

Cloudpath as RADIUS server and as a Hotspot (WISPr) Portal

Best Practices and Deployment Guide



November 2017

Table of Contents

Intent of this Document	3
Cloudpath Workflow Overview	4
Onboarding and Secure WLANs on a Cisco WLAN Controller	5
1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES	5
2) Login to the WLC and add dynamic user interfaces (VLANs)	7
3) Create a preauthentication Access Control List (ACL) for the onboarding WLAN	9
4) Define a RADIUS Authentication Server as the Cloudpath RADIUS server	13
5) Define the RADIUS Accounting Server as the Cloudpath RADIUS server	15
6) Create Two WLAN profiles	17
7) Edit the Secure (802.1X) WLAN profile	18
8) Edit the onboarding WLAN profile	21
9) Create or Edit an AP group to deploy WLANs	24
10) Don't do this: Configuring Web Auth default policy option	28
About Ruckus	29

This table of contents can be used as a checklist in the future.



November 2017

Intent of this Document

Cloudpath Best Practices and Deloyment Guides are meant to address specific subjects in Ruckus Cloudpath deployments and to tackle those subjects in bite sized chunks. Although Cloudpath is simpler and more user-friendly than competitors, there are many options within Cloudpath and network administrators will benefit from a series of targeted Best Practices and Deployment Guides.

What is Ruckus Cloudpath? Cloudpath is a self-service onboarding portal for secure networks. We are all familiar with captive portals for public access/hotspot networks. Unlike those systems, Cloudpath can support self-service secure registration for networks, combining everything necessary for:

- Policy Management Is the user a student or a teacher? Is the device a phone or a laptop?
- Device Enablement Is the anti-virus up-to-date? Is the firewall running and the OS patched?
- Certificate Deployment and Management Certificates are deployed automatically, uniquely identifying all devices

IT gets more control and more information, while spending less time on password problems and basic access issues.

This document walks through the deployment of a Cloudpath workflow (or registration portal), on a Cisco WLAN Conroller (WLC) It supports the typical case of two WLANs (SSIDs) – one for the onboarding portal, one for secure users. The secure SSID is 802.1X certificate secured for users and is accessible only after they have registered their devices at the onboarding portal. The open SSID can serve double duty as both the secure user onboarding portal, and also as the guest WLAN with automatic MAC registration of guest devices. Configuration of both options is described below.

This document is not a Cloudpath installation guide or a complete Cisco WLC configuration guide

Cloudpath ES server should already be fully deployed and accessible, locally or as a cloud system. An external database of users should be available.* A workflow should already be configured on Cloudpath ES. If necessary, consult the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - secure users and MAC auth guests".

Similarly, a Cisco WLC should already be deployed, with at least one AP connected to it. To test, Wi-Fi client devices such as tablets, smart phones, or laptops will be needed.

*There is a limited onboard database in Cloudpath that can be used in a lab environment, but it is not recommended for a production environment



November 2017

Cloudpath Workflow Overview

A workflow is a tree of network access policy/classification steps contained in a series of web pages. A policy is built in a series of steps, and then published as an Onboarding Portal (web pages) on the Cloudpath web server. Adding a step usually involves adding a web page, but it could be a filter or other classification step that automatically flows through to the next step/page. A workflow generally ends in downloading a *Device Configuration* onto a secure client. A Cloudpath *Device Configuration* is typically a WLAN/SSID profile, including security settings and an 802.1X certificate. However, it may end in some alternative grant of network access, such as a PSK, a Ruckus Dynamic PSK, or display of a voucher code for a guest user.

Hotspot Portal SSID and RADIUS Secured SSID

This document describes deployment of a Cloudpath workflow for an environment with two WLANs/SSIDs. The first WLAN is a secure/employee SSID that uses 802.1X certificate authentication (supported by the Cloudpath RADIUS server). Take special note – the Cloudpath ES RADIUS server authenticates the certificates for access to the secure network. At registration, there will need to be an authentication server (database) of employees (secure users) that Cloudpath can check before distributing profiles and certificates.

The second SSID is an open WLAN redirected as a Hotspot/WISPr portal. It serves both as employee registration and as a Guest Access portal. Secure users (employees) initially register their devices and download a certificate on the open SSID. It is a one-time process for each employee device, and once a device is registered and has a unique certificate, it immediately, and always thereafter, connects to the secure network.

Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal will open up (the walled garden will open) and they will be granted Internet access.

This is designed to be a simple but effective workflow that can be built on, and necessary configuration of Cloudpath is described in the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - Secure Users and MAC-auth Guests".

