Zero-Touch Enrollment

Android 8.0 and higher includes the capability for a device running Google Mobile Services (GMS) to support **zero-touch enrollment**, which enables Enterprise customers to automatically provision devices they own with no user action required to initiate the process.

Enterprise setup occurs automatically in Setup Wizard: On first boot, devices check to see if they have been assigned to an Enterprise. If so, the device initiates the Device Owner provisioning method and downloads the correct Device Policy Client app, which then completes setup of the managed device.

Zero-touch enrollment workflow

To configure a device with zero-touch enrollment, the Enterprise is allocated a set of devices by the sales channel that supplies the Enterprise. The process begins with the Manufacturer, who creates a set of device identifiers (IMEI or Serial number) and passes that to the Reseller, who uploads a mapping of the device identifiers to a customer, who finally configures the correct provisioning parameters for the allocated devices.

The following steps occur during the provisioning of a zero-touch enrollment device:

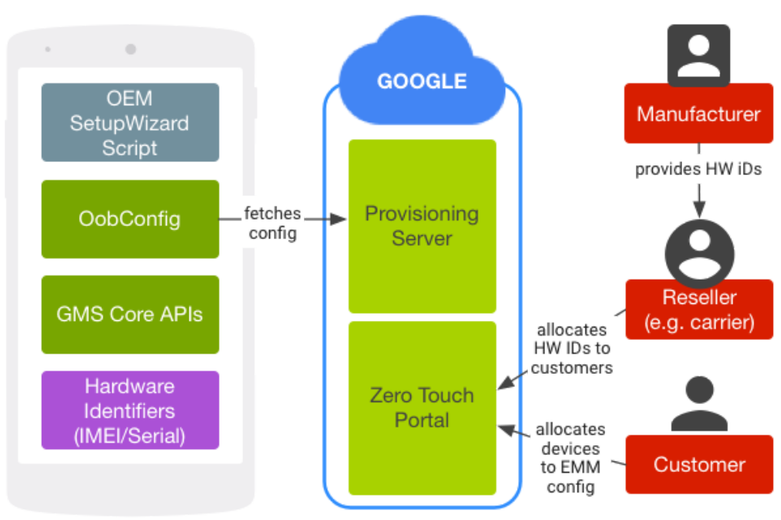

Figure 1. Zero-touch enrollment workflow

1. Manufacturer produces a set of devices correctly configured to perform zero-touch enrollment.
2. Manufacturer allocates a batch of these devices to a reseller (e.g., a carrier). The manufacturer must provide the hardware identifiers in a way that allows a reseller to know the hardware identifiers for each device in their inventory.
3. Reseller creates a Customer account for the customer on the zero-touch enrollment portal.
4. Reseller sells batches of devices to a customer. Using the zero-touch enrollment portal or reseller APIs, reseller allocates those devices (using the hardware identifiers) to the customer.
5. Customer uses the zero-touch enrollment portal to allocate an EMM configuration to each device. This creates a Device Provisioning Record (DPR) within the Google Provisioning Server.
6. Device turns on for the first time and checks with the Google Provisioning Server to see if the device has a DPR:
   a. If a DPR exists, the Google Provisioning server sends it to the device, which uses the record to initiate Managed Provisioning with the specified configuration values.
   b. If no DPR exists, setup continues normally without latency (there is no additional cost in setup time in the typical consumer case).

   If a device cannot check-in with Google servers as part of the normal SetupWizard flow, the device maintains a flag that indicates it should check-in when network connectivity becomes available. If during the subsequent check-in a device is configured as zero-touch, it notifies the user and initiates a factory reset after two hours. Until the subsequent check-in, the ability to OEM unlock the device (*Settings > Developer*) is not available but the device is otherwise usable.

Implementing zero-touch enrollment

The following on- and off-device components are required to deliver zero-touch enrollment.

On Device	Off Device
• Implement valid unique hardware identifiers • Implement relevant Android framework APIs (Android 8.0 or higher) • Preload relevant Google APKs • Configure the framework • Ensure the bootloader cannot be unlocked prior to zero-touch enrollment check • Add zero-touch enrollment SetupWizard steps • Declare the zero-touch enrollment feature • Request whitelisting (cellular devices and/or Wi-Fi-only devices)	• Manufacturer transmits hardware identifiers to resellers • Reseller uses zero-touch enrollment portal to map devices to customers • Customer uses zero-touch enrollment portal to map allocated devices to correct EMM configurations • Request that Google whitelist the manufacturer for zero-touch enrollment

The following sections detail the required on-device components. Documentation for off-device components (e.g., reseller and customer portals) will be supplied to those parties and is not provided here.

Meeting hardware ID, API, and APK requirements

The following components are required to enable zero-touch enrollment:

Component	Description
Valid Hardware Identifiers	• Each device that implements zero-touch enrollment must have a unique serial number for a given Manufacturer and Model pair (as per the Compatibility Definition Document/CDD) and a globally unique IMEI/MEID if the device supports telephony. • Google Provisioning uses and validates the MANUFACTURER value reported by the device during check-in. **Manufacturers must share the `MANUFACTURER` value they intend to use prior to any integration testing**. • Devices are uniquely identified by resellers through these identifiers. If a reseller creates a DPR for a particular identifier, any device that has this identifier and implements zero-touch enrollment will be provisioned in zero-touch enrollment mode using this DPR.

