# **PTT Pro and Profile Manager**

**Workcloud Communication** 



# **AD/ADFS Integration Guide**

#### 2025/05/06

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.

# **Objectives**

A large percentage of the Workcloud Communication deployments already have Active Directory (AD) and Active Directory Federated Services (ADFS) deployed in their enterprise.

The purpose of this document is to inform the administrator of the items necessary for PTT Pro and Profile Manager to provide authentication, provisioning, and transformation using the existing AD database.

# **Environment Description**

The Workcloud Communication solution supports the use of OAuth2 authentication using ADFS to provide the ability for a single device to be used by multiple users. This is often referred to as the Shared Device Model as opposed to the Dedicated Device Model.

The support of a Shared Device model is based on the configuration of a Relying Party Trust in the customer's ADFS server. A fully integrated Workcloud Communication solution includes integrating with an Identity Provider (IdP) solution, like AD/ADFS. The functionality of an IdP connection serves three purposes:

- 1. User Authentication
  - Granting user access to the system by validating credentials
  - Providing a shared device usage model
- 2. User Provisioning
  - As associates join and leave the enterprise, they are added to and deleted from the IdP by the customer administrators. The connection to the IdP with Profile Manager and PTT Pro provides the ability to automatically synchronize the user databases with changes made in the IdP.
- **3.** Attribute Transformations
  - Various elements in the IdP database can be evaluated to determine the profile configuration sent to the users.

When the Workcloud Communication solution is fully integrated with AD/ADFS, all three functions are available. Both Profile Manager and PTT Pro rely on the IdP to simplify and automate what would otherwise be a manual process.

The focus of this document is the ADFS configuration and how this determines the configuration of PTT Pro and Profile Manger.

#### **PTT Pro Setup**

When PTT Pro is deployed, Zebra requires the following information to configure the and for the customer.

- PTT Pro configuration elements:
  - OAuth URL
  - Access URL
  - OAuth Token

The configuration elements are available through the Well-Known URL.



#### NOTE:

To support the shared-device model, the serial numbers of each device must be entered into the .

- The can support a mix of OAuth and Activation Code device users.
- Each device user must have an OAuth user name to authenticate to the Azure AD.

#### **Profile Manager Setup**

When the Profile Manager is deployed, Zebra requires the following information to configure the server for the customer.

- Host URL
- Authentication Path
- Token Path
- Client ID
- Client Secret
- Token UserName
- · Client Authentication Header or Body

#### **ADFS** Configuration

Workcloud Communication supports the Forms based sign-on process. Some deployments use Windows Integrated Authentication (WIA) which is not compatible.

This guide assumes the following:

- **1.** The customer has an existing 2016 Windows Server with ADFS installed. Additional documentation describes differences when a Windows 2019 and Windows 2022 server.
- 2. Current Certificates are installed on the ADFS server.
- 3. The ADFS services are installed on a server that is joined to the Active Directory Domain Controller.
- **4.** Administrative privileges are assigned to the user configuring the system.

If the deployment uses WIA, please review the following information:

How to configure intranet forms-based authentication for devices that do not support Windows
 Integrated Authentication (WIA) | Microsoft Docs

#### **ADFS Server Versions**

#### Windows 2016

Windows 2016 Datacenter server supporting SPA (Single Page Authentication)

version 1607 10.0.14393 Build 14393

#### Server 2019 and 2022

Concepts presented for Server 2016 can be applied to Server 2019 and 2022.

# **Prerequisite Information**

The PTT Pro and Profile Manager servers both require specific URL and Token information to provide a connection to ADFS.

This section describes how to use the Well-Known URL to discover this information

# About the Well-Known URL for ADFS

The Well-Known URL concept was created to provide a publicly available central location for server and metadata resources. It provides publicly available information about a site.

A Well-Known URL defines a sign-in flow that enables a client application to authenticate a user and to obtain information (or claims) about that user, such as the user name, email, and so on. It is useful to identify URLs, encryption schemes, and other information useful in establishing server-to-server communications.

Customers may know their Well-Known URL. The construction of the Well-Known URL is typically https://<server\_DNS>/adfs/.well-known/openid-configuration, although there can be differences.

#### How to Find the Well-Known URL

You can determine the Well-Known URL using the ADFS Management Console.

#### Navigate to **Endpoints**.

The Well-Known URL is constructed by taking the customer host name and appending the value of the OpenID Connect Discovery.

🐐 File Action View Window Help							
💠 🔿 🙍 🔟 📓 📷							_
aD FS	Endpoints						
Service     Attribute Stores     Attribute Stores     Authentication Methods     Certificates     Certificates     Claim Descriptions	Enabled Yes No Yes	Proxy Enabled No No Yes	URL Path /adfs/services/tsuttop/windows /adfs/services/tsut/adfactresolution /adfs/oauth2/	Type WS-Inust 2005 SAML-AtifactResolution OAuth	Authentication Type Local Windows Anonymous Anonymous	Security Mode Message Transport Transport	^
Device Registration Endpoints Cope Descriptions Web Application Proxy Access Control Policies	Yes Yes Yes OpenID C	Yes Yes No	/adfs/services/trust/mex /Federation/Metadata/2007-06/Federation/Metadata.xml /adfs/fs/Rederationservenservice.asmx	WS-MEX Federation Metadata ADFS 1.0 Metadata	Anonymous Anonymous Anonymous	Transport Transport Transport	
<ul> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul>	Yes Yes Proxy Yes K	Yes Yes Yes	/adfa/weikkrown/opend-configuration /adfa/dacovery/keya /adfa/useinfo /adfa/proxy/	OpenID Connect Decovery OpenID Connect JWKS OpenID Connect UserInfo Web Application Proxy	Anonymous Anonymous Anonymous Proxy Trust Certificate	Transport Transport Transport Transport	~

#### How to Use the Well-Known URL

The Well-Known URL helps configure the Profile Manager and PTT Pro servers to connect to the ADFS environment.

The URL returns a JSON listing of the OpenID/OAuth endpoints, supported scopes and claims, public keys used to sign the tokens, and other details. The clients can use this information to construct a request to the OpenID server.

