Zebra Services Agent for 42Gears SureMDM

Installation Guide

MN-005029-05EN Rev A

ZEBRA

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

Copyright

2026/10/06

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

42Gears SureMDM 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

Devices must be enrolled as **Fully Managed Device** using the 42Gears MDM's Nix Agent Android application.

To verify if devices are configured as **Fully Managed Device**, log into the **42Gears SureMDM Console**, select the **Device**, and then click **Check Value of Android Enterprise** from the top-right corner.

ZSA Device Setup

Setting up the ZSA app on the device:

1. Download the APK file and add it to the MDM app store.
2. Create an installation job and configure the application.
3. Granting required permissions for the ZSA application on non-Zebra devices.
4. Assign all created jobs to the devices and verify the ZSA application on each device (Refer to the FAQs).
5. Allow the ZSA to read the serial number and assign that job to the devices.

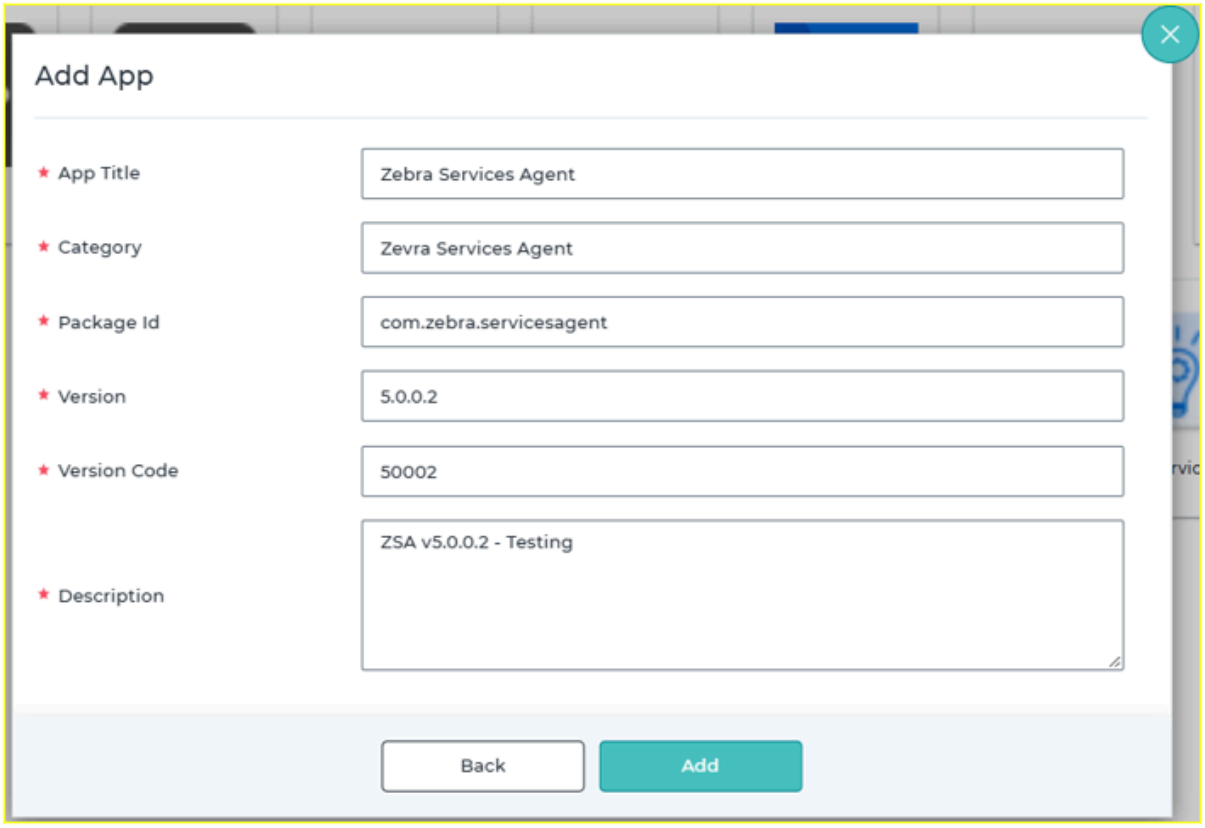
Deploying Zebra Services Agent

To add the Zebra Services Agent (ZSA) app to the MDM app store:

1. Download the `Zebra_Services_Agent_V5.0.0.x.apk` file from zebra.com/zebra-services-agent.
2. Go to **42Gears SureMDM Console** > **App Store** > **Android**.
3. Click **Add New App** and select **Upload APK**.
4. Click **Browse File** to upload the application.

   A security warning message is displayed.
5. Select the checkbox and click **OK** to proceed.

   After selecting the application, the **Add App** page displays.
6. Enter the **Category** and **Description** details, then click **Add**.

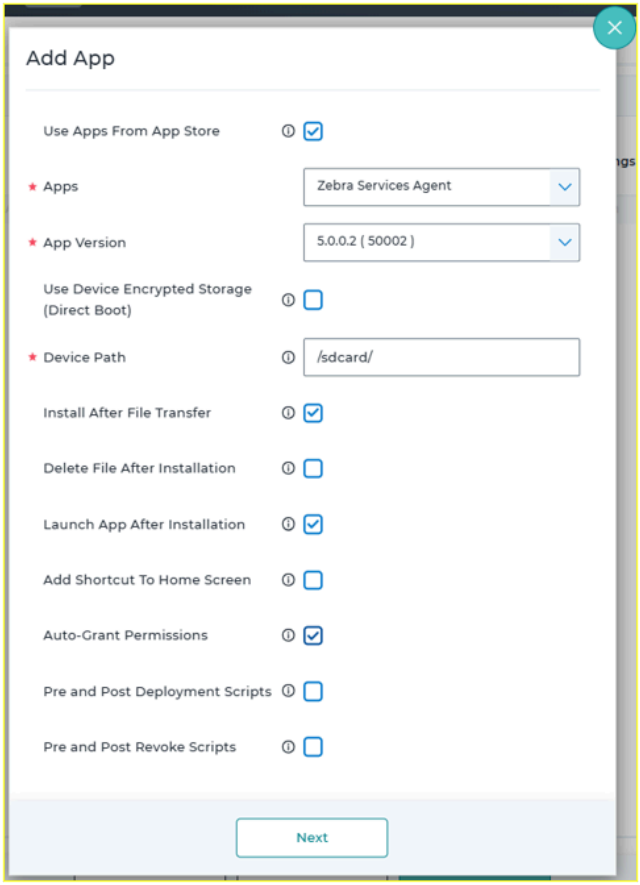


Installing Job Application for ZSA App with Managed Configuration Settings

Follow the steps below to add the ZSA app to the newly created job.

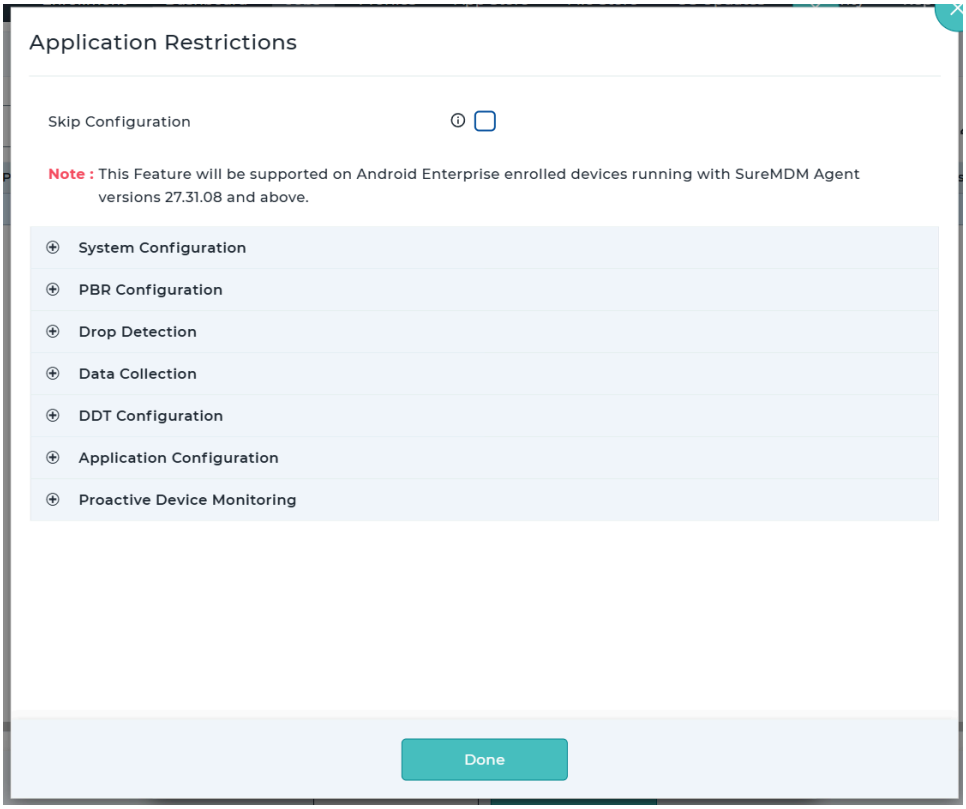
1. Go to **Jobs** > **New Job** > **Android**.
2. Select **Install Application Job**, enter a **Job Name**: `Install ZSA`, and click **Add APP**.

   The **Install Job** page displays.
3. Select the **Use Apps From App Store** checkbox.

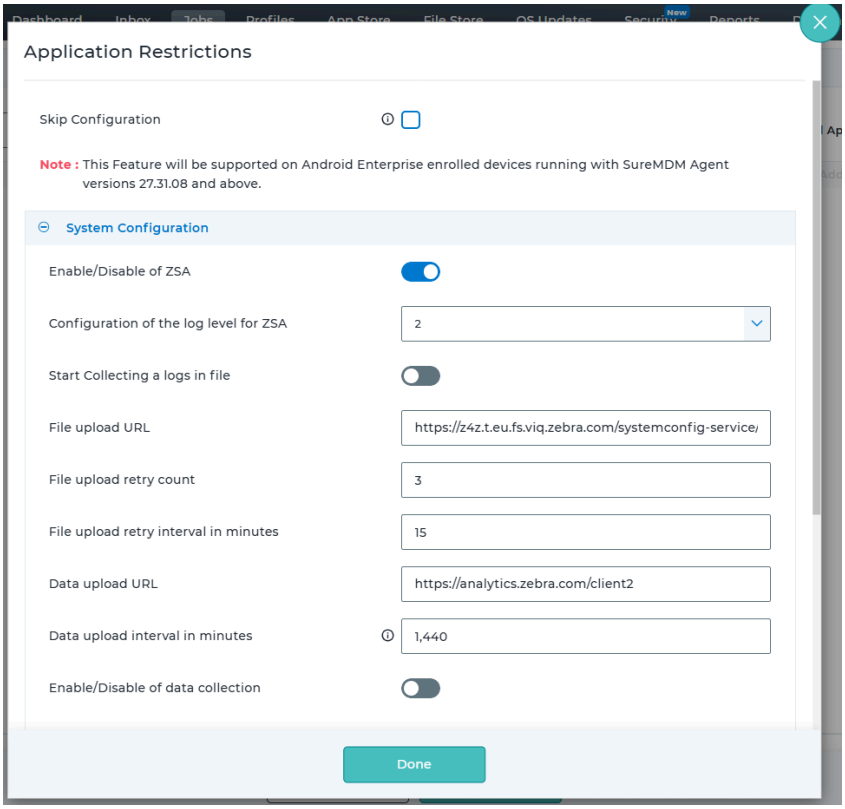


4. Select the application from the **Apps** drop-down menu.
5. Select the application version from the **App Version** drop-down menu.
6. Select the **Install After Copy** and **Launch App Upon Installation** checkboxes.
7. Select **Auto-Grant Permissions** checkbox.
8. Click **Next** to configure additional settings for ZSA and its modules.