Android Framework APIs	The device factory image must be Android 8.0 or higher.
Preloaded Google APKs	The device system image must include `OobConfig.apk` (provided in the preview GMS bundle for 8.0 and higher). In addition, zero-touch enrollment relies on GMS Core APIs and can be used only on devices running GMS.

Configuring the framework

In the device-specific overlay for `frameworks/base/core/res/res/values/config.xml`, ensure the OOB provisioning package is set:

```
<!-- Package name for the device provisioning package. -->
    <string
name="config_deviceProvisioningPackage">com.google.android.apps.work.oobconfig</string>
```

Configuring the bootloader

To ensure devices that have been allocated a DPR can actually retrieve that record, manufacturers should configure the bootloader so that it cannot be unlocked until the device has successfully checked-in. To do so, ensure the bootloader cannot be unlocked until `OemLockManager#isOemUnlockAllowedByUser` and `OemLockManager#isOemUnlockAllowedByCarrier()` return `true`.

Configuring the Setup Wizard

When you are customizing the Google Setup Wizard (SUW) flow (e.g. adding additional steps), apply the following steps to customize your script to call the Zero Touch action:

Note: If you are not customizing the Google SUW, you do not need to make any modifications (skip this section).

1. In your Setup Wizard Wizard Script customization package, add an XML file such as `partner_gms/apps/GmsSampleIntegration/res/raw/wizard_script_zero_touch_flow.xml` (found in the 8.0 and higher GMS bundles). This script calls Google components in the correct order and should not be customized.
2. In your main Wizard Script, add a reference to the script in the customization package:

```
<WizardAction id="zero_touch"
 wizard:script="LOCATION_OF_CUSTOMIZATION_PACKAGE_SCRIPT">
 <result wizard:name="dpm_user_complete" wizard:resultCode="111" />
</WizardAction>
```

3. Set the `zero_touch` action to be triggered as soon as the device has network connectivity and performs a Google check-in:

```
<WizardAction id="ACTION_THAT_ESTABLISHES_NETWORK_CONNECTIVITY"
 wizard:uri="ACTIVITY">
    <result wizard:action="gms_checkin" />
</WizardAction>

<WizardAction id="gms_checkin"
 wizard:uri="intent:#Intent;action=com.google.android.setupwizard.GMS_CHECKIN;end">
    <result wizard:action="zero_touch" />
</WizardAction>
```

If network connectivity is skipped entirely, then zero-touch does not need to run.

In Android 8.0 and higher, the `WizardAction` (in step 2 above) can be added directly beneath the step that does the Google check-in, and the next action will be set implicitly.

Declaring the zero-touch feature flag

To allow customers and resellers to easily identify devices that support zero-touch enrollment (and to facilitate GTS testing), manufacturers should declare the `com.google.android.feature.ZERO_TOUCH` feature in all builds supporting zero-touch enrollment.

Requesting whitelisting for cellular devices

For a specific manufacturer's device to be able to use zero-touch enrollment, Google must whitelist the Build.MANUFACTURER value that will be returned by devices. To whitelist devices with cellular radio, contact your Google Technical Account Manager (TAM).

Requesting whitelisting for Wi-Fi devices

For Wi-Fi-only devices (such as tablets), zero-touch enrollment uses a combination of the device's serial number and model instead of a cellular modem ID. To register new models for whitelisting, complete the Zero-touch OEM Whitelisting Form. Google will privately whitelist the new models until you inform Google that those models are launched, at which point Google will add those models to the public list of public list of manufacturer names and models. To report issues, contact your Google TAM.

Testing zero-touch enrollment

To confirm zero-touch is working, confirm the device `logcat` contains the following line immediately after boot:

```
08-31 22:22:20.856 10038 7546 8240 I OobConfig: zeroTouchConfig set: false,
simLockConfig set: false, disallowOemUnlock restriction set: false
```

The appearance of any line matching this format (regardless of the value of the `zeroTouchConfig`, `simLockConfig`, or `disallowOemUnlock` fields) indicates the zero-touch code is being called.

To test zero-touch enrollment end-to-end, manufacturers can provide a small list (up to 50) of device identifiers to Google, who will map the IDs to a test customer DPR that installs TestDPC onto the devices. To request devices to be setup for testing, use the Zero Touch Device Provisioning Request form.

Implementation recommendations

For resellers to be able to configure devices, they must be able to identify a device to Google using the hardware identifiers. Manufacturers should ensure that they provide this information to resellers in a way that enables resellers to tie the hardware identifiers to a physical device in their inventory.

Caution: Manufacturers must not change these identifiers in any way between updates of the same device.

In addition, we recommend the hardware identifiers be visible outside of the device to allow customers to identify the correct physical devices (such as checking the model, serial, etc. on the box).