Zebra Services Agent for 42Gears SureMDM

ZEBRA

Installation Guide

Copyright

2025/06/13

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.

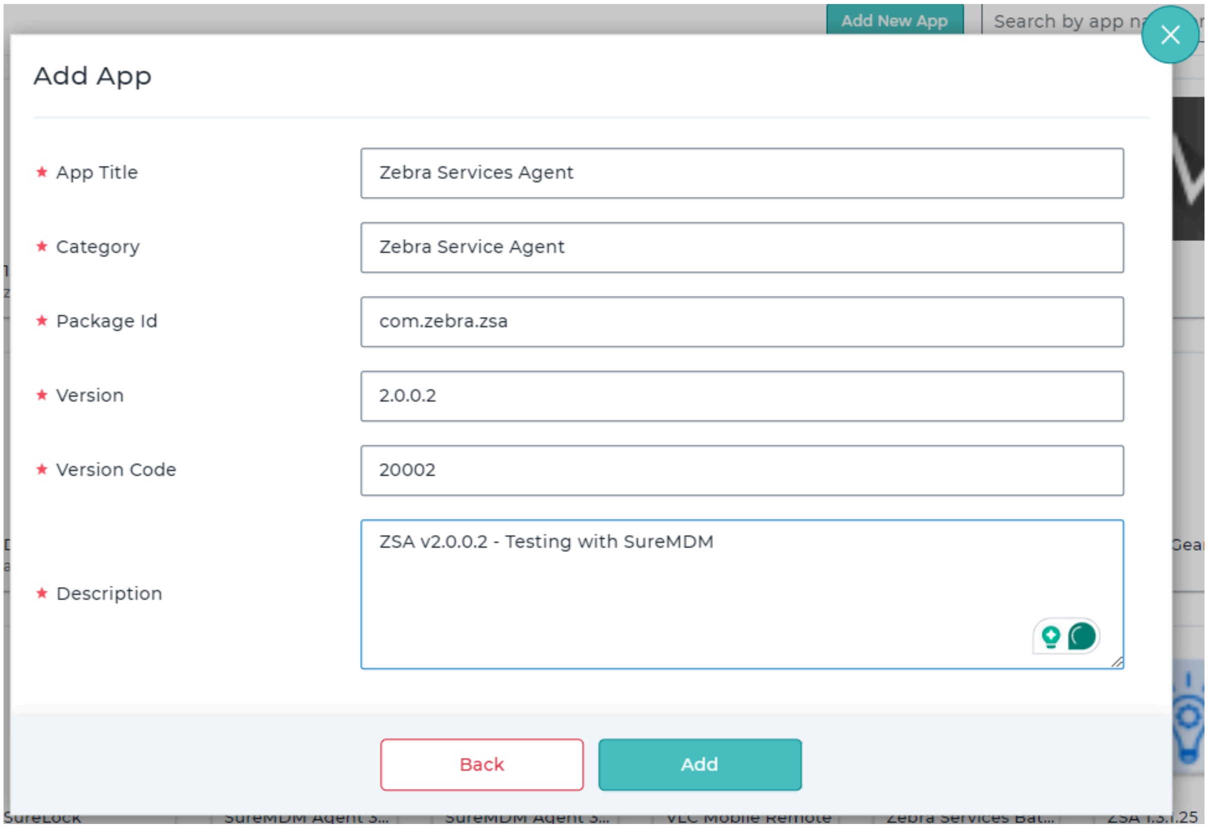
Download the `Zebra_Services_Agent_V3.0.0.5.apk` file from zebra.com/zebra-services-agent.

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**.



Add App

★ App Title: Zebra Services Agent

★ Category: Zebra Service Agent

★ Package Id: com.zebra.zsa

★ Version: 2.0.0.2

★ Version Code: 20002

★ Description: ZSA v2.0.0.2 - Testing with SureMDM

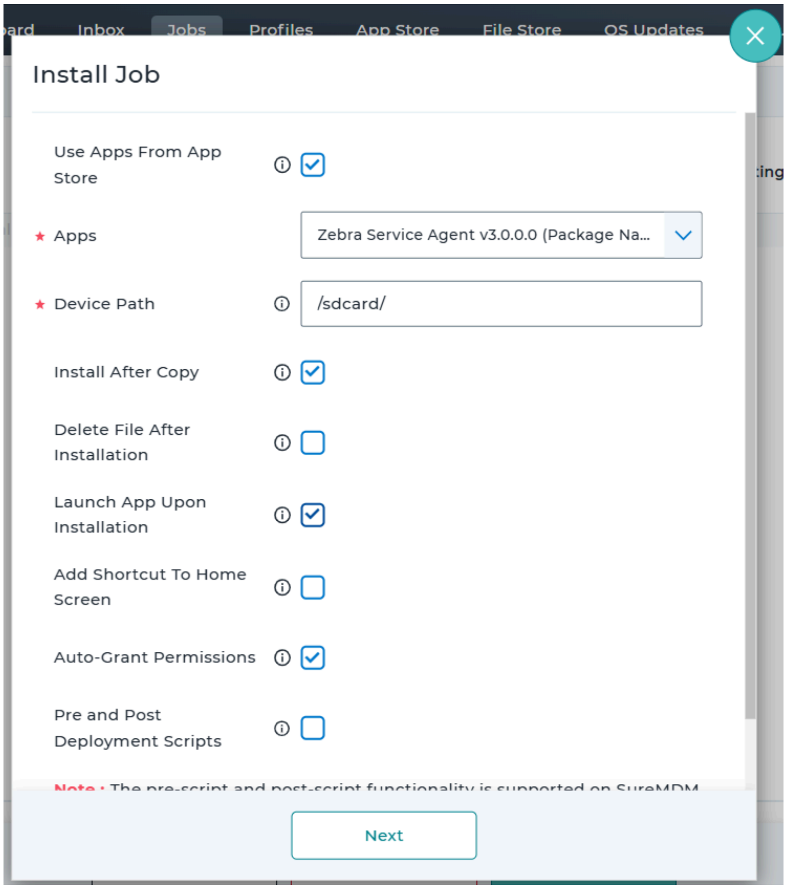
Installing Job Application for ZSA App with Managed Configuration Settings

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.



Install Job

Use Apps From App Store ☑

* Apps: Zebra Service Agent v3.0.0.0 (Package Na...

* Device Path: /sdcard/

Install After Copy ☑

Delete File After Installation ☐

Launch App Upon Installation ☑

Add Shortcut To Home Screen ☐

Auto-Grant Permissions ☑

Pre and Post Deployment Scripts ☐

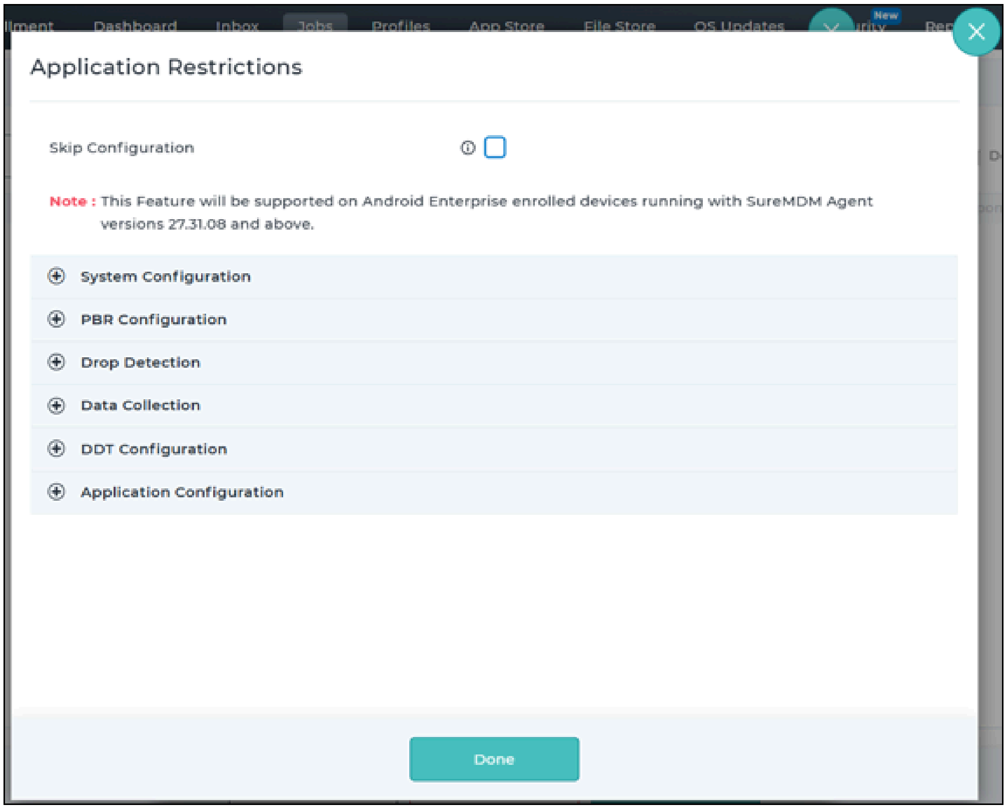
Note : The pre-script and post-script functionality is supported on SureMDM

Next

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**.



