

Rugged device management (Zebra devices)



Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview - Rugged Device Management	5
Chapter 2. Creating and configuring Zebra StageNow profile.....	6
Creating a Profile in Zebra StageNow.....	6
Adding Required Configuration Settings.....	6
Chapter 3. Device Enrollment.....	13
Chapter 4. Post-Enrollment Management	14
Integrating Zebra OEMConfig app.....	14
Deploying Enterprise Home Screen (EHS) Kiosk Policies.....	15
Chapter 5. Device Diagnostics and Logs.....	17
Chapter 6. Unenrol.....	18
Index.....	

Chapter 1. Overview - Rugged Device Management

This document provides comprehensive end-user and administrative instructions for configuring, deploying, and managing rugged devices within the enterprise environment. Following this workflow ensures that all devices meet corporate security requirements, adhere to default Mobile Device Management (MDM) policies, and maintain optimal operational health.

Supported Devices

- **Validated Models:** Zebra TC27
- **Minimum Android OS Version:** Android 10.0 or higher (required for BigFix MCM Android Enterprise management).
- **Minimum Zebra MX Version:** Zebra Mobility Extensions (MX) 10.0 or higher.
- **GMS Certification & OS Variant:** Devices must be **GMS-certified** (Google Mobile Services) to support standard Android Enterprise framework features, zero-touch enrollment, and Managed Google Play access. Standard Android Enterprise zero-touch enrollment is not supported on AOSP-only (non-GMS) builds without specialized offline staging configurations.

System Setup Requirements

- **Android Enterprise Binding** - This is mandatory for deploying the OEMConfig app and utilizing Android Enterprise Device Owner mode.
- **App Catalog Prep** - Pre-approve and add the "Zebra OEMConfig Powered by MX" application from Managed Google Play to the app catalog.
- **Network Access** - Ensure the corporate firewall or Wi-Fi network whitelists the following:
 - Google Services: All standard Android Enterprise and Google Play Store domains (e.g., *.[google.com](https://www.google.com), *.[googleapis.com](https://apis.google.com), *.[android.com](https://www.android.com)).
 - Bigfix UEM's enrollment URL
 - Zebra Services - For StageNow barcode generation (*.[zebra.com](https://www.zebra.com)).
- **Zebra Account** - Ensure your organization has registered for a Zebra account and linked your Zebra credentials (client ID/secret) to the Bigfix UEM's integration settings.
- **Admin Workstation Setup** - Download and install the latest version of Zebra StageNow tool on the primary IT Operator Windows device.
- **Create StageNow profile** - Create a StageNow profile with required configurations that includes credentials for a dedicated provisioning Wi-Fi network so devices can connect to the internet instantly upon scanning the first barcode.
- **Device Readiness** - Factory State: Devices must be in a factory-reset state (out-of-box experience) to be enrolled in Android Enterprise "Device Owner" mode. If a device was previously used, you must perform an Enterprise Reset or Factory Reset.
- **Battery Level** - To prevent interruptions during the enrollment flow or OS updates, ensure devices maintain at least a 30% battery charge prior to initiating provisioning.

Chapter 2. Creating and configuring Zebra StageNow profile

The Zebra StageNow profile enables automated device enrollment by generating staging barcodes during pre-provisioning. Key components include Wi-Fi configuration, conditional checks, remote file downloads, and automated app setup to streamline device onboarding.

Creating a Profile in Zebra StageNow

This topic provides step-by-step instructions for creating a new profile in the Zebra StageNow Workstation Tool.

Prerequisites

Ensure you have the Zebra StageNow Workstation Tool installed on your PC and have the necessary credentials to sign in.

Step-by-Step Instructions

1. **Open the StageNow Workstation Tool** on your PC and sign in with your credentials.
2. Click **Create New Profile** from the main dashboard.
3. In the **Target Device MX Version** drop-down menu, select the appropriate MX version for your devices.



Note: If you are managing a mixed fleet, choose the lowest MX version present among your devices to ensure compatibility.

4. Select **Xpert Mode** (or **Enroll in an MDM** if applicable) and click **Create**.
5. Enter a **Profile Name** (for example, *Zebra_AMAPI_Enrollment*) in the provided field and click **Start**.

