WORKFORCE CONNECT
Profile Manager

Administrator’s Guide
Copyright

© 2020 ZIH Corp. and/or its affiliates. All rights reserved. ZEBRA and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

Terms of Use

• Proprietary Statement

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

• Product Improvements

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

• Liability Disclaimer

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

• Limitation of Liability

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

Publication Date

August 25, 2020
Revision History

Changes to the original guide are listed below:

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MN-003433-03 Rev A</td>
<td>11 August 2020</td>
<td>Updates for RRR delivery for WFC Profile Manager Version 4.2</td>
</tr>
<tr>
<td>MN-003433-02 Rev A</td>
<td>22 April 2020</td>
<td>Updates for RRR delivery for WFC Profile Manager Version 4.0</td>
</tr>
<tr>
<td>MN-003433-01 Rev B</td>
<td>12 December 2019</td>
<td>Updates for RRR delivery</td>
</tr>
<tr>
<td>MN-003433-01 Rev A</td>
<td>June 2019</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
System Management .......................................................................................................................... 20
Introduction ........................................................................................................................................ 20
Portal User Role Management ........................................................................................................... 20
  View Portal User Roles .......................................................................................................................... 21
  Create Portal User Roles ...................................................................................................................... 21
  Edit Portal User Roles ........................................................................................................................... 22
  Delete Portal User Roles ...................................................................................................................... 24
Portal User Management ...................................................................................................................... 24
  Create Portal Users ................................................................................................................................ 24
  Edit Portal Users ................................................................................................................................... 26
  Delete Portal Users .................................................................................................................................. 27
Device User Attribute Management ........................................................................................................ 28
  Create Device User Attributes ............................................................................................................... 28
  Edit Device User Attributes .................................................................................................................. 29
Device User Role Management ............................................................................................................. 30
  Create Device User Roles ..................................................................................................................... 31
  Edit Device User Roles ........................................................................................................................ 32
  Delete Device User Roles .................................................................................................................... 33
Device User Management ..................................................................................................................... 33
  View Device Users .............................................................................................................................. 33
  Add and Update Device Users .............................................................................................................. 34
    Add/Update Multiple Device Users (Bulk Import Device Users) ......................................................... 34
    Add a Device User ............................................................................................................................... 34
    Edit a Device User .............................................................................................................................. 35
  Delete a Device User ............................................................................................................................ 36
  Refresh a Device User’s Status .............................................................................................................. 36
Device Management .............................................................................................................................. 36
  License Management Through Device Licenses ................................................................................... 37
  View Devices ....................................................................................................................................... 37
  Add/Enroll and Update Devices .......................................................................................................... 37
    Add/Update Multiple Devices/Enroll Multiple Devices (Bulk Import Devices) ................................. 38
    Add a Device ..................................................................................................................................... 39
    Edit a Device .................................................................................................................................... 39
  Delete/De-Enroll a Device .................................................................................................................... 40
  Refresh a Device’s Status ..................................................................................................................... 42
Profile Definition Management ............................................................................................................. 42
  Create Profile Definitions .................................................................................................................... 42
## Contents

Edit Profile Definitions ............................................................................................................ 43  
Delete Profile Definitions ........................................................................................................ 44  
Profile Configuration Management ............................................................................................... 44  
Create Profile Configurations ...................................................................................................... 45  
Edit Profile Configurations ......................................................................................................... 46  
Delete Profile Configurations ...................................................................................................... 47  
Rule Management ......................................................................................................................... 47  
View Rules .................................................................................................................................. 48  
Create Rules ................................................................................................................................. 48  
Publish Rules ............................................................................................................................... 51  
Delete Rules ................................................................................................................................. 52  
System Report Management ........................................................................................................ 53  
Generate Reports ............................................................................................................................ 53  
Export Reports .............................................................................................................................. 54  
Create Report Templates .............................................................................................................. 54  
Edit Report Templates .................................................................................................................. 55  
Delete Report Templates .............................................................................................................. 56  
Identity Provider (IDP) Import Management ................................................................................ 57  
Introduction .................................................................................................................................. 57  
Device User Attribute Mappings .................................................................................................... 57  
View Mappings ............................................................................................................................. 57  
Add an Attribute or Constant ......................................................................................................... 58  
Clear an Attribute Mapping ........................................................................................................... 59  
Import Job Management ................................................................................................................ 60  
Introduction .................................................................................................................................. 60  
View Import Jobs ........................................................................................................................... 60  
Create Import Jobs ......................................................................................................................... 60  
Edit Jobs ........................................................................................................................................ 62  
Delete Jobs ..................................................................................................................................... 63  
Run Import Jobs ............................................................................................................................ 63  
View Import Job History ................................................................................................................ 64  
Import Job Notifications ................................................................................................................ 65  
Introduction .................................................................................................................................. 65  
View Import Job Notifications ....................................................................................................... 65  
Create Import Job Notifications .................................................................................................... 66  
Edit Import Job Notifications ........................................................................................................ 67  
Delete Import Job Notifications ..................................................................................................... 68  
Import Job Scheduler ..................................................................................................................... 69  
Introduction .................................................................................................................................. 69  
View Import Job Schedules ........................................................................................................... 69
Introduction

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 into Profile Manager and PTT Pro** 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.

Notational Conventions

The following conventions are used in this document:

- "tablet" refers to the Zebra XXXX tablet.
- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
• Icons on a screen
• Key names on a keypad
• Button names on a screen.
• Bullets (•) indicate:
  • Action items
  • Lists of alternatives
  • Lists of required steps that are not necessarily sequential.
• Sequential lists (such as 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 graphic icons are used throughout the documentation set. These icons and their associated meanings are described below.

- **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—EYE INJURY:** Wear protective eyewear when performing certain tasks.
- **CAUTION—PRODUCT DAMAGE:** If the precaution is not taken, the product could be damaged.
- **CAUTION:** If the precaution is not heeded, the user could receive minor or moderate injury.
- **CAUTION—HOT SURFACE:** Touching this area could result in burns.
- **CAUTION—ESD:** Observe proper electrostatic safety precautions.
- **CAUTION—ELECTRIC SHOCK:** Disconnect the printer power before performing certain procedures to avoid the risk of electric shock.
- **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.
- **NOTE:** This is an icon for wired networking notes.
- **NOTE:** This is an icon for wireless networking notes.
Related Documents and Software

The following documents provide more information about the Zebra Profile Manager.

• Workforce Connect Profile Client Device User’s Guide - MN-003602-01

For the latest version of this guide and all guides, go to http://www.zebra.com/support.

