Copyright

© 2019 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

December 12, 2019
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>B</td>
<td>12 December 2019</td>
<td>Updates for RRR delivery</td>
</tr>
<tr>
<td>A</td>
<td>June 2019</td>
<td>Initial release</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Copyright</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Revision History</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>About this Guide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Chapter Descriptions</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Notational Conventions</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Related Documents and Software</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Service Information</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Getting Started</td>
<td></td>
<td></td>
</tr>
<tr>
<td>About this Chapter</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Introduction to Zebra Workforce Connect Profile Manager</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Profile Manager Functions</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Interconnection Details</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Implementation Types</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Full Implementation</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Logging In to Profile Manager</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Main Screen in Profile Manager</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Customer Setup</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Creating a Customer</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Editing a Customer</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Deleting a Customer</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>System Controls Panel (Customer Dashboard)</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Navigating the Profile Manager Portal Dashboard</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Dashboard Quick Link Buttons</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Return to the Dashboard</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Required Information</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Icons</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Slider Switches</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Success and Error Messages</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Search and Filter Functionality</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>
Active Directory Import Management

Introduction ..................................................................................................................................... 55
Device User Attribute Mappings ..................................................................................................... 55
View Mappings ............................................................................................................................... 55
Add an Attribute or Constant ........................................................................................................ 56
Clear an Attribute Mapping ........................................................................................................... 57
Import Job Management .................................................................................................................. 57
View Import Jobs ........................................................................................................................... 57
Create Import Jobs ......................................................................................................................... 58
Edit Jobs ....................................................................................................................................... 59
Delete Jobs .................................................................................................................................... 60
Run Import Jobs ............................................................................................................................ 60
View Import Job History ................................................................................................................ 61
Import Job Notifications ................................................................................................................ 63
Introduction ..................................................................................................................................... 63
View Import Job Notifications ....................................................................................................... 63
Create Import Job Notifications .................................................................................................... 63
Edit Import Job Notifications ........................................................................................................ 64
Delete Import Job Notifications .................................................................................................... 64
Import Job Scheduler ..................................................................................................................... 65
Introduction ..................................................................................................................................... 65
View Import Job Schedules ............................................................................................................ 65
Create Import Job Scheduler ......................................................................................................... 66
Edit Import Job Schedulers ........................................................................................................... 67
Delete Import Job Schedulers ......................................................................................................... 67

Client Device Setup Using Telephony Manager and Profile Manager

Introduction ....................................................................................................................................... 69
Client Device Setup Using Telephony Manager and Profile Manager ............................................ 69
Overview - Telephony Manager Provisioning ................................................................................ 69
Prerequisites .................................................................................................................................... 69
Configure Telephony Manager Using a CSV File (automated option) ............................................ 70
Confirm Successful Import of Data from the CSV File ................................................................... 70
Manually Configure Telephony Manager (for technical support) ................................................ 71
Enter the Store / Site ID Information ............................................................................................ 71
Enter the PBX Information ............................................................................................................. 72
Add Department Information ......................................................................................................... 73
Enter PBX Extension Information ................................................................................................. 75
Configure Zebra Profile Manager .................................................................................................. 76
Confirm the End-to-End Configuration of Telephony Setup ....................................................... 76
Important Notes About Verifying Correct End-to-End Configuration ......................................... 79
Telephony Management
Introduction ..................................................................................................................................... 80
Extensions ...................................................................................................................................... 80
   View Extensions ........................................................................................................................ 80
   Refresh Extensions ................................................................................................................... 81
Extension Import Management ....................................................................................................... 81
Other Telephony Management Options .......................................................................................... 82

Profile Manager Licenses
Introduction ..................................................................................................................................... 83
About Licenses .......................................................................................................................... 83
   Profile Manager User Licenses ........................................................................................... 83
   Profile Manager Device Licenses ........................................................................................ 83
View Application Licenses ......................................................................................................... 83
Update Application Licenses ..................................................................................................... 84

JSON Configuration for the Workforce Connect Profile Client
JSON Configuration ........................................................................................................................ 85
About this Guide

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.
- **Active Directory Import Management** provides information on the bulk import of users, devices, and extensions.
- **Telephony Management** provides information on importing extensions.
- **Profile Manager Licenses** provides information on the device licenses for your enterprise.