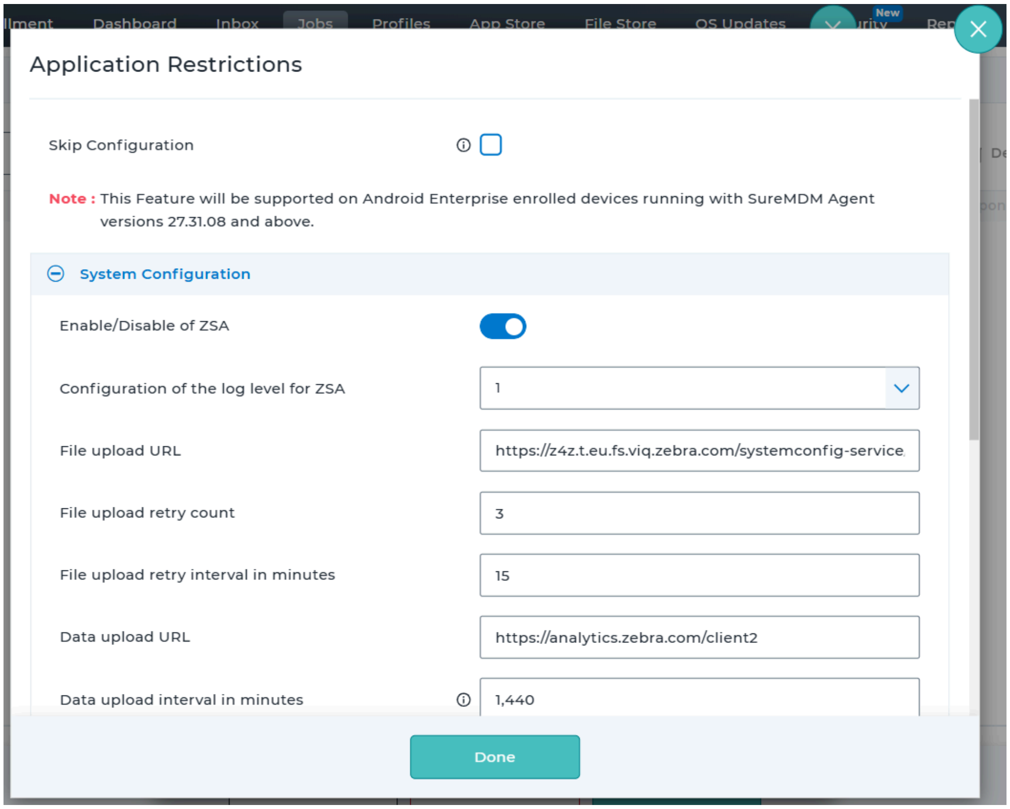
Application Restrictions

Skip Configuration □

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

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



Application Restrictions

Skip Configuration ⓘ □

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

System Configuration

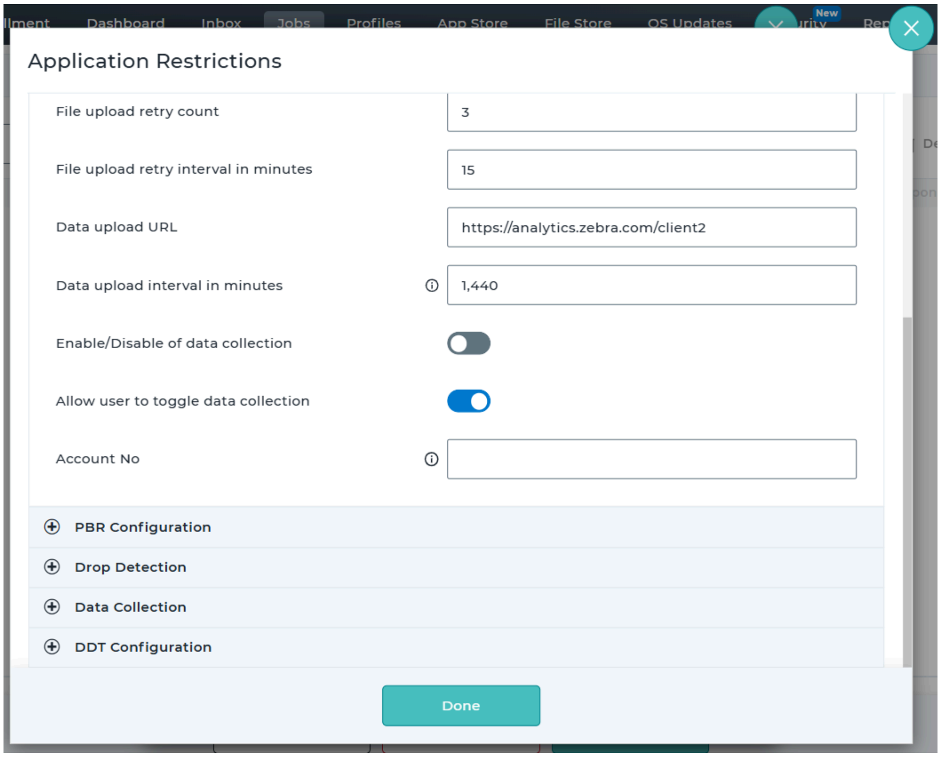
Enable/Disable of ZSA	●
Configuration of the log level for ZSA	1
File upload URL	https://z4z.t.eu.fs.viq.zebra.com/systemconfig-service
File upload retry count	3
File upload retry interval in minutes	15
Data upload URL	https://analytics.zebra.com/client2
Data upload interval in minutes ⓘ	1,440

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).



Application Restrictions

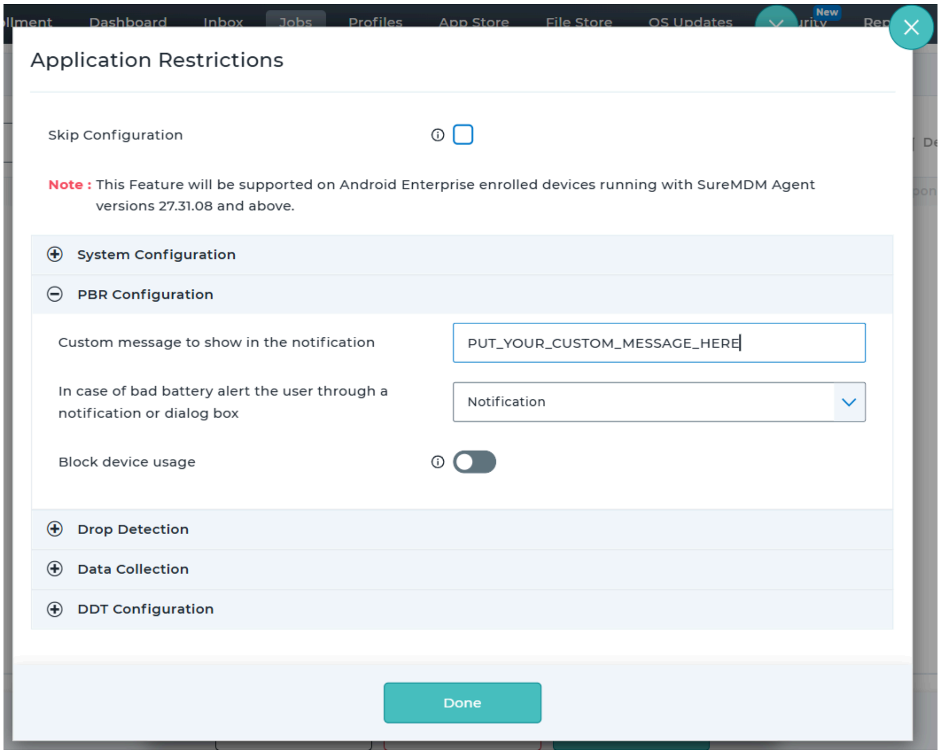
File upload retry count	3
File upload retry interval in minutes	15
Data upload URL	https://analytics.zebra.com/client2
Data upload interval in minutes ⓘ	1,440
Enable/Disable of data collection	○
Allow user to toggle data collection	●
Account No ⓘ	

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.



