Zebra Access Management System (ZAMS)

Cloud and Client

Troubleshooting Guide

ZEBRA

MN-004916-04EN Rev A

Copyright

2024/10/21

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

Contents

About This Guide

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

For the latest version of this guide, go to zebra.com/intelligent-cabinets.

ZAMS Overview

ZAMS application is a secure solution designed to help organizations reduce the number of missing or unaccounted mobile computers.

The elements of the ZAMS software consist of Mobile Device applications and services, the KIOSK application and services, and the Cloud resident console.

- Mobile Device application and services - provides the lock screen user interface (UI) and services for Android-based mobile devices.
- KIOSK application and services - provides on-site device management, user interface, and information to the Cloud-based console. The kiosk application is designed for the CC6000 device.
- Cloud resident console - the Web portal that provides various administration-level tasks and reports. The server access portal is at zams.zebra.com.

ZAMS Product Documentation

Documentation and software are available on the Intelligent Cabinets support page.

The following documents are available:

- Zebra Access Management System Installation Guide

  This guide explains the software installation, registration, and use of Zebra value-added tools (DataWedge and StageNow) essential for ZAMS setup and functionality. It also specifies the required files for EMM/MDM installation.

- Zebra Access Management System User Guide

  This guide explains the ZAMS product and key usage features. The features are accessible through the ZAMS portal and KIOSK user interface (UI). The UI is a reference to understand feature constraints and limitations.

- ZAMS Cabinet and Mobile Device Quick Reference Guide

  This poster guide provides a quick reference to the ZAMS and the Mobile Device application.

Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (for example, 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 visual indicators are used throughout the documentation set.

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.

CAUTION: If the precaution is not heeded, the user could receive a minor or moderate injury.

WARNING: If danger is not avoided, the user CAN be seriously injured or killed.

DANGER: If danger is not avoided, the user WILL be seriously injured or killed.

Service Information

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

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number

Zebra responds to calls by email, telephone, or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Limitations and Recommendations

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

NOTE: *Versions prior to 24.3.0 support 100 devices and 500 registered users per KIOSK.

- KIOSK and DEVICE must be on the same version, between the current major release (N) and no older than N-2.

Bluetooth Proximity

If the Company Admin turns on the optional Bluetooth proximity feature on the portal, Bluetooth Proximity is enabled automatically after the ZAMS device is successfully registered with the Cabinet.

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

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

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

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

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

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

When Bluetooth Proximity is enabled from the ZAMS portal, ensure that **Bluetooth** and **Location** are enabled on the Mobile device.

NOTE: The Bluetooth Proximity feature is functional on Android 13 for both the Device and the KIOSK.

Portal to KIOSK and KIOSK to Portal Sync

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

There are two configurable timers running on the KIOSK:

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

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

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

Tools and Applications

The ZAMS troubleshooting process can be implemented using several methods:

- Device Resident Browser (Chrome) - To verify network connections.
- RxLogger - To collect device and application logs for advanced analysis, triage, and fault isolation.
- Remote Screen Viewer - To capture screen views on Android devices, including the KIOSK.
- Network Tracing Tools - To collect network logs for advanced triage and fault isolation.
- User Interface Access to Network and Firewall Settings - Enables network and firewall settings access via the device's user interface. Their specific requirements are outlined in the Zebra Access Management System Installation and User Guide.

Verification of ZAMS Operational Functions

The verification process ensures that the ZAMS functions across its key components as intended.

Mobile Device

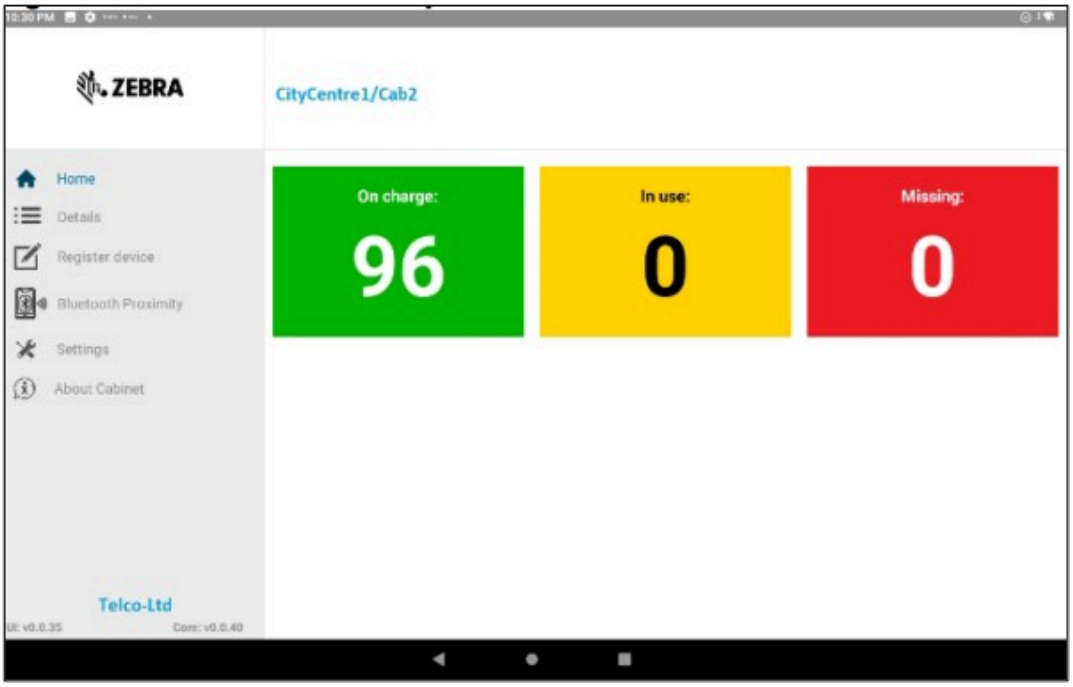
Verify the Mobile Device functions as described below.