Notational Conventions

The following conventions are used in this document:

- **Bold** text identifies
  - 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
• Numbered lists indicate sequential lists (e.g., those that describe step-by-step procedures).

---

**Related Documents and Software**

The following document also provides 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: [zebra.com/support](http://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: [zebra.com/support](http://zebra.com/support).

When contacting support, please have the following information available:

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

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

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

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

---

**Provide Documentation Feedback**

If you have comments, questions, or suggestions about this guide, send an email to EVM-Techdocs@zebra.com.
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 of
  - Device users
  - Extensions
• 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

Implementation Types

Standalone Implementation

The standalone implementation provides a single partition for Profile Manager. This implementation allows for a single WFC Profile Manager environment, with its own security and configuration settings and without other environment partitions.

Full Implementation

The full implementation provides multiple partitions for Profile Manager. This implementation allows for multiple WFC Profile Manager environments, each partition with its own security and configuration settings for each environment / partition.

Logging In to Profile Manager

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. Enter user ID, password, and customer ID.
3. Click Log in.

The Profile Manager portal appears. If incorrect credentials are entered, the Login dialog box displays an error message.

Main Screen in Profile Manager

Upon login to Profile Manager Portal, the left panel displays the Customers link and the right panel displays a Customers space where customer cards can be added, one card per customer.

If there is already a customer card in the right panel, it should look like the following.
Customer Setup

To manage a customer system with Profile Manager, first you must create an access point in the main screen of Profile Manager. These access points are called customers or customer “cards”. In Profile Manager, each customer must have its own customer card.

Creating a Customer

Prerequisites

Your own role must allow you to create Customers.

To create a Customer:

1. In the right pane of the main screen of Profile Manager, click +Add Customer.
   The Create Customer dialog box appears.

   Figure 4  Create Customer Dialog Box

   - Customer ID *
   - Name *
   - Description
   - Authentication Method *
     Select
   - * Required
   - Cancel  Create

2. Enter the required information and click Create.
   The following is an example of a card in the right panel of the main screen of Profile Manager.

   Figure 5  Customer Card in Right Panel
Editing a Customer

Prerequisites
Your own role must allow you to edit Customers.

To edit a Customer:

1. On the customer card for the customer you want to edit, click the pencil icon. The Edit Customer dialog box appears.

Figure 6  Edit Customer Dialog Box

2. Update the information and click Update.

Deleting a Customer

Prerequisites
Your own role must allow you to delete Customers.

To delete a Customer:

1. On the customer card for the customer you want to delete, click the trashcan icon. The Delete Customer dialog box appears.

Figure 7  Delete Customer Dialog Box

2. To cancel, click No. To continue, click Yes.
System Controls Panel (Customer Dashboard)

Just as there is a separate customer “card” for each customer, there is also a separate System Controls panel (customer dashboard) for each customer. To access the System Controls panel (dashboard) for a customer, click the arrow at the bottom right of the customer card for the customer you want to manage.

The following example shows the System Controls panel (dashboard) for the ACME XYZ customer. The customer whose dashboard you are viewing displays on the dashboard screen.

Figure 8  Customer Dashboard: System, Import, and Telephony Management Functions

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.

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:

- 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 9  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 1  Icons

<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>
</tbody>
</table>
Table 1  Icons (Continued)

<table>
<thead>
<tr>
<th>Permission Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 2  Slider Switch States

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

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.
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 own role must allow you to view portal user roles.

To view portal user roles:

From the dashboard, click Portal User Roles.

The Portal User Roles screen appears.
Create Portal User Roles

Prerequisites

Your own role must allow 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 own role must allow 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 15**   Edit Portal User Role Dialog Box

<table>
<thead>
<tr>
<th>Role Name</th>
<th>ACME_Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>ACME Permission</td>
</tr>
<tr>
<td>Permissions</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>View - Create - Edit - Delete - Bulk Import</td>
</tr>
<tr>
<td>Device Users</td>
<td>View - Create - Edit - Delete - Bulk Import</td>
</tr>
<tr>
<td>Device User Attribute Mappings</td>
<td>View - Create - Edit - Delete</td>
</tr>
<tr>
<td>Device User Roles</td>
<td>View - Create - Edit - Delete</td>
</tr>
<tr>
<td>Import Jobs</td>
<td>View - Create - Edit - Delete - Run Job - View History - View Job History Detail</td>
</tr>
<tr>
<td>Import Job Notifications</td>
<td>View - Create - Edit - Delete</td>
</tr>
<tr>
<td>Import Job Scheduler</td>
<td>View - Create - Edit - Delete</td>
</tr>
<tr>
<td>Licenses</td>
<td>View - Update</td>
</tr>
<tr>
<td>Portal Roles</td>
<td>View - Create - Edit - Delete</td>
</tr>
<tr>
<td>Portal Users</td>
<td>View - Create - Edit - Delete - Unlock - Reset Portal Users Password</td>
</tr>
</tbody>
</table>

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 own role must allow 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.

