Zebra Access Management System (ZAMS) v25.1.2

Release Notes – July 2025

Highlights

- Bug fixes to resolve customer-reported issues

Device and Portal Support

Mobile Devices (Android version 8, 10, 11, 13,14)

- Zebra full touch devices (TC15, TC2x, TC5x, TC7x, EC5x, HC2x, HC5x).
- Zebra keyboard device (MC22xx, MC33xx, MC93xx, MC94xx).
- Zebra small devices (EC3x, EC5x, WT6300).
- Zebra Android tablets (ET4X, ET5X).
- Exceptions: Mobile devices with external power packs. Support on a case-by-case basis.

Kiosk Devices

- CC6000 (Android version 8, 10, 11, 13, 14).
- ET40 (Android version 11 and 13, 14).

Portal UI

- Chrome version 9 or later.
- Microsoft Edge version 124 or later.

Updates in this release

- Portal: AMS Server (v4.3.3)
- Kiosk: AMS (v2.2.1).
- Device: AMS (v3.2.1).

New Features

- N/A

Usage Notes

- Refer to ZAMS Installation Guide

Requirements

- Refer to ZAMS Installation Guide for SSO configuration.

Resolved Issues

- SFDC Case # 22445897 : Resolved the Historical Report issue of Device status not showing Serial Number
- SFDC Case # 19569281 : Resolved the portal issue of Not able to delete Sites from ZAMS portal
- SFDC Case # 21233229 21799807 : Resolved the ZAMS Application Crashes on device when SIM card is inserted
- SFDC Case # 21337611 : Resolved the Bluetooth Proximity issue while using Imprivata
- SFDC Case # 21233229 21838999 : Resolved the ZAMS Portal issue for user login does not work with lowercase
- SFDC Case # 21824414 : Resolved the portal issue of Device Alias name not getting updated on portal with bulk upload
- SFDC Case # 21733711 : Resolved the portal issue of daily scheduled report missing full Device list.
- SFDC Case # 21892256 : Resolved the portal issue of External users not able to delete from the ZAMS portal
- SFDC Case # 22217520 : Resolved the Historical Report Issues
- Resolved the kiosk issue of Send Alarm and RMA functionality not working in 25.1.1 release

Known Issues

- For optimal Imprivata app performance, turn off "App Login on Reboot" and BLE proximity settings.
- Scheduled Email: To adjust for daylight saving time, update scheduled email time in the ZAMS Portal.
- Imprivata SSO intent known issues:
    - Avoid special characters in usernames.
    - Send login intents only when the device is outside the charger.
    - Configure ZAMS client to hide PIN UI to prevent unintended alarms.
- When pin uniqueness is set to "SITE LEVEL" for a company, company admin is unable to deactivate global users associated with their company. Pins are unique across the company / site.
- In Portal, while updating Role_Device_User, editing any field apart from PIN and Click on Save, sometimes error "PIN is already in use!" may appear.
- User login and user logout information sync between kiosk and portal takes approximately Sync_Time_Configured + up to 3 minutes. This affects "One Device One User" functionality during this window.
- For SSO enabled login users, Identity Guardian screen saver is displayed on charging screen, when device is on charge. As of now, this prevents device alias name from displaying on charging screen.

- In the portal, when an admin edits a company edit page in the Portal and enters incorrect authentication protocol information for Single Sign-On (SSO) configuration, an error "status:500, error FileNotFoundException" message is displayed (While users would be expecting a more relevant error description)
- When using Single Sign-On (SSO) with SAML authentication on Portal, it is strongly recommended to follow below practices to avoid other users or malicious websites to reuse persistent cookies after logging out:
    - Use incognito mode / private mode of browser for portal usage.
    - Close the browser session after portal usage is over and log out action is completed.
- Previous version of ZAMS has a known issue when "One Device User" setting is enabled. Users may experience error "User already logged in on another device". The current release of ZAMS addresses this error. It is recommended to delete and recreate user who has experienced this error to prevent further issues.
- For devices running Imprivata versions 7.15 and above, you might encounter an "Error to logout Imprivata" popup when placing the device in the cradle. If this issue arises, please resolve it by uninstalling and then reinstalling both the ZAMS device APK and the Imprivata APK.
- In the portal, customers should create only one Email configuration per site in the Email notification.

Important Links

- Intelligent Cabinet Support and downloads – downloads, User Guide, Installation Guide and Troubleshooting Guide

About Zebra Access Management System

Zebra Access Management System (ZAMS) is an easy to use software solution to manage and control your mobile assets. The intelligent way to keep your mobile computers safe.

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 administration level tasks and reports. The server access location is https://zams.zebra.com/