COMMSCOPE®

RUCKUS®

Deployment Guide

Cloudpath Okta Integration using SAML 2.0

July 2021

Table of Contents

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”.

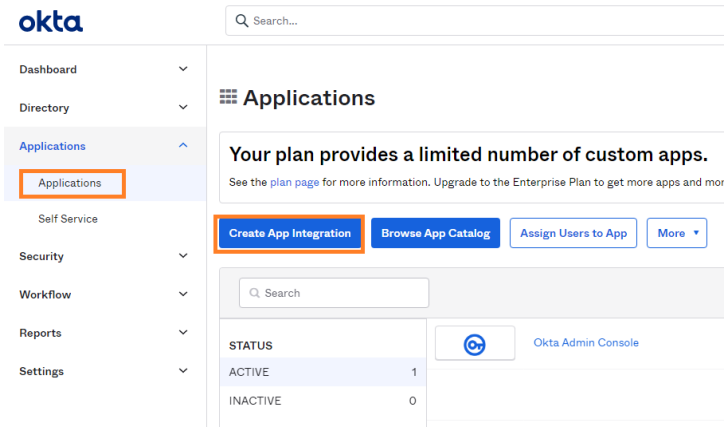

FIGURE 1 OKTA ADMIN UI

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

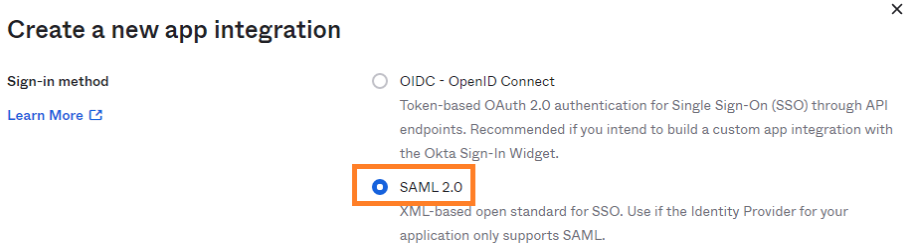

FIGURE 2 NEW APP INTEGRATION

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.

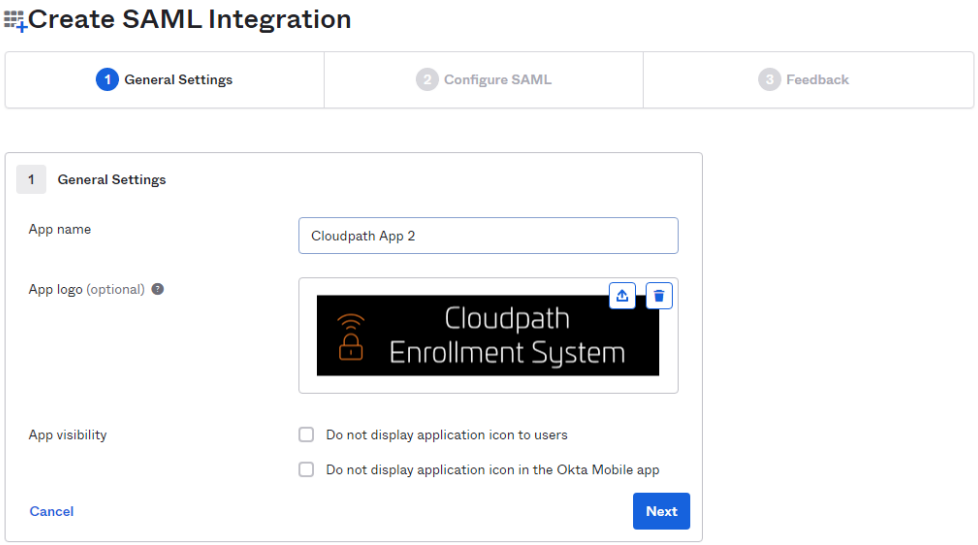

FIGURE 3 GENERAL SETTINGS

Configure SAML

Section "A" SAML Settings → General

- Single Sign on URL - Cloudpath workflow URL plus "samlAssertionConsumer" (e.g. https://mycloudpath.mydomain.com/enroll/companyname/Workflowname/samlAssertionConsumer) The Cloudpath workflow can be found in Cloudpath → Configuration → Workflows → select the workflow that the OKTA SAML app will be used → Advanced tab → 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