Application Restrictions

Skip Configuration ⓘ □

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

⊕ System Configuration

⊖ PBR Configuration

Custom message to show in the notification: PUT_YOUR_CUSTOM_MESSAGE_HERE

In case of bad battery alert the user through a notification or dialog box: Notification

Block device usage ⓘ ○

⊕ Drop Detection

⊕ Data Collection

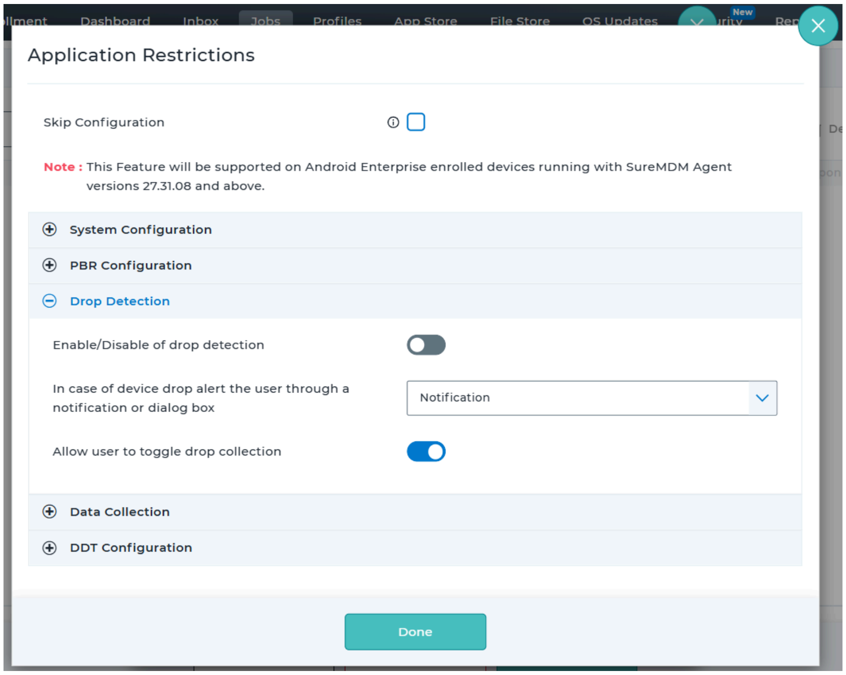
⊕ DDT Configuration

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.



Application Restrictions

Skip Configuration ⓘ □

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

⊕ System Configuration

⊕ PBR Configuration

⊖ Drop Detection

Enable/Disable of drop detection ○

In case of device drop alert the user through a notification or dialog box: Notification

Allow user to toggle drop collection ●

⊕ Data Collection

⊕ DDT Configuration

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

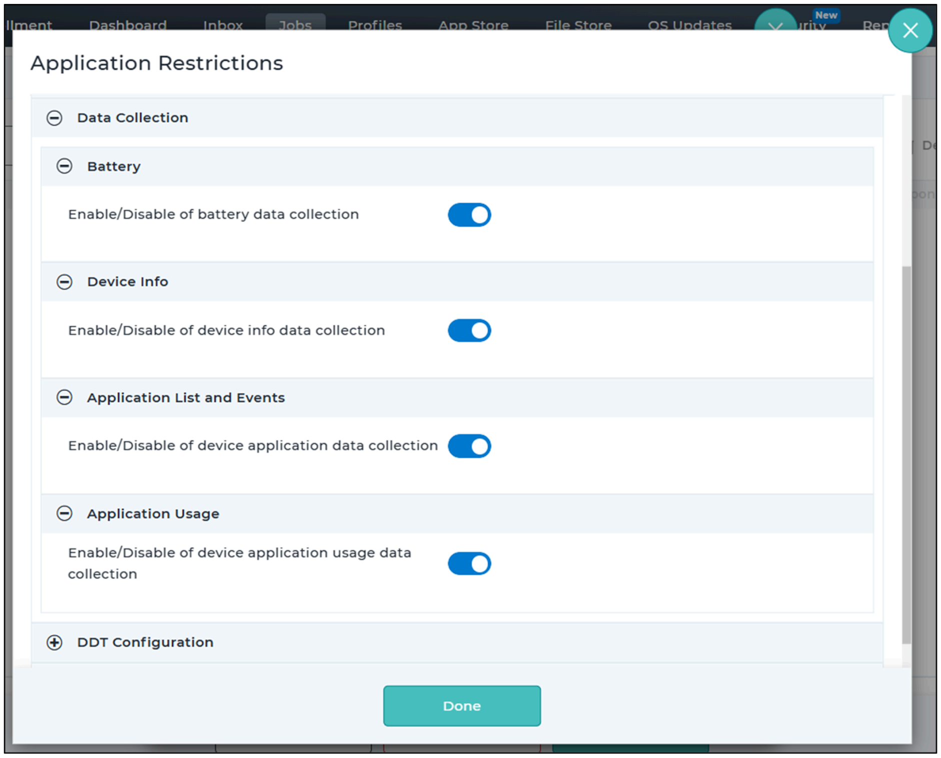
18. The **Allow user to toggle drop collection** is enabled by default. Users can control this feature, and admins can disable it to restrict access for users.

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.



Application Restrictions

⊖ Data Collection

⊖ Battery

Enable/Disable of battery data collection ●

⊖ Device Info

Enable/Disable of device info data collection ●

⊖ Application List and Events

Enable/Disable of device application data collection ●

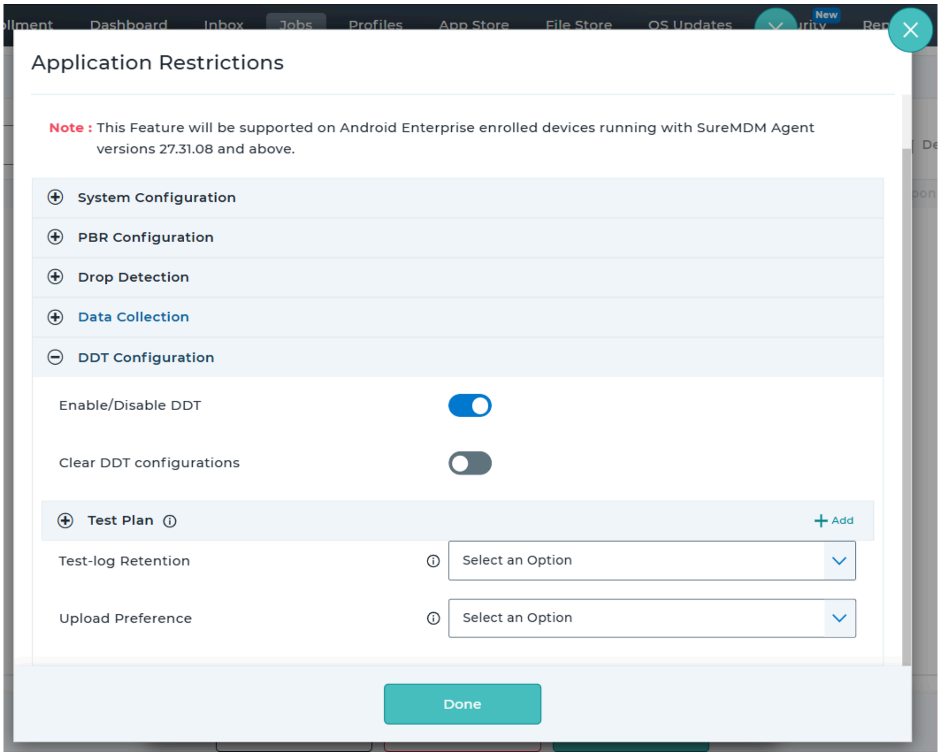
⊖ Application Usage

Enable/Disable of device application usage data collection ●

⊕ DDT Configuration

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.



