CONFIGURATION GUIDE



Cloudpath Enrollment System Cisco Wireless LAN Controller-Redirect Configuration Guide, 5.6

Supporting Cloudpath Software Release 5.6

Part Number: 800-72492-001 Rev A Publication Date: 15 December 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 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, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex 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

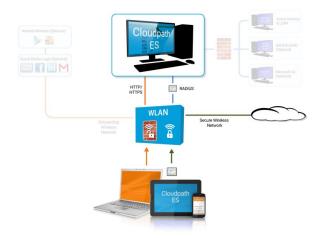
Overview	4
Prerequisites	
Configuring the Cisco WLC for Web Passthrough	
Configure Access Control Lists	
Configure WLAN	6
Configure the Web Login Page	
Configuring Cloudpath for Web Passthrough	8
Add the Redirect Step to the Workflow	
Testing the Configuration	9
Verify Client State	

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

3 🕢 🕈 🗃 http://1992.168.4	.80/scre	ens/haves	ated P .	🧭 XpressCo 🧭	NpressC	Osco 🤞	ApressC 🛞 CA	rix Onl 🥑 403 For	b 🧭 Osco	× . 0		0 🖈	0
Ele Edit Yew Favorites	Tools	5Mp											
🚕 🍠 Wininet Apps failing when	L 7	¥ 802.1x - 0	Cross Forest Auth	Configuring Certifica	te-Base 🕖 201	11 Annual Conferen	oe Ex 🔞 2012 A	nnual Conference Ex	TN Add Publisher	d Certificates	t		19
K Find: 5.71	_		Previo	us Next 🥖 Optic	ns •								
cisco	HON	ITOR 10	IANI CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	Sage O	orfiguratio	h I Bing I	Legad Bef	resh
Security A	Acc	ess Cor	ntrol Lists > Ed	it						c Back	Add N	ew Rule	,
• AAA General	Gene	eral											
RADRUS Authentication Accounting	Acces	s List Nem	e AllowXg 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	55	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	2	Permit	0.0.0.0	1	0.0.0.0	/	UDP	Any	DHCP Client	Any	Any		
Local EAP Priority Order	A	Permit	0.0.0.0	7	0.0.0.0	/	UDP	Any	DHCP Server	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 Server	Any	Any		
IPSec Certs	2	Permit	0.0.0.0	1	0.0.0.0	1	UDP	DNS	Any	Any	Any		
Wireless Protection Policies	2	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		
												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

Second guration and a second guration and gurated guration and guration and guration and guration and guratin	Cisco - Windows Internet Ex	xplorer		_0×
Windnet Acpos failing when L TV 802.1x - Cross Forest Auth X Configuring Certificate-Base 2011 Annual Conference Ex >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	C C V //192.168.	3.4.80/so 🔎 🔄 👉 🎯 Xp 🧭 Xp 🧭 Cisco 🧭 Xp 🔅 Cit 🥥 40	🦪 c. 🗙 🎐 co	6 ☆ ☺
Wilder Apps faling when L TN B02.1x - Cross Forest Auth \$ Configuring Certificate-Base 2 2011 Annual Conference Ex X Find: Saye Configuration Ping Logout Refresh C1SCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MAAAGEMENT COMMANDS HELP WLANS WLANS WLANS Controller Wire Controller Controler Controler Controller	Ele Edit Yew Favorites	Tools Help		
Image: Second	🛛 🐅 🍠 WinInet Apps failing whe	en I 👖 802.1x - Cross Forest Auth 💢 Configuring Certificate-Base 🔞 2011 Annu	al Conference Ex	**
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS WLANS > Edit < Back Apply WLANS WLANS > Edit < Back Apply WLANS General Security QoS Advanced WLANS Layer 2 Layer 3 AAA Servers <	× Find: 5.71	Previous Next 📝 Options -		
WLANS WLANS WLANS AP Groups VLAN General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security None Image: Conditional Web Policy Authentication Image: Passthrough Conditional Web Redirect Preauthentication ACL AllowXpc Image: Conditional Web Redirect				
WLANS AP Groups VLAN Layer 2 Layer 3 AAA Servers Layer 3 Security None Web Policy Authentication Passthrough Conditional Web Redirect Preauthentication ACL AllowXpc Email Input	WLANs	WLANs > Edit	< Back	Apply
AP Groups VLAN	* WLANS	General Security QoS Advanced		
Web Policy Authentication Passthrough Conditional Web Redirect AllowXpc Email Input		Layer 2 Layer 3 AAA Servers		
* 100% - //		Web Policy Authentication Passthrough Conditional Web Redirect AllowXpc		
				* 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	olorer						
🔆 🕑 💌 🧭 http://192.168.4	.80/sci 🔎 🔹	🧭 Xp 🧭 Xp	🥑 Cisco 🧭 Xp.		🥶 40 🥶 c. 🗙	🤌 Co	♠ ☆ @
Ele Edit Yew Favorites	Iools Help						
👍 🍠 WinInet Apps failing when	I 7N 802.1x - G	ross Forest Auth 💢	Configuring Certific	ste-Base 🔞	2011 Annual Conferen	nce Ex	**
× Find: 5.71		Previous	Next 🥖 Opti	ons +			
ahaha					Save Configurati	on <u>P</u> ing Log	out <u>R</u> efresh
cisco	MONITOR WI	ANS <u>C</u> ONTROLLER	R WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	Web Login P	age			1	Preview	Apply
 AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Access Control Lists IPSec Certs Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events 	Web Authent	ication Type			ternal server) 🗸		
Summary							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