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

Onboarding and Secure WLANs on a Cisco WLAN Controller

1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES

Configuration of a basic workflow in Cloudpath ES should have already been completed. However, before moving on to a WLAN controller, there are two pieces of information that will be needed:

- o The Enrollment Portal URL
- The Cloudpath ES RADIUS settings

Cloudpath A Ruckus Brand				0 :						
Dashboard	Configuration > Workflows			Add Workflow						
Mortflour	Workflows	Status	Enrollment Portal URL	Last Publish Time						
TOTALIONS	BasicWorkflow	Published	/enroll/Brocade2/BasicWorkflow/	20170612 2152 GMT						
Device Configurations	aerohive	Published	/enroll/Brocade2/aerohive/	20170612 2152 GMT						
RADIUS Server	dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170612 2152 GMT						
Authentication Servers	Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170612 2152 GMT						
Firewalls & Web Filters	Corporate	Published	/enroll/Brocade2/Production/	20170612 2152 GMT						
MAC Registrations	Properties Enrollment Process	Look & Feel Snapshot(s)	Advanced							
API Keys										
Sponsorship	Portal URLs									
Certificate Authority	Enrollment Portal URL:	https://demo.cloudpath.net/enro	oll/Brocade2/BasicWorkflow/							
Administration	Passpoint OSU URL:	Passpoint OSU URL: https://demo.cloudpath.net/passpoint/Brocade2/BasicWorkflow/entry								
Support	QR Code:									
	> Managed Chromebook	Setup								

- Login to Cloudpath ES and navigate to:
- o Configuration
- Workflow
- o Click on the workflow to be deployed
- o Click on the workflow's Advanced tab
- Go to the Enrollment Portal URL.
- Copy this URL to a text editor for later (or be prepare to return to this window).
- o This URL will be added to the WLAN in the Cisco WLC as an external portal

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

Dashboard 🕨	Configuration > RADIUS Server										
Configuration 🔫											
Workflows	Status Policies Clients eduroam Attributes External Open Access Accounting										
Device Configurations											
RADIUS Server	RADIUS Server Status										
Authentication Servers	The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).										
Firewalls & Web Filters	Status: 🔴 Activated										
MAC Registrations	Connection Tracking: Active Disable										
API Keys	COA: Active Disable										
Sponsorship 🕨	RADIUS Server Settings										
Certificate Authority	This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.										
ådministration k	IP Address: demo.cloudpath.net										
	Authentication Port: 12975										
Support 🕨	Shared Secret: ***** Q New Random Set										
	RADIUS Server Certificate										
	The RADIUS server certificate is used to authenticate the network to the client, allowing the client to verify that it is connecting to the real network and not an evil										

- WLC will need the RADIUS server settings. On the main menu bar, navigate to Configuration -> RADIUS Server. Copy the following information for later
- The IP address
- NB must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN
- o Authentication port
- The Accounting port (optional)
- The Shared Secret which can be revealed by clicking on the magnifying glass

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

2) Login to the WLC and add dynamic user interfaces (VLANs)

 Monitoring Network Summary 			Q, A	P or Client Search	Advanced 🖂 🌣
Access Points Clients	NETWORK SUMM	ARY			0
€ Rogues Access Points Clients	Wireless Networks 7 9	Access Points	Active Clients 2.4GHz () 5GHz ()	Rogues APs 11 Clients 1	Interferers 2.4GHz 0 5GHz 0
Dinterferers Client Performance	ACCESS POINTS BY USAGE				⊞ ×
♥ Best Practices					

- \circ $\,$ Login to the Cisco WLC $\,$
- Navigate to **Advanced**
- o Click on **Controller** to access the Controller menu

				7						
cisco	MONITOR	<u>W</u> LANs <u>C</u>	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	Save Configuration
Monitor	Summary									
Summary Access Points Cisco CleanAir Statistics	cisco			2 Access Point	s Supported	Cisco 5500 Serie	s Wireless Contr Hode	oller 1 5508		
CDP	Controller	Summary				R	ogue Summa	ry		
Rogues	Management IP Address	10.3.7.210	, ::/128				Active Rogue APs			1
Clients	Service Port IP Address	0.0.0.0 , ::;	/128			4	Active Rogue Clie	nts		1
Sleeping Clients	Software	8.5.103.0				1	Adhoc Rogues			(
Multicast Applications Lync	Field Recovery Image Version	6.0.182.0				s	Rogues on Wired	Network		
Local Profiling	System Name	Cisco_bf:83	3:a4							
	Up Time	77 days, 8	hours, 32 min	utes		т				
	System	Thu Oct 26	22:01:08 201	7			op WLANS			

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

Best practices would suggest that authenticated user and guest traffic should be isolated from each other by VLAN. Create VLANS as **Dynamic Interfaces** as appropriate for the network under configuration.

