

Provisioning Manager

Version 3.0.22402

Workforce Connect



ZEBRA

Customer Administrator Guide

2023/07/26

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal.

COPYRIGHTS: zebra.com/copyright.

PATENTS: ip.zebra.com.

WARRANTY: zebra.com/warranty.

END USER LICENSE AGREEMENT: 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.

Contents

About this Guide.....	5
Notational Conventions.....	5
Related Documents.....	6
Icon Conventions.....	6
Service Information.....	6
Revision History.....	6
Getting Started with Provisioning Manager.....	8
WFC Provisioning Manager Administration Overview.....	8
WFC Voice Client Licensing.....	8
Bootstrapping Overview.....	10
Exploring Provisioning Manager User Interface.....	12
Provisioning Manager Administration URL.....	12
Resetting Administration Portal Password.....	13
Dashboard.....	14
Top Toolbar.....	15
Customer Details.....	15
Logged in User.....	16
Provisioning Manager APIs.....	16
Log Out.....	19
Navigation Menu.....	20
Tokens.....	21
Reports.....	27
Licenses.....	28

System..... 30

Software Version..... 34

Third-Party Device Support and Automated Provisioning..... 35

 Device and Client Requirements.....35

 Limitations..... 35

 Support of WFC Voice for Third-Party Devices..... 36

 Extension Manager (EXM).....36

 Provisioning Manager (PVM).....36

 Support of PTT Pro for Third-Party Devices..... 36

 Automatic Provisioning Overview..... 36

 Enabling Automatic WFC PTT Pro Provisioning..... 37

About this Guide

This document explains the administrative functions of the WFC Provisioning Manager and includes an overview of the Provisioning Manager and instructions for using the portal.

- [About this Guide](#) describes document conventions and related documentation.
- [Getting Started with Provisioning Manager](#) includes an overview of the WFC Provisioning Manager and the functionalities the customer administrator performs using the Provisioning Manager.
- [Provisioning Manager User Interface](#) familiarizes the customer administrator with the WFC Provisioning Manager interface and associated activities.
- [Third-Party Devices](#) provides information about the automated provisioning of third-party devices in the WFC Provisioning Manager and Extension Manager.



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

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.

Related Documents

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

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 keep the following information ready:

- 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 Zebra Customer Support cannot solve the problem, 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-004027-01EN Rev A	11/2020	Initial release
MN-004027-02EN Rev A	06/2021	Updated WFC Voice Client, Token, and Bootstrap-related information.

About this Guide

Revision	Date	Description
MN-004027-03EN Rev A	11/2021	Updated the UI changes-related information.
MN-004027-04EN Rev A	03/2022	Updated the UI changes and obsoletes devices features and color indicators.
MN-004027-05EN Rev A	06/2022	The color Indicator (Solid Blue and Blue with red outline) description was updated for the Assigned Tab.
MN-004027-06EN Rev A	09/2022	Color indicators have been removed, and screenshots have been updated,
MN-004027-07EN Rev A	01/2023	Added Third-Party devices and WFC_Central_Service_Android.
MN-004027-08EN Rev A	03/2023	Removed limitations and updated third-party device support for automated provisioning.
MN-004027-09EN Rev A	07/2023	Updated the Assigned Tab fields.

Getting Started with Provisioning Manager

This section includes the main functions of the Provisioning Manager.

- [WFC Provisioning Manager Administration Overview](#)
- [WFC Voice Client Licensing](#)
- [Bootstrapping Overview](#)

WFC Provisioning Manager Administration Overview

As a component in the WFC Solution Architecture, the WFC Provisioning Manager provides two main functions:

- As a crucial component in WFC Voice Client licensing, the Provisioning Manager allows the administrator to display WFC Voice licenses and the devices to which they are assigned, as well as obsoletes the devices with licenses, which releases the licenses. *WFC Voice Client Administrator Guide for Licensing* describes licensing in more detail.
- The Provisioning Manager allows bootstrapping, which is a method to download configuration information to the various WFC clients; bootstrapping can simplify configuration by eliminating the need to download configuration files directly to the device. The administrator can use the Provisioning Manager to associate the configuration snippets with tokens. The tokens are then used at the device to retrieve the configuration information.

In support of WFC Voice Licensing and Bootstrapping, Provisioning Manager offers the following administrative functions:

- A dashboard which provides an overview of licensing and token requests.
- Reports, which provides a history of device requests as well as an event log.

The administrator can use these functions to monitor the activity on the Provisioning Manager.

WFC Voice Client Licensing

Starting with WFC Voice Client 9.0.20306, the voice device obtains its license from the Provisioning Manager, or from the Extension Manager, if the Extension Manager is part of the customer deployment. The Provisioning Manager obtains the licenses from the licensing system in bulk, and distributes the licenses to devices, or communicates and syncs with the Extension Manager to allow it distribute the licenses.

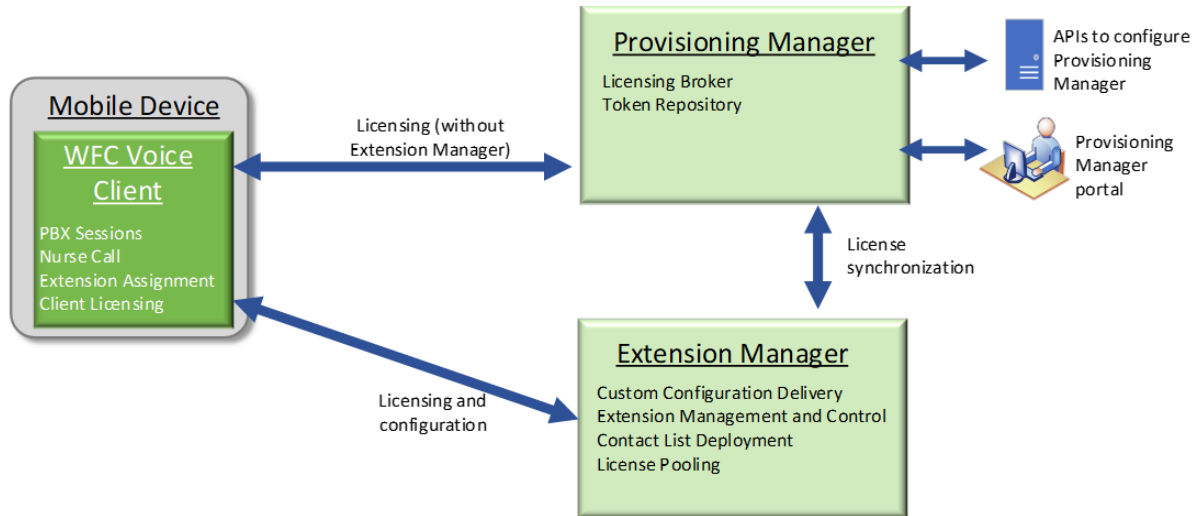
This licensing architecture offers the following advantages:

- Reduction in load on the back-end licensing system

- Improved licensing reliability and response time for the client
- Pooling of standard WFC-Voice licenses when the customer uses the Extension Manager

The Provisioning Manager Ecosystem follows:

Figure 1 WFC Voice Client Architecture



To enable this licensing architecture, Zebra programs the following two tokens for the Provisioning Manager and provides them to the customer in the Welcome email in alphanumeric and QR code format.

- The Direct Access Token activates licenses using the Provisioning Manager. When entered in the WFC Voice client, this token associates the device with the proper customer account in the Provisioning Manager to activate licenses. For more information about the Direct Access token/bootstrap, refer to [Creating Bootstraps and Tokens](#) on page 21.
- The Extension Manager Token provides access to the Extension Manager for customers configured with the Extension Manager. When entered in the WFC Voice client, this token configures the client with the necessary information to connect to the Extension Manager and retrieves the configuration and licensing information. For more information about the Extension Manager token/bootstrap, see [Creating Bootstraps and Tokens](#) on page 21.

Instructions for entering the tokens into the WFC Voice client are included in the customer Welcome email, the WFC Voice Licensing Guide for 9.0.20306 and later, and the WFC Voice PBX Administrator Guides.

The Provisioning Manager portal provides information related to license status, such as the number of available licenses, the number of used licenses, the expiration date, and the devices in which the licenses have been activated. This information is also available in the Extension Manager for customers configured with the Extension Manager. For more information about WFC Voice licenses, refer to WFC Voice Client Administrator Guide for Licensing for 9.0.20306 and later.



NOTE: Customers who do not wish to use the Extension Manager, should use the Direct Access Token.

