# Secure a Flexconnect AP Switchport with Dot1x

### Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Configure
Network Diagram
AP configuration:
Switch Configuration
ISE configuration:
Verify
Troubleshoot
References

# Introduction

This document describes the configuration to secure Switchports where FlexConnect Access Points (AP) authenticate with Dot1x.

# Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- FlexConnect on Wireless Lan Controller (WLC)
- 802.1x on Cisco Switches
- Network Edge Authentication Topology (NEAT)

#### **Components Used**

The information in this document is based on these software and hardware versions:

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Identity Service Engine (ISE) 2.0
- IOS-based Access Points (x500,x600,x700 series).

Wave 2 APs based on AP OS do not support flexconnect trunk dot1x as of time of this writing.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure

#### **Network Diagram**



In this setup the access point acts as the 802.1x supplicant and is authenticated by the switch against ISE using EAP-FAST. Once the port is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully.

Once the access point authenticates successfully against ISE, the switch receives Cisco VSA Attribute "device-traffic-class=switch and it automatically moves the port to trunk.

This means, if the AP supports FlexConnect mode and has locally switched SSIDs configured, it is able to send tagged traffic. Ensure that vlan support is enabled on the AP and the correct native vlan is configured.

#### **AP configuration:**

1. If the AP is already joined to the WLC, go the Wireless tab and click on the access point. Go the Credetials field and nder the 802.1x Supplicant Credentials heading, check the **Over-ride Global credentials** box to set the 802.1x username and password for this access point.

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ontroller	WIRELES	s <u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MM/
Wireless	All APs > [	Details fo	or Aks_des	k_3502			
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> </ul>	General	Creden	tials Int	erfaces	High Availabil	ity Inventory	/ Fle
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Crede	e <b>ntials</b> e Global cre	dentials				
Advanced Mesh	802.1x Sup	oplicant Cro	edentials				
> ATF	Over-ride	e Glo <mark>b</mark> al cre	dentials				
RF Profiles	Username ritmahaj						
FlexConnect Groups	Passwo	ord	•••••				
FlexConnect ACLs FlexConnect VLAN Templates	Confirr	n Password	•••••				

You can also set a comman username and password for all the access points that are joined to the WLC with the Global Configuration menu.

	CISCO	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
10	lisalaaa	CDP Stat	le			۲		to	3600)	/	120
VV	lieless	Etherne	et Interfac	e# CD	P State			AF	Primed	Join Timeout(120 -	0
	Access Points	0		×.				43	200 sec	onds)	0
	All APs	1		×.				Ba	ick-up Pr	imary Controller IP	
	<ul> <li>Radios</li> </ul>	2		×.				Ad	ldress(Ip	v4/Ipv6)	
	802.11a/n/ac	3		2				Ba	ick-up Pr	imary Controller name	
	Dual-Band Radios	4		8				Ba	ick-up Se	econdary Controller IP	-
	Global Configuration	Radio S	Slot#	CD	P State			Ad	ldress(Ip	ov4/Ipv6)	
	Advanced	0		<ul> <li>Image: A start of the start of</li></ul>				Ba	ck-up Se	econdary Controller	<b>—</b>
		1						na	me		<u> </u>
	Mesh	2		2				TCD	MEG		
•	ATF	1		-				TCP	M55		
	RF Profiles	Login C	redential	5				Glo 13	bal TCP	Adjust MSS (IPv4: 536 : 1220 - 1331)	. 🛛
	FlexConnect Groups	Usern	ame						otrono	mit Config	
	FlexConnect ACLs	Passw	ord					Para	meter	s	
	Templates	Enable	e Password					AF	Retrans	mit Count	5
	OEAP ACLS							AF	Retrans	mit Interval	3
	Network Lists	802.1x	Supplica	nt Credential	5			0	Retrains	and Interver	2
Þ	802.11a/n/ac	802.1x	Authentica	tion				OEA	P Conf	ig Parameters	
•	802.11b/g/n	Usern	ame					Di	sable Lo	cal Access	
Þ	Media Stream	Passw	ord					NO ED	TE: abling t	his feature could viol	ate se
Þ	Application Visibility And Control	Confir	m Password					wi	thin you mpliance	ir organization. Pleas e with all regulations	e mai s befo.

