Zebra Services Agent for 42Gears SureMDM

Installation Guide

ZEBRA

MN-005029-03EN Rev A

Copyright

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

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.

Deploying Zebra Services Agent

Install the Zebra Services Agent (ZSA) app on the devices.

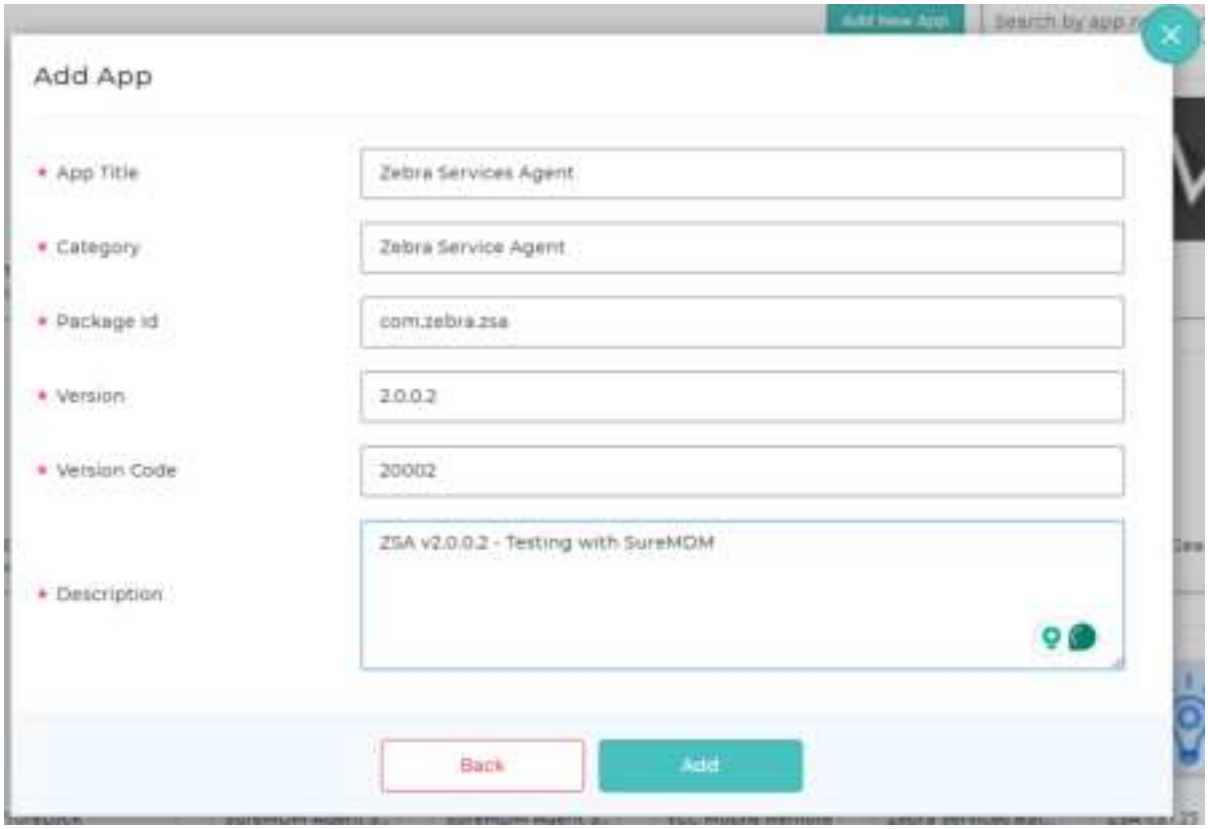
Download the `Zebra_Services_Agent_V3.0.0.5.apk` file from zebra.com/zebra-services-agent.

1. Go to **42Gears SureMDM Console** > **App Store** > **Android**.
2. Click **Add New App** and select **Upload APK**.
3. Click **Browse File** to upload the application.

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

   After selecting the application, the **Add App** page displays.

5. Enter the **Category** and **Description** details, then click **Add**.



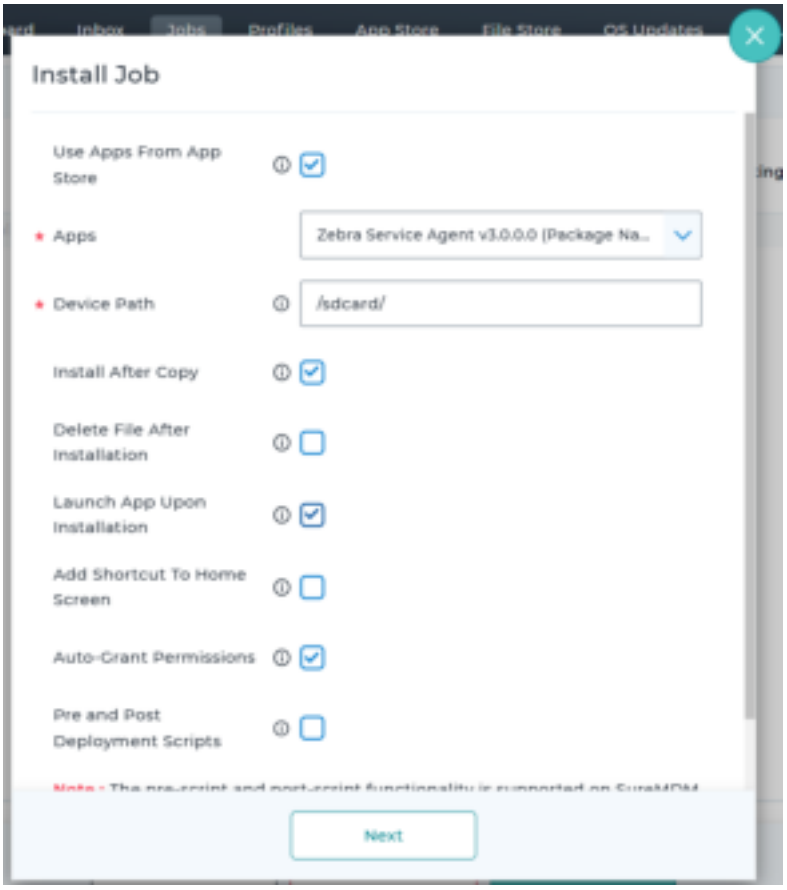
Installing Job Application for ZSA App with Managed Configuration Settings

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**, and click **Add**.

   The **Install Job** page displays.

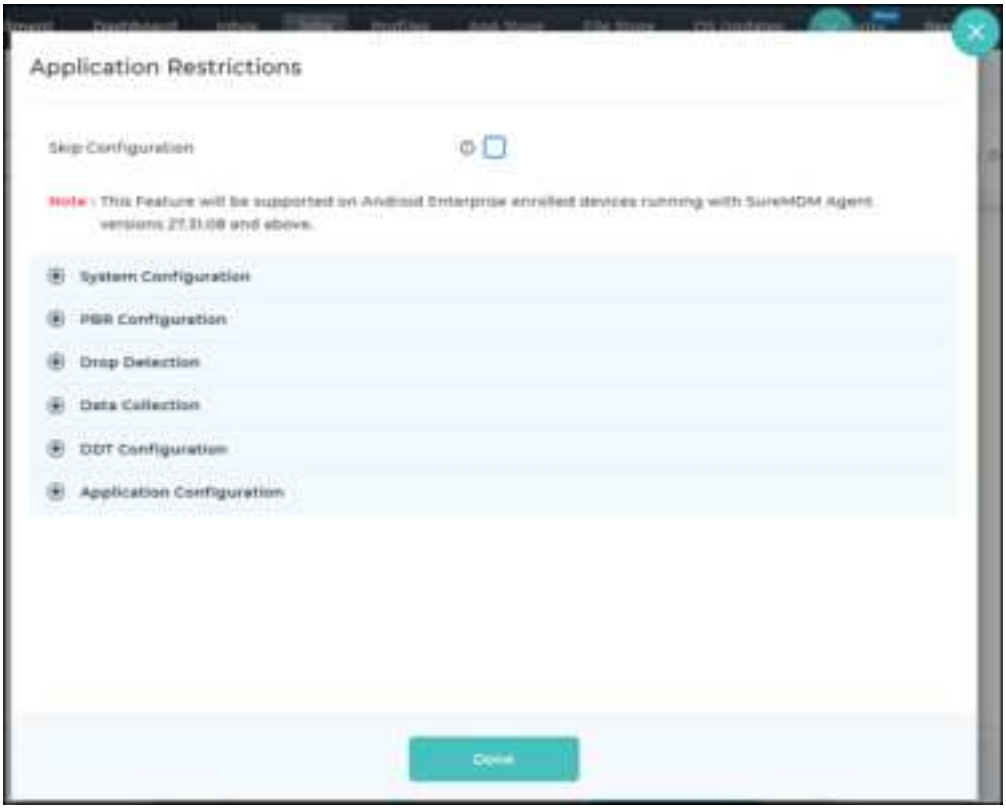
3. Select the **Use Apps From AppStore** checkbox.



