

# PTT Pro

## Workcloud Communication



**ZEBRA**

## **Installation Guide**

2024/04/01

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](https://zebra.com/linkoslegal).

COPYRIGHTS: [zebra.com/copyright](https://zebra.com/copyright).

PATENTS: [ip.zebra.com](https://ip.zebra.com).

WARRANTY: [zebra.com/warranty](https://zebra.com/warranty).

END USER LICENSE AGREEMENT: [zebra.com/eula](https://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

<b>About this Guide.....</b>	<b>5</b>
Chapter Descriptions.....	5
Notational Conventions.....	6
Icon Conventions.....	6
Related Documents.....	6
Service Information.....	7
Revision History.....	7
<b>Installing Zebra PTT Pro on Android Devices.....</b>	<b>9</b>
System Requirements.....	9
Install the Application.....	9
Google Play Store Availability.....	10
Install Using Google Play Store (GMS Devices Only).....	10
Install Using a Sideload Method.....	12
Install Using Email (GMS Devices Only).....	13
Activate and Grant Permissions.....	14
Activate Zebra PTT Pro.....	14
Grant Permissions to PTT Pro for Android.....	17
Install PTT Lite.....	27
<b>Installing Zebra PTT Pro for iOS.....</b>	<b>29</b>
PTT Pro for iOS System Requirements.....	29
Apple App Store Availability.....	29
Installing PTT Pro for iOS By Email.....	29
Installing PTT Pro for iOS Manually.....	34

- Installing PTT Pro for iOS with an MDM..... 35
  - Configuring the PTT Pro for iOS with Profile Manager..... 36
  - Example iso\_mdm\_specfile.plist.....36
  - Example ios\_mdm\_specfile.....37
- Activating PTT Pro for iOS.....40
  - Entering an Activation Code for PTT Pro for iOS..... 41
  - Activate PTT Pro for iOS With Profile Manager.....42
- Troubleshoot Activation Issues..... 46**
- Firewall Configuration and Troubleshooting.....47**
  - Configure the Firewall..... 47
  - Troubleshoot Firewall Issues.....48
- Open Source Software Disclosure.....51**
  - OpenSSL..... 51
  - Opus CODEC..... 52

# About this Guide

This guide describes the installation, activation, and configuration of Workcloud Communication PTT Pro for Android. The features and operation of each application are described separately in corresponding guides. Go to [Related Documents](#) for a list of guides.



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



**NOTE:** Email and text activation is only supported in the United States and Canada.



**WARNING:**

The Workcloud Communication PTT Pro supports using secure protocols, such as HTTPS, and cleartext network traffic, such as cleartext HTTP. Zebra strongly recommends customers use secure protocols such as HTTPS to access their data. Zebra always uses the secure protocol HTTPS to communicate with a PTT Pro Server or Provisioning Manager. If customers elect to use cleartext network traffic, the customer assumes the risk of exposing data on the network.

## Chapter Descriptions

Topics covered in this guide are as follows:

- [Installing Zebra PTT Pro on Android Devices](#) describes installing PTT Pro on an Android AOSP and GMS device.
- [Installing Zebra PTT Pro on iOS](#) describes how to install PTT Pro on an iOS device.
- [Accessing Zebra PTT Pro Management Portal](#) describes how to access Zebra PTT Pro Management Portal.
- [Activation Troubleshooting](#) describes how to avoid certain issues when activating PTT Pro.
- [Firewall Configuration and Troubleshooting](#) describes how to configure and troubleshoot firewall issues.

## Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown 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.

## Related Documents

- Workcloud Communication PTT Pro for iOS User Guide Discusses Zebra PTT Pro for iOS features and operation.
- Workcloud Communication PTT Pro for Android User Guide Discusses Zebra PTT Pro for Android features and operation.
- Workcloud Communication PTT Pro Management Portal Discusses the portal, which provides an interface for administrators or technical representatives to manage an organization's PTT Pro accounts.
- Workcloud Communication Provisioning Manager Customer Administrator Guide Discusses the configuration and licensing of Workcloud Communication clients.

For the latest version of this guide and all guides, go to [zebra.com/support](https://zebra.com/support).

### Service Information

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

Changes to the guide are listed below:

Change	Date	Description
MN-002658A-03 Rev A	November 2018	Updated Android Installation information.
MN-002658A-04 Rev A	November 2019	Updated the list of Google API addresses in Configure Firewall section.
MN-002658A-06 Rev A	December 2019	Updated supported versions of Windows and Android.
MN-002658A-07 Rev A	March 2020	Added note about ESN activation on Android 10.
MN-002658A-08 Rev A	June 2020	Updated Android installation instructions for Play Store and Android 10.
MN-002658A-09 Rev A	September 2020	Updated for the new version of the iOS client.
MN-002658A-09 Rev B	September 2020	Fixed URL reference.
MN-002658A-09 Rev C	November 2020	Fixed URL reference and added a note to the iOS install process.
MN-002658A-10 Rev A	June 2021	Updated for Android 11, IOS changes added legacy Android Installation.

## About this Guide

Change	Date	Description
MN-002658A-11 Rev A	June 2022	Updated for PTT Lite and supported versions of Android and iOS. Removed Gen 1 client installation instructions.
MN-002658A-12 Rev A	September 2022	Added app availability information for Google Play and Apple App stores. Updated spec and mdm files for iOS.
MN-002658A-13 Rev A	March 2023	Updated supported operating systems and permissions for Android 13.
MN-002658A-14 Rev A	March 2024	Rebranded to Workcloud Communication and updated activation of PTT Lite.



# Installing Zebra PTT Pro on Android Devices

This chapter describes the system requirements for PTT Pro for Android, methods for installing the software, and activating the client.

PTT Pro for Android supports two types of Android systems:

- AOSP (Android Open Source Project)
- GMS (Google Mobile Services)



**NOTE:** In order to complete the activation of the PTT Pro for Android, the system administrator first must provision a user in the Workcloud Communication PTT Pro Management Portal.

## System Requirements

Installation of PTT Pro for Android is supported on the following versions of Android and requires location configuration.

- Android versions 8, 10, 11, and 13.
- Location must be enabled in Settings to take advantage of the full PTT Pro for Android functionality.

## Install the Application

Installation of the PTT Pro for Android client software can be accomplished in multiple ways, and the enterprise may choose the method that works best for their mode of operation. These methods are described below.

Android devices can be classified as GMS (Google Mobile Services) devices or AOSP (Android Open Source Project) devices (also known as non-GMS devices).

The supported installation methods for GMS and AOSP devices differ as indicated in the following table:

**Table 1** Installation Methods

Method	GMS or ASOP	Description
Mobile Device Management (MDM)	Both	Download the PTT Pro for Android client software via MDM, if supported by your enterprise. Many enterprises use MDMs to manage the applications and other aspects of their Android devices. Using a file manager, find the APK on the device and click it to install.
Sideload	Both	Install the PTT Pro for Android application without using Google Play store via one of the many sideloading methods.

**Table 1** Installation Methods (Continued)

Method	GMS or ASOP	Description
App Store	GMS	Search for PTT Pro for Android and follow the instructions to install the software on the device.
Email	GMS	Click on the link to the software download package contained in the email from your system administrator. In order to use this method, the user must be provisioned in the Workcloud Communication PTT Pro Management Portal.

MDM and sideloading are well-known techniques already in widespread use and which vary between devices and MDM platforms.

## Google Play Store Availability

PTT Pro for Android Client v3.3 is not available in the following countries from the Google Play Store:

- China
- Egypt
- Georgia
- Jordan
- Qatar
- Pakistan

## Install Using Google Play Store (GMS Devices Only)

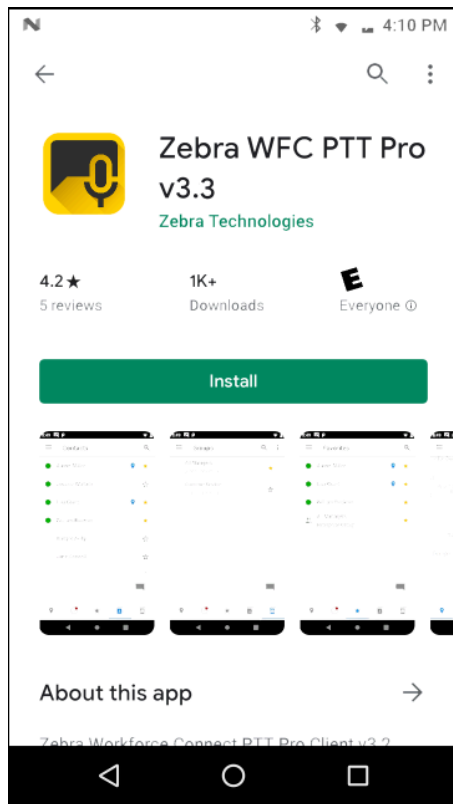
To use this method, the following prerequisite exists:

A Google account is required to download the software from the Google Play Store.

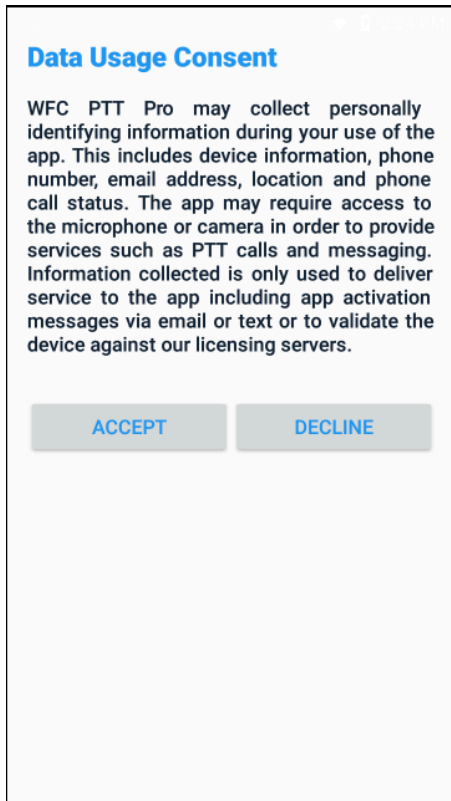
1. Go to <https://play.google.com/store/apps/details?id=com.symbol.wfc.pttpro> or search for Zebra PTT Pro v3.3. The Zebra PTT Pro application displays. Tap the icon to see the application details.

2. Tap **Install** on the **Zebra PTT Pro Application Details** screen.

If you are not logged into Google, you will be prompted to log in. Tap **Sign In**, fill in your login details and tap **Next**.



3. Select **OPEN** and the Data Usage Consent screen displays.



4. Tap **ACCEPT**. If the user declines, Zebra PTT Pro displays a message and exits. The Data Usage Consent appears the next time PTT Pro is started.
5. Proceed to [Activate and Grant Permissions](#) for details on activating the software.

### Install Using a Sideload Method

Sideloading allows the installation of Android applications without using the Google Play Store. You can choose multiple methods to sideload the app. These include the AirDroid application, Android Debug Bridge (ADB), and manual installation. This section describes the manual installation method.

The sideload method requires the following:

- Access to the PTT Pro for Android APK is required for sideloading. Contact your system administrator or Zebra customer manager for more information.
- A File Manager or other Android application is required to allow you to traverse the device's file structure.
- You must enable **Unknown Sources** in Security Settings. You may disable it again after the installation process is complete.

#### Sideload PTT Pro for Android

1. Copy the PTT Pro for Android APK to your computer.
2. Connect the Android device to a computer (for example, using a USB port).
3. Copy the PTT Pro for Android APK to your Android device.

4. Use the File Manager to locate the PTT Pro for Android APK.
5. Click the APK file to install PTT Pro for Android.
6. When the application has completed installation, click **Done** to exit the installation process, or click **Open** to open the application, and proceed to [Activate and Grant Permissions](#) for details on activating the software.

### Install Using Email (GMS Devices Only)

You can install PTT Pro for Android by downloading the APK from an email sent by the PTT Pro Server.

Installing the app from an email or text message requires the following:

- A valid email address where the activation email can be received must be available and accessible by the device. This email does not have to be unique; (for example, it can be used to install software on multiple devices).
- The system administrator must provision the user in the Workcloud Communication PTT Pro Management Portal with a valid email address. This causes an installation email with instructions for installation to be generated.
- A Google account is required to download the software from the Google Play store.



**NOTE:** Email and text activation is only supported in the United States and Canada.

1. Open the Workcloud Communication PTT Pro Activation email on the device where the application is being installed. Click the setup link to initiate installation. An example email extract follows:

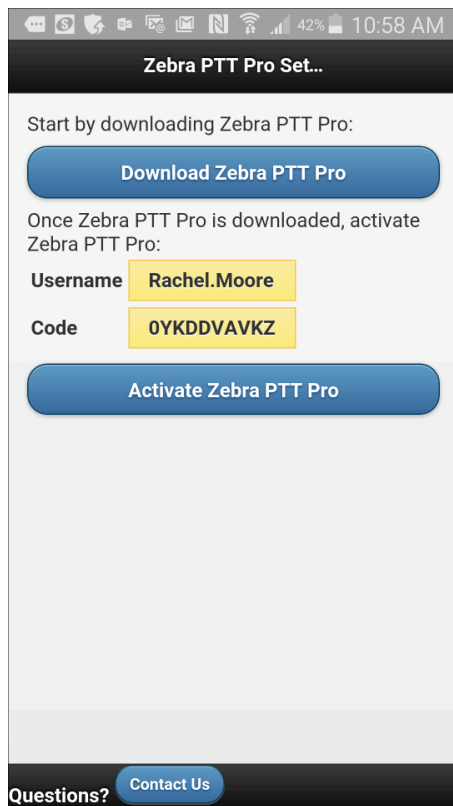
Please use the information on the following link to setup Zebra PTT Pro:

<https://provision.pttpro.zebra.com/setup.php?ac=0RFTLEHXMT>

For questions and additional support, please contact your internal IT Department help desk.

Thank you,  
The Zebra PTT Pro Support Team

2. A PTT Pro for Android Setup screen will open using the device browser. Select **Download Zebra PTT Pro**. Do not dismiss this window, as you will need to return to it after installation to complete the activation of the application.



The Zebra PTT Pro application page opens when you tap **Download** in the Google Play Store.

3. At this point, the installation instructions are identical to [Install Using Google Play Store \(GMS Devices Only\)](#), starting with Step 2: Select **Install**.

## Activate and Grant Permissions

After you install PTT Pro for Android, activate the application, and give the app permission to access device functions.

### Activate Zebra PTT Pro

Activation correlates the application on the device with a provisioned user in the Workcloud Communication PTT Pro Management Portal. This is required in order for permissions, contacts, groups, and other information particular to that user to be available.

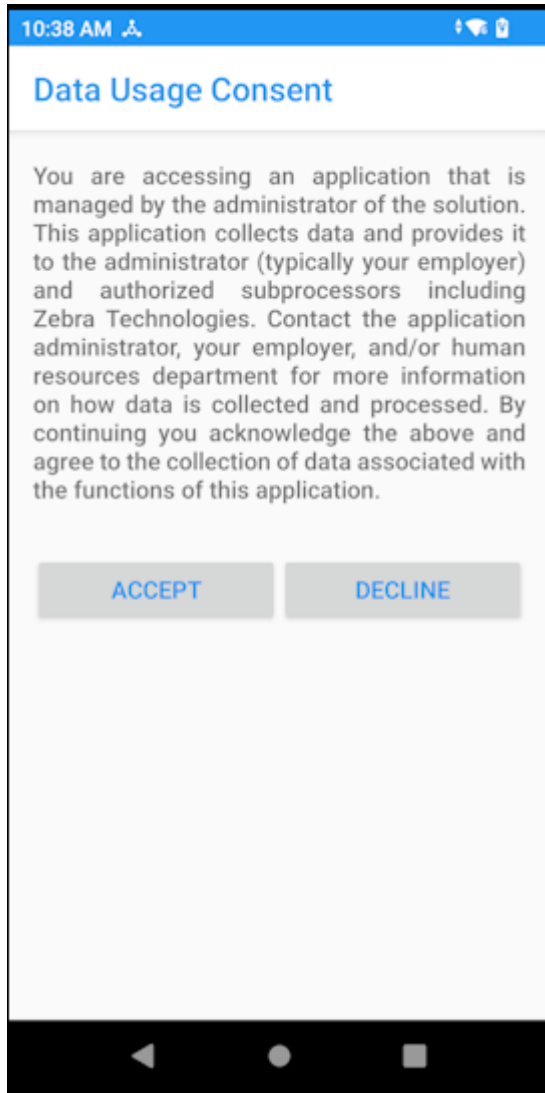


**NOTE:** Before performing the activation process, see [Troubleshoot Activation Issues](#).

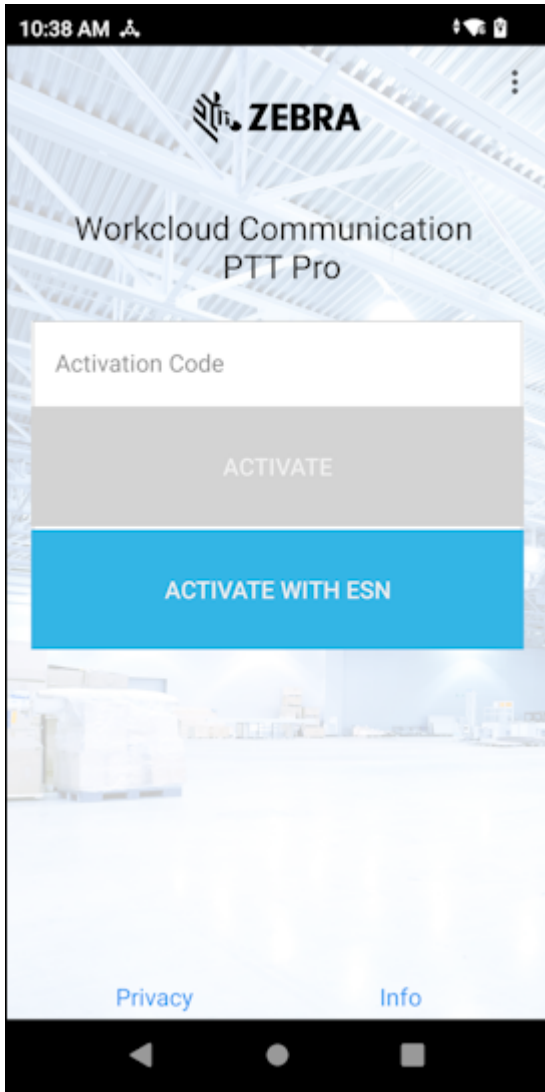
For a device to be activated, a user must be provisioned in the Workcloud Communication PTT Pro Management Portal. An activation code must be associated with the user in the portal (i.e. the user can not be inactive). If the user is inactive, they must be activated as described in the Workcloud Communication PTT Pro Management Portal Customer Administrator Guide.

After you install and open PTT Pro for Android, the Data Consent screen displays, followed by the Activation Options screen.

**Figure 1** Data Consent Screen for PTT Pro for Android



Accept the Data Usage Consent to proceed with the activation of PTT Pro for Android.



1. Enter the activation code associated with the desired user.

For example, if this device with PTT Pro for Android is intended for the user Diane.Newland, the activation code associated with Diane.Newland in the Workcloud Communication PTT Pro Management Portal should be entered in the **Activation Code** field. Contact your system administrator if you do not know the proper activation code.

2. Click **Activate** or **Activate with ESN**.

If the user clicks **Activate with ESN**, then the administrator needs to have populated the device's serial number for the activation code in Workcloud Communication PTT Pro Management Portal.



## Grant Permissions to PTT Pro for Android

After you install the PTT Pro for Android app, provide permissions to ensure the app functions properly. Permissions are different for different versions of the Android OS. Choose the correct permissions for the OS of your device.

### Android 13 Permissions

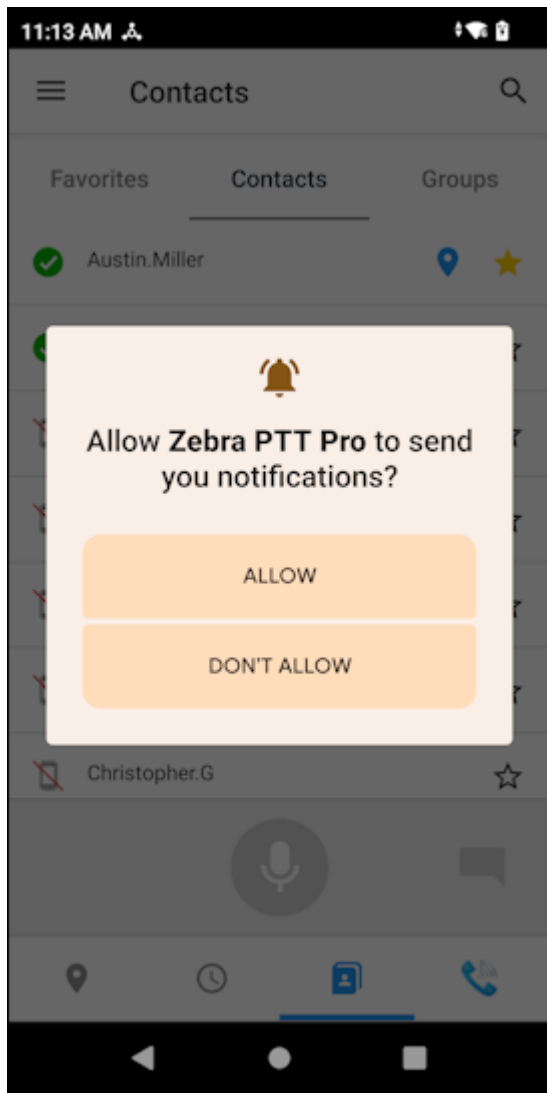
Android 13 introduces new permissions and modifies the location permission. The permission to display over other apps and to record audio is similar to previous versions of Android. PTT Pro for Android requires these permissions to function properly.

#### Allow Notifications

Allow Notifications is a new permission in Android 13.

Select **ALLOW** to receive notifications for messages and PTT calls.

**Figure 2** Allow Notifications Permission

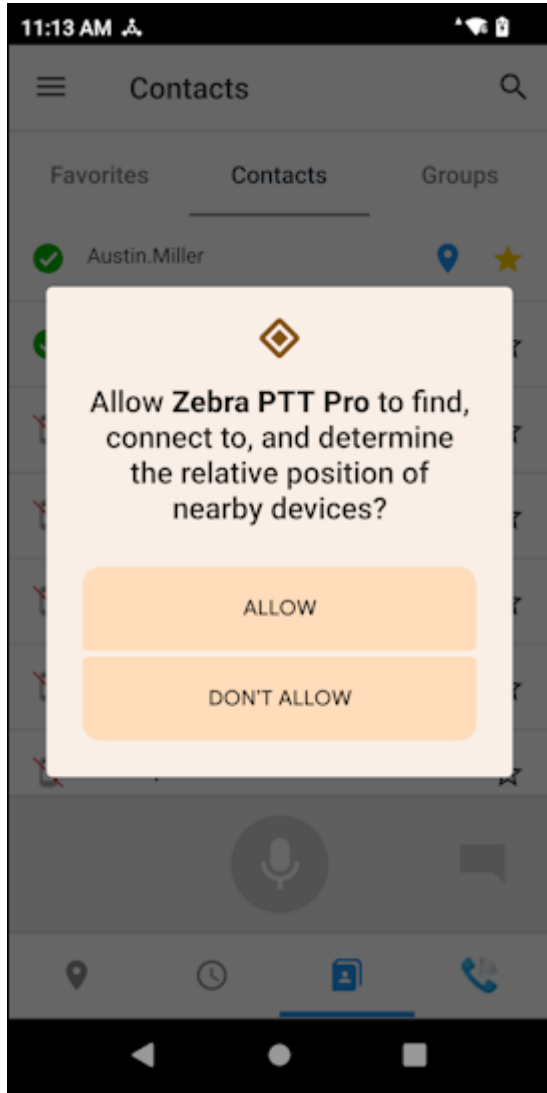


## Find Nearby Devices

Find Nearby Devices is a new permission in Android 13. PTT Pro for Android requires permission to support Bluetooth BLE devices.

Select **ALLOW**.

**Figure 3** Find Nearby Devices Permission

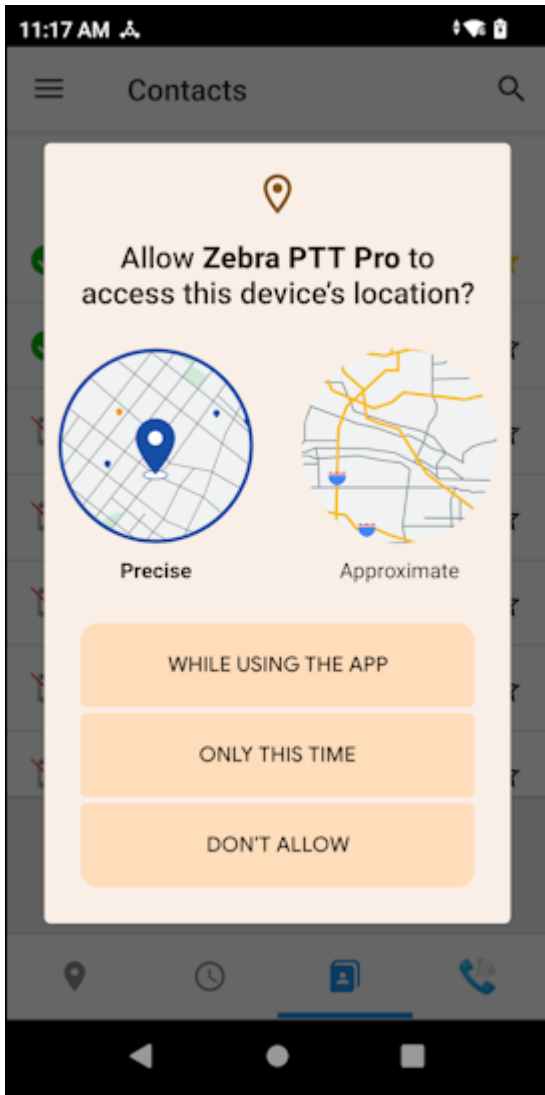


## Location

The Location permission has changed in Android 13. You have the option of sharing your precise location or an approximate location. A precise location is required for features such as Drop Detect and improves the experience of making calls and sending messages through the map.

Select **Precise** and **WHILE USING APP**.

**Figure 4** Location Permission

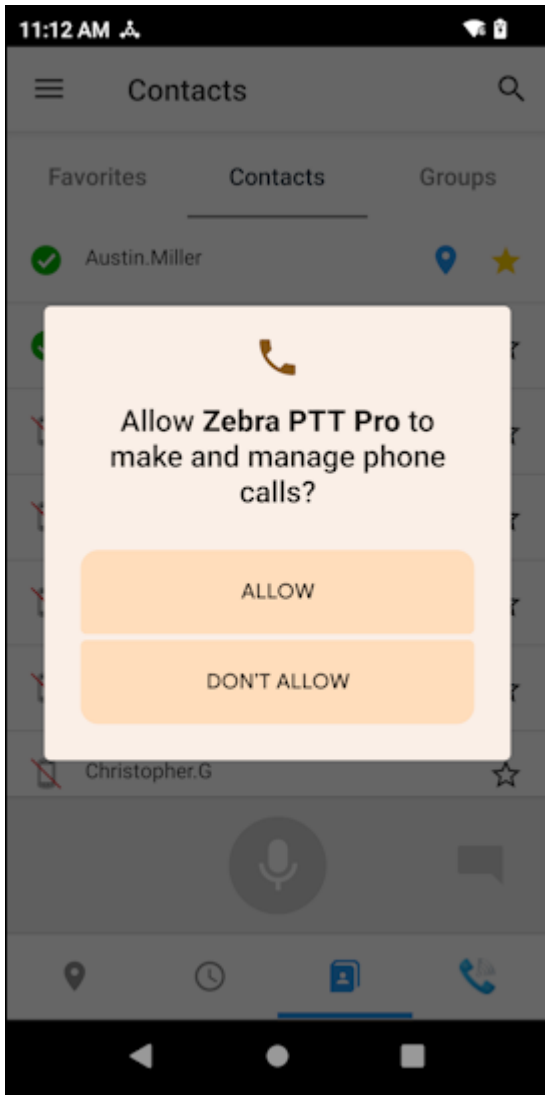


**Make and Manage Phone Calls**

The Make and Manage Phone Calls permission enables PTT Pro for Android to respond properly to incoming calls and messages.

Select **ALLOW**.

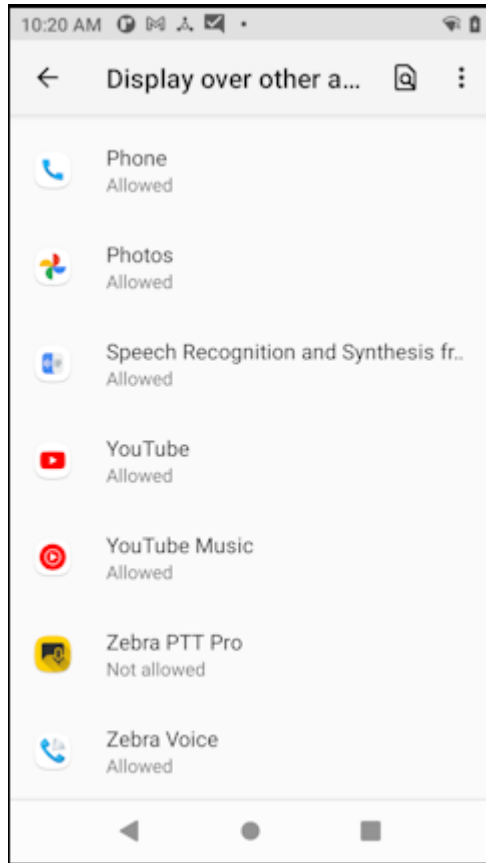
**Figure 5** Make and Manage Phone Calls Permission



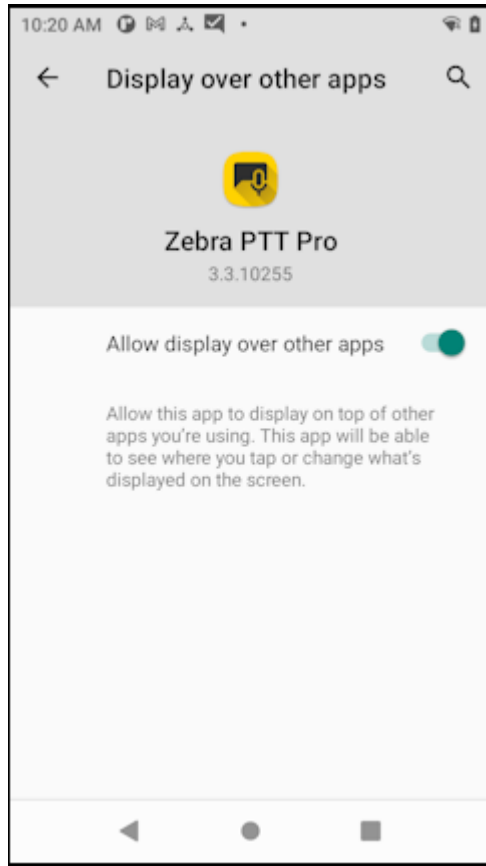
## Android 11 Permissions

PTT Pro for Android requires the following permissions when running on Android 11. These permissions enable the app to function properly.

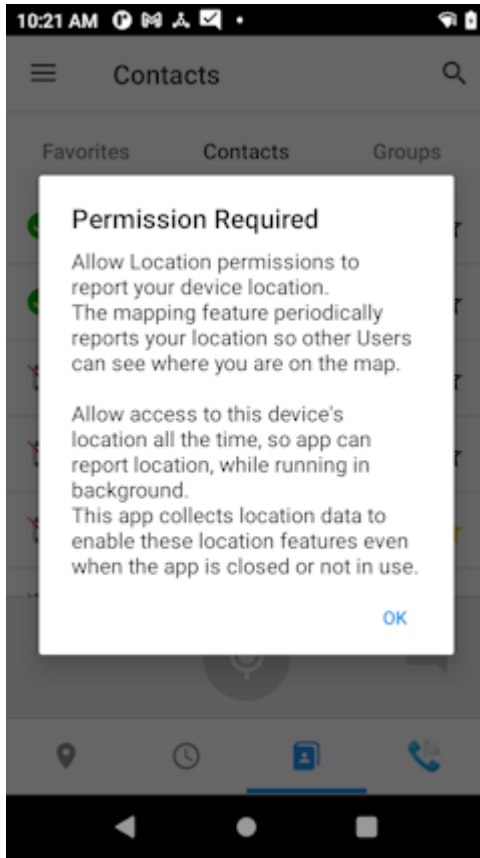
1. The **Display over other apps** screen appears. Scroll down, tap Zebra PTT Pro, and enable the permission.



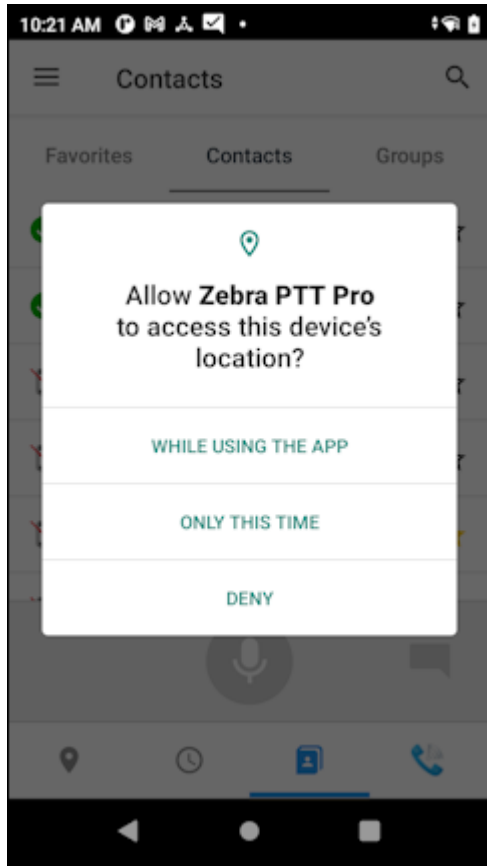
## Installing Zebra PTT Pro on Android Devices



2. The **Permission Required** screen displays.

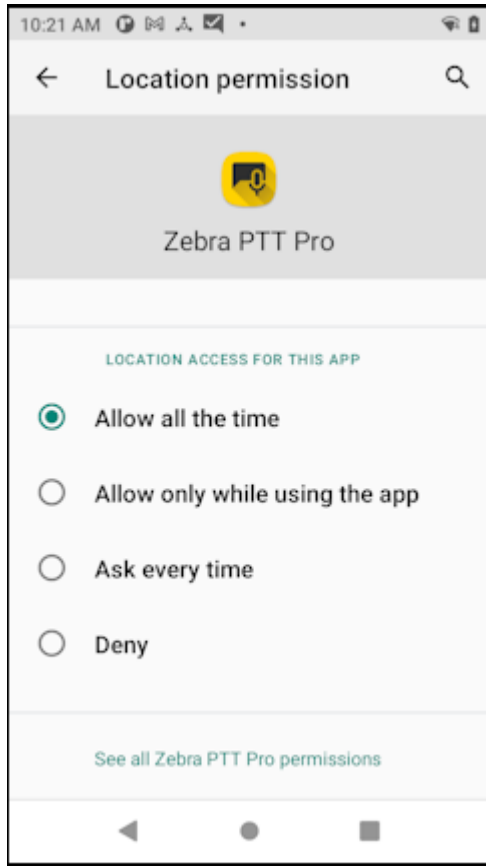


a) Tap **OK** and the **Allow Zebra PTTPro to access this device's location?** screen displays.



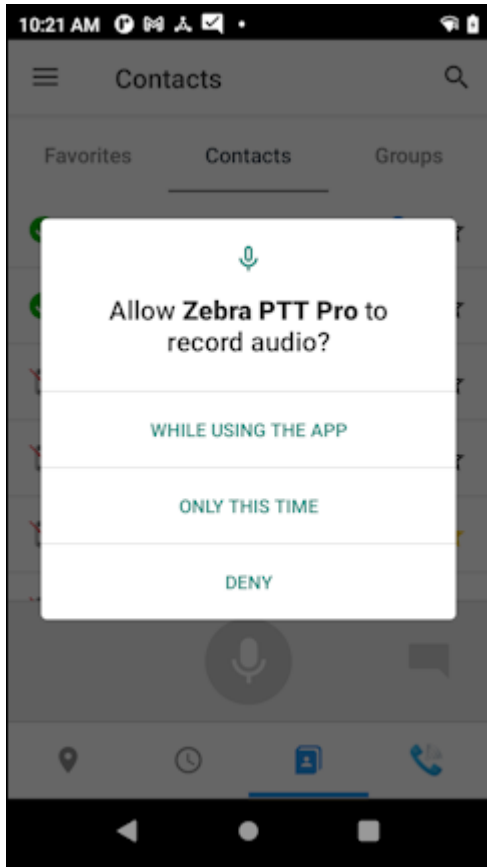
- b) Tap **WHILE USING THE APP** and the **LOCATION ACCESS FOR THIS APP** displays.





c) Tap **Allow all the time**.

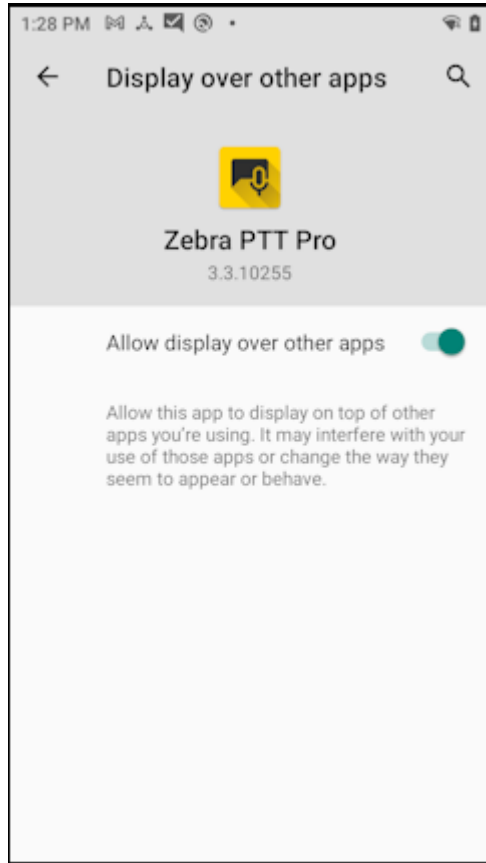
3. The **Record Audio** permission screen displays. Select **WHILE USING THE APP**.



## Android 10 and Below Permissions

PTT Pro for Android requires the permissions described below to function properly on Android 10 and Android 8.

1. The **Display over other apps** screen appears. Toggle the slider to the on position.

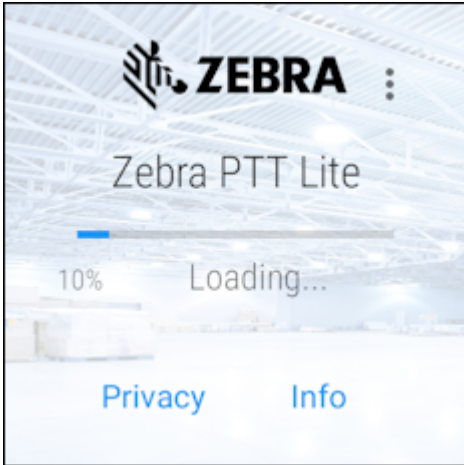


2. Tap the back arrow to return to the installation screens.
3. The **Permission Required** screen displays for location permission. Tap **OK**.
4. The PTT Pro for Android application asks permission to access the phone, audio, location, photos, media, and files. Grant the application permissions to ensure proper performance.

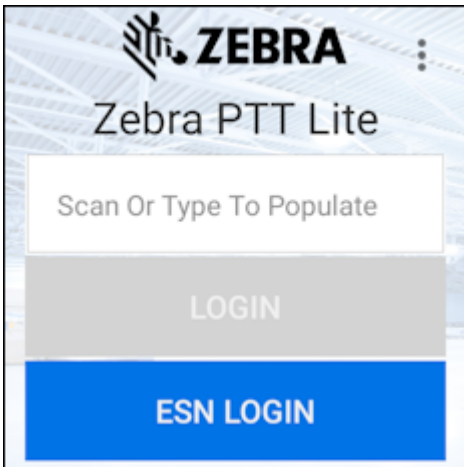
## Install PTT Lite

PTT Lite is intended for use on Zebra WS50 Android Wearable Computer devices. The installation uses the same Android application package (APK) as PTT Pro for Android. Install PTT Lite using the sideload method.

Follow the procedure described in [Sideload Zebra PTT Pro](#) to install PTT Lite. When PTT Lite starts, you see the Loading screen.



PTT Lite displays the activation screen after loading the first time.



To activate PTT Lite using ESN LOGIN, refer to the OAuth2 Device Authorization section in the Workcloud Communication PTT Pro for Android User Guide.

# Installing Zebra PTT Pro for iOS

This section describes the installation and activation of PTT Pro for iOS. PTT Pro for iOS supports the following methods for installation:

- Email installation
- Manual installation
- Mobile Device Management (MDM) installation

## PTT Pro for iOS System Requirements

- iOS version 14, 15, 16, or 17 and a compatible iPhone, iPad, and iPod touch.
- To install by email notification, the system administrator must add a valid email address accessible from the target device.
- To activate the client on the target device, the system administrator must add a corresponding user to the Workcloud Communication PTT Pro Management Portal.

When the system administrator adds the user for the device, the PTT Pro Server generates an activation code. This activation code is used to activate the device.

## Apple App Store Availability

PTT Pro for iOS is not available in the following countries from the Apple App Store:

- China
- Egypt
- Georgia
- Jordan
- Qatar
- Pakistan

## Installing PTT Pro for iOS By Email

Use email installation if the device has a phone number and a cellular carrier or if the device has an email address. If the user account in the Workcloud Communication PTT Pro Management Portal includes this

information, the system administrator can send an activation message to the device with instructions to set up the account.

To use this method, the following requirements must be met:

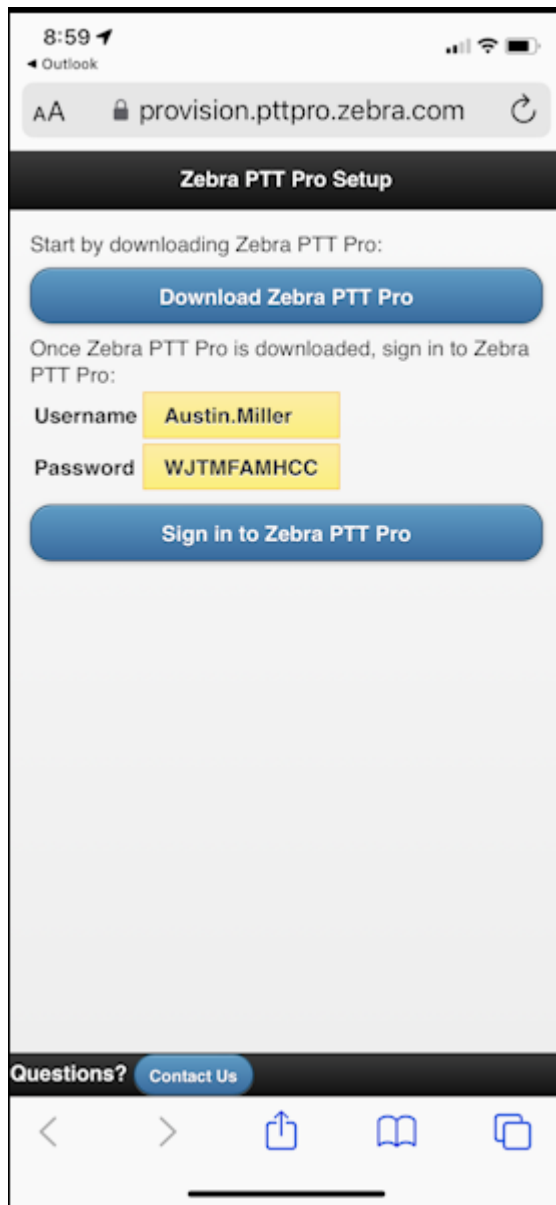
- An Apple ID to download the software from the Apple App Store.
- An email account is accessible from the device.

When the system administrator adds a user with a valid email address, PTT Pro Server sends an email notification.

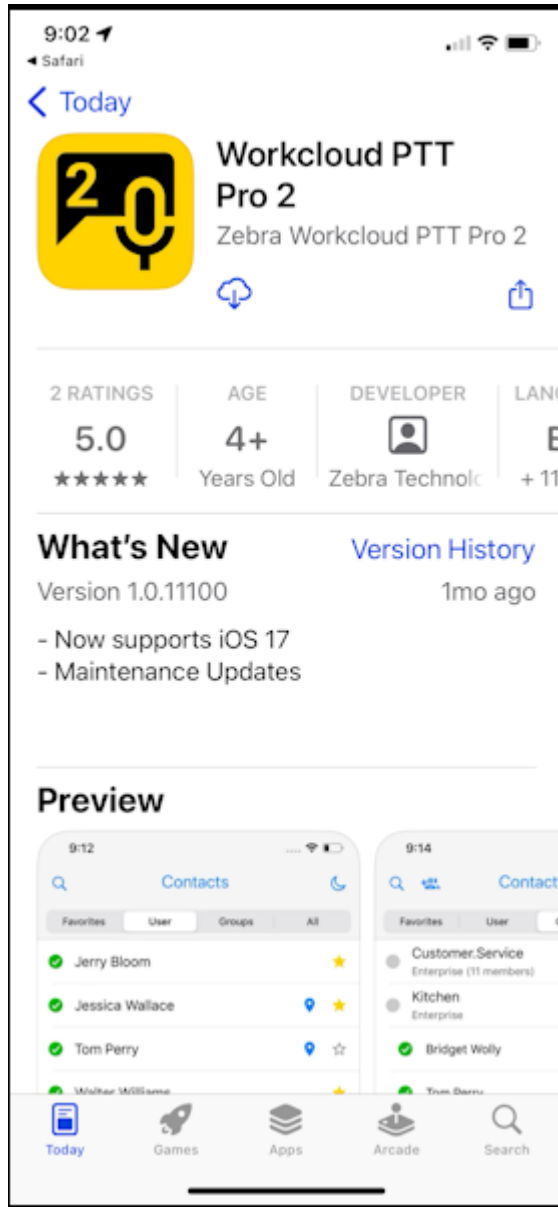
1. On the device, open the activation email and tap **Download Zebra PTT Pro** to download Zebra PTT Pro from the App Store.



**NOTE:** Do not close this screen because it contains the activation code.

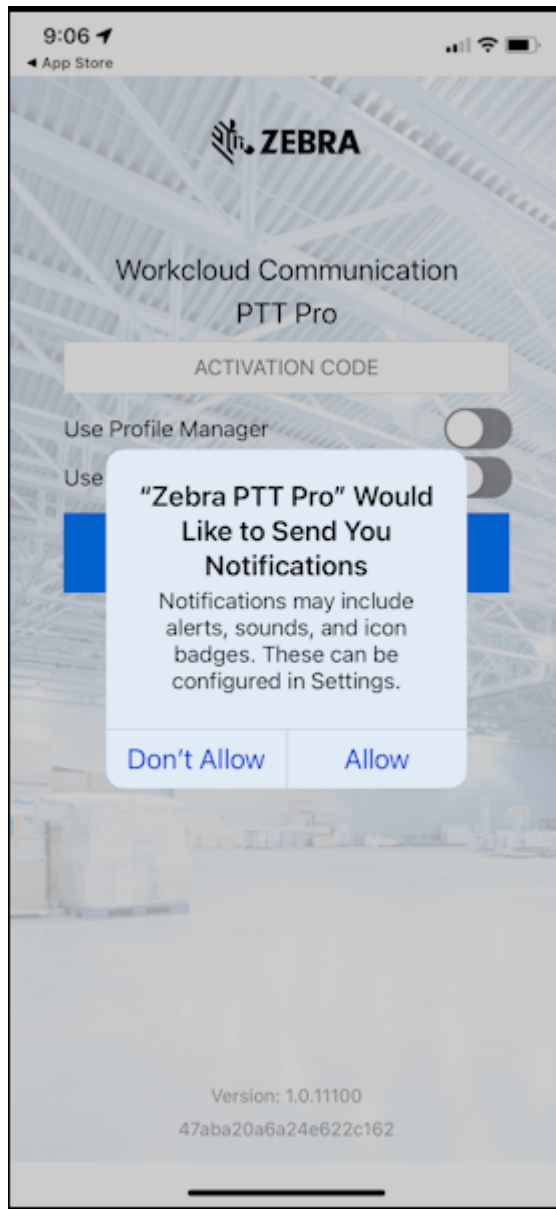


2. Tap download to install PTT Pro for iOS on the device.



After installation, the download icon changes to **Open**

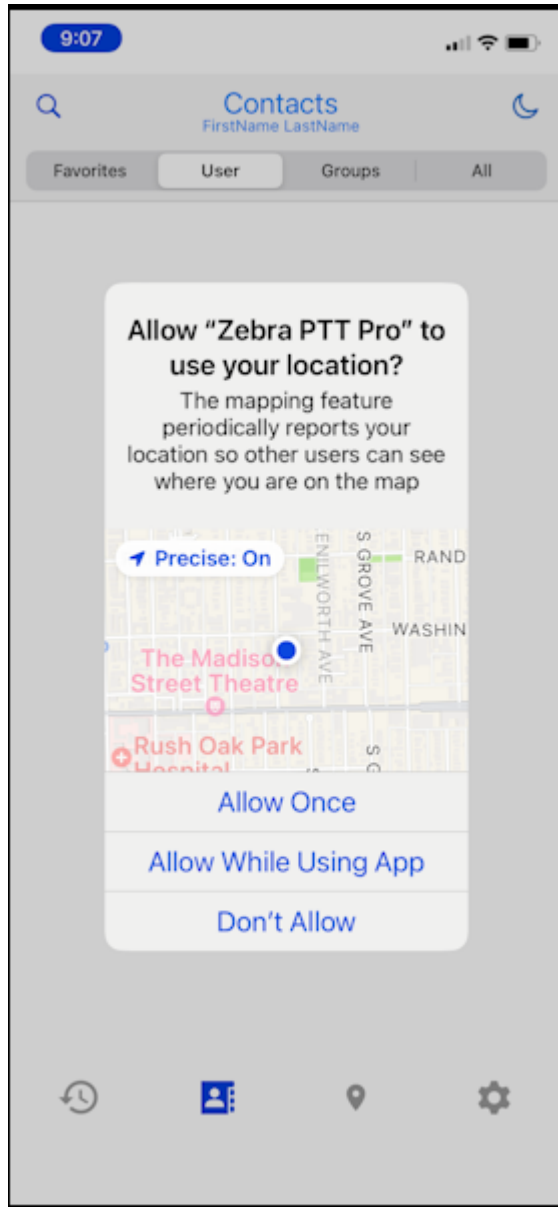
3. Tap **Open** to start PTT Pro for iOS. The notification permission dialog displays.



4. Tap **Allow**.
5. Enter the activation code in the **ACTIVATION CODE** field and tap **ACTIVATE**.

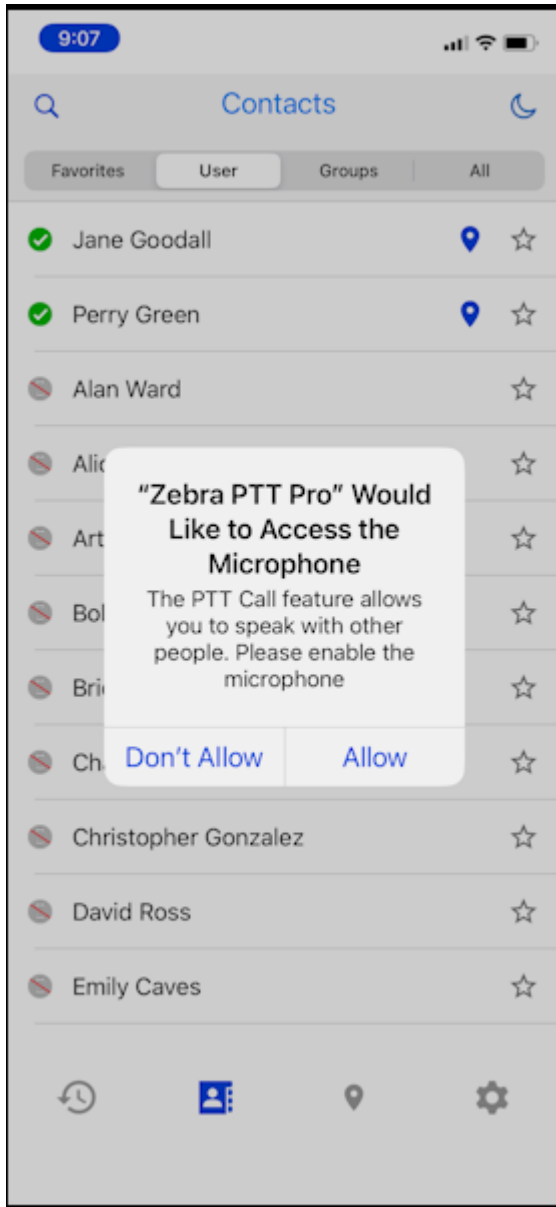


6. PTT Pro for iOS prompts for permission to use the device location. Select **Allow While Using App**.



7. Enter the activation code provided by your system administrator and select **ACTIVATE**.

8. PTT Pro for iOS prompts for permission to use the device microphone. Tap **Allow**.



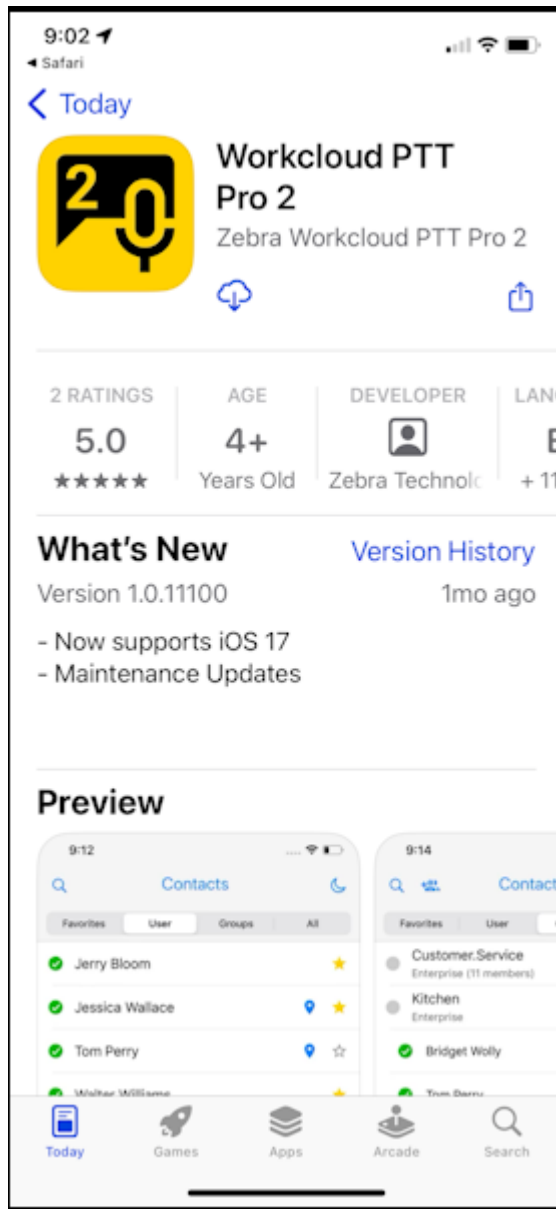
PTT Pro for iOS is activated and ready for use.

## Installing PTT Pro for iOS Manually

Manual installation requires an Apple ID and access to the Apple App Store.

1. Open the Apple App Store on the device.

## 2. Search for **Workcloud PTT Pro 2**.



3. Tap the download link to load the app on the device.
4. Tap **Open** to start the app.
5. Select **Allow** to enable the requested permissions and proceed to [Activating PTT Pro for iOS](#) to activate the app.

## Installing PTT Pro for iOS with an MDM

Enterprise administrators can install the PTT Pro for iOS to devices using MDM software. PTT Pro for iOS supports standard iOS device management features described at the following sites:

- [Managed App Configuration](#)
- [AppConfig](#)



**NOTE:** When an administrator pushes the PTT Pro for iOS client to a device, the user needs to manually activate the application. See [Activate PTT Pro for iOS With Profile Manager](#)

1. Open the Zebra PTT Pro app.

The app displays a message requesting permission to send notifications.

2. Select **Allow** and proceed to [Activating PTT Pro for iOS](#) to activate the app.

## Configuring the PTT Pro for iOS with Profile Manager

An administrator can push a Workcloud Communication Profile Manager configuration file to the PTT Pro for iOS client. The configuration file provides the connection details for Profile Manager. Refer to the Workcloud Communication Profile Manager Administrator Guide for information about using Profile Manager.

Two different files are available, depending on the MDM used.

- ios\_mdm\_specfile.plist
- ios\_mdm\_specfile.xml

Each file includes the same parameters for the Profile Manager connection.

**Table 2** MDM Parameters for iOS

Server	Parameter	Description
Profile Manager	pmCustomerID	ID for the customer or tenant.
	pmServerUri	URL to Profile Manager server.
	pmSiteID	ID for the site or department in Profile Manager.
Zebra Enterprise Messaging Service	zemsEnabled	Enables ZEMS.
	zemsServerURL	URL to ZEMS server.
	zemsServerApiKey	ZEMS authentication token.
Interworking Gateway (IWG)	iwgEnabled	Enables message of the day (MOTD).
	iwgServerURL	URL to the IWG server.
	iwgApiToken	IWG API authentication token

### Example iso\_mdm\_specfile.plist

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <key>Configuration</key>
  <dict>
    <key>pmEnabled</key>
    <true/>
    <key>pmCustomerId</key>
    <string>1</string>
    <key>pmServerUri</key>
```

```

<string>https://pfm_server_url</string>
<key>pmSiteId</key>
<string>10</string>
<key>iwgEnabled</key>
<true/>
<key>iwgServerURL</key>
<string>https://iwg_server_url/gw/upload/media</string>
<key>iwgApiToken</key>
<string>zebra</string>
<key>zemsEnabled</key>
<true/>
<key>zemsServerURL</key>
<string>https://zems_server_url</string>
<key>zemsServerApiKey</key>
<string>zebra</string>
</dict>
</plist>

```

## Example ios\_mdm\_specfile

```

<managedAppConfiguration>
  <version>1</version>
  <bundleId>com.zebra.wfc.pttpro</bundleId>
  <dict>
    <boolean keyName="pmEnabled">
      <defaultValue>
        <value>>false</value>
      </defaultValue>
    </boolean>
    <string keyName="pmCustomerId">
      <defaultValue>
        <value></value>
      </defaultValue>
    </string>
    <string keyName="pmServerUri">
      <defaultValue>
        <value></value>
      </defaultValue>
    </string>
    <string keyName="pmSiteId">
      <defaultValue>
        <value></value>
      </defaultValue>
    </string>
    <boolean keyName="iwgEnabled">
      <defaultValue>
        <value>>false</value>
      </defaultValue>
    </boolean>
    <string keyName="iwgServerURL">
      <defaultValue>
        <value></value>
      </defaultValue>
    </string>
  </dict>
</managedAppConfiguration>

```

```

        </defaultValue>
    </string>
    <string keyName="iwgApiToken">
        <defaultValue>
            <value></value>
        </defaultValue>
    </string>
    <boolean keyName="zemsEnabled">
    </boolean>
    <string keyName="zemsServerURL">
    </string>
    <string keyName="zemsServerApiKey">
    </string>
</dict>
<presentation defaultLocale="en-US">
<fieldGroup>
    <name>
        <language value="en-US">Profile Manager</language>
    </name>
    <field keyName="pmEnabled" type="checkbox">
        <label>
            <language value="en-US">Enabled</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="pmCustomerId" type="input">
        <label>
            <language value="en-US">Customer ID</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="pmServerUri" type="input">
        <label>
            <language value="en-US">Server URI</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="pmSiteId" type="input">
        <label>
            <language value="en-US">Site ID</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
</fieldGroup>
</fieldGroup>
<fieldGroup>
    <name>

```

```

        <language value="en-US">IWG</language>
    </name>
    <field keyName="iwgEnabled" type="checkbox">
        <label>
            <language value="en-US">Enabled</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="iwgServerURL" type="input">
        <label>
            <language value="en-US">Server URL</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="iwgApiToken" type="input">
        <label>
            <language value="en-US">API Token</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
</fieldGroup>
<fieldGroup>
    <name>
        <language value="en-US">ZEMS</language>
    </name>
    <field keyName="zemsEnabled" type="checkbox">
        <label>
            <language value="en-US">Enabled</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="zemsServerURL" type="input">
        <label>
            <language value="en-US">Server URL</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>
    <field keyName="zemsServerApiKey" type="input">
        <label>
            <language value="en-US">API Token</language>
        </label>
        <description>
            <language value="en-US"></language>
        </description>
    </field>

```

```
</field>  
</fieldGroup>  
</presentation>  
</managedAppConfiguration>
```

### Activating PTT Pro for iOS

Two methods are available to activate PTT Pro for iOS.

- Enter the activation code into the client.
- Use Workcloud Communication Profile Manager.

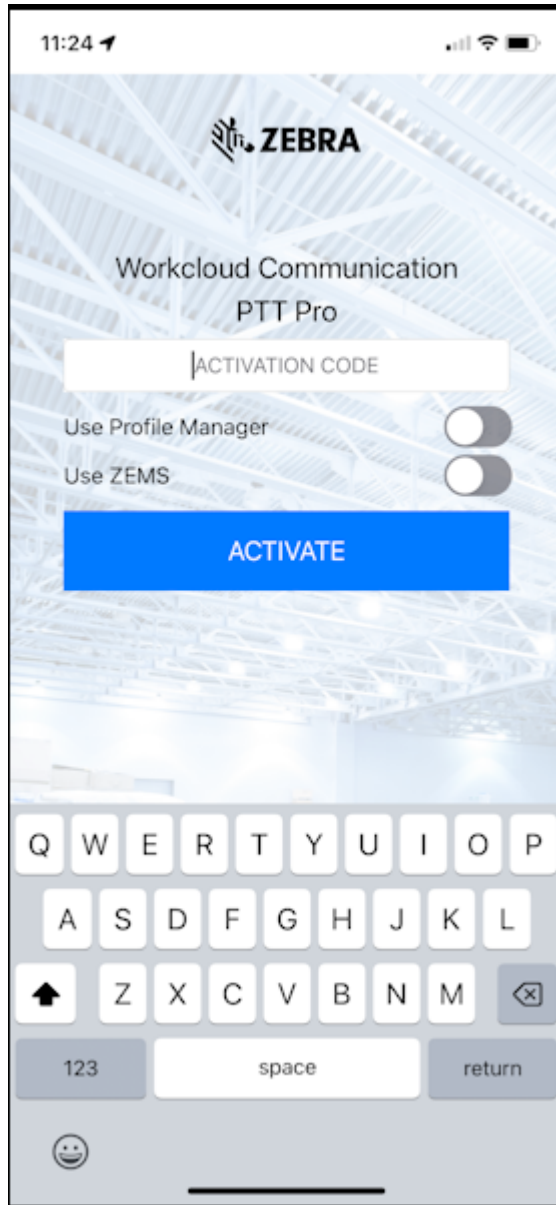
Both methods require an activation code for the user in the Workcloud Communication PTT Pro Management Portal.



## Entering an Activation Code for PTT Pro for iOS

When an administrator creates a user in the Workcloud Communication PTT Pro Management Portal, the user account includes an activation code. The activation code is used to activate Zebra PTT Pro for the user.

1. Open the PTT Pro for iOS app.



2. Enter the activation code in the **ACTIVATION CODE** field and tap **ACTIVATE**.

PTT Pro for iOS opens to the **Contacts** screen, synchronizes with the PTT Pro Server, and is ready to use.

## Activate PTT Pro for iOS With Profile Manager

Activating PTT Pro for iOS with Profile Manager requires a connection to the Profile Manager server. The connection information can be entered by the user, shown in the following figure, or it can be pushed to the device using an MDM.

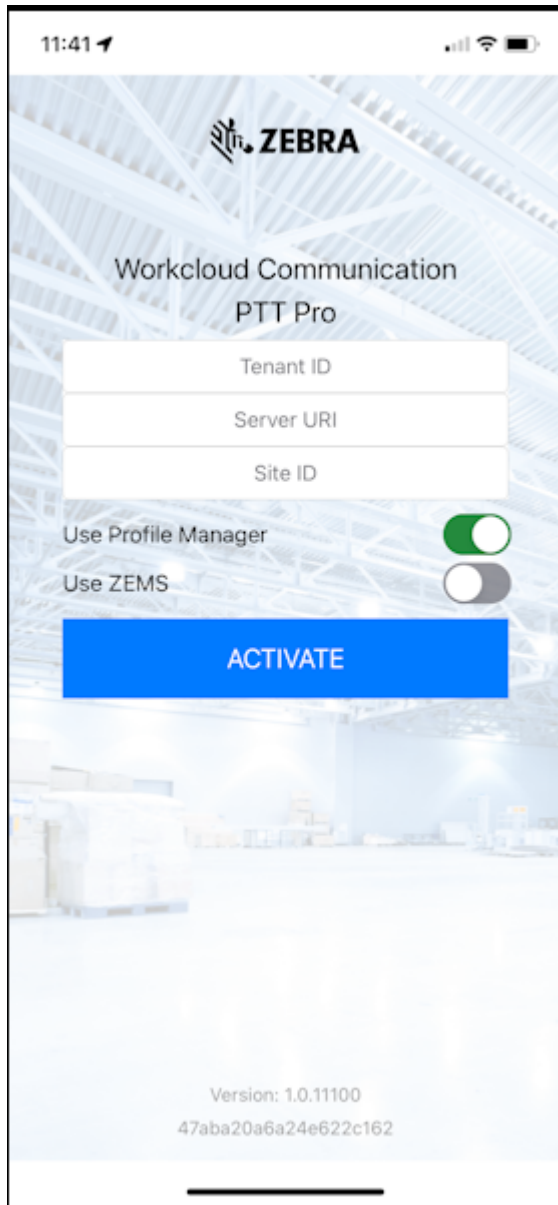


**NOTE:** You can also use Workcloud Communication Provisioning Manager to configure and activate PTT Pro for iOS. See the Workcloud Communication Provisioning Manager Customer Administrator Guide for more information.



**NOTE:**

- The device ID must be entered into the Profile Manager Devices table.
- The device ID must be entered into the Workcloud Communication PTT Pro Management Portal.
- The device ID for an iOS device changes when a factory reset is performed on the device.

**Figure 6** PTT Pro for iOS with Profile Manager Fields

### Entering Profile Manager Credentials

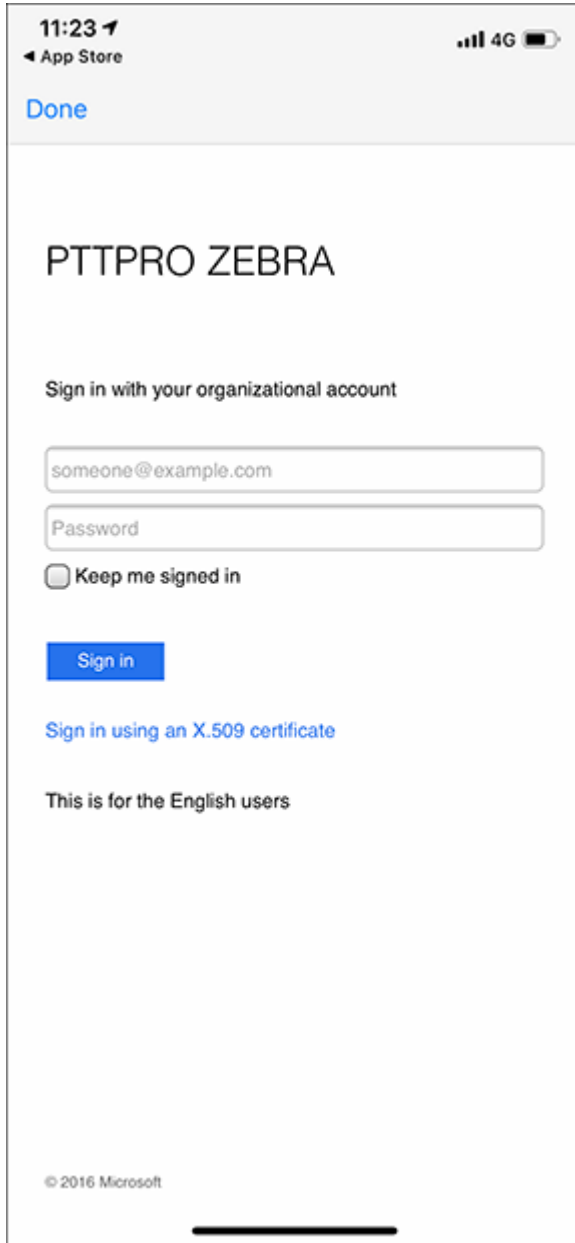
If the administrator requires the user to enter the Profile Manager connection parameters, complete the following steps. Otherwise, proceed to [Logging In and Selecting a Role](#).

1. Select **Use Profile Manager**.
2. Enter the Tenant ID, Profile Manager URL, and Site ID provided by the system administrator into the matching fields.
3. Click **Activate**.

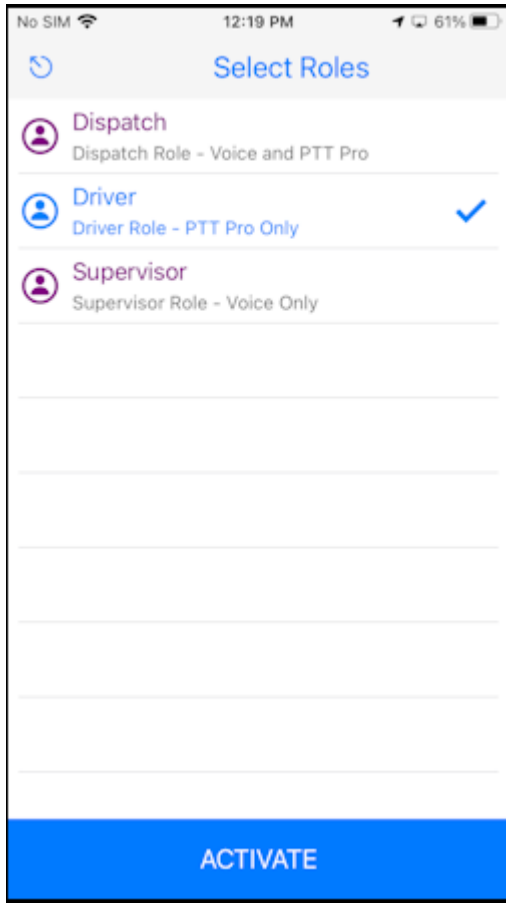
## Logging In and Selecting a Role

When Profile Manager is configured, you will need to log in through the Identity Provider and select a role.

1. Open PTT Pro for iOS and enter your username and password and tap **Sign in**.



2. Select a role and click **ACTIVATE**.



PTT Pro for iOS opens to the **Contacts** screen.

# Troubleshoot Activation Issues

You can activate a device using a unique activation code or by adding the device serial number to the Workcloud Communication PTT Pro Management Portal. For more information see the Workcloud Communication PTT Pro Management Portal Customer Administrator Guide.

- The Workcloud Communication PTT Pro Management Portal is not aware of the client type before the device has been activated. When using the email method to download software and activate the client, the user must select the download and activation links on the device being activated. Selecting the link on another device may cause incorrect information to be recorded in the server regarding the type of device being activated and interfere with activation on the correct device.
- An activation code may only be used once. Attempting to activate another device with the same activation code will fail. If the application software is deleted and reinstalled on the same device, a new activation code must be generated in the Workcloud Communication PTT Pro Management Portal (**Resend Activation**).
- If the user has previously activated a device and then switched to a new device, the system admin must clear the public key in the Workcloud Communication PTT Pro Management Portal; otherwise, the user will experience an Authentication error.
- The device installing the app must have the correct date/time; this is sometimes an issue with Android AOSP devices. An incorrect date/time on the device may cause problems with activation (typically failed activation with error code 54 is seen).
- Activation via ESN (Electronic Serial Number) on the device must be preceded by adding the ESN in the Workcloud Communication PTT Pro Management Portal.

# Firewall Configuration and Troubleshooting

The Zebra PTT Pro client requires specific network routes to communicate between the host device running the client and the PTT Pro Server. If the client device has a firewall enabled or is on a network that operates behind a firewall, such as many corporate wired and Wi-Fi networks, then the required communication routes may need to be configured in the firewall. Many issues with the client are caused by missing or incorrect configuration in the firewall.

## Configure the Firewall

The table below lists the required routes and the consequences if they are not properly configured in the firewall. [PORT], [PORT-RANGE] and [SERVER] represent enterprise-specific configuration information. Contact your IT department to determine the proper values for [PORT], [PORT-RANGE] and [SERVER].



**NOTE:** The use of IP addresses is acceptable when necessary, it is recommended to define firewall rules using DNS server names whenever possible for future compatibility.

**Table 3** Firewall Routes Required by Zebra PTT Pro

Description	Server	Type	Port	Potential Client Firewall Issue
PTT Pro Provisioning server	provision.pttpro.zebra.com	TCP	443	The client displays a failure message after attempting to activate using its Activation Code.
PTT Pro Management Server	[SERVER]	TCP	443	The client displays a failure message during registration.
PTT Pro Enterprise Server, PTT Pro Signaling Port	[SERVER]	TCP	[PORT] 443	The client displays a failure message during provisioning, registration, or other operation.
PTT Pro Enterprise Server, PTT Pro Data Port Range	[SERVER]	UDP	[PORT-RANGE]	The client unsuccessfully sends or receives audio during a call.
PTT Pro Download Server	download.pttpro.zebra.com	TCP	443	User unable to download client.
Google, PTT Pro Client Mapping Tiles	APNS *.push.apple.com	TCP	80, 443, 5223, 2195, 2196, 2197	The client displays a failure message during provisioning, registration, or other operation.

**Table 3** Firewall Routes Required by Zebra PTT Pro (Continued)

Description	Server	Type	Port	Potential Client Firewall Issue
	Certificate Enrollment	TCP	1640	The client displays a failure message during provisioning, registration, or other operation.

## Troubleshoot Firewall Issues

This section describes troubleshooting procedures if the client cannot connect to a server. When this occurs, the client might display a red **Disconnected from server** notification at the top of its main screen. Some procedures may be specific to a Windows computer hosting the PTT Pro PC Client, while some procedures may also be useful on a device operating with Wi-Fi service.

Before proceeding, contact your IT department to obtain the correct [PORT], [PORT-RANGE], and [SERVER] values.

1. Verify that the firewall is configured correctly. Firewall settings should be checked at multiple levels:
  - a) Contact IT to confirm that the enterprise firewall is configured correctly based on the routing information described [Configure the Firewall](#).
  - b) Check the device's local Windows firewall if applicable. If the firewall is enabled, try the following options:
    - Turn the Firewall off.
    - Follow the instructions for your Windows release to allow an application (For example, Zebra PTT Pro) through the firewall.
  - c) Check if the device is running an Anti-Virus/Firewall program, such as Bitdefender.
    - If such as program is running, then inspect if its configuration/rules are blocking the Zebra PTT Pro client network operation.
    - Consider adding an exception, such as adding the Zebra PTT Pro or its network routes to the white list of allowed operations. Otherwise, consider disabling the Anti-Virus/Firewall program temporarily to test the Zebra PTT Pro client program operation without it.
2. Verify that the device has internet connectivity.
  - Ping a well-known address (for example, ping `www.google.com`). If the ping command is successful, the device has internet connectivity. You may also ping the PTT servers, for example `ping provision.pttpro.zebra.com`.
3. Verify if the device's IP address is constant or changing over time.
  - Does the device's IP address change over time? Each time the device's IP address changes, the dispatch client will re-register with the server.
  - Display the device's IP address at different times (for example, `ipconfig` command for Windows) such as each hour or day and note the IP Address value each time.



#### 4. Verify that the Zebra PTT Pro client can connect to the PTT Pro Server TCP port.

There are multiple methods for checking TCP/UDP connectivity between the Zebra PTT Pro client and server.

- a) The nmap command: Nmap is a useful port diagnosis tool that is available for Windows, although you may need to install it. The Windows procedure is below.
  1. Start a Windows Command Shell.
  2. Run nmap for each TCP port number described in [Configure the Firewall](#). Example: `nmap -sT -p 80 [SERVER]`. Examine the results for a successful response.
- b) Run nmap for each UDP port number in [Configure the Firewall](#). Example: `nmap -sU -p [PORT] [SERVER]`.
- c) The telnet command: Telnet establishes a TCP connection between the originating computer and the specified destination. The Windows procedure is below.
  1. Start a Windows Command Shell.
  2. Run telnet for each TCP port number in [Configure the Firewall](#). Example: `telnet [SERVER] 80`. Examine the results for a successful response (the Command Shell clears to all black).



**NOTE:** Telnet cannot be used for UDP.

- d) Commercial and free software is available, as well as free online services, to check TCP and UDP port connectivity. Consult your IT department for more information.
- #### 5. For a Windows client, check if the Windows User account has the correct privileges for installing and running the client.
- On a Windows single or multi-user workstation: Verify that the PTT Pro PC Client is installed from and run by a Windows User account with appropriate network and other privileges, such as the Windows Administrator account or an account with Administrator privileges.
- #### 6. For a Windows client, verify the PTT Pro PC Client version number and ensure the most recent version is installed.
- a) Start PTT Pro PC Client, if possible.
  - b) Click the **About** button.



**NOTE:** The PTT Pro PC Client value is displayed in the **About** screen.

- c) Click **Cancel** to close the **About** screen.
  - d) Contact IT to confirm the PTT Pro PC Client version number.
- #### 7. Check if more than one PC client is simultaneously running on the computer.
- If more than one PC Client is running on the computer, then one of the clients usually stays connected to the server, while each other client(s) displays a red Disconnected from server notification at the top of its main screen.
  - Right-click the Windows taskbar and select the Task Manager menu item. Then, view the Processes tab, where a single PTT Pro PC Client should be displayed under the OpenJDK Platform binary process.
  - The Windows taskbar should contain a single PTT Pro PC Client icon.

**8.** Verify that access to the Google DNS server names for Mapping Tiles is properly configured.

- maps.googleapis.com
- maps.gstatic.com
- khmdb0.googleapis.com
- khmdb1.googleapis.com
- khm.googleapis.com
- khm0.googleapis.com
- khm1.googleapis.com
- khms0.googleapis.com
- khms1.googleapis.com
- khms2.googleapis.com
- khms3.googleapis.com
- <https://maps.googleapis.com/>

# Open Source Software Disclosure

Workcloud Communication PTT Pro uses the following open-source software.

## OpenSSL

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
- The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
- Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

## Opus CODEC

Copyright (c) 2011 Xiph.Org Foundation, Skype Limited Written by Jean-Marc Valin and Koen Vos

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

