

Zebra Services Agent for SOTI MobiControl



ZEBRA

Installation Guide

2025/06/13

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. ©2025 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/informationpolicy.

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.

Overview

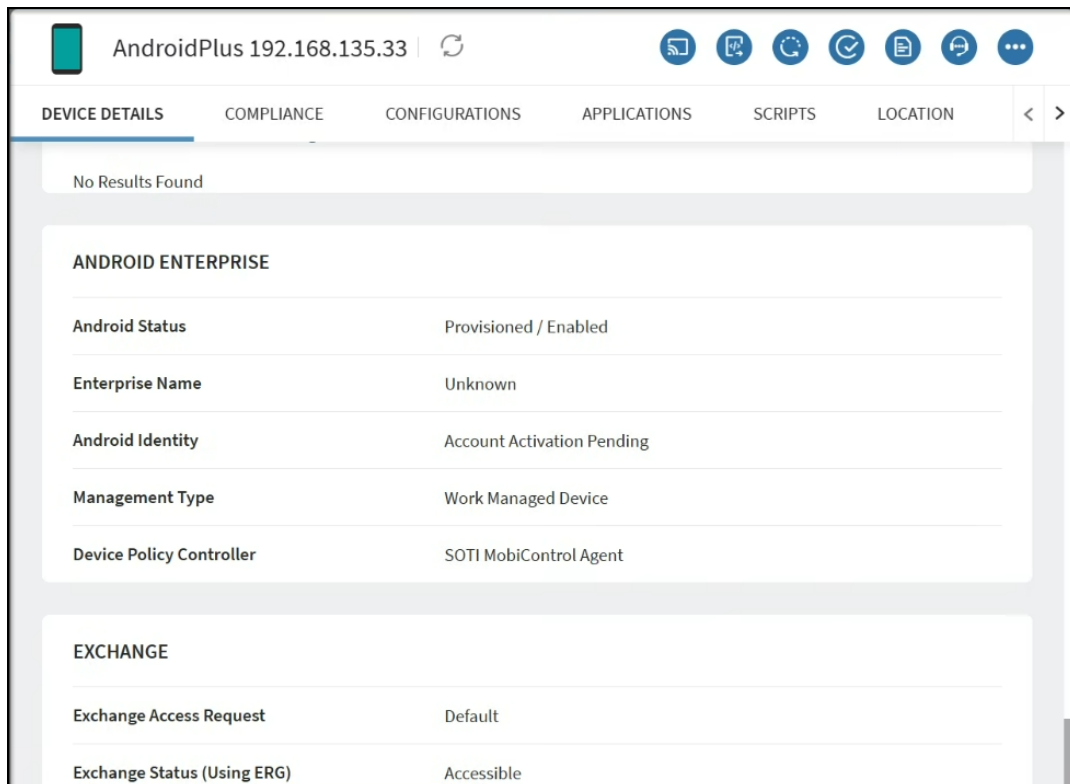
SOTI MobiControl is an Enterprise Mobility Management (EMM) solution that enables companies to securely manage devices and endpoints with any form factor and operating system throughout their lifecycle, from deployment to retirement.

The **Zebra Services Agent (ZSA)** app is designed to be installed and configured through EMM tools.

Pre-requisites

All target devices for the app installation must be enrolled in Soti Mobicontrol under one or more Organization Groups. Devices must be enrolled as **Work Managed** with the SOTI MobiControl Android application.

To verify if devices are configured as **Work Managed**, select **Group** > **Device name** > **Device Details** > **Android Enterprise** > **Management Type**. **Work Managed Device** displays.

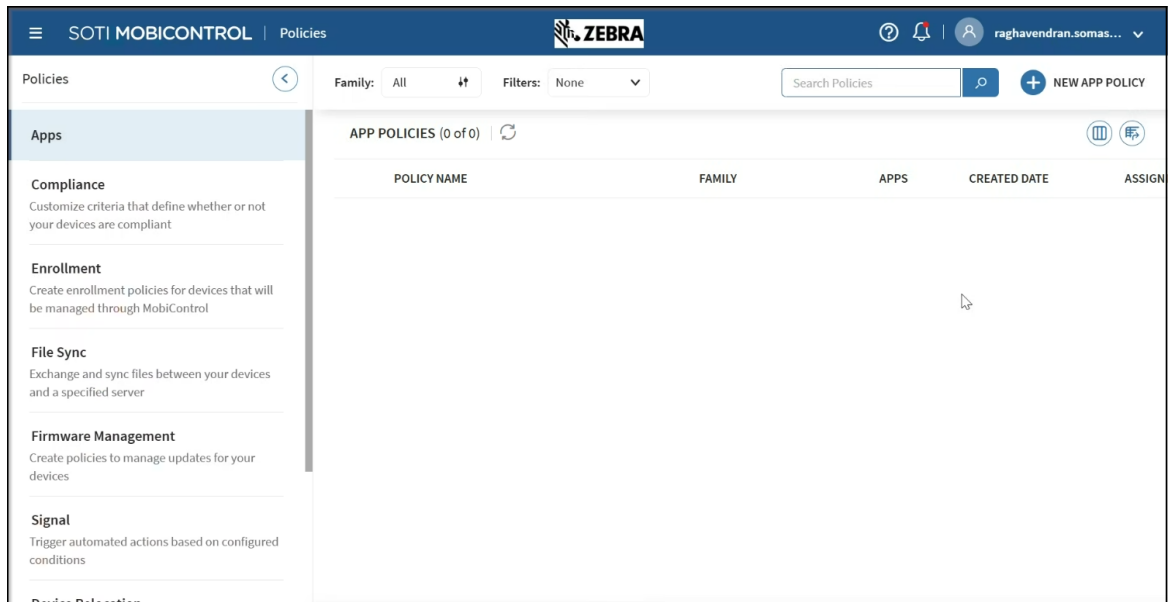


Deploying Zebra Services Agent

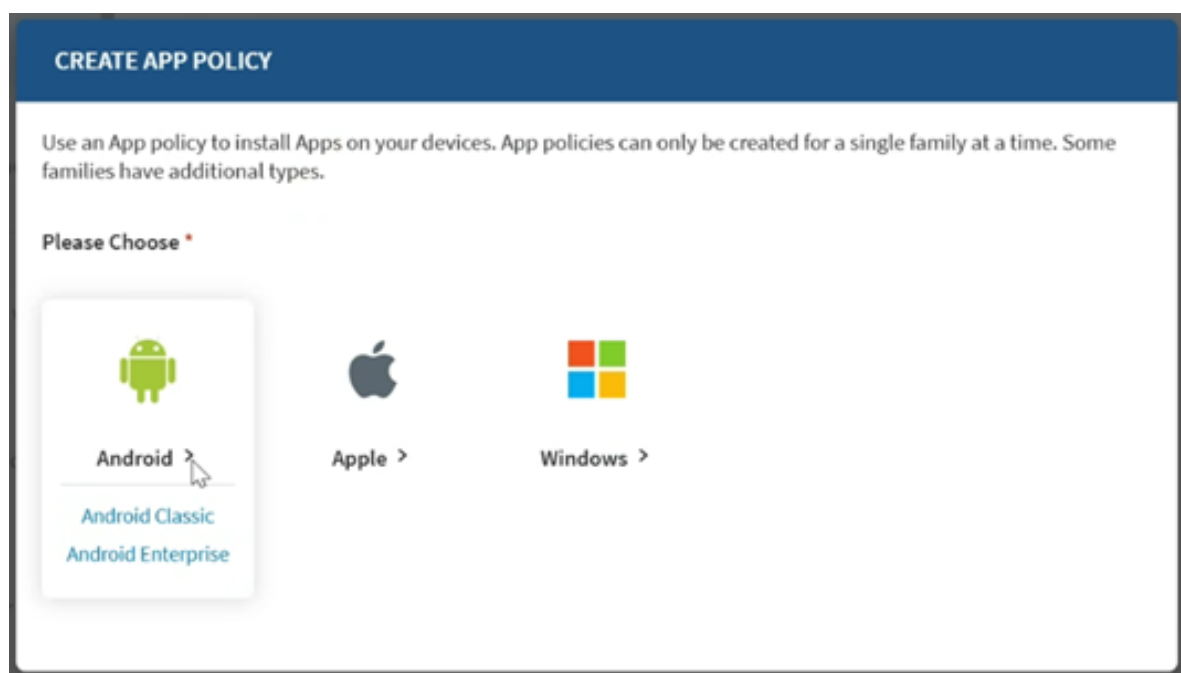
Install the ZSA app on the devices.

Download the Zebra_Services_Agent_V3.0.0.5.apk file from zebra.com/zebra-services-agent.

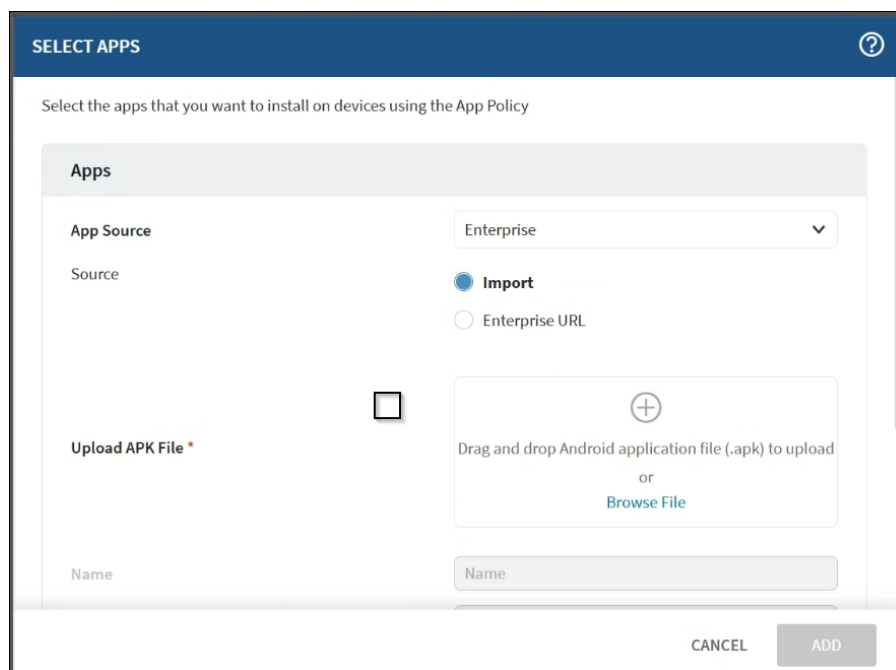
1. Log into **Soti Mobicontrol Web Console**.
2. Select **Menu** and scroll down to **Configuration** section.
3. In the **Configuration** section, navigate to **Policies** and then choose **Apps**.
4. Select **New App Policy** from the top-right corner. After you make the selection, a **Create App Policy** dialog box displays.



5. Go to **Android option** > **Android Enterprise**.



6. Select **Enterprise** as **App Source**.



7. Select **Import** under the **Source** field.
8. Click **Browse File** to upload the **APK** file.

9. Click **ADD**.

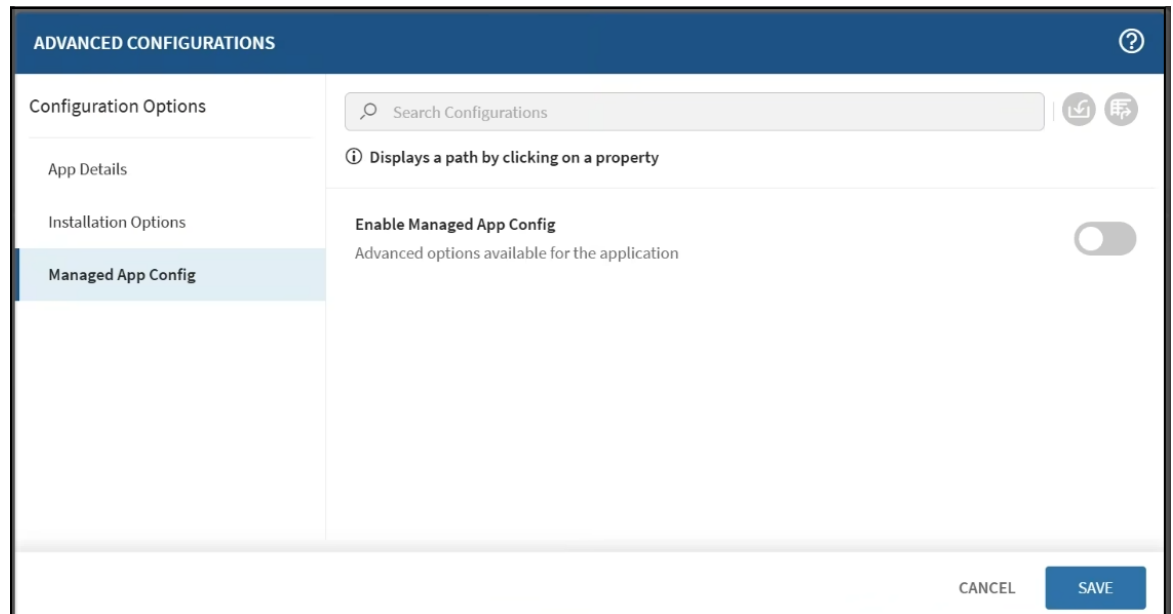
The Advanced Configurations page displays.

The screenshot shows a web interface titled "ADVANCED CONFIGURATIONS" with a help icon in the top right. On the left is a sidebar with "Configuration Options" containing three items: "App Details" (highlighted), "Installation Options", and "Managed App Config". The main area is titled "Details of the application you are adding or editing" and contains the following fields:

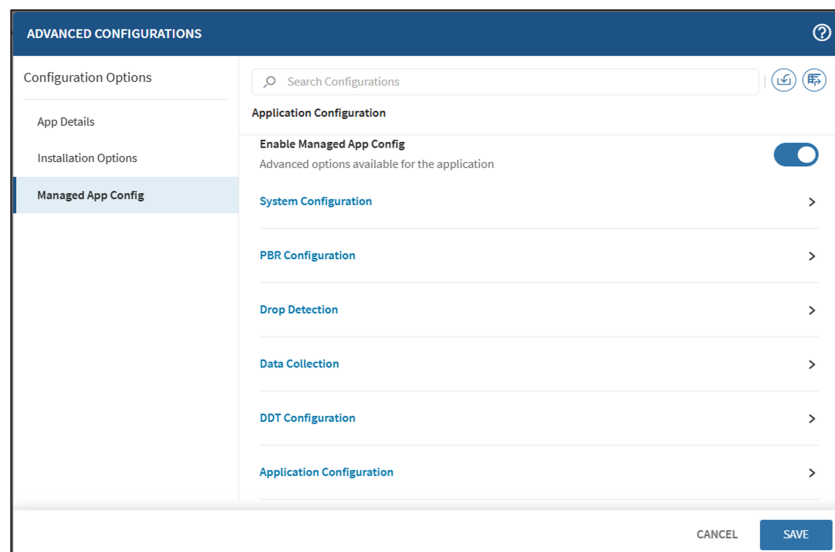
- Name:** Zebra Services Agent
- Package Name:** com.zebra.zsa (with a copy icon)
- Version:** 3.0.0.1
- Seller:** (empty text field)
- Description:** (empty text area)

At the bottom right of the form are two buttons: "CANCEL" and "SAVE".

10. After uploading the **APK** file, scroll down, and select **Configure**:
- Keep the **App Details** and **Installation Options** as they are, or modify them as required.
 - To configure **Zebra Service Agent**, enable the **Enable Managed App Config** option.



The configuration app lists display.



- Under the **System Configuration** section, enable the **Enable/Disable of ZSA** option and set the **Configuration of the log level for ZSA** with the following values:
 - 0: Info
 - 1: Debug
 - 2: Sensitive

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with the 'Managed App Config' tab selected. Under the 'System Configuration' section, the following settings are visible:

- Enable Managed App Config:** A toggle switch that is currently turned on (blue).
- System Configuration:** A dropdown menu showing a downward arrow.
- Enable/Disable of ZSA:** A toggle switch that is currently turned on (blue).
- Configuration of the log level for ZSA:** A dropdown menu set to '1'.
- File upload URL:** A text input field containing 'https://z4z.t.eu.fs.viq.zebra.com/system'.
- File upload retry count:** A text input field containing '3'.
- File upload retry interval in minutes:** A text input field containing '15'.

At the bottom right of the window are 'CANCEL' and 'SAVE' buttons.

- d) The system settings include three features for uploading log files:
- **File upload URL:** Specifies the server path for uploading log files.
 - **File upload retry count:** Defines the number of retry attempts if the upload fails.
 - **File upload retry interval in minutes:** Sets the duration (in minutes) between each retry attempt after a failed upload.
- e) Settings for managing data uploads on non-Zebra devices:
- **Data Upload URL:** Specifies the server path for uploading details of data collection. -
 - **Data Upload Interval in minutes:** Sets the frequency of uploads, defaulting to 24 hours (1440 minutes).

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with the 'Managed App Config' tab selected. Under the 'Data Upload' section, the following settings are visible:

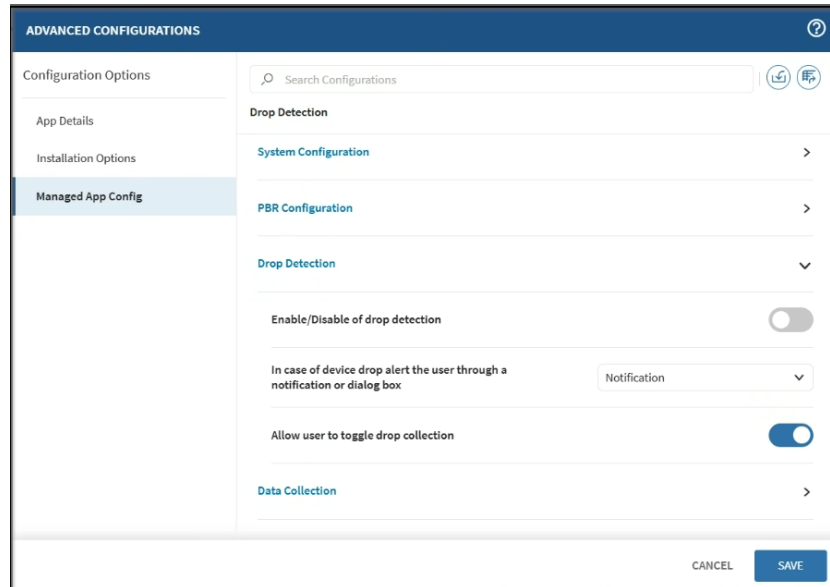
- File upload retry interval in minutes:** A text input field containing '15'.
- Data upload URL:** A text input field containing 'https://analytics.zebra.com/client2'.
- Data upload interval in minutes:** A text input field containing '1440'.
- Enable/Disable of data collection:** A toggle switch that is currently turned off (grey).
- Allow user to toggle data collection:** A toggle switch that is currently turned on (blue).
- Account No:** An empty text input field.

At the bottom right of the window are 'CANCEL' and 'SAVE' buttons. A 'PBR Configuration' link with a right arrow is also visible at the bottom of the configuration area.

- f) Data collection settings for non-Zebra devices:
- **Enable/Disable of data collection:** Data collection is turned off by default. When enabled, it gathers information such as battery status, device details, installed applications, and usage analytics, which can be uploaded to the server specified in the **Data upload URL**.
 - **Allow user to toggle data collection:** Enabled by default, allowing users to change the status of data collection via the app. Administrators can disable this option to restrict user access.
- g) For the **Account No**, users must enter their MDM account number for non-Zebra devices.
- h) Go to **PBR Configuration**, provide a **Custom Message** as required.

The screenshot shows the 'ADVANCED CONFIGURATIONS' interface. On the left, a sidebar lists 'Configuration Options', 'App Details', 'Installation Options', and 'Managed App Config' (which is highlighted). The main content area is titled 'PBR Configuration' and includes a search bar. Below this, there are expandable sections for 'System Configuration', 'PBR Configuration' (which is expanded), 'Drop Detection', and 'Data Collection'. The expanded 'PBR Configuration' section contains three settings: 'Custom message to show in the notification' with a text input field containing 'YOUR_CUSTOM_MESSAGE_HERE'; 'In case of bad battery alert the user through a notification or dialog box' with a dropdown menu currently set to 'Notification'; and 'Block device usage' with a toggle switch that is currently turned off. At the bottom right of the main area are 'CANCEL' and 'SAVE' buttons.

- i) Set the **In case of bad battery alert the user through a notification or dialog box** with the following values:
- Notification (default)
 - Dialog
 - Dialogue with Assist
- j) The **Block device usage** option is disabled by default. If enabled by the administrator, it prevents device access when a bad battery is detected.
- k) Go to **Drop Detection**, toggle the **Enable/Disable of drop detection** option as required.



- l) Set the **In case of device drop alert the user through a notification or dialog box** with the following values:
 - Notification (default)
 - Dialog
 - Dialogue with Assist
- m) The **Allow user to toggle drop collection** is enabled by default. Users can control this feature, and admins can disable it to restrict access for users.
- n) Navigate to the **Data Collection** section. The settings for data collection on non-Zebra devices are as follows:
 - The **Battery** is enabled by default and collects data every 15 minutes. Only the admin can enable or disable this option to restrict user access; however, the collection interval cannot be modified.
 - The **Device Info** is enabled by default and collects data every 6 hours (360 minutes). Only the admin can enable or disable this option to restrict user access; however, the collection interval cannot be modified.
 - The **Application List and Events** is enabled by default. It collects information on installed applications and tracks events such as installations, uninstallations, upgrades, and downgrades. Only the admin can enable or disable this option to restrict user access; however, the collection interval cannot be modified.

- The **Application Usage** option is enabled by default. It tracks the duration apps spend in the foreground. Only the admin can enable or disable this option to restrict user access; however, the collection interval cannot be modified..

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with a sidebar on the left containing 'Configuration Options', 'App Details', 'Installation Options', 'Managed App Config' (highlighted), and 'App Permissions'. The main area is titled 'Data Collection > Battery' and includes a search bar. It lists expandable sections: 'Data Collection', 'Battery', and 'Device Info'. Under 'Battery', the toggle for 'Enable/Disable of battery data collection' is turned on. Under 'Device Info', the toggle for 'Enable/Disable of device info data collection' is also turned on. At the bottom right are 'CANCEL' and 'SAVE' buttons.

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with the same sidebar. The main area is titled 'Data Collection > Application Usage'. It lists expandable sections: 'Device Info', 'Application List and Events', 'Application Usage', and 'DDT Configuration'. Under 'Application Usage', the toggle for 'Enable/Disable of device application usage data collection' is turned on. At the bottom right are 'CANCEL' and 'SAVE' buttons.



NOTE: Data is uploaded based on the configured **Data Upload URL** and interval settings in the **System Configuration**.

- o) Under the **DDT Configuration**, enable the **Enable/Disable DDT** option, keep the **Clear DDT configurations** disabled in primary setup and click **Add Test Plan**.

ADVANCED CONFIGURATIONS

Configuration Options

- App Details
- Installation Options
- Managed App Config**

Search Configurations

DDT Configuration

Data Collection

DDT Configuration

Enable/Disable DDT ☒

Clear DDT configurations ☐

Test Plan

Add Test Plan

NAME

CANCEL SAVE

p) Under the **Schedule** section, configure the test plan with the following values:

ADVANCED CONFIGURATIONS

Configuration Options

- App Details
- Installation Options
- Managed App Config**

← Add Test Plan > Delivery

Schedule

Test Day Monday

Test Time 12:20

Activity

System to Test Bluetooth

Delivery

Protocol FTP

IP Address 192.168.2.107

User Name User1

Password Soti@123

CANCEL SAVE

- **Test Day:** Day of the Week (For example, Monday)
- **Test Time:** Time of the day for the test (HH: MM format)

q) Select **Bluetooth** as the **System to Test** option.

r) Under the **Delivery** section, select the **Protocol** as **FTP**, enter a valid **IP Address**, **User Name**, and **Password**, then click **Save**.

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with the 'Managed App Config' tab selected. The 'Add Test Plan > Delivery' configuration is displayed, showing settings for Schedule, Activity, and Delivery. The 'Schedule' section includes 'Test Day' (Monday) and 'Test Time' (12:20). The 'Activity' section includes 'System to Test' (Bluetooth). The 'Delivery' section includes 'Protocol' (FTP), 'IP Address' (192.168.2.107), 'User Name' (User 1), and 'Password' (Soti@123). At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

The DDT Configuration page displays.

- s) Select the **Test-log Retention** as required.

The screenshot shows the 'ADVANCED CONFIGURATIONS' window with the 'Managed App Config' tab selected. The 'DDT Configuration' section is visible, showing 'Enable/Disable DDT' (checked) and 'Clear DDT configurations' (unchecked). Below this is the 'Test Plan' section with an 'Add Test Plan' button and a table with one entry: 'Test Plan 1'. The 'Test-log Retention' dropdown menu is open, showing options: 'No Selection', 'Keep after upload', and 'Delete after upload'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

- t) Select the **Upload Preference** as required.

- u) Under the **Application Configuration** section, there are two options, **Wireless Insight** and **ZDS**, which are designated for Zebra devices only. More applications will be supported in the future.

- **Wireless Insight:** Configured using Managed Configuration through MDM or VIQ.
- **Configuration ID:** Pre-defined ID specific to the Wireless Insight configuration that includes several options.

ADVANCED CONFIGURATIONS

Configuration Options

- App Details
- Installation Options
- Managed App Config**

Search Configurations

Application Configuration > Wireless Insight

Data Collection

DDT Configuration

Application Configuration

Wireless Insight

Configuration ID

Custom Configuration

No Selection

Start Wifi Analysis

Start Cellular Analysis

Start both (Wifi and Cellular) Analysis

Stop Wifi Analysis

Stop Cellular Analysis

Stop both (Wifi and Cellular) Analysis

No Selection

CANCEL SAVE

- **Custom Configuration:** Add the custom Wireless Insight configuration as a value.
- **ZDS:** Configured through VIQ with a custom ZDS configuration.

v) Select **Save > Add**.

11. The **Zebra Services Agent** app is added. Click **Save and Assign**.

EDIT APP POLICY | ZSA v3.0.0.1

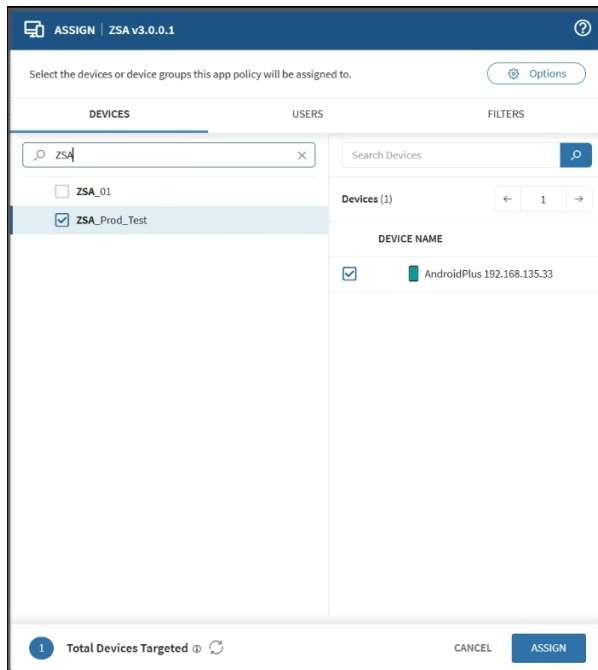
GENERAL APPS

APPS

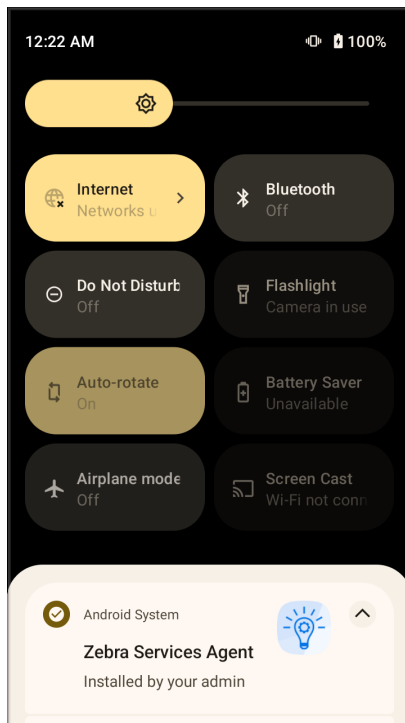
NAME	VERSION	MANAGED CONFIG	APP SOURCE	DEPLOYMENT TYPE
Zebra Services Agent	3.0.0.1	Configured	Enterprise	Mandatory

CANCEL SAVE AND ASSIGN SAVE

12. Assign to a group device or single device.



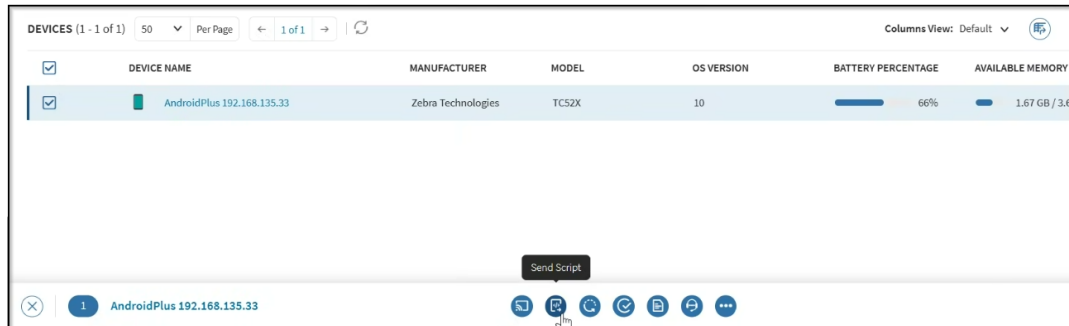
The application is now installed on the devices.



Auto-launching Zebra Services Agent

After deploying the apps, set the app to auto-launch:

1. Select **Devices** from the menu.
2. Select all devices and click **Send Script** from the available options below.



3. Select **Manage Scripts**.

SEND SCRIPT

Provide a script that will be executed by the MobiControl agent on the selected devices. Refer to the MobiControl help for supported script commands and syntax. ⓘ

⚠ Changing the values of this form will refresh the compatibility check.

⚠ When sending a script for resetting passcode or wiping device, utilize the 'Reset Passcode' or 'Wipe' device actions to utilize Direct Boot mode functionality.

Scripts MANAGE SCRIPTS

Script Type: JavaScript

Execute Saved Script: Please Select

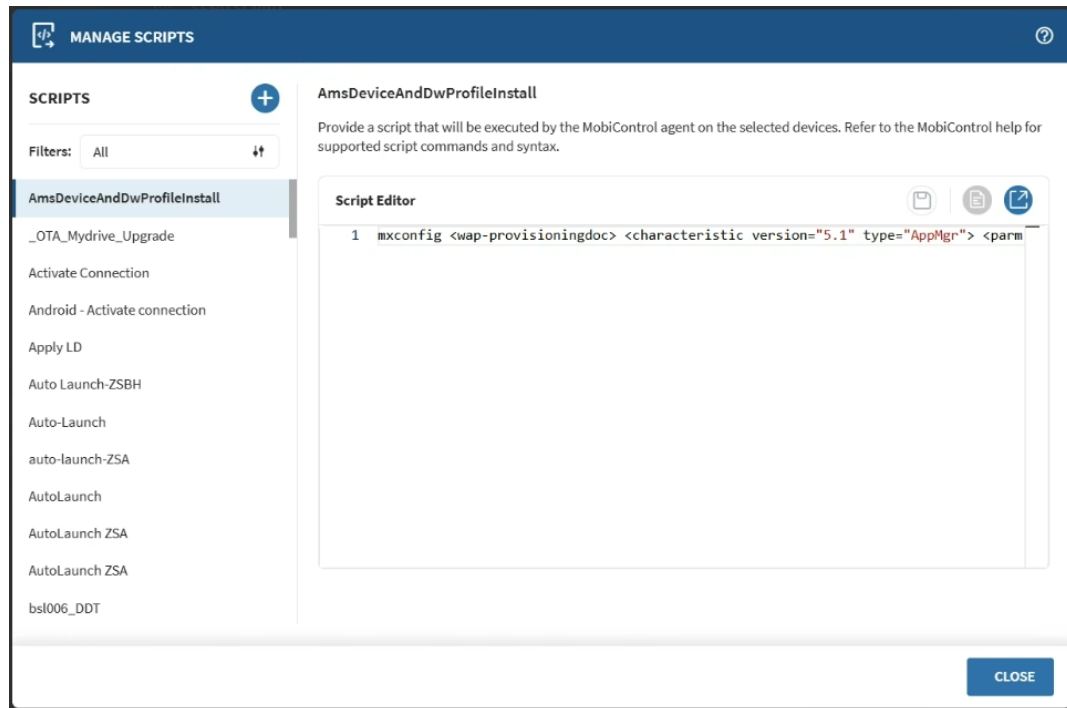
Script Editor

Delivery: Script will be sent directly to the MobiControl agent. MobiControl Agent

Queue messages for offline devices: ☒

✓ 1 of 1 device(s) will receive this action. CANCEL SEND SCRIPT

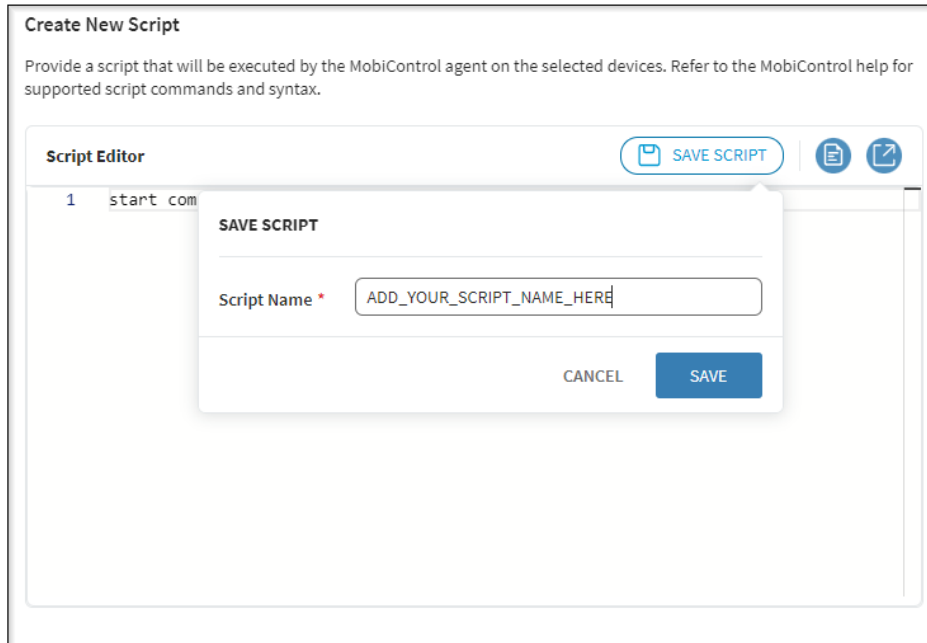
4. Select **Add New Script**.



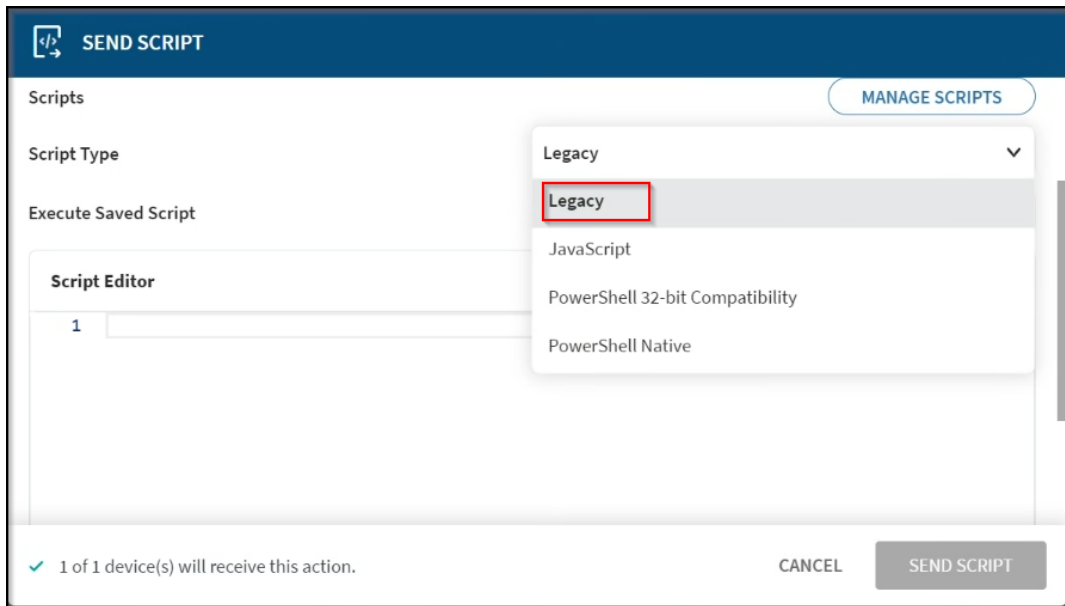
5. Add the command below to the script and then click **Save Script**.



6. Add a name for the script, and then click **Save**.



7. Save the script and close the portal.
8. Repeat step 2.
9. Select **Legacy** as the script type option.

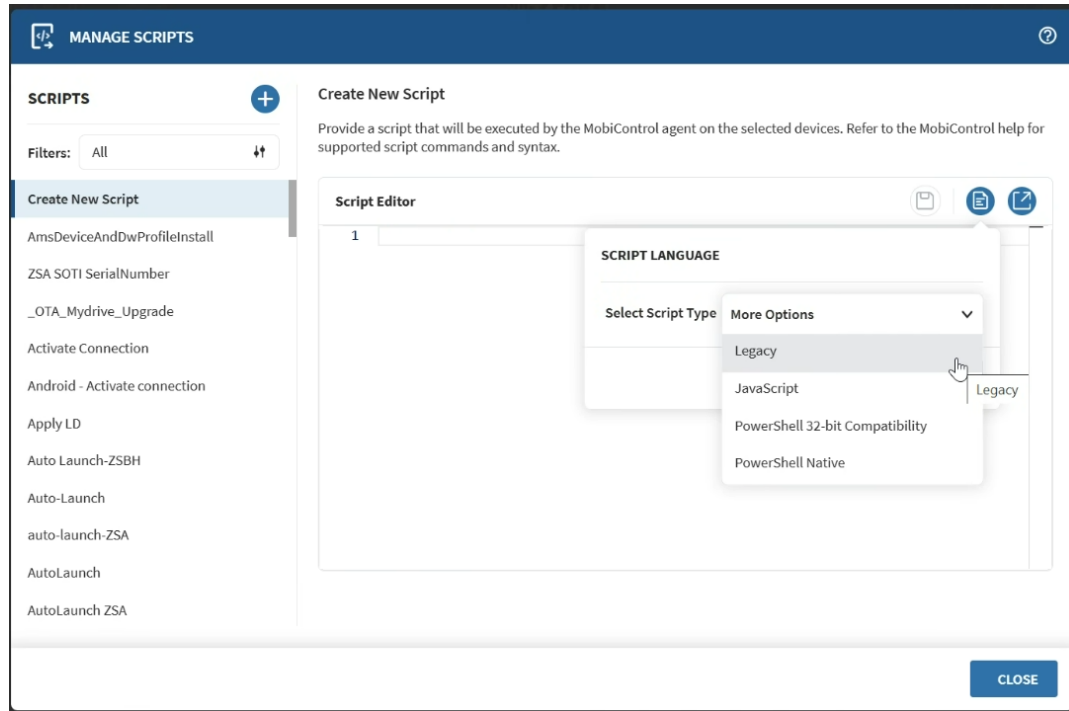


10. Select your saved script as **Execute Saved Script** from the drop-down menu.
11. Click **Send Script** to deploy the script to all selected devices. This action launches the Zebra Services Agent application on the targeted group of devices.

Allowing ZSA Application to Read Device Serial Numbers

To enable the ZSA application to obtain the serial number:

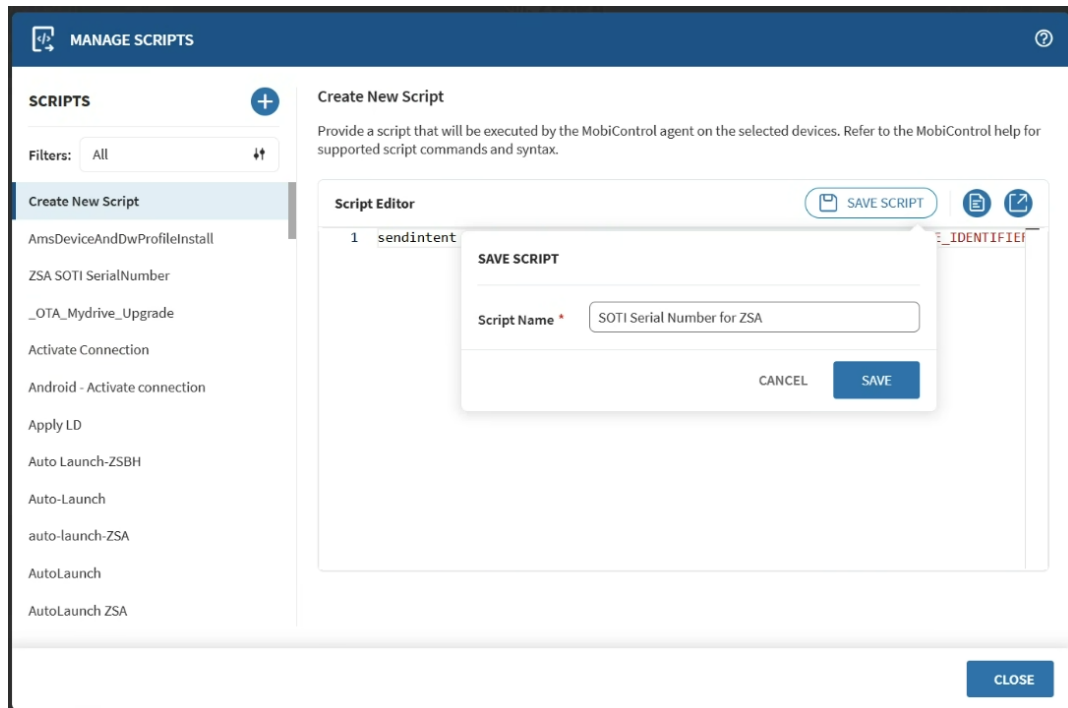
1. Go to **Devices > All devices > Send Script > Manage Scripts > Add New Script**.



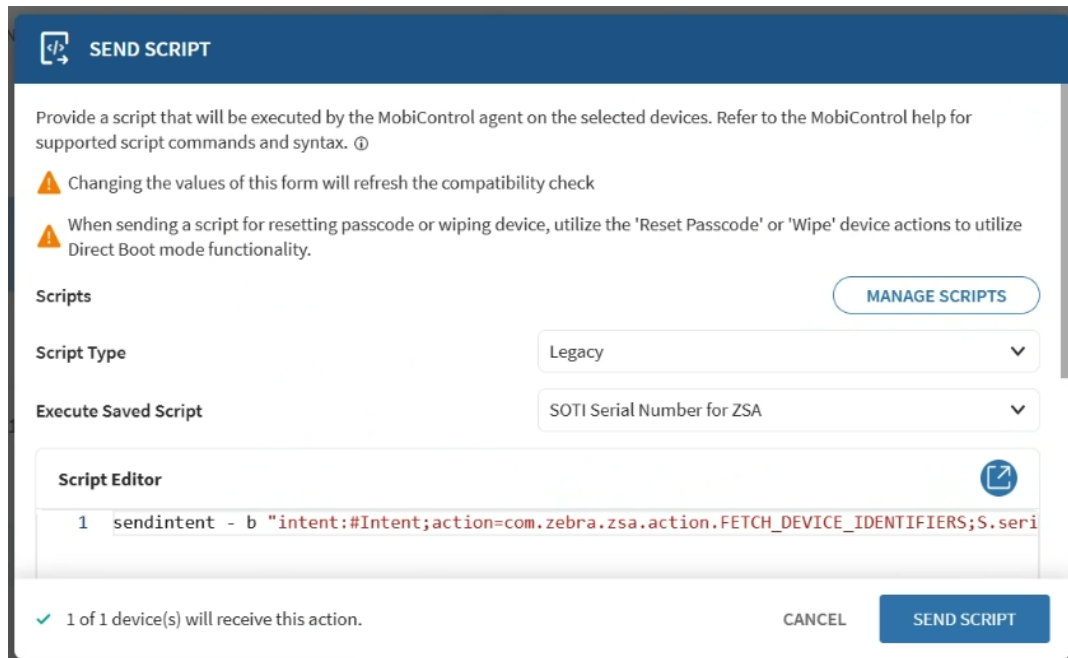
2. Select **Legacy** as the script type in the **Script Language** section, and add the command below in the editor section.

```
sendintent -b
"intent:#Intent;action=com.zebra.zsa.action.FETCH_DEVICE_IDENTIFIERS;
S.serialNumber=%SERIALNUM%;component=com.zebra.zsa/com.zebra.utility.
deviceIdentifier.SOTIReceiver;end;"
```

3. Save the script with an appropriate name.



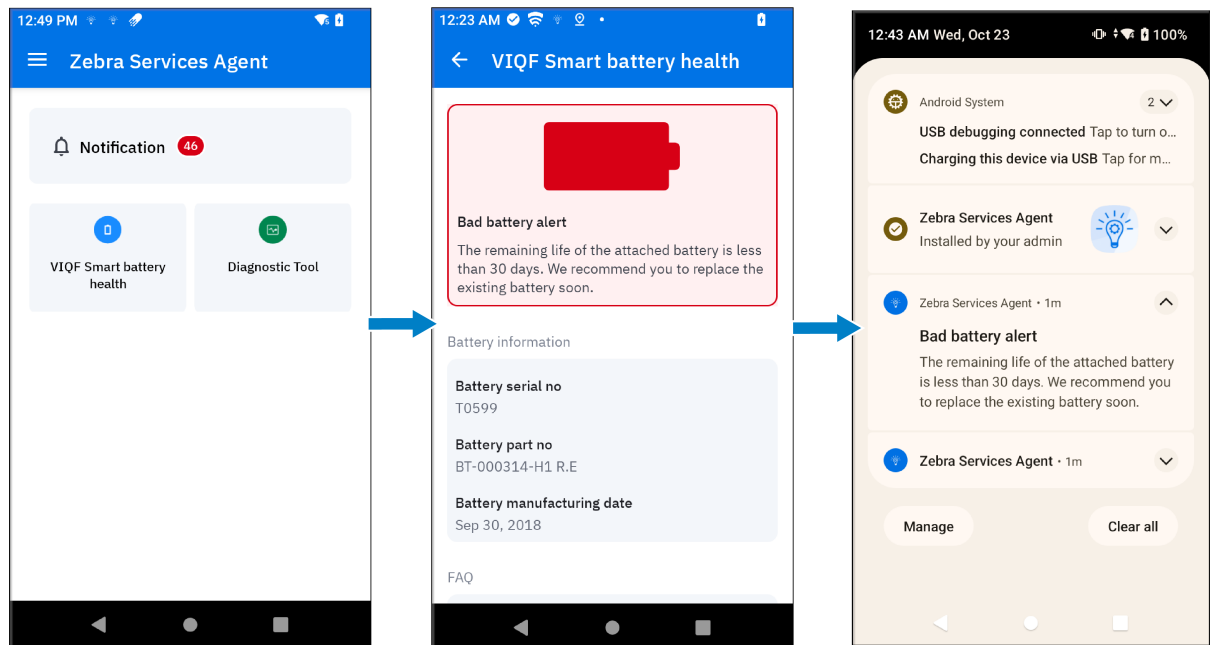
4. Navigate to **Devices > All devices > Send Script**. Choose **Legacy** as the script type and select created scripts from **Executed Saved Script**.



Expected Behaviour After Auto-launching Zebra Services Agent

This section explains the behavior of the ZSA app after the auto-launching.

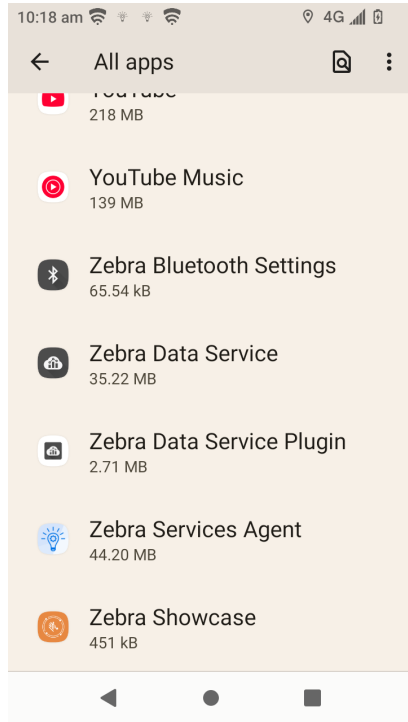
1. Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
2. If the Proactive Battery Health (PBR) module is entitled, the ZSA app automatically launches it after a few seconds.
3. The PBR screen displays both good and bad battery details, and if a **bad battery** condition is detected, a notification will display.
4. After a few seconds, the battery details screen and the ZSA app will close.



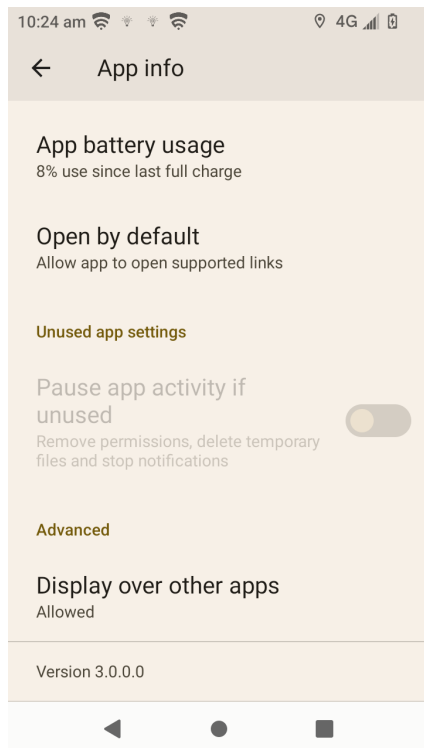
Verifying App Installation and Connection to Zebra Servers

To verify if the app is installed with the correct permissions and is able to connect to Zebra servers:

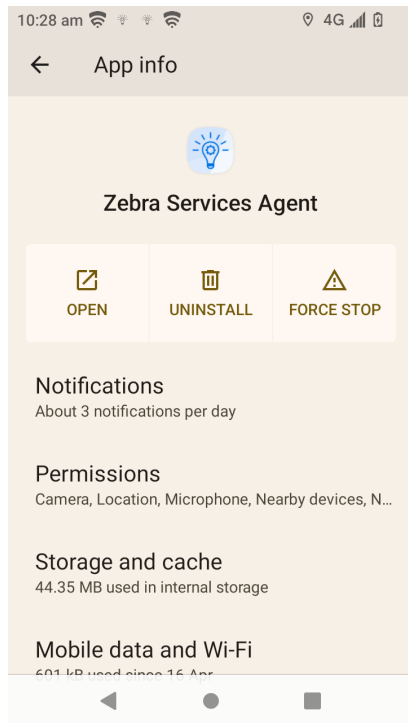
1. Go to **Settings > Apps > All apps** and select **Zebra Services Agent**.



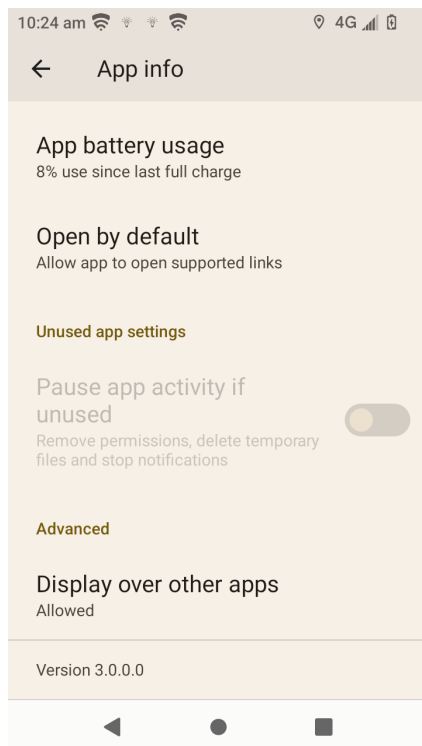
The **App Info** page displays the **Version**.



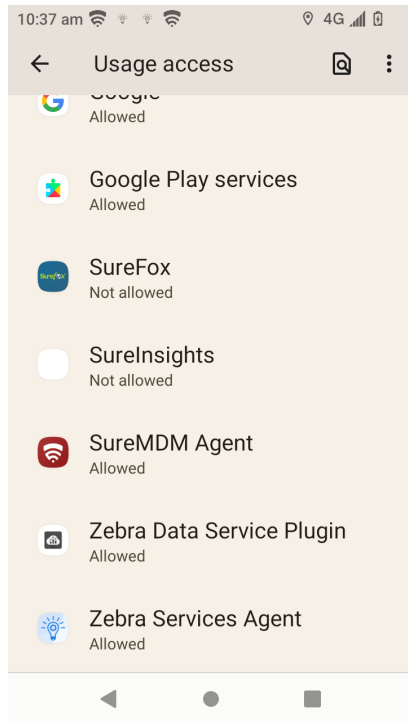
2. For the ZSA Permissions, go to **Settings > Apps > All apps > Zebra Services Agent > Permissions**.



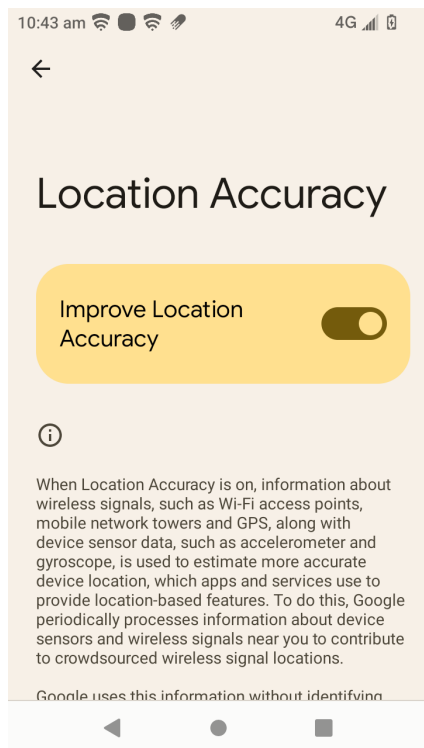
3. To verify the Display over other apps permission, go to **Settings > Apps > All apps > Zebra Services Agent > Advanced > Display over other apps**.



4. To verify Usage access permission, go to **Settings > Apps > Special app access > Usage Access > Zebra Service Agent**.

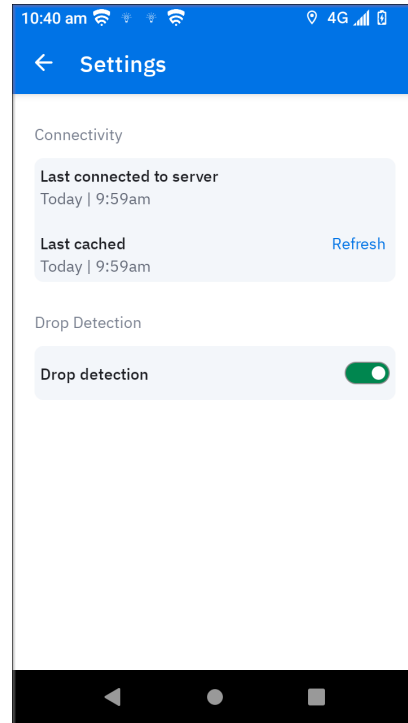
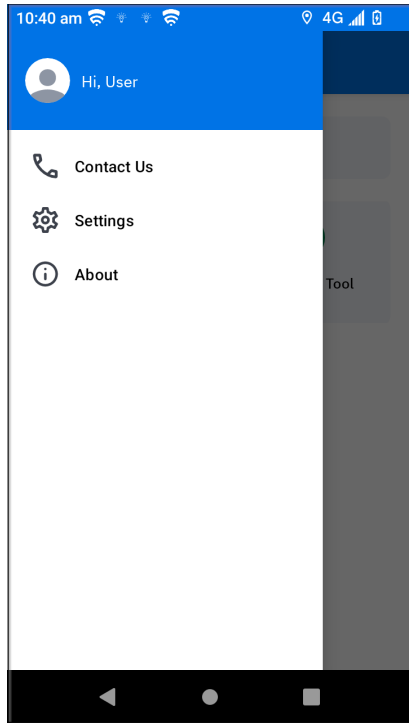


5. For the **Device action > Outdoor Location Tracking** feature, ensure that location accuracy is enabled on the device for precise location information. Navigate to **Settings > Location > Location Services > Location Accuracy**.



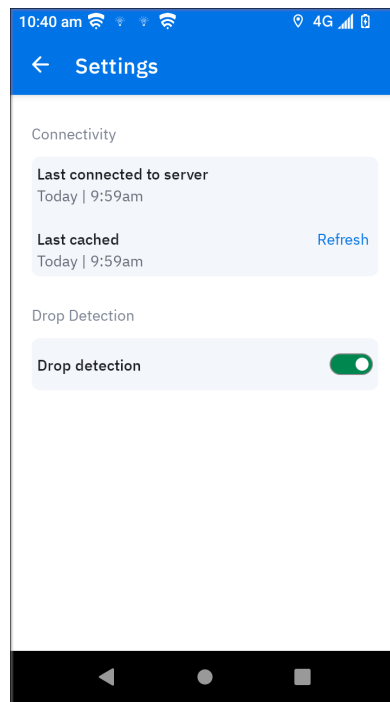
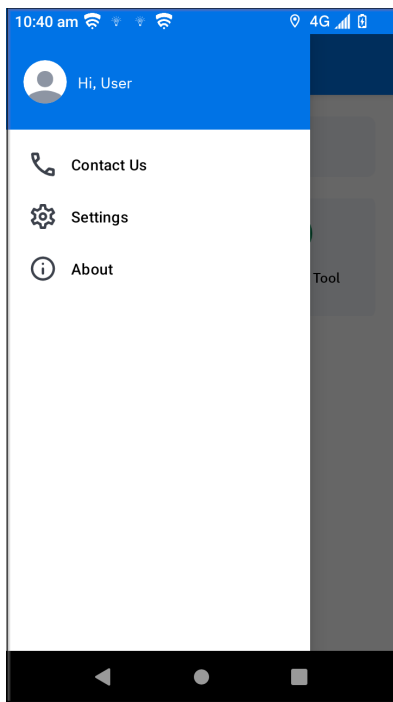
6. To verify ZSA Network connectivity to the Zebra URL:

- Launch ZSA and go to **Settings > Refresh**.



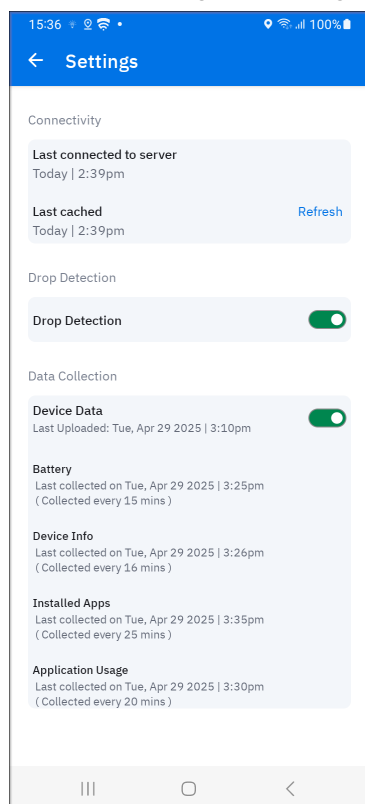
7. To verify the Drop Detection status:

Launch ZSA and go to **Settings**. Enable **Drop detection**. The user can enable or disable drop detection if the administrator provides toggle access.



8. To verify Data collection in a non-Zebra device:

Launch ZSA and go to **Settings > Data Collection**.



In data collection, the **last uploaded time** indicates when all data was successfully sent to the server. Each data type has its own **last collected time** and a specific collection interval.