After Completing the Steps

Once you have created the new profile, you can proceed to configure the specific settings and actions required for your deployment scenario. This may include adding configuration steps, specifying device behaviors, or setting up enrollment parameters.

After finalizing the profile configuration, you can generate a barcode for device staging, or export the profile for use with your device fleet. For more detailed information and advanced configuration options, refer to the official Zebra StageNow documentation: [Zebra StageNow Administrator's Guide](#)

Adding Required Configuration Settings

This topic describes how to add essential configuration service providers (CSPs) to your profile sequence, including Wi-Fi, Condition Manager, File Manager, Application Manager, and Intent parameters. Each CSP must be configured with specific settings to enable automated device setup and management. Follow the outlined steps to ensure all required configurations are applied correctly.

Add the following CSPs to your profile sequence by clicking the (+) button next to each item:

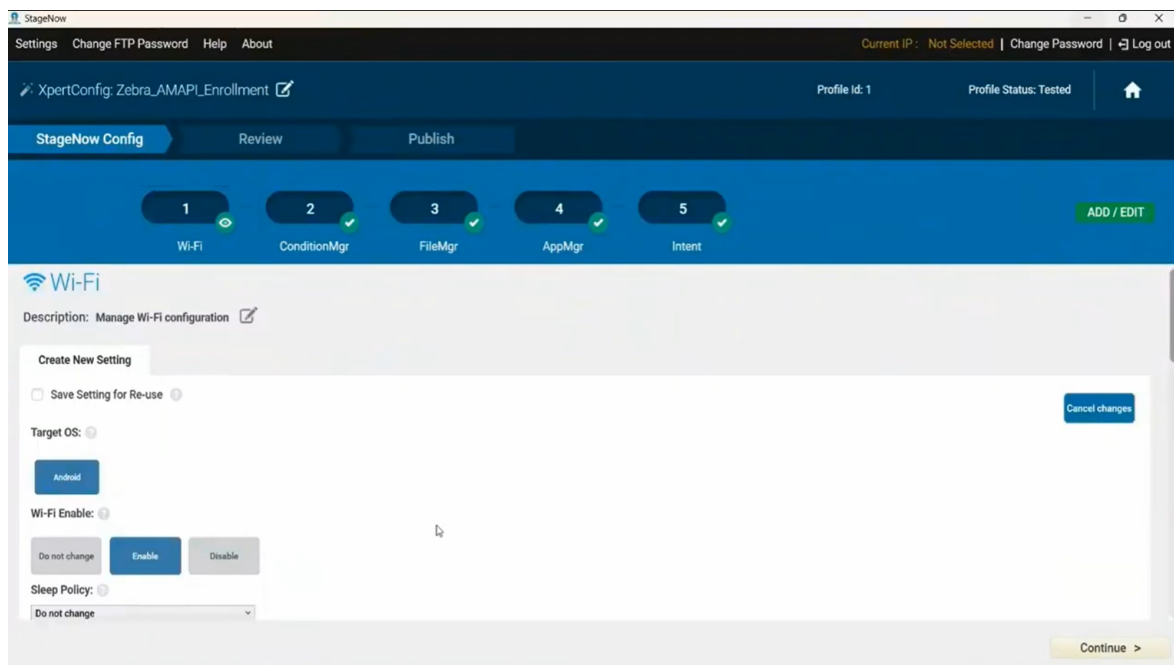
1. **Wi-Fi:** Enable Wi-Fi automatically and add your enterprise SSID and security credentials (e.g., WPA/WPA2-Enterprise or PSK).
2. **ConditionMgr (Condition Manager):** Configure a string evaluation test (e.g., evaluating pre-defined system string values like MX Version) to run conditional checks before proceeding.
3. **FileMgr (File Manager):** Configure the remote staging server URI to download payload packages (e.g., <https://play.google.com/managed/downloadManaging/>) to the device's target destination.
4. **AppMgr (Application Manager):** Define app installation rules, silent APK deployments, and package names.
5. **Intent (Intent Parameters):** Enter required intent parameters and DPC extras to automate background configurations and enrollment tokens.

