Zebra Services Agent for Omnissa Workspace ONE

Installation Guide

MN-005030-05EN Rev A

ZEBRA

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

Copyright

2026/10/09

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

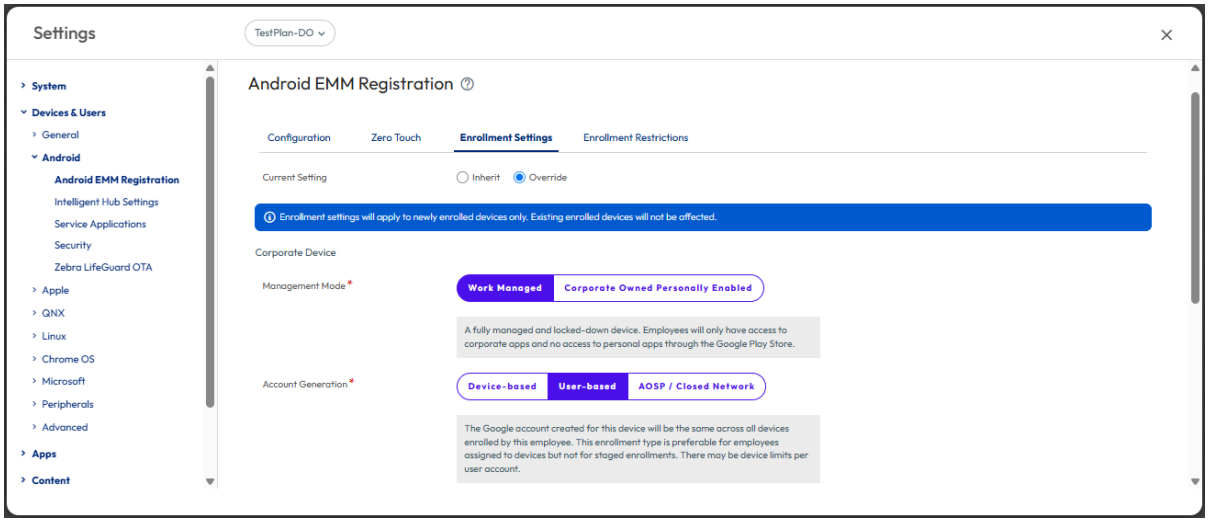
VMware AirWatch is an Enterprise Mobility Management (EMM) solution that enables companies to securely manage devices and endpoints with any form factor and operating system throughout their lifecycle, from deployment to retirement.

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

Pre-requisite

Devices must be enrolled as **Work Managed** with AirWatch Hub application.

1. To verify if devices are configured as **Work Managed**, log into the **AirWatch Console**.
2. Select **Groups & Settings** > **All Settings** > **Devices & Users** > **Android** > **Android EMM Registration** > **Enrollment Settings**.
3. Verify the two settings below under **Enrollment Settings**.



- Management Mode for Corporate Devices: **WORK MANAGED**
- Google Account Generation for Corporate Devices: **USER-BASED**

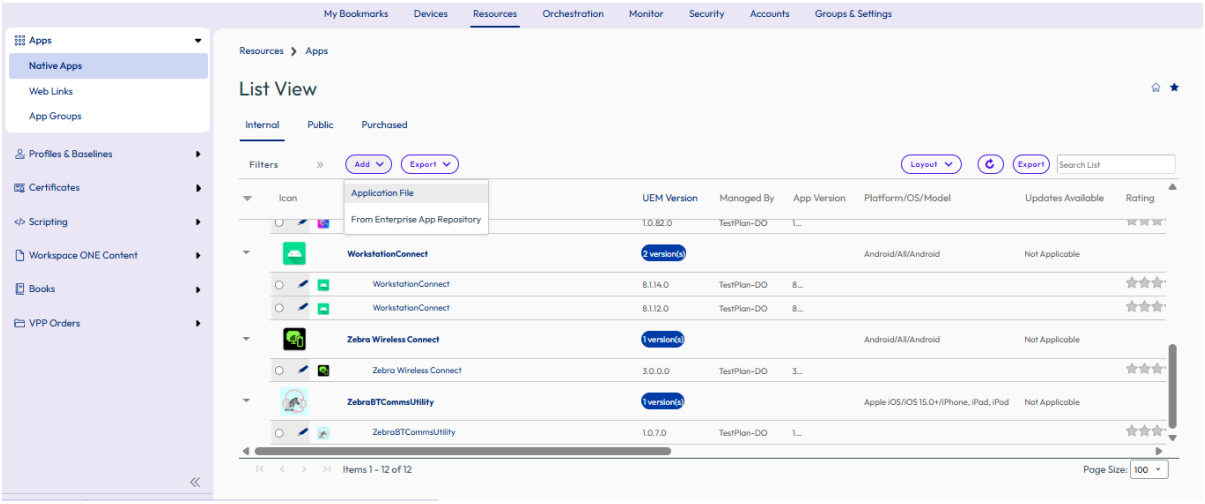
4. Click **Save**.

Deploying Zebra Services Agent

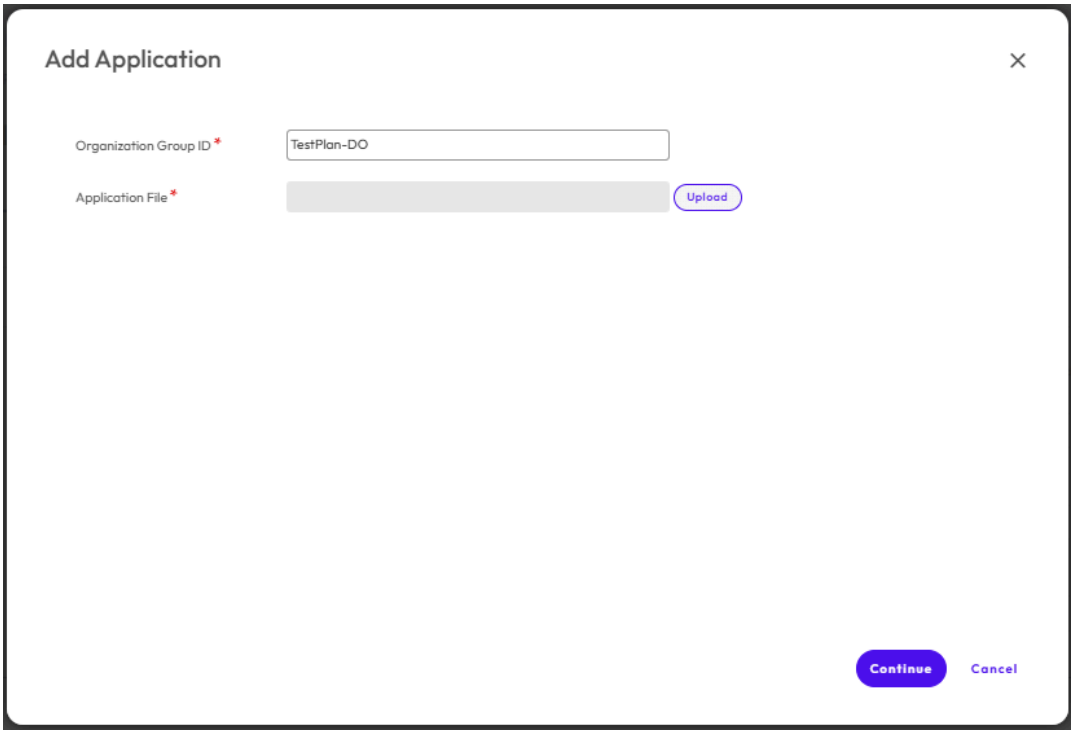
Install the Zebra Services Agent (ZSA) app on the devices.

Download the `Zebra_Service_Agent_V5.0.0.x.apk` file from zebra.com/zebra-services-agent.

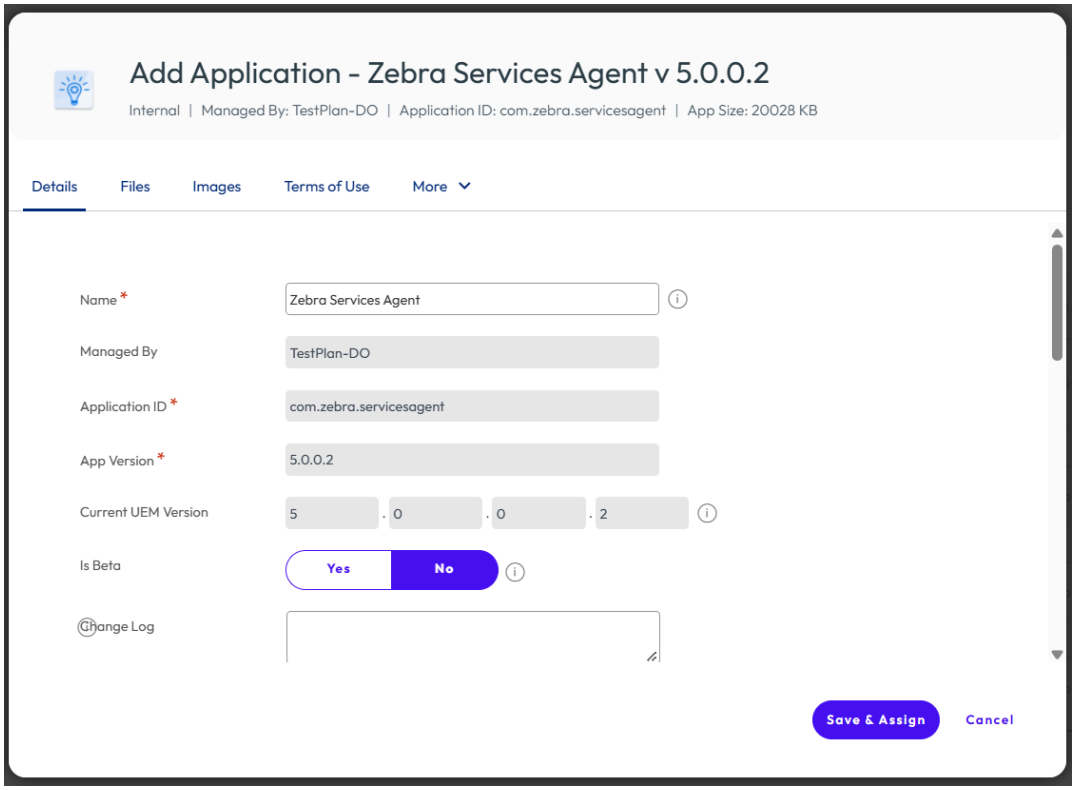
1. Log into the **AirWatch Console**.
2. Click **Resources** > **Apps** > **Native Apps** > **List View** > **Add** > **Application File**.



3. Upload the **ZSA APK** file, and click **Continue**.

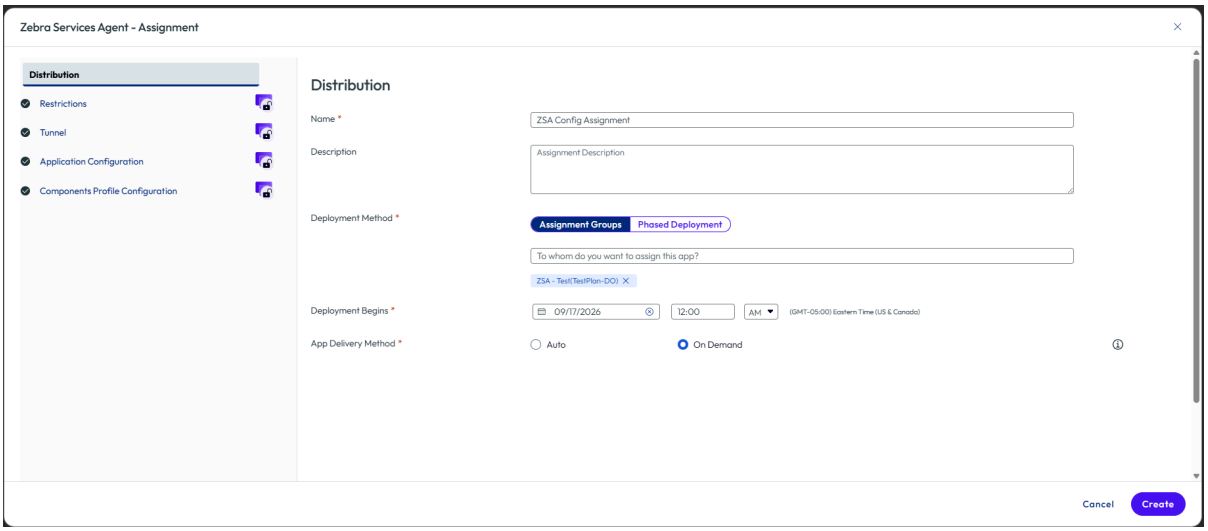


4. Click **Save & Assign**.



The next screen prompts to configure application assignment parameters.

5. Assignment Configuration:
   a. Enter a distribution **Name**.
   b. Add **Assignment Groups**, the organization groups created during registration.
   c. Select the **App Delivery Method** to **Auto**.

