PTT Pro and Profile Manager

Workcloud Communication

SAML Integration Guide

ZEBRA

MN-004608-03EN Rev A

Copyright

2025/04/10

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.

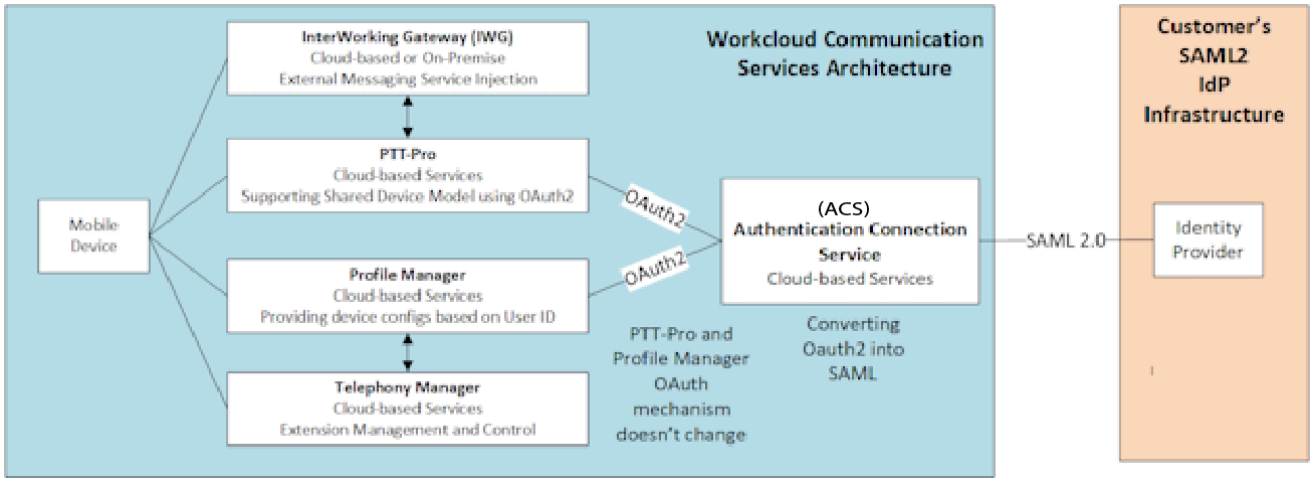
NOTE: based on a customized open-source Keycloak environment. The off-the-shelf Keycloak system does not provide the capabilities described in this document.

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.

Figure 1 Workcloud Communication



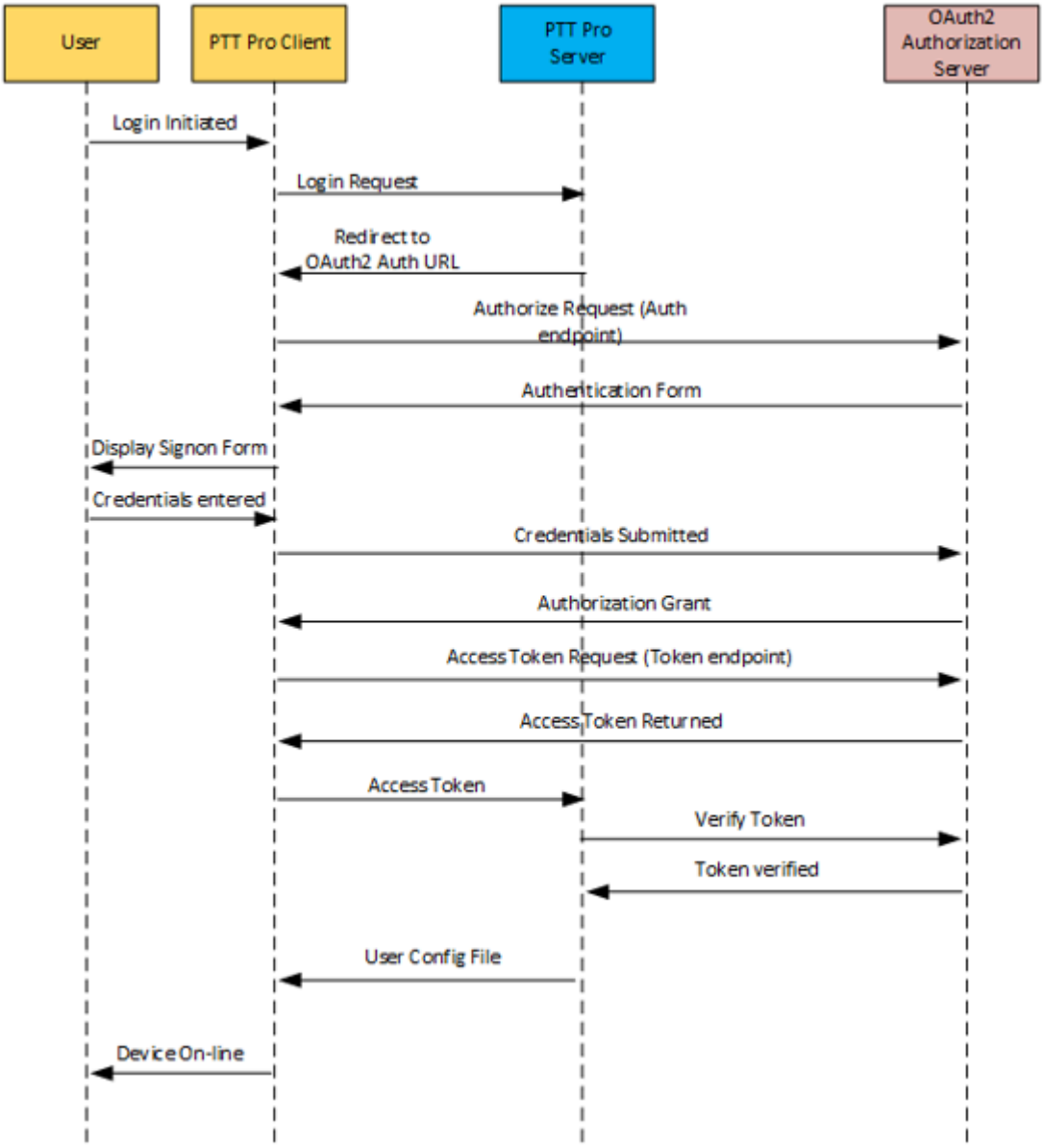
User Authorization Diagrams

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.

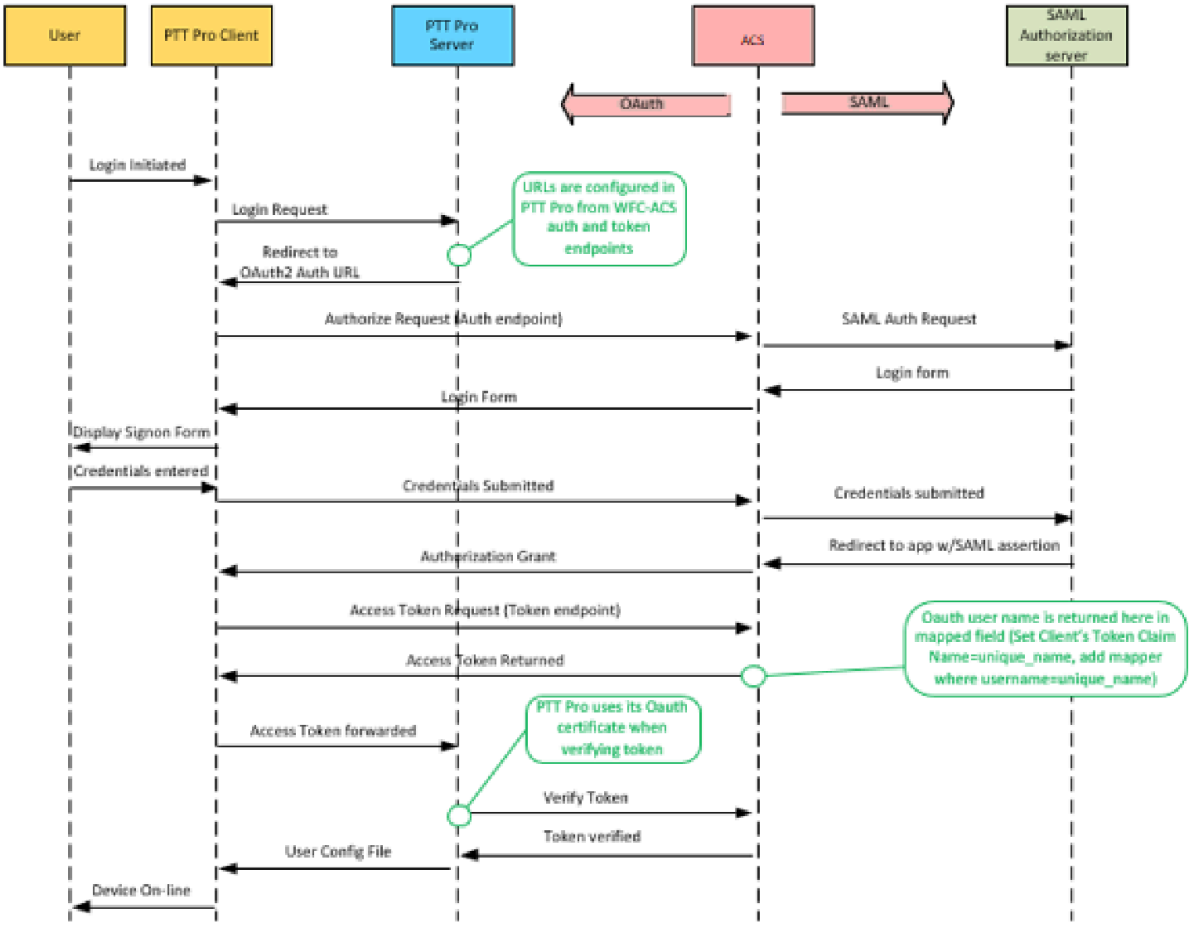
After the administrator understands the AD/ADFS (Active Directory / Active Directory Federated Services) operations, the next diagram introduces ACS and how the flow of authorization is transferred or converted from OAuth to SAML. Both PTT Pro and Profile Manager servers are shown.

Figure 2 PTT Pro Shared Device Using OAuth2



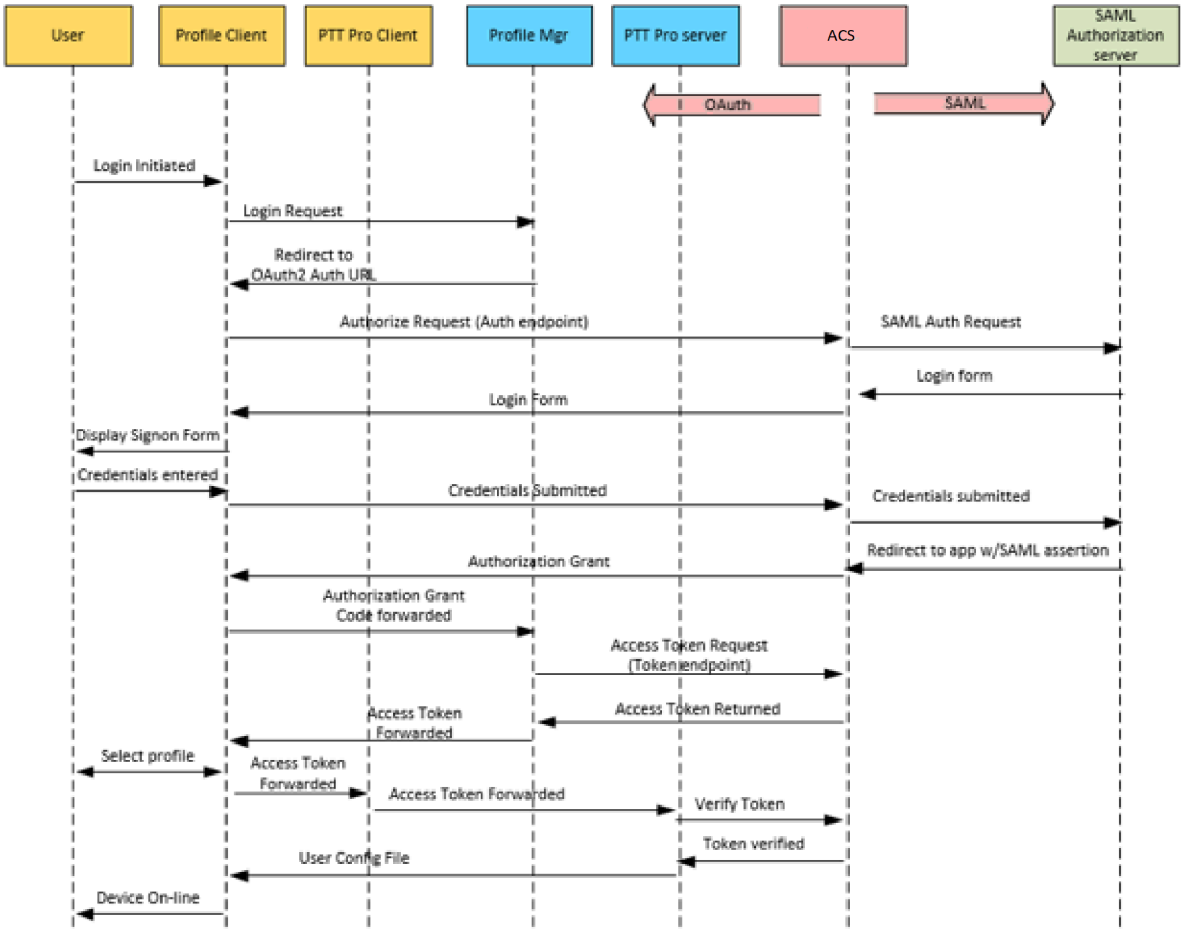
Once an understanding of the AD/ADFS (Active Directory / Active Directory Federated Services) is developed, the following diagram shows the introduction of ACS and in a standalone PTT Pro configuration.