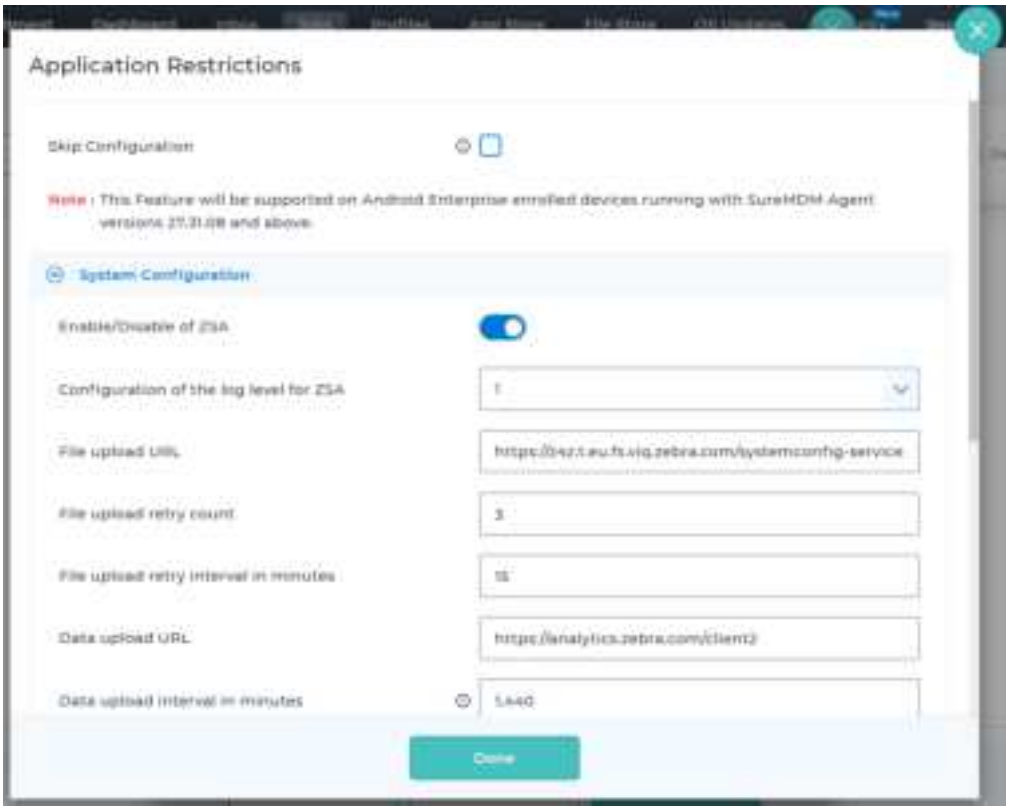
4. Select the application from the **Apps** drop-down menu.
5. Select the **Install After Copy** and **Launch App Upon Installation** checkboxes.
6. Click **Next** to configure additional settings for ZSA and its modules.

   The **Application Restrictions** page displays.

7. You can skip the configuration by selecting **Skip Configuration** or configure the required settings and click **Done**.



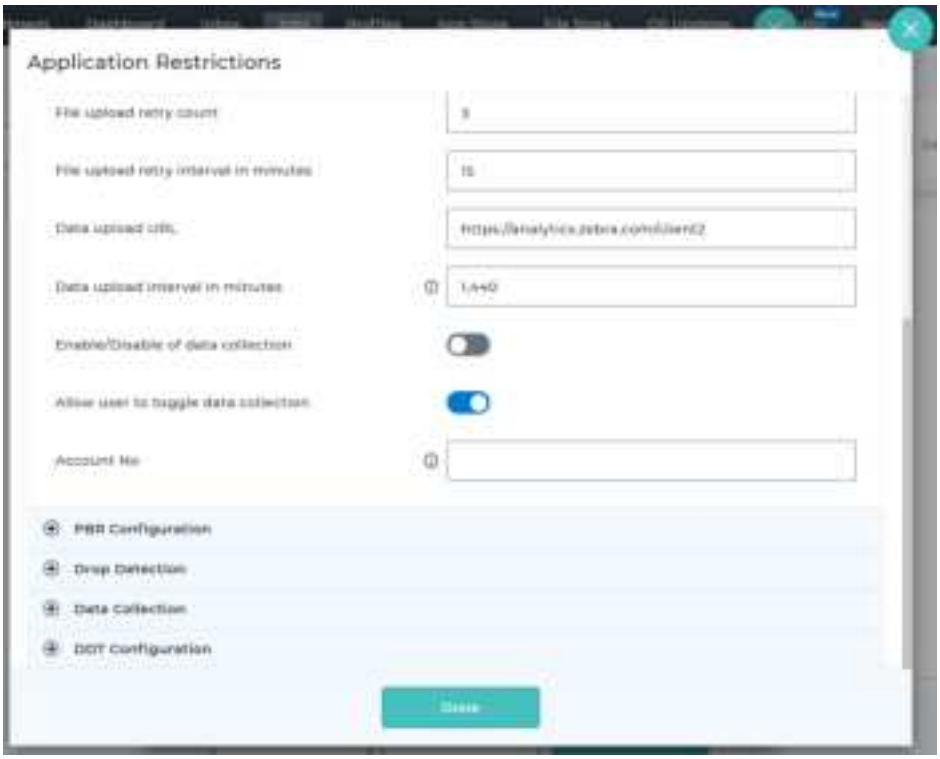
8. Go to **System Configuration**, enable the **ZSA Configuration** option and set the **Configuration of the log level for ZSA** with the following values:
   - 0: Info
   - 1: Debug
   - 2: Sensitive



9. 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.

10. 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).

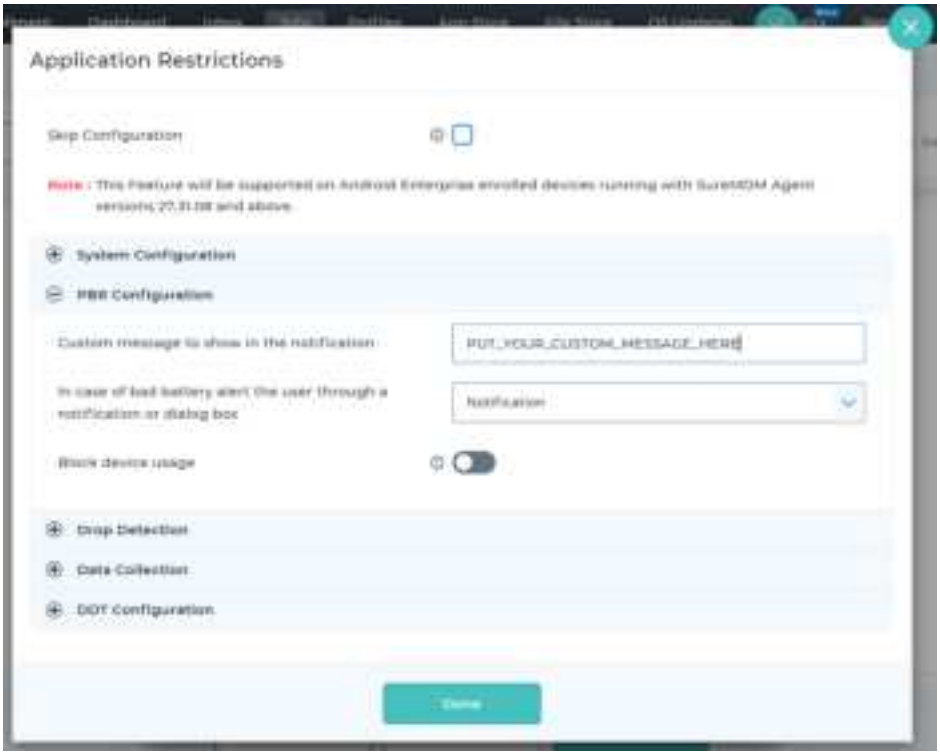


11. Data collection settings for non-Zebra devices:

- **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.

