ZAMS Release Notes

Version 21.2.1 September 21, 2021

Contents

Introduction 1
Version scheme 2
Target Environments 3
Change Highlights (v21.2.0) 3
Documentation 4
AMS Server (v2.0.14) 4
Cabinet Kiosk AMS (Core v0.0.47 and UI v0.0.43) 4
Device AMS (v2.1.51) 5
Known Constraints and Workarounds 5
Important Links 6
Addendum – Previous Release History 6
AMS Server (v2.14) 6
Cabinet Kiosk AMS (Core v0.0.46 and UI v0.0.42) 7
Device AMS (v2.1.50) 8
Highlights (V3.0.1) 9
AMS Server (v2.0.9) (No change) 9
Cabinet Kiosk AMS (Core v0.0.44 and UI v0.0.40) 9
Device AMS (v2.1.46) 10
Highlights (V3.0) 10
AMS Server v2.0.9-jwt 10
Cabinet AMS (Core v0.0.43 and UI v0.0.39) 11
Device AMS (v2.1.45) 12
Document Revision History 13

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 device.
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 to operate AMS
AMS UI .APK	Kiosk	UI APK for CC6000 user interface
AMS Device APK	Mobile Device	APK for mobile devices in AMS application
dwprofile_AmsDevice.db	Mobile Device	DataWedge profile for AMS application device registration
dwprofile_amsPin.db	Mobile Device	DataWedge profile for AMS application PIN scanning
ZamsAutoInstall.zip	Kiosk and Mobile Device	Supporting files and documentation used to automate installation or deploy via EMM

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 **Mobile**

Devices

- All Zebra GMS and Non-GMS Android M devices and later
- Non-Zebra Android devices Android M and later but limited to not include ○ 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+)

Portal UI

- Chrome desktop version 9 or later

Change Highlights (v21.2.0)

This is a regularly scheduled Product Increment (PI) release.

Updates in this release

- Documentation
- AMS Server (change to v2.0.14)

- Kiosk AMS (Core v0.0.47 and UI v0.0.43)
- Device AMS (v2.1.51)

Documentation

- Revamped product version scheme to better algin with incremental based release practices
- Creation of ZamsInstall.zip to provide supplemental information needed for automated installation and EMM based deployments

AMS Server (v2.0.14)

- Server was release prior to APK postings. See previous release history section in this document.
- Server updates will list portal changes on the portal itself after this release.

Cabinet Kiosk AMS (Core v0.0.47 and UI v0.0.43)

See previous release history section in this document for changes made from last posted release.

Issues Fixed

- At the time of installation issue fixed related to updating AMS Core and AMS UI from previous version.
- One user login on two cabinets within one minute issue (Repro steps > Login on device 1 on cabinet A > Login on device 2 on cabinet B Wait for two minutes and login with same pin on cabinet A Device 1).
- Invalid toast message appearing on UI screen while setting up New Cabinet, Synchronizing cabinet.
- Progress bar stuck when Synchronizing cabinet if any of the device status is not valid (null pointer exception).
- “About Cabinet” on CC6000 not showing any data after rebooting CC6000 when WIFI is disabled and enabled after few minutes.

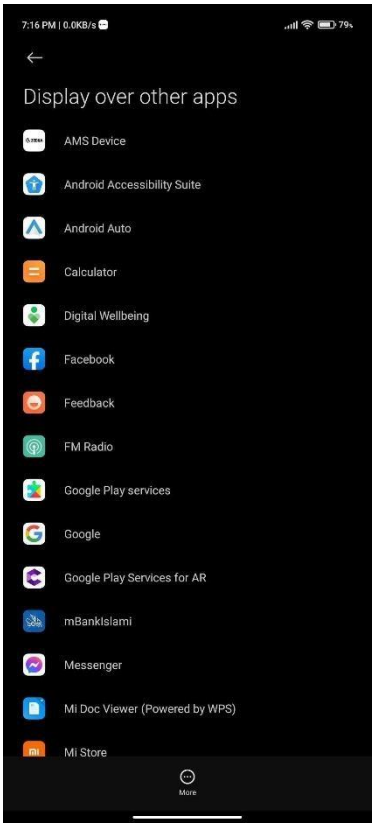
Changes:

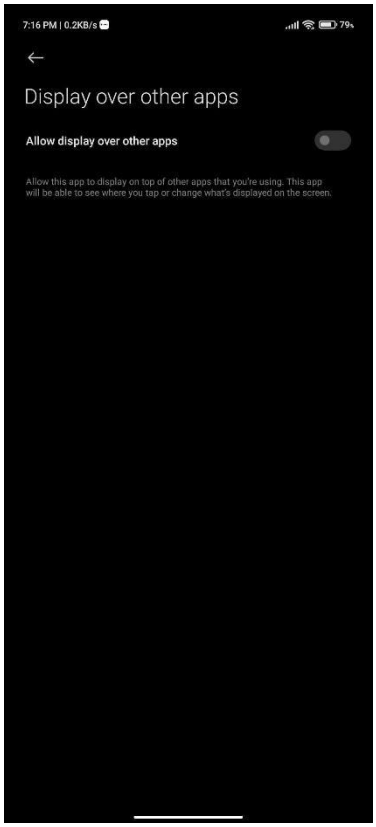
- When WIFI is connected but server is not reachable then "Unable to communicate with server" toast appears after 30 seconds, previously the toast was set to appear within “10 seconds”.

Device AMS (v2.1.51)

See previous release history section in this document for changes made from last posted release. **Issue Fixed**

- Android 10 AMS Device app not launching due to permission "allow over other apps". After granting all required permissions following pop-up will appear requiring permission for "allow over other apps". The pop up will appear only on android 10 or greater.





Known Constraints and Workarounds

1. BT proximity range could be seen as inconsistent due to several factors including device limitations and RF environmental influences.
2. Support of external chargers requires the use of BT proximity to avoid untended lockout when device is place into the external charger.
3. TC51 UV Trace integration on Android M is not supported. UV Trace is targeted for Android O and later
4. Enabling BT proximity on Android 10 devices may cause failures in the PIN screen and usage reporting. Issue is related to Android requiring new permission management for Blue tooth.

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

Addendum – Previous Release History

AMS Server (v2.14)

- Company name is preselected in all the relevant fields when the user is signed in as Company_Admin to the ZAMS Portal. The Company is preselected on the Dashboard, New Site creation form, New Cabinet creation form, Notification Configuration form and all other relevant forms.
- Cabinet Supports LAN connection, an update on Portal.
    - Under create a new Cabinet: Connectivity Method ETHERNET is added in drop down options.
- Device Login length has been set to min. 3 and max. 30 characters. Special characters other than [_ - .] not allowed. Additionally, a Device Login can't begin or end with a special character e.g. (-Steve), (Adam.) or (john_) and other such logins will not be accepted as a valid Device Login.
- Company Admin Password: Under Administration>User-Management a Company Admin is authorized to edit the password for any other Company Admin and his own password along with other credentials. Now, a single blank password field will be shown when it's desired to change credentials and password, but if User click on password field and enter a new password a confirm password field will be displayed and its mandatory if password change is intended. In case the password field is not intended to be changed the User can leave the password field blank and modify other required fields as needed this way the changes will be stored by clicking the save button without changing the password.
- Hard Delete Functionality: If Company_Admin intends to delete a Company_Admin or Device_User then all the associated Historical Data for relevant User will be deleted from the db. A confirmation message will be displayed before performing the action.
    - Note: All historical data associated with this user will be deleted.
- Master QR Code is unique for every company.
- Bulk Import CSV file related issues fixed. The new and improved version of CSV file will handle errors and exceptions reported. There are couple of major changes for the data required for respective Security Role.
    - For Device User the Device Login Field is Mandatory, whereas email filed is set to optional for Device User and any valid email entered in Email field will be stored as Contact Email.

- Changes in Device User creation form. Device Login field is set as mandatory field to be displayed as UserName on portal and Kiosk. Contact Email field is optional as compared to the previous versions of the portal where Email ID was mandatory in addition to being the default entry for User Name. The Portal & Cabinet will display Device Login in the Username field. Incase the Device Login field is empty, Email Id for the Device User will be shown as the User Name, this is only in case of an old user on portal with the Device Login field Empty.
- New Field created when creating a Site, user has the option to select the Time zone of his choice for the site.
- Alert EMAIL time stamp in local time.

Issue Fixed

- Bug Fixed HTTP (zams.zebra.com) was not automatically redirecting to HTTPS.
- Pin Code field for User Device_User was accepting letters and specials characters. Pin Code field will only accept digits as per the set rule of the company.
- Multiple Issue fixed including Historical Reports should display Username Instead of User ID.
- Bug fixed related to One User One Login RMA/BER: Device does not release the login automatically, when device goes in RMA/BER.
- Device User Deactivation Issue fixed.

Cabinet Kiosk AMS (Core v0.0.46 and UI v0.0.42)

- Added support for wired LAN connection to portal. Note mobile devices still need internal WIFI connection to the kiosk.
- Cabinet Supports LAN connection. Enables CC6000 to be able to connect over Ethernet to the internet.
    - When Ethernet is connected the Cabinet will display Connectivity Method: Ethernet under About Cabinet. ○ The Cabinet AMS UI will display two tabs under Register device a) WIFI, b) ETHERNET.
    - When Cabinet is connected via Ethernet, ETHERNET tab will be highlighted in blue and QR code will be displayed that can be used to scan and register a device to the Cabinet. ○ When Cabinet is connected via WIFI, WIFI tab will be highlighted in blue and QR code will be displayed that can be used to scan and register a device to the Cabinet.
    - If the Cabinet is connected through Ethernet via LAN and the AMS Devices are registered to the cabinet, both the Cabinet and the associated AMS Devices should be connected through same network. ○ In case a No. of devices are registered to a Cabinet having Connectivity method ETHERNET and then the Connectivity method of the Cabinet is changed to WIFI then the status of the registered devices will no longer

be updated on the Cabinet. It will be required to reregister the devices as new cabinet devices to the same cabinet scanning the WIFI QR code.

- Report version of AMS Core & AMS UI to backend.
- The CC6000 will display Device Login in the Username field. In case the Device Login field is empty, Email Id for the Device User will be shown as the User Name, this is only in case of an old user on portal with the Device Login field Empty.

Issue Fixed

- AMS UI 0.041 Crashes when (30+) devices power up at once & Connectivity method WIFI.
- Error toast appearing on new cabinet registration removed.

Device AMS (v2.1.50)

- DND prompt while setting up a new Device is removed.
- Enable physical keyboard entry for PIN code for the AMS Device to accept entry from physical keyboard in case of specific Zebra models.
- Allow AMS Device to scan QR code from the CC6000 to register the device. The Cabinet AMS UI will display two options for QR code under Register Device; a) WIFI, b) ETHERNET. The User can scan the relevant QR code displayed on the Cabinet to register the device depending on the connectivity method displayed of the Cabinet i.e., WIFI or ETHERNET.
- Screen saver added to address the potential screen burn issue.
    - Screen saver will kick off 3 minutes after the device has been put on charge and has recorded no user interaction.
    - If user presses a button, touches the screen or takes the device off charge, device will go back to the normal AMS screen.
- Master QR Code is unique for every company.
- Report version of AMS Device to backend.

Issue Fixed

- Bug fixed related One User One Login RMA/BER: Device does not release the login automatically, when device goes in RMA/BER.
- Issue with Cradle lock for KLM Demo: Flashing pattern for cradle lock Issue fixed.
- Auto Registration Failure in Android 10 devices.
- Device Battery Percentage not updating on CC6000 & Dashboard when the Device docked and on charge position. When there is percentage increase on Device no update on CC6000 & Dashboard.

Highlights (V3.0.1)

Note: The main purpose of this this release is to correct a background battery update reporting issue (#34364). Battery updates were intermittently not being made to the kiosk and portal

Updates in this release

- AMS Server (no change)
- Cabinet Kiosk AMS (Core v0.0.44 and UI v0.0.40)
- Device AMS (v2.1.46)

AMS Server (v2.0.9) (No change)

Although the server has not been updated at this time the following items will be made on an upcoming server update. **Issues Fixed**

1. ***Master QR Code*** Universal Issue Fixed. Master QR Code is unique across the companies.
2. ***Pin Code*** field for User Device Users was accepting letters and special characters. With the change, the pin field will only accept numbers.
3. Device User ***Deactivation*** Issue fixed.

Changes:

1. Alert ***EMAIL time stamp*** in local time, picked up from the Site default time zone. See new feature.
2. Changes in Device User creation form. ***Device Login*** field is set as mandatory field to be displayed as ***UserName*** on portal and Kiosk. ***Contact Email*** field is optional as compared to the previous versions of the portal where Email ID was mandatory in addition to being the default entry for Username.

New Feature:

1. New Field created when creating a Site, user selects the **Time Zone** from a drop-down list.

Cabinet Kiosk AMS (Core v0.0.44 and UI v0.0.40)

Issues Fixed

1. 34634: "Battery" and "last updated" not changing on the CC6 or the portal

New Feature:

2. Send the version number of Core & UI to the server to help support the product

Device AMS (v2.1.46)

New Features:

1. Master QR Code is unique for every company. The Master QR Code generated by super admin is Universal.
2. A **Screen saver** has been added to address the potential screen burn issue.
    a. Screen saver will kick off 3 minutes after the device has been put on charge and has recorded no user interaction
    b. If user presses a button, touches the screen or takes the device off charge, device will go back to the normal AMS screen
3. Send version number of the AMS Device to the server to help support activities

Highlights (V3.0)

AMS Server v2.0.9-jwt

1. "#" and "." are now treated as special characters in password
2. Replaces the word "character" with "letter" in password validation message for lower- and upper-case validation statements
3. "Historical Reports" have been added to the Reports Menu, which allows the company admin to view and download three types of reports. "Cabinet Devices Report", "Device Status Reports" & "User Device Report" with searchable parameters and selectable date range.
4. On new company creation the form," One Device User Enabled" field is added along with a check box
5. Bug Fixed: NOT_RETURNED Status Log not showing in Database Reporting.
6. Bug Fixed: INVALID_LOGIN Status reason not updating on Portal.
7. Password length issue – Now min 8 characters are acceptable
8. Device login issue – issue where token couldn't be renewed
9. New Feature: One User Login allowed on Device APK – Configurable
10. Historical Reporting – Latest feedback addressed
11. Added headers to the reports
12. Provide searchable Cabinet name, Device serial number and Username
13. Minor cosmetic fixes

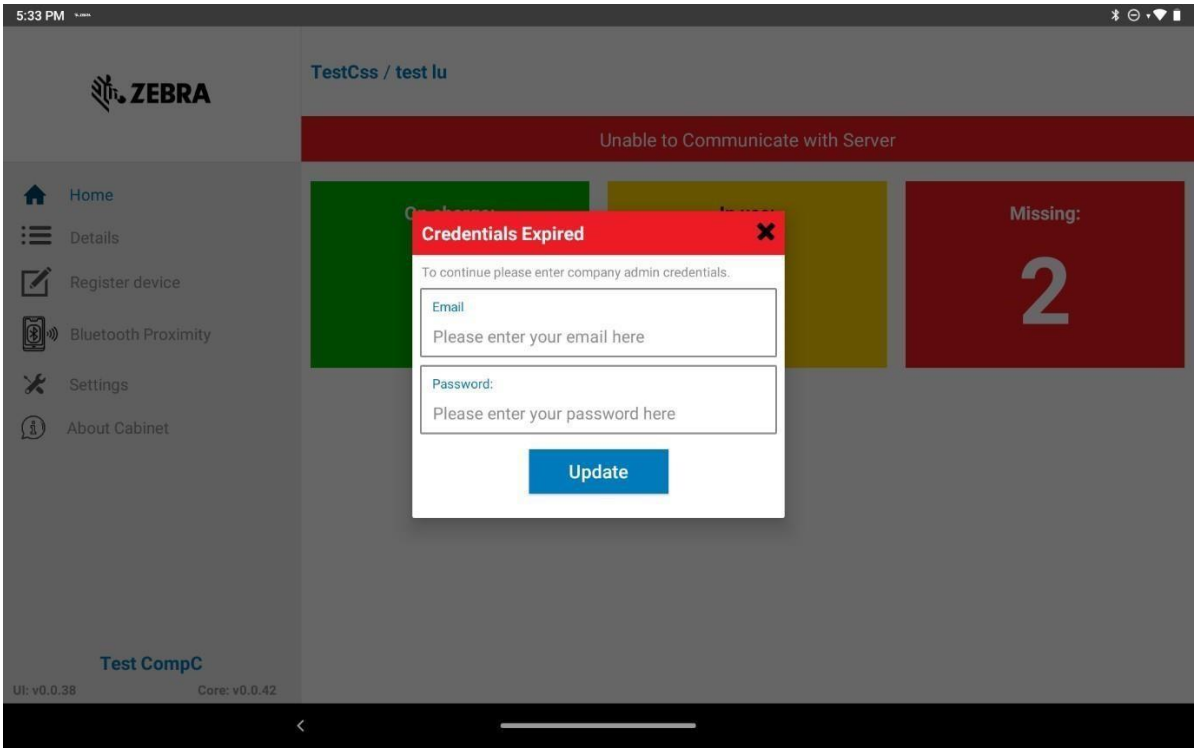
14. Constraint violation error (duplicate entry) was not showing properly.
15. On new company creation the "Alarm Enabled" and "Charging Screen Visible" fields were not checked (ticked) by default.
16. Fixed Pagination Issue under Administration.
17. Allow Hyphen in first and last name.
18. Fixed: Reset password issue under Account>Password.
19. Bugs Fixed in Entry Fields in Create New Company, Create New Site. Issue resolved where optional fields if filled and then later on kept empty were showing error.

Cabinet AMS (Core v0.0.43 and UI v0.0.39)

1. Fixed Issue: ANR issue fixed when switching between AMS UI screens (AMS UI)

Fixed Issue: Go to Details > ON_CHARGE and wait for 10 seconds, after 10 seconds only all devices currently on ON_CHARGE status will appear in the list. The devices with MISSING or IN_USE status will appear in respective list. In the Previous Versions there was a bug which was causing all the device to be listed under ON_CHARGE in the Details section after 10 sec. On the other hand the home screen use to show the accurate status and the device nos. as per respective status (AMS UI)

2. Fixed Issue: Go to Details Screen => minimize app then resume app, after repeating mentioned steps ON_CHARGE, MISSING, IN_USE tabs are added again and again every time the app is resumed after minimizing. (AMS UI)
3. CHANGE: Show permanent text "Wifi not connected" in red color on Register Device Screen when WIFI is not connected. (AMS UI)
4. CHANGE: Show permanent text "Bluetooth proximity is disabled" on Bluetooth Proximity Screen when it is disabled on portal (AMS UI)
5. Ask admin to enter credentials only if token is expired and previous admin credentials are changed or expired. (AMS UI)



6. Token renewal enhancement. (AMS Core & UI)
7. One User at a time Company level check fixed. (AMS Core)

Device AMS (v2.1.45)

1. The Device AMS v2.1.43 supports Android 10 & all other devices running lower OS versions.
2. NEW: Scan Pin Code for login and in-cradle-lock scan. Create a new DataWedge profile, add Lock activity in associated apps and under Input/output section add broadcast intent with action "com.zebra.device.pin.ACTION".
3. Fixed Issue: Bluetooth clash with UVTrace (AMS engaging when placed for sanitization using UVTrace)
4. CHANGE: If logged in using cradle lock and device is not removed from cradle for 1 minute then AMS engages on device and status is updated to ON_CHARGE on CC6000. Previously time to remove device from cradle was 10 seconds. **** amended as per documentation.
5. Flexible Screen Sizes, compatible for all devices (including EC30, TC51, TC75x and others)
6. App should not launch after reboot while Device is out of BLE range & on Charge in specific customer scenario.
7. Flashing pattern working very fast on cradle lock.
8. Master QR-code was not expiring after 48 hours.

9. When a user enters a valid pin and the device is successfully logged in, the same pin can't be used by any other user from Company to login in. Once a user enters the same pin that is already in use, a message will appear on the screen "User is already logged-in on device "1xxxxxxxxxxx9" The counter and alarm are uninterrupted will not stop unless a valid login has completed.
10. One User at a time Company level check fixed
11. AMS Device UVTRACE crash fixed

Document Revision History

Rev	Description	Date
3.0	Feature Release v3.0 (PI21.1)	4/27/21
3.0.1	Correction Release V3.0.1 Fix to Background battery update	5/19/2021
21.2.0	Scheduled posted release (PI21.2)	8/12/2021
21.2.1	Replaced DW profile for PIN scanning. Original needed a second activity added to work with cradle locks.	9/21/21