Service Information

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

When contacting support, please have the following information available:

• Serial number of the unit
• Model number or product name
• Software/firmware type or 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.

Feedback

If you have comments, questions, or suggestions about this guide, send an email to EVM-techdocs@zebra.com.
About this Chapter

This chapter covers the following topics.
- Introduction to Zebra Workforce Connect Profile Manager
- Profile Manager Functions
- Interconnection Details
- Logging In to Profile Manager Portal
- Logging Out of Profile Manager Portal
- Resetting Your Administrator Password
- Main Screen in Profile Manager
- System Controls Panel (Dashboard)
- Navigating the Profile Manager Portal Dashboard

Introduction to Zebra Workforce Connect Profile Manager

Profile Manager Functions

The Zebra Workforce Connect Profile Manager (Zebra Profile Manager) provides a portal 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 or customer administrators to configure and control the operation of mobile devices 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
  - Device users
  - Extensions
**Getting Started**

- Presence service management
- Monitoring of user and device activity
  - Real time usage
  - Historical data
- Report generation.

**Interconnection Details**

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

- Workforce Connect Voice
- PTT Pro
- relationship to PTT Pro
- relationship to WFC Profile Client
- Active Directory Server

**Logging In to Profile Manager Portal**

**Prerequisites**

Administrator must have an account in the Profile Manager portal.

To log in to the Profile Manager portal

1. Navigate to the Profile Manager portal.
2. If you are a first-time user of the Profile Manager portal, do the following.
   - Enter user ID, password, and customer ID

*Figure 1* Profile Manager Portal Login Dialog Box - First-time Profile Manager User
If you are a returning user of the Profile Manager portal, do the following.

- Enter user ID and password

Figure 2  Profile Manager Portal Login Dialog Box - Returning Profile Manager User

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 (see Figure 1).

Logging Out of Profile Manager Portal

To log out of 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 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.

   ![admin](image)

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

   ![Change Password](image)

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

Main Screen in Profile Manager

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

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

In the System Controls panel (dashboard), the links in the left panel take you to the same categories of the Profile Manager administration screens listed of 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 3    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
  - Rule Management
  - System Reports
- Active Directory Import Management
- Telephony Management
- Licenses.
Navigating the Profile Manager Portal Dashboard

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.

Figure 4  Dashboard Quick Link Button

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.

<table>
<thead>
<tr>
<th>Permission Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>View or edit</td>
</tr>
<tr>
<td>Action</td>
<td>Delete</td>
</tr>
<tr>
<td>Action</td>
<td>Delete/De-enroll device</td>
</tr>
<tr>
<td>Action</td>
<td>Refresh</td>
</tr>
<tr>
<td>Action</td>
<td>Reset password</td>
</tr>
<tr>
<td>Action</td>
<td>Mask</td>
</tr>
<tr>
<td>Action</td>
<td>Unmask</td>
</tr>
<tr>
<td>Action</td>
<td>Expand side navigation</td>
</tr>
<tr>
<td>Action</td>
<td>Expand drop-down</td>
</tr>
<tr>
<td>Action</td>
<td>Collapse drop-down</td>
</tr>
<tr>
<td>Action</td>
<td>Display history</td>
</tr>
<tr>
<td>Action</td>
<td>Run</td>
</tr>
<tr>
<td>Action</td>
<td>Search</td>
</tr>
<tr>
<td>Action</td>
<td>Search</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Opens dashboard</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Opens Device User Management</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Opens Rules</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Opens Reports</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Opens Telephony Manager</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Dashboard</td>
</tr>
</tbody>
</table>
Slider Switches

Click slider switches to enable and disable features.

<table>
<thead>
<tr>
<th>Setting</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Success and Error Messages

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

Figure 5    Action Message — Success

![Delete Success](image)

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

Figure 6    Action Message — Error

![Error](image)

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 7    Portal User Search Field and Drop-Down Filter

![Search Field](image)
Introduction

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

- Portal user roles
- Portal users
- Device user attributes
- Device user roles
- Device Users
- Devices
- Profile definitions
- Profile configurations
- Rules
- System reports.

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

**Prerequisites**
Your privileges must permit you to view portal user roles.

To view portal user roles:

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

The **Portal User Roles** screen appears.

**Figure 8**   **Portal User Roles Screen**

Create Portal User Roles

**Prerequisites**
Your privileges must permit you to create portal user roles.

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.
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**

**Prerequisites**

Your privileges must permit you to edit portal user roles.

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 10**  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 will apply to anyone who is assigned the updated portal user role.
Delete Portal User Roles

Prerequisites
Your privileges must permit you to delete portal user roles.

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.

![Delete Portal User Role](image)

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

Prerequisites

- 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.

To create portal user roles:

1. From the dashboard, click Portal Users.
   The Portal Users screen appears.
2. Click Create Portal User.
   The Create Portal User dialog box appears.
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

Prerequisites

Your privileges must permit you to edit portal users.

To edit portal users:

1. From the **dashboard**, click **Portal Users**. The Portal Users screen appears.

**Figure 13** 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.

Click the following icon for the portal user whose password you want to reset.

Choose the type of reset: Manual or email. Complete the other fields in the dialog box. Then click **Reset** to close the Reset Password dialog box.

1. Click **** for the portal user you wish to edit. The Edit Portal User dialog box appears.
2. Update entries in the fields in the **Create Portal User** dialog box.
3. Click the slider switches to enable/disable the **user role(s)**.
4. Click **Update**.

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

### Delete Portal Users

**Prerequisites**

Your privileges must permit you to delete portal users.

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.
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.

Prerequisites

Your privileges must permit you to create device user attributes.

To create device user attributes:

1. From the dashboard, click Device User Attributes.
   
   The Device User Attributes screen appears.

2. Click Create User Attribute.
   
   The Create Device User Attribute dialog box appears.
3. Use the following table to set up the device user attribute.

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

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**

**Prerequisites**

Your own role must allow editing device user attributes.

To edit 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 17**  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
- Update the permissions for an existing device user role.
Create Device User Roles

**Prerequisites**

Your privileges must permit you to create device user roles.

To create device user roles:

1. From the **dashboard**, click **Device User Roles**.
   
   The **Device User Roles** screen appears.

   ![Device User Roles Screen](image)

   **Figure 18**  Device User Roles Screen

2. Click **Create Device User Role**.
   
   The Create **Device User Roles** dialog box appears.

