ZEBRA

Device Guardian + Device Guardian Access Management

Migration Customer Journey

Version 1.0
December 16, 2025

ZEBRA GUARDIAN PORTFOLIO INTRODUCTION.

This document outlines the steps that a customer must perform to upgrade, configure, and use the Zebra Device Guardian and Device Guardian Access Management from ZAMs.

Zebra guardian offers a streamlined experience at every stage of device use for frontline workers – starting with secure access and ending with safe storage and readiness for the next shift. These four integrated solutions work seamlessly together to minimize lost device incidents, maximize productivity, and ensure your devices are always available and secure. These are:

a. Four key solutions:

- **Identity Guardian – Device Access:** Worker access devices securely with personalized credentials, including facial biometrics and single sign on ensuring fast and safe logins
- **Device Guardian – Find/Prevent Lost Devices:** Quickly find misplaced devices and proactively prevent loss, protecting both your investment and productivity
- **Device Guardian Access Management – Device Status:** Monitor device status and availability in real time, ensuring devices are always charger and ready for user
- **Guardian Cabinets – Device Status and Storage**: Smart storage solutions control device access and automate device readiness from shift start to finish.

b. Supported MDMs:

An MDM is required for the enrollment of devices, the supported MDMS are:

- ZDNA - ZDNA set-up
- SOTI - SOTI- set-up
- WORKSPACE ONE UEM - WORKSPACE - ONE UEM - set-Up
- 42 GEARS SUREMDM – 42 GEARS set-up
- Microsoft Intune - Intune set-up

c. Upgrade Prerequisites:

- Identity Guardian compatible hardware listed here.
- Device Guardian and Device Guardian Access Management compatible hardware listed here.
- Zebra DNA compatible hardware listed here.
- Device Guardian and Device Guardian access Management Setup requirements listed here.
- Refer to Skills Matrix here.

INSTALLATION AND CONFIGURATION OVERVIEW.

1. Zebra will contact customers with upgrade information and schedule on agreed timing.
    a. Customers will review the supported MDMs and upgrade prerequisites as listed here.
2. At designated timing, Customer will download and deploy DGAM APK to devices/kiosk and Login into DGAM portal.
    a. **Action:** Complete steps as outlined under Guided Walkthrough section.

STAGE 1: PURCHASE AND ONBOARDING

Customer Action

- Purchase or renew DGAM license

Zebra Action

- Provisions for a new DGAM cloud instance
- Send onboarding email with:
    1. DGAM portal URL
    2. Login credentials
    3. APK download link
    4. User guide

Customer Outcome

- Customers are onboard and ready to begin migration

STAGE 2: MIGRATION PLANNING AND READINESS

Customer Action

- Aligns with Zebra on the migration time window
- Prepares MDM for device re-enrollment

Zebra Action

- Confirms migration slot
- Prepares ZAMS data for migration

Customer outcome

- Migration plan is finalized with minimal business disruption

STAGE 3: PORTAL DATA MIGRATION

Customer Action

- Logs into DGAM portal using onboarding credentials received in welcome email
- Reviews migrated data

ZEBRA ACTION

Migrates the following data from ZAMS to DGAM

- Sites
- Admin users

CUSTOMER OUTCOME

Customer sees the ZAM's data migrated and available in DGAM

STAGE 4: DEVICE AND KIOSK MIGRATION PREPARATION

Customer Action

- Initiates ZAMS application removal from devices/kiosk

Customer Outcome

- Devices/kiosks are prepared for DGAM installation

STAGE 5: ZAMS APPLICATION UNINSTALLATION

Path A: USING STAGENOW

Scan StageNow barcode

- Below Android 13 -> Uninstall_ZAMS_Device
- Android 13 & above -> A13_Uninstall_ZAMS_Device

Outcome

- ZAMS application is removed from the device

Path B: Using MDM

Customer Action

- Run ZamsDevice_Uninstall.xml via MDM

Outcome

- Devices are cleared of ZAMS and ready for DGAM.
- For more information on migration set-up please refer to the Migration User Guide.

Refer the below Guided walkthrough on setting up DGAM and configuring your devices and kiosks

GUIDED WALKTHROUGH

Phase 1: Download and Set Up DGAM through MDM

Goal: Prepare your environment and deploy the DGAM application on your devices and kiosks.

Step 1: Download the DGAM Package

• Option 1: Visit Zebra.com and download the latest (DGAM) package Device Guardian Software Downloads | Zebra.

• Option 2: Download "Device Guardian APK" from Google play store

Step 2: Upload the DGAM Package to Your MDM

- Sign in to your preferred Mobile Device Management (MDM) platform or Enterprise Mobility Management.
- Upload the DGAM application package to your MDM console to make it available for deployment.

Step 3: Enroll Devices and Kiosks

- Use your MDM/EMM to enroll in all devices and kiosks. Device enrolment can only be completed via MDMs. *See Supported MDMs*.
- Download the enrollment kit from the DGAM portal and integrate it with your MDM.
- Integration of the **authentication keys in the enrollment kit** ensures that each device and kiosk is linked to the correct DGAM instance associated with your tenant.
- Refer to your MDM-specific documentation for detailed enrollment steps.

Outcome: Once enrollment is complete, the DGAM app becomes visible on both kiosks and mobile devices.

Phase 2: New Site Creation in the DGAM Portal

Goal: Create and activate sites for your organization.

1. Sign-in to the DGAM Portal.
2. Navigate to Sites → Create Site.
3. Enter the required site details and activate it.

Outcome: The site created becomes available for linking kiosks in the next step. Refer to "create site" guide for more details.

