Zebra Services Agent for SOTI MobiControl

Installation Guide

MN-005037-05EN Rev. A

Zebra Technologies | 3 Overlook Point | Lincolnshire, IL 60069 USA
zebra.com

Copyright

2026/10/07

The Zebra wordmark and logo are trademarks of Zebra Technologies Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2026 Zebra Technologies Corp. and/or its affiliates.

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

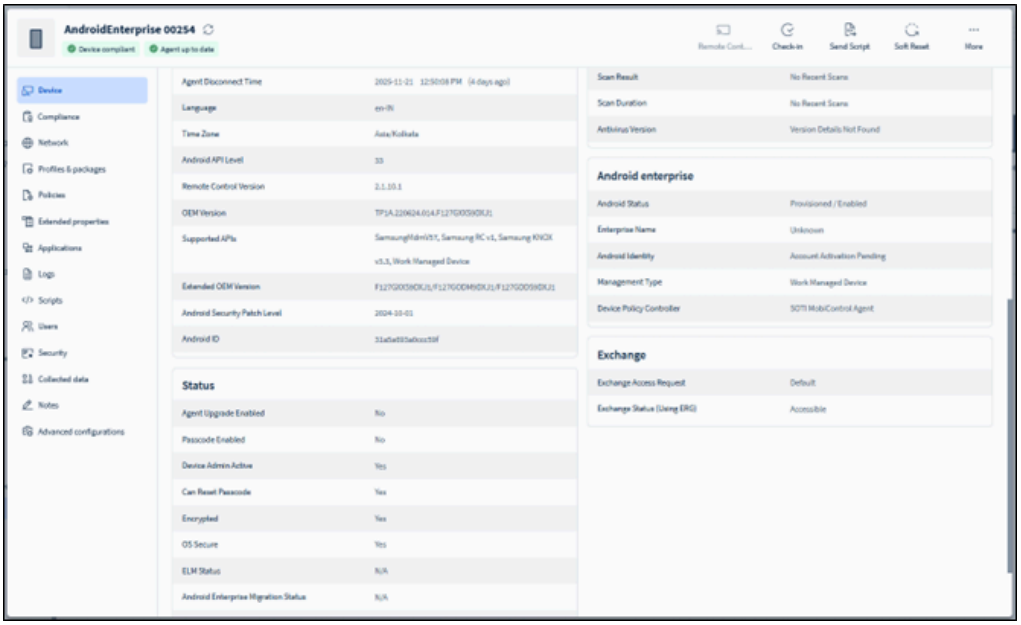
SOTI MobiControl is an Enterprise Mobility Management (EMM) solution that enables companies to securely manage devices and endpoints with any form factor and operating system throughout their lifecycle, from deployment to retirement.

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.

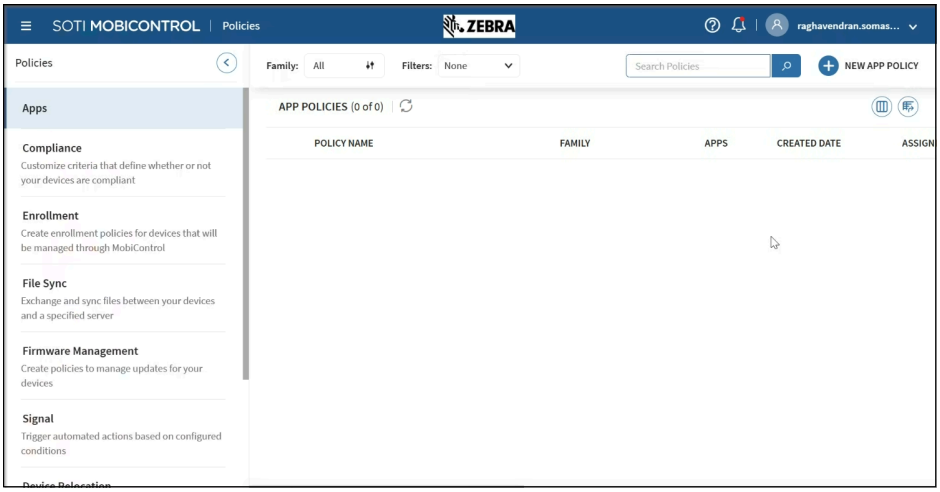


Deploying Zebra Services Agent

Install the ZSA app on the devices.

Download the `Zebra_Services_Agent_V5.0.0.x.apk` file from zebra.com/zebra-services-agent.

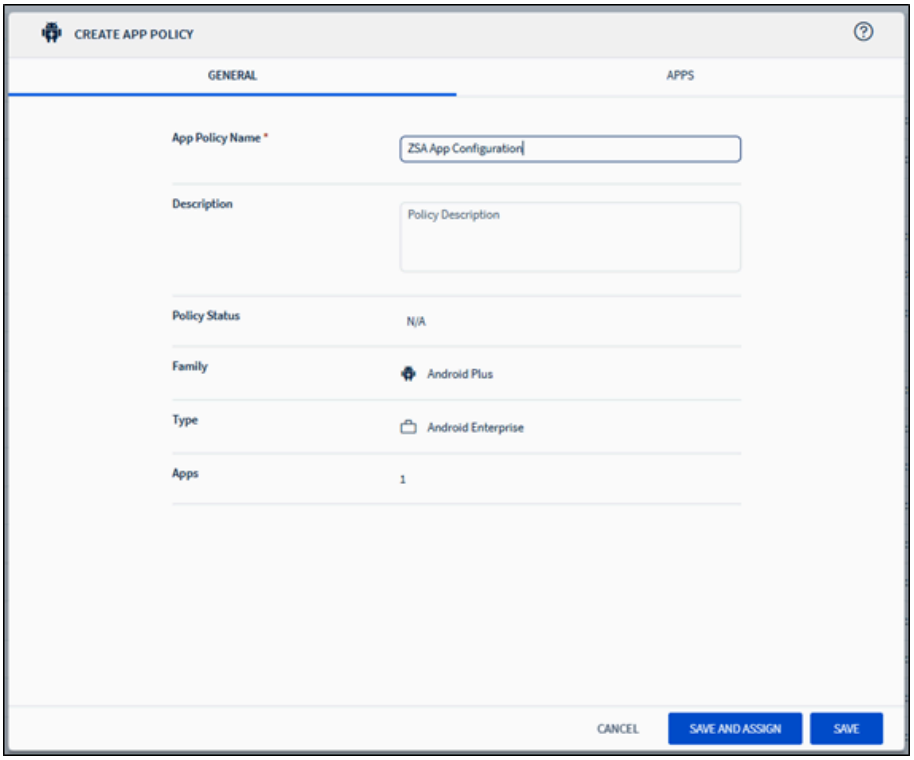
1. Log into **Soti Mobicontrol Web Console**.
2. Select **Menu** and scroll down to **Configuration** section.
3. In the **Configuration** section, navigate to **Policies** and then choose **Apps**.
4. Select **New App Policy** from the top-right corner. After you make the selection, a **Create App Policy**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



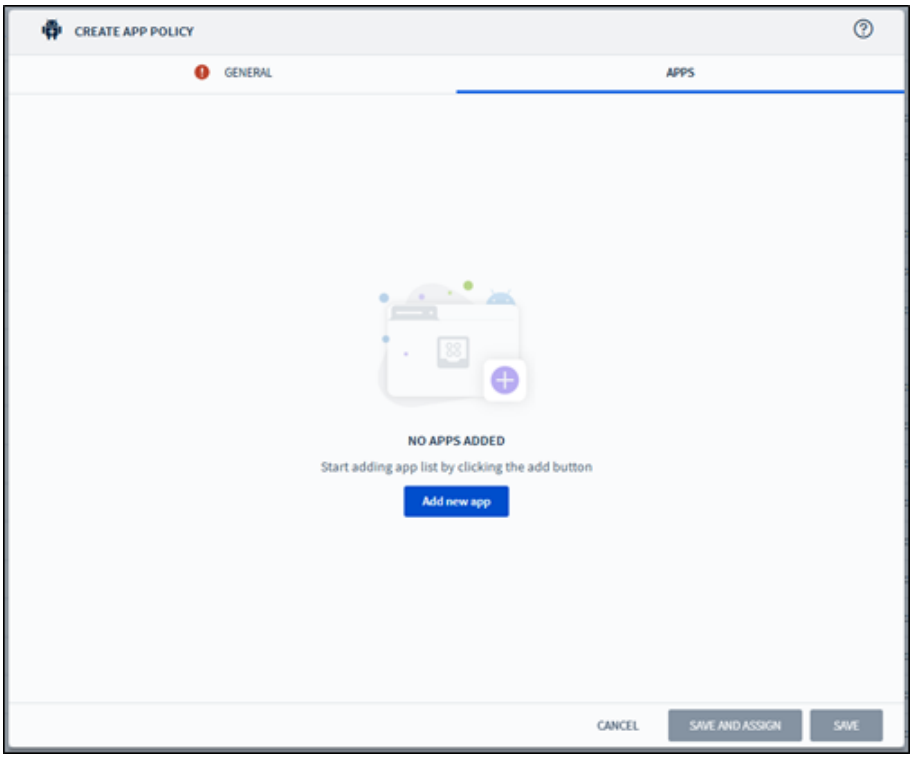
5. Go to **Android option** > **Android Enterprise**.



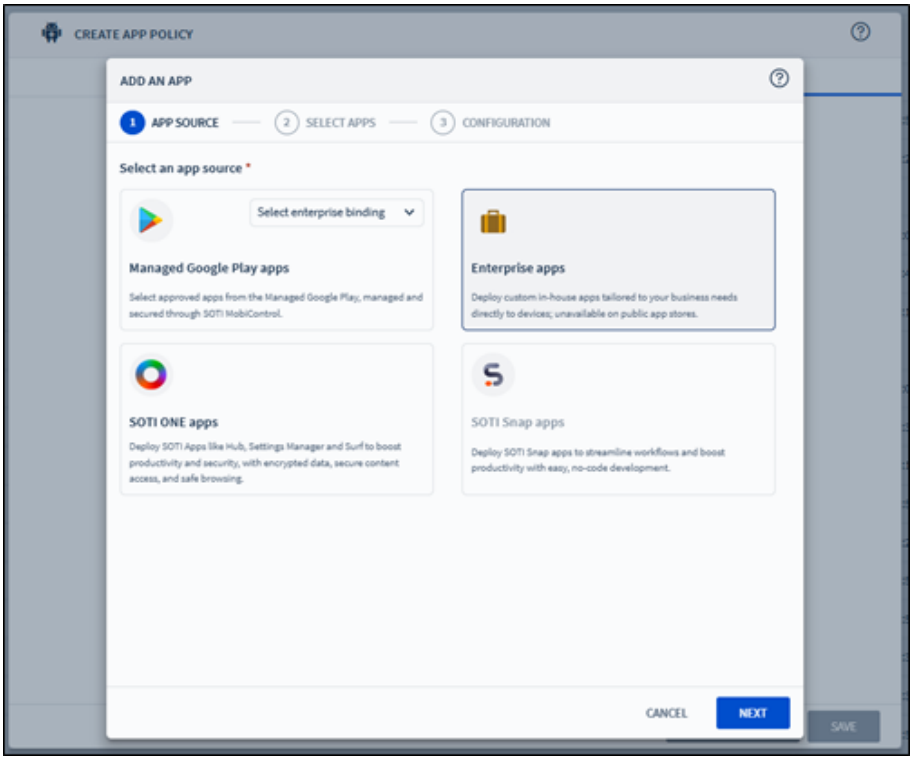
6. In **General** tab, provide **App Policy Name**.



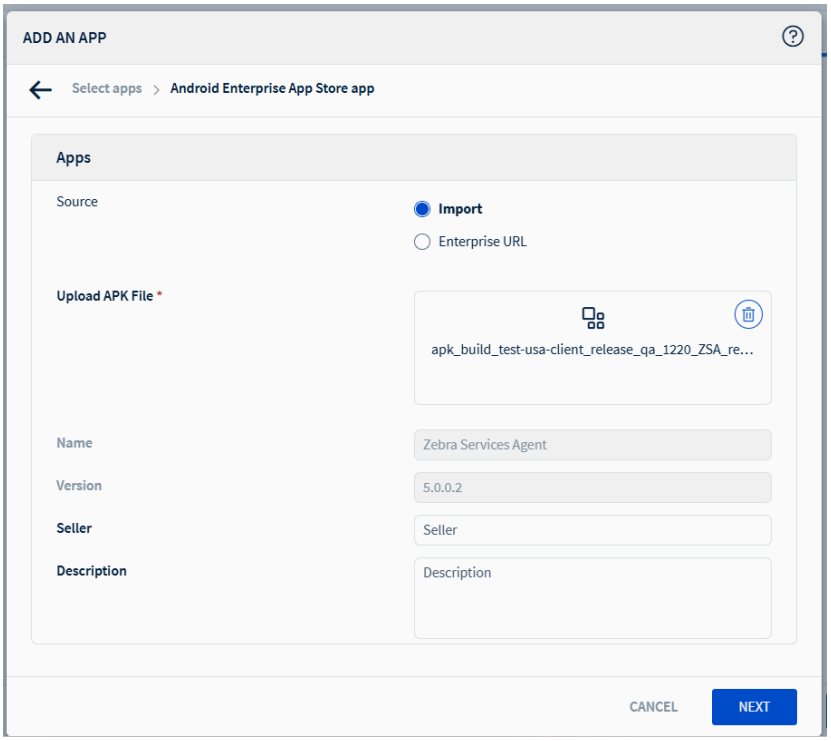
7. Go to **Apps** tab, click on **Add new app**.



