Zebra Access Management System (ZAMS) (Cloud and Client)

Troubleshooting Guide

Final Draft v.1.0

October 20, 2023

Contents

1. Overview

1.1. Purpose

The intent of this document is to cover troubleshooting process to support for Zebra Access Management System (ZAMS) SW Solution. This document does not cover the support structure. This document is for internal purpose only and not to be share with anyone outside Zebra

1.2. Non-disclosure

The design, service description, and technical information furnished with this document is proprietary information of Zebra Technologies or its affiliates. Such information is not to be disclosed publicly or in any manner to anyone without the express written permission of Zebra Technologies.

2. Product Overview

The Zebra Access Management System (ZAMS) device monitoring application is a secure cloud based solution designed to enable organizations reduce the number of missing or unaccounted for mobile computers, optimize work flows and deliver measurable benefits.

The ZAMS Software Product consists of the following elements:

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/ and is used by all customers.

2.1. Key Product documentation

Customer facing documents and software are published at https://www.zebra.com/us/en/support-downloads/software/productivity-apps/intelligent-cabinets.html Refer to that location for the latest posted versions.

The following documents are helpful references in the verification and troubleshooting process:

- Zebra Access Management System Installation Guide

  Explains the SW installation, registration and use of Zebra value add tools (e.g. DataWedge, StageNow) used by ZAMS installation and usage.

  The install guide also points out the files needed for EMM/MDM installation.

- ZAMS User Guide

  Explains the ZAMS product and key usage features in more detail. Most features are exposed in the ZAMS portal and kiosk UI. The UI can also be used as means to understand the feature constraints and limitations.

- ZAMS Cabinet and Mobile Device QRG

  This is a poster like document that is used to give a very high level quick reference guide of the product.

3. Tools and Applications

The following tools are helpful in diagnosing ZAMS issues:

- Device resident browser (Chrome)

  Useful for verifying network connections.

- RxLogger

  Useful for collecting device and application logs needed for advanced triage and fault isolation

- Remote screen viewer

  Used to capture screen views on the android devices including the kiosk.

- Network tracing tools

  Used to collect network logs for advanced triage and fault isolation

- UI Access to network and firewall settings.

  Used to confirm network requirements are properly established. The installation and user guide explains the specific requirements.

4. Verification of proper operation

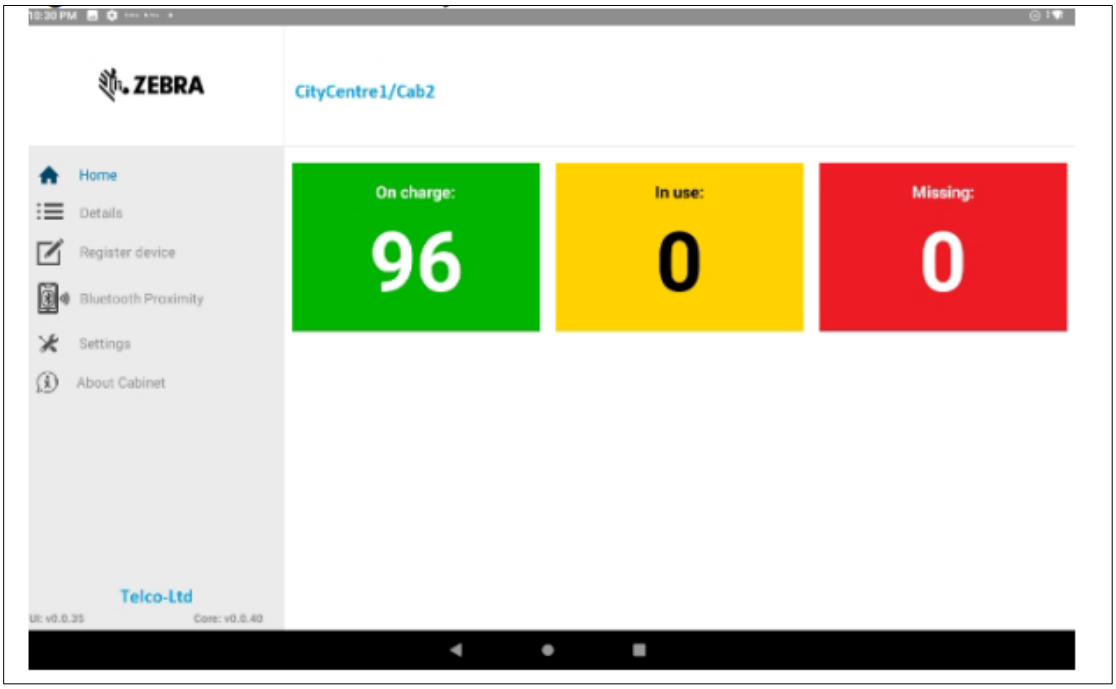
The following are typical tests to confirm proper operation of the ZAMS SW

4.1. Verification of mobile device functions

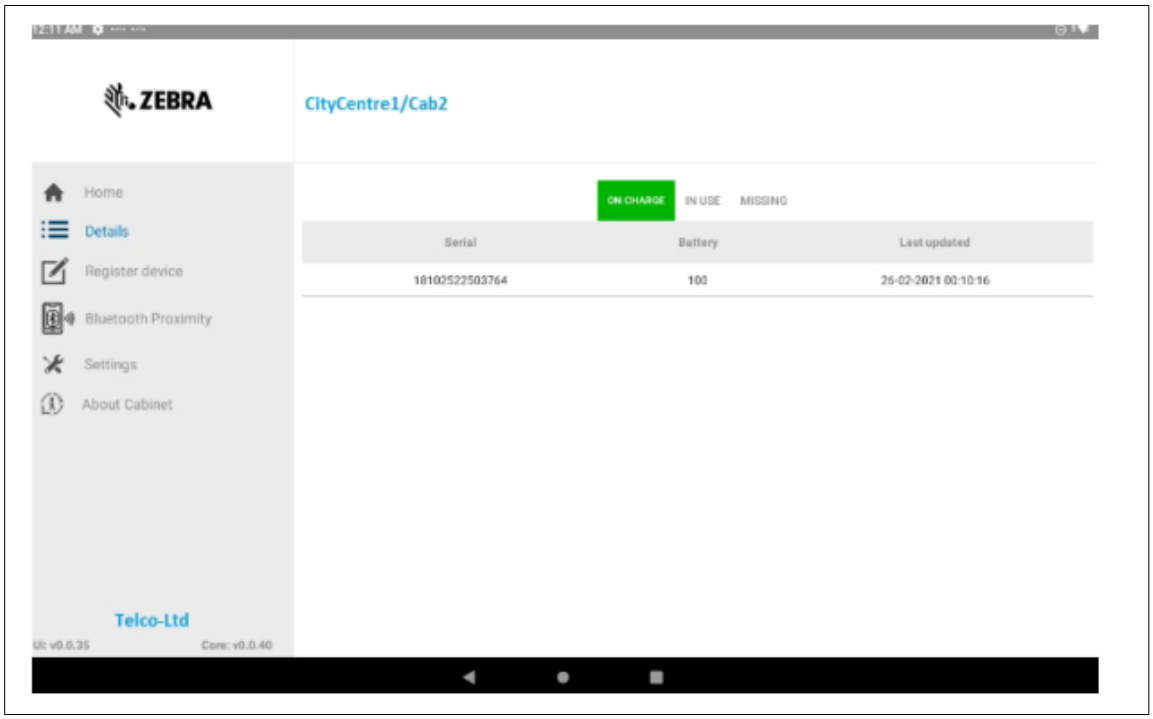
- When device is in the charger, the charge screen is shown
- When device is removed from the charger, a log in prompt is shown along with a countdown timer shown.
- If the user does not log in within the timeout period, the device alarms. Placing the device back in the charger or logging in stops the alarm.
- User can log in to device when valid credentials are entered. The ZAMS screen is no longer seen

4.2. Verification of kiosk functions

- Verify the kiosk dashboard shows the proper state and count for total number of assets (e.g. mobile devices) the kiosk is managing.



- Verify summary counts of each state in the dashboard changes based on the device state. A device in the cradle shows Green/Charging, a device that is out of the cradle and not logged in by a user, is shown as Red/Missing, a device that is out the cradle and has a user logged is in the yellow/in-use state.
- Spot check the device ID on the state/color details matches the proper state. As the device is removed and logged in, the kiosk should report the device in the proper details section for that state/color



- Verify kiosk has connectivity to the portal
    - Portal dashboard state matches the kiosk state when the kiosk is properly selected in the portal.
    - A browser launch from the kiosk to browse the portal page should show the portal's home page.

4.3. Verification Portal functions

- Verify user functions
    - An Admin user can log in. Note only admin type users can log into the portal. ZAMS has several administrative user account roles (reflected in the user management UI page on the portal). When a customer account is first created, Zebra only establishes one admin account with the "company admin" role. The customer is responsible to use this account to create additional accounts that can log into the portal.
    - Logged in user can view and create other user accounts via the UI.
    - Logged in user can import and export user accounts via the UI
    - Logged in user can view reports, export and schedule via the UI.
- Verify kiosk connectivity functions
    - Verify kiosk state matched the portal state for the selected kiosk

- If the kiosk state changes, the portal state should show the changes within a couple of minutes but is typically within seconds.

5. Common errors

5.1. Kiosk or wifi is down, device alarms if is removed

- Admin user will need to generate the ZAMS bypass barcode form the portal. This barcode will be used to bypass the ZAMS login needed to unlock or turn off the alarm

5.2. Kiosk reports not connecting message

- Verify network port settings are established as per the installation documentation
- Verify network connection from kiosk is working by browsing to the portal URL via a web browser. Chrome is the OS resident browser on Android devices.
- Note for ZAMS, the mobile devices do not connect directly to the portal. The mobile devices connect to the kiosk, using a custom port as specified in the installation documents. The kiosk connects to the portal over https. See installation document for more details.

5.3. Portal is down

- If not able to access the home page or site, verify access via a public internet connection. If portal is still not accessible, escalate for immediate reboot/restart of the portal
- If Portal pages is accessible from the public network and not from within customer network, check the customer network settings
- If Portal is accessible from kiosk browser but kiosk reports connection errors, collect RxLogger logs and escalate for review. A reboot of the kiosk or restart of the kiosk core services can be used to recover from the issue.
- If Zebra monitoring services auto-detects the portal is down, the issue is to be escalated immediately for recovery. A server restart should resolve the problem.

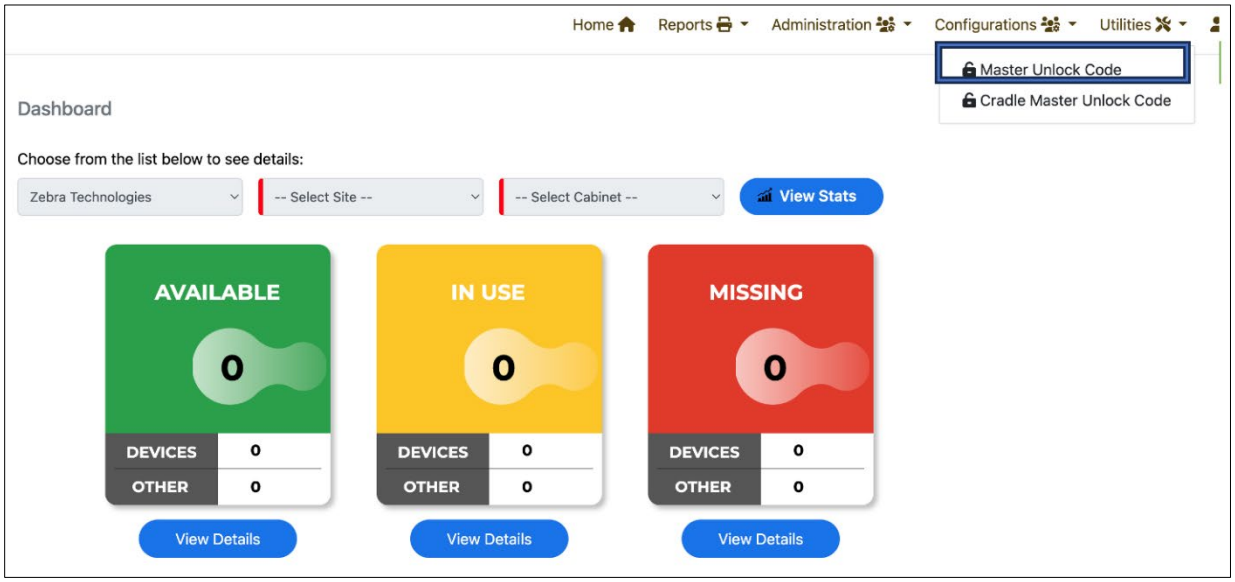
5.4. Master Unlock:

Master Unlock Code: (How to find the missing device)

Send the alarm from the ZAMS Portal and when the device was found,

Device_User can stop the alarm in below process **(using any one of the below steps):**

- Enter the passcode.
- Place the device back to the cradle.
- Administrator can scan the QRcode from the UI (Utilities) << Master Unlock Code



- Scan the QRcode from the UI (Utilities scan)

- Scan the BARcode from the UI (Utilities scan) .- Only applicable for linear devices.

Cradle Master Unlock Code: (How to log in to the device when Portal and KIOSK or only KIOSK are down)

Access to the Zebra support portal and generate the Cradle Master Unlock QR code from Utilities<Cradle Master Unlock Code screen (Wi fi is require). This QR code is valid for 48 hours. Any time Wi fi (KIOSK and Portal or only Kiosk) goes down, user can use this QR code (within 48 hours) and can use to log in. No limitation on device count log in.

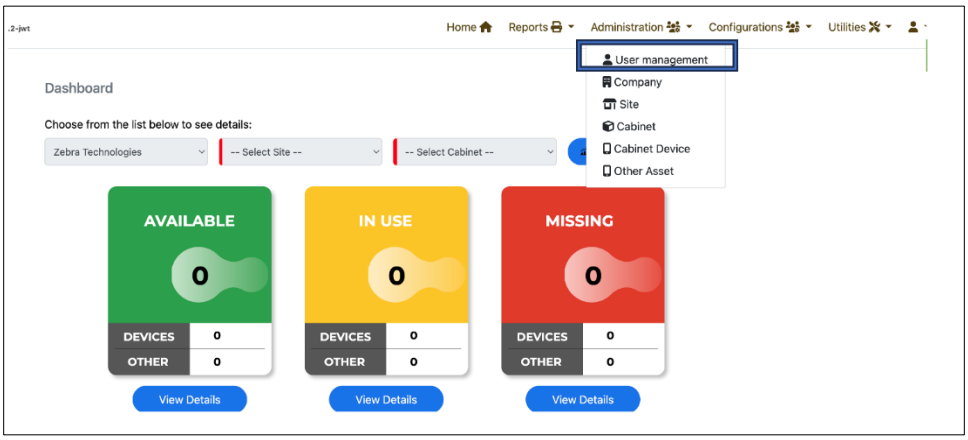
5.5. Portal and KIOSK or only KIOSK is down: (Break Glass)

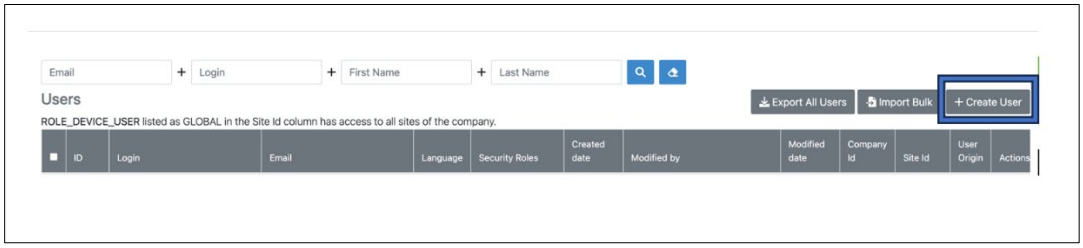
Option 1:

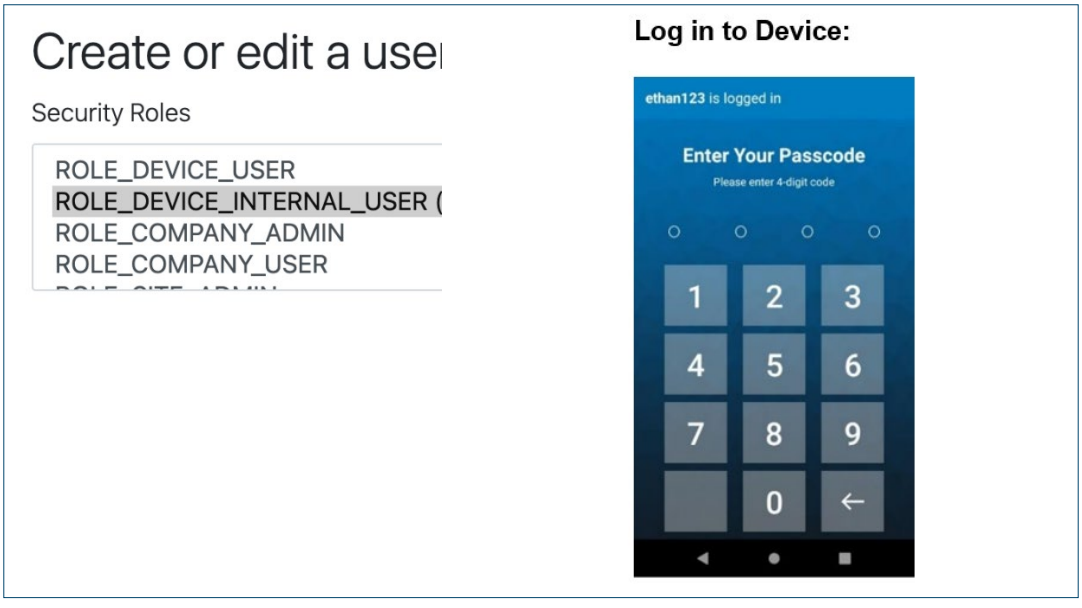
Please use **Cradle Master Unlock Code functionality as mentioned above**.

Option 2:

Company admin can assign “ROLE_DEVICE_INTERNAL_USER” to any 5 employees in each site in User Management and when Kiosk and Portal or only Kiosk goes down, ROLE_DEVICE_INTERNAL_USER can log in to the device and pass the device to the Device User (who will be using the devices). Note: ROLE_DEVICE_INTERNAL_USER is a privileged Role, and it will be assigned only to 5 privileged users in every site.







5.6. Forgot user password

- For first time log in, a common issue is someone clicked on a “one time” use URL that resets the only portal account password given to the customer. If that URL was clicked on or used to set a password the customer forgot to the only company admin “role” account, their issue must be escalated to the ZAMS DB owner to reset the password.
- Company admins are encouraged to create additional administrative accounts on the portal. If another administrator account is present, they can change the password for other users including other admin accounts. The use of additional administrative accounts allows the customer to correct the problem without the help of Zebra.
- For security reasons, Zebra does not have access to the customer data except in special circumstances. Therefore, customers need to establish additional administrative accounts to avoid delays in resetting their password.

5.7. Device state showing up on a different kiosk or not at all

- The mobile device is registered to a given kiosk regardless of where it is charged. If the device is reporting status to a kiosk in an unexpected location, the device should either be moved to the expected cabinet, or the device needs to be registered to the new kiosk.
- Refer to the installation guide on how to register a device to the kiosk.
- An upcoming release of ZAMS will support return to a different cabinet but the initial registration of the mobile device to a kiosk is still required.

5.8. Unable to log into Zebra support site to access the ZAMS software

- Access to the Zebra support portal requires registration of the ZAMS contract ID to a customer. The customer needs to obtain the contract ID from their sales rep or a ticket needs to be raised to the Zebra order management owner for ZAMS.