1. When the device is charging, the charge screen is displayed.
2. After removing the device from the charger, a login screen with a countdown timer appears.
3. The alarm can be stopped by logging in or placing the device back in the charger.
4. Users can access the device by entering valid credentials. The ZAMS screen no longer appears.

KIOSK

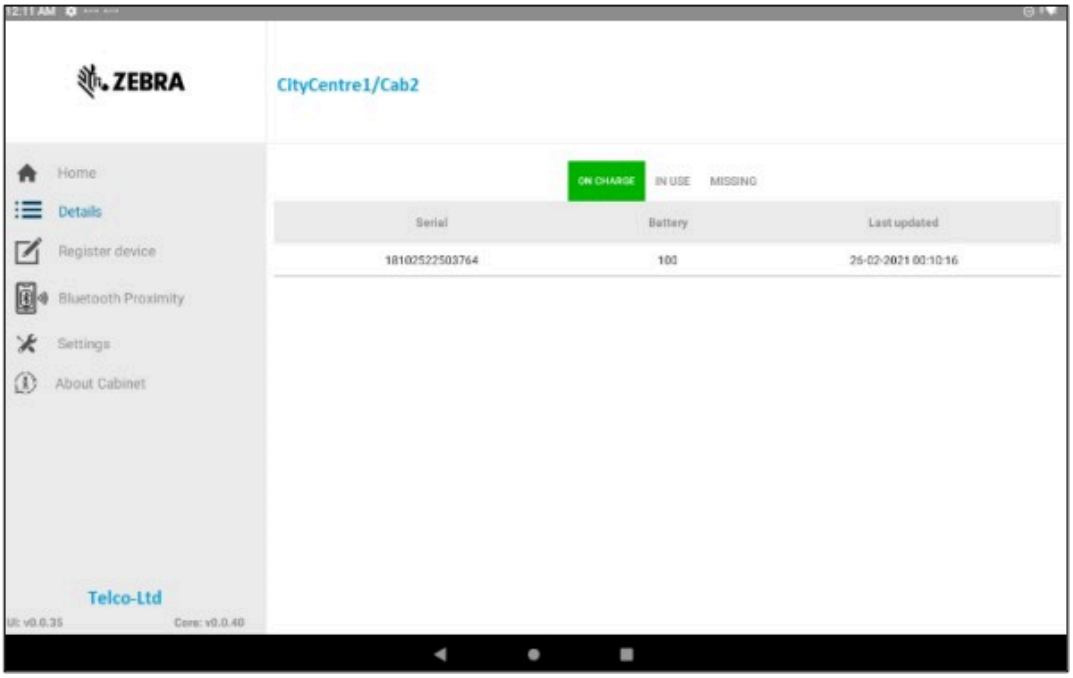
Verify the KIOSK functions as described below.

- The KIOSK dashboard must accurately display the total number of managed assets, such as mobile devices.



- Ensure that the dashboard updates summary counts based on device states:
  - Green/Charging for devices in the cradle.
  - Red/Missing for devices out of the cradle and not logged in.
  - Yellow/In-Use for devices out of the cradle and with a user logged in.

- The device ID on the state or color details must match their respective state. Ensure the KIOSK reports the device accurately when it is removed and logged in.



- Ensure the KIOSK has access to the Portal:
  - The dashboard Portal state must match the selected KIOSK state.
  - A browser launched from the KIOSK should display the Portal's homepage.

Portal

Verify the Portal as described below.

- User Functions:

NOTE: Only admin-type users can log into the Portal.

  - The Portal allows access only to the **Admin User**. ZAMS has several administrative user account roles (reflected in the user management UI page on the Portal). When a customer account is created, Zebra only establishes one admin account with the **Company Admin** role. The customer is responsible for using this account to create additional accounts that can log into the Portal.
  - Logged-in Admin Users can view and create new user accounts via the UI.
  - Logged-in Admin Users can import and export user accounts via the UI.
  - Logged-in Admin Users can view reports, exports, and schedules via the UI.
- KIOSK Connectivity Functions:
  - Ensure the KIOSK state matches the Portal state for the selected KIOSK.
  - If the KIOSK state changes, the Portal state should ideally reflect the changes within a few minutes but typically within seconds.

Common Errors

This section explains the common errors in the Mobile Device, Portal, KIOSK, or Wi-Fi.