8. Select **Enterprise apps** as **App Source** and click **Next**.

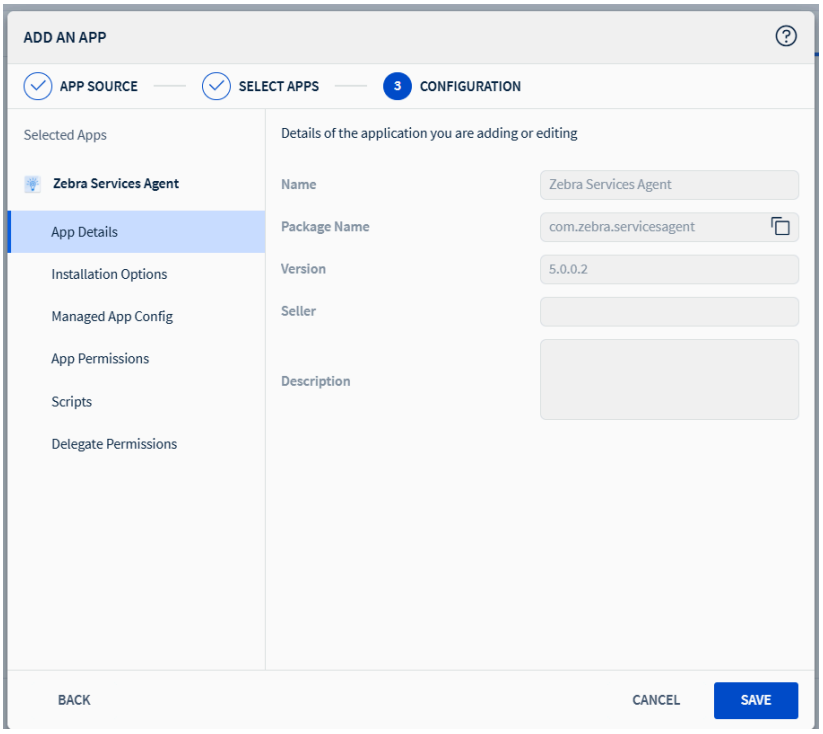


9. Click **+ Upload new apk** and select **Import** under the **Source** field.
10. Click **Browse File** to upload the **APK** file.

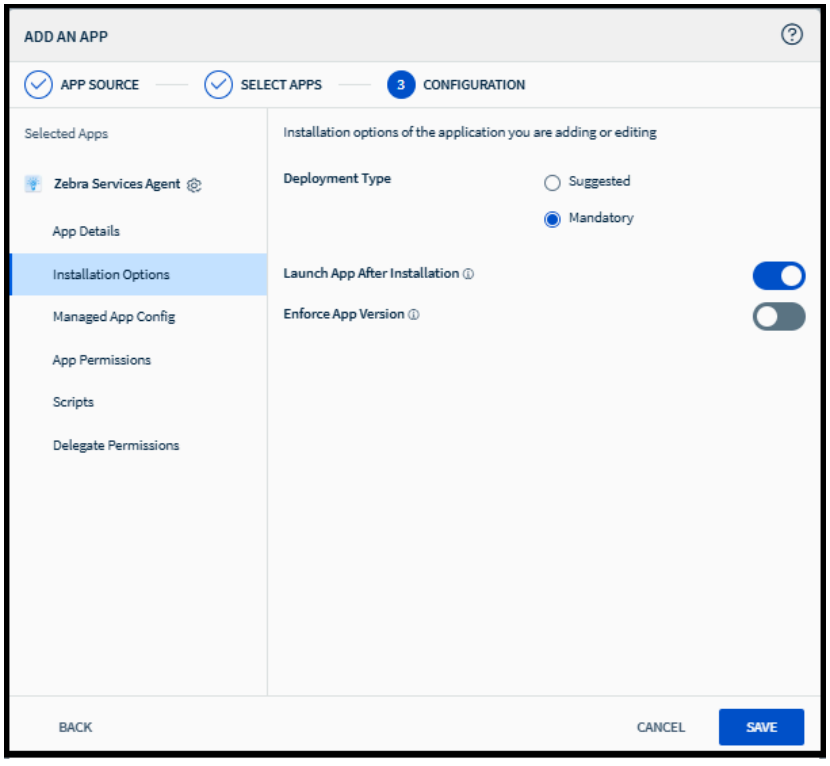


11. Click **Next**.

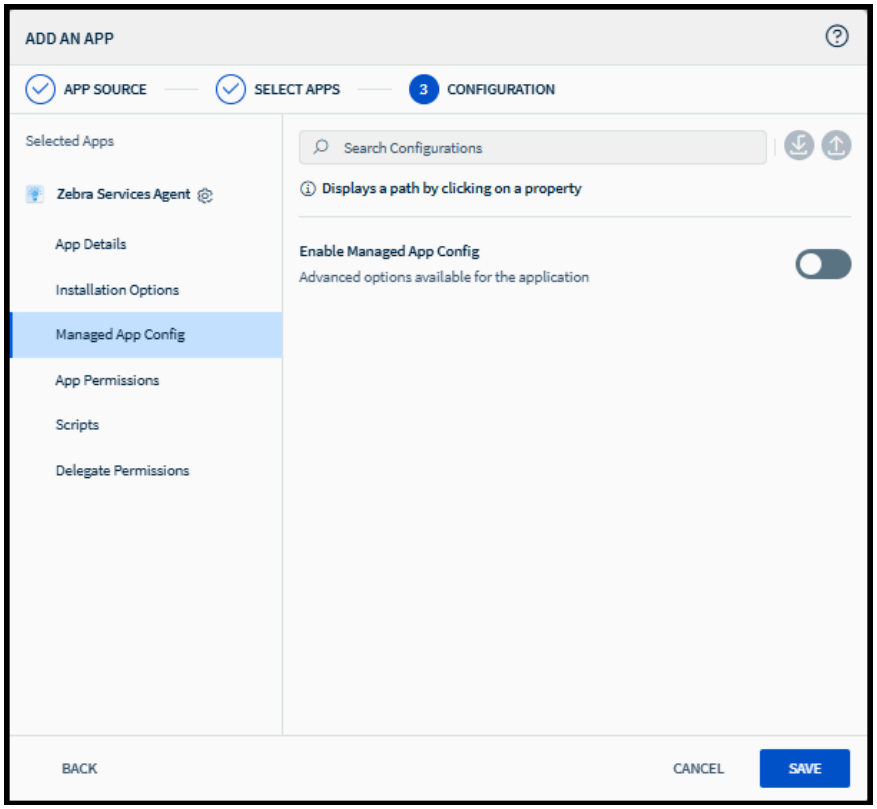
It will redirect to **Configuration** step.

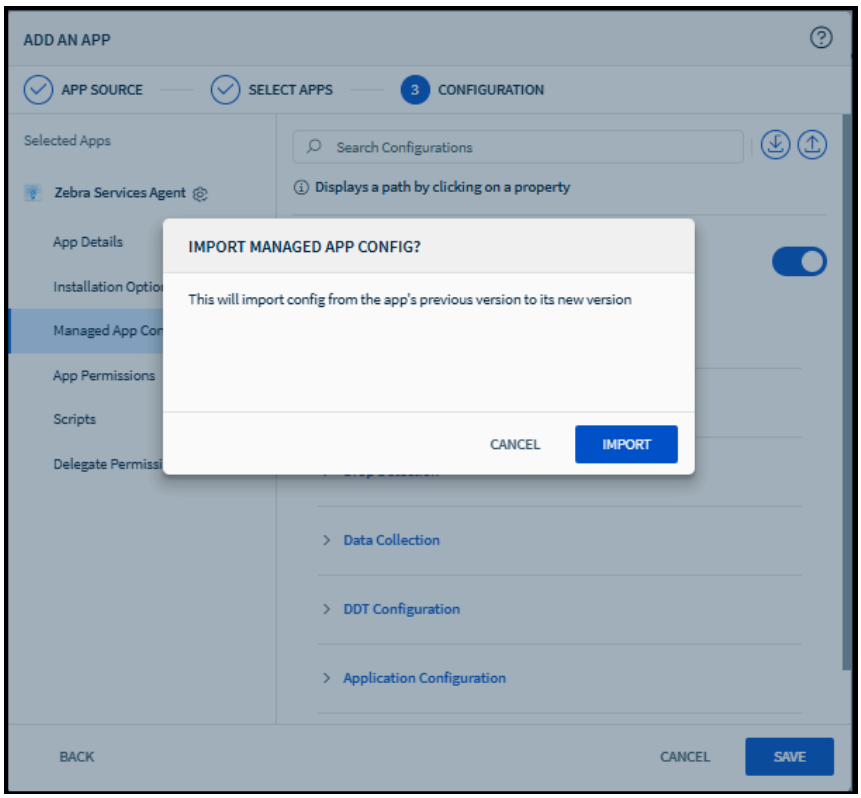


a. Go to **Installation Options** and enable **Launch App After Installation**.

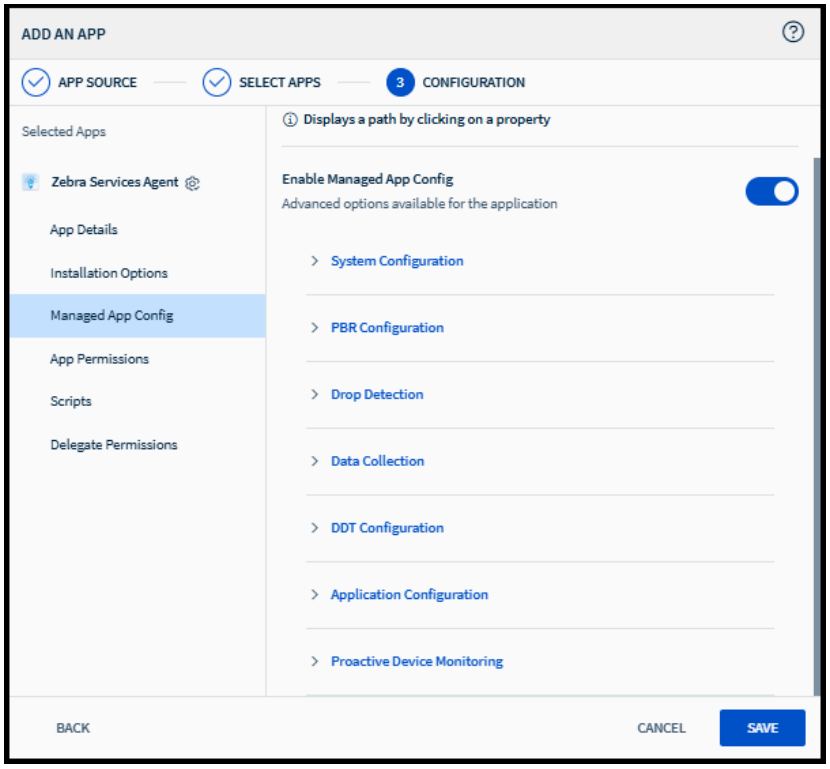


b. Go to **Managed App Config**, enable the **Enable Managed App Config** option and **Import**.





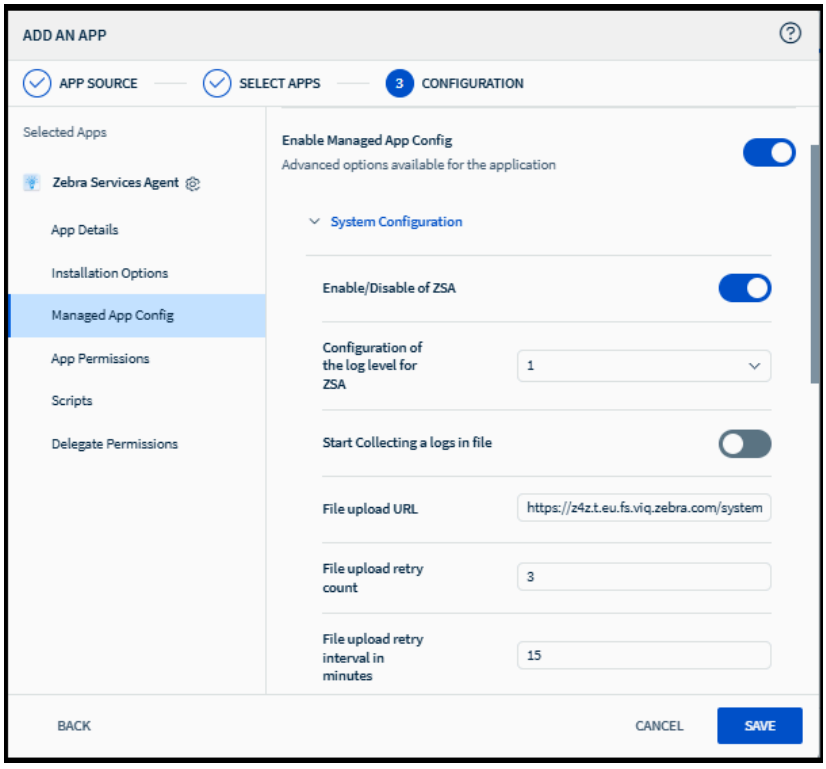
The configuration app list display.



c. 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

d. Enable **Start Collecting a logs in file** to capture ZSA logs.

