Profile Manager

Workforce Connect

ZEBRA

Customer Administrator Guide

MN-003433-14EN Rev A

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.

Contents

About This Guide

This guide provides information about using the Workforce Connect Profile Manager.

NOTE: Screens and windows pictured in this guide are samples and can differ from actual screens.

Chapter Descriptions

Topics covered in this guide are as follows:

- Getting Started provides an introduction and description of graphical conventions used in this document.
- System Management provides information on the management of users, devices, and roles.
- Identity Provider (IDP) Import Management provides information on the bulk import of users, devices and extensions.
- Client Device Setup Using Telephony Manager and Profile Manager provides information on client device setup for sites using advanced features.
- Telephony Management provides information on importing extensions.
- Profile Manager Licenses provides information on the device licenses for your enterprise.
- Intents and Actions provides information on how to install and configure the WFC Profile Client.
- Bulk Import Device Users provides information on how to import users into Profile Manager and PTT Pro.
- Multiple Role Values from Attributes provides information on how to read an AD attribute with multiple roles and proliferate it to the UI of the mobile device.
- Role Level Selection provides information about assigning a collection of roles under a role level name.

Notational Conventions

The following conventions are used in this document:

- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.

NOTE: The text here indicates information that is supplemental for the user to know and that is not required to complete a task.

IMPORTANT: The text here indicates information that is important for the user to know.

CAUTION: If the precaution is not heeded, the user could receive a minor or moderate injury.

WARNING: If danger is not avoided, the user CAN be seriously injured or killed.

DANGER: If danger is not avoided, the user WILL be seriously injured or killed.

Service Information

If you have a problem with your equipment, contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number

Zebra responds to calls by email, telephone, or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Revision History

Change	Date	Description
MN-003433-01 Rev A	06/2019	Initial Release
MN-003433-01 Rev B	12/2019	Updates for RRR delivery.
MN-003433-02 Rev A	04/2020	Updates for RRR delivery for WFC Profile Manager Version 4.0.
MN-003433-03 Rev A	08/2020	Updates for RRR delivery for WFC Profile Manager Version 4.2.
MN-003433-04 EN Rev A	04/2021	Updates for custom delivery.
MN-003433-05EN Rev A	07/2021	Added Add, Find, Substitute, and Replace functions and whitelist attributes.
MN-003433-06EN Rev A	12/2021	Added the Update Tenant Configuration.
MN-003433-07EN Rev A	03/2022	Added Client Authentication for THD.
MN-003433-08EN Rev A	06/2022	Import Job History status details provided.
MN-003433-09EN Rev A	10/2022	Added Transfer Role and Import Job run.
MN-003433-10EN Rev A	12/2022	Added Device role and device user naming convention.
MN-003433-11EN Rev A	03/2023	Added Device Cleanup Threshold and Landing Application.
MN-003433-12EN Rev A	07/2023	Added Role Display Preference, Role Selection Quantity, updated Edit Job, and View Import Job History.
MN-003433-13EN Rev A	10/2023	Updated Add to AllDynamicGroup parameter in Update Tenant Configuration.
MN-003433-14EN Rev A	01/2024	Added the ZEMS Tenant Configuration parameters and User Import.

Getting Started

This chapter includes the following topics:

Introduction to Workforce Connect Profile Manager

The Workforce Connect Profile Manager (WFC Profile Manager) provides a user interface (dashboard) for administrators or technical representatives to manage an organization’s use of mobile devices. The target audience for this guide is Zebra administrators and customer administrators who configure and control the operation of mobile device deployment.

The portal includes role-based access to the following functions:

- Authentication of portal user accounts
- Creation and management of
  - Portal users
  - Device users
  - Applications
- Importing
  - Devices users
  - Extensions
- Presence service management

- Monitoring of user and device activity
  - Real time usage
  - Historical data
- Report generation

Interconnection Details

The WFC Profile Manager has direct and indirect connections and relationships to many devices, including but not limited to the following:

- WFC Voice Client
- PTT Pro Client
- PTT Pro Management Portal
- WFC Profile Client
- Active Directory Server

Logging In to Profile Manager Portal

Administrator must have an account in the **Profile Manager** portal.

1. Navigate to the **Profile Manager** portal.
2. Enter the **User ID**, **Password**, and **Customer ID**.

Figure 1 Profile Manager Portal Login Dialog Box

3. Click **Log in**.

   If incorrect credentials are entered, the **Login** dialog box displays an error message.

   If correct credentials are entered, the main screen of the **Profile Manager Portal** appears.

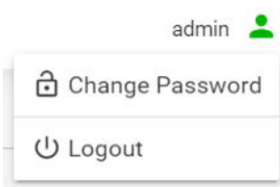
NOTE: Other system events, including but not limited to server re-installation, server upgrade, server restart, or clearing of cache on browser might require you to re-enter the Customer ID as a first-time user on your next login to the Profile Manager Portal.

Logging Out of Profile Manager Portal

To log out of the Profile Manager Portal, do the following:

1. Navigate to the **Profile Manager Portal** screen that has the following icon in the top right corner.

2. Click the icon and select **Logout** in the drop-down list.



Resetting Your Administrator Password

There are two ways to reset your administrator password.

- Resetting Your Administrator Password Before Logging In
- Resetting Your Administrator Password After Logging In

Resetting Your Administrator Password Before Logging In

To reset your password from the login dialog box, do the following:

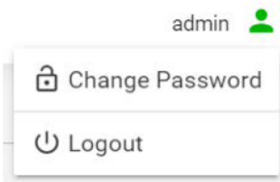
1. In the login dialog box, click the link for **Forgot password**?
2. In the **Reset Password** dialog box, enter your email address and Customer ID.
3. Select **Reset**.
4. Follow the instructions in your email to reset your password.

Resetting Your Administrator Password After Logging In

To reset your password after successfully logging in to the Profile Manager Portal, do the following:

1. Navigate to a **Profile Manager Portal** screen that has the following icon in the top right corner.

2. Click the icon and select **Change Password** in the drop-down list.



3. Complete the fields in the **Reset Password** dialog box and click **Save**.

NOTE: The Zebra Administrator may create two administration accounts. One account is for the customer administrator. The second account is used by the Active Directory Connector, which is specified during the deployment. Do not change the password used by the Active Directory Connector without consulting the Zebra Administrator, otherwise, the connector is not able to communicate with the Profile Manager.

Main Screen in Profile Manager

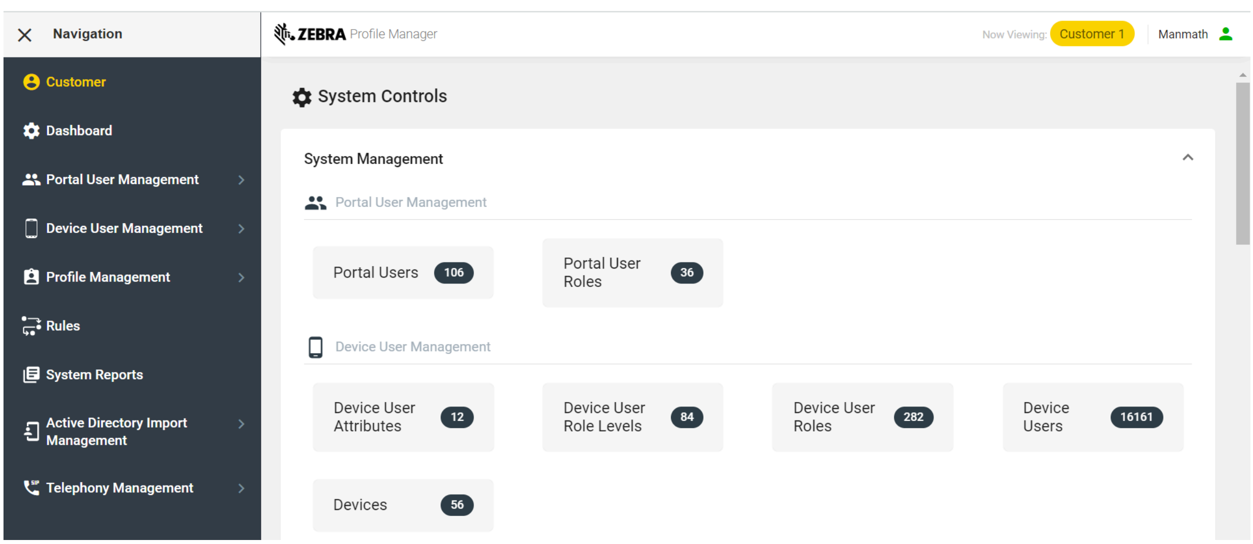
After you log in to the Profile Manager Portal, the System Controls panel (dashboard) appears.

System Controls Panel

The left panel of the **System Controls** (Dashboard) panel is the **Navigation** panel. The **Navigation** panel contains shortcut links to the functions in the right panel.

In the **System Controls** (Dashboard) panel, the links in the left panel take you to the same categories as the Profile Manager administration screens listed on the left panel. Or you can click the quick link buttons in the right panel to access the administration screens. For more information, see Dashboard Quick Link Buttons.

Figure 2 System Controls Panel (Dashboard)



Your access to functions and actions in the dashboard is controlled by the permissions in your assigned role(s) for any Profile Manager portal functions, such as the following:

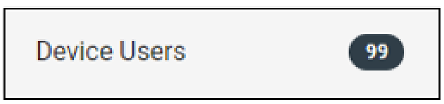
- System Management
    - Portal User Management
    - Device User Management
    - Profile Management
    - Rules
    - System Reports
- Active Directory Import Management
- Telephony Management
- Licenses.

Navigating the Profile Manager Portal Dashboard

This chapter describes the features linked to each icons and provides the details of those icons.

Dashboard Quick Link Buttons

Each Quick Link button displays the function name and number of items defined for that function. Click a Quick Link button to manage that function.



Return to the Dashboard

- Click the Zebra logo or **Dashboard** to return to the **Dashboard** from any Profile Manager screen.

Required Information

An asterisk (*) appears for required information.

Icons

Icons represent actions, shortcut links, or descriptions. Click an icon to perform the action or navigate to the link. Hover on the icon for a description of the action, shortcut link, or parameter. Shortcut links are on the side Navigation bar or top bar of every page.

Permission Category		Description
	Action	View or edit
	Action	• Delete • Delete/De-enroll the device

Permission Category		Description
	Action	Refresh
	Action	Reset password
	Action	Mask
	Action	Unmask
	Action	Expand side navigation
	Action	Expand drop-down
	Action	Collapse drop-down
	Action	Display history
	Action	Run
	Action	Search
	Action	Search
	Shortcut	Opens dashboard
	Shortcut	Opens Device User Management
	Shortcut	Opens Rules
	Shortcut	Opens Reports
	Shortcut	Opens Telephony Manager
ZEBRA	Shortcut	Dashboard

Slider Switches

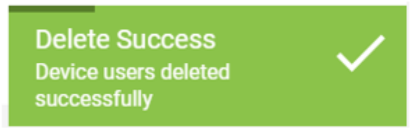
Click slider switches to enable and disable features.

Setting	State
	Disabled
	Enabled

Success and Error Messages

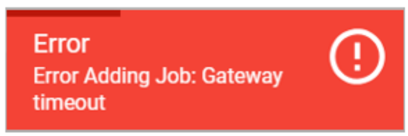
When an action such as **Create**, **Edit**, or **Delete** is successful, a message similar to the following appears.

Figure 3 Action Message-Success



When an action such as **Create**, **Edit**, or **Delete** is unsuccessful, a message similar to the following appears.

Figure 4 Action Message-Error



Search and Filter Functionality

All items inside each function are searchable.

- There are search options in many screens throughout the portal.
- Some screens also have drop-down filters.
- Wild card characters limit the search results. For example, use an asterisk to enter part of a search term.

Figure 5 Portal User Search Field and Drop-Down Filter

System Management

This chapter describes how to use Profile Manager to control and manage the system.

- Tenant Configuration
- Portal User Role Management
- Portal User Management
- Device User Attribute Management
- Device User Role Management
- Device User Management
- Device Management
- Profile Definition Management
- Profile Configurations Management
- Rule Management
- System Report Management

Tenant Configuration

This section describes how to:

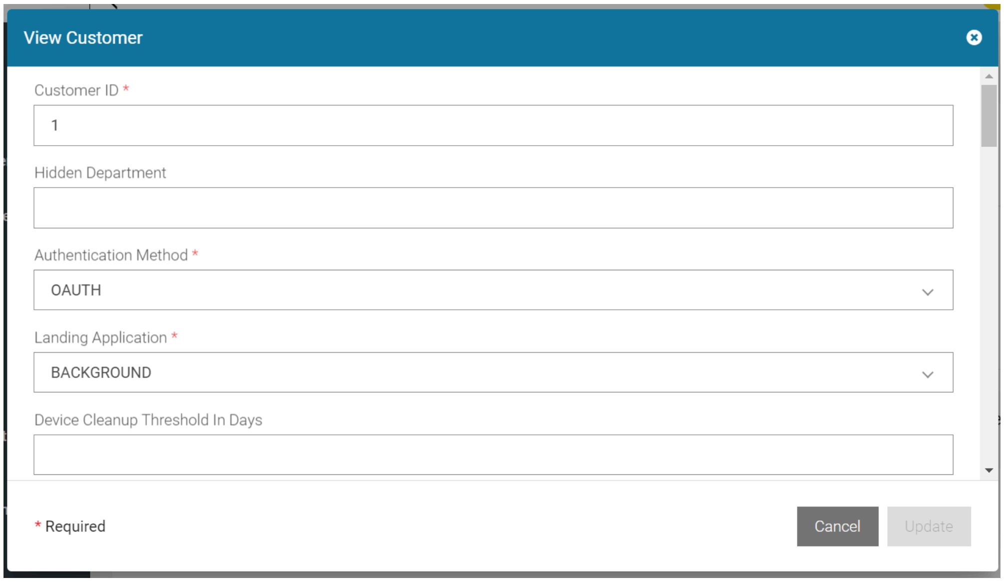
- View Tenant configuration
- Update Tenant configuration

View Tenant Configuration

You must have privileges to view tenant configuration.

From the dashboard, click **Customer** icon.

The **View Customer** screen appears.



Update Tenant Configuration

You must have privileges to update tenant configuration.

1. From the dashboard, click **Customer** icon.

   The **Update Tenant Configuration** screen appears.

2. Edit the fields.
3. Click **Update**.

   Figure 6 Edit Customer Screen

Use the following table to set up the Tenant Configuration:

Parameter	**Description**
Customer ID	Customer Identifier. View only field.

Parameter	Description
Hidden Department	Name of the hidden department configured in the extension manager. This field is used to reserve the extension for the user.
Authentication Method	Authentication method. Possible values include: OAUTH, IMPRIVATA, LAUNCHER
Landing Application	This feature enables the customer to choose which application to display in the foreground after the role is selected in the Profile Client. Possible values: • BACKGROUND: This feature enables the customer to choose which application to display in the foreground after the role is selected in the Profile Client. • VOICE: If the roles selected have both PTT PRO and VOICE profiles, then the VOICE application displays in the foreground after the role selection. If there is only a PTT PRO profile, then the PTT PRO application appears in the foreground. • PTT PRO: If the selected roles have both PTT PRO and VOICE profiles, then the PTT PRO application displays in the foreground after the role selection. If there is only a VOICE profile, then the VOICE application appears in the foreground. • PROFILE CLIENT: Profile Client displays in the foreground. • Default Value: BACKGROUND
Device Cleanup Threshold in Days	All the devices in this tenant which are not logged in to the PFM system for this cleanup and threshold days are deleted from PFM, PTT PRO, and obsoleted from Extension Manager and PVM systems. If the Extension Manager and the PVM device are obsoleted instead of forced delete. This is important when we cannot get the permanent device identifier for the devices. For example, in Third-Party Android devices or in the future version of Android OS, the device ID is changed after the factory reset. If this field is not configured, then device cleanup for this tenant is not performed. Possible values: 2 to 365 days If there are no third-party devices, we recommend not configuring this parameter.
OAUTH Details	
Host Url	URL to the OAuth server.
Authentication Path	URI endpoint for the OAuth server.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Token Path</td><td>Token path to the OAuth server.</td></tr>
<tr><td>Client ID</td><td>Customer-generated Client ID (comes from the Customer's OAuth server).</td></tr>
<tr><td>Client Secret Key</td><td>Client secret key. It is an optional field for some of the OAUTH configurations.</td></tr>
<tr><td>Token Username</td><td>The user field within the token is used to identify the individual user.

NOTE: OAUTH details fields are applicable for all authentication methods.</td></tr>
<tr><td>Client Authentication</td><td>Possible values:
• Send client credentials in the body.
• Send as Basic Auth header.

NOTE:
For the existing tenants, if this field is not configured, then the client credentials are sent in both header and body.

All existing tenants are not able to modify any tenant configurations and save them unless they select one of the values in client authentication. And after selecting the value, the default value changes, and the client configurations are only sent either in the header or body.</td></tr>
<tr><td>Active Directory Details</td><td>Active Directory ObjectClass value is used to identify the type of object during user roles import. Default value: group</td></tr>
<tr><td>Group Class</td><td>Active Directory ObjectClass value is used to identify the type of object during user roles import. Default value: group</td></tr>
<tr><td>User Class</td><td>Active Directory ObjectClass value is used to identify the type of object during user import. Default value: person.</td></tr>
<tr><td>AD Whitelist</td><td>List of AD attribute names. Changes to these attributes are ignored during the user import.</td></tr>
<tr><td>Limits</td><td></td></tr>
<tr><td>Return to Foreground Interval (earlier it is called Interval)</td><td>Sets the interval, in minutes, to bring the profile client to the foreground if the client is already logged in and waiting for the user input to select a site or a role. This is required when the user has not completed his login and returned to some other application Default value: 0 (disabled)</td></tr>
<tr><td>No of attempts to return to foreground</td><td>Sets the number of attempts to return to the foreground. Possible values: 0 to 100. Default Value: 0 (disabled).</td></tr>
</table>

Parameter	Description
Return to Login Interval	Sets the interval, in minutes, to show the Click **Login** button to remind the user to log in and select a role. Default value: 0 (disabled)
Max Report Records	A maximum number of records can be downloaded from System Reports.
Pttpro Settings	
Default Callee group	The default group name is used to make a call when the PTT key is pressed. **NOTE:** This does not work when a voice command is enabled.
AllStoreGroup Name	Configures Default dynamic group name where all the users are added. For example, all. store Default value: Empty (User is not added to any group). **NOTE:** The group name should be added as a role in the system.
Add to AllDynamicGroup	Configures how users are added to the dynamic group. When true, the user is added to all of the dynamic groups/roles. • is added to the currently selected dynamic group with receiveCall and originateCall as true and talker override as false. The user can initiate or listen to group calls. During logout, the group membership is set with receiveCall, originateCall, and talker override as false. • is added to the non-selected dynamic group to which the user is assigned with the receiveCall=false, originateCall =true, and talker override=false. The user can initiate a group call but is not able to listen to the group calls. During logout or switching roles, the group membership is set with receiveCall, originateCall, and talker override as false. When false (default), the user is added to the currently selected dynamic group with receiveCall, originateCall, and talker override based on the group user template selected for the user during import. If no template is selected, the STANDARD template is used. During logout or switching roles, the group membership is set with receiveCall, originateCall, and talker override as false. **NOTE:** • During the logout, the users are not removed from the group, so the login time is reduced as less number of API requests are triggered to PTT Pro server during login. • When Profile Manager is deployed with the ZEMS server, if there is a broadcast message to a group

Parameter	Description
	when the user is logged out, those messages are visible when the user logs in again. It happens because the Profile Manager does not remove the user from the group during logout and the ZEMS server does not keep track of receiveCall group membership settings while sending the message.
Site Selection	Configures whether the user has the capability to change the site dynamically during the profile client login. When true, the device user is presented with a Site Selection page. When false (default), the user has no capability to change the site dynamically. **NOTE:** List of sites is taken from the PTT Pro Side configuration (ESN).
Role Settings	Displays the preference in the **Profile Client Role Selection** page.
Transfer Role Settings	
Transfer Role	Enable/Disable Default Value: Disable If it is disabled, Transfer Role settings during Role configuration are ignored at the time of device login.
Transfer Role Count Down in Seconds	Countdown Timer in seconds Possible values: 5 to 300 Default value: 15 Notification is displayed on both devices until this countdown timer elapses. It is considered a force transfer if the countdown timer elapses without the user replying to the message.
Role Display Preference	Displays the preference in the **Profile Client Role Selection** Page. Possible Values: • Roles and Description – Displays both the Role and the Description. • Roles Only– Displays role name only. • Description Only – Displays description only. • Default Value: Displays roles and descriptions. If this field is not configured, the role and the description are displayed on the **Role Selection** Page during the device login.
Role Selection Quantity	The number of roles allowed for the selection in the Profile Client Role Selection page. Possible Values: 1 to 4

Parameter	Description
	Default Value: 4 If this field is not configured, a maximum of 4 roles are allowed in the **Role Selection** Page during device login.
Flat File Variance	
Threshold in %	This is the file variance threshold allowed in percentage. Variance is checked for a higher or lower boundary. Import job execution fails if the number of records in the user import flat file is beyond the allowed variance, After comparing with the previous successful run. This is to prevent any incomplete user import flat file from being used during import, which would result in deleting the records which are not present in the flat file. If this field is not configured, then there is no validation during the user import. Possible Values: 1 to 100
Notification Email	One or more email addresses are separated by commas. If the job execution fails, the mail is sent to these emails **NOTE:** If the same email id is configured in the job scheduler, email notifications for failure, or both, the user receives multiple emails if the job fails.
Zebra Enterprise Messaging Server (ZEMS)	
ZEMS Url	ZEMS Server URL. Requires if the ZEMS Manager association is required during user import.
ZEMS API Key	ZEMS Server API Key Requires if the ZEMS Manager association is required during user import.
License	
Utilization Threshold In %	Device License Utilization Threshold in Percentage. Sends the email to the configured emails if the defned threshold value exceeds. Possible values: 1 to 100 Default Value: Empty **NOTE:** NOTE: Threshold check is done based on the cron job setting (scheduler.notification.cron) specified

Parameter	Description
	in the deployment configuration. This should be set to once in a day
Utilization Notification Email	List of email addresses separated by comma (,) or can be a group email ID. Must be a valid email address. Default Value: Empty Email body contains tenant name and license utilization details.

Portal User Role Management

This section describes how to:

- View user roles
- Create user roles
- Update user role permissions
- Delete user roles.

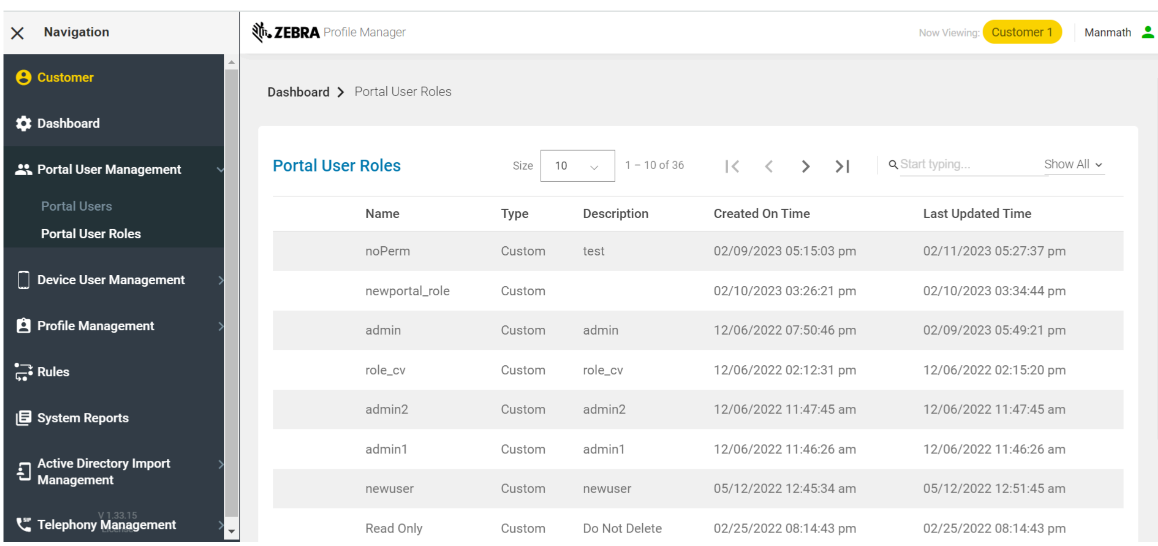
View Portal User Roles

Your privileges must permit you to view portal user roles.

- From the dashboard,expand the **Portal User Management** , click **Portal User Roles**.

  The **Portal User Roles** screen appears.

Figure 7 Portal User Roles Screen



Create Portal User Roles

Your privileges must permit you to create portal user roles.

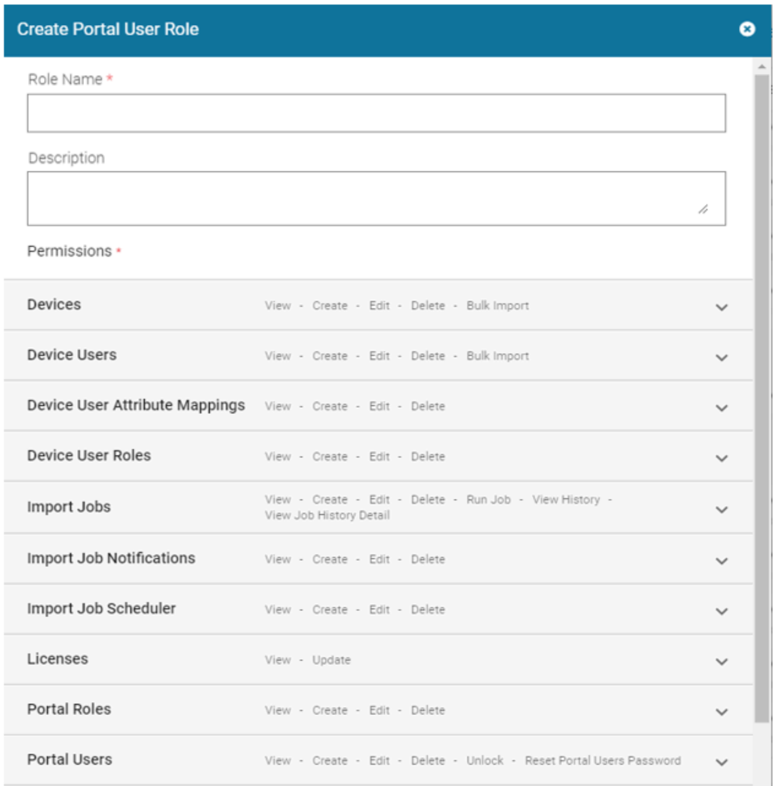
1. From the dashboard, click **Portal User Roles**.

   The **Portal User Roles** screen appears.

2. Click **Create Portal User Role**.

   The **Create Portal User Role** dialog box appears.

   Figure 8 Create Portal User Role Dialog Box



3. Enter the **Role Name** and **Description**.

4. Click on each drop-down and click the slider switches to enable or disable permissions for each category.

5. After setting the permissions, click **Create**.

   The **Create Portal User Role** dialog box closes and the role can now be assigned to portal users.

Edit Portal User Roles

Your privileges must permit you to edit portal user roles.

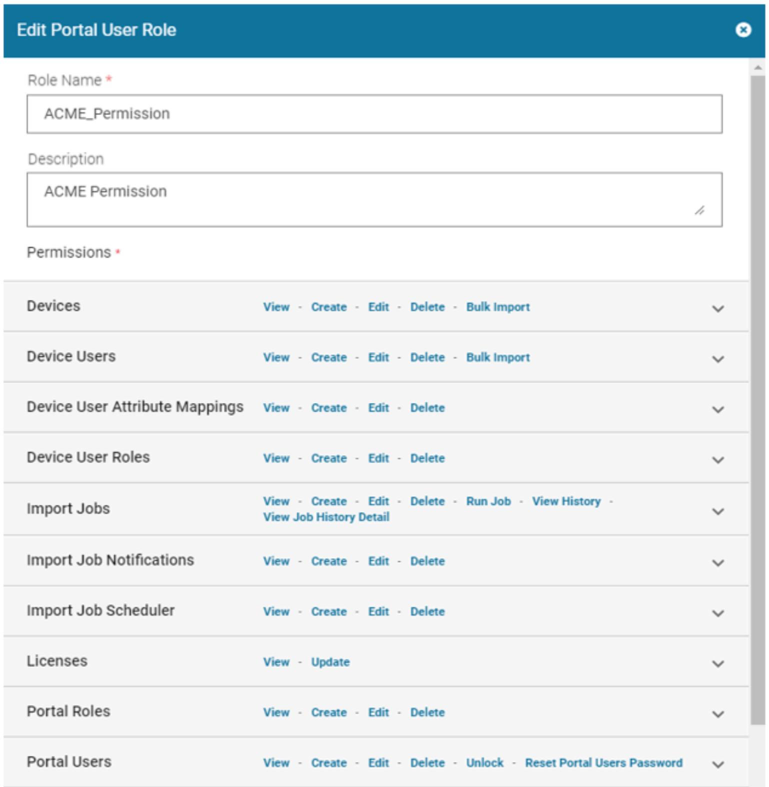
1. From the dashboard, click **Portal User Roles**.

   The **Portal User Roles** screen appears.

2. Click for the role you wish to edit.

   The **Edit Portal User Role** dialog box appears, with granted permissions displayed in bold blue text.

   Figure 9 Edit Portal User Role Dialog Box



3. Update the permission fields as in Create Portal User Roles .
4. Click **Update**.

   The **Edit Portal User Role** dialog box closes and the new settings applies to anyone who is assigned the updated portal user role.

Delete Portal User Roles

Your privileges must permit you to delete portal user roles.

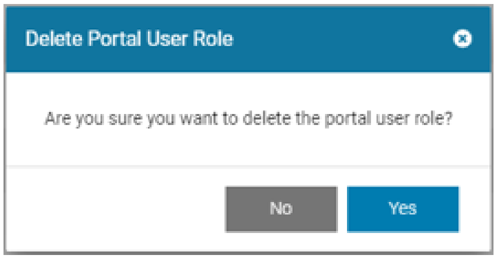
1. From the dashboard, click **Portal User Roles**.

   The **Portal User Roles** screen appears.

2. Click for the user role you wish to delete

   The **Delete Portal User Role** dialog box appears.

   Figure 10 Delete Portal User Role



3. Click **Yes** to delete.

Portal User Management

This section describes the following:

- Create Portal Users
- Edit Portal Users
- Delete Portal Users

Create Portal Users

- Your privileges must permit you to create portal users.
- The user roles must be created if you want to assign them while creating portal users.

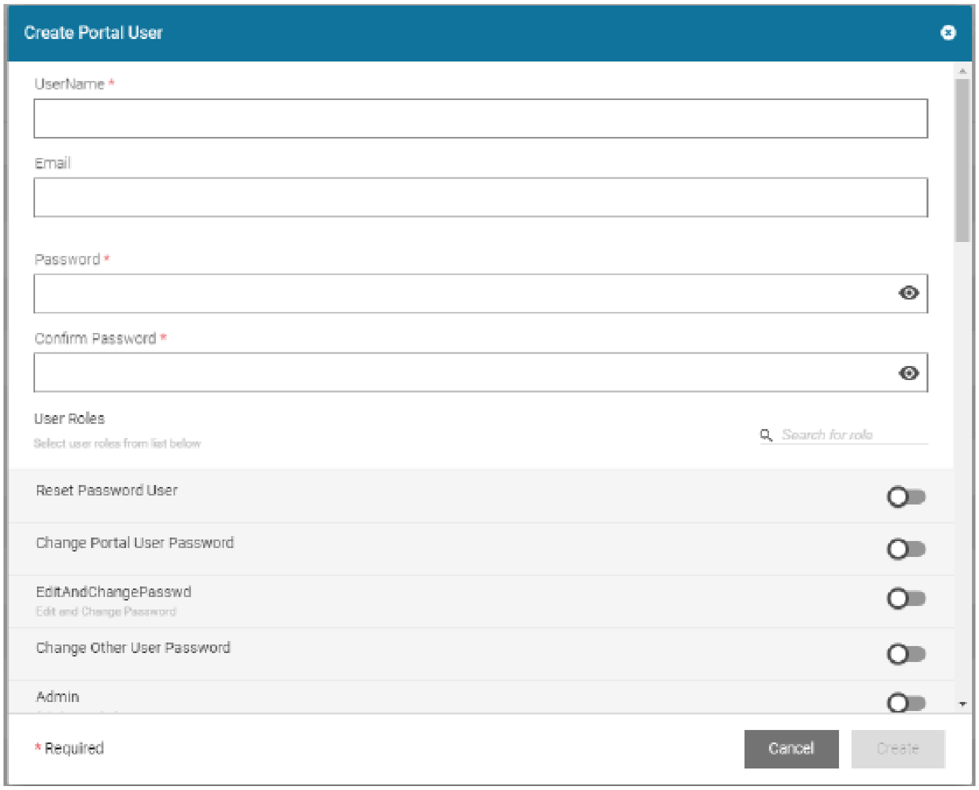
1. From the dashboard, click **Portal Users**.