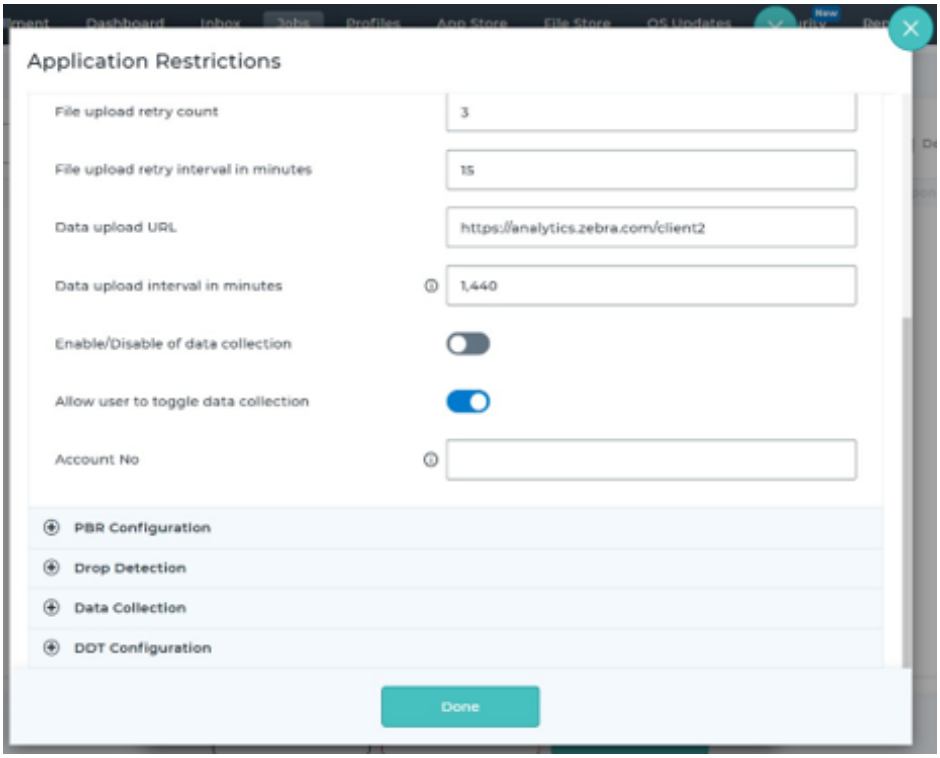
   The **Application Restrictions** page displays.
9. You can skip the configuration by selecting **Skip Configuration** or configure the required settings and click **Done**.



10. Go to **System Configuration**, enable the **ZSA Configuration** and **Start Collecting a logs in file** options and set the **Configuration of the log level for ZSA** with the following values:
    - 0: Info
    - 1: Debug
    - 2: Sensitive



11. 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.
12. 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 (or 1440 minutes).



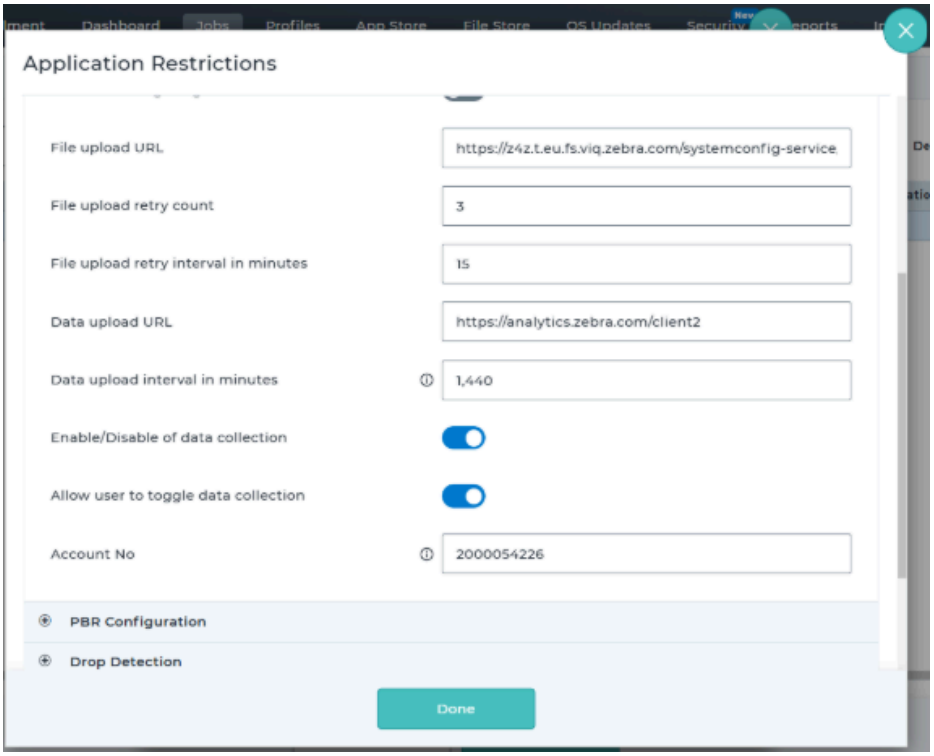
13. Data collection settings for non-Zebra devices:

    - **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.

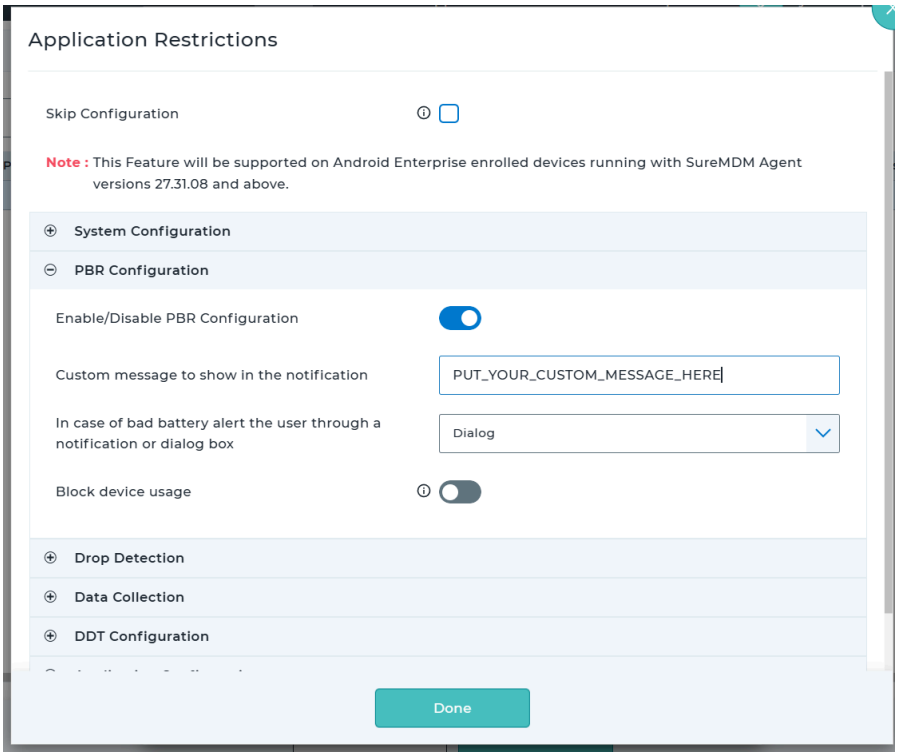
14. **Mandatory Setup for Non-Zebra Devices**

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

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



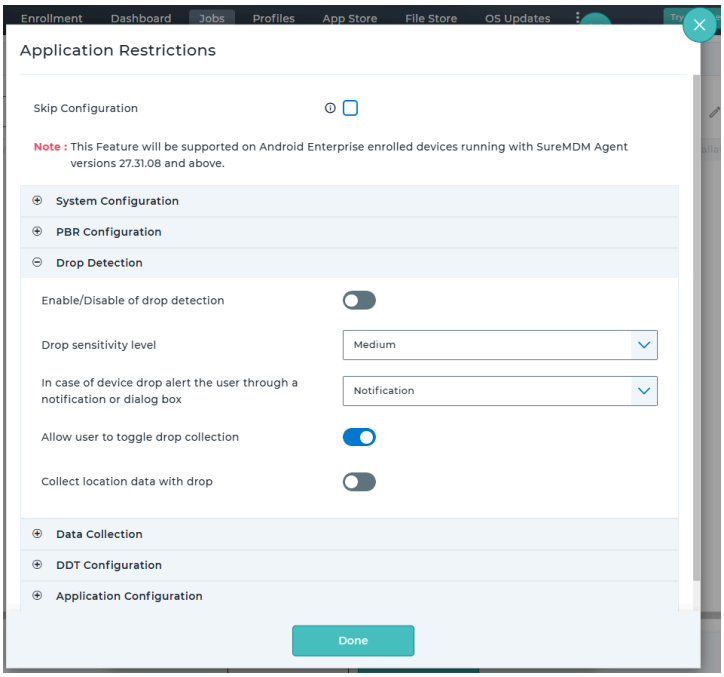
15. Go to **PBR Configuration**, enable the **Enable/Disable PBR Configuration** option, and provide a **Custom Message** as required.



16. 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 Dialog with Assist

17. The **Block device usage** option is disabled by default. If enabled by the administrator, it prevents device access when a bad battery is detected.
18. Go to **Drop Detection**, toggle the **Enable/Disable of drop detection** option as required.



