CONFIGURATION GUIDE



# Cloudpath Enrollment System Cisco Wireless LAN Controller-Redirect Configuration Guide, 5.7

Supporting Cloudpath Software Release 5.7

## **Copyright, Trademark and Proprietary Rights Information**

© 2020 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

### **Export Restrictions**

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

### Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

### **Limitation of Liability**

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

### Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

Overview	4
Prerequisites	4
Configuring the Cisco WLC for Web Passthrough	4
Configure Access Control Lists	5
Configure WLAN	6
Configure the Web Login Page	7
Configuring Cloudpath for Web Passthrough	8
Add the Redirect Step to the Workflow	8
Testing the Configuration	9
Verify Client State	9

# **Overview**

If you use Cloudpath to onboard wireless devices to a secure SSID, and would like to implement a Cisco Wireless LAN Controller to manage network policy, you can easily configure Cloudpath to redirect users through the WLAN Controller.

Cloudpath manages the entire enrollment process, opening the firewall to the open SSID, and passing the user through your policy management system before onboarding them to your secure WPA2- Enterprise wireless network.

FIGURE 1 Cloudpath With WLC Passthrough



## **Prerequisites**

Before you can configure Cloudpath and Cisco WLAN Controller for web passthrough, you must have the following set up in your network.

- Cisco Wireless LAN Controller configured in your network
- IP address of Cloudpath system
- A Cloudpath enrollment workflow configured for your network

## **Configuring the Cisco WLC for Web Passthrough**

This section describes how set up the preauthentication ACL, the WLAN, and the Web Authentication Page on the Cisco WLC.

## **Configure Access Control Lists**

Configure a preauthentication ACL to allow access from the controller to and from Cloudpath.

1. On the Cisco WLAN Controller, under Security, expand Access Control Lists, and select the ACL to use for preauthentication.

FIGURE 2 Set Up the Preauthentication ACL

Cisco - Windows Internet En	plorer											لع	
G C * B http://192.166.	<.80/scre	ens/franes	et herei 🖉 🛃 🤒	🧭 XpressCo 🤇	🖞 XpressC 🧕	Osco 🧭	XpressC (2) O	ibis: Onl 🥝 403 For	thui 🥝 Osco	×	onpeti	0 🛠	0
Ele Edit Yew Pavorites	Tools	5Mp											
🚕 🍯 Winitnet Apps failing whe	n1 7	¥ 802.1x - 0	Cross Forest Auth	Configuring Certific	ate-Base 🔞 20	11 Annual Conferen	ce Ex 🔞 2012 /	Annual Conference Ex	TN Add Publish	ed Certificates	s t		
× Find: 5.71			Previo	us Next 📝 Opt	ions +								
ululu cisco	Mon	ITOR M	ILANIS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sage	Configuratio	n   Eing	Logout Bef	resh
Security ^	Acc	ess Cor	ntrol Lists > Ed	it						< Back	Add N	lew Rule	-
- AAA	Gen	eral											
General • RADRUS	Acces	s List Nam	ne AllowXo	¢									
Authentication Accounting	Seq	Action	Source IP/Masl		Destination I	P/Mask	Protocol	Source Port	Dest Port	DSCP	Direction		
TACACS+     LDAP     Local Net Users	1	Permit	0.0.0.0	/	192.168.5.71 255.255.255.2	/	Any	Any	Any	Any	Any	•	
MAC Filtering Disabled Clients	2	Permit	192.168.5.71 255.255.255.255	/	0.0.0.0	/	Any	Any	Any	Any	Any		
User Login Policies AP Policies	a	Permit	0.0.0.0	1	0.0.0.0	/	UDP	Any	DHCP Client	Any	Any		
Local EAP     Defaulty Order	4	Permit	0.0.0.0	/	0.0.0.0	/	UDP	Any	DHCP Serve	Any	Any	•	
* Access Control Lists	4	Permit	0.0.0.0	/	0.0.0.0	/	TCP	Any	DHCP Client	Any	Any		
Access Control Lists CPU Access Control Lists	4	Permit	0.0.0.0	1	0.0.0.0	/	TCP	Any	DHCP Serve	Any	Any		
> IPSec Certs	2	Permit	0.0.0.0	1	0.0.0.0	/	UDP	DNS	Any	Any	Any		
Wireless Protection     Policies		Permit	0.0.0.0	/	0.0.0.0	/	TCP	DHCP Server	Any	Any	Any		
• Web Auth	2	Permit	0.0.0.0	/	0.0.0.0	1	TCP	DHCP Client	Any	Any	Any		~
r cuis					3000000							100%	