Application Restrictions

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

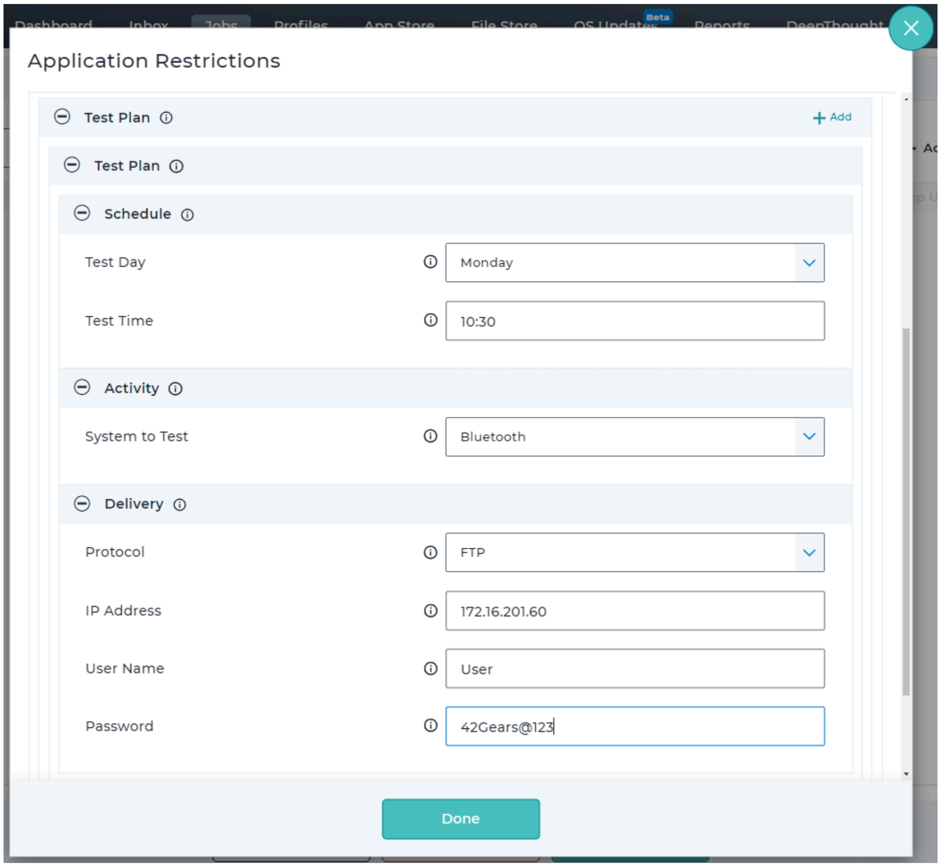
Enable/Disable DDT ●

Clear DDT configurations ○

Test-log Retention: Select an Option

Upload Preference: Select an Option

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



Test Day: Monday

Test Time: 10:30

System to Test: Bluetooth

Protocol: FTP

IP Address: 172.16.201.60

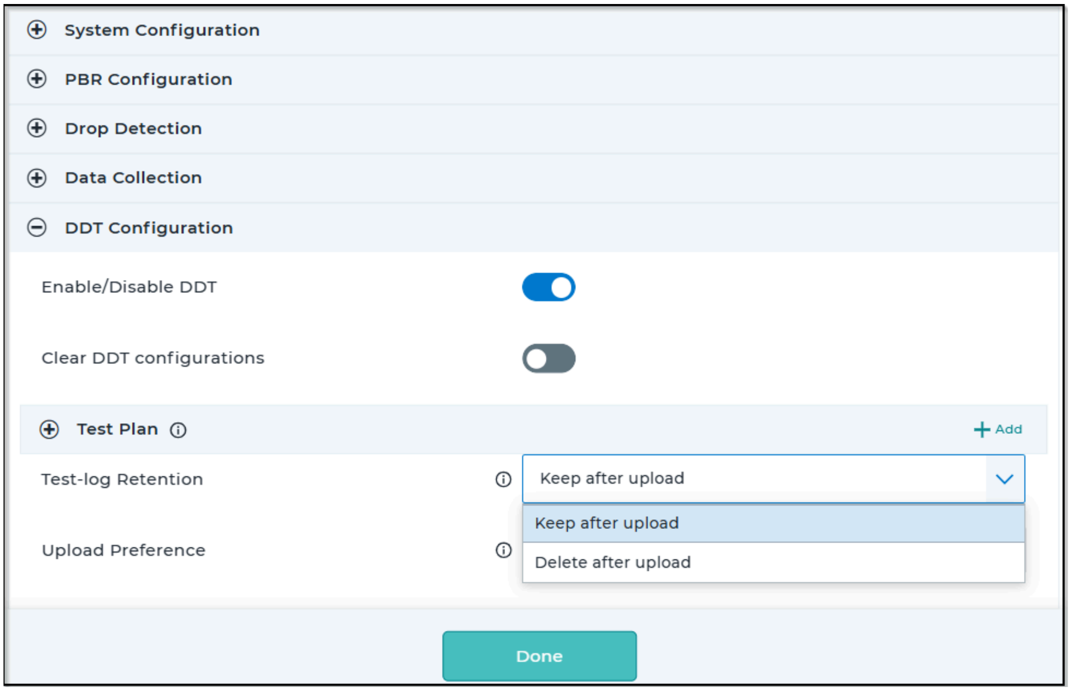
User Name: User

Password: 42Gears@123

- **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.



System Configuration

PBR Configuration

Drop Detection

Data Collection

DDT Configuration

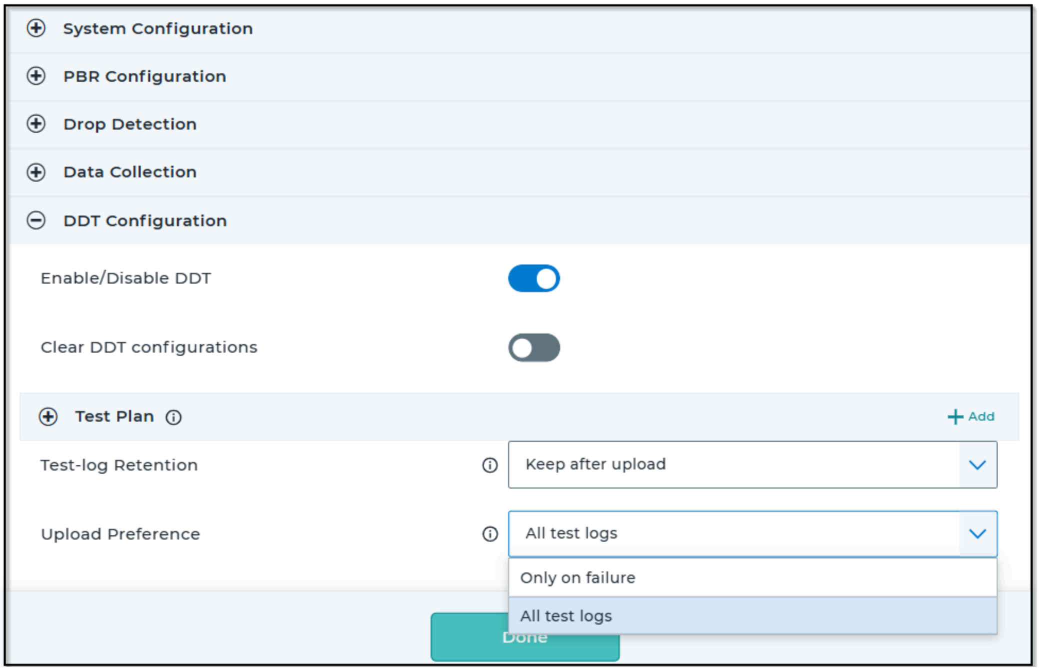
Enable/Disable DDT

Clear DDT configurations

Test Plan

Test-log Retention: Keep after upload

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



System Configuration

PBR Configuration

Drop Detection

Data Collection

DDT Configuration

Enable/Disable DDT

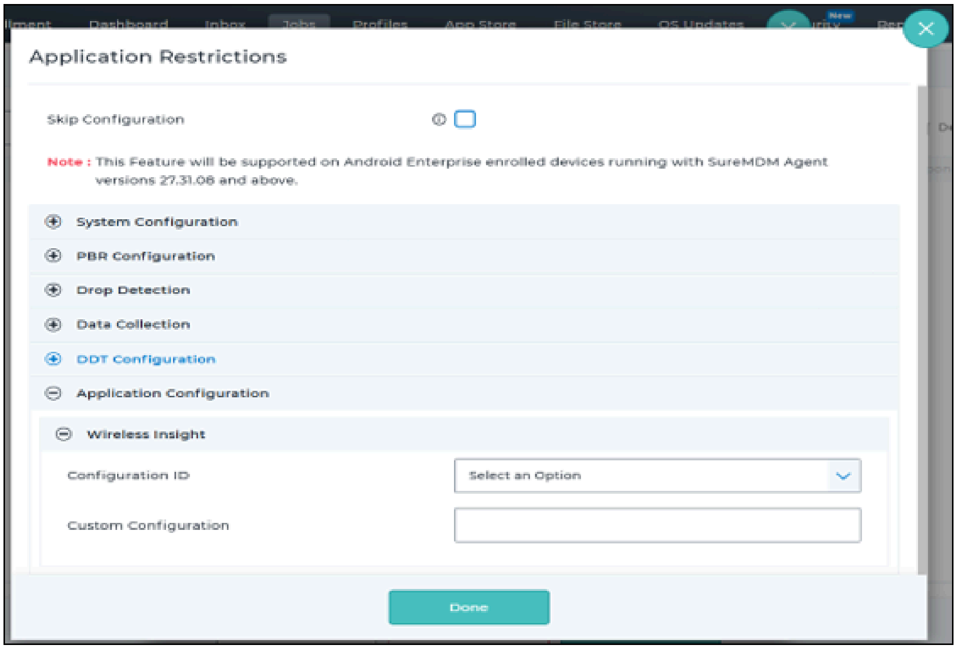
Clear DDT configurations

Test Plan

Test-log Retention: Keep after upload

Upload Preference: All test logs

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.



Application Restrictions

Skip Configuration ⓘ □

Note : This Feature will be supported on Android Enterprise enrolled devices running with SureMDM Agent versions 27.31.08 and above.