Configuring Wi-Fi in StageNow

This topic provides step-by-step instructions for configuring Wi-Fi settings in a StageNow profile using the StageNow Workstation Tool. It covers accessing the Wi-Fi configuration, setting general Wi-Fi parameters, entering network credentials, and saving the configuration. Follow these steps to ensure your device connects to the correct enterprise Wi-Fi network during staging.

Follow these steps to configure a Wi-Fi setting profile within the **StageNow Workstation Tool**.

1. Access the Wi-Fi Configuration



- a. Open your active profile (e.g., Zebra_AMAPI_Enrollment) in the **StageNow Workstation Tool**.
 - b. Select **Wi-Fi** from the profile sequence bar at the top or click **ADD / EDIT** to include the Wi-Fi setting.
2. Configure General Wi-Fi Settings
 3. Add Network Credentials

- a. Under **Target OS**, ensure **Android** is selected.
 - b. Under **Wi-Fi Enable**, choose **Enable** to ensure the Wi-Fi radio turns on automatically during staging.
 - c. Select your desired **Sleep Policy** setting (e.g., Keep Wi-Fi on during sleep).
 - a. Scroll to the network settings section and set **Action** to **Add/Update Network**.
 - b. In the **SSID** field, enter your enterprise Wi-Fi network name.
 - c. Select the appropriate **Security Mode** (e.g., WPA/WPA2-Enterprise or WPA/WPA2-PSK).
 - d. Enter the required authentication credentials (e.g., *Passphrase or Enterprise Security Certificate/Identity details*).
4. Save and Proceed
- a. Click **Continue** in the bottom-right corner to save the Wi-Fi parameters.
 - b. Verify that the **Wi-Fi** step shows a green checkmark in the navigation bar before moving to the next configuration step (e.g., *ConditionMgr, FileMgr, or AppMgr*).
 - c. Click **Add** to proceed through each configuration page. Complete the required parameter fields for each selected CSP and click **Continue**.

Configuring Condition Manager (ConditionMgr) in StageNow

The Condition Manager (ConditionMgr) step in StageNow enables administrators to perform conditional checks before executing subsequent staging actions. This process involves selecting a data type, configuring a string data source, defining a condition test and value, and saving the configuration. Proper setup ensures that only devices meeting specified criteria proceed to the next stage.

Follow these steps to configure a string evaluation test.

The screenshot displays the StageNow web application interface. At the top, the navigation bar includes 'Settings', 'Change FTP Password', 'Help', and 'About'. The current profile is 'XpertConfig: Zebra_AMAPI_Enrollment' with 'Profile Id: 1' and 'Profile Status: Incomplete'. The 'StageNow Config' tab is active, showing a progress bar with five steps: 1. Wi-Fi (checked), 2. ConditionMgr (checked), 3. FileMgr (checked), 4. AppMgr (checked), and 5. Intent (checked). An 'ADD / EDIT' button is visible on the right. The 'ConditionMgr' configuration screen is shown, with a 'Save Setting for Re-use' header. It includes sections for 'Data Type' (Boolean, Integer, String), 'String Data Source' (String System Property, Pre-defined System String Value), 'String System Value' (MX Version, OSX Version), 'String Condition Test' (Equal to a Constant String), and 'String Constant Value'. A 'Cancel changes' button is on the right, and 'Back' and 'Continue' buttons are at the bottom.

