8/4/2021 – Will Smith CSE (Version 1.4)

Aruba Central – SAML SSO Okta Integration Guide

WILL.SMITH@HPE.COM

Configure SAML SSO Integration with Okta IdP

This procedure describes the steps required for configuring service provider metadata in Okta.

NOTE

This topic provides a basic set of guidelines required to configure SSO using the Okta service. The images and attributes may change with Okta software updates.

Before you Begin

Go through the SAML SSO feature description to understand how SAML framework works in the context of Aruba Central.

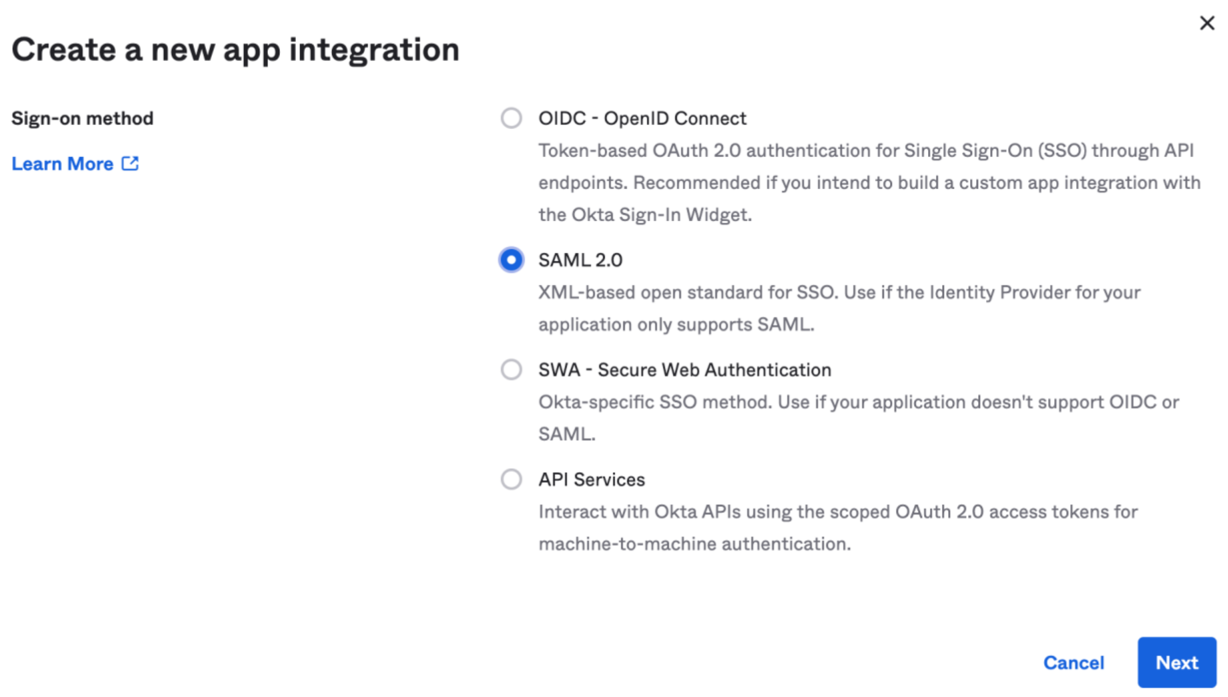
Steps to Configure SSO/SAML Application in Okta

To configure application metadata in Okta, complete the following steps:

- Step 1: Create an Okta SAML application
- Step 2: Configure Sign On settings
- Step 3: Export the SAML 2.0 IdP metadata
- Step 4: Create SAML Authorization Profile in Aruba Central

Step 1: Create an Okta SAML Application

1. Log in to the Okta administration console.
2. Click **Applications > Create App Integration.** The Create a new app integration window opens.
3. Select SAML 2.0 and click Next.