The Authorization endpoint is shown below. In this example, the Identifier for the Relying Party Trust is Z-Test-Trust. The authorization\_endpoint: "https://pttproadfs.pttpro.zebra.com/adfs/oauth2/authorize/" becomes https://pttproadfs.pttpro.zebra.com/adfs/oauth2/ authorize?resource=Z-Test-Trust. Pasting this URL in a browser reveals helpful discovery information.

```
{
    issuer: https://PTTPRO-ADFS.pttpro.zebra.com/adfs,
   authorization_endpoint: https://pttproadfs.pttpro.zebra.com/adfs/oauth2/authorize/,
   token_endpoint: https://pttproadfs.pttpro.zebra.com/adfs/oauth2/token/,
   jwks_uri: https://pttproadfs.pttpro.zebra.com/adfs/discovery/keys,
 .
   token_endpoint_auth_methods_supported: [
       "client_secret_post",
"client_secret_basic",
        "private_key_jwt",
        "windows_client_authentication"
   ],
 response_types_supported: [
        "code",
       "id_token",
        "code id_token",
        "id_token token",
        "code token",
        "code id_token token"
   ],
 response_modes_supported: [
        "query",
        "fragment",
        "form_post"
   ],
   grant_types_supported: [
        "authorization_code",
        "refresh_token"
        "client_credentials",
        "urn:ietf:params:oauth:grant-type:jwt-bearer",
        "implicit",
        "password",
        "srv_challenge",
        "urn:ietf:params:oauth:grant-type:device_code",
        "device_code"
   ],
 subject_types_supported: [
        "pairwise
   1.
 scopes_supported: [
        "winhello_cert",
       "vpn_cert",
        "email".
        "allatclaims",
        "profile",
        "logon_cert",
        "user_impersonation",
        "aza",
        "openid"
    1,
 id_token_signing_alg_values_supported: [
        "RS256"
    ],
 .
   token_endpoint_auth_signing_alg_values_supported: [
        "RS256"
    ],
```

This information is provided here as an introduction to the Well-Known URL which is helpful in establishing the server connections to ADFS.

More information about using the Well-Known URL is provided in the validation section.

# **ADFS Setup Flows**

The following process describes steps for configuring the ADFS services running on a Windows 2016 server.

#### **ADFS Server Definition**

Windows 2016 Datacenter server supporting SPA (Single Page Authentication)

version 10.0.14393 Build 14393

#### **Global Rule**

Workcloud Communication depends on Forms-Based authentication.

Open the ADFS Management Console and navigate to **Service** > **Authentication Methods** to open the **Edit Authentication Methods** screen.

Figure 1 Edit Authentication Methods Screen.

🗢 🔿 🙍 📰 📓 🗊		
AD FS A	ithentication Methods	
Service     Attribute Stores	Authentication Methods Overview	
<ul> <li>Authentication Methods</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Device Registration</li> <li>Endpoints</li> <li>Scope Descriptions</li> <li>Web Application Proxy</li> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul>	Ye       Edit Authentication Methods       X         Primary       Multi-factor         Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.         Finance       Finance         Edit Authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to suthenticate with at sign in.         Finance       Finance         Edit Authentication method on browsers that support Integrated Windows authentication.         Editanet       Forms Authentication         Cetificate Authentication       Device Authentication         Device Authentication       Microsoft Passport Authentication         Windows Authentication       Windows Authentication         Device Authentication       Oncosoft Passport Authentication         Device Authentication       Windows Authentication         Or Cetificate Authentication       Oncosoft Passport Authentication         Device Authentication       Microsoft Passport Authentication         Or To use device authentication methods will not be available until an Azure Active Directory tenant is configured. Learn More         Ot use device registration.       Directory tenant is configured. Learn More         DK       Cancel       Apply	эл. Yc

The internal and external network methods may be different.

Set Forms Authentication as the primary method for the network supporting mobile devices.



**NOTE:** This is an enterprise-wide setting. Changing the setting may affect existing operations. Check with the System Administrator before modifying.

# **Configuration Process Overview**

This outline describes the process to properly establish an ADFS configuration to support PTT Pro and Profile Manager OAuth2 authentication. This outline may be helpful for advanced users familiar with ADFS configurations.

- Add a Relying Party Trust
  - Name the Trust
  - Skip the Cert not required
  - Skip the URL not required
  - Configure the Trust Identifier
  - Choose the Access Control Policy
- Configure Claims Issuance Transform Rules
  - Add Rule
  - Select Passthrough Claim Rule Template
  - Create Pass Though for Name
  - Create Pass Through for UPN
- Bind the Token Decrypting Cert to Relying Trust
  - Select the Token Decrypting cert
  - Copy Cert to File -- Name and Save base64 cert file type
  - Bind the cert to the Relying Party Trust in Signature
  - Export the Token Signing Cert to be used in the PTT Pro OAuth configuration
- Create Application Groups
  - Add an Application Group
    - Select Standalone / Native application
  - Capture Client ID
  - Redirect = <u>https://localhost</u>
  - Select Standalone Web API
  - Add identifier
  - Select Access Control Policy
  - Add Application Permissions
  - Add Issuance Transform Rules
  - Add Rules
    - Select passthrough Claim Rule Template
    - Create Pass Through for Name
    - Create Pass Through for UPN
  - Apply Access Control policy
  - Config Application Permissions to include Openid and Profile

# **Create a Relying Party Trust**

Add a Relying Party Trust using the ADFS Management Console.

- 1. Open the ADFS Management Console.
- 2. Select and Add Relying Party Trust.



3. Select Claims aware.

Madd Relying Party Trust V	Vizard	~
Welcome		
Steps 9. Welcome	Welcome to the Add Relying Party Trust Wizard	
Select Data Source     Choose Access Control     Policy	Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more	
Ready to Add Trust	Oaims aware	
• Frash	Non claims aware	
	< Previous Stat Cano	el

4. Select the option to Enter the data about the relying party manually.



5. Enter a name for the relying party in the **Display name** field.

🎕 Add Relying Party Trust	Wizard	×
Specify Display Nam	e	
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Z-Demo-Trust	
Specify Display Name	Notes:	
<ul> <li>Configure Certificate</li> </ul>		~
<ul> <li>Configure URL</li> </ul>		
<ul> <li>Configure Identifiers</li> </ul>		
<ul> <li>Choose Access Control Policy</li> </ul>		~
Ready to Add Trust	-	
• Finish		
	< Previous Next > Cance	

6. Click Next.

🍿 Add Relying Party Trust V	Vizard	×
Configure Certificate		
Steps • Welcome • Select Data Source • Specify Display Name • Configure Cetificate • Configure URL • Configure Identifiers • Choose Access Control Policy • Ready to Add Trust • Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.           Issuer:         Subject:           Brective date:         Expiration date:	
	< Previous Next > Cancel	

7. No certificate is required. Click Next.



- 8. No URL is required. Click Next.
- 9. In the Relying party trust identifier field, enter a meaningful name for the relying trust, and click Add.In this example, the identifier Z-Relying-Party-Trust-ID is used.