   ![Create Device User Role Dialog Box](image)

   **Figure 19**  Create Device User Role Dialog Box

3. Enter the role name in **Name**.

4. Enter a description of the role in **Description**.
5. Make a selection in **PTT Pro Group**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No Device User Role (a.k.a. group) is created in PTT Pro.</td>
</tr>
<tr>
<td>Static</td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>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 Dynamic group in PTT Pro allows a Device User to be dynamically assigned and unassigned (added and removed) from the Dynamic Group in PTT Pro.</td>
</tr>
</tbody>
</table>

6. 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**

**Prerequisites**

Your privileges must permit you to edit device user roles.

To edit device user roles:

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

   The **Device User Roles** screen appears.

2. Click **Edit** for the device user role you wish to edit.

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

**Figure 20**  Edit Device User Role Dialog Box

3. Update the fields.
Delete Device User Roles

Prerequisites
Your privileges must permit you to delete device user roles.

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

1. To cancel, click No. To continue, click Yes.

To delete 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 delete.
   
The Delete Device User Role dialog appears.

**Figure 21** 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 current information for all device users, such as login status and logged in users.

**Prerequisites**
Your privileges must permit you to view device users.
To view device users:
From the dashboard, click Device Users.
The Device Users screen appears.

**Figure 22** 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.

Add/Update Multiple Device Users (Bulk Import Device Users)

The support of Bulk Import Device Users is detailed in the Bulk Import Device Users into Profile Manager and PTT Pro on page 93.

Add a Device User

Use this procedure to create device users.

**Prerequisites**
- 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.

To create device users:
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 23** Create Device User Dialog Box

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

4. Click **Create**.

**Edit a Device User**

**Prerequisites**

Your privileges must permit you to edit device users.

To edit device user roles:

1. From the **dashboard**, click **Device Users**. The **Device Users** screen appears.

2. Click **edit** 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**.
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 device user, add a temporary password to the Password and Confirm Password fields. Give the device user the temporary password. Then the device user can log into the system and change their temporary password to a different password.

4. Click Update.

Delete a Device User

Use this procedure to delete a device user.

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

Prerequisites

Your privileges must permit you to delete device users.

To delete device users:

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.

3. Click Yes to delete.

Refresh a Device User’s Status

To refresh a device user’s presence:

1. From the dashboard, click Device Users.
   The Device Users screen appears.

2. Click 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.

Prerequisites

Your privileges must permit you to view devices.

To view devices:

From the dashboard, click Devices.
The Devices screen appears.

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.

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

Prerequisites

• 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.

To bulk import devices:

1. From the dashboard,click Device.
   The Devices screen appears.
2. Click Import Devices.
   The Bulk Import Devices dialog box appears.

   Figure 26   Bulk Import Devices Dialog Box

   Bulk Import Devices
   □ Overwrite deltas   □ Replace entire database
   Upload or Drag CSV file here

   Click here to download CSV template

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.

To add a device:

1. From the dashboard, click Device.
   The Devices screen appears.

2. Click +Add Device.
   The Add Device screen appears.

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 at a later time.

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

Prerequisites

Your privileges must permit you to edit devices.

To edit a device:
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. Click **Update**.

**Delete/De-Enroll a Device**

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

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

**Prerequisites**

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

1. Click 💼 for the device(s) to delete/de-enroll. The **Devices** screen appears.

![Figure 28 Devices Screen](image)

The **De-Enroll Device** dialog box appears.
2. Click **Yes** to delete/de-enroll.

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

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

   If a 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.
Refresh a Device's Status

To refresh a device's presence:
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.

Prerequisites

Your privileges must permit you to create profile definitions.

To create profile definitions:
1. From the dashboard, click Profile Definitions.
   The Profile Definition screen appears.

Figure 30    Profile Definitions Screen
2. Click **Create Profile Definition**.
   
   The **Create Profile Definition** dialog box appears.

   **Figure 31** Create Profile Definition Dialog Box

   ![Create Profile Definition](image)

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 ![JSON](image) to enter the profile definition in JSON format, include `app_info` and `app_setting` definitions.
7. Click ![Layout](image) to verify the JSON.
8. Click **Create**.

**Edit Profile Definitions**

**Prerequisites**

Your privileges must permit you to edit profile definitions.

To edit profile definitions:

1. From the **dashboard**, click **Profile Definitions**.
   
   The **Profile Definition** screen appears.

2. Click ![Edit](image) 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

Prerequisites
Your privileges must permit you to delete profile definitions.
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

Prerequisites

- 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.

To create profile configurations:

1. From the dashboard, click Profile Configurations.
   
The Profile Configurations screen appears.

Figure 32 Profile Configurations Screen
2. Click **Create Profile Configuration**.
   The **Create Profile Configuration** dialog box appears.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for this configuration.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the profile configuration.</td>
</tr>
<tr>
<td>Profile Definition</td>
<td>Depending on the profile definition you choose, options will appear in Settings.</td>
</tr>
</tbody>
</table>

4. Click **Next**.
   A list of options associated with the profile definition, if any, appears.

5. Complete **Settings**.
6. Click **Create**.

**Edit Profile Configurations**

**Prerequisites**
Your privileges must permit you to edit profile configurations.

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.


4. Click Next.

5. Make desired changes on the Settings tab.

6. Click Update.

Delete Profile Configurations

Prerequisites
Your privileges must permit you to delete profile configurations. 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

**Prerequisites**
You own role must allow you to view the list of rules.

To view the list of rules:
From the dashboard, click **Rules**.
The list of rules appears.

**Figure 33**  Rules Screen

Create Rules

**Prerequisites**
You own role must allow you to create rules.

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 entered 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 users.

14. Click **Create**.
   
   The new rule is created.
Publish Rules

Prerequisites

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

- You own role must allow you to publish rules.

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

Prerequisites
You own role must allow you to delete rules.

To delete rules:
1. From the dashboard, click Rules.
   The Rules screen appears.

   \[\text{Figure 41} \quad \text{Rules Screen}\]

2. Select the checkbox for the rule(s) you wish to delete.
   The Delete Rules button appears.

   \[\text{Figure 42} \quad \text{Delete Selected Rule(s) Button}\]

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

Prerequisites

You own role must allow you to generate system reports.

To generate reports:

1. From the dashboard, click System Reports.
   The Generate System Report screen appears.

2. Click the Select Saved Report drop-down.
3. Select the report that you wish to generate.
4. Click **Generate Report**.
   
   The report appears.

**Figure 44**  Generated Report

---

### Export Reports

**Prerequisites**

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

To export 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

**Prerequisites**

Your privileges must permit you to create report templates.

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 45  Create Saved Report**

---

**Edit Report Templates**

**Prerequisites**

Your privileges must permit you to edit report templates.

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

Prerequisites

Your privileges must permit you to delete report templates.

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 (IDP) Import Management

Introduction

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 IDP user characteristics into PTT Pro and Profile Manager Systems.

