

Comma

CONSOLE WALKTHROUGH

Google Workspace MDM - Admin Console Walkthrough

Every screen, click, and field to deploy the Comma Compliance
Messages Archiver to fully-managed Android devices

CONSOLE WALKTHROUGH

Google Workspace MDM - Admin Console Walkthrough

Every screen, click, and field to deploy the Comma Compliance Messages Archiver to fully-managed Android devices

About this walkthrough

This is the **click-by-click** companion to *Set Up RCS/SMS Archiving on Android with Google MDM*. It walks through the exact **Google Admin console** (admin.google.com) screens to deploy the **Comma Compliance Messages Archiver** (`com.commacompliance.archiver`) to fully-managed Android devices using **Google Workspace Endpoint Management**, **managed Google Play**, and **managed configuration** - no third-party EMM for the app itself.

It covers **all three ways a device enrolls with Comma**, because they suit different rollouts:

- **Shared fleet token (recommended for fleets)**. One reusable token, pushed OU-wide via managed configuration. Every phone enrolls itself with **no user interaction** and no per-device work - the lowest-touch path for company-owned fleets.
- **OAuth self-service**. No token; each employee signs in once in the app. Best when employees set up their own corporate phones.
- **Single-use device token**. A one-time token bound to one phone - for enrolling devices one at a time.

Parts 1-5 are the **same for every path**. They differ only at Part 6 (the managed configuration you push) and Part 7 (the on-device step).

Navigation in this guide is written as breadcrumbs you follow in the Admin console, e.g. **Menu -> Apps -> Web and mobile apps**. Google occasionally renames a label or moves a control; where that happens, the surrounding screen description should still let you find it.

WHAT YOU NEED BEFORE YOU START

- **Edition:** a Google Workspace edition that supports **advanced mobile management** and company-owned inventory (Business Plus, Enterprise, Education Standard/Plus, or Cloud Identity Premium).
- **Admin privileges:** *Mobile Device Management* (for app + managed config), and *Services and devices* (for company-owned inventory).
- **Comma web-app prerequisites done:** an admin has enabled **Android RCS+SMS capture** for the team (see the overview guide). The **Default backfill window** only updates already-connected devices, so for new managed devices set per-device **backfill_days** in Part 6.
- **Token paths only:** if you'll use a **shared fleet token** (recommended) or a **single-use device token**, generate it in the Comma web app first (**Account -> your team -> Android RCS+SMS capture**). The token is shown once. OAuth self-service teams skip this.

Values you'll enter

Keep these handy - you'll type them into the managed-configuration screen.

Field	Value
backend_url	https://app.commacompliance.com (your backend; must be https)
enroll- ment_token	Your token from Comma (<code>amenr_...</code>) - a shared fleet token (reusable) or a single-use device token . Token paths only; omit for OAuth self-service
backfill_days	90 (or 0 for forward-only)
Archiver app pack- age	<code>com.commacompliance.archiver</code>
Google Messages package	<code>com.google.android.apps.messaging</code>
Google Messages key	<code>messages_archival = com.commacompliance.archiver</code>

Part 1 - Turn on advanced mobile management

App management and managed configuration require **advanced** mobile management (the default "basic" tier can't push apps or config).

1. Go to **Menu -> Devices -> Mobile & endpoints -> Settings -> Universal**.
2. Click **General -> Mobile management**.
3. Select **Advanced**.
4. Click **Save**.

PER ORGANIZATIONAL UNIT

You can apply Advanced management to a specific organizational unit (OU) . Put the users whose devices you'll manage into that OU, and select it on the left before saving.

Part 2 - Add devices to the company-owned inventory

Adding a device's serial number to the company-owned inventory makes it enroll as **fully managed (device owner)** during setup - which is the mode the archiver requires. (Work-profile / BYOD devices are not supported.)

1. Go to **Menu -> Devices -> Mobile & endpoints -> Company-owned inventory**.
2. At the top, click **Import company owned devices**.
3. Choose the device type (**Android**) and click **Download import template**.
4. In the template, enter each device's **serial number** (and optional asset tag); Android also accepts IMEI. One device per line.
5. Upload the completed file to import. Devices appear in the inventory.

When one of these devices is **new or factory-reset**, it automatically enters **fully managed** mode during the on-device setup (Part 7) - no work profile is offered.

Part 3 - Add and approve the archiver app

Comma makes the archiver available to your enterprise's managed Google Play; you then approve it. (The same app is also on the **public Play Store** at <https://play.google.com/store/apps/details?>

`id=com.commacompliance.archiver` - useful for one-off installs, but for a managed fleet bring it in through the console as below.)

1. Go to **Menu -> Apps -> Web and mobile apps**.
2. Click **Add app -> Search for apps**.
3. Search for **Comma Compliance Messages Archiver** and click **Select**. *(If it doesn't appear, contact Comma at contact@commacompliance.com to have it targeted to your organization's managed Google Play.)*
4. When prompted, choose who can access it - **Select organizational units** (or **Select groups**) and pick the OU from Part 1 - then click **Continue / Done**.