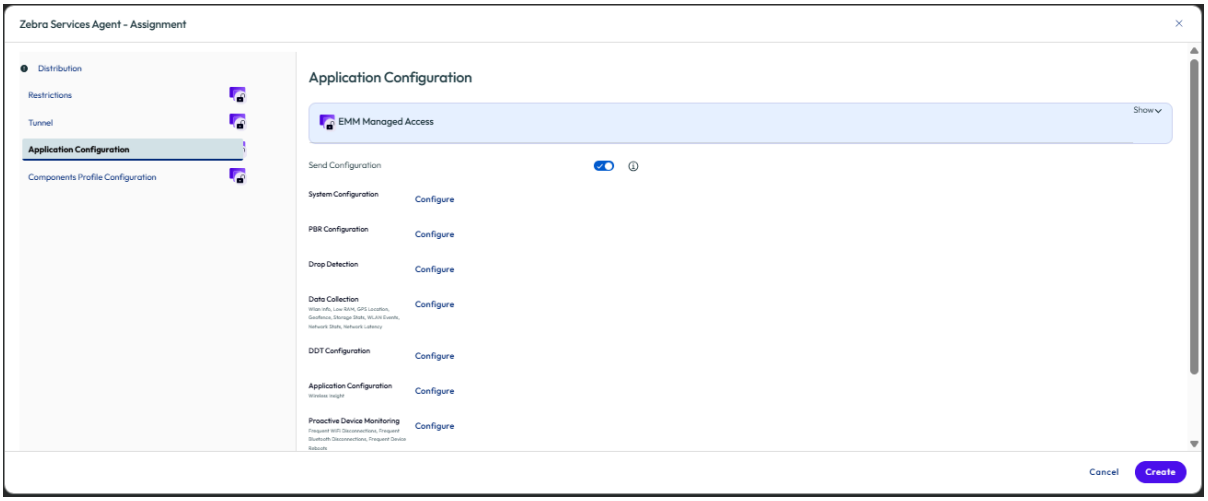


   d. Click **Create**.

6. Managed Configuration:

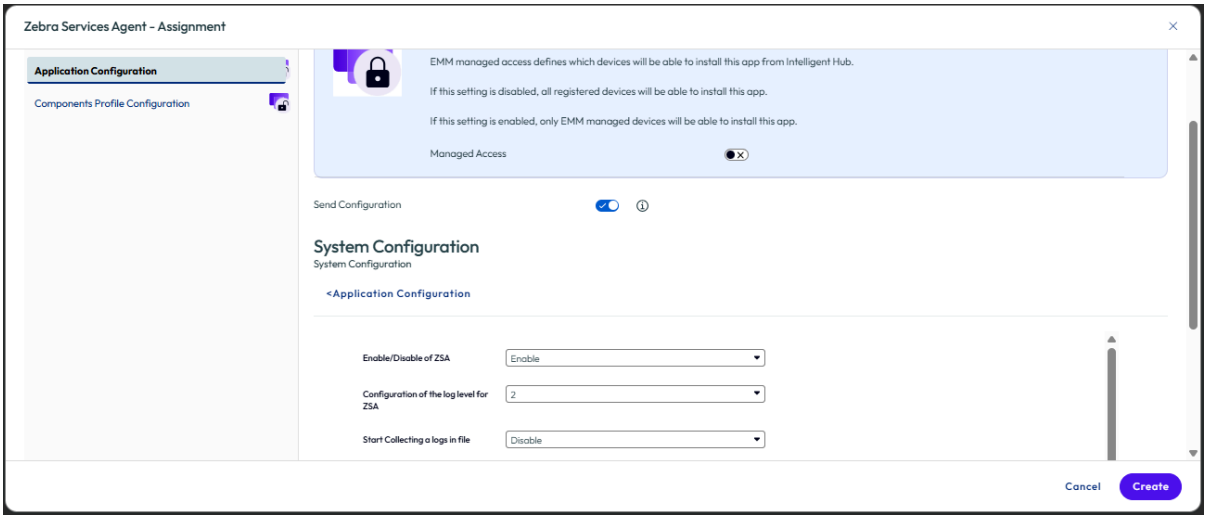
a. The ZSA Managed Configuration contains seven modules, each with an enable/disable feature to set the configuration.

b. To set the configurations for devices, go to **Application Configuration** > **Send Configuration**.

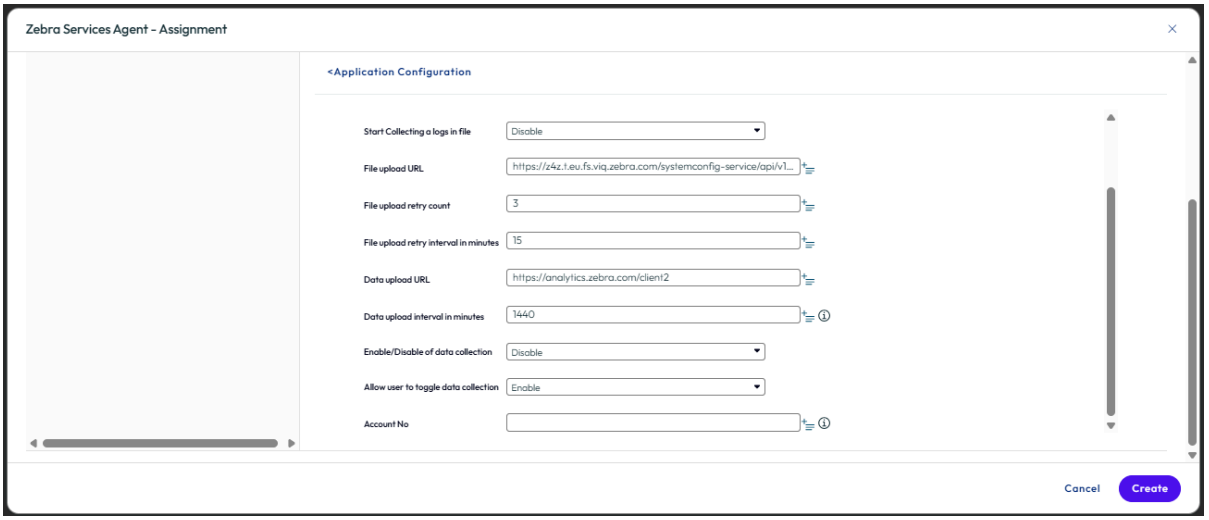


c. Under the **System Configuration**, enable the **ZSA Configuration** option and set the **Configuration of the log level for ZSA** with the following values:

- 0: Info
- 1: Debug
- 2: Sensitive



d. Enable the **Start Collecting a logs in file** option.



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 details of data collection. -
- **Data Upload Interval in minutes**: Sets the frequency of uploads, defaulting to 24 hours (or 1440 minutes), with a minimum allowed interval of 15 minutes.

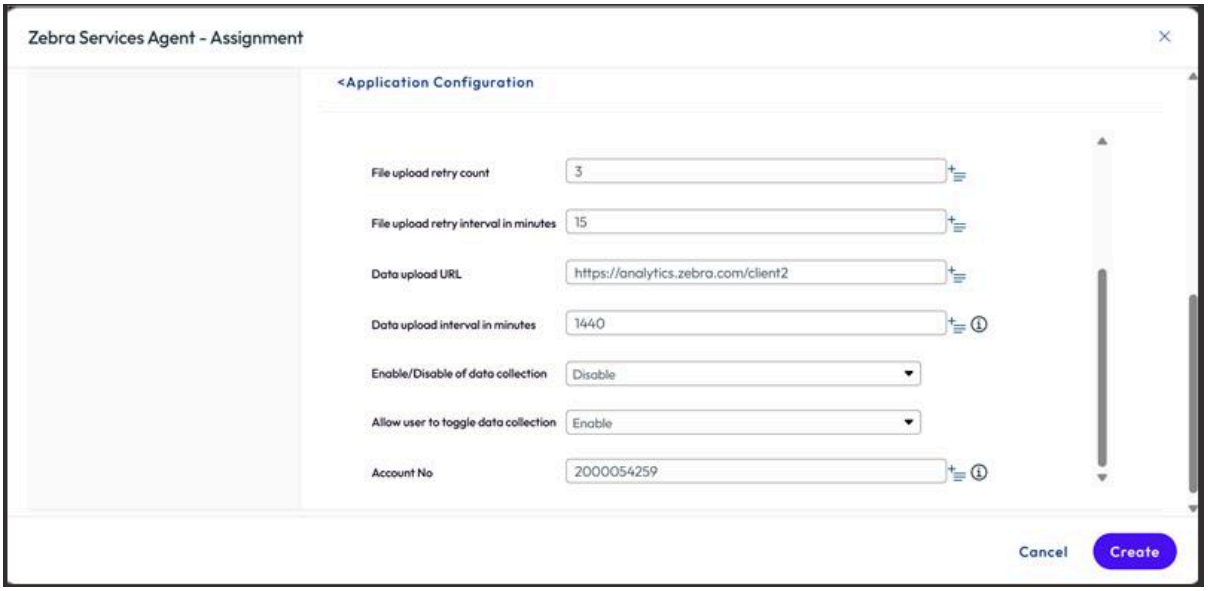
g. Data collection settings for non-Zebra devices:

- **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.

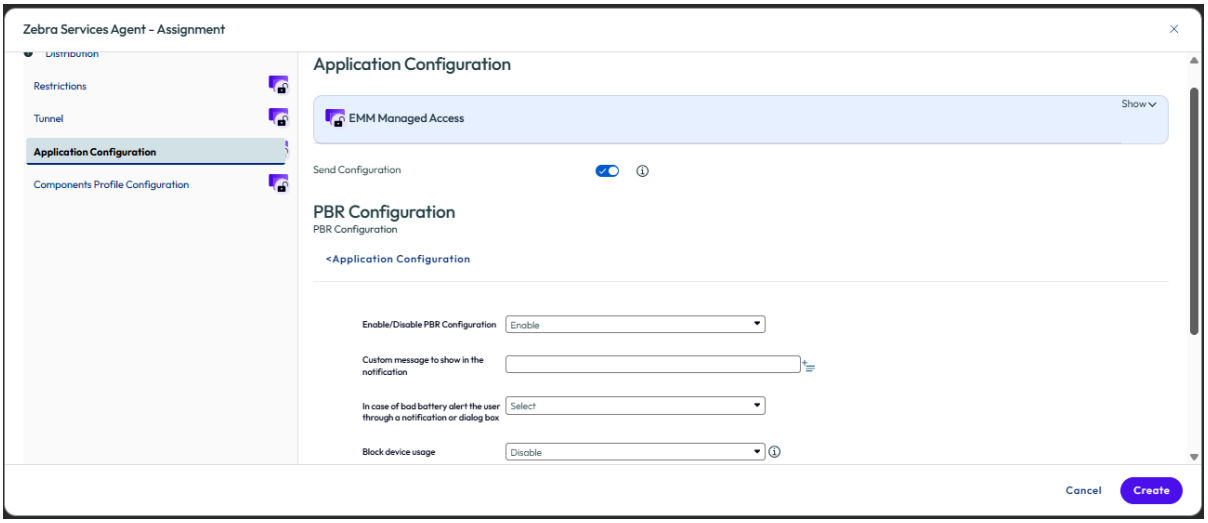
h. **Mandatory Setup for Non-Zebra Devices**

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

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



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

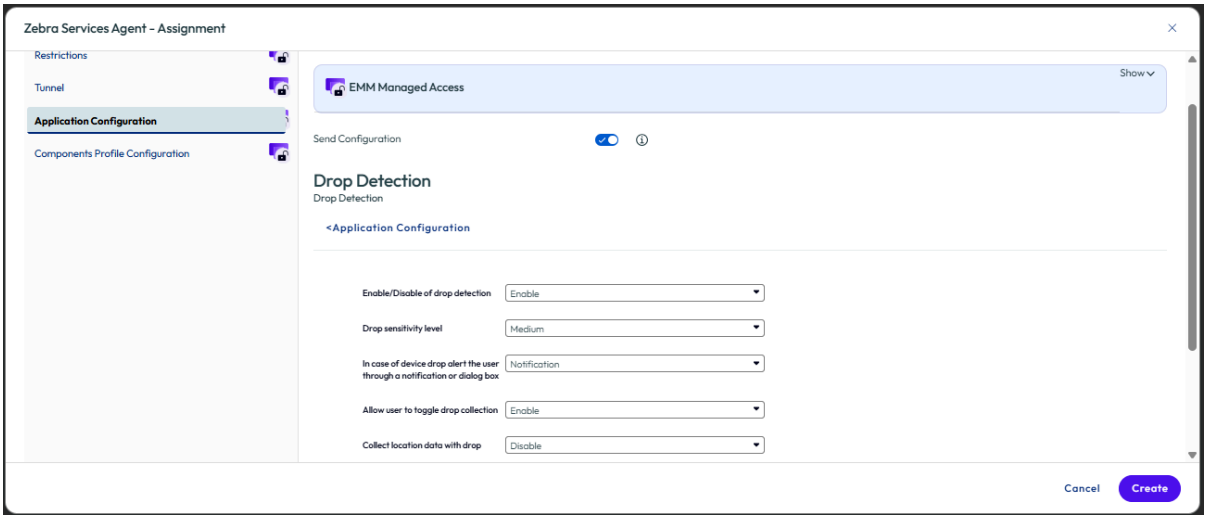


j. Set the **Dialog** in **In case of bad battery alert the user through a notification or dialog box** from the following values:

- Notification
- Dialog
- Alert Dialog 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. In the **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 **Notification** in the **In case of device drop alert the user through a notification or dialog box** with the following values:

- Notification
- Alert Dialog
- Alert Dialog 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 **Collection location data with drop** allows to capture location(lat-long) data of the device when device drop occurs.