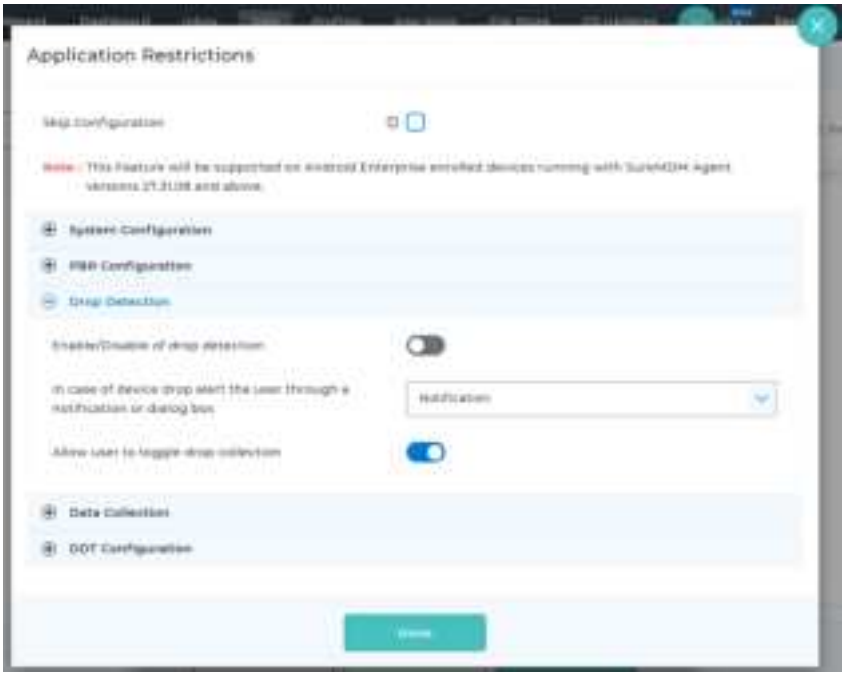
12. For the **Account No**, users must enter their MDM account number for non-Zebra devices.

13. Go to **PBR Configuration**, provide a **Custom Message** as required.



14. 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
15. The **Block device usage** option is disabled by default. If enabled by the administrator, it prevents device access when a bad battery is detected.

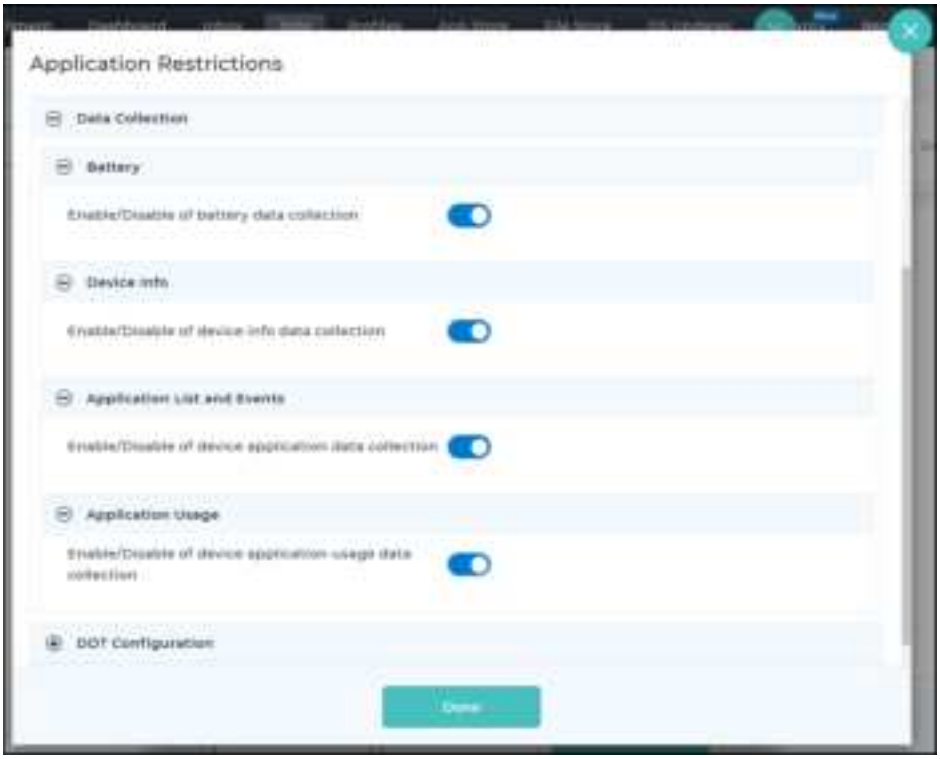
16. Go to **Drop Detection**, toggle the **Enable/Disable of drop detection** option as required.



17. 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
18. 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.
19. 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.

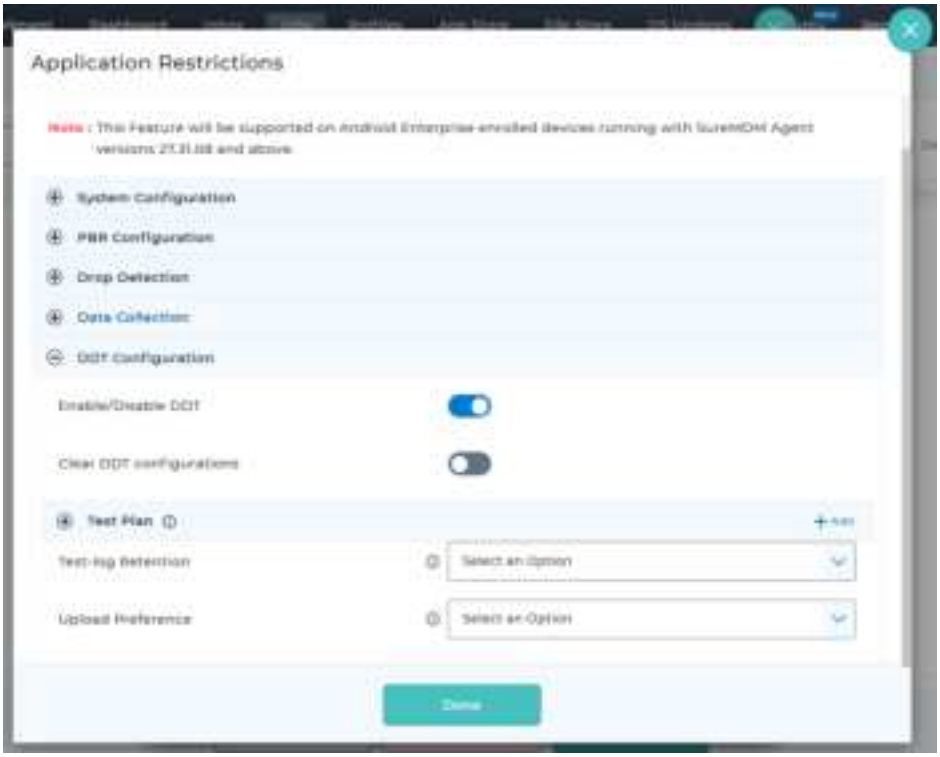
Only the admin can enable or disable this option to restrict user access; however, the collection interval cannot be modified.

