<mark>Guide</mark> Cisco public IIIIII CISCO The bridge to possible

Cisco Catalyst 9800 FlexConnect Branch Deployment Guide

Contents

Introduction	4
Supported platforms	4
Supported releases	4
FlexConnect architecture	5
Advantages of centralizing access point control traffic	5
Advantages of distributing client data traffic	6
FlexConnect modes of operation	7
WAN requirements	7
Feature Matrix	7
Wireless branch network design	7
Primary design requirements	8
Overview	8
Advantages	8
Features addressing branch network design	9
Cisco Catalyst wireless config model	9
Profiles and tags	10
Basic wireless setup wizard	14
Advanced wireless setup wizard	19
Manual configuration	29
FlexConnect VLAN override	45
Summary	45
Procedure to enable VLAN	45
FlexConnect VLAN-based central switching	61
Summary	61
Steps to configure FlexConnect VLAN-based central switching	62
Local authentication and backup radius server	81
Summary	82
Local authentication with external radius server	82
AP as radius server	95
Procedure	95
CCKM/OKC and PMK caching	97
Limitation	97

Peer-to-peer blocking	98
Steps	98
FlexConnect ACL	99
Summary	99
Client ACL overview	108
FlexConnect VLAN override	109
AP pre-image download	110
Summary	110
Procedure	111
Limitation	112
FlexConnect smart AP image upgrade	113
Summary	113
Procedure	114
FlexConnect pre-auth ACL and URL filtering	115
Summary	115
LWA flow with URL filter	117
CWA flow on flex	126
Limitation	136
Client association limit per WLAN/AP	137
Summary	137
Procedure	137
Limitations	138
Fault tolerance	138
Summary	139
Limitations	139
VideoStream for FlexConnect local switching	139
Introduction	139
Summary	139
Procedure for enabling VideoStream	140
Flex IP Overlap Support	147
Introduction	147
Procedure for enabling Flex IP Overlap	148
Glossary	150

Introduction

This document describes how to deploy a Cisco FlexConnect[®] wireless branch solution on the Cisco Catalyst[™] wireless platform. The Catalyst wireless platform is 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 to 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. The Catalyst 9800WC and virtual cloud controller run on the Cisco IOS[®] XE software base, utilizing the flexibility and modularity available with the platform.

Refer to the following documentation for how to get started on 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 cover the features that are supported on the following platforms and releases.

Supported platforms

Catalyst wireless platforms

11ac Wave 1 and Wave 2 Access Points - 18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

11ax Access Points - 9105, 9115, 9117, 9120, 9130

Supported releases

IOS-XE 16.10 and higher.

FlexConnect architecture



Figure 1.

FlexConnect Architecture and Traffic Flow

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

The FlexConnect solution enables the customer to:

- · Centralize control and manage the 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 sizes that can scale up to 100 APs and 250,000 square feet (5000 square 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.

 Table 1.
 L2 security support for centrally and locally switched users

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

 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

Table 3. Flexconnect modes of operation

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

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	100	1000
Data	1.44 Mbps	1 sec	100	1000
Data + voice	128 Kbps	100 ms	5	25
Data + voice	1.44 Mbps	100 ms	100	1000
Monitor	64 Kbps	2 sec	5	N/A
Monitor	640 Kbps	2 sec	100	N/A

 Table 4.
 FlexConnect WAN Bandwidth and latency requirements

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 to the FlexConnect matrix document in the link below to validate the list of supported features.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b flexConnect feature matrix.html

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 square 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. 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 the figure below



Figure 2.

Design replication across stores by mapping different site tags and policy tags

Features addressing branch network design

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

Table 5.	Features	addressing	branch	network	desian
	i outuroo	uuuuuuu	branon	110100110	acoign

Features	Highlights
New config model on Catalyst wireless family	Ability to decouple and modularize the configuration entities. This enables you to have the same configuration across different stores by having the same profiles across stores and using a different tag 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 that has a flex profile will auto-convert the AP to FlexConnect mode without user intervention.
Efficient AP image upgrade	Reduces downtime when upgrading your branch. 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 that is a tunnel to a controller in the DMZ zone.
URL ACL	Ability to support use cases of bring your own device (BYOD) at the branch
Backup 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 the modularized and reusable model with logical decoupling of configuration entities.

The model introduces the uses of tags and profiles. The below table gives an overview of the tags and profiles used within the new Catalyst wireless products.

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.

Tags and profile	Highlights
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 with the APs. Profiles are reusable entities that 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 characteristics 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 with it. This property is in turn inherited by an associated client/AP. There are various types of tags, each associated with 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

The 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

The policy profile is an entity that comprises of network and switching policies for a client, except for QoS, which constitute the AP policies as well.

The 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 of 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 the client policy).

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



Figure 3.

Components of Policy Tag

AP join profile

The 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 the CAPWAP connection to be reset since these parameters pertain to the characteristics of the AP.

Flex profile

The flex profile contains the remote site-specific parameters – for example, the primary and secondary AP list, the EAP profiles that 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 of a site tag and define the characteristics of a local or remote site.

Site tag

The site tag constitutes 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 the central and remote sites are part of the AP join profile. The attributes that are specific to the flex/remote site are part of the flex profile.

The default site tag constitutes the default AP join profile. There is no default flex profile. The default AP join profile values will be the same as that for the global AP parameters today plus a few parameters from the AP group in today's configuration like "preferred mode," 802.11u parameters, location, etc.



Figure 4. Components of Site Tag

RF profile

By default, there exist 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

The RF tag constitutes the 11a and 11b RF profiles. The default RF Tag constitutes the default 802.11a RF profile and the default 802.11b RF profile.

The default 11a RF profile and 11b RF profile contain default values for global RF profiles for the respective radios.



Figure 5. Components of RF Tag

AP tag

Access points are tagged based on the SSIDs and the associated policies they broadcast 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.



Figure 6.

Tags and Profiles association and mapping relationship

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 advanced wireless setup wizard
- Manual configuration

Please refer to the controller deployment guide for controller bring-up, SVI creation, and management of 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 that has the following deployment model will be used to showcase the configuration model.

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

A guest SSID that is centrally switched.

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

 Table 7.
 Deployment scenario examples

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

Basic wireless setup wizard

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

Procedure

Step 1. Click on the wireless setup wizard.

Cisco Ca	talyst C9800-CL. Wireless Controller		Welcome sand 🛛 🗰 🌠 🖨 🎯 🕼 🚱 🛛 🕪
Q Search Mona terra	Basic Wireless Setup		1
🔜 Deshboard	+ Add		Click on wireless setup wizard
Monitaring >		No locations available	
Sconfiguration			
💮 Administration 🕠			
👷 Troubleshooting			

Step 2. Select the basic setup wizard from the drop-down box and click on "Add."

Cisco Cisco	Cetalyst C9800-CL Wireless Controller	0	Welcome send 🗰 🐔 🖪 🖨 🔯 😡 🔅
Q Search Meru tens	Basic Wireless Setup		Wreless Setup Select Type Colect Type
Dashboard	+ Add		Advanced
Monitoring		No locations available	
			4
() Administration			
X Troubleshooting			
			J

Interface Services Q Search Menu Items AireOS Config Translator ashboard Ethernet Application Visibility 100 Wireless **Cloud Services Custom Application** Monitoring Layer2 $(\underline{\cdot}]$ > IOx. VLAN Configuration Multicast VTP NetFlow Administration Python Sandbox 20 5 QoS CleanAir Troubleshooting RA Throttle Policy High Throughput Media Parameters Network AP Join Parameters Flex RRM Policy (Ir) Routing Protocols OSPF Tags WLANs 🕀 Security AAA Access Points ACL Advanced EAP Advanced Air Time Fairness PKI Management Fabric Local EAP Media Stream Local Policy Mesh TrustSec Mobility Threat Defense URL Filters Wireless Setup Web Auth Wireless AAA Policy Advanced Wireless Protection Policies

An administrator can also start the wizard by navigating to Configuration > Wireless Setup >

Basic.

Step 3. Select a name for the remote site, and 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: store1						
+ Back						🖹 Apply
General Wreles	ss Networks AP Provisi	oning				
A This Location Type is not recomme	ended for On-Premise deployments			AAA Servera		
Location Name*	store1	0		Available (0)	Selected (0)	
Description	store1					
Location Type	Local · Fex2			No AAA servers available	No AAA servers selected	
Client Density	Low Typical High))				
Native VLAN ID	3 (3)	Add AAA Server		×	Add New Server	
		IP Address*	9.1.0.100			
		Key*		45		
		Cancel		+ Ada		

Step 4. 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 Wireless Setup: store1					
← Back					
General Wireless Networks	AP Provisioning				
+ Add 🗱 Delete	Add WLAN				×
WI ANS on this Location	General	Security	Adva	inced	
W AN Name	Profile Name*	store-ssid	Radio Policy	All	
items per page	SSID	store-ssid	Broadcast SSID		
WIRELESS NETWORKS	WLAN ID*	5			
+ Add R Delete Enable WLAN	Status				
Number of WLANs selected : 0					
Name					
wic-twa					
wic-mab					
open_wlan					
dot1x_wian	Cancel			冒 Save & App	ly to Device

General	Security	Advanced	
Layer2	Layer3	AAA	
Layer 2 Security Mode	WPA + WPA2 V	Fast Transition	Adaptive Enabled 🗸
MAC Filtering		Over the DS	
Protected Management Frame		Reassociation Timeout	20
PMF	Disabled 🔻		
WPA Parameters			
WPA Policy			
WPA2 Policy			
WPA2 Encryption	AES(CCMP128) CCMP256 GCMP128 GCMP256		
Auth Key Mgmt	PSK V		
PSK Format			
Pre-Shared Key			

Step 5. Define the policy for the WLAN.

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

Basic Wireless Setup: store1 ← Back	× Delete Locat	
General Wreless Networks AP Provisioning + Add x Delete		
WLANs on this Location		
WLAN Name	VLAN/VLAN Group	
4 4 0 ▶ ▶ 10 → Items per page		No items
Wireless Network Details	Policy Details	
WLAN* store-ssid	VLAN/VLAN Group* 10 (E.g. 1,2,5-7))
	ACL Search or Select	
	QoS Search or Select	
	CFF Central Switching CN Central Authentication	
	OFF Central DHCP	
	x	

Step 6. 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, the AP will reboot to boot in FlexConnect mode.

Q Search
AP Name - Status
er page No items to di

Step 7. Click apply to complete the wizard.

heral Wireless Networks AP Provisioning			
Add/Select APs		APs on this Location	
MAC Address	0	Associated AP list Number of selected APs : 0	Q. Search
ailable AP list	Q Search	AP MAC	 Status
mber of selected APs : 0		B0e0.1d70.d4f4 ap-1-3700	Joined
AP MAC AP Name		cc16.7e83.c598 ap-2-3800	Joined
	No been to display	cc16.7e83.c4ea ap-1-3800	Joined
tiens page	Ho iteria to oropiay	I≪ ≪ 1 ≫ ≫I 500 v items per page	1 - 3 of 3 item

Advanced wireless setup wizard

In this section, the advance config wizard is used to create a guest SSID with web authentication, which would be centrally switched through a WLC at the data center.

Procedure

Step 1. Click on the wireless setup wizard.

Cisco Cat cisco Listo Etatorio	alyst C9800-CL Wireless Controller		Welcome sand 🛛 🐗 🌄 🛱 🛱 🙆 🛛 Թ
Q. Search Menuicema	Basic Wireless Setup		1
Dashboard	+ Add		Click on wireless setup wizard
Monitoring >		No locatione available	
Configuration >			
Administration >			
💥 Troubleshooting			

Step 2. Select the advanced option.

Cisco Cati	lyst C9800-CL Wireless Controller		Welcome sand 🛛 🏘 🕵 🖺
Q. Search Menu Items	Basic Wireless Setup		Wireless Setup Select Type Select Type
👼 Dashboard	+ Add		Basic Advanced
Monitoring >		No locations available	
\sim Configuration \rightarrow			
() Administration >			
💥 Troubleshooting			

An administrator can also start the wizard by navigating to Configuration > Wireless Setup > Advanced.



Step 3. The advanced config wizard gives an overview of the flow of tags and policies. Click on the "Start Now" button to start the wizard.

Q Search Menu Items	Advanced Wireless Setup			
Dashboard	This screet creating P	Wire n allows you to Policies and Ta deployed	less Setup Flow Oven o design Wireless LAN gs. Once the design is to the Access Points ri	view Configuration. It involves completed, they can be ght here.
			DESIGN PHASE	
Configuration >			Tags & Prohles	
 (○) Administration → 	WLA (Ma	AN Policy andatory)	Site Policy (Optional)	Radio Policy (Optional)
💥 Troubleshooting	WLAN	Profile	AP Join Profile	RF Profile
	Policy	Profile	Flex Profile	RF Tag 🥔
	Policy	Tag 🛷	Site Tag 🛛 🥔	
			DEPLOY PHASE	
		Select Af	Apply to APs (Mandatory) Tag APs 2s and push configurati	on to them
	т	FERMINOLOGY		ACTIONS
	Tag WLAN Polic Site Policy Radio Polic	cy, Policy Profi - AP Profile, S cy - Radio Chai	ite Profile	Go to List View Create New
			Start Now	

Step 4. Click on the "+" icon to start creating the WLAN.

			\frown		
Wireless Setup Flow	Overview		(Start)		
This screen allows you to design Wireless creating Policies and Tags. Once the desi deployed to the Access Po	LAN Configuration. It involves ign is completed, they can be pints right here.		Tags & Pro	ofiles	
DESIGN PHAS	SE .				
Tags & Profi	les		WLAN Prof	ile ill	*
WLAN Policy Site Policy (Mandatory) (Optional)	Radio Policy (Optional)		Policy Prof	ile 📔	+ click on the "+" ic
WLAN Profile AP Join Profile	e RF Profile		Policy Tag	4	i +
Policy Profile Flex Profile	RF Tag 🛷		AP Join Pr	ofile	1 +
Policy Tag 🛷 Site Tag	ø	Start Now 🛶	Flex Profile		i 🔸
DEPLOY PHAI	SE		O Site Tag	4	i 🔸
Apply to AF	28				
(Mandatory	<i>i</i>)		RF Profile	i	i +
Tag APs Select APs and push confi	guration to them		Ø RF Tag		1 +
	LOTION		Apply		
TERMINOLOGY	ACTIONS		Tag APs		1
Tag WLAN Policy, Policy Profile Site Policy - AP Profile, Site Profile	Go to List View		Done		

	Security	Adva	anced	
Profile Name*	guest_ssid	Radio Policy	All	
SSID	guest_ssid	Broadcast SSID		
WLAN ID*	1			
Status				

Step 5. Define the SSID name and security type for the WLAN.

Add WLAN			×
General	Security	Advanced	
Layer2	Layer3	AAA	
Layer 2 Security Mode	None •	Fast Transition Over the DS Reassociation Timeout	Adaptive Enabled v
Cancel			Save & Apply to Device

Add WLAN				×
General	Security	Y	Advanced	
Layer2	Layer3	1	ААА	
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	o work, please aaa authorization in the device			
D Cancel			📓 Save & Apply to	Device

Step 6. Create a policy profile for the SSID.

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

nced Wirele	ess Setup		×						
Start				+ Add	🗙 Delete	Enable WLAN		ble WL	AN
Ľ	Tags & Profil	es		Number of WLAN	Is selected : 0				
				Name		×	ID	×	SSID
0	WLAN Profile			open_wi	an		1		open_wlan
6	Policy Profile		I +	4 4 1	▶ ▶ 10	▼ items per page			
0	Policy Tag		I +						
				click on "+" icon to add a policy					
0	AP Join Profile	e 📕	+						
0	Flex Profile		+						
6	Site Tag	ø	+						
Ø	RF Profile	I	I +						
0	RF Tag	4	+						

eneral	Access Policies	QOS and AVC	Mobility	Advanced
	A Configuring in enable	d state will result in loss of c	connectivity for clients associ	ated with this profile.
Name*	guest	_ssid	WLAN Switching Pe	plicy
Description	Enter	Description	Central Switching	
Status	ENABLE		Central Authentication	
Passive Client		ABLED	Central DHCP	
Encrypted Traff	ic Analytics	ABLED	Central Association	
CTS Policy			Flex NAT/PAT	
Inline Tagging				
SGACL Enforce	ement			
Default SGT	2-655	519		

Step 7. 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	Ad	dvanced	
WLAN Local Profiling		w	LAN ACL		
HTTP TLV Caching		IPv	4 ACL	Search or Select	•
RADIUS Profiling		IΡ\	6 ACL	Search or Select	•
DHCP TLV Caching		UI	RL Filters		
Local Subscriber Policy Name	Search or Select	Pro	e Auth	Search or Select	•
VLAN		Po	st 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.





Step 8. An optional attribute to set is the export anchor configuration. Please refer to the mobility deployment guide to set up mobility peers.