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

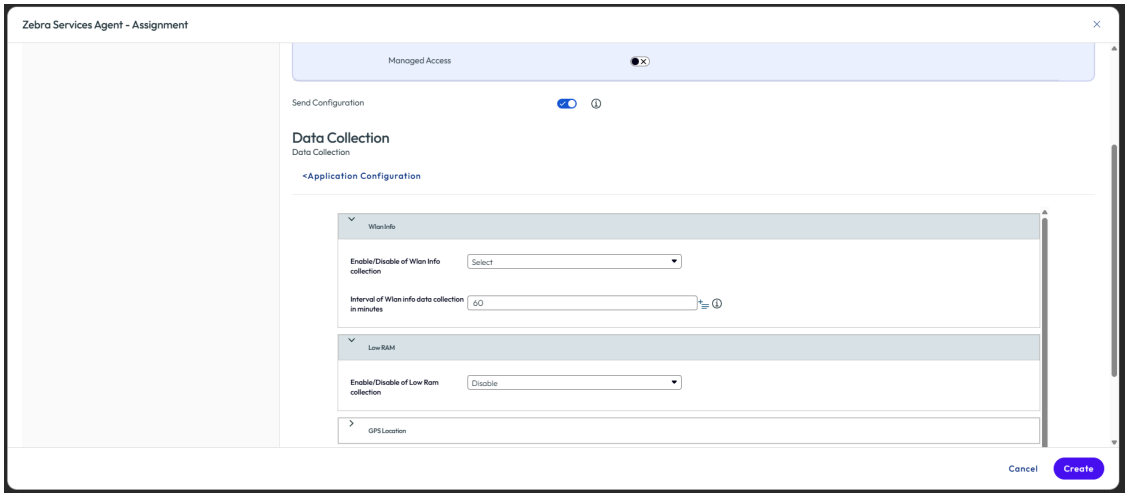
Default enabled data collections:

- **Battery**
- **Device Info**
- **Application List and Events**
- **Application Usage**
- **Battery Events**
- **Bluetooth Events**
- **RAM Stats**
- **Flash Stats**
- **Utilization**
- **WWAN Information**

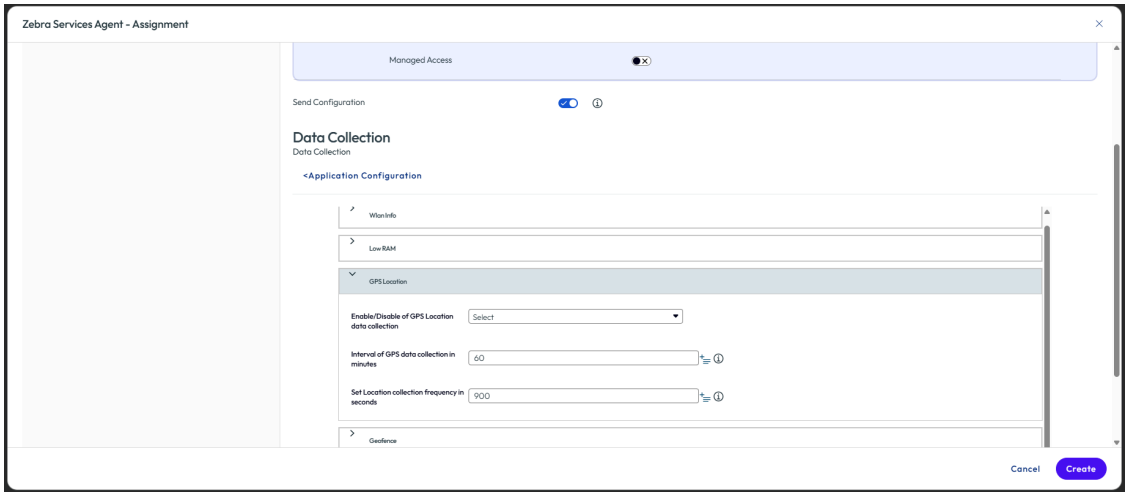
- **Screen Brightness**
- **WLAN Stats**
- **Device Usage**
- **Feature Usage**
- **Doze Mode**
- **Scanner Info**

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.

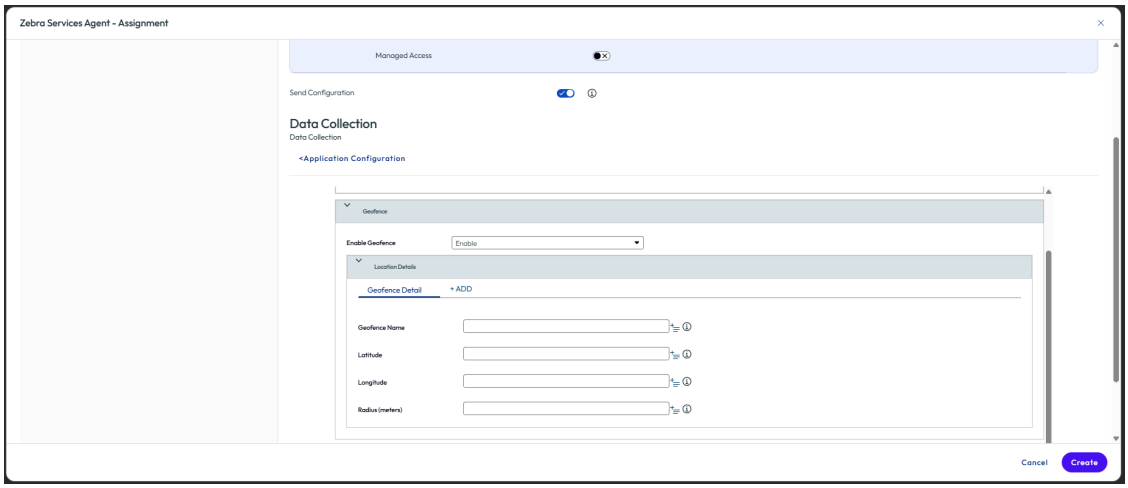


- **GPS Location**: Track the device by enabling the **Enable/Disable of GPS location data collection** option and set the **Interval of GPS data collection in minutes**.

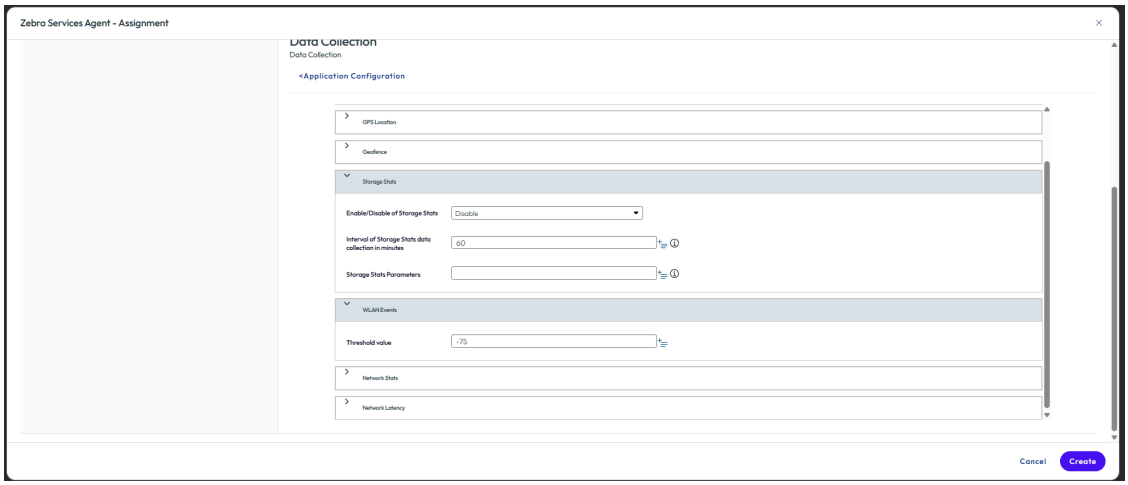


- **Geofence**: Receive notifications when the device leaves a predefined area by enabling **Enable Geofence** option and add **Location Details** information as follows:
  - **Geofence Name**: Name of the area.

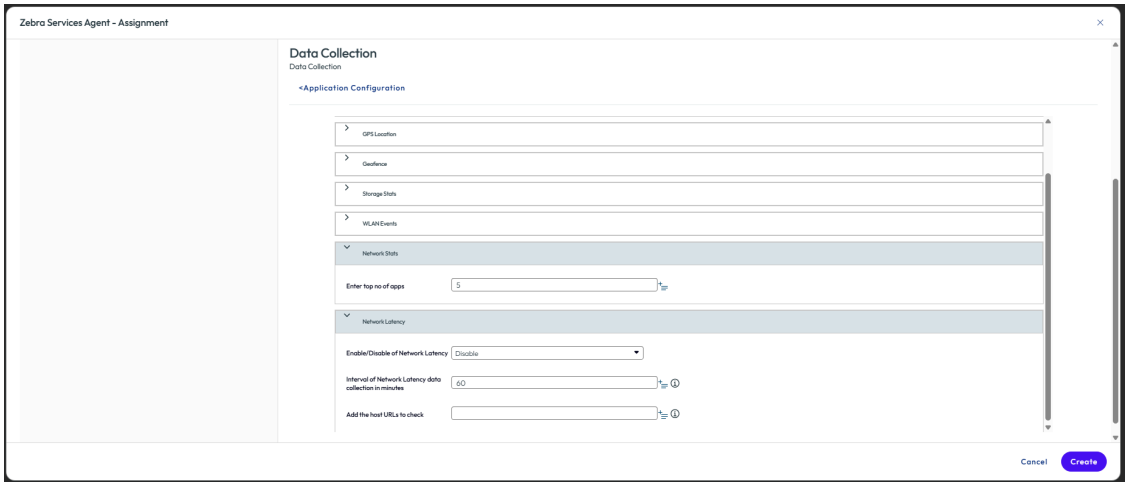
- **Latitude & Longitude**: Coordinates of the specific area.
- **Radius (meters)**: The radius in meters to cover around the specified latitude and longitude.



- **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.



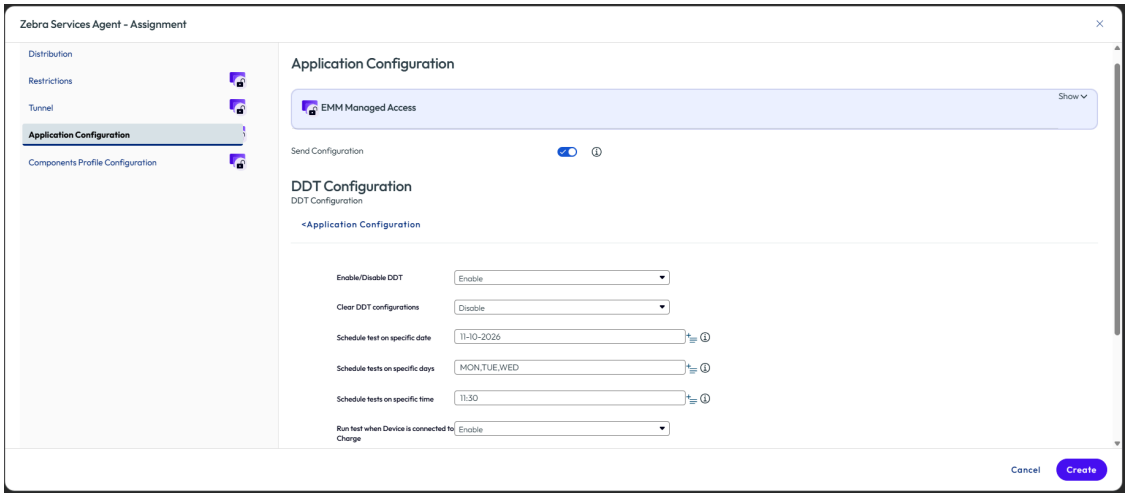
- **Network Stats**: Enabled by default and cannot be disabled. The admin can adjust the top no of app counts.
- **Network Latency:** Disabled by default, if enabled record network performance details for configured host URLs, including the target host, measured latency, network type, signal strength,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



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

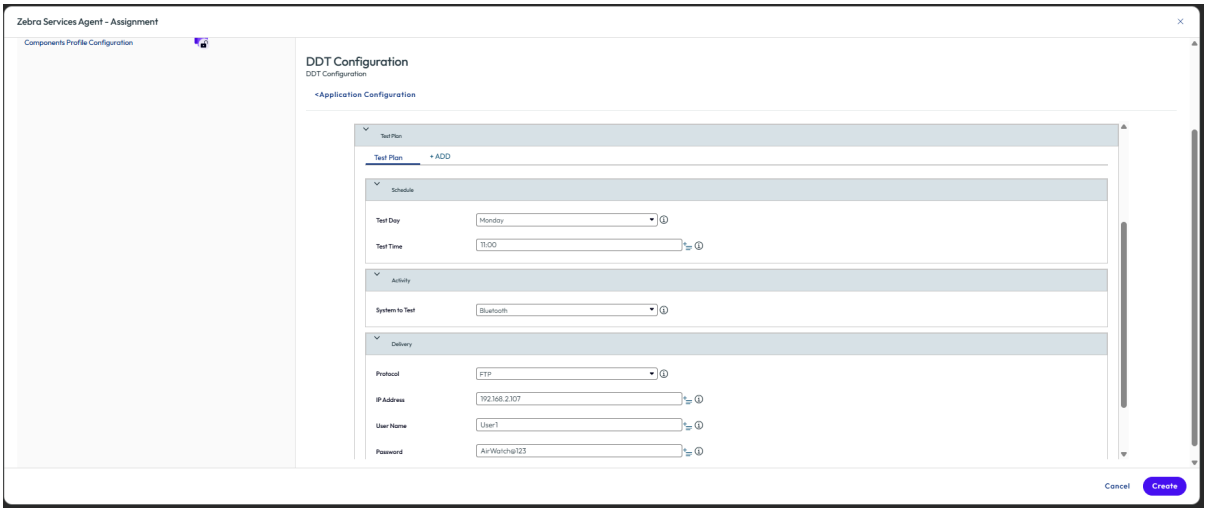
r. In the **DDT Configuration** section:

- 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 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.
- **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.



