PTT Pro

Workcloud Communication



Okta Integration Guide

2024/01/22

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal. COPYRIGHTS: zebra.com/copyright. PATENTS: ip.zebra.com. WARRANTY: zebra.com/warranty. END USER LICENSE AGREEMENT: zebra.com/eula.

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Introduction

Workcloud Communication supports OAuth2 authentication using the Okta identity provider. Using OAuth2, multiple users can share a single device. This is referred to as the Shared Device Model.

When you install a Workcloud Communication solution with AD/ADFS services, User Authentication, User Provisioning, and Attribute Transformations are possible using LDAP services. The Okta integration only supports User Authentication. User Provisioning and Attribute Transformations are supported indirectly by using the Flat File Import functionality provided by Workcloud Communication.

The Okta integration uses the OpenID Connect (OIDC) protocol, which requires the Authentication Connection Service (ACS). ACS enables Workcloud Communication to authenticate with Okta using OIDC.

This document describes the Okta and ACS configuration required to support user authentication, and how this affects the configuration of PTT Pro for Android and Workcloud Communication Profile Manager.

Requirements

You must have an Okta instance configured and running and the PTT Pro for Android users must be provisioned in the Okta IdP.

- Okta IdP is installed and in operation.
- Users are provisioned in the Okta IdP.

Configuration Overview

The configuration process is divided into four phases. Complete each phase sequentially because each phase uses configuration elements from the previous phase.

Phase 1

Establish the Realm and Client on the ACS server. The Realm is required to create a client, and the client URL is required to configure Okta.

Phase 2

Create the Application in the Okta server. In this phase, the Authentication and Token Access URLs are created along with the Client ID and Client Secret. These elements are required to create the Identity Provider connection in the ACS.

Phase 3

Create the Identity Provider and finalize the ACS configuration.

Phase 4

Configure the PTT Pro Server OAuth connection with the URLs and Certificate needed to connect to the ACS.

Phase 1 – Configuring the ACS

In Phase 1 you will create the realm, copy the signing certificate, configure the client, and create the user property matcher.

In Phase 1, complete the following tasks:

- Create the realm.
- Retrieve the signing certificate for the realm.
- Configure the client.
- Create the user property mapper.

• Capture the IdP redirect URL.

Creating the Realm

Create the realm and enter a meaningful name. The following example uses WFC-OKTA-Connector for the realm name.

1. Select Add realm from the Select realm menu.

Select realm 🗸 🗸	Add realm	
	Import	Select file 🖄
	Name *	WFC-Okta-Connector
	Enabled	CH
		Create Cancel

- 2. In the Name text box, enter the name for the new realm.
- 3. Click Create.

WFC	-Okta-Connector 👻	WFC-Okta-Conr	nector 👕			
Config	pire	General Login	Keys Email Themes Localization Cache Tokens Clie	nt Registration	Client Policies	Security Defenses
	Realm Settings	• Name	WFC-Oxta-Connector			
٦ ج	Clients Client Scopes	Display name				
=	Roles	HTML Display name				
=	Identity Providers	Frontend URL @				
=	User Federation	Enabled @	ON			
-	Authentication	User-Managed Access @	Olt			
Manag	la .	Endpoints @	OpenID Endpoint Configuration			
44	Groups		SAML 2.0 Identity Provider Metadata			
<u>=</u>	Users		Same Carrol			
Ø	Sessions		anne Canace			

The realm is enabled, and the OpenID endpoint is created.

Retrieving the Signing Certification of the Realm

The signing certification is required to configure the PTT Pro Server.

1. Navigate to **Realm Settings** > **Keys**.

Configure	General	Login	Keys Email Themes Localization Cache	Tokens	Client Re	gistration Client i	Alicies Securi	ty Defenses
III Realm Settings	Active Pa	ssive I	Disabled Providers					
© Cliens	Search_		9					
💩 Client Scopes	Algorithm	Type	Kid	Use	Priority	Provider	Public keys	
Roles	AES	OCT	ece020b7-94ef-4435-8bd9-19da4f37fea7	ENC	100	aes-generated		
Identity Providers	H5256	OCT	900e8b31-713a-44e7-bee3-ed9f7486a0ef	96	100	hmac-generated		
E liker Federation	R5256	RSA	h93vw_NXDDe3Qw4ISHhU2W[kdZbpPrcD-8gpaCPNxig	ENC	100	rsa-enc-generated	Public key	Certificate
	R5256	RSA	d-262-DaHMidmCHjklkrzFivLwExf-qTK8NjdHDKD_c	96	100	rsa-generated	Public key	Certificate

2. Copy the RS256, RSA signing certificate, to a convenient local location on your computer. You use this signing certificate to configure the PTT Pro Server.



NOTE: There are two RSA keys. One is for encoding, ENC, and the other for Signing, SIG. The PTT Pro Server uses the signing certificate.

WPC-Okta-Connector ~	WFC-Okta General		ISseCCA2xCBgGBpowrCaANBgraphGGW0BAQ+FADAdMBawGQY0VQ NDoElwrthefMllwidj3MTLathjDrwitheMMawQj3MTLathsLawWjAdM S1Do2SuMNO53hrggBMAGG545Q42DQEBAQUAA4BDwwlogBMA MBladDiwlindca2Shumh9ThgNQj4QLwcCbyG+QWMGThgAbB499	QDDBJIRHAHT IswGQYDVQQ oIBAQCacbyBi IQm+aQDXjyZ QioS2yhSHKUS	2±0Y51Db25u DOBJORkAVET2t RijEeDXn8VeK Yxy3wkisBjTq 3c8txyytLTqur	ration Client Pr	ilicies Securi	ty Defenses
III Realm Settings	Active Pass	10 11	UPTPQC1bc2rQpeonAmmH4+FJM5st0lQ2807xD1g69lQ1hIW3+y1Cs GWmIn681FscsnrdLDivd2c84x2sMCxTMnC9PYu3FGO0xDHsT1eoN=	MoLp4F685dQ	-pmkwh8jml n1zD4k5XcOk			
Clients	Frank	21	oO#G4tzAgMSAAEwDQYJKsZIhutNAQELBQADggEBAFVIS-35OKPubl	WPUPttNjpWf	WGTBpcVGoh			
	Algorithm	1 21	o2w01IfDU+D5aaGSiy/yBxL7HiujtPoWtwUMyfBZNH14Xp4Scwb258	radECPSBNCG	+j4s1rwfac5Y	rovider	Public keys	
E Roles	AES	 V^A O 	TswjcePF=r4VsHz5/TgdMhjiha1wl7GKgzr5XOeg2C462/eQMINLTk55X 2017DHefi5Xiq0js/Dn/NReuc6Oix4AIHh0C/SFhAT201Pi/Pbn7Y(3v57Tne-	W6m+xkkzU/o -dMk=p1A=	wmh0/sGjOTE	es-generated		
	H5256	4	, , , , , , , , , , , , , , , , , , , ,			mac-generated		
User Federation	R5256	RSA	h93ve_NXDDe3Qve45HhU2WjkdZbpPrcD-8gpaCPNotg			rsa-enc-generated	Public key	Certificate
	R5256	RSA	d 26c DeHMidmOHprintsRvLwExt-qTX8NpdHDKD_c		100	rsa-generated	Public key	Certificate

3. Save the certificate in the X.509 format.

The Realm is established.