- 2. Edit the ACL to add rules to permit the client to and from Cloudpath.
- 3. Apply changes.

## **Configure WLAN**

Configure the WLAN to enable web passthrough and allow the preauthentication ACL created in the previous step.

1. On the Cisco WLAN Controller, under **WLANs**, edit the WLAN to use for the passthrough.

#### FIGURE 3 Edit WLANs

Cisco - Windows Internet Ex	(plorer	_O×
C C v 6 http://192.168.	4.80/scr 🔎 🛃 🥌 xp 🦪 xp 🦪 Cisco 🦪 xp 🥳 Cis 🥳	40 🥶 c. 🗙 🎐 co 👘 🔝 🔅
Ele Edit View Favorites	Iools Help	
🛛 🍰 🍠 WinInet Apps failing whe	en I 👖 802.1x - Cross Forest Auth 💢 Configuring Certificate-Base 🔞 20	11 Annual Conference Ex **
× Find: 5.71	Previous Next   🥖 Options -	
ahaha cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	Save Configuration   Ping   Logout   Refresh MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit	< Back Apply ^
₩LANs	General Security QoS Advanced	
WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Layer 3 Security None	
	O Authentication	
	Passthrough	
	Conditional Web Redirect     Preauthentication ACL	
	Email Input	
		~
		* 100% - //

- 2. Select the **Security** tab and the **Layer 3** tab.
- 3. In the Layer 3 Security section, check the Web Policy box and select Passthrough. Leave Layer 3 Security at None.
- 4. Set the Preauthentication ACL. Leave Email Input unchecked.
- 5. Apply changes.

## **Configure the Web Login Page**

Set up the Cloudpath captive portal page. The WLC redirects the users to the Cloudpath captive portal, where they must accept the network AUP before they are moved to the open SSID for onboarding. Cloudpath manages the onboarding process instead of the WLC.

1. On the Cisco WLAN Controller, under Security, expand Web Auth, and select Web Login Page.

#### FIGURE 4 Configure Web Login Page

Cisco - Windows Internet Exp	lorer						
C C + 102.168.4	.80/sc 🔎 💽 😚 🏹	э 👩 Хр 🥳	Cisco 🧭 Xp	. @ Gt 3	🥑 40  🥶 C. 🗙	🤌 Co	$\odot$
Ele Edit Yew Favorites	Iools Help						
🛛 🍰 🍠 WinInet Apps failing when	I 7N 802.1x - Cross For	rest Auth 💢 Co	nfiguring Certifica	te-Base 🔞 2	2011 Annual Conferen	ce Ex	**
× Find: 5.71		Previous N	iext 🛛 🥖 Optic	ns •			
ahaha					Save Configuratio	in   <u>P</u> ing   Logi	out <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	Web Login Page				1	Preview	Apply
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS                 Authentication                 Accounting</li> <li>TACACS+                 LDAP                 Local Net Users                 MAC Filtering                 Disabled Clients                 User Login Policies                 AP Policies</li> </ul> </li> <li>Local EAP         <ul> <li>Priority Order</li> <li>Access Control Lists</li> </ul> </li> </ul>	Web Authenticatio	on Type	External (	Redirect to ext	ternal server)		
<ul> <li>IPSec Certs</li> <li>Wireless Protection Policies</li> <li>Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary</li> </ul>						•	100% • //

- 2. Select External (Redirect to external server).
- 3. Enter the URL of Cloudpath.
- 4. Apply changes.