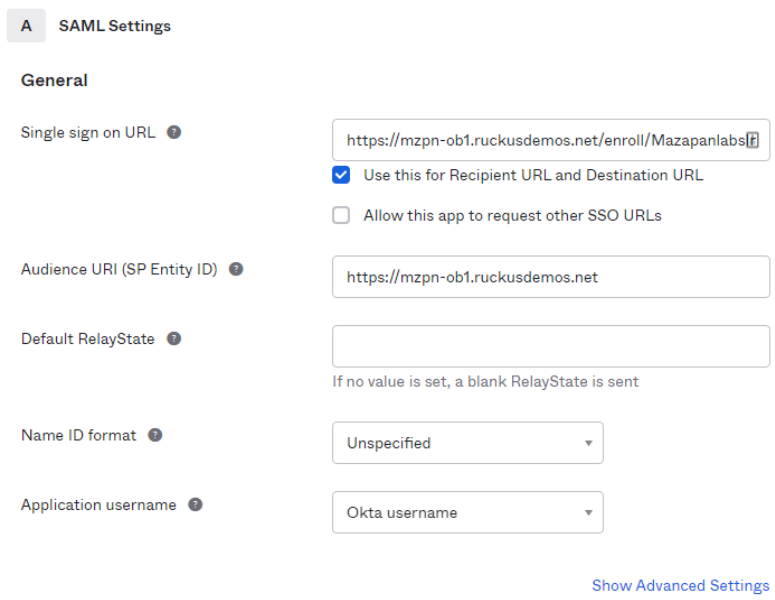

FIGURE 4 GENERAL SAML SETTINGS

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):

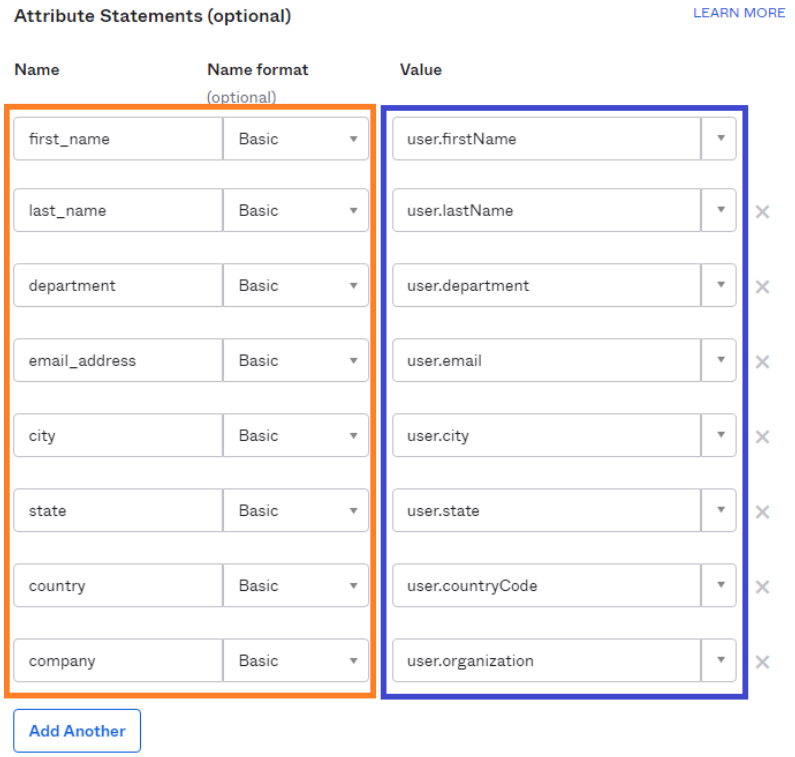

FIGURE 5 ATTRIBUTE STATEMENTS. ORANGE = CLOUDPATH NAME MAPPINGS, BLUE = OKTA VALUES.

