

# ZAMS Release Notes

ZAMS Release Sprint-22.4.1, January 20, 2023

## Contents

Introduction.....	3
Version scheme .....	4
Target Environments .....	4
1 Change Highlights (Release Sprint-22.4.1) .....	5
1.1 ZAMS Server (v3.2.0).....	5
1.1.1 New Features.....	5
1.1.2 Bug Fixes.....	7
1.2 Cabinet Kiosk AMS (Core v1.4.1 and UI v1.3.0).....	7
1.2.1 New Features: .....	7
1.2.2 Bug Fixes.....	8
1.3 Device AMS (v2.4.0).....	9
1.3.1 New Features: .....	9
1.3.2 Bug fixes.....	9
2 Known Constraints and Workarounds.....	10
3 Appendix.....	11
3.1 Non-Android.....	11
3.1.1 ZAMS Server .....	11
i. Dashboard .....	11
ii. Mark an Asset to RMA or Lost.....	13
iii. Register a new Other Asset .....	13
iv. Bulk Import Other Asset.....	15
v. Other Asset Management after Registration.....	16
vi. Edit Asset Attribute and Mark Lost/RMA.....	17
vii. Reports .....	18
3.1.2 KIOSK and UI.....	19
i. Data wedge Profile for Kiosk .....	19
ii. Register/Return Other Asset .....	19
iii. Register a New Other Asset by clicking Return Button.....	20
iv. Return an Asset already registered to the Kiosk.....	22
v. Move an Other Asset marked RMA/Lost Back to ZAMS .....	22

vi. Checkout Other Asset.....	23
vii. Checkout an Asset already registered to the Kiosk.....	23
viii. Register a new Asset at Checkout.....	24
ix. Details Tab.....	26
x. About Tab.....	27
3.1.3 Imprivata and ZAMS reference information.....	28
4 Important Links.....	30

## Introduction

This document outlines the new features and changes since last release Zebra Access Management System (ZAMS) software.

ZAMS software is comprised of 3 elements that are recommended to be installed at the same time. Although various combinations of the software elements may work without issue, release validation and support is limited to the underlying version configurations noted.

ZAMS Software elements contain:

1. **Mobile Device application and services:** provides the lock screen UI and services for the android based mobile devices.
2. **Kiosk application and services:** provides on-site device management, UI and provides information to cloud based console. The Kiosk application is designed for Zebra’s CC6000/ET40 devices.
3. **Cloud resident console:** Web portal that provides various administration level tasks and reports. The server access location is <https://zams.zebra.com/>

The following is an explanation of the files distributed in this release.

ZAMS SW release components

Item	Area	Description
AMS Server (URL) <a href="https://zams.zebra.com">https://zams.zebra.com</a>	Portal	ZAMS (cloud) Portal
AMS Core APK	Kiosk	Core services APK for CC6000/ET40 to operate AMS
AMS UI APK	Kiosk	UI APK for CC6000/ET40 user interface
AMS Device APK	Mobile Device	APK for mobile devices in AMS application
dwprofile_AmsDevice.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application device registration
dwprofile_amsPin.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application PIN scanning

dwprofile_code128_barcode_profile.db (part of auto install content)	Mobile Device	DataWedge profile for AMS application code128 barcode scanning
dwprofile_nmc.db (part of auto install content)	Kiosk	DataWedge profile for AMS application to scan barcodes for non-mobile devices
ZamsAutoInstall files and directory structure. (See install doc for details)	Kiosk and Mobile Device	Supporting files and documentation used to automate installation or deploy via EMM or stage Now and set permissions that may not be exposed via the OS UI.

## Version scheme

As a part of continual development and maintenance, it is highly recommended scheduled installation updates are planned for. Currently AMS releases major updates on a quarterly basis.

The versioning scheme for ZAMS software documentation is as follows:

**<yy>.<pi>.<rel#> <suffixes> where**

- **<yy>** is the 2-digit year of release
- **<pi>** is the major product increment number of the release. Typically, there are 4 major incremental releases to correspond to 4 quarterly scheduled releases.
- **<rel#>** is the incremental release number since last product increment. This number is updated to note a change to collection of release elements.
- **<suffixes>** are optional text characters used to denote a branched set of changes from a baseline release. It is typically used to denote hot fixes or custom changes of a release

## Target Environments

ZAMS supports the following target environments

- All Zebra GMS and Non-GMS Android M devices and later
- Non-Zebra Android devices support for Android M and later but does not include Zebra Value Add (ZVA) compatibility such as MX, DataWedge, StageNow, etc. This generally means the following may not be supported if the desired ZVA equivalent feature is not specifically integrated into the ZAMS application on a case-by-case basis.
  - Vendor specific scanning or API support
  - OEM specific OS restrictions (e.g., serial number and permissions setting access)
- Exceptions
  - Mobile devices with external power packs. Support on a case-by-case basis.

## Kiosk

- CC6000 (Android O+)
- ET40 (Android 11+)

## Portal UI

- Chrome desktop version 9 or later

# 1 Change Highlights (Release Sprint-22.4.1)

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

## Updates in this release

- Auto Install document
- AMS Server (v3.2.0)
- Kiosk AMS (Core v1.4.1 and UI v1.3.0)
- Device AMS (v2.4.0)

## 1.1 ZAMS Server (v3.2.0)

The following changes have been made to the ZAMS server

### 1.1.1 New Features

Below are the new features introduced in this version.

## Support for Mobile device with 1D liner barcode scanners

ZAMS support 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 msword
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.

Please see the below image for reference.



PI2240 Cabinet

[Download](#)

## 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.

## 1.1.2 Bug Fixes

- i. **ZAMS Portal not allowing to create a user with password that start with numbers**  
Now Company Admin will be able to create user with passwords starting with numbers.
- ii. **ZAMS Portal “View Stats” not clickable when browser width is reduced.**

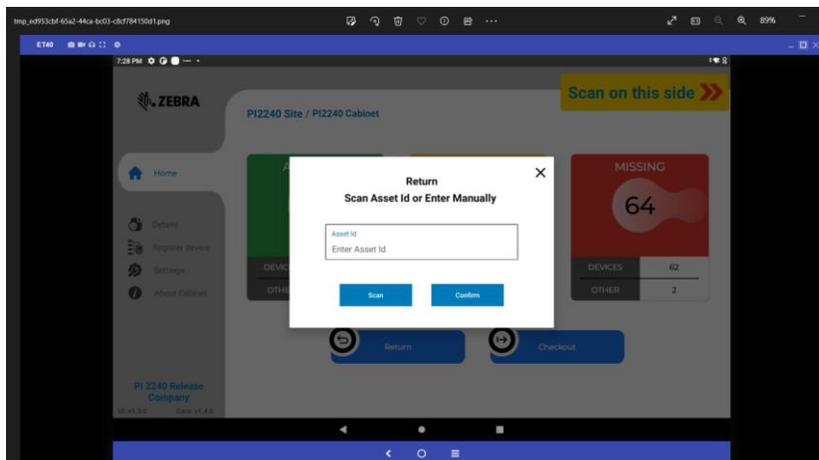
## 1.2 Cabinet Kiosk AMS (Core v1.4.1 and UI v1.3.0)

The following changes have been made to the Kiosk

### 1.2.1 New Features:

#### Support for ET40 tablets.

- ZAMS support Zebra “ET40” tablets to run Kiosk AMS apks.
- On ET40, AMS enables screen saver on AMS UI home screen when no activity for 15 mins.
- Short press on power button, will turn off the display momentarily and AMS home page re-appears on the screen. A message “ZAMS has disabled button pressed” will be displayed
- On selecting check-in/check-out of NMC devices, AMS UI provides a direction (Scan on this side) on from which side of ET40 Kiosk does user should scan the barcode. Please refer to the following image for reference



## 1.2.2 Bug Fixes

### i. User unable to login to a device handed over outside of cradle - Switch Device

This issue occurs whenever “one device user” option enabled, and user want to handover device to another user outside of cradle.