Device User Attribute Mappings

View Mappings

Prerequisites

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

![PTT Pro System Tab](image)

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

   The **Transformations** content is populated.

**Add an Attribute or Constant**

**Prerequisites**

Your privileges must permit you to modify user attribute mappings.

To add an attribute or constant to a mapping:

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 47**  PTT Pro System Tab

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

**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

Introduction

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

Prerequisites

Your privileges must permit you to view import jobs.

To view import jobs:

From the dashboard, click Import Jobs.

The Import Jobs Screen appears.

Create Import Jobs

Prerequisites

Your privileges must permit you to create import jobs.

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 49** Create Job Dialog Box

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Job Name</td>
</tr>
<tr>
<td>Scope</td>
<td><strong>Active Directory Search Scope</strong></td>
</tr>
<tr>
<td></td>
<td>• Object: base object</td>
</tr>
<tr>
<td></td>
<td>• One Level: immediate children of base object</td>
</tr>
<tr>
<td></td>
<td>• Subtree: base object and all child objects.</td>
</tr>
<tr>
<td>Query</td>
<td>Search the active directory. For example: OU=users,DC=PTTPRO,DC=ZEBRA</td>
</tr>
<tr>
<td>Filter</td>
<td>Search for a subset of user(s). For example, to search for anyone with the name of Andrew: (name=andrew*)</td>
</tr>
<tr>
<td>Description</td>
<td>Optional description of the purpose of the import.</td>
</tr>
</tbody>
</table>
Edit Jobs

Prerequisites

Your privileges must permit you to edit import jobs.

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 50   Edit Job Dialog Box

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

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

Prerequisites
Your privileges must permit you to delete jobs.
To delete jobs:

1. From the dashboard, click Import Jobs.
   The Import Jobs screen appears.
2. Click the icon next to the job you wish to delete.
   The Delete Job dialog box appears.
3. Click Yes to delete.

Run Import Jobs

Prerequisites
• Your privileges must permit you to run import jobs.
• The mapping must be set up correctly.
To run import jobs:
1. From the dashboard, click Import Jobs.
2. From the Import Jobs screen, click the icon for the job you wish to run.
   The Run Job dialog box appears.

Figure 51 Run Job Dialog Box

3. Click Yes to run the job.
View Import Job History

Prerequisites
Your privileges must permit you to view job history.

To view import 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 52 Import Job History Screen

<table>
<thead>
<tr>
<th>Import Job History (doctor role)</th>
<th>Dispatchers</th>
<th>Query Name</th>
<th>Process State</th>
<th>Error Message</th>
<th>Start Time</th>
<th>End Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>03/20/2019 01:45:56 pm</td>
<td>03/20/2019 01:45:56 pm</td>
<td>0.27 sec</td>
</tr>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>03/25/2019 02:00:00 am</td>
<td>03/25/2019 02:00:02 am</td>
<td>1.31 sec</td>
</tr>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>04/01/2019 02:00:02 am</td>
<td>04/01/2019 02:00:03 am</td>
<td>0.30 sec</td>
</tr>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>05/15/2019 07:17:23 am</td>
<td>05/15/2019 07:17:24 am</td>
<td>0.27 sec</td>
</tr>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>05/16/2019 04:15:32 am</td>
<td>05/16/2019 04:15:32 am</td>
<td>0.20 sec</td>
</tr>
<tr>
<td>View Deltas</td>
<td>Profile Manager</td>
<td>doctor role</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>05/22/2019 12:06:03 pm</td>
<td>05/23/2019 12:06:03 pm</td>
<td>0.20 sec</td>
</tr>
</tbody>
</table>

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

3. Click to view details.
4. Click View Deltas to view more information.

The Deltas dialog box appears:

Figure 53 Deltas Dialog Box
5. Click an option in the **Dispatchers** column to more information.

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

![Dispatcher History (PTT Pro) Dialog Box](image)

### Import Job Notifications

**Introduction**

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

**View Import Job Notifications**

**Prerequisites**

Your privileges must permit you to view import job notifications.
To view import job notifications:

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

The **Import Job Notifications** screen appears.

**Figure 55** Import Job Notifications Screen

### Create Import Job Notifications

**Prerequisites**

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

To create import job notifications:

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 56**  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**

**Prerequisites**

Your privileges must permit you to edit import job notifications.

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

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

To delete import job notifications:
1. From the dashboard, click **Import Job Notifications**.
2. Click for the notification you wish to delete.
3. The **Delete Notification** dialog box appears.

Figure 57 Delete Notification Dialog Box

4. Click **Yes** to delete.
Import Job Scheduler

Introduction

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

View Import Job Schedules

Prerequisites
Your privileges must permit you to view import job schedulers.

To view import job schedulers:
From the dashboard, click Import Job Scheduler.
The Import Job Scheduler screen appears.

Prerequisites
Your privileges must permit you to create import job schedulers.

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.

![Create Scheduler Dialog Box](image)

3. Enter a name for the scheduler in the **Name** field.
4. Select one or more checkboxes from the right.
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

**Prerequisites**
Your privileges must permit you to edit import job schedulers.

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

**Prerequisites**

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

To delete import job schedulers:

1. From the **dashboard**, click **Import Job Scheduler**.
2. Click ![Scheduler Icon] for the scheduler you wish to delete.
3. The **Delete Scheduler** dialog box appears.

**Figure 60**  Delete Scheduler Dialog Box

Are you sure you want to delete the scheduler?

| No | Yes |

4. Click **Yes** to delete.
Client Device Setup Using Telephony Manager and Profile Manager

Introduction

This chapter describes the following.

- Client Device Setup Using Telephony Manager and Profile Manager
- Configure Telephony Manager Using a CSV File (automated option)
- Manually Configure Telephony Manager (for technical support)
- Configure Zebra 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 on page 83.

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.

Configure Telephony Manager Using a CSV File (automated option)

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.

To import the list of Extensions using a CSV file, see the Extension Import Management.
Confirm Successful Import of Data from the CSV File

1. Open the Zebra 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 Extension_Password (depending on your site’s configuration)
4. Close the Zebra 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 would be 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 Extension_Password (depending on your site’s configuration)
Enter the Store / Site ID Information

**IMPORTANT:** 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 and from 1 to 19 digits long.

**Figure 61** The Update Store Screen

![Update Store Screen](image)

2. Click **Update**.
   
The following screen appears.

**Figure 62** The Stores Data Screen

![Stores Data Screen](image)

**IMPORTANT:** In Telephony Manager, make sure that the value for **Store ID** is the same value 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 following screen displays.