ı. cısco	MONITOR WLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	Save Configuration Ping Logout R
Controller	Interfaces							Entries 1 - 6 of 6 New
General Icons	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management		IPv6 Address	
Inventory	management	untagged	10.3.7.210	Static	Enabled		::/128	
Interfaces	redundancy-management	untagged	0.0.00	Static	Not Supported			
Interface Groups	redundancy-port	untagged	0.0.0.0	Static	Not Supported			
Multicast	service-port	N/A	0.0.00	DHCP	Disabled		::/128	
Network Routes	virtual	N/A	1.1.1.1	Static	Not Supported			

- On the Controller Menu, click on Interfaces and then on New
- o Define the interface/VLAN as appropriate for the network
- o Repeat, if necessary, for the authenticated users WLAN

ontroller		
General	General Information	
Icons		
Inventory	Interface Name	GuestWLAN
Interfaces	MAC Address	00:07:7d:bf:83:af
Interface Groups	Configuration	
Multicast	comgutation	
Network Routes	Guest Lan	
Redundancy	Quarantine	
Internal DHCP Server	Quarantine Vlan Id	0
Mobility Management	NAS-ID	none
Ports	Physical Information	
NTP	The interface is attached	to a LAG.
CDP	Enable Dynamic AP Mana	agement
PMIPv6		
Tunneling	Interface Address	
IPv6	VLAN Identifier	101
mDNS	IP Address	192.168.149.10
Advanced	Netmask	255.255.255.0
	Gateway	192.168.149.1
	IPv6 Address	::
	Prefix Length	128
	IPv6 Gateway	::
	Link Local IPv6 Address	fe80::207:7dff:febf:83af/64
	DHCP Information	
	Primary DHCP Server	102 168 140 1



3) Create a preauthentication Access Control List (ACL) for the onboarding WLAN



- Click on **Security** to access the Security menu
 - Expand Access Control Lists and then click on Access Control Lists (yes, it appears twice)
 - Click New (alternatively, click on an existing ACL that you will modify)





Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

Name the ACL and click Apply



o Now click on the ACL name to edit it

Walled Garden In order for the Onboarding Portal to function, specific network traffic must be allowed before the user is authenticated in order to support the authentication process. The exact entries depend on the local network. The following are generally required

- o DHCP server the client generally needs an IP address
- DNS server
- o Gateway (in many case, all three are the same)
- o Cloudpath server, including subdomains of the enrollment URL





November 2017

I I I I I I I I I I I I I I I I I I I		ER WIREL	ess <u>s</u> ecuri	ty m <u>a</u> n,	AGEMENT	Sa <u>v</u> e Confi C <u>O</u> MM	guration	n <u>P</u> ing HELP	EEEDBA
Security AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Password Policies	Counters	e Clo 0 Source IP/Mask	Edit Undpath-Portal Destination IP/Mask	Protocol	Source Port	Dest Port	< Back	Direction	Number of Hits

o Use the Add New Rule button to add the first rule

IIIIII CISCO <u>M</u> ONITOR <u>W</u>	LANs <u>C</u> ONTROLLER	WIRELESS SECURITY	Save Con MANAGEMENT COMMANDS	iguration Ping Logout Refresh HELP FEEDBACK
Security AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP	Access Control Sequence Source Destination Protocol DSCP Direction Action	Lists > Rule > New 1 Any Permit Permit	IP Address 12.18.39.43	< Back Apply Netmask 255.255.255

- Create a rule that allows traffic to the Cloudpath server and click Apply
- Similarly, create another rule that allows inbound traffic from the Cloudpath server.
- Continue as necessary to allow access to the gateway, DHCP and DNS server(s)



November 2017

- Details of the ACL rules depend on the network in questions and its security standards
- For more detailed discussion, see the Cisco documentation

CISCO	MONI	TOR V	LANs		WIRELESS	SEC	URITY	MANAGEMENT	COM	MANDS	HELP	FEED	BACK			n Hon
Security	Acce	ess Cor	ntrol Li	ists > Edit										< Back	Add	New Rule
 ▼ AAA General ▼ RADIUS Authentication Accounting Fallback DNS Downloaded AVP 	Gene Access Deny	e ral s List Nam Counters	ne	Cloudpath-F	Portal											
Downloaded AVP TACACS+	Seq	Action	Sourc	e IP/Mask	Destination IP/Mask		Protoc	ol Source	Port	Dest Por	t	DSCP	Direction	Number o	of Hits	
LDAP Local Net Users MAC Filtering	1	Permit	0.0.0.	0 /	12.18.39.43 255.255.255.255	. '	Any	Any		Any		Any	Outbound	0		
 Disabled Clients User Login Policies AP Policies 	2	Permit	12.18 255.2	.39.43 / 55.255.255	0.0.0.0 0.0.0.0	/	Any	Any		Any		Any	Inbound	0		
Decouverd Policies	_															