This issue is fixed to enable user to handover devices, when ‘one device user’ is enabled, without need to return the device to cradle before switching.

#### How it works?

- One Device User is enabled at company configuration in portal.
- User1 logs into Device1.
- User1 wants to handover the device 1 to User2.
- Now Device 1 allows User2 to login.
- Now User1 can login to any other device (User1 must give 1 min gap before taking any other device)

### ii. PIN entry issue

There are some instances where user unable to take devices out of cradle after entering pin or via barcode scan.

This issue has been fixed.

### iii. Kiosk Unable to Communicate with Server/Red Banner issue/Unable to communicate with server

This issue might occur when ever Kiosk unable to handle error/exception conditions properly. If more such exceptions occur, Kiosk mark itself that server is not reachable and shows the banner.

This issue has been fixed by handling exceptions appropriately.

**Now Kiosk shows this banner only if it is unable to communicate with server due to network issues.**

- iv. **When Devices are marked as lost in the portal it blocks the last user from taking another device.**

This issue occurs when 'one device user' is enabled. This has been fixed so that, user associated with devices marked as lost can now be able to login to another device.

- v. **Mobile Devices are throwing users back to the ZAMS login screen during device use**

Once user enters pin and Device Ams Device app automatically gets closed, it is expected not to click on Device Ams app, unless user wants to swap the device with another user.

If user clicks on Device Ams app after user gets logged in then pin screen starts popping up and it is expecting another user to log in, it will only stop, if any other user login happens.

This has been fixed by allowing same user to login again if PIN Screen pops up.

## **1.3 Device AMS (v2.4.0)**

### **1.3.1 New Features:**

#### **Support for Mobile device with 1D liner barcode scanners**

A new scanner capability has been added to MC33X Devices to register devices using 1D barcode scanners.

A new data wedge profile(dwprofile\_code128\_barcode\_profile.db) must be imported and setup to support the functionality of the scanner activity.

The required data wedge profile is shared along with the release (Device folder). The new file Should be pushed to the Mobile Device during installation process.

### **1.3.2 Bug fixes**

- i. **Users unable to upgrade devices from 5.3.56 to 5.3.57 version.**

Build number has been updated for device. User with 5.3.56 can directly upgrade their device to 5.4.0.

## 2 Known Constraints and Workarounds

1. BT proximity range could be seen as inconsistent due to several factors including device limitations, BLE poll rates and RF environmental influences. Devices need to be placed within environment specific acceptable ranges to obtain consistency. It is recommended to verify proximity consistency during installation.
2. A new security certificate was released at the end of June. This resulted in a mandatory update of all ZAMS installs to v22.1 or later. Any legacy DW profiles also need to be updated. Otherwise some scanning functions will not work.
3. It is recommended that setting “ App Login on Reboot” should be turned off while using Imprivata APP.
4. It is recommended to turn off BLE proximity Imprivata while using Imprivata.
5. A Random behavior has been reported in Android 8 (Oreo) devices that Sometimes A 8 device takes long time to connect to the wifi and toast (wifi not connected) appears.
6. Bug – Scheduled Email Configuration – After the daylight saving time came into effect There was one-hour time difference delay in the delivery of the email reported by Zebra. The work-around to resolve this issue at present is just to change the scheduled time of the Configuration by signing into the ZAMS Portal if the delivery of the Scheduled Email has been disturbed.
7. After a factory reset on the CC6000, the offline cabinet files may fail to be processed the first time if placed on the device by Stage Now. It may begin working with
  - a Retry
  - b Retry of the profile after uninstalling the applications or relaunching them the apps after clearing from the Recent apps.
8. ZAMS SSO intent known issues:
  - a Login status may not update on portal when Special character is used in the user name field while logging in.
  - b When device is AVAILABLE, if a user log in intent is sent, the AVAILABLE status is lost and may not be recoverable. The intent must only be sent when the device is outside of the charger.
  - c When using the intent, the ZAMS client should be configured (via the portal) so PIN UI is not shown. In this case, if “send alarm” is sent via the port UI, there is not UI prompt so the device will alarm until the unit is placed back into the cradle.
9. One user login Bug with Other asset (Login with user 1 on multiple Other Asset , Login on device 1 with user 1 , now put device 1 on charge , login on device 2 with user 1 now it shows up user is already logged in )
10. Username disappearing when new Other Asset is checkout (Random Bug)

11. Based on quality of network performance and/or wifi coverage. Server updates from the kiosk may take up to a few minutes.
12. Stagenow profiles in the installation admin sub-folder doesn't contain latest APK. APK files in each profile need to be updated by the Stagenow administrator prior to use.
13. Device status not syncing properly between Portal and Kiosk. Fix for this issue is in progress. However, this sync issue will get corrected by itself after few minutes.

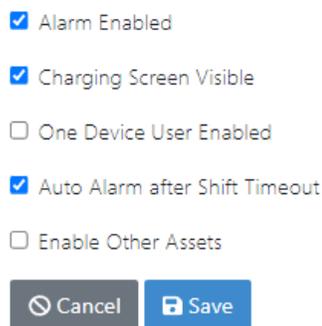
## 3 Appendix

### 3.1 Non-Android

#### 3.1.1 ZAMS Server

##### *i. Dashboard*

Non Android Assets will be referred to as (OTHER) on the Dashboard whereas Mobile computers are referred to as (Devices) on the overview. There is a configuration setting added at the Company level : Administration<Company: "Enable Other Assets"

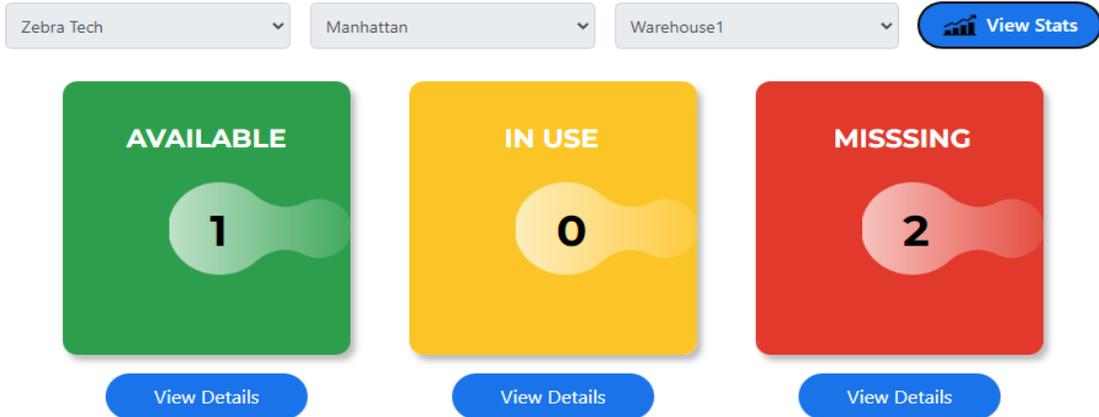


A screenshot of a configuration interface showing several settings with checkboxes. The settings are: 'Alarm Enabled' (checked), 'Charging Screen Visible' (checked), 'One Device User Enabled' (unchecked), 'Auto Alarm after Shift Timeout' (checked), and 'Enable Other Assets' (unchecked). At the bottom, there are two buttons: 'Cancel' and 'Save'.

When "Enable Other Assets" is unchecked, only Devices registered with that company will be displayed on Dashboard, as following.

## Dashboard

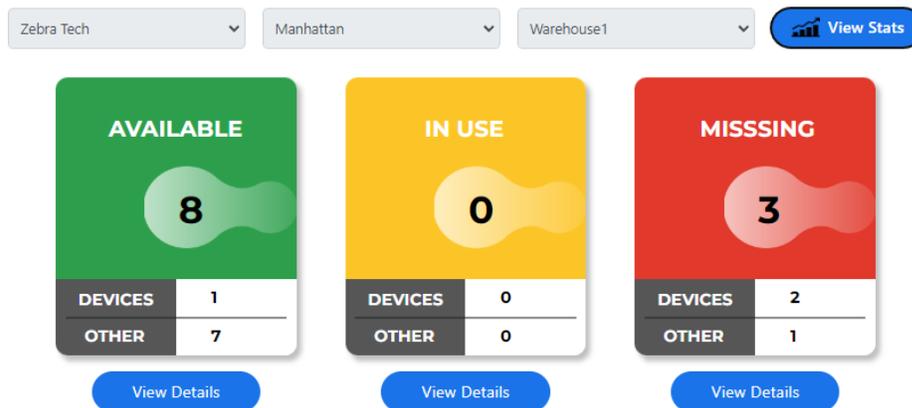
Choose from the list below to see details:



When “Enable Other Assets” is Checked, Devices & Other Assets registered with that company will be displayed on Dashboard, as following.

## Dashboard

Choose from the list below to see details:



These are changes to the Dashboard view:

- ON\_Charge (the Green Box) Status has been replaced and will appear as AVAILABLE.
- When “Enable Other Assets” is unchecked, only Devices registered with that company will be displayed on Dashboard.

- When “Enable Other Assets” is Checked, Devices & Other Assets registered with that company will be displayed on Dashboard. The big number in the middle will be the sum of statuses of Mobile and Non Mobile devices.
- The view details Button for each respective Status i.e, Available, IN USE & Missing displays the list of Devices and Other Assets based the configuration set from the Company settings whether to show Other Asset in addition to Devices or Just to display Devices.

## *ii. Mark an Asset to RMA or Lost*

An Other Asset can be Marked RMA or Lost using two methods.

1. Dashboard
2. From Other Asset Page.

### **Dashboard: Marking an Asset as Lost or RMA**

1. From the IN\_Use state: Click View Details<Under Mark Device < Click Mark Lost OR RMA.
2. From the Missing state: Click View Details<Under Mark Device < Click Mark Lost OR RMA.

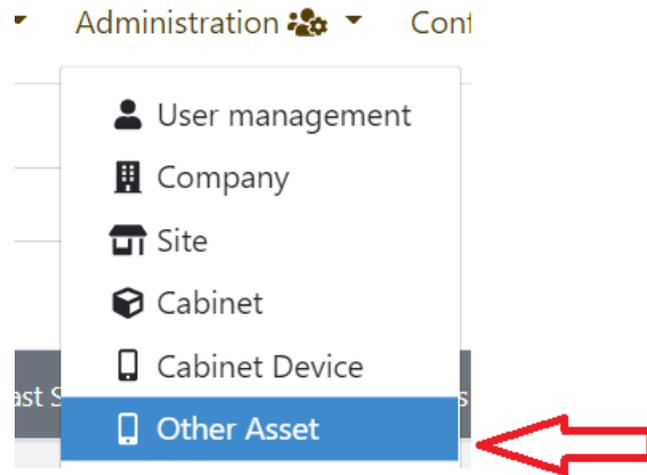
### **From Other Asset Page**

- Go to Administration <“ Other Asset ”
- Click Edit for the Desired Other Asset
- Click RMA or Lost

## *iii. Register a new Other Asset*

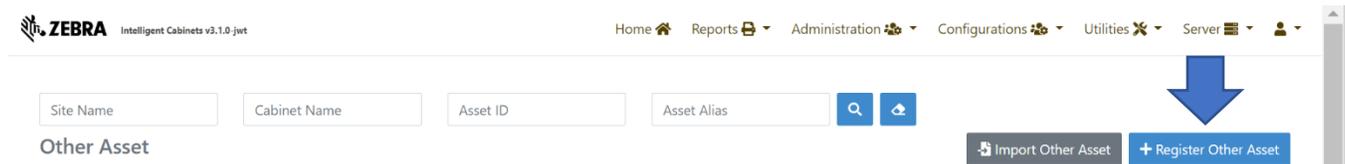
Go to the new tab created under Administration Menu.

Administration à“ Other Asset ”



All the Non Android ( Other Asset) will be displayed here and also Other Assets can be Registered here.

To Register a new Other Asset, Click on “Register Other Asset”



Fill the required information. The fields Marked as red. Only optional Field on this form is “Alias”

The Required fields are

1. Company (It will be prepopulated)
2. Site (Select a site from drop down list)
3. Cabinet/Kiosk (Select one from drop down list)
4. Asset ID
  - i. Asset ID must be unique across the Zams Portal
  - ii. Asset ID must contain minimum eight characters & maximum of 30 characters.
  - iii. Space bar (  ) is not allowed as valid character in the Asset Id fields.
  - iv. The Asset can contain special characters. Special characters are allowed keeping in view that some barcode contains special characters like [ - . \_ ]

## Register or edit Other Asset

Company

Site

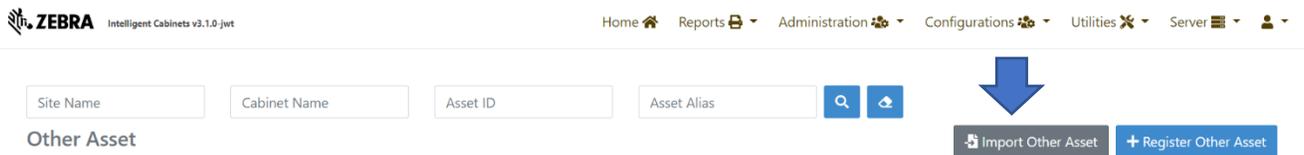
Cabinet

Asset ID

Alias

### iv. Bulk Import Other Asset

To Import OtherAssets Via CSV in Bulk click on “Import Other Asset”



The screenshot shows the top navigation bar with the ZEBRA logo and version 'Intelligent Cabinets v3.1.0-jwt'. The navigation menu includes Home, Reports, Administration, Configurations, Utilities, and Server. Below the navigation bar, there are four search input fields: 'Site Name', 'Cabinet Name', 'Asset ID', and 'Asset Alias'. To the right of these fields are search and refresh icons. Below the search fields, there are two buttons: 'Import Other Asset' and 'Register Other Asset'. A blue arrow points to the 'Import Other Asset' button.

## 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 Alias.

**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

Import

Input file has header - Please ignore first line

[< Go Back](#)

Sample Template is provided to guide the users and required information is mentioned on this page.

### v. *Other Asset Management after Registration*

Once an Other Asset is registered from the Portal the new created Asset is updated in the Other Asset list and its status is automatically marked as ON-Charge (AVAILABLE State). An Admin with access to the Portal can perform the following after an asset is registered.

Go to Administration <“Other Asset”

All the Other Asset will be displayed depending on the Security Role. Company\_Admin have full Privileges; Site Admin has Privileges for the specific Site only whereas Company User has view only Privilege.

Select or search for a Other Asset to perform required actions.

Click on the view button.

81086	BT-1098-63	977/BT-1098-63	Battery	351	743	29-Sep-2022 22:14:35	ON_CHARGE	imprivta	 
-------	------------	----------------	---------	-----	-----	----------------------	-----------	----------	--

All the details will be listed for the particular Other Asset.

A QR code will be displayed as well along with the Human Readable text which is the Asset ID. This QR code can be downloaded if required it can be pasted on Assets that will enable the Kiosk to Return and Checkout Assets.

## Other Asset Cabinet Device 81086

**Device Name**

BT-1098-63

**Cab. Id/Serial**

977/BT-1098-63

**Alias**

Battery

**Created On**

29-Sep-2022 22:14:35

**Last Status Update**

29-Sep-2022 22:14:35

**Status**

ON\_CHARGE

**Cabinet**

imprivta

**BT-1098-63**[Download As PNG](#)[← Back](#) [✎ Edit](#)

### vi. *Edit Asset Attribute and Mark Lost/RMA*

By clicking the Edit Button From the Action Column or from the view option, detail relating to the Asset is listed.

- a. User can mark an asset Lost or RMA, If the Status of the device is IN\_USE or Missing.
- b. Once marked Lost or RMA, the asset will disappear from Dashboard and the Kiosk in couple of minutes.
- c. If asset is found at a later stage, then user can click on mark found. In case the device was marked RMA then user can click Recover from RMA/BER.
- d. Note: To bring an Other Asset back to ZAMS even if Marked Found, there are two ways:
  - i. User has to go the same Kiosk and click on “Return” Button on the Home screen and then either scan or enter the Asset Id. Once scanned successfully toast appear “Asset returned successfully” The Asset will move to AVAILABLE state.
  - ii. User can go to the same Kiosk and click on “Check Out ” button from the home screen and then either scan or enter the Asset Id. Once scanned successfully user will be prompted to enter the Device User pin code. If valid pin is entered toast will appear “Asset checked out successfully” The Asset will move to IN-Use state directly.
- e. The Other Asset can be registered to a new Kiosk by clicking on “Return” button on home screen after scanning the barcode or by entering the Asset ID a dialog box will open prompting the user to enter “Site Admin Pin to Register Asset” Once a valid Site Admin pin is enter associated to the same site the Asset will registered to the new Kiosk.

## Register or edit Other Asset

ID

81044

Company

imprivata

Site

imprivata site

Cabinet

imprivta

Asset ID

202245225EFG124

Alias

MyDevice2

 Mark Lost

 RMA

 Cancel

 Save

## vii. Reports

Reports can be generated by users having the Privileges to view and generate reports from the ZAMS Portal after logging in. A column “Asset Type” has been added to each of the following Reports:

- Missing Devices Report
- Lost Devices
- Found Devices
- RMA Devices
- BER Devices
- Repaired Devices
- Historical Reports

As shown below in the Missing Device Report under Asset Type Column Device & Other is listed to differentiate between the Asset Type.

## Missing Devices Report

Zebra Tech    Manhattan    Warehouse1    Show

List of Missing devices:								
#	Device Name/Asset ID	Calb. Id/Serial	Alias	Last Status Update	User Name	Status Reason	Last User	Asset Type
33416	21142523021692	919/21142523021692		23-Sep-2022 16:14:31		COMMUNICATION_LOST	jskjdskjgaskas	Device
33418	20323522503223	919/20323522503223		23-Sep-2022 17:04:42		COMMUNICATION_LOST	jskjdskjgaskas	Device
33427	gyjgygyufukgfytyktyf	919/gyjgygyufukgfytyktyf		23-Sep-2022 17:30:01	jskjdskjgaskas	NOT_RETURNED	jskjdskjgaskas	Other

### 3.1.2 KIOSK and UI

#### i. Data wedge Profile for Kiosk

New scanner capability added to Kiosk to register non-android devices using Kiosk scanner. Kiosk scanner can be used to scan the barcode of the non-android devices and can register the device.

A New Datawedge profile must be imported and setup to support the functionality of the scanner activity for the Kiosk.

The required datawedge profile is shared along with the release. The new file Should be pushed to the Kiosk during installation process.

- Open Data wedge from the Kiosk
- Click settings
- Select Import datawedge profile.

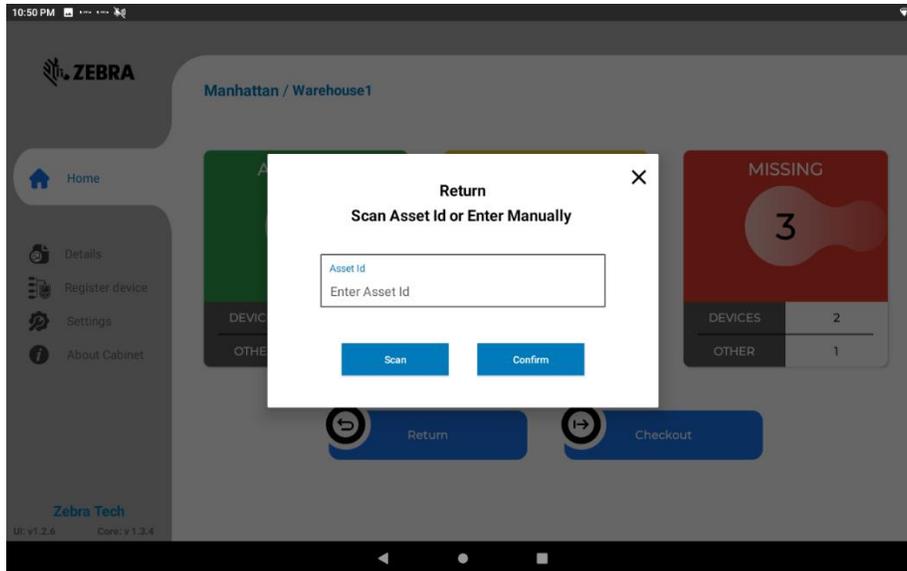
#### ii. Register/Return Other Asset

Users can press the "Return" Button on the Kiosk Home page to do the following:

1. Register a new Asset if it's not registered to the Kiosk. Only Site Admin for that specific site has the authority to register an Other Asset.
2. Return an Other Asset already registered to the Kiosk
3. Move an Other Asset Back to ZAMS if it had been previously marked RMA/Lost

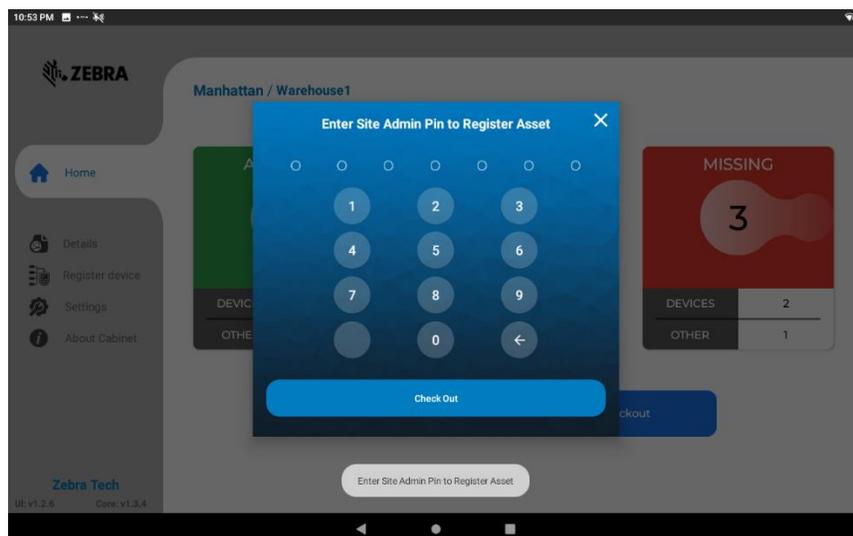
### iii. Register a New Other Asset by clicking Return Button

User has to click on Return Button on the Kiosk and a new dialog box will open.



A dialog box saying “Scan Asset Id or Enter Manually” will open. At this point the scanner of the Kiosk will activate automatically for a fixed interval. The User can scan the barcode of the Asset or Enter the asset ID manually.

1. If the barcode of the Asset is scanned successfully a toast message will appear and a new dialog box will open asking for site Admin pin. The pin code can be either entered on the onscreen keypad followed by pressing checkout button or a User badge can be scanned instead of entering while the scanner of the Kiosk is active. The Site Admin must be associated to the same site of the Company. There must be at least one site Admin setup and associated to the site if registration from the Kiosk is required to use this feature of registration of Asset from the Kiosk.