Phase 3: Kiosk Association to Site

Goal: Link kiosks to the correct site.

1. Open the Kiosk section in the DGAM Portal.
2. Select the site you created earlier.
3. Assign each kiosk to the appropriate site.

Outcome: Kiosks are now successfully mapped to their respective sites. Refer to kiosk to site allocation for detailed instructions.

Phase 4: Device-to-Kiosk Association

Goal: Register mobile devices at their respective kiosks. Choose one of the following methods:

Option 1: Bulk Upload

- Go to the Kiosk Device page in the DGAM Portal.
- Use the Bulk Upload option to register multiple devices at once.

Refer to "Device to Kiosk assignment" for upload format and steps.

Option 2: Manual Registration

• On the kiosk, select Register / Sync to scan and pair device

Refer to "Register device to kiosk" and "Import the Data Wedge profile" for step-by-step details.

Option 3: Auto-Assignment

• Enable Device-to-Kiosk Auto-Assignment in the DGAM Portal.

• Devices will be automatically assigned to the kiosk.

Refer to "Device to kiosk Auto Assignment" guide for configuration steps.

Outcome: Devices are successfully registered and linked to their respective kiosks.

Phase 5: Download Identity Guardian (IG)

Visit Zebra.com and download the latest (IG) package Identity Guardian Support | Zebra.

Phase 6: Configure Identity Guardian (IG)

Goal: Enable secure user authentication using Identity Guardian.

Step 1: Enroll Users

User enrollment depending upon the device access method can be classified into the following

- Shared device – Two methods under shared device are standard enrollment and self-enrollment
- Personally Assigned device

Follow the IG user enrollment guide to add users to the IG system.

Step 2: Configure Authentication Methods **through MDM**

• Choose your primary and secondary authentication methods

• Provide a valid comparison source for identity matching.

• Refer to Authentication documentation for detailed step by step instruction.

Step 3: Set Up Admin Bypass Code

• Create an Admin Bypass Code for use in emergencies or unexpected login issues.

Outcome: Users can now authenticate securely using IG on mobile devices.

Phase 7: Bulk upload device users in the DGAM Portal

a) Deploy ZDNA client with configuration token (Required only during cloud passcode authentication)

Goal: Install the ZDNA application with the correct DGAM configuration token

Steps:

1. Download the ZDNA configuration token from the DGAM portal (Available in Device Users -> User management)
2. Push ZDNA client application through respective MDM/EMM by configuring it with ZDNA configuration token downloaded from the DGAM portal
3. Ensure the ZDNA client is deployed in all the devices

Outcome:

ZDNA client is successfully installed

b) Deploy and configure Identity Guardian (cloud passcode) via MDM

Goal: Install Identity Guardian on devices with cloud passcode enabled

Steps:

1. Login to the respective MDM/EMM
2. configure Identity Guardian with Primary authentication factor as cloud passcode and comparison source as cloud
3. Deploy the Identity Guardian application to selected devices

Outcome:

IG is deployed and configured to authenticate users with cloud passcode

C)Add Device Users to the DGAM Portal

Goal: Add device users and cloud passcode required for authentication in DGAM portal

Steps:

1. Go to the user management section (device users) in the DGAM portal
2. Download the CSV file template available inside the 'Bulk Upload' option
3. To upload device user details, first update the CSV file with device user details, and then use the 'Bulk Upload' option located within the device user's section of the user management page.
4. View the status of the bulk upload by click on “view import jobs” available in the device user’s section in user management page

Outcome:

Device users and their cloud passcodes are successfully uploaded

d)User authentication on device using cloud passcode

Goal: Allow users to authenticate and complete onboarding using cloud passcode

Steps:

1. Launch Identity Guardian (IG) on the device
2. Tap **Enter Passcode**
3. Enter the **Cloud Passcode** uploaded during the DGAM bulk upload
4. IG verifies the passcode and logs the user into the device.

Outcome:

Device users are authenticated successfully

Note: For detailed steps of device users bulk upload through DGAM portal please refer the user flow updated in "Device users"

Phase 8: Validation and Readiness

Goal: Verify that everything is working correctly.

1. Confirm that for all the devices and kiosks, the profiles created have been pushed through the respective MDM/EMM.
2. Log in to mobile device using IG authentication.
3. Test device user access to ensure successful login.
4. The device counts are shown accordingly in the Available, In-Use & Missing Tabs in Kiosk after device users check-in/check-out.

Outcome: With DGAM successfully set up and configured, it allows you to explore all available features and capabilities in it.

Useful Links
Device Guardian Technical Documentation
Supported MDMs
Identity Guardian Technical Documentation

For any issues, please visit Zebra Software Support for assistance.

GLOSSARY

Term	Definition
Kiosk	A physical touch screen tablet mounted on the Guardian Cabinet. It displays device status such as Available, In Use, Missing, and allows users to check devices in/out.
Site	A site represents a physical location or operational unit within an organization where devices are deployed, tracked and managed
Device	The mobile device docked inside the Guardian cabinet. Users can check these out to perform daily operational task
Enrollment Kit	A package available in the DGAM portal that contains the required configurations to enroll devices and kiosks into DGAM server though MDM
MDM (Mobile Device Management) or EMM (Enterprise Mobility Management)	A Management system like ZDNA, AirWatch or SOTI is used to deploy applications, push configurations and manage mobile devices.
IG	Identity Guardian
DGAM	Device Guardian Access Management