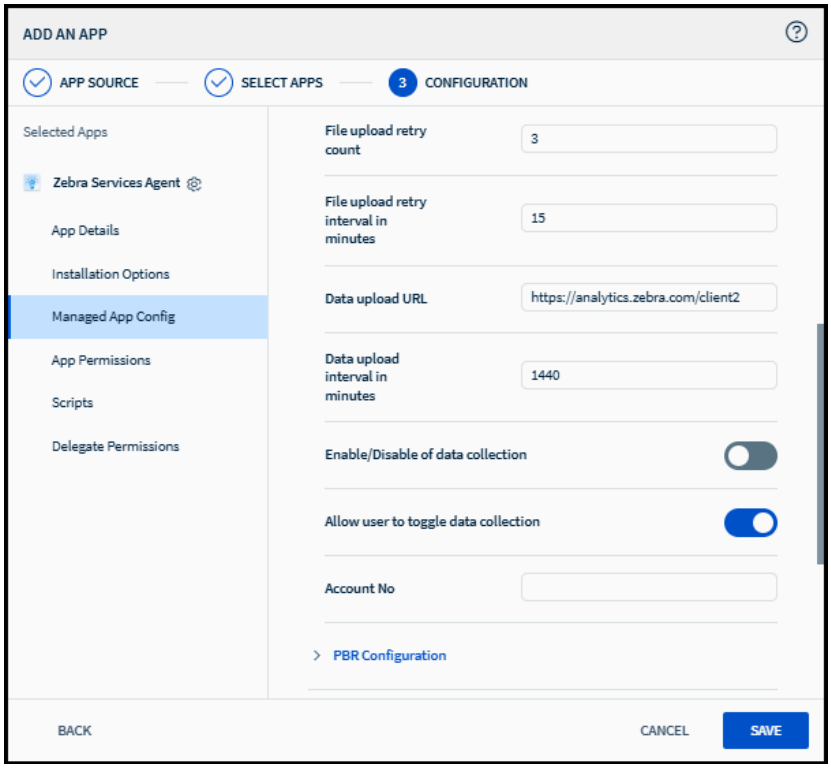


e. The system settings include three features for uploading log files:

- **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.

f. Settings for managing data uploads on non-Zebra devices:

- **Data Upload URL**: Specifies the server path for uploading data collection details.
- **Data Upload Interval in minutes**: Sets the frequency of uploads, defaulting to 24 hours (1440 minutes).



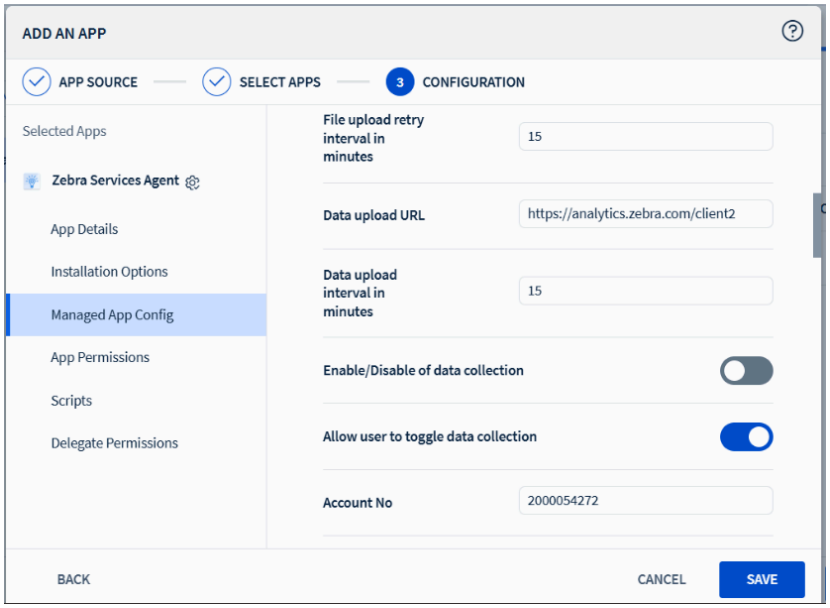
g. Data collection settings for non-Zebra devices:

- **Enable/Disable of data collection**: Data collection is turned off by default. When enabled, it gathers information on default enabled data collections, which can be uploaded to the server specified in the **Data upload URL**. Admin can modify the data collection that is default disabled.
- **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.

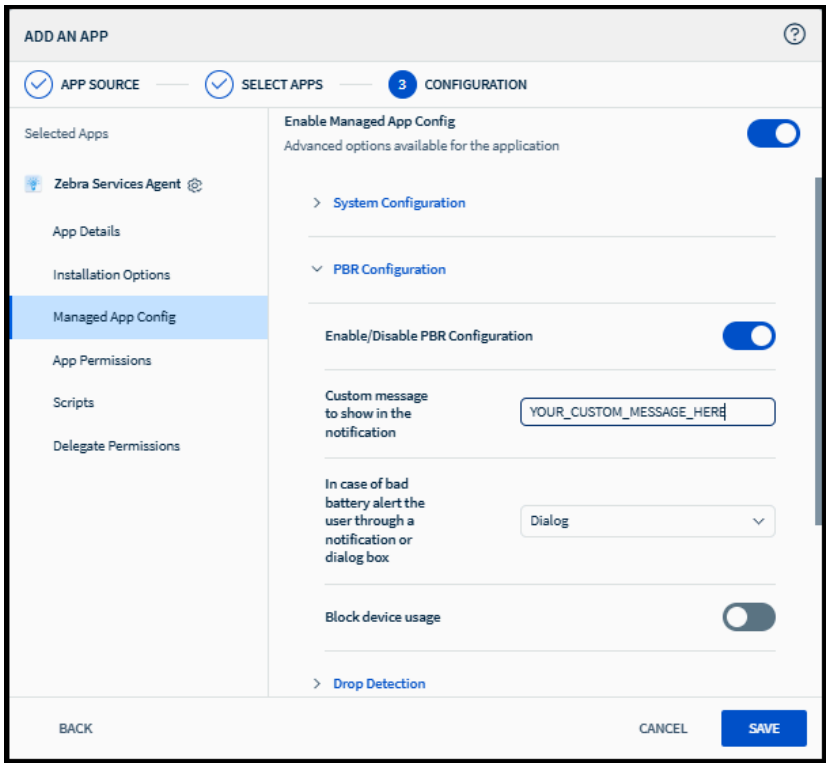
h. Mandatory setup for non-Zebra devices:

To view data on the VisibilityIQ portal, you must enter the **Account ID** provided by your Zebra onboarding team during the **ZSA installation**.

NOTE: This step is mandatory for all non-Zebra devices to enable data visibility.



i. Go to **PBR Configuration**, turn on **Enable/Disable PBR Configuration**, and provide a **Custom Message** as required.



j. Set the **In case of bad battery alert the user through a notification or dialog box** with the following values:

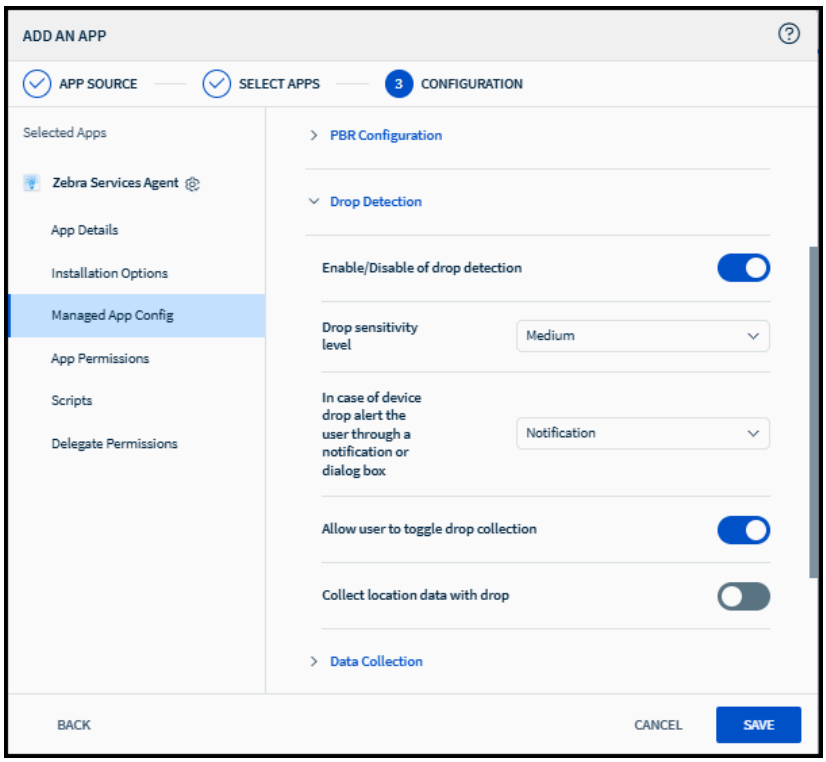
- Notification
- Alert Dialog (default)
- Alert Dialogue with Assist

k. The **Block device usage** option is disabled by default. If enabled by the administrator, it prevents device access when a bad battery is detected.

l. Go to **Drop Detection**, toggle the **Enable/Disable of drop detection** option as required.

m. Set the **Drop sensitivity level** with the following values:

- High
- Medium (default)
- Low



n. Set the **In case of device drop alert the user through a notification or dialog box** with the following values:

- Notification (default)
- Alert Dialog
- Alert Dialogue with Assist

o. 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.

p. The **Collect location data with drop** allows capturing location (latitude-longitude) data of the device when the device drops.

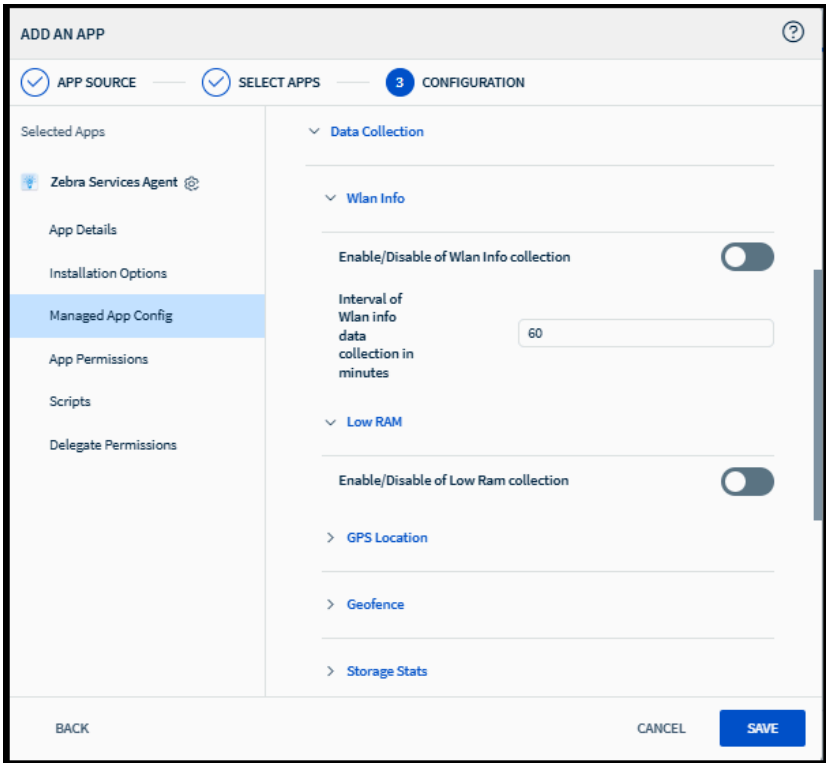
q. Navigate to the **Data Collection** section. The settings for data collection on non-Zebra devices are as follows:

- Default enabled data collections:
  - Battery
  - Device Info
  - Application List and Events

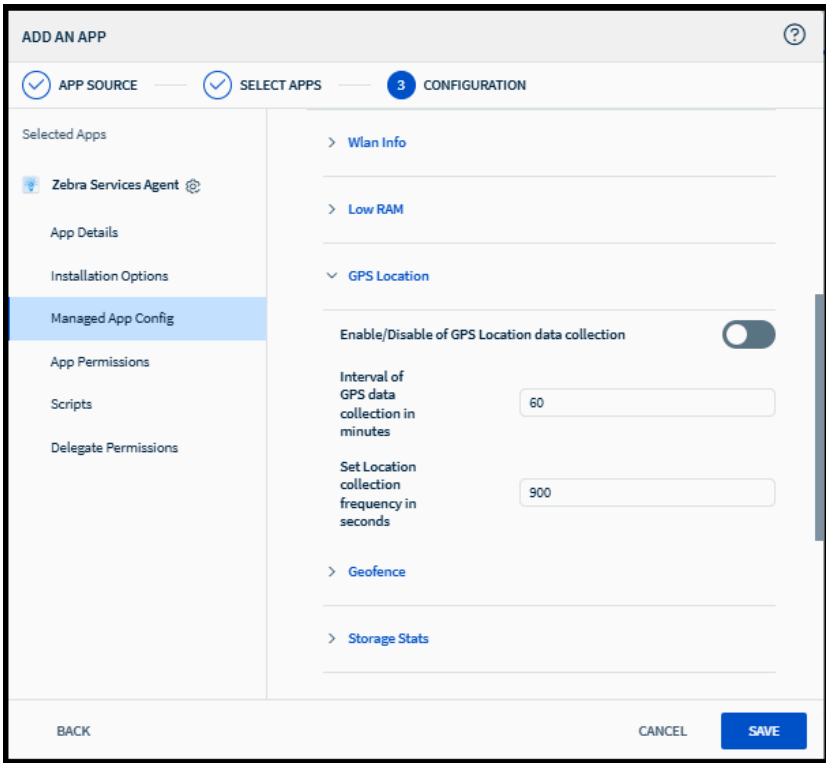
- Application Usage
- Battery Events
- Bluetooth Events
- RAM Stats
- Flash Stats
- Utilization
- WWAN Information
- Screen Brightness
- WLAN Stats
- Device Usage
- Feature Usage
- Doze Mode
- Scanner Info

Admin can change below data collections:

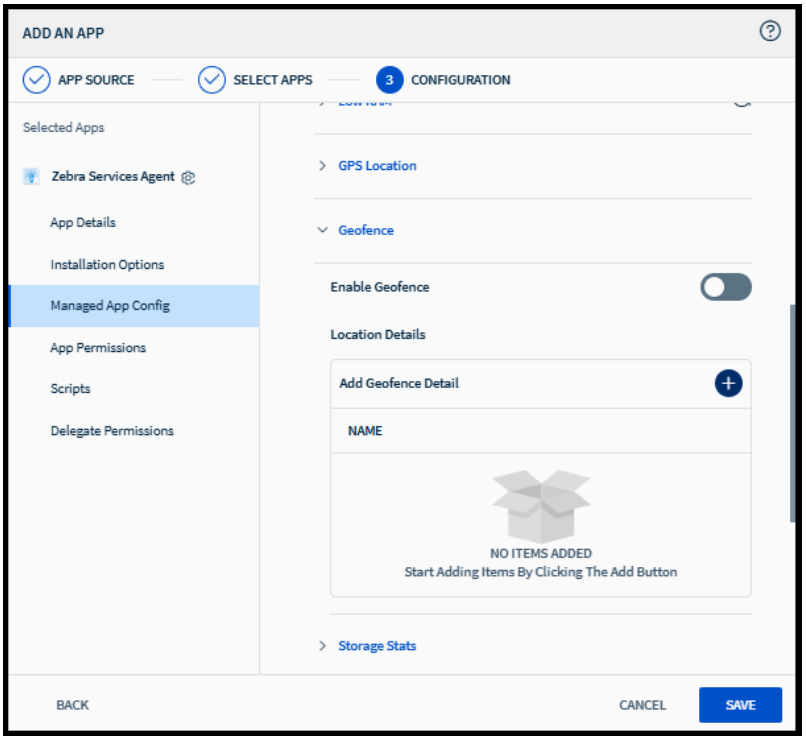
- **WLAN Info**: Select **Enable/Disable of WLAN info collection** and add value in **Interval of WLAN info data collection in minutes**.
- **Low RAM**: Select **Enable/Disable of Low RAM collection**.