- Click **Add** in the **Test Plan** section.

s. Configure the **Test Plan** and click **Save**.

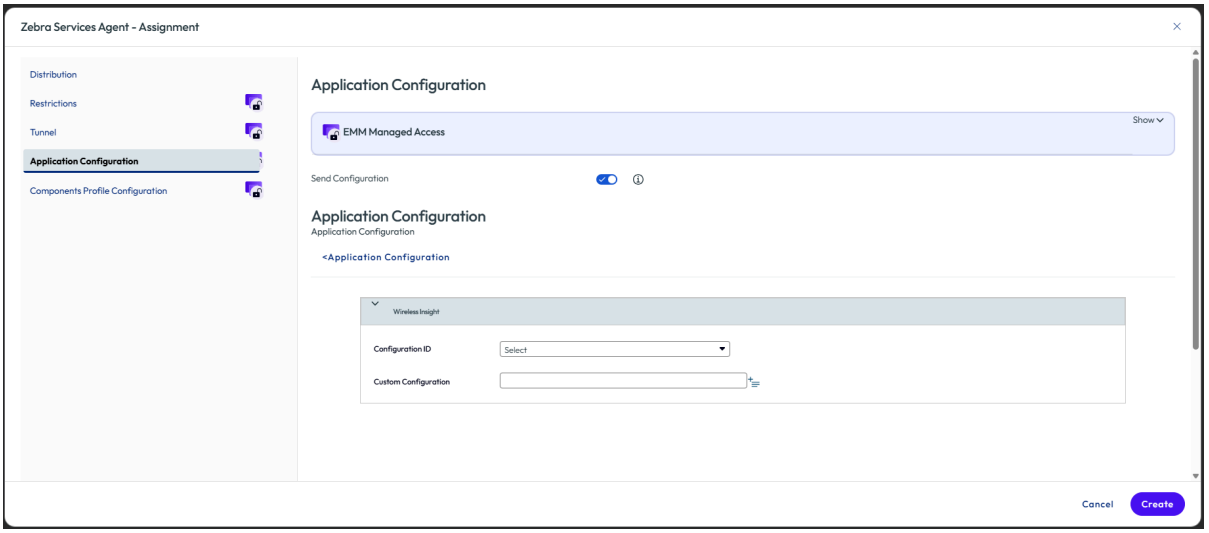


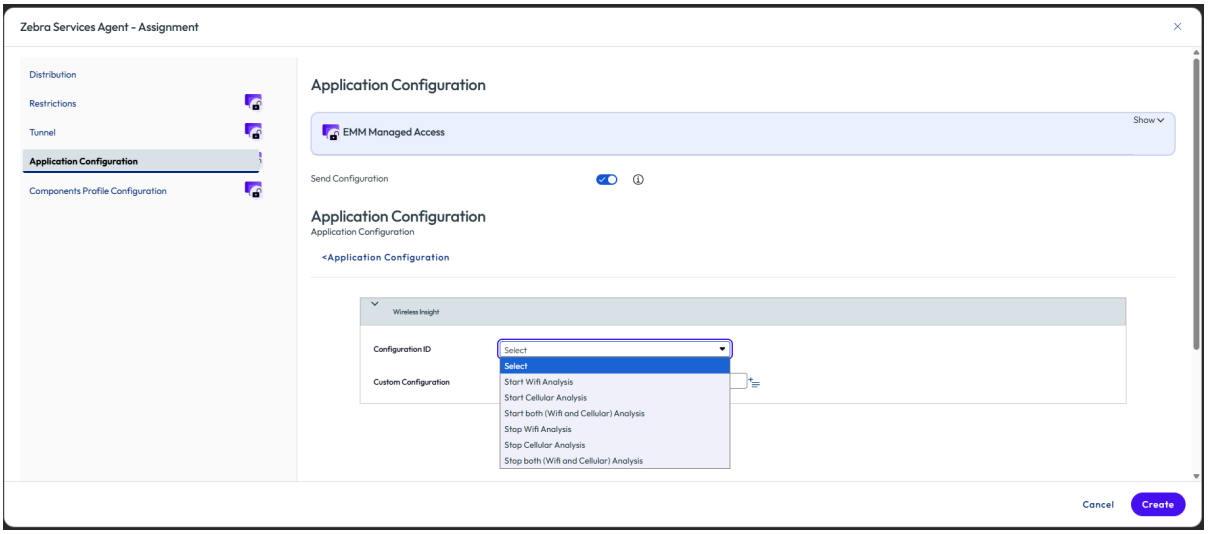
t. The **Application Configuration** is designated for Zebra devices. It currently supports the **Wireless Insight** application and the **ZDS** application, with more applications to be supported in the future.

u. The **Wireless Insight** application can be 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.

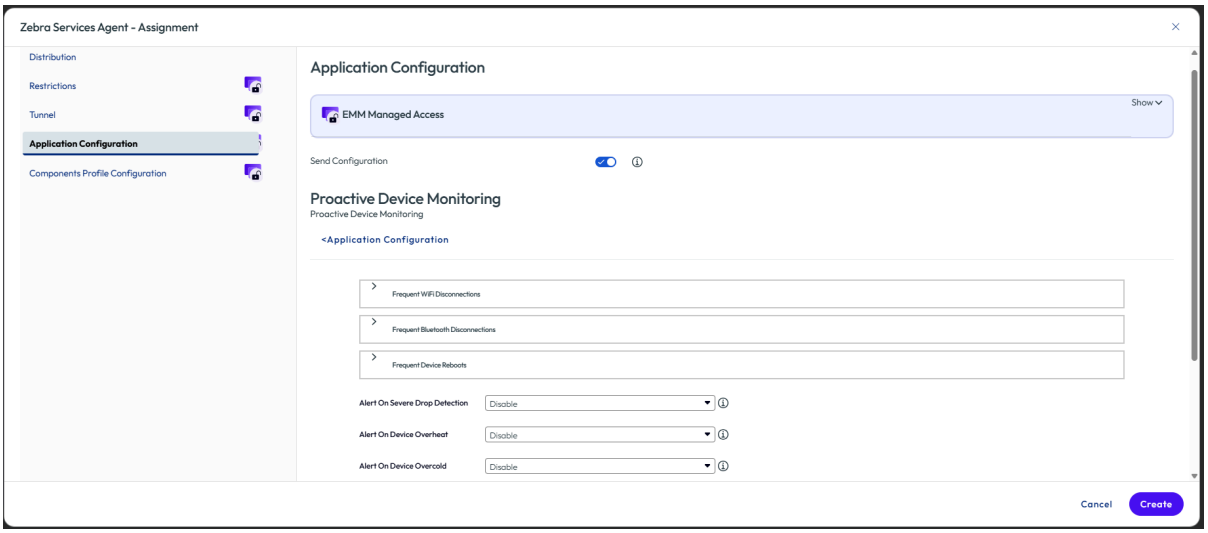
v. The **ZDS** can be configured through VIQ with a custom ZDS configuration.





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

- **Frequent Wi-Fi Disconnections**
- **Frequent Bluetooth Disconnections**
- **Frequent Device Reboots**
- **Alert on Severe Drop Detection**
- **Alert on Device Overheat**
- **Alert on Device Over cold**



1. **Frequent Wi-Fi Disconnections**

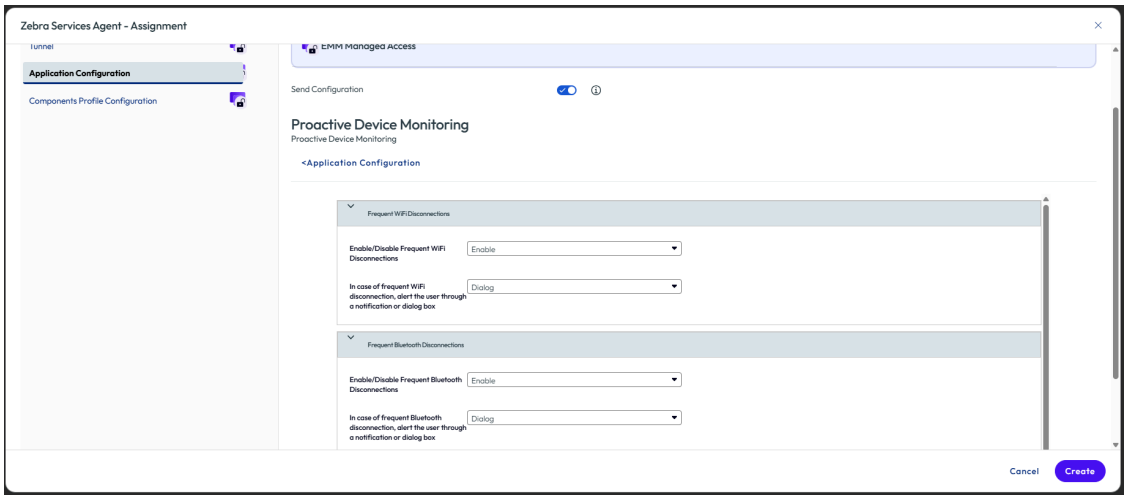
   Enable the **Enable/Disable Frequent Wi-Fi Disconnections** and set **Dialog** in the **in case of Frequent Wi-Fi disconnection, alert the user through a notification or dialog box** with the following values:

   - Notification
   - Dialog

2. **Frequent Bluetooth Disconnections**

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

- Notification
- Dialog



3. **Frequent Device Reboots**

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

   - Notification
   - Dialog

4. **Alert on Severe Drop Detection**

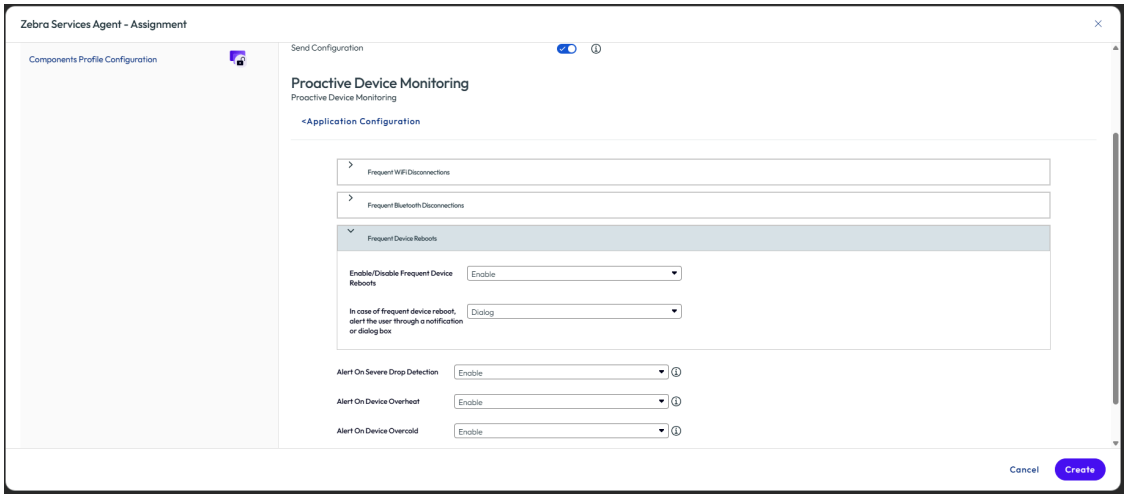
   Disabled by default. When enabled by an administrator, this feature allows the device to receive commands from ZDS upon detecting a severe drop.

5. **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.

6. **Alert on Device Over cold**

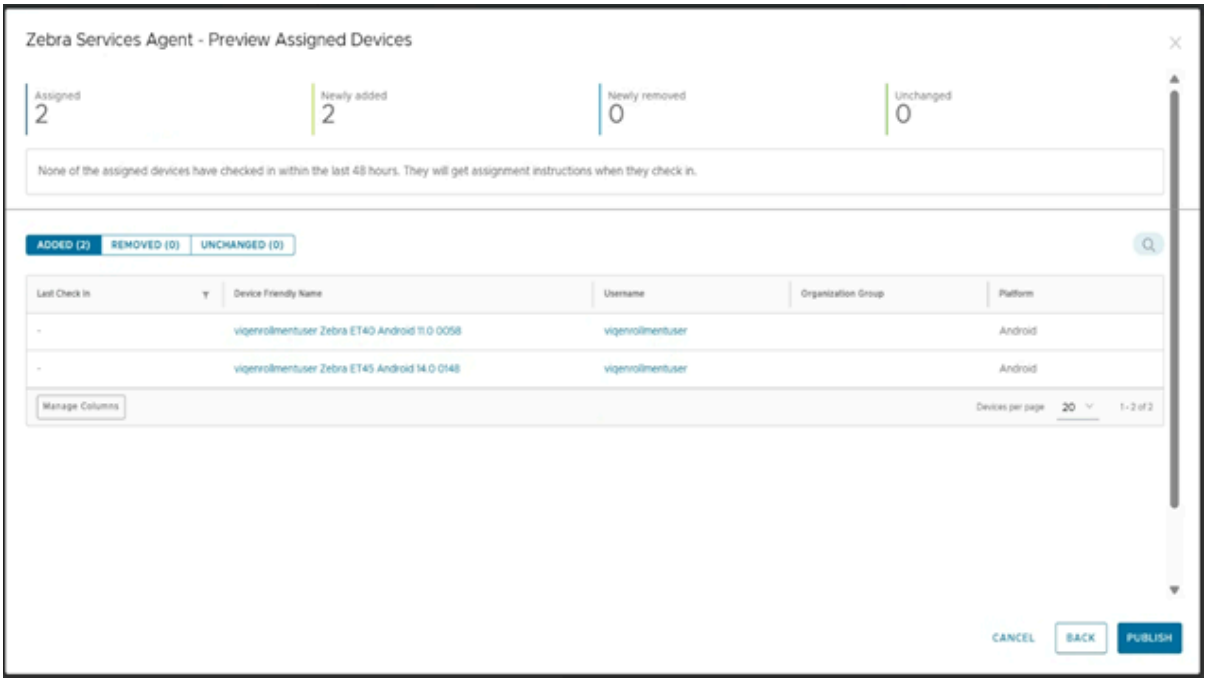
   Disabled by default. When enabled by an administrator, this feature allows the device to receive commands from ZDS upon detecting an under-temperature or overcooling event.