输 Add Relying Party Trust Wiz	tard	×
Configure Identifiers		
Steps Welcome	Relying parties may be identified by one or more unique identifier strings. Specify the identifier party trust.	s for this relying
Select Data Source	Relying party trust identifier:	P
Specify Display Name		Add
Configure Certificate	Example: https://fs.contoso.com/adfs/services/trust	
Configure URL	Relying party trust identifiers:	
<ul> <li>Configure Identifiers</li> </ul>	Z-Relying-Party-Trust-ID	Remove
<ul> <li>Choose Access Control Policy</li> </ul>		
<ul> <li>Ready to Add Trust</li> </ul>		
<ul> <li>Finish</li> </ul>		
	< Previous Next >	Cancel

#### 10. Click Next.

The wizard advances to Choose Access Control Policy screen.

输 Add Relying Party Trust V	Wizard		×
Choose Access Contr	ol Policy		
Steps Welcome	Choose an access control policy:		
Select Data Source     Specify Display Name     Configure Certificate     Configure URIL     Configure Identifiens     Choose Access Control     Policy     Ready to Add Trust     Finish	Pemit everyone Pemit everyone and require MFA Pemit everyone and require MFA for specific group Pemit everyone and require MFA from edizanet access Pemit everyone and require MFA flow automatic device registr Pemit everyone for intranet access Deams reaction constr Policy Pemit everyone	Description Grant access to everyone. Grant access to everyone and requi Grant access to everyone and requi Grant access to the intranet users and requi Grant access to everyone and requi	
	I do not want to configure access control policies at this time. No application.	user will be permitted access for this	
	< Pret	vious Next > Cancel	

- **11.** In the **Choose an access control policy** field, choose **Permit everyone**.
- **12.** Leave the Access Control Policy option unchecked.

#### 13. Click Next.

The wizard advances to **Ready to Add Trust**. The summary page provides the ability to review all selections made.

Deads to Add Tourt	
Ready to Add Trust	
Steps	The relying party trust has been configured. Review the following settings, and then click Next to add the
Welcome	relying party trust to the AD FS configuration database.
Select Data Source	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note
Specify Display Name	Specify the monitoring settings for this relying party trust.
Configure Certificate	Relying party's federation metadata URL:
Configure URL	
Configure Identifiers	
Choose Access Control	Montor reying party
Policy	Automatically update relying party
Ready to Add Trust	This relying party's federation metadata data was last checked on:
Finish	<never></never>
	This relying party was last updated from federation metadata on:
	<never></never>
	1

14. Click Next.



**15.** Ensure the **Configure claims issuance policy for this application** box is checked.

**16.** Click **Close** to finish. The console returns to the Relying Party Trusts summary page.

👣 File Action View Window Help				_	
ad FS	Relying Party Trusts				
Senice     Access Control Pelicies     Relying Party Trutts     Claims Provider Trusts     Application Groups	Dapley Name ptiproauth adigatent Z-Demo-Truat	Enabled Yes Yes Yes	Type WS-T WS-T WS-T	Identifier newpftproauth2 adtysteet 1 2:Relying-Pany-Trust-ID	Access Control Policy Permit everyone Permit everyone Permit everyone

# **Configure Relying Trust for Claim Issuance Policy**

Edit the Claim Issuance Policy of the Relying Trust policy.

1. Right-click on the new Relying Trust policy and select Edit Claim Issuance Policy.

2. Click Add Rule.

Edit Claim Issuance Policy for Z-Demo-Trust	×
Issuance Transform Rules	
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	\$ \$
Add Rule Edit Rule Remove Rule	
OK Cancel A	pply

3. In the Open rule template drop-down, select Pass Through or Filter an Incoming Claim.

🎕 Add Transform Claim Ru	le Waard X		
Select Rule Template			
Steps e Onnee Rule Type e Configure Clein Rule	Select the template for the claim rule free you went to create from the following list. The description provides details about each claim rule template		
	< Previous Net > Cancel		

- 4. Click Next.
- 5. Enter a name in the Claim rule name field.
- 6. Select Name from the Incoming claim type menu.

7. Select Pass through all claim values.

🐏 Add Transform Claim	Rule Wizard		х
Configure Rule			
Steps Choose Rule Type	You can configure this rule to p claims that are generated by pr claim values should pass throu	pass through or filter an incoming claim. You can also configure this rule to filte revious rules. Specify the claim type and whether only some claim values or all gh.	ř
Configure Claim Rule	Claim rule name:		
	Pass-Through-Name		
	Rule template: Pass Through a	r Filter an Incoming Claim	
	Incoming claim type: Na	ame	$\sim$
	Incoming name ID format:		~
	Pass through all claim value	85	
	O Pass through only a specific	c claim value	
	Incoming claim value:		
	O Pass through only claim val	ues that match a specific email suffix value:	
	Email suffix value:		
	Bo	ample: fabrikam.com	
	<ul> <li>Pass through only claim val</li> </ul>	ues that start with a specific value:	
	Stats with:	sends: EADDYANS	_
	D	ampre: FABHINANI'	
		< Previous Finish Cancel	

8. Click Finish.

The console returns to the Insurance Transform Rules screen.

Edit Claim	Issuance Policy for Z-C	Verno-Trust	×
The fold	wing transform rules speci	fy the claims that will be sent to the relying p	arty.
Order	Rule Name	Issued Claims	
1	Pass-Through-Name	Name	
			金
			101
			14
Add P	Lie Edit Rule	Remove Rule	
		OK Cancel	Apply

9. Click Add Rule to add another Rule for UPN.

it ages	You can configure this rule to pass th	rough or filter an incoming claim. You can also configure this rule to filter			
Choose Rule Type	claims that are generated by previous claim values should pass through	make. Specify the claim type and whether only zone claim values or all			
Configure Claim Rule	Carr nia name				
	Page Trough UPN				
	Pule-template: Para Through or Filter	an Incoming Claim			
	Incoming claim type:				
	Incoming name Diferent				
	· Para mough a cain value				
	Pass Presign only a specific claim	( Value			
	Incoming chain value				
	O Pass through only claim values the	at match a specific amail suffix value:			
	ferral auffic value				
	Darph	fabrikan com			
	O Pass Prought only claim values in	a dari wen a specific value			
	Stats etc.	ELEPTRING.			
	compe.	ringramment.			

