

Kio Staff Safe

User Management Guide

Table of Contents

- User access management 3
 - Things to know 3
 - About user profiles 3
 - Staff Safe: roles and permissions 4
 - Add a user and assign their roles 5
 - Edit a user's assigned roles 5
 - Remove a user's access to Kio Cloud 6



User access management

For those who require access to **Kio Staff Safe**, they need to be added as users and assigned roles from the Kio Cloud Users app. Kio Cloud utilizes role-based permissions to control user access to Kio apps and their permission levels.

Things to know

- You must be assigned to the Administrator role within User Management to view, add, and edit users.
- If a user is not assigned to a role within an app, the app is not displayed in their Kio Cloud Launchpad.
- A user's email address can only be associated with a single Kio Cloud account.
- Once a user is added, only the Kontakt.io support team can change their email address. You will need to submit a Kontakt.io support request for an email address change.
- If your organization has integrated Kio Cloud with its Single Sign-On (SSO) identity provider (IdP), user management within the Kio Cloud Users app is limited to viewing SSO users and their assigned roles. The first time a user authenticates to Kio Cloud with their SSO credentials, their user profile is automatically created within the Kio Cloud Users app.
- The apps available are those activated in your organization's Kio Cloud account. If you don't see an app or want to activate another app, submit a Kontakt.io support request

Roles associated to Kio Staff Safe administration

Optionally, you may also choose to assign the Kio Staff Safe users to roles within the related apps, which include Company Settings and Entity Manager. These users are commonly those responsible for administration type tasks.

- **Company Settings** Includes Entity and Room Management.
Entity Management is where Entity Types (staff roles) and Entities (staff) are also managed.
Room Management includes room types, room matching, and room type rules by entity type. Room management is only managed from Company Settings and is shared with each of the Kio solution-based apps.
- **Entity Manager** Commonly used by those only responsible for adding and managing staff and assigning and distributing badges. The Mobile App user role also grants a user's access to the Kio Entity Manager mobile app to assign badges to staff.

About user profiles

Each user has a unique profile that includes the following details.

- **First Name, Last Name, Email**



- **Unique Ext id:** A unique Staff ID (Entity ID in Company Settings) that allows up to a maximum of 35 characters.

Commonly, an unique identifier from an external system or can be a ID for use within the Kio solution-based apps.


Additionally, required to access the iOS Kio Nurse Assistant mobile app for Asset Tracking and Hand Hygiene.

- **Sign-in method:** identifies if the user's sign in and authentication method, either SSO or email.
- **Roles for apps:** identifies the user's assigned role within each app within the Kio Cloud platform.

Staff Safe: roles and permissions



All roles will receive in-app visual and audio notifications for critical alert types.

Role	Permissions
Administrator	<p>✔ This role has full permissions — they can view and manage everything within the app.</p> <p>What a user assigned to this role can do:</p> <ul style="list-style-type: none"> • View all data and perform actions within all menus - including Alerts, Analysis, and Settings. • Manage Staff including adding and editing Staff Types (basic settings), Staff (basic settings), and Staff Groups. • Manage (add, edit, delete) Alert Rules. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> Advanced Staff (Entity) management is completed from Company Settings. This includes the capabilities to manage the advanced settings for Staff Roles (Entity Types) and Staff (Entities), including the capabilities to delete Staff Roles and remove Staff.</p> <p>For those only responsible for managing Staff, consider assigning a user to the Staff Manager role in the Entity Manager app. This role has limited permission that restricts a user to only adding and editing Staff.</p> <p>For those only responsible for assigning Smart Badges to Staff, consider assigning a user to the Mobile User role in the Entity Manager app. This role has limited permissions that restricts a user to assigning badges from the Kio Entity Manager mobile app.</p> </div>



Role	Permissions
User	<p>✔ This role has restricted permissions to only the Alerts and Dashboard menus — they can view all data within these menus and perform all actions including changing the status of an alert (acknowledged, resolved) and download alert incident reports.</p> <p>✘ This role does not have permission to the Settings menu.</p> <p>Role is ideal for: those that require access to alert activity and metrics, and may also be responsible for responding to alerts and tasked with documenting incident activities.</p>
Alert User	<p>✔ This role has restricted permission to only the Alerts menu including the List and Simple View — they can view all alerts and details, change the status of an alert (acknowledge, resolve), and download alert incident reports.</p> <p>✘ This role does not have permission to the Analysis and Settings menus.</p> <p>Role is ideal for: those responsible for responding to alerts and tasked with documenting alert incident activities.</p>

Add a user and assign their roles

1. From your **Kontakt.io Launchpad**, select **Users**.
2. From the upper-right corner, select **Add User**.
3. Enter their **details** > select **Add User**. They will receive an email from hello@kontakt.io to set their password.
4. Next, you'll need assign their role for the apps they require access to. From the **list of users**, search for their name > select their **name**.
5. From the section **Roles for Apps** > select **Edit**.
6. From each app they require access to, **select a role** to assign their permissions > select **Save**.

Edit a user's assigned roles

A user's assigned role determines their access and permissions within each of the apps. If a user is not assigned to a role within an app, the app is not available from their Kontakt.io Launchpad.

1. From your **Kontakt.io Launchpad**, select **Users**.
2. From the list of users, locate the user > select their **Name**.
3. From the **Roles for Apps** section, select **Edit**.
4. From an app, update their assigned role > select **Save**.



Remove a user's access to Kio Cloud

From a user profile, the disable and delete options allow you to remove a user's access to your Kio Cloud account. Once removed, all user activity within the Kio apps is retained for historical metrics and reference. Commonly, this action is performed when a user has left your organization or no longer requires access to Kio Cloud.

- **Disable option:** Only applies to users that sign in with SSO.
- **Delete option:** Only applies to users that sign-in with email.