Figure 3 PTT Pro Shared Device Using ACS



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

Figure 4 Profile Manager and PTT Pro Shared Device Using ACS



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

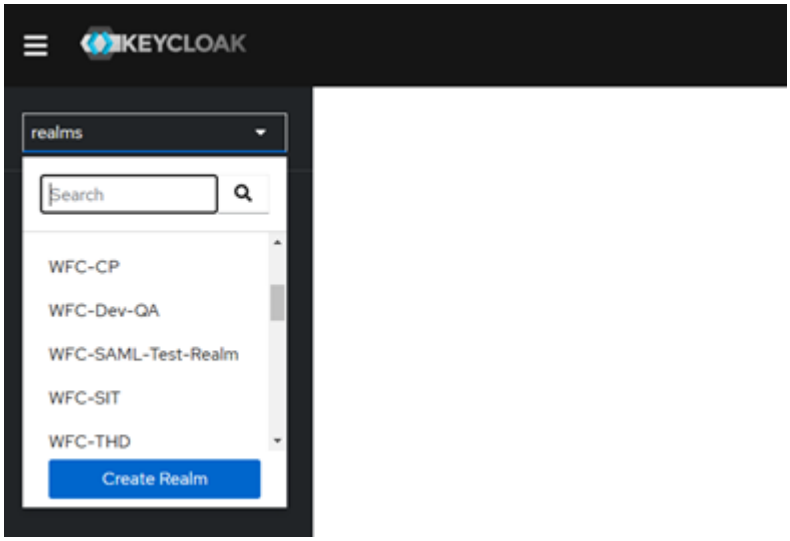
The identity provider communicates with the SAML server using the SAML protocol.

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.

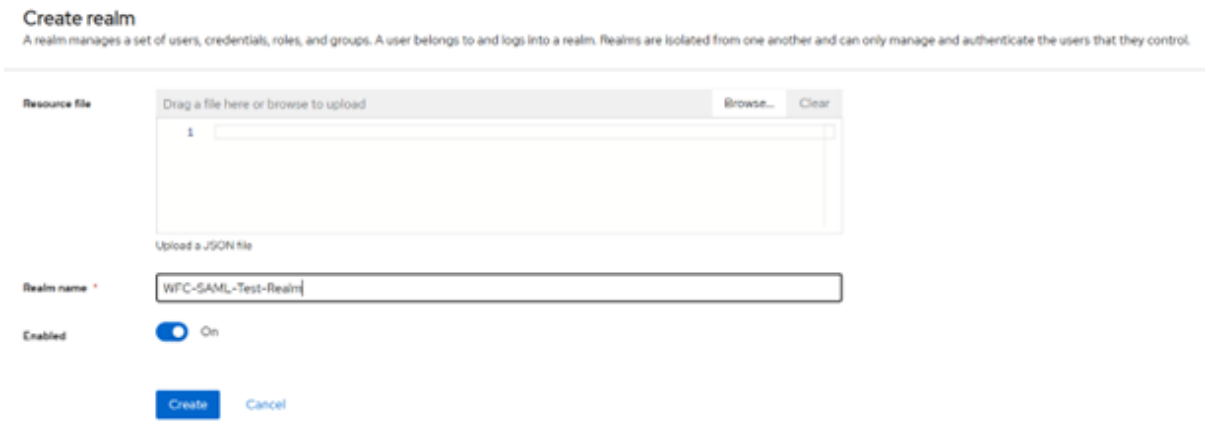
1. Browse to the assigned ACS service and sign in.



   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.

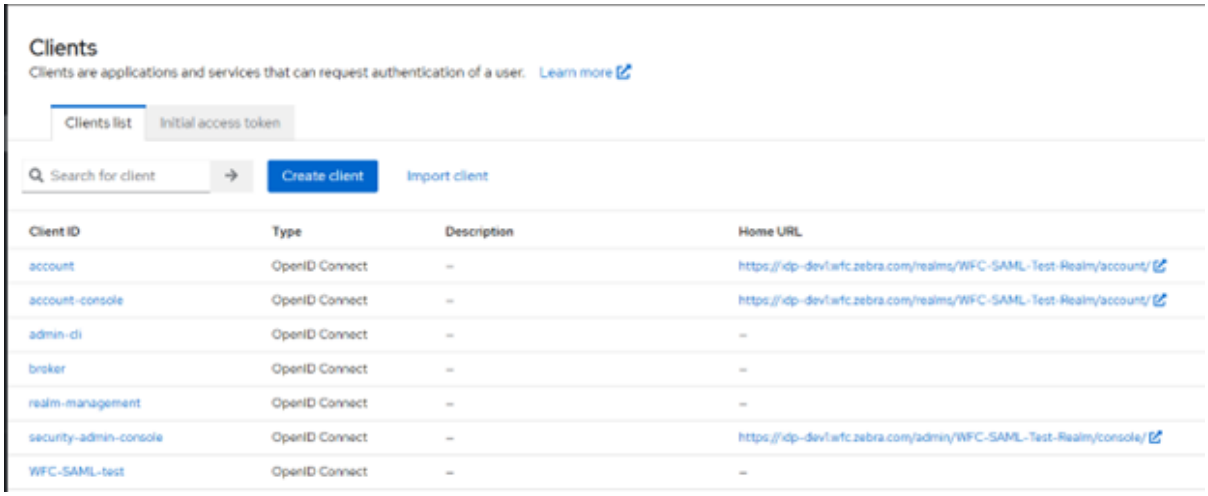


Creating the Clients

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.

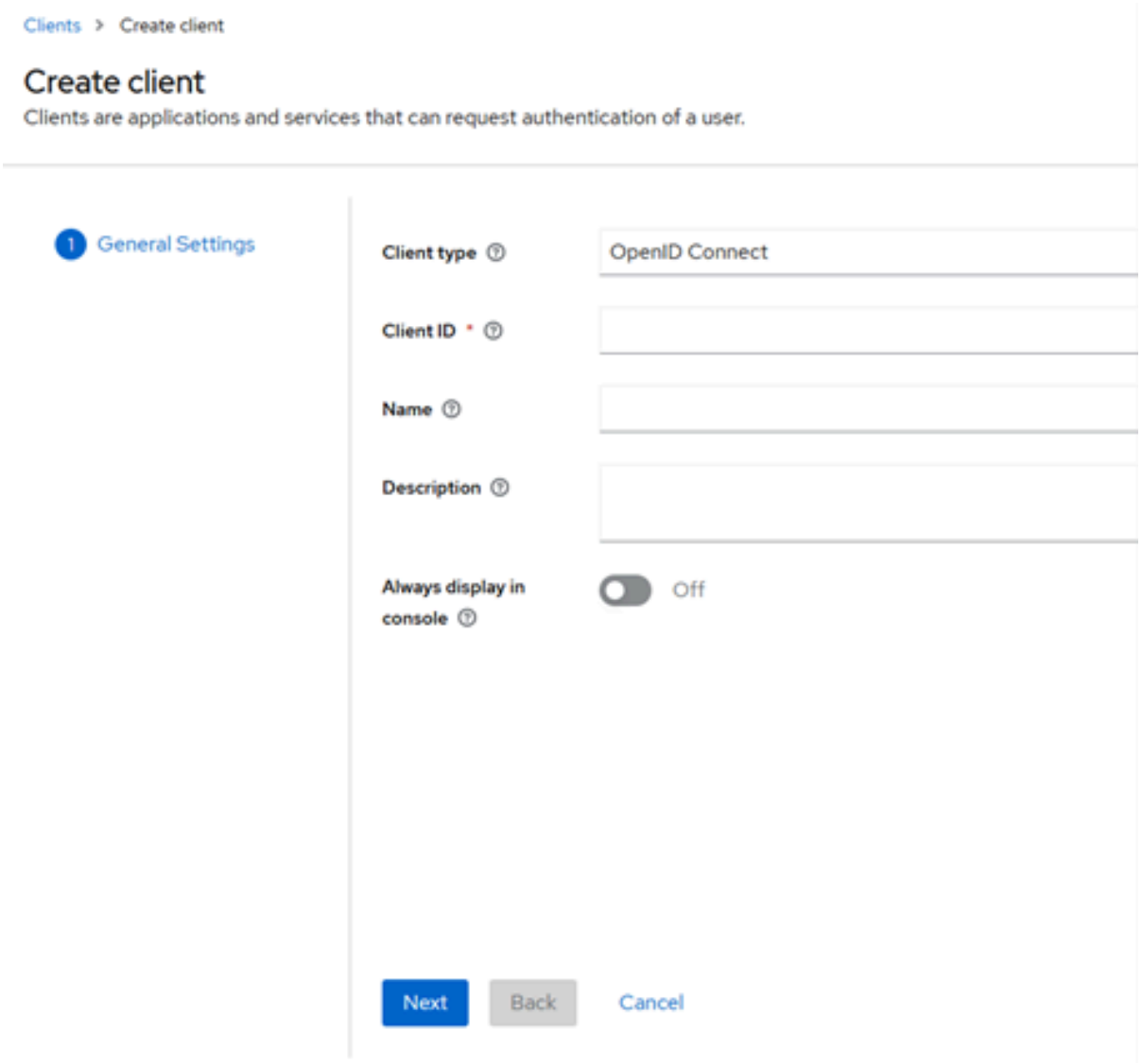
1. Click **Create** to display the **Add Client** dialog.



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.



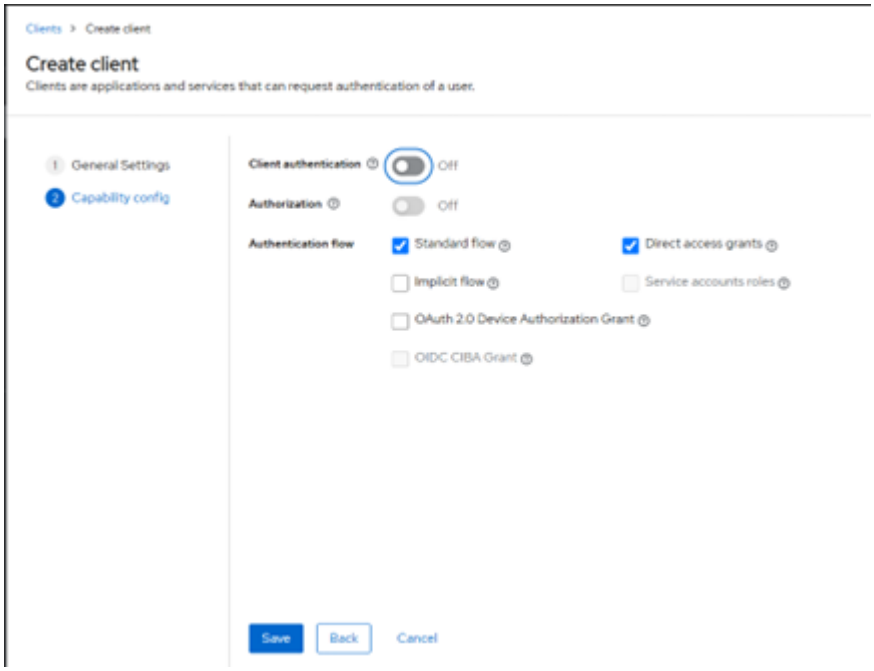
   c) Click **Next**.

   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**.

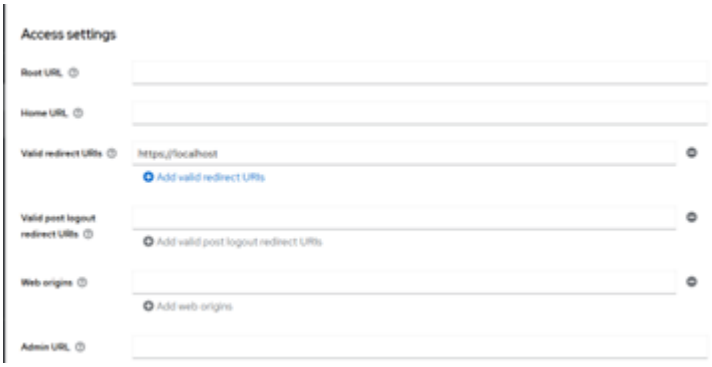
3. Click **Save** to display the rest of the settings.