Sample Signing Certificate



NOTE: The line length is formatted to fit on the page.

```
MIICszCCAZsCBgGBpcwvCzANBgkqhkiG9w0BAQsFADAdMRswGQ
YDVQQDDBJXRkMtT2t0YS1Db25uZWN0b3IwHhcNMjIwNjI3MTUzM
jEwWhcNMzIwNjI3MTUzMzUwWjAdMRswGQYDVQQDDBJXRkMtT2t0
YS1Db25uZWN0b3IwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggE
KAoIBAQCacby8lfRjEeDXn8VeKaxMBxxuQAkhiC/tnKC6q2MKCW
IHESQqK21H1Z/Pj1HbnDM7GGpBn7zvhQm+aCJ0XjyZiYxy3wkisB
JTqdc6JEzdEXwWxkZ58huenh/PTkpNQy0JLzwCOyzG+iQWWGTY
b/xBuBtY9QJoS2yhSHKU53c8txyytLTqurYNUPTfQC1bcZrQJpe
onAmmH4+FjM5sf0IQ2807xD1g69IQ1hiW3+y1CsMoLp4F68SdQ+
pmkwH8jmIdLGWmIn6R1FsccnrdLDiydZc84sZcMCKTMnC9PYu3F
GQQzDHsT1goN+QDDfMhCUzbm1zQ4kSXcOkzHoOaG44zAgMBAAE
```

```
wDQYJKoZIhvcNAQELBQADggEBAFvl6+350lKPsbEWPUPttNJpWf
WGTBpcVGohNmt8e2tfVj0GT7xh4zvNmQvxh+eaewhzuwKhpT/J
G8dyuQVhF4020s2W8YPZqvtLWS0cOY9kljqRl1A3zlo2w0lIfDU
+D5aaGSkylyBxL7HkuJsPoWtwUMyfBZNH14Xp4Scwb25BfddECP
SBNCGJ+j4s1rwfac5YVKTswjcePF+r4VsHzEfTgdMhjJhalwI7G
KgzrBXOagZCA6ZfeQMINLTkBSXW6m+xkkcU/owmMXsGJ0TEQOTT
0HefiBXq0Jt/0h/NReuc6Qk4AlJHh0Cj9FhAT2OTPvPbn7Yj3vB
7Tne+dMk+p1A=
```

Creating the Client

Create a client so that PTT Pro for Android users can authenticate using Okta.

1. Select **Clients** to display the list of default clients.

onfigure	Lookup 🕑					
III Realm Settings	Search	Q				Create
Clients	Client ID	Enabled	Base URL	Actions		
\delta Client Scopes	account	True	https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-Okta-Connector/account/	Edit	Export	Delete
Roles	account-console	True	https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-Okta-Connector/account/	Edit	Export	Delete
	admin-cli	True	Not defined	Edit	Export	Delete
Hoencey Providers	broker	True	Not defined	Edit	Export	Delete
User Federation	realm-management	True	Not defined	Edit	Export	Delete
Authentication	security-admin-console	True	https://wfc-keycloak2.pttpro.zebra.com/auth/admin/WFC-Okta-Connector/console/	Edit	Export	Delete

- 2. Click Create.
- 3. In the Client ID text box, enter a name for the client.

The client name in this example is oidc.client.

WFC	-Okta-Connector 🗸	Clients > Add Client	
Config	jure	Add Client	
	Realm Settings	Import	Select file 🖄
7	Clients	Client ID * 😡	oidc.client
&	Client Scopes	Client Protocol @	openid-connect 🗸
	Roles		
	Identity Providers	Root URL 😡	
	User Federation		Save Cancel
	Authentication		

- 4. Verify that the Client Protocol is openid-connect.
- 5. Click Save to proceed and configure the client.

Configuring the Client

Complete the configuration of the client to ensure the integration with PTT Pro for Android.

- **1.** Click **Clients** under the **Configure** menu.
- 2. Select the client.

The client name in this example is oidc.client

WFC-Okta-Connector ~	Clients		
Configure	Lookup 🕖		
111 Realm Settings	Search Q		
😚 Clients	Client ID	Enabled	Ba
🚓 Client Scopes	account	True	ht
Roles	account-console	True	ht
≓ Identity Providers	admin-cli	True	No
	broker	True	No
User Federation	oldc.client	True	No
Authentication	realm-management	True	No
	security-admin-console	True	ht
Manage	1		

3. Select **Settings** and verify the following settings.

WFC-Okta-Conne	ector 🗸	Clients > oide	. client							
Configure		Oidc.clie	ent 👕							
H Realm Setting	5 2	Settings	Keys Ro	oles	Client Scopes 😡	Mappers 😡	Scope 😡	Revocation	Sessions 😡	Offlin
Clients			Client ID @		oidc.client					
\delta Client Scope	s		Name Ø							_
Roles										_
Identity Prov	iders		Description @							
User Federat	llon		Enabled 😡		ON					
Authentication	n	Always Displa	y in Console 😡		OFF					
Manage		Conse	nt Required 😡		OFF					
A Groups			opin Theme B	- 6						v
👗 Users			ogni menne o							-
 Sessions 		Cli	ent Protocol 😡		openid-connect					~
📋 Events			Access Type 😡		confidential					~
Import		Standard Fl	low Enabled 😡		ON					
Export		Implicit Fl	low Enabled 😡		OFF					
		Direct	Access Grants Enabled @		ON T					
		Service Accou	ints Enabled 😡		OFF					
		OA Autho	uth 2.0 Device rization Grant Enabled @		OFF					
		OIDC CIBA Gr	ant Enabled 😡		OFF					
		Authorizat	ion Enabled 😡		OFF					
			Root URL 😡							
		• Valid R	edirect URIs 😡		https://localhost					-

- Client Protocol is openid-connect.
- Access Type is confidential
 - · The access type public works but does not use a client secret.
 - Switching from confidential to public and back to confidential resets the client's secret to a new value.
 - The access type bearer-only does not work.
- Standard Flow Enabled is ON. If not selected, PTT Pro for Android displays a blank screen and does
 not prompt for credentials.
- **Direct Access Grants Enabled** is ON. If not selected, PTT Pro for Android displays a login screen but then displays a blank screen and does not complete the connection.
- Enter https://localhost in the Valid Redirect URIs field. An invalid URI generates an error on the device when connecting to the ACS; the login screen does not display.