- 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.

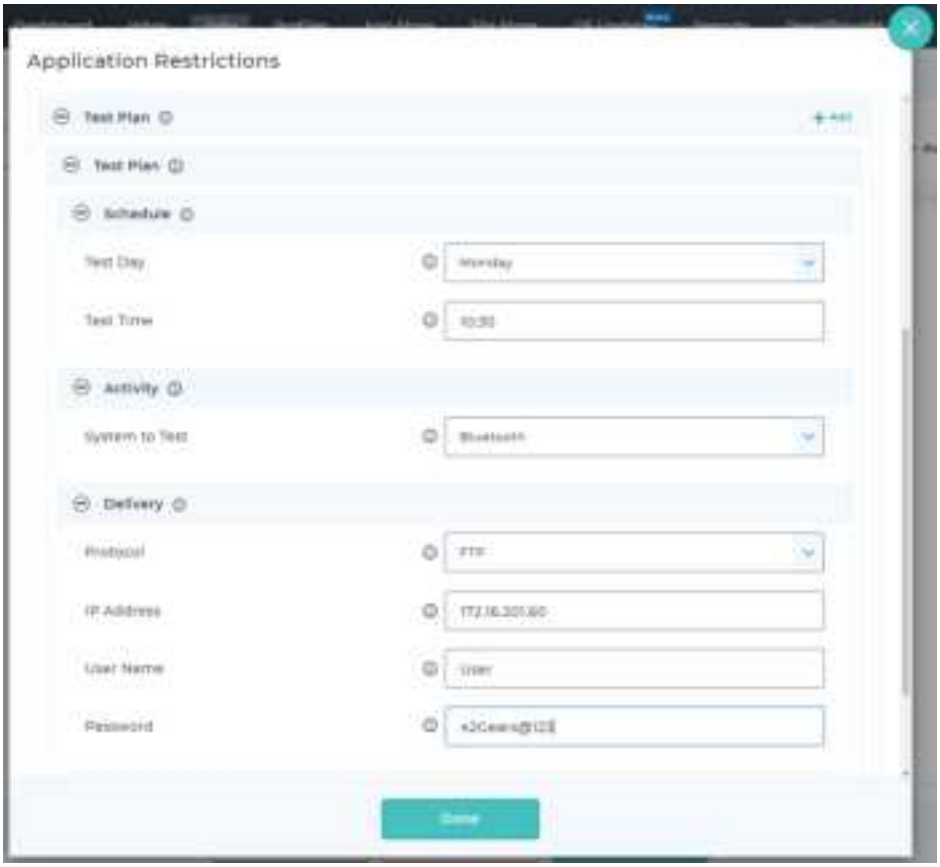


NOTE: Data is uploaded based on the configured **Data Upload URL** and interval settings in the **System Configuration**.

20. In the **DDT Configuration** section, enable the **Enable/Disable DDT** option, keep the **Clear DDT configurations** disabled in the primary setup, and click **Add** in the **Test Plan** section.



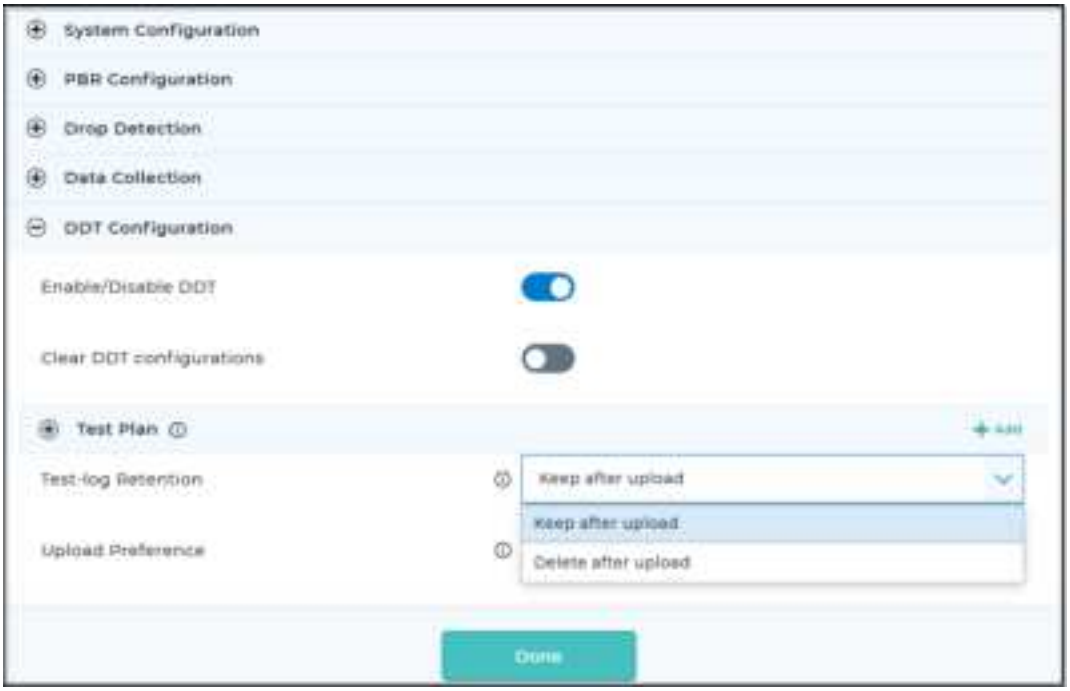
21. Under the **Schedule** section, configure the test plan with the following values:



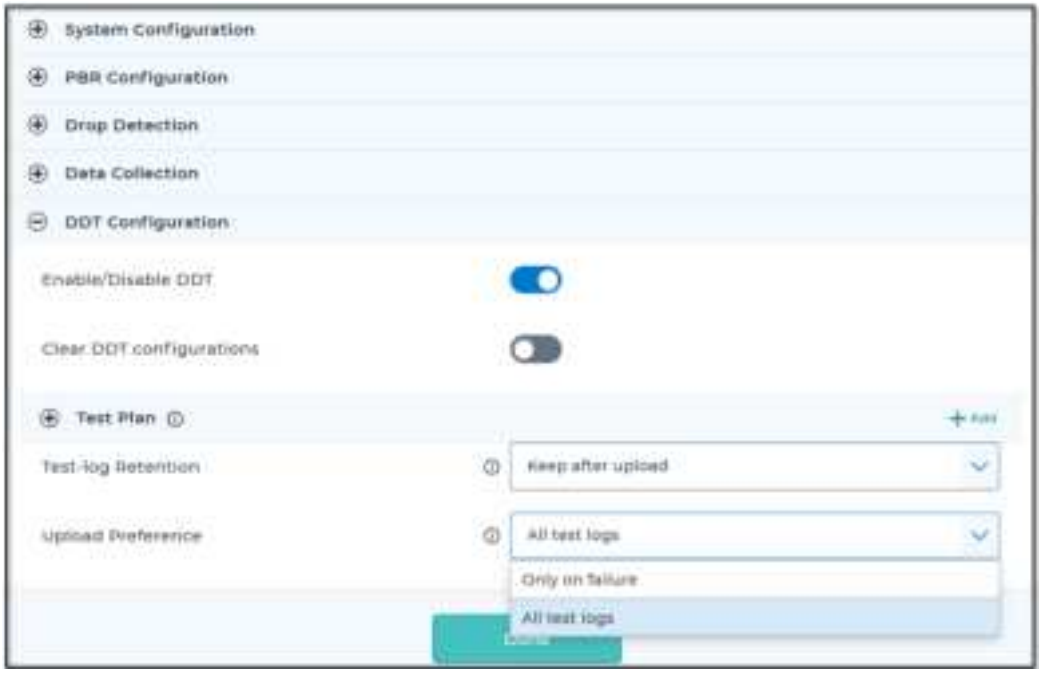
- **Test Day**: Day of the Week (For example, Monday)
- **Test Time**: Time of the day for the test (HH: MM format)
- **System to Test**: Select the test to schedule (For example, Bluetooth)

