

Release Notes

- [1.5.0](#)
- [1.6.0](#)

1.5.0

What's new in KMM?

This release adds notifications to the console and makes managed configurations easier to copy and trace.

Notifications

Notification bell. A bell in the header shows how many notifications you have. Opening it lists them, for example when a task sent to a device completes. Each notification links to the item it concerns, and you can dismiss them one by one or all at once.

Managed configurations

Copy. A copy button on the list and on the detail page creates a copy of a configuration under a new name.

Where a configuration is used. The list has two new columns, Assigned application and Assigned device group. The detail page shows the same information.

Deleting. A configuration that an application or device group uses cannot be deleted. Remove the assignment first.

KMM Client configuration. The KMM Client's server address is set automatically and no longer needs to be entered. Gesture navigation shows as an on/off setting, matching what the device receives.

Device groups

Security service switch. Device groups have a separate switch for the KMM security service. New groups have the KMM client on and the security service off. Existing groups keep their current setup. When the security service is on, it is installed on the group's devices automatically and stays installed.

Save and publish. The save and publish buttons show that they are working until the group is saved or published.

Enrollment without an initial group. Devices enrolled without an initial group now receive the configured group.

Devices

Refresh device data. The device page has a refresh that fetches the latest device data from Google, without waiting for the automatic update.

Renamed devices. Device updates from Google are matched by serial number, so a renamed device keeps updating.

Audit log

Who did it. Entries show who performed each action by email address.

Sign-ins. User sign-ins are recorded in the audit log.

Retention. Audit log records are kept for 36 months.

Enterprises

New enterprises. A new enterprise is created with a complete default policy and a working default enrollment token.

1.6.0

What's new in KMM?

This release puts your devices on a map, shows live whether each device's KMM Client is connected, and lets you act on many devices at once from the device list.

Device map

Available with KMM Client v0.6.0 (42). Devices report their location through the KMM Client app. The map starts working when KMM Client v0.6.0 (42) is released from beta and installed on your devices.

Map of your devices. The device list has a new Map tab next to the List tab. It shows every device that has reported its location, using the same search filters as the list. Nearby devices are grouped into a numbered marker until you zoom in. Clicking a marker opens the device.

Location on the device page. Each device page has a Location tab with the device's latest position.

Refreshing locations. You can ask one device, or all devices at once, to report a fresh location. New locations appear on the map as soon as the device answers.

Marker colours. Markers use the same colours as the connection dot: green for connected, red for not connected, grey for devices without the KMM Client. The colours change live as devices connect and disconnect.

Location policy. Location is now enforced by default for device groups that have no device function policy, so devices can report where they are.

Client connection

Connection dot. The "Client Active" column and row are replaced by "Client connection": a coloured dot that shows whether the KMM Client app on the device is connected to KMM. Green means connected, red means not connected, grey means the device's group does not use the KMM Client. Hover the dot for the meaning. A question mark next to the title explains that this is the

KMM Client's connection, not the device's network connection.

Weak connections. A device whose connection is slow or keeps dropping shows a yellow dot. Hovering it shows the current response time.

Live updates. The dot in the device list and on the device page changes as soon as a device connects, disconnects or its connection quality changes. No reload is needed.

Connection filter. The device list can be filtered by Connected, Weak, Not connected or No client.

Last connection change. The device page and the device list show when the client last connected or disconnected. The old "Last Status Report Time" is gone, because it did not tell when the device itself was last in contact.

Device list

Select several devices. Every row has a checkbox, and a checkbox in the header selects the whole page. With devices selected you can change their group or reboot them in one go. The result is reported per device, and devices that failed stay selected so you can retry.

Group change in progress. A device that is still applying a group change shows a lock instead of a checkbox and is left out of "select all". The lock's tooltip explains why.

Device group filter. The Device Group filter is now a dropdown of your groups instead of a text field, and it matches the chosen group exactly.

Compliance filter. An advanced filter "Has Compliance Issues" shows only devices with policy problems. The Compliance Error card on the dashboard opens the list with this filter already applied.

Device count. The number of devices matching your search is shown next to the page controls.

Hardware number. The hardware number column and filter were removed from the list. The number is shown on the device page, right after the serial number.

Tidier filters. "Is Deleted" moved under Advanced search. Filters are kept in the page address, so a copied link opens the same search.

Device page

Grouped details. Device details are grouped into Device, Status and Device Group sections. Brand and Model moved to the Hardware tab and API Level to the Software tab.

Refresh Device Data. The page reloads as soon as the refresh from Google finishes, instead of waiting 20 seconds.

Installed applications. The Applications tab has a search field and a state filter, so you can find one application on a device with hundreds. The heading shows how many match.

Tasks and screenshots update themselves. The Tasks tab updates when a task completes or fails, and a requested screenshot appears as soon as the device sends it. Both also produce a notification in the bell.

Long values. Long values such as a build signature now wrap inside their field instead of running over the edge of the page.

Device groups

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

Client switches together. The Use Security Service switch sits next to the Use Client switch in the group form.

Tasks for offline devices. When a group is published, tasks for devices that are not connected wait until the device connects instead of showing as failed. Publishing to a large group is also faster.

Quick setup removed. The Quick Setup page and button are gone. Device groups and policies are created through their own pages.

Help

Help icons. A question mark beside every field on the device group pages, and beside every section on the policy pages, opens a short explanation of what the setting does.

Alerts

Announcements from Kuori. Important announcements, such as breaking changes or news, appear in a popup when you open the console. You see each alert once and confirm it with "Got it" or the X. A click outside the popup or the Escape key does not dismiss it, so an alert cannot be confirmed by accident.

Alerts page. Current alerts can be read again under Info, Alerts, and past alerts can be shown on request.

Bug fixes

Links between enterprises. A link to a page in another enterprise opens in that enterprise, so shared links show what the sender saw.

Mobile navigation. The Info links in the mobile menu open the same pages as on a desktop.

Duplicate policy names. Saving an application setting policy with a name that is already in use shows a clear message instead of an error.

Group tasks. Devices always receive the apps and files of their own group and enterprise, each task is sent once, and devices enrolled through an initial group receive their kiosk app as intended.

Group change errors. If Google rejects a group change or reboot, the console now reports it instead of showing success. A group change lock can always be lifted, and the console warns if the device may be out of sync.

Patched vulnerabilities

- [CVE-2026-9358](#)
- [CVE-2026-45819](#)
- [CVE-2026-67213](#)
- [CVE-2026-73088](#)
- [CVE-2026-73089](#)
- [CVE-2026-75604](#)
- [CVE-2026-84375](#)
- [GHSA-2XP9-VWFH-VXW4](#)
- [GHSA-2X7J-588G-CCC2](#)
- [GHSA-5P4M-2WFM-XMQJ](#)
- [GHSA-8M3C-C648-2XJJ](#)
- [GHSA-CC9R-2J5M-2M83](#)
- [GHSA-G7R4-M6W7-QQQR](#)
- [GHSA-RGJ7-G3M4-5G8C](#)
- [GHSA-WMMP-3585-3RMP](#)