   Figure 16 Delete Portal User Role

3. Click Yes to delete.

Portal User Management

This section describes how to:

- Create portal users
- Update user roles for a portal user
- Delete portal users.

Create Portal Users

Prerequisites

- Your own role must allow 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.

**Figure 17** Create Portal User Dialog Box

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

**Edit Portal Users**

**Prerequisites**

Your own role must allow you to edit portal users.

To edit portal users:

1. From the dashboard, click **Portal Users**.
   The **Portal Users** screen appears.
2. Click the user you wish to edit. The Edit Portal User dialog box appears.

3. Update entries in the fields in the Create Portal User dialog box.

4. Click the slider switches to enable/disable the user role(s).

5. Click Update.

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

**Prerequisites**

Your own role must allow 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 how to:

• Create device user attributes
• Edit device user attributes.

Create Device User Attributes

Use this procedure to create device user attributes.

**Prerequisites**

Your own role must allow 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.

**Figure 21  Create Device User Attribute Dialog Box**

- Name *
- Display Name *
- UI Order *

Options:
- Required
- Unique
- Editable (on update)

Type *

Select

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

### Table 3  User Attribute Parameters

<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 <strong>Create Device User</strong> dialog box</td>
</tr>
<tr>
<td>UI Order</td>
<td>Sequence of where the attribute appears in the <strong>Create Device User</strong> dialog box</td>
</tr>
<tr>
<td>Required</td>
<td>Enable to make the attribute a required field in the <strong>Create Device User</strong> 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 **Edit** for the device user attribute you wish to edit.
   The **Edit Device User Attribute** dialog box appears.
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 own role must allow 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.
2. Click **Create Device User Role**.
   The Create **Device User Roles** dialog box appears.

**Figure 24**  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 4**  Settings for Ptt Pro Group

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>None</strong></td>
<td>A Device User Role is not created in Ptt Pro.</td>
</tr>
<tr>
<td><strong>Static</strong></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><strong>Dynamic</strong></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 own role must allow 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 🖋 for the device user role you wish to edit.
   The **Edit Device User Role** dialog box appears.

**Figure 25**  Edit Device User Role Dialog Box

3. Update the fields.
4. Click **Update**.

### Delete Device User Roles

**Prerequisites**

Your own role must allow you to delete device user roles.

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.
3. The Delete Device User Role dialog appears.
4. To cancel, click No. To continue, click Yes.

Device User Management

This section describes the following.

- License management Using Device User Management
- View device users
- Add and Update Device Users
- Add a Device User
- Edit a Device User
- Delete a Device User
- Refresh device users

License Management Using Device User Management

If your site is set up for device user licenses to allow device users to access the system, device users can be added, updated and deleted to control device user licenses. The procedures in this section describe device user license management.

View Device Users

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

Prerequisites

Your own role must allow you to view device users.

To view device users:
From the dashboard, click Device Users.

The Device Users screen appears.
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.

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

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

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

Prerequisites

- Your own role must allow you to bulk import device users.
- The import file must be CSV format.
- The device users to be synchronized must already exist in the database.
- The Profile Manager database is case sensitive. Review the CSV file before upload.

To import device users:

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

2. Click **Import Device Users**.
The **Bulk Import Users** dialog box appears.

**Figure 28** Bulk Import Users Dialog Box

![Bulk Import Users Dialog Box](image)

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 import.

### Add a Device User

Use this procedure to create device users.

**Prerequisites**

- Your own role must allow 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 29    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 own role must allow you to edit device users.

To edit device user roles:
1. From the dashboard, click Device Users.
   The Device Users screen appears.
2. Click for the device user you wish to edit.
   The Edit Device User dialog box appears.
3. Update the fields as in Add a Device User.
4. 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 own role must allow 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.

Figure 30  Delete Device User

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 Using Device Management
If your site is set up for device licenses to 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 own role must allow you to view devices.