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

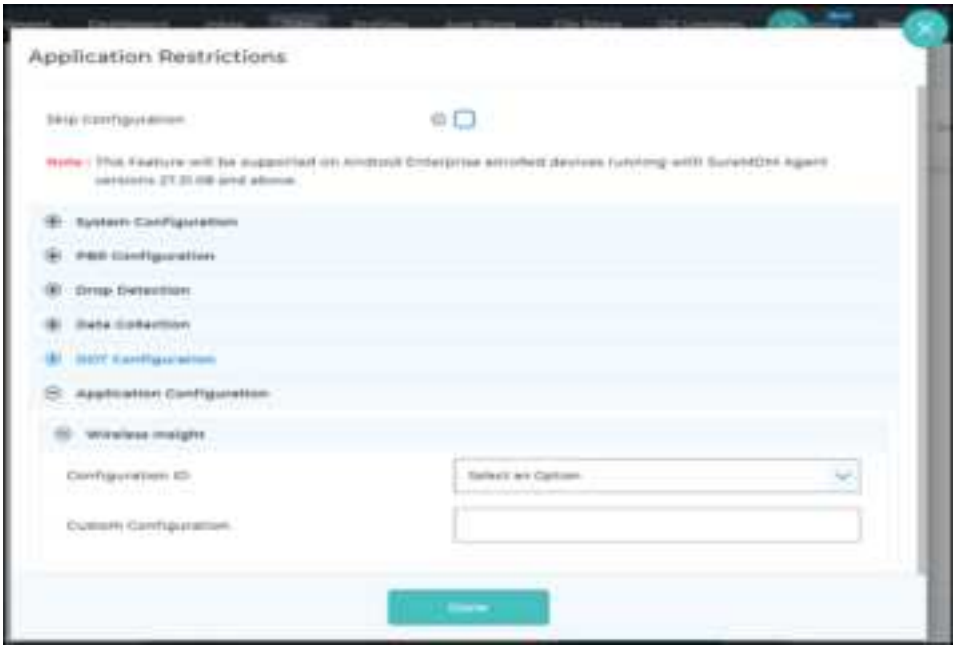
23. Select the **Test-log Retention** as required.



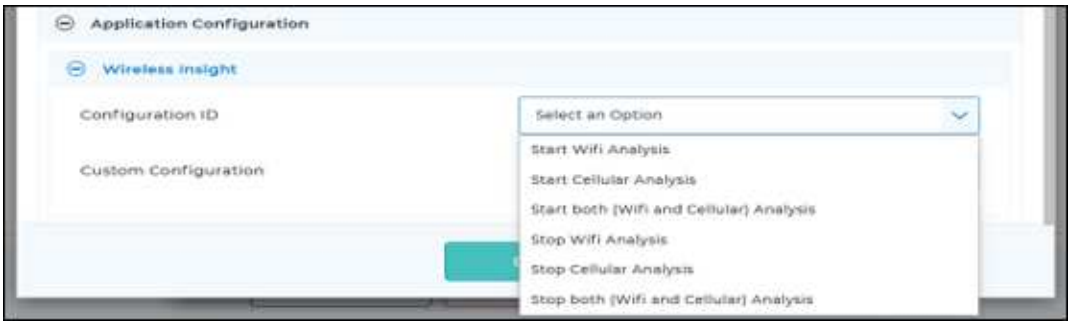
24. Select the **Upload Preference** as required.



25. 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.

26. Click **Done**.

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

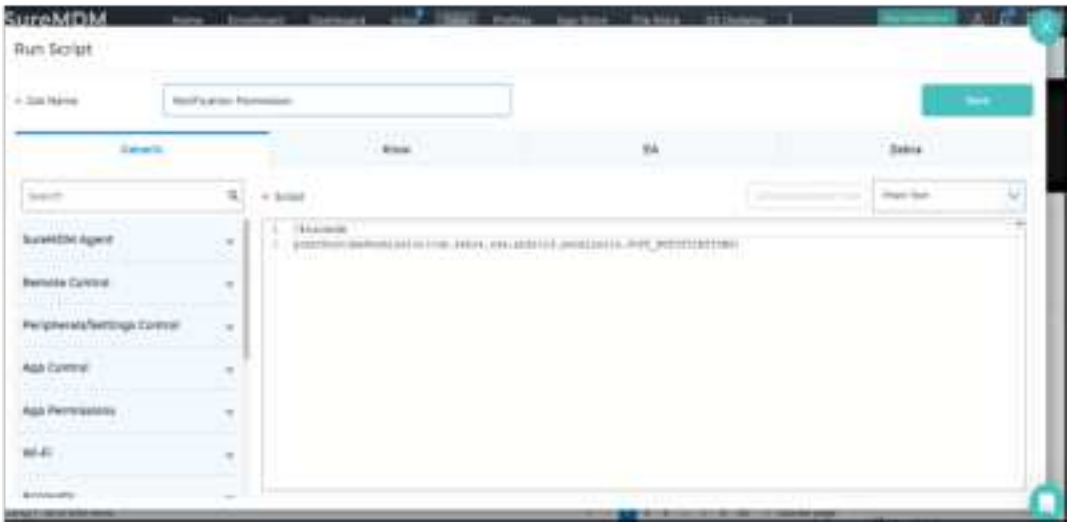
Granting Required Permission for the ZSA Application

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** and enter the following script:

```
#suremdm
```

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



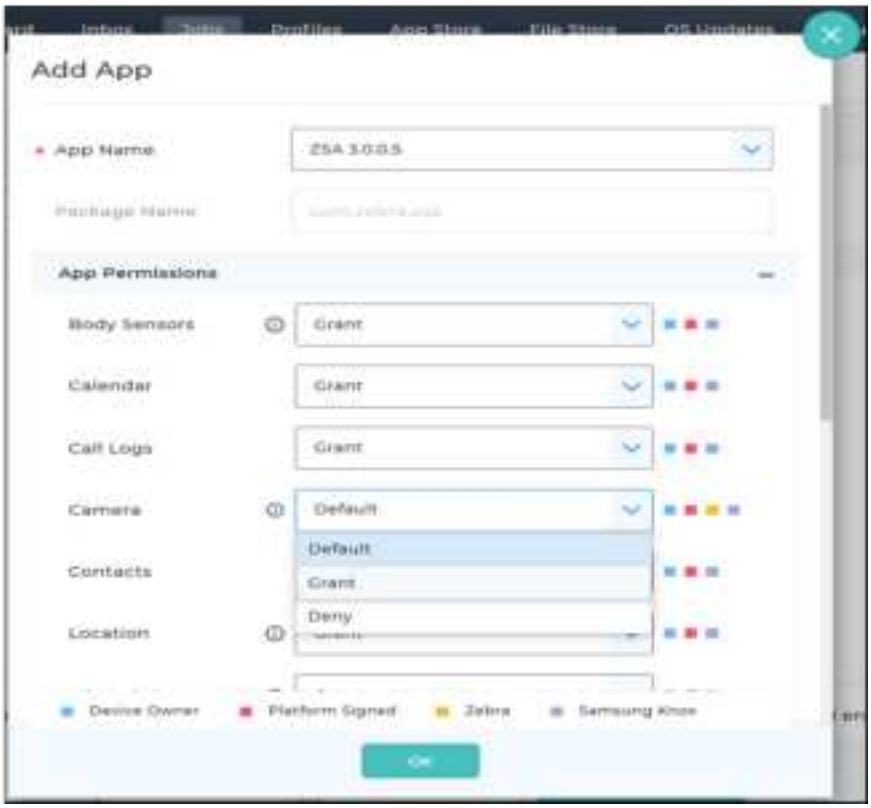
   c) Click **Save**.