KIOSK or Wi-Fi

The KIOSK or Wi-Fi is down, and the device alarms if it is removed.

Admin users can generate a ZAMS Master Unlock Code from the portal to disable the alarm without logging in.

A Wi-Fi connection is required for the ZAMS device to function correctly. Without Wi-Fi, the ZAMS PIN screen will not display for user login.

KIOSK Reports Message

The KIOSK reports not connecting messages.

- Verify that the network port settings are configured per the Zebra Access Management System Installation Guide.
- Ensure the network connection from the KIOSK is working by browsing the portal URL via Chrome browser on Android devices.

NOTE: In ZAMS, the Mobile Devices do not connect directly to the Portal. The Mobile Devices connect to the KIOSK using a custom port specified in the installation guide. The KIOSK connects to the Portal over HTTPS. Refer to the Zebra Access Management System Installation Guide for more details.

System Degradation

If the application displays incorrect counts or experiences out-of-memory issues, it may be due to an excessive number of users per Site or too many devices per KIOSK. The synchronization settings are too low for the current configuration.

Here is what you can do:

1. Clear the KIOSK data during peak usage. This may need to be done once or more times per day.
2. Upgrading to ET40.
3. Split users into smaller sites.
4. Split devices into multiple KIOSK.

5. Increase the settings for Portal to Kiosk User Sync and Kiosk to Portal Device Sync.

Clear Storage

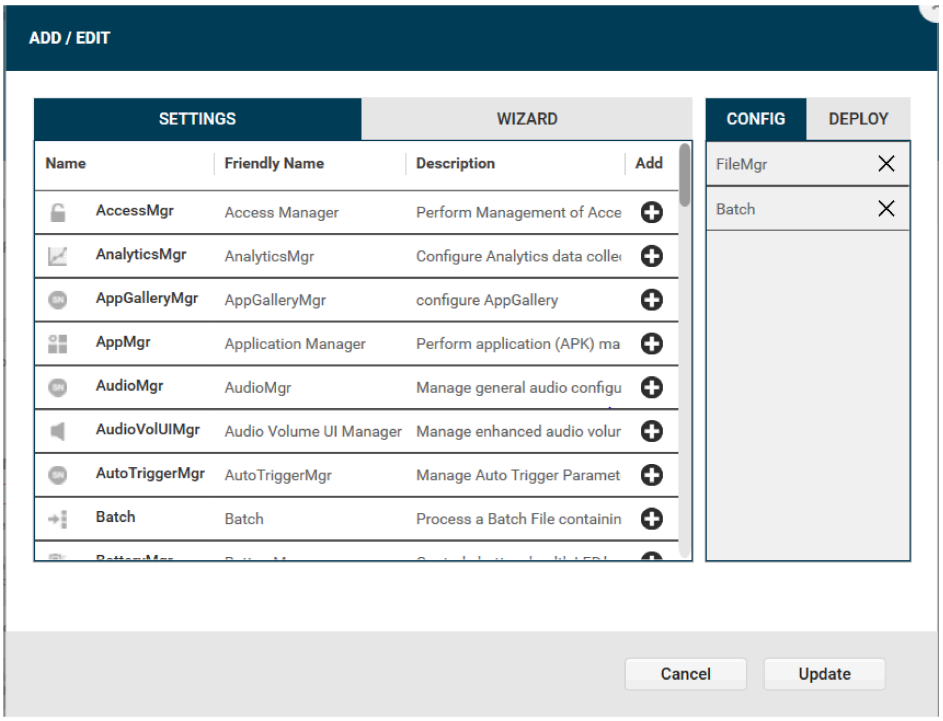
Run the clear storage scripts on the KIOSK when:

1. Before upgrading the APK from one version to another.
2. When a user is not able to log in to the device.
3. If the KIOSK app crashes or does not respond.
4. When devices lose connection with the KIOSK, even though both the device and KIOSK are connected to the same network.

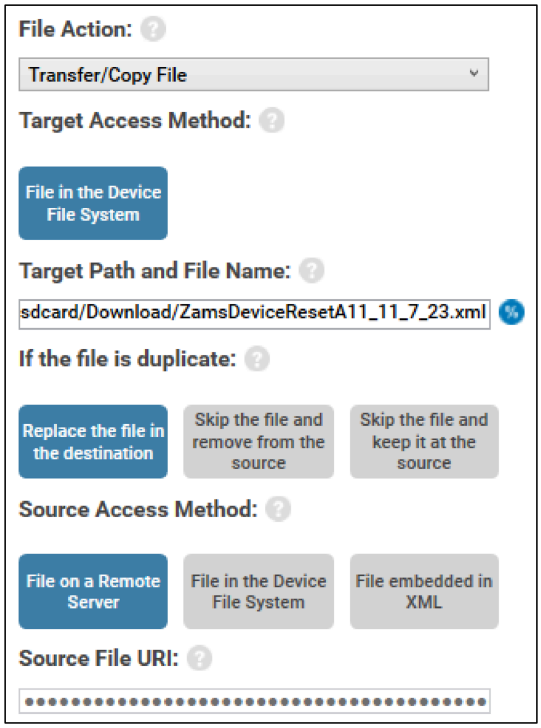
Device Reset

This section explains how to create a StageNow profile to clear **AMS device** storage data. Following these steps will reset the application, requiring a re-registration at the ZAMS KIOSK. If a `cabinet-device.config` file is used for the initial registration, the script will automatically rename it, ensuring the device re-registers to the KIOSK without any manual intervention.

