Profile Manager

Workforce Connect

Provisioning Guide

MN-004414-04EN Rev A

Copyright

2022/10/10

Terms of Use

Proprietary Statement

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

Product Improvements

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

Liability Disclaimer

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

Limitation of Liability

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

Contents

About this Guide..... 6

Chapter Descriptions..... 6

Notational Conventions..... 6

Icon Conventions..... 7

Service Information..... 7

Revision History..... 7

Getting Started..... 8

Provisioning Architecture..... 9

File Import Functional Architecture..... 10

Operational Process Flow..... 11

Flat File Import Outline..... 11

Outline of AD and ADFS Import Process..... 12

Flat File Import Process..... 14

Profile Manager Proxy..... 17

User Classifications..... 17

Standard Site User..... 18

Virtual Site User..... 18

Transient User..... 18

Allowed and Disallowed Sites..... 19

Allowed Sites..... 19

Disallowed Sites..... 20

Virtual Sites....20
Sticky Element Concept....20
Dynamic Ad-Hoc User Provisioning....20
Dynamic Profile Client Configuration....22

Flat File Import File Creation....24
Site Map CSV File....24
User Import CSV File....26
User Import CSV Column Heading Requirements....26
User Assumptions on Importing CSV....27
Sample CSV User Import File....27
CSV User Import File Definition Table....27
Servers Setup Information....29
Configuration Elements....30
General Customer Profile....30
LDAP Configuration Elements....31
Flat File General Configuration Elements....32
Flat File Dynamic Ad-Hoc User Provisioning AD Connector Elements....33
Flat File Dynamic User Provisioning Access Token Attributes....33
Flat File Encryption Elements....34
Flat File Site Map Configuration Elements....35
GCP Cloud Storage Container....36
SFTP Cloud Storage Container....36
Profile Manager Proxy Configuration....37

Attribute Transformations....38
AD Attributes Identification....38
Creating Attribute Transformation Definition....40
Evaluating AD Attribute Transformation....40
Configuring Flat File Attribute Transformations....43

Import Process....44
Import Job Dependencies....44

Create WFC PTT Pro Departments....44
Create Roles and Role Levels....45
AD and ADFS Query....46
GCP Bucket and SFTP File Repository....48
Creating an Import Job....49
Reviewing Import Job Status....50
Import Job Status....52

Direct Console Import....53
Sample Populated CSV File Template....54

About this Guide

The Profile Manager (PFM) platform can import, or provision users into PFM as well as Zebra PTT Pro. This functionality has been expanded from provisioning users from AD/ADFS to provisioning users from a text file.

This document is focused on user provisioning and attribute transformation aspects provided by PFM and does not address user authentication.

Chapter Descriptions

- About this Guide explains document convention and service information.
- Getting Started explains import architecture and operation process flow..
- Flat File Import File Creation explains flat file import and creation process.
- Attribute Transformation explains attribute transformation using AD connector.
- Import Process explains flat file creation an, department creation, and import job creation.
- Console Import Process explains the different services and console import process.

Notational Conventions

The following conventions are used in this document:

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

- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

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

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

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

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

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

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

Service Information

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

When contacting support, please have the following information available:

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

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

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

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

Revision History

Revision	Date	Description
MN-004414-01EN	12/2021	Initial Release.
MN-004414-02EN	03/2022	Added PFM Proxy Configuration.
MN-004414-03EN	05/2022	Updated Pro Server ID.
MN-004414-04EN	10/2022	Added a note in Import Job Status.

Getting Started

In a Profile Manager and Zebra PTT Pro environment fully integrated with an Identity Provider (IDP) solution, such as AD/ADFS, the IDP connection provides three fundamental functions:

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

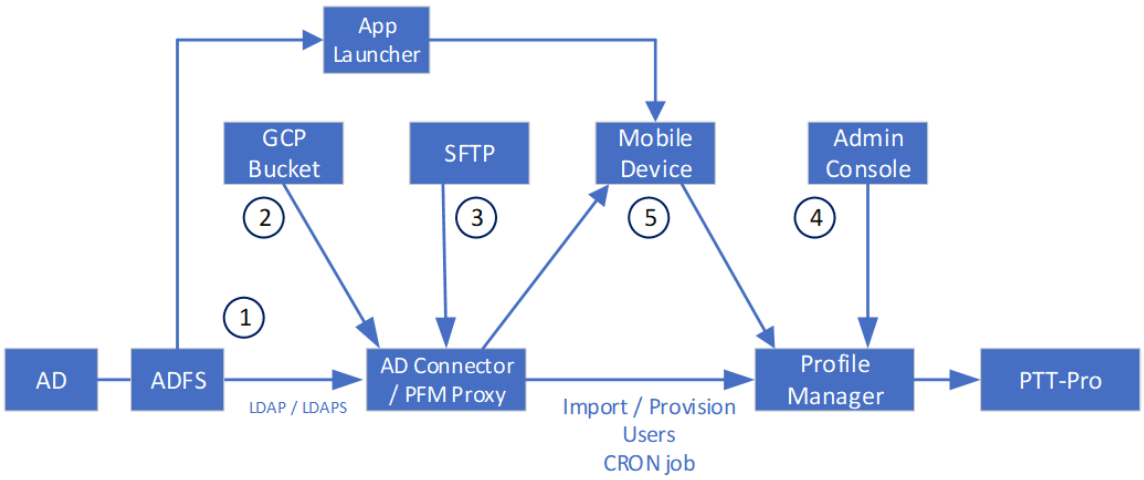
When the WFC environment is fully integrated with AD/ADFS, all three functions are available. In some deployments, the customer may not support LDAP/LDAPS services and the PFM access to the AD database is not available for user provisioning and attribute transformations.

Providing a flat file user import function provides flexibility for environments that do not support LDAP/LDAPS. A flat file import capability supports user provisioning and attribute transformations but does not address user authentication.

Provisioning Architecture

There are several methods of providing the user provisioning and attribute transformation functions. Shown in this diagram is the general system architecture.

Figure 1 Provisioning Architecture for Profile Manager and PTT Pro



1	Existing LDAP connection to ADFS. User database is read and evaluated by an LDAP query created in Profile Manager. The Import job is scheduled for automatic updates. This method provisions users into Profile Manager and PTT Pro server. Provides attribute transformation for role selection presentation.
2	Import flat file from cloud-based GCP bucket. The import is scheduled for automatic update. This method provisions users into Profile Manager and PTT Pro server. Provides attribute transformation for role selection presentation.
3	Import flat file from cloud-based SFTP service. The import is scheduled for automatic update. This method provisions users into Profile Manager and PTT Pro server. Provides attribute transformation for role selection presentation.
4	Manually enter each user into Profile Manager and PTT Pro Server. Is a one-at-time time activity initiated by the administrator and does not provide automated updates. Provides attribute transformation for role selection presentation.
5	Import dynamic-ad-hoc device by passing the token for a user who is authenticated to the IDP with the APP Launcher. The validated identity of the user is to the PFM Proxy service along with the information which is retrieved from the Access Token. The PFM Proxy Provides the server connection related information.

Reviewing the five provisioning methods:

- Method 1 is the most common and is available to any customer supporting AD/ADFS's LDAP services. Connection to an AD/ADFS environment provides user provisioning, attribute transformations, and user authentication. A PFM import job can be scheduled for regular user provisioning updates.
- Methods 2 and 3 are new functions and use the same approach for user provisioning and attribute transformations. The same comma-separated value (csv) file construct is used for either the GCP or

SFTP method. The file repository is either a customer hosted Google Bucket or an SFTP site. An import job can be scheduled for regular user provisioning updates.

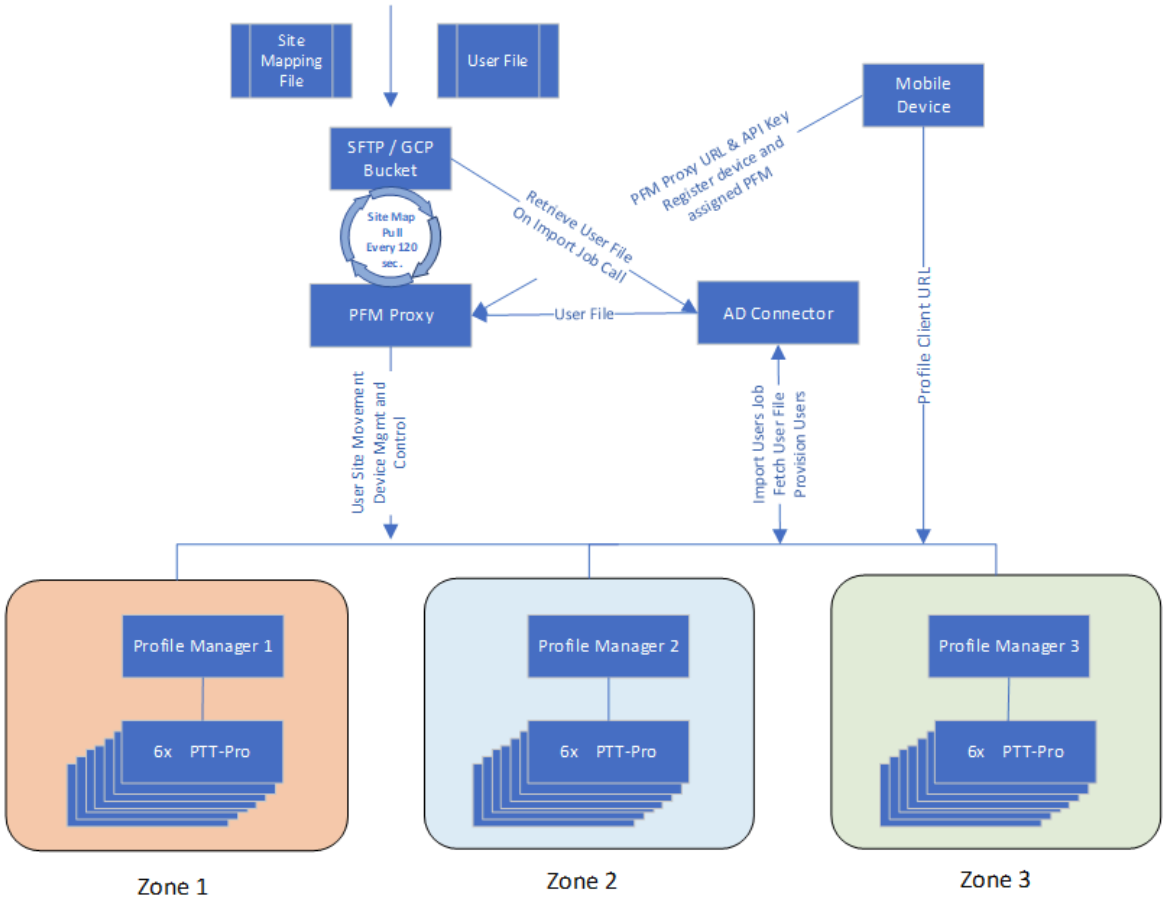
- Method 4 is a legacy approach to user provisioning. It is a manual, single event method. It is documented here for completeness.
- Method 5 is a new function that allows ad-hoc provisioning for users who are not added by the User Import csv file. This capability is provided by a returned JWT Access Token from the IDP to an authenticated device user. After the user successfully signs-in through the App Launcher, UserID and SiteID are captured and combined with additional elements found in the received Access Token. This combined information allows user successfully provisioning into the system at the correct site and server.

File Import Functional Architecture

The following diagram shows the functional components of the system. This example environment is characterized by three Business Operational Zones, perhaps characterized by a geographic organization with East, Central, and West regional zones.

Each region is characterized by a Profile Manager Tenant, and up to six Zebra PTT Pro instances. To import users into this configuration, the user Import and site mapping csv files are located in a file repository, a GCP Bucket, or an SFTP Folder or in two separate repositories. The user import file is the complete population of Workforce Connect users across all three regions. The site mapping file determines the following:

- Which Profile Manager server is populated
- Which of the six Zebra PTT Pro servers to place the user
- The site (Zebra PTT Pro Department) to populate the user



Operational Process Flow

To help understand the differences in the user provisioning methods, the following compares the flat file import with the AD/ADFS process.

Because of the similarities between the two processes, the flat file import is described first then the AD attribute analysis. The Profile Manager operations are nearly identical for both processes.

Flat File Import Outline

Use the outline to perform tasks in the proper order when you use the import file process to create users and sites in Profile Manager and Zebra PTT Pro.

1. Analyze the AD user database to identify useful user attributes for attribute transformations.
2. Create the user import file.
   - Use a file name that indicates the file contents. The file name is specified in the import job.
   - Encrypt the user import file.

