FlexConnect Catalyst Wireless Branch Deployment Guide



Table of Contents

Introduction 3

Supported Platforms 3 Supported releases 3 FlexConnect Architecture 4 Wireless Branch Network Design 6 Cisco Catalyst Wireless Config Model 9 Flexconnect VLAN override 50 FlexConnect VLAN Based Central Switching 67 Local Authentication and Backup Radius server 89 CCKM/OKC and PMK Caching 107 Peer to Peer Blocking 107 FlexConnect ACL 109 AP Pre-Image Download 121 FlexConnect Smart AP Image Upgrade 123 Flexconnect Pre-auth ACL and URL filtering 126 Client Association Limit per WLAN/AP 151 Summary 151 Procedure 151 Limitations 152

Fault Tolerance **152** VideoStream for FlexConnect Local Switching **153** Glossary **161**

Introduction

This document describes how to deploy a Cisco FlexConnect wireless branch solution on the Catalyst wireless platform. The Catalyst wireless platform are available in two flavors, the virtual form factor and a hardware appliance

The Virtual form factor can be deployed on any x86 server that supports hypervisor such as - VMware ESXi, KVM etc. To get the list of supported hypervisors and the versions, please refer the deployment guide of the catalyst wireless family. The Virtual form factor can be deployed on prem with an enterprise or can be installed on cloud providers such as AWS.

The Catalyst 9800 Wireless Controller is the hardware appliance for the Catalyst wireless family. Catalyst 9800WC and virtual cloud controller runs on the IOS-XE software base, utilizing the flexibility and modularity available with the platform.

Refer the following documentation on bring up of the catalyst 9800 and cloud based virtual wireless Lan controller.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-

8/b_c9800_wireless_controller_virtual_dg.html

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-

8/b_c9800_wireless_controller_series_web_dg.html The documents covers the features that is supported on the

following platforms and releases.

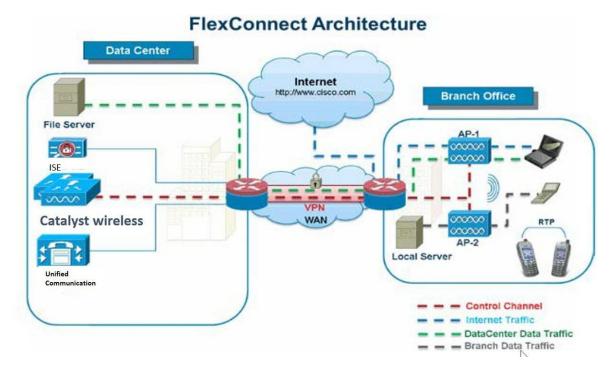
Supported Platforms

Catalyst wireless platforms 11ac Wave 1 and Wave 2 Access Points AP18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

Supported releases

IOS-XE -16.10

FlexConnect Architecture



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.
- Distribute the client data traffic at each Branch Office.

Advantages of Centralizing Access Point Control Traffic

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

Advantages of Distributing Client Data Traffic

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

The Cisco FlexConnect solution also supports Central Client Data Traffic, the table below defines the supported layer 2 and layer 3 security types only for central switched and local switched users.

WLAN L2 Security	Туре	Result		
None	N/A	Allowed		
WPA + WPA2	802.1x	Allowed		
	ССКМ	Allowed	Allowed	
	802.1x + CCKM	Allowed	Allowed	
	PSK	Allowed		
802.1x	WEP	Allowed		
Static WEP	WEP	Allowed		
WEP + 802.1x	WEP	Allowed		

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	WEP	Allowed
Splash Page Web Redirect	WEP	Allowed

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.

FlexConnect Mode	Description
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.

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



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

Feature Matrix

Refer the flexconnect matrix document on the below link to validate the list of supported feature.

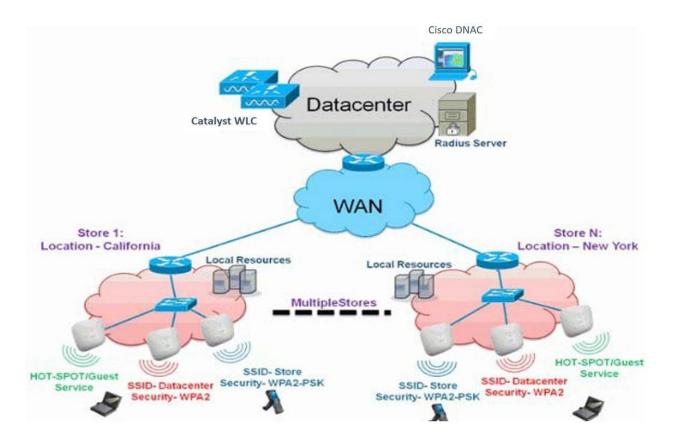
Wireless Branch Network Design

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 the following design requirements.

Primary Design Requirements

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 sq. feet per AP)
- · Central management and troubleshooting

- No operational downtime
- Client-based traffic segmentation
- · Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests



Overview

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

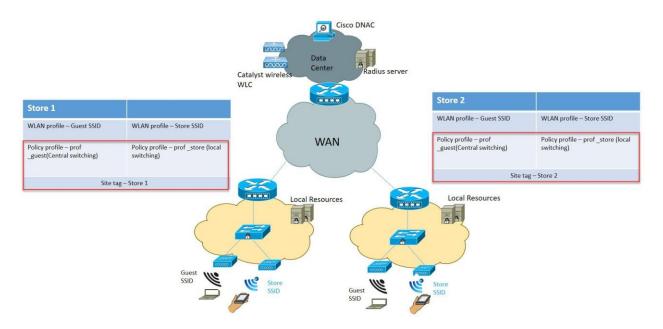
The FlexConnect solution virtualizes the complex security, management, configuration, and troubleshooting operations within the data center and then transparently extends those services to each branch. Deployments using FlexConnect are easier for IT to set up, manage and, most importantly, scale.

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 different policy profiles and site tags per store while maintaining the same WLAN profile as seen in figure below:

Figure 1: Design replication across stores by mapping different site tags and policy tags



Features Addressing Branch Network Design

The rest of the sections in the guide captures feature usage and recommendations to realize the typical branch network design.

Features	Highlights
New config model on catalyst wireless family.	Ability to decouple and modularize the configuration entities. This enables to have the same configuration across different stores by having the same profiles across stores and using a different tags for each store.
Fault Tolerance	Improves the wireless branch resiliency and provides no operational downtime.
Client Limit per WLAN	Limiting total guest clients on branch network.
Auto-convert APs in FlexConnect	Assigning a Site tag which has a flex profile will autoconvert the AP to flexconnect mode without user intervention.
Efficient AP image upgrade	Reduces downtime when upgrading your branch and efficient AP upgrade saves WAN bandwidth and enables a branch AP to upgrade at a much faster pace.
Guest Access	Continue existing Cisco's Guest Access Architecture with FlexConnect by having a central switched SSID which is tunnel to a controller in the DMZ zone.

Features	Highlights
URL ACL	Ability to support use cases of BYOD at the branch
Back up radius server	Provides resiliency at the branch due to WAN outage
AAA override	Provides segmentation and polices per user

Cisco Catalyst Wireless Config Model

This section describes the new config model introduced in the Catalyst wireless platforms.

The new config model goes towards Modularized and Reusable model with Logical decoupling of configuration entities

The model introduces the uses of tags and profiles. The below tables gives an overview of the tags and profile used within the new catalyst wireless products.

Table 3: Tags and Profiles

Tags and Profile	Highlights
WLAN profile	Creation of WLAN with the corresponding security. Addition of AAA entities and configuring the advanced capabilities of the WLAN
Policy profile	Defines the policy of the WLAN such as central /local switching, ACL, VLAN mapping for the WLAN, QOS, AAA policy and export anchor
Policy Tag	Defines the mapping of the WLAN to the Policy profile.
Flex profile	Flex profile defines the WLAN to VLAN mapping, for flex deployment, ACL mapping and radius server configuration.
AP Join profile	Defines the CAPWAP and AP parameters related to join procedures
RF profile /RF tag	RF characteristics of the site mapped to an RF tag
Site Tag	Site tags maps the flex profile and the AP join profile
AP tag	Maps the policy tag, site and RF tag on to the AP

The model follows the design and provision theme.

The design phase involves creating the elements necessary for the wireless networks such as wireless SSID, policy management, RF tagging flex profile etc. The deployment phase is where the designed elements are provisioned on the AP.

Profiles and tags

Profiles represent a set of attributes that are applied to the clients associated to the APs .Profiles are reusable entities which can be used across tags. Profiles (used by Tags) define the properties of the AP or associated clients.

There are different kinds of profiles depending on the characteristic of the entities they define. These profiles are in turn part of a larger construct called a Tag.

A Tag's property is defined by the property of the profiles associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

No two types of Tags include profiles having common properties. This helps eliminate the precedence amongst the configuration entities to a large extent. Every Tag has a default that is created when the system boots up.

WLAN Profile

WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN.

Policy Profile

Policy profile is an entity that constitutes of the all network and switching polices for a client with the exception of QoS which constitute the AP policies as well.

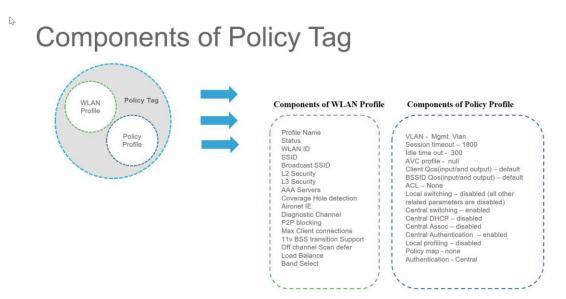
Policy profile is a reusable entity across tags. Anything that is a policy for the client applied on the AP/controller is moved to the policy profile. For example, VLAN, ACL, QOS, Session timeout, Idle timeout, AVC profile, Bonjour profile, Local profiling, Device classification etc.

The WLAN Profile and Policy Profile are both part a Policy Tag and define the characteristics and policy definitions of a set of WLANs. The intent of decoupling the policies from the SSID even though it is a one-to-one mapping, is to give more flexibility to the admin in configuring site based policies(local or remote) while keeping the WLAN definition common.

Policy Tag

Policy tag constitutes the mapping of WLAN Profiles to Policy profiles. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS which constitutes the AP Policy as well as client policy)

A default policy tag with WLAN Profiles with WLAN ID < 16 is mapped to a default policy profile.



AP Join Profile

Following parameters will be part of the AP join profile – CAPWAP IPV4/IPV6, UDP Lite, High availability, Retransmit config parameters, global AP failover, Hyper location config parameters, Telnet/SSH, 11u parameters etc. For AP join profile changes, a small subset requires CAPWAP connection to be reset since these parameters pertain to the characteristic of the AP.

Flex Profile

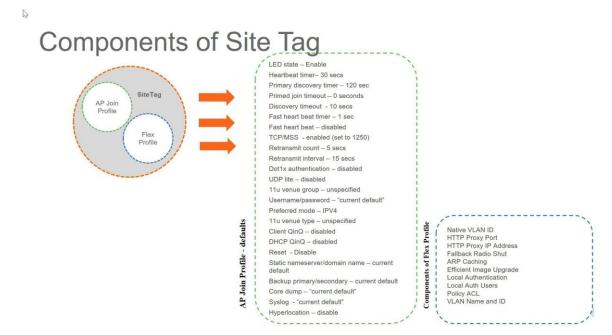
The flex profile contains the remote site specific parameters. For example, the master and slave AP list, the EAP profiles which can be used for the case where AP acts as an authentication server, local radius server information, VLAN-ACL mapping etc. There is no default flex profile, however a custom flex-profile can be added to the default Site Tag.

The AP Join Profile and Flex Profile are both part a Site Tag and define the characteristics of a local or remote site.

Site tag

Site tag constitutes of two profiles, the flex profile and the AP join profile. The site tag defines the properties of a site, both central as well as remote (FlexConnect) site. The attributes of a site that are common across central and remote site are part of the AP Join profile. The attributes that are specific to flex/remote site are part of the flex profile.

Default Site Tag constitutes of the default AP Join profile. There is no default flex profile. The default AP join profile values will be same as that for the global AP parameters today plus few parameters from the AP group in today's configuration like "preferred mode", 802.11u parameters, Location etc.



RF Profile

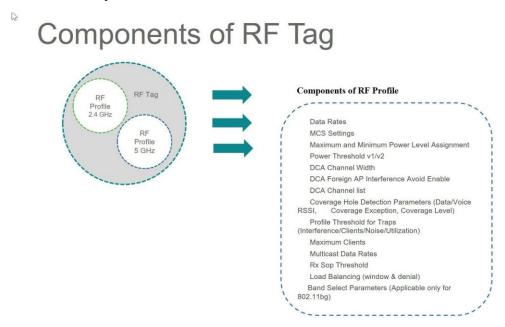
By default, there exists two default RF Profiles (one for 802.11a and one for 802.11b). RF profiles constitute the RF specific configurations such as Data rates, MCS settings, Power assignment, DCA parameters, CHDM variables and HDX features. One 802.11a RF profile and one 802.11b RF profile can be added to an RF Tag.

RF Tag

RF tag constitutes of the 11a and 11b RF profiles Default RF Tag constitutes of the default 802.11a RF profile and the default 802.11b RF Profile.

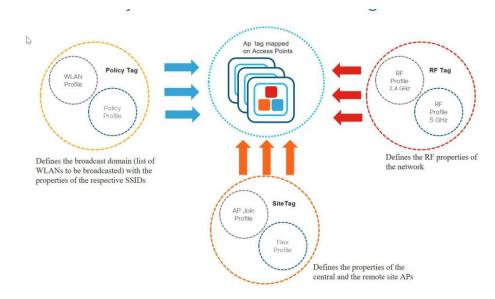
The default 11a RF profile and 11b RF profile contains default values for global RF

Profiles for the respective radios.



AP Tag

Access Points are tagged based on the SSIDs and the associated policies it broadcasts by associating a policy with the AP, the site it belongs to and the RF characteristics desired for that access point by mapping the respective tags. Once tagged, the AP gets a list of WLANs to be broadcasted along with the properties of the respective SSIDs, properties of the local/remote site and the RF properties of the network.



There are three different options for an administrator to accomplish the flow of creating profiles and tags.

- Use of the Basic wireless setup wizard
- Use of advance wireless setup wizard
- Manual configuration

Please refer the controller deployment guide for controller bring up, SVI creation and management GUI access.

The following sections will cover the method and ways a profile and tags can be configured on the catalyst wireless platforms.

An example of a store which has the following deployment model will be used to show case the configuration model.

A store SSID which has a WPA-PSK security enabled, to connect the handhelds used in a store .The SSID would be locally switched SSID

A guest SSID which is centrally switched

An enterprise SSID for employees which has got dot1x enabled and uses radius server for authentication.

SSID	Security	Switching	
Store-SSID	WPA-PSK	Local	
Guest SSID	Web-auth	Central	
Enterprise SSID	Wpa-2/dot1x	Local	

Basic wireless setupwizard

In the basic wireless setup wizard, we will cover the use of creating a store SSID with WP-PSK security.

Procedure

Step1 Click on the wireless setup wizard .



Step2 Select the basic setup wizard from the drop down box and click on "Add".

Cisco Catalyst C9800-CL Wireless Controller	~	Welcome send # The B O B O
Q: Several Meler Name		Windess Setual Select Type + Select Type
Dashboard		Basic Advanced
	No locations available	
🕄 Configuration 🔸		5
Administration		
💥 Troubleshooting		

An Administrator can also start the wizard by navigating to Configuration7wireless setup 7basic

Q Search Menu Items		Ħ	Interface	6	Services
			Logical		AireOS Config Translator
🔚 🖢ashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
🕜 Monitoring	>	品	Layer2		Custom Application
		800	VLAN		IOx
Configuration	>		VTP		Multicast
					NetFlow
(၀) Administration	>		Radio Configurations		Python Sandbox
-			CleanAir		QoS
💥 Troubleshooting	20		High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
			Parameters		Flex
			RRM		Policy
		(tr	Routing Protocols		RF
			OSPF		Tags
		$\widehat{\mathbb{G}}$	Security		WLANs
			AAA		Wireless
			ACL		Access Points
			Advanced EAP		Advanced
			PKI Management		Air Time Fairness
			Local EAP		Fabric
			Local Policy		Media Stream
			TrustSec		Mesh
			Threat Defense		Mobility
			URL Filters		Wireless Setup
			Web Auth		Basic
			Wireless AAA Policy		Advanced
			Wireless Protection Policies		Auvanceu
					s

Step3 Select a name for the remote site, specify the location type as flex for branch deployments.

The native VLAN id refers to the Native vlan id pushed to the AP, the AAA server defines the radius server address pushed to the AP in the branch for local authentication.

To add a new server click on "Add New server" and specify an IP address and a secret key

Basic Wireless Setup: ← Back	store1					R Delete Location	B Apply
General	Wireless Networks AP	Provisioning					
A This Location Type is not	recommended for On-Premise deployment	15		AAA Servers			
Location Name*	store1	0		Available (0)	Selected (0)	_	
Description	store1						
Location Type	🔍 Local 🔹 Flex	2		No AAA servers avallable	No AAA servers selected		
Client Density	Low Typical	High					
Native VLAN ID	3 🚯	Add AAA Server		×	Add New Server		
-		IP Address*	9.1.0.100				
		Кеу*		10			
		Cancel		+ Ada			

Step4 Click on the wireless network to create an SSID along with the policy.

To create a new WLAN click on "define new".

Define the security for the WLAN, for reference an SSID with PSK is created here.

Basic 1	Wireless Setup: store1					
🔶 Bac	k					
	ieneral Wireless Networks	AP Provisioning				
t	Add 🗱 Delete	Add WLAN				×
WL	ANs on this Location	General	Security	Advar	nced	
-	WLAN Name	Profile Name*	store-ssid	Radio Policy	All	
н	 ■ 0 ▶ ▶ 10 • tems per page 	SSID	store-ssid	Broadcast SSID	ENABLED	
WIRI	ELESS NETWORKS	WLAN ID*	5			
+	Add & Delste Enable WLAN	Status				
Numbe	er of WLANs selected : 0					
	Name					
	wichiwa	1				
	wic-mab					
	open_wlan					
	dot1x_wlan	Cancel			🔋 Save & Appl	y to Device

Add WLAN			x
General	Security	Advanced	Â
Layer2	Layer3	ААА	
Layer 2 Security Mode	WPA + WPA2	▼ Fast Transition Adaptive Enabled ▼	l
MAC Filtering		Over the DS	L
Protected Management Frame		Reassociation Timeout 20	
PMF	Disabled	•	
WPA Parameters			L
WPA Policy WPA2 Policy			
WPA2 Encryption	AES(CCMP128) CCMP256 GCMP128 GCMP256		l
Auth Key Mgmt	PSK	·	L
PSK Format	ASCII		
Pre-Shared Key		Ф.	
			Ŧ
Cancel		📔 Save & Apply to Devic	e

Step5 Define the policy for the WLAN.

The VLAN/VLAN group defines the VLAN used by the SSID.

Basic Wireless Setup: store1			
← Back			* Delete Location
General Wireless Networks AP Provisioning + Add x Delete			
WLANs on this Location			
WLAN Name	VLAN/VLAN Group		
i			No items
Wireless Network Details	Policy Details		
WLAN* store-ssid v or <u>Define new</u>	VLAN/VLAN Group*	10	(E.g. 1,2,5-7)
	ACL	Search or Select	or <u>Define new</u>
	QoS	Search or Select	
	OFF Central Switching	ON Central Authentication	1
	OFF Central DHCP	OFF Central Association	
	× ~		<u>क</u> ्त

Step6 Click on the AP provisioning to provision the SSID and policy profile on the selected AP.

Once the AP is provisioned the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, ap would reboot to boot in flex connect mode.

	Add/Select APs		APs on this L	ocation
AP MAC Address		0	Associated AP list Number of selected APs : 0	Q Search
Available AP list Number of selected APs : 3	Q	Search	AP MAC ··· AP Name	🗟 Status 🗟
		3	4 4 0 ▶ ▶ 500 v items per page	No items to display
AP MAC C016.7e83.04e9	< AP Name	×.		
	ap-1-3800 ap-2-3800			
CC16.7e83.c598	ap-1-3700			
		· *		

Step7 Click apply to complete the wizard.

Add/Select APs		APs on this Loo	ation
P MAC Address	0	Associated AP list Number of selected APs : 0	Q. Search
vailable AP list	Q Search	AP MAC - AP Name	- Status -
lumber of selected APs : 0		80e0.1d70.d4f4 ap-1-3700	Joined
AP MAC - AP Name	×	cc16.7e83.c598 ap-2-3800	Joined
4 4 0 ► ► 500 ▼ items per page	No items to display	cc16.7e83.c4ea ap-1-3800	Joined
		i 🛋 1 🕨 🕨 🚺 500 🗸 items per page	1 - 3 of 3 items

Advanced wireless setup wizard

In this section, the advance config wizard is used to create a Guest SSID with web-authentication which would be central switched through a WLC at the datacenter.

Procedure

Step 1	Click on the wireless setup wizard.		
	Cisco Catalyst C9800-CL Wireless Controller		Welcome sand 🛛 🖨 🌾 🖹 🌣 💐 😧 🗍 🗭
	Q. Search Meric terns Basic Wireless Setup		1
	Deshboard + Add		Click on wireless setup wizard
	(2) Monitoring >	No locadore available	
	h Configuration		
	(c) Administration →		
	💥 Troubleshooting		
Step 2	Select the advanced option.		
	Cisco Catalyst C9800-CL Wireless Controller		Welcome sand 🛛 🏘 🍢 🖺
	Q Search Manu Kens Basic Wireless Setup		Wireless Setup Select Type Select Type
	Bashboard + Add		Basic Advanced
	Monitoring >	No locations available	
	v Configuration →		
	Administration		
	🖉 Troubleshooting		

An Administrator can also start the wizard by navigating to Conifguration > wireless setup > advanced.

C Search Menu Items		Logical Ethernet	Services AireOS Config Translator Application Visibility Cloud Services
 Monitoring Configuration Administration Troubleshooting 	 . .	Wireless Layer2 VLAN VTP Radio Configurations CleanAir High Throughput Media Parameters Network Parameters RRM Routing Protocols OSPF Security AAA ACL Advanced EAP PKI Management Local EAP Local Policy TrustSec Threat Defense URL Filters Web Auth Wireless AAA Policy Wireless Protection Policies	Cloud Services Custom Application IOx Multicast NetFlow Python Sandbox QoS RA Throttle Policy Tags & Profiles AP Join Flex Policy RF Tags WLANS Wireless Access Points Advanced Air Time Fairness Fabric Media Stream Mesh Mobility Wireless Setup Basic

Step3 The Advanced config wizard gives an overview of the flow of tag and policies . Click on the "Start Now" button to start the wizard.

This screen allows you to creating Policies and Ta	gs. Once the design to the Access Points DESIGN PHASE Tags & Profiles	N Configuration. It involves is completed, they can be s right here.
creating Policies and Tai deployed WLAN Policy	gs. Once the design to the Access Points DESIGN PHASE Tags & Profiles	is completed, they can be s right here.
	Tags & Profiles	
	Site Policy (Optional)	Radio Policy (Optional)
WLAN Profile	AP Join Profile	RF Profile
Policy Profile	Flex Profile	RF Tag 🛛 🧳
Policy Tag 🛛 🥔	Site Tag 🧳	i l
	DEPLOY PHASE	
Select AF	Apply to APs (Mandatory) Tag APs S and push configur	ation to them
TERMINOLOGY		ACTIONS
Site Policy - AP Profile, S	ite Profile	Go to List View
	Policy Tag Policy Tag Select Al TERMINOLOGY W.AN Policy, Policy Polic Ste Policy - AP Profile, S	Policy Tag Policy Tag Ste Tag DEPLOY PHASE Apply to APs (Mandatory) Tag APs Select APs and push configur TERMINOLOGY Tag WcAI Policy, Policy Police Policy Policy Policy Police Policy Polic

Step4 click on the "+" icon to start creating the WLAN.

Wireless Setup	Wireless Setup Flow Overview							
This screen allows you to design W creating Policies and Tags. Once t deployed to the Acc	he design is c	ompleted, they can be		Start	Tags & Profile	S		
DESIG	N PHASE				-			
Tags	& Profiles			0	WLAN Profile		•	~
	Policy tional)	Radio Policy (Optional)		0	Policy Profile			click on the "+" icor
WLAN Profile AP Join	n Profile	RF Profile		0	Policy Tag	#	-	•
Policy Profile Flex Pri	ofile	RF Tag 🧳		0	AP Join Profile		≡ +	•
Policy Tag 🛷 Site Tag	0 🛷		Start Now 🛶	0	Flex Profile		= +	•
DEPLO	Y PHASE			0	Site Tag	ø	-	•
Appl	ly to APs							
(Ma	ndatory)			0	RF Profile	1	= +	•
Tag AP Select APs and pus		n to them		0	RF Tag	ø	•	•
TERMINOLOGY		ACTIONS			Apply			
Tag WLAN Policy, Policy Profile		Go to List View		0	Tag APs	1		
Site Policy - AP Profile, Site Profile Radio Policy - Radio Characteristics		Dreate New		Done				

Step5 Define the SSID name and security type for the WLAN.

Profile Name* guest_ssid Radio Policy Ali SSID guest_ssid WLAN ID* 1 Status ENABLED ENABLED Status	d WLAN	Security	Advar	aced	
General Security Advanced Layer2 Layer3 AAA yer 2 Security Mode None Over the DS	SSID WLAN ID*	guest_ssid			•
ver 2 Security Mode None AC Filtering	d WLAN General				Save & Apply to Dev
	iyer 2 Security Mode		▼ Fast T • Over t	the DS	

Add WLAN				×
General	Security	1	Advanced	
Layer2	Layer3	1	АДА	
Web Policy			Show Advanced Settings >>>	
Webauth Parameter Map	global	•		
Authentication List	Select a value	•		
For Local Login Method List to make sure the configuration 'a network default local' exists o	aaa authorization			
Cancel			🛛 🗎 Save & Appl	y to Device

Step6 Create a policy profile for the SSID.

Define the policy profile to be central switched and central authentication.

Advanced	Miralana	Catur
✓ Advanced	wireless	Setup

				+ Add X Delete			
	Tags & Profiles			Number of WLANs selected : 0			
a	WLAN Profile			Name	~ II	> ×	SSID
	WEAN FIOTIE			open_wlan	1		open_wlan
0	Policy Profile		+	< < 1 ▶ ▶ 10 ▼	items per page		
0	Policy Tag 🛛 🛷		+				
				click on "+" icon to add a policy			
0	AP Join Profile		+				
400							
1	and the second se	100000					
6	Flex Profile	≣	+				
0	Flex Profile		+				
Ĭ.							
Ĭ.							
0	Site Tag 🛛 🛷		+				

eneral A	ccess Policies	QOS and AVC	Mobility	Advanced
A	Configuring in enabled	state will result in loss of	connectivity for clients assoc	iated with this profile.
Name*	guest_s	ssid	WLAN Switching P	olicy
Description	Enter De	escription	Central Switching	
Status	ENABLED		Central Authenticatio	n 🗹
Passive Client		BLED	Central DHCP	
Encrypted Traffic Ar	nalytics	BLED	Central Association	
CTS Policy			Flex NAT/PAT	
Inline Tagging				
SGACL Enforcemen	t 🔲			
Default SGT	2-6551	9		

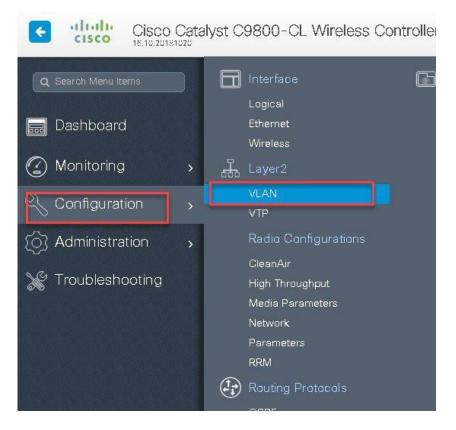
Step7 Define a VLAN for the SSID under the access policies, in the example below the VLAN 10 is mapped on the policy profile.

