

FAQ

Frequently Asked Questions

- [FAQ](#)

FAQ

Short answers to the questions that come up most often, collected from the manuals. Each answer names the manual with the full story.

Getting Started

In what order should I set things up?

Add the apps (*Application List*), create managed configurations for the apps that need settings (*Managed Configurations*), create the policies you need (the policy manuals), combine them into a device group (*Device Groups*), and finally create an enrollment token and enroll the devices (*Enrollment Tokens*). The *Quick Start Guide* walks through one app end to end.

I created a policy but nothing happens on the devices.

A policy does nothing on its own. It takes effect when a device group uses it and devices are enrolled in that group. See the *Device Groups* manual.

How long does it take for a change to reach the devices?

After a group is synced or a device is moved, the device picks up the new policy within about ten minutes. Commands such as reboot can also take up to ten minutes to arrive. If nothing happens after that, see [Connectivity and the KMM Client](#).

Why can't I see any Create or Edit buttons?

Your account has a viewer role (Viewer or Enterprise Viewer), which is read-only. See *User Roles* in the manual index.

What does Unspecified mean in the dropdowns?

"Do not manage this setting". The device keeps its own default behaviour. Leaving a dropdown as Unspecified is always safe.

What does the Min Android column in the policy lists mean?

The oldest Android version a device needs in order to apply everything in that policy. Each policy manual lists which settings raise it.

A popup with an announcement appeared when I logged in. What is it?

It is an alert from Kuori, for example about a breaking change. Confirm it with **Got it** or the **X**; clicking outside or pressing Escape does not close it. You can read current alerts again under **Info, Alerts** and show past ones with **Show history**.

Devices and Enrollment

How do I enroll a new device?

Three ways, all described in the *Enrollment Tokens* manual: scan the token's QR code (tap the welcome screen of a factory-reset device six times), enter `afw#setup` when the setup wizard asks for an email and then give the token, or use zero-touch enrollment for devices bought from a zero-touch reseller. Kuori usually manages the zero-touch portal. See *Zero-touch / Enrollment*.

The device shows "Wrong account" during setup.

The enrollment token has a Required Account Email and someone signed in with a different account. Sign in with exactly the required address.

A token that used to work no longer enrolls devices.

The token has either expired (it carries an **Expired** badge) or was created as **One Time Only** and has been used. Create a new token.

Why does the enrollment form only offer an initial_ name for my group?

The group contains an uploaded APK app with the Kiosk role, so devices must first pass through its automatically created initial setup group. The token is created from it, and the device moves to the actual group by itself. See the *Device Groups* and *Custom APK to Kiosk* manuals.

How do I move a device to another group?

Open the device, go to the **Actions** tab, pick the new **Device group** and select **Save**. The change waits until the device is online, and actions are locked meanwhile. An administrator can cancel a stuck change with **Lift Lock (Return to previous group)**. See the *Devices* manual.

To move several devices, tick them in the device list and select **Change group**. The result is reported per device; devices that failed stay selected so you can retry. If Google rejects the change, the console reports the error instead of success.

Applied Group Name and Configured Group Name differ. Is something wrong?

No. A group change has been started and the device has not applied it yet. Give the device time online.

What happens if I delete a device?

It is removed from management **and wiped**. Google resets it. To use it again, enroll it from scratch. Deleted devices remain findable in the device list with the **Is Deleted** filter. This is for getting a confirmation of device deletion from AMAPI and for the possible case of re-enrollment.

A device is marked non-compliant. Where do I see why?

Open the device; the **Policy Compliance** tab opens first when the device is non-compliant and lists each reported issue with the setting and reason. Common causes are an unmet policy requirement or an app that failed to install.

Reboot seems to do nothing.

Reboot works only on fully managed devices running Android 7.0 or newer, and the command can take up to ten minutes to reach the device.

Where did the Hardware Number column go?

It is shown on the device page, right after the serial number, and can be edited on the Actions tab. It is no longer a list column or filter.

Where is Last Status Report Time?

Removed. It did not tell when the device itself was last in contact. The device page and the device list now show **Client Last Connected (UTC)**, the time the KMM Client last connected or disconnected.

Why is a device shown with a lock instead of checkbox?

A group change is still in progress on it. It is left out of *select all* until the device has applied the change.

Connectivity and the KMM Client

My device shows red or grey dot under Client connection

Grey means the device's group does not use the KMM Client, so there is nothing to connect; enable **Use Client** in the group if you need client features. Red means the group uses the client but the client is not connected.