   The **Portal Users** screen appears.

2. Click **Create Portal User**.

   The **Create Portal User** dialog box appears.

Figure 11 Create Portal User Dialog Box



3. Complete the fields in the **Create Portal User** dialog box.
4. Click the slider switches to enable the applicable user role(s).
5. Click **Create**.

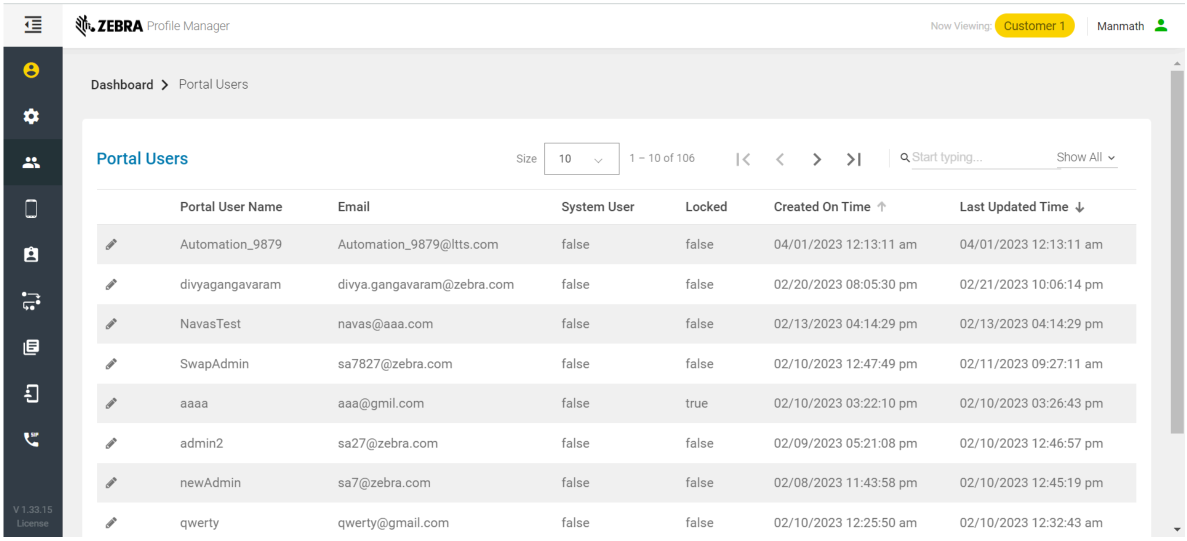
Edit Portal Users

Your privileges must permit you to edit portal users.

1. From the dashboard, click **Portal Users**.

   The **Portal Users** screen appears.

   Figure 12 Portal Users Screen



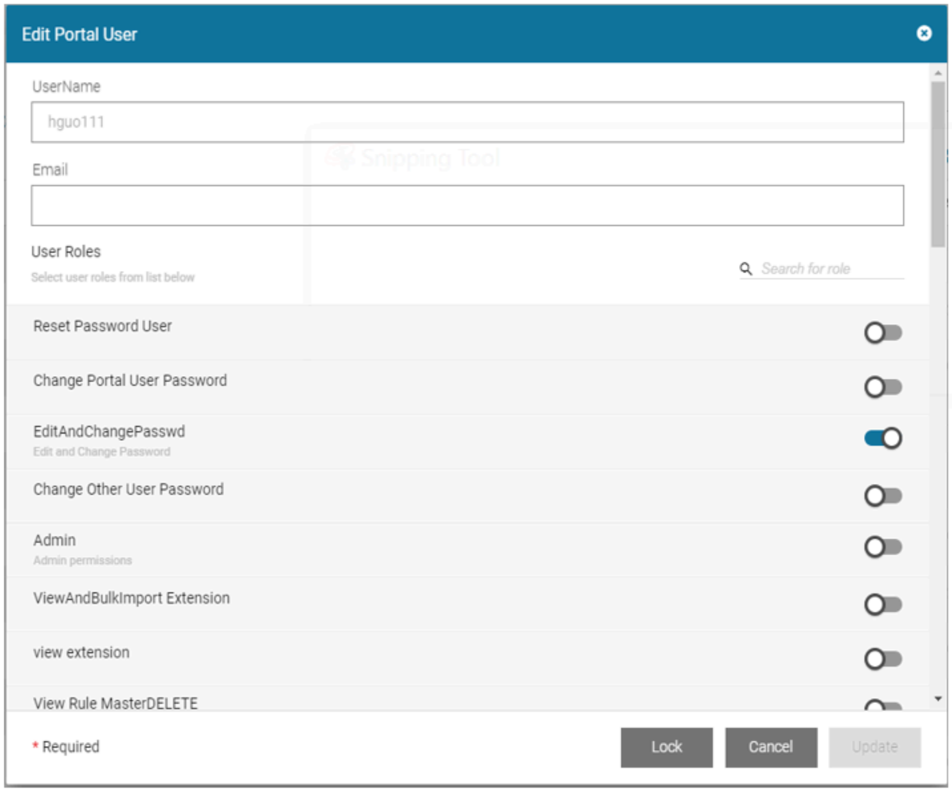
NOTE: If your role allows you to reset the passwords of Profile Manager portal users, you can use the Portal Users screen to do this. To reset the password of another Profile Manager Portal User, do the following at the Portal Users Screen.

2. Click **Reset** icon for the portal user whose password you want to reset.
3. Choose the type of reset: Manual or email. Complete the other fields in the dialog box.
4. Click **Reset** to close the **Reset Password** dialog box.

5. Click for the portal user, you wish to edit.

   The **Edit Portal User** dialog box appears.

   Figure 13 Edit Portal User Dialog Box



6. Update entries in the fields in the **Create Portal User** dialog box.
7. Click the slider switches to enable/disable the **user role(s)**.
8. Click **Update**.

   The **Edit Portal User** dialog box closes, and the portal user is updated with the user role(s).

Delete Portal Users

Your privileges must permit you to delete portal users.

1. From the dashboard, click **Portal Users**.

   The **Portal Users** screen appears.

2. Click for the portal user, you wish to delete.

   The **Delete Portal User** dialog box appears.

3. Click **Yes** to delete.

NOTE:

If there is a PTT Pro Group defined for the role, deleting a role also deletes the corresponding PTT Pro Group asynchronously. This may take some time to reflect in the PTT Pro portal.

Device User Attribute Management

This section describes the following:

- Create Device User Attributes
- Edit Device User Attributes

Create Device User Attributes

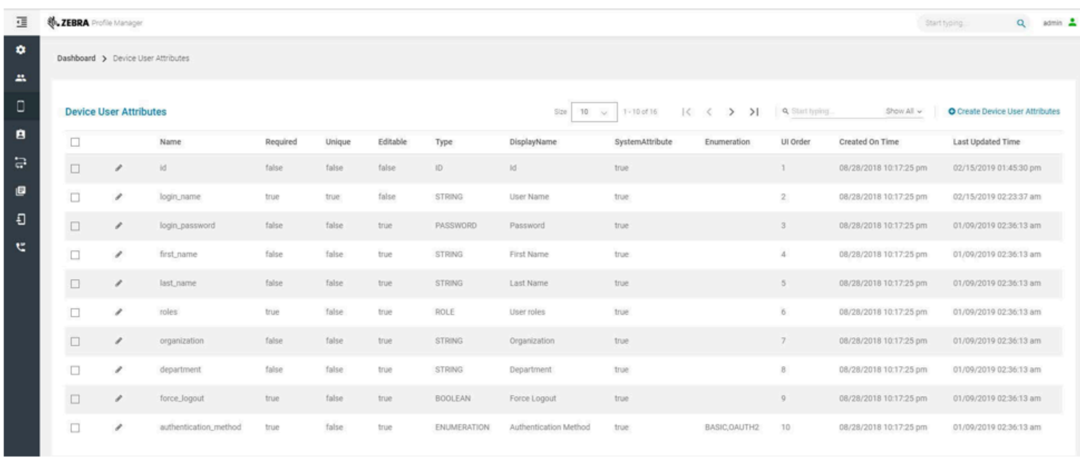
Use this procedure to create device user attributes.

Your privileges must permit you to create device user attributes.

1. From the dashboard, click **Device User Attributes**.

   The **Device User Attributes** screen appears.

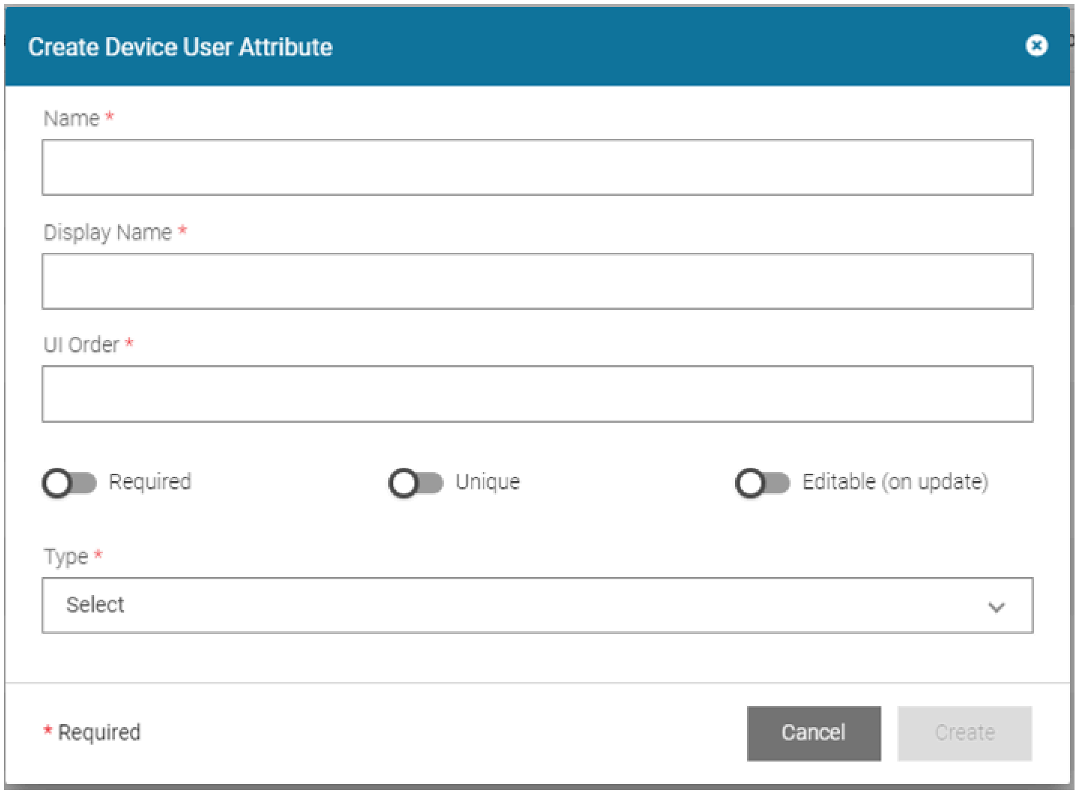
Figure 14 Device User Attributes Screen



2. Click **Create User Attribute**.

   The **Create Device User Attribute** dialog box appears.

   Figure 15 Create Device User Attribute Dialog Box



3. Use the following table to set up the device user attribute.

Parameter	Description
Name	The internal name of the attribute.
Display Name	The name displayed in the **Create Device User** dialog box.
UI Order	Sequence of where the attribute appears in the **Create Device User** dialog box.
Required	Enable to make the attribute a required field in the **Create Device User** dialog box.
Unique	Enable to make the attribute unique for each user.
Editable (on update)	Enable to allow edits for the device user attribute.
Type	Data type, for example: string, string array, password, boolean, or enumeration.

4. Click **Create**.

   The **Create Device User Attribute** dialog box closes and the new attribute appears on the **Device User Attributes** screen.

Edit Device User Attributes

Your own role must allow editing device user attributes.

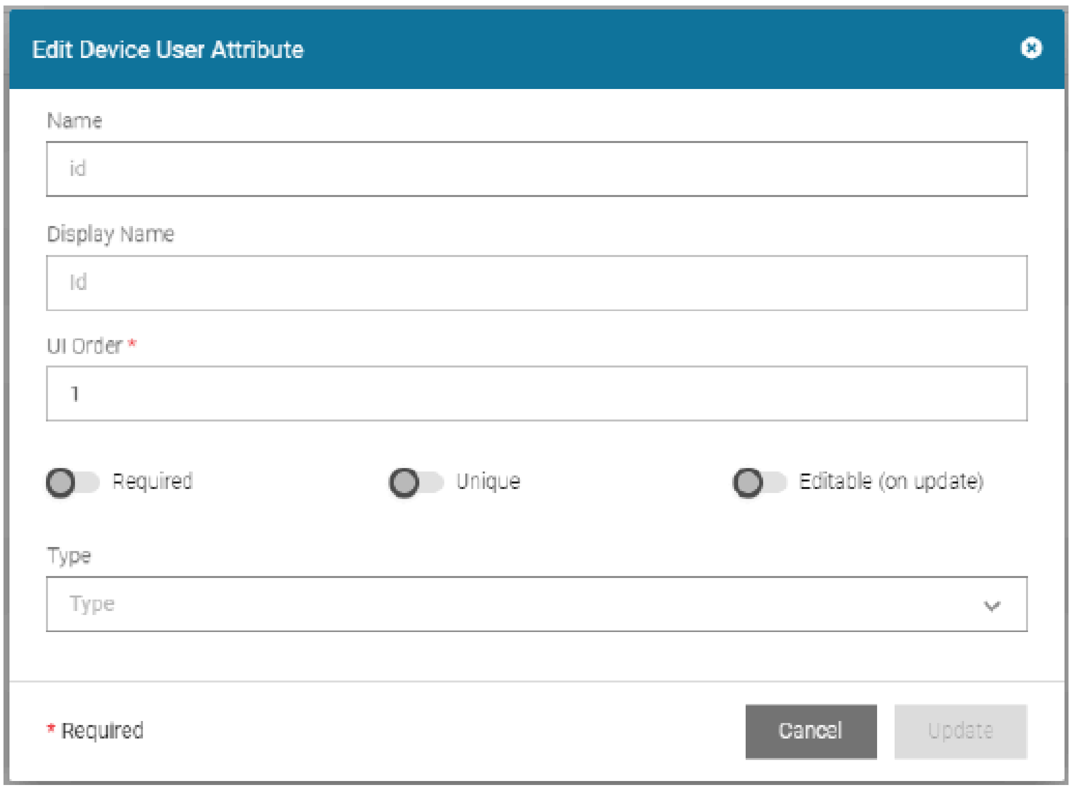
1. From the dashboard, click **Device User Attributes**.

   The **Device User Attributes** screen appears.

2. Click for the device user attribute you wish to edit.

   The **Edit Device User Attribute** dialog box appears.

   Figure 16 Edit Device User Attribute Dialog Box



3. Update the fields as in Create Device User Attributes.
4. Click **Update**.

Device User Role Management

This section describes how to:

- Create a device user role
- Edit Device User Roles
- Delete Device User Roles

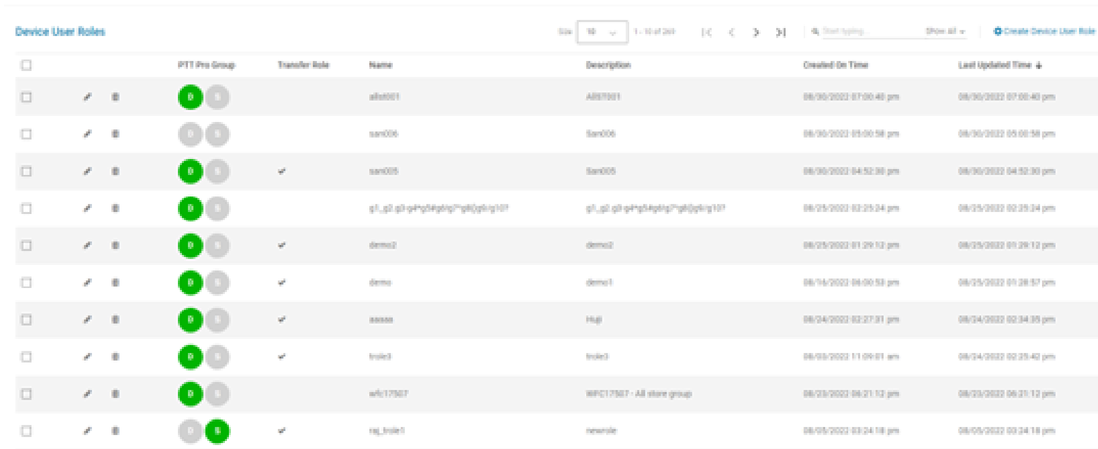
Create Device User Role

Your privileges must permit you to create device user roles.

1. From the dashboard, click **Device User Roles**.

   The **Device User Roles** screen appears.

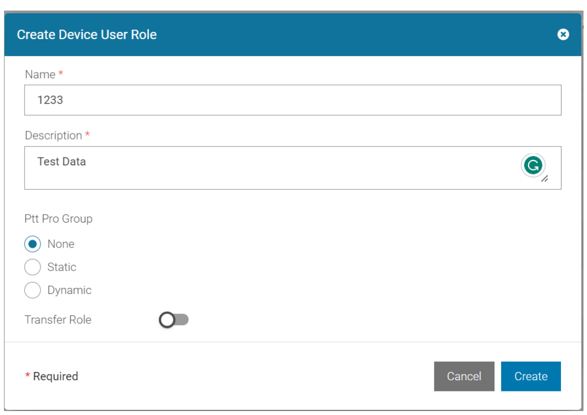
   Figure 17 Device User Roles Screen



2. Click **Create Device User Role**.

   The **Create Device User Roles** dialog box appears.

   Figure 18 Create Device User Role Dialog Box



3. Enter the role name in **Name**. Only alphanumeric and _.*#!/?$ characters are allowed. Roles are mapped to the PTT Pro group name. The maximum length allowed for the PTT Pro group is 33 characters. Generally, the group name is prefixed with the site name. Hence, one must limit the role name's length to 33 characters to accommodate the site name.
4. Enter a description of the role in **Description** box.
5. Make a selection in **PTT Pro Group**.

Setting	Definition
None	No Device User Role (a.k.a. group) is created in PTT Pro.

Setting	Definition
Static	The Device User Role is created as a Static group in PTT Pro when users are imported from Active Directory (AD) to PTT Pro. The Static group in PTT Pro contains all imported users, and the static group does not allow users to be added or removed when the Device User changes/switches their Device User Role in the WFC Profile Client application.
Dynamic	The Device User Role is created as a Dynamic group in PTT Pro when users are imported from Active Directory (AD) to PTT Pro. The Dynamic group is created empty, without any users inside of it. When a Device User changes/switches their Device User Role in the WFC Profile Client application, the group settings are updated appropriately in PTT Pro based on the "Add to AllDynamicGroup" tenant configuration.

6. Enable **Transfer Role**, if the Voice Role is transferable between 2 users. It enables the user to take ownership of the Role/Extension from another user who is currently owning the Role/Extension but may not be actively using it. If the **Transfer Role** configuration is turned off at the Tenant configuration level, and then nobody can change this configuration. This configuration is applicable only to the Voice Profile. The PTT Pro group must not be assigned to this role.
7. Click **Create**.

   The **Create Device User Roles** dialog box closes, and the new role appears on the **Device User Roles** screen.

Edit Device User Roles

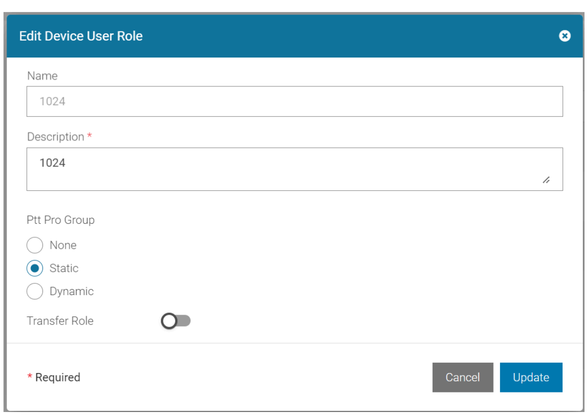
Your privileges must permit you to edit device user roles.

1. From the dashboard, click **Device User Roles**.

   The **Device User Roles** screen appears.
2. Click  for the device user role you wish to edit.

   The **Edit Device User Role** dialog box appears.

   Figure 19 Edit Device User Role Dialog Box



3. Transfer Role is disabled if the **Transfer Role Configuration** is turned off at the Tenant configuration level.
4. Update the fields.

5. Click **Update**.

Delete Device User Roles

Your privileges must permit you to delete device user roles.

NOTE: No Device User may be assigned to the role you wish to delete.

- To cancel, click **No**. To continue, click **Yes**.

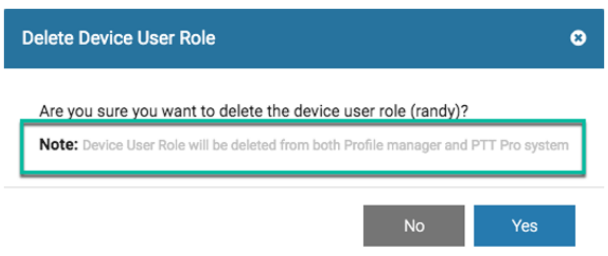
1. From the dashboard, click **Device User Roles**.

   The **Device User Roles** screen appears.

2. Click for the device user role you wish to delete.

   The **Delete Device User Role** dialog appears.

   Figure 20 Delete Device User Role Dialog Box



Device User Management

This section describes the following:

- View Device Users
- Add and Update Device Users
- Delete a Device User
- Refresh a Device User's Status

View Device Users

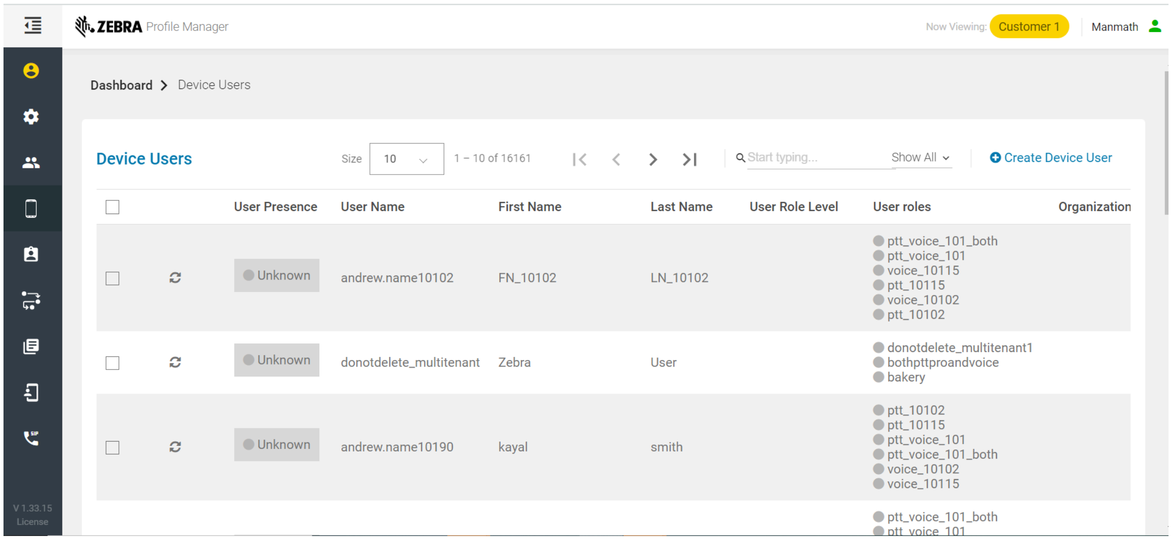
The **Device Users** screen displays the current information for all device users, such as login status and logged-in users.

Your privileges must permit you to view device users.

From the dashboard, click **Device Users**.

The **Device Users** screen appears.

Figure 21 Device Users Screen



Add and Update Device Users

For device users to connect to the Profile Manager network, they must be added in the Profile Manager application.

There are two ways to add device users.

- add/update multiple device users (bulk import device users).
- add a device user.
- through the AD Connector Service.
- through the Flat File Import.

The Profile Manager Provisioning Guide describes how to import users through bulk import, the AD Connector, or a flat file using Google Cloud Platform and Secure FTP. The Profile Manager Provisioning Guide provides detailed information regarding the architecture of the various methods of importing multiple users into the Profile Manager and PTT Pro, where applicable. In addition, the guide describes the process for each import method, the associated Attribute Transformations, and the information required from the customer to enable each method.

Add or Update Multiple Device Users

The support of Bulk Import Device Users (Bulk Import Device Users) is detailed in the Bulk Import Device Users.

Add a Device User

Use this procedure to create device users.

- Your privileges must permit you to create device users.
- User role(s) to assign must already have been created, as in Create Device User Roles.

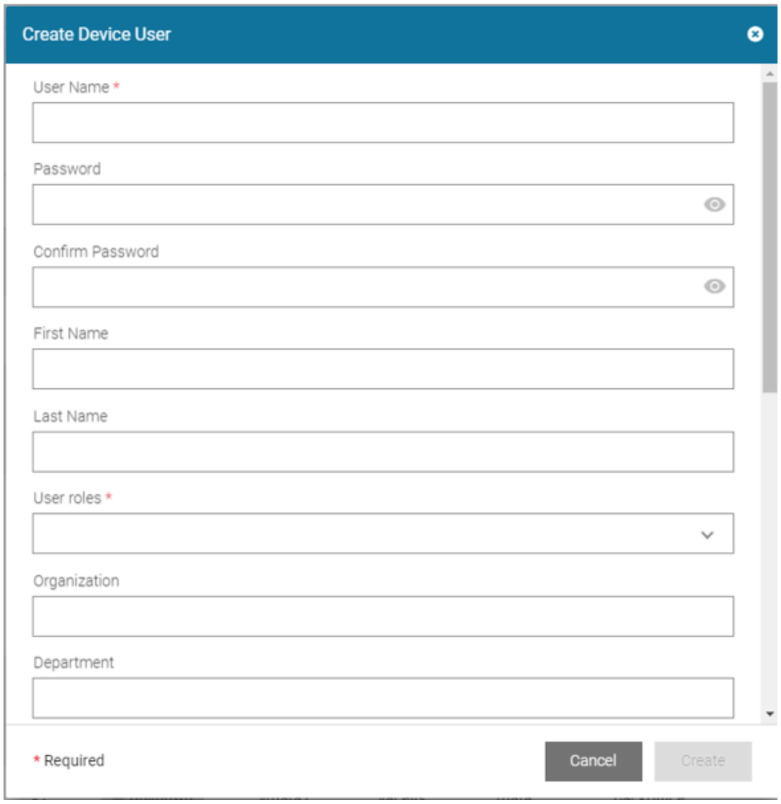
1. From the dashboard, click **Device Users**.

   The **Device Users** screen appears.

2. Click **Create Device User**.

   The **Create Device User** dialog box appears.

   Figure 22 Create Device User Dialog Box



3. Complete the fields in the **Create Device User** dialog box.

4. Select either **Role Level** or **Roles** for the user. If the **Role Level** is selected, the associated roles to the **Role Level** are assigned to the user. If both **Roles** and **Role Level** are provided, **Role Level** takes precedence over the **Roles**

5. If the **Authentication Type** in the Tenant Configuration is LAUNCHER or IMPRIVATA, the **Force Logout** box is hidden. The values set earlier for this box are ignored during the device's login.

6. Click **Create**.

Edit a Device User

Your privileges must permit you to edit device users.

1. From the dashboard, click **Device Users**.

   The **Device Users** screen appears.

2. Click  for the device user you wish to edit.

   The **Edit Device** User dialog box appears.

3. Update the fields as in Add a Device User.
4. Select either **Role Level** or **Roles** for the user. If the **Role Level** is selected, the associated roles to the **Role Level** are assigned to the user. If both **Roles** and **Role Level** are provided, the **Role Level** takes precedence over the**Roles**. If the user enables **Save Role Selection** during the device Login, any changes to the associated user roles clear the **Save Role Selection** flag so that the user is presented with a **Role Selection** screen when the user logs in next time.

NOTE: If your role allows you to reset the passwords of device users, you can use the Edit Device User dialog to do this. To reset the password of the device user, add a temporary password to the Password and Confirm Password fields. Provide the device user with a temporary password. Then the device user can log into the system and change their temporary password to a different password.

5. Click **Update**.

Delete a Device User

Use this procedure to delete a device user.

Your privileges must permit you to delete device users.

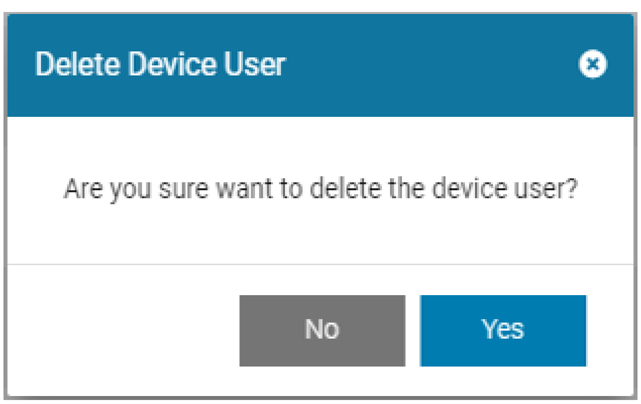
NOTE: To bulk delete more than one device user, see the procedure for Add/Update Multiple Devices/Enroll Multiple Devices (Bulk Import Devices).

1. From the dashboard, click **Device Users**.

   The **Device Users** screen appears.
2. Click for the device user you wish to delete.

   The **Delete Device User** dialog box appears.

   Figure 23 Delete Device User



3. Click **Yes** to delete.

Refresh a Device User Status

1. From the dashboard, click **Device Users**.

   The **Device Users** screen appears.

2. Click ![refresh icon] for the device user whose presence you wish to refresh.

   The **User Presence Indicator** displays the latest information.

Device Management

This section describes the following:

- License management Using Device Management
- View devices
- Add/Enroll and Update Devices
- Delete/De-Enroll a Device
- Refresh devices

License Management Through Device Licenses

Device Licenses allow users to access the system, devices can be added/enrolled, updated and deleted/de-enrolled to control device licenses. The procedures in this section describe device license management.

View Devices

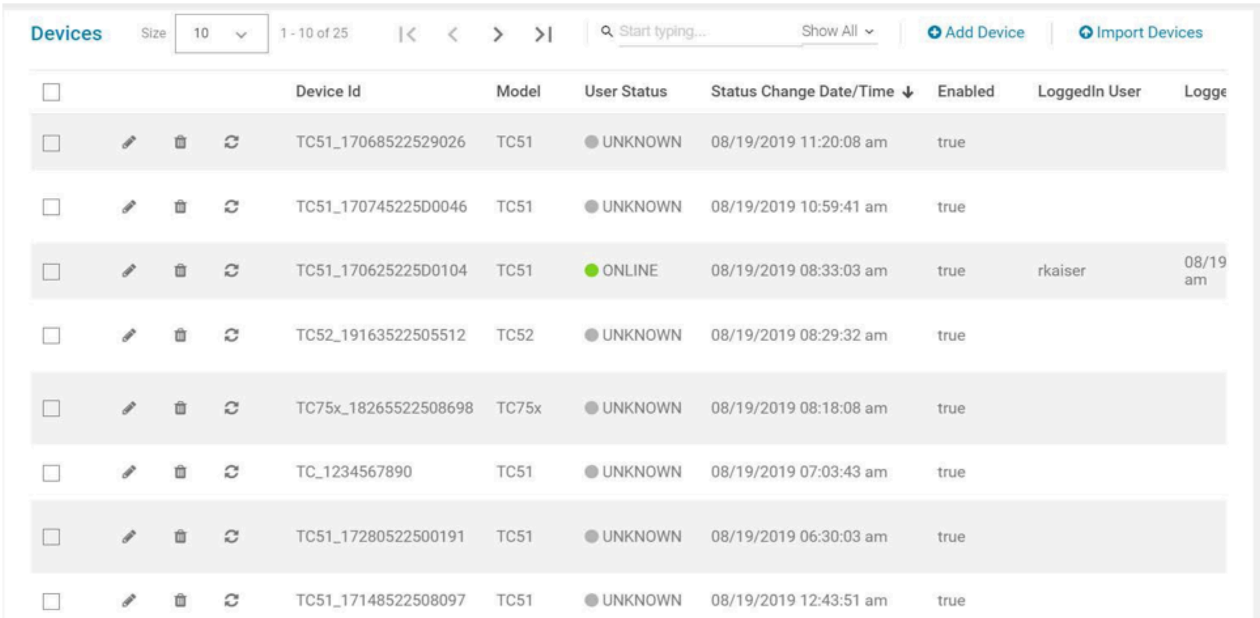
The Devices screen displays current information for all devices, such as login status and logged in users.