Create a new app integration

Sign-on method

Learn More

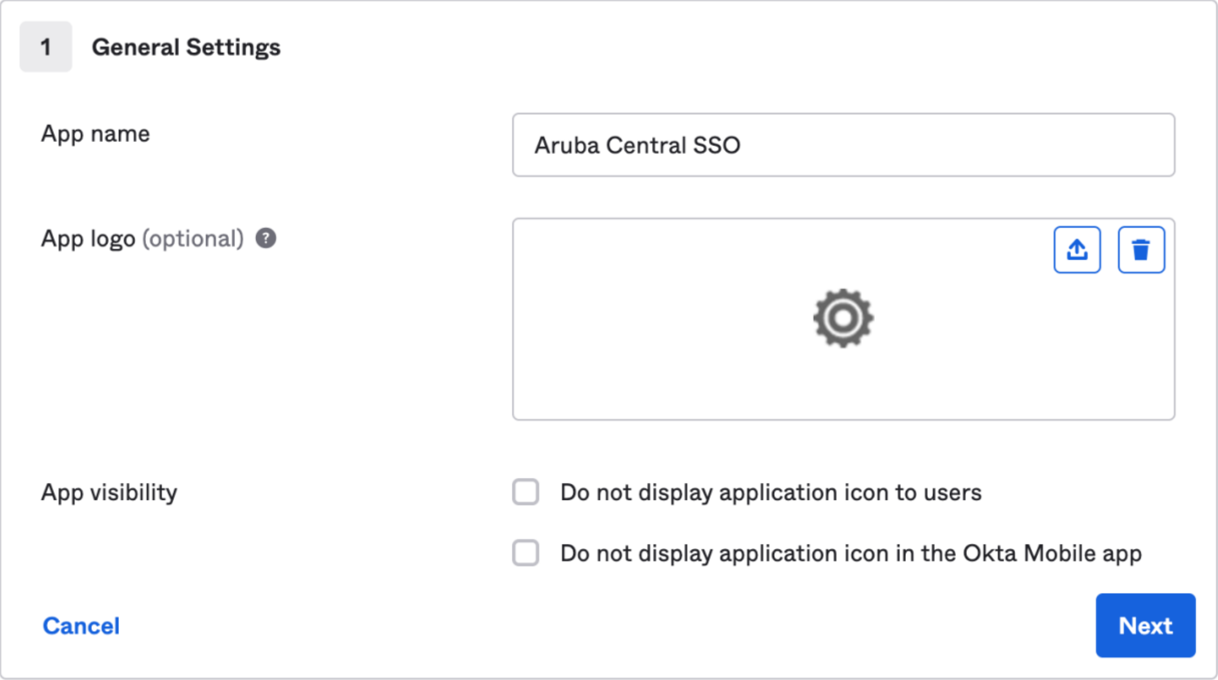
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

4. Provide a name for the Aruba Central SSO service (Okta Application)



1 General Settings

App name: Aruba Central SSO

App logo (optional)

App visibility

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

Step 2: Configure Single Sign On settings

1. Enter the SAML information.

Under General **> Single Sign on URL** configure the URL based on your cluster and add your **Domain Name**:

US-1: https://portal.central.arubanetworks.com/global_login/aaa_saml/**<<Domain Name>>?**acs
US-2: https://portal-prod2.central.arubanetworks.com/global_login/aaa_saml/**<<Domain Name>>?**acs
US-WEST-4: https://portal-uswest4.central.arubanetworks.com/global_login/aaa_saml/**<<Domain Name>>?**acs
China-1: https://portal.central.arubanetworks.com.cn/global_login/aaa_saml/**<<Domain Name>>?**acs
Canada-1: https://portal-ca.central.arubanetworks.com/ global_login/aaa_saml/**<<Domain Name>>?**acs
EU-1: https://portal-eu.central.arubanetworks.com/ global_login/aaa_saml/**<<Domain Name>>?**acs
APAC-1: https://portal-apac.central.arubanetworks.com/ global_login/aaa_saml/**<<Domain Name>>?**acs
APAC-EAST1: https://portal-apaceast.central.arubanetworks.com/ global_login/aaa_saml/**<<Domain Name>>?**acs
APAC-SOUTH1: https://portal-apacsouth.central.arubanetworks.com/ global_login/aaa_saml/**<<Domain Name>>?**acs

Example US-2: https://portal-prod2.central.arubanetworks.com/global_login/aaa_saml/customerxyz.com?acs

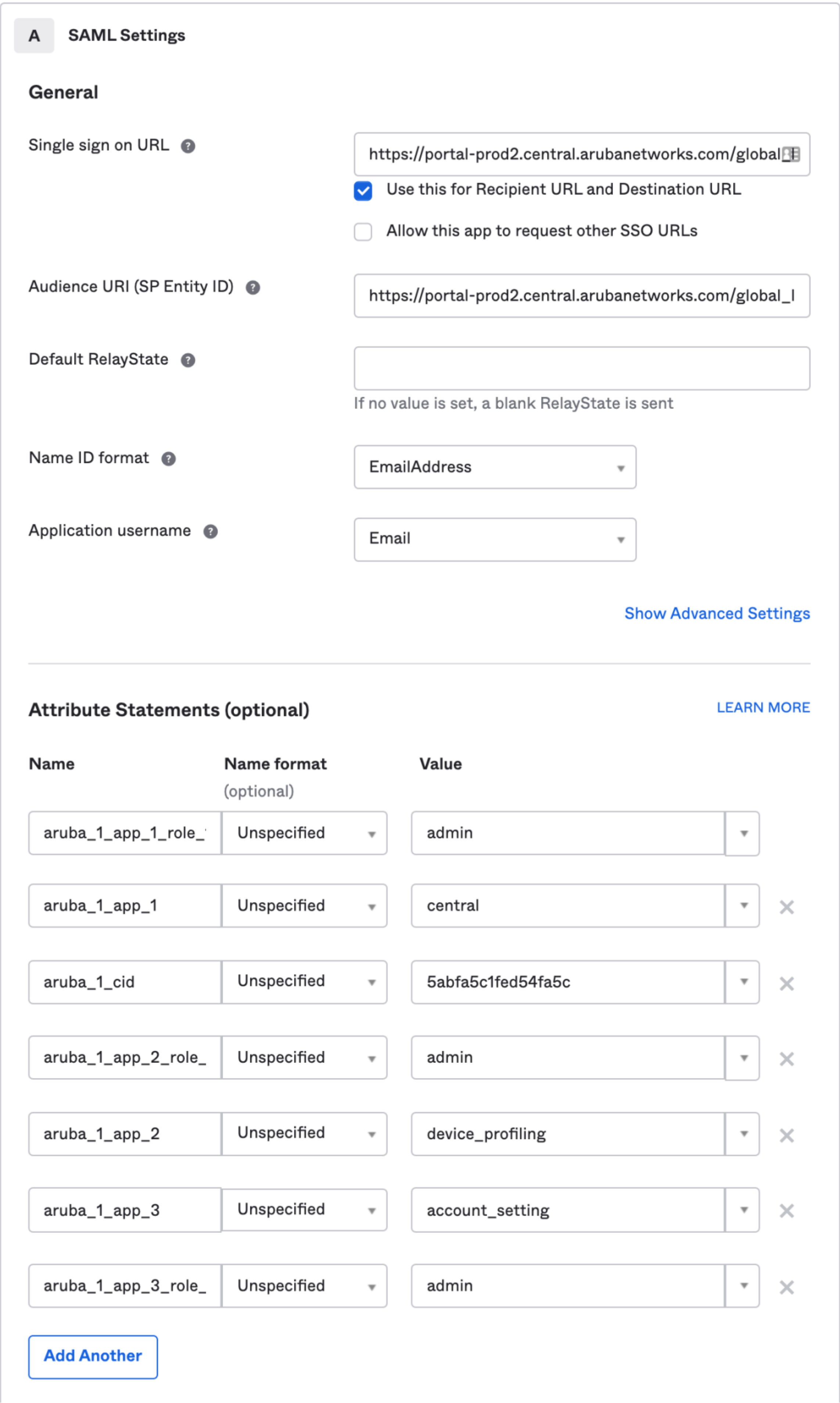
Audience URI (SP Entity ID) set to the same URL as above (**Single Sign on URL**)

