

Zebra Access Management System (ZAMS)



ZEBRA

User Guide

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2024 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal

COPYRIGHTS: zebra.com/copyright

PATENT: ip.zebra.com

WARRANTY: zebra.com/warranty

END USER LICENSE AGREEMENT: zebra.com/eula

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Publication Date

September 12, 2024

Contents

About This Document	5
Introduction	5
Chapter Descriptions.....	5
Notational Conventions	5
Icon Conventions	6
Related Documents and Software	6
Getting Started	7
Zebra Access Management System Overview	7
Operator Process Overview	7
Admin Process Overview	8
ZAMS Network Requirements	8
Target Environments	9
Limitations and Recommendations	10
Bluetooth Proximity	10
Portal to KIOSK and KIOSK to Portal Sync	10
ZAMS General Usage	11
ZAMS Mobile Devices.....	11
General Usage	11
Swap User without a Cradle	13
ZAMS Cabinet (KIOSK ET40 or CC6000)	14
Home	14
App Login on Reboot.....	17
ZAMS Cabinet Set Up.....	18
ZAMS Portal Access and Usage	19
Zebra Access Management System Portal.....	19
Portal SSO.....	19

Contents

Device SSO	22
Accessing ZAMS Account	26
Resetting Password.....	26
Selecting ZAMS Portal Dashboard Options	27
Viewing Device Details	29
Finding a Lost Device	30
Administration	35
Reports	43
Historical Reports	46
Generating Unlock Code	52
Adding a Device User	53
Device User Roles	54
Cradle Lock	56
Troubleshooting	60
Technical Support	61

About This Document

Introduction

The guide provides information about installing and using the Zebra Access Management System (ZAMS) software that is used with the Zebra Intelligent Cabinet product.

ZAMS software comprises of three 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 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 Android-based mobile devices.
2. KIOSK application and services: provides on-site device management UI and provides information to the cloud-based console. The KIOSK application is designed for Zebra's ET40 or CC6000 devices.
3. Cloud resident console: a web portal that provides various administration-level tasks and reports. The server access location is zebra.com/zams.



IMPORTANT: If you have a problem with your equipment, contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

Chapter Descriptions

Topics covered in this guide are as follows:

- [Getting Started](#) provides an overview of the ZAMS application, Cabinet set up, and network requirements.
- [ZAMS General Usage](#) provides information on battery indications, creating a PIN, using the dashboard, device registration, and Bluetooth proximity.
- [ZAMS Portal Access and Usage](#) provides information on accessing and using ZAMS on the portal.
- [Troubleshooting](#) provides information on potential problems, causes, and solutions.

Notational Conventions

The following conventions are used in this document:

- Bullets (•) indicate:
 - Action items

- Lists of alternatives
- Lists of required steps that are not necessarily sequential.
- Sequential lists (such as those that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set. These icons and their associated meanings are described below.



NOTE: The text here indicates information that is supplemental for the user to know and that is not required to complete a task.



IMPORTANT: The text here indicates information that is important for the user to know.



WARNING: Warning text goes here. If danger is not avoided, the user CAN be seriously injured or killed. Confirm with your Compliance Engineer before using this.

Related Documents and Software

The following documents provide more information about Intelligent Cabinets:

- Racks 1 & 2 Shipping and Unpacking Quick Reference Guide
- Zebra Cabinet Site Installation Guide
- Zebra Cabinet Shelf Assembly Instructions
- Access Management System Installation Guide
- Access Management System Cabinet and Mobile Device Quick Reference Guide
- dwprofile_amsPIN.db - DataWedge profile for AMS application PIN scanning
- dwprofile_AmsDevice.db - DataWedge profile for AMS application device registration
- StageNow installation files¹ - StageNow software staging solution for simple profile creation and device deployment
- Release notes¹

For the latest version of this guide and all guides, go to zebra.com/support.

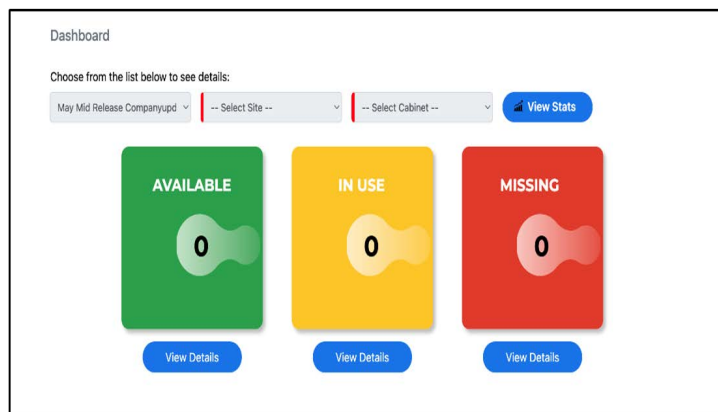
¹ Actual filenames may have a version extension to match the software release it applies to.

Getting Started

Zebra Access Management System Overview

The Zebra Access Management System (ZAMS) application is a secure solution designed to help organizations reduce the number of missing or unaccounted mobile computers.

Figure 1 ZAMS Dashboard



Deploy and manage this low-touch solution on Zebra Android Mobile devices to easily account for your mobile assets and minimize potential losses.

The solution monitors devices by serial number, user, and location, enabling quick detection of missing devices.

The ZAMS portal is an ideal solution for setting up device management across multiple locations. With password-protected user access, users can easily manage missing devices across a mobile computer fleet, whether at a local or global level. This gives customers the necessary tools to keep track of their assets more efficiently.

Operator Process Overview

Designed not to intrude on a user's daily activity, ZAMS provides a simple security screen or a lock-screen, displayed on the device, while the device is On Charge.

The user facing security screen highlights the devices batteries charge level (while in its cradle) and this clear visual que helps users pick a device that's charged ready for the shift.

To activate a device for the shift, the operator scans the PIN from the barcode or other authentication process to unlock the security screen.

The operator is driven to unlock the device within a few minutes. If the unit is not successfully unlocked within a specified time frame, a built-in timer sounds a reminder alarm to drive the correct process and make sure the application can pass the user ID and serial combination to the servers.

Once the unit is returned to the Cabinet or charging dock, it automatically logs the user off, and reports the device has been returned to the charging location.

Adding devices to Locations (Company, Site, & Cabinet)

Adding devices to a location is a simple process that requires firstly that the ZAMS APK is installed on the devices.

Installation Process

Refer to the **Rack Model 1 & 2 Installation Guide - MN-003984-02EN Rev A** for the installation process.



NOTE: Installation guide through MDM is available to the below location:

zebra.com/us/en/support-downloads/software/productivity-apps/intelligent-cabinets.html

Adding devices to the Database

Each device is registered, logged, and linked to the location (ZAMS database using a dynamic barcode) that is either printed from the administration portal for use by the installation team or displayed locally at the charging location on the optional display KIOSK.

Once the devices are registered, they are ready to go to work, no other intervention is required on the mobile computers.

Using the Reporting and Administration Portal

The ZAMS portal is password protected and authorized users can create custom locations and add user IDs.

Admin Process Overview

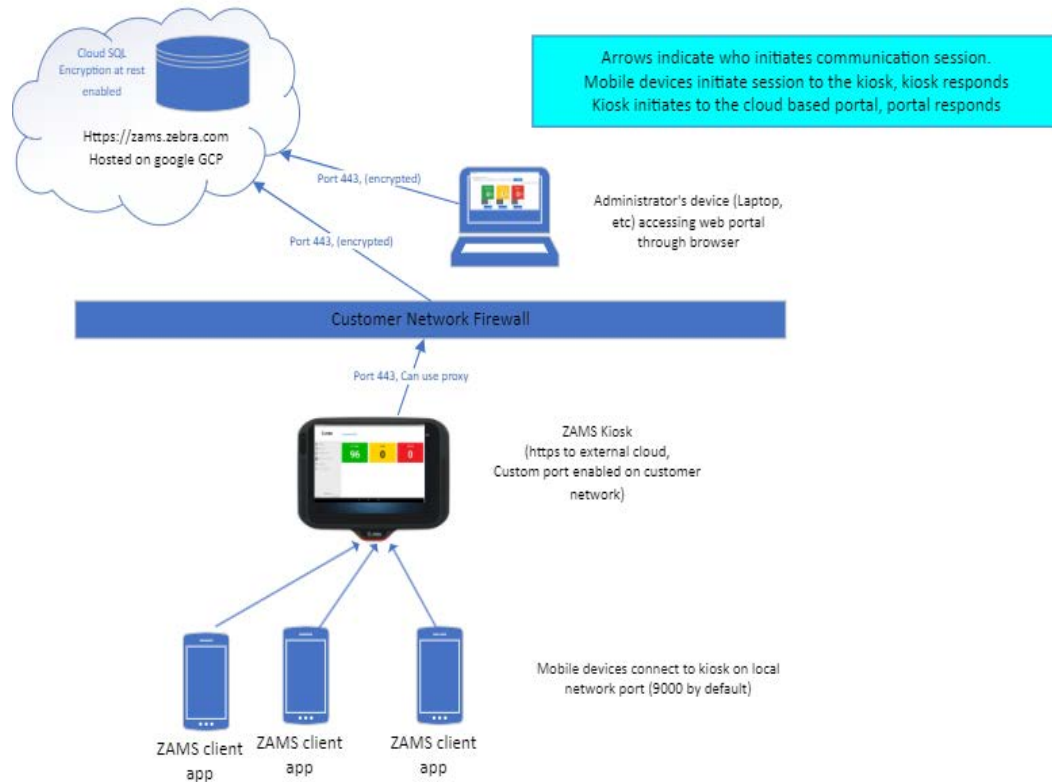
The Reporting and Admin portal provides the client the ability to set up the solution.

The password protected, multi-level menu helps drive the administration staff to add mobile computers to the database (by location), add users and monitor devices On Charge, monitor devices in use with which operators, and monitor missing devices.

ZAMS Network Requirements

The ZAMS network is picture in [Figure 2](#). Refer to the ZAMS Installation Guide for detailed network requirements (see [Related Documents and Software](#)).

Figure 2 ZAMS Network



Target Environments

ZAMS supports the following target environments:

- Mobile Devices (Android version 8, 9, 10, 11, 13)
 - Zebra full touch devices (TC15, TC2x, TC5x, TC7x)
 - Zebra keyboard devices (MC22xx, MC33xx, MC93xx)
 - Zebra Android Tablets (ET4x, ET5x, CC6000)
 - Zebra small devices (EC3x, EC5x)
 - Exceptions: Mobile devices with external power packs. Supported on a case-by-case basis.
- KIOSK
 - CC6000 (Android version 8, 9, 10, 11, 13)
 - ET40 (Android version 11 and 13)
- Portal UI
 - Chrome version 9 or later
 - Microsoft Edge version 124 or later

Limitations and Recommendations

- Each KIOSK is limited to connecting 100 devices (mobile computers).
- Each KIOSK is limited to syncing 500 registered users, combining both Global and Site Users.

Bluetooth Proximity

If the Company Admin turns on the optional feature Bluetooth proximity on the portal, then Bluetooth Proximity is enabled automatically after successful registration of the ZAMS device with the Cabinet.

For example, you may want to consider using this feature in the case of a truck driver checks out the device at the start of shift (near the cabinet) and may charge the device in the truck during the day, so this feature will allow them to do that without popping up a PIN screen or charge screen to interrupt drivers everyday work.

When Bluetooth Proximity is enabled, the device can pair with the Cabinet dashboard and measure the distance between the mobile device and the Cabinet dashboard device. If the user is more than approximately 2 meters away from the Cabinet dashboard, the alarm triggers regardless of timer duration. No data is transferred between the dashboard and the mobile device over the Bluetooth connection. It is there only to measure the distance.

When Bluetooth Proximity is enabled and you are successfully logged in, ZAMS is only triggered when the device is put back on power within 2 meters of the Cabinet dashboard.



NOTE: Electro-magnetic noise at a site can interfere with the ability of the devices to measure the distance accurately.

The message **Bluetooth proximity is disabled** displays when Bluetooth is disabled.

Bluetooth Proximity can be enabled from the ZAMS portal at Company (for all locations) or at a Location level.



NOTE: If Bluetooth proximity is enabled in the Portal, it will enable Bluetooth on both the KIOSK and the Device. Ensure the device's location is enabled for successful synchronization.

Portal to KIOSK and KIOSK to Portal Sync

The frequency at which the KIOSK communicates with the server/portal is changed to reduce the computation load on the KIOSK.

There are two configurable timers running on the KIOSK:

- 1 - 15 minutes: This timer can be set between 1 to 15 minutes and is used to fetch a list of users, lost devices, and other information.
- 10 - 60 seconds: This timer can be set between 10 to 60 seconds and is used to update the status of devices (available, in use, missing) to the server.

Customers can configure timer values via **MDM** configuration or by placing a configuration file in the **Downloads** folder. When new timer values are configured, they become effective starting with the following cycle. For example, if the user adjusts the timer from a 15 minutes interval to 10 minutes, this new setting will be applied after the current 15 minutes timer ends. Subsequently, the timer will operate at 10 minutes intervals.



NOTE: Refer to the [Zebra Access Management System Installation Guide](#) for details on configuring with Mobile Device Manager (MDM).

ZAMS General Usage

ZAMS Mobile Devices

This section describes the following ZAMS app features:

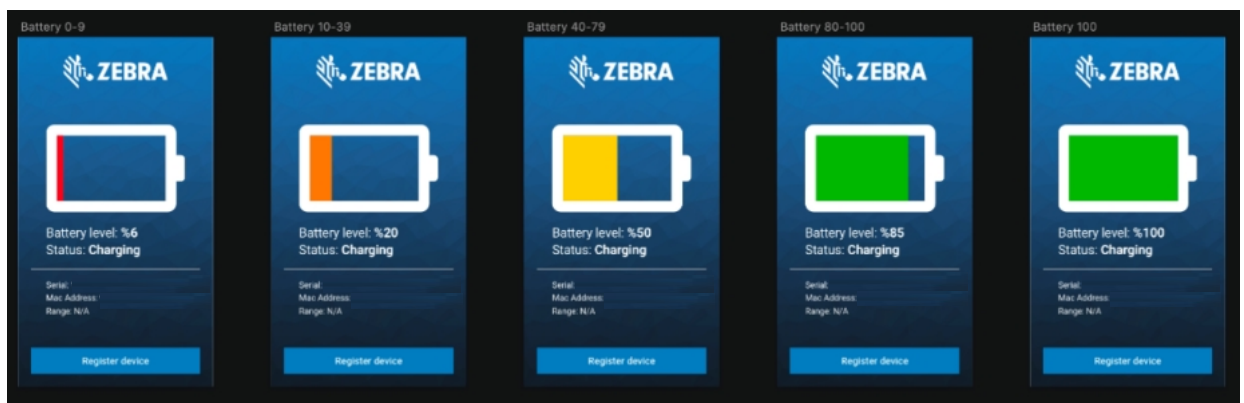
- Battery indications
- PIN code entry and considerations
- ZAMS Cabinet set up and registration.

General Usage

1. Take only devices with fully charged batteries from the Cabinet. Devices that are fully charged have a green battery indicator.

