ZAMS Release Notes

ZAMS Release 22.2, July 2022

Contents

1 Introduction 2

1.1 Version scheme 3

1.2 Target Environments 3

2 Change Highlights (Release 22.2) 4

2.1 New Auto-install document 4

2.2 ZAMS Server (v3.0.18) 4

2.2.1 Updated security certificate 4

2.2.2 Mark Device Lost / Found 4

2.2.3 Lost and Found Reports 6

2.2.4 Send alarm (aka “Speaker Squawk”) 6

2.2.5 Auto-Alarm 8

2.2.6 User and Admin role changes 8

2.2.7 User Management Page 10

2.2.8 Import Bulk Users Page 10

2.2.9 Export All Users 11

2.2.10 Delete Multiple Users 11

2.2.11 Configurations 11

2.2.12 Changes to battery level update 12

2.2.13 Bugs Fixed: 12

2.3 Cabinet Kiosk AMS (Core v1.2.23 and UI v1.1.8) 12

2.3.1 New Features: 12

2.3.2 Bugs Fixed: 12

2.4 Device AMS (v2.3.50) 12

2.4.1 New Features 12

2.4.2 Bugs Fixed: 13

3 Known Constraints and Workarounds 14

4 Important Links 16

1 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 (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
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.

1.1 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

1.2 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

2 Change Highlights (Release 22.2)

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

Updates in this release

- New (Auto) install document
- AMS Server (v3.0.18)
- Kiosk AMS (Core v1.2.23 and UI v1.1.8)
- Device AMS (v2.3.50)

2.1 New Auto-install document

The ZAMS installation documentation and accompanying deployment files have been revamped to better address the various installment audiences. The new document explains the various phases of the install process, what is typically needed with more step by step details and options on how to automate.

Accompanying the document is a set of support files shipped alongside with ZAMS APKs.

2.2 ZAMS Server (v3.0.18)

The following changes have been made to the ZAMS server

2.2.1 Updated security certificate

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

2.2.2 Mark Device Lost / Found

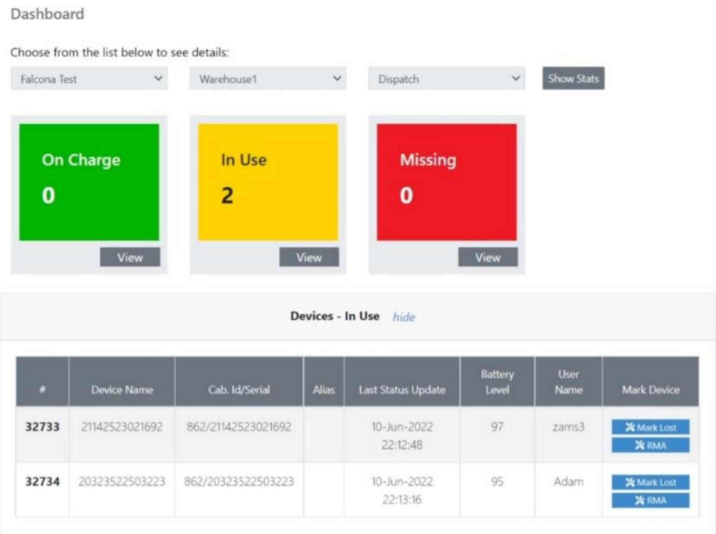
New feature has been introduced on the portal: Mark Lost & Mark Found. Marking a device lost removes it from the ZAMS active devices. Therefore, they will no longer show up as missing.

A Mobile Device can be Marked lost via the following pages

1. Dashboard/Home
2. From Cabinet Device List.

Dashboard Page: marking a device as lost

1. From the IN_Use state: Under View Mark Lost and RMA buttons Added.
2. From the Missing state: Under Missing Mark Lost and RMA tabs Added.