Your privileges must permit you to view devices.

From the dashboard, click **Devices**.

The **Devices** screen appears.

Figure 24 View Devices Screen



Add/Enroll and Update Devices

For devices to connect to the Profile Manager network, they must be added/enrolled in the Profile Manager application.

There are two ways to add/enroll devices.

- add/update multiple devices (bulk import devices)
- add a device.

Add/Update Multiple Devices/Enroll Multiple Devices (Bulk Import Devices)

Use this procedure to upload a file from another system to replace an entire database or to synchronize changes.

- Your privileges must permit you to bulk import devices.
- The import file must be CSV format.
- The devices to be synchronized must already exist in the database.
- The Profile Manager database is case sensitive. Review the CSV file before upload.

NOTE: You can delete devices in a bulk using this procedure, by bulk importing an updated devices list that does not contain the devices that you like to delete, and using the **Replace entire database** option during the bulk import.

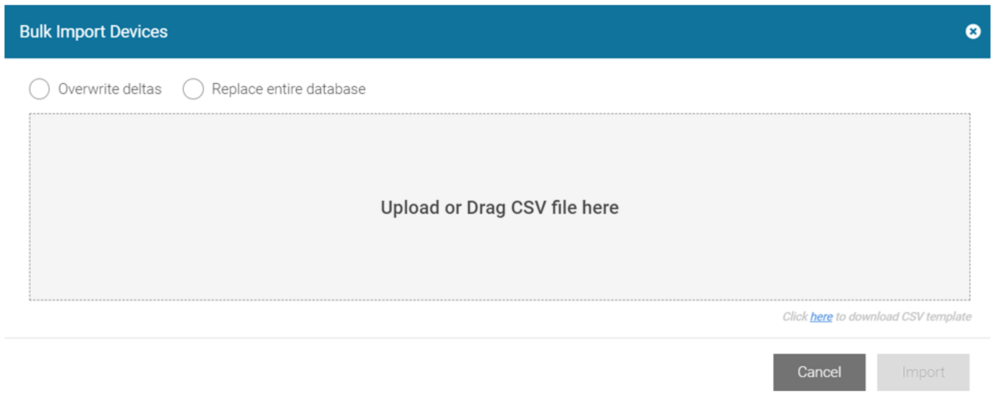
1. From the dashboard, click **Device**.

   The **Devices** screen appears.

2. Click **Import Devices**.

   The **Bulk Import Devices** dialog box appears.

   Figure 25 Bulk Import Devices Dialog Box



3. Select an option.
   - To synchronize the database updates from the import file, select **Overwrite deltas**.
   - To overwrite the existing database, select **Replace entire database**.
4. To upload a file, click **Upload** or Drag csv file here and browse to select the CSV file.

NOTE: To download a CSV template file to use to create the file to upload, click the link at bottom right of the dialog box, prepare the CSV file, and then return to this procedure.

5. Follow the screen prompts to complete the bulk import.

Add a Device

Your privileges must permit you to add devices.

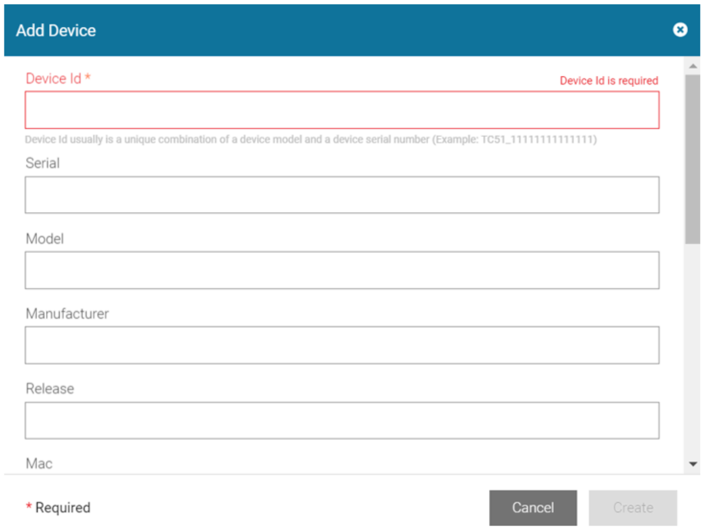
1. From the dashboard, click **Device**.

   The **Devices** screen appears.

2. Click **+Add Device**.

   The **Add Device** screen appears.

   Figure 26 Add Device Screen



3. In the **Device Id** field, enter the device ID.

NOTE: Device Id usually is a unique combination of a device model and a device serial number (Example: TC51_11111111111111) The device ID must be from 10 to 64 alphanumeric characters in length. The allowed special characters are underscore (_) hyphen (-) and period (.).

   The other fields may be completed now or later.

4. Click **Create**.

   If you entered invalid information, the system displays an error message.

   The device created is listed in the **Devices** screen.

Edit a Device

Your privileges must permit you to edit devices.

1. From the dashboard, click **Devices**.

   The **Devices** screen appears.

2. Click for the device you wish to edit.

   The **Edit Device** dialog box appears.

3. Update the changes and click **Update**.

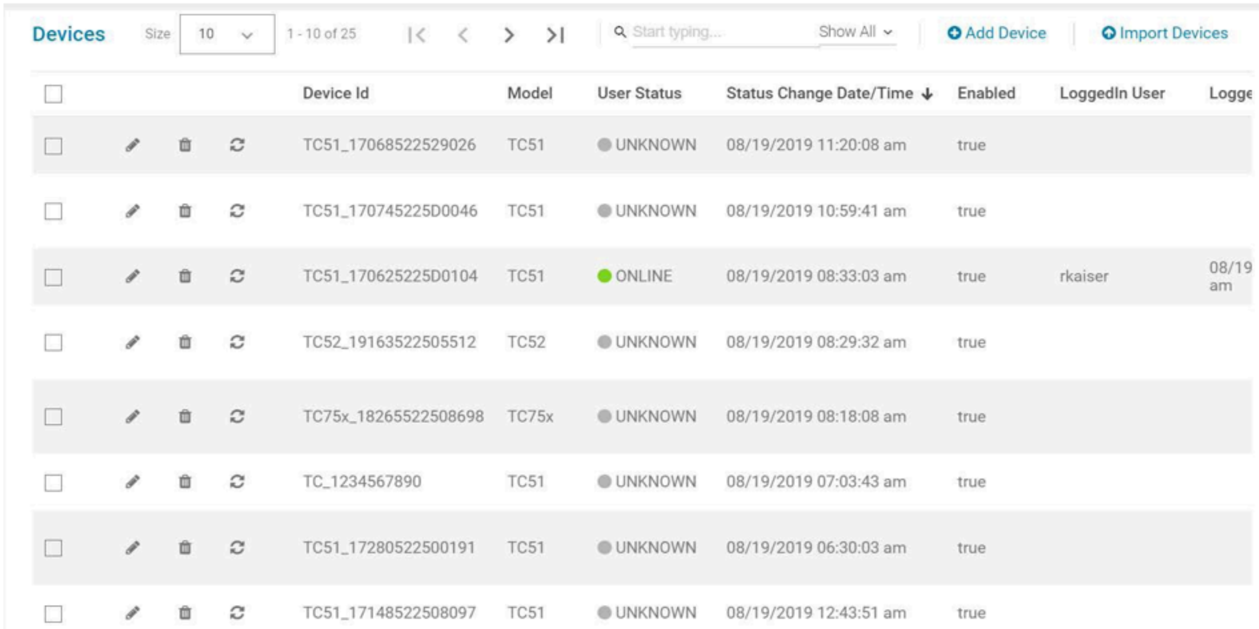
Delete/De-Enroll a Device

Use this procedure to delete/de-enroll a device.

Your role privileges must permit you to delete/de-enroll devices.

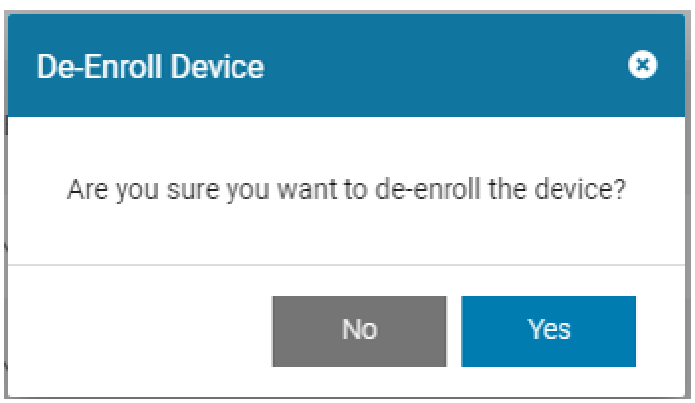
1. Click 🗑 for the device(s) to delete/de-enroll.

Figure 27 Devices Screen



The **De-Enroll Device** dialog box appears.

Figure 28 De-Enroll Device Dialog Box



2. Click **Yes** to delete/de-enroll.

The device is deleted/de-enrolled, and the device is removed from the device list.

The device is deleted from the WFC PTT Pro system, obsoleted from Extension Manager/Provisioning Manager, and deleted from the Profile Manager system. If the device is not found in WFC PTT Pro and

Extension Manager, it proceeds further to delete the device from the Profile Manager system. Displays either the consolidated message with the deletion status of each system or the system error message.

If a device is deleted/de-enrolled while a user is logged into the device, the user's session of the WFC Profile Client is ended automatically, and the user is automatically logged out of the device.

If login is attempted on a deleted/de-enrolled device, the login is denied and the device displays a message that the device is not activated.

NOTE:

Device Id usually is a unique combination of a device model and a device serial number (Example: TC51_11111111111111). The device ID in the WFC PTT Pro system is expected to be just the serial number part of it. After the last underscore, the system strips the characters and treats that as the serial number. If there is no underscore, then it deletes the complete device ID specified in the WFC PTT Pro system.

If multiple devices are selected for deletion, then there is a consolidation message about whether the devices are deleted successfully or failed. If any device is failed to delete, a failure message is displayed.

In case of Extension Manager, there should be at least one super administrator-defined for this tenant in the Extension Manager to delete/obsolete the device. Otherwise, the delete activity fails. If the device is present in a different tenant than the one which we are trying to delete, then the delete activity continues deleting from other systems with an appropriate status message.

Refresh a Device Status

1. From the dashboard, click **Device**.

   The **Devices** screen appears.

2. Click for the device whose presence you wish to refresh.

   The status indicator displays the latest information.

Profile Definition Management

This section describes how to:

- Create profile definitions
- Edit profile definitions
- Delete profile definitions.

Create Profile Definitions

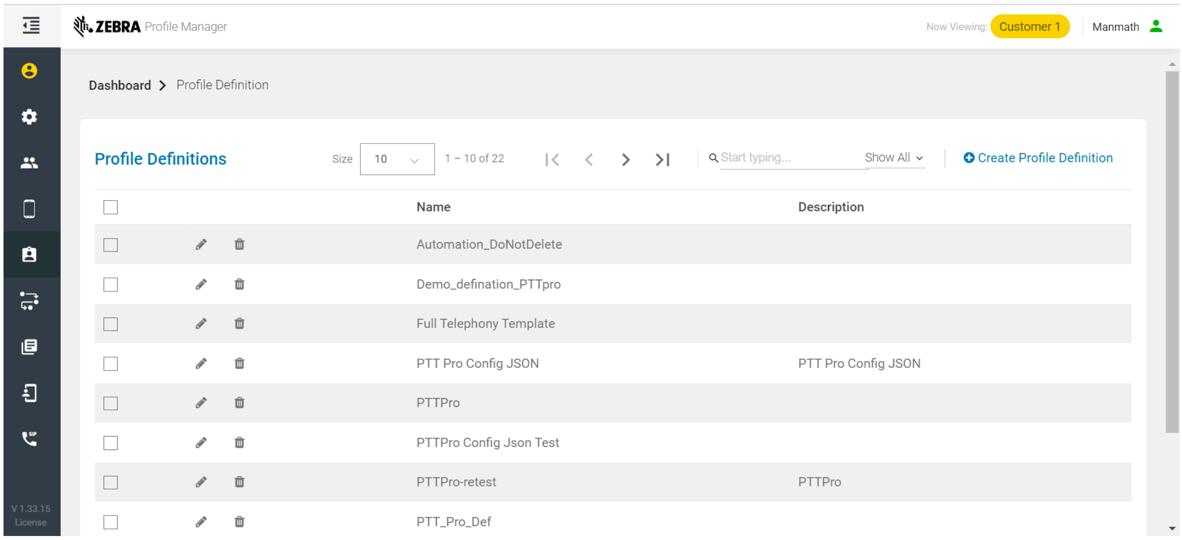
Use this procedure to add profile definitions.

Your privileges must permit you to create profile definitions.

1. From the dashboard, click **Profile Definitions**.

   The **Profile Definition** screen appears.

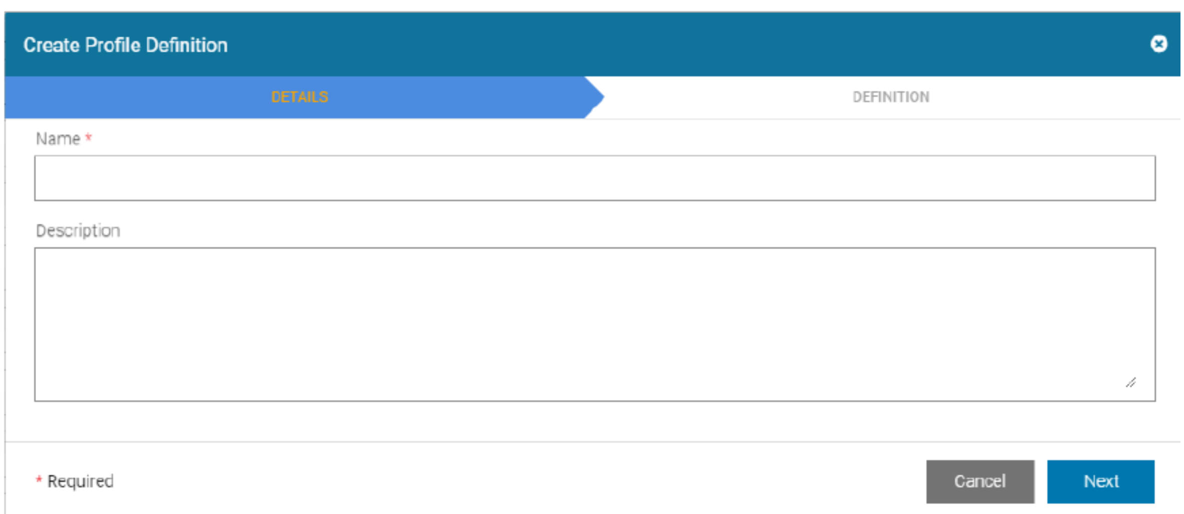
   Figure 29 Profile Definitions Screen



2. Click **Create Profile Definition**.

   The **Create Profile Definition** dialog box appears.

   Figure 30 Create Profile Definition Dialog Box



3. In the **Name** field, enter a name for the profile definition.
4. In the **Description** field, enter a description for the profile definition.
5. Click **Next**.
6. Click  to enter the profile definition in JSON format, include **app_info** and **app_setting** definitions.

7. Click LAYOUT to verify the JSON.
8. Click **Create**.

Edit Profile Definitions

Your privileges must permit you to edit profile definitions.

1. From the dashboard, click **Profile Definitions**.

   The **Profile Definition** screen appears.
2. Click for the profile definition you wish to edit.

   The **Edit Profile Definition** dialog box appears.
3. Update the fields as in Create Profile Definitions.
4. Click **Update**.

Delete Profile Definitions

Your privileges must permit you to delete profile definitions.

1. From the dashboard, click **Profile Definitions**.

   The **Profile Definition** screen appears.
2. Click for the profile definition you wish to delete.

   The **Delete Application Definition** dialog box appears.
3. Click **Yes** to delete.

Profile Configuration Management

This section describes how to:

- Create profile configurations.
- Edit profile configurations.
- Delete profile configurations.

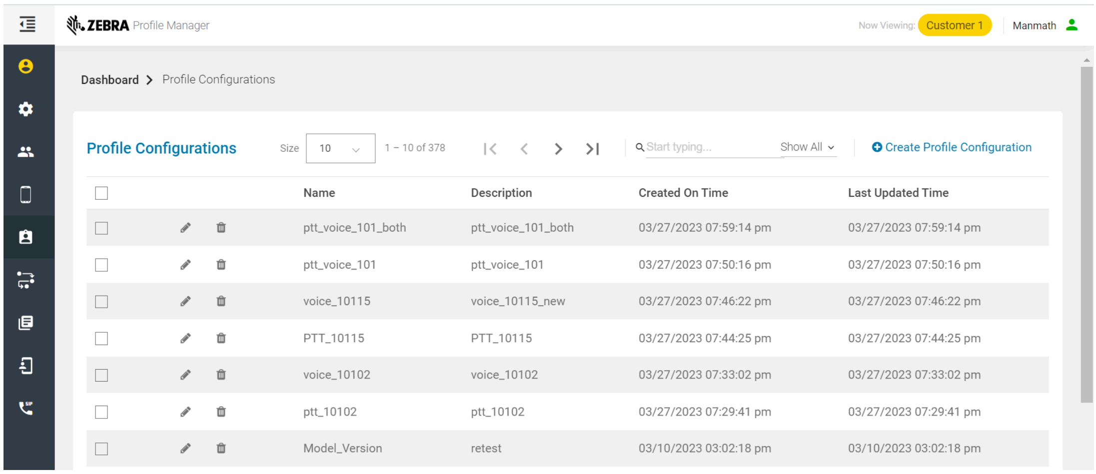
Create Profile Configurations

- Your privileges must permit you to create profile configurations.
- The necessary profile definitions must already be created if you want to assign them while creating profile configurations.

1. From the dashboard, click Profile **Configurations**.

   The **Profile Configurations** screen appears.

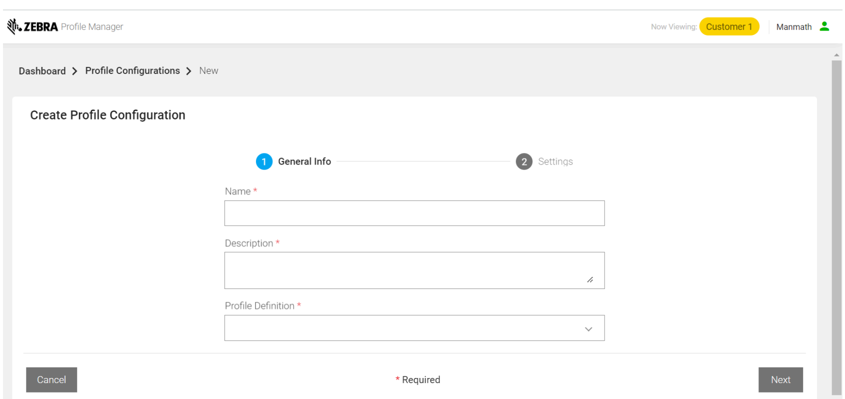
   Figure 31 Profile Configurations Screen



2. Click **Create Profile Configuration**.

   The **Create Profile Configuration** dialog box appears.

   Figure 32 Profile Configuration Dialog Box Screen



3. Use the following table to complete the **Create Profile Configuration** dialog box.

Parameter	Description
Name	Unique name for this configuration.
Description	Description of the profile configuration.
Profile Definition	Depending on the profile definition you choose, options appear in Settings.

4. Click **Next**.

   A list of options associated with the profile definition, if any, appears.

5. Click **Create**.

Edit Profile Configurations

Your privileges must permit you to edit profile configurations.

1. From the dashboard, click **Profile Configurations**.

   The **Profile Configurations** screen appears.

2. Click for the profile configuration you wish to edit.

   The **Update Profile Configuration** screen appears.

3. Make desired changes on the **General Info** tab.
4. Click **Next.**
5. Make desired changes on the **Settings** tab.
6. Click **Update**.

Delete Profile Configurations

Your privileges must permit you to delete profile configurations.

1. From the dashboard, click **Profile Configurations**.

   The **Profile Configurations** screen appears.

2. Click for the profile configuration you wish to delete.

Rule Management

The **Rules** function provides rules that control actions in the Profile Manager portal.

This section describes how to:

- View list of rules
- Create rules
- Publish rules
- Delete rules

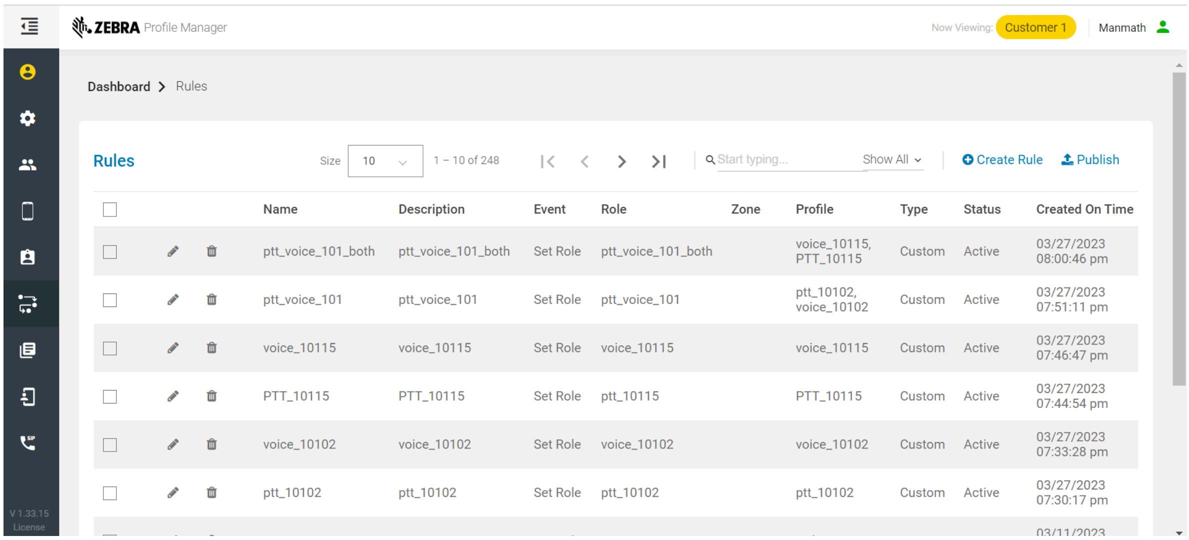
View Rules

The role you own must allow you to view the list of rules.

- From the dashboard, click **Rules**.

  The list of rules appears.

Figure 33 Rules Screen



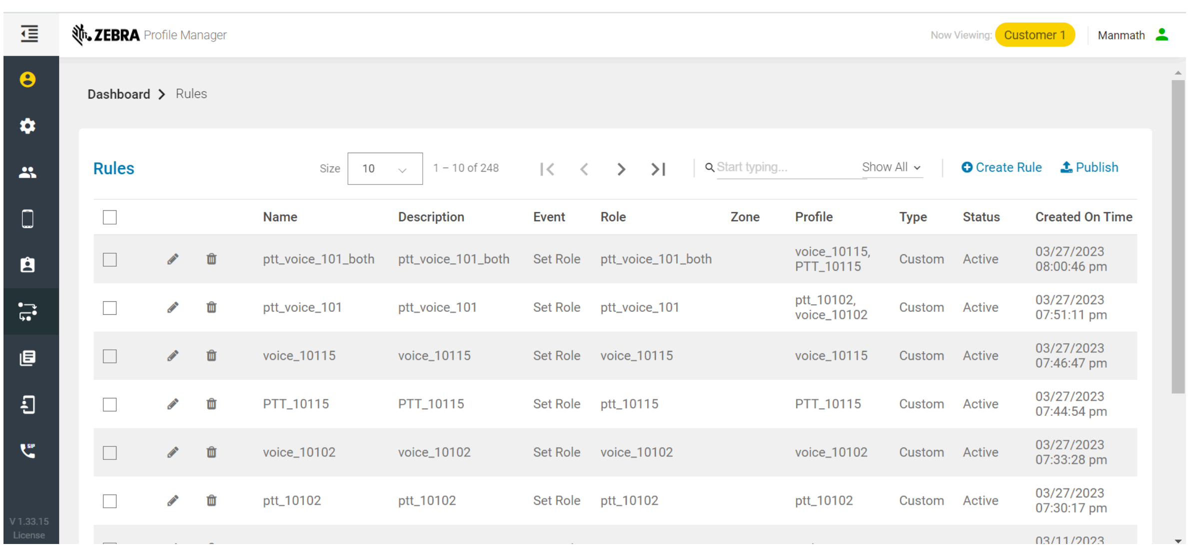
Create Rules

You own role must allow you to create rules.

1. From the dashboard, click **Rules**.

   The **Rules** screen appears.

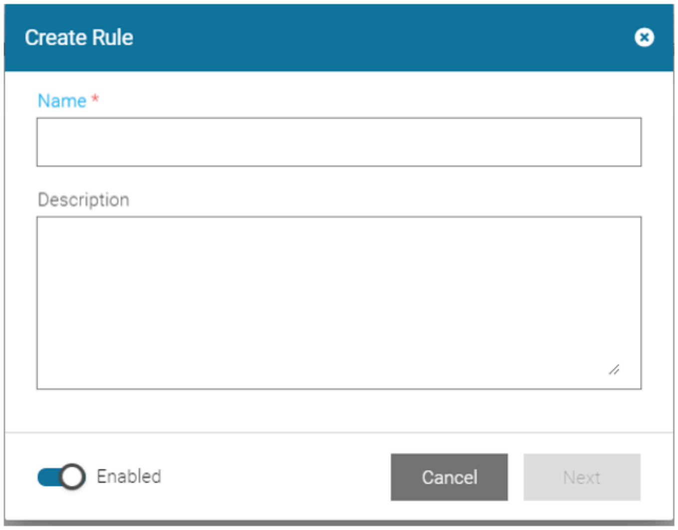
Figure 34 Rules Screen



2. Click **Create Rule**.

   The **Create Rule** dialog box appears.

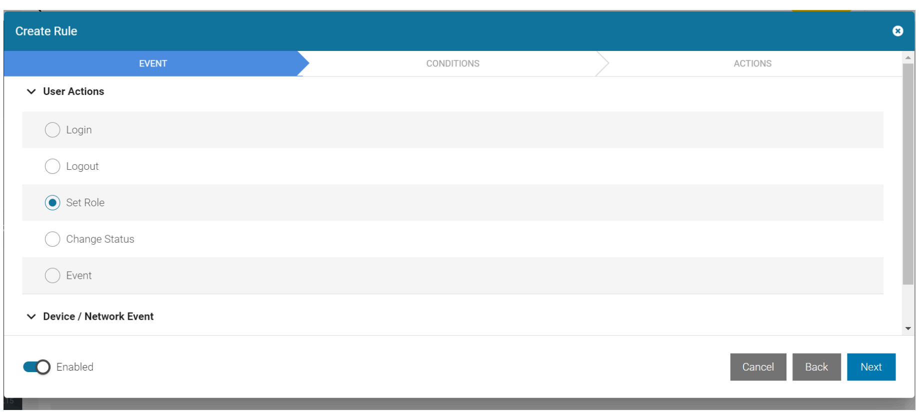
Figure 35 Create Rule Dialog Box



3. Enter a name in the **Name** field.
4. Enter a description in the **Description** field.
5. Click **Next**.

   The **Event** screen appears.

Figure 36 Create Rule — Event Screen

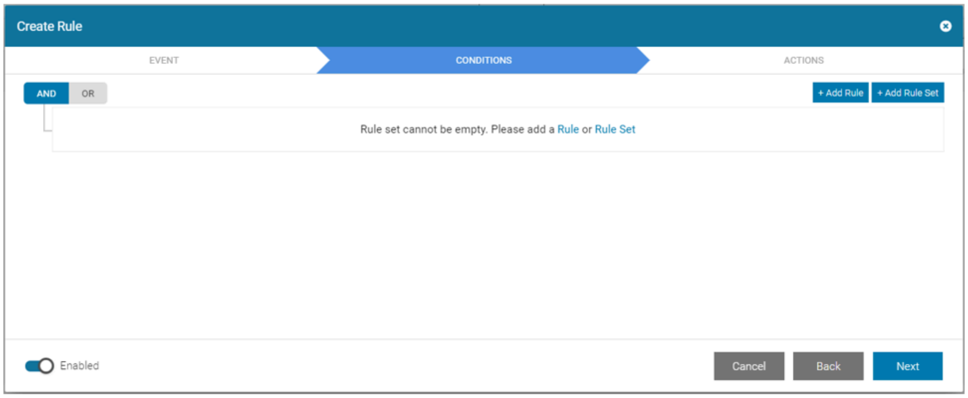


6. Select options for **User Actions**, **Automation**, and **Location Events**.

7. Click **Next**.

   The **Conditions** screen appears.

   Figure 37 Create Rule - Conditions Screen

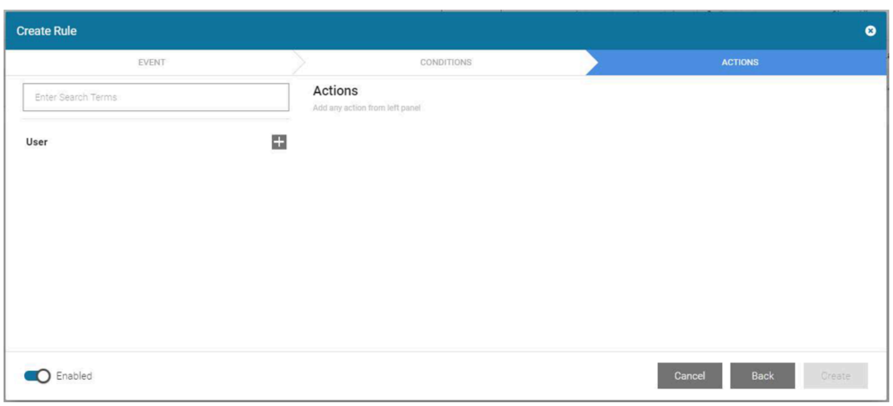


8. Leave setting at **AND**, or select **OR**.
9. To add a rule, click **+Add Rule**. Otherwise, to add a rule set click **+Rule Set**.

   If you enter invalid information, the system displays an error message.
10. Select options from the **Field**, **Operator**, and **Value** drop-downs.
11. Click **Next**.

    The **Actions** screen appears.

    Figure 38 Create Rule - Actions Screen



12. Select **Actions**.
13. Select **User**.
14. Click **Create**.

    The new rule is created.

Publish Rules

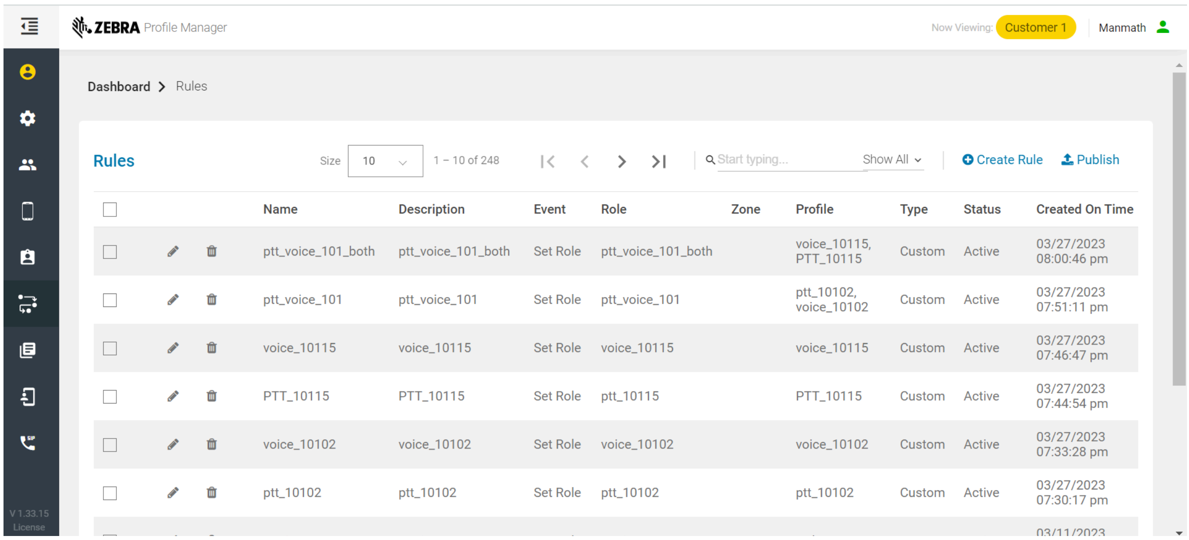
NOTE: Once the rule is created and any time a rule is edited, it must be published.

The role that you own allows you to publish rules.

1. From the dashboard, click **Rules**.

   The **Rules** screen appears.