Work through these in order:

1. Confirm the device has internet access at all (open a web page on it, or check Wi-Fi in its Network and Connectivity policy).
2. Confirm the network lets the device reach KMM and Google. The device needs HTTPS and WebSocket (WSS) access to `mdm.kuori.com` on port 443, plus Google's Android Enterprise endpoints. Corporate firewalls, proxies and SSL inspection are the usual cause. Give your network team the firewall guide:

- <https://kuori.atlassian.net/wiki/spaces/SC/pages/450592769>

- <https://wiki.kuori.com/books/troubleshooting-Edq/page/firewall-rules-and-encryption-kmm>

3. Confirm the device's group has **Use Client** enabled. Without the client the device is still managed by Google policies, but the dot stays grey and client features are unavailable.
4. Wait about ten minutes after enrollment or a group sync. The client connects once it is installed and the policy has been applied.

See the *KMM Client* manual.

What does a yellow dot under Client connection mean?

The client is connected but the connection is weak: the round trip is slow or heartbeat replies are being missed. Hover the dot to see the current response time. Tasks and screenshots still work, only slower. If it stays yellow, check the device's Wi-Fi or mobile signal.

Which features need the KMM Client?

Online status, screenshots, custom APK installs, file uploads, background image, display rotation, gesture navigation and device location (map and Location tab, KMM Client `v0.6.0 (40)` or newer). Screenshots, display rotation and gesture navigation also need the Security Service app on the device. Plain Google Play app installs and policy enforcement work without the client. See the *KMM Client* manual.

Why is Request Screenshot disabled?

Check the **Client connection** dot in the Status section of the device page (it must be green or yellow) and **Use Client** in its group. Or a screenshot has already been requested and is on its way; the button reads **Screenshot Requested** until the screenshot arrives or the device reports **Screenshot Failed** in the bell.

A task shows Failed.

The **Reason** column says why. The common ones are the device being offline and insufficient storage. Fix the cause and select **Rerun**. If the reason is offline and the device is powered on, go through the connectivity checklist above.

The device enrolls but never gets its apps or policies.

Android Device Policy on the device talks to Google, not to KMM, so a firewall that blocks Google Play or Firebase Cloud Messaging stops enrollment and policy delivery even when KMM itself is reachable. The firewall guide links Google's own list of required endpoints. IP-based allowlisting does not work for Google traffic; allow by hostname or allow general outbound access.

My device is not on the map

The device must run KMM Client `v0.6.0 (40)` or newer, have location services on (groups without a Device Function policy enforce location by default; otherwise set ****Location Mode**** to

****LocationEnforced****), and have reported a position. Select ****Refresh location**** on the device page or ****Refresh all**** on the map, then wait for the device to answer. The map uses the same filters as the list, so clear the filters if the device is filtered out.

Why is marker grey?

The device's group no longer use the KMM Client. Marker colours are the same as the connection dot.

Device Groups and Syncing

Why does my device group keep showing Out of Sync?

That is by design: editing a policy or a managed configuration does not push changes to devices automatically. The groups using it are marked Out of Sync. Select the amber sync icon in the group list to push. See the *Device Groups* manual.

A task for a device that is not connected no longer fails; it waits until the device connects. The Tasks tab updates itself when the task completes or fails.

The device group list can be filtered to the out-of-sync groups (**Out of Sync** filter), and the **Out of Sync** card on the dashboard opens the list with that filter applied.

What is the initial_ group I see when viewing a group?

An automatically created companion group used to install an uploaded kiosk APK before the device locks into kiosk mode. It is managed entirely by the system; your own group names may not start with `initial_`.

Where do devices go when I remove them from a group?

To the **default** group, which every enterprise has and which cannot be deleted.

Why can't I delete this group / policy / app / configuration?

Things that are in use cannot be deleted, from the bottom up: an app used by an Application policy, a configuration used by a policy or group, a policy assigned to a group, a group with devices in it. Remove the usage first. The error message names what is blocking.

Can I copy a group to another enterprise?

Yes. **Export** the group as a JSON file and **Import** it in the other enterprise. Google Play apps are recreated automatically; uploaded APK apps must be uploaded there first. See the *Device Groups* manual.

Apps and Managed Configurations

The Google Play window stays empty when adding an app.

The embedded store takes a small moment to load. If it never appears, check that the browser can reach Google Play (firewall, ad blocker). The administrator browser rules are in the firewall guide linked above.

What is the difference between Available, ForceInstalled and RequiredForSetup?

Available lets the user install the app from Play but does not install it. **ForceInstalled** installs it automatically and the user cannot remove it. **RequiredForSetup** installs it during enrollment before the device can be used. Uploaded APKs are always **Custom** and are installed by the KMM Client. See *Application Management*.

Uploading an APK fails with "File too large" or a file type error.