The Controller also needs a layer 2 VLAN or a layer 3 SVI to be created to centrally switch the traffic from the controller.

General Access Policie	S QOS and AVC	Mobility	Ac	dvanced	
WLAN Local Profiling		WLA	N ACL		
HTTP TLV Caching		IPv4 A	ACL	Search or Select	•
RADIUS Profiling		IPv6 A	ACL	Search or Select	•
DHCP TLV Caching		URL	Filters	<u>.</u>	
Local Subscriber Policy Name	Search or Select	Pre A	uth	Search or Select	×
VLAN		Post /	Auth	Search or Select	
VLAN/VLAN Group	10 🔹				
Multicast VLAN	Enter Multicast VLAN				

In this example we create a layer 2 VLAN on the controller,

Navigate to Configuration > VLAN



VLAN				
SVI VLAN	MLAN Group Create VLAN	_	_	×
+ Add 🛛 🗶 Delete	VLAN ID*	10	add the vian id	
	Name			
1	State			
□ 4 □ 5	RA Throttle Policy	None		
15	IGMP Snooping	DISABLED		
	ARP Broadcast	DISABLED		
	Port Members		Q Search	
		Available (1)	Associated (0)	
		Gi1		<u>^</u>
		click to add the interfac	e	
		Construction Construction in Construction	~	
			No Associated Members	
				•
	Cancel			Apply to Device

Step8 An optional attribute to set is the export anchor configuration, please refer the mobility deployment guide to set up mobility peers.

Add Poli <mark>cy</mark> Pro	file				×
General	Access Policies	QOS and AVC	Mobility	Advanced	
Mobility Anch					
Export Anchor		elect the option for export anchor	5		
Static IP Mobilit	y DISABLED				
	nchors will cause the enabled esult in loss of connectivity for	방법이 잘 해외하는 것이 없는 것을 알았는 것을 알았다. 나라가 이 가슴이 빠지?			
Drag and Drop/do	ouble click/click on the arrov	v to add/remove Anchors			
Available (1)		Selected (0)			
Anchor IP		Anchor IP	Anchor Priority		
9 .1.5.16	→		Anchors not assigne	d	
Cancel	click to add the anchar controller,			Save & Apply	r to Device

Step9 Create a policy tag which binds the SSID and policy profile together.

Start)			+ Add X Delete		
Tags & Profiles			Number of WLANs selected : 0		Advanced Wireless Setup
			Name	× ID × SSID	
WLAN Profile			open_wlan	1 open_wlan	Start
O Policy Profile	1	+	≪ ≪ 1 ► ► 10	▼ items per page	Tags & Pr
0 Policy Tag	•	+			0 WLAN Pro
					Bolicy Pro
O AP Join Profile	I	+			
GFlex Profile		+			G ········ Policy Tag
0 Site Tag		+			AP Join P
O RF Profile		+			Flex Profil
0 RF Tag	P 🔳	+			Site Tag
Apply					RF Profile
	_				GRF Profile
• Tag APs	1				

Step 10 Define a flex profile, the flex profile is used for configuring the VLANs on the AP which is used for the local switched SSID's.

In this example the guest SSID is centrally switched, in cases where there is a mix of central switched and local switched SSID's, an administrator can create a flex profile and define the VLAN's to be used by the local switched SSID's.

Advanced	Wireless	Setup

	Tags & Profiles			Number of WLANs selected : 0			
				Name	v.	ID v	SSID
0	WLAN Profile			open_wlan		1	open_wlan
0	Policy Profile		+	4 4 1 ► ► 10 •] items per page		
0	Policy Tag 🛛 🧳		+				
0	AP Join Profile Flex Profile		+				
Ī			+	click on "+" icon to add a policy			
0	Flex Profile] 🔳	*				

Step11 Define the native VLAN for the flexconnect AP's.

Name*	branch_flex_profile	Multicast Overridden Interface	
Description	Enter Description	Fallback Radio Shut	
Native VLAN ID	2	Flex Resilient	
		ARP Caching	
HTTP Proxy Port	0	Efficient Image Upgrade	
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	
CTS Policy		Join Minimum Latency	
Inline Tagging			
SGACL Enforcement	× 🔲		
CTS Profile Name	default-sxp-profilex		

Step12 Define the VLANS to be used for the local switched SSID.

ieneral Loo	cal Authentication	Palicy ACL	VLAN				
HAdd 🛛 🗶							
VLAN Name	V ID V ACL	Name	× <				
< 0 n	▶ 10 ¥ items	per page		VLAN Name*	10		
		No items to) display	VLAN Id*	10		
				ACL Name	Select ACL	•	
				🖌 Save		🔊 Cancel	8
			0				0

Step 13

Define a site tag which binds the Flex profile and a default AP join profile. To add a flex profile on a site tag, uncheck the "enable local site" option.

			×	+ Add x Delete			
Start							
	Tags & Profiles			Number of WLANs selected : 0			
		1.		Name	×.	ID 🗸	SSID
0	WLAN Profile			open_wlan		1	open_wlan
0	Policy Profile		+	I I I I I	 Items per page 		
6	Policy Tag 🛛 🤞	,	+				
	2 I I I I I I I I I I I I I I I I I I I						
		-					
6	AP Join Profile		+				
0	Flex Profile		+				
Ĭ							
0 0	Flex Profile		+				
Ĭ							
Ĭ			+	click on "+" icon			
0	Site Tag 🔹		+	click on "+" icon to add a policy			

tart	+ Add x Dele		
Tags & Profiles	Site Tag Name		- Description
	Add Site Tag		
0 WLAN Profile	Name*	site_tag	
0 Policy Profile 🔳 4			
	Description	Enter Description	
🛚 Policy Tag 🛛 🖉 📕	AP Join Profile	default-ap-profile 🔻	
0 AP Jain Prañie	Flex Profile	branch_flex_profile	
0 Fiex Profile	Control Plane Name		
gSte Tag 🗳	Enable Local Site		

Step14 The final stage is to provision the policy, site and RF tag on the AP.

Click on Tag APs to select the profiles and have it configured for the AP.

In this example the AP is tagged using a default RF tag.

Once the AP is provisioned with the site tag, the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, AP would reboot to boot in flex connect mode.

The assigning of tag does the auto conversion of the AP mode based on properties of the tag.

ced Wireless Setup	*		3			
Start		+ Tag APs				
Tags & Profiles		Imber of APs: 3 elected Number of APs: 3	Tag APs			×
0 ······ WLAN Profile	•	AP × AP Model	Tags			Pr Fa
O Policy Profile	+ 5	AIR-AP380		2		27
6 Policy Tag 🛷 🏢	•	AIR-AP380	Policy	store_policy		ər
		D 1-3700 AIR-CAP37	Site	site_tag		or
O AP Join Profile	•	1 1 10	RF	default-rf-tag	v6	
Flex Profile			Changing AP	Tag(s) will cause assoc	iated AP(s) to reconnect	
0 Site Tag 🖌 📕	•		Cancel		Save & Apply to Device	
GRF Profile	+					
0 RF Tag 🗳 📕						
Apply						
6 Tag APs 🚺						
Done						

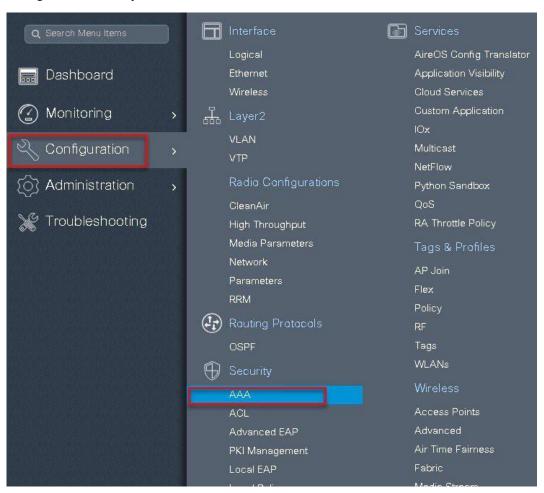
Manual Configuration

The manual configuration for creating the SSID /tags and profiles is done using the WLC GUI, in this section we will cover creating an enterprise SSID with dot1x enabled.

The first step in creating an enterprise SSID with dot1x is to define the AAA server for authentication.

Procedure

Step1 Define an AAA server and method list for dot1x which is mapped to the WLAN. The AAA server is created by navigating to the following:



Configuration > security > AAA

Step2 Use the AAA wizard to create the server and server groups.

Cisco Cata	alyst C9800-CL Wireless	Controller		
Q. Search Menu Items Dashboard Monitoring	Authentication Authoriza	tion and Accounting Servers / Groups AAA Advance	d	
Configuration >	General Authentication	Local Authentication	Default • Default •	
💥 Troubleshooting	Authorization Accounting	Radius Server Load Balance Show Advanced Settings >>>	DISABLED	

Step 3

B Define a name for the server and specify the IP address and shared secret.

Add Wizard			×
			Basic O Advanced
	SERVER	SERVER GROUP ASSOCIATION	МАР ААА
RADIUS 🔽	TACACS+ 🗌 LDA	AP	
RADIUS			
Name*	ISE		
IPv4 / IPv6 Server Address*	9.1.0.20		
PAC Key			
Key*			
Confirm Key*			
Cancel			Next 🗲

Step4

Create a server group and map the server in the group.

Add Wizard		×
		Basic Advanced Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
RADIUS		
Name*	ISE	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none	
Dead-Time (mins)	1-1440	
Available Servers	Assigned Servers	
freerad ISE-2 ISE	> ISE *	
← Previous		Next 🗲

Step 5

Enable dot1x system control and check mark the authentication and Authorization profile.

Add Wizard	-	×
		Basic Advanced
Ø	⊘	•
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authenticati	ion 🗌 Authorization 🗌 Accounting 🔲	
General		
aaa_dot1x_system_auth_control	ENABLED	
Local Authentication	Default	
Local Authorization	Default	
Radius Server Load Balance	DISABLED	
Show Advanced Settings >>>		
← Previous		🖺 Save & Apply to Device

Step6 Check mark the authentication list and define the method type as Dot1x and map the server group.

Add Wizard		×
		Basic O Advanced
<u>√</u> k		
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authentication		
General Authentication Au	thorization	
Method List Name*	dot1x	
Type*	dot1x 🔹	
Group Type	group	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap tacacs+ rad-group freerad radgrp_branch *	S ISE	
← Previous		冒 Save & Apply to Device

Step7

Check mark the authorization list and define the method type as network and map the server group.

Add Wizard			
			🖲 Basic 🛛 🔿 Adva
SERVER	SERVER	GROUP ASSOCIATION	мар ада
General 📝 Authenti	ation 🗹 Authorization 🗸	Accounting	
General Authentication	Authorization		
Method List Name*	authz		
Туре*	network		
Group Type	group 🔻		
Fallback to local			
Available Server Groups	Assigned Se	erver Groups	
Idap * tacacs+ rad-group freerad radgrp_branch *	> ISE	*	
	A		
			📔 Save & Apply to Devi

Step8 Create a Dot1x WLAN and map the method list on the WLAN. Navigate to the ConfigurationTags & profiles > WLAN to create the SSID.

Q Search Menu Items			Interface	G	Services
			Logical		AireOS Config Tran
📻 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
Monitoring	5	品	Layer2		Custom Application
<u> </u>		000	VLAN		IOx
🔾 Configuration	>		VTP		Multicast
	915 T				NetFlow
(O) Administration	>		Radio Configurations		Python Sandbox
ing this share share this			CleanAir		QoS
K Troubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
			Parameters		Flex
			RRM		Policy
			Routing Protocols		RF
			OSPF		Tags
					WLANs
		(4)	Security		WHERE AN AS

WIRELESS NETWORKS					
+ Add X Delete Er					
Number of WLANs selected : 0					
Name	Add WLAN				×
open_wlan	General	Security	Adva	anced	
	Profile Name*	dot1x_wlan	Radio Policy	All	
⊳	SSID	dot1x_wlan	Broadcast SSID		
-77 -	WLAN ID*	2			
	Status				
	L				
	Cancel			冒 Save & Apply t	to Device

Step9 Define the security for the WLAN.

Add WLAN			×
General 🔓	Security	Advanced	Â
Layer2	Layer3	AAA	-1
Layer 2 Security Mode	WPA + WPA2 🔹	Fast Transition Adaptive Enabled 🗸	
MAC Filtering		Over the DS	
Protected Management Frame		Reassociation Timeout 20	
PMF	Disabled v		
WPA Parameters			
WPA Policy			•
Cancel		🛛 📔 Save & Apply to Dev	ce

Add WLAN			×
General	Security	Advanced	
Layer2	Layer3	AAA	
Authentication List	dot1x	•	
Local EAP Authentication			
Cancel			冒 Save & Apply to Device

Step10 Create a policy profile which defines switching capability of the WLAN and the interface mapping to the WLAN.

Image: Section of Section (Section	Q Search Menu Items	Logical	Services AireOS Config Translator
Configuration IOX Administration Radio Configurations Troubleshooting Radio Configurations Python Sandbox Index In	詞 Dashboard	Ethernet	Application Visibility
Image: WIP NetFlow Image: Administration Radio Configurations Python Sandbox Image: Troubleshooting CleanAir QoS Image: Troubleshooting High Throughput RA Throttle Policy Image: Media Parameters Tags & Profiles Network AP Join Parameters Flex RRM Policy Image: OSPF Tags Image: OSPF MediaNas Image: OSPF </td <td><u> </u></td> <td></td> <td>lOx</td>	<u> </u>		lOx
		Radio Configurations	Python Sandbox
OSPF Tags WLANs WICHNS Wireless	₩ Troubleshooting	High Throughput Media Parameters Network Parameters	RA Throttle Policy Tags & Profiles AP Join Flex
Advanced EAP Advanced PKI Management Air Time Fairness Local EAP Fabric		OSPF Security AAA ACL Advanced EAP PKI Management	RF Tags WLANs Wireless Access Points Advanced Air Time Fairness

Policy Profile				
+ Add R Delete				
	ld Poli cy Profile			×
Policy Profile Name open_wian	General Access Po	licies QOS and AVC	Mobility	Advanced
default-policy-profile	A Configurin	g in enabled state will result in loss of con	nectivity for clients assoc	lated with this profile.
	Name*	dot1x_wlan	WLAN Switching P	Policy
	Description	Enter Description	Central Switching	
	Status		Central Authenticatio	n 🗹
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	S Cancel			🛱 Save & Apply to Device

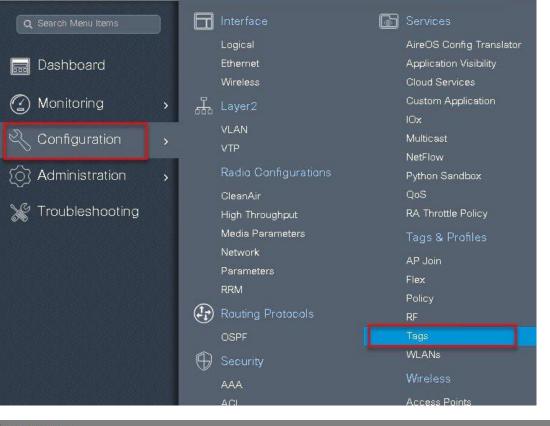
Step11 Define the VLAN to be used by the SSID.

General	Access Policies	QOS and AVC	Mobility	Ad	lvanced	
WLAN Local P	rofiling		WLA	N ACL		
HTTP TLV Cach	ing		IPv4 A	ACL	Search or Select	•
ADIUS Profilin	g		IPv6 A	ACL	Search or Select	•
HCP TLV Cacl	ning		URL	Filters		
ocal Subscribe.	er Policy Name	Search or Select 🔻	Pre A	uth	Search or Select	•
/LAN			rie A	aun		Ŀ
/LAN/VLAN Gr	oup	11	Post A	Auth	Search or Select	•
Aulticast VLAN		Enter Multicast VLAN	1			

Access Po	olicies	QOS and AVC	Mobility	Advanced
			Fabric Profile	Search or Select 💌
sec)	1800		Umbrella Parameter Map	Not Configured
	300		WLAN Flex Policy	
tes)	0		VLAN Central Switch	ning
imeout 🛛 📝	60		Split MAC ACL	Search or Select
			Air Time Faimess	Policies
			2.4 GHz Policy	Search or Select
ddress	0.0.0.0		5 GHz Policy	Search or Select 👻
de				
	default-aa	a-policy		
	Search or	Select		
	(sec)) tes)	tes) 0 imeout ♥ 60 wddress 0.0.0.0	(sec) 1800 300 tes) 0 imeout \bigcirc 60 address 0.0.0.0	(sec) 1800 (sec) 1800 300 Umbrella Parameter Map 300 WLAN Flex Policy tes) 0 VLAN Central Switch imeout 60 Split MAC ACL Air Time Faimess 2.4 GHz Policy address 0.0.0 5 GHz Policy

Step 12 Create a policy tag which bundles the policy profile and WLAN profile together.

Navigate to configuration > Tag and create a policy tag mapping the WLAN and policy profile.



Manage Tag:	5					
Policy	Site	RF	AP			
		Add Policy Tag				×
+ Add	X Delete	Name*	branch_policy			
Policy	Tag Name	Description	Enter Description			
branc		+ Add 🛛 🗶 De				
	t-policy-tag					
ia a 1	F H 10	WLAN Profile	~	Policy Profile		~
		2 < 0 > >	10 🔻 items per page		No items to a	display
		Map WLAN and Po	licy			
		WLAN Profile*	dot1x_wlan 🗸 🕄	Policy Profile*	dot1x_wlan 🗸	
		-	×	~		-
		Cancel			Save & Apply to D	evic 4

Step 13Create a flex profile that defines the flex AP properties.To create a flex profile navigate to Configuration > Tags and Profile >flex.

Image: Dashboard Ethernet Application Visibility Image: Omega: Dashboard Wireless Cloud Services Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Omega: Dashboard Image: Dashboard Image: Dashboard Cloud Services Image: Omega: Dashboard Image: Dashboard Image: Dashboard Cloud Services Image: Omega: Dashboard Image: Dashboard Image: Dashboard Cloud Services Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Omega: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image: Dashboard Image:		1			
Image: Dashboard Ethernet Application Visib Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring Image: Omnitoring I	Q Search Menu Items			Interface	Services
Image: Wireless Cloud Services Image: Wireless Cloud Services Image: Wireless Custom Application Image: Configuration Image: Wireless Image: Configuration VLAN Image: Configuration VLAN Image: Configuration Radio Configurations Image: Configuration Radio Configurations <t< th=""><th>an na shingi shingi shingi shingi shingi sh Ta ka sa ka saka saka</th><th></th><th></th><th>Logical</th><th>AireOS Config Tr</th></t<>	an na shingi shingi shingi shingi shingi sh Ta ka sa ka saka saka			Logical	AireOS Config Tr
Image: Wireless Cloud Services Image: Wireless Cloud Services Image: Wireless Custom Application Image: Configuration Image: Wireless Image: Configuration VLAN Image: Configuration Radio Configurations	ashboard			Ethernet	Application Visibi
Configuration Configuration Administration CleanAir Froubleshooting Froublesho				Wireless	Cloud Services
Configuration VLAN Configuration VLAN Administration Radio Configurations Troubleshooting High Throughput High Throughput RA Throttle Polici Media Parameters Tags & Profiles Network AP Join Parameters Flex RRM Policy OSPF Tags OSPF Tags Security AAA ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness	(C) Monitoring	>	Д.	Laver2	Custom Applicati
✓ Configuration ∨TP Multicast ✓ Administration ✓ Radio Configurations Python Sandbox ✓ Troubleshooting CleanAir QoS ✓ High Throughput RA Throttle Policy Metwork AP Join Parameters Flex RRM Policy ØSFF Tags OSFF Tags Security AAA ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness			000		IOx
Image: Administration Radio Configurations Python Sandbox Image: Troubleshooting CleanAir QoS Image: Troubleshooting High Throughput RA Throttle Policy Media Parameters Tags & Profiles Network AP Join Parameters Flex RRM Policy Image: Policy OSPF Image: OSPF Tags Image: OSPF Tags Image: Addition of the policy AAA Image: Addition of the policy Image: Policy Image: Addition of the policy Image: Policy Image: Policy RRM Policy Image: Policy OSPF Tags Image: Policy AAA Wireless Image: Policy AAA Accl Image: Policy AAA Accl Image: Policy Advanced EAP Advanced Image: PKI Management Air Time Fairness	Configuration	5			Multicast
CleanAir QoS High Throughput RA Throttle Polic Media Parameters Tags & Profiles Network AP Join Parameters Flex RRM Policy Routing Protocols RF OSPF Tags Security AAA ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness		ada ti		VIP	NetFlow
Image: Security High Throughput RA Throttle Policy Media Parameters Tags & Profiles Network AP Join Parameters Flex RRM Policy OSPF Tags Security WLANs AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness	(O) Administration	>		Radio Configurations	Python Sandbox
Media Parameters Tags & Profilest Network AP Join Parameters Flex RRM Policy OSPF Tags Security WLANs AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness				CleanAir	QoS
Network AP Join Parameters Flex RRM Policy Routing Protocols RF OSPF Tags VLANs VLANs Security AAA ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness	💥 Troubleshooting			High Throughput	RA Throttle Policy
Network AP Join Parameters Flex RRM Policy OSPF Tags OSPF Tags WLANs Wireless AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness				Media Parameters	Tags & Profiles
Parameters Flex RRM Policy Policy Policy Policy Security VLANs VLANs Vireless AAA ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness	The Section Section			Network	5
RRM Policy Routing Protocols RF OSPF Tags VLANs VLANs AAA Vireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness	san al anter anter anter anter anter a			Parameters	
Reprotocols RF OSPF Tags Tags WLANs Security Wireless AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness				RRM	
WLANs AAA ACL Advanced EAP Advanced PKI Management				Routing Protocols	07 (0000 1 99)
Security Wireless AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Air Time Fairness				OSPF	Tags
AAA ACL Advanced EAP Advanced EAP Advanced Advanced Advanced Advanced Advanced Advanced			\oplus	Security	WLANs
Advanced EAP Advanced PKI Management Air Time Fairness				AAA	Wireless
PKI Management Air Time Fairnes				ACL	Access Points
The management				Advanced EAP	Advanced
Local EAP Fabric	san ad san ad san ad san ad san ad sa	N.		PKI Management	Air Time Fairness
				Local EAP	Fabric

Step 14 Define the native VLAN for the Flexconnect AP.

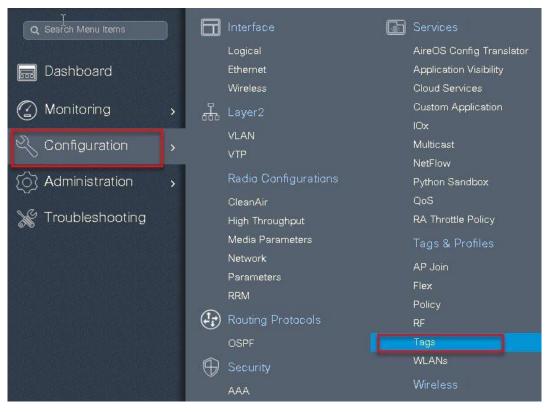
Flex Profile N			- Descriptio	on
default-flex-p	Add Flex Profile			
< 1 ▶ 3	General Local	Authentication Policy ACL	VLAN	
	Name*	branch_flex_profile	Multicast Overridden Interface	
	Description	Enter Description	Fallback Radio Shut	
	Native VLAN ID	3	Flex Resilient	
	HTTP Proxy Port	0	ARP Caching	
			Efficient Image Upgrade	
	HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	
	CTS Policy		Join Minimum Latency	
	Inline Tagging			
	SGACL Enforcement			
	CTS Profile Name	default-sxp-profilex		

Step 15 Define the VLANS to be used for local switched SSID, in this example we use VLAN 11 which is local switched VLAN from the AP.

d Flex Profile	ter in the second s		
General Local Authentication Policy ACL	'LAN		
+ Add Stelete			
VLAN Name 🗸 ID 🧭 ACL Name	≪ ◀		
🖌 🚽 0 🕨 📕 🛛 10 🔻 items per page	VLAN Name*	11	
No items to disp	VLAN Id*	11	
	ACL Name	Select ACL	
	🖌 🖌 Save	D Cancel	
	1		
D Cancel		📕 🗎 Save & /	Apply to Device

Step16 Create a site tag that maps the flex and RF profile.

To create a site tag navigate to Configuration > Tags and Profile > Tags.



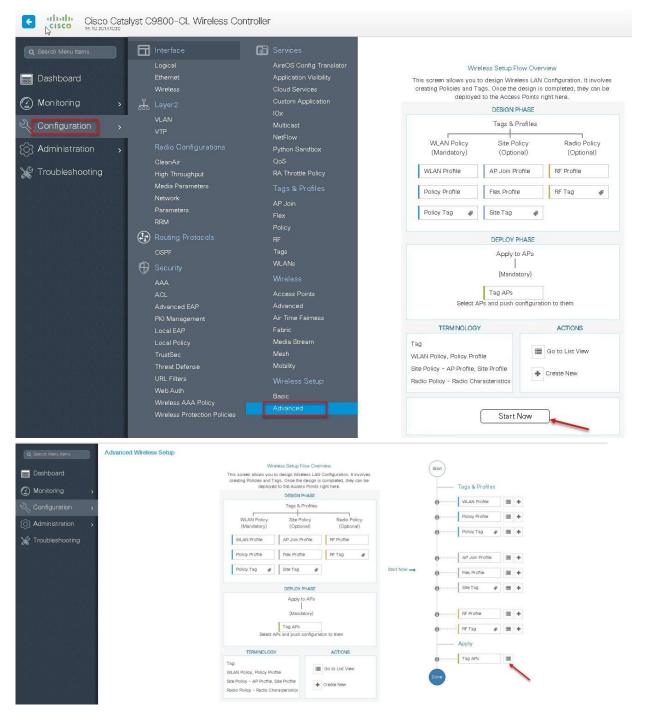
Step 17 Uncheck "enable local site" to map the flex profile on the site tag.

lanage Tags			
Policy	Site RF	AP	
+ Add X D	Add Site Tag		×
Site Tag Name	Name*	site_tag	
SS	Description	Enter Description	1
branch	AP Join Profile	default-ap-profile	
default-site-tag	Flex Profile 3	branch_flex_profile	
(4 4 1 > >)	Control Plane Name	· · · · · · ·	
	Enable Local Site 2		
	Cancel		🖹 Save & Apply to De 4

Step18 Map the policy site tag and RF tag on the AP. To tag the AP an Administrator can use the following options.