Dashboard

Choose from the list below to see details:

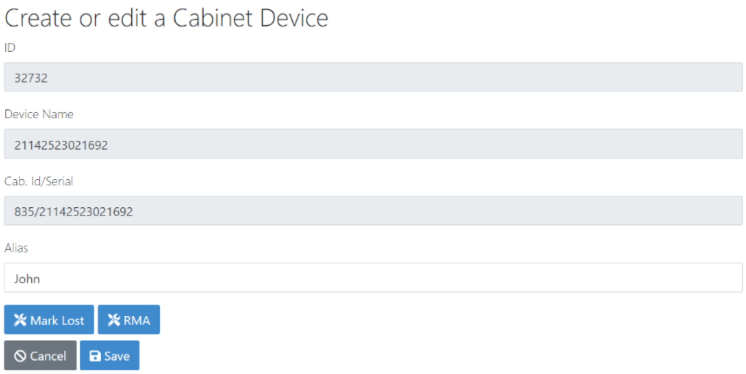
Falcona Test | Warehouse1 | Dispatch

Devices - In Use *hide*

#	Device Name	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Mark Device
32733	21142523021692	862/21142523021692		10-Jun-2022 22:12:48	97	zams3	Mark Lost RMA
32734	20323522503223	862/20323522503223		10-Jun-2022 22:13:16	95	Adam	Mark Lost RMA

From Cabinet Device List

a. Go to Administration<Cabinet Device<Search the desired Device<Click Edit.
b. In the new view after Edit is clicked click on Mark Lost.
c. The Device will disappear from Dashboard and the Kiosk in couple of minutes.
d. If Device is found at a later stage then Click Edit I Cabinet Device and mark found.
e. Note: To bring the Device back to ZAMS even if Marked Found, the Device should be put ON-Charge if its in the WIFI range of the Kiosk it was previously registered to.
f. If Found Device in not in range of the original Kiosk then it can be registered to a new Kiosk by scanning the barcode and the Device will register to the new Kiosk.



Create or edit a Cabinet Device

ID: 32732

Device Name: 21142523021692

Cab. Id/Serial: 835/21142523021692

Alias: John

In Actions column in Cabinet Devices Changes made: RMA can accessed by pressing Edit instead of view.

2.2.3 Lost and Found Reports

Two new reports added to the Reports list. These reports can be generated by a Company_Admin or Site_Admin role type of user.

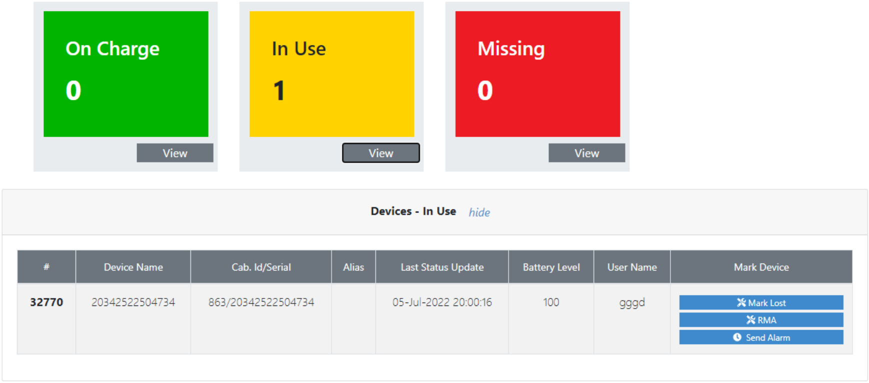
1. Lost Devices
   a. The generated Report displays all the Mobile Devices Marked Lost for the Selected Site and Kiosk/Cabinet of the Company.
2. Found Device
   a. The generated Report displays all the Mobile Devices Marked Found for the Selected Site and Kiosk/Cabinet of the Company.

2.2.4 Send alarm (aka "Speaker Squawk")

A "Send Alarm" Button has been added to the Device Column List on the Dashboard for In-use and Missing devices. The "Send Alarm" button sends an internal message to the Mobile Device (via the kiosk) to prompt for log in. If the Mobile Device is on the same network as of the Kiosk then upon successful communication the pin screen shows up on the screen and the alarm timeout starts with the ZAMS log in screen UI.

If user does not log in within the 2 mins (or configurable Alarm timeout of the Company), device alarms until:

a. Battery dead
b. User logs in by entering a valid pin
c. Device returned to charger and its in range
d. Master QR Scanned. If ZAMS UI is turned off via a configuration setting, scanning an unlock code is managed by the application presenting the UI on the mobile device.

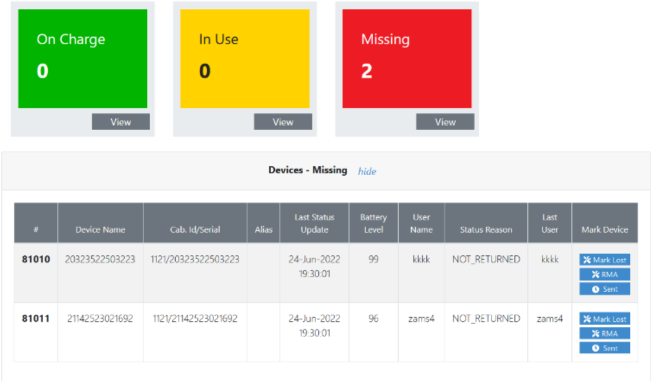


Devices - In Use

#	Device Name	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Mark Device
32770	20342522504734	863/20342522504734		05-Jul-2022 20:00:16	100	gggd	Mark Lost RMA Send Alarm

The "Send Alarm" Functionality will not be applicable to devices in the Missing State with the "*Communication_Lost"* reason type.

On the Dashboard the "Send Alarm" will change to "Sent" after being pressed. The portal will communicate with the Kiosk and the Kiosk will send the Alarm notification to the particular device. The "Sent" button will be automatically refreshed to "Send Alarm" within one minute.

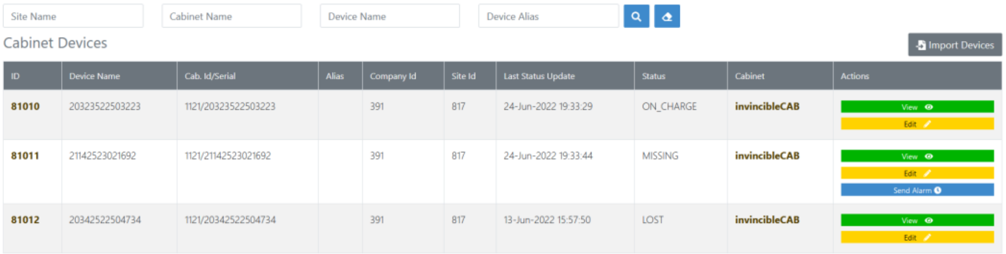


Devices - Missing

#	Device Name	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Status Reason	Last User	Mark Device
81010	20323522503223	1121/20323522503223		24-Jun-2022 19:30:01	99	kkkk	NOT_RETURNED	kkkk	Mark Lost RMA Sent
81011	21142523021692	1121/21142523021692		24-Jun-2022 19:30:01	96	zams4	NOT_RETURNED	zams4	Mark Lost RMA Sent

"Send Alarm" button is also available in Actions columns in the **Administration< Cabinet Devices** list. All the Rule are applicable as described above about the "Send Alarm". There is only one exception once the "Send Alarm" is pressed it will change to "Sent". The Portal will send a call to the Kiosk and the Kiosk will communicate with the Device. The only exception is the "sent" button will not automatically revert to "Send Alarm". Once the page is refreshed the "sent" button will change to "Send Alarm".

In the Cabinet Devices page, the status reason of missing is not mentioned.



Cabinet Devices

ID	Device Name	Cab. Id/Serial	Alias	Company Id	Site Id	Last Status Update	Status	Cabinet	Actions
81010	20323522503223	1121/20323522503223		391	817	24-Jun-2022 19:33:29	ON_CHARGE	**invincibleCAB**	View Edit
81011	21142523021692	1121/21142523021692		391	817	24-Jun-2022 19:33:44	MISSING	**invincibleCAB**	View Edit Send Alarm
81012	20342522504734	1121/20342522504734		391	817	13-Jun-2022 15:57:50	LOST	**invincibleCAB**	View Edit

2.2.5 Auto-Alarm

The latest version of Core v 1.2.23 is required to run this feature.

An "auto alarm" configuration option has been added. If enabled, missing devices will automatically sound and alarm until no longer missing.

Portal UI has a configurable setting to enable auto-alarm when device goes Missing-Not Returned after shift timeout, at Company Level.

2) A new setting added to the Company Settings page.

   ☑ Auto Alarm after Shift Timeout

3) If checked, device will alarm automatically when it is not returned to cradle after shift timeout.
4) ZAMS client on Mobile Device knows it is missing based on shift duration.
5) On Mobile Device, if shift duration has expired, log in screen come on the UI
6) If user does not log in within the 2 mins(configurable Alarm timeout), device alarms until---
   a. battery dead.
   b. user logs in.
   c. device returned to cabinet/charger and in range.
   d. Master unlock barcode is scanned. If ZAMS UI is turned off via a configuration setting, scanning an unlock code is managed by the application presenting the UI on the mobile device.

2.2.6 User and Admin role changes

Refinements to the Device_User role

There are now two types of device user roles.

1. Device_User which is associated to a particular site
   - The Device_User will have restricted access in terms to checking out a Device. Such a Device_User will only be able to check out a Mobile Device associated to the particular Site using his/her pin code. If the pin code of Device associated to a particular site is enter on a Mobile Device Associated to another site then error will be displayed "Invalid Pin"

2. Global Device_User which has no association to a particular site.

- A Device_User with the attributes Global can access any site associated to the Company. A Device_user can use his/her pin code to checkout a Mobile Device from any of the site belonging to the company.

The initial site a Device_User is associated to can be assigned at the time of creation by Site_Admin or Company_Admin. The Company_Admin has an additional right to switch Sites for a Device_User or make it Global.

Refinements to Role Site_Admin user role

1. Site_Admin Can create a new Device_User that can be only associated to his respective site.
2. At the time of creation of the Device_User the Company and Site settings are prepopulated with the site information associated with the site admin creating the user.
3. Site_Admin Can Edit/view particulars of a new Device_User which has been associated to his respective site.
4. Site_Admin Can delete a new Device_User associated to his respective site.
5. The signed in Site_Admin has authority to either view or click on “Claim” tab to associate global Device_user to the respective site of the Site_Admin.
6. Site_Admin can click on “Claim” in the “Actions” column in the User Management and associate a Device_User listed as Global in the “Site Id” column to the respective site of the site_admin who has logged in.
7. Once a Global_Device_User is associated to a Site by the logged in Site_Admin, the Site_Admin can perform any of the following action to the Device_User Associated to his Site:
    - View
    - Edit
    - Delete
8. In the User_Management table a new column is added “Site Id”. The Site Id represents the Site Id of the Site name to which a Site_Admin or a Device_User is Associated to.
9. In the “Site Id” column in the User Management, the Site Id of all the Site_Admins and Device_Users will be listed associated to the same site to which the signed in Site-Admin belongs to. If a Device_User is not associated to a site then in the “Site Id” column “Global” will be displayed.

Refinements to Role Company_Admin

1. Company_Admin can create the Device_User and has to enter the required information.
    - The company is preselected.
    - In the Site Id/Name field Global is pre populated.
    - If Global is selected then the newly created Device_User will categorized as Global_Device_User.
    - The Global Device_user will be visible to all company Admins and all the Site-Admins belonging to any of the sites associated to the same Company.

- By clicking the dop-down menu the Site a Company_Admin can select a particular Site from the list of sites.
- By choosing a site the Device_User will be associated that particular site only.

2.2.7 User Management Page

Changes made:

1. A new line of text has been added stating. **ROLE_DEVICE_USER** listed as GLOBAL in the Site Id column has access to all sites of the company.
2. New column “Site Id” added to the user table UI.
   Columns when logged in as Company Admin

Security Role	Site Id (Column)
Company_Admin	N/A
Company_User	N/A
Device User	Site Id(if the User is associated to a site) or Global
Site_Admin	Site Id

   Columns when logged in as Site Admin

Security Role	Site Id (Column)
Device User	Site Id (site of Device user) or Global
Site_Admin	Site Id

3. New Claim Button added in the Actions column. Allows user to be associated with a site if not assigned one.

2.2.8 Import Bulk Users Page

Different Bulk upload users page view for SITE_ADMIN and COMPANY_ADMIN

Logged in as Company Admin

- Changes have been made to the Bulk Import page
- Changes have been made to accommodate the Device_user related process after introduction of field Site.
- Site field for the Device_User must contain either of the two:
  a) Site Name
  If the correct name of the site Name is entered the record will be processed where all other entries are valid for that record.
- b) Global.

Global (it’s not case sensitive) should be entered in Site field for Device_User.

- If anything else is entered apart from correct site name or Global in the site field for Device_User the record will not be processed.

Logged in as Site_Admin

- A New page will be visible to Site_Admin for Bulk Import.
- Changes have been made to the main Bulk Import page.
- New CSV template for Site_Admin has been added.
- The Site_Admin can upload a CVC to ZAMS portal and has the privilege to Import new Device_users or update existing Device_Users.
- New CSV sample template for Site_Admin has been added.
- In the CSV the Correct Site Name must be entered.
- If the Site Name is incorrect or the field is left blank then the record/s containing the incorrect or blank site name will not be processed.

2.2.9 Export All Users

Signed in as Site_Admin

1. Site_Admin has the authority to use the Export All Users feature from the User Management main page. By performing this action all the Users (Site_Admins & Device_Users) associated to the assigned site of Site_Admin will be exported.
2. Note: Global Users will not be in the Exported even if they are listed.
3. Company_Admin can export all Users.

2.2.10 Delete Multiple Users

Site_Admin has the privilege to use the Delete multiple entries from the User Management main page.

2.2.11 Configurations

Site_Admin has the privilege to create the following offline configurations:

1. Offline Cabinet Setup
2. Offline Cabinet Device Setup

2.2.12 Changes to battery level update

Battery timestamp updates after every minute on Kiosk and Portal after battery level reaches 100%. Previously Timestamp updates stopped after 100% since level was not expected to change.

2.2.13 Bugs Fixed:

- Company user can deactivate other users.

  This bug was reported that If the Company_User click on the Active/Deactivate button the status of the Activate/Deactivate button does change on the UI, but there is no change at the Back end. Once the page is refreshed the status of the Activate/Deactivate button will revert back to the original state and will reflect the true status. The bug is fixed.

- Previous state time and new state time are showing same time.

2.3 Cabinet Kiosk AMS (Core v1.2.23 and UI v1.1.8)

2.3.1 New Features:

1. Changed to support new server features
   - Marking device as lost
   - Send alarm
   - Battery reporting

2.3.2 Bugs Fixed:

- Previous state time and new state time were reported to the portal as the same time.
- Exception causing Red Banner Issue.
- Date Parsing exception.

2.4 Device AMS (v2.3.50)

2.4.1 New Features

Added support for new portal features:

- Show log-in prompt when “Send Alarm” message is sent. If user does not log in, the device will alarm. See server section for more details.
- Support serve option to enable “auto alarm” when the Device goes into the Missing State. If enabled, the device will alarm automatically when it is not returned to cradle after shift timeout.

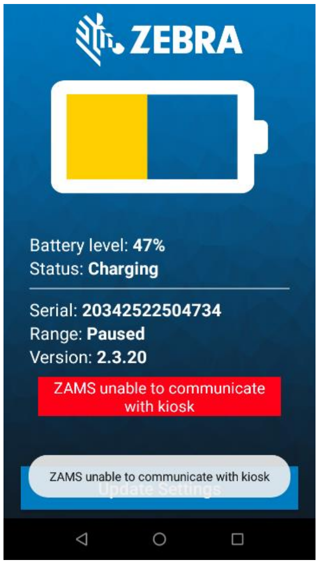
2.4.2 Bugs Fixed:

1. SSO API/intent introduced back into ZAMS standard release. This was unintentionally removed in previous releases. When an application on the mobile device acts as the login agent, it is expected to manage the UI prompt to collect the user name and password and call into the ZAMS services with the following code. Note the ZAMS portal has an option to turn off the ZAM UI to best support this feature.

   ```
   void LoginUser(){
      Intent i = new Intent();
      i.setAction("com.zebra.ams.device.action.USER_LOGIN");
      i.putExtra("EXTRA_ZAMS_USER_ID", "Smith, John 1234");
      sendBroadcast(i);
   }
   ```

   The intent must only be sent when the device is outside of the charger. See known issues. When using the intent, the ZAMS client should be configured (via the portal) so PIN UI is not shown.

2. Bluetooth Proximity not working on Android 11
3. ZamsAutoInstall fixed Issues related to Android 10 MX Install
   a. Toast Message on the AMS Device UI while its On_Charge and no connectivity with the Kiosk



Battery level: **47%**
Status: **Charging**

Serial: **20342522504734**
Range: **Paused**
Version: **2.3.20**

ZAMS unable to communicate with kiosk

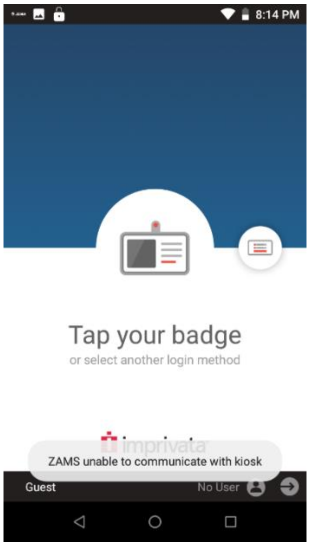
ZAMS unable to communicate with kiosk

4. Imprivata integration changes. Note Imprivata is a common SSO provider in healthcare. When Imprivata is in installed, ZAMS screens are managed by the Imprivata client.

   a. Added error toast message to reflect when "ZAMS is unable to communicate to kiosk"

In a condition that Kiosk is down due to Connectivity, power failure or connection issue with the Server the following details the workflow to expect

- The Imprivata User pickup up a device from the cradle and logs in to the device using valid Imprivata Credentials before alarm time. The user will be able to log in successfully while the alarm timeout still running in the background.
- With the new Changes in effect the after-alarm timeout runs out the alarm will not sound but a toast message will appear on the screen, if the Imprivata has successfully logged into the device before alarm time out while Kiosk is down.
- After alarm timeout runs out an Alert toast message "ZAMS unable to communicate to kiosk" will appear 4 times after every 10 seconds.
- If the Kiosk is back online after some time and Kiosk is able to communicate with the Device, The Kiosk will update the new status of the Device from ON_Charge to IN-Use and the credentials of logged in user will be updates as well on Kiosk UI and Portal.



Tap your badge

or select another login method

ZAMS unable to communicate with kiosk

b. Fixed Bug: Imprivata User does not log out when the device reboots while the initial status was IN_USE. Prior to the fix, the devices successfully were logged into Imprivata but ZAMS would alarm since it did not know user was already logged in upon bootup.

3 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 ON_CHARGE, if a user log in intent is sent, the ON_CHARGE 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 ZAMS SSO 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 portal UI, there is not UI prompt so the device will alarm until the unit is placed back into the cradle.
   d. QR code scanning to turn off the alarm is not possible if ZAMS is configured not to show the UI on the device.
9. Marking a device as lost does not free up the user if one device per user is enabled.

4 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