altOS Device Software Release 10.1.0

Operating System Version 10.1.0 Final Release Notes

BASED ON ANDROID 10.0

Build numbers:

- Pixel 3a: 1615150713
- Pixel 3a XL: 1615173550
- Pixel 4a: 1615152863

Summary Release Notes

altOS Device version 10.1.0 requires altOS Server version 6.1.0

Security patches

May 5, 2020 AOSP security patch implemented

New features/functions

- Security Enhancements were added to reduce exposure to common vulnerabilities.
- Remove hard coded recovery password from client, now enabled using policy specified value to recover a container password.
- Enable additional permission checks for whitelisted apps
- Add package "com.atakmap.app" to the whitelisted apps list

Bug Fixes

- Resolved: Unable to turn ON airplane mode while Secure Mode is enabled.
- Resolved: NFC enabled but when toggled off in secure mode, can't be toggled back on.
- Resolved: NFC/Bluetooth toggles back on when switching containers.

Detailed Release Notes

altOS Device version 10.1.0 requires altOS Server version 6.1

Some client features (Backup and Restore and Password Recovery) are dependent on altOS Server version 6.1.

Security Enhancements were added to improve the overall security of the product.

- Remove unused code and default values
- Replace remaining SHA1 usages with SHA256
- Implemented BoringSSL random number generator in place of java.util.random
- Removed temporary file creation vulnerability ref: https://jira.sonarsource.com/browse/RSPEC-2976
- Remove external storage permissions from apps that don't use external storage
- Remove backup ability for altOS apps

Remove hard coded recovery password from client, use policy specified value to recover a container password.

- The recovery password or recovery pin specified on the policy is now used to recover the container on the device. Previously hard code values ('0000' or ‘aaaa’) were used.

Enable additional permission checks for whitelisted apps

- Whitelisted apps can now use “getCurrentUser” and “ACTION_USER_SWITCHED”.

Add package "com.atakmap.app" to the whitelisted apps list.

- Whitelisted apps now also have system permissions.

Known Issues:

- Emergency calls allowed when in Secure Mode – currently when the device is switched into Secure Mode, a device user could still place an emergency call (e.g. a 911 call). This may be undesirable for certain use cases as the device would re-connect to the cellular network even if cellular network access was disabled in the Secure Mode profile.
- Wi-Fi hotspot captive portal screen is not displayed if mobile data enabled.
- altOS menu item sometimes does not show in Settings menu on first time invocation (after first boot or factory reset). Workaround: dismiss the Settings view if the menu option is not shown, selecting Settings again, should show the menu option.
- Provisioning a regular container with no password set will fail.
  Workaround: set a password (or PIN) on the invitation, when provisioning the container.
- Bluetooth disconnected in hidden container after sleep timeout and screen locked.
- Cannot install Play Store app in a hidden or regular container if the Play Store is disabled in the Primary container.
- Cannot provision additional containers to a device when the device has not restored a container backup.
- Encrypted apps and files are not installed with local policy update files.
- Processing an online Policy Push command will fail after a local policy update file has been applied
- Notification for space with CSN=HIDE not hidden in other space if pill selected
- “OTA Automatic check for updates” is enabled even when set to off in policy
- Bluetooth enabled in non owner space but does not see available devices.
  Workaround: Pair the device while in the primary container.