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

2. Granting runtime permissions and special permissions.

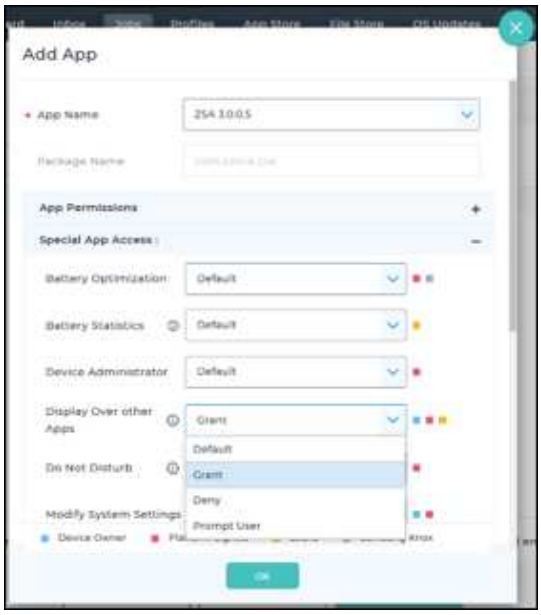
   a) Navigate to **Jobs** > **New Job** > **Android** > **Application Permission**.

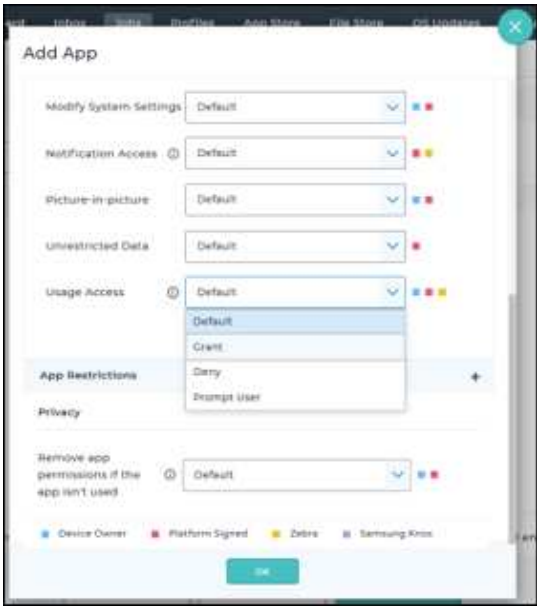
   b) From the dialog box, add a **Job Name** and click **+Add**.



   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.

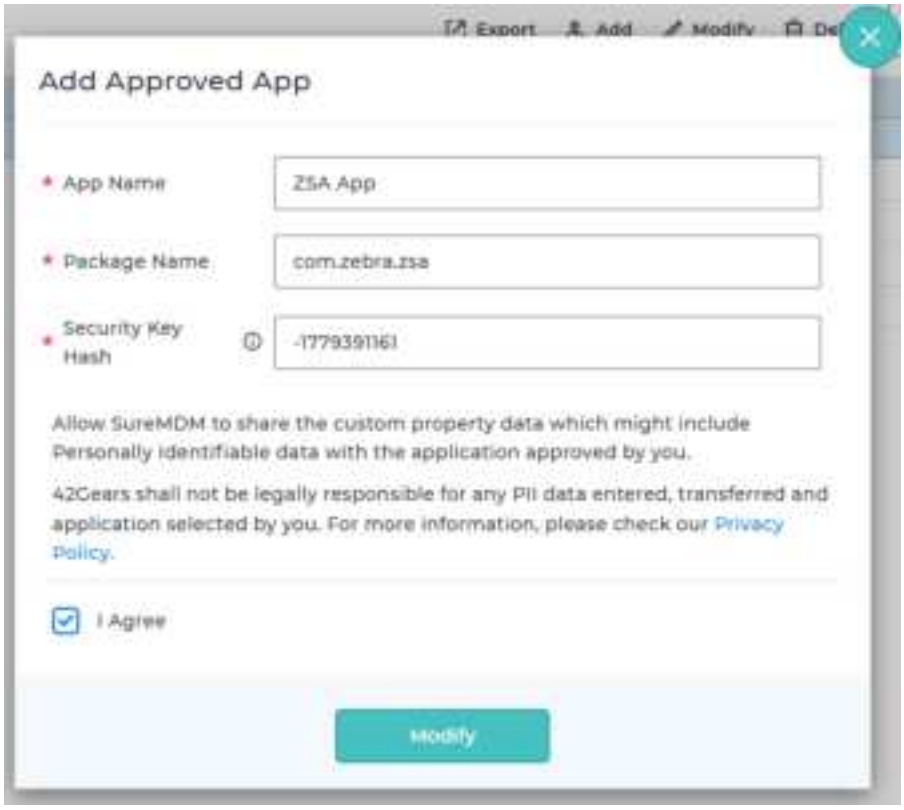
NOTE: The newly created job displays in the **Jobs List** section.

Allowing the ZSA Application to Read Device Serial Numbers

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

1. Go to **MDM Account Settings** > **Device Properties**.
2. Select **Approved 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.zsa** 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**.

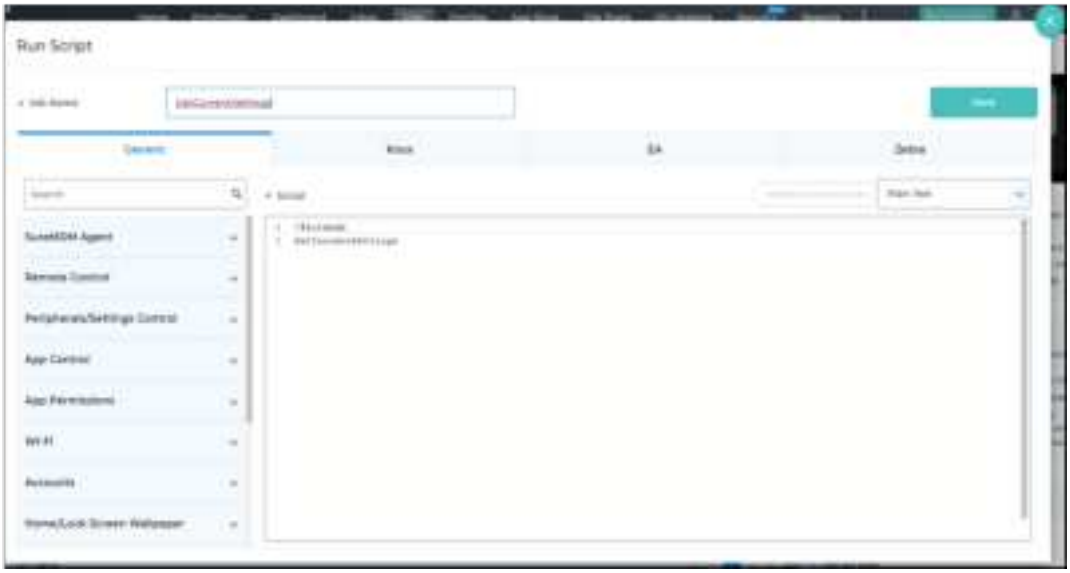
d) Accept the **Privacy Policy** by checking the **I Agree** checkbox.

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** and enter the following script:

```
#suremdm
```

```
GetCurrentSetting
```



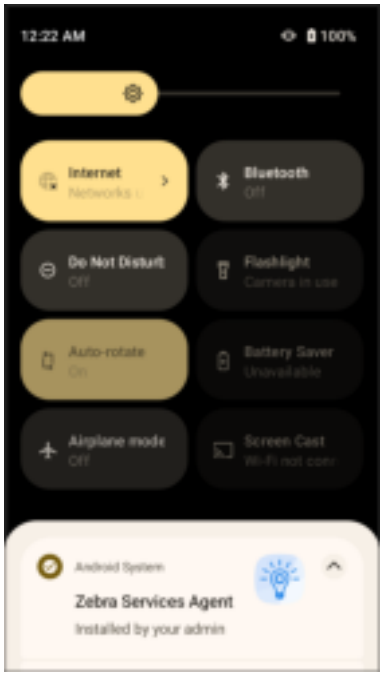
   b) Click **Save**.

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

Installing Apps

After creating the profiles, install the apps.

