Manage the Threema Work App Despite "Bring Your Own Device" (BYOD)

With Threema Work, you can enforce company policies and ensure that business communication remains secure and privacy-compliant even in BYOD scenarios, i.e., when employees use their own devices for work purposes. The management cockpit allows you to manage the Threema Work app even on devices used for BYOD.

In the menu item "App configuration," you can enforce or deactivate various features in the Threema Work app. Here are a few examples of configuration settings:

- **Contact list settings:** For a neat and tidy contact list, you can define your employees' first name (using `th_firstname`) and last name (using `th_lastname`). Further, `th_category` allows you to define the department, region, etc. This value will also be displayed in the company directory.

- **Restrict communication to internal contacts (closed user groups):** To prevent communication with external IDs, you can restrict communication to contacts of the same subscription. As administrator, you also decide which external IDs will be manually added to the contact list. This way, you stay in control of the corporate communication.

- **Backups:** The setting `th_safe_enable` defines whether the Threema Safe backup is obligatory for all users or whether it cannot be activated by anyone.

- **Automatically delete messages:** The setting `th_keep_message_days` allows you to set a period of time (one week to ten years, set in days) after which old messages are automatically deleted.

- **Prevent saving and sharing media outside of Threema Work:** To protect sensitive information shared via Threema Work, you can use the configuration settings `th_disable_share_media` and `th_disable_save_to_gallery`. If activated, media and files cannot be saved outside of Threema Work, and neither can they be shared using apps other than Threema Work.

Top-Down Communication with Threema Broadcast

Threema Broadcast allows you to include employees who use their own device in corporate communication. You can create distribution lists, centrally managed groups, feeds, and bots. Further information about Threema Broadcast can be found here.

Staff Changes

If an employee leaves the company, you can exclude them from internal communication as follows:

1. Withdraw their access to the Threema Work app by deleting their credentials. This ensures that they can no longer access confidential information in the app.

2. By revoking their Threema ID, you ensure that the employee can no longer send and receive messages.