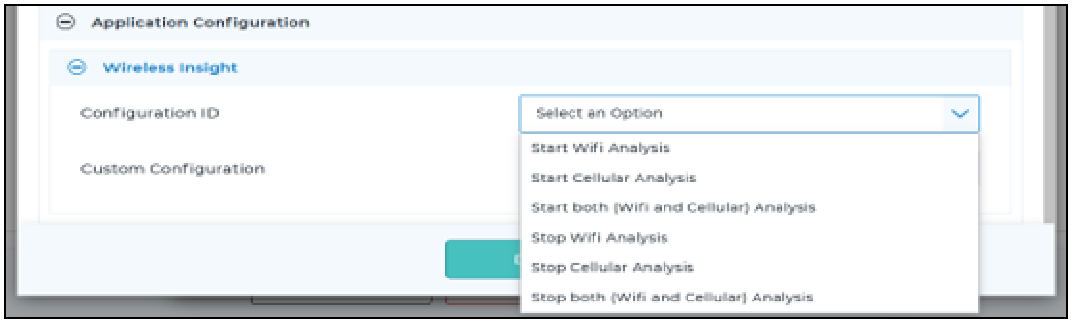
- ⊕ System Configuration
- ⊕ PBR Configuration
- ⊕ Drop Detection
- ⊕ Data Collection
- ⊕ DDT Configuration
- ⊖ Application Configuration
  - ⊖ Wireless Insight

Configuration ID: Select an Option

Custom Configuration:

Done

- **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.



⊖ Application Configuration

⊖ Wireless Insight

Configuration ID: Select an Option

- Start Wifi Analysis
- Start Cellular Analysis
- Start both (Wifi and Cellular) Analysis
- Stop Wifi Analysis
- Stop Cellular Analysis
- Stop both (Wifi and Cellular) Analysis

Custom Configuration

  - **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:

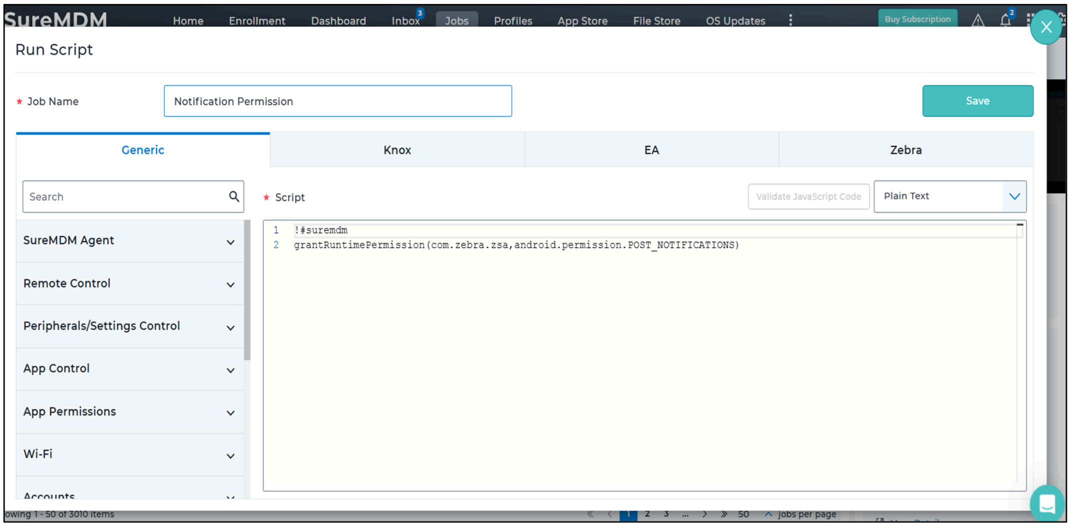
1. Granting notification permission.

   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)
```



Run Script

* Job Name: Notification Permission

* Script: Plain Text

```
!#suremdm
grantRuntimePermission(com.zebra.zsa,android.permission.POST_NOTIFICATIONS)
```

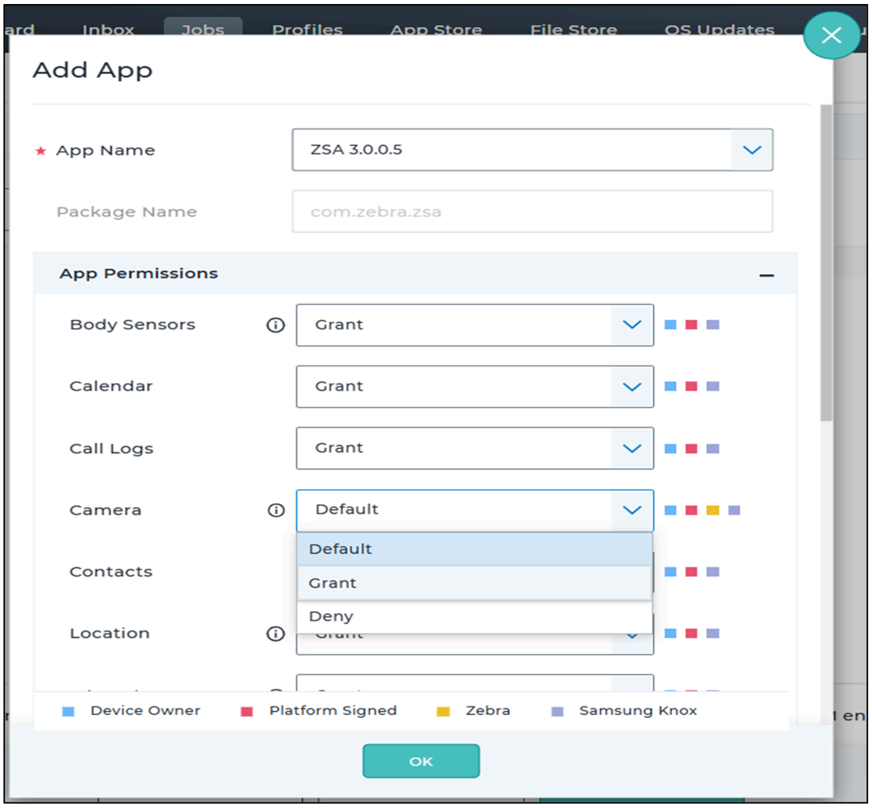
   c) Click **Save**.

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**.



Add App

* App Name	ZSA 3.0.0.5
Package Name	com.zebra.zsa

App Permissions

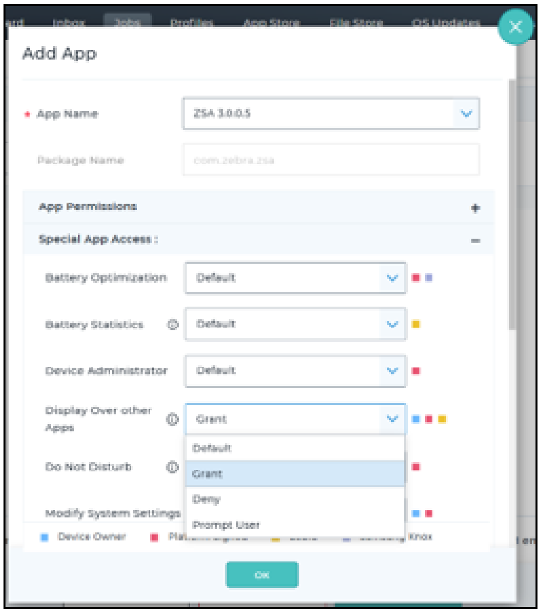
Body Sensors	Grant	🟦 🟥 🟪
Calendar	Grant	🟦 🟥 🟪
Call Logs	Grant	🟦 🟥 🟪
Camera	Default	🟦 🟥 🟨 🟪
Contacts		🟦 🟥 🟪
Location	Grant	🟦 🟥 🟪

Default
Grant
Deny

🟦 Device Owner 🟥 Platform Signed 🟨 Zebra 🟪 Samsung Knox

   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**.



Add App

App Name: ZSA 3.0.0.5

Package Name: com.zebra.zsa

Special App Access :

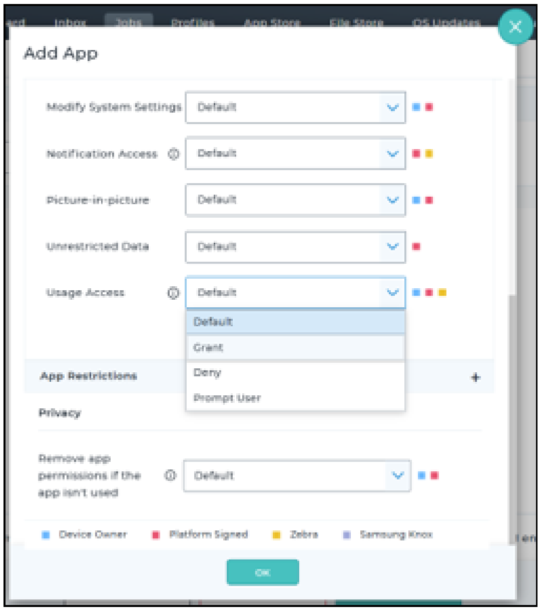
Battery Optimization: Default

Battery Statistics: Default

Device Administrator: Default

Display Over other Apps: Grant

Modify System Settings



Add App

Modify System Settings: Default

Notification Access: Default

Picture-in-picture: Default

Unrestricted Data: Default

Usage Access: Default

Privacy

Remove app permissions if the app isn't used: Default

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

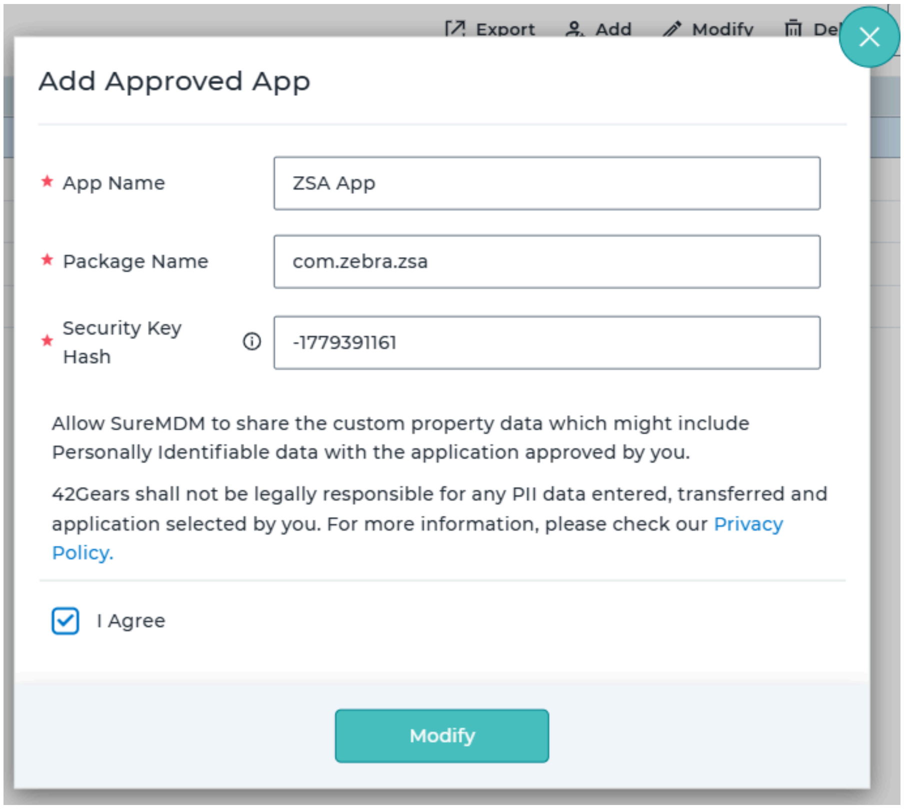
NOTE: The newly created job displays in the **Jobs List** section.

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:



Add Approved App

* App Name: ZSA App

* Package Name: com.zebra.zsa

* Security Key Hash: -1779391161

Allow SureMDM to share the custom property data which might include Personally Identifiable data with the application approved by you.

42Gears shall not be legally responsible for any PII data entered, transferred and application selected by you. For more information, please check our Privacy Policy.

☑ I Agree

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.

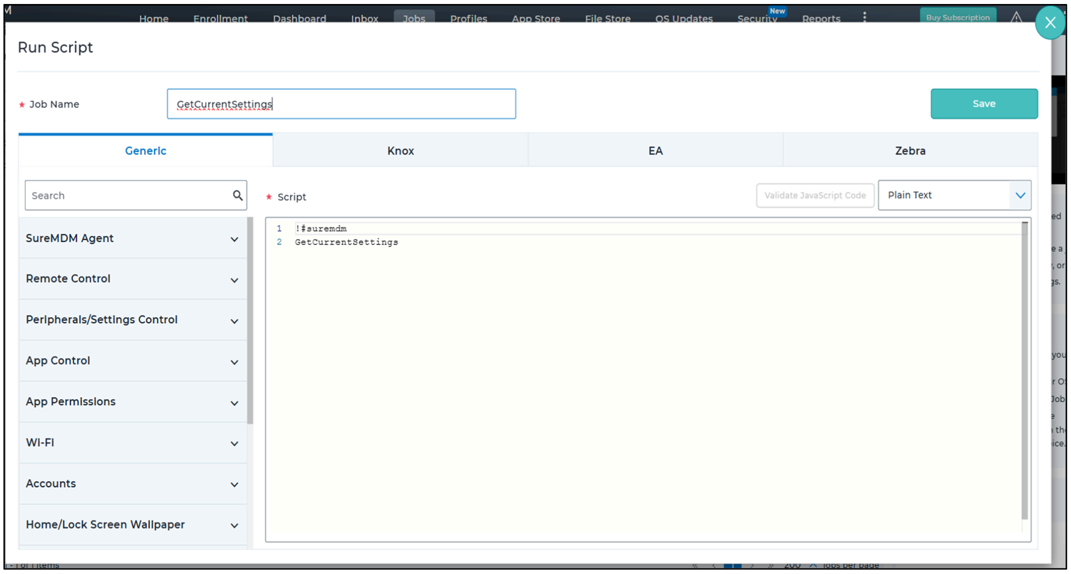
e) Click **Modify** to add the application to the allowed list.

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
```