# **Configuring Cloudpath for Web Passthrough**

This section describes how to configure Cloudpath to manage the redirect URL from the WLC, including any parameters that must exist on the inbound request, and move the user to the captive portal to complete the onboarding process.

## Add the Redirect Step to the Workflow

This section describes how to create a redirect step to the enrollment workflow to allow Cloudpath to accept an inbound connection request from the WLC, redirect the user to an Cloudpath-managed captive portal, and provide the onboarding process.

- 1. Navigate to **Configuration** > **Workflow**.
- 2. Select your passthrough workflow configuration.
- 3. In the workflow, insert the redirect step.

#### NOTE

In this example, the redirect occurs after the user accepts the AUP. However, the redirect step can be placed anywhere in the enrollment workflow.

- 4. The workflow plug-in selection page opens.
- 5. Click Redirect the User.
- 6. Select Use a new redirect and click Next. The Create Redirect page opens.

#### FIGURE 5 Create Redirect

Display Name:	Cisco WLAN Login
Description:	
Redirect URL:	\${switch_url}? buttonClicked=4&redirect_url=https:// <redirect_website>/en roll/syour_Account&gt;/Production/submit-redirect</redirect_website>
Use POST:	
DOST Parameters:	[ex. username=bob]
Allow Continuation:	
i) Kill Session:	

7. Enter the **Reference information** for the Cisco WLAN passthrough.

#### 8. Enter the Redirect URL in this format:

```
${switch_url}?buttonClicked=4&redirect_url=https://<redirect_website>/enroll/<your_Account>/
Production/submit-redirect
```

Note: The first part of this URL (\${switch\_url}?buttonClicked=4&redirect\_url) takes the inbound request from the WLC and opens the firewall. The second part of this URL (https://<redirect\_website>/enroll/<your\_Account>/ Production/submit-redirect) points the user to the Cloudpath captive portal.

9. Leave Use POST unchecked.

Note: Cisco WLAN Controllers allow both Get and POST for the URL call, but we recommend using Get.

- 10. Check the Allow Continuation box. If this is left unchecked, the submit-redirect call is ignored.
- 11. If needed, configure Filters & Restrictions to control when this redirect is utilized.

By default the redirect is applied to all users. However, you can specify a filter such that the redirect is applied only to enrollments matching the filter.

12. Save the workflow.

In this workflow example, the WLC passes the user to the Cloudpath captive portal, to accept the AUP. The Cisco WLAN redirect opens the firewall so that the client can access Cloudpath for the onboarding process. If the user selects the guest enrollment path, the device is moved to the **Guest** - **Internet Only:** network and given a short-term guest client certificate.

#### FIGURE 6 Completed Enrollment Workflow with Redirect Step

•									
	Step 1:	Require the u	iser to accept th	e AUP Welcom	e Message and AUP		1	×	
•									
	Step 2:	Redirect the u	user based on C	isco WLAN Lo	gin.		1	×	
•									
	Step 3:	All matches in	n: 🗙 🖍 Gu	est [All Options	5] * +	1	≡	×	
•									
	Step 4:	Authenticate	the user via Fac	ebook Login			1	×	
•									
	Result:	Move user to	Guest: Interne	t-only and assi	gn certificate using One	-day guest templa			1

## **Testing the Configuration**

This section describes how to test the configuration for Cloudpath redirect through a Cisco WLAN Controller.

### **Verify Client State**

Use this information to verify the client state before and after the firewall is opened.

On the Cisco WLAN Controller, under Wireless, view the Client Properties.

Before the firewall is opened, the **Policy Manager State** for the user should be in the **WEBAUTH\_REQD** state. In this state, the WLAN Controller redirects all traffic.