- Use the advanced config wizard
- Use a Static mapping
- Use a filter

Using the Advanced config wizard to tag the AP's Navigate to Configuration > wireless setup > Advanced



2 Search Menu Items	Advanced Wirel	ess Setup															Bac
Dashboard	Start	Tags & Profiles		Nur	+ Tag APs aber of APs: 3 icted Number of	APs: 3											
Configuration	0	WLAN Profile	=	+	AP Nome	AP Model	AP MAC -	AP - Mode	Admin Status	 Operation Status 	Policy -	Site - Tag		Location ~	Country	Hyperiocation Method	0
Administration	0	Policy Profile	=	+	sand-ewic- ap-1	AIR-AP3802I-B- K9	0081.c4s0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	us	Local	
Troubleshooting	0	Policy Tag 🛷	=	+ 2	sand-ewic- ap-2	AJR-AP3802I-8- K9	0081.c4a0.7550	Flex.	Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	us	Local	
Troubleshooting				2	sand-3700	AIR-CAP3702I- A-K9	80e0.1d7b.8610	Flex.	Enabled	Registered	sand-policy	sand-site	ciefault-rf- tag	default location	US	Local	
	0	AP Join Profile	=	+	- 1 F	10 👻 items p	ier poge									1 - 3 of 3 items	
	0	Fiex Profile		+													
	0	Site Tag 🛛 🛷		+													
	0	RF Profile		+													
	0	RF Tag 🛷	=	+													
		Apply															
	0	Tag APs															

Advanced Wireless	s Setup gs & Profiles.	*	Numt	Tag AF ber of APs	: 3	APs: 3							
0	VLAN Profile			AP Name	×.	AP Model	¥.	AP MAC	AP Mode	×	Admin Status	×	Op Sta
Ø F	Policy Profile			ap1-38		AIR-AP3802I-I K9	3	0081.c4a0.6fe0	Flex		Enabled		Re
0 [F	Policy Tag 🛛 🥔			ap2-3	Tag	APs							×
				ap1-3	Ta	gs				_			
0 A	AP Join Profile	≡ +	14	4 1	Po	licy	branc	h-policy	•				
0	lex Profile	=+			Sit	e	site_t	ag	•	L			
0 8	Site Tag 🛷				RF		defau	lt-rf-tag	•	L			
0 F	& Profile	≡ +			Ch	anging AP Tag(s	:) will	cause associated	l AP(s) to n	econn	ect		
0 F	FTag 🥔	= +			5	Cancel			₿ Save:	& Ap	ply to Dev	ice	

Using a static mapping to tag the AP's.

Dashboard	Policy	Site R		
Monitoring >	Priority	Tag Source	Filter	
, Administration 🔹 🔉	0	Static		
Troubleshooting	1	Location	Ø	
	2	Filter		
	з	AP		

Static Mapping – In the static mapping, the administrator need to specify the mac address of the AP along with the site, policy and RF tag.

Q Search Menu Items	Manage Tags				
🚃 Dashboard	Palicy	Site RF	AP		
Monitoring	Tag Source	Static	Filter		
Configuration	+ Add ×	Pelete			
() Administration	AP MAC Addre	165	 Policy Tag N 	lame	Site Tag Name
💥 Troubleshooting		10 🔻 items per j	page		
Associate Tags to	AP 1122.3344.5566		add the mac a	address of	×
Policy Tag Name	branch-policy	•	the AP	audress 01	
Site Tag Name	site_tag	•			
RF Tag Name	default-rf-tag	•			
Cancel				📔 Save	& Apply to Device

age Tags				
Policy Site RF	AP			
Tag Source Static	Filter			
+ Add × Delete				
AP MAC Address	Policy Tag Name	✓ Site Tag Name	🖂 RF Tag Name	
1122.3344.5566	branch-policy	site_tag	default-rf-tag	

Using a Filter to tag the AP

Gesich Menu benis Manago Tags Dashboard Policy Site RF AP			
) Monitoring > Teg Source Static Filter			
3 Administration > Priority < Rule Name < AP name regex	 Policy Tag Name 	 Site Tag Name 	 RF Tag Name
Troubleshooting			No items to disp
Associate Tags to AP			×
Rule Name* rule_1	Policy Tag Name	branch-policy 🗙 🔻	
AP name regex ap*	Site Tag Name	site_tag × ·	
Active YES	RF Tag Name	default- <u>rf</u> -tag × •	
Priority* 0-127			
Cancel		📔 Save & App	ly to Device
anage Tags			
Policy Site RF AP			
Tag Source Static Filter			
+ Add x Delete			
Priority V Rule Name V AP name regex	 Policy Tag Name 	 Site Tag Name 	RF Tag Name
1 rule_1 ap*	branch-policy	site_tag	default-rf-tag

The Access point summary page show the source based on which the tags was assigned to an AP.

Access Points											
V All Acces	ss Points										
Number of AP(s):	3										
							-			-	1
AP Name 🗸	Total Slots	AP Model ~	Base Radio MAC	AP Mode	Admin	Operation Status	- Policy Tag	Site Tag	× RF Tag ×	Tag Source	< Location
ap-1-3800	3	AIR-AP3802I-8-K9	0081.c4a0.6fe0	Flex	Enabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location
ap-2-3800	3	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location
ap-1-3700	2	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Disabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location
ia a 1	► 10 • Its	ems per nade					L				1 - 3 of 3 ac

Once the AP is provisioned with the site tag, the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, AP would reboot to boot in flex connect mode.

The assigning of tag does the auto conversion of the AP mode based on properties of the tag.

Flexconnect VLAN override

AAA override of VLAN on individual WLAN is supported for local switching. In order to have dynamic VLAN assignment, AP would have the VLAN pre-created based on a configuration using the flex profile mapped to the site tag. The VLAN's used in the flex profile is pushed to the AP and overriding of the WLAN is done using the VLAN the AP is programmed to.

Summary

- AAA VLAN override is supported on WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on the policy profile mapped to the WLAN.
- The FlexConnect AP should have VLAN pre-created from WLC, this is done in the flex profile mapped to the site tag.
- If VLANs returned by AAA override are not present on AP, client will be excluded and not allowed access to the network.
- Multicast traffic on a AAA overridden VLAN is not supported

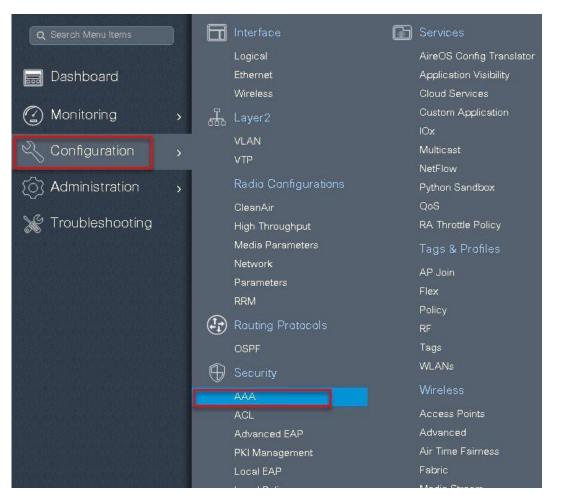
Procedure to Enable VLAN

The procedure to enable VLAN override is outlined below along with the GUI configuration. The WLAN here is enabled for dot1x based authentication.

Procedure

Step1 Define a AAA server and method list for dot1x which is mapped to the WLAN. The AAA server is created by navigating to the following:

Configuration > security > AAA



Step 2

Use the AAA wizard to create the server and server groups.

Cisco Cata	lyst C9800-CL Wireless C	ontroller	
Q Search Menu Items Dashboard Monitoring	Authentication Authorization + AAA Wizard AAA Method List	Servers / Groups AAA Advanced	
Configuration > Administration > Troubleshooting	General Authentication Authorization Accounting	Local Authentication Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default Default DiSABLED

Step3 Define a name for the server and specify the IP address and shared secret.

Add Wizard					×
				Basic	O Advanced
	SERVER		SERVER GROUP ASSOCIATION	MAP AAA	
RADIUS 🔽	TACACS+	LDAP			
RADIUS					
Name*	ISE				
IPv4 / IPv6 Server Address*	9.1.0.20				
PAC Key					
Key*					
Confirm Key*					
Cancel					Next 🗲

Step4 Create a server group and map the server in the group.

		🖲 Basic 🛛 Advance
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
RADIUS		
Name*	ISE	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none 🔻	
Dead-Time (mins)	1-1440	
vailable Servers	Assigned Servers	
freerad SE-2 ISE	S ISE	
← Previous		Next 🗲

Step5 Enable dot1x system control and check mark the authentication and Authorization profile.

SER. Authorization	/ER GROUP ASSOCIATION		Basie MAP AAA	c Advanced
			МАР ААА	
ABLED				
fault ,	•			
fault ,	•			
DISABLED				
	fault	fault v	fault •	fault

Step6

Define the method type as Dot1x and map the server group.

← Previous

Add Wizard		•
		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 🛛 Auther	tication 🗹 Authorization 🖌 Accounting 🗌	
General Authentication	Authorization	
Method List Name*	dot1x	
Type*	dot1x 🔹	
Group Type	group	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap // tacacs+ rad-group freerad radgrp_branch	> ISE	
♦ Previous		Save & Apply to Device

Step7 Define the method type as network and map the server group.

🖺 Save & Apply to Device

Add Wizard		×
		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
General 🗹 Authentication 🗹 🗛 General Authentication Authorization	thorization 🗹 Accounting	
Method List Name* authz		
Type*	•	
Group Type group	v	
Fallback to local Available Server Groups Idap tacacs+ rad-group freerad radgrp_branch	Assigned Server Groups	
✓ Previous		Save & Apply to Device

Step8 Create a Dot1x WLAN and map the method list on the WLAN.

Navigate to the Configuration > Tags& profiles > WLAN to create the SSID.

Q Search Menu Items		Interface	🐻 Services
		Logical	AireOS Config Translator
📰 Dashboard		Ethernet	Application Visibility
		Wireless	Cloud Services
Monitoring	>	品 Layer2	Custom Application
		VLAN	IOx
Configuration	>	VTP	Multicast
	curso -	V IF	NetFlow
(O) Administration	>	Radio Configurations	Python Sandbox
		CleanAir	QoS
💥 Troubleshooting		High Throughput	RA Throttle Policy
		Media Parameters	Tags & Profiles
		Network	AP Join
		Parameters	Flex
		RRM	Policy
		Routing Protocols	RF
		OSPF	Tags
lan selamat banat banat banat ba		🕀 Security	WLANs

WIRELESS NETWORKS + Add Kumber of WLANs selected : 0	able WLAN	sable WLAN			
Name	Add WLAN				×
open_wian	General	Security	Adva	anced	
	Profile Name*	dot1x_wlan	Radio Policy	All	
▶	SSID	dot1x_wlan	Broadcast SSID	ENABLED	
	WLAN ID*	2			
	Status				
	D Cancel			🗎 Save	& Apply to Device

Add WLAN			×
General 🔓	Security	Advanced	4
Layer2	Layer3	ААА	
Layer 2 Security Mode	WPA + WPA2 V	Fast Transition Adaptive Enabled 🗸	L
MAC Filtering		Over the DS	
Protected Management Frame		Reassociation Timeout 20	L
PMF	Disabled 🔻		-
WPA Parameters			
WPA Policy			*
Cancel		🛛 🗎 Save & Apply to Devic	e)

Add WLAN				×
General	Security		Advanced	
Layer2	Layer3		AAA	
Authentication List	dot1x	•		
Local EAP Authentication				
				P Cause & America to Designed
Cancel				🖹 Save & Apply to Device

Step9 Create a flex profile, Create a Vlan on the Flex profile which is the VLAN returned by the AAA.

Q Search Menu Items	Interface	Services
	Logical	AireOS Config Translator
🔜 Dashboard	Ethernet	Application Visibility
	Wireless	Cloud Services
(2) Monitoring	Layer2	Custom Application
	VLAN	IOx
🔍 Configuration 🕠		Multicast
	VTP	NetFlow
👩 Administration 🛛 🔸	Radio Configurations	Python Sandbox
	CleanAir	QoS
💥 Troubleshooting	High Throughput	RA Throttle Policy
	Media Parameters	Tags & Profiles
	Network	AP Join
sarah sarah sarah sarah sarah sarah	Parameters	Flex
	RRM	Policy
	Routing Protocols	RF
	OSPF	Tags
	G Security	WLANs
	AAA	Wireless
	ACL	Access Points
	Advanced EAP	Advanced
	PKI Management	Air Time Fairness
	Local EAP	Fabric

Name Add Flex Profile		 Description 	on	
-p	I Authentication Policy A	CL VLAN		
Name*	branch_flex_profile	Multicast Overridden Interface		
Description	Enter Description	Fallback Radio Shut		
Native VLAN ID	3	Flex Resilient		
	0	ARP Caching		
HTTP Proxy Port	0	Efficient Image Upgrade		
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP		
CTS Policy		Join Minimum Latency		
Inline Tagging				
SGACL Enforcemen				
CTS Profile Name	default-sxp-profilex -			

neral Local Auther	ntication Policy ACL VLAN	J			
Add 🕺 🗶 Delete					
AN Name 🖂 I	ID 🤟 ACL Name 🖂				
4 0 P P 1	0 🔹 items per page	VLAN Name*	11		
<u></u>	No items to display	VLAN Id*	11		
		ACL Name	Select ACL	×	
		🗸 Save		D Cancel	

Step 10 Create a policy profile enable local switching and central authentication on the profile also map the default vlan for the WLAN and enable AAA override .

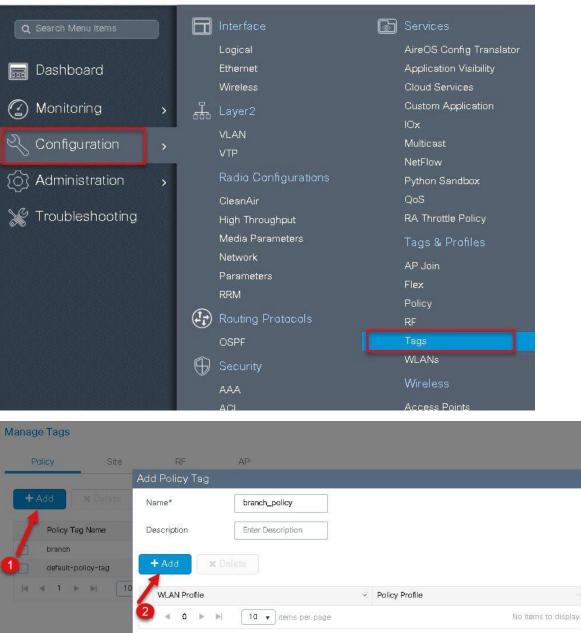
Q Search Menu Items		Interface	Services
		Logical	AireOS Config Translator
📰 Dashboard		Ethernet	Application Visibility
		Wireless	Cloud Services
🕜 Monitoring	→ ¹ / ₄	Layer2	Custom Application
		VLAN	lOx
🔧 Configuration	>	VTP	Multicast
杰			NetFlow
(0) Administration	>	Radio Configurations	Python Sandbox
SG Traublasheating		CleanAir	QoS
💥 Troubleshooting		High Throughput	RA Throttle Policy
		Media Parameters	Tags & Profiles
		Network	AP Join
		Parameters	Flex
		RRM	Policy
	(fi	Routing Protocols	RF
		OSPF	Tags
	Ĥ	Security	WLANs
		AAA	Wireless
		ACL	Access Points
		Advanced EAP	Advanced
		PKI Management	Air Time Fairness
		Local EAP	Fabric

+ Add 🗱 Delete	dd Poli cy Profile				×
Policy Profile Name	General Access P	olicies QOS and AVC	Mobility	Advanced	
default-policy-profile	🛦 Configur	ing in enabled state will result in loss of	connectivity for clients as	sociated with this profile.	
	Name*	dot1x_wlan	WLAN Switchin	g Policy	
	Description	Enter Description	Central Switching		
	Status		Central Authentic		
	Passive Client	DISABLED	Central DHCP		
	Encrypted Traffic Analytics	DISABLED	Central Associatio		
	CTS Policy		Flex NAT/PAT		
	Inline Tagging				
	SGACL Enforcement				
	Default SGT	2-65519			
d \ Policy Profile	Cancel	-		I Save & Apply to Dev	
d <mark>≹</mark> Policy Profile General <u>Access</u>		S and AVC Mob	ility Ac	Save & Apply to Dev	
		S and AVC Mob	ility Ac WLAN ACL		
General Access		S and AVC Mob			
General Access WLAN Local Profiling		S and AVC Mob	WLAN ACL	lvanced	
General Access WLAN Local Profiling HTTP TLV Caching		S and AVC Mob	WLAN ACL	Ivanced	
General Access WLAN Local Profiling HTTP TLV Caching RADIUS Profiling	Policies QO		WLAN ACL	Ivanced	
General Access WLAN Local Profiling HTTP TLV Caching RADIUS Profiling DHCP TLV Caching	Policies QO		WLAN ACL IPv4 ACL IPv6 ACL URL Filters Pre Auth	Ivanced Search or Select	
General Access WLAN Local Profiling HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Nam	Policies QO		WLAN ACL IPv4 ACL IPv6 ACL URL Filters	Vanced Search or Select	
General Access WLAN Local Profiling HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Name VLAN	e Policies QO	r Select	WLAN ACL IPv4 ACL IPv6 ACL URL Filters Pre Auth	Ivanced Search or Select	
General Access WLAN Local Profiling HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Name VLAN	e Policies QO	r Select	WLAN ACL IPv4 ACL IPv6 ACL URL Filters Pre Auth	Ivanced Search or Select	

General	Access Pol	Icles	QOS and AVC	Mobility	Advanced
VLAN Timeout				Fabric Profile	Search or Select
ession Timeout (sec)	1800		Umbrella Parameter Map	Not Configured
lle Timeout (sec)		300		WLAN Flex Policy	
lle Threshold (by	tes)	0		VLAN Central Switc	hing
llient Exclusion Ti sec)	imeout 🛛 🗹	60		Split MAC ACL	Search or Select
HCP				Air Time Faimess	Policies
HCP Enable				2.4 GHz Policy	Search or Select
HCP Server IP A	ddress.	0.0.0.0		5 GHz Policy	Search or Select
w more >>>					
AAA Policy					
llow AAA Overri	de				
AC State					
olicy Name		default-aaa-	policy 🔻		
.ccounting List		Search or Se	elect		

Step11 Map the WLAN to policy profile.

Navigate to configurationTag and create a policy tag mapping the WLAN and policy profile.



Map WLAN and Policy WLAN Profile* dot1x_wlan
Policy Profile* dot1x_wlan Cancel

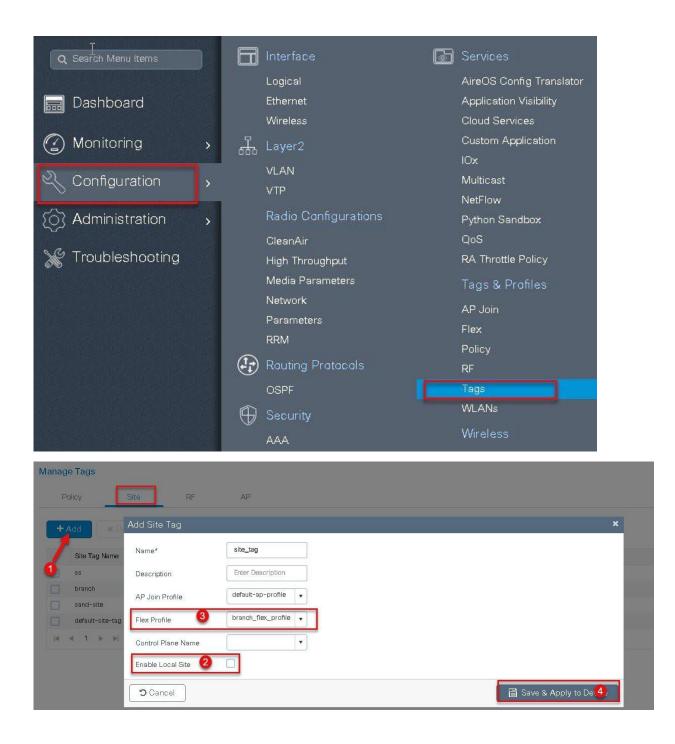
Save & Apply to Devic 4

Step 12Create an Authorization profile on the ISE to override the VLAN from AAA.Create the respective authorization rules to return the authorization profile as part of Access accept.The screenshot below is for the authorization profile , the authorization rules should refer the profile created.

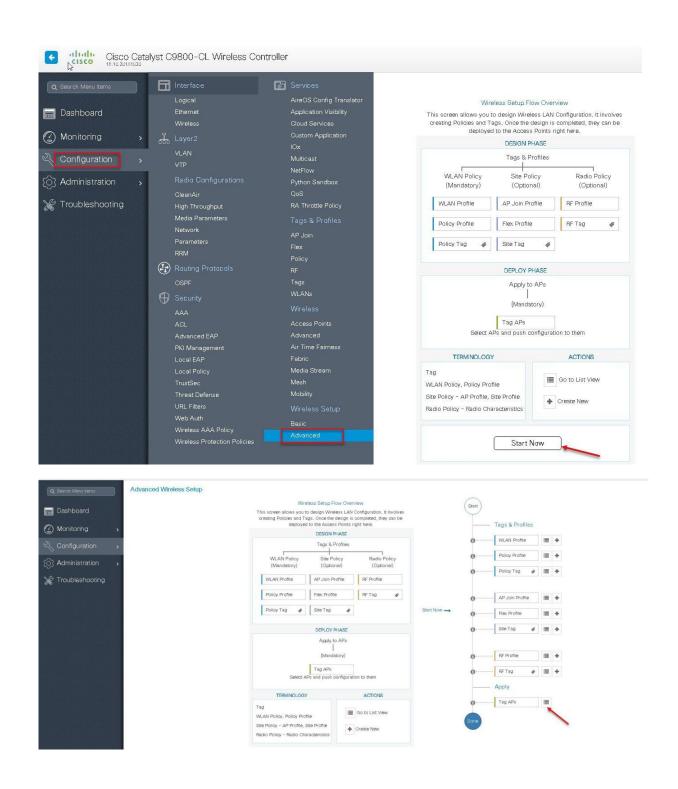
×

dentity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
Policy Sets Profiling Posture	Client Provisioning - Policy Elements
Dictionaries + Conditions - Resul	ts
	Authorization Profiles > sand-vlan
Authentication	Authorization Profile
★ Authorization	* Name sand-ylan
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Device Profile 👘 Cisco 💌 🕀
Posture	Service Template
Client Provisioning	Track Movement 📋 🕡
	Passive Identity Tracking 📋 🕧
	▼ Common Tasks
	DACL Name
	ACL (Filter-ID)
	Security Group
	Coounty choop
	VLAN Tag ID 1 Edit Tag ID/Name 11
	 Advanced Attributes Settings
	🛛 Select an item 💿 =
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:11
	Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6
	Save

Step 13 Create a site tag and map the flex profile on the site tag.



Step14Map the policy site tag and RF tag on the AP using the advanced config wizard .Navigate to Configuration wireless setup Advanced



), Search Menu Items	Advanced Wireless S	etup																E
Dashboard	Start		* 🕇	Tag APs														
	Y.	D (1)		er of APs: 3	-	•												
Monitoring		k Profiles		ted Number of /				AP	Admin	< Operatik	on v	Policy ~	Site ~				Hyperlocat	tion
Configuration >		I Profile	·····	AP Name v			AP MAC	< Mode	Status	Status		Tag	Tag	RF Tag ~ default-rf-	Locatio		ry 🧹 Method	
Administration >		Profile		ap-1 sand-øwic-	K9 AIR-AF		0081.c4a0.61		Disabled	Register		sand-policy	sand-site	tag default-rf-	location default	116	Local	
Troubleshooting	OPolic	Tag 🦸 🔳	+	ap-2 sand-3700	K9 AIR-CA		30e0.1d7b.8		Enabled	Register		sand-policy	sand-site	tag default-rf-	default	1	Local	
	AP.I	in Profile 🗮	- H	4.1.1	A-K9	• Items per								tag	location	1	1 - 3 of 3 ite	erns
	Ø Fiex I																	
	6 Stel																	
	0 Contraction		*															
	0 RE P	ofile	+															
			-															
a choice of a la	0 RF T	0 0 🔳	*															
		0 0 🖉 🔳	*															
	Apply		*															
			*															
	Apply		•															
	Apply		•															
	Apply Gunne		•															
Advanced Win	Apply Gunne		•															
Advanced Win	Apply Gunne		•	<i>K</i>														
	Apply Gunne		•	*	+	Tag A	Ps											
Advanced Win	Apply Gunne		•	*	+	Tag A	Ps											
	eless Setup	⊳	•	Ļ		Tag A												
	Apply Gunne	⊳	•	N	lumbe		s: 3	APs: 3									l	
	eless Setup	⊳		N	lumbe ielecte	er of AP ed Numl	s: 3 ber of a	APs: 3	1							Admin		0
	eless Setup	sfiles		N	lumbe ielecte	er of AP ad Numl AP	s: 3		el	~ A	PMAC		A ~ M			Admin		
Start	eless Setup	sfiles		N	lumbe electe	er of AP ed Numl	s: 3 ber of a	AP Mod			P MAC			p ode		Admin Status		Of
Start	eless Setup	n h		N	lumbe electe	er of AP ad Numl AP	s: 3 ber of <i>i</i>	AP Mod				30.6fe	~ M					St
Start 0	eless Setup	n h		N	lumbe electe	er of AP ad Numl AP Name	s: 3 ber of <i>i</i>	AP Mod AIR-AP3 K9					~ M	ode		Status		St Re

Step 15 Associate a client on the WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN as the attribute.