November 2017

4) Define a RADIUS Authentication Server as the Cloudpath RADIUS server

uluulu cisco	MONITOR	<u>W</u> LANs <u>C</u>	ONTROLLER	WIRELE		MANAGEMENT	COMMANDS	HELP	FEEDBACK	Sa <u>v</u> e Configura	tion Ping Logout P
Security	RADIUS	Authentica	tion Serve	rs							Apply New
AAAA General Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP	Auth Cal Use AES MAC Del Framed	led Station ID 1 Key Wrap imiter MTU	Type AP	MAC Address signed for FI	e) PS customers and	requires a key wrag	o compliant RADII	US server)			
LDAP Local Net Users	Network User	Management	Tunnel S t Proxy I	erver ndex S	erver Address(I;	pv4/Ipv6)		P	ort	IPSec	Admin Status
Disabled Clients		2	0 1	* 7	2.18.151.72			-		Disabled	Enabled
User Login Policies AP Policies Password Policies											
Local FAP											

- o Click on Security to access the Security menu
 - Expand AAA, expand RADIUS and then click on Authentication
 - Accept Auth Called Station ID Type as AP MAC Address the default)
 - Accept MAC Delimiter as Colon (the default)
 - Click New

MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	ne
RADIUS Authentication Serve	ers > New <back ap<="" td=""><td>ply</td></back>	ply
Server Index (Priority)	2 🛊 📜	
Server IP Address(Ipv4/Ipv6)		
Shared Secret Format	ASCII \$	
Shared Secret		
Confirm Shared Secret		
Apply Cisco ISE Default settings		
Key Wrap	(Des ed for FIPS customers and requires a key wrap compliant RADIUS server)	
Port Number	1812	
Server Status	Enabled \$	
Support for CoA	Disabled \$	
Server Timeout	5 seconds	
Network User	C Enable	
Management	C Enable	
Management Retransmit Timeout	5 seconds	
Tunnel Proxy	Enable	
IPSec	Enable	

• The RADIUS Authentication Server is the Cloudpath RADIUS server from section 1



November 2017

- Fill in the Server IP Address of the Cloudpath Server
- Fill in the Shared Secret and the Confrim Shared Secret with the Shared Secret from the Cloudpath ES RADIUS server
- Fill in the **Port Number**
- The defaults should be correct for the rest
- Click Apply

The RADIUS Authentication Server is defined in the list

	MONITOR	<u>W</u> LANs (CONTROLL	ER WI	RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	Save Conligue	auon <u>P</u> ing Logo	out <u>R</u> eiresn
Security	RADIUS	Authentica	ation Ser	vers								Apply	New
AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+	Auth Cal Use AES MAC Del Framed	lled Station ID Key Wrap limiter MTU	Type (AP MAC A Designed Colon	for FIPS o	tustomers and	requires a key wra	p compliant RADI	IUS server)			
LDAP Local Net Users	Network User	Managemen	Tunnel t Proxy	Server Index	Serv	er Address(I;	ov4/Ipv6)			Port	IPSec	Admin Stat	tus
Disabled Clients		•		1	* 72.1	8.151.72			-		Disabled	Enabled	
User Login Policies AP Policies Password Policies		2		2	10.1	0.10.10				1812	Disabled	Enabled	





November 2017

5) Define the RADIUS Accounting Server as the Cloudpath RADIUS server

 cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	Save Configuration Ping Logout P S HELP FEEDBACK
Security	Acct Called Station ID Type AP MAC Address	Apply New
RADIUS Authermation Accounting Fallback DNS	MAC Delimiter Colon : Network Tunnel Server User Proxy Index Server Address(Ipv4/Ipv6) Prove Address(Ipv4/Ipv6)	Port IPSec Status
Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	2 <u>1</u> * 72.18.151.72	Disabled Enabled

- o Click on Security to access the Security menu
 - Expand AAA, expand RADIUS and then click on Accounting
 - Accept Auth Called Station ID Type as AP MAC Address (the default)
 - Accept MAC Delimiter as Colon (the default)
 - Click New