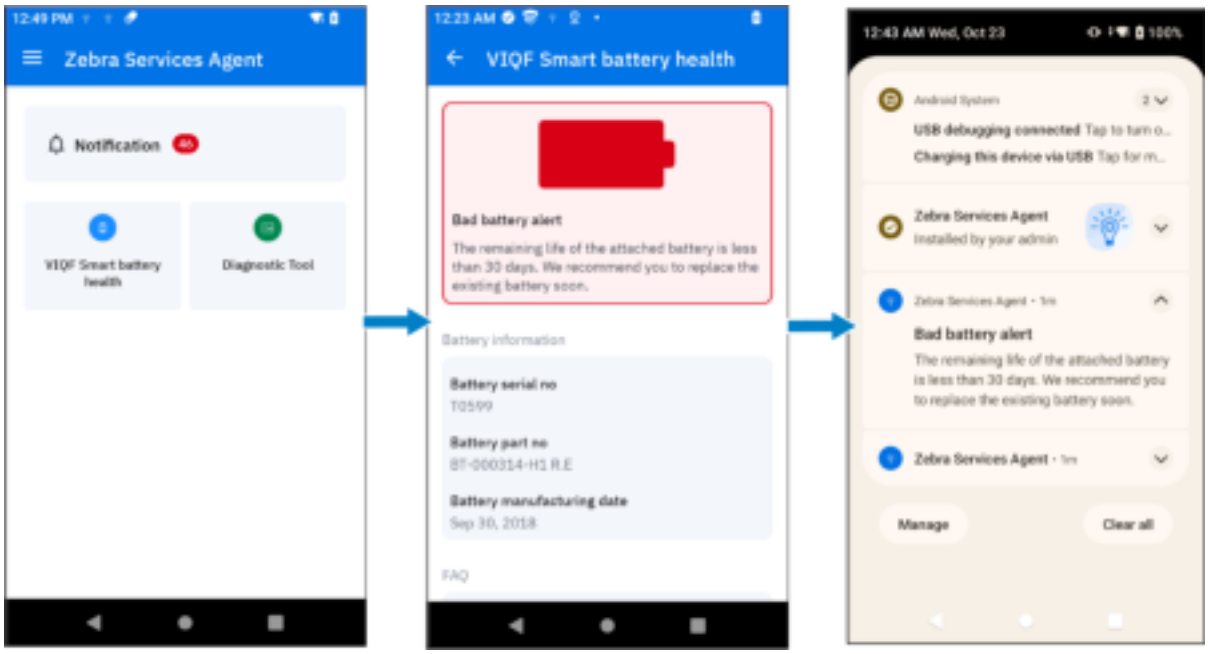
1. Go to **Home**, select **All Devices**, and then click **Apply Jobs** in the following sequence:
   a. Install the App Job
   b. Notification Permission Job
   c. Application Permission Job
   d. Get Current Settings Job
2. The application is now installed on the devices.



Expected Behaviour After Auto-launching Zebra Services Agent

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

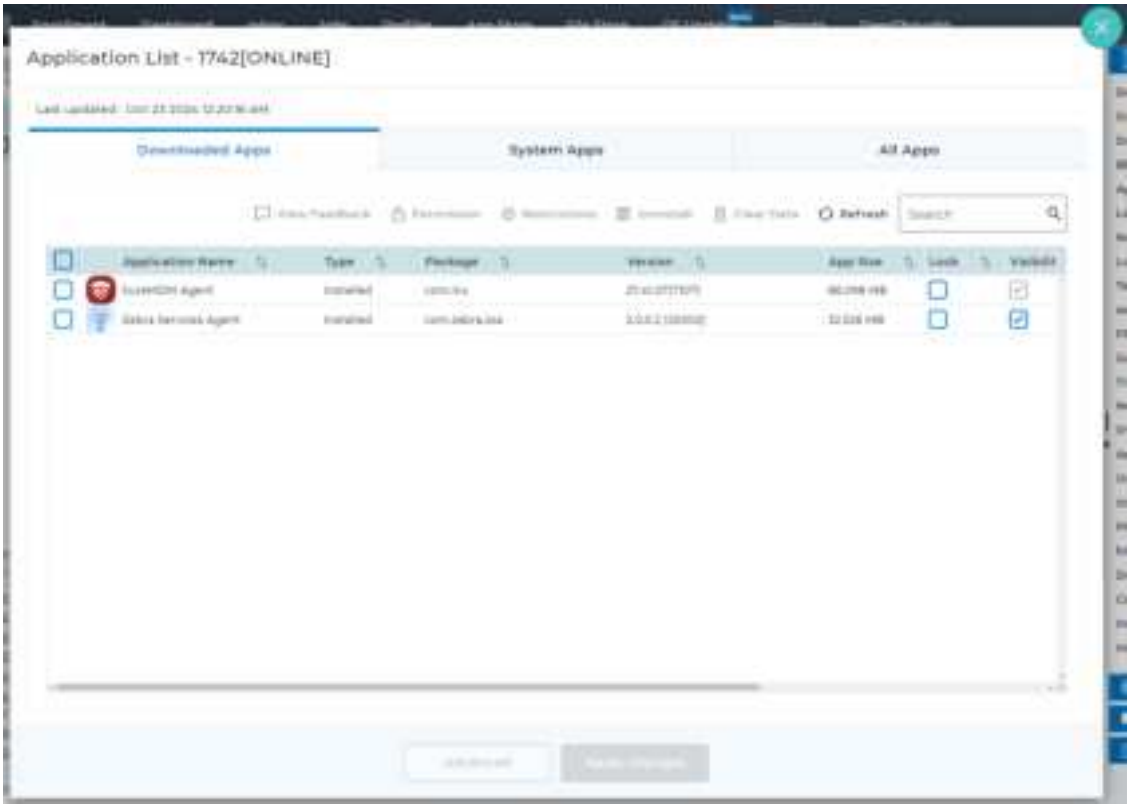
1. Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
2. If the ZSBH module is entitled, the ZSA app automatically launches it after a few seconds.
3. The ZSA home screen displays the VIFQ Smart battery health and Diagnostic tool, and if a **bad battery** condition is detected, a notification will display.
4. After a few seconds, the ZSA app will close.



FAQs

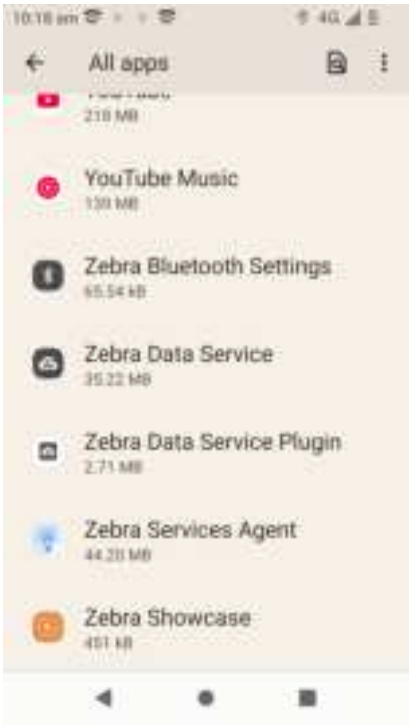
1. How do you determine which apps are installed on the devices in 42Gears?
   a) Go to **Home** > **Device List**.
   b) Select any device mentioned in the list.

