CONFIGURATION GUIDE



# Configuring Cloudpath to Redirect Through a Cisco Wireless LAN Controller

**Supporting Software Release 5.2** 

Part Number: 800-71654-001 Publication Date: August 2017

### **Copyright Notice and Proprietary Information**

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

### **Destination Control Statement**

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United 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. BROCADE and RUCKUS WIRELESS, INC. AND THEIR 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. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

#### **Limitation of Liability**

IN NO EVENT SHALL BROCADE OF 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.

### **Trademarks**

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

# 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

🕒 🕑 🕈 🔂 hitsi.()192.168.9	4.80/scre	ens/Tranes	ethed Pr	🧭 XpressCo	StpressC	Osco 🧭	XpressC (2) O	brix Onl	6 🥑 Osco	×		0 \$	0
Be Edk Yew Favorites	Lools	<u>Help</u>											
沟 🍠 Wininet Apps failing when	n1 7	802.1x -	Cross Forest Auth	Configuring Centrics	ste-Base 👩 20	11 Annual Conferen	ce Ex 🔞 2012 /	Innual Conference Ex	TN Add Publish	ed Certificates	st		3
K Find: 5.71			Previo	us Next 📝 Opti	ons •								
ll cisco	MON	TOR V	YLANIS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Saya	lorfiguratio	n I Eina I	Legout   Befr	resh
Security ^	Acc	ess Cor	ntrol Lists > Ed	it						< Back	Add N	lew Rule	,
- AAA General	Gene	eral											
RADIUS     Authentication     Accounting	Acces	s List Nerr	Source IP/Masl	< k	Destination	IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction		
TACACS+     LDAP     Local Net Lines	1	Permit	0.0.0.0	/	192.168.5.71	/	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	•	1
User Login Policies AP Policies	a	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	/	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	/	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	1	0.0.0.0	1	TCP	DHCP Client	Any	Any	Any		
r clus												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 E	xplorer		_O×
C C + 1/192.168	8.4.80/so 🔎 💽 🔄 🧑 xp 🧔 xp 🦪 Cisco 🧔 xp 🔅 Cit 🥘 40	🦪 c. 🗙 🎐 Co	(∩ ☆ (2)
Ele Edit Yew Favorites	Tools Help		
🛛 🍰 🍠 WinInet Apps failing whe	en I 👖 802.1x - Cross Forest Auth 💢 Configuring Certificate-Base 🔞 2011 Ann	al Conference Ex	**
× Find: 5.71	Previous Next / 🔗 Options +		
ululu cisco	Saye C MONITOR WLANS CONTROLLER WIRELESS SECURITY MANA	onfiguration <u>P</u> ing GEMENT C <u>O</u> MMAN	Logout <u>R</u> efresh DS HE <u>L</u> P
WLANs	WLANs > Edit	< Back	Apply
- WLANS	General Security QoS Advanced		
WLANs AP Groups VLAN	Layer 2 Layer 3 AAA Servers		
	Layer 3 Security None Web Policy Authentication Passthrough Conditional Web Redirect AllowXpc 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						
G C + 102.168.4	.80/sc 🔎 🔹 🚱 🖉	р 🧭 Хр 🌜	Cisco 🧭 Xp.		🍯 40 🤇 🥶 C. 🗙	🔶 Co	☆☆ ☺
Ele Edit View Favorites	Iools Help						
🛛 🍰 🍠 WinInet Apps failing when	I 7N 802.1x - Cross Fo	orest Auth 💢 Co	nfiguring Certifica	te-Base 🔞 2	2011 Annual Conferen	ce Ex	**
X Find: 5.71		Previous N	iext 🛛 🥜 Optic	ns •			
ahaha					Save Configuration	n Ping Log	out   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	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> <ul> <li>Local EAP</li> <li>Priority Order</li> <li>Access Control Lists</li> </ul> </li> </ul>	Web Authenticati	ion Type	External (	Redirect to ext Production/	ternal server)		
<ul> <li>Wireless Protection Policies</li> <li>Trusted AP Policies</li> <li>Rogue Policies</li> <li>Standard Signatures</li> <li>Custom Signatures</li> <li>Signature Events</li> <li>Summary</li> </ul>						1	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. Select Redirect the User and click Next.
- 6. Select Use a new redirect and click Next. The Create Redirect page opens.