Configuring the Access Settings

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

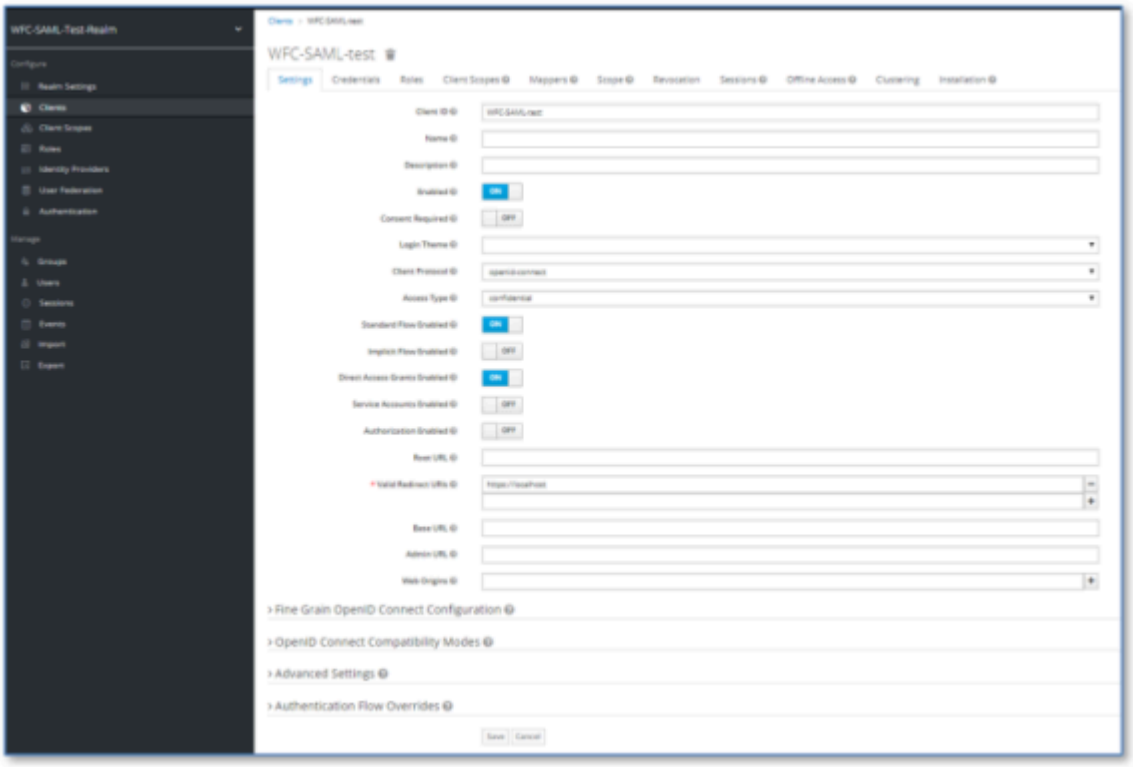
Enter `https://localhost` in the **Valid Redirect URI** field.



Configuring the Endpoint Settings

Configure the settings for the OAuth client endpoint.

1. Set **Enabled** to **ON**.



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

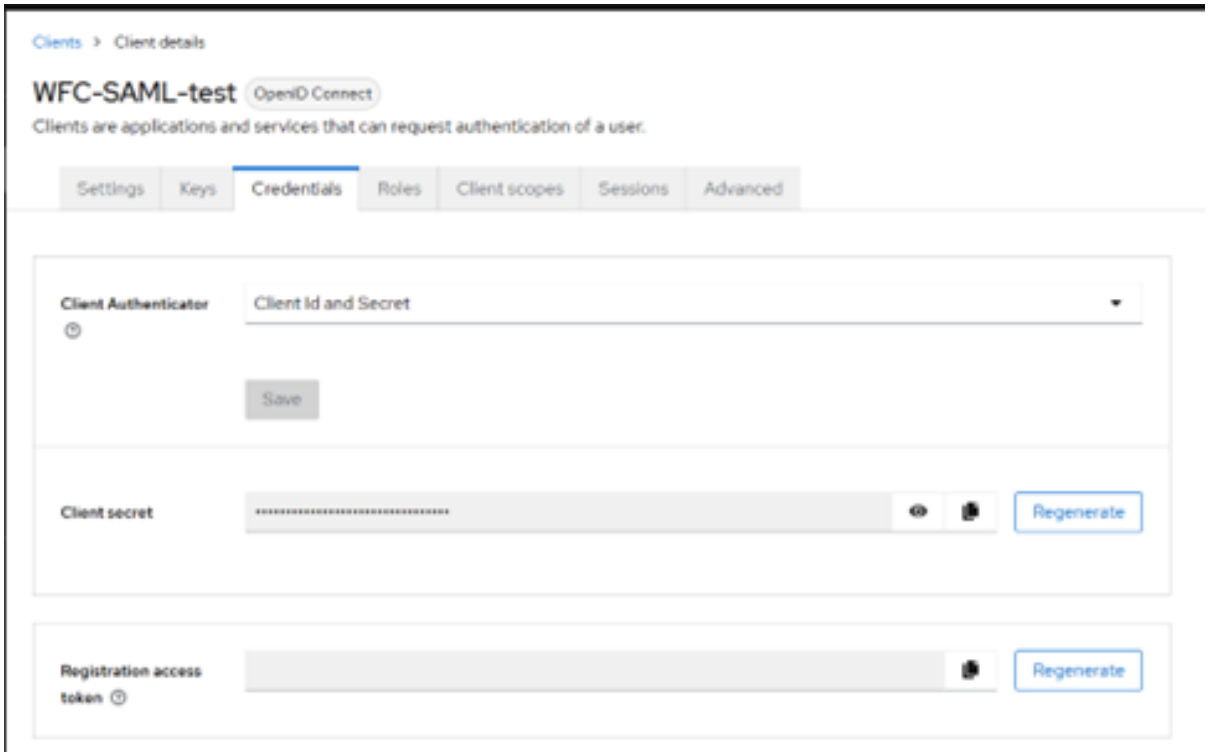
   This field is required but is not used for this implementation. It enables Keycloak to call back to its resource manager.
4. Click **Save** to display the **Credentials** tab.

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.



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"
```

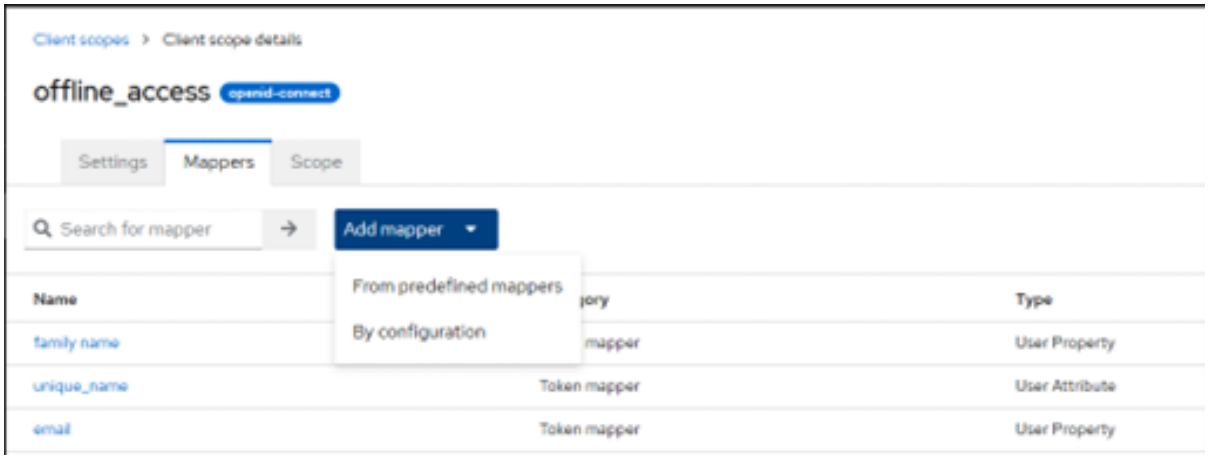
Configuring the Endpoint Mappings

Map the Oauth username to the SAML username.

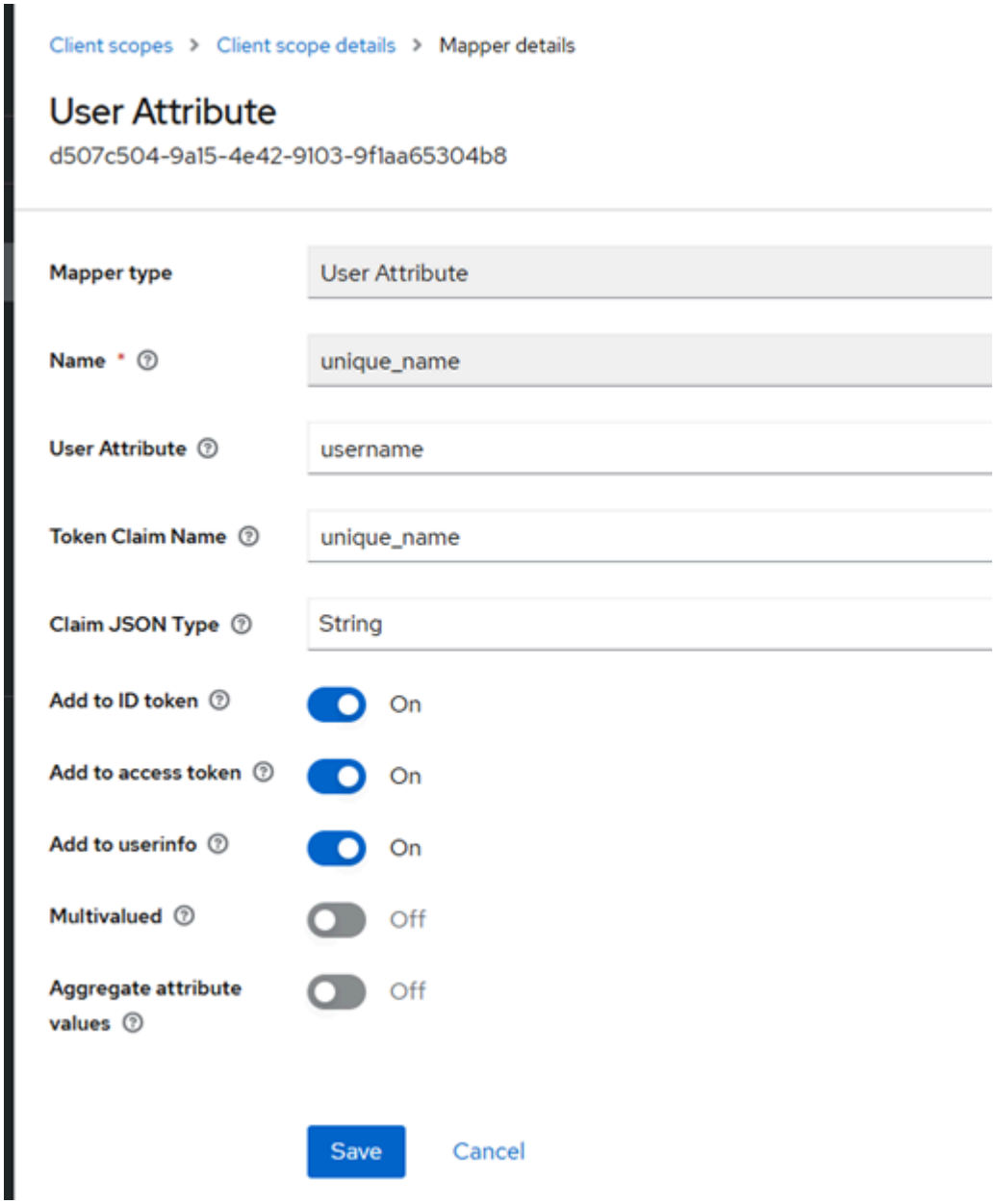
1. Select the **Client Scopes** option on the left pane.
2. Select **offline_access** scope under client scopes in the right pane.

   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**.



4. Click **User Attribute**.

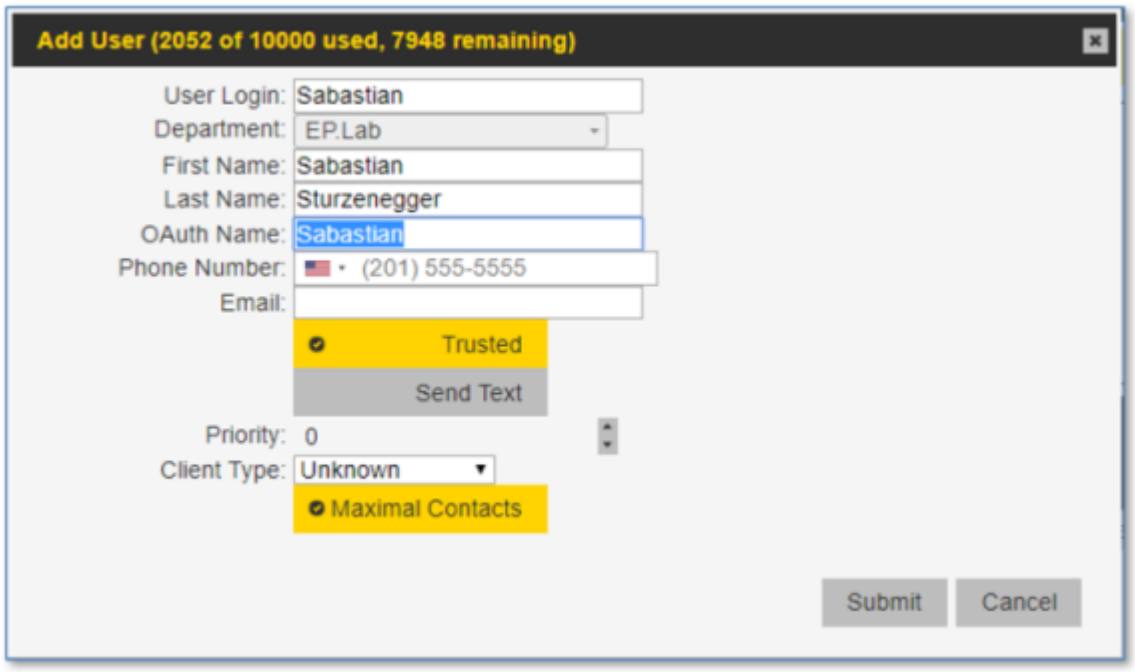


5. Enter the following details:
   a) Enter `unique_name` in the **Name** field.
   b) Enter `username` in the **User Attribute** field.
   c) Enter `unique_name` in the **Token Claim Name** field.
   d) Enable the **Add to ID token**, **Add to access token**, and **Add to userinfo**.

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.



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 Sample Descriptor File 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.

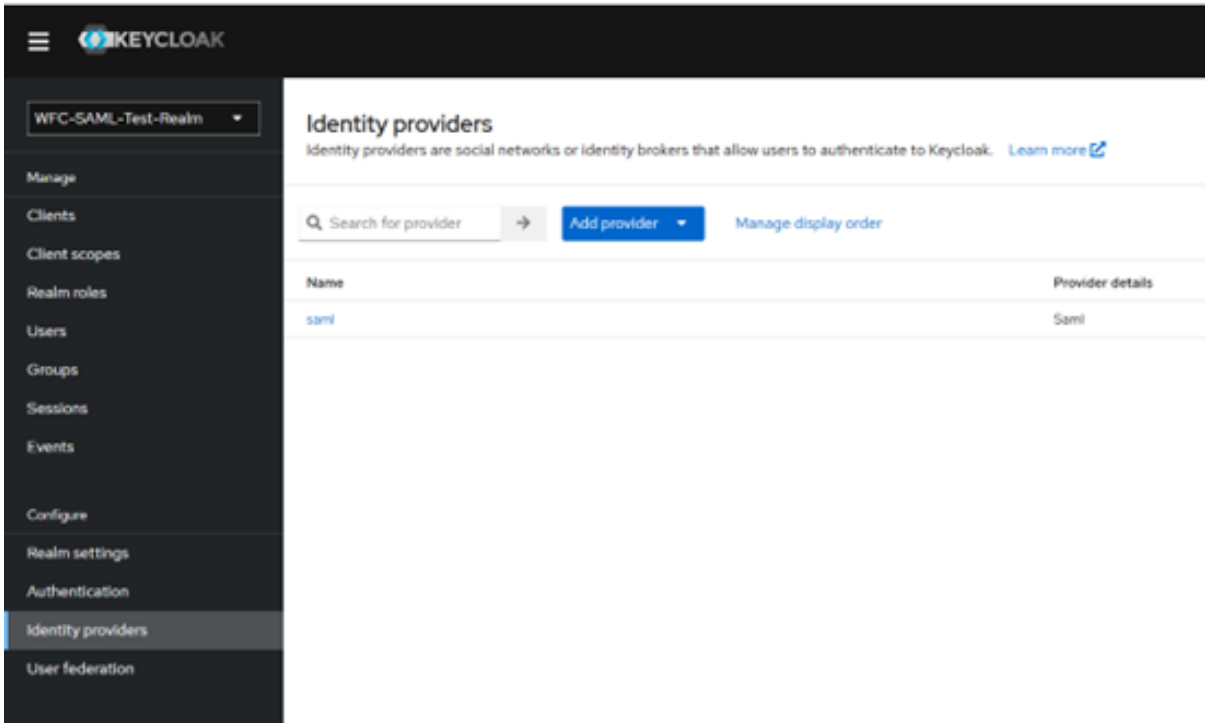
Figure 5 SAML Descriptor File