**10.** Click **Finish** when UPN is complete.

Edit Claim	Issuance Policy for Z-Demo-Trust	×
Issuance '	Transform Rules	
The folk	owing transform rules specify the claims that will be sent to the relying party.	
Order	Rule Name Issued Claims	
1	Pass-Through-Name Name	
2	Pass-Through-UPN UPN	
		•
		4
Add F	Rule Edt Rule Remove Rule	1
	OK Cancel	Apply

**11.** Click **Apply** to return to the Relying Trusts listing.

# Export the Token Decrypting Certificate

Select the certificate for decrypting the token and export it for later use.

1. Select **ADFS** > **Service** > **Certificates** from the ADFS Management Console view.

Service     Antibut Stones     Antibut Stones     Antibut Stones     Cestificates     Chain Descriptions     Device Registration     Endpoints     Sospe Descriptions     Web Application Proxy     Access Carbol Policies	Subject Sarvice communications Sarvice communications Sarvice communications Schwadt S Encopton - PTTPROAD Schwadt S Encopton - PTTPROAD Schwadt S Encopton - PTTPROAD SCHWADT S Encopton - PTTPROADCFS SCHWADT S Encopton - PTTPROADCFS SCHWADT S Encopton - PTTPROADCFS	Issuer CNI-Thuste RSACA 2018, OU-work digos CNI-ADFS Encogelion - PTTPROADFSutton CNI-Thuste RSACA 2018, OU-work digos CNI-ADFS Surgery - PTTPROADFS approx.
Scope Desciptions Web Application Proxy Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Token-signing CN-ADFS Sgreg - FTTPROADFS CN-* ptpro.sebra.com, O-Zelma Te	CNI-ADFS Sgring - PTTPRO CNI-Theete RSA CA 2018, O

The **Certificate** window appears.

2. Select the appropriate token-decrypting certificate from the Certificates window.

Certificate	
Show: <al></al>	~ V
Field	Value ^
Version	V3
Serial number	04 b9 a5 36 4c f4 26 ae 3e a3
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Thawte RSA CA 2018, www.di
Valid from	Wednesday, January 5, 2022
Valid to	Thursday, January 5, 2023 11
	Edd Despertise
	gat Properbes

**3.** Right-click on the desired certificate, click the **Details** tab and copy the certificate to a file on your computer.

 Use the Certificate Export Wizard to export the Token Encryption Certificate to a Base-64 .CER file type.

🗧 😼 Certificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)	
Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
Enable certificate privacy	
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	
Next Can	cel
THORE	

- **5.** Name the exported cert and save it to a location on your computer.
- 6. Click Save to finish.

# Bind the Token Decrypting Certificate to the Relying Party Trust

Select the Token-Decrypting Certificate you created earlier and bind it to the Relying Party Trust.

1. Select Relying Party Trusts to display the list Replying Party Trusts.

ADFS	Relying Party Trusts				
Artivica Surra     Activate Surra     Authentication Methods     Cartificates     Cartificates     Device Registration     Device Registration     Scope Desciptions     Web Application Prony     Access Control Policies     Relying Party Touts     Cleme Dovice Touts     Application Coups	Display Name ptpress.dn odbydfed Edit Asso Edit Cia Disable Propert Delete Help	Graßied Yee Yee Yee Item Federation Mitadata en Insaaron Policy	Type WS-T WS-T.	lövelfer nevetforsaufs2 adlpdref1 2.Malyng hay Tout (C)	Access Control Pulcy Parent envyrone Parent envyrone Parent envyrone

2. Right-click on the trust and select Properties.

3. Select the Signature tab and click Add.

ganization	Endpoints Proxy	Endpoints Notes	Advance
onitoring Ide	ntifiers Encryptic	on signature Acc	epted Clain
ecify the signatu ty.	re verfication certfi	cates for requests from th	is relying
Subject	lssuer	Effective Date	Expirati
	Marri	Denne	
Add.	WWW	Premove	

4. Browse for and select the exported Token Encryption Certificate and click **Open** to add the certificate.

Z-Demo-Trust Properti	es		×
Organization Endp Monitoring Identifie	oints Proxy Endp rs Encryption	oints Notes Signature Accep	Advanced ted Claims
Specify the signature ve party.	enfication certificates	for requests from this	relying
Subject	Issuer	Effective Date	Expiratio
CN=*.pttpro.z	CN=Thawte RS	1/5/2022 12:00:	1/5/20:
<			>
Add	View Re	move	
Add	nom Ive	inv tu	
	OK	Cancel	Apply

5. Click Apply and OK to finish.

### **Export Token Signing Certificate**

Export the Token-Signing Certificate using the same method as the Token Decrypting Certificate to a Base-64 .CER file type.

1. Return to **Certificates** and select a valid Token Signing Certificate.



2. Export the selected certificate in that same fashion as the Token Decryption Certificate.

Save the certificate. You will use the Token Signing Certificate to configure OAuth2 in the PTT Pro Server.

#### **Create the Application Group**

When you define the Application Group, the template selection determines whether a Client Secret is used. The process flow below describes two flows. The first process flow steps through a configuration without the Client Secret, and the second process flow shows a configuration with a Client Secret. Workcloud Communication supports both configurations.

The use of a Client Secret is up to the Customer. If the customer wants to use a Client Secret:

- The Client Secret must be defined in the Profile Manager.
  - If the secret is not populated or is incorrect for the customer in Profile Manager, the user is prompted for credentials but the Profile Client displays an "Unknown Error" message when the credentials are entered.
- The Client Secret must be included in the PTT Pro Client configuration.
  - If the Client Secret is not included in the PTT Pro client JSON configuration file, the client displays a security error when the connection is activated.

#### **Create a Standalone Application Group**

After you create the application group, you need to create a Web API Application Group. If the customer requires a client secret, choose the procedure referenced in the post-requisites.