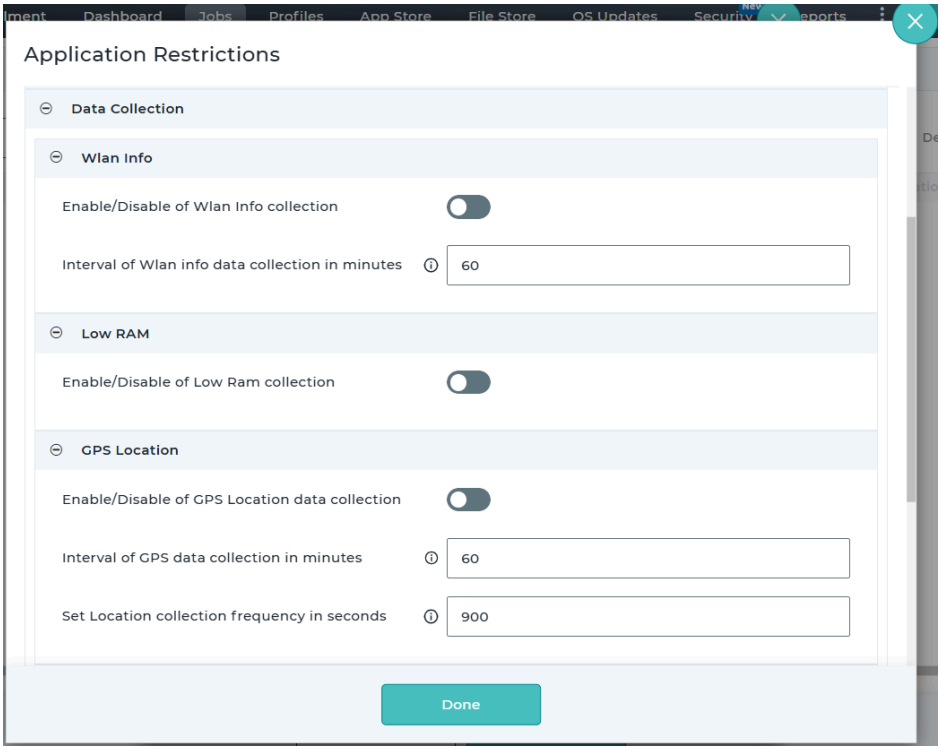
19. Set the **Drop sensitivity level** with the following values:
    - High
    - Medium (default)
    - Low
20. Set the **In case of device drop alert, the user should be alerted through a notification or dialog box** with the following values:
    - Notification (default)
    - Alert Dialog
    - Alert Dialog with Assist
21. 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.
22. The **Collect location data with drop** allows to capture location (lat-long) data of the device when device drop occurs.
23. Navigate to the **Data Collection** section. The settings for data collection on non-Zebra devices are as follows:

    Default enabled data collections:

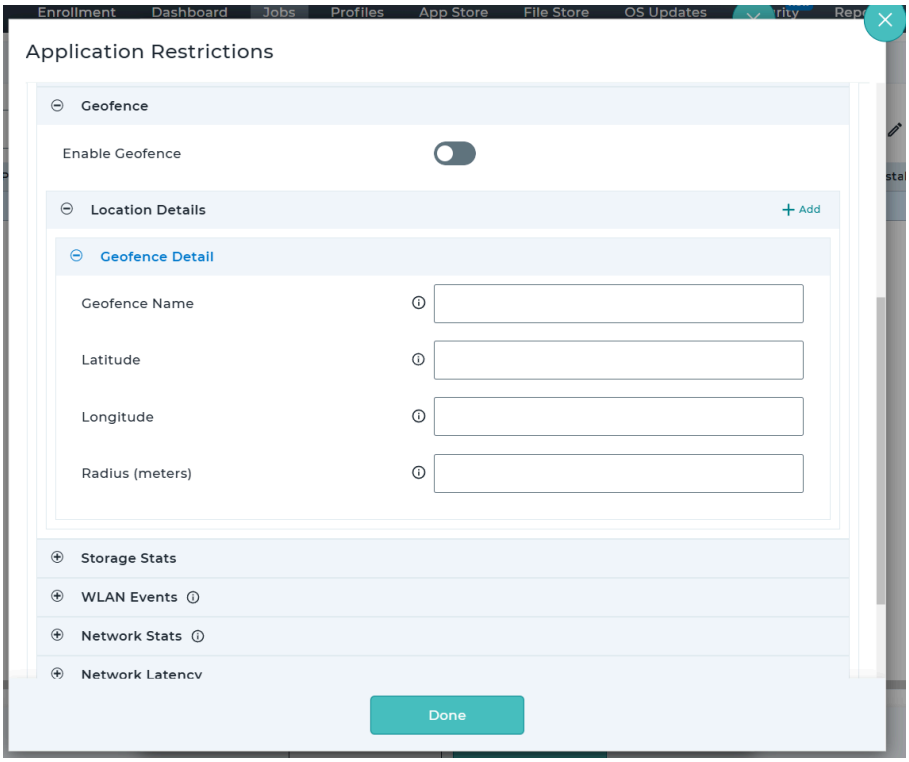
    - **Battery**
    - **Device Info**

- **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**

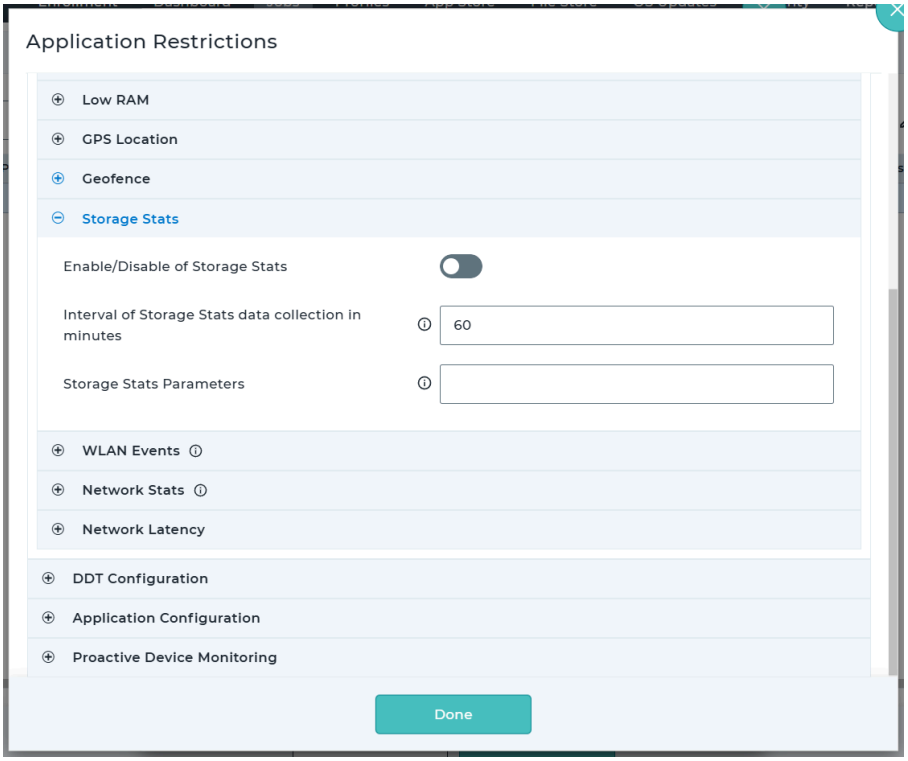
24. The Admin can modify the following data collections:
    - **WLAN Info**: Enable the **Enable/Disable of WLAN info collection** option and add value in **Interval of WLAN info data collection in minutes**.
    - **Low RAM**: Enable the **Enable/Disable of Low RAM collection** option.
    - **GPS Location**: Track the device by enabling the **Enable/Disable of GPS location data collection** option and set the **Interval of GPS data collection in minutes**.



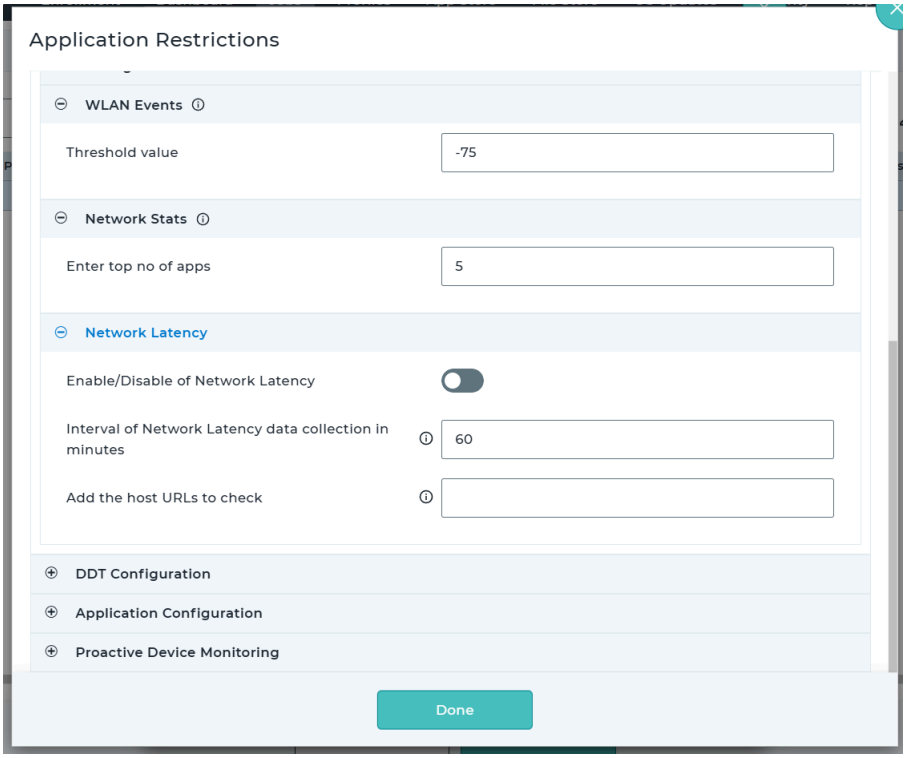
- **Geofence**: Receive notifications when the device leaves a predefined area by enabling **Enable Geofence** option and add **Location Details** information as follows:
  - **Geofence Name**: Name of the area.
  - **Latitude & Longitude**: Coordinates of the specific area.
  - **Radius (meters)**: The radius in meters to cover around the specified latitude and longitude.



