

Zebra Services Agent for AirWatch



ZEBRA

Installation Guide

2025/06/16

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

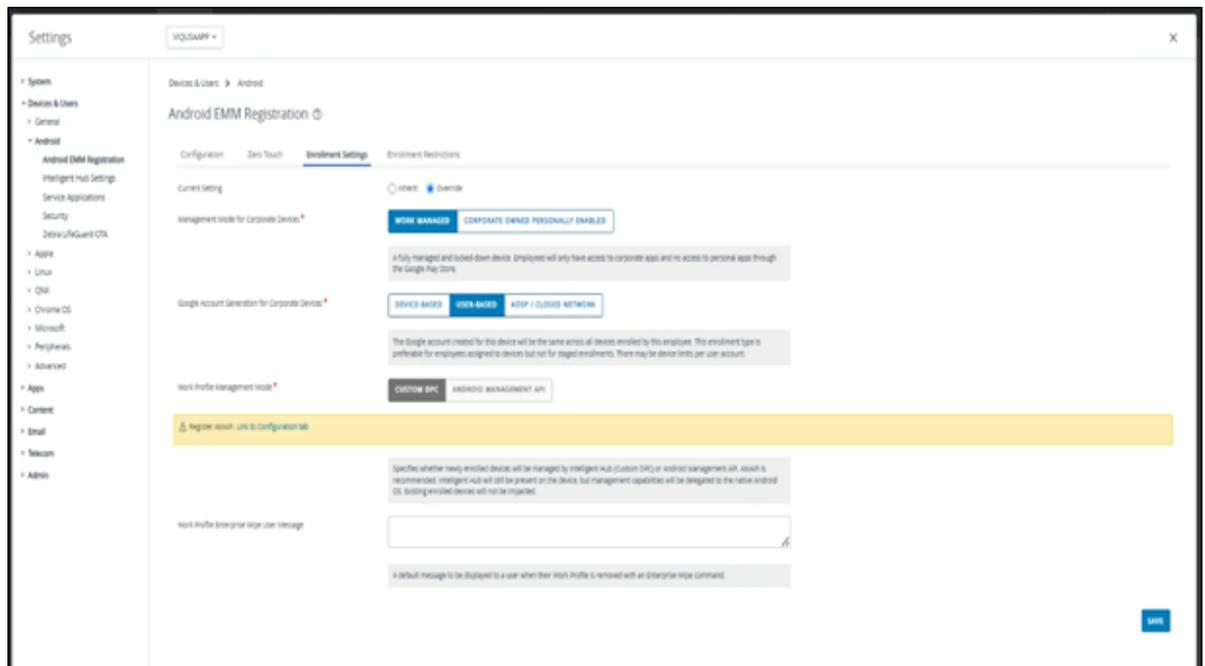
VMware AirWatch is an Enterprise Mobility Management (EMM) solution that enables companies to securely manage devices and endpoints with any form factor and operating system throughout their lifecycle, from deployment to retirement.

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**.

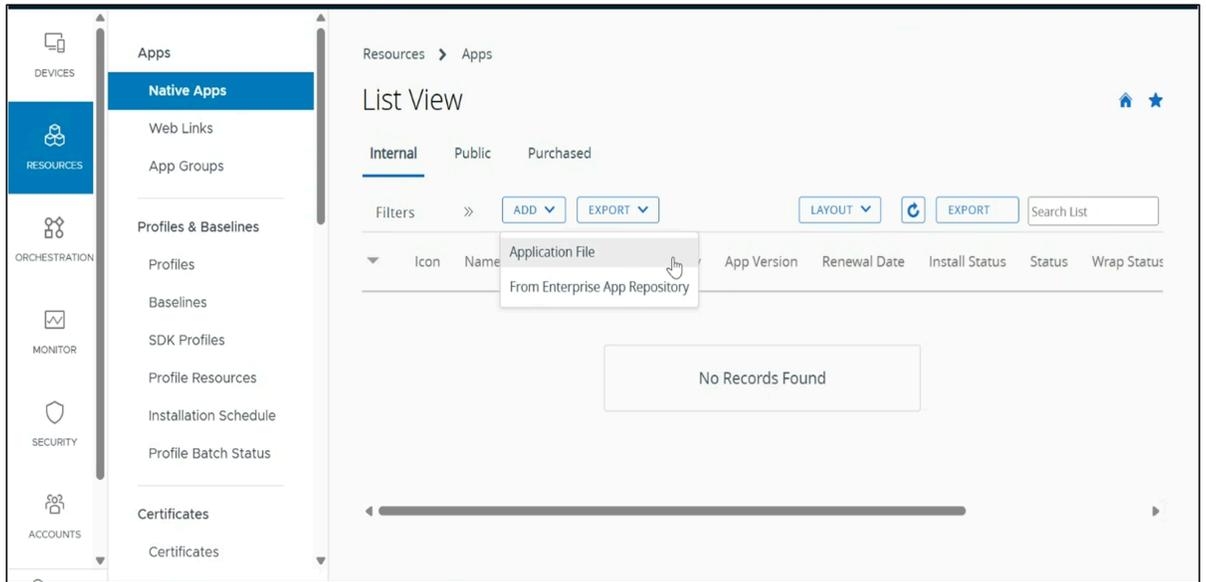
Deploying Zebra Services Agent

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

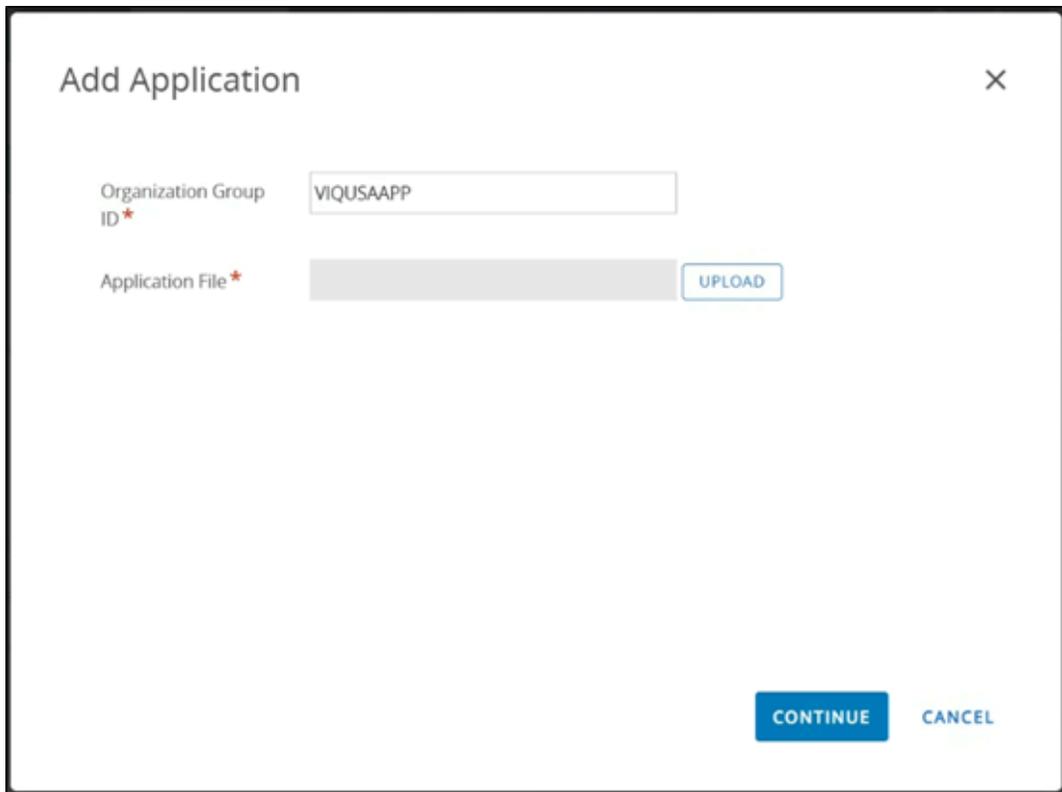
Download the Zebra_Service_Agent_V3.0.0.5.apk file from zebra.com/zebra-services-agent.

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**.