1. In the ADFS Management Console, right-click on **Application Groups** and select **Add Application Groups**.



2. In the Templates list, select Native Application from the Stand Alone Application list.

Reps	Name	
Welcome	Table: Z. Ann Con or David Bore Nation Ann	
Native application Summary Complete	Description:	
	Template: Client-Server applications	
	Native application accessing a web API	
	Web browser accessing a web application	
	Standarone applications	
	Web AP1	
	Man information	

**3.** Enter a meaningful name and click **Next**.

The Client Identifier is displayed in the Add Application Group Wizard.

- a) Copy the Client Identifier so that you can paste it into a validation application such as Postman.
- **b)** Enter https://localhost in the **Redirect URL** field.

Neicone		
	Z-App-Group-Stand-Abne-Native-App - Native application	
Native-application	Over identifier	
Summery	(3910ka0-2478-046e-904a3830127647b	
Complete	Protect a 1000	
	Reserve Unit	
	Example: https://conside.com	700
		Benove
	Description	
		-

#### 4. Click Next and Close.

The next depends on whether the customer requires a client secret:

- If a client secret is not required, proceed to Create Standalone Web API Application Group on page 26.
- If a client secret is required, proceed to Create a Web API Application Group with a Client Secret on page 29.

#### **Create Standalone Web API Application Group**

Use this task to create an application group that does not use a shared secret.

1. Open the ADFS Management Console

- 2. Right-click the Application Group and select Add Application Group.
- 3. In the Templates list, select Web API from the Stand Alone Application list.

Welcome	
Reps Weicom	Name: Z App Group Stand Hone-Native App
Native application Summary Complete	Descriptor:
	Tangkat: Clent Sover applications Site Sover application accessing a web API Sover application accessing a web API Standalone applications Standalone applications Sandalone applications Mative application Sover application Web Note: Web API
	More information.

4. Configure the Web API.

Steps	Name	
<ul> <li>Welcone</li> </ul>	Z-App-Group-Stand-Alone-Native-App - Web AP1	
Configure Web API	Vertile	
<ul> <li>Apply Access Control Policy</li> </ul>	atorial	
Configure Application	pprn	
Permosono		Parrove
<ul> <li>Summery</li> </ul>		
Conpete		
	Description:	

a) Enter a name in the Name field.

The name is appended to the Access URL to access the ADFS Application Group, as in https:// <server\_name>/adfs/oauth2/authorize?resource=pttpro-id in this example.

b) Click Add.

5. Click Next to advance.

The Access Control Policy defaults to Permit Everyone.

Change of the second se		
ange -	Choose an access control policy.	
Welcome	Nane	Description
<ul> <li>Server application</li> </ul>	Permit everyone	Grant access to everyone.
Conligue Application	Femil everyone and require MFA	Grant access to everyone and require MEA1
Credential	Permit everyone and require MFA for specific group	Grant access to everyone and require VEAL
Configure Web AP1	Femil everyone and require MFA from extranet access	Grant access to the intranet users and requir.
Apply Access Control Policy	Femil everyone and require MFA from unauthenticated	Grant access to everyone and require WFAF
Configure Application	Permit everyone and require MPA, allow automatic dev	Grant access to everyone and require WEAT
Permissions	Forme everyone for Penane access	Cred access to the interest cases.
Summery	Park brone group	Grant access to paiers or one or more special
Complete	Policy	
	Panit everyone	
	- Like not want to configure the access control policy at the	is time. No users will be permitted access for this

6. Click Next to advance.

Under Permitted Scopes, the application permissions default is openid. Also ensure profile is checked.

Reps	Configure contribution	raits applie clast projections to access the Web API	
Welcome	Cient analization in	ala/	
Configure Web API	-	Recording	
Apply Access Control Policy	7 Are Owner She	utersongtion	
Configure Application Permissions	L'AP-STAP-SK		
Sunnay			
Camplete			
	Pensited scopes:	Add	Renove
	Penitted scopes: Scope Name alustaire Scope Name alustaire scop scole y scole	Add	Renove
	Penitted scopes: Scope Name distutions Stop amai logon_pet dissenid yordie use_impanse. ixon_peni	Add.	Annove

7. Click Next to advance.

A summary is shown.

Summery	
Sege Selection Cardigue Mo JPI Andry Access Cartell Pelay Cardigue Avaliation Presentina Summary Complete	Perver the following settings and dolt. Not, 'to onsite the application.           Application Group           Name: 2-App-Group-Stand-Rise-Flattve-App           Web: API           Name: 2-App-Group-Stand-Rise-Flattve-App           Web: API           Name: 2-App-Group-Stand-Rise-Flattve-App           Name: 2-App-Group-Stand-Rise-Flattve-App           Name: 2-App-Group-Stand-Rise-Flattve-App           Name: 2-App-Group-Stand-Rise-Flattve-App           Name: 2-App-Group-Stand-Rise-Flattve-App           Application periodsome           Application periodsome           Z-App-Group-Stand-Rise Native-App

8. Click Next to close and finish.

#### Create a Web API Application Group with a Client Secret

Use this task to create an application group that uses a shared secret.

If the customer uses a Client Secret, the Application Group configuration is different.

1. Select Server Application accessing a web API from Client-Server Applications instead of Native Application from Standalone applications.

🗌 Add Application Group W	/izard X
Welcome	
Steps	Name:
<ul> <li>Welcome</li> </ul>	Z.App.Group.Secret
Server application     Configure Application     Credentials     Configure Web API	Description:
Apply Access Control Policy	
<ul> <li>Apply Access Control Policy</li> <li>Configure Application Permissions</li> <li>Summary</li> <li>Complete</li> </ul>	Template:          Client-Server applications         Native application accessing a web API         Server application accessing a web API         Web browser accessing a web application         Standalone applications         Native application         Native application

**2.** Enter a meaningful name in the **Name** field.

The Client Identifier is automatically generated. Copy the Client Identifier for later use.

Mad Application Group W	fizard	×
Server application		
Steps	Name:	
Welcome	Z.App.Group.Secret - Server application	
Server application	Clast Identifier:	
<ul> <li>Configure Application Credentials</li> </ul>	e7d167db-bd99-406a-bfee-146363444419	
Configure Web API	Redirect URI:	
Apply Access Control Policy	Example: https://Contoso.com	Add
<ul> <li>Configure Application Permissions</li> </ul>	https://localhost	Remove
Summary		
Complete		
	Description:	
		<b>0</b>
	< Previous Next >	Cancel

- **3.** Enter https://localhost in the **Redirect URI** field.
- 4. Click Next to advance.

