MICROSENS

NMP/SBM

User Management Guide

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany
Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

Table of Contents

Chapter 1. Introduction

MICROSENS NMP Enterprise and MICROSENS SBM are comprehensive client server applications demanding a secure but convenient user administration.

This user management guide will help you properly manage users and their respective access rights of both NMP (Professional and Enterprise) and SBM applications for secure operation.

If any issues occur, please refer to the following documentations:

- Application’s User Manual
- Trouble Shooting Guide
- Best Practises Guide
- Installation Guide

All these documents are available from the MICROSENS website www.microsens.com/support.

If these specific documents do not solve your issues please contact the technical support team of MICROSENS.

1.1. User Management Steps

The following steps have proven to be useful when starting with the application’s user management:

1. Specify the user roles that fit your needs.
    - Check whether the default user access levels are sufficient or not.
    - Only in exceptional cases change the access levels of these user roles.
      It is better to create new user roles with specific access levels (see Section 4.7).
2. Create user accounts.
3. Assign user roles to accounts.

1.2. Terms and Definitions

To avoid misunderstandings, this user management guide uses the following terms:

Term	Definition
Server Manager	The GUI of the respective application’s server component (i.e. NMP Enterprise, SBM). It is used to configure, start and stop the actual server process.
Server process	The server process (hereafter referred to as "instance") which is communicating with the network devices and the web client after being successfully started.

Term	Definition
Web client / Web UI	The web client accessing the application’s web server via web browser.
Access Level	The access level allows or permits the read/write access to specific NMP and SBM features. By assigning an access level to a user it is possible to give or prohibit this user access to these specific features without having to deal with access to every single feature.

Chapter 2. Access Level and Permission Basics

An *access level* is a set of permissions to block read/write access or both to specific features.

The following access levels are defined by default:

- **Super Admin:** System administration with full read/write access to all apps and features.
- **System Admininstrator:** System administration with restricted rights to SBM.
- **Building Administrator:** System administration with restricted rights to NMP.
- **Admin:** Administration with even more restricted rights to NMP and SBM.
- **Manager:** Management access with read/write access to the most NMP and SBM data (but without administration rights).
- **User:** Read-only access to e.g. statistics and status dialogues.

> It is not possible to delete these default access levels. It is only allowed to change their permissions for specific apps or features.
>
> **We strongly recommend not to change permissions of default access levels but to create new access levels that fit your needs!**

A permission can be:

- `no access`: The user is blocked from opening a specific app or feature.
- `read`: The user can open an app or feature but is not able to change settings or values. This is intended for users who just have to see statistics or status dialogues.
- `read/write`: The user has full read/write access to specific apps or features. This is intended for administrators with full access to either specific apps or features.
  The access level "Super Admin" is an exceptional case with full access to all apps and features.

Users can be granted (or denied) access for two separate scopes of operation:

Access levels for NMP

- This affects the management of physical network devices (i.e. switches etc.)

Access levels for SBM

- This affects the management of Smart Building components (i.e. devices, actors, sensors, data points etc.)

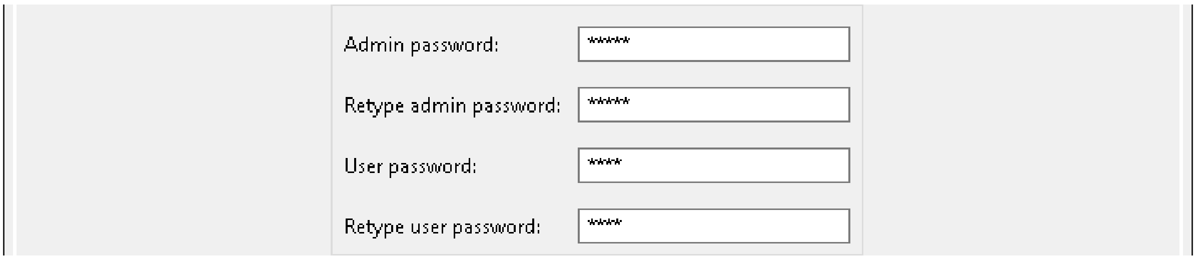
It is possible to grant and manage access for both NMP and SBM applications simultaneously.

Chapter 3. User Management with NMP Professional

While NMP Enterprise comes with comprehensive user administration options, NMP Professional simply offers changing the passwords of both users "admin" and "user".

> Only a user with administrative rights can change NMP settings.

1. Select Settings › Security Settings from the menu.
   - The application settings dialogue opens with the tab Security Settings selected.



Admin password: ******
Retype admin password: ******
User password: *****
Retype user password: *****

Figure 1. NMP Professional - Application Settings - Security Settings

2. Assign a new login name and password for the administrator and standard user to access NMP Professional.
3. Click Apply to save the respective input.

> For security reasons the password should be at least 8 characters long, containing a combination of letters, numbers, punctuation and special characters.

Chapter 4. User Management via Web Client

4.1. General Prerequisites for Managing Users

Before managing users, the prerequisites are as follows:

- Valid application license is uploaded to the server.
- The application’s server instance is started with the web server enabled and is accessible via network.
- Login to web UI as a user with at least user management rights (e.g. as user "Super Admin" directly after application installation).

4.2. Start Server Manager

In order to start the Server Manager use one of the links provided in the Microsoft Windows® Start menu:

- Start › MICROSENS › MICROSENS NMP/SBM Server

or

- Start › MICROSENS › MICROSENS NMP/SBM Server (Debug Mode)

> Starting the server in debug mode will open an additional Microsoft Windows® command line interface (`cmd`), where all the logs and errors will be displayed.

The Server Manager opens with its main window, showing the tab Server Settings.

4.3. Start Server Process

Click on the button Start Server to start the server process.

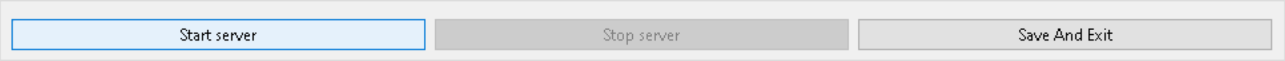
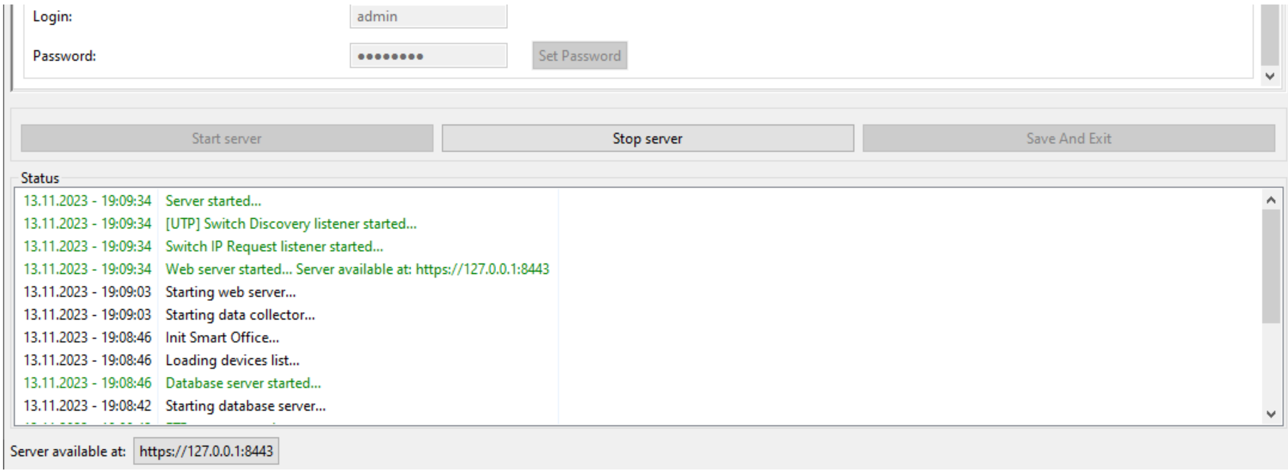


Figure 2. Server Manager - Start Server Process

If the server process was started successfully, you should see `Server started…` as last message on top of the status field as follows:



Login: admin

Password: ••••••••

```
13.11.2023 - 19:09:34   Server started...
13.11.2023 - 19:09:34   [UTP] Switch Discovery listener started...
13.11.2023 - 19:09:34   Switch IP Request listener started...
13.11.2023 - 19:09:34   Web server started... Server available at: https://127.0.0.1:8443
13.11.2023 - 19:09:03   Starting web server...
13.11.2023 - 19:09:03   Starting data collector...
13.11.2023 - 19:08:46   Init Smart Office...
13.11.2023 - 19:08:46   Loading devices list...
13.11.2023 - 19:08:46   Database server started...
13.11.2023 - 19:08:42   Starting database server...
```

Server available at: https://127.0.0.1:8443

Figure 3. Server Manager - Status Field and Server URL

Please note the SBM server URL on the bottom left corner below the status field.