Add Application - Zebra Services Agent v 3.0.0.1
Internal | Managed By: VIQUSAAPP | Application ID: com.zebra.zsa | App Size: 14767 KB

Details | Files | Images | Terms of Use | More ▾

Name* ⓘ

Managed By

Application ID*

App Version*

Current UEM Version ⓘ

Is Beta ⓘ

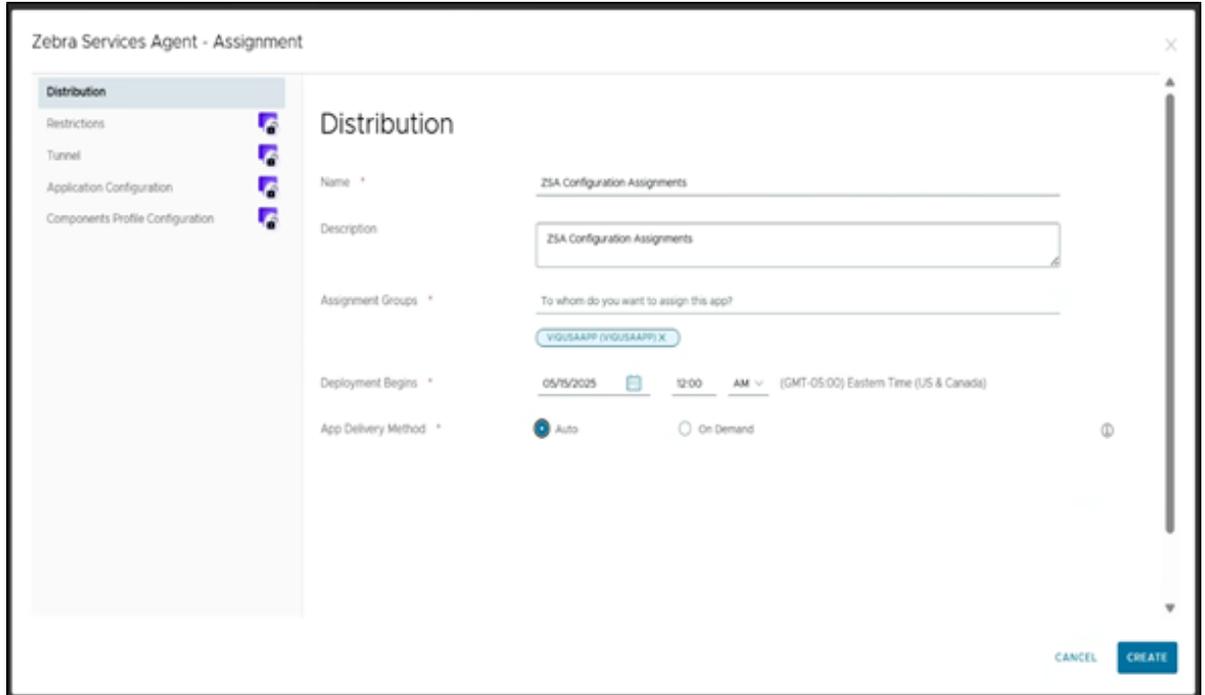
Update Notifications ⓘ

Change Log

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**.



The screenshot shows the 'Zebra Services Agent - Assignment' configuration window. The 'Distribution' tab is selected in the left sidebar. The main area is titled 'Distribution' and contains the following fields:

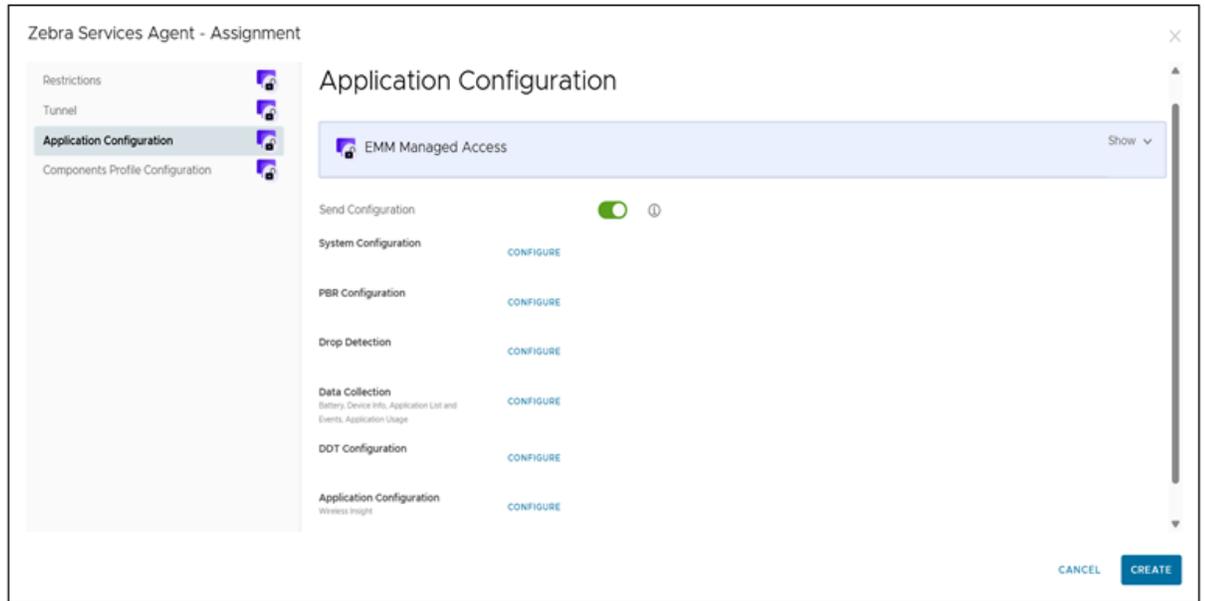
- Name ***: ZSA Configuration Assignments
- Description**: ZSA Configuration Assignments
- Assignment Groups ***: To whom do you want to assign this app? (VGUSAAPF (VGUSAAPF) X)
- Deployment Begins ***: 05/16/2025 12:00 AM (GMT-05:00) Eastern Time (US & Canada)
- App Delivery Method ***: Auto On Demand

At the bottom right, there are 'CANCEL' and 'CREATE' buttons.

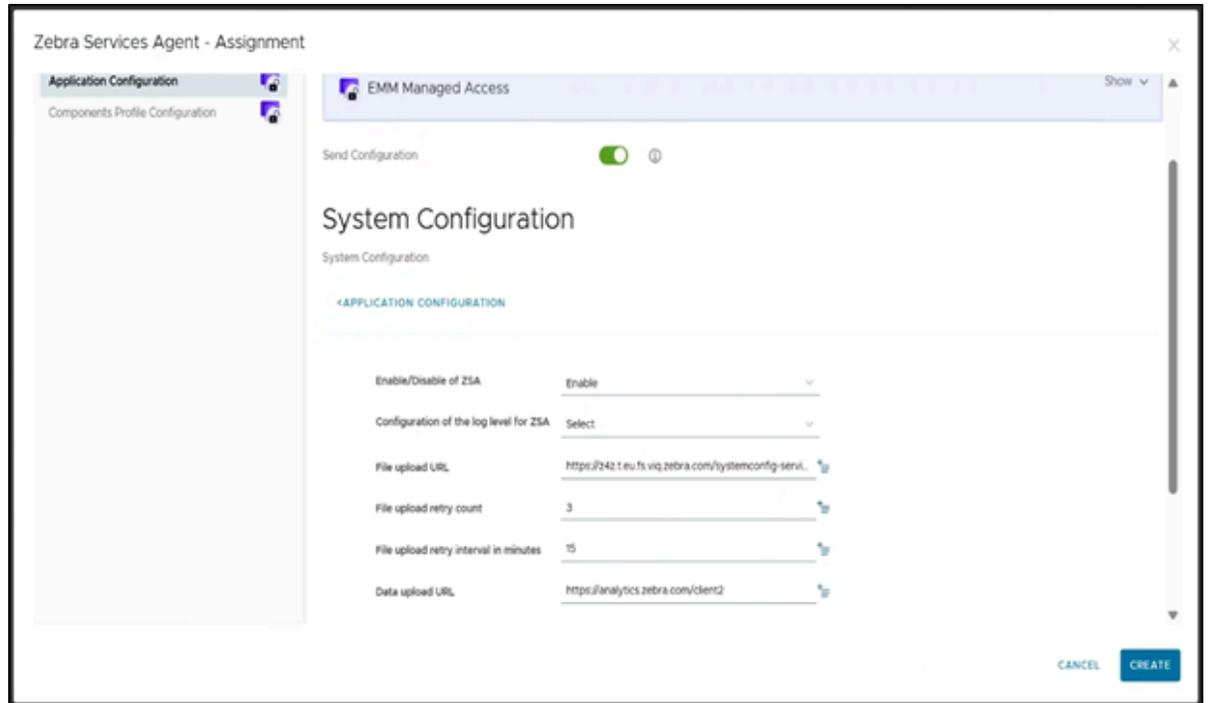
- d) Click **Create**.

6. Managed Configuration:

- a) The ZSA Managed Configuration contains six modules, each with an enable/disable feature to set the configuration.
- b) To send the configurations to 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



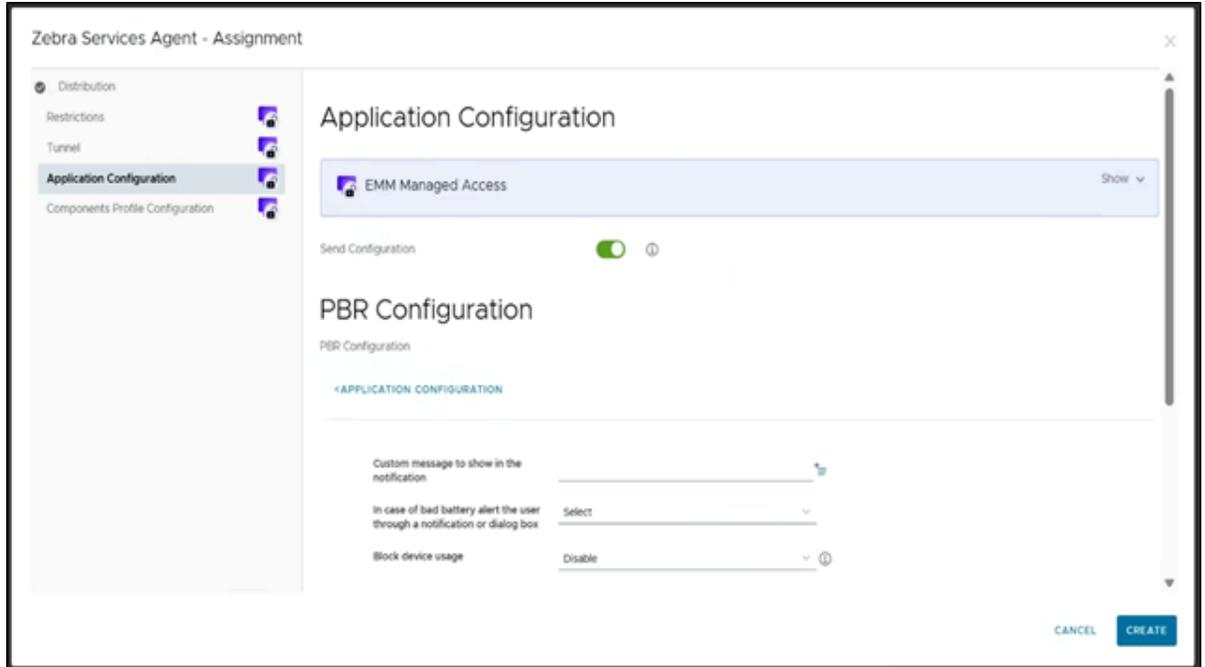
- d) The system settings include three features for uploading log files:
- **File upload URL:** Specifies the server path for uploading log files.
 - **File upload retry count:** Defines the number of retry attempts if the upload fails.
 - **File upload retry interval in minutes:** Sets the duration (in minutes) between each retry attempt after a failed upload.
- e) 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.