ADIUS Accounting S Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format	2 ; ASCII ;		< Back Appl
Confirm Shared Secret Port Number	1813		
Server Status	Enabled \$		
Server Timeout	5 seconds		
Network User	Enable		
Tunnel Proxy	Enable		
IPSec	Enable		

- The RADIUS Accounting Server is the Cloudpath RADIUS server from section 1
 - Fill in the Server IP Address of the Cloudpath Server



November 2017

- Fill in the Shared Secret and the Confrim Shared Secret with the Shared Secret from the Cloudpath ES RADIUS server
- Fill in the **Port Number**
- The defaults should be correct for the rest
- Click Apply

The RADIUS Accounting Server is defined in the list

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK				6	Ho
Security	RADIUS	Accour	ting Servers								l	Apply	New	
AAA General RADIUS Authentication	Acct Cal MAC Del	ed Station imiter	ID Type AP	MAC Address	•									
Fallback	Network User	Tunnel Proxy	Server Index	Server Address	(Ipv4/Ipv6)		Po	rt_I	PSec	Admin Status				
Downloaded AVP			1 *	2.18.151.72				D	isabled	Enabled				
LDAP			2	0.10.10.10			18	13 D	isabled	Enabled				
Local Net Users MAC Filtering • Disabled Clients User Login Policies AP Policies Password Policies														

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

6) Create Two WLAN profiles

One profile is for the secure/802.1X WLAN, the second for the onboarding/guest WLAN

սիսիս										Sa <u>v</u> e Configurati	on <u>P</u> ing Logout <u>R</u> efre
CISCO	MONITOR Y	MLANS Q	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBA	7	n Horr
WLANs	WLANs										Entries 1 - 16 of 16
WLANS	Current Filter	None	[Chang	e Filter] [Clea	ar Filter]		C	create New	¢ Go		
 Advanced AP Groups 	U WLAN ID	Туре	Profile Nan	ne		WLAN SSID		A	dmin Status	Security Policies	
		WLAN	610-2-2G			610-2-2G		Di	sabled	[WPA2][Auth(PSK)]	
	□ <u>2</u>	WLAN	test1			test1		Di	sabled	None	
	0 3	WLAN	610-2-5G			610-2-5G		Er	nabled	[WPA2][Auth(PSK)]	
	0 4	WLAN	TME-Chrome	ebooks		TME-Chromebool	s	Di	sabled	None	
	0.5							-			-

- o Click on WLANs to access the WLANs menu
 - Expand WLANs, and then click on WLANs (yes, it appears twice)
 - Choose Creat New and Click Go
 - Alternately, modify an existing WLAN by clicking on the WLAN ID

վուլո		5	Save Configuration Ping Logout Refresh
CISCO MONITOR	<u>W</u> LANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
WLANs	WLANs > New		< Back Apply
VLANs	Туре	WLAN 🗘	
Advanced	Profile Name	Cloudpath portal	
AP Groups	SSID	Onboarding	
	ID	17 \$	

- Choose type WLAN
- Type a Profile Name for the Secure/802.1X WLAN
- Type an SSID for the Secure/802.1X WLAN
- o Click Apply

Repeat for the Onboarding/Guest WLAN

 \circ $\,$ Choose Create New and Click ${\bf Go}$

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

- Choose type WLAN
- Type a **Profile Name** for the Onboarding/Guest WLAN
- Type an **SSID** for the Onboarding/Guest WLAN
- Click Apply

7) Edit the Secure (802.1X) WLAN profile

cisco		<u>W</u> LANs <u>C</u> C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		Lung cogott Concom
WLANs	WLANs										Entries 1 - 16 of 16
 WLANs WLANs Advanced 	Current	None	[Chang	ge Filter] [Clea	r Filter]	WI AN COTO	0	reate New	÷ Go	Security Balicies	
AP Groups		WLAN	610-2-2G	ire		610-2-2G		D	isabled	[WPA2][Auth(PSK)]	
	0 2	WLAN	test1			test1		D	isabled	None	
	□ <u>3</u>	WLAN	610-2-5G			610-2-5G		E	nabled	[WPA2][Auth(PSK)]	
	0 <u>4</u>	WLAN	TME-Chrom	ebooks		TME-Chromebook	s	D	isabled	None	
	0.5							-		· · · · ·	-

o Click on the WLAN ID of the Secure WLAN profile

LANs > E	dit 'Cloud	path-seo	cure-Jims'				<	Back	Apply
General	Security	QoS	Policy-Mapping	Advanced					
Profile Na	ime	Clou	Jdpath-secure-Jims 🤛						
Туре		WLA	AN						
SSID		Bas	icDevConf						
Status		🗹 E	Enabled						
Security	Policies	[WI (Mod	PA2][Auth(802.1X)] difications done under se	curity tab will app	ear afte	r applying the change	es.)		
Radio Pol	icy	All	÷ 🖌						
Interface	/Interface Group	o(G) vla	in tag 💠						
Multicast	Vlan Feature	E	nabled						
Broadcas	t SSID	🗹 E	nabled						
NAS-ID		non	e						