```
-->
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Name=
"urn:keycloak">
<EntityDescriptor entityID="https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm">
<IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo>
<ds:KeyName>hUZRioKF37oEHBGkHpdQky9QsGbbf6Bpk0Y799ttxOA</ds:KeyName>
<ds:X509Data>
<ds:X509Certificate>
MIICtTCCAZ0CBgFwU7lhlzANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDDBNXRkMtU0FNTC1UZXN0LVJlYWxtMB4XDTIwMDIxNzElMTUyMloXDTMwMDIxNzElM
TcwMlowHjEcMBoGA1UEAwwTV0ZDLVNBTUwtVGVzdC1SEWFabTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIyaupwSIC+gOuvvym4yxErDiu6K4p
AaqmjRMYllLE5TTzyh0RbiG9tGrr86jXFzlFdkEV6GST1FT4e3r2Z9VUE+eNGgeCun6IsMyXjwzHprkH9NG+BnZ9ulExrT7nfp4PSk/FA8TkETqhzqla+12Yn
olUi5w/OI+v7oJwVn7+AZsCR5wMGU3R/7vhml/zDfS0uOfsIDFtlhgKlxKtel6PobhBn29kFWASNGm9vs/YTybraaOyCA3B4i+0tGPDLeZFpMsr7KOPPNLeOo
XlukMsDkABAnZap6MBPyZu+RnA+6xhQErh8ddobeU7Z2ob1tOZtkzbq6bhlFBDHDMDJTUI0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEANG24BxiAv1gtk32qd
D4w85pXnNmj168M84Z9mftAn4IHIw7+Wl3IjrK66EewBGa7djRG1IaHsPxRvJ7NP6DWPCiGsVhCwcKS6C0Zi9irpAHCndAoxYnLoy5kGgMhvofK/WSM4PG3E
idhlI5bOgVpzA0wAReZFHPebueJVNM8Puo+JAqaMEkkH/P0VrchCldfeMAsMa/6ws1X6ZpUKP9lDhOCs2kLsGIWnu2erv5SeR+agKL/6t04jUNIF2/C+2uIpB
rSVkw0bHIrZpmom/rjfu+Q0TAO3iOBbe/9GhQshEuNQdiAqyXbYpmeNG9PGPL4fMndmnZKiSLo7mzE75KoQ==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=
"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
<NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=
"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
"https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml"/>
</IDPSSODescriptor>
</EntityDescriptor>
</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.

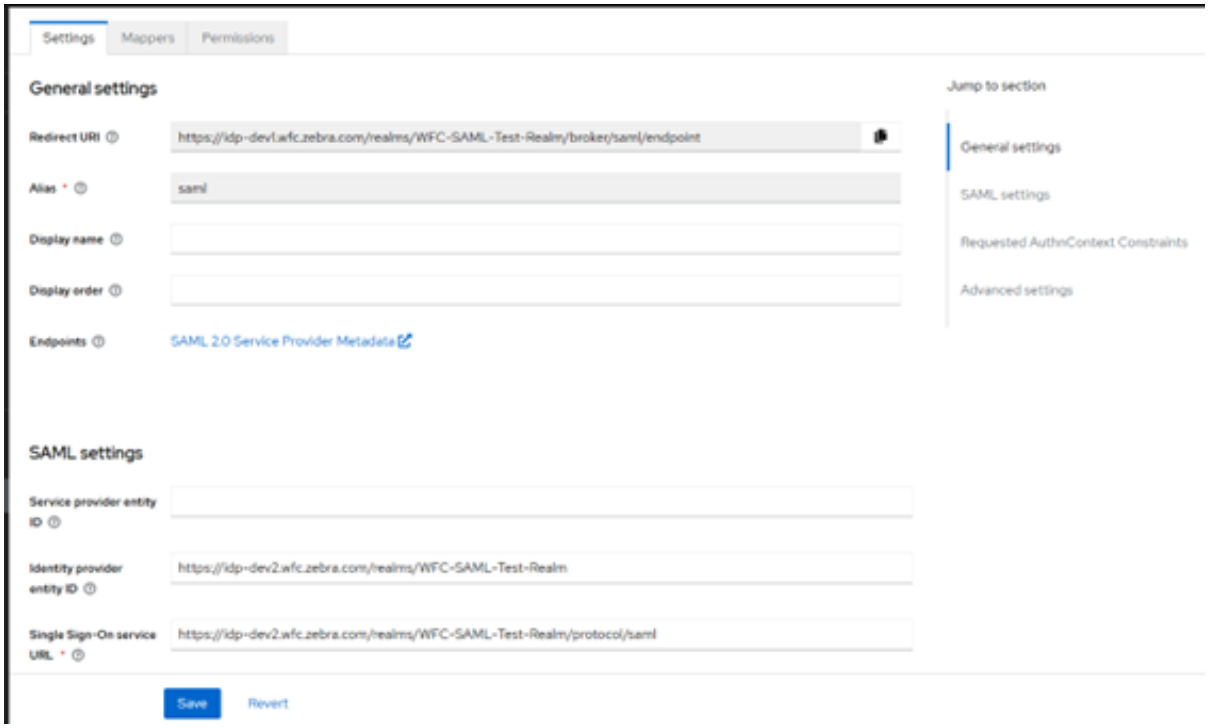


2. Select **SAML v2.0** from the Add Provider drop-down menu.
3. Enter the redirect URL in the **Redirect URI** field. The **Redirect URI** entry is constructed as follows: https://wfc-keycloak.pttpro.zebra.com/auth/realms//broker/ /endpoint .

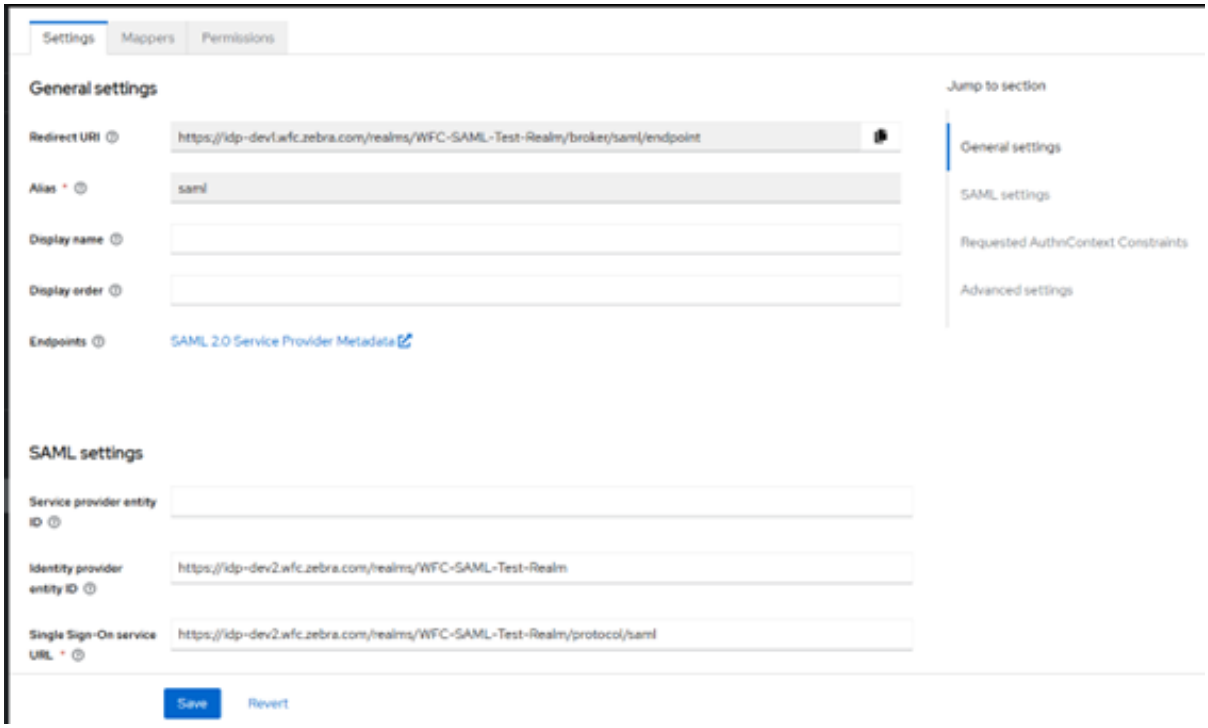
   The <Alias>is a convenient label. Change it to an appropriate value. In this example, the alias is WFC-SAML-Auth that results in the following redirect URI: https://wfc-keycloak.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/ broker/WFC-SAML-Auth/endpoint
4. Set the **Entity Descriptor** on.
5. Enter 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
Mappers
Permissions
General settings
Redirect URI
https://idp-dev1.wfc.zebra.com/realms/WFC-SAML-Test-Realm/broker/saml/endpoint
Alias *
saml
Display name
Display order
Endpoints
SAML 2.0 Service Provider Metadata
Jump to section
General settings
SAML settings
Requested AuthnContext Constraints
Advanced settings
SAML settings
Service provider entity ID
Identity provider entity ID
https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm
Single Sign-On service URL *
https://idp-dev2.wfc.zebra.com/realms/WFC-SAML-Test-Realm/protocol/saml
Save
Revert

7. Configure the SAML details.



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:

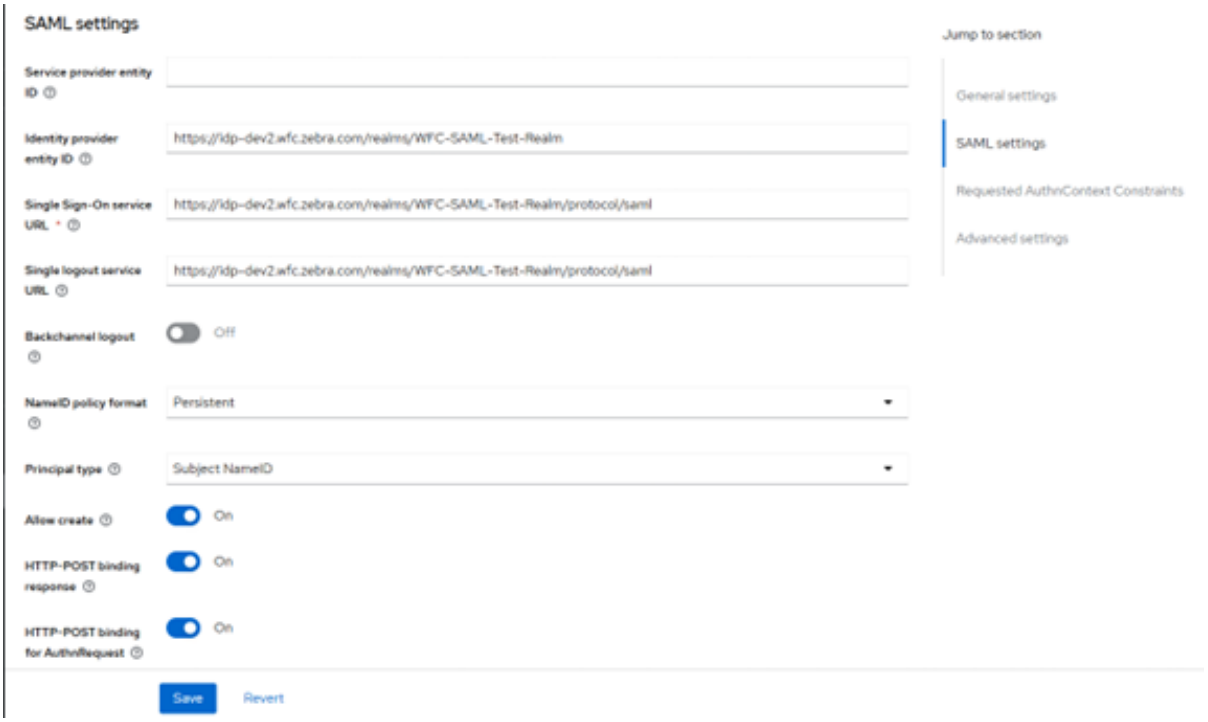
```
https://wfc-keycloak2.pttpro.zebra.com/auth/realms/WFC-SAML-Test-Realm/protocol/saml
```

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**.