4. Click Save to continue.

* Valid Redirect URIs @	https://localhost	-
		+
Base URL @		
Admin URL 🖗		
Web Origins 😡		+
Backchannel Logout URL 🖗		
Backchannel Logout Session Required @	ON	
Backchannel Logout Revoke Offline Sessions @	OFF	
> Fine Grain OpenID Co	nnect Configuration 🕢	
> OpenID Connect Com	npatibility Modes 🖗	
> Advanced Settings @		
> Authentication Flow C	Dverrides 🛛	
	Save Cancel	

Copying the Client Secret

The client secret is used to configure PTT Pro for Android. Copy the secret and the Client ID.

1. Click the **Credentials** tab to access the client secret.

WFC-Okta-Connect	or 🗸	Clients > oide	client							
Configure		Oidc.clie	ent 👕							
III Realm Settings		Settings	Credentials	Keys R	oles	Client Scopes 😡	Mappers 😡	Scope 🚱	Revocation	Sess
Clients		Installatio	n 🖸							
🛞 Client Scopes		Client A	uthenticator @	Client Id a	nd Secre					
Roles										
🚍 Identity Provide	**5		Secret	31941cec-9	9616-465	8-8749-2e6c3fa4ff23	Reg	enerate Secret		
📒 User Federatio	n			_						
Authentication		Registration a	access token 🖗				Reg	enerate registrat	tion access token	
Manage										

2. Copy the client secret.

The client secret is automatically generated.

3. Save the client secret and the client ID, oidc.client, in this example, to a convenient location.

Example Client Secret

31941cec-9b16-46b8-8749-2e6c3fa4ff23

Creating a User Property Mapper

This task maps the token claim sub to the username attribute used by PTT Pro for Android. If this procedure is not completed, the device user is presented with the credentials screen, but after entering the credentials, the device displays a blank screen.

1. Click the Mappers tab in the client definition.

WFC-Okta-Connector v	Clients > oldc.client
Configure	Oidc.client a
111 Realm Settings	Settings Credentials Keys Roles Clent Scope Ø Mappers Ø Scope Ø Revocation Sessions Ø Offline Access Ø Clustering
Q Cierts	Installation @
🛞 Client Scopes	
E Roles	Verez Add Suiter
😑 Identity Providers	ra mayor a versions
User Federation	
Authentication	
Manage	

- 2. Click Create to define a mapping.
 - Enter username in the **Name** field.
 - Select User Property from the Mapper Type menu.
 - Enter username in the **Property** field.
 - Enter sub in the Token Claim Name field.
 - Select String from the Claim JSON Type menu.

Clients > oidc.client > Mappers > Create Protocol Mappers					
Create Protocol M	lapper				
Protocol 😡	openid-connect				
Name 😡	username				
Mapper Type 😡	User Property 🗸				
Property 😡	username				
Token Claim Name 😡	sub				
Claim JSON Type 😡	String 🗸				
Add to ID token 😡	ON				
Add to access token 😡	ON				
Add to userinfo 😡	ON				
	Save Cancel				

3. Click Save to return to the client definition screen.

Copying the Identity Provider Redirect URI

Copy the Redirect URI from the ACS to complete the Okta configuration. The ACS IdP requires information from the Okta application configuration, which you complete after the Okta Application is established.

1. Select **Identity Providers** from the client configuration.

WFC	Okta-Connector	~	Identity Providers
Config	jure		
999	Realm Settings		
Ð	Clients		
- 80	Client Scopes		\rightarrow
=	Roles		
#	Identity Providers		Identity Providers
8	User Federation		Through Identity Brokening it's easy to allow users to authenticate to Keycloak using external Identity Providers or Social Networks. We have built-in support for OpenID Connect and SAML 2.0 as well as a number of social networks such as Google. GitHub, Facebook and Twitter.
•	Authentication		To get started select a provider from the dropdown below:
Manag	je		Add provider 👻

- 2. Select Open ID Connect 1.0 from the menu to display the redirect URI.
- 3. Copy the redirect URI from the Redirect URI field.

WFC	-Okta-Connector 🗸	Identity Providers > Add Iden	tity provider
Config	jure	Add identity pro	vider
919	Realm Settings	Redirect URI @	https://www.weineter.org/arth/realms/WFC-Okta-Connector/broker/okta.c
Ø	Clients	* Alias 😡	okta.oldc.connector
& =	Client Scopes Roles	Display Name 😡	okta.oldc.connector
=	Identity Providers	Enabled @	ON
	User Federation	Store Tokens @	ON
•	Authentication	Stored Tokens Readable	ON
Manag	ge		
- 4 <u>4</u>	Groups	Trust Email 😡	OFF
4	Users	Account Linking Only 😡	OFF
Ø	Sessions	Hide on Login Page 😡	OFF
	Events	GUI order @	
2	Import		
	Export	First Login Flow @	Simple Login Flow
		Post Login Flow ©	~
		Sync Mode 😡	import 🗸
		~ OpenID Connect C	onfig 😡

Example Redirect URI

In this example, the redirect URI is: https://<ACS-server-name>/auth/realm/WFC-Okta-Connector/broker/okta.oidc.connector/endpoint.

Phase 2 – Configuring Okta

In this phase, you add and configure a new Workcloud Communication native application using configuration elements from the ACS. The users should already exist in the Okta system.

Creating an App

Use Okta to create a new native application for PTT Pro for Android.

1. Open Okta and navigate to Applications > Applications and click Create App Integration.

okta		Q Search			
Dashboard	×	Applications			
Customizations	~		-		
Applications	^	Developer Edit	ion prov	ides a li plans page. C	imited number of apps. Contact us to find a plan that is right for your organization.
Applications		Create App Integration	Browse Ap	p Catalog	Assign Users to App More *
Self Service					
Security	~	Q, Search			
Workflow	~	STATUS		&	Native App PTT-Pro Client ID: 0ca5ddvi4IGDU18nl5d7
Reports	~	ACTIVE	1		
Settings	~	INACTIVE	0	0	Okta Admin Console
				0	Okta Browser Plugin
					Okta Dashboard

2. Select OIDC - OpenID Connect as the Sign-in method.

3. Select Native Application as the Application type.

Create a new app integration		`
Sign-in 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.
	0	SWA - Secure Web Authentication Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
	0	API Services Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.
Application type	0	Web Application
What kind of application are you trying to integrate with Okta?		server side applications where authentication and tokens are nandled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
Specifying an application type customizes your experience and provides the best configuration, SDK,	0	Single-Page Application Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
and sample recommendations.	•	Native Application Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)
		Cancel Next

4. Click Next.

Configuring the New Native App

Configure the app with the described settings. Settings include naming the app and adding the redirect URI that you previously created.