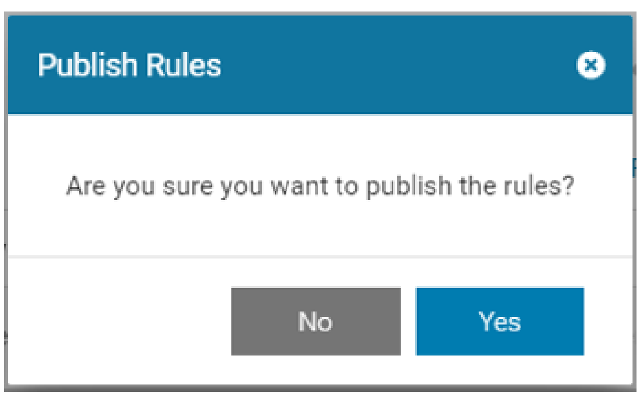
   Figure 39 Rules Screen



2. Click **Publish**.

   The **Publish Rules** dialog box appears.

   Figure 40 Publish Rules Dialog Box



3. Click **Yes**.

   The rules are published.

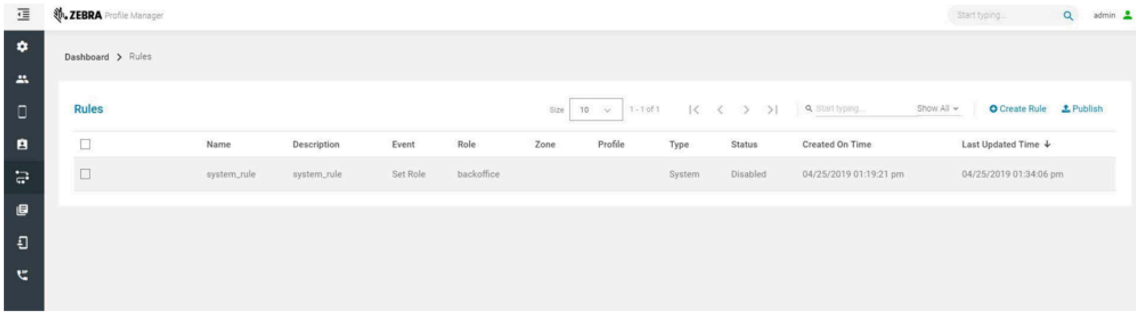
Delete Rules

The role that you own must allow you to delete rules.

1. From the dashboard, click **Rules**.

   The **Rules** screen appears.

   Figure 41 Rules Screen

2. Select the checkbox for the rule(s) you wish to delete.

   The **Delete Rules** button appears.

3. Click **Delete Selected Rule(s)**.

   The rule(s) are deleted.

System Report Management

The **System Reports** function provides historical reporting of actions performed in the Profile Manager portal.

This section describes how to:

- Generate system reports
- Export system reports
- Create report templates
- Edit report templates
- Delete report templates.

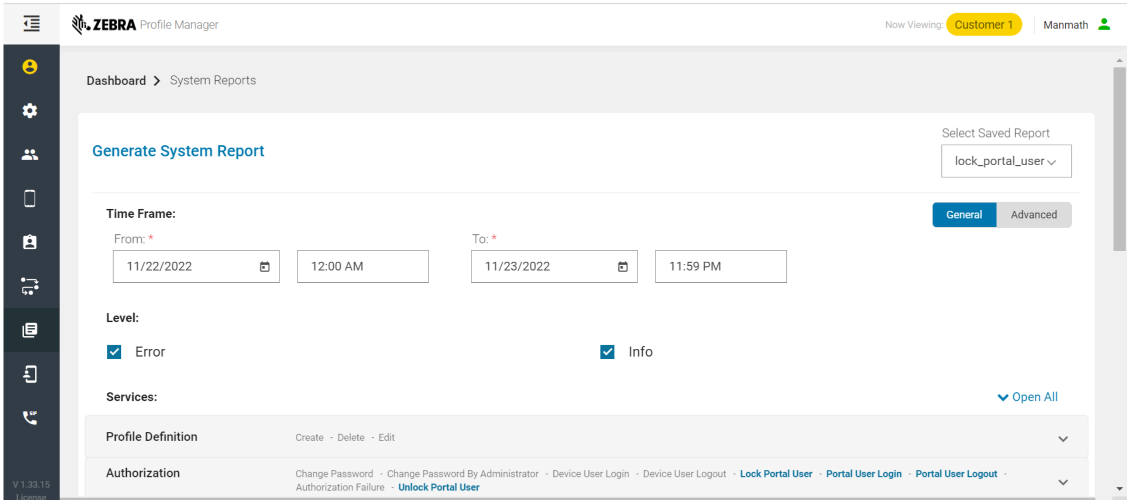
Generate Reports

The role that you own must allow you to generate system reports.

1. From the dashboard, click **System Reports**.

   The **Generate System Report** screen appears.

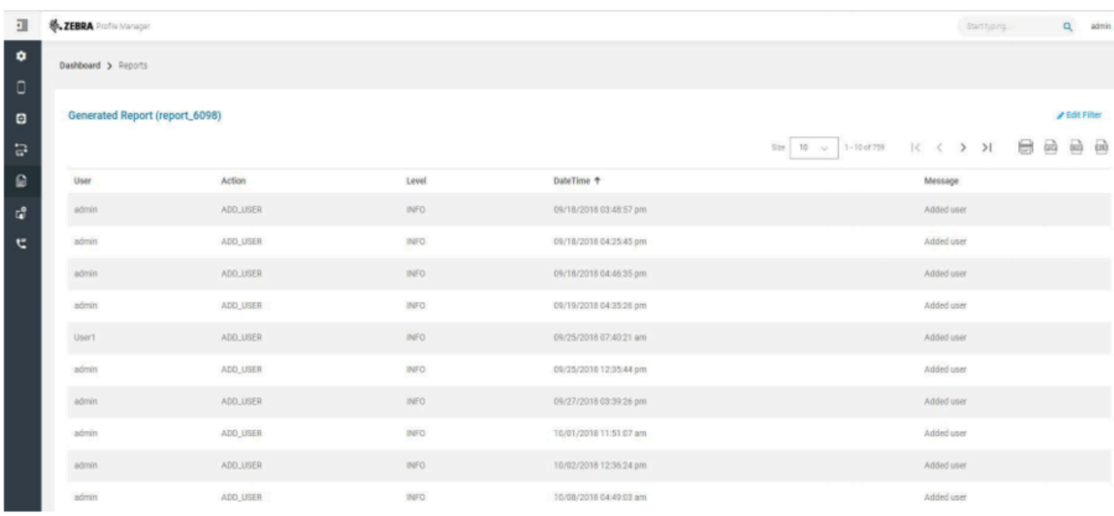
   Figure 42 Generate System Report Screen



2. Click the **Select Saved Report** drop-down and select the report that you wish to generate.
3. Click **Generate Report**.

   The report appears.

   Figure 43 Generate Report



Export Reports

- Your privileges must permit you to export system reports.
- You must generate a report to export it, see Generate Reports.

1. Generate a report, as previously described.

   The **Generated Report** screen appears.

2. From the **Generated Report** screen, select the icon for the export (**Print**, **PDF**, **CSV**, or **XLS**).

   If you selected **Print**, options for printing the report appear. Otherwise, the file (PDF, CSV, or XLS) is generated and automatically downloaded.

Create Report Templates

Your privileges must permit you to create report templates.

1. From the dashboard, click **System Reports**.

   The **Generate System Report** screen appears.

2. Enter the start and end times in the **To** and **From Time Frame** fields.

3. Select one or more **Level** boxes.

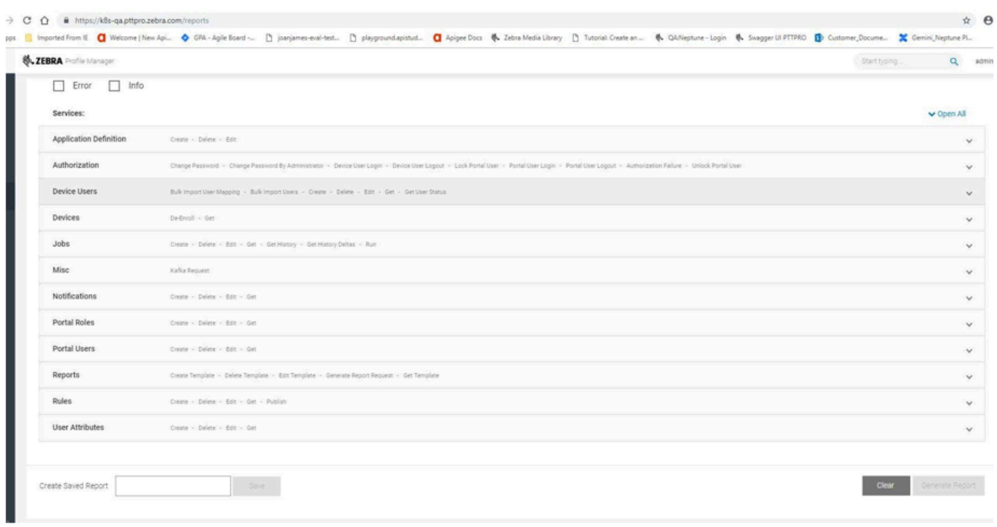
4. Click the **Services** drop-downs and use the slide switches to enable functions for the report.

5. Enter a report name in the **Create Saved Report** box in the bottom left of the **Generate Report** screen.

6. Click **Save**.

   The report template appears in the **Select Saved Report** drop-down.

Figure 44 Create Saved Report



Edit Report Templates

Your privileges must permit you to edit report templates.

1. From the dashboard, click **System Reports**.

   The **Generate System Report** screen appears.

2. Click **Select Saved Report** from the upper right and select the report template you wish to edit.

   The saved report populates the screen.

3. Make the desired changes to the **General** and **Advanced** tabs as in Create Report Templates.
4. Scroll down and click **Save**.

   The report template is updated.

Delete Report Templates

Your privileges must permit you to delete report templates.

1. From the dashboard, click **System Reports**.

   The **Generate System Report** screen appears.
2. Click Select Saved Report from the upper right and click for the report template you wish to delete.

   The **Delete Template** confirmation dialog box appears.
3. Click **Yes** to delete.

   The report template is removed from the **Select Saved Report** list.

Identity Provider Import Management

This chapter describes how to manage:

- Device user attribute mappings
- Import jobs
- Import job notifications
- Import job scheduler.

This next section provides the ability to import specific fields from your Identity Provider (IDP) user characteristics into PTT Pro and Profile Manager Systems.

The Profile Manager Provisioning Guide describes how to import users through bulk import, the AD Connector, or a flat file using Google Cloud Platform and Secure FTP. The Profile Manager Provisioning Guide provides detailed information regarding the architecture of the various methods of importing multiple users into the Profile Manager and PTT Pro, where applicable. In addition, the guide describes the process for each import method, the associated Attribute Transformations, and the information required from the customer to enable each method.

Device User Attribute Mappings

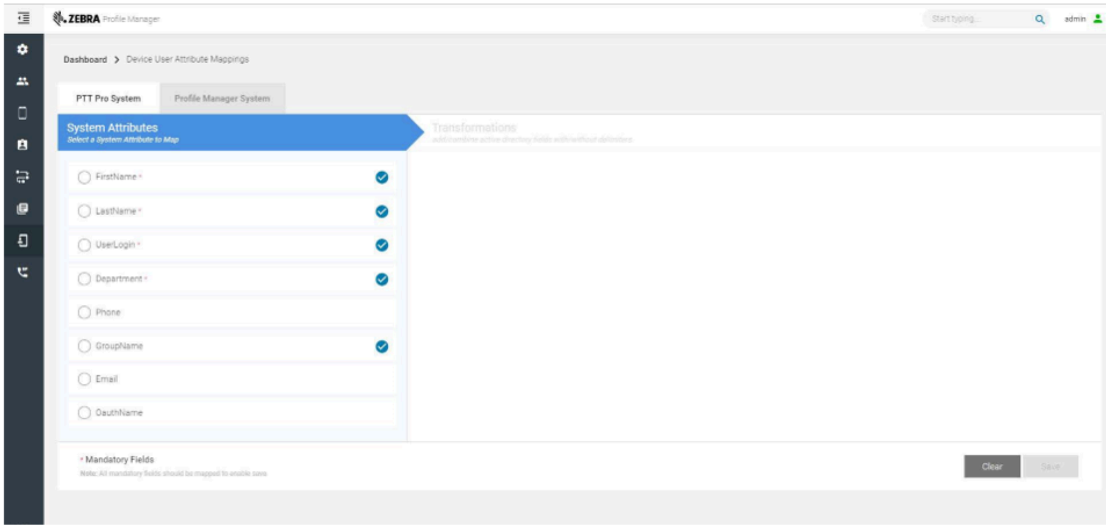
View Mappings

Your privileges must permit you to view device user attribute mappings.

1. From the dashboard, click **Device User Attribute Mappings**.

   The **PTT Pro System** tab displays the **System Attributes** and **Transformations** sub tabs.

   Figure 45 PTT Pro System Tab



2. To view a mapping for the **PTT Pro System**, click **System Attribute**. Otherwise, click the **Profile Manager System** tab and click **System Attribute**.

   The **Transformations** content are populated.

Add an Attribute, Constant or Function

Your privileges must permit you to modify user attribute mappings.

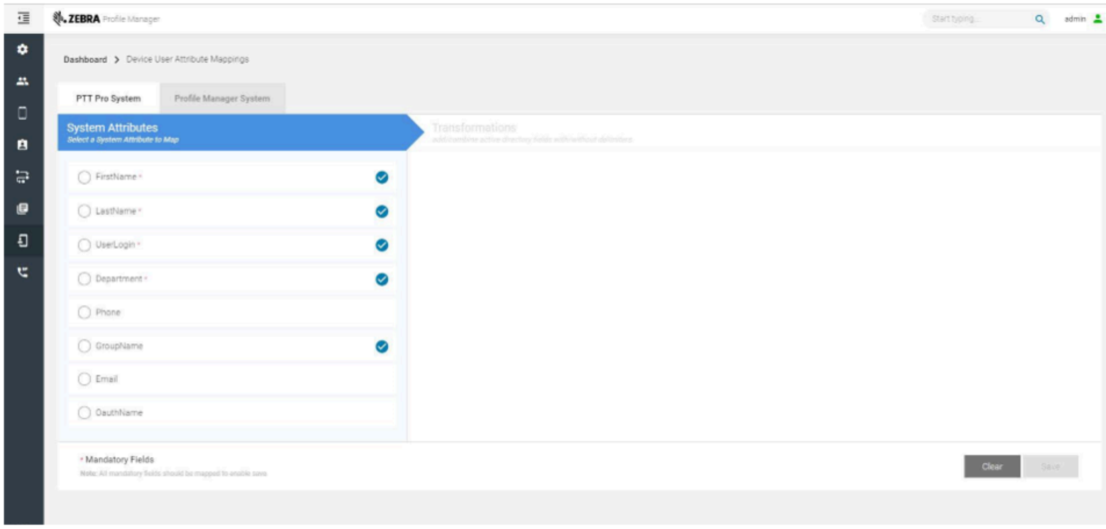
1. From the dashboard, click **Device User Attribute Mappings**.

   The **PTT Pro System** tab displays the **System Attributes** and **Transformations** subtabs.

2. Click a system attribute.

   The **Transformations** content is populated.

   Figure 46 PTT Pro System Tab



3. From the **Transformations** subtab, click the **Add Attribute** button or the **Add Constant** button or the**Add Function** button.
4. In the box that appears, enter the required information.
5. Select an option from the drop-down.
6. Add more attributes or constants, if needed.
7. Click **Save**.

NOTE:

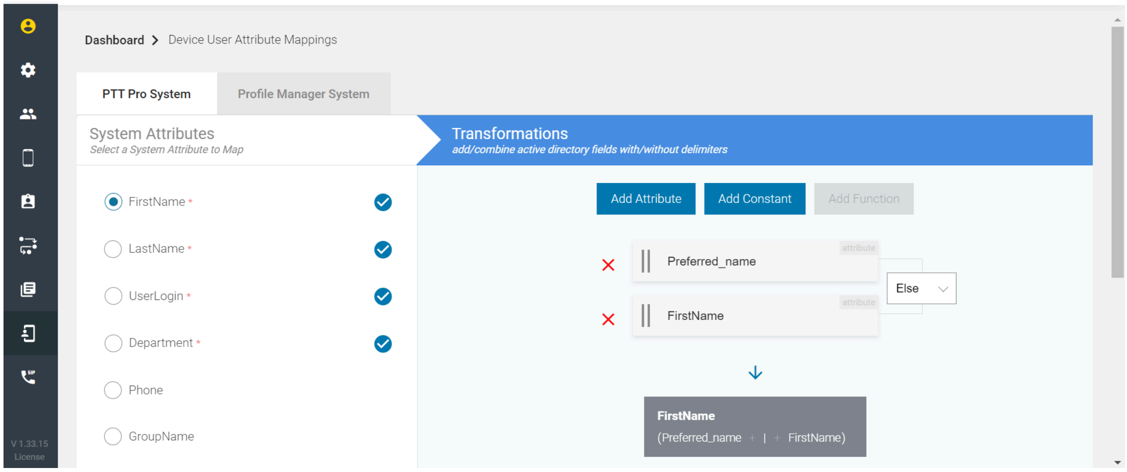
- All the mandatory user attributes are mapped to either attribute, constant, or function. In case of Profile Manager,
  - User Roles and User Role Levels are optional user attributes. However, one of them must be mapped properly.
  - If the Authentication Type in the Tenant Configuration is IMPRIVATA or LAUNCHER, the **Force Logout** mapping can be anything. This is ignored during the device Login.

Add Attributes

User attributes can be mapped any of the attributes coming from LDAP or flat file system, in case of LDAP, the attribute name should be given in lowercase.

In case of a flat file system, the attribute name should be given in the same case as given in the CSV file header fields.

User attributes can be mapped with IF THEN ELSE conditional expression by using the Else separator between the attributes. If the first attribute is not present or the attribute value is not present, then the second attribute value is used for user attribute mapping. One can define multiple LDAP attributes with an Else separator between them. Subsequent attributes are evaluated only when the previous evaluation does not result in any value.



Example

The Map user attributes First Name to preferred_name or fist_name LDAP attribute with Else separator. In this case, the First Name is mapped with preferred_name if it is present; otherwise, it maps with the first_name attribute.

NOTE: There is special support given to the LDAP member of attribute for user attribute Role Level and Roles. This converts the list having attribute name CN into comma-separated values.

Example

```
[
"CN=Smartphones_SM1,OU=Security
 Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca",
"CN=Smartphones_SM2,OU=Security
 Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca",
"CN=Smartphones_SM3,OU=Security
 Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca"
]
```

is converted as Smartphones_SM1, Smartphones_SM2, Smartphones_SM3

Add Function

This feature is added to extract the part of the AD attribute value or substitute with lookup feature to map with the user attribute value. Function can be mapped with any of the PTT Pro or Profile Manager user attribute. Function is added as JSON string with required parameters for each function. An example of JSON is added in the text field when the Add Function button is clicked. User can modify as per the requirement.

```
Default Function Template
{
"function":"find",
"params":{
"value":"Enter here",
"pattern":"Enter here",
"index": 0,
"group": 0
```

```
}
}
```

Table 1 Function JSON Parameters

Attribute Name	Data Type	Description
function	String	Name of the function. Supported functions: find, substitute, and replace.
params	JSON	Parameters for the function. List of parameter attributes varies for.

Find Function

This function is used to extract the part of the AD attribute value.

Params JSON Parameters for Find Function

Attribute Name	Data Type	Description
value	String	Value field on which regex pattern is applied. This could be the combinations of one or many AD attributes or constants strings. For example, if the AD attribute value of given name is paul, ${givenname}@pttpro is evaluated as paul@pttpro **NOTE:** If the value requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\).For example, value pttpro\${givenname} should be given as pttpro\\${givenname}.
pattern	String	regex pattern to be applied on the value. **NOTE:** If the pattern requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\). For example; pattern ^\ For example; pattern ^\d{4} should be given as ^\\d{4}
index (optional)	Integer	If the pattern matches with multiple values:- If value is less than 0, then returns all the matching regex expression value separated by comma. If value is greater than or equal to 0, then returns the pattern value at the given index. Default Value: 0
group (optional)	Integer	If the regex uses grouping, it returns the group value. Default value:0

Example 1

Map the user attribute department to the AD attribute extensionattribute7. The extensionattribute7 value in AD is 1024-0843 SS-Apparel function mapping for department attribute.

```
"
function":"find",
"params":{
"value":"${extensionattribute7}",
"pattern":"^\\d{4}",
"index": 0,
"group": 0
}}
```

This should extract first 4 digits from extensionattribute7 AD attribute value and map to the user attribute department.

Example 2

if the member of AD attribute has the following value

```
[
"CN=Smartphones_SM1,OU=Security
Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca",
"CN=Smartphones_SM2,OU=Security
Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca",
"CN=Smartphones_SM3,OU=Security
Groups,OU=Groups,OU=East,OU=Resources,DC=rona,DC=ca"
]
User Role Level mapping mapping with below find function mapping results
in same list of role levels with comma separation
{
"function": "find",
"params": {
"value": "${memberof}",
"pattern": "CN=(.?),",
"index": -1,
"group": 1
}
}
```

is converted as Smartphones_SM1, Smartphones_SM2, Smartphones_SM3

Substitute Function

This function is used to extract the part of the AD attribute value and use it as key for a lookup table provided in the function to get the corresponding value from the lookup table.

Table 2 Params JSON Parameters for Substitute Function

Attribute Name	Data Type	Description
value	String	Value field on which regex pattern is applied. This could be the combinations of one or many AD attributes or constants strings. For example, if the AD attribute value of extensionattribute7 is 10245-0843-SRE-Apparel, ${extensionattribute7} is evaluated as 10245-0843-SRE-Apparel **NOTE:** If the value requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\).For example, value pttpro\${givenname} should be given as pttpro\\${givenname}.
pattern	String	regex pattern to be applied on the value. **NOTE:** If the pattern requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\). For example; pattern ^\d{4} should be given as ^\\d{4}.
index (optional)	Integer	If the pattern matches with multiple values, it returns the pattern value at the given index. Default Value: 0
group (optional)	Integer	If the regex uses grouping, it returns the group value. Default value:0

map	Map of Name and Value	List of name and value pair for replacing the key name with value.
		
		For example;
		
		`{`
		`"1023": "admin",`
		`"1024": "sme",`
		`"1025":"associate",`
		`"1026":"standard"`
		`}`

Example 1

Map the user attribute department to the AD attribute extensionattribute7. The extensionattribute7 value in AD is 10245-0843-SRE-Apparel.

Function of mapping the department attribute

```
{
```

```
"function":"substitute",
"params":{
"value":"${extensionattribute7}",
"pattern":"^\\d{4}",
"index": 0,
"group": 0,
"map": {
     "1023": "admin",
     "1024": "associate",
     "1025":"sme",
     "1026":"standard"
      }
}
}
```

This should extract first 4 digits from extensionattribute7 AD attribute value and lookup for the map attribute to get the value pair for this name and map to the user attribute.department.

In the above example first 4 digit extracted to 1024.

Look up for 1024 in the map attribute which is associated with user attribute department and user attribute department sets with associated value.

Example 2

Map the user attribute department to the AD attribute extensionattribute7. Theextensionattribute7 value in AD is jobid=1024.

Function of mapping the department attribute

```
{
"function":"substitute",
"params":{
"value":"${extensionattribute7}",
"pattern":"(jobid=)(\\d{4})",
"index": 0,
"group": 2,
"map": {
       "1023": "admin",
       "1024": "associate",
       "1025":"sme",
       "1026":"standard"
       }
      }
}
```

In this example, pattern is used to divide the value in 2 groups. This should return the 4 digit value from the second group. (group 0 always returns the entire source string). Once the digits are extracted, look up for the map attribute to get the value pair for this name and map to user attribute department .

In the above example first 4 digit extracted to 1024.

Look up for the 1024 in the map attribute which is associated with the user attribute department and user attribute department sets with the associated value.

NOTE:

- if the key (1024 in this example) is not found in the map, it sets the null value to the department user attribute.
- If user attribute is mandatory type, then importing of user fails.

Replace Function

This function is used to replace the ad attribute value with replace string.

Table 3 Params JSON parameters for replace function

Attribute Name	Data Type	Description
value	String	Value field on which regex pattern is applied. This could be the combinations of one or many AD attributes or constants strings. For example; if the AD attribute value of extensionattribute7 is 10245-0843-SRE-Apparel, ${extensionattribute7} is evaluated as 10245-0843-SRE-Apparel **NOTE:** If the value requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\).For example, the value pttpro\${givenname} should be given as pttpro\\${givenname}
search	String	Search pattern to be applied. **NOTE:** If the value requires backslash (\) or double quotes, then these characters should be escaped with another backslash (\). For example; pattern ^\d{4} should be given as ^\\d{4}
replace	String	Replace the string for all the search patterns. Search pattern is checked by ignoring the case.
max (optional)	Interger	Number of occurrences to replace. Default value: -1 (ALL) – Case sensitive 1 – Replace first string – Case sensitive N – Replace nth string – Ignore Case

Example

Map the user attribute department to the AD attribute extensionattribute7. The extensionattribute7 value in AD is 1024-0843-SRE-Apparel.

Function mapping for department attribute

```
{"
function":"replace",
"params":{
"value":"${extensionattribute7}",
"search":"1024",
```

```
"replace": "software"
}
```

It replaces all search strings 1024 in extensionattribute7 AD attribute value with replace string software and map to user attribute department.

In the above example 1024 is replaced with software. The user attribute department uis set with value of software-0843-SRE-Apparel.

NOTE: If the key is not found in the map, it does not replace the string.

Create Extension During User Import

When importing the user into the Profile Manager system, it can automatically create and reserve an extension in the Extension Manager. The following details are needed for reserving an extension during the user import.

Name	Description
Department	User attribute mapping for Profile Manager. This field should contain a valid site name defined in the Extension Manager.
Hidden Department Name	Name of the department in the extension manager. This should be configured for this tenant in the tenant configuration. If the department is not present in the extension manager, it creates one for the first user import. Extensions are created under this department.
PBX Extension	This is the sip_mac or extension value of the PBX, depending on the target PBX. Target PBX is configured as the default PBX for the customer in the Extension Manager.

If the PBX Extension is changed during subsequent user import, the old extension is deleted, and a new one is created.

NOTE:

- Create PBX Extension using the User Create/Edit UI.
- Creating the PBX extension is not supported in the user import using a CSV file.

Integrating Zebra Enterprise Messaging Server (ZEMS) During User Import

During the user import, one can associate the user as a manager of the site or region in the ZEMS system. Actual association happens when the ZEMS system is synced with the PTT PRO server. Usually, ZEMS syncs once a day unless sync is triggered manually. One must configure the ZEMS sync time after the Profile Manager user import job scheduled time.

The following details are needed for the association:

1. Configure the ZEMS URL and API key in the tenant configuration.
2. Add the manager and region fields in the user input CSV file or identify these fields in LDAP attributes.

3. Add the PTT PRO user mapping for the manager and region attributes, as shown in the following table.

Name	Description
Manager	The mapping attribute value in LDAP or CSV file should be either true or false. If the field value is true, and it was false or empty during the last import, a user is associated as a manager to the site and region list specified in the region field. If the field value is true, and it was true during the last import, the user is associated as a manager to the site and region list, which are newly added. Also removed from the association if it is removed from the list. If the field value is false, and it was true during the last import, the user is removed from the previous site and region association. If the field value is false, and it was false during the last import, no changes in the association.
Region	The mapping attribute value in an LDAP or CSV file should contain a list of sites or regions separated by a comma. By default, the user's current site is associated using the Department field. If the user needs to be associated with other sites, it should be included in the region field.

Clear an Attribute Mapping

To clear a user attribute mapping:

1. Navigate to the attribute mapping to clear, as in View Mappings.

2. Click **Clear**.

Import Job Management

The Import Job takes the information from the attribute mappings, and populates the information in the Profile Manager and PTT Pro Systems.

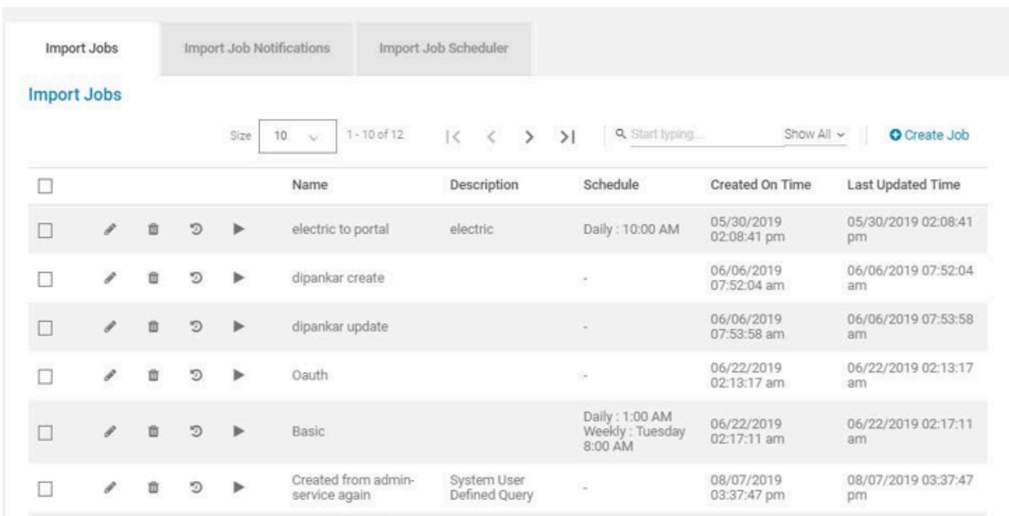
View Import Jobs

Your privileges must permit you to view import jobs.

- From the dashboard, click **Import Jobs**.

  The **Import Jobs** screen appears.

Figure 47 Import Jobs Screen



Create Import Jobs

Your privileges must permit you to create import jobs.

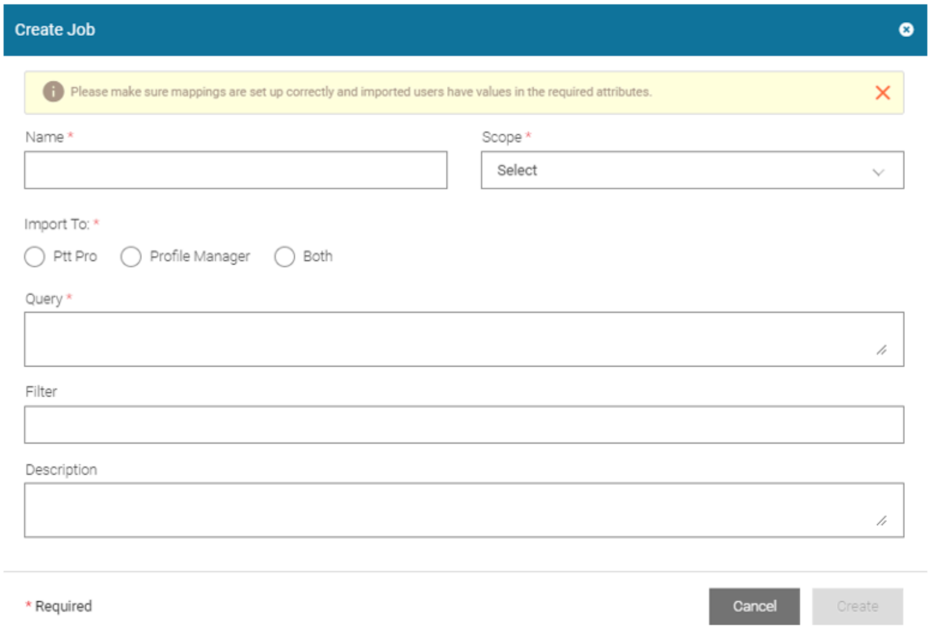
1. From the dashboard, click **Import Jobs**.

   The **Import Jobs** screen appears.

2. Click **Create Job**.

   The **Create Job** dialog box appears.

   Figure 48 Create a Job Dialog Box



3. Use the following table to complete the fields in the **Create Job** dialog box.

Field Name	Description
Name	Job Name
Scope	Active Directory Search Scope • Object: base object • One Level: immediate children of the base object • Subtree: base object and all child objects.
Query	Search the Active Directory. For example: OU=users,DC=PTTPRO,DC=ZEBRA For Flat file import, this field is ignored. Users can enter any value. For clarity, users can enter GCP for the Google Cloud storage and SFTP for the SFTP server.
Filter	Search for a subset of the user(s). For example, to search for anyone with the name Andrew: (name=andrew*) For Flat file import, this field should be filled with the file name that needs to be downloaded from the Google Cloud bucket or SFTP server.
Description	Optional description of the purpose of the import.

Edit Jobs

Your privileges must permit you to edit import jobs.