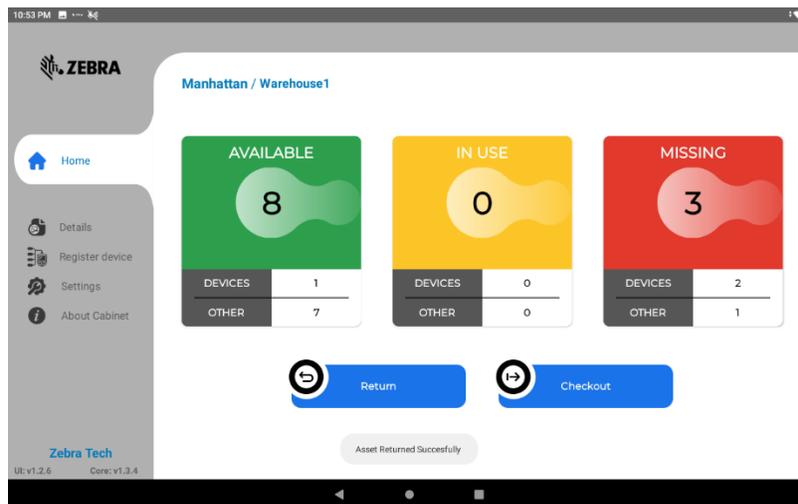


Once a valid Side Admin Pin is entered, click “Checkout”

Once the Site Admin Pin is validated successfully, the confirmation toast “Asset Registered Successfully”

The Asset will be registered and the newly registered asset will be move to AVAILABLE state on the Kiosk and Portal.

If a valid Site Admin pin code is entered or scanned then toast will appear “Asset Registered Successfully”. The Site Admin must be associated to the same site of the Company. There must be at least one site Admin setup and associated to the



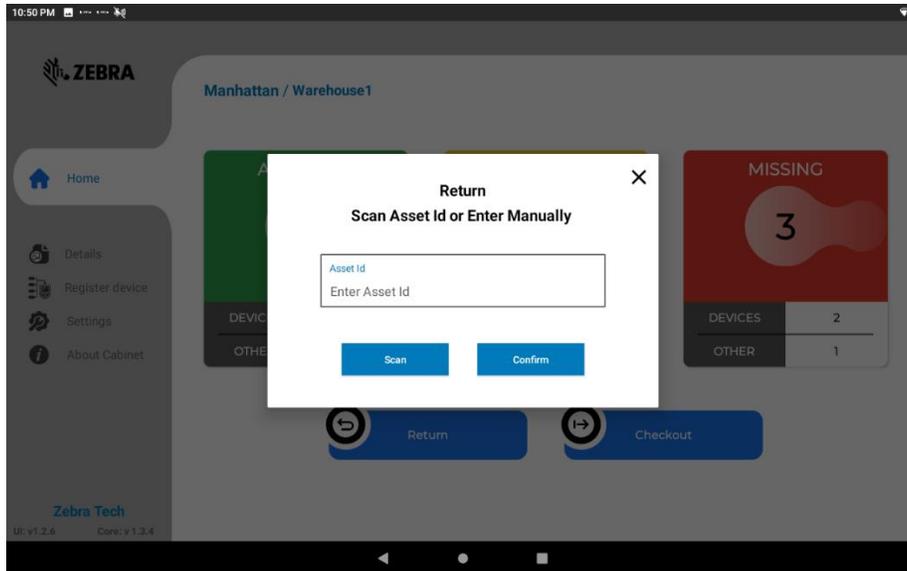
2. If the Asset ID is entered manually, the user has to press confirm to go to the next step. The Asset Id should have the following attributes:
  - a. Asset ID must be unique across the Zams Portal.
  - b. Asset ID must contain minimum eight characters & maximum of 30 characters.
  - c. Space bar  is not allowed as valid character in the Asset Id fields.
  - d. The Asset can contain special characters. Special characters are allowed keeping in view that some barcode contains special characters like [ - . \_ ]

After pressing the confirm button a toast message will appear and a new dialog box will open asking to the Site Admin pin. The pin code can be either entered on the onscreen keypad followed by pressing checkout button or a User badge can be scanned instead of entering while the scanner of the Kiosk is active.

- a) If a valid Site Admin pin code is entered or scanned then toast will appear “Asset Registered Successfully”. The Site Admin must be associated to the same site of the Company. There must be at least one site Admin setup and associated to the site if registration from the Kiosk is required to use this feature of registration of Asset from the Kiosk.
- b) If an Invalid Site Admin pin is entered on this screen or the pin entered does not belong to a site Admin from the same site then an error the pin screen will be minimized and toast message will be displayed. “User is Not Site Admin”

#### iv. *Return an Asset already registered to the Kiosk*

When a user clicks on Return Button on the Kiosk a new dialog box opens



A dialog box saying “Scan Asset Id or Enter Manually” will open. At this point the scanner of the Kiosk will activate automatically for a fixed interval. The User can scan the barcode of the Asset or Enter Asset Id manually and click Confirm.

- i. If the Asset is already registered with the Kiosk a confirmation toast will appear “Asset Returned Successfully” and the Asset will move to AVAILABLE state. In case the asset is not registered a dialog box will open directing user to Enter Site Admin Pin to Register Asset.

#### v. *Move an Other Asset marked RMA/Lost Back to ZAMS*

An Asset Previously marked RMA/Lost can be returned to ZAMS by following these steps.

- i. User has to go the same Kiosk and click on “Return” Button and then either scan or enter the Asset Id. Once Asset Id scanned/entered successfully a toast will appear “Asset Returned Successfully” The Asset will move to AVAILABLE state.
- ii. User can go to the same Kiosk and click on “CheckOut” and then either scan or enter the Asset Id. Once Asset Id scanned/entered successfully user will be prompted to enter a valid pin code. Once pin code is validated a toast will appear “Asset checked out successfully” The Asset will move to IN-Use state directly.
- iii. The Asset can be registered to a new Kiosk by clicking on “Return” Button after scanning the barcode or by entering the Asset ID the Asset will registered to the new Kiosk after entering the Site\_Admin’s Pin. In the ZAMS db a new Cabinet Device/Asset ID will be allocated to the asset with new Serial No ( Cabinet Id/Serial)

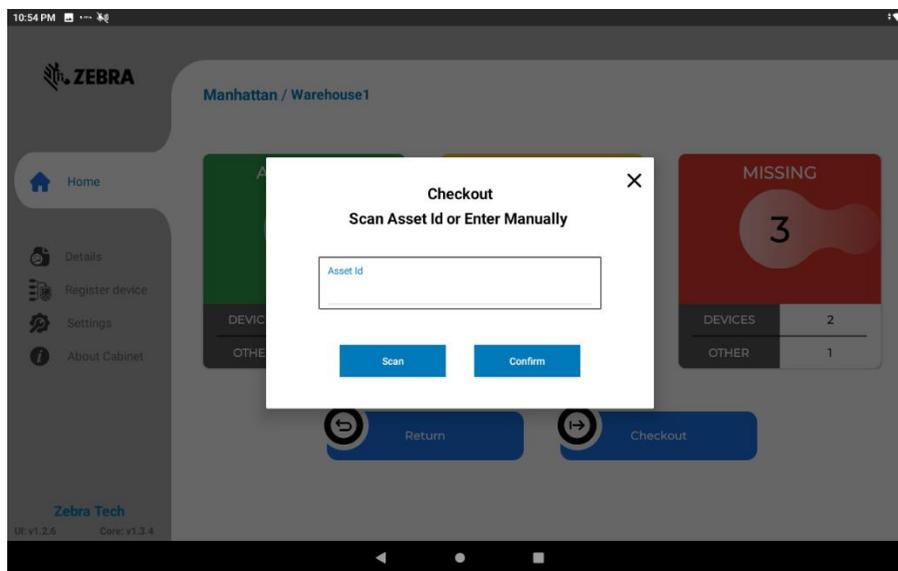
## vi. Checkout Other Asset

Users can press the Checkout Asset Button on the Kiosk Home page to do the following:

1. Checkout an Asset already registered to the Kiosk
2. Register a new Asset if it's not registered to the Kiosk. Only Site Admin has the authority to register an a new asset.
3. Move an Asset Back to ZAMS if it had been previously marked RMA/Lost

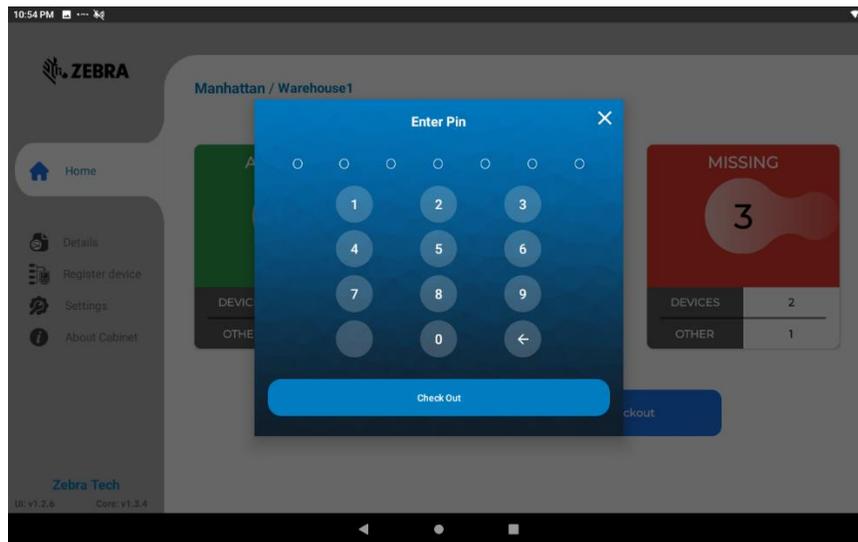
## vii. Checkout an Asset already registered to the Kiosk

User has to Click on "Return" Button on the Kiosk a new dialog box will open



A dialog box saying "Scan Asset Id or Enter Manually" will open. At this point the scanner of the Kiosk will activate automatically for a fixed interval. The User can scan the barcode of the Asset or Enter it manually.

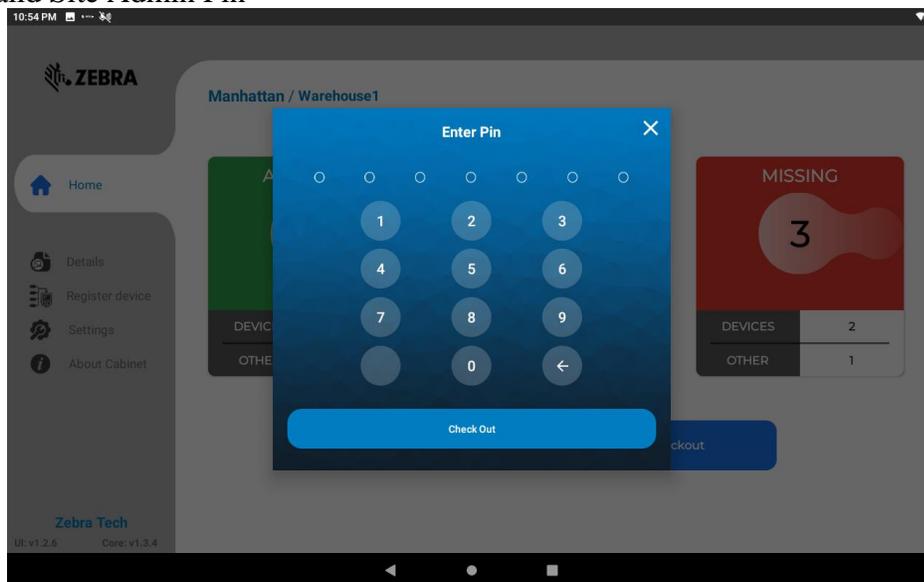
1. If an Asset barcode is scanned successfully and the Asset is registered to the Kiosk and its state is AVAILABLE the user is prompted to enter a valid pin for a Device User associated to the same site or with Global attribute to check out Asset button or a User badge can be scanned instead of entering while the scanner of the Kiosk is active.
2. Likewise, if an Assis Id is entered click Confirm, after validating that Asset is registered to the Kiosk and its state is AVAILABLE the user is prompted to enter a valid pin for a Device User associated to the same site or with Global attribute to check out Asset.



3. If a valid pin code is entered or Badge Id scanned via Kiosk scanner & the Device user belongs to the same site or the Device User is Global then the confirmation toast will appear “Asset Checked Out Successfully”

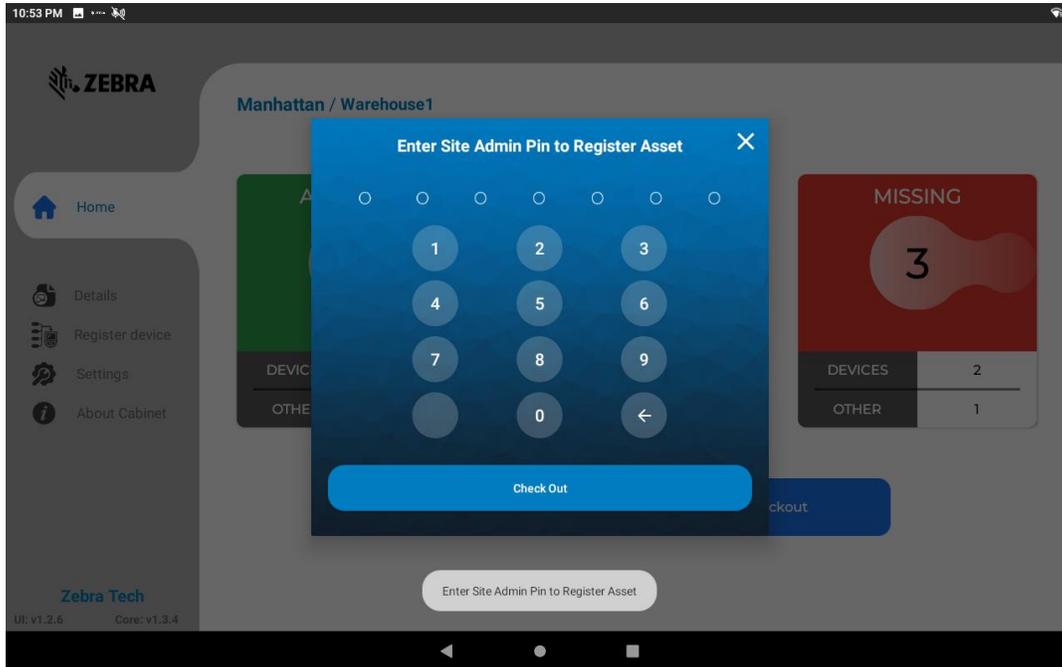
**viii. Register a new Asset at Checkout**

1. Click “Checkout” Button on Kiosk
2. A dialog box will appear. Enter a New Asset ID click confirm or Scan the barcode of the new Asset.
3. New Dialog box will open “Enter Pin”
4. Enter a valid Site Admin Pin



5. If a Device user pin is entered toast will appear “User is not Site Admin”

- Next dialog box will open prompting user to confirm Site-Admin pin.



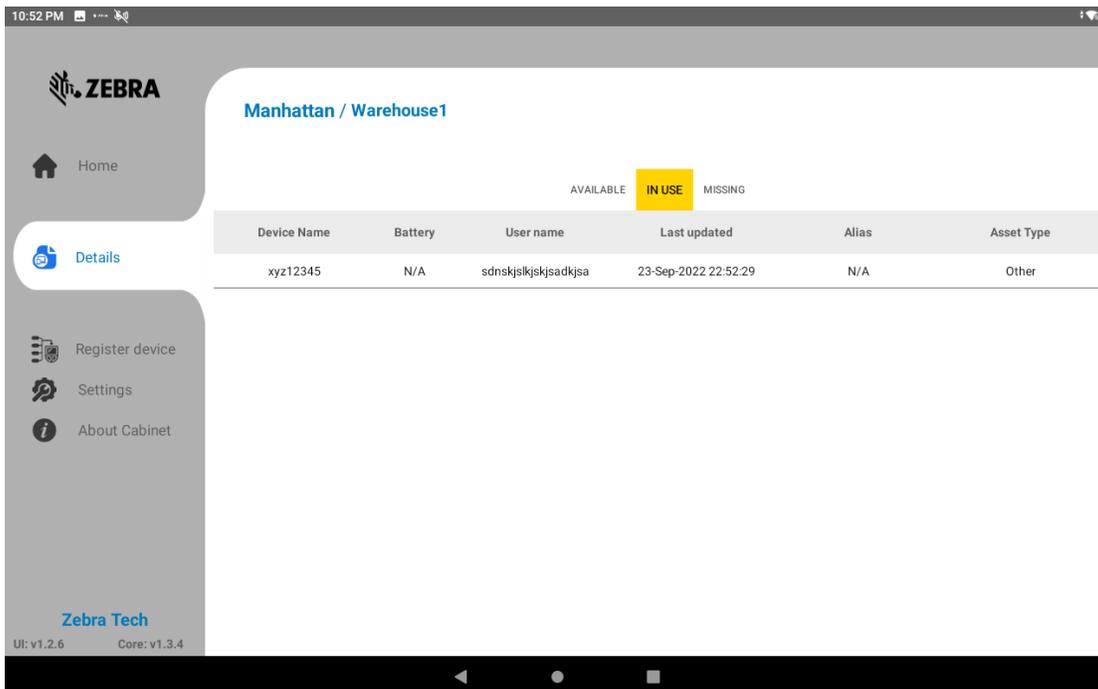
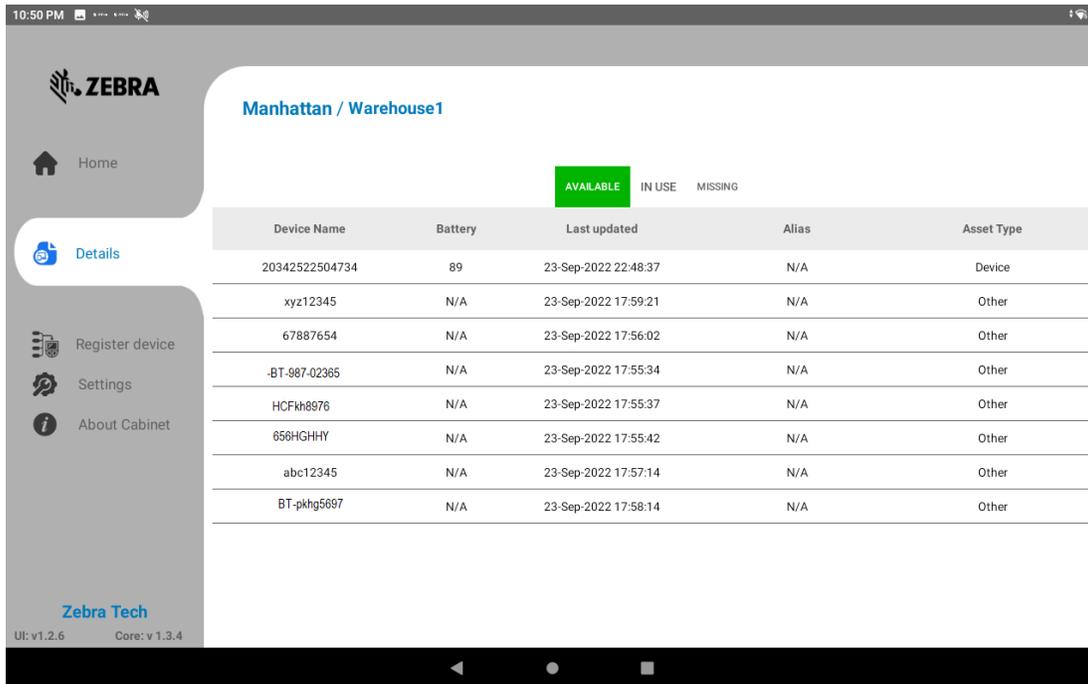
- If a valid Site Admin pin code is entered or scanned then toast will appear “Asset Checked out Successfully”. The Site Admin must be associated to the same site of the Company. There must be at least one site Admin setup and associated to the site if registration from the Kiosk is required to use this feature of registration of Asset from the Kiosk.
- The newly created Asset will be register to the ZAMS db, its status will update on the Kiosk as IN-Use and will be updated to the Portal as well.
- If an Invalid pin (not a Site Admin) is entered on this screen or the pin entered does not belong to a site Admin from the same site then an error the pin screen will be minimized and toast message will be displayed. “User is Not Site Admin”

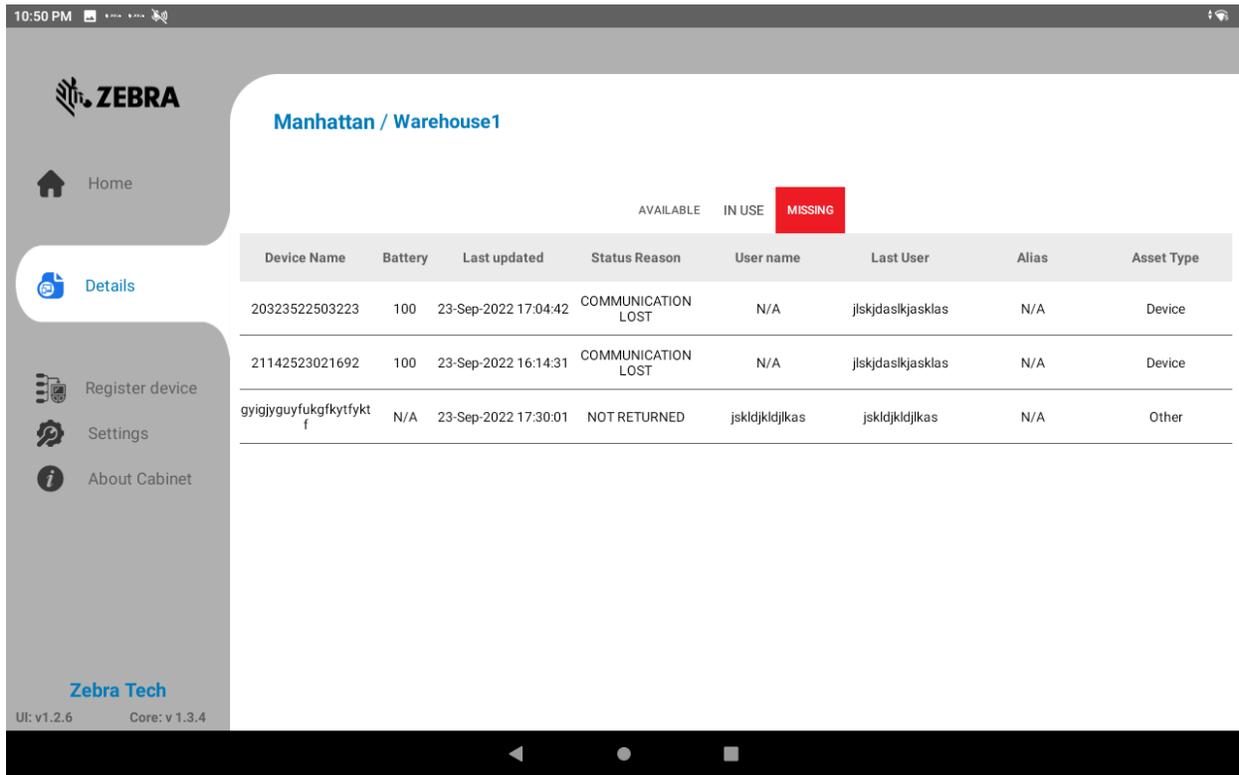
Notes:-

- Previously marked RMA/Lost Other Asset can be returned to ZAMS using Checkout Button—see Section No. 1.3.6 for details. The steps has to be followed in the similar manner.
- A Device User or Site Admin can checkout out multiple assets.
- When  One Device User Enabled – from the Company settings. A Device User can check out Only one Mobile (MC) but the same user can checkout multiple Other Assets.

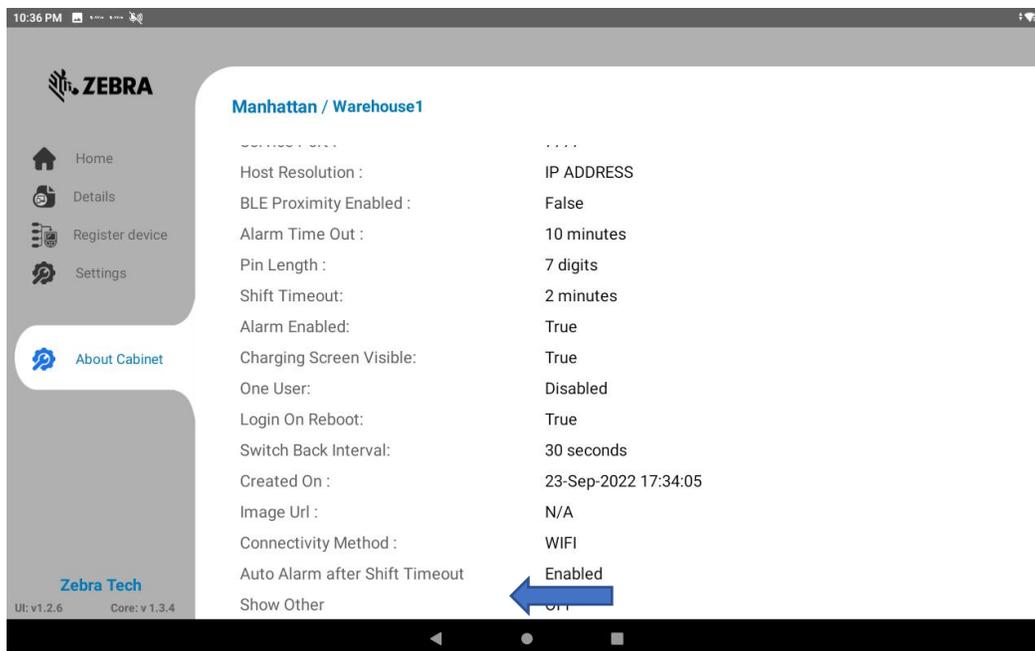
### ix. Details Tab

On the left side Menu, Details Tab list both Devices and Other Assets for the three States: AVAILABLE, IN USE, MISSING.





x. *About Tab*



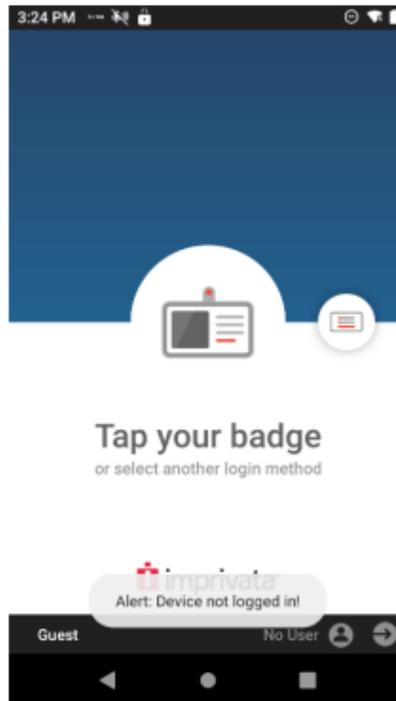
### 3.1.3 Imprivata and ZAMS reference information

The following are some key notes on the ZAMS and Imprivata feature integration requirements

**MDM Note:**

1. MDM will be managing the Kiosk and devices.
2. If Zebra EHS (Enterprise Home Screen) or MDM Launcher is used, it must be configured to allow both the ZAMS app and the Imprivata app to pop up over the launcher as needed.

**ZAMS/Imprivata Workflow: Device In Cradle:**



1. ZAMS notifies Imprivata that user returned device to cradle.
2. Imprivata logs off user, then notifies ZAMS when logoff complete.
3. ZAMS Kiosk and Portal show device "On Charge"
4. ZAMS charge screen/screensaver is shown on device.
5. If the ZAMS charge screen is dismissed (home button pressed for instance), it will pop back up after a set time, but this is not intended to lock the device down.

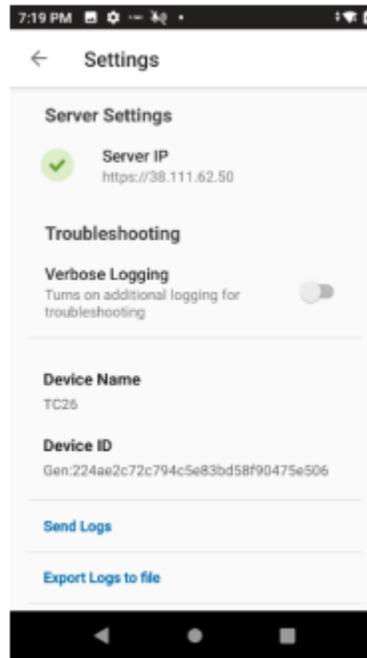
MDM Launcher or Zebra EHS can be used to block unauthorized access to the device.

If ZAMS lock screen is minimized by pressing home button then the ZAMS lock screen should reengage (pop-up) automatically after a configurable time 30, 60, 90 or 120 seconds. The timing is configurable at site level.

#### **Device out of Cradle:**

1. ZAMS kiosk and portal shows device as "Missing"
2. Imprivata screen is shown. User must log in to get past Imprivata screen
3. If user does not login, ZAMS app on the device will sound alarm on device after a timer expires (ex 2 minutes).
4. A toast message "Alert Device not logged in!" will pop-up on the screen once device is taken out of the cradle.
5. If user has still not logged in within 5 minutes, device moves to "Missing/Invalid Login" in ZAMS kiosk and portal, and email will be sent by ZAMS if configured to do that.
6. Once user logs in to Imprivata:
  - a. ZAMS alarm on device will stop if it was sounding
  - b. ZAMS alarm timer on device will stop
  - c. ZAMS kiosk and portal will show device "In Use" by the user who was passed from the Imprivata app to the ZAMS app on the device.
  - d. ZAMS shift duration timer starts. (configurable duration)
  - e. If device does not come back at end of shift, device moves to "Missing/Not Returned" in ZAMS kiosk and portal (showing user who last logged in), email will be sent (if configured)
  - f. At end of shift, user puts device in cradle (see above "Device In Cradle" section)
7. Optionally, user can pass device that they are using to another user without returning to cabinet.
  - a. New user will log in to the Imprivata app
  - b. Imprivata notifies ZAMS that user has returned the device. Imprivata notifies ZAMS of the new user.
  - c. ZAMS kiosk and portal will show the device "In Use" associated to the new user and restart the shift duration timer.
  - d. If the new user login fails for some reason, ZAMS will continue to show the device associated to the previous user. Setting up Imprivata APP.

## Setting up Imprivata APP.



Server IP (shared by Imprivata) Must be entered in the Settings. To enter to the settings Menu tap on the Imprivata Home screen repeatedly until the Settings window opens.

## 4 Important Links

- [Zebra Techdocs](#) - Zebra community support
- [Developer Tools](#) - Zebra Developer support
- [Partner Portal](#) – Zebra Partner news and other support
- [Intelligent Cabinet Support and downloads](#) – Zebra support and downloads