1. Enter a name in the App integration name field.

okta		Q Search		0	88	steve.zimmer okta-dev-84		
Dashboard	~							
Directory	~	🗮 New Native App Integra	tion					
Customizations	~	General Settings						
Applications	~	• We found some errors. Please review the f	orm and make corrections.					
Security	~	App integration name	Native PTT-Pro App					
Workflow	~	ter Orient						
Reports	~	Logo (Optional)			Ŀ	1		
Settings	~		r y					
		Grant type Learn More ES	Client acting on behalf of a user Authorization Code Interaction Code Refresh Token Resource Owner Password SAML 2.0 Assertion Device Authorization Token Exchange Implicit (hybrid)					
		Sign-in redirect URIs Okta sends the authentication response and ID token for the user's sign-in request to these URIs Learn More 12	Allow wildcard * in sign-in URI redirect. https://wfs/insystem/auth https://localhost + Add URI	/realms/WFC-O	kta-Cr) ×) ×		
		Sign-out redirect URIs (Optional) After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs. Learn More ES	com.okta.dev-84941762:/ + Add URI] 🗙		
		Assignments Controlled access Select whether to assign the app integration to	Allow everyone in your organization to acce Limit access to selected groups Sitis groups professory for access	55				
		everyone in your org, only selected group(s), or skip assignment until after app creation.	Ship group assignment for now	Broker Made				
		Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.	Enable immediate access with Pederation Broker Mode To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode.					
				San	•	Cancel		

2. Optionally, add an application logo.

- 3. Select the Grant type.
 - Authorization Code is automatically selected.
 - Refresh Token sets the refresh from persistent to a time interval.
 - Additional types can be selected if required.
- 4. Modify the Sign-in redirect URIs.
 - a) Delete the default redirect URI.
 - **b)** Enter the Redirect URI from the OIDC Identity Provider. Go to Copying the Identity Provider Redirect URI on page 11.
 - c) Click Add URI and enter https://localhost
- 5. Do not modify the Sign-out redirect URIs.
- 6. Under Assignments, determine how users are granted access to the application.
 - Set Controlled Access to Allow everyone in your organization to access.
 - Choose whether to grant immediate access with the Federation Broker Mode.
 - When enabled, all users are eligible to access the application. Custom access token claims are applied to these users.
 - When disabled, users are selectively granted access and customized claims need to be created and applied to the users. When the broker is not enabled, additional configuration is required. See Configuring Access to the Native App on page 16.
- 7. Click Save to preserve the General Settings.

Configuring Access to the Native App

When the Federation Broker is not used to grant users access to the application, complete the following task to determine who can access the app.

1. Open the application and select the Assignments tab.

ieneral !	Sign On Assig	nments Okta API	Scopes	
Assign •	Convert assi	gnments ·	Q Search	Groups •
ilters	Priority	Assignment		
eople	1	O Everyone All users in your o	organization	× ×
roupu			-	

2. Select the access appropriate for your environment.

In this example, the PTT-Pro App is made available to the group Everyone.

Completing the Native App Configuration

Complete the configuration of the app to finish the ACS Identity Provider.

1. Open the application and perform the following steps under the **General** tab.

okta		Q Search		
Dashboard	v	← Back to Applications		
Directory	v		PTT-Pro App	
Customizations	×	Active •	See View Logs	
Applications	^	General Sign On Assignmen	ts Okta API Scopes	
Applications				
Self Service		Client Credentials		Edit
Security	×	Client ID	0	
Workflow	Ý		Public identifier for the client that is r	equired for all OAuth
Reports	~		flows.	
Settings	ř	Client authentication	None Client secret Public key / Private key	
		CLIENT SECRETS		
			Gener	ate new secret
		Creation date Secret		Status
		him 27, 2022		e Active v

- 2. Click Edit.
- **3.** Copy the client credentials from the **Client ID** field.

In this example, the client ID is: 0oa5km1v306LXN57y5d7

4. Under **CLIENT SECRETS**, reveal the secret, and copy the secret to your computer for later in the configuration.

In this example, the client secret is: QUndeR7dkcARwPFjVyGVh6NeFjzbs00Md2xWYFLS

5. Click the Sign On tab to edit the OpenID Connect ID Tokenscreen.

OpenID Connect ID Token	Cancel
Issuer	Okta URL (https://dev-84941762.okta.com) *
Audience	0oa5ddvj4IGDU18nI5d7
Claims	Claims for this token include all user attributes on the app profile.
Groups claim type	Filter •
Groups claim filter 💿	groups Matches regex ↓ .*
	Save Cancel

- 6. Select Okta URL from the Issuer menu.
- 7. Audience is automatically populated with the Client ID.
- 8. Select Filter for the Group claims type.
- 9. Enter the Group Claims Filter.

A typical filter is .*.

10. Click Save.

Review the remaining configuration options of the native application and make any modifications necessary for your environment.

Phase 3 – Completing the ACS Configuration

You completed the application configuration with the Client ID and Client Secret. In this section, you will complete the configuration of the Identity Provider with information from the Okta configuration.

Creating A Simple Login Authentication Flow

The authentication flow enables the mobile client to seamlessly pass credentials through ACS to the Okta IdP.

Complete the Authentication Flow before completing the IdP definition. The Authentication Flow is not required, and other configurations are possible, but it improves the sign-in experience for the user.

For example, if the ACS IdP configuration specifies:

- Browser for the First Login Flow, the user cannot progress past the login screen.
- First Broker Login, the user is prompted to enter their first name, last name, and email address. While this configuration works, it is a poor user experience.
- Direct Grant generates a missing parameter error.
- Registration flow requires that the user enter their user profile information before continuing.

The ACS adds users to the user table as they access the system. The Simple Login Flow automatically populates the user table with the user name when the user signs in. No passwords are examined or tracked. The user authentication occurs on the Okta system

Creating the Authentication Flow

Create an authentication flow to enable the device client to pass credentials through the ACS to the Okta IdP.