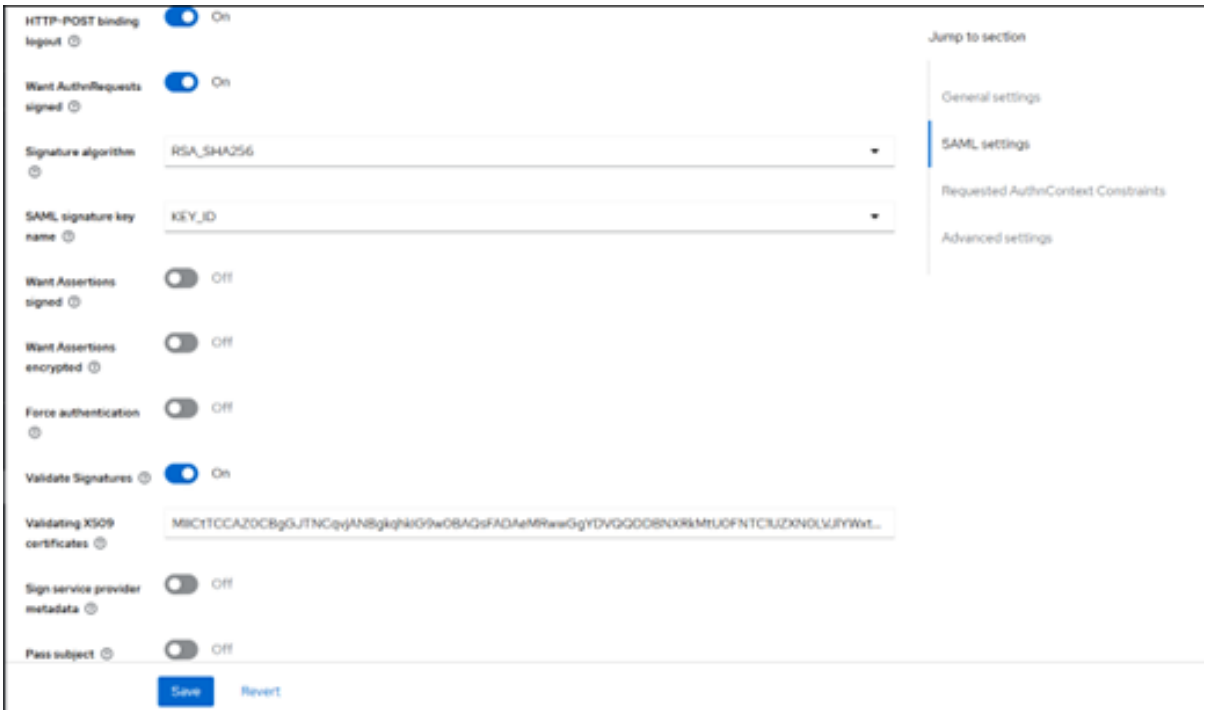


e) Enable **HTTP-POST Binding for AuthnRequest**.

f) Enable **HTTP-POST Binding Logout**.

g) Enable or Disable **Want AuthnRequests Signed**.

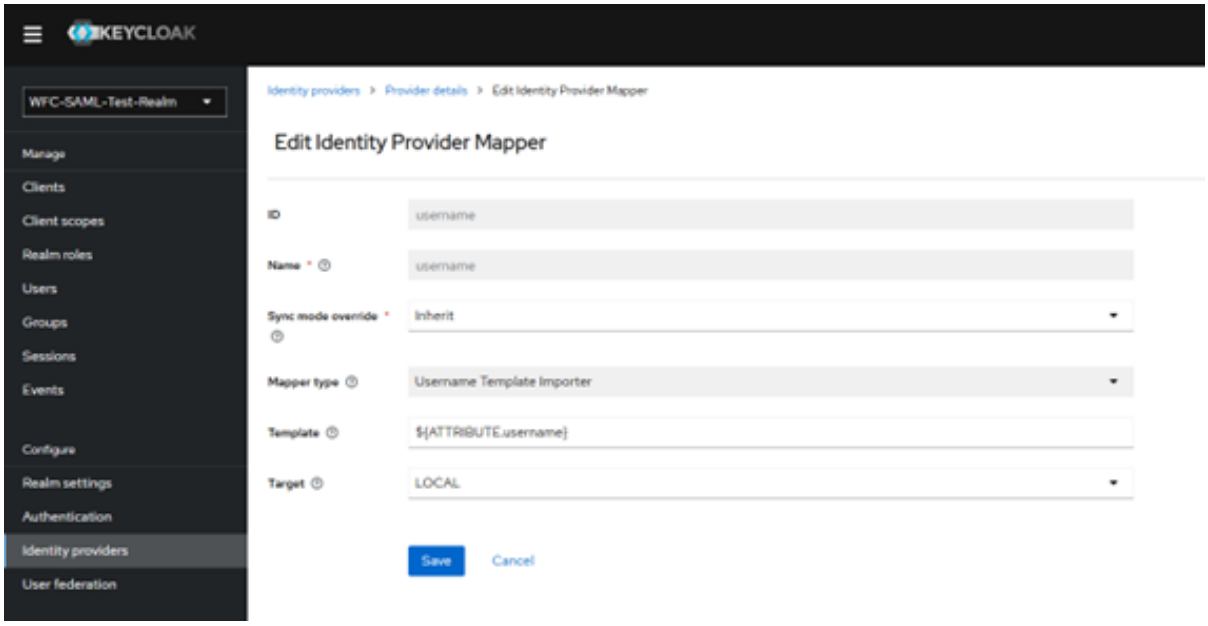
h) Click **Save**.



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.

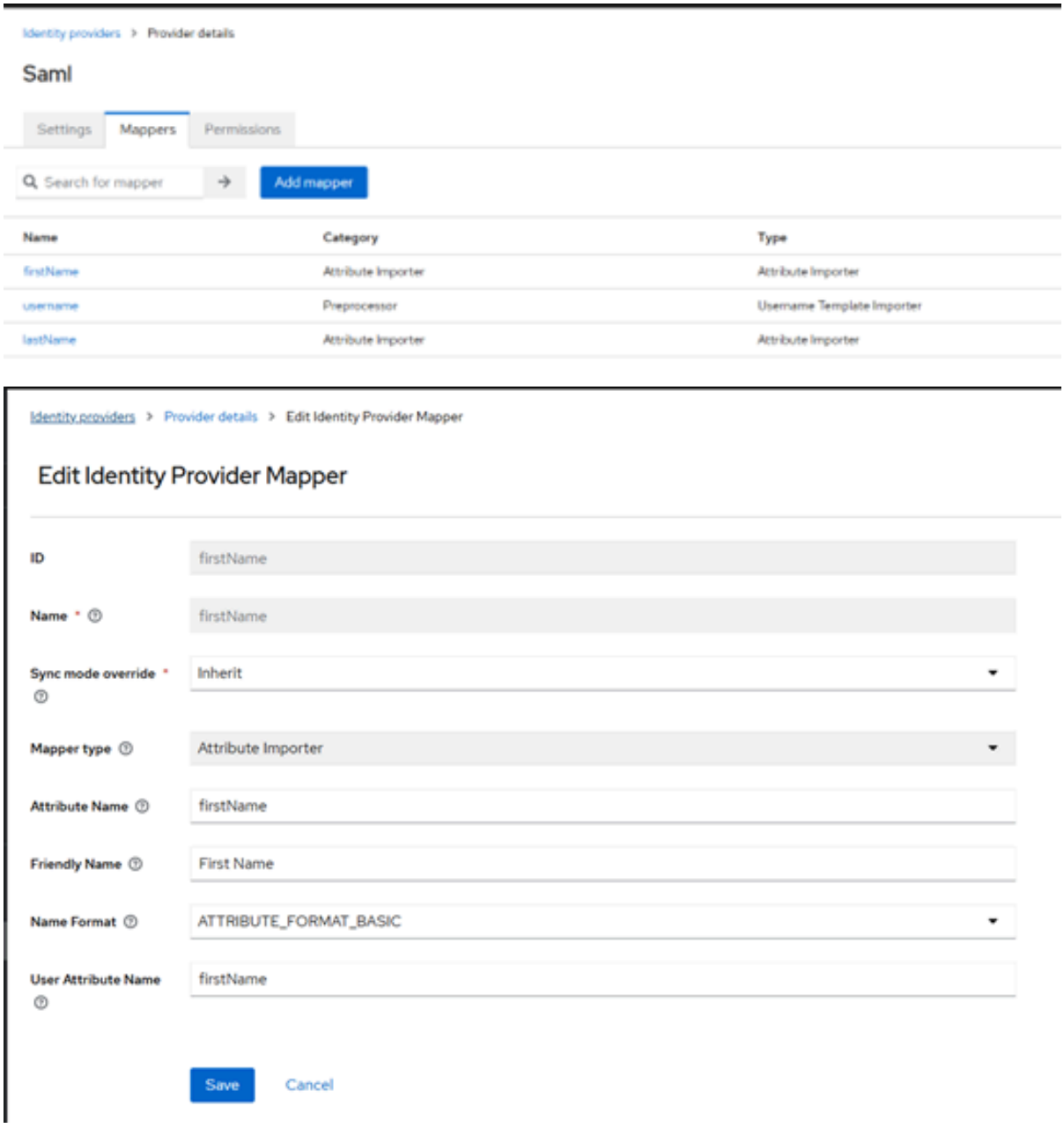
1. Select the **Mappers** tab.



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.

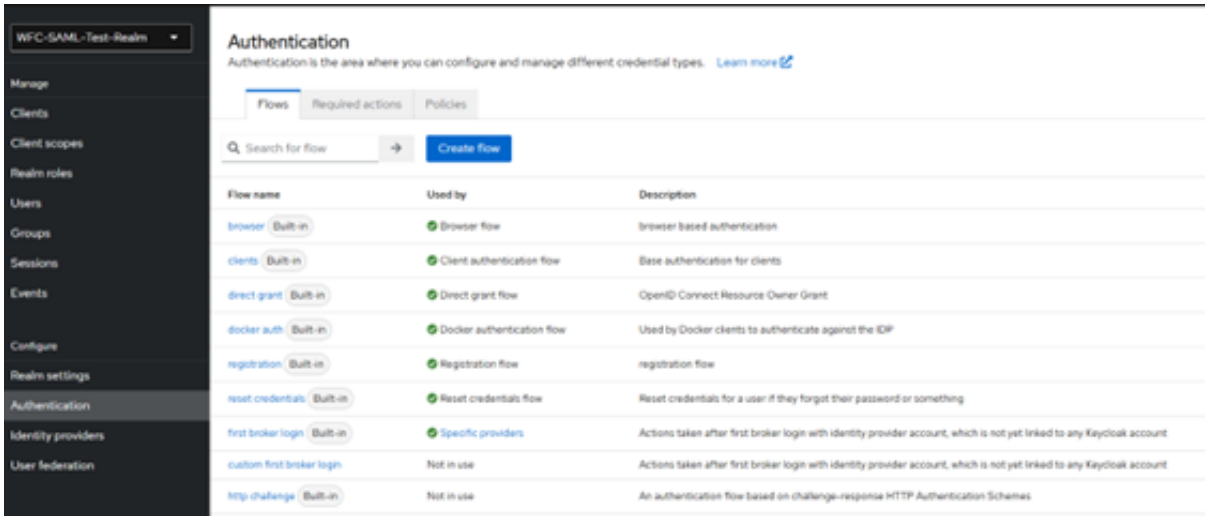


NOTE: In case of Azure AD, following attribute mapping needs to be done for **username**, **firstName**, **lastName**, and **email** fields.

