Zebra Identity Guardian 2.0
Release Notes – March 2025

Highlights

- Supports Zebra devices with Android 14.
- Integrates Zebra Device Guardian with Identity Guardian for accountability and single sign-on (SSO) functionality.
- Introduces an alarm feature for devices that are disconnected from power without a user sign-in.
- Implemented a temporary block on user login after multiple failed attempts with the Admin Bypass passcode.

Device Support

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

New Features

- Identity Guardian now extends its support to Zebra devices operating on Android 14.
- Integrated Zebra Device Guardian with the Identity Guardian client. Device Guardian v1.0 now fully supports Identity Guardian, enabling the collection of device check-in/check-out data and providing single sign-on (SSO) capabilities.
  Note: Identity Guardian will continue to support the Device Tracker application until the end of 2025. Customers are encouraged to migrate to the Device Guardian application by then.
- Introduced a new feature that sounds an alarm if a device is disconnected from its power source and the user doesn't log back in within a predetermined timeout period. This functionality is designed to prevent device misplacement and loss.
- Introduced a security enhancement that temporarily blocks device login for 5 minutes after five failed attempts with the Admin Bypass passcode.

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.

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 where the “Enroll User” option was absent on the Identity Guardian lock screen when no user verification method was configured under Authentication Configuration in Managed Configuration through the EMM.
- Modified Identity Guardian to accept empty values for the Legacy Barcode Prefix, permitting users to scan non-Identity Guardian barcodes without a specified prefix for device sign-in.

Known Issues

- On Android 14 devices, the Guardian Safe and Autofill SSO features are not functioning consistently. To resolve this, manually disable and re-enable the Android Accessibility Service permission under the Guardian Safe settings menu.
- Users are unable to answer a call from the notification bar if the Identity Guardian blocking screen is in the foreground, even if the application is in the allowed list to appear over the blocking screen. Ensure the Identity Guardian blocking screen is not active in the foreground when attempting to answer a call from the notification bar.
- When Identity Guardian is configured with Single Sign-On authentication mode via VMware Workspace ONE UEM, the Chrome custom tab does not automatically close upon performing a manual sign-out operation. To address this, ensure that a value is assigned to Verification Setup for the ‘On device manual checkin’ option in the Identity Guardian Managed Configurations setting.
- Single Sign-On (SSO) credentials are not automatically populated during the Identity Guardian login process for devices configured in shared mode using the Microsoft Authenticator app with Microsoft Entra ID SSO. To resolve this issue, enable both the Guardian Safe and Auto Fill for SSO options in the Guardian Safe configuration.
- After adding the Identity Guardian package name under “Apps Allowed on Lock Screen,” users cannot access the Guardian Safe app list on the device.
- Users may experience a brief delay in password autofill when using the Auto Fill SSO or Guardian Safe features, particularly after a device reboot or when the device wakes from a low-power state (doze mode). To minimize this impact, allow a few seconds after your device has restarted or woken up before attempting to log in.
- When using the Microsoft Authenticator app in shared mode for Microsoft Entra ID single sign-on (SSO), users may be unable to modify credentials saved in Identity Guardian. To resolve this, remove the existing app entry from the Guardian Safe list. On the next app login attempt, the user is prompted to save their credentials, allowing them to update their credentials afterward.
- 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 via Google Play, the authentication screen might 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 might 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 might experience a one-time issue preventing them from signing in 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.