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

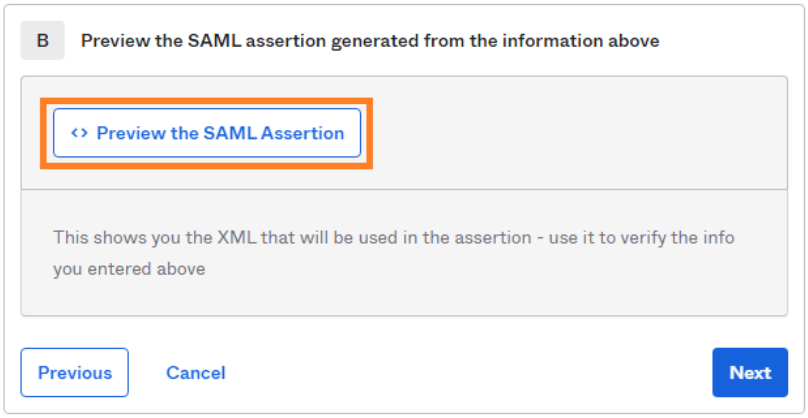

FIGURE 6 PREVIEW THE SAML ASSERTION

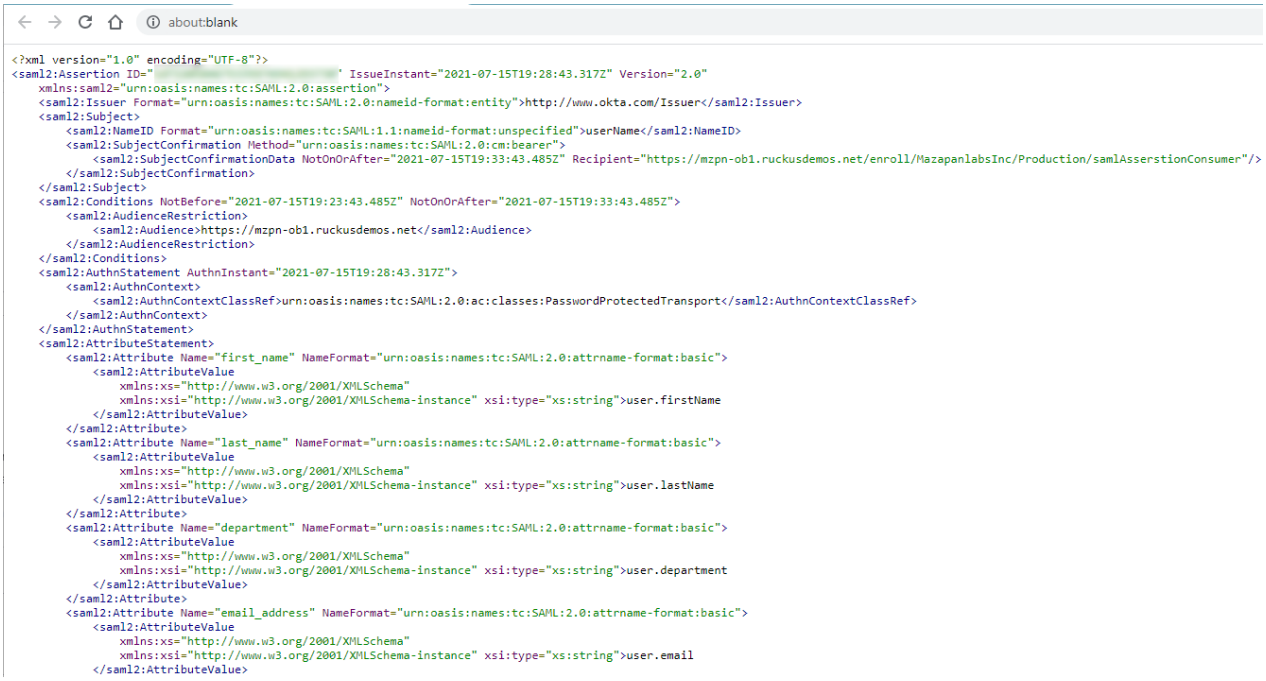

FIGURE 7 SAML ASSERTION XML OUTPUT

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

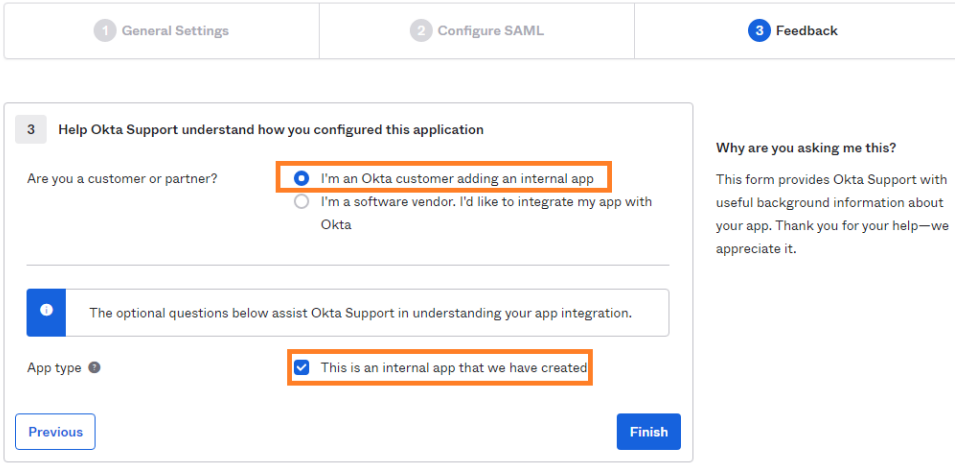

FIGURE 8 FEEDBACK SETTINGS

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.

FIGURE 9 IDP SSO URL/ISSUER INFORMATION