Name ID format EmailAddress
Application username Email

Attributes Statement
-For the purpose of this guide, the values are **static**. Depending on the customer most likely these values will be dynamic as this will control what access to services (read/write) each user will be granted. *End of the documents I've provided an example of a dynamic lookup of the central role using attributes from the Okta user profile.*

aruba_1_cid = <customer-id>
# app1, scope1
aruba_1_app_1 = central
aruba_1_app_1_role_1 = <readonly>
aruba_1_app_1_group_1 = groupx, groupy
aruba_1_app_2 = device_profiling
aruba_1_app_2_role_1 = <readonly>
aruba_1_app_3 = account_setting
aruba_1_app_3_role_1 = <readonly>

See here for IdP attribute details: **https://help.central.arubanetworks.com/2.5.3/documentation/online_help/content/nms/user-mgmt/conf-idp-attributes.htm**



A **SAML Settings**

General

Single sign on URL ?
https://portal-prod2.central.arubanetworks.com/global

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?
https://portal-prod2.central.arubanetworks.com/global_l

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ? EmailAddress ▾

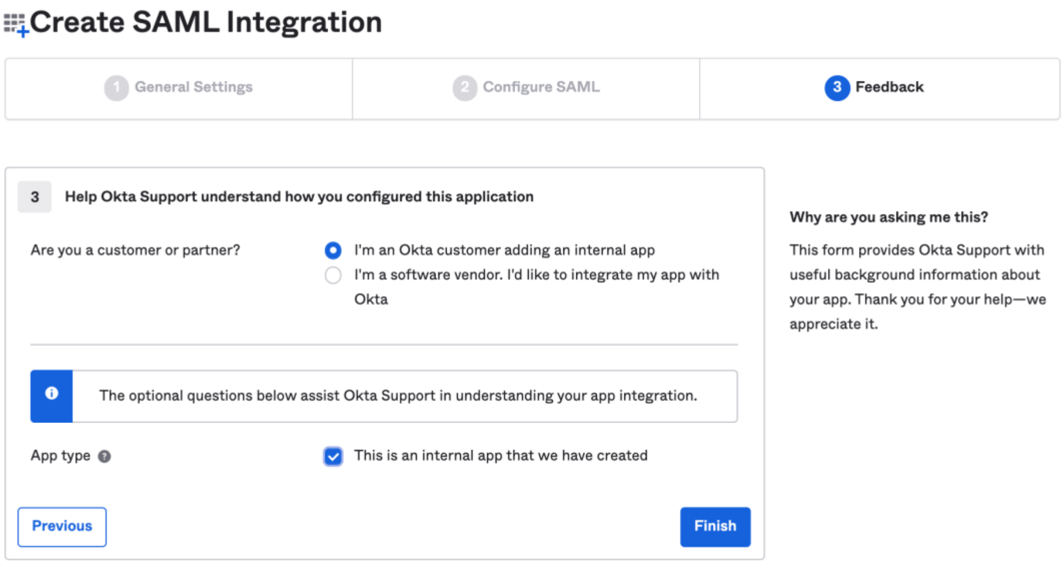
Application username ? Email ▾

Attribute Statements (optional)

Name	Name format (optional)	Value
aruba_1_app_1_role_	Unspecified ▾	admin ▾
aruba_1_app_1	Unspecified ▾	central ▾
aruba_1_cid	Unspecified ▾	5abfa5c1fed54fa5c ▾
aruba_1_app_2_role_	Unspecified ▾	admin ▾
aruba_1_app_2	Unspecified ▾	device_profiling ▾
aruba_1_app_3	Unspecified ▾	account_setting ▾
aruba_1_app_3_role_	Unspecified ▾	admin ▾

2. Complete the setup.

Click Next and Select “Internal App” then Finish



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?
● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type
☑ This is an internal app that we have created

Why are you asking me this?