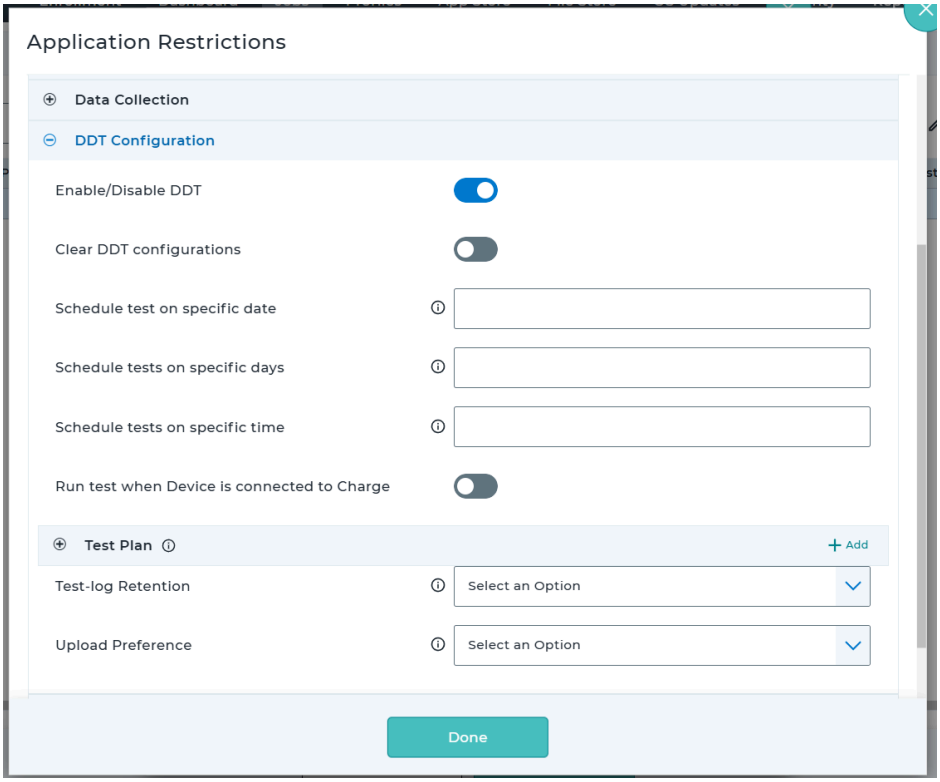
- **Storage Stats**: Enable the **Enable/Disable of Storage Stats** option and add value in **Interval of Storage Stats data collection in minutes.**
  - **Storage Stats Parameters**: Configure the package names for monitoring.



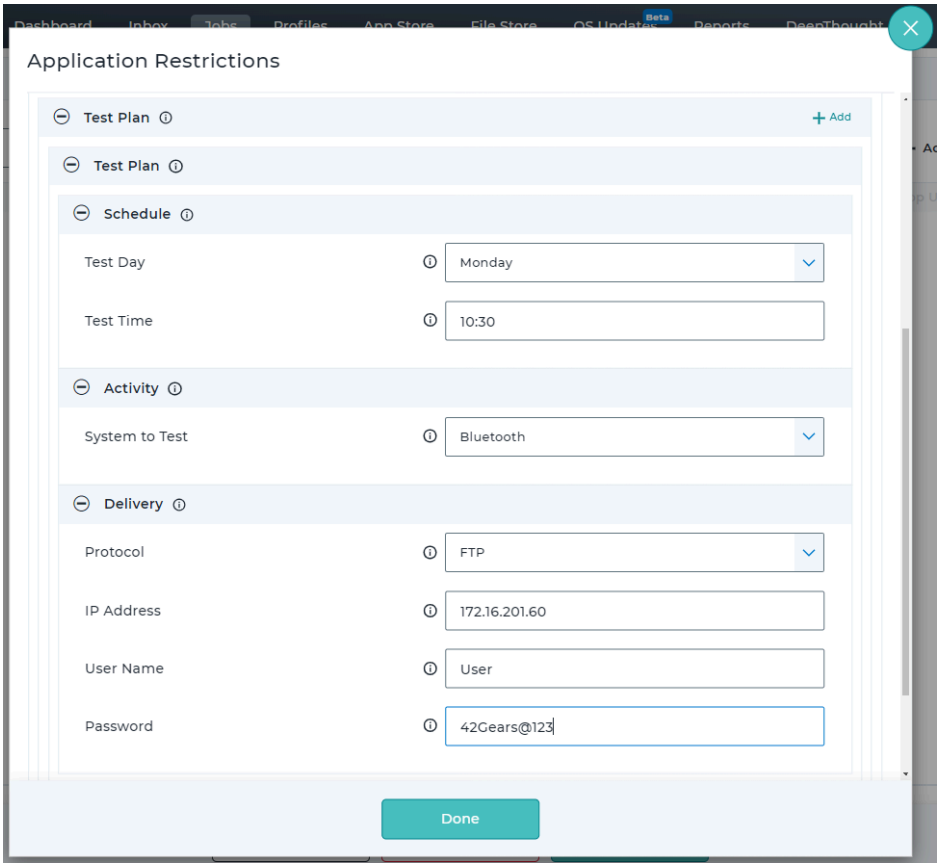
- **WLAN Events**: Enabled by default and cannot be disabled. The admin can adjust the threshold value (in Minutes).
  - **WLAN** event data is collected based on the configured threshold value.
- **Network Stats**: Enabled by default and cannot be disabled. The admin can adjust the top no of app counts.
- **Network Latency**: Disabled by default, if enabled record network performance details for configured host URLs, including the target host, measured latency, network type, signal strength, connection information, and request result stats as error message.



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

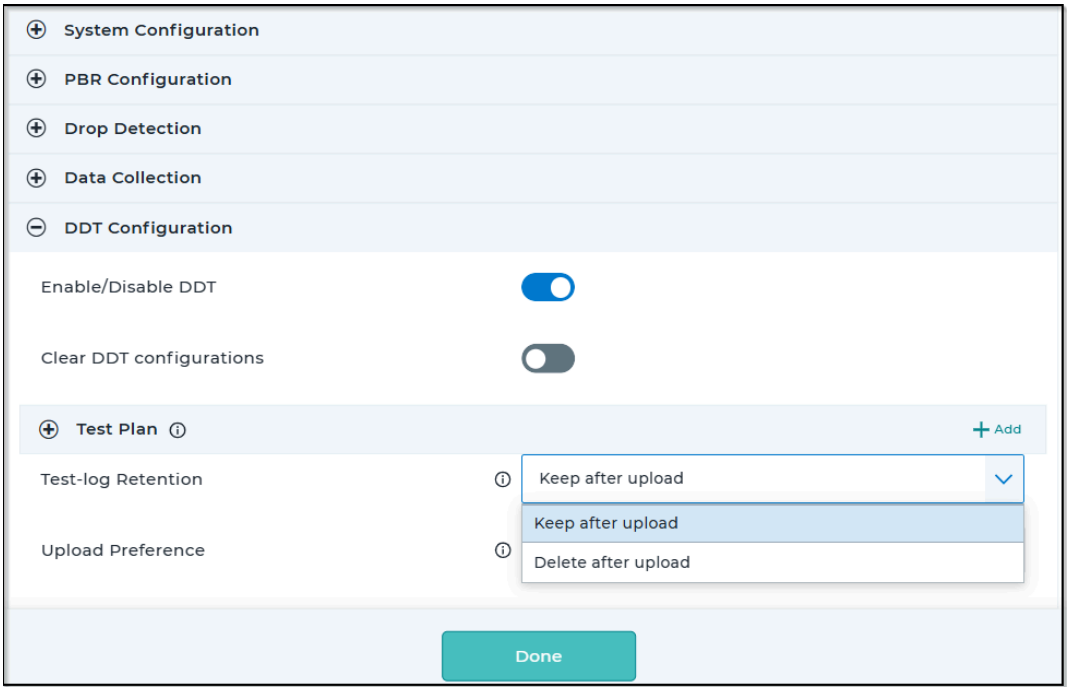


26. Under the **Schedule** section, configure the test plan with the following values:

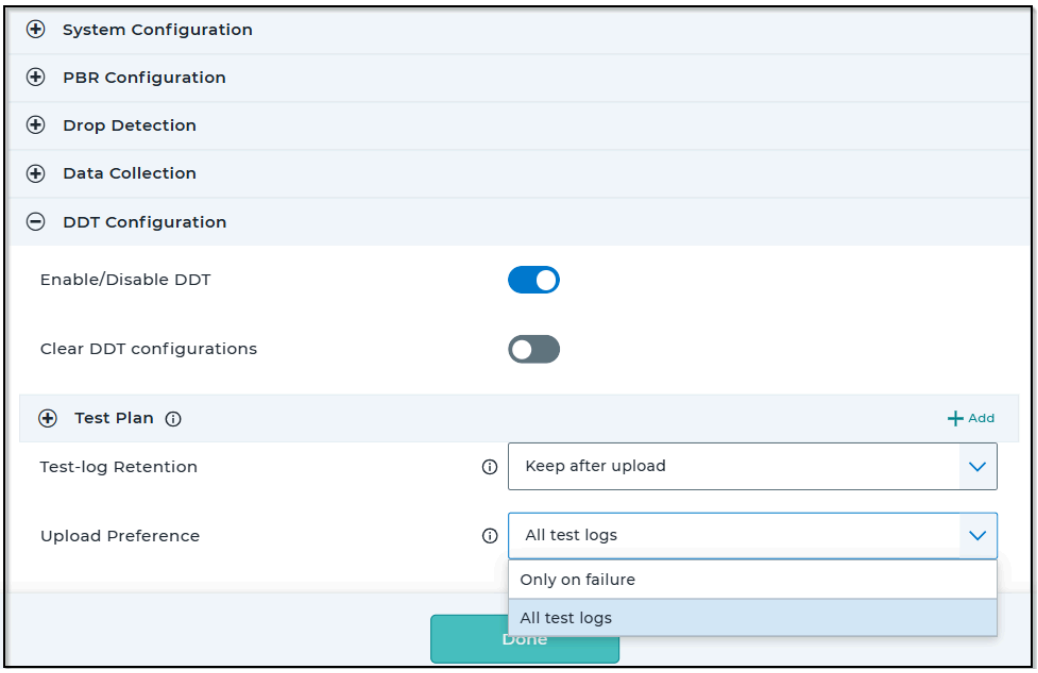


- **Test Day**: Day of the Week (For example, Monday)
- **Test Time**: Time of the day for the test (HH: MM format)
- **System to Test**: Select the test to schedule (For example, Bluetooth)

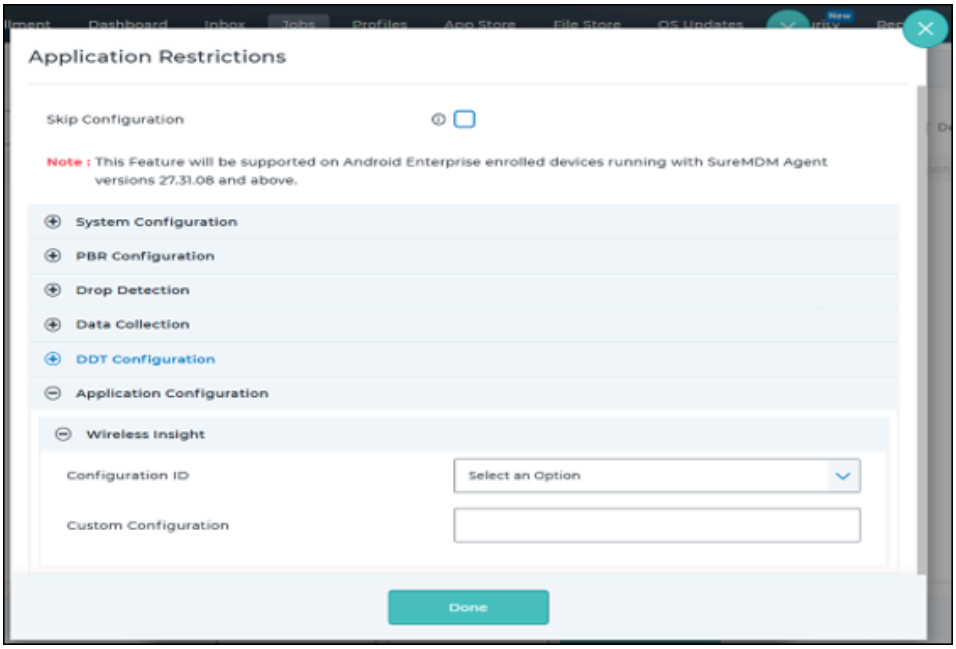
27. Under the **Delivery** section, select the **Protocol** as **FTP**, enter a valid **IP Address**, **User Name**, and **Password**.
28. Select the **Test-log Retention** as required.