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.

Assignments Tab

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

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

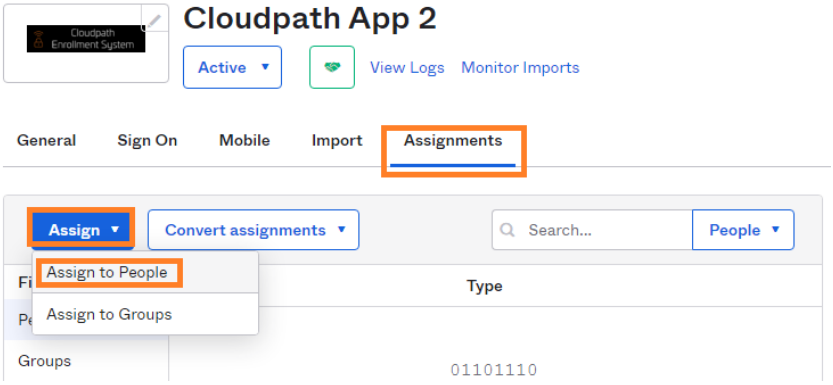

FIGURE 12 ASSIGN TO PEOPLE

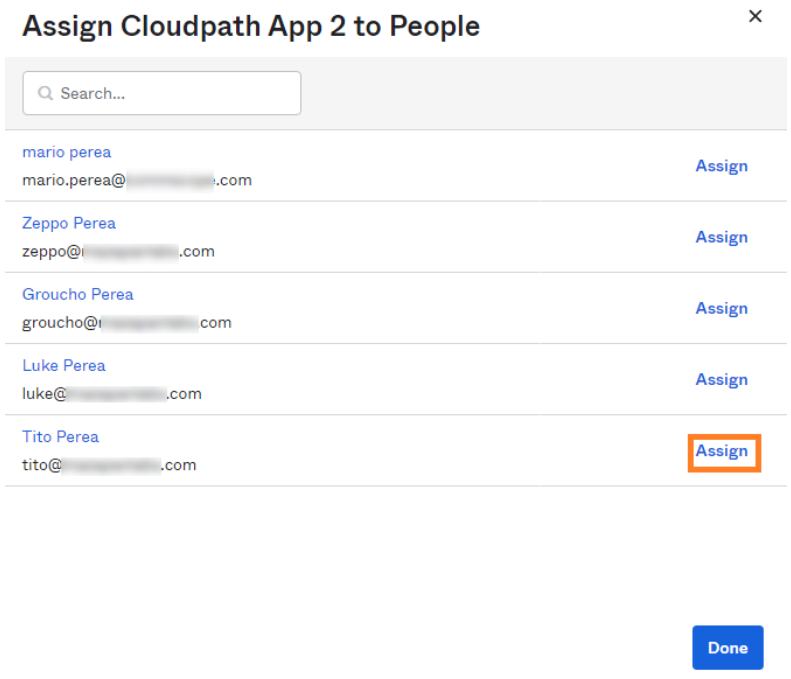

FIGURE 13 LIST OF USERS

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 → Authentication Servers → and click on Add Server