Verify the client connectivity by navigating to monitoring wireless clients and verify the access vlan the client is mapped to

Policy

Site

RF

Cancel

branch-policy

default-rf-tag

Changing AP Tag(s) will cause associated AP(s) to reconnect

site_tag

۲

•

•

🗑 Save & Apply to Device

Double click on the client mac to open up the details of the Client session

i +

1

AP Join Profile

Flex Profile

Site Tag

RF Profile

RF Tag

a

0

	Clients							
ashboard	Clients Sleeping (Clients Excluded Clients						
	N Delete							
	The supervision and supervision							
	Total Client(s) in the Network: 1							
	Total Client(s) in the Network: 1 Client MAC Address	IPv4/IPv6 Address	< AP Name	< WLAN	 State Protoco 	ol 🧹 User Name	< Device Type	< Role
Configuration		 IPv4//Pv6 Address 9.1.11.252 	 AP Name ap-1-3800 	< WLAN 10	 State Protoco Run 11ac 	ol - User Name sand-wireless	 Device Type 	 Role Local

lients	Client					
Clients Sleeping Clients Excluded Clients	General QOS Statistics ATF Statistics Mobility History Call Statistics					
	Client Properties AP Properties Security Information Client Statistics QOS Properties					
* Delete	MAC Address 1c36.bbef.6492					
	IPV4 Address 9.1.11.252					
otal Client(s) in the Network: 1	User Name sand-wireless					
Client MAC Address v IPv4/IPv6 Address v AP Name	V Policy Profile dot1x_wlan					
1c36.bbef.6492 9.1.11.252 ap-1-3800	Flex Profile branch_flex_profile					
	Wireless LAN Id 10					
🖂 🚽 1 🕞 10 👻 items per page	Wireless LAN Name dot1x_wlan					
	BSSID 0061.c4a0.6fee					
click on the client mac to open up,	Uptime(sec) 104 seconds					
details page)	GCX version No GCX support					
	Power Save mode OFF					
	Current TxRateSet m9 ss3					
	Supported Rates 9.0,18.0,36.0,48.0,54.0					
	Policy Manager State Run					
	Last Policy Manager State IP Learn Complete					
	Encrypted Traffic Analytics No					
	Multicast VLAN 0					
	Access VLAN 11					
	Anchor VLAN 0					
	Server IP 9.1.0.20					
	DNS Snooped IPv4 Addresses None					
	DNS Snooped IPv6 Addresses None					
	11v DMS Capable No					
	FlexConnect Data Switching Local					
	FlexConnect DHCP Status Local					
	FlexConnect Authentication Central					

lient									
General	QOS St	atistics	ATF S	Statistics	Mobility Histo	ry	Call Statistic	S	
Client Prop	perties	AP Prop	erties	Security	Information	Clie	nt Statistics	QOS Properties	
Encryption (Sipher			CCMI	P (AES)				
Authenticati	on Key Mar	nagement		802.1	x				
EAP Type				PEAF	1				
Session Tim	eout			1800					
Session Man	ager								
Interface				capw	ap_90000007				
IIF ID				0x900	00007				
Authorized				TRUE					
Common Se	ssion ID			1004	0109000000F03/	45544	0		
Acct Sessio	n ID			0x000	000000				
Auth Method	d Status Lis	t							
Method				Dot1>	<				
SM State				AUTH	HENTIGATED				
SM Bend St	ate			IDLE					
Local Policie	8								
Service Tem	plate			wlar	n_svc_dot1x_wlan	(priori	ity 254)		
Absolute Tim	ner			1800	D				
Server Polici	es								
Output SGT				0010	0-35				
VLAN				11					
Resultant Po	licies								
Output SGT				0010	0-35				
VLAN				11					
Absolute Tim	ner			1800	D C				

FlexConnect VLAN Based Central Switching

VLAN based central switching is a feature that will enable central or local switching based on the VLAN returned as part of the AAA override. If the VLAN provided by the AAA is part of the VLAN present on the AP, the client would be locally switched and if the VLAN returned by the AAA is not present in the AP and is available at the WLC, the client would be centrally switched.

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 excluded with the reason VLAN failure.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the Flex Connect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client will be assigned a VLAN mapped on the policy profile that is attached to the policy tag on that FlexConnect AP and traffic will switch locally.
- If the VLAN returned as part of the AAA attribute is present on both the AP and WLC, the client will be locally switched. The vlan on the AP takes precedence over the one on the WLC.

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

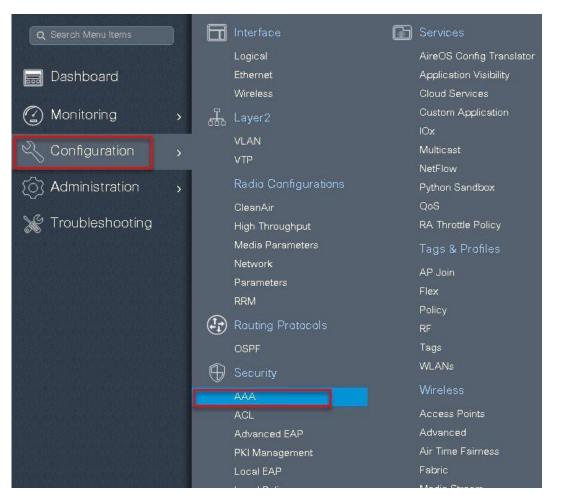
- If the VLAN returned by an AAA server is not present in the Flex AP database, the client will be put to default VLAN (that is the VLAN mapped on the policy profile which is linked to the WLAN). When the AP connects back, this client will be de-authenticated and will switch traffic centrally.
- If the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

Steps to configure FlexConnect VLAN Based Central Switching

Procedure

Step1 Define a AAA server and method list for dot1x which is mapped to the WLAN. The AAA server is created by navigating to the following :

Configuration > security > AAA.



Step 2

Use the AAA wizard to create the server and server groups.

Cisco Cata Cisco Cata A Cisco Cata A Cisco Cata A Cisco Cata Cisco Cata	alyst C9800-CL Wireless Con		
Dashboard Monitoring	+ AAA Wizard	Servers / Groups AAA Advanced	
Configuration Administration Troubleshooting	General Authentication Authorization Accounting	Local Authentication Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default Default DisableD

Step3 Define a name for the server and specify the IP address and shared secret.

Add Wizard							×
						Basic	O Advanced
	SERVER		SER	VER GROUP ASSO	OCIATION	MAP AAA	
RADIUS 🔽	TACACS+	LDAP					
RADIUS							
Name*	ISE						
IPv4 / IPv6 Server Address*	9.1.0.20						
PAC Key							
Кеу*							
Confirm Key*	1						
Cancel							Next 🗲

Step 4

4 Create a server group and map the server in the group.

Add Wizard		,
		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
RADIUS		
Name*	ISE	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none 🔹	
Dead-Time (mins)	1-1440	
Available Servers	Assigned Servers	1
freerad ISE-2 ISE	> ISE *	
*	×	
Frevious		Next 🗲

Step 5

Enable dot1x system control and check mark the authentication and Authorization profile.

		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
General 🗹 Authenticatio	on Authorization Accounting	
General		
aaa_dot1x_system_auth_control	ENABLED	
ocal Authentication	Default	
ocal Authorization	Default	
adius Server Load Balance	DISABLED	

← Previous Save & Apply to Device

Step 6

Define the method type as Dot1x and map the server group.

Add Wizard		×
		Basic O Advanced
Co la	0	
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🖌 Authenticati	on 🗹 Authorization 🗹 Accounting 🗌	
General Authentication	Authorization	
Method List Name*	dot1x	
Туре*	dot1x v	
Group Type	group	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap tacacs+ rad-group freerad radgrp_branch	ISE *	
♦ Previous		📓 Save & Apply to Device

Step7 Define the method type as network and map the server group .

Add Wizard		×
		Image: Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authentication 🖌	Authorization 🗹 Accounting 🗌	
Method List Name*	authz	
Туре*	network 🔹	
Group Type	group	
Failback to local Available Server Groups Idap tacacs+ rad-group freerad radgrp_branch	Assigned Server Groups	
✓ Previous		🖹 Save & Apply to Device

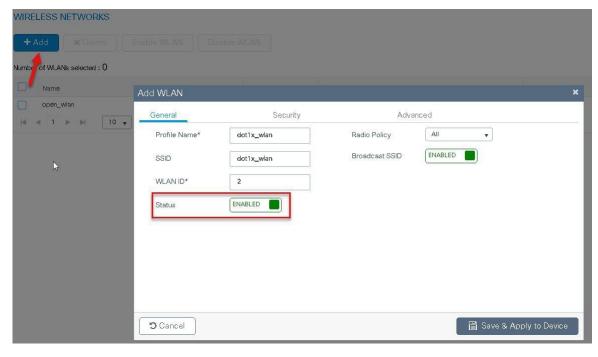
Step 8

Create a Dot1x WLAN and map the method list on the WLAN.

To create an SSID navigate to Configuration > Tags & Profiles > WLANs.

s

Q Search Menu Items		Interface	Services
		Logical	AireOS Config Translator
🔜 Dashboard		Ethernet	Application Visibility
		Wireless	Cloud Services
(2) Monitoring	>	品 Layer2	Custom Application
		VLAN	IOx
🔍 Configuration	>	VTP	Multicast
			NetFlow
(O) Administration	>	Radio Configurations	Python Sandbox
		CleanAir	QoS
💥 Troubleshooting		High Throughput	RA Throttle Policy
		Media Parameters	Tags & Profiles
		Network	AP Join
	X115 - 30	Parameters	Flex
		RRM	Policy
		🕞 Routing Protocols	BE
	NIT: 10	OSPF	Tags
		~	WLANs
		🕤 Security	



Add WLAN			×
General ଢ	Security	Advanced	<u>^</u>
Layer2	Layer3	AAA	
Layer 2 Security Mode	WPA + WPA2	Fast Transition	Adaptive Enabled 🔻
MAC Filtering		Over the DS	
Protected Management Frame		Reassociation Timeout	20
PMF	Disabled 👻		<u>e</u> .
WPA Parameters			
WPA Policy			•
Cancel			Save & Apply to Device
Add WLAN			×
Add WLAN	Security	Advanced	×
ind there	Security Layer3	Advanced	×
General			×
General Layer2	Layer3		×
General Layer2 Authentication List	Layer3		×
General Layer2 Authentication List	Layer3		×
General Layer2 Authentication List	Layer3		×
General Layer2 Authentication List	Layer3		×
General Layer2 Authentication List	Layer3		*

Step9 Create a policy profile enable local switching and central authentication on the profile also map the default vlan for the WLAN and enable AAA override .

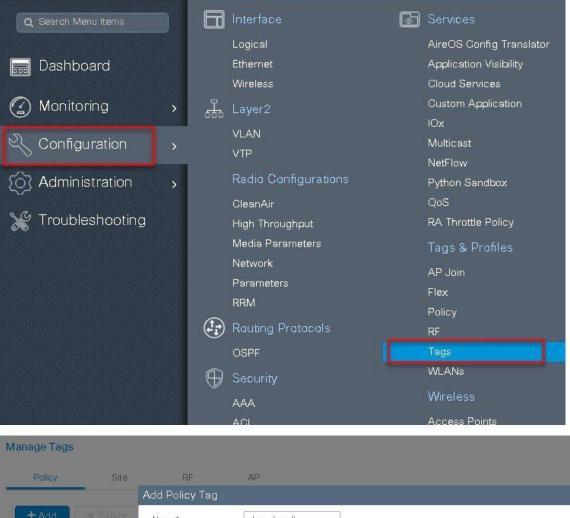
Q Search Menu Items	Interface	Services
	Logical	AireOS Config Translator
📰 Dashboard	Ethernet	Application Visibility
	Wireless	Cloud Services
🕜 Monitoring 🛛 🕥	Layer2	Custom Application
<u> </u>	VLAN	lOx
🔍 Configuration 🛛 🔸	VTP	Multicast
	VIP	NetFlow
👩 Administration 🛛 🔉	Radio Configurations	Python Sandbox
u de la companya de la compa	CleanAir	QoS
💥 Troubleshooting	High Throughput	RA Throttle Policy
	Media Parameters	Tags & Profiles
	Network	AP Join
	Parameters	Flex
	RRM	Policy
	Routing Protocols	RF
	OSPF	Tags
	Security	WLANs
	AAA	Wireless
	ACL	Access Points
	Advanced EAP	Advanced
	PKI Management	Air Time Fairness
	Local EAP	Fabric
CONTRATISON OF STREET, SOUTH ST		

+ Add so Delete				
	Add Policy Profile			
Policy Profile Name open_wian	General Access Po	plicies QOS and AV	/C Mobility	Advanced
default-policy-profile	🛦 Configuri	ing in enabled state will result in Ic	oss of connectivity for clients as	sociated with this profile.
	Name*	dot1x_wlan	WLAN Switchin	g Policy
	Description	Enter Description	Central Switching	
	Status Passive Client		Central Authentic	ation 🔽
	Encrypted Traffic Analytics		Central Associati	on 🔲
	CTS Policy		Flex NAT/PAT	
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	O Cancel			Save & Apply to Device
Ad 🖁 Policy Profile				:
General Acces	s Policies QOS			
		and AVC N	lobility Adv	anced
WLAN Local Profiling		and AVC N	lobility Adv	anced
WLAN Local Profiling		and AVC M		Search or Select
		and AVC M	WLAN ACL	Search or Select
HTTP TLV Caching		and AVC M	WLAN ACL	
HTTP TLV Caching RADIUS Profiling DHCP TLV Caching			WLAN ACL	Search or Select
HTTP TLV Caching			WLAN ACL IPv4 ACL IPv6 ACL	Search or Select
HTTP TLV Caching RADIUS Profiling DHCP TLV Caching			WLAN ACL IPv4 ACL IPv6 ACL URL Filters	Search or Select Search or Select
HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Nan			WLAN ACLIPv4 ACLIPv6 ACLURL FiltersPre Auth	Search or Select Search or Select Search or Select
HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Nan VLAN	me Search or	Select	WLAN ACLIPv4 ACLIPv6 ACLURL FiltersPre Auth	Search or Select Search or Select Search or Select
HTTP TLV Caching RADIUS Profiling DHCP TLV Caching Local Subscriber Policy Nan VLAN	me Search or	Select •	WLAN ACLIPv4 ACLIPv6 ACLURL FiltersPre Auth	Search or Select Search or Select Search or Select

	Access F	Policies Q	OS and AVC	Mobility	Advanced
WLAN Timeou	t			Fabric Profile	Search or Select
Session Timeou	:(sec)	1800		Umbrella Parameter Map	Not Configured 🗸
Idle Timeout (se	=)	300		WLAN Flex Policy	
ldle Threshold (k	oytes)	0		VLAN Central Switch	ning 🔽
Client Exclusion (sec)	Timeout 🧕	60		Split MAC ACL	Search or Select
DHCP				Air Time Faimess	Policies
DHCP Enable				2.4 GHz Policy	Search or Select
DHCP Server IP	Address	0.0.0.0		5 GHz Policy	Search or Select 🗸
ow more >>>					
AAA Policy					
171	ride				
AAA Policy Allow AAA Over NAC State	ride				
Allow AAA Over	ride	default-aaa-polic	y v		

Step 10 Map the WLAN to policy profile.

Navigate to configuration > Tag and create a policy tag mapping the WLAN and policy profile.



	Add Policy Tag					
+ Add	Name*	branch_policy				
Policy Tag Name	Description	Enter Description				
branch						
default-policy-tag						
a a 1 k k 10	WLAN Profile		×	Policy Profile		
	2 ⊲ 0 ⊳ 1	10 🔹 items per	page		No ite	ems to display
	Map WLAN and	Policy				23
	WLAN Profile*	dot1x_wlan	• 3	Policy Profile*	dot1x_wlan	•
	L	2016 2016	×		15	
	Cancel				📔 Save & Appl	y to Devic 4

Step11 Create a flex profile and defines a VLAN on the flex profile returned by the AAA radius server.

Q Search Menu Items)	П	Interface (b	Services
			Logical		AireOS Config Translator
📷 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
🕜 Monitoring	>	.	Layer2		Custom Application
	-		VLAN		IOx
Configuration			VTP		Multicast
		d.			NetFlow
() Administration	>		Radio Configurations		Python Sandbox
			CleanAir		QoS
💥 Troubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		- AP Join
			Parameters		Flex
			RRM		Policy
			Routing Protocols		RF
			OSPF		Tags
					WLANs
		9	Security		
			ААА		Wireless
			ACL		Access Points
			Advanced EAP		Advanced
			PKI Management		Air Time Fairness
			Local EAP		Fabric

Flex Profile	Add Flex Profile		- Descriptic	on X
	General Local Name* Description	Authentication Policy ACL branch_flex_profile Enter Description	VLAN Multicast Overridden Interface Fallback Radio Shut	
Native VLAN ID HTTP Proxy Port HTTP-Proxy IP Address CTS Policy		3 0 0.0.0.0	Flex Resilient ARP Caching Efficient Image Upgrade Office Extend AP Join Minimum Latency	
	Inline Tagging SGACL Enforcement CTS Profile Name	default-sxp-profile _x		冒 Save & Apply to Device

General Local	Authentication Policy ACL VLAN			
+ Add × D				
VLAN Name	✓ ID ✓ ACL Name ✓	<		
4 4 0 💶 H	10 🔹 items per page	VLAN Name*	11	
	No items to display	VLAN Id*	11	
		ACL Name	Select ACL	
		Save	Cancel	
		4		

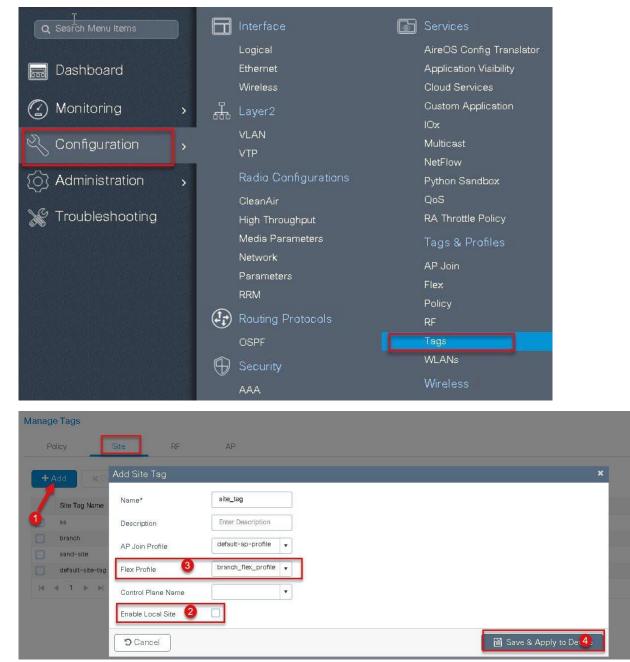
Step12

Create an Authorization profile on the ISE to override the VLAN.

Create the respective authorization rules to return the authorization profile as part of Access accept.

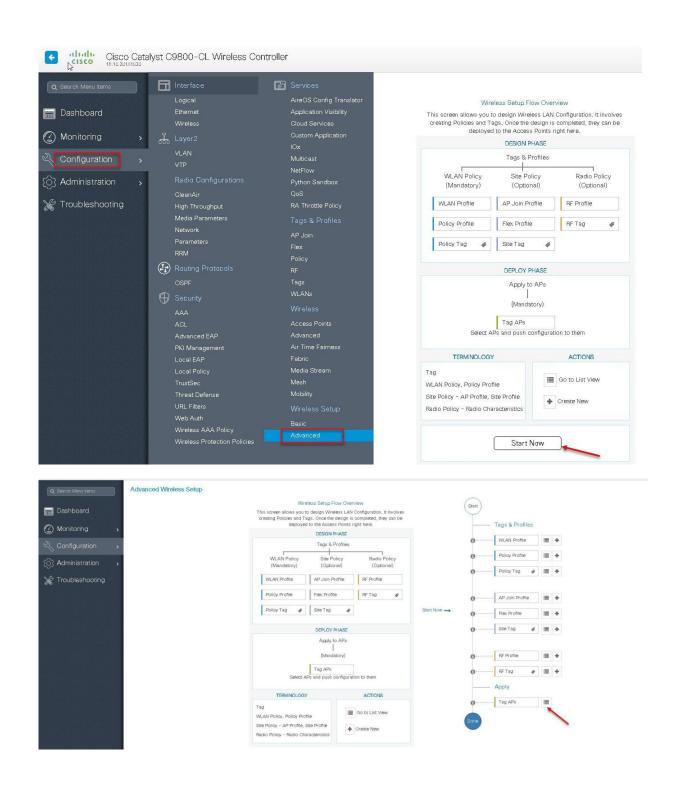
In this example vlan 11 is a present on the AP and would make the client in local switched mode.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	ient Provisioning - Policy Elements
Dictionaries + Conditions Result	8
Authentication	Authorization Profiles > sand-vlan Authorization Profile
* Authorization	* Name sand-vlan
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Device Profile data Cisco 💌 🕀
▶ Posture	Service Template
► Client Provisioning	Track Movement 📋 🕧
	Passive Identity Tracking 📋 🕧
	Common Tasks
	DACL Name
	ACL (Filter-ID)
	Security Group
	VLAN Tag D 1 Edit Tag D/Name 11
	Advanced Attributes Settings
	📱 Select an item 💿 = 🥥 — 🕂
	Attributes Details Access Type = ACCESS_ACCEPT
	Turnel-Type = 1:13 Turnel-Type = 1:6
	Tunnel-Medium-Type = 1:6



Step13 Create a site tag and map the flex profile on the site tag.

Step14Map the policy site tag and RF tag on the AP using the advanced config wizard.Assigning a site tag on a AP would result in AP reboot due to conversion to flexconnect mode.The reboot is avoided if the AP is already in flexconnect mode,Navigate to Configuration > wireless setup > Advanced



Search Menu Items	Advanced Wireless Se	tup															Baci
Dashboard	Start		*	+ Tag APs													
Monitoring >	\sim	Profiles		imber of APs: 3 lected Number o													
Configuration			+		AP Model	- AP	MAC	P ≺ Admi lode Statu		tion Y Pe		Site ~ Tag	RF Tag	Location V.	Country v	Hyperlocation Method	n K
Administration			+	sand-ewic-	AIR-AP38		31.c430.6fe0 F				ind-policy s		default-rf-	default location	US	Local	
	O Policy	Тад 🛷 🔳	+ 5	sand-ewic- ap-2	AIR-AP38 K9	1021-B- 008	31.0430.7550 F	lex Disab	bled Regist	ered sa	ind-policy s	sand-site	default-rf-	default location	us	Local	
Troubleshooting			5	2 sand-3700	AIR-CAPS A-K9		e0.1d7b.8610 F	ler. Enabl	ied Regist	ered sa	nd-policy s	sand-site	default-rf- tag	default location	us	Local	
	• AP Jo	in Profile	+	(4 4 1 »	10 🗸) items per pa	ĝe.									1 - 3 of 3 items	0
	G Flex F	rofile	•														
	G Site T	a e III	+														
	0 RF Pr	nie III	+														
	0 RF Ta																
a start a total	Apply																
	0 Tag A																
	Uone																
				10 A													
Start				*	+	Tag A	\Ps										
Start				*	<u> </u>	Tag A		~									
Start	– Tags & Pi	ofiles		×	Numb	er of Al		Ps: 3									
			11		Numb	er of Al	Ps: 3	Ps: 3					AP		Admir	1 ~	
Start	- Tags & Pi][=	«	Numb	er of Al	Ps: 3 hber of A	Ps: 3 AP Model		AP M	AC	*	AP Mode		Admir Status		
•	WLAN Pro	file		+	Numb Select	er of Al ed Nurr AP Name	Ps: 3 hber of A						Mode		Status		
		file] 🔳		Numb Select	er of Al ed Nurr AP	Ps: 3 hber of A 	AP Model AIR-AP38 (9			AC c4a0.6						
0	···· WLAN Pro	file		+	Numb Select	er of Al ed Nurr AP Name	Ps: 3 hber of A 800 /	AP Model AIR-AP38 (9					Mode		Status		
•	WLAN Pro	file		+	Numb Select	er of Al ed Nurr AP Name ap1-3 ap2-3	Ps: 3 Inber of A 800 { Tag A	AP Model AIR-AP38 (9 APs					Mode		Status		
0	···· WLAN Pro	file		+	Numb Select	er of Al ed Num AP Name ap1-3	Ps: 3 hber of A 800 { Tag A	AP Model AIR-AP38 (9 APs					Mode		Status		
0	WLAN Pro	ifile file] [=]	+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 Inber of A 800 { Tag A	AP Model AIR-AP38 (9 APs					Mode		Status		
0	···· WLAN Pro	ifile file		+	Numb Select	er of Al ed Nurr AP Name ap1-3 ap2-3	Ps: 3 Inber of A 800 { Tag A	AP Model XIR-AP38 (9 APs 8	302I-B-		c4a0.6		Mode		Status		
0 0	WLAN Pro Policy Pro Policy Tai AP Join F	nfile file 3 Ø		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 heer of A 800 Tag A Tag	AP Model XIR-AP38 (9 APs 8	302I-B-	0081.	c4a0.6	ife0	Mode		Status		
0 0	WLAN Pro	nfile file 3 Ø] [=]	+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 heer of A 800 Tag A Tag	AP Model XIR-AP38 (9 APs 8	302I-B-	0081. nch-polic	c4a0.6	ife0	Mode		Status		
0 0 0	WLAN Pro Policy Pro Policy Tai AP Join P Fiex Profi	nfile nfile a se		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 her of A 800 (Tag / Polic	AP Model XIR-AP38 (9 APs 8	3021-B-	0081. nch-polic	c4a0.6	ife0	Mode		Status		
0 0 0	WLAN Pro Policy Pro Policy Tai AP Join F	nfile file 3 Ø		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 her of A 800 (Tag / Polic	AP Model XIR-AP38 (9 APs 8	302I-B-	0081. nch-polic	c4a0.6	ife0	Mode		Status		2
0 0 0 0	WLAN Pro Policy Pro Policy Tai AP Join P Fiex Profi	nfile nfile a se		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 hober of A 800 (Tag A Polic Site	AP Model XIR-AP38 (9 APs 8	302I-B-	0081. nch-polic _tag	c4a0.6	ife0	Mode		Status		
0 0 0	WLAN Pro Policy Pro Policy Tai AP Join P Fiex Profi	nfile nfile a se		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 her of A 800 (Tag A Polic Site RF	AP Model AIR-AP38 (9 APS 8	302I-B-	0081. nch-polic _tag sult-rf-ta	c4a0.6	ife0	Mode Flex		Status		
0 0 0	WLAN Pro Policy Pro Policy Tai AP Join P Fiex Profi	nfile a a rofile e		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 her of A 800 (Tag A Polic Site RF	AP Model AIR-AP38 (9 APS 8	302I-B- brar site defa	0081. nch-polic _tag sult-rf-ta	c4a0.6	ife0	Mode Flex		Status		
0 0 0 0 0 0 0	 WLAN Pro Policy Pro Policy Tai AP Join F Flex Profi Site Tag 	nfile a a rofile e		+	Numb Select	er of Al red Nurr AP Name ap1-3 ap2-3 ap1-3	Ps: 3 her of A 800 (Tag A Polic Site RF <i>Char</i>	AP Model AIR-AP38 (9 APS 8	302I-B- brar site defa	0081. nch-polic _tag sult-rf-ta	c4a0.6	ife0	Mode Flex	reconn	Status		*

Step 15 Associate a client on the WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN as an attribute.

Verify the client connectivity by navigating to monitoring > wireless > clients and verify the access vlan the client is mapped.

In this step the AAA returns vlan 11 which is present in the AP database results in local switched WLAN.

