

**RUCKUS**<sup>®</sup>

'india kus'

**Deployment Guide** 

Cloudpath Okta Integration using SAML 2.0 July 2021

RUCKUS®

## **Table of Contents**

TABLE OF CONTENTS	2
INTENDED AUDIENCE	3
OVERVIEW	4
Okta Configuration	4
SAML 2.0 Application	4
General Settings	5
Configure SAML	5
Feedback	8
Sign On Tab	8
Assignments Tab	10
Cloudpath Configuration	11
Authentication Server Configuration	11
Required SAML Information	11
SAML Attribute to Enrollment Mappings	12
SAML Options	12
Import X.509 Certificate to Cloudpath Truststore	13
SmartZone Configuration	14
WISPr/Captive Portal Walled Garden	14
User Experience	15



## **Intended Audience**

This document provides an overview of how to configure Ruckus products to support a Cloudpath SAML integration. Step-by-step procedures for configuration are demonstrated. Some knowledge of Cloudpath, SmartZone, Okta and SAML 2.0 is recommended.

This document is written for and intended for use by technical engineers with background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

## **Overview**

This document describes how to configure the Cloudpath Enrollment System to support a SAML 2.0 integration with the Okta Identity Platform. The document is broken into the following main categories

- Okta (v. 2021.07.0) Configuration
- Cloudpath (v. 5.8.5012) Configuration
- SmartZone (v. 6.0.0.0.1213) Configuration

### **Okta Configuration**

The Okta identity management platform has many features to provide access for a workforce or customer user base. This configuration will utilize the onboard Okta LDAP Interface populated with a local database of users to prove out the concept of SAML 2.0 integration with Cloudpath. User creation and additional Directory Integrations within Okta (Active Directory or external LDAP Directory) are beyond the scope of this document.

### **SAML 2.0 Application**

Currently there is no native Cloudpath SAML 2.0 application within the Okta app catalog, so this process will go over the creation of a custom application that can be used to connect to the Cloudpath Enrollment Server.

In the Okta administrator page, expand the Applications section and go to Applications and click on "Create App Integration".

okta		Q Search		
Dashboard	~			
Directory	~	Applications	i	
Applications	^	Your plan provid	les a limited n	umber of custom apps.
Applications		See the plan page for more in	nformation. Upgrade to th	e Enterprise Plan to get more apps and mor
Self Service		Create App Integration	Browse App Catalog	Assign Users to App More 🔻
Security	~			
Workflow	~	Q. Search		
Reports	~	STATUS	6	Okta Admin Console
Settings	~	ACTIVE	1	
		INACTIVE	0	

FIGURE 1 OKTA ADMIN UI

The new app integration configuration wizard will pop up. For Sign-in method, select SAML 2.0 and click Next.

Create a new app integration	î
Sign-in method	OIDC - OpenID Connect
Learn More 🖸	Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with
	the Okta Sign-In Widget.  SAML 2.0  XML-based open standard for SSO. Use if the Identity Provider for your





### **General Settings**

Enter a name for the application. Enter a logo (optional). Select any App visibility selections if required, (this example will not make any selections). Click Next.

<b>Create</b>	SAML	Integration
---------------	------	-------------

1 General Settings	2 Configure SAML	3 Feedback
1 General Settings		
App name	Cloudpath App 2	
App logo (optional) 💿	Cloudpath Enrollment System	
App visibility	Do not display application icon to users	
	Do not display application icon in the Okta Mobile a	арр
Cancel		Next

### FIGURE 3 GENERAL SETTINGS

#### **Configure SAML**

#### Section "A" SAML Settings → General

• Single Sign on URL - Cloudpath workflow URL plus "samlAssertionConsumer" (e.g.

<u>https://mycloudpath.mydomain.com/enroll/companyname/Workflowname/samlAssertionConsumer</u>) The Cloudpath workflow can be found in Cloudpath  $\rightarrow$  Configuration  $\rightarrow$  Workflows  $\rightarrow$  select the workflow that the OKTA SAML app will be used  $\rightarrow$  Advanced tab  $\rightarrow$  copy the Enrollment Portal URL.