The screenshot shows the 'Zebra Services Agent - Assignment' configuration window. The 'System Configuration' section is active, displaying the following settings:

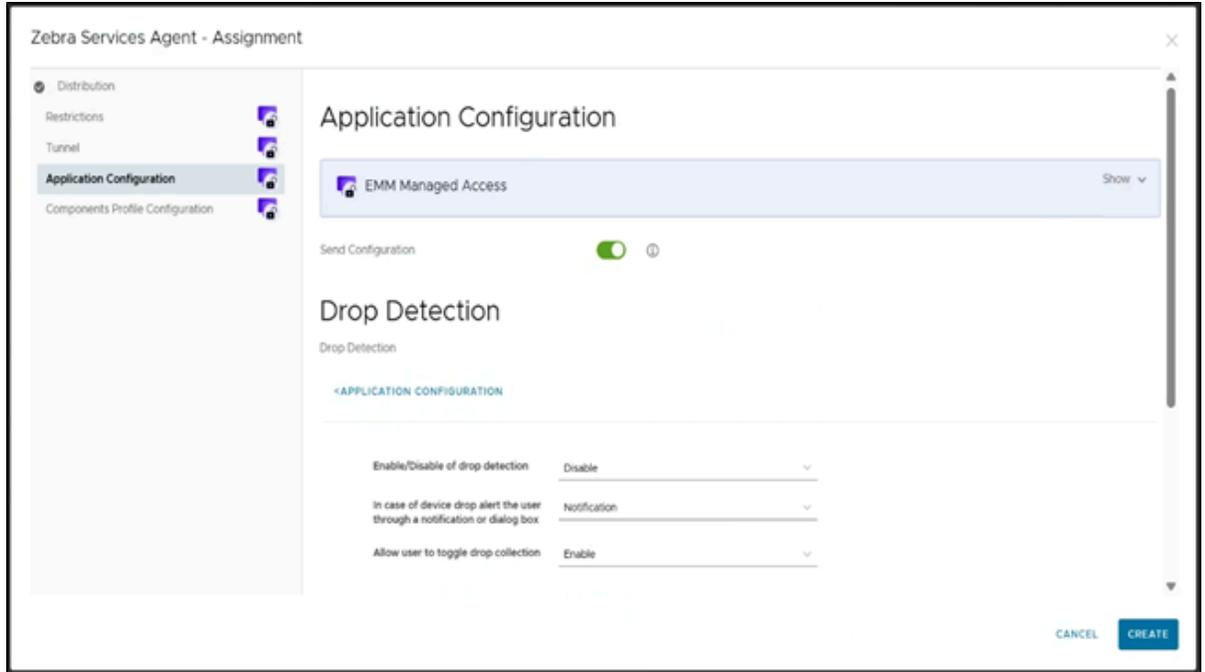
Setting	Value
Enable/Disable of ZSA	Enable
Configuration of the log level for ZSA	Select
File upload URL	https://2421.eu.fs.viq.zebra.com/systemconfig-servi...
File upload retry count	3
File upload retry interval in minutes	15
Data upload URL	https://analytics.zebra.com/client2
Data upload interval in minutes	1440
Enable/Disable of data collection	Disable
Allow user to toggle data collection	Enable
Account No	

Buttons for 'CANCEL' and 'CREATE' are visible at the bottom right of the window.

- f) 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.
- g) For the **Account No**, users must enter their MDM account number for non-Zebra devices.
- h) In the **PBR Configuration**, provide a **Custom Message** as required.



- i) 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
- j) The **Block device usage** option is disabled by default. If enabled by the administrator, it prevents device access when a bad battery is detected.
- k) In the **Drop Detection**, toggle the **Enable/Disable of drop detection** option as required.

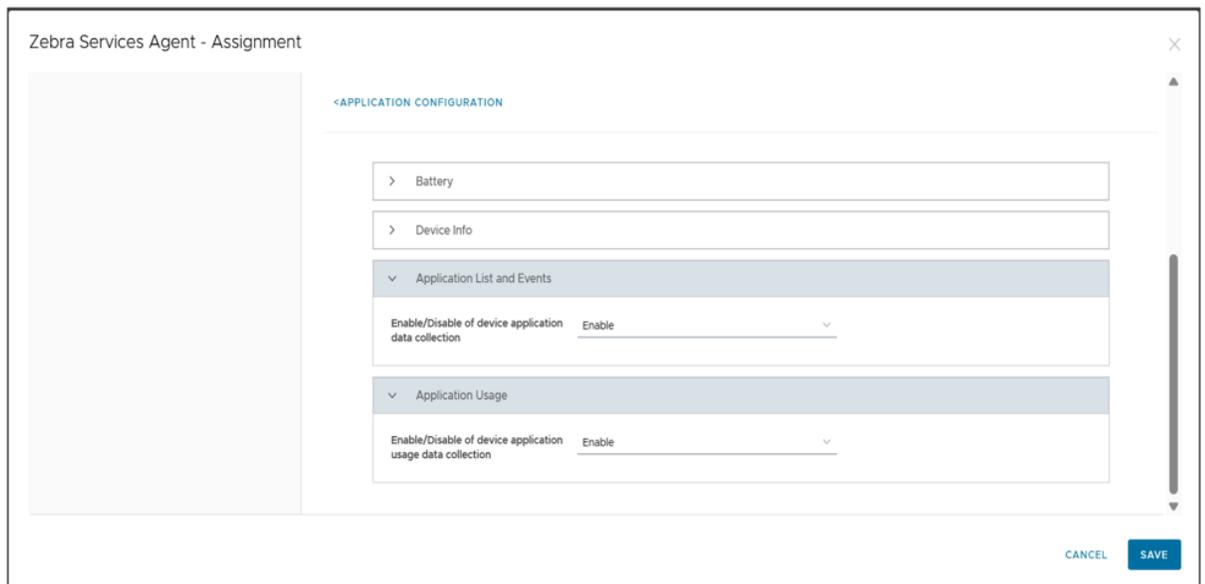
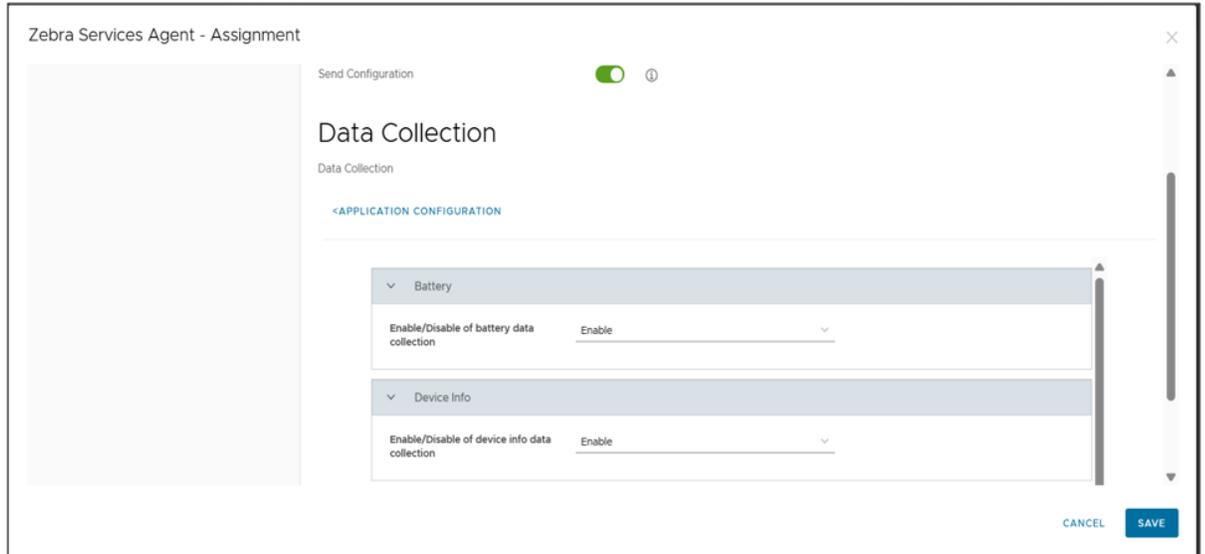


- l) Set the **In case of device drop alert the user through a notification or dialog box** with the following values:
- Notification (default)
 - Dialog
 - Dialogue with Assist
- m) The **Allow user to toggle drop collection** is enabled by default. Users can control this feature, and admins can disable it to restrict access for users.
- n) In the **Data Collection**, the **Battery** option is enabled by default. It collects battery data every 15 minutes, and admins can enable or disable this collection.
- o) **Device Info** option is enabled by default. It collects device info data every 6 hours (360 minutes), and admins can enable or disable this option.