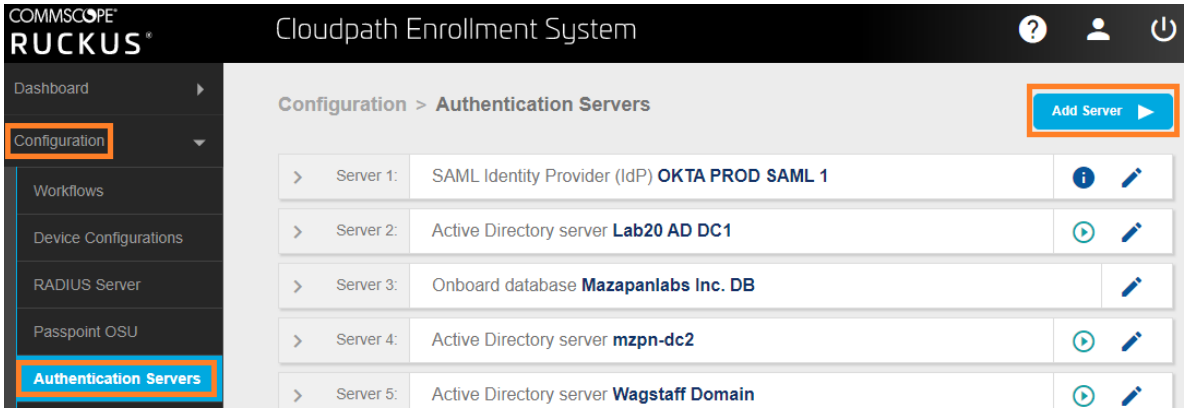

FIGURE 14 ADD AUTHENTICATION SERVER

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)