- Check the "Use this for Recipient URL and Destination URL" box.
- Audience URI Fully Qualified Domain Name for the Cloudpath server. (e.g.
  - https://mycloudpath.mydomain.com)
- Default RelayState Leave blank
- Name ID format Unspecified
- Application username Okta username
- Leave advanced settings at their default

## **COMMSCOPE**<sup>®</sup>

**Cloudpath OKTA Integration using SAML 2.0** 

A SAML Settings	
General	
Single sign on URL 👔	https://mzpn-ob1.ruckusdemos.net/enroll/Mazapanlabs
	Use this for Recipient URL and Destination URL
	Allow this app to request other SSO URLs
Audience URI (SP Entity ID) 🛛	https://mzpn-ob1.ruckusdemos.net
Default RelayState 🛛 🕲	
	If no value is set, a blank RelayState is sent
Name ID format 🚳	Unspecified •
Application username	Okta username 🔹
	Show Advanced Settings

FIGURE 4 GENERAL SAML SETTINGS

### Attribute and Group Attribute Statements (optional)

When you create a new SAML integration, or modify an existing one, you can define custom attribute statements. These statements are inserted into the SAML assertions shared with your app.

This example will add the following Attributes (Group Attributes are not configured):

lame	Name format (optional)	_	Value	
first_name	Basic	•	user.firstName	•
last_name	Basic	•	user.lastName	•
department	Basic	•	user.department	•
email_address	Basic	•	user.email	•
city	Basic	•	user.city	•
state	Basic	•	user.state	•
country	Basic	•	user.countryCode	•
company	Basic	•	user.organization	•

FIGURE 5 ATTRIBUTE STATEMENTS. ORANGE = CLOUDPATH NAME MAPPINGS, BLUE = OKTA VALUES.

**RUCKUS**<sup>®</sup>

In section "B", you can click on the "Preview the SAMLAssertion" to verify the info that was previously entered.

B Preview the SAML assertion generated from the information above				
Preview the SAML Assertion				
This shows you the XML that will be used in the assertion - use it to verify the info you entered above				
Previous Cancel Next				

### FIGURE 6 PREVIEW THE SAML ASSERTION



### Click Next.



### Feedback

- Are you a customer or partner? check "I'm an Okta customer adding an Internal app"
- App type check the box for "This is an internal app the we have created"
- Click Finish



### FIGURE 8 FEEDBACK SETTINGS

### Sign On Tab

Click on "View Setup Instructions", this will open a browser tab with the following information:

- Identity Provider Single Sign-On URL Copy this to a text editor file
- Identity Provider Issuer Copy this to a text editor file
- X.509 Certificate click on Download certificate to save the file.
- Optional this example will not use the IdP metadata information but rather a URL link to reference the IdP metadata information.
- Close the browser tab.

Но	w to Configure SAML 2.0 for Cloudpath App 2 Application
The	e following is needed to configure Cloudpath App 2
1	Identity Provider Single Sign-On URL:
	https://dev-: .okta.com/app/dev-14851062_cloudpathapp2_1 /sso/saml
2	Identity Provider Issuer:
	http://www.okta.com/

### FIGURE 9 IDP SSO URL/ISSUER INFORMATION

3	X.509 Certificate:
100	rabos dor anoucor

END CERTIFICATE			
Download certificate			
nal			

### FIGURE 10 X.509 CERTIFICATE

Back in the Sign on tab, click on the "Identity Provider metadata" link to open a new browser tab with the IdP Metadata. Copy this URL to a text editor file. Close the browser tab.



FIGURE 11 IDP METADATA

Sign On Policies are not configured for this example.

RUCKUS®



~

Done

### **Assignments Tab**

Assign the application to specific people or groups. This example will assign to specific users.

Click on Assign  $\rightarrow$  Assign to People  $\rightarrow$  search for or select the displayed users that require this app and click "Assign". Click Done to finish.

Cloudpath App 2				
General Sign On Mobile	Import Ass	ignments		
Assign V Convert assign	nments 🔻	Q Search	People <b>v</b>	
Fi Assign to People		Туре		
Pe Assign to Groups Groups		01101110		

FIGURE 12 ASSIGN TO PEOPLE

Assign Cloudpath App 2 to People ×				
Q Search				
mario perea mario.perea@.com	Assign			
Zeppo Perea zeppo@i .com	Assign			
Groucho Perea groucho@i com	Assign			
Luke Perea luke@com	Assign			
Tito Perea tito@com	Assign			

FIGURE 13 LIST OF USERS

### **Cloudpath Configuration**

In order to integrate Okta as a SAML 2.0 Identity Provider on Cloudpath, it needs to be added as an Authentication Server, then included as a step in a Cloudpath workflow. This example will use a simple Certificate (EAP-TLS) based enrollment workflow to illustrate the use of the Okta SAML authentication server. This document will not cover creating all workflow steps. Workflow basics can be referred to here.