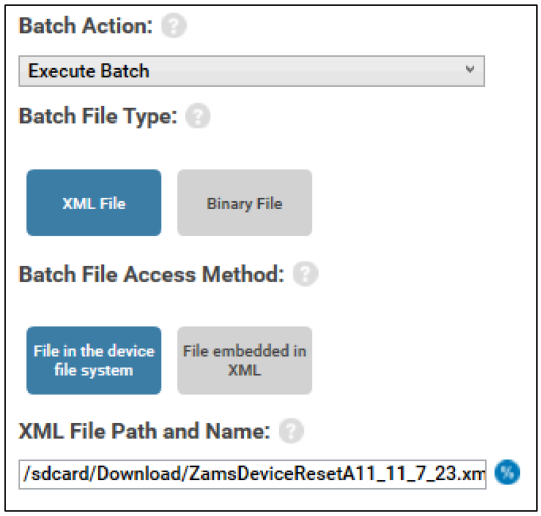
1. Open the StageNow application and create a new profile.
2. Select the appropriate MX version.
3. Select Xpert Mode.
4. Choose one File Manager and one Batch Operation from the available options.



5. Use File Mgr to transfer the `ZamsDeviceResetA11_11_7_23.xml` to device storage.



6. Use Batch Mgr to execute the script on the device.



7. Complete the profile and generate the StageNow barcode.
8. Scan the StageNow barcode to reset the data storage.
9. If you are not using the `cabinet-device.config` file, scan the registration QR code on the KIOSK.

Device Reset Configuration File

The following shows the device reset configuration settings. The configuration file is read each time the application starts.

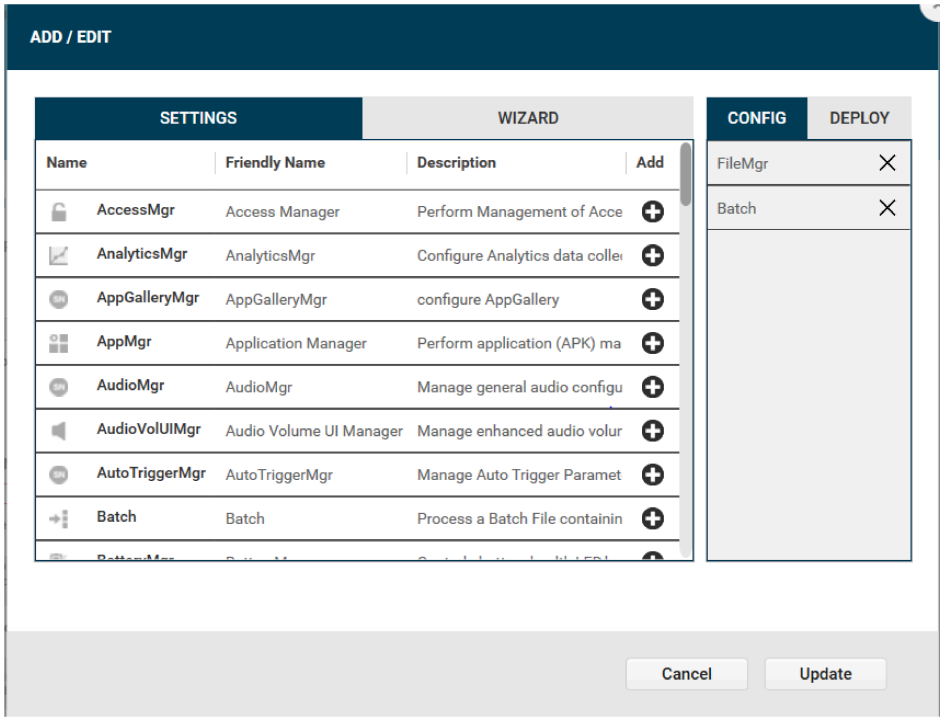
```
<wap-provisioningdoc>
 <characteristic version="8.3" type="FileMgr">
       <parm name="FileAction" value="1" />
       <characteristic type="file-details">
       <parm name="TargetAccessMethod" value="2" />
       <parm name="TargetPathAndFileName" value="/sdcard/Download/cabinet-
device.config" />
       <parm name="SourceAccessMethod" value="2" />
       <parm name="SourcePathAndFileName" value="/sdcard/Download/cabinet-
device-bak.config" />
       </characteristic>
 </characteristic>
 <characteristic version="9.3" type="AppMgr">
       <parm name="Action" value="ClearApplicationUserData" />
       <parm name="Package" value="com.zebra.ams.device" />
 </characteristic>
</wap-provisioningdoc>
```