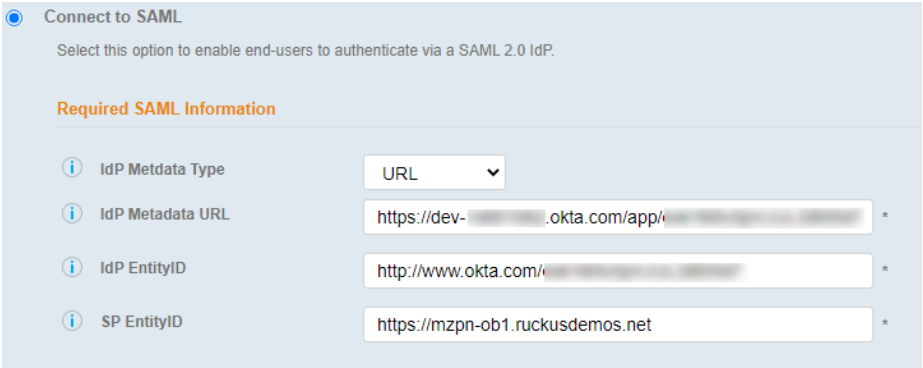

FIGURE 15 REQUIRED SAML INFORMATION

SAML Attribute to Enrollment Mappings

The following attributes are used to map to the Okta app

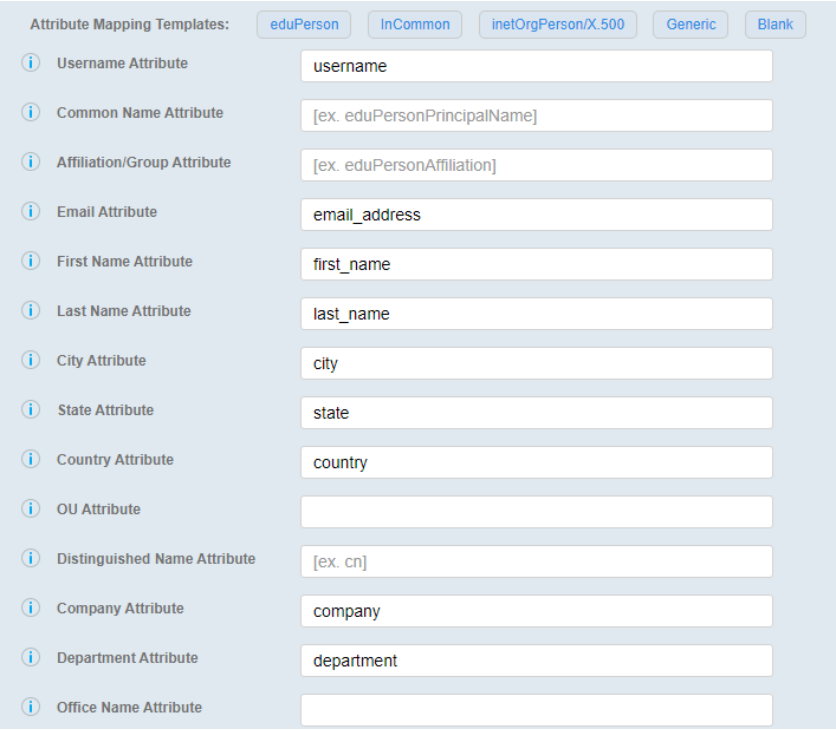

FIGURE 16 SAML ATTRIBUTE TO ENROLLMENT MAPPINGS

SAML Options

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

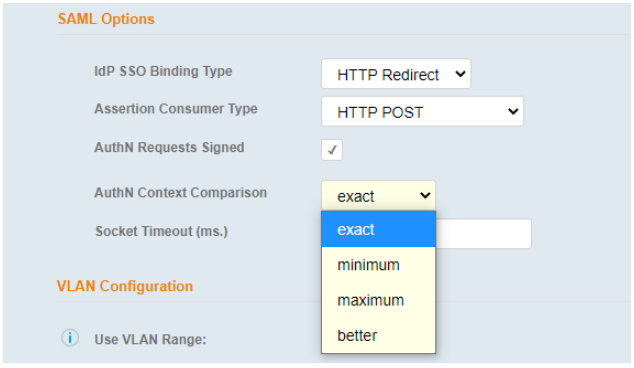

FIGURE 17 SAML OPTIONS

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)

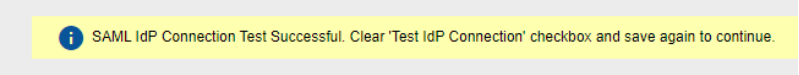

FIGURE 18 IDP CONNECTION TEST SUCCESS MESSAGE

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

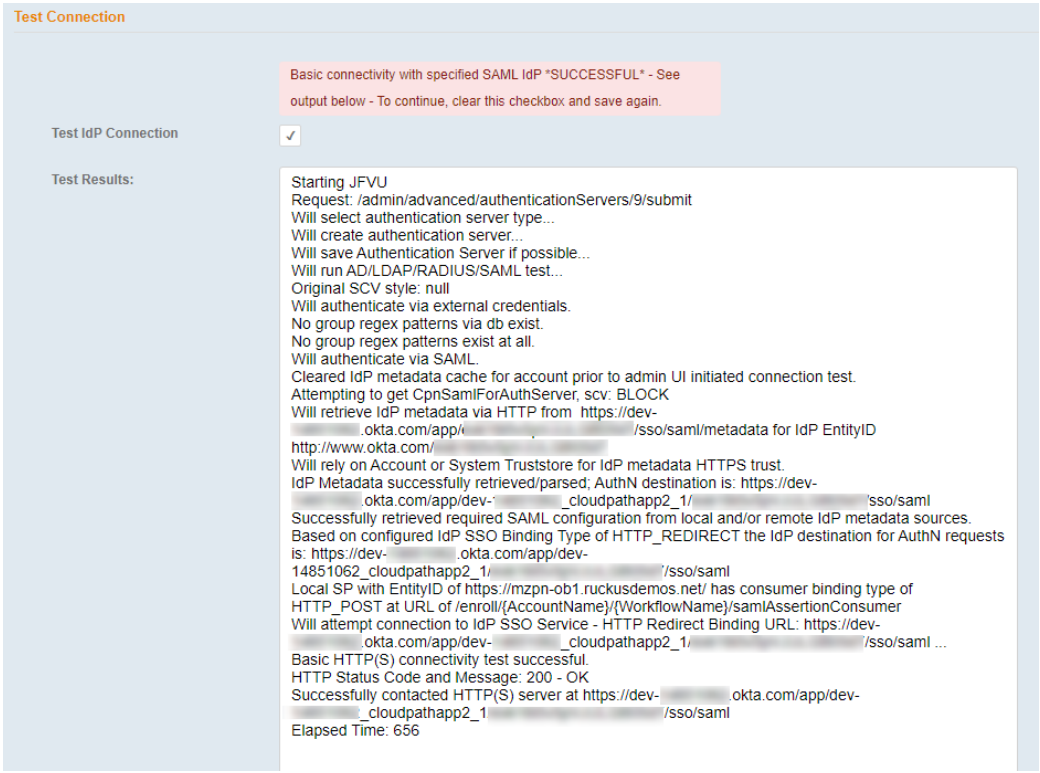

FIGURE 19 IDP CONNECTION TEST RESULTS

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 → Truststore →click "Add"