   **Figure 63** The PBX Update Screen

   ![PBX Update Screen](image)

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

   **IMPORTANT**: 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 64** Sample PBX Entries

<table>
<thead>
<tr>
<th>PBX Type</th>
<th>PBX Address</th>
<th>Parameters (JSON)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk</td>
<td>18.211.19.155</td>
<td>{}</td>
</tr>
<tr>
<td>CUCM</td>
<td>10.11.18.9</td>
<td>{}</td>
</tr>
<tr>
<td>CUCM</td>
<td>172.19.18.11</td>
<td>{}</td>
</tr>
</tbody>
</table>

### Add Department Information

**IMPORTANT:** 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.

<table>
<thead>
<tr>
<th>Telephony Manager</th>
<th>Profile Manager</th>
<th>PBX</th>
<th>Worforce Connect Profile Client Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>must match ---›</td>
<td>&lt;--- must match</td>
<td>WFC Client Device becomes activated ---›</td>
<td>As a result of device activation on PBX---</td>
</tr>
<tr>
<td>Department</td>
<td>User Role/Department</td>
<td>---› User Role/Department is populated into the WFC Client Device from Profile Manager</td>
<td></td>
</tr>
</tbody>
</table>
After a device becomes activated on a PBX, the User Role/Department field is displayed on the Profile Client device as shown.

**Figure 65** 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 66** 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 complete, the Departments will be displayed. The sample Department list shows results filtered on Store 9999.

**Figure 67** Sample Department List

<table>
<thead>
<tr>
<th>Store</th>
<th>Department</th>
<th>Description</th>
<th>Auto</th>
<th>Hidden</th>
<th>Reserved</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>9999</td>
<td>Clothing</td>
<td>Clothing</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>9999</td>
<td>Line.Manager 1</td>
<td>Line.Manager 1</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>9999</td>
<td>Manufacturing</td>
<td>Manufacturing</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>9999</td>
<td>Quality.Control</td>
<td>Quality.Control</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>9999</td>
<td>Shipping</td>
<td>Shipping</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

**Enter PBX Extension Information**

**IMPORTANT:** 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 68** 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 69** Sample Extensions List (on Extensions Data Screen)

---

**Configure Zebra Profile Manager**

To configure Zebra Profile Manager, do the following.

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.

   ![Role Selection Screen]

   The Role Section screen displays.

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 WFC Profile Client for this user to the list of roles that are configured for this user in the Zebra Profile Manager application. See Edit Device User Roles.

If the roles in WFC Profile Client and in the Zebra 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 provisioning of extensions for all the roles. A checkmark indicates that a role has been selected.
6. Select 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.

**IMPORTANT:** 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.
Introduction

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:

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

   The **Extensions screen appears**.

**Figure 70**   Extensions Screen

---

## Refresh Extensions

**Prerequisite**

Your privileges must permit you to refresh extensions.

To refresh extensions:

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

   The **Extensions screen appears**.

2. Click **for the extension to refresh.**

---

## Extension Import Management

**Prerequisite**

- 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.

To import extensions:

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.
Introduction

This chapter describes following.

• About licenses
• View Profile Manager application licenses
• Update Profile Manager application licenses.

About Licenses

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

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

**Prerequisite**
Your privileges must permit you to view application licenses.

To view licenses:

1. From the **bottom of the dashboard**, click **License**.
   
   The **Licenses screen** appears.

**Figure 71** Licenses Screen

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Count</th>
<th>Maximum Count</th>
<th>Expiration</th>
<th>Created On Time</th>
<th>Last Updated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>wfcpm-feature-connector</td>
<td>1.0</td>
<td>2</td>
<td>2</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-adms</td>
<td>1.0</td>
<td>10</td>
<td>10</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-base</td>
<td>1.0</td>
<td>1</td>
<td>2</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-device</td>
<td>1.0</td>
<td>53</td>
<td>53</td>
<td>08/05/2024 06:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-eon-manager</td>
<td>1.0</td>
<td>2</td>
<td>2</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-ext-manager</td>
<td>1.0</td>
<td>2</td>
<td>2</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-ha-containers</td>
<td>1.0</td>
<td>8</td>
<td>8</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
<tr>
<td>wfcpm-feature-presence</td>
<td>1.0</td>
<td>1</td>
<td>2</td>
<td>03/01/2024 05:59:59 pm</td>
<td>08/08/2019 11:47:51 am</td>
<td>08/18/2019 07:30:00 pm</td>
</tr>
</tbody>
</table>

Update Application Licenses

**Prerequisite**
Your privileges must permit you to update application licenses.

To update 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.
Introduction

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

Profile Manager Client Configuration File Elements

The WFC Profile Client will still operate without the JSON configuration file, however, the user will need to configure the required Profile Manager connectivity parameters manually through the app's UI.

Sample WFCDFSConfig.json file:

```
{
    "customer_id": "3001",
    "sfs_url": "https://<PFM_server.com",
    "site_id": 5000,
    "log_level": "debug",
    "confirm_role":false,
    "interval": 0,
    "power_connected_logout":true,
    "return_to_click_page_interval": 0,
    "log_file": true,
    "dnd_switch":true,
    "config_settings":0,
    "key_user_name": "userNameInput",
    "key_user_pwd": "passwordInput",
    "key_submit": "submitButton",
    "key_domain": "ptpro"
}
```

See Table 72 on page 89 for descriptions of JSON elements.
### Profile Client json Config Variables