3. Create the site mapping file.
    - Use the file name agreed upon with your Zebra administrator. The name of the site mapping file is embedded in the Profile Manager database configuration and cannot be changed.
    - Encrypt the site mapping file.
4. Copy the user import and site mapping files to the GCP or SFTP file repository.
5. Verify that Zebra PTT Pro includes the departments (sites) that are populated with users during the import process. If the departments are not present, create the departments prior to import. Note that department names are case-sensitive.
6. Configure Profile Manager.
    - Create the User Roles and Role Levels as defined in the user import file.
    - Create the attribute transformations.
        - Zebra PTT Pro
        - Profile Manager
        - Specify the import file column headers, maintain case sensitivity.
    - Create the import job.
        - Name the job.
        - Specify whether to import into Profile Manager, Zebra PTT Pro, or both.
        - Specify the name of the encrypted user import file
    - Run the import job.
    - Review the job logs.

NOTE: In the PFM Proxy environment with multiple PFM Servers, the Import Job is executed only from a designated PFM server. The AD Connector and PFM Proxy are responsible for populating all the PFM and PTT Pro Servers in the environment.

Outline of AD and ADFS Import Process

Use the outline to perform tasks in the proper order when you import users and sites from AD and ADFS.

1. Analyze the Active Directory user database and identify useful user attributes for attribute transformations.
2. Verify that Zebra PTT Pro includes the departments (sites) that are populated with users during the import process. If the departments are not present, create the departments prior to import. Note that department names are case-sensitive.

3. Configure Profile Manager:
    - Create the User Roles and Role Levels as defined in the user import file.
    - Create the attribute transformations.
        - Zebra PTT Pro
        - Profile Manager
    - Create the import job.
        - Name the job.
        - Select the scope.
        - Specify whether to import into Profile Manager, Zebra PTT Pro, or both.
        - Specify the LDAP query.
        - Define the query filter.
    - Run the import job.
    - Review the job logs.

Flat File Import Process

The following ladder diagrams show the sequence of events for Importing users into the environment and the elements involved with the device sign-on.

Figure 2 Importing User Logical Sequence

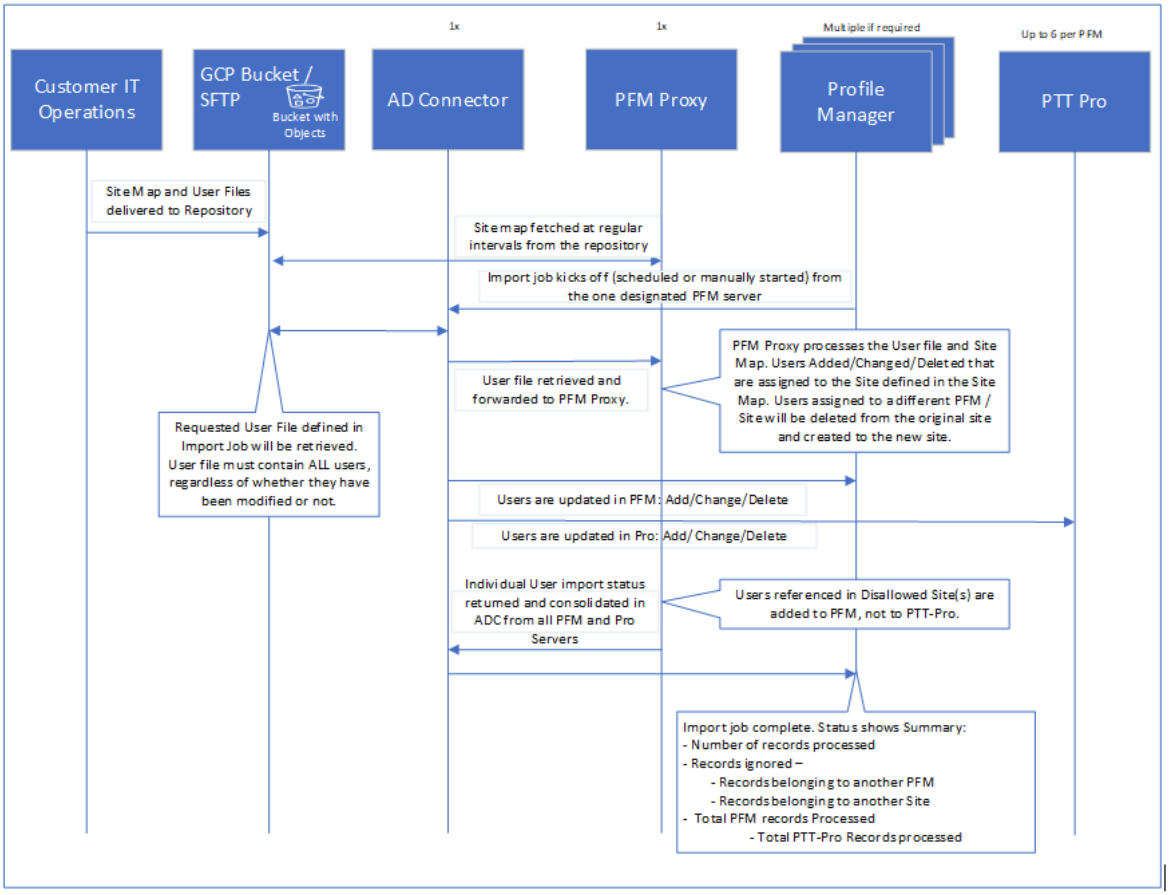
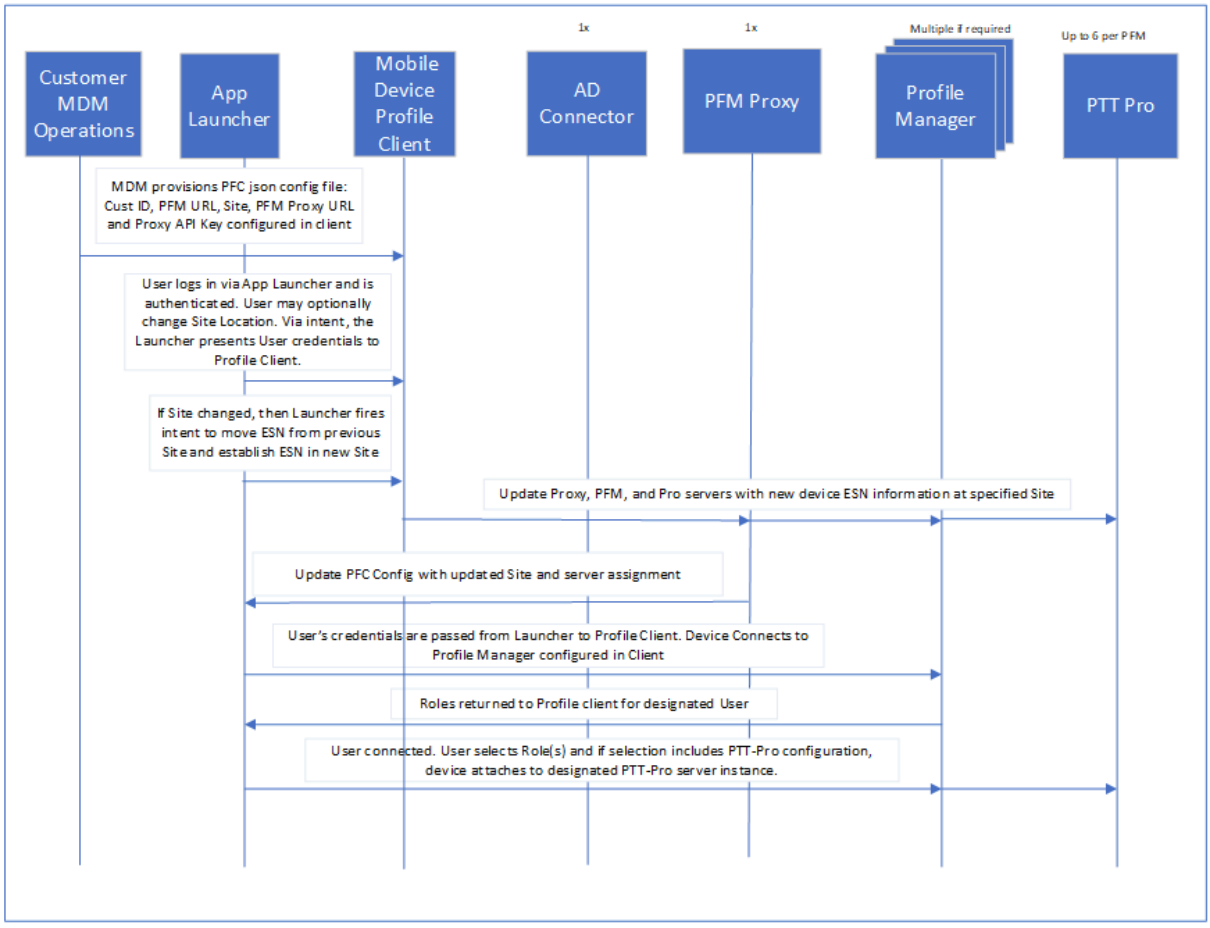


Figure 3 Device Connection Logical Sequence



Profile Client JSON configuration file which is mentioned in the flow diagram is shown below. The Proxy URL and the Proxy API Key are two new elements described later in this document.

NOTE: All the devices across the Enterprise deployment can use one configuration file when the PFM Proxy service is used.

```
{
    "customer_id": "20",
    "sfs_url": "https://<pfm-server1>",
    "proxy_url": "https://<pfm-proxy-server>",
    "proxy_url_api_key": "<api_key>",
    "site_id": 199,
    "log_level": "debug",
    "confirm_role": false,
    "power_connected_logout": false,
    "log_file": true,
    "config_settings": 0
}
```

The Launcher issues a broadcast intent to initiate the login process of the Profile Client which is included in the JWT Access Token intent. For more information about Intent details, refer to the Profile Client Configuration and Programmer Guide.

Profile Manager Proxy

Profile Manager Proxy (PFM Proxy.), a powerful feature recently added to the Profile Manager environment. This service contains several compelling features and is required for the Enterprise to support a large-scale deployment when multiple Profile Manager Servers are required to support the deployment.

For supporting Flat File User Deployment in a collection of Profile Manager and PTT Pro servers, the Proxy provides the ability to move mobile users between PTT Pro cluster instances in the Profile Manager server environment.

Beyond the import capability, the administrator can define users and how the collection of Enterprise Users are added to the WFC system. PFM Proxy Services also provide the system administrator the ability for Users to move from Site to Site without any administrative intervention. Further, users who are not populated in the system can be added dynamically to the WFC system without administrative intervention.

NOTE: To support the PFM Proxy and all the services the Profile Client must be 2.0.21402 or later

The following pages describe these advanced features:

- User Classifications
- Allowed and Disallowed Sites
- Virtual Sites
- User's Sticky Element
- Dynamic Ad Hoc User Provisioning
- Dynamic Profile Client Configuration

User Classifications

The WFC System supports three classifications of users. The User classifications are a way of stating use cases and an operation description rather than a system setting. These classifications describe how users are handled during the import and Sign-In process, the details are described below:

- Standard Users
- Virtual Users
- Transient Users

The User Classification aspect is key to understand because of the interaction with the features that follows the :

- Allowed/Disallowed Sites,

- Virtual Sites,
- Sticky Element,
- Dynamic Ad Hoc User Provisioning.

Standard Site User

A PFM User is enrolled to a specific PTT Pro Site with all the capabilities of any PTT Pro user. This User is an employee who is essentially assigned to a specific physical site location and is not expected to initiate a move from site-to-site. The WFC system does support moving a Standard User to other sites through daily user import job, for example, during a job change. The assumption with a Standard User is assigned and remained in a physical site.

Virtual Site User

A Virtual User is one who may at any time move from one Site to another within a Region of Sites connected or related in some business function. During the original user import, the Virtual User is initially assigned to a Virtual Site, which is a holding the site within the collection of PFM and PTT Pro servers assigned to the region

The Virtual User is initially imported into the system to a Virtual Site. When the Virtual Users visit a physical site, they sign-in using one of the site's devices which is configured specifically for that Site. The WFC System then knows which site this Virtual User is now located, and moves the User from the Virtual Site, or their previously visited site, into the current physical site. Then, as the Virtual User moves to another site and signs-in, the Virtual User is moved to that new Site.

If a Virtual User's Sticky element setting is set to 'yes' then the Users remains at their currently registered site during the daily User File Import process. If the Sticky element is set to 'no', then the users are moved back into their originating Virtual Site.

