Enterprise Reset

How to preserve secure Launcher/Kiosk lockdown settings following an Enterprise Reset

OVERVIEW

This document explains how to preserve settings following an Enterprise Reset on a persistence-enabled device that implements a secure Android launcher and/or its Kiosk Mode feature deployed using the Zebra StageNow administration tool or an enterprise mobile management (EMM) system. This document covers the VMware AirWatch EMM.

This process addresses configuration conflicts that exist between the Persistence Manager CSP and the Android Setup Wizard (SUW, also known as the "Welcome Screen") when attempting to restore settings of a secured device after it has been reset. To avoid these conflicts and restore the device to its original secure state, Zebra recommends the use of the "Setup Wizard Bypass" parameter of the Power Manager CSP.

ZEBRA STAGENOW

When creating a persistent profile that includes an Enterprise Reset, use PowerMgr to set the "Bypass GMS Welcome Screen" parameter to True, as shown below. This will cause the Android Setup Wizard to be skipped when the device restarts following the reset.

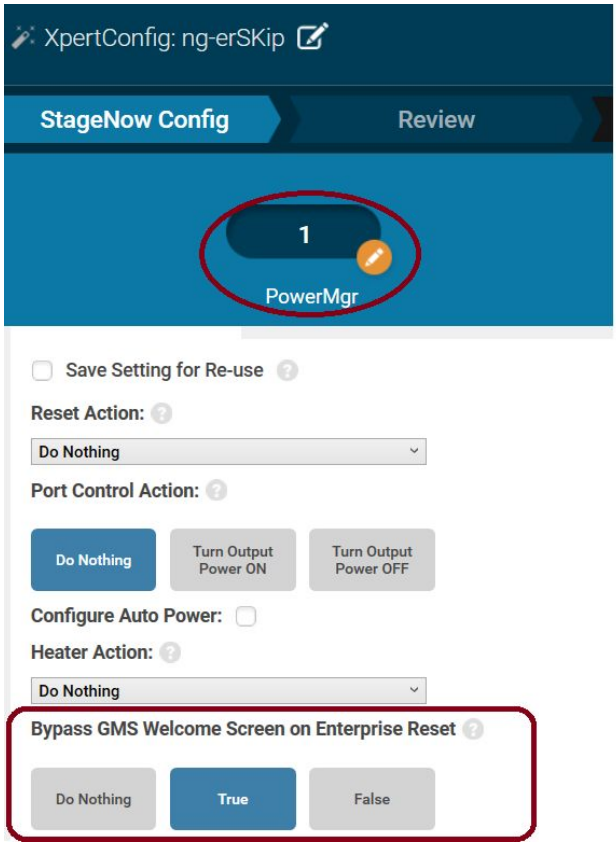

FIgure 1: *Zebra StageNow tool showing Power Manager's Bypass Setup Wizard parameter.*

NOTE: The bypass setting does not persist on the device following an Enterprise Reset. If SUW bypass is desired following an Enterprise Reset, the setting (bypass=true) must be included in the same Profile that is used to initiate the Enterprise Reset. **Note: The bypass flag was intended to be available as an option ONLY when Enterprise Reset is selected. However,** MX 7.1 and 7.2 allow SUW bypass to be configurable regardless of the Enterprise Reset parameter setting. Once pushed to such devices, a bypass flag value of "true" will persist until an Enterprise Reset is executed or the flag is changed to "false" by a subsequent profile.

VMWARE AIRWATCH

This section covers the specific procedures for using AirWatch to restore EHS and/or Kiosk Mode security settings on a device following an Enterprise Reset.

IMPORTANT:

- **For restoration of *any* enterprise settings to be possible**, the device must have been configured with the Zebra persistence framework in advance of the Enterprise Reset reset action. This is generally done during the initial device enrollment process.
- **Enterprise settings also can be preserved** immediately prior to an Enterprise Reset by using the fault tolerance settings of the AirWatch console. **Zebra recommends that AirWatch customers execute Enterprise Reset in this manner.** The state of such devices will be returned to their enrolled state in the EMM system (restoring the AirWatch Agent and Service) without intervention only if the device was originally enrolled using a barcode or sideload methodology.
- **Devices originally enrolled manually** (by typing EMM server name and user credentials) cannot be returned to their enrolled state without further intervention.
- **An Enterprise Reset will restore the latest Agent and Service** only if the upgrade was performed through the Files/Action -> MDM Agent Upgrade method.

Enterprise Reset

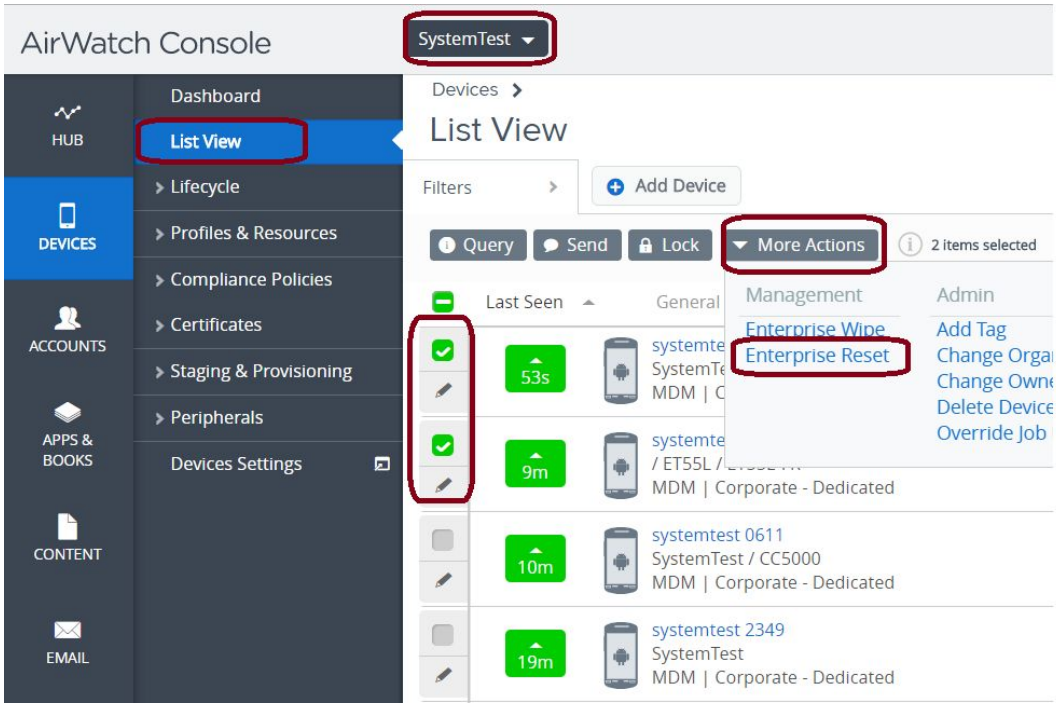

FIgure 2: *The AirWatch Command Console, showing settings for executing an Enterprise Reset on multiple (checked) devices.*

AIRWATCH NOTES

- Devices available for selection in List View varies by the group-filtering settings of an organization.
- Enterprise Reset can be selected for execution on more than one device at a time.
- The AirWatch agent will not execute an Enterprise Reset command on any device with a battery charge less than 50%.
- If an Enterprise Reset is sent to a device while it is being charged, the reset action will be executed when the battery charge level reaches 50%.
- AirWatch does not support persistence on devices in Android enterprise work-managed device mode.