Zebra Identity Guardian 1.1
Release Notes – February 2024

Highlights

- Enhancements to blocking screen experience
- Resolved issues

Device Support

No new device support 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.
- Identity Guardian can be installed and configured from Zebra DNA Cloud (My Apps > Zebra Collection), Zebra StageNow or a company’s own EMM system.
- 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

- Enhanced Identity Guardian blocking screen behavior to appear quicker after device reboot.
- Resolved an issue where Identity Guardian’s managed configuration was not loading from the EMM UI.
- Ping Identity SSO configurations now consistently functions with Identity Guardian when set up from EMMs.

Known Issues

- On TC22 or TC27 devices, occasionally an error message may appear requiring the MDNA license following a device restart.

Important Links

- About Identity Guardian
- Identity Guardian User Guide
- Identity Guardian Setup
- Identity Guardian Manage Config
- 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.