KIOSK Reset

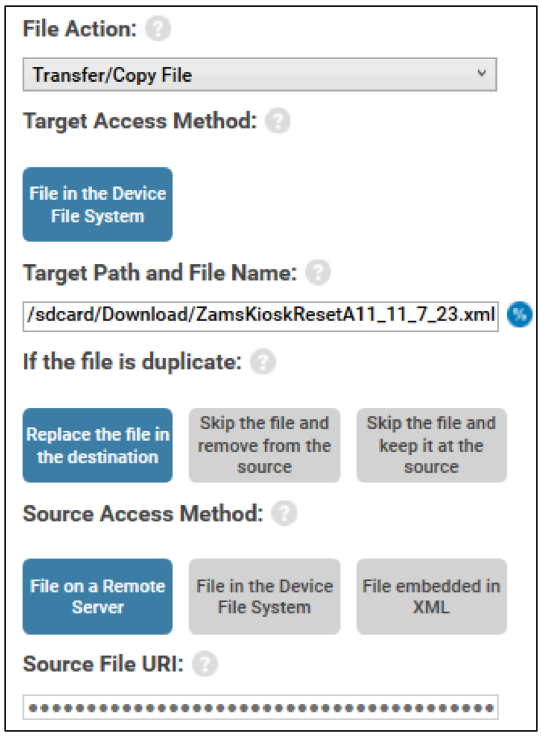
This section explains how to create a StageNow profile to clear **AMS core** and **AMS Ui** storage data. Following these steps will reset the application, requiring a re-registration at the ZAMS Portal. If a `cabinet.config` file is used for the initial registration, the script will automatically rename it, ensuring the KIOSK re-registers to the Portal without any manual intervention.

1. Open the StageNow application and create a new profile.
2. Select the appropriate MX version.
3. Select Xpert Mode.

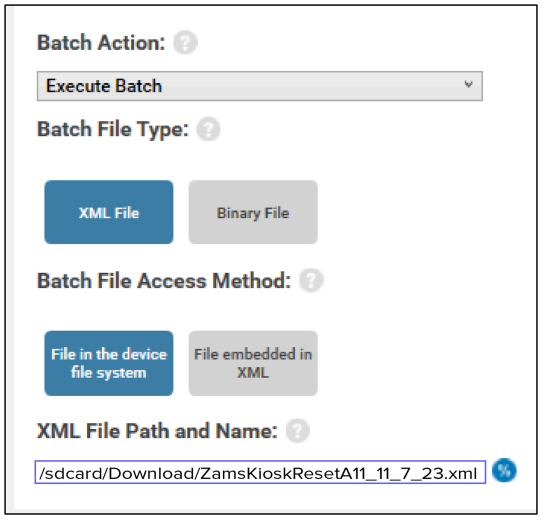
4. Choose one File Manager and one Batch Operation from the available options.



5. Use File Mgr to transfer the `ZamsKioskResetA11_11_7_23.xml` to device storage.



6. Use Batch Mgr to execute the script on the device.



7. Complete the profile and generate the StageNow barcode.
8. Scan the StageNow barcode to reset the data storage.
9. If you are not using the `cabinet.config` file, you need to manually sign in to the KIOSK and register in the Portal using the original cabinet name.

KIOSK Reset Configuration File

The following shows the KIOSK reset configuration settings. The configuration file is read each time the application starts.

```
<wap-provisioningdoc>
<characteristic version="8.3" type="FileMgr">
     <parm name="FileAction" value="1" />
     <characteristic type="file-details">
     <parm name="TargetAccessMethod" value="2" />
     <parm name="TargetPathAndFileName" value="/sdcard/Download/
cabinet.config" />
     <parm name="SourceAccessMethod" value="2" />
     <parm name="SourcePathAndFileName" value="/sdcard/Download/cabinet-
bak.config" />
     </characteristic>
</characteristic>
<characteristic version="9.3" type="AppMgr">
     <parm name="Action" value="ClearApplicationUserData" />
     <parm name="Package" value="com.zebra.ams.ui" />
</characteristic>
</wap-provisioningdoc>
```

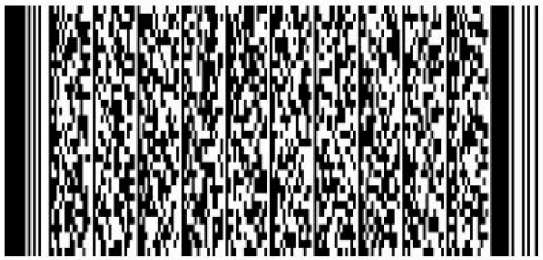
Device Registration Error

This section explains how to register Android 10 and 11 devices when facing permission issues.

- The error occurs due to permission issues when obtaining the build serial number or **MANAGE_EXTERNAL_STORAGE**.
- To resolve the issue, ensure to transfer the `AmsDeviceExecute.xml` file in the `/sdcard/Download/` directory on your device. Then, open the StageNow app and scan the V2 Barcode.

