Overview

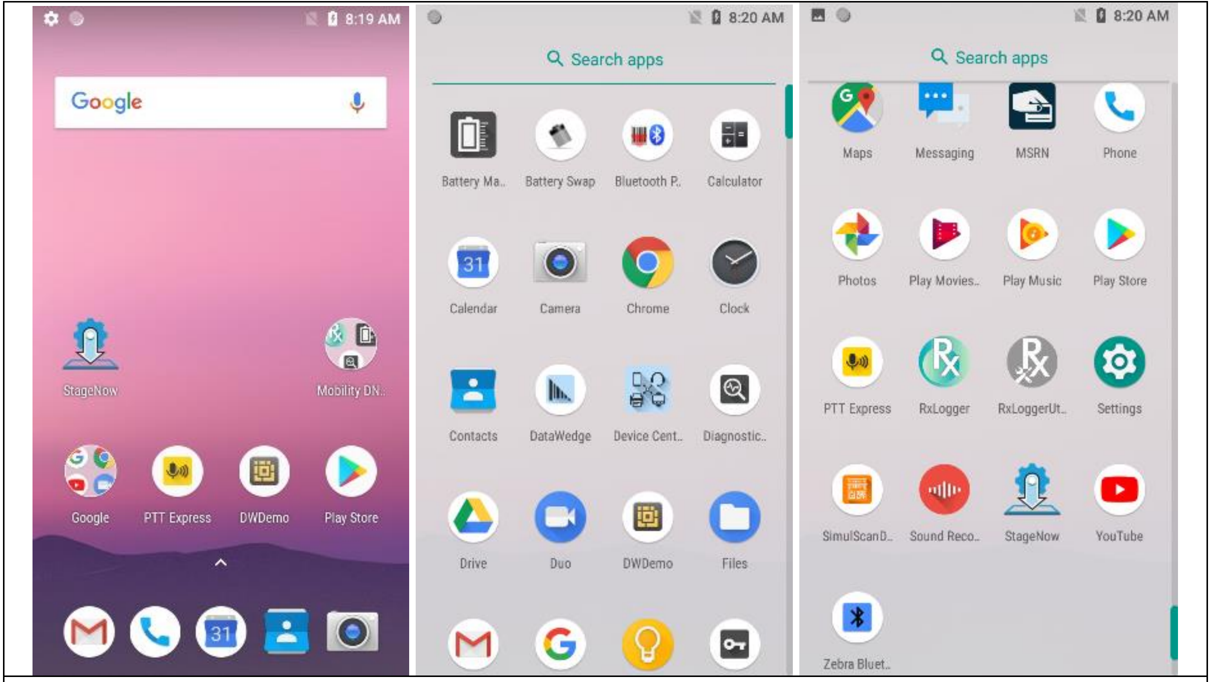
Zebra's GMS Restricted is a device state that provides complete control over which GMS applications and services are available on a Zebra device. Activating this state disables all Google applications and services that are part of Google Mobile Services, providing improved control over data privacy.

In practice, this means that many applications on a GMS Restricted device are disabled, including Google Chrome, the Play Store app, YouTube, Gmail, Google Maps, Photos, etc. Any applications that depend on Google Play Services in any way can no longer rely on those Play Services being available; Play Services cover a range of functionality, with the most commonly used in enterprise being location, safetynet, maps and Firebase cloud messaging.