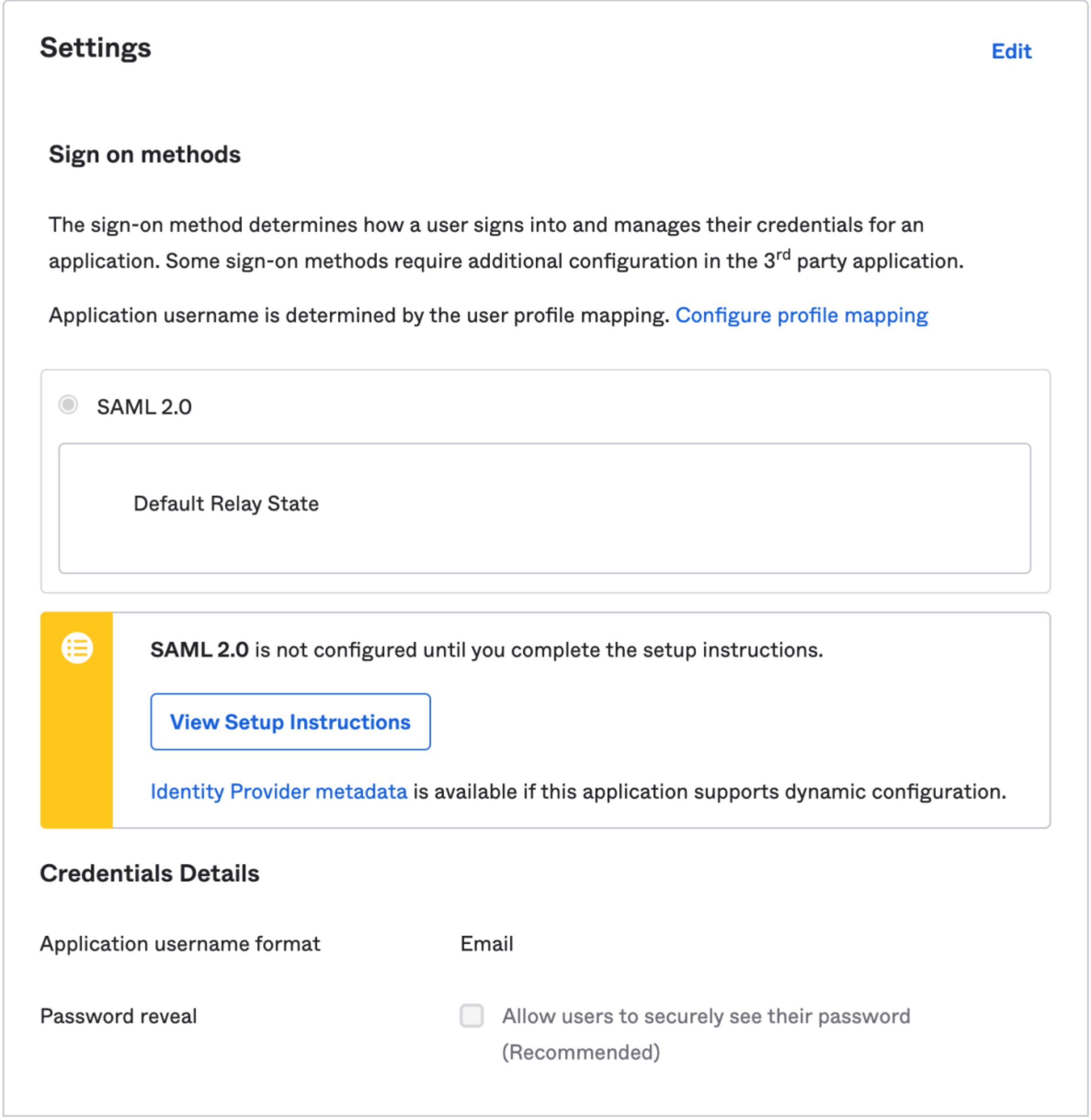
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Step 3: Export the SAML 2.0 IdP metadata

1. Click Next – Configure the Sign On settings

   Two options available: **View Setup Instructions** which steps through the SAML config or **Identity Provider metadata** will produce an XML that can be loaded into Aruba Central.