Scan Barcodes with StageNow Client:

1



Device Configuration File

The following shows the `AmsDeviceExecute.xml` configuration file settings. The `AmsDeviceExecute.xml` configuration file is read each time it is transferred to the `/sdcard/Download/` directory on the device.

```
<wap-provisioningdoc>
  <characteristic version="5.1" type="AppMgr">
    <parm name="Action" value="Install" />
    <parm name="APK" value="/sdcard/Download/AmsDevice.apk" />
  </characteristic>
  <characteristic version="5.0" type="FileMgr">
    <parm name="FileAction" value="1" />
    <characteristic type="file-details">
    <parm name="TargetAccessMethod" value="2" />
    <parm name="TargetPathAndFileName" value="/enterprise/device/settings/
datawedge/autoimport/dwprofile_amsPin.db" />
    <parm name="SourceAccessMethod" value="2" />
    <parm name="SourcePathAndFileName" value="/sdcard/Download/
dwprofile_amsPin.db" />
    </characteristic>
  </characteristic>
  <characteristic version="5.0" type="FileMgr">
    <parm name="FileAction" value="1" />
    <characteristic type="file-details">
    <parm name="TargetAccessMethod" value="2" />
    <parm name="TargetPathAndFileName" value="/enterprise/device/settings/
datawedge/autoimport/dwprofile_AmsDevice.db" />
    <parm name="SourceAccessMethod" value="2" />
```

```
    <parm name="SourcePathAndFileName" value="/sdcard/Download/
dwprofile_AmsDevice.db" />
    </characteristic>
  </characteristic>
  <characteristic version="6.0" type="DevAdmin">
    <characteristic type="AppAsDevAdmin">
    <parm name="DevAdminAction" value="1" />
    <characteristic type="DevAdminDetails">
    <parm name="DevAdminPkg" value="com.zebra.ams.device" />
    <parm name="DevAdminClass"
 value="com.zebra.backsafe.android.splash.BacksafeAdmin" />
    </characteristic>
    </characteristic>
  </characteristic>
  <characteristic version="4.3" type="Intent">
    <parm name="Action" value="StartActivity" />
    <parm name="ActionName" value="android.intent.action.MAIN" />
    <parm name="Package" value="com.zebra.ams.device" />
    <parm name="Class"
 value="com.zebra.backsafe.android.splash.SplashActivity" />
  </characteristic>
  <characteristic version="4.2" type="XmlMgr">
    <parm name="ProcessingMode" value="2" />
  </characteristic>
  <characteristic version="6.0" type="ConditionMgr">
    <parm name="DataType" value="3" />
```

Portal Unavailability

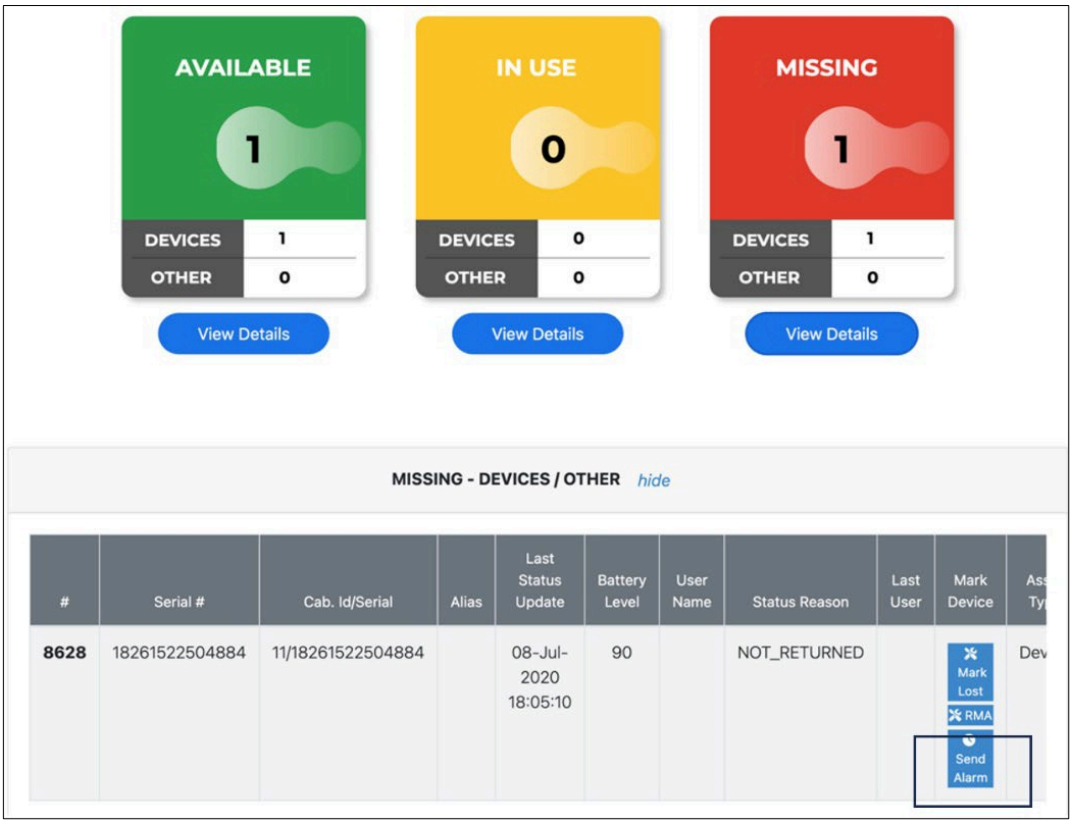
The Portal is down due to connection issues.

- If you need help accessing the home page or site, verify access via public internet. If the Portal is still not accessible, escalate for an immediate reboot/restart of the Portal.
- If Portal pages are accessible from the public network and not from within the customer network, verify the customer network settings.
- If Portal can be accessed from the KIOSK browser, but the KIOSK reports connection errors, collect RxLogger logs and escalate for review. To recover from the issue, reboot or restart the KIOSK core services.
- If the Zebra monitoring services auto-detect the Portal is down, the issue will be escalated for recovery. A server restart can fix the problem.

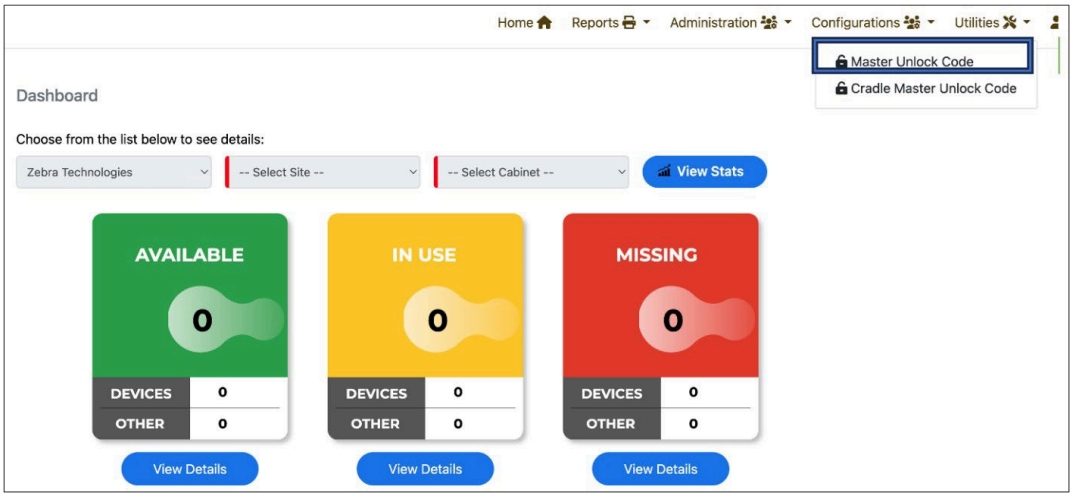
Master Unlock Code: Finding the Missing Device

Master Unlock Code.

1. Send an alarm from the ZAMS Portal when the device is not visible.



2. After the device is found, the Device User can stop the alarm using any of the following methods:
   - Enter the passcode.
   - Place the device back into the cradle.
   - You can scan the QR Code from the **Utilities** > **Master Unlock Code**.



   - Scan the QR code from the UI.

   - Scan the Barcode from the UI. It is only applicable to linear devices.

Cradle Master Unlock Code

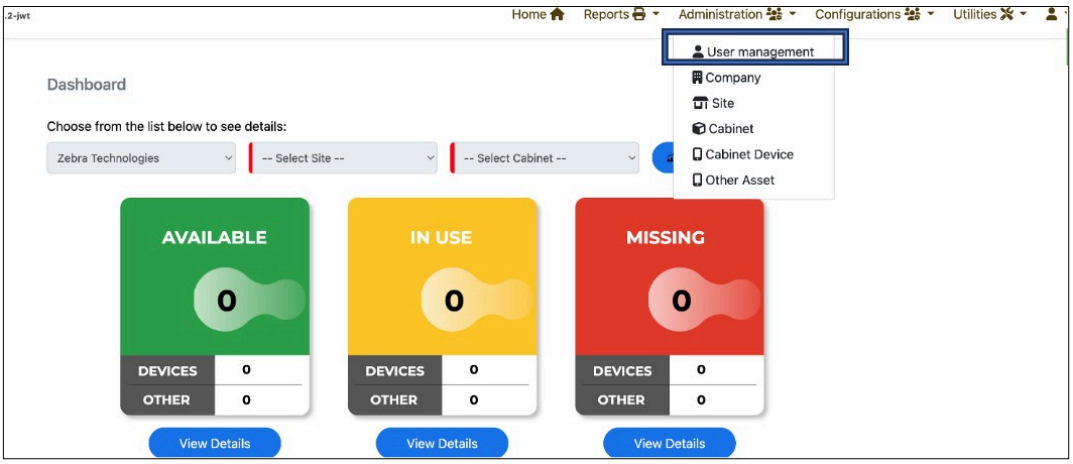
This section explains how to access the device when the Portal or KIOSK is unavailable.

- Access the Zebra support portal and generate the Cradle Master Unlock QR code from the **Utilities** > **Cradle Master Unlock Code** screen using a Wi-Fi connection.
- This QR code is valid for 48 hours. If Wi-Fi (KIOSK and/or Portal) is down, users can use this QR code to log in within 48 hours.
- There are no limitations to the number of logins on a device.

NOTE: Generate a **Cradle Master Unlock QR Code** or create a **ROLE_DEVICE_INTERNAL_USER** as a prerequisite before KIOSK downtime. It is important to create the Role Internal Device User as it will sync to the KIOSK at one-minute intervals, and internal users are automatically pushed to the device when the KIOSK is down. The **ROLE_DEVICE_INTERNAL_USER** allows users to unlock and log into the device as the authentication process is handled internally, which ensures access and functionality during KIOSK downtimes.

Portal and KIOSK or only KIOSK is down: Break Glass

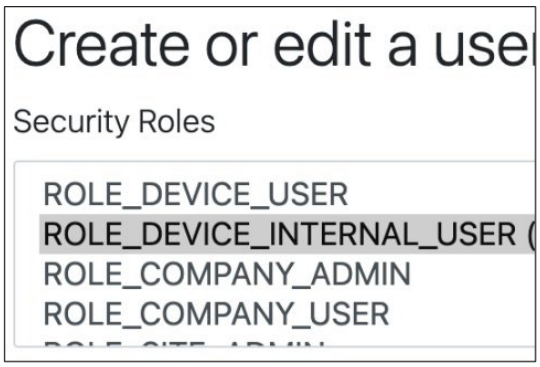
1. To unlock the Cradle Master, use the Cradle Master Unlock Code feature described above.
2. Company admins can assign the **ROLE_DEVICE_INTERNAL_USER** to up to five employees per site in User Management.



3. When KIOSK and Portal or only KIOSK are down, **ROLE_DEVICE_INTERNAL_USER** can log in and pass the device to the Device User.

NOTE: Generate a **Cradle Master Unlock QR Code** or create a **ROLE_DEVICE_INTERNAL_USER** as a prerequisite before KIOSK downtime. It is important to create the Role Internal Device User as it will sync to the KIOSK at one-minute intervals, and internal users are automatically pushed to the device when the KIOSK is down. The **ROLE_DEVICE_INTERNAL_USER** allows users to unlock and log into the device as the authentication process is handled internally, which ensures access and functionality during KIOSK downtimes.

NOTE: ROLE_DEVICE_INTERNAL_USER is a privileged role assigned to five users per site.



4. Log into the device.

Forgot User Password

- A common issue faced during first-time login is when a user clicks on a **one-time** use URL that resets the only portal account password given to them. This may happen when the user forgets to set a password using the company admin role account. If this happens, the issue must be escalated to the ZAMS Database owner to reset the password.
- Company admins are encouraged to create additional administrative accounts on the portal. If another administrator account is present, they can change the password for other users, including other admin accounts. Additional administrative accounts allow the customer to correct the problem without needing assistance from Zebra.
- For security reasons, Zebra cannot access customer data except in exceptional circumstances. Therefore, customers are required to set up additional administrative accounts to avoid delays in resetting their passwords.

Device State Discrepancies

The device state is either displayed on a different KIOSK or not.

- The Mobile Device is registered to a given KIOSK regardless of where it is charged. Suppose the device is reporting status to a KIOSK in an unexpected location, the device should be moved to the expected cabinet or registered to the new KIOSK.
- Refer to the Zebra Access Management System Installation Guide for information on registering a device at the KIOSK.

- An upcoming release of ZAMS will support the return to a different cabinet. However, the initial registration of the Mobile Device to a KIOSK is still required.

Unable to Log into Zebra Support Site

To access the ZAMS software, customers must register their ZAMS contract ID to access the Zebra support portal. The contract ID can be obtained from their sales representative. Alternatively, customers can raise a ticket with ZAMS's Zebra order management owner.

Device SSO Login

If the SSO users cannot log into the device because of Identity Provider (IDP) redirection not working or an IDP error page loading:

- Verify if the IDP details under the MDM configuration are correct. Verify the metadata URL and ensure that the Client ID is correct.
- If all MDM configurations are correct and the SSO login is still unsuccessful, cancel the SSO login and use failback user credentials to continue operations. For further assistance, contact the Zebra Help Desk.

If the IDP login page is not loading:

- Verify if the IDP details under the MDM configuration are correct. Verify the metadata URL and ensure that the Client ID is correct.
- Verify if the IDP is reachable and examine the network strength.

If the IDP login page is loaded but the login is not working:

- Verify the credentials provided.
- Verify if the user is assigned to the application on IDP.
- Verify if the user is active on IDP.
- Verify with IDP configuration for the ZAMS device application.

If an SSO user logs into the Device, but the device status does not change to **IN_USE** on KIOSK:

- Replace the `ZamsDeviceA10Permission.xml` on the device's `/sdcard/download` folder with the `ZamsDeviceA10Permission.xml` from the **24.3.0 zip file**, and then reinstall the ZAMS application.

Portal SSO Login

If the Identity Provider (IDP) login page is loaded but the SSO login is not working:

- Verify the credentials provided.
- Verify if the user is assigned to the application on IDP.
- Verify if the user is active on IDP.
- Verify with IDP configuration for the ZAMS portal application.

If the IDP login page is not loading:

- Clear the browser cache and retry.
- Verify if the IDP is reachable or accessible.

If the SSO users cannot log into the portal because of IDP redirection not working or an IDP error page loading:

- Contact the Zebra Help Desk for assistance.