Once approved for your organization, the app is usually ready within about 10 minutes.

Part 4 - Force-install the app to your devices

1. Still in **Web and mobile apps**, click the **Comma Compliance Messages Archiver** row to open its detail page.
2. Click **User access**. In the left sidebar, click the **OU (or group)** that holds your managed devices, set user access to **On**, and click **Save**.
3. Open the app's **Settings**. Find **Access method** and choose **Force install** (this auto-installs the app on managed devices, versus *Available*, where users install it themselves).
4. Select the checkbox to **prevent users from uninstalling a force-installed app** so the archiver can't be removed. Click **Save**. (You'll apply the same protection to Google Messages in Part 5 - capture needs **both** apps protected.)

Part 5 - Wire Google Messages to the archiver

Google Messages must be told which app to wake on each message. That's the `messages_archival` key on the Google Messages app, and it is **required for every connection path**.

1. Add **Google Messages** (`com.google.android.apps.messaging`) in **Web and mobile apps** the same way as Part 3, and force-install it (Part 4) so the OU runs a current build - and select the **prevent users from uninstalling** checkbox for it too. *An out-of-date Google Messages build captures nothing, and capture breaks if a user disables, force-stops, or clears **either** the archiver or Google Messages - so both packages must be protected from user control.*
2. Open Google Messages -> **Managed configurations -> Add managed configuration**, and set:
 - `messages_archival` = `com.commacompliance.archiver`

3. Assign the configuration to the same OU (open Google Messages -> **Settings**, select the OU, pick the configuration in the **Managed configuration** dropdown, and **Save**).

IMPORTANT LIMITATION - THE ADMIN CONSOLE MAY NOT ACCEPT THIS KEY

The Admin console's managed-configuration form only shows the keys an app publishes in its schema. `messages_archival` is an undocumented key that Google Messages does not publish, so it will likely not appear in the form (and if Google Messages exposes no managed configuration at all, the option won't be available). This key is required : without it, capture does not work as supported - the archiver and device are otherwise ready, but capture depends on this key (it is not only about real-time wake-up). If the console won't let you set it:

- Deliver it through an EMM that supports **raw key/value** managed configuration (Microsoft Intune, VMware Workspace ONE) or the **Android Management API**, while keeping everything else in this guide as-is, **or**
- Contact Comma (contact@commacompliance.com) - capture depends on this key.

Part 6 - Connect devices to Comma: choose your path

Everything up to here is identical for every device. Now choose how each device enrolls with your Comma backend. **Most fleets use a shared fleet token (6A)** for a zero-touch rollout; OAuth self-service (6B) suits employee-provisioned phones, and a single-use device token (6C) is for enrolling devices one at a time.

6A - Shared fleet token (recommended)

One reusable token enrolls your whole OU - no per-device work and no user sign-in.

1. In the Comma web app (**Account -> your team -> Android RCS+SMS capture**), generate a **shared fleet token**. Optionally set a **seat cap** (max devices) and an **expiry** of 1-90 days (default 7). Copy the token when it appears - it is shown once.
2. On the **Comma Compliance Messages Archiver** detail page, click **Managed configurations -> Add managed configuration**.
3. Enter a **configuration name** (e.g. `Comma archiver - fleet`) and fill in:
 - **backend_url** = `https://app.commacompliance.com`
 - **enrollment_token** = your shared fleet token (`amenr_...`)
 - **backfill_days** = `90` (optional; `0` = forward-only)
4. Click **Save**.

5. Assign it: open the app's **Settings**, select the **OU/group** that holds your managed devices, then in the **Managed configuration** dropdown pick the configuration you just created, and click **Save**.

Because the fleet token is reusable, the **same configuration enrolls every device in the OU** - each phone enrolls itself on first run and claims a seat. You manage devices from the roster in the Comma web app, and can revoke any single device or rotate/revoke the token to stop new enrollments.

MAKE IT FULLY UNATTENDED: PRE-GRANT THE SMS PERMISSION

On fully-managed devices you can often pre-grant runtime permissions to a managed app. Where your console supports it, open the archiver's Settings -> Permissions (or your MDM's app permission policy) and set the SMS / message-access permission to Grant for the archiver. Verify it on a test device: where supported, the user is not prompted, and with a shared fleet token the device enrolls and starts archiving with no interaction; otherwise the app asks for message access once on first launch.

6B - OAuth self-service

No token - one managed configuration covers your whole OU, and each employee signs in once on the device (Part 7).

1. On the **Comma Compliance Messages Archiver** detail page, click **Managed configurations** -> **Add managed configuration**.
2. Enter a **configuration name** (e.g. `Comma archiver - self-serve`).
3. Fill in just these fields - **leave enrollment_token empty**:
 - **backend_url** = `https://app.commacompliance.com`
 - **backfill_days** = 90 (optional; 0 = forward-only)
4. Click **Save**, then assign it OU-wide (app's **Settings** -> [OU] -> **Managed configuration** dropdown).

