexDemo | WLAN SSID FlexDemo | < Back | Clear AVC Stats |
| FlexConnect Groups | | | | | | | | |

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

| nitor | ElexConnect > Groups > 0 | lient > Annli | cation Stat | stics | iciti Ggara | and under Eccodede | ē. | | | < Back | Class AVC Eta |
|--------------------------|-------------------------------|---------------|-------------|------------------------|-------------|---------------------------|--------------|------------|----------|--------|---------------|
| | riexconnect - oroups - c | ment - Abbu | cation orac | 13410.5 | | | | | | < DOCK | CHAP AYE STA |
| Summary Access Points | Max Number of Records 10 | 1 | | | | | | | | | |
| Cisco CleanAir | Aggregate Upstream | Downstrea | m | | | | | | | | |
| Statistics | Application Name | Packet Count | Byte Count | Average Packet Size | Usage(%) | Application Name | Packet Count | Byte Count | Usage(%) | | |
| CDP | oposte-services | 3866 | 3.05 MB | 836 | 91.36 | google-services | 3866 | 3.08 MB | 89.98 | | |
| a second | 0 | \$32 | 127.86 KB | 255 | 3.70 | 0 | 593 | 139.13 KB | 3.96 | | |
| cogues | skype | 240 | 54.29 KB | 231 | 1.57 | skype | 240 | 54.29 KB | 1.55 | | |
| lients | ssi | 86 | 40.47 KB | 481 | 1.17 | icloud | 123 | 42.28 KB | 1.20 | | |
| leeping Clients | voutube | 96 | 26.99 KB | 309 | 0.84 | sal | 86 | 40.47 KB | 1.15 | | |
| to this act | Icloud | 56 | 19.66 KB | 359 | 0.57 | youtube | 96 | 28.99 KB | 0.83 | | |
| uncast | yaboo-mail | 49 | 13.75 KB | 287 | 0.40 | facebook | 116 | 16.60 KB | 0.47 | | |
| pplications | dns | 66 | 7.19 KB | 111 | 0.21 | yahoo-mail | 49 | 13.75 KB | 0.39 | | |
| VLAN | facebook | 25 | 3.27 KB | 133 | 0.09 | dns | 116 | 11.99 KB | 0.34 | | |
| Reconnect Groups | icmp | 13 | 3.25 KB | 256 | 0.09 | icmp | 16 | 4.43 KB | 0.13 | | |
| ocal Profiling | Application Last 90 Secs Usag | le(%) | | | | Application Cumulative Us | age(%) | | | | |
| Local Profiling | | | | | | | | | | | |

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

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

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

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

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

Note: If your browser was already open with YouTube, refresh the browser for the AVC profile to take effect.

VLAN Support / Native VLAN on FlexConnect Group

Feature Introduction

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

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

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

VLAN Support/ Native VLAN on FlexConnect Group

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

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



AP Fallback Behavior

With Override Flag Enabled on Secondary Controller

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



With Override Flag Disabled on Secondary Controller

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



Upgrade and Downgrade Considerations

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

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

When downgrading from release 8.1:

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

Configuring VLAN Support / Native VLAN Using Web UI

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

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

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

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

| cisco | | <u>W</u> LANs | | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | â | |
|--|----------|---------------|------------------|---------------|----------|-------------|------------|-------|------------------|-----|-----------------|
| Wireless | FlexConr | nect Gro | ups > Edit 'Ne | ewFlexGro | up' | | | | | | |
| Access Points All APs Radios B02.11a/n/ac | General | Loca | Authentication | Image | Upgrade | ACL Mapping | Central Di | ICP V | WLAN VLAN mappir | g W | LAN AVC mapping |
| 802.11b/g/n Dual-Band Radios Global Configuration | VLAN S | Support | 8 | Native VLAN I | D 10 | | | | | • | |
| Advanced | Overri | de Native | VLAN on AP 🕑 | | | | | | | | |
| Mesh | WLAN | LAN Ma | pping | | | | | | | | |
| ▶ ATF | - | | | | | | | | | | |
| RF Profiles | WLAN | Id 1 | _ | | | | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | Vian I | Add | I | | | | | | | | |
| OEAP ACLS | WLAN I | d | WLAN Profile Nan | ne | Vlan | | | | | | |
| Network Lists | 1 | FlexD | lemo | | 11 | | | | | | |
| ▶ 802.11a/n/ac | | | | | | | | | | | |
| > 802.11b/g/n | | | | | | | | | | | |
| Media Stream | | | | | | | | | | | |