* Job Name: GetCurrentSettings

* Script (Plain Text):

```
!#suremdm
GetCurrentSettings
```

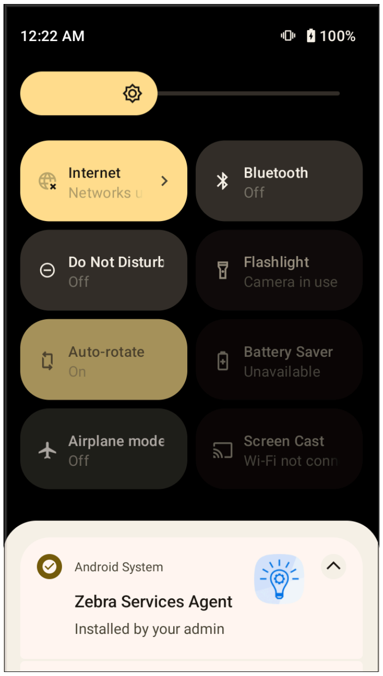
   b) Click **Save**.

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.



Internet
Networks u

Bluetooth
Off

Do Not Disturb
Off

Flashlight
Camera in use

Auto-rotate
On

Battery Saver
Unavailable

Airplane mode
Off

Screen Cast
Wi-Fi not conn

Android System

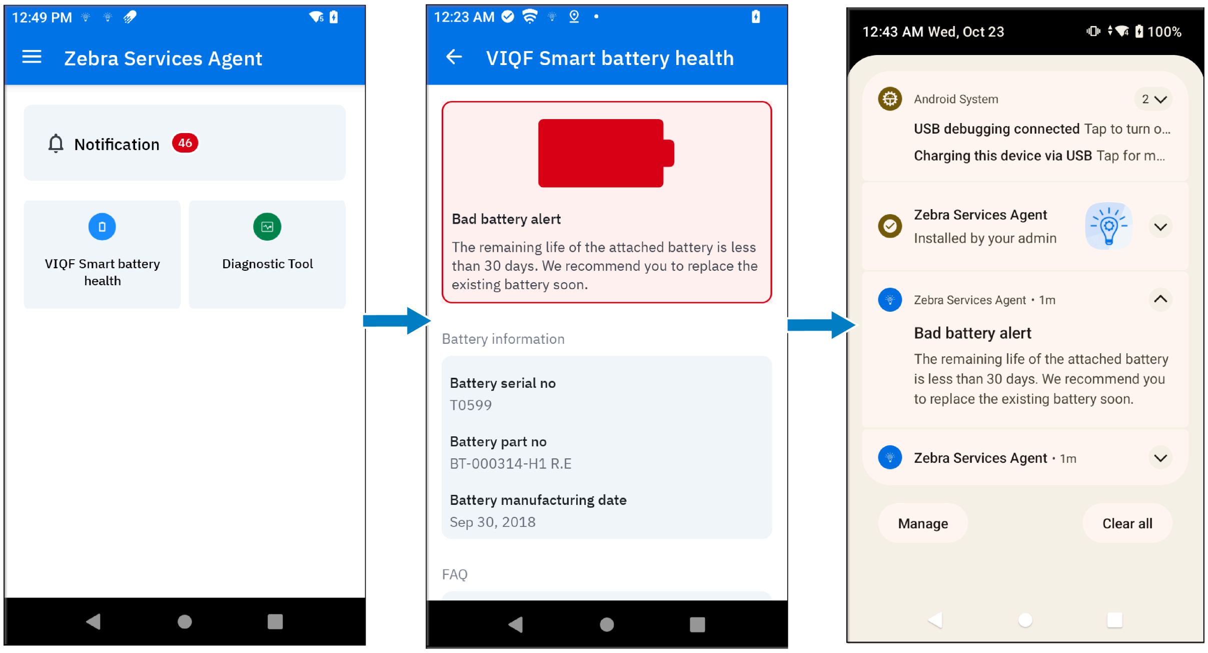
Zebra Services Agent

Installed by your admin

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.