5. Select Generate a shared secret in the Configure Applications Credentials screen.

輸 Add Application Group V	/izard >
Configure Application	Credentials
Steps  Welcome Server application Credentials  Configure Application Apply Access Control Policy  Apply Access Control Policy  Summary Complete	Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.         Register a key used to sign JSON Web Tokens for authentication         Configure         Windows Integrated Authentication         Select the AD Account:         Example: CONTOSO/expensevc         Select         Generate a shared secret         Secret:         XregNSc8hB7WY0h-IIGF5pvgaKRD38T-E0v3MbR       Copy to clipboard         Opy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later f required.

- 6. Copy and save the secret that is generated. The shared secret will not be shown again.
- **7.** Complete the creation of the application group as previously described Create a Standalone Application Group on page 24.

# Add Claims to the Application Group

After creating the Application Group, the Claims Issuance may not be automatically prompted for and must be added.

1. Right-click on the Application Group and select **Properties**.

App-Group-standAlone-Native	mapp Properties
eneral	
Name:	
Z-App-Group-StandAlone-Native-/	App
Description:	
applications:	
Name	Description
Native application	
Z-App-Group-StandAlone-Native	-App - Native ap
Web API	
Z-App-Group-StandAlone-Native	-App - Web API
	Edg Barrows
Add application	EQU Nemove
Add application	
Add application	

2. Select the Web API application and click Edit.



3. Select the Issuance Transform Rules tab.

4. Click Add Rule and enter two rules, one for Name and one for UPN.



Using two rules provides flexibility. The required Transform Rule is based on the content of the Access Token.

In this snippet, we see both the UPN and the Name (unique\_name) in the token. Refer toExamine the Returned Access Token on page 43 for more details.



5. Select Pass Through or Filter an Incoming Claim from the Open rules template drop-down menu.

<ul> <li>Onosee Rule Type</li> </ul>	Select the template for the claim rule that you want to create from the following lat. The description provides datally about each claim rule template.
Configure Claim Rule	Catery rules template:
	Pass Through or Fiter an Incoming Claim V
	Clean rule template description:
	with a solution down type. The can also filter the values of incoming claims with a selected dam type. For example, we can use the number to create a number that send all incoming group claims. Thus can also use the rule to send only UPN claims that and with "Stitution". Multiple claims with the same claim type may be entitled from the rule. Sources of incoming claims vary based on the rules being edited

- 6. Click Next.
- 7. Enter a name in the **Claim rule name** field and select **Name** from the **Incoming claim type** drop-down menu.

Ensure that **Pass through all claim values** is selected.

🎕 Add Transform Claim R	Ae Waard	2
Configure Rule		
Steps Crosse Rule Type Configure Claim Rule	You can configure this rule to pass through on filter an incoming claim. You can also configure this rule to filter claim that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values (rule) pass through. Claim sule name.	
	Pasa Through Name	
	Rule template: Pass Through or Filter an Incoming Claim	
	Incarning claim type: Kano	
	Incoming name ID-format	
	Pass through all claim values	
	Pass through only a specific claim value	
	Incoming claim value:	
	Pass through only claim values that match a specific email suffix value:	
	Ernal auftic value:	
	Example Tabrikan core	
	Pass through only claim values that start with a specific value:	
	Reference Concernen	
	Example: PARPINARY	
	< Previous Finish Cancel	
		-

8. Click on Finish to return to the Add Transform Claim Rule Wizard.

9. Repeat these steps to add a Pass Through UPN claim rule.

Configure Rule	
Reps	You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter
Choose PLde Type	claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
Configure Claim Rule	Cain rule name:
	Pass Through UPN
	Rule template: Pres Through or Filter an Incoming Claim
	Incoming claim type:
	Incoming name ID format
	(e) Pass through all claim values
	<ul> <li>Pass through only a specific claim value</li> </ul>
	Rest through only a specific claim value     Incoming claim value:
	Pass through only a specific claim value     Incoming claim value:     Pass through only claim values that match a specific ornal suffix value:
	Pass through only a specific claim value Incoming claim value:     Pass through only claim values that match a specific ornal suffix value:     Email suffix value:
	Pass through only a specific claim value Incoming claim values Incoming claim values Incoming claim values Incoming claim values that match a specific onal suffix value: Enal suffix value: Enal suffix value: Example: fabricam.com
	Pass through only a specific claim value     Incoming claim value:     Pass through only claim values that match a specific small suffix value:     Eval suffix value:
	Pass through only a specific claim value     Incoming claim values     Incoming claim values     Pass through only claim values that match a specific email auflix value:     Email auflix value:     Email auflix value:     Dosmple: thorison.com     Pass through only claim values that start with a specific value:     Starts with:
	Pass through only a specific claim value     Incoming claim values     Incoming claim values     Pass through only-claim values that match a specific onsal suffix value:     Enail suffix value:     Enail suffix value:     Example: fabricam.com     Pass through only-claim values that safe a specific value:     Starts with:     Example: FABFICAMY.
	Pass through only a specific claim value     Incoming claim values     Incoming claim values     Pass through only claim values that match a specific onail suffix value:     Eval suffix value:     Eval suffix value:     Dample: fibrikam.com     Pass through only claim values that with a specific value:     Stats with:     Evaluation     Dample: TAEFORATION
	Pass through only a specific claim value     Incoming claim values     Incoming claim values     Incoming claim values that match a specific onal suffix value:     Enail suffix value:     Enail suffix value:     Enail bit start with a specific value:     Starts with:     Ecomple: TAEFORGAIN

**10.** Click **Finish** and **Apply** to display a list of the rules.

Z-App-Gr	oup-Sta	ndAlone-Native-App	- Web API P	roperties		×
Identifiers	Notes	Access control policy	Issuance Tr	ansform Rules	Client Permissio	ns
The follo	wing tran	aform rules specify the	claims that will	be sent to the	relying party.	
Order	Rule N	ame		Issued Claims		
1	Pass T	hrough Name		Name		
2	Pass T	hrough UPN		UPN		
						1
						4.
						-
Add R	ule	Edit Rule Re	move Rule			
			0	к	ancel	Apply

**11.** Click on **Apply** and **OK** to finish.

If the procedures under the ADFS Setup Flows were followed, the ADFS server support for the PTT Pro server and Profile Manager should now be established.

