ZAMS Release Notes

ZAMS 22.1, April 2022

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 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	Part of the Auto-install files. DataWedge profile for AMS application device registration.
dwprofile_amsPin.db	Mobile Device	Part of the Auto-install files. 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 and set permissions that may not exposed via the OS UI. See Autoinstall guide in zip file for details.
mac_randomization.xml and mac_randomization_xxx.pdf	kiosk	Part of the Auto-install files. Supporting file used to turn off an OS setting via MX that randomizes the MAC address of the Wi-Fi network. Not having this option disabled impacts the static IP requirement of the kiosk The PDF file is a scannable Stage Now barcode that applies the xml file.
AmsDeviceRemove.xml and AmsDeviceRemove_xxx.pdf	device	Part of the Auto-install files. Supporting file used to ease the removal of the device APK since it is a device admin type application. The PDF file is a scannable Stage Now barcode that applies the xml file

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+)

Portal UI

- Chrome desktop version 9 or later

Change Highlights (22.1)

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

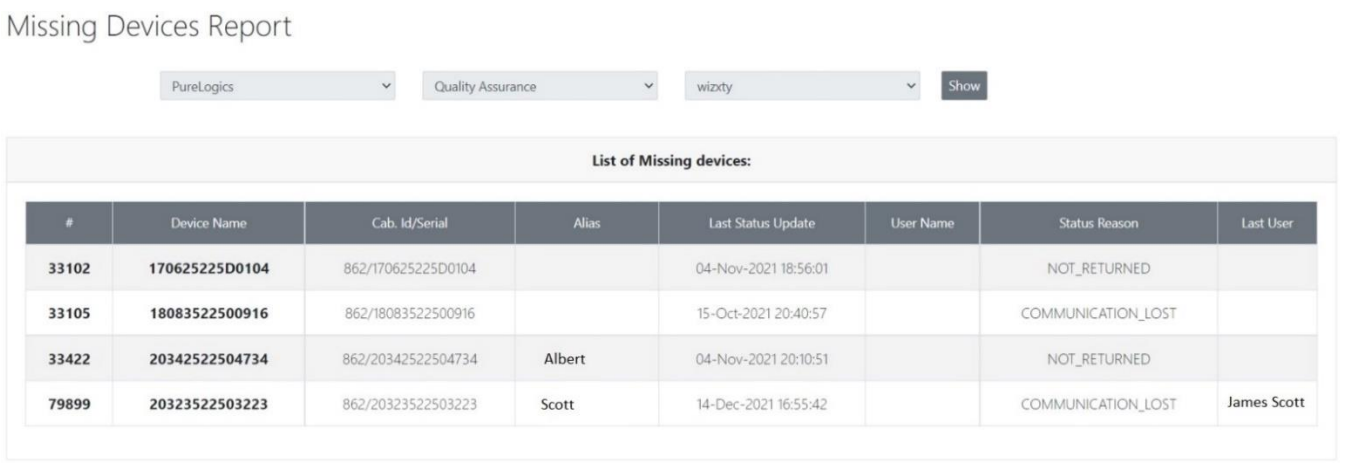
Updates in this release

- AMS Server (v3.0.14)
- Kiosk AMS (Core v1.2.3 and UI v1.1.2)
- Device AMS (v2.3.16)

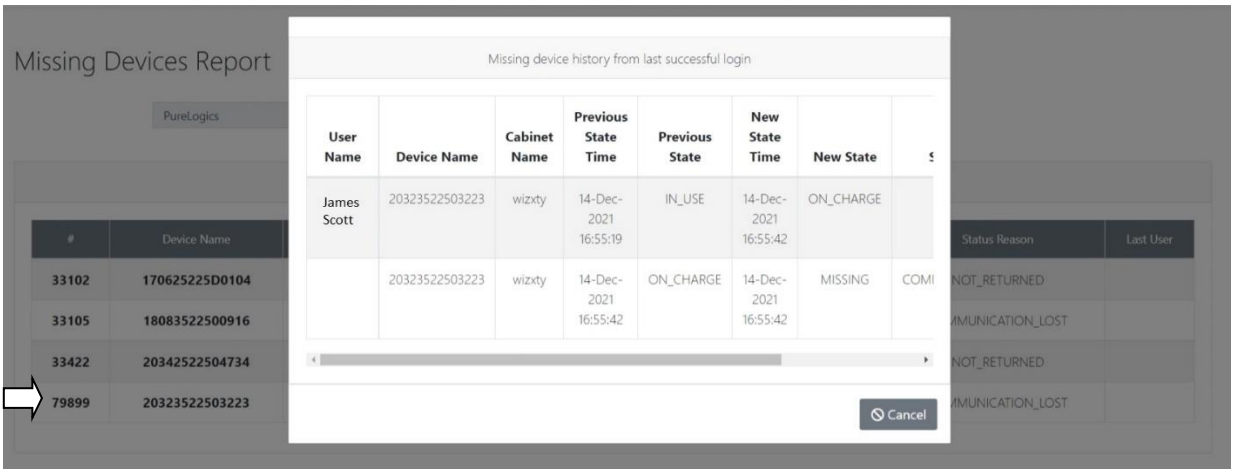
ZAMS Server (v3.0.14)

The following changes have been made to the ZAMS server (posted earlier)

1. Privacy policy URL added to the footer sections of the web pages.
2. Missing device report
   Accessible via **Reports / Missing Devices**
   Select the desired Site & Cabinet – List of missing Device will be displayed.



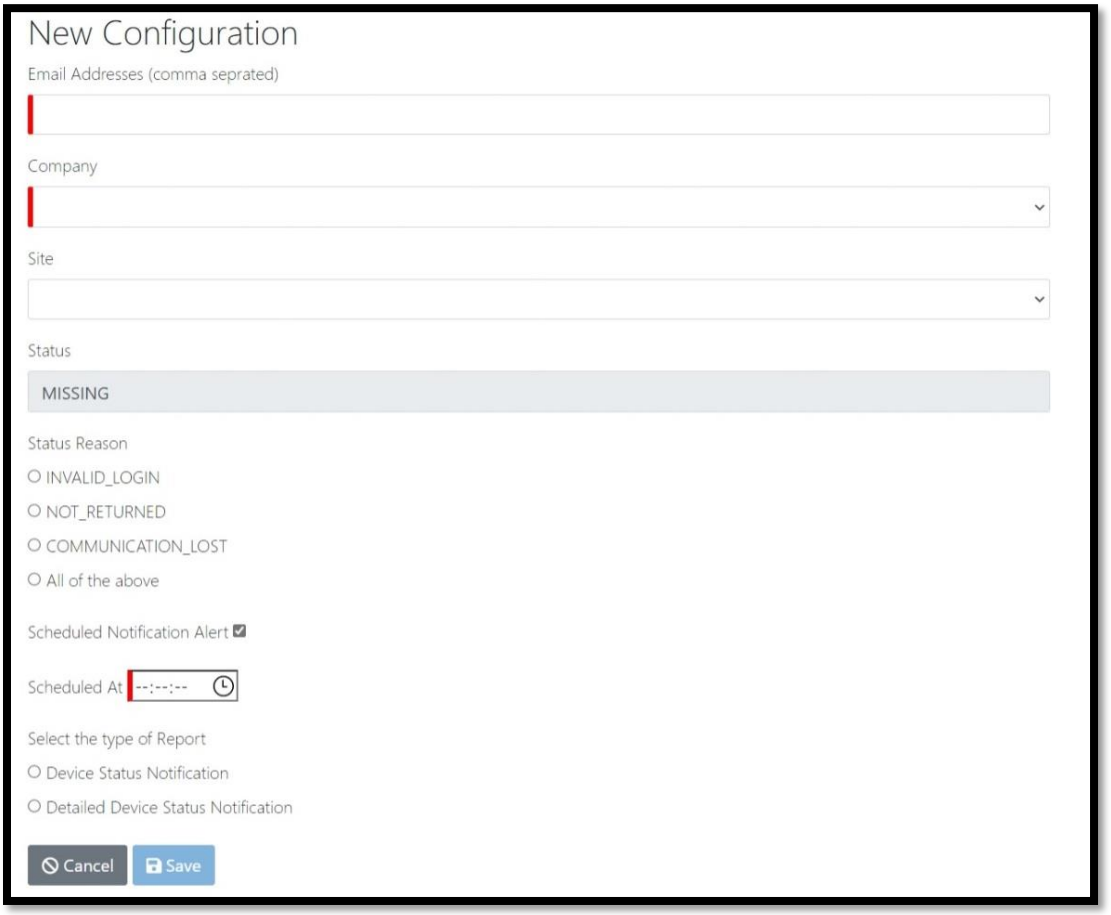
To view the detailed history for any device of selected cabinet starting from the last successful login just click on the Device Name or Serial Number. A window will pop up with detailed history of the last successful logins for that device.



3. Scheduled Notification Configuration
   Setup a scheduled notification via **Configuration / Notification-Configuration**

   a. Click on "+**Add a new Configuration**"
   b. **Enter Required Fields:**
      Email:
      Company:
      Site:
      Select Status Reason:

   c. To set Scheduled Notification: ✓ Check Scheduled Notifications Alert
      Select the desired Scheduled time
      Select the type of Report:
         Detailed Status Notification or
         Detailed Device Status Notification



Examples of the Notification Email Reports received via email.

Device Notification Report.

#	Device Name	Cab. Id/Serial	Alias	Last Update	Battery Level	UserName	Status	Status Reason	TimeZone
80188	18102522503711	998/18102522503711		28-Feb-2022 17:41:34	98	A James	MISSING	NOT_RETURNED	Europe/London

Detailed Device Notification Report.

UserName	Device Name	Cabinet Name	Previous State Time	Previous State	New State Time	New State	Status Reason	Battery Level
Ethan James	18102522503711	r3gCab01	28-Feb-2022 17:21:29	IN_USE	28-Feb-2022 17:21:29	MISSING		98
	18102522503711	r3gCab01	28-Feb-2022 17:21:29	MISSING	28-Feb-2022 17:24:52	ON_CHARGE		98
	18102522503711	r3gCab01	28-Feb-2022 17:24:52	ON_CHARGE	28-Feb-2022 17:32:42	MISSING	COMMUNICATION_LOST	98

Cabinet Kiosk AMS (Core v1.2.3 and UI v1.1.2)

The following changes have been made to the ZAMS kiosk software.

1. A mandatory and critical update to replace a soon to be expiring security token. Kiosks not updated with the new kiosk core APK will fail in June 2022.

2. Support for Android 11 (A11) Kiosk OS installs has been added. Note the following:

   a. ZAMS Kiosk APKS must be AMS Core v1.1.7 & AMS UI v1.1.2. or later. The same APKs can run on earlier device OS versions.

      The following should be noted when updating from older installations

      (1) When upgrading from some older versions of the kiosk, the currently installed devices to no longer authenticate. It is recommended to update both the kiosk and devices at the same time. The device APKs may not work until they are updated

      (2) To ease with the removal and replace method of update, this release contains an MX XML file and corresponding stage now barcode to remove the device apks. Since the device apks were installed with device admin level access, they need an MX setting in place to be removed.

      (3) There have been changes made to the Data Wedge (DW) profiles over the past year. New DW profiles should be installed. If using custom DW profiles, the standard profiles packaged with ZAMS should be edited with changes.

      Even without custom changes, the update of ZAMS needs to include the new DW profiles for the APKs to work properly.

   b. By default, Android 11 defaults to a MAC randomization setting which means that a static IP reservation in a network will no longer work. Therefore, off MAC address randomization should be turned off prior to installing ZAMS.

      A sample Zebra MX setting file has been provided with the release along with a Stage Now barcode that be can be used to configure the setting. The following URL documents the setting in more detail.
      https://techdocs.zebra.com/mx/wifi/#mac-randomization-enabledisable

   c. When applying XML and device settings via an automated process, it is possible there could be some delay or conditions that need to be before the application software can consume the changes. Therefore, it is recommended to either reboot the device or the application after installation to ensure the proper integration of new settings.

Device AMS (v2.3.16)

The following changes have been made ZAMS device software:

1. Support for A11 Device OS installs added
   AMS Device APKS must v2.3.16 or later for A11 installed devices. The same APKs can run on earlier device OS versions.

2. Bug Fixed: On A10 devices, the serial number does not show on the charge screen when the device first boots in cradle.

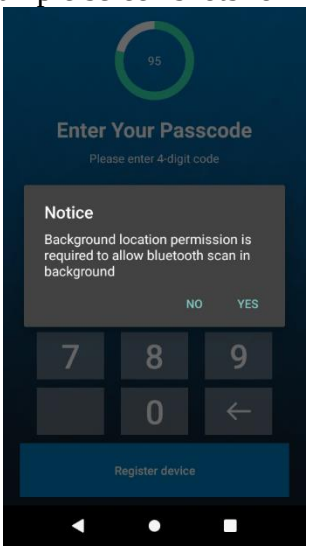
3. Update of datawedge profile "dwprofile_amsPin.db" to support QR Code scanning of Pin and Swap user features (described later in this document).

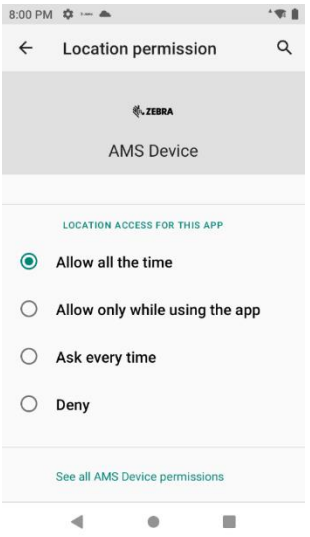
   See notes in the kiosk section about updated installation of the DW profiles.

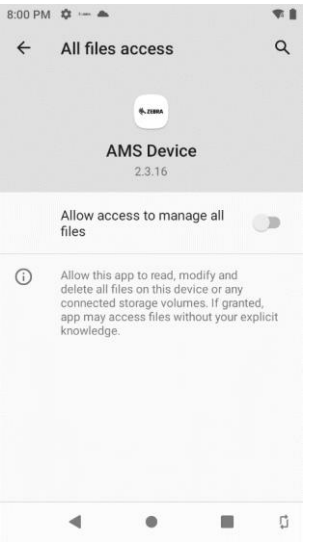
4. The following new permissions settings were added and will cause a prompt on Manual Installations. XML files has been updated to the auto-install contents

   a. Background Location permission
   b. Application File access

   Sample screen shots for manual installation below:







5. Added Ability to Swap user (logging IN/Out of AMS) without the need of Cradle:
   This functionality allows an active user to Log out of the AMS and pass on the device to another user without returning the device to the Cradle. This functionality allows the next user to enter his valid pin to login in.
   By following the simple steps this functionality can be used running the latest AMS Device APK.
   a. A user undocks a Device from the cradle and Logs in using his valid credentials.
   b. The Device is assigned to the user and the particular device will be displayed as IN_USE as standard behavior.

   c. At any point during the shift time or after the sift ends if the user wants to pass the device to another user, then the user has to simply press of the AMS Device Icon. Pressing the AMS Device Icon the AMS Device a new Pin Screen will launch as given below.

The screen displays the Device Login of the current user logged in.

d. At this point a new user, can enter their credentials and the particular device will be assigned to them.

   If home button is pressed to minimize this screen the screen will pop-up again after few seconds. Therefore, the login screen can't be dismissed until a valid login is entered or the device is returned to cabinet.

   *Note: The device needs to be connected to the Kiosk in order for a log in to occur.

6. Added support for Zebra Partner Imprivata's SDK implementation of Single Sign On (SSO). Imprivata is a common SSO provider in healthcare. When Imprivata is in installed, ZAMS screens are managed by the Imprivata client application. See appendix for additional reference details on how the SDK integration works.

   a. The setting " App Login on Reboot" should be turned off while using Imprivata APP. Otherwise ZAMS log in screens could be hidden or confuse a user.

   b. It is recommended BLE proximity alarm should be turned off since healthcare workers may not understand the feature, need increased distance before logging in or can have noisy BT environments that could potentially impact performance.

Appendix 1: Imprivata and ZAMS reference information

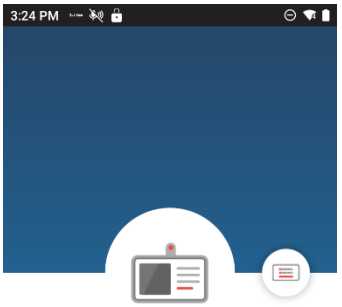
The following are some key notes on the ZAMS and Imprivata feature integration requirements

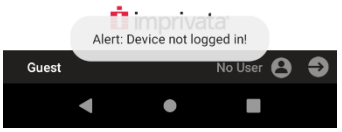
MDM Note:

1.MDM will be managing the Kiosk and devices.

2. If Zebra EHS (Enterprise Home Screen) or MDM Launcher is used, it must be configured to allow both the ZAMS app and the Imprivata app to pop up over the launcher as needed.

ZAMS/Imprivata Workflow: Device In Cradle:





1. ZAMS notifies Imprivata that user returned device to cradle.
2. Imprivata logs off user, then notifies ZAMS when logoff complete.
3. ZAMS Kiosk and Portal show device "On Charge"
4. ZAMS charge screen/screensaver is shown on device.
5. If the ZAMs charge screen is dismissed (home button pressed for instance), it will pop back up after a set time, but this is not intended to lock the device down. MDM Launcher or Zebra EHS can be used to block unauthorized access to the device.

    If ZAMS lock screen is minimized by pressing home button then the ZAMS lock screen should reengage (pop-up) automatically after a configurable time 30, 60, 90 or 120 seconds. The timing is configurable at site level.

Device out of Cradle:

1. ZAMS kiosk and portal shows device as "Missing"

2. Imprivata screen is shown. User must log in to get past Imprivata screen

3. If user does not login, ZAMS app on the device will sound alarm on device after a timer expires (ex 2 minutes).

4. A toast message “Alert Device not logged in!” will pop-up on the screen once device is taken out of the cradle.

5. If user has still not logged in within 5 minutes, device moves to "Missing/Invalid Login" in ZAMS kiosk and portal and email will be sent by ZAMS if configured to do that.

6. Once user logs in to Imprivata:

a. ZAMS alarm on device will stop if it was sounding

b. ZAMS alarm timer on device will stop

c. ZAMS kiosk and portal will show device "In Use" by the user who was passed from the Imprivata app to the ZAMS app on the device.

d. ZAMS shift duration timer starts. (configurable duration)

e. If device does not come back at end of shift, device moves to "Missing/Not Returned" in ZAMS kiosk and portal (showing user who last logged in), email will be sent (if configured)

f. At end of shift, user puts device in cradle (see above "Device In Cradle" section)

7. Optionally, user can pass device that they are using to another user without returning to cabinet.

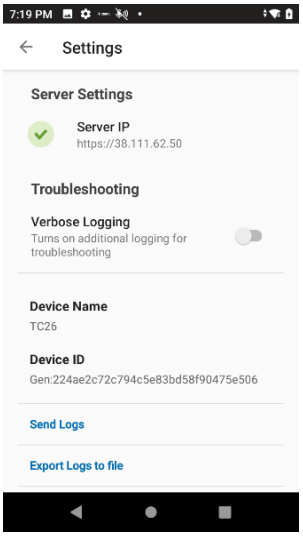
a. New user will log in to the Imprivata app

b. Imprivata notifies ZAMS that user has returned the device. Imprivata notifies ZAMS of the new user.

c. ZAMS kiosk and portal will show the device "In Use" associated to the new user and restart the shift duration timer.

d. If the new user login fails for some reason, ZAMS will continue to show the device associated to the previous user.

Setting up Imprivata APP.



1. Server IP (shared by Imprivata) Must be entered in the Settings. To enter to the settings Menu tap on the Imprivata Home screen repeatedly until the Settings window opens.

Known Constraints and Workarounds

1. A Random behavior has been reported in Android 8 (Oreo) devices that Sometimes A 8 device takes long time to connect to the Wi-Fi and toast (Wi-Fi not connected) appears.
2. It's recommended BLE proximity is turned off if not understood. Customers that are like to move away from the cabinet before logging in may see this as an issue especially in noisy BT environments.

   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.

3. A new DW profile was added in v2.3.16 to support QR code scanning on Pin Activity and User Swap. If DW is not updated these features will not work as designed.
4. The XML settings in the sample auto-install files have shown isolated cases where a setting was not in place which required a restart of the application to work correctly. When applying XML and device settings via an automated process, it is possible there could be some delay or conditions that need to be before the application software can consume the changes. Therefore, it is recommended to either reboot the device or the application after installation to ensure the proper integration of new settings.
5. The setting "App Login on Reboot" should be turned off while using Imprivata APP. Otherwise ZAMS log in screens could be hidden or confuse a user.
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 to change the scheduled time in the ZAMS Portal if the delivery of the Scheduled Email has been disturbed.
7. Bug: Missing device report details show same values for previous and new state times

8.

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