Add Policy Pro	file				×
General	Access Policies	QOS and AVC	Mobility	Advanced	
Mobility Anch	ors				
Export Anchor	S - C	elect the option for expo anchor	<u>t</u>		
Static IP Mobility	DISABLED				
Adding Mobility An disable and may re	chors will cause the enabled ¹ Soult in loss of connectivity for	WLANs to momentarily r some clients.			
Drag and Drop/do	whe click/click on the arrow	v to add/remove Anchor	2		
Available (1)		Selected (0)	R.		
Anchor IP		Anchor IP	Anchor Priority		
9.1.5.16	÷				
	1		Anchors not assigne	ed	
	click to add the				
	anchor controller				

Step 9. Create a policy tag that binds the SSID and policy profile together.

Start				+	Add X Delete Enab			
Tags	& Profiles			Numbe	er of WLANs selected : 0			Advanced Wireless Se
0	NI Drofile				Name	v. ID	- SSID	
	AV FIONE.				open_wlan	1	open_wlan	Start
O Pol	cy Profile		+	(4	◄ 1 ► ► 10 + items	per page		Tags
0 Pol	cy Tag 🛛 🛷	≣	+					0 WLAI
								Polio
0 AP	Join Profile	=	+					
0 Flex	Profile		+					Policy
GSite	Tan 4	=						
C.	- tog							• AP Jo
0	Drofile	-						• Flex f
U	FIONE		-					G Site T
0 RF	Tag 🛷	=	+					
Арр	У							RE Pr
0 Tag	APs							
								0 RF Ta

Step 10. Define a flex profile. The flex profile is used for configuring the VLANs on the AP that is used for the local switched SSIDs.

In this example, the guest SSID is centrally switched. In cases where there is a mix of centralswitched and local-switched SSIDs, an administrator can create a flex profile and define the VLANs to be used by the local-switched SSIDs.

Start	+ Add × Delete Er	able WLAN	Disable WL	AN
Tags & Profiles	Number of WLANs selected : 0			
MI ANI DISEN	Name	×.	ID <	SSID
WULANN PTOINE	open_wlan		1	open_wlan
OPolicy Profile	≪ ≪ 1 ► ► 10 ¥ ita	ems per page		
0 Policy Tag 🛷 📃 🕇				
0 AP Join Profile 📃 🕇				
AP Join Profile I Flex Profile				
AP Join Profile AP Join Profile Flex Profile Site Tag	click on "+" icon			
AP Join Profile Image: the second s	click on "+" icon to add a policy			
AP Join Profile AP Join Profile Flex Profile Site Tag RF Profile Frofile Frofile	click on "+" icon to add a policy			

Step 11. Define the native VLAN for the FlexConnect APs.

Add Flex Profile			8
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	
Nauve VEANID		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		
Cancel			📓 Save & Apply to Device

Step 12. Define the VLANS to be used for the local-switched SSID.

ieneral Local Auther	ntication	Policy ACL	VLAN				
Add 🗙 Delete							
VLAN Name 🛛 😪	ID 🗹 ACL	Name	< ◀	-			
4 0 0 H 1	0 🔹 items	per page		VLAN Name*	10		
		No items t	o display	VLAN Id*	10		
				ACL Name	Select ACL	•	
				✓ Save		O Cancel	
			0				

Step 13. Define a site tag that 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.

Start	* + Add * Delete	Enable WLAN	ble WLAN
Tags & Profiles	Number of WLANs selected : 0		
MI AN Drobin	Name	v. ID	 ✓ SSID
VVLAN Prome	open_wlan	1	open_wlan
Policy Profile		items per page	
() Policy Tag 🛷 📳	E +		
AP Join Profile	E +		
Flex Profile	≣ ◆		
Image: Site Tag Image: Sit			
 ● Flex Profile ● Site Tag 			
Image: Flex Profile Image: Flex Profile	<pre>E + E + click on "+" icon to odd a policy.</pre>		

Advanced Wireless Setup			
Start	+ Add × Delate		
Tags & Profiles	Site Tag Name		< Description
0 WLAN Profile	Add Site Tag		
O Policy Profile	Name*	Site_Lag	
0 Policy Tag 🧳 🔳 🔸	AP Join Profile	default-ap-profile	
g AP Join Profile 🗮 🔶	Flex Profile	branch_flex_profile	
6 Flex Profile 🗮 🔶	Control Plane Name	·	
6 Ste Tag 🖉	Enable Local Site		
6 RF Profile	Cancel		Save & Apply to Device

Step 14. 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, the AP would reboot to boot in FlexConnect mode.

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

Advanced Wireless Setup		
(Start	+ Tag APs	
Tags & Profiles	Number of APs: 3 Selected Number of APs: 3 Tag. APs	×
0 ····· WLAN Profile	Vame AP Model Tags	Policy Fag
O·····Policy Profile	yp-1-3800 AR-AP380 K9	branch_pol
6 Policy Tag 🛷 🔳 🕇	Policy store_policy	aranch_pol
	p-1-3700 Kg Site site_tag v	branch_pol
6 AP Join Profile	2 1 P 10 RF default- <u>rf</u> -tag	
6 Flex Profile	Changing AP Tag(s) will cause associated AP(s) to reconnect	
() Site Tag	🙄 Cancel 📔 Save & Apply to	Device
0 RF 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

Step 1. 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



	Authentication Authoriza	ation and Accounting	
a Dashboard	T AVA WIZITU		
Monitoring >	AAA Method List	Servers / Groups AAA Advance	ed
Configuration	General	Local Authentication	Default
Administration	Authentication	Local Authorization	Default 🔹
C Troubleshooting	Authorization	Radius Server Load Balance	DISABLED
	Accounting	Show Advanced Settings >>>	

Step 2. Use the AAA wizard to create the server and server groups.

Step 3. Define a name for the server and specify the IP address and shared secret.

Add Wizard							×
						Basic	O Advanced
c. 74	SERVER		SERVER GROUP	ASSOCIATION	MA	PAAA	
RADIUS 🔽	TACACS+	LDAP [
Name*	ISE						
IPv4 / IPv6 Server Address*	9.1.0.20						
PAC Key							
Key*							
Confirm Key*	1						
Cancel							Next 🗲

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

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

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.

Add Wizard		×
		Basic O Advanced
0	0	
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🖌 Authentication	Authorization Accounting	
General		
aaa_dot1x_system_auth_control		
Local Authentication	Default 🔻	
Local Authorization	Default 🔻	
Radius Server Load Balance	DISABLED	
Show Advanced Settings >>>		
← Previous		Save & Apply to Device

Step 6. Checkmark the authentication list and define the method type as dot ix and map the server group of the server group	Step 6.	Checkmark the authentication	list and define	the method type as	dot1x and map the serve	r group
--	---------	------------------------------	-----------------	--------------------	-------------------------	---------

		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	мар ааа
General 🖌 Authe	ntication 🗹 Authorization 🖌 Accounting	
General Authentication	Authorization	
Nethod List Name*	dot1x	
уре*	dot1x 🔻	
Group Type	group	
allback to local		_
wailable Server Groups	Assigned Server Groups	1
Idap	A ISE A	1
rad-group		1
freerad		1
TADUTO DEATEST	×	
1009.P_0.0101		

Step 7. Checkmark the authorization list, define the method type as network, and map the server group.

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

Step 8. Create a dot1x WLAN and map the method list on the WLAN.

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

Q Search Menu Items		B	Interface	Services
			Logical	AireOS Config Tran
📰 Dashboard			Ethernet	Application Visibility
			Wireless	Cloud Services
🕜 Monitoring	>	규	Layer2	Custom Application
5			VLAN	IOx
🔧 Configuration	>		VTP	Multicast
~				NetFlow
OS Administration	>		Radio Configurations	Python Sandbox
5.6			CleanAir	QoS
I roubleshooting			High Throughput	RA Throttle Policy
			Media Parameters	Tags & Profiles
			Network	AP Join
			Parameters	Flex
			RRM	Policy
		(Ì)	Routing Protocols	RF
			OSPF	Tags
		Ĥ	Security	WLANs

WIRELESS NETWORKS					
+ Add & Delate 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		
	WLAN ID*	2			
	Status				
	L				
	Cancel			🗎 Save & Apply 1	to Device

Step 9. Define the security for the WLAN.

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

Ad	d WLAN				×
	General	Security	Advanced		
_	Layer2	Layer3	AAA		
	Authentication List	dot1x1			
	Local EAP Authentication				
	🕽 Cancel			🗎 Save & Apply to Device]

Step 10. Create a policy profile that defines the switching capability of the WLAN and the interface mapping to the WLAN.



Policy Profile					
+ Add × Delete					
Ad	ld Poli cy Profile				×
Policy Profile Name	General Access Po	licies QOS and A	VC Mobility	Advanced	
default-policy-profile	🛦 Configurir	ng in enabled state will result in I	loss of connectivity for clients asso	ciated with this profile.	
	Name*	dot1x_wlan	WLAN Switching	Policy	
	Description	Enter Description	Central Switching		
	Status		Central Authenticati	on 🗹	
	Passive Client	DISABLED	Central DHCP		
	Encrypted Traffic Analytics	DISABLED	Central Association		
	CTS Policy		Flex NAT/PAT		
	Inline Tagging				
	SGACL Enforcement				
	Default SGT	2-65519			
	O Cancel			📓 Save & Apply t	to Device

Step 11. Defi	ne the VLAN	to be used	by the SSID.
---------------	-------------	------------	--------------

General Access Policies	QOS and AVC	Mobility	Advanced	
WLAN Local Profiling		WLAI	N ACL	
HTTP TLV Caching		IPv4 A	CL Search or Sele	ect 🔹
RADIUS Profiling		IPv6 A	CL Search or Sele	ect 🔹
DHCP TLV Caching		URLI	Filters	
ocal Subscriber Policy Name	Search or Select 🔹	Pre Au	uth Search or Sele	ect 🔻
VLAN		Dect A	Search or Sele	
/LAN/VLAN Group	11 🔹	FUSLA		
Multicast VLAN	Enter Multicast VLAN			

WLAN Timeout					
ession Timeout (Fabric Profile	Search or Select
	(sec)	1800		Umbrella Parameter Map	Not Configured
dle Timeout (sec))	300		WLAN Flex Policy	
dle Threshold (by	tes)	0		VLAN Central Switch	hing
lient Exclusion T sec)	imeout	60		Split MAC ACL	Search or Select
DHCP				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
AAA Policy	de				
olicy Name		default-aa	a-policy 🔻		
Accounting List		Search or	Select		
Step 12. Create a policy tag that bundles the policy profile and WLAN profile together.

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

Q. Search Menu Items		Ħ	Interface	Services
			Logical	AireOS Config Translator
📰 Dashboard			Ethernet	Application Visibility
			Wireless	Cloud Services
🕜 Monitoring	>	Å.	Layer2	Custom Application
2			VI AN	IOx
🔍 Configuration	>		VTP	Multicast
				NetFlow
(O) Administration	>		Radio Configurations	Python Sandbox
~ 0 -			CleanAir	QoS
Troubleshooting			High Throughput	RA Throttle Policy
			Media Parameters	Tags & Profiles
			Network	AP Join
			Parameters	Flex
		(RRM	Policy
			Routing Protocols	RF
			OSPF	Tags
		Ĥ	Security	WLANs
			AAA	Wireless
				Access Points

anage Tags					
Policy	Site	RF	AP		
		Add Policy Tag			
+ Add		Name*	branch_policy		
Policy	Tag Name	Description	Enter Description		
branch					
default	-policy-tag	+ Add 🗶			
4 4 1	► ► 10	WLAN Profile		V Policy Profile	
		2 < 0 > 1	10 🔻 items per page		No items to display
		Map WLAN and I	Policy		
		WLAN Profile*	dot1x_wlan 🗸 🕄	Policy Profile*	dot1x_wlan 🔻
			×	× .	
		(Constal			
		Juancel			Save & Apply to Devic

Step 13. Create a flex profile that defines the flex AP properties.

To create a flex profile, navigate to Configuration > Tags and Profile > Flex.

Q Search Menu Items	Ē	Interface	ß	Services
		Logical		AireOS Config Tr
🔜 Dashboard		Ethernet		Application Visibi
		Wireless		Cloud Services
Monitoring Monitoring	، ال	Layer2		Custom Applicati
20 0 0	7	VLAN		lOx
S Configuration	>	VTP		Multicast
~ · · · · ·		Padia Capfaurationa		NetFlow
20 Administration	>	Radio Configurations		Python Sandbox
S CA T I I I I		CleanAir		QoS
X I roubleshooting		High Throughput		RA Throttle Policy
		Media Parameters		Tags & Profiles
		Network		AR Join
		Parameters		Flow
		RRM		Delies
	(I.	Routing Protocols		Policy
Francisco de de completa de la comp	<u>e</u> 1	/ Rodding Protocols		RF -
		OSPF		lags
	Ĥ) Security		WLANs
		ААА		Wireless
		ACL		Access Points
		Advanced EAP		Advanced
		PKI Management		Air Time Fairness
		Local EAP		Fabric

Step 14. Define the native VLAN for the FlexConnect AP.

Flex Profile	elete				
Flex Profile Nar	ne Add Flex Profile		✓ Descriptic	20	×
	General Local	Authentication Policy ACL	VLAN		
	Name*	branch_flex_profile	Multicast Overridden Interface		
	Description	Enter Description	Fallback Radio Shut		
ſ	Native VLAN ID	3	Flex Resilient		
L	HTTP Prove Port	0	ARP Caching		
			Efficient Image Upgrade		
	Address	0.0.0.0	Office Extend AP		
	CTS Policy		Join Minimum Latency		
	Inline Tagging				
	SGACL Enforcement				
	CTS Profile Name	default-sxp-profile _x			
	Cancel				🛱 Save & Apply to Device

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

eneral Local Authen	tication Policy ACL	VLAN				
Add 🗱 Delete						
VLAN Name 😪 II	D 🗹 ACL Name	~ <		<u></u>		
4 0 F F 10	D 🔻 items per page		VLAN Name*	11		
	No item	is to display	VLAN Id*	11		
			ACL Name	Select ACL	•	
			✓ Save		Cancel	
		5				_

Step 16. Create a site tag that maps the flex and RF profile.

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

Q Search Menu Items			Interface	Services
			Logical	AireOS Config Translator
🔜 Dashboard			Ethernet	Application Visibility
			Wireless	Cloud Services
(2) Monitoring	>	규	Layer2	Custom Application
		000	VI AN	lOx
🔍 Configuration	>			Multicast
				NetFlow
(0) Administration	>		Radio Configurations	Python Sandbox
			CleanAir	QoS
💥 Troubleshooting			High Throughput	RA Throttle Policy
			Media Parameters	Tags & Profiles
			Network	AP Join
			Parameters	Flex
			RRM	Policy
		(ł.	Routing Protocols	RF
			OSPF	Tags
			Security	WLANs
			ААА	Wireless

Step 17. Uncheck "Enable Local Site" to map the flex profile on the site tag.

Manage Tags					
Policy	Site RF	AP			
+ Add × D	Add Site Tag	_		×	
Site Tag Name	Name*	site_tag			
0 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 F H	Control Plane Name	•	-		
	Enable Local Site 2				
	Cancel			📓 Save & Apply to De 4	

- **Step 18.** 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 APs:

Navigate to Configuration > Wireless Setup > Advanced.