The validation procedures provide tools and methods to help validate the configuration settings.

# Updating the Access and Refresh Token Lifespans

You can update the lifespan for access tokens and refresh tokens according to the requirements of your business. The commands listed below require administrator privileges and must be run in Powershell.



**NOTE:** The access token lifespan must be less than the refresh token lifespan.

1. Run the following command to issue refresh tokens. If refresh tokens are issued, you can skip this step.

set-AdfsRelyingPartyTrust -TargetName "RelyingPartyTrust\_name" IssueOAuthRefreshTokensTo AllDevices

Replace RelyingPartyTrust\_name with the address of the ADFS server.

2. Set the access token lifespan. This value is at the Relying Party Trust level.

```
set-AdfsWebApiApplication -TargetIdentifier Identifier_name -
tokenlifetime timeInMin
```

set-AdfsWebApplicationProxyRelyingPartyTrust -TokenLifetime timeInMin

```
set-AdfsRelyingPartyTrust -TargetName RelyingPartyTrust_name -
TokenLifeTime timeInMin
```

Replace *Identifier\_name*, *timeInMin*, and *RelyingPartyTrust\_name* with values appropriate for your environment. The value of *timeInMin* is in minutes.

**3.** Set the refresh token lifespan. This is a global setting.

```
set-AdfsProperties -ssolifetime timeInMin
```

Replace the value of *timeInMin* with the refresh token lifespan. The value is in minutes.

# Validating the Configuration

After the ADFS server is configured, validate the configuration to ensure the PTT Pro and Profile Manager servers operate as expected.

The following tools can be used to validate the configuration.

#### Postman

Postman is an API platform for building and using APIs. <u>https://www.postman.com/downloads/</u>

#### JWT Token validator

JSON Web Tokens are an open, industry standard <u>RFC 7519</u> method used to represent claims securely between two parties. JWT.IO allows you to decode, verify, and generate a JSON Web Token. <u>https://jwt.io</u>

#### **JSONLint**

Validates the structure of a JSON file. JSONLint validates and reformats JSON, a lightweight datainterchange format. Copy and paste, directly type, or input a URL in the editor and let JSONLint tidy and validate your messy JSON code. <u>https://jsonlint.com</u>

#### **KeyCDN Cert Checker**

KeyCDN is a web-based certificate checker. tools.keycdn.com

# The Well-Known URL

When the Well-Known URL is pasted into a browser, it returns a JSON listing of the OpenID/OAuth endpoints, supported scopes and claims, public keys used to sign the tokens, and other details.

Clients can use this information to construct a request to the OpenID server. The example below is the response returned from the ADFS server for the Well-Known URL.





The response includes the two URLs required by the PTT Pro server to complete the OAuth configuration: the Access URL and the Token URL. Examine the Well-Known response to find the Authorization Endpoint and the Token Endpoint.

Authorization endpoint: https://pttproadfs.pttpro.zebra.com/adfs/oauth2/authorize

• Token endpoint: https://pttproadfs.pttpro.zebra.com/adfs/oauth2/token

Once the Authorize URL has been identified, resources will need to be added to the URL.

rganization	Endpoints	Proxy Env	dpoints	Notes	Advanced
lonitoring	Identifiers	Encryption	Signat	ure Ad	ccepted Claims
pecify the dis	play name and	identifiers for	this relyin	g party tru	ist.
Display nam	e:				
Z-Test-Rely	ng-Party				
Debine and	u identifian				
neiying part	y identitier.				
				_	Add
Example: htt	ps://fs.contos	o.com/adfs/s	ervices/tr	ust	
Relying part	y identifiers:				
Z Test Taus					
12.1 Col. 11Uo					Remove
Z*Test*Tius					Remove
2-103-1103					Remove
Z. Test Trus					Remove
z. resc mus					Remove
					Remove
					Remove
<u>En les intes</u>					Remove
					Remove
					Remove
		01			Remove

In our example, the Identifier for the Relying Party Trust is *Z*-Test-Trust, and the PTT Pro server authorization URL becomes:

https://pttproadfs.pttpro.zebra.com/adfs/oauth2/authorize?resource=Z-Test-Trust

#### **Using Postman**

Postman is a graphical tool used to test APIs and construct HTTP requests. You can also use Postman to validate the Authorization and Token URLs, the Client ID, and the Client Secret you will need to access the ADFS server from PTT Pro and Profile Manager.



**NOTE:** Postman can be freely downloaded from the web.

You can use a tool like Postman to validate expected connection attributes and retrieve an Access Token from the connection.

#### Figure 3 Requesting an Access Token

			Current Token			
ype	OAuth 2.0	~	warrent futuri			
			Access Token		Available Tokens	$\sim$
The authorization data will be equest. Learn more about au	automatically generated when you thorization A	send the			Access Token	
dd authorization data to	Request Headers	~				
			Header Prefix (1)		Bearer	
			Configure New Token			
			Configuration Options	Advanced Options		
			Token Name		Enter a token name	
			Grant Type		Authorization Code	×
			Callback URL ③		https://localhost	
					Authorize using browser	
			Auth URL ①		https://pttproadfs.pttpro.zebra.com/ad	dfs/or
			Access Token URL ①		https://pttproadfs.pttpro.zebra.com/ac	dfs/oi
			Client ID ①		36848406-9e11-4324-b813-895227b	6E 🛆
			611-1-1 6-1-1-1 ()			
			Client Secret (1)		Client Secret	
			Scope ①		openid	
			State ①		openid	
			Client Authentication		Send client credentials in body	$\sim$

Use the information collected from the customer environment and enter the following information into Postman:

1. Enter the Authorization URL in the Auth URL field.

The Authorization URL is found in the response from the Well-Known URL and then adding the identifier from the Web API Application Group with ?resource=.

2. Enter the client identifier in the Client ID field.

The client identifier is found in the Native Application Group.

3. Enter openid in the Scope field.

The openid is specified in Web API Application Group when creating the application permissions.

4. Enter openid in the State field.

After you enter the required information, clear any cookies that may be present and initiate the Get New Access Token. If the settings are accurate, the console will prompt you for AD credentials. Enter valid user credentials to retrieve the Access Token.