The upload limit is 1 GB; pick a smaller build. Only real `.apk` files are accepted, so a renamed or corrupted file is rejected.

Why is Download disabled for some apps?

Google Play apps are not stored as files in KMM, so only uploaded APKs can be downloaded. Play apps also show no version or filename; that is expected.

"No Managed Configurations available for this package". Why?

The app does not declare any configurable settings. For Google Play apps there is nothing to do; for an uploaded APK the restrictions must be built into the APK itself. See the *Managed Configurations* manual.

What is the amber warning triangle on an APK package or setting?

The package's restriction structure is unfinished: dropdown and multi-select settings cannot be read from an APK file and their selectable values must be filled in by hand under **Applications → APK Restrictions Structure**. See the *APK Restrictions Structure* manual.

I uploaded a new APK version but its new settings don't show up.

The restriction structure is read only when the app is first uploaded. Later uploads never change it, which also protects your hand-filled values. See the *APK Restrictions Structure* manual for the trade-offs.

A value like %store_id% appears on the device as-is.

The placeholder was not filled in. Each Application policy that uses the configuration gets an input field per placeholder. Open the policy's **Managed Configuration** section and give the value.

What are policy templates and why can't I save one?

Templates are global base settings, visible to everyone across all enterprises, and maintaining them is an administrator task. Anyone can create a policy from one with **Create → Create from template +**. See the *Policy Templates* manual.

Policies: Common Surprises

Devices have no lock screen after I created a Security policy.

A new Security policy starts with **Lockscreen disabled** set to **Yes**. Switch it to **No** if the devices should lock. See the *Security Policy* manual.

A device wiped itself after wrong password attempts.

The Security policy's password rule has **Maximum failed for swipe** set. The device is wiped after that many failed attempts. An Administrative policy's enforcement rule can also end in a wipe. Both manuals carry warnings.

Why must I fill in every Kiosk setting?

The kiosk settings are all-or-nothing: if one is set, all must be set. Use **Clear Kiosk settings** in the Interaction policy to reset them all.

The setup action doesn't run on devices.

If the group uses the KMM client, the policy's setup action is replaced by the system's own client-launch action. Also check that the launched app is in the group with install type **RequiredForSetup**. See the *Interaction Policy* manual.

My kiosk app never gets updates.

An app pinned to the foreground can only update inside a maintenance window. Set the System Update policy's **Update Type** to **Windowed**. Play app updates happen in the same window. See the *System Update Policy* manual.

Updates install even though a freeze period is active.

Freeze periods only work when **Update Type** is something other than **Unspecified**. Note that an active freeze period blocks security patches too. See the *System Update Policy* manual.

The minimum password character fields do nothing.

Minimum letters, **Minimum numeric** and the other per-kind minimums apply only when **Quality** is **Complex**. See the *Security Policy* manual.

Devices lost their Wi-Fi networks after I applied a Network and Connectivity policy.

The policy disallows Wi-Fi changes on fully managed devices. Add the needed networks under **Network Configurations**, or turn on **Escape Hatch Enabled**.

Wi-Fi networks with EAP (802.1x) never reach the devices.

Enterprise (EAP) Wi-Fi configurations are currently not delivered to devices. Use a personal (PSK) network for now. The *Network and Connectivity Policy* manual notes this limitation.

"... with this name already exists in this enterprise"

Names must be unique within the enterprise for each policy type. Pick a different Description Name.

Devices report their location although I never asked for it

Location is enforced by default for device groups that have no Device Function policy, and a new Device Function policy starts with **Location Mode** set to **LocationEnforced**. Set it to **LocationUserChoice** or **LocationDisabled** in the group's Device Function policy to change that.

Enterprise Features

Management, Required Account Email or the Administrative policy's authentication fields are crossed out.

These are Google-mandated features that require a Domain-Managed Enterprise. The enterprise must be bound under your own Google domain (upgrade via the **Enterprise** page). The selectable emails are then the accounts of that domain. See the *Administrative Policy* and *Enrollment Tokens* manuals.

"Required account email must be provided when Management is PersonalUsageDisallowed"

Either give a Required Account Email, or choose **PersonalUsageDisallowedUserless** as the Management value.

Who sees what? What do the roles mean?

Admin, Editor and Viewer work across every enterprise; Enterprise Admin, Enterprise Editor and Enterprise Viewer are the same permission levels limited to their own enterprise. Viewers are read-only. See *User Roles* in the manual index.

Where to look next

- <https://wiki.kuori.com/books/troubleshooting-Edq>
- <https://wiki.kuori.com/books/getting-started>

- <https://wiki.kuori.com/books/features>