Zebra Access Management System (ZAMS)

Installation Guide

2025/06/03

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.

Contents

About This Guide

The guide provides information about installing and using the Zebra Access Management System (ZAMS) software that is used with the Zebra Intelligent Cabinet.

ZAMS Overview

The elements of the ZAMS software consists of mobile device application and services, KIOSK application and services, and the Cloud resident console.

- Mobile device application and services - Provides the lock screen user interface (UI) and services for Android-based mobile devices.
- KIOSK application and services - Provides on-site device management, UI, and information to the Cloud-based console. The KIOSK application is designed for the CC6000 device.
- Cloud resident console - the Web portal that provides various administration level tasks and reports. The server access portal is at zams.zebra.com.

Refer to the ZAMS Release Notes on the supported operating system platform for the version-specific supported features.

Installation Tools

The ZAMS installation process can be implemented using several methods, and users can choose a method based on preference and capabilities. This guide focuses on the default installation process, which uses Zebra Value Add (ZVA) and configuration tools such as StageNow and DataWedge. These tools are generic installation methods across Zebra customer environments with automation reuse, which can be configured by most Enterprise Mobility Management (EMM) software products.

Supporting references and notes for other non-ZVA installation options are for information only, and it is not intended to be a complete reference. Refer to the supported files used by the ZVA tools to understand how to reuse and integrate them into a specific support environment.

More references about the ZVA tools are available at techdocs.zebra.com. The ZAMs installation process relies on the following ZVA components:

- DataWedge profiles enable configuring data capture services like barcode scanning outside without the need to modify software applications.
- StageNow barcodes and support files allow for automated installation by scanning barcodes into the device resident StageNow application and service.

- Mobility DNA Extensions (MX) enables configuring an application and device without the need to prompt users.

A typical updated ZAMS release contains the application software and the supporting files applicable to the device that is being installed, such as the mobile device or KIOSK. There is no installation file for the ZAMS portal, however, all ZAMS KIOSKs are required to have connectivity to the portal.

After installing the ZAMS software on the KIOSK and mobile devices for the first time, you must register the software before use. The ZAMS portal can create offline configuration files that can be incorporated into the device and KIOSK for automatic software registration. Therefore, the ZAMS portal is also considered a tool to install the ZAMS software.

Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.

NOTE: The text here indicates information that is supplemental for the user to know and that is not required to complete a task.

IMPORTANT: The text here indicates information that is important for the user to know.

CAUTION: If the precaution is not heeded, the user could receive a minor or moderate injury.

WARNING: If danger is not avoided, the user CAN be seriously injured or killed.

DANGER: If danger is not avoided, the user WILL be seriously injured or killed.

ZAMS Installation Overview

The ZAMS installation process includes completing the installation prerequisites and server setup regardless of the installation method used. Once the installation is completed, update the KIOSK and mobile devices separately.

Contact Zebra Technical Support at supportcommunity.zebra.com/s/contactsupport if you need assistance.

Performing Installation Prerequisites

The initial procedure to install ZAMS is to download the latest software, rename the APK file, and then configure and validate the network.

1. Obtain the latest ZAMS software on the Intelligent Cabinets support page.
2. Download the latest ZAMS software.

   ZAMS is continually updated, and the latest software is posted every quarter. Click **Subscribe to ZAMS Software Updates** on the Intelligent Cabinets support page to receive an email alert when a new version of ZAMS Software is available for download.
3. Rename the APK file.

   You must rename the APK file before installing the file on the mobile device and KIOSK. The APK file downloaded from Zebra support follows a naming convention that includes the version number of the relevant APK. For example, an APK provided in the download is named `ams-device-2.3.16.apk`. Rename the file to `AmsDevice.apk` before the file is pushed to the device or Mobile Device Management (MDM) before installation.
4. Perform network configuration and validation.

   Ensure you meet the ZAMS network requirements so that the KIOSK can communicate to the Cloud portal and the mobile devices can communicate with the KIOSK.
5. ZAMS limitations and recommendations:
   - *Each KIOSK is limited to connecting 300 devices (mobile computers).
   - *Each KIOSK is limited to syncing 5000 registered users, combining both Global and Site Users.

NOTE: *Versions prior to 24.3.0 support 100 devices and 500 registered users per KIOSK.

   - KIOSK and DEVICE must be on the same version, between the current major release (N) and no older than N-2.
6. Before installing the ZAMS APK files on the KIOSK and Device, enable installation from **Unknown Sources**.

7. Before installing the AMS KIOSK app from the ZAMS release version 24.2.0 or later, uninstall both AMS Core and AMS UI.

Performing Server Setup

The next procedure is setting up the server.

1. Create and manage user accounts.

   On the ZAMS Portal at zams.zebra.com, log in with a Company Admin account. ZAMS has one initial admin user only who can create an account for all other users. Before installing ZAMS, create a new Company Admin to log into the ZAMS Portal and a number of Device Users to log into the devices.

2. Create a Cabinet.

   Create Cabinets on the ZAMS Portal before installation by signing in as a Company Admin user. During the installation process and depending on which installation method is used that is outlined in this document, you can:

   - Load a configuration file that is going to automatically configure the Cabinet.
   - Create a Cabinet on the ZAMS user interface after the software is installed on the CC6000.
   - Synchronize a previously created Cabinet on the ZAMS user interface.

3. Create the Cabinet and device configuration files.

   Depending on the installation method used, you may be required to create a Cabinet configuration file and a Cabinet device configuration file. Create these configuration files after logging in as a Company Admin user on the ZAMS Portal. Load the configuration files to the CC6000 KIOSK and mobile device to automatically create the Cabinet on the KIOSK and automatically register the mobile device with a pre-configured Cabinet.

Installation Prerequisites

The ZAMS installation prerequisites process consists of obtaining and downloading the latest ZAMS software, renaming the downloaded APK files, and performing network configuration and validation for the cabinets.

Obtaining the Latest ZAMS Software

Go to the Intelligent Cabinets support page to check for the latest ZAMS software.

ZAMS software undergoes continuous updates to enhance the software and introduce new features. Backward compatibility for legacy systems is maintained.

NOTE: Android operating systems constantly evolve; therefore, ZAMS products and its install base undergo updates, too.

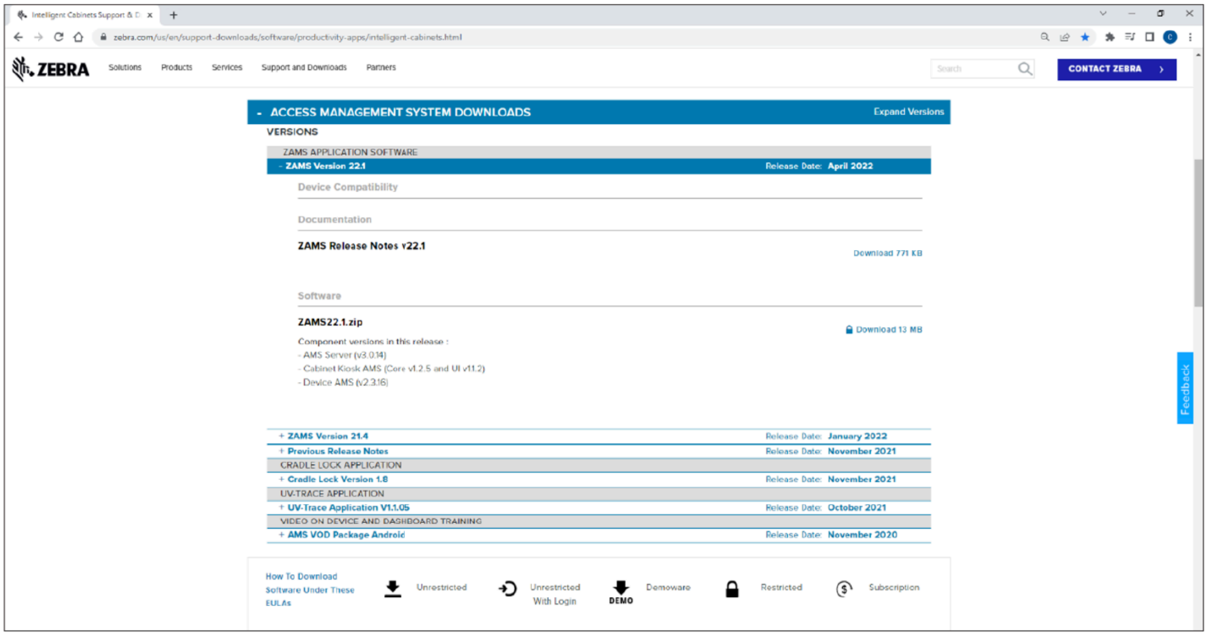
Downloading the Latest ZAMS Software

The KIOSK and mobile device subfolders are in the ZAMS Auto Install folder.

1. Go to the Intelligent Cabinets support page.

2. Download the latest ZAMS release zipped file.

NOTE: ZAMS application is a restricted software, so you must enter a **Contract Number** (1) on the **Alternate Validation Option** screen.


Intelligent Cabinets Support & D
zebra.com/us/en/support-downloads/software/productivity-apps/intelligent-cabinets.html
ZEBRA
Solutions
Products
Services
Support and Downloads
Partners
Search
CONTACT ZEBRA
Feedback

- ACCESS MANAGEMENT SYSTEM DOWNLOADS — Expand Versions

VERSIONS

ZAMS APPLICATION SOFTWARE

- ZAMS Version 22.1 — Release Date: April 2022

Device Compatibility

Documentation

ZAMS Release Notes v22.1 — Download 771 KB

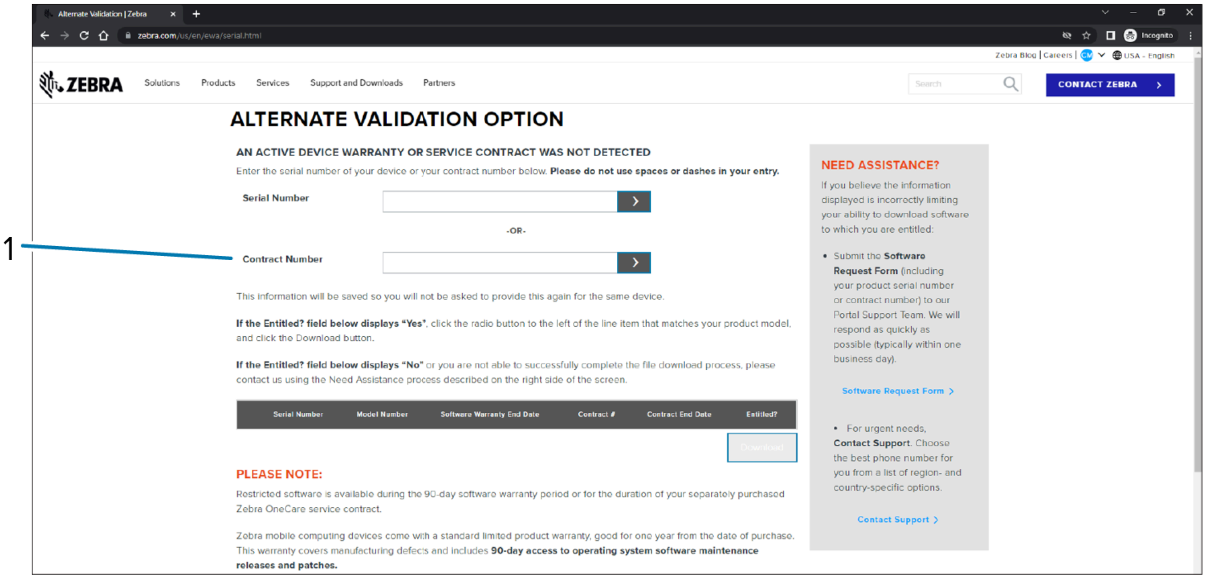
Software

ZAMS22.1.zip — Download 13 MB

Component versions in this release :
- AMS Server (v3.0.14)
- Cabinet Kiosk AMS (Core v1.2.5 and UI v1.1.2)
- Device AMS (v2.3.16)

+ ZAMS Version 21.4	Release Date: January 2022
+ Previous Release Notes	Release Date: November 2021
CRADLE LOCK APPLICATION	
+ Cradle Lock Version 1.8	Release Date: November 2021
UV-TRACE APPLICATION	
+ UV-Trace Application V1.1.05	Release Date: October 2021
VIDEO ON DEVICE AND DASHBOARD TRAINING	
+ AMS VOD Package Android	Release Date: November 2020

How To Download Software Under These EULAs — Unrestricted — Unrestricted With Login — DEMO Demoware — Restricted — Subscription



ALTERNATE VALIDATION OPTION

AN ACTIVE DEVICE WARRANTY OR SERVICE CONTRACT WAS NOT DETECTED

Enter the serial number of your device or your contract number below. **Please do not use spaces or dashes in your entry.**

Serial Number

-OR-

Contract Number

This information will be saved so you will not be asked to provide this again for the same device.

If the Entitled? field below displays "Yes", click the radio button to the left of the line item that matches your product model, and click the Download button.

If the Entitled? field below displays "No" or you are not able to successfully complete the file download process, please contact us using the Need Assistance process described on the right side of the screen.

Serial Number	Model Number	Software Warranty End Date	Contract #	Contract End Date	Entitled?

PLEASE NOTE:

Restricted software is available during the 90-day software warranty period or for the duration of your separately purchased Zebra OneCare service contract.

Zebra mobile computing devices come with a standard limited product warranty, good for one year from the date of purchase. This warranty covers manufacturing defects and includes **90-day access to operating system software maintenance releases and patches.**

NEED ASSISTANCE?

If you believe the information displayed is incorrectly limiting your ability to download software to which you are entitled:

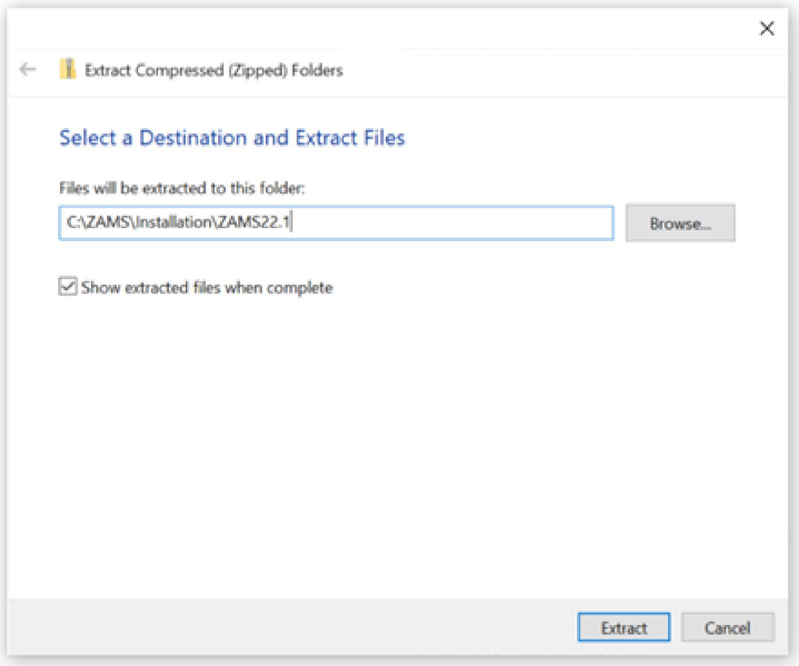
- Submit the **Software Request Form** (including your product serial number or contract number) to our Portal Support Team. We will respond as quickly as possible (typically within one business day).

Software Request Form >

- For urgent needs, **Contact Support**. Choose the best phone number for you from a list of region- and country-specific options.

Contact Support >

3. Extract the downloaded zipped file.



Extract Compressed (Zipped) Folders

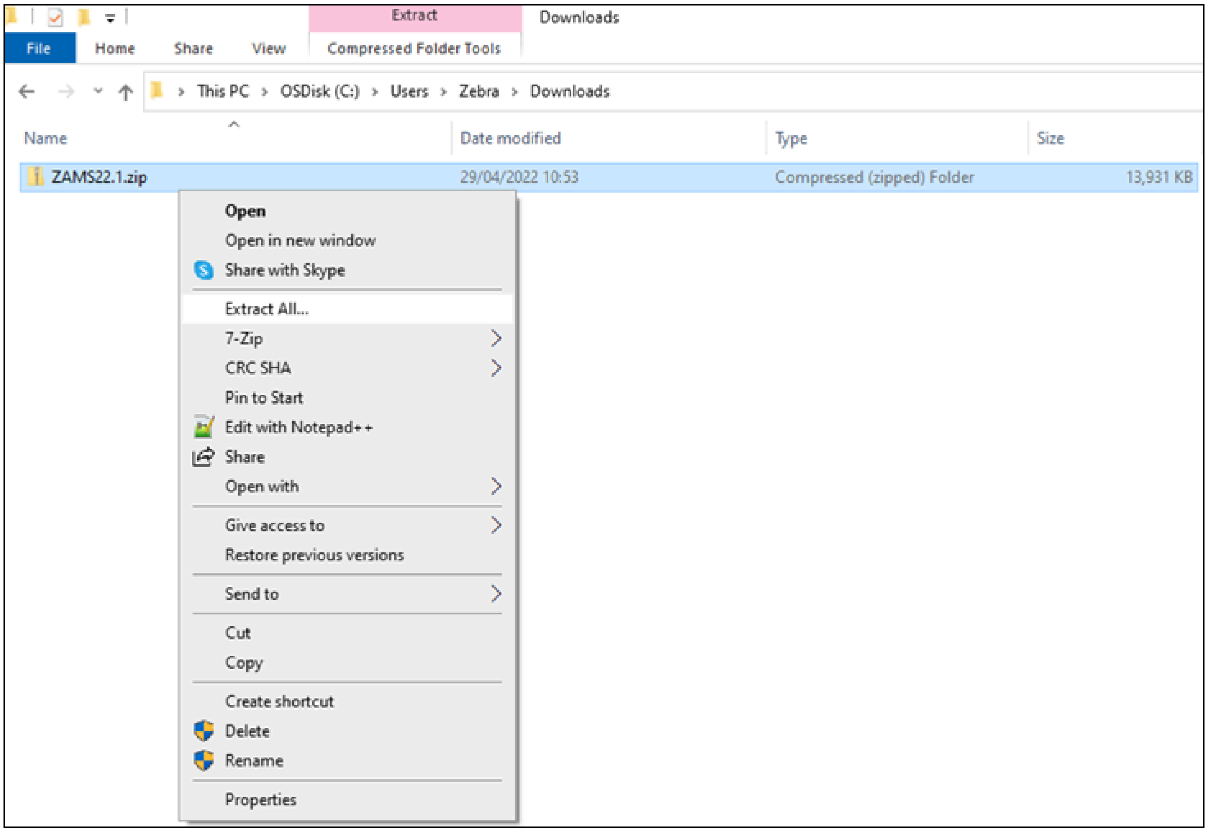
Select a Destination and Extract Files

Files will be extracted to this folder:

C:\ZAMS\Installation\ZAMS22.1

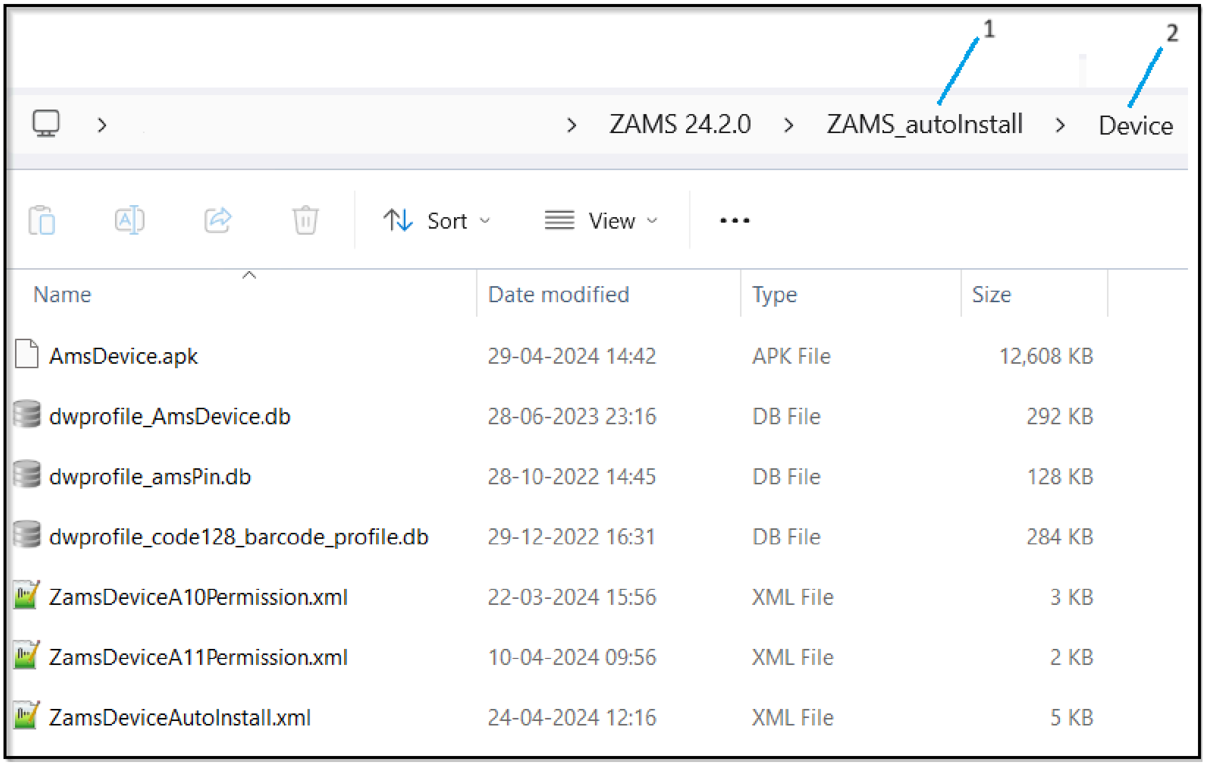
☑ Show extracted files when complete

4. Select a destination to extract the files.

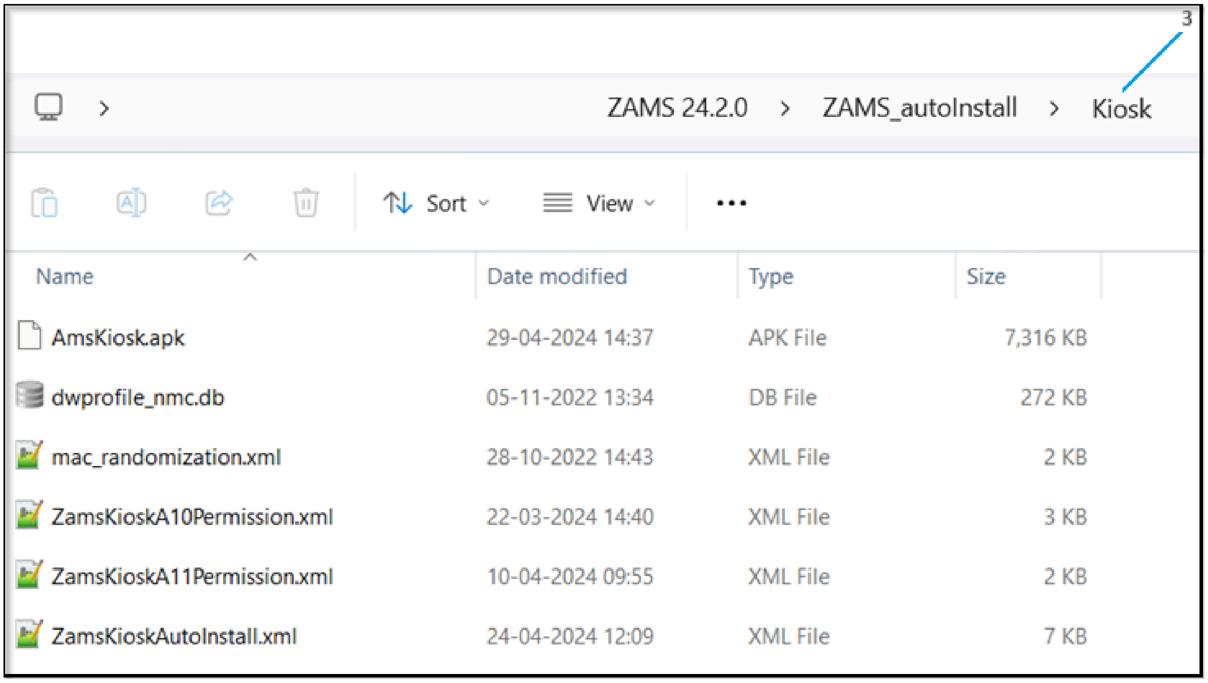


Name	Date modified	Type	Size
ZAMS22.1.zip	29/04/2022 10:53	Compressed (zipped) Folder	13,931 KB

5. After the files have been extracted, in the subfolders in the ZAMS Auto Install folder (1), locate the installation files for the mobile devices (2) and the KIOSK (3).



Name	Date modified	Type	Size
AmsDevice.apk	29-04-2024 14:42	APK File	12,608 KB
dwprofile_AmsDevice.db	28-06-2023 23:16	DB File	292 KB
dwprofile_amsPin.db	28-10-2022 14:45	DB File	128 KB
dwprofile_code128_barcode_profile.db	29-12-2022 16:31	DB File	284 KB
ZamsDeviceA10Permission.xml	22-03-2024 15:56	XML File	3 KB
ZamsDeviceA11Permission.xml	10-04-2024 09:56	XML File	2 KB
ZamsDeviceAutoInstall.xml	24-04-2024 12:16	XML File	5 KB

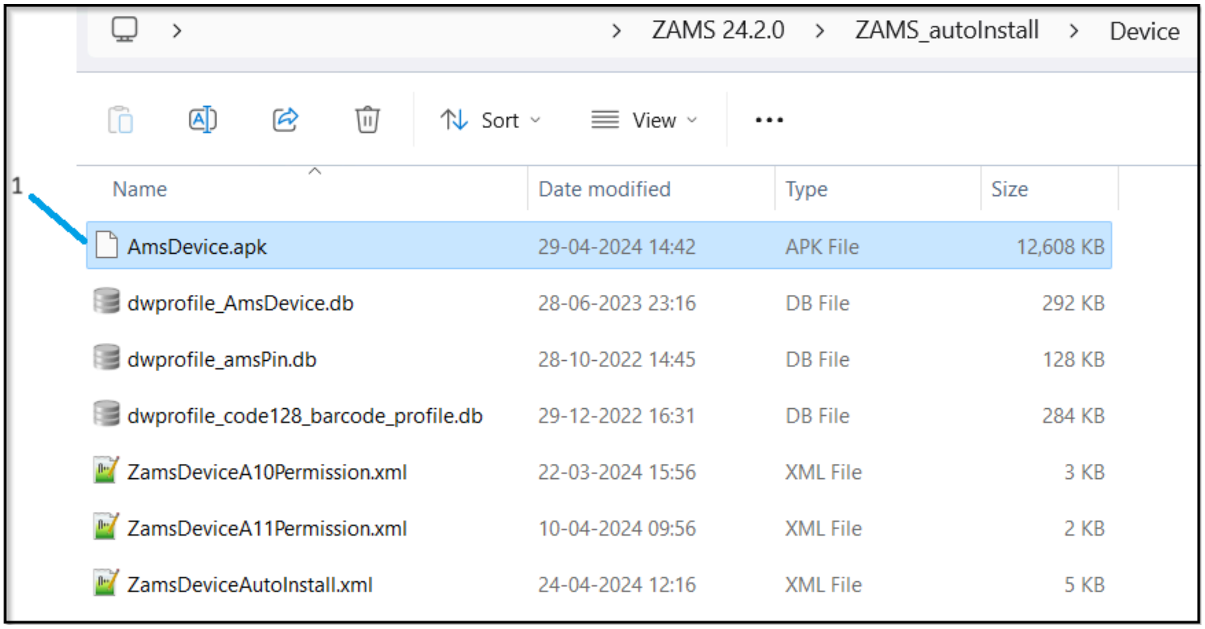


Name	Date modified	Type	Size
AmsKiosk.apk	29-04-2024 14:37	APK File	7,316 KB
dwprofile_nmc.db	05-11-2022 13:34	DB File	272 KB
mac_randomization.xml	28-10-2022 14:43	XML File	2 KB
ZamsKioskA10Permission.xml	22-03-2024 14:40	XML File	3 KB
ZamsKioskA11Permission.xml	10-04-2024 09:55	XML File	2 KB
ZamsKioskAutoInstall.xml	24-04-2024 12:09	XML File	7 KB

Renaming the APK Files

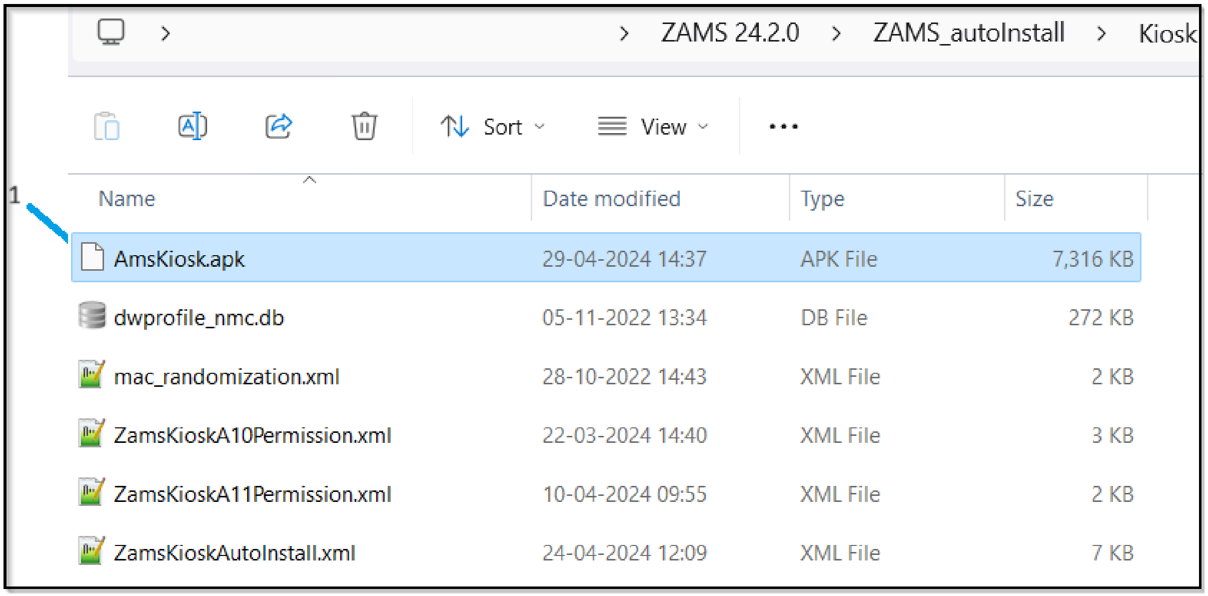
Before installing ZAMS software on the KIOSK and mobile devices, rename some files in the extracted zipped file. The name of the APK file downloaded from Zebra support follows a naming convention that includes a version number of the APK. For example, `ams-device-2.3.16.apk`. The file name identifies the version of the APK in use and ensures that the most recent version of the APK is installed.

1. In the **Device** folder, rename `ams-device-x.x.x.apk` to `AmsDevice.apk` (1).



Name	Date modified	Type	Size
AmsDevice.apk	29-04-2024 14:42	APK File	12,608 KB
dwprofile_AmsDevice.db	28-06-2023 23:16	DB File	292 KB
dwprofile_amsPin.db	28-10-2022 14:45	DB File	128 KB
dwprofile_code128_barcode_profile.db	29-12-2022 16:31	DB File	284 KB
ZamsDeviceA10Permission.xml	22-03-2024 15:56	XML File	3 KB
ZamsDeviceA11Permission.xml	10-04-2024 09:56	XML File	2 KB
ZamsDeviceAutoInstall.xml	24-04-2024 12:16	XML File	5 KB

2. In the **KIOSK** folder, rename the following APK file name:
   - Rename `ams-kiosk-x-x-x.apk` to `AmsKiosk.apk` (1).

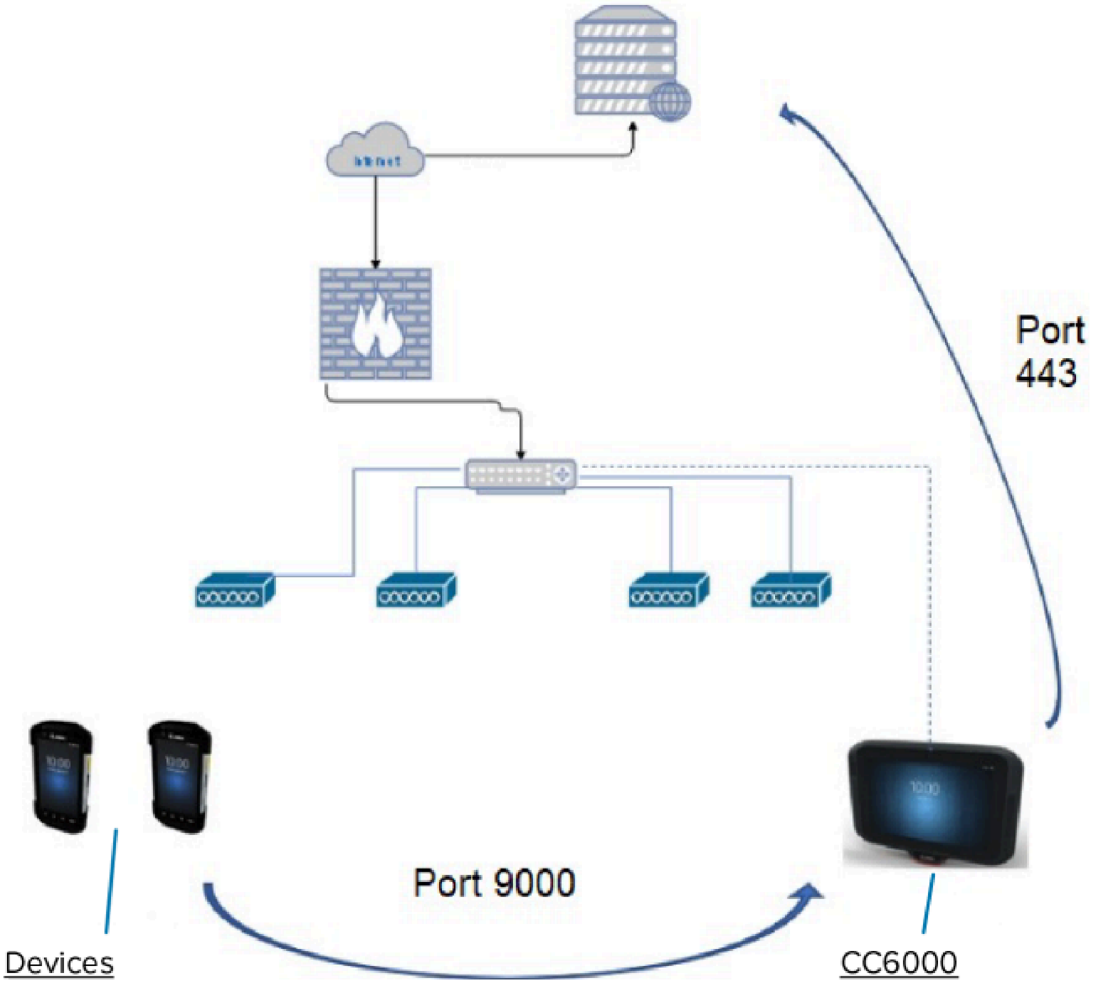


Name	Date modified	Type	Size
AmsKiosk.apk	29-04-2024 14:37	APK File	7,316 KB
dwprofile_nmc.db	05-11-2022 13:34	DB File	272 KB
mac_randomization.xml	28-10-2022 14:43	XML File	2 KB
ZamsKioskA10Permission.xml	22-03-2024 14:40	XML File	3 KB
ZamsKioskA11Permission.xml	10-04-2024 09:55	XML File	2 KB
ZamsKioskAutoInstall.xml	24-04-2024 12:09	XML File	7 KB

Network Configuration and Requirements

ZAMS has three key components: Cloud portal, Cabinet APKs, and device APK. Communication between the three key components is crucial to ensure the ZAMS software works. Therefore, ensure the required network configurations are met before deploying the application in the environment.

Figure 1 ZAMS Network



The C6000 KIOSK requirements are:

- Static IP address
- Wi-Fi or Ethernet access to zams.zebra.com
- TCP port 443 open
- Apply proxy settings (if required).

The mobile device requirements are:

- Wi-Fi enabled
- Wi-Fi or WLAN connectivity to the CC6000
- TCP port 9000 is used between mobile devices and CC6000 by default.

Server Setup

The server setup process consists of creating the user accounts to log into the ZAMS network, and setting up the Cabinet in the ZAMS portal.

User Management

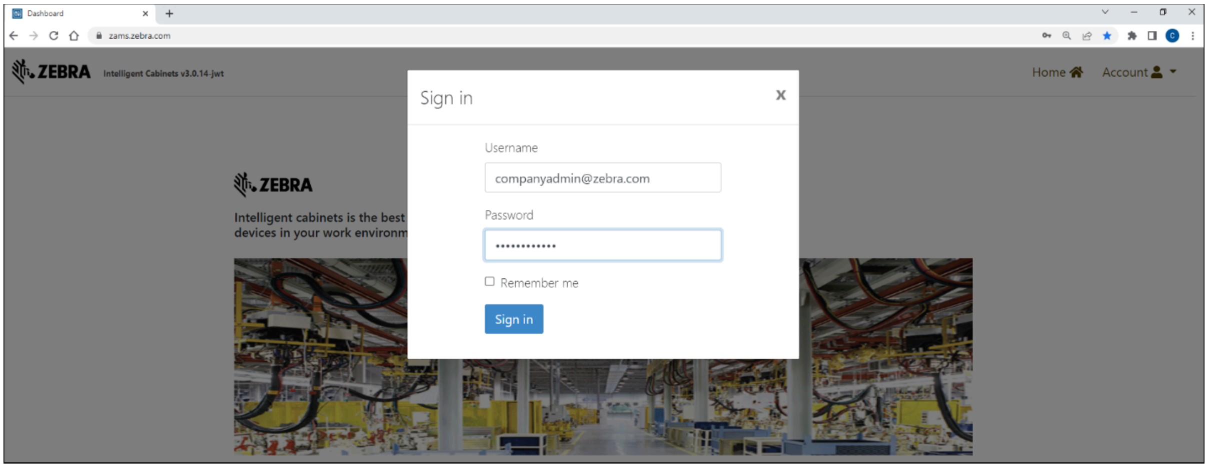
Before installing ZAMS KIOSK and mobile device APKs, create a new **Company Admin** user for the ZAMS Portal access. For initial testing, create at least three to five **Device Users** to log into the devices.

Create a **Company Admin** user solely for the Cabinet registration. Once the username and password of this **Company Admin** user are configured, they should not be changed to prevent the Cabinet from prompting new credentials.

Creating a User Account

Create user accounts in zams.zebra.com before installing ZAMS software.

1. Log into the ZAMS Portal at zams.zebra.com with the Company Admin credentials.

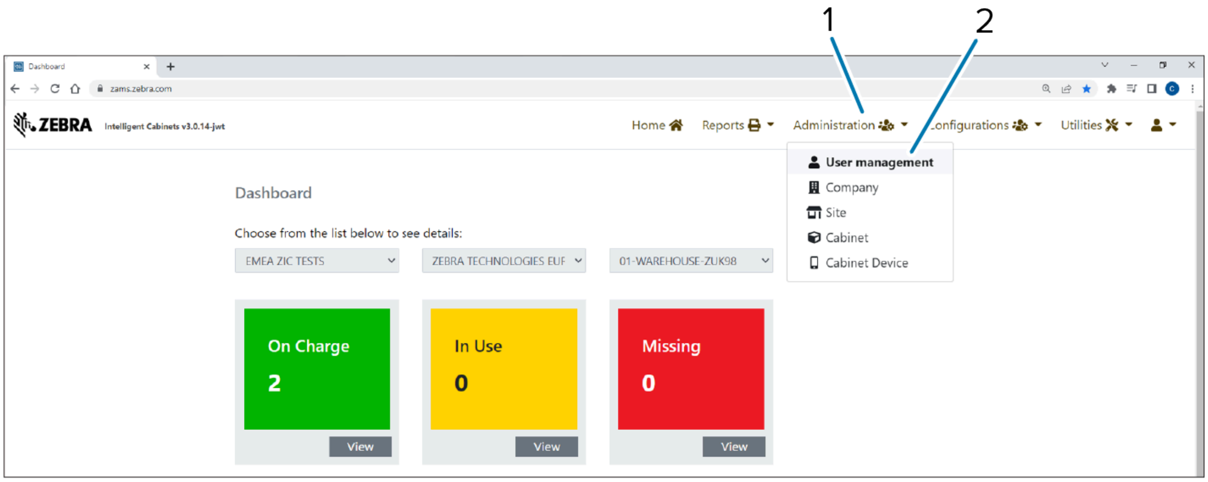

Dashboard
zams.zebra.com
ZEBRA
Intelligent Cabinets v3.0.14-jwt
Home
Account
ZEBRA
Intelligent cabinets is the best
devices in your work environm
Sign in
x
□ Remember me
Sign in

Sign in

Username: companyadmin@zebra.com

Password: ••••••••••••

2. On the **Dashboard** screen, select **Administration** (1) › **User Management** (2).



Dashboard

Choose from the list below to see details:

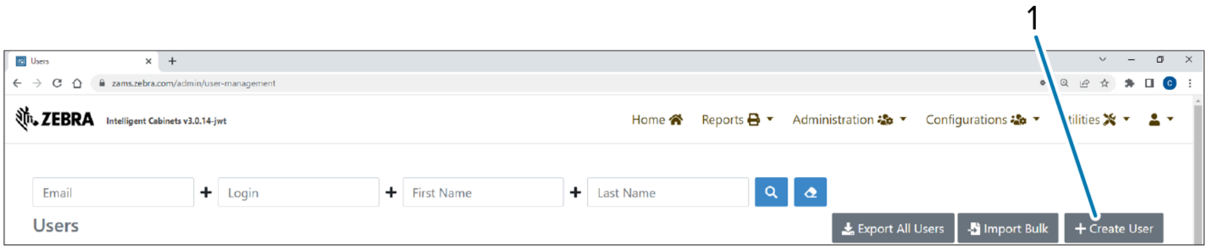
EMEA ZIC TESTS | ZEBRA TECHNOLOGIES EUF | 01-WAREHOUSE-ZUK98

On Charge 2

In Use 0

Missing 0

3. Click + **Create User** (1).

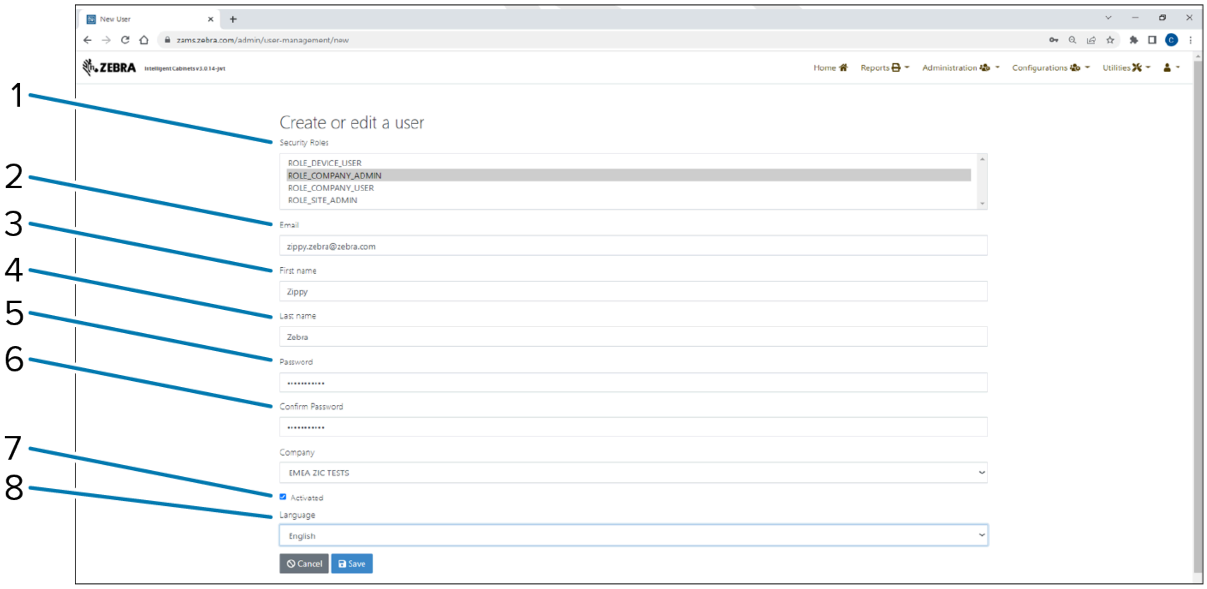


Creating a Company Admin User

A Company Admin User is an administrator account with full access to manage settings and configurations on the ZAMS Portal. The Company Admin is able to create and manage users and Cabinets, Return Material Authorization (RMA) and Beyond Economical Repair (BER) devices, view reports, generate configuration files, and generate a Master Unlock Code.

To open the **Create or edit a user** screen, see Creating a User Account on page 16.

1. From the **Create or edit a user** screen, select the **ROLE_COMPANY_ADMIN** in the **Security Roles** drop-down list (1).


1
2
3
4
5
6
7
8
New User
zams.zebra.com/admin/user-management/new
ZEBRA Intelligent Cabinets v3.0.14-jwt
Home
Reports
Administration
Configurations
Utilities

Create or edit a user

Security Roles

ROLE_DEVICE_USER
ROLE_COMPANY_ADMIN
ROLE_COMPANY_USER
ROLE_SITE_ADMIN

Email: zippy.zebra@zebra.com

First name: Zippy

Last name: Zebra

Password: ••••••••••••

Confirm Password: ••••••••••••

Company: EMEA ZIC TESTS

☑ Activated

Language: English

Cancel | Save

2. Complete the **Email** (2), **First name** (3), and **Last name** (4) fields.
3. Create a **Password** (5) that complies with the indicated criteria.
4. Enter the password again in the **Confirm Password** (6) field.
5. Check the **Activated** (7) box.
6. Select **Language** (8) from the drop-down list.
7. Click **Save**.

A Company Admin user is created and this user has access to the ZAMS Portal.

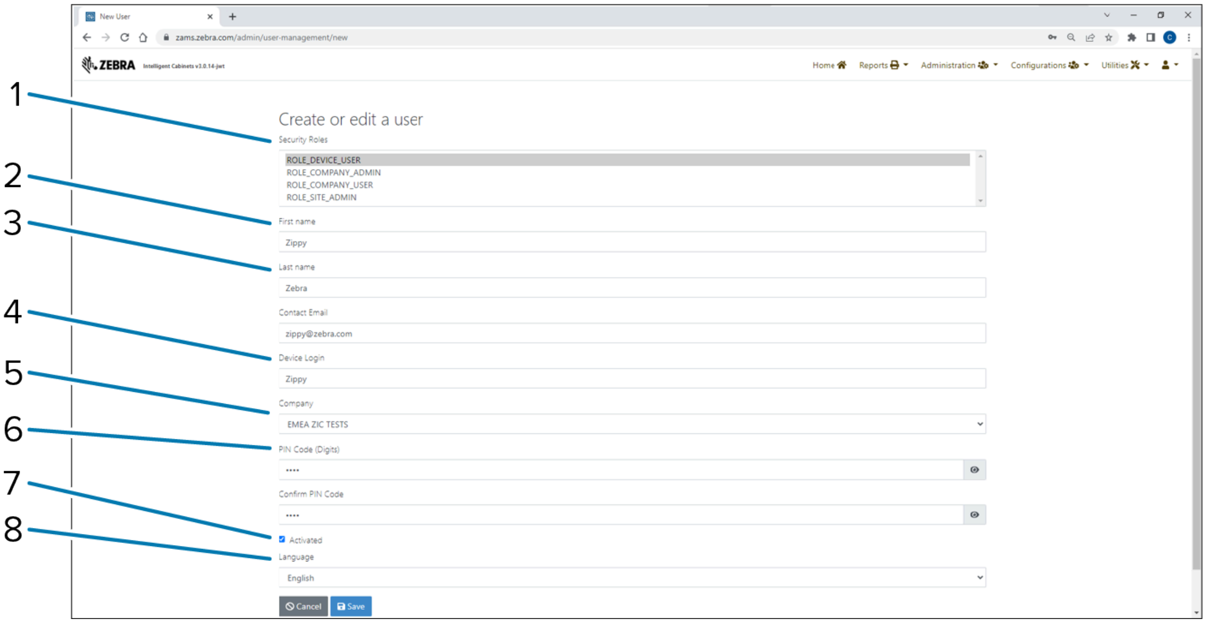
Creating a Device User

A Device User is an account that is used by an operator to log into a mobile device manually by entering a unique PIN code on the device, or scanning the PIN code from a barcode on an ID badge. The Device User does not have access to the ZAMS Portal, but can only use the unique PIN Code to log into a mobile device.

To open the **Create or edit a user** screen, see Creating a User Account on page 16.

NOTE: The **Device Login** account is used to identify the user who has a specific device that is in use and the account is displayed on the ZAMS Cabinet and ZAMS Portal.

1. From the **Create or edit a user** screen, select the **ROLE_DEVICE_USER** in the **Security Roles** drop-down list (1).


1
2
3
4
5
6
7
8
New User
zams.zebra.com/admin/user-management/new
ZEBRA Intelligent Cabinets v3.0.14-jwt
Home
Reports
Administration
Configurations
Utilities
Cancel
Save

Create or edit a user

Security Roles
ROLE_DEVICE_USER
ROLE_COMPANY_ADMIN
ROLE_COMPANY_USER
ROLE_SITE_ADMIN

First name: Zippy

Last name: Zebra

Contact Email: zippy@zebra.com

Device Login: Zippy

Company: EMEA ZIC TESTS

PIN Code (Digits): ••••

Confirm PIN Code: ••••

☑ Activated

Language: English

2. Complete the **First name** (2), **Last name** (3), and **Device Login** (4) fields.
3. Assign the User to a specific **Site** or create a **Global** user from the **Site Id / Name** (5) drop-down list.
4. Enter a unique **PIN Code** (6).
5. Check the **Activated** (7) box.
6. Select **Language** (8) from the drop-down list.
7. Click **Save**.

A Device User is created and this user can now log into a device.

Cabinet Setup

ZAMS requires KIOSK APKs to be installed on the KIOSK when setting up a Cabinet. Users can use two methods to set up the Cabinet.

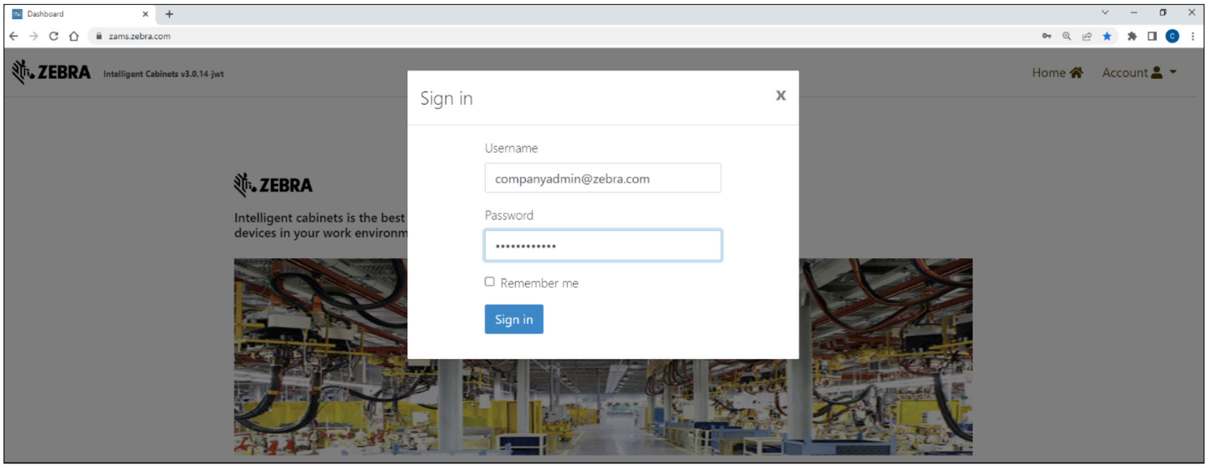
The first method is to configure the Cabinet in the ZAMS Portal when users log in as a Company Admin. This method allows for a configuration file to be created and pushed to the KIOSK during the installation process, which automatically sets up the Cabinet on the KIOSK.

The second method allows a Company Admin to create the Cabinet on the KIOSK after the KIOSK APK is installed. This method allows a Company Admin to enter the credentials on the KIOSK to create a new Cabinet or synchronize an existing Cabinet that was created on the ZAMS Portal previously.

Setting up a Cabinet on ZAMS Portal

Set up a Cabinet on the ZAMS Portal at zams.zebra.com.

1. Log into the ZAMS Portal at zams.zebra.com with the Company Admin credentials.



Dashboard
zams.zebra.com
ZEBRA Intelligent Cabinets v3.0.14-jwt
Home
Account
Intelligent cabinets is the best
devices in your work environm
Sign in

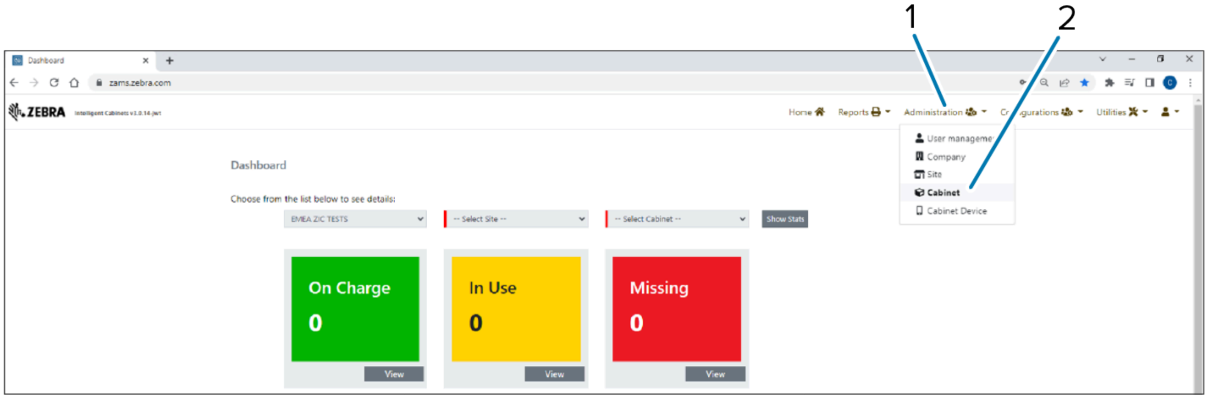
Username: companyadmin@zebra.com

Password: ••••••••••••

□ Remember me

The ZAMS Portal Dashboard displays.

2. Select **Administration** (1) › **Cabinet** (2).

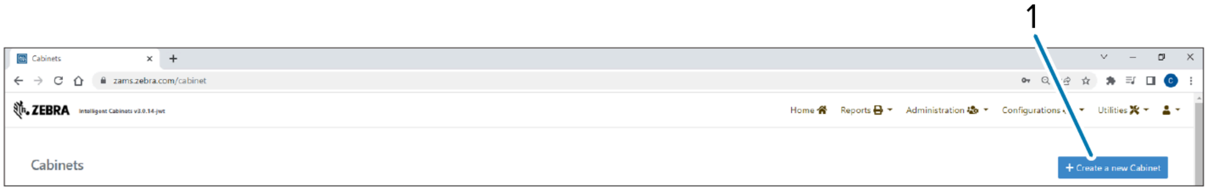


Choose from the list below to see details:

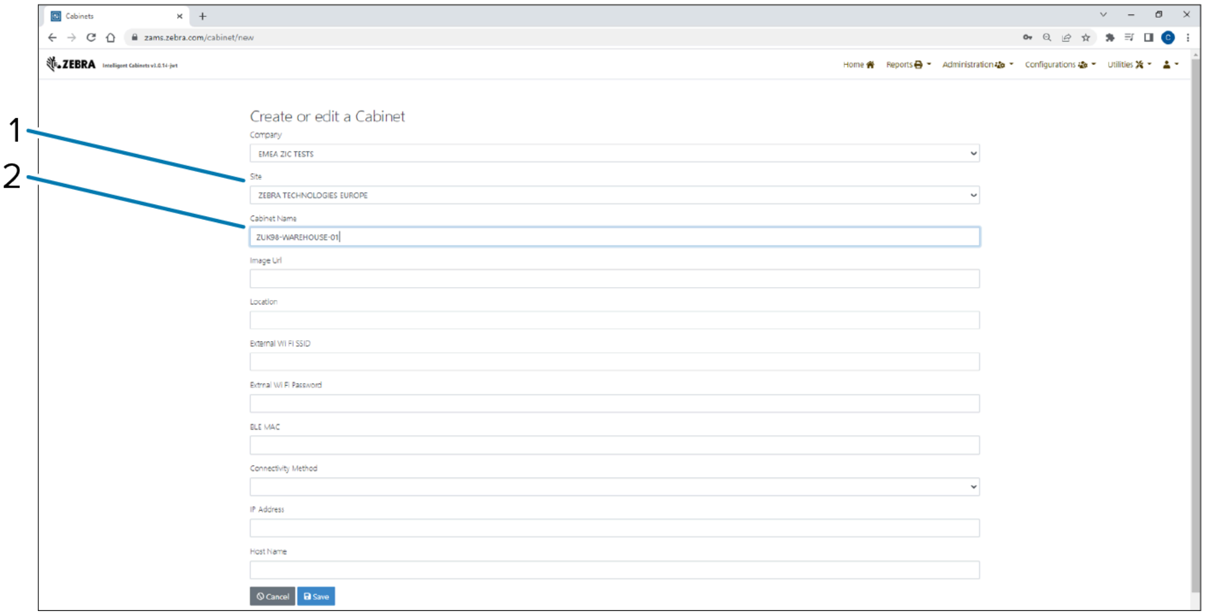
EMEA ZIC TESTS | -- Select Site -- | -- Select Cabinet --

On Charge 0 | In Use 0 | Missing 0

3. Click **+ Create a new Cabinet** (1).



4. Select a site from the **Site** drop-down list (1), and then enter a **Cabinet Name** (2).



Create or edit a Cabinet

Company: EMEA ZIC TESTS

Site: ZEBRA TECHNOLOGIES EUROPE

Cabinet Name: ZUK98-WAREHOUSE-01

Image Url

Location

External WI FI SSID

Extrnal WI FI Password

BLE MAC

Connectivity Method

IP Address

Host Name

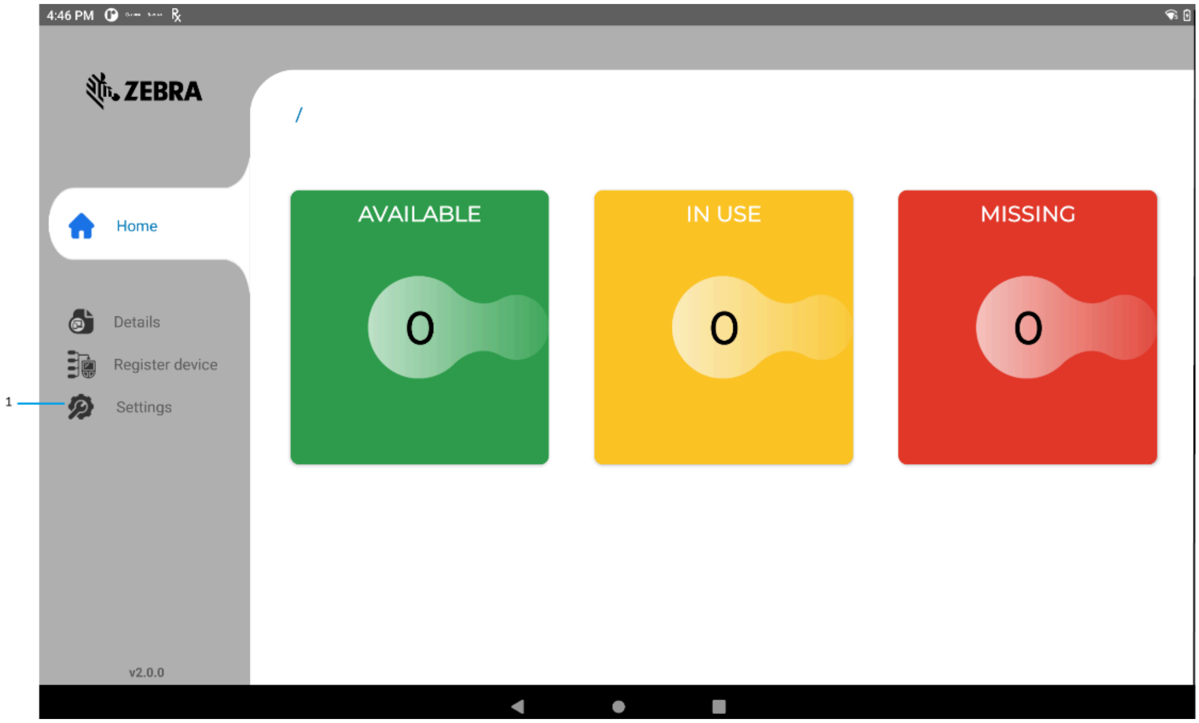
5. Click **Save**.

A Cabinet is created.

Setting up a Cabinet on the KIOSK

After ZAMS is installed on the KIOSK, users can set up the Cabinet through the ZAMS user interface on the KIOSK. The Company Admin credentials are required to create a new Cabinet.

1. To set up the Cabinet in the KIOSK, touch **Settings** (1) on the ZAMS Home screen.

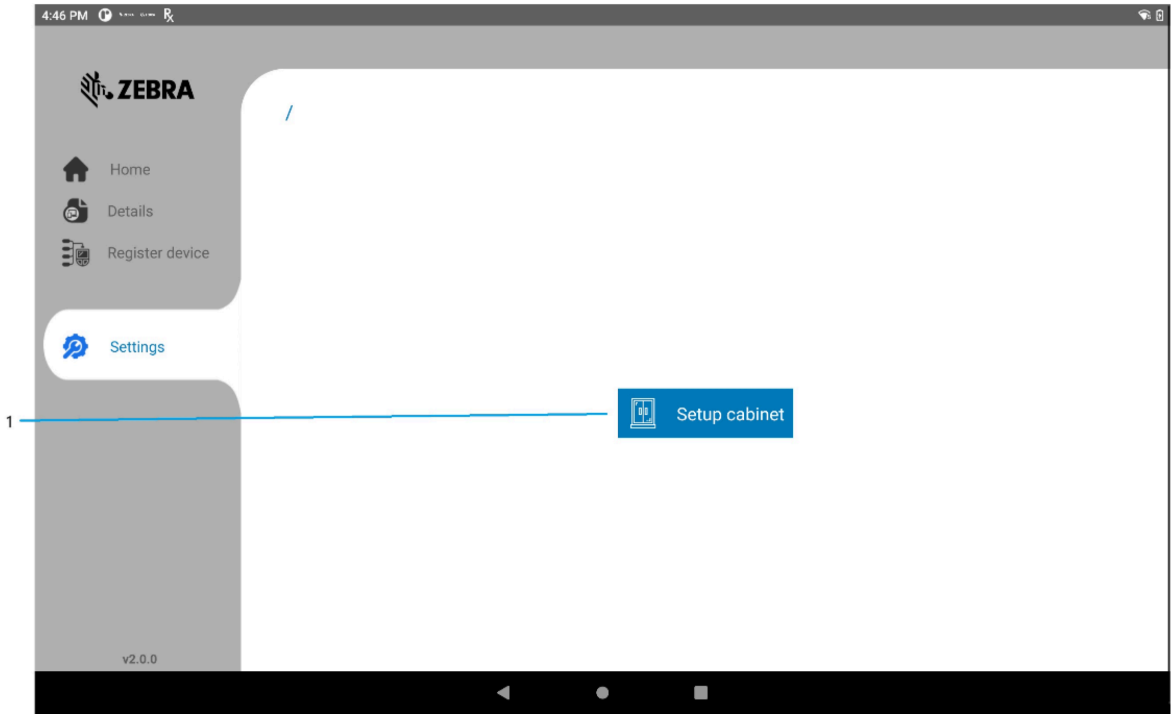


AVAILABLE 0

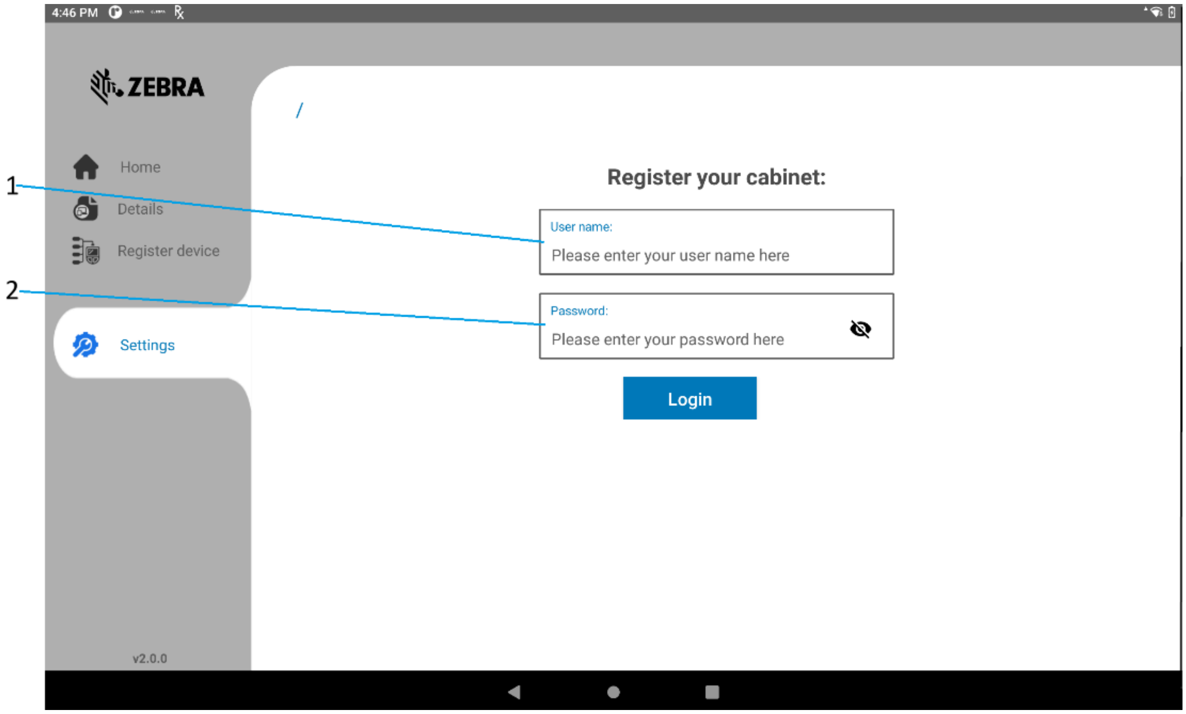
IN USE 0

MISSING 0

2. Touch **Setup cabinet** (1).



3. Enter a **Username** (1) and **Password** (2) of a user with the Company Admin credentials, and then click **Login**.

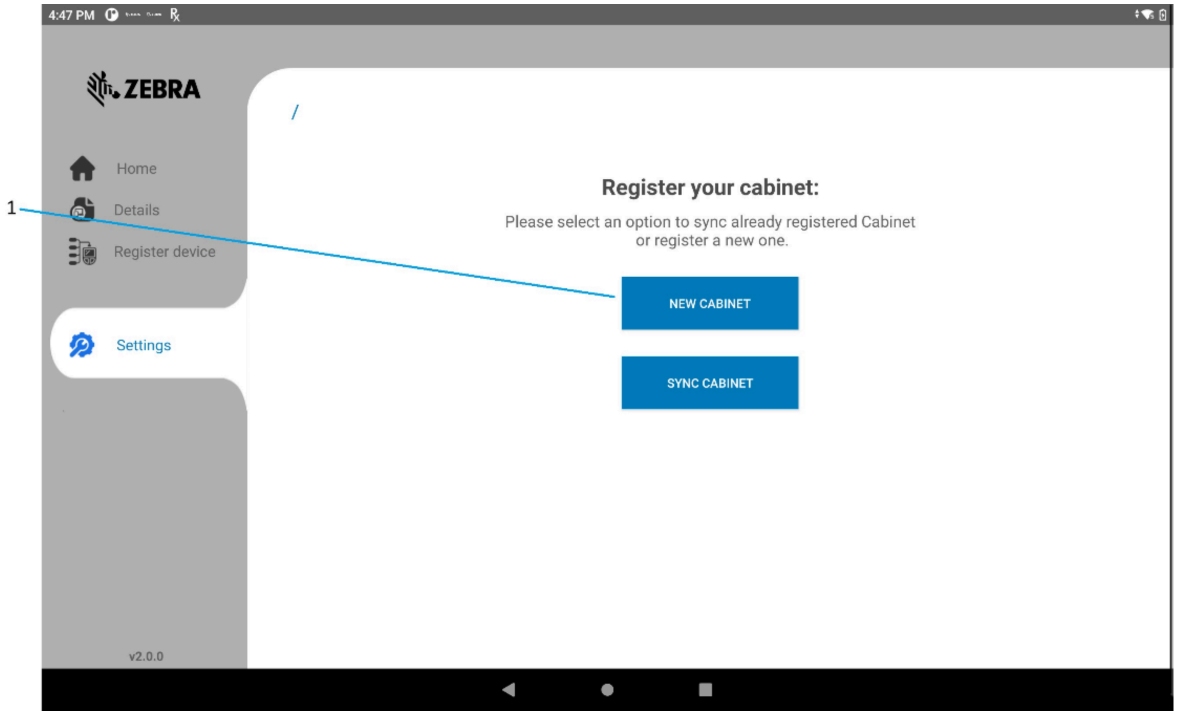


Register your cabinet:

User name: Please enter your user name here

Password: Please enter your password here

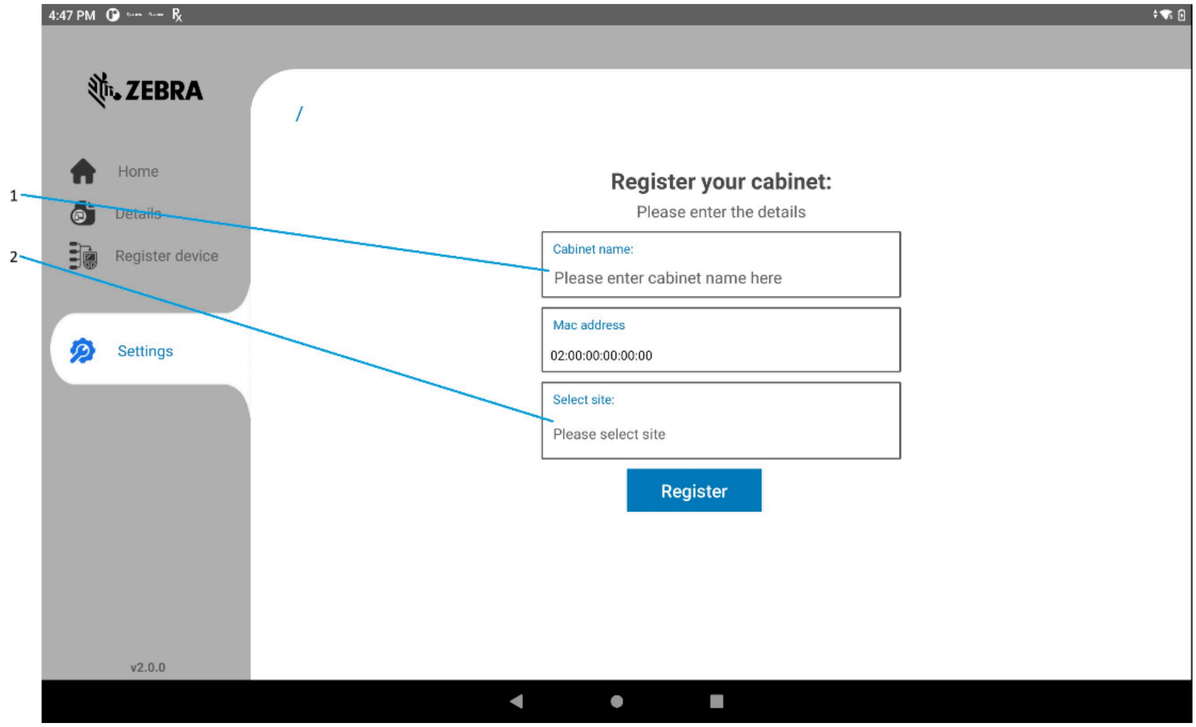
4. Click **NEW CABINET** (1).



Register your cabinet:

Please select an option to sync already registered Cabinet or register a new one.

5. Enter a new **Cabinet name** (1) and select a site from the **Select site** (2) drop-down list.



Register your cabinet:

Please enter the details

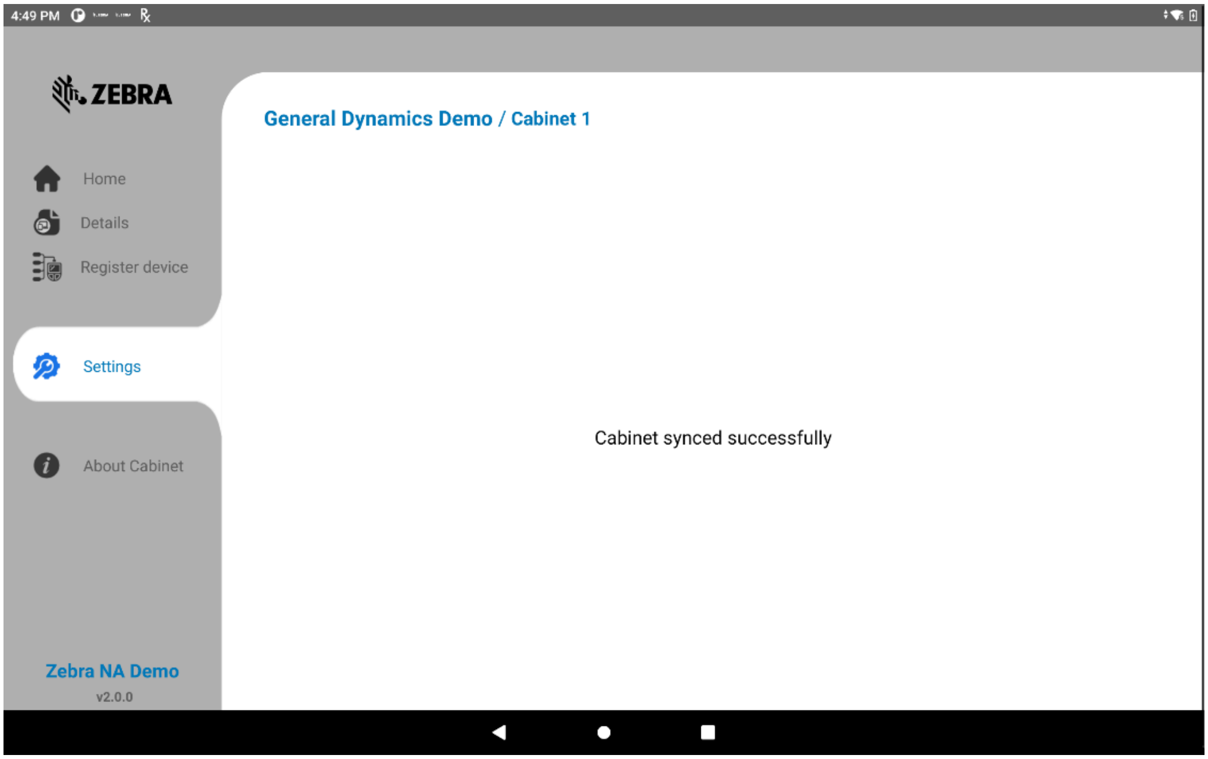
Cabinet name:
Please enter cabinet name here

Mac address
02:00:00:00:00:00

Select site:
Please select site

6. Click **Register**.

   A Cabinet is registered successfully.



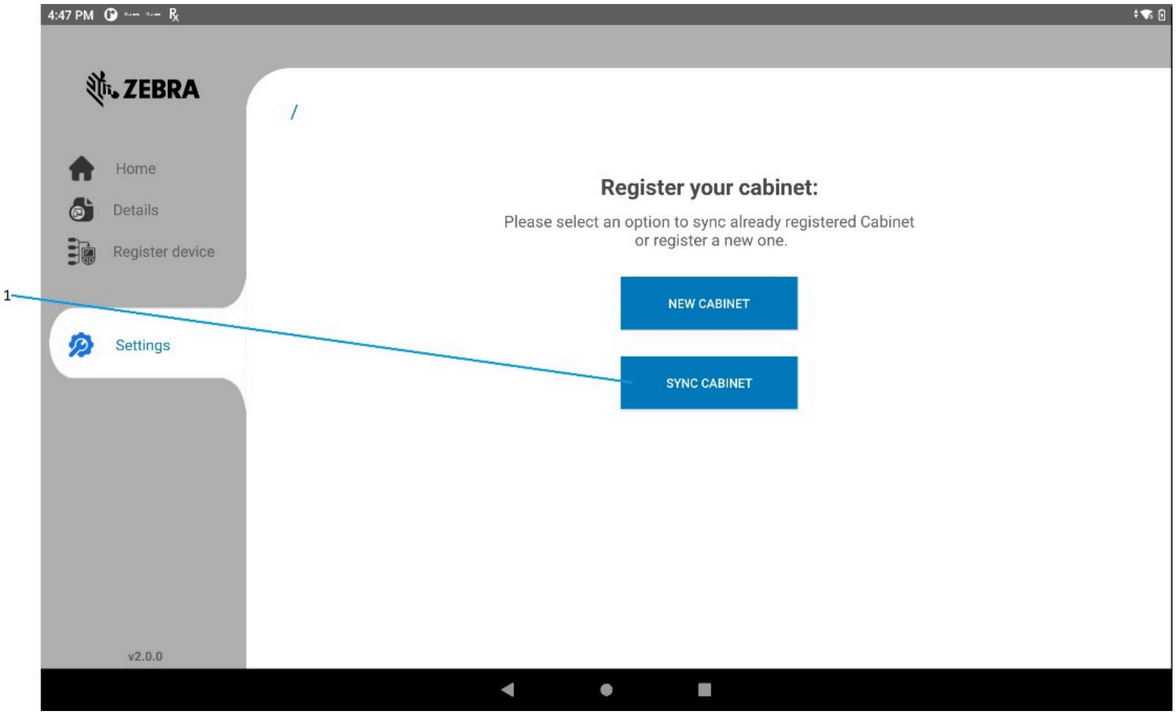
Cabinet synced successfully

Synchronizing a Cabinet on the KIOSK

After ZAMS is installed on the KIOSK, synchronize a Cabinet created previously through the ZAMS user interface.

1. Touch **Settings** on the ZAMS Home screen.

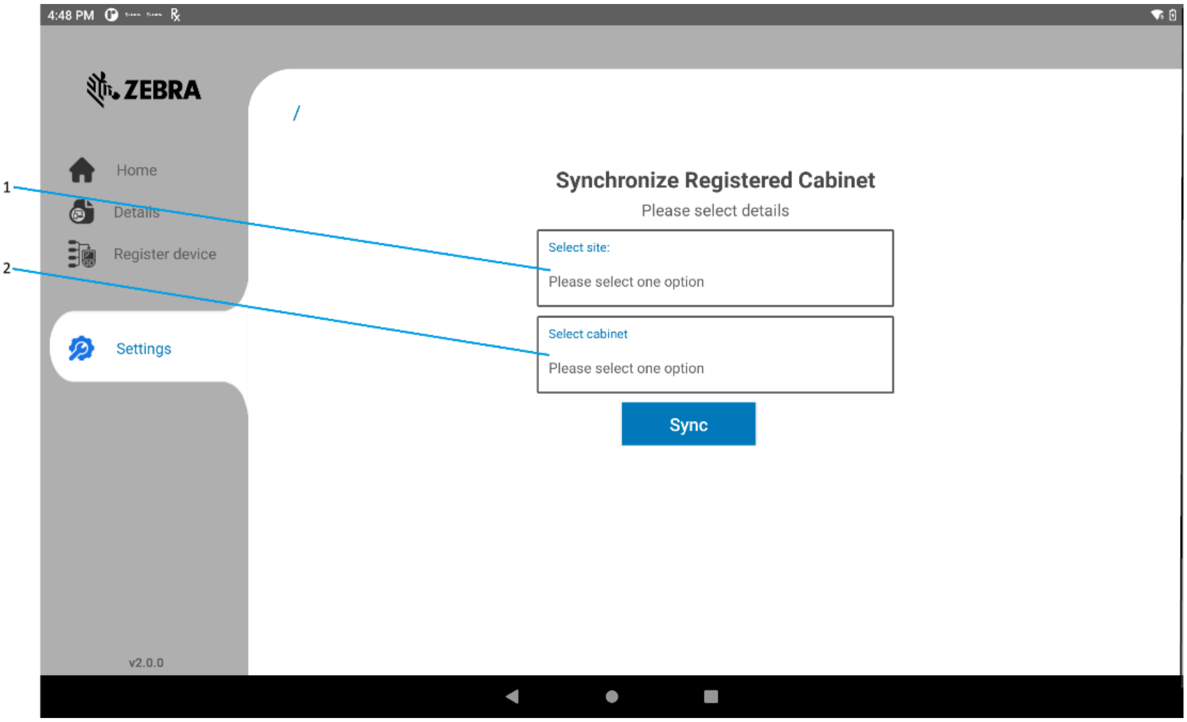
2. To synchronize a registered Cabinet, click **SYNC CABINET** (1).



Register your cabinet:

Please select an option to sync already registered Cabinet or register a new one.

3. Select the appropriate site and Cabinet from the **Select site** (1) and **Select cabinet** (2) drop-down list, and then click **Sync**.



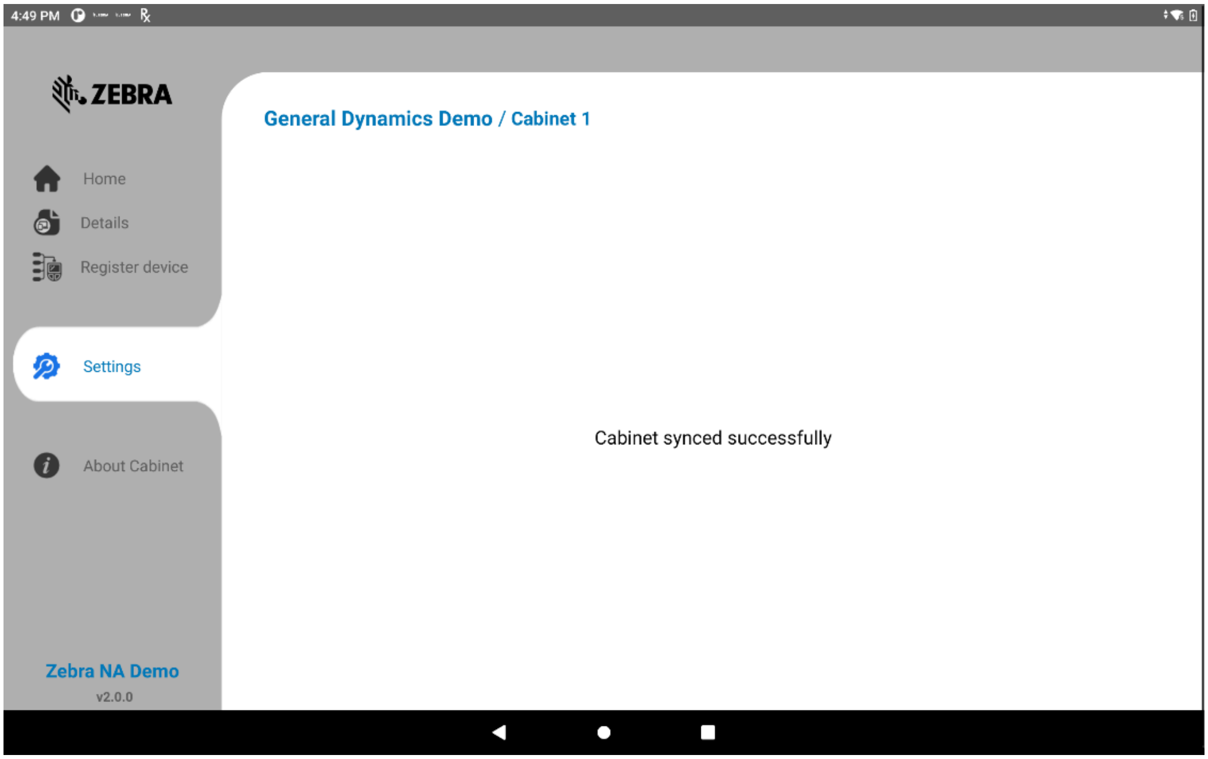
Synchronize Registered Cabinet

Please select details

Select site: Please select one option

Select cabinet Please select one option

The Cabinet is synchronized successfully.



General Dynamics Demo / Cabinet 1

Cabinet synced successfully

Cabinet and Device Configuration Files

The Cabinet and device configuration files can be generated by the Company Admin user. Configuration files are required in the StageNow automated installation with a manual file copy process.

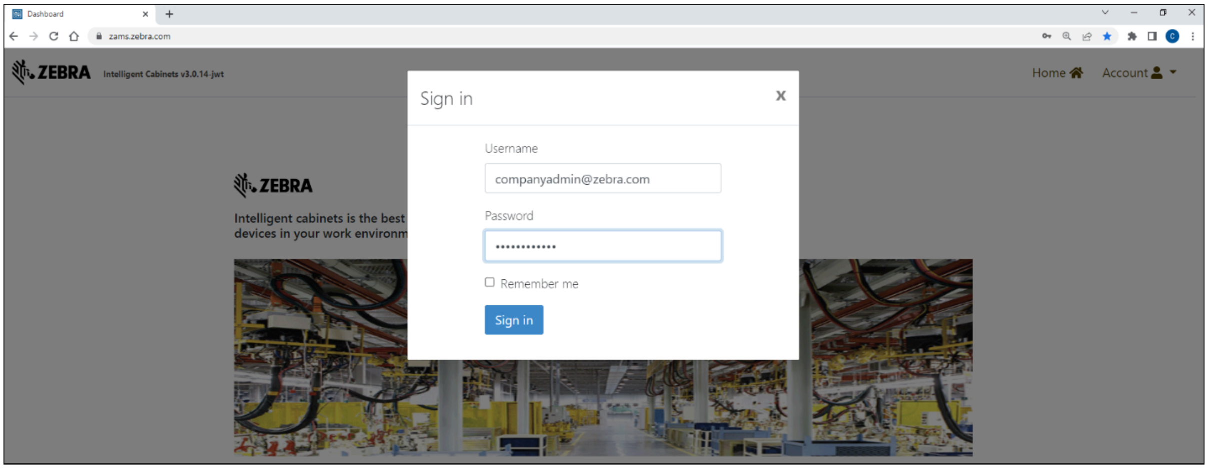
By using the configuration files, when installing a Cabinet, the files automatically create a Cabinet on the KIOSK without having to set up the Cabinet or synchronize a Cabinet using the ZAMS UI on the KIOSK as described in Setting up a Cabinet on the KIOSK on page 21 and Synchronizing a Cabinet on the KIOSK on page 24.

When installing a Cabinet on the mobile device, the configuration file automatically registers the device with the Cabinet without the need to manually link a mobile device with the Cabinet by scanning the QR Code displayed on the **Register device** screen on the KIOSK.

Generating the Cabinet Configuration Files

The Company Admin can generate the Cabinet configuration files at the ZAMS Portal.

1. Log into the ZAMS Portal at zams.zebra.com with the Company Admin credentials.

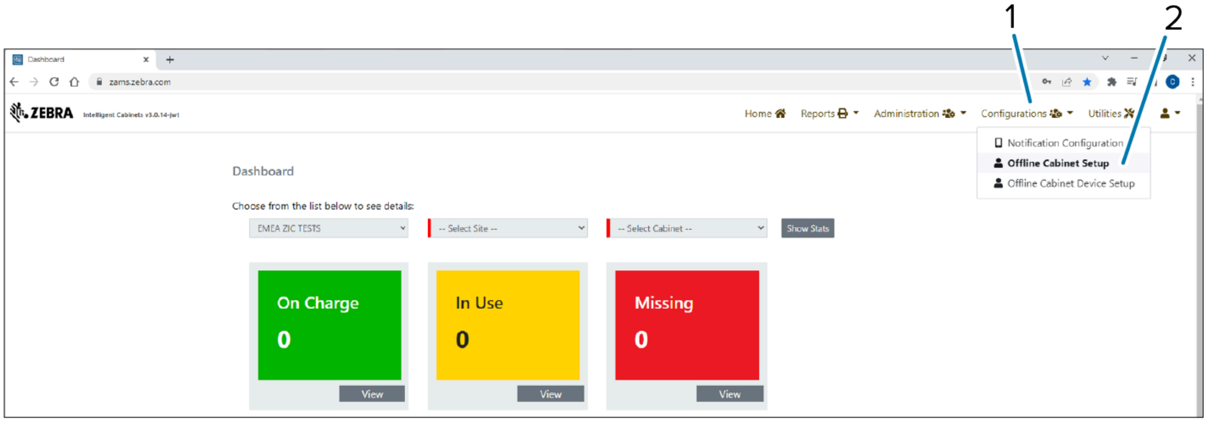

Dashboard
zams.zebra.com
ZEBRA Intelligent Cabinets v3.0.14-jwt
Home
Account
ZEBRA
Intelligent cabinets is the best
devices in your work environm
Sign in
Remember me
Sign in

Sign in

Username: companyadmin@zebra.com

Password: ••••••••••••

2. Select **Configurations** (1) › **Offline Cabinet Setup** (2).



Dashboard

Choose from the list below to see details:

EMEA ZIC TESTS | -- Select Site -- | -- Select Cabinet --

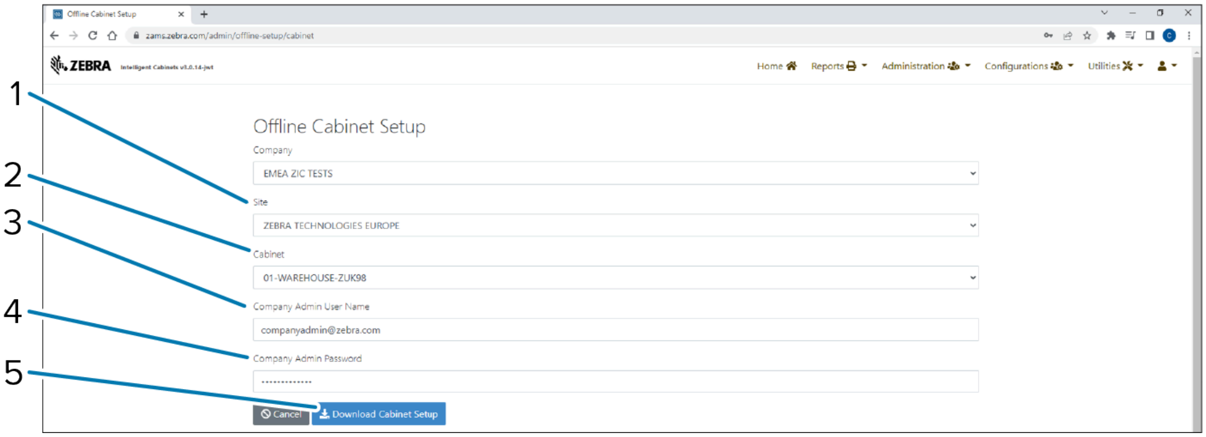
On Charge 0

In Use 0

Missing 0

The **Offline Cabinet Setup** screen displays.

3. To generate the offline Cabinet configuration file, select a site and a Cabinet configured previously in the **Site** (1) and **Cabinet** (2) drop-down list.



Offline Cabinet Setup

Company: EMEA ZIC TESTS

Site: ZEBRA TECHNOLOGIES EUROPE

Cabinet: 01-WAREHOUSE-ZUK98

Company Admin User Name: companyadmin@zebra.com

Company Admin Password: ••••••••••••

4. Enter the Company Admin login credentials in the **Company Admin User Name** (3) and **Company Admin Password** (4) text boxes, and then click **Download Cabinet Setup** (5).

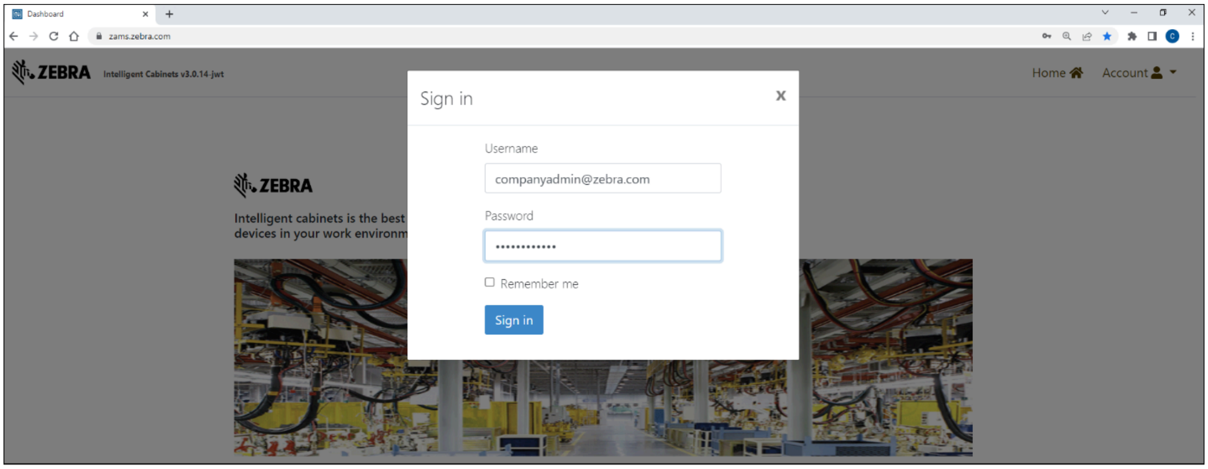
The `cabinet.config` file is downloaded automatically.

Transfer the `cabinet.config` file to the `/sdcard/Download/` folder before installing the application on the KIOSK.

Generating the Device Configuration File

The Company Admin can generate the configuration file of the device at the ZAMS Portal.

1. Log into the ZAMS Portal at zams.zebra.com with the Company Admin credentials.


Dashboard
zams.zebra.com
ZEBRA Intelligent Cabinets v3.0.14-jwt
Home
Account
ZEBRA
Intelligent cabinets is the best
devices in your work environm
x

Sign in

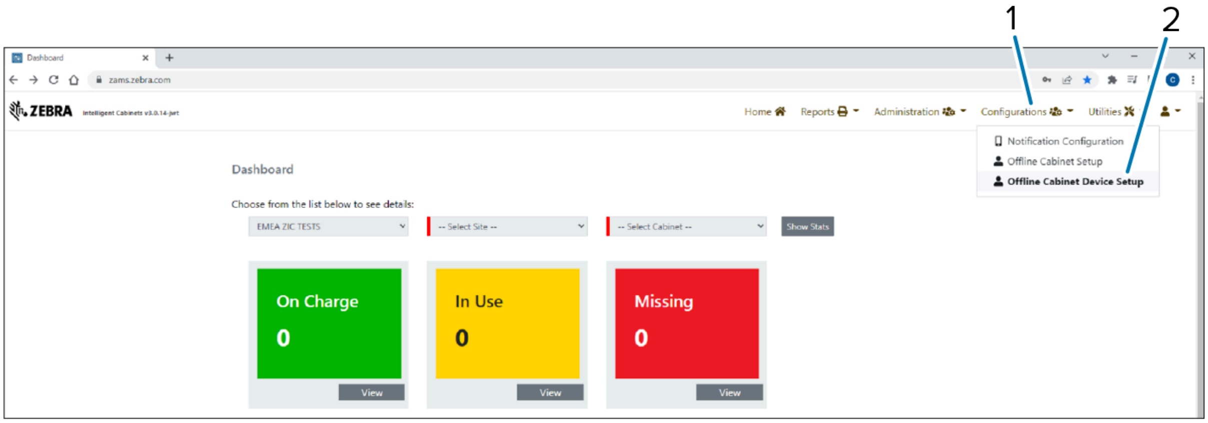
Username: companyadmin@zebra.com

Password: ••••••••••••

☐ Remember me

Sign in

2. Select **Configurations** (1) › **Offline Cabinet Device Setup** (2).



Dashboard

Choose from the list below to see details:

EMEA ZIC TESTS | -- Select Site -- | -- Select Cabinet --

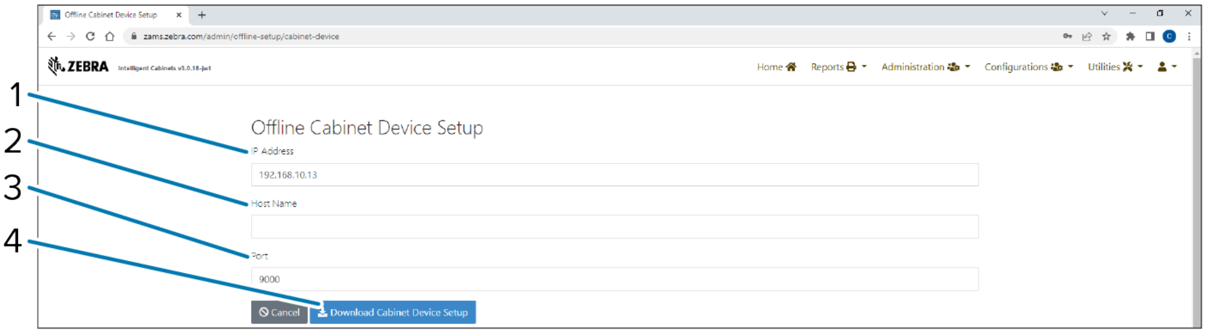
On Charge 0

In Use 0

Missing 0

The **Offline Cabinet Device Setup** screen displays.

3. Enter an IP address and host name in the **IP Address** (1) or **Host Name** (2) text boxes.


1
2
3
4
Offline Cabinet Device Setup
zams.zebra.com/admin/offline-setup/cabinet-device
ZEBRA Intelligent Cabinets v3.0.18-jet
Home
Reports
Administration
Configurations
Utilities
Cancel
Download Cabinet Device Setup

Offline Cabinet Device Setup

IP Address: 192.168.10.13

Host Name:

Port: 9000

4. Enter `9000` in the **Port** (3) field, and then click **Download Cabinet Device Setup** (4).

The `cabinet-device.config` file is downloaded automatically.

Transfer the `cabinet-device.config` file to the `/sdcard/Download/` folder before installing the application on the mobile device.

APK Installation

ZAMS Software contains several components that must be installed on the KIOSK and mobile devices. ZAMS can be installed on both the KIOSK and devices using StageNow with manual file push, StageNow with local server push, and various MDM applications.

Review the Installation Prerequisites before proceeding with the KIOSK and mobile device installations.

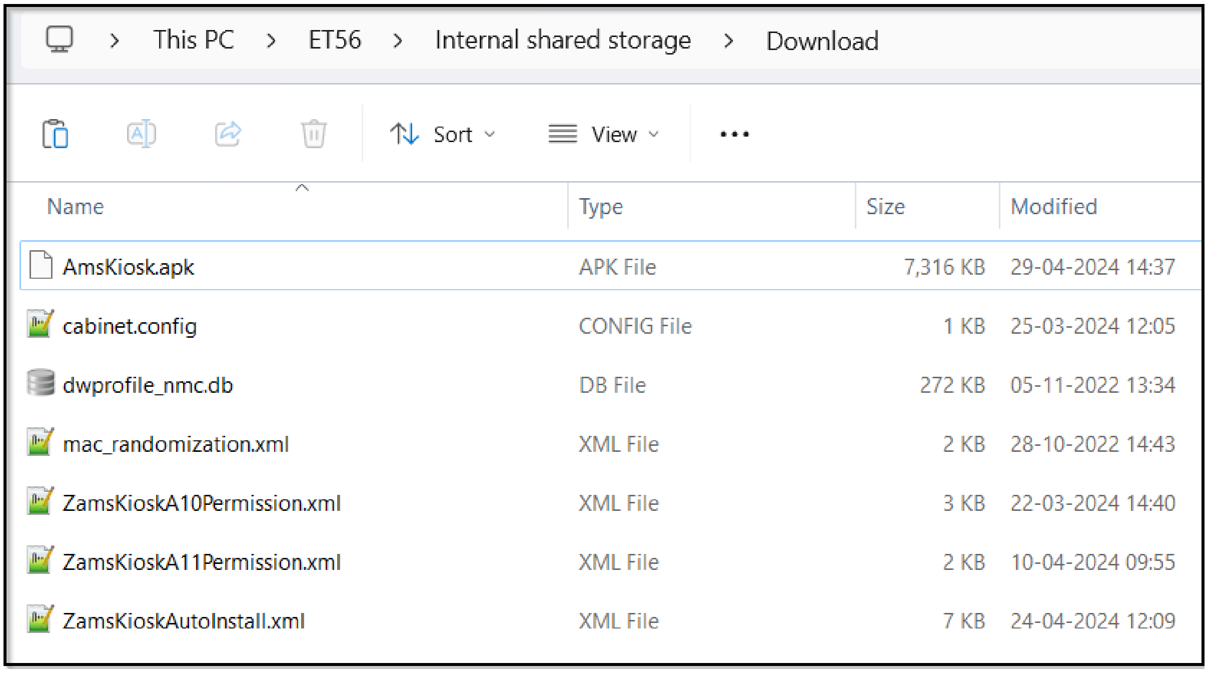
KIOSK Installation

Install ZAMS on the KIOSK by manually copying or transferring files from the local server in StageNow or using an MDM tool. ZAMS supports only SOTI, 42Gears, or AirWatch.

Copying Files Manually in StageNow

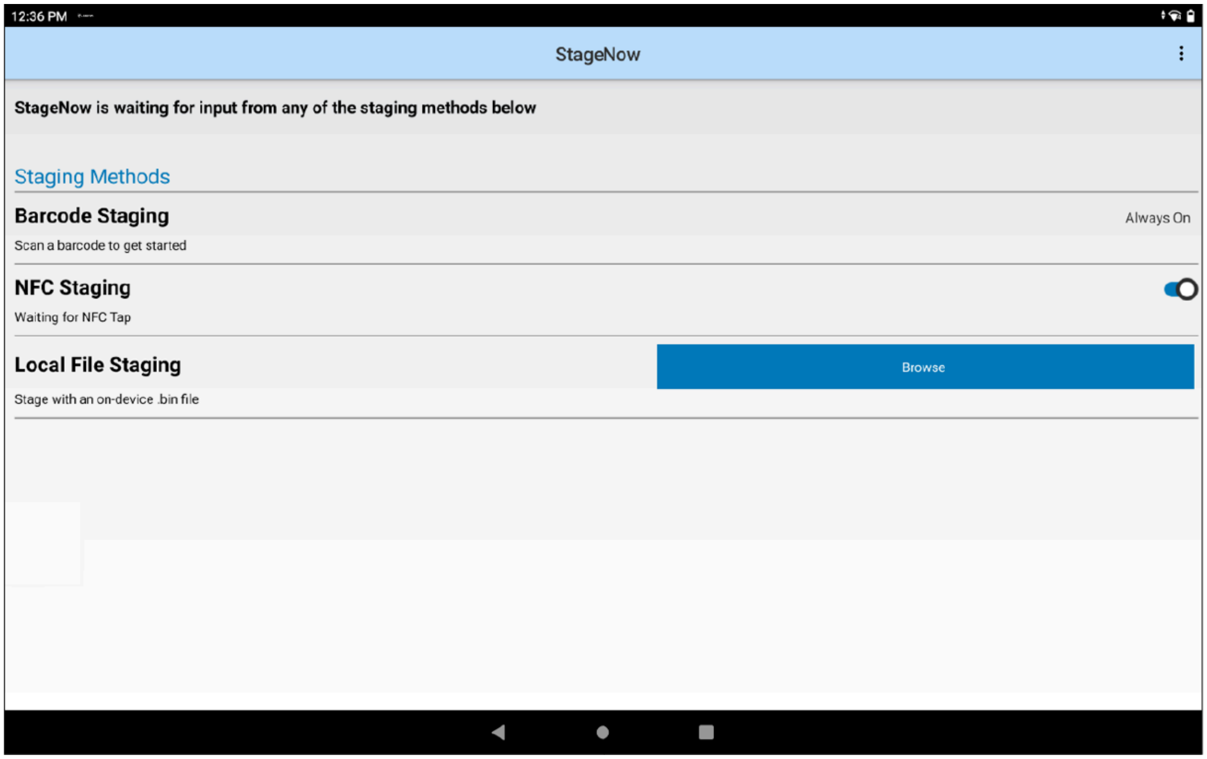
See Installation Prerequisites on page 10 and Cabinet and Device Configuration Files on page 27 to learn how to download the appropriate APK and configuration files from zebra.com/support.

1. Copy the following files into the `/sdcard/Download` folder in the KIOSK:
   - `AmsKiosk.apk`
   - `ZamsKioskAutoInstall.xml`
   - `cabinet.config`
   - `dwprofile_nmc.db`
   - `mac_randomization.xml`
   - `ZamsKioskA10Permission.xml`
   - `ZamsKioskA11Permission.xml`.



Name	Type	Size	Modified
AmsKiosk.apk	APK File	7,316 KB	29-04-2024 14:37
cabinet.config	CONFIG File	1 KB	25-03-2024 12:05
dwprofile_nmc.db	DB File	272 KB	05-11-2022 13:34
mac_randomization.xml	XML File	2 KB	28-10-2022 14:43
ZamsKioskA10Permission.xml	XML File	3 KB	22-03-2024 14:40
ZamsKioskA11Permission.xml	XML File	2 KB	10-04-2024 09:55
ZamsKioskAutoInstall.xml	XML File	7 KB	24-04-2024 12:09

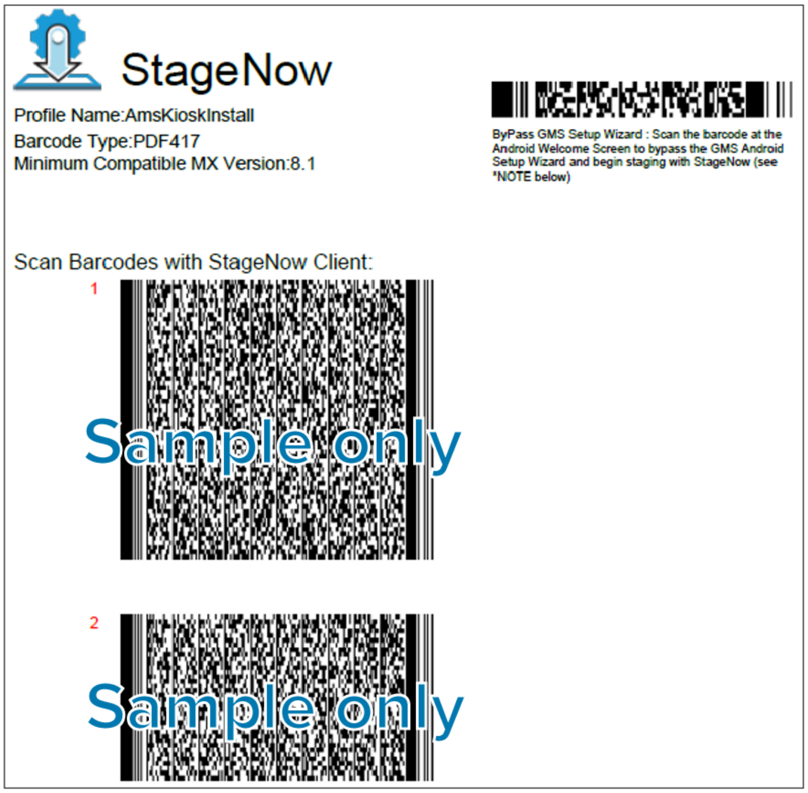
2. Open the **StageNow** application in the KIOSK.



12:36 PM
StageNow
StageNow is waiting for input from any of the staging methods below
Staging Methods
Barcode Staging
Always On
Scan a barcode to get started
NFC Staging
Waiting for NFC Tap
Local File Staging
Browse
Stage with an on-device .bin file

3. For a KIOSK:
   - With an Android 13 operating system, open the **A13_ZamsKioskAutoInstall** PDF file from the extracted zipped file.
   - With an operating system below Android 13, open the **ZamsKioskAutoInstall** PDF file from the extracted zipped file.

4. Scan the barcodes in this PDF file using the StageNow application to automatically install and configure the ZAMS application on the KIOSK.



StageNow

Profile Name:AmsKioskInstall

Barcode Type:PDF417

Minimum Compatible MX Version:8.1

ByPass GMS Setup Wizard : Scan the barcode at the Android Welcome Screen to bypass the GMS Android Setup Wizard and begin staging with StageNow (see *NOTE below)

Scan Barcodes with StageNow Client:

1
Sample only
2
Sample only

ZAMS is now installed in the KIOSK.

NOTE: See step 5 in Downloading the Latest ZAMS Software on page 10 to locate the PDF file.

Loading Files from Local Server in StageNow

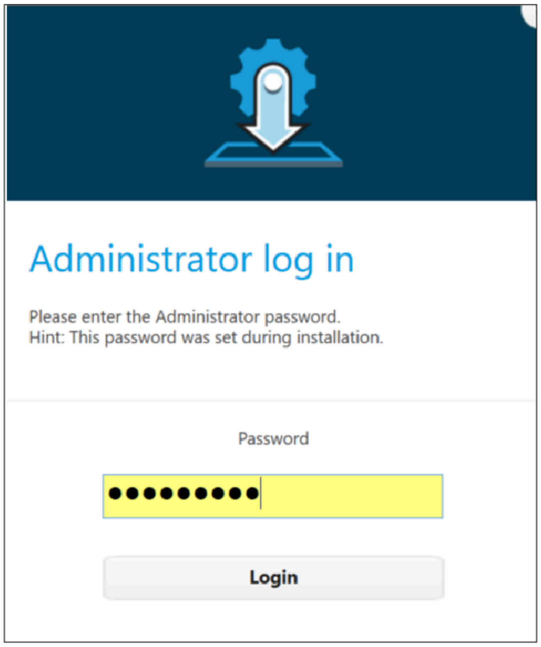
This method uses the StageNow administrator tool to import a StageNow profile to a host computer. The StageNow profile then uses the local File Transfer Protocol (FTP) storage to store the files required for the installation. Upon scanning the StageNow barcodes, the files are automatically loaded and installed on that KIOSK.

NOTE: The computer hosting the StageNow local FTP storage and the KIOSK must be connected to the same local area network (LAN).

1. After extracting the zipped file, navigate to the **Admin** and locate the **StageNow Profile** for ZAMS KIOSK installation named, `Local_Server_ZamsKioskInstall.zip`.

2. Open StageNow on the host computer, and then select **Administrator Login**.

3. Log into StageNow using an Administrator password.



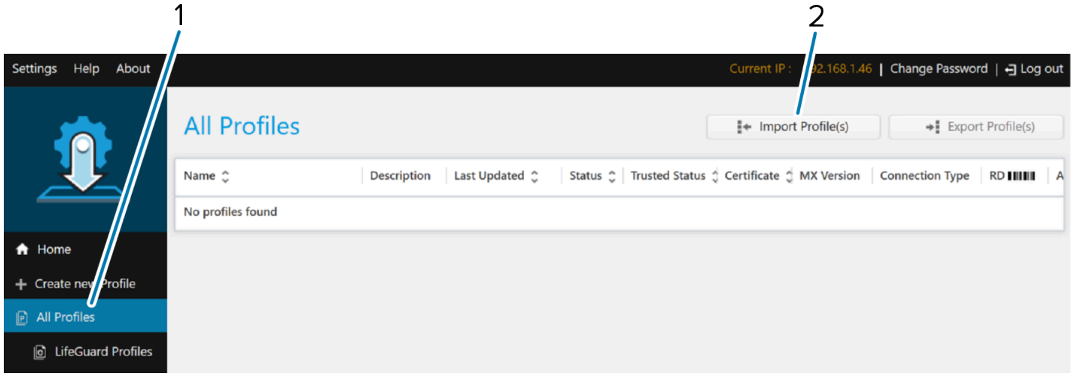
Administrator log in

Please enter the Administrator password.
Hint: This password was set during installation.

Password

●●●●●●●●●

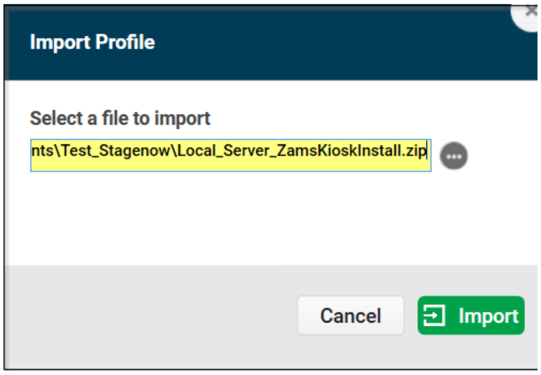
4. Select **All Profiles (1)** , and then click **Import Profile(s) (2)**.



All Profiles

Name	Description	Last Updated	Status	Trusted Status	Certificate	MX Version	Connection Type	RD	A
No profiles found									

5. Select the file location that has the zipped file, and then click **Import**.

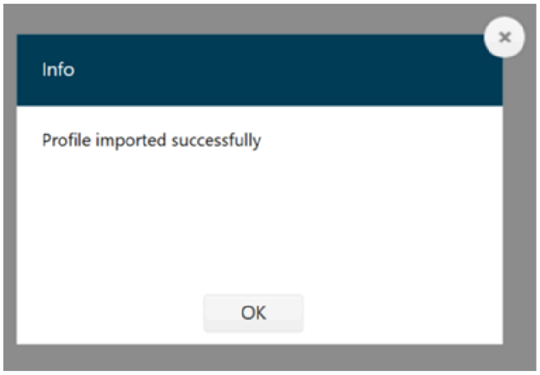


Import Profile

Select a file to import

nts\Test_Stagenow\Local_Server_ZamsKioskInstall.zip

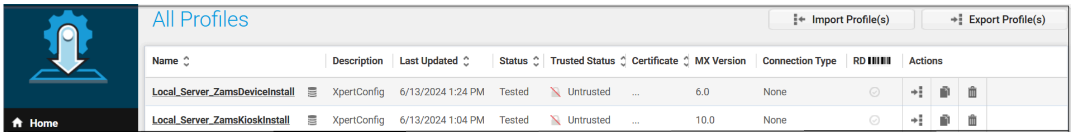
The window displays a **Profile imported successfully** message.



Info

Profile imported successfully

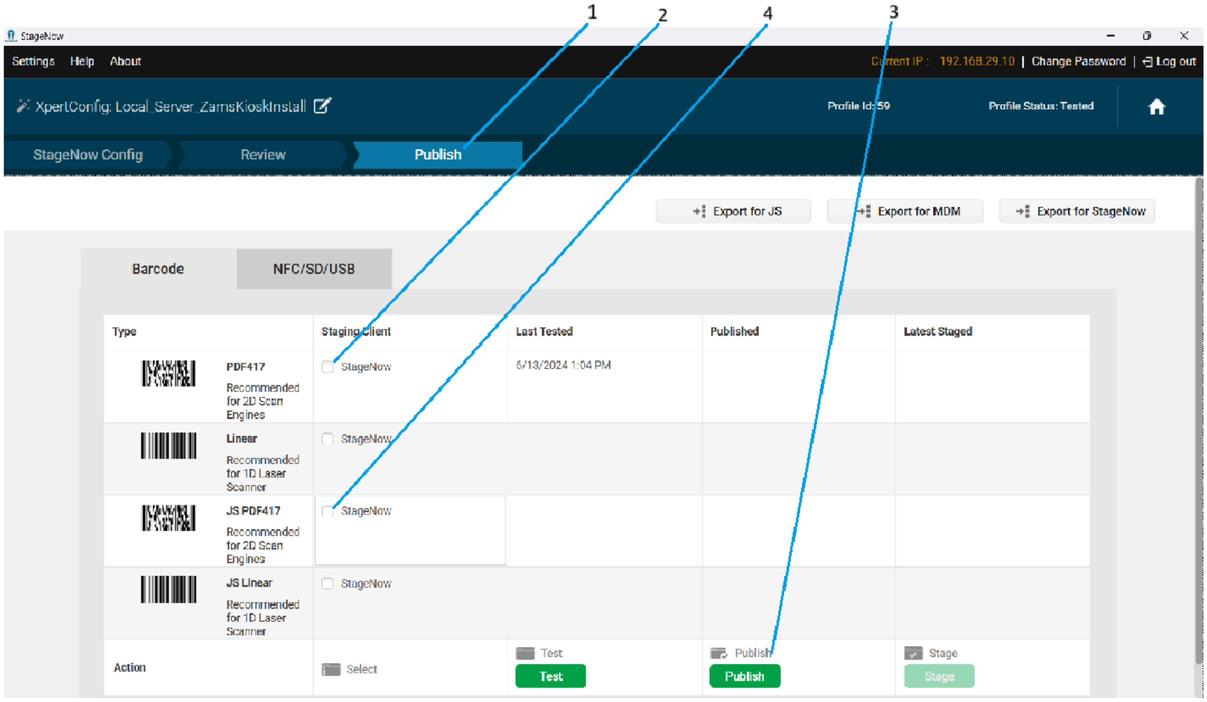
6. On the **All Profiles** screen, select the **Local_Server_ZamsKioskInstall** profile.



All Profiles

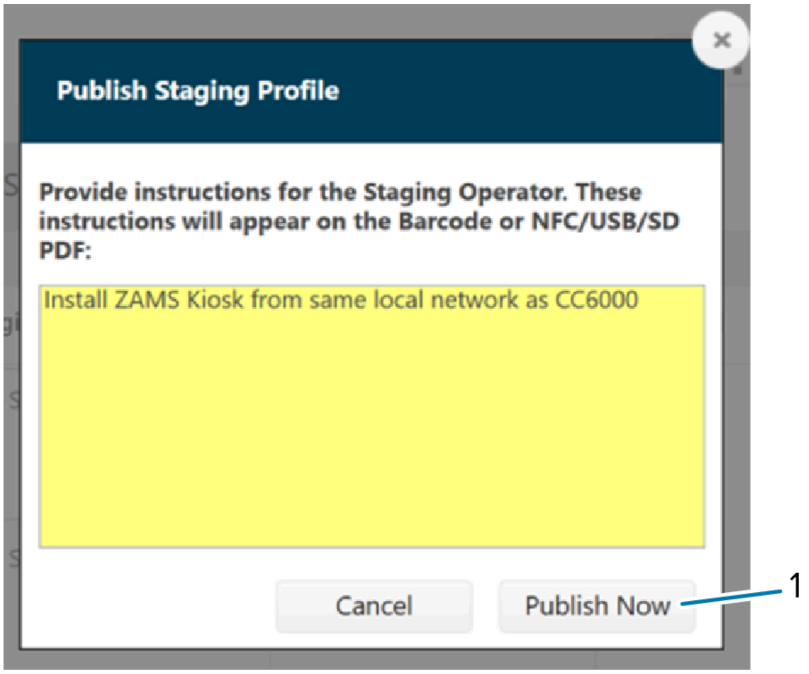
Name	Description	Last Updated	Status	Trusted Status	Certificate	MX Version	Connection Type	RD	Actions
Local_Server_ZamsDeviceInstall	XpertConfig	6/13/2024 1:24 PM	Tested	Untrusted	...	6.0	None		
Local_Server_ZamsKioskInstall	XpertConfig	6/13/2024 1:04 PM	Tested	Untrusted	...	10.0	None		

7. For a KIOSK:
   - Below Android 13, select **Publish (1)** > **Staging Client (2)** > **Publish (3)**.
   - On Android 13, select **Publish (1)** > **Staging Client (4)** > **Publish (3)**.



Type		Staging Client	Last Tested	Published	Latest Staged
	PDF417 Recommended for 2D Scan Engines	☐ StageNow	6/13/2024 1:04 PM		
	Linear Recommended for 1D Laser Scanner	☐ StageNow			
	JS PDF417 Recommended for 2D Scan Engines	☐ StageNow			
	JS Linear Recommended for 1D Laser Scanner	☐ StageNow			
Action		Select	Test Test	Publish Publish	Stage Stage

8. Add a custom instruction, and then click **Publish Now (1)**.

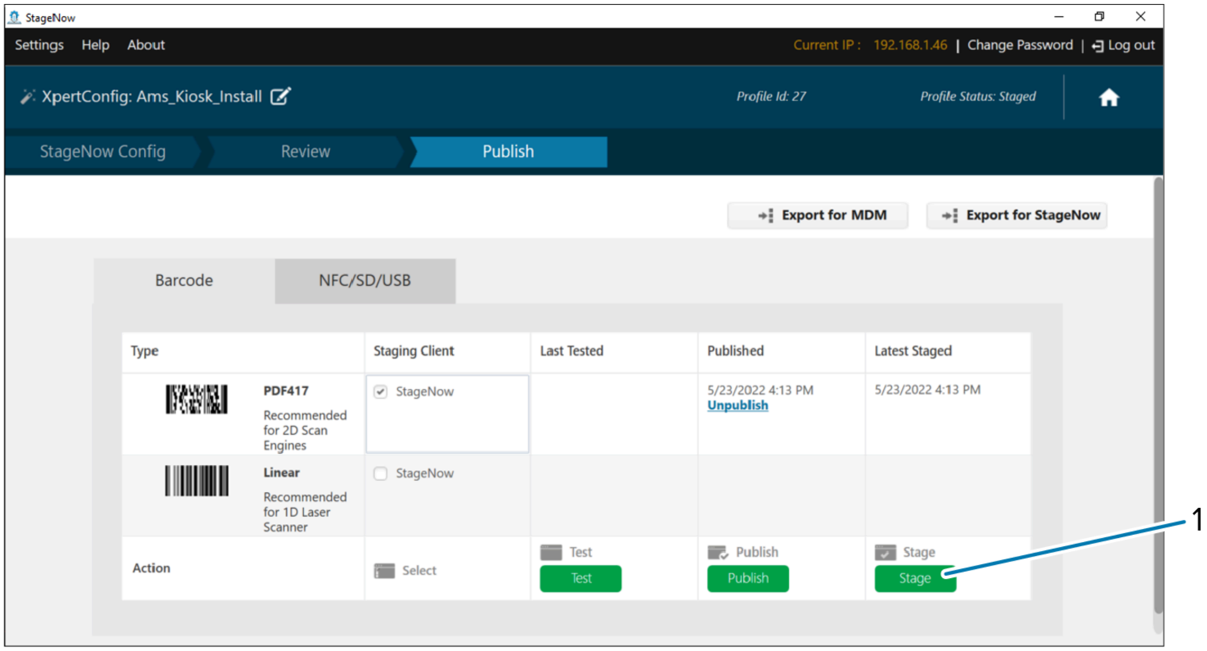


Publish Staging Profile

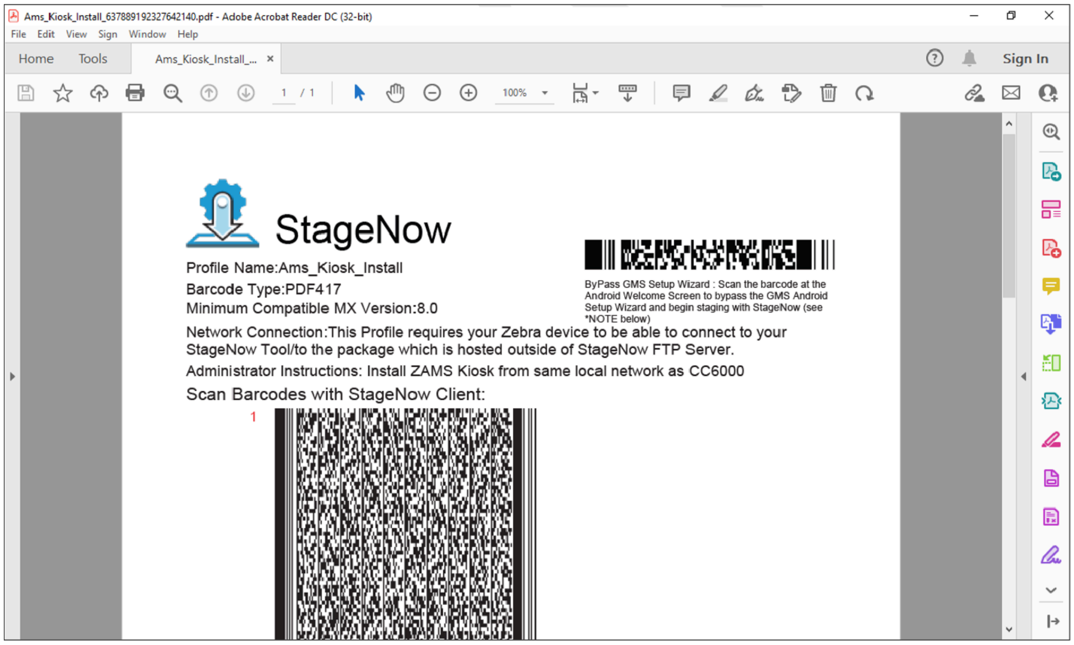
Provide instructions for the Staging Operator. These instructions will appear on the Barcode or NFC/USB/SD PDF:

Install ZAMS Kiosk from same local network as CC6000

9. Click **Stage (1)** to generate a PDF with barcodes.



Type		Staging Client	Last Tested	Published	Latest Staged
	PDF417 Recommended for 2D Scan Engines	☑ StageNow		5/23/2022 4:13 PM Unpublish	5/23/2022 4:13 PM
	Linear Recommended for 1D Laser Scanner	☐ StageNow			
Action		Select	Test Test	Publish Publish	Stage Stage



Profile Name:Ams_Kiosk_Install
Barcode Type:PDF417
Minimum Compatible MX Version:8.0

ByPass GMS Setup Wizard : Scan the barcode at the Android Welcome Screen to bypass the GMS Android Setup Wizard and begin staging with StageNow (see *NOTE below)

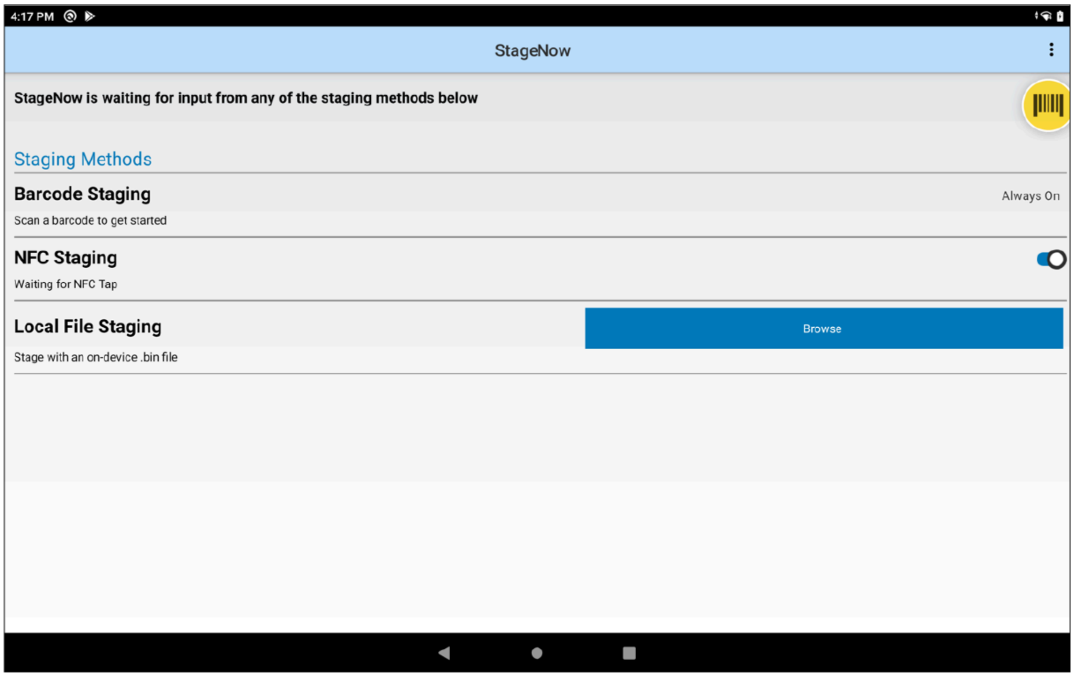
Network Connection:This Profile requires your Zebra device to be able to connect to your StageNow Tool/to the package which is hosted outside of StageNow FTP Server.

Administrator Instructions: Install ZAMS Kiosk from same local network as CC6000

Scan Barcodes with StageNow Client:

The barcodes are generated.

10. Open the StageNow application on the KIOSK, and then scan the barcodes generated in step 9 to automatically install the ZAMS software into the KIOSK.



StageNow is waiting for input from any of the staging methods below

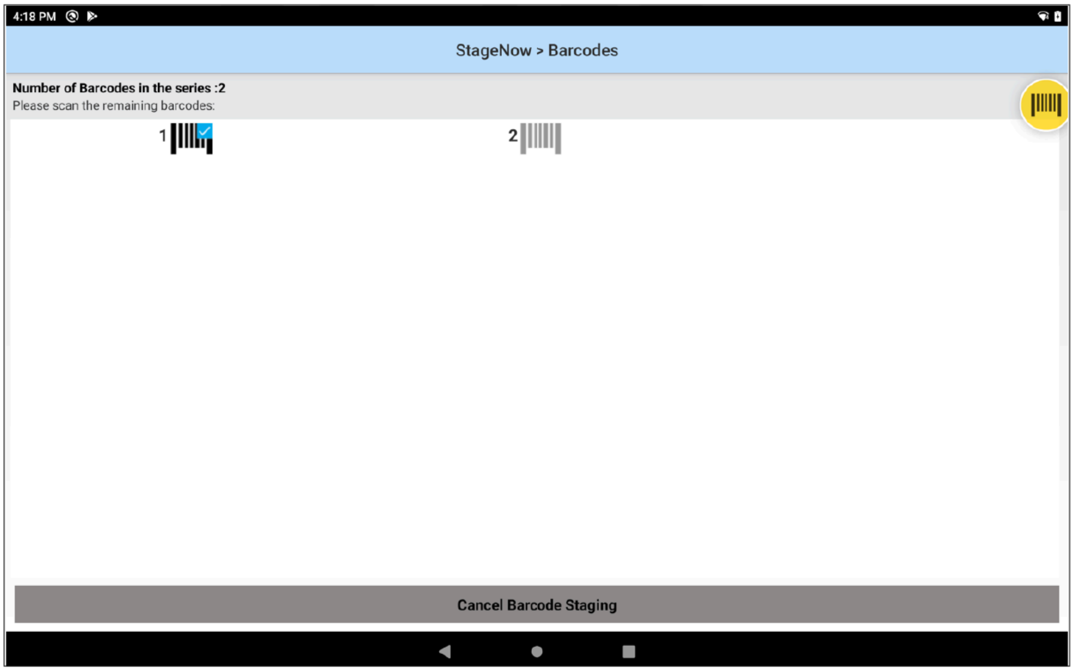
Staging Methods

Barcode Staging — Always On
Scan a barcode to get started

NFC Staging
Waiting for NFC Tap

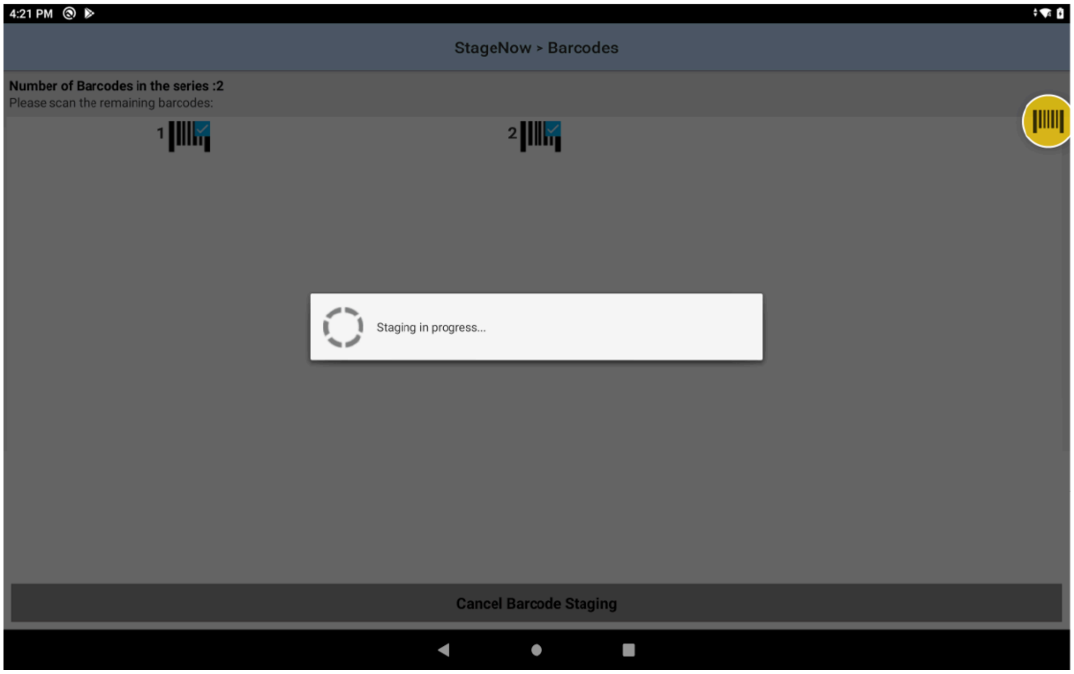
Local File Staging
Stage with an on-device .bin file

11. Follow the steps on the screen to scan the remaining barcodes.



StageNow > Barcodes

Number of Barcodes in the series :2
Please scan the remaining barcodes:



StageNow > Barcodes

Number of Barcodes in the series :2
Please scan the remaining barcodes:

Staging in progress...

ZAMS is installed on the KIOSK.

Device Installation

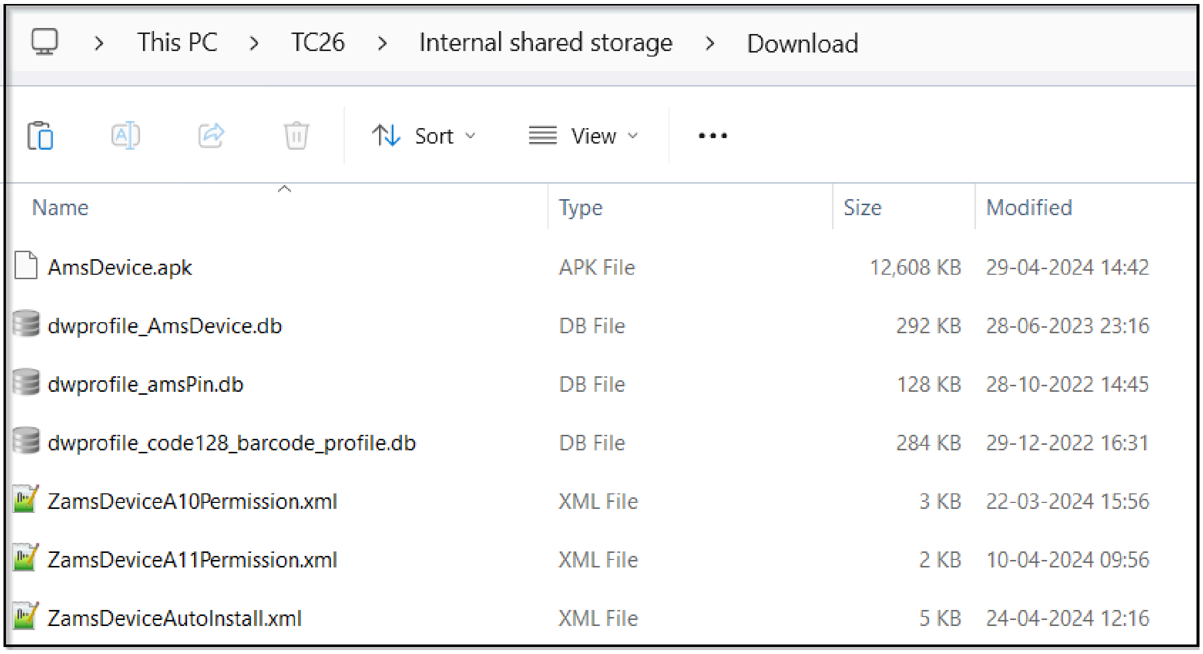
Install ZAMS on the mobile device by manually copying or transferring files from the local server in StageNow or using an MDM tool. ZAMS supports only SOTI, 42Gears, or AirWatch.

Copying Files Manually in StageNow

This method requires you to manually copy the required ZAMS files in the device folder of the extracted ZIP file to the internal storage of the mobile device and then use the StageNow application on the mobile device to complete the installation.

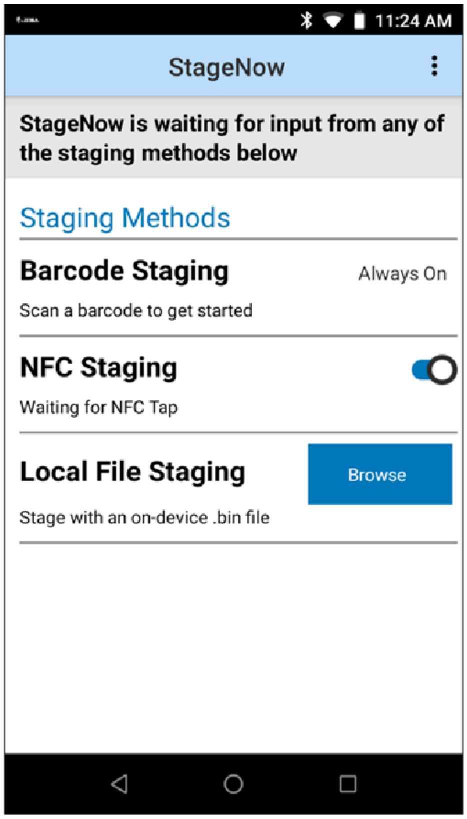
See Installation Prerequisites on page 10 and Cabinet and Device Configuration Files on page 27 to learn how to download the appropriate APK and configuration files from zebra.com/support.

1. Copy the following files into the `/sdcard/Download` folder in the mobile device:
   - `AmsDevice.apk`
   - `Cabinet-device.config`
   - `device.config.json`
   - `dwprofile_AmsDevice.db`
   - `dwprofile_amsPin.db`
   - `dwprofile_code128_barcode_profile.db`.
   - `ZamsDeviceA10Permission.xml`
   - `ZamsDeviceA11Permission.xml`
   - `ZamsDeviceAutoInstall.xml`



Name	Type	Size	Modified
AmsDevice.apk	APK File	12,608 KB	29-04-2024 14:42
dwprofile_AmsDevice.db	DB File	292 KB	28-06-2023 23:16
dwprofile_amsPin.db	DB File	128 KB	28-10-2022 14:45
dwprofile_code128_barcode_profile.db	DB File	284 KB	29-12-2022 16:31
ZamsDeviceA10Permission.xml	XML File	3 KB	22-03-2024 15:56
ZamsDeviceA11Permission.xml	XML File	2 KB	10-04-2024 09:56
ZamsDeviceAutoInstall.xml	XML File	5 KB	24-04-2024 12:16

2. Open the **StageNow** application on the mobile device.



11:24 AM

StageNow

StageNow is waiting for input from any of the staging methods below

Staging Methods

Barcode Staging — Always On

Scan a barcode to get started

NFC Staging

Waiting for NFC Tap

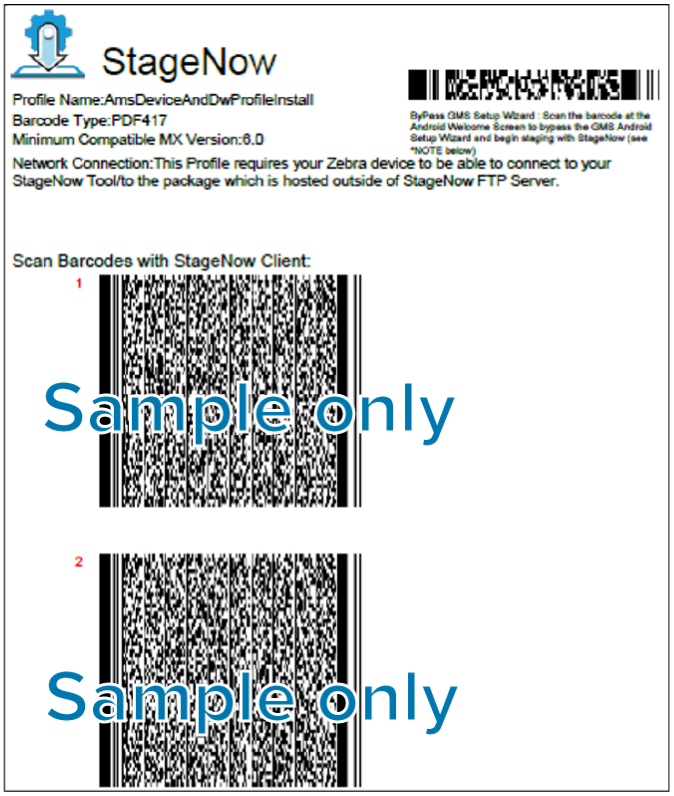
Local File Staging

Stage with an on-device .bin file

3. For a KIOSK:

    - With an Android 13 operating system, open the **A13_ ZamsDeviceAutoInstall** PDF file from the extracted zipped file.
    - With an operating system below Android 13, open the **ZamsDeviceAutoInstall** PDF file from the extracted zipped file.

4. Scan the barcodes in this PDF file using the StageNow application to automatically install and configure the ZAMS application on the KIOSK.



StageNow

Profile Name:AmsDeviceAndDwProfileInstall
Barcode Type:PDF417
Minimum Compatible MX Version:6.0

ByPass GMS Setup Wizard : Scan the barcode at the Android Welcome Screen to bypass the GMS Android Setup Wizard and begin staging with StageNow (see *NOTE below)

Network Connection:This Profile requires your Zebra device to be able to connect to your StageNow Tool/to the package which is hosted outside of StageNow FTP Server.

Scan Barcodes with StageNow Client:

ZAMS is now installed on the mobile device.

NOTE: See step 5 in Downloading the Latest ZAMS Software on page 10 to locate the PDF file.

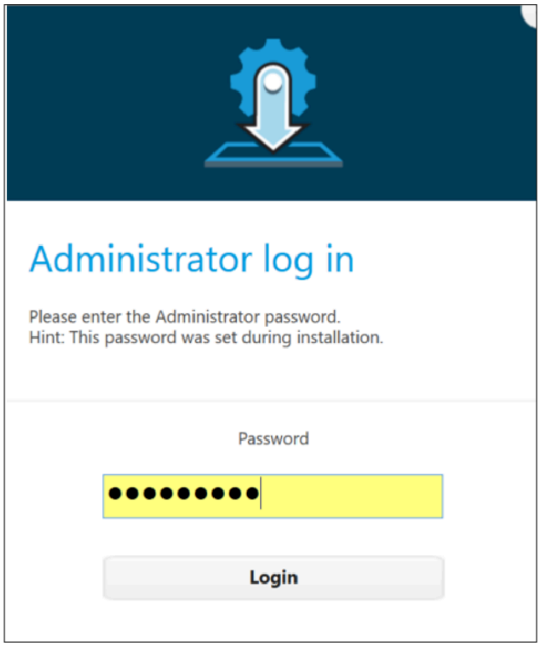
Loading Files from the Local Server in StageNow

This method uses the StageNow administrator tool to import a StageNow profile to a host computer. The StageNow profile then uses the local FTP storage to store the files required for the installation. Upon scanning the StageNow barcodes, the files are automatically loaded and installed on that mobile device.

NOTE: The computer hosting the StageNow local FTP storage and the mobile device must be connected to the same local area network (LAN).

1. After extracting the zipped file, navigate to the **Admin** and locate the **StageNow Profile** for ZAMS Device installation named, **`Local_Server_ZamsDeviceInstall.zip`**.
2. Open StageNow on the host computer, and then select **Administrator Login**.

3. Log into StageNow using an Administrator password.



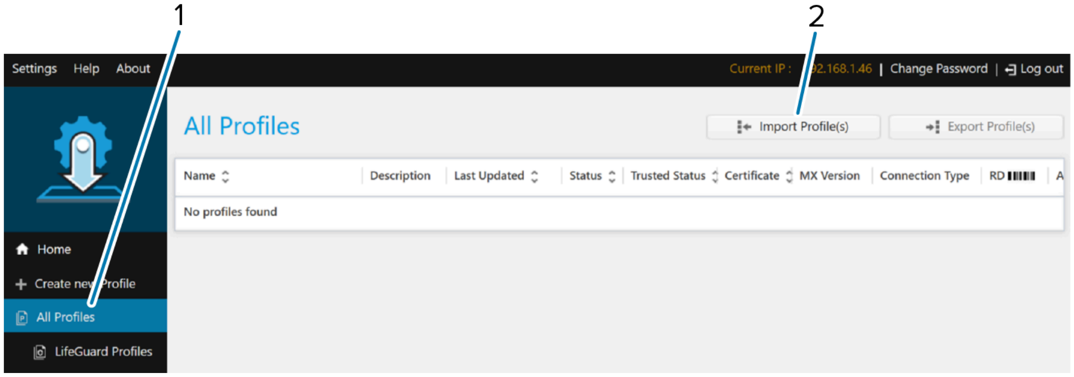
Administrator log in

Please enter the Administrator password.
Hint: This password was set during installation.

Password

●●●●●●●●●

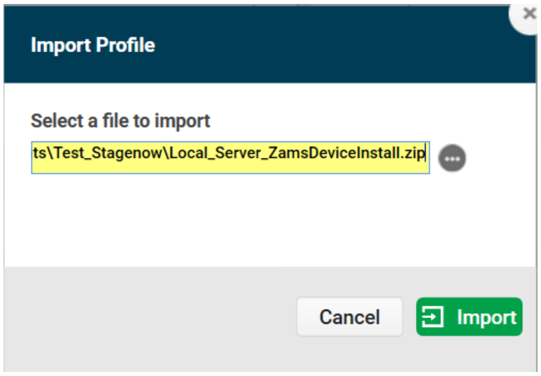
4. Select **All Profiles (1)**, and then click **Import Profile(s) (2)**.



All Profiles

Name	Description	Last Updated	Status	Trusted Status	Certificate	MX Version	Connection Type	RD	A
No profiles found									

5. Select the file location that has the zipped file, and then click **Import**.

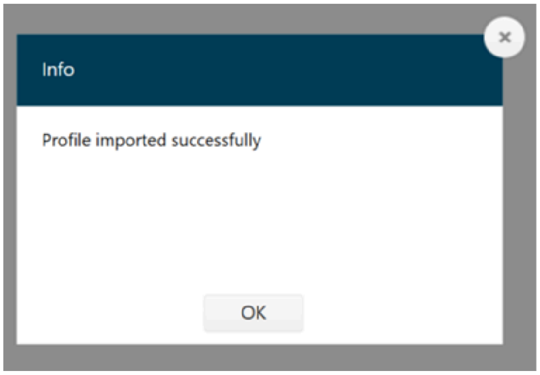


Import Profile

Select a file to import

ts\Test_Stagenow\Local_Server_ZamsDeviceInstall.zip

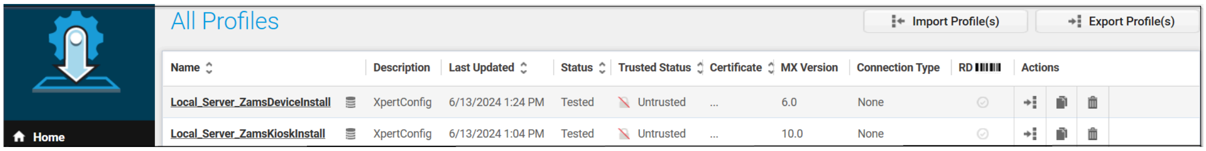
The window displays a **Profile imported successfully** message.



Info

Profile imported successfully

6. On the **All Profiles** screen, select the **Local_Server_ZamsDeviceInstall** profile.

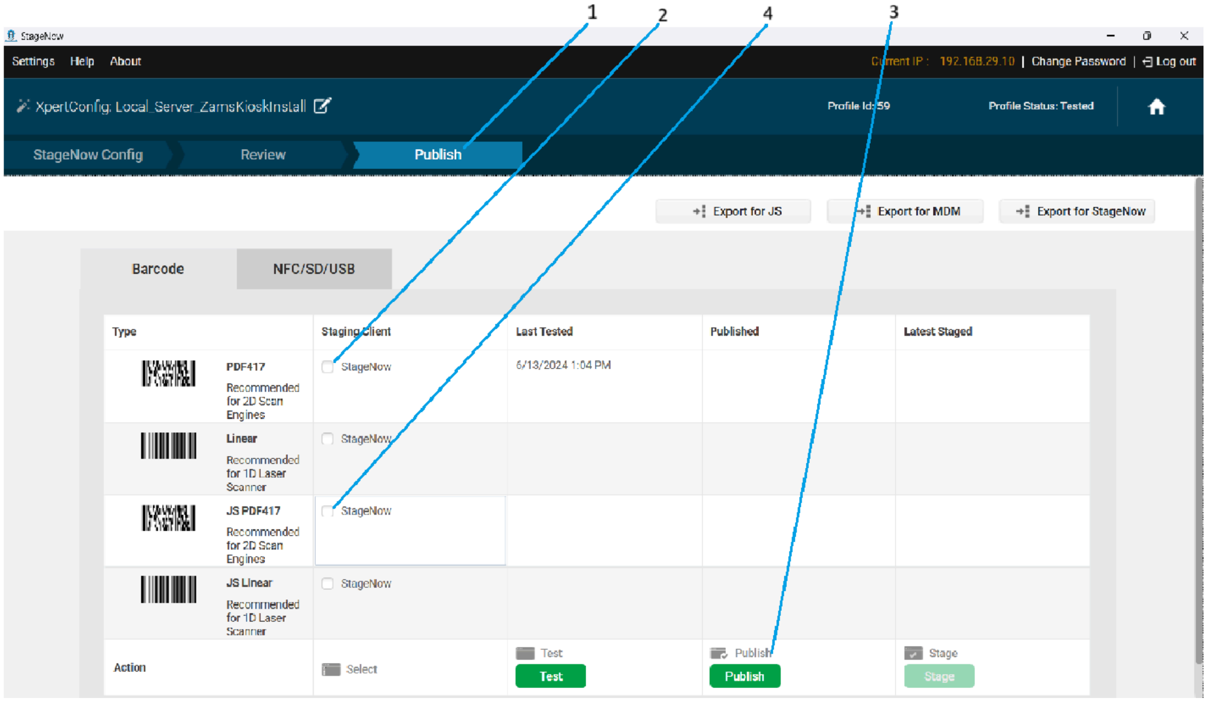


All Profiles

Name		Description	Last Updated	Status	Trusted Status	Certificate	MX Version	Connection Type	RD	Actions
Local_Server_ZamsDeviceInstall		XpertConfig	6/13/2024 1:24 PM	Tested	Untrusted	...	6.0	None		
Local_Server_ZamsKioskInstall		XpertConfig	6/13/2024 1:04 PM	Tested	Untrusted	...	10.0	None		

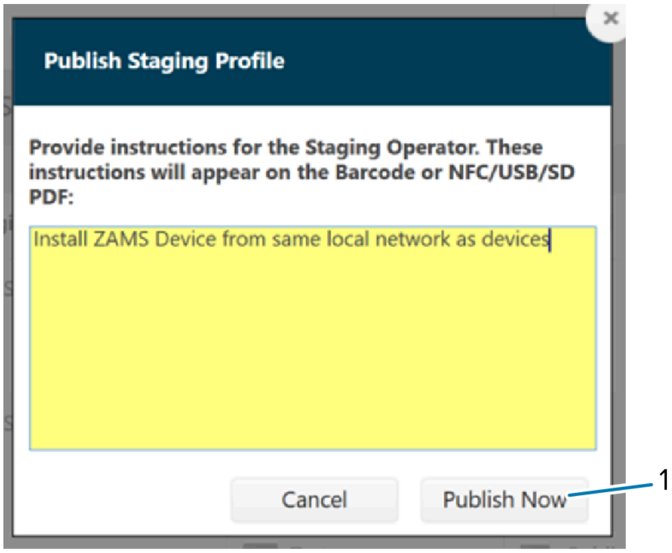
7. For a KIOSK:

   - Below Android 13, select **Publish (1)** > **Staging Client (2)** > **Publish (3)**.
   - On Android 13, select **Publish (1)** > **Staging Client (4)** > **Publish (3)**.



Type		Staging Client	Last Tested	Published	Latest Staged
	PDF417 Recommended for 2D Scan Engines	□ StageNow	6/13/2024 1:04 PM		
	Linear Recommended for 1D Laser Scanner	□ StageNow			
	JS PDF417 Recommended for 2D Scan Engines	□ StageNow			
	JS Linear Recommended for 1D Laser Scanner	□ StageNow			
Action		Select	Test Test	Publish Publish	Stage Stage

8. Add a custom instruction, and then click **Publish Now (1)**.

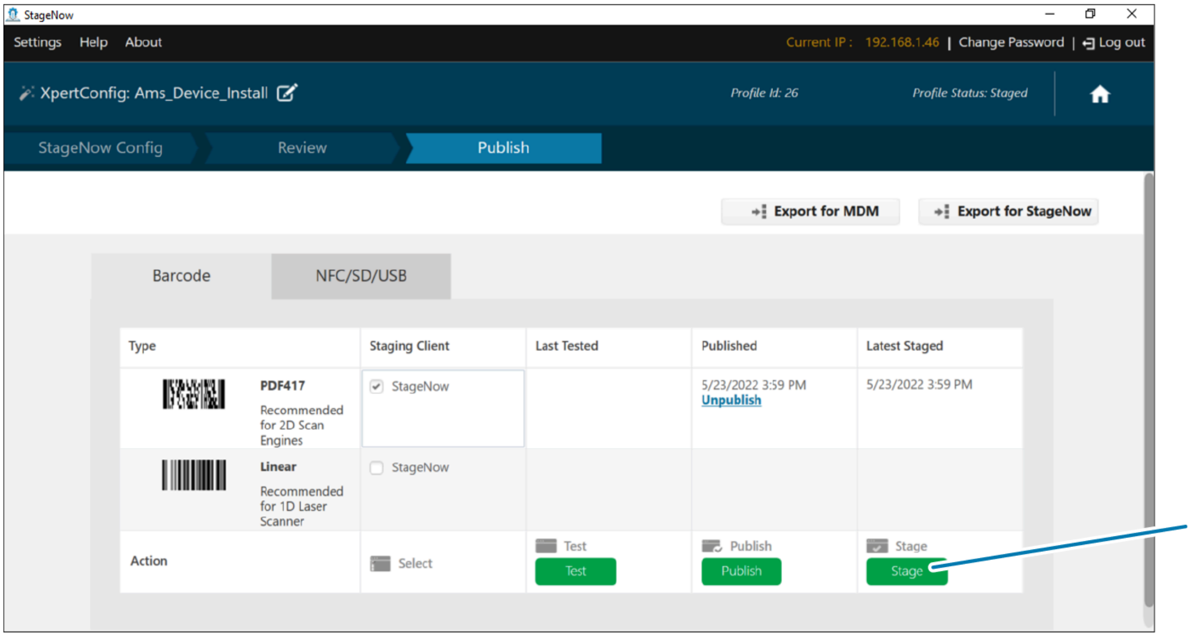


Publish Staging Profile

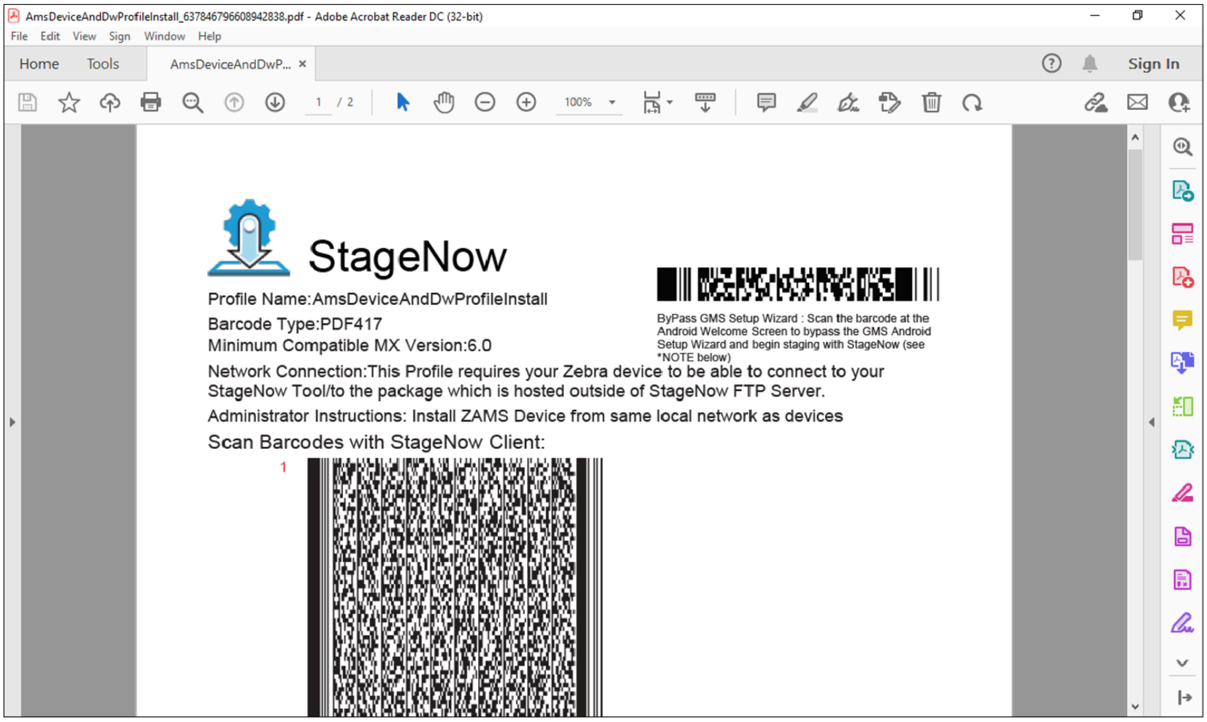
Provide instructions for the Staging Operator. These instructions will appear on the Barcode or NFC/USB/SD PDF:

Install ZAMS Device from same local network as devices

9. Click **Stage (1)** to generate a PDF with barcodes.



Type		Staging Client	Last Tested	Published	Latest Staged
	PDF417 Recommended for 2D Scan Engines	☑ StageNow		5/23/2022 3:59 PM Unpublish	5/23/2022 3:59 PM
	Linear Recommended for 1D Laser Scanner	□ StageNow			
Action		Select	Test Test	Publish Publish	Stage Stage


AmsDeviceAndDwProfileInstall_637846796608942838.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools AmsDeviceAndDwP... ×
Sign In
1 / 2
100%
StageNow
1

Profile Name:AmsDeviceAndDwProfileInstall

Barcode Type:PDF417

Minimum Compatible MX Version:6.0

Network Connection:This Profile requires your Zebra device to be able to connect to your StageNow Tool/to the package which is hosted outside of StageNow FTP Server.

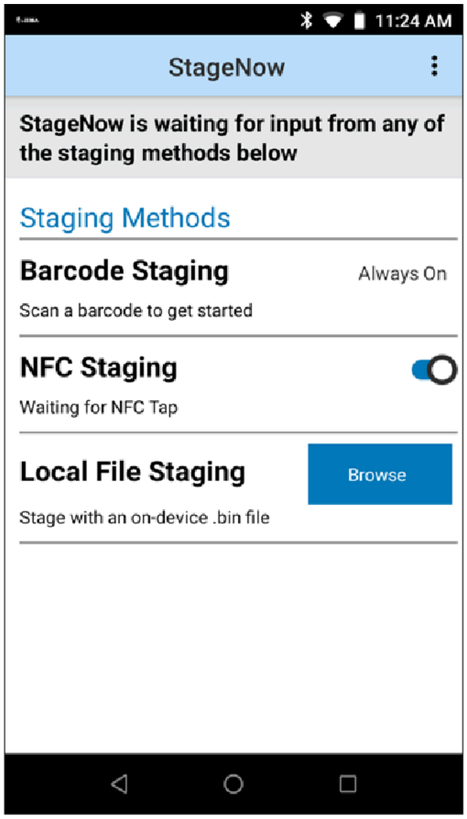
Administrator Instructions: Install ZAMS Device from same local network as devices

Scan Barcodes with StageNow Client:

ByPass GMS Setup Wizard : Scan the barcode at the Android Welcome Screen to bypass the GMS Android Setup Wizard and begin staging with StageNow (see *NOTE below)

The barcodes are generated.

10. Open the StageNow application on the mobile device, and then scan the barcodes generated in step 9 to automatically install the ZAMS software into the mobile device.



11:24 AM

StageNow

StageNow is waiting for input from any of the staging methods below

Staging Methods

Barcode Staging — Always On

Scan a barcode to get started

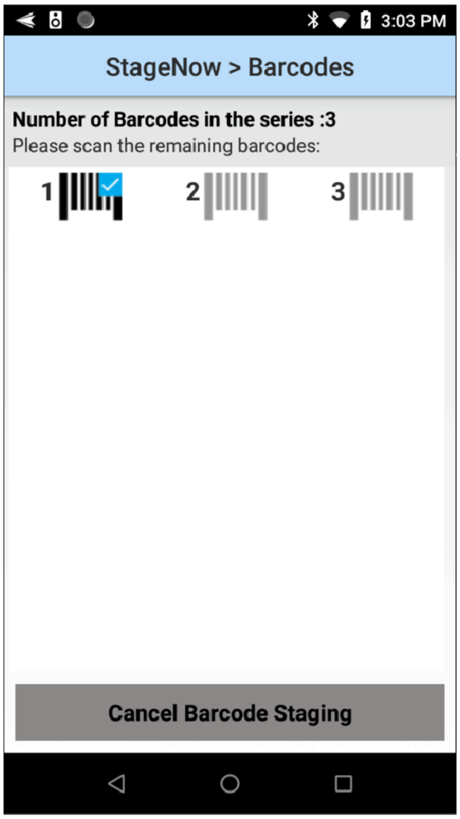
NFC Staging

Waiting for NFC Tap

Local File Staging

Stage with an on-device .bin file

11. Follow the steps on the screen to scan the remaining barcodes.

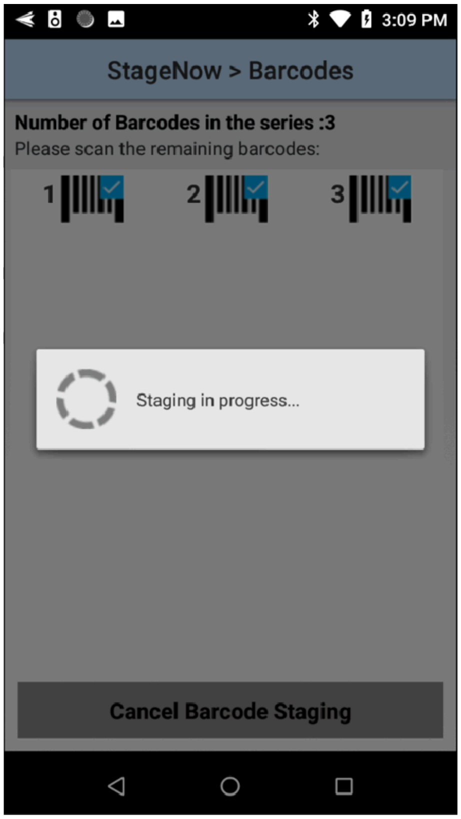


3:03 PM

StageNow > Barcodes

Number of Barcodes in the series :3

Please scan the remaining barcodes:



3:09 PM

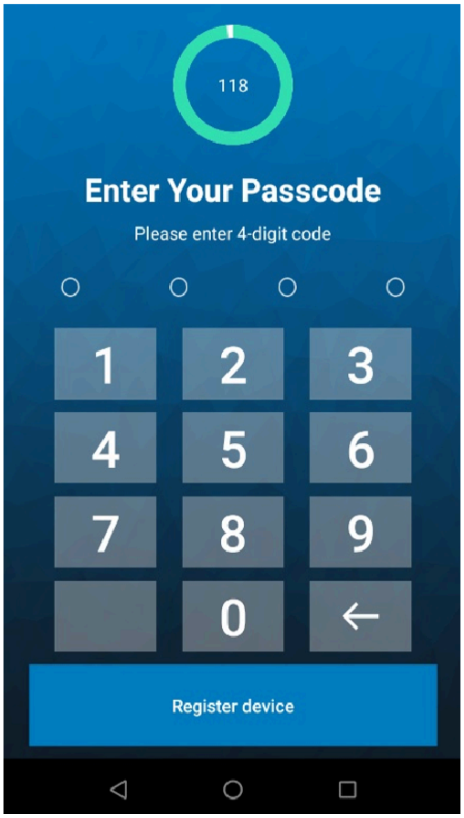
StageNow > Barcodes

Number of Barcodes in the series :3

Please scan the remaining barcodes:

Staging in progress...

ZAMS is installed on the mobile device, and the screen displays an **Enter Your Passcode** message, number keypads, and a **Register device** button.



118

Enter Your Passcode

Please enter 4-digit code

○ ○ ○ ○

Cabinet Registration on Devices

You must register a Cabinet on the mobile device before the ZAMS Software is configured on the device. After registering with the Cabinet, you can then unlock the device.

Two methods to register Cabinet on the mobile device are as follows:

- Load the `cabinet-device.config` file to the mobile device before installing the APK on the device. This configuration file automatically registers the mobile device with a selected Cabinet.
- Scan a QR Code displayed on the Cabinet UI to manually register the Cabinet.

Automatic Registration

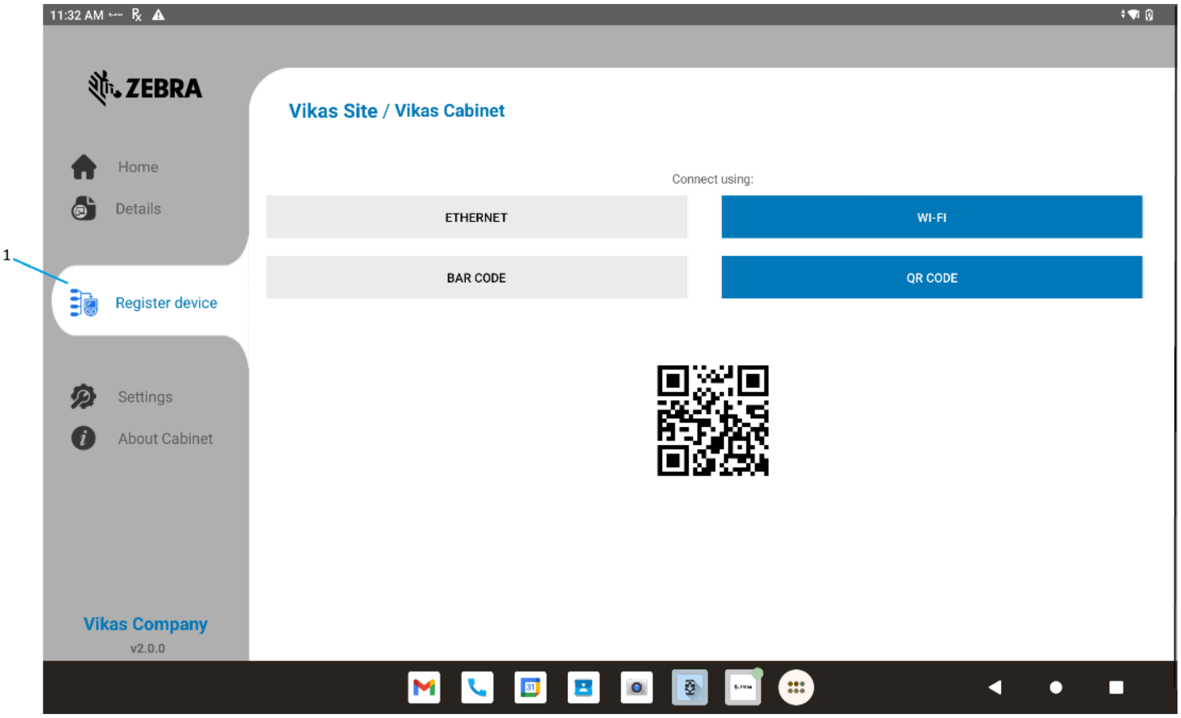
You can use the **StageNow** application to register the mobile device with the Cabinet automatically when installing ZAMS on the device.

Load the `cabinet-device.config` file to the mobile device before installing the APK on the device. This configuration file automatically registers the mobile device with a selected Cabinet. See Loading Files from the Local Server in StageNow on page 42 to learn how to load the configuration file.

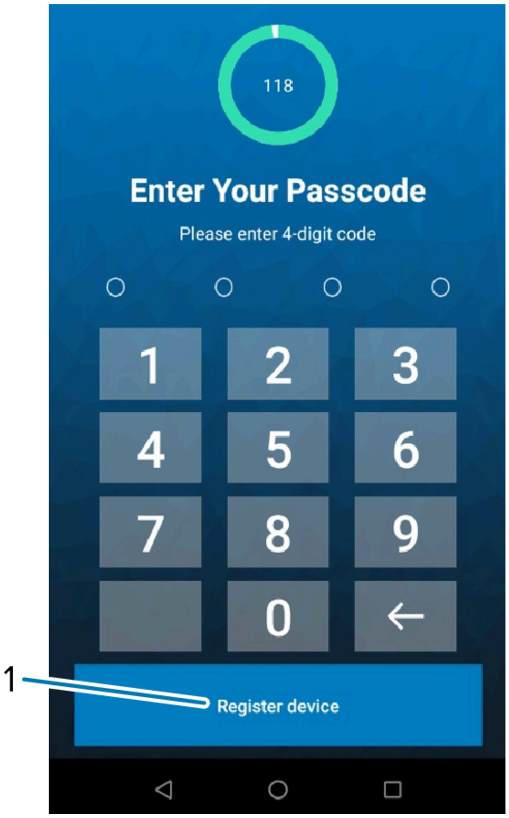
Manually Registering the Mobile Device

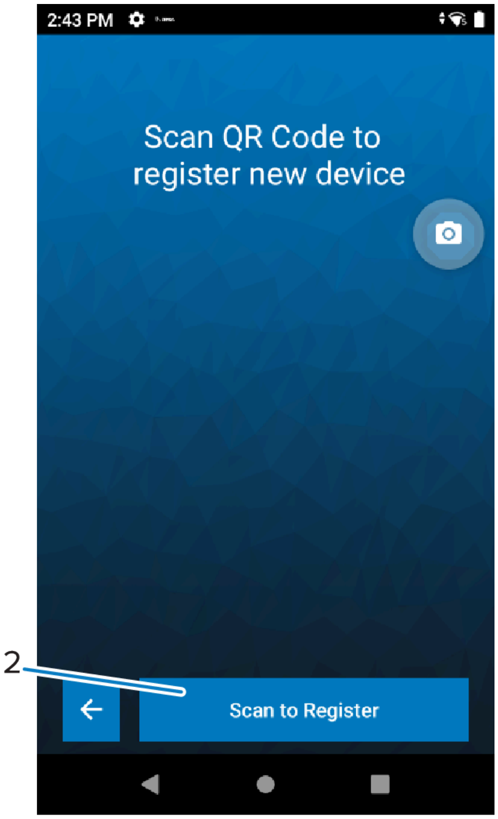
When installing the ZAMS software on the mobile device, you may be required to manually register the Cabinet on the mobile device by scanning a QR Code displayed on the Cabinet user interface.

1. On the CC6000 KIOSK, touch **Register device** (1).

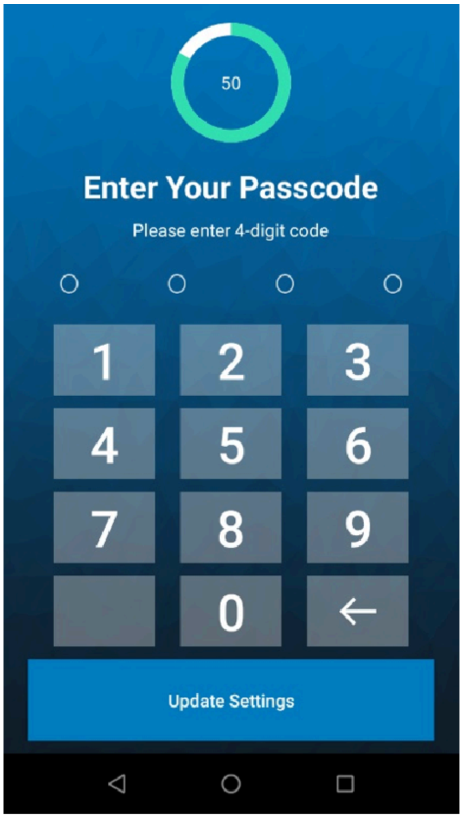


2. On the mobile device, touch **Register device** (1), and then **Scan to Register** (2).





3. Point the exit window of the device at the barcode display on the CC6000 KIOSK to register ZAMS on the mobile device.



The mobile device displays an **Enter Your Passcode** message with number keypads on the screen after the registration is successful.

The mobile device is now associated with the Cabinet and ready to use.

Configuring Sync Interval Frequency

To optimize communication between the KIOSK and the server/portal and reduce computational load, you can adjust two configurable timers on the KIOSK:

- **1 - 15 minutes** - This timer, set between 1 to 15 minutes, fetches a list of users, lost devices, and other information.
- **10 - 60 seconds** - This timer, adjustable between 10 to 60 seconds, and updates the status of devices (available, in use, missing) to the server.

There are two methods to configure the intervals.

1. **Using MDM Managed Configurations**:

   Utilizing the Mobile Device Management (MDM) feature, you can send Managed Configurations to the app. This feature enables you to set interval values within the range of **10 to 60 seconds** and **1 to 15 minutes** using the keys **syncCabinetAndDeviceStatusInterval** and **syncUserAndDeviceListInterval**, respectively.

2. **Using JSON File**:

   If you do not have an MDM setup or cannot send Managed Config to the app, use a JSON file to read the values. To set the values to the intervals, use a JSON file named `kioskconfig.json` and format it as shown below.

   Place this file in the `Download` folder and relaunch the KIOSK app. You can only change the values for the intervals. The keys and file structure remain the same. The values listed are in milliseconds.

   The following shows the `kioskconfig.json` configuration settings.

```
{
  "kioskConfig":
     {
      "syncIntervals":
       {
        "syncCabinetAndDeviceStatusInterval": 60000,
        "syncUserAndDeviceListInterval": 900000
       }
     }
}
```

   You can also push this JSON file from MDM. When using MDM to push the file, you must send a broadcast message to the app with the action `com.backsafe.kioskcore.action.READ_CONFIG` after pushing the file to the KIOSK's `Download` folder.

SSO Configuration

ZAMS supports Single Sign-On (SSO) login on Zebra Mobile devices from the 24.3.0 release (AMS device v3.1.0).

Users must install the Identity Guardian and AMS apps on Zebra Mobile devices to enable SSO login.

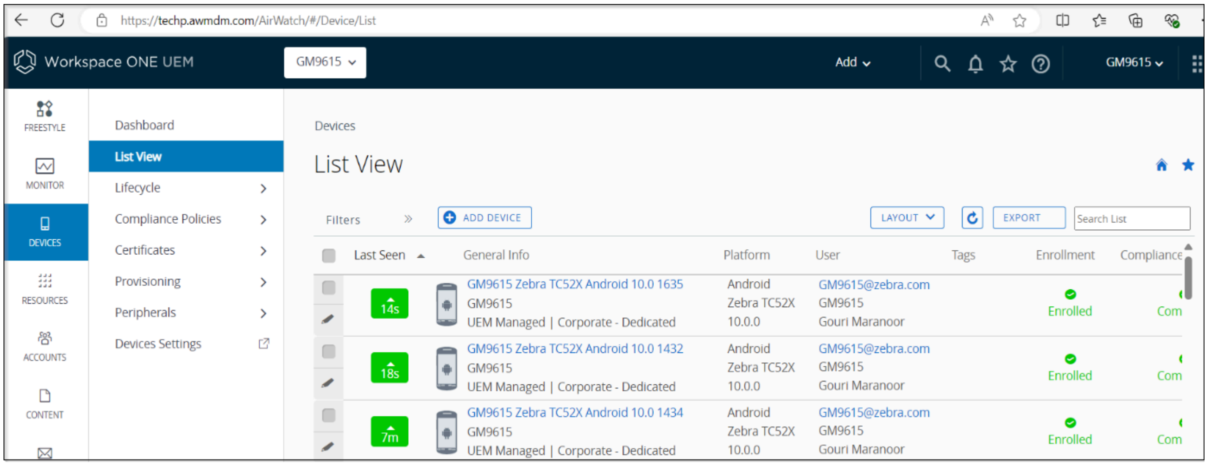
Follow the below steps to install the Identity Guardian (IG) app - To know more about Identity Guardian (IG): zebra.com/identityguardian.

NOTE: ZAMS only supports SSO on Zebra Mobile devices with Android 11 and Android 13.

Enrolling a Device

Enabling a device with AirWatch MDM.

1. Reset the device.
2. After the reset, tap five times on the welcome screen to open the camera for scanning.
3. Scan the QR Code displayed on the portal.
4. Connect to a network, and the enrollment completes automatically.
5. Click **Accept and Continue** and **Next** when prompted.
6. Accept the Google terms and conditions and click **Done**.
7. To confirm enrollment, navigate to **Devices** > **List View** to verify if the devices are enrolled.



Last Seen	General Info	Platform	User	Tags	Enrollment	Compliance
14s	GM9615 Zebra TC52X Android 10.0 1635 GM9615 UEM Managed | Corporate - Dedicated	Android Zebra TC52X 10.0.0	GM9615@zebra.com GM9615 Gouri Maranoor		Enrolled	Com
18s	GM9615 Zebra TC52X Android 10.0 1432 GM9615 UEM Managed | Corporate - Dedicated	Android Zebra TC52X 10.0.0	GM9615@zebra.com GM9615 Gouri Maranoor		Enrolled	Com
7m	GM9615 Zebra TC52X Android 10.0 1434 GM9615 UEM Managed | Corporate - Dedicated	Android Zebra TC52X 10.0.0	GM9615@zebra.com GM9615 Gouri Maranoor		Enrolled	Com

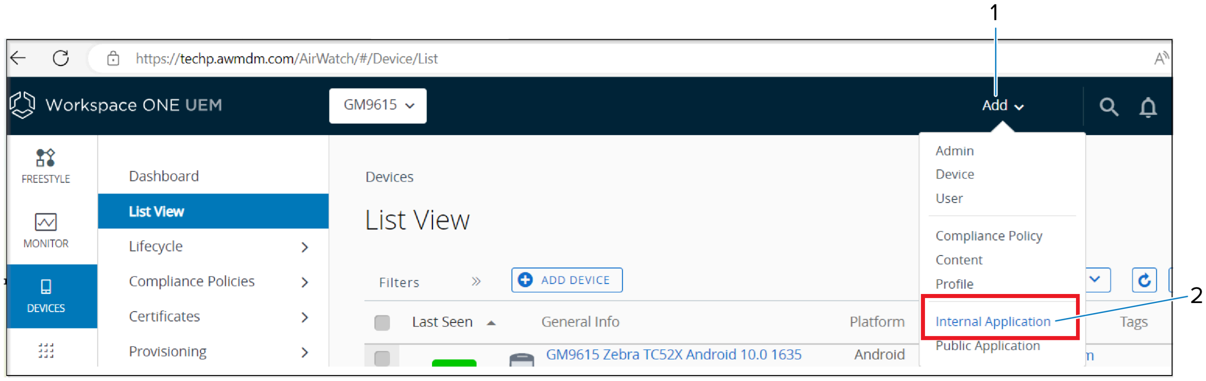
Adding Identity Guardian Application

This section shows how to add Internal and External applications to the Identity Guardian Application.

Internal Application

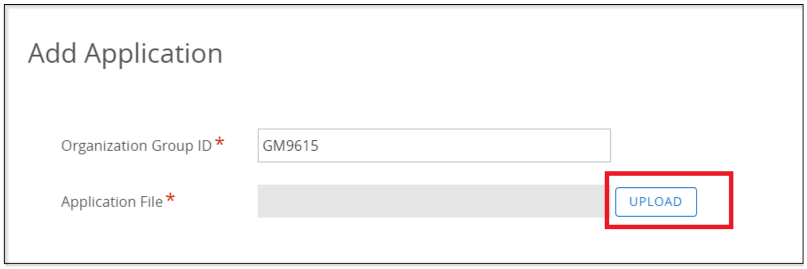
The Internal Application explains how to add to the Identity Guardian Application.

1. Click **Add** (1) at the top-right corner and select **Internal Application** (2).



The **Add Application** page displays.

2. Click **Upload**.

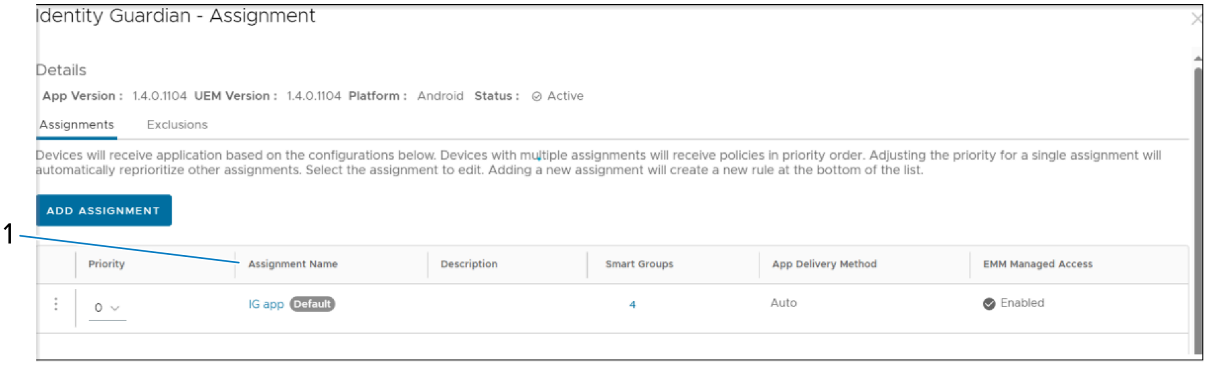


Add Application

Organization Group ID * GM9615

Application File * UPLOAD

3. Navigate to the assignments page.



Identity Guardian - Assignment

Details

App Version : 1.4.0.1104 **UEM Version :** 1.4.0.1104 **Platform :** Android **Status :** Active

Assignments Exclusions

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically reprioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

ADD ASSIGNMENT

Priority	Assignment Name	Description	Smart Groups	App Delivery Method	EMM Managed Access
0	IG app Default		4	Auto	Enabled

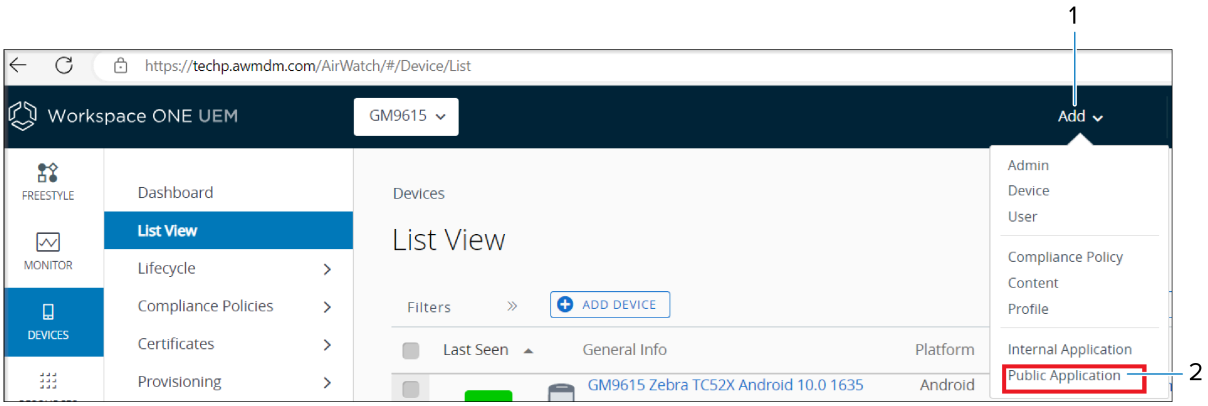
4. Click **Assignment Name** (1).

The next steps will continue from Identity Guardian configuration.

External Application

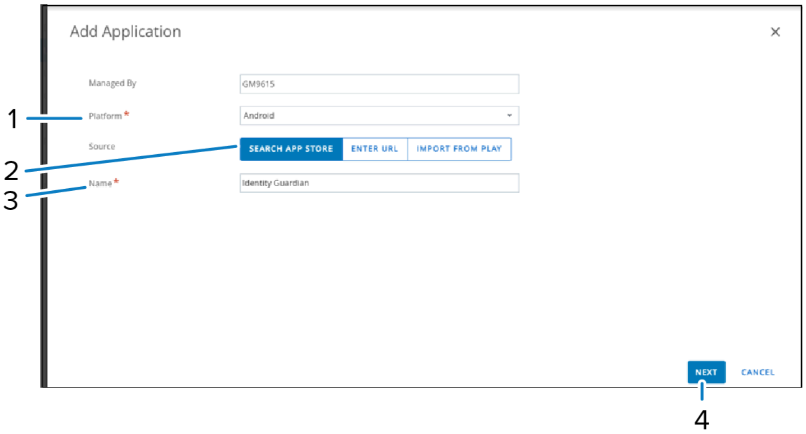
The External Application explains how to add to the Identity Guardian Application.

1. Click **Add** (1) at the top-right corner and select **Public Application** (2).



The **Add Application** page displays.

2. In the **Add Application** section, select the **Platform** (1), click **Search App Store** (2) as the source, enter the appropriate **Name** (3), and click **Next** (4).


Add Application

Managed By: GM9615

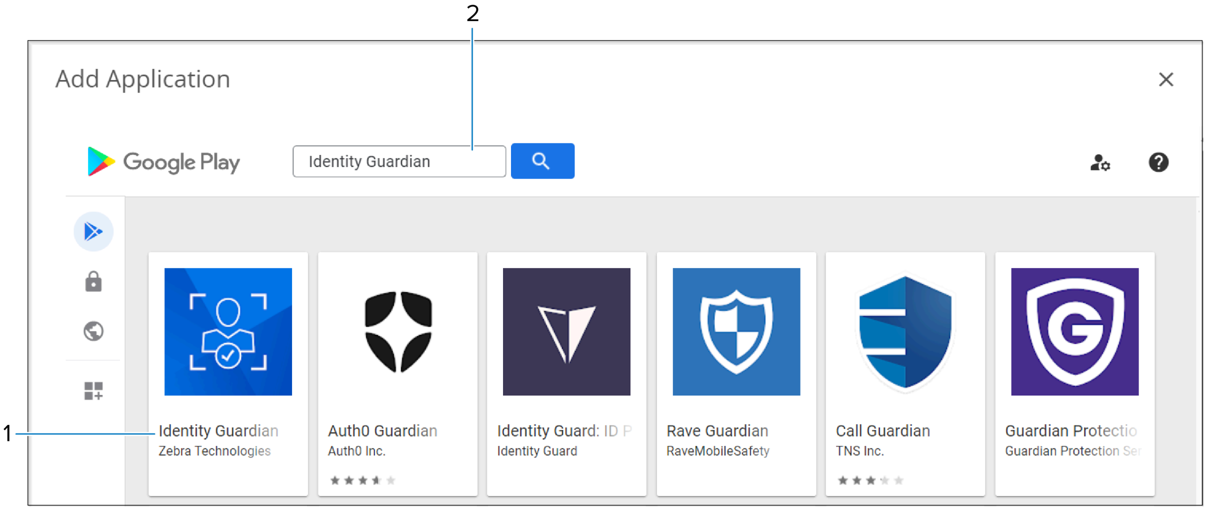
Platform*: Android

Source: SEARCH APP STORE

Name*: Identity Guardian

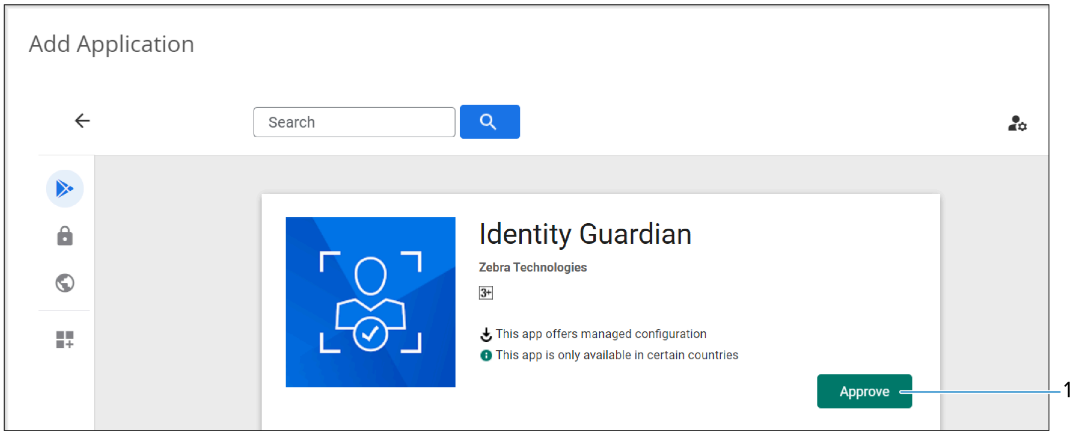
The **Add Application Google Play** page displays.

3. Select the **Identity Guardian** (1) application, or you can also search for the application via the **Search Engine** (2).



The **Identity Guardian** application displays.

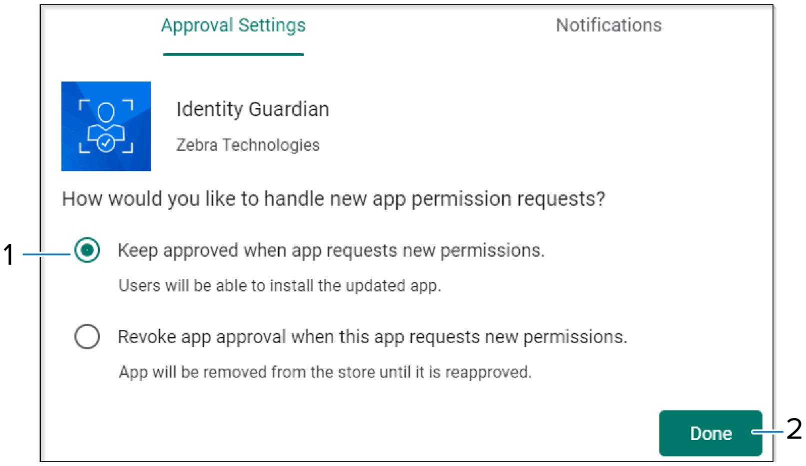
4. Click **Approve** (1) .



This app offers managed configuration

This app is only available in certain countries

5. Select **Keep approved when the app requests new permissions** (1) and click **Done** (2) .



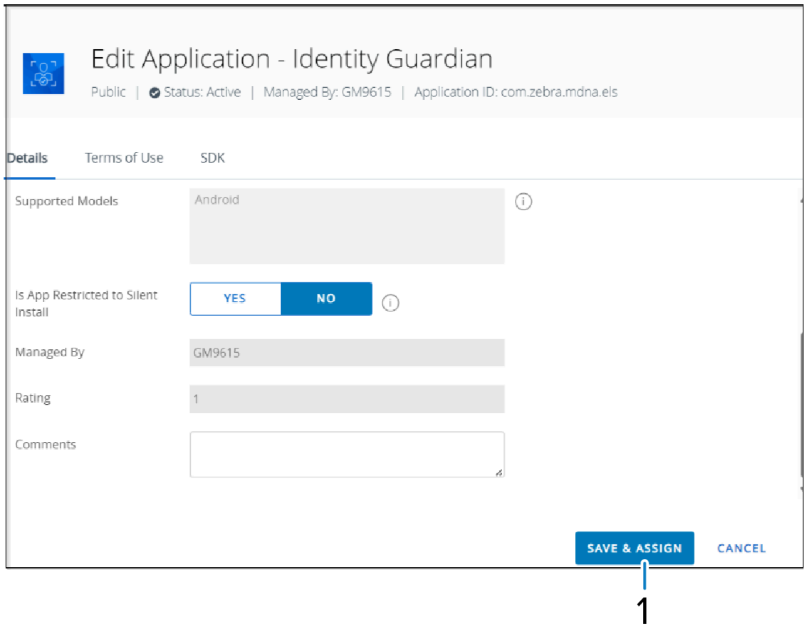
How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

The **Edit Application Identify Guardian** page displays.

6. In the **Edit Application** section, do not select any settings and click **Save and Assign** (1) .



Edit Application - Identity Guardian

Public | Status: Active | Managed By: GM9615 | Application ID: com.zebra.mdna.els

Details | Terms of Use | SDK

Supported Models: Android

Is App Restricted to Silent Install: YES | NO

Managed By: GM9615

Rating: 1

Comments:

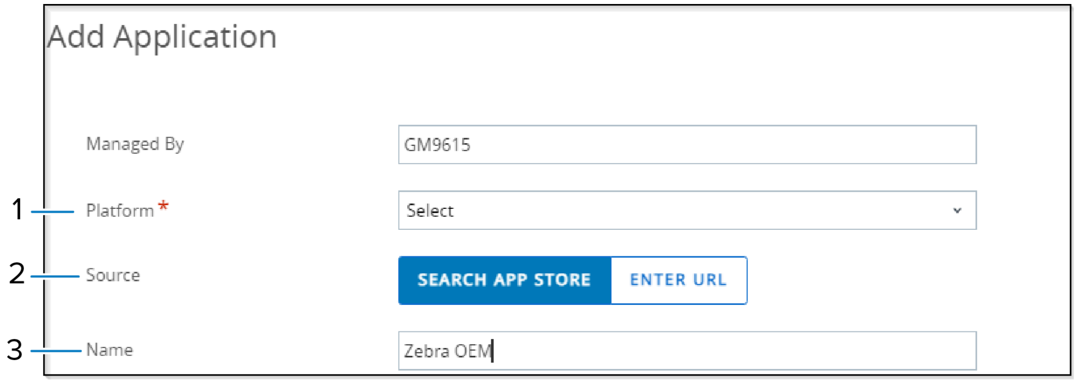
Installing a Zebra OEM Application

To use the full version of Identity Guardian, user need to install the Zebra OEM application to AirWatch and include the Smart Group being used (Refer to the Creating a Smart Group and assign devices for more details).

1. Navigate to **Resources** > **Apps** > **Native**.

2. Select **Public Apps**.

3. Click **Add Application**.



Add Application

Managed By: GM9615

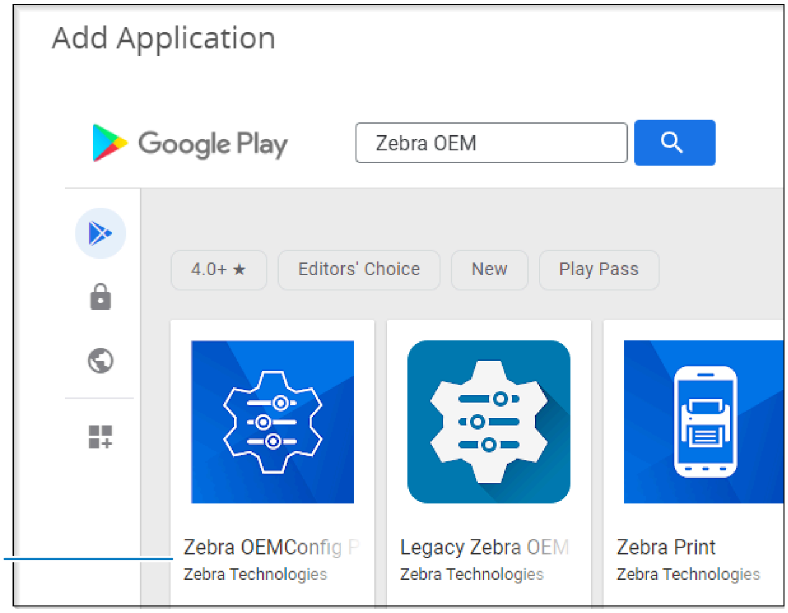
Platform*: Select

Source: SEARCH APP STORE | ENTER URL

Name: Zebra OEM

4. Select the **Platform** (1), click **Search Appstore** (2) as the source, and enter a **Name** (3).

5. Click **Next**.



Add Application

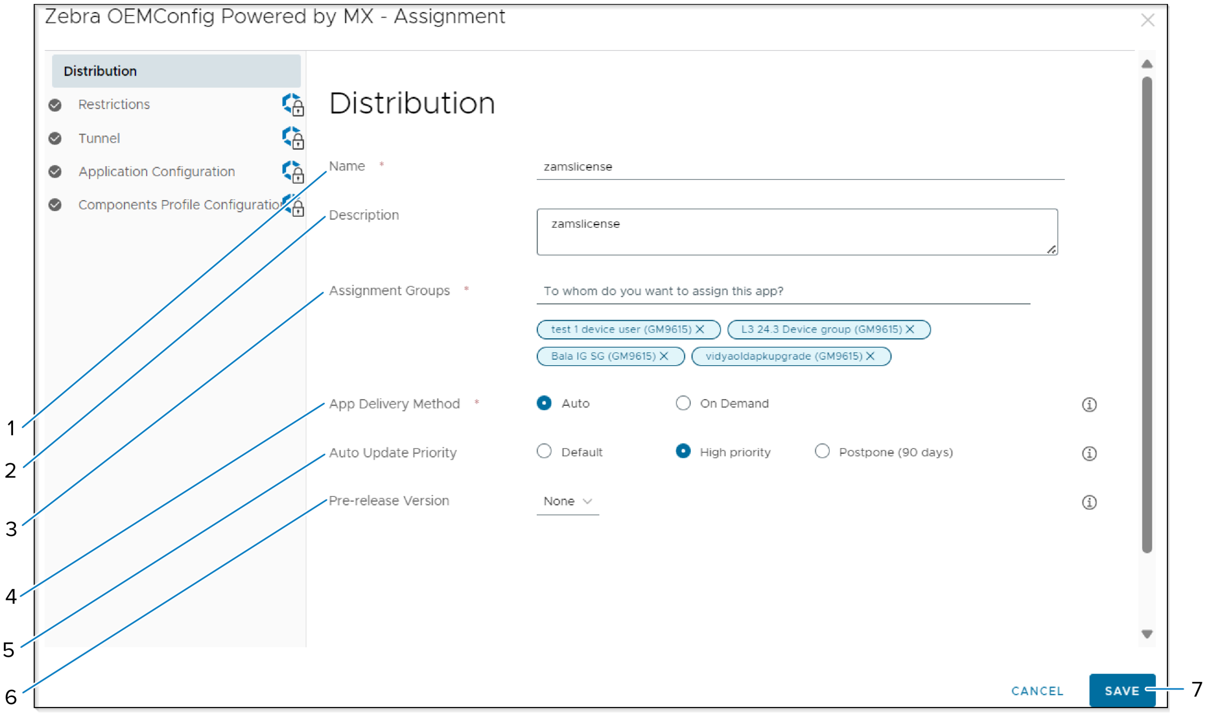
Google Play: Zebra OEM

The **Add Application Google Play** page displays.

6. Select the **Zebra OEM Configuration** (1) app and click **Approve**. In the display message, select **Keep approved when app requests new permissions**.

   The **Edit Application** page displays.

7. In the **Edit Application** page, click **Save and Assign**.



Zebra OEMConfig Powered by MX - Assignment

Distribution

Name *: zamslicense

Description: zamslicense

Assignment Groups *: To whom do you want to assign this app?
test 1 device user (GM9615) X; L3 24.3 Device group (GM9615) X; Bala IG SG (GM9615) X; vidyaoldapkupgrade (GM9615) X

App Delivery Method *: ● Auto ○ On Demand

Auto Update Priority: ○ Default ● High priority ○ Postpone (90 days)

Pre-release Version: None

The **Assignment** page displays.

8. In the **Assignment** page, provide the **Name** (1), **Description** (2), **Assignment Group (Smart Group)** (3), set the **App delivery method** (4) as **Auto**, **Auto Update Priority** (5) as **High priority**, **Pre-release version** (6) as **None**, and click **Save** (7).

NOTE: The Zebra Licensing Team will provide the **Name** and **Server URL** details:

Name: idguardian-XX-XXXXX (example)

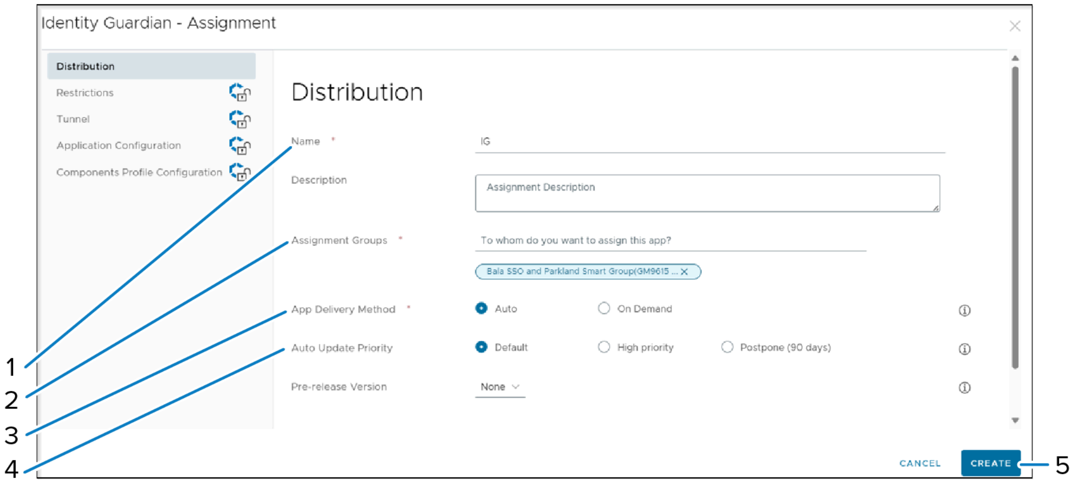
Server URL: https://zebra-licesnsing-xxxxxx (example)

Identify Guardian Configurations

The user is directed to the Assignment Page when adding an Internal or External applications.

Assignment

The following information must be included on the **Assignment** page:



Identity Guardian - Assignment

Distribution

Name * IG

Description: Assignment Description

Assignment Groups * To whom do you want to assign this app?

Bala SSO and Parkland Smart Group(GM9615 ... ×

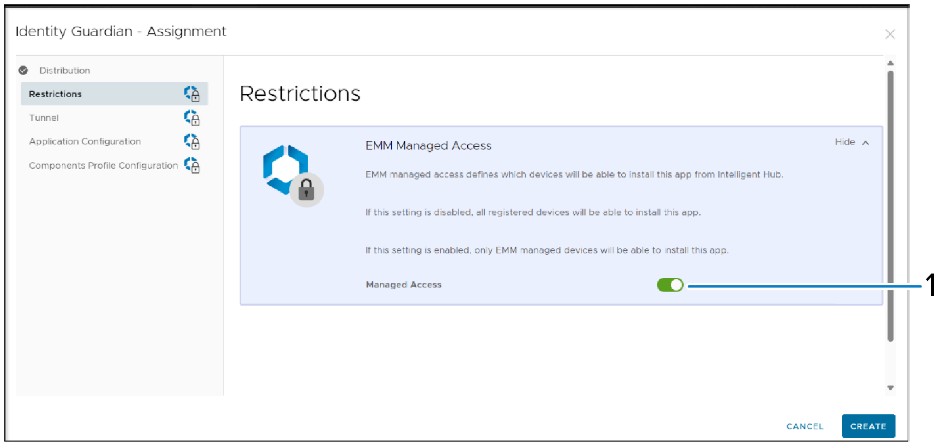
App Delivery Method * ● Auto ○ On Demand

Auto Update Priority ● Default ○ High priority ○ Postpone (90 days)

Pre-release Version None

1. Enter the distribution **Name** (1) on the Assignment page.
2. Specify the **Assignment Groups** (2).
3. Set the **App Delivery Method** (3) to **Auto**.
4. Set the **Auto-Update Priority** (4) to **Default**.
5. Click **Create** (5).

Restrictions:



Identity Guardian - Assignment

Restrictions

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access

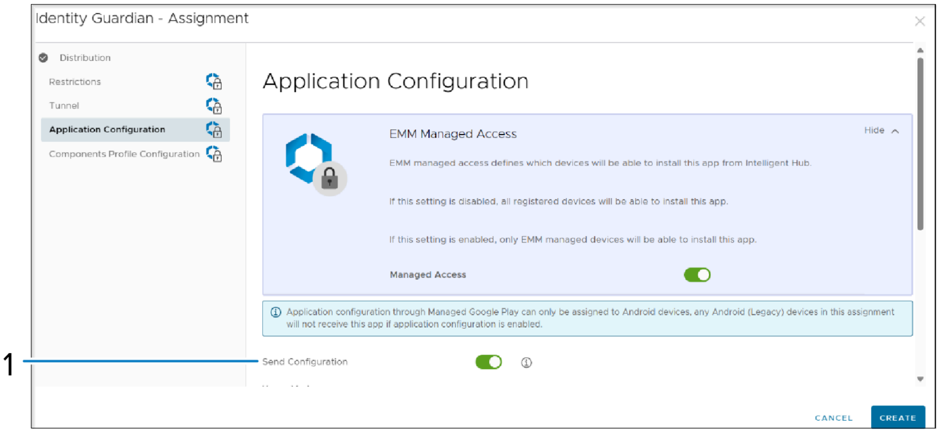
- Navigate to **Restrictions** to enable **Managed Access** (1).

NOTE: Do not make any changes to the Tunnel Settings.

Application Configuration

To configure the application:

1. Navigate to **Application Configuration** and select **Send Configuration** (1).



Identity Guardian - Assignment

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

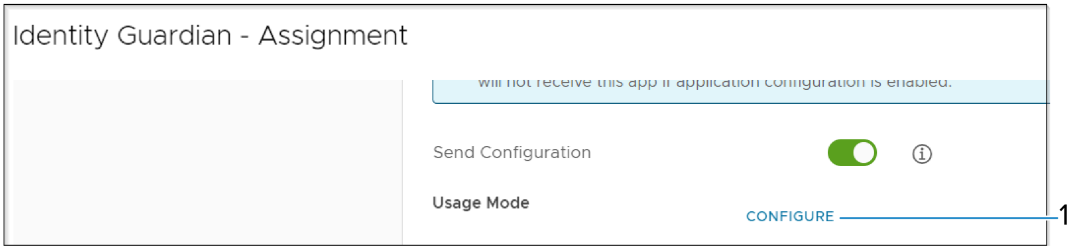
If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access

Application configuration through Managed Google Play can only be assigned to Android devices, any Android (Legacy) devices in this assignment will not receive this app if application configuration is enabled.

Send Configuration

2. Click **Configure** (1) for **Usage Mode**.



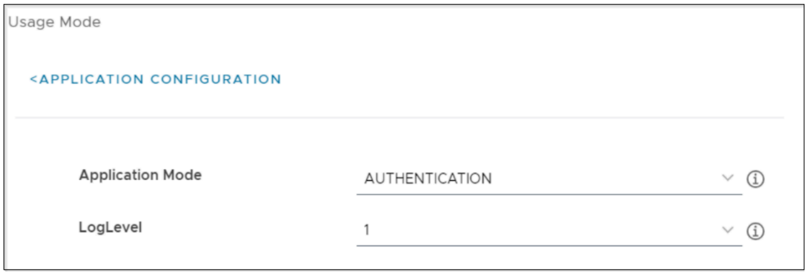
Identity Guardian - Assignment

will not receive this app if application configuration is enabled.

Send Configuration

Usage Mode

3. Set the **Application Mode** to **Authentication** and **Log Level** to **1**.



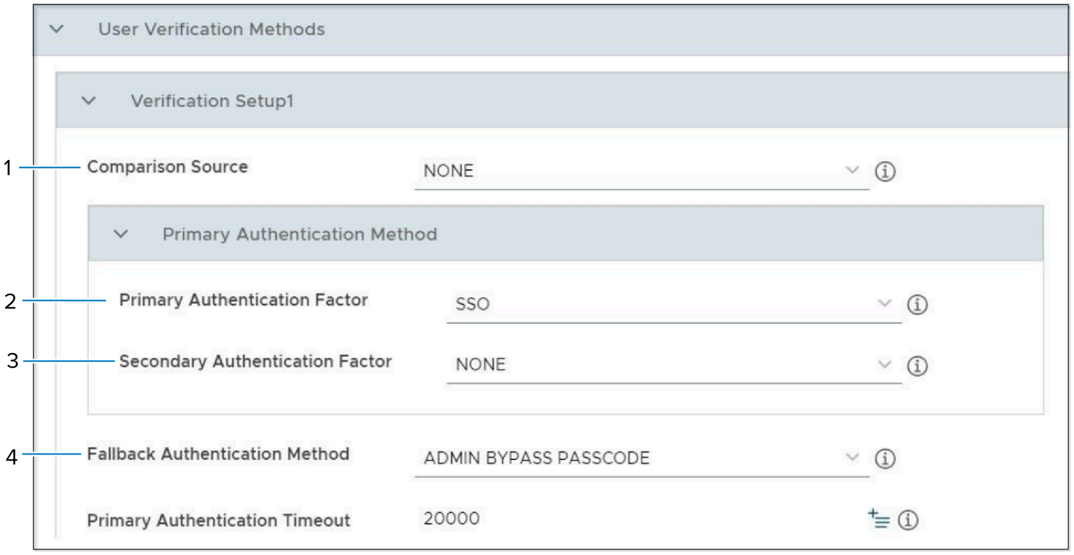
Usage Mode

<APPLICATION CONFIGURATION

Application Mode: AUTHENTICATION

LogLevel: 1

- Skip **Enrollment Configuration**.
- Click **Authentication Configuration**.
- Select **Verification Setup 1**.
- In **Verification Setup 1**, configure the following:



User Verification Methods

Verification Setup1

Comparison Source: NONE

Primary Authentication Method

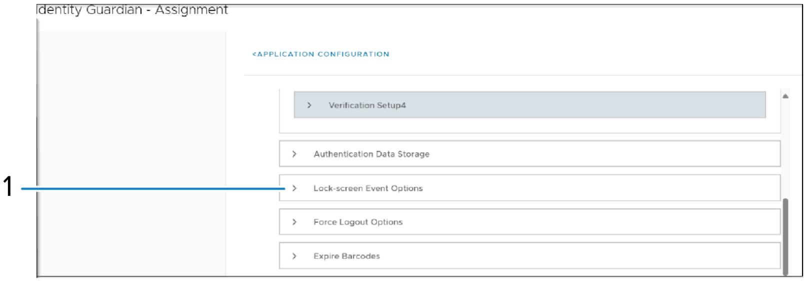
Primary Authentication Factor: SSO

Secondary Authentication Factor: NONE

Fallback Authentication Method: ADMIN BYPASS PASSCODE

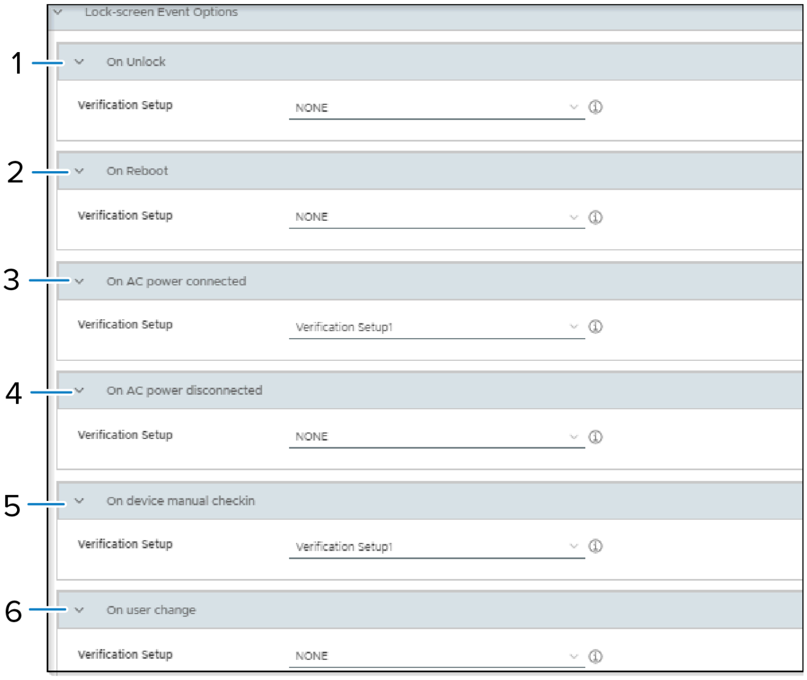
Primary Authentication Timeout: 20000

- **Comparison Source: None** (1)
- **Primary Authentication Method:**
  - **Primary Authentication Factor: SSO (Single Sign On)** (2)
  - **Secondary Authentication Factor: None** (3)
  - **Fallback Authentication Method: Admin Bypass Passcode** (4)
- Click **Lock Screen Event Options** (1).



dentity Guardian - Assignment
<APPLICATION CONFIGURATION
Verification Setup4
Authentication Data Storage
Lock-screen Event Options
Force Logout Options
Expire Barcodes
1

- In the lock screen options, add the following:



Lock-screen Event Options

On Unlock

Verification Setup: NONE

On Reboot

Verification Setup: NONE

On AC power connected

Verification Setup: Verification Setup1

On AC power disconnected

Verification Setup: NONE

On device manual checkin

Verification Setup: Verification Setup1

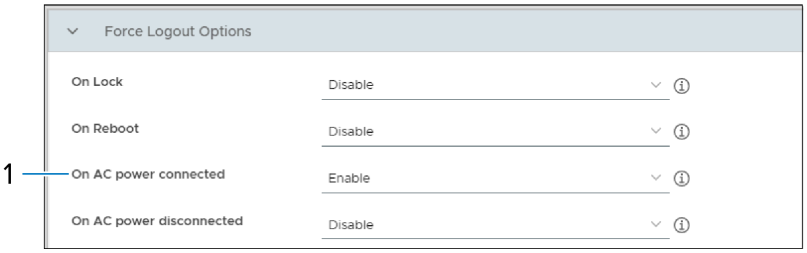
On user change

Verification Setup: NONE

- **On Unlock: None** (1)
- **On Reboot: None** (2)
- **On AC power connected: Verification Setup 1** (3)
- **On AC power disconnected: None** (4)
- **On device manual check-in: Verification Setup 1** (5)
- **On user change: None** (6)

NOTE: If **Bluetooth Proximity** is enabled in Portal, set **On AC Power Connected** as **None**.

4. Click **Force Logout Options**.



Force Logout Options

On Lock: Disable

On Reboot: Disable

On AC power connected: Enable

On AC power disconnected: Disable

5. Set **On AC Power Connected** as **Enabled** (1).

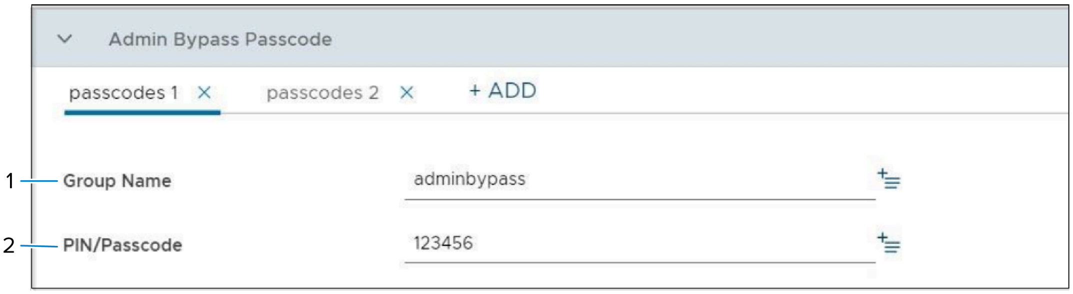
NOTE: If **Bluetooth Proximity** is enabled in Portal, set **On AC Power Connected** as **Disabled**.

6. Save the configurations.

Admin Bypass Passcode

For the Admin Bypass Passcode:

1. Click **Admin Bypass Passcode**.



Admin Bypass Passcode

Group Name: adminbypass

PIN/Passcode: 123456

2. Enter values for **Group Name** (1) and **PIN/Passcode** (2).

Signature Permission for Device & KIOSK

Signature Permissions are documented for both KIOSK and Device, with consideration for different Operating System (OS) versions, ensuring that permissions can be configured correctly in the Mobile Device Management (MDM) system.

Device Permissions

This section explains the Device's operating system.

Android 13 (A13) Specific Permission:

```
<uses-permission android:name="android.permission.BLUETOOTH_SCAN" />
```

```
<uses-permission android:name="android.permission.BLUETOOTH_CONNECT" />
```

```
<uses-permission android:name="android.permission.POST_NOTIFICATIONS"/>
```

Android 11 (A11) Specific Permissions:

```
<uses-permission android:name="android.permission.MANAGE_EXTERNAL_STORAGE"/>
```

```
<uses-permission
 android:name="android.permission.ACCESS_BACKGROUND_LOCATION" />
```

```
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
```

```
<uses-permission android:name="android.permission.CAMERA" />
```

```
<uses-permission android:name="android.permission.REORDER_TASKS" />
```

```
<uses-permission android:name="android.permission.SCHEDULE_EXACT_ALARM" />
```

```
<uses-permission android:name="android.permission.USE_EXACT_ALARM" />
```

`android.permission.BIND_DEVICE_ADMIN`: `BIND_DEVICE_ADMIN` permission in Android is a special permission used with the Device Administration API.

- **Device Administration**: The primary role of `BIND_DEVICE_ADMIN` is to enable an application to become a device administrator on the device. This allows the application to perform specific administrative tasks that affect the overall device behavior.
- **Enterprise Use:** This permission is used by enterprise applications, such as those for managing corporate devices or implementing Mobile Device Management (MDM) solutions.

KIOSK Permissions

This section explains the KIOSK's operating system.

Android 13 (A13) Specific Permissions:

```
<uses-permission android:name="android.permission.BLUETOOTH_SCAN" />
```

```
<uses-permission android:name="android.permission.BLUETOOTH_CONNECT" />
```

```
<uses-permission android:name="android.permission.POST_NOTIFICATIONS"/>
```

Android 11 (A11) Specific Permissions:

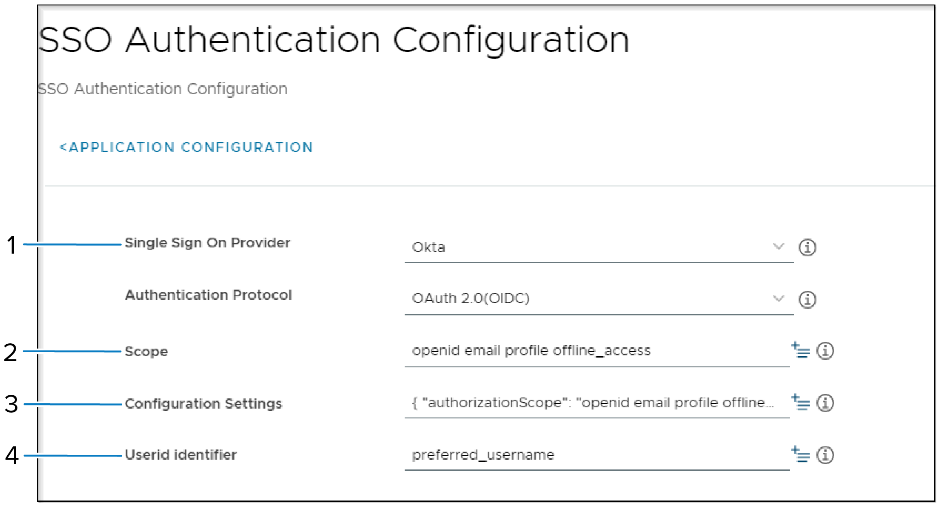
```
<uses-permission android:name="android.permission.MANAGE_EXTERNAL_STORAGE"/>
```

```
<uses-permission
 android:name="android.permission.ACCESS_BACKGROUND_LOCATION" />
```

SSO Authentication Configuration

This section explains how to configure SSO Authentication by specifying and saving specific settings.

1. Click the **SSO Authentication Configuration**.



SSO Authentication Configuration

SSO Authentication Configuration

<APPLICATION CONFIGURATION

1 Single Sign On Provider: Okta

Authentication Protocol: OAuth 2.0(OIDC)

2 Scope: openid email profile offline_access

3 Configuration Settings: { "authorizationScope": "openid email profile offline...

4 Userid identifier: preferred_username

2. Select the **Single Sign-on Provider** (1).
3. Provide the **Scope** (2), **Configuration Settings** (3), and **User ID Identifier** (4).

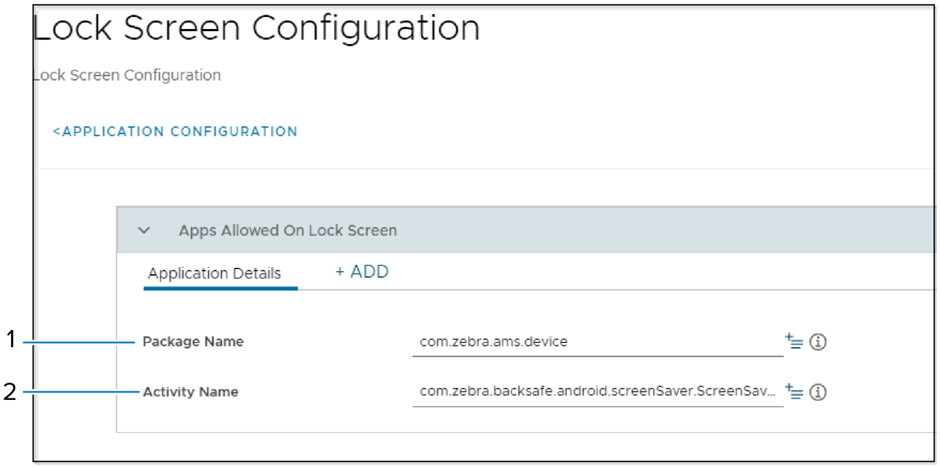
NOTE: For the above details, refer to the Technical Documents.

4. Save the configurations.

Lock Screen Configuration

This section explains how to configure the lock screen on a device.

1. Click **Lock Screen Configuration**.



Lock Screen Configuration

Lock Screen Configuration

<APPLICATION CONFIGURATION

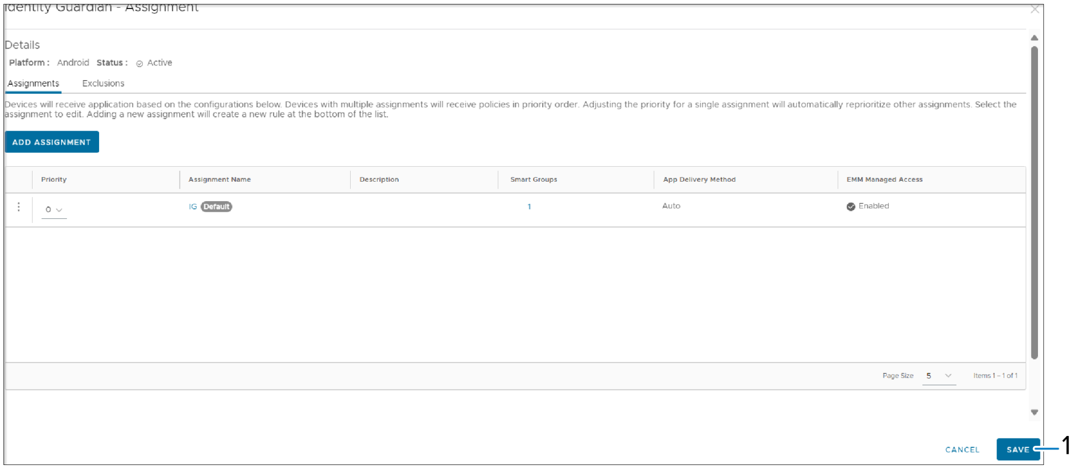
Apps Allowed On Lock Screen

Application Details   + ADD

1 Package Name: com.zebra.ams.device

2 Activity Name: com.zebra.backsafe.android.screenSaver.ScreenSav...

2. Add the package and activity details as follows:
   - **Package Name: `com.zebra.ams.device`** (1)
   - **Activity Name: `com.zebra.backsafe.android.screenSaver.ScreenSaverActivity`** (2)
3. Click **Create** and then **Save** (1).



Identity Guardian - Assignment

Details

Platform : Android Status : Active

Assignments Exclusions

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically reprioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

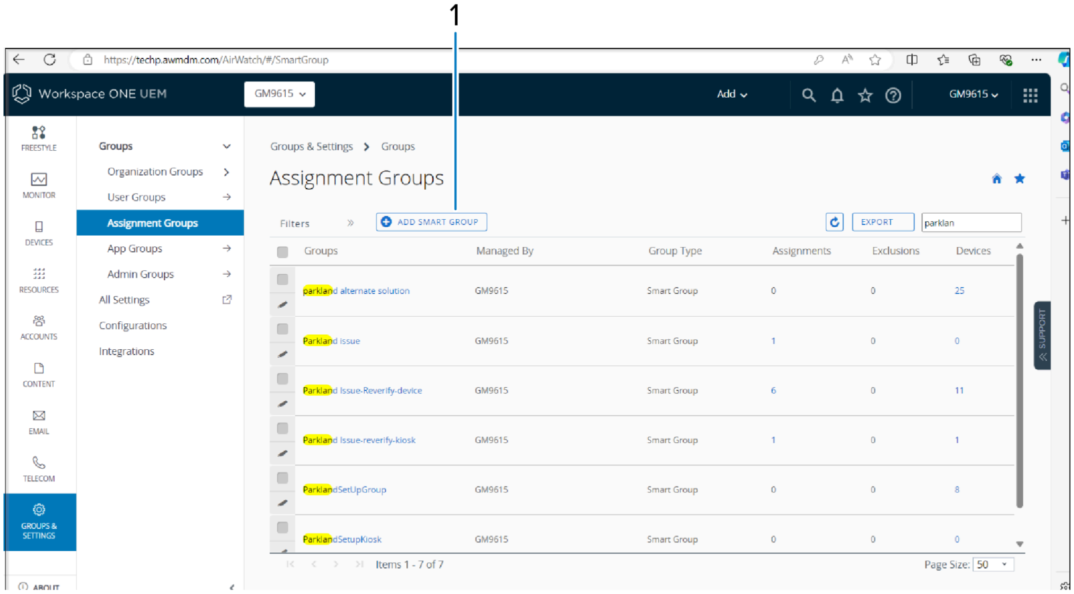
Priority	Assignment Name	Description	Smart Groups	App Delivery Method	EMM Managed Access
0	IG Default		1	Auto	Enabled

Page Size 5 Items 1 - 1 of 1

Creating a Smart Group

To create a smart group:

1. Navigate to **Groups and Settings** > **Groups** > **Assignment Groups**. Click **Add Smart Group** (1).



https://techp.awmdm.com/AirWatch/#/SmartGroup

Groups & Settings > Groups

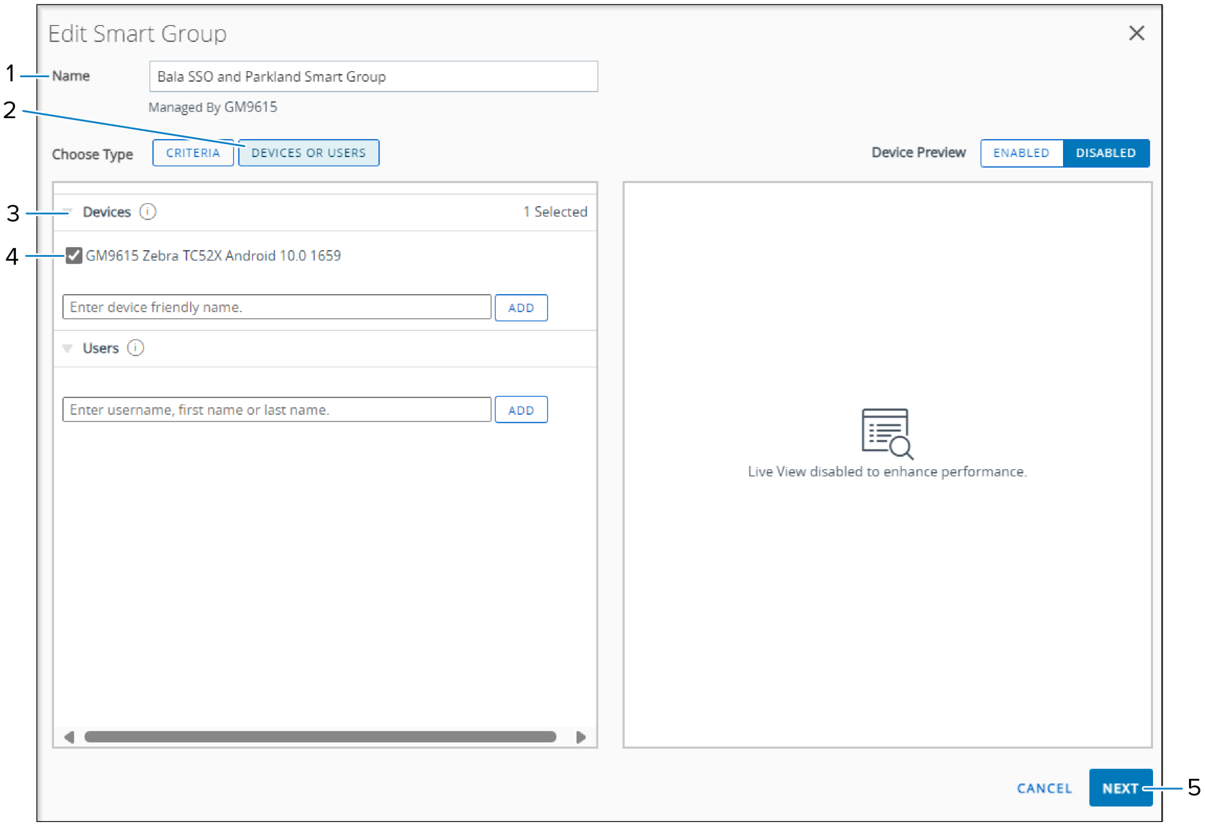
Assignment Groups

Groups	Managed By	Group Type	Assignments	Exclusions	Devices
parkland alternate solution	GM9615	Smart Group	0	0	25
Parkland issue	GM9615	Smart Group	1	0	0
Parkland Issue-Reverify-device	GM9615	Smart Group	6	0	11
Parkland Issue-reverify-kiosk	GM9615	Smart Group	1	0	1
ParklandSetUpGroup	GM9615	Smart Group	0	0	8
ParklandSetupKiosk	GM9615	Smart Group	0	0	0

Items 1 - 7 of 7 Page Size: 50

The **Edit Smart Group** page displays.

2. Enter a **Name** (1).



Edit Smart Group

Name: Bala SSO and Parkland Smart Group

Managed By GM9615

Choose Type: CRITERIA | DEVICES OR USERS

Device Preview: ENABLED | DISABLED

Devices — 1 Selected

☑ GM9615 Zebra TC52X Android 10.0 1659

Enter device friendly name. ADD

Users

Enter username, first name or last name. ADD

Live View disabled to enhance performance.

CANCEL NEXT

3. Click **Devices or Users** (2) to assign the list of enrolled devices.

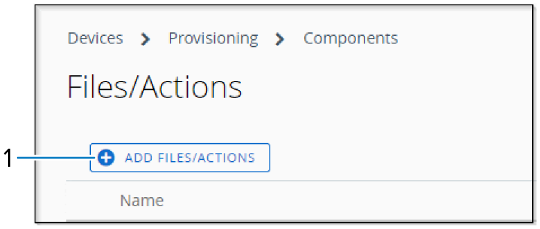
4. Select your enrolled **Devices** (3).

NOTE: Do not select anything under user **Gouri Maranoor, GM9615@zebra.com** (4), as this is for reference purposes. Select your device user.

5. Click **Save** (5).

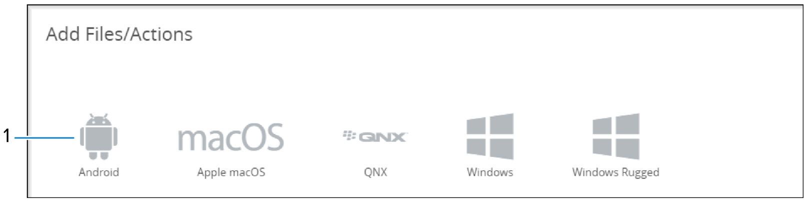
6. After creating the smart group, proceed with the following:

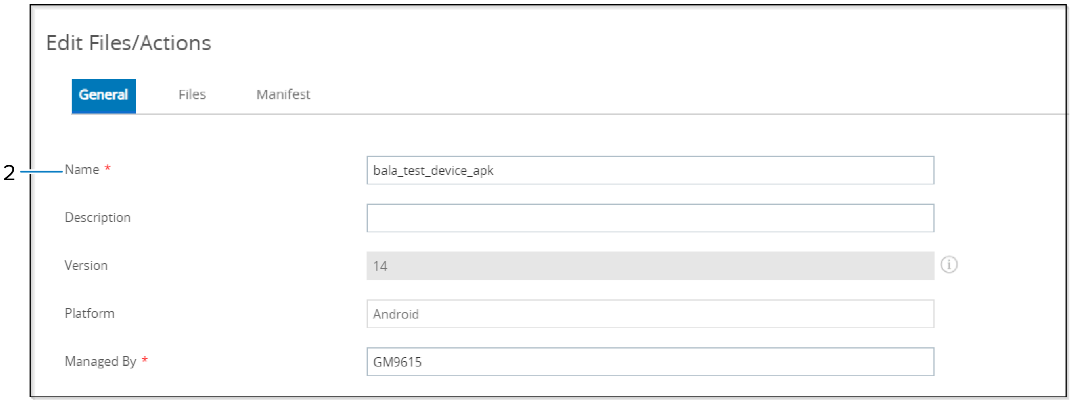
   a) Navigate to **Devices** > **Components** > **Files/Actions**. Click **Add Files/Actions** (1).



   The **Add Files/Actions** page displays.

   b) Select **Android** (1) and provide a **Name** (2).





Name * bala_test_device_apk

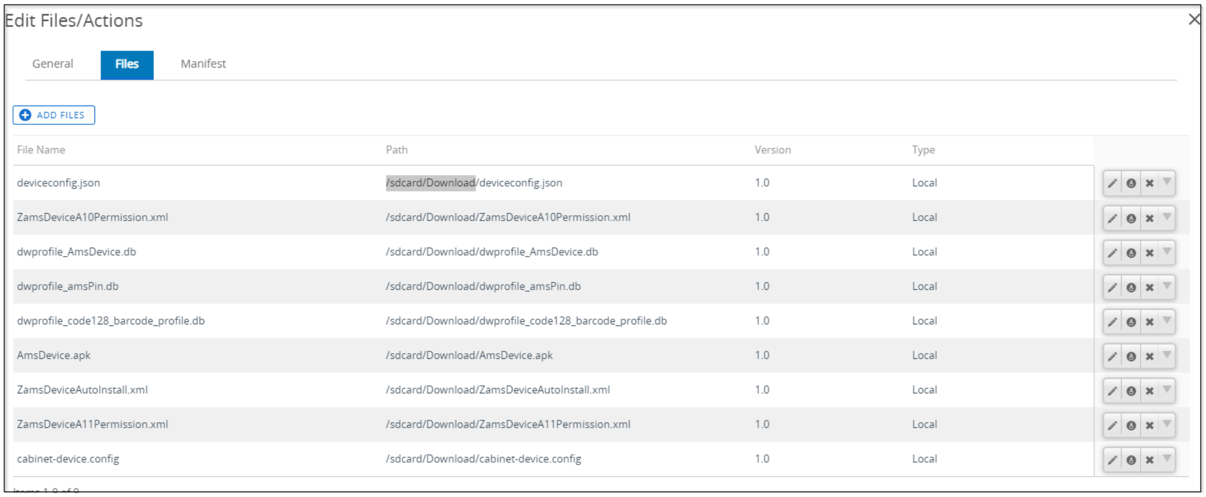
Description

Version 14

Platform Android

Managed By * GM9615

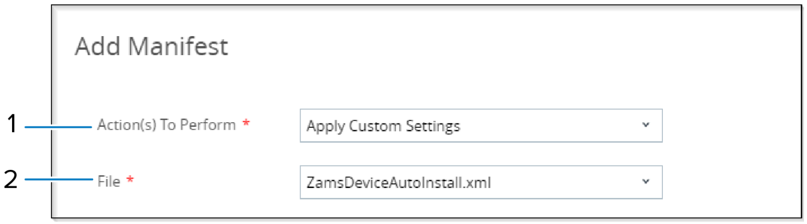
   c) Navigate to **Files** and add all the supporting files with the path set to **`/sdcard/Download`**.



File Name	Path	Version	Type
deviceconfig.json	/sdcard/Download/deviceconfig.json	1.0	Local
ZamsDeviceA10Permission.xml	/sdcard/Download/ZamsDeviceA10Permission.xml	1.0	Local
dwprofile_AmsDevice.db	/sdcard/Download/dwprofile_AmsDevice.db	1.0	Local
dwprofile_amsPin.db	/sdcard/Download/dwprofile_amsPin.db	1.0	Local
dwprofile_code128_barcode_profile.db	/sdcard/Download/dwprofile_code128_barcode_profile.db	1.0	Local
AmsDevice.apk	/sdcard/Download/AmsDevice.apk	1.0	Local
ZamsDeviceAutoInstall.xml	/sdcard/Download/ZamsDeviceAutoInstall.xml	1.0	Local
ZamsDeviceA11Permission.xml	/sdcard/Download/ZamsDeviceA11Permission.xml	1.0	Local
cabinet-device.config	/sdcard/Download/cabinet-device.config	1.0	Local

Items 1-9 of 9

   d) Navigate to **Manifest** and click **Add Manifest**.



Add Manifest

Action(s) To Perform * Apply Custom Settings

File * ZamsDeviceAutoInstall.xml

e) Select **Apply Custom Settings** (1) from the option.

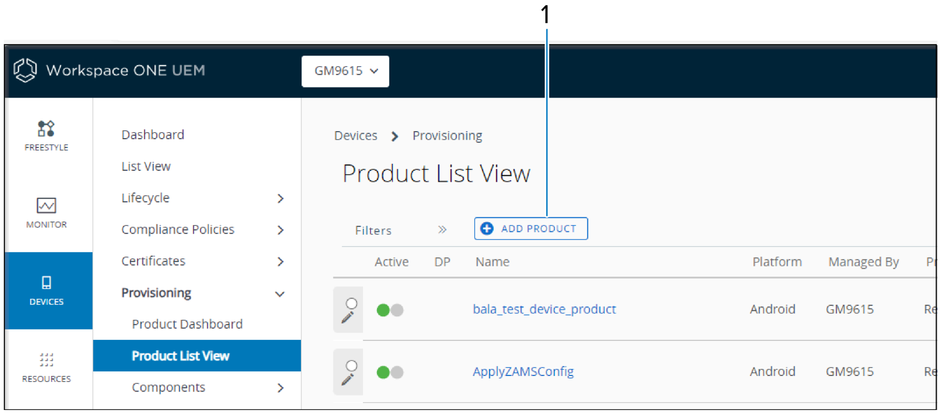
f) Select the file **`ZamsDeviceAutoInstall.xml`** (2) from the option.

g) Click **Save** and also **Save** the profile.

Provisioning

To provision a new product:

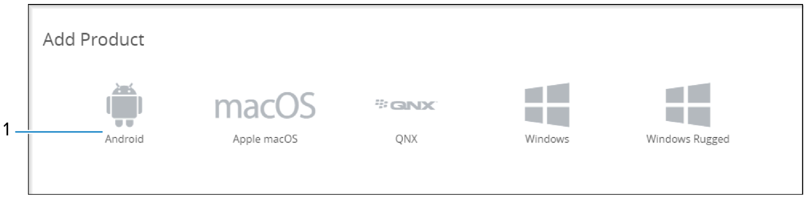
1. Go to **Device** > **Product List View**. Click **Add Product** (1).



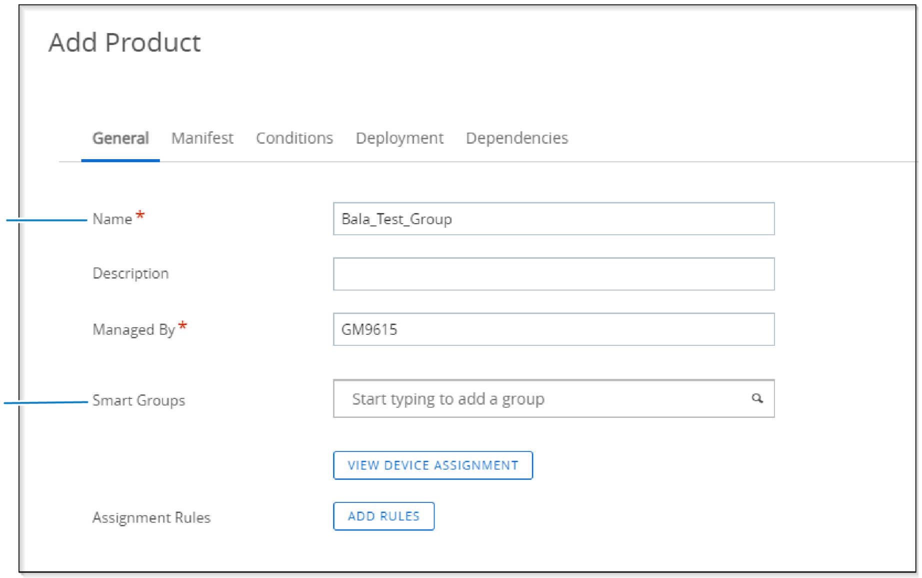
Active	DP	Name	Platform	Managed By	P
● ●		bala_test_device_product	Android	GM9615	Re
● ●		ApplyZAMSConfig	Android	GM9615	Re

The **Add Product** page displays.

2. Select **Android** (1).



3. In the **General** tab, enter the product **Name** (1) and **Smart Groups** (2).



Name* Bala_Test_Group

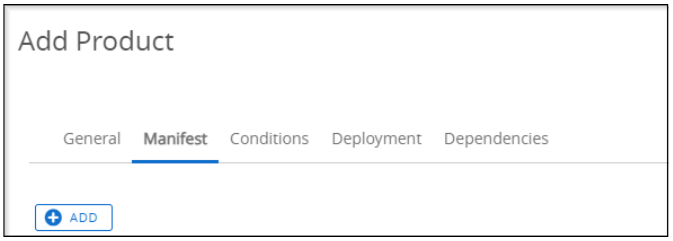
Description

Managed By* GM9615

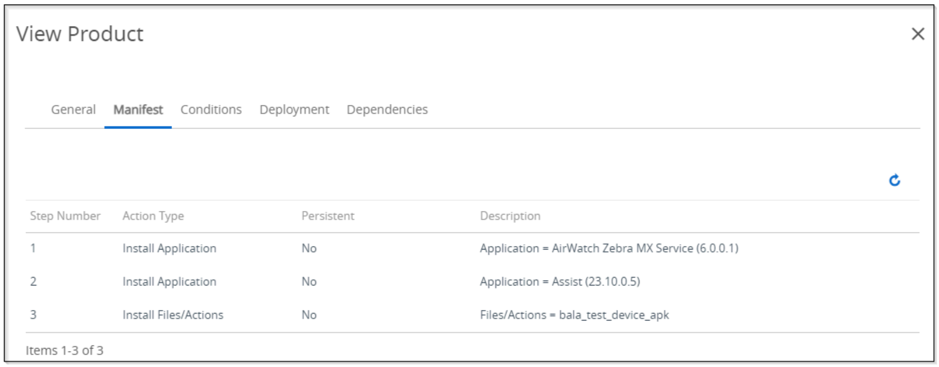
Smart Groups Start typing to add a group

Assignment Rules

4. Navigate to **Manifest** and click **Add**.



5. Add the following **Action Type** listed in the **Manifest** tab.



Step Number	Action Type	Persistent	Description
1	Install Application	No	Application = AirWatch Zebra MX Service (6.0.0.1)
2	Install Application	No	Application = Assist (23.10.0.5)
3	Install Files/Actions	No	Files/Actions = bala_test_device_apk

Items 1-3 of 3

NOTE: Do not add anything in Conditions, Deployment, or Dependencies.

The product is activated with Identity Guardian (IG) installed first, followed by the Zebra Access Management System (ZAMS) APK.

Software Updates

ZAMS software undergoes continuous updates to enhance the software and introduce new features. Therefore, it is necessary to update the APKs on the KIOSK and mobile devices.

ZAMS can always be updated to replace the existing APKs in the KIOSK or mobile device by using any installation methods described in this guide.

After updating the ZAMS software in the KIOSK or mobile devices, it is not required to register Cabinet or mobile computer again.

Uninstallation

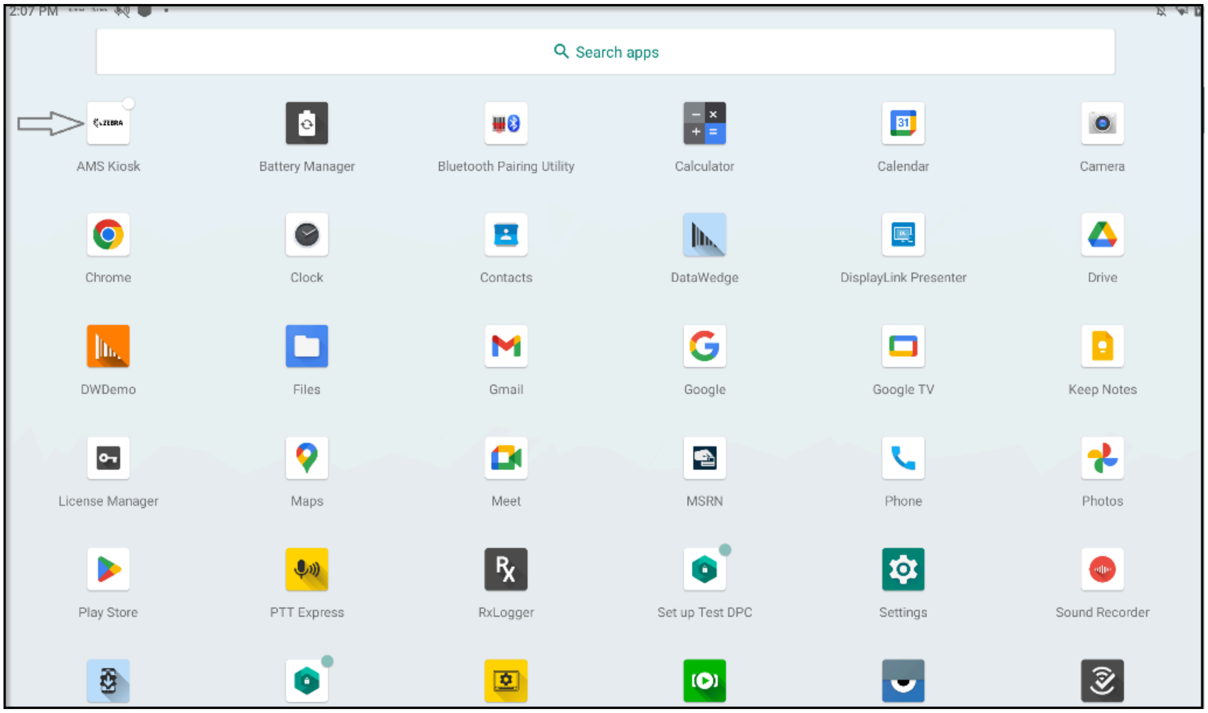
Uninstall the ZAMS software on the KIOSK or mobile device manually when the software is not required.

NOTE: Uninstalling ZAMS using the Mobile Device Managers (MDM) or other applications may require separate procedures from the following sections.

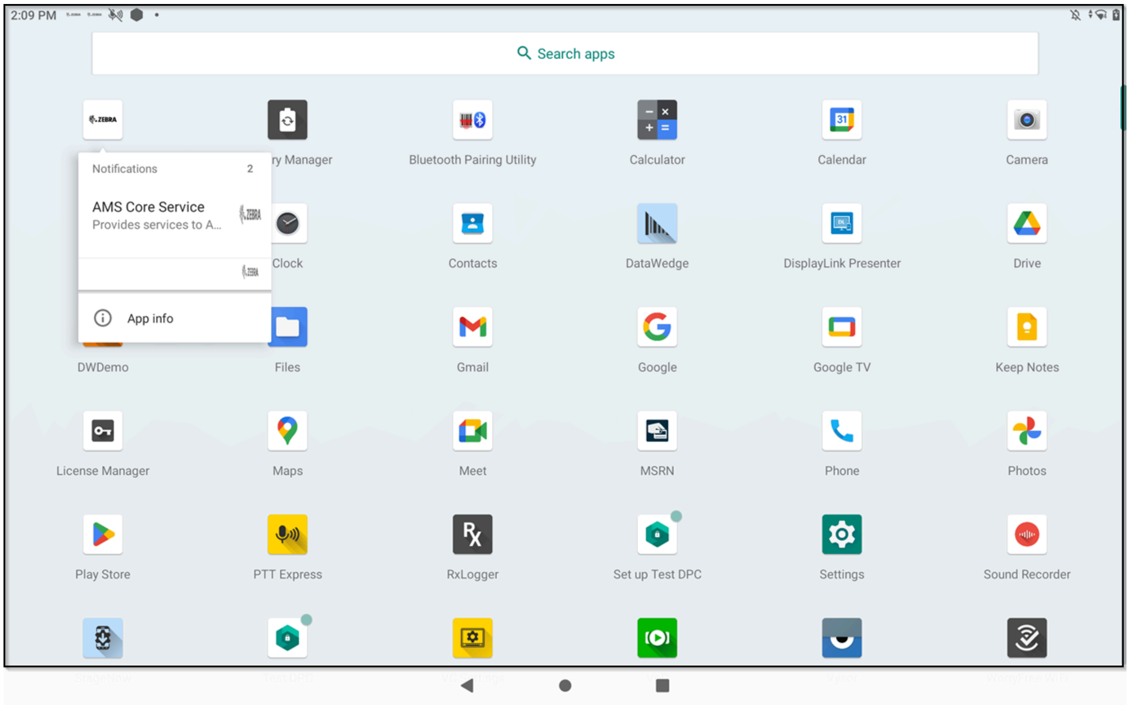
Uninstalling the APKs in the KIOSK

To uninstall the ZAMS APKs in the KIOSK, remove both the **AMS KIOSK** application.

1. Locate the **AMS KIOSK** application in the application menu.



2. Press and hold the **AMS KIOSK** application.

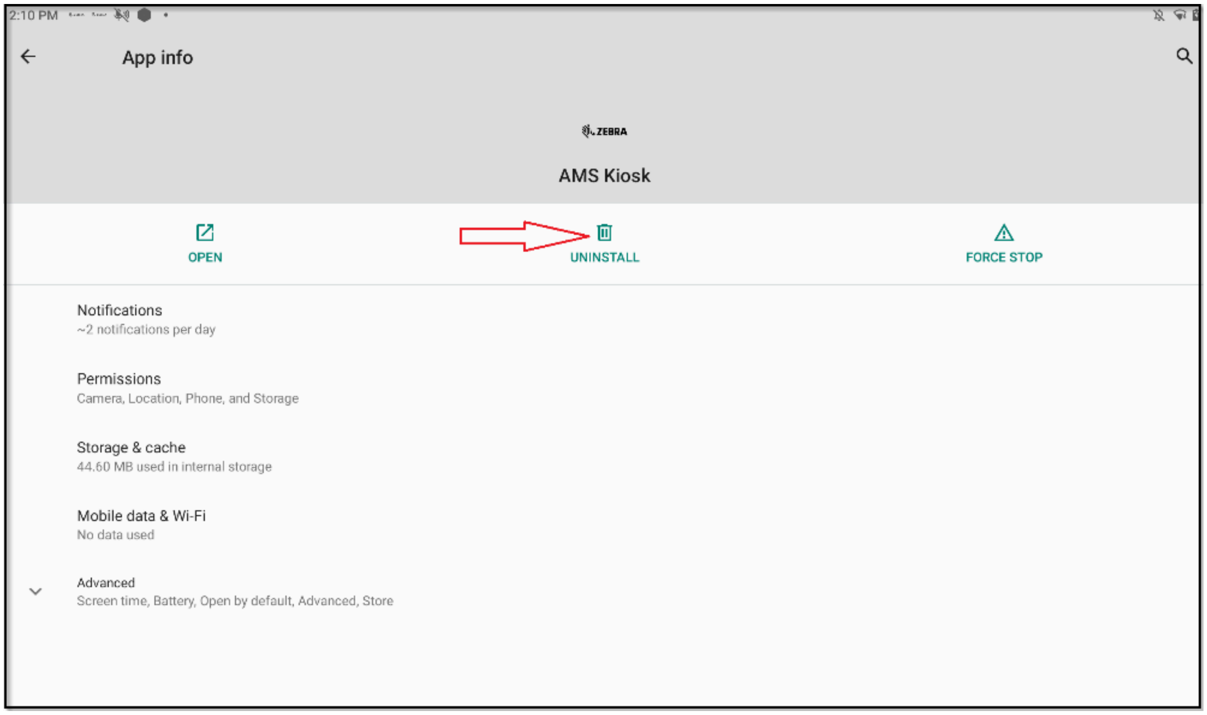


An **App info** dialogue box displays.

3. Touch **App info**.

   The **App info** screen displays.

4. On the **App info** screen, touch **UNINSTALL**.



Notifications
~2 notifications per day

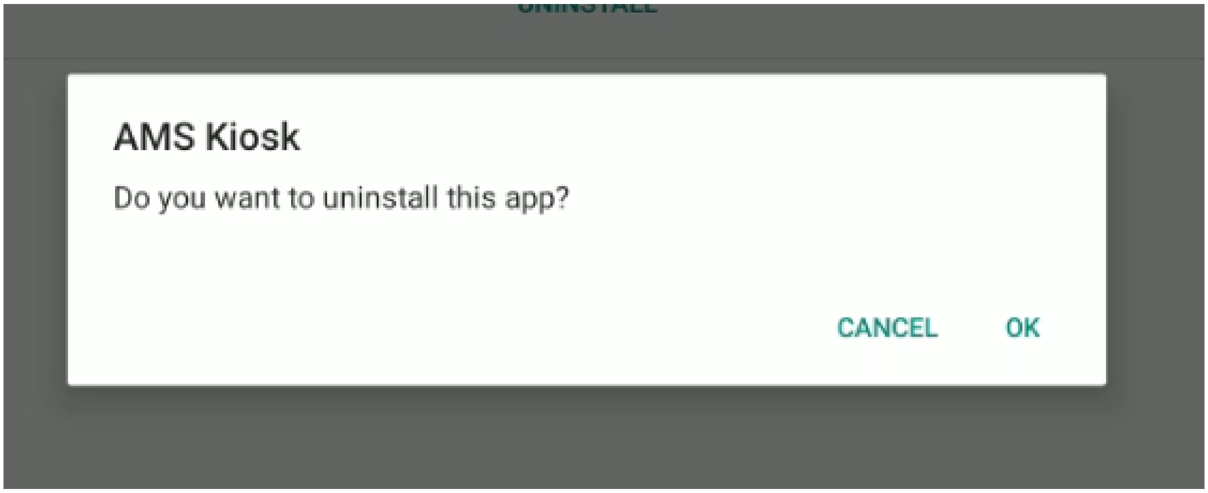
Permissions
Camera, Location, Phone, and Storage

Storage & cache
44.60 MB used in internal storage

Mobile data & Wi-Fi
No data used

Advanced
Screen time, Battery, Open by default, Advanced, Store

5. On the confirmation dialog box, touch **OK**.



AMS Kiosk

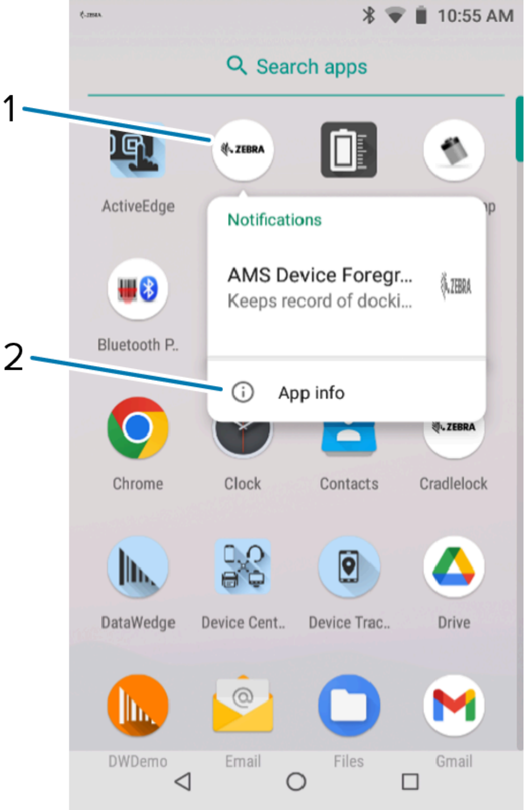
Do you want to uninstall this app?

The **AMS KIOSK** application no longer displays in the application menu.

Uninstalling the APKs in the Mobile Device

To uninstall the ZAMS APKs in the mobile device, remove the **AMS Device** application.

1. Locate the **AMS Device** (1) application in the application menu, and then press and hold the icon.



Notifications

AMS Device Foregr...
Keeps record of docki...

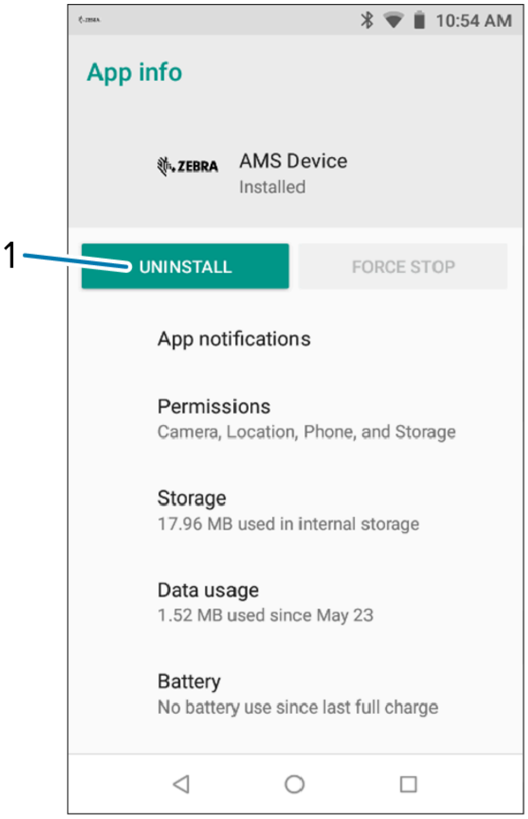
App info

An **App info** (2) dialogue box displays.

2. Touch **App info** (2).

   The **App info** screen displays.

3. On the **App info** screen, touch **UNINSTALL** (1).



AMS Device
Installed

App notifications

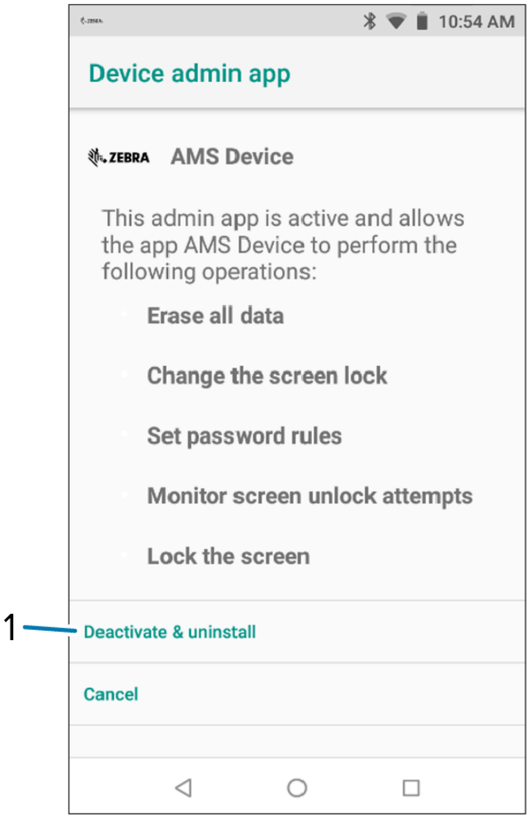
Permissions
Camera, Location, Phone, and Storage

Storage
17.96 MB used in internal storage

Data usage
1.52 MB used since May 23

Battery
No battery use since last full charge

4. On the **Device admin app** screen, touch **Deactivate & uninstall** (1).



10:54 AM

Device admin app

AMS Device

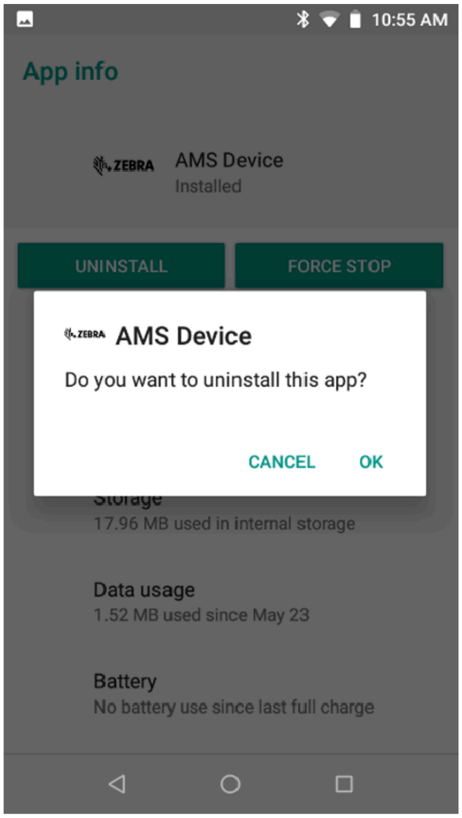
This admin app is active and allows the app AMS Device to perform the following operations:

- Erase all data
- Change the screen lock
- Set password rules
- Monitor screen unlock attempts
- Lock the screen

Deactivate & uninstall

Cancel

5. On the confirmation dialog box, touch **OK**.



10:55 AM

App info

AMS Device
Installed

AMS Device

Do you want to uninstall this app?

Storage
17.96 MB used in internal storage

Data usage
1.52 MB used since May 23

Battery
No battery use since last full charge

The **AMS Device** application no longer displays in the application menu.

Glossary

Refer to this list of terms and definitions when installing ZAMs software on the KIOSK and mobile devices.

Term	Description
`AmsKiosk.apk`	An APK file of the ZAMS KIOSK must run on the KIOSK to enable the KIOSK functionality.
`AmsDevice.apk`	An APK file of the ZAMS Device must run on the mobile device to enable the core mobile device functionality.
`ZamsDeviceAutoInstall.xml`	An XML file used by the MDM to install the ZAMS Device application and DataWedge profiles on the mobile device.
`ZamsDeviceAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to manage the installation of the ZAMS Device application and DataWedge profiles on the mobile device.
`ZamsKioskAutoInstall.xml`	An XML file is used by the MDM to install the ZAMS application on the KIOSK.
`ZamsKioskAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to manage the installation of the ZAMS application on the KIOSK.
`AmsKioskInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to manage the installation of the ZAMS Core and ZAMS UI application on the KIOSK.
`Cabinet.config`	A configuration file is used during the KIOSK installation process to automatically register a Cabinet on the KIOSK.
`Cabinet-device.config`	A configuration file is used during the mobile device installation to automatically register the mobile device in the KIOSK.

Term	Description
device.config.json	The deviceconfig file includes parameters such as TxPower, ENVIRONMENTAL_FACTOR, and DistanceRange, which are used for the Bluetooth proximity feature. It is important to note that measuring distance with RSSI values over Bluetooth Low Energy (BLE) may be inaccurate. Environmental interference, signal multipath, device differences, RSSI fluctuations, and calibration can all affect the accuracy of the measurements. The deviceconfig file provides default configuration values. However, if users encounter issues with the Bluetooth Proximity functionality or if environmental conditions require adjustments, they can modify these values in the deviceconfig file located in the download folder. isSSOConfigured: This is used when SSO needs to be enabled on the device.
DataWedge	
dwprofile_AmsDevice.db	A DataWedge profile is used by the mobile device to enable barcode scanning functionality to manually register a mobile device in the KIOSK.
Dwprofile_amsPin.db	A DataWedge profile is used by the mobile device to enable barcode scanning functionality to enter a PIN code by scanning a barcode.
KIOSK	An Android concierge KIOSK runs the ZAMS KIOSK applications
mac_randomisation.xml	An XML file that disables MAC randomization on a KIOSK that is running the Android 11 operating system.
Mobile device	An Android mobile device runs the ZAMS Device application.
Zebra Mobility DNA (MX)	An additional enterprise-class security and management function layer for Android devices.
StageNow	An Android and Windows Desktop application that can perform automated application and service installation into the device by scanning barcodes.
ZAMS	Zebra Access Management System
ZamsDeviceA10Permission.xml	An XML file to use to enable certain permissions on mobile devices with the Android 10 operating system during the ZAMS installation process.

Term	Description
`ZamsDeviceA11Permission.xml`	An XML file to use to enable certain permissions on mobile devices with the Android 11 operating system during the ZAMS installation process.
`ZamsDeviceAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to automatically install the ZAMS Device on the mobile device. For Android OS below 13 only.
`A13_ZamsDeviceAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to automatically install the ZAMS Device on the mobile device. For Android 13 only.
`ZamsKioskA10Permission.xml`	An XML file to use to enable certain permissions on the s with the Android 10 operating system during the ZAMS installation process.
`ZamsKioskA11Permission.xml`	An XML file to use to enable certain permissions on the s with the Android 11 operating system during the ZAMS installation process.
`ZamsKioskAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to automatically install AMS KIOSK on the device. For Android OS below 13 only.
`A13_ZamsKioskAutoInstall.zip`	A zipped file containing the StageNow profile that can be imported into the StageNow administrator tool to automatically install AMS on the device. For Android 13 only.