To view devices:

From the dashboard, click Devices.

The Devices screen appears.

Figure 31   Devices Screen

---

Add/Enroll and Update Devices

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

There are two ways to add/enroll devices.

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

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

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

**NOTE** You can bulk delete devices using this procedure, by bulk 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 own role must allow 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 32** Bulk Import Devices Dialog Box

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

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

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

Add a Device

Your own role must allow 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.

**Figure 33**  Add Device Screen

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

**NOTE** Device Id usually is a unique combination of a device model and a device serial number (Example: TC51_111111111111111). 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 own role must allow 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 own role must allow you to delete/de-enroll devices.

1. To delete/de-enroll devices:
   - The Devices screen appears.
   - Click for the device to delete/de-
   - From the dashboard, click Devicesenroll.
   - The De-Enroll Device dialog box appears.

   ![De-Enroll Device Dialog Box](image)
   
   **De-Enroll Device**
   
   Are you sure you want to de-enroll the device?
   
   ![Yes/No Buttons]

   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, any the user's session of WFC Profile Client is ended automatically and the user is automatically logged out from 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.

   ![Refresh Button]

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 own role must allow you to create profile definitions.

To create profile definitions:

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

   **Figure 35**  Profile Definitions Screen

   ![Profile Definitions Screen](image)

   2. Click **Create Profile Definition**.
      The **Create Profile Definition** dialog box appears.
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 own role must allow 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 own role must allow 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 own role must allow 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.
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>Table 5 Profile Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Profile Definition</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 own role must allow 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 own role must allow 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 38**  Rules Screen

![Rules Screen Image]

**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.
2. Click **Create Rule**.
   The **Create Rule** dialog box appears.

3. Enter a name in the **Name** field.
4. Enter a description in the **Description** field.
5. Click **Next**.
   The **Event** screen appears.
6. Select options for User Actions, Automation, and Location Events.

7. Click Next.
   The Conditions screen appears.

Figure 42  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.
12. Select actions.
13. Select users.
14. Click **Create**.

The new rule is created.

**Publish Rules**

**Prerequisites**

You own role must allow you to publish rules.

To publish rules:

1. From the dashboard, click **Rules**.
   
   The **Rules** screen appears.

**Figure 44**  Rules Screen

2. Click **Publish**.

   The **Publish Rules** dialog box appears.
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.

2. Select the checkbox for the rule(s) you wish to delete.
   The Delete Rules button appears.
3. Click **Delete Selected Rule(s)**. The rule(s) are deleted.

---

**System Report Management**

The **System Reports** function provides historical reporting of actions performed in the Profile Manager portal. This section describes how to:

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

**Generate Reports**

**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 49** Generated Report

---

**Export Reports**

**Prerequisites**

- Your own role must allow 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 own role must allow 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.

Figure 50  Create Saved Report
Edit Report Templates

Prerequisites
Your own role must allow 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 own role must allow 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.
Introduction

This chapter describes how to manage:

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

Device User Attribute Mappings

View Mappings

Prerequisites

Your own role must allow 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.
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 own role must allow 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.
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**

**View Import Jobs**

**Prerequisites**

Your own role must allow 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 own role must allow 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.
3. Use the following table to complete the fields in the Create Job dialog box.

**Table 6  Create Job Dialog Box Fields**

<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>Active Directory Search Scope</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 own role must allow 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 55** 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 own role must allow you to delete jobs.

To delete jobs:

1. From the dashboard, click **Import Jobs**.
   The **Import Jobs** screen appears.
Active Directory Import Management

2. Click next to the job you wish to delete. The **Delete Job** dialog box appears.
3. Click **Yes** to delete.

Run Import Jobs

**Prerequisites**
- Your own role must allow 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 for the job you wish to run. The **Run Job** dialog box appears.

**Figure 56** Run Job Dialog Box

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

View Import Job History

**Prerequisites**
Your own role must allow 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.
Actions available on the Import Job History screen are view details, view deltas, and view dispatcher.

1. Click to view details.
2. Click View Deltas to view more information.

The Deltas dialog box appears:

3. 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:
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 own role must allow you to view import job notifications.

To view import job notifications:

From the dashboard, click Import Job Notifications.

The Import Job Notifications screen appears.

Create Import Job Notifications

Prerequisites

- Your own role must allow 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 61**  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 own role must allow 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 own role must allow 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 62  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 own role must allow you to view import job schedulers.