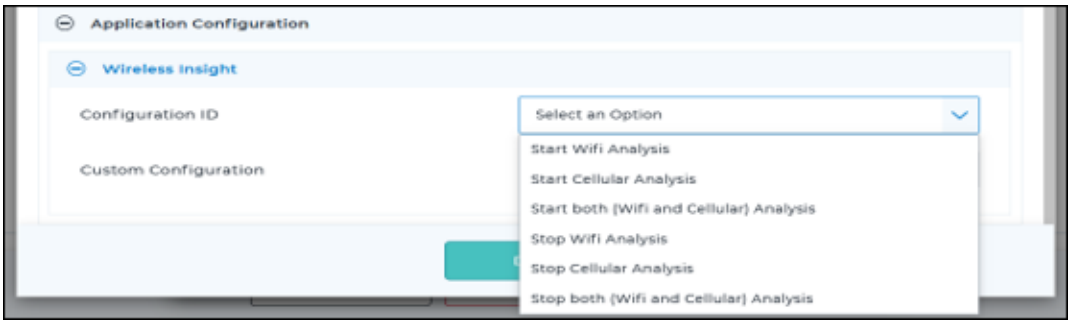
29. Select the **Upload Preference** as required.



30. 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.



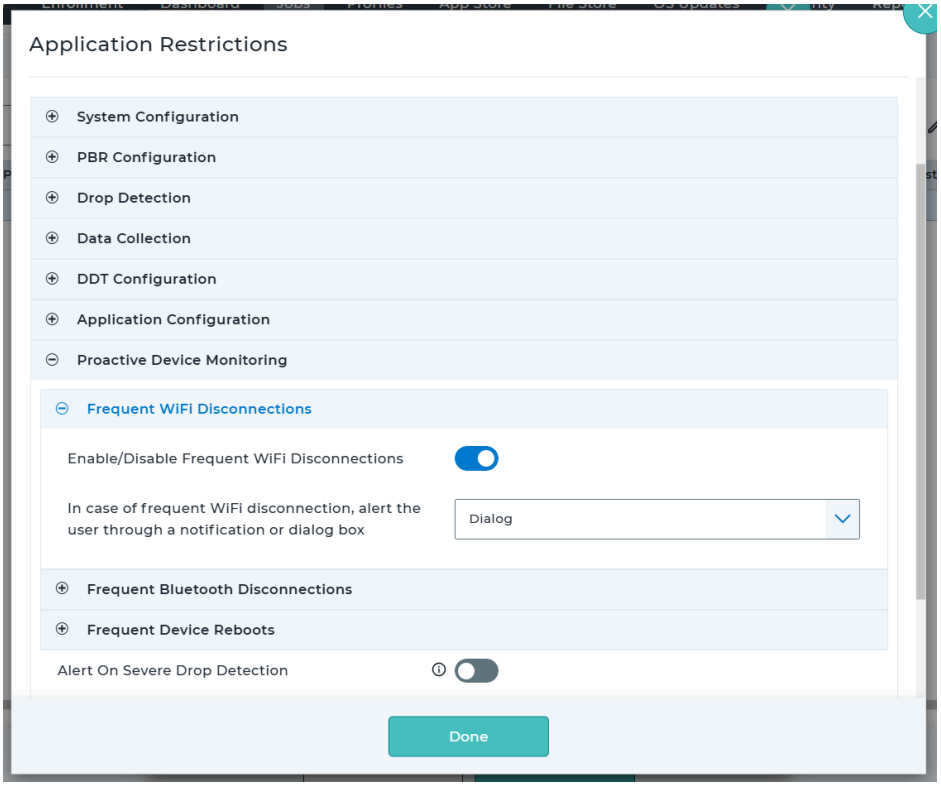
  - **Custom Configuration**: Add the custom Wireless Insight configuration as a value.
- **ZDS**: Configured through VIQ with a custom ZDS configuration.

31. Under the **Proactive Device Monitoring** sections, enable the following options:

    a. **Frequent Wi-Fi Disconnections**

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

    - Notification
    - Dialog (default)



b. 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 values:

- Notification
- Dialog (default)

c. 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 values:

- Notification
- Dialog (default)

d. Alert on Severe Drop Detection

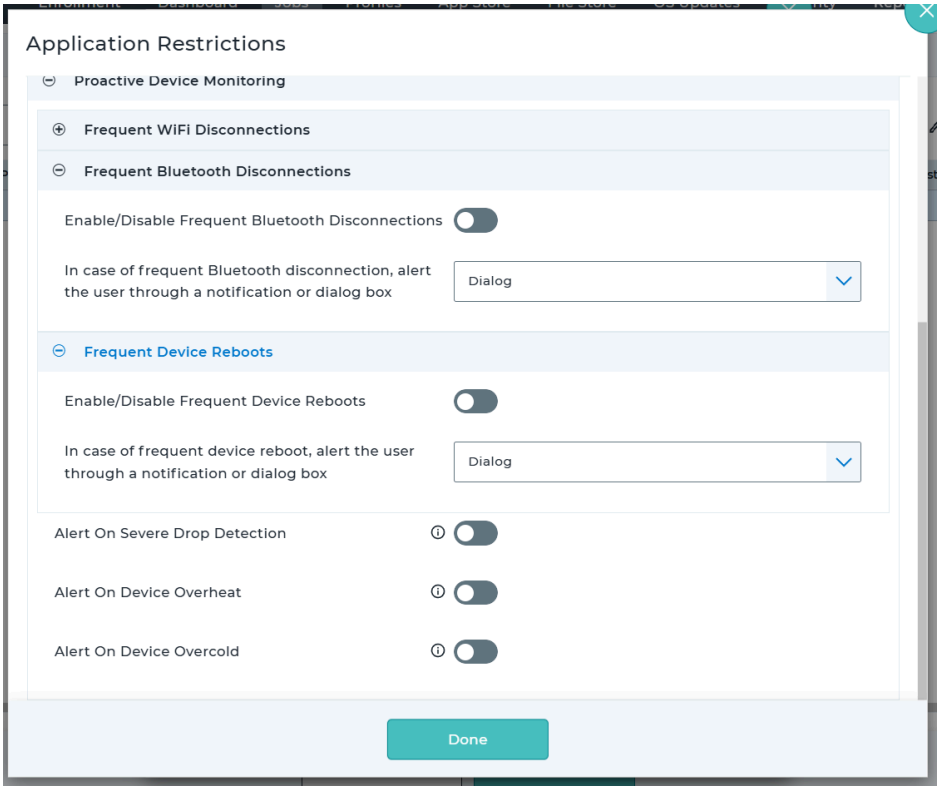
Disabled by default. When enabled by an administrator, this feature allows the device to receive commands from ZDS upon detecting a severe drop.

e. Alert on Device Overheat

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

f. Alert on Device Over cold

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



32. Click **Done**.

NOTE: The newly created job displays in the **Jobs List** section.

Granting Required Permission for the ZSA Application for non-Zebra Devices

To grant all the required permissions to the ZSA application:

1. Granting notification permission.
   a. Navigate to **Jobs** > **New Job** > **Android** > **Run Script**.
   b. Add a **Job Name**: ZSA `Notification Permission` and enter the following script:

```
!#suremdm
```

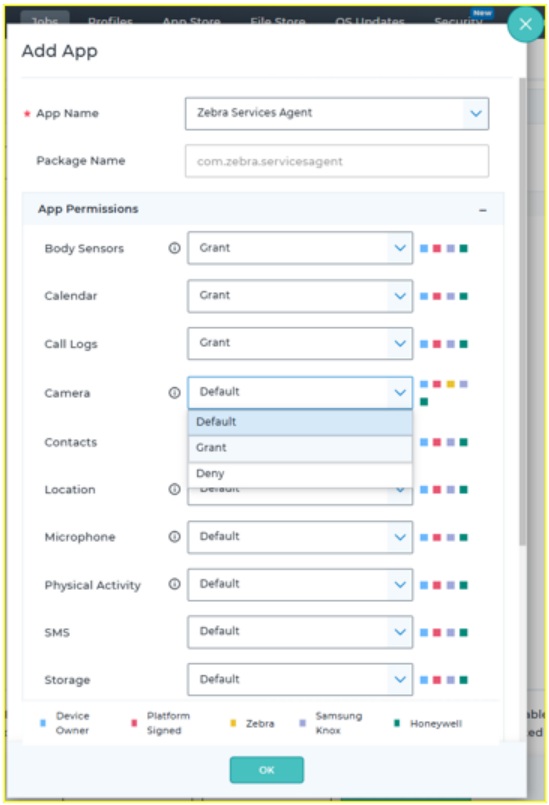
```
grantRuntimePermission(com.zebra.servicesagent,
android.permission.POST_NOTIFICATION)
```



c. Click **Save**.

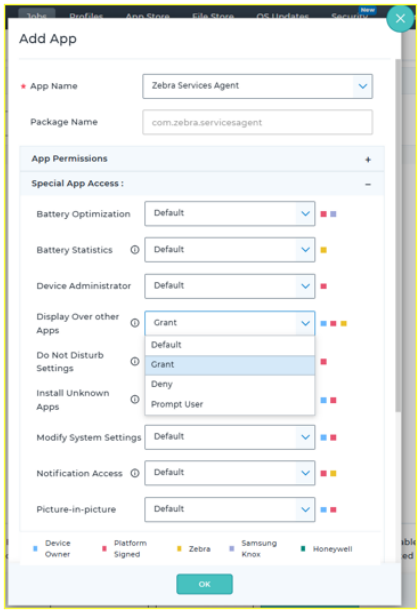
NOTE: The newly created job displays in the **Jobs List** section.