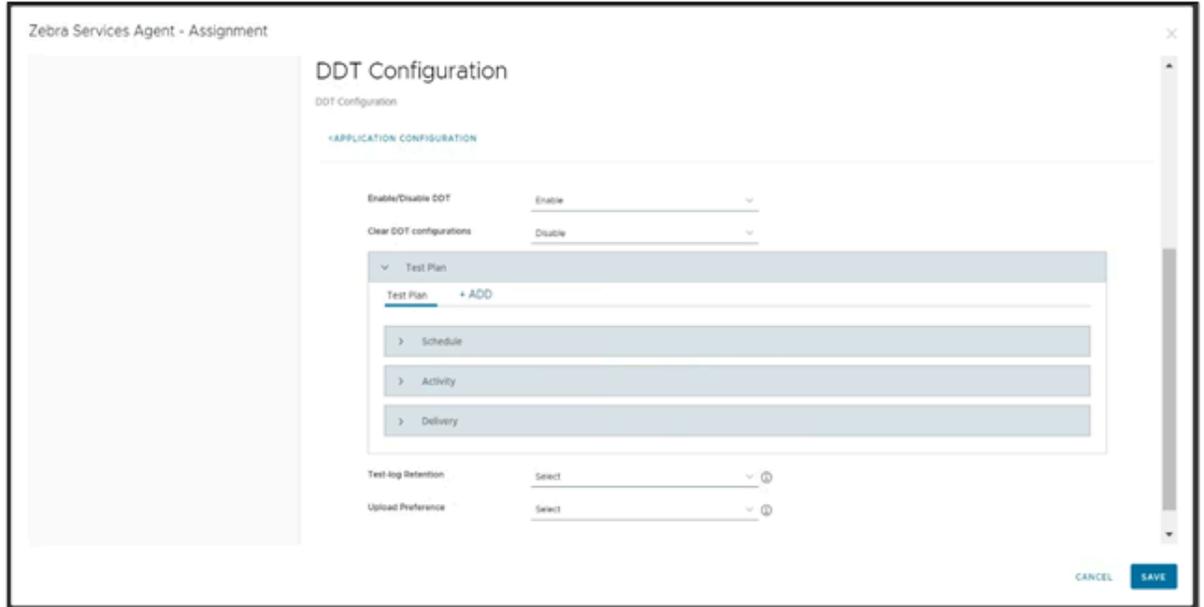


NOTE: Data is uploaded based on the configured **Data Upload URL** and interval settings in the **System Configuration**.

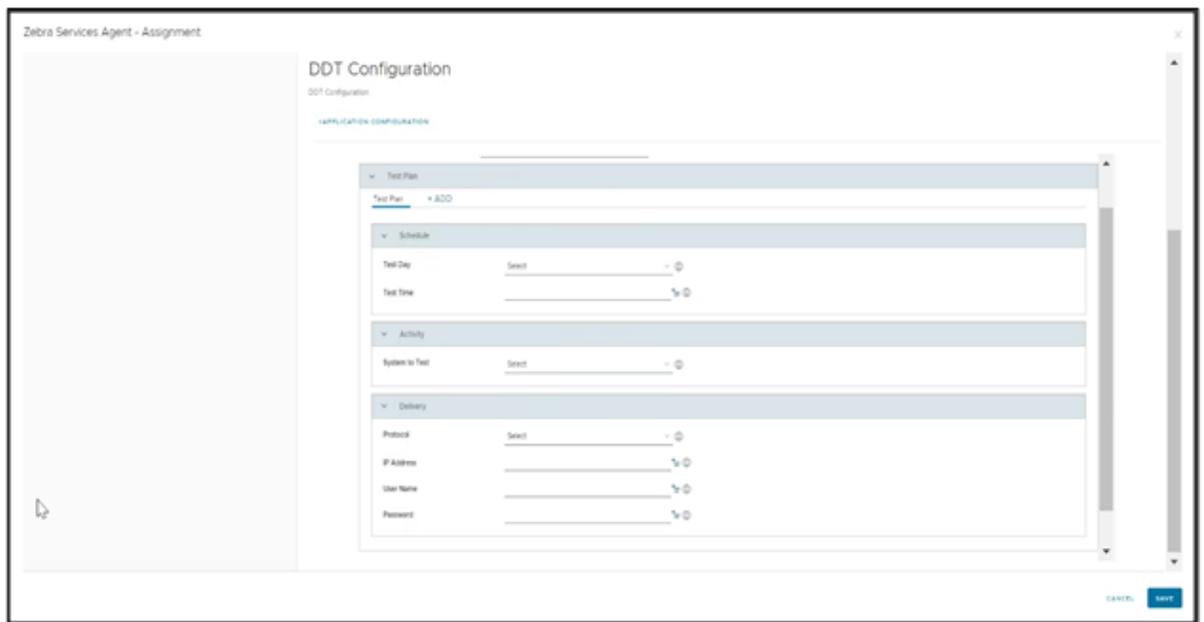
- p) The **Application List and Events** option is enabled by default. It collects information on installed applications and tracks events such as installations, uninstallations, upgrades, and downgrades. Admins can enable or disable this collection.
- q) The **Application Usage** option is enabled by default. It tracks the duration apps spend in the foreground, and admins can enable or disable this option.



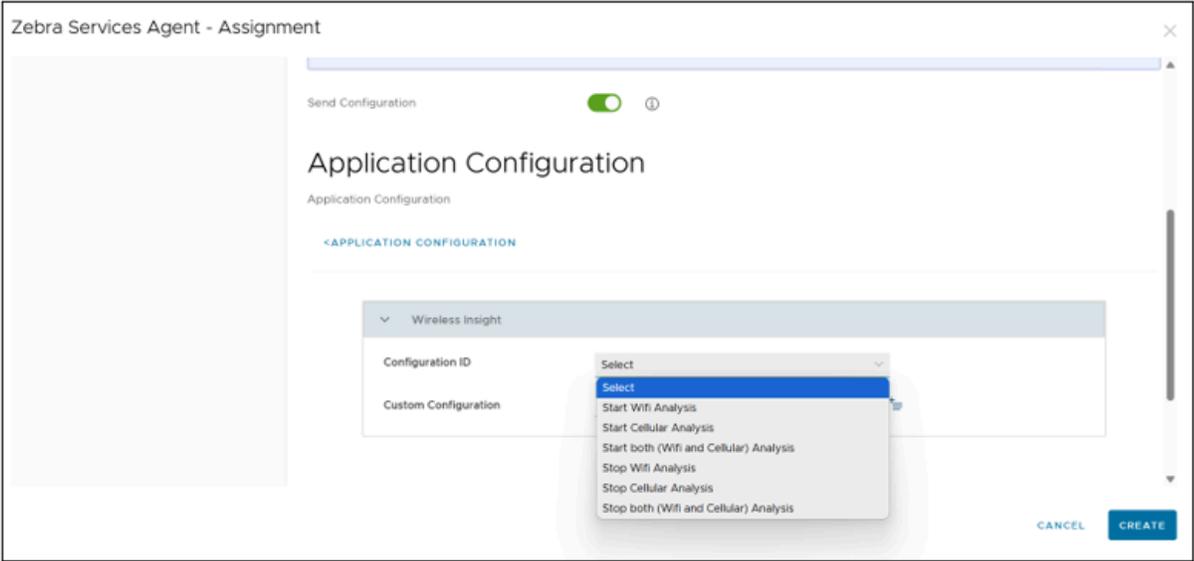
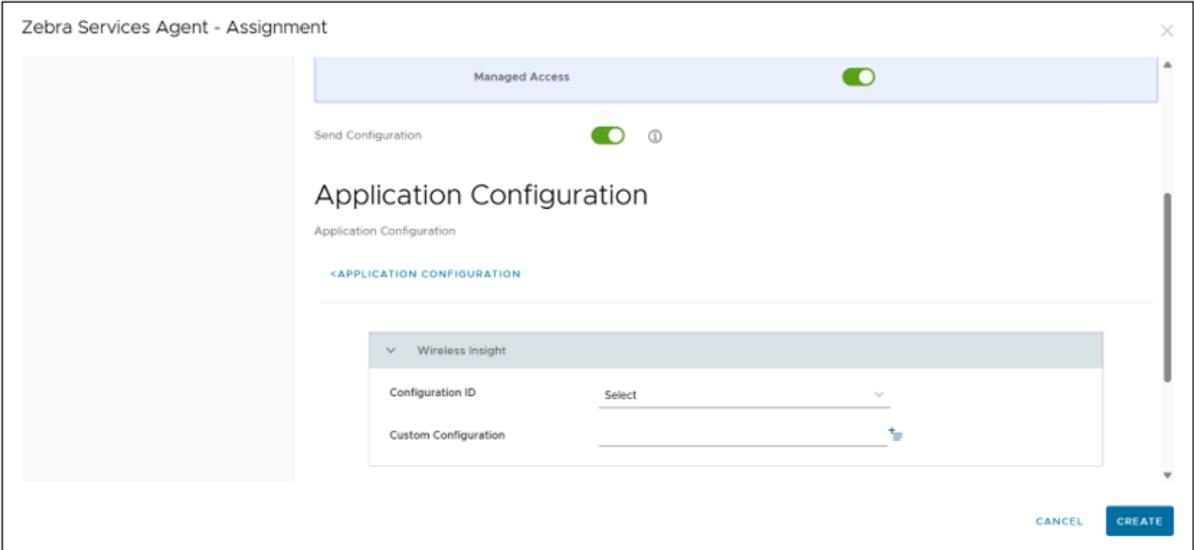
- r) Under the **DDT Configuration**, enable the **Enable/Disable DDT** option, keep the **Clear DDT configurations** disabled in the primary setup, and click **Add** in the **Test Plan** section. Select **Test-log Retention** and **Upload Preference**.