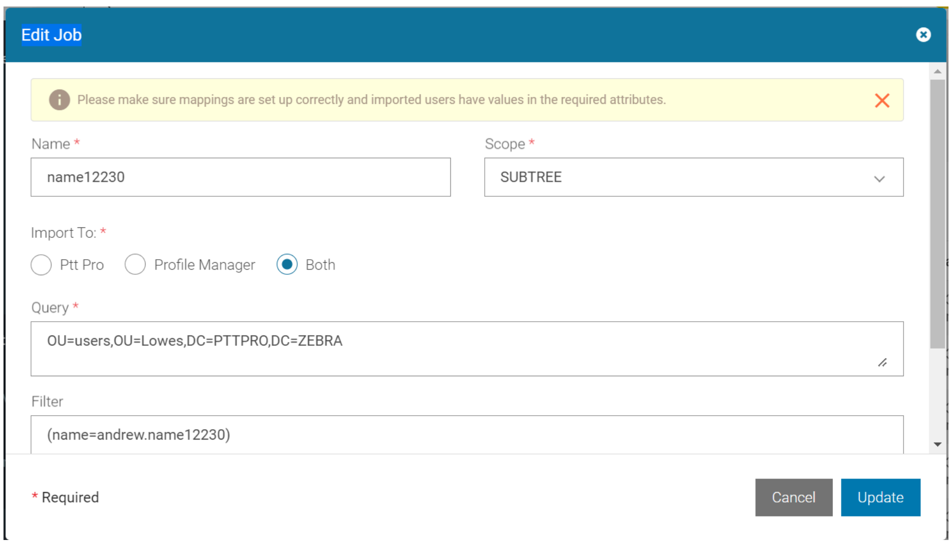
1. From the Dashboard, click **Import Jobs**.

   The **Import Jobs** screen appears.

2. Click  next to the job you wish to edit.

   The **Edit Job** dialog box appears.

   Figure 49 Edit Job Dialog Box



3. Update the fields as in Create Job Dialog Box.

4. Click **Update**.

   It is recommended not to change the Query and Filter parameter values during the editing job. Instead, one should create a new job if any changes are required in the query. This is mostly applicable to the LDAP-based import job. If there are users imported with the original job, those users might get imported again with the new job if the query matches. Because the job is created new, all those users are displayed as New records in the job history for the first run. However, job execution creates or updates the record depending on whether a user exists in Profile Manager or in the PTT Pro system.

   If the job import has huge sets of users, then creating a new job takes a lot of time to import the users for the first time. In this case, one can change the query/filter. It adds or deletes the new set of users based on new query/filter criteria.

   If the same user is imported with multiple import jobs, irrespective of the job history status for that user (New, Modified, or Deleted), if the user already exists, it updates the user with new details. The user has the details from the job which is executed last.

NOTE: If you change the name of a job, be sure to edit the job name in any Import Job Notifications associated with the job.

Delete Jobs

Your privileges must permit you to delete jobs.

1. From the dashboard, click **Import Jobs**.

   The **Import Jobs** screen appears.

2. Click next to the job you wish to delete.

   The **Delete Job** dialog box appears.

3. Click **Yes** to delete.

Run Import Jobs

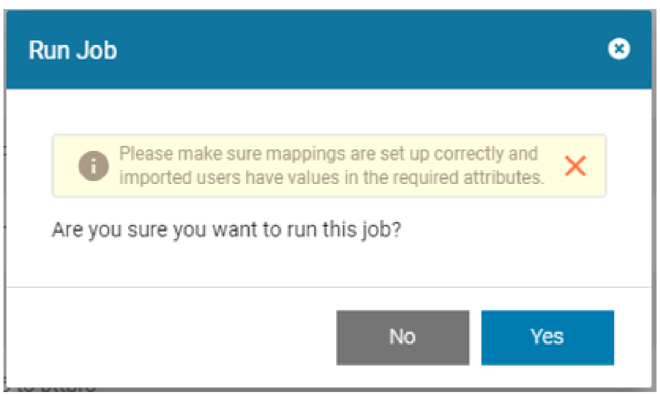
- Your privileges must permit you to run import jobs.
- The mapping must be set up correctly.

1. From the dashboard, click **Import Jobs**.

2. From the Import Jobs screen, click for the job you wish to run.

   The **Run Job** dialog box appears.

   Figure 50 Run Job Dialog Box



3. Click **Yes** to run the job.

NOTE: Jobs run using the **Run Job** option are executed sequentially even if more than one Job run is triggered simultaneously.

View Import Job History

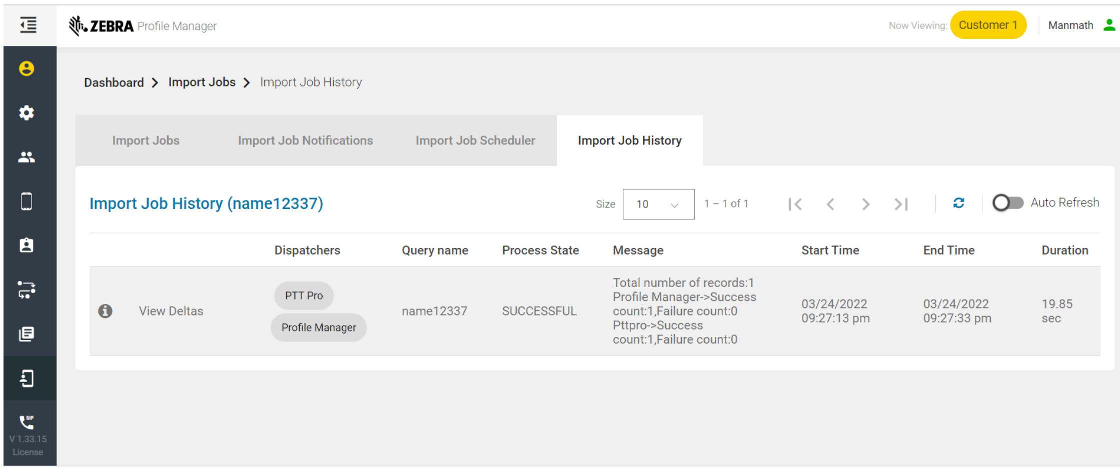
Your privileges must permit you to view the job history.

1. From the dashboard, click **Jobs**.

2. Click For the import job history you wish to view.

The **Import Job History** screen appears.

Figure 51 Import Job History Screen



Process State displays the job execution status. The status gets periodically updated depending on the BULK_UPDATE_RECORD_SIZE (Default Value = 50) configuration in the AD-Connector service. The import job execution runs parallel with multiple threads depending on the number of PTT Pro instances configured for that tenant. BULK_UPDATE_RECORD_SIZE is applicable per thread. Hence the exact number of records processed in each status update varies for each deployment.

For example, if the number of PTT Pro instances is 24 and BULK_UPDATE_RECORD_SIZE = 50, the status is updated and displayed after 24*50 = 1200 records.

Along with the status update, all relevant job history and delta records also get updated in the Profile Manager.

After the job is executed, it goes through the following statuses:

Job Status	Description
IN_PROGRESS	When the job started execution.
FAILURE	When the job execution fails.
SUCCESSFUL	When the job execution becomes successful.
STOP_TRIGGERE	If the user has initiated the Stop feature on the running job. From this state, jo,b status can go into the following status: • `FAILURE`: If execution fails before the stop is processed. • `STOPPED`: If more records are pending to be completed, and can stop the job before processing all the records. • `SUCCESSFUL`: If no more records are pending processing. All the records are already processed before the Stop feature is processed.

STOPPED	If the job execution is stopped and records remain to be processed. The stopped jobs can be restarted like any other jobs.

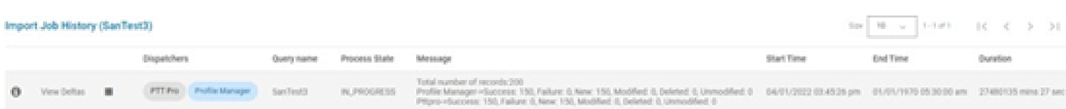
The Message column displays the error message in case of FAILURE or a summary of the import relevant to job configuration.

This includes:

- The number of records processed.
- The number of successful and failed records for the Profile Manager and PTT Pro.
- The number of modified, unmodified, new, and deleted Profile Manager and PTT Pro records.
- The number of ignored records is because of either no matching site entry defined in the sitemap file or the site is defined for a different Profile Manager cluster (This applies only to the non-proxy environment with sitemap present in AD-Connector-service).
- In case of Flat File Import, the job can also fail if the number of records in the usermap CSV file exceeds the flat-file variance threshold percentage allowed for this tenant. Variance is checked against the previous successful run on upper and lower boundaries. This would prevent any wrongly generated CSV file from being used for import which causes deleting previous records not present in the current CSV file.
- In case of Flat File Import, the job can also fail if the usermap CSV file does not contain the header row. Two mandatory columns Department and UserName, identify the header row. The name of these columns can be changed during deployment based on the usermap header format.
    - The Department column header name can be changed using the general site-header-name or CSV_SITE_HEADER environment variable. (Default Value: Department).
    - The UserName column header name can be changed using ldap.uniqueName or LDAP_UNIQUE_NAME environment variable (Default value: samaccountname).
    - For all other header columns, it just loads the column as is. The sample error message for missing header follows:

NOTE:

- In case of PFM-Proxy, the number of records processed is equal to the number of records of either Profile Manager or PTT Pro, depending on the selected dispatcher.
- In case of non-proxy, the number of records processed is equal to the number of records of either Profile Manager or PTT Pro.

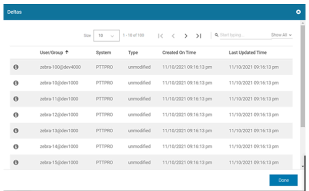


NOTE: The sitemap file contains the mapping for the site to the Profile Manager instance.

Actions available on the **Import Job History** screen are view details, view deltas, and view dispatcher.

3. Click ⓘ to view details.

4. Click to stop the running job. This icon is visible only for the jobs that have started execution.



After clicking the Stop icon, the job goes into the STOP_TRIGGERED state. The execution of the job stops after processing all the current set of records as defined by the BULK_UPDATE_RECORD_SIZE (Default Value = 50 per thread). The exact number of records in a chunk depends on the number of threads (number of PTT Pro instances).

When all the records in the current chunk are processed, the job goes to either STOPPED (if there are more records to be processed) or SUCCESSFUL (if all the records are processed).

If the job status is in the STOPPED state, during the next subsequent execution, all unprocessed records from the previous run, along with any error and modified records, are processed.

NOTE:

- The number of enhanced PTT Pro instances configured in the sitemap determines the number of users created/updated in parallel. The number of enhanced PTT Pro server names determines the number of users deleted in parallel. Refer to the Profile Manager Provisioning Guide for information about importing the users using flat files.
- Clicking the Stop icon stops the execution of the jobs that are in process with a large number of records, allows fixing the configuration error, and then restarts the jobs.

5. Click **View Deltas** to view more information.

   The **Deltas** dialog box appears.

   The **Type** column displays the status of the record, such as new, modified, deleted, or unmodified. Whether or not the unmodified records are listed depends on the AD-Connector service configuration. Typically, we should turn this off for the user import using a flat file to reduce the required storage.

   The Import function checks for changes to the user data by comparing it with the current user data and ignoring the AD whitelist attributes configured for the tenant. If there is no AD whitelist configured for the tenant, it uses the default whitelist attributes configured in the ad-connector service system setting (general.attributesWhitelist).

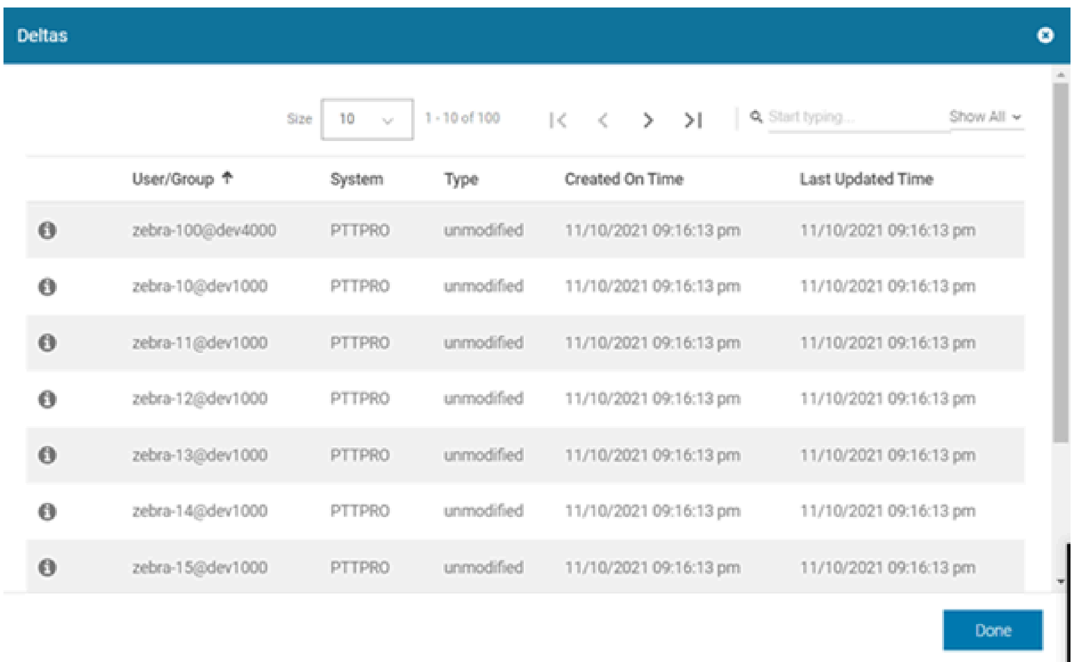
In the AD-Connector service, the default whitelist attributes are: “uncreated, whenchanged, dscorepropagationdata, unchanged, whencreated, pwdlastset, lastlogontimestamp” unless it is changed in the deployment configuration.

This page supports sorting for entire database records instead of just the displayed page. All the displayed columns are included in the sorting.

This page also supports search on the following columns:

- User/Group
- System (Profile Manager/PTT Pro)
- Type (new/modified/unmodified/deleted)

Figure 52 Deltas Dialog Box



6. Click an option in the **Dispatchers** column to more information.

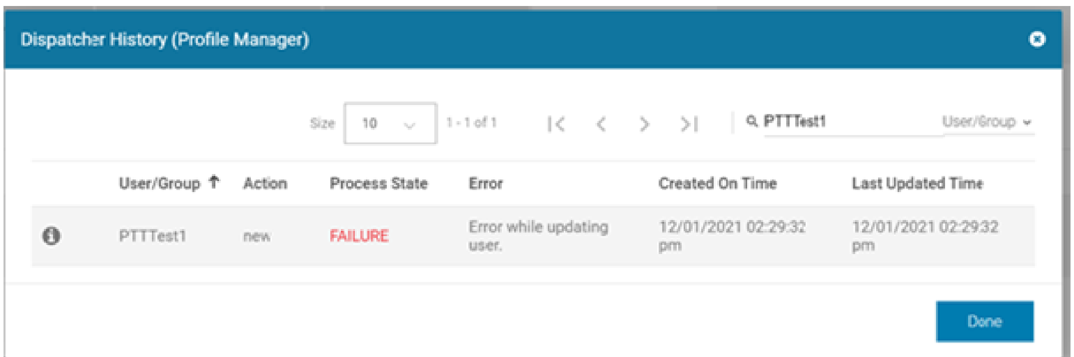
   The **Dispatcher History** dialog box appears in the STOPPED in this example, and it is for the PTT Pro dispatcher:

   This page supports sorting for entire database records instead of just the displayed page. All the displayed columns are included in the sorting.

   This page also supports search on the following columns:

   - User/Group
   - Action (new/modified/deleted)
   - Process State (FAILURE/SUCCESSFUL)

Figure 53 Dispatcher History (PTT Pro) Dialog Box



NOTE: The User/Group field is populated using the LDAP_UNIQUE_NAME attribute value specified in the AD Connector service. By default, this is mapped to samaccounname during deployment.

Import Job Notifications

Import job notifications are email messages based on the result of LDAP jobs. Profile Manager can send messages to one or more email addresses for import job success, failure, or both.

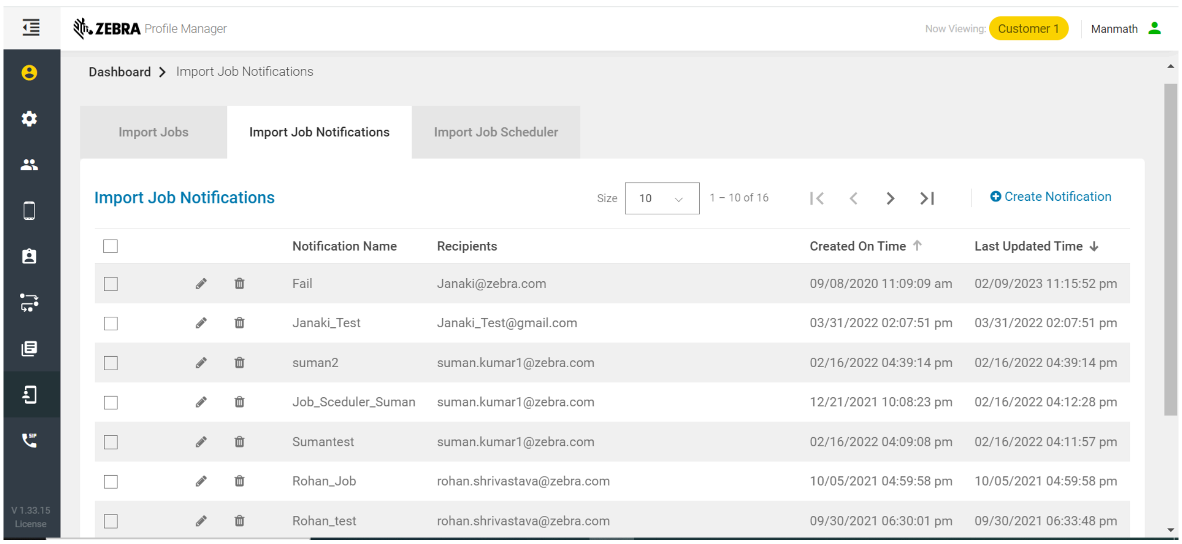
View Import Job Notifications

You must have privileges to view import job notifications.

- From the dashboard, click **Import Job Notifications**.

  The **Import Job Notifications** screen appears.

Figure 54 Import Job Notifications Screen



Create Import Job Notifications

- Your privileges must permit you to create import job notifications.
- At least one query must already be created. To

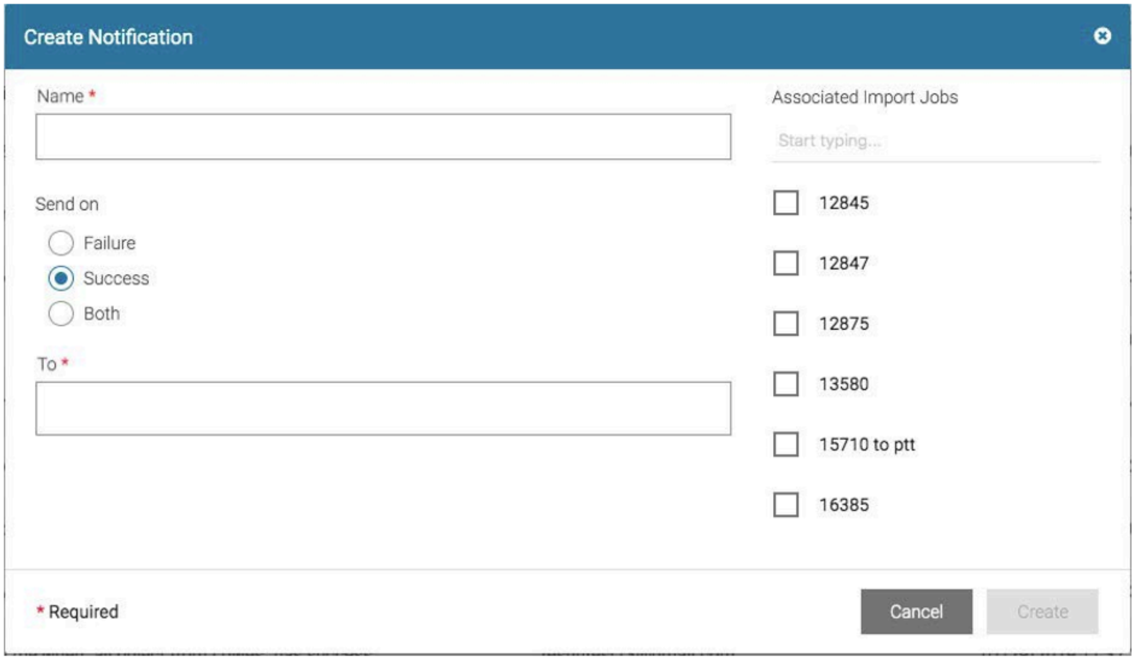
1. From the dashboard, click **Import Job Notifications**.

   The **Import Job Notification** screen appears.

2. Click **Create Notification**.

   The **Create Notification** dialog box appears.

   Figure 55 Create Notification Dialog Box



3. Enter a name for the notification in the Name field.
4. Select one or more checkboxes from the right.
5. Enter one email address in the **To** field and press **Enter**. Repeat for any additional email addresses.
6. Click **Create**.

Edit Import Job Notifications

Your privileges must permit you to edit import job notifications.

1. From the dashboard, click **Import Job Notifications**.
2. Click  for the notification you wish to edit.
3. Modify the **Edit Import Job Notification** dialog box as in Create Import Job Notifications.
4. Click **Update**.

Delete Import Job Notifications

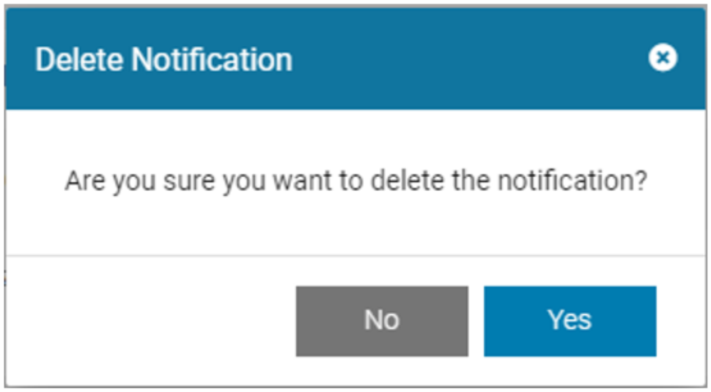
Your privileges must permit you to delete an import job notification.

1. From the dashboard, click **Import Job Notifications**.

2. Click for the notification you wish to delete.

   The **Delete Notification** dialog box appears.

   Figure 56 Delete Notification Dialog Box



3. Click **Yes** to delete.

Import Job Scheduler

Use the Import Job Scheduler to set schedules for when import jobs occur.

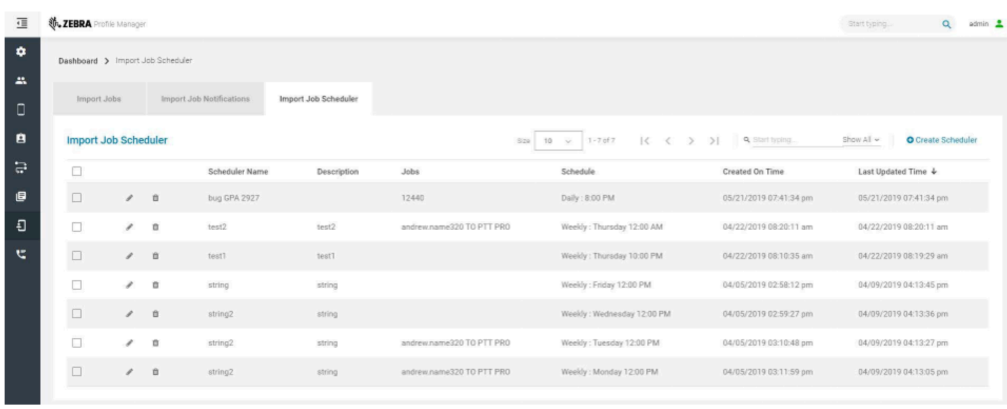
View Import Job Schedules

Your privileges must permit you to view import job schedulers.

- From the dashboard, click **Import Job Scheduler**.

  The **Import Job Scheduler** screen appears.

  Figure 57 Import Job Notifications Screen



Create Import Job Scheduler

Your privileges must permit you to create import job schedulers.

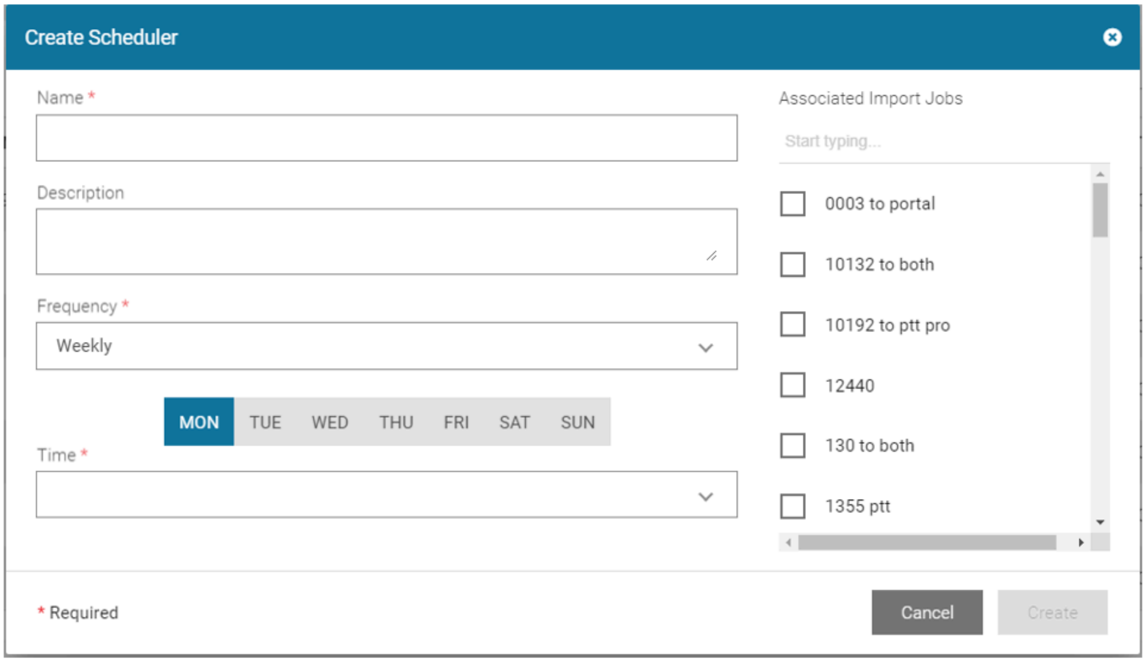
1. From the dashboard, click **Import Job Scheduler**.

   The **Import Job Scheduler** screen appears.

2. Click **Create Scheduler**.

   The **Create Scheduler** dialog box appears.

   Figure 58 Create Scheduler Dialog Box



3. Enter a name for the scheduler in the **Name** field.
4. Select one or more checkboxes from the right. If more than one job is selected, then all those jobs get executed parallelly during the scheduled time. Even if the jobs are part of two different scheduled times, they get executed parallel. If more than one job is scheduled at the same time, one must ensure that those jobs must not have the same user.
5. Select an option from the Frequency drop-down.
6. Select an option from the Time drop-down.
7. Click **Create**.

Edit Import Job Schedulers

Your privileges must permit you to edit import job schedulers.

1. From the dashboard, click **Import Job Scheduler**.
2. Click  for the scheduler you wish to edit.
3. Modify the **Edit Scheduler** dialog box as in Create Import Job Scheduler.
4. Click **Update**.

Delete Import Job Schedulers

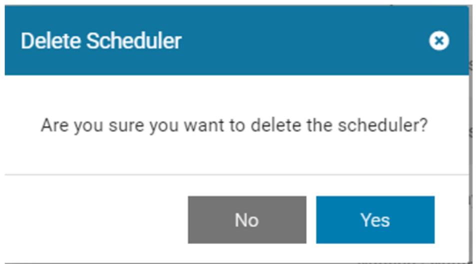
Your privileges must permit you to delete an import job scheduler.

1. From the dashboard, click **Import Job Scheduler**.

2. Click  for the scheduler you wish to delete.

   The **Delete Scheduler** dialog box appears.

   Figure 59 Delete Scheduler Dialog Box



3. Click **Yes** to delete.

Client Device Setup Using Telephony Manager and Profile Manager

Client device setup using Telephony Manager and Profile Manager is for sites that use other Telephony Manager features and functions in addition to viewing and refreshing. For information on setting up the Client Device, refer to the Workforce Connect Profile Client Guide MN-003602.

This chapter describes the following:

- Configure Telephony Manager Using a CSV File
- Manually Configure Telephony Manager (for technical support)
- Configure WFC Profile Manager
- Confirm the End-to-End Configuration of Telephony Setup
- Important Notes About Verifying Correct End-to-End Configuration
- For an overview of Telephony Manager, see Telephony Management

Configure Telephony Manager Using a CSV File

A CSV file (automated option) is used to automate the data import process. Using a CSV import eases the effort of initial deployment, configuration and incremental updates.

To import the list of Extensions using a CSV file, see the Extension Import Management on page 97.

Confirm Successful Import of Data from the CSV File

1. Open the WFC Profile Manager application.
2. In the Dashboard, navigate to **Telephony Management** and then open the **Extensions** screen.
3. In the list of extensions, confirm that the expected entries and their corresponding values appear, including the information for the following:
   - Store_Name
   - Dep_Name
   - Extension Name
   - Profile_type
   - Sip_remhost
   - Sip_Mac_address or Exension_Password (depending on your site's configuration)
4. Close the WFC Profile Manager application.

Manually Configure Telephony Manager (for technical support)

The procedures in this section are for manually entering the required information into Telephony Manager. This is done to itemize the details and dependencies of specific fields. Typically, this information is imported into Telephony Manager using a CSV file. A CSV file is used to automate the data import process. Using a CSV import eases the effort of initial deployment, configuration and incremental updates.

Accessing the Console as described here is considered more appropriate for minor (manual) configuration updates.

There are several steps to configure the Telephony Manager. The basic elements that must be configured first are the following:

- Store_Name
- Dep_Name
- Extension Name
- Profile_type
- Sip_remhost
- Sip_Mac_address or Exension_Password (depending on your site's configuration)

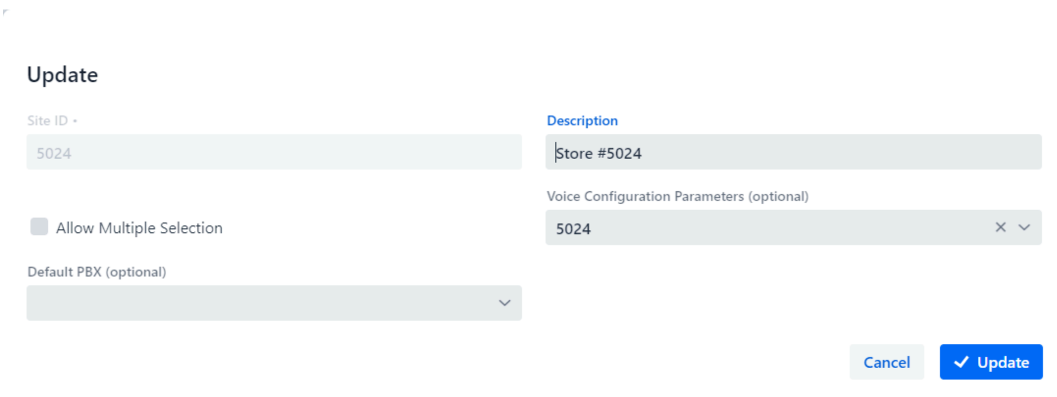
Enter the Store or Site ID Information

NOTE: In Telephony Manager, the Store (Site ID), Departments, and PBXs must be added before Extensions can be added.

In Telephony Manager, the Store (Site ID), Departments, and PBXs must be added before Extensions can be added.

1. In Telephony Manager, navigate to the **Stores** tab and select Update to add a Store entity. The Store value must be numeric only, from 1 to 19 digits long.

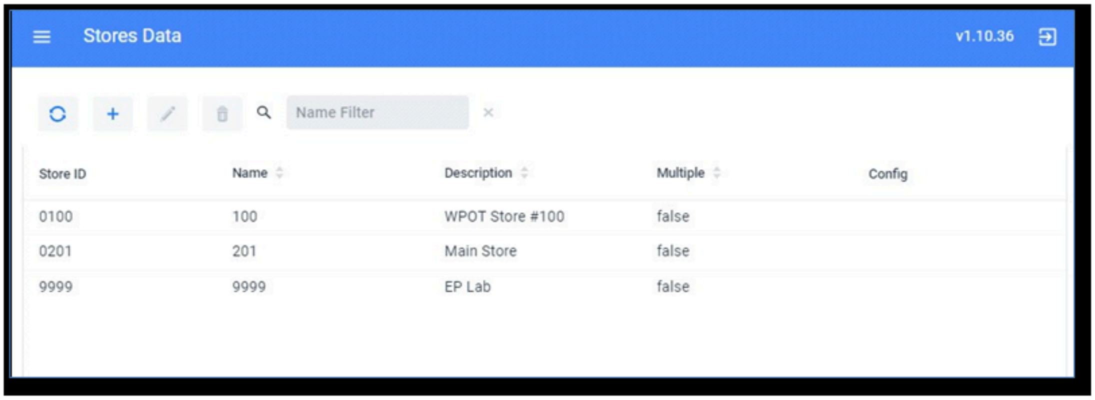
Figure 60 Update Store Screen



2. Click **Update**.

   The **Store Data** screen appears.