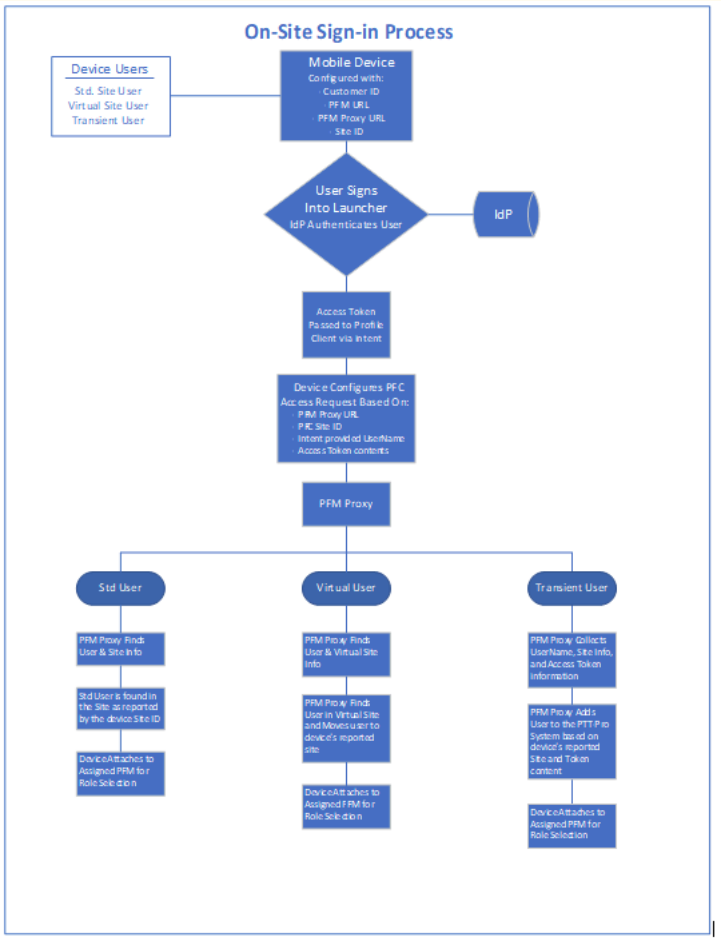
Transient User

A Transient User is also known as Corporate User, exists within the Enterprise's IDP and is a valid user who is populated in the PFM server but not populated in the PTT Pro server during the csv import process. These users require occasional WFC System activation when visiting a remote Site, and they are purged from the PTT Pro system during the daily import process.

The Transient Users, like Standard and Virtual Users, need to be authenticated by the enterprise's IDP system. Once authenticated, they are dynamically added to the system at the Site, they are visiting based on the configuration of the Site's mobile device. As opposed to Standard and Virtual Users, Transient Users only exist within the Profile Manager system during sign-in and based on the device and access token information they are then added to the PTT Pro system.

The following diagram differentiates the operation based on the three User Classifications during the sign-in process.

Figure 4 On-slte Sign-in Process



Allowed and Disallowed Sites

There are two categories of Site definitions: Allowed and Disallowed Sites. Since the User import file can represent the enterprise's entire user database, both WFC System users as well as non-WFC users, the Allowed / Disallowed logic provides a mechanism to determine which users are added to the PTT Pro system. Each user's record in the user's import file requires a Site ID, and during the Import process, users with a site matching a Disallowed Site are added to the Profile Manager system and are not added to the PTT Pro system.

NOTE:

Any Site referenced in the User File must be included in the Site Map File. Failure to include in the Site map creates ambiguous error messages during the import process.

Allowed Sites

- All sites, unless other specified as disallowed, are Allowed Sites.
- The Allowed Sites are defined in the Site Map File.

- When the User import file is interrogated, the users who are mapped to these sites are automatically added to and become PTT Pro Site Members.
- These sites can be actual sites or Virtual Sites.

Disallowed Sites

- Disallowed Sites are defined in the general configuration of the PFM Proxy.
- During the User Import process, Users who are specified in a Disallowed Site list are added to the Profile Manager system and are not added to the PTT Pro system.

Virtual Sites

Virtual Sites are non-physical sites for Virtual Users who move from one site to another site, they are not assigned to a physical site. Users are added to the Virtual Site during the User Import process. Pre-populating Users in the appropriate PFM server and PTT Pro instance minimizes the login time, allowing the system to perform a simple move as opposed to the more complex User Deletion and Addition.

Upon system Sign-in, the actual physical site information that is reported by the site device back to the system, the Virtual Users are moved to that site. The Users are then able to participate in WFC communication with others in the site as specified by the PTT Pro Configuration.

In conjunction with the Sticky Element

- If the Virtual User Sticky = yes, then at the next User import the User remains populated in currently established Site. During the User's subsequent sign-in, if in a different site, the device site configuration information determines if the User is to be moved to the new site or to remain in the existing site.
- If the User Sticky = no, then at next User import – assumed to be one time per day – the users are returned to the Virtual Site. When the Users sign-in at a site, the device configuration information causes the users to be moved from the Virtual Site to the Actual Site.

Sticky Element Concept

A capability provided in the Profile Manager environment allows addition of users into the WFC system who may not be permanently assigned to a designated site or may roam between several sites. Among three types of users, the Sticky Element applies only to the Virtual Users.

Virtual Users originate in a Virtual Site but are populated in the Physical Site for many days. In this scenario, they should be considered Sticky. If they are defined as non-Sticky, during next user import process, the Virtual Users are simply returned to their originating Virtual Site. Virtual Users dynamically move to other sites when the other users arrive at a new site and sign-in the new site's device. Upon successful sign-in, the users are removed from the previous site and added to the current site.

Dynamic Ad-Hoc User Provisioning

The User Import Process adds users to the WFC system, populating them in the correct site during sign-in and usage. Ad-Hoc Provisioning is intended for Transient Users who are authenticated against the IDP and are not included in the User File Import Process, to be dynamically added to the WFC system.

This capability is provided through the User's IDP-Login Process, through the implementation of a Launcher App, and successfully authenticating and receiving an access token. The Launcher app is responsible for passing token information to the Profile Client. In conjunction with information available in the Profile

Client, the claims set in the JWT Access Token may have additional information to better refine the User's Provisioning detail to be added to a site on-the-fly.

The Access Token should include the following information. If this information is not in the token then default values configured in the PFM Proxy is used.

- Firstname
- Lastname
- UserRoleLevel
- Userroles
- OauthName
- Authentication Method
- ForceLogout

The UserName, Site ID, PFM Proxy URL, and the PFM Proxy API key exist in payload from Profile Client running on the mobile device. The additional required information to dynamically add the user is extracted from the JWT Access Token. The Sticky element does not apply for the Transient User and is logically 'no'. Meaning at the User Import job, the Transient user is removed from the PTT Pro site.

To support dynamic Ad-Hoc User Provisioning, based on the user details in the access token, the users are created in Profile Manager and PTT Pro. Field names in the access token may be different from the column header names in the usermap csv file. The following attributes mapping is used to transform the JWT Access Token attributes to usermap column header attributes.

Table 1 Access Token Attributes

userKey	tokenKey	Description
firstName	fname	If empty, the value is set the "UserName".
lastName	lname	If empty, the value is set the "UserName".
uswerRoleLevel	rolelevel	Default Value: <empty>
UserRoles	role	Default Value: admin
oauthName	sub	If empty, the value is set the "UserName".
authenticationMethod	auth	Default Value: OAUTH2s
forceLogout	flogout	Default Value: True
objectClass	objectclass	Default Value: person

It is important for the Integration Consultant to provide Zebra with appropriate and meaningful default values for elements missing in the Access Token.

When working with Access Tokens, two tools are helpful to extract and decrypt the token. Postman can be downloaded from https://www.postman.com/ and provides the ability to collect a token. Then the Access Token can be decoded by browsing to https://jwt.io and pasting the token into the interface.

The following is a sample of additional information provided in an Access Token.. The token claims area displays the claim information for the User are shown in the example below:

```
{
"scope":"openid profile email",
```

```
"sid"
```

In the PFM Proxy configuration, there is a table to be populated with the elements retrieved from the Access Token.

```
ENERAL_USERATTRIBUTESLIST_0_USERKEY: FirstName
GENERAL_USERATTRIBUTESLIST_0_TOKENKEY: given_name

GENERAL_USERATTRIBUTESLIST_1_USERKEY: LastName
GENERAL_USERATTRIBUTESLIST_1_TOKENKEY: family_name

GENERAL_USERATTRIBUTESLIST_2_USERKEY: UserRoleLevel
GENERAL_USERATTRIBUTESLIST_2_TOKENKEY: rolelevel
GENERAL_USERATTRIBUTESLIST_2_DEFAULTVALUE: ""

ENERAL_USERATTRIBUTESLIST_3_USERKEY: Userroles
GENERAL_USERATTRIBUTESLIST_3_TOKENKEY: role
GENERAL_USERATTRIBUTESLIST_3_DEFAULTVALUE: "

GENERAL_USERATTRIBUTESLIST_4_USERKEY: OauthName
GENERAL_USERATTRIBUTESLIST_4_TOKENKEY: email
GENERAL_USERATTRIBUTESLIST_4_DEFAULTVALUE: ""

GENERAL_USERATTRIBUTESLIST_5_USERKEY: AuthenticationMethod
GENERAL_USERATTRIBUTESLIST_5_TOKENKEY: auth
GENERAL_USERATTRIBUTESLIST_5_DEFAULTVALUE: “OAUTH2”

GENERAL_USERATTRIBUTESLIST_6_USERKEY: ForceLogout
GENERAL_USERATTRIBUTESLIST_6_TOKENKEY: flogout
GENERAL_USERATTRIBUTESLIST_6_DEFAULTVALUE: "TRUE"
```

As shown in this table, for each of the 7 attributes the **UserKey** field must match with csv column header in the User Import file. (This field is case-sensitive). This is also the string value entered in the configuration for Profile Manager and PTT Pro Transformations configuration.

The **TokenKey** is the element name for the attribute in the Access Token.

The **DefaultValue** element is the value which is inserted into the **UserKey** field if the Token does not provide the information.

Dynamic Profile Client Configuration

For the enterprise that requires multiple Profile Managers to support many sites, the new benefit of the PFM Proxy is having one Profile Client configuration. When implemented with a launcher, the Site Map in the PFM Proxy dynamically reconfigures the Profile Client to attach to the correct Profile Manager and PTT Pro instance. Consider the following example.

Original Profile Client Config

```
{
```

```
    "customer_id": "20",
    "sfs_url": "https://<pfm-server1>",
    "proxy_url": "https://<pfm-proxy-server>",
    "proxy_url_api_key": "<api_key>",
    "site_id": 199,
    "log_level": "debug",
    "confirm_role": false,
    "power_connected_logout": false,
    "log_file": true,
    "config_settings": 0

}
```

This WFCDFSConfig.json file can be loaded in all devices throughout the deployment.

When the User signs into the device Launcher, among other elements, the Launcher sends the Site ID to the Profile Client via intent. The Site ID is updated in the JSON file and the device connects to the PFM Proxy.

The PFM Proxy has a listing of all the Sites and responds back to the Profile Client with the correct PFM URL (sfs_url) and the PFM Tenant ID (customer_ID). The Profile Client configuration is dynamically updated for the correct server connection.

```
{
    "customer_id": "21",
    "sfs_url": "https://<pfm-server2>",
    "proxy_url": "https://<pfm-proxy-server>",
    "proxy_url_api_key": "<api_key>",
    "site_id": 299,
    "log_level": "debug",
    "confirm_role": false,
    "power_connected_logout": false,
    "log_file": true,
    "config_settings": 0

}
```

The Device then attaches to the correct servers and the user is presented with their appropriate Roles and configuration.

NOTE:

For this functionality to work across multiple PFM Servers and PTT Pro Clusters, the serial number for the device must be present in each Profile Manager and PTT Pro Cluster.

Flat File Import File Creation

To successfully provision the users through csv files, two files are required:

1. The Site Map File
2. The User Import file

Details of these file requirements are described in the following sections.

Site Map CSV File

The Site Map File determines the Profile Manager and Zebra PTT Pro server in which to provision users. In each of the three example regions, there are up to six PFM Proxy. Profile Manager/Zebra PTT Pro sets. When Profile Manager initiates the import job, the single, populated user file and site map file are downloaded from the file repository into PFM Proxy. Profile Manager processes the user file, examines the Site field of each user, and compares it with the Site field in the Mapping file to determine the server combination in which to provision the user.

NOTE:

- If the deployment can be housed on one Profile Manager instance the Site Mapping file is not required.
- To ensure the Sites are populated in the correct and expected PTT Pro Instance, they are required to be created prior to the User Import job being executed. Do not create sites manually in the PTT Pro console. All Site creation must be performed in the Profile Manager's API interface (Swagger). When Adding Sites via the API, the AD Connector and all other necessary configuration elements are also updated to ensure the entire WFC system knows the correct PTT Pro Instance of the Site.
- Any Site referenced in the User File must be included in the Site Map File. Failure to include in the Site map creates ambiguous error messages during the import process.

The following Site mapping file example is followed by the field description.

Table 2 Store Mapping File

site	siteName	pfmurl	customerid	pfmApiKey	proserverId
1001	Site 1001	https://<pfm-server1>.pttpro.com/admin-service/v1	1	12345	Dev03

Table 2 Store Mapping File (Continued)

site	siteName	pfmurl	customerid	pfmApiKey	proserverId
1002	1002 Store	https://<pfm-server1>.pttpro.com/admin-service/v1	1	12345	Dev03
1003	St. Louis	https://<pfm-server2>.pttpro.com/admin-service/v1	1	98765	Dev03b
1004	1004	https://<pfm-server2>.pttpro.com/admin-service/v1	1	98765	Dev03b
1005	Site-1005	https://<pfm-server3>.pttpro.com/admin-service/v1	1	1a2b3c	Dev03c
1005	North Oaks	https://<pfm-server3>.pttpro.com/admin-service/v1	1	1a2b3c	Dev03c

NOTE: The Zebra PTT Pro Server URL is not included in the Mapping file. The Profile Manager server configuration has an existing Zebra PTT Pro server definition table for each PFM Tenant.