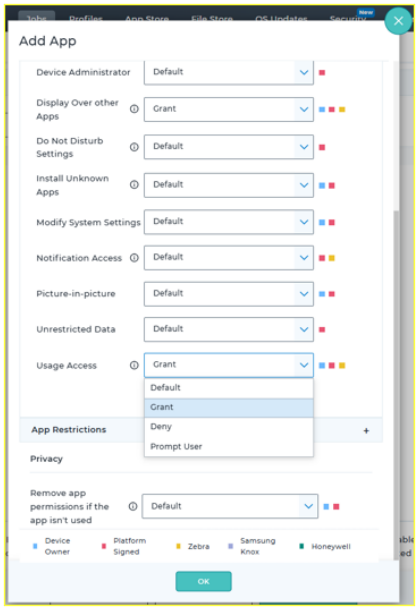
2. Granting runtime permissions and special permissions.
   a. Navigate to **Jobs** > **New Job** > **Android** > **Application Permission**.
   b. From the dialog box, add a **Job Name**: ZSA `Permissions` and click **+Add**.



c. The **Add App** page displays. Select the ZSA App from the **App Name** drop-down list and grant all permissions from the **App Permission** list.

d. Under the **App Permissions**, click **Special App Access** and grant all permissions specifically **Display Over Other Apps** and **Usage Access**.





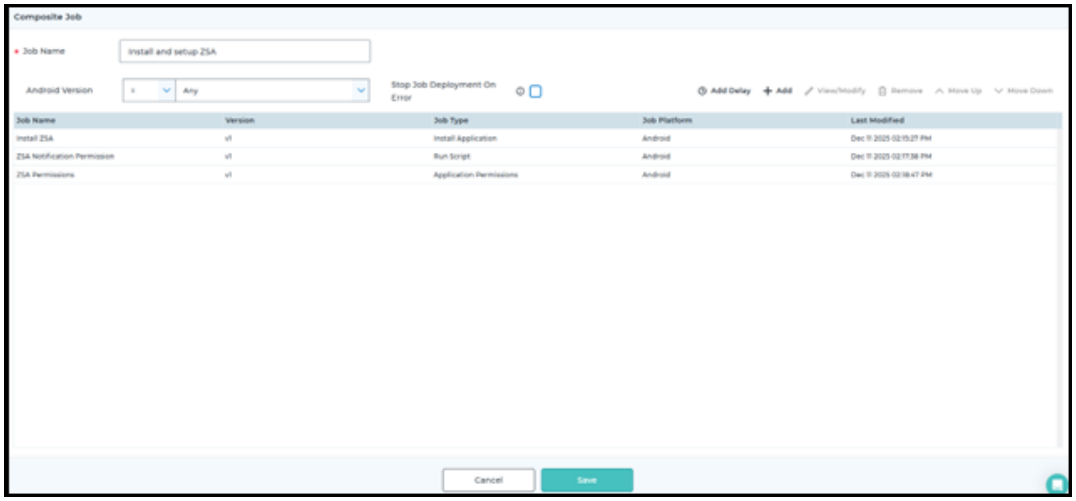
e. Click **OK**, confirm the action, and save the job.

NOTE: The newly created job displays in the **Jobs List** section.

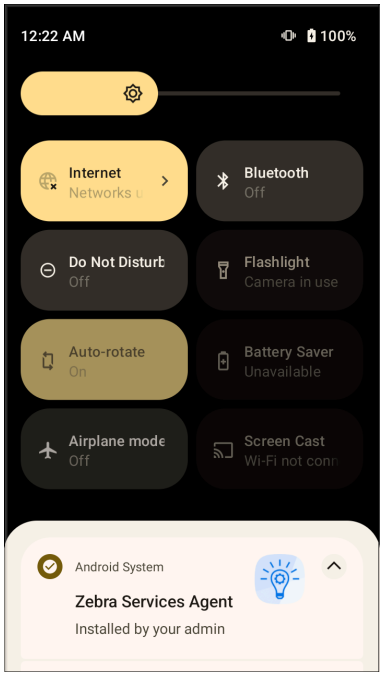
Creating a Composite Job for ZSA App Installation

After creating the jobs, combine them into a single job by following these steps:

1. Navigate to **Jobs** > **New Job** > **Android** > **Composite Job**.
2. Enter the **Job Name**: `Install and Setup ZSA`.
3. Click **Add** and include all the created jobs.



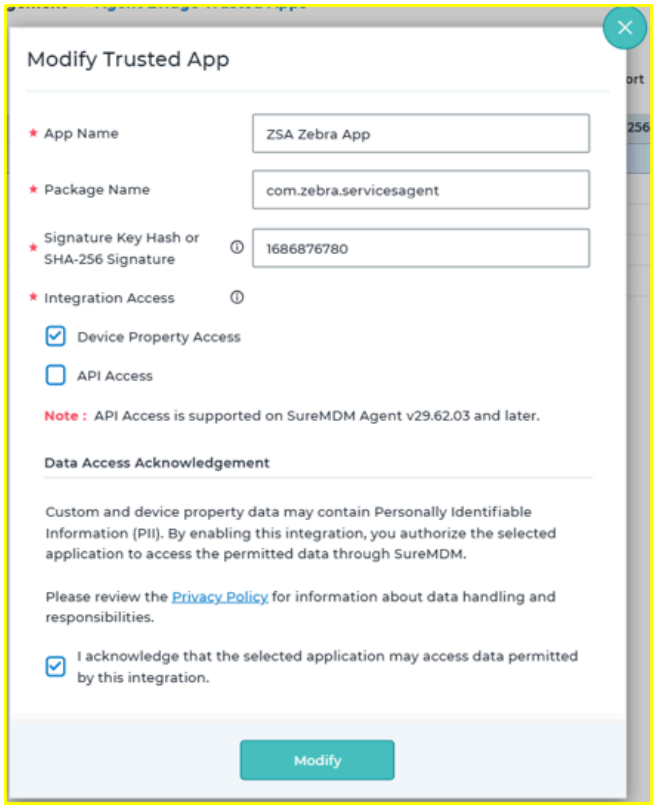
4. Click **Save**.
5. Go to **Home**, select **All Devices**, and then click **Apply Job** and select **Install and Setup ZSA**.



Allowing the ZSA Application to Read Device Serial Number

To enable the ZSA application in your 42Gears SureMDM account:

1. Go to **MDM Account Settings** > **Android Management**.
2. Select **Agent Bridge Trusted Apps**.
3. Click **+ Add** and enter the ZSA details in the dialog box.
4. To add ZSA to the allowed list for accessing device properties:



a. Enter **ZSA App** as the **App Name**.

b. Enter **com.zebra.servicesagent** as the **Package Name**.

c. Obtain the **Security Key** by navigating to **Home** > **Select Device** > **Apps** > **Zebra Service Agent** > **Signature Key Hash**. Copy and paste the **Signature Key Hash** value in the **Security Key Hash**.

d. Accept the **Privacy Policy** by checking the **I Agree** checkbox.

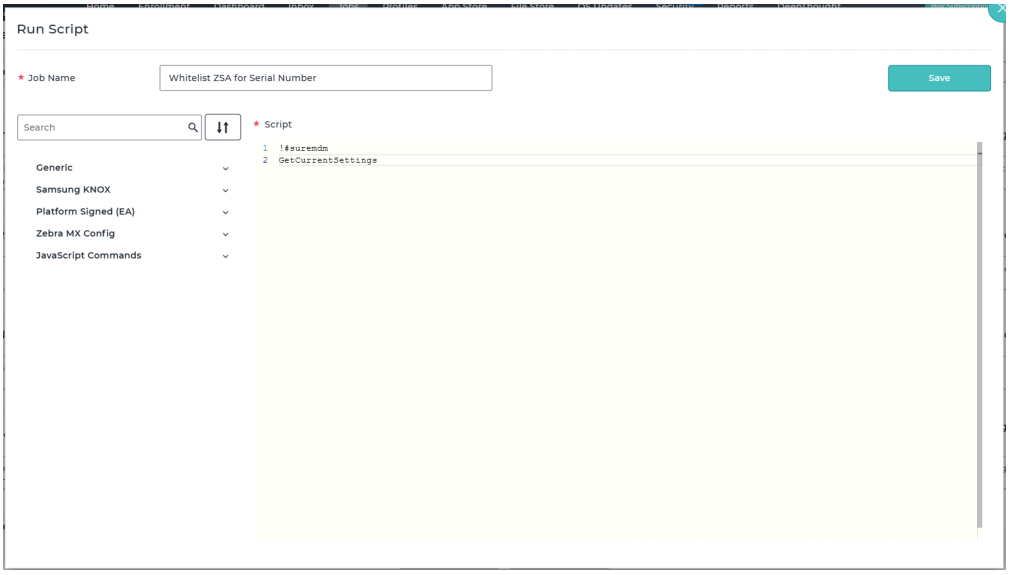
e. Click **Modify** to add the application to the allowed list.

5. To refresh the device properties in MDM, go to **Jobs** > **New Job** > **Android** > **Run Script**.

   a. Add a **Job Name**: `Whitelist ZSA for Serial Number` and enter the following script:

```
!#suremdm
```

```
GetCurrentSettings
```



b. Click **Save**.

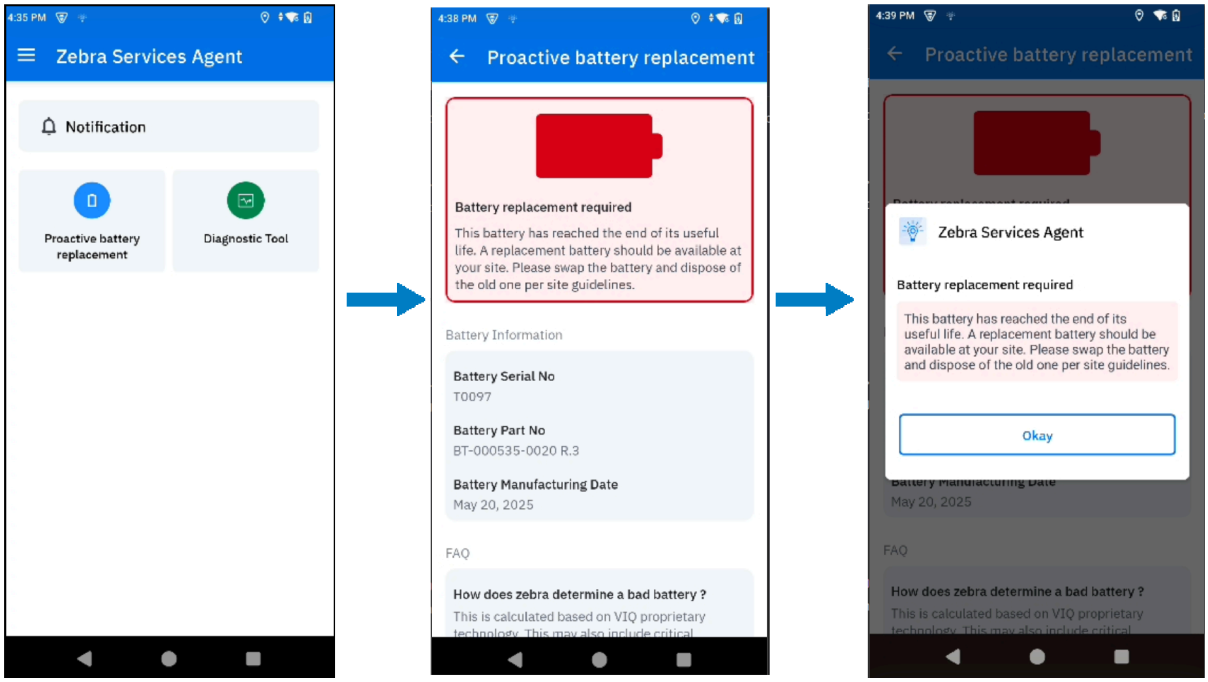
NOTE: The newly created job displays in the **Jobs List** section.