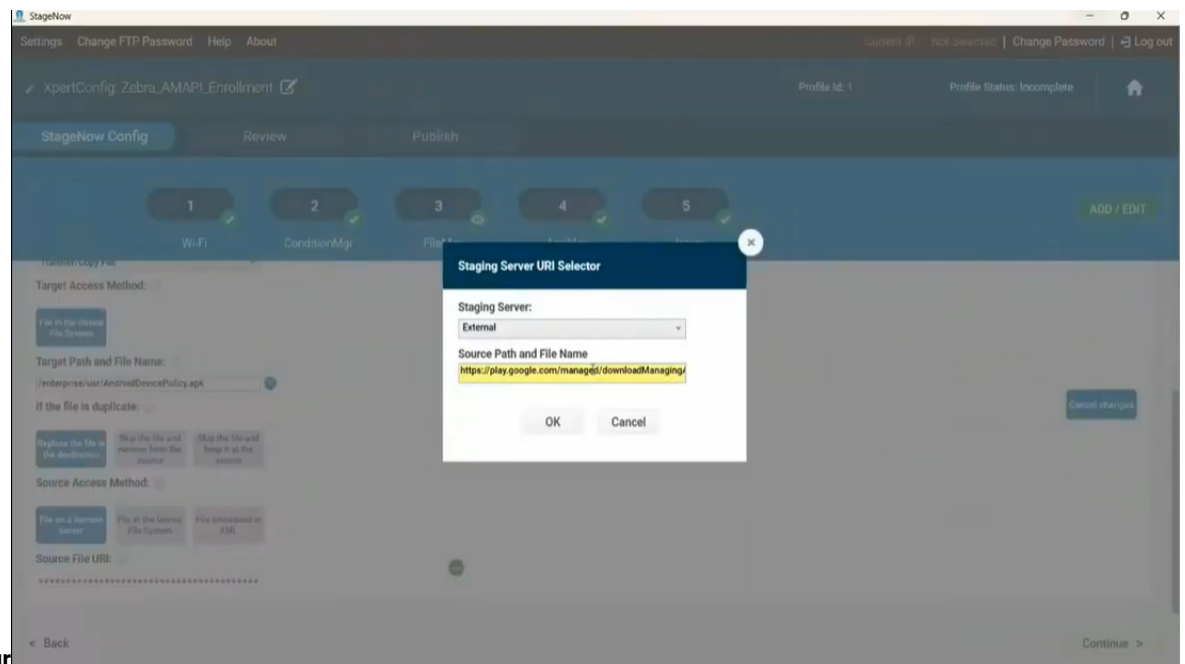
1. Select Data Type
 - a. In your active StageNow profile (e.g., Zebra_AMAPI_Enrollment), navigate to the **ConditionMgr** step.
 - b. Under **Data Type**, select **String**.
2. Configure String Data Source
 - a. Select **Pre-defined System String Value** under **String Data Source**.
 - b. Under **String System Value**, choose the system property you wish to test:
 - **MX Version** (*Selected*)
 - **OSX Version**
3. Define Condition Test & Value
 - a. Under **String Condition Test**, select the evaluation operator from the drop-down menu:
 - **Equal-to a Constant String**
 - b. In the **String Constant Value** field, enter the expected target value (e.g., the minimum required MX version string).
4. Save & Continue
 - a. Click **Continue >** in the bottom-right corner to save the condition parameters.
 - b. Verify that **ConditionMgr** displays a green checkmark in the profile sequence bar before proceeding to the next step (**FileMgr**).

Configuring Staging Server URI (FileMgr) in StageNow

Learn how to configure a remote server URI in the FileMgr step of StageNow to enable downloading payload files from an external or internal staging server. This process involves selecting the server type, entering the source path and file name, and applying the configuration within your active profile. Follow these steps to ensure proper setup for file management in StageNow workflows.

Follow these steps to configure a remote server URI for downloading payload files (e.g., downloadManaging) within a StageNow **FileMgr** step:

1. From your active profile (e.g., Zebra_AMAPI_Enrollment), navigate to



2. Next, to the **Source File URI** field, click the ellipsis button (...) to launch the **Staging Server URI Selector** modal.
3. Select the Staging Server Type: In the **Staging Server** drop-down menu, select **External** (or select the local StageNow FTP server if hosted internally).
4. Enter the Source Path and File Name:
 - a. In the **Source Path and File Name** field, enter the full remote URL of the target binary or package:
 - b. Plaintext `https://play.google.com/managed/downloadManaging/`
5. Confirm and Apply
 - a. Click **OK** to populate the URI into the **Source File URI** field of the **FileMgr** step.
 - b. Click **Continue >** to save the configuration and proceed to the next staging step (**AppMgr**).

Configuring Application Manager (AppMgr) in StageNow

The **Application Manager (AppMgr)** setting allows administrators to define app installation rules, perform silent APK deployments, and assign necessary system permissions during initial device provisioning.

Follow these steps to configure AppMgr in StageNow.