- The Site Map file name is configured explicitly in the Profile Manager database and the file name must be jointly agreed upon between the customer and Zebra. Because the file name is configured in the database, it is unnecessary to specify it in the import job.
- Like the User file, the Site Map file should be encrypted. A file encryption script can be provided to ensure compatibility. Note: if using encryption, both files must be encrypted with the same algorithm.
- If the user file references a site number not included in the mapping file, an error occurs, and the users associated with that site are not added to the system.
- The column headings in the csv file are case sensitive and must match those specified in the example above. If extra columns are present in the file, they are ignored.

Table 3 Store Mapping Elements

Field	Description
Site	Identifies the Customer's Site name (or Department) in the Zebra PTT Pro server. The Site string may contain alpha characters that are acceptable to the Zebra PTT Pro Department entry requirements.
site Name	Description of the Site. Any string is possible
PFM URL	The URL for the Profile Manager includes the 'admin-service/v1' declaration.
Customer ID	The Profile Manager Customer (or Tenant) ID, is found in the PFM Tenant definition.
PFM API Key	The API Key for the PFM Tenant is assigned at tenant creation time. The key is found in the console browser interface of the PFM Tenant definition, or through the API interface for each tenant.

Table 3 Store Mapping Elements (Continued)

Field	Description
Pro Server ID	Name of the PTT Pro server instance where the site is created. For example, if the dev03 PTT Pro cluster has 6 instances then these names could be one of dev03, dev03b, dev03c, dev03d, dev03e, dev03f If these instances are configured, then the unique PTT Pro server name is determined as dev03.

NOTE: The number of unique PTT Pro instances configured determines the number of users who are created/updated in parallel. The number of unique PTT Pro server names determines the number of users who are deleted in parallel.

User Import CSV File

The User file lists all the customer users defined in the PFM/PTT Pro systems. The process of flat file import replicates the Customer's AD database by providing this single csv file. The csv file must contain all of the attributes required for the attribute transformation process.

User Import CSV Column Heading Requirements

There is flexibility in the column header names, with two exceptions:

- site
- UsrerName
- Zebra recommends to use the field names stated in the table below.
- Transformation attributes are case sensitive and use the case of the column headings.
  - The characters in the csv column heading are the string specified in the transformation mapping attribute.
- There can be more columns present in the csv file than are required for the transformation. Extra columns are ignored.
- If the user data contains a comma, as in role1,role2,role3, the value should be enclosed in double quotes.
- The csv file should include all users required to be populated into the PFM and Zebra PTT Pro Systems for each import. After the initial import is performed:
  - If a user csv record is removed, the user is deleted from the servers.
  - If a user csv record is added, a new user is populated to the servers.
  - If a user csv record is changed, those changes are made for that user.
  - If a user csv record is present and no changes are identified, the user is unmodified.

User Assumptions on Importing CSV

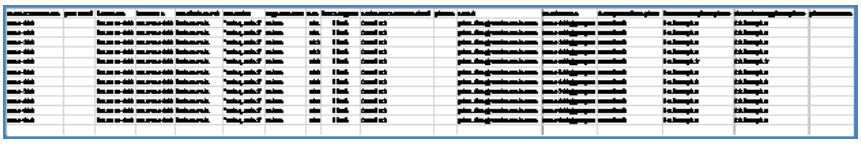
The following list identifies the dependencies and assumptions of the environment:

- The user csv file includes fields for both Profile Manager and Zebra PTT Pro. If both systems are being populated, then the import file must be populated with data for both services for each user.
- Importing data into PTT Pro can take more time because of the complex record interaction into the PTT Pro server for processes such as group creation.
- Creating Profile Manager users and assigning user roles requires that the roles and role levels exist in Profile Manager prior to the import.
  - If using role levels, the user import file does not include the role information. If both exist, the role level is applied to the user and the roles information is discarded.
- The data entry restrictions of shared data elements, like User Name, between Profile Manager and Zebra PTT Pro may be different. User names must meet the lowest common denominator for entry. This is detailed in the table that follows.
- The attribute transformations must be defined before the import job is executed.

NOTE: Any site referenced in the user file must be included in the Site Map File. Failure to include in the Site map creates ambiguous error messages during the import process.

Sample CSV User Import File

A small sample of a User Import File is shown follows:



The following table defines the entry requirements for each column.

CSV User Import File Definition Table

Bulk User Import File Definition						
	Server Usage					
	PFM	Pro	Req'd	Profile Manager Usage	WFC PTT Pro Usage	Comments
samaccountname	✓	✓	✓	This is the User Name field in Profile Manager and is required. Field accepts from 1 to 255 alphanumeric and special characters.	The User Login field in Zebra PTT Pro and is required. Field accepts from 1 to 24 alphanumeric characters, dash, and period	The column heading for this element must be samaccount name. Create user names that meet the requirements in both systems.
password				<Not used>	<Not used>	Not used but column is required.

Bulk User Import File Definition						
firstname	✓	✓	✓	Field accepts from 1 to 255 alpha numeric characters and special characters.	Field accepts from 1 to 30 alpha numeric characters and special characters.	The first name must meet the requirements in both systems.
lastname	✓	✓	✓	Field accepts from 1 to 255 alpha numeric characters and special characters.	Field accepts from 1 to 30 alpha numeric characters and special characters.	The last name must meet the requirements in both systems.
userRoleLevel	✓		✓	Specify role level used in hierarchical role selection based on the attribute "memberof".	<Not used>	If both userRoleLevel and userroles columns are populated, userRoleLevel is used and the useroles column is ignored. Separate multiple role levels with commas. The role level is case sensitive. When the level is created, the same case must be used in the user import file. Roles must exist in Profile Manager before the import is executed.
userroles	✓		✓	Specify the user role. User roles must be created prior to import.	<Not used>	If userRoleLevel is not specified, then this column is a comma separated list of roles. One or more roles must be defined. Roles must exist before the import is executed.
organization	✓			Field describing the users organization. Field accepts from 1 to 255 alpha numeric characters and special Characters.	<Not used>	Descriptive field.
site	✓	✓	✓	Field describing the department. Field accepts from 1 to 255 alpha numeric characters and special Characters.	<Not used>	For PFM this is a description field. In PTT Pro this field must exactly match any existing department for the customer. If the department does not exist, it is created.

Bulk User Import File Definition						
forceLogout	✓			When enabled if the user logs in on another device without logging off of the first device, the system automatically logs off the user from the first device.	<Not used>	Value is either 'true' or 'false'
authenticationMethod	✓		✓	The supported option is OAUTH2.	<Not used>	The PTT Pro server does support Oauth to provide a shared device model, but there is no actual Authentication Method switch per user.
phone		✓		<Not used>	Phone number if SMS activation is planned.	This is not a required field.
email		✓		<Not used>	Email address of the user.	This is not a required field.
oauthName		✓	✓	<Not used>	Populated in the PTT Pro server to support a shared device model.	Format can be either: "domain\username" or "username@domain"
GroupUserTemplate		✓	✓	<Not used>	Defines the talk group template to use. Four possible entries are: associate, SME, associate, or standard.	Used in the PTT Pro server to determine talk group behavior.
featureKeysTemplate				<Not used>	Assigns a pre-configured template to the user. The template must exist in the PTT Pro server for this to be assigned.	Must match an existing PTT Pro Feature Keys template.
clientSettingsTemplate		✓		<Not used>	Assigns a pre-configured Template to this user. The Template must exist in the PTT Pro server for this to be assigned.	Must match an existing PTT Pro Client Setting Template.
PBX Extension				<Not used>	<Not used>	Optional pseudonym for the PBX extension. Used in conjunction with Extension Manager Hidden Department to reserve and extension for the identified user.

Servers Setup Information

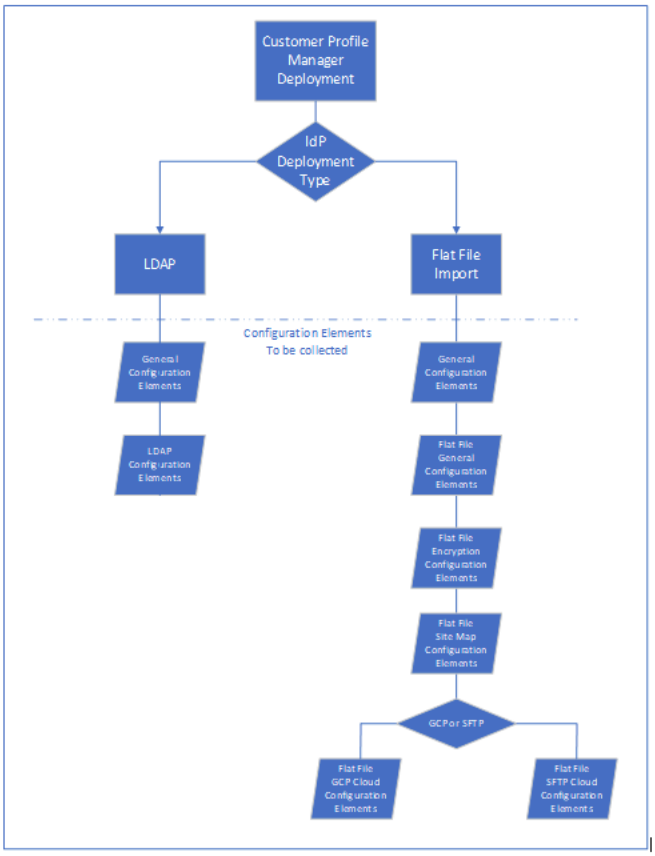
To configure the necessary servers in the Workforce Connect environment, information must be jointly understood and collected from the Customer and the Zebra Integration Consultants. This information is

provided to the Zebra Server administrators. The tables that follow could be used as worksheets to guide the customer conversation in developing the system definition.

The following pages identify which configuration elements need to be collected depending on the integration. Afterwards, the individual configuration element tables are described

Configuration Elements

Depending on the customer's IDP integration approach, the following diagram identifies the various configuration elements to collect.



General Customer Profile

This information needs to be collected in any deployment.

General Configuration			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
CUSTOMER_ID	Tenant ID established in Profile Manager.	✓		✓
ADMIN_SERVICE_BASEURL	Profile Manager URL.	✓		✓
ADMIN_SERVICE_API_KEY	Profile Manager tenant APIKey found in tenant configuration.	✓		✓

General Configuration			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
QUERY_CONNECTOR	Defines the main connection type for retrieving the import files. Flat file import supports gcp-cs and sftp. Accepted values are: • ldap, gcp-cs or sftp Default value: ldap.	✓	✓	
GENERAL_SEND_UNMODIFIED_DATA	Send the unmodified user record deltas to PFM. Use false for file-based user import. Flat file import requires that the file contain the entire user database. In daily processing, the unmodified record set is potentially very large and consumes unnecessary processing. • true • false Default value: true	✓		✓

LDAP Configuration Elements

Customers using an LDAP deployment need the following the information.

LDAP Configuration Elements			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
LDAP_USER_DN	LDAP object DN	✓	✓	
LDAP_HOST	LDAP server host name. A DNS name is recommended.	✓	✓	
LDAP_PORT	LDAP port access.	✓	✓	
LDAP_USER_PASSWORD	Password when LDAPS is used.	✓	✓	
LDAP_BASE_DN	The targeted base DN	✓	✓	

LDAP Configuration Elements			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
LDAP_UNIQUE_NAME	Attribute name used to uniquely identify each imported user. This field determines if the user is new and should be added, exists and should be modified, or absent and should be deleted. This field value is displayed in the import job history details (dispatcher and view delta screen user field). Default value: samaccountname **NOTE:** samaccountname works only for ADFS. For other directory systems, a different attribute may have to be used to uniquely identify users.	✓	✓	

Flat File General Configuration Elements

Flat file configuration elements are required when using the file import method. These elements are required for both GCP or STFP.

Flat File General Configuration			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
SITEMAP_CONNECTOR	Connector is used for the site map file when it differs from the user file connection. If the same repository is used, this is not required. Possible values: • "gcp-cs" for cloud storage • "sftp" for SFTP By default, no value is set. It is considered as no sitemap file is configured for this deployment.	✓	✓	
SITE_MAPPING_FILE	Name of the site mapping file. Default value is empty, indicating user records are processed by the AD-Connector Service.	✓	✓	
CSV_SITE_HEADER	Header field identifies the site column name (PTT Pro Department) in the user mapping file. Default value: site.	✓		✓
DOWNLOAD_FOLDER	AD Connector folder for storage of received user and site import files. Default value is `/tmp/downloads`	✓		✓

Flat File Dynamic Ad-Hoc User Provisioning AD Connector Elements

When ad-hoc user provisioning is used, these elements define the mapping from the received JWT Access Token to the Profile Manager Attribute Transformation Configuration.