Bootstrapping Overview

The Provisioning Manager provides one of several ways to configure WFC clients.

Table 1 Configuration Overview Chart

Application to Configure	Manual	File	Profile Manager	AppConfig	Extension Manager	Provisioning Manager (bootstrap)
WFC Voice	Yes	XML	Yes (Using Profile Client)		Yes	Yes
WFC PTT Pro (Android)	Yes	JSON	Yes (Using Profile Client)			Yes
WFC PTT Pro (iOS)	Yes			Yes		Yes
WFC PTT Pro (Dispatch)	Yes					
WFC Profile Client	Yes	JSON				Yes

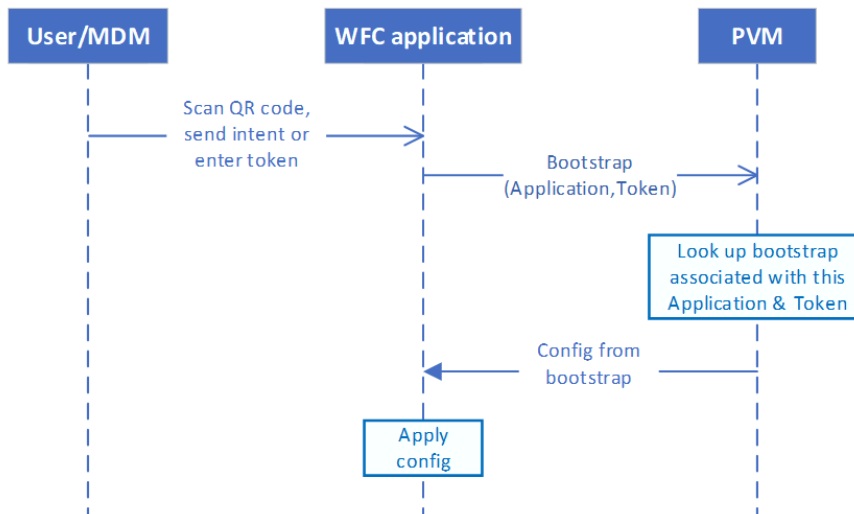
The initial client version supporting bootstrapping, as indicated in the following table:

Table 2 Initial Bootstrapping Support Version

Application	Version
WFC Voice	9.0.20207
PTT Pro Android	3.3.10107
Profile Client	2.0.20207
WFC PTT Pro (iOS)	1.0.11078

The Provisioning Manager supports a method of configuration called bootstrapping, which consists of creating a segment of configuration data (the bootstrap) and associating it with a token. When a device uses a token associated with a bootstrap, the device loads the configuration data contained in the bootstrap, as illustrated in the following diagram:

Figure 2 Bootstrap Ladder Diagram



As shown in the Initial Bootstrapping Support Version table, the Provisioning Manager currently supports the configuration of the WFC Voice, PTT Pro Android, PTT Pro iOS, and Profile Clients.

Configuring bootstraps and tokens can help the customer to achieve specific configuration objectives without loading files on the device.

The bootstraps are useful in the following scenarios:

1. Associate a device with the customer to activate a WFC Voice license.
The Direct Access Token provided in the Welcome email addresses this objective.
2. Configure the WFC Voice client to access the Extension Manager using the `var_location` parameter.
The Extension Manager Token provided in the Welcome email (if the customer is entitled to the Extension Manager) addresses this objective. For more information about configuring the WFC Voice client to access the Extension Manager, refer to the WFC Voice Client PBX Administrator Guides.
3. Configure the WFC Profile Client to access the Profile Manager using the `sfs_url` parameter.
After the Profile Client connects to the Profile Manager, it assists in profile selection as well as the configuration of the WFC Voice and/or PTT Pro clients.
For more information, refer to the WFC Profile Manager Administrator Guide.
4. Replace XML or JSON configuration files. Instead of deploying an XML or JSON configuration file on the devices, a bootstrap and associated token can import the contents of the files.



NOTE: XML must be converted to JSON before using in the Provisioning Manager.

Exploring Provisioning Manager User Interface

This section includes the following topics:

- [Provisioning Manager Administration URL](#)
- [Resetting Administration Portal Password](#)
- [Dashboard](#)
- [Top Toolbar](#)
- [Navigation Menu](#)
- [Tokens](#)
- [Creating Bootstraps and Tokens](#)
- [Reports](#)
- [Licensing](#)
- [System](#)
- [Software Version](#)

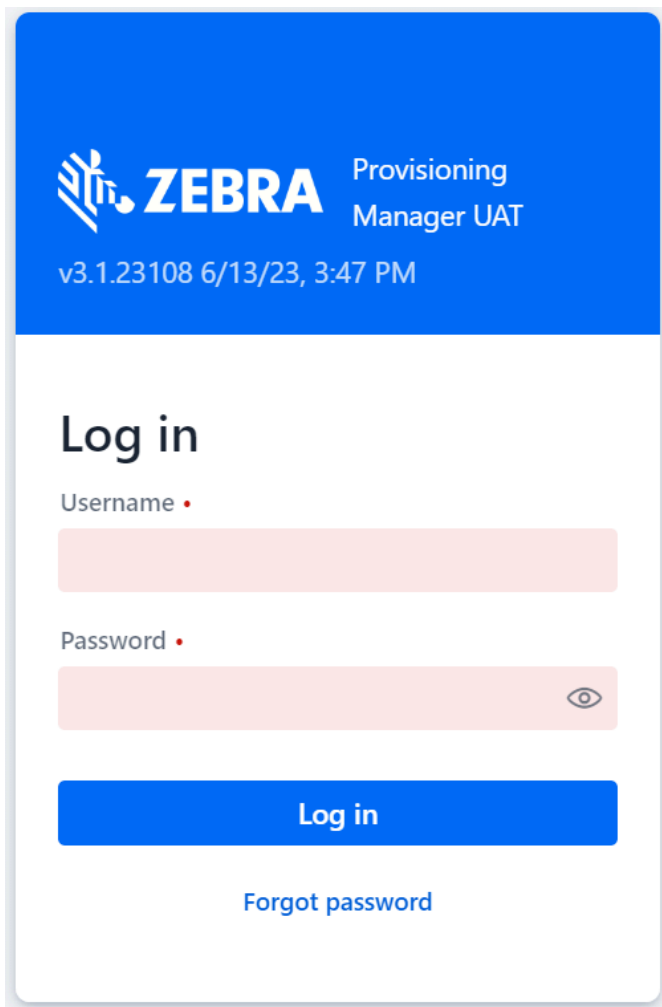
Provisioning Manager Administration URL

The URL points to the multi-tenant WFC Provisioning Manager server. Ensure that you are using the correct URLs for the server(s) in which your access and tenant are provisioned.

To access the login screen for the Provisioning Manager interface, use the following URL:

<https://wfc-provisioning1.pttpro.zebra.com/admin/login>

Figure 3 Provisioning Manager Login Screen



Resetting Administration Portal Password

To reset your Provisioning Manager Administration Portal password, perform the following steps:

1. Go to the URL <https://wfc-provisioning1.pttpro.zebra.com/admin/login>
The Provisioning Manager **Log in** screen appears.
2. Click **Forgot password** link.
The **Reset your password** screen appears.
3. In the **Email** box, enter your registered email ID.
4. Click **Submit**.

Dashboard

- **Assigned licenses:** This line graph displays the number of purchased and assigned licenses by date and by license type (premium Vs standard, purchased Vs assigned/used).
- **Token requests:** This line graph displays the token requests from the devices by day and applications (Voice, PTT-A, PTT-Win, WPC, and PTT-iOS). The number of requests generally peaks when using tokens to deploy new devices or update configurations.

Figure 4 Provisioning Manager - Dashboard



Table 3 Provisioning Manager Dashboard Graph Description

Callout	Region	Description
1	Assigned Licenses graph: Range Selector	Select the date range to be displayed in the License Utilization report, either by clicking a predefined range in months (for example 1m, 3m, 6m) or by specifying the date in the calendar drop-down in the top right corner of the Assigned License screen.
2	Assigned Licenses graph: License Utilization Reports	Displays the License Utilization reports for Premium Used, Premium Total, Standard Used, and Standard Total.
3	Assigned License graph: Report Toggle	Displays the date based on the date selected in the Range Selector bar.
4	Token Requests graph: Token Utilization Reports	Select one of the License Utilization report types to turn the display on and off for the selected type (Premium Used, Premium Total, Standard Used, and Standard Total).
5	Token Requests graph: Report Toggle	Select one of the Token Utilization report types to turn the display on and off for the selected type. Reports can be toggled by the WFC application (WFC Voice, PTT Pro Android, PTT Pro Windows, WFC Profile Client, PTT Pro iOS, and WFC Central).