- The **General** tab appears if not, click on it
- Confirm the Profile Name and SSID are correct (or modify as necessary)
- Set Status to Enabled



Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

- As appropriate for the WLAN, choose **Radio Policy, Interface**, etc.
- Move on to the Security tab

ency Securit	ty QoS Policy-Mapping Advanced	
Layer 2 Layer	3 AAA Server	
Layer 2 Security	WPA+WPA2	
	MAC Filtering ²	
Fast Transition		
Fast Transition	Adaptive \$	
Over the DS		
Reassociation Timeout	t 20 Seconds	
Protected Managem	ient Frame	
PMF	Disabled 🗘	
WPA+WPA2 Paramo	eters	
WPA Policy		
WPA2 Policy		
WPA2 Folicy		
WPA2 Encryption		
OSEN Policy		
Authentication Key	Managemen 2	
802.1X	C Enable	

- Under the **Security** tab, go to the **Layer 2** tab
 - For Layer 2 Security choose WPA_WPA2
 - Under WPA + WPA2 Parameters choose WPA2 and WPA if required, and choose AES for encryption
 - Under Authentication Key Management, Enable 802.1X
 - Move on the AAA Servers tab

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

eneral S	Security	QoS Pr y	/-Mappin	g Advanced			
ayer 2	Layer 3	AAA Servers					
	0	ita interfaca 🗌 En					
RADIUS Se Apply Cisco	Authentica	t Settings En	abled abled Accoun	ting Servers	2	EAP Parameters	
RADIUS Se Apply Cisco Server 1	Authentica	t Settings End	abled abled Accoun S Enab	ting Servers led 10.10.10, Port:1813	3 \$	EAP Parameters Enable	
RADIUS Se Apply Cisco Server 1 Server 2	Authentica C Enabled IP:10.10.1 None	t Settings Ena	abled abled Accoun Enab P:10. None	ting Servers led 10.10.10, Port:1813	3 0	EAP Parameters Enable	
RADIUS Se Apply Cisco Server 1 Server 2 Server 3	Authentica C Enabled IP:10.10.1 None None	t Settings End	abled abled Accoun ♥ Enab ♥ IP:10. ♥ None ♥ None	ting Servers led 10.10.10, Port:1813		EAP Parameters Enable	
RADIUS Se Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica C Enabled IP:10.10.1 None None None	t Settings Ena	abled abled Accoun Enab TP:10. None None None	ting Servers led 10.10.10, Port:1813		EAP Parameters Enable	
RADIUS Se Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Authentica C Enabled IP:10.10.1 None None None None None	t Settings Ena	abled abled Accoun Enab i IP:10. i None i None i None i None	ting Servers led 10.10.10, Port:1813		EAP Parameters Enable	

- o Under the Security tab, go to the AAA Servers tab
 - Choose and Enable the Authentication Server and the Accounting Server previously defined – that is, the Cloudpath RADIUS server
 - Click Apply

The Secure 802.1X WLAN is defined.



November 2017

8) Edit the onboarding WLAN profile

cisco		<u>W</u> LANs g	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	Colle coningeration	n Eng i Sogoot Eon € Ho
WLANs	WLANs										Entries 1 - 16 of 1
 WLANs WLANs Advanced 	Current	None	Profile Na	ge Filter] [Clea	r Filter]	WI AN SCID		reate New	Go	Security Policies	
AP Groups		WLAN	610-2-2G	inc		610-2-2G			isabled	[WPA2][Auth(PSK)]	
	0 2	WLAN	test1			test1		D	isabled	None	
	03	WLAN	610-2-5G			610-2-5G		E	nabled	[WPA2][Auth(PSK)]	
	0 4	WLAN	TME-Chrom	nebooks		TME-Chromebook	5	D	isabled	None	
								-		·····	-

o Click on the WLAN ID of the onboarding WLAN profile

				5a <u>v</u>	e configuration Ping	Logout Keine
cisco	MONITOR WLANS CONTROL	ller w <u>i</u> reless <u>s</u> ecur	ITY MANAGEMENT	C <u>O</u> MMANDS HEL	P <u>F</u> EEDBACK	<u>n H</u> or
٧s	WLANs > Edit 'Cloudpath	ı-portal'			< Back	Apply
ANs ANs	General Security Q	S Policy-Mapping	Advanced			
Groups	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vian Feature Broadcast SSID NAS-ID	Cloudpath-portal WLAN CP-portal-JimS C Enabled WEB POLICY,On-MAC-Filt (Modifications done under sec All ‡ Vian tag ‡ Enabled C Enabled none	er-failure, MAC Filteri urity tab will appear afte	ng[WPA2][Auth(PSK er applying the changes.)	

