Enterprise Home Screen 4.0
Release Notes – June, 2020

Highlights

- **Android 10 Support** – EHS 4.0 now supports Zebra devices running Android 10
- **Configurable display of** Recent Apps and Wireless Info to User

Device Support

- **Newly added device support in this release**: TC21, MC33x, PS20, TC26, TC52 running Android 10
- **Device support dropped with this release**: None

See **all supported devices**

New in Enterprise Home Screen 4.0

User Access to Recent Apps Now Configurable

EHS 4.0 introduces an option to allow or block access by the device User to the list of apps recently launched by User (blocked by default). Visit **TechDocs** for details.

Ability to Select Wireless info Viewable by User

EHS 4.0 can optionally suppress the display of IP address, BSSID, MAC address and other sensitive wireless network information while in User mode. Administrators can now configure which wireless information is displayed for User (all sensitive info blocked by default). Visit **TechDocs** for details.

Resolved Issues

- None

Usage Notes

- To preserve an application's state when returning it to the foreground, the Recent Applications feature must be enabled.

Known Issues

- When EHS is running in Google Multi-User mode on Android 10 devices, app icons are sometimes not shown on secondary user's home screen while switching back and forth between primary and secondary users.
- When auto-launching two or more apps at startup on Android 10 devices, the feature might work improperly when a delay longer than two (2) seconds is set between launching the apps.

- The Camera and Google Search apps are not visible in User mode after rebooting the device with Android Multi-user mode enabled.

Important Links

- Installation and setup instructions
- See all supported devices

About Enterprise Home Screen

Enterprise Home Screen for Android provides a simple way for administrators to control access to apps and settings on a Zebra device without the need to write custom code. Using a simple touch interface, EHS easily limits usage to one or more specified applications, prevents changes to device settings and locks down the file system. It can be configured in seconds, and settings can be deployed via MDM. EHS settings are stored in a simple XML file that's easy to read and edit by hand, if necessary.