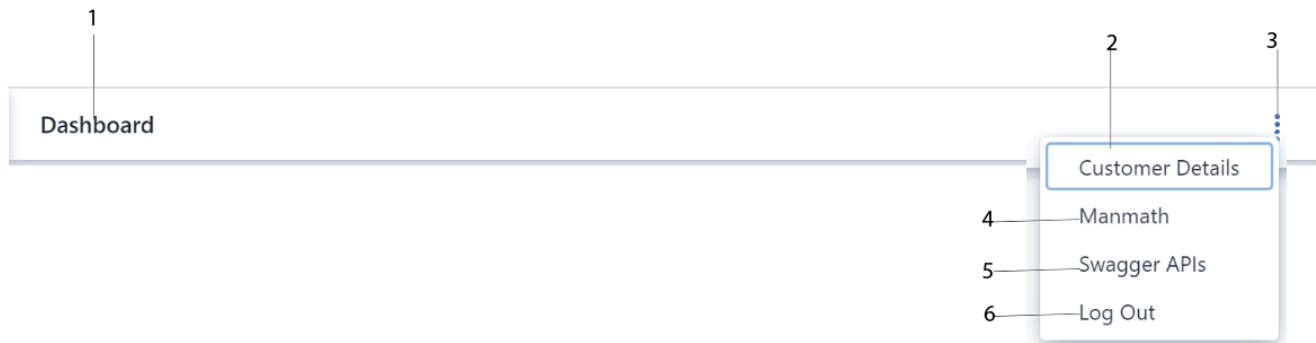
NOTE: Customizing the date range can only be performed on the data collected since this graph's introduction.

Top Toolbar

The Top Toolbar has the following elements:

- [Customer Details](#)
- [Logged in User](#)
- [Swagger APIs](#)
- [Log out](#)

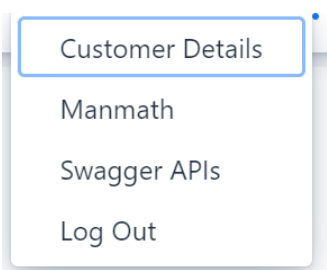
Figure 5 Top Toolbar




Callout	Description
1	Displays the selected menu.
2	Displays the user details.
3	Expands the Show menu.
4	Displays the user name.
5	Displays the Swagger API link.
6	Logs out when selected.

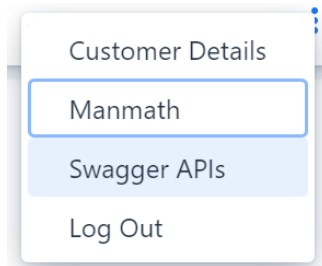
Customer Details

Select **Customer Details** from the **Show** menu  to display customer details.



Logged in User

The **Show** menu  displays the logged-in user name.

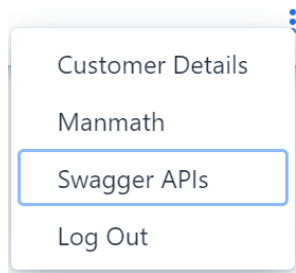


Provisioning Manager APIs

The Provisioning Manager provides APIs to manage tokens, bootstraps, and devices. A Swagger API page details API information and allows the administrator to try the APIs.

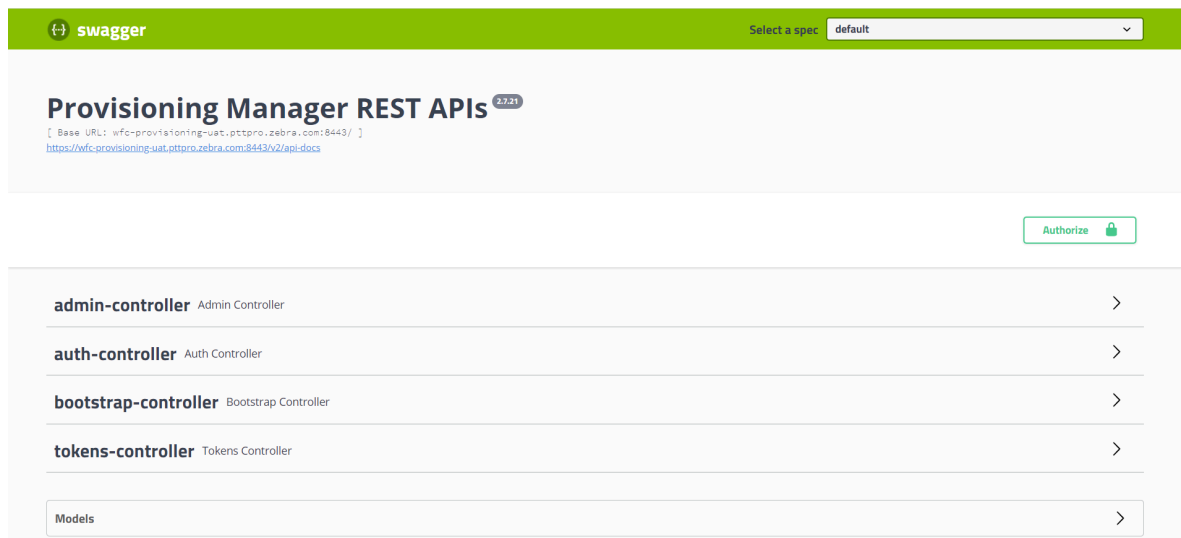
To access the **Swagger API** page,

1. In the top toolbar, click the **Show** menu and select **Swagger APIs**.



The **Swagger API** page opens in a separate browser.


Figure 6 Provisioning Manager REST API



The API provides an auth-controller that contains a login procedure. An access token with a token type of Bearer is returned in the response. This token must be included in an authorization header in all other API requests as a form of authentication. An example header is below:

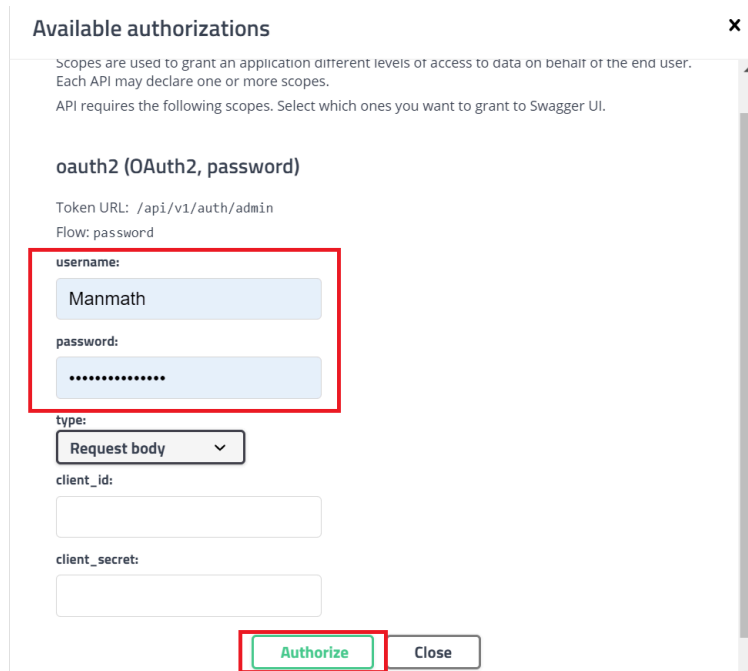
```
authorization: Bearer <accessToken>
```



NOTE: When the Swagger page is used, we recommend using the  button on the top right instead of the auth-controller as described in the following steps 2 through 5.

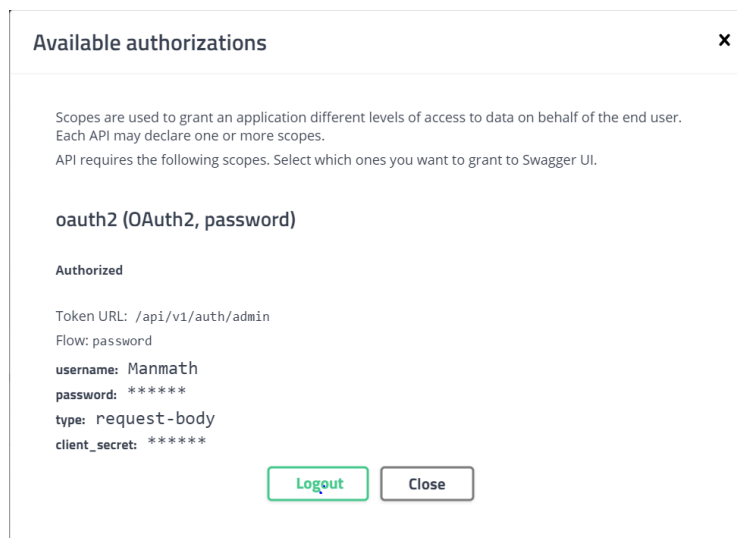
2. Click the  button to authorize the API access.

The **Available Authorization** screen appears.



3. Enter the username and password, and do not modify any other field.
4. Click **Authorize** button.

The **Authorized** screen appears.



5. Click **Close**.

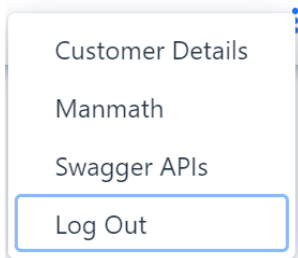
6. The remaining controllers provided in the Provisioning Manager API are as follows:
 - `bootstrap-controller` allows viewing and managing bootstraps as follows:
 - Add/update a bootstrap by name
 - Delete a bootstrap by name
 - Get a bootstrap by name
 - Get a list of all bootstraps
 - `admin-controller` allows deleting devices by device ID to obsolete the selected device and return all assigned licenses for that device to the pool of available licenses.
 - `tokens-controller` allows viewing and managing tokens and their association with bootstrap parameters as follows:
 - Add/update a token by name
 - Delete a token by name
 - Get a token by name
 - Get a list of all tokens
7. To access the API endpoint information, select the carat symbol > at the far right of each controller group. The **Swagger API** page provides API details and an option to try the APIs.
8. To return to the Provisioning Manager interface, select the browser tab where the Provisioning Manager application is running.



IMPORTANT: When updating information for the Provisioning Manager, use either the Provisioning Manager interface or the Provisioning Manager APIs. Do not use the interface and the APIs at the same time, as this could cause synchronization issues.

Log Out

Click the **Show** menu  and select **Log Out** to log out of the Provisioning Manager.



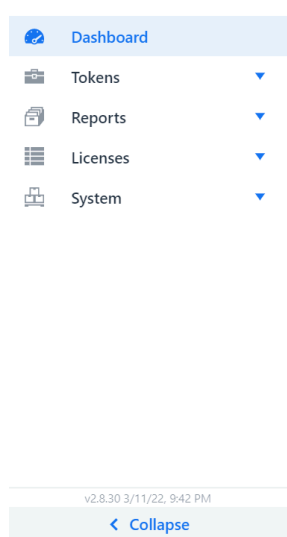
Navigation Menu

The following step describes how the customer administrator uses the Provisioning Manager Navigation menu:

- Log in to the <https://wfc-provisioning1.pttpro.zebra.com/admin/login>

The **Dashboard** is selected by default in the **Navigation** menu.

Figure 7 Expanded Navigation Menu



Use the **Navigation** menu to access the following information:

- **Dashboard**
 - **Tokens**
 - Tokens
 - Bootstraps
 - **Reports**
 - History
 - Events
 - **Licenses**
 - License
 - Assigned
 - **System**
 - Portal Users
 - Devices
 - **Software Version**
- To expand the **Navigation** menu, click **> Expand** provided in the menu. The menu is expanded by default.

- To collapse the **Navigation** menu, click [< Collapse](#) provided in the menu. The following shows the **Navigation** menu when collapsed.

Figure 8 Collapsed Navigation Menu



Tokens

Use the Tokens menu option to view and manage bootstraps and tokens.

Creating Bootstraps and Tokens

To create a bootstrap/token pair:

1. Add a bootstrap in the Provisioning Manager. For more about bootstrapping, see [Bootstrapping Overview](#) on page 10
2. Add a token using the Provisioning Manager, associate the new token with an existing bootstrap, and choose the client to which it applies to: `WFC_VOICE_ANDROID`, `WFC_PRO_ANDROID`, `WFC_PC_ANDROID` or `WFC_PRO_IOS`, `WFC_CENTRAL_SERVICE_ANDROID`.



NOTE: The PTT Pro PC Client for Windows is not supported.

For more information, see [Adding Tokens](#) on page 25.




As described in WFC Voice client licensing, two bootstrap/token pairs are automatically created for customers who have the WFC Voice Client, as illustrated in the following examples:

- The Direct Access bootstrap is empty (it contains empty brackets), indicating there is no associated configuration data. The Direct Access token is associated with the Direct Access bootstrap, and the Voice client App ID is displayed as follows:

Figure 9 Bootstrap Direct Access

Name	Parameters (JSON)
Direct-Access-Bootstrap	{}

Figure 10 Direct Access Tokens




Token/Device ID	App	QR-CODE	Bootstrap	JSON	Description
Direct-Access-Token			Direct-Access-Bootstrap		

- The Extension Manager bootstrap includes the `var_location` parameter, as defined in the WFC Voice PBX Administrator Guide and the Extension Manager Customer Administrator Guide. The Extension Manager token is associated with the Extension Manager bootstrap and with the Voice Client App ID. An example follows:

Figure 11 Extension Manager Bootstrap

Name	Parameters (JSON)
Extension-Manager-Bootstrap	{ "var_location" : "https://extension-manager.com/profiles/stores/?api_key=cust-secret" }

Figure 12 Extension Manager Token

Token/Device ID	App	QR-CODE	Bootstrap	JSON
Extension-Manager-Token			Extension-Manager-Bootstrap	

The Extension Manager Bootstrap `var_location` parameter includes:

- An API key is unique to each customer. Contact Zebra Technical Support to obtain your API key.
- Customize the `var_location` parameter to control the behavior of the WFC Voice client; for example, site identification, department identification, reservations, and other attributes can be specified. For information about configuring this parameter, refer to the Extension Manager Administrator Guide. Modify the Extension Manager bootstrap in the Provisioning Manager to include the desired options.

Using Tokens in the Device

Once the bootstrap and token are set up, the device must be programmed with the token. For instructions on using tokens to license WFC Voice clients, refer to the customer Welcome email, WFC Voice PBX Administrator Guides, or the WFC Voice Licensing Guide for 9.0.20306 and later.

Use one of the following options for using tokens:

- Scan the QR code associated with the token. The QR code is displayed next to the token in Provisioning Manager.
- Send an intent for the appropriate application. The intents in ADB format are as follows, where <token> is replaced by the token created:

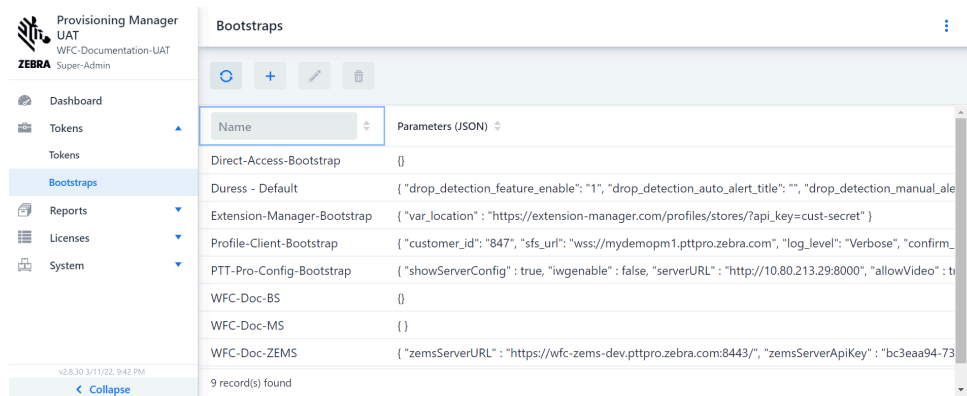
Client	Intent
PTT Pro Android client	<code>adb shell am start -a android.intent.action.VIEW -d "wfctp://<token>"</code>
Profile client	<code>adb shell am start -a android.intent.action.VIEW -d "wfcpp://<token>"</code>
WFC Voice client	<code>adb shell am start -a android.intent.action.VIEW -d "wfcvp://<token>"</code>
WFC Central Service	<code>adb shell am start -a android.intent.action.VIEW -d "wfccs://<token>"</code>

Adding Bootstraps

Before adding a token, add the bootstrap in the Provisioning Manager as follows:

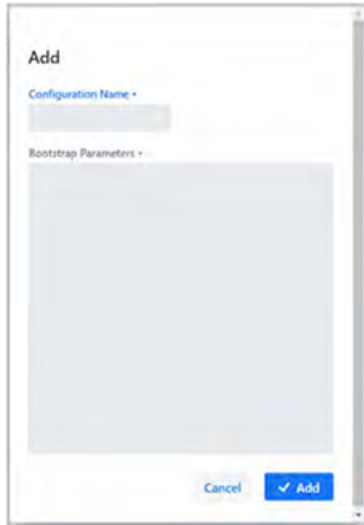
1. From the **Navigation** menu, select **Tokens > Bootstraps**.

In the right panel, the **Bootstraps** screen appears, which allows you to add, edit, delete, sort, and search the information.



2. Click the **Add** icon.

The **Add** bootstrap dialog box appears.

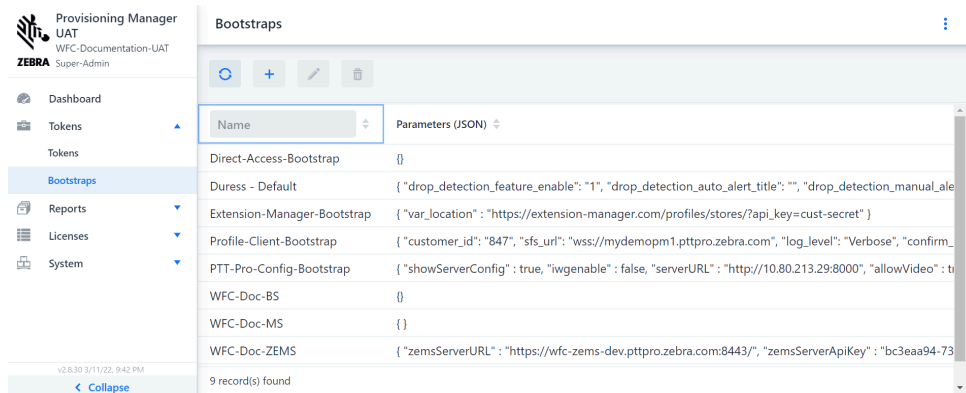


3. Enter the required information.

- The bootstrap must contain valid JSON and include the parameters supported by the intended client. Currently supported clients are WFC Voice, PTT Pro Android, and Profile Client.
- PVM only validates a valid JSON format, not the parameters contained within.
- The PTT Pro Android Client and the Profile Client support JSON-based configuration, but the WFC Voice Client uses an XML file. Convert the XML to JSON before adding to the bootstrap.
- No new parameters are introduced using bootstraps. For information about parameters available for configuration, refer to the WFC Voice PBX Administrator Guide and Profile Manager Administrator Guide.

4. Click **Add** to add the bootstrap.

The **Bootstrap** screen updates to display the added bootstraps.



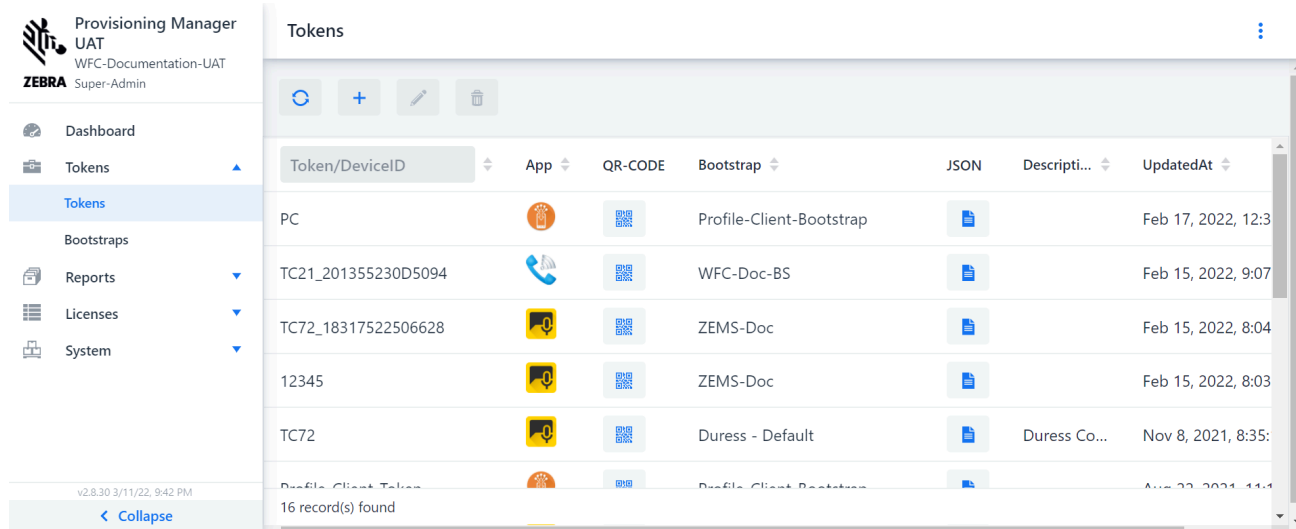
NOTE: If the list does not reflect the updates, click **Refresh**.

Adding Tokens

Ensure at least one bootstrap has been created before adding a token. For more information, see [Adding Bootstraps](#) on page 23.

1. Click the **Navigation** icon and select **Tokens > Tokens**.

In the right panel, the **Tokens** screen appears, which allows you to add, edit, delete, sort, and search the information.



2. Click the **Add** icon.
3. Enter the required data in the fields as described in the following table:

Table 4 Add Token Field Description

Fields Name	Description
Token	An alphanumeric (case insensitive) string not to exceed 64 characters. Provisioning Manager, Extension Manager, and Voice allow dash (-) as a special character in the token value. Avoid using other special characters as the token value because the token value is used in URL or HTTP headers.
App ID	In the drop-down list, select one of the following: <ul style="list-style-type: none"> • WFC_VOICE_ANDROID (WFC Voice client) • WFC_CENTRAL_SERVICE_ANDROID • WFC_PRO_ANDROID (PTT Pro on Android) • WFC_PC_ANDROID (Profile Client on Android) • WFC_PRO_IOS (PTT Pro on IOS)
Bootstrap	The value for bootstrap must be the name of one of the previously created bootstrap parameter sets.
Description	Short token description (optional).

Creating Bootstraps and Tokens with a Script

Use the Swagger APIs, accessible via the Provisioning Manager Portal, to generate a cURL command for adding a bootstrap or token. Insert the cURL command into a script that processes the bootstraps/tokens that need to be added to the Provisioning Manager.

The script must first authenticate with the Provisioning Manager by using `/admin/api/v1/auth/admin` with the body `{"username": "myUserName", "password": "myPassword"}`. Upon successful authentication, the Provisioning Manager returns an `accessToken` and `tokenType` ("Bearer"). These are combined into a `stringBearer <accessToken>` and sent as the authorization header shown in the cURL examples.

Example of a cURL command to add a bootstrap called "myBootstrap"

```
curl -X POST https:// <PVM URL>/admin/api/v1/bootstrap?name=myBootstrap
-H "accept: */*"
-H "authorization: Bearer <myAccessToken>"
-H "Content-Type: application/json"
-d "{\"site\": \"site-1094\"}"
```

Example of a cURL command to add a token called "myToken" using the "myBootstrap"

```
curl -X POST https:// <PVM URL>/admin/api/v1/token?appId=WFC_PRO_ANDROID
&bootstrap=myBootstrap&description=<optional-description>
&name=myToken
-H "accept: */*"
-H "authorization: Bearer <myAccessToken>"
```

Reports

Use the Reports menu option to access history and events logs.

History

To view, sort, and search for history information,

- From the **Navigation** menu, select **Reports > History**.

In the right panel, the **History** screen appears.

Customer	Timestamp	Action	Token	App	Dev
WFC-Dev-UAT	Mar 15, 2022, 3:30:17 AM	LICENSE	WFC-dev		TC51_
WFC-Dev-UAT	Mar 15, 2022, 3:14:16 AM	LICENSE	WFC-dev		TC51_
WFC-Dev-UAT	Mar 15, 2022, 3:13:11 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:12:46 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:12:17 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:12:07 AM	LICENSE	Activation_token		TC56_
WFC-Dev-UAT	Mar 15, 2022, 3:11:36 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:10:47 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:10:18 AM	LICENSE	TC52_18304522512397		TC52_
WFC-Dev-UAT	Mar 15, 2022, 3:04:36 AM	LICENSE	TC52_18304522512397		TC52_

60008 record(s) found

Events

To view, sort, and search user-specific information:

1. From the **Navigation** icon, select **Reports > Events**.

In the right panel, the **Events** screen appears.

Timestamp	User	All Types	Severity	Info
Mar 14, 2022, 9:35:02 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 8:35:03 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 7:35:01 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 6:35:02 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 5:35:03 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 4:35:01 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 3:35:02 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 2:35:03 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 1:35:01 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT
Mar 14, 2022, 12:35:02 PM		LICENSE_SYNC_GET	INFO	Ext3OPUAT

351 record(s) found

2. Select the user from the **User Filter** drop down list. If you have super-admin access, other customer appear in the drop down list.
3. From the **Event Type** drop down list, select the the specific event from the drop down.
The event information details display, based on the selected criteria.

Licenses

Use the Licenses menu to view license assignments.

Summary

To view license information, perform the following steps:

- From the **Navigation** icon, select **Licenses > Summary**.

The **Summary** screen appears.

Customer	State	License	AID	Total Purchased	Total Used	Expiration	Updated
Alcatel-DSPP	Active	Standard	***e295-c6... 1 Year Term	20	2	2/6/24, 5:29:59 AM	5/17/23 4/26/23,
Aruba Networks	Active	Standard	***4070-37... Trial	100	12	3/3/25, 5:29:59 AM	5/17/23 4/26/23,
Aruba Networks	Active	Premium	***a453-9c... Test	100	1	3/3/25, 5:29:59 AM	5/17/23 4/26/23,
Cisco requested by Ohad Shatil	Active	Standard	***a96e-0fb7 Trial	15	1	2/13/24, 5:29:59 AM	5/17/23 4/26/23,
Cisco requested by Ohad Shatil	Active	Premium	***17ff-438c Trial	15	0	2/13/24, 5:29:59 AM	5/17/23 4/26/23,
Cisco-IVT	Active	Standard	***8f46-38... Trial	10	0	4/28/26, 5:29:59 AM	5/17/23 4/28/23,
Cisco-IVT	Active	Premium	***3019-e6... 1 Year Term	10	7	9/30/24, 5:29:59 AM	5/17/23 4/26/23,
Cisco1	Active	Standard	***8f46-38... Trial	10	0	4/28/26, 5:29:59 AM	5/17/23 4/28/23,
Cisco1	Active	Premium	***29f3-c97a 5 Year Term	10	2	4/8/26, 5:29:59 AM	5/17/23 4/26/23,

118 record(s) found

Table 5 Summary Tab Column Description

Column	Description
State	ACTIVE indicates a valid license. EXPIRED indicates that the license has expired, been removed from the account, or is invalid in some other way.
License	Feature licenses associated with purchased products. Refer to Workforce Connect Voice Administrator Guide for Licensing for more information about each feature license.
AID	Activation ID associated with the feature license. Note that this is not used to activate the client.
Total Purchased	The total number of licenses purchased.
Total Used	The total number of licenses that have been assigned.
Expiration	Expiration date and time of your licenses.

Table 5 Summary Tab Column Description (Continued)

Column	Description
Created/Updated On Time	The top date/time indicates when the licenses were last verified with the licensing system. This value updates when the Provisioning Manager performs a nightly sync with the licensing system or if the licenses are synced manually by a Zebra administrator. The bottom date/time indicates when the licenses were added to the Provisioning Manager.



NOTE: If the list does not update immediately, use the **Refresh** icon to refresh the list.

Assigned

To view assigned licenses information:

- Click the **Navigation** icon and select **Licenses > Assigned**.

In the right panel, the **Assigned** screen appears.

Customer	License	Use Status	Device ID	Feature	Expiration
WFC_BLR_ST1	Unassigned	Not in use	EC30_191525230D0095	Rauland	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	EC30_191525230D0095	Local	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	EC30_182955201E0181	Basic CUCM	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	EC30_182955201E0181	Asterisk	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	EC30_182955201E0181	Mitel	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	EC30_182955201E0181	Generic PBX	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	TC52_181445225E0224	Basic CUCM	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	TC52_181445225E0224	Asterisk	5/18/23, 5:29:59
WFC_BLR_ST1	Unassigned	Not in use	MC20_210865230D5014	Generic PBX	5/18/23, 5:29:59

Table 6 Assigned Tab Column Description

Column	Description
Customer	Name of the customer.
License	Assigned status indicates that the device currently holds the feature license. Assigned licenses count towards the number of licenses used on the Summary page.
	Unassigned status indicates that the license is no longer assigned to the device.
Use Status	Use status indicates that the feature license is currently in use by the device. These licenses display as Unassigned in the License column.
	Not in Use status indicates that the license is not assigned to the device.

Table 6 Assigned Tab Column Description (Continued)

Column	Description
	Not in Use (*) status indicates a premium license not currently used by a device but still assigned to the device. This occurs, for example, when a device using a premium license logs out of the Extension Manager. To release the license, the device must be obsoleted. These licenses display as Assigned in the License column.
Device ID	The device to which the license is assigned.
Feature	The configured PBX in the device. Alcatel, Asterisk, CME standard, CUCM standard, IP Office, Mitel, and Rauland PBXs. Each PBX uses a Standard license, while Aura Premium, CUCM Premium, and CME Premium use a Premium license.
Expiration	The date and time when the license expires.
AID	Activation ID associated with the license.
App Version	The WFC Voice version used by this device is represented by the last part of the version. For example, for version 9.0.20406, only 20406 displays.
Updated/Created on	The top date/time indicates when the device was last in contact with the provisioning Manager. The bottom date/time indicates when the license was first assigned to the device.



NOTE: If the list does not update the newly registered devices, click **Refresh**.

System

Use the System menu option to access screens to add, change, or delete portal users and devices. This section provides details of Tokens, Reports, and Licensing.

Viewing Sites

The Provisioning Manager maintains a list of PTT Pro sites/departments for those customers who have PTT Pro to enable Automatic PTT Pro Provisioning. The customer can view the list of sites by displaying the Site tab in the PVM.

- Click a site to display the list of devices currently registered on that site.

The screenshot displays the Provisioning Manager interface. On the left is a sidebar menu with the following items: Dashboard, Tokens, Reports, Licenses, System, Sites (highlighted), Devices, and Portal Users. The main area is titled 'Sites' and contains a table with two columns: 'Name' and 'Pro Server Name'. The table lists five records, with 'CapPro0001' highlighted. Below this table, it indicates '5 record(s) found' and provides a link to view 'CapPro0001 devices'. This link leads to a detailed table for that site:

Device ID	State	Model	OS	Version
KAM_ZBRP_j1_1	Active	TC51	Android Oreo 1.0.1	9.0.22102

Devices

To view, sort, obsolete, and search device information:

1. From the **Navigation** menu, select **System > Devices**.

In the right panel, the **Devices** screen appears.

Figure 13 Devices

State Filter	Device Filter	Model/Version	Site/Assigned On	Updated/Created On
Active	TC21_201335230D5089	TC21 Android 11 11-26-05.00-RG-U00-STD-HEL-04		Jan 13, 2023, 9:10:50 PM Dec 5, 2021, 1:25:34 AM
Active	TC72_181175225E0136	TC72 Android 10 10-16-10.00-QG-U120-STD-HEL-04		Jan 4, 2023, 5:45:28 AM Jun 29, 2021, 7:56:15 PM
Active	TC72_18317522506628	TC72 Android 10 10-16-10.00-QG-U114-STD-HEL-04		Jun 14, 2022, 2:47:47 AM Feb 15, 2022, 8:04:39 PM
Active	TC77_19216522505484	TC77 Android 11 11-14-02.00-RG-U00-PRD-HEL-04		Apr 25, 2022, 4:50:41 AM Feb 12, 2021, 10:46:33 PM
Active	TC77_918883711374	TC77 Android 11 11-14-02.00-RG-U00-PRD-HEL-04		Apr 25, 2022, 4:46:49 AM Jun 2, 2021, 12:50:51 AM
Active	TC21_201355230D5094	TC21 Android 11 11-10-13.00-RG-U00-PRD-HEL-04		Mar 1, 2022, 9:45:37 PM Feb 15, 2022, 9:07:07 PM

2. Click the **Refresh** icon to refresh the list to include recently registered devices.
3. To view license information about a device, select the device ID. Similar license information is displayed in the **Assigned** tab.
4. To obsolete a device, select the device ID and click the **Obsolete** icon. The **Active** status of the device turns into **Inactive** status and the licenses are released.



NOTE:

- If the customer uses the Extension Manager, devices must be obsoleted in the Extension Manager.
- Obsoleting the device in the Extension Manager also obsoletes the same device from the Provisioning Manager.
- Obsoleting the device in the Provisioning Manager does not obsolete the same device from the Extension Manager.

Device IDs in the WFC Ecosystem

Device IDs are the primary means of identifying devices in the WFC ecosystem and are visible in most WFC Portals (For example, PVM, EXM, etc).

Zebra device IDs and iOS device IDs are constructed the same regardless of the WFC app version. Third-party Android device IDs are constructed differently based on the type of device and the version of the client being used.

The following table summarizes how device IDs are constructed. In the table below, “+” indicates concatenation.

Device Type	App Release	Device ID
Zebra Android devices	WFC PTT Pro or WFC voice, any release.	Model (Build. Model) + “_” + serial number.
iOS device	WFC PTT Pro only, any release.	Model + “_” + iOS ID.

Device Type	App Release	Device ID
Third-party Android devices*	PTT Pro Android prior to Android v3.3.10197 PTT Pro Android v3.3.10197 and later. WFC Voice v9.0.22308 and later.	OS prior to Android 10: model (Build. Model) + “_” + serial number. OS Android 10 or later: model (Build. MODEL) + “_” + Android ID. Model (Build. Model) + “_TAI” + Android ID. Spaces in Build. The Model is removed before using it in the device ID.
Zebra Android devices>=13	WFC Voice v9.0.22405 and later.	If the Model serial number is not found, then Model (Build. Model) + “_ZAI” + Android ID.



NOTE: A third-party Android device is identified by Build.MANUFACTURER not including “TAI”

Obsoleting Devices

Obsoleting a device means deleting the device from the WFC PTT Pro database if the device is registered for WFC PTT Pro, as well as releasing any voice licenses in use. As before, if a device is active in the Extension Manager, it must be obsoleted in the Extension Manager. Otherwise, the device can be deleted at the Provisioning Manager. The scenarios are described below:

Scenario	Obsoleting Procedure
The device has activated only the voice client; no EXM	Obsolete in PVM. The device is marked inactive in PVM, and voice licenses are released.
The device has been activated only in the Voice Client; EXM is in use.	Obsolete in EXM. The device is marked inactive in PVM and EXM, and voice licenses are released.
The device is registered for automatic provisioning for WFC PTT Pro only.	Obsolete in PVM. The device is marked inactive in PVM and deleted from the WFC PTT Pro database.
The device has been activated in the Voice Client and registered for automated provisioning for PTT Pro, no EXM.	Obsolete in PVM. The device is marked inactive in PVM, deleted from the WFC PTT Pro database, and voice licenses are released.
The device has been activated in the Voice Client and registered for automated provisioning for WFC PTT Pro; EXM is in use.	Obsolete in EXM. The device is marked inactive in PVM and EXM, deleted from the WFC PTT Pro database, and voice licenses are released. If this device is obsoleted in the PVM, the voice licenses in the EXM are not obsoleted and released.



NOTE:

To obsolete many devices, customers use a script through the PVM/EXM APIs.

Portal Users

The table User Roles describes the Provisioning Manager User Roles, which are the multi-levels of access for portal users.

Table 7 User Roles

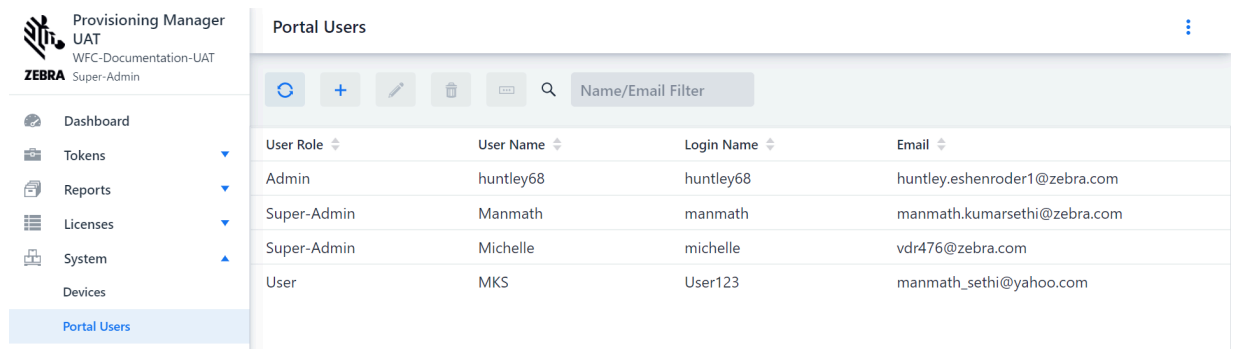
User Role	Customer VS Zebra	Description
Super-Admin	Customer-level	Highest level of customer access. The user with the Super Admin role can view licenses and modify tokens, bootstraps, and devices and can add other portal users.
Admin	Customer-level	Customer-level access. The user with the Admin role can view reports and view/modify tokens and bootstraps. This role cannot view licenses or other portal users.
User	Customer-level	Customer-level read-only access. The user with the User role can view reports, tokens, and bootstraps. This role cannot view licenses or other portal users.

To view, sort, search, update, and delete information in the Portal Users screen:

1. From the **Navigation** menu, select **System > Portal Users**.

In the right panel, the **Portal Users** screen appears.

Figure 14 Portal Users



2. To add a portal user, select the **Add** icon.
3. In the **Add** a portal user dialog box, enter the required data.
4. Click **Add** to add the portal user to the portal.

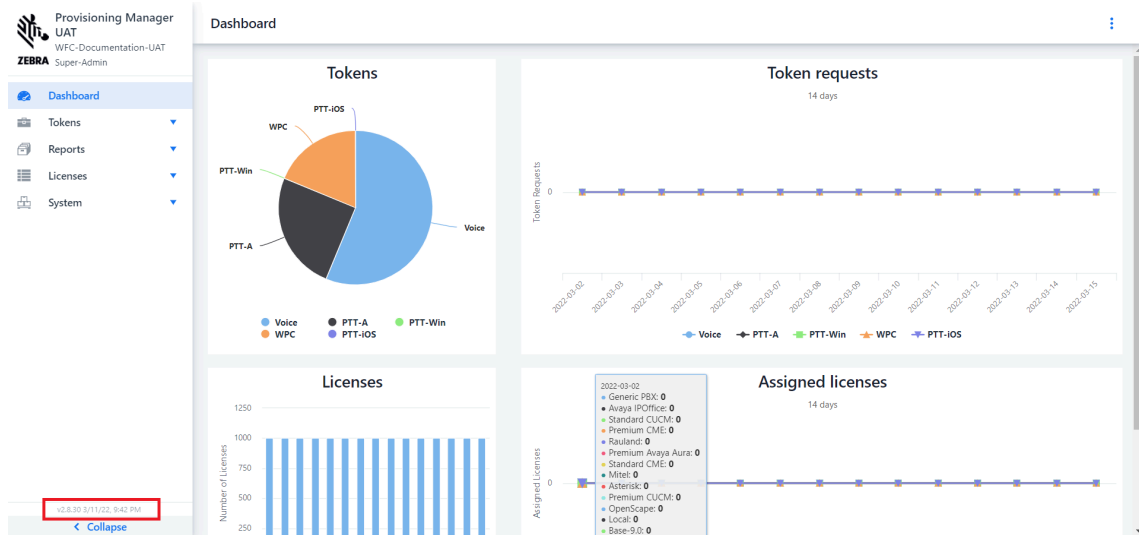


NOTE: If the list does not update immediately, use the **Refresh** icon to refresh the list.

Software Version

The software version at the bottom of the left panel of the Provisioning Manager indicates the software version running on the Provisioning Manager server.

Figure 15 Software Version



Third-Party Device Support and Automated Provisioning

Zebra supports the deployment of WFC Voice and PTT Pro clients on third-party Android devices. In addition, PTT Pro is supported on iOS.

For security reasons, Android started restricting access to device serial numbers in Android 10, which prevents most third-party devices from identifying themselves with serial numbers as Zebra devices do. The serial number has always been restricted for iOS devices.

WFC applications on third-party devices use the Android ID or iOS UDID, non-permanent identifiers. These device IDs are re-generated upon factory reset, which has the following impact on WFC applications:

- WFC Voice licenses may be tied to device IDs (Android IDs) that are no longer associated with any currently active device due to device reset.
- The PTT Pro device table, used for shared devices that authenticate with OAuth, may be populated with device IDs that are no longer associated with any currently active device due to a device reset.

The remainder of this chapter describes the operation and requirements of the system for third-party devices, including Automatic PTT Pro Device ID provisioning is supported by PVM when Profile Manager is not deployed. The Profile Manager manages PTT Pro device IDs in environments where it is deployed.

Device and Client Requirements

Devices and WFC Client versions must meet the following requirements:

- WFC Voice on third-party devices and automatic PTT Pro provisioning are supported on Android 8 and above. Current PTT Pro supports third-party devices and does not have to meet these requirements.
- Third-Party Android devices are supported on WFC-Voice v9.0.22308 or above.
- All PTT Pro Android versions support third-party devices. To support automatic PTT Pro Device ID Provisioning as described in this document, the PTT Pro Android version must be v3.3.10197 or above.
- The PTT Pro iOS version must be v1.0.11086 or above to support automatic provisioning as described in this document.

Limitations

- Premium voice licenses, including Cisco Premium, CME Premium, and Aura Premium, are not supported on third-party devices.

Support of WFC Voice for Third-Party Devices

In the WFC Voice ecosystem, the PVM and EXM assign licenses to devices as requested. The role of PVM and EXM in voice licensing is described in the WFC Voice Client Licensing section of the PVM Customer Administration Guide. The licenses are registered against the device ID. For Zebra devices, this is the device serial number. For Third-Party Devices, the device ID is constructed as described in the [Third-Party Device IDs](#) and includes the Android ID. As previously mentioned, the Android ID is non-permanent. When the device is factory reset, a new Android ID, and therefore a new device ID is generated. Any license registered under the previous device ID is orphaned and is not associated with any currently active device.

The following mechanisms exist to ensure that licenses are not tied to Inactive device IDs indefinitely.

Extension Manager (EXM)

The EXM assigns extensions and licenses when the device is registered to the EXM. When the device signs out, the EXM releases extensions and the associated standard licenses. If the device is still signed in but does not check in within the release interval (one hour), the EXM releases extensions and associated standard licenses. Premium licenses are not released.

Provisioning Manager (PVM)

When the device is not connected to the EXM, licenses are obtained directly from the PVM. Standard licenses are released if the device is not checked in within the release interval. The release interval is set to 30 days.

Support of PTT Pro for Third-Party Devices

Third-party devices are already supported for PTT Pro clients. However, managing third-party device IDs becomes complicated for customers using the PTT Pro shared device model.

PTT Pro customers deploying a shared device model must provision device IDs in the PTT Pro server device table of the appropriate site (called department in PTT Pro). Third-Party Devices complicate provisioning the device IDs because:

- The device ID is unknown until the PTT Pro application is loaded and opened on the device. Only then the device ID can be read out and provisioned into the PTT Pro server device table.
- The device ID changes after a factory reset, meaning the new device ID must be re-provisioned into the PTT Pro device table. In addition, the old device ID is now invalid and no longer tied to an active device.

To manage third-party device IDs more simpler, Automatic PTT Pro Device ID Provisioning (automated provisioning of the device ID in the PTT Pro devices table) for new customers has been added to the system. It can be used for Zebra devices as well as third-party devices.

Automatic Provisioning Overview

The PVM enables a simpler way of managing device IDs, for both third-party devices and Zebra devices. Provided with the device ID and site ID, the PVM provisions of the PTT Pro device table for that site. In addition, the PVM removes device IDs from the PTT Pro device table if the device is not checked-in. The parameter controlling this removal defaults to 30 days.

Automatic provisioning requires the latest release of PTT Pro Android or iOS. Refer to [Device and Client Requirements](#) on page 35.

The customers who activate with the activation codes do not need to provision devices into the PTT Pro device table and therefore do not benefit from or require automatic provisioning.

Customers using the shared device model are not required to use automatic provisioning but are then required to manually provision the PTT Pro device table.

Enabling Automatic WFC PTT Pro Provisioning

To enable automatic WFC PTT Pro provisioning, the following steps are required:

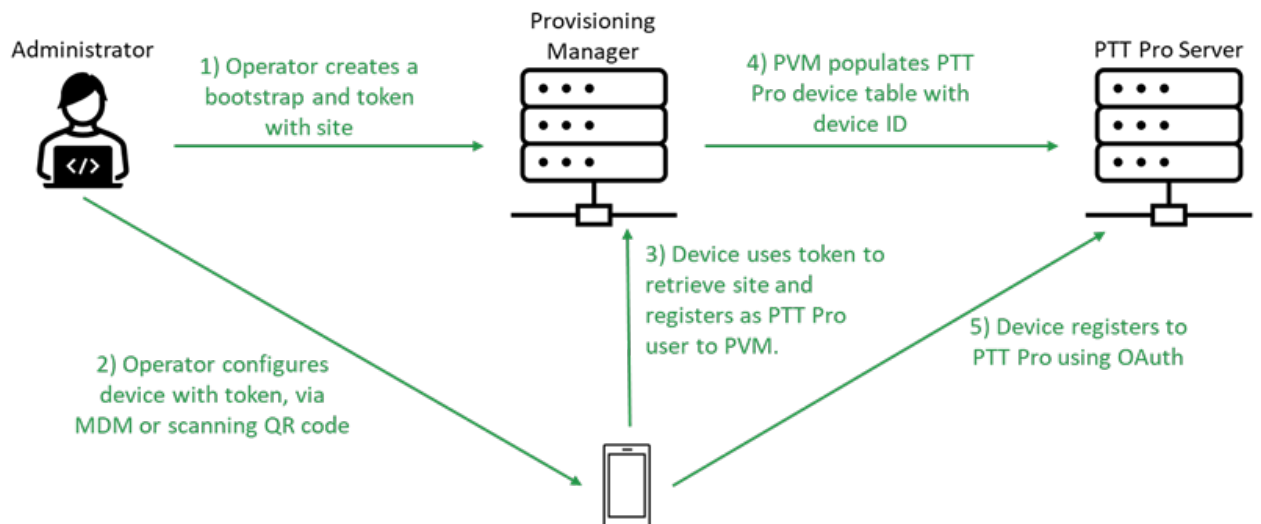
1. [Create a bootstrap](#) with the site ID, and then create a token using bootstrap. Other information may be included in the bootstrap (for example, task tracker or ZEMS configuration information).

Using the APIs, customers with many sites use a [script to add bootstraps and tokens](#) to the Provisioning Manager.

2. Configure the token in the device, for example, via MDM or scanning the token QR code.
3. The device uses the token to retrieve the site and then registers with the Provisioning Manager.
4. Upon receiving the registration, the PVM provisions the device ID in the WFC PTT Pro device table.

To change the site, a device is registered/provisioned in and re-scan with a different token/site. It moves the device from the current site to the new site.

The token must be configured in the device after installing WFC PTT Pro but can be configured either before or after activating WFC PTT Pro. If the device has already activated WFC PTT Pro and failed, it is reregistered after receiving the token and registering with the Provisioning Manager.



Devices that have registered for automatic provisioning as described above are recognizable in the PVM on the Devices tab, where the registered site is displayed. Refer to the **Device** section of this WFC Provisioning Manager Customer Administrator Guide.

To be able to provision bootstraps and tokens, the customer and customer administrator must be provisioned in the PVM to configure tokens and bootstraps. Contact Zebra Support if you don't have access to the Provisioning Manager.

The following table summarizes the options for customers using the shared device model (customers using Activation Codes do not need to populate the WFC PTT Pro device table):

5.

Shared Device Model Summary

App Release	No Token w/site	Using Tokens with Site
WFC PTT Pro Android prior to v3.3.10197 WFC PTT Pro iOS prior to v1.0.11086	Using a token with the site has no effect on earlier versions of WFC PTT Pro. Customers must populate the device ID into the WFC PTT Pro device table manually.	
WFC PTT Pro Android v3.3.10197 and later WFC PTT Pro iOS v1.0.11086 and later	Customers must populate the device ID into the WFC PTT Pro device table manually.	The device ID is automatically populated in the WFC PTT Pro table and automatically removed after a period of inactivity.

**WARNING:**

If a device is manually populated in a WFC PTT Pro device table and then that device goes through automatic provisioning, the results can be unpredictable.

1. If the device ID manually populated is the same as the device ID being automatically provisioned and the site is the same, automatic provisioning succeeds.
2. If the device ID manually populated is the same as the device ID being automatically provisioned, but it is registering to a different site, automatic provisioning fails. The device ID must be deleted manually from the incorrect site.
3. If the device ID manually populated is different from the device ID being automatically provisioned, the system does not recognize that these devices are the same, and both device IDs remain in the system. The manually populated device ID is not subject to automatic removal.