In order to make and save changes of the server configurations, the server process must be stopped. It is not possible to make or save changes of the configuration in a running server process.

A click on the button Stop Server will stop the server process.

After all changes have been made, a click on the button Save And Exit will save the changes in the server configuration and exit.

4.4. Login to Web UI

After starting the server instance, a web browser can be used to access the server with one of the following URL addresses. You can find the server IP address and the server port on the bottom left corner of the server manager window right below the status list.

For secured HTTP connections, if the secured HTTP was not unchecked https://<server_ip_address>:<https_server_port>/

For standard HTTP connections http://<server_ip_address>:<http_server_port>/

You have to insert valid credentials into the login screen before accessing the Web UI of the application’s web server.

A user account with administrator access rights (e.g. "Super Admin") is mandatory to make changes in the respective application.

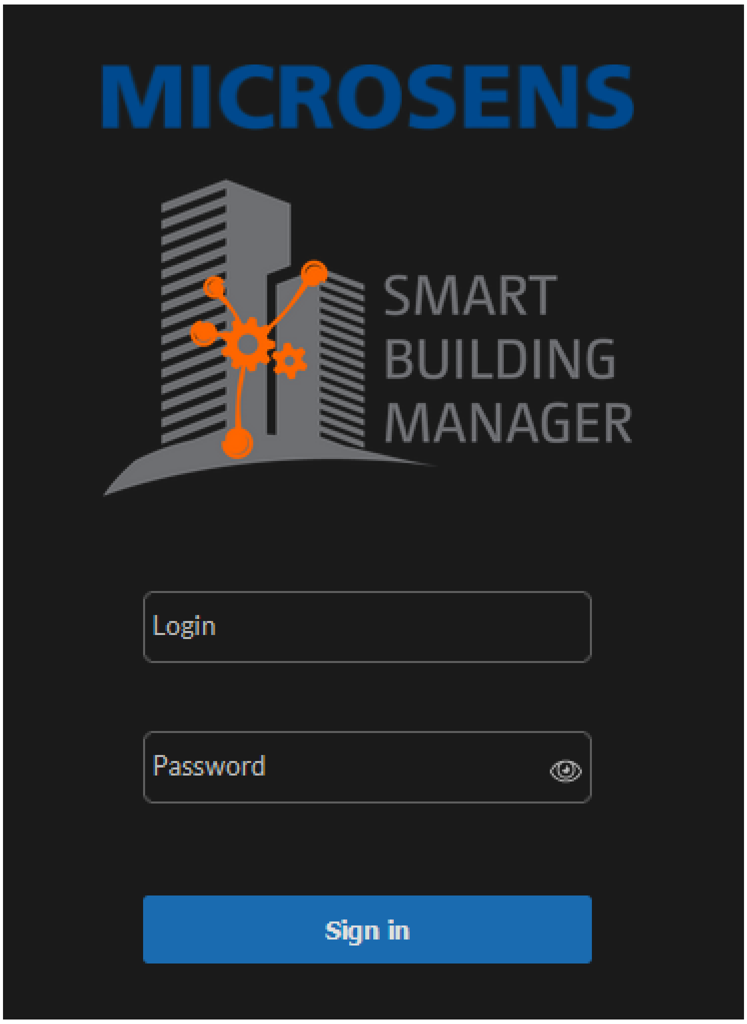


Figure 4. WEB UI - Login Screen

Depending on the user’s access level, the Web UI opens with several application tiles for:

- Building Management
- Building Configuration
- Device Management
- User Management
- Licence Management
- Server Configuration

If you do not see one or more of these tiles you do not have the respective access level for this application.

4.5. Start the App

Depending on the user’s access level, the Web UI opens with several application tiles. If you do not see a specific tile you do not have the respective access level for this application.

There are two possible ways to start the app:

Directly on login

After successfull login into the Web UI, the tiles of all available applications appear.

Click on the tile of the application you want to open.

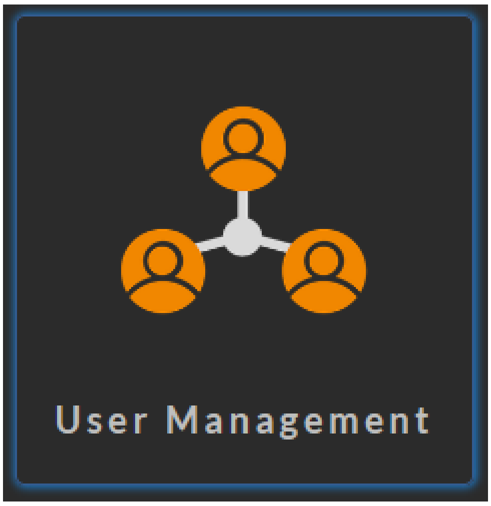


Figure 5. Web UI - Application "User Management"

The respective application’s start page opens.

Changing apps

As long as another app is active, you have to logout of the active application first by selecting <user> › Select app from the drop-down menu on the top right of the web UI.

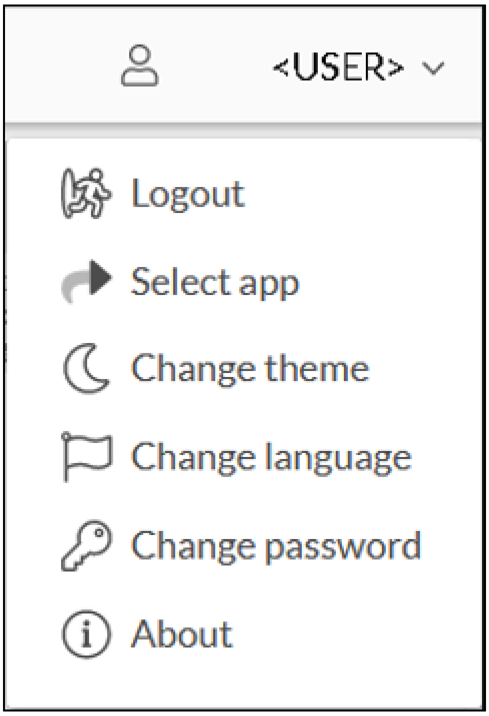
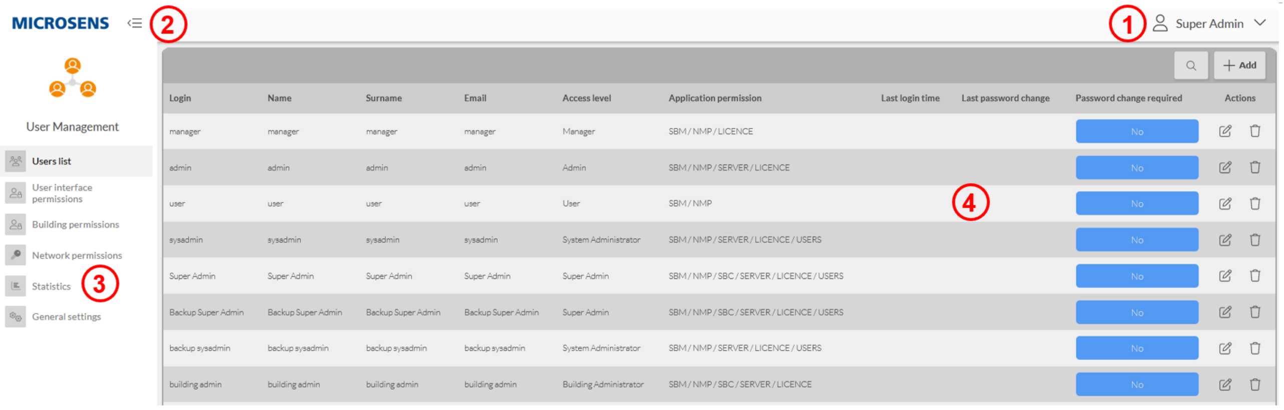


Figure 6. Web UI - User Menu

The tiles of all available applications appear (see above).

4.6. User Management Overview

After login to the app, the user management screen with the users list appears by default.