To create an Authentication Server, go to Configuration  $\rightarrow$  Authentication Servers  $\rightarrow$  and click on Add Server

COMMSCOPE" RUCKUS "	Cloudpath Enrollment System		2	<u>ل</u>
Dashboard	Configuration	> Authentication Servers	Add Ser	ver 🕨
Workflows	> Server 1:	SAML Identity Provider (IdP) OKTA PROD SAML 1	0	1
Device Configurations	> Server 2:	Active Directory server Lab20 AD DC1	⊘	1
RADIUS Server	> Server 3:	Onboard database Mazapanlabs Inc. DB		1
Passpoint OSU	> Server 4:	Active Directory server mzpn-dc2	۲	1
Authentication Servers	> Server 5:	Active Directory server Wagstaff Domain	⊘	1

FIGURE 14 ADD AUTHENTICATION SERVER

In the Authentication Server Configuration page, select "Connect to SAML".

### **Authentication Server Configuration**

### **Required SAML Information**

- IdP Metadata Type URL
- IdP Metadata URL paste the Identity Provider Metadata URL link that was copied previously (Figure 11 IdP Metadata)
- IdP EntityID paste the Identity Provider Issuer information that was copied previously (Figure 9)
- SP EntityID enter the FQDN of the Cloudpath Server (e.g. https://mycloudpath.mydomain.com)

Connect to SAML		
Select this option to enable end-users to aut	thenticate via a SAML 2.0 IdP.	
Density & CANULE formation		
Required SAML Information		
i IdD Metdata Type		
	URL V	
i IdP Metadata URL	https://devokta.com/app/e	*
i IdP EntityID	http://www.okta.com/	*
SD EntitudD	https://www.chd.austur.downe.cot	
SP EnutyID	https://mzpn-ob1.ruckusdemos.net	*





### SAML Attribute to Enrollment Mappings

The following attributes are used to map to the Okta app

Attribute Mapping Templates: edu	IPerson InCommon inetOrgPerson/X.500 Generic Blank
(i) Username Attribute	username
(i) Common Name Attribute	[ex. eduPersonPrincipalName]
(i) Affiliation/Group Attribute	[ex. eduPersonAffiliation]
i Email Attribute	email_address
(i) First Name Attribute	first_name
(i) Last Name Attribute	last_name
(i) City Attribute	city
(i) State Attribute	state
(i) Country Attribute	country
(i) OU Attribute	
(i) Distinguished Name Attribute	[ex. cn]
(i) Company Attribute	company
(i) Department Attribute	department
(i) Office Name Attribute	

FIGURE 16 SAML ATTRIBUTE TO ENROLLMENT MAPPINGS

### **SAML Options**

Set AuthN Context Comparison to "exact" in the drop down menu. Leave the other settings at their default.

SAML Options	
IdP \$\$O Binding Type	HTTP Redirect 💙
Assertion Consumer Type	HTTP POST 🗸
AuthN Requests Signed	✓
AuthN Context Comparison	exact 🗸
Socket Timeout (ms.)	exact
	minimum
/LAN Configuration	maximum
Use VLAN Range:	better

#### FIGURE 17 SAML OPTIONS

Check the "Test IdP Connection box and click Save to test the connection to the Okta SAML app.

A banner with a Success message should appear at the top of the browser. (Figure 18)

3 SAML IdP Connection Test Successful. Clear 'Test IdP Connection' checkbox and save again to continue.

FIGURE 18 IDP CONNECTION TEST SUCCESS MESSAGE

In the Test Results section, you should see the output and a success message as well.

Test Connection	
Test IdP Connection	Basic connectivity with specified SAML IdP *SUCCESSFUL* - See output below - To continue, clear this checkbox and save again.
Test Results:	Starting JFVU Request: /admin/advanced/authenticationServers/9/submit Will select authentication server type Will select authentication server Will save Authentication server if possible Original SCV style: null Will authenticate via external credentials. No group regex patterns exist at all. Will authenticate via SAML. Cleared IdP metadata cache for account prior to admin UI initiated connection test. Attempting to get CpnSamiForAuthServer, scv: BLOCK Will retrieve IdP metadata cache for account prior to admin UI initiated connection test. Attempting to get CpnSamiForAuthServer, scv: BLOCK Will retrieve IdP metadata via HTTP from https://dev- /sso/sami/metadata for IdP EntityID http://www.okta.com/ Will retly on Account or System Truststore for IdP metadata HTTPS trust. IdP Metadata successfully retrieved/parsed; AuthN destination is: https://dev- 

#### FIGURE 19 IDP CONNECTION TEST RESULTS

### Import X.509 Certificate to Cloudpath Truststore

In order for Cloudpath to trust communication from Okta, a "Pinned" certificate is required to be added to the Cloudpath Truststore. Use the certificate file that was previously downloaded (Figure 10).