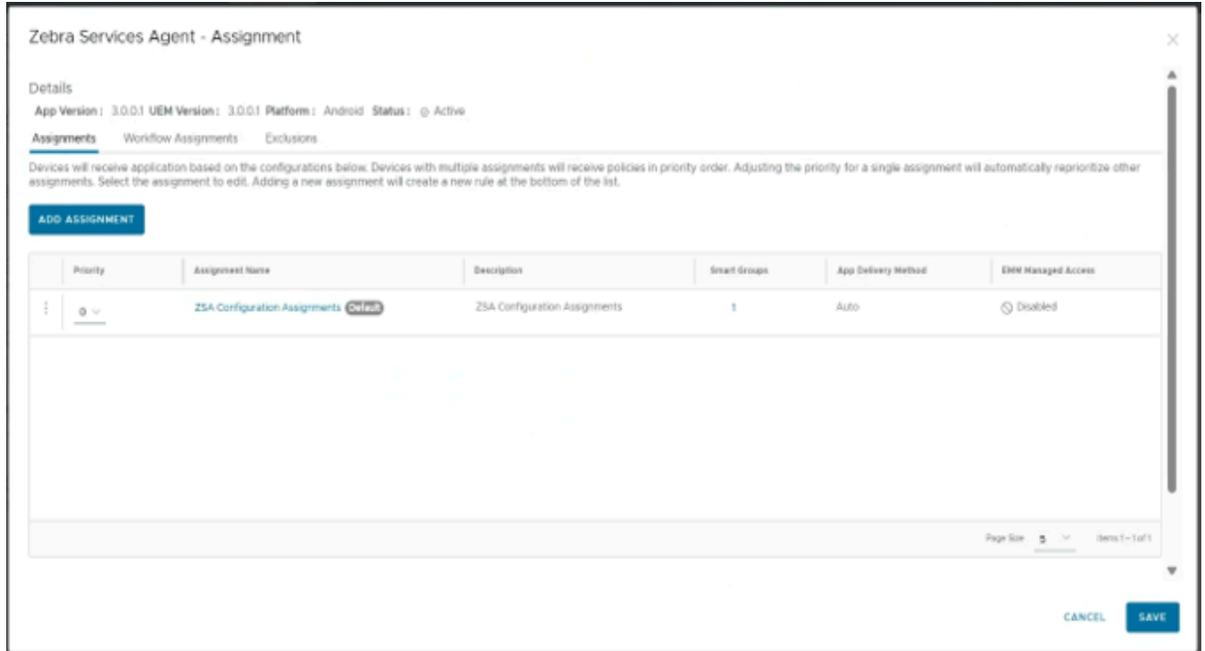
s) Configure the **Test Plan** and click **Save**.



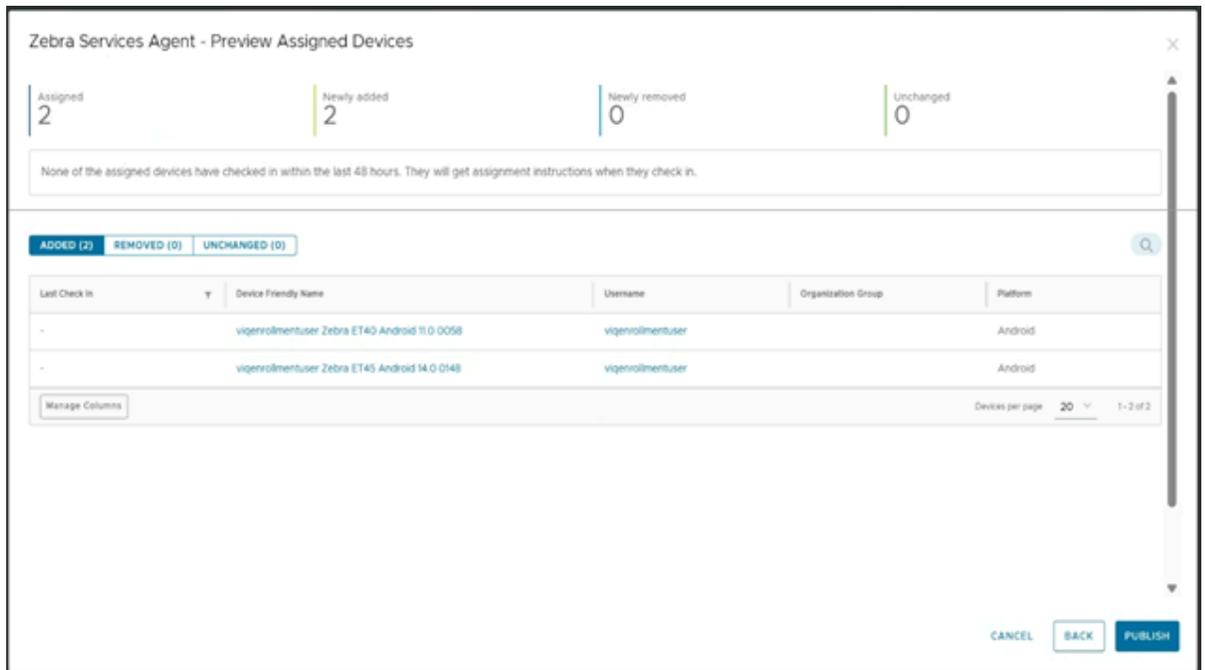
- t) The **Application Configuration** is designated for Zebra devices. It currently supports the **Wireless Insight** application and the **ZDS** application, with more applications to be supported in the future.
- u) The **Wireless Insight** application can be configured using Managed Configuration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



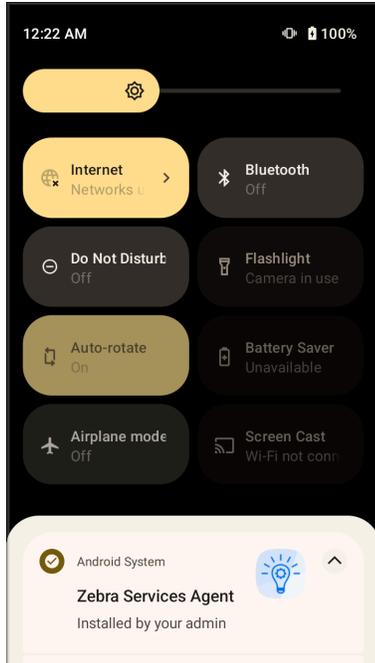
The ZSA Assignment page displays.



w) 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 > Components > Product Profiles > Add Profiles > Android**.

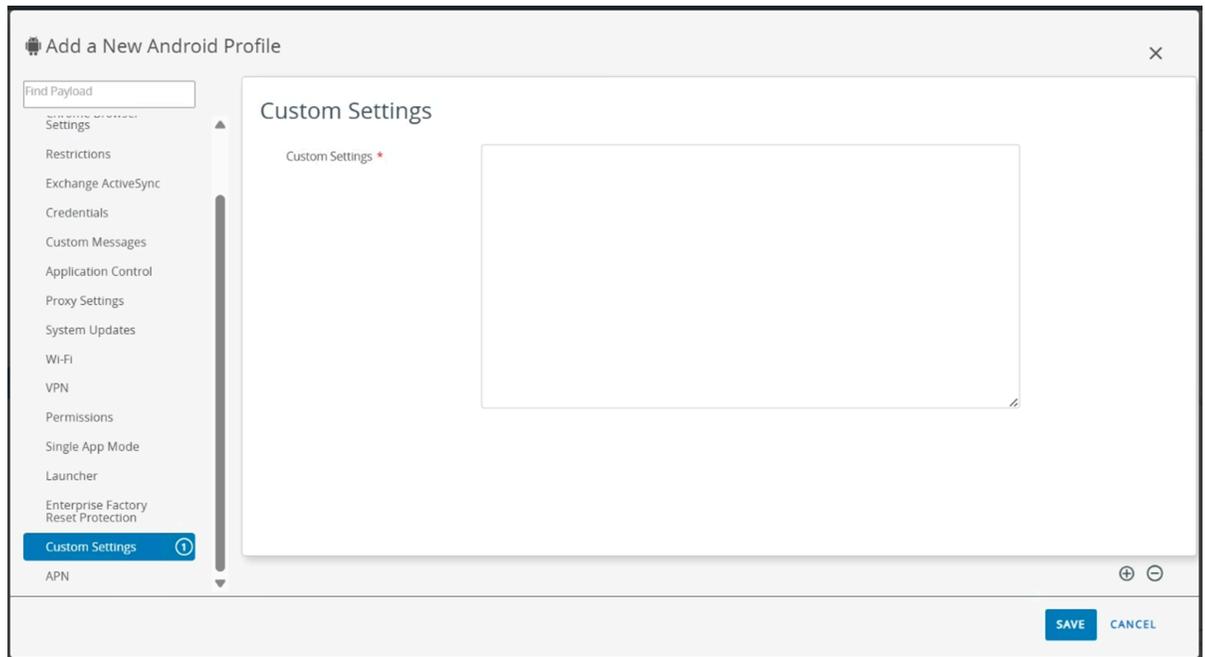
The **Add a New Android Profile** page display. Enter the name as **Grant ZSA Permissions Profile**.