2. If the access point has not joined a WLC yet, you must console into the LAP to set the credentials and use this CLI command:

#### LAP#debug capwap console cli

LAP#capwap ap dot1x username <username> password <password>

#### **Switch Configuration**

1. Enable dot1x on the switch globally and add ISE server to switch

aaa new-model

!

aaa authentication dot1x default group radius

!

aaa authorization network default group radius

!

dot1x system-auth-control

!

radius server ISE address ipv4 10.48.39.161 auth-port 1645 acct-port 1646 key 7 123A0C0411045D5679

2. Now configure the AP switch port

interface GigabitEthernet0/4 switchport access vlan 231 switchport trunk allowed vlan 231,232 switchport mode access authentication host-mode multi-host authentication order dot1x authentication port-control auto dot1x pae authenticator spanning-tree portfast edge

#### **ISE configuration:**

1. On ISE, one can simply enable NEAT for the AP Authorization profile in order to set the correct attribute, however, on other RADIUS servers, you can configure manually.

Authorization	Profiles	> AP	_Flex	Trunk
---------------	----------	------	-------	-------

Authorization Profil	e	
* Name	AP_Flex_Trunk	]
Description		1
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	disco Cisco 💌 🕀	
Service Template		
Track Movement	i)	
▼ Common Tasks		
NEAT		
<ul> <li>Attributes Details</li> </ul>		
Access Type = ACCESS_ACCEP cisco-av-pair = device-traffic-cla	r ass=switch	

2. On ISE, one also needs to configure Authentication policy and Authorization policy. In this case we hit the default authentication rule which is wired dot1x but one can customize it as per the requirement.

As for Authorization policy (Port\_AuthZ), in this case we added the AP credentials to a user group (APs) and pushed the Authorization Profile (AP\_Flex\_Trunk) based on this.

orizatio	n Policy				
e the Autho olicy Export	rization Policy by con t go to Administration	figuring rules based on iden > System > Backup & Rest	tity groups and/or other conditions. Drag and drop rules to change ore > Policy Export Page	e the order.	
Matched R	ule Applies	-			
xception	s (0)				
tandard					
Status	Rule Name		Conditions (identity groups and other conditions)	Permissions	
	Port_AuthZ	if	APs AND Wired_802.1X	then AP_Flex_Trunk	
	Antipaction a the Author tolicy Export Matched R Exception tandard Status	Status     Rule Name       Status     Rule Name       Image: Status     Port_AuthZ	Authorization Policy         e the Authorization Policy by configuring rules based on identification > System > Backup & Rest         Matched Rule Applies         Exceptions (0)         tandard         Status       Rule Name         Image: Port_AuthZ       if	Norization Policy         e the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change olicy Export go to Administration > System > Backup & Restore > Policy Export Page         Matched Rule Applies         Exceptions (0)         tandard         Status       Rule Name       Conditions (identity groups and other conditions)         Image: Policy Export Page         Image: Policy Export Page	Norization Policy         e the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.         Natched Rule Applies         Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.         Matched Rule Applies         Conditions (identity groups and other conditions)         Permissions         Status         Rule Name       Conditions (identity groups and other conditions)       Permissions         Image: Status       Rule Name       Conditions (identity groups and other conditions)       Permissions         Image: Status       Rule Name       Conditions (identity groups and other conditions)       Permissions         Image: Status       Rule Name       Conditions (identity groups and other conditions)       Permissions         Image: Status       Rule Name       Conditions (identity groups and other conditions)       Permissions         Image: Status       Rule Name       Conditions (identity groups and other conditions)       Permissions

# Verify

Use this section to confirm that your configuration works properly.

