ZAMS Release Notes

ZAMS Release Sprint-22.4.3, April 12, 2023

Contents

Introduction

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

ZAMS software is comprised of 3 elements that are recommended to be installed at the same time. Although various combinations of the software elements may work without issue, release validation and support is limited to the underlying version configurations noted.

ZAMS Software elements contain:

1. **Mobile Device application and services**: Provides the lock screen UI and services for the android based mobile devices.
2. **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.
3. **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.

ZAMS SW release components

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
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.

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#> <suffixes> 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.
- **<suffixes>** are optional text characters used to denote a branched set of changes from a baseline release. It is typically used to denote hot fixes or custom changes of a release.

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.
  - Vendor specific scanning or API support
  - 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

1 Change Highlights (Release Sprint-22.4.3)

This is a patch release.

Updates in this release

- Auto Install document.
- AMS Server (v3.2.1)
- Kiosk AMS (Core v1.4.2 and UI v1.3.0)
- Device AMS (v2.4.1)

1.1 ZAMS Server (v3.2.1)

The following changes have been made to the ZAMS server.

1.1.1 Bug Fixes

i. **ZAMS-1001: Device User can login 2 different device available in 2 different cabinets, One Device User Enabled at company configuration.**

Device associated with user, when marked as “LOST” was not dis-associated from user. This has been fixed.

1.2 Cabinet Kiosk AMS (Core v1.4.2 and UI v1.3.0)

The following changes have been made to the Kiosk.

1.2.1 Bug Fixes

i. **ZAMS-924: Single user can login into two devices while One Device User Enabled in portal.**

This issue occurs where initially “one device user” option is disabled and login to two devices with same user and then enable “one device user” option, put both the devices on charge and try to login with same user. This issue is fixed when “one device user” option is enabled it will not allow same user to login to two devices.

ii. **ZAMS-1001: Device User can login 2 different device available in 2 different cabinets, One Device User Enabled at company configuration.**

This issue occurs when “one device user” option is enabled, and same user tries to login to two different devices from different cabinets.

This issue is fixed when “one device user” option is enabled it will not allow same user to login to two devices from two different cabinets.

Known Constraints:

* If user has picked one device from one cabinet, then he must wait for minimum 1 to 2 minutes so that same user is not allowed to pick another device from another cabinet.

* By mistake if situation arises where two devices are logged in with same user when “one device user” option is enabled, in this condition we should keep both the devices on charge to get back to normal state.

* When the device is marked as Lost/RMA then it takes up to 10 minutes to release the previous user.

1.3 Device AMS (v2.4.1)

1.3.1 Bug Fixes

i. **ZAMS-802: AMS device app crashes, device (Linear scanner without camera) is allowed to use without entering the PIN.**

ZAMS device application crashes when camera icon is selected on devices with no camera, like EC30.

It has been fixed. A toast message **"The device don't have camera."** will appear on touching camera icon.

2 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. A new security certificate was released at the end of June. This resulted in a mandatory update of all ZAMS installs to v22.1 or later. Any legacy DW profiles also need to be updated. Otherwise some scanning functions will not work.
3. It is recommended that setting " App Login on Reboot" should be turned off while using Imprivata APP.
4. It is recommended to turn off BLE proximity Imprivata while using Imprivata.
5. 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.
6. 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.
7. 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
    a. Retry
    b. Retry of the profile after uninstalling the applications or relaunching them the apps after clearing from the Recent apps.
8. ZAMS SSO intent known issues:
    a. Login status may not update on portal when Special character is used in the user name field while logging in.
    b. 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.
    c. 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.
9. One user login Bug with Other asset (Login with user 1 on multiple Other Asset , Login on device 1 with user 1 , now put device 1 one charge , login on device 2 with user 1 now it shows up user is already logged in)
10. Username disappearing when new Other Asset is checkout (Random Bug)

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

12. Stagenow profiles in the installation admin sub-folder doesn't contain latest APK. APK files in each profile need to be updated by the Stagenow administrator prior to use.

3 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