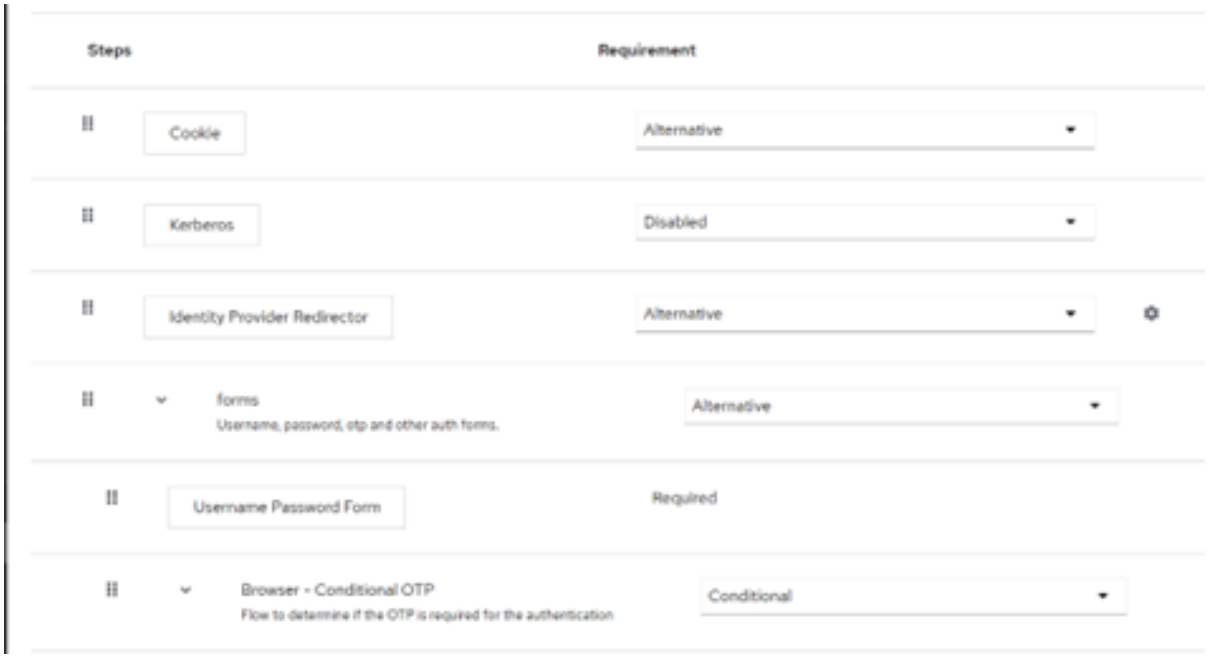
Auto Launching the SAML Login

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

1. Navigate to the **Authentication** view.



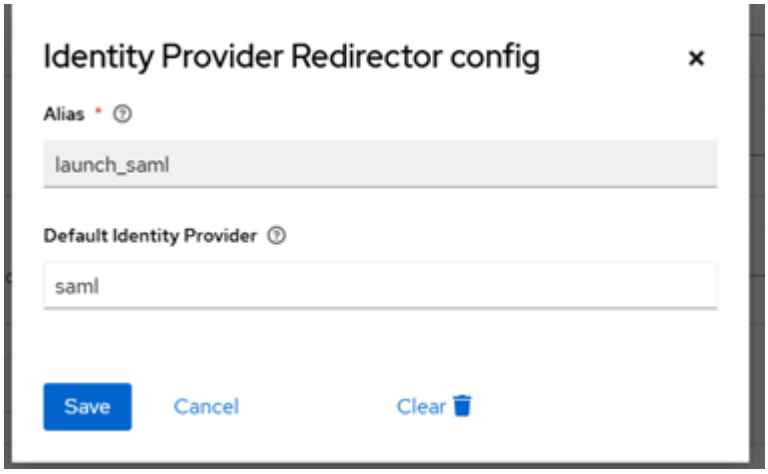
2. Select the **Flows** tab.
3. Click the **Browser** link.
4. Click **Settings** in the Identity Provider Redirector step.



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**.



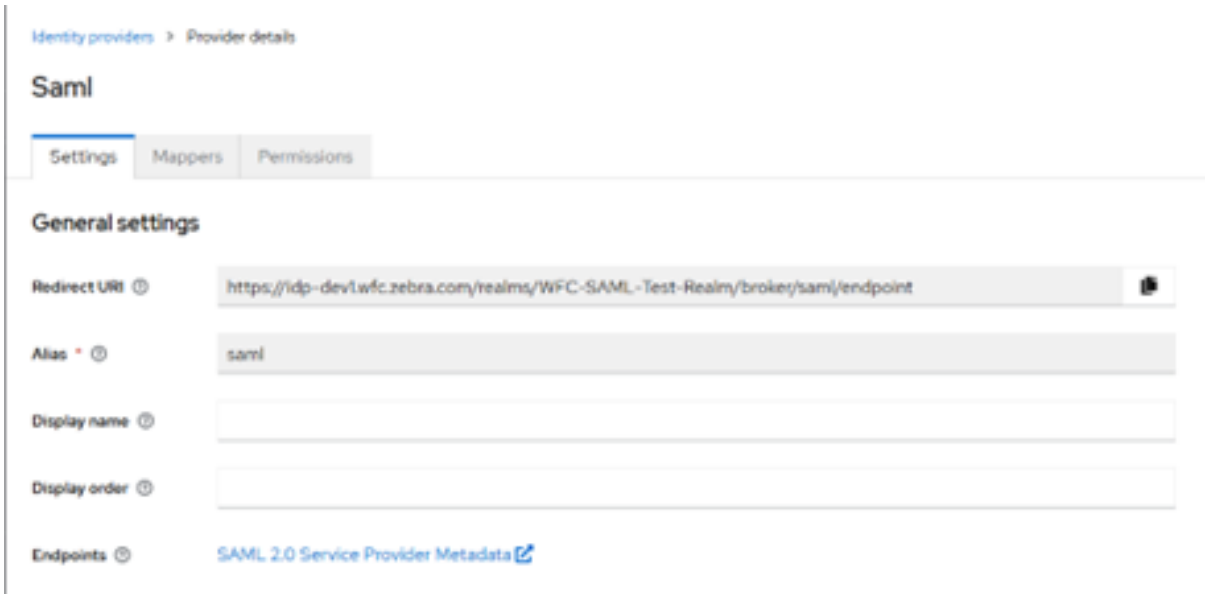
8. Click **First broker login flow** under **Flows** tab.

   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.

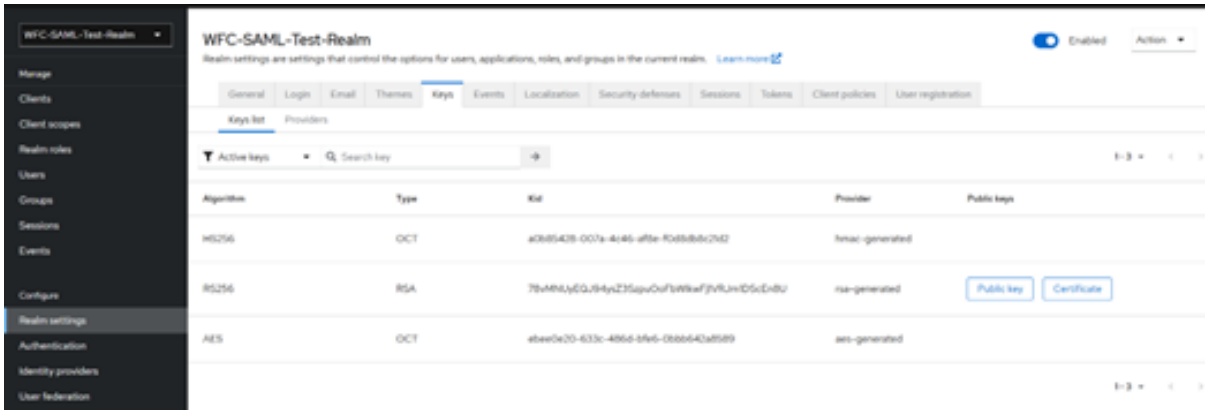


3. Copy the x509 Certificate and paste it into a text file with a file extension of `<filename>.pem`.
4. Import `<filename>.pem` into the SAML server.

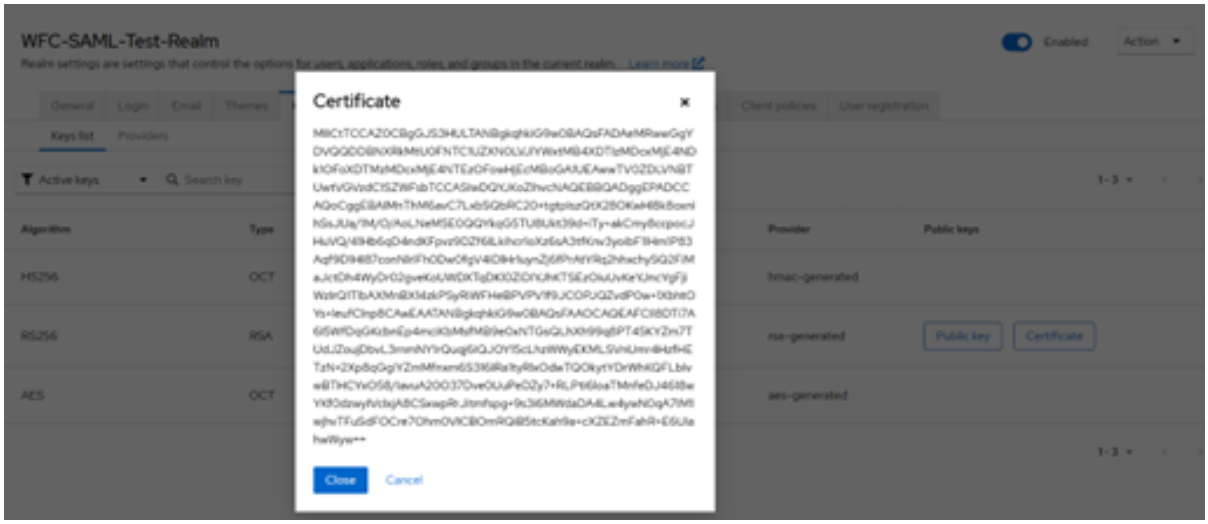
Exporting the ACS Certificate to PTT Pro

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.