#### **Examine the Returned Access Token**

After you sign on using Postman, the next step is to examine the returned JSON Web Token Access Token (JWT) using the JWT Token Analyzer.

Copy the Access Token returned from Postman and paste the token into the analyzer at https://jwt.io.

Review the Payload portion of the token. For example:



- Valid encryption is expected, for example, RS256.
- The **aud** field contains the correct identifier.
- The identifier in the token must match the Relying Party Identifier stated in the Standalone Web API in the Application Group.
- The Claims Issuance examines the token contents, so the Claims can use the UPN. The Name is not
  included in the Token so is not used or needed in this definition. If other elements are available, the
  Claims can be refined with the token elements.

This process is also helpful in the Profile Manager environment to identify token elements used to determine User Profile assignment.

#### Validate the Signing Certificate

A valid signing certificate is required for the PTT Pro server OAuth2 configuration. In a previous step, you exported the Signing Certificate for later use. This process reveals if the Signing Certificate is valid and can be used in the PTT Pro server runtime configuration.

Open the Signing Certificate in Notepad and copy the certificate into the clipboard.

Verify the integrity of the certificate using a validation tool such as <u>Certificate Checker</u>. Pasting the token into the tool enables you to verify that the token details are as expected.





The Certificate Checker produces JSON output, which is not shown here for security purposes. The Certificate Checker provides information including:

- Validity of the certificate
- Expiration timing
- The Signature RSA encoding

After you perform the validation steps, you can begin to configure the PTT Pro server and Profile Manager.

# **Configuring PTT-Pro to Support OAuth2**

Configure the PTT Pro server to use OAuth2 to authorize requests and grants through tokens between the customer's identification provider and PTT Pro.

The OAuth2 Access URLs and the ADFS Signing Certificate token must be entered in the PTT Pro Management Portal.

**1.** Open the PTT Pro Management Portal through a Web browser and navigate to the Customer Configuration.



#### 2. Click Modify OAuth or Enable OAuth.

The **Configure OAuth** dialog box appears.

- **3.** Enter the OAuth URL and the Access URL.
  - OAuth URL example: https://<server.domain.com>/adfs/oauth2/authorize? resource=pttpro-id
  - Access URL example: https://<server.domain.com>/adfs/oauth2/token

- 4. Select Dynamic or Static for the OAuth Certificate Usage.
  - If you select Static, copy the ADFS Signing Certificate token you created previously and paste it into the OAuth Token Certificate field. If the certificate changes, you must update the token to maintain the Replying Party Trust with the PTT Pro Server.

Configure OAuth				E	×
OAuth URL: Access URL: OAuth Certificate	https://pttproa https://pttproa	adfs.pttpro. adfs.pttpro.	.zebra.cor .zebra.cor		
Usage: OAuth Token Certificate:	Dynamic BEGIN Cl MIIGeTCCBV kiG9w0BAQs MQswCQYD W5jMRkwFw	Static ERTIFICAT VGgAwIBA FADBe VQQGEwJ YDVQQLE	TE \glQCaOibAXZW9w+JDzXKY7hRzANBgkqt IVUzEVMBMGA1UEChMMRGInaUNIcnQgS ixB3		
			Submit Car	ncel	

 If you select Dynamic, enter the Open ID Metadata URL into the Open ID Metadata URL field. The URL automatically handles certificate rotation.

For example, <Server URL>/.well-known/openid-configuration .

Configure OAuth						×
OAuth URL: Access URL: OAuth Certificate	https://pttproa https://pttproa	dfs.pttpro.	zebra.cor zebra.cor			
Usage:	Dynamic	Static				
Open ID Metadata URL:				This field is re	quired.	
					Submit	Cancel

#### 5. Click Submit.

The Relying Party Trust is established in the PTT Pro Server.

# **Configuring Profile Manager to Support OAuth2**

The steps for configuring Profile Manager to support OAuth2 differ from the steps to configure PTT Pro.

Profile Manager configuration requires five elements, each element can be derived from the Well- Known URL, the ADFS Configuration, or the Token Certificate.

• Enter each of the elements in the OAuth Details screen, as shown in the example below.

OAuth Details:
Host Url
pttproadfs.pttpro.zebra.com
Authentication Path
/adfs/oauth2/authorize?resource=pttpro-id
Token Path
/adfs/oauth2/token
Client ID
f3918ba0-2478-4b6e-9f0d-a3830127647b
Client Secret Key
Token Username
upn
Client Authentication *
Send client credentials in body

#### Host URL

The is the customer domain. The Host URL is the prefix for the Authentication and Token Path. https is assumed and automatically added by the system.

#### **Authentication Path**

The authorization path is found by browsing to the Well-Known URL. The Resource query of the Relying Trust Identifier must be added to the URL, as in ?resource=pttpro-id.

#### **Token Path**

The token path is appended to the Host URL as it is captured in the JSON response from the Well-Known URL.

#### **Client ID**

The Client ID is provided by the customer and copied at the time of creating the Relying Trust.

#### **Client Secret Key**

The secret is provided by the Customer and it is created when the Native Application Group is established.

#### Token Username

The Token Name can be determined by using the JWT.IO web site to examine the access token retrieved by Postman.

# **External References**

There are a number of ways to configure ADFS but the configuration should allow Workcloud Communication servers to communicate with the ADFS deployment.

The ADFS administrator may find the following links helpful.

- Single log-out for OpenID Connect with AD FS | Microsoft Docs
- How to enable cross-app SSO on Android using MSAL Microsoft identity platform | Microsoft Docs
- Mobile application authentication documentation | Microsoft Docs
- <u>The mystery of the missing ADFS OAuth JWT claims | by Rory Braybrook | The new control plane |</u>
   <u>Medium</u>
- How to configure intranet forms-based authentication for devices that do not support Windows
   Integrated Authentication (WIA) | Microsoft Docs
- AD FS 2016 Single Sign On Settings | Microsoft Docs
- AD FS OpenID Connect/OAuth Concepts | Microsoft Docs

# **Revision History**

Changes to the guide are listed below:

Change	Date	Description
MN-004591-01	08/2022	First version.
MN-004591-02	02/2024	Added topic for changing the access and refresh token lifespans.
MN-004591-03	05/2024	Updated OAuth configuration for the PTT Pro Server.



www.zebra.com