	Catalyst C	9800-CL Wireless Co	ontrolle	Г				
Q Search Menu Items Dashboard Monitoring Configuration Administration Troubleshooting) (1) ,	Interface Logical Ethernet Wireless Layer2 VLAN VTP Radio Configurations CleanAir High Throughput Media Parameters Network	6	Services AireOS Config Translator Application Visibility Cloud Services Custom Application IOX Multicast NetFlow Python Sandbox QoS RA Throttle Policy Tags & Profiles AP. Join		Wire this screen allows you to creating Policies and Ta deployed WLAN Policy (Mandatory) WLAN Profile Policy Profile	less Setup Flow C design Wireless I so. Once the design to the Access Poin DESIGN PHASE Tags & Profile Site Policy (Optional) AP Join Profile Flex Profile	AN Configuration. It involves is completed, they can be its right here. Radio Policy (Optional) RF Profile RF Tag
	(†	Parameters RRM Routing Protocols OSPF Security AAA ACL Advanced EAP		Flex Policy RF Tags WLANs Wreless Access Points Advanced		Policy Tag #	Site Tag DEPLOY PHASE Apply to APa (Mandatory) Tag APs s and push config	e uration to them
		PKI Management Local Policy TrustSec Threat Defense URL Filters Web Auth Wireless AAA Policy Wireless Protection Policies	_	Air Time Fairness Fabric Media Stream Mesh Mobility Wireless Setup Basic Advanced	T V S R	TERMINOLOGY ag ALAN Policy, Policy Profi ite Policy - AP Profile, S adio Policy - Radio Char	le Ite Profile acteristics Start Now	ACTIONS Go to List View Creste New

Q, Search Menu Items	Advanced Wireless Setup					
		Wireless Setup Fil	ow Overview		Grant	
Dashboard		This screen allows you to design Wirel	ess LAN Configuration. It involves			
		creating Policies and Tags. Once the deployed to the Access	design is completed, they can be Points right here.		Tags & Profiles	
Monitoring >		DESIGN P	HASE		Togs at romos	
Configuration		Tags & P	rofiles		WLAN Profile	
		WLAN Policy Site Po	licy Radio Policy		Policy Profile	= +
205 Administration >		(Mandatory) (Option	al) (Optional)		Policy Tag	
💥 Troubleshooting		WLAN Profile AP Join Pr	ofile RF Profile			
		Delinu Drofile	OF Tag			- Province (province)
		Policy Profile	in ing a		AP Join Profile	■ +
		Policy Tag 🛷 Site Tag	4	Start Now	Flex Profile	= +
						3
		DEPLOY P	HASE		G Site Tag #	
han an a		Apply to	APs			
		Manda	tory)		BF Profile	= +
18월 28일 전 전 18일 전 18 18월 18일 전 18일 전 18월 18일 전 18g 전					C L L L L L L L L L L L L L L L L L L L	
1 20.00		Tag APs			@ RF Tag #	i≡ +
		Select APs and push o	onnguration to them		Apply	
에서 이는 바이다. H. 이		TERMINOLOGY	ACTIONS		- Hobbit	
		Tan			O Tag APs	=
		WLAN Policy, Policy Profile	Go to List View			
		Site Policy - AP Profile, Site Profile			Done	
		Radio Policy - Radio Characteristics	Create New		-	



Advanced Wireless Setup					
Start	+ Tag APs Number of APs: 3	~			
Tags & Profiles	Selected Number of	of APs: 3			
🖲 WLAN Profile 🗮 🕇	AP V Name	AP Model 🗸		AP × Mode	Admin Status Ope
O Policy Profile 🗮 🕇	💟 ap1-3800	AIR-AP3802I-B- K9	0081.c4a0.6fe0	Flex	Enabled Reg
6 ····· Policy Tag	🖌 ар2-3 Тас	g APs			× ,
	🖌 ар1-3 Т	ags			g
O AP Join Profile	N N N	olicy bran	ch-policy 🗸)	
6 Flex Profile	s	iite site_	tag 🗸		
6 Site Tag 🛷 🔳 🕇	R	C defa	ult-rf-tag 🗸 🗸		
	_	Changing AP Tag(s) will	l cause associated A	VP(s) to reconn	ect
0 RF Profile					
0 R∉ Tag 🕜 🔳 🔶		D Cancel		Save & Ap	ply to Device

Using a static mapping to tag the APs.

		Manage Tags			
🔜 Dashboard		Policy	Site	RF AP	
Monitoring	>	Tag Sourc	e Static	Filter	
🖏 Configuration	>	Priority	Tag Source	Status	
() Administration	>	0	Static		
💥 Troubleshooting		1	Location		
		2	Filter		
		з	AP		
		Drag and Drop T Revalidate Tag S Apply	ag Sources to change priorities iources on APs		

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

	Manage Tags		
📷 Dashboard	Policy Site F	RF AP	
Monitoring >	Tag Source Static	Filter	
🖏 Configuration 🔹 🔸	+ Add at Delete		
ⓒ Administration >	AP MAC Address	✓ Policy Tag Name	✓ Site Tag Name
💥 Troubleshooting	≪ ≪ 0 ► ► 10 v items	per page	

AP MAC Address*	1122.3344.5566		add the man address of
Policy Tag Name	branch-policy	•	the AP
Site Tag Name	site_tag	•	
RF Tag Name	default-rf-tag	•	

Manage 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	
4 4 1 ▶ ▶ 10 v items per page	3			1 - 1 of

Using a filter to tag the AP:

Q Search Menu Items	Manage Tags			
Dashboard	Policy Site RF AP			
Monitoring >	Tag Source Static Filter			
Representation Sciences	+ Add St Delete			
တြဲ Administration 🤸	Priority - Rule Name - AP name regex	Policy Tag Name	 Site Tag Name 	 RF Tag Name
💥 Troubleshooting	[4 4 0 ⊨ ⊨] 10 • kems per page			No items to display

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				

Manage Tags										
Policy	Site	RF AP								
Tag Source	Static	Filter								
+ Add ×										
Priority	Rule Name	Ý	AP name regex	×.	Policy Tag Name	×.	Site Tag Name	×	RF Tag Name	
	rule_1		ap*		branch-policy		site_tag		default-rf-tag	1
4 4 1 k	► 10 v iter	ms per page								1-

The access point summary page shows the source based on which tags were assigned to an AP.

Access Point	s																					
V All Acce	ess	Points																				
Number of AP(s): 3																					
AP Name		Total Slots	×	AP Model	×.	Base Radio MAC	×	AP Mode	¥.	Admin Status	×	Operation Status		Policy Tag	×	Site Tag	×	RF Tag	×	Tag Source		Location
ap-1-3800	3	3		AIR-AP3802I-B-K9		0081.c4a0.6fe0		Flex		Enabled		Registered		branch-policy	y	site_tag		default-rf-ta	g	Filter	T	default location
ap-2-3800	3	3		AIR-AP3802I-B-K9		0081.c4a0.7550		Flex		Disabled		Registered	- 1	branch-policy	y	site_tag		default-rf-ta	g	Filter	t.	default location
ap-1-3700	2	2		AIR-CAP3702I-A-KS	3	80e0.1d7b.8610		Flex		Disabled		Registered		branch-policy	y	site_tag		default-rf-ta	g	Filter	Т	default location
ie e 1	ь	10 .	ite	ms ner nade											-				-			1 - 3 of 3 a

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 will reboot to boot in FlexConnect mode.

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

FlexConnect VLAN override

AAA override of VLAN on individual WLAN is supported for local switching. In order to have a dynamic VLAN assignment, the AP would have the VLAN pre-created based on a configuration using the flex profile mapped to the site tag. The VLANs used in the flex profile are 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 modes.
- 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 the AAA override are not present on the AP, the client will be excluded and not allowed access to the network.
- Multicast traffic on an 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

Step 1. 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



Step 2. Use the AAA wizard to create the serve	r and server groups.
--	----------------------

cisco Ca te.te.zoteteza Q Search Manu Items Dashboard	talyst C9800-CL Wireless Co Authentication Authorizatio	ntroller n and Accounting	
Monitoring	AAA Method List	Servers / Groups AAA Advanced	1
Configuration >	General	Local Authentication	Default
 Administration Troubleshooting 	Authentication Authorization Accounting	Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default

Step 3. Define a name for the server and specify the IP address and shared secret.

Add Wizard						×
					Basic	c 🔿 Advanced
S. 77.	SERVER		SERVER GROUP ASSO	CIATION	MAP AAA	
RADIUS 🔽	TACACS+	LDAP	ו			
Name*	ISE					
IPv4 / IPv6 Server Address*	9.1.0.20					
PAC Key						
Key*						
Confirm Key*						
Cancel						Next 🗲

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

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

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.

Add Wizard		×
		Basic Advanced
0	O	
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authentication	Authorization Accounting	
in a second s		
aaa_dot1x_system_auth_control		
Local Authentication	Default 🔻	
Local Authorization	Default	
Radius Server Load Balance	DISABLED	
Show Advanced Settings >>>		
← Previous		🖺 Save & Apply to Device

Add Wizard		×
		Basic O Advanced
	⊘	
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authentic	ation 🖌 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	> ISE *	
← Previous		📓 Save & Apply to Device

Step 6. Define the method type as dot1x and map the server group.

Step 7. 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		
Method List Name*	authz		
Туре*	network 🔹		
Group Type	group v		
Fallback to local			
Available Server Groups	Assigned Server Groups		
♥ Previous		🖹 Save & Apply	y to Device

Step 8. Create a dot1x WLAN and map the method list on the WLAN.

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

Q Search Menu Items			Interface	6	Services
			Logical		AireOS Config Translator
🔜 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
(2) Monitoring	>	ᅹ	Layer2		Custom Application
		000	MAN		lOx
义 Configuration	>				Multicast
			VIF		NetFlow
(O) Administration	>		Radio Configurations		Python Sandbox
			CleanAir		QoS
💥 Troubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
가지 않는 것이 있는 것이 있는 것이 있는 것이 있는 것이 있는 것이 있다. 같은 것이 같은 것이 있는 가 같은 것이 같은 것이 같은 것이 있는 것이 있는 것이 있는 것이 있는 것이 있는 것이 없는 것			Parameters		Flex
가 있는 것이 있는 것이 있는 것이 있는 것이 있는 것이 있다. 같이 많은 것이 있는 것이 많은 것이 없다. 같이 있는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것			RRM		Policy
		(t)	Routing Protocols		RF
			OSPF		Tags
		\oplus	Security		WLANs

WIRELESS NETWORKS + Add × Delete Fi Number of WLANs selected : 0	nable WLAN	able WLAN			
Name Name	Add WLAN				×
open_wlan	General	Security	Adva	anced	
	Profile Name*	dot1x_wlan	Radio Policy	All	- 1
	SSID	dot1x_wlan	Broadcast SSID		- 1
	WLAN ID*	2			- 1
	Status				- 1
					- 1
					- 1
					- 1
					_
	Cancel			📓 Save & Apply to De	vice

Add WLAN			ŝ
General	Security	Advanced	
Layer2	Layer3	ААА	
Layer 2 Security Mode	WPA + WPA2 V	Fast Transition Adaptive Enabled	
MAC Filtering		Over the DS	
Protected Management Fran	ne	Reassociation Timeout 20	
PMF	Disabled v		
WPA Parameters			
WPA Policy			
D Cancel		📔 Save & Apply to D)evice

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

Step 9. Create a flex profile. Create a VLAN on the flex profile, which is the VLAN returned by the AAA.

Q Search Menu Items		Interface	ß	Services
		Logical		AireOS Config Translator
🔜 Dashboard		Ethernet		Application Visibility
		Wireless		Cloud Services
(2) Monitoring	〉 品	Layer2		Custom Application
		M AN		Юх
义 Configuration	>			Multicast
	-			NetFlow
(0) Administration	>	Radio Configurations		Python Sandbox
		CleanAir		QoS
💥 Troubleshooting		High Throughput		RA Throttle Policy
		Media Parameters		Tags & Profiles
		Network		AP Join
		Parameters		Flex
		RRM 📙		Policy
	(1	Routing Protocols		RF
		OSPF		Tags
	\oplus	Security		WLANs
		AAA		Wireless
		ACL		Access Points
		Advanced EAP		Advanced
		PKI Management		Air Time Fairness
		Local EAP		Fabric

Fiex Profile I	Name Add Flex Profile		✓ Descriptic	n	
default-flex-	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		
			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 v			

Seneral Local Authentication	on Policy ACL VLAN			
+ Add X Delete				
VLAN Name 🛛 🖬 D 🗟	ACL Name v	•		
	items per page	VLAN Name*	11	
	No items to display	VLAN Id*	11	
		ACL Name	Select ACL	
		✓ Save	Ca	ncel

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

Q Search Menu Items			Interface	6	Services
			Logical		AireOS Config Translator
📻 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
🕜 Monitoring	>	놂	Layer2		Custom Application
	-		VLAN		lOx
Configuration	>		VTP		Multicast
\sim .					NetFlow
{O} Administration	>		Radio Configurations		Python Sandbox
			CleanAir		QoS
💥 Troubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
			Parameters		Elev
			RRM		Policy
		(1 , 1)	Routing Protocols		RF
			OSPF		Tags
		Ĥ	Security		WLANs
			AAA		Wireless
			ACL		Access Points
			Advanced EAP		Advanced
			PKI Management		Air Time Fairness
			Local EAP		Fabric

Policy Profile				
+ Add × Delete Ac	Id Policy Profile General Access Po	licies QOS and AVC	Mobility Ad	X dvanced
default-policy-profile	🛕 Configurir	ng in enabled state will result in loss of cor	nectivity for clients associated	d with this profile.
	Name*	dot1x_wlan	WLAN Switching Polic	y
	Description	Enter Description	Central Switching	
	Status		Central Authentication	
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	D Cancel			🗃 Save & Apply to Device

dd Poli cy Profile						
General A	ccess Policies	QOS and AVC	Mobility	Adv	anced	
WLAN Local Profiling	L		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 🚽	Pro A	uth	Search or Select	
VLAN			165	au i		
VLAN/VLAN Group		10 🔻	Post /	Auth	Search or Select	•
Multicast VLAN		Enter Multicast VLAN				
		·				
Cancel					Save & Apply to	Device

General	Acces	s Policies	QOS and AVC	Mobility	Advanced
WLAN Timeou	ıt			Fabric Profile	Search or Select
Session Timeou	t (sec)	1800		Umbrella Parameter Map	Not Configured
dle Timeout (se	c)	300		WLAN Flex Policy	t in the second s
dle Threshold (I	oytes)	0		VLAN Central Switc	hing
Client Exclusion sec)	Timeout	60		Split MAC ACL	Search or Select
DHCP				Air Time Faimess	Policies
HCP Enable				2.4 GHz Policy	Search or Select 🔹
HCP Server IP	Address	0.0.0.0		5 GHz Policy	Search or Select
ow more >>>					
AAA Policy					
Allow AAA Ove	rride				
NAC State					
Policy Name		default-a	aa-policy 🔻		
Accounting List		Search or	r Select		

Step 11. Map the WLAN to the policy profile.

Navigate to Configuration > Tags and create a policy tag mapping the WLAN and policy profile.



Mana	ge Tags							
	Policy	Site	RF	AP				
			Add Policy Tag					×
+	Add	* Delete	Name*	branch_policy				
	Policy Ta	ag Name	Description	Enter Description				
	branch							
1	default-p	olicy-tag	+ Add ×					
H	∢ 1 ▶	► ► <u>10</u>	WLAN Profile		×	Policy Profile		×
			2 < 0 > >	I 10 🔻 items per page			No items to) display
			Map WLAN and F	Policy				
			WLAN Profile*	dot1x_wlan 🔻	3	Policy Profile*	dot1x_wlan ,	
					×	×		
			Cancel				📔 Save & Apply to I	Devic 4

Step 12. Create 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 to the profile created.

diate Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ient Provisioning -Policy Elements
Dictionaries Conditions -Result	8
0	
Authentication	Authorization Profile Authorization Profile
✓ Authorization	* Name sand-vlan
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
	VLAN Tag ID 1 Edit Tag ID/Name 11
	★ Advanced Attributes Settings
	E Select an item
	★ Attributes Details
	Access Type = ACCESS_ACCEPT Tuppel-Private-Group-ID = 1:11
	Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6
	Save Reset



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

Manag	e Tags						
Pr	olicy	Site RF	AP				
+/	Add 🗙 D	Add Site Tag	_			×	
	Site Tag Name	Name*	site_tag				
1	SS	Description	Enter Description				
	branch	AP Join Profile	default-ap-profile	•			
	sand-site default-site-tag	Flex Profile	branch_flex_profile	•	1		
14	4 1 × H	Control Plane Name		•	-		
		Enable Local Site 2					
		Cancel				🖹 Save & Apply to De 4	

Step 14. Map the policy site tag and RF tag on the AP using the advanced config wizard.



Navigate to Configuration > Wireless Setup > Advanced.



CISCO CISCO Cat	aiyst Caroo-CF M	vireless Contro	Siler										weicome sa	10 10	40 E 1		(III)
	Advanced Wirele	ess Setup															Back
Dashboard	Start	Tags & Profiles		4 Nur Sei	+ Tag. APs nber of APs: 3 acted Number of	AP8: 3											
	Ø	WLAN Profile		+	AP Name	AP Model ~	AP MAC ~	AP - Mode	Admin Status	 Operation Status 	✓ Policy ✓ Tag	Site - Tag	RF Tag 🗸	Location ~	Country -	Hyperiocation Method	× 1
Administration	0	Policy Profile		+	sand-ewic- ap-1	AIR-AP38021-8- K9	0081.c4s0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
Tenchlophenting	0	Policy Tag 🛷		+ -	sand-ewic- ap-2	AIR-AP3802I-8- K9	0081.04a0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
roubleshooting		Te] sand-3700	AIR-CAP3702I- A-K9	80e0.1d7b.8610	Flex.	Enabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
	0	AP Join Profile		+	(4 1 ⊨	10 🔹 items p	ser page									1 - 3 of 3 items	c
	0	Flex Profile		+													
	0	Ste Tag 🧳		+													
	0	RF Profile		+													
	0	RF Tag 🥔		+													
		Apply															
	0	Tag APs															
			2														

Advanced Wireless Setup					
Start Tags & Profiles	+ Tag APs Number of APs: 3 Selected Number of	If APs: 3			
• WLAN Profile	AP Vame	AP Model 🗸	AP MAC 🖂	AP < Mode	Admin Y Ope Status Stat
Policy Profile	🖌 ap1-3800	AIR-AP3802I-B- K9	0081.c4a0.6fe0	Flex	Enabled Reg
0 Policy Tag	🖌 ap2-3 Tag	g APs			* .
	🖌 ap1-3 🏅	ags			q
0 AP Join Profile	H K T	olicy bran	ch-policy 🗸]	
6 Fiex Profile	s	ite site_	tag 🗸		
0 Site Tag	R	F	ult-rf-tag 🔻		
0 RF Profile 🔳 🕇		hanging AP Tag(s) wil	l cause associated A	AP(s) to reconn	pect
0 RF Tag 🕜 🔳 🕇		D Cancel) Save & Ap	pply to Device

Step 15. Associate a client on the WLAN and authenticate using the username 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 that the client is mapped to.