**Supported in version 2.0.20207+**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Type</th>
<th>Default</th>
<th>Config via UI?</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_id</td>
<td>Maps to the Profile Manager’s Tenant ID provided by the system administrator.</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>Yes</td>
</tr>
<tr>
<td>dfs_url</td>
<td>The FQDN of the Profile Manager secure web socket connection provided by the system administrator.</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>Yes</td>
</tr>
<tr>
<td>log_level</td>
<td>Log options are: Info (default), Debug, Warning, Error, and Verbose</td>
<td>string</td>
<td>info</td>
<td>Yes</td>
</tr>
<tr>
<td>log_file</td>
<td>Enable application to record logs and store on the sdcard of device. Logs are available at /sdcard/DFS/</td>
<td>Boolean</td>
<td>FALSE</td>
<td>Yes</td>
</tr>
<tr>
<td>confirm_role</td>
<td>When set to True, once the roles are selected the user will be prompted to confirm the selections.</td>
<td>Boolean</td>
<td>TRUE</td>
<td>Yes</td>
</tr>
<tr>
<td>site_id</td>
<td>Is the value correlated in Extension Manager’s Store ID value. Upon match will align the group of extensions available to the User based on the Roles configured.</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>Yes</td>
</tr>
<tr>
<td>interval</td>
<td>Allows admin to configure the interval to show the &quot;Click To Login&quot; button, reminding the user to login in and select a role.</td>
<td>integer</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>return_to_click_page_interval</td>
<td>Configures the interval for the Profile Client to show the &quot;Click To Login&quot; screen while user is idle at the login page for an extended period. The interval time can be any value between 0-60 minutes. Min: 1, Max: 60, disable: 0</td>
<td>integer</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>dnd_switch</td>
<td>Allows user to display/remove the dnd_switch in Profile Client</td>
<td>Boolean</td>
<td>TRUE</td>
<td>No</td>
</tr>
<tr>
<td>config_settings</td>
<td>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</td>
<td>integer</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>power_connected_logout</td>
<td>When enabled will Sign out Profile Client User, when device is put in cradle for charging</td>
<td>Boolean</td>
<td>FALSE</td>
<td>Yes</td>
</tr>
<tr>
<td>secret_key</td>
<td>Key used to decrypt the login blob delivered from the Launcher app via intent to the Profile Client.</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>No</td>
</tr>
<tr>
<td>key_user_name</td>
<td>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: <code>&lt;input type=&quot;text&quot; name=&quot;username&quot; id=&quot;username&quot; class=&quot;textinput&quot; value=&quot;&quot;&gt;</code></td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>No</td>
</tr>
<tr>
<td>key_user_pwd</td>
<td>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: <code>&lt;input type=&quot;password&quot; name=&quot;password&quot; id=&quot;password&quot; class=&quot;textinput&quot; autocomplete=&quot;off&quot;&gt;</code>,</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>No</td>
</tr>
<tr>
<td>key_submit</td>
<td>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: <code>&lt;input type=&quot;submit&quot; value=&quot;Login&quot; id=&quot;submit&quot; class=&quot;submit&quot; tabindex=&quot;4&quot; role=&quot;button&quot;&gt;</code></td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>No</td>
</tr>
<tr>
<td>key_domain</td>
<td>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: &quot;ptptpro&lt;username&gt;&quot;</td>
<td>string</td>
<td>&lt;null&gt;</td>
<td>No</td>
</tr>
</tbody>
</table>
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 concept provides the Customer the ability to keep the existing Launcher for the User signon process, and then to pass the user information to the Profile Manager client for authentication to 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:

```html
<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;"/>
  </span>
</div>
```
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 DFS client receives the credentials via intent from the third party Launcher application, and will pass the credentials to the appropriate tagged fields. The DFS 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. And, the 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 would be populated with:

- Key_user_name: “username”
- Key_user_pwd: “password”
- Key_submit: “submit”

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

**ADB Supported Commands**

### Install the PFM Client

- Can use MX (this gives the APK all permissions requested)
- Side load and manual startup requires permissions acknowledgement:
  
  `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 will look for the default file ‘WFCDFSConfig.json’ in the /sdcard/ folder.

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

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

### Starting the DFS Client

- Starting the client will start the activity. 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 will cause the client to restart.
Reconfiguring a Running Client

