

Cloudpath Enrollment System

Configuring Cloudpath to Redirect Through a Cisco Wireless LAN Controller

Software Release 5.0

December 2016

Summary: This document describes the requirements for setting up web passthrough in your network, how to configure the Cisco WLC and Cloudpath for web passthrough, and how to test the configuration. **Document Type:** Configuration **Audience:** Network Administrator



Configuring Cloudpath to Redirect Through a Cisco Wireless LAN Controller

Software Release 5.0 December 2016

Copyright © 2016 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex[™], BeamFlex[™], MediaFlex[™], ChannelFly[™], and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

Configuring Cloudpath to Redirect Through a Cisco Wireless LAN Controller

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.





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 pre-authentication 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.

• • • • • • • • • • • • • • • • • • •	•.80/scre	ensjih arvese		SpressCo	XpressC	Osco 🦪	SpressC (A CI	oto: Onl 🧐 403 For	0 🙆 Cisco	× <u>•</u> 0	Jegm	0 12
Ele Edt Yew Favorites	Tools	Fielb										
Wininet Apps failing when	nI 7	¥ 802.1x - 0	Cross Forest Auth	Configuring Certifica	ite-Base 💔 20	11 Annual Conferen	oe Ex 💔 2012 A	nnual Conference Ex	TN Add Publishe	d Certificates	.t	
1 Find: 5.71			Previo	us Next 🛛 🍠 Opti	ons •							
uluulu cisco	MONT	TOR M	LANS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Saye C	onfiguration	i Eine I	Logout Befo
ecurity A	Acci	ess Con	ntrol Lists > Ed	it	63 - CA					< Back	Add	tew Rule
***	Gene	eral										
General	Acces	s List Nam	e AllowXp	c	Destination 1	D /Mark	Besteval	Saure Boat	Dart Boat	0679	Direction	
	1	Permit	0.0.0.0	/	192.168.5.71	/	Any	Any	Any	Any	Any	
Local Net Users MAC Filtering Disabled Clients	2	Permit	192.168.5.71 255.255.255.255	1	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	Απγ	•
Local EAP Priority Order	A	Permit	0.0.0.0	/	0.0.0.0	/	UDP	Any	DHCP Server	Any	Any	
Access Control Lists	2	Permit	0.0.0.0	/	0.0.0.0	/	TCP	Any	DHCP Client	Any	Any	
Access Control Lists CPU Access Control Lists	<u>6</u>	Permit	0.0.0.0	1	0.0.0.0	/	TCP	Any	DHCP Server	Any	Any	
IPSec Certs	2	Permit	0.0.0.0	/	0.0.0.0	/	UDP	DNS	Any	Any	Any	•
Wireless Protection Policies	.8	Permit	0.0.0.0	1	0.0.0.0	'	TCP	DHCP Server	Any	Any	Any	
Web Auth	2	Permit	0.0.0.0	1	0.0.0.0	/	TCP	DHCP Client	Any	Any	Any	
LIUS												100%

FIGURE 2. Set Up the Preauthentication ACL

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 pre-authentication 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 Exp	plorer	×
COO - 6 http://192.168.4	1.80/50 P 🛨 😏 🧭 Xp 🦉 Xp 🧭 Clsco 🧭 Xp 🔅 Cl 🧭 40 🦉 C. 🗙 🔺 Co 🕥 🏠 🏠	3
Ele Edit View Favorites	Icols Help	
😪 ダ WinInet Apps failing when	1 🍿 802.1x - Cross Forest Auth 💢 Configuring Certificate-Base 🕡 2011 Annual Conference Ex	>>
X Find: 5.71	Previous Next 🧳 Options -	
սիսիս	Save Configuration Ping Logout Refres	h
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit < Back Apply	~
▼ WLANs	General Security QoS Advanced	
WLANS AP Groups VI AN	Layer 2 Layer 3 AAA Servers	
	Layer 3 Security None	
	Web Policy Authentication	
	Passthrough	
	Conditional Web Redirect	
	AllowXpc	
	🗋 Email Input	
		~
		-
	5 100% ·	14

- 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.

Cisco - Windows Internet Exp	plorer							
😋 💽 🔻 🧭 http://192.168.4	4.80/so 🔎 🖅 🍘 xp 🧑 Xp 🦉 Clsco 🧭 xp 🔅 Ck 🧭 40 🦉 C. 🗙 🔺 Co 🕥 🕠	* 🕸						
Ele Edit View Favorites Iools Help								
🛛 🚖 🍠 WinInet Apps failing when	n I 🍿 802.1x - Cross Forest Auth 💢 Configuring Certificate-Base 🕡 2011 Annual Conference Ex	>>						
× Find: 5.71	Previous Next 📝 Options -							
սիսիս	Sage Configuration Ping Logout	Refresh						
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HE	P						
Security	Web Login Page Preview App	ply						
 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 Standard Signatures Custom Signatures Custom Signatures Signature Events Signature Events	Web Authentication Type External (Redirect to external server) URL https://test71.cloudpath.net/enroll/TestAccount/Production/							
Summary	*, 100*	% • //						

FIGURE 4. Configure Web Login Page

- 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

Create Redirect	Cancel < Back Save
Reference Information	
🖲 Name:	Cisco WLAN Login *
Description:	
🖲 Redirect URL:	<pre>\${switch_url}? buttonClicked=4&redirect_url=https://<redirect_website>/enroll/<your _account="">/Production/submit-redirect //</your></redirect_website></pre>
🖲 Use POST:	
POST Parameters:	[ex. username=bob]
Allow Continuation:	
• Kill Session:	
Filters & Restrictions	

- 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

Tip >>

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.