A screenshot of the 'Add a New Android Profile' configuration page. The page has a sidebar on the left with a search bar and a list of categories: General (selected), Passcode, Chrome Browser Settings, Restrictions, Exchange ActiveSync, Credentials, Custom Messages, Application Control, Proxy Settings, System Updates, Wi-Fi, VPN, and Permissions. The main area is titled 'General' and contains the following fields:

- Name: Grant ZSA Permissions Profile
- Version: 1
- Description: (empty)
- OEM Settings: ENABLE (selected) and DISABLE (disabled)
- Profile Scope: Production (dropdown)
- Allow Removal: Always (dropdown)
- Managed By: TestPlan-DO

At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

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="W3sicGFja2FnZU5hbWUiOiJjb20uemVicmEuenNhIiwicGVybWlzc2l2bnMiOiBbey
  JuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX0NPTlRBQ1RTIiwidmFsdWUiOiIxIn0s
  CnsibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5DQUxMX1BIT05FIiwidmFsdWUiOiIxIn0sCn
  sibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5SRUNPUkRfQVVEVSU8iLlJ2YWxlZSI6IjEifSwK
  eyJuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLlJFQUJURfQ090VEF0VFMiLlJ2YWxlZSI6IjEifS
  wKeyJuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLk1OVEVSTkVUiiwidmFsdWUiOiIxIn0sCnsi
  bmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5SRUFEX1NFVFRJTkdtIiwidmFsdWUiOiIxIn0sCn
  sibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5SRUFEX1BIT05FX1NUQVRFIiwidmFsdWUiOiIx
  In0sCnsibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5SRUFEX0VYVEVSTkFMX1NUT1JBR0UiLC
  J2YWxlZSI6IjEifSwKeyJuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX0VYVEVSTkFM
  X1NUT1JBR0UiLlJ2YWxlZSI6IjEifSwKeyJuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLlJFQU
  RfUFJPRklMRSIsInZhbHVlIjoIMSj9LA7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uVVFNF
  X0NSRURFTlRlRjQUxTiiwidmFsdWUiOiIxIn0sCnsibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi
  5NQUSBR0VfQUNDT1VOVFMiLlJ2YWxlZSI6IjEifSwKeyJuYWllIjoieW5kcm9pZC5wZXJtaXNz
  aW9uLlJFQUJURfU1l0Q19TVEF0UyIsInZhbHVlIjoIMSj9LA7Im5hbWUiOiJhbmRyb2lkLnBlcm
  1pc3Npb24uUkVBRf9TWU5DX1NFVFRJTkdtIiwidmFsdWUiOiIxIn0sCnsibmFtZSI6ImFuZHIJv
  aWQucGVybWlzc2l2bvi5XUklURV9TWU5DX1NFVFRJTkdtIiwidmFsdWUiOiIxIn0sCnsibmFtZS
  I6ImFuZHIJvaWQucGVybWlzc2l2bvi5SQULTRURfVEhSRUFEX1BSSU9SSVRZIIiwidmFsdWUiOiIx
  In0sCnsibmFtZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5QT1NUX05PVElGSUNBVElPTlMiLlJ2YW
  xlZSI6IjEifSwKeyJuYWllIjoieW5kcm9pZC5wZXJtaXNzaW9uLlJFQUJURfUJk1MRUdFRf9Q
  SE9ORV9TVEFURSIIsInZhbHVlIjoIMSj9LA7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUk
  VDRU1WRV9CT09UX0NPTVBMRVRFRClIsInZhbHVlIjoIMSj9LA7Im5hbWUiOiJhbmRyb2lkLnBl
  cm1pc3Npb24uQUNDRVNTX05FVfDPUktfU1RBVEUiLlJ2YWxlZSI6IjEifSwKeyJuYWllIjoieW
  5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19XSUZjX1NUQVRFIiwidmFsdWUiOiIxIn0sCnsibmFt
  ZSI6ImFuZHIJvaWQucGVybWlzc2l2bvi5DSEFOR0VfV0lGSV9TVEFURSIIsInZhbHVlIjoIMSj9LA
```

```
p7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQkxVRVRPT1RIiIiwidmFsdWUiOiIxIn0sCnsi
bmFtZSI6ImFuZHJvaWQucGVybwWlzc2l2vbi5CTFVfVE9PVEhfQURNSU4iLCJ2YWx1ZSI6IjEifS
wKeyJuYW11IjojYW5kcm9pZC5wZXJtaXNzaW9uLkxJMVUVUT09USF9DT05ORUNUiiwidmFsdWUi
OiIxIn0sCnsibmFtZSI6ImFuZHJvaWQucGVybwWlzc2l2vbi5CTFVfVE9PVEhfU0NBtiIsInZhbH
VlIjojMSJ9LAp7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQkxVRVRPT1RiX0FEVksVSVElT
RSIsInZhbHVlIjojMSJ9LAp7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkVBRF9QSE9ORV
9OVU1CRVJTIiwidmFsdWUiOiIxIn0sCnsibmFtZSI6ImFuZHJvaWQucGVybwWlzc2l2vbi5TWVNU
RU1fQUxfulRfV01ORE9XIiwidmFsdWUiOiIxIn0sCnsibmFtZSI6ImFuZHJvaWQucGVybwWlzc2
l2vbi5DQU1FUkEiLCJ2YWx1ZSI6IjEifSswKeyJuYW11IjojYW5kcm9pZC5wZXJtaXNzaW9uLlJF
QURfQVbQX1NQRUNJRk1DX0xPQ0FMRVMiLCJ2YWx1ZSI6IjEifSswKeyJuYW11IjojYW5kcm9pZC
5wZXJtaXNzaW9uLkhJR0hfU0FNUEXJTkdfUkFURV9TRU5TT1JTIiwidmFsdWUiOiIxIn0sCnsi
bmFtZSI6ImFuZHJvaWQucGVybwWlzc2l2vbi5BQ0NFU1NFQ09BU1NFxPQ0FUSU90IiwidmFsdW
UiOiIxIn0sCnsibmFtZSI6ImFuZHJvaWQucGVybwWlzc2l2vbi5BQ0NFU1NFRk1ORV9MT0NBVElP
TiIsInZhbHVlIjojMSJ9LAp7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQUNDRVNTX0JBQ0
tHUK9VTkrfTE9DQVRJT04iLCJ2YWx1ZSI6IjEifSswKeyJuYW11IjojYW5kcm9pZC5wZXJtaXNz
aW9uLlFVRVJZX0FMTF9QQUNLQUdfUyIsInZhbHVlIjojMSJ9LAp7Im5hbWUiOiJhbmRyb2lkLn
Blcm1pc3Npb24uUEFDS0FHRV9VU0FHRV9TVEFUYyIsInZhbHVlIjojMSJ9LAp7Im5hbWUiOiJh
bmRyb2lkLnBlcm1pc3Npb24uRk9SRUdSt1VORF9TRVJWSUNFX0RBVEFfU1lloQyIsInZhbHVlIj
oiMSJ9LAp7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uRk9SRUdSt1VORF9TRVJWSUNFIiwi
dmFsdWUiOiIxInldfv0K" type="string" /></characteristic>
```



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

```
{ "packageName": "com.zebra.zsa", "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" },
```

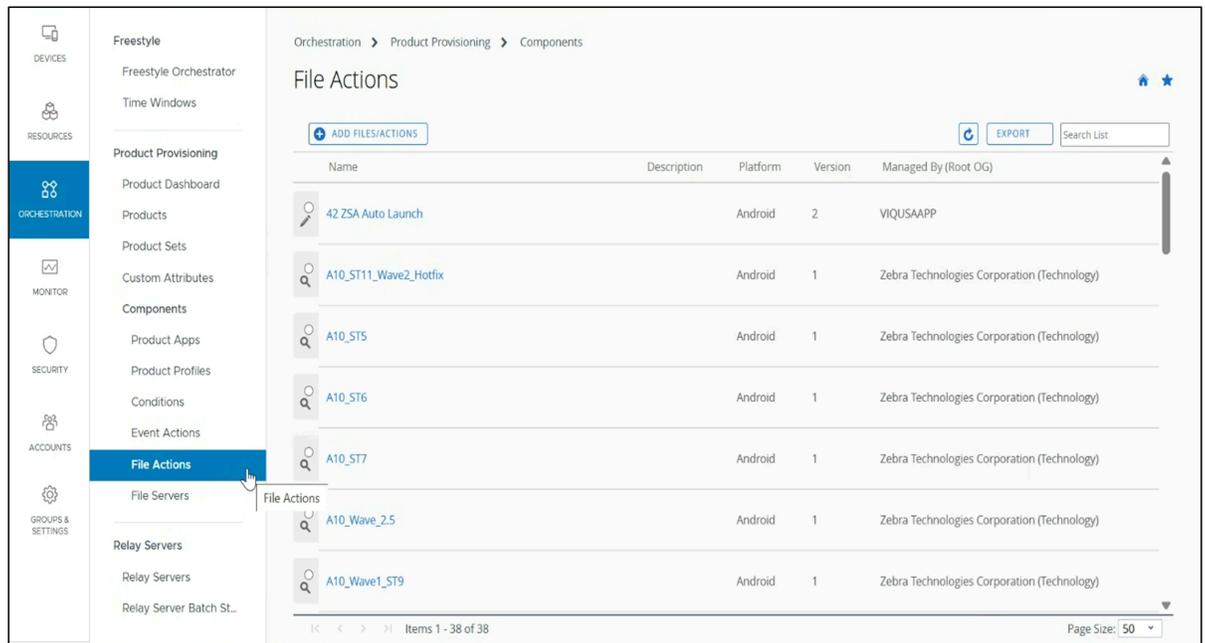
```
{
  "name": "android.permission.SYSTEM_ALERT_WINDOW", "value": "1"},
  "name": "android.permission.CAMERA", "value": "1"},
  "name": "android.permission.READ_APP_SPECIFIC_LOCALES", "value": "1"},
  "name": "android.permission.HIGH_SAMPLING_RATE_SENSORS", "value": "1"},
  "name": "android.permission.ACCESS_COARSE_LOCATION", "value": "1"},
  "name": "android.permission.ACCESS_FINE_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"}
}
```

3. Click **Save**.

Auto-launching Zebra Services Agent

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

1. Select **Orchestration > 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**.



- 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.zsa,class=com.zebra.zsa.ui.splash.SplashActivity
```

```
TimeOut: -1
```