Double-click on the client MAC to open up the details of the client session.

Cisco Cataly	yst C9800-CL Wireless Controller						Welcon	ne sand 🛛 💏	*	• 0	0 (H
Q. Sesrch Menu Items	Clients										
Dashboard	Clients Sleeping Clients	Excluded Clients									
Monitoring >	at Delete										
Configuration	Total Client(s) in the Network: 1										
A destruction	Client MAC Address	IPv4/IPv6 Address	AP Name	< WLAN	 ✓ State 	< Protocol	< User Name	< Device Typ	8	< Role	4
Administration >	1c36.bbef.6492	9.1.11.252	ap-1-3800	10	Run	11ac	sand-wireless			Loca	2
💥 Troubleshooting	i4 4 1 ⊨ 10 v items per page									1 - 1 of 1 d	ents C

Clients				Client		
Clients Sleeping Clients	Excluded Clients			General QOS Statistics ATF S	Statistics Mobility History Call Sta	atistics
X Delets Total Client(s) in the Network: 1 Client MAC Address Client MAC Address Client MAC Address Client MAC Address click on the client mac to open up, delaits page	 IPv4/IPv8 Address 9.1.11.252 	< AP Name ap-1-3800	× V	Client Properties AP Properties MAC Address IPV4 Address User Name Policy Profile Flex Profile Wireless LAN 1d Wireless LAN 1d Wireless LAN 1d Uptime(sec) OCX version Power Save mode Current TriArelSet Supported Rates	Security Information Client Statisti 1c36.bbef.6492 9.1.11.252 sand-vireleas dot1x_wlen branch_flex_profile 10 dot1x_wlen 0081.c490.6fee 104 seconde No CCX support OFF m9 ss3 9.0,18.0,36.0,48.0,54.0 Den	cs QOS Properties
				Puicity waininger state Last Policy Manager State Encrypted Traffic Analytics Multiceatt U.AN Access VLAN Access VLAN Senerr IP DNS Snooped IPv4 Addresses DNS Snooped IPv6 Addresses 11v DMS Capable FlexConnect Data Switching FlexConnect Authentication	Ruine Complete No 0 11 0 9.1.0.20 None No Local Local Central	

Client		
General QOS Statistics ATF	Statistics Mobility Histor	ry Call Statistics
Client Properties AP Properties	Security Information	Client Statistics QOS Properties
Encryption Cipher	CCMP (AES)	•
Authentication Key Management	802.1x	
ЕАР Туре	PEAP	
Session Timeout	1800	
Session Manager		
Interface	capwap_90000007	
IIF ID	0x90000007	
Authorized	TRUE	
Common Session ID	10040109000000F03A	\$55440
Acct Session ID	0x00000000	
Auth Method Status List		
Method	Dot1x	
SM State	AUTHENTICATED	
SM Bend State	IDLE	
Local Policies		
Service Template	wlan_svc_dot1x_wlan	(priority 254)
Absolute Timer	1800	
Server Policies		
Output SGT	0010-35	
VLAN	11	
Resultant Policies		
Output SGT	0010-35	
VLAN	11	
Absolute Timer	1800	-

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 being VLAN failure.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client will be assigned a 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

Step 1. 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.



Step 2.	Use the AAA	wizard to	create t	he server	and server	groups.
---------	-------------	-----------	----------	-----------	------------	---------

Cisco Catal	lyst C9800-CL Wireless Co	ntroller	
Sesrah Mesu Items Dashboard Monitoring	Authentication Authorization	n and Accounting Servers / Groups AAA Advanced	i
Configuration	General Authentication Authorization Accounting	Local Authentication Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default Default DisableD

Step 3. Define a name for the server and specify the IP address and shared secret.

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

Add Wizard		
		Basic O Advance
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
RADIUS		
Name*	ISE	
Group Type	RADIUS	
MAC-Delimiter	none 🔻	
MAC-Filtering	none v	
Dead-Time (mins)	1-1440	
Available Servers	Assigned Servers	1
freerad ISE-2 ISE	<pre>> ISE * </pre>	
♦ Previous		Next 🗲

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

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.

Add Wizard				\$
				Basic Advanced
0-		O		
SERVI	R	SERVER GROUP ASSOCIATIO	NC	MAP AAA
General 🖌 A	uthentication 🗌 Aut	horization 🗌 Accountin	g	
General				
aaa_dot1x_system_auth_c	ontrol			
Local Authentication	Default	•		
Local Authorization	Default	•		
Radius Server Load Balanc		ED		
Show Advanced Settings >	>>			
				🗃 Save & Apply to Device

Add Wizard		×
		Basic O Advanced
0		
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🖌 Authentica	ation 🕢 Authorization 🖌 Accounting	
General Authentication	Authorization	
Method List Name*	dot1x	
Type*	dot1x 🔹	
Group Type	group 👻	
Fallback to local		
Available Server Groups	Assigned Server Groups	
Idap A tacacs+ rad-group freerad	> ISE ^	
radgrp_branch 👻	*	
← Previous		Save & Apply to Device

Step 6. Define the method type as dot1x and map the server group.

Step 7. Define the method type as network and map the server group.

Add Wizard			×
		• Basic	O Advanced
SERVER	SERVER GROUP ASSOCIATION	MAP AAA	
General 🗹 Authentication General Authentication Aut	Authorization Accounting		
Method List Name*	authz		
Type*	network v		
Group Type	group v		
Available Server Groups	Assigned Server Groups		
Idap tacacs+ rad-group freerad radgrp_branch +	> ISE *		
← Previous		📔 Save & App	ly 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.

Q Search Menu Items			Interface	6	Services
			Logical		AireOS Config Translator
🔜 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
(2) Monitoring	> ,	Д.	Layer2		Custom Application
-			VIAN		IOx
🔍 Configuration	>				Multicast
			VIF		NetFlow
(0) Administration	>		Radio Configurations		Python Sandbox
			CleanAir		QoS
💥 Troubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
			Parameters		Flex
			RRM		Policy
	(1	Routing Protocols		RF
			OSPF		Tags
	(Ð	Security		WLANs

WIRELESS NETWORKS + Add x Delete Et Number of WLANs selected : 0	nable WLAN	able WLAN			
Name Name	Add WLAN				×
open_wlan	General	Security	Adva	anced	
	Profile Name*	dot1x_wlan	Radio Policy	All	
	SSID	dot1x_wlan	Broadcast SSID		
	WLAN ID*	2			
	Status				
	Cancel			冒 Save & Apply to I	Device

Add WLAN			
General	Security	Advanced	
Layer2	Layer3	ААА	
Layer 2 Security Mode	WPA + WPA2 •	Fast Transition Adaptive Enabled	
MAC Filtering		Over the DS	
Protected Management Fran	ne	Reassociation Timeout 20	
PMF	Disabled •		
WPA Parameters			
WPA Policy			
D Cancel		📓 Save & Apply to D	evice

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

Step 9. Create a policy profile, enable local switching and central authentication on the profile, map the default VLAN for the WLAN, and enable AAA override.



Policy Profile				
+ Add × Delete				
Policy Profile Name	ld Policy Profile			×
d open_wian	General Access Po	licies QOS and AVC	Mobility	Advanced
default-policy-profile	🛦 Configurir	ng in enabled state will result in loss of c	onnectivity for clients associa	ted with this profile.
	Name*	dot1x_wlan	WLAN Switching Po	licy
	Description	Enter Description	Central Switching	
	Status		Central Authentication	
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	D Cancel			🛱 Save & Apply to Device

General Access Policies	QOS and AVC	Mobility	Advance	ed	
WLAN Local Profiling		WLA	N ACL		
HTTP TLV Caching		IPv4 /	ACL	arch or Select	•
RADIUS Profiling		IPv67	ACL Se	arch or Select	•
DHCP TLV Caching		URL	Filters		
Local Subscriber Policy Name	Search or Select	Pre A	uth Sea	arch or Select	•
VLAN				prab or Coloat	
VLAN/VLAN Group	10 🔻	Post	Auth 58	arch or object	•
Multicast VLAN	Enter Multicast VLAN				

	Access	Policies	QOS and AVC	Mobility	Advanced
MLAN Timeo	ut			Fabric Profile	Search or Select
Session Timeo	ıt (sec)	1800		Umbrella Parameter Map	Not Configured
Idle Timeout (si	ec)	300		WLAN Flex Policy	1
Idle Threshold (bytes)	0		VLAN Central Swite	ching 🔽
Client Exclusior (sec)	Timeout	60		Split MAC ACL	Search or Select
DHCP				Air Time Fairness	a Policies
DHCP Enable				2.4 GHz Policy	Search or Select 🔹
DHCP Server If	Address	0.0.0.0		5 GHz Policy	Search or Select 👻
AAA Policy	prride				
Allow AAA Ove					
Allow AAA Ove NAC State Policy Name		default-aaa-po	alicy v		

Step 10. Map the WLAN to the policy profile.

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



Manage Tag	is						
Policy	Site	RF	AP				
		Add Policy Tag					×
+ Add	N Delete	Name*	branch_policy				
Polic	cy Tag Name	Description	Enter Description				
bran	ch						
defai	ult-policy-tag	+ Add × De					
4 4 1	▶ ▶ 10	WLAN Profile		×	Policy Profile		v i
		2 < 0 > >	10 🔹 items per page			No items	to display
		Map WLAN and Po	licy				
		WLAN Profile*	dot1x_wlan	3	Policy Profile*	dot1x_wlan	•
				×	*		
		Cancel				📓 Save & Apply to	o Devic 4

Step 11. Create a flex profile and define a VLAN on the flex profile returned by the AAA radius server.

Q Search Menu Items	Interface	🐻 Services
	Logical	AireOS Config Translator
🔜 Dashboard	Ethernet	Application Visibility
	Wireless	Cloud Services
Monitoring >	🖧 Layer2	Custom Application
	VLAN	IOx
Configuration	VTP	Multicast
\sim	De die Oesterweitere	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
	(Protocols	POlicy
		Tane
	🕒 Security	WEAINS
second from the other than the second	ААА	Wireless
	ACL	Access Points
	Advanced EAP	Advanced
	PKI Management	Air Time Fairness
	Local EAP	Fabric

Flex Profile +Add Flex Profile Nam default-flex-p	e Add Flex Profile		✓ Descriptic	n X
H 4 1 + +	General Local	Authentication Policy ACL	VLAN	
	Name*	branch_flex_profile	Multicast Overridden Interface	
	Description	Enter Description	Fallback Radio Shut	
	Native VI AN ID	3	Flex Resilient	
L			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		
(Cancel			l Save & Apply to Device

ieneral Local Authentic	ation Policy ACL	N			
+ Add 🔉 🕫 Delete					
VLAN Name 🛛 D	 ACL Name 	. •			
i 🛛 o 🚺 🖂 🛛 10	items per page	VLAN Name*	11		
	No items to display	VLAN Id*	11		
		ACL Name	Select ACL	•	
		✓ Save	5	Cancel	

Step 12. 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.

diale Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cliv	ent Provisioning - Policy Elements
Dictionaries + Conditions - Results	5
0	
Authentication	Authorization Profile
✓ Authorization	* Name sand-xtan
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
	VLAN Tag D 1 Edit Tag D/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 Reset


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

Manage	Tags							
Pal	icy	Site RF	AP					
+ A	dd 🗶 D	Add Site Tag	_			_	×	
1	Site Tag Name	Name*	site_tag					
0	85	Description	Enter Description					
	branch	AP Join Profile	default-ap-profile	•				
	sand-site	A	hunnah flav avafila					
	default-site-tag	Flex Profile	branch_nex_pronie					
14		Control Plane Name		•				
		Enable Local Site 2						
		Cancel				🗎 Save & App	ly to De <mark>4</mark>	

Step 14. Map the policy site tag and RF tag on the AP using the advanced config wizard.

Assigning a site tag on an 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.

Q. Search Menu Items	Advanced Wireless Setup		
Dashboard		Wreless Setup Flow Overview This screen allows you to design Wreless LAN Configuration, it involves creating Policies and Tags. Once the design is completed, they can be designed to be Access Polish right here.	art Tags & Profiles
Monitoring >		DESIGN PHASE	
🖧 Configuration 🕠		Tags & Profiles	WLAN Profile
Administration >		WLAN Policy Ste Policy Radio Policy (Mandatory) (Optional) (Optional)	Policy Profile
💥 Troubleshooting		WLAN Profile AP Join Profile RF Profile	Policy Tag 🏼 🖗 🔳 🗭
		Policy Profile RF Tsg @	AP Join Profile
		Policy Tag # Site Tag # Start Now ->	Berner Flex Profile
· 동안 한 것이 하는 것도 ~ -		DEPLOY PHASE	9 Site Tag 🛷 📰 🛧
		Apply to APs (Mandatony) Tag APs Betect APs and push configuration to them	0
		TERMINOLOGY ACTIONS	
		Tag W.A.N Policy, Policy Profile Site Policy - AP Profile, Site Profile Radio Policy - Radio Charscteristics	α Της ΑΡ3

sana Menu tenter Dashboard Montoring Configuration Troubleshooting Tr	15 CO 16 10 20181020																	
Desthboard Monitoring → Configuration → Administration → Troubleshooting Troubleshooting	h Meriu Items	Advanced Wirele	ess Setup															Bac
Configuration	hboard itoring >	Start .	Tags & Profiles		-* Nar Sei	+ Tag APs nber of APs: 3 acted Number of	APs: 3											
dministration Perior Parker Perior Parker<	figuration >	ø	WLAN Profile		+	AP Name	AP Model 🖂	AP MAC ×	AP Mode	Admin Status	Operation Status	 ✓ Policy Tag 	Site ~ Tag	RF Tag 🗸	Location ~	Country ~	Hyperlocation Method	
ub/schooling Policy Tag # III + Policy Tag # II	inistration >	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	
Discription of Profile II + (Pring + Tring + II + (Pring +	11-11-11-11-11-11-11-11-11-11-11-11-11-	0	Policy Tag 🗳	=	+ -	sand-ewic- ap-2	AJR-AP3802I+8- K9	0081.c4s0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
0 Image: AP Join Pathe Image: AP Join Path Image: AP Join Pathe Image: AP	bleshooting				R	sand-3700	AIR-CAP3702I- A-K9	80e0.1d7b.8610	Flex	Enabled	Registered	sand-policy	sand-site	default-rf- tag	default location	US	Local	
0 III +	병은 이번 도망한	ø	AP Join Profile	=	•	(1)×	10 🔹 items p	er page									1 - 3 of 3 items	c
Che Tro E		o	Flex Profile	=	٠													
0 RF Profile		e	Site Tag 🧳	=	+													
0 10 TO 0 = +		o	RF Profile		+													
		0	RF Tag 🛷		٠													
Apply			Apply															
Tra APA		0	Tog APS															

Advanced Wireless Setup					
Start Tags & Profiles	+ Tag APs Number of APs: 3 Selected Number of A	Ps: 3			
🚯 WLAN Profile	AP × Name	AP Model 🛛 👒	AP MAC 🗸	AP × Mode	Admin V Ope Status Stat
O······Policy Profile 🔳 +	🖌 ap1-3800 🕌	AIR-AP38021-B- (9	0081.c4a0.6fe0	Flex	Enabled Reg
O Policy Tag	ap2-3 Tag A	\Ps			×
	ap1-3 Tag	8		_	g
O AP Join Profile	Polic	brand	ch-policy 🗸]	
🚯 Flex Profile 📃 🕇	Site	site_	tag 🗸		
6 Site Tag 🛷 🔳 🕇	RF	defau	ult-rf-tag 🗸		
	Char	nging AP Tag(s) will	cause associated A	AP(s) to reconn	ect
RF Profile					
0 RF Tag 🧳 🧮 🕇	5	Cancel		j Save & Ap	ply to Device

Step 15. Associate a client on the WLAN and authenticate using the username 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 to.

In this step, the AAA returns VLAN 11, which is present in the AP database results in the localswitched WLAN. Double-click on the client MAC to open the details of the client session.