Flat File Ad-Hoc User Provisioning Configuration		Supplied By		
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
USERMAP_USERNAME_ATTRIBUTE	CSV Import column header identifying the user name in the User Import file. Default value is UserName.	✓	✓	
USERMAP_FIRSTNAME_ATTRIBUTE	CSV Import column header identifying the first name in the User Import file. Default value is FirstName.	✓	✓	
USERNAME_LASTNAMME_ATTRIBUTE	CSV Import column header identifying the last name in the User Import file. Default value is LastName. **NOTE:** If the token attribute mapping for this field is empty, usermap data are populated with user Login,	✓	✓	
USERMAP_OAUTH_ATTRIBUTE	AD Connector folder for storage of received user and site import files. Default value is OauthName.	✓	✓	
USERMAP_OBJECTCLASS_ATTRIBUTE	Define the object class name for creating users. Default value is person.	✓	✓	
DISALLOWED_SITES	A comma separated list of site (PTT Pro Dept.) name. Users who are reference to these site are not created.		✓	

Flat File Dynamic User Provisioning Access Token Attributes

When using Ad-Hoc User Provisioning, these are elements extracted from the JWT Access Token. Based on the user details in the access token, user is created in PFM and in PTT Pro. The field names in the access token may be different from the column header names in the usermap csv file. The following attribute mapping is used to transform the JWT Access Token attributes to usermap column header attributes.

Table 4 Access Token Attributes

userKey	tokenKey	Description
firstName	fname	If empty, the value is set as "UserName".
lastname	lname	If empty, the value is set as "UserName".
userRoleLevel	rolelevel	Default Value: <empty>
userRoles	role	Default Value: admin
oauthName	sub	If empty, the value is set as "UserName".

Table 4 Access Token Attributes (Continued)

userKey	tokenKey	Description
authenticationMethod	auth	Default Value: OAUTH2
forceLogout	flogout	Default Value: true
objectClass	objectclas	Default Value: person

Flat File Encryption Elements

Zebra highly recommends that encryption is used when importing data with the flat file method.

NOTE: The Site Map file may be encrypted differently from the user file. For simplicity purposes, this is not recommended.

Table 5 Flat File Encryption Configuration

Flat File Encryption Configuration Elements			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
SITE_MAPPING_FILE_IS_ENCRYPTED	Specifies if the site map file is encrypted and uses the same encryption scheme and credentials as the user import file. Possible values: • true • false	✓	✓	
CRYPTO_IS_ENCRYPTED	Specifies if the site map and user import files are encrypted. When true, both the site maps and user import files are encrypted. Possible values: • true • false When false, the remaining parameters are ignored.	✓	✓	
CRYPTO_PASSWORD_FOR_KEY	String value for the AES256 encryption password	✓ (if encrypted)	✓	
CRYPTO_SALT	String for the Salt value for AES256 HMAC key generation.	✓ (if encrypted)	✓	
CRYPTO_ITERATION_COUNT	Iteration count to decrypt file. This number has to be same as encrypt file. Default value is 100000	✓ (if encrypted)	✓	

Table 5 Flat File Encryption Configuration (Continued)

Flat File Encryption Configuration Elements			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
CRYPTO_KEY_LENGTH	Specifies the key length for decryption. Default value is 256.	✓ (if encrypted)	✓	

Flat File Site Map Configuration Elements

A site map file is optional and may not be necessary for smaller deployments with a single PFM tenant. For larger deployments, a site map file can be useful and the configuration elements for a site map file are provided in the following table:

Flat File Site Map Configuration			Supplied By	
Parameter Name	**Description**	**Required**	**Customer**	**Zebra**
CSV_SITE_HEADERS_SITE	Identifies the site name or Department in Zebra PTT Pro. The site name must contain alphanumeric characters are acceptable to the Zebra PTT Pro Department entry requirements.	✓	✓	
CSV_SITE_HEADERS_SITENAME	Corresponds to the site name description in the site map file. This field provides a user-friendly site name.		✓	
CSV_SITE_HEADERS_PFM_URL	URL of the Profile Manager.	✓		✓
CSV_SITE_HEADERS_PFM_API_KEY	The API key for the PFM tenant that is assigned when the tenant is created. The key can be found in the console browser interface of the PFM tenant definition or through the API interface of the tenant.	✓		✓
CSV_SITE_HEADERS_CUSTOMER_ID	The customer (or tenant) ID that is specified in the PFM tenant definition.	✓		✓
CSV_SITE_HEADERS_PROSERVER_ID	The Zebra PTT Pro record index number for the customer defined in the Zebra PTT Pro server. This number is the customer ID found.	✓		✓
When GCP is used for the site map File, SFTP parameters are ignored.				
GCP_SITEMAP_PROJECT_ID	GCP project identifier.	✓	✓	
GCP_SITEMAP_BUCKET_NAME	Bucket Name.	✓	✓	
GCP_SITEMAP_KEY_FILE	Service account access key (JSON file).	✓	✓	
When SFTP is used for the site map file, then GCP parameters are ignored.				

Flat File Site Map Configuration			Supplied By	
Parameter Name	Description	Required	Customer	Zebra
SFTP_SITEMAP_HOST	SFTP server host name or IP address. DNS host name is recommended.	✓	✓	
SFTP_SITEMAP_USER	SFTP user name.	✓	✓	
SFTP_SITEMAP_PASSWORD	SFTP password.	✓	✓	
SFTP_SITEMAP_KEY_FILE	SSH key file.	✓	✓	
SFTP_SITEMAP_PASSPHRASE	Passphrase for the key file.	✓	✓	
SFTP_SITEMAP_FOLDER	SFTP repository folder path.	✓	✓	

GCP Cloud Storage Container

The Google Cloud Platform (GCP) bucket can be used for the User Import.csv file.

GCP User File Storage Container			Supplied By	
Parameter Name	Description	Required	Customer	Zebra
GCP_PROJECT_ID	GCP project identifier	✓	✓	
GCP_BUCKET_NAME	Name of the bucket	✓	✓	
GCP_KEY_FILE	Service account access key (JSON).	✓	✓	
LDAP_UNIQUE_NAME	Attribute name used to uniquely identify each imported user. This field determines if the user is new and should be added, exists and should be modified, or absent and should be deleted This field value is displayed in the import job history details (dispatcher and view delta screen user field).	✓	✓	

SFTP Cloud Storage Container

An SFTP repository can be used for the User Import.csv files.

SFTP User File Cloud Storage Container			Supplied By	
Parameter Name	Description	Required	Customer	Zebra
SFTP_HOST	SFTP server host name or IP address. DNS strongly recommended.	✓	✓	
SFTP_USER	SFTP user name.	✓	✓	
SFTP_PASSWORD	SFTP password.	✓	✓	
SFTP_KEY_FILE	SSH key file.	✓	✓	

SFTP User File Cloud Storage Container			Supplied By	
Parameter Name	Description	Required	Customer	Zebra
SFTP_PASSPHRASE	Passphrase for the key file.	✓	✓	
SFTP_FOLDER	SFTP repository folder path.	✓	✓	
SFTP_KNOWN_HOSTS	String for the "known_hosts" path containing the server's RSA fingerprint.	✓		✓
LDAP_UNIQUE_NAME	Attribute name to uniquely identify each imported user. This field determines if the user is new and should be added, exists and should be modified, or absent and should be deleted. This field value is displayed in the import job history details (dispatcher and view delta screen user field).	✓	✓	

Profile Manager Proxy Configuration

These elements are used to configure the Profile Client for successful connection to the PFM Proxy.

Profile Manager Profile Configuration			Supplied By	
Parameter Name	Description	Required	Customer	Zebra
PROXY_PFM_URL	PFM Proxy URL	✓		✓
PROXY_PFM_API_KEY	PFM Proxy API key	✓		✓

Attribute Transformations

Regardless of which user provisioning method you use, AD import or flat file import, attribute transformations map data elements to required fields used by Profile Manager and Zebra PTT Pro. The process of identifying attributes and transforming these into useful data fields is important to successful user provisioning.

This section first describes the process of Attribute Transformation using an Active Directory import. Applying these principles to the Flat File import is described afterward.

AD Attributes Identification

Use an LDAP browser to find and examine a specific user. Roles in Profile Manager are typically descriptive words so find an attribute that can be transformed into a PFM user role. In this example, we use 'extensionAttribute7' to specify the Wire, Screws, and Nails Roles.

Figure 5 extensionAttribute 7

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

Case sensitivity must be observed when generating the attributes described in this document.

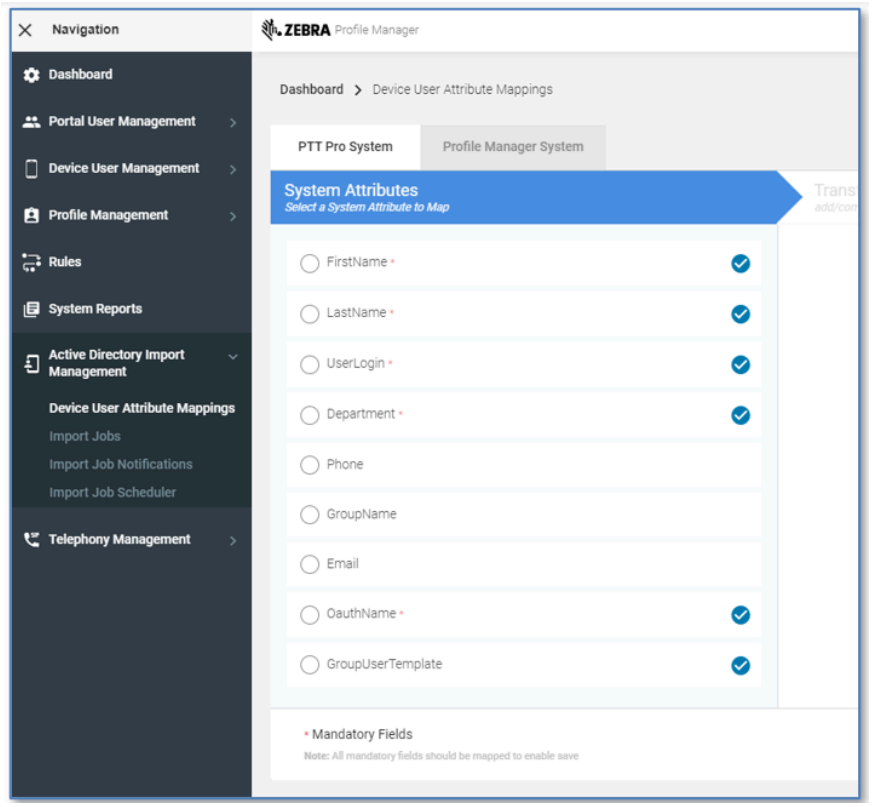
Next, review the attributes for the user. This table shows all the available attributes for a particular user.

Attribute Type	Value
cn	zman1
instanceType	4
nTSecurityDescriptor	
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=PTTPRO,DC=ZEBRA
objectClass	organizationalPerson
objectClass	person
objectClass	top
objectClass	user
accountExpires	9223372036854770000
badPasswordTime	132397473873874000
badPwdCount	0
businessCategory	OAUTH2
codePage	0
company	Zebra
countryCode	0
department	Minnetonka
description	worker
displayName	zman1
distinguishedName	CN=zman1,OU=Users,OU=zebra,DC=PTTPRO,DC=ZEBRA
dSCorePropagationData	16010101000000.0Z
extensionAttribute5	TRUE
extensionAttribute7	wire,screws,nails
givenName	zman1
lastLogoff	0
lastLogon	132398374406244000
lastLogonTimestamp	132405114529723000
logonCount	22
memberOf	CN=Imprivata,DC=PTTPRO,DC=ZEBRA
name	zman1
objectGUID	(non string data)
objectSid	(non string data)
physicalDeliveryOfficeName	Eden Prairie
primaryGroupID	513
pwdLastSet	132393993097741000
sAMAccountName	zman1
sAMAccountType	805306368
sn	Zimmerman1
telephoneNumber	9525551212
title	Associate
userAccountControl	66048
userPrincipalName	zman1@PTTPRO.ZEBRA
uSNChanged	4206643
uSNCreated	4173760
whenChanged	20200729155052.0Z
whenCreated	20200716185509.0Z
aCSPolicyName	
adminCount	
adminDescription	
adminDisplayName	

In this view, all populated attributes move to the top of the list and are alphabetized. Reviewing these attributes provides an opportunity to determine which fields can be used to populate user information when the user is provisioned.

Creating Attribute Transformation Definition

When using either AD import or flat file import, browse to Profile Manager and navigate to the **Active Directory Import Management** tab. Select **Device User Attribute Mappings**.



In the center pane, both **PTT Pro System** and **Profile Manager System** are shown. Required elements are indicated by the asterisk. These data elements must be populated for Zebra PTT Pro and Profile Manager when the import job is executed and the transformation is completed.

For flat file import, choose the required values in PFM and PTT Pro and select the appropriate column heading for the data representing that element. Note that the attribute headings are case sensitive.