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

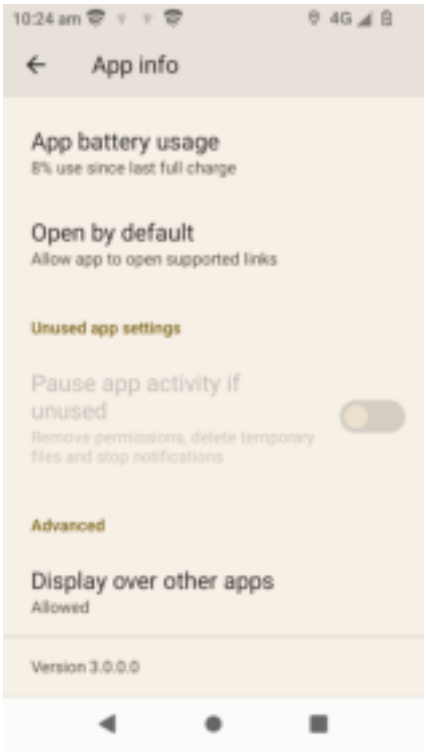


2. How do you verify if the app is installed with the correct permissions and is able to connect to Zebra servers?

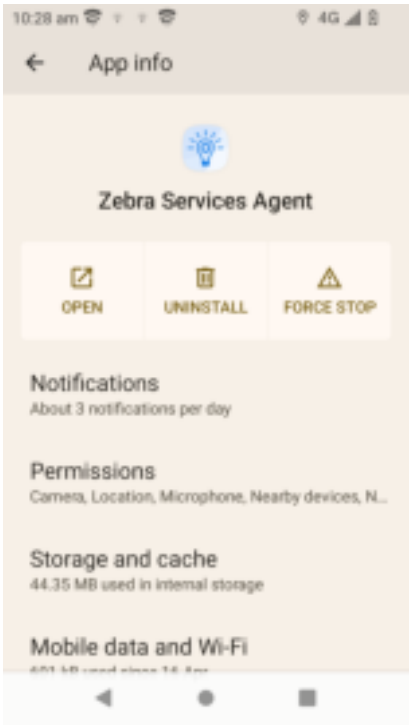
   a) To verify the app version, go to **Settings** > **Apps** > **All apps** and select **Zebra Services Agent**.



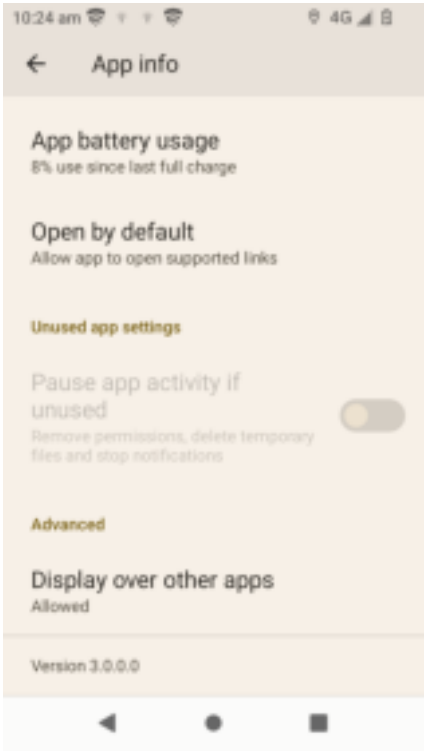
   b) The **App Info** page displays the **Version**.



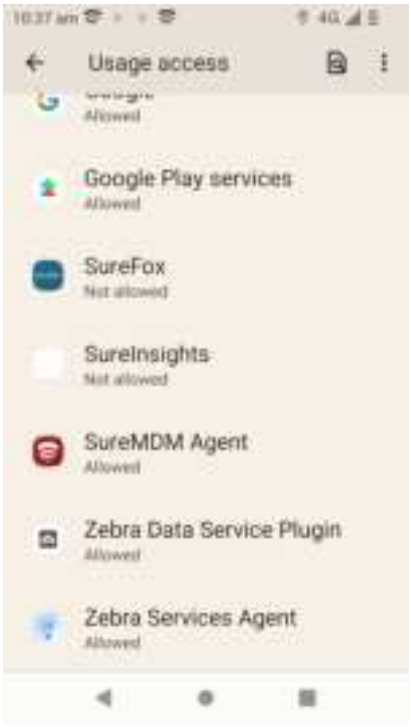
c) To verify the ZSA Permissions, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Permissions**.



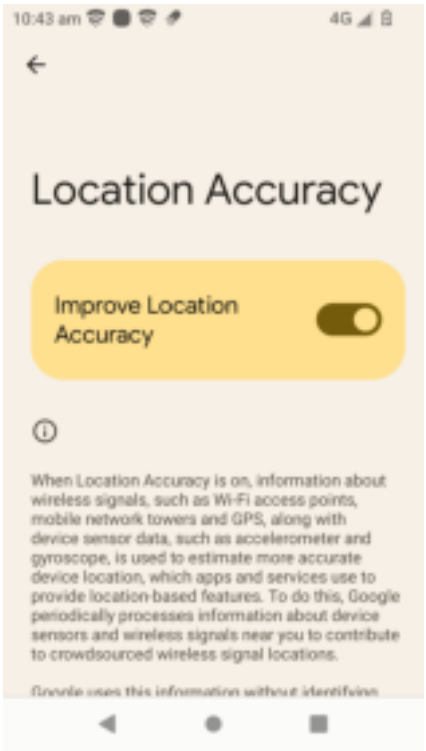
d) To verify the Display over other apps permission, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Advanced** > **Display over other apps**.



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

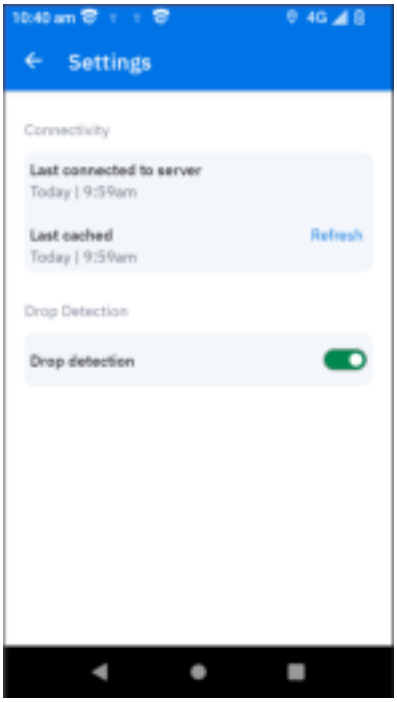


f) For the **Device action** > **Outdoor Location Tracking** feature, ensure that location accuracy is enabled on the device for precise location information. Navigate to **Settings** > **Location** > **Location Services** > **Location Accuracy**.



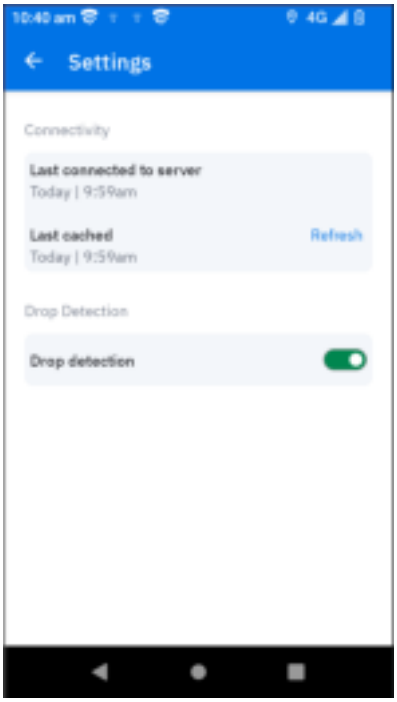
g) To verify ZSA Network connectivity to the Zebra URL:

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



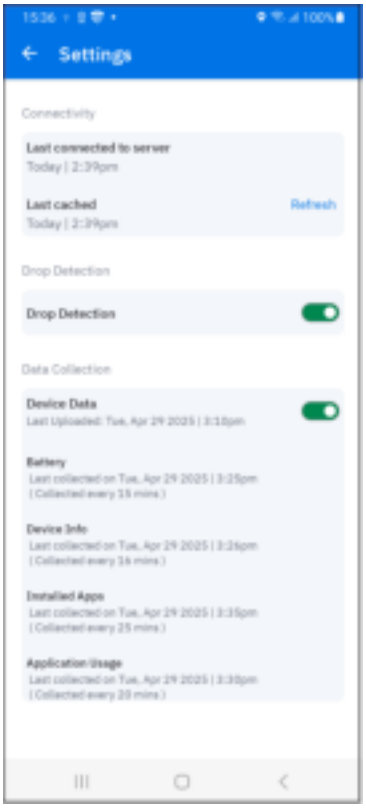
h) To verify the Drop Detection status:

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.