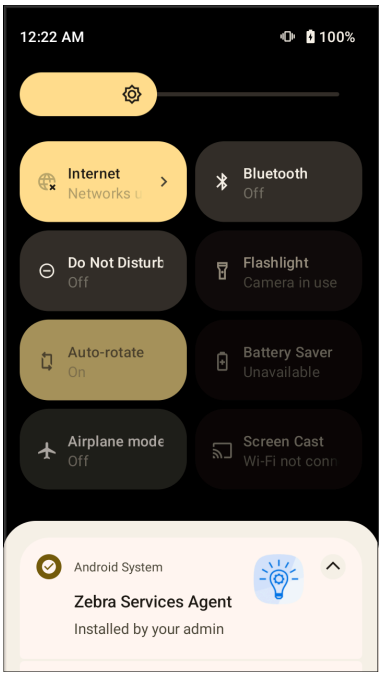
The ZSA Assignment page displays.



x. Preview the **Assigned Devices** to ensure only the target devices are listed, then click **Publish**.



The application is now installed on the devices.

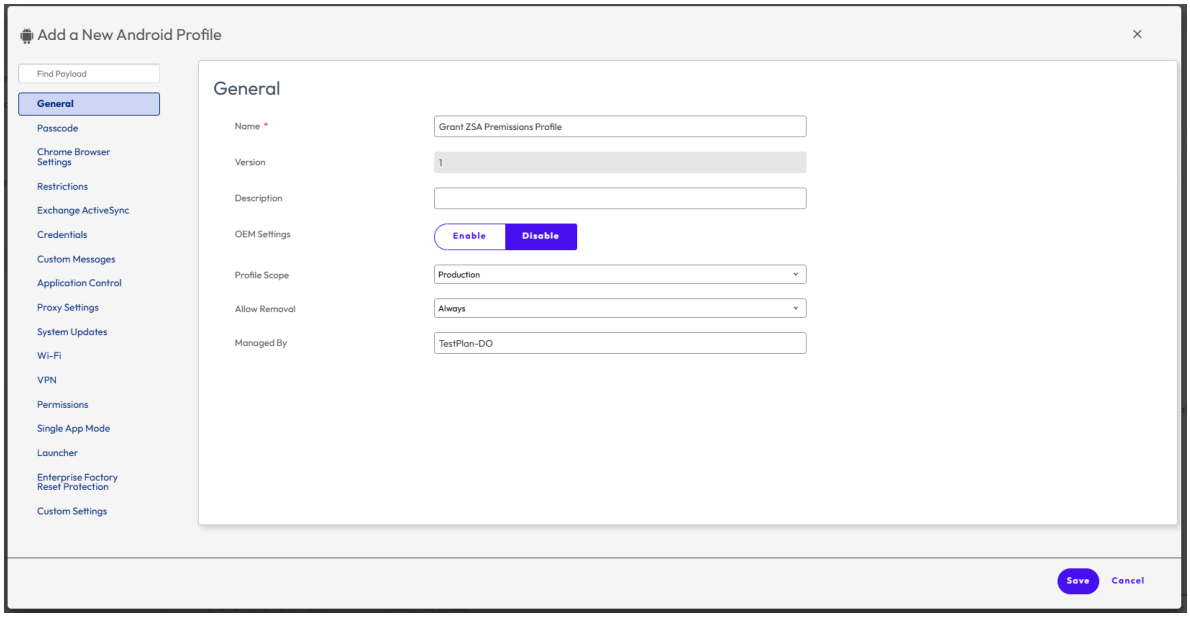


Auto-Grant Permissions for Zebra Services Agent

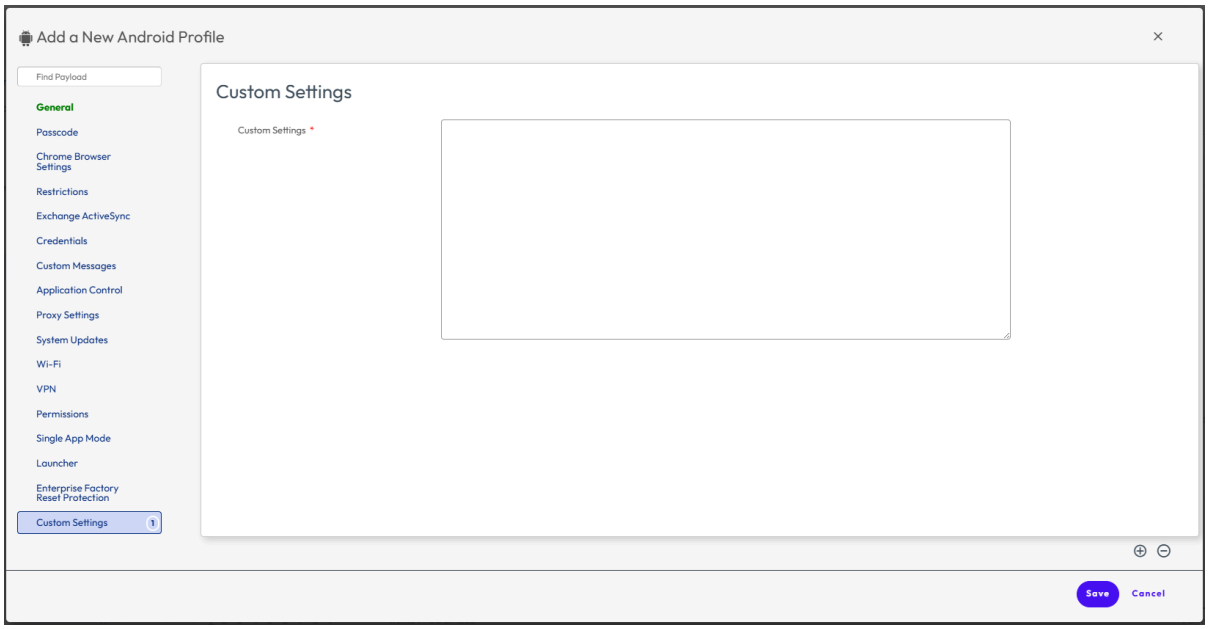
To add the automatic permissions:

1. Select **Orchestration** > **Product Provisioning** > **Components** > **Product Profiles** > **Add Profiles** > **Android**.

   The **Add a New Android Profile** page display. Enter the name as **Grant ZSA Permissions Profile**.



2. Scroll down to **Custom Settings**, select **Configure**, and then add the below script:




```
<characteristic uuid="e135b2b0-e9ac-4dd2-8b92-65eb259dc301 "
 type="com.airwatch.android.androidwork.permissions"target="1"><parm
 name="MasterRuntimePermission" value="1" type="integer" /><parm name
 ="AppLevelRuntimePermissions"
 value="W3sicGFja2FnZU5hbWUiOiJjb20uemVicmEuenNhIiwicGVybWlzc2lvbnMi
Olt7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uV1JJVEVfQ09OVEFDVFMiLCJ2YWx1ZSI6
IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQ0FMTF9QSE9ORSIsInZhbHVlIjoi
MSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUNPUkRfQVVESU8iLCJ2YWx1ZSI6
IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkVBRF9DT05UQUNUUyIsInZhbHVl
IjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5JTlRFUk5FVCIsInZhbHVlIjoi
```

```
MSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX1NFVFRJTkdTIiwidmFsdWUi
OiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLlJFQURfUEhPTkVfU1RBVEUiLCJ2
YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkVBRF9FWFRFUk5BTF9T
VE9SQUdFIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRF
X0VYVEVSTkFMX1NUT1JBR0UiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1p
c3Npb24uUkVBRF9QUk9GSUxFIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJt
aXNzaW9uLlVTRV9DUkVERU5USUFMUyIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQu
cGVybWlzc2lvbi5NQU5BR0VfQUNDT1VOVFMiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRy
b2lkLnBlcm1pc3Npb24uUkVBRF9TWU5DX1NUQVRTIiwidmFsdWUiOiIxIn0seyJuYW1lIjoi
YW5kcm9pZC5wZXJtaXNzaW9uLlJFQURfU1lOQ19TVEFUUzUSHUyIsInZhbHVlIjoiMSJ9LHsi
bmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5XUklURV9TWU5DX1NFVFRJTkdTIiwidmFsdWUi
OiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLlJBSVNFRF9USFJFQURfUFJJT1JJ
VFkiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUE9TVF9OT1RJ
RklDQVRJT05TIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLlJF
QURfUFJJVklMRUdFRF9QSE9ORV9TVEFURSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJv
aWQucGVybWlzc2lvbi5SRUNFSVZFX0JPT1RfQ09NUExFVEVEIiwidmFsdWUiOiIxIn0seyJu
YW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19ORVRXT1JLX1NUQVRFIiwidmFsdWUi
OiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19XSUZJX1NUQVRFIiwi
dmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLkNIQU5HRV9XSUZJX1NU
QVRFIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLkJMVUVUT09U
SCIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5CTFVFVE9PVEhf
QURNSU4iLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQkxVRVRP
T1RIX0NPTk5FQ1QiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24u
QkxVRVRPT1RIX1NDQU4iLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Np
b24uQkxVRVRPT1RIX0FEVkVSVElTRSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQu
cGVybWlzc2lvbi5SRUFEX1BIT05FX05VTUJFUlMiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJh
bmRyb2lkLnBlcm1pc3Npb24uU1lTVEVNX0FMRVJUX1dJTkRPVyIsInZhbHVlIjoiMSJ9LHsi
bmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5DQU1FUkEiLCJ2YWx1ZSI6IjEifSwKeyJuYW1l
IjoiYW5kcm9pZC5wZXJtaXNzaW9uLlJFQURfQVBQX1NQRUNJRklDX0xPQ0FMRVMiLCJ2YWx1
ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uSElHTl9TTUFQTElOR19SQVRF
X1NFTlNPUlMiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQUND
RVNTX0NPQVJTRV9MT0NBVElPTiIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVy
bWlzc2lvbi5BQ0NFU1NfRklORV9MT0NBVElPTiIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFu
ZHJvaWQucGVybWlzc2lvbi5BQ0NFU1NfQkFDS0dST1VORF9MT0NBVElPTiIsInZhbHVlIjoi
MSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5RVUVSWV9BTExfUEFDS0FHRVMiLCJ2
YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUEFDS0FHRV9VU0FHRV9T
VEFUUyIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5GT1JFR1JP
VU5EX1NFUlZJQ0VfREFUQV9TWU5DIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5w
ZXJtaXNzaW9uLkZPUk9VTkRfU0VSVklDRSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJv
aWQucGVybWlzc2lvbi5GT1JFR1JPVU5EX1NFUlZJQ0VfUkVNT1RFX01FU1NBR0lORyIs
InZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5XQUtFX0xPQ0siLCJ2
YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uVVNFX0VYQUNUX0FMQVJN
IiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLk1BTkFHRV9FWFRF
Uk5BTF9TVE9SQUdFIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9u
LlNDSEVEVUxFX0VYQUNUX0FMQVJNIiwidmFsdWUiOiIxIn1dfV0=" type="string" /></
characteristic>
```