Evaluating AD Attribute Transformation

The table below is a spreadsheet to illustrate one way of determining key attributes and the targeted fields to populate in the Profile Manager and WFC PTT Pro servers.

The table shows each of the required elements in the WFC PTT Pro and Profile Manager systems. The idea is to identify an AD attribute for each of the required WFC 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.

Profile Manager Attribute Transformations Mapping		
PTT-Pro		
Element	AD Attribute Name	Value
First Name		
Last Name		
User Login		
Department		
OAuthName		
Group User Template		
Proile Manager		
Element		
User Name		
First name		
Last Name		
User Role Levels		
User Roles		
Organization		
Department		
Force Logout		
Authentication Method		

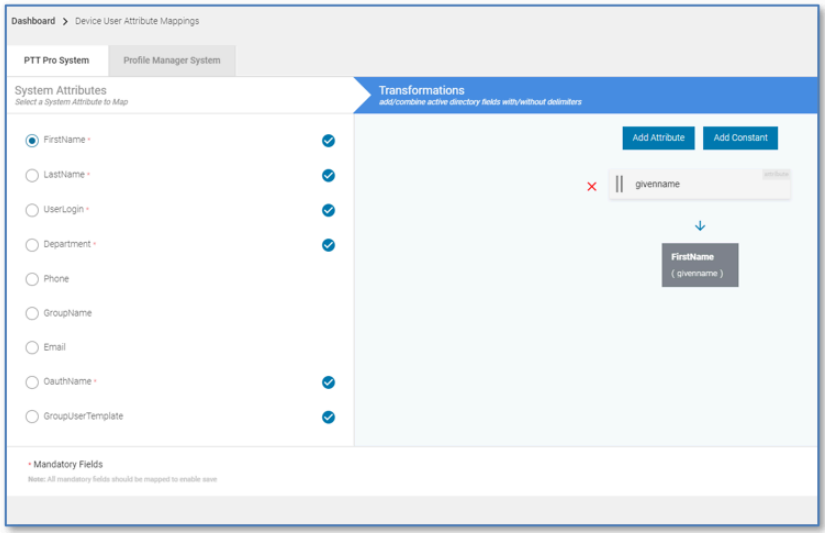
In the AD snippet shown above, as an example, the following AD attributes are used.

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

Then to complete the table for this illustration, the defined AD attributes are populated into PFM and WFC PTT Pro during the import process defined by the transformation.

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

Once it has been determined the attributes and values to use, you can configure the Profile Manager server.



Click on each of the required fields for WFC PTT Pro and Profile Manager. The Transformation field prompts to enter the selected AD attribute.

Complete the transformation for each required field in the WFC PTT Pro and Profile Manager sections. Once complete, you can define and execute an import job.

Configuring Flat File Attribute Transformations

The concept of Flat file import replaces direct access to the Customer's AD database with importing the flat csv file of all Users to populate into the system. The csv file provided by the customer must contain all the required attributes required in the Attribute Transformation process. The csv column headers are the attributes to specify in the Transformation Process.

Import Process

After you configure the Attribute Transformation, you can create the User Import job. There are four methods for importing users into the Profile manager and Zebra PTT Pro environment:

- AD/ADFS query
- GCP Bucket Repository
- SFTP File Repository
- Direct Console Import

This section describes the process an administrator follows for each of these methods. Because the GCP and SFTP repository methods are similar, these two methods are combined. The Direct Console Import process uses different services and has a different operational process and is described last.

NOTE:

In the PFM Proxy environment with multiple PFM Servers, the Import Job is executed from only a designated PFM server. The AD Connector and PFM Proxy are responsible for populating all of the PFM and PTT Pro Servers in the environment.

Import Job Dependencies

Before performing the Import Job complete two configuration dependencies.

1. PTT Pro Departments must be created (if not already present) before the import.
2. Profile Manager Roles and Role Levels must be created before initiating any user-provisioning process.

Create WFC PTT Pro Departments

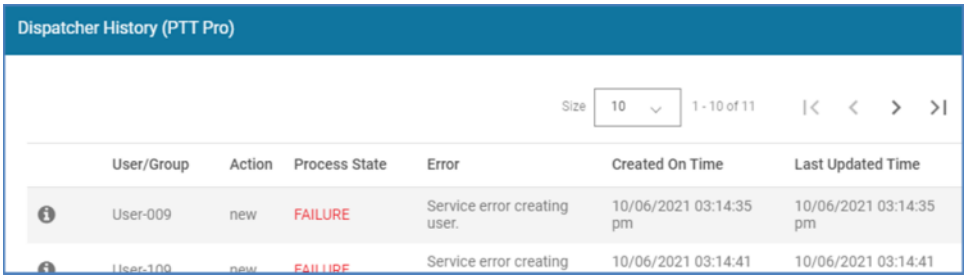
If you import users into PTT Pro, the Departments (Sites) must be created before the import process.

- The ESN Manager is a Profile Manager service that manages Site information. It can create and delete a site in WFC PTT Pro and is the central authority for Site management..
- ESN Manager creates a department if there is a one-to-one ratio between the PFM tenant and the PTT Pro Server Instance.
- When multiple PTT Pro servers are served by a single PFM tenant, then the Sites need to be created in advance in ESN Manager.

If the Departments are created through ESN Manager and then deleted through the PTT Pro Management Console, those Departments are not re-recreated during import and must be manually created. If a

Department does not exist, then an error is generated for each user. in the Department. The Dispatcher History displays an error:

Figure 6 Dispatcher History Error For No Departments



Click the icon to reveal the log information:

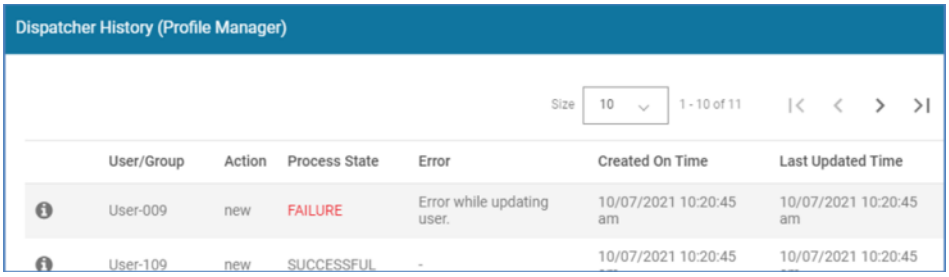

```
],
    "samaccountname": "User-009",
    "lastname": "LN.User-009",
    "password": null,
    "clientSettingsTemplate": "CS.Templ.1",
    "userroles": "role1,role2",
    "authenticationMethod": "OAUTH2",
    "phone": null,
    "organization": "zebra",
    "pbxextension": null,
    "department": "156-BigW",
    "email": "john.doe@ontheweb.com"
  },
  "responseCode": 400,
  "processState": "FAILURE",
  "tenantId": "1",
  "error": {    "responseBody": "{\"code\":10,\"response\":{\"message\":
\"cannot create a user in PTTPRO Server\"},\"success\":false}",
    "statusText": "",
    "message": "Service error creating user.",
    "statusCode": 400

           }
```


Create Roles and Role Levels

Role Levels and Roles need to be created in Profile Manager before executing an Import Job to import users. See the Profile Manager Customer Administrator Guide for information about creating Role Levels and Roles.

If the Roles or Role Levels do not exist, an error is generated for each user. Open the **Dispatcher History** to view the error.

Figure 7 Dispatcher History



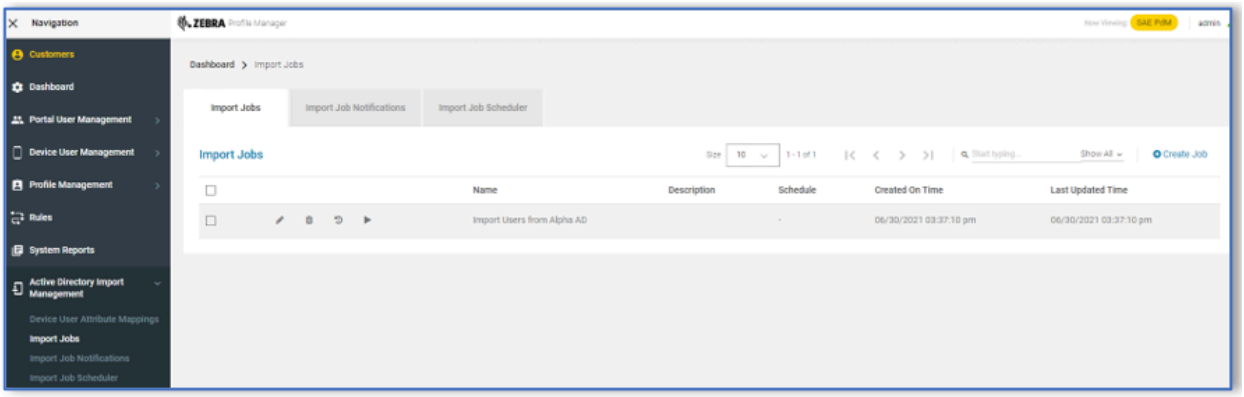
Click the icon to reveal the log information.


```
{,
  "samaccountname": "User-009",
  "lastname": "LN.User-009",
  "password": null,
  "clientSettingsTemplate": "CS.Templ.1",
  "userroles": "role1,role2",
  "authenticationMethod": "OAUTH2",
  "phone": null,
  "organization": "zebra",
  "pbxextension": null,
  "department": "156-BigW",
  "email": "john.doe@ontheweb.com"
},
"responseCode": 400,
"processState": "FAILURE",
"tenantId": "1",
"error": {
"responseBody": "{\"httpErrorCode\":400,\"errorMessage\":\"Role
 Level :RoleLevel2 not found for User: user-009\"}",
    "statusText": "",
    "message": "Error while updating user.",
    "statusCode": 400
}
```

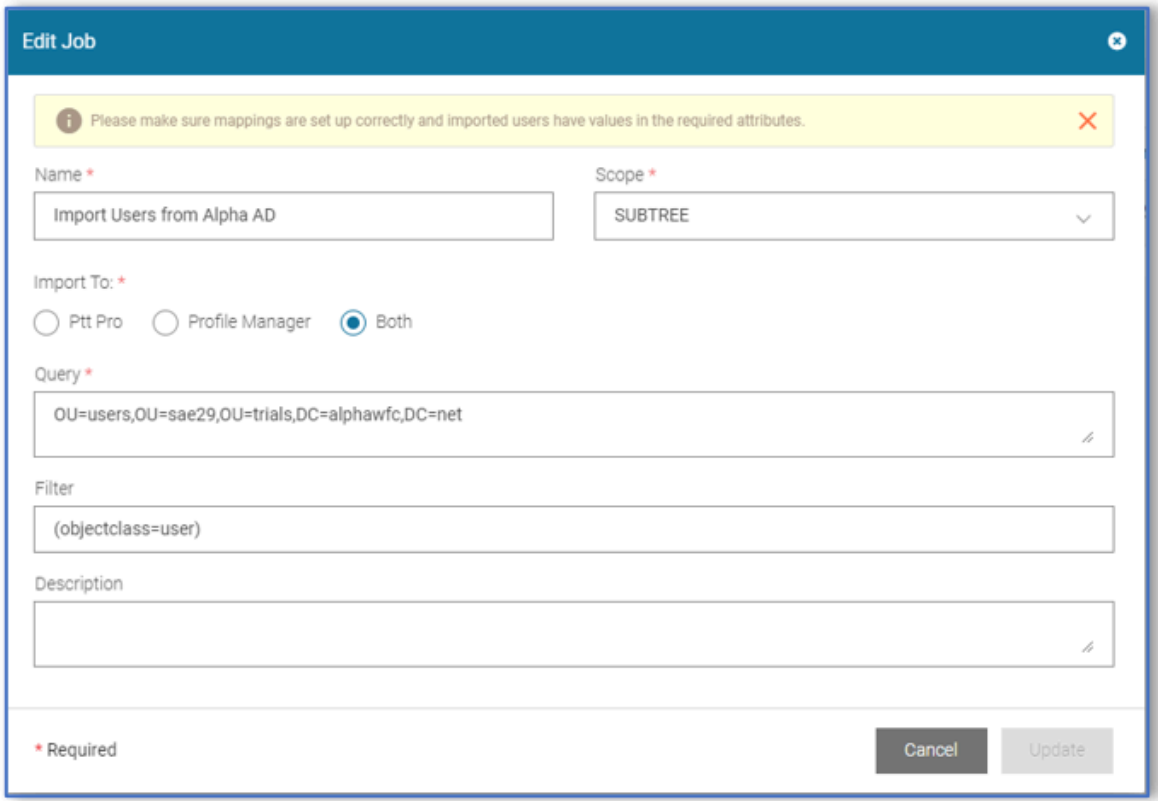

AD and ADFS Query

Setting up the environment for connection from Profile Manager to a customer's AD/ADFS infrastructure is beyond the scope of this document which is detailed in Profile Manager's Import Job configuration from AD.