When the device is placed On Charge, the ZAMS application displays the charging screen with battery status indicators:

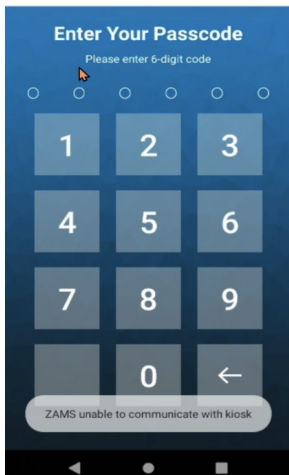
- Mostly or fully charged displays a green battery indicator.
- Approximately half or more of charged capacity displays a yellow battery indicator.
- Less than half displays an orange battery indicator.
- Critically low charge displays a red battery indicator.



2. Once the device has been removed from its cradle, the ZAMS application displays a prompts to enter a Passcode Identification Number (PIN).

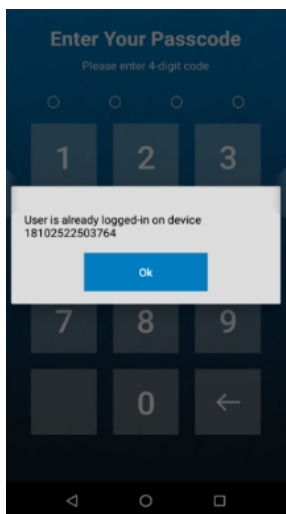


NOTE: A PIN is a form of User ID. Do not confuse this with a password that is often associated with the term PIN.



Considerations:

- The application triggers an alarm if a valid PIN is not entered within a specified period (configurable by Company or Location). The alarm volume cannot be adjusted. Users can place the device back into the Cabinet if they do not want to continue using it. If the PIN is invalid, then an **invalid PIN** message displays.
- Swipe down from the Battery icon on the charging screen if the device is locked in the ZAMS cradle lock. This triggers the **Enter Your Passcode** screen in the same way as if the device is undocked. If the correct PIN is entered, the device unlocks.
- If the correct PIN is entered, but the device is not removed from the cradle within 30 seconds, the cradle will lock again. If the device is not removed after an additional 60 seconds, the app will return to the charging screen. This applies only to customers who use Cradle locks.
- If a valid PIN is entered and the device is successfully logged in, no other user from the same company can use the same PIN to log in. If a user tries to enter a PIN that is already in use, they will see an error message indicating that the user is already logged in on a specific device. For example, the error message might read **User is already logged in on device 1xxxxxxxxxxx9**.



- The Scan PIN Code for login functionality allows the user to scan a barcode while the device is docked and the cradle lock is on. To enable this functionality, there is a requirement to create a new DataWedge profile. See the ZAMS Installation Guide for detailed information.

- Once the device is registered, the **Register Device** button label at the bottom of the ZAMS screen changes to a new label **Update Settings**. This function allows updating the settings of the application. This button can be used to scan BLE QR code to trigger BLE proximity function or scan a Master Unlock Code in case of lost power or other emergencies.
- If a device is taken out from the cradle and a PIN is not entered, press the home screen to go into the OS. However, the app continues to come to the foreground after fixed intervals to prompt the user to enter the PIN before the timer expires.
- When the device is docked (status On Charge) then the last updated time on Cabinet and Portal updates once the battery percentage level changes.
- An **Unable to communicate with cabinet** error message displays on the ZAMS device charging screen when there is no connectivity between the ZAMS device and Cabinet.
- At the time of registration of the ZAMS device with a Cabinet, the timer is updated on the lock screen according to the settings of alarm timeout configured for the respective Cabinet.
- While the Device is docked and in On Charge status, it goes to sleep as per the time configured. The ZAMS screen is still visible, and the brightness of the screen is reduced.
- If you need to troubleshoot a device that cannot be accessed with a PIN, or even during a remote-control session, the easiest way to do it is to put the device on charge and press the home button (the circle button at the bottom of the screen). While the device is charging, the PIN screen will not aggressively pop up over whatever you are trying to do, such as configuring Wi-Fi.

Swap User without a Cradle

This functionality allows an active user to log out of the ZAMS and pass on the device to a different user without returning the device to the Cradle. This functionality allows the following user to enter his valid PIN to log in.

By following the simple steps, this functionality can be used running the latest ZAMS Device APK:

- A user undocks a Device from the cradle and logs in using their valid credentials.
- When the device is assigned to the user, the device will be displayed as IN_USE as standard behavior.
- At any point during or after the shift ends, if the user wants to pass the device to another user, then the user must press the ZAMS Device Icon. Tapping the ZAMS Device Icon, the new PIN Screen will launch as given below.



- At this point, a new user can enter their credentials, and the device will be assigned to them. If the home button is tapped to minimize this screen, it will reappear after a few seconds. Therefore, the login screen cannot be dismissed until a valid login is entered or the device is returned to the cabinet.



NOTE: The device must be connected to the KIOSK for a login.

ZAMS Cabinet (KIOSK ET40 or CC6000)

The Zebra Access Management System provides a display module on or near the Cabinet to display the current statistics of the devices.

Home

Select **Home** to display a summary of the current devices registered with the Cabinet. The statistics on this page update automatically when there is a change to the state of any of the devices.

- **Available** – The number of devices that are currently On Charge in the Cabinet.
- **In Use** – The number of devices that have been removed from the Cabinet and successfully logged in.
- **Missing** – The number of devices that have been removed from the Cabinet and have not yet logged in. This list also display the items with missing status having a status reason (Not Returned, Communication Lost, & Invalid PIN).

The location and the Cabinet name is displayed at the top of the screen. The Company that the Cabinet belongs to displays at the bottom of the screen.

App Switchback Interval for Cabinet dashboard

If the AMS charge screen is minimized by pressing the home button, then the AMS charge screen re-engages automatically after a configurable time of 30, 60, 90, or 120 seconds. This time is configurable at the site level through the App Switchback Interval settings.

The timing is configurable at the site level from the ZAMS portal zebra.com/zams. Go to administration a Site and Edit/Create Site. There is also a configurable option; if the “turned off” option is selected, the screen does not pop back on.

Figure 3 AMS Charge Screen

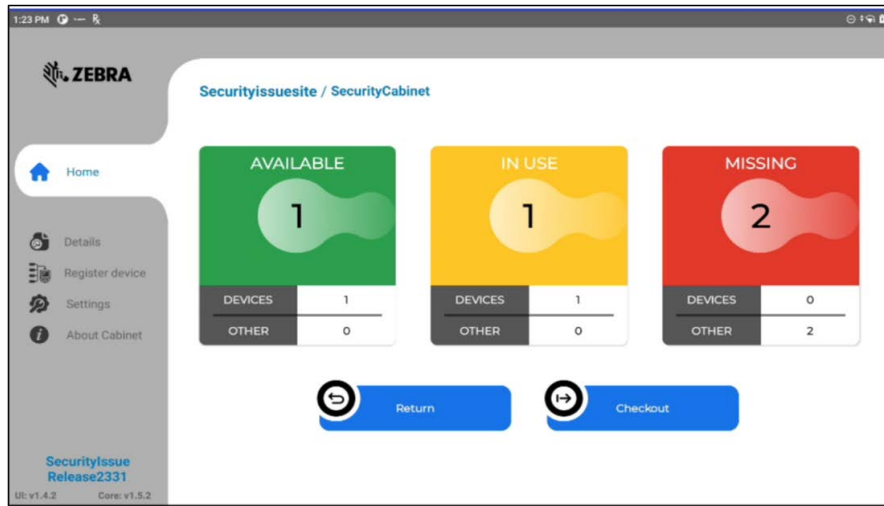
The screenshot shows two dropdown menus. The first is labeled 'Time Zone' and has a red vertical bar on the left. The second is labeled 'App Switch Back Interval' and has '30 Seconds' selected. Both menus have a downward arrow on the right side.



NOTE: A screen saver is added to address the potential screen burn issue.

- Screen saver will kick off 3 minutes after the device is on charge and record no user interaction.
- If the user presses a button, touches the screen, or takes the device off charge, the device will resume to the standard AMS screen.

Figure 4 ZAMS Home Summary Screen

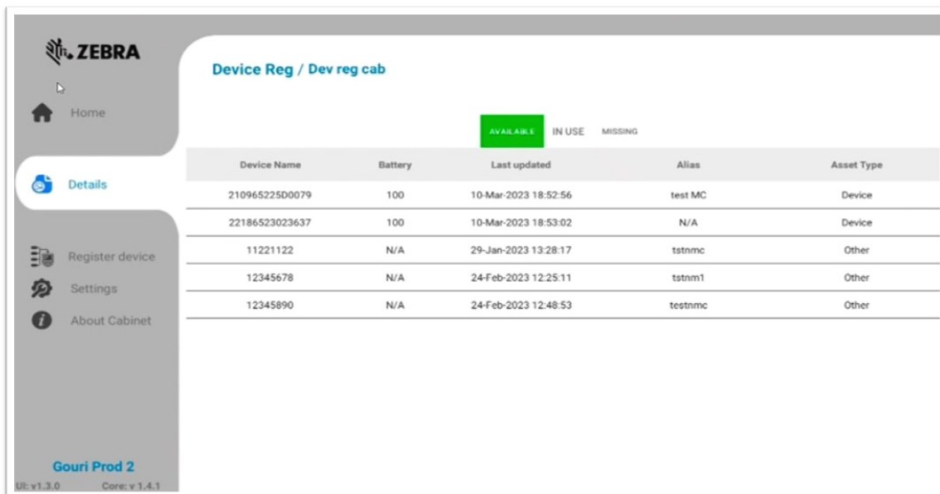


Available

The **AVAILABLE** tab lists all the devices currently On Charge in the Cabinet by serial number. It also displays the latest battery level along with a time stamp of the entry into the database.

To view the On Charge devices:

1. Click **Details**.



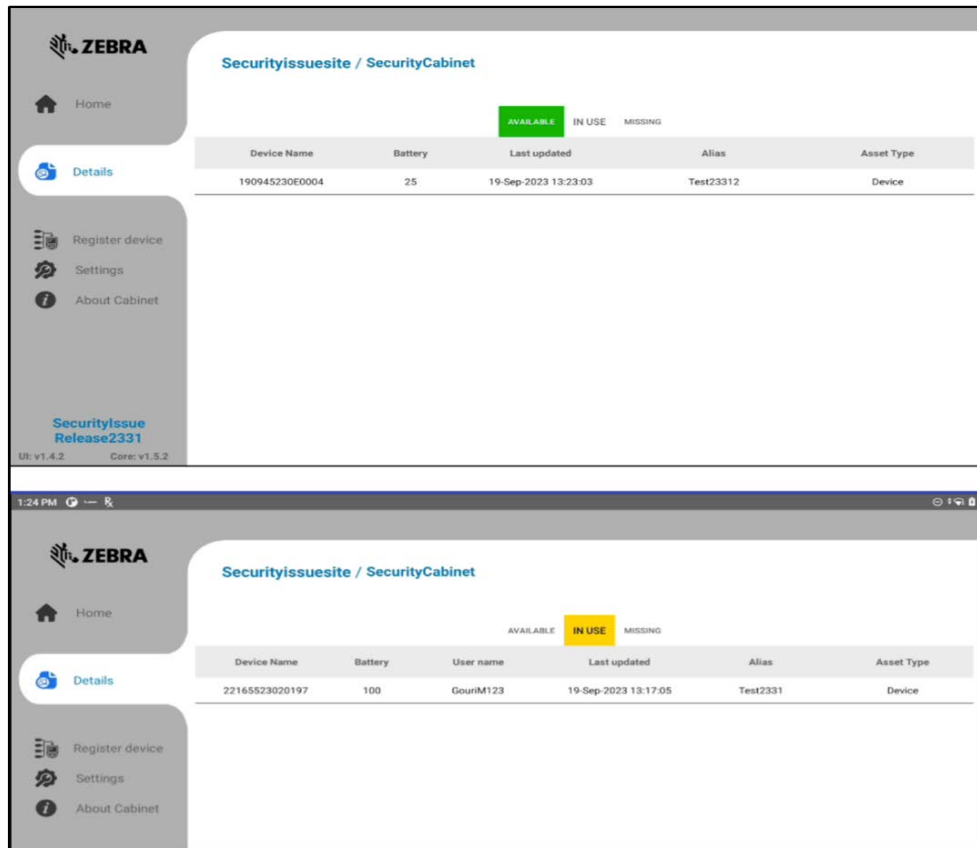
2. Click **Available**.

In Use

The **IN USE** tab lists all the devices that are no longer in the Cabinet. The list displays the users who have been successfully logged in along with the serial number of the devices. The username of the device is also shown along with a time stamp of when the device was logged in.

To view the in use devices:

1. Click **Details**.



2. Click **IN USE**.

Missing

The **MISSING** tab lists all the devices removed from the Cabinet but not logged in. These devices are not highlighted with color.

The devices classified as missing for more than five minutes are highlighted in RED at the top. This list shows the serial numbers of the devices and when the devices were removed from the Cabinet. The devices in this category are listed as Missing with three Status reasons.

Status	Status Reason	Details
MISSING	INVALID_LOGIN	Failed to log in and the device was not placed.
MISSING	NOT_RETURNED	The user has not return the device on time. Note: Shift duration is set for 8 hours. After 8 hours, the device is not placed in the cradle.
MISSING	COMMUNICATION_LOST	The user logged into the device and then took the device outside the network or disconnected the Wi-Fi.

To view devices considered missing:

1. Click **Details**.

Device Reg / Dev reg cab								
AVAILABLE IN USE MISSING								
Device Name	Battery	Last updated	Status Reason	User name	Last User	Alias	Asset Type	
210965225D0079	100	13-Mar-2023 19:45:26	COMMUNICATION LOST	N/A	Test123	test MC	Device	
22264523021423	99	01-Feb-2023 14:41:25	COMMUNICATION LOST	N/A	deviceuser1.03	lstmc	Device	
22153522504263	97	01-Feb-2023 20:30:01	NOT RETURNED	site	site	N/A	Device	
22186523025343	100	10-Mar-2023 11:49:51	COMMUNICATION LOST	N/A	N/A	N/A	Device	
22165523021315	100	10-Mar-2023 11:49:50	COMMUNICATION LOST	N/A	N/A	N/A	Device	
190945230E0004	97	10-Mar-2023 11:49:50	COMMUNICATION LOST	N/A	N/A	N/A	Device	
22186523023637	100	13-Mar-2023 19:45:26	COMMUNICATION LOST	N/A	Test123	N/A	Device	

2. Click **Missing**.

App Login on Reboot

This option allows you to log in to ZAMS again after a reboot or battery swap, even if the device is not on charge. This can be configured in the site settings. Go to **Administration and Site** and **Edit or Create Site**.

Select the **App Login on Reboot** checkbox to enable the login after the reboot.

App Login On Reboot

Alarm Timeout (Minute) Inherited?

Enable Bluetooth Proximity Inherited?

Shift Duration (Minute) Inherited?

ZAMS Cabinet Set Up

1. The ZAMS installation process consists of establishing network connectivity, accessing the Portal, and installing APKs and supporting files for the cabinets.
2. For detailed installation and set up information, refer to the ZAMS Installation Guide (see [Related Documents and Software](#)).

ZAMS Portal Access and Usage

Zebra Access Management System Portal

The ZAMS management portal is a cloud-based server accessible from a web page that allows for remote management of the ZAMS system across cabinets and company sites.

Portal SSO

ZAMS supports Single Sign-On (SSO) login on Zebra Mobile devices from the 24.3.0 release (AMS device v3.1.0).