1. 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 will be logged out of the 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 will read the config and restart the client with the new parameters. The user will be logged out of the 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 would be 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 --es user_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 {}
  ```
About this Chapter

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 Using Role Level, the .csv file would not include the Role information. If both exist, the Role Level would be used for the user and the Roles information would be discarded.
- The User import will create 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 will remain 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 will appear.

Figure 73   Device Users Screen
2. Then, click on 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 74**  Bulk Import Users Screen

**Figure 75**  Sample Populated CSV File Template

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
<th>First Name</th>
<th>Last Name</th>
<th>User Role Levels</th>
<th>User roles</th>
<th>Organization</th>
<th>Department</th>
<th>Force Logout</th>
<th>Authentication Method</th>
<th>Telephone</th>
<th>Group/GroupTemplate</th>
<th>Country/Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserA1</td>
<td>99999999</td>
<td>Jean-Louie</td>
<td>John</td>
<td>Hardware</td>
<td></td>
<td>NA</td>
<td>Paris</td>
<td>TRUE</td>
<td>BASIC</td>
<td>standard</td>
<td></td>
<td>111111</td>
</tr>
<tr>
<td>UserA2</td>
<td>99999999</td>
<td>Frank</td>
<td>Johnson</td>
<td>Services</td>
<td></td>
<td>NA</td>
<td>Name</td>
<td>TRUE</td>
<td>OAuth2</td>
<td>standard</td>
<td></td>
<td>222222</td>
</tr>
<tr>
<td>UserA3</td>
<td>99999999</td>
<td>Lloyd</td>
<td>Smith</td>
<td>Leadership</td>
<td></td>
<td>NA</td>
<td>Oceo</td>
<td>TRUE</td>
<td>OAuth2</td>
<td>standard</td>
<td></td>
<td>333333</td>
</tr>
</tbody>
</table>

- 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 76 on page 96**.
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** will leave the user records in place, making adjustments to any existing records as specified in the .csv. If there are new records, they will be added.

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

**Figure 77** 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 78**  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 complete, the system will return to the **Device User** screen.

**Figure 79** is a sample of an import file and the resulting status.

**Figure 79**  Import File

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
<th>First Name</th>
<th>Last Name</th>
<th>User Role</th>
<th>Organizational</th>
<th>Department</th>
<th>Force Login</th>
<th>Authentication</th>
<th>TelePHON</th>
<th>Group Use</th>
<th>OAuth Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>User_A1</td>
<td>Bicycle995Jean-LouisJohnSamuHardware</td>
<td>floor_swe NALA</td>
<td>Paris</td>
<td>TRUE</td>
<td>BASIC</td>
<td>standard</td>
<td>111111</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User_A2</td>
<td>Bicycle995Frankjohnson1Services</td>
<td>floor_swe EMEA</td>
<td>Rome</td>
<td>TRUE</td>
<td>OAuth2</td>
<td>standard</td>
<td>222222</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User_A3</td>
<td>Bicycle995LloydSmith2smiLeadership</td>
<td>trash_haul APAC</td>
<td>Oslo</td>
<td>TRUE</td>
<td>OAuth2</td>
<td>standard</td>
<td>333333</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. To check on the job status, click on **Import Device Users**, then select **View Last Import Status**.

**Figure 80** View Last Import Status Screen

In this three User example, 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.

10. Verify all records were added as expected to Profile Manager and PTT Pro servers.
Multiple Role Values from Attributes

About this Chapter

This chapter covers the following topics.

- Description
- Assumptions
- Configuration Process
- Overview
- Identification of AD Attributes
- Import Attribute Transformations
- Create an Import Job
- Researching Provisioning Errors
- Successful Provisioning and Attribute Mapping

Description

Previous versions of Profile Manager supported only one Role assignment that could be obtained from an Active Directory (AD) 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 will be used in the attribute values.
- Any of the delimiters used will not be 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 will describe various entities and elements within a successful configuration. The configuration process is:

• Identify an AD Attribute suitable for Role definition.
• Identify all AD attributes that will be 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 LDAP 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 81    Role and Attribute Example

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dSCorePropagationData</td>
<td>1601010100000000.C07</td>
</tr>
<tr>
<td>extensionAttribute5</td>
<td>TRUE</td>
</tr>
<tr>
<td>extensionAttribute7</td>
<td>wire, screws, nails</td>
</tr>
<tr>
<td>givenName</td>
<td>zman1</td>
</tr>
<tr>
<td>lastLogoff</td>
<td>0</td>
</tr>
<tr>
<td>lastLogon</td>
<td>132398374405244000</td>
</tr>
<tr>
<td>lastLogonTimestamp</td>
<td>132405114529773000</td>
</tr>
<tr>
<td>logonCount</td>
<td>22</td>
</tr>
</tbody>
</table>

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.
## Figure 82 Attributes

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>zman1</td>
</tr>
<tr>
<td>instanceType</td>
<td>4</td>
</tr>
<tr>
<td>nTSecurityDescriptor</td>
<td></td>
</tr>
<tr>
<td>objectCategory</td>
<td>CN=Person,CN=Schema,CN=Configuration,DC=PTTPRO,DC=ZEBRA</td>
</tr>
<tr>
<td>objectClass</td>
<td>organizationalPerson</td>
</tr>
<tr>
<td>objectClass</td>
<td>person</td>
</tr>
<tr>
<td>objectClass</td>
<td>top</td>
</tr>
<tr>
<td>objectClass</td>
<td>user</td>
</tr>
<tr>
<td>accountExpires</td>
<td>9223372036854770000</td>
</tr>
<tr>
<td>badPasswordTime</td>
<td>132397473873874000</td>
</tr>
<tr>
<td>badPwdCount</td>
<td>0</td>
</tr>
<tr>
<td>businessCategory</td>
<td>OAUTH2</td>
</tr>
<tr>
<td>codePage</td>
<td>0</td>
</tr>
<tr>
<td>company</td>
<td>Zebra</td>
</tr>
<tr>
<td>countryCode</td>
<td>0</td>
</tr>
<tr>
<td>department</td>
<td>Minnetonka</td>
</tr>
<tr>
<td>description</td>
<td>worker</td>
</tr>
<tr>
<td>displayName</td>
<td>zman1</td>
</tr>
<tr>
<td>distinguishedName</td>
<td>CN=zman1,OU=Users,OU=zebra,DC=PTTPRO,DC=ZEBRA</td>
</tr>
<tr>
<td>dSCorePropagationData</td>
<td>16010101000000.0Z</td>
</tr>
<tr>
<td>extensionAttribute5</td>
<td>TRUE</td>
</tr>
<tr>
<td>extensionAttribute7</td>
<td>wire,screws,nails</td>
</tr>
<tr>
<td>givenName</td>
<td>zman1</td>
</tr>
<tr>
<td>lastLogoff</td>
<td>0</td>
</tr>
<tr>
<td>lastLogon</td>
<td>13239837406244000</td>
</tr>
<tr>
<td>lastLogonTimestamp</td>
<td>13240511452972300</td>
</tr>
<tr>
<td>logonCount</td>
<td>22</td>
</tr>
<tr>
<td>memberOf</td>
<td>CN=Imprivata,DC=PTTPRO,DC=ZEBRA</td>
</tr>
<tr>
<td>name</td>
<td>zman1</td>
</tr>
<tr>
<td>objectGUID</td>
<td>(non string data)</td>
</tr>
<tr>
<td>objectSid</td>
<td>(non string data)</td>
</tr>
<tr>
<td>physicalDeliveryOfficeName</td>
<td>Eden Prairie</td>
</tr>
<tr>
<td>primaryGroupID</td>
<td>513</td>
</tr>
<tr>
<td>pwdLastSet</td>
<td>132393993097741000</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>zman1</td>
</tr>
<tr>
<td>sAMAccountType</td>
<td>805306368</td>
</tr>
<tr>
<td>sn</td>
<td>Zimmerman1</td>
</tr>
<tr>
<td>telephoneNumber</td>
<td>9525551212</td>
</tr>
<tr>
<td>title</td>
<td>Associate</td>
</tr>
<tr>
<td>userAccountControl</td>
<td>66048</td>
</tr>
<tr>
<td>userPrincipalName</td>
<td><a href="mailto:zman1@PTTPRO.ZEBRA">zman1@PTTPRO.ZEBRA</a></td>
</tr>
<tr>
<td>uSNChanged</td>
<td>4206643</td>
</tr>
<tr>
<td>uSNCreated</td>
<td>4173760</td>
</tr>
<tr>
<td>whenChanged</td>
<td>20200729155052.0Z</td>
</tr>
<tr>
<td>whenCreated</td>
<td>20200716185509.0Z</td>
</tr>
<tr>
<td>aCSPolicyName</td>
<td></td>
</tr>
<tr>
<td>adminCount</td>
<td></td>
</tr>
<tr>
<td>adminDescription</td>
<td></td>
</tr>
<tr>
<td>adminDisplayName</td>
<td></td>
</tr>
</tbody>
</table>
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 83.

1. In the center pane, both PTT Pro 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 83  Device User Attribute Mappings

2. The table below shows each of the required elements in the PTT Pro 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.
In the AD snippet, as an example, the following AD Attributes will be used.

3. Then to complete the table, populate the AD attribute values that will be relevant to the Profile Manager and PTT Pro transformation.
4. Once the Attributes and values to use are determined, the Profile Manager server can be configured.

**Figure 86** Profile Manager Attribute Transformations Mapping with Values

<table>
<thead>
<tr>
<th>Element</th>
<th>AD Attribute Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>givenname</td>
<td>zman1, 2, 3</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Zimmerman1, 2, 3</td>
</tr>
<tr>
<td>User Login</td>
<td>displayname</td>
<td>zman1, 2, 3</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
<td>Minnetonka</td>
</tr>
<tr>
<td>OAuthName</td>
<td>userprinciplename</td>
<td><a href="mailto:zman1@PTTPRO.ZEBRA">zman1@PTTPRO.ZEBRA</a></td>
</tr>
<tr>
<td>Group User Template</td>
<td>title</td>
<td>Associate</td>
</tr>
</tbody>
</table>

**Profile Manager**

<table>
<thead>
<tr>
<th>Element</th>
<th>AD Attribute Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>displayname</td>
<td>zman1, 2, 3</td>
</tr>
<tr>
<td>First name</td>
<td>givenname</td>
<td>zman1, 2, 3</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Zimmerman1, 2, 3</td>
</tr>
<tr>
<td>User Role Levels</td>
<td>employeetype</td>
<td>services</td>
</tr>
<tr>
<td>User Roles</td>
<td>extensionattribute</td>
<td>wire, screws</td>
</tr>
<tr>
<td>Organization</td>
<td>company</td>
<td>Zebra</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
<td>Minnetonka</td>
</tr>
<tr>
<td>Force Logout</td>
<td>extensionattribute</td>
<td>TRUE</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>businesscategory</td>
<td>OAUTH2</td>
</tr>
</tbody>
</table>

5. For each System being populated, PTT Pro and Profile Manager, click on each of the required fields. The Transformation field will prompt for the selected attribute to be entered.

**IMPORTANT:** The AD attribute is case sensitive. If the input attribute case does not match, the import job will fail.

6. Complete the transformations for the required fields in the PTT Pro and Profile manager sections.
Create an Import Job

Once the transformations have been identified, Creation of an Import job will add (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 88 Import Jobs Screen

2. Click Create Job.

Figure 89 Edit Job Screen

3. Create the job by entering the various fields required.
4. For the query, the Organization structure of AD must be entered correctly. Also 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 set properly, it may be set to run on a scheduled basis.

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

**Figure 90** Import Job History

<table>
<thead>
<tr>
<th>Dispatchers</th>
<th>Query name</th>
<th>Process State</th>
<th>Error</th>
<th>Start Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Deltas</td>
<td>Test4</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020</td>
</tr>
</tbody>
</table>

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

**Figure 91** Profile Manager Dispatcher History Status

<table>
<thead>
<tr>
<th>User/Group</th>
<th>Action</th>
<th>Process State</th>
<th>Error</th>
<th>Created On Time</th>
<th>Last Updated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>zman2</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:54 pm</td>
<td>07/17/2020 02:43:54 pm</td>
</tr>
<tr>
<td>zman1</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:54 pm</td>
<td>07/17/2020 02:43:54 pm</td>
</tr>
<tr>
<td>zman3</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:55 pm</td>
<td>07/17/2020 02:43:55 pm</td>
</tr>
</tbody>
</table>
Multiple Role Values from Attributes

**Figure 92** PTT Pro Dispatcher History Status

<table>
<thead>
<tr>
<th>User/Group</th>
<th>Action</th>
<th>Process State</th>
<th>Error</th>
<th>Created On Time</th>
<th>Last Updated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>zman2</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:49 pm</td>
<td>07/17/2020 02:43:49 pm</td>
</tr>
<tr>
<td>zman1</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:52 pm</td>
<td>07/17/2020 02:43:52 pm</td>
</tr>
<tr>
<td>zman3</td>
<td>new</td>
<td>SUCCESSFUL</td>
<td>-</td>
<td>07/17/2020 02:43:54 pm</td>
<td>07/17/2020 02:43:54 pm</td>
</tr>
</tbody>
</table>

7. If there are import errors, click on the ![icon](image) to reveal the JSON detail for each of the relevant users. **Figure 93** 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 94** shows attribute “extensionAttribute7” from the AD via an LDAP Browser.
Multiple Role Values from Attributes

**Figure 94**    “extensionAttribute7”

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>employeeType</td>
<td>Services</td>
</tr>
<tr>
<td>extensionAttribute5</td>
<td>true</td>
</tr>
<tr>
<td>extensionAttribute7</td>
<td>wire,screws</td>
</tr>
<tr>
<td>givenName</td>
<td>zman1</td>
</tr>
</tbody>
</table>

10. Yet, the actual attribute delivered to Profile Manager from AD is shown in the JSON log detail in **Figure 95**.

**Figure 95**    JSON Log