Login	Name	Surname	Email	Access level	Application permission	Last login time	Last password change	Password change required	Actions
manager	manager	manager	manager	Manager	SBM / NMP / LICENCE			No	
admin	admin	admin	admin	Admin	SBM / NMP / SERVER / LICENCE			No	
user	user	user	user	User	SBM / NMP			No	
sysadmin	sysadmin	sysadmin	sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS			No	
Super Admin	Super Admin	Super Admin	Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS			No	
Backup Super Admin	Backup Super Admin	Backup Super Admin	Backup Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS			No	
backup sysadmin	backup sysadmin	backup sysadmin	backup sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS			No	
building admin	building admin	building admin	building admin	Building Administrator	SBM / NMP / SBC / SERVER / LICENCE			No	

Figure 7. Web UI - User Management Start Screen

- **1:** Scroll-down menu for user/administrator settings and log-out
- **2:** Toggle icon to show or hide the navigation bar
- **3:** Navigation bar
- **4:** Data panel of the selected menu category, optionally with additional action buttons

The user management application allows the management of users in the following aspects:

- Basic operations like
  - Creating or deleting user entries
  - Changing user properties (i.e. name, email address, credentials and access level)
- User role and access level management for
  - User interfaces
  - Building permissions (SBM only)
  - Network permissions

Besides that, the user management application allows the analysis of basic user statistics.

Finally, general settings about session management and blocking users are available.

To leave the user management app, open the scroll-down menu of administrator settings and either click on Logout or Select app.

4.7. Managing Access Levels

To manage access levels, open User interface permissions in the navigation bar. The window for managing access levels and permissions appears, showing the following sections:

- Manage access levels
- List of registered users

4.7.1. Add New Access Level

To add a new access level follow these steps:

1. In the section Selected access level click on +Create.
   - The app selection dialogue opens:

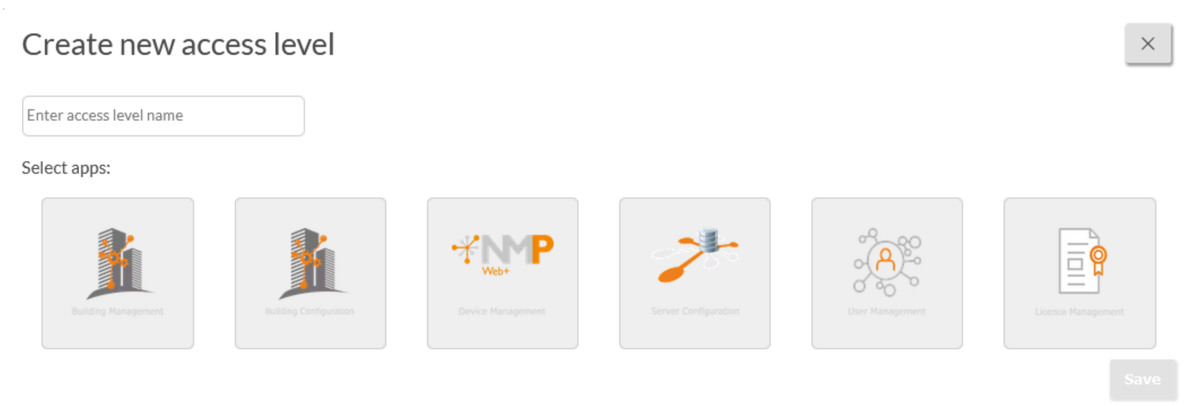
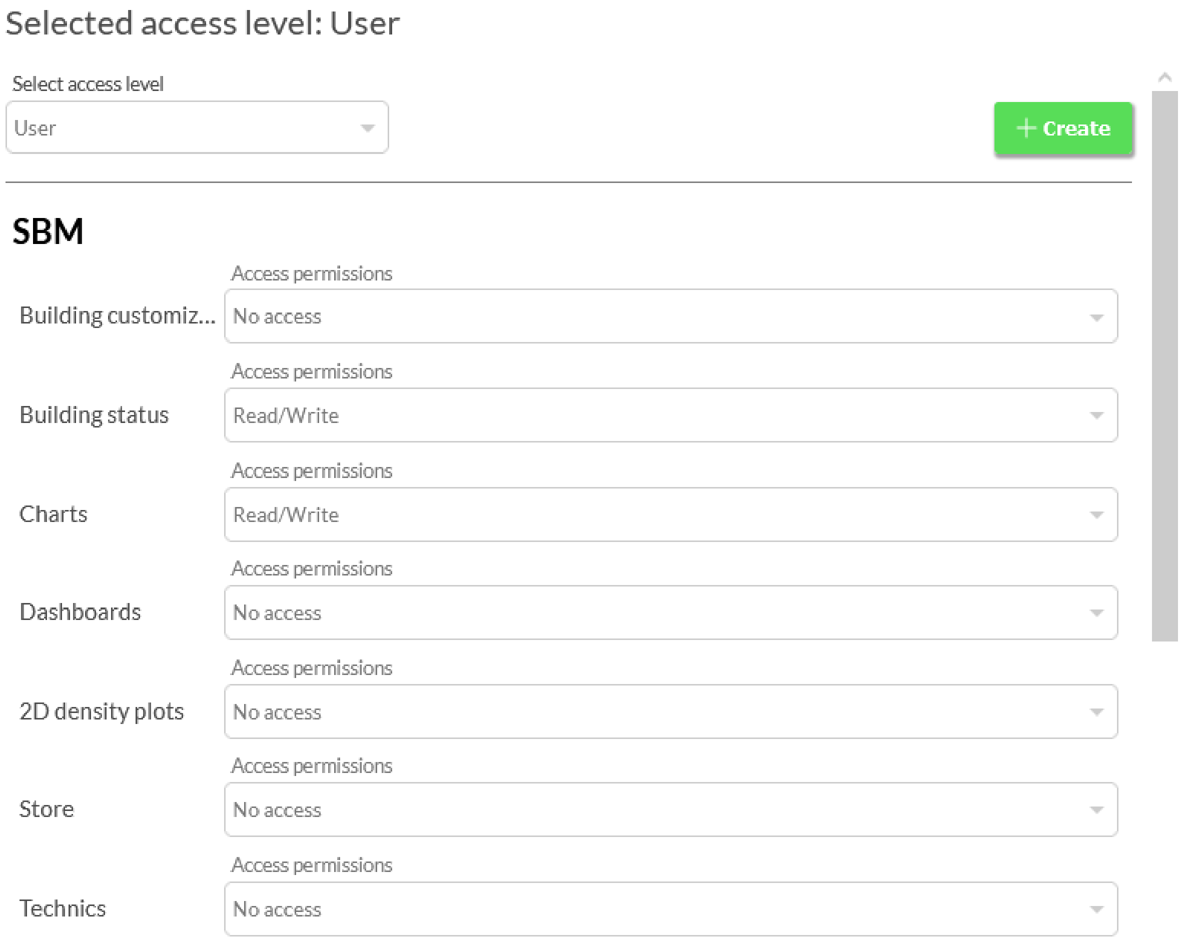


Figure 8. User Management - User Interface Permissions - Selected Access Level - Create New Access Level - Select Apps

2. Click on the respective icon to enable access for NMP and/or SBM.
   - So it is possible to limit the access to only one application. E.g., an SBM user only needs to see statistics about devices, actors and sensors and no information about network topology.

     > It is possible to enable all icons to grant access for all applications.

   - The button Save is enabled.
3. Click on Save to open the access level data input dialogue.



Selected access level: User

Select access level: User

SBM

	Access permissions
Building customiz...	No access
Building status	Read/Write
Charts	Read/Write
Dashboards	No access
2D density plots	No access
Store	No access
Technics	No access

Figure 9. User Management - User Interface Permissions - Selected Access Level - Create New Access Level

4. Enter the name of the new access level. Use a descriptive name.
5. Select the specific permissions for the respective topic.

> Most of these topics correspond to the menu items in the navigation bar of the respective application. So if you assign the permission `no access` to a topic, the user will not see this item in the menu bar.

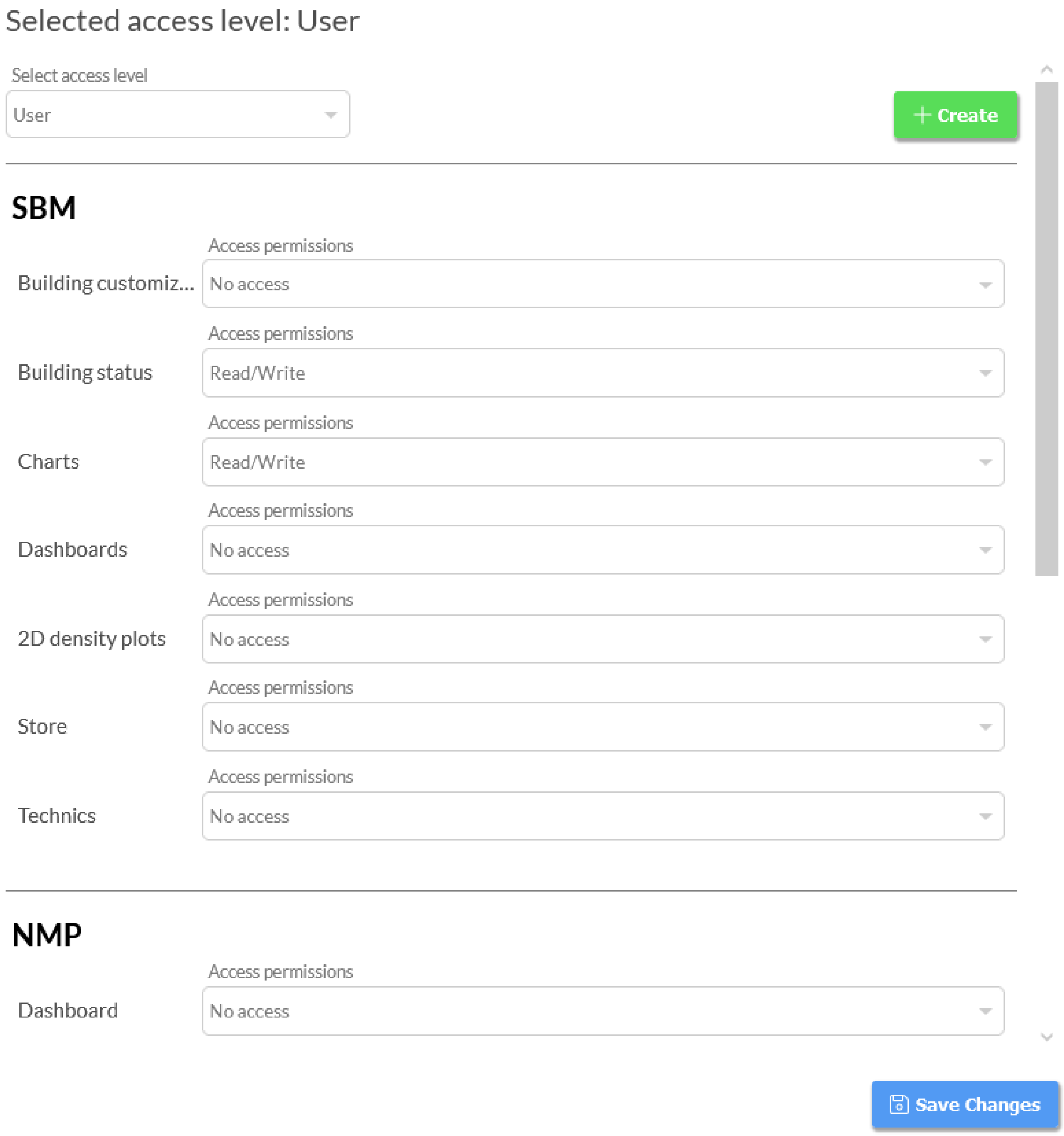
6. Click on +create at the bottom of the dialogue to save the new access level. Click on x on the top of the dialogue to cancel and leave the dialogue without saving your changes.
   - The new entry will appear in the drop-down list of access levels.

4.7.2. Edit Access Levels

> We strongly recommend not to change permissions of default access levels but to create new ones that fit your needs!

To edit an existing access level, follow these steps:

1. Select the respective access level from the drop-down list at the top of the window.
    - This will update the indicator list of applications and respective permissions below.



Selected access level: User

Select access level: User

SBM

	Access permissions
Building customiz...	No access
Building status	Read/Write
Charts	Read/Write
Dashboards	No access
2D density plots	No access
Store	No access
Technics	No access

NMP

	Access permissions
Dashboard	No access

Figure 10. User Management - User Interface Permissions - Selected Access Level

2. Change the permission of specific topics as needed by selecting the respective entry from the drop-down list.
3. Click on Save Changes.

To cancel the changes, just select another access level from the drop-down list at the top of the window. This will leave the settings unchanged.

4.7.3. Delete Access Levels

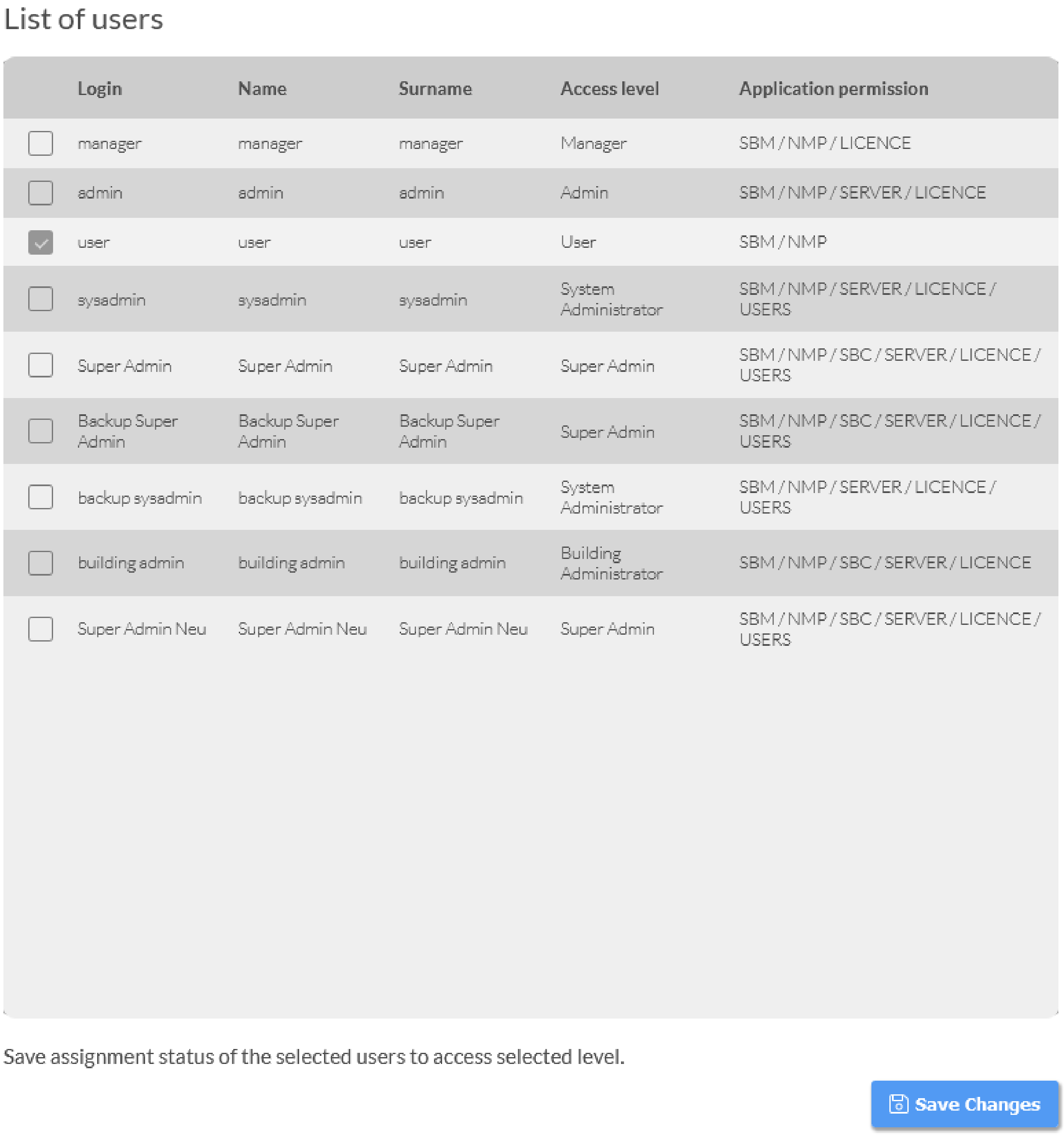
To delete an access level follow these steps:

1. Select the respective entry from the drop-down list at top of the window.
2. Click on Remove at the bottom of the window.
3. Confirm the security prompt.
   - The access level entry will be deleted from the drop-down list.

> ℹ It is not possible to delete the default access levels.

4.7.4. Assign/Unassign Access Levels to Users

As soon as an access level is selected from the drop-down list, the list of users will show their actual assignments. The affected user is marked by a hook.



List of users

	Login	Name	Surname	Access level	Application permission
☐	manager	manager	manager	Manager	SBM / NMP / LICENCE
☐	admin	admin	admin	Admin	SBM / NMP / SERVER / LICENCE
☑	user	user	user	User	SBM / NMP
☐	sysadmin	sysadmin	sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS
☐	Super Admin	Super Admin	Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS
☐	Backup Super Admin	Backup Super Admin	Backup Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS
☐	backup sysadmin	backup sysadmin	backup sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS
☐	building admin	building admin	building admin	Building Administrator	SBM / NMP / SBC / SERVER / LICENCE
☐	Super Admin Neu	Super Admin Neu	Super Admin Neu	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS

Save assignment status of the selected users to access selected level.

Figure 11. User Management - User Interface Permissions - Selected Access Level - List Of Users

To change access levels for users, follow these steps:

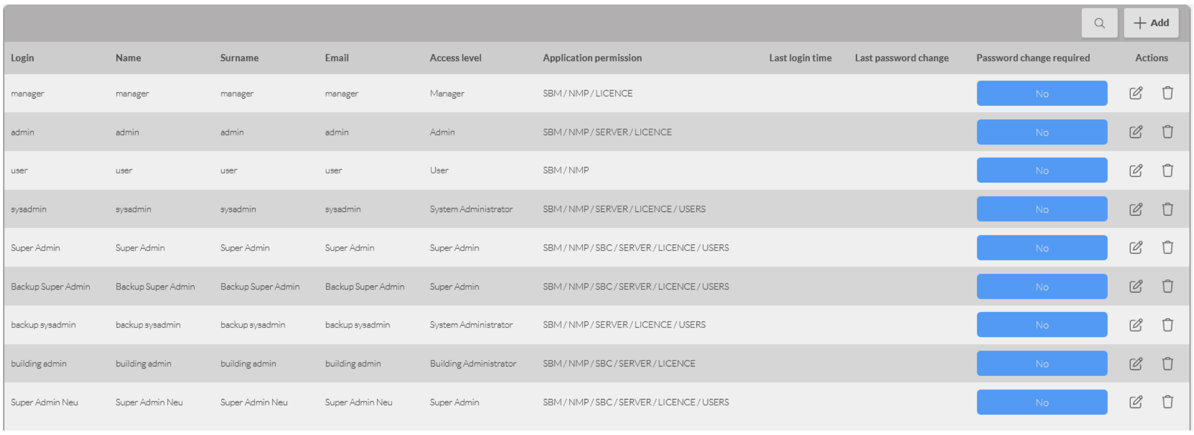
1. Select the access level from the drop-down list in the left-hand pane.
   - This will update the list of users with the respective indicators in the right-hand pane.
2. Check or uncheck the user whose access level you want to change.
3. Click on Save Changes to save the changes.

The access role association for at least on user with role "sysadmin" or "Super Admin" cannot be deleted. Therefore it is not possible for this users to accidentally block their own comprehensive access level.

4.8. Adding, Editing and Deleting User Entries

4.8.1. Add User Entries

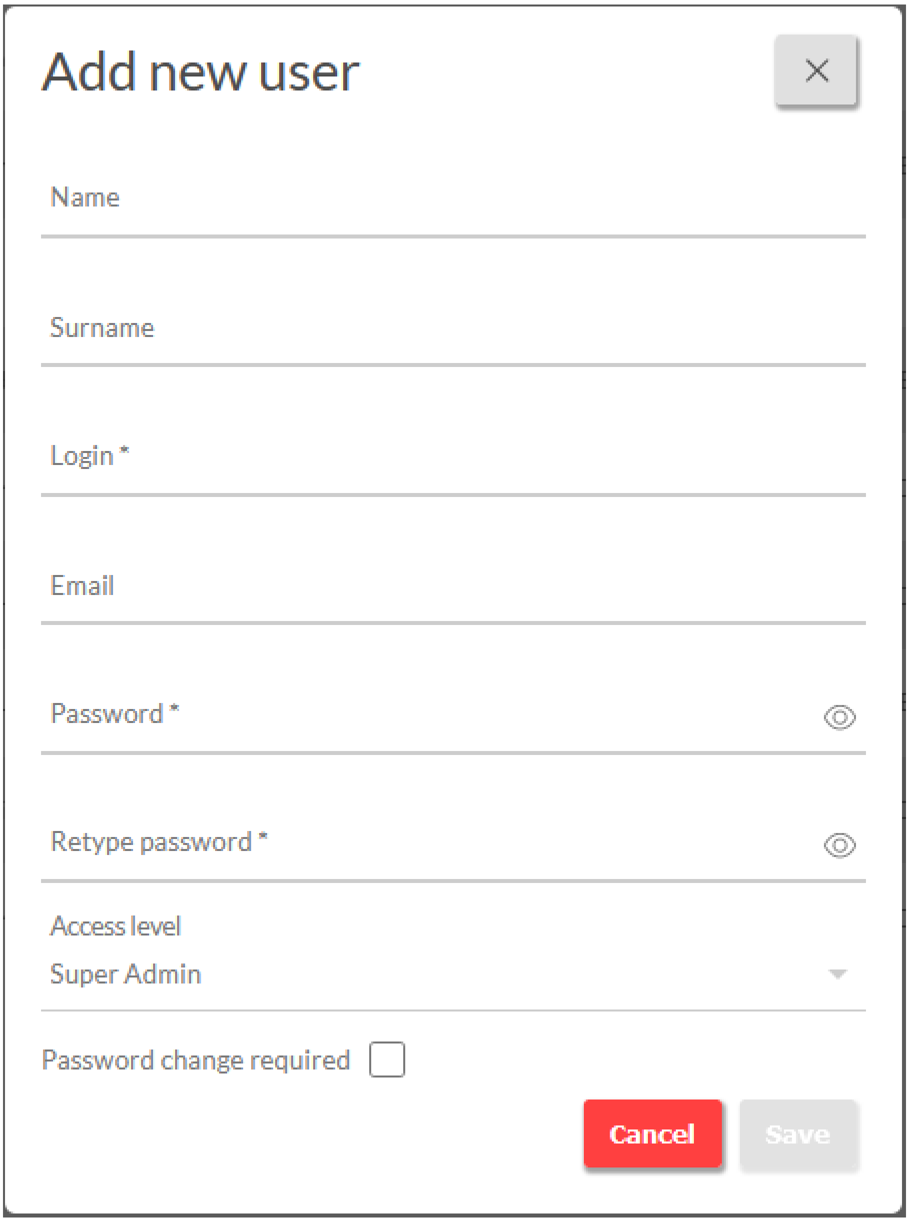
1. In the left-hand navigation bar click on Users list.
   - The data panel shows a tabular overview of all registered users with their respective user data and credentials



Login	Name	Surname	Email	Access level	Application permission	Last login time	Last password change	Password change required	Actions
manager	manager	manager	manager	Manager	SBM / NMP / LICENCE			No	✎ 🗑
admin	admin	admin	admin	Admin	SBM / NMP / SERVER / LICENCE			No	✎ 🗑
user	user	user	user	User	SBM / NMP			No	✎ 🗑
sysadmin	sysadmin	sysadmin	sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS			No	✎ 🗑
Super Admin	Super Admin	Super Admin	Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS			No	✎ 🗑
Backup Super Admin	Backup Super Admin	Backup Super Admin	Backup Super Admin	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS			No	✎ 🗑
backup sysadmin	backup sysadmin	backup sysadmin	backup sysadmin	System Administrator	SBM / NMP / SERVER / LICENCE / USERS			No	✎ 🗑
building admin	building admin	building admin	building admin	Building Administrator	SBM / NMP / SBC / SERVER / LICENCE			No	✎ 🗑
Super Admin Neu	Super Admin Neu	Super Admin Neu	Super Admin Neu	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS			No	✎ 🗑

Figure 12. User Management - Users List

2. Click on +Add on the top right.
   - The following pop-up window opens:



Add new user

Name

Surname

Login *

Email

Password *

Retype password *

Access level
Super Admin

Password change required □

Figure 13. User Management - Add New User

3. Enter the following user data:
    - User's name and surname (optional)
    - User's login name (required)
    - User's email address (optional)
    - User's password (required, retype for security reasons)
    - Select the user's access level from the drop-down list.
    - Check or uncheck the option "password change required".

> When this option is enabled, the user will be forced to change the password on first login. This is strongly recommended!

4. Click on Save to apply the change or on Cancel to discard the changes.
   - If saved, the new entry appears in the tabular overview.
   - The user will be notified of the registration through the email address provided.

4.8.2. Edit User Entries

1. Click on Edit (notepad icon) on the right of the respective entry.
   - The edit dialogue pops up (similar to the "add user" dialogue).
2. Edit the user’s entries as needed.
3. Click on Save to apply the change or on Cancel to discard the changes.
   - If saved, the entry appears in the tabular overview, showing the changed data.
   - The user will be notified of the data changes through the email address provided.

4.8.3. Delete User Entries

1. Click on Delete (waste bin icon) on the right of the respective entry.
2. Confirm the security prompt with Ok.

4.9. Manage Building Groups and Permissions

This section describes how to manage SBM groups and permissions. SBM groups (or "tenants") serve to distinguish between responsible organisations or persons using the same building infrastructure independently (e.g. two companies using the same building, but different floors or rooms).

4.9.1. Additional or Differing Prerequisites

Before managing SBM groups and permissions the prerequisites must be as follows:

- All general prerequisites must be met.
- Essentially, a building structure must be available for this process. If no structure was created previously, it is not possible to create building groups. Change to app "Building Management" to create and manage the necessary building structures.

4.9.2. Define New Group with Assigned Structure

1. In the left-hand navigation bar click on Building permissions.
   - The data panel shows a list of all registered users on the left and a list of existing groups with group members and the assigned building structure on the right.

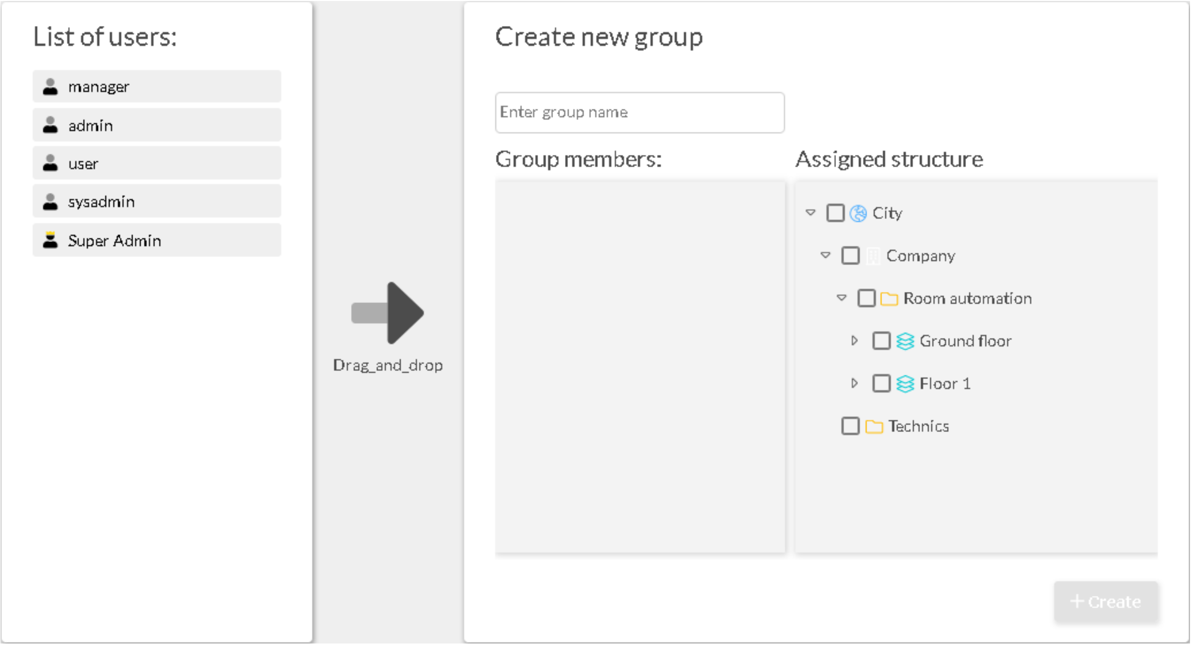


Figure 14. Data Panel Building Permissions

2. If necessary (i.e. at least one group exists) click on Create new group. The group name text field becomes editable.
3. Enter a descriptive group name into the text field.
4. Check or uncheck the specific structural components that need or need not be included into the group.

> Selecting a lower level node (e.g. "Technics") automatically auto-checks all upper level nodes (i.e. "Company" and "City") but not the nodes on the same level (i.e. "Room automation" and its contained nodes). * As soon as the nodes are selected, the button +create becomes active.

5. Click the button +create to save the new group.
   - The new entry is listed in the group’s drop-down list.

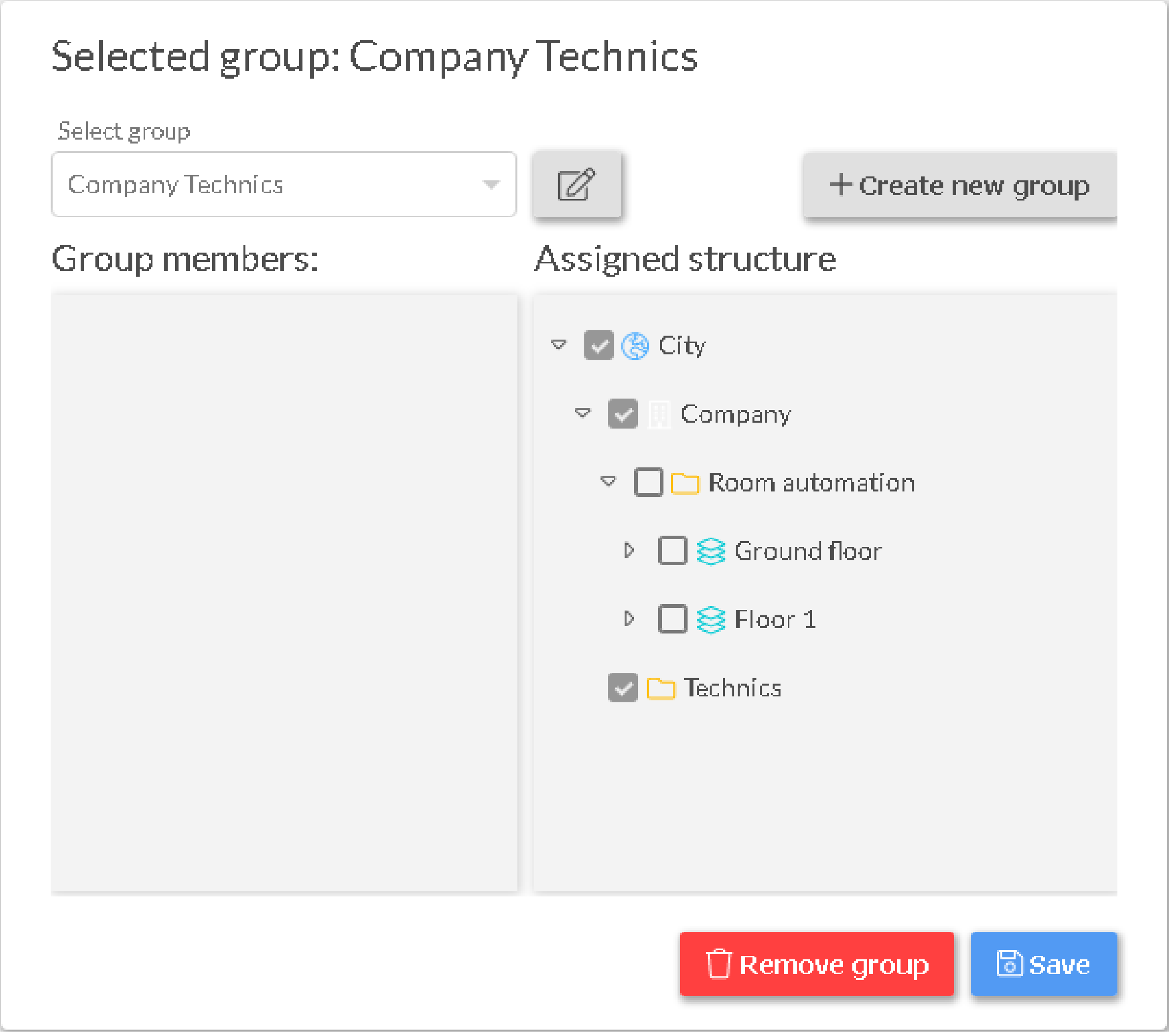


Figure 15. Data Panel Building Permissions - Selected Group

4.9.3. Edit Group Name

1. Select an existing group entry from the drop-down list.
   - The list of entries contain the group members and the assigned structure.
2. Click on Edit on the right of the drop-down list.
   - The text field becomes editable.
3. Change the group name as needed.
4. Click on Save to apply the name change.

4.9.4. Edit Assigned Structure

> Handle with care! Consider carefully, whether any of the group members should have access to the newly assigned structure.

1. Select an existing group entry from the drop-down list.

    - The assigned structure shows actual entries.
2. Check or uncheck the respective nodes as needed.
3. Click on Save to apply the new structure.

4.9.5. Remove Group

1. Select an existing group entry from the drop-down list.
2. Click on Remove Group.
3. Confirm the security prompt.
    - The entry is deleted from the drop-down list.

> All group members will lose the access to the previously assigned structure. Consider carefully, whether any of the group members should have access to only parts of this structure or to the entire structure.

4.9.6. Add or Detach Group Members

1. To add a user, drag and drop a user from the list of users to the group members field.
2. To detach a user from the group, click on the icon x on the right of the respective group member entry.
3. Click on Save to apply the group member changes.

4.10. Manage Network Permissions

This section describes how to to define and assign network access rights for registered users.

4.10.1. Additional or Differing Prerequisites

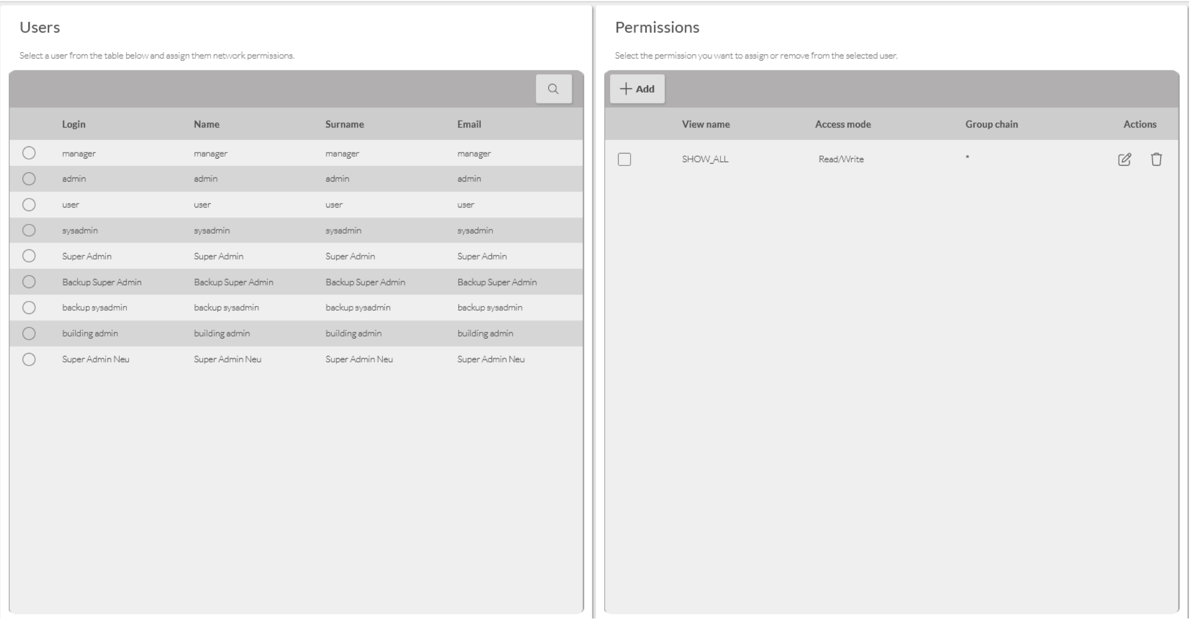
Before managing network permissions the prerequisites must be as follows:

- All general prerequisites must be met.
- Essentially, a network device list tree must be available for this process. If there are no devices it is not possible to create access views. Change to app "Device Management" to manage the necessary network devices.

4.10.2. Create Access Views

To create a new access view, follow these steps:

1. In the left-hand navigation bar click on Network permissions.
    - The data panel consists of three main elements:



Users

Select a user from the table below and assign them network permissions.

	Login	Name	Surname	Email
○	manager	manager	manager	manager
○	admin	admin	admin	admin
○	user	user	user	user
○	sysadmin	sysadmin	sysadmin	sysadmin
○	Super Admin	Super Admin	Super Admin	Super Admin
○	Backup Super Admin	Backup Super Admin	Backup Super Admin	Backup Super Admin
○	backup sysadmin	backup sysadmin	backup sysadmin	backup sysadmin
○	building admin	building admin	building admin	building admin
○	Super Admin Neu	Super Admin Neu	Super Admin Neu	Super Admin Neu

Permissions

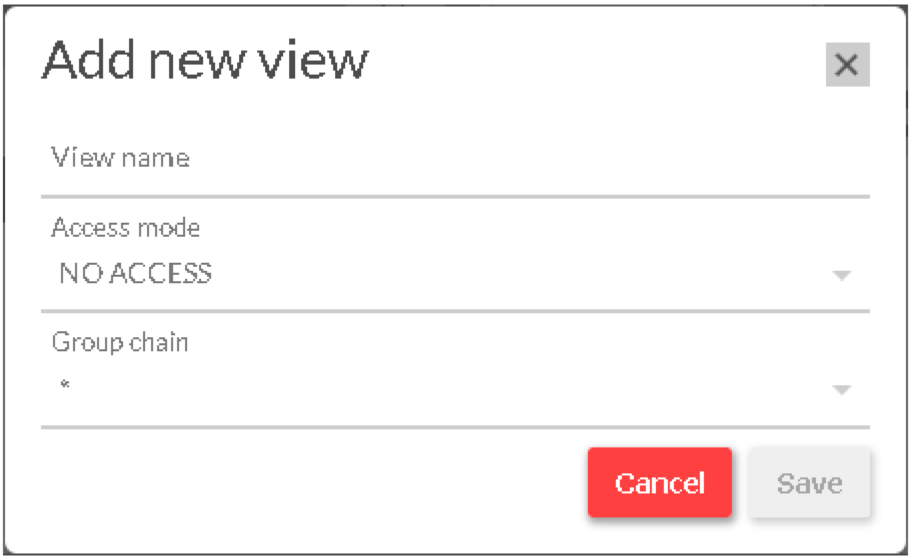
Select the permission you want to assign or remove from the selected user.

	View name	Access mode	Group chain	Actions
□	SHOW_ALL	Read/Write	*	

Figure 16. Data Panel Network Permissions

- **Users:** List of existing user accounts (with possibility to search for accounts).
- **User permissions:** Assigned access view for the account selected in the left-hand pane.
- **Permissions:** List of defined access views.

2. In the right-hand pane click on +Add.
3. In the opening dialogue enter the specific access view data.



Add new view

View name

Access mode: NO ACCESS

Group chain: *

Figure 17. Data Panel Network Permissions - Add Access View

- **View Name:** Enter a name for a new device list view or click on a previously defined view in the view list table.
  This entry has to be unique.

- **Access mode:** Select one of the following access modes:
    - NO_ACCESS: This mode blocks the access to the respective group chain.
    - READ ONLY: This mode allows read-only access to the respective group chain.
    - READ & WRITE: This mode allows access to the respective group chain.
- **Group chain**: The drop-down list mirrors the node structure of the device list tree. After selecting the first node, subsequent drop-down lists appear for further selection.

The access mode is applied for the last node of the group chain. The group chain can end with one of the following entries:

- "" (empty): If the group chain ends with "", it means that the devices at this group should be hidden. All its subgroups are visible to the user.
- "*" (asterisk): If the group chain ends with "*", it means that the same access mode is also applied to subgroups of this node (inheritance). It is also possible to hide some group and its subgroups ("*") and to show one of the subgroups with another view. In such a case, the group in the device list tree is visible to the user marked with a grey icon and the name of group is replaced with NO_ACCESS.

> ℹ The view "SHOW_ALL" with READ & WRITE access to the entire device list is predefined, non-erasable, and is associated with the user "Super Admin" by default.

4.10.3. Edit Access Views

To edit an existing access view, follow these steps:

1. Click on Edit (notepad icon) to the right of the respective entry.
    - The edit dialogue pops up (similar to the "add access view" dialogue).
2. Edit the views entries as needed.
3. Click on Save to save the changes or on Cancel to discard the changes.
    - If saved, the entry appears in the tabular overview, showing the changed data.

4.10.4. Delete Access Views

To delete an existing access view, follow these steps:

1. Click on Delete (waste bin icon) to the right of the respective entry.
2. Confirm the security prompt with Ok.

> ℹ The Super Admin’s list view association cannot be deleted. Therefore it is not possible for the Super Admin to accidentially block his own comprehensive device list view.

4.10.5. Assign Access View to User

To assign an existing access view to a user account, follow these steps:

1. In the left-hand pane select a listed user account from the list.
2. In the right-hand pane click on Assign view next to the view entry you want to assign.
   - In the middle pane "User Permissions" the assigned access view for the selected user is listed.

4.10.6. Remove Access View from User

To remove an existing access view from a user account, follow these steps:

1. In the left-hand pane select a listed user account from the list.
   - In the middle pane a list of assigned access views appears.
2. Click on Delete (waste bin icon) next to the entry you want to remove.
   - The access view will removed from this user immediately without a security prompt.

4.11. Analyse User Statistics

The user management app allows the basic analysis of user actions.

4.11.1. Additional or Differing Prerequisites

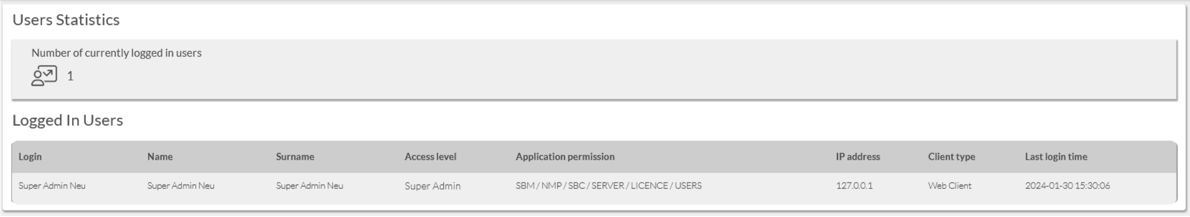
Before using the analysis tool, the prerequisites are as follows:

- All general prerequisites must be met, except the user access rights.
- Login to the web UI as a user with statistics access rights.

4.11.2. Dashboard

To view the data follow these steps:

1. In the navigation bar change to Statistics.
   - The statistics dashboard opens in the data panel.



Users Statistics

Number of currently logged in users

1

Logged In Users

Login	Name	Surname	Access level	Application permission	IP address	Client type	Last login time
Super Admin Neu	Super Admin Neu	Super Admin Neu	Super Admin	SBM / NMP / SBC / SERVER / LICENCE / USERS	127.0.0.1	Web Client	2024-01-30 15:30:06

Figure 18. Data Panel User Statistics

This dashboard can be used to review the following data:

- Number of currently logged in users
- List of currently logged in users

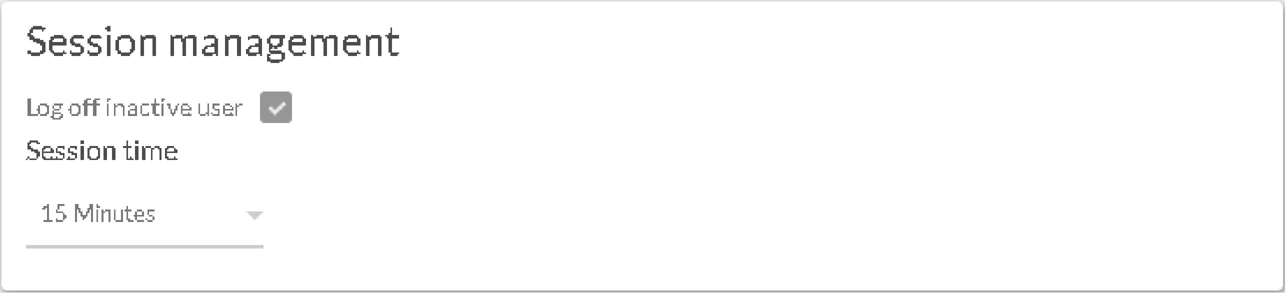
4.12. General Settings

The user management app offers the control of some basic user session activities:

- Session inactivity behavior
- Login attempt behavior

4.12.1. Session Inactivity

1. In the left-hand navigation bar click on General Settings.



Session management

Log off inactive user ☑

Session time

15 Minutes

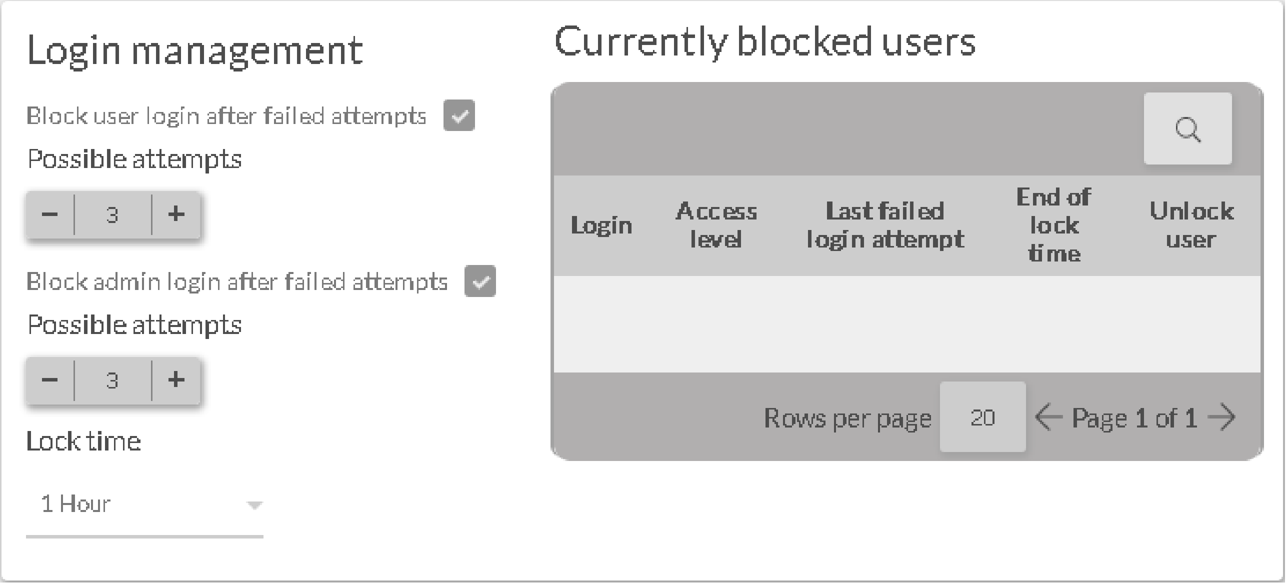
Figure 19. Data Panel - General Settings - Session Management

- **Log off inactive user:** Check or uncheck this option to enable (default) or disable logging off inactive users.
- **Session time:** If logging off users due to inactivity is enabled, select the specific session inactivity time, after which the user is logged out automatically.

  The setting change is saved automatically.

4.12.2. User Login Attempts

In order to avoid e.g. brute-force attacks by flooding the login process with lots of password attempts.



Login management

Block user login after failed attempts ☑

Possible attempts

− 3 +

Block admin login after failed attempts ☑

Possible attempts

− 3 +

Lock time

1 Hour

Currently blocked users

Login	Access level	Last failed login attempt	End of lock time	Unlock user

Rows per page 20 ← Page 1 of 1 →

Figure 20. Data Panel - General Settings - Login Management

The user management also provides a function to control the handling of failed logon attempts.

- **Block user/admin login after failed attempts:** Check or uncheck this option to enable (default) or disable lockout of users/admins after invalid login attempts

  With this option enabled, a user/admin will be locked out when the maximum number of failed login attempts is reached.

  In the case that a user account is locked, the user has to contact an administrator for unlocking the account.

- **Possible attempts:** This parameter defines the number of failed login attempts before user/admin login is locked.

  The number of failed login attempts before an account is locked can be

  - min. value = 2
  - default value = 3
  - max. value = 10

- **Lock time:** Sysadmin and Super Admin accounts will never be locked out!

  Instead the account will be blocked for a certain period of time if the max. number of failed login attempts is reached.

  The blocking period can be set between

  - min. value = 5 min
  - default value = 1 h
  - max. value = 24 h

ℹ | The setting change is saved automatically.

Our General Terms and Conditions of Sale (GTCS) apply to all orders (see https://www.microsens.com/fileadmin/files/downloads/Impressum/MICROSENS_AVB_EN.pdf).

Disclaimer

All information in this document is provided 'as is' and is subject to change without notice.

MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or ensuing damage.

Any product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

Document ID: DEV-EN-common-user-management_v0.5