   Figure 61 Store Data Screen



NOTE: In Telephony Manager, ensure that the value for Store ID is the same as the Site ID value from the WFC Profile Client (in this case, 9999). For instructions on finding the Site ID for a WFC Profile Client for a device, see the Workforce Connect Profile Client User Guide MN-003602.

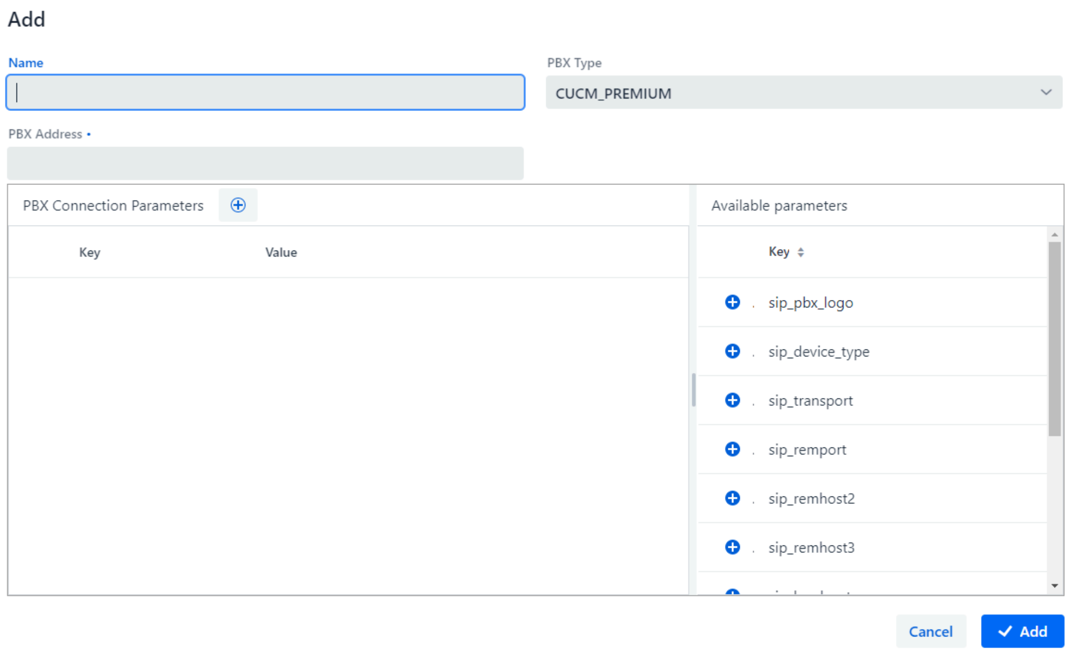
Enter the PBX Information

Establishing the targeted PBX is required. The targeted PBX can be one unique PBX per site location or one PBX shared across several or all sites. The required fields are **PBX Type** and **PBX Address**.

1. In Telephony Manager, navigate to the **PBX** tab and select **Update** to add a PBX entity.

   The **Update** screen appears.

   Figure 62 PBX Update Screen



2. Enter the information for **PBX Type** and **PBX Address**.

NOTE:

For the **PBX Type**, enter a string value. The **PBX Type** parameter is passed to the Profile Client device and must be identifiable by the device for specific PBX activation. For the valid PBXs supported for the WFC Voice Client, refer to the Administration Guide for Workforce Connect Voice Client.

3. Select **Update**.

   The following are sample PBX entries.

   Figure 63 Sample PBV Entries

Name	PBX Type	PBX Address	Parameters (JSON)
zave-test-asterisk	Asterisk	pbx-stage.pttpro.zebra.com	{"sip_remhost2":"10.10.10.10"}
secondary	CUCM_PREMIUM	10.10.10.10	{}
zave-nuc	CUCM_PREMIUM	10.11.18.9	{"sip_device_type":"9971"}

Add Department Information

NOTE: In Telephony Manager, the Store (Site ID), Departments and PBXs must be added before Extensions can be added.

Phones are assigned extensions based on Departments. There might be multiple unique extensions defined for a Department. Telephony Manager controls the distribution of the extensions provided by the PBX Administrator.

The following are the inter-relationships of the data across the subsystems.

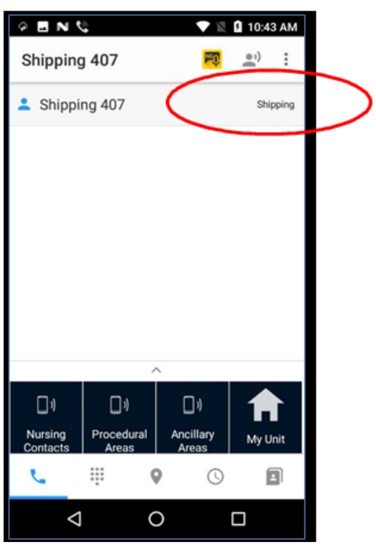
- When adding Departments, the Department Name value in Telephony Manager must match the User Role/Department value in Profile Manager.
- After a device becomes activated on a PBX, the User Role/Department value is displayed on the Profile Client device.

The following shows the relationship of the values in Telephony Manager, Profile Manager, and WFC Profile Client.

Telephony Manager	Profile Manager	PBX	Workforce Connect Profile Client Device
must match ---> Department	<--- must match User Role/ Department	WFC Client Device becomes activated --->	As a a result of device activation on PBX-- ---> User Role/Department is populated into the WFC Client Device from Profile Manager

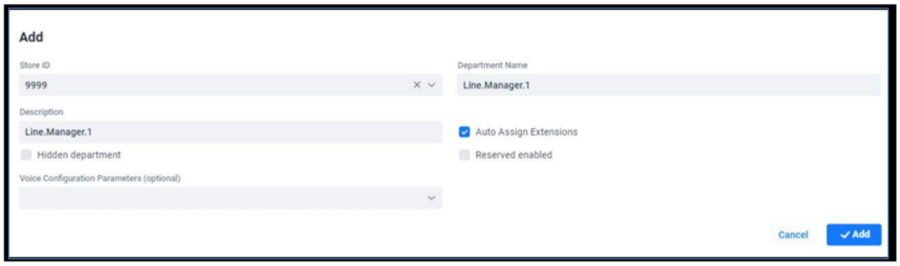
After a device becomes activated on a PBX, the User Role/Department field is displayed on the Profile Client device as shown.

Figure 64 User Role/Department Field on WFC Profile Client Device (After Device Activation on PBX)



1. Select the Store ID and Enter the Department Name and Description.

Figure 65 Sample Add Store Screen

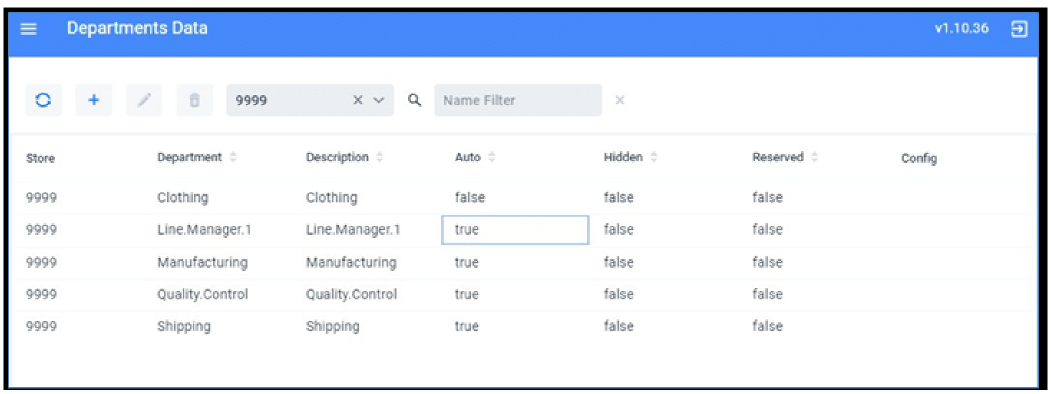


2. Select the Site ID from the drop down list and enter the Department Name and Description.
3. Check the **Auto Assign Extensions** box. This allows Telephony Manager to distribute available extensions to a device.

NOTE: The Department Name must match the User Role Definition field in Profile Manager.

When completed, the Departments is displayed. The sample Department list shows results filtered on Store 9999.

Figure 66 Sample Department List

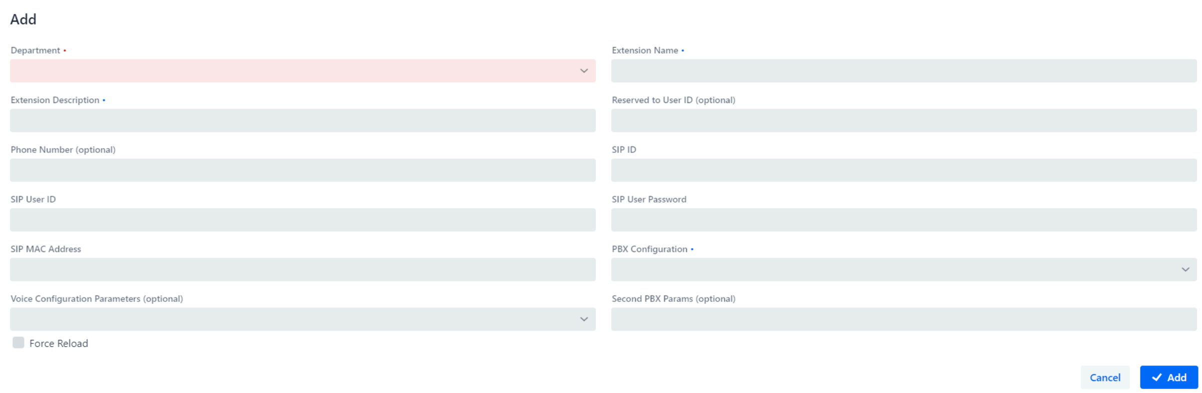


Enter PBX Extension Information

NOTE: In Telephony Manager, the Store (Site ID), Departments and PBXs must be added before Extensions can be added.

1. Navigate to the **Add Extension** screen.

Figure 67 Sample Add Extension Screen



2. Add the Extension Name and Extension Description.

NOTE: For the CUCM Premium PBX, the MAC address for the Specific Extension is entered.

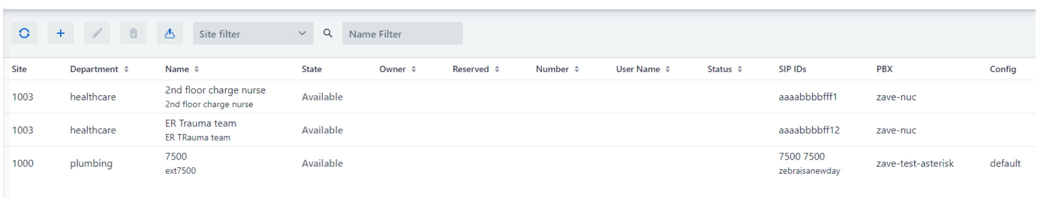
The Department assignment for the given extension is selected from the Drop Down list. This has been previously created.

The PBX Configuration is selected from the drop-down list previously created.

3. Click **Add**.

After all extensions are created, the extension list displays a list of the extensions.

Figure 68 Sample Extensions List (on Extensions Data Screen)



Configure WFC Profile Manager

Create device user roles. See Device User Role Management:

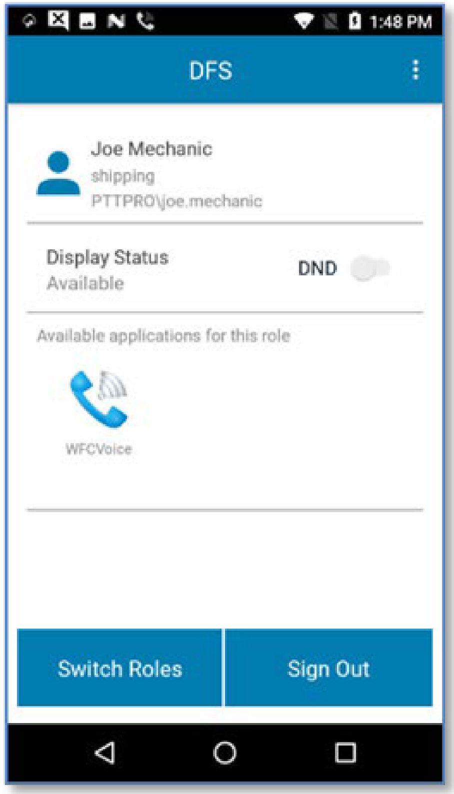
1. Create device user roles. See Device User Role Management.
2. Create device users. See Device User Management.
3. Create profile configurations. See Profile Configuration Management.
4. Create rule sets. See Rule Management.

Confirm the End-to-End Configuration of Telephony Setup

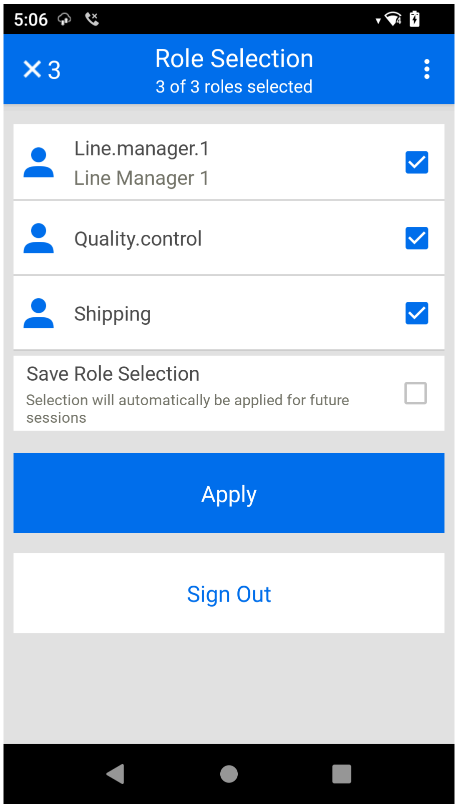
1. On a client device, log into WFC Profile Connect as the user whose User Profile you want to confirm.

   In this procedure, the example shown is for user Joe Mechanic.

2. During login, at the **Profile Client Role Selection** Screen, select **Switch Roles**.



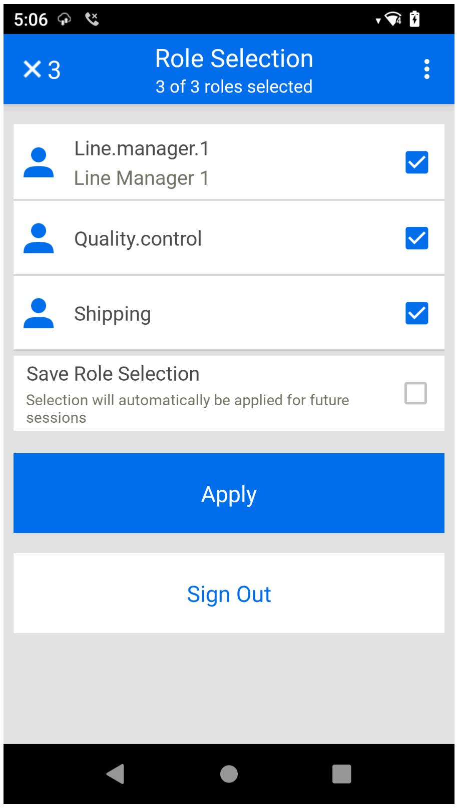
The **Role Selection** screen appears



3. In the **Role Selection** screen, the user Joe Mechanic has three roles available:
   - Line.Manager.1
   - Quality.Control
   - Shipping
4. Compare the list of roles that is in the **Role Selection** screen in the WFC Profile Client for this user to the list of roles that are configured for this user in the WFC Profile Manager application. See Edit Device User Roles.

   If the roles in WFC Profile Client and in the WFC Profile Manager application match for this user, continue with this procedure. Otherwise, check with your system administrator to confirm the list of roles to be assigned to the device user.

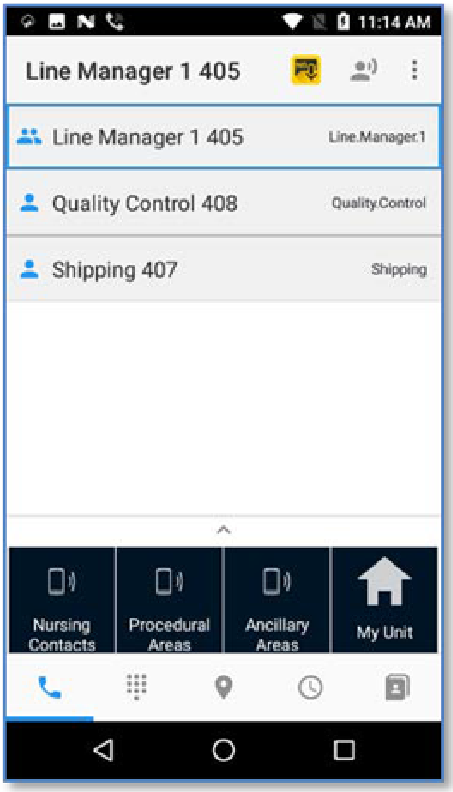
5. In the WFC Profile Client, select all roles listed to activate the provisioning of extensions for all the roles. A check mark indicates that a role has been selected.



6. Click **Apply**.

   Telephony Manager provisions the available extensions for those departments in the WFC Profile Client device.

   As shown, WFC Profile Client is showing all configured Roles for the User as defined in the User Profile.



7. To switch among roles, select the back arrow to navigate to the **Profile Client Role Selection** screen.

Important Notes About Verifying Correct End-to-End Configuration

The extensions provisioned from Telephony Manager are determined by the following:

- The Roles presented to the User, which are defined in the User Profile
- The Role(s) that are selected by the user
- If the User selects only one role, Telephony Manager finds the extension attributes associated with that Role and provisions that information to the mobile device.
- If the User selects multiple roles, Telephony Manager provisions the extension attributes to the mobile device.
- At Rule Evaluation Time, all rules are evaluated.

NOTE: If a user is defined in multiple Rule Sets, all the Rule Sets where the user is defined are applied simultaneously to the user. It is important to make sure that this is the desired result for the user. Otherwise, it might be necessary to adjust the Rule Set definitions to get the desired result.

Telephony Management

This chapter describes how to manage the following:

- Extensions (viewing and refreshing)
- Extension Import Management
- Other Telephony Management Options

When you use the Telephony Management links in Profile Manager, they take you to the **Extension Manager Web Portal login** screen, which lets you manage these Telephony options directly in **Extension Manager Web Portal**.

Extensions

This section describes how to:

- view extensions.
- refresh extensions.

View Extensions

Prerequisite

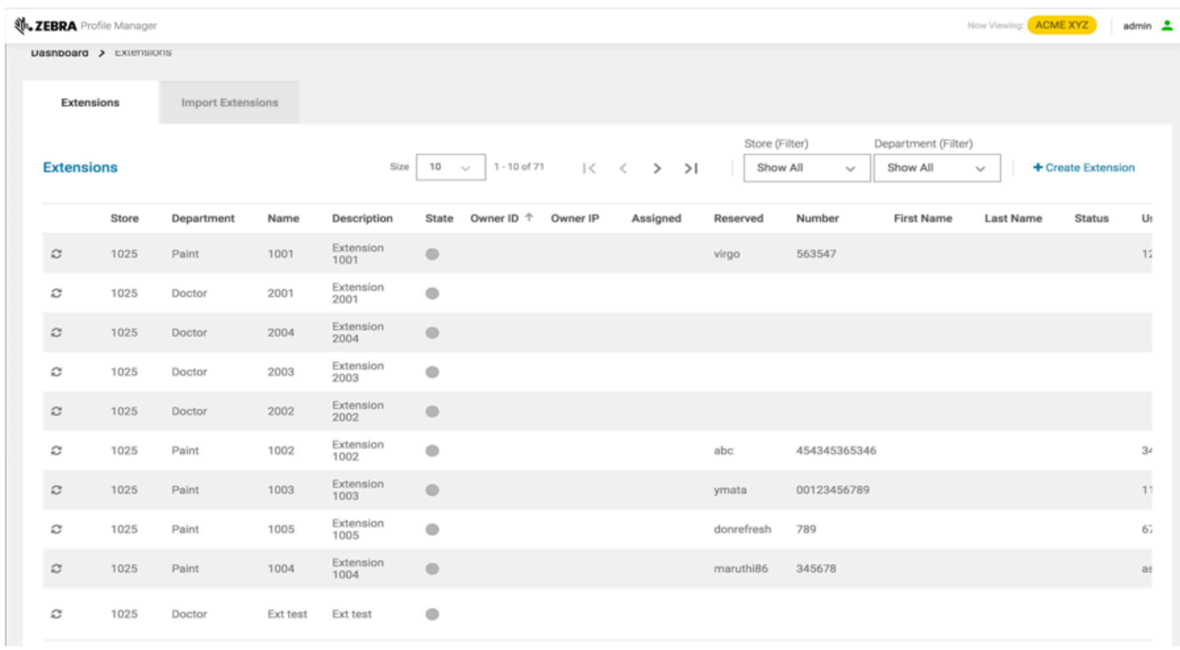
Your privileges must permit you to view extensions.

To view extensions:

- From the dashboard, click **Extensions**.

  The **Extensions** screen appears.

Figure 69 Extensions Screen



Refresh Extensions

Your privileges must permit you to refresh extensions.

1. From the dashboard, click **Extensions**.

   The **Extensions** screen appears.

2. Click  for the extension to refresh.

Extension Import Management

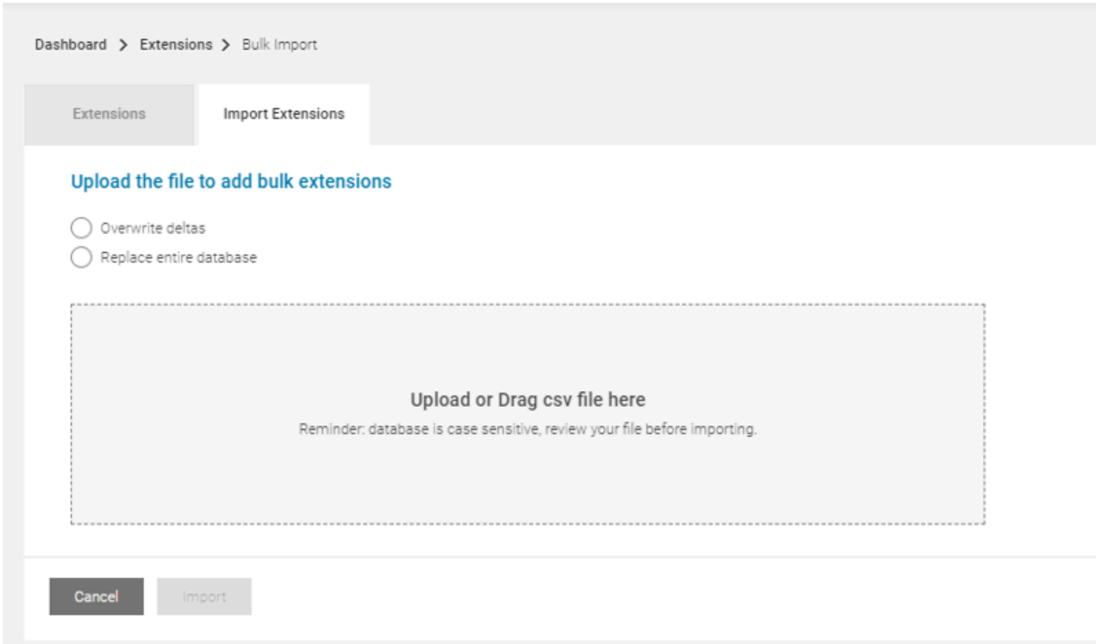
- Your privileges must permit you to bulk import extensions.
- The import file must be CSV format.
- The extensions to be synchronized must already exist in the database.
- The Profile Manager database is case sensitive. Review the CSV file before importing.

1. From the dashboard, click **Extensions**.

   The **Extensions** screen appears.

2. Click the **Import Extensions** tab.

   The **Import Extensions** screen appears.



3. Select an option:
   - To synchronize the database updates from the import file, select **Overwrite deltas**.
   - To overwrite the existing database, select Replace entire database.
4. To upload a file, click **Upload** or Drag csv file here and browse to select the CSV file. Otherwise, click and drag the CSV file from its folder to the box.
5. Follow screen prompts to complete the import.

Other Telephony Management Options

The following telephony options are also available to be managed:

- History (this option is view only)
- Store IPs
- Contacts
- Stores
- Departments
- PBXs
- Configurations.

NOTE: When you use the Telephony Management links in Profile Manager, they take you to the **Extension Manager Web Portal Login** screen, which lets you manage these Telephony options directly in Extension Manager Web Portal.

Profile Manager Licenses

The WFC Profile Manager Administrator has the ability to view the license information for the Administrator user.

This chapter describes following:

- View Profile Manager Application Licenses
- Update Profile Manager Application Licenses

Profile Manager Device Licenses

If your site is set up for device licenses to allow users to access the system, then the device licenses for the WFC Profile Client application are shared among a larger number of devices. When you log into a device for WFC Profile Client, a license is provided to the device from a license server.

The system administrator must manually control which devices are enabled to be provided the device licenses.

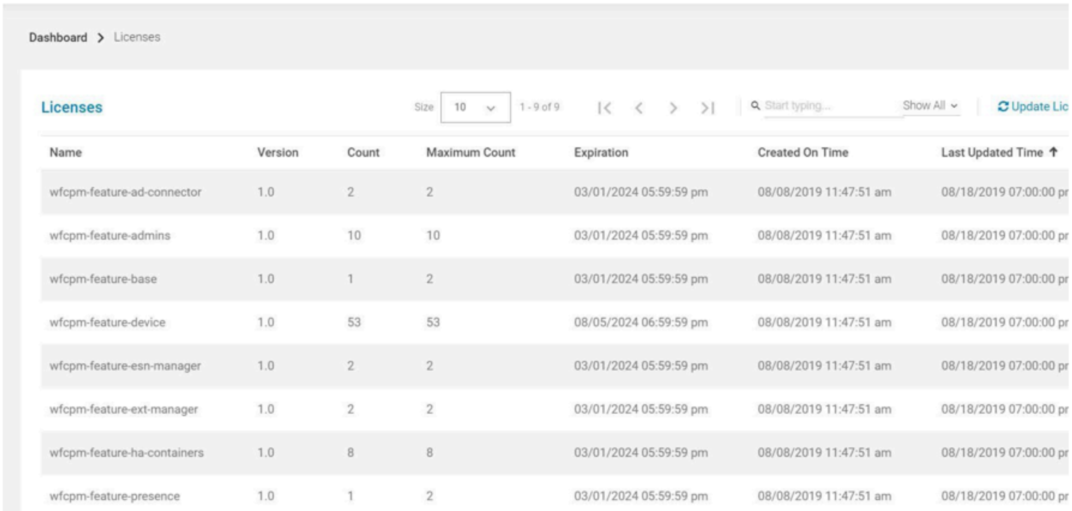
View Application Licenses

Your privileges must permit you to view application licenses.

From the bottom of the dashboard, click **License**.

The **Licenses** screen appears.

Figure 70 Licenses Screen



Update Application Licenses

Your privileges must permit you to update application licenses.

1. From the bottom of the dashboard, click **License**.

   The **Licenses** screen appears.

2. In the **Licenses** screen, select **+Update Licenses**.

   The **Licenses** screen is updated with the latest information.

Intents and Actions

This document describes the installation and configuration capabilities of the Profile Client. The capabilities described in the document are based on version 2.0.20207 or greater

Profile Manager Client Configuration File Elements

needs to configure the required Profile Manager connectivity parameters manually through the client UI.

Sample WFCDFSConfig.json file:

```
{
"customer_id": "3001",
"sfs_url": "https://<PFM_server.com>",
"site_id": 5000,
"log_level": "debug",
"confirm_role":false,
"power_connected_logout":true,
"log_file": true,
"dnd_switch":true,
"config_settings":0,
"secret_key": "my_secret_key",
"login_page_delay": 500,
"key_user_name": "userNameInput",
"key_user_pwd": "passwordInput",
"key_submit": "submitButton",
"key_domain": "pttpro"
}
```

See JSON Configuration Variables for the WFC Profile Client Table for descriptions of JSON elements.

Table 4 JSON Configuration Variables for the WFC Profile Client

Profile Client json Config Variables Supported in version 2.0.20207+				
Label	**Description**	**Type**	**Default**	**Config via UI?**
customer_id	Maps to the Profile Manager's Tenant ID provided by the system administrator.	string	<null>	Yes
sfs_url	The FQDN of the Profile Manager secure web socket connection provided by the system administrator.	string	<null>	Yes
log_level	Log options are: Info (default), Debug, Warning, Error, and Verbose.	string		Yes
log_file	Enable application to record logs and store on the sdcard of device. Logs are available at / sdcard/DFS/	Boolean		Yes
confirm_role	When set to True, once the roles are selected the user is prompted to confirm the selections.	Boolean		Yes
site_id	Is the value correlated in Extension Manager's Store ID value. Upon match, it aligns the group of extensions available to the User based on the Roles configured.	string	<null>	Yes
dnd_switch	Allows user to display/remove the dnd_switch in Profile Client.	Boolean	TRUE	No
config_settings	Configures the user's visibility of the Settings Menu where: 0 = (default) Allows the user to access and edit the client's settings 1 = Show the Client's setting but to not allow modification 2 = Hides the Settings Menu.	integer	0	No
disable_signout_btn_bluefletch	Configures whether the Signout button is visible when the auth type is bluefletch. false = (default) Signout button is visible true = Hides the Signout button	Boolean	FALSE	No

Table 4 JSON Configuration Variables for the WFC Profile Client (Continued)

Profile Client json Config Variables Supported in version 2.0.20207+				
Label	**Description**	**Type**	**Default**	**Config via UI?**
supress_network_disconnect_bar	Configures whether the network disconnect bar is visible at the bottom of the screen during a network disconnect. true = (default) Network disconnect bottom bar is not visible. false = Network disconnect bottom bar is visible.	Boolean	TRUE	No
power_connected_logout	When enabled, the Profile Client User is signed out, when device is put in cradle for charging	Boolean	FALSE	Yes
secret_key	Key used to decrypt the login blob delivered from the Launcher app via intent to the Profile Client.	string	<null>	No
key_user_name	Used in conjunction with 3rd Party Launcher apps. This tag identifies the Username ID field and allows input on the presented login web page. Sample html: <input type="text" name="username" id="username" class="textinput" value="">	string	<null>	No
key_user_pwd	Used in conjunction with 3rd Party Launcher apps. This tag identifies the Password ID field and provides input on the presented login web page. Sample html <input type="password" name="password" id="password" class="textinput" autocomplete="off">.	string	<null>	No
key_submit	Used in conjunction with 3rd Party Launcher apps. This tag identifies the Submit ID field for acceptance of credentials on the presented login web page. Sample.html: <input type=" submitButton" value="Login" id="submit" class="submit" tabindex="4" role="button" >	string	<null>	No

Table 4 JSON Configuration Variables for the WFC Profile Client (Continued)

Profile Client json Config Variables Supported in version 2.0.20207+				
Label	**Description**	**Type**	**Default**	**Config via UI?**
key_domain	Used in conjunction with 3rd Party Launcher apps. This tag provides the insertion of a Domain name string to add before username.The slash separators are automatically added. IE: "pttpro" becomes "pttpro\\<username>"	string	<null>	No
username_layout	Used to configure the user name field of the customized EKB layout in EC30 devices. May require change if the layout encryption file uses different name in future.	string	usernamela yout	No
password_layout	Used to configure the password field of the customized EKB layout in EC30 devices. May require change if the layout encryption file uses different name in future.	string	passwordla yout	No

Support for Third-Party Launchers

In the varied environments where the Profile Manager solution is installed, there may be an existing launcher application running on the device. This provides the customer with the ability to keep their existing launcher for the user sign-on process and then pass the user information to the Profile Client to authenticate with the Profile Manager.

