Zebra Identity Guardian 1.3

Release Notes – April 2024

Highlights

- Now available for download from Google Play.
- The Authentication Data Storage feature, formerly a preview, is now officially launched. It allows for temporary storage of user barcode data, simplifying subsequent logins throughout a work shift.

Device Support

No new devices added in this release. See the Zebra Support Portal for a list of supported devices.

Usage Notes

- Screen lock in Android device settings must be set to "None." Other types of screen locks, such as swipe or pin, are not supported.
- For users of the 42Gears EMM system, apps installed through ZDNA in app update mode must be set as high priority.
- While performing facial authentication on an ET45, the device must not be rotated.

Requirements

- Refer to the System Requirements section in Identity Guardian documentation.
- Refer to the System Requirements section in ZDNA Cloud documentation.

Resolved Issues

- Resolved an issue on Android 13 devices that automatically upgraded applications from the Play store, in which Identity Guardian would display its blocking screen on devices that were not configured with Identity Guardian. This is resolved with Identity Guardian v1.3.0.1104.
- Resolved an intermittent issue where devices displayed a "Scan to Unlock" button on the blocking screen instead of the "Unlock" button when device authentication was set to a mode that does not require the end user to scan a barcode.
- Resolved an issue where an end user was not able to login to the device using the Admin Bypass Passcode as the fallback authentication.

Known Issues

- Uninstalling Identity Guardian from the blocking screen disables the home button on the device. To remedy this, either reinstall Identity Guardian or set it to enrollment mode before uninstallation.

- When installing Identity Guardian in enrollment mode from VMWare Workspace ONE UEM (AirWatch) EMM via Google Play, the authentication screen may appear instead of the expected enrollment screen. To prevent this, install, and configure the application from the VMWare private app store instead of the public Play store.
- When using Microsoft Entra ID for single sign-on (SSO), a new user will not be automatically logged into Microsoft Associated apps following the sign out of a previous user. To address this, users can either relaunch the Microsoft Associates apps or enter the newly logged in user ID when prompted, ensuring a successful login.
- A user authentication error may occur intermittently if a user attempts to cancel SSO authentication and then tries to re-authenticate. To resolve this, click on any button on the error screen to dismiss the error, allowing the user to proceed further.
- When PingFed is used for single sign-on (SSO) and Identity Guardian is upgraded, users may experience a one-time issue where they cannot sign out from Identity Guardian on a shared device. This is overcome by rebooting the device, docking it on a cradle, or locking/unlocking the device based on the configuration set by the system administrator. This issue does not recur after the first sign-out attempt.

Important Links

- About Identity Guardian
- Identity Guardian User Guide
- Identity Guardian Setup
- Identity Guardian Managed Configurations
- Identity Guardian API

About Zebra Identity Guardian

Zebra's **Identity Guardian** simplifies device authentication by combining facial biometric recognition, multifactor login, and single sign-on (SSO) for a personalized role-based experience. It uses facial biometrics to unlock mobile devices securely, regardless of whether they are shared or personally assigned. If facial biometrics is not the preferred choice, a unique barcode or PIN offers an alternative secure access method.

Identity Guardian ensures full protection of employee data. In a shared device model, user data is securely encrypted in a personal barcode stored on the device, which can optionally be created based on facial recognition. For personally assigned devices, the data is secured within the Android framework, making it inaccessible even to the organization itself.