   Suggestion: Click **Identity Provider metadata** and save the XML data to a file.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

Credentials Details

Application username format	Email
Password reveal	□ Allow users to securely see their password (Recommended)

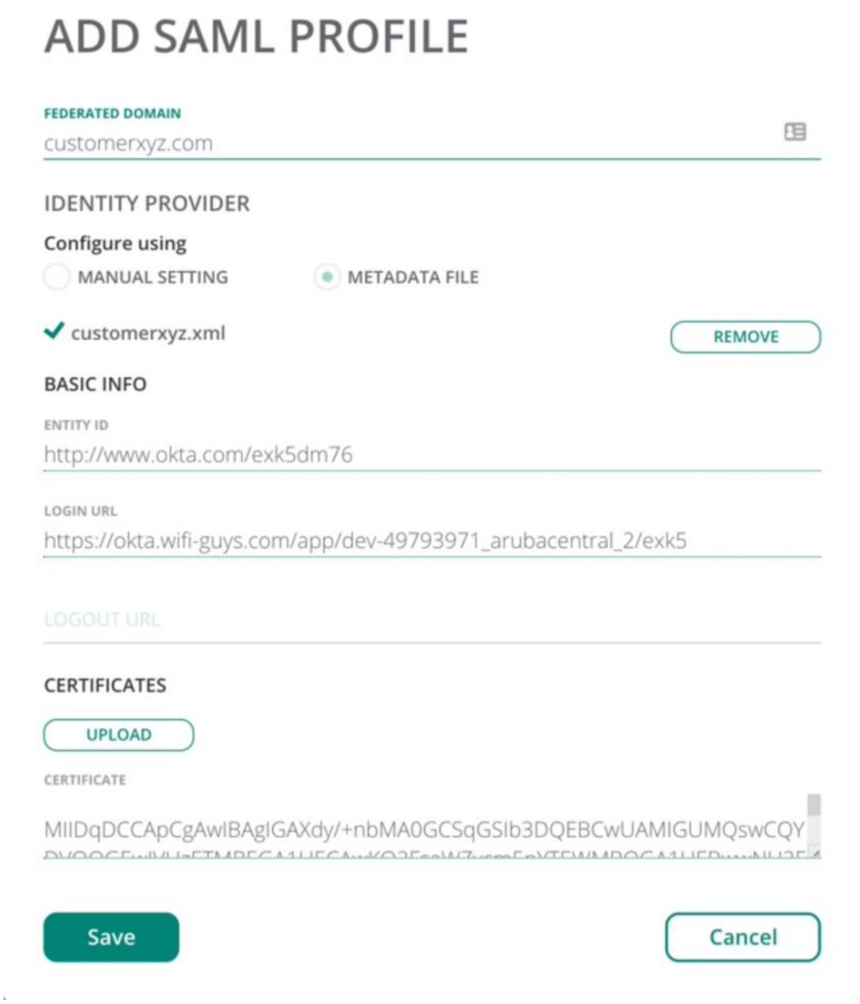
2. Click Next
3. Select Internal app and Click Finish

Step 4: Create SAML Authorization Profile in Aruba Central

1. Log into Aruba Central – Account Home > Click Single Sign On
2. Create a new SAMPL profile – Enter the customer domain name and Click Add SAML Profile
   -Before you can add a new SAML profile, you must have at least one local user account with that domain.
3. Enter the metadata from the above step

   Suggestion use Metadata file – select and import the XML

   Manual Settings are also supported – copy and paste the info from the previous step



ADD SAML PROFILE

FEDERATED DOMAIN
customerxyz.com

IDENTITY PROVIDER

Configure using
○ MANUAL SETTING ● METADATA FILE

✓ customerxyz.xml

BASIC INFO

ENTITY ID
http://www.okta.com/exk5dm76

LOGIN URL
https://okta.wifi-guys.com/app/dev-49793971_arubacentral_2/exk5

LOGOUT URL

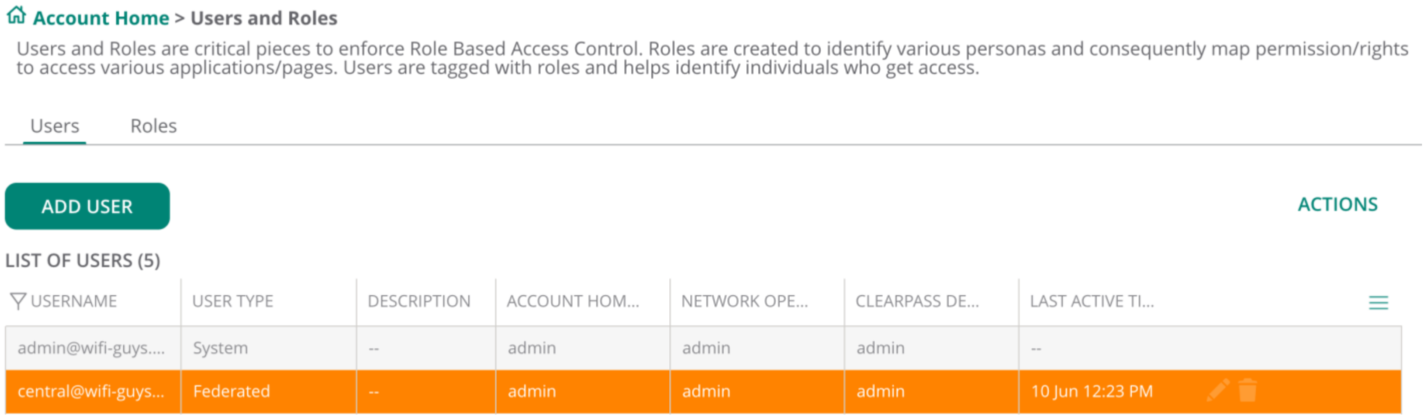
CERTIFICATES

CERTIFICATE
MIIDqDCCApCgAwIBAgIGAXdy/+nbMA0GCSqGSIb3DQEBCwUAMIGUMQswCQY

4. Click Save

Testing and Troubleshooting:

Attempt to log into Aruba Central – once you enter an email with the domain, you will be redirected to the SSO provider. Once you authenticate you will be redirected back to Aruba Central with the proper permissions. You can verify this by clicking under Aruba Central Home > Users and Roles > then verify the user type is **Federated** and the account permissions.