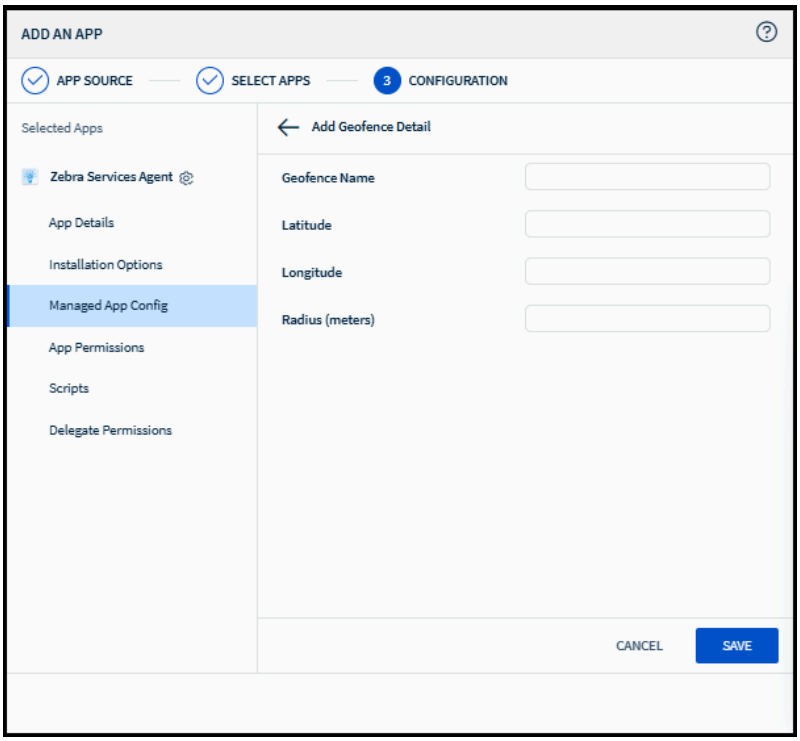


- **GPS Location**: Track device with turning on **Enable/Disable of GPS Location data collection** and add values in **Interval of GPS data collection in minutes**.



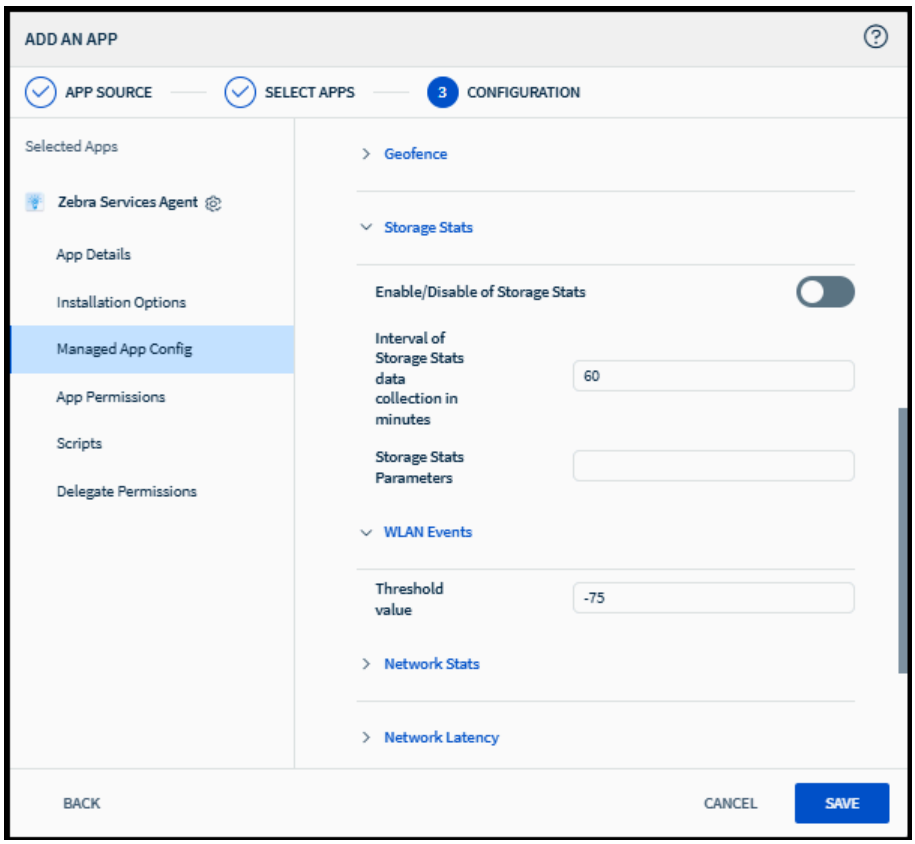
- **Geofence**: Get notified when the device leaves the predefined fencing area by selecting **Enable Geofence** and add **Location details**.
  - **Geofence Name**: Name of the area
  - **Latitude-Longitude**: Lat-long of the specific area
  - **Radius (meter)**: Radius area to cover around specified lat-long



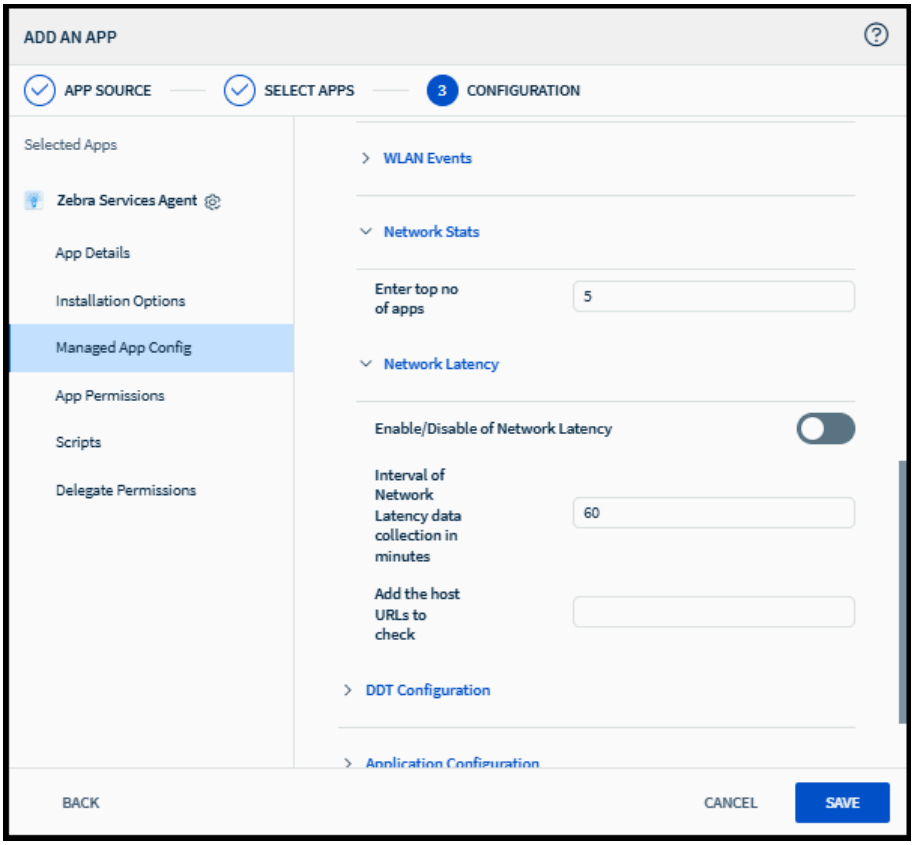


- **Storage Stats**: Enable the **Enable/Disable of Storage Stats** option and add a value in the **Interval of Storage Stats data collection in minutes**.
  - **Storage Stats Parameters**: Configure the package names for monitoring.

- **WLAN Events**: Enabled by default and cannot be disabled. The admin can adjust the threshold value (in minutes).
  - **WLAN** event data is collected based on the configured threshold value.



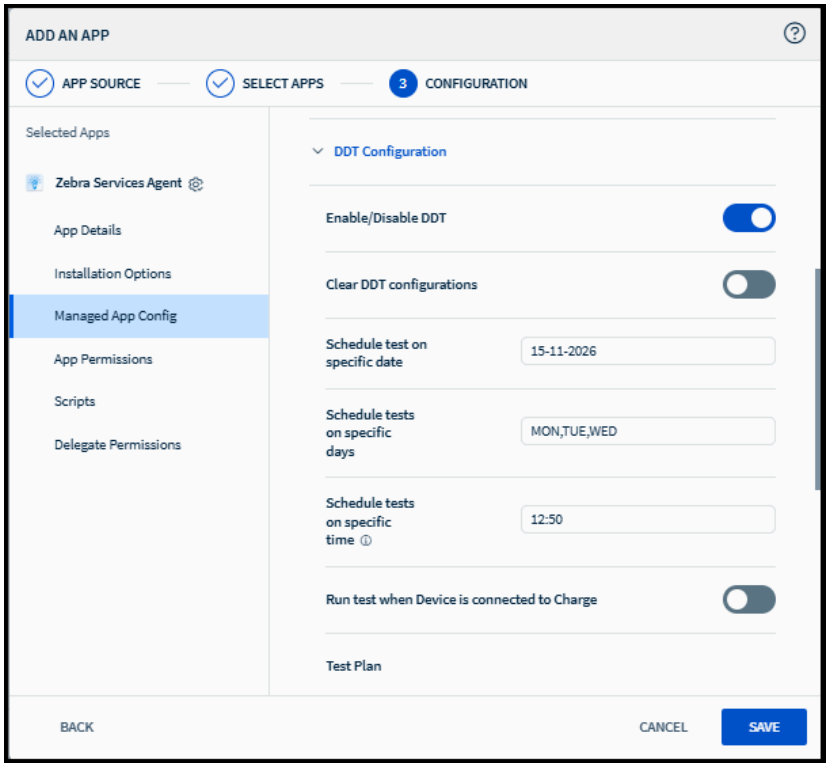
- **Network Stats**: Enabled by default and cannot be disabled. The admin can adjust the top no of app counts.
- **Network Latency**: Disabled by default, if enabled, it records network performance details for configured host URLs, including the target host, measured latency, network type, signal strength, connection information, and request result stats as an error message.