12:49 PM

Zebra Services Agent

Notification 46

VIQF Smart battery health

Diagnostic Tool

12:23 AM

VIQF Smart battery health

Bad battery alert

The remaining life of the attached battery is less than 30 days. We recommend you to replace the existing battery soon.

Battery information

Battery serial no
T0599

Battery part no
BT-000314-H1 R.E

Battery manufacturing date
Sep 30, 2018

FAQ

12:43 AM Wed, Oct 23 100%

Android System 2

USB debugging connected Tap to turn o...

Charging this device via USB Tap for m...

Zebra Services Agent
Installed by your admin

Zebra Services Agent • 1m

Bad battery alert

The remaining life of the attached battery is less than 30 days. We recommend you to replace the existing battery soon.

Zebra Services Agent • 1m

Manage

Clear all

FAQs

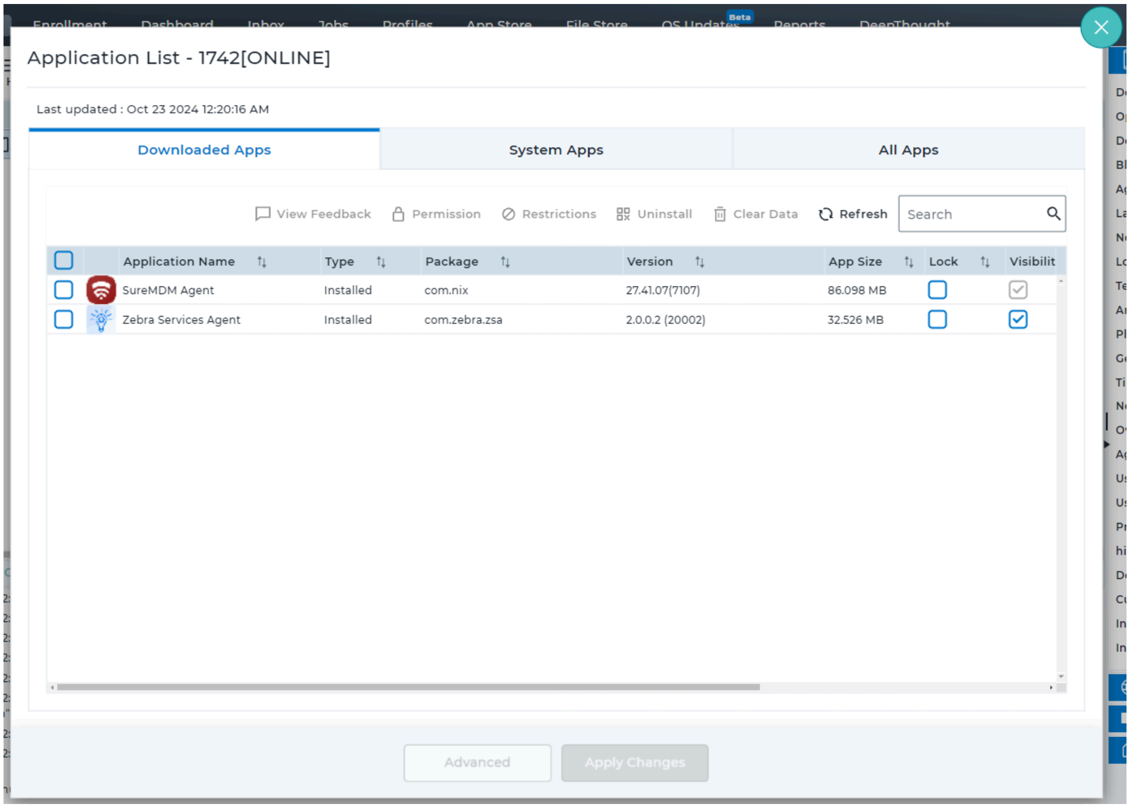
1. How do you determine which apps are installed on the devices in 42Gears?

   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.



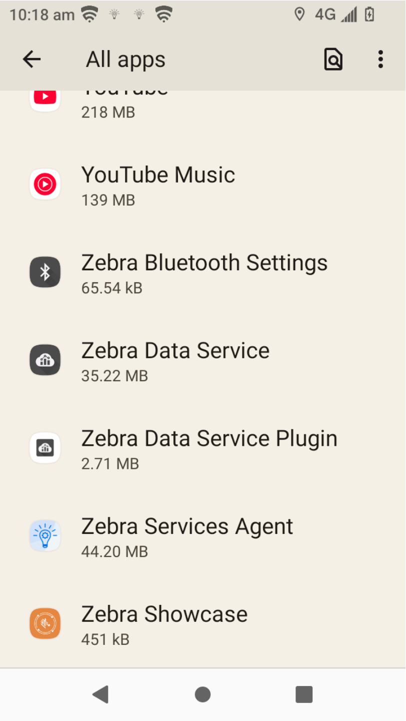
Application List - 1742[ONLINE]

Last updated : Oct 23 2024 12:20:16 AM

□		Application Name	Type	Package	Version	App Size	Lock	Visibilit
□		SureMDM Agent	Installed	com.nix	27.41.07(7107)	86.098 MB	□	☑
□		Zebra Services Agent	Installed	com.zebra.zsa	2.0.0.2 (20002)	32.526 MB	□	☑

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**.



10:18 am 4G

All apps

YouTube
218 MB

YouTube Music
139 MB

Zebra Bluetooth Settings
65.54 kB

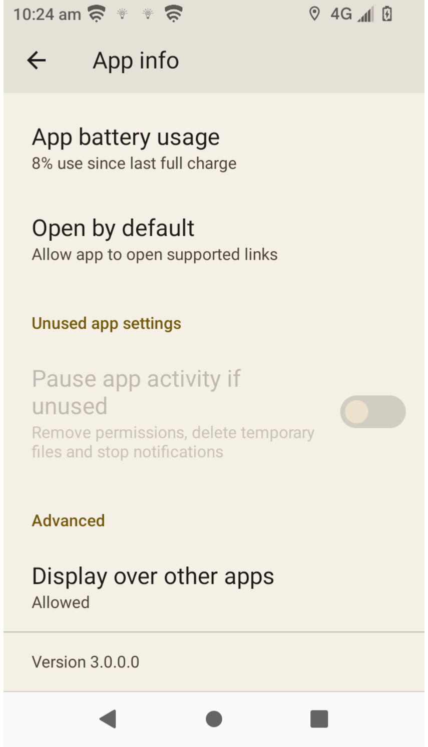
Zebra Data Service
35.22 MB

Zebra Data Service Plugin
2.71 MB

Zebra Services Agent
44.20 MB

Zebra Showcase
451 kB

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



10:24 am 4G

App info

App battery usage
8% use since last full charge

Open by default
Allow app to open supported links

Unused app settings

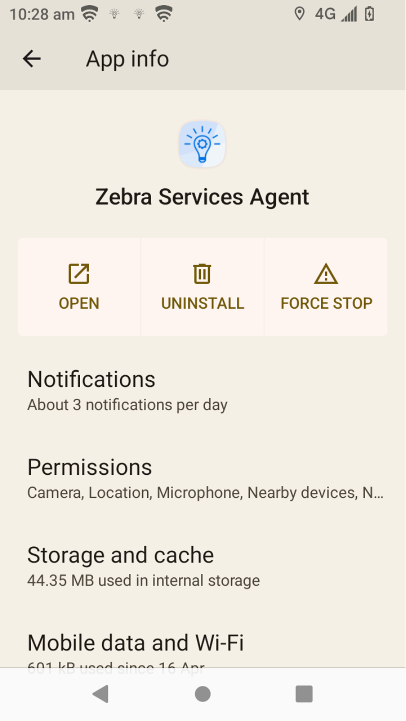
Pause app activity if unused
Remove permissions, delete temporary files and stop notifications

Advanced

Display over other apps
Allowed

Version 3.0.0.0

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



Zebra Services Agent

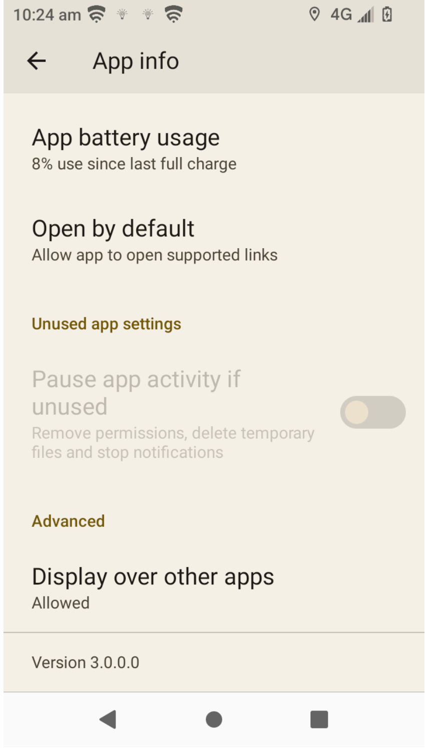
Notifications
About 3 notifications per day

Permissions
Camera, Location, Microphone, Nearby devices, N...