Account Home > Users and Roles

Users and Roles are critical pieces to enforce Role Based Access Control. Roles are created to identify various personas and consequently map permission/rights to access various applications/pages. Users are tagged with roles and helps identify individuals who get access.

LIST OF USERS (5)

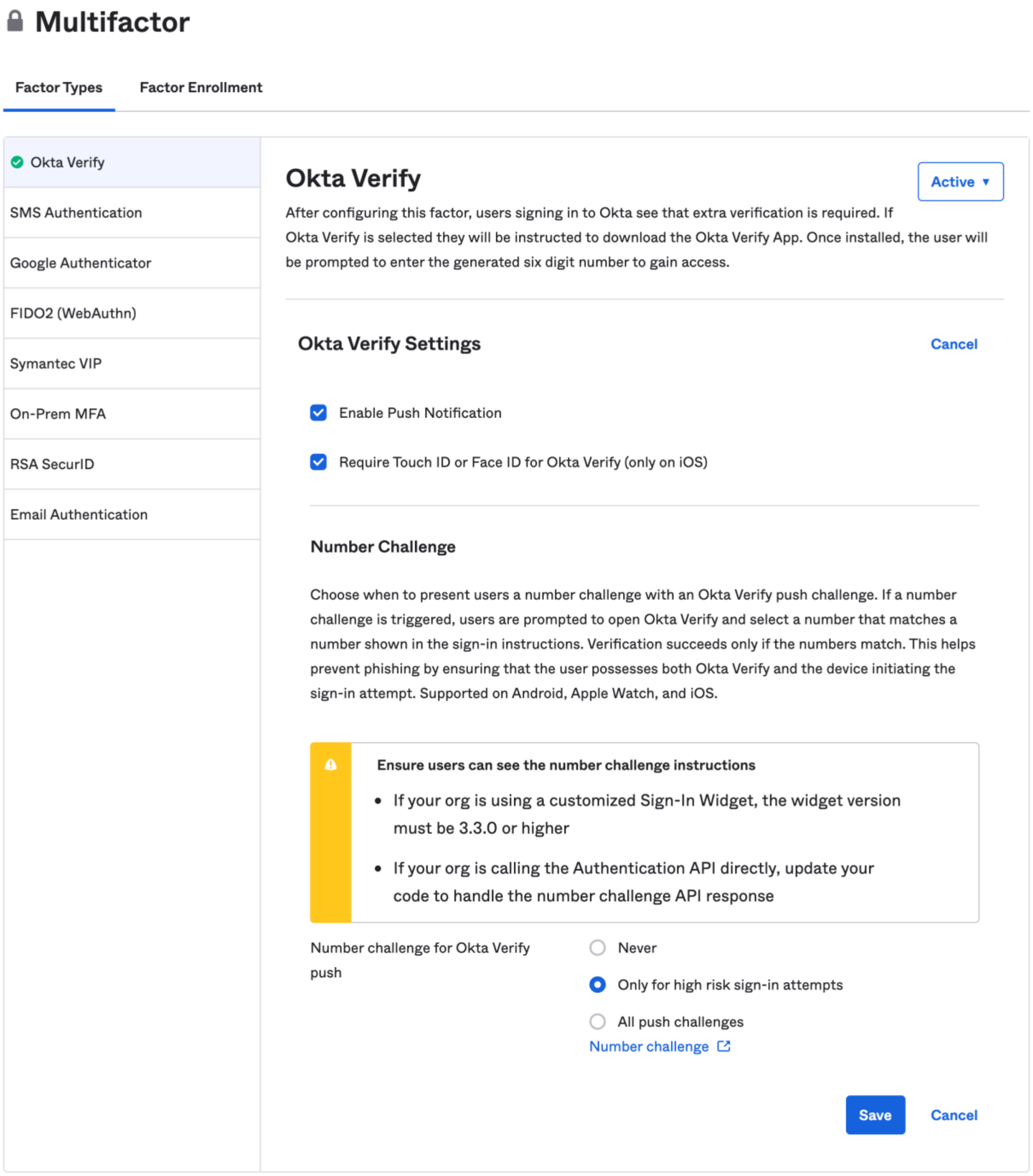
USERNAME	USER TYPE	DESCRIPTION	ACCOUNT HOM...	NETWORK OPE...	CLEARPASS DE...	LAST ACTIVE TI...
admin@wifi-guys....	System	--	admin	admin	admin	--
central@wifi-guys...	Federated	--	admin	admin	admin	10 Jun 12:23 PM

Additional Notes:

- There must be at least **one** verified user belonging to the **domain** in the system users' list.
- Each domain can have only one federation
- The SAML authorization profile configuration feature is available only for the admin users of an Aruba Central account. Aruba Central allows only MSP admin users to configure SAML authorization profiles for their respective tenant accounts.
- SAML user access is determined by the role attribute included in the SAML token provided by the IdP.
- SAML users with admin privileges can configure system users in Aruba Central.
- SAML users can initiate a Single Sign On request by trying to log in to Aruba Central (SP-initiated login). However, SAML users cannot initiate a single logout request from Aruba Central.
- The following menu options in Aruba Central UI are not available for a SAML user. Enable MSP and Disable MSP—SAML users cannot enable or disable MSP deployment mode in Aruba Central. Change Password—Aruba Central does not support changing the password of a SAML user account.
- For more troubleshooting: https://help.central.arubanetworks.com/2.5.3/documentation/online_help/content/nms/user-mgmt/trblsht-saml.htm

Okta MFA Example:

- Okta as well as many cloud identity providers support various MFA and other types of additional security policies.
- Okta Verify (Okta native MFA app) example:
- Okta Admin portal > Security > MFA > Factor Type - Okta Verify Enable



Multifactor

Factor Types | Factor Enrollment

- ✓ Okta Verify
- SMS Authentication
- Google Authenticator
- FIDO2 (WebAuthn)
- Symantec VIP
- On-Prem MFA
- RSA SecurID
- Email Authentication

Okta Verify

Active ▾

After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.

Okta Verify Settings

Cancel

☑ Enable Push Notification

☑ Require Touch ID or Face ID for Okta Verify (only on iOS)

Number Challenge

Choose when to present users a number challenge with an Okta Verify push challenge. If a number challenge is triggered, users are prompted to open Okta Verify and select a number that matches a number shown in the sign-in instructions. Verification succeeds only if the numbers match. This helps prevent phishing by ensuring that the user possesses both Okta Verify and the device initiating the sign-in attempt. Supported on Android, Apple Watch, and iOS.

Ensure users can see the number challenge instructions

- If your org is using a customized Sign-In Widget, the widget version must be 3.3.0 or higher
- If your org is calling the Authentication API directly, update your code to handle the number challenge API response

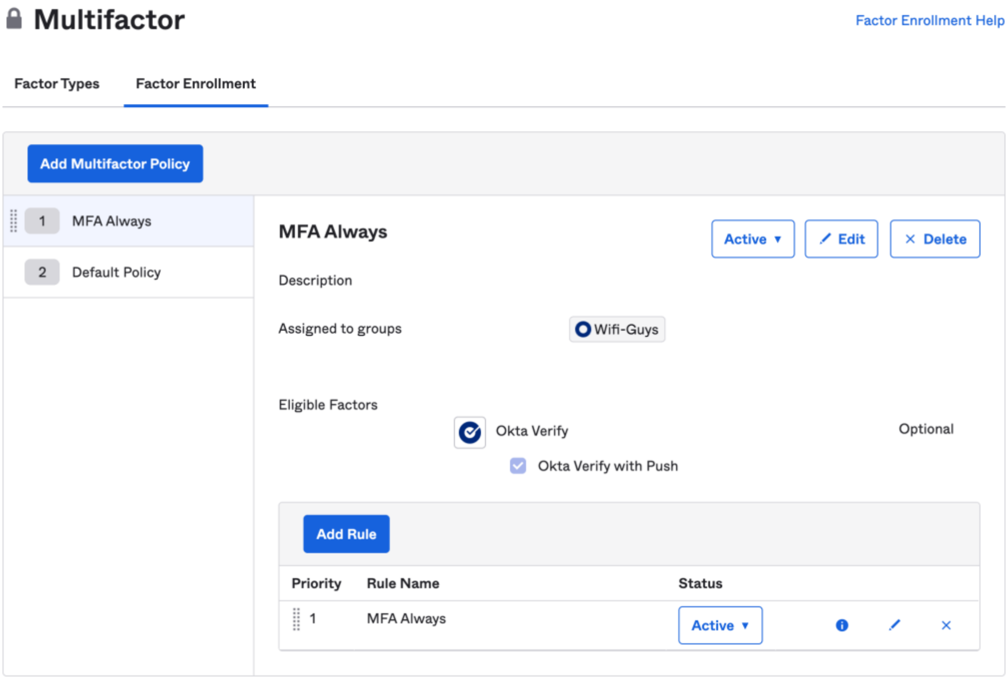
Number challenge for Okta Verify push

○ Never
● Only for high risk sign-in attempts
○ All push challenges

Number challenge

Save | Cancel

- Click Factor Enrollment and create an enrollment policy.
- Then select the user groups to apply this policy to.
- For MFA enable verify with push.