NOTE: it is required to configure Attribute Transformation before executing an Import job.



1. In the Web Console, navigate to **Active Directory Import Management** and select **Import Jobs**. This window displays any existing Jobs.
2. Click the **Create Job** button.



1. Provide a unique name for the Job.
2. From the **Scope** dropdown list select Subtree, Object, or One Level to determine the depth of the query.
   - Users can be imported into Profile Manager and / or PTT-Pro. Select the appropriate import destination.
   - The Query is key to determine where the import should begin. The query syntax is standard LDAP construction
   - Filter can further refine query, selecting specific records found from the query.

3. Click **Add** to create the Job.

   Once added, the Job can be executed by clicking the arrow icon. The other icons allow for editing, deleting and reviewing the Import Job History.

   Also note that users can create an Import Job Schedule and Job status notifications. Once the initial configuration has been established, the Schedule and Notification are useful services.

GCP Bucket and SFTP File Repository

When GCP or SFTP is used to import data, the customer provides a repository to Profile Manager to access and retrieve the user and site mapping files. These two files define each user and the server to which the user belongs.

The configuration of the import job is the same as the AD/ADFS import job. The job can be scheduled and, once established as working, can be setup to run automatically through the scheduler. The job populates PFM and PTT Pro users.

NOTE: You are required to configure Attribute Transformation before running the import job.

The requirements of a flat file import job include:

- The query field can be populated with anything.
  - A best practice is to describe the import job as GCP or SFTP.
- The configuration for GCP or SFTP is setup by the Zebra administrators in the AD Connector.
  - This information is provided by the customer to Zebra.
- The Filter is the exact file name (encrypted file name) of the user import file.
- The Site Map file is a mutually agreed upon name that is established in the Profile Manager database. The Site Map file is not referenced in the Import Job configuration.
- Do not schedule the initial import that includes PTT Pro users. The import into PTT Pro can take a long time and the scheduler should not be configured and activated until PTT Pro is fully populated.
- For each Import Job the customer can:
  - Review import history in the job history interface. The job history displays user updates as Added, Deleted, and Modified
  - Can setup job status notifications.
  - Can schedule import jobs .
- Import jobs can be scheduled to run on a regular basis.
- The import file should be encrypted. An unencrypted file is supported but not recommended.
- The import file must be a comma separated value format with UTF-8 or ANSI encoding.

NOTE: There are several csv file types available in Excel, but not all are UTF-8 or ANSI encoded. One method to validate a csv file is to open it in Notepad++ and click the **Encoding** tab in the toolbar.

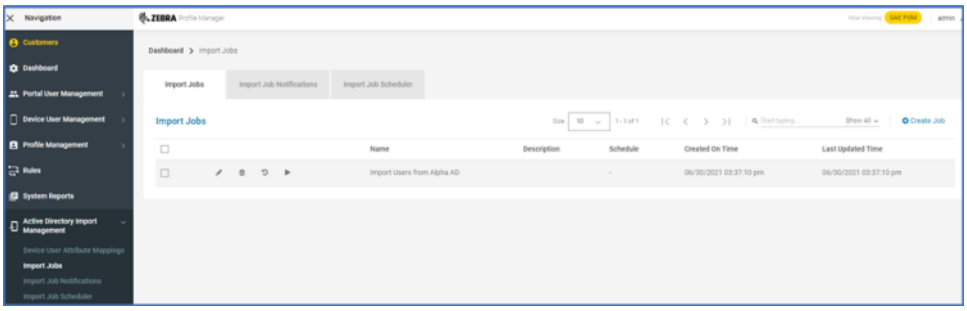
Creating an Import Job

Create an Import Job that configures Profile Manager to retrieve users from Active Directory.

NOTE: You must configure Attribute Transformations before running an import job.

1. In the Web Console, navigate to **Active Directory Import Management** and select **Import Jobs**.

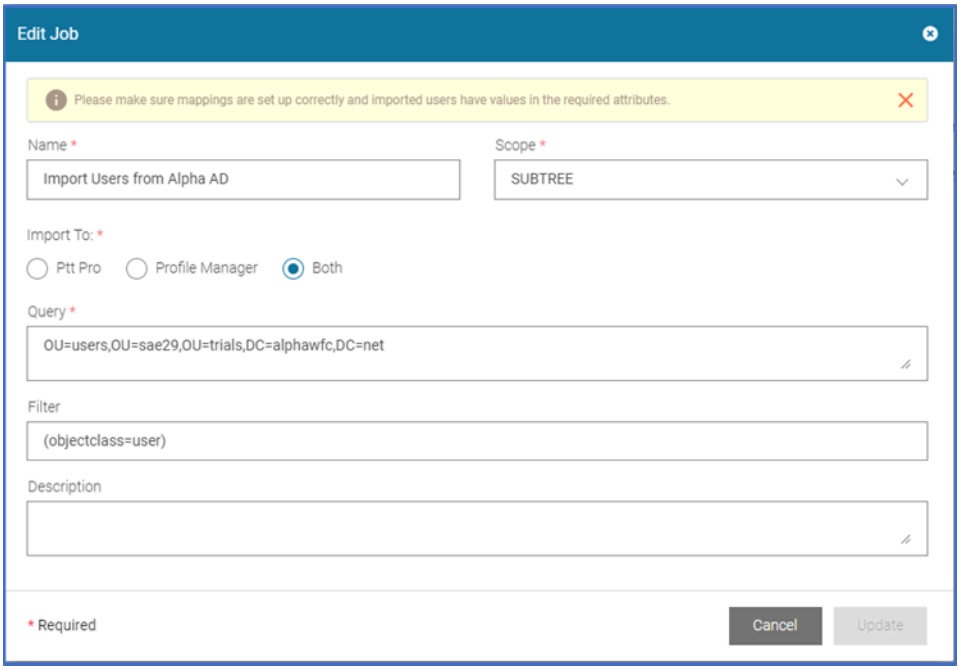
   Figure 8 Import Jobs Screen



   Existing jobs, if any, are listed.

2. Click **Create Job** button to open the **Edit Job** screen.

   Figure 9 Edit Job Screen



3. Enter a job unique name in the **Name** field.
4. From the Scope drop down list, select **Subtree**, **Object,** or **One Level** to determine the depth of the query
5. From the **Import To** option, select the appropriate import destination either **PTT Pro**, **Profile Manager**, or **Both**.

6. In the **Query** field, enter the query syntax .

   The query determines where the import should begin. The query syntax uses the standard LDAP construction.

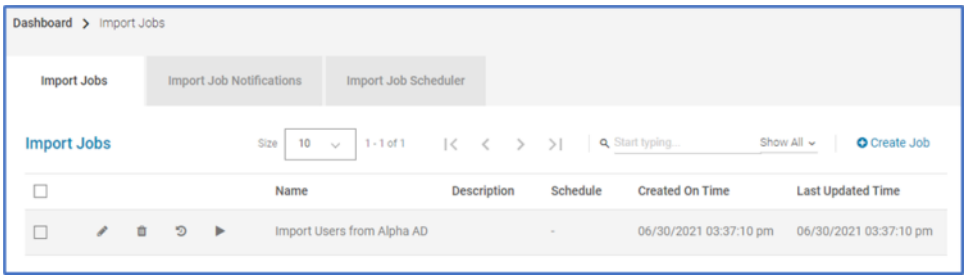
7. In the **Filter** field, enter the filter criteria to refine the query further.

   You can select specific records found from the query.

8. In the **Description** field, you can enter description.

9. Click **Update** to create the job.

Figure 10 New Import Job



10. One job is added, click Run  .

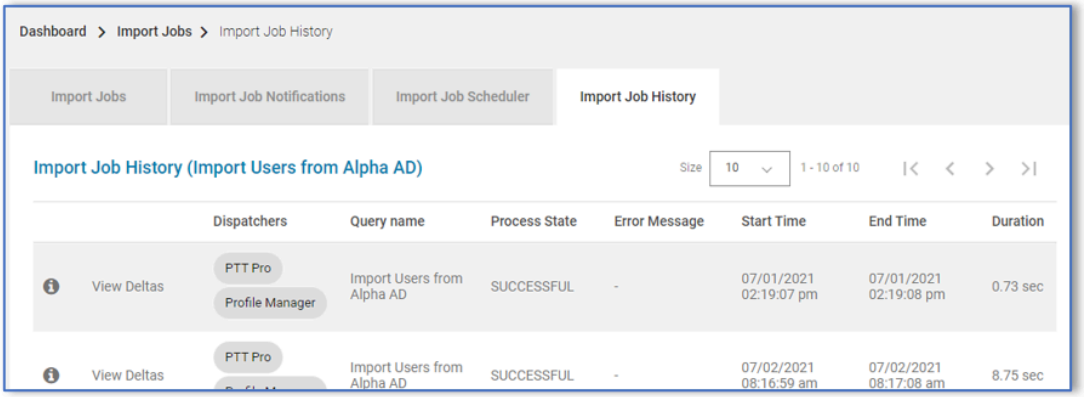
    You can edit delete, and review import job history by clicking the  ,  , or  icons.

NOTE: You can create an Import Job Schedule and Job status Notifications. Once the initial configuration is established, the Schedule and Notification are useful services. For details see Profile Manager Customer Administrator Guide.

Reviewing Import Job Status

Review the import job status for details about the job.

1. After clicking Run icon, check the job completion status by clicking the Job History Icon.

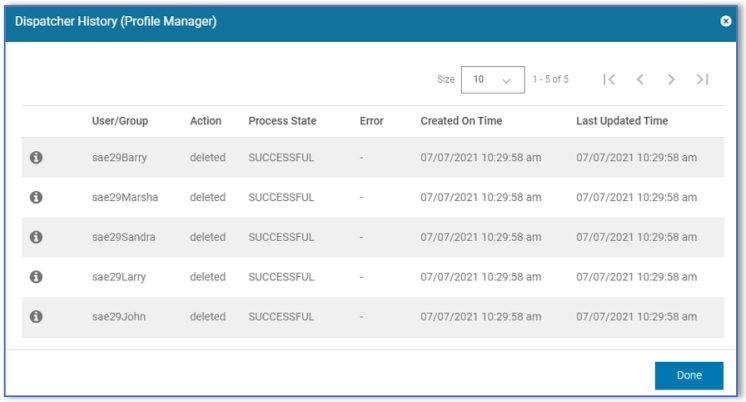


A listing of each run is displayed for that Job with its overall job status. Clicking on the Dispatchers column reveals import details for Profile Manager and WFC PTT Pro if the job was configured for both.

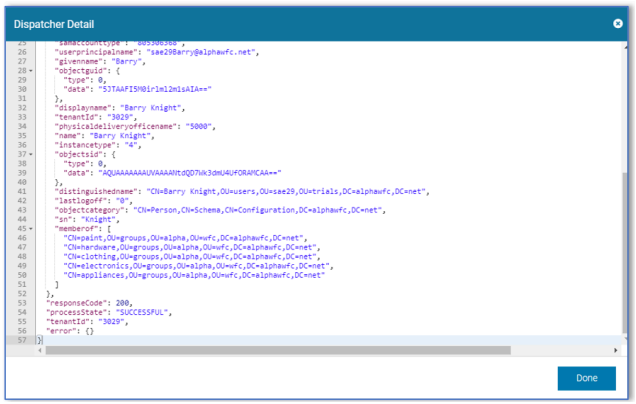
2. Click the value under **Dispatchers** column.

   The import details are displayed for Profile Manager and WFC PTT Pro if the job was configured for both.

   Sample Results are displayed for Profile Manager. This job indicates that five users were removed from the source database, so these were deleted from the Profile Manager.

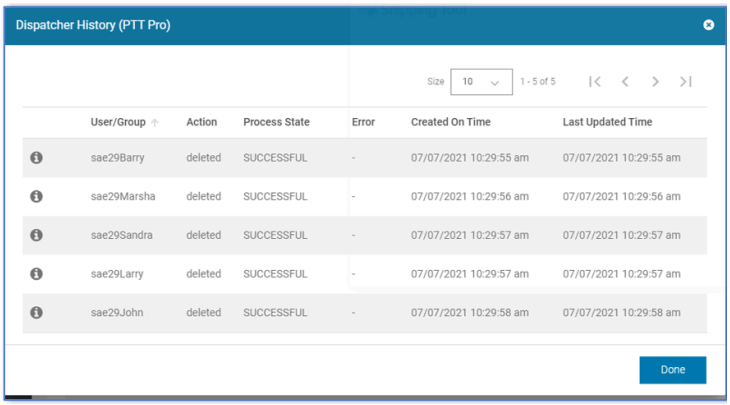


3. On each displayed line item, click the  icon to view the details of each json file record such as addition, modification, and deletion.



   The json file detail can be copied into a text editor for complete viewing.