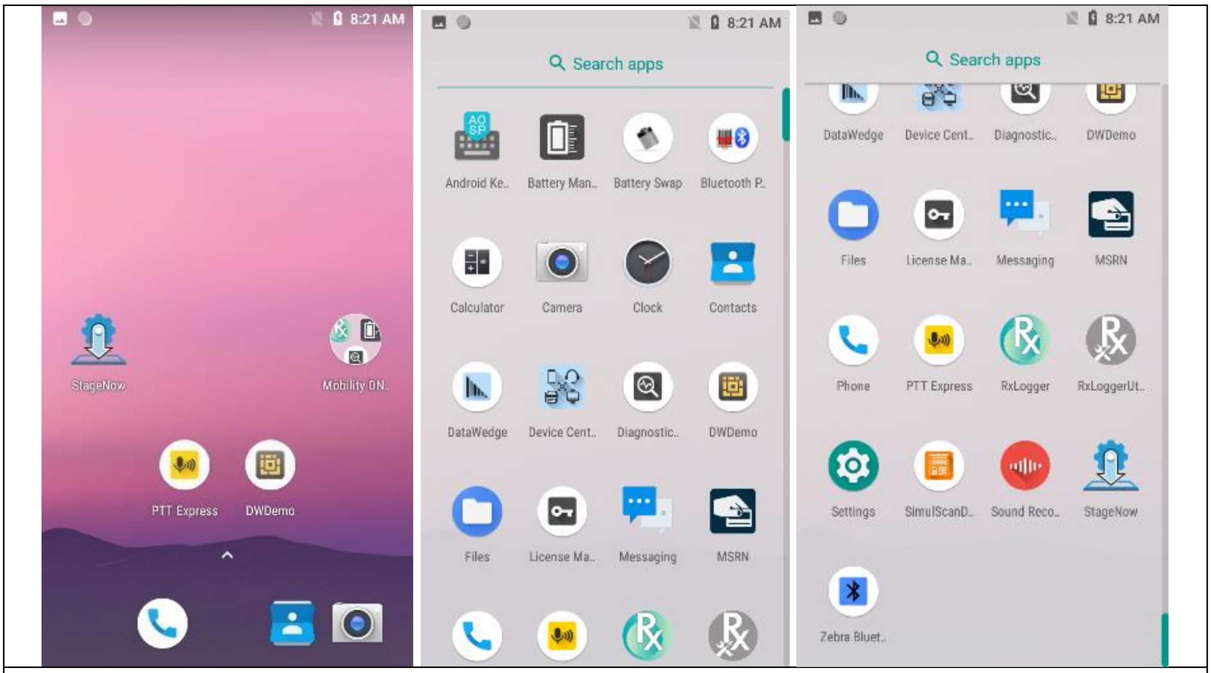
Important Notes:

- When location services are disabled, the device is set to "Device Only" location mode when in a restricted state.
- Zebra make no guarantees that third-party applications from the Play Store will run under GMS Restricted since the dependencies of these applications on Play Services are unknown.
- Firebase Cloud Messaging (FCM) is used by many third-party applications to provide on-demand notification delivery. Applications that use FCM no longer receive cloud messages through this framework when GMS Restricted is in effect.
- The ability to add or manage users on a device is prevented by GMS Restricted; any existing Google accounts are disabled.

In exchange for the absence of Google applications and services, a GMS Restricted device cannot communicate with Google servers for any purpose. This can help alleviate privacy concerns, reduce network bandwidth, and to a lesser degree help reduce the device memory footprint.



Example device experience out of the box



Example device experience after applying GMS Restricted

A device in the GMS Restricted state enforces no limitations on non-GMS applications. Since not all GMS applications are mandatory, the GMS apps on a Zebra device might differ from a consumer smartphone to best suit enterprise use cases. A GMS Restricted device is **still able to**:

- Run applications that are not part of GMS (on the condition that they do not have dependencies on GMS components).
- Run third party applications (on the condition that they do not have dependencies on GMS components).
- Run Zebra value-add applications built into the device
- Run Zebra value-add applications that are post-loaded onto the device (for example, Enterprise Browser)
- Make and receive phone calls
- Use a WAN data connection
- Send Zebra analytics (unless disabled) or analytics for third-party applications

Entering GMS Restricted

GMS Restricted is a configuration setting applied to a GMS device; it is not a separate product.

To activate GMS Restricted on a device using Zebra StageNow:

CSP	Action	Description	Applies to
App Manager	DisableGMSApps	Disables all GMS applications and services on a device that are "safe to disable." For example the Play Store app, YouTube, Gmail, Google Maps, Photos, Chrome and Play Services.	OSX: 8.1+ MX: 8.0+ Android API: 24+ SDM-660 platform devices only

		A device with this setting applied cannot communicate with Google servers, helping to alleviate privacy concerns for some customers. Subsequent calls to the EnableApplication Action are effective.	
App Manager	EnableGMSApps	Enables all GMS applications and services on a GMS device. This action undoes the effects caused by the DisableGMSApps Action and returns the device to the standard configuration. This setting ignores any previous calls to EnableApplication or DisableApplication Actions; subsequent Actions are effective.	OSX: 8.1+ MX: 8.0+ Android API: 24+ SDM-660 platform devices only

The DisableGMSApps action acts immediately to disable all GMS packages deemed safe to disable. When a device is in this state:

- No GMS packages are able run or communicate with Google servers including (but not limited to) the following apps:
  - The Play Store
  - Chrome
  - YouTube
  - Search
  - Gmail
  - Play Music
  - Google Drive
  - Google Maps
  - Google Play Movies
  - Google Photos
  - Hangouts
    - The list of GMS apps can vary from one Android version to another
    - This includes (but is not limited to) the following services:
      - Enhanced location (high-accuracy or battery saving that depends on nearby Wi-Fi access points)
      - Google Play Services
      - Google's Play Protect
      - Creating unmanaged Google accounts
    - Because enhanced location is not available, the only way for a device to determine its position is through GPS (if it has the appropriate hardware) or through off-device RTLS technologies.
- Neither built-in applications nor the platform itself can exchange diagnostic data, analytics data or location information with Google.
- Applications that depend on GMS packages or applications have reduced functionality, notably any application that depends on Google Play Services.
  - Some examples of use cases that are not available on a GMS Restricted device:
    - Applications that use the Google Maps component must find an alternative.
    - Applications that verify the integrity of the device might use the attestation API.
- The device keyboard is handled as a special case. When GMS Restricted is applied, the GMS keyboard is disabled and the keyboard from the Android Open Source project is automatically enabled. Administrators are free to replace this open source keyboard with Zebra's own Enterprise Keyboard if it better suits their deployment.
- Having a secondary or guest user on the device is not compatible with GMS Restricted; only the primary user is supported. In most instances the user is prevented from creating secondary users when the device is in the GMS Restricted state. Although a Device Owner is

still technically capable of creating additional users on a device in the GMS Restricted state, **Zebra strongly discourages this practice because GMS Restricted is not in effect for those additional users**.

When to Apply

If GMS Restricted state is to be used, Zebra strongly recommends that it be employed as soon as possible after device boot and before establishing a Wi-Fi connection. Before the GMS Restricted Action is applied, the device can communicate with Google, potentially allowing data to "escape." This can be achieved in StageNow by applying the GMS Restricted Action as one of the first steps in the initial staging profile.

- Set-up wizard bypass barcode is scanned, and automatically launches the StageNow client on the device. This is not required for GMS Restricted but is common to many workflows.
- A staging profile is scanned and performs the following actions:
  1. GMS Restricted is applied using the DisableGMSApps Action of App Manager CSP
  2. The Power Manager's "Setup Wizard Bypass" action is set to "true." This step is required if persisting the configuration following an Enterprise Reset.
  3. Perform additional staging actions, such as configuring the Wi-Fi network.

If a deployment uses a SIM card that can access a public APN, Zebra recommends that this SIM card be installed after the device is put into a GMS Restricted state to prevent data from leaving the device.

Moving from AOSP to GMS Restricted

The following applications are present on non-GMS (AOSP) devices but do not have an out-of-box equivalent on a GMS-Restricted device:

- Browser
- Email
- Gallery
- Calendar
- Music
- Search

Applications should not be re-enabled piecemeal in this release. Alternative third-party applications could be deployed to re-enable any missing capabilities, although Zebra does not make any recommendations on which alternative applications to use.

Doze mode is disabled on devices in the GMS Restricted state. This matches the behaviour of non-GMS (AOSP) devices, which do not have doze mode enabled.

Line-of-business or third-party applications that ran on AOSP devices continue to run on devices in the GMS Restricted state. However, third-party applications often make use of Google Play Services to provide core functionality, so be sure to thoroughly test any application not specifically designed to run on non-GMS (AOSP) devices before deployment to a device in GMS Restricted.

Although the Play Store is not available on a GMS-Restricted device, any of the techniques for distributing applications that work for non-GMS devices also work to distribute applications to GMS-Restricted devices. The most popular technique is to use the StageNow AppManager CSP to install and upgrade applications. Side-loading apps also is an option, but side-loading of GMS applications is not supported or allowed under the terms of conditions of those apps.

How does it work?

GMS Restricted works at the application level, not the network level. This means that although no GMS packages on the device can communicate externally, non-GMS applications such as a third-party web browsers are not prevented from communicating with www.google.com, for example.

Persisting GMS Restricted

Device Reboot and OS Update

GMS Restricted persists across a device reboot or OS update and no special action is taken during an OS Update. This means that any GMS applications present in the new OS update not present before will **not** be disabled unless and until the “DisableGMSApps” App Manager Action is invoked again. This is because the list of GMS packages that can be safely disabled might vary before and after an OS Update. Therefore, ***Zebra recommends invoking the "EnableGMSApps" prior to an OS update to exit GMS Restricted state and re-entering GMS Restricted state (by invoking “DisableGMSASpps”) afterward, if desired*.**

Enterprise Reset

To enable persistence following an Enterprise Reset, it is necessary to use the Persistence Manager, set the Power Manager’s ‘Setup Wizard Bypass’ action to “true,” and initiate the Enterprise Reset via the Power Manager. This prevents the setup wizard from being displayed while GMS Restricted is being applied following the reset.

Factory Reset

It is not possible to persist the GMS Restricted state following a Factory Reset.