NOTE: The **AppLevelRuntimePermissions value** is encoded using the below permission JSON value into base64 via base64decode.org:


```
[{"packageName":"com.zebra.servicesagent","permissions":
 [{"name":"android.permission.WRITE_CONTACTS","value":"1"},
```

```
{"name":"android.permission.CALL_PHONE","value":"1"},
{"name":"android.permission.RECORD_AUDIO","value":"1"},
{"name":"android.permission.READ_CONTACTS","value":"1"},
{"name":"android.permission.INTERNET","value":"1"},
{"name":"android.permission.READ_SETTINGS","value":"1"},
{"name":"android.permission.READ_PHONE_STATE","value":"1"},
{"name":"android.permission.READ_EXTERNAL_STORAGE","value":"1"},
{"name":"android.permission.WRITE_EXTERNAL_STORAGE","value":"1"},
{"name":"android.permission.READ_PROFILE","value":"1"},
{"name":"android.permission.USE_CREDENTIALS","value":"1"},
{"name":"android.permission.MANAGE_ACCOUNTS","value":"1"},
{"name":"android.permission.READ_SYNC_STATS","value":"1"},
{"name":"android.permission.READ_SYNC_SETTINGS","value":"1"},
{"name":"android.permission.WRITE_SYNC_SETTINGS","value":"1"},
{"name":"android.permission.RAISED_THREAD_PRIORITY","value":"1"},
{"name":"android.permission.POST_NOTIFICATIONS","value":"1"},
{"name":"android.permission.READ_PRIVILEGED_PHONE_STATE","value":"1"},
{"name":"android.permission.RECEIVE_BOOT_COMPLETED","value":"1"},
{"name":"android.permission.ACCESS_NETWORK_STATE","value":"1"},
{"name":"android.permission.ACCESS_WIFI_STATE","value":"1"},
{"name":"android.permission.CHANGE_WIFI_STATE","value":"1"},
{"name":"android.permission.BLUETOOTH","value":"1"},
{"name":"android.permission.BLUETOOTH_ADMIN","value":"1"},
{"name":"android.permission.BLUETOOTH_CONNECT","value":"1"},
{"name":"android.permission.BLUETOOTH_SCAN","value":"1"},
{"name":"android.permission.BLUETOOTH_ADVERTISE","value":"1"},
{"name":"android.permission.READ_PHONE_NUMBERS","value":"1"},
{"name":"android.permission.SYSTEM_ALERT_WINDOW","value":"1"},
{"name":"android.permission.CAMERA","value":"1"},
{"name":"android.permission.READ_APP_SPECIFIC_LOCALES","value":"1"},
{"name":"android.permission.HIGN_SMAPLING_RATE_SENSORS","value":"1"},
{"name":"android.permission.ACCESS_COARSE_LOCATION","value":"1"},
{"name":"android.permission.ACCESS_FILE_LOCATION","value":"1"},
{"name":"android.permission.ACCESS_BACKGROUND_LOCATION","value":"1"},
{"name":"android.permission.QUERY_ALL_PACKAGES","value":"1"},
{"name":"android.permission.PACKAGE_USAGE_STATS","value":"1"},
{"name":"android.permission.FOREGROUND_SERVICE_DATA_SYNC","value":"1"},
{"name":"android.permission.FOREGROUND_SERVICE","value":"1"},
{"name":"android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING","value":"1"},
{"name":"android.permission.WAKE_LOCK","value":"1"},
{"name":"android.permission.USE_EXACT_ALARM","value":"1"},
{"name":"android.permission.MANAGE_EXTERNAL_STORAGE","value":"1"},
{"name":"android.permission.SCHEDULE_EXACT_ALARM","value":"1"}]}]
```

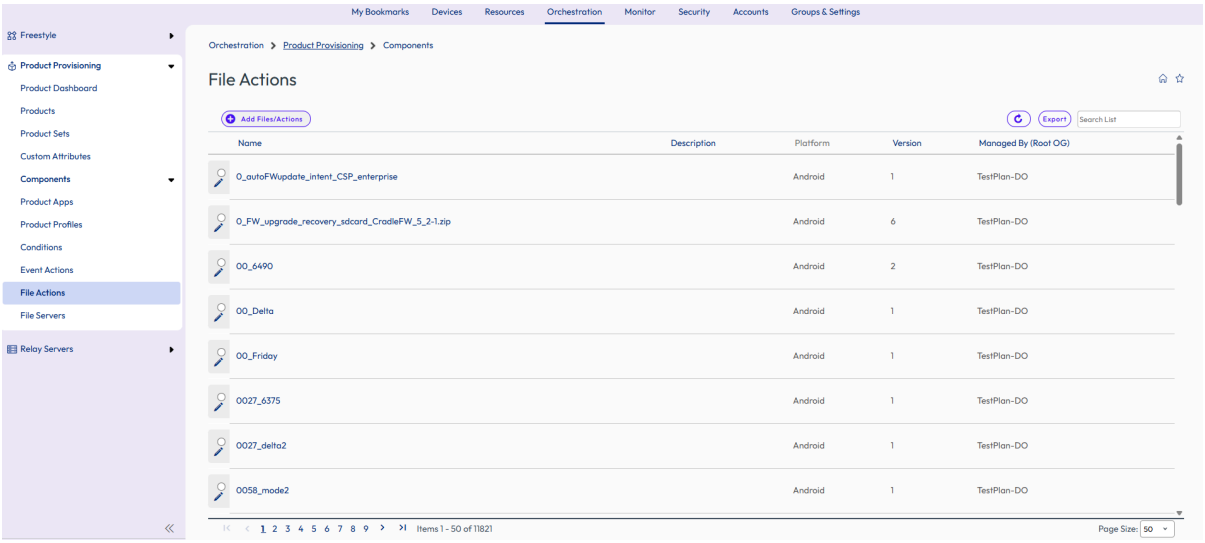

3. Click **Save**.

Auto-launching Zebra Services Agent

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

1. Select **Orchestration** > **Product Provisioning** > **Components** > **Files Action** > **Android**.
2. In the **General** tab, enter the **Name and Description**.

3. In the **Manifest** tab, click **Add Action** under **Install Manifest**.



4. Configure the following information in the **Add Manifest** options.
   - Action(s) to Perform: Run Intent
   - Command Line and Arguments to run:

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,
package=com.zebra.servicesagent,
class=com.zebra.servicesagent.ui.splash.SplashActivity
```