Changes the Inheritance Level at the AP to "Group-specific".

| I APs > D | etails for AP2 | 700 | | | | |
|---|-------------------|-----------------|-------------------|------------|-------------|----------|
| General | Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced |
| VLAN Support Inheritano Level Native VL | Group-Specifi | c N Mappings | Make VLAN AP | Specific ÷ | Go | |
| FlexConne Group Name | ect FlexGroupA | | | | | |
| VLAN Ten | nplate Name | Department-Map | ping | | | |
| PreAuthenti | ication Access Co | ntrol Lists | | | | |

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

| AP Name | | AP2700 | | | |
|------------|------------|-------------------|------|---------|--------------|
| Base Radi | o MAC | f0:7f:06:3d:f1:c0 | | | |
| VLAN VL | AN Mapp | bing | | | |
| Make A | P Specific | ÷ Go | | | |
| WLAN | | | VLAN | | |
| Id | SSID | | ID | NAT-PAT | Inheritance |
| 1 | enjoy | | 57 | no | Group-specit |
| 2 | ciscowlc | | 56 | no | Wlan-specifi |
| 4 | ciscowlc- | peap | 56 | no | Wlan-specifi |
| 5 | ciscowlc- | eaptis | 56 | no | Wlan-specifi |
| | | | | | |
| | | | | | |
| centrally: | switched | Wans | | | |
| WLAN Id | SSID | | VL | AN ID | |
| | | | | | |

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

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

| ululu cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK | |
|----------------|---|--|
| Wireless | All APs > Details for AP3600 General Credentials Interfaces High Availability Inventory FlexConnect Advanced VLAN Support VLAN AP Specific Inheritance AP-Specific Native VLAN ID 20 VLAN Mappings FlexConnect General NewFlexGroup Name VLAN Template Name none VLAN Template Name none | |

VLAN Support / Native VLAN on FlexConnect Group

| All APs > Details for Al | 2700 | | | | | |
|---|-------------------|------------------|------------|-------------|----------|--|
| General Credentials | Interfaces H | igh Availability | Inventory | FlexConnect | Advanced | |
| VLAN Support Inheritance Level Native VLAN ID | LAN Mappings | Make VLAN AP | Specific : | Go | | |
| FlexConnect Group FlexGroup/ Name | | | | | | |
| VLAN Template Name | Department-Mappin | 9 | | | | |
| VLAN Name Id Mappings | | | | | | |
| PreAuthentication Access | Control Lists | | | | | |
| External WebAuthentication | ACLS | | | | | |

| AP Name | А | P2700 | | | | | |
|------------|--------------|------------------|----------|------------|---------|--------------|--|
| Base Radi | io MAC f(| 0:7f:06:3d:f1:c0 | | | | | |
| WLAN VL | AN Mappin | g | | | | | |
| Make A | AP Specific | \$ Go | | | | | |
| | SSID | | | VLAN ID | NAT-PAT | Inheritance | |
| 1 | enjoy | | [| 58 | no | AP-specific | |
| 2 | ciscowlc | | [| 56 | no | Wlan-specifi | |
| 4 | ciscowlc-pea | ар | [| 56 | no | Wlan-specifi | |
| 5 | ciscowlc-eap | otls | [| 56 | no | Wlan-specifi | |
| Centrally | switched W | lans | | | _ | | |
| WLAN Id | SSID | | | VL | ANID | | |
| 3 | enjoy-Web | Auth | | N/4 | 4 | | |
| AP level V | LAN ACL | Mapping | | | | | |
| Vlan Id | Ingre | ess ACL | Egress A | CL | | | |
| | | | | | | | |

