ZAMS Release Notes: 23.4.0

1. Introduction

This document outlines the new features and changes since the last release of Zebra Access Management System (ZAMS) software.

ZAMS software comprises 3 elements recommended to be installed at the same time. For current release validation and support are limited to the underlying version configurations noted.

ZAMS Software elements contain:

Mobile Device application and services: Provides the lock screen UI and services for the android based mobile devices.

Kiosk application and services: Provides on-site device management, UI and provides information to cloud based console. The Kiosk application is designed for Zebra's CC6000/ET40 devices.

Cloud resident console: Web portal that provides various administration level tasks and reports. The server access location is https://zams.zebra.com/

The following is an explanation of the files distributed in this release

1.1. ZAMS SW release components

The following is an explanation of the files distributed in this release:

Item	Area	Description
AMS Server (URL) https://zams.zebra.com	Portal	ZAMS (cloud) Portal
AMS Core APK	Kiosk	Core services APK for CC6000/ET40 to operate AMS
AMS UI APK	Kiosk	UI APK for CC6000/ET40 user interface
AMS Device APK	Mobile Device	APK for mobile devices in AMS application
dwprofile_AmsDevice.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application device registration
dwprofile_amsPin.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application PIN scanning
dwprofile_code128_barcode_profile.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application code128 barcode scanning

Item	Area	Description
dwprofile_nmc.db (part of auto install content)	Kiosk	DataWedge profile for AMS application to scan barcodes for non-mobile devices
ZamsAutoInstall files and directory structure. (See install doc for details)	Kiosk and Mobile Device	Supporting files and documentation used to automate installation or deploy via EMM or Stage Now and set permissions that may not exposed via the OS UI.

1.2. Version scheme

As a part of continual development and maintenance, it is highly recommended scheduled installation updates are planned for. Currently AMS releases major updates on a quarterly basis.

The versioning scheme for ZAMS software documentation is as follows:

 <yy>.<pi>.<rel#>.<patch#> where

- **<yy>** is the 2-digit year of release.

- **<pi>** is the major product increment number of the release. Typically, there are 4 major incremental releases to correspond to 4 quarterly scheduled releases.

- **<rel#>** is the incremental release number since last product increment. This number is updated to note a change to collection of release elements.

- **<patch#>** It is typically used to denote hot fixes or patches or custom changes of a release.

1.3. Target Environments

ZAMS supports the following target environments:

- All Zebra GMS and Non-GMS Android M devices and later.

- Non-Zebra Android devices support for Android M and later but does not include Zebra Value Add (ZVA) compatibility such as MX, DataWedge, StageNow, etc. This generally means the following may not be supported if the desired ZVA equivalent feature is not specifically integrated into the ZAMS application on a case-by-case basis.

  o Vendor specific scanning or API support
  o OEM specific OS restrictions (e.g., serial number and permissions setting access)

Exceptions

- Mobile devices with external power packs. Support on a case-by-case basis.

Kiosk

- CC6000 (Android O+)

- ET40 (Android 11+)

Portal UI

- Chrome desktop version 9 or later

2. Change Highlights (Release 23.4.0)

This is a major release:

2.1. Updates in this release

- AMS Server (v3.4.0)
- Kiosk AMS (Core v1.6.0, UI v1.5.0)
- Device AMS (v2.6.0)

2.2. Features

Enhanced the flexibility to set up the Pin code uniqueness at company level. The uniqueness level of the pin is determined by the value selected in the Pin Uniqueness Set At field.

Example:

- Pin Uniqueness is set to Company. If the passcode 3423 is used for Site XXX, it cannot be used for Site YYY or any Global user.
- Pin Uniqueness is set to Site. The Site Users in Site XXX and Site YYY can use the same passcode, 3423. However, Global Users cannot use the same passcode.
- Pin Uniqueness is set to Site. If the passcode 3423 is used for Global user, no other user on the Site XXX or Site YYY can use the same passcode. Additionally, the passcode 3423 cannot be used again by any other Global user.

When the Administrator changes the setting of Pin Uniqueness Set At from Company to Site or Site to Company, the passcode field will be null, and the passcode must be reset again for the devices. Suggestion to use this functionality as a time set up to avoid resetting the passcode of all devices.

Reloading/re-setting of passcodes can be done manually or through bulk user upload.

Login button is introduced to the Device screen and "Update Settings" is replaced with a gear icon.

- Gear icon functionality remains the same as "Update Settings" functionality. Gear icon will be used to scan the cradle master unlock code. Note: Log in Button functionality is limited to only log in screen.
- Arrow position in registration screen is moved from top to bottom.
- Improved the Passcode screen UI is improved with adding additional space on the screen.
- Provided auto-navigation to home screen when no activity on the Kiosk for more than 2 minutes.
- Screensaver improvement: Limited the area of floating battery icon and added Device serial number to the screensaver screen.

2.3. Bug Fixes

1. ZAMS-1627: Intelligent Cabinets ZAMs asking for manual login when Portal is down for some time.

    - Kiosk login expires every 30 days. Hence Kiosk AMS asking for login.

        - **Resolution:** Fixed this such that Kiosk will not ask for manual login unless Kiosk apk is reinstalled or upgraded or application cache or data cleared.

2. ZAMS-1793: ZAM's kiosk crashes after bulk upload of users and alias performed on ZAM's portal.

    - Kiosk crashing while syncing high volume of data from Portal. This results in device status/count mismatches between Portal and Kiosk. As Kiosk is crashing/busy in processing and saving large volume of user information (synced from Portal), sometimes it is unable to process device login request as well.

        - **Resolution:** Fixed by limiting the sync to site level and global level users.

3. ZAMS-1700: User login/logout issue & ZAMS-1418: Device app is not re-launching, when user undock the device by using master cradle unlock code and place the device back to charging.

    - When Bluetooth Proximity is enabled, to logout user, device should be within 2 meters from Kiosk. In some cases, though device is within the range, BLE api is giving wrong value (>2 meters). So, the issue.

        - Resolution: Fixed by adding a re-discover logic. Device will try to re-discover Kiosk when placed on charging.

4. ZAMS-1586: ZAMS PIN Entry Bypass.

    - Resolution: PIN screen bypass issue by relaunching the PIN screen on closing it.

5. ZAMS-1626: ZAM's portal down due to OutOfMemory Issue.

    - Resolution: Improved the ZAMS infrastructure with increasing the server size and configuration

6. ZAMS-1748: ZAM's app crashing on MC33 and MC93 model devices for A10 and A11.

    - Resolution: Resolved ZAMS app crashing issue on MC33 and MC93 model for A10 and A11 with adding additional null pointer checks.

3. Upgrade instructions

If KIOSK AMS or Device AMS is being upgraded from any of its previous versions, please follow below steps before upgrade.

1. Please press and hold on AMS Core app on the Kiosk, it will show App info window, please click on App info -> click on Storage -> click on CLEAR DATA.

2. Please press and hold on AMS UI app on the Kiosk, it will show App info window, please click on App info -> click on Storage -> click on CLEAR DATA.

4. Known Constraints and Workarounds

1. BT proximity range could be seen as inconsistent due to several factors including device limitations, BLE poll rates and RF environmental influences. Devices need to be placed within environment specific acceptable ranges to obtain consistency. It is recommended to verify proximity consistency during installation.

2. It is recommended that setting "App Login on Reboot" should be turned off while using Imprivata APP.

3. It is recommended to turn off BLE proximity while using Imprivata.

4. A Random behavior has been reported in Android 8 (Oreo) devices that Sometimes A 8 device takes long time to connect to the wifi and toast (wifi not connected) appears.

5. Bug – Scheduled Email Configuration – After the daylight-saving time came into effect There was one-hour time difference delay in the delivery of the email reported by Zebra. The work-around to resolve this issue at present is just to change the scheduled time of the Configuration by signing into the ZAMS Portal if the delivery of the Scheduled Email has been disturbed.

6. After a factory reset on the CC6000, the offline cabinet files may fail to be processed the first time if placed on the device by Stage Now. It may begin working with

   • Retry

   • Retry the profile after uninstalling the applications or relaunching the apps after clearing from the Recent apps.

7. ZAMS SSO intent known issues:

   • Login status may not update on portal when Special character is used in the username field while logging in.

   • When device is AVAILABLE, if a user log in intent is sent, the AVAILABLE status is lost and may not be recoverable. The intent must only be sent when the device is outside of the charger.

- When using the intent, the ZAMS client should be configured (via the portal) so PIN UI is not shown. In this case, if "send alarm" is sent via the port UI, there is not UI prompt so the device will alarm until the unit is placed back into the cradle.

8. Username disappearing when new Other Asset is checkout (Random Bug)

9. Based on quality of network performance and/or wifi coverage. Server updates from the kiosk may take up to a few minutes.

10. Current release and solution are limited to handle up to max of 500 users (combined as global and site level together) for all the cabinets at a site. In case, there is a requirement to have more users at site level, product needs to be enhanced.

11. Bulk-Upload functionality supports only upload of 2000 user records at a time.

5. Important Links

- [Zebra Techdocs](#) - Zebra community support
- [Developer Tools](#) - Zebra Developer support
- [Partner Portal](#) – Zebra Partner news and other support
- [Intelligent Cabinet Support and downloads](#) – Zebra support and downloads