1. On the switch, once can use the command "debug authentication feature autocfg all" to check if the port is being moved to trunk port or not.

```
Feb 20 12:34:18.119: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to up
Feb 20 12:34:19.122: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed
state to up
akshat_sw#
akshat_sw#
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle:
3372220456
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Device Type = Switch
```

Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] new client Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Internal Autocfg Macro Application Status: 1 Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Device type : 2 Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp has port\_config 0x85777D8 Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp port config has bpdu guard config 2 Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applying auto-cfg on the port. Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231 Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applying dot1x autocfg supp macro Feb 20 12:38:11.116: Applying command... 'no switchport access vlan 231' at Gi0/4 Feb 20 12:38:11.127: Applying command... 'no switchport nonegotiate' at Gi0/4 Feb 20 12:38:11.127: Applying command... 'switchport mode trunk' at Gi0/4 Feb 20 12:38:11.134: Applying command... 'switchport trunk native vlan 231' at Gi0/4 Feb 20 12:38:11.134: Applying command... 'spanning-tree portfast trunk' at Gi0/4 Feb 20 12:38:12.120: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed state to down Feb 20 12:38:15.139: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed state to up

2. The output of "show run int g0/4" shows that the port has changed to a trunk port.

Current configuration : 295 bytes ! interface GigabitEthernet0/4 switchport trunk allowed vlan 231,232,239 switchport trunk native vlan 231 switchport mode trunk authentication host-mode multi-host authentication order dot1x authentication port-control auto dot1x pae authenticator spanning-tree portfast edge trunk end

3. On ISE, under Operations>>Radius Livelogs one can we the authentication being successful and the correct Authorization profile being pushed.

Time	Status	Details	Repeat Count	Identity ()	Endpoint ID	Endpoint Profile	Authentication Policy (i)	Authorization Policy	Authorization Profiles	
2017-02-20 15:05:48.991	0	ò	0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk	
2017-02-20 15:05:48.991		ò.		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk	a
2017-02-20 15:04:49.272	×	ò.		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ		a

4. If we connect a client after this then its mac address is learnt on the AP switch port in the client vlan 232.

akshat\_sw#sh mac address-table int g0/4 Mac Address Table

Vlan Mac Address Type Ports

---- -----

231 588d.0997.061d STATIC Gi0/4 - AP 232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Client On the WLC, in the client detail it can be seen that this client belongs vlan 232 and the SSID is locally switched. Here is a snippet.

(Cisco Controller) >show clien	t detail c0:ee:fb:d7:88:24
Client MAC Address	c0:ee:fb:d7:88:24
Client Username	N/A
AP MAC Address	
AP Name	Aks_desk_3502
AP radio slot Id	
Client State	Associated
Client User Group	
Client NAC OOB State	Access
Wireless LAN Id	
Wireless LAN Network Name	(SSID) Port-Auth
Wireless LAN Profile Name	Port-auth
Hotspot (802.11u)	Not Supported
BSSID	b4:14:89:82:cb:9f
Connected For	
Channel	44
IP Address	192.168.232.90
Gateway Address	
Netmask	255.255.255.0
Association Id	1
Authentication Algorithm	Open System
Reason Code	
Status Code	0

FlexConnect Data Switching	Local
FlexConnect Dhcp Status	Local
FlexConnect Vlan Based Central Swit	ching No
FlexConnect Authentication	Central
FlexConnect Central Association	No
FlexConnect VLAN NAME	vlan 232
Quarantine VLAN	0
Access VLAN	. 232
Local Bridging VLAN	232

# Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- If authentication fails, use **debug dot1x**, **debug authentication** commands.
- If the port is not moved to trunk, enter the **debug authentication feature autocfg all** command.
- Ensure you have multi-host mode (authentication host-mode multi-host) configured. Multi-Host has to be enabled in order to allow client wireless MAC addresses.
- "aaa authorization network" command must be configured in order for the switch to accept and apply the attributes sent by ISE.

Cisco IOS based access points only support TLS 1.0. This can cause a problem if your RADIUS server is configured to only allow TLS 1.2 802.1X authentications

# References

Configure dot1x supplicant with AP and a 9800 WLC