Double click on the client mac to open up the details of the Client session

Search Menu Items								
Dashboard Clients Sleeping Clients	Excluded Clients							
Aonitoring > Michiete								
Configuration > Total Client(s) in the Network: 1								
Cliers MAG Address	IPv4/IPv6 Address 9.1.11.252	 AP Name ap-1-3800 	< WLAN	- State	< Protocol	 User Name sand-wireless 	< Device Type	 Role Local
roubleshooting	9.1.11.252	ap-1-3800	10	Hun	1180	sand-wireless		Local 1 - 1 of 1 clients C
ent								×
anc								
General QOS Statistics ATF	Statistics	Mobility His	story	Call Stati	istics			
Client Properties AP Properties	Security	nformation	Clier	nt Statistics	s C	OS Properties	i i	
Current TxRateSet	m8 ss	3						
Supported Rates	9.0,18	.0,36.0,48.0,5	4.0					
Policy Manager State	Run							
Last Policy Manager State	IP Lea	rn Complete						
Encrypted Traffic Analytics	No							
Multicast VLAN	0							
Access VLAN	11	1						
Anchor VLAN	0							
Server IP	9.1.0.2	20						
DNS Snooped IPv4 Addresses	None							
DNS Snooped IPv6 Addresses	None							
11v DMS Capable	No	_						
FlexConnect Data Switching	Local							
FlexConnect DHCP Status	Local							
FlexConnect Authentication	Centra	Î.						
FlexConnect Central Association	Yes							
antenna 0	lsag	o34	dBm					
antenna 1	lsag	o34	dBm					
Eogre Client	False							
Eogre Match Status	no tun	nel profile or a	iaa data					
lobility								
Move Count	0							
Role	Local							
Roam Type	None							
Complete Timestamp		2018 02:23:04	1 UTC					parent.
abric								

General QOS St	otiotico ATE	Statistics	Mobility Histor	v Call St	otiotico	
General QUS SL	atistics ATF	Statistics	MODIIILY HISLO	y Gall St	atistics	
Client Properties	AP Properties	Security	y Information	Client Statist	ics QOS	S Properties
Encryption Cipher		CCM	IP (AES)			
Authentication Key Mar	nagement	802.1	1x			
EAP Type		PEAF	2			
Session Timeout		1800)			
ession Manager						
Interface		capv	vap_90000007			
IIF ID		0x90	000007			
Authorized		TRUE				
Common Session ID		1004	0109000000F03A	55440		
Acct Session ID		0x00	000000			
Auth Method Status Lis	t					
Method		Dot1	x			
SM State		AUTI	HENTICATED			
SM Bend State		IDLE				
ocal Policies						
Service Template		wla	n_svc_dot1x_wlan	(priority 254)		
Absolute Timer		180	0			
erver Policies						
Output SGT		001	0-35			
VLAN		11				
esultant Policies						
Output SGT		001	0-35			
VLAN		11				

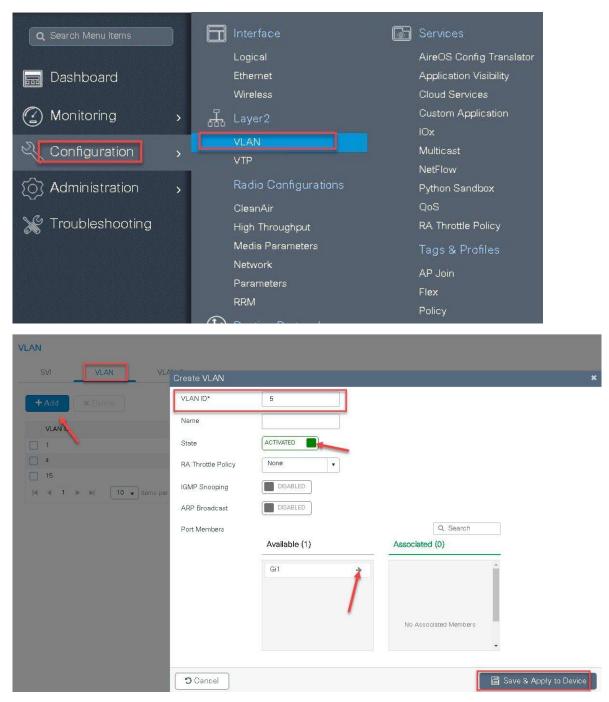
Step 16

Create an Authorization profile to return a VLAN which is not present on the AP database but on the WLC.

In this example VLAN 5 is present on the WLC and not on the AP database which results in WLAN being central switched.

ender Identity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
Policy Sets Profiling Posture Clie	ent Provisioning Policy Elements
Dictionaries + Conditions - Results	
0	
Authentication	Authorization Profiles > vlan-wlc Authorization Profile
 Authorization 	* Name vian-wic
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Device Profile des Cisco 💌 🕀
▶ Posture	Service Template
Client Provisioning	Track Movement
	Passive Identity Tracking 📋 👔
	▼ Common Tasks
	* Cuminur rasks
	DACL Name
	ACL (Filter-ID)
	Security Group
	VLAN Tag ID 1 Edit Tag ID/Name 5
	 Advanced Attributes Settings
	🛛 Select an item 🔍 = 💟 — 🕂
	Access Type = ACCESS_ACCEPT
	Tunnel-Private-Group-ID = 1:5 Tunnel-Iype = 1:13
	Tunnel-Medium-Type = 1:6
	Save Reset

Step 17Validation on the presence of VLAN 5 on the WLC .Navigate to Configuration >Vlan.



Step18 Associate a client on the WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN(VLAN5) as the return attribute.

Verify the client connectivity by navigating to monitoring > wireless > clients and verify the access vlan the client is mapped and switching properties for the client.

Double click on the client mac to open up the details of the Client session.

Cisco Cata	ilyst C9800-CL Wireless Contr	oller								Welcon	ne sand	*
Q Search Menu Items	Clients											
🚃 Dashboard	Clients Sleeping (Clients Excluded Clients										
Monitoring >	X Delete											
🗞 Configuration 🕠	Total Client(s) in the Network: 1											
	Client MAC Address	 IPv4/IPv6 Address 	v.	AP Name	< WLAN	v. State	×	Protocol	×	User Name	≪ D	evice Ty
 (∂) Administration → (∂) Administration → 	□ 1c36.bbef.6492	9.1.5.200 click on client mac to open s per page the details		ap-1-3800	10	Run		1ac		sand-wireless		

ent		
General QOS Statistics A	ATF Statistics Mobility History Call Statistics	
Client Properties AP Propertie	es Security Information Client Statistics QOS Properties	
MAC Address	1c36.bbef.6492	
IPV4 Address	9.1.5.200	
User Name	sand-wireless	
Policy Profile	dot1x_wlan	
Flex Profile	branch_flex_profile	
Wireless LAN Id	10	
Wireless LAN Name	dot1x_wlan	
BSSID	0081.c4a0.6fee	
Uptime(sec)	162 seconds	
CCX version	No CCX support	
Power Save mode	OFF	
Current TxRateSet	m9 ss3	
Supported Rates	9.0,18.0,36.0,48.0,54.0	
Policy Manager State	Run	
Last Policy Manager State	IP Learn Complete	
Encrypted Traffic Analytics	No	
Multicast VLAN	0	
Access VLAN	5	
Anchor VLAN	0	
Server IP	9.1.0.20	
DNS Snooped IPv4 Addresses	None	
DNS Snooped IPv6 Addresses	None	
11v DMS Capable	No	
FlexConnect Data Switching	Central	
FlexConnect DHCP Status	Local	
FlexConnect Authentication	Central	
FlexConnect Central Association	No	

lient						*
General	QOS Statistics	ATF Statistics	Mobility Histo	ry Call Sta	atistics	
Client Pro	perties AP Prop	erties Secu	ity Information	Client Statisti	ics QOS Propert	ies
Encryption	Cipher	CC	MP (AES)			
Authentica	tion Key Management	80	2.1x			
EAP Type		PE	AP			
Session Tir	neout	18	00			
Session Ma	nager					
Interface		са	pwap_90000007			
IIF ID		0x	90000007			
Authorized		TR	UE			
Common S	ession ID	10	0401090000001303E	3C4500		
Acct Sessi	on ID	Ox	0000000			
Auth Metho	od Status List					
Method		Do	tlx			
SM State		AL	ITHENTICATED			
SM Bend S	tate	IDI	E			
Local Policie	98					
Service Ter	nplate	W	lan_svc_dot1x_wlan	(priority 254)		
Absolute Ti	mer	1	300			
Server Polic	ies					
Output SGT		0	010-35			
VLAN		5				
Resultant Po	olicies					
Output SGT		0	010-35			
VLAN		5				
Absolute Tir	mer	1	800			

Local Authentication and Backup Radius server

In most typical branch deployments, it is easy to foresee that client 802.1X authentication takes place centrally at the WLC located at the Data center .However there arises certain concerns with central authentication at the WLC.

How can wireless clients perform 802.1X authentication and access Data Center services if WLC 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?

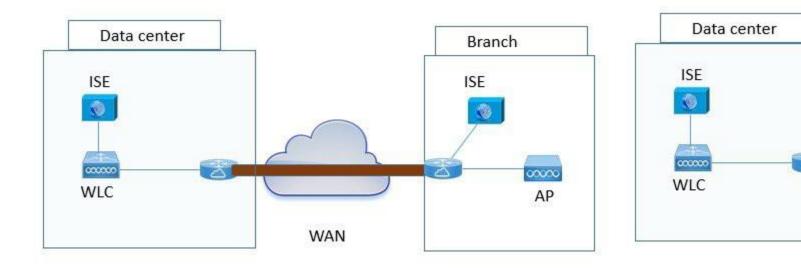
Does the Flex Connect Solution provide no operational branch downtime?

Flexconnect Local authentication and Backup/Local Radius can address the above concerns by enabling branch to operated independently in case of WAN outage or connectivity issue with the controller.

Summary

- The use of local authentication in branch enables resiliency at the branch location by providing wireless access in scenarios where the WAN connectivity is lost with the Data center. The AP moves to standalone mode and provides wireless access with authentication for dot1x directed to a radius server available at the branch side.
- The AP can act as a radius server and this feature is only supported on the Wavel AP's.
- This feature can be used with central authentication or local authentication .In Central authentication case the WLC will authenticate the wireless clients as long as the AP is in connected mode.
- Once the AP loses connectivity with the WLC the AP will move to standalone and authenticate the client locally.
- This feature can be used with local authentication and local switching, in cases where there is a local radius server at the branch, the AP can forward the radius request to the radius server at the branch thereby avoiding the latency variation caused by the WAN links.
- EAP-LEAP is the only method supported for AP as radius Server.

Local Authentication with External radius server



Steps for Local Authentication and Backup Radius server

Procedure

 Step1
 Define an AAA server, For Branch deployment specify the AAA server used at the branch side.

 Navigate to Configuration > Security > AAA and start the AAA wizard

The wizard helps in creating the following flow.

• Create a radius server.

- Create a server group and map the radius server on the server group.
- Map the server for dot1x authentication .

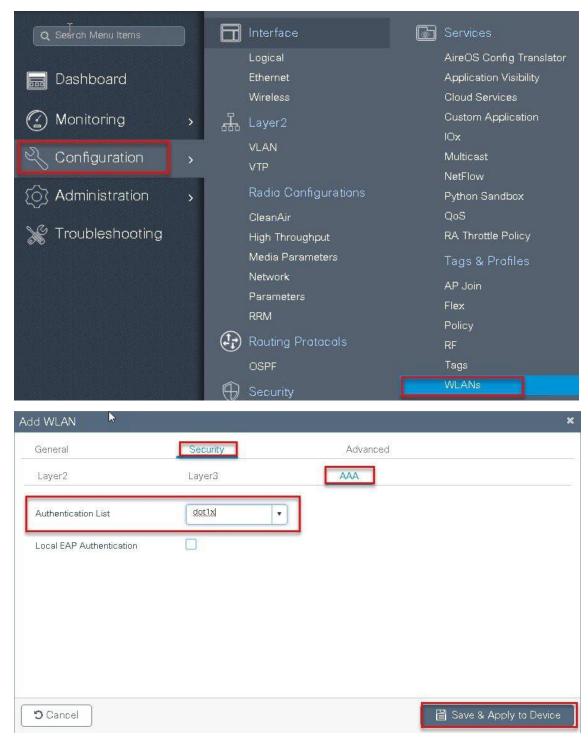
Q. Search Menu Items Dashboard Monitoring Configuration	Authentication Authorization a + AAA Wizard AAA Method List General Authentication	Servers / Groups AAA Advanced	Default	
() Administration 쑸 Troubleshooting	Authenication Authorization Accounting	Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default VISABLED	
Add Wizard				×
			Basic	
	SERVER	SERVER GROUP ASSOCIATION	Basic MAP AAA	Advanced
RADIUS RADIUS	SERVER TACACS+ LDAP	SERVER GROUP ASSOCIATION		Advanced
RADIUS 🖌		SERVER GROUP ASSOCIATION		Advanced
RADIUS 🔽		SERVER GROUP ASSOCIATION		Advanced
RADIUS RADIUS	TACACS+ LDAP	SERVER GROUP ASSOCIATION		Advanced
RADIUS RADIUS RADIUS Name* IPv4 / IPv6 Server Address*	TACACS+ LDAP	SERVER GROUP ASSOCIATION		Advanced
RADIUS RADIUS Name* IPv4 / IPv6 Server Address* PAC Key	TACACS+ LDAP	SERVER GROUP ASSOCIATION		Advanced

Add Wizard		
Le .		Basic Advanced Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
RADIUS		
Name*	freerad	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none 🔻	
Dead-Time (mins)	1-1440	_
Available Servers	Assigned Servers]
freerad		
v	*	1
♦ Previous		Next 🗲
n k d Wizard		×
		Basic Advanced
SERVER	SERVER GROUP ASSOCIATION	
General 📝 Authentication	Authorization 🖌 Accounting 🗌	
General Authentication Aut	horization	
aa_dot1x_system_auth_control	ENABLED	
ocal Authentication	Default 🔻	
ocal Authorization	Default	
Radius Server Load Balance	DISABLED	
Show Advanced Settings >>>		
← Previous		冒 Save & Apply to Device
- Troviddo		E save a Apply to Device

dd Ņ Vizard		
		🖲 Basic 🔿 Advand
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
General 🗹 Authentic	ation 🖌 Authorization 🖌 Accounting 🗌	
General Authentication	Authorization	
ethod List Name*	dot1x	
/pe*	dot1x 🔻	
roup Type	group v	
allback to local		
railable Server Groups	Assigned Server Groups	
adius 🔹	> freerad	
ad-group adgrp_branch 🗸	×	
← Previous		⊂ 🛱 Save & Apply to Devic
d Wizard		×
		Basic Advanced
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
ieneral 📝 Authenticat	ion 🖌 Authorization 🖌 Accounting 🗌	
eneral Authentication	Authorization	
thod List Name*	authz	
ce*	network	
оир Туре	group 🔻	
llback to local		
ailable Server Groups	Assigned Server Groups	
adius 🔺 lap acacs+	> freerad	
ad-group	< 	
← Previous		Save & Apply to Device

Step2 Create an SSID on the controller for dot1x authentication.

To create an SSID navigate to Configuration >Tags& profiles >WLANs.



Defines the method list created for dot1x on the WLAN AAA settings.

Add WLAN				×
General 🗟	Security		Advanced	^
Layer2	Layer3		ААА	
Layer 2 Security Mode	WPA + 1	WPA2	2 0012 001	
			Fast Transition	Adaptive Enabled
MAC Filtering			Over the DS	
Protected Management Fran	TIÐ		Reassociation Timeout	20
PMF	Disabled	t ▼ k		
WPA Parameters				
WPA Policy				*
Cancel				🖁 Save & Apply to Device 🔵
WIRELESS NETWORKS				
+ Add X Delete E				
Number of WLANs selected : 0				
Name	Add WLAN			×
open_wlan	General	Security	Adva	nced
≪ ≪ 1 ▷ ▷ [10 ▼	Profile Name*	dot1x_wlan	Radio Policy	All
×	SSID	dot1x_wlan	Broadcast SSID	ENABLED
45	WLAN ID*	2		
	Status	ENABLED		
	Cancel			冒 Save & Apply to Device

Step3 Create a policy profile enable local switching and central authentication on the profile.

Q Search Menu Items	Interface	Services
📰 Dashboard	Logical Ethernet Wireless	AireOS Config Translator Application Visibility Cloud Services
Monitoring > Configuration >	문 Layer2 VLAN	Custom Application IOx Multicast
Administration	VTP Radio Configurations CleanAir	NetFlow Python Sandbox QoS
₩ Troubleshooting	High Throughput Media Parameters Network Parameters	RA Throttle Policy Tags & Profiles AP Join Flex
	RRM Routing Protocols OSPF Decurity	Policy RF Tags WLANs
	AAA ACL Advanced EAP	Wireless Access Points Advanced Air Time Fairness
	PKI Management Local EAP	Air Time Fairness Fabric

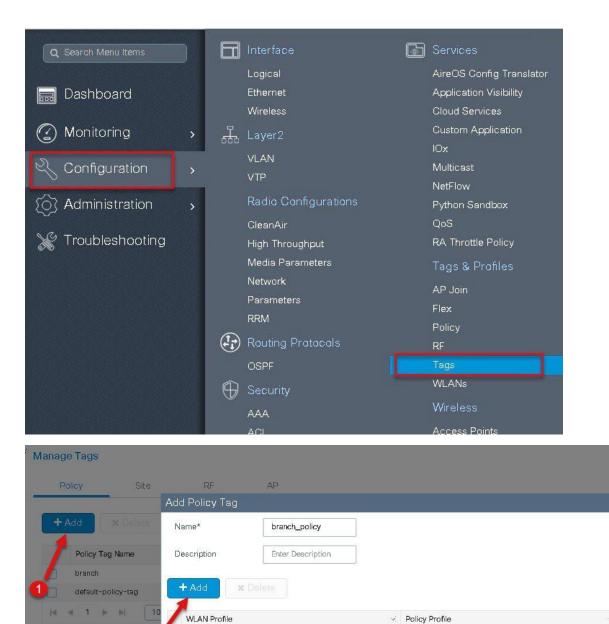
Policy Profile				
	dd Policy Profile General Access Po		Mobility	× Advanced
	A Configurir	ng in enabled state will result in loss of con	WLAN Switching Po	
	Description Status		Central Switching Central Authentication Central DHCP	
	Passive Client Encrypted Traffic Analytics CTS Policy		Central Association	
	Inline Tagging SGACL Enforcement Default SGT	2-65519		
	"Cancel		[冒 Save & Apply to Device

Step4 Map the Default VLAN for the WLAN.

General Access Policie	QOS and AVC	Mobility	A	dvanced	
WLAN Local Profiling		WLA	N ACL		
HTTP TLV Caching		IPv4 A	ACL	Search or Select	•
RADIUS Profiling		IPv6 A	ACL .	Search or Select	•
DHCP TLV Caching		URL	Filters	<u>N-</u>	
Local Subscriber Policy Name	Search or Select.	Pre A	uth	Search or Select	•
VLAN		- Post /		Search or Select	
VLAN/VLAN Group	10 🔻	Post	Autri	Gearch or Select	
Multicast VLAN	Enter Multicast VLAN	-			

Step5 Map the WLAN to policy profile.

Navigate to configuration > Tag and create a policy tag mapping the WLAN and policy profile



10 🔹 items per page

3

Policy Profile*

•

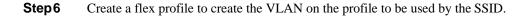
dot1x_wlan

No items to display

v

dot1x_wlan

l Save & Apply to Devic



🕽 Cancel

WLAN Profile*

2

4 0 > >

Map WLAN and Policy

Q Search Menu Items	Logical	Services AireOS Config Translator
詞 Dashboard	Ethernet Wireless	Application Visibility Cloud Services
Monitoring > Configuration >	Layer2 VLAN VTP	Custom Application IOx Multicast
Image: Contraction in the second s	Radio Configurations CleanAir	NetFlow Python Sandbox QoS
₩ Troubleshooting	High Throughput Media Parameters Network	RA Throttle Policy Tags & Profiles AP Join
	Parameters RRM	Flex Policy
	OSPF	RF Tags
	Security AAA	WLANs Wireless
	ACL Advanced EAP	Access Points Advanced
	PKI Management Local EAP	Air Time Fairness Fabric

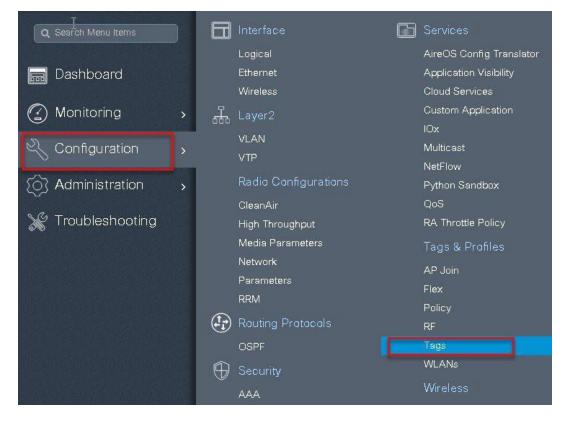
Flex Profile	dete				
4					
Flex Profile Nar	ne Add Flex Profile		✓ Descrip	tion	×
efault-flex-p	ander og en stor	Authentication Policy ACL	VLAN		
	Name*	branch_flex_profile	Multicast Overridden Interface	s 🔲	
	Description	Enter Description	Fallback Radio Shut		
	Native VLAN ID	3	Flex Resilient		
L. L	HTTP Proxy Port	0	ARP Caching		
	HTTP-Proxy IP Address	0.0.0.0	Efficient Image Upgrade		
	CTS Policy		Office Extend AP Join Minimum Latency		
	Inline Tagging		John Minimum Catericy	U	
	SGACL Enforcement				
	CTS Profile Name	default-sxp-profilex 🔹			
	Cancel				Save & Apply to Device
Add Flex Prof	ile				
General	Local Authentic	ation Policy ACL	VLAN		
Radius Server	Group	freerad 🔹	LEAF	3	
EAP Fast Profi	la la	Select Profile	PEAF	5	
LAFTASTITO	e		TLS		
Users			RADI	US	
+ Add	🗙 Delete				
Userna	me		*		
	▶ ▶ 10	- Itoms por page			
		▼ items per page No items t	o display		
			ECONVERSION CONTRACTOR		

d Flex Profile General Lo	cal Authentication Policy ACL VLAN			
+ Add 🛛 🗶	Delate.			
VLAN Name	v. ID v. ACL Name v. v.			
< 0 V>	No items to display	VLAN Name*	10	
	No tenta to diapray	VLAN Id*	1q	
	\mathbb{R}^{2}	ACL Name	Select ACL	
		✓ Save	Cancel	
		1		
9 Cancel			🗎 Save & Ap	pply to Devi

Step7

Create a site tag and map the flex profile on the site tag.

Uncheck the "Enable local site " to add the flex profile on the site tag .



Manage Tags				
Palicy	Site RF	AP		
+ Add	Add Site Tag		•	
Site Tag Name	Name*	site_tag		
1 55	Description	Enter Description		
branch sand-site	AP Join Profile	default-ap-profile 🔻		
default-site-tag	Flex Profile	branch_flex_profile		
H 4 1 F H	Control Plane Name			
	Enable Local Site			
	Cancel		🗎 Save & Apply to De 4	1

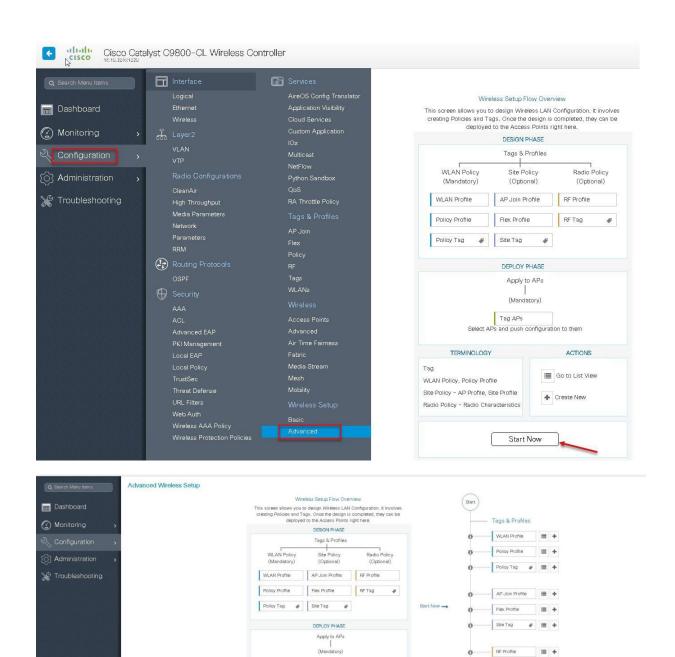
Step8 Map the policy profile and site tag on the AP. To tag the AP open the advanced config wizard and tag the AP with corresponding tags.

The mapping can be provisioned by creating a filter list based on the AP name.

Assigning a site tag on a AP might result in AP reboot due to conversion to flexconnect mode.

The reboot is avoided if the AP is already in flexconnect mode.

Navigate to Configuration > wireless setup > Advanced



Tag APs Select APs and push configu

ACTIONS

🔠 Go to List View

+ Create New

TERMINOLOGY

Radio Policy - Radio Characteristics

WLAN Policy, Policy Profile Site Policy - AP Profile, Site Profile

Tag

0----- RF Tag

Apply

Tag APs

0

∉ ≡ +

-

103

earch Menu Items	dvanced Wireless Setup													B
ashboard	Start	* (+)	Tag APs											
fonitoring >	Tags & Profiles		er of APs: 3 ed Number of APs: 3	•										
ionfiguration >	0 ······ WLAN Profile		AP Nome V AP N	fodel - AP MAC	AP	- Admin Status	< Operation Status	< Policy < Tag	Site < Tag	RF Tag 🗸	Location	Gountry v	Hyperiocation Method	n
dministration >	Policy Profile	+		AP3802I-B- 0081.c4a0	6fe0 Flex	Disabled	Registered	sand-policy		default-rf- tag	default location	us	Local	
roubleshooting	🚯 Policy Tag 🛷 🔳	*	sp-2 K9	AP38021-8- 0081.c4a0		Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	us	Local	
				CAP3702I- 80e0.1d7b	8610 Flex	Enabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
		*		Thems ber page									1.5 9.01 9 1410	
	 € Flex Profile € Site Tag 	+												
	G	T												
	RE Profile	+												
	0 RF Tag # 🔳	+												
	Apply													
	O Tag APs													
	Done													
dvanced Wire	alace Catur													
avanced vin	sicos ociap													
\sim			*											
Start				🕂 Tag APs										
Start														
Start			Nur	nber of APs: 3										
Start	• Tags & Profiles		Nur											
	-	iai	Nur Sele	nber of APs: 3		•				AP	×	Admir	1 ×	
Start	Tags & Profiles		Nur	nber of APs: : ected Number AP			~ A	P MAC	×	AP Mode		Admir Status		
	WLAN Profile		Nur Sek	nber of APs: : acted Number AP Name	of APs: 3	lodel				Mode		Status	1	1
	-		Nur Sek	nber of APs: : acted Number AP Name	of APs: 3			P MAC 081.c4a0					1	1
	WLAN Profile		Nur Sek	nber of APs: : acted Number AP Name ap1-3800	of APs: 3 AP M AIR-4 K9	lodel				Mode		Status	1	
	WLAN Profile		Nur Sek	nber of APs: : acted Number AP Name ap1-3800	of APs: 3	lodel				Mode		Status	1	
0	WLAN Profile		Nur Sek	nber of APs: : acted Number AP Name ap1-3800 ap2-3	of APs: 3 AP M AIR-4 K9 ag APs	lodel				Mode		Status	1	
0	WLAN Profile		Nur Sek	nber of APs: : acted Number AP Name ap1-3800 ap2-3	of APs: 3 AP M AIR-4 K9	lodel				Mode		Status	1	
0 0	WLAN Profile Policy Profile Policy Tag		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 T ap1-3	of APs: 3 AP M AIR-A Ag APs ag APs Tags	lodel	-B- 0(081.c4a0	.6fe0	Mode		Status	1	
0	WLAN Profile		Nur Selu + V	nber of APs: : ected Number AP Name ap1-3800 ap2-3 T ap1-3	of APs: 3 AP M AIR-4 K9 ag APs	lodel		081.c4a0		Mode		Status	1	
0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile 		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 T ap1-3	of APs: 3 AP M AIR-A Ag APs ag APs Tags	lodel	-B- 0(081.c4a0	.6fe0	Mode		Status	1	
0 0	 WLAN Profile Policy Profile Policy Tag 		Nur Sek	nber of APs: : acted Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-A Ag APs ag APs Tags	lodel	-B- 0(081.c4a0 policy	.6fe0	Mode		Status	s ed	
0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile 		Nur Sek	nber of APs: : acted Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-7 Ag APs ag APs Tags Policy	lodel	-B- OI	081.c4a0 policy	.6fe0	Mode		Status	s ed	
0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile 		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-4 Ag APs ag APs Tags Policy Site	lodel	-B+ of branch- site_tag	D81.c4a0 policy	.6fe0	Mode		Status	s ed	
0 0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile Flex Profile 		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-7 Ag APs ag APs Tags Policy	lodel	-B- OI	D81.c4a0 policy	.6fe0	Mode		Status	s ed	
0 0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile Flex Profile 		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-4 K9 ag APs Tags Policy Site RF	lodel 1938021- ((-B- Or branch- site_tag default-r	D81.c4a0 policy rf-tag	.6fe0	Mode Flex		Status	s ed	
0 0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile Flex Profile Site Tag 		Nur Seli	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-4 K9 ag APs Tags Policy Site RF	lodel 1938021- ((-B- Or branch- site_tag default-r	D81.c4a0 policy	.6fe0	Mode Flex		Status	s ed	
0 0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile Flex Profile 		Nur Sek	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-4 K9 ag APs Tags Policy Site RF	lodel 1938021- ((-B- Or branch- site_tag default-r	D81.c4a0 policy rf-tag	.6fe0	Mode Flex		Status	s ed	
0 0 0 0	 WLAN Profile Policy Profile Policy Tag AP Join Profile Flex Profile Site Tag 		Nur Seli	nber of APs: : ected Number AP Name ap1-3800 ap2-3 ap1-3	of APs: 3 AP M AIR-4 K9 ag APs Tags Policy Site RF	lodel 1738021- (((((((((((((((((((-B- Or branch- site_tag default-r	D81.c4a0 policy rf-tag	.6fe0	Mode Flex	reconr	Status	s ed	

AP as Radius Server

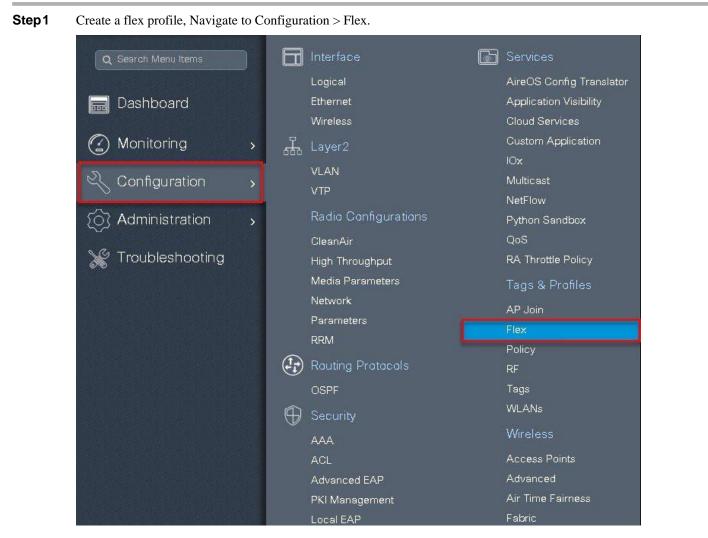
FlexConnect AP can be configured as a RADIUS server for LEAP client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will do dot1x authentication on the AP itself using the local radius facility.