1. Select Authentication > Flows > New.

WFC-C	kta-Connector	~	Authentication						
Configur	•		Flows Bindings Required Action	ons Password Policy OTP Policy	WebAuthn Policy @	WebAuthn Passwor	diess Policy	A Policy	
	Realm Settings		Http Challenge 🗸 0					New Copy	
	Clients		Auth Type		Requirement				
- db (Client Scopes		Browser Redirect/Refresh		REQUIRED				
- E 1	Roles		Authentication Options O		REQUIRED	O ALTERNATIVE	O DISABLED	O CONDITIONAL	
= 1	Identity Providers			Basic Auth Challenge	CIRIUGIA ®	O ALTERNATIVE	O DISABLED		
	User Federation			Basic Auth Password+OTP	OREQUIRED	OALTERNATIVE	@ DISABLED		
•	Authentication			Kerberos	OREQUIRED	OALTERNATIVE	@ DISABLED		

2. Enter a name in the Alias field and select generic from the Top Level Flow Type menu.

WFC	-Okta-Connector 🗸	Create Top Level Form								
Config	jure	Flows Bindings	Required Actions	Password Policy	OTP Policy	WebAuthn Policy 😡	WebAuthn Pass			
111	Realm Settings	Alias @	Simple Login Fl	ow						
ø	Clients	Description								
&	Client Scopes	<i>Description</i>								
=	Roles									
=	Identity Providers									
8	User Federation	Top Level Flow Type @	generic				~			
۵	Authentication		Sum Cancel	1						
Manag	ge		Cancel	1						

3. Click **Save** to create the flow.

4. Select the new flow from the Authentication view and click Add Execution.

WFC	Okta-Connector	*	Auther	ntication						
Config	μre		Flows	Bindings	Required Actions	Password Policy	OTP Policy	WebAuthn Policy 😡	WebAuthn Passwordless Policy 🛛	CIBA Policy
	Realm Settings		Simple	ogin Flow 👻	0				New Copy Delete	Edit Flow Add execution Add flow
	Clients		No execut	ions available						
	Client Scopes									
	Roles									
	Identity Providers									
	User Federation									
•	Authentication									

5. Select Create User If Unique from the Provider menu.

WFC	-Okta-Connector 🗸 🗸	Create	e Authent	ticato	r Execu	tion			
Confi	gure	Flows	Bindings	Requir	red Actions	Password Policy	OTP Policy	WebAuthn Policy 😡	WebAuthn Pass
986	Realm Settings		Provider 6	9	Create User If	Unique			~
¢	Clients				Save Cancel	1			
8	Client Scopes				Concer				
=	Roles								
≓	Identity Providers								
8	User Federation								
۵	Authentication								
Mana	ge								

- 6. Click Save.
- 7. In the Authentication view, select Alternative to activate the flow. The configuration is automatically saved.

WFC-Okta-Connector ~	Authentication					
Configure	Flows Bindings Required Actions Password Policy	OTP Policy WebAuthr	Policy WebAuthn Passw	ordless Poli	cy O CIBA Polic	У
III Realm Settings	Simple Login Row 👻 🔍			New Copy	Delete Edit Flow	Add execution Add flow
Clens	Auth Type	Requirement				
🛞 Client Scopes	 Create User If Unique 	O REQUIRED		Opes	ABLED	Actions ~
El Roles						
Identity Providers						
User Federation						
Authentication						
Manage						

Creating the Identity Provider

Create the identity provider using information from Okta to complete the configuration.

1. Select Identity Providers from the ACS interface.

WFC-Okta-Connector 🗸	Identity Providers
Configure	
111 Realm Settings	
Clients	
🛞 Client Scopes	\equiv
E Roles	
Identity Providers	Identity Providers
User Federation	Through Identity Brokering it's easy to allow users to authenticate to Keycloak using external Identity Providers or Social Networks. We have built in support for OpenID Connect and SAML 2.0 as well as a number of social networks such as Google. GitHub. Facebook and Twitter
Authentication	To get started select a provider from the dropdown below.
Manage	Add provider

2. Select Open ID Connect 1.0 from the menu.

3. Configure the Identity Provider.

WFC	Okta-Connector 🗸	Identity Providers -> Add identity provider	
Config	ure	Add identity pro	vider
919	Realm Settings	Redirect URI @	https://wfs.keyslaaidit.programshaa.com/auth/realms/WFC-Okta-Connector/broker/okta.c
Ø	Clients	* Alias 😡	okta.oidc.connector
&₀ =	Client Scopes Roles	Display Name 😡	okta.oidc.connector
=	Identity Providers	Enabled O	ON DI
	User Federation	Store Tokens @	ON
•	Authentication	Stored Tokens Readable	ON
Manag	je		
- 4 <u>4</u>	Groups	Trust Email 😡	OFF
1	Users	Account Linking Only 😡	OFF
Ø	Sessions	Hide on Login Page 😡	OFF
#	Events	GUI order @	
2	Import		
	Export	First Login Flow @	Simple Login Flow
		Post Login Flow @	×
		Sync Mode 😡	import Y
		 OpenID Connect C 	onfig 🚱

- Alias, okta.oidc.connector in this example.
- Set Enabled to On.
- (Optional) Set Store Tokens to On.
- (Optional) Set Store Tokens Readable to On.
- Select Simple Login Flow from the First Login Flow menu.

The redirect URI is displayed in the **Redirect URI** field and is used as the Okta Redirect for the native app. In this example, the redirect URI is:

https://<acs-server-name>/auth/realms/WFC-Okta-Connector/broker/ okta.oidc.connector/endpoint

Collecting Information from the Well-Known URL

To complete the configuration of the Identity provider, collect additional information from the well-known URL.

To complete the Identity Provider configuration the following elements are required:

- Authentication URL from the well-known URL
- Token URL from the well-know URL

- Client Authentication
- Client ID
- Client Secret
- Client Assertion Signature Algorithm

You can obtain this information by browsing into the Okta IdP using the well-known URL. The Okta domain and client ID are required to create the well-known URL.

Accessing the Well-Known URL

Use the Okta domain and the client ID to create the well-known URL.

A well-known URL uses the following structure:

```
https://<domain>/.well-known/openid-configuration?client_id=<client-id>
```

In this example, the well-known URL becomes:

```
https://dev-84941762.okta.com/.well-known/openid-configuration?
client_id=0oa5km1v306LXN57y5d7
```

- The domain is dev-84941762.okta.com.
- The Client ID, 0oa5km1v306LXN57y5d7, was generated when you created the Native App.

Figure 1 Native App with Client ID

Applications			
Developer Edit Deactivate unused apps or	ion prov check out our	ides a l i plans page. C	mited number of apps. Contact us to find a plan that is right for your org
Create App Integration	Browse Ap	p Catalog	Assign Users to App More 🔹
Q Search			
STATUS		Ø	Native App PTT-Pro Client ID: 0oa5ddvj4IGDU18nI5d7
ACTIVE	1	~	
INACTIVE	2	O	Okta Admin Console

Entering the well-known URL in a web browser returns a response in a JSON file format. The JSON response includes information required for the ACS configuration:

- Authorization endpoint
- Token endpoint

The supported encrypting format

```
{
"issuer": "https://dev-84941762.okta.com",
"authorization_endpoint": "https://dev-84941762.okta.com/oauth2/v1/
authorize",
"token_endpoint": "https://dev-84941762.okta.com/oauth2/v1/token",
"userinfo_endpoint": "https://dev-84941762.okta.com/oauth2/v1/userinfo",
"registration_endpoint": "https://dev-84941762.okta.com/oauth2/v1/
clients/0oa5km1v306LXN57y5d7",
"jwks uri": "https://dev-84941762.okta.com/oauth2/v1/keys?
client_id=0oa5km1v306LXN57y5d7",
"response_types_supported": [
"code"
],
"response_modes_supported": [
"query",
"fragment",
"form_post",
"okta_post_message"
],
"grant types supported": [
"authorization_code",
"refresh_token",
"password",
"urn:ietf:params:oauth:grant-type:token-exchange"
],
"subject_types_supported": [
"public"
],
"id_token_signing_alg_values_supported": [
"RS256"
],
"scopes_supported": [
"openid",
"email",
"profile",
"address",
"phone",
"offline_access"
],
"token_endpoint_auth_methods_supported": [
"client_secret_basic"
],
"claims_supported": [
"iss",
"ver",
"sub",
"aud",
"iat",
"exp",
"jti",
"auth_time",
```

```
"amr",
"idp",
"nonce",
"name",
"nickname",
"preferred_username",
"given_name",
"middle name",
"family_name",
"email",
"email_verified",
"profile",
"zoneinfo",
"locale",
"address",
"phone_number",
"picture",
"website",
"gender",
"birthdate",
"updated_at",
"at_hash",
"c_hash"
],
"code_challenge_methods_supported": [
"S256"
],
"introspection_endpoint": "https://dev-84941762.okta.com/oauth2/v1/
introspect",
"introspection_endpoint_auth_methods_supported": [
"client_secret_basic"
],
"revocation_endpoint": "https://dev-84941762.okta.com/oauth2/v1/revoke",
"revocation_endpoint_auth_methods_supported": [
"client_secret_basic"
],
"end_session_endpoint": "https://dev-84941762.okta.com/oauth2/v1/logout",
"request_parameter_supported": true,
"request_object_signing_alg_values_supported": [
"HS256",
"HS384",
"HS512"
],
"device_authorization_endpoint": "https://dev-84941762.okta.com/oauth2/v1/
device/authorize",
"pushed_authorization_request_endpoint": "https://dev-84941762.okta.com/
oauth2/v1/par"
}
```



NOTE: The authorization and token URLs are shown in the response from the well-known URL. If the Okta system uses a Federation Broker, modify the authorization and token URLs.

The original URLs from the JSON response:

- "authorization_endpoint": "https://dev-84941762.okta.com/oauth2/v1/ authorize"
- "token_endpoint": "https://dev-84941762.okta.com/oauth2/v1/token"

Modify the URLs to include the Authorization Server:

- "authorization_endpoint": "https://dev-84941762.okta.com/ oauth2/<server_name>/v1/authorize"
- "token_endpoint": "https://dev-84941762.okta.com/oauth2/<server_name>/v1/ token"

Completing the Identity Provider Configuration

Use the information from the JSON response to the well-known URL to complete the configuration of the Identity Provider.

1. Open the Identify Provider and complete the configuration.

 OpenID Connect Config Ø 		
* Authorization URL 😡	https://dev-84941762.okta.com/oauth2/v1/authorize	
Pass login_hint @	OFF	
Pass current locale @	OFF	
* Token URL 😡	https://dev-84941762.okta.com/oauth2/v1/token	
Logout URL @		
Backchannel Logout @	OFF	
Disable User Info 😡	OFF	
User Info URL 😡		
* Client Authentication @	Client secret as jwt	
* Client ID 😡	0oa5km1v306LXN57y5d7	
★ Client Secret @	QUndeR7dkcARwPFjVyGVh6NeFjzbs00Md2xWYFLS	
 ★ Client Assertion Signature Algorithm @ 	HS256	
Issuer 😡		
Default Scopes 😡	openid profile	
Prompt 😡	login	
Accepts prompt=none forward from client	OFF	
Validate Signatures @	OFF	
Use PKCE @	OFF	
PKCE Method @		
Allowed clock skew @		
Forwarded Query Parameters @		
	Save Cancel	

- **2.** The example configuration uses the following data.
 - Authorization URL is https://dev-84941762.okta.com/oauth2/v1/authorize
 - Token URL is https://dev-84941762.okta.com/oauth2/v1/token
 - Set Client Authentication to Client secret as jwt
 - Sent as Post also works
 - basic auth also works
 - JWT Signed with Private Key will fail. The device displays the error, An Unexpected error when authenticating with the Identity Provider after entering credentials
 - Client ID is 0oa5km1v306LXN57y5d7

This value is assigned by the Okta system for the Native App definition. Go to Completing the Native App Configuration on page 17.

• Client Secret is QUndeR7dkcARwPFjVyGVh6NeFjzbs00Md2xWYFLS

This value is assigned by the Okta system for the Native App definition. Go to Completing the Native App Configuration on page 17.

• Client Assertion Signature Algorithm is HS256 (HS384 or HS512)

The authentication algorithm is specified in the response from the well-known URL. If the algorithm is not supported, the device displays an authentication error after the credentials are entered.

- Enter openid, offline_access, and profile as space-separated strings in the **Default Scopes** field. These scope values are returned in the response from the well-known URL.
 - • If only openid is entered, authentication does not advance beyond the credentials screen.
 - If only offline_access is entered, authentication does not advance beyond the credentials screen.
 - If only profile is entered, the device displays a web page not available error.
- Enter login in the **Prompt** field.
 - The Consent and Select_Account parameters also work.
 - Unspecified results in a blank screen on the device after the credentials are entered.
 - Non results in a blank screen.
- 3. Click Save.

Setting the Login Browser Flow

After you configure the Identity Provider, you can complete the configuration of the ACS Identity Provider.

The Identity Provider Redirector should be set to the Identity Provider to enable the Okta login screen. If this step is not performed, the user is presented with the ACS login screen.

WFC-OKTA-CONNECTOR	
Sign in to your account	
Username or email	
Password	
Sign In	
Or sign in with	
okta.oidc.connector	



NOTE: A user could click on the **okta.oidc.connector** to log in, but this can be confusing in a runtime environment.

1. Select Authentication and click the Flows tab to list all of the authentication types.

WFC-Okta-Connector ~	Authentication							
Configure	Flows Bindings Required Actions	Password Policy OTP Policy	WebAuthn Policy O	WebAuthn Passv	vordless Policy O	CIBA Policy		
II Realm Settings	Browser v 0						6	New Copy
© Gers	Auth Type			Requirement				
💩 Clerc Scopes	Cookie			O REQUIRED	# ALTERNATIVE	ODISABLED		
E Reles	Kerberos			O REQUIRED	OALTERNATIVE	■ DISABLED		
Identity Providers	Identity Provider Redirector (pidc.connector)			O REQUIRED	@ ALTERNATIVE	O DISABLED		Actions ~
User Federation	Forms Q			O REQUIRED	@ ALTERNATIVE	ODISABLED	O CONDITIONAL	
Authentication		Username Password Form		# REQUIRED				
Manage		Browser - Conditional OTP 0		OREQUIRED	OALTERNATIVE	ODISABLED	CONDITIONAL	
4. Groups			Condition - User Configured	REQUIRED	ODISABLED			
± Users			OTP Form	REQUIRED	O ALTERNATIVE	O DISABLED		
O Services						1		

- 2. Click the **Actions** menu on the right side of the screen and select **Configuration** for the Identity Provider Redirector.
- **3.** Configure the oidc.connector.

WFC-Okta-Connector 🗸	Authentication Rows > Browser > olidc.connector		
Configure	Oidc.connector 👕		
111 Realm Settings	ID	6ca948e0-813d-4072-9f6e-ff13669a288a	
Cleros	Alias @	oidc.connector	
🛞 Client Scopes	Default Identity Provider @	nits oldr conserver	
Roles	Contract of the second of the	ona out to rector	
Identity Providers		Save Cancel	
User Federation			
Authentication			
Manage			

- Enter an Alias. In this example, oidc.connector.
- Enter the **Default Identity Provider**. In this example, okta.oidc.connector.

4. Click Save.

Validate the Configuration

Validate the configuration before testing with a mobile device. Two tools are used to validate the configuration: the Postman application and the jwt.io token validator.

Validating with Postman

Testing access with Postman validates that the collected information is accurate and produces the expected results.

Create a profile with the following configuration parameters:

- Auth URL
- Access Token URL
- Client ID
- Client Secret
- Scope with the space-separated values of openid, profile, and offline_access

The profile scope is used to get a refresh token.

1. Insert the following URLs into the Postman profile along with the Client ID and Client Secret.

The URLs can be found by entering the well-known URL into a browser. In this example, the well-known URL is https://<acs-server-name>/auth/realms/WFC-Okta-Connector/.well-known/ openid-configuration

- Authorization endpoint URL: https://<acs-server-name>/auth/realms/WFC-Okta-Connector/protocol/openid-connect/auth
- Access Token URL: https://<acs-server-name>/auth/realms/WFC-Okta-Connector/ protocol/openid-connect/token

Header Prefix (1)	Bearer
Configure New Token	
Configuration Options Advanced Options	
Token Name	Enter a token name
Grant Type	Authorization Code \checkmark
Callback URL	https://localhost
	Authorize using browser
Auth URL	https://www.incomentation.com/aut
Access Token URL ④	https://www.ayuuuu.ayuu
Client ID	oidc.client
Client Secret ④	31941cec-9b16-46b8-8749-2e6c3fa4ff1 🛆
Scope ④	openid offline_access profile
State (1)	State
Client Authentication	Send client credentials in body \sim
Clear cookies	
Get New Access Token	

Remember to clear the cookies before running the test again.

2. Click Get New Access Token.

A successful test displays the Okta login screen from the ACS.

₹.ZEBRA	
Sign In	
Username	
1	
Password	
0	
Keep me signed in	
Sign in	
Forgot password? Help	



NOTE: The branding icons in the example are configured separately and outside the scope of this document.

3. Enter user credentials.

MANAGE ACCESS TOKENS			×
All Tokens Delete 🗸		WCLL_SDn6pQ0HIuVHSjk0XHSR0-w00VzE0u8dq5LC-d5Z5la0xi uXoPChCWO0zUVHSjkVjAg30xQaJinJD9aOPvjirPmc8D9NLL-qL8 D3V5It27nHF8X0QuGn2K3L9Wk0Hg3yF7Jg	
	Token Type	Bearer	
	expires_in	3600	
	scope	offline_access profile openid	
	refresh_token	tE6opgg7UeAU9yqZ-xvrBvWeQXW5XHiYh9g9ufotUM	-1
	id_token	eyJraWQK0LTTRkUxVUTWek1CUnJSWm5uTS1mdTE3Q0k4Uk0151 CMWZoNimd0dURKQkg0fwirWinnijoiUMyNTYifQ eyJzdWK0kwM U12jB5eHhq122wN0QMDVkNybiam5h6MUR0J8EWFuNTALcJ22 XR0jEshinezyBehn0dH8b0k9Z0V21Q007Qh42YU,mH0GEvr29 L29hdXRoM9kZW2hdWx0kiwY9Xikij6iM09hNWRkdmo0bE6EVTE bmm12Dcil.CJpYXQ10jE2NTYwkDMbN2gaImV4cCiEMTY1NjkaNT 30CmianRpijoiSUQub0ozb0UyWEVK2W60WD8yUVNnimpNY1Bik Z20R2V8TFheFM5XDoetVK2yIshimFic88Wj.hdv2Q0SwiiWRkij0 MDBvNWNkaDdiN015bQVNFM12Dcil.CJwcm/m2Xy2WRtd0kic	: 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1

4. Analyze the access token by entering it into the <u>https://jwt.io/</u> token analysis site.

JUT Debugger Lib	raries Introduction Ask Crafted by 🛟 authO
ncoded PAISTE A TOREN HERE	Decoded EDIT THE PRIVLOAD AND SECRET
eyJraWQiOiJTRkUxVU1Wek1CUnJ5Wm5uTS1mdTE 3Q0k4Uk01S1FCMWZoNmd0dURKQkg0IiwiYWxnIj oiUlMyNTYifQ.eyJ2ZXIi0jEsImp0aSI6IkFULm FHRVZwaVBPUkNkSXNuaEUydUZ00WdIZ2U1TFQ4V FJjbGFBNnZZLWI0VFEub2FyaX16cWV1SkR2STJk c2g1ZDYiLCJpc3Mi0iJodHRwczovL2Rldi04NDk 0MTc2Mi5va3RhLmNvbS9vYXV0aDIvZGVmYXVsdC IsImF1ZCI6ImFwaTovL2RlZmF1bHQiLCJpYXQi0 jE2NTYwMDIwNzgsImV4cCI6MTY1NjAwNTY30Cwi Y21kIjoiMG9hNWRkdm00bEdEVTE4bmw1ZDciLCJ 1aWQi0iIwMHU1ZjB5eHhqQ1ZwNGJQMDVkNyISIn NjcCI6WyJvZmZsaW51X2FjY2VzcyIsInByb2Zpb GUiLCJvcGVuaWQiXSwiYXV0aF90aW11IjoxNjU2 MDAyMDc2LCJzdWI10iJ6bWFuMTBAemVicmEuY29 tIiwiRGVwYXJ0bWVudCI6I1BsdW11bW5nIiwiUG 9zdGFsLkNvZGUi0IIxMjM0NTY30DkwQUI1LCJDb 3VudHJ5IjoiVVMiLCJUaXRsZSI6I1N1cGVydm1z b3IiLCJEaXZpc21vb116IkVuZ21uZWVyaW5nIn0 .Keose1BC21NrUI13nZ0gk0J56LatM9- aauQDS1NPo6a- CLgFgZdUQEiAnVv9XQMcX2zVNIFqRynVHj472LS WPGne4z1CcdvH_qXXZjeF4EMgWu0ac3CHrUIknw Ngkwklqvhj9an2U_6vy4Ln0c3_Q2ttV1yjD8ZMC	<pre>HEADER: ALGORITHM & TOKEN TYPE { "kid": "SFE1UMV2MBRryZnnM-fu17CI8RM5KQ81fh6gtuDJBH4", "alg": "RS256" } PARLOAD: DATA { (</pre>

5. Review the decoded payload data and verify the user identification. In this example, the sub claim is the UserID used by Workcloud Communication.



NOTE: Additional claims are shown in this example. You can provide custom access token claims by configuring and mapping attributes in the Okta Directory / Profile Editor. This is not covered in this document.

Configuring the Workcloud Communication System

After validating the basic Okta and ACS configuration, configure the PTT Pro Server. PTT Pro on mobile devices first connects to the PTT Pro Server and uses the URLs to connect to the ACS server, which redirects the user to the Okta system.

The PTT Pro Server requires three configuration parameters:

- Access URL
- Token URL
- Signing certificate
- Log in to the Workcloud Communication PTT Pro Management Portal and navigate to Customer > Profile to configure OAuth.

- 2. Enter the Access URL and Authorization Endpoint URL (OAuth URL) in the Configure OAuth dialog.
 - The Authorization Endpoint URL is the **Oauth URL** field: https://[acs-server-name]/auth/ realms/WFC-Okta-Connector/protocol/openid-connect/auth
 - The Access URL is the Access URL field: https://[acs-server-name]/auth/realms/WFC-Okta-Connector/protocol/openid-connect/token

These are the same URLs used to validate the configuration with Postman and obtained from the JSON output of the well-known URL.

Configure OAuth
OAuth URL: https://www.buckeyuprocestr Access URL: https://www.buckeyuprocestr OAuth Token Certificate: BEGIN CERTIFICATE MIICuTCCAaECBgF/IrJbRTANBgkqhkiG9w0BAQsFADAgMR4wHAYDVQQDDBVXRkMtVEhEL URVY3VtZW50YXRpb24wHhcNMjiwMJjyMTgyODA4WhcNMzIwMjiyMTgyOTQ4WjAgMR4wHA YDVQQDDBVXRkMtVEhELURVY3VtZW50YXRpb24wggEiMA0GCSqGSIb3DQEBAQUAA4IBD wAwggEKAoIBAQCgeGPKhh0LMW5hx/LrkuUcWiJE9IIbeH3z2Us9DPZFRmF9eWHQMnH9rdfv •

 Enter the OAuth Token Certificate. You copied the certificate previously in Retrieving the Signing Certification of the Realm on page 5.

Copy the certificate and paste it into a text editor such as Notepad++. Add Begin Certificate and End Certificate as shown in the example.

```
----BEGIN CERTIFICATE----
```

```
MIICszCCAZsCBgGBpcwvCzANBgkqhkiG9w0BAQsFADAdMRswGQYDVQQDDBJXRkMt
T2t0YS1Db25uZWN0b3IwHhcNMjIwNjI3MTUzMjEwWhcNMzIwNjI3MTUzMzUwWjAd
MRswGQYDVQQDDBJXRkMtT2t0YS1Db25uZWN0b3IwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCacby81fRjEeDXn8VeKaxMBxxuQAkhiC/tnKC6q2MKCWIHES
QqK21HlZ/Pj1HbnDM7GGpBn7zvhQm+aCJ0XjyZiYxy3wkisBJTqdc6JEzdEXwWxkZ
58huenh/PTkpNQy0JLzwCOyzG+iQWWGTYb/xBuBtY9QJoS2yhSHKU53c8txyytLTq
urYNUPTfQC1bcZrQJpeonAmmH4+FjM5sf0IQ2807xD1g69IQ1hiW3+y1CsMoLp4
F68SdQ+pmkwH8jmIdLGWmIn6R1FsccnrdLDiydZc84sZcMCKTMnC9PYu3FGQQzDH
sT1goN+QDDfMhCUzbm1zQ4kSXcOkzHoOaG44zAgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAFv16+3501KPsbEWPUPttNJpWfWGTBpcVGohNmt8e2tfVj0GT7xh4zvNmQv
xh+eaewhzuwKhpT/JG8dyuQVhF4020s2W8YPZqvtLWS0cOY9kljqRl1A3z1o2w0
1IfDU+D5aaGSkylyBxL7HkuJsPoWtwUMyfBZNH14Xp4Scwb25BfddECPSBNCGJ+j
4s1rwfac5YVKTswjcePF+r4VsHzEfTgdMhjJha1wI7GKgzrBXOagZCA6ZfeQMINL
TkBSXW6m+xkkcU/owmMXsGJOTEQOTT0HefiBXq0Jt/0h/NReuc6Qk4AlJHh0Cj9
FhAT2OTPvPbn7Yj3vB7Tne+dMk+p1A=
----END CERTIFICATE--
```



NOTE: Do not add or remove any characters from the certificate because it will cause the authentication to fail.

4. Enter the device serial number in the PTT Pro Server and create OAuth user accounts with an accurate OAuth name.

Modify User (3 of 25 u	sed, 22 remaining) 🔳
User Login:	zman10
Department:	test x -
First Name:	Steve
Last Name:	Zimmerman
OAuth Name:	zman10@zebra.com
Phone Number:	Click to Assign
Email:	
Activation Method:	Trusted Automatic Manual Send Text
Priority:	0
Client Type:	Unknown
	Maximal Contacts
Deactivate Resen	d Activation New Activation Code Submit Cancel

5. Add the JSON configuration to the mobile devices so that the PTT Pro client connects to the ACS server.

```
{
    "oAuthClientID" : "oidc.client",
    "oAuthClientSecret" : "31941cec-9b16-46b8-8749-2e6c3fa4ff23",
    "oAuthBasicHeader" : true
}
```

6. Use a mobile device to verify the configuration. The Okta sign-on screen should display.

2:27 PM 🕅 🖾 🜿 🛦	T A 1			
्राः JEBRA	:			
Connecting to 🗖				
र्री•• ZEBRA				
Sign In				
Username				
Password	0			
Keep me signed in				
Sign in				
< ● ■				

If the device displays a blank screen after entering the credentials, potential causes include a certificate with unprintable characters or white space. Another potential cause is that the Authorization Endpoint URL or Access URL is not correct.

PTT Pro Okta Integration Guide



Revision History

Revision	Date	Description
MN-004831-01EN	January, 2024	First version.



www.zebra.com