Storage and cache
44.35 MB used in internal storage

Mobile data and Wi-Fi
601 kB used since 16 Apr

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



App battery usage
8% use since last full charge

Open by default
Allow app to open supported links

Unused app settings

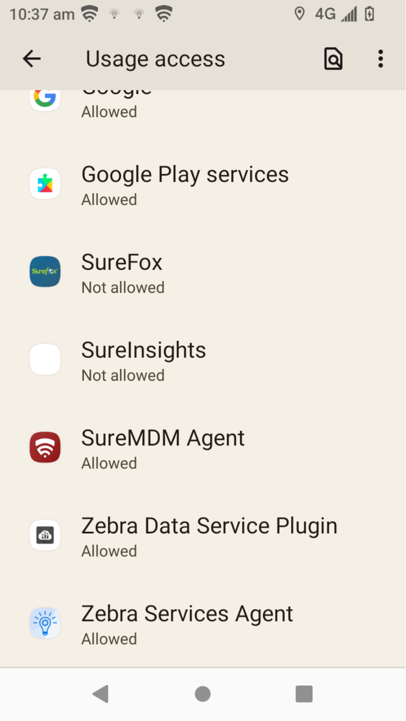
Pause app activity if unused
Remove permissions, delete temporary files and stop notifications

Advanced

Display over other apps
Allowed

Version 3.0.0.0

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



10:37 am 4G

Usage access

Google
Allowed

Google Play services
Allowed

SureFox
Not allowed

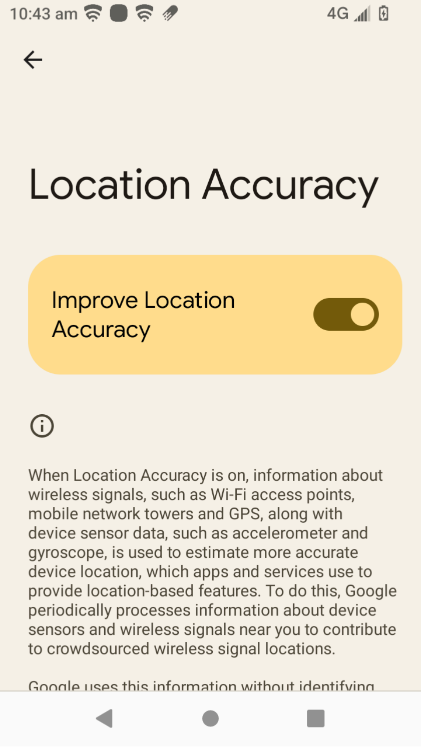
SureInsights
Not allowed

SureMDM Agent
Allowed

Zebra Data Service Plugin
Allowed

Zebra Services Agent
Allowed

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**.



10:43 am 4G

Location Accuracy

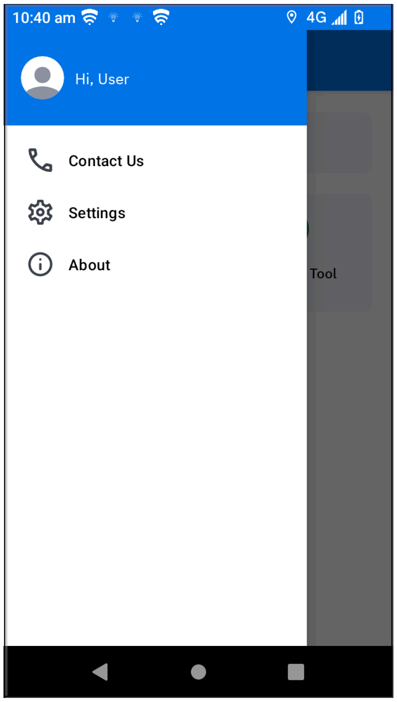
Improve Location Accuracy

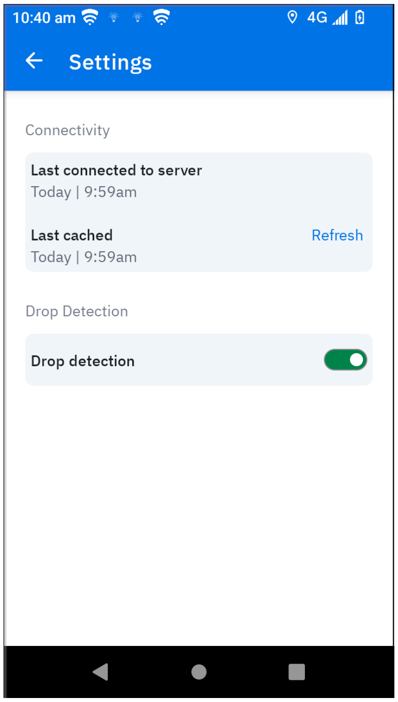
When Location Accuracy is on, information about wireless signals, such as Wi-Fi access points, mobile network towers and GPS, along with device sensor data, such as accelerometer and gyroscope, is used to estimate more accurate device location, which apps and services use to provide location-based features. To do this, Google periodically processes information about device sensors and wireless signals near you to contribute to crowdsourced wireless signal locations.

Google uses this information without identifying

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

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





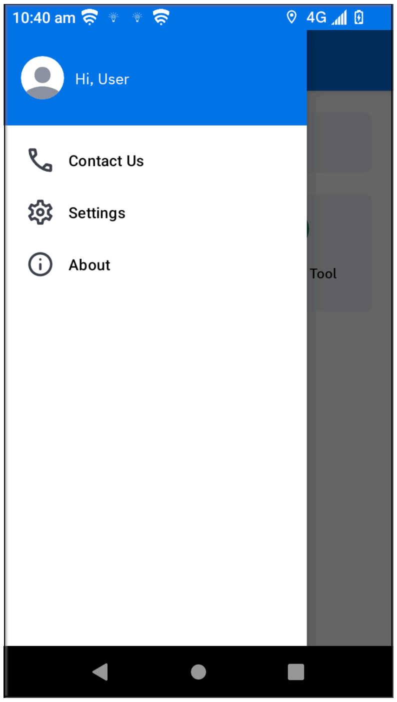
Last connected to server
Today | 9:59am

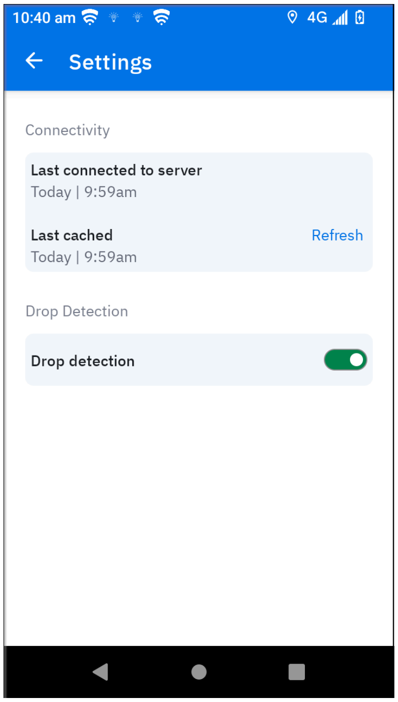
Last cached
Today | 9:59am

Drop detection: on

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.





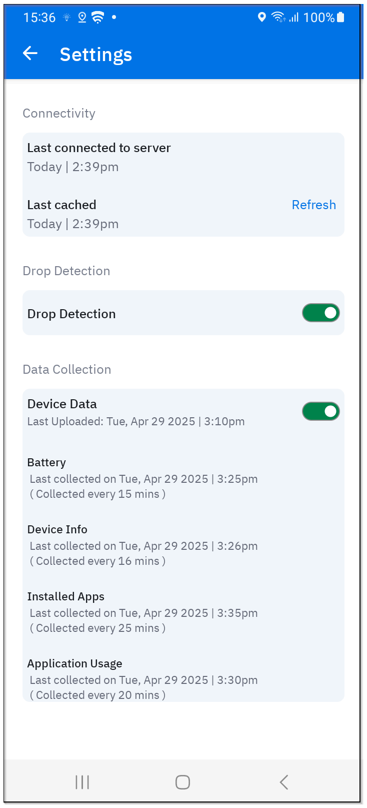
Last connected to server
Today | 9:59am

Last cached
Today | 9:59am

Drop detection: on

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

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



15:36 100%

Settings

Connectivity

Last connected to server
Today | 2:39pm

Last cached — Refresh
Today | 2:39pm

Drop Detection

Drop Detection — On

Data Collection

Device Data — On
Last Uploaded: Tue, Apr 29 2025 | 3:10pm

Battery
Last collected on Tue, Apr 29 2025 | 3:25pm
(Collected every 15 mins)

Device Info
Last collected on Tue, Apr 29 2025 | 3:26pm
(Collected every 16 mins)

Installed Apps
Last collected on Tue, Apr 29 2025 | 3:35pm
(Collected every 25 mins)

Application Usage
Last collected on Tue, Apr 29 2025 | 3:30pm
(Collected every 20 mins)

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.