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

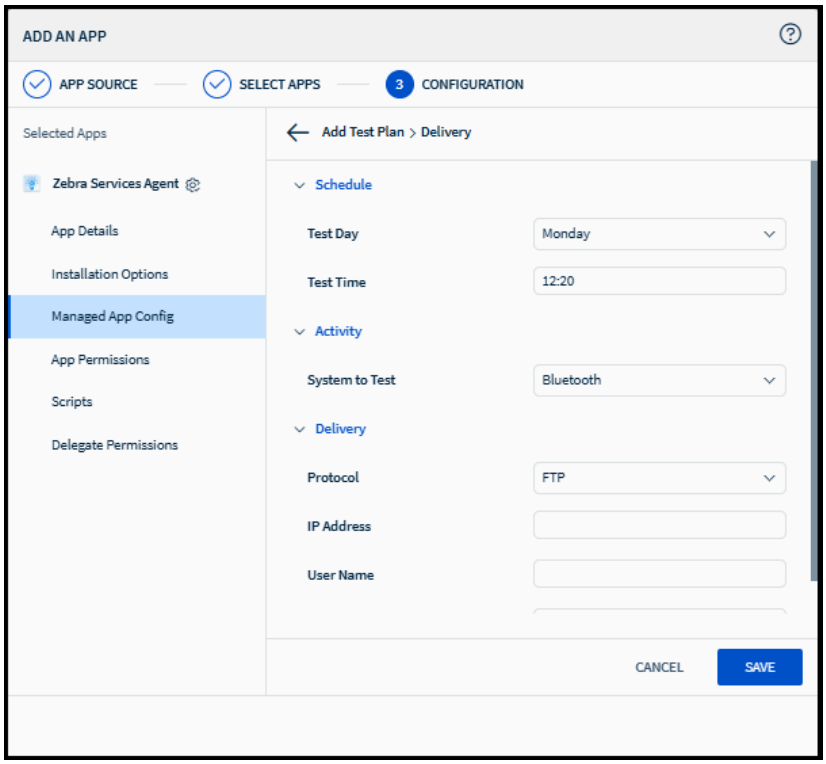
r. Under the **DDT Configuration**:

- Enable the **Enable/Disable DDT** option.
- Keep the **Clear DDT configurations** option disabled in the primary setup.
- **One-time tests**: Set the **Schedule test on specific date** in DD-MM-YYYY format if required to schedule one-time tests.
- **Repetitive tests**: For repetitive tests, specify days using the format MON,TUE,WED in the **Schedule tests on specific days** section.
- In **Schedule tests on specific time**, enter the test time in HH:MM 24-hour format for executing one-time or periodic tests.
- **Run test when device is connected to charge**: Disable by default, when enabled, the scheduled test runs only when the device is connected to charge.
- Click **Add** in the **Test Plan** section.



s. Under the **Schedule** section, configure the test plan with the following values:

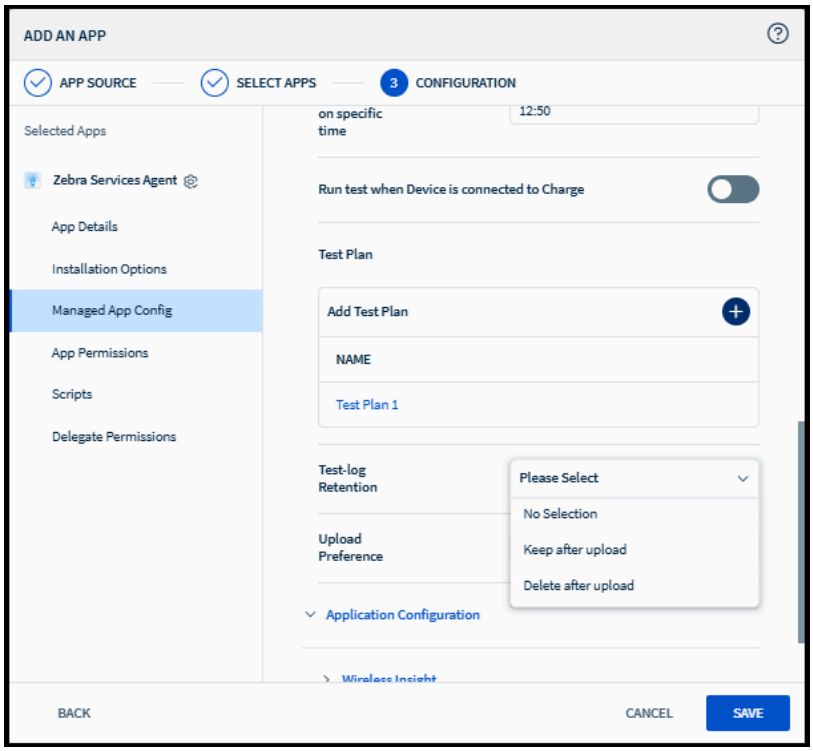
- **Test Day**: Day of the Week (For example, Monday)
- **Test Time**: Time of the day for the test (HH:MM format)



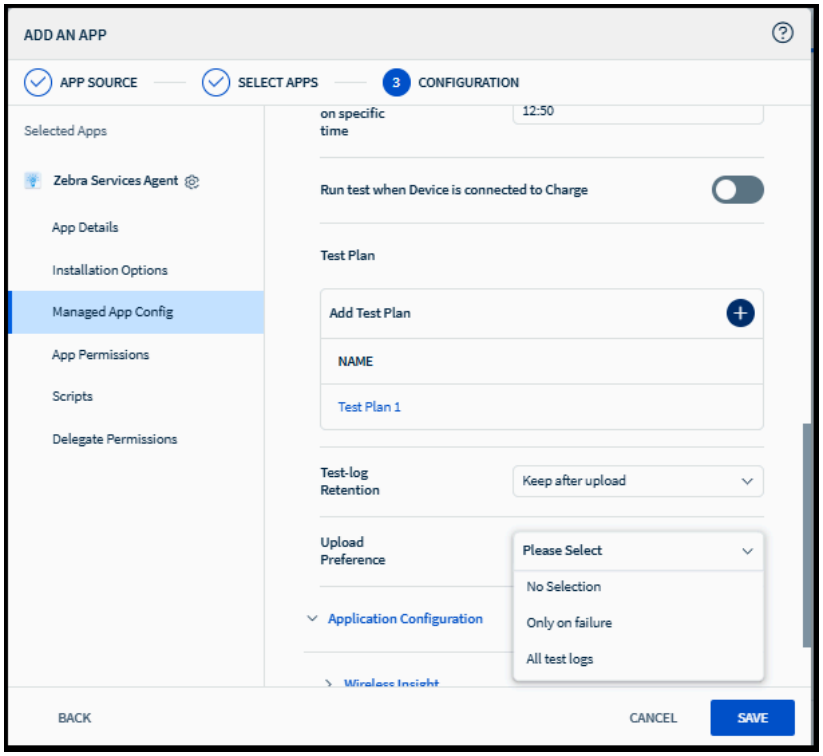
t. Select **Bluetooth** as the **System to Test** option.

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

v. Select the **Test-log Retention** as required.

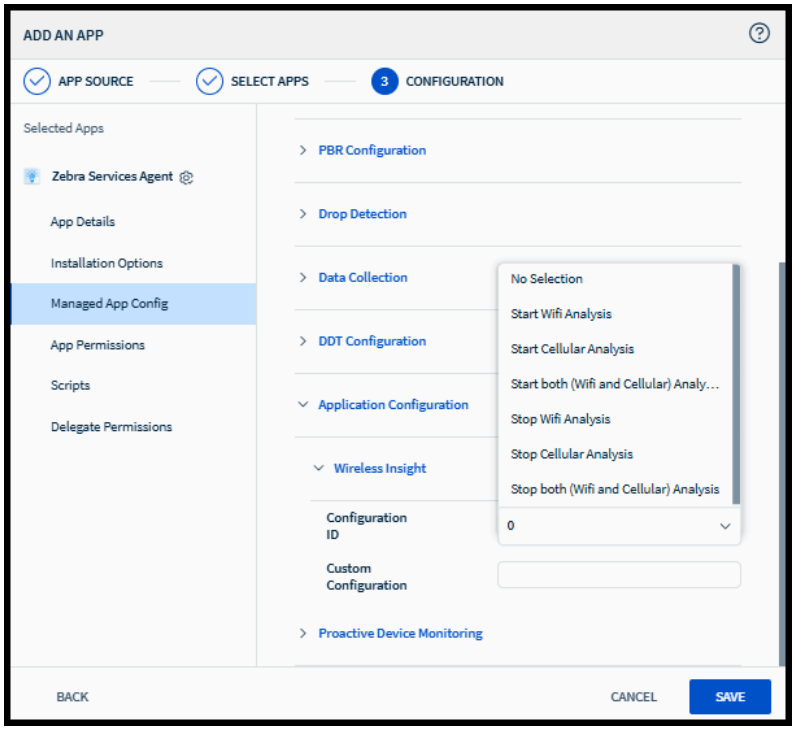


w. Select the **Upload Preference** as required.



x. 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.



- **Custom Configuration**: Add the custom Wireless Insight configuration as a value.

- **ZDS**: Configured through VIQ with a custom ZDS configuration.

y. Go to the **Proactive Device Monitoring** option and enable the following settings.

- **Frequent Wi-Fi Disconnections**

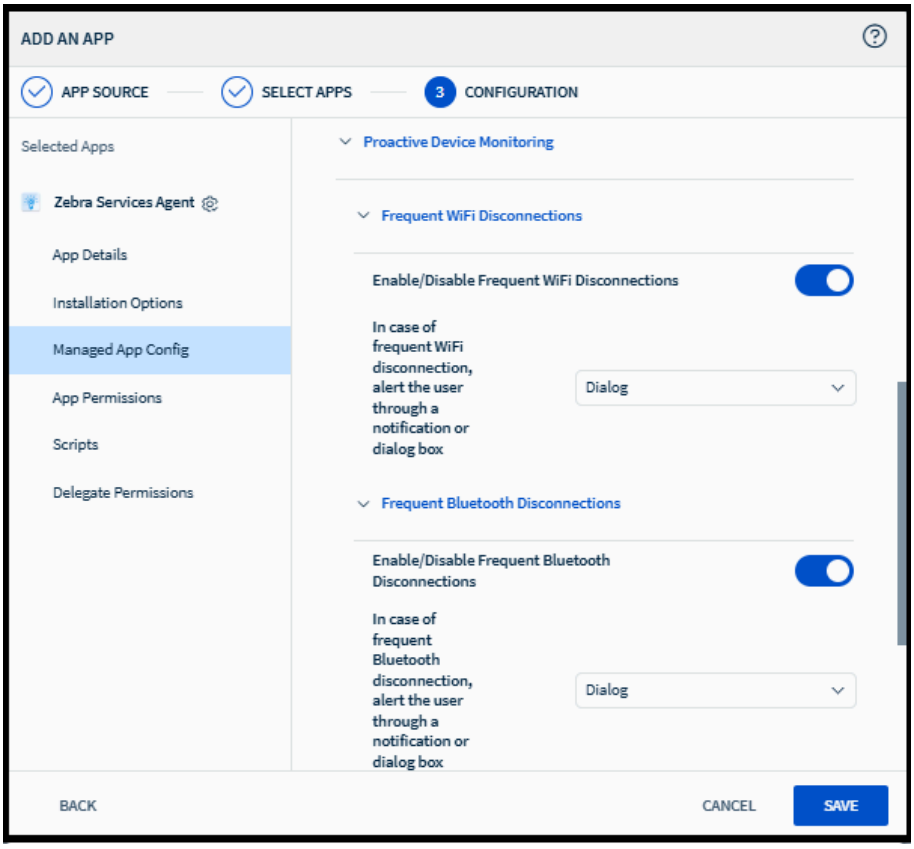
  Enable the **Enable/Disable Frequent Wi-Fi Disconnections** and set the **In case of Frequent Wi-Fi disconnection, alert the user through a notification or dialog box** with the following options:

  - Notification
  - Dialog (Default)

- **Frequent Bluetooth Disconnections**

  Enable the **Enable/Disable Frequent Bluetooth Disconnections** and set the **In case of Frequent Bluetooth disconnection, alert the user through a notification or dialog box** with the following options:

  - Notification
  - Dialog (Default)



- **Frequent Device Reboots**

  Enable the **Enable/Disable Frequent Device Reboot** and set the **In case of Frequent device reboot, alert the user through a notification or dialog box** with the following options:

  - Notification
  - Dialog (Default)

- **Alert on Severe Drop Detection**

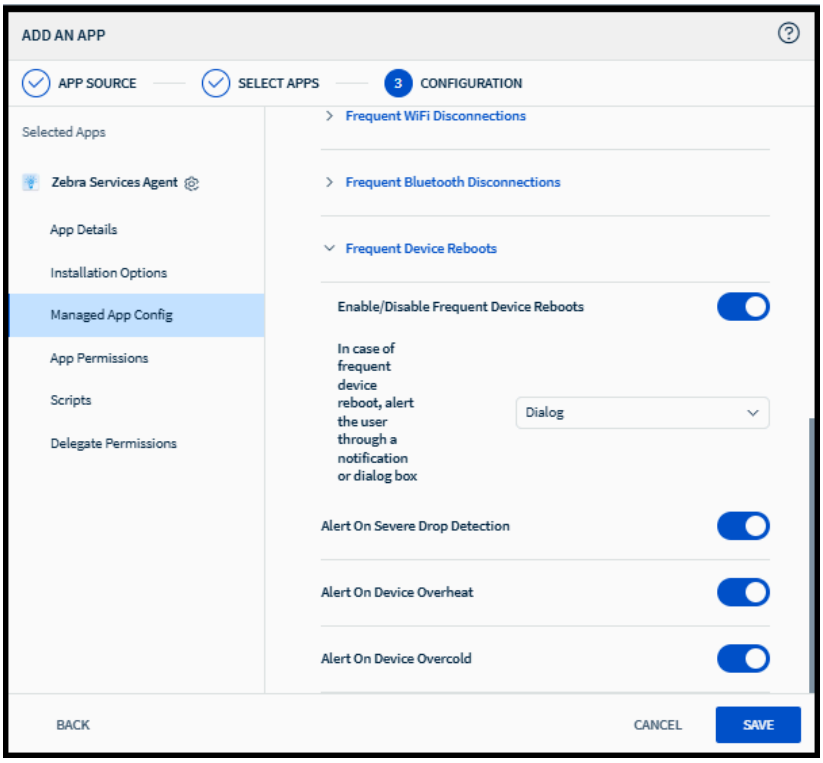
  Disabled by default. When enabled by an administrator, it allows the device to receive commands from ZDS upon detecting a severe drop.

- **Alert on Device Overheat**

  Disabled by default. When enabled by an administrator, it allows the device to receive commands from ZDS upon detecting an overheat event.

- **Alert on Device Over cold**

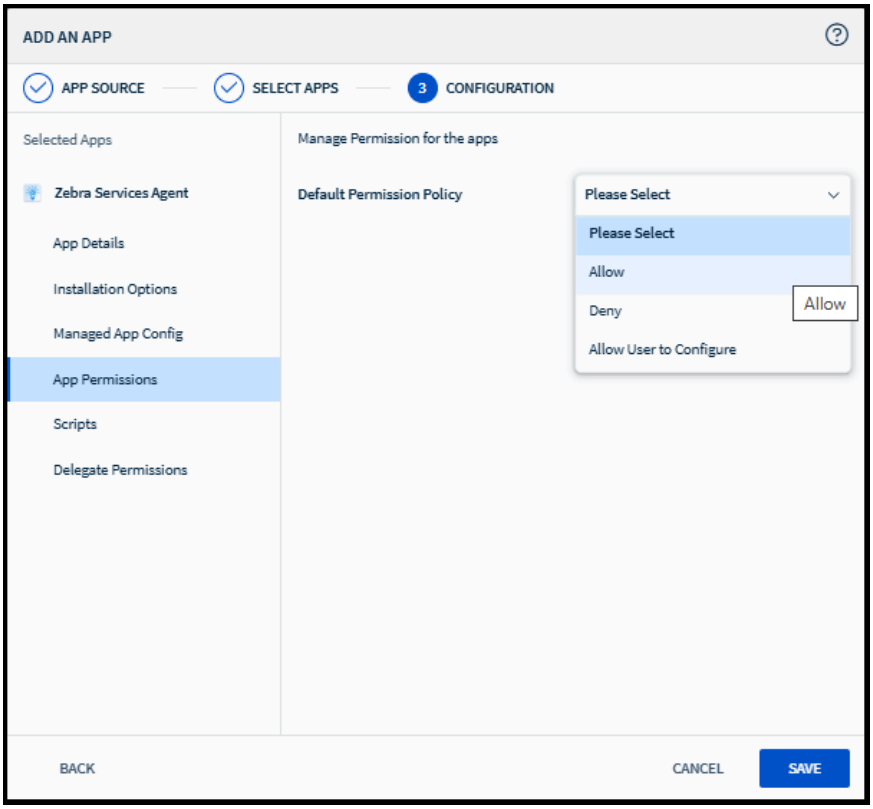
  Disabled by default. When enabled by an administrator, it allows the device to receive commands from ZDS upon detecting an under-temperature or overcooling event.



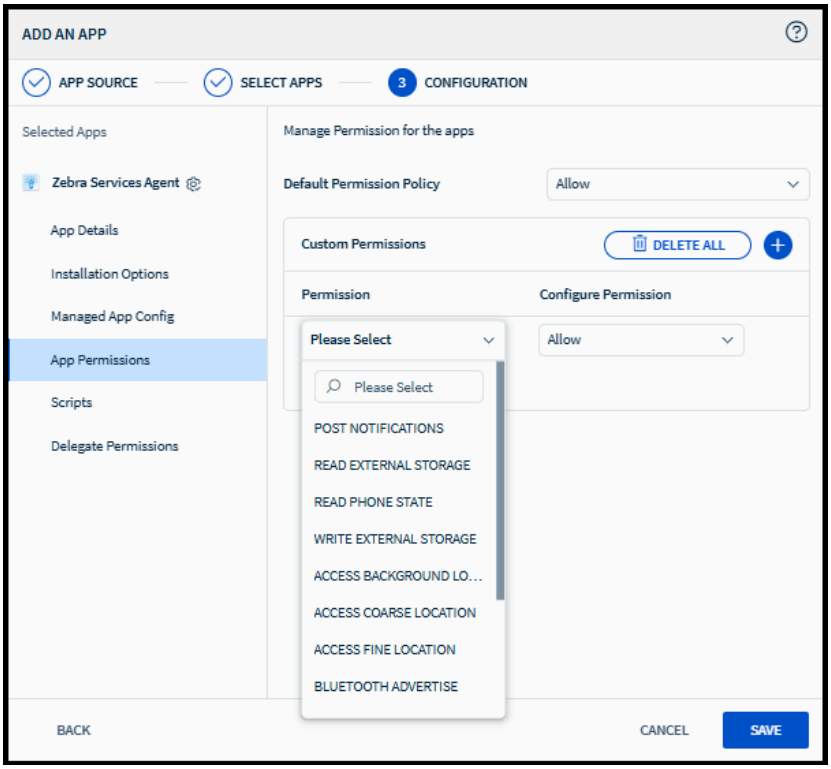
z. Click on **Save**.

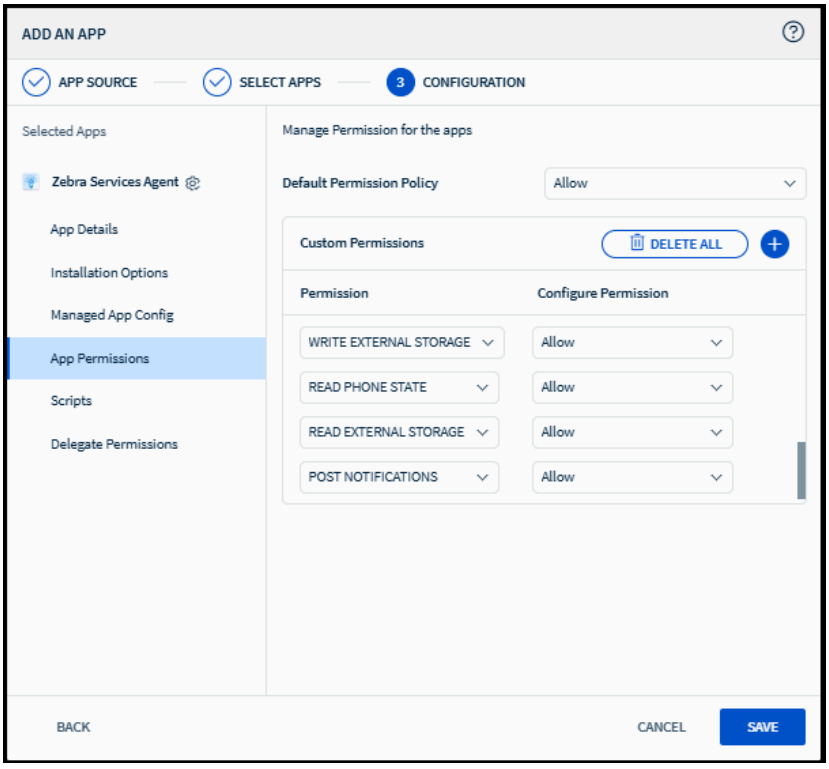
aa. From the left panel of **Configuration Options**, select **App Permissions**.

- Select **Allow** from the drop-down of **Default Permission Policy**.



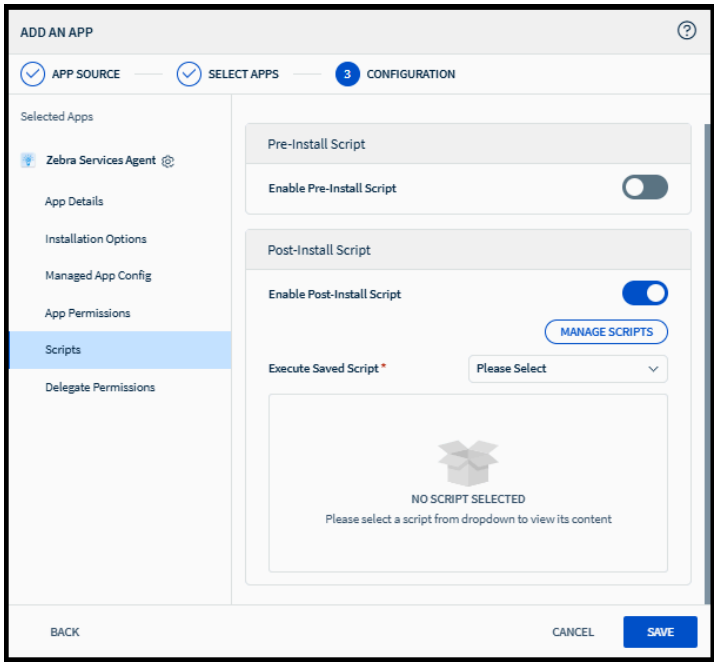
- Click on **+ Add** and select all permissions one by one from the **Permission** drop-down.





- Select **Save**.

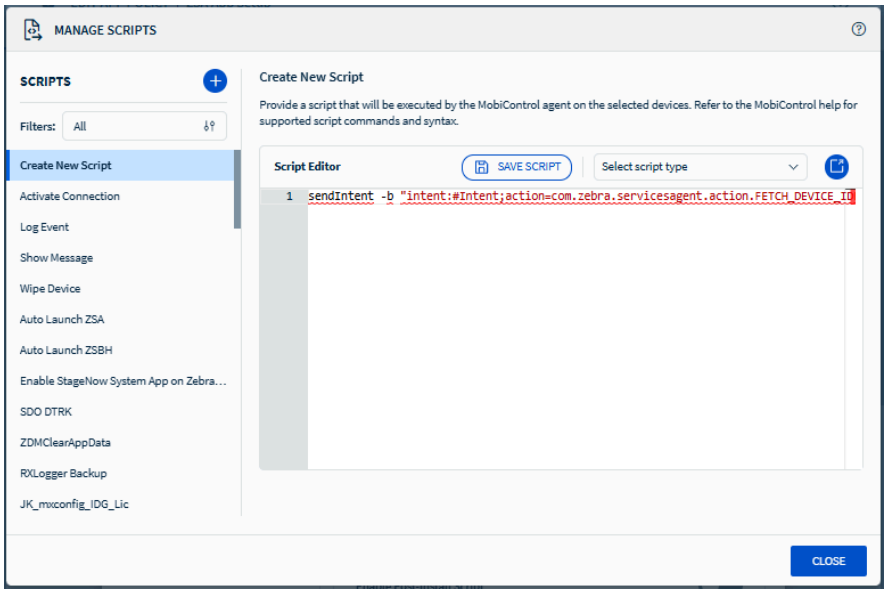
ab. From the left panel, go to **Scripts** > **Manage Scripts**.



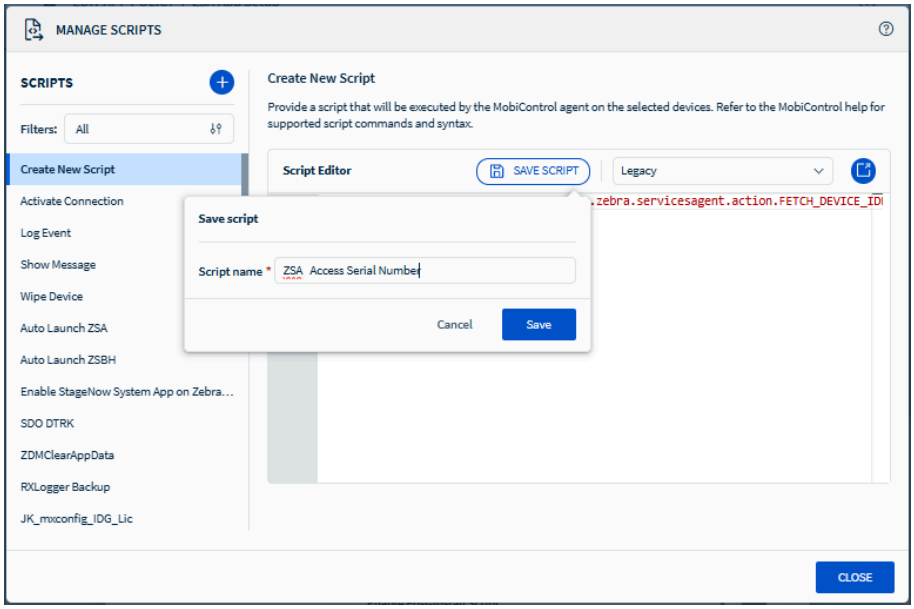
ac. Select **Create New Script** and add the script below in the **Script Editor**.

```
sendintent -b
```

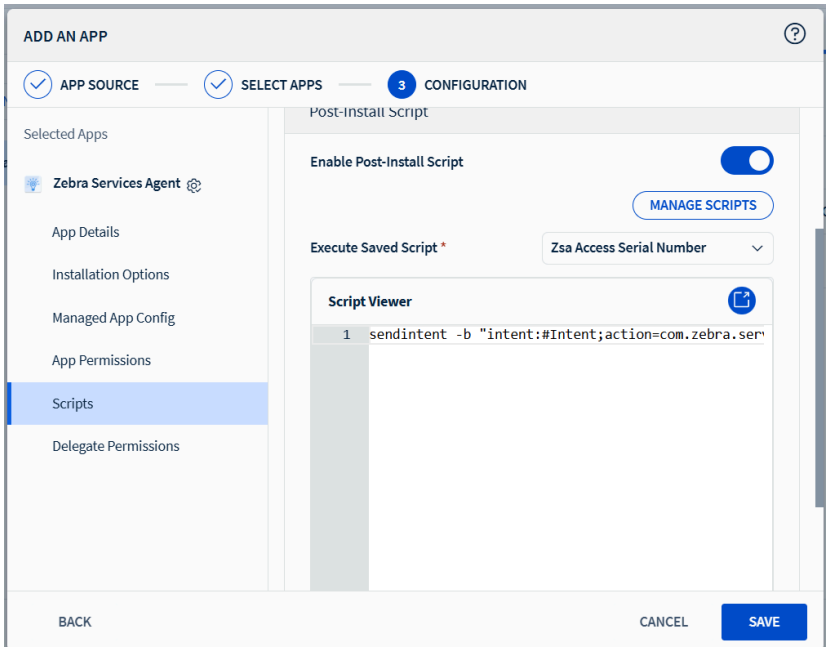
```
"intent:#Intent;action=com.zebra.servicesagent.action.FETCH_DEVICE_IDEN
TIFIERS;
 S.serialNumber=%SERIALNUM%; component=com.zebra.servicesagent/
com.zebra.utility.deviceIdentifier.SOTIReceiver; end;"
```



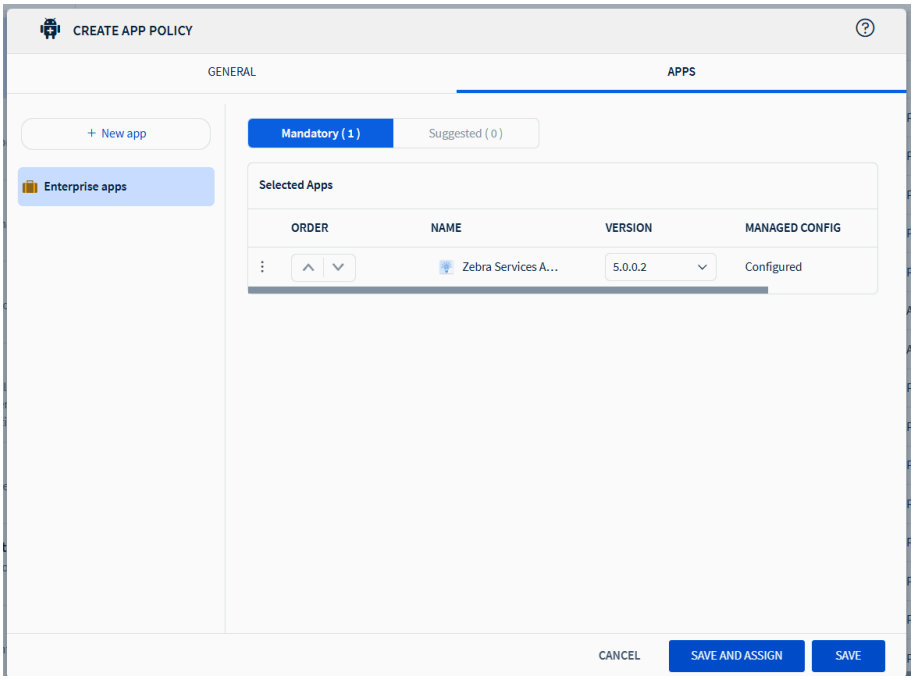
ad. Click on **Save Script** and add **Script name - ZSA Serial Number** and click **Save**.



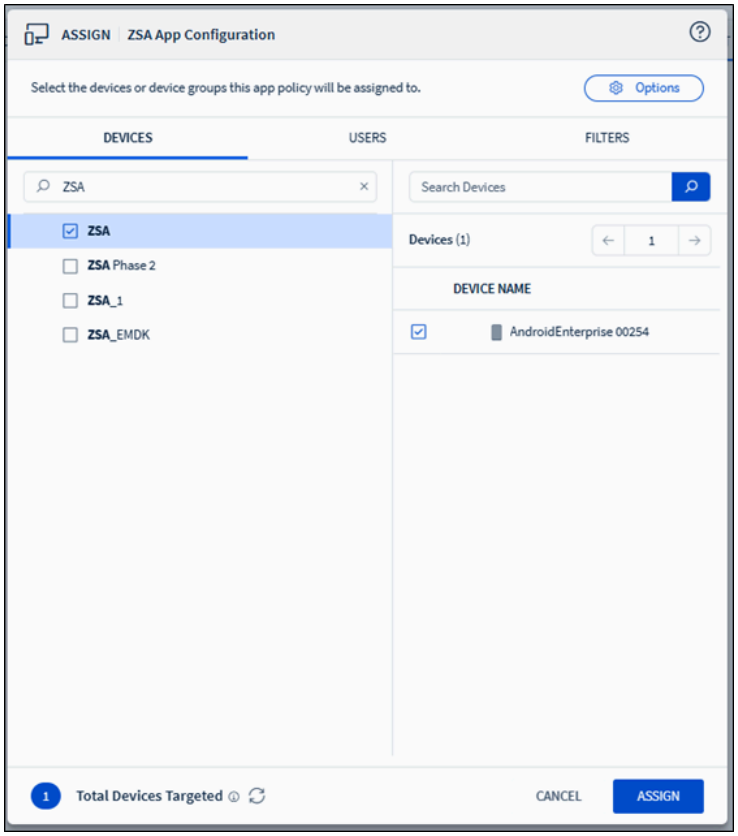
ae. Select **ZSA Access Serial Number** script from **Execute Saved Script** drop down and click **Save**.



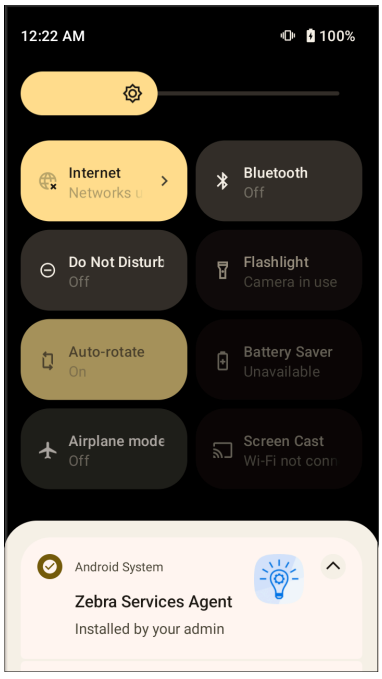
- The **Zebra Services Agent** app is added. Click **Save and Assign**.



af. **Assign** to a group device or a single device.



The application is now installed on the device.



Grant Usage Access Permission on Datalogic Device

Using the Datalogic Scan2Deply application, we can grant the usage access permission silently. The steps are as follows:

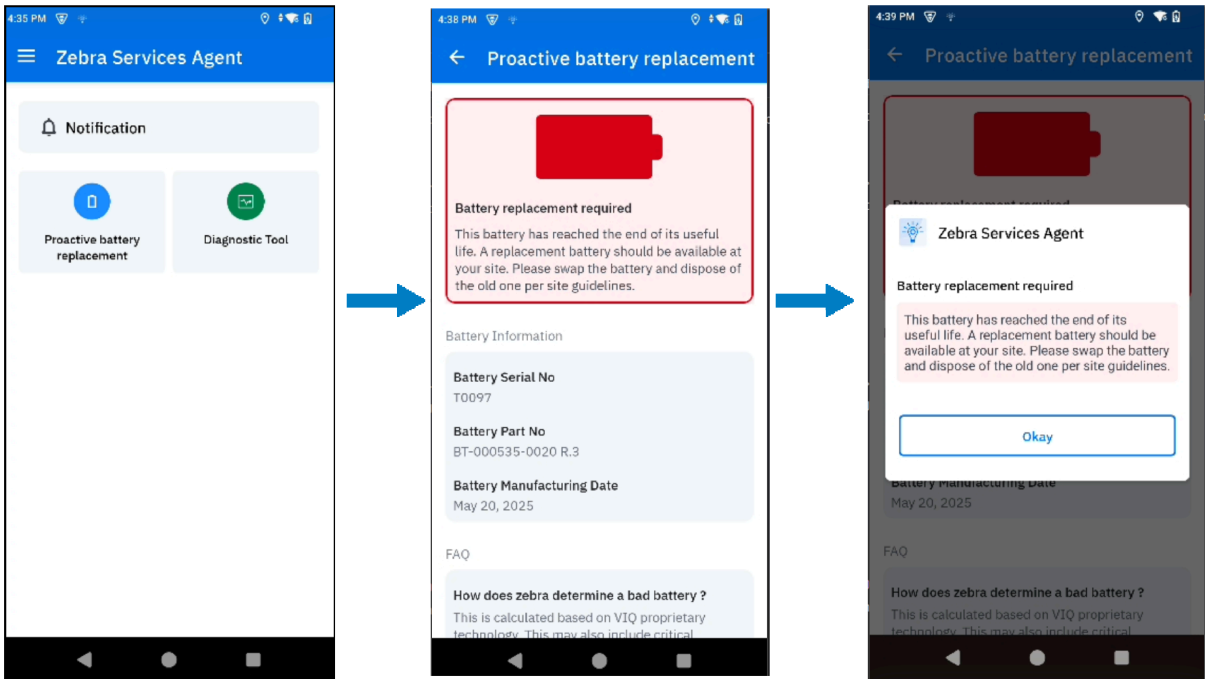
1. Generate the script to grant permission.
2. Push the configuration script to /sdcard on the device.
3. To apply the configuration, trigger the Scan2Deply Using SOTI Send Script.

Reach out to the Zebra Services Agent (ZSA) team for the procedure for generating the configurations.

Expected Behavior After Auto-launching Zebra Services Agent

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

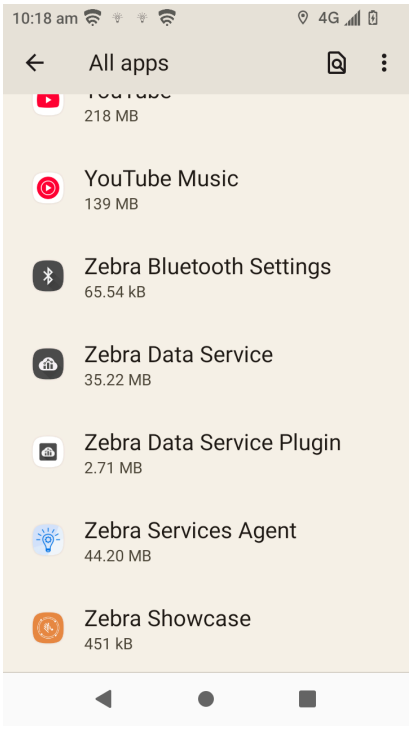
1. Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
2. If the Proactive Battery Health (PBR) module is entitled, the ZSA app automatically launches it after a few seconds.
3. The PBR screen displays both good and bad battery details, and if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



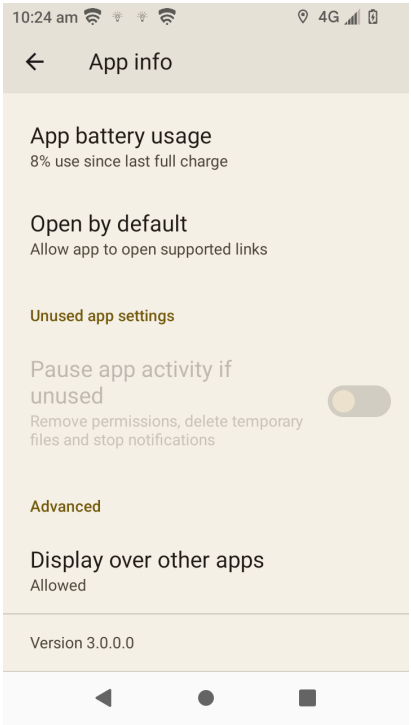
Verifying App Installation and Connection to Zebra Servers

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

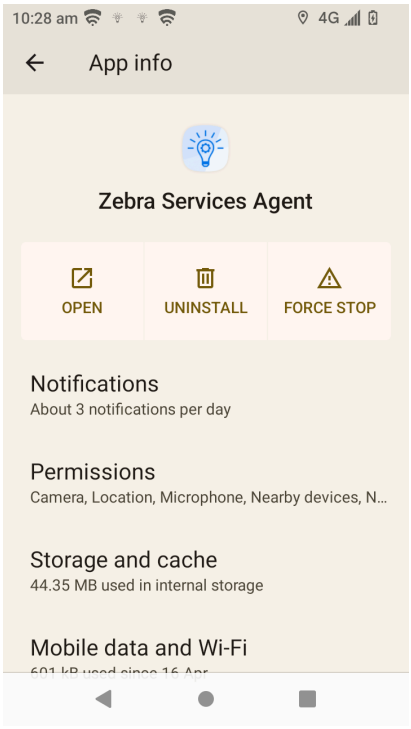
1. Go to **Settings** > **Apps** > **All apps** and select **Zebra Services Agent**.



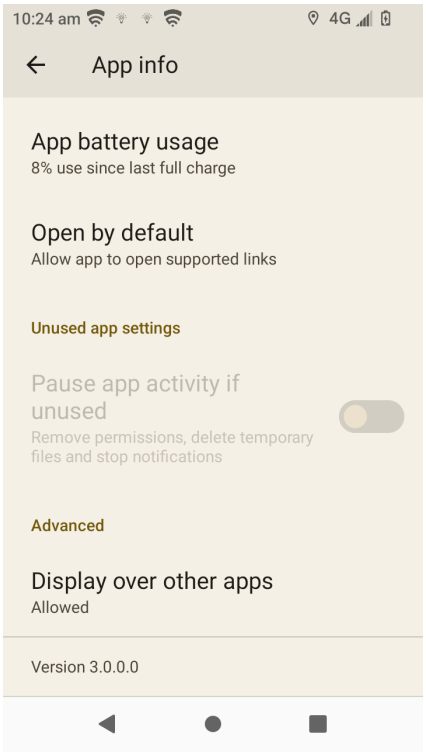
The **App Info** page displays the **Version**.



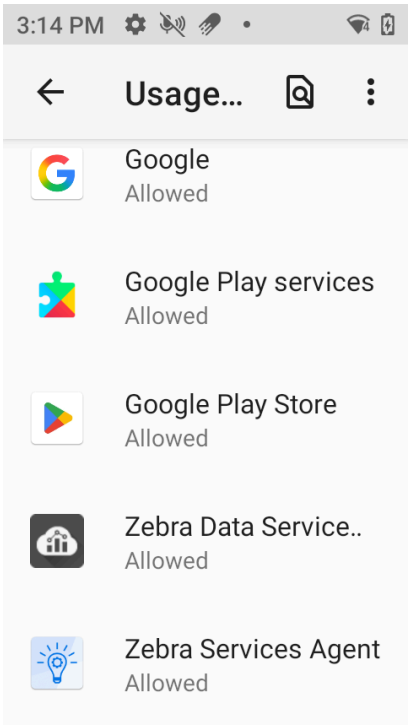
2. For the ZSA Permissions, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Permissions**.



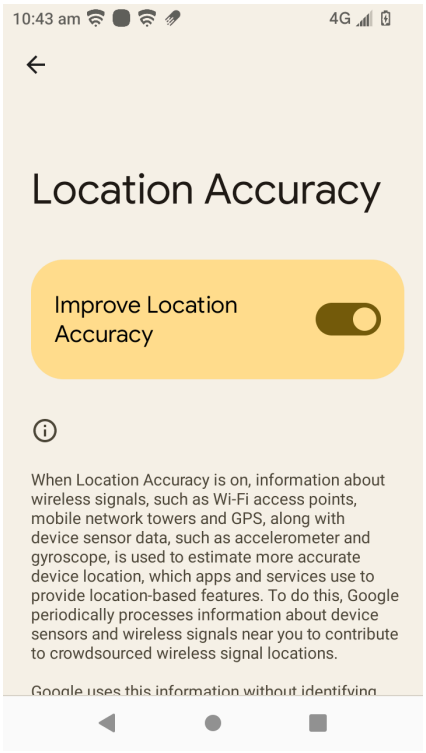
3. To verify the Display over other apps permission, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Advanced** > **Display over other apps**.



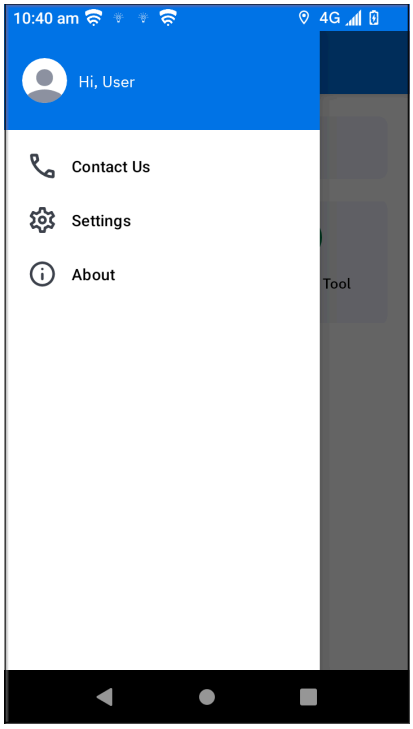
4. To verify Usage access permission, go to **Settings** > **Apps** > **Special app access** > **Usage Access** > **Zebra Service Agent**. Refer Grant Usage Access Permission on Datalogic Device.

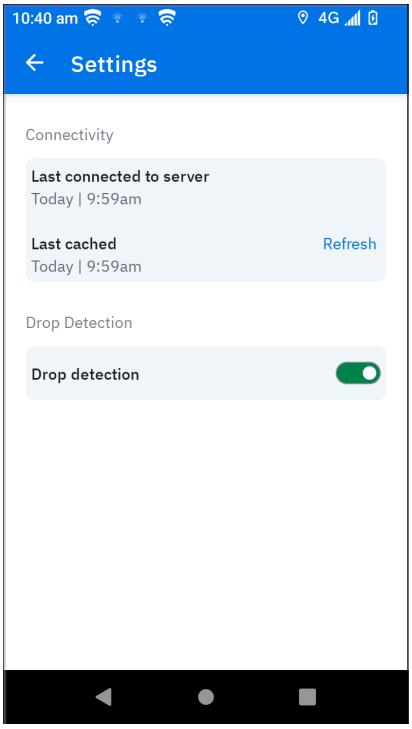


5. For the **Device action** > **Outdoor Location Tracking** feature, ensure that location accuracy is enabled on the device for precise location information. Navigate to **Settings** > **Location** > **Location Services** > **Location Accuracy**.



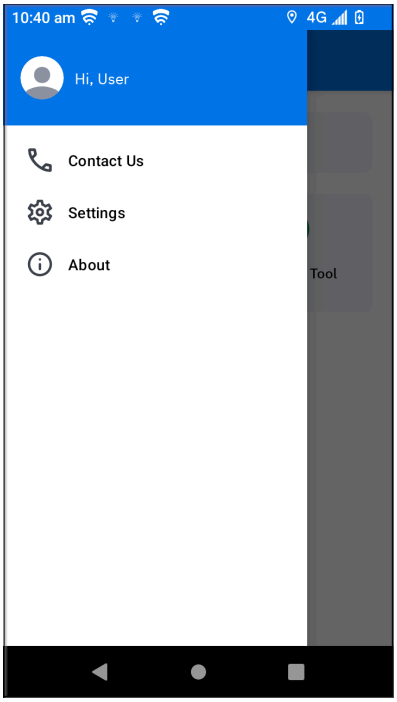
6. To verify ZSA Network connectivity to the Zebra URL:
   - Launch ZSA and go to **Settings** > **Refresh**.

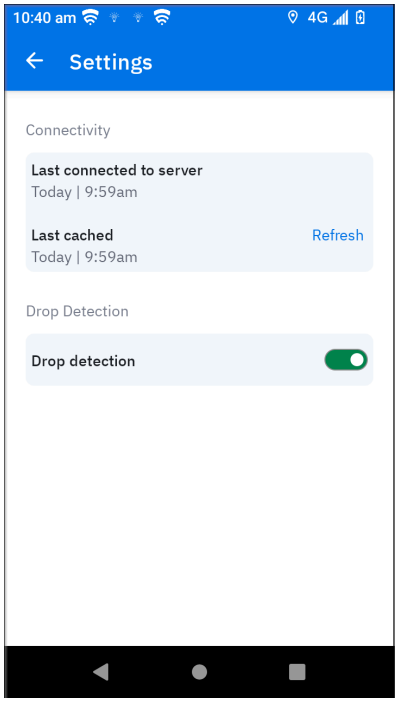




7. To verify the Drop Detection status:

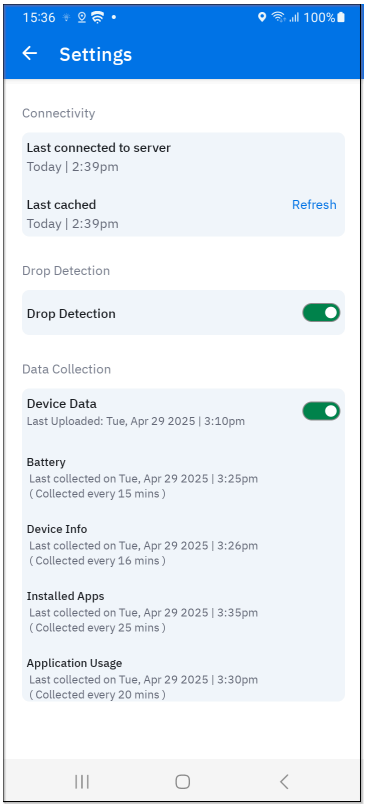
   Launch ZSA and go to **Settings**. Enable **Drop detection**. The user can enable or disable drop detection if the administrator provides toggle access.





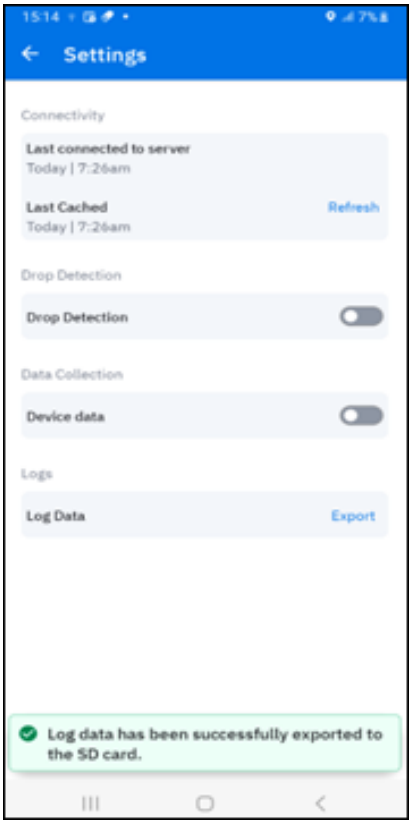
8. To verify Data collection in a non-Zebra device:

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

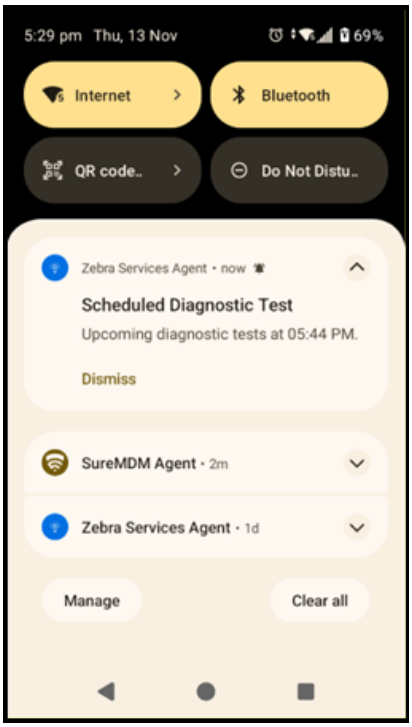


In data collection, the **last uploaded time** indicates when all data was successfully sent to the server. Each data type has its own **last collected time** and a specific collection interval.

9. To verify the log collection status, click on **Export**.



10. Swipe down the Notification panel to verify the reminder about the upcoming alarm.



11. Verify Proactive Device Monitoring and event alerts by observing the alert dialog workflows for severe device drop, frequent disconnections (WI-Fi or Bluetooth), unexpected reboots, and thermal anomalies.

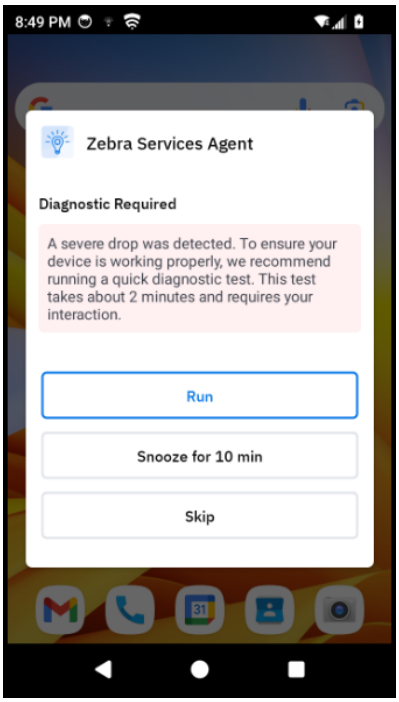
NOTE: The following behavior applies to all supported troubleshoot events, including:

- **Severe device drop**
- **Frequent Wi-Fi Disconnections**
- **Frequent Bluetooth Disconnections**
- **Frequent Device Reboots**

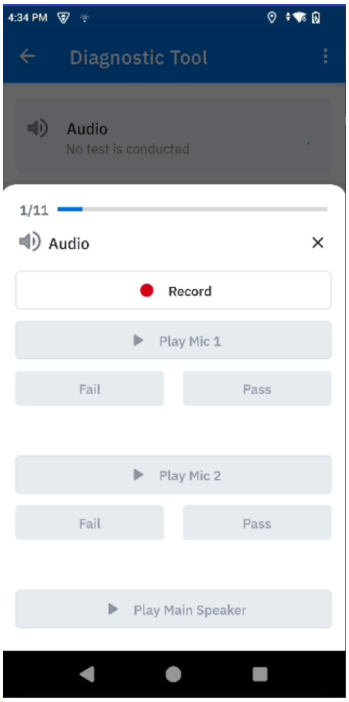
The following workflow uses the **Severe device drop** scenario as an example.

- **Alert on Severe Drop Detection**:

  The application receives a **Severe device drop** event from the **ZDS Application**. An alert dialog is displayed to inform the user and recommend running all DDT tests.

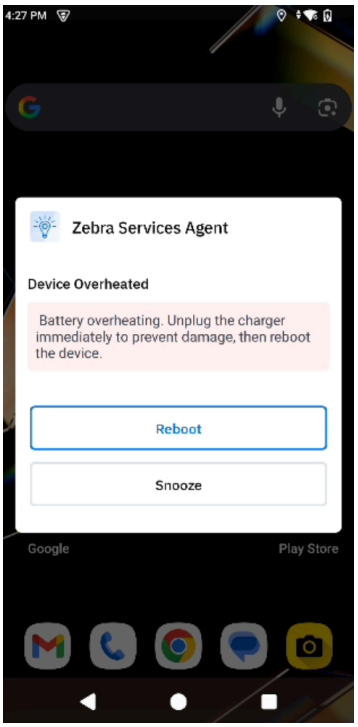


  - **Run**: Starts the DDT diagnostic process by executing all DDT tests sequentially.
  - **Snooze for 10 min**: Dismisses the alert dialog, and the prompt reappears after 10 minutes.
  - **Skip**: Skips the diagnostics and reports the skip action to the administrator.



- **Thermal anomalies**
  - **Alert on Device Overheat**:

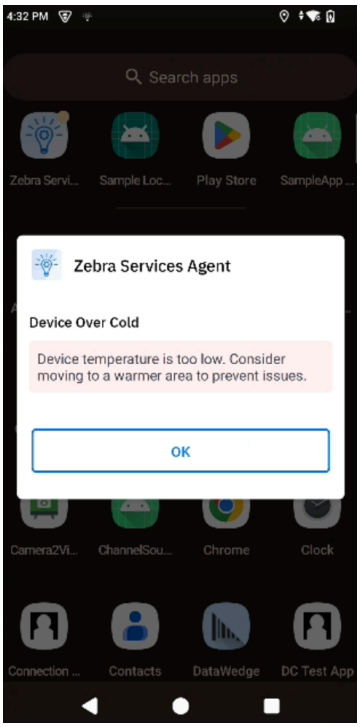
    ZSA receives the device overheat event from ZDS and displays the alert dialog to the user:



    - **Snooze**: Dismisses the alert dialog, and the prompt reappears after 5 minutes.
    - **Reboot**: Reboot the device.

- **Alert on Device Over-Cold**:

  ZSA receives the device over-cold event from ZDS and displays the alert dialog to the user:



  - **Ok**: Dismisses the alert.