Tip >>

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 or 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.

Completed Enrollment Workflow with Redirect Step

Workflow Cis	co Passthrough View: Workflow Look & Feel Properties	×		
A workflow def display of mes Each item belo of row.	ines the sequence a user must go through to register and connect to the network. This includes the ssages to the user, the acceptance of use policies, and authentication of the user and/or device. w represent a step within the process. To add additional steps, click the insert arrow on the left side			
Step 1:	Require the user to accept the AUP Welcome Message and AUP	JXQ		
Step 2:	Redirect the user based on Cisco WLAN Login.	JXQ		
Step 3:	Split users by: X Guest Employees	ℓ ≡ × Q,		
Step 4:	Authenticate the user via LinkedIn, Facebook, or Gmail	JXQ		
Result:	Move user to Guest - Internet only and assign certificate using 1-day Guest Template.			

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.

Cisco - Windows Internet	Explorer 68.4.80/screens/fra 🔎 🖅 🌠 Xpree	s 🧭 Osco 🛛 🏉 Xpr	ess 🥳 Obrix O 🧭 403 Fo 👔	Gisco 🗙 💪 Compa	
Ele Edit View Favorite	s Iools Help when I IN 802.1x - Cross Forest Auth	X Configuring Certificate-Ba	se 🕡 2011 Annual Conference Ex	2012 Annual Conference Ex	39
× Find: 5.71	Pre	rious Next 📝 Options +			
	MONITOR WLANS CONTRO	DILLER WIRELESS SE	S CURITY MANAGEMENT COMM	Saye Configuration Ping ANDS HELP	Logout Befresh
Wireless	Clients > Detail			< Back Link Test	Remove
* Access Points	Client Properties		AP Properties		
All APs Radios 802.11k/n 802.11k/g/n * AP Configuration Mesh Rogues Clients 802.11a/n 802.11a/n 802.11a/n Country Timers	MAC Address IP Address Client Type User Name Port Number Interface VLAN ID CCX Version E2E Version Bobility Role Mobility Role Mobility Poer IP Address Policy Manager State	00:23:14:ba:85:34 192.168.6.90 Regular 1 management 0 CCKv4 E2Ev1 Local N/A WEBAUTH_REQD	AP Address AP Name AP Type WLAN Profile Status Association ID 802.11 Authentication Reason Code Status Code CF Poll Beounst Short Preamble	00:18:74:d3:a5:80 AP0018.ba75.a24e 802.11a Sample Campus - Setu Associated 1 Open System 0 0 Not Implemented Not Implemented	
	Planagement Frame Procection	NO	Pour	Not Implemented	
	Security Information Security Policy Completed Policy Type	No N/A	Timeout WEP State	0 WEP Disable	
	Encryption Cipher EAP Type	None N/A			V

FIGURE 6. Client Detail Before Redirect

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

Cisco - Windows Internet Ex	plorer				_IO ×
🕒 🕒 🔻 🥖 http://192.168.	A.80,'screens,i'ra 🔎 🔹 😏 💋 Xprese	🥖 Cisco 🥖 Xpress	Citrix O 🥝 403 Fo 🧷	🗿 Cisco 🗙 🔔 Compa	0 \$ 0
Ele Edit View Favorites	Icols Help				_
😪 🍠 WinInet Apps failing whe	n I TN 802.1x - Cross Forest Auth	X Configuring Certificate-Base	2011 Annual Conference Ex	2012 Annual Conference Ex	39
× Find: 5.71	Previ	ous Next 📝 Options 🕶			
uhuhu cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECUR	S ITY MANAGEMENT COMM	Saxe Configuration Ping ANDS HELP	Logout Befresh
Wireless	Clients > Detail			< Back Link Test	Remove
* Access Points	Client Properties		AP Properties		
all APS	MAC Address	00:23:14:ba:85:34	AP Address	00:18:74:d3:a5:80	
802.11a/n 802.11b/g/n	IP Address	192.168.6.90	AP Name	AP0018.ba75.a24e	
	Client Type	Regular	AP Type	802.11a	
Mesh	User Name		WLAN Profile	Sample Campus - Setu	
Rogues	Port Number	1	Status	Associated	
Clients	Interface	management	Association ID	1	
▶ 802.11a/n	VLAN ID	0	802.11 Authentication	Open System	
▶ 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 IP Address	N/A	CE Poll Request	Not Implemented	
	Policy Manager State	RUN	Short Preamble	Not Implemented	
5.	Management Frame Protection	NO	PBCC	Not Implemented	
	Convrity Information		Channel Agility	Not Implemented	
	Security Information		Timeout	0	
	Security Policy Completed	Yes	WEP State	WEP Disable	
	Policy Type	N/A			
	Encryption Cipher	None			~
	EAP Type	N/A			100% •

FIGURE 7. Client Detail After Redirect

9