Description:		
Redirect URL:	\${switch_uri)?	
, neurona	stymict_uity r buttonClicked=4&redirect_url=https:// <redirect_website>/en roll/<your_account>/Production/submit-redirect</your_account></redirect_website>	
Use POST:		
POST Parameters:	[ex. username=bob]	
Allow Continuation:		
) 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 us	ser to accept t	the AUP Welcom	e Message and AUP		1	×	
•	Step 2:	Redirect the u	ser based on	Cisco WLAN Lo	gin.		1	×	
•	Step 3:	All matches in	× / G	iuest [All Options	s] ¥ +	1	≡	×	
•	Step 4:	Authenticate t	he user via Fa	acebook Login			/	×	
•	Result:	Move user to	Guest: Intern	et-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

	s Iools Help when I 770 802.1x - Cross Forest Auth.	. 🙀 Configuring Certificate-Base	0 2011 Annual Conference Ex	2012 Annual Conference Ex	
K Find: 5.71	P	evious Next 📝 Options •			
 cısco	MONITOR WLANS CONTI	ROLLER WIRELESS SECU		Saxe Configuration Ping ANDS HELP	Logout Befres
Wireless	Clients > Detail		1	< Back Link Test	Remove
* Access Points	Client Properties		AP Properties		
 Radios 802.11a/n 802.11b/g/n AP Configuration Mesh Rogues Clients 802.11a/n 802.11b/g/n Country Timers 	MAC Address IP Address Client Type User Name Port Number Interface VLAN ID CCX Version E2E Version Mobility Role Mobility Peer 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 Recuest	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 Prame Protection Security Information Security Policy Completed Policy Type Encryption Cipher	WEBAUTH_REQD No N/A None	Short Preamble PBCC Channel Agility Timeout WEP State	Not Implemented Not Implemented 0 WEP Disable	

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

FIGURE 8 Client Detail After Redirect

	68.4.80/screens/ins P 🔹 🔧 🍘 Xpress es Icols Help	s 🥌 Cisco 🥌 Xpress	🥸 Cibrix O 🏈 403 Fo 🥼	🗿 Cisco 🗙 🏓 Compa	
	when I 7 802.1x - Cross Forest Auth		🕜 2011 Annual Conference Ex	2012 Annual Conference Ex	
K Find: 5.71	Previ	ious Next 📝 Options •			
cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECU			Logout Befres
Wireless	Clients > Detail			< Back Link Test	Remove
Access Points All APs	Client Properties		AP Properties		
 ✓ Radios 802.11a/n 802.11b/g/n ✓ AP Configuration Mesh 	MAC Address IP Address Client Type User Name	00:23:14:ba:85:34 192.168.6.90 Regular	AP Address AP Name AP Type WLAN Profile	00:18:74:d3:a5:80 AP0018.ba75.a24e 802.11a Sample Campus - Setu	
 Rogues Clients 802.11a/n 802.11b/g/n Country Timers 	Port Number Interface VLAN ID CCX Version E2E Version Mobility Role Mobility Role Policy Manager State	1 management 0 CCXv4 E2Ev1 Local N/A RUN	Status Association ID 802.11 Authentication Reason Code Status Code CF Pollable CF Pollable Short Preamble	Associated 1 Open System 0 0 Not Implemented Not Implemented Not Implemented	
	Management Frame Protection Security Information Security Policy Completed	Yes	PBCC Channel Agility Timeout WEP State	Not Implemented Not Implemented 0 WEP Disable	
	Policy Type Encryption Cipher EAP Type	N/A None N/A			



© 2019 CommScope, Inc. All rights reserved. Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc. 350 West Java Dr., Sunnyvale, CA 94089 USA www.ruckuswireless.com