Procedure

To have the flexconnect AP configured as the radius server repeat the steps 2,3,4,5,7 and 8 in the procedure section of Local Authentication with External radius server 1.

The flex profile needs to be reconfigured to enable local radius server functionality.

Procedure



Step2Specify the native VLAN ID for the AP, on the local authentication specify the EAP methods to be used.Add local users for authentication on the AP, the local users resides on the AP.

Ad Flex Profile				×
General Local	Authentication Policy ACL	VLAN		
Name*	branch_flex_profile	Multicast Overridden Interface		
Description	Enter Description	Fallback Radio Shut		
Native VLAN ID	2	Flex Resilient		
	0	ARP Caching		
HTTP Proxy Port		Efficient Image Upgrade		
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP		
CTS Policy		Join Minimum Latency		
Inline Tagging				
SGACL Enforcement				
CTS Profile Name	default-sxp-profilex			
Cancel				Save & Apply to Device
Jeancer				
Add Flex Profile				×
General Local A	Authentication Policy ACL	VLAN		
Radius Server Group	Select Server Group	LEAP		
EAP Fast Profile	Select Profile	PEAP		
		TLS		
2. • • • • • • • • • • • • • • • • • • •		RADIUS		
+ Add × Del		<u>.</u>		
Username		**		
IA A 0 0 H	10 🔹 Items per page	Username *	sample	
	No items to (Password Type		
		Password *		
		Confirm *	· · · · · · · · · · · · · · · · · · ·	
		Password		
		✓ Save	Canc	el
Cancel		2	(Save & Apply to Dev

eneral Local Authentication Policy ACL	VLAN		
► Add X Delete			
VLAN Name 🤟 ID 🗟 ACL Name	× 🖣 🛌 💶		
 ■ 0 ► ► 10 T items per page 	VLAN Name*	10	
No items to	display VLAN Id*	ıq	
	ACL Name	Select ACL	
<u>∫</u> ₹	✓ Save	🕤 Cancel	
	1		
Cancel			& Apply to De

CCKM/OKC and **PMKC**aching

CCKM /OKC and PMK caching enables fast roaming for wireless clients .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 controller supports CCKM/OKC and PMK caching, the controller takes care of distributing the master key to the AP's. The controller distributes the master key to all the Ap's whose site tag and policy tag are the same, this results in ability to do fast roaming across the AP within the same site. The distribution of the master key is done based on the site tag of the AP site the client initially associates, the controller now find's all the AP's which has a similar site tag and policy tag and pushes the master key on those AP' and thus enabling fast roaming among the AP's.

Limitation

- The AP in standalone mode can support a maximum of two radius servers, the first server added in the server group acts as the primary. The second radius server acts as a backup for the primary.
- The AP as radius server is supported only on Wave 1 AP's . On 16.10 the EAP method supported for AP as radius server is EAP-LEAP.
- Fast roaming is not supported with default site-tag, if the AP's are mapped to a default site tag then the master key for caching is not shared among those APs.

Peer to Peer Blocking

The Controller supports peer to peer blocking in local switching mode, the configuration for the peer to peer blocking is available while creating the WLAN.

Peer to peer blocking can be configured with any of the following 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.

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.

Steps

Procedure

Refer the steps defined in the advanced config wizard of this document to create an SSID, policies and tags on the controller.

Advanced wireless setup wizard

Select the peer to peer blocking action in the advanced tab of the WLAN creation to have the feature configured.

Add WLAN			×
General	Security	Advanced	
Coverage Hole Detection		Universal Admin	
Aironet IE		Load Balance	
Diagnostic Channel		Band Select 🗹	
P2P Blocking Action	Disabled 🗸	IP Source Guard	- 1
Multicast Buffer	Disabled Drop	WMM Policy Allowed v	
Media Stream Multicast- direct	Forward-UpStream	Off Channel Scanning Defer	
Max Client Connections		Defer Priority 0 1 2	
Per WLAN 0		3 4 75	-
Cancel		☐ Save & Apply to D	evice

Once the P2P Blocking action is configured on the WLAN configured it is pushed from the WLC to the FlexConnect APs. The config will be retained by the AP when it moves from connected mode to standalone mode.

FlexConnect ACL

ACL usage on FlexConnect deployment provides a way to cater the need to provide 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 on a flex profile which is mapped to a site tag. The site tag gets assigned to an AP. The ACL name can also be returned as part of an attribute from AAA.

Summary

The ACL implementation for branch deployments can be done through the following methods:

- WLAN ACL The ACL applied on the WLAN dot11 interface and is enforced to all the client connecting on that SSID
- WLAN ACL The ACL applied on the WLAN dot11 interface and is enforced to all the client connecting on that SSID
- Client ACL- The ACL returned as part of the AAA attribute and is enforced for the specific client

The ACL for the enforcement needs to be created on the WLC and also needs to be pushed to the Flex AP, the way to push the ACL to the flex AP is using the flex profiles. An administrator can create policy ACL on the flex profile to push the ACL on the AP or use a dummy VLAN to ACL mapping on the flex profile. When a wireless client joins an SSID and an ACL is enforced either through WLAN/VLAN or AAA, the WLC checks if the ACL is also pushed to the AP. If the ACL is not present on the AP the client is moved to exclusion list .

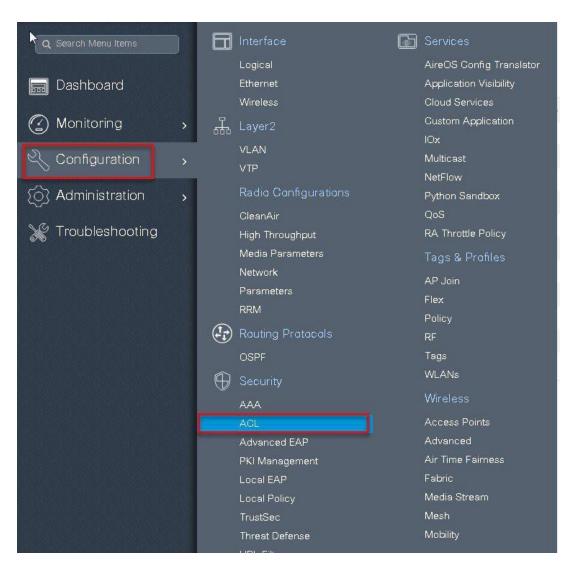
Procedure for WLAN ACL

Procedure for WLAN ACL

- Create an ACL on the controller.
- Apply the ACL on the respective policy profile for the WLAN
- Now create a flex profile and add a policy ACL and map the corresponding ACL on the flex profile.
- Also add the ACL as part of the policy profile
- Connect the client and validate the ACL works.

Procedure

Step1 Create an ACL on the WLC by navigating to Configuration7 Security 7 ACL.



Step 2 Perform the following steps:

- Click on Add to create an ACL, define an ACL name.
- Specify the type of ACL-Standard or Extended
- Define the rules for the ACL
- Specify the action as permit or deny
- Add the ACL rules and save the ACL

Q. Search Menu Items	Access Control	List				
📻 Dashboard	+ Add	🖒 🖉 🖉 Associatir	ng Interfaces			
		ACL-REDIRECT	ACL Name		V IPv4 Exten	ACL Type
S Configuration	, <u> </u>	F Add ACL Setup				×
Administration		fit ACL Name*	flex_acl_11	ACL Type	IPv4 Extended 🗸	
∽ ₩ Troubleshooting		in Rules				2
000		pi Sequence*	1	Action	deny 🗸]
		in Source Type 3	any 🔹		4	
		pi Destination Type	any 🔻		-	
	≪ 1 >	Protocol	ahp			
		Log		DSCP	None]
		+ Add 🛛 🗱 Del				
		5 equence <	Source - Source -	 Destination < Destinati IP Wildcar 		Destination × Port DSCP × Log ×
		< < 0 > >	10 🔻 items per page			No items to display
		Cancel				🖀 Save & Ap 6 to Device

Step3 Refer the steps in the procedure of advanced configuration wizard for the following :

- Create a WLAN
- Creation of policy profile (refer the screenshot below to add the ACL)
- Policy tag mapping
- Flex profile (refer the screenshot below to map the ACL using the Policy ACL)
- Creation of Site Tag
- Tagging the AP

Advanced wireless setup wizard.

The ACL is attached to the WLAN through the policy profile.

General Access P	Policies QOS a	and AVC	Mobility	Advar	nced	
🛦 Configur	ring in enabled state will res	ult in loss of conr	ectivity for clients	associated wit	h this profile.	
Name*	open_wlan		WLAN Switch	ing Policy		
Description	Enter Description		Central Switchi	ng		
Status			Central Authen	ication		
Passive Client	DISABLED		Central DHCP			
Encrypted Traffic Analytics	DISABLED		Central Associa	ition		
CTS Policy			Flex NAT/PAT			
Inline Tagging						
SGACL Enforcement						
Default SGT	2-65519					
Derault Out	2-03313					
					Save & Apply t	o Dev
Cancel Policy Profile General Access P	Policies QOS a	and AVC	Mobility	Advar		o Dev
d Policy Profile	ⁱ olicies QOS a	and AVC				to Dev
d Policy Profile General <u>Access P</u>	^t olicies QOS a	and AVC	WL	Advar AN ACL		
Policy Profile General Access P MLAN Local Profiling	^t olicies QOS a	and AVC	WL IPv2	Advar AN ACL ACL	nced	
Policy Profile General Access P MLAN Local Profiling ITTP TLV Caching	Policies QOS a	and AVC	IPv4	Advar AN ACL	nced flex_acl_11	
Policy Profile General Access P MLAN Local Profiling ITTP TLV Caching ADIUS Profiling	Policies QOS a		WL IPva IPva UR	Advar AN ACL ACL	nced flex_acl_11	 • •
Policy Profile General Access P MLAN Local Profiling ITTP TLV Caching ADIUS Profiling OHCP TLV Caching			WL IPv4 IPv4 UR Pre	Advar AN ACL ACL	nced Rex_acl_11 Search or Select Search or Select	
Policy Profile General Access P WLAN Local Profiling ITTP TLV Caching IADIUS Profiling IHCP TLV Caching ocal Subscriber Policy Name			WL IPv4 IPv4 UR Pre	Advar AN ACL ACL	nced flex_acl_11 Search or Select	
Policy Profile General Access P MLAN Local Profiling ITTP TLV Caching MADIUS Profiling OHCP TLV Caching ocal Subscriber Policy Name	Search or Se	elect	WL IPv4 IPv4 UR Pre	Advar AN ACL ACL	nced Rex_acl_11 Search or Select Search or Select	

Step4 Assign the ACL on the Flex profile , by mapping the VLAN and ACL.

General Loca	al Authentication Policy AC	CL VLAN	
lame*	branch_flex_profile	Multicast Overridden Interface	
Description	Enter Description	Fallback Radio Shut	
lative VLAN ID	2	Flex Resilient	
		ARP Caching	
ITTP Proxy Port	0	Efficient Image Upgrade	
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	
CTS Policy		Join Minimum Latency	
nline Tagging			
GACL Enforcemen	t 🔲		
CTS Profile Name	default-sxp-profile _x		

Define the native VLAN for the flexconnect AP's.

Step5 Push the ACL to AP by using the Policy ACL configuration on the flex profile .

+ Add 🛛 🗶 De	lete	
ACL Name	Central✓Pre Auth✓WebauthURL Filter	ACL Name* Tex-acl11
< 0 н н	10 🔻 items per page No items to display	Central Webauth
		Pre Auth URL Filter
		Save Gancel

Step6 Verification on the controller.

Navigate to Monitoring > Wireless > Clients

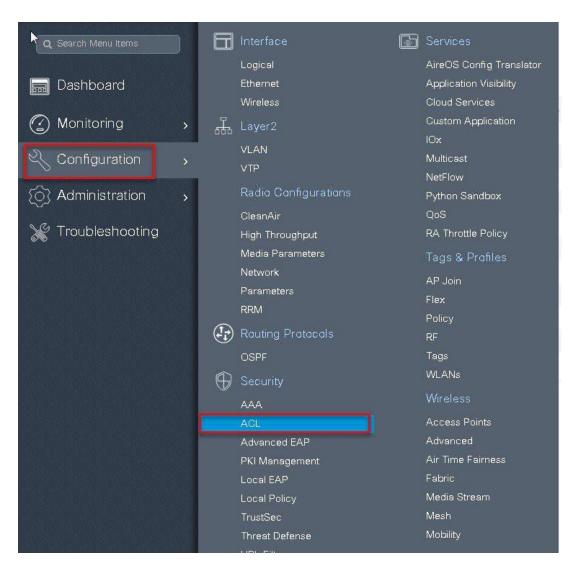
lients			Client	
Clients Sleeping C	lients Excluded Clients			Statistics Mobility History Call Statistics
			Client Properties AP Properties	Security Information Client Statistics QOS Properties
# Delete			Auth Method Status List	
			Method	Dot1x
Fotal Client(s) in the Network: 1			SM State	AUTHENTICATED
Client MAC Address	V IPv4/IPv6 Address	< AP Name	SM Bend State	IDLE
			Local Policies	
1c:36:bb:ef:64:92	9.1.11.252	sand-ewic-ap-1		
4 4 1 > 10 - items	per page		Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
			Absolute Timer	1800
click on Mac addres	SS		VLAN	
			Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
			Absolute Timer	1800
			VLAN	11
			Server Policies	
			Filter-ID	flex_acl_12
			Output SGT	0011-34
			Filter-ID	flex_acl_12
			Output SGT	0011-34
			Resultant Policies	
			Filter-ID	flex_acl_12
			Output SGT	0011-34
			VLAN	11
			Absolute Timer	1800
			Filter-ID	flex_acl_12

Procedure for VLAN ACL

- Create an ACL on the controller.
- Create a flex profile and add a VLAN mapped to the WLAN.
- Map the ACL on the VLAN interface.
- Connect the client and validate the ACL works.

Procedure

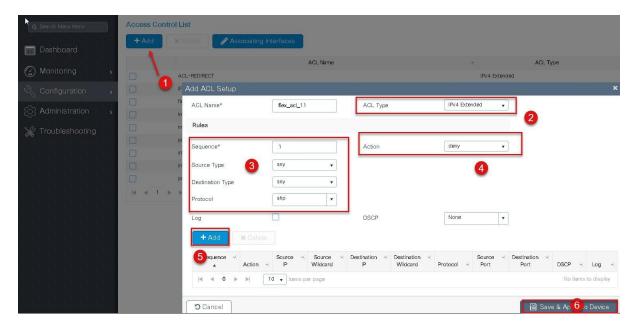
Step1 Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step 2

Perform the steps below:

- Click on Add to create an ACL, define an ACL name.
- Specify the type of ACL Standard or Extended
- Define the rules for the ACL
- Specify the action as permit or deny
- Add the ACL rules and save the ACL



Step3 Refer the steps in the procedure of advanced configuration wizard for the following:

- Create a WLAN
- Creation of policy profile
- Policy tag mapping
- Flex profile creation
- Creation of Site Tag
- Tagging the AP

Advanced wireless setup wizard

The ACL is attached to the WLAN through the policy profile.

Add Policy Prof	ile				×
General	Access Policies	QOS and AVC	Mobility	Advanced	
	A Configuring in enabled	state will result in loss of c	onnectivity for clients assoc	ciated with this profile.	
Name*	open_1	wlan	WLAN Switching F	Policy	
Description	Enter D	escription	Central Switching		
Status	ENABLE		Central Authenticatio	on 🔽	
Passive Client		ABLED	Central DHCP		
Encrypted Traf	ffic Analytics	ABLED	Central Association		
CTS Policy			Flex NAT/PAT		
Inline Tagging					
SGACL Enforc	ement				
Default SGT	2-655	19			
Cancel				📓 Save & Apply t	o Device

General	Access Policies	QOS and AVC	Mobility	Advanced	
WLAN Local F	Profiling		WLA	N ACL	
HTTP TLV Cach	ning		IPv4 /	ACL Search or S	ielect 🔹
RADIUS Profilin	g		IPv67	ACL Search or S	elect 🔻
DHCP TLV Cac	hing		URL	Filters	
Local Subscribe	er Policy Name	Search or Select	Pre A	uth Search or S	ielect 🔻
VLAN			Post	Auth Search or S	elect 🔹
VLAN/VLAN Gr	oup	10	(031)		
Multicast VLAN		Enter Multicast VLAN			

Step4 Assign the ACL on the Flex profile, by mapping the VLAN and ACL.

Define the native VLAN for the flexconnect AP's.

flex_profile	Multicast Overridden Interface Fallback Radio Shut Flex Resilient ARP Caching			
scription	Flex Resilient ARP Caching			
	ARP Caching			
	Efficient Image Upgrade			
	Office Extend AP			
	Join Minimum Latency			
xp-profile _x				
	sxp-profile _x	Join Minimum Latency	Join Minimum Latency	Join Minimum Latency

Step5 Define the VLAN and ACL mapping on the flex profile.

eneral Local Authentication Policy ACL	0	
Add Selete		
ALAN Name 🗸 ID 🗸 ACL Name 🗸 🗸		
	VLAN Name*	10
No items to display	VLAN Id*	1 to 4096
	ACL Name	flex_acl_11
	✓ Save	Cancel
	4	
Cancel	1	📔 Save & Apply to I

Client ACL overview

- This feature allows application of Per-Client ACL for locally switching WLANs.
- Client ACL is returned from the AAA server on successful Client authentication.
- The AP needs to be provisioned with the ACL by using the policy ACL or dummy vlan acl mapping on the flex profile.
- The ACL will be pushed to all the AP's that has the same site tag and policy tag mapped.
- 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 name 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 same site tag and policy tag.

Procedure for Client ACL

- Create an ACL on the controller
- Create a Dot1x based SSID
- Enable AAA override on the policy profile
- Return the ACL name as part of the AAA access-accept from AAA

For the creation of ACL refer the steps in the WLAN ACL use case .Refer the step5 in the WLAN ACL section to push the ACL on to the AP.

Procedure for WLAN ACL

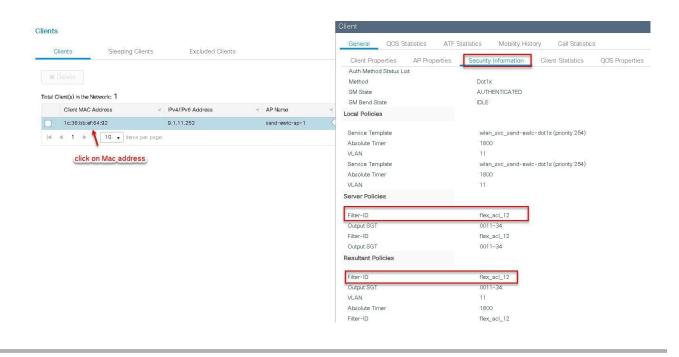
For creating a dot1x WLAN and enabling AAA override, refer the procedure section of the VLAN override Use case

Flexconnect VLAN override

Procedure

	d-acl
Authorization Profile	
* Name	sand-acl
Description	
* Access Type	ACCESS_ACCEPT *
Network Device Profile	🔐 Cisco 🔹 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
DACL Name	
ACL (Filter-ID) Security Group VLAN	[flex_ad_12] in
Security Group VLAN Advanced Attribut	tes Settings
Security Group	
Security Group VLAN Advanced Attribut	tes Settings
Security Group VLAN Advanced Attribut Select an item Attributes Details	tes Settings
Security Group VLAN Advanced Attribut	tes Settings
Security Group VLAN Advanced Attribut Select an item Attributes Details Access Type = ACCESS 4	tes Settings

Step2verification of ACL getting enforced on the AP and WLC .Navigate to Monitor > wireless >Clients



Limitations

- The use of downloadable ACL is not supported on flex connect local switching, downloadable ACL are only supported for central switching.
- In case of central authentication if an ACL is returned from the AAA server but the corresponding ACL is not present on the AP, the client will be excluded with the reason as ACL failure.
- In case of the Local authentication the client will be Deauthenticated continuously

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. For the AP preimage download to work the controller should be install mode of operation. If the controller is running in bundle mode, first have it converted to install mode before proceeding to AP pre-image download.

Summary

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

Procedure

Procedure

Step1 Copy the image on the controller flash and the add the file using the install command.

wlc-2#install add file bootflash:wlc9500C-universalk9.BLD_V1610_THROTTLE_ 010435.SSA.bin

The install file command runs base compatibility checks on a file to ensure that the package is supported on the platform. It also adds an entry in the package, so that its status can be monitored and maintained.

wlc-2 [Cha State	2#sh issis (St)	install summary 1] Installed Package(s) Information:): I - Inactive, U - Activated & Uncommitted, C - Activated & Committed, D - Deactivated & Uncommitted
Type	St	Filename/Version
IMG IMG	Ċ	16.10.1.0.1026 16.10.1.0.41
Auto	abort	timer: inactive

Step2 Once the file is added, the image can be pushed to the Ap using the following CLI :

"ap image predownload"

wlc-2# wlc-2#ap image p wlc-2#ap image predownload wlc-2#ap ap image wlc-2#ah ap image lotal number of APs: 3						
Number of APs Initiated Predownloading Completed predownloading Not Supported Failed to Predownload AP Name	: 0 : 3 : 0 : 0 Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry Time	Ret
ар-1-3800 ар-2-3800 ар-1-3700	16.10.1.37 16.10.1.37 16.10.1.37 16.10.1.37	16.11.1.11 16.11.1.11 0.0.0.0	Predownloading Predownloading Predownloading	16.10.1.33 16.10.1.33 16.10.1.33	0 0 0	

Once the download is completed on the AP, issue the following CLI to swap the image and reset the AP.

- ap image swap
- ap image reset

wlc-2#sh ap image Total number of APs: 3 Number of APs Initiated Predownloading Completed predownloading Not Supported Failed to Predownload					
Failed to Predownload AP Name	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry T
ap-1-3800 ap-2-3800 ap-1-3700	16.10.1.37 16.10.1.37 16.10.1.37 16.10.1.37	16.10.1.33 16.10.1.33 16.10.1.33 16.10.1.33	Complete Complete Complete Complete	16.10.1.33 16.10.1.33 16.10.1.33	0 0 0
wlc-2#ap image swap wlc-2#sh ap image Total number of APs: 3					
Number of APs Initiated Predownloading Completed predownloading Not Supported Failed to Predownload					
AP Name	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry T
ар-1-3800 ар-2-3800 ар-1-3700	16.10.1.33 16.10.1.33 16.10.1.33	16.10.1.37 16.10.1.37 16.10.1.37 16.10.1.37	Complete Complete Complete Complete	16.10.1.33 16.10.1.33 16.10.1.33	0 0 0
wlc-2#ap image reset wlc-2#					

Step3 After the AP has been reset, using the following CLI to activate the image on the controller.

"Install Activate"

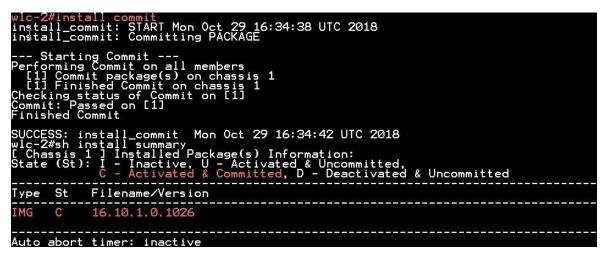
The Install activate runs compatibility checks, installs the package, and updates the package status details. For a non-restartable packages it triggers a reload. The systems will prompt for saving the config and a reboot during the process . Please input the response to save the config and reboot the WLC.

wlc-2 [Cha State	2#sh i assis e (St)	nstall summary 1] Installed Package(s) Information: : I - Inactive, U - <mark>Activated & Uncommitted,</mark> C - Activated & Committed, D - Deactivated & Uncommitted
		Filename/Version
IMG	U	16.10.1.0.1026
Auto	abort	timer: active on install_activate, time before rollback - 05:57:09

Step 4 Once the systems is rebooted ,use the following CLI to have the changes persist across reboot.

"Install Commit"

Commits the activation changes to be persistent across reloads The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.



Limitation

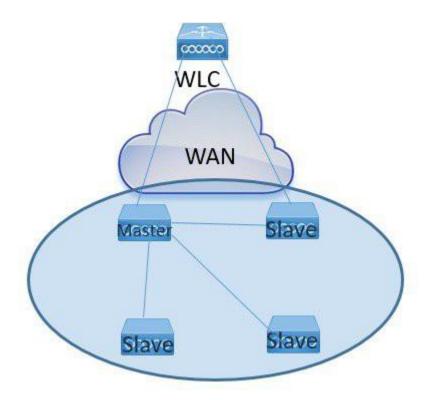
The Controller needs to be install mode for the AP pre-image to work, if a controller works in bundle mode it needs to be converted to install mode. Please refer cisco.com for the conversion for bundle mode to install mode.

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 Master/Server, and the rest of the APs of the same model will work as

Slave/Client and will pre-download the AP image from the master. 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

- Master and Slave APs are selected for each AP Model per site tag
- Master downloads image from WLC
- Slave downloads image from Master AP using tftp
- Reduces downtime and saves WAN bandwidth
- The master is choosen by the system , the AP with the lowest mac among the same type and model is to become a master

Procedure

Procedure

Step1 For steps to create a flex profile and to have it applied on the AP, refer the steps in the Advanced config wizard of the document at Advanced wireless setup wizard

Enable smart AP image upgrade on the flex profile.

Start	+ Add 🛛 🗶 Delet			
Tags & Profiles	Add Flex Profile			
	General Local	Authentication Policy AC	L VLAN	
WLAN Profile	Name*	branch_flex_profile	Multicast Overridden Interface	
Policy Profile	Description	Enter Description	Fallback Radio Shut	
O Policy Tag I	Native VLAN ID	3	Flex Resilient	
	HTTP Proxy Port	0	ARP Caching	
AP Join Profile			Efficient Image Upgrade	
Flex Profile	HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	
0 Site Tag 🕜 🔳 🕇	CTS Policy		Join Minimum Latency	
	Inline Tagging			
O····· RF Profile 🔳 🕈	SGACL Enforcement			
0 RF Tag 🕢 🔳 🕇	CTS Profile Name	default-sxp-profile _X 🔻		

Step2 Download the image on the controller as outlined in step1 of the AP image pre-download process. Issue the CLI below to initiate the smart ap image upgrade and also to see the master AP elected for a given type of AP and the also master downloading image from the controller.

AP Pre-Image Download

ap image predownload site-tag <site_name> start

It is important to give the site tag and start the pre-image download process as this would initiate the smart AP image upgrade process, if the site tag is not specified the download falls back to the normal pre-image download process.

ulc-2#sh ap master li ulc-2#sh ap master list uP Name	WTP Mac	AP Model	Site Tag			
p-2-3800 master AP	0081.c4a0.7550	AIR-AP3802I-B-K9	site_tag			
lc-2#sh ap im lc-2#sh ap image otal number of APs: 2						
umber of APs Initiated Predownloading Completed predownloadin Not Supported	9 . 00					
Failed to Predownload P Name	:0 Primary Image	Backup I	mage	Predownload Status	Predownload Version	Next Retry 1
p-1-3800 ← slave Ap p-2-3800	16.10.1.33 16.10.1.33	16.11.1. 16.11.1. 16.11.1.		None Predownloading	0.0.0.0 16.10.1.37	N/A Ø

Step3 After the image predownload on the AP is completed, follow the sequence below:

- Swap the AP image and reset the AP using the CLI "ap image swap" and "ap image reset"
- Activate the image using the "Install activate" CLI
- During the activation the WLC will go for a reboot, use the CLI install Commit to persist the changes across reboot

Number of APs Initiated Predownloading Completed predownloading Not Supported Failed to Predownload					
	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry Tim
р-1-3800 р-2-3800 р-1-3700	16.10.1.33 16.10.1.33 16.10.1.33	16.10.1.37 16.10.1.37 0.0.0.0	Complete Complete None	16.10.1.37 16.10.1.37 0.0.0.0	0 0 N/A
Jlc-2#ap im Jlc-2#ap image swap Jlc-2#sh ap image Jlc-2#sh ap image otal number of APs: 3					
Number of APs Initiated Predownloading Completed predownloading Not Supported Failed to Predownload					
P Name	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry Tim
ap-1-3800 ap-2-3800 ap-1-3700	16.10.1.37 16.10.1.37 6.3.0.1	16.10.1.33 16.10.1.33 16.10.1.33	Complete Complete None	16.10.1.37 16.10.1.37 0.0.0.0	0 0 N/A
ulc-2#ap im ulc-2#ap image rese ulc-2#ap image reset					

Limitation

The system decides on the election of a master AP and the decision on who the master is decided when the smart AP image download process is initiated. Once the decision is made any AP that joins after and which has a lower mac will not alter or change the master AP already elected.

Flexconnect Pre-auth ACL and URL filtering

The URL filtering is an extension to the ACL deployments current in place, with the addition of URL filtering the ACL can accept internet domain names in addition to the existing IP address rules. The Flexconnect deployments supports the LWA, CWA and BYOD flow. The LWA refers to the local web authentication done on the WLC while the CWA refers to the guest authentication done on the identity service engine. The BYOD flow requires access to the play store for downloading the supplicant for which URL filters can be used. The use for URL filter can also be extended to CMX connect social login where the authentication happens on the social network site.

Summary

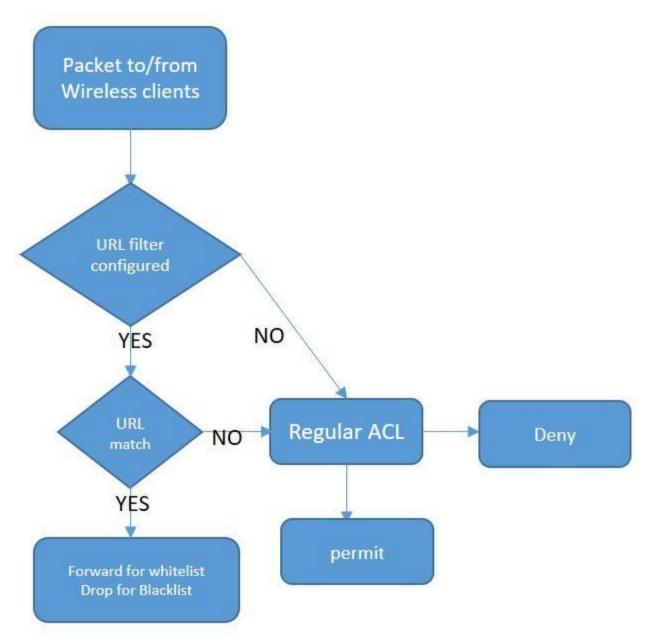
Pre-auth ACL refers to a state when a wireless client would require access to resources prior to getting authenticated. In case of the LWA/CWA or BYOD the client might require access to resources before getting full access into the network. The URL filtering for flex is supported only on the Wave 2 platforms. The url filtering follows a whitelist and black list model of working, the administrator can specify up to 20 URLS within a URL filter. The URL filter supports wild card matching to support sub URL matching.

For e.g.:

URL type	Definition
cisco*	match any URL that starts with Cisco
*cisco.com	match any URL that ends in cisco.com
www.cisco.com	match the exact string

The URL filtering ACL works along with a regular ACL, to have the URL ACL pushed to a flex AP it needs to be linked with a regular ACL in the flex profile .The URL ACL works by snooping the DNS transaction between the DNS client and a DNS server, for flex deployment the DNS snooping is performed on the AP for each client. With snooping in place, AP learns the IP address of

the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is mapped in the ACL for locally switched traffic. The rules created from DNS parsing has a permit or deny based on the URL filtering rules which is either white listing or blacklisting. When a packet from or to a client traverses through the AP, the DNS rules are processed first before proceeding with the regular ACL processing. The URL filtering is optional configuration on the LWA and CWA flow.

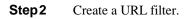


LWA flow with URL filter

This section describes the steps to set up LWA with pre-auth ACL and URL filter, for the local web authentication the pre-auth ACL and URL filtering is optional.

Procedure

Step 1	To create a URL filter navigate to Configuration > security and URL filters.								
	C Search Menu Items			Interface	Services				
				Logical	AireOS Config Translator				
	📰 Dashboard			Ethernet	Application Visibility				
				Wireless	Cloud Services				
	🕜 Monitoring	>	500	Layer2	Custom Application				
				STP	lOx				
	🔍 Configuration	>		VLAN	Multicast				
	~~			VTP	NetFlow				
	(o) Administration	>		Radio Configurations	Python Sandbox				
	💥 Troubleshooting				QoS				
				CleanAir	RA Throttle Policy				
				High Throughput	Tags & Profiles				
				Media Parameters	Air Time Fairness				
				Network	AP Join				
				Parameters	Flex				
			~	RRM	Policy				
			(††)	Routing Protocols	RF				
				OSPF	Tags				
			\oplus	Security	Wireless				
				AAA	Access Points				
				ACL	Advanced				
				Advanced EAP	Fabric				
				PKI Management	Media Stream				
				Local EAP	Mesh				
				Local Policy	Mobility				
				TrustSec	WLANs				
				Threat Defense	Wireless Setup				
				URL Filters	Basic				
				Web Auth	Alice and a second				



	List Name*	url-pre-auth	Redirect	Servers
List Nam	Туре	PRE-AUTH	IPv4	XXX.XXX.XXX
• • •	Action	PERMIT	IPv6	XIXIXIX
	URLS	Enter a URL every new line dns.cisco.com playstore.google.com	ise permit to create Wh use (deny to create a bla	ite list

Step3 Create an ACL on the WLC to link with the URL ACL.

Q Search Menu Items	Interface	Services	Access Control List		
📷 Dashboard	Logical Ethernet Wireless	AireOS Config Translator Application Visibility Cloud Services	+Add 🛛 🖉 🛶 🖉 Assoca	aling Interfaces	
	> 🖧 Layer2			ACL Name	 ACL Type
Configuration	STP	IOx Multicast	AQL-REDIRECT		Pv4 Exanded
	VLAN VTP		Add ACL Setup		
Administration	> Radio Configurations	Python Sandbox QoS	AC. Name*	fex-ad_11 ACL Type	IPv4 Stendard 💗
💥 Troubleshooting	CleanAir	RA Throttle Policy			
	High Throughput		Rules		
	Media Parameters Network Parametars RRM		Sequence"	Action (any)	pernit •
	Routing Protocols		Lag	0	
	OSPF				
	G Security		H K 1 H		
	AAA	Access Points Advanced	Sequence ~	Source - Source - Destination - Destinatio	in v Source v Destination v
	AGL Advanced EAP	Fabric		on P Widcard P Widcard	
	PKI Management	Media Stream	14 4 0 P P	10 v iterss per page	No items to disclay
	Local EAP	Mesh	17		
	Local Policy	Mobility			
	TrustSec	WLANs	Cancel		間 Save & Apply to Device

Step4 Create an Authentication list on the WLC to be used on the LWAWLAN. The authentication list can point to a Radius server or can do a local lookup.

Navigate to Configuration > Security > AAA

Authentication Au	thorization and Accounting			
+ AAA Wizard				
AAA Method L	ist Servers / Groups	AAA Advanced		
+ Add	Create AAA Radius Server			×
1	Name*	freerad		
RADIUS	IPv4 / IPv6 Server Address*	9.1.0.21		
	PAC Key			
LUMP	Key*			
	Confirm Key*			
	Auth Port	1812		
	Acct Port	1813		
	Server Timeout (seconds)	000 T - T		
	Retry Count	0-100		
	Support for CoA			
	Cancel			Bave & Apply to Device
Authentiaction Autho	rization and Accounting			
+ AAA Wizard	nzation and Accounting			
AAA Method List	Servers / Groups AAA Adv	anced		
+ Add × De	léte			
RADIUS				
TACACS+	Servers Server	Groups		
LDAP	Name	× Server 1	Server 2	Server 3
	ise	ise Items per page	N/A	N/A
		Januar 2020		

Authentication Authorization and Ad	counting		
+ AAA Wizard			
AAA Method List Serve	rs / Groups AAA Advanc	ed	
+ Add × Delete	Create AAA Radius Serve	er Group	×
RADIUS	Name*	rad-group	
TACACS+	Group Type	RADIUS	
LDAP	MAC-Delimiter	none 🔹	
	MAC-Filtering	none 🔹	
	Dead-Time (mins)	1-1440	
	Available Servers	Assigned Servers	
	ise .	freerad	
	Cancel	Save & Apply to Device	
Authentication Authorization and Accouted	nting		
+ AAA Wizard	inding		
AAA Method List Servers # C	Groups AAA Advanced		
General	Quick Setup: AAA Authe	entication	×
Authensisten	Add Method List Name*	lwa	
Authorization	Name Type* 2	login	
Accounting	dot1x_methoc Group Type	group 🔻	
i4	Fallback to local		
	Available Server Groups radius Idap tacacs+ freerad radgrp_branch	Assigned Server Groups	
	Cancel	Bave & Apply to	C <mark>4</mark> ce

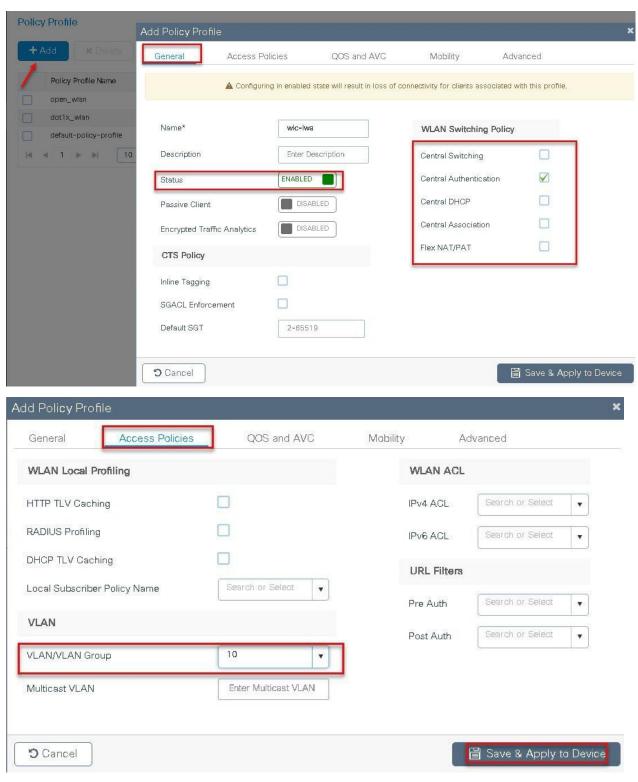
Step5Create a WLAN to local web-authentication flow.Navigate to Configuration > Tags& profiles > WLAN.

WIRELESS NETWORKS					
+ Add X Delete	Add WLAN				×
Number of WLANs selected : 0	General	Security	Advan	ced	
h Name	Profile Name*	wic-iwa	Radio Policy	All	•
open_wian	SSID	wic-lwa	Broadcast SSID		
dot1x_wlan	WLAN ID*	2			
	Status				
	Cancel			B	Save & Apply to Device
Add WLAN					×
General	Security		Advanced		
Layer2	Layer3		AAA		
			Fast Transition	A	daptive Enabled 💂
Layer 2 Security Mode	Nor	ie 🔹	Over the DS		
MAC Filtering					
			Reassociation Ti	meout	20

ſ	🕽 Cancel	1	P	Save & Apply to Device

dd WLAN				×
General	Security	Advanced		
Layer2	Layer3	AAA		
Web Policy		Show Advanced Settings	>>>	
Webauth Parameter Map	global 🔹	clicko	n Advanced ettings	
Authentication List For Local Login Method List	Iwa Select a value			
nake sure the configuration network default local' exists	aal			
Cancel			🛱 Save & Apply to Devic	e
dd WLAN				
3 2				
Web Policy		<< Hide On Mac Filter Failure		
Webauth Parameter Map	global 🔪 🔻	Conditional Web Redirect	DISABLED	
Authentication List	lwa 🔹	Splash Web Redirect	DISABLED	
For Local Login Method Li make sure the configuratio network default local' exis	on 'aaa authorization	Preauthentication ACL		
		IPv4	flex_acl_11	
		IPv6	none	
			. <u></u>	
O Cancel			📓 Save & Apply to I	Davie
Gancer				DEVICE

Step6 Create a policy profile.



Step7 Create a flex profile.

Navigate to Configuration > Tags & Profiles > Flex

Name*	branch_flex-profile	Multicast Overridden Interface	Add
Description	Enter Description	Fallback Radio Shut	G
Vative VLAN ID	3	Flex Resilient	
	0	ARP Caching	
ITTP Proxy Port	U	Efficient Image Upgrade	
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	H
CTS Policy		Join Minimum Latency	
nline Tagging			
SGACL Enforcement			
CTS Profile Name	default-sxp-profilex		

Step8Create a Site tag mapping the policy tag and flex profile.Navigate to Configuration > Tags & Profiles > Tags

Manage Tags				
Policy Site	RF	AP		
+ Add × Delete	Add Policy Tag			×
	Name*	branch_policy		
Policy Tag Name	Description	Enter Description		
branch	Beeenpuon			
default-policy-tag				
≪ ≪ 1 ≫ ≫ 10	1			
	WLAN Profile		 Policy Profile 	×
				No items to display
	Map WLAN and P	olicy		
	WLAN Profile*	wic-iwa 🗸	8 Policy Profile*	wic-iwa 🔻
	-		×	
	Cancel			Save & Apply to Device 5

Manage Tags				
Policy	Site	AP		
+ Add × D	Add Site Tag			×
Site Tag Name	Name*	site_tag		
1 ss	Description	Enter Description		
branch sand-site	AP Join Profile	default-ap-profile 🔻	_	
default-site-tag	Flex Profile 3	branch_flex_profile		
H 4 1 > >	Control Plane Name	· · · · · ·		
	Enable Local Site 2			_
	Cancel			冒 Save & Apply to De 4.

Step9 Map the tags on the AP, Once the AP's are tagged with a policy profile the AP 's will reboot due to conversion from local mode to flex-connect mode.

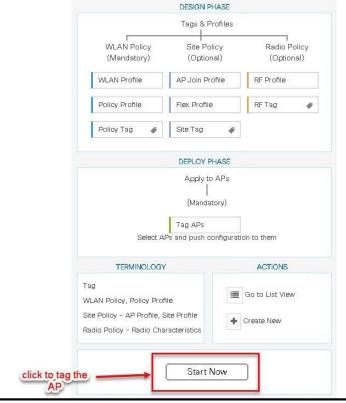
If the AP's are already in flex mode, the reboot wouldn't be triggered.

Navigate to Configuration > Wireless Setup > Advanced

Advanced Wireless Setup

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.



Advanced Wireless Set

Advanced Wireless Setup	+ Tag APs Number of APs: 3	.				
Tags & Profiles	Selected Number of	APs: 3		AP 🗸	Admin	√ Ope
🚯 WLAN Profile 📃 🕈	Name	AP Model 🛛 🗸	AP MAC 🛛 🗸		Status	Stati
OPolicy Profile	ap1-3800	AIR-AP3802I-B- K9	0081.c4a0.6fe0	Flex	Enabled	Regi
0 Policy Tag 🏼 🧳	🖌 ap2+3 Tag	APs				×gi
	ар1-3 Та	ags				gi
O AP Join Profile	Ne e 1 Po	licy bran	ch-policy 🗸			
Flex Profile	Sit	te site_	tag 🗸			н
6 Site Tag 🛷 🔳 🕇	RF	defau	ult-rf-tag 🗸			
	Ch	anging AP Tag(s) will	cause associated A	P(s) to reconn	iect	
0 RF Profile			_			_
0 RF Tag 🛷 🔳 🕇) Cancel		Save & Ap	oply to Devic	e

CWA flow on Flex

This section describes the steps to set up CWA with URL filter, for CWA flow the URL filter is optional.

- Create a server and server group for mac auth and AAA attributes
- Create an authorization list on the controller
- Create a MAB SSID and map the authorization list on the SSID
- Create a redirect ACL and a URL filter(optional) on the controller
- Bind the URL filter and ACL on the flex profile
- Create an Authorization profile on ISE to return Cisco AV pair of url-redirect and url-redirect-acl.

Procedure

Step1Create an Authentication and Authorization list on the WLC.
Navigate to Configuration > Security > AAA.
Use the AAA wizard to create the server and server groups.

	Authentication Authorizati	on and Accounting	
Dashboard	+ AAA Wizard		
) Monitoring >	AAA Method List	Servers / Groups AAA Advanc	ed
Configuration >	General	Local Authentication	Default
Administration >	Authentication	Local Authorization	Default 🔻
' Troubleshooting	Authorization	Radius Server Load Balance	DISABLED
	Accounting	Show Advanced Settings >>>	

Step 2

Define a name for the server and specify the IP address and shared secret.

Add Wizard						×
					 Basic 	O Advanced
	SERVER		SERVER GROL	P ASSOCIATION	MAP AAA	
RADIUS 🔽	TACACS+	LDAP				
RADIUS Name*	ISE					
IPv4 / IPv6 Server Address*	9.1.0.20					
PAC Key						
Key*	(and a					
Confirm Key*						
D Cancel						Next 🗲

Step3 Create a server group and map the server in the group .

		Basic
SERVER	ER SERVER GROUP ASSOCIATION	
SERVE		WAL AAA
RADIUS		
Name*	ISE	
Group Type	RADIUS	
MAC-Delimiter	colon 🔻	
MAC-Filtering	none v	
Dead-Time (mins)	1-1440	
Available Servers	Assigned Servers	1
freerad	ISE	
	>	
	*	
	•	ļ
Previous	•]
	control and check mark the authentication and Authori	zation profile.
	*	zation profile.
Enable dot1x system c	*	zation profile. • Basic
Enable dot1x system c Add Wizard	control and check mark the authentication and Authori	Basic
Enable dot1x system c	control and check mark the authentication and Authori	
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER SERVER GROUP ASSOCIATION	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER SERVER GROUP ASSOCIATION uthentication Authorization Accounting control	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER SERVER GROUP ASSOCIATION uthentication Authorization Accounting Control ENABLED Default Default	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER SERVER GROUP ASSOCIATION uthentication Authorization Accounting Control ENABLED Default Default	Basic
Enable dot1x system of Add Wizard	control and check mark the authentication and Authori ER SERVER GROUP ASSOCIATION uthentication Authorization Accounting Control ENABLED Default Def	Basic

Step5 Define the method type as Dot1x and map the server group.

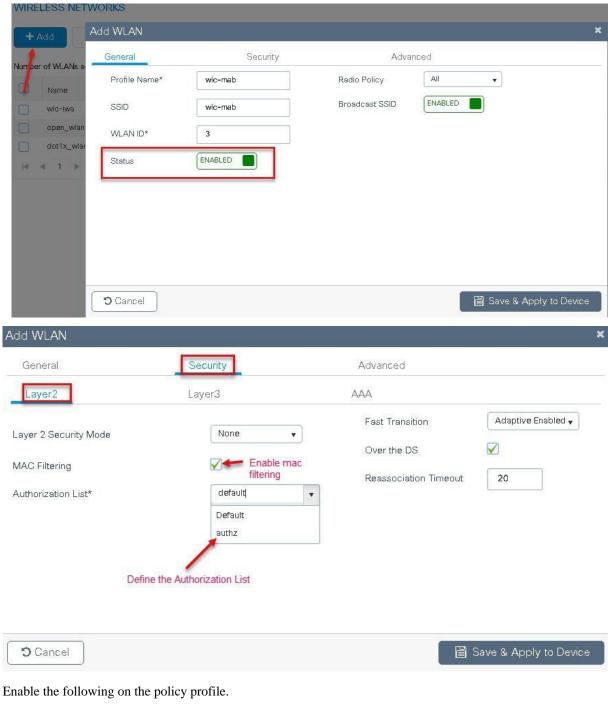
Add Wizard		*
		Basic O Advanced
Co là		
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🖌 Authenticat	ion 🗹 Authorization 🗹 Accounting 🗌	
General Authentication	Authorization	
Method List Name*	dot1x	
Туре*	dot1x 🔹	
Group Type	group	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap tacacs+ rad-group freerad radgrp_branch v	S ISE	
Sector Contraction (1997)		
← Previous		📔 Save & Apply to Device

Step 6

Define the method type as network and map the server group.

Add Wizard		×
		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authentication	Authorization Accounting	
General Authentication	thorization	
Method List Name*	authz	
Туре*	network v	
Group Type	group 🔹	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap tacacs+ rad-group freerad radgrp_branch *	> ISE *	
		📓 Save & Apply to Device

Step7Create a MAB SSID and map the authorization method list.Navigate to Configuration > Tags & Profiles > WLAN.



- Local VLAN present on the AP (mapped in the flex profile)
- AAA override

Step8

• NAC

Navigate to Configuration > Tags & Profiles > policy.

	General Access Po	plicies QOS and AV0	C Mobility	Advanced
Policy Profile				
wic-lwa	🛕 Configurii	ng in enabled state will result in los	s of connectivity for clients associa	ted with this profile.
open_wlan dot1x_wlan		·		
default-policy	Name*	wlc-mab	WLAN Switching Po	licy
1 -	Description	Enter Description	Central Switching	
	Status 2		Central Authentication	
	Passive Client		Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		

dd Poli <mark>cy</mark> Profile				
General Access Policies	QOS and AVC	Mobility	Advanced	
WLAN Local Profiling		WLAN	N ACL	
HTTP TLV Caching		IPv4 A	CL Search or Select	•
RADIUS Profiling		IPv6 A	CL Search or Select	•
DHCP TLV Caching		URL F	Filters	
Local Subscriber Policy Name	Search or Select 🔹	Pre Au	uth Search or Select	•
VLAN		Post A	uth Search or Select	
VLAN/VLAN Group	10			
Multicast VLAN	Enter Multicast VLAN			

🕽 Cancel

📔 Save & Apply to Device

ieneral	Access Po	licies	QOS and AVC	Mobility	Advanced
/LAN Timeo	ut			Fabric Profile	Search or Select
ession Timeou	ut (sec)	1800		Umbrella Parameter Map	Not Configured
le Timeout (se	ec)	300		WLAN Flex Policy	
le Threshold ((bytes)	Ô		VLAN Central Switch	ing
lient Exclusior ec)	n Timeout 🛛 🗹	60		Split MAC ACL	Search or Select 🔹
HCP				Air Time Faimess	Policies
HCP Enable				2.4 GHz Policy	Search or Select 🔹
HCP Server IF	^o Address	0.0.0.0		5 GHz Policy	Search or Select
w more >>> AA Policy Ilow AAA Ove AC State	erride	2			
olicy Name		default-aaa-	policy		
ccounting Lis	t	Search or Se	lect		

Step9Map the policy profile to the WLAN in the policy tag .Navigate to configuration > tags and profiles > tags

Manage Tags				
Policy Sit	e RF	AP		
+ Add × Dalet	Add Policy Tag			×
1	Name*	branch_policy		
Policy Tag Name branch	Description	Enter Description		
default-policy-tag	+ Add 🛛 🛪 D			
	2 WLAN Profile		Policy Profile	×
		10 🔹 items per page		No items to display
	Map WLAN and Po	blicy		
	WLAN Profile*	wic-mab 🔹	3 olicy Profile*	wic-mabl
				4
	Cancel			Save & Apply to D 5 be

Step 10 Create a redirect ACL and an optional URL filter. The option to create a URL filter depends on access to resources during the pre-auth phase.