Clinis Clinis Dashboard Image: Clinis O Monitoring Image: Clinis Configuration Image: Clinis Configuration Toul Clinis Other Mon. Address Image: Clinis Clinis Image: Clinis Clinis Image: Clinis Image: Clinis Image: Clinis<	Cisco Cataly	st C9800-CL Wireless Controller						Welcom	ne sand 🏻 🏘	% E	0 0	0
Distribution Clients Steping Clients Excluded Clients (2) Monitoring Image: Configuration Image: Configuration Image: Client Simple Client Si	Q. Search Menu Items	Clients										
Monitoring M	📰 Dashboard	Clients Sleeping Clients	Excluded Clients									
?: Configuration → Total Glen(a) in the Newerk: 1 Get Glen(b) in the Newerk: 1 Clent MAC Adviews Nov/PVC Adviews AP Name WLAN Same Protocol User Name Device Type Ref GADMinistration > Inclicitude 432 9.1.11.252 Sp-1-3803 10 Fan 11ac sand-writes Locid VP TroubleShooting 4 1 1 press per page 11 for lowes 11 for lowes	Monitoring >	at Delete										
Administration >> Concert MuCAdviews >> PAXPAPA Adviews >> AP Name >> WLAN >> Same >> Protocol >> User Name >> Device Type >> Rele Tools best 6422 0.11.052 8pr-3800 10 Pau 11ac sand-writes >> Local PC Troubletshooting 4>1 Pa	2 Configuration	Total Client(s) in the Network: 1										
00 Administration → 1c38.bdet.64z2 9.1.11.252 tep-1-3800 10 Run 11ac sand-winders Local NP Troubleshooting H 1 10 tems pir page 1 - 1 of 1 direts	A destate to a sector	Client MAC Address	IPv4/IPv6 Address	< AP Name	< WLAN	< State	- Protocol	< User Name	< Device Ty	pe	< Role	4
Troubleshooting	Administration >	1c36.bbef.6492	9.1.11.252	ap-1-3800	10	Run	11ac	sand-wireless			Loca	E .
	💥 Troubleshooting	iems per page									1 - 1 of 1 d	ients C

General QOS Statistics ATF S	Statistics	Mobility Histo	ſy	Call Statistics		
Client Properties AP Properties	Security I	nformation	Client	Statistics	QOS Properties	
Current TxRateSet	m8 ss3	1				
Supported Rates	9.0,18.	0,36.0,48.0,54.0				
Policy Manager State	Run					
Last Policy Manager State	IP Lear	n Complete				
Encrypted Traffic Analytics	No					
Multicast VLAN	0					
Access VLAN	11					
Anchor VLAN	0					
Server IP	9.1.0.2	0				
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	Ē				
FlexConnect Central Association	Yes					
antenna 0	1 s ago	-34 dB	m			
antenna 1	1 s ago	34 dB	m			
Eogre Client	False					
Eogre Match Status	no tunr	nel profile or aaa	data			
lobility						
Move Count	0					
Role	Local					
Roam Type	None					
Complete Timestamp	10/24/	2018 02:23:04 U	TC			

Client	-					3
General	QOS Statistics	ATF Statistics	Mobility Histor	ry Call Statistic	s	
Client Prop	perties AP Prop	erties Securit	y Information	Client Statistics	QOS Properties	
Encryption (Cipher	CCN	IP (AES)			-
Authenticati	ion Key Management	802.	1x			
EAP Type		PEA	P			
Session Tim	neout	180	D			
Session Mar	nager					
Interface		cap	wap_90000007			- 1
IIF ID		0x90	000007			
Authorized		TRU	E			
Common Se	ession ID	100	40109000000F03A	55440		
Acct Sessio	on ID	0x00	0000000			
Auth Metho	d Status List					
Method		Dot1	x			
SM State		AUT	HENTICATED			
SM Bend St	ate	IDLE				
Local Policie	18					- 1
Service Terr	plate	wla	n_svc_dot1x_wlan	(priority 254)		- 1
Absolute Tin	ner	180	00			
Server Polici	ies					- 1
Output SGT		00	0-35			- 1
VLAN		11				
Resultant Po	licies					- 1
Output SGT		00'	0-35			- 1
VLAN		11				
Absolute Tin	ner	180	00			

Step 16. Create an authorization profile to return a VLAN that is not present on the AP database but on the WLC.

In this example,	VLAN 5 is prese	nt on the	WLC and	not or	n the AP	database,	which	results in	the
WLAN being ce	ntral switched.								

diate Identity Services Engine	Home
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements
Dictionaries + Conditions - Results	
Authentication	Authorization Profiles > vlan-wlc Authorization Profile
▼ Authorization	* Name vlan-w/c
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Device Profile 🛛 🔐 🕀
▶ Posture	Service Template
➤ Client Provisioning	Track Movement
	Common Tasks DACL Name ACL (Filter-ID) Security Group
	VLAN Tag ID 1 Edit Tag ID/Name SI
	Advanced Attributes Settings
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:5 Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6
	Save Reset

Step 17. Validation on the presence of VLAN 5 on the WLC.

Navigate to Configuration > VLAN.



VLAN			
SVI VLAN VLA	Create VLAN		×
+ Add × Delete	VLAN ID*	5	
VLAN	Name		
	State		
4	RA Throttle Policy	None	
□ 15	IGMP Snooping	DISABLED	
14 4 1 ▶ ▶ 10 v items per	ARP Broadcast		
	Dest Manakana		0 Search
	Port Members	Available (1)	Associated (0)
		Gil	
			NO Associated Members
	Cancel		🖺 Save & Apply to Device

Step 18. Associate a client on the WLAN and authenticate using the username 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 to and the switching properties for the client.

Double-click on the client MAC to open the details of the client session.

Cisco Cata	lyst C9800-CL Wireless Controller						Welcome sand	1 🕷
Q. Search Menu Items	Clients							
📷 Dashboard	Clients Sleeping Clients	Excluded Clients						
Monitoring >	* Delete							
Configuration	Total Client(s) in the Network: 1							
	Client MAC Address	IPv4/IPv6 Address	< AP Name	~ WLAN	< State	< Protocol	< User Name ≤	Device Ty
203 Administration \$	1c36.bbef.6492	9.1.5.200	ap-1-3800	10	Run	11ac	sand-wireless	
💥 Troubleshooting	4 4 1 ▶ 10 → items perman	the details						

ent				
General QOS Statistics A	TF Statistics Mobility H	listory	Call Statistics	
Client Properties AP Propertie	s 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	e		
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			

ient								
General QOS S	Statistics	ATF S	tatistics	Mobility History	Y	Call Statistic	S	
Client Properties	AP Prop	erties	Security	y Information	Client	Statistics	QOS Properties	
Encryption Cipher		1	CCM	IP (AES)				
Authentication Key Ma	anagement		802.	1x				
EAP Type			PEAR	P				
Session Timeout			1800)				
Session Manager								
Interface			capv	vap_90000007				
IIF ID			0x90	000007				
Authorized			TRUE	E				
Common Session ID			1004	01090000001303B	C4500			
Acct Session ID			0x00	000000				
Auth Method Status L	ist							
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	00				
Server Policies								
Output SGT			001	0-35				
VLAN			5					
Resultant Policies								
Output SGT			001	0-35				
VLAN			5	1				
Absolute Timer			180	0				

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 the WLC fails?

How can wireless clients perform 802.1X authentication if the WAN link between the branch and data center fails? Is there any impact on branch mobility during WAN failures?

Does the FlexConnect solution provide no operational branch downtime?

FlexConnect local authentication and backup/local radius can address the above concerns by enabling the branch to operate independently in case of a 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 Wave 1 APs.
- This feature can be used with central authentication or local authentication. In the 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



Figure 7.

Local Authentication with External RADIUS server at the Branch

Steps for local authentication and backup radius server

Procedure

Step 1. 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 >	Authentication Authorization + AAA Wizard AAA Method List	n and Accounting Servers / Groups AAA Advance	зd	
Configuration	Ceneral Authentication Authorization Accounting	Local Authentication Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default Default CISABLED	

Add Wizard								×
							 Basic 	O Advanced
	SERVER		S	ERVER GROUP	ASSOCIATION	3	- O MAP AAA	
RADIUS 🛛	TACACS+	LDAP						
Name*	freerad1							
IPv4 / IPv6 Server Address*	9.1.0.21							
PAC Key								
Key*								
Confirm Key*								
Cancel								Next >

Add Wizard		*
		Basic O 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	1
ISE * freerad *	> freerad *	
+ Previous		Next 🗲

Add Wizard			×
			Basic O Advanced
SERVER	SERVER GRO	OUP ASSOCIATION	МАР ААА
General 🖌 Authentication 🖌	Authorization 🗹	Accounting	
General Authentication Author	prization		
aaa_dot1x_system_auth_control	ENABLED		
Local Authentication	Default 🔹		
Local Authorization	Default 🔹		
Radius Server Load Balance	DISABLED		
Show Advanced Settings >>>			
			🗃 Save & Apply to Device

Add Wizard		×
		Basic O Advanced
SERVER	SERVER GROUP ASSOCIATION	МАР ААА
General 🖌 Auth	Authorization 🖌 Accounting 🗌	
Method List Name*	dot1x	
Туре*	dot1x 🔹	
Group Type	group v	
Fallback to local		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+ rad-group radgrp_branch	freerad	
+ Previous		冒 Save & Apply to Device

Add Wizard		×
		Basic O Advanced
Ø		
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authenticatio	n 🖌 Authorization 🖌 Accounting 🗌	
General Authentication	Authorization	
Method List Name*	authz	
Туре*	network 🔹	
Group Type	group 🔻	
Fallback to local		
Available Server Groups	Assigned Server Groups	
radius ▲ Idap tacacs+ rad-group radgrp_branch ▼	> freerad	
← Previous		Save & Apply to Device

Step 2. 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.



Id WLAN			
General	Security	Advanced	
Layer2	Layer3	AAA	
Authentication List	dot1x		
Local EAP Authentication		_	
Cancel		📓 Save 3	& Apply to Device

Add WLAN			
General	Security	Advanced	
Layer2	Layer3	ААА	_
Layer 2 Security Mode	WPA + WPA2 V	Fast Transition Adaptive Enabled	
MAC Filtering		Over the DS	
Protected Management Fram	6	Reassociation Timeout 20	
PMF	Disabled 🔻		
WPA Parameters			
WPA Policy			
O Cancel		冒 Save & Apply to D	evice

WIRELESS NETWORKS + Add	Enable WLAN	able W.AN			×
open_wian	General	Security	Adva	anced	
	Profile Name* SSID WLAN ID* Status	dot1x_wlan dot1x_wlan 2 ENABLED	Radio Policy Broadcast SSID	AII	
	Cancel			🗎 Save & Ap	ply to Device

Step 3. Create a policy profile and enable local switching and central authentication on the profile.



Policy Profile					
+ Add × Delete	ld Policy Profile				×
Policy Profile Name open_wian	General Access Po	QOS and AVC	Mobility	Advanced	1
default-policy-profile	A Configurir	ng in enabled state will result in loss o	of connectivity for clients associat	ed with this profile.	
	Name*	dot1x_wlan	WLAN Switching Pol	icy	
	Description	Enter Description	Central Switching		
	Status		Central Authentication		
	Passive Client	DISABLED	Central DHCP		
	Encrypted Traffic Analytics	DISABLED	Central Association		
	CTS Policy		Flex NAT/PAT		
	Inline Tagging				
	SGACL Enforcement				
	Default SGT	2-65519			
	D Cancel		1	🗃 Save & Apply to Device	

Step 4. Map the default VLAN for the WLAN.

General Access Policies	QOS and AVC	Mobility	Advanced	
WLAN Local Profiling		WLA	N ACL	
HTTP TLV Caching		IPv4 A	ACL Search or Select	•
RADIUS Profiling		IPv6 A	CL Search or Select	•
HCP TLV Caching		URL	Filters	
Local Subscriber Policy Name	Search or Select 🔹	Pre A	uth Search or Select	•
VLAN				
/LAN/VLAN Group	10 🔻	Post A	Auth Search or Select	۲
Multicast VLAN	Enter Multicast VLAN	-		
	J			

Step 5. Map the WLAN to policy profile.

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

Q Search Menu Items			Interface	Services
			Logical	AireOS Config Translator
🔜 Dashboard			Ethernet	Application Visibility
			Wireless	Cloud Services
(2) Monitoring	>	뷺	Layer2	Custom Application
		000	VI AN	lOx
🔍 Configuration	>			Multicast
				NetFlow
(0) Administration	>		Radio Configurations	Python Sandbox
			CleanAir	QoS
Troubleshooting			High Throughput	RA Throttle Policy
			Media Parameters	Tags & Profiles
			Network	AP Join
			Parameters	Flex
			RRM	Policy
		(t)	Routing Protocols	RF
			OSPF	Tags
		(f)	Security	WLANs
			AAA	Wireless
			40	Access Points

Manage Tags				
Policy Site	RF AF	p		
	Add Policy Tag			×
+ Add * Delete	Name*	pranch_policy		
Policy Tag Name	Description	Enter Description		
default-policy-tag	+ Add X Delete			
	WLAN Profile	Ý	Policy Profile	~
	2 • • • • [10 🔻 items per page		No items to display
	Map WLAN and Policy			
	WLAN Profile*	ot1x_wlan 🔹 3	Policy Profile*	dot1x_wlan 🔻
		×	*	
	Cancel			冒 Save & Apply to Devic 4

Step 6. Create a flex profile to create the VLAN on the profile to be used by the SSID.

Q Search Menu Items		Interface	6	Services
		Logical		AireOS Config Translator
🔜 Dashboard		Ethernet		Application Visibility
		Wireless		Cloud Services
Monitoring	› <u>بل</u>	Layer2		Custom Application
		VIAN		IOx
🔍 Configuration	>	VTP		Multicast
~	4			NetFlow
(O) Administration	>	Radio Configurations		Python Sandbox
		CleanAir		QoS
X Troubleshooting		High Throughput		RA Throttle Policy
		Media Parameters		Tags & Profiles
		Network		AP Join
		Parameters		Flex
		RRM 📙		Policy
	(Ì)	Routing Protocols		RF
		OSPF		Tags
	\oplus	Security		WLANs
		ААА		Wireless
		ACL		Access Points
		Advanced EAP		Advanced
		PKI Management		Air Time Fairness
and here all the state of the state of the		Local EAP		Fabric

Flex Profile	ne Add Flex Profile		 Description 	on	×
H 4 T F F	General Local	Authentication Policy ACL	VLAN		
	Name*	branch_flex_profile	Multicast Overridden Interface		
	Description	Enter Description	Fallback Radio Shut		
	Native VI AN ID	3	Flex Resilient		
l			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-profile _X			
	Cancel				冒 Save & Apply to Device

and certer aroup	Teerad Y	LEAP	
AP Fast Profile	Select Profile	PEAP	
		TLS	
		RADIUS	
ers			
+ Add X Delete			

Add 🗙 D					
VLAN Name	🗹 ID 🧭 ACL Name	× 🖣 🛌 🔤			
4 0 Þ ÞI	10 🔻 items per page	VLAN Name*	10		
	No iten	ns to display VLAN Id*	١٩		
		ACL Name	Select ACL	•	
		✓ Save		Cancel	

Step 7. Create a site tag and map the flex profile on the site tag.

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



Manage Tags							
Policy	Site	AP					
+Add × D	Add Site Tag					×	
Site Tag Name	Name*	site_tag					
1 55	Description	Enter Description					
branch	AP Join Profile	default-ap-profile	•				
default-site-tag	Flex Profile	branch_flex_profile	•				
	Control Plane Name		•				
	Enable Local Site 2						
	Cancel				冒 Save & Apply to D	e 4 .	

Step 8. 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 an 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.

Cisco Ca	t C9800-CL Wireless Controller	
Q. Search Menuitems Dashboard Monitoring Configuration Administration X Troubleshooting	Interface Services Logical AireOS Config Translator Ethernet Application Visibility Wireless Cloud Services Layer2 Custom Application VLAN IOx VLAN Multicast VTP NetFlow Radio Configurations Python Sandbox CleanAir QoS High Throughput RA Throttle Policy Media Parameters Tags & Profiles Network AP Join	olves h be
	Parameters Flox RRM Policy RAUting Protocols RF OSPF Tags Security WLANs AAA Wireless ACL Access Points Advanced EAP Advanced PKI Management Advances	
	Local EAP Fabric Local EAP Fabric Local Policy Media Stream TrustSec Mesh Threat Defense Mobility URL Filters Wireless Setup Wireless AAA Policy Advianced Wireless Protection Policies Start Now	

Q. Search Menu Items	Advanced Wireless Setup									
		Wireless Set	up Flow Overv	iew		Grant				
📷 Dashboard	This	creen allows you to design	Wireless LAN C	configuration. It involves		()				
Monitoring		deployed to the A	coess Points rig	pht here.			Tags & Profiles			
		DES	GN PHASE				WI AN Profile	-	4	
🔾 Configuration 💦 🔸		Tag	s & Profiles						-	
Administration		WLAN Policy Sil	te Policy	Radio Policy		0	Policy Profile	100	+	
		(Mandatory) (C	(ptional)	(Optional)		0	Policy Tag 🛷	=	+	
* Troubleshooting		AP Jo	oin Profile	RF Profile						
[[[[변성금: 굵변 6] 목		olicy Profile Flex P	Profile	RF Tag 🛷		0	AP Join Profile		+	
	1	olicy Tag 🚜 Site T	30 4		Start Now -	Ĩ	-			
						0	Flex Profile	圕	+	
		DEPL	OY PHASE			0	Site Tag 🛛 🦸		+	
		Ap	ply to APs							
1 [방송] : : (방송] : : : : : : : : : : : : : : : : : : :		(N	landatory)			0	RF Profile	-	*	
		L.				Ŭ	-			
에 알퉁물로 모나 삼 것		Select APs and p	ush configuratio	in to them		0	- RF Tag 🛷	懎	+	
lan ^{ba} shiri i						_	Apply			
		TERMINOLOGY		ACTIONS			Tag APs	-		
	Тад			Go to List View		-	Lindiana			
	WLAT	Policy, Policy Profile				Done				
집 방송 전 기법 집 중	Site F	Diloy - AP Profile, Site Profile Dolloy - Radio Characteristi	*	Create New						
	- House									



Advanced Wireless Setup						
Start	+ Tag APs					
Tags & Profiles	Selected Number of	of APs: 3				
6 ····· WLAN Profile	AP ~ Name ~	AP Model 🗸	AP MAC ~	AP × Mode	Admin Status	 ✓ Ope Stat
e Policy Profile	🖌 ap1-3800	AIR-AP3802I-B- K9	0081.c4a0.6fe0	Flex	Enabled	Regi
8 Policy Tag 🧳 🗮 🔶	🖌 ap2-3 Ta	g APs				×g
	🖌 ap1-3	lags				gi
AP Join Profile	N N P	Policy bran	ch-policy 🗸			
🚯 Flex Profile 🔳 🔶	s	Site site_	tag 🗸			× 1
6 Site Tag 🖌 🔳 🕇	R	RF defa	ult-rf-tag 🗸			- 1
	L	Changing AP Tag(s) wil	l cause associated A	P(s) to reconn	nect	- 1
6 ····· RF Profile						_
0 RF Tag 🧳 🔳 🔶		D Cancel		Save & Ap	oply to Dev	ice

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 perform dot1x authentication on the AP itself using the local radius facility.