- The **General** tab appears if not, click on it
 - Confirm the **Profile Name** and **SSID** are correct (or modify as necessary)
 - Set Status to Enabled
 - As appropriate for the WLAN, choose **Radio Policy, Interface**, etc.
 - Move on to the **Security** tab



Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

/LANs > Edit 'C' (dpath-portal'		< Back App
General Security QoS Policy-I	lapping Advanced	
Layer 2 Layer 3 AAA Serve		
Layer 2 Security 🤨 None	\$	
MAC Filtering ²		
Fast Transition		
Fast Transition Disable 🗘		
Lobby Admin Configuration		
Lobby Admin Access		

- Under the **Security** tab, go to the **Layer 2** tab
 - For Layer 2 Security choose None
 - Move on to the Layer 3 tab



Deploying a Cloudpath workflow on a Cisco WLAN Controller

N			-20	17
\sim	over	nner		
			20	

ANs > E	dit 'Cloudp	ath-portal'		< Back	Ap
eneral	Security	QoS Policy-Mapping	Advanced		
ayer 2	Layer 3	AAA Servers			
Layer 3 Captive	Security ¹ Network Assista	Web Policy ¢			
Pass	through				
Conc	lition Web Red	irect			
🔘 Spla	st ge Web Re	direct			
🖸 On M	IAC Filter failure	<u>ه</u>			
Preauth	entication ACL	IPv4 Cloudpath-JimS \$	IPv6 None VebAuth FlexAcl No	ine 🛊	
Sleeping	g Client 🗌 Ena	ble			
Override	e Global Config ²	🗹 Enable	<u> </u>		
Web Au	th type	External(Re-direct to ex	ternal server) \$		
Dedirect	LIRI https://	emo.cloudpath.net/enroll/Broca	de2/BasicWorkflow/res		

- o Under the **Security** tab, go to the **Layer 3** tab
 - For Layer 3 Security choose Web Policy
 - Among the radio buttons, choose **On MAC Filter failure**
 - For **Preauthentication ACL**, choose the previously defined ACL
 - For Web Auth Type choose External (Re-direct to external server)
 - For Redirect URL enter the URL of the workflow defined on Cloudpath, as described in section 1
 - Click Apply

The Onboarding Portal is defined.

November 2017

9) Create or Edit an AP group to deploy WLANs

alada		Sa <u>v</u> e Configuration Ping Logout Recess					
	OR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECUR	ITY MANAGEMENT COMMANDS HELP FEEDBACK					
WLANs	AP Groups	Entries 1 - 12 of 12 Add Group					
WLANS WLANS Advanced AP Groups	AP Group Name <u>11ac-Test</u> <u>3rd-party-testing-group</u> <u>610-1</u>	AP Group Description					
	610-2 AppleClassroom	Apple Classroom					
	BS-Open BS-Test						
	Chrome ClassromTest_channel36	4720 Competitive					
	<u>Cloudpath-JimS</u>						

- o Click on WLANs to access the WLANs menu
 - Expand Advanced, and then click on AP Groupss
 - Create a new Group by clicking on Add Group
 - Alternately, modify an existing Group by clicking on the AP Group Name

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGE	EMENT	Sa <u>v</u> e Conf	iguration HE <u>L</u> P	<u>P</u> ing <u>F</u> EEDB#	Logout <u>R</u> efresi ACK <mark>A</mark> <u>H</u> ome
WLANS WLANS Advanced AP Groups		AP Grou Add New AP Grou Descript	p Name ion Add	Cancel				Entri	es 1 - 12	of 12	Add Group
		AP Group	Name			AP Group	Descrip	ition			

- The Add New AP Group section appears
 - Enter a name in the **AP Group Name**
 - Optionally, add a Description
 - Click Add