6. Navigate to **Home**, select **All Devices**, then click **Apply**. Select **Whitelist ZSA for Serial Number** and click **Apply**.

Expected Behaviour After Auto-launching Zebra Services Agent

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

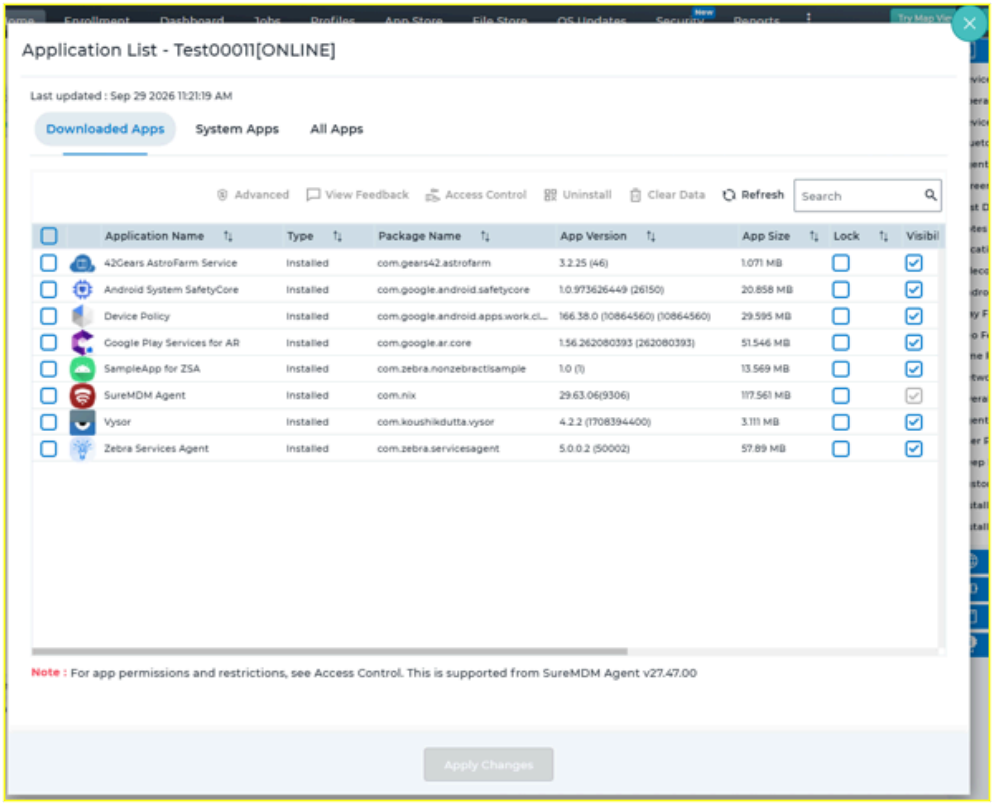
1. Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
2. If the Proactive Battery Health (PBR) module is entitled, the ZSA app automatically launches it after a few seconds.
3. The PBR screen displays both good and bad battery details, and if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



FAQs

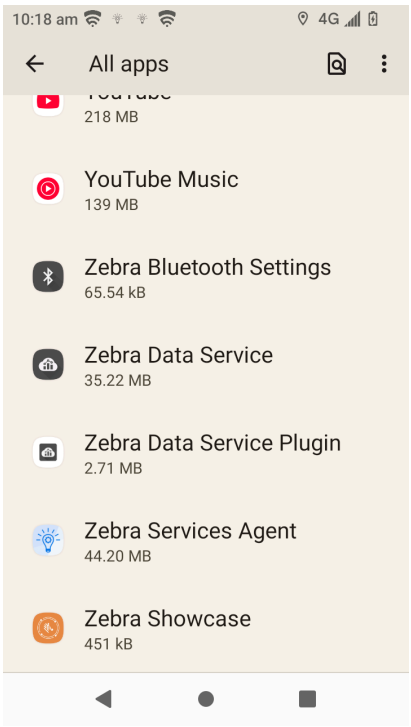
1. How do you determine which apps are installed on the devices in 42Gears?
   a. Go to **Home** > **Device List**.
   b. Select any device mentioned in the list.

      The **Application List** page displays.
   c. Click the **Downloaded Apps** tab, then scroll down or use the **Search** feature to find the ZSA app.

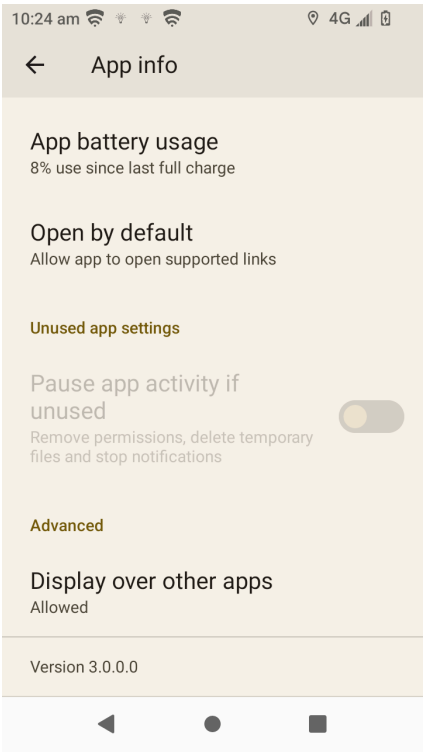


2. How do you verify if the app is installed with the correct permissions and is able to connect to Zebra servers?

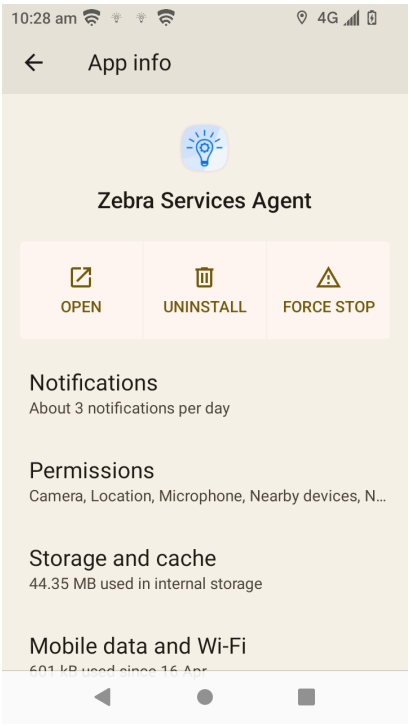
   a. To verify the app version, go to **Settings** > **Apps** > **All apps** and select **Zebra Services Agent**.



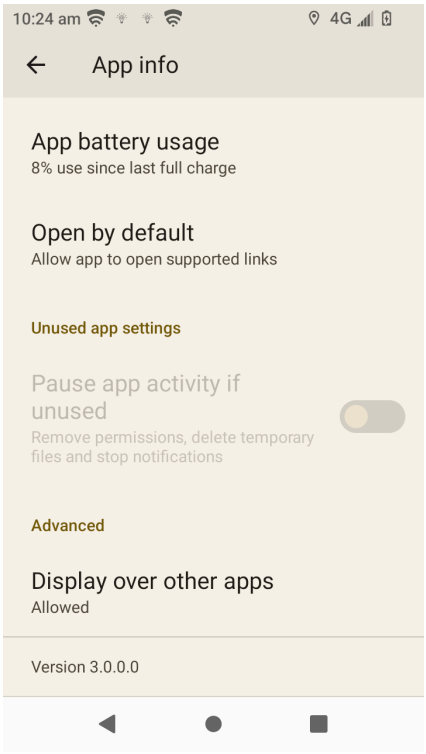
b. The **App Info** page displays the **Version**.



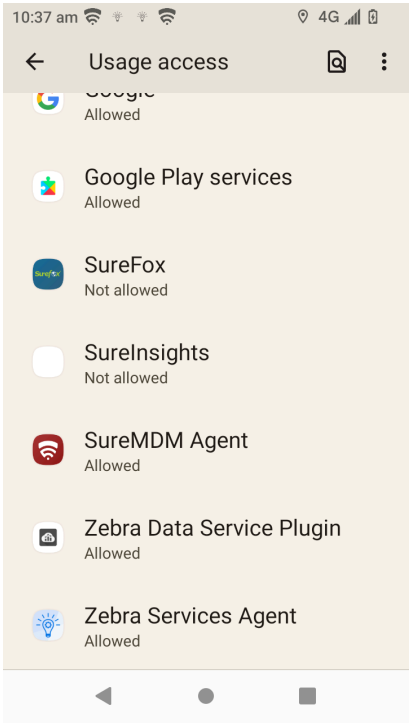
c. To verify the ZSA Permissions, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Permissions**.



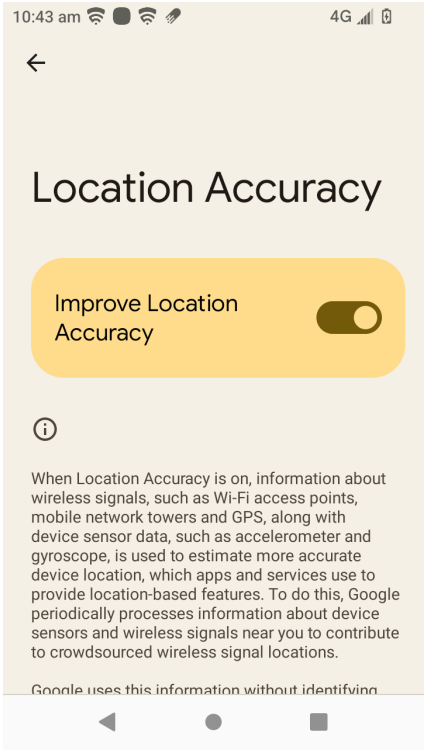
d. To verify the Display over other apps permission, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Advanced** > **Display over other apps**.