To add the certificate, go to Configuration  $\rightarrow$  Truststore  $\rightarrow$  click "Add"

Configuratio	on > Truststore	
Trusted CAs	Server Status	
Trusted (	CAs & Pinned Certificates	Add
The follo	wing list of certificate authorities and pinned server certificates will be trusted for communications from this server to external servers. This	list should be populated
with CA(	(s) used by the external systems to which this system communicates. For example, if a notification is configured to be sent to https://api.systems.com/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.systems/api.sys	stem.com, the CA for the
web serv	ver certificate on api.system.com should be added to the list below.	

FIGURE 20 ADD PINNED CERTIFICATE

**RUCKUS**<sup>®</sup>

## Upload the certificate and go to the Server Status tab to verify.

Trusted CAs Server Status						
V System: 🕑 dev-	.okta.	com:443				
Name: de	ev-14851062.okta.cor	m:443				
Type(s): S	AML					
Resolved IP: 4	4.234.52.10					
Status:	Verified.					
Certificate Chain:	Server Certificate:	*.okta.com	1011 1011	20220502	DigiCert TLS RSA SHA256 2020 CA1	Sent by server.
	Intermediate CA:	DigiCert TLS RSA SHA256 2020 CA1		20300923	DigiCert Global Root CA	Sent by server.

FIGURE 21 SERVER STATUS TAB

Go back to Configuration → Workflows and **add the necessary steps** to build a workflow using the new OKTA SAML Authentication Server. Publish the workflow.

•	Production		Published	> /enroll/MazapanlabsInc/Production/
Properties	Enrollment Process	Look & Feel Snapshot(s)	Advanced	
+				
ę	Step 1: Require the	s user to accept the AUP MZPN AU	IP	
⇒				
ę	Step 2: All matches	S IN: MZPN AD OKTA PROD SAML 1	X 💉 OTKA SAML 2.0	+
+				
5	Step 3: Prompt the	e user for credentials from OKTA S	SAML 2.0	
+				
F	Result: Move user	to OKTA Dev Config and assign c	ertificate using <b>username@</b>	ĝokta.mazapa

### FIGURE 22 WORKFLOW

### SmartZone Configuration

### Hotspot (WISPr) Walled Garden Entries

To allow access to the Okta sign-in page during enrollment, two "Walled Garden" entries are required in the Hotspot (WISPr) captive portal that is used for the Onboarding WLAN. This example utilizes the Virtual SmartZone Essentials controller and steps will be shown for that WLAN controller.

In SmartZone go to Services  $\rightarrow$  Hotspots & Portals  $\rightarrow$  Hotspot (WISPr)

*	🛃 Monitor	🛔 Network	Security	<b>¢</b> ₿ Services	Administration	*
	Hotspots & Po	ortals	Tunnels &	Ports	DHCP & NAT	
Gu	lest Access		Ruckus GRE		DHCP Setting (AP)	
Ho	otspot (WISPr)		SoftGRE		DHCP Pools (AP)	
Ho	otspot 2.0		IPsec		DHCP Profiles (DP)	

### FIGURE 23 HOTSPOT (WISPR)

Select the Hotspot WISPr entry that is used for the Onboarding WLAN, click Configure.

In the Edit Hotspot Service menu, expand the Walled Garden / Traffic Class Profile section.

Walled Garde	en / Traffic Class Profile	▼
Walled Garden	* Walled Garden Entry + Add Import CSV V Cancel 🗊 Delete	
	Walled Garden Entry 🔺	
	*.1e100.net	
	*.apple.com	
	*.okta.com	
	*.oktacdn.com	



Add the following entries

- \*.okta.com
- \*.oktacdn.com

Click OK.

### **User Experience**

Users should see the SAML workflow step during enrollment.



FIGURE 25 IOS USER ENROLLMENT

The Okta login page should appear and when the user's credentials are entered correctly, the user will be passed onto the next workflow step.

2:35		
e dev-	.okta.com	۵
Connect Sign-in with your okta C	a-dev- a-dev- loudpath App 2	an S <mark>istem</mark> unt to access
	okta	
	Sign In	
Username		
luke@	kcom	
Password		
*******		
Remember m	e	
Need help signing	in?	
$\leftarrow \rightarrow$	+ 16	

### FIGURE 26 OKTA LOGIN PAGE

In this case, the next step is to download the iOS mobile configuration profile and follow the on-screen steps.



FIGURE 27 IOS MOBILE CONFIG PROFILE INSTALLATION PAGE

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT



# RUCKUS®

#### commscope.com

Visit our website or contact your local CommScope representative for more information.

© 2021 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by <sup>®</sup> or <sup>™</sup> are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO9001, TL9000, ISO14001 and ISO45001. Further information regarding CommScope's commitment can be found at www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability.