# User

All users created in the system are displayed in a table under this menu item. New users can be added or edited in the table at any time. You can also use the search function to search for a specific user name. In addition, various filters are available, e.g. to display only users with administrator rights.

The users created in the system can be exported as a CSV file. It is also possible to import users via a CSV file.

### Mass editing of users

KentixONE offers the option of changing different settings for different users at the same time. This is helpful if, for example, a new alarm group is to be assigned to several users. To do this, all users to be edited are selected and edited using the edit icon below the table. The selected settings can be set for all selected users individually (Edit) or via a central input field for all users simultaneously (Overwrite).

### Manage KentixONE App access

As soon as the online service has been activated, each user can be granted individual mobile access to the system with the KentixONE app.

To do this, click on the icon and select the option “Manage KentixONE app access”.

The use of the KentixONE online service is linked to the activation of a KentixONE plan.

An invitation to use the KentixONE app is sent to the address stored in the user profile. The user must confirm the invitation to activate access.

As soon as the invitation has been sent, the icon is highlighted in green.

The user receives an e-mail to set a password if the e-mail address for the KentixONE app has not yet been used.
An e-mail address for the KentixONE app can access any number of KentixONE systems.
If the e-mail address is already used for the KentixONE app, the user receives an invitation that must be accepted.

By clicking on the green icon again, the user can withdraw the use of the app in this system and test the push notification function for the app.

## Account settings

To be able to create a user, at least the user name, the full name and the user group must be configured.

To access the web interface of a KentixONE device, the user requires a password with which he can log in in combination with the user name.

An e-mail address can be configured to receive notifications from the system by e-mail. Configuring an e-mail address does not automatically activate notifications via this channel. To do this, the corresponding authorizations must be set in the “Notifications” category.

A user always requires one of the three available permission levels. As a standard user, he has a user group that determines his authorizations in the web interface, as well as alarm groups and access profiles assigned to him. Access and display of logbooks and the Detail View are restricted to these. An administrator has unrestricted access to the system and can use all functions of the web interface. A guest user does not have access to the web interface and the monitoring functions. This permission level is intended for users who are only to use the access functions.

The assigned alarm groups allow a user to see these alarm groups and their subordinate devices in the Detail View. With the appropriate authorization from the user group, he can arm and disarm the alarm groups and acknowledge alarms.

The access profiles define when a user may open which DoorLocks. This applies to openings via RFID transponder, remote opening and via the KentixONE app.

A user account can be activated or deactivated both manually and automatically. For automatic activation or deactivation, simply enter the relevant date and time.

## Notifications

For each user, you can specify the notification channel via which the various alarm types are signaled.

Each of the five alarm types has its own configuration options for its notification. For both alarms (red frame) and warnings (yellow frame), you can specify which notification channel is to be used.

Notification by e-mail is available on all KentixONE devices, but requires a separate SMTP server or the mailing service integrated in KentixONE Plan.

For devices with an active SIM card, which is possible with SiteManager and AlarmManager, notification via SMS can also be configured. A cell phone number must be entered in the “General” category.

With an active KentixONE plan, you also have the option of receiving push notifications. The use of this function requires the installation of the KentixONE app for mobile devices.

## Billing

Here you can select which invoices a user receives. Invoices contain the consumption and costs of defined SmartMeters and SmartPDUs at defined tariffs. These can be configured in the menu under SmartPDU/Billings. By default, statements are sent by e-mail.

# General

Additional user information and authorizations are configured in this category.

The user needs a telephone or cell phone number to receive SMS notifications from the SiteManager or AlarmManager. This must be entered in the format +123456... format.

If SmartAccess components with an integrated PIN input field are present in the system and PIN authentication is active, a PIN can be assigned to a user. The required length of the PIN depends on the setting under Configuration/Security.

The DoorLock-RA4 rack lock only supports the digits 1 to 4.

To ensure that doors can be opened even in the event of a communication failure between DoorLocks and AccessManagers, the user can be assigned emergency access. If a DoorLock cannot reach its AccessManager, this means that no access evaluation can take place. Users with emergency access can still open the door in this case. As this is purely a security function, it is recommended that this authorization is only granted to selected users. Attention: Emergency accesses are only transferred to the door locks during the first booking after the user's configuration has been saved.

The transponder ID is the ID of the RFID transponder with which the user can book at DoorLocks. If no transponder ID is stored, doors can only be opened via remote opening or the app.

If the user is to be able to arm and/or disarm alarm groups when using SmartAccess components, the corresponding authorization must be set.

# API access

An API Bearer token is assigned to each new user created in the system. This token is used for authorization for the KentixONE SmartAPI (Application Programming Interface).