Procedure

To have the FlexConnect AP configured as the radius server, repeat steps 2, 3, 4, 5, 7, and 8 in the procedure section of configuring local authentication with external radius server.

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

Procedure



Q Search Menu Items		Interface	G	Services
		Logical		AireOS Config Translator
🔜 Dashboard		Ethernet		Application Visibility
		Wireless		Cloud Services
🕜 Monitoring	> 규	Layer2		Custom Application
~		VLAN		lOx
🔧 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
		Parameters		Flex
		RRM L		Policy
	(tr) Routing Protocols		PE
		ocpr		Togo
		USPF		Tays
	6	Security		WLANS
		AAA		Wireless
		ACL		Access Points
		Advanced EAP		Advanced
		PKI Management		Air Time Fairness
		Local EAP		Fabric

Step 2. Specify the native VLAN ID for the AP. On the local authentication, specify the EAP methods to be used.

dd 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	
		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		
D Cancel			Save & Apply to Device

Add local users for authentication on the AP. The local users reside on the AP.

Add Flex Profile			×
General Local Authentication Policy ACL VLAN			
Radius Server Group	LEAP		
EAP Fast Profile	PEAP		
	TLS		
	RADIUS		
Users	L		
+ Add			
Userheime	Licercome *	sample	
I I I I I I I I I I I I I I I I I I I	Osemanie Deserved Tess		
	Password Type	UNENCRYPTED	
	Password *		
	Confirm *		
	✓ Save	Cancel	
			_
Cancel	2	冒 Sa	ve & Apply to Dev

Add						_
ALANI Name	✓ ID ✓ ACL Name I 10 ▼ items per page	×	VLAN Name*	10		
	1	No items to display	VLAN Id*	10		
			ACL Name	Select ACL	•	
			✓ Save		D Cancel	
			1			

CCKM/OKC and PMK caching

CCKM/OKC and PMK caching enables fast roaming for wireless clients. Fast roaming is achieved by caching a derivative of the primary 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, and the controller takes care of distributing the primary key to the APs. The controller distributes the primary key to all the APs whose site tag and policy tag are the same. This results in the ability to do fast roaming across the AP within the same site. The distribution of the primary key is done based on the site tag of the AP site the client initially associates, and the controller now finds all the APs that have a similar site tag and policy tag and pushes the primary key on those APs, thus enabling fast roaming among the APs.

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 APs. On 16.10, the EAP method supported for the AP as the radius server is EAP-LEAP.
- Fast roaming is not supported with the default site tag. If the APs are mapped to a default site tag, the primary 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 upstream 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 the WLC to FlexConnect APs.
- Peer-to-peer blocking action configured as drop or forward-upstream on WLAN is treated as peer-topeer blocking enabled on the FlexConnect AP.

Steps

Procedure

Refer to 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	- 1
Diagnostic Channel		Band Select	- 1
P2P Blocking Action	Disabled 🔹	IP Source Guard	- 1
Multicast Buffer	Disabled Drop	WMM Policy Allowed 🗸	
Media Stream Multicast- direct	Forward-UpStream	Off Channel Scanning Defer	
Max Client Connections		Defer Priority 0 1 2	
Per WLAN 0]	3 4 🖌 5	-
O Cancel		📓 Save & Appl	y to Device

Once the P2P blocking action is configured on the WLAN, 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 that 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 is applied on the WLAN dot11 interface and is enforced to all the clients connecting on that SSID.
- WLAN ACL The ACL is applied on the WLAN dot11 interface and is enforced to all the clients connecting on that SSID.
- Client ACL- The ACL is 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 a 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 the 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, 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 that the ACL works.

Procedure

Step 1. Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step 2. Perform the following steps:

- Click on "Add" to create an ACL, and 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 L	st				
ashboard	+ Add 🙁 (Associating I	nterfaces			
Monitoring >		1 - BEDIEDENT	ACL Name		v Dvil Extende	ACL Type
Configuration		Add ACL Setup			Countre	×
Administration		ACL Name*	flex_acl_11	ACL Type	IPv4 Extended	
W Troubleshooting		Rules				3
	in D	Sequence*	1	Action	deny v	
		Source Type	any 🔻		4	_
	4 4 1 b b	Destination Type	any 🔹			
		Protocol	ahp		(max)	
		Log		DSCP	None	
e, a er adan e		+ Add x Delete				
		Action	Source V Source V IP Wildcard	IP Wildcard	Protocol - Port	Port DSCP × Log ×
			10 🔹 items per page			No items to display
		Cancel				🗎 Save & Ap <mark>6</mark> to Device

Step 3. Refer to the steps in the procedure of the advanced configuration wizard for the following:

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

Advanced wireless setup wizard:

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

ieneral	Access Policies	QOS and AVC	Mobility	Advanced
	A Configuring in enabled	I state will result in loss of	f connectivity for clients asso	ciated with this profile.
Name*	open_1	wlan	WLAN Switching	Policy
Description	Enter D	Description	Central Switching	
Status	ENABLE		Central Authenticati	on 🗹
Passive Client		ABLED	Central DHCP	
Encrypted Traffic	Analytics	ABLED	Central Association	
CTS Policy			Flex NAT/PAT	
Inline Tagging			-	
SGACL Enforcem	ient			
Default SGT	2-655	19		

Add Policy Profile					×
General Access Po	QOS and AVC	Mobility	Advanced		
WLAN Local Profiling		WLA	N ACL		
HTTP TLV Caching		IPv4 A	ACL [flex_acl_1	1	
RADIUS Profiling		IPv6 A	ACL Search or	Select 🔻	
DHCP TLV Caching		URL	Filters		
Local Subscriber Policy Name	Search or Select	Pre A	uth Search or	Select 🗸	
VLAN		Doot /	Auth Search or	Select -	
VLAN/VLAN Group	10 🔻	FUSLA			
Multicast VLAN	Enter Multicast VLAN				
Cancel			📔 Save & A	Apply to Devic	е

Step 4. Assign the ACL on the flex profile by mapping the VLAN and ACL.

Define the native VLAN for the FlexConnect APs.

General Loca	al Authentication Policy ACL	VLAN	
Name*	branch_flex_profile	Multicast Overridden Interface	
Description	Enter Description	Fallback Radio Shut	
Notive M AN 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	t 🔲		
CTS Profile Name	default-sxp-profilex		
CTS Profile Name	derauit-sxp-profilex		

Step 5. Push the ACL to AP by using the policy ACL configuration on the flex profile.

Add Flex Profile		×
General Local Au	uthentication Policy ACL VLAN	
+ Add 🛛 🗶 Dele		
ACL Name	Central 🗸 Pre Auth 👒	ACL Name* flex-aci11
1 ч о н н	10 v items per page	Central Webauth
	NU ILEMS ID DISplay	Pre Auth URL Filter Search or Select
		Save Save Save
Cancel		留 Save & Apply to Device

Step 6. Verification on the controller.

Navigate to Monitoring > Wireless > Clients.

Clients	Client
	General QOS Statistics ATF Statistics Mobility History Call Statistics
Clients Sleeping Clients Excluded Clients	Client Properties AP Properties Security Information Client Statistics QOS Propertie
	Auth Method Status List
* Delete	Method Dot1x
Total Official (1) is the Material 1	SM State AUTHENTICATED
Total Cilencis) in the Network: 1	SM Bend State IDLE
Client MAC Address V IPv4/IPv8 Address V AP Name	Local Policies
10:36:bb:ef:64:92 9.1.11.252 sand-ewlo-ap-1	
4 4 1 ⊨ 10 v items per page	Service Template wlan_svc_sand-ewlc-dot1x (priority 254)
	Absolute Timer 1800
click on Mac address	VLAN 11
	Service Template wian_svc_sand-ewic-dot1x (priority 254)
	Accolute Inter 1800
	VLAN
	Server Policies
	Filter-ID flex_scl_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 that the ACL works.

Procedure

Step 1. 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 and 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 tems	Access Control	List				
Dashboard	+ Add	Collete 🖉 🔗 Associating	j Interfaces			
Monitoring >		ACL-REDIRECT	ACL Name		UPv4 Extend	ACL Type
🔍 Configuration 🕠	0	Add ACL Setup				×
 Administration 		ACL Name*	flex_acl_11	ACL Type	IPv4 Extended 🔹	
X Troubleshooting	0	n Rules				
		Sequence*	1	Action	deny 👻	
		in Source Type	any		4	
		Destination Type	any 🔻		-	
		Protocol	ahp			
		Log		DSCP	None 🔻	
		+ Add as Dele				
		Sequence ✓ Action	Source - Source - Wildcard	Destination × Destination IP Wildcard	n < Source < I Protocol < Port	Destination < Port DSCP < Log <
		⊲ ⊲ 0 ⊳ ⊳	10 🔹 items per page			No items to display
		Cancel				📓 Save & Ap <mark>6</mark> to Device

- Step 3. Refer to the steps in the procedure of the 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.

ieneral	Access Policies	QOS and AVC	Mobility	Advanced	
	A Configuring in enal	oled state will result in loss	of connectivity for clients ass	ociated with this profile.	
Name*	оре	en_wlan	WLAN Switching	Policy	
Description	Ent	er Description	Central Switching		
Status	ENAE	BLED	Central Authentica	tion 🔽	
Passive Client		DISABLED	Central DHCP		
Encrypted Traf	Tic Analytics	DISABLED	Central Association		
CTS Policy			Flex NAT/PAT		
Inline Tagging			-		
SGACL Enforc	ement				
Default SGT	2-6	35519			

General Access Policies	QOS and AVC	Mobility	Advanced	
WLAN Local Profiling		WLA	NACL	
HTTP TLV Caching		IPv4 A	ACL Search or Se	elect 🔹
RADIUS Profiling		IPv6 A	ACL Search or Se	elect 🔹
OHCP TLV Caching		URL Filters		
ocal Subscriber Policy Name	Search or Select	Pre A	uth Search or Se	elect 🔹
VLAN/VLAN Group	10	Post /	Auth Search or Se	elect 🔻
Multicast VLAN	Enter Multicast VLAN			
🕽 Cancel			📔 Save & Ap	oply to Devic

Step 4. Assign the ACL on the flex profile by mapping the VLAN and ACL.

Define the native VLAN for the FlexConnect APs.

dd Flex Profile			
General Local	Authentication Policy ACL	VLAN	
Name*	branch_flex_profile	Multicast Overridden Interface	
Description	Enter Description	Fallback Radio Shut	
Native VI AN ID	21	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-profile _x		
D Cancel			Bave & Apply to Device

Step 5. Define the VLAN and ACL mapping on the flex profile.

dd Flex Profile			×
General Local Authentication Policy ACL VLAN	1		
+ Add x Delete			
VLAN Nime 🗸 ID 🗟 ACL Name 🗸			
I I V Items per page	VLAN Name*	10	
No items to display	VLAN Id*	1 to 4096	
	ACL Name	flex_acl_11 v	
	✓ Save	Cancel	
	4		
Cancel	1	📓 Save & Apply to De	ev <mark>.5</mark>

Client ACL overview

- This feature allows application of the 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 APs that have 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 the AAA.

For the creation of the ACL, refer to the steps in the WLAN ACL use case. Refer to step 5 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 to the procedure section of the VLAN override use case.

FlexConnect VLAN override

Procedure

Step 1. Authorization profile on ISE for returning ACL as an AAA attribute.

uthorization Profile	
action izacion Profile	
* Name	sand-acl
Description	
* Access Type	
100000 1)pc	ACCESS_ACCEPT Y
Network Device Profile	deta Cisco 💌 🕀
Service Template	
Track Movement	
Dessive Identity Treation	
Passive identity Tracking	
🖉 ACL (Filter-ID)	flex_acl_12 in
Security Group	
 Security Group VLAN Advanced Attribut 	tes Settings
Security Group VLAN Advanced Attribut	tes Settings
Security Group VLAN Advanced Attribut	tes Settings
Security Group VLAN Advanced Attribut	tes Settings
Security Group VLAN Advanced Attribut Select an Rem Attributes Details	tes Settings
Security Group VLAN Advanced Attribut Select an Rem Attributes Details Access Type = ACCESS J	tes Settings
Security Group VLAN Advanced Attribut Select an Rem Attributes Details Access Type = ACCESS_f Filter-ID = flex_ad_12.in	tes Settings
Security Group VLAN Advanced Attribut Select an Rem Attributes Details Access Type = ACCESS_f Filter-ID = flex_ad_12.in	tes Settings

Step 2. Verification of ACL getting enforced on the AP and WLC.

Navigate to Monitor > Wireless > Clients.

lients	Client
	General QOS Statistics ATF Statistics Mobility History Call Statistics
Clients Sleeping Clients Excluded Clients X Delete Total Client (a) In the Network: 1 Client MAC Address × IPv4/Pv6 Address × AP Name 1c:38:bbxef64:92 9:1.11.252 sand-ewio-ap-1 4 4 1 1 10 tems per page	Client Properties AP Properties Security Information Client Statistics QOS Propert Auth Method Status List Method Dot1x SM State AUTHENTICATED SM Brend State Local Policies Service Template wlan_svc_sand-ewlc-dot1x (priority 254) Absolute Timer 1800
click on Mac address	VLAN 11 Service Template wlan_avc_sand-ewlc-dot1x (priority 254) Absolute Timer 1800 VLAN 11 Server Policies 11
	Filter-ID flex_acl_12 Output SGT 0011-34
	Filter-ID flex_acl_12 Output SGT 0011-34
	Resultant Policies
	Fiter-ID flex_aci_12
	VLAN 11
	Absolute Timer 1800
	Filter-ID flex_acl_12

Limitations

- The use of downloadable ACL is not supported on FlexConnect local switching. The downloadable ACLs
 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 being ACL failure.
- In the case of local authentication, the client will be de-authenticated 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 pre-image download to work, the controller should be in 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

Step 1. 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 in ssis (St):	nstall summary L] Installed Package(s) Information: : I - Inactive, U - Activated & Uncommitted, C - Activated & Committed, D - Deactivated & Uncommitted
Туре	St	Filename/Version
IMG IMG	Ċ	16. 10. 1. 0. 1026 16. 10. 1. 0. 41
Auto	abort	timer: inactive

Step 2. Once the file is added, the image can be pushed to the AP using the following CLI:

"ap image predownload"

wic-2# wic-2#ap image p wic-2#ap image predownload wic-2#ap image predownload wic-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 Time Re
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	16.11.1.11 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					
AP Name	Primary Image	Backup Image	Predownload Status	Predownload Version N	Next Retry T
ap-1-3800 ap-2-3800 ap-1-3700	16.10.1.37 16.10.1.37 16.10.1.37	16.10.1.33 16.10.1.33 16.10.1.33	Complete Complete Complete	16.10.1.33 16.10.1.33 16.10.1.33	000
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
ap-1-3800 ap-2-3800 ap-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	16.10.1.33 16.10.1.33 16.10.1.33	0 0 0
wlc-2#ap image reset wlc-2#					

Step 3. After the AP has been reset, use 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 package, 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#sh install summary [Chassis 1] Installed Package(s) Information: State (St): I - Inactive, U - <mark>Activated & Uncommitted</mark> , C - Activated & Committed, D - Deactivated & Uncommitted						
Туре	St	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 system is rebooted, use the following CLI to have the changes persist across reboot.

"Install Commit"

This 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 in 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 to 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 Primary/Server, and the rest of the APs of the same model will work as Secondary/Client and will pre-download the AP image from the primary. The distribution of AP images 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.



Figure 8.

FlexConnect Smart AP Image Upgrade Mechanism

Summary

- · Primary and secondary APs are selected for each AP model per site tag
- Primary downloads image from WLC
- Secondary downloads image from primary AP using TFTP
- · Reduces downtime and saves WAN bandwidth
- The primary is chosen by the system. The AP with the lowest MAC among the same type and model is to become a primary

Procedure

Procedure

Step 1. For steps to create a flex profile and to have it applied on the AP, refer to the steps in the advanced config wizard section of the document.