```
TimeOut: -1
```

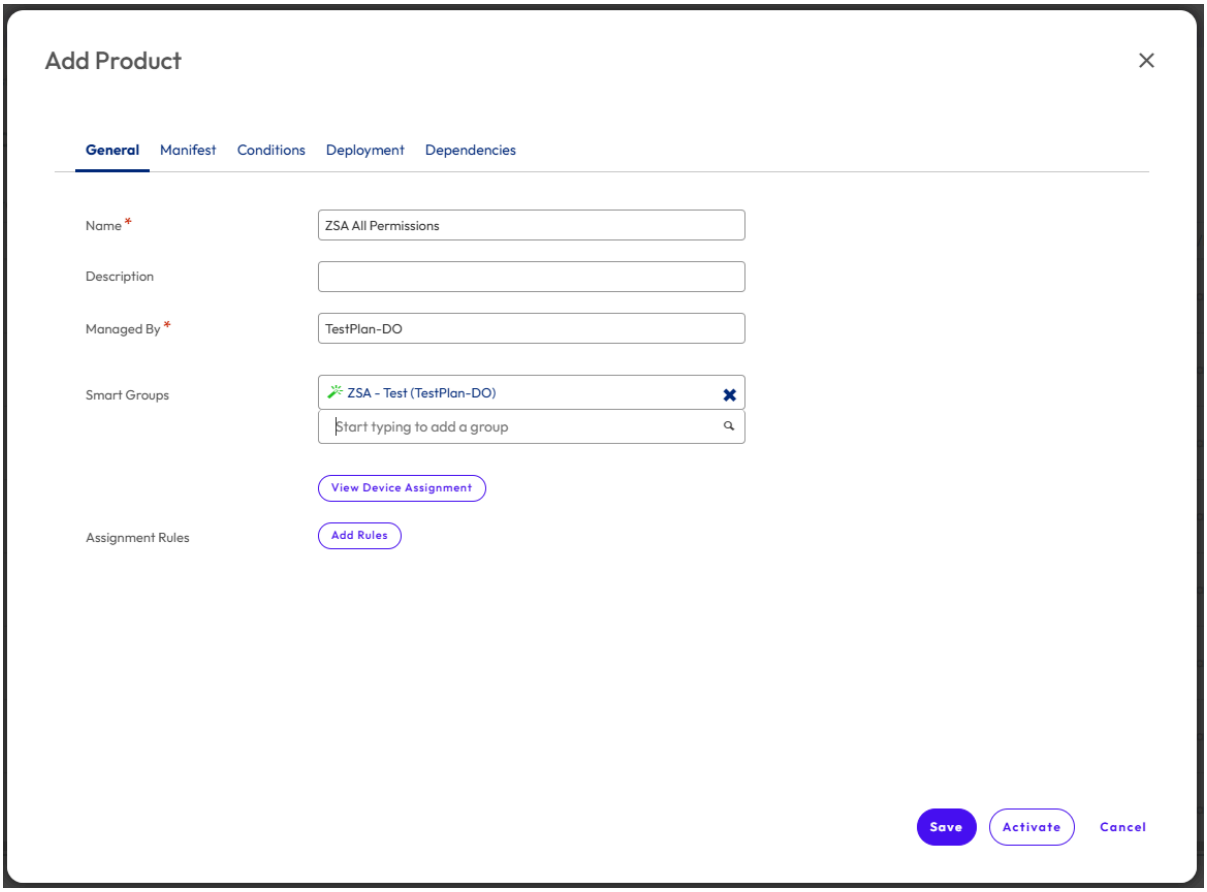


5. Click **Save**.

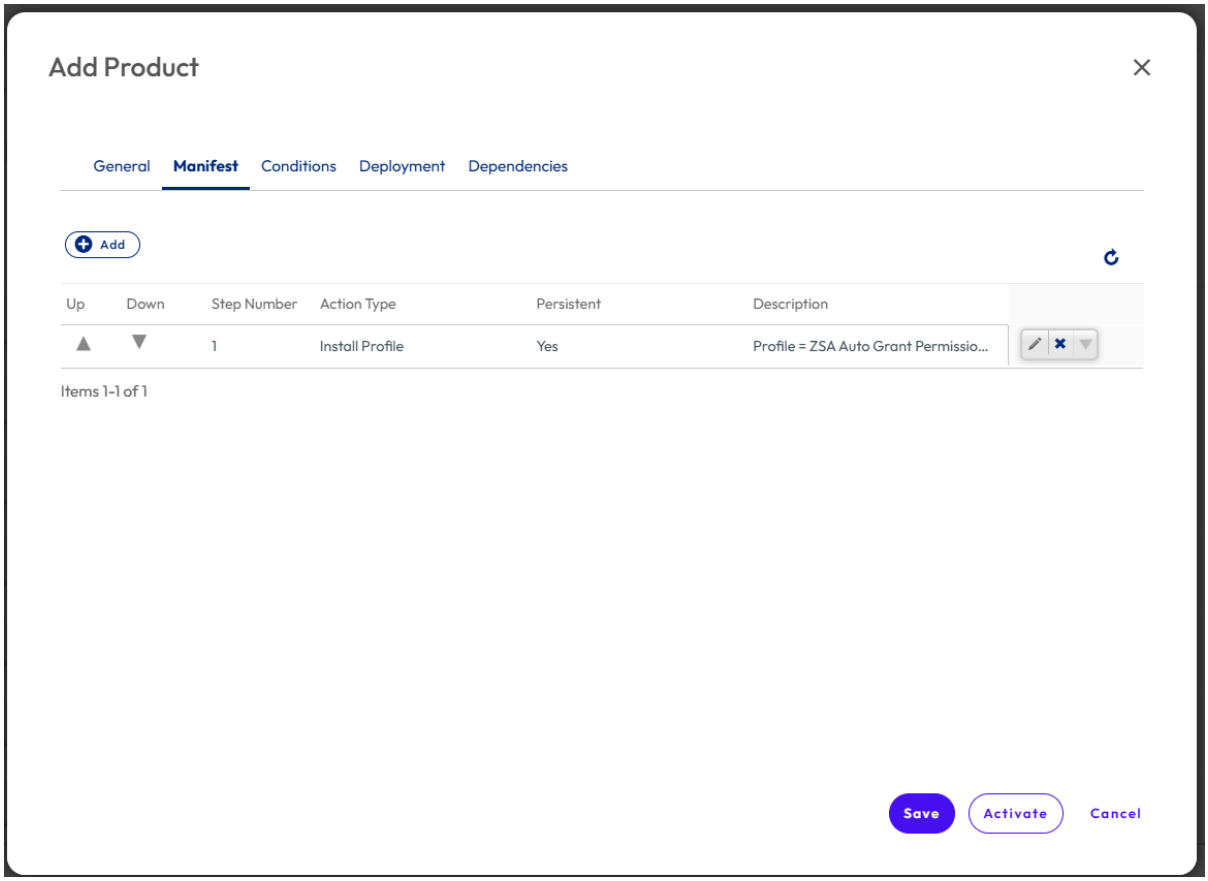
Activating Permissions Product

To activate the Permissions Product:

1. Go to **Orchestration** > **Product Provisioning** > **Products** > **Product List View**.
2. Click **Add Product**, and select **Android**.
3. In the **General** tab, fill in the **Name**, **Description**, and **Smart Groups** fields.



4. Click **Save**.
5. In the **Manifest** tab, click **Add**.
6. Configure the following information in the **Add Manifest** options.



a. Select **Profile Install** from the drop-down list.

b. Search for the permissions profile of Zebra Services Agent and select the permissions profile.

c. Select the **Persistent** checkbox via enterprise reset.

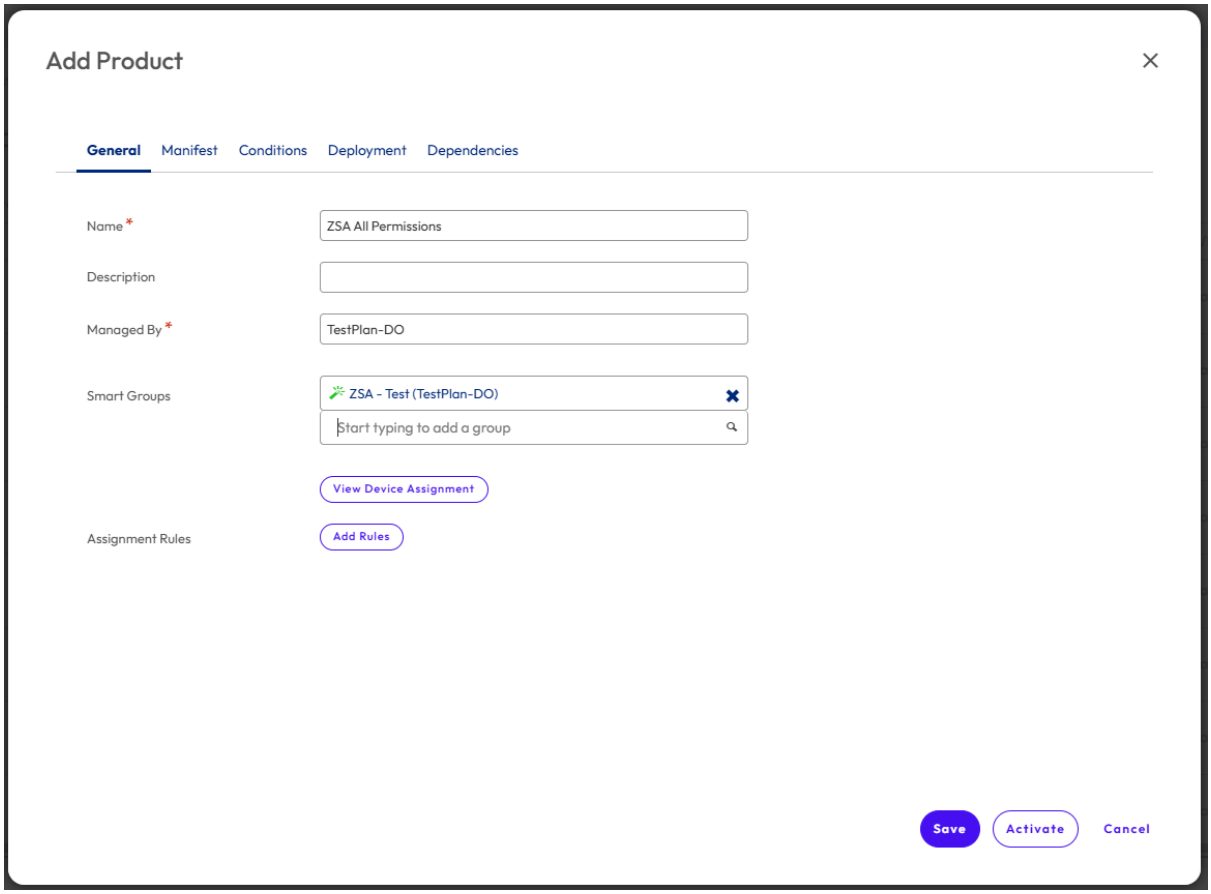
d. Click **Save**.

e. Repeat steps **a - e** to add Zebra Services Battery Health permissions.

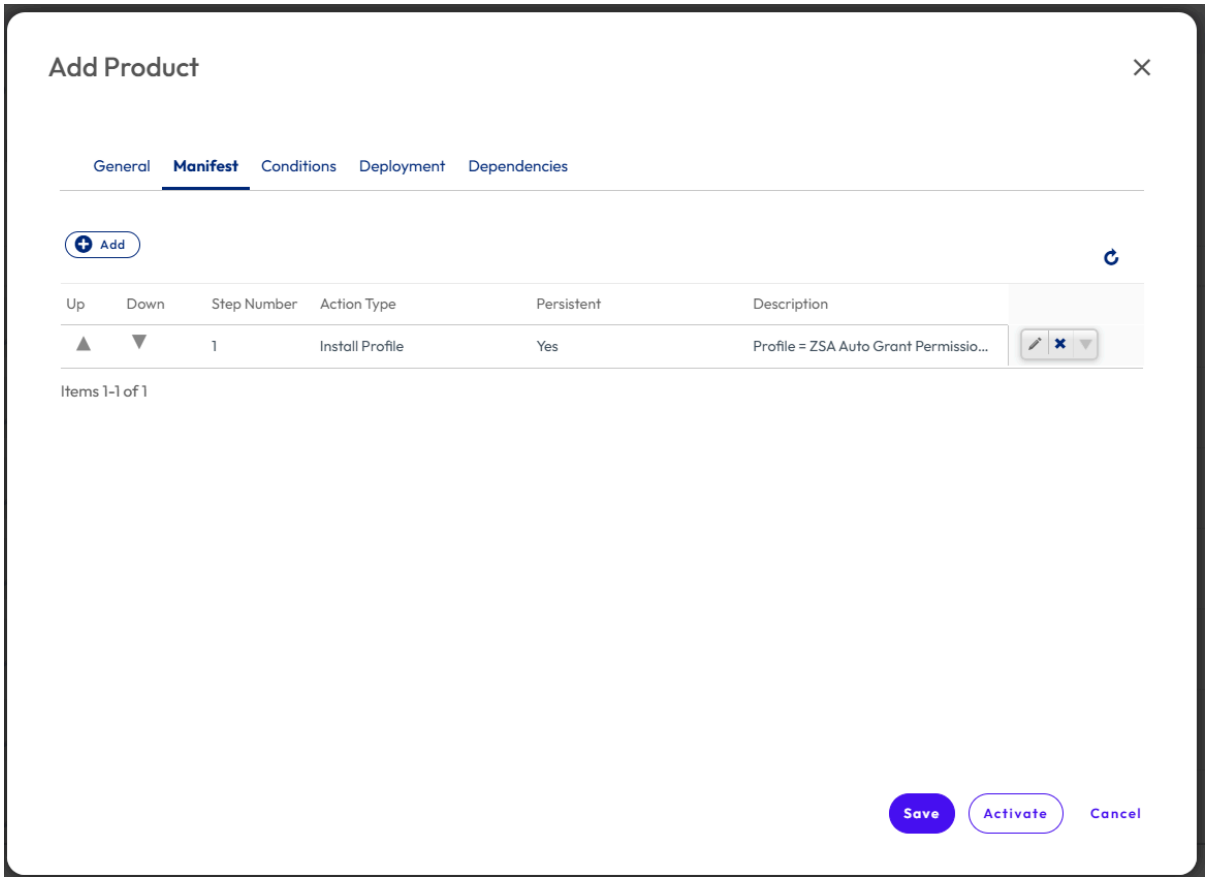
Creating an Auto-launch Product

To create an Auto-launching Product:

1. Go to **Orchestration** > **Product Provisioning** > **Products** > **Product List View**.
2. Click **Add Product and** select **Android**.
3. In the **General** tab, fill in the **Name**, **Description**, and **Assigned Groups** fields.



4. Click **Save**.
5. In the **Manifest** tab, click **Add**.
6. Configure the following information in the **Add Manifest** options.



a. Select **File/Action** from the drop-down list.

b. Search the auto-launch File/Action for Zebra Services Agent.

c. Select the auto-launch File/Action.

d. Select the **Persistent** checkbox via enterprise reset.

e. Click **Save**.

After creating two products, activate the first permission product and wait for it to comply with all devices.

IMPORTANT:

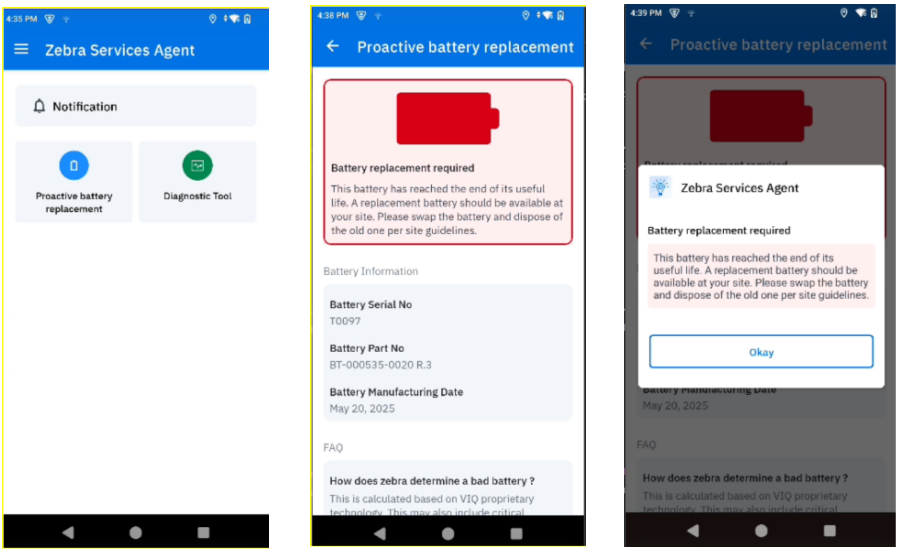
You are only required to **Activate** the Zebra Services Agent autolaunching products from the list of products under Provisioning.

Expected Behaviour After Auto-launching Zebra Services Agent

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

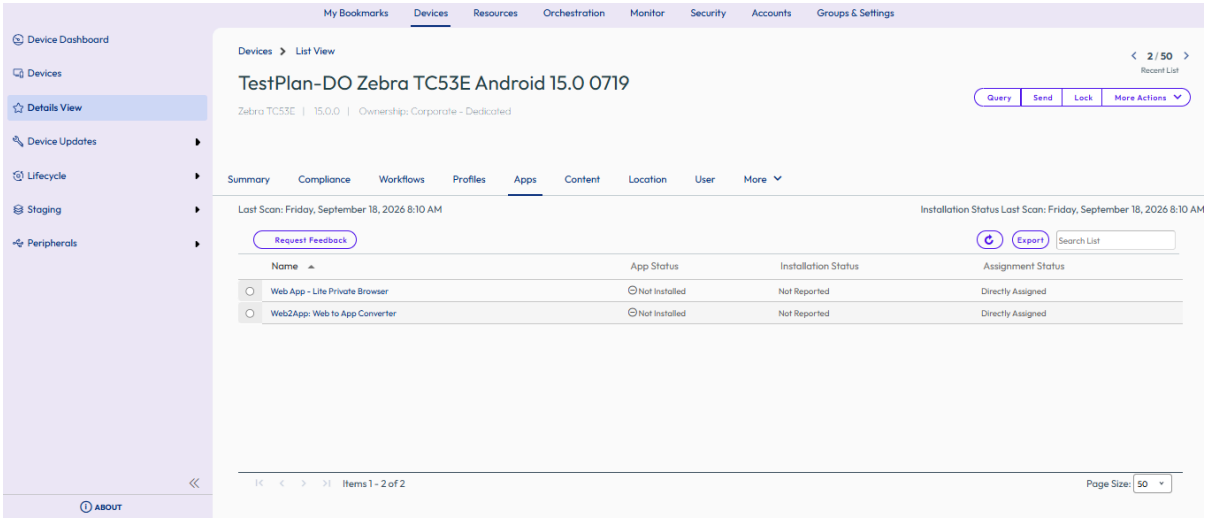
1. Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
2. If the Proactive Battery Health (PBR) module is entitled, the ZSA app automatically launches it after a few seconds.

3. The PBR screen displays both good and bad battery details, and if a **bad battery** condition is detected, a dialog will display.



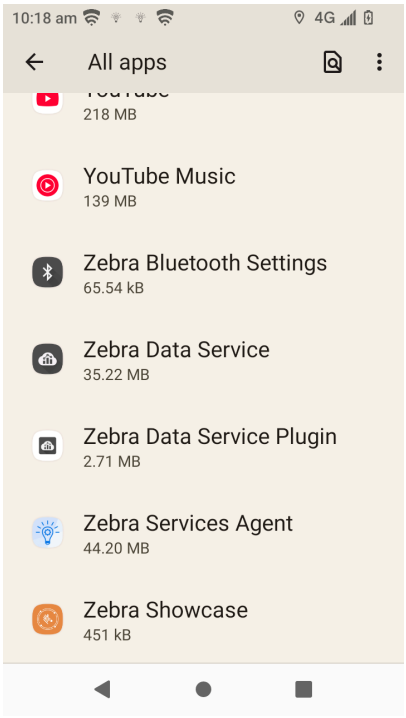
FAQs

1. How do you determine which apps are installed on the devices in AirWatch?
   a. Go to **Devices** > **List View**.
   b. Select any device from the list, and it provides information about the selected device.

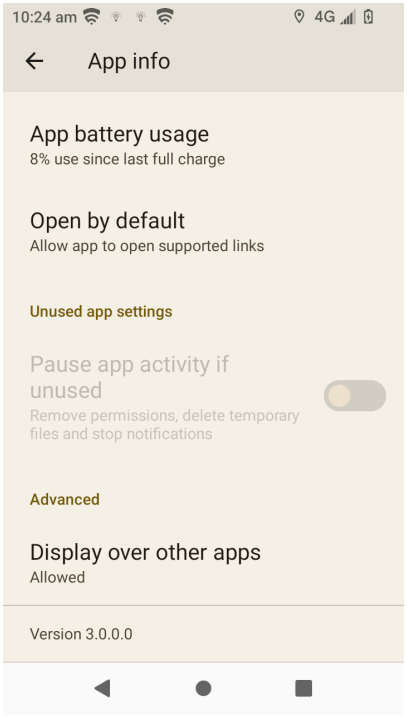


   c. Click the **Apps** tab, then scroll down or use the **Search** feature to find the ZSA app.

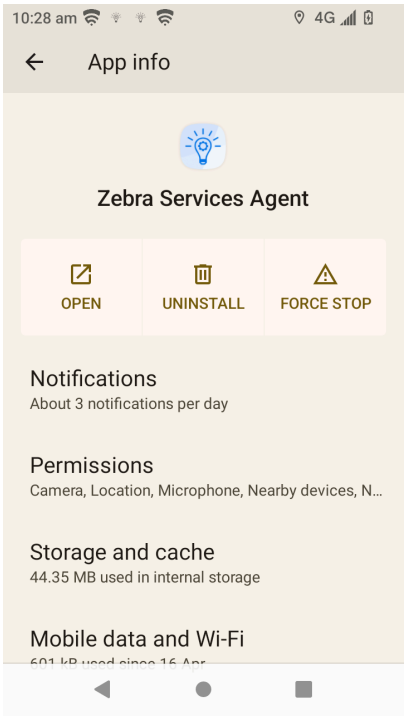
2. How can the user verify if the app is installed with the correct permissions and is able to connect to Zebra servers?