1. Access the AppMgr Setting
 - a. Open your active profile (e.g., Zebra_AMAPI_Enrollment) in the **StageNow Workstation Tool**.
 - b. Select **AppMgr** from the profile sequence bar at the top or click **ADD / EDIT** to include the AppMgr setting.
2. Select Application Action
 - a. In the **Application Action** drop-down menu, select **Install** (or **Upgrade**) to manage local application installation.
 - b. Choose **Slightly / Silently Install** to enable background installation without requiring user interaction.

3. Define Target Path and Package Details

- a. In the **Target Path and File Name** field, enter the exact local storage path on the Zebra device where the downloaded APK was placed by the previous **FileMgr** step (e.g., /enterprise/usr/AndroidDevicePolicy.apk).
- b. In the **Package Name** field, specify the application package identifier (e.g., com.google.android.apps.work.clouddpc or com.hcl.bigfixuem.dev).

4. Save and Proceed

- a. Click **Continue >** in the bottom-right corner to save the AppMgr parameters.
- b. Confirm that **AppMgr** displays a green checkmark in the navigation bar before moving to the next configuration step (**Intent**). During device staging, the StageNow engine executes the AppMgr payload to silently install the enrollment application package in the background and grant necessary administrative permissions.

Configuring Intent in StageNow

The **Intent** setting allows administrators to configure custom Android intents and DPC extras to automatically launch the MDM enrollment agent and pass background configuration parameters upon barcode scanning.

1. Access the Intent Setting

- a. Open your active profile (e.g., Zebra_AMAPI_Enrollment) in the **StageNow Workstation Tool**.
- b. Select **Intent** from the profile sequence bar at the top or click **ADD / EDIT** to include the Intent setting.

2. Select Intent Type and Target Action

- a. In the **Action** field, set the intent action (e.g., android.intent.action.MAIN or Start Activity).
- b. Specify the target **Package Name** (e.g., com.google.android.apps.work.clouddpc or com.hcl.bigfixuem.dev) and class path to trigger the enrollment client.

3. Add DPC Extras & Enrollment Tokens

- a. Navigate to the **Intent Extras / DPC Extras** parameters section.
- b. Enter required key-value pairs (e.g., com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN) to supply enrollment tokens and server URIs, automating onboarding without requiring manual user input.

4. Save and Proceed

- a. Click **Continue >** in the bottom-right corner to save the Intent parameters.
- b. Confirm that **Intent** displays a green checkmark in the navigation bar to complete the profile sequence.

Upon scanning the staging barcode, the StageNow engine executes the configured Intent payload to launch the MDM agent interface, pass the enrollment token, and automatically initiate endpoint onboarding.

Review and Publish Profile

Review the profile verifying configuration parameters, ensuring encryption is enabled, and selecting the correct barcode format for publishing. The process includes testing and generating a printable barcode PDF, with considerations for Android version compatibility. This ensures secure and accurate deployment of the profile.

1. Review all configured parameters on the Review screen.
2. Ensure StageNow Encryption remains checked to secure sensitive payload data.
3. Select the Barcode tab in the Publish section. Choose the appropriate barcode format (PDF417 or Linear, noting that newer Android versions like Android 14 may require specific barcode handling).
4. Click Test to verify, then click Publish and Stage to generate the final printable barcode PDF.

Review the configuration

1. Expand the settings list on the **Review** screen to verify all parameters.
2. (Optional) Click **Change** to edit any settings or click the pencil icon to add a profile description.
3. Ensure **StageNow Encryption** remains checked to secure sensitive payload data.
4. Click **Complete Profile**.

Publish and Generate the Barcode

1. Select the **Barcode** tab in the **Publish** section.
2. Select the barcode type required for your deployment:
 - **PDF417** (*Recommended for complex payloads*)
 - **Linear**
3. Click **Test** to generate a preliminary barcode PDF and verify functionality.
4. Once verified, click **Publish** and enter staging instructions for the operator.
5. Click **Stage** to generate the final printable PDF containing the staging barcode.

