ZAMS Release Notes

ZAMS Release Sprint-23.2.0, June 29, 2023

Contents

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. Although various combinations of the software elements may work without issue, release validation and support are 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 23.2.0)

This is a major release.

Updates in this release

- AMS Server (v3.3.0)
- Kiosk AMS (Core v1.5.0 and UI v1.4.0)
- Device AMS (v2.5.0)

1.1 Features

1.1.1 Cradle Master Unlock Code

Cradle Master Unlock Code enables users to take the device out of cradle without a need to enter PIN. This is designed to use in **emergency situations**.

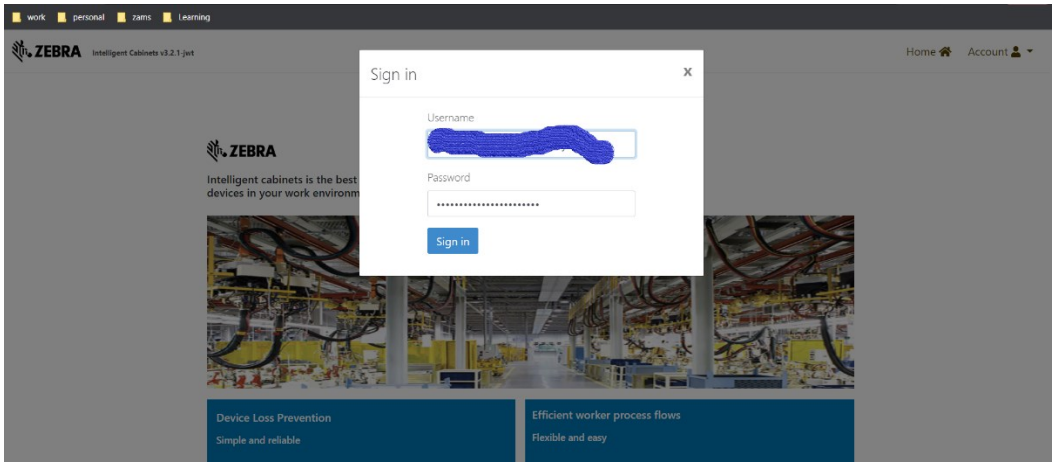
This feature helps users in situations like kiosk going into an un-responsive state for long time and not allowing the users to take device from cradle.

Users with roles ‘Company Admin/Site Admin/Company User’ can generate this unlock code from portal.

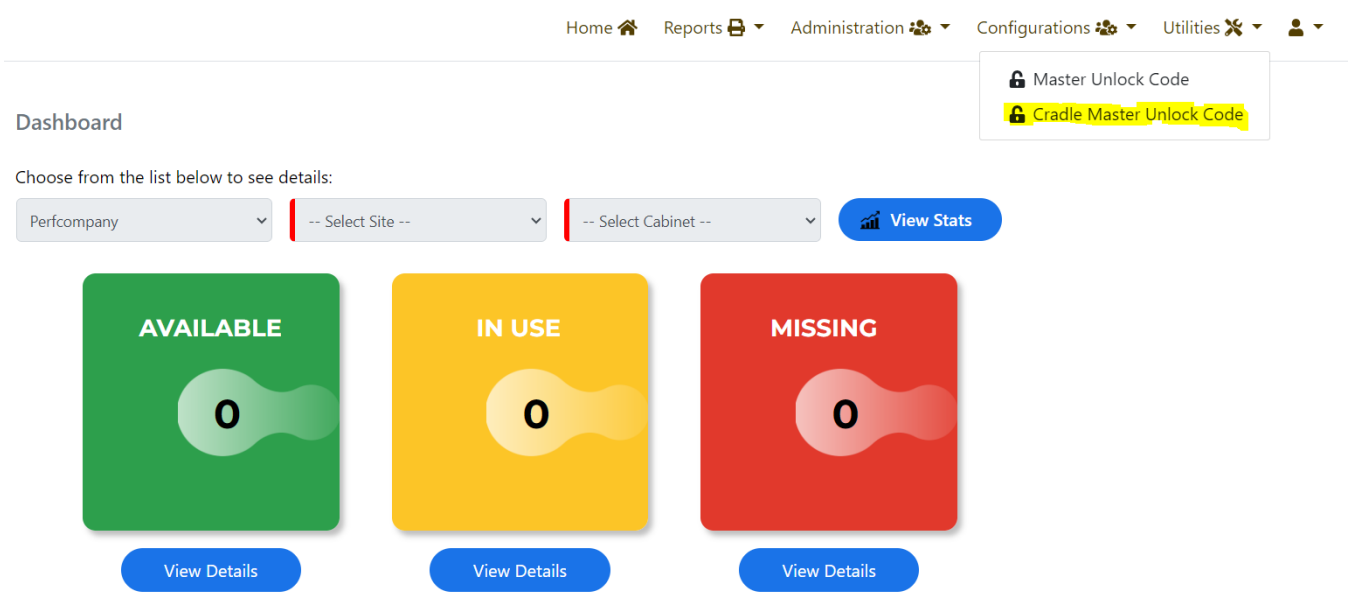
This unlock code can be downloaded and printed on to a paper and same can be used to unlock the device.

Below are the steps for generating Cradle Master Unlock Code

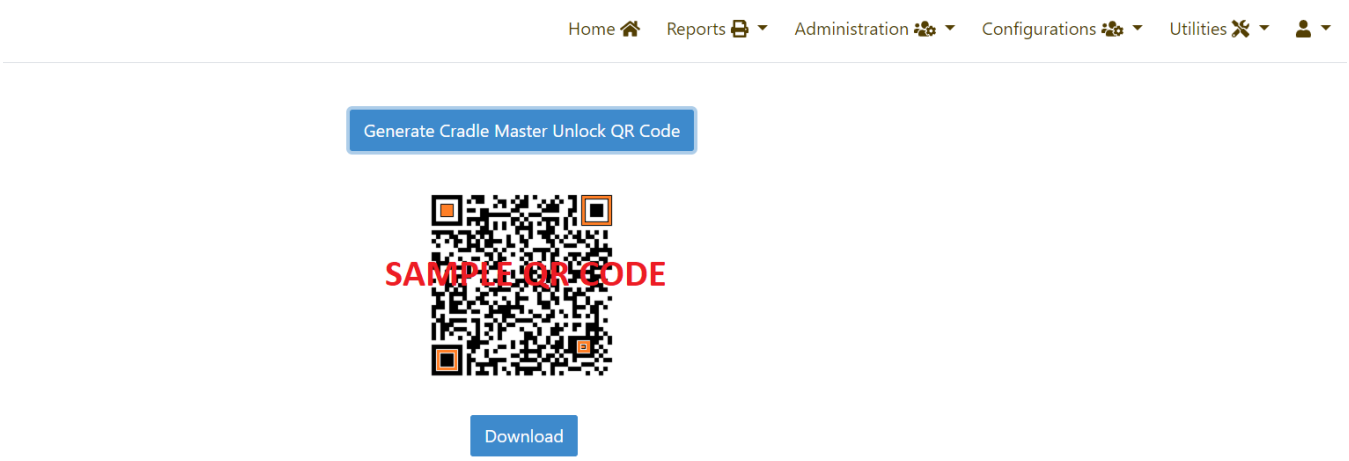
Login into ZAMS portal as a Company Admin/Site Admin/Company User



Go to Utilities and select “Cradle Master Unlock Code.”



Click on “Generate Cradle Master Unlock Code” to generate a QR code. Click on “Download” to download the QR code.

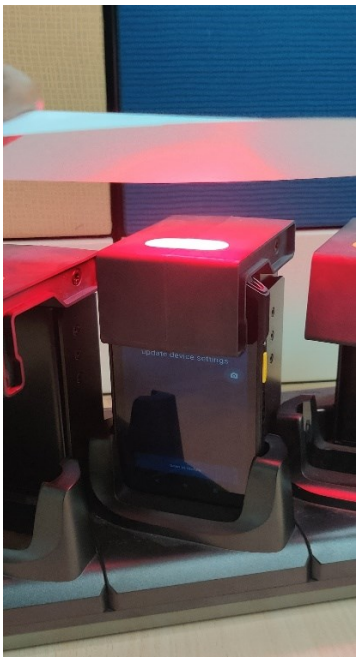


Downloaded QR code can be printed on a paper.

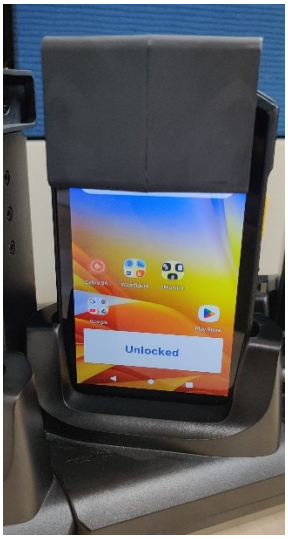
To unlock the device from Cradle, select “update settings” from charging screen as shown in the picture.

On “update settings” page select “scan to update” button as shown in the picture. Device starts scanner beam.

Place the QR code, printed on the paper, just above the device slot of cradle.



On successful scanning of the QR code, Device gets unlocked.



1.2 Bug Fixes

1.2.1 AMS Server v3.3.0

i. User not able to create a Site Name that was already created by another company.

This issue has been fixed in Portal version 3.3.0. Now the site name is made as a unique only within the company.

For Example, company A and company B can create a site with same name. But **no** company can create multiple sites, that belongs to same company, with same name. Site name is made unique within the company namespace only.

ii. NMC/MC device alias name is getting updated with cab id/asset id whenever device is marked as LOST/RMA from portal.

Asset id is getting appended with Alias name whenever device is marked as LOST/RMA.
This issue has been fixed by not appending the asset id.

iii. ZAM's portal down and customers are not able to login in Production / Performance Issues on Portal with 502 Bad Gateway Error

ZAMS portal has bee migrated to Google Cloud Platform and enabled high availability and health checks. This will bring down the frequent server failures.

iv. Typo "seprated" in Notification Configuration edit screen.

Typo “Seprated” in Notification Configuration has been fixed.

1.2.2 Kiosk AMS (Core v1.5.0 and UI v1.4.0)

i. Multiple Kiosks to 1 Cabinet Invalid Configuration

A single cabinet can be synced with multiple Kiosks. This results in an issue where Portal Dashboard shows devices from both the Kiosks.

This issue has been fixed by not allowing a Kiosk to sync with any existing cabinet which is already synced with another Kiosk.

This has an impact on Kiosk replacement procedure. With this fix, User must follow below steps to replace any faulty Kiosk and sync with existing cabinet.

Steps to replace a faulty Kiosk with new Kiosk.

a. Company admin should either uninstall ZAMS from old/faulty Kiosk or remove old/faulty Kiosk from the network.
b. Company Admin must “un-register” the old/faulty Kiosk by pressing on “un-register” button from Cabinet page on portal.
c. Company Admin will setup new Kiosk using his/her credentials.
d. Select same site and select same Cabinet.
e. Press on sync button on to sync the New Kiosk with Cabinet

ii. Unable to login to the device with the pin for the customers HubOne and Beta-Trans S.P.A. / Kiosk failed to allow user to access device due to date format contains month in French language on the Kiosk.

This issue happens when Kiosk (CC6000/ET series tablets) is configured to run any time zone except US time zone. With this fix, kiosk can run in any time zone.

iii. Device Aliases not showing on the Kiosk and Device after updating the 22.4.1 APKs.

Previously assigned device alias names were no loner working after upgrading to latest apks.

This issue has been fixed by making necessary changes to Kiosk Core apk.

iv. Invalid Hostname error should not be generic toast message.

Kiosk is popping up invalid toast when generating “Register Device” QR code. These invalid messages are like “*Kiosk Core Service Not Running*”, “*the connection port has been changed. Please restart AMS UI.*”

This issue has been fixed. The error message has been corrected and will be displayed as follows.

If Host Name value is present in Cabinet setting in the portal, then error message:

"Failed to connect to Kiosk <host_name>"

If Host Name value is empty in Cabinet setting in the portal, then error message:

"Failed to connect to Kiosk <default host_name of kiosk>".

1.2.3 Device AMS (v2.5.0)

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

This issue was happening only on devices with no camera. On selecting camera icon on “update settings” page on device, device app crashes and allows the user to use the device with out asking for PIN.

This issue has been fixed by popping up a toast message “The device doesn’t have camera”. The app no more crashes.

ii. PIN prompt behavior not consistent for A11 during device handoff.

On device with A11, pin screen does not repeatedly pop up after a handoff if nobody logs in. This leads to security issue where user can start using the device without entering the PIN.

This issue has been fixed now and PIN screen will prompt repeatedly as the time passes by.

iii. Master Unlock bar code is not working on Linear scanner devices.

This issue has been fixed by updating the datawedge db file. Updated datawedge db file packaged along with latest device apks.

iv. Duplicate Entries in the AndriodManifest.xml file caused issues while APK's installation using MDM SOTI

If user tries to deploy AmsDevice or AmsCore, SOTI is giving an error “You have selected a file with incorrect format. Please select another .apk file, in an app policy.

Issue fixed by removing duplicate permission entries from the manifest file of AmsDevice and AmsCore.

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

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

11. 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