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

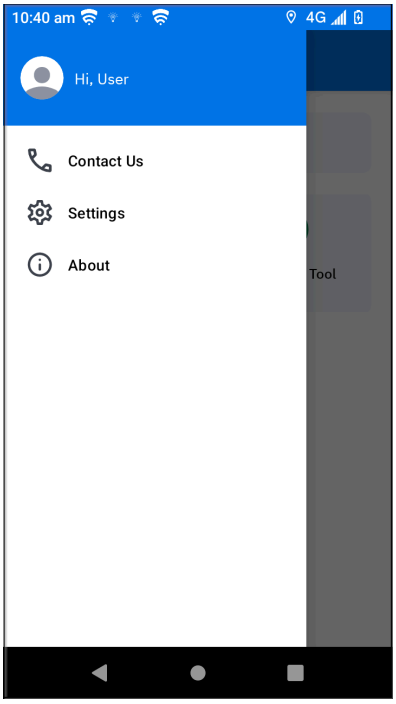


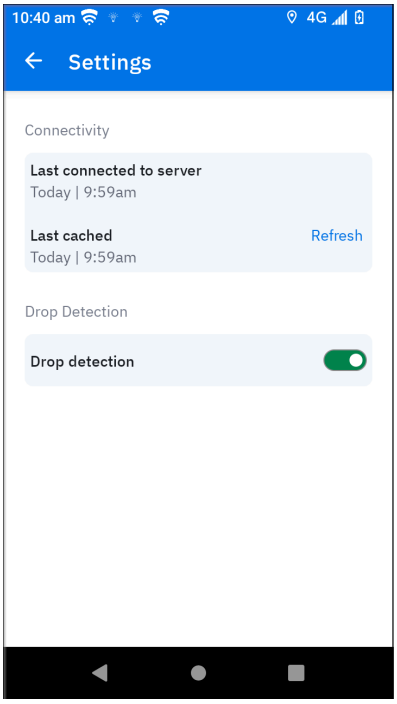
f. For the **Device action** > **Outdoor Location Tracking** feature, ensure that location accuracy is enabled on the device for precise location information. Navigate to **Settings** > **Location** > **Location Services** > **Location Accuracy**.



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

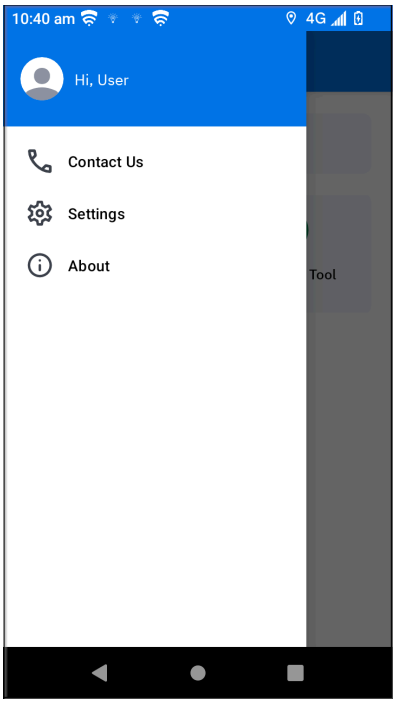
Launch ZSA and go to **Settings** > **Refresh**.

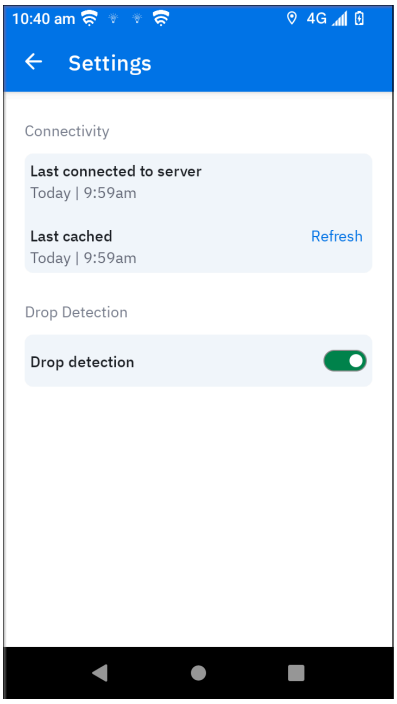




h. To verify the Drop Detection status:

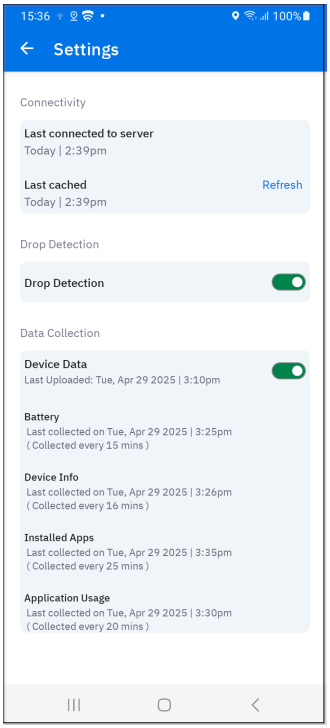
Launch ZSA and go to **Settings**. Enable **Drop detection**. The user can enable or disable drop detection if the administrator provides toggle access.





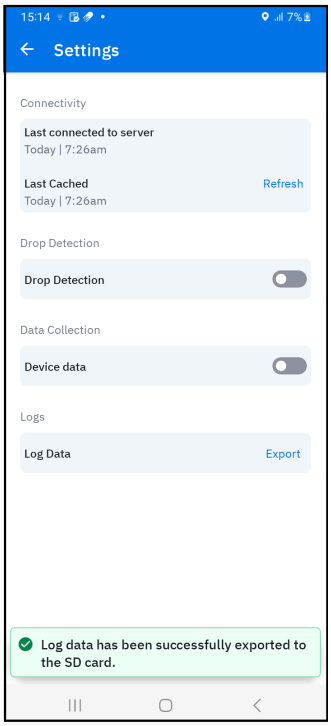
i. To verify Data collection in a non-Zebra device:

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

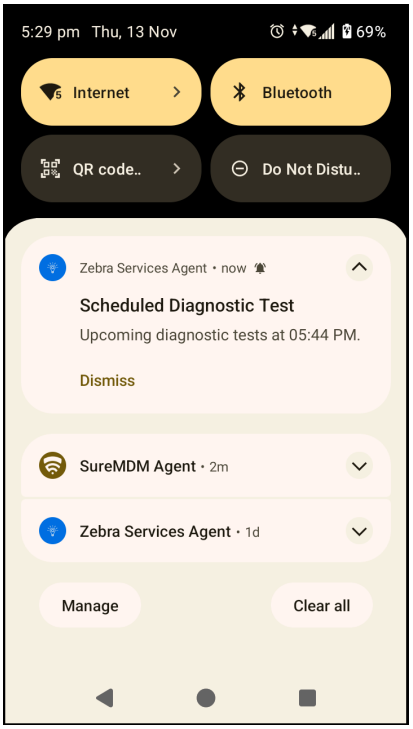


In data collection, the **last uploaded time** indicates when all data was successfully sent to the server. Each data type has its own **last collected time** and a specific collection interval.

j. To verify the **Log Data** collection status, click **Export**.



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



l. **Proactive Device Monitoring**

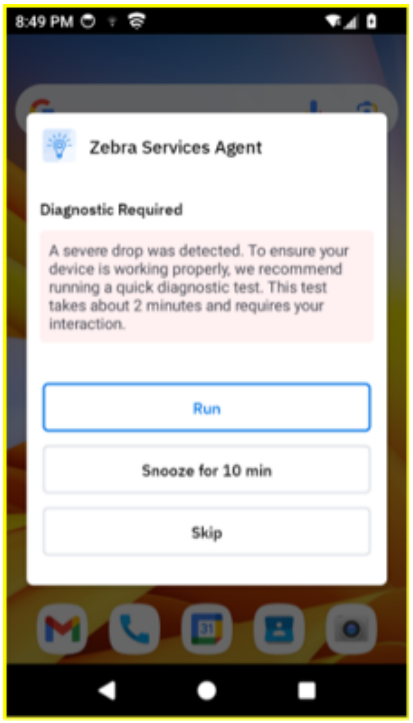
Verify Proactive Device Monitoring and event alerts by observing the alert dialog workflows for Severe device drop, Frequent network disconnections (Wi-Fi/Bluetooth), unexpected reboots, and thermal anomalies:

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

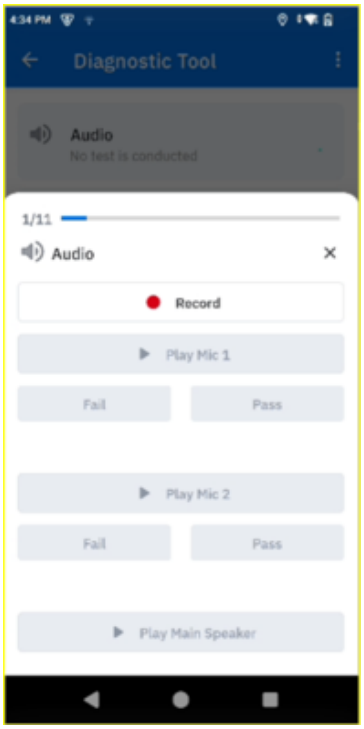
- Severe device drop
- Frequent Wi-Fi Disconnections
- Frequent Bluetooth Disconnections
- Frequent Device Reboots

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

The Application monitors **Severe device drop** events from **ZDS Application**; an alert dialog is shown to inform the User and recommend running all the DDT tests



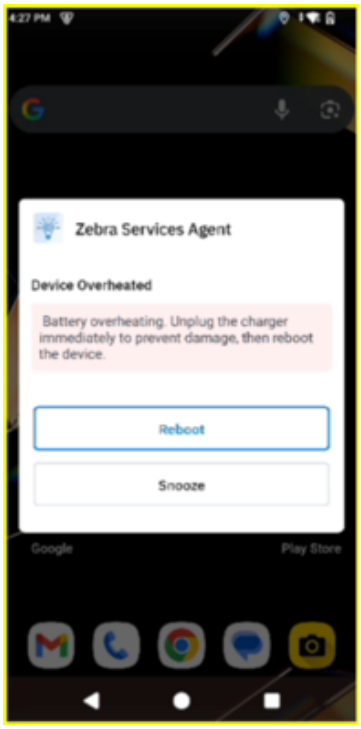
- **Run** – Starts the DDT diagnostic process by executing all DDT tests sequentially.
- **Snooze for 10 min** – Dismisses the alert dialog and the prompt will appear again after 10 minutes.
- **Skip** – Skips the diagnostics and reports to the admin about the skip action.



- **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 will appear again 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** – Dismiss the alert.