Chapter 3. Device Enrollment

The Zebra devices can be enrolled through the following methods:

Standard Android Enterprise Enrollment

Applicable for Zebra GMS devices, running modern Android through ADP. Enrollment possible through Android Zero-Touch or QR code enrollment. For more details, refer to https://help.hcl-software.com/bigfix/11.0/mcm/MCM/Config/t_android_enrollment_mcm.html

Using Zebra StageNow Barcode

1. Open the generated PDF on your PC or print a physical copy.
2. Power on the target Zebra device and launch the **StageNow** client application.
3. Open the StageNow app on the Zebra device and scan the generated barcode using the device scanner.

The device processes the configuration payload and automatically initiates enrollment with the MDM server.

Chapter 4. Post-Enrollment Management

These features are continuous, policy-driven functions enforced by the MDM agent after the device has been successfully enrolled and is in active operation:

- **Integrating Zebra OEMConfig app (on page 14):** Pushing Zebra-specific hardware configurations (advanced scanner parameters, button remapping) dynamically from BigFix MCM.
- **Deploying Enterprise Home Screen (EHS) Kiosk Policies (on page 15):** Deploy Enterprise Home Screen (EHS) to lock down devices to approved applications.
- **Battery & Device Health Operations:** [Monitoring battery cycle counts, health metrics, and automated diagnostics](#). Monitor battery cycle counts, charge state, and health metrics to schedule proactive replacements.
- **Boundary Rules & Security Controls:** Create [geofence boundary rules](#) to restrict unauthorized network access and prevent sideloading of unapproved applications.
- **Root Detection & Integrity Compliance:** Enforcement of [jailbreak/root detection](#). Automatic compliance scans verify device integrity and block compromised or rooted devices from accessing corporate data.

Integrating Zebra OEMConfig app

Follow these steps to install and configure the Zebra OEMConfig app with managed configurations using BigFix MCM policy deployment:

1. App Catalog Preparation & Approval

1. **Pre-approve Application:** Search for and pre-approve "Zebra OEMConfig Powered by MX" from Managed Google Play and add it to the BigFix MCM App Catalog.
2. **Verify Enterprise Binding:** Ensure the Android Enterprise binding is active in BigFix MCM for seamless silent app distribution and payload delivery.

2. Creating the Managed Configuration Policy in BigFix MCM

1. Log in to the BigFix WebUI and navigate to **Apps > MCM > Policies / Configurations**.
2. Click **Create Policy** and select **Android Managed Configuration Policy** (Application Configuration).
3. Select **Zebra OEMConfig Powered by MX** as the target application.

3. Configuring Granular Hardware Settings

- **Physical Key Remapping:** Remap dedicated physical hardware buttons (such as PTT side keys) to trigger barcode scanning via DataWedge (com.symbol.datawedge) or launch designated enterprise applications.
- **Advanced Scanner Parameters:** Define scanner parameters, beam width, decode feedback, and allowed barcode symbologies.

- **Hardware Restrictions & Lockout:** Disable physical volume keys, power options, or hardware reset button combinations to prevent unauthorized user tampering.
- **Factory Reset Restrictions:** Block access to factory reset settings (**Settings > System > Reset options > Erase all data**) and configure a system message indicating that factory reset is disabled for the user.

4. Policy Group Deployment

1. Save the OEMConfig Managed Configuration policy.
2. Assign the policy to a **Policy Group** and target the appropriate Zebra device group or Smart Group.
3. Deploy the policy dynamically over-the-air (OTA) to enforce settings on enrolled endpoints without requiring new barcodes or physical access.

Deploying Enterprise Home Screen (EHS) Kiosk Policies

Zebra Enterprise Home Screen (EHS) is a custom launcher (com.zebra.mdna.enterprisehomescreen) deployed via BigFix MCM to lock down rugged devices into secure, single-purpose or multi-app kiosk environments, restricting user access strictly to approved enterprise applications and settings.

1. Deploying EHS App Catalog

1. **Pre-Approve Application:** Search for and pre-approve "Enterprise Home Screen" (com.zebra.mdna.enterprisehomescreen) from Managed Google Play in the BigFix MCM App Catalog.
2. **Deploy Launcher Package:** Target the EHS app payload to designated Zebra device groups via BigFix MCM policy groups for background installation and default launcher assignment.
3. **Admin Mode Passcode:** Configure a secure Admin Mode Passcode within the EHS configuration to allow authorized IT personnel to temporarily unlock device settings on the physical endpoint.