The four tags used in this environment are:

- Key_user_name
- Key_user_pwd
- Key_submit
- Key_domain

The values entered in these tags identify the input fields to automate the login process. As an illustration, shown below is the actual html of a sample login screen:

```
<div class="input-row">
  <table>
    <tr>
```

```
      <td>
        <p> <label style="margin-top:-14px" for="username">Login ID:</
label></p>
      </td>
      <td>
         <span class="ctrl">
             <input type="text" name="username" id="username"
 class="textinput" value=""/>
         </span>
      </td>
    </tr>
  </table>
</div>
<div class="input-row">
  <table>
     <tr>
       <td>
         <p> <label style="margin-top:-14px" for="password">Password:</
label></p>
      </td>
      <td>
       <span class="ctrl">
    <input type="password" name="password" id="password"
 class="textinput"autocomplete="off"/>
      </span>
    </td>
  </tr>
</table>
</div>
<div class="button-row">
 <span class="ctrl">
    <input type="submit" value="Login" id="submit" class="formButton"
onclick="this.disabled=true;document.body.style.cursor = 'wait';
this.className='formButton-disabled';form.submit();return false;"/>
```

The highlighted fields in the HTML example are the content of the login screen sent to the mobile device from the customer's authentication system. Once authenticated, the Profile Client receives the credentials through an intent from the third-party launcher application and passes the credentials to the appropriate tagged fields. The Profile Client receives the input from the launcher by intent, and then provides the input to the User ID = id="username", and Password = id="password" entries. These fields are sent back to the authorizing system with id="submit".

By correctly identifying the html entry ID Fields, the third-party application can pass the credentials to the Profile Client to log in with the credentials passed to the Client.

In this example, the three tags are populated with:

- Key_user_name: "username"
- Key_user_pwd: "password"
- Key_submit: "submit"

NOTE: The domain prefix is not shown in this example.

Access Tokens

Third-party launchers such as BlueFetch can send an access token (user_accesscode), refresh token (refresh_token) and the refresh token expiration time (refresh_token_expiration) in seconds. Access tokens take precedence over the user name and password fields.

When the refresh_token_expiration time elapses, the user is signed out. Third-party launchers must send a new intent with the refreshed user_accesscode, refresh_token and refresh_token_expiration before the expiration time of the previous toke elapses.

ADB Supported Commands

Install the PFM Client

- Can use MX (this gives the APK all permissions requested)
- Side load and manual startup requires permissions acknowledgment:

```
adb install -r -g C:\WFCProfileClient-geminiRelease-2.0.19306.26150066.apk
Where:
-g accepts all permissions listed in the app manifest
-r Reinstall the existing app keeping its data
```

Handling the PFM Configuration File

The Config.json file, detailed below, can be loaded onto the device in any meaningful folder and have any valid.json file name.

If the filename is not specified, the client looks for the default file ‘WFCDFSConfig.json’ in the /sdcard/ folder.

When the Client is instructed to ingest the configuration upon successful read, the file is deleted. If there are errors (file not found, incorrect syntax, invalid parameters, etc.), the file remains, and errors are posted in Logcat.

```
adb push ".\WFCDFSConfig.json" /sdcard/
```

Starting the Profile Client

- The activity is started when the client starts. No configuration is ingested.

```
adb shell am start -n com.zebra.dfs/.LoginActivity
```

NOTE: If this intent is delivered to a currently running client, it makes the client to restart.

Reconfiguring a Running Client

- If the client is running and there is a required configuration change, an updated .json file must be delivered to the device, and an intent must be sent instructing the client to ingest the new configuration.

```
adb shell am start -a com.zebra.dfs.ACTION_NEW_CONFIG --es profile_uri
/sdcard/WFCDFSConfig.json
```

a) Once the config file is ingested, the .json file is deleted from the folder.

b) If the client is running, the user is logged out of the Zebra PTT Pro and Voice applications returning them to the PFM Sign-In Screen.

c) If the JSON filename is at /sdcard/WFCDFSconfig.json, the extra string parameter (--es...) is not required.

Start/Restart the Client with a New Configuration

- If a new .json config file has been delivered to the device and the default filename is used, the following intent reads the config and restarts the client with the new parameters. The user is logged out of the Zebra PTT Pro and Voice applications returning them to the PFM Sign-In Screen.

```
adb shell am start -a "com.zebra.dfs.ACTION_NEW_CONFIG"
```

- The following command includes the syntax for including a specific config file name:

```
adb shell am start -a "com.zebra.dfs.ACTION_NEW_CONFIG" --es profile_uri
/sdcard/WFCDFSConfig.json
```

NOTE: The broadcast function for Action_New_Config has been deprecated starting in version 2.0.20207. Start should now be used going forward.

- Useful for the Administrator, this is used by the administrator to prepare the device for runtime by ingesting the configuration and then logging out the user. To log out a currently logged in user:

```
adb shell am broadcast -a "com.zebra.dfs.ACTION_SERVICE_LOGOUT" --es Exit
 stop
```

Sending Credentials from a Third Party Launcher

- When using a Third Party launcher application, the application that captures the user’s credentials can pass these values to the Profile Client for including Profile Manager in the log-in process. The adb command to do this is:

```
adb shell am start -a “com.zebra.dfs.ACTION_NEW_CONFIG” --es user_name
 123456 --esuser_pwd mypassword
```

- When login credentials are captured by the Launcher app, they are passed to the Profile Client by broadcast intent:

```
adb shell am broadcast -a “com.zebra.dfs.ACTION_LOGIN” --es config_profile
 {}
```

Bulk Import Device Users

Use Bulk Import to import users from Active Directory into the Profile Manager and WFC PTT Pro.

The Profile Manager Provisioning Guide describes how to import users through bulk import, the AD Connector, or a flat file using Google Cloud Platform and Secure FTP. The Profile Manager Provisioning Guide provides detailed information regarding the architecture of the various methods of importing multiple users into the Profile Manager and WFC PTT Pro, where applicable. In addition, the guide describes the process for each import method, the associated Attribute Transformations, and the information required from the customer to enable each method.

This chapter covers the following topics:

- Description
- Assumptions
- Import Process

Description

Within the Administrator Portal in Profile Manager, the ability to import users into Profile Manager currently exists. This feature has been expanded to also provision the users into both Profile Manager and PTT Pro for the desired Customer.

In a fully integrated solution when Active Directory supports both, Profile Manager and PTT Pro, the Active Directory connection provides three fundamental functions:

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 and are added to and deleted from Active Directory, this connection to Profile Manager and PTT Pro automatically modifies the User databases reflecting the changes.

3. Attribute Transformations

- Various elements in Active Directory can be evaluated to determine the Profile configuration received by the Users.

  The Import Device Users feature is provided for Customers:

- Without integration into Active Directory for User provisioning, and provides a simple method to populate user information into the Profile Manager and PTT Pro Systems.
- Use of this feature for trials and implementations before the investment is made to integrate the Workforce Connection Solution with the Enterprise Active Directory system.

Assumptions

The following list identifies the dependencies and assumptions of the environment.

- The CSV file contains fields for both Profile Manager and PTT Pro. If both systems are being populated, then the .csv must be populated with data for both services.
- Populating data into PTT Pro import may take longer time because of the complex record interaction update into PTT Pro server, group creation, etc. If slow, import times are experienced, consider breaking the csv into multiple files.
- Creation of Profile Manager Users and the User’s Role assignment requires the Roles and Role Levels to exist in Profile Manager prior to the .csv import.
- If Role Level is , the .csv file does not include the Role information. If both exist, the Role Level is used for the user and the Roles information is discarded.
- The User import creates the PTT Pro Departments and Talk Groups defined in the .csv.
- If importing into an existing PTT Pro structure using the **reset entire database** option, and the Departments or Talk Groups information has changed, the existing elements remains intact.
- The data entry restrictions of shared data elements, like User Name, between Profile Manager and PTT Pro may be different. They must, therefore, meet the lowest common denominator for entry. This is detailed in the table that follows.

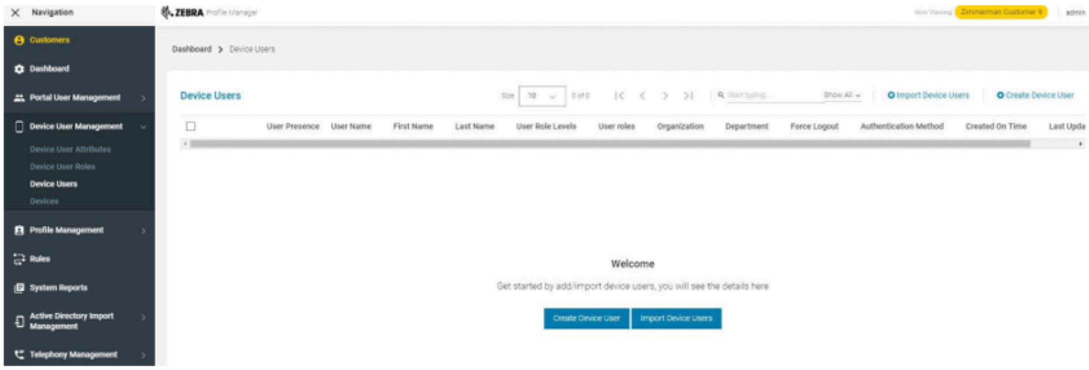
Import Process

To get started, navigate to Profile Manager and download a copy of the build user import template.

1. From the Dashboard, click **Device User Management**, and then **Device Users**.

   The **Device Users** screen appears.

   Figure 71 Device Users Screen



2. Click the **Import Device Users** link in the right pane.
3. The CSV template can be downloaded by the link shown in the **Bulk Import User** screen.
4. Once the template is downloaded, populate with the desired information.

   Figure 72 Bulk Import Users Screen

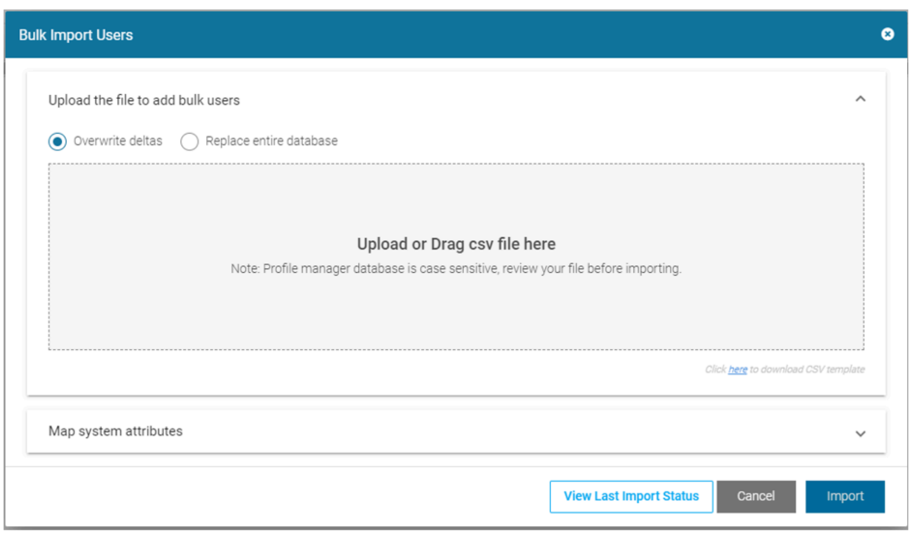


   Figure 73 Sample Populated CSV File Template

User Name	Password	First Name	Last Name	User Role Levels	User roles	Organization	Department	Force Logout	Authentication Method	TelePHONE	GroupUserTemplate	OauthName
User.A1	Bicycle9999!	Jean-Louise	John Samuel	Hardware		NALA	Paris	TRUE	BASIC		standard	111111
User.A2	Bicycle9999!	Frank	johnson1	Services		EMEA	Rome	TRUE	OAUTH2		standard	222222
User.A3	Bicycle9999!	Lloyd	smith2smith	Leadership		APAC	Oslo	TRUE	OAUTH2		standard	333333

   a) As stated above, there are common data columns used both by Profile Manager and by PTT Pro. Details of each element’s use is listed in Table 5 User Import File Column Head Descriptions on page 112.

   b) The Elements required to populate the template are:

Table 5 User Import File Column Head Descriptions

Name	Server Usage			Profile Manager Usage	PTT Pro Usage	Comments
	PFM	Pro	Req'd			
User Name	*	*	*	The User Name field is required. The field accepts from 1 to 255 alphanumeric and special characters.	The User Login field is required. The field accepts from 1 to 24 alphanumeric characters, a dash, and a period.	Determine the User name (userID) that meets the requirements in both systems. If the user name contains a domain name like user2@pttpro or pttpro \user2, the domain name is stripped and the element is set to login name.
Password	*			Password should contain minimum 10 characters and maximum 128 characters. Password must meet at least 3 out of the following 4 complexity rules, (at least 1 lowercase, uppercase, digit & special character). not more than 2 identical characters in a row.	<Not used>	
First Name	*	*	*	The field accepts from 1 to 255 alphanumeric characters and special characters.	Field accepts from 1 to 30 alphanumeric characters and special characters.	Determine the User's first name that meets the requirements in both systems.
Last Name	*	*	*	The field accepts from 1 to 255 alphanumeric characters and special characters.	The field accepts from 1 to 30 alphanumeric characters and special characters.	Determine the User's last name that meets the requirements in both systems.
User Role Levels	*		*	Specify the Role level used in hierarchical Role selection.	<Not used>	If both Role Level and Role columns are populated for a User, the Role Level is used and the Role column is ignored. Specify only One Role Level. Role Level is case sensitive. When the level is created, the same case must be used in the csv import.

Table 5 User Import File Column Head Descriptions (Continued)

Name	Server Usage			Profile Manager Usage	PTT Pro Usage	Comments
	PFM	Pro	Req'd			
User Roles	*		*	Select User Role from the drop-down list. User Roles must be established prior to import.	<Not used>	If Role Level is not specified, then this column is a listing of Roles for the user. One or more Roles must be defined and separated by commas. Roles must exist before the import is executed.
Organization	*			Field describing the User's organization. The field accepts from 1 to 255 alphanumeric characters and special characters.	<Not used>	
Department	*	*	*	The field describes the User's Department. The field accepts from 1 to 255 alphanumeric characters and special characters.	The field describes the User's Department. The field accepts from 1 to 25 alphanumeric characters and special Characters. Entry specifically identifies which Department to create the user.	For PFM this is simply a description field. In Pro, this field must exactly match an existing Department container for the given customer.
Force Logout	*			When enabled if the user logs in on another device without logging off of the first device, the system automatically logs off the first device.	<Not used>	
Authentication Method	*		*	Selection options are BASIC or OAUTH2. Basic causes the user's credentials to be validated from the User name and Password entered above. OAUTH2 causes the user's credentials to be prompted for and validated against the AD-connected system.	<Not used>	The WFC PTT Pro server does support Oauth to provide a shared device model, but there is no actual Authentication Method switch per user. The entry must be made in capital letters -- BASIC or OAUTH2

Table 5 User Import File Column Head Descriptions (Continued)

Name	Server Usage			Profile Manager Usage	PTT Pro Usage	Comments
	PFM	Pro	Req'd			
PBX Extension				Create the extension in the extension manager.	<Not used>	This functionality is not supported in the CSV import. Available only at the time of creating a user, updating UI, and importing the active directory.
Telephone		*		<Not used>	User's phone number if SMS activation is planned. This is not a required field.	
Group User Template		*	*	<Not used>	Defines the Talk Group Template to use. Four possible entries are admin, sme, associate, or standard.	
FeatureKeysTemplate		*	*	<Not used>	Defines the Feature Key template to be mapped to the user. This template is created in PTT Pro at the customer level before importing the user.	
ClientSettings Template		*	*	<Not used>	Defines the Feature Key template to be mapped with the user. This template is created in PTT Pro at the customer level before importing the user.	
OauthName		*	*	<Not used>	During Oauth validation the response from AD this return string determines the User's profile.	

5. Once the import.csv table is built, it may be imported via the browser or the API interface.

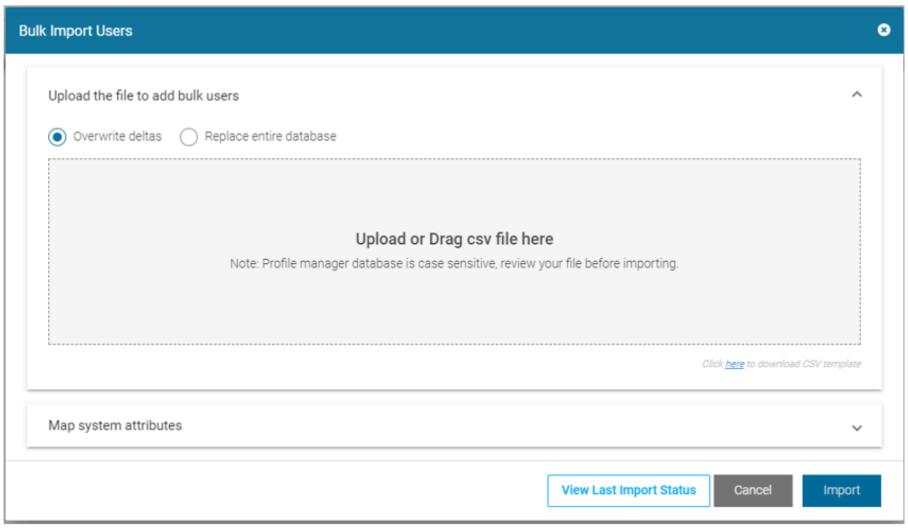
6. To import through the browser, return to the Device User page and click Import.
7. Navigate to or drag the .csv into the window to import it.

   There is a choice to Overwrite the existing records or to Replace the entire database. Replacing deletes all user records from the system, so be mindful of this operation, if selected.

   a) **Overwrite** leaves the user records in place, making adjustments to any existing records as specified in the .csv. If there are new records, they are added.

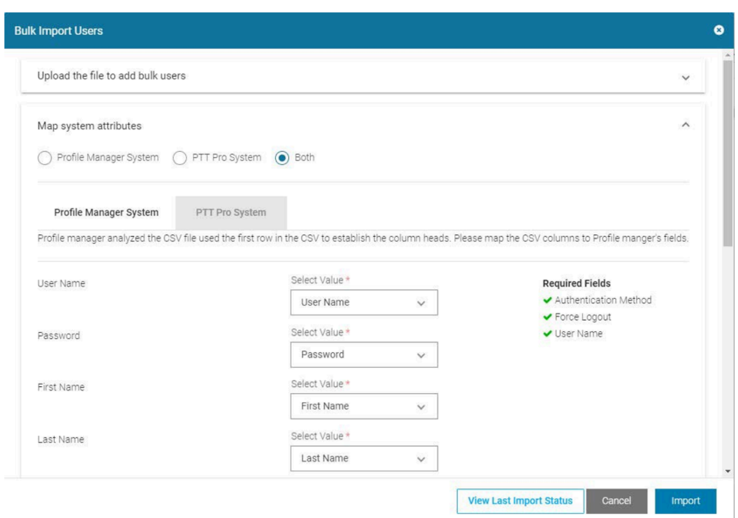
   b) **Replace Entire Database** initializes all User records, and then imports the records into the Profile Manager and PTT Pro server as specified in the .csv. In PTT Pro, all existing Users are deleted for the Customer, but the Departments remain intact.

   Figure 74 Import via Browser



8. In **Map System Attributes**, select the desired button to add users to **Profile Manager System**, **PTT Pro System**, or **Both** servers.

Figure 75 Map System Attributes Screen



9. In the lower section of the screen, click on the **Profile Manager System** or **PTT Pro System** tabs to map the .csv elements to various data fields in each of the servers.

The mapping for all columns in the .csv must be assigned to server target data elements, or set to be **Ignored**.

10. Once the attribute mapping is complete, click **Import** to begin the job.

When completed, the system returns to the **Device User** screen.

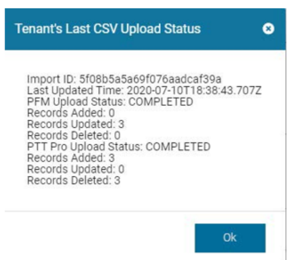
Figure 76 is a sample of an import file and the resulting status.

Figure 76 Import File

User Name	Password	First Name	Last Name	User Role	User roles	Organizati	Departmer	Force Logc	Authentica	TelePHON	GroupUser	OauthName
User.A1	Bicycle999	Jean-Louis	John Samu	Hardware	floor_swe	NALA	Paris	TRUE	BASIC		standard	111111
User.A2	Bicycle999	Frank	johnson1	Services	floor_swe	EMEA	Rome	TRUE	OAUTH2		standard	222222
User.A3	Bicycle999	Lloyd	smith2smi	Leadershir	trash_haul	APAC	Oslo	TRUE	OAUTH2		standard	333333

11. To check the job status, click **Import Device Users**, then select **View Last Import Status**.

Figure 77 View Last Import Status Screen



In these three User examples, the import used the **Reset** the entire User Database option and was imported into both **Profile Manager (PFM)** and PTT Pro. The Profile Manager had no existing user records, and there were three existing User records in PTT Pro prior to the import.

12. Verify all records were added as expected to Profile Manager and PTT Pro servers.

Multiple Role Values from Attributes

Description

Previous versions of Profile Manager supported only one Role assignment that could be obtained from an Active Directory attribute. Now, Role assignment has been expanded and Profile Manager has the capability to read an AD attribute with multiple roles and proliferate it to the UI of the mobile device.

Any Active Directory attribute can be selected. The attribute must have the ability to support a string of characters delimited with the following supported characters: semi colon, comma, #, @, ~, ^, space, *, !, and $.

Support of this feature provides administrative flexibility to the dynamic environment of the remote site. User configurations may be provisioned into the Profile Manager Solution from the Active Directory import job on a scheduled basis, providing flexible Role Selections to the device user to meet business demands

Assumptions

- Only one kind of delimiter is used in the attribute values.
- Any of the delimiters used is not present as part of a role name.
- Number of roles present in an attribute value depends on the limitation of the AD attribute length.
- AD System Attribute Transformation configurations have been properly configured and verified in Profile Manager.
- All established Roles defined in the AD Attribute have also been configured in Profile Manager.

Configuration Process

Overview

This document describes various entities and elements within a successful configuration. The configuration process is:

- Identify an AD Attribute suitable for Role definition.
- Identify all AD attributes those are imported from AD into Profile Manager.
- Configure Profile Manager for the import job Transformation – for both Profile Manager and PTT Pro, if applicable.
- Create a Job in Profile Manager to import (provision) users from AD into Profile Manager.
- Review Job Logs and results.

Identification of AD Attributes

1. Using an Active Directory browser, find and examine a specific User. Roles are commonly descriptive words, so select an attribute that supports alphanumeric input.

   In this case, we are using 'extensionAttribute7' to specify the Wire, Screws, and Nails Roles.

   Figure 78 Role and Attribute Example

dSCorePropagationData	16010101000000.0Z
extensionAttribute5	TRUE
extensionAttribute7	wire,screws,nails
givenName	zman1
lastLogoff	0
lastLogon	132398374406244000
lastLogonTimestamp	132405114529723000
logonCount	22

NOTE: Case sensitivity must be observed when generating the attribute Roles, described later in this document.

2. Next, review the attributes for the user.

   In this view, all populated attributes move to the top of the list and are alphabetized. Review to become familiar with what is populated.

Table 6 Attributes

Attribute Type	Value
cn	zman1
instanceType	4
nTSecurityDescriptor	
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=PTTPRO,DC=ZEBRA
objectClass	organizationalPerson
objectClass	person

Table 6 Attributes (Continued)

Attribute Type	Value
objectClass	top
objectClass	user
accountExpires	9223372036854770000
badPasswordTime	132397473873874000
badPwdCount	0
businessCategory	OAUTH2
codePage	0
company	Zebra
countryCode	0
department	Minnetonka
description	worker
displayName	zman1
distinguishedName	CN=zman1,OU=Users,OU=zebra,DC=PTTPRO,DC=ZEBRA
dSCorePropagationData	16010101000000.0Z
extensionAttribute5	TRUE
extensionAttribute7	wire,screws,nails
givenName	zman1
lastLogoff	0
lastLogon	132398374406244000
lastLogonTimestamp	132405114529723000
logonCount	22
memberOf	CN=Imprivata,DC=PTTPRO,DC=ZEBRA
name	zman1
objectGUID	(non string data)
objectSid	(non string data)
physicalDeliveryOfficeName	Eden Prairie
primaryGroupID	513
pwdLastSet	132393993097741000
sAMAccountName	zman1
sAMAccountType	805306368
sn	Zimmerman1
telephoneNumber	9525551212
title	Associate

Table 6 Attributes (Continued)

Attribute Type	Value
userAccountControl	66048
userPrincipalName	zman1@PTTPRO.ZEBRA
uSNChanged	4206643
uSNCreated	4173760
whenChanged	20200729155052.0Z
whenCreated	20200716185509.0Z
aCSPolicyName	
adminCount	
adminDescription	
adminDisplayName	

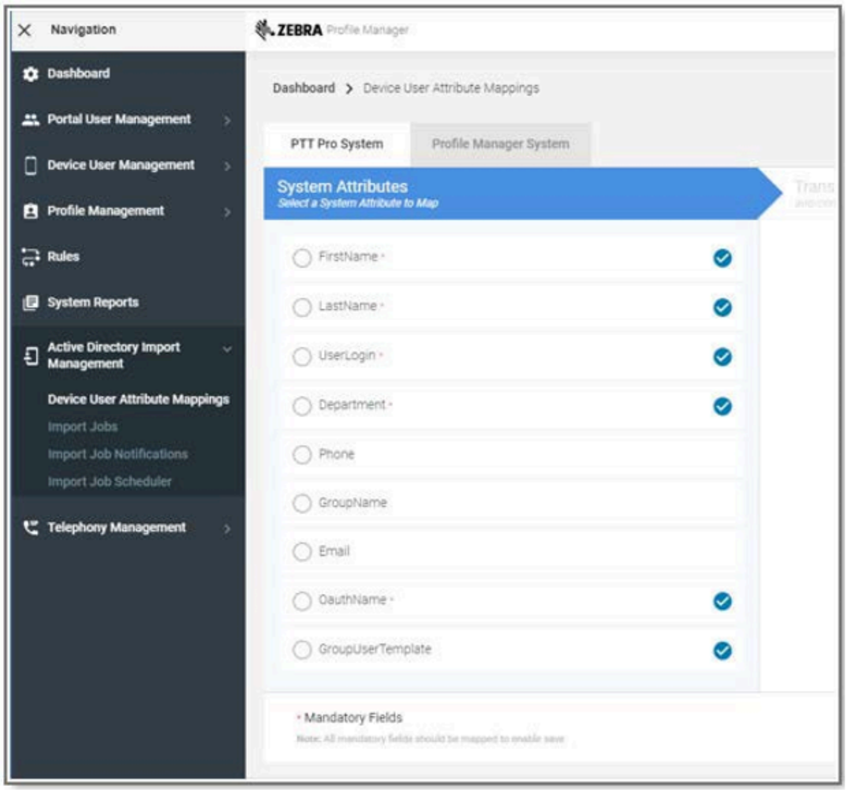
Import Attribute Transformations

Once familiar with the populated attributes in Profile Manager, navigate to the Active Directory Import Management tab and select Device User Attribute Mappings as shown in Figure 80-Device User Attribute Mappings.

1. In the center pane, both PTT Pro System and Profile Manager Systems are shown. Some of these existing elements are required, indicated by the asterisk. These are the data elements in the PTT Pro

and Profile Manager (PFM) solutions that need to be populated when the AD import job is executed, and the transformation is completed.

Figure 79 Device User Attribute Mappings



2. The table below shows each of the required elements in the PTT Pro System and Profile Manager Systems.

   The idea is to identify an AD attribute for each of the required PTT Pro and Profile Manager data elements. The data elements used in this example work for this test environment. AD Attributes used in production can vary dramatically.

Table 7 Profile Manager Attribute Transformations Mapping

PTT Pro		
Element	**AD Attribute Name**	**Value**
First Name		
Last Name		
User Login		
Department		
OAuthName		
Group User Template		
Profile Manager		

Table 7 Profile Manager Attribute Transformations Mapping (Continued)

PTT Pro		
Element	**AD Attribute Name**	**Value**
Element		
User Name		
First name		
Last Name		
User Role Levels		
User Roles		
Organization		
Department		
Force Logout		
Authentication Method		

In the AD snippet, as an example, the following AD Attributes are used.

Table 8 Profile Manager Attribute Transformations Mapping with AD Attribute Name

Profile Manager Attribute Transformations Mapping		
PTT Pro		
Element	**AD Attribute Name**	**Value**
First Name	givenname	
Last Name	sn	
User Login	displayname	
Department	department	
OAuthName	userprinciplename	
Group User Template	title	
Profile Manager		
Element	AD Attribute Name	
User Name	displayname	
First name	givenname	
Last Name	sn	
User Role Levels	employeetype	
User Roles	extensionattribute7	
Organization	company	
Department	department	
Force Logout	extensionattribute5	

Table 8 Profile Manager Attribute Transformations Mapping with AD Attribute Name (Continued)

Profile Manager Attribute Transformations Mapping		
PTT Pro		
Element	**AD Attribute Name**	**Value**
Authentication Method	businesscategory	

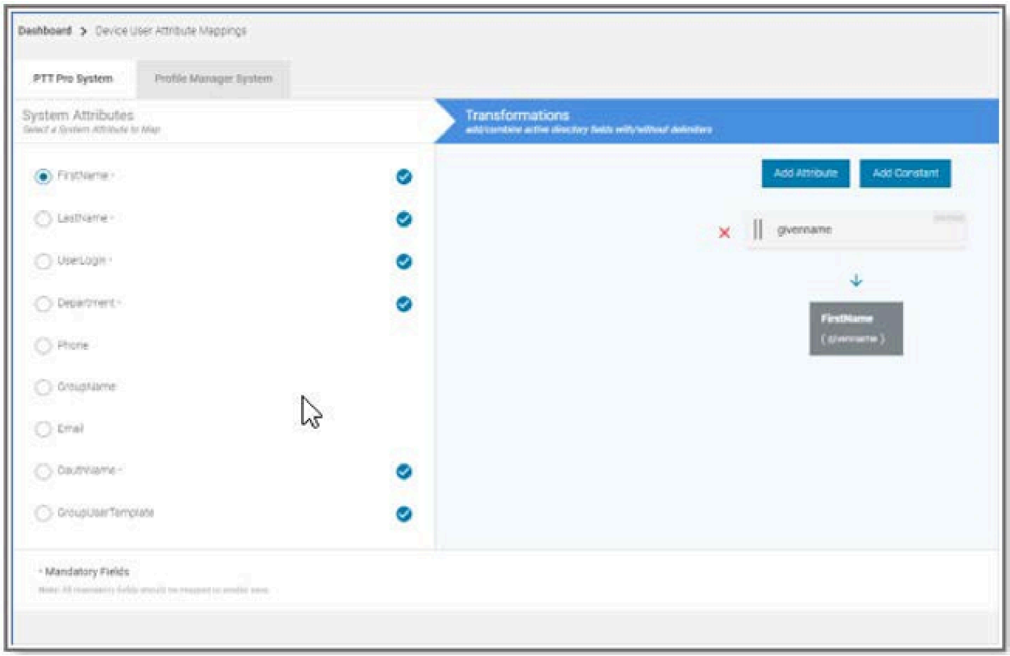
3. Then to complete the table, populate the AD attribute values which are relevant to the Profile Manager and PTT Pro transformation.

Table 9 Profile Manager Attribute Transformations Mapping with Values

Profile Manager Attribute Mapping		
PTT Pro		
Element	**AD Attribute Name**	**Value**
First Name	givenname	zman1, 2, 3
Last Name	sn	Zimmerman1,2,3
User Login	displayname	zman1, 2, 3
Department	department	Minnetonka
OAuthName	userprincipleName	zman1@PTTPRO.ZEBRA
Group User Template	title	Associate
Profile Manager		
Element	AD Attribute Name	Value
User Name	displayname	zman1, 2, 3
First name	givenname	zman1, 2, 3
Last Name	sn	Zimmerman1,2,3
User Role Levels	employeetype	services
User Roles	extensionattribute7	wire,screws
Organization	company	Zebra
Department	department	Minnetonka
Force Logout	extensionattribute5	TRUE
Authentication Method	businesscategory	OAUTH2

4. Once the Attributes and values to use are determined, the Profile Manager server can be configured.

Figure 80 System Attributes Screen



5. For each System being populated, **PTT Pro System** and **Profile Manager System**, click each of the required fields.

   The Transformation field prompts for the selected attribute to be entered.

NOTE: The AD attribute is case sensitive. If the input attribute case does not match, the import job fails.

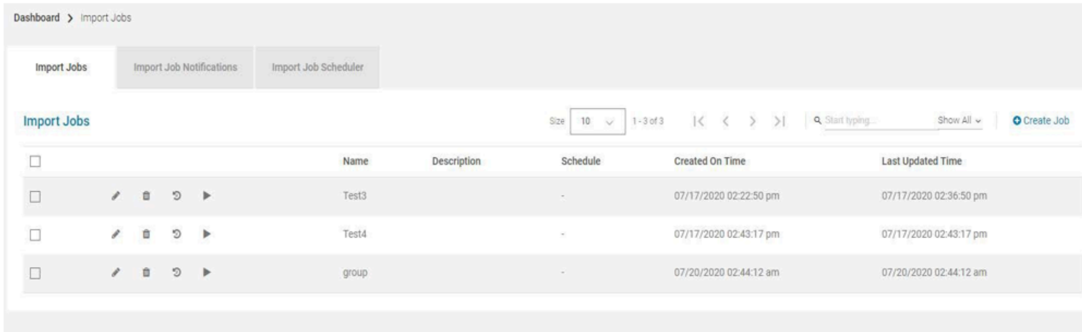
6. Complete the transformations for the required fields in the **PTT Pro System** and **Profile Manager System** sections.