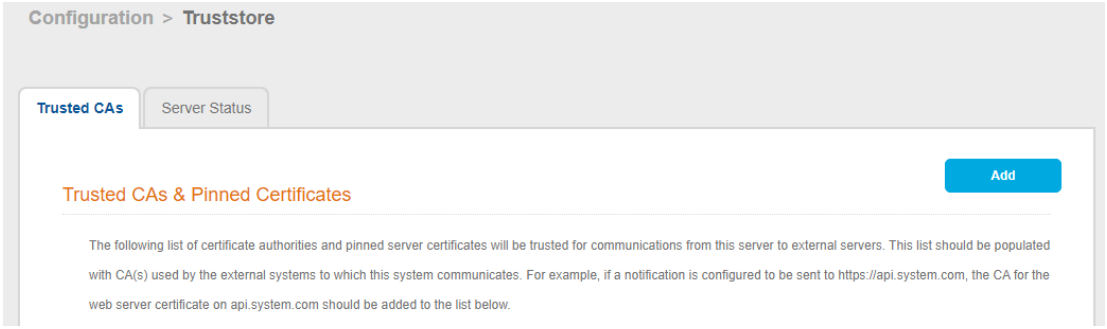

FIGURE 20 ADD PINNED CERTIFICATE

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

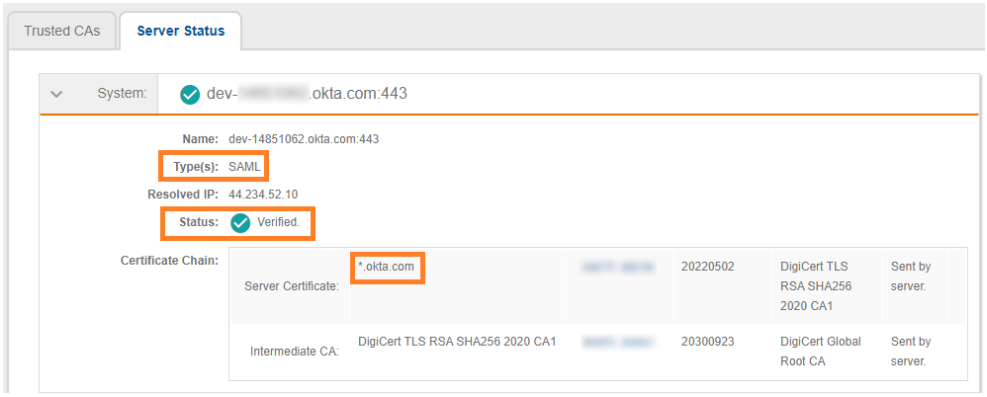

FIGURE 21 SERVER STATUS TAB

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

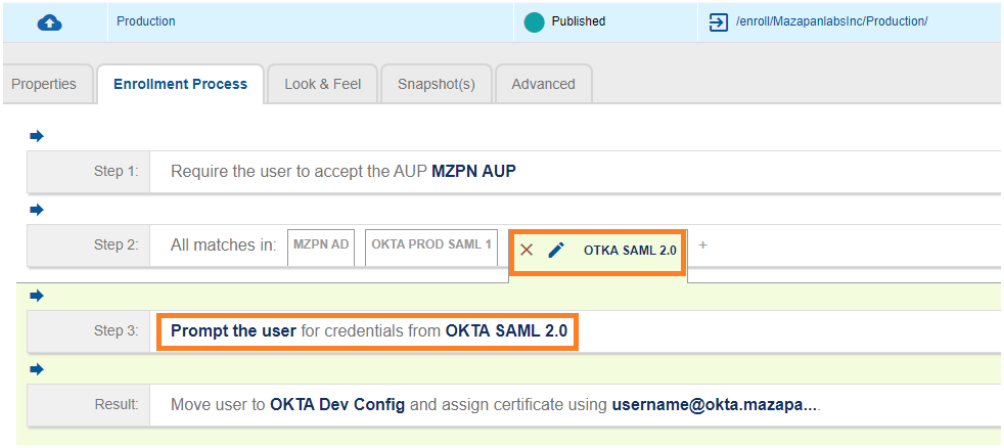

FIGURE 22 WORKFLOW

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 → Hotspots & Portals → Hotspot (WISPr)

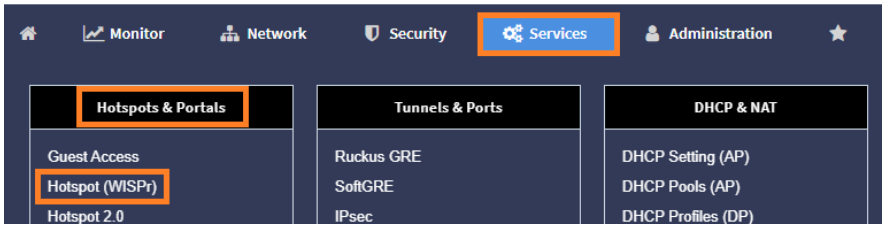

FIGURE 23 HOTSPOT (WISPR)

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.