```json
    "department": "Minnetonka",
    "useraccountcontrol": "66048",
    "employeeType": "Services",
    "extensionAttribute7": "wire,screws",
    "extensionAttribute5": "true",
    "cn": "zman2",
```

**NOTE:** The attribute specified in Transformations should be “extensionAttribute7” and will fail 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 will reject the import.

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

**Figure 96**    Failed Provisioning Detail

```json
    },
    "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 will be provisioned into Profile Manager with the specified Roles. Then, at user sign-on, the Roles assigned in AD will be available to the user.

Figure 97  Role Selection
Role Level Selection

About this Chapter

This chapter covers the following topics.

- Introduction
- Dependencies
- Adding and Assigning Role Levels
- Applying the Role Level
- Device Operation

Introduction

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 will present 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.
Dependencies

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

1. 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 98  Edit Portal User Role

<table>
<thead>
<tr>
<th>Device User Role</th>
<th>View</th>
<th>Create</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permissions to view list of device user roles</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Create</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permissions to create device user roles</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Edit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permissions to edit device user roles</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permissions to delete device user roles</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

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

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

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

   The user will not see the Role Level Name, just the Roles that are 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 102**  Create Role Level (Fields Added)

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

**Figure 103**  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. Click “here” link to download the CSV template.

**Figure 104**  Bulk Import Role Level Dialog

3. Edit the template as shown in **Figure 105**.

**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 Roles is permitted.

**NOTE:** Role levels may be assigned to the users by CSV import or by AD Attribute assignment.
4. 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.

   **NOTE**: If a Role Level is currently assigned to one or more Users, an attempt to modify or delete the role Level will fail, generating an error.
Applying the Role Level

1. Once the Role Level is established, it may be applied to a Device User.
   In this example, the User will be assigned to the Role Level ‘Services’ in the User profile.

   **Figure 108**  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 will override the individual Roles. (Normally, if a Role Level is specified, then User Roles would be left blank.)

   **Figure 109**  User Roles and User Role Level Both Selected Dialog
In this case, **Services** will be assigned and the user will be prompted for **carryout** and **heavylift** when the sign-in occurs.

**Figure 110**  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 111**  Roles

![Role Selection](image)

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

<table>
<thead>
<tr>
<th>Role Level</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Carryout, Heavy Lift</td>
</tr>
<tr>
<td>Hardware</td>
<td>Screws, Wire, Nails</td>
</tr>
<tr>
<td>Mix</td>
<td>Carryout, Screws</td>
</tr>
</tbody>
</table>
The Role Level 'Mix' contains Roles from Hardware and Services producing this result.

Figure 112  Role Level Mix