- Click **Save**.

Activating Permissions Product

To activate the Permissions Product:

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

The screenshot shows the 'Add Product' dialog box with the following details:

- Title:** Add Product
- Tab:** General (selected)
- Name ***: ZSA All Permission
- Description**: (empty)
- Managed By ***: TestPlan-DO
- Smart Groups**: ZSA - Test (TestPlan-DO)
- Buttons:** VIEW DEVICE ASSIGNMENT, ADD RULES, SAVE, ACTIVATE, CANCEL

- Click **Save**.
- In the **Manifest** tab, click **Add**.

6. Configure the following information in the **Add Manifest** options.

The screenshot shows the 'Add Product' dialog box with the 'Manifest' tab selected. The dialog contains a table with the following data:

Up	Down	Step Number	Action Type	Persistent	Description	
▲	▼	1	Install Profile	Yes	Profile = Zebra Services Age...	✎ ✕ ▼

Items 1-1 of 1

Buttons: SAVE, ACTIVATE, CANCEL

- Select **Profile Install** from the drop-down list.
- Search for the permissions profile of Zebra Services Agent and select the permissions profile.
- Select the **Persistent** checkbox via enterprise reset.
- Click **Save**.
- Repeat steps **a - e** to add Zebra Services Battery Health permissions.

Creating an Auto-launch Product

To create an Auto-launching Product:

- Go to **Orchestration > Products > Product List View**.
- Click **Add Product**, and select **Android**.

3. In the **General** tab, fill in the **Name**, **Description**, and **Assigned Groups** fields.

Add Product [X]

General Manifest Conditions Deployment Dependencies

Name * ZSA - Auto Launch

Description

Managed By * TestPlan-DO

Smart Groups ZSA - Test (TestPlan-DO) [X]
Start typing to add a group [Q]

VIEW DEVICE ASSIGNMENT

Assignment Rules ADD RULES

SAVE ACTIVATE CANCEL

4. Click **Save**.
5. In the **Manifest** tab, click **Add**.

6. Configure the following information in the **Add Manifest** options.

The screenshot shows the 'Add Product' dialog box with the 'Manifest' tab selected. The dialog has a title bar with a close button (X) and a refresh button (circular arrow). Below the title bar are tabs for 'General', 'Manifest', 'Conditions', 'Deployment', and 'Dependencies'. A '+ ADD' button is on the left, and a refresh button is on the right. A table lists the manifest items:

Up	Down	Step Number	Action Type	Persistent	Description	
▲	▼	1	Install Files/Actions	Yes	Files/Actions = 42 ZSA Auto ...	✎ ✕ ▼

Items 1-1 of 1

At the bottom right, there are three buttons: 'SAVE' (blue), 'ACTIVATE' (white with blue border), and 'CANCEL' (white with blue border).

- Select **File/Action** from the drop-down list.
- Search the auto-launch File/Action for Zebra Services Agent.
- Select the auto-launch File/Action.
- Select the **Persistent** checkbox via enterprise reset.
- Click **Save**.

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



IMPORTANT:

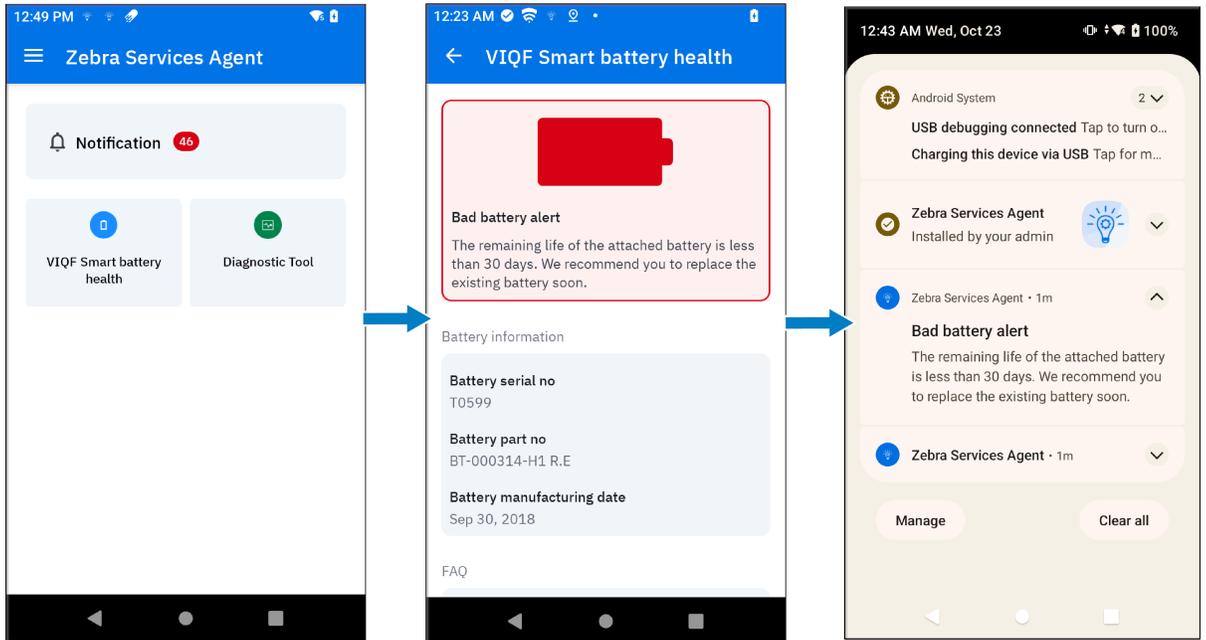
You are only required to **Activate** the Zebra Services Agent autolaunching products from the list of products under Provisioning.

Expected Behaviour After Auto-launching Zebra Services Agent

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

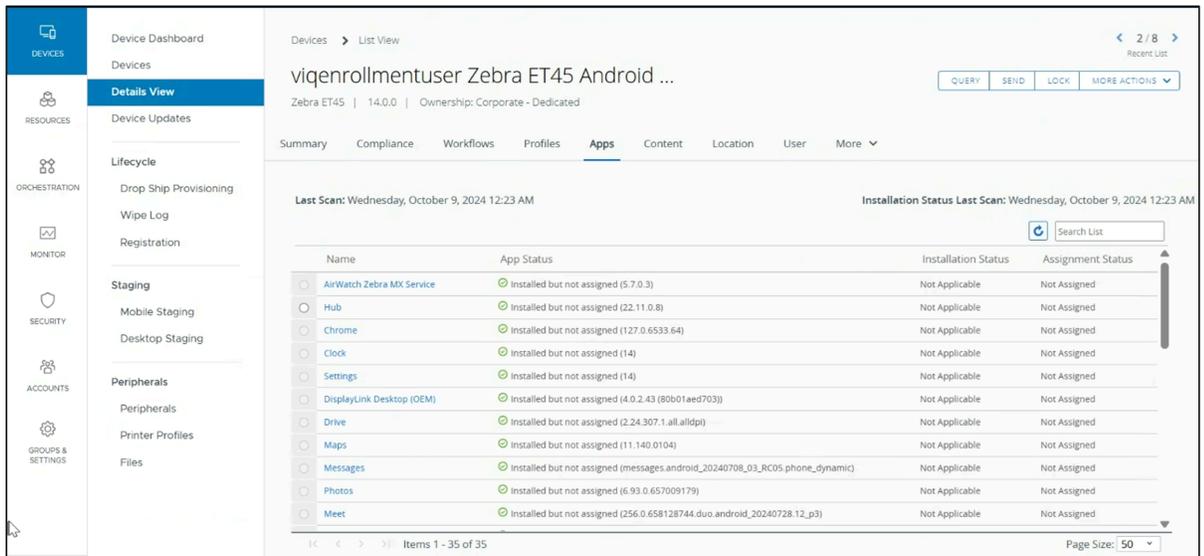
- Auto-launching the ZSA application on your device. The ZSA home screen displays the appropriate entitlement.
- If the ZSBH module is entitled, the ZSA app automatically launches it after a few seconds.

- 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.
- After a few seconds, the ZSA app will close.