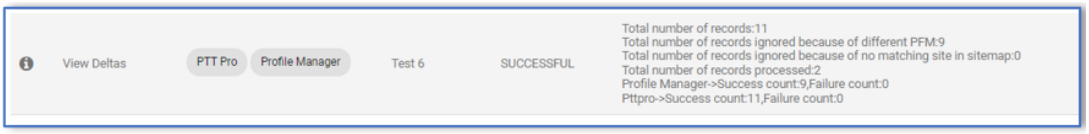
   Sample results are shown for WFC PTT Pro. This job indicates that five users were removed from the source database, so these were deleted from WFC PTT Pro.



4. Click the icon to view the details of each json file record such as addition, modification, and deletion.

Import Job Status

The import job status view reveals additional information, especially when you import users and sites with CSV files. Unchanged users are not listed as records in the Dispatcher information.



The message section displays a summary of the Import Process:

- The number of records in the CSV file.
- Ignored records that belong to another server.

NOTE: In the case of Proxy setup, though there is no change in the user data in the Usermap CSV file, the record status is displayed as “Modified” in the following conditions:

- If the Sticky User logs in to a different site other than the one defined in the CSV file, in such a situation, the user is not moved to the original site and is always displayed as “Modified” for each job execution until the user’s current site and the one defined in the Usermap CSV file are same.
- While importing users to the PTT Pro server, if any error occurs, the records are re-imported in the Profile Manager though there are no modifications to those records.

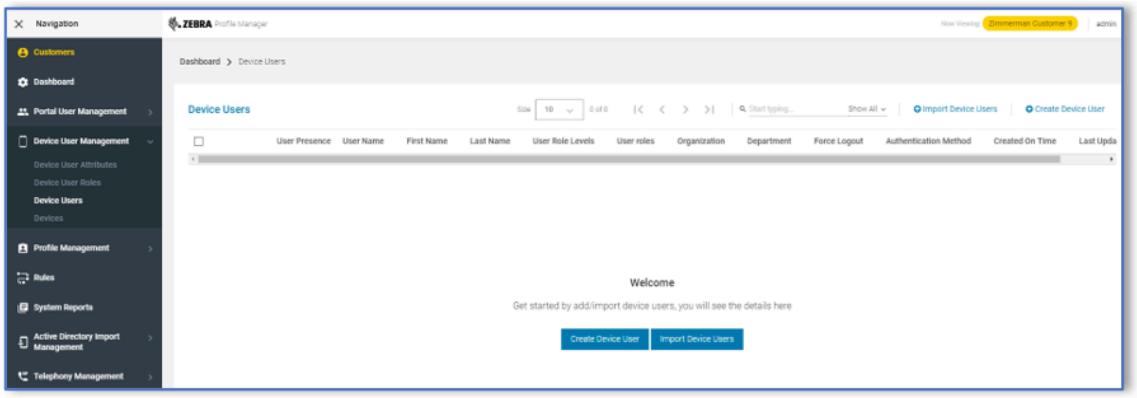
Direct Console Import

The Direct Console Import process uses different services compared to the AD and Flat File import methods. The import template is the same as the GCP Bucket and the STFP methods but the Console Import Process differs as follows:

- Does not use the Import Job services.
- Uses its own Attribute Transformations engine.
- It is a manual process and has no scheduler.

This process is described below:

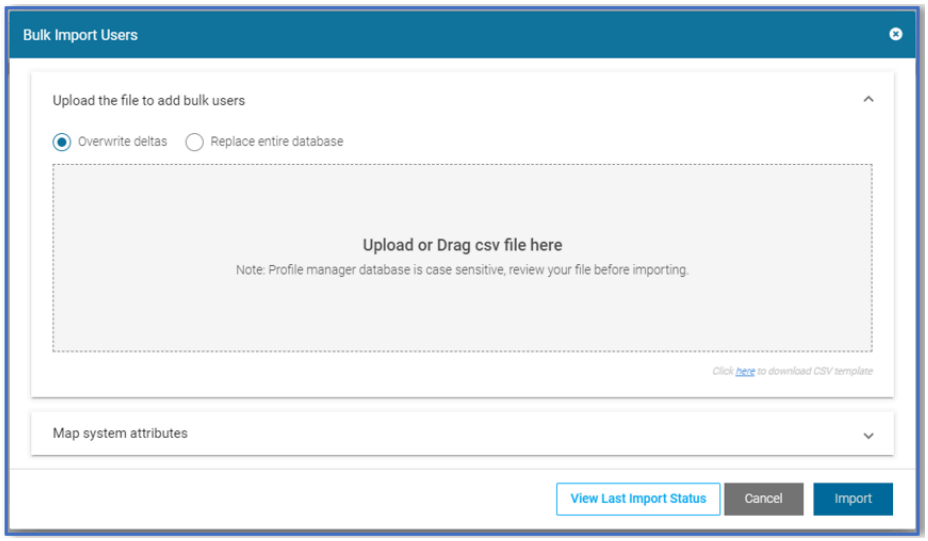
1. To get started navigate to PFM and download a copy of the build user import template.



2. Navigate to**Device User Management** >> **Device Users** .

   The **Device Users** screen appears

3. click **Import Device Users** button.



4. Click the **Click here to download the csv template** to download the file.

   Once the template is downloaded, the desired information is displayed.

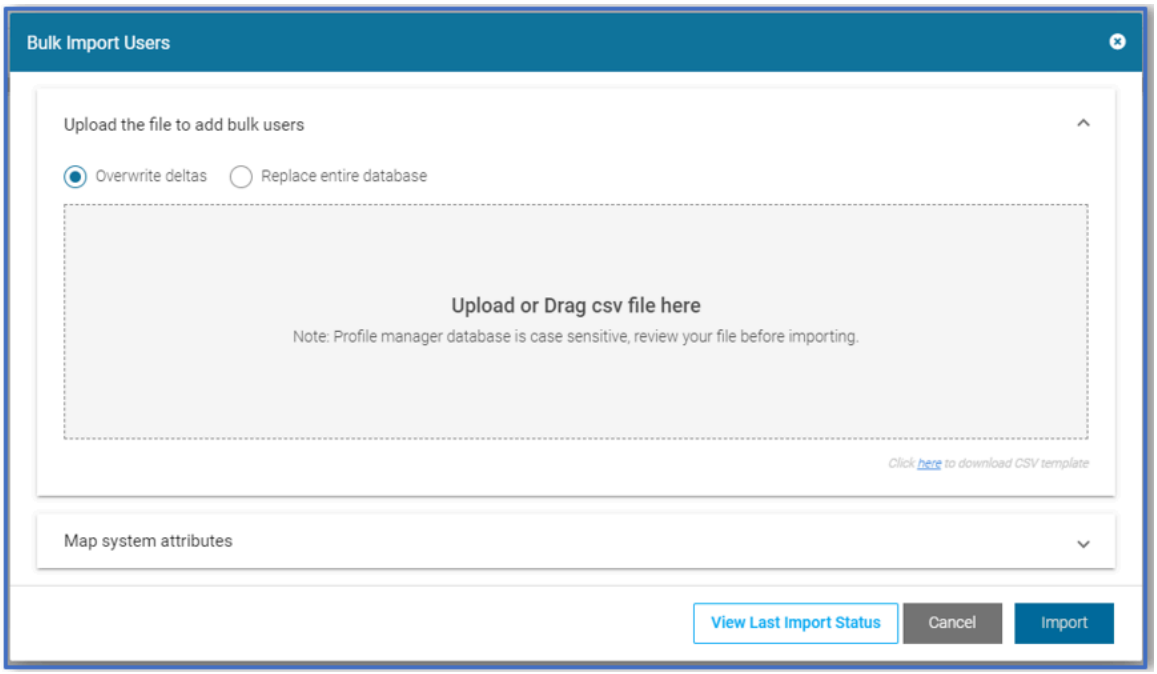
User Name	Password	First Name	Last Name	User Role Levels	User roles	Organization	Department	Force Logout	Authentication Method	TelePHONE	GroupUserTemplate	OauthName
User.A1	Bicycle9999!	Jean-Louise	John Samuel	Hardware		NALA	Paris	TRUE	BASIC		standard	111111
User.A2	Bicycle9999!	Frank	johnson1	Services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

Sample Populated CSV File Template

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 the table below.

Once the import csv table is built it may be imported via the Browser or the API interface. To import through the browser, return to the Device User page and click on Import.

1. To import through the browser, return to the **Device User** page and click **Import**.

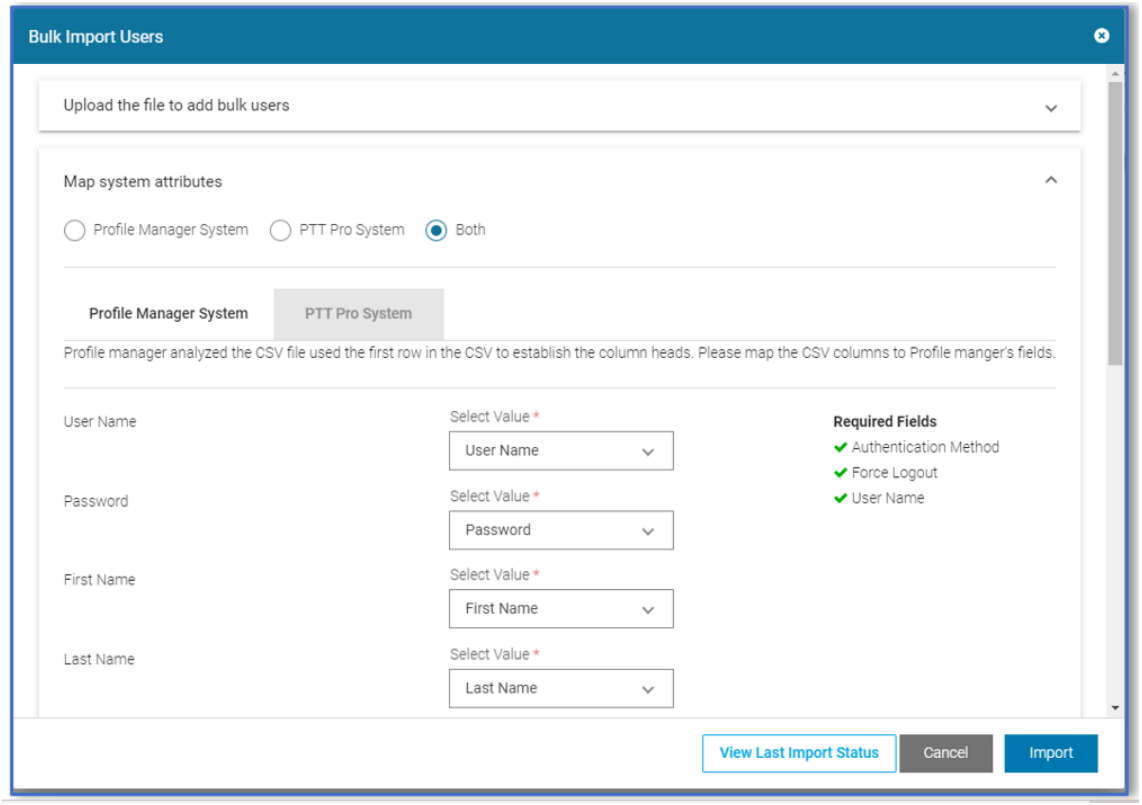


2. Navigate or drag the csv to import into the window.

   There is a choice to overwrite the existing records, or to replace the entire database. Replacing option deletes all user records from the system, so be careful of this operation if selected.

   - Overwrite leaves the user records in place, making adjustments to any existing records as specified in the csv. If there are new records they are added.
   - Replace Entire Database selection initializes all User records and imports the records into the Profile Manager and PTT Pro server as specified in the csv. In PTT Pro all existing Users are deleted for the customer but the Departments remains intact.

3. Click the**Map system attributes** to select the operation to add users to Profile Manager, PTT Pro, or to the both servers.

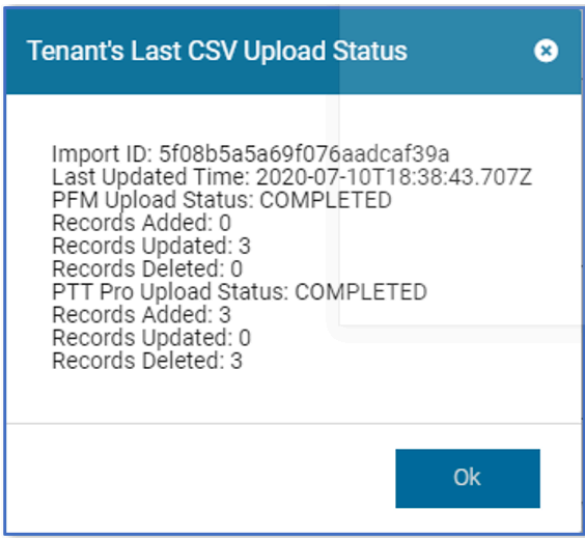


In the lower section of the screen clicking on the Profile Manager or PTT pro tabs provides the ability to map the csv elements to various data fields in each of the servers. The mapping for all columns in the csv must be assigned to server target data elements, or set to be 'Ignored'.

4. Select the either **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 as Ignored.

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



Here in this 3-User example the import used the Reset the entire User Database option and was imported into both Profile Manager 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.

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