Start	+ Add	* Dolère		
Ŷ	Add Flex	Profile		
Tags & Profiles	Genera	Local Authentication Poli	cy ACL VLAN	
WLAN Profile	Name*	branch_flex_profile	Multicast Overridden Interface	
Policy Profile	+ Descript	Enter Description	Fallback Radio Shut	
● ······ Policy Tag ● i	*		Flex Resilient	
	Native V	LANID	ARP Caching	
AP Join Profile	+ HTTP Pr	oxy Port 0	Efficient Image Upgrade	
0 Flex Profile	HTTP-P Address	roxy IP 0.0.0.0	Office Extend AP	
0 Site Tag 🖌 🔳	CTS Po	licy	Join Minimum Latency	
	Inline Ta	gging		
O······ RF Profile	SGACL	Enforcement		
0 RF Tag /	CTS Pro	file Name default-sxp-profile _x v]	

Enable smart AP image upgrade on the flex profile.

Step 2. Download the image on the controller as outlined in step 1 of the AP image pre-download process. Issue the CLI below to initiate the smart AP image upgrade and also to see the primary AP elected for a given type of AP and the primary 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.

plc-2%ap image predownload site- wic-2%sh ap mst wic-2%sh ap master li wic-2%sh ap master list AP Name W	iag site_tag st	AP Model	Site Tag			
ap-2-3800 master AP 00	081.c4a0.7550	AIR-AP3802I-B-K9	site_tag			
wlc-2#sh ap im wlc-2#sh ap image Total number of APs: 2						
Number of APs Initiated Predownloading Completed predownloading Not Supported AP Name Failed to Predownload	: 0 : 1 : 0 : 0 : 0 Primary Image	Backup I	mane	Predownload Status	Predownload Version	Next Petry Tim
Ar Name	Frimany image	Dackup	mage	Predownioad Status	Fredownioad version	Next Retry IIII
ap-1-3800 ← slave Ap ap-2-3800	16.10.1.33 16.10.1.33	16:11:1: 16:11:1:	11 11	None Predownloading	0.0.0.0 16.10.1.37	N/A Ø

Step 3. After the image pre-download 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 the reboot.

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 Time
ap-1-3800 ap-2-3800 ap-1-3700	16.10.1.33 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
wlc-2#ap im wlc-2#ap image swap wlc-2#sh ap image vlc-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 Time
ap-1-3800 ap-2-3800 ap-1-3700	16.10.1.37 16.10.1.37 0.0.0.0	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
wlc-2#ap im wlc-2#ap image rese wlc-2#ap image reset wlc-2#					

Limitation

The system decides on the election of a primary AP, and the decision on who the primary 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 primary AP already elected.

FlexConnect pre-auth ACL and URL filtering

The URL filtering is an extension to the ACL deployments currently 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 support 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 app store for downloading the supplicant for which URL filters can be used. The use of 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 before getting authenticated. In the case of LWA/CWA or BYOD, the client might require access to resources before getting full access to the network. The URL filtering for flex is supported only on the Wave 2 platforms. The URL filtering follows a permit list and block 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, the 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 have a permit or deny based on the URL filtering rules, which is either permit listing or block listing. 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 an optional configuration on the LWA and CWA flow.



Figure 9. URL-filtering ACL logic

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 > URL Filters.



Step 2. Create a URL filter.

URL Filters	Add URL Filter				×
+ Add	List Name*	url-pre-auth	Redirect	Servers	
List Nam	Туре	PRE-AUTH 🗸	IPv4	XXX.XXXX.XXXX	
	Action		IPv6	XIXIXIX	
	URLs	Enter a URL every new line dns.cisco.com playstore.google.com	use permit to create Wh	nite list	
	Cancel			📔 Save & Apply 1	to Device

Step 3. Create an ACL on the WLC to link with the URL ACL.

Q. Search Menu Items	Interface		Access Control List
Dashboard	Logical Ethernet Wireless	AireOS Config Transistor Application Visibility Cloud Services	+Ads # Dever Associating interfaces
Monitoring >		Custom Application	AQ, Nune · AQ, Type
Configuration	STP	IOx Multicast	AQREDRECT VV4 Estanded
	VLAN VTP	NetFlow	Add ACL Setup
20 Administration		Python Sandbox OoS	ACL Name* fex-ad_11 ACL Type IPv4 Stendard •
💥 Troubleshooting			
이 전 비가 물을 가 없	High Throughput		Rules
Le sug alma	Network	Air Time Fairness AP, Join	Sequence" Action permit •
(C. 2010)	Parameters opt/		
나무 너희물 물문 양공	Routing Protocols		source ride
이 동물 동물을 가지?	OSPF		
			+ Acc x Delete
회에는 형들			
1명 학원님, 이정	ACL Advanced FAP	Advanced Fabric	Sequence × Source × Source × Destination × Destination × Action × P Wildcard P Wildcard Pott Port DSCP × Log ×
	PKI Management		4 4 0 ≥ P 10 • Items per page No temo to discher
다 없는 것 같아.	Local EAP	Mesh Metallar	
	TrustSec	WLANs	D Cancel

Step 4. Create an authentication list on the WLC to be used on the LWA WLAN. The authentication list can point to a radius server or can do a local lookup.

Authentication A	uthorization and Accounting		
AAA Methad	List Servers / Groups	AAA Advanced	
+ Add	Create AAA Radius Server		×
1	Name*	freerad	
RADIUS	IPv4 / IPv6 Server Address*	9.1.0.21	
	PAC Key		
LUAF	Key*		
	Confirm Key*		
	Auth Port	1812	
	Acct Port	1813	
	Server Timeout (seconds)	1-1000	
	Retry Count	0-100	
	Support for CoA		
	Cancel		Bave & Apply to Devic

Navigate to Configuration > Security > AAA.

Authentication Authorization and	Accounting			
+ AAA Wizard				
AAA Method List	rvers / Groups AAA Adva	anced		
+ Add × Delete				
TACACS+	Servers Server C	Groups		
LDAP	Name	Server 1	Server 2	Server 3
	ise	ise	N/A	N/A
		jitems per page		

Authentication Authorization + AAA Wizard	and Accounting		
AAA Method List	Servers / Groups AAA Adv	vanced	
+ Add × Delete	Create AAA Radius S	erver Group	×
RADIUS	Name*	rad-group	
TACACS+	Group Type	RADIUS	
LDAP	MAC-Delimiter MAC-Filtering Dead-Time (mins)	none	- 1
	Available Servers	Assigned Servers	
	Sancel	Freerad	ply to Device

Authentication Authorization	n and Accounting				
+ AAA Wizard					
AAA Method List	Servers / Groups	AAA Advanced			
General		Quick Setup: AAA Auther	ntication		×
Authentication	+ Add ×	Method List Name*	Iwa		
Authorization	Name	Type*	login 🔹		G
Accounting	dot1x_methoc	Group Type	group 🔹		N
	4 4 1 ⊳	Fallback to local			
		Available Server Groups	Assigned Server Groups		
		radius Idap	* > rad-group	-	
		tacacs+ freerad	<	0	
		radgrp_branch	•	*	
		Cancel		Save & Apply to 🛙	4 ce

Step 5. Create 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	Adv	anced	
h Name	Profile Name*	wic-lwa	Radio Policy	All	
open_wlan	SSID	wic-lwa	Broadcast SSID		
dot1x_wian	WLAN ID*	2			
	Status				
	Cancel			🛙 🗎 Save	e & Apply to Device

dd WLAN			
General	Security	Advanced	
Layer2	Layer3	AAA	
aver 2 Security Mode	None	Fast Transition	Adaptive Enabled 🗸
		Over the DS	
MAC Filtering		Reassociation Timeout	20
D Cancel			Save & Apply to Device

dd WLAN		×
General	Security	Advanced
Layer2	Layer3	AAA
Web Policy		Show Advanced Settings >>>
Webauth Parameter Map	global 🔻	click on Advanced
Authentication List	lwaj 🔹	Gennigs
For Local Login Method List	Select a value	
make sure the configuration network default local' exists	on the device	
Cancel		冒 Save & Apply to Device

2				
'eb Policy		<< Hide On Mac Filter Failure	•	
'ebauth Parameter ap	global 🔻	Conditional Web Redirect	DISABLED	
uthentication List	lwa 🔻	Splash Web Redirect	DISABLED	
or Local Login Method Li ake sure the configuratic atwork default local' exis	st to work, please in 'aaa authorization its on the device	Preauthentication /	ACL	
		IPv4	flex_acl_11	•
		IPv6	none	•

Step 6. Create a policy prof	ile.
------------------------------	------

Policy Profile	Add Policy Profile					×
+ Add * Delete	General Access Po	olicies QC	IS and AVC	Mobility	Advanced	
Policy Profile Name	🛦 Configurir	ng in enabled state will	result in loss of co	nnectivity for clients associ	lated with this profile.	
dot1x_wian	Name*	wic-iwa		WLAN Switching Po	olicy	
	Description	Enter Description	1	Central Switching		
	Status			Central Authentication	n 🔽	
	Passive Client	DISABLED		Central DHCP		
	Encrypted Traffic Analytics	DISABLED		Central Association		
	CTS Policy			Flex NAT/PAT		
	Inline Tagging				25	
	SGACL Enforcement					
	Default SGT	2-65519				
	D Cancel				📋 Save & Apply t	to Device

dd Poli cy Profile			
General Access P	olicies QOS and AVC	Mobility	Advanced
WLAN Local Profiling		WLAN	ACL
HTTP TLV Caching		IPv4 ACI	L Search or Select 🔻
RADIUS Profiling		IPv6 ACI	L Search or Select 🗸
DHCP TLV Caching		URL Filt	ters
Local Subscriber Policy Name	Search or Select	Pre Auth	Search or Select
VLAN		Post Aut	th Search or Select 🔻
VLAN/VLAN Group	10 🔻		
Multicast VLAN	Enter Multicast VLAN		
D Cancel			🛛 🗎 Save & Apply to Device

Step 7. Create a flex profile.

Navigate to Configuration > Tags & Profiles > Flex.

Vame*	branch_flex-profile	Multicast Overridden Interface	Add Elov
Description	Enter Description	Fallback Radio Shut	Add Hex
Native VLAN ID	3	Flex Resilient	Genera
		ARP Caching	T Add
TTP Proxy Port	0	Efficient Image Upgrade	ACL N
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	4 -4
CTS Policy		Join Minimum Latency	
nline Tagging			
SGACL Enforcement			
CTS Profile Name	default-sxp-profilex		

Step 8. Create a site tag mapping the policy tag and flex profile.

Navigate to Configuration > Tags & Profiles > Tags.

Manage Tags				
Policy Site	RF	AP		
+ Add × Belete	Add Policy Tag			×
1	Name*	branch_policy		
Policy Tag Name branch	Description	Enter Description		
default-policy-tag	+ Add × D			
14 4 1 5 5 10 ,	WLAN Profile		V Policy Profile	×
	2 < 0 > >	10 🔹 items per page		No items to display
	Map WLAN and P	olicy		
	WLAN Profile*	wic-iwa 🔻	3 Policy Profile*	wic-iwa 🔻
			× 🖌 🔶 🕘	
	Cancel			Save & Apply to Device 5

anage Tags	Rite RF	AD.	
+Add ×D	Add Site Tag		×
Site Tag Name	Name*	site_tag	
ss	Description	Enter Description	
branch sand-site	AP Join Profile	default-ap-profile	
default-site-tag	Flex Profile	branch_flex_profile v	
	Control Plane Name	•	
	Enable Local Site		
	Cancel		📓 Save & Apply to De 4

Step 9. Map the tags on the AP. Once the APs are tagged with a policy profile, the APs will reboot due to conversion from local mode to FlexConnect mode.

If the APs 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.	
	DESIGN PHASE	
	Tags & Profiles WLAN Policy Site Policy Radio Policy (Mandatory) (Optional) (Optional)	
	WLAN Profile AP Join Profile RF Profile	Advanced Wireless Set
	Policy Profile Flex. Profile RF Tag 🥔	
	Policy Tag 🛷 Site Tag 🛷	
	DEPLOY PHASE	
	Apply to APs (Mandatory) Tag APs Select APs and push configuration to them	
	TERMINOLOGY ACTIONS	
	Tag Image: Constraint of the second	
	click to tag the Start Now	

Advanced Wirele	ess Setup		0							
Start		*	+	Tag APs						
	Tags & Profiles		Select	er of APs: ed Number	of APs: 3					
0	WLAN Profile	=+		AP Name	× AP Model	×.		AP 🛛 😪 Mode	Admin Status	 ✓ Ope Stat
0	Policy Profile	=+		ap1-3800	AIR-AP380 K9	2I-B-	0081.c4a0.6fe0	Flex	Enabled	Reg
0	Policy Tag 🛛 🧳	=+		ap2-3	ag APs					×
				ap1-3	Tags					g
o	AP Join Profile	=+	M	× 1	Policy	bran	ch-policy 🔻			
o	Flex Profile	=+			Site	site_	tag 🗸			1
0	Site Tag 🛛 🧳	=+			RF	defa	ult-rf-tag 🗸			- 1
					Changing AP Ta	ag(s) will	cause associated A	NP(s) to reconn	ect	- 1
0	RF Profile	= +				2	_			_
0	RF Tag 🛛 🛷	=+			Cancel	J		Save & Ap	ply to Dev	ice

CWA flow on flex

This section describes the steps to set up CWA with the 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 the url-redirect and url-redirect-acl Cisco AV pair.

Procedure

Step 1. Create an authentication and authorization list on the WLC.

Navigate to Configuration > Security > AAA.

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

Cisco Catal	yst C9800-CL Wireless Co	ntroller	
Q. Search Menu Items Dashboard Monitoring	Authentication Authorization + AAA Wizard AAA Method List	Servers / Groups AAA Advanced	
Configuration	General Authentication Authorization Accounting	Local Authentication Local Authorization Radius Server Load Balance Show Advanced Settings >>>	Default Default Default Default DiSABLED

Step 2. Define a name for the server and specify the IP address and shared secret.

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

Step 3. Create a server group and map the server in the grou	p.
---	----

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

Step 4. Enable dot1x system control and checkmark the authentication and authorization profile.

Add Wizard		×
		Basic Advanced
0	0	
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 Authenticatio	on Authorization Accounting	
General		
aaa_dot1x_system_auth_control		
Local Authentication	Default	
Local Authorization	Default	
Radius Server Load Balance	DISABLED	
Show Advanced Settings >>>		
← Previous		🗃 Save & Apply to Device

Add Wizard		×
		Basic Advanced Advanced
Ø		•
SERVER	SERVER GROUP ASSOCIATION	MAP AAA
General 🗹 🛛 Authen	tication 🖌 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 v	S ISE	
€ Previous		冒 Save & Apply to Device

Step 5. Define the method type as dot1x and map the server group.

Step 6. Define the method type as "network" and map the server group.

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

Step 7. Create a MAB SSID and map the authorization method list.

Navigate to Configuration > Tags & Profiles > WLAN.

WIRELESS NET	WORKS				
+ Add	Add WLAN				×
Number of MANE E	General	Security	Adva	anced	
Name	Profile Name*	wlc-mab	Radio Policy	All	
wic-lwa	SSID	wlc-mab	Broadcast SSID		
open_wlan	WLAN ID*	3			
dot1x_wlar	Status				
	Cancel			☐ Save & Apply to De	vice

Add WLAN			
General	Security	Advanced	
Layer2	Layer3	ААА	
Laver 2 Security Mode	None	Fast Transition	Adaptive Enabled 🗸
Layer 2 Security Mode		Over the DS	
MAC Filtering	Filtering	Reassociation Timeout	20
Authorization List*	defaultį 🔻		
	Default		
	authz		
Define	the Authorization List		
O Cancel			Save & Apply to Device

Step 8. Enable the following on the policy profile:

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

Navigate to Configuration > Tags & Profiles > Policy.

Policy Profile Gener	ral Access Po	licies QOS	and AVC	Mobility	Advanced
wic-lwa open_wlan	🔺 Configurin	ig in enabled state will r	esult in loss of conne	activity for clients associ	ated with this profile.
dot1x_wlan Nam default~policy	ie*	wic-mab		WLAN Switching Po	blicy
Desc	cription	Enter Description		Central Switching	
State	us 🛛 🔰			Central Authentication	
Pass	sive Client	DISABLED		Central DHCP	
Encr	ypted Traffic Analytics	DISABLED	I	Central Association	
CTS	S Policy			Flex NAT/PAT	
Inline	e Tagging		L		
SGA	CL Enforcement				
Defa	ault SGT	2-65519			

General Access Policie	s QOS and AVC	Mobility	Advanced
WLAN Local Profiling		WLAN	ACL
HTTP TLV Caching		IPv4 A	CL Search or Select 🔻
RADIUS Profiling		IPv6 A	CL Search or Select 🔻
DHCP TLV Caching		URL F	ilters
Local Subscriber Policy Name	Search or Select	Pre Au	th Search or Select 🔍
VLAN		Deat &	
VLAN/VLAN Group	10 🔻	Post A	
Multicast VLAN	Enter Multicast VLAN		

General	Access	Policies	QOS and AVC	Mobility	Advanced
WLAN Timeoi	ıt			Fabric Profile	Search or Select
Session Timeou	it (sec)	1800		Umbrella Parameter Map	Not Configured
dle Timeout (se	ec)	300		WLAN Flex Policy	
idle Threshold (bytes)	0		VLAN Central Switch	ing
Client Exclusion (sec)	Timeout	60		Split MAC ACL	Search or Select
DHCP				Air Time Faimess I	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			<u>6</u>		
Allow AAA Ove	rride				
NAC State					
Policy Name		default-a	aa-policy 🔻		
Accounting List		Search o	r Select		

Step 9. Map 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 × Delet	Add Policy Tag			×
Dellas Tan Nome	Name*	branch_policy]	
branch	Description	Enter Description]	
default-policy-tag	+ Add × D			
	2 WLAN Profile		V Policy Profile	×
		10 🔻 items per pa	ge	No items to display
	Map WLAN and P	olicy		
	WLAN Profile*	wic-mab 🗸	3 olicy Profile*	wic-mati
			× ✓	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:



To create a URL filter, navigate to Configuration > Security > URL Filters.