Configuring VLAN Support / Native VLAN Using CLI

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

Enable or disable VLAN Support at the FlexConnect Group

FlexConnect Client Troubleshooting

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

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

config flexconnect group <groupName> vlan override-native-ap <enable / disable> To configure the AP-specific configuration, the following CLIs can be used:

- Existing CLI to Configure VLAN Support at FlexConnect AP
- config ap flexconnect vlan <enable/disable> <AP Name>
 Existing CLI to Configure Native VLAN ID at FlexConnect AP
- config ap flexconnect vlan native <vlan-ID>
 New CLI to Remove Native VLAN ID configuration at FlexConnect AP

config ap flexconnect vlan native remove <AP Name>

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

(Cisco Controller) >show flexconnect group detail NewFlexGroup

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

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

(Cisco Controller) > show ap config general AP3600

```
<snip>
Native Vlan Inheritance: ..... AP
FlexConnect Vlan mode :.... I0
    WLAN 1 :.... 11 (Group-Specific)
FlexConnect VLAN ACL Mappings
FlexConnect Group..... NewFlexGroup
Group VLAN ACL Mappings
<snip>
```

FlexConnect Client Troubleshooting

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

Key Enhancements

Ability to track a given client in a branch

FlexConnect Client Troubleshooting

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

Debug per AP

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

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

| (POD6-WLC | <pre>>debug flexconnect client ap POD6-AP3600 ?</pre> |
|------------|--|
| add | Configures the client mac addresses on AP for debug |
| delete | Deletes the client mac addresses on AP |
| ayalog | Configures syslog server for debug logging |
| | |
| (POD6-WLC) | >debug flexconnect client ap POD6-AP3600 add aa:bb:cc:dd:ee:ff |

Debug per FlexConnect Group (FCG)

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

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

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

Enabling Syslog on FlexConnect AP and FlexConnect Group

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

FlexConnect Client Troubleshooting

| Current Directory | C:\Users\Ali\Download | • | Browse |
|-------------------|-----------------------|---------------|---------|
| Server interfaces | 10.10.105.99 | Intel(R) PR 💌 | Show Di |
| Thtp Server Sys | log server Log viewer | | 15 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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

| GLOBAL TFTP DHCP | SYSLO |)G | |
|------------------|-------|----|------|
| • | | | |
| Start Services | | | |
| ✓ TFTP Server | | | |
| TFTP Client | | | |
| SNTP server | | | |
| Syslog Server | | | |
| T DHCP Server | | | |
| DNS Server | | | |
| | | | |
| | | | |

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

Web Links

Syslog Per FlexAP

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

Syslog Per FlexConnect Group

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

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

| lex-AP Client Debugging | enabled | |
|--|----------------------------------|--|
| AP Name | Syslog IP Address | Mac Addresses |
| OD6-AP3600 | 10.10.60.51 | aa:bb:cc:ff:ee:10 aa:bb:cc:dd:ee:ff |
| | | |
| lex-Group Client Debugg | ing enabled | |
| Plex-Group Client Debugg | ing enabled | W \$44 |
| Plex-Group Client Debugg Group Name | ing enabled Syslog IP Address | Mac Addresses |

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

Web Links

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

Terminology

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

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

FAQ

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

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

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

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

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

Q. Can I do web authentication with Local switching?

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

Cisco Support Community - Featured Conversations

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.

| cisco | Discussions Happening Now in The Cisco Support Community | | | | | |
|--------------------------|---|-------------------|--|--|--|--|
| Want to see mo | re? Join us by clicking here | | | | | |
| WLAN desig | n guide for branch office gariup.guido 12 Replies 10 mon | ths, 1 week ago | | | | |
| Flex 7500 st ago | pported RADIUS Servers jburk at pmm-i.com 2 Replies | 9 months, 2 weeks | | | | |
| Cisco Flex 7 | 500 Series Wireless dvaggalis 3 Replies 1 year, 1 month | i ago | | | | |
| ASK THE EX months ago | PERTS:Branch Office Wireless ciscomoderator 25 Rep | ilies 1 year, 5 | | | | |
| HREAP Sca | ability - Clients wirelessdeploy 2 Replies 1 year, 1 month | ago | | | | |
| | Start A New Discussion | Subscribe 🛐 | | | | |

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