Create an Import Job

After the transformations have been identified, creating an Import job adds (provision) the user to the PTT Pro and the Profile Manager solutions.

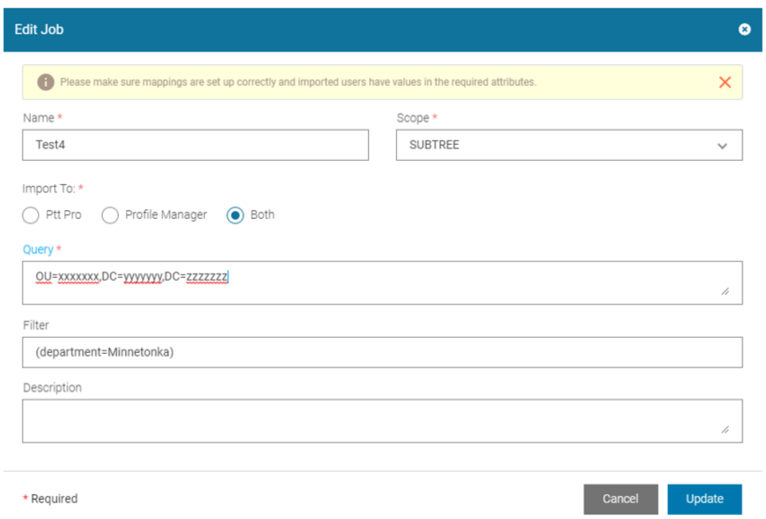
1. In the Profile Manager UI, navigate to **Active Directory Import Management** > **Import Jobs**.

Figure 81 Import Job Screen



2. Click **Create Job**.

Figure 82 Edit Job Screen



3. Create a job by entering the various fields required.
4. For the query, the Organization structure of AD must be entered correctly.

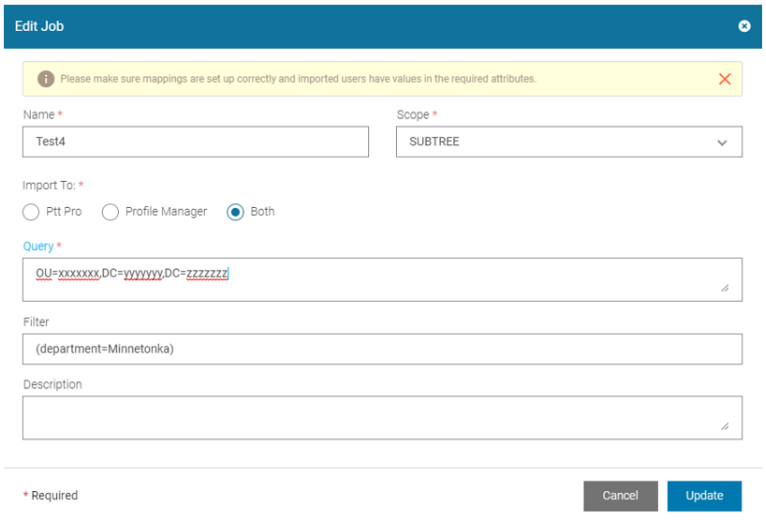
NOTE: There is an option to import into **PTT Pro**, **Profile Manager** or **Both**.

5. Once created, click the Arrow  to manually run the job.

   Once the job is validated and appropriately set, it may be set to run on a scheduled basis.

6. After the job is run, check the status of the job by clicking the  icon.

Figure 83 Import Job History



The Job status is shown and the status for each of the **Dispatchers**, **PTT Pro** and **Profile Manager**, can be viewed.

Figure 84 Profile Manager Dispatcher History Status

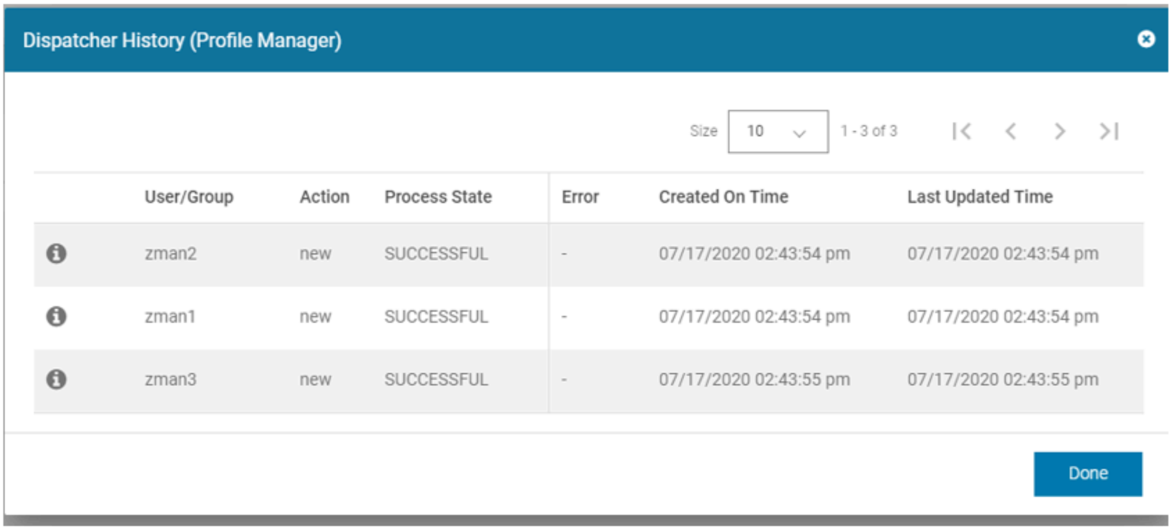
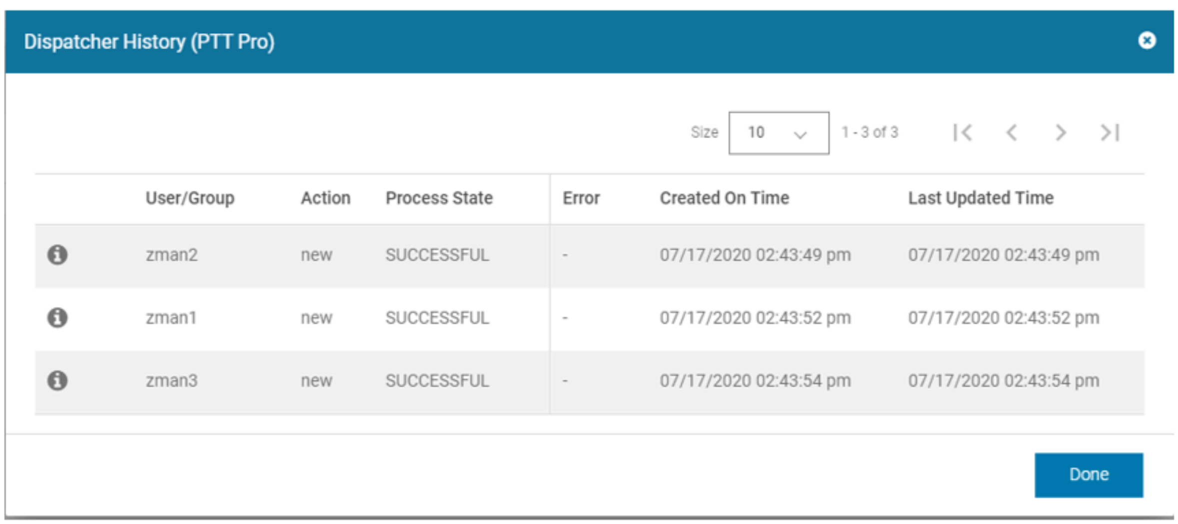


Figure 85 Dispatcher History (PTT Pro)



7. If there are import errors, click the icon to reveal the JSON detail for each of the relevant users.

Figure 86 JSON Detail Information

8. Scroll through the detail to evaluate.

9. Be very mindful of the AD attributes. As previously stated, the Attributes entered in the transformations must be the same case in the AD structure. Figure 92 shows attribute "extensionAttribute7" from the AD via an Active Directory Browser.

Figure 87 extensionAttribute7

employeeType	Services
extensionAttribute5	true
extensionAttribute7	wire,screws
givenName	zman1

10. Yet, the actual attribute delivered to Profile Manager from AD is shown in the JSON log detail in Figure 93

Figure 88 JSON Log


```
"department": "Minnetonka",
"useraccountcontrol": "66048",
"employeetype": "Services",
"extensionattribute7": "wire,screws",
"extensionattribute5": "true",
"cn": "zman2",
```


The attribute specified in Transformations should be "extensionattribute7" afailled if "extension Attribute7" is entered.

Researching Provisioning Errors

Provisioning Failure may also occur in different ways. For example, a Role Level Selection in Profile Manager supports only one Role Level statement. If the Attribute, employeeType in this case, has multiple level statements, Profile Manager rejects the import.

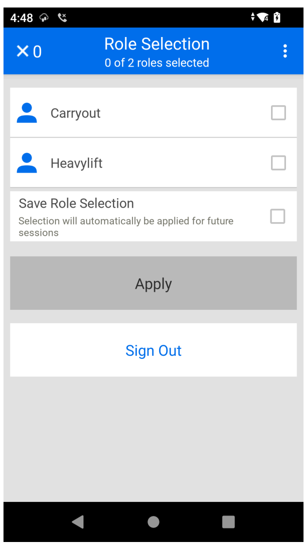
Review the error in Profile Manager, the Role Level Hardware was not available for this user.

```
},
"responseCode": 400,
"processState": "FAILURE",
"tenantId": "9",
"error": {
  "responseBody": "{\"httpErrorCode\":400,\"errorMessage\":\"Role Level :Hardware not found for User: zman1\"}",
  "statusText": "",
  "message": "Error while updating user.",
  "statusCode": 400
}
```


Successful Provisioning and Attribute Mapping

When the job is successful, the user is provisioned into Profile Manager with the specified roles. Then, during user sign-on, the roles assigned in AD are available to the user.

Figure 89 Role Selection



Role Level Selection

The Role Level Selection is a convenient way to assign a collection of roles under one Role Level Name. When a user is assigned a Role Level, the Profile Client interface presents them with the list of roles associated with the Role Level.

The value of this feature combines multiple roles in one Role Level Definition. Different Role Levels may combine commonly used roles to form different configuration assignments. For example, Role #1 may be found in Role Level Grouping A and Role Level Grouping B. This is additionally helpful when the customer's IDP database may have only one assigned attribute and wished to have multiple role selections derived from that single user attribute.

This chapter covers the following topics:

- Dependencies
- Applying the Role Level
- Device Operation

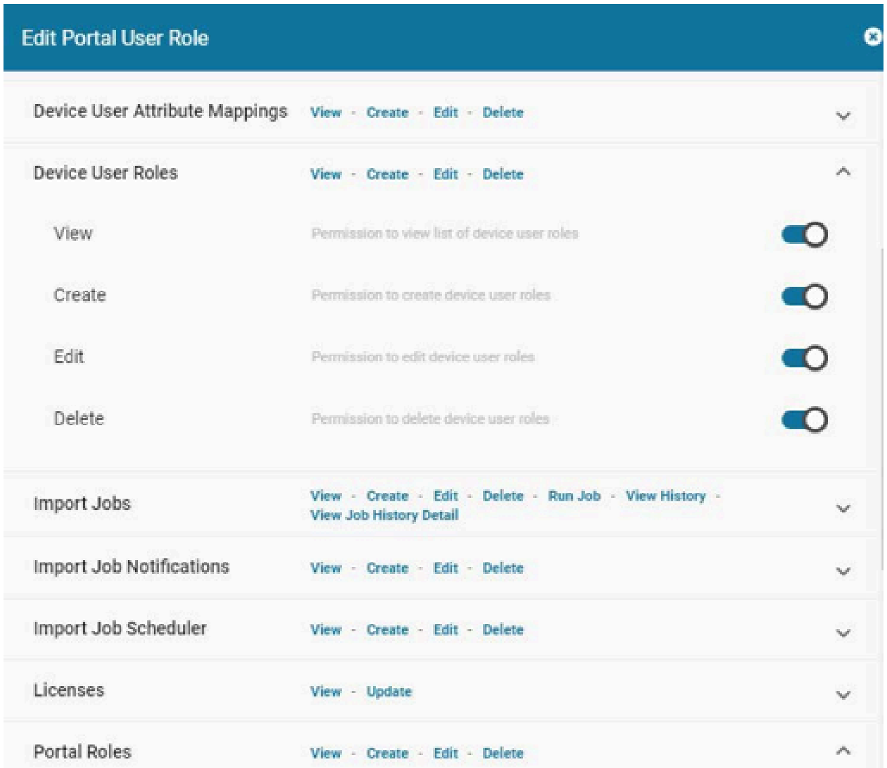
Dependencies

The Console admin user must have Device User Roles permissions enabled in the assigned Console Role to view and edit Roles.

Create and apply the appropriate Portal Role to the assigned portal administrator.

NOTE: The Roles must be created prior to being referenced by the User Role Level attribute.

Figure 90 Edit Portal User Role



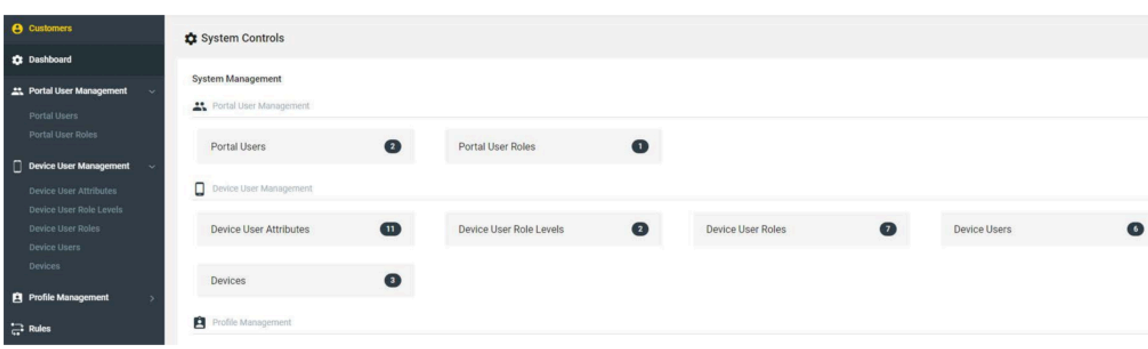
Adding and Assigning Role Levels

Role Levels can be added in the Admin Console or through the Swagger API interface.

Adding Role Levels from the Portal

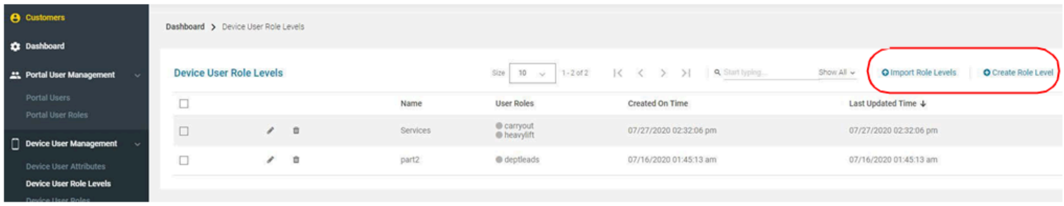
1. To add via the admin console, navigate to the Dashboard and select **Device User Role Levels**.

Figure 91 Device User Role Levels



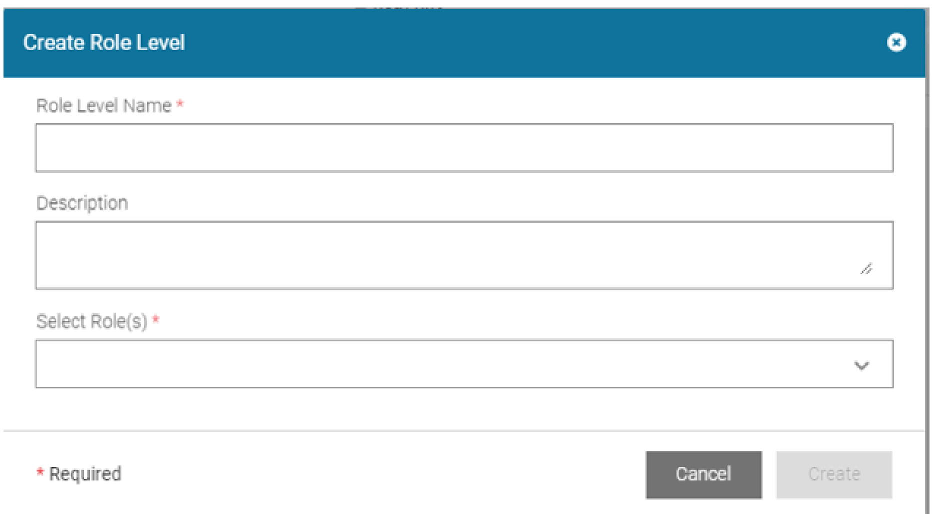
2. Click the link for **Import Role Levels** to import via a .csv file or **Create Role Level** to manually enter the role level.

Figure 92 Import Role Levels



3. Most often, Role Levels are imported through a .csv file, but creating a Role Level one at a time is possible. Click the **Create Role Level** link.

Figure 93 Create Role Level



4. Enter the desired **Role Level Name**. Only alphanumeric and _.*#!/?$ characters are allowed.

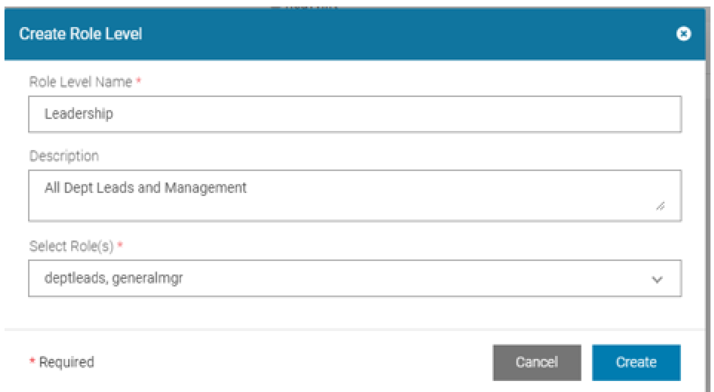
   The Name is used as a reference in the specified Device User definition. The Role Level Name can also be targeted by an AD Transformation identifier.

   The user does not see the Role Level Name, just the Roles bound to it. The entry does not support spaces, but special characters are supported.

   a) Enter a desired **Description**.

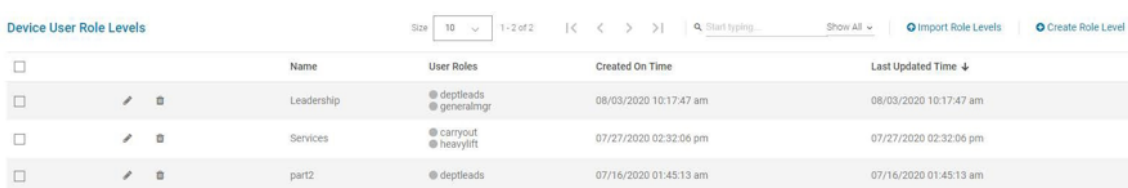
   b) Then from the dropdown menu, select the **Roles** to be bound to the Role Level.

   Figure 94 Create Role Level (Fields Added)



5. Once the Role Level is added, it appears in the Console.

   Figure 95 Console Showing Device User Role Levels

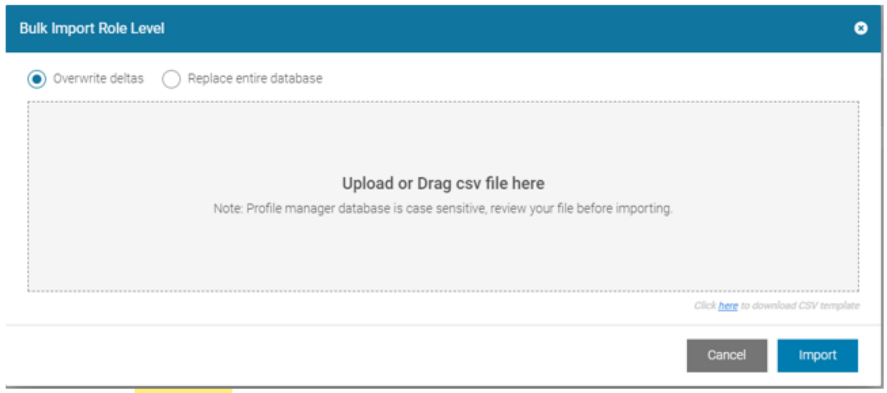


Importing Role Levels from a .csv File

1. Click the **Import Role Levels** link to open the Bulk Import Role Level dialog.

2. Download the CSV template by clicking the click here link above the **Cancel** and **Import** button as shown in the below screenshot.

Figure 96 Bulk Import Role Level Dialog



a) Edit the template as shown in Figure 102.

NOTE:

- The roles specified must match the case and spelling of the established roles being referenced. It is not possible to add new roles in this process. Spaces between the string of comma separated by roles is permitted.
- Role levels may be assigned to the users by CSV import or by AD Attribute assignment.

Figure 97 CSV File

	A	B	C	D
1	name	description	roles	
2	Speciality	Department Specialists	Screws,Wire,Nails	
3				
4				
5				
6				
7				

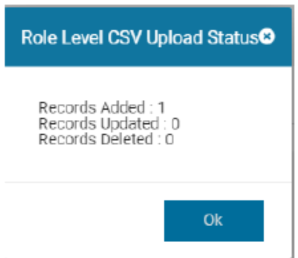
3. When the .csv file has been updated, drag the file into the import window.

   a) There are two import options available.

      - The **Overwrite Deltas** option updates the existing records and adds the new records while keeping the other records intact.
      - The **Replace** entire database deletes all existing Role Level information and inserts the new records.

   b) Once the import option is determined, click **Import** to begin the process.

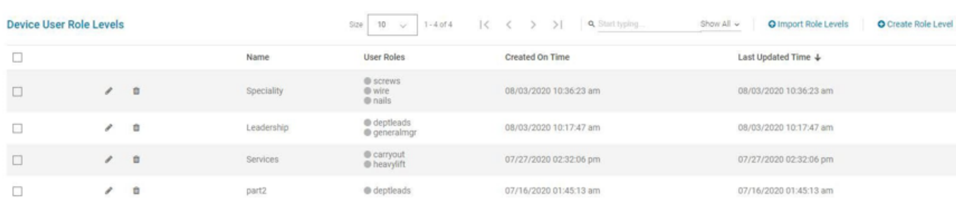
Figure 98 Role Level CSV Upload Status Dialog



When the import process is complete. Depending on the Import Type selected, the status message box displays the import results.

NOTE: If a Role Level is currently assigned to one or more Users, an attempt to modify or delete the role Level fails, and generates an error.

Figure 99 Successful Import Shown in Device User Role Level Summary Screen

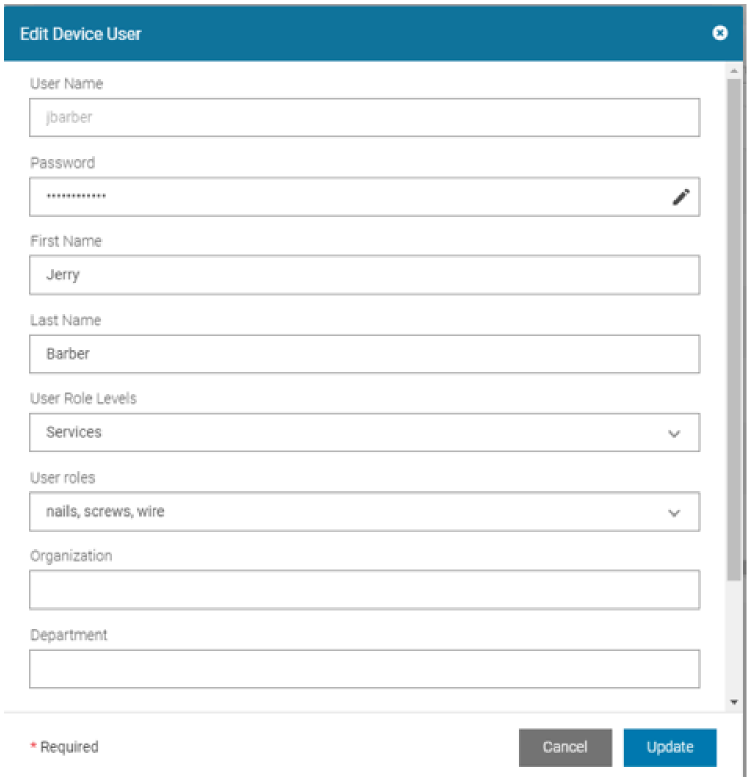


Applying the Role Level

1. Once the Role Level is established, it may be applied to a Device User.

   In this example, the user is assigned to the Role Level **Services** in the User profile.

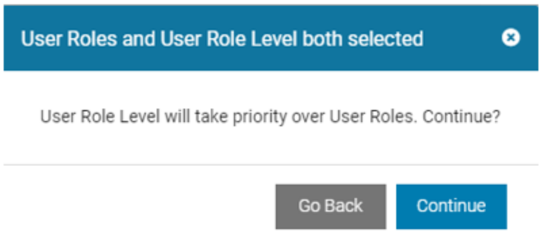
   Figure 100 Edit Device User



2. In this example, the User's Role level is set to Services, and the User Roles are set to **nails**, **screws**, and **wire**.

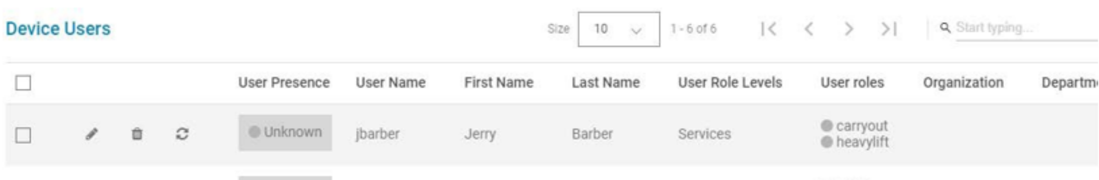
   This conflict is resolved at login in the Role Level assignment process. If there is a Role Level defined in addition to specified roles, the specified Role Level overrides the individual roles. (Normally, if a Role Level is specified, then User Roles is left blank.)

   Figure 101 User Roles and User Role Level Both Selected Dialog

   In this case, Services are assigned and the user is prompted for carryout and heavy lift when the sign-in occurs.

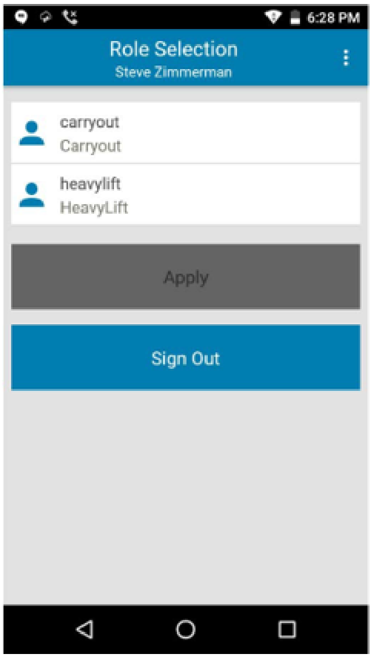
   Figure 102 Successful Role Level Applied in Device User Summary Screen

Device Operation

When the user signs on and is validated, the Roles defined by the Role Level are displayed.

Figure 103 Roles

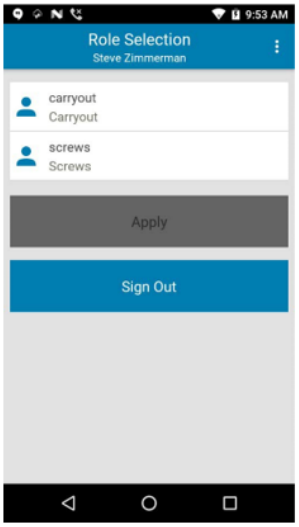


It is possible to create multiple Role Levels with common Roles. In this example:

Role Level	Roles
Services	Carryout, Heavy Lift
Hardware	Screws, Wire, Nails
Mix	Carryout, Screws

The Role Level 'Mix' contains Roles from Hardware and Services producing this result.

Figure 104 Role Level Mix



ZEMS and Profile Manager

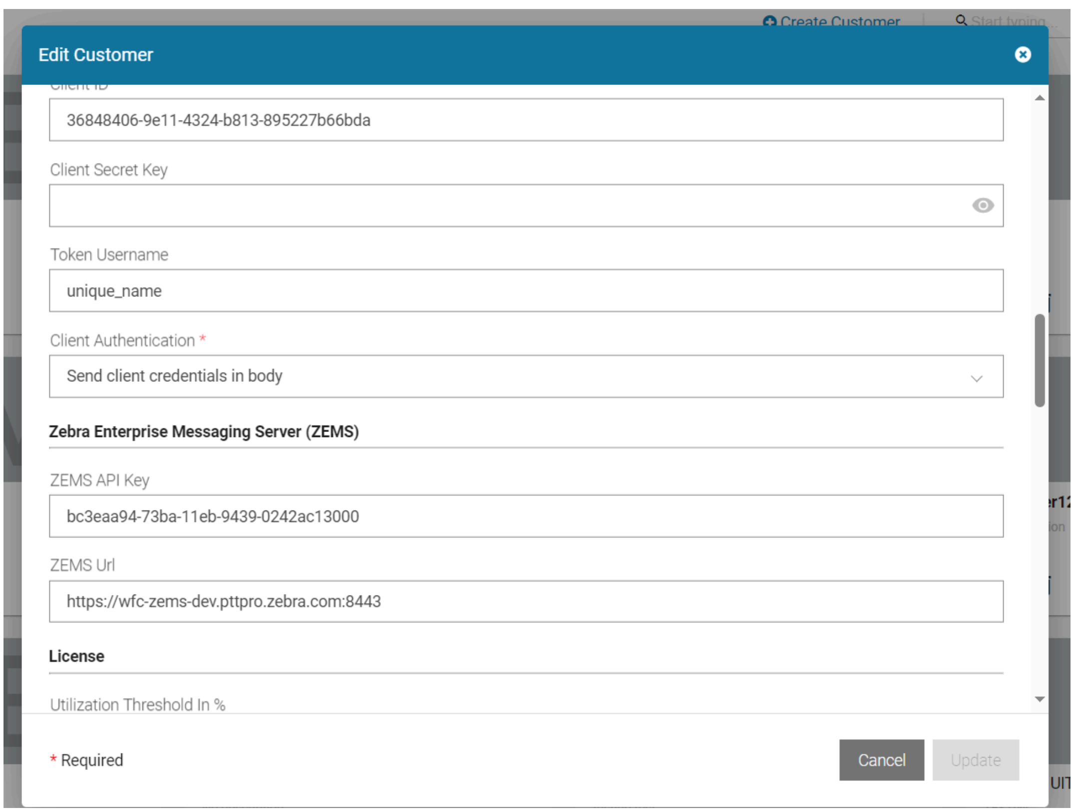
This feature allows associating the manager to the site of the region in the Zebra Enterprise Messaging Service (ZEMS) using the Profile Manager user import feature. Any changes in the user profile can be seamlessly synced to the ZEMS along with the user import.

These users are synced to ZEMS when the periodic sync between PTTPRO and ZEMS is executed. Refer to the ZEMS Customer Administrator Guide to understand the sync configuration in ZEMS.

Updating Users via Flat File (PFM) to Include Manager Association

To enable this feature (including Store, Region, District, or Corporate), do the following configurations:

1. Configure **ZEMS Url** and **API Key** in the Profile Manager Tenant configuration.



2. Configure PTT Pro user mappings for manager and region fields to respective CSV or LDAP attributes fields.

   After the above configuration is completed, if there are any value changes to the **Manager** and the **Region** during user import, ZEMS is notified to associate the manager with the site and regions. The actual association happens when the periodic sync between the PTT Pro and ZEMS is executed or when the user manually triggers the sync in the ZEMS admin portal. Typically, user import in Profile Manager is also synced daily at a specific time. One must configure the ZEMS-sync start time so that user import in Profile Manager must be completed before that.

   Profile Manager notifies the ZEMS in the following conditions:

   - If the ZEMS URL and the ZEMS Api Key are configured in the tenant configuration.
   - If the **Manager** field in the user mapping is true, and it was false during the last import. This would notify ZEMS to associate this user with all the regions specified in the **Region** field along with the user's site
   - If the **Manager** field in the user mapping is false and was true during the last import. This would notify ZEMS to dis-associate this user from all the regions specified in the **Region** field along with the user's site.
   - If the **Manager** field in the user mapping is true, and it was true during the last import. If there are any value changes in the **Region** field or site, This would notify ZEMS to associate or disassociate this user from all the regions specified in the **Region** field along with the user's site