

ZAMS Release Notes

ZAMS Release 23.3.0, August 31, 2023

Contents

Introduction	2
Version scheme	3
Target Environments	3
1 Change Highlights (Release 23.3.0)	4
1.1 Features	4
1.1.1 New Security Role: ROLE_DEVICE_INTERNAL_USER	4
1.2 Bug Fixes	8
1.2.1 AMS Server v3.3.1	8
2 Known Constraints and Workarounds	8
3 Important Links	9

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 be 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 23.3.0)

This is a major release.

Updates in this release

- AMS Server (v3.3.1)
- Kiosk AMS (Core v1.5.1 and UI v1.4.1)
- Device AMS (v2.5.1)

1.1 Features

1.1.1 New Security Role: `ROLE_DEVICE_INTERNAL_USER`

ZAMS introducing new security role called `ROLE_DEVICE_INTERNAL_USER`.

Security roles `ROLE_DEVICE_USER` and `ROLE_DEVICE_INTERNAL_USER` have almost same privileges except that user assigned with the role `ROLE_DEVICE_INTERNAL_USER` will be able to check out MC devices from cradle even if Kiosk and Portal are not reachable/down.

As of today, a MC device can be checked out of cradle by below ways:

1. User with `ROLE_DEVICE_USER`, can enter a valid pin and unlock a MC device from cradle.
2. If Kiosk is down, Site Admin or Company Admin can generate Cradle Master Unlock Code from Portal and this QR code can be used to unlock device from cradle.

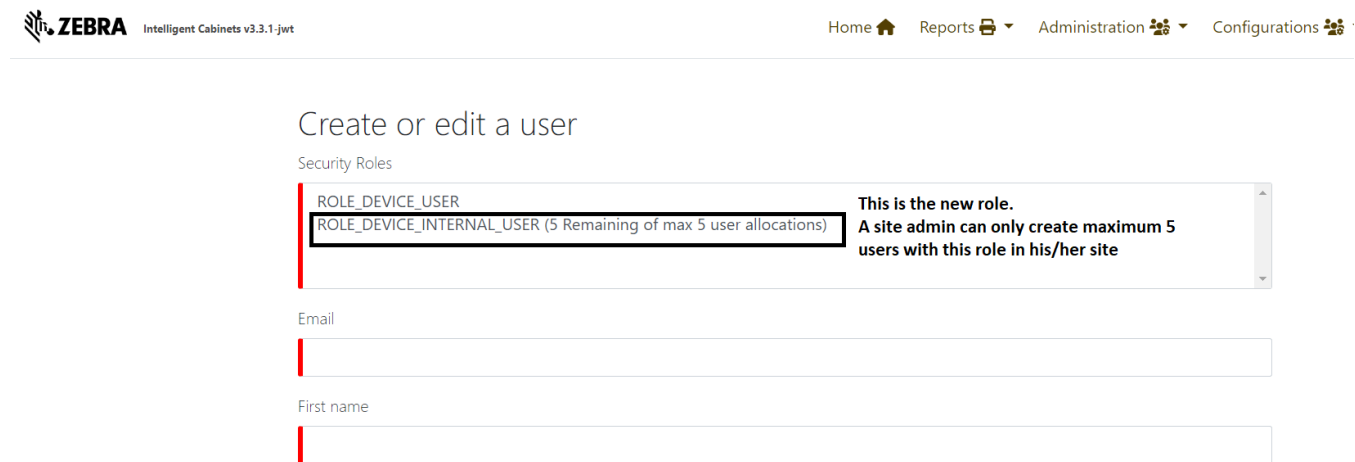
What if both Kiosk and Portal are unfortunately down?

This is where a user with `ROLE_DEVICE_INTERNAL_USER` comes to rescue.

How to create Users with ROLE_DEVICE_INTERNAL_USER role?

On ZAMS portal, a Company Admin/Site Admin can traverse to Administration → User Management and select “Create User” button.

A page as shown below will be displayed. Highlighted is the new role. A site admin can only create 5 users with this role in his/her site.



Home Reports Administration Configurations

Create or edit a user

Security Roles

ROLE_DEVICE_USER	
ROLE_DEVICE_INTERNAL_USER (5 Remaining of max 5 user allocations)	This is the new role. A site admin can only create maximum 5 users with this role in his/her site

Email

First name

A company admin with 24 sites should be able to create maximum 120 users (Max 5 users/site. Hence 120 users for 24 sites) with this role.

A company admin will come to know the remaining number of users that he/she can create in a selected site as shown below.

Create or edit a user

Security Roles

ROLE_DEVICE_USER
ROLE_DEVICE_INTERNAL_USER (120 Remaining of max 120 user allocations)
ROLE_COMPANY_ADMIN
ROLE_COMPANY_USER

If a company having 24 sites. A company admin can create maximum 120 users.

First name

Last name

Contact Email

Device Login

Company

Zebra Technologies

Site Id/Name

5/Dan Silva Demo

5 Remaining of max 5 user allocations for the selected site

It also shows number users that company admin can create on selected site. It displays 0 if all users are exhausted and company admin cannot create role device internal user for selected site

PIN Code (Digits)

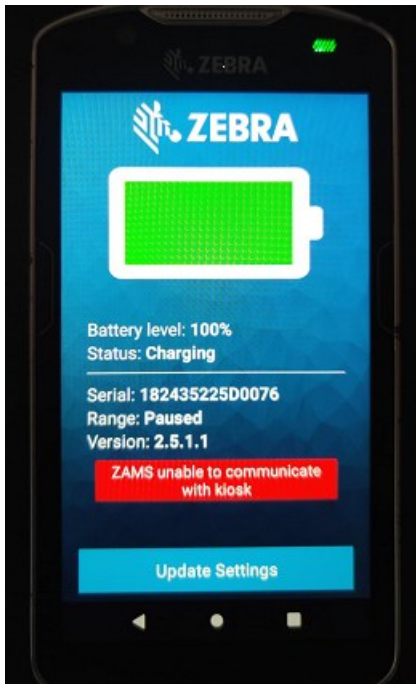
How does it work?

From ZAMS version 23.3.0, a Company Admin or a Site Admin should be able to create users with role “ROLE_DEVICE_INTERNAL_USER”.

Once users are created with the above role, these users’ data will be synced to Kiosk and intern will be synced to MC devices.

In situations where, both Kiosk and Portal are down, Site Admin or Company Admin can share the “ROLE_DEVICE_INTERNAL_USER” PIN to MC device users so that MC devices can be unlocked from cradle (**provided these users are created before any such situation arises**).

MC device display below error message if it cannot communicate with Kiosk. In this scenario, a user with ROLE_DEVICE_INTERNAL_USER role can swipe the battery screen and enter the PIN on PIN screen to unlock the device.



Things to Remember

1. **Only 5** active `ROLE_DEVICE_INTERNAL_USER` can be created **per site**.
2. Any number of inactive device internal users can be created. But at any point of time only 5 device internal users can be active.
3. A deactivated device internal user cannot login to device
4. It is recommended to create these users before hand so that these users can be handy in emergency situations.
5. User with `ROLE_DEVICE_INTERNAL_USER` cannot be GLOBAL.
6. A Site Admin can only create 5 active device internal users in the site within his/her purview.
7. A Company Admin can create device internal users across the site within his/her company but can only create maximum 5 such users per site.
8. “ONE DEVICE USER ENABLED” rule will not apply for users with `ROLE_DEVICE_INTERNAL_USER` role.
9. Any change on device internal user data made on ZAMS portal will take 1.5 minute to sync to MC device.

1.2 Bug Fixes

1.2.1 AMS Server v3.3.1

i. Device Status count discrepancy between Kiosk and Portal dashboard.

This issue has been fixed in Portal version 3.3.1.

ii. Cannot update Site Name to GLOBAL for Site Admin User account in ZAM's portal.

A site admin cannot be Global. So, the GLOBAL option on site admin create/update page has been removed to avoid confusion.

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