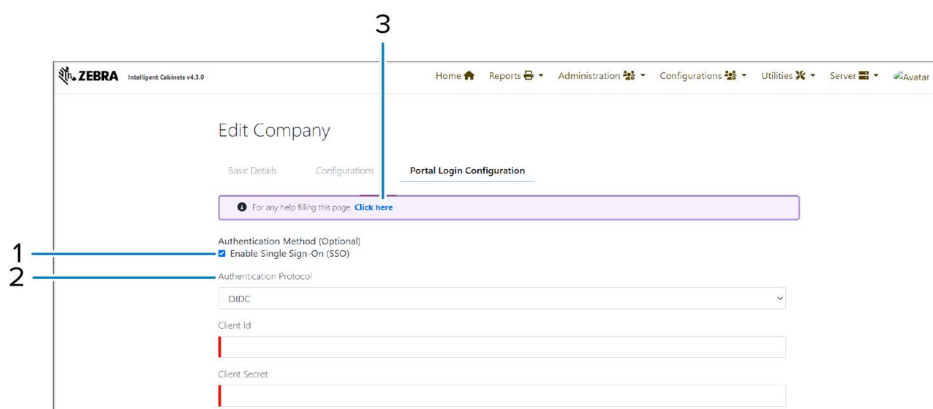
Users must install the Identity Guardian and ZAMS only supports SSO on Zebra Mobile devices with Android 11 and Android 13. AMS apps on Zebra Mobile devices to enable SSO login.



NOTE: ZAMS only supports SSO on Zebra Mobile devices with Android 11 and Android 13.

Enabling SSO

To enable SSO in the ZAMS Portal, follow the instructions below:



1. Log in as the Company Admin using username and password.
2. Navigate to **Edit company > Portal Login Configuration**. Click **Enable SSO** (1) and select the **Authentication Protocol** (2). Then, fill in the required details.
3. If you need assistance, click **Click Here** (3) to download the help document.
4. The Company Admin enters all details by referring to the downloaded document.



NOTE: The onboarding team will create a Company Admin with ZAMS credentials and provide those credentials to the customer for portal login.

1

5. Ensure all details are accurate before the Company Admin clicks the **Save** (1), as displayed below.



NOTE: If any of the details mentioned in the below form are incorrect, the admin will not be able to login to the portal. In such cases, the admin must create a ticket with the Zebra support team to rectify the issue.

SSO Login

To login as SSO User:

1. Enter the domain **Email ID** (1) and click **Continue** (2).

ZAMS Portal Access and Usage

1 Username*
au5657

2 Password*

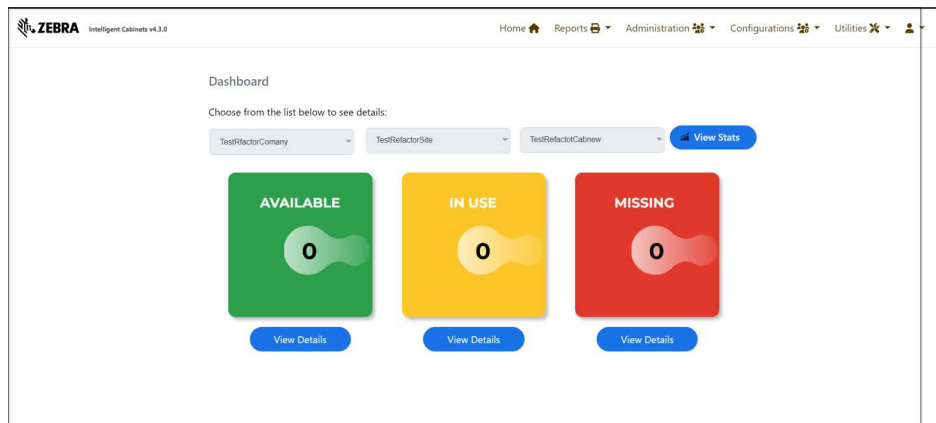
3 Sign In

Forgot your password? [Reset Password](#)

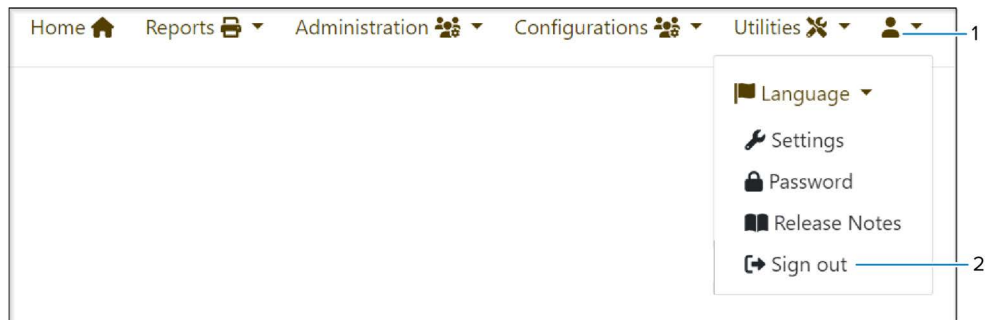
Need to change your password? [Change Password](#)

This site uses cookies to manage user authentication, analytics, and to provide an improved digital experience. You can learn more about the cookies we use as well as how you can change your cookie settings by [clicking here](#). By continuing to use this site without changing your settings, you agree to our use of cookies.

1. Provide the SSO credentials by entering the **Username** (1) and **Password** (2).
2. Click **Sign-In** (3). Upon successful login, the portal dashboard displays.



3. The Company Admin can perform the required actions after successfully logging in to the portal.



4. To exit the application, the Company Admin can click the **User Profile** (1) drop-down at the top-right corner and select the **Sign-Out** (2) option.

Device SSO

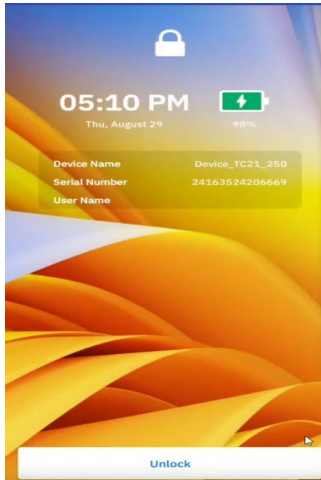
To enable SSO on a device, the Identity Guardian application must be installed, followed by the installation of the ZAMS device APK.



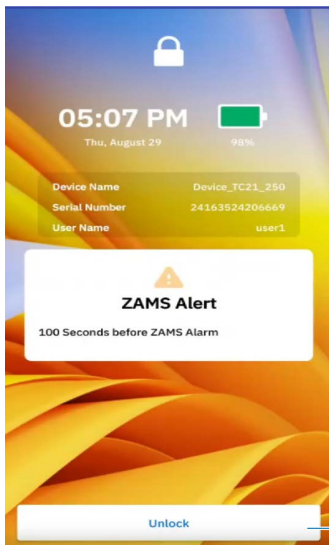
NOTE: Refer to the [ZAMS Installation Guide](#) to install the Identity Guardian application and enable SSO.

After installing and configuring the Identity Guardian and ZAMS device APKs on a Zebra Mobile device, the SSO flow displays as follows:

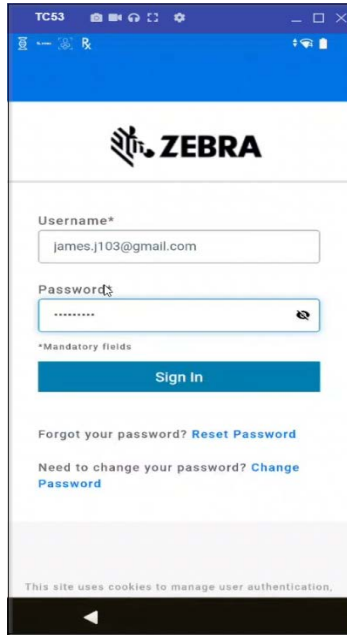
1. Charging Screen when the Device is docked.



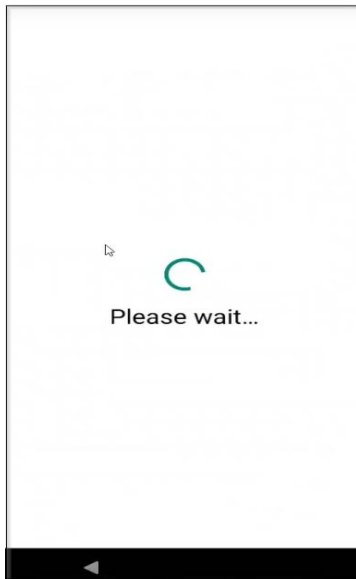
2. Charging Screen when the Device is undocked.



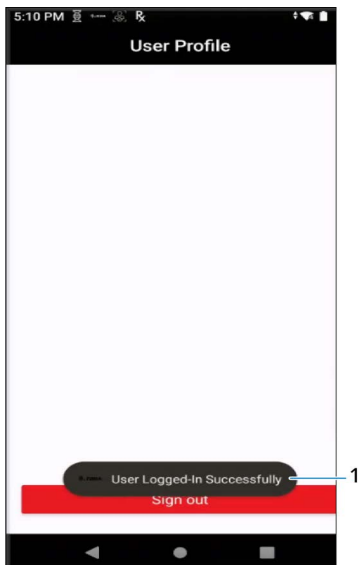
3. After clicking **Unlock** (1) (see previous step), the user can view the SSO Login Screen corresponding to the configured Identity Provider.



4. After entering the credentials, the **SSO Loading Screen** displays.



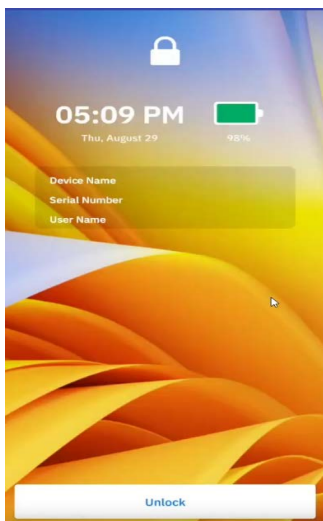
5. Upon successful login, the user can view the SSO **User Logged-In Successfully (1)** screen.



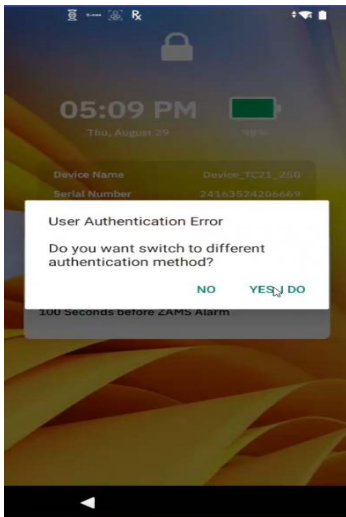
6. Click **Sign Out (1)**, and the confirmation screen displays.



7. Charging Screen after the user is signed out.



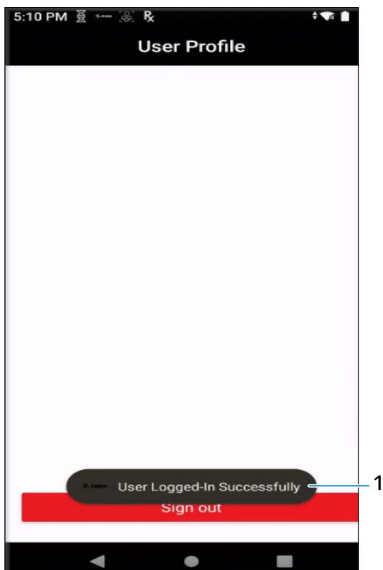
8. Switching to a different authentication method on **User Authentication Error**.



9. **Admin Bypass Passcode** screen for login.

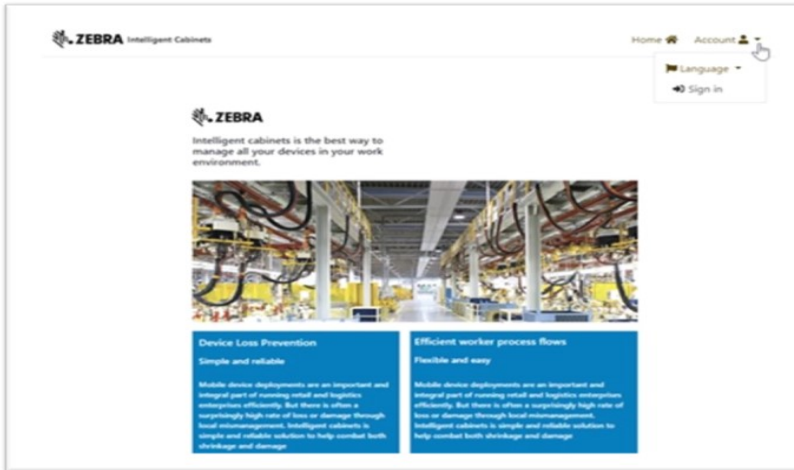


10. **Admin Bypass Passcode User Logged-In Successfully (1)**.

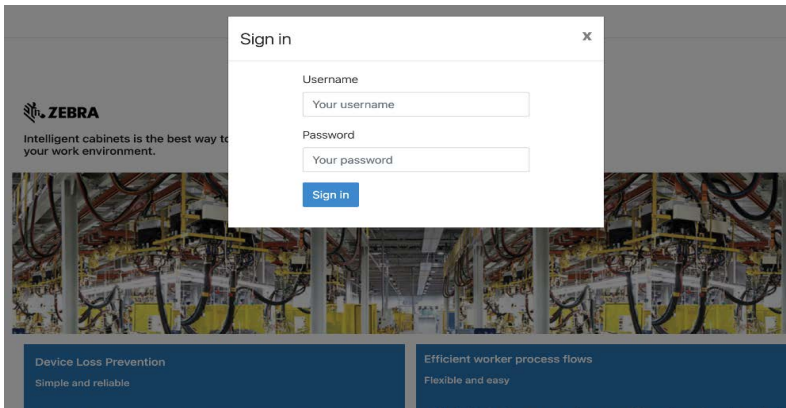


Accessing ZAMS Account

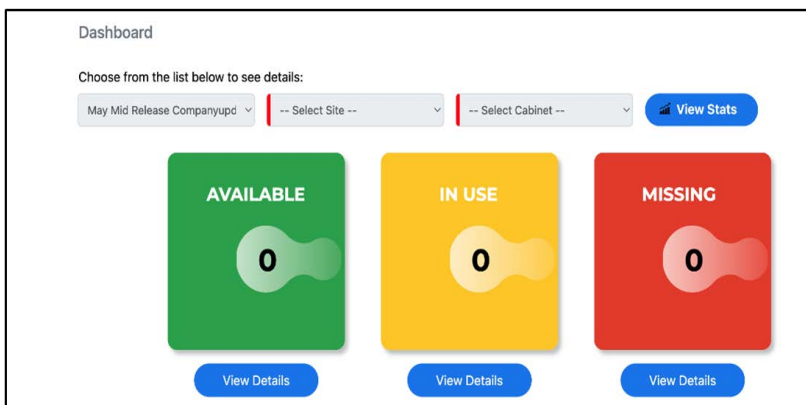
1. Open a browser on your PC or laptop and enter the URL: zebra.com/zams.



2. From the **Account** drop-down menu, click **Sign in**. The Sign in dialogue box displays.
3. Enter the Username and Password.



4. Click **Sign in**. The ZAMS Portal dashboard displays.



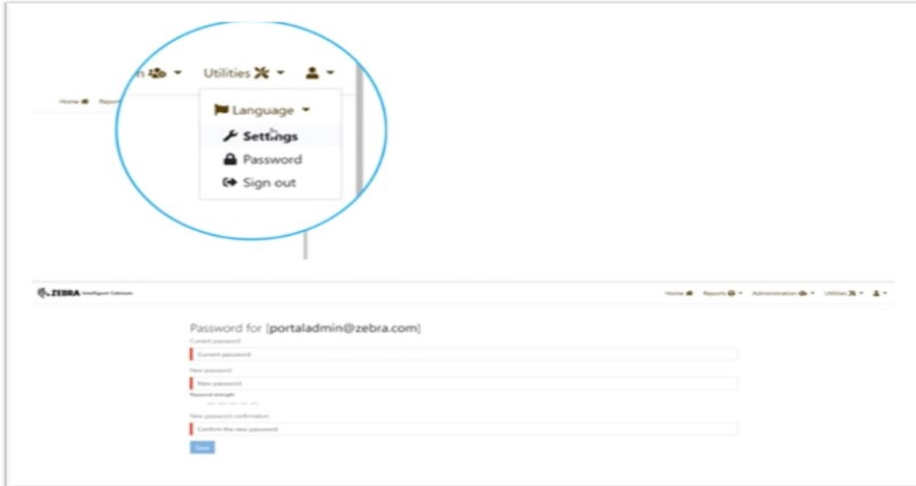
Resetting Password

The password must include the following criteria:

- Between 8 and 50 characters long
- Contain at least one digit
- Contain at least one lowercase character
- Contain at least one uppercase character
- Contain at least one special character

To change your password:

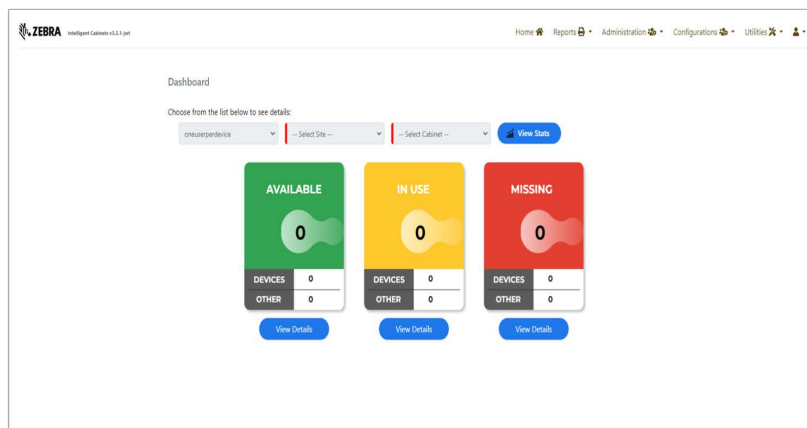
1. Select **Password** from the Account drop-down menu. Criteria is listed above.



2. Complete all fields and click **Save**.

Selecting ZAMS Portal Dashboard Options

The initial screen of the application is the Zebra Access Management System dashboard.



1. Click the drop-down menus and select the desired **Company**, **Site**, and **Cabinet**.

A notification banner appears on the dashboard for maintenance-related changes, such as planned or recent updates.

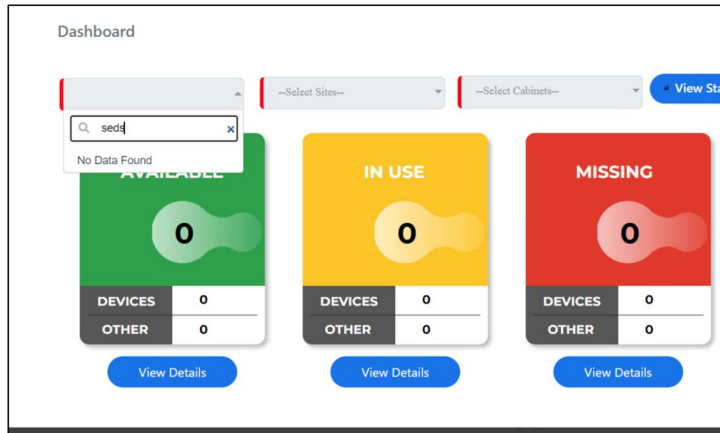
2. Click **View Stats**.

The application displays real-time statistics for a selected Cabinet within a Site of a Company while keep the user on the same page.

Enhanced Device Search (Portal)

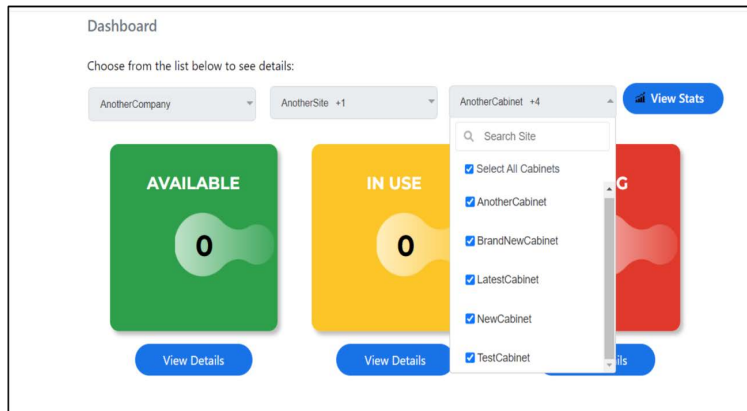
In the ZAMS Portal, users can now search for reports of missing, lost, found, RMA, BER, or repaired devices for a single cabinet. The latest release of the portal has improved this functionality by allowing users to search for devices across multiple cabinets simultaneously.

If you have a **Company Admin** role, you can view a list of all the **Missing Devices** by selecting multiple sites and multiple cabinets in the selected sites. On the other hand, if you have a **Site Admin** role, you can view a list of all the **RMA Devices** by selecting multiple cabinets within your control.



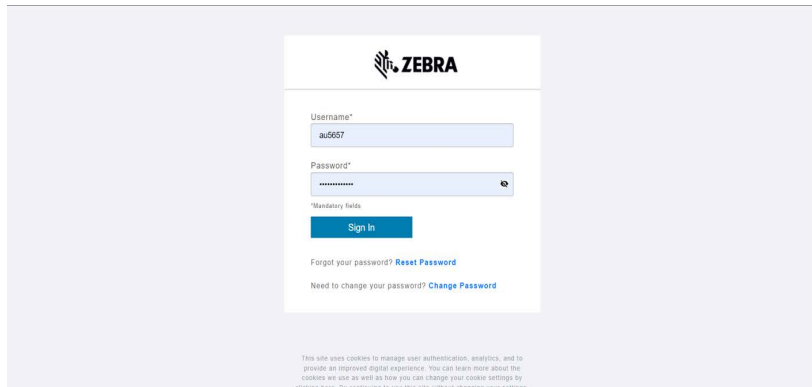
On the dashboard, a **Company Admin** role user can determine the device status by selecting multiple sites and cabinets with the following functions:

- Provide search functionality in drop-down list, which is sorted in alphanumeric order.

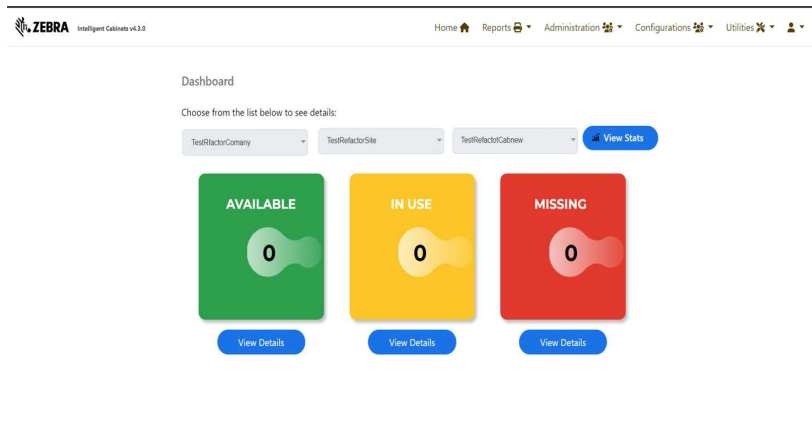


- Users can search for site and cabinet names from the list.
- Users can select or deselect items from the list based on the search results.
- Search functionality is available for the company list of users with the super admin role.
- This search feature applies to both the dashboard and all report screens.

Site Admins can view device status from multiple cabinets, including Missing, Lost, Found, RMA, BER, and Repaired devices reports under **Reports** section. Below is the sample report: Missing Device Report for all cabinets under TestSiteACO.



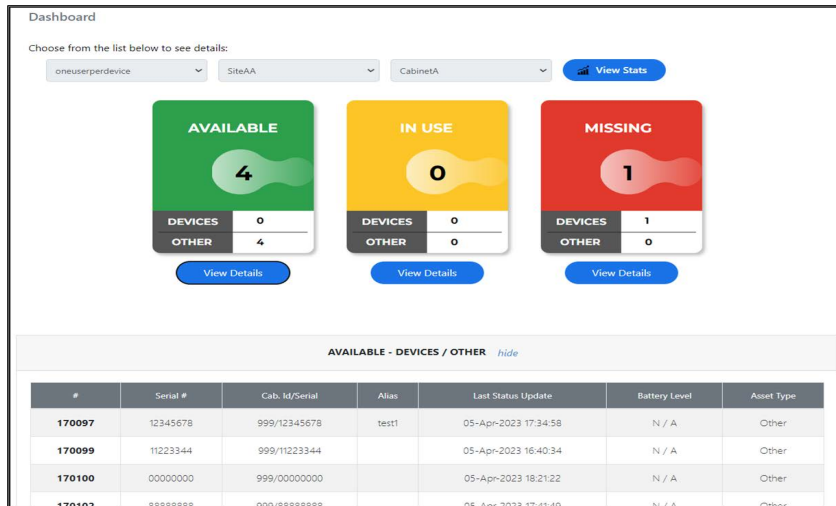
Below is the dashboard showing the status of devices with the option to select multiple sites and cabinets.



Viewing Device Details

To view device details:

1. Click **View** on the dashboard statistics to see details for device sets. The page does not automatically update.



2. The list of devices displays and provides information on each individual device in the selected state which include:

- **On Charge** – The number of devices currently docked in the Cabinet.
- **In Use** – The number of devices removed from the Cabinet and successfully logged in.
- **Missing** – There are three classifications of the Missing status, which cover three reasons for a device not being logged in after it has been removed from the Cabinet.

Status	Status Reason	Details
MISSING	INVALID_LOGIN	Failed to login and the device is not placed.
MISSING	NOT_RETURNED	The user does not return the device on time. Note: Shift duration is set for 8 hours. After 8 hours, the device is not placed in the cradle.
MISSING	COMMUNICATION_LOST	The user logged into the device and then took the device outside the network or disconnected from Wi-Fi.

Finding a Lost Device

1. Click **View Status** for Missing devices in the ZAMS home screen in the portal and make the alarm sound.

2. When the alarm is triggered, the **Send Alarm** button will change to **Sent Alarm**.

The screenshot displays three status cards: AVAILABLE (1 device), IN USE (0 devices), and MISSING (1 device). Below these is a table titled 'MISSING - DEVICES / OTHER' with the following data:

#	Serial #	Cab. ID/Serial	Alias	Last Status Update	Battery Level	User Name	Status Reason	Last User	Mark Device	Asst Ty
8628	18261522504884	11/18261522504884		08-Jul-2020 18:05:10	90		NOT_RETURNED		<input type="checkbox"/> Mark Lost <input type="checkbox"/> Send Alarm	Dev

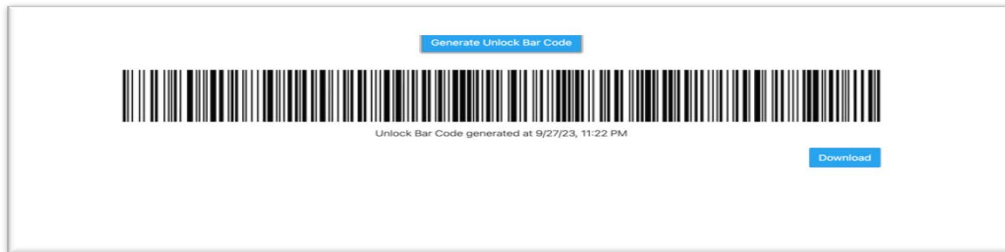
3. After the device is found, the Device User can stop the alarm using any of the following steps:

- Enter the passcode.
- Place the device back into the cradle.
- Scan the QR Code from the UI (Utilities scan).

The screenshot shows the ZAMS portal dashboard with the following navigation menu: Home, Reports, Administration, Configurations, Utilities. The dashboard displays three status cards: AVAILABLE (0 devices), IN USE (0 devices), and MISSING (0 devices). Below the cards are filters for 'Zebra Technologies', 'Select Site', and 'Select Cabinet', along with a 'View Stats' button.

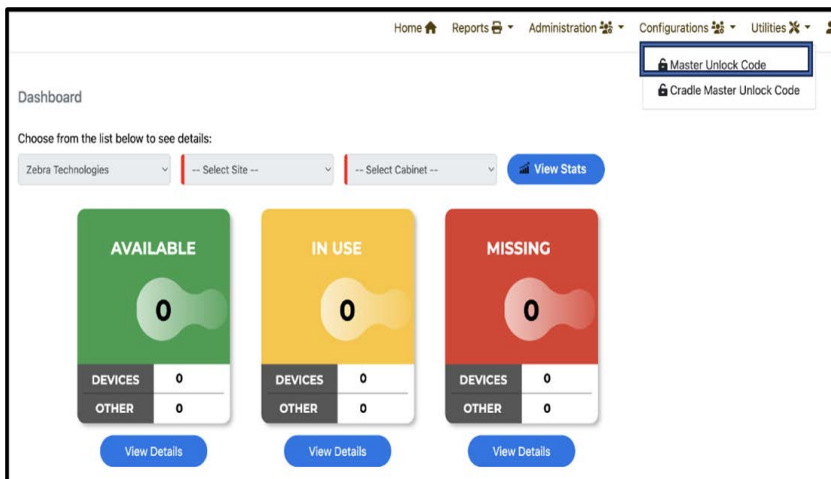
The screenshot shows two buttons: 'Generate Unlock QR Code' (highlighted in blue) and 'Generate Unlock Bar Code'. Below the buttons is a QR code.

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



Master Unlock Code : Finding the Missing Device

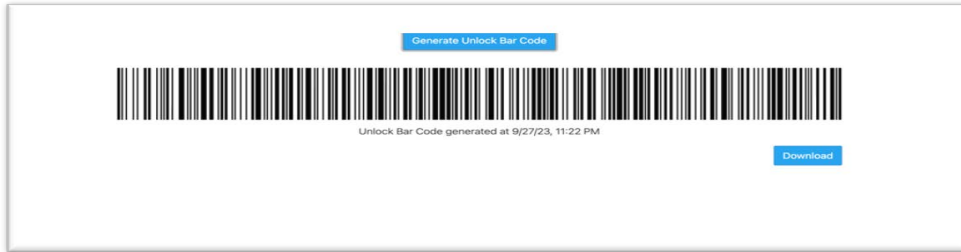
1. Send the alarm from the ZAMS Portal when the device is found.
2. After the device is found, the Device User can stop the alarm using any of the following steps:
 - Enter the passcode.
 - Place the device back into the cradle.
 - Administrator can scan the QR Code from the UI (Utility scan) > Master Unlock Code.



- Scan the QR code from the UI (Utilities scan)



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



Cradle Master Unlock Code: Logging into the Device when Portal/KIOSK are Down

Access the Zebra support portal and generate the Cradle Master Unlock QR code from the Utilities > Cradle Master Unlock Code screen (Wi-Fi is required). This QR code is valid for 48 hours. Any time Wi-Fi (KIOSK and/or Portal) goes down, the user can use this QR code (within 48 hours) and can use it to log in. Device count logins have no limitations.

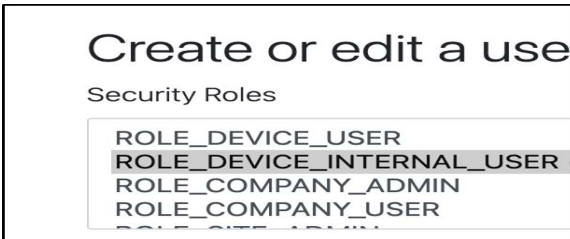
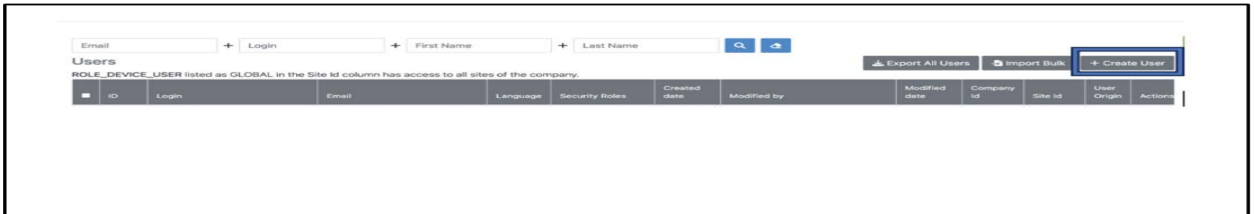
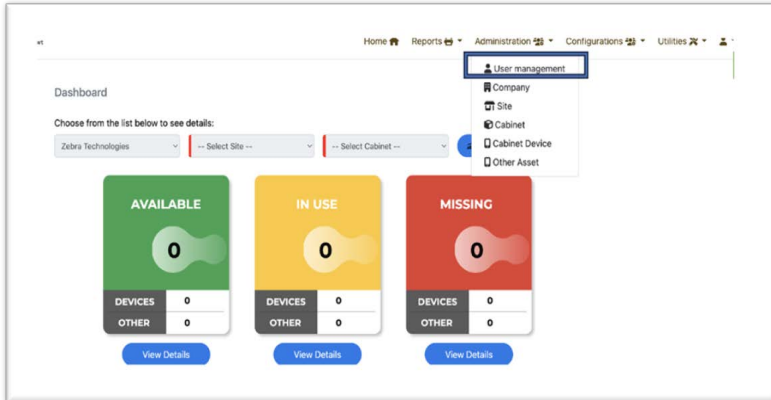


Portal and KIOSK or only KIOSK is down : Break Glass

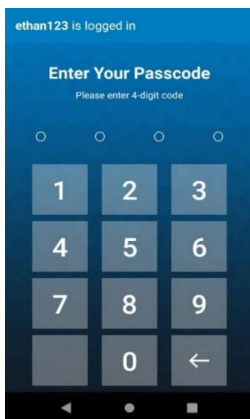
1. To unlock the Cradle Master, use the Cradle Master Unlock Code feature mentioned above.
2. Company admin can assign **ROLE_DEVICE_INTERNAL_USER** to any five employees in each site in User Management. When KIOSK and Portal or only KIOSK goes down, **ROLE_DEVICE_INTERNAL_USER** can log in to the device 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 on every site.



3. Login into device:



Logging into Another Device

If the first device is broken or not functioning, change the company settings to allow logging into another device:

1. Login to the portal and go to the company settings screen to disable **One device user enabled**.
2. Then, try logging in to a second device.

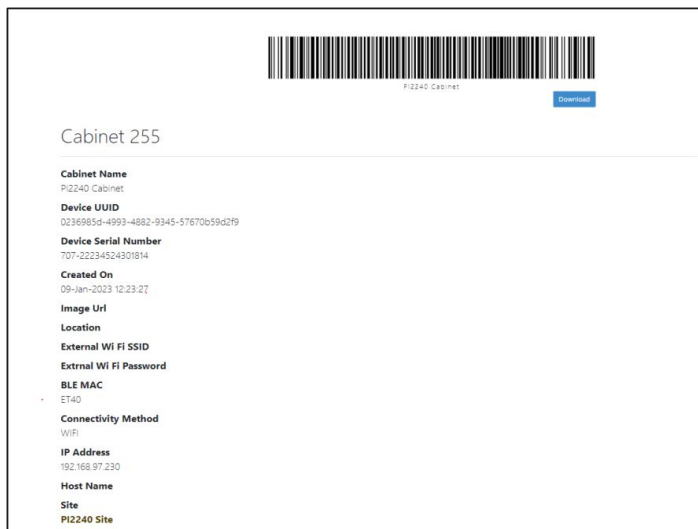
Support for mobile devices equipped with 1D linear barcode scanners

ZAMS allows registering mobile devices with 1D linear barcode scanners (MC33X) which do not have cameras to scan QR codes for registration.

To register MC33x devices to a specific cabinet:

1. Access the portal with a **Company_Admin** or **Site_Admin** roles.
2. Navigate to **Administration**, click **Cabinet**, and select the appropriate option.
3. Select **View** on the cabinet to ensure proper IP address provided.
The barcode displays (see the following image).
4. Download the barcode and copy the barcode onto MS Word.
5. Print a copy of the Word document and paste it into the corresponding physical cabinet.
6. Devices installed with AMS v2.4.0 can register with cabinets by scanning the downloaded barcode.

Please refer to the image below for reference:



NOTE:

- The barcode is generated when the **IP Address** or **Host Name** have values.
- If both **IP Address** and **Host Name** have values, the barcode is generated with **IP Address** by default.
- If the cabinet uses only the **Host Name**, the length should not exceed 23 characters.

Administration

Company

- To set up the company, the super admin can go to the **Administration > Company screen**.
- The super admin or company admin can view or edit the company details.
- If the **One Device User Enabled** feature prevents a user from logging into two devices within one minute. This feature promotes the one device, one user functionality. This functionality is available in all supported versions.

- For one user, one device functionality, an additional sync time of approximately 3 minutes on the configured time (sync frequency) is necessary.

PIN Configuration

The uniqueness level of the PIN is determined by the value selected in the **PIN Uniqueness Set At** field.

- PIN Uniqueness is set to **Company**. If the passcode 3423 is used for Site XXX, it cannot be used for Site YYY or any Global user.
- PIN Uniqueness is set to **Site**. The Site Users in Site XXX and Site YYY can use the same passcode, 3423. However, Global Users cannot use the same passcode.
- PIN Uniqueness is set to **Site**. If the passcode 3423 is used for **Global user**, no other user on the Site XXX or Site YYY can use the same passcode. Additionally, the passcode 3423 cannot be used again by any other Global user.

When the Administrator changes the setting of **PIN Uniqueness Set At** from Company to Site or Site to Company, the passcode field will be null, and the passcode must be reset again for the devices. Suggestion to use this functionality as a time set up to avoid resetting the passcode of all devices.

Site Id/Name
2/Brno

PIN Code (Digits)

Activated

Site

- Super admin, company admin, or site admin can set up the site from **Administration > Site screen**.
- They can also view or edit the site details.
- Checking the **Inherited** option, the Company level setting will override the Site level setting for that specific field.

Contact Mobile Number

Contact Extension

Time Zone
Asia/Kolkata

App Switch Back Interface

Enable Alarm (Inherited?)

Alarm Timeout (Minutes)

Inherited?

Enable Bluetooth Proximity (Inherited?)

Bluetooth Duration (Minutes)

Inherited?

Inherited?

Cancel Save

Cabinet

- Super admin, company admin, or site admin can set up the site from **Administration > Cabinet screen**.

- They can also view or edit the cabinet details.

Intelligent Cabinets v3.3.2-jet

Home Reports Administration Configurations

Create or edit a Cabinet

Company
May Mid Release Company updated

Site

Cabinet Name

Image Url

Location

External Wi-Fi SSID

External Wi-Fi Password

BLE MAC

Connectivity Method

Create or edit a Cabinet

ID
397

Company
ZAMSTESTAa

Site
BALA SITE A

Cabinet Name
BALA CABINET A

Device UUID
d9816214-3fe0-455e-bb56-3f4c15dfd8e1

Device Serial Number
173-19337521400845

Image Url

Location

External Wi-Fi SSID

Un-register

- The device can be enrolled or unrolled with the cabinet from the cabinet edit screen.

Cabinet Device

- Super admin, company admin, or site admin can import devices from the **Administration > Cabinet device screen**.
- They can also view or edit the cabinet device details.

ZEBRA Intelligent Cabinets v3.3.2-jet

Home Reports Administration Configurations Utilities

Site Name Cabinet Name Device Name Device Alias

Cabinet Devices

ID	Device Name	Crib, IQSerial	Alias	Company Id	Site Id	Last Status Update	Status	Actions
----	-------------	----------------	-------	------------	---------	--------------------	--------	---------

Import Devices

User management
Company
Site
Cabinet
Cabinet Device
Other Asset

- To import cabinet devices, click **Import devices** and upload the file.

A sample template has been displayed on the screen.

Bulk upload devices
Update Device alias in bulk by uploading a CSV file with the device's information like Name, Company, and Site.
Required Fields: Following are required fields.
CABINET DEVICE
• Device Name
Notes
• Please make sure your file has 3 columns i.e. Device Name, Alias, Company Id.
[Download Sample Template](#)
Import Devices
Choose file No file chosen
 Input file has header - Please ignore first line

Device Aliases (Friendly Name)

A company can use Device Aliases to have their unique identification of devices. This can be set via portal UI or a CSV file import. Go to **Administration > Cabinet Device > Edit** to add or change the Alias.



NOTE: Alias (Device friendly name) will be displayed on the dashboard and cannot be set or changed on the device by the user.

Create or edit a Cabinet Device
ID
170090
Device Name
22294523021582
Cab. Id/Serial
999/22294523021582
Alias

CSV Import for Device Alias

1. This CSV bulk import option can be accessed via the Import Alias (friendly name) CSV file in the Portal. To access it, the Company-Admin must go to **Administration > Cabinet Device**.
2. The **Import Device** button will be displayed on the top right corner after the page loads.

ZEBRA Intelligent Cabinets v3.2.1-jwt
Home Reports Administration Configurations Utilities

Site Name Cabinet Name Device Name Device Alias

Cabinet Devices

ID	Device Name	Cab. Id/Serial	Alias	Company Id	Site Id	Last Status Update	Status	Cabinet	Actions
170090	22294523021582	999/22294523021582		353	673	06-Apr-2023 11:02:54	LOST	CabinetA	View Edit
170091	210965225D0079	999/210965225D0079		353	673	06-Apr-2023 20:00:01	LOST	CabinetA	View Edit
170093	210965225D0079	1000/210965225D0079		353	673	05-Apr-2023 22:41:41	LOST	CabinetB	View Edit

- Click on the button, and a new page will load. This page displays all the details regarding Bulk Import Alias CSV file import. This page mentions all the requirements, including the template and the Upload Link.



NOTE: Select the **Input file has header - Please ignore first line** checkbox to not show the first row as a header in the CSV file.

Import Devices

Choose File No file chosen Import

Input file has header - Please ignore first line

- If the check box is select, the first row of the CSV will not be header.
- If the check box is deselect, the first row of the CSV will still be processed.



NOTE: It is important for the alias to be unique within the company's domain.

- After selecting the correct file, click **Import**. The file will then be processed, and a message will be displayed.

Operation completed : [Download Report.](#)

- Access the option to search for a device by Alias or Device Name at **Administration > Cabinet Device**.

Site Name Cabinet Name Device Name Device Alias

Cabinet Devices

Other Asset

- Devices that are not Android devices and not connected to charge, fall under the **Other Asset** category. Examples include ring scanners, hammers, and helmets. **Other Asset** do not have **Alarm Functionality**.
- During shift hours, while the device is being used, it will be categorized as **In use** along with other asset devices. If the device is not returned after the shift duration, it will be moved to the **Missing** category. At this point, the administrator can choose to mark the device as **Lost** if it has not been returned.
- Other Asset** hashas **Asset ID** or **Barcode** linked to each device. **Other Asset** will be registered with Asset ID to the Portal.
- The **Other Asset** feature for the Portal can be enabled or disabled from the Company settings screen.

Alarm Timeout (Minute)

Enable Bluetooth Proximity

KIOSK Port

PIN Length

Host Resolution

Shift Duration (Minute)

Alarm Enabled

Charging Screen Visible

One Device User Enabled

Auto Alarm after Shift Timeout

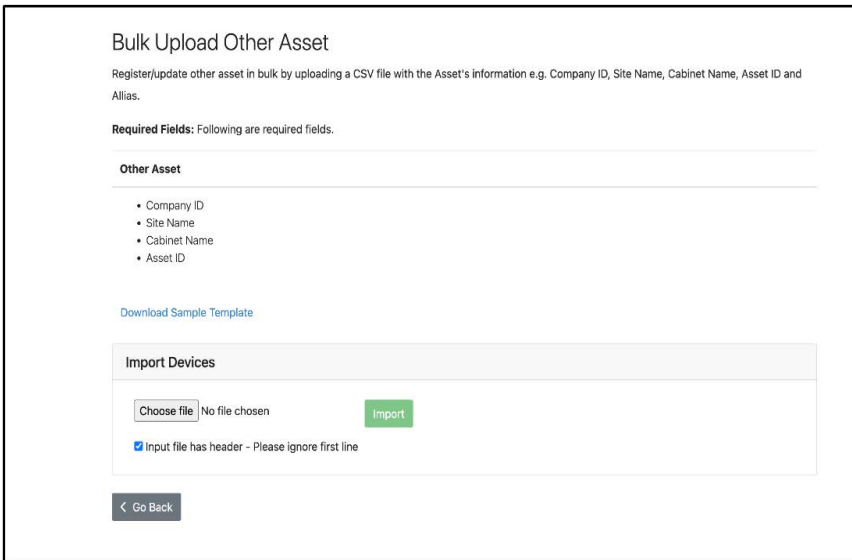
Enable Other Assets

- Super admin, company admin, or cite admin can import or register **Other Asset** from **Administration > Other Asset** screen.
- Super admin, company admin, or site admin can view or edit the Other Asset details.



Import Other Asset

- To import other asset, click **Other Asset** and upload the file.
- A sample template has been displayed on the screen.

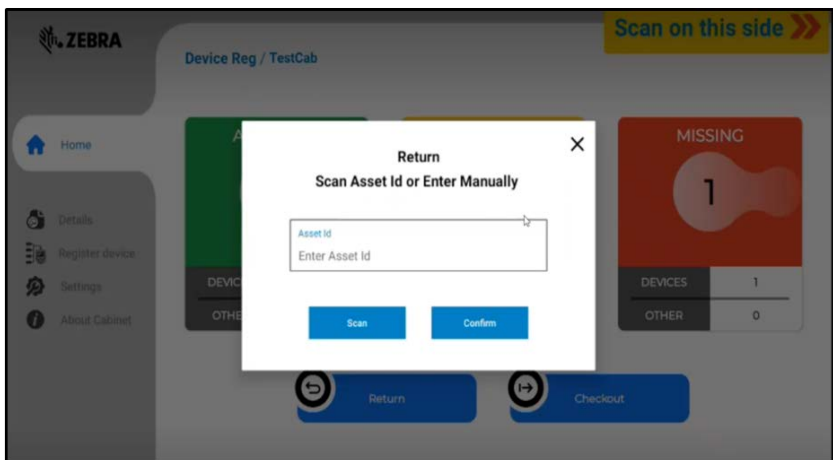
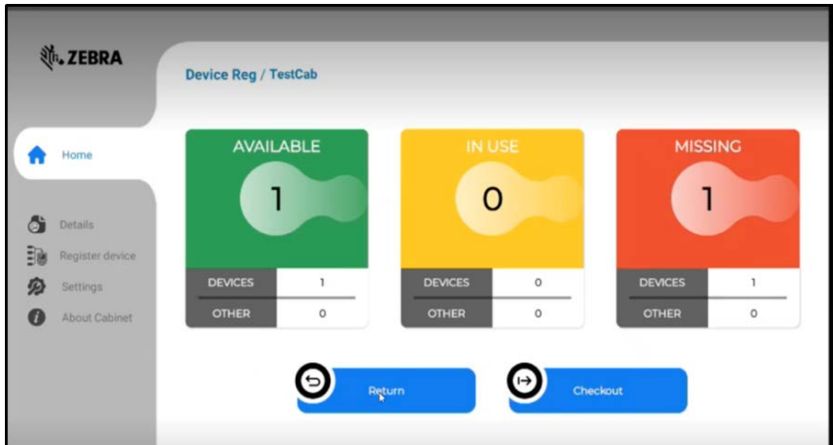



Register Other Asset



Registration of Other Asset via KIOSK

The Other Asset registration can be completed via **Return > Enter Asset ID > Scan**. It requires the Site Administrator's PIN and can be done by either the Company or Site Administrator.

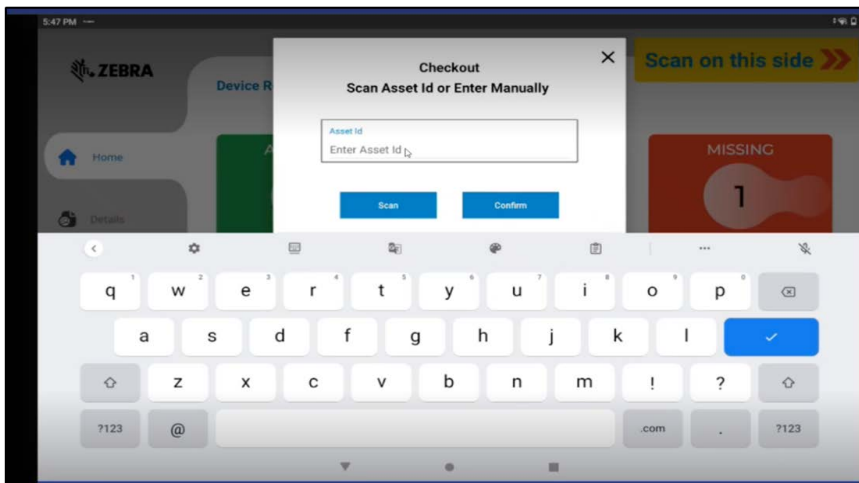
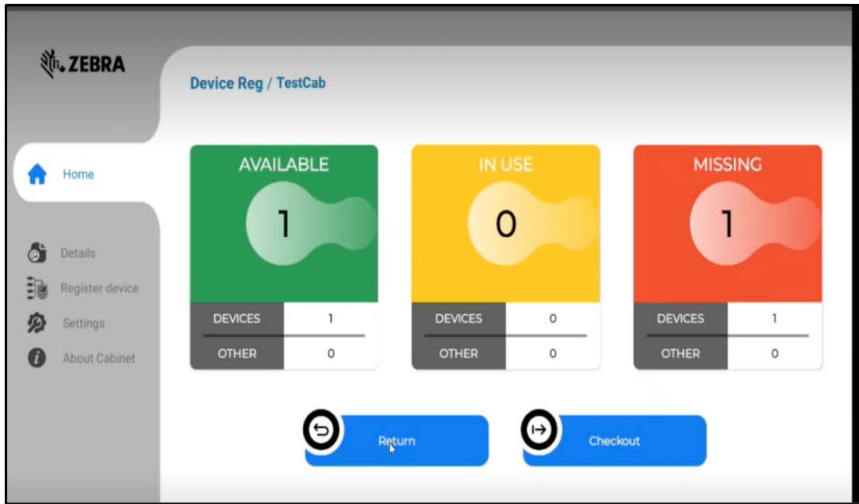


 **NOTE:** Only Site Administrators can register and check out devices from KIOSK. Registration by company administrators must be done through the Portal.

Check Out Process

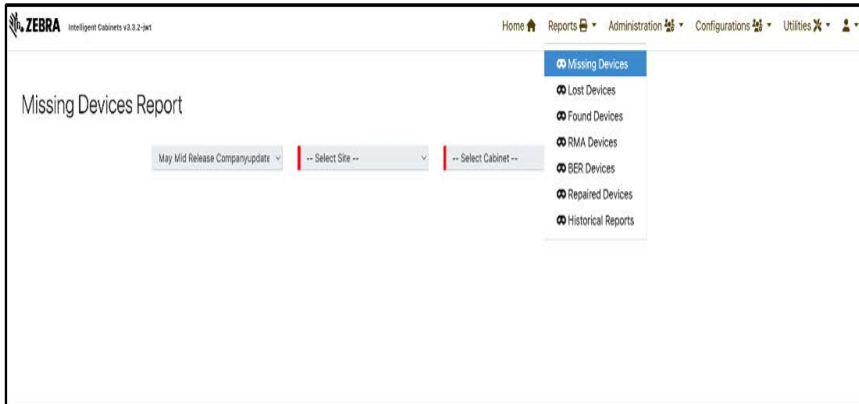
1. The **ROLE** device user will interact with the KIOSK by selecting checkout.
2. Upon selecting the checkout function, the user will select **SCAN**, and then the scanner will be activated on the KIOSK.
3. Scan the asset you desire to checkout and select confirm, then the user will be requested to enter their PIN code.

- This feature only works with implementations whereby the PIN code is the established authentication method.



Reports

All the reports are available under the **Report** section.



Missing Devices Report

The Cabinet has devices that are not logged in. Missing status has three classifications and covers three reasons: Not_Returned, Invalid_Login, Communication_Lost.

To view a missing devices report:

1. Select the **Location** and **Cabinet** that you want to see the Missing devices.
2. Click **View Stats**. The report lists the below information:

Lost Devices

When a device is marked as lost, it is removed from the list of active devices in ZAMS and will no longer appear as missing.

To mark a mobile device as lost, you can use the pages listed below:

1. Dashboard or Home.
2. Go to **Administration > Cabinet Device > Choose cabinet > Click Edit > Mark as Lost** in Cabinet Device List.

From the dashboard, mark the device as Lost.

The dashboard shows three status cards: AVAILABLE (1), IN USE (0), and MISSING (1). Below them is a table titled 'MISSING - DEVICES' with the following data:

#	Serial #	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Status Reason	Last User	Mark Device
178	22186523025343	93/22186523025343		22-Jun-2023 13:00:00	100	DeviceUser	NOT_RETURNED	DeviceUser	Mark Lost RMA Send Alarm

Found Devices

The administrator can mark the device as **Found** when returned.

Go to **Administration > Cabinet Device > Select the cabinet > Edit > Mark as Lost**.

The 'Found Devices Report' interface includes filters for 'May Mid Release Companyupdate', 'MaranoorSite', and 'MaranoorCabinet', with a 'Show' button. Below the filters is a table titled 'List of Found devices:' with the following columns: #, Device Name/Asset ID, Cab. Id/Serial, Alias, Last Status Update, and Asset Type.

RMA Devices

The 'RMA Devices Report' interface includes filters for 'Dev Test Company', 'Test Site', and 'Mycab_1', with a 'Show' button. Below the filters is a table titled 'List of RMA Devices' with the following data:

Reference Number	Device Name/Asset ID	Cabinet ID/Serial Number	Alias	Last status update	Asset Type
1	2217452322563	1/2217452322563		Feb 23, 2021	Device
2	2034952302323	1/2034952302323		Feb 23, 2021	Device
3	2109652300079	1/2109652300079		Feb 23, 2021	Device
4	22186523025343	1/22186523025343		Feb 23, 2021	Device

BER Devices

BER or beyond Economical Repair are devices that were sent for repair but were not repaired successfully and will not be returned.

Reference Number	Device Name/Asset ID	Cabinet ID/Serial Number	Alias	Last status update	Asset Type
1	2217452252563	1/2217452252563		Feb 23, 2021	Device
2	20349123023233	1/20349123023233		Feb 23, 2021	Device
3	21096522500079	1/21096522500079		Feb 23, 2021	Device
4	22186523025343	1/22186523025343		Feb 23, 2021	Device

Repaired Devices

List of devices that were returned from the repair shop after successful repairs.

#	Device Name/Asset ID	Cab. ID/Serial	Alias	Last status update	Asset Type
---	----------------------	----------------	-------	--------------------	------------

Historical Reports

Historical Reports can be exported to CSV and PDF formats. As mentioned above, only Company Admin and Company User can generate and Export Historical reports to CSV in addition to PDF format.

A Site Admin can only generate and Export Historical Reports for the relevant Site. There are four types of historical reports:

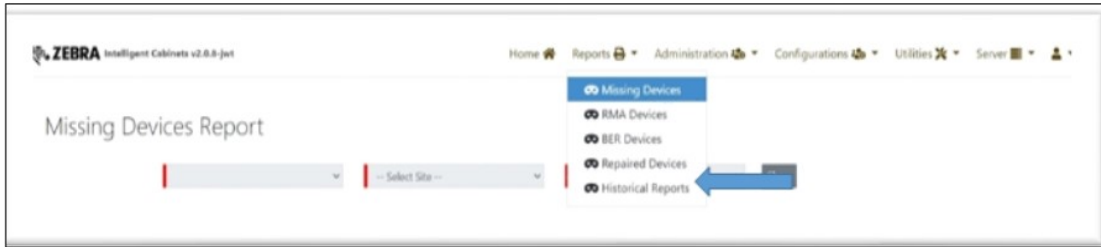
- [Cabinet Devices Report](#)
- [Device Status Report](#)
- [User Device Report](#)
- [User Metrics Report \(Portal\)](#)

Generating Historical Reports

To generate and download reports:

1. Log in to the Portal using Company Admin credentials.

2. Click on **Reports** from the top tabs.
3. Click on **Historical Reports** from the drop-down menu. The Historical Reports screen displays.



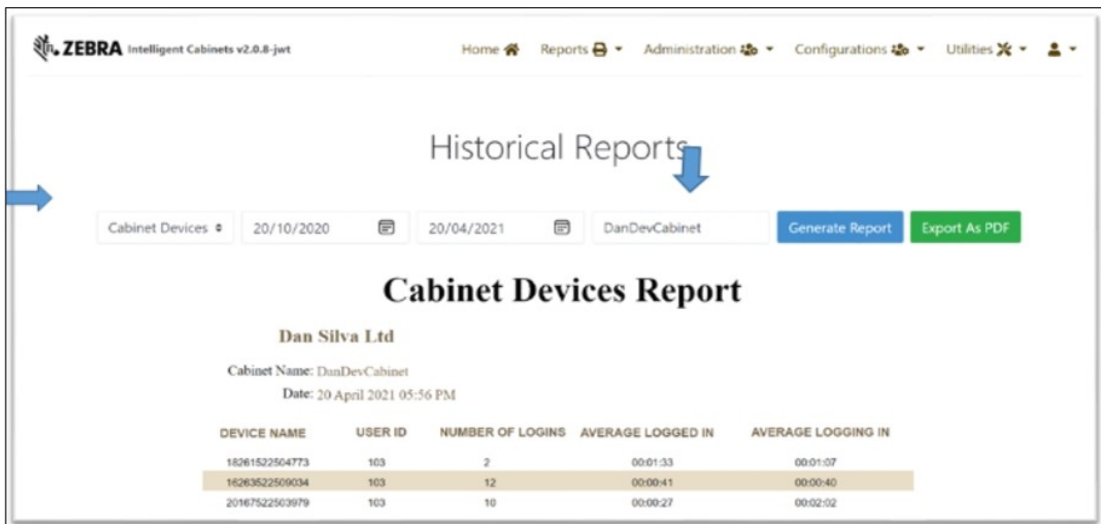
4. Select the desired report to generate from the **Select Report** drop-down menu.



Cabinet Devices Report

To generate a Cabinet Devices Report:

1. Select the desired date from the **Begin Date** field.
2. Select the desired date from the **End Date** field.
3. Enter the **Cabinet name** (for example: DanDevCabinet).
4. Click on **Generate Report**.



Device Status Report

To generate a **Device Status Report**:

1. Select the desired date from the **Begin Date** field.
2. Select the desired date from the **End Date** field.

3. Enter the **Device name** (example: DanDevCabinet).
4. Click on **Load Cabinet**. All the cabinets associated with s/n of the Device Name entered loads.
5. There are two report generation options:
6. If a cabinet is not selected and **Generate** is selected, the complete history of the Device Status Report loads (device associated with all the cabinets in the selected date range). Cabinet name **Multiple** generates a complete list with all the cabinets the device has been associated and all relevant data.

Historical Reports

Device Status: 20/10/2020 - 20/04/2021 16263522509034 Load Cabinets Generate Report Export As PDF

Device Status Report

Dan Silva Ltd

Device Name: 16263522509034
Cabinet Name: <Multiple>
Date: 20 April 2021 06:12 PM

USER ID	CABINET	PREVIOUS STATE	PREVIOUS STATE TIME	NEW STATE	NEW STATE TIME	BATTERY LEVEL (%)
0	DanDev1	MISSING	17 Nov 2020 06:10:23 PM	ON_CHARGE	17 Nov 2020 06:18:09 PM	100
0	DanDev1	ON_CHARGE	17 Nov 2020 06:18:09 PM	MISSING	17 Nov 2020 06:18:28 PM	100
100	DanDev1	MISSING	17 Nov 2020 06:18:28 PM	IN_USE	17 Nov 2020 06:18:38 PM	100
0	DanDev1	IN_USE	17 Nov 2020 06:18:38 PM	ON_CHARGE	17 Nov 2020 06:26:21 PM	99
0	DanDev1	ON_CHARGE	17 Nov 2020 07:14:27 PM	MISSING	17 Nov 2020 07:15:04 PM	100
100	DanDev1	MISSING	17 Nov 2020 07:15:04 PM	IN_USE	17 Nov 2020 07:15:36 PM	100
0	DanDev1	IN_USE	17 Nov 2020 07:15:36 PM	MISSING	17 Nov 2020 09:14:25 PM	99
0	DanDev1	MISSING	20 Nov 2020 05:43:00 PM	ON_CHARGE	20 Nov 2020 05:44:55 PM	95
0	DanDev1	ON_CHARGE	20 Nov 2020 05:44:55 PM	MISSING	20 Nov 2020 05:44:56 PM	95
100	DanDevCabinet	MISSING	23 Dec 2020 02:28:57 PM	IN_USE	23 Dec 2020 02:29:04 PM	43
0	DanDevCabinet	IN_USE	23 Dec 2020 02:29:04 PM	ON_CHARGE	23 Dec 2020 02:29:37 PM	100
0	DanDevCabinet	ON_CHARGE	23 Dec 2020 02:35:41 PM	MISSING	23 Dec 2020 02:35:44 PM	99
100	DanDevCabinet	MISSING	23 Dec 2020 02:35:44 PM	IN_USE	23 Dec 2020 02:35:51 PM	99
0	DanDevCabinet	IN_USE	23 Dec 2020 02:35:51 PM	ON_CHARGE	23 Dec 2020 02:36:10 PM	99
0	DanDevCabinet	ON_CHARGE	23 Dec 2020 02:36:10 PM	MISSING	23 Dec 2020 02:36:14 PM	99
100	DanDevCabinet	MISSING	23 Dec 2020 02:47:46 PM	IN_USE	23 Dec 2020 02:48:00 PM	96

7. If a Cabinet is selected and **Generate** is selected, the Device Status Report only for that specific cabinet in the selected date range generates.

Historical Reports

Device Status: 20/10/2020 - 20/04/2021 16263522509034 Load Cabinets DanDevCabinet Generate Report Export As PDF

Device Status Report

Dan Silva Ltd

Device Name: 16263522509034
Cabinet Name: DanDevCabinet
Date: 20 April 2021 06:12 PM

USER ID	CABINET	PREVIOUS STATE	PREVIOUS STATE TIME	NEW STATE	NEW STATE TIME	BATTERY LEVEL (%)
100	DanDevCabinet	MISSING	23 Dec 2020 02:28:57 PM	IN_USE	23 Dec 2020 02:29:04 PM	43
0	DanDevCabinet	IN_USE	23 Dec 2020 02:29:04 PM	ON_CHARGE	23 Dec 2020 02:29:37 PM	100
0	DanDevCabinet	ON_CHARGE	23 Dec 2020 02:35:44 PM	MISSING	23 Dec 2020 02:35:44 PM	99
100	DanDevCabinet	MISSING	23 Dec 2020 02:35:44 PM	IN_USE	23 Dec 2020 02:35:51 PM	99
0	DanDevCabinet	IN_USE	23 Dec 2020 02:35:51 PM	ON_CHARGE	23 Dec 2020 02:36:10 PM	99
0	DanDevCabinet	ON_CHARGE	23 Dec 2020 02:36:10 PM	MISSING	23 Dec 2020 02:36:14 PM	99
100	DanDevCabinet	MISSING	23 Dec 2020 02:47:46 PM	IN_USE	23 Dec 2020 02:48:00 PM	96

User Device Report

The generate a **User Device Report**:

1. Select the desired date from the **Begin Date** field.
2. Select the desired date from the **End Date** field.
3. Enter the **User ID**.

4. Click **Generate**.

Historical Reports

User Devices 20/10/2020 20/04/2021 Alex Smith [Generate Report](#) [Export As PDF](#)

User Devices Report

Dan Silva Ltd

User Id: 103
 First Name: Alex
 Last Name: Smith
 Date: 20 April 2021 06:29 PM

DEVICE NAME	USER NAME	NUMBER OF LOGINS	LOGGED IN	AVG LOGGED IN	LOGGING IN	AVG LOGGING IN	PAST TIME
8024352380034	1234 1234	7	02:21:59	00:23:36	00:28:36	01:24:26	0
8729952382009	1234 1234	1	00:00:00	00:00:00	00:00:00	00:00:00	0
8024352380773	1234 1234	2	00:01:33	00:01:33	00:02:16	00:01:07	0
8024352380034	1234 1234	12	00:02:64	00:00:41	00:02:42	00:00:40	0
2014752383079	1234 1234	10	00:02:43	00:00:27	00:12:17	00:02:02	0

Total Number of Logins: 32 Total logged in time: 02:28:27

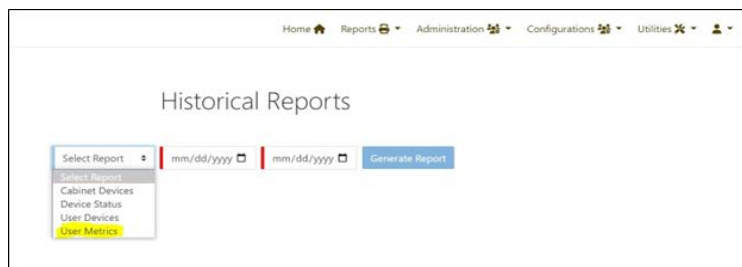
User Metrics Report (Portal)

A new Historical Report now displays device usage data for users. The report includes the following details:

- The serial number of the device.
- The time at which the user logged into and out from the device.
- The total time the user spent on the device in each session (from login to logout).
- The total number of logins.
- The total time the user has used the device until the report is generated.

This report is available on the ZAMS Portal and can be exported as a PDF or CSV file.

Users can access the **User Metrics** report by navigating to **Reports > Historical Reports > Select Report > User Metrics**.



Below is the sample User Metrics Report:

Historical Reports

User Metrics | 02/01/2024 | 02/26/2024 | user1 | [Generate Report](#) | [Export As](#)

User Metrics Report

UserMetricsTestCompany

User Id: 9246
 Device Login: user1
 First Name: user
 Last Name: one
 Start Date: 01 Feb 2024
 End Date: 26 Feb 2024

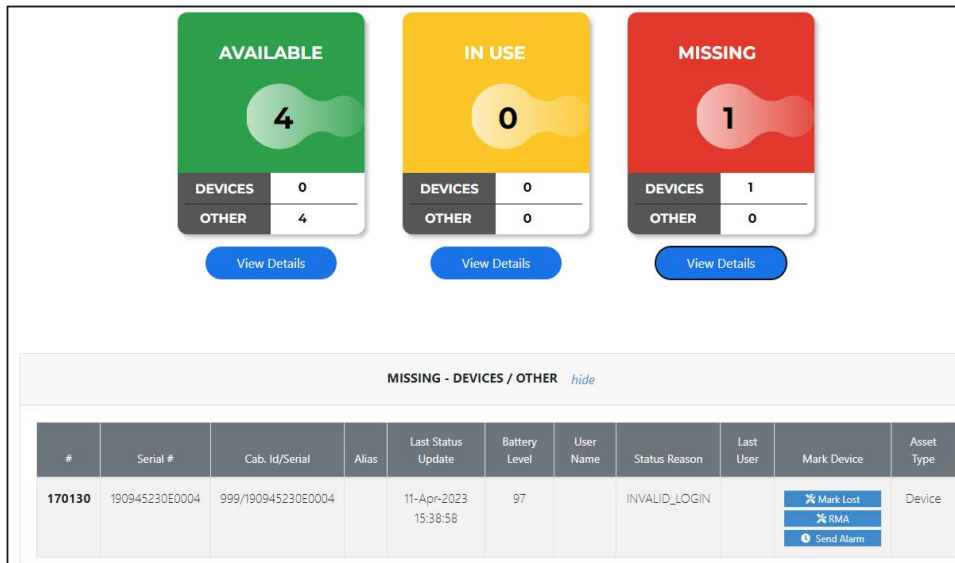
DEVICE NAME	CABINET NAME	LOGGED IN AT [i]	HANDOVER / RETURN AT [i]	USAGE TIME [i]
22165523021315	UserMetricsTestCabinet	06 Feb 2024 10:00:00 PM	06 Feb 2024 10:10:28 PM	00:10:28
22165523021315	UserMetricsTestCabinet	06 Feb 2024 10:14:06 PM	06 Feb 2024 10:17:16 PM	00:03:10
22165523021315	UserMetricsTestCabinet	07 Feb 2024 11:44:12 AM	07 Feb 2024 12:24:38 PM	00:40:26
22165523021315	UserMetricsTestCabinet	21 Feb 2024 11:27:34 AM	21 Feb 2024 11:34:40 AM	00:07:06
22165523021315	UserMetricsTestCabinet	21 Feb 2024 12:08:05 PM	21 Feb 2024 12:33:39 PM	00:25:34
22165523021315	UserMetricsTestCabinet	21 Feb 2024 01:20:19 PM	21 Feb 2024 01:21:44 PM	00:01:25

Monday, 26 February 2024 Page 1 of 2

Alarms: Send Alarms & Auto Alarms

1. The dashboard now features a **Send Alarm** button for both in-use and missing devices, located in the Device Column List.
2. Pressing this button will send an internal message to the Mobile Device via the KIOSK, prompting for login.
3. If the Mobile Device is on the same network as the KIOSK, the PIN screen will appear on the device's screen upon successful communication.
4. The alarm timeout begins with the ZAMS log-in screen UI.
5. If the user does not log in within the 2 minutes (or configurable Alarm timeout of the Company), the device alarms until:
 - a. The battery is dead.
 - b. The user logs in by entering a valid PIN.
 - c. The device returned to the charger, and it is in range.

- d. The Domain QR 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.



The **Send Alarm** functionality will not apply to devices in the Missing State with the Communication_Lost reason type.

On the dashboard, the **Send Alarm** will change to **Sent** after being tapped. The portal will communicate with the KIOSK, and the KIOSK will send the Alarm notification to the device. The **Sent** button will automatically change to “Send Alarm” within one minute.

The **Send Alarm** button is also available in the Actions columns in the Administration Cabinet Devices list. All the rules are applicable as described above. There is only one exception: after 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 that the “sent” button will not automatically revert to **Send Alarm**. The page needs to be refreshed to take effect.

Auto Alarm

An **Auto Alarm** configuration option enables missing devices to automatically sound an alarm until they are found.

From the dashboard, go to **Administration > Company** scroll down to find the check box.

If checked, the device will alarm automatically when not returned to the cradle after shift timeout.

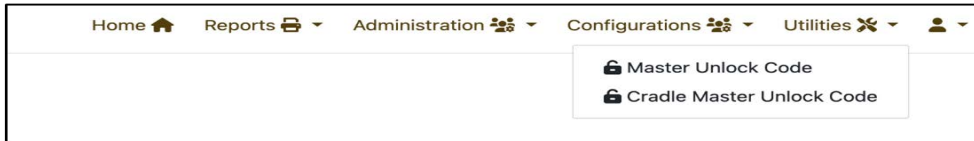
- ZAMS client on Mobile Device based on shift duration.
- On Mobile Devices, if the shift duration has expired, the login screen displays on the UI.

- If the user does not log in within 2 minutes (configurable Alarm timeout), the device alarms until either the battery is dead, the user logs in, or the device is returned to the cabinet/charger and in range. Also, the domain unlock barcode is scanned, and 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.

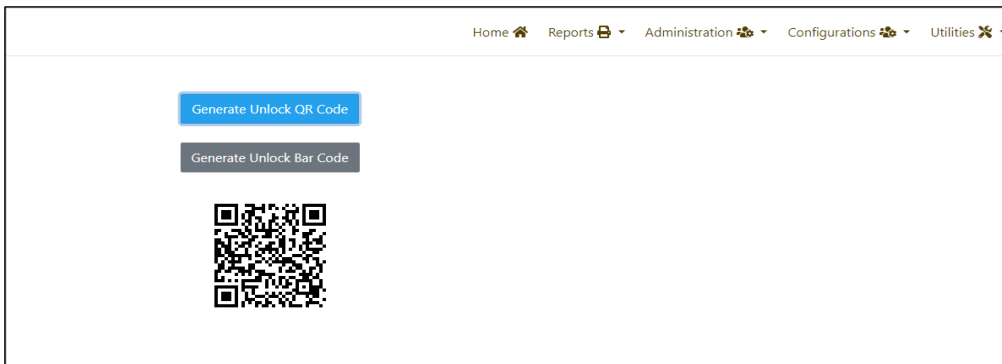
Generating Unlock Code

To generate a QR Code to unlock devices in the event of a power failure:

1. Select **Master Unlock Code** from the **Utilities** drop-down menu.



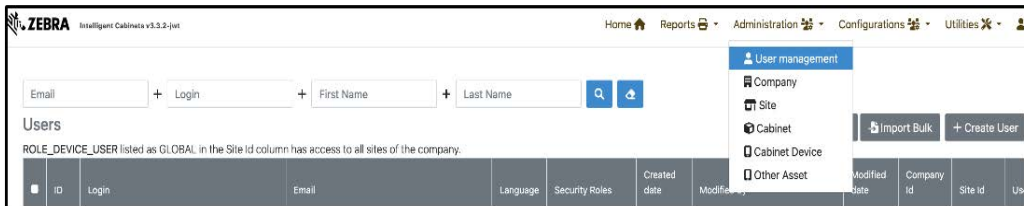
2. Select **Generate Unlock QR Code**.
3. Scan the QR Code from the portal to unlock the mobile device.



NOTE: The QR code is set to expire after 48 hours after being generated. The Qr code is unique for every company. The administrator generates the QR code.

User Management

Administrators can add users from the Portal **Create User** or **Bulk User** functionality.



Import Bulk

Administrators can import multiple users at a time using **Import Bulk**. A sample file is added to the screen.

Bulk upload users
Add users in bulk by uploading a CSV file with users' information like Name, Email, and Password.

Required Fields: Following are required fields.

ROLE_COMPANY_ADMIN	ROLE_COMPANY_USER	ROLE_DEVICE_USER	ROLE_SITE_ADMIN
<ul style="list-style-type: none"> Email First name Last name Password Company Id 	<ul style="list-style-type: none"> Email First name Last name Password Company Id 	<ul style="list-style-type: none"> First name Last name Company Id Site Name or None (For Global User) Device Login PIN Code (4-10) digits 	<ul style="list-style-type: none"> Email First name Last name Password Company Id Site Name Device Login PIN Code (4-10) digits

Notes

- Email for device user is optional, if entered then it will be reflected as contact email.
- Password must be (8-50) characters and should contain at least one upper case, one lower case, a digit and a special character [@ # \$ % ! . ,].
- Device login must be (3-30) characters and can contain alphabets, digits and special characters from [_ - .].

[Download Sample Template](#)

Import Users

No file chosen



NOTE: ROLE_DEVICE_INTERNAL_USER cannot be added through the “Import Bulk” functionality.

Adding a Device User

A Company Admin can create device users as follows:

1. Log in to ZAMS web portal as Company Admin.
2. Go to **Administration > User Management**.
3. Click on **Create User**.
4. Select Role as **Role_Device_User/ Role_Company_Admin / Role_Company_User/Role_Site_Admin/ ROLE_DEVICE_INTERNAL_USER**.
5. Provide a unique email address that has not been used before.
6. Enter first name and last name.
7. Enter device login.
8. Select Company from the drop-down menu.
9. Enter a unique PIN code. The app provides information on how many digits based on the Company PIN code configuration. This PIN should be unique as it identifies the user to the system.
10. Check the **Activated** box.
11. Select the default language.
12. Save the record.



NOTE: If the email address or the PIN code already exists, an error message displays at the top of the screen and disappears after a few seconds.

Device User Roles

Different user roles can be assigned while creating a new user, as shown in the screenshot below.

The screenshot shows a web form titled "Create or edit a user". Under the heading "Security Roles", there is a dropdown menu. The dropdown is open, displaying four options: "ROLE_DEVICE_USER" (which is highlighted in blue), "ROLE_DEVICE_INTERNAL_USER (40 Remaining of max 45 user allocations)", "ROLE_COMPANY_ADMIN", and "ROLE_COMPANY_USER". Below the dropdown menu is a text input field labeled "First name".

- **SITE ADMIN:** A Site_Admin has valid credentials to access the ZAMS Portal and have a limited role in accessing the relevant company data. Site Admin has access to:
 - The dashboard where they can only view stats of their site and cabinets registered to that site.
 - Register KIOSK with valid credentials.
 - Device User Login Credentials in addition to being a Site Admin. Therefore, additional user fields are needed when creating the user.
 - Create Notification Configuration (Email Alerts) for the relevant site.
 - Generate reports for his site only.
 - Site Admin has only access to:
 - Admin Users (User Management)
 - Admin Company – Read Only.
 - Site Admin has access at site level for the following:
 - **Administration > Site Authority** to Create and Edit a Site.
 - Site Admin has the authority to create new cabinets. View and Edit access for corresponding Cabinets for the site.
 - Generate a QR code from the Utilities Menu if needed.
- **COMPANY USER:** A Company User has valid credentials to access the ZAMS Portal. Below are the functions:
 - A Company User has full access to generate and export reports in addition to having access to generate QR codes.
 - A Company User has Read Only access to the following:
 - Dashboard
 - **Administration > User Management**
 - **Administration > Site Administration > Cabinet o Administration > Cabinet Device.**
- **DEVICE USER:** There are two types of device users: A Particular Site and Global.

A device user for a particular site has restricted access to check out a Device. A Device User can only check out a Mobile Device associated with the Site using their PIN code. If the Device's PIN code associated with a particular site is entered on a Mobile Device Associated with another site, an error will be displayed: **Invalid PIN.**

Device Users with the attribute **Global** can access any site associated with the Company. A Device user can use their PIN code to check out a Mobile Device from any of the sites belonging to the company. A user is assigned to a site 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.

Deleting Users

Company Admins can delete users in bulk by selecting the check box and clicking **Delete Multiple**.



Caution: When a user is deleted, all user-related information will also be deleted.

ID	Login	Email	Language	Security Roles	Created date	Modified by	Modified date	Company Id	Site Id	User Origin	
59931	gourione@zebra.com	gourione@zebra.com Activated	en	ROLE_COMPANY_ADMIN	04-Apr-2023 14:15:13	muralikrishna.vedantam@zebra.com	04-Apr-2023 14:17:35	353	N/A	AMS	
<input checked="" type="checkbox"/>	59932	1234@oneuserperdevice	1234@oneuserperdevice Activated	en	ROLE_DEVICE_USER	04-Apr-2023 14:22:14	gourione@zebra.com	11-Apr-2023 14:14:52	353	GLOBAL	AMS
<input checked="" type="checkbox"/>	59933	deluserp@oneuserperdevice	deluserp@oneuserperdevice Activated	en	ROLE_DEVICE_USER	04-Apr-2023 14:22:45	gourione@zebra.com	03-May-2023 19:46:36	353	GLOBAL	AMS

A company admin can delete a single user at a time.

Email	Language	Security Roles	Created date	Modified by	Modified date	Company Id	Site Id	User Origin	Actions
may@zebra.com	gourimay@zebra.com Activated	en	02-May-2023 12:04:57	gourimay@zebra.com	13-Jul-2023 09:52:41	7	N/A	AMS	View Edit Delete

Bulk User Export

Under **Administration > User Management**, click **Export All Users** to export all existing users to a CSV file. This is a feature for the company administrator only.

ID	Login	Email	Language	Security Roles	Created date	Modified by	Modified date	Company Id	Site Id	User Origin	
		com	en	ROLE_COMPANY_ADMIN	04-Apr-2023 14:15:13	muralikrishna.vedantam@zebra.com	04-Apr-2023 14:17:35	353	N/A	AMS	
<input checked="" type="checkbox"/>	59932	1234@oneuserperdevice	1234@oneuserperdevice Activated	en	ROLE_DEVICE_USER	04-Apr-2023 14:22:14	gourione@zebra.com	11-Apr-2023 14:14:52	353	GLOBAL	AMS
<input checked="" type="checkbox"/>	59933	deluserp@oneuserperdevice	deluserp@oneuserperdevice Activated	en	ROLE_DEVICE_USER	04-Apr-2023	gourione@zebra.com	03-May-	353	GLOBAL	AMS

When logged in as Company admin, ensure the site name and site field are entered correctly for other device users in the CSV files while uploading in bulk. If anything else is entered apart from the correct site name or Global in the site field for the device user, the record will not be processed.

When logged in as Site admin, you can upload a CVC to the ZAMS portal and have the privilege to import or update new device users. Ensure the site name entered is correct. Incorrect or blank fields will not be processed.

Cradle Lock

Device Security (Only for TCx series)

The Zebra AMS system aims to improve device management by providing a logging-based system that maintains a record of who has taken what device, and when it was returned. This system will significantly reduce device loss by making users aware that an action is being recorded whenever they take a device and log onto it. The user returning the device to the cradle is also logged, and this action of docking the device logs them out of the device. This system will significantly affect the casual loss of devices by encouraging users to return their devices.

The cradle lock takes the device security to the next level, whereby the devices are physically retained in the cradle until a valid unlock code is entered into the device.

Able unlock the device from the cradle by scanning with the Master QR Code, which can be generated from the portal as described in the above steps, on an emergency basis. The QR code is used when the KIOSK/PORTAL is down.

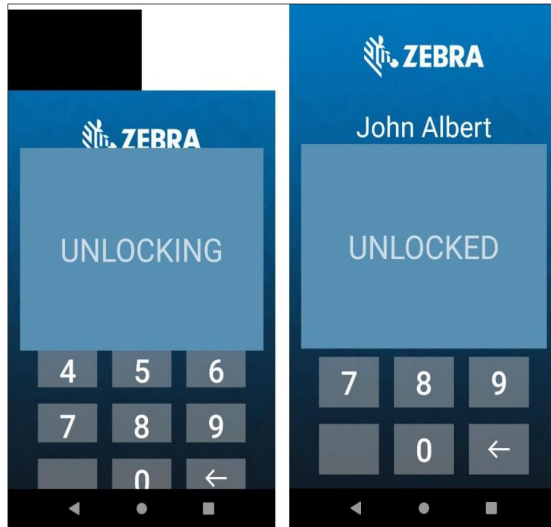
Figure 5 Cradle Lock, Cradle & Devices



Using the Cradle Lock

1. Swipe the battery icon or tap on Log.
2. Enter a PIN while the device is docked and locked in the cradle lock.
 - If the entered PIN is invalid, a message displays **Invalid PIN entry – Please, try again.**

- If a valid PIN is entered, the following messages are displayed.



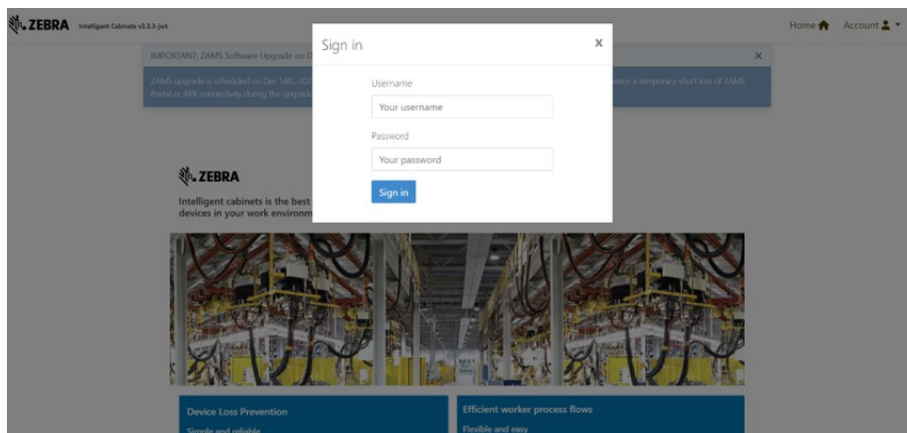
Cradle Master Unlock Code

The Cradle Master Unlock Code enables users to take the device out of the cradle without a need to enter the PIN. This is designed to be used in emergencies. This feature helps users in situations such as a KIOSK going into an unresponsive state for a long time and not allowing the users to take the device from the cradle.

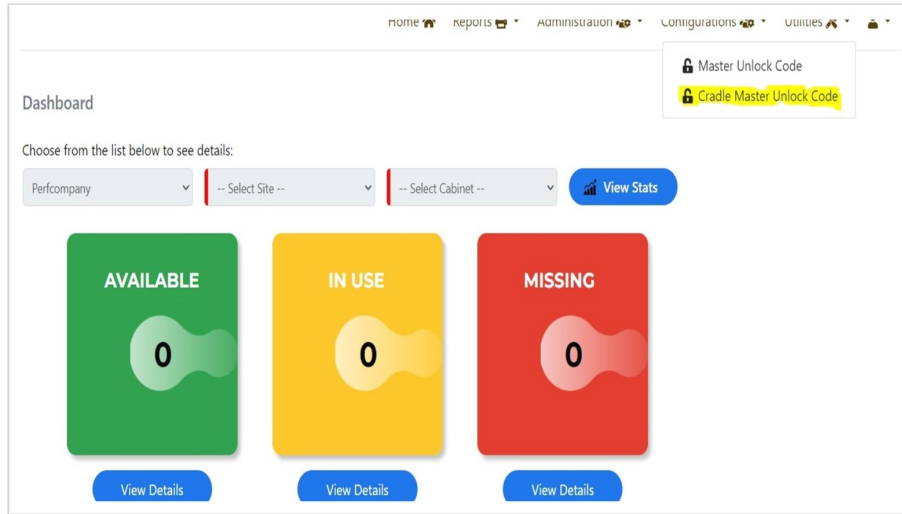
Users with Company Admin, Site Admin, or Company User roles can generate unlock codes from the portal. This code can be downloaded and printed to unlock the device.

Below are the steps describing how to generate a Cradle Master Unlock Code:

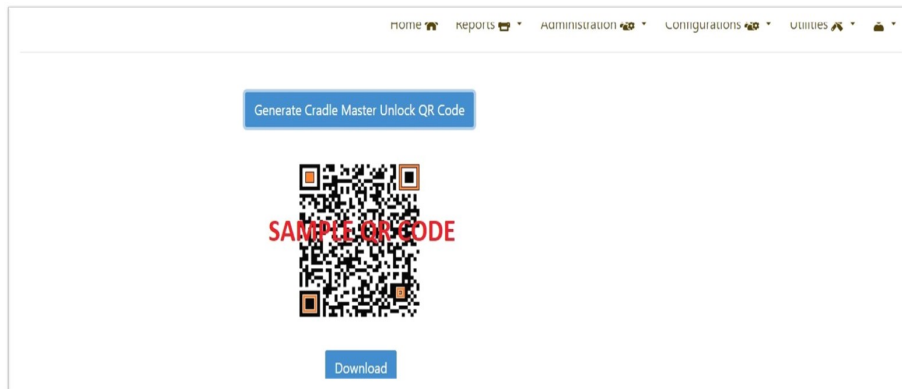
1. Login into the ZAMS portal as a Company Admin, Site Admin, or Company User.



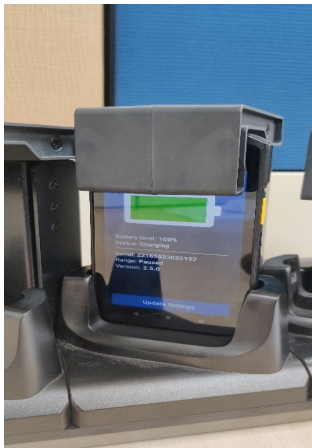
2. Go to Utilities and select **Cradle Master Unlock Code**.



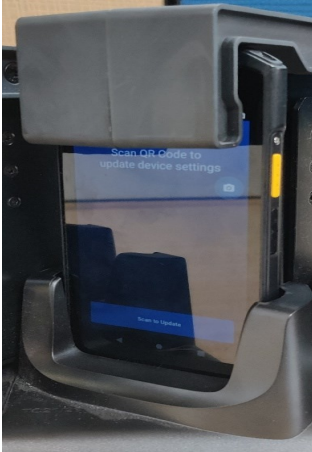
3. Click **Generate Cradle Unlock Code** to generate a QR code. Click **Download** to download the QR code. Downloaded QR codes can be printed on paper.



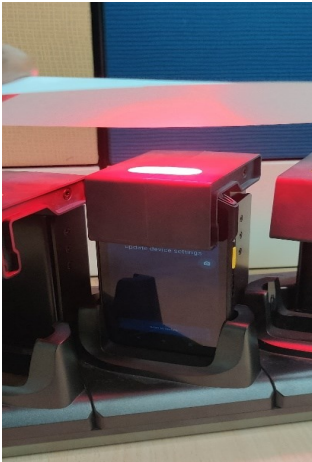
4. Touch **Update Settings** from the charging screen to unlock the device from the Cradle, as shown in the picture.



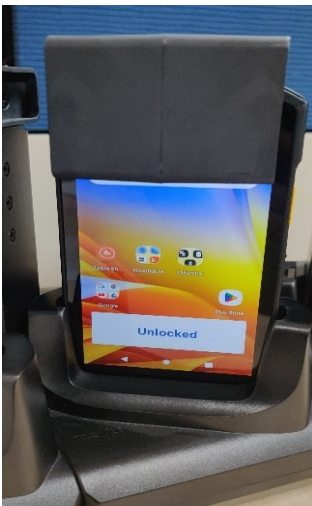
5. Touch **Scan to Update** on the update settings page. The device starts the scanner beam.



6. Place the paper with QR code above the cradle's device slot.



7. Once the QR code is scanned successfully, the device will be unlocked.



Troubleshooting

Table 4 Troubleshooting

Problem	Possible Cause	Possible Solution
Zebra device displays Unable to communicate with cabinet message displayed when docked.	There is a connectivity issue between the mobile computers and the KIOSK module. Check that the Wi-Fi networks are running correctly.	Press Update Settings on the device and scan the Unlock barcode from the portal as a temporary solution to allow the user to work.
Unable to reach to the Cabinet. Please scan QR code message displayed if undocked.		
ZAMS application does not allow a user to log on to the device.	The password is not recognized as valid.	Return the device to its Location/cradle to stop the alarm sounding and reset the Lock screen. Report the password issue to your Help Desk.
Access denied to the Admin Portal.	The password is not valid. Check your password before attempting to log in again.	Report the problem to your help desk.
The ZAMS Lock screen does not appear, but the alarm still sounds.	To allow some third-party applications to have access, ZAMS can move into the background but still function.	Tap the AMS Device System icon and bring it to the foreground to allow sign-on.
		Alternatively, return the device to its Location/cradle to stop the alarm and reset the lock screen.
The ZAMS Lock screen does not come to the foreground when the device is returned to its charging cradle.	Check that the device is seated correctly in the cradle, the cradle is functioning correctly, and power is supplied.	If the issue persists, report it to your help desk.
Mobile Computer does not allow one or some of the following: <ul style="list-style-type: none"> • Scan QR code • Access to its location • Store its registration data. 	If during the initial loading of the APK, permission is not granted for Camera / Location / Microphone / access to storage or the Telephone, then the application will not function correctly.	Reinstall the Zebra Access Management System APK and accept all permissions.

Technical Support

When your own Help Desk is unable to solve an issue that is entitled to technical support, you can escalate issues to the Zebra support team. Escalate issues to Zebra only after you have utilized your own support procedures and still require assistance.

Multi-lingual support is provided during normal regional business hours only. After hours technical support is provided in English only for products under contracts that include 24/7 support. Each region observes various local regional holidays, and days are subject to change from year to year. For information regarding Zebra Support go to: zebra.com/support.

Zebra also provides access to technical and solution training as well as access to professional services offerings to ensure your ability to effectively deploy Zebra solutions.

Contact your account team to learn more.