2. Configuring Kiosk Policy & System Lockdown

Configure system restriction controls in the BigFix MCM Kiosk Policy payload:

- **System Navigation Controls:** Restrict system navigation drawer and hardware buttons:
 - **Disabled Navigation:** Completely disables Home and Recent Apps/Overview buttons to enforce single-app or lock-screen operation.
 - **Home Button Only:** Enables strictly the Home button, preventing multi-tasking and app switching.
- **Status Bar & Notification Controls:** Restrict top-bar expansion and notification drawer access:

- **Notifications & System Info Disabled:** Prevents users from pulling down the notification shade, accessing quick settings toggles, or viewing system notifications.
- **System Info Only:** Displays battery and connection status while blocking interactive notification expansion.
- **Power Button Actions:** Disables the power menu upon long-pressing the physical power button to prevent unauthorized reboots, shutdowns, or safe-mode booting.
- **Device Settings Access:** Blocks launch access to system Settings (com.android.settings), preventing users from altering Wi-Fi networks, display timeouts, or device options outside EHS admin mode.
- **System Error & Warning Handling:** Mutes system crash dialogs and unresponsive app warnings to maintain a seamless, uninterrupted kiosk UI.

3. App Whitelisting & Launcher Layout

- **Application Whitelisting:** Explicitly define approved internal and line-of-business application package names to display on the EHS home screen layout.
- **Hide Unauthorized Apps:** Automatically suppress all system and unapproved third-party icons from the launcher interface.

Chapter 5. Device Diagnostics and Logs

When operational or network issues arise, administrators can collect detailed telemetry and logs directly from the device. This enables real-time troubleshooting, remote diagnostics, and continuous monitoring of hardware health metrics such as battery and Wi-Fi status. This topic describes how administrators can gather device telemetry, access RxLogger logs, and perform remote diagnostics using BigFix MCM and the Zebra Device Diagnostics app.

Prerequisites

- Administrator access to the device and BigFix WebUI
- Zebra Device Diagnostics and RxLogger apps installed on the device

Accessing RxLogger for Diagnostic Troubleshooting

1. Log in to the device BigFix WebUI.
2. Take device control via [remote access](#) using BigFix MCM.
3. Open the BigFix MCM console.
4. Locate the target device in the device inventory.
5. Initiate a remote session to the device.
6. On the device, open the application drawer. Launch the Zebra Device Diagnostics app. Within the diagnostics app, open RxLogger to access detailed system, kernel, and network logs. Export or view log files as needed to diagnose connectivity, application crashes, or enrollment failures.

Monitoring Battery and Wi-Fi Health Metrics

The Zebra Device Diagnostics app provides real-time monitoring of battery and Wi-Fi health. Administrators can review these metrics remotely to assess device performance and preemptively address potential issues.

Exporting and Reviewing Logs

In RxLogger, select the desired log files (system, kernel, network, etc.). Choose the export option to save logs locally or upload them to a designated server for further analysis. Review the exported logs to identify and resolve issues such as connectivity failures, application crashes, or device enrollment problems.

Best Practices

- Regularly monitor device health metrics to detect issues early.
- Use remote access tools like BigFix MCM to minimize physical device handling.
- Maintain up-to-date versions of the Zebra Device Diagnostics and RxLogger apps.
- Securely store and manage exported log files for compliance and troubleshooting history.

Chapter 6. Unenrol

Learn how to unenroll devices configured via StageNow barcode by performing an Enterprise or Factory Reset using a profile generated with Zebra StageNow PowerManager CSP. For devices enrolled through standard Android Enterprise methods, initiate the Unenroll action from the BigFix WebUI.

- **Barcode Enrollment:** To unenroll devices configured via StageNow barcode, create and scan an Enterprise Reset or Factory Reset profile generated using Zebra StageNow PowerManager (PowerMgr) CSP. For more information, refer to <https://techdocs.zebra.com/stagenow/5-10/csp/power/>
- **Standard Android Enterprise (QR Code / Zero-Touch):** To unenroll devices enrolled via standard Android Enterprise methods, initiate an [Unenroll action](#) directly from the BigFix WebUI.