Q Search Menu Items			Interface	6	Services
			Logical		AireOS Config Translator
📰 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
(2) Monitoring	>	규	Layer2		Custom Application
			STP		lOx
代 Configuration	>		VLAN		Multicast
~			VTP		NetFlow
O Administration	>				Python Sandbox
SCAT II I I			Radio Configurations		QoS
1 roubleshooting			CleanAir		RA Throttle Policy
			High Throughput		Tags & Profiles
			Media Parameters		Air Time Fairness
			Network		AP Join
			Parameters		Flex
		~	KKM		Policy
		(1 , 1)	Routing Protocols		RF
			OSPF		Tags
		\bigoplus	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		

Step 11. Create a URL filter.

Permit action creates a permit list, 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 needs to be configured
- ACL and URL filter needs to be mapped

URL Filters					
+ Add	Add URL Filter				×
4	List Name*	url-pre-auth	Redirect S	ervers	
List Nam	Туре	PRE-AUTH	IPv4	XXX.XXX.XXX	>
	Action		IPv6	XIXIXIX	
	URLs	Enter a URL every new line			
		playstore.google.com			
	Cancel			📔 Save & Apply to	Device

Advanced Wireless Setup			
(Start) *	+ Add at Delete		
Y III	Add Flex Profile		×
Tags & Profiles	General Local Authentication Policy ACL	VLAN	
0 ····· WLAN Profile		Maliana Consideration	
e Policy Profile	Name*	Mulucast Overnoden Intenace	
Policy Tag # = +	Description Enter Description	Fallback Radio Shut	
	Native VLAN ID 0	Flex Resilient	
	HTTP Proce Port	ARP Caching	
		Efficient Image Upgrade	
Bex Profile	Address 0.0.0	Office Extend AP	
0 Site Tag 🧳 🔳 🕇	CTS Policy	Join Minimum Latency	
	Inline Tagging		
e RF Profile 🗮 🕇	SGACL Enforcement		
0 RF Tag 🕜 🔳 🕇	CTS Profile Name default-sxp-profilex		
Apply	Cancel		冒 Save & Apply to Device

General Local	Authentication Policy ACL VLAN		
	 Central ✓ Pre Auth URL ✓ Webauth Filter 10 → items per page. No items to display 	ACL Name* Central Webauth Pre Auth URL Filter	ACL-REDIRECT • • • • • • • • • • • • • • • • • • •
O Cancel	5		Bave & Apply to Device

eneral Local Authentication	Policy ACL VLAN	1			
Add 🗰 Delete					
LANIName 🗹 ID 🤟 .	ACL Name 🗸	•		2	
 4 0 ▶ ▶ 10 ▼ ite 	ems per page	VLAN Name*	10		
	No items to display	VLAN Id*	10	-3	
		ACL Name	Select ACL	•	
		🛩 Save		Cancel	
	0				

Step 13. For assigning the flex profile on the site tag and mapping it on the AP, refer to the steps in the advanced configuration wizard of this document.

Step 14. Create an authorization profile and rule on ISE to return the CWA attributes.

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

Authorization Profiles > sand-cura-auto		
Authorization Profile		
* Name sand-rwa-ewic		
Access Type ACCESS_ACCEPT	<u>*</u>	
Network Device Profile		
Service Template		
Track Movement		
Passive Identity Tracking		
Common Tasks Voice Domain Permission		
Web Redirection (CWA, MDM, NSP, CPP)		
Centralized Web Auth + A	ACL ACL-REDIRECT Value sand-cwa v	
Display Certificates Renewal Message		
	91020	
▼ Advanced Attributes Settings		
Select an item	0 - +	
✓ Attributes Details		
Access Type = ACCESS_ACCEPT		
cisco-av-pair = url-redirect-acl=ACL-REDIRECT cisco-av-pair = url-redirect=https://9.1.0.20:port/portal/g	/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa	
Save		

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

Limitation

- The URL filter is only supported on Wave 2 APs 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 addresses the requirement when an administrator would want to restrict the number of clients accessing the wireless service – for example, limiting total guest clients from branch tunnelling 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 is limited on a per-WLAN basis

Per-AP per-WLAN - here the client association is 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 to the section of setting up the WLAN in the advanced wireless setup wizard of this document.

Procedure

During the WLAN configuration phase, enable the feature.

inced Wireless Setup						
(Start)	+ Add × Deleter					
Tags & Profiles	Add WLAN					
	General	Security	Adva	anced		
dick on ** symbol a add	Coverage Hole Detection		Universal Admin			
Policy Profile	Aironet IE		Load Balance			
OPolicy Tag 🖌 🔳 🕇	Diagnostic Channel		Band Select			
	P2P Blocking Action	Disabled 🔹	IP Source Guard			
AP Join Profile	Multicast Buffer	DISABLED	WMM Policy	Allowe	ed 🔻	drop
G Fiex Profile 🗮 🕈	Media Stream Multicast- direct		Off Channel Sc	anning Defe	ər	down the scroll bar
() Site Tag / 🗮 🕇	Max Client Connections		Defer	0]1 🔲 2	
0 RF Profile 🗮 🕇	Per WLAN 0		Priority	3	4 😿 5	
0 RFTag / 🔳 +	Cancel				📓 Save 8	Apply to Device
Apply						

Multicast Buffer	DISABLED	WMM Policy	Allowed 🔻	
Media Stream Multi direct	cast-	Off Channel	Scanning Defer	
Max Client Conne	actions	Defer Priority	0 1 2	
Per WLAN	50		3 4 🖌 5	
Per AP Per WLAN	100		6 7	
Per AP Radio Per WLAN	150	Scan Deter Time	100	
		Assisted Ro	paming (11k)	

Limitations

This feature does not enforce client limit when the FlexConnect is in the 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 the FlexConnect AP provides 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 works smoothly, both the controllers need to have identical configs such as:

- WLANM 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 Wave 1 and Wave 2 APs.

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 network, multicast and broadcast are sent out over the wireless medium at the lowest data rate with no acknowledgement and the packet delivery for such streams is on a best-effort basis. This makes the usage of multicast unreliable on a WLAN network. The usage of multicast for delivering critical applications 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 APs
- Supported for FlexConnect local switching and central authentication
- With VideoStream in FlexConnect 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 streams from the controller. It is expected that the branch network will be enabled for multicast.

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 other than on the wireless controller.

Procedure for enabling VideoStream

The steps here include only the changes to enable VideoStream.

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

Procedure

Step 1. Enable multicast globally on the controller.

Navigate to Configuration > Services > Multicast.



ilobal Wireless Multicast Mode					MLD Snooping	DISABLED
Vireless mDNS Bridging	DISABLED			1	IGMP Snooping Querier	ENABLED
Vireless Non-IP Multicast	DISABLED				IGMP Snooping	ENABLED
Vireless Broadcast	DISABLED				Last Member Querier Interval (milliseconds)	1000
P Capwap Multicast	Unicast	•				
						-
						Apply to Dev
CMD Speeping						
anne anooping						
ame shooping						
abled		Enabled	Q 800	woh		
abled Status VLAN ID	Name	Enabled	Q. See	areh Name		
abled Status VLAN ID	Name	Enabled Status	VLAN ID 1	Name default	÷	
abled Status VLAN ID	Name	Enabled Status O	VLAN ID 1 4	Name default VLAN0004	*	
abled Status VLAN ID	Name	Enabled Status © ©	Q. See VLAN ID 1 4 15	Name default VLAN0004 VLAN0015	* * *	
abled Status VLAN ID	Name	Enabled Status © ©	VLAN ID 1 4 15	Veh default VLAN0004 VLAN0015	¢ ¢ ¢	
abled Status VLAN ID No Vian a	Name	Enabled Status © ©	VLAN ID 1 4 15	Vame default VLAN0004 VLAN0015	* * * *	
abled Status VLAN ID No Vian a	Name	Enabled Status © ©	VLAN ID 1 4 15	Veb default VLAN0004 VLAN0015	*	
sabled Status VLAN ID No Vian a	Name	Enabled Status © ©	VLAN ID 1 4 15	Veh default VLAN0004 VLAN0015	*	

Step 2. Enable media stream on the dot11 interface.

Disable the appropriate radio interface before enabling the media stream.

Navigate to Configuration > Radio Configurations > Network.

Disable 5 or 2.4 GHz radio. In this example, we are enabling media streaming on 5 GHz radio.



5 GHz Band	2.4 GHz Band	1			
General	(disable 5ghz radio)				
5 GHz Network S	tatus		-		
Beacon Interval*		10	00		
Fragmentation Th	reshold(bytes)*	23	346		
DTPC Support					
CCX Location M	leasurement				
Mode					
Data Rates					
6 Mbps	Mandatory 🔻	9 Mbps	Supported v	12 Mbps	Mandatory
18 Mbps	Supported 🗸	24 Mbps	Mandatory 🔻	36 Mbps	Supported
48 Mbps	Supported 🔻	54 Mbps	Supported 🔻		

Step 3. Navigate to Configuration > Radio Configurations > Media Parameters.



/ledia		Voice	
General		Call Admission Control (CAC)	
Unicast 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
Maximum Media Bandwidth (%)*	85	Max Streams*	2
Client Minimum Phy Rate (kbps)	6000 🗸	Inactivity Timeout	
Maximum Retry Percent (%)*	80		
Media Stream - Multicast Direct Parameter	3		
Multicast Direct Enable			
Max streams per Radio	3		
Max streams per Client	3 🔹		
Inactivity Timeout			

Step 4. Enable the media stream on the WLAN creation page on the advanced tab. Refer to the advanced configuration wizard section for WLAN creation.

dd WLAN			
General	Security	Advanced	
Coverage Hole Detection		Universal Admin	
Aironet IE		Load Balance	
Diagnostic Channel		Band Select 🛛	
P2P Blocking Action	Disabled 🗸	IP Source Guard	
Multicast Buffer	DISABLED	WMM Policy Allowed	
Media Stream Multicast- direct		Off Channel Scanning Defer	
Max Client Connections		Defer Priority 0 1 2	
Per WLAN 0		3 4 🖌 5	
D Cancel		🛛 🗃 Save & Apply to De	evice

Step 5. Define the media stream multicast address configuration.

Navigate to Wireless > Media Stream.

Q Search Menu items			Interface	6	Services
			Logical		AireOS Config Translator
🔜 Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
Monitoring	>	.	Layer2		Custom Application
2			VLAN		IOx
Configuration	>		VTP		Multicast
			Padia Configurationa		NetFlow
203 Administration	>		Radio Configurations		Python Sandbox
SG T- HI-L-H			CleanAir		QoS
* I roubleshooting			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
			Network		AP Join
			Parameters		Flex
		_	RRM		Policy
		(t)	Routing Protocols		RF
			OSPF		Tags
		Ĥ	Security		WLANs
		S	ААА		Wireless
			ACL		Access Points
			Advanced EAP		Advanced
			PKI Management		Air Time Fairness
			Local EAP		Fabric
			Local Policy		Media Stream
	San		Terretoria		Mash
a Stream					
----------------------------	-----------				
General Streams					
Multicast Direct Enable					
Session Message Config					
Session Announcement State					
Session Announcement URL					
Session Announcement Email					
Session Announcement Phone					
Session Announcement Note					
	🖌 🖌 Apply				

Media Stream			
General Streams			
	Add Media Stream		×
+ Add × Dislate	General		
ierns per pag	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) Para	imeters	
	Average Packet Size*	1200	
	Policy	admit v	
	Priority	4	
	QOS	Video	
	Violation	Drop	
	Cancel	📓 Save & Apply to Device	

General							
5 GHz Network Status	3						
🛦 Please disat	ole 5 GHz Network	Status to configure Be	eacon Interva	al, Fragmentation Thresho	ld, DTPC Support.		
Beacon Interval*			100				
Fragmentation Thresh	nold(bytes)*		2346				
DTPC Support							
CCX Location Measurement	surement						
Mode							
Data Rates							
	🛦 Please	disable 5 GHz Networ	k Status to o	configure Data Rates			
6 Mbps	Mandatory	• 9 Mbps		Supported 🔻	12 Mbps	Mandatory	¥
18 Mbps	Supported	• 24 Mbp	S	Mandatory 🔻	36 Mbps	Supported	•
10.1.1	Supported	- 54 Mbr		Supported -			

Step 6. Enable the dot11 interface on which the media stream was enabled.

Connect the 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.

wlc-2#sh flexconne 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 1c36.bbef.6492	check1	224.0.0.251 224.0.0.252 239.1.1.1 239.255.255.250	ap-1-3800 ap-1-3800 ap-1-3800 ap-1-3800 ap-1-3800	10 10 10 10	Multicast-Only Multicast-Only Multicast-Direct Multicast-Only

Flex IP Overlap Support

Introduction

Multiple customers tend to use cookie-cutter configurations across the sites and branches. This includes local or DHCP servers configured with the same subnet. Before 17.4, the controller detected this is IP THEFT and clients would be blacklisted.



Figure 10.

Behavior of overlapping IPs across sites before Release 17.4

Release 17.4 adds support for overlapping IP addresses across different flex sites.

For this to work, every site needs to be assigned to a unique site-tag > C9800 uses the combination of site-tag + IP address as a unique ID for the client (called zone-id).

It is important to note that this is only available for Flex local DHCP/ local switching; for all other deployments (local mode, central switching, central DHCP, etc.), overlapping IPs are still not supported.



Figure 11.

Behavior of overlapping IPs across sites starting Release 17.4

This feature is supported on all C9800 appliances (physical and virtual). It is not supported on EWC on Catalyst AP and Catalyst 9k switch because these are meant for single site deployments.

Procedure for enabling Flex IP Overlap

Enable and disabling the feature is controlled via the config knob under the Flex Profile.

Configuration • >	Edit Flex Profile	
+ Add >	General Local Authentication	Policy ACL VLAN
	Umbrella	
Flex Profile		Shut
🗌 р	Description Enter Description	
test-profile	Nativa	Flex 🗖 Resilient
flex-overlap	VLAN ID	
test-flex-profi	HTTP	ARP 🔽 Caching
default-flex-pi	Proxy Port	Efficient
flex-profile-no	HTTP-	
flex ip overla	Proxy IP 0.0.0.0 Address	opgrade
	CTS Policy	
	Inline 🗖 Tagging	Join Minimum 🗖 Latency
	SGACL Enforcement	IP Overlap

```
The equivalent CLI command is:
(config) #wireless profile flex flex1
(config-wireless-flex-profile) #ip overlap
To verify execute the following command:
9800-wlc#show wireless profile flex detailed flex1
Fallback Radio shut
                               : DISABLED
ARP caching
                               : ENABLED
Efficient Image Upgrade
                               : ENABLED
OfficeExtend AP
                               : DISABLED
Join min latency
                               : DISABLED
IP overlap status
                               : ENABLED
```

"Show wireless device-tracking database ip <ip>" CLI will not be supported when IP overlap feature is enabled. Any filtering based on IP or Zone should be performed only on "Show wireless device-tracking database ip".

9800-wlc#show wireless device-tracking database ip

ZONE-ID I	P	STATE	DISCOVERY	MAC
0x0000004	21.21.0.1	Reachable	IPv4 Packet	74da.3864.2a83
0x000000c	21.21.0.1	Reachable	IPv4 DHCP	74da.3873.2a8b
0x8000400a	fe80::76da:38ff:fe64:2a83	Reachable	IPv6 Packet	74da.3864.2a83
0x8000c00a	fe80::76da:38ff:fe73:2a8b	Reachable	IPv6 Packet	74da.3873.2a8b

In order to enable or disable the Overlap IP Support which are part of the flex profile, 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>

Glossary

- VLAN: virtual LAN
- RF: radio frequency
- FT: fault tolerance
- WAVE 1 AP: AP which supports WAVE 1 802.11ac (Cisco 3700)
- WAVE 2 AP: AP which supports WAVE f2 802.11ac (Cisco 1800/2800/3800/4800)
- WLC: wireless LAN controller

Americas Headquarters Cisco Systems, Inc.

San Jose, CA

Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA