Zebra Access Management System
Portal / Cabinet / Device

User Guide

Final Draft Rev B
17/10/2023

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
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.

Contents

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 is comprised 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 is limited to the underlying version configurations noted.

ZAMS Software elements contain:

1. **Mobile Device application and services:** provides the lock screen UI and services for the

android based mobile devices.

2. **Kiosk application and services**: provides on-site device management, UI and provides

information to cloud-based console. The Kiosk application is designed for Zebra's ET40 or 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/

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
- dwprofile_code128_barcode_profile.db - StageNow software staging solution for simple profile creation and device deployment.
- Release notes[1]

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.

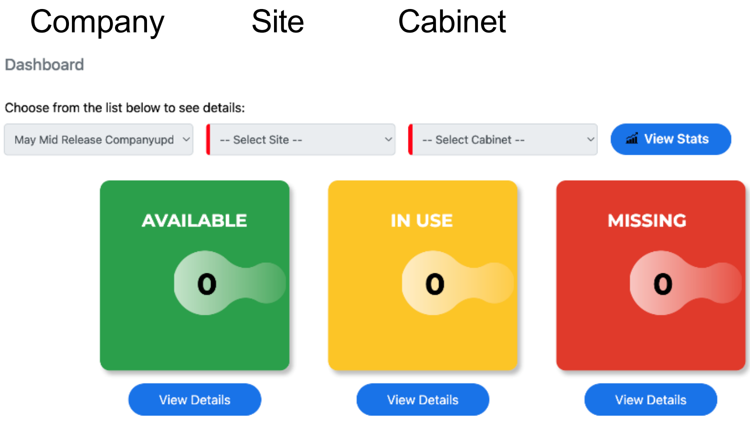
Getting Started

Zebra Access Management System Overview

Product 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



Dashboard

Choose from the list below to see details:

May Mid Release Companyupd | -- Select Site -- | -- Select Cabinet --

Designed to run on Zebra Android Mobile devices, this low touch solution is easily deployed and managed, providing the perfect way of accounting for your mobile assets while keeping the overhead of managing the potential losses to a minimum.

The solution uniquely monitors and reports on the devices by serial number, user, and location providing organizations with the clarity required to quickly recognize if terminals are missing.

The ZAMS portal is the perfect way to set up the solution across multiple locations. Password protected user access allows visibility of assets at a local or global level giving customers the tools to manage missing terminals from a mobile computer fleet easily.

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 devices On Charge.

The user facing security screen highlights the device 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 scan PIN from bar code or other authentication process to unlock the security screen.

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

Installation Process:

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

Rack Model 1 & 2 Installation Guide

MN-003984-02EN Rev. A

Note: Installation guide through MDM is available to the below location: (Will be published along with the User Guide)

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

Adding devices to the Database

Each device is registered and 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 to the charging location on the optional display Kiosk.

Once the devices have been 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, authorized users can create custom locations and add user IDs.

Admin Process Overview

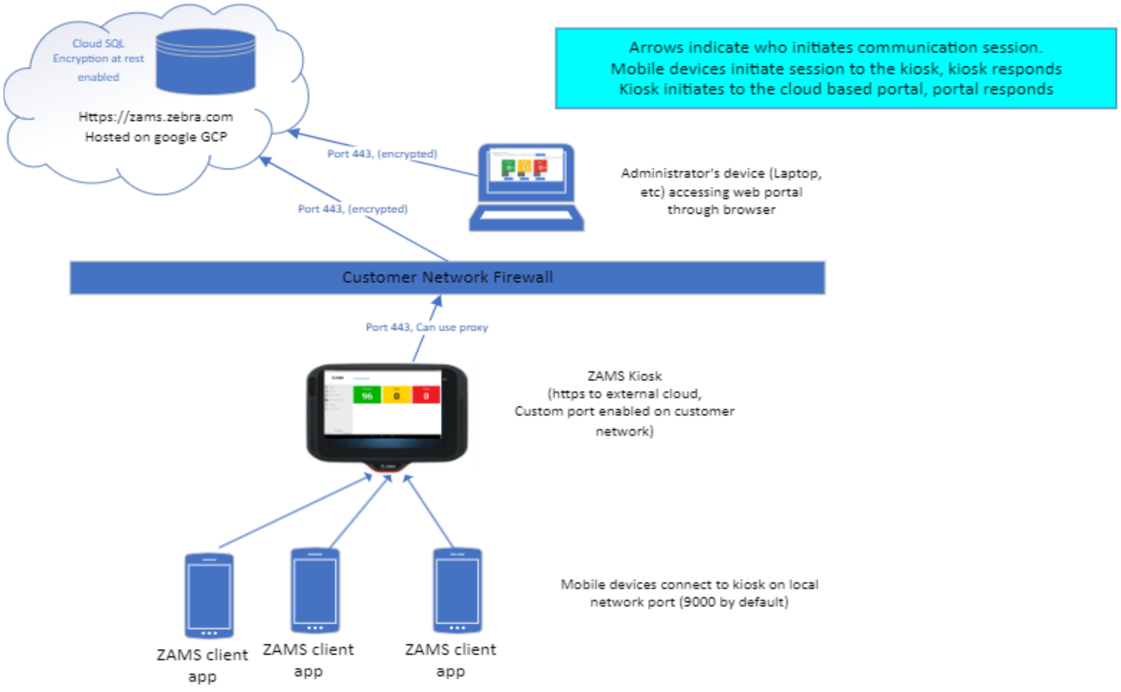
The Reporting and Admin portal provides the client the ability to set up the solution.

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 on page 3).

Figure 2 ZAMS Network


Cloud SQL
Encryption at rest
enabled
Https://zams.zebra.com
Hosted on google GCP
Arrows indicate who initiates communication session.
Mobile devices initiate session to the kiosk, kiosk responds
Kiosk initiates to the cloud based portal, portal responds
Port 443, (encrypted)
Port 443, (encrypted)
Administrator's device (Laptop, etc) accessing web portal through browser
Customer Network Firewall
Port 443, Can use proxy
96
0
0
ZAMS Kiosk
(https to external cloud,
Custom port enabled on customer
network)
Mobile devices connect to kiosk on local network port (9000 by default)
ZAMS client app
ZAMS client app
ZAMS client app

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.

Example: You may want to consider using this feature in the case of … Truck driver checks out device at start of shift (near the cabinet) 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 normal 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's 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.

ZAMS General Usage

ZAMS Cabinet (KIOSK ET40 or CC6000)

The Zebra Access Management System provides a display Kiosk 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.

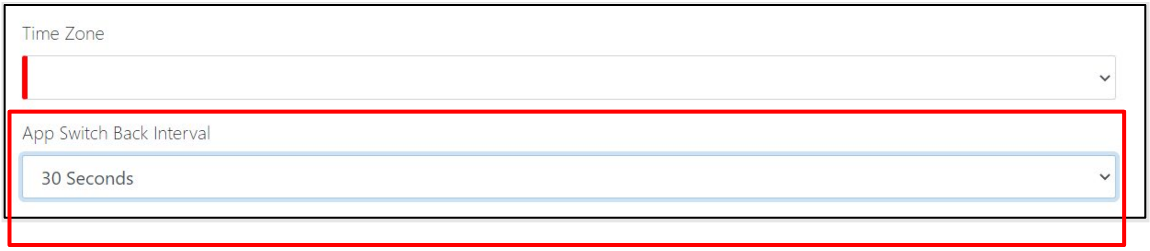
- **Available** – The number of devices that are currently On Charge in the Cabinet.
- **In Use** – The number of devices that have been removed from the Cabinet and successfully logged in.
- **Missing** – The number of devices that have been removed from the Cabinet and have not yet logged in. This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

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

App Switchback Interval for Cabinet dashboard:

If AMS charge screen is minimized by pressing home button, then the AMS charge screen should reengage (pop-up) automatically after a configurable time 30, 60, 90 or 120 seconds. This time is configurable at site level through the App Switchback Interval settings.

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



Time Zone

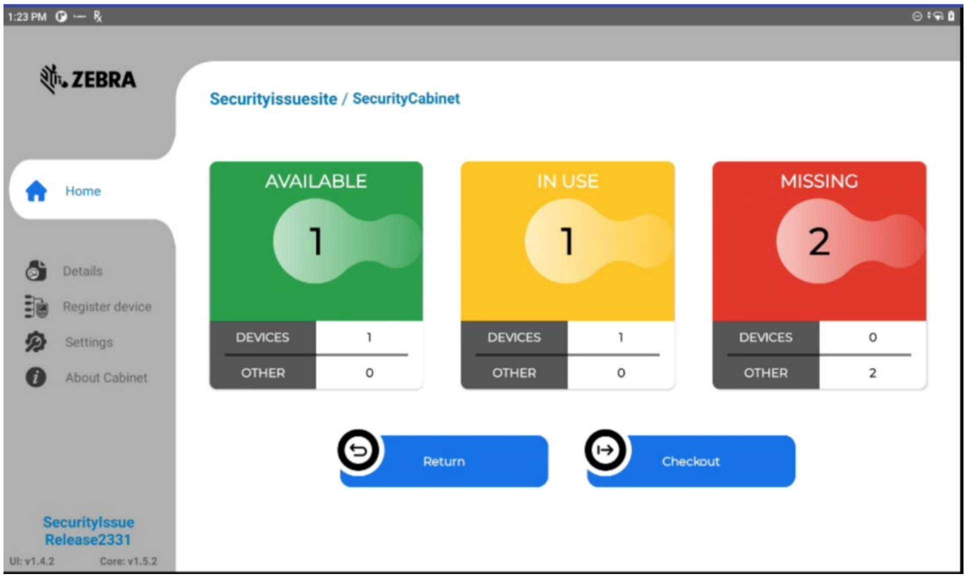
App Switch Back Interval

30 Seconds

NOTE :A Screen saver has been added to address the potential screen burn issue.

- Screen saver will kick off 3 minutes after the device has been put on charge and has recorded no user interaction.
- If user presses a button, touches the screen, or takes the device off charge, device will go back to the normal AMS screen.

Figure 4 ZAMS Home Summary Screen



Securityissuesite / SecurityCabinet

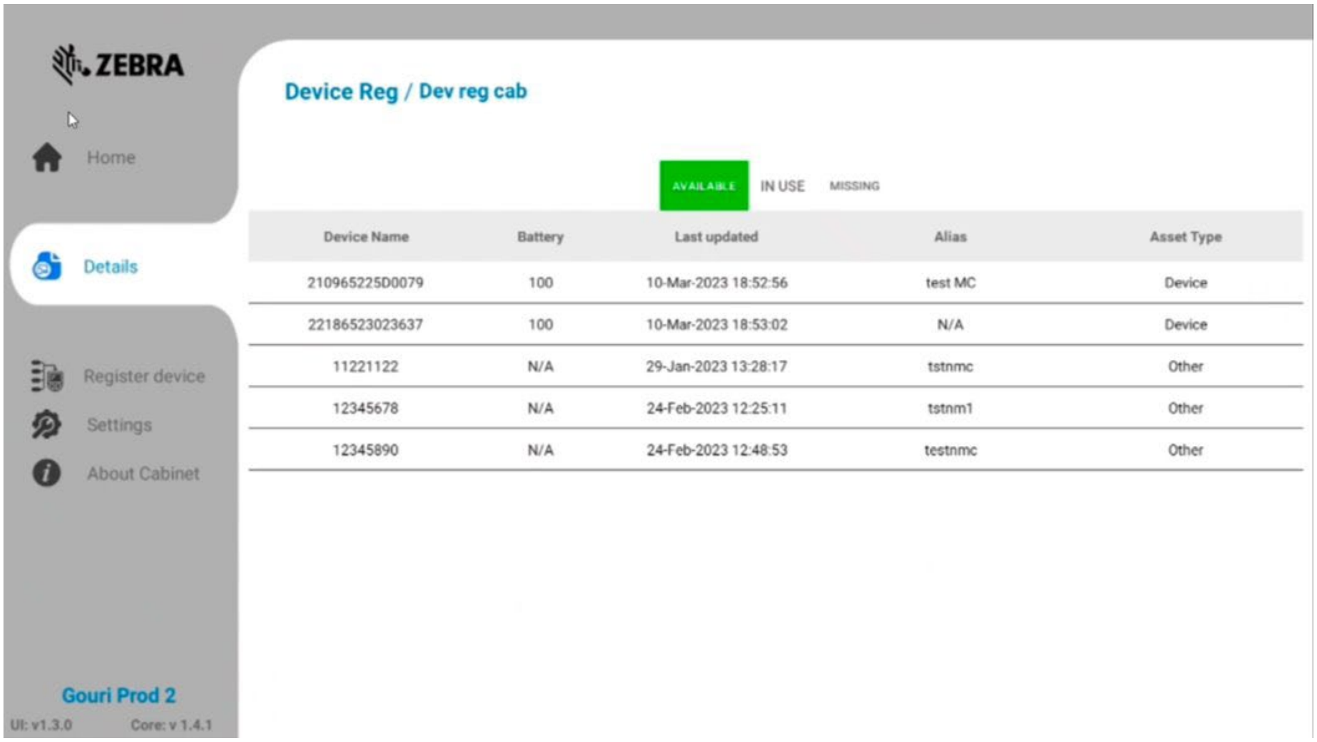
AVAILABLE		IN USE		MISSING	
1		1		2	
DEVICES	1	DEVICES	1	DEVICES	0
OTHER	0	OTHER	0	OTHER	2

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. Tap **Details.**



Device Reg / Dev reg cab

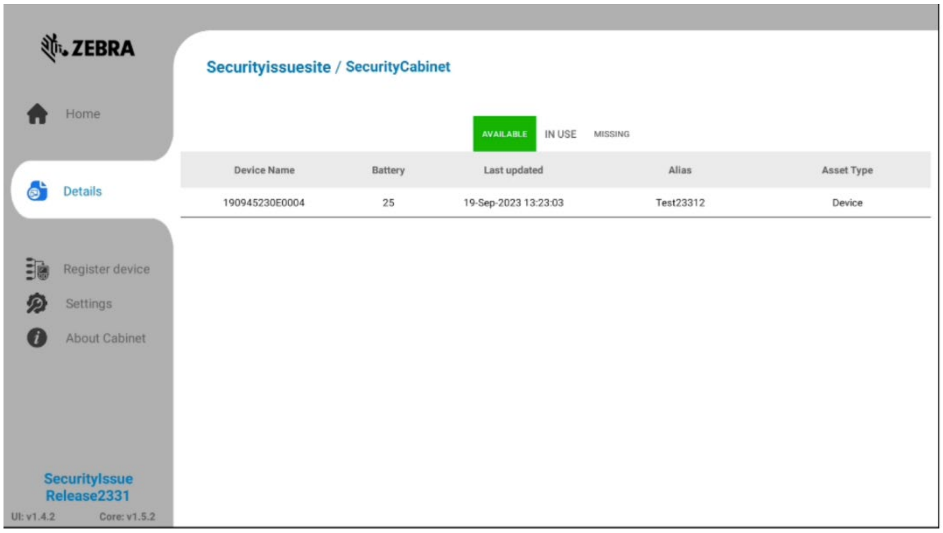
Device Name	Battery	Last updated	Alias	Asset Type
210965225D0079	100	10-Mar-2023 18:52:56	test MC	Device
22186523023637	100	10-Mar-2023 18:53:02	N/A	Device
11221122	N/A	29-Jan-2023 13:28:17	tstnmc	Other
12345678	N/A	24-Feb-2023 12:25:11	tstnm1	Other
12345890	N/A	24-Feb-2023 12:48:53	testnmc	Other

IN USE:

The **IN-USE** tab lists all the devices that are no longer in the Cabinet and not missing. 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.

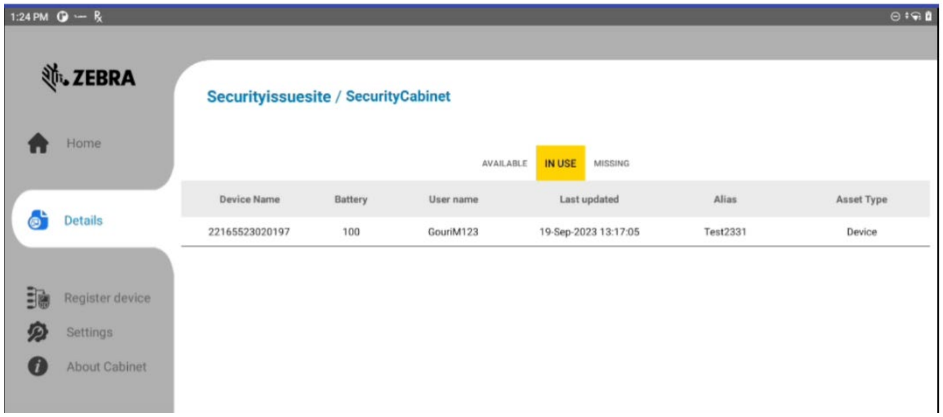
To view the in use devices:

1. Tap **Details.**
2. **Tap “In USE”**



Securityissuesite / SecurityCabinet

Device Name	Battery	Last updated	Alias	Asset Type
190945230E0004	25	19-Sep-2023 13:23:03	Test23312	Device



Securityissuesite / SecurityCabinet

Device Name	Battery	User name	Last updated	Alias	Asset Type
22165523020197	100	GouriM123	19-Sep-2023 13:17:05	Test2331	Device

MISSING:

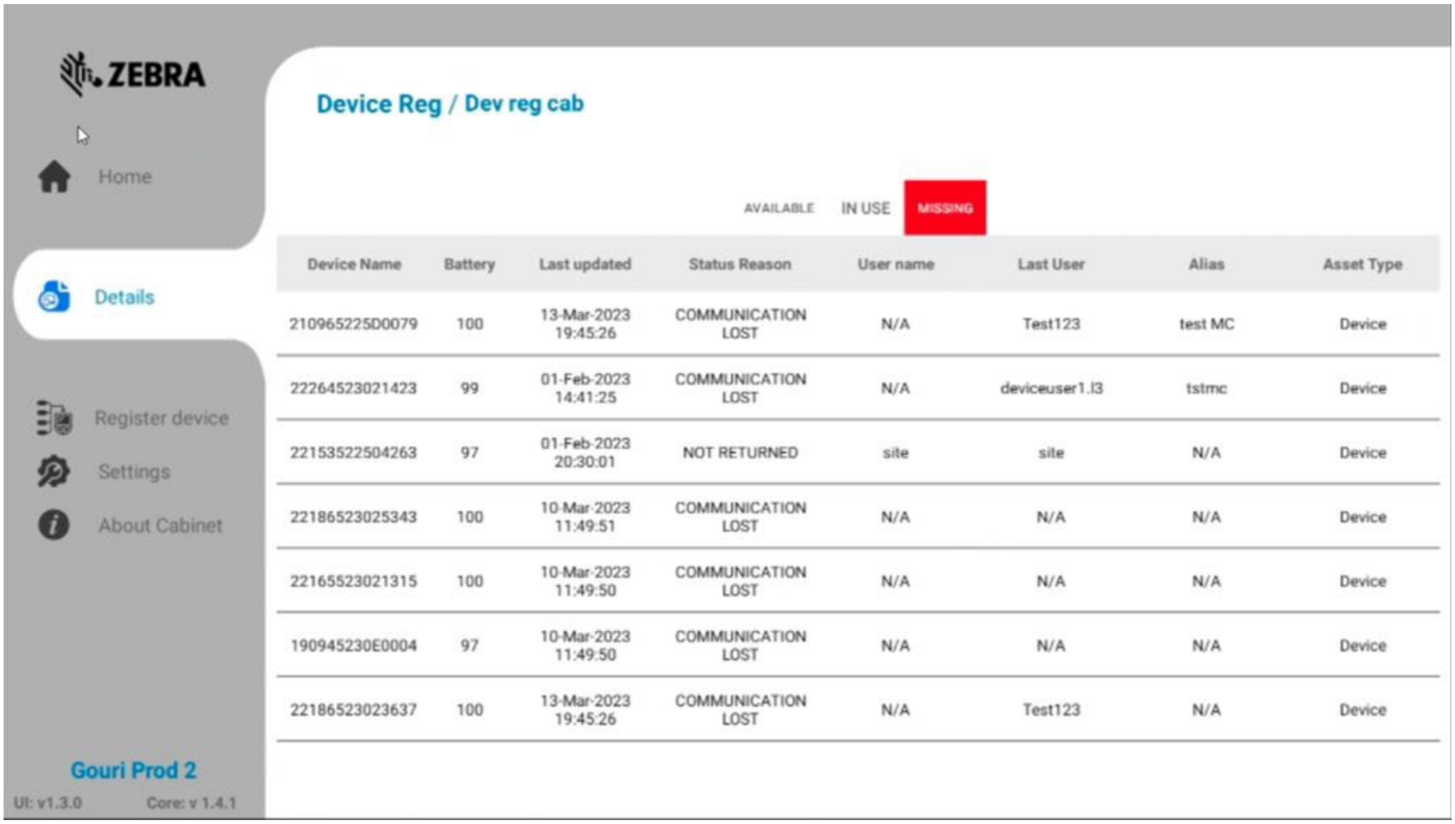
The **MISSING** tab lists all the devices that have been removed from the Cabinet but not yet logged in. These devices are not highlighted with any color.

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

Status	Status Reason	Detail
MISSING	INVALID_LOGIN	Failed to log in and the device is not placed back
MISSING	NOT_RETURNED	User didn't return the device on time, Note: Shift duration is set for 8 hours, Post 8 hours completion, device is not placed to the cradle
MISSING	COMMUNICATION_ LOST	User logged in to the device and then user has taken the device outside the network/ wifi disconnection observed.

To view devices considered missing:

1. Tap **Details.**
2. **Tap MISSING**



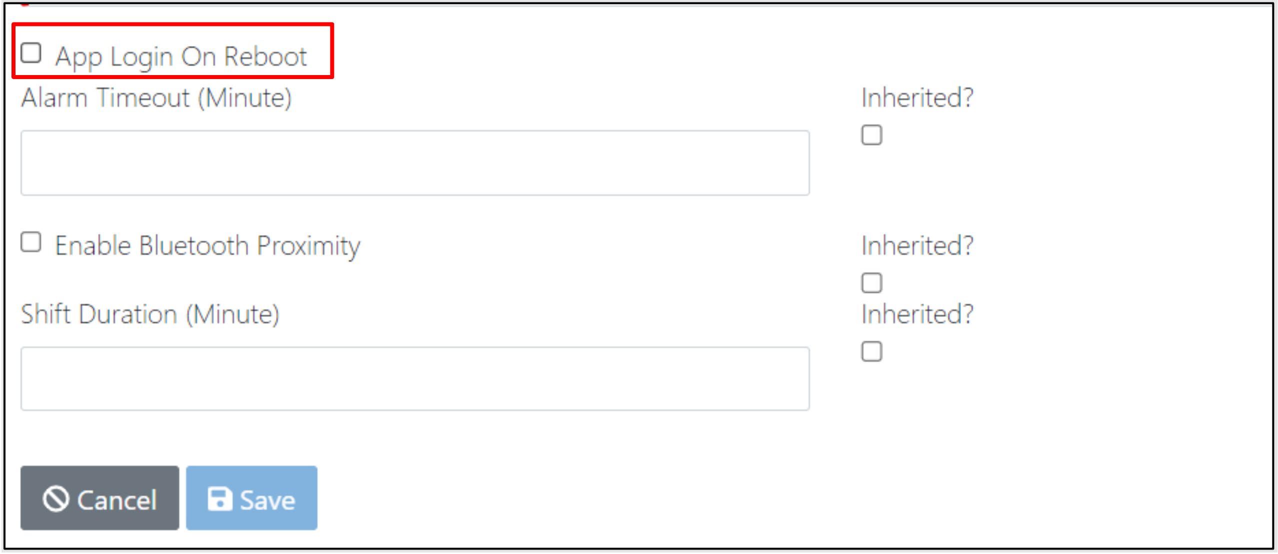
Device Reg / Dev reg cab

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.l3	tstmc	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

App Login on Reboot:

This option provides the ability to require to login to ZAMS again after reboot or battery swap even if device does not go back on charge. This can be configured at the site settings. **Go to Administration and** Site a Edit/Create Site.

The option: App Login on Reboot should be checked to enable Login after reboot.



☐ App Login On Reboot

Alarm Timeout (Minute)

Inherited? ☐

☐ Enable Bluetooth Proximity

Inherited? ☐

Shift Duration (Minute)

Inherited? ☐

ZAMS Cabinet Set Up

The ZAMS installation process consists of establishing network connectivity, accessing the Portal, and installing APKs and supporting files for the cabinets. For detailed installation and setup information, refer to the ZAMS Installation Guide (see Related Documents and Software on page 3).

ZAMS Portal Access and Usage

ZAMS Mobile Devices

This chapter describes the following ZAMS app features:

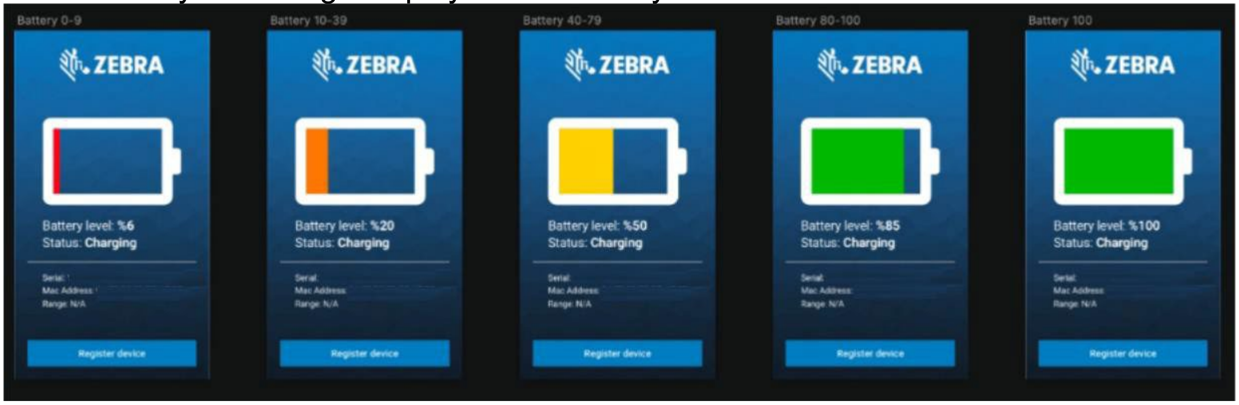
- Battery indications
- PIN code entry and considerations
- ZAMS Cabinet set up and registration.

General Usage

1. Recommendation to 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 as follows:

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



Battery level: %6
Status: Charging
Serial:
Mac Address:
Range: N/A

Battery level: %20
Status: Charging
Serial:
Mac Address:
Range: N/A

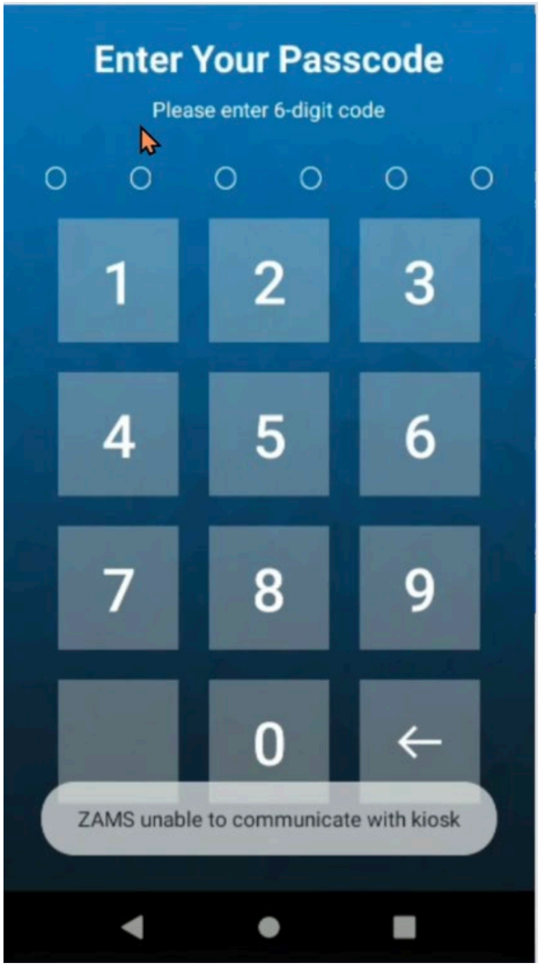
Battery level: %50
Status: Charging
Serial:
Mac Address:
Range: N/A

Battery level: %85
Status: Charging
Serial:
Mac Address:
Range: N/A

Battery level: %100
Status: Charging
Serial:
Mac Address:
Range: N/A

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

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



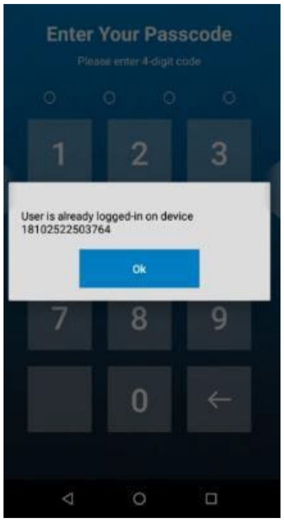
Enter Your Passcode

Please enter 6-digit code

ZAMS unable to communicate with kiosk

Considerations:

- If a valid PIN is not entered within a specified time period (configurable by Company or Location), the application triggers an alarm. The alarm volume cannot be adjusted. Users can place the device back into the Cabinet if they do not want to continue using the device. If the PIN is invalid, then an **invalid pin** message displays.
- If the device is physically locked in ZAMS cradle lock, swipe the left from the **Battery** icon on the charging screen. 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 after 30 seconds, the cradle locks again and after 60 seconds, the app goes back to the charging screen. (Only applicable for customers who use Cradle lock).
- When a valid PIN is entered and the device is successfully logged in, the same PIN cannot be used by any other user from Company to log in. Once a user enters the same PIN which is currently in use, an error message displays (for example, **User is already logged-in on device 1xxxxxxxxxxxx9**).



Enter Your Passcode

Please enter 4-digit code

User is already logged-in on device 18102522503764

- 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.

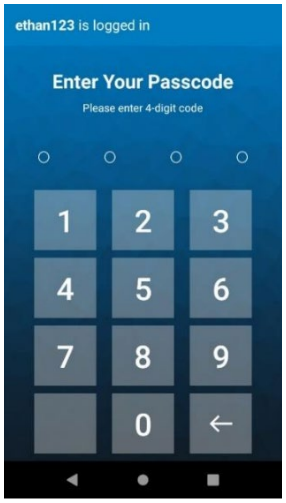
- Once the device is registered, the **Register Device** button label at the bottom of the ZAMS screen changes to a new label **Update Settings**. This function allows updating the settings of the application. This button can be used to register to a cabinet or scan a master unlock barcode.
- If a device 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 **ZAMS Unable to communicate with Kiosk** 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 troubleshooting is needed on the device while it is not able to be checked out with a pin (or even during a remote control session), the easiest way is to put the device on charge and hit the home button (circle button at the bottom of the screen). If the device is on charge, the pin screen will not aggressively pop up over whatever they are trying to do (maybe configure WiFi for instance)

Swap user (logging IN/Out of ZAMS) without the need of 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 next user to enter his valid pin to login 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 his valid credentials.
- When the device is assigned to the user and the device will be displayed as IN_USE as standard behavior
- At any point during the shift time or after the shift ends if the user wants to pass the device to another user, then the user must simply press on the ZAMS Device Icon. Tapping the ZAMS Device Icon, the new Pin Screen will launch as given below.



ethan123 is logged in

Enter Your Passcode

Please enter 4-digit code

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

NOTE:

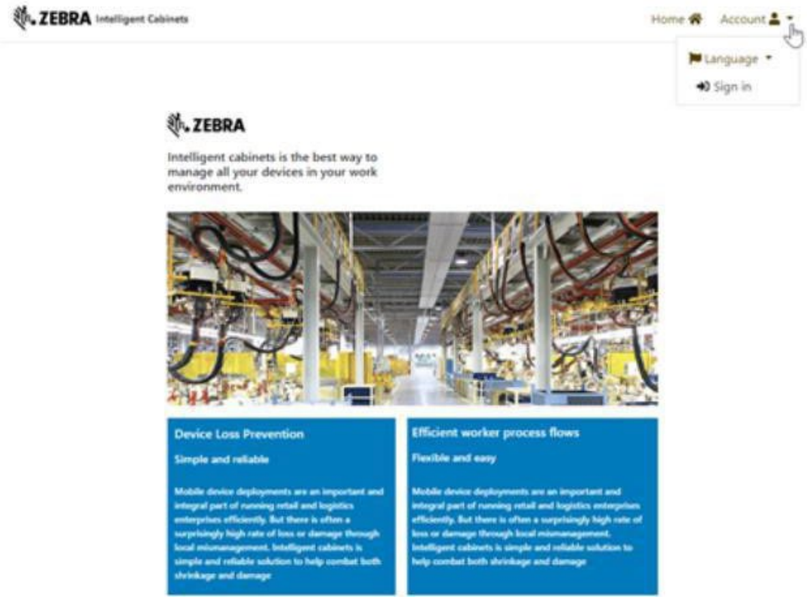
The device needs to be connected to the Kiosk in order for a log in to occur.

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.

Accessing ZAMS Account

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



Intelligent cabinets is the best way to manage all your devices in your work environment.

Device Loss Prevention

Simple and reliable

Mobile device deployments are an important and integral part of running retail and logistics enterprises efficiently. But there is often a surprisingly high rate of loss or damage through local mismanagement. Intelligent cabinets is simple and reliable solution to help combat both shrinkage and damage

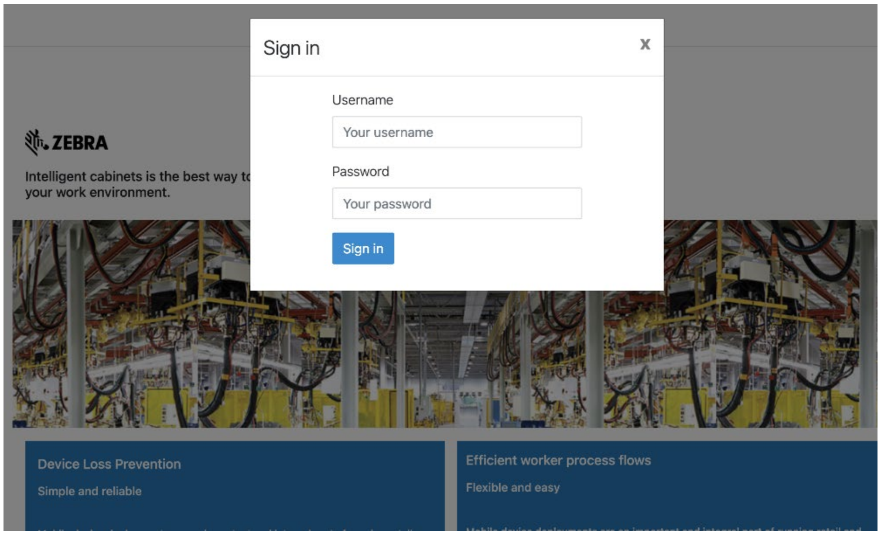
Efficient worker process flows

Flexible and easy

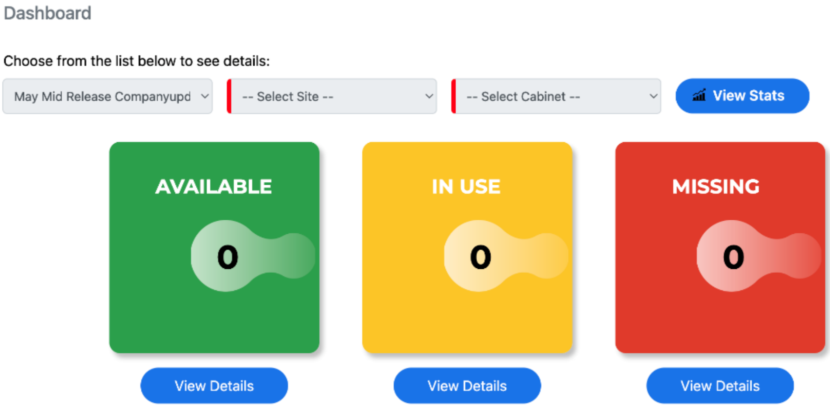
Mobile device deployments are an important and integral part of running retail and logistics enterprises efficiently. But there is often a surprisingly high rate of loss or damage through local mismanagement. Intelligent cabinets is simple and reliable solution to help combat both shrinkage and damage

2. From the Account drop-down menu, click **Sign in.** The Sign in dialogue box displays.

3. Enter Username and Password.



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



Dashboard

Choose from the list below to see details:

May Mid Release Companyupd | -- Select Site -- | -- Select Cabinet --

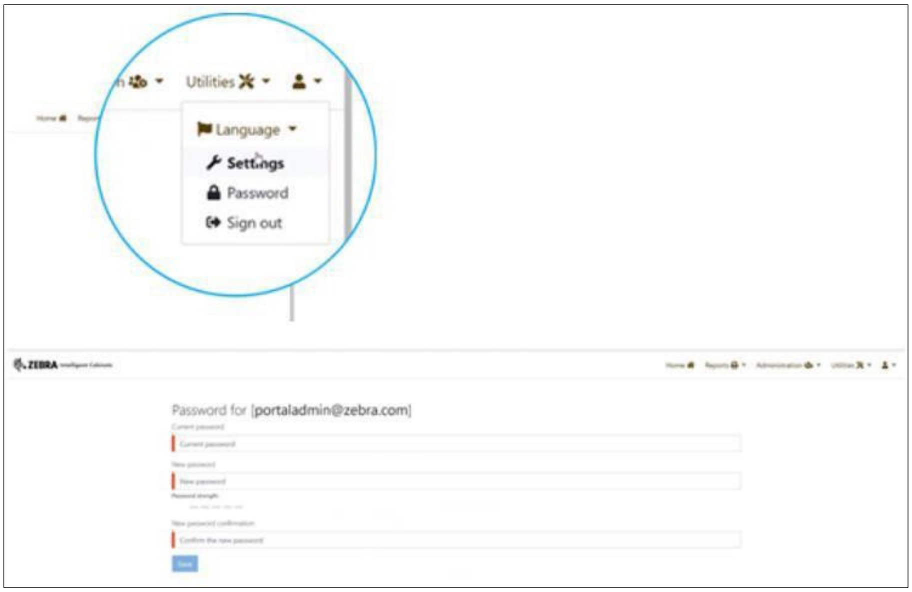
Resetting Password

The password must include the following criteria:

- Be between 8 and 50 characters long.
- Contain at least one digit.
- Contain at least one lower case character.
- Contain at least one upper case character.
- Contain at least one special character.

To change your password:

1. Select **Password** from the Account drop-down menu. The password must contain at least 8 characters (letters or numbers).



Password for [portaladmin@zebra.com]

Current password

Current password

New password

New password

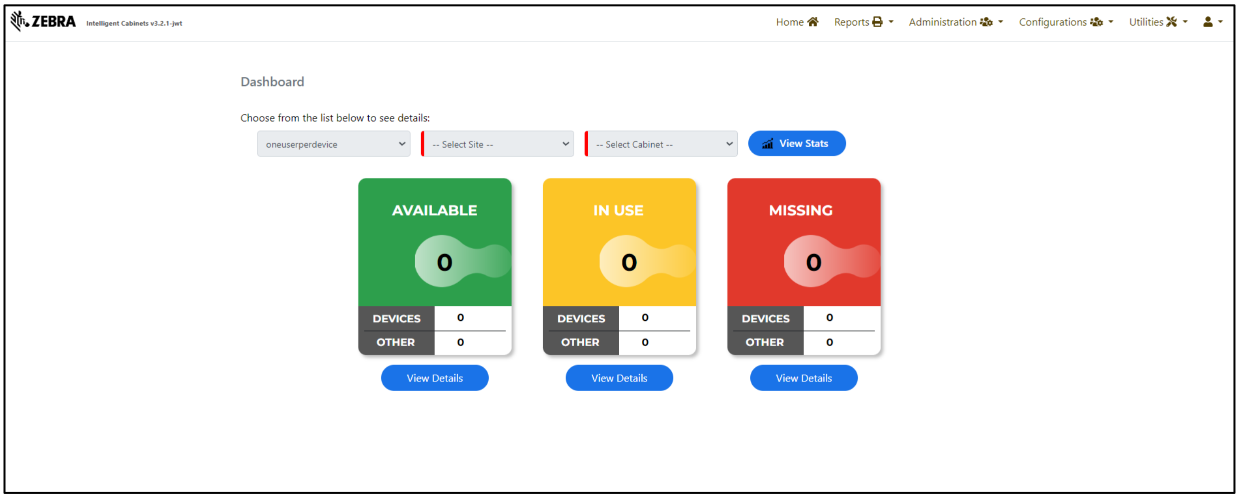
Password strength

New password confirmation

Confirm the new password

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

Selecting ZAMS Portal Dashboard Options



Dashboard

Choose from the list below to see details:

oneuserperdevice | -- Select Site -- | -- Select Cabinet --

AVAILABLE	IN USE	MISSING
0	0	0
DEVICES 0	DEVICES 0	DEVICES 0
OTHER 0	OTHER 0	OTHER 0

The first screen the application displays is the Zebra Access Management System Dashboard.

1. Click on the drop-down menus and select the desired **Company**, **Site**, and **Cabinet**.
2. A notification banner also appears on the dashboard to let users know of maintenance related changes (e.g., planned updates or recent updates)

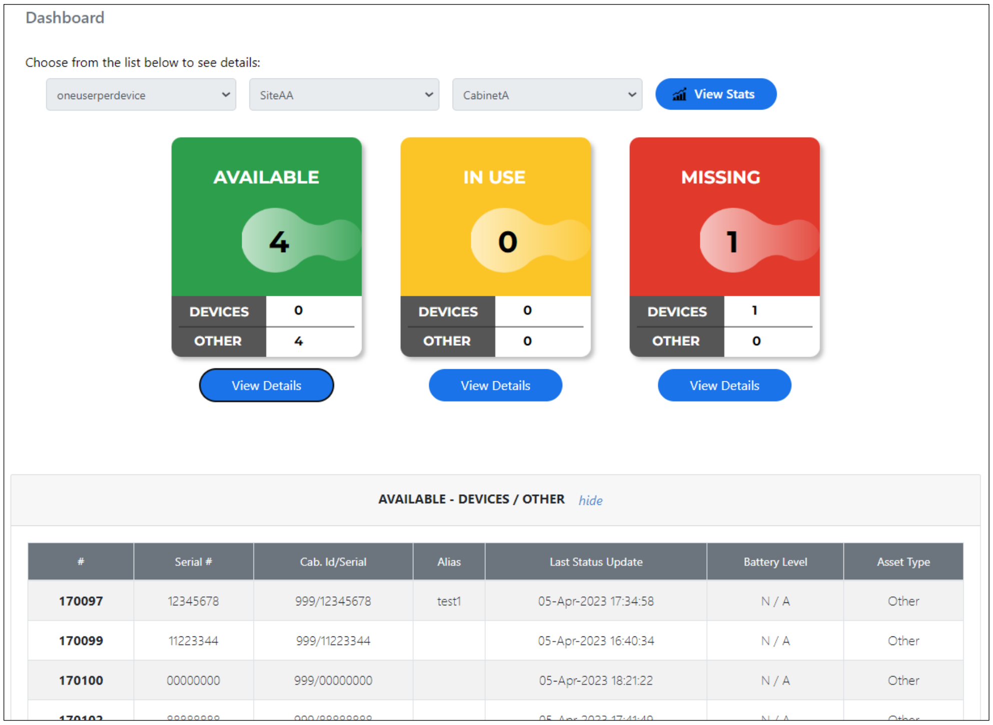
3. Click on **View Stats**.

The application displays real -time statistics from the selected Cabinet of the desired Site belonging to the relevant Company while the browser remains on the page.

Viewing Device Details

To view device details:

1. From the dashboard statistics display, click **View** to see the details of any set of devices. This page does not update automatically.



Dashboard

Choose from the list below to see details:

oneuserperdevice | SiteAA | CabinetA | View Stats

AVAILABLE	4
DEVICES	0
OTHER	4

View Details

IN USE	0
DEVICES	0
OTHER	0

View Details

MISSING	1
DEVICES	1
OTHER	0

View Details

AVAILABLE - DEVICES / OTHER *hide*

#	Serial #	Cab. Id/Serial	Alias	Last Status Update	Battery Level	Asset Type
170097	12345678	999/12345678	test1	05-Apr-2023 17:34:58	N / A	Other
170099	11223344	999/11223344		05-Apr-2023 16:40:34	N / A	Other
170100	00000000	999/00000000		05-Apr-2023 18:21:22	N / A	Other
170102	88888888	999/88888888		05-Apr-2023 17:41:40	N / A	Other

2. The list of devices displays and provides information on each individual device in the selected state which include:
   - **Available** – The number of devices currently On Charge in the Cabinet.
   - **In Use** – The number of devices removed from the Cabinet and successfully logged in.
3. **Missing** – The number of devices removed from the Cabinet and have not yet logged in. The Missing status has three classifications and cover three Status reasons for missing device;

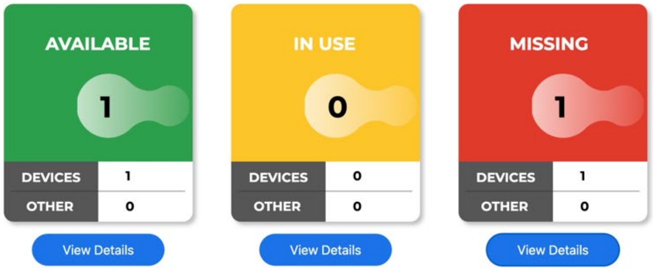
Status	**Status Reason**	**Detail**
MISSING	INVALID_LOGIN	Failed to log in and

		the device is not placed back
MISSING	NOT_RETURNED	User didn't return the device on time, Note: Shift duration is set for 8 hours, Post 8 hours completion, device is not placed to the cradle
MISSING	COMMUNICATION_LOST	User logged in to the device and then user has taken the device outside the network/ wifi disconnection observed.

How to find a lost device:

Click on "View Status" for Missing devices in ZAMS homescreen in the portal and make the alarm sound.

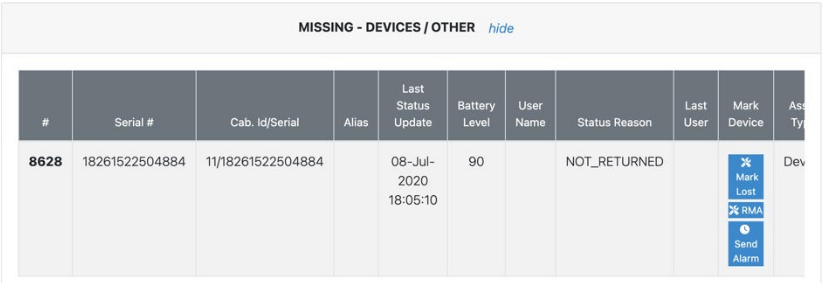
Once the alarm is triggered, the "Send Alarm "button will move to "Sent Alarm".



AVAILABLE	
	1
DEVICES	1
OTHER	0

IN USE	
	0
DEVICES	0
OTHER	0

MISSING	
	1
DEVICES	1
OTHER	0

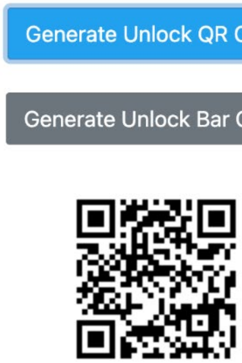


MISSING - DEVICES / OTHER *hide*

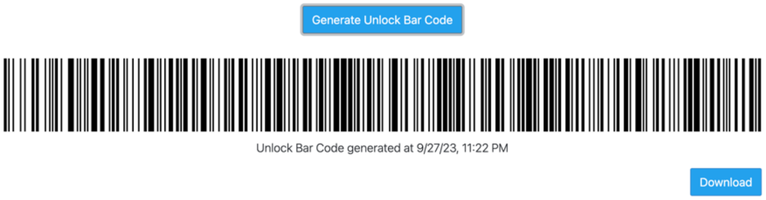
#	Serial #	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Status Reason	Last User	Mark Device	Ass Ty
8628	18261522504884	11/18261522504884		08-Jul-2020 18:05:10	90		NOT_RETURNED		Mark Lost RMA Send Alarm	Dev

Once the device is found, either Device_User can stop the alarm in below process **(using anyone of the below steps):**

- Enter the passcode.
- Place the device back to the cradle.
- Scan the QRcode from the UI (Utilities scan)



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



Unlock Bar Code generated at 9/27/23, 11:22 PM

Break Glass: (Kiosk and Portal are down)

- Option 1: Pre-requisite: Access to the Zebra support portal and generate the Cradle Master Unlock QR code from Utilities<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.

- Option 2: Company admin can assign “ROLE_DEVICE_INTERNAL_USER” to any 5 employees in each site 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.

How to log in to another device when the first device is broken/not working (One Device User is enabled)

- Log in to Portal and uncheck the “One device user enabled” in company setting screen. And try to log in to the second device.

Support for Mobile device with 1D linear barcode scanners:

ZAMS allows registering mobile devices with 1D liner barcode scanners (MC33X) which don’t have camera to scan QR codes for registration.

To register devices (MC33x) to a particular cabinet follow below steps:

1. User with Company_Admin/Site_Admin roles must login to the portal

2. Navigate to Administration → Cabinet and select the appropriate cabinet from the list of cabinets.

3. Select "view" on the cabinet. Make sure that cabinet is having proper ip address provided

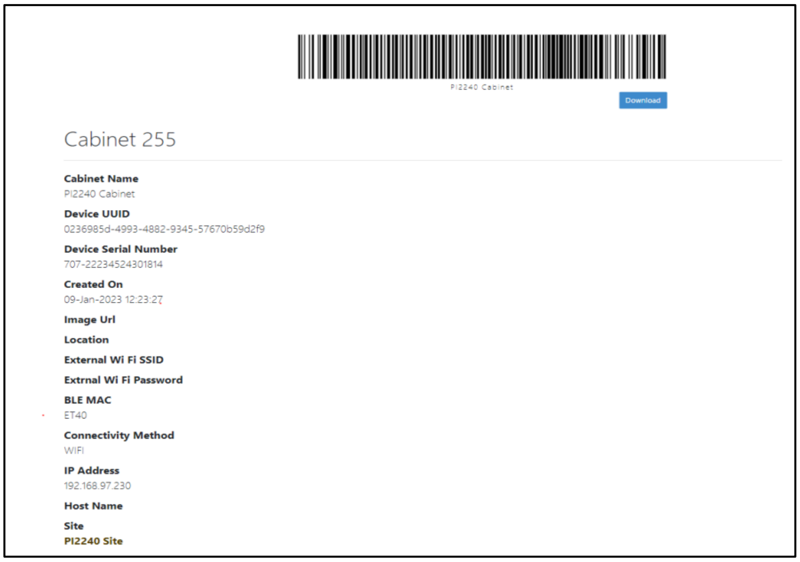
4. Barcode will be visible as shown in below image.

5. Download the barcode, copy the barcode on to MS Word

6. Take a print and paste it on to the corresponding physical cabinet.

7. Devices installed with AMS v2.4.0 should be able to scan the barcode downloaded as mentioned in above steps and get registered with the cabinets.

See image below for reference:



Cabinet 255

Cabinet Name
PI2240 Cabinet

Device UUID
0236985d-4993-4882-9345-57670b59d2f9

Device Serial Number
707-22234524301814

Created On
09-Jan-2023 12:23:27

Image Url

Location

External Wi Fi SSID

Extrnal Wi Fi Password

BLE MAC
ET40

Connectivity Method
WIFI

IP Address
192.168.97.230

Host Name

Site
PI2240 Site

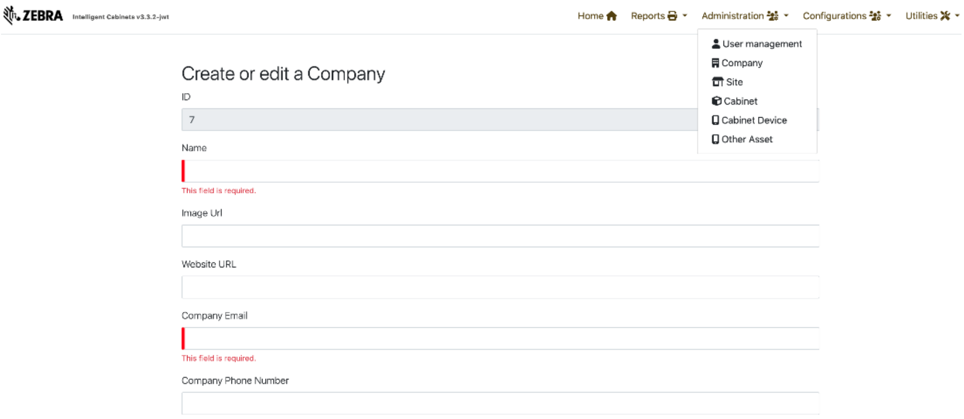
NOTE:

- Barcode will get generated only when either "IP Address" or "Host Name" have values.
- If Both "IP Address" and "Host Name" have values, barcode will get generated with "IP Address" by default.
- If cabinet is using only Host Name, then the length of Host Name should not exceed 23 characters.

Administration:

Company:

- Super admin will be able to set up the company from Administration < Company screen.
- Super admin/Company admin will be able to View/Edit the company details.
- When "**One Device User Enabled**", the user tries to take a second device within a minute after he has taken the first device, user will be able to take the second device. Waiting 1 minute is must for "1 device 1 user" functionality. This is generic functionality with all supported versions.



Create or edit a Company

ID: 7

Name:

This field is required.

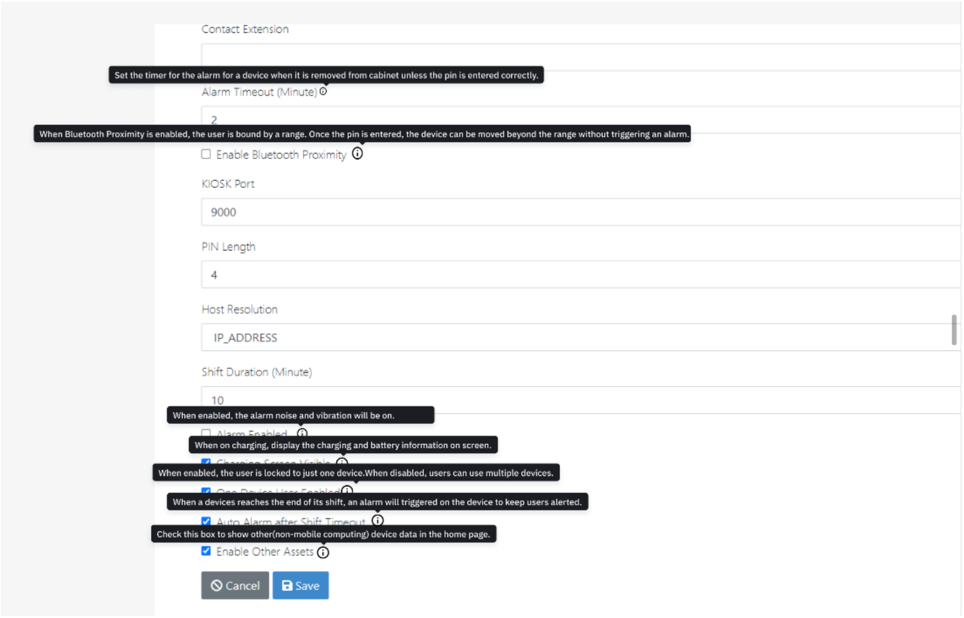
Image Url:

Website URL:

Company Email:

This field is required.

Company Phone Number:



Contact Extension:

Set the timer for the alarm for a device when it is removed from cabinet unless the pin is entered correctly.

Alarm Timeout (Minute): 2

When Bluetooth Proximity is enabled, the user is bound by a range. Once the pin is entered, the device can be moved beyond the range without triggering an alarm.

☐ Enable Bluetooth Proximity

KIOSK Port: 9000

PIN Length: 4

Host Resolution: IP_ADDRESS

Shift Duration (Minute): 10

When enabled, the alarm noise and vibration will be on.

☐ Alarm Enabled

When on charging, display the charging and battery information on screen.

☑ Charging Screen Visible

When enabled, the user is locked to just one device.When disabled, users can use multiple devices.

☑ One Device User Enabled

When a devices reaches the end of its shift, an alarm will triggered on the device to keep users alerted.

☑ Auto Alarm after Shift Timeout

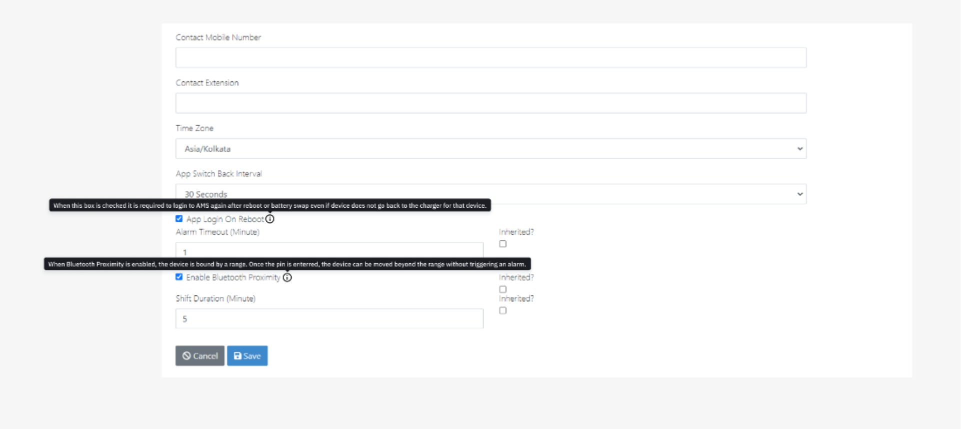
Check this box to show other(non-mobile computing) device data in the home page.

☑ Enable Other Assets

Site:

- Super admin /Company admin/Site admin will be able to set up the Site from Administration < Site screen.
- Super admin/Company admin/Site admin will be able to View/Edit the site details.

- Checking the “Inherited “option, Company level setting will override the particular Site level setting for those specific field.



Contact Mobile Number

Contact Extension

Time Zone

Asia/Kolkata

App Switch Back Interval

30 Seconds

When this box is checked it is required to login to AMS again after reboot or battery swap even if device does not go back to the charger for that device.

☑ App Login On Reboot ⓘ

Alarm Timeout (Minute) — 1 — Inherited? □

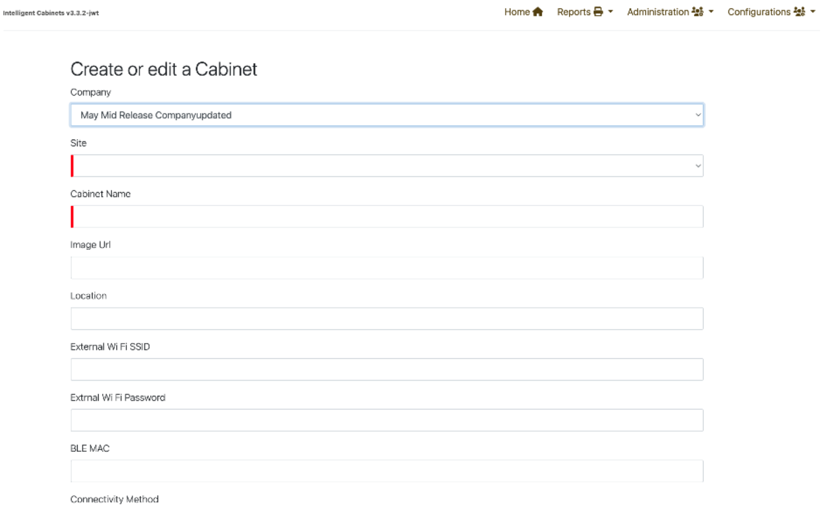
When Bluetooth Proximity is enabled, the device is bound by a range. Once the pin is enterred, the device can be moved beyond the range without triggering an alarm.

☑ Enable Bluetooth Proximity ⓘ — Inherited? □

Shift Duration (Minute) — 5 — Inherited? □

Cabinet:

- Super admin /Company admin/Site admin will be able to set up the Site from Administration < Site screen.
- Super admin/Company admin/Site admin will be able to View/Edit the site details.



Create or edit a Cabinet

Company: May Mid Release Companyupdated

Site

Cabinet Name

Image Url

Location

External Wi Fi SSID

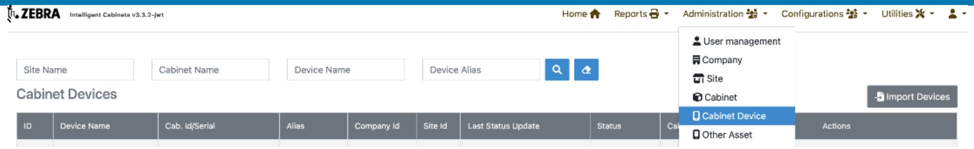
Extrnal Wi Fi Password

BLE MAC

Connectivity Method

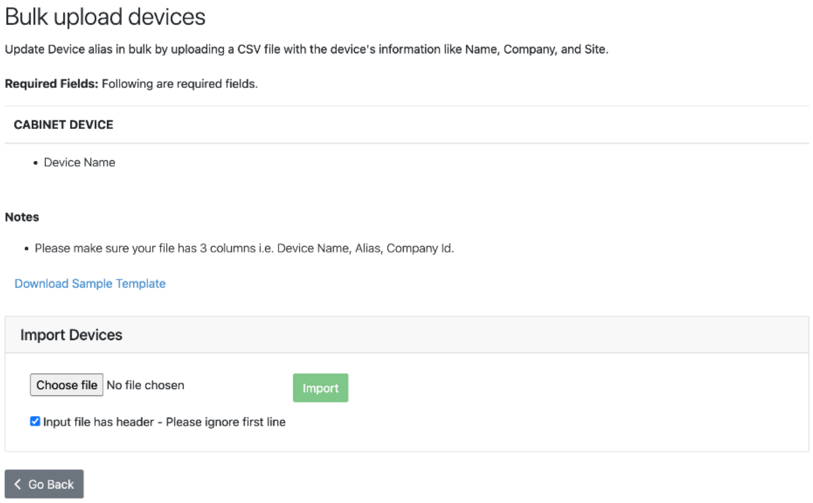
Cabinet Device:

- Super admin /Company admin/Site admin will be able to import devices from Administration < Cabinet device screen.
- Super admin/Company admin/Site admin will be able to View/Edit the device details.



- Click on “Import devices”, import the file to import cabinet devices.

Sample template is already provided to 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

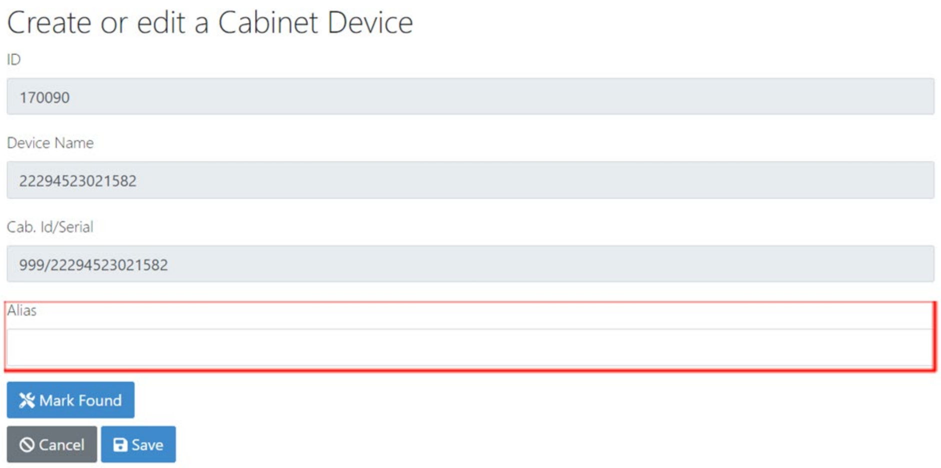
Choose file No file chosen Import

☑ Input file has header - Please ignore first line

Device Aliases (Friendly Name)

Device Aliases can be used by a company to have their unique identification of devices. This can be set via portal UI or a CSV file import. To add/change the Alias go to Administration à Cabinet-Device à Edit.

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



Create or edit a Cabinet Device

ID

170090

Device Name

22294523021582

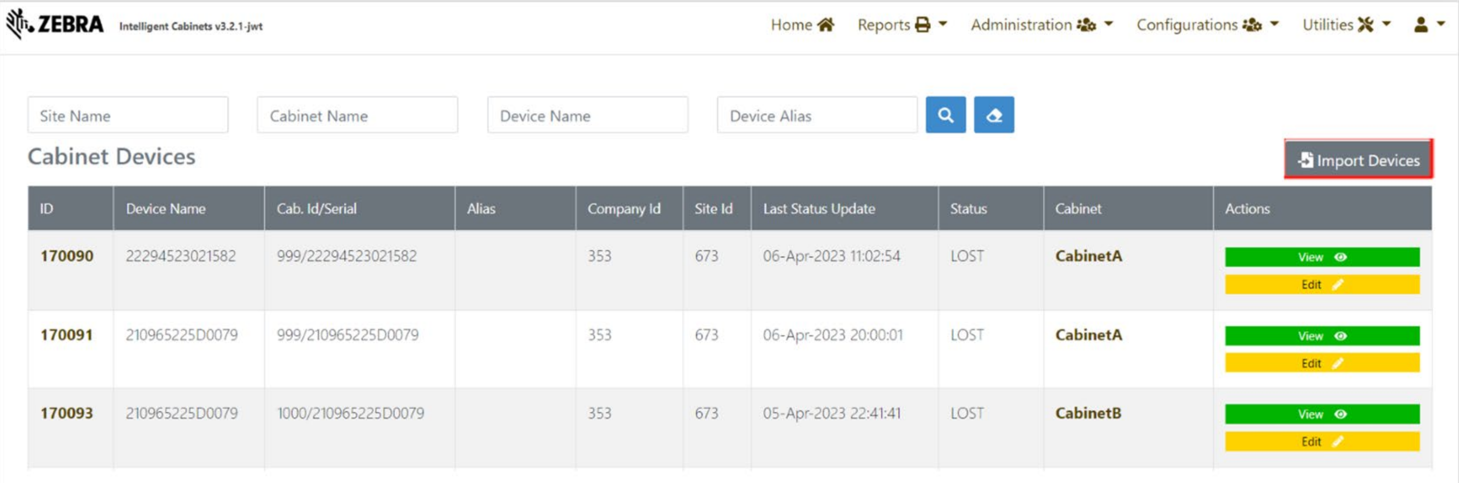
Cab. Id/Serial

999/22294523021582

Alias

Steps to use CSV import set device alias (friendly name)

1. This CSV Bulk import option has been added to Import Alias (friendly name) CSV file via the Portal. To access this option the Company-Admin must go to Administration à Cabinet Device.
2. The page will load, and this button will be displayed on top right corner of page

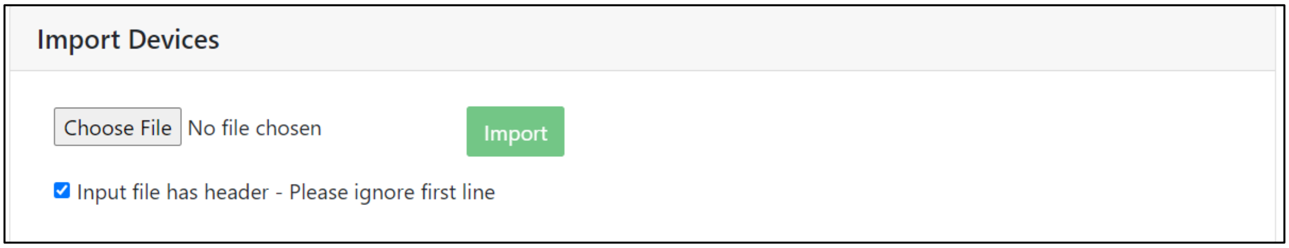


Cabinet Devices

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

3. Click on the button and a new page will load. This page displays all the details regarding Bulk Import Alias CSV file import. All the requirements are mentioned on this page including the template and the Upload Link.

NOTE: There is a check box placed underneath the choose file option. At the time of selecting CSV file to upload the option states.


Import Devices

Choose File No file chosen

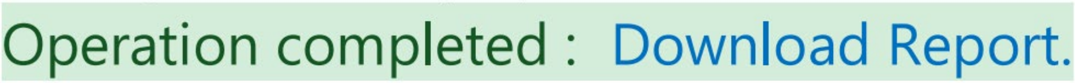
☑ Input file has header - Please ignore first line

If the check box is ticked – The first row of the CSV will be ignored being treated as header.

If the check box is unticked – The first row of the CSV will be processed as well.

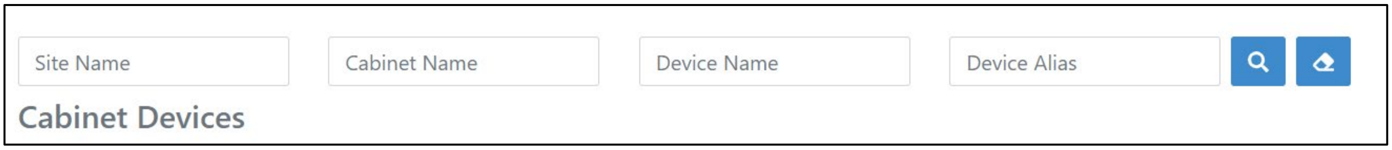
NOTE: Alias should be Unique at company Level.

4. After choosing the right file the user must click import. The file will be processed, and message will be displayed.



Operation completed : Download Report.

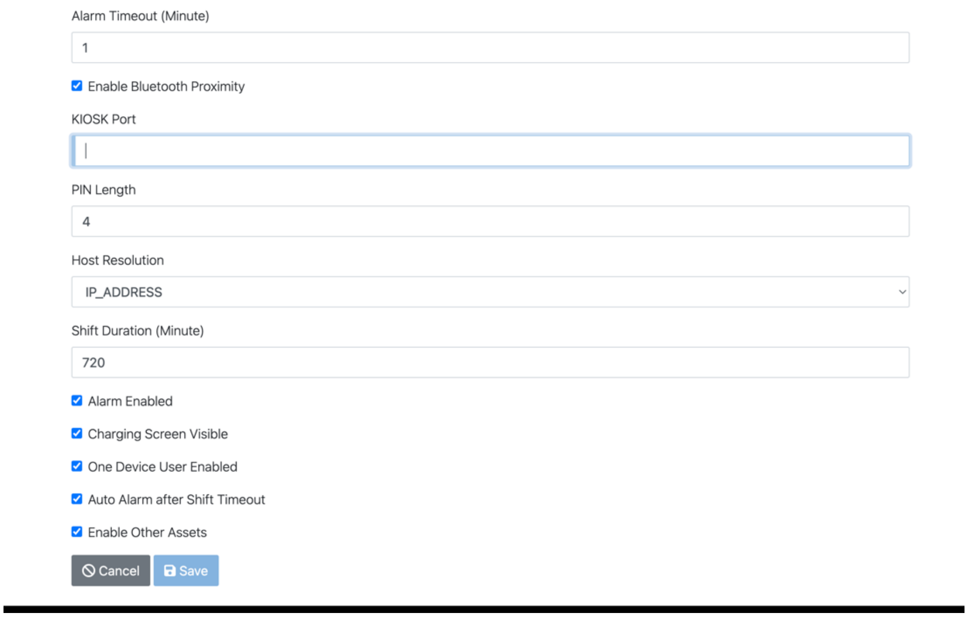
5. Search for device by Alias / Device Name Option can be accessed via Administration à Cabinet Device



Cabinet Devices

Other Asset:

- Devices which are not Android devices, and which are not connected to charge – fall under “Other Asset” category. Eg: Ring Scanner, Hammers, Helmet etc. No “Alarm functionality “is available for Other Asset.
- During the shift hours, when the device will be used, other asset devices will be in “In use” category. Once the shift duration is over and the device is not returned, in this case device will be moved to “missing” category and Admin can mark the device as “Lost” if it is not returned.
- Other Assets will have Asset ID/Barcode linked to each device. Other Assets will be registered with Asset ID to the Portal.
- From the Company setting screen, Other Asset functionality can be turned On/Off for Portal.



Alarm Timeout (Minute)

1

☑ Enable Bluetooth Proximity

KIOSK Port

|

PIN Length

4

Host Resolution

IP_ADDRESS

Shift Duration (Minute)

720

☑ Alarm Enabled

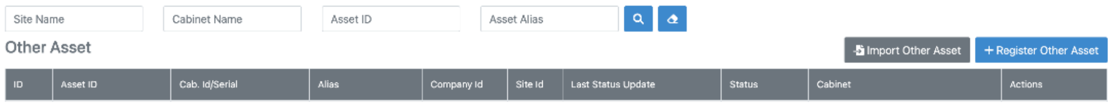
☑ Charging Screen Visible

☑ One Device User Enabled

☑ Auto Alarm after Shift Timeout

☑ Enable Other Assets

- Super admin /Company admin/Site admin will be able to import or register “Other Assets from Administration < Other Asset screen.
- Super admin/Company admin/Site admin will be able to View/Edit the Other Asset details.



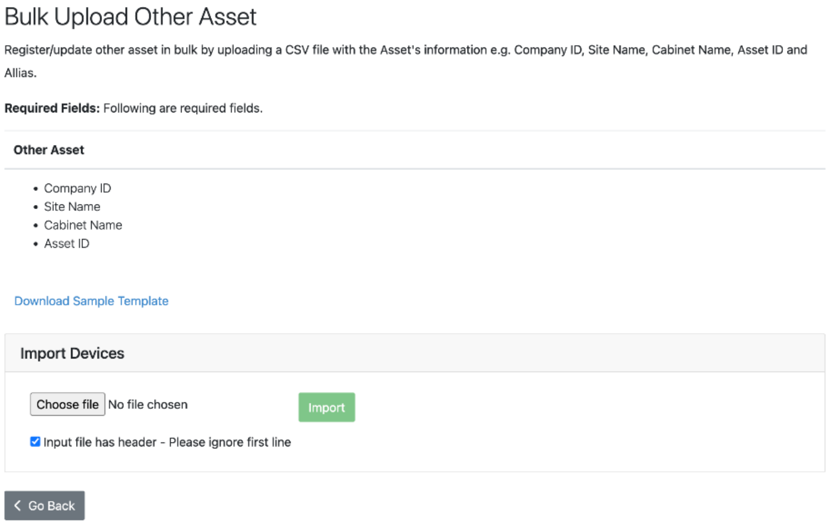
Other Asset

ID	Asset ID	Cab. Id/Serial	Alias	Company Id	Site Id	Last Status Update	Status	Cabinet	Actions

Import Other Asset:

- Click on “Import Other Asset”, import the file to import other Asset.

  Sample template is already provided to the screen.



Bulk Upload Other Asset

Register/update other asset in bulk by uploading a CSV file with the Asset's information e.g. Company ID, Site Name, Cabinet Name, Asset ID and Allias.

Required Fields: Following are required fields.

Other Asset

- Company ID
- Site Name
- Cabinet Name
- Asset ID

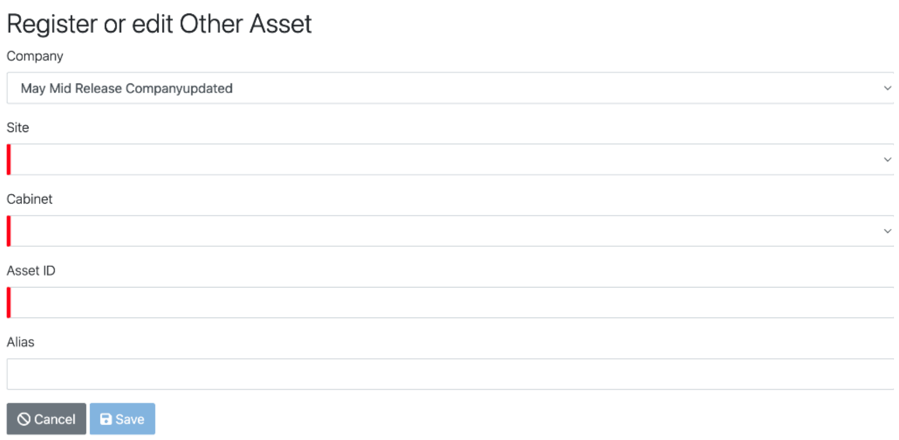
Download Sample Template

Import Devices

Choose file No file chosen

☑ Input file has header - Please ignore first line

Register Other Asset:



Register or edit Other Asset

Company

May Mid Release Companyupdated

Site

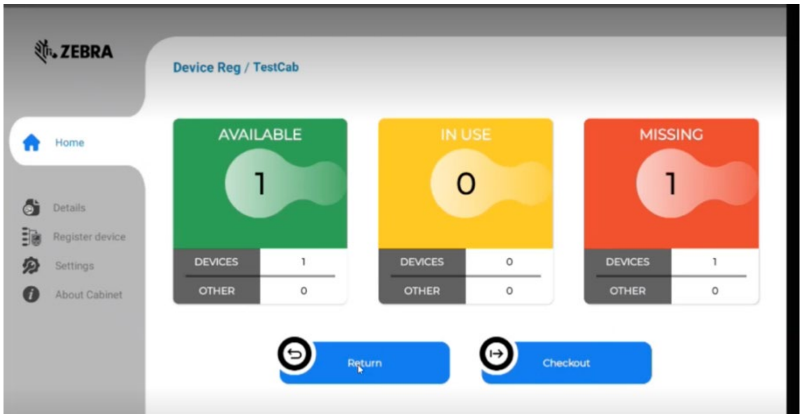
Cabinet

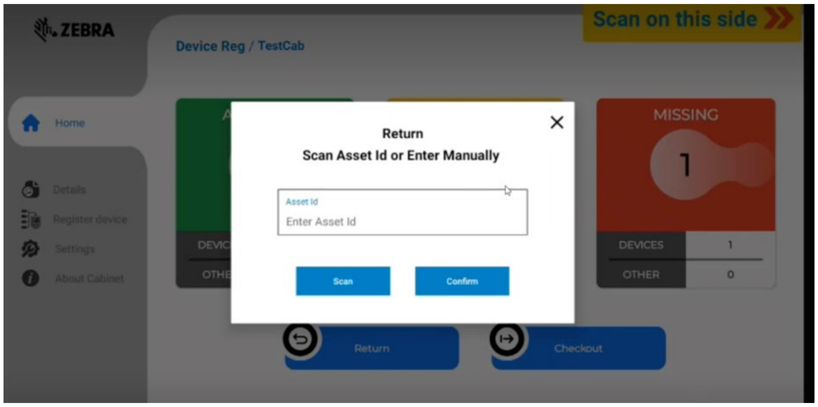
Asset ID

Alias

Registration of Other Asset through KIOSK:

Other Asset registration can happen through “Return” Button <Enter Asset ID< Scan. It will be registered with Site_Administrator pin.Registration can be done by Company administrator/ site administrator.

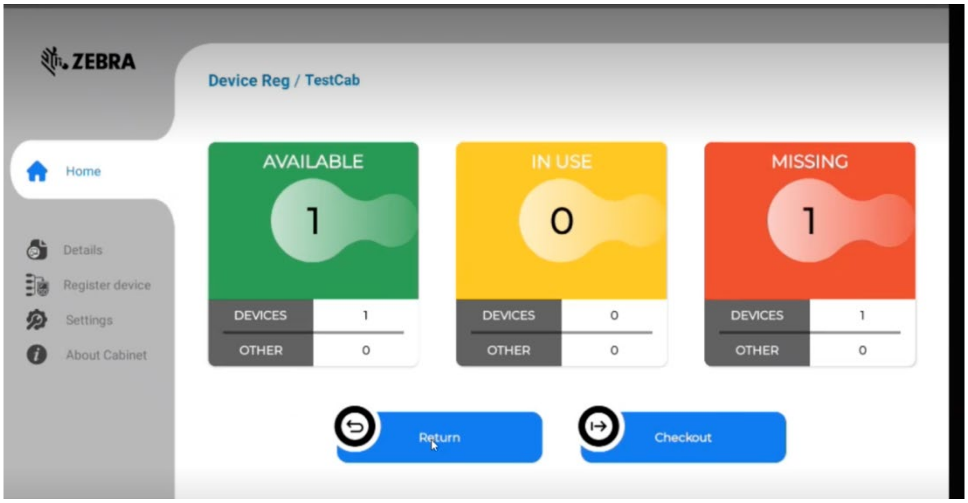


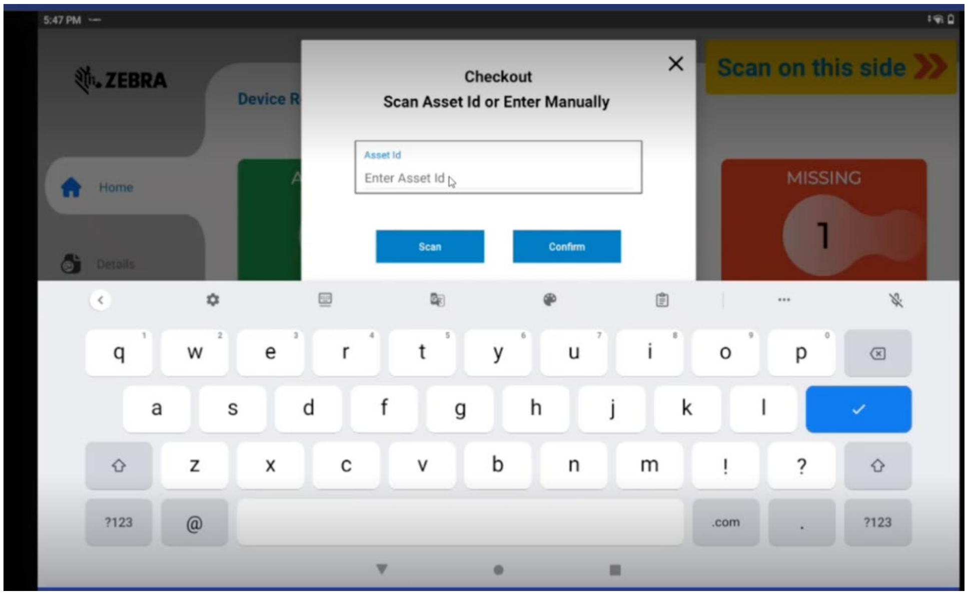


Note: When registration happens in KIOSK, only Site administrators can register the device and check out. When registration happens from Portal by Company Administrator,

Check Out Process:

User of type of ROLE device user would interact with the Kiosk by selecting checkout. Upon selecting checkout function user will select "SCAN" and then the scanner will be activate on the kiosk. Scan the asset you desire to checkout and select confirm, then user will be requested to   enter their PIN code. This feature will only work with those implementations whereby PIN code is the established authentication method.

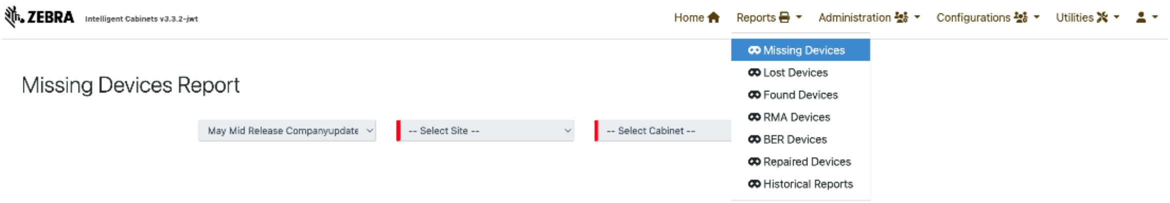




Checkout
Scan Asset Id or Enter Manually

Reports:

All the reports are available under the Report section.



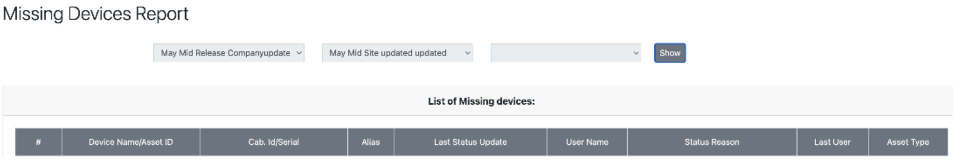
Missing Devices Report

Missing:

The number of devices removed from the Cabinet and have not yet logged in. The Missing status has three classifications and cover three Status reasons for missing device; Missing> Not_Returned, Missing> Invalid_Login, Missing> Communication_Lost.

To view a missing devices report:

1. Select the **Location** and **Cabinet** for which you would like to see the Missing devices.
2. Click **View Stats**. The report lists the below information.



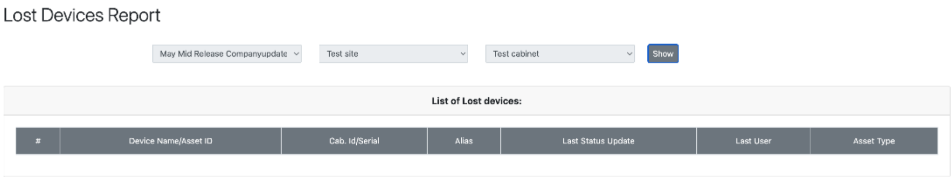
Missing Devices Report

List of Missing devices:

#	Device Name/Asset ID	Cab. Id/Serial	Alias	Last Status Update	User Name	Status Reason	Last User	Asset Type

Lost Devices:

Marking a device lost removes it from the ZAMS active devices. Therefore, they will no longer show up as missing.



Lost Devices Report

May Mid Release Companyupdate | Test site | Test cabinet | Show

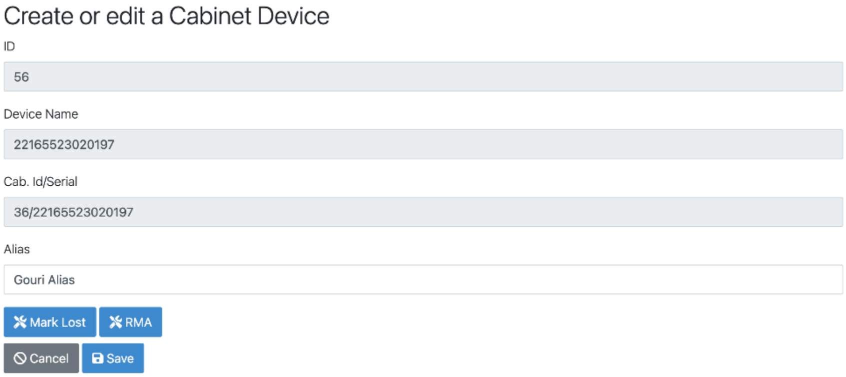
List of Lost devices:

#	Device Name/Asset ID	Cab. Id/Serial	Alias	Last Status Update	Last User	Asset Type

A Mobile Device can be marked lost via the following pages:

1. Dashboard/Home

2. From Cabinet Device List - Go to Administration à Cabinet Device à Choose the cabinet to be changed à Click Edit à Mark as Lost.



Create or edit a Cabinet Device

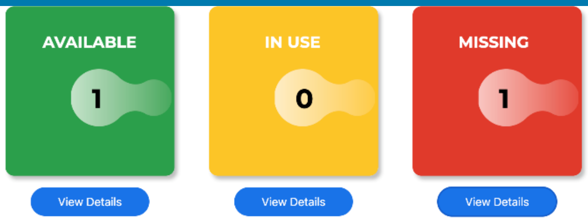
ID: 56

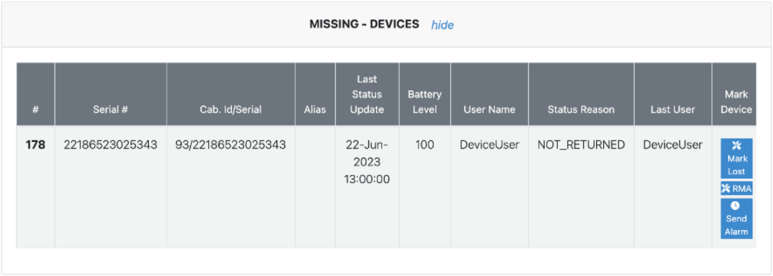
Device Name: 22165523020197

Cab. Id/Serial: 36/22165523020197

Alias: Gouri Alias

From Dashboard, Device can be marked as Lost.



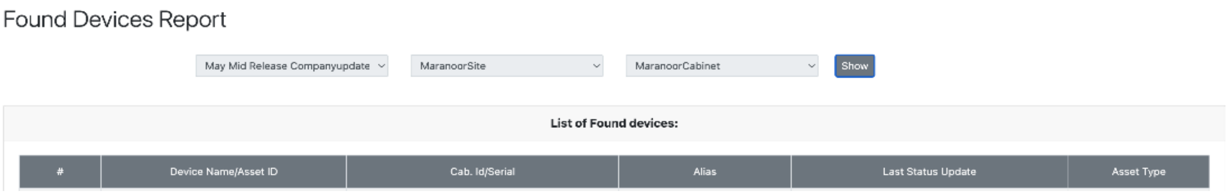

MISSING - DEVICES *hide*

#	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:

Administrator can mark the device as “Found” when it is returned.

From Cabinet Device List - Go to Administration à Cabinet Device à Choose the cabinet to be changed à Click Edit à Mark as Lost.

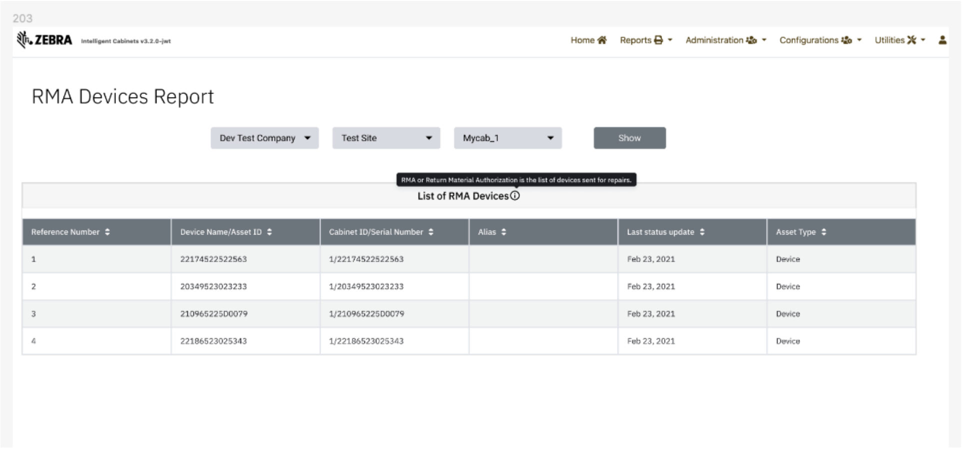

Found Devices Report

May Mid Release Companyupdate | MaranoorSite | MaranoorCabinet | Show

List of Found devices:

#	Device Name/Asset ID	Cab. Id/Serial	Alias	Last Status Update	Asset Type

RMA Devices:


203

RMA Devices Report

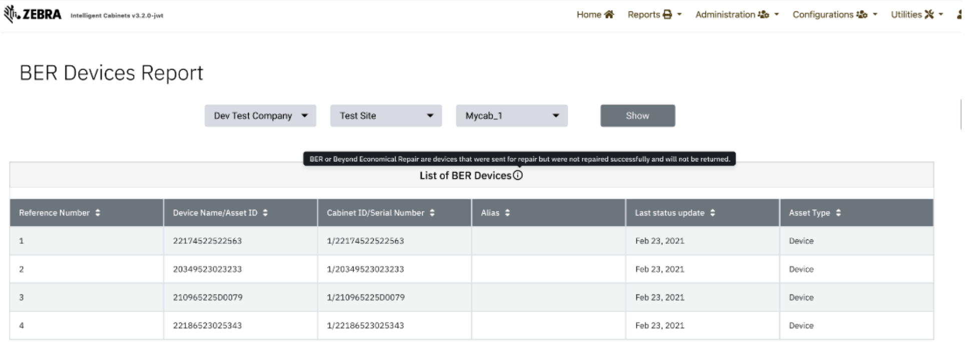
Dev Test Company | Test Site | Mycab_1 | Show

RMA or Return Material Authorization is the list of devices sent for repairs.

List of RMA Devices

Reference Number	Device Name/Asset ID	Cabinet ID/Serial Number	Alias	Last status update	Asset Type
1	22174522522563	1/22174522522563		Feb 23, 2021	Device
2	20349523023233	1/20349523023233		Feb 23, 2021	Device
3	210965225D0079	1/210965225D0079		Feb 23, 2021	Device
4	22186523025343	1/22186523025343		Feb 23, 2021	Device

BER Devices:



BER Devices Report

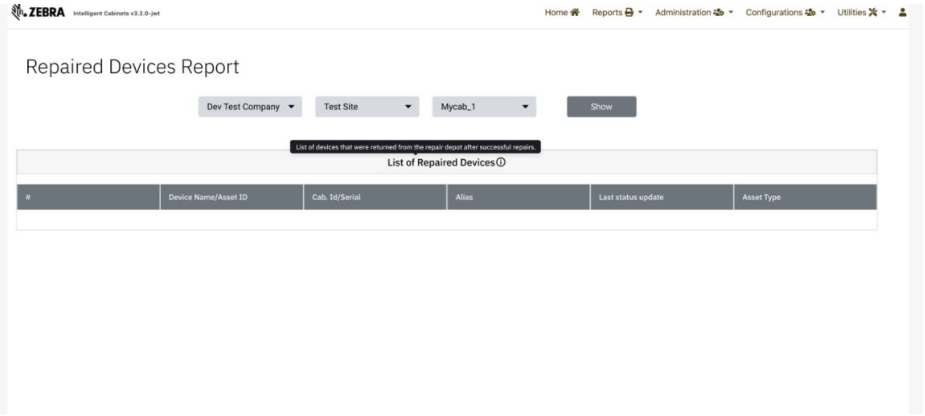
Dev Test Company | Test Site | Mycab_1 | Show

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

List of BER Devices

Reference Number	Device Name/Asset ID	Cabinet ID/Serial Number	Alias	Last status update	Asset Type
1	22174522522563	1/22174522522563		Feb 23, 2021	Device
2	20349523023233	1/20349523023233		Feb 23, 2021	Device
3	210965225D0079	1/210965225D0079		Feb 23, 2021	Device
4	22186523025343	1/22186523025343		Feb 23, 2021	Device

Repaired Devices:



Repaired Devices Report

Dev Test Company | Test Site | Mycab_1 | Show

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

List of Repaired Devices

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

Historical Reports

Historical Reports can now be exported to CSV format in addition to PDF format. As stated above, Company Admin and Company User will be able to generate and Export Historical reports to CSV in addition to PDF format.

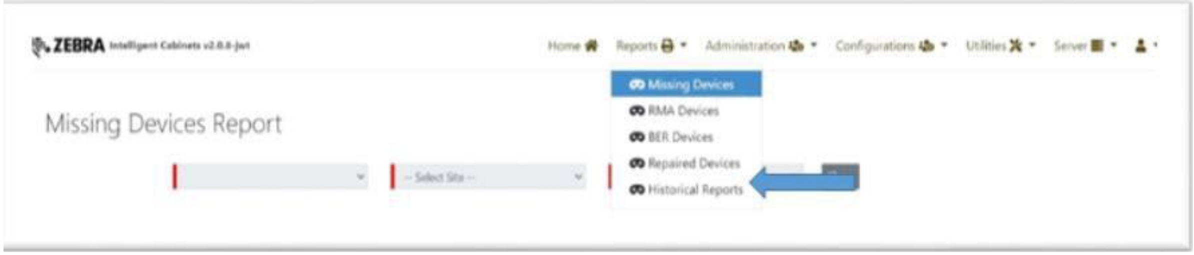
~~On contrary~~ A Site Admin will be able to generate and Export Historical Reports only for the relevant Site. There are three types of historical reports:

- Cabinet Devices Report (see To generate a Cabinet Devices Report: on page 20)
- Device Status Report (see To generate a Device Status Report: on page 21)
- User Devices Report (see The generate a User Device Report: on page 22)

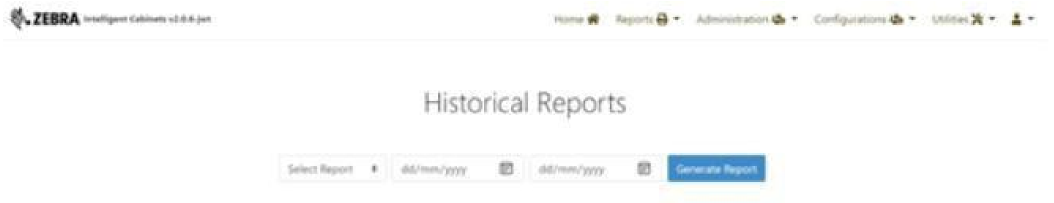
Generating Historical Reports

To generate and download reports:

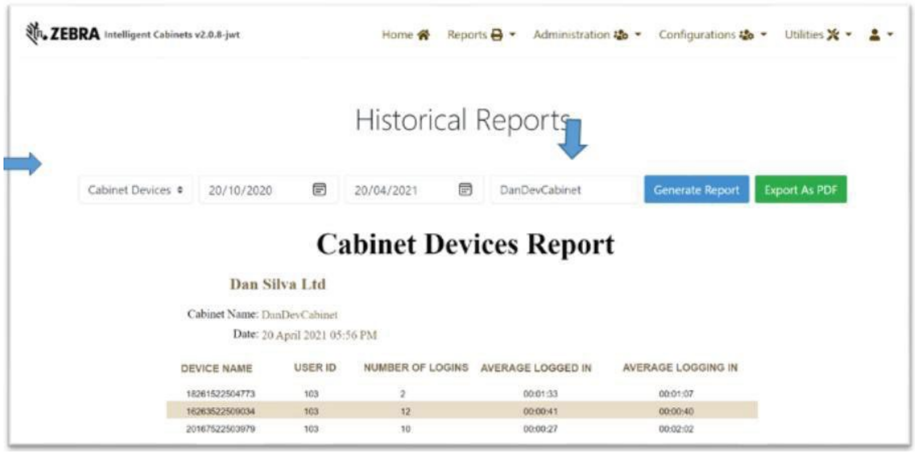
1. Log in to the Portal using Company Admin credentials.
2. Click on **Reports** from the top tabs.
3. Click on **Historical Reports** from the drop-down menu. The Historical Reports screen displays.



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



- To generate a **Cabinet Devices Report**:
  a. Select the desired date from the **Begin Date** field.
  b. Select the desired date from the **End Date** field.
  c. Enter the **Cabinet name** (example: DanDevCabinet)
  d. Click on **Generate Report.**



Cabinet Devices Report

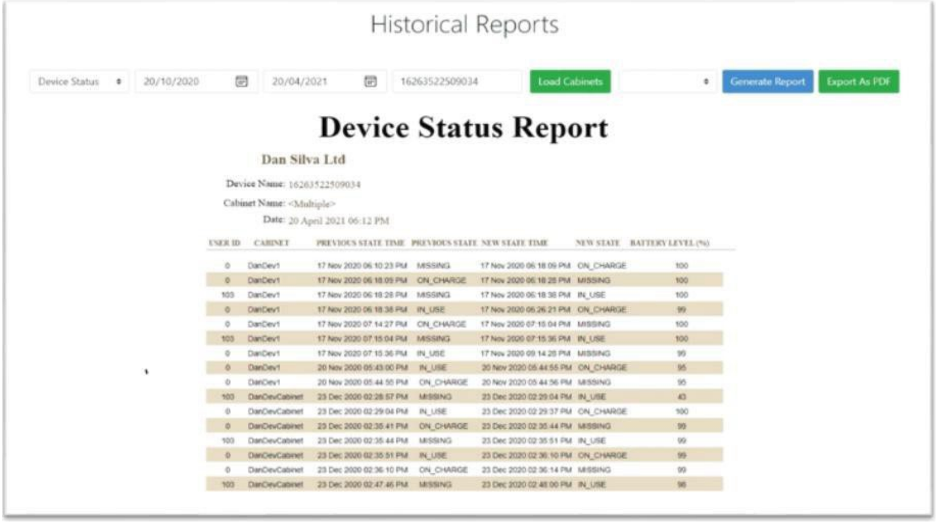
Dan Silva Ltd

Cabinet Name: DanDevCabinet

Date: 20 April 2021 05:56 PM

DEVICE NAME	USER ID	NUMBER OF LOGINS	AVERAGE LOGGED IN	AVERAGE LOGGING IN
18261522504773	103	2	00:01:33	00:01:07
16263522509034	103	12	00:00:41	00:00:40
20167522503979	103	10	00:00:27	00:02:02

- To generate a **Device Status Report**:
  a. Select the desired date from the **Begin Date** field.
  b. Select the desired date from the **End Date** field.
  c. Enter the **Device name** (example: DanDevCabinet).
  d. Clock on **Load Cabinet**. All the cabinets associated with s/n of the Device Name entered loads.
  e. There are two report generation options:
     - 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



Device Status Report

Dan Silva Ltd

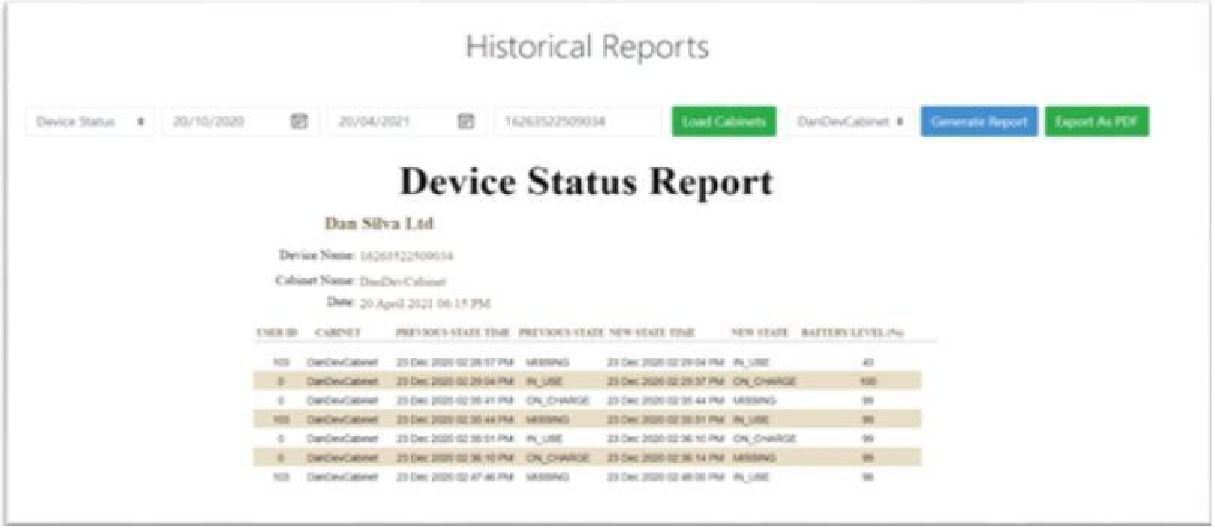
Device Name: 16263522509034

Cabinet Name: <Multiple>

Date: 20 April 2021 06:12 PM

USER ID	CABINET	PREVIOUS STATE TIME	PREVIOUS STATE	NEW STATE TIME	NEW STATE	BATTERY LEVEL (%)
0	DanDev1	17 Nov 2020 06:10:23 PM	MISSING	17 Nov 2020 06:18:09 PM	ON_CHARGE	100
0	DanDev1	17 Nov 2020 06:18:09 PM	ON_CHARGE	17 Nov 2020 06:18:28 PM	MISSING	100
103	DanDev1	17 Nov 2020 06:18:28 PM	MISSING	17 Nov 2020 06:18:38 PM	IN_USE	100
0	DanDev1	17 Nov 2020 06:18:38 PM	IN_USE	17 Nov 2020 06:26:21 PM	ON_CHARGE	99
0	DanDev1	17 Nov 2020 07:14:27 PM	ON_CHARGE	17 Nov 2020 07:15:04 PM	MISSING	100
103	DanDev1	17 Nov 2020 07:15:04 PM	MISSING	17 Nov 2020 07:15:36 PM	IN_USE	100
0	DanDev1	17 Nov 2020 07:15:36 PM	IN_USE	17 Nov 2020 09:14:28 PM	MISSING	99
0	DanDev1	20 Nov 2020 05:43:00 PM	IN_USE	20 Nov 2020 05:44:55 PM	ON_CHARGE	95
0	DanDev1	20 Nov 2020 05:44:55 PM	ON_CHARGE	20 Nov 2020 05:44:56 PM	MISSING	95
103	DanDevCabinet	23 Dec 2020 02:28:57 PM	MISSING	23 Dec 2020 02:29:04 PM	IN_USE	43
0	DanDevCabinet	23 Dec 2020 02:29:04 PM	IN_USE	23 Dec 2020 02:29:37 PM	ON_CHARGE	100
0	DanDevCabinet	23 Dec 2020 02:35:41 PM	ON_CHARGE	23 Dec 2020 02:35:44 PM	MISSING	99
103	DanDevCabinet	23 Dec 2020 02:35:44 PM	MISSING	23 Dec 2020 02:35:51 PM	IN_USE	99
0	DanDevCabinet	23 Dec 2020 02:35:51 PM	IN_USE	23 Dec 2020 02:36:10 PM	ON_CHARGE	99
0	DanDevCabinet	23 Dec 2020 02:36:10 PM	ON_CHARGE	23 Dec 2020 02:36:14 PM	MISSING	99
103	DanDevCabinet	23 Dec 2020 02:47:46 PM	MISSING	23 Dec 2020 02:48:00 PM	IN_USE	98

- 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 | DanDevCabinet

Device Status Report

Dan Silva Ltd

Device Name: 16263522509034

Cabinet Name: DanDevCabinet

Date: 20 April 2021 06:15 PM

USER ID	CABINET	PREVIOUS STATE TIME	PREVIOUS STATE	NEW STATE TIME	NEW STATE	BATTERY LEVEL (%)
103	DanDevCabinet	23 Dec 2020 02:28:57 PM	MISSING	23 Dec 2020 02:29:04 PM	IN_USE	40
0	DanDevCabinet	23 Dec 2020 02:29:04 PM	IN_USE	23 Dec 2020 02:29:37 PM	ON_CHARGE	100
0	DanDevCabinet	23 Dec 2020 02:35:41 PM	ON_CHARGE	23 Dec 2020 02:35:44 PM	MISSING	99
103	DanDevCabinet	23 Dec 2020 02:35:44 PM	MISSING	23 Dec 2020 02:35:51 PM	IN_USE	99
0	DanDevCabinet	23 Dec 2020 02:35:51 PM	IN_USE	23 Dec 2020 02:36:10 PM	ON_CHARGE	99
0	DanDevCabinet	23 Dec 2020 02:36:10 PM	ON_CHARGE	23 Dec 2020 02:36:14 PM	MISSING	99
103	DanDevCabinet	23 Dec 2020 02:47:46 PM	MISSING	23 Dec 2020 02:48:00 PM	IN_USE	98

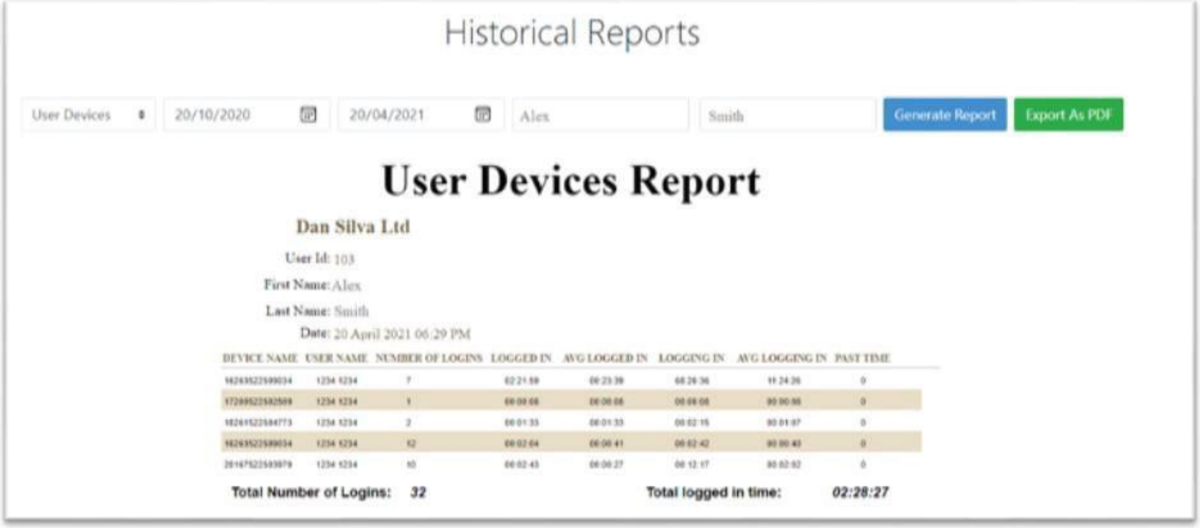
- The generate a **User Device Report**:

a. Select the desired date from the **Begin Date** field.

b. Select the desired date from the **End Date** field.

c. Enter the **User ID.**

d. Click **Generate**.



Historical Reports

User Devices | 20/10/2020 | 20/04/2021 | Alex | Smith

User Devices Report

Dan Silva Ltd

User Id: 103

First Name: Alex

Last Name: Smith

Date: 20 April 2021 06:29 PM

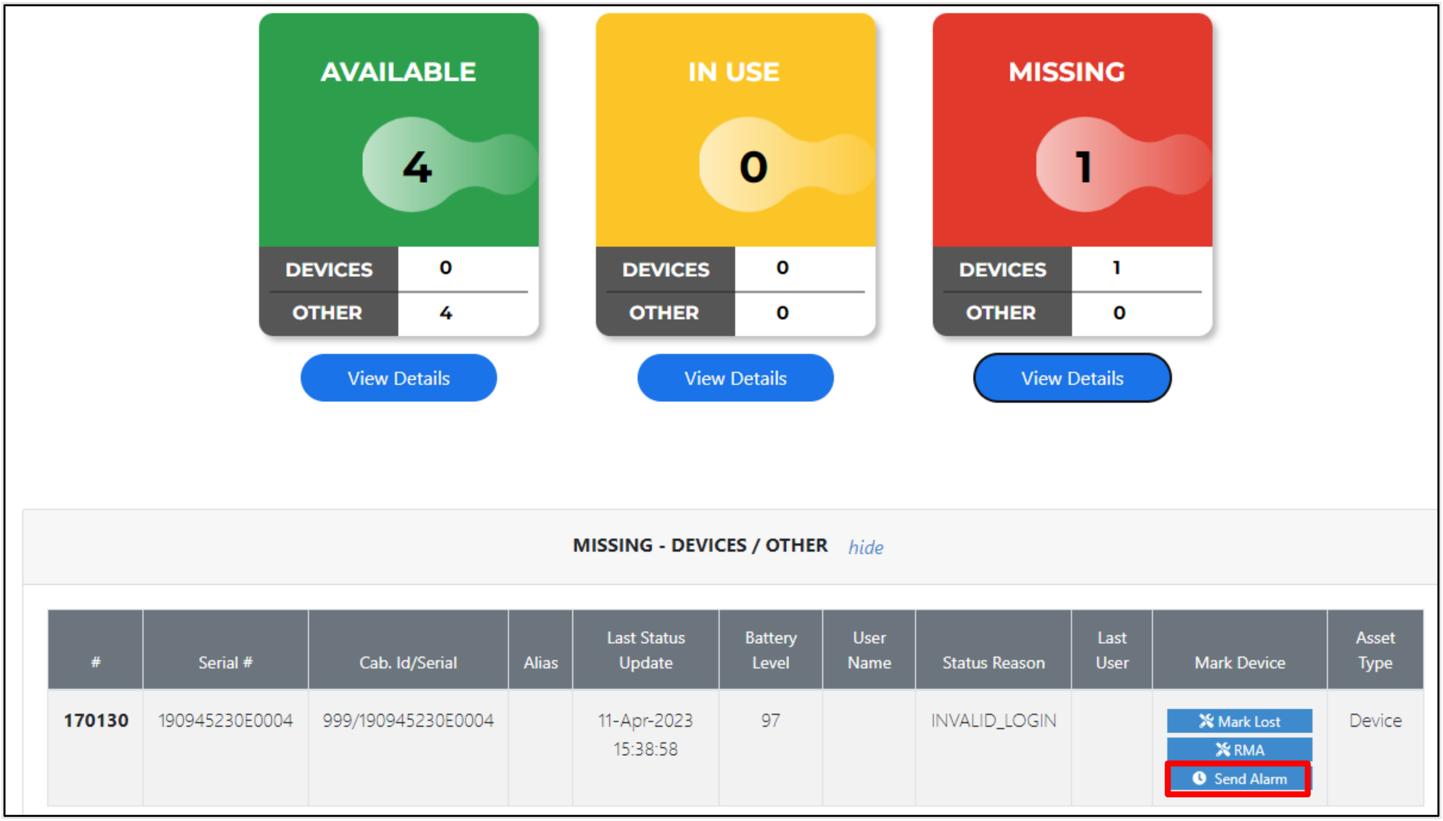
DEVICE NAME	USER NAME	NUMBER OF LOGINS	LOGGED IN	AVG LOGGED IN	LOGGING IN	AVG LOGGING IN	PAST TIME
16263522509034	1234 1234	7	02:21:59	00:23:39	68:26:36	11:24:26	0
17289522582509	1234 1234	1	00:00:08	00:00:08	00:08:08	00:00:08	0
16261522584773	1234 1234	2	00:01:33	00:01:33	00:02:15	00:01:07	0
16263522509034	1234 1234	12	00:02:04	00:00:41	00:02:42	00:00:43	0
20167522593979	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*

Alarms: Send alarms & Auto alarms

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

If user does not log in within the 2 mins (or configurable Alarm timeout of the Company), device alarms until:
a. Battery dead
b. User logs in by entering a valid pin
c. Device returned to charger and its in range
d. Master QR Scanned. If ZAMS UI is turned off via a configuration setting, scanning an unlock code is managed by the application presenting the UI on the mobile device



MISSING - DEVICES / OTHER *hide*

#	Serial #	Cab. Id/Serial	Alias	Last Status Update	Battery Level	User Name	Status Reason	Last User	Mark Device	Asset Type
170130	190945230E0004	999/190945230E0004		11-Apr-2023 15:38:58	97		INVALID_LOGIN		Mark Lost RMA Send Alarm	Device

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

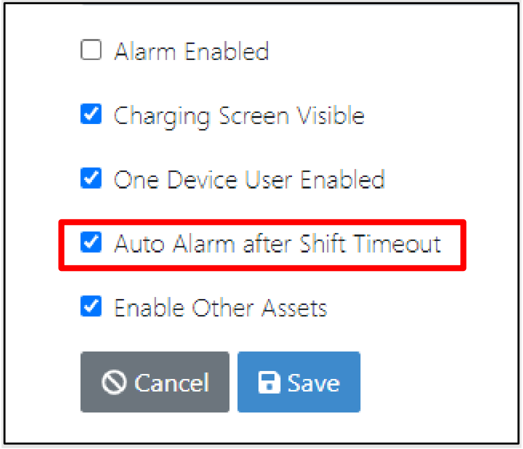
On the Dashboard the "Send Alarm" will change to "Sent" after being tapped. The portal will communicate with the Kiosk and the Kiosk will send the Alarm notification to the device. The "Sent" button will be automatically changed to "Send Alarm" within one minute.

"Send Alarm" button is also available in Actions columns in the Administration à Cabinet Devices list. All the rules are applicable as described above. There is only one exception: once the "Send Alarm" is pressed it will change to "Sent". The Portal will send a call to the Kiosk and the Kiosk will communicate with the Device. The only exception is the “sent” button will not automatically revert to “Send Alarm”. The page needs to be refreshed in order for that to take effect.

Auto alarms

An “auto alarm” configuration option enables missing devices to automatically sound an alarm until no longer missing.

From the dashboard, go to Administration à Company à Scroll down to find the check box :



□ Alarm Enabled

☑ Charging Screen Visible

☑ One Device User Enabled

☑ Auto Alarm after Shift Timeout

☑ Enable Other Assets

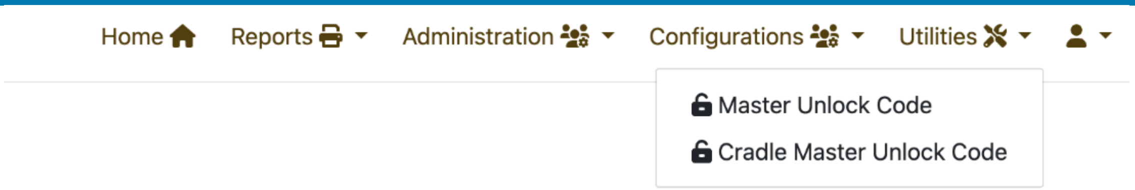
If checked, device will alarm automatically when it is not returned to cradle after shift timeout.

- ZAMS client on Mobile Device knows it is missing based on shift duration.
- On Mobile Device, if shift duration has expired, log in screen come on the UI
- If user does not log in within the 2 minutes (configurable Alarm timeout), device alarms until either the is battery dead, user logs in or the device is returned by the user to cabinet/charger and in range. Also, Master 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:

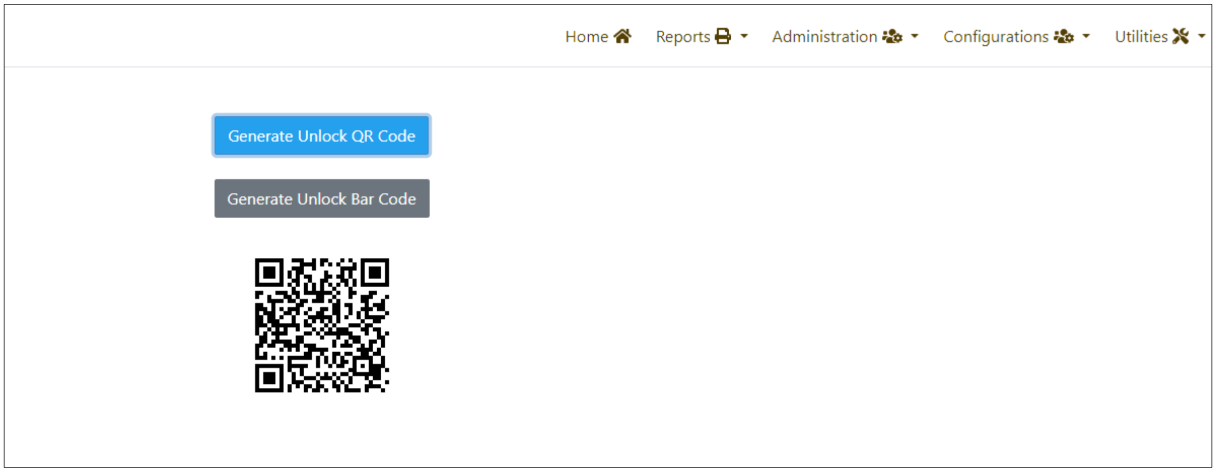
1. Click **Master Unlock Code** from the **Utilities** drop-down menu.



Click **Generate Unlock**

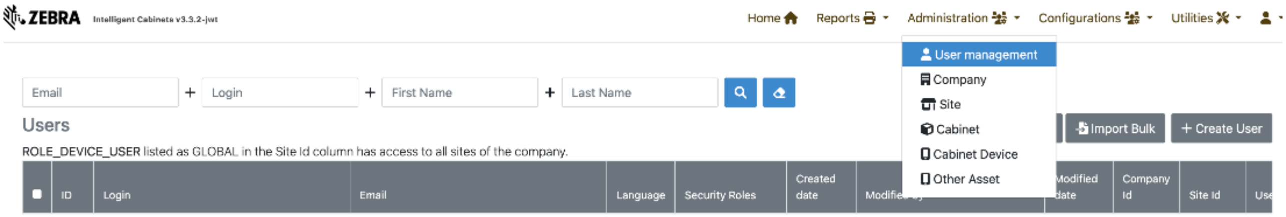
2. Scan the QR Code from the portal to unlock the mobile device.

NOTE: The Master QR is set to expire after 48 hours after being generated. Master QR Code is unique for every company. The Master QR Code generated by Administrator



User Management:

Administrators can add the users either from Portal "Create User “or “Bulk User” functionality.



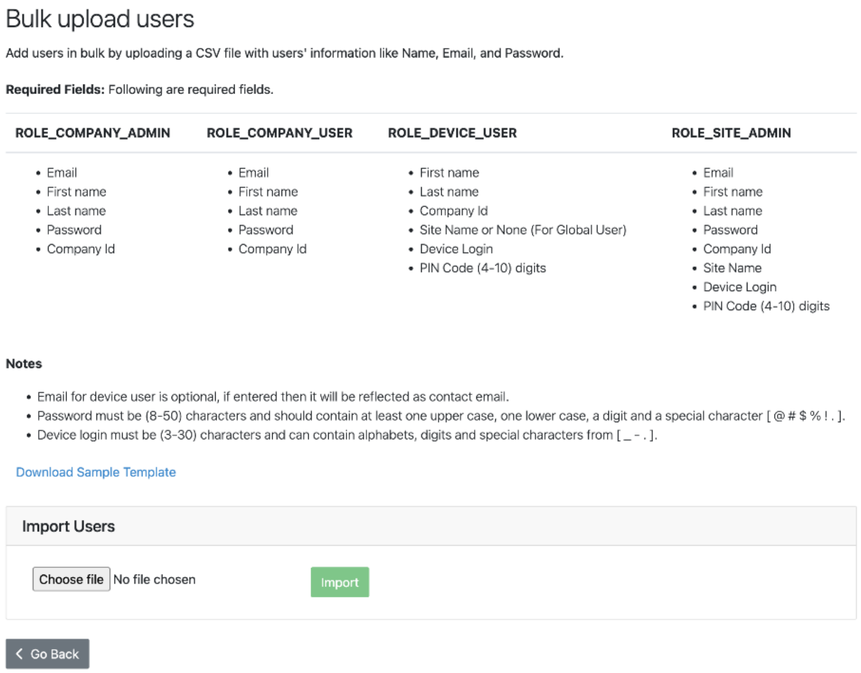
Users

ROLE_DEVICE_USER listed as GLOBAL in the Site Id column has access to all sites of the company.

■	ID	Login	Email	Language	Security Roles	Created date	Modifie	Modified date	Company Id	Site Id	Use

Import Bulk:

Administrators will be able to import multiple users at a time using “Import Bulk”.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
• Email • First name • Last name • Password • Company Id	• Email • First name • Last name • Password • Company Id	• First name • Last name • Company Id • Site Name or None (For Global User) • Device Login • PIN Code (4-10) digits	• 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

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

Adding Device User

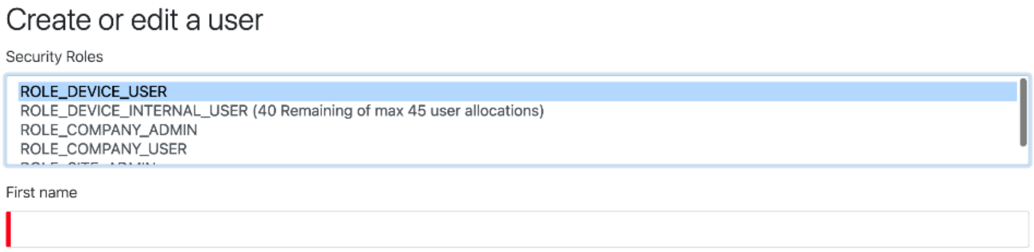
A Company Admin can create new device users as follows:

1. Login 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

There are different types of user roles that can be created while creating a new user as seen from the screenshot below.



Create or edit a user

Security Roles

ROLE_DEVICE_USER
ROLE_DEVICE_INTERNAL_USER (40 Remaining of max 45 user allocations)
ROLE_COMPANY_ADMIN
ROLE_COMPANY_USER

First name

1. **SITE ADMIN**: A Site_Admin will have valid credentials to access to the ZAMS Portal. Site Admin will have a limited role in terms of accessing the relevant company data. Site Admin will have access to the following:

- A Site Admin will have access to the Dashboard where he/she can only view stats of his/her site and cabinets registered to that site.
- Site Admin can Register Kiosk with valid credentials.
- Site Admin also has Device User Login Credentials in addition to being a Site Admin. Therefore, additional user fields are needed when creating the user.
- Site Admin can create Notification Configuration (Email Alerts) for the relevant site.
- Site Admin can generate reports for his site only.
- Site Admin have Read only access to the following:
    - 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 authority to create new cabinets. View and Edit access for corresponding Cabinet/s for the site.
    - Generate Master QR code from Utilities Menu if needed.

2. **COMPANY USER**: A Company User will have valid credentials to access to the ZAMS Portal. These are the functions:

    - A Company User full access to generate and export Reports in addition to having access to generate Master QR code.
    - A Company User will have Read Only access to the following:
        - Dashboard
        - Administration > User Management

- Administration > Site Administration > Cabinet o Administration > Cabinet Device

3. **DEVICE USER:** there are two types of device users: 1) For a particular site 2) Global

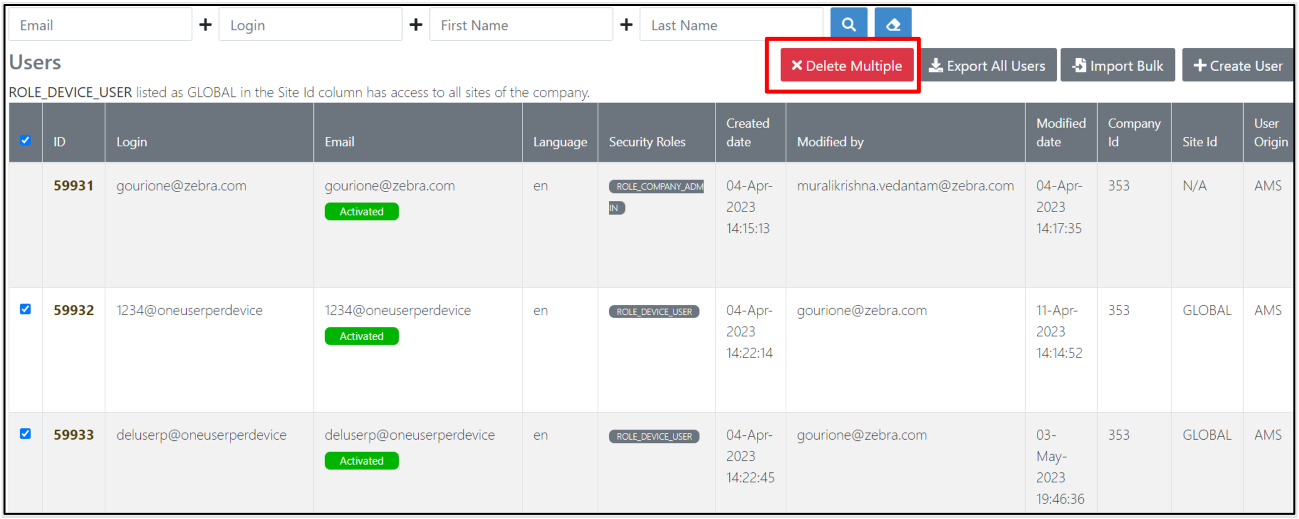
A device user for a particular site will have restricted access in terms to checking out a Device. Such a Device User will only be able to check out a Mobile Device associated to the Site using his/her pin code. If the pin code of Device associated to a particular site is, enter on a Mobile Device Associated to another site then error will be displayed “Invalid Pin”.

Device User with the attributes “**Global”** can access any site associated to the Company. A Device user can use his/her pin code to checkout a Mobile Device from any of the 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 on “Delete Multiple”.

Caution: When the user is deleted, user related information will be deleted.

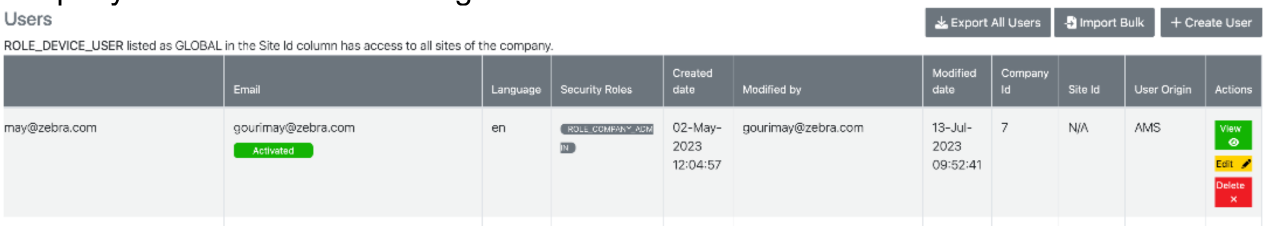


Users

ROLE_DEVICE_USER listed as GLOBAL in the Site Id column has access to all sites of the company.

☑	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
☑	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
☑	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

Company admin can delete a single user at a time.



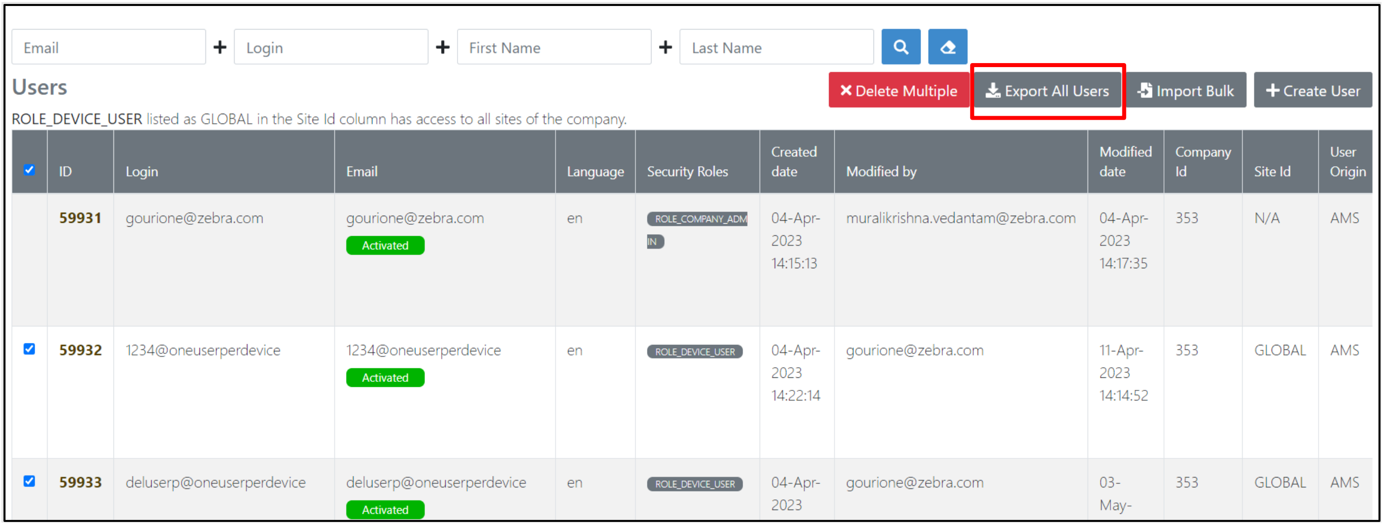
Users

ROLE_DEVICE_USER listed as GLOBAL in the Site Id column has access to all sites of the company.

	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	ROLE_COMPANY_ADMIN	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. Just by a click of a button all the existing users of the company can be exported to a CSV file. This is a feature for the company administrator only.



Users

ROLE_DEVICE_USER listed as GLOBAL in the Site Id column has access to all sites of the company.

☑	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
☑	**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
☑	**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 correct site name or Global in the site field for device user the record will not be processed.

When logged in as Site admin: can upload a CVC (CSV?) to ZAMS portal and has the privilege to Import new Device users or update existing Device Users. Furthermore, 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 whereby a record is maintained of who has taken what device and when it was returned. This system will significantly reduce device loss, simply by making the users aware that whenever they take a device and log onto it that that action is being recorded. 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 have a huge effect upon the casual loss of devices simply by encouraging users to return their device and discouraging a casual attitude to the 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 onto the device.

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

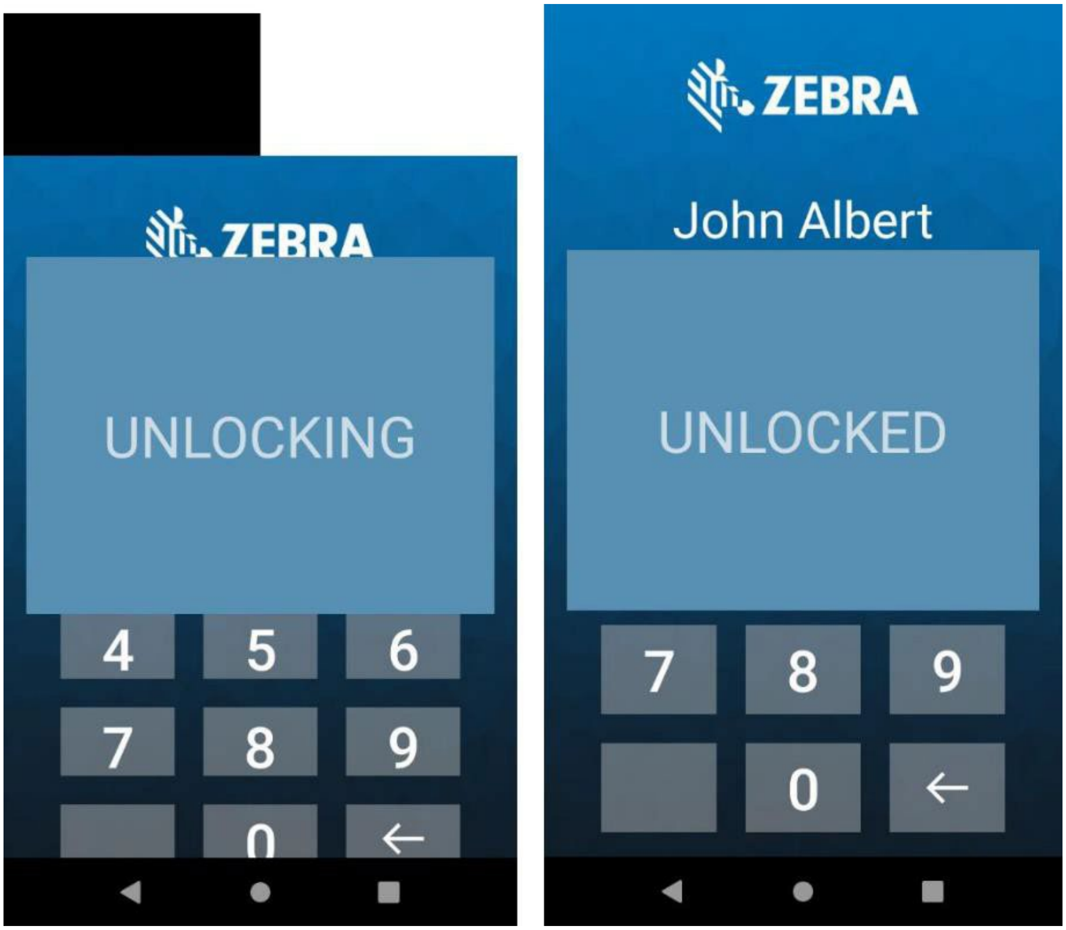
Cradle Lock, Cradle & Devices

Using the Cradlelock:

Swipe the battery icon or Tap to the Log in Button

Enter a PIN while the Device is Docked and locked in the cradle lock.

- If the entered PIN is **invalid** a toast appears: “Invalid PIN entry – Please, try again.”
- If **valid** PIN is entered, then the following messages is shown on the Device UI.



UNLOCKING

John Albert

UNLOCKED

Cradle Master Unlock Code

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

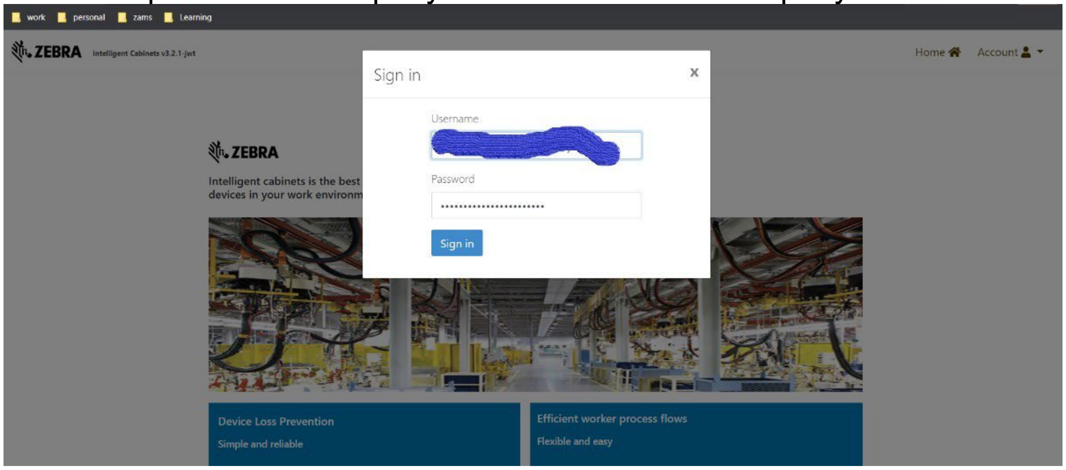
This feature helps users in situations like kiosk going into an un-responsive state for long time and not allowing the users to take device from cradle.

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

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

Below are the steps for generating Cradle Master Unlock Code

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



Intelligent cabinets is the best
devices in your work environm

Sign in ×

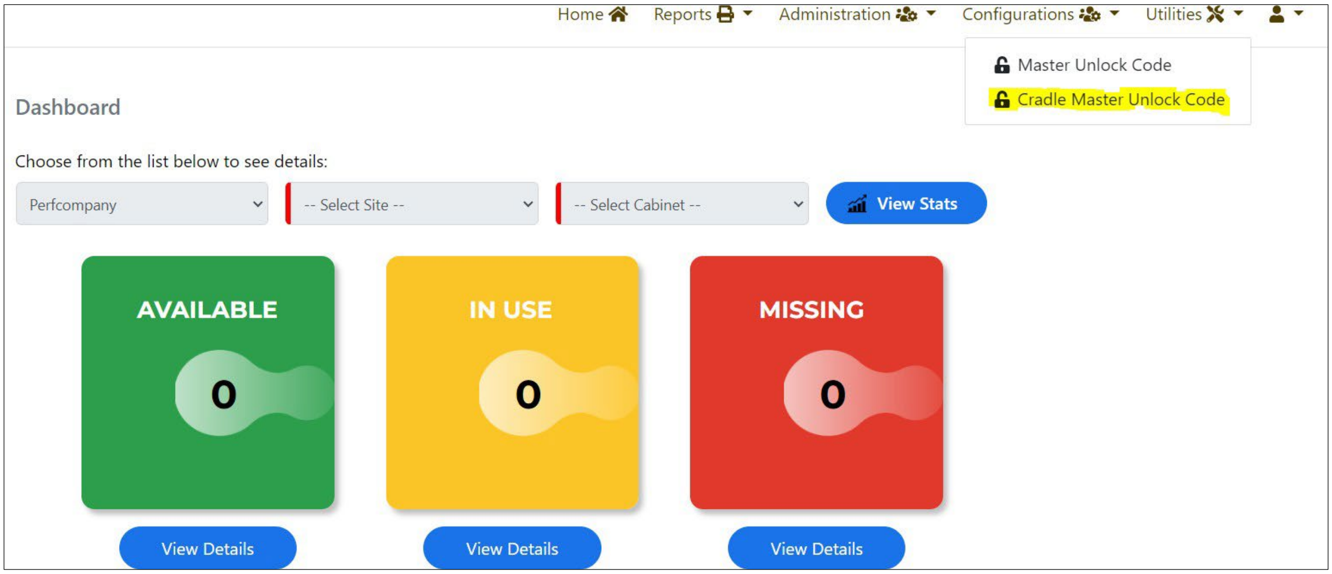
Username [redacted]

Password ••••••••••••••••••••••••

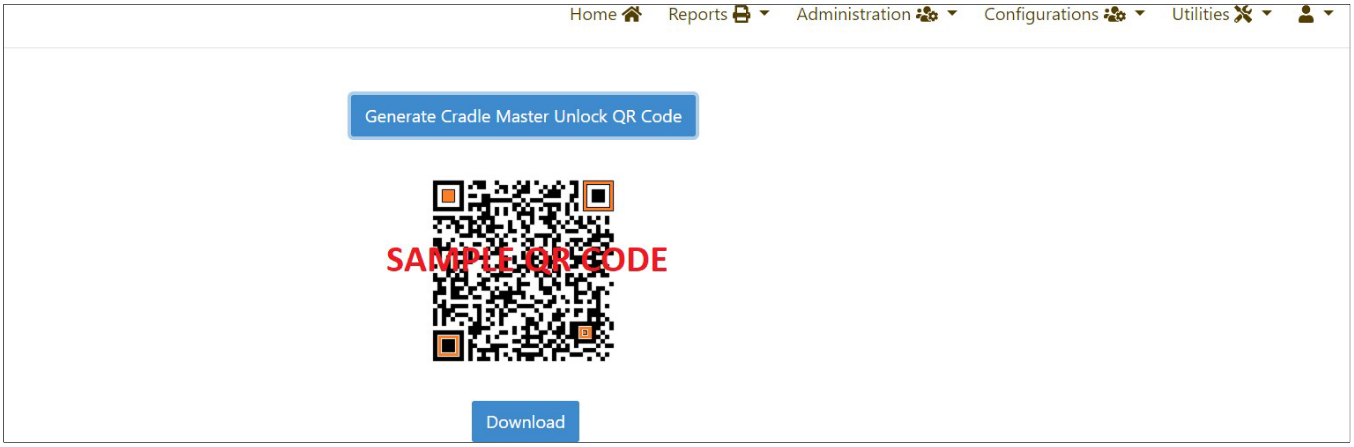
Sign in

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

Cradle Lock Feature

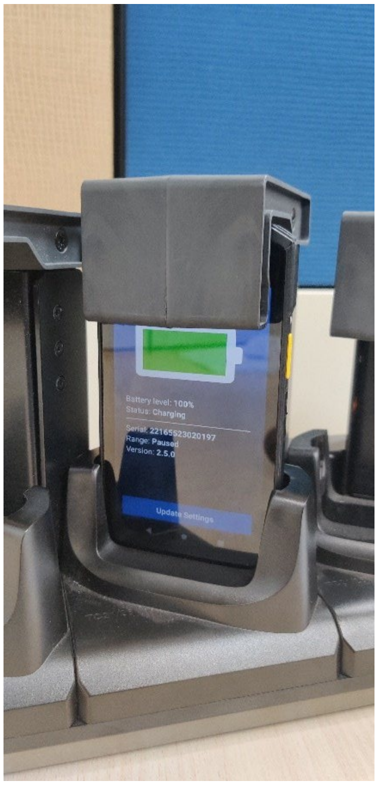


Click on “Generate Cradle Master Unlock Code” to generate a QR code. Click on “Download” to download the
QR code.

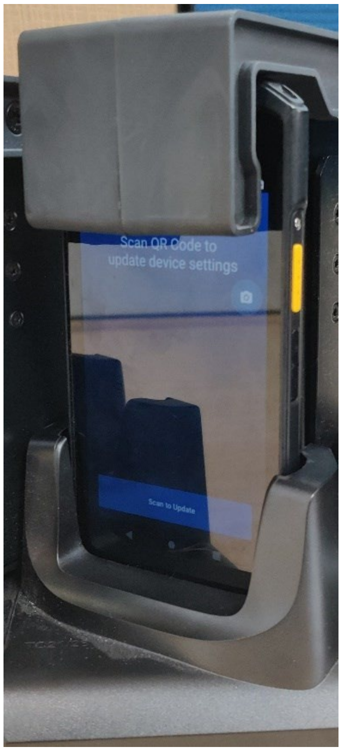


Downloaded QR code can be printed on a paper.

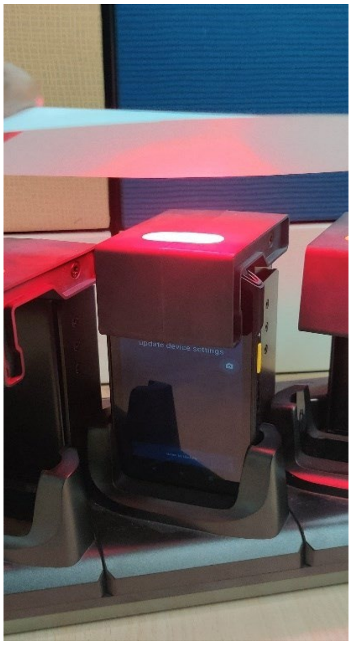
To unlock the device from Cradle, select “update settings” from charging screen as shown in the picture.



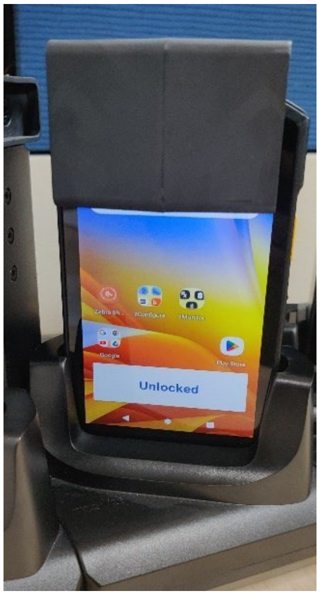
On “update settings” page select “scan to update” button as shown in the picture. Device starts scannerbeam.



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



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



Troubleshooting

Table 4 Troubleshooting

Problem	Possible Cause	Possible Solution
Zebra Terminal 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 Master Unlock barcode from the portal as a temporary solution to allow the user to work.
Unable to reach the Cabinet. Please scan QR code message displayed if undocked.		
ZAMS application does not allow a user to log on to the terminal.	The password is not recognized as valid.	Return the terminal 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.
ZAMS Lock screen is not shown but the alarm is sounding after the allotted time.	To allow some third-party applications to have access, ZAMS can to move into the background but still function.	Tap on the **AMS Device System** Icon and bring it to the foreground to allow sign on.

		Alternatively, return the terminal to its Location/cradle to stop the alarm sounding and re-set the lock screen.
The ZAMS Lock screen does not come to the foreground when the terminal is returned to its charging cradle.	Check that the terminal 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: • Scan QR code	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.
• Access to its location • Store its registration data.		

Technical Support

When your own Help Desk is unable to solve your issue entitled to technical support, you can escalate issues to the Zebra support team. Please 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/us/en/about-zebra/contact-zebra/contact-tech-support.html.

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.