To view import job schedulers:

From the dashboard, click Import Job Scheduler.

The Import Job Scheduler screen appears.
Create Import Job Scheduler

Prerequisites

Your own role must allow 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.
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 own role must allow 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 own role must allow you to delete an import job scheduler.

To delete import job schedulers:
1. From the dashboard, click **Import Job Scheduler**.

2. Click 🗑️ for the scheduler you wish to delete.

3. The **Delete Scheduler** dialog box appears.

**Figure 65** Delete Scheduler Dialog Box

![Delete Scheduler Dialog Box](image)

---

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
- Overview - Telephony Manager Provisioning
- 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

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.

Overview - Telephony Manager Provisioning

Prerequisites

There must be a customer ID set up for the client device(s) you are configuring.

Relationships Between Ptt Pro, Telephony Manager and Profile Manager

The following diagram is an overview illustrating a sample configuration and the relationships between Ptt Pro, Telephony Manager, and Profile Manager configuration elements.
After the Telephony Manager provisioning is completed successfully, the events for the device user are represented in the final column of the diagram (rows 4 and 5 in the diagram).

**Figure 66** Relationships of Data - From Subsystems to Device User

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

**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.
• 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 67**  The Update Store Screen

   ![Update Screen](image)

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

**Figure 68** 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 69** 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 70**  Sample PBX Entries

![Sample PBX Entries](image)

### 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 7**  Department Information - Establishment in Zebra Profile Manager Ecosystem

<table>
<thead>
<tr>
<th>Telephony Manager</th>
<th>Profile Manager</th>
<th>PBX</th>
<th>Workforce Connect Profile Client Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>must match ---&gt;</td>
<td>--- must match</td>
<td></td>
<td>As a result of device activation on PBX--</td>
</tr>
<tr>
<td>Department</td>
<td>User Role/Department</td>
<td>---</td>
<td>---&gt; User Role/Department is populated into the WFC Client Device from Profile Manager</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.
1. Select the Store ID and Enter the Department Name and Description.

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.
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.

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.
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.

Confirm the End-to-End Configuration of Telephony Setup

1. On a client device, log into WFC Profile Connect as the user whose User Profile you want to confirm.
   In this procedure, the example shown is for user Joe Mechanic.
2. During login, at the Profile Client Role Selection Screen, select Switch Roles.

The Role 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.

1. The Roles presented to the User, which are defined in the User Profile
2. 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.
3. At Rule Evaluation Time, all rules are evaluated.

1. **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 own role must allow you to view extensions.

To view extensions:
From the dashboard, click Extensions.
The Extensions screen appears.
Refresh Extensions

Prerequisite

Your own role must allow 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 own role must allow 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.
Profile Manager Licenses

Introduction

This chapter describes following.

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

About Licenses

Profile Manager User Licenses

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

The system administrator must manually control which users are enabled to be provided the user licenses.

Profile Manager Device Licenses

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

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

View Application Licenses

Prerequisite

Your own role must allow you to view application licenses.

To view licenses:

From the bottom of the dashboard, click License. The Licenses screen appears.
Update Application Licenses

Prerequisite

Your own role must allow 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.
This chapter describes how to configure the JSON format for the WFC Profile Client.

JSON format example:

```
{
  "customer_id": "847",
  "sfs_url": "wss://pttpro.zebra.com/mqtt",
  "log_level": "Verbose",
  "confirm_role": true,
  "site_id": "8002",
  "config_settings": 0/1/2
}
```

To configure the JSON format:

1. Prepare JSON in above format with required parameters as desired for the above keys ("customer_id","sfs_url","log_level","site_id") in the JSON file.

2. Push the JSON file created, either directly or by `adb` command:
   ```sh
   adb push C:\Users\xyz2452\Desktop\filename /sdcard/
   ```

3. Install WFC Profile Client, allow permissions, and broadcast the following Intent using an `adb` command:
   ```sh
   adb shell am broadcast -a "com.zebra.dfs.ACTION_NEW_CONFIG" --es profile_uri /sdcard/filename
   ```
   - If "config_settings" parameter is 0, the settings are visible and editable.
   - If "config_settings" parameter is 1, the settings are visible but not editable.
   - If "config_settings" parameter is 2, the settings are not visible and not editable.

4. Replace filename above with created JSON filename.