FIGURE 7 Client Detail Before Redirect

🕒 🕑 💌 🧭 http://192.1/	68.4.80/screens/fra 🔎 🛃 😚 Xpre	ss 🧭 Cisco 🥳 Xpress	. 🔆 Cibrix O 🎯 403 Fo	🗿 Cisco 🗙 🏓 Compis 💿 🏠 🕄
Ele Edit Yew Favorite	s Icols Help			
🍰 🍠 WinInet Apps failing v	when I 7 802.1x - Cross Forest Auth	X Configuring Certificate-Base	2011 Annual Conference Ex	2012 Annual Conference Ex
K Find: 5.71	Pre	vious Next 📝 Options •		
 cısco	MONITOR WLANS CONTR	OLLER WIRELESS SECUR	S ITY MANAGEMENT COMM	iage Configuration   Ping   Logout   Befre ANDS   HELP
Wireless	Clients > Detail		1	< Back Link Test Remove
Access Points	<b>Client Properties</b>		AP Properties	
<ul> <li>Access Points All APs <ul> <li>Radios 802.11a/n 802.11b/g/n <li>AP Configuration Mesh Rogues Clients 802.11a/n 802.11a/n 802.11b/g/n Country Timers</li> </li></ul> </li> </ul>	MAC Address IP Address Client Type User Name Port Number Interface VLAN ID CCX Version E2E Version E2E Version Mobility Role Mobility Porer IP Address	00:23:14:ba:85:34 192.168.6.90 Regular 1 management 0 CCXv4 E2Ev1 Local N/A	AP Address AP Name AP Type WLAN Profile Status Association ID 802.11 Authentication Reason Code Status Code CF Pollable CF Poll Request	00:18:74:d3:a5:80 AP0018.ba75.a24e 802.11a Sample Campus - Setu Associated 1 Open System 0 0 Not Implemented Not Implemented
	Policy Manager State management Frame Protection Security Information	WEBAUTH_REQD	Short Preamble FBCC Channel Agility Timeout	Not Implemented Not Implemented O
	Policy Type Encryption Cipher	N/A None	WEP State	WEP Disable
	EAP Type	N/A		

After the firewall is opened, the Policy Manager State for the user should be in the RUN state.

FIGURE 8 Client Detail After Redirect

Cisco - Windows Internet	Explorer			
🔁 🕙 💌 🤮 http://192.1	68.4.80 iscreens ifra 🔎 🛨 🛃 🏹 Xpress	s 🦪 Cisco 🔏	Xpress 🤅 Citrix O 🎯 403 Fo	🍯 Cisco 🗙 📥 Compa 🕥 🔝 🕄
Ele Edit Yew Favorite	s Icols Help			
😘 🍠 WinInet Apps failing v	when I TN 802.1x - Cross Forest Auth	X Configuring Certifical	te-Base 🕡 2011 Annual Conference Ex (	🕜 2012 Annual Conference Ex
× Find: 5.71	Previ	ious Next 📝 Optio	ns •	
ာါကျက cisco	MONITOR WLANS CONTRO	LLER WIRELESS	SECURITY MANAGEMENT COMM	Saye Configuration Ping Logout Befree IANDS HELP
Wireless	Clients > Detail		1	< Back Link Test Remove
Access Points     All APs	Client Properties		AP Properties	
	MAC Address	00:23:14:ba:85:34	AP Address	00:18:74:d3:a5:80
<ul> <li>AP Configuration</li> </ul>	Client Type	192.168.6.90 Regular	AP Name AP Type	802.11a
Mesh	User Name		WLAN Profile	Sample Campus - Setu
Rogues Clients	Port Number	1	Status	Associated
▶ 802.11a/n	LI AN TO	nanayement.	PO2 11 Authentication	A Costom
802.11b/g/n	CCX Version	CCXv4	Reason Code	0
Country	E2E Version	E2Ev1	Status Code	0
Timers	Mobility Role	Local	CF Pollable	Not Implemented
	Mobility Peer ID Address	N/A	CF Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Not Implemented
	Management Frame Protection	NO	PBCC	Not Implemented
	Security Information		Channel Agility	Not Implemented
	Security Policy Completed	Yes	WEP State	WEP Disable
	Policy Type	N/A		
	Encryption Cipher	None		
	EAP Type	N/A		



© 2020 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com