2. Click on **Certificate** in the RS256 row.

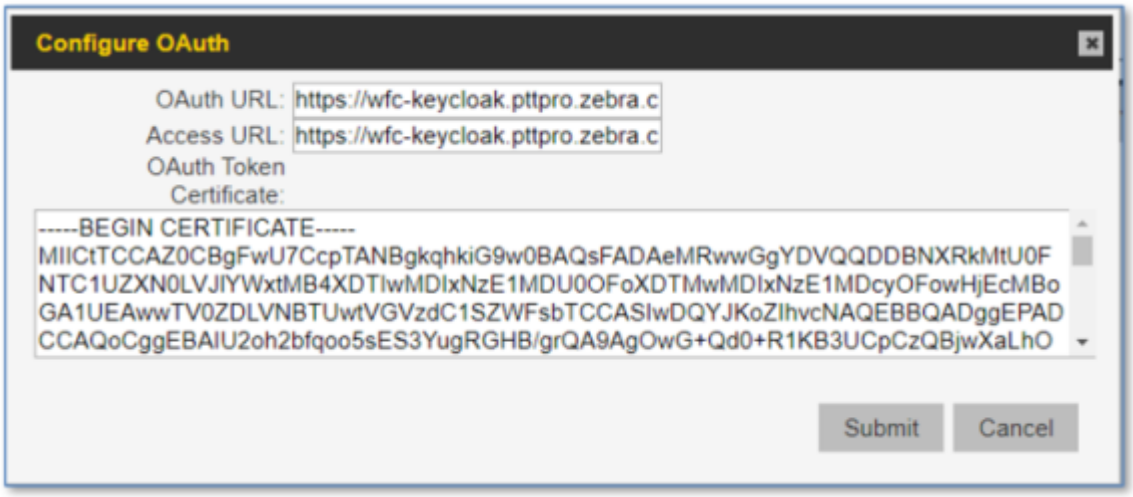


3. Copy the certificate to the OAuth definition in the PTT Pro portal, as shown below.

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>
```

```
-----End Certificate-----
```



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

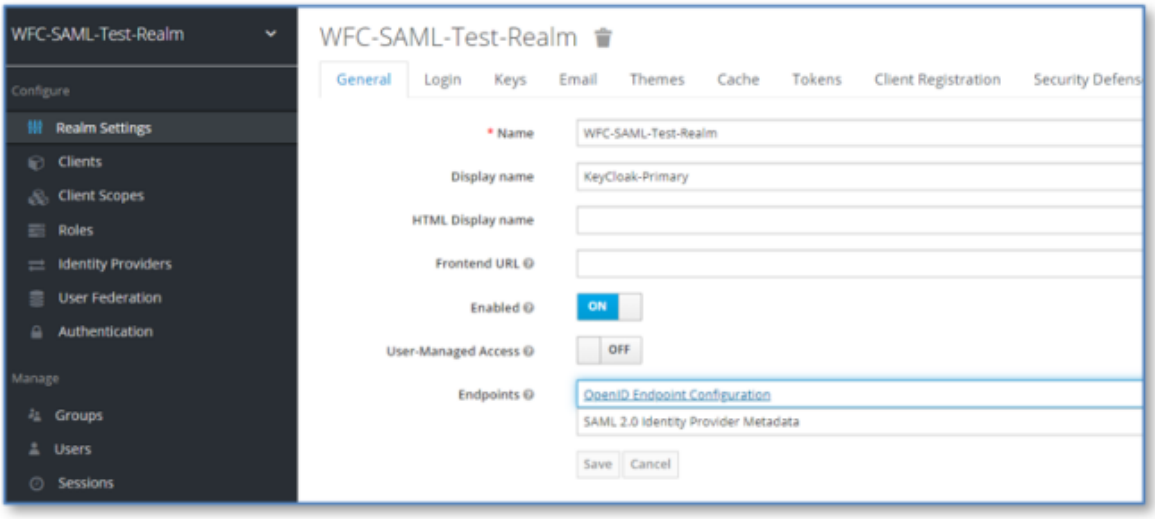
The Profile Manager server requires four configuration elements to connect to an OAuth server because the Profile Manager uses OAuth to authorize users. Using ACS requires that the Profile Manager use the Keycloak server instead of an ADFS server.

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**.



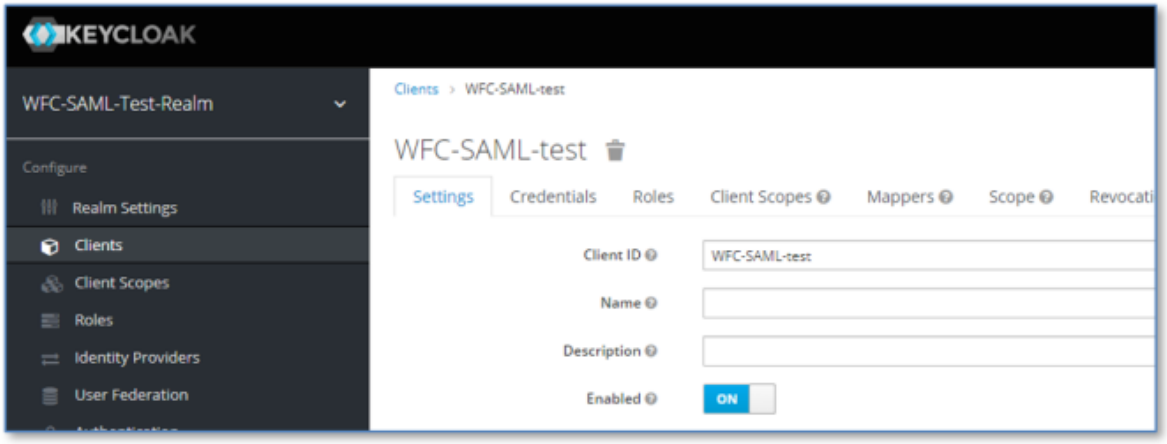
The Authorization Endpoint is copied to the OAuth URL in the PTT Pro server and provided to the Profile Manager administrator.

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.

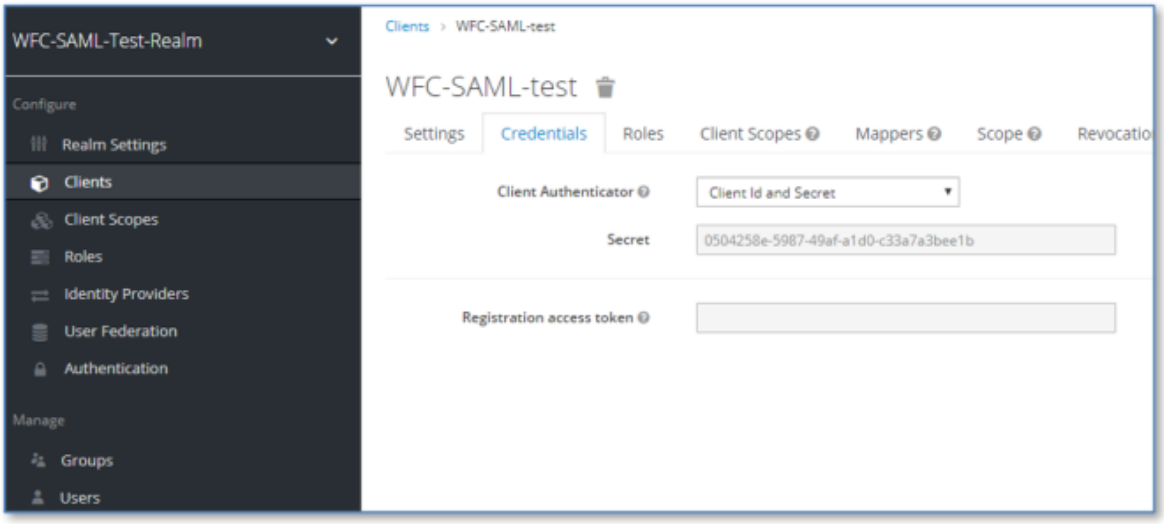
Figure 6 Client ID



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.

Figure 7 Client Secret



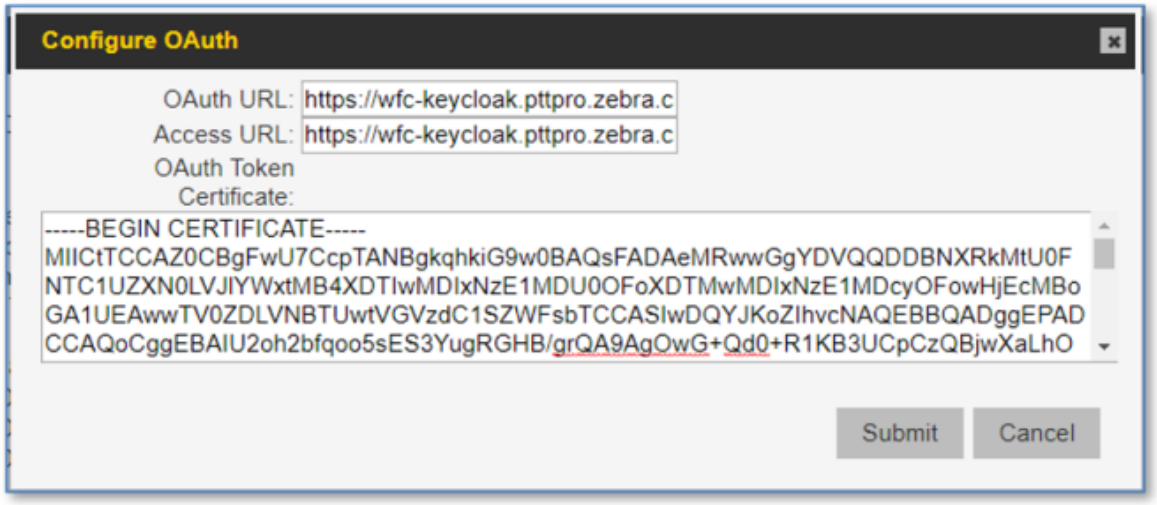
Configure the PTT Pro Server

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

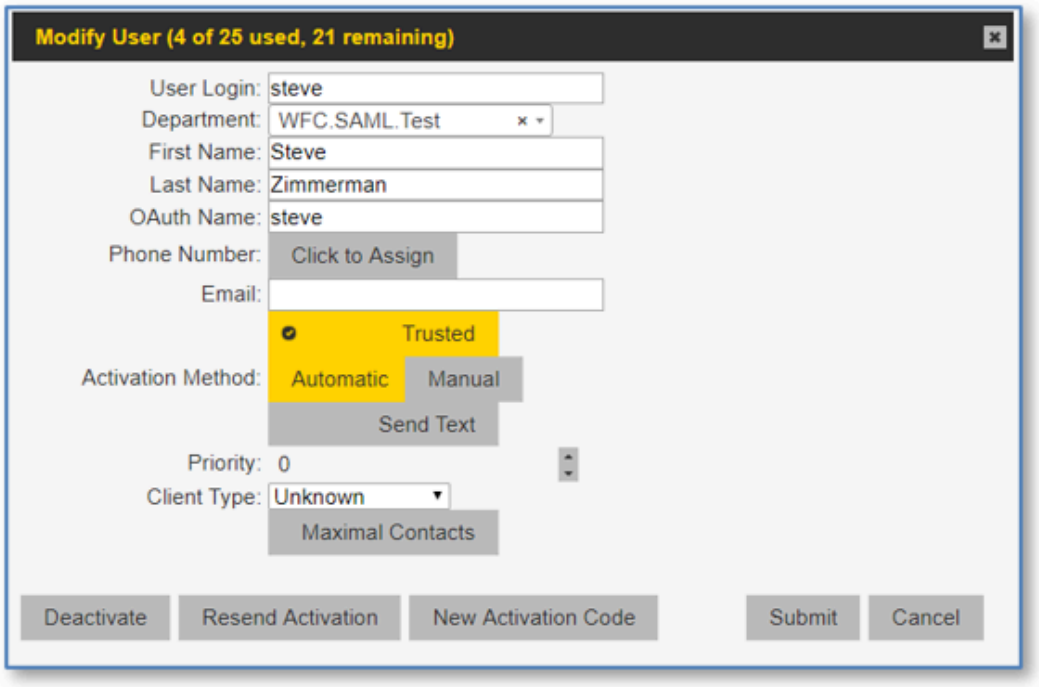
Figure 8 PTT Pro OAuth Configuration



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.

Figure 9 PTT Pro User with SAML username

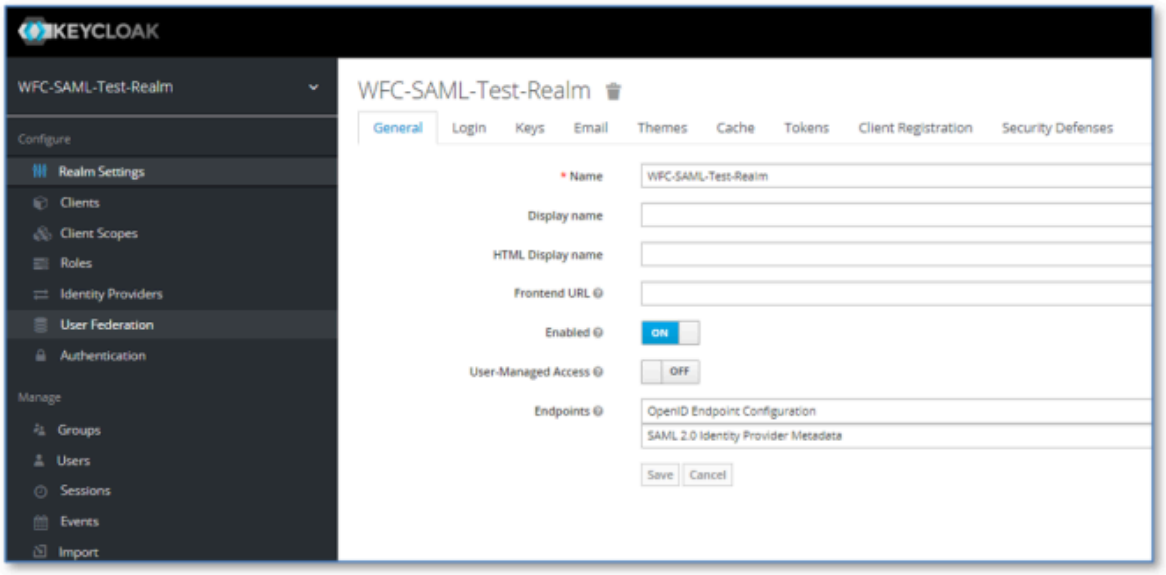


Obtain the OAuth and Access URLs

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**.

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

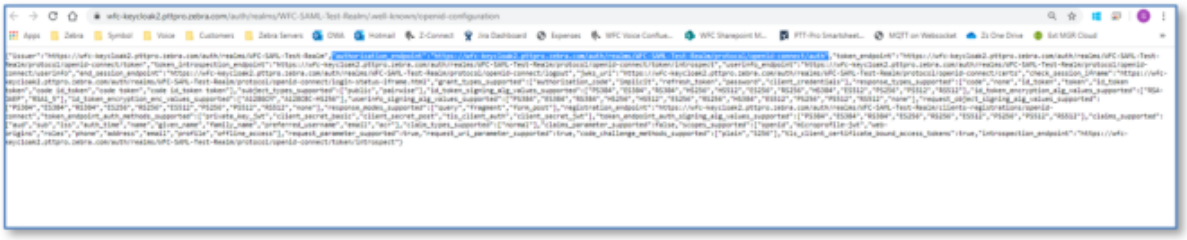
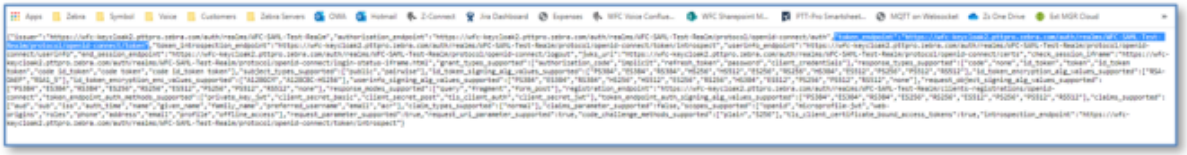


Figure 12 Access URL for PTT Pro Access URL Field



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.

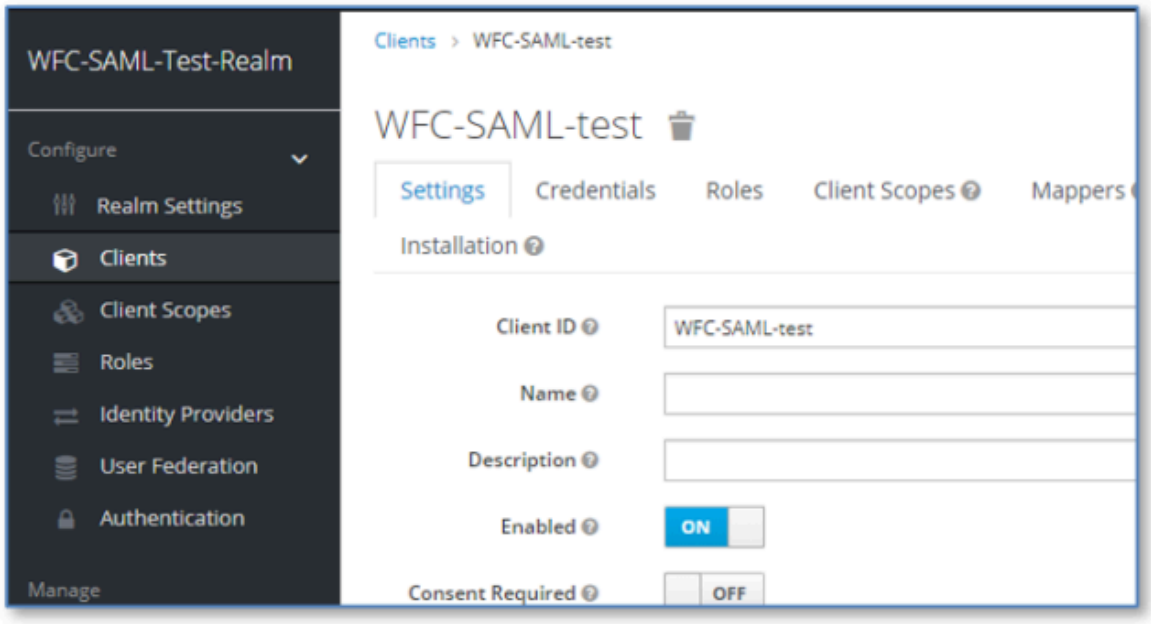
Configure the PTT Pro Client

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

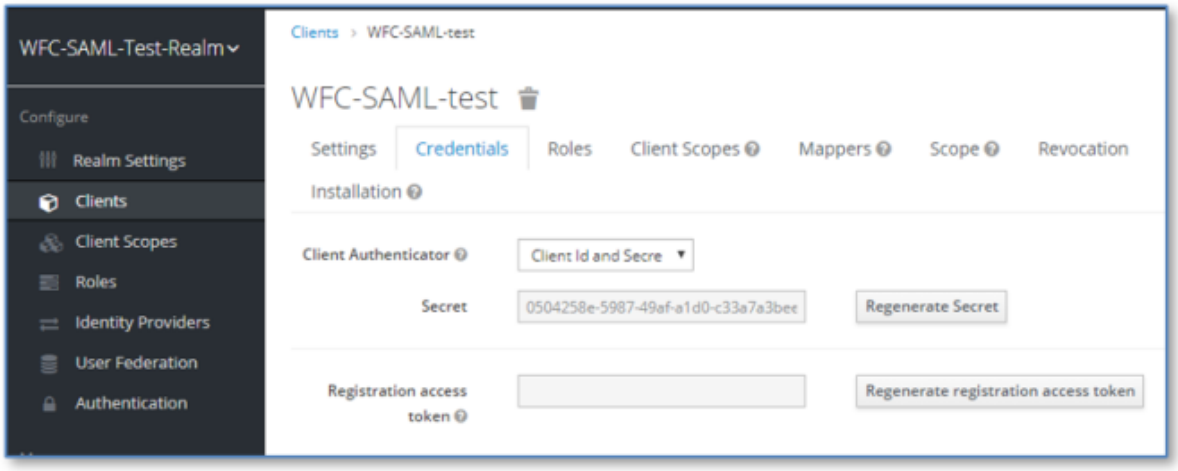
The `oauthClientID` field is obtained from the ACS service and is the value of the **Client ID** field in the **Settings** tab of the **Clients** view.

Figure 13 oAuthClientID Value



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

Figure 14 oAuthClientSecret Value



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