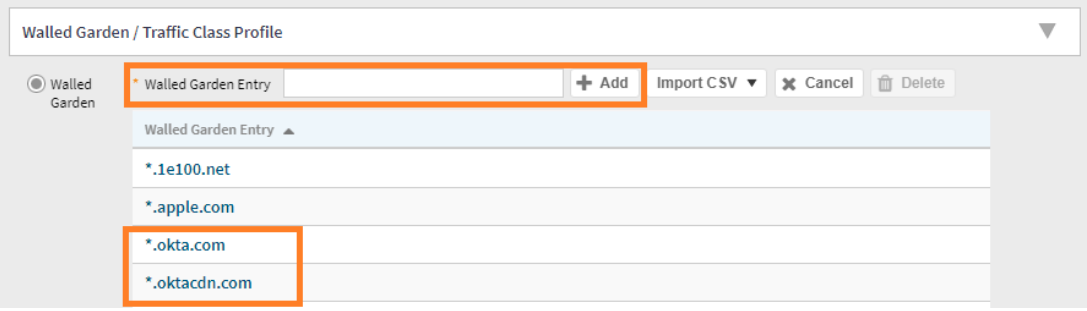

FIGURE 24 WALLED GARDEN ENTRY IN HOTSPOT (WISPR)

Add the following entries

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

Click OK.

User Experience

Users should see the SAML workflow step during enrollment.

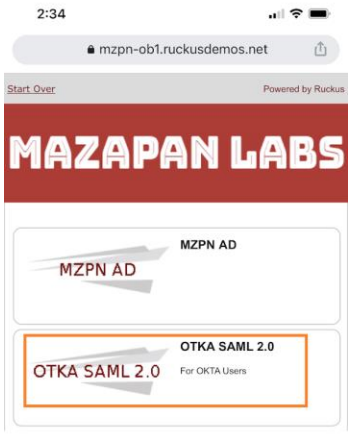

FIGURE 25 IOS USER ENROLLMENT

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.

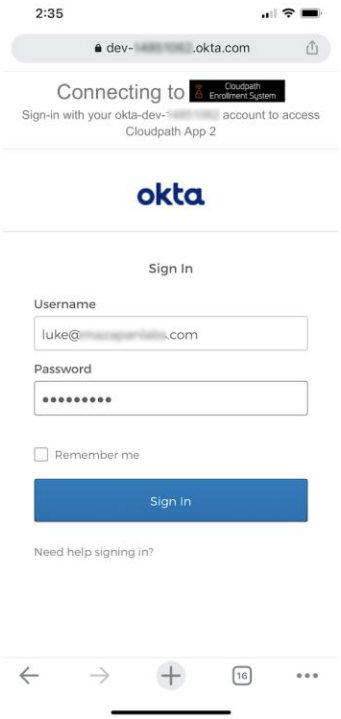

FIGURE 26 OKTA LOGIN PAGE

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

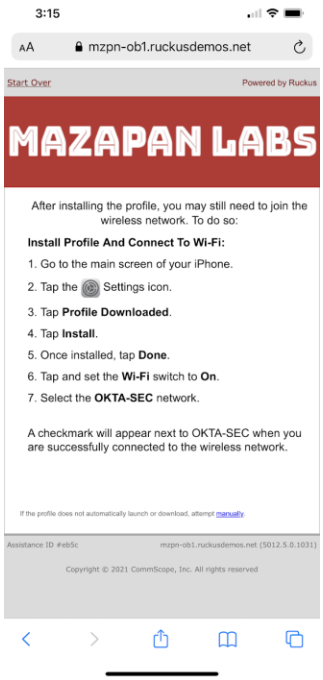

FIGURE 27 IOS MOBILE CONFIG PROFILE INSTALLATION PAGE

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

COMMSCOPE®

RUCKUS®

commscope.com

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