Multifactor

Factor Enrollment Help

Factor Types | Factor Enrollment

Add Multifactor Policy

1 MFA Always

2 Default Policy

MFA Always

Active ▾ | Edit | × Delete

Description

Assigned to groups: Wifi-Guys

Eligible Factors

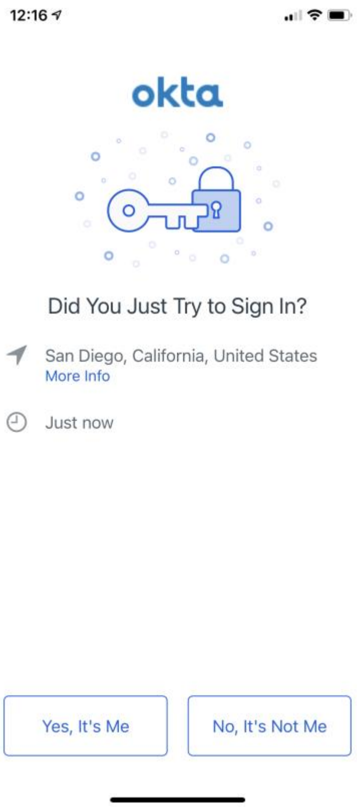
Okta Verify: Optional

☑ Okta Verify with Push

Add Rule

Priority	Rule Name	Status
1	MFA Always	Active ▾

When the user attempts to log into Aruba Central they will be sent a challenge through the Okta app. If this is the first time, the user may be asked to enroll by installing the app and scanning a QR code. After that they should only receive the push MFA notification.



12:16

okta

Did You Just Try to Sign In?

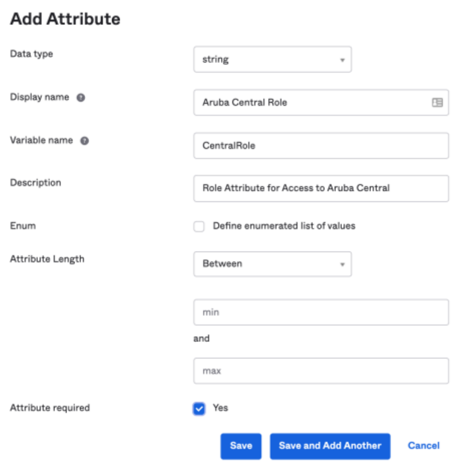
San Diego, California, United States
More Info

Just now

Yes, It's Me | No, It's Not Me

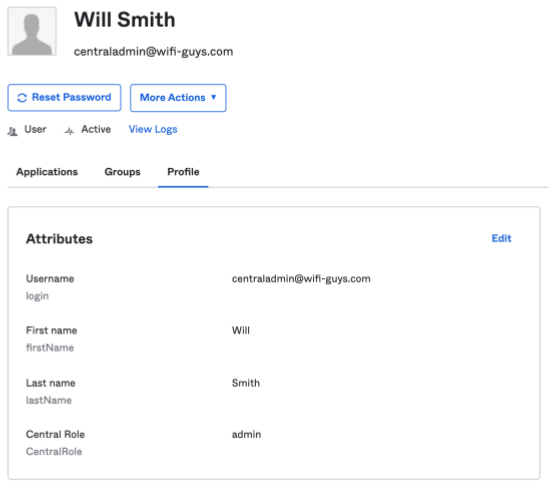
Okta Custom Attribute Example for Central:

- Okta and other cloud providers support custom attributes tied to the user's profile. These are useful to provide role-based access control (RBAC) to Central.
- Common use-case is to allow admin access for network admins and read-only for helpdesk users.
- The example below show a custom attribute **"CentralRole"** which can be referenced by the application in the attribute statement using "**user.CentralRole"**.



Add Attribute

Data type	string
Display name	Aruba Central Role
Variable name	CentralRole
Description	Role Attribute for Access to Aruba Central
Enum	□ Define enumerated list of values
Attribute Length	Between min and max
Attribute required	☑ Yes

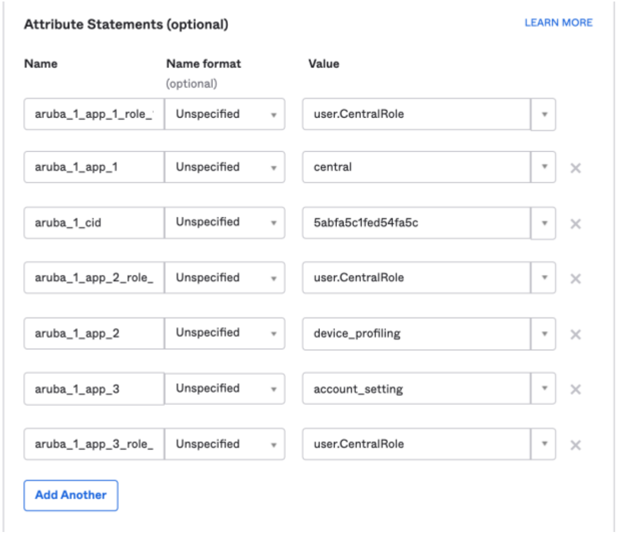


Will Smith

centraladmin@wifi-guys.com

Attributes

Username login	centraladmin@wifi-guys.com
First name firstName	Will
Last name lastName	Smith
Central Role CentralRole	admin



Attribute Statements (optional)

Name	Name format (optional)	Value
aruba_1_app_1_role_	Unspecified	user.CentralRole
aruba_1_app_1	Unspecified	central
aruba_1_cid	Unspecified	5abfa5c1fed54fa5c
aruba_1_app_2_role_	Unspecified	user.CentralRole
aruba_1_app_2	Unspecified	device_profiling
aruba_1_app_3	Unspecified	account_setting
aruba_1_app_3_role_	Unspecified	user.CentralRole