Because no token is involved, the **same configuration works for any number of devices** in the OU; the only per-device step is the employee's one-time sign-in.

6C - Single-use device token (one device at a time)

A single-use token binds to one phone, so this is a per-device setup.

1. Get a **single-use device token** from Comma for that phone.
2. Add a managed configuration named for the device (e.g. `Comma archiver - device 0142`) with **backend_url**, the device's **single-use enrollment_token**, and optional **backfill_days**.
3. Assign it to a **single-device OU/group** (see the warning).

MATCH THE TOKEN TYPE TO THE ASSIGNMENT

A shared fleet token is meant to go OU-wide (6A) - that's the recommended path. A single-use device token is consumed by the first device that reads it, so assign it to one device only ; if you put a single-use token on a multi-device OU, the first phone enrolls and the rest fail. When in doubt, use a shared fleet token (6A) - it's reusable across the OU and needs no per-device configuration.

Part 7 - Provision and connect the device (on-device)

Provision every device the same way; the final connect step depends on the path you chose in Part 6.

Provision (every path):

1. Power on a **new or factory-reset** device whose serial is in your company-owned inventory (Part 2).
2. Connect to Wi-Fi and sign in with the user's **managed Google Workspace account**. Because the device is in company-owned inventory, setup proceeds straight into **fully managed (device owner)** mode - no work profile is offered.
3. Let setup finish. The force-installed apps (the archiver and Google Messages) install automatically.
4. Set **Google Messages as the default SMS/RCS app** and make sure **RCS chat features** are turned on.

Then connect:

- **Shared fleet token (6A) or single-use token (6C):** no sign-in step. The app reads the token from managed configuration and **enrolls itself** on first run. If you pre-granted the SMS/message-access permission (Part 6A note), there is no prompt at all; otherwise the app asks once for message access.
- **OAuth self-service (6B):** the employee opens the **Comma Compliance Messages Archiver** app. On first launch it shows a plain-language summary of what's captured and, unless message access is already granted by device policy, asks for the **message-access (SMS) permission** - the employee grants it. They tap **Connect to your organization** - the backend URL is already supplied by the managed configuration, so there is nothing to type - and sign in when the **secure browser tab** opens (OAuth in a Chrome Custom Tab - no password is ever typed into the app), then tap **Authorize**. The device registers under that employee's own membership.

Either way, the archiver then shows the persistent notification and begins archiving (verify in Part 8).

Part 8 - Verify

1. The archiver shows a **persistent "archiving for compliance" notification** that names your organization, and the app reports it is **Connected**.
2. In the Comma web app, the device appears under **Account -> your team -> Messages Archiver devices** with an **Active** status and recent **Last seen / Last upload** times. From here you can revoke any single device, or rotate/revoke a fleet token.
3. Send a **test SMS** and a **test RCS** message; they appear in the archive under **Messages -> RCS** within a short time.

If nothing arrives: the usual causes are an out-of-date Google Messages build, a missing/mistyped `messages_archival` key (Part 5), or a device that isn't fully managed.

HOW ENROLLMENT IS SECURED

Every path is protected the same way: the device generates an Ed25519 key pair and proves possession by signing a one-time server challenge (the private key never leaves the device); the server can verify the device and app with Google Play Integrity ; each challenge is single-use and expires in about five minutes; and an admin can revoke a device immediately or rotate/revoke a token to stop new enrollments. Full background is in the overview guide.

Quick reference - every screen path

Task	Admin console path
Advanced mobile management	Devices -> Mobile & endpoints -> Settings -> Universal -> General -> Mobile management -> Advanced
Company-owned inventory	Devices -> Mobile & endpoints -> Company-owned inventory -> Import company owned devices
Add / approve app	Apps -> Web and mobile apps -> Add app -> Search for apps
Distribute to OU	Web and mobile apps -> [app] -> User access -> [OU] -> On -> Save
Force install	Web and mobile apps -> [app] -> Settings -> Access method -> Force install
Wire Google Messages	Web and mobile apps -> Google Messages -> Managed configurations -> messages_archival
Config - fleet token (recommended)	Archiver app -> Managed configurations -> backend_url + shared enrollment_token (+ backfill_days), assign OU-wide
Config - OAuth self-service	Archiver app -> Managed configurations -> backend_url (+ backfill_days), no token , assign OU-wide
Config - single-use token	Archiver app -> Managed configurations -> backend_url + per-device enrollment_token , assign to a single-device OU
Assign managed config	Web and mobile apps -> [app] -> Settings -> [OU] -> Managed configuration drop-down

QUESTIONS

Full background on all three enrollment paths is in the overview guide, Set Up RCS/SMS Archiving on Android with Google MDM . To have the app targeted to your managed Google Play, or to request enrollment tokens, email contact@commacompliance.com . Learn more at commacompliance.com.