```
{
  "oAuthClientID":"WFC-SAML-test",
  "oAuthClientSecret":"0504258e-5987-49af-a1d0-c33a7a3bee1b"
```

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

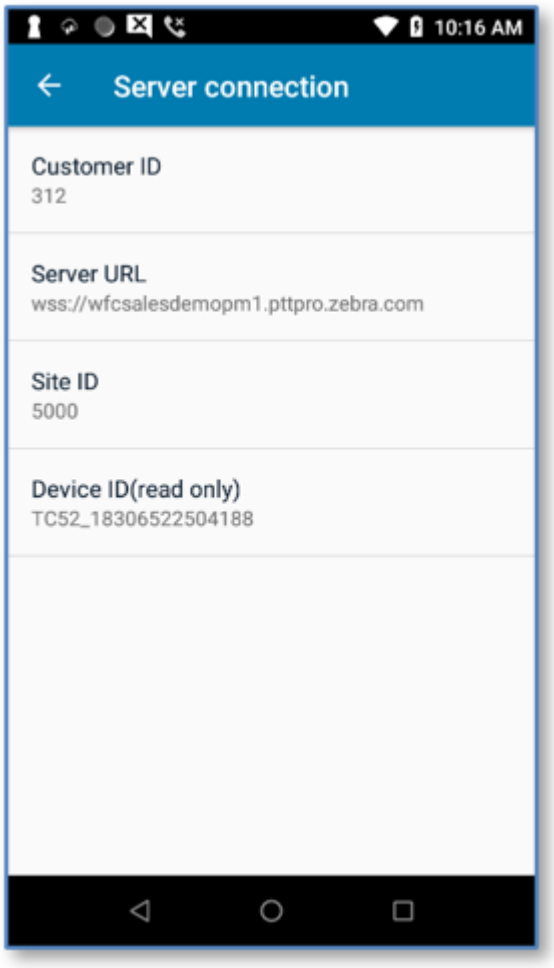
```
adb shell am broadcast -a com.symbol.wfc.pttpro.ACTION_DEFAULT_CONFIG --es
 "configpath" /sdcard/WFCPTTProDefault.json"
```

Configure the Profile Client

The configuration of the Profile Client requires two parameters.

- Customer ID
- Server URL

Figure 15 Profile Client Configuration



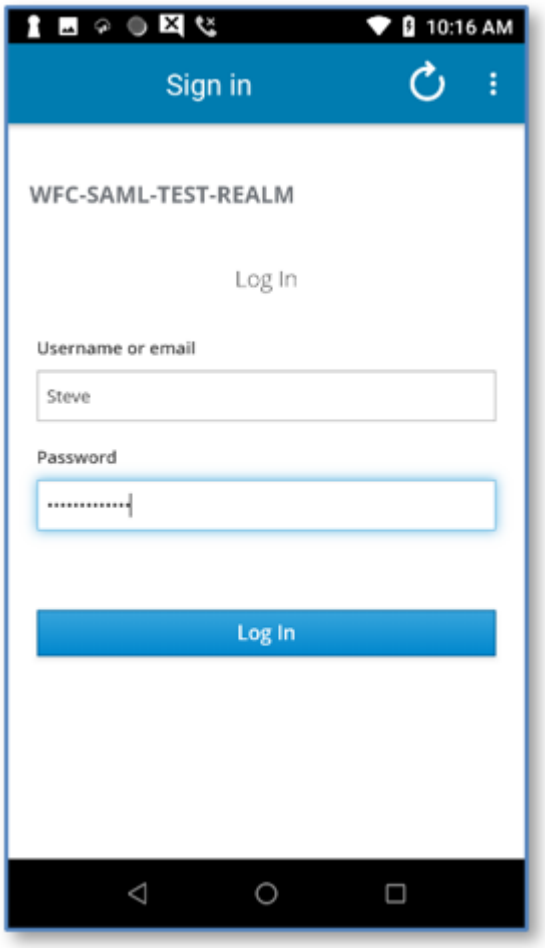
For the Customer ID, use the Tenant ID assigned by the Zebra Administrator in the Profile Manager.

The Server URL is the URL of the Profile Manager server configured to support OAuth.

Device Operation

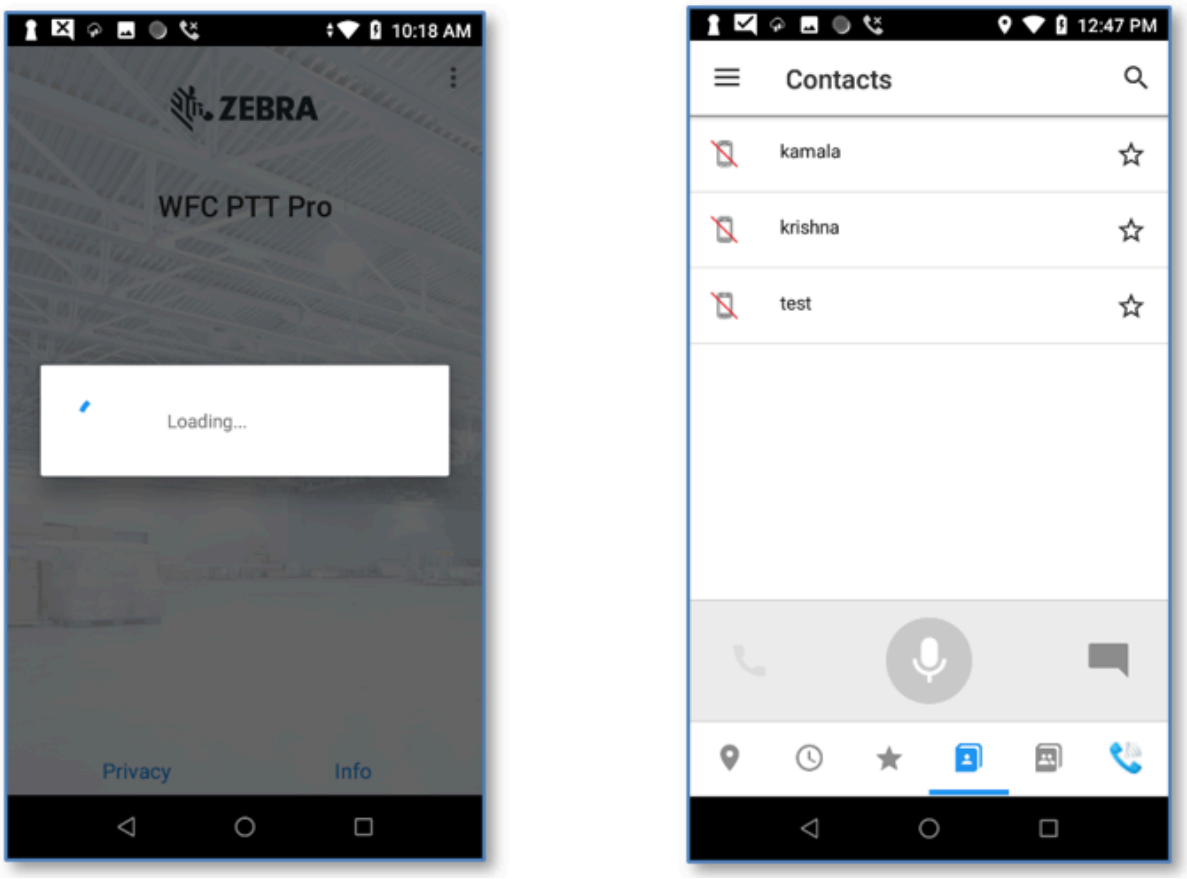
After you configure the servers and the mobile devices, launch the Profile Client to log in.

Figure 16 Profile Client Log In Screen



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



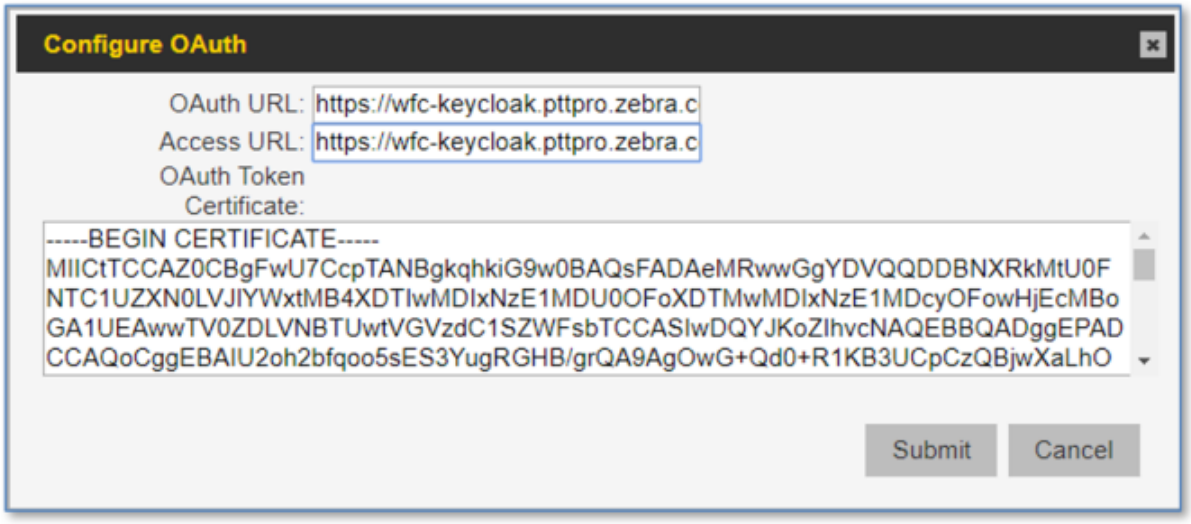
Your configuration is complete.

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.



Copy the certificate to the clipboard.

The certificate still looks right.

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

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.

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.