   a. To verify the app version, go to **Settings** > **Apps** > **All apps** and select **Zebra Services Agent**.



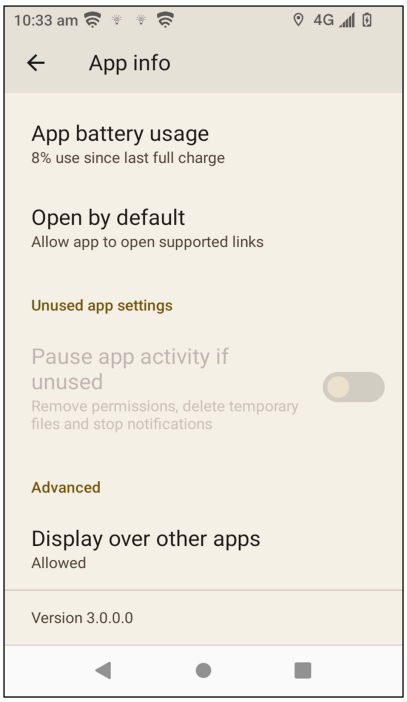
b. The **App Info** page displays the **Version**.



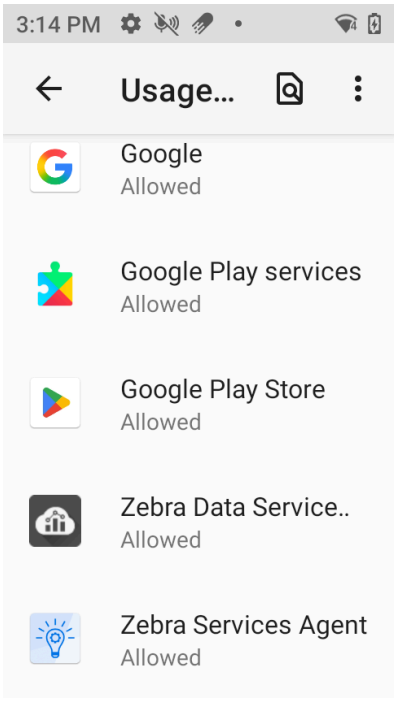
c. To verify the ZSA Permissions, go to **Settings** > **Apps** > **All apps** > **Zebra Services Agent** > **Permissions**.



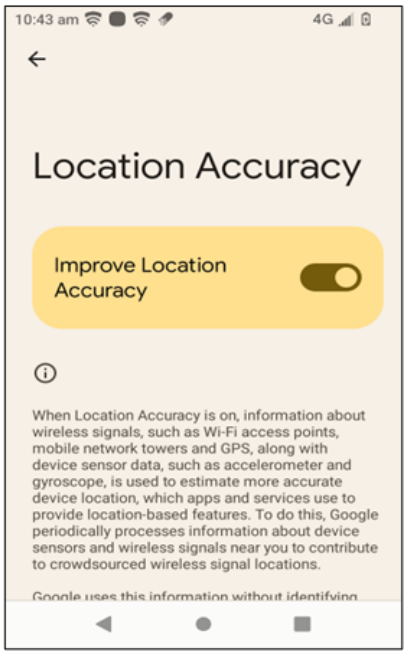
d. To verify the Display over other apps permission, go to **Settings** > **Apps** > **All apps** > **Zebra Service Agent** > **Advanced** > **Display over other apps**.



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

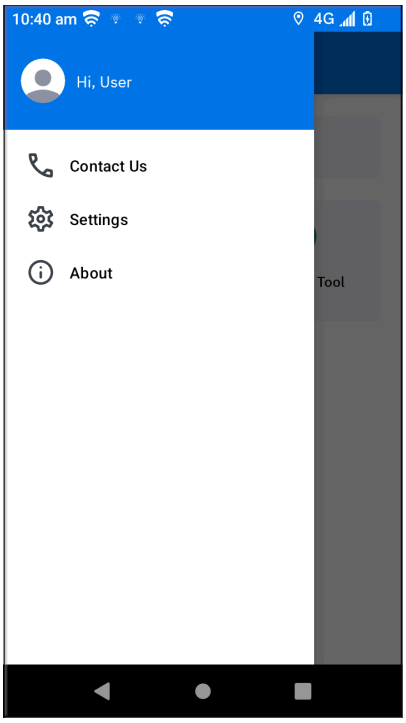


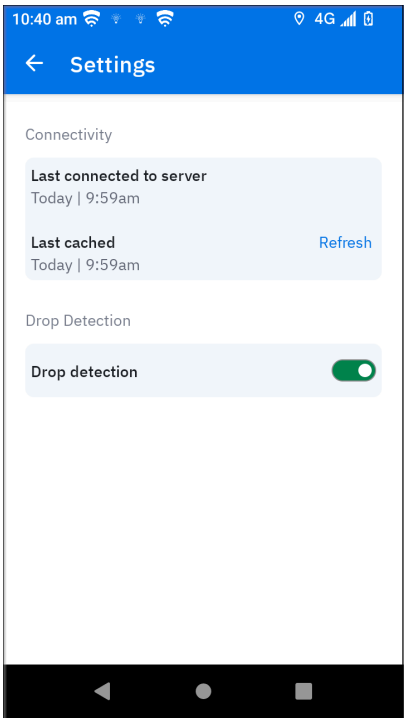
f. For **Device action** > **Outdoor Location Tracking** feature, ensure the location accuracy is enabled on the device to get precise location information. Go to **Settings** > **Location** > **Location Services** > **Location Accuracy**.



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

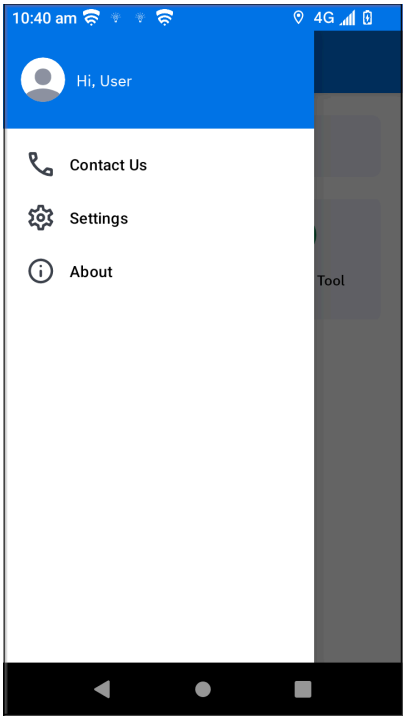
Launch ZSA and go to **Settings** > **Refresh**.

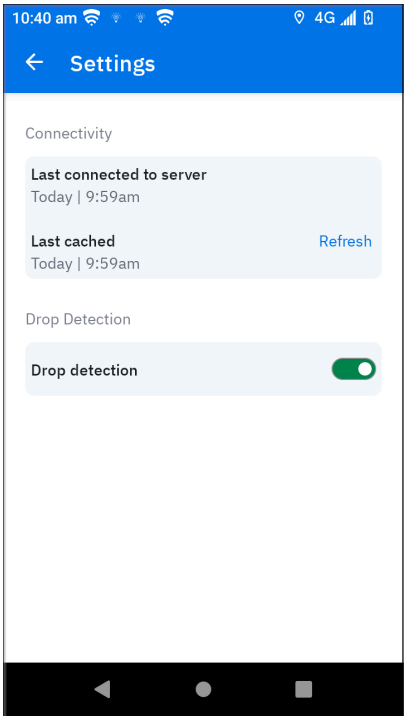




h. To verify the drop detection status:

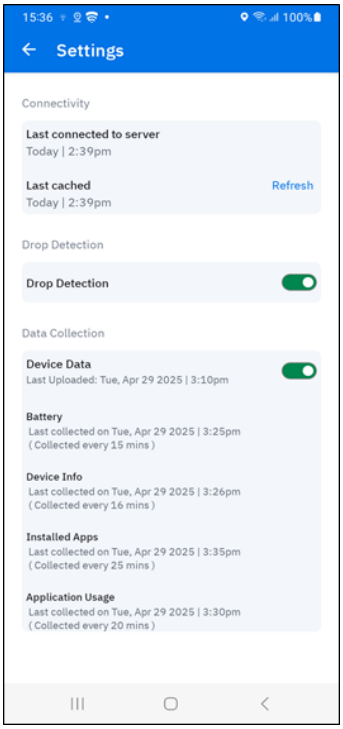
Launch ZSA and go to **Settings**, check the **Drop detection** option. The user can enable/disable the drop detection if the administrator provides the toggle access.



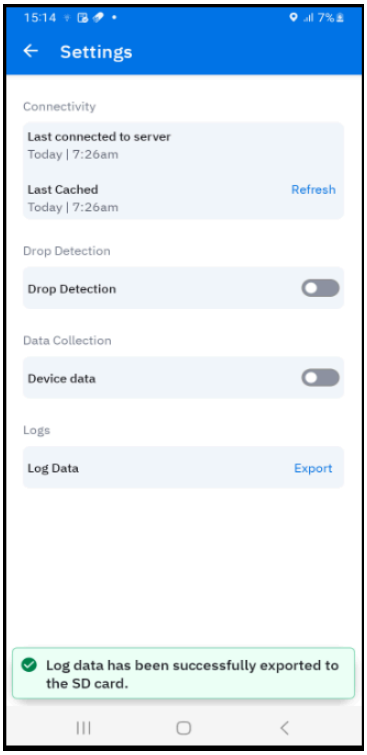


i. To verify Data collection in a non-Zebra device:

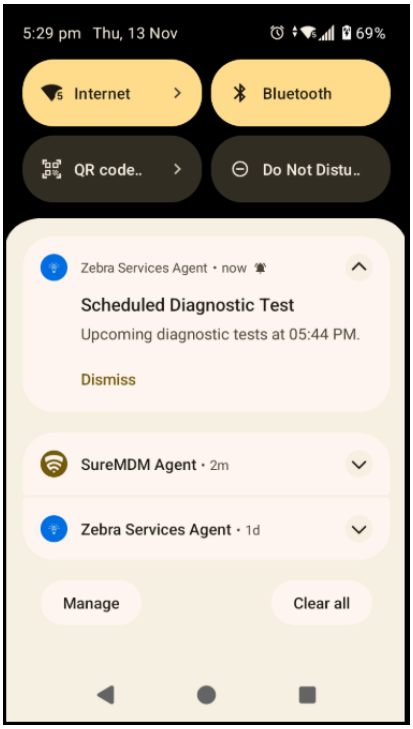
Launch ZSA and go to **Settings** > **Data Collection**. In data collection, the last uploaded time indicates when all data was sent to the server, while each data type has its own last collected time and collection interval.



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



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



I. Proactive Device Monitoring

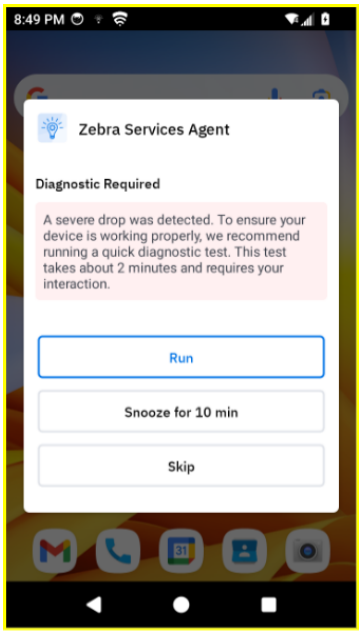
Verify Proactive Device Monitoring and event alerts by observing the alert dialog workflows for Severe device drop, Frequent network disconnections (Wi-Fi/Bluetooth), unexpected reboots, and thermal anomalies:

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

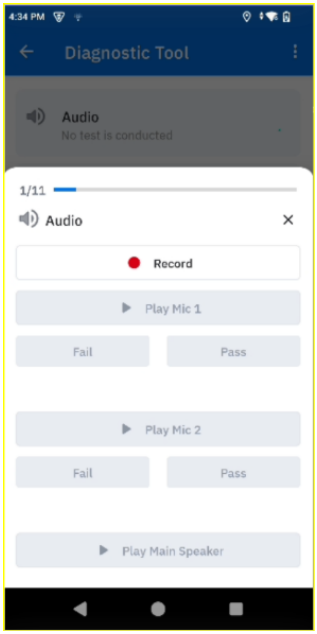
- Severe device drop
- Frequent Wi-Fi Disconnections
- Frequent Bluetooth Disconnections
- Frequent Device Reboots

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

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

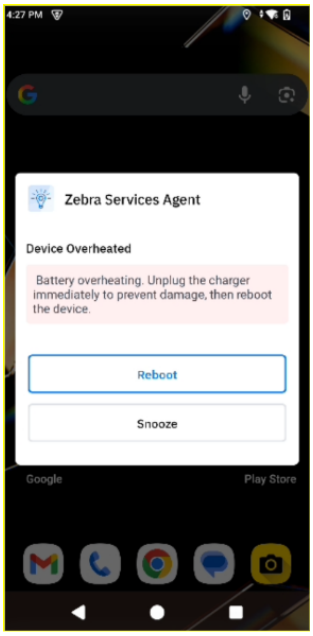


- **Run** – Starts the DDT diagnostic process by executing all DDT tests sequentially.
- **Snooze for 10 min** – Dismisses the alert dialog and the prompt will appear again after 10 minutes.
- **Skip** – Skips the diagnostics and report to admin about the skip action.



- **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.