#### FIGURE 5 Create Redirect

Display Name:	Cisco WI AN Login
Display Hame.	CISCO WEAN EUGIN
) Description:	
Redirect URL:	\${switch_urf}? buttonClicked=4&redirect_url=https://credirect_website>/en
	roll/ <your_account>/Production/submit-redirect</your_account>
) Use POST:	
) POST Parameters:	[ex. username=bob]
Allow Continuation:	
Kill Session:	
Filters & Restriction	2

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	s] <b>*</b> +	1	≣	×	
•	Step 4:	Authenticate	the user via Fac	ebook Login			1	×	۲
	Result:	Move user to	Guest: Interne	t-only and assi	gn certificate using One	e-day guest templa	a		/

### **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

	68.4.80/screens/fra , 0 💌 49 / 65 tores		27. Chrix O. 403 Fo.	Corro X Corros	n +
ie Edit Vew Favorite	s Tools Help		1		
Wininet Acos falino v	hen L., 7N 802.1x - Cross Forest Auth	X Confrauring Centificate-Base	2011 Annual Conference Ex	2012 Annual Conference Ex	
Find: 5.71	Prev	ious Next 📝 Options •			
uluilu cisco	MONITOR WLANS CONTRO	ILLER WIRELESS SECU	S RITY MANAGEMENT COMM	Sage Configuration Ping Logos ANDS HELP	t i Befre
Vireless	Clients > Detail		1	< Back Link Test Rer	nove
Access Points	Client Properties		AP Properties		
<ul> <li>Access Points All APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>AP Configuration</li> <li>Mesh</li> <li>Rogues</li> <li>Clients</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>Country</li> <li>Timers</li> </ul>	MAC Address IP Address Client Type User Name Port Number Interface VLAN ID CCX Version E2E Version Mobility Role Mobility Role	00:23:14:ba:85:34 192.168.6.90 Regular 1 management 0 CCXv4 E2Ev1 Local N/A	AP Address 00:18:74:d3:a5:80 AP Name AP0018.ba75.a24e AP Type 802.11a WLAN Profile Sample Campus - Setu Status Associated Association ID 1 802.11 Authentication Open System Reason Code 0 Status Code 0 CF Pollable Not Implemented		
	Policy Manager State Hanagement Franke 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 O WEP Disable	
	EAP Type	N/A			100%

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			
😋 🕑 🗢 🧭 Fittp://192.16	68.4.80/screens/fra 🔎 🛃 🚱 Xpress	🧉 Osco 🔏	Storess 🥳 Citrix O 🎯 403 Fo 👔	🎯 Osco 🗙 📥 Comps 🕥 🏠 🕄
Ele Edit Yew Favorite	s Iools Help			
🚕 🍠 WinInet Apps failing w	hen I TN 802.1x - Cross Forest Auth	X Configuring Certifica	ke-Base 👩 2011 Annual Conference Ex	2012 Annual Conference Ex »
× Find: 5.71	Previ	ous Next 📝 Optic	ons •	
ululu cisco	MONITOR WLANS CONTRO	LLER WIRELESS	SECURITY MANAGEMENT COMM	Saye Configuration   Ping   Logout   Befresh ANDS   HELP
Wireless	Clients > Detail			< Back Link Test Remove
* Access Points All APs	<b>Client Properties</b>		AP Properties	
▼ Radios 802.11a/n 802.11b/g/n	MAC Address IP Address	00:23:14:ba:85:34 192.168.6.90	AP Address AP Name	00:18:74:d3:a5:80 AP0018.ba75.a24e
<ul> <li>AP Configuration</li> <li>Mesh</li> </ul>	Client Type User Name	Regular	AP Type WLAN Profile	802-11a Sample Campus - Setu
Rogues     Clients	Port Number Interface	1 management	Status Association ID	Associated
<ul> <li>802.11a/n</li> <li>802.11b/g/n</li> </ul>	VLAN ID CCX Version	0 CCXv4	802.11 Authentication Reason Code	Open System
Country Timers	E2E Version Mobility Role	E2Ev1 Local	Status Code CF Pollable	0 Not Implemented
	Mobility Peer ID Address	N/A	CE Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Not Implemented
	Management Frame Protection	NO	PBCC Channel Agility	Not Implemented Not Implemented
	Security Policy Completed	Yes N/A	Timeout WEP State	0 WEP Disable
	Encryption Cipher	None		~
	EAP Type	N/A		* 100% -