November 2017

11 111 11							Save Com	iguration		out <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	n <u>H</u> ome
WLANs		AP Grou	ips				En	tries 1 - 1	L2 of 12	Add Group
• WLANs WLANs		AP Group	Name			AP Group Descrip	otion			
Advanced		11ac-Test								•
AP Groups		3rd-party-	testing-group							•
		<u>610-1</u>								-
		<u>610-2</u>								*
		AppleClass	sroom			Apple Classroom				-
		BS-Open								-
		BS-Test								•
		Chrome								-
		ClassromT	est_channel36			4720 Competitive				•
		Cloudpath	-JimS							-

• Now click on the AP Group Name to edit

cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEME	SA INT C <u>O</u> MM	a <u>v</u> e coning 1ANDS	HELP	<u>P</u> ing Logo <u>F</u> EEDBACK	ut <u>k</u> eiresi <mark>i H</mark> ome
WLANs • WLANs		Ap Grou	ps > Edit	BE Profile	nS'	802.11u	Location	Ports	/Module	< Ba	ck
WLANS Advanced AP Groups								A	Apply		
		AP Gro AP Gro	up Name up Description	Cloudpath	loudpath-JimS						
		NAS-ID Enable	Client Traffic Qin	Q O							
		Enable QinQ S	DHCPv4 QinQ ³ ervice Vlan Id <u>10</u>	0							
		CAPW	AP Preferred Mode	e 🗌 Not-(Configured						

• Go to the **WLANs** tab



Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	n j
Ap Group	os > Edit	'Chudpath2							< Back
General	WLAN	RF Profil	e APs	802.11u	Location	Ports/Module			
								Add New	
Add Nev	v				-				
WLAN S	SID	BasicDevConf	(15)	\$					
Interfac /Interfa Group(0	ce G)	management		\$	1				
SNMP N	AC State	Add Can	cel						
WLAN ID	WLAN	N SSID(2)(6)		Interface/	Interface Grou	p(G) SNM	P NAC S		
14	CP-po	rtal-JimS		manageme	nt	Disab	led		

- o In the WLANs tab, click the Add New button
 - Choose the WLAN SSID of the onboarding portal
 - Choose the interface for the WLAN
 - Click Add
- o repeat for the authenticated WLAN
 - In the WLANs tab, click the Add New button
 - Choose the WLAN SSID of the 802.1X authenticated WLAN
 - Choose the **interface** for the WLAN
 - Click Add

Be careful not to add the wrong WLAN or an extra WLAN. To remove a WLAN, the group has to be deleted and recreated.

Deploying a Cloudpath workflow on a Cisco WLAN Controller



November 2017

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	T COMMANDS	HELP	FEEDBACK	n <u>H</u> om
Ap Groups	s > Edit	'Cloudpath2	· .	1					< Back
General	WLAN	s RF Profil	e APs	802.11u	Location	Ports/Module			
APs curre	ntly in th	e Group Etherne	t MAC	Remove AP:	S Add APs	d.74ff.8382-JimS	Group default-	Name -group	Add APs

- o Go to the **APs** tab
 - Under Add APs to the Group, check the APs that will be part of the group and will service our two WLANs
 - Click Add APs

Configuration of the WLC is done and ready for testing.



November 2017

10) Don't do this: Configuring Web Auth default policy option

A global Web Auth policy can be set for the WLAN controller. The Onboarding Portal can be setup under the Security -> Web Auth menu. Best Practices are to add the onboarding Prtal URL to the WLAN profile as we did above. Associating the onboarding profile to only specific SSIDs is cleaner and more flexible. Furthermore, the MAC auth Guest passthrough from the onboarding profile does not work correctly when using the global Web Auth setting. However, if you are NOT using MAC auth passthrough, this configuration does work, and is included here for completeness.

	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Save Conr	iguration HELP	FEEDBACK	
Security	Web	Login Pa	ige				- <u>-</u>	F	Preview	Apply
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Profestion Web Auth Web Login Page Certificate 	Web Redii Login Exter QrCc QrCc	Authentica rect URL aft n Success P rnal Webau ode Scannin ide Scannin	tion Type ter login age Type th URL g Bypass Timer g Bypass Count	htt	External (Red https://demo. ps://demo.clou	firect to external second	erver) •	Workflow/		
TrustSec										

- o Click on **Security**
- In the Security menu, expand Web Auth and choose Web Login Page
- o For Web authentication Type choose External (Redirect to external server)
- o At External Webauth URL insert the Cloudpath ES enrollment URL found in section 1
- Click apply

Now any WLAN with a L3 security policy set to Web Policy will default to the Cloudpath URL



November 2017

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor "Smart Wi-Fi" products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit http://www.ruckuswireless.com.

Ruckus and Ruckus Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries.





Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved.

Copyright Notice and Proprietary Information No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL