PTT Pro and Profile Manager

Workcloud Communication



SAML Integration Guide

2025/04/10

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. ©2025 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/informationpolicy. 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

The support of a shared device model for Workcloud Communication products focuses on AD/ADFS (Active Directory / Active Directory Federated Services) using the OAuth2 protocol. The widespread adoption of PTT Pro and Profile Manager has created the need to support SAML 2.0 (SAML2) as an authorizing protocol.

Keycloak adds the support of SAML2 without changing the current product support of OAuth2. The SAML2 capability is provided by the Authentication Connection Service (ACS), which brokers access authorization between the SAML Identity Management infrastructure and the OAuth2 authorization capabilities of Workcloud Communication.

This guide describes how the ACS architecture is positioned in the Workcloud Communication environment and how to configure the PTT Pro and Profile Manager OAuth authorization services' connection services into the SAML2 Identity Management (IdP) infrastructure.

Document Layout

This guide includes the following sections.

Solution Components and Architecture

Provides a high-level overview of the components, from the mobile device to the IdP server. This section also includes detailed communication flows identifying each component's task and the sequence in which these tasks must occur.

Configure ACS

Describes the ACS configuration process and illustrates the Workcloud Communication to OAuth configuration as well as the SAML2 to IdP configuration elements.

Configure Workcloud Communication

This section describes the system from an operational perspective. Here, the mobile device, Profile Manager, and PTT Pro server configurations are described. The mobile device configuration should be reviewed and adjusted as necessary to produce a smooth user experience.

Troubleshooting

This section describes issues that can be encountered during the configuration process.

Solution Components and Architecture

ACS provides the ability for existing systems to authorize services from a SAML IdP. With the ACS service, no software changes are required for the systems or the SAML infrastructure.



NOTE: based on a customized open-source Keycloak environment. The off-the-shelf Keycloak system does not provide the capabilities described in this document.

ACS Component Diagram

The figure below shows products, including Telephony Manager, which is not involved with OAuth or SAML. Both the PTT Pro and Profile Manager Server use OAuth for user authorization. The ACS server

is the broker between the Workcloud Communication OAuth services and the customer's SAML IdP infrastructure.





User Authorization Diagrams

The following ladder diagrams illustrate the sequence of authentication events and which component performs which function.

The first illustration shows the existing PTT Pro OAuth sequence to an AD/ADFS infrastructure. This is provided for the administrator to understand operations before introducing ACS.

After the administrator understands the AD/ADFS (Active Directory / Active Directory Federated Services) operations, the next diagram introduces ACS and how the flow of authorization is transferred or converted from OAuth to SAML. Both PTT Pro and Profile Manager servers are shown.



Figure 2 PTT Pro Shared Device Using OAuth2

Once an understanding of the AD/ADFS (Active Directory / Active Directory Federated Services) is developed, the following diagram shows the introduction of ACS and in a standalone PTT Pro configuration.





The following ladder diagram describes the flow of authorization in a deployment with Profile Manager servers.





Prerequisites

The ACS is supported for the software versions listed below. In addition, it requires TCP port 443.

Minimum software versions

- PTT Pro server v4.7.3.1
- PTT Pro client v3.2.10084
- Profile Manager client v 2.0.19406
- Voice Client v9.0.19409 (The Voice client does not require OAuth or SAML for authentication.)
- Profile Manager server v1.14.34

Firewall ports

The ACS is a cloud service that requires access to the following ports.

- TCP port 443 for the URL to the ACS service
- Web browser access to the ACS service

Configure ACS

You configure the ACS service by developing a configuration for OAuth communications and a configuration for SAML connectivity.

Create a Realm

The configuration requires creating a realm that contains both the OAuth configuration and the SAML configuration. The Oauth configuration is used by Workcloud Communication applications, and the SAML configuration is used to connect to the SAML server.

Configure the realm with two endpoints:

- OpenID Endpoint (OAuth): from the ACS service perspective, this is called the Client.
- SAML2.0 IdP Endpoint: from the ACS service perspective, this is called the Identity Provider.

Create the OAuth Client

The OAuth client communicates with the PTT Pro server and the Profile Manager using the OAuth protocol.

- 1. Configure the Client ID, Protocol (OAuth), Access Type (Confidential), and Redirect URI.
- 2. Configure the credentials. Select a client authentication of Client ID and secret (automatically generated), which correspond to the PTT Pro JSON parameters of oClientId and oAuthClientSecret.
- 3. Map the username parameter to unique_username, which is what the system uses.

Create the Identity Provider

The identity provider communicates with the SAML server using the SAML protocol.

- **1.** Obtain the SAML descriptor file.
 - Configure the Single Sign-On Service URL.
 - Configure security settings such as Signature Validation (enable), the Signature Algorithm (RSA256), and the Validating x 509 Certificate.
 - Map the User ID entity from the IdP (SAML protocol) to the client (OAuth protocol).
 - Create a default authentication to automatically launch the IdP authentication.
- 2. Export certificates to the IdP and to the PTT Pro server.
 - Export the ACS SAML certificates to the SAML server.
 - Copy the certificate into a .pem file to the SAML server.
 - Import the .pem file into SAML server.
 - Export the ACS Realm certificate to the PTT Pro server and copy the certificate into the PTT Pro OAuth configuration.

Creating a Realm

Create a realm to contain the OAuth configuration and the SAML configuration. The OAuth configuration is used by Workcloud Communication applications, and the SAML configuration is used to connect to the SAML server.

1. Browse to the assigned ACS service and sign in.



Existing realms are shown in the right pane. There will always be at least one Master realm.

- 2. Create a new realm by clicking Select Realm in the left pane.
- 3. Configure the realm.
 - a) Enter the Realm name in the Realm Name field.
 - b) Set Enabled to ON.
 - c) Click Create.

The new realm should be selected in the left pane. It is important to ensure you have switched to the correct realm in the left pane realm drop-down to prevent the configuration of the Master realm.

t of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolate	d from one an	other and	an only manage and authenticate the users	that they control.
Drag a file here or browse to upload	Browse	Clear		
WFC-SAML-Test-Realm				
	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolate Drag a file here or browse to upload 1 Upload a JSON file WFC-SAML-Test-Realm On	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one an Drag a file here or browse to upload Browse 1	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and o Drag a file here or browse to upload Clear Upload a JSON file WFC-SAML-Test-Realm On	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users Drsg a file here or browse to upload Clear Upload a JSON file UPIC-SAML-Test-Realm Con

Creating the Clients

Create the OAuth client used by the PTT Pro and Profile Manager servers.

When you select **Clients** in the left pane, the right pane displays the default client listing for the Realm. The **Client ID** column shows that the **account** and **security-admin-console** fields are automatically populated with the URL for the Realm.

1. Click Create to display the Add Client dialog.

Clients are applications and services that can request authentication of a user. Learn more C Clients list Initial access token					
Q. Search for client ->	Create client	Import client			
Client ID	Туре	Description	Home URL		
account	OpenID Connect	-	https://dp-devl.wfc.zebra.com/realms/WFC-SAML-Test-Realm/account/ 🗹		
account-console	OpenID Connect	-	https://dp-devl.wfc.zebra.com/realms/WFC-SAML-Test-Realm/account/ 🗹		
admin-di	OpenID Connect	-	-		
broker	OpenID Connect	-	-		
realm-management	OpenID Connect	-	-		
security-admin-console	OpenID Connect	-	https://idp-devt.wfczebra.com/admin/WFC-SAML-Test-Realm/console/ 🗹		
WFC-SAML-test	OpenID Connect	-	-		

- **2.** Configure the client.
 - a) Enter a name in the **Client ID** field. This name is used in the PTT Pro client configuration JSON file as the value for the oAuthClientID parameter.
 - **b)** Select openid-connect from the **Client Protocol** drop-down menu.

Clients > Create client		
Create client Clients are applications and serv	vices that can request authe	ntication of a user.
1 General Settings	Client type 🕥	OpenID Connect
	Client ID * 🕤	
	Name 🛞	
	Description ③	
	Always display in console 🕤	Off
	Next Back	Cancel

c) Click Next.

The Capability Config Settings appears.

Configuring the Capability Settings

- 1. Select the Standard Flow and Direct Access Grants checkbox under Authorization Flow to enable.
- 2. Enable Client authentication.

3. Click Save to display the rest of the settings.

Capability config Autherization © Off Autherization © Off Autherization flow © Standard flow © Direct access grants © Implicit flow © Service accounts roles © OAuth 2:0 Device Authorization Grant © OIDC CIBA Grant ©	General Settings	Client authentication (9 () Off	
Authentication flow Implicit flow () Implicit flow () Implicit flow () Implicit flow () Output 2.0 Device Authorization Grant () OIDC CIBA Grant ()	Capability config	Authorization ()	O off	
Implicit flow Service accounts roles Authorization Grant OIDC CIBA Grant		Authentication flow	Standard flow 🛞	Direct access grants
OAuth 2.0 Device Authorization Grant () OIDC CIBA Grant ()			Implicit flow ()	Service accounts roles @
OIDC CIBA Grant @			OAuth 2.0 Device Authori	zation Grant 🛞
			OIDC CIBA Grant @	
		Save Back	Cancel	
See Ret Covel		and here	Taoline Party P	

Configuring the Access Settings

Procedure to configure the Access settings for the OAuth client endpoint.

Enter https://localhost in the Valid Redirect URI field.

Access settings		
Root URL ①		
Home URL 🗇		
Valid redirect URIs 🗇	https://locabost	¢
	Add valid redirect URIs	
Valid post logout		4
redirect URIs ①	Add valid post logout redirect URs	
Web origins ①		4
	O Add web origins	
Admin URL ①		

Configuring the Endpoint Settings

Configure the settings for the OAuth client endpoint.

1. Set Enabled to ON.

wFC-SAML-Test-Realm +	Cleme > 10FCSAULinest		
Contra o	WFC-SAML-test #		
la Barte Lerrer	Settings Credentials Roles Client	Icopes @ Mappers @ Scope @ Revolution Sessions @ Offine Access @ Custering Installation @	
a contractor			
S Clart Sciper	Clerifie	INCOMP. WE	_
E fam	Nama D		
11 Identity Providers	Descriptor @		
E User federation	Enabled ()		
E Authentication	Consert Required @	011	
Harage	Login There @		
6. Service	Cherry Restored B.	and a start	-
£ Uwes			<u> </u>
O Sessions	Access Type @	ordena	-
E terts	Standard Row Brakiled @		
	Implicit Flow Stabiled ID	(SFE	
11 10000	Direct Access Grants Drafited ()		
	Service Accounts Brutiled @	001	
	Authorization Brabied @	3W	
	Rest URL 0		
	* Valid Redirect URs @	https://teathord	-
	Berr UR, O		
	Admin URL D		
	Web Orgina B		٠
	> Fine Grain OpenID Connect Configur	ation Ø	
	> OpenID Connect Compatibility Mode	50	
	Advanced Settings @		
	> Authentication Flow Overrides @		
		fame famed	

- 2. Select Confidential from the Access Type drop-down menu.
- 3. Enter https://localhost in the Valid Redirect URI field.

This field is required but is not used for this implementation. It enables Keycloak to call back to its resource manager.

4. Click Save to display the Credentials tab.

Configuring the Endpoint Credentials

Configure the endpoint credentials to create the secret key.

1. Select Client ID and Secret from the Client Authenticator drop-down menu.

This generates a random client secret.

Settings	Keys	Credentials	Roles	Client scopes	Sessions	Advanced		
Client Auther	vticator	Client Id and	Secret					
_		Save						
Client secret							0 j i	Regenerat

2. Copy the values of the client name and the client secret key to configure the PTT Pro client.

The secret key, along with the client name must be configured in the JSON configuration file of the PTT Pro client.

Example

```
"oAuthClientId": "WFC-SAML-test"
"oAuthClientSecret": "0504258e-5987-49af-a1d0-c33a7a3bee1b"
```

Configuring the Endpoint Mappings

Map the Oauth username to the SAML username.

- **1.** Select the **Client Scopes** option on the left pane.
- **2.** Select **offline_access** scope under client scopes in the right pane.

This is the built in scope for **openID connect**.

3. Select the **Mappers** tab and select **By configuration** from **Add Mapper** drop-down box. **By configuration**.

Client scopes > Client scope details offline_access (spanid-connect Settings Mappers Scop	e					
Q. Search for mapper →	Q. Search for mapper → Add mapper →					
Name	From predefined mappers	lory	Туре			
family name	By configuration	mapper	User Property			
unique_name	Toke	n mapper	User Attribute			
email	Toker	n mapper	User Property			

4. Click User Attribute.

Client scopes > Client sc	cope details > Mapper details
User Attribute d507c504-9a15-4e42-	9103-9f1aa65304b8
Mapper type	User Attribute
Name * 🕐	unique_name
User Attribute 💿	username
Token Claim Name 💿	unique_name
Claim JSON Type 💿	String
Add to ID token ⑦	On On
Add to access token ⑦	On On
Add to userinfo ③	On On
Multivalued ⑦	Off
Aggregate attribute values ⑦	Off
	Save Cancel

- 5. Enter the following details:
 - a) Enter unique_name in the Name field.
 - **b)** Enter username in the **User Attribute** field.
 - c) Enter $\texttt{unique}_\texttt{name}$ in the Token Claim Name field.
 - d) Enable the Add to ID token, Add to access token, and Add to userinfo.



NOTE: This value might be different based on your implementation.

6. Click Save.

The SAML username is returned as the **OAuth Name** in each user definition of the PTT Pro server.

Add User (2052 of 100	00 used, 7948 remaining)	×
User Login:	Sabastian	1
Department:	EP.Lab *	
First Name:	Sabastian]
Last Name:	Sturzenegger	
OAuth Name:	Sabastian]
Phone Number:	(201) 555-5555	
Email:]
	Trusted	
	Send Text	
Priority:	0 0	
Client Type:	Unknown	
	Maximal Contacts	
		Submit Cancel

SAML Descriptor File

The SAML Descriptor file provides information needed to configure the ACS service.

A sample SAML Descriptor file is shown below. You can also view a sample file at the <u>Sample Descriptor</u> <u>File</u> link.

You can access the Descriptor file from the Keycloak user interface. Navigate to the **Realm Settings** > **General** tab. Click on the **SAML 2.0 IdP Metadata** field under **Endpoints** to reveal the descriptor file.)

In the example Descriptor file below, the following lines contain the information needed to configure the ACS service.

- The tag <dsig:x509Certificate> on line 10 contains the x509 certificate to import into the ACS service to provide access to the IdP.
- The tag <SingleLogoutService> on line 15 contains the URL to be copied into the SAML Single Logout Service URL in the ACS service.
- The tag <SingleSignOnService> on line 29 contains the URL to copy into the SAML Single Sign-On Service URL in the ACS service.



1	
2	CEntitiesDescriptor xmlns="urn:oasis:names:to:SAME:2.0:metadata" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Name=
	Untrive Descriptor antitut TB"https://wfo.kewoloak2.pttpro_sabra_com/auth/yaalms/MEP-SAMI-Test-Baalm">
4	Contractive Section of the section o
	Claubacrister una finizzation and
6	
2	(deig: FeyName) M/281 of F370 FHE/kHod/ky@0a/kb/f6Bok0Y700++v045//deig: FeyName)
8	Colera XS09Data>
	Contract (figure)
10	MIICTCCA20CBgFw07lh1zANBgkqhki09w0BAQsFADAeMRwwGgTDVQQDDBNXRkMtU0FNTC1VZXN0LVJ1YWxtMB4ZDTIwMDIxNzElMTUyMIoXDTMwMDIxNzElM TowHIowIjEeMBoALUEAwwTV0EDLVNBTVwtV0VadCISERFabTCCASIw0gTNoElhvcNAGEBDQADggEPADCCAQoCggEBALyanpwSTc9G0uvym4yzEtDiu4%Ap Aaqnj80t11LE5TTzyh0RbiG9tGr86jXFz1FdkZV6GST1FT43z225VUE+eNGgoCun6isMyXjwzHprkHNNO+BnZ9ulExzT7nfp4F8k/FABTkETqhzqla+121n olu55v/1+v7oJvkn7+AZzc55w60JR/7vha1/aDfS0uofs1DvL1hqPLxtL16PobbBc9kFMSNOm9vs/TyTkracoyCa28H4i+0tGPDEzETPyMirFXOFQ XlukMaDkABAnZap6HBPyZu+RuA+6xhQBrb8ddobeU7E2obltOXtkzbq6bh1FBDHDHDJ7UI0CAWEATANBgkqhki09w0BAQsFAAOCAQEANG24BxiAv1gtk32qd D4w%5pXnmj16MH4Z9mfzAn41H1w7+H131jrK66EswBGa7djRG11aHsPxRv7JNF6DWFCiG4VhOwcK56GD219irpADHCmdAoxTnLoy5kGq6HvofK/MSM4FG3E idh115bOgVpzA0wAnaFFHFebueJVH08Puv+JAqaMEkKH/P0VrchCidfeMAaMa/6ws1X6LQVB7DD0c28LE01Hnu2erv55eR+agRL/6t04jUNIF2/C+2u1pB r5Vkw0bH1rZpmon/jfu+Q0TAO310Bbe/90DaBzNQdiAqyXbXpmeH09F0FL426Mm2KiSL07hzE75koQ==
11	
1.2	
13	
14	-
15	<pre><singlelogoutservice binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-POST" location="</pre"></singlelogoutservice></pre>
	"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml*/>
16	<pre><singlelogoutservice binding="urn:oasis:names:to:SAML:2.0;bindings:HTTP-Redirect" location="</pre"></singlelogoutservice></pre>
	"https://wfo-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml=/>
17	© <nameidformat></nameidformat>
18	urn:oasis:names:to:SAML:2.0:nameid-format:persistent
19	-
20	E
21	urn:oasis:names:to:SAML:2.0:nameid-format:transient
22	-
23	<pre>GeneIDFormat></pre>
24	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
25	-
26	E (Name IDFormat)
27	urn:oasis:names:to:SAML:1.1:nameid=format:emailAddress
28	
29	<pre>designOnService Binding**urn(oasis(names(to)SAME(2.0)bindings(MTTP-POST* Location*)</pre>
	"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
	<pre><singlesignonservice binding="urn:oasis:names:to:SAME:2.0:bindings:MTTP-Redirect" location="</pre"></singlesignonservice></pre>
	"https://www.meyoloaxz.pttpro.mebra.com/auth/realms/MPC-XAML-Test-Reals/protocol/saml"/>
31	<pre>coinglesignonService Binding="urn:oasis:names:to:SAME:2.0:Dindings:SOAP" Location=</pre>
	"https://wto-keyoloakz.pttpro.zebra.com/auth/realms/WFC-KAML-Test-Realm/protocol/saml"/>
32	-/IDF30Descriptor>
33	

34 </EntitiesDescriptor>

Configuring the Identity Provider

Use the information from the SAML Descriptor file to configure the Identity Provider.

1. Click Identity Providers in the left pane of the Keycloak user interface.

WFC-SAML-Test-Realm	Identity providers Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. Lea	im more 🗹
Manage		
Clients	Q, Search for provider	
Client scopes		
Realm roles	Name	Provider details
Users	sami	Sami
Groups		
Sessions		
Events		
Configure		
Realm settings		
Authentication		
Identity providers		
User federation		

- 2. Select SAML v2.0 from the Add Provider drop-down menu.
- **3.** Enter the redirect URL in the **Redirect URI** field. The **Redirect URI** entry is constructed as follows: <u>https://wfc-keycloak.pttpro.zebra.com/auth/realms//broker/ /endpoint</u>.

The <Alias>is a convenient label. Change it to an appropriate value. In this example, the alias is WFC-SAML-Auth that results in the following redirect URI: <u>https://wfc-keycloak.pttpro.zebra.com/auth/realms/</u><u>WFC-SAML-Test-Realm/ broker/WFC-SAML-Auth/endpoint</u></u>

- 4. Set the Entity Descriptor on.
- 5. Enter the SAML descriptor URL in the SAML entity descriptor field.

The SAML descriptor URL pulls all the SAML endpoints, certificates etc from the SAML identity provider.

6. Click Save.

Settings Mapper	rs Permissions	
General settings		Jump to section
Redirect URI	https://idp-devLwfc.zebra.com/realms/WFC-SAML-Test-Realm/broker/saml/endpoint	General settings
Alias * (1)	sani	SAML settings
Display name		Requested AuthnContext Constraints
Display order ①		Advanced settings
Endpoints ①	SAML 2.0 Service Provider Metadata 🕑	
SAML settings		
Service provider entity ID ①		
Identity provider entity ID ①	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm	
Single Sign-On service URL * ③	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm/protocol/saml	
	Save Revert	

7. Configure the SAML details.

Settings Mapper	s Permissions	
General settings		Jump to section
Redirect URI ()	https://idp-devLwfc.zebra.com/realms/WFC-SAML-Test-Realm/broker/saml/endpoint	General settings
Alias * ©	sani	SAML settings
Display name 🗇		Requested AuthnContext Constraints
Display order ①		Advanced settings
Endpoints ()	SAML 2.0 Service Provider Metadata 🗹	
SAML settings		
Service provider entity ID ①		
Identity provider entity ID ③	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm	
Single Sign-On service URL * ①	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm/protocol/saml	

a) Enter the single sign-on URL in the Single Sign-On URL Service field.

The Single Sign-On Service URL can be copied from the <SingleSignOnService> parameter in the **SAML Descriptor** field. In this example it is:

https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/ protocol/saml

b) Enter the single logout service URL in the Single Logout Service UR field.

The Single Logout Service URL can be copied from the <SingleLogoutService> parameter in the SAML Description field.

- c) Enable Validate Signature.
- d) Enable HTTP-POST Binding Response.

PTT Pro and Profile Manager SAML Integration Guide

SAML settings		Jump to section
Service provider entity ID ①		General settings
Identity provider entity ID ①	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm	SAML settings
Single Sign-On service URL * ①	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm/protocol/saml	Requested AuthnContext Constraints Advanced settings
Single logout service	https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm/protocol/saml	
Backchannel logout	Off Off	
NameID policy format	Persistent	
Principal type ①	Subject NameID •	
Allow create ①	Con	
HTTP-POST binding response ③	On	
HTTP-POST binding for AuthnRequest ③	On On	
	Save Revert	

- e) Enable HTTP-POST Binding for AuthnRequest.
- f) Enable HTTP-POST Binding Logout.
- g) Enable or Disable Want AuthnRequests Signed.
- h) Click Save.

HTTP-POST binding legevit ③	On On	Jump to section
Want AuthinRequests signed ①	Con Con	General settings
Signature algorithm	RSA_SHA256 -	SAML settings
SAME, signature key name	KEV_ID •	Requested AuthinContext Constraints Advanced settings
Want Assertions signed ①	Off Off	
Want Assertions encrypted ①	CM Off	
Force authentication	CM Off	
Validate Signatures ①	Con Con	
Validating X509 certificates ①	MICTTCCA20CBgGJTNCqvjAN8gkqhikG9w0BAGsFADAeMRwwGgYDVGG00BN0RkMtU0FNTCTU20N0LVJYWr	
Sign service provider metadata ©	Off Off	
Pass subject (3)	OT Off	
	Save Revert	

Mapping the User Name from the IDP

ACS uses the user name for the roles and profile assignments in the Workcloud Communication environment. The user name is mapped to the correct profile on the device when the user signs in.

1. Select the Mappers tab.

E ORKEYCLOAK			
WFC-SAML-Test-Realm •	Identity providers > Pro	vider details > Edit Identity Provider Mapper	
Manage	Edit Identity P	rovider Mapper	
Clients			
Client scopes	10	usemame	
Realm roles	Name * ①	usemame	
Users			
Groups	Sync mode override *	Inberit	•
Sessions	Ū.		
Events	Mapper type 💿	Username Template Importer	•
	Template 🔿	\${ATTRIBUTE.username}	
Configure			
Realm settings	Target ①	LOCAL	•
Authentication			
Identity providers		Save Cancel	
User federation			

- 2. Enter username in the Name field.
- 3. Select Username Template Importer from the Mapper type drop-down box.
- 4. Enter \${Attribute.name} in the **Template** field.

This enables the **username** field from the IdP to pass to the OAuth services. The attribute name comes from the IDP and may differ in your environment.

5. Enter any additional attribute mapper for firstName, and lastName field.

Saml			
Settings Mappers	Permissions		
Search for mapper	→ Add mapper		
lame	Category	Туре	
instName	Attribute Importer	Attribute Impo	rter
semane	Preprocessor	Usemame Terr	plate Importer
otNome	Attribute Importer	Attribute Impo	rter
Edit Identity P	rovider Mapper		
Edit Identity P	firstName		
Edit Identity P	firstName		
Edit Identity P	firstName		
Edit Identity P	firstName firstName		•
Edit Identity P	firstName firstName Inherit Attribute Importer		•
Edit Identity P ID Name * ① Sync mode override * ⑦ Mapper type ① Attribute Name ⑦	firstName firstName Inherit Attribute Importer firstName		•
Edit Identity P ID Name * ③ Sync mode override * ⑦ Mapper type ③ Attribute Name ③ Friendly Name ③	firstName firstName Inherit Attribute Importer firstName First Name		•
Edit Identity P	firstName firstName Inherit Attribute Importer firstName First Name ATTRIBUTE_FORMAT_BASIC		•



NOTE: In case of Azure AD, following attribute mapping needs to be done for **username**, **firstName**, **lastName**, and **email** fields.

Auto Launching the SAML Login

Configure SAML to automatically launch the SAML login page when the mobile device connects to the ACS.

1. Navigate to the Authentication view.

WFC-SAML-Test-Realm •	Authentication Authentication is the area where you can configure and manage different oredential types. Learn more 🗹				
Clienta	Flows Required actions	Policies			
Client scopes	Q, Search for flow 🔶	Create flow			
Realm roles					
Users	Flow name	Used by	Description		
Groups	browser (Built-in)	O Drowser flow	browser based authentication		
Sessions	clients Duit-in	Client authentication flow	Base authentication for clients		
Events	drect grant Built-in	O Direct grant flow	OpenID Connect Resource Owner Grant		
Continue	docker auth Built-in	O Docker authentication flow	Used by Docker clients to authenticate against the IDP		
Realm settings	registration Built-in	Registration flow	registration flow		
Authentication	reset credentals Built-in	Reset credentials flow	Reset credentials for a user if they forget their password or something		
Identity providers	first broker login Built-in	Specific providers	Actions taken after first broker login with identity provider account, which is not yet linked to any Keydoek account		
User federation	custom first broker login	Not in use	Actions taken after first broker login with identity provider account, which is not yet linked to any Keycloak account		
	http://walange.@ult-in	Not in use	An authentication flow based on challenge-response HTTP Authentication Schemes		

2. Select the Flows tab.

E.

- 3. Click the Browser link.
- 4. Click Settings in the Identity Provider Redirector step.

Steps	,	lequirement	
н	Cookie	Alternative	-
н	Kerberos	Disabled	-
н	Identity Provider Redirector	Alternative	• 0
н	 forms Username, password, otp and other auth forms. 	Alternative	•
н	Username Password Form	Required	
н	 Browser - Conditional OTP Flow to determine if the OTP is required for the authentication 	Conditional	•

- 5. Enter a name in the the Alias field.
- 6. Enter the client string of the Identity Provider in the Default Identity Provider field.

For more information, see Configuring the Identity Provide for the client string. In this example, the client string is WFC-SAML-Auth.

7. Click Save and then Close.

Identity	Identity Provider Redirector config ×				
Alias * 🗇	Alias * 💿				
launch_san	nl				
Default Ident	Default Identity Provider ③				
Save	Save Cancel Clear				

8. Click First broker login flow under Flows tab.

Update any steps details if needed. For e.g Review Profile, Handle Existing Account etc. Refer Keycloak user manual for more details on each configuration details. By default, there is no change required for any of the steps .

Exporting the ACS Certificate to SAML

Establish trust from the ACS to the SAML server.

- 1. Navigate to the Identity Providers view.
- 2. Click Endpoints URL to display the descriptor file from the ACS instance.

Identity providers 🔸 Pro	vider details
Saml	
Settings Mappe	rs Permissions
General settings	
Redirect URI	https://idp-devl.wfc.zebra.com/realms/WFC-SAML-Test-Realm/broker/saml/endpoint
Alias * ③	sami
Display name 💿	
Display order ③	
Endpoints ③	SAML 2.0 Service Provider Metadata 🗹

- 3. Copy the x509 Certificate and paste it into a text file with a file extension of <filename>.pem.
- 4. Import <filename>.pem into the SAML server.

Exporting the ACS Certificate to PTT Pro

Export the ACS certificate to the PTT Pro server. The PTT Pro server requires a certificate for the OAuth connection to Keycloak.

1. Navigate to the Realm Settings and select the Keys tab.

WFC-GAML-Text-Headen	WFC-SAML-Test- Realm settings are settings	Realm that control the options for users, applics	etions, roles, and groups in the current realm. Learn more 😫		Crubbed Action •
Gireta	General Login	Enal Thenes Keys Events	Localization Security-defenses Sessions Tokens	Client policies User registrat	lon.
Client scopes	Keysilet Providen				
Realm roles	T Active laws	Q. Search key			10 · ()
Users					
Groups	Algorithm	Type	Ka	Provider	Public large
Sessions	H1104	007	contracts only and also beautions	have exceeded	
Events	1000	00.1		and growing	
Configure	R5256	RSA	784494,633949325a940476W8w734RumD5cEn8U	rsa-penerated	Public key Certificate
Realm settings					
Authentication	AES	007	45440420-633c-4868-6946-088664245589	are-generated	
identity providers					
User federation					1.3 * ()

2. Click on Certificate in the RS256 row.

M

WFC-SAML-Test-Realm Realm settings are settings that control the opti-	ns for users, applications, roles, and groups in the current realm. Learn more 🗹		C Enabled Action •
General Login Email Themes	Certificate ×	Client policies User re-	
Keysilat Providers	MIC:TCCA20CBgGJS3HULTANBpkphkG9w0BAQuFADAeMRawGgY		
T Active keys • Q, Search key	DVGGDDBROBANLOFTTELDENGLEVHILMBAKDTBROGMERAD krOFWDTMLMDolMjEAVTELDENHIEGHBIGAUEANINVOZDU/NBT UNTVSVIdCISZWEIbTCCASINDOVKOZDNICHAGEBBGADgEFADOC ADC/2020/EDMIN_2C3.ut520/EC320.ntmin/pd0/2020/EDBIBB		1-3 * - (-)
Algorithm Type	NSisJUa/IN/O/AuLNeMSEOGGN/kgG5TU8Ukt09d=ITy=akCmy8cepecJ	Presider	Public keys
H5256 OCT	Hung Heleoguesia puriocradul antication activity appendiated a Agronetic contribution of the Antication activity and a automative activity and antication activity and antication activity of Wald Charles and and an antication activity and activity and activity of wald Charles and and an antication activity and activity of the act	hmac-generated	
R5256 R5A	Ys-leu/Cirp8CAwEAATNNBpkpMiG9w08A0sFAADCAGEAFCI8DT7A 659/70-656/birEp4exik3Ms/M89eOx1T6xGLN099ig8PT45KV2w7T Ud.20xgDexL3mmNY10xq860.30Y55L3x1W9K0M_Shitum84cHe 7x1-0x20xgDexL3mmNY10xq860.30Y55L3x1W9K0M_Shitum84cHe	rsa-generated	Publickey Certificate
AES OCT	13H-2xpppug - zminimessa sina eryekise i UUKyr UHWAL+EW w&THCYx05(/aux200370veOUAPe02y7+R, Pellos TMHeDJ468k YR30tavyNcbjA8CswgR-Jtm/tpg-Rc36AMitaDA8, wlyxN04X7MI whT1Ls6H0CH70Mr0VCB0mR04555ta16e-c2022mfa8-H68Ja	ass-generated	
	NaWyer+ Cove Cancel		1+3 • ()

3. Copy the certificate to the OAuth definition in the PTT Pro portal, as shown below.

NOTE: The CR/LF characters are critical for the server to properly digest the certificate.

```
----Begin Certificate---- <CR/LF> <Certificate information pasted here> <CR/LF>
```

Configure OAuth	
OAuth UF	L: https://wfc-keycloak.pttpro.zebra.c
Access UF	L: https://wfc-keycloak.pttpro.zebra.c
OAuth Tok	en
Certifica	te:
BEGIN CERTIFIC	CATE
/IIICtTCCAZ0CBgFv	vU7CcpTANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDDBNXRkMtU0F
VTC1UZXN0LVJIYW	/xtMB4XDTIwMDIxNzE1MDU0OFoXDTMwMDIxNzE1MDcyOFowHjEcMB@
3A1UEAwwTV0ZDL	VNBTUwtVGVzdC1SZWFsbTCCASIwDQYJKoZIhvcNAQEBBQADggEPAI
CAQoCggEBAIU20	h2bfqoo5sES3YugRGHB/grQA9AgOwG+Qd0+R1KB3UCpCzQBjwXaLhO

4. Click Submit.

Configure Workcloud Communication

After you have configured the ACS service, configure the Workcloud Communication servers and clients.

This section describes the configuration of:

- Profile Manager
- PTT Pro Server
- PTT Pro for Android
- Profile Client

Configure Profile Manager

The Profile Manager server requires four configuration elements to connect to an OAuth server because the Profile Manager uses OAuth to authorize users. Using ACS requires that the Profile Manager use the Keycloak server instead of an ADFS server.

The four configuration elements you need to configure Profile Manager administrator are:

- Authentication URL
- Access Token URL
- Client ID
- Client secret

Authentication URL and Access Token URL

The Authentication URL and the Access Token URL are obtained by clicking on the **OpenID Endpoint Config** under the **General** tab in the **Realm Settings**.

WFC	SAML-Test-Realm 🗸	WFC-SAML-Test-Rea	lm 👕
Config		General Login Keys	Email Themes Cache Tokens Client Registration Security Defens
- 18	Realm Settings	* Name	WFC-SAML-Test-Realm
Ð	Clients	Display name	KevCloak-Primary
&	Client Scopes	Display name	ney-under Friendry
=	Roles	HTML Display name	
=	Identity Providers	Frontend URL @	
8	User Federation	Enabled ©	ON
-	Authentication	User Managed Lawrence	015
Manai		User-Managed Access @	Urr
		Endpoints @	OpenID Endpoint Configuration
⁴⁴	Groups		SAML 2.0 Identity Provider Metadata
-	Users		Save Cancel
Ø	Sessions		

The Authorization Endpoint is copied to the OAuth URL in the PTT Pro server and provided to the Profile Manager administrator.



The Token Endpoint URL is copied to the Access URL in the PTT Pro server must be provided to the Profile Manager administrator.



Client ID

The **Client ID** is the name of the clients in the configured realm. In this example, the Client ID is WFC-SAML-test. The Client ID must be provided to the Profile Manager administrator and included in the PTT Pro JSON configuration file.

Figure 6 Client ID

0	KEYCLOAK							
WFC-SAML-Test-Realm 🗸		Clients > WFC-SAML-test						
Config			WFC-SA	ML-test 🍵				
	Realm Settings		Settings	Credentials Roles	Client Scopes 🚱	Mappers 🚱	Scope 😡	Revocati
Ð	Clients			Client ID @	WFC-SAML-test			
	Client Scopes			N0				
	Roles			Name 🥑				
	Identity Providers			Description 😡				
	User Federation			Enabled 😡	ON			
	1.46							

Client Secret

The client's secret is also found in the Clients definition. Open the **Clients** definition of the realm and navigate to the **Credentials** tab to reveal the **Secret**. The secret must be provided to the Profile Manager administrator and included in the PTT Pro client JSON configuration file.



WFC-SAML-Test-Realm 🗸		Clients > WFC	-SAML-test					
Config	ure	WFC-SA	ML-test 1	Î				
111 Realm Settings		Settings	Credentials	Roles	Client Scopes 😡	Mappers 😡	Scope 😡	Revocatio
•	Clients		Client Authentio	ator 😡	Client Id and Secret	•	1	
&	Client Scopes					4 10 00 7 01	1	
	Roles			Secret	0504258e-5987-49af	-a1d0-c33a7a3bee	:1b	
🚍 Identity Providers								
	User Federation	Reg	gistration access to	oken 😡				
	Authentication							
Manaş	36							
	Groups							
1	Users							

Configure the PTT Pro Server

The customer profile in the PTT Pro server supports an OAuth connection. Modify the configuration to use Keycloak for user authorization.

The configuration of the PTT Pro server requires:

- OAuth URL
- Access URL
- OAuth Certificate

Figure 8 PTT Pro OAuth Configuration

Configure OAuth	×
OAuth URL: https://wfc-keycloak.pttpro.zebra.c Access URL: https://wfc-keycloak.pttpro.zebra.c OAuth Token	
BEGIN CERTIFICATE MIICtTCCAZ0CBgFwU7CcpTANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDDBNXRkMtU0F NTC1UZXN0LVJIYWxtMB4XDTIwMDIxNzE1MDU0OFoXDTMwMDIxNzE1MDcyOFowHjEcMBo GA1UEAwwTV0ZDLVNBTUwtVGVzdC1SZWFsbTCCASIwDQYJKoZIhvcNAQEBBQADggEPAD CCAQoCggEBAIU2oh2bfqoo5sES3YugRGHB/grQA9AgOwG+Qd0+R1KB3UCpCzQBjwXaLh0	
Submit Cancel	

If you are using a shared device model using OAuth:

- The device serial numbers must be provisioned in the server.
- The User definition requires that the Oauth Name field is populated correctly, as shown below. The Oauth name must match the username in the SAML server.



Modify User (4 of 25 u	sed, 21 remaining)
User Login:	steve
Department:	WFC.SAML.Test × *
First Name:	Steve
Last Name:	Zimmerman
OAuth Name:	steve
Phone Number:	Click to Assign
Email:	
Activation Method:	Crusted Automatic Manual Send Text
Priority:	0 2
Client Type:	Unknown Maximal Contacts
Deactivate Resen	d Activation New Activation Code Submit Cancel

Obtain the OAuth and Access URLs

You can find the OAuth and Access URLs in the Keyloak server or from a URL.

To find the URLs through the KeyCloak user interface, navigate to **Realm Settings** and click on **OpenID Endpoint Configuration** under **Endpoints**.

WIKEYC LOAK		
WFC-SAML-Test-Realm ~	WFC-SAML-Test-Realm 🝵	
Configure	General Login Keys Email	Themes Cache Tokens Client Registration Security Defenses
111 Realm Settings	* Name	WFC-SAML-Test-Realm
Clients	Display name	
🛞 Client Scopes		
📰 Roles	HTML Display name	
☐ Identity Providers	Frontend URL @	
User Federation	Enabled @	ON CON
Authentication	User-Managed Access @	OFF
Manage	Endpoints @	OpenID Endpoint Configuration
社 Groups		SAML 2.0 Identity Provider Metadata
≗ Users		Env Count
 Sessions 		Save Cancer
🛗 Events		
Import		

Figure 10 OpenID Endpoint Configuration

To find the URLs through a web link, substitute <WFC-SAML-Test-Realm> with the name of the Realm in the following URL:

https://wfc-keycloak.pttpro.zebra.com/auth/realms/<WFC-SAML-Test-Realm>/.well-known/openid-configuration

The output from the Keycloak user interface and the URL are shown below.

Figure 11 Authorization URL for PTT Pro OAuth URL Field

A A A A A A A A A A A A A A A A A A A					
C 7 G Q * #dcappda2.ptpprocess.com/subjustment/WC-SML-bit Reserved encounterpress.com/ptpprocecom/subjustment/WC-SML-bit Reserved encounterpress.com/subjustment/WC-SML-bit Res Reserved encounterpress.com/subjustment/WC-SML-bit Reserved encounterpress.com/subjustment/WC-SML-bit Reserved encounterpress.com/subjustment/WC-SML-bit Reserved encounterpress.com/subjustment/Reserved encounterpress.com/subjustment/Re	94 1	8			11
H App 246 246 4 Long to the control of the control	 Sartisti com/auto Test/-Res (KC_0-0400) Res⁻¹, "Isi (KC_0-0400) Res⁻¹, "Isi (KC	R Cloud OnesCer Gerprot Ren'', ' River,	inFC-5 location location location location location	Art, -ta perilo ttps:// mi*-(* seport	20 30- 1/2022 2027 1

Figure 12 Access URL for PTT Pro Access URL Field

🗄 Apps 📑 Zelona 📑 Symbol 📑 Value 📑 Custo	mers 🧧 Zelona Servers 🧕 CMIA. 🧕 Hotmail 🍕 Z-Car	net 👷 Jis Dahloard 👩 Espenses 🚯 WFC Was Confus 🚯 WF	C Sharepoint M., 🛐 PTT-Pro Smartsheet. 🛞 MQTT on Websocket 🌰 3	ls One Drive 🍵 Ext MGR Doual 🔹 💌
Characteristic Managerovania de la companya de la c	$\label{eq:constraints} \begin{split} & (n_1,n_2,n_3,n_4,n_4,n_4,n_4,n_4,n_4,n_4,n_4,n_4,n_4$	the control of the second sec	(article) and the second states of the second stat	A standard a standard and a standard and a standard standard M. Mar, "Managaro tasks to present a standard M. Mar, "Managaro tasks to present standard and the standard and the standard and the standard standard standard and the standard standard standard and the standard standard

Obtain the OAuth Certificate

See Exporting the ACS Certificate to PTT Pro on page 27 for the process of exporting the OAuth certificate to the PTT Pro server.

Configure the PTT Pro Client

The PTT Pro client is configured through the WFCPTTProDefault.json file. The file contains many elements, but the operation of the OAuth services to support the shared device model requires two parameters.

- oAuthClientID
- oAuthClientSecret

The oauthClientID field is obtained from the ACS service and is the value of the **Client ID** field in the **Settings** tab of the **Clients** view.



WFC-SAML-Test-Realm	Clients > WFC-SAML-test	
Configure 🗸	WFC-SAML-test	T
制 Realm Settings	Settings Credentials	Roles Client Scopes 🚱 Mappers 🖗
😚 Clients	Installation 😡	
🙈 Client Scopes	Client ID @	WEC-SAMI -test
Roles		
😅 Identity Providers	Name 😡	
User Federation	Description @	
Authentication	Enabled ©	ON
Manage	Consent Required @	OFF

The oAuthClientSecret is also obtained in the **Clients** configuration. Navigate to the **Credentials** tab to reveal the secret.



WFC-SAML-Test-Realm v		Clients > WFC-SAML-test
Configure		WFC-SAML-test 👕
111 R	Realm Settings	Settings Credentials Roles Client Scopes (Mappers (Scope (Revocation
(Clients	Installation 😡
- 86 (Client Scopes	Client Authenticator
- E	Roles	
= 1	Identity Providers	Secret 0504258e-5987-49af-a1d0-c33a7a3bee Regenerate Secret
8 L	User Federation	
Authentication		Registration access Regenerate registration access token

Copy and paste this information in to the WFCPTTProDefault.json file for the PTT Pro client:

```
{
    "oAuthClientID":"WFC-SAML-test",
    "oAuthClientSecret":"0504258e-5987-49af-ald0-c33a7a3bee1b"
```

Import the JSON file into the device and consume the configuration with an intent.

```
adb shell am broadcast -a com.symbol.wfc.pttpro.ACTION_DEFAULT_CONFIG --es
"configpath" /sdcard/WFCPTTProDefault.json"
```

Configure the Profile Client

The configuration of the Profile Client requires two parameters.

- Customer ID
- Server URL

Figure 15 Profile Client Configuration

1 🖓 🔘 🖾 🜿 💦 💎 🛿 10:16 AM
← Server connection
Customer ID 312
Server URL wss://wfcsalesdemopm1.pttpro.zebra.com
Site ID 5000
Device ID(read only) TC52_18306522504188
< 0 □

For the Customer ID, use the Tenant ID assigned by the Zebra Administrator in the Profile Manager. The Server URL is the URL of the Profile Manager server configured to support OAuth.

Device Operation

After you configure the servers and the mobile devices, launch the Profile Client to log in.

Figure 16 Profile Client Log In Screen

2 🖬 🤉 🕒 🖾 🖏	💎 🛿 10:16 AM				
Sign in	: ڻ				
WFC-SAML-TEST-REALM					
Log In					
Username or email					
Steve					
Password					
Log in					
< 0					

The device connects to Profile Manager, which redirects the client to authenticate to the SAML IdP through the ACS service. If the user is properly authenticated the username is returned through the network to the device and provisioned with the correct PTT Pro profile for the user.

Figure 17 Client Provisioning



Your configuration is complete.

Troubleshooting the Client Error Message: ADFS Error

After completing the user login sequence, the mobile device stalls, trying to connect to the PTT Pro server. The certificate in the PTT Pro server OAuth configuration is malformed and needs to be correctly loaded. Check the certificate configuration in the PTT Pro server. The format rendering of the imported certificate looks correct.

PTT Pro and Profile Manager SAML Integration Guide

Configure OAuth	×
OAuth URL: https://wfc-keycloak.pttpro.zebra.c Access URL: https://wfc-keycloak.pttpro.zebra.c OAuth Token Certificate: BEGIN CERTIFICATE MIICtTCCAZ0CBgFwU7CcpTANBgkqhkiG9w0BAQsFADA NTC1UZXN0LVJIYWxtMB4XDTIwMDIxNzE1MDU0OFoXD GA1UEAwwTV0ZDLVNBTUwtVGVzdC1SZWFsbTCCASIw CCAQoCggEBAIU2oh2bfqoo5sES3YugRGHB/grQA9AgOv	eMRwwGgYDVQQDDBNXRkMtU0F TMwMDIxNzE1MDcyOFowHjEcMBo vDQYJKoZIhvcNAQEBBQADggEPAD wG+Qd0+R1KB3UCpCzQBjwXaLhO Submit Cancel

Copy the certificate to the clipboard.



The certificate still looks right.

View the certificate with Notepad++ with the view set to show all characters.

BEGIN ·
CERTIFICATEMIICTTCCA20CBgFwU7CcpTANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDDBNXRkMtU0FNTC1UZXN0LVJ1YWxtMB4XDTIw
MDIxNzE1MDU00FoXDTMwMDIxNzE1MDcyOFowHjEcMBoGA1UEAwwTV0ZDLVNBTUwtVGVzdC1S2WFsbTCCASIwDQYJKoZ1hvcNAQEBBQADggEP
ADCCAQoCggEBAIU2oh2bfqoo5sE33YugRGHB/grQA9AgOwG+Qd0+R1KB3UCpCzQBjwXaLhOn8zvhi8gVnugipqVCjGtHSmCWco4N482SvjHw
$\label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qNjQm+n70LHwat2g2kridm4DlApHBp104A2V2WL/0AnXrhM0f3RdxKd6RTC5Rq2T2lWqzalGICLaetDBmTN2aVWsDm7Lu08pqH} \label{eq:listGNxbgD2qW}$
XWiGs1pUXvm6KnuWt/V/oPpXp5fkAvPCZW7qJi0hoU7eJj5yt+RrUkfxeONZdL8t1D56UlFThw7QLImG/LMSGxP/im/uG2svWCwoyxsYE3yz
112a6c/qtG+WjbiNsGjbE8PONU//sb0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAPOH/Kr74TlhVlvA6TN9ozwuq6TMJm3AWWZ7UZwqQ3UVB
$\tt I3006R9iPqLqiJSo1XBgC8zBntTwxrTeYf1poJaYV3nmgrzo7oX5zA40VtCTdtzmfTeroF2WLpxRgJ+hHrAGa5RvXzNAfpJ3MkiTyp6oXqVPIastrone and the state of the state $
dvAC917Ugyp42s13fwrbD4Ek+orzHD6ivsd5YqVX5uRo7E0vxD8/yC8KnJrmJSUmxTvr17c6NFT2LPLraZ5QrwbeEb/xSASDkF9hvU8aBhwT
vxI9YUT549It4BRU1N3bPYhJ5BP3kZUIPbrEaFajlzzyYbXM7XWZXWA3KGfltUOmSAxE6hMV+28iVa6eHA==
END CERTIFICATE GRAD

The PTT Pro server displayed the certificate so that it looked like there is a CR/LF after the ----Begin Certificate---- statement. Examining the certificate in Notepad++ revealed that CR/LF was missing.



NOTE: You can verify a certificate at the website https://jwt.io

Revision History

Changes to the guide are listed below:

Change	Date	Description
MN-004608-01 Rev A	09/2022	First version.

PTT Pro and Profile Manager SAML Integration Guide

Change	Date	Description
MN-004608-02EN Rev A	04/2024	Rebranded to Workcloud Communication.
MN-004608-03EN Rev A	04/2025	Added Configuring Capability Settings, Access Settings, and updated the Configuring Endpoint Credentials, Endpoint Mappings, Identity Provide, Creating the Clients, Creating a Realm, Username Mapping, Auto Launch SAML Login Page, and Exporting ACS Certificate to SAML and PTT Pro.



www.zebra.com