To create a redirect ACL use the CLI on the controller. Have the rules created as shown below:

ip acces	adding "DNS ACCESS"
deny	udp any any eq domain ACL to allow DNS access
deny	adding "DHCP ACCESS"
remark	adding "DHCP ACCESS"
deny	udp any eq bootps any
deny	udp any any eq bootps any ACL to allow DHCP access
remark	adding "ISE ACCESS"
deny	ip any host 9.1.0.20 ACL to allow ISE ACESS
deny	ip host 9.1.0.20 any
remark	adding "rules for redirection"
permit	top any any eq www
permit	tcp any any eq 443

To create a URL filter navigate to Configuration > security and URL filters.

Logical AireOS Config Tra Dashboard Ethernet Application Visibili	10
🚍 Dashboard 🛛 🔅 Ethernet Application Visibili	
	ty
Wireless Cloud Services	
Monitoring > 🗄 Layer2 Custom Application	n
IOx IOx	
Configuration > VLAN Multicast	
VTP NetFlow	
O Administration VIP Python Sandbox	
Radio Configurations QoS	
CleanAir RA Throttle Policy	
High Throughput Tags & Profiles	
Media Parameters Air Time Fairness	
Network AP Join	
Parameters	
RRM Policy	
Routing Protocols	
OSPF Tags	
Gecurity Wireless	
AAA Access Points	
ACL Advanced	
Advanced EAP Fabric	
PKI Management Media Stream	
Local EAP Mesh	
Local Policy Mobility	
TrustSec WLANs	
Threat Defense Wireless Setup	
URL'Filters	
Web Auth	

Step11 Create a URL filter.

Permit action creates a whitelist while the deny action creates a blacklist.

Step 12 Enable the following on the flex profile.

Navigate to configuration > tags and profiles > flex.

- Local VLAN need to be configured
- ACL and URL filter needs to be mapped

URL Filters	Add URL Filter					×
+ Add	List Name*	url-pre-auth	Re	direct Server	s	
List Nam	Туре	PRE-AUTH	IΡv	/4 ×	2006,2006,2006,200	P
≪ ≪ 0)	Action	PERMIT	IPv	/6 ×		
	URLs	Enter a URL every new line dns.clsco.com olavstore.google.com				
	Cancel			(🗑 Save & Apply	y to Device

nced Wirele	ess Setup						
Start			×	+ Add X Dels			
			1	Add Flex Profile			×
	Tags & Profiles		/	General Local	Authentication Policy AC	L VLAN	
0	WLAN Profile		+		branch_flex_profile	Multicast Overridden Interface	
0	Policy Profile		+	Name*	branch_tiex_profile		
6	Policy Tag 🛛 🛷		-	Description	Enter Description	Fallback Radio Shut	
Ů				Native VLAN ID	0	Flex Resilient	
		i cent		LITTO Desce Dest	0	ARP Caching	
0	AP Join Profile		+	HTTP Proxy Port		Efficient Image Upgrade	
0	Flex Profile			HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	
0	Site Tag 🛛 🛷		+	CTS Policy		Join Minimum Latency	
				Inline Tagging			
0	RF Profile]	+	SGACL Enforcement			
0	RF Tag 🛛 🧳]	+	CTS Profile Name	default-sxp-profilex v		
	Apply			Cancel			🗃 Save & Apply to Device

General Local Authentication Policy ACL VLAN			×
+ Add × Delete			
Ac Name Central Pre Auth URL Webauth Fliter 0 1 10 items per page No items to display	ACL Name* Central Webauth Pre Auth URL Filter	ACL-REDIRECT Concentration of the second s	
Cancel 5	7	🛛 🗎 Save & Apply to Devic	6
General Local Authentication Delicy ACL MAN			
General Local Authentication Policy ACL VLAN + Add Celete	1		
	VLAN Name* VLAN Id*	10 10 10	
+ Add x Delete AAN Name ✓ ID ✓ ACL Name ✓ 0 ► II 10 ▼ items per page		10	

- **Step 13** For assigning the flex profile on the site tag and mapping it on the AP, refer the steps in the advanced configuration wizard of this document.
- **Step14** Create an Authorization profile and rule on ISE to return the CWA attributes.

For more details on ISE rules and configuration, please refer the deployment guide.

<pre>* Name sand-cwa ewkd Description * Access Type Access Accept * Access Type Access Accept * Access Type Access Accept * Track Movement * * Service Tamplate * Track Movement * * Service Tamplate * Service Tamplate * Other Dennia Permission * Web Redirection (OVA, MDM, NSP, CPP) * Centralized Web Auth * AcL AcL_REDIRECT * Value sand-owa * Other Service * * Static Pt-Hotst name FODN * J. D. 20 * Static Pt-Hotst name FODN * J. D. 20 * * Actual Activity Service * Static Pt-Hotst name FODN * J. D. 20 * * Attributes Settings * * Attributes Details ** ** ** ** ** ** ** ** ** ** ** ** **</pre>	uthorization Profiles > sand-cv	wa-ewic
Description * Access Type Access Type Access Type Access Type Service Template Teck Movement Image: Service Template Select an Rem Image: Service Template Image: Service Template Select an Rem Image: Service Template Select an Rem Image: Service Template Service Template Service Template Service Template Service Template Image: Service Template Image: Service Template <t< td=""><td>uthorization Profile</td><td></td></t<>	uthorization Profile	
*Access Type Access AccePT Access Type Access AccePT Accest Access Acce Accest Accest Accest Acce	*Name sa	nd-cwa-ewic
etwork Device Profile Service Template Track Movement Image: Track Movement <td>Description</td> <td></td>	Description	
Service Template Track Movement Trac	* Access Type	CESS_ACCEPT *
Track Movement	letwork Device Profile	Cisco 🔹 🕀
Accl_REDIRECT Value sand-cwa	Service Template	
Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) Centralized Web Auth ACL Centralized Web Auth ACL Olisplay Certificates Renewal Message Static IP Atost name.FGDN 9.1.0.20 Advanced Attributes Settings Select an item Attributes Details Attributes Details	Track Movement	0
Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) Centralized Web Auth ACL Centralized Web Auth ACL Olisplay Certificates Renewal Message Static IP Atost name.FGDN 9.1.0.20 Advanced Attributes Settings Select an item Attributes Details Attributes Details	Passive Identity Tracking 📋	D.
Voice Domain Permission Webs Redirection (GWA, MDM, NSP, CPP) ② Centralized Web Auth ■ ACL ACL-REDIRECT Value sand-cwa ■ Display Certificates Renewal Message Static P/Host name/FODN 9.1.0.20 Advanced Attributes Settings Select an item The set of the se		
Web Redirection (CWA, MDM, NSP, CPP) Centralized Web Auth ACL ACL ACL-REDIRECT Value sand-cwa Display Certificates Renewal Message Static IP/Host name/FQDN 9.1.0.20 Advanced Attributes Settings Select an Rem Image: Static IP/Host name/FQDN Select an Rem Image: Static IP/Host name/FQDN Advanced Attributes Settings Select an Rem The second settings Constrained Settings Access Type = ACCESS ACCEPT Sisco-av-pair = uf-redirect-act_ACL-REDIRECT Sisco-a	Common Tasks	
Centralized Web Auth ACL ACL Display Certificates Renewal Message Static IP/Host name/FQDN 9.1.0.20 Advanced Attributes Settings Select an item Attributes Details access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-ad=ACL-REDIRECT access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-ad=ACL-REDIRECT	Voice Domain Permission	
Static IP/Host name/FQDN 9.1.0.20 Advanced Attributes Settings Select an item Select an item The second set is a second set in the set is a second set in the second set is a second set if the second set is a second set is a second set in the second set in the second set in the second set is a second set in the second s	Centralized Web Auth	ACL ACL-REDIRECT Value sand-cwa
Advanced Attributes Settings Select an item = Attributes Details access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-acl=ACL-REDIRECT	Display Certificates	Renewal Message
Select an item = <li=< td=""><td>Static IP/Host name</td><td>FQDN 9.1.0.20</td></li=<>	Static IP/Host name	FQDN 9.1.0.20
Select an item = <li=< td=""><td></td><td></td></li=<>		
Select an item = <li=< td=""><td>Advanced Attributes</td><td>Settinas</td></li=<>	Advanced Attributes	Settinas
Attributes Details xccess Type = ACCESS_ACCEPT isco-av-pair = url-redirect-acl=ACL-REDIRECT isco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa		
access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-acl=ACL-REDIRECT isco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa	Select an item	
access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-acl=ACL-REDIRECT isco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa		
access Type = ACCESS_ACCEPT isco-av-pair = url-redirect-acl=ACL-REDIRECT isco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa		
isco-av-pair = url-redirect-acl=ACL-REDIRECT isco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa		
	cisco-av-pair = url-redirect-a	d=ACL-REDIRECT
	cisco-av-pair = url-redirect=f	rctps;//9.1.u.zu:port/portal/gateway/session1d=Session1dvalue&portal=9c1e4bc2-631e-11eb-9498-3e482c4f19ba&action=cwa
	Save Reset	

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html#anc6

Limitation

- The URL filter is only supported on wave2 AP's and is not supported on wave 1 APs.
- Post Auth support for URL filter is not supported for local switched clients.

Client Association Limit per WLAN/AP

The Client limit per WLAN features address the requirement when an administrator would want to restrict the number of the clients accessing the wireless service For example, limiting total Guest Clients from branch tunneling back to the Data Center.

Summary

The controller supports limiting the number of client associations in the following ways .

Per WLAN basis-here the client association are limited on a per WLAN basis

Per AP Per WLAN-here the client Association are limited on a per WLAN per AP basis

Per AP radio per WLAN-Client association limited on a per radio per WLAN basis

Procedure

To enable a WLAN please refer the section of setting up the WLAN in the advanced config wizard of this document.

Advanced wireless setup wizard

Procedure

During the WLAN configuration phase enable the feature,

Start	+ Add & Delete					
Tags & Profiles	Add WLAN		_	_		
	General	Security	Advar	nced		
cilek on '+' symbol	o add Coverage Hole Detection		Universal Admin			^
O Policy Profile	Aironet IE		Load Balance			
O Policy Tag 🗳 🔳	 Diagnostic Channel 		Band Select			
	P2P Blocking Action	Disabled 🗸	IP Source Guard			
O AP Join Profile	+ Multicast Buffer	DISABLED	WMM Policy	Allowed	•	drop 🖌
Flex Profile	Media Stream Multicast- direct		Off Channel Scar	nning Defer		down the scroll bar
	Max Client Connections	1	Defer Priority	0 1	2	
0 ····· RF Profile	+ Per WLAN 0			3 4	5	

Aulticast Buffer		WMM Policy	Allowed	¥	
Media Stream Mult lirect	icast-	Off Channel	Scanning Defer		
Max Client Conn	ections	Defer Priority	0 1	2	
er WLAN	50		3 4	5	
Per AP Per VLAN	100		6 7		
Per AP Radio Per WLAN	150	Scan Defer Time	100		
er wear	on Support	Assisted Ro	aming (11k)		

Limitations

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

Fault Tolerance

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

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

FlexConnect Fault Tolerance, along with Local authentication on Flex Connect AP 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. To ensure Fault Tolerance to works smoothly both the controller needs to have identical config such as:

- Wlan config and policy profile
- AP join profile/ flex profile
- RF profile and RF tag
- Site tag

The management IP address of the controller can be different, an administrator can take a backup config of the primary controller and have it installed on the secondary controller to maintain config consistency.

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.
- Supported on both Wave1 and Wave 2 AP's.

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.
- FlexConnect primary and backup controllers must be in the same mobility domain.

VideoStream for FlexConnect Local Switching

Introduction

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.

On a traditional WLAN networks multicast and broadcast is send out over the wireless medium at the lowest data rate with no acknowledgement and the packet delivery for such streams are on a best effort basis .This makes the usage of multicast unreliable on a WLAN network . The usage of multicast for delivering critical application has become a demand and need of the hour. There is also a need to differentiate multiple streams and assign priority and weightage based on the applications supported. With the adoption of 802.11ac and the data rates supported it is possible to deliver multicast streams using the data rates available on 11ac with reliability and priority built in.

Summary

- VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP
- Supported on Wave 1 and Wave 2 AP's
- · Supported for flexconnect local switching and Central authentication
- With video stream in flex connect local switching the multicast to unicast conversion happens on the AP
- The branch infrastructure should have multicast enabled
- · Admission control is currently not supported

• IPv6 support for media stream is not supported

The section below details the procedure for configuring media stream from the controller. It is expected the branch network is enabled for multicast. Please refer the cisco.com on enabling multicast on the switching platforms.

Please ensure the following multicast features are enabled on the network.

- Multicast routing protocol PIM sparse/dense mode
- IGMP version 2 or 3
- IGMP snooping

This section doesn't cover enabling multicast on the infrastructure rather on the wireless controller.

Procedure for enabling Video Stream

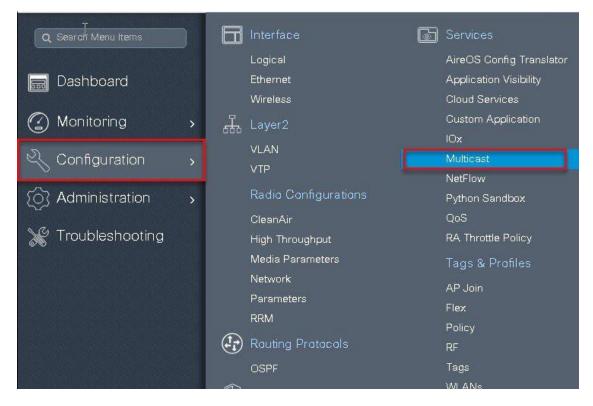
: The steps here includes only the changes to enable video stream

The advanced configuration section can be used to set up the SSID, profiles and tags. The section below details the configuration of media stream on the 5Ghz radio.

Procedure

Step1 Enable multicast globally on the controller.

Navigate to configuration > services > Multicast



Multicast

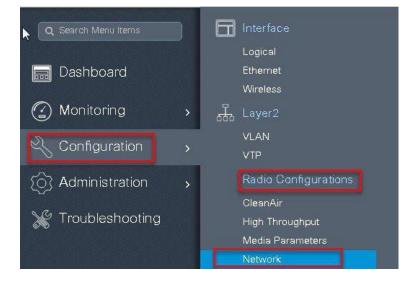
Global Wireless Multicast Mode					MLD Snooping	DISABLED
Wireless mDNS Bridging	DISABLED				IGMP Snooping Querier	ENABLED
Wireless Non-IP Multicast	DISABLED				IGMP Snooping	ENABLED
Wireless Broadcast	DISABLED				Last Member Querier Interval (milliseconds)	1000
AP Capwap Multicast	Unicast 🔹					
						✓Apply to De
						Apply to be
IGMP Snooping						
			0.80			
sabled		Enabled		Xan	<u> </u>	
Status VLAN ID	Name	Status	VLAN ID	Nam	e	
		ø	T.	default	÷	
		Q	4	VLAN0004	*	
		O	15	VLAN0015	*	
No Vian ava	ilable	L				
No Vian ava	ilable					
No Vian ava	llable	L				
No Vian ava	liable					

Step2 Enable media stream on the Dot11 interface.

Disable the appropriate radio interface before enabling the media stream

Navigate to Configuration > Radio Configurations > Network.

Disable 5ghz or 2.4 ghz radio, in this example we are enabling media stream on 5ghz radio.



5 GHz Band	2.4 GHz Band				
General	disable 5ghz radio				
5 GHz Network SI			-		
Beacon Interval*		10	00		
Fragmentation Th	reshold(bytes)*	23	346		
DTPC Support					
CCX Location N	leasurement				
Mode					
Data Rates					
6 Mbps	Mandatory 🗸	9 Mbps	Supported 🔻	12 Mbps	Mandatory
18 Mbps	Supported 🗸	24 Mbps	Mandatory 🚽	36 Mbps	Supported
48 Mbps	Supported 🗸	54 Mbps	Supported 🔻		

Step3 Navigate to Configuration > Radio Configurations > Media Parameters

Q Search Menu Items	D		Interface	Ŀ
			Logical	
🔜 Dashboard			Ethernet	
		1	Wireless	
Monitoring	>	品	Layer2	
			VLAN	
Configuration	>		VTP	
() Administration	>		Radio Configurations	
			CleanAir	
X Troubleshooting			High Throughput	
			Media Parameters	
			Network	
			Parameters	
그 않는 것 않는 것 않는 것 않는 것 않는 것			RRM	

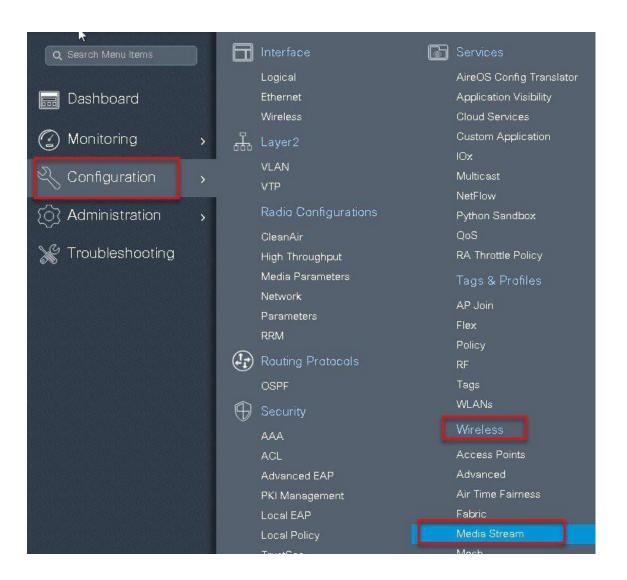
<i>l</i> ledia		Voice	
General		Call Admission Control (CAC)	
Jnicast Video Redirect		Admission Control (ACM)	
Multicast Direct Admission Control		Traffic Stream Metrics	
Media Stream Admission Control (ACM)		Metrics Collection	
Maximum Media Stream RF bandwidth (%)*	5	Stream Size*	84000
/laximum Media Bandwidth (%)*	85	Max Streams*	2
Client Minimum Phy Rate (kbps)	6000 🔹	Inactivity Timeout	
Jaximum Retry Percent (%)*	80		
Media Stream - Multicast Direct Parameter	3		
Aulticast Direct Enable			
lax streams per Radio	3		
fax streams per Client	3 🔹		
nactivity Timeout			

Step4 Enable media stream on the WLAN creation page on the advanced TAB, Refer the advanced configuration wizard section for WLAN creation.

Add WLAN		×
General S	ecurity	Advanced
Coverage Hole Detection	Universal Adr	Imin 🔲
Aironet IE	Load Balance	e 🗌
Diagnostic Channel	Band Select	
P2P Blocking Action Disable	ed 🔹 IP Source Gu	uard
Multicast Buffer	ABLED WMM Policy	Allowed
Media Stream Multicast-	Off Channel	al Scanning Defer
Max Client Connections	Defer Priority	/ 0 01 02
Per WLAN 0		3 4 25
Cancel		Save & Apply to Device

Step5 Define the media stream multicast address configuration.

Navigate to wirless > Mediastream



Multicast Direct Enable	
Session Message Config	
Session Announcement State	
Session Announcement URL	
Session Announcement Email	
Session Announcement Phone	
Session Announcement Note	

Mpdia Stream			
General Streams			
+ Add M Delete	Add Media Stream		×
	General		
Stream Name	Stream Name*	check_1	
	Multicast Destination Start IPv4/IPv6 Address*	239.1.1.1	
	Multicast Destination End IPv4/IPv6 Address*	239.1.1.10	
	Maximum Expected Bandwidth*	1000	
	Resource Reservation Control (RRC) Pa	arameters	
	Average Packet Size*	1200	
	Policy	admit 🔹	
	Priority	4	
	QOS	Video	
	Violation	Drop	
	Cancel	📔 Save & Apply to Devi	
	92.°		

Step6 Enable the dot11 interface on which media stream was enabled.

neral			-		
Hz Network St	atus				
A Please o	lisable 5 GHz Network Status	to configure Beacon Int	erval, Fragmentation Thresh	old, DTPC Support.	
con Interval*		10	0		
mentation Th	reshold(bytes)*	23	46		
'C Support					
X Location M	leasurement				
le					
a Rates					
	🛕 Please disable	5 GHz Network Status	to configure Data Rates		
Mbps	Mandatory 🔻	9 Mbps	Supported 🕌	12 Mbps	Mandatory 💡
3 Mbps	Supported 🔻	24 Mbps	Mandatory 🔻	36 Mbps	Supported 🔻
3 Mbps	Supported 🔻	54 Mbps	Supported 🔹		

Connect wireless client and subscribe to the respective multicast video stream

Issue the CLI " show flexconnect media client summary " to see the multicast transmission being classified as multicast direct /video stream.

Client Mac	ct media-stream client Stream Name	Summary Multicast IP	AP-Name	VLAN	Туре
1c36.bbef.6492 1c36.bbef.6492 1c36.bbef.6492 1c36.bbef.6492	check1	224.0.0.251 224.0.0.252 239.1.1.1 239.255.255.250	ар-1-3800 ар-1-3800 ар-1-3800 ар-1-3800 ар-1-3800	10 10 10 10	Multicast-Only Multicast-Only Multicast-Direct Multicast-Only

FlexConnect IP Overlapping across Sites

Multiple customers in the branch deployment space tend to use cookie cutter configurations across the sites and branches which also includes local DHCP servers configured with the same subnet. Prior to this feature, the wireless controllers in this topology would detect the multiple client sessions with the same IP as IP Theft and clients would be blacklisted.

With this feature being introduced in IOS-XE Release 17.4, we can support overlapping IP address across different flex sites and still provide all the functionalities that are supported in the flex deployments. In order to accomplish this, a zone-ID along with IP-Address combination is used to prevent duplicate IP address across sites where Zone-ID will be different. Zone-ID is a running index that is generated per every site and persisted.

Configuration via CLI and WebUI

Configuration knob to enable/disable this feature is part of the flex profile

<config> wireless profile flex flex1 (config-wireless-flex-profile)#[no] ip overlap

By default, this configuration is disabled.

The following show commands can be used to display the zone ID along with IP address of the client.

wlc#show wireless device-tracking database ip

 IP
 ZONE-ID
 STATE
 DISCOVERY
 MAC

 9.91.59.154
 0x00000002
 Reachable
 IPv4 Packet 6038.e0dc.3182

 1000:1:2:3:90d8:dd1a:11ab:23c0
 0x00000002
 Reachable
 IPv6 Packet 58ef.680d.c6c3

 1000:1:2:3:f9b5:3074:d0da:f93b
 0x0000002
 Reachable
 IPv6 Packet 58ef.680d.c6c3

 2001:9:3:59:f9b5:3074:d0da:f93b
 0x0000002
 Reachable
 IPv6 NDP
 58ef.680d.c6c3

 2001:9:3:59:f9b5:3074:d0da:f93b
 0x00000002
 Reachable
 IPv6 NDP
 58ef.680d.c6c3

 680::f9b5:3074:d0da:f93b
 0x80000001
 Reachable
 IPv6 NDP
 58ef.680d.c6c3

Wlc#show wireless profile flex detailed flex1

Fallback Radio shut	: DISABLED
ARP caching	: ENABLED
Efficient Image Upgr	ade : ENABLED
OfficeExtend AP	: DISABLED
Join min latency	: DISABLED
IP overlap status	: DISABLED

To configure this feature using the WebUI, select the IP Overlap checkbox under the General tab under flex profile.

Configuration • > E	dit Flex Profile	
+ Add >	General Local Authentication	Policy ACL VLAN
	Umbrella	
Flex Profile		Shut
p	Description Enter Description	
test-profile	Native	Flex Resilient
flex-overlap	VLAN ID	400
test-flex-profi	HTTP _ 0	ARP Caching
default-flex-pr	Proxy Port	Efficient
flex-profile-no	HTTP- Proxy IP 0.0.0.0	Image 🔽 Upgrade
flex_ip_overla	Proxy IP 0.0.0.0 Address	
[4 4] 1 ▼]	CTS Policy	Office Extend AP
	Inline 🗖 Tagging	Join Minimum 🔲 Latency
	SGACL	IP Overlap

The feature can be verified by looking at the client statistics tab under General client details. The Zone ID will be populated along with the IP address indicating that this feature is turned on. When this feature is disabled the zone ID will show a value of zero.

60 View Gene	QOS Statist	ics ATF Statistics	Mobility History	Call Statistics	
lient Properties	AP Properties	Security Information	Client Statistics	QOS Properties	EoGRE
Number of Bytes R	eceived from Client	152145			
Number of Bytes S	ent to Client	11857			
Number of Packets	Received from Client	1634			
Number of Packets Sent to Client		78			
Number of Policy E	rrors	0			
Radio Signal Stren	gth Indicator	-36 dBm			
Signal to Noise Rat	io	49 dB			
IP Address		Zone-Id			
80.80.80.252		0x0000001	^		
fe80::552b:3b25:8	5cf3:50ac	0x80010320			
[a] a] 1 y]	▶ ▶ 10	 items per page 	1 - 2 of 2 items		

Configuration via Programmable Interfaces

In order to enable or disable the overlap IP support which is part of the flex profile, the following NETCONF RPC is defined

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="urn:uuid:a90868eb-1b78-43b4-a949-
2dca79687a69">
 <nc:edit-config>
 <nc:target>
  <nc:running/>
  </nc:target>
  <nc:config>
   <flex-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-flex-cfg">
   <flex-policy-entries>
    <flex-policy-entry>
     <policy-name>Flex_profile</policy-name>
     <description/>
     <ip-overlap-cfg>
      <flex-overlapping-ip-enable>true</flex-overlapping-ip-enable>
     </ip-overlap-cfg>
    </flex-policy-entry>
   </flex-policy-entries>
  </flex-cfg-data>
 </nc:config>
 </nc:edit-config>
</nc:rpc>
```

Invalid/Not Supported Scenarios

- Client Join when VLAN- based Central Switching for Flex Connect: With VLAN Based Central switching enabled, AP tunnels the traffic back to the controller. This scenario inherently will not support Overlapping IP support as it falls under central switched use case.
- Client Join when AP in Local Mode: No support for Overlapping IP for all the Local Mode configuration where the traffic is centrally switched
- Client Join with Flex with Central Switching: AP is in Flex mode but operated in Central switching mode. Here the DHCP server is also central and the IP overlapping case is not valid
- Flex Local Switching with Central DHCP: With the central DHCP, we still like to detect the IP Theft cases even though it is flex local

switched site. This feature will not be supported with this configuration

- EWC on Catalyst 9100s: This feature is not applicable since multiple sites cannot be supported with EWC
- Fabric or SD-Access wireless deployments are not supported

Glossary

- VLAN—Virtual LAN
- RF-Radio frequency
- FT-Fault Tolerance
- WAVE1 AP-All AP which supports WAVE1 802.11ac (Cisco -3700AP)
- WAVE2 AP AP which supports WAVE2 802.11ac (Cisco 1800/2800/3800/4800)

• WLC- Wireless LAN controller

uļuļu cisco.

Americas Headquarters Cisco Systems, Inc. San Jose, CA 95134-1706 USA Asia Pacific Headquarters CiscoSystems(USA)Pte.Ltd. Singapore Europe Headquarters CiscoSystemsInternationalBV Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.