FAQs

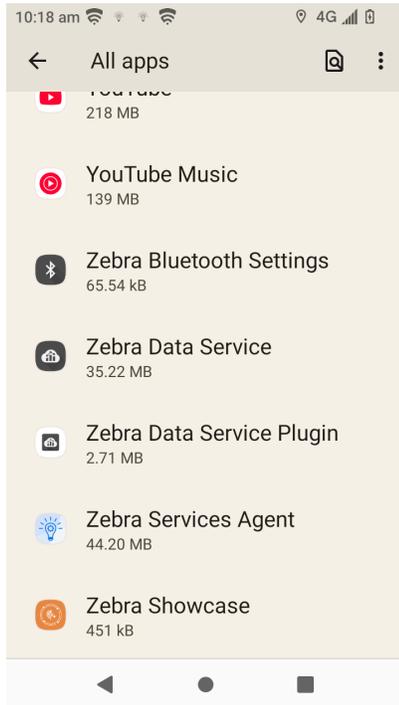
- How do you determine which apps are installed on the devices in AirWatch?
 - Go to **Devices > List View**.
 - Select any device from the list, and it provides information about the selected device.



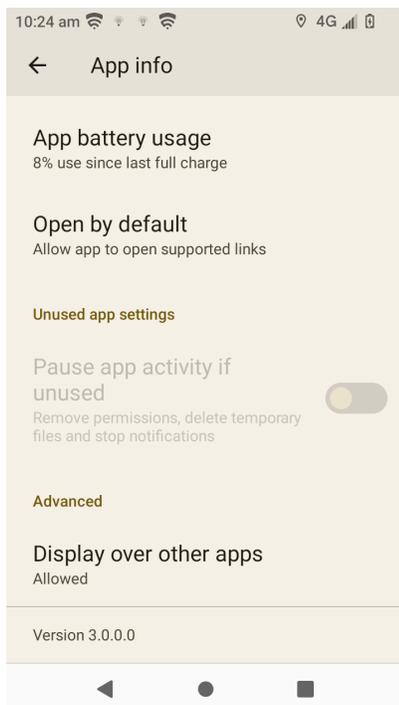
- Click the **Apps** tab, then scroll down or use the **Search** feature to find the ZSA app.

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

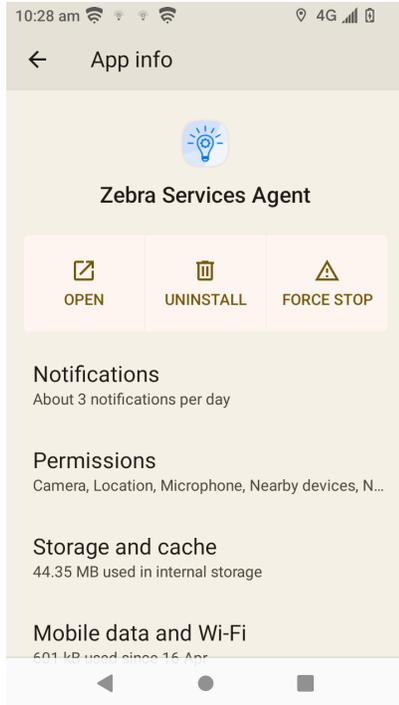
a) To verify the app version, go to **Settings > Apps > All apps** and select **Zebra Services Agent**.



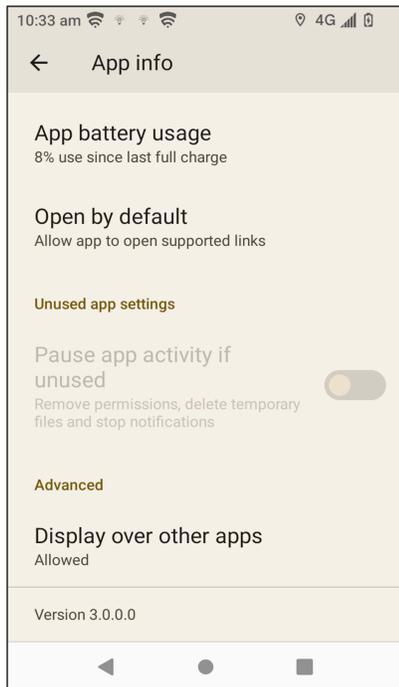
b) The **App Info** page displays the **Version**.



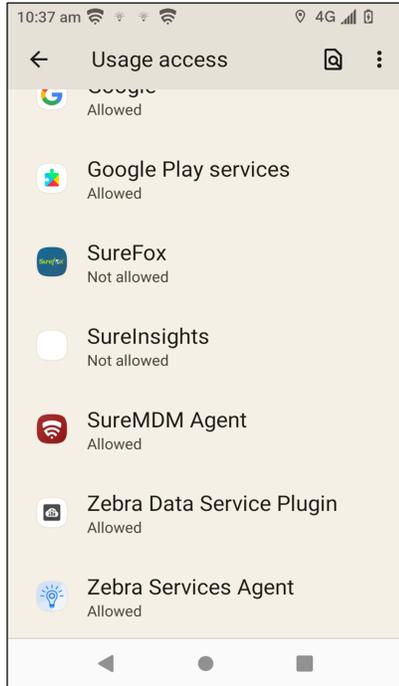
c) To verify the ZSA Permissions, go to **Settings > Apps > All apps > Zebra Services Agent > Permissions**.



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



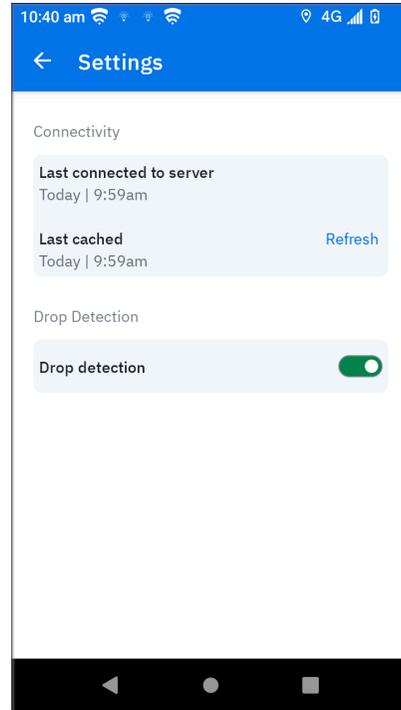
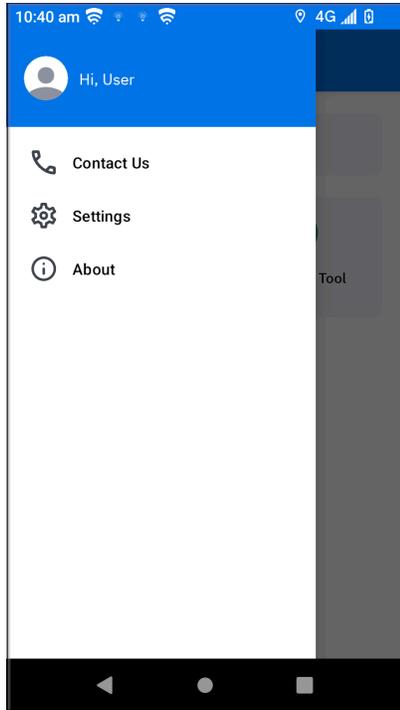
- e) To verify Usage Access permission, go to **Settings > Apps > Special app access > Usage Access > Zebra Service Agent**.



- 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**.

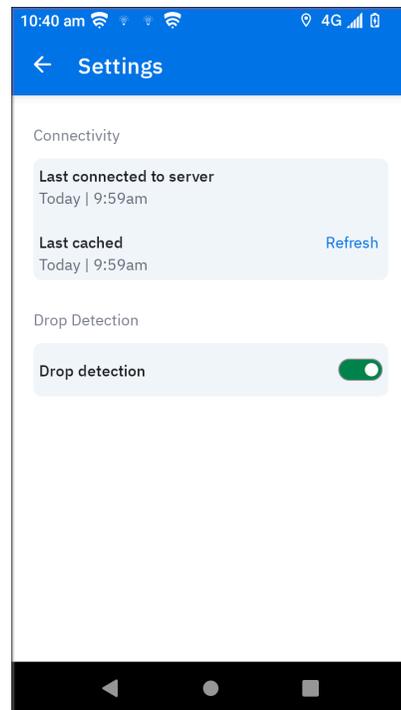
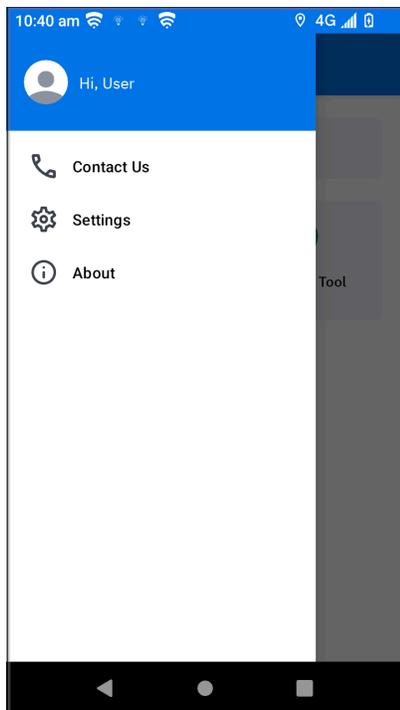


- g) To verify ZSA Network connectivity to the Zebra URL:
Launch ZSA and go to **Settings > Refresh**.



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.

