

Smart Building Manager

Quick Start 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

1. Summary	1
1.1. Information available from the MICROSENS Website	1
1.2. Before you begin	2
2. Overview	3
3. System Requirements	4
4. Install the Application	5
4.1. Run the Install Executable	5
4.2. Choose Components	6
4.3. Choose Users	7
4.4. Choose Install Location	8
4.5. Start Server Manager	8
5. Configure Server Manager	10
6. Working with the Web UI	12
6.1. Enable Web Server	12
6.2. Start Server Process	12
6.3. Login to Web UI	13
6.4. Switching Applications	14
6.5. Discover Devices	15
6.6. Logout from Web UI	16
7. Working with the Stand-alone Client	18
7.1. Starting the Client on Windows®	18
7.2. Login via Stand-alone Client	18
7.3. Change Password for User "Super Admin"	19
7.4. Create additional Admin Users	21
7.5. Create Building Topology	22
7.6. Discover Devices for Room Automation	25
7.7. Adjust Communication Parameters for Polling Rate	26
7.8. Assign Devices to the Corresponding Node of Building Topology Tree	29
7.9. Define Data Points per Device for History Data Charts	31

1. Summary

In this document you will learn how to install, configure and use the Smart Building Manager (SBM) for room automation on Microsoft Windows® systems.

For further information about Smart Building facilities, standards, parameters and options please refer to the chapters "Apps" and "SmartOffice" in the Firmware Generation 6 product manual. This manual is included in each software archive containing firmware G6. It can also be downloaded from the link **Documentation** in the device's web manager navigation bar.

For detailed information on using Smart Building Manager please refer to Smart Building Manager user manual. This user manual is included in SBM server manager and SBM client component via **help** menu. It describes in detail on how to use Smart Building Manager properly.

1.1. Information available from the MICROSENS Website

Registered users can find the latest firmware versions as well as further information on our web site:

- Registration
 - Go to www.microsens.com
 - Click on **Login** and follow the link **Not registered?**
 - Fill in the opening email form and submit it to MICROSENS.
 - You will receive an email from MICROSENS with a user name and a password
- Login
 - Go to www.microsens.com
 - Login with your user name and password
 - Click on **Login**.
- Firmware images
 - Navigate to the device and select the tab **Services**

For further information select one of the other tabs.

NOTE | Make sure the browser allows the execution of scripts.

NOTE | After updating the firmware either by Web Manager or CLI be sure to clear the cache of the browser you are using to open the Web Manager of the respective device. This will force the browser to reload the device's updated web GUI data instead of using the outdated data from its cache.

1.2. Before you begin

In case of questions please contact your sales representative to make sure that you received the application's latest version including a valid licensing key file.

Also please check if the computer system where the application will be installed matches the system requirements. (see section [System Requirements](#))

2. Overview

This document will guide you through the following steps to properly install the MICROSENS Smart Building Manager:

1. Check the prerequisites.
2. Install the SBM software.
3. Apply a licence key file.
4. Configure the SBM Server Manager.
5. Start the SBM Server process.
6. Start the web browser and open the SBM Web UI.
7. Login via the SBM Web UI.
Alternatively, start SBM Client component and execute the steps.
8. Change the password for user "Super Admin".
9. Create an additional admin user.
10. Create the building topology.
11. Discover devices for room automation.
12. Adjust communication parameters for polling rate.
13. Assign devices to the corresponding node of building topology tree.
14. Define data points per device for history data charts.

IMPORTANT

Due to further development of the application, since version v3.0 the stand-alone client component of SBM will be deprecated and replaced by the web client operated by your web browser.

3. System Requirements

The application is designed to run on personal computers or servers with the following minimum requirements. These requirements are defined for dedicated systems.

NOTE | The application requires a 64-bit operating system.

- | | |
|---------------------------|--|
| Operating system | <ul style="list-style-type: none">• Windows 10, Linux Debian 11 (SBM, client component)• Windows Server 2016, Linux Debian 11 (SBM, server component) |
| RAM | <ul style="list-style-type: none">• 8 GB (SBM, server component)• 4 GB (SBM, client component) |
| Free disk space | <ul style="list-style-type: none">• 2 GB + 1 GB/1.000 additional managed devices (SBM, server component)• 1 GB (SBM, client component) |
| CPU | <ul style="list-style-type: none">• 3 GHz, typically 4-6 Core CPU (current Xeon Server CPU; multi-Core i7/i5 Desktop CPU) (SBM, server component)• 2 GHz, typically 4-6 Core CPU (multi-Core i7/i5 Desktop CPU) (SBM, client component) |
| Display resolution | <ul style="list-style-type: none">• at least 1280*1024• recommended: 1920*1080 |

IMPORTANT | On start-up, the installer application verifies whether the minimum system requirements are met. If this is not the case, the application installation will not start.

NOTE | Please refer also to the latest application release notes document. In case of doubt, it contains the latest installation requirements.

NOTE | For network access a network interface with TCP/IP stack must be installed and configured.

4. Install the Application

This section describes the installation process of all components of the application.

NOTE

You need administrative rights as a prerequisite to install the application's server component.

NOTE

To use the server component, a valid licence key file is required.

In order to install the application, start the provided installer utility and follow the steps described below.

NOTE

The language for the installation process depends on the language setting of the operation system. It has no influence on the language setting of the management application.

NOTE

The following steps describe the installation process on a Microsoft Windows® based system.

4.1. Run the Install Executable

The naming convention of the installer is as follows:

- MICROSENS_SBM_Installer_v2.x.y_win64.exe

On the welcome screen click the button **Next** in order to enter the licence agreement dialogue.

After reading the licence agreement click the button **I Agree** to go to the product selection dialogue.

NOTE

It is necessary to scroll down the licence agreement to the end to enable the button **I Agree**

4.2. Choose Components

With SBM there are two components available for selection:

- **Server:** Installs the server component of SBM and its respective supplements.
- **Client:** Installs the client component of SBM and its respective supplements.

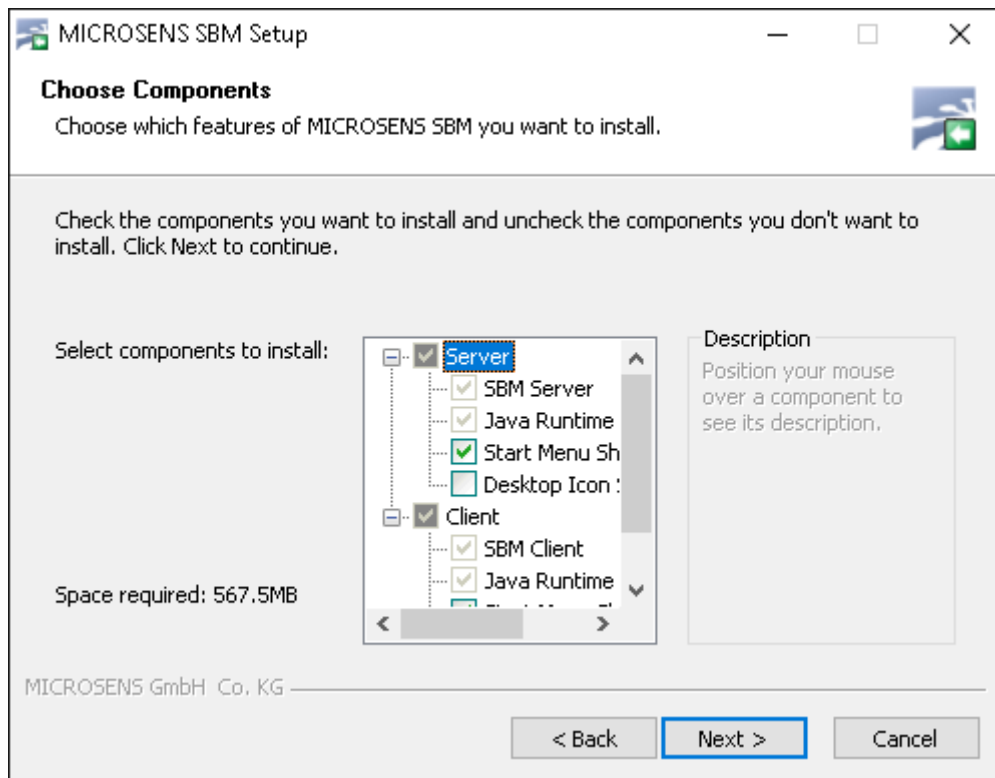


Figure 1. Choose SBM Components

Check or uncheck the components and their respective supplements for installation and hit the button **Next**.

IMPORTANT

Due to further development of the application, since version v3.0 the stand-alone client component of SBM will be deprecated and replaced by the web client operated by your web browser.

NOTE

The use of a client is mandatory to access the SBM server process. For separate installations of clients prior version v3.0 on respective computers uncheck the option "Server".

4.3. Choose Users

On the user selection screen, select the group of users who are to use this software:

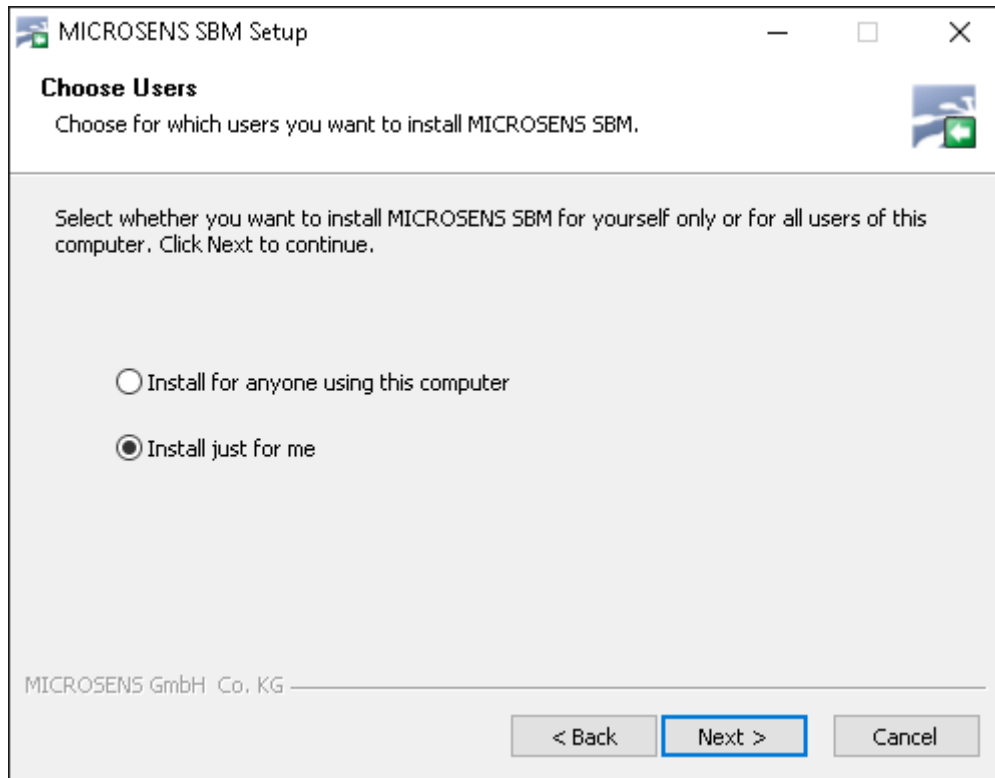


Figure 2. Choose Users

Install for anyone using this computer: Every registered user on this computer is able to use the management application after installation. This should be enabled in exceptional cases if it is ensured that only the responsible network administrator have access to this computer.

Install just for me: Only the user logged in can use the management application, whereas other users can't (default option for security reasons).

Hit the button **Next** to go to the components selection screen.

4.4. Choose Install Location

On the respective installation location screens determine the destination folders for SBM Server and SBM Client (if SBM Client installation was previously selected).

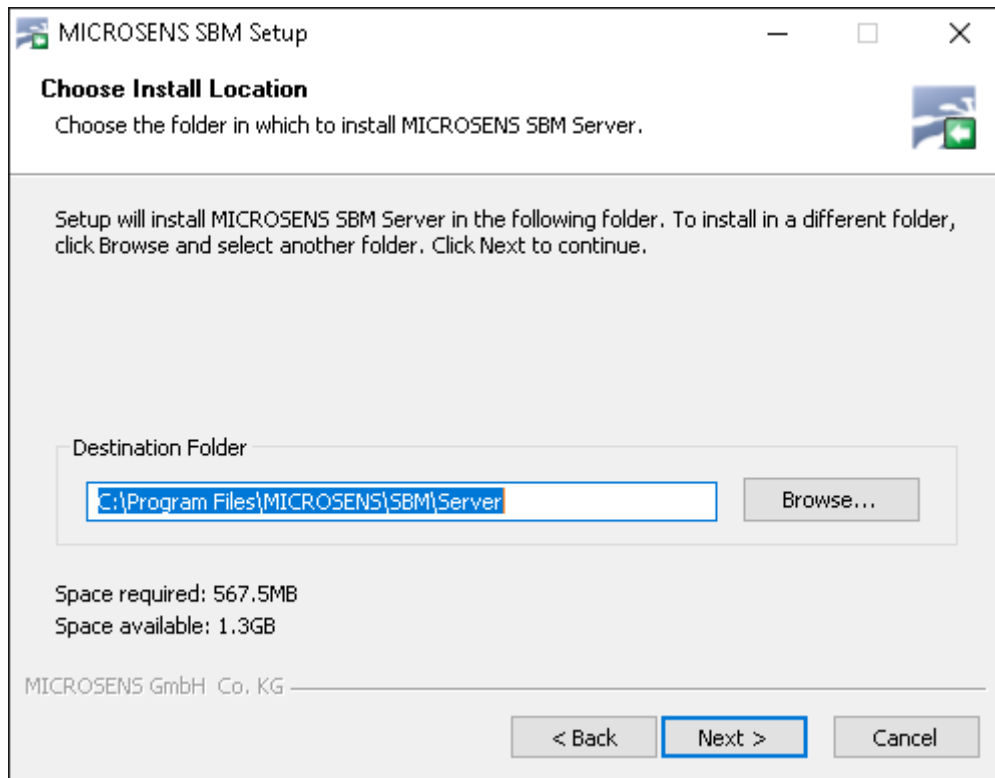


Figure 3. Choose Install Folder

Hit the button **Next** (for SBM Client installation folder, if applicable) and the button **Install** to start the installation process on the system.

When the installation process is finished successfully click the button **Finish**.

MICROSENS Smart Building Manager is ready to be started.

Unresolved directive in 00_index.adoc - include::.../..common/licensing/apply-lic-key-file.adoc[leveloffset=+1]

Unresolved directive in 00_index.adoc - include::.../..common/licensing/apply-lic-key-file_usb-dongle.adoc[leveloffset=+2]

4.5. 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 SBM Server**

or

- **Start > MICROSENS > MICROSENS SBM Server (Debug Mode)**

NOTE

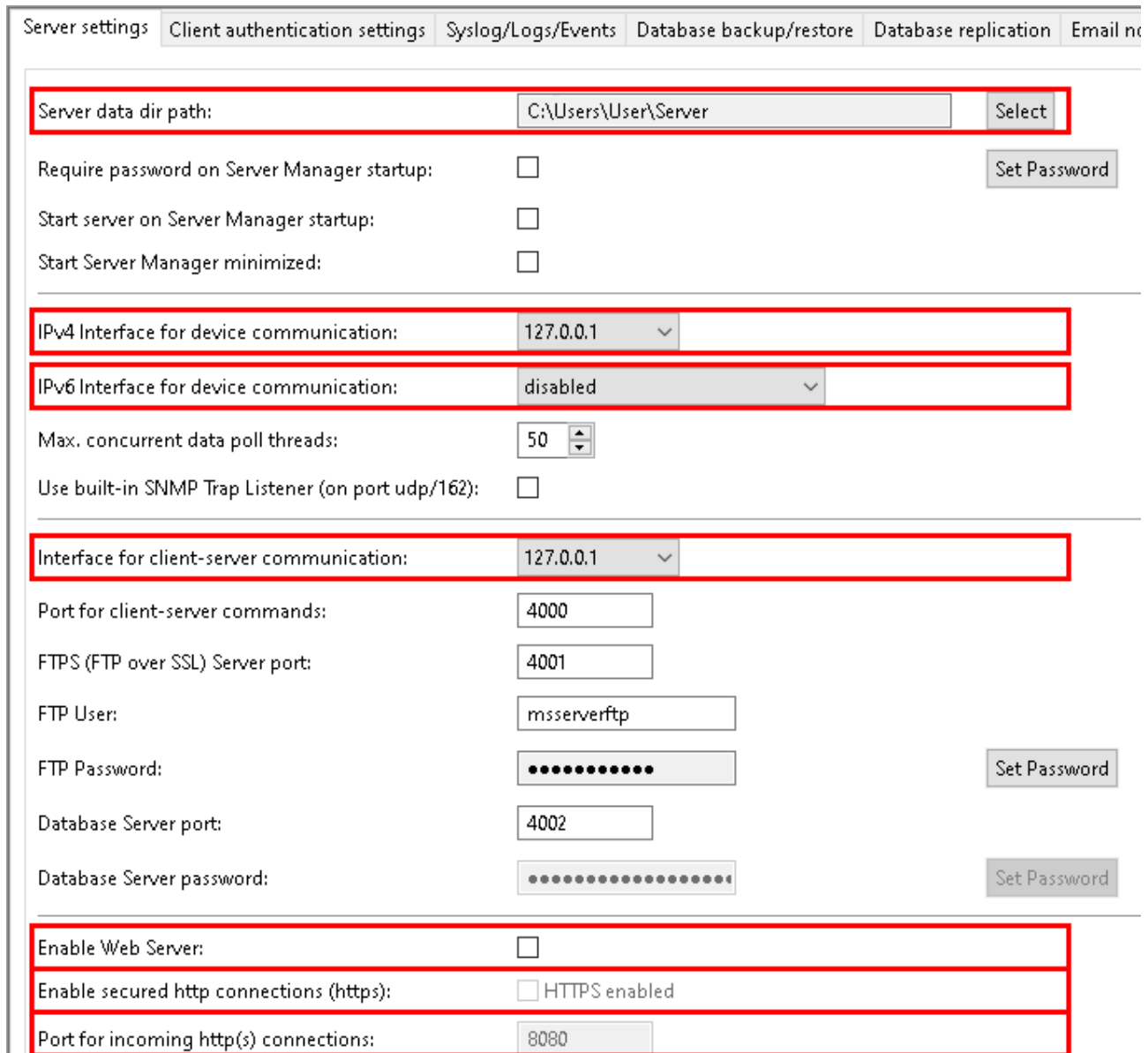
Starting the server in debug mode will open an additional Microsoft Windows® command line interface (**cmd**), where all the logs and errors will be displayed.

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

Unresolved directive in 00_index.adoc - include::.../../common/licensing/apply-lic-key-file_select.adoc[leveloffset=+2, tag=!NMP]

5. Configure Server Manager

The most important settings for first configuration are marked in the following figure:



Server settings | Client authentication settings | Syslog/Logs/Events | Database backup/restore | Database replication | Email notifications

Server data dir path: C:\Users\User\Server

Require password on Server Manager startup: ☐

Start server on Server Manager startup: ☐

Start Server Manager minimized: ☐

IPv4 Interface for device communication: 127.0.0.1 ▼

IPv6 Interface for device communication: disabled ▼

Max. concurrent data poll threads: 50 ▼

Use built-in SNMP Trap Listener (on port udp/162): ☐

Interface for client-server communication: 127.0.0.1 ▼

Port for client-server commands: 4000

FTPS (FTP over SSL) Server port: 4001

FTP User: msserverftp

FTP Password:

Database Server port: 4002

Database Server password:

Enable Web Server: ☐

Enable secured http connections (https): ☐ HTTPS enabled

Port for incoming http(s) connections: 8080

Figure 4. Server Manager - Tabbed Server Configuration Panel - Server Settings

Configure Server data directory path: Configure the directory where the server will save all necessary configuration files and database data. The default folder is: `$USER_HOME\SBM Server`

If you select a different folder, a new folder `SBM Server` will be created within.

IPv4 Interface for device communication: The IPv4 address of the network interface that will be used for communication with the managed devices. In a more complex network infrastructure where the server hardware has more than one network adapter, it is possible to use one interface (accessible exclusively from secured local network) for device communication and another one (accessible from external net-

work) for client access. Thanks to this function the clients do not have direct access to managed devices. The devices can be accessed exclusively through the server.

IPv6 Interface for device communication: The IPv6 address of the network interface that will be used for communication with the managed devices.

Interface for client-server communication: The IPv4 address of the network interface that will be used for access via client component. If the HTTP server is enabled for Web Client access, the interface is also used by the built-in HTTP server.

Enable HTTP Web Server: Enables or disables the built-in HTTP server that is used for Web Client access.

IMPORTANT

Due to further development of the application, since version v3.0 the stand-alone client component of the application will be deprecated and replaced by the web client operated by your web browser. It is mandatory for application's version v3.0 and newer to enable the HTTP web server!

Enable secured http connections (https): The server offers secured HTTP connections for web access. The https connections are encrypted so the communication between clients and server is safe. It is recommended to enable HTTPS for all installations.

Port for incoming http(s) connections: The port that will be used for the HTTP(S) server. On default the server uses the 8443 for HTTPS connections.

NOTE

See also the application's Configuration Guide for a detailed description of the Server Manager configuration.

6. Working with the Web UI

6.1. Enable Web Server

1. On the tab **Server Settings** of the server manager enable the option **Enable Web Server**.
2. It is recommended to enable **secured HTTP connections (HTTPS)**.
3. As long as it does not prove necessary, leave the default **Port for incoming http(s) connections** (8443) as is.

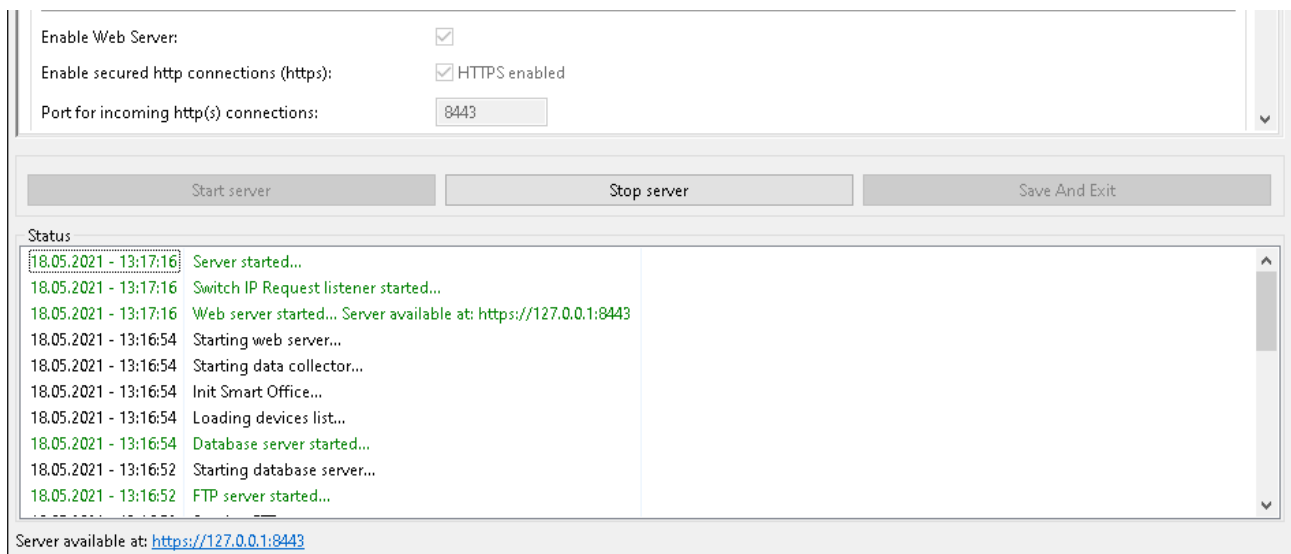


Figure 5. SBM Server Manager - Configuring and Starting the Web Server

After enabling the required HTTP(S) service and starting the server instance, a web browser can be used to access the server with one of the following URL addresses.

For standard HTTP connections

`http://<server_ip_address>:<http_server_port>/`

For secured HTTP connections, if the secured HTTP was configured

`https://<server_ip_address>:<https_server_port>/`

NOTE

You will find the linked URL also at the bottom of the Server Manager window.

6.2. Start Server Process

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

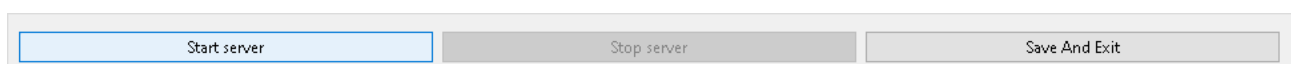


Figure 6. Server Manager - Start Server Process

If the server process was started successfully, you should see **Server started...** as last

message on top of the status field as follows:

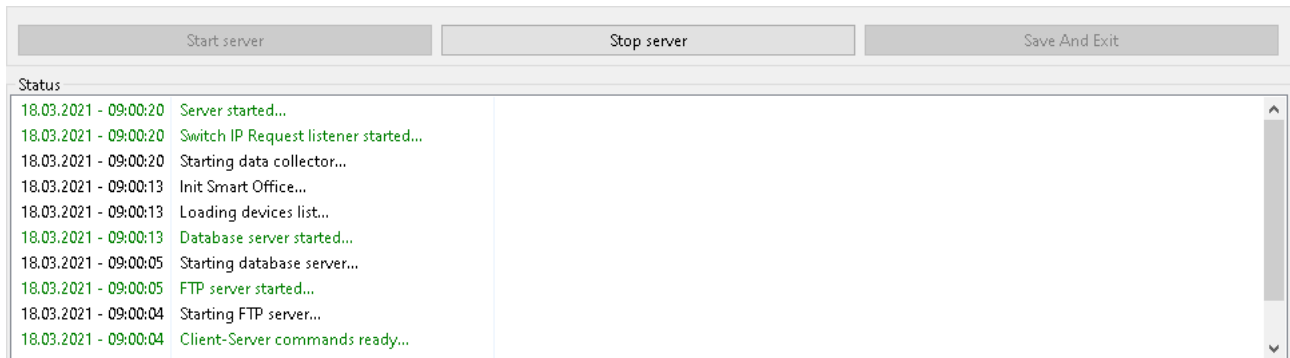


Figure 7. Server Manager - Status Field

6.3. Login to Web UI

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.

NOTE

For a valid list of user accounts ask the responsible system administrator. Additionally, if you are using the stand-alone client yet, change to the perspective **Window > Switch Perspective > User Administration** to find a list of available user accounts.

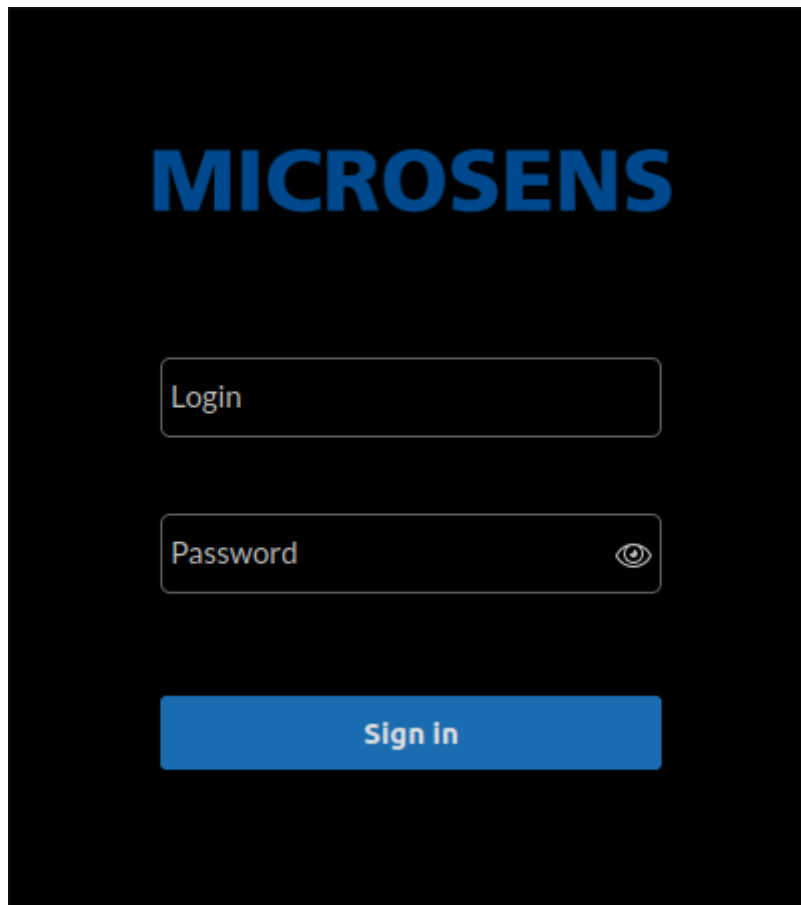


Figure 8. WEB UI - Login Screen

NOTE

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

- Building Management
- 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.

6.4. Switching Applications

1. Logout of the active application by selecting **<user>** > **Select app** from the drop-down menu on the top right of the web UI.

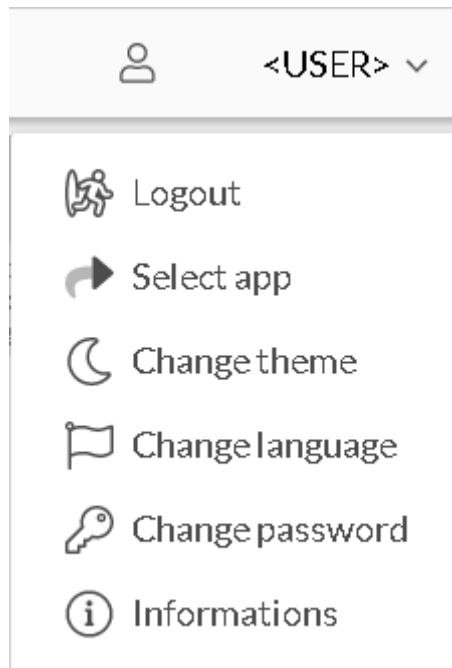


Figure 9. Web UI - User Menu

- The tiles of all available applications appear.

NOTE

Depending on the user's access level, the web UI opens with several application tiles. If you do not see one or more of these tiles you do not have the respective access level for this application.

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

- The respective application's start page opens.

Unresolved directive in 00_index.adoc - include:../common/user-management/web_usermanagement_change-password-adminuser.adoc[leveloffset=+2, tag=!NMP]

Unresolved directive in 00_index.adoc - include:../common/user-management/web_usermanagement_create-additional-admin-users.adoc[leveloffset=+2, tag=!NMP]

Unresolved directive in 00_index.adoc - include:../common/web/review-building-summary.adoc[leveloffset=+2]

Unresolved directive in 00_index.adoc - include:../common/web/create-building-topolgy.adoc[leveloffset=+2]

6.5. Discover Devices

NOTE

Administrator access rights are essential for using device management!

1. If not already active, change to the device management application.

2. Change to **Devices** > **Auto discovery**.

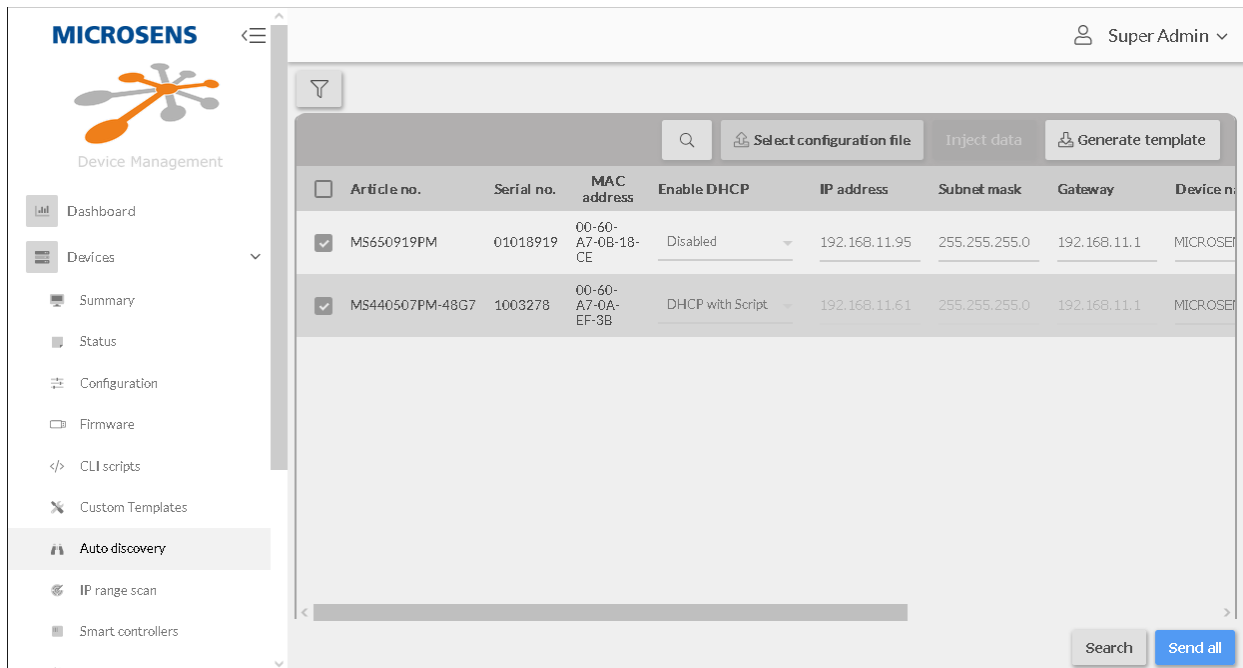


Figure 10. Web UI - Device Management - Devices - Auto Discovery

- A tabular overview of already detected devices is shown in the right-hand pane.

3. Click on the button **Search** to start auto discovery.

- The client starts to search for devices in the corporate network.

NOTE

Discovery could take some time, depending on the size of the network.

4. After the discovery scan is finished all additionally found devices are listed in the tabular overview.

- Review the list of detected devices.
- Check all devices in the first column that should be part of your device list.
- All selected devices will be added to the device list automatically.

Unresolved directive in 00_index.adoc - include::.../common/web/review-history-charts.adoc[leveloffset=+2]

6.6. Logout from Web UI

1. Logout of the active application by selecting **<user>** > **Logout** from the drop-down menu.

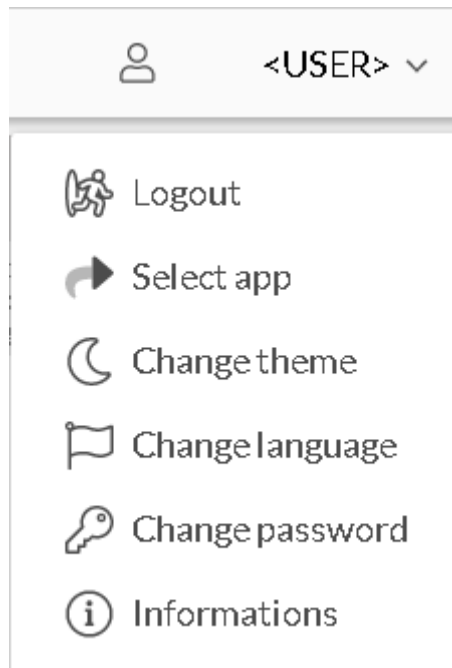


Figure 11. Web UI - User Menu

- The login dialogue appears.

7. Working with the Stand-alone Client

7.1. Starting the Client on Windows®

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

Start > MICROSENS > MICROSENS SBM Client

or

Start > MICROSENS > MICROSENS SBM Client (Debug mode)

NOTE

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

The stand-alone client opens with its login dialogue.

7.2. Login via Stand-alone Client

Login into the client with valid user credentials.

At the very first time please login with the following credentials:

- Login: Super Admin
- Password: Super Admin

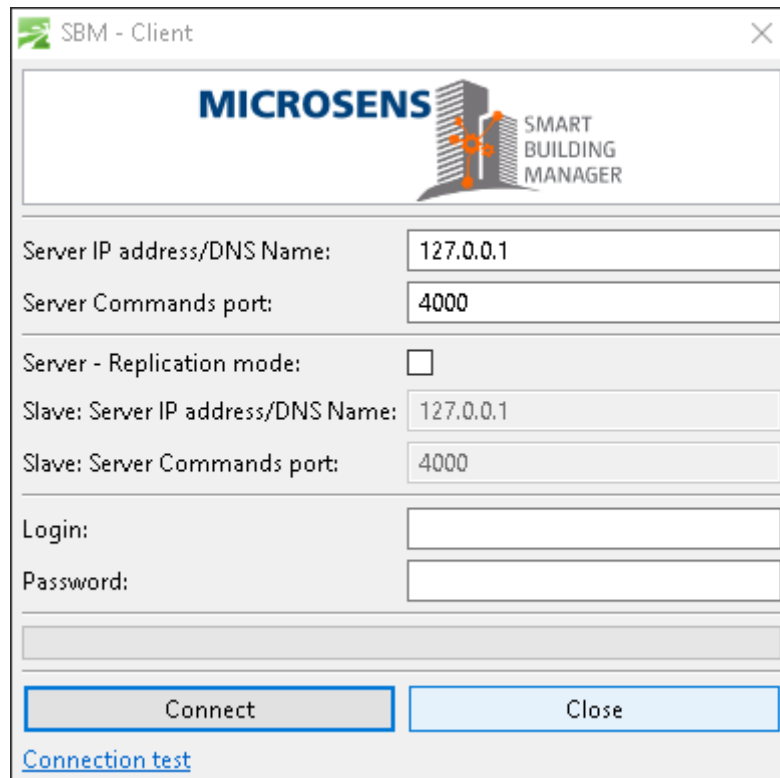


Figure 12. Stand-alone Client - Login

IMPORTANT

For security reasons it is strongly recommended to change the credentials for this user after first login!

7.3. Change Password for User "Super Admin"

IMPORTANT

Due to security reasons it is strongly recommended to change all default passwords, especially for the user "Super Admin"!

1. Change to the menu entry **Window > Switch Perspective** and click on the entry **User Administration**.

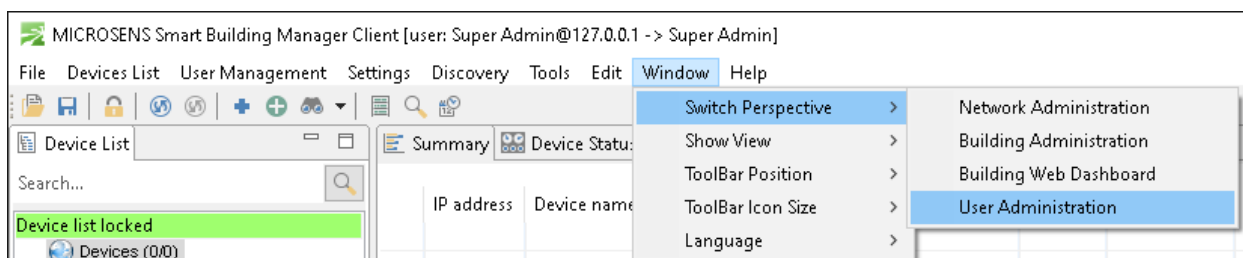


Figure 13. SBM Client - Window - Switch Perspective - User Administration

2. Click on the key lock icon right below the main menu bar on the upper left to unlock user list.

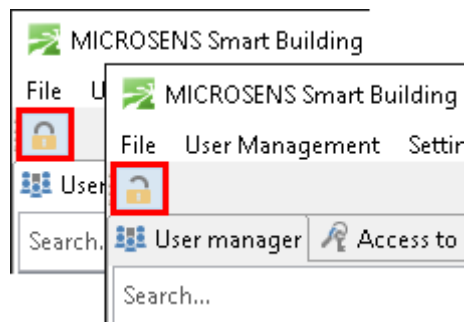


Figure 14. SBM Client - User Administration - Unlock User List

- The lock icon changes to an "open lock" symbol.
3. On the tab **User Manager** select the user with the name "Super Admin" and click the edit icon.

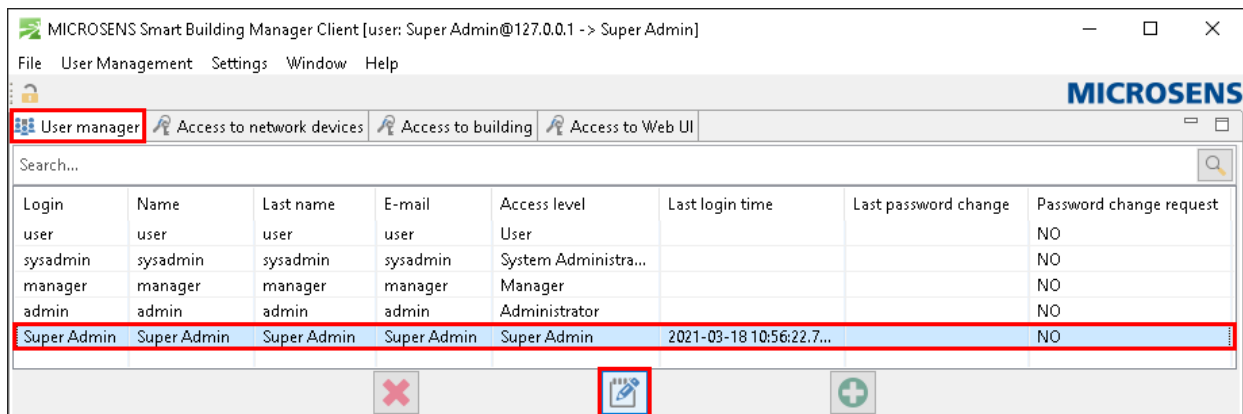


Figure 15. SBM Client - User Administration - Select User

- The user properties dialogue opens up.
4. Set the new password, retype it and click on the button **Apply**.

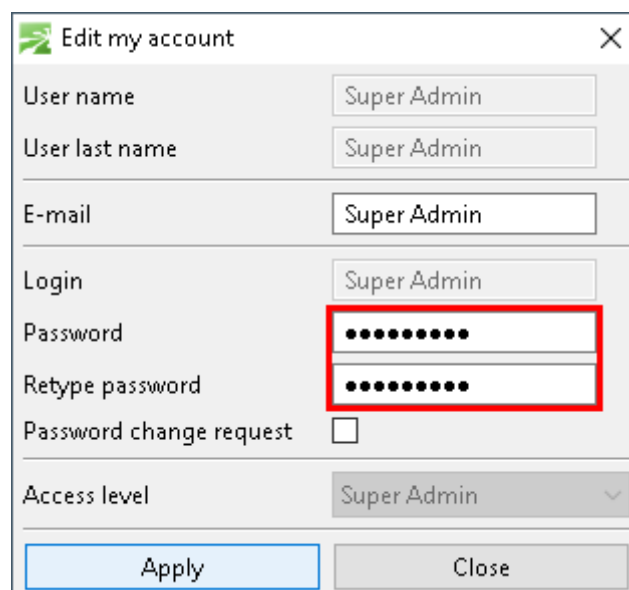


Figure 16. SBM Client - User Administration - Edit User

- Finally click on the "open lock" icon on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.4. Create additional Admin Users

NOTE

It is strongly recommended to add additional users with Smart Building Administrator access rights.

- If the user administration is not already active, change to the menu entry **Window** > **Switch Perspective** and click on the entry **User Administration**.
- Click on the key lock icon (🔒) right below the main menu bar on the upper left:

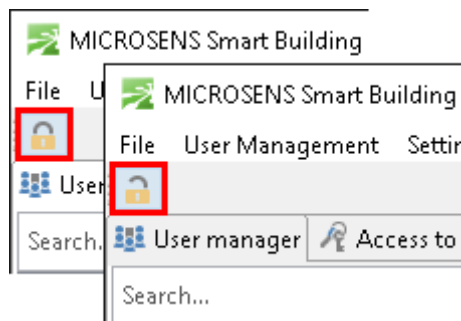


Figure 17. SBM Client - User Administration - Unlock User List

- Now the lock icon changes to an "open lock" symbol.
- Hit the button **+** to add a user. The user properties dialogue opens, where you can enter the new users data and credentials.

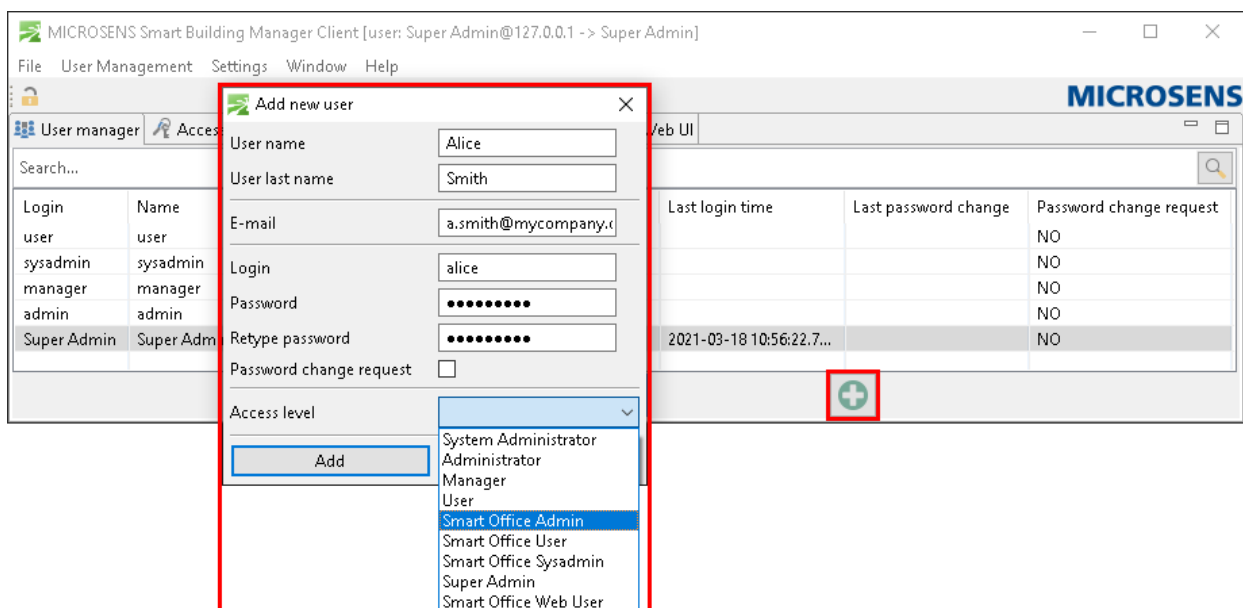


Figure 18. SBM Client - User Administration - Add New User

- Enter name, last name and e-mail address.
- Enter credentials (login name and password).

- From the drop down list select the entry "Smart Office Admin" as access level.
4. Hit the button **Add** to create the new user.
 5. Finally click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.5. Create Building Topology

1. Change to the menu entry **Window > Switch Perspective** and click on the entry **Building Administration**.

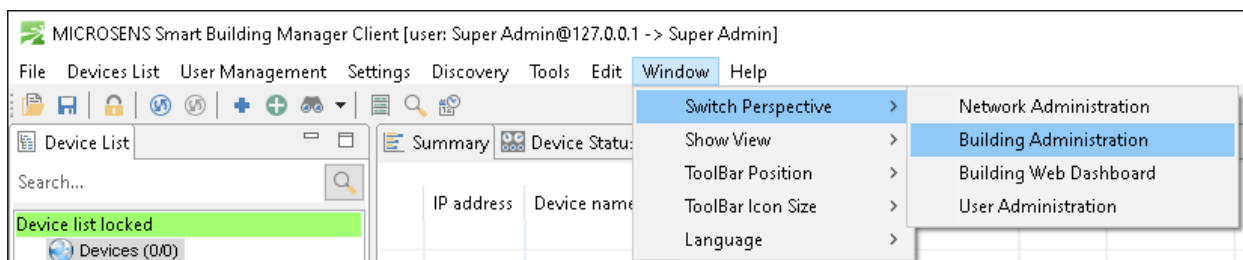


Figure 19. SBM Client - Window - Switch Perspective - Building Administration

2. Click on the key lock icon (🔒) right below the main menu bar on the upper left.

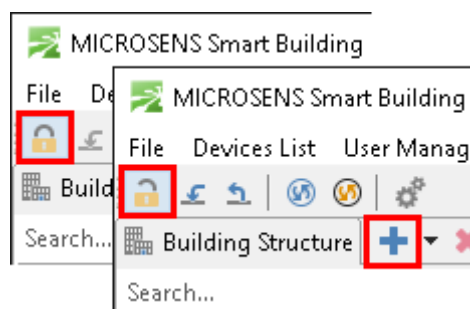


Figure 20. SBM Client - Building Administration - Unlock Smart Office Configuration

With a fresh SBM Client installation the building structure is empty. The following steps will guide you to create a building structure with the following hierarchical structure:

- Location
 - Building
 - Room Automation
 - Floor
 - Room
3. Hit the button **+** to add a location.
 4. In the opening dialogue enter the name of the new location.

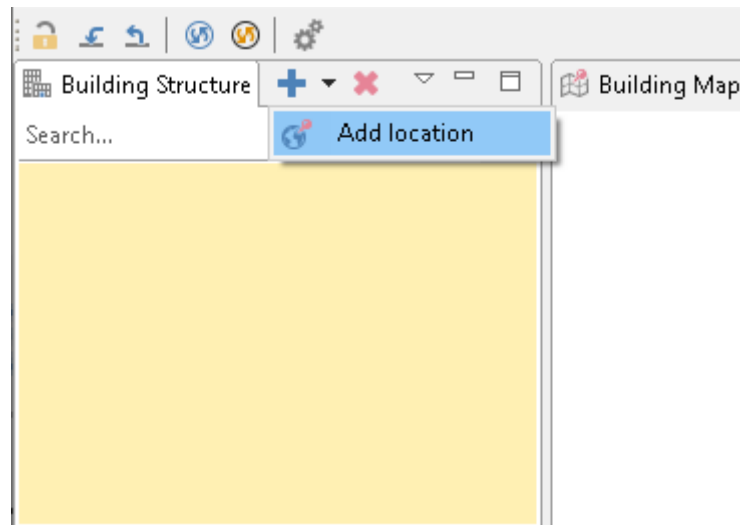



Figure 21. SBM Client - Building Administration - Add Location

5. Select the created location and hit the button  to add a building. In the opening dialogue enter the name of the new building.

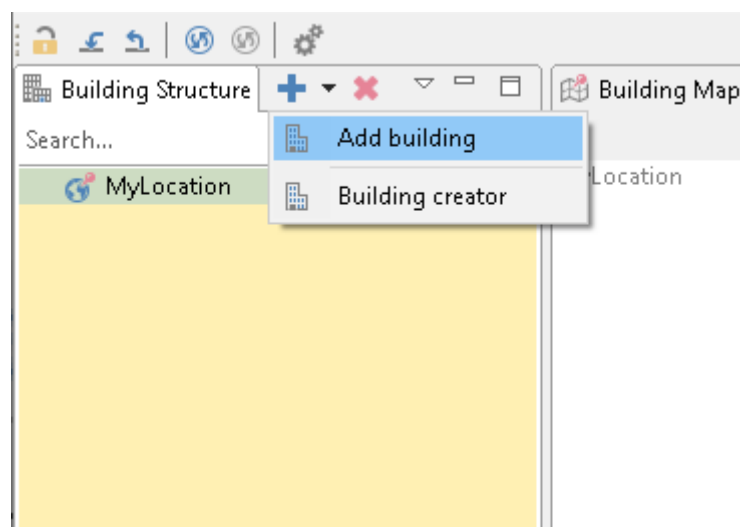



Figure 22. SBM Client - Building Administration - Add Building

6. After the building was created expand the building node and select the node with the name "Room automation". Hit the button  to add a floor. In the opening dialogue enter the name of the new floor.

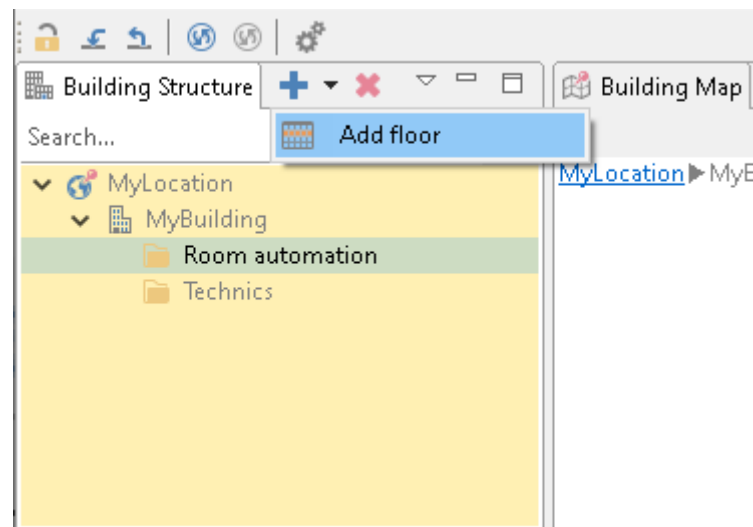



Figure 23. SBM Client - Building Administration - Structure

7. Select the created floor and hit the button  to add one or more rooms. In the opening dialogue enter the name of the new room.

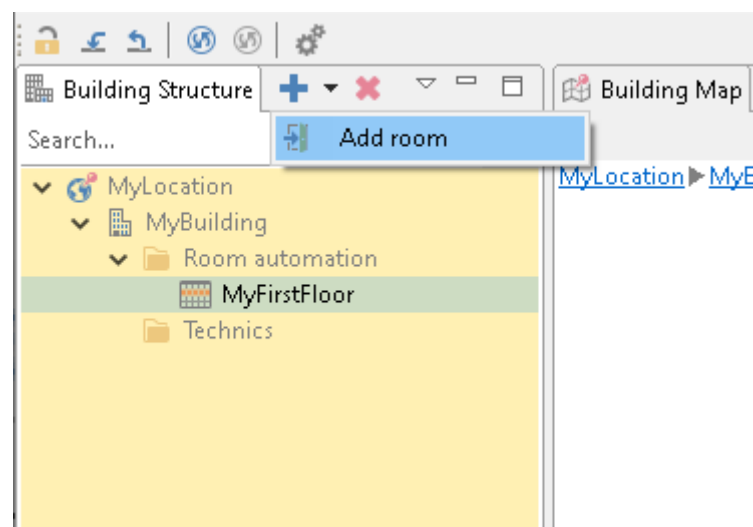


Figure 24. SBM Client - Building Administration - Add Room

- The resulting building topology tree now should look like this.

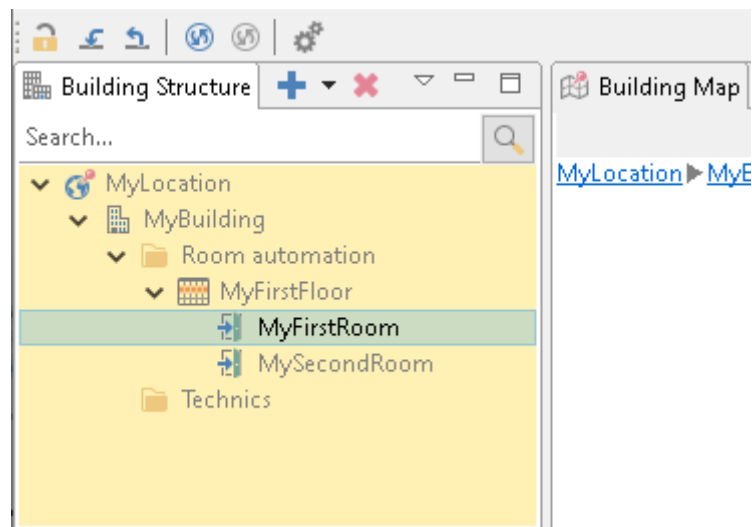


Figure 25. SBM Client - Building Administration - Structure

8. Finally click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.6. Discover Devices for Room Automation

1. Change to the menu entry **Window > Switch Perspective** and click on the entry **Network Administration**.

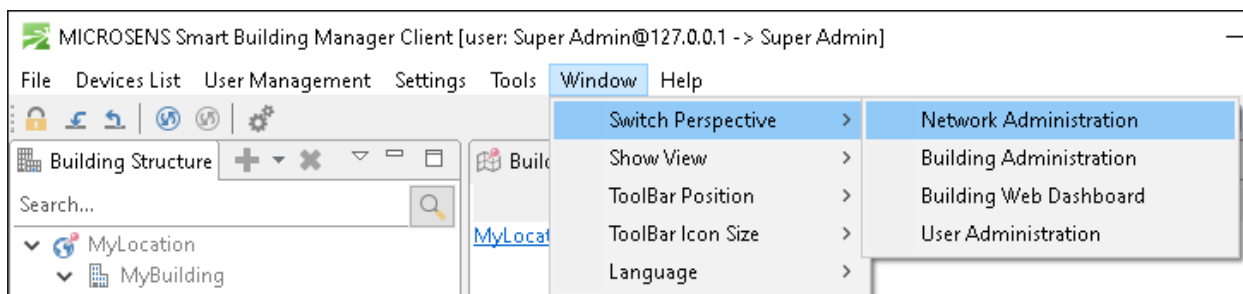


Figure 26. SBM Client - Window - Switch Perspective - Network Administration

2. Click on the key lock icon (🔑) right below the main menu bar on the upper left:

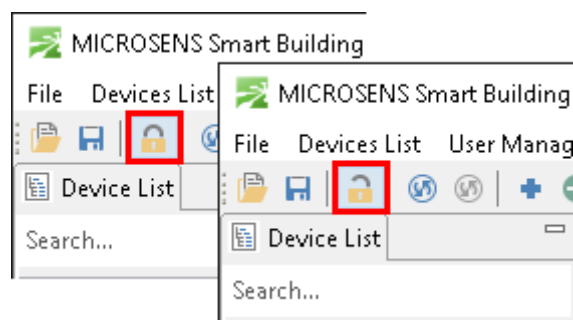


Figure 27. SBM Client - Network Administration - Unlock Configuration

3. Click on the entry **Discovery > Device auto discovery** to start auto discovery.

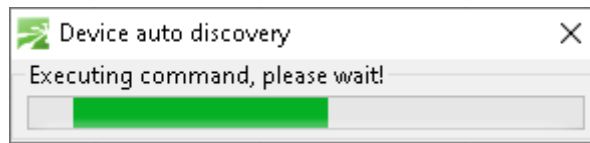


Figure 28. SBM Client - Network Administration - Discovery - Device Auto Discovery

- SMB Client starts to search for devices in the corporate network.

NOTE

Discovery takes some time. As long as the discovery is running you will see the green progress bar.

- After the discovery scan is finished you will see a separate dialogue which contains the list of the detected devices.

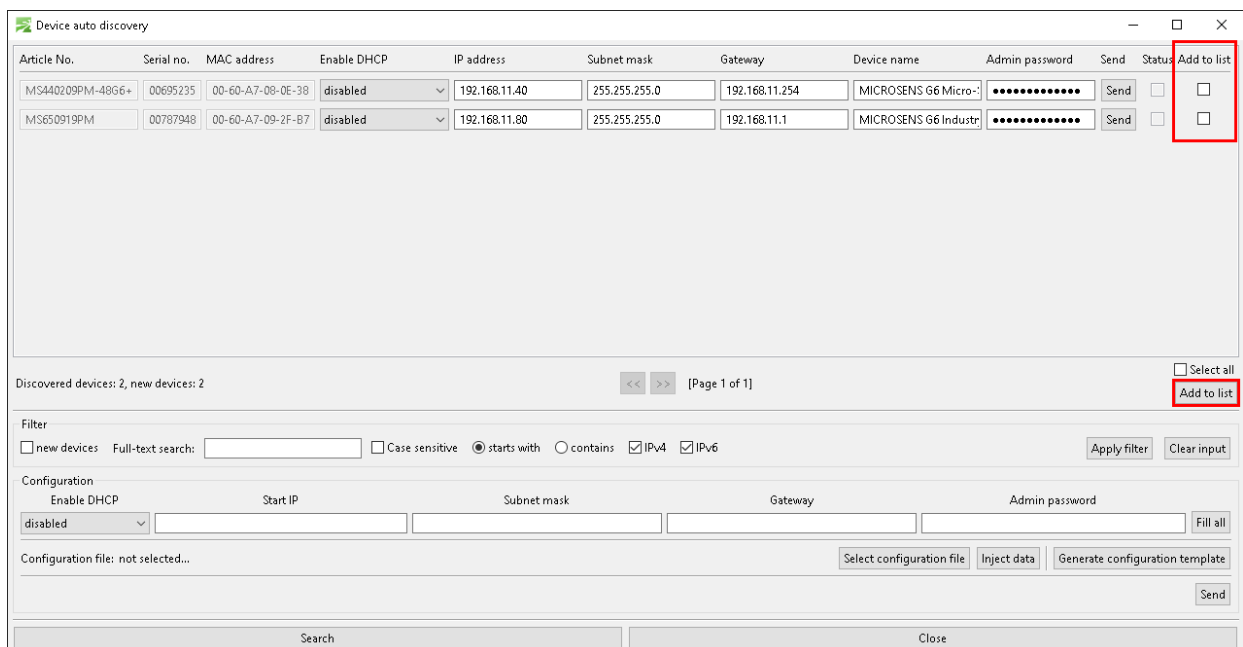


Figure 29. SBM Client - Network Administration - Device Auto Discovery - Results

- Review the list of detected devices.
 - Check all devices in the column "Add to list" that should be part of your device list.
 - Afterwards hit the button **Add to list**.
- Hit the button **Close** to close the dialogue. All checked devices are now part of the device list. You will find the discovered devices in the building structure under the node **Scan results > Device auto-discovery**.
 - Finally click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.7. Adjust Communication Parameters for Polling Rate

- If the network administration is not already active change to the menu entry **Window > Switch Perspective** and click on the entry **Network Administration**.

2. Click on the key lock icon (🔒) right below the main menu bar on the upper left:

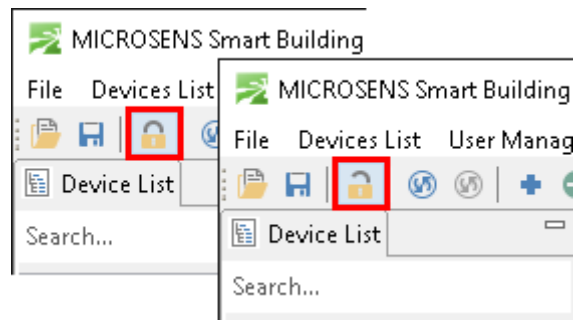


Figure 30. SBM Client - Network Administration - Unlock Configuration

3. Select the building structure node "Devices", open the context menu with a left mouse click and select the menu item **Add new Subgroup**.

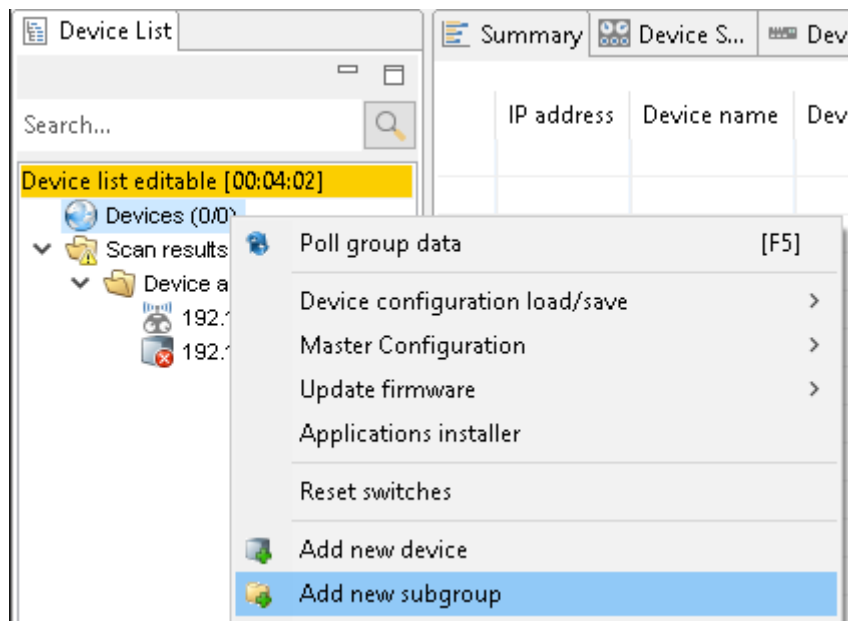


Figure 31. SBM Client - Network Administration - Devices Context Menu - New Subgroup

4. Define the name of the new device group. This device group is used as a container which contains all devices in which you are interested on.
5. Afterwards use drag & drop to assign a device from the "Device auto-discovery" group to your new group.
6. Select the node name of your group and do a right mouse click to open the context menu.

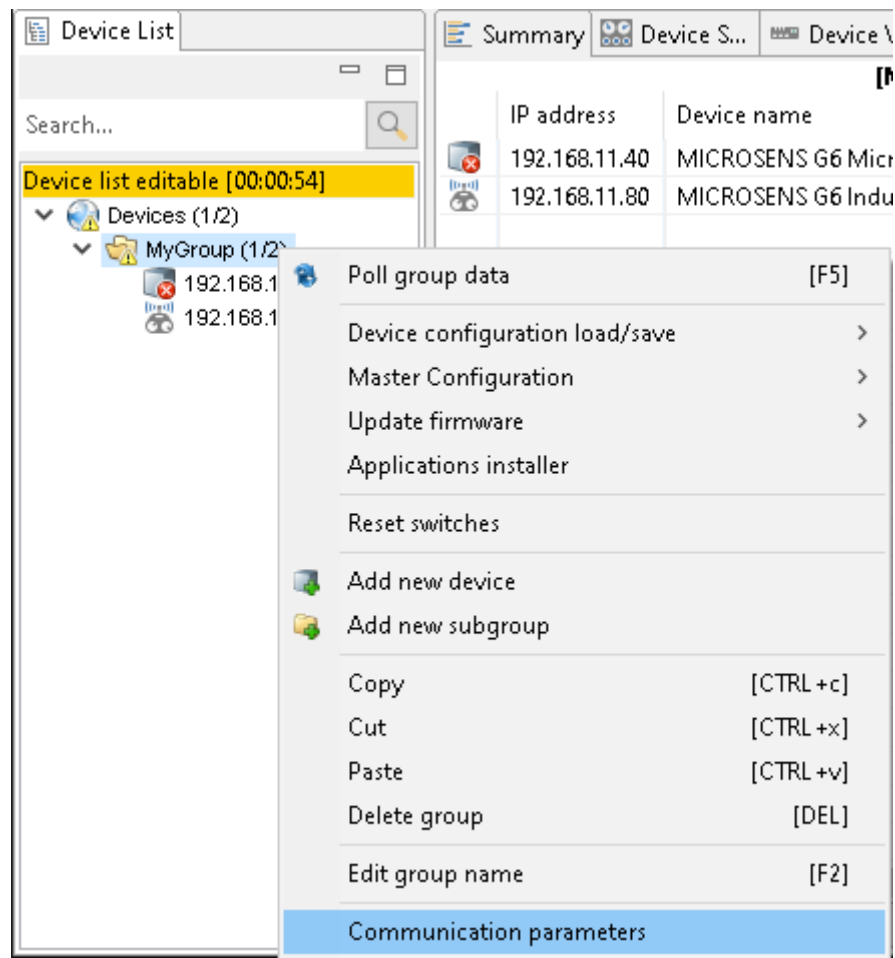


Figure 32. SBM Client - Network Administration - Devices Context Menu - Communication Parameters

- Click on the menu item **Communication parameters** to open the configuration dialogue. At the bottom of the dialogue you see the parameter setting for the polling.

Please set the parameters as shown in the following figure and hit the button **Apply**.

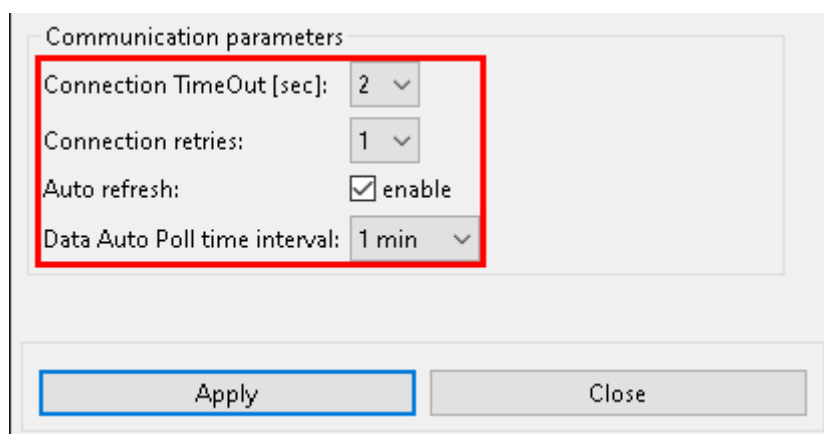


Figure 33. SBM Client - Network Administration - Devices - Communication Parameters

8. Finally click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.8. Assign Devices to the Corresponding Node of Building Topology Tree

1. Change to the menu entry **Window > Switch Perspective** and click on the entry **Building Administration**.

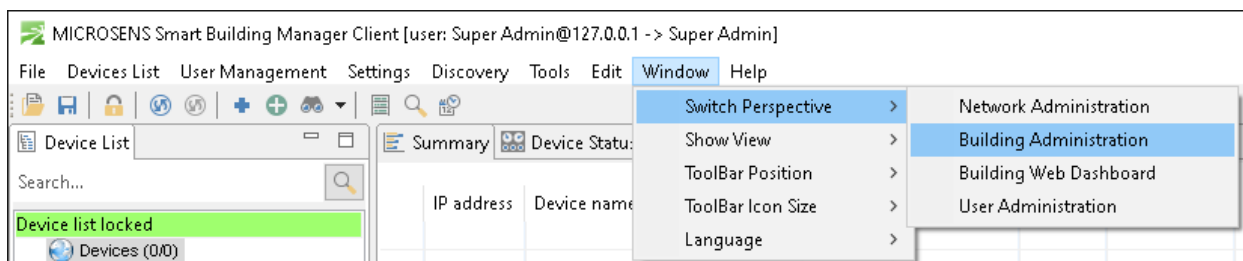


Figure 34. SBM Client - Switch Perspective - Building Administration

2. Click on the key lock icon (🔒) right below the main menu bar on the upper left:

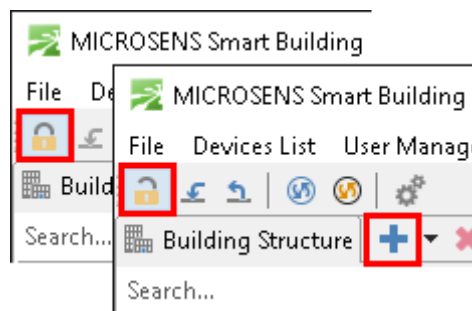


Figure 35. SBM Client - Building Administration - Unlock Configuration

- All devices found in the previous step are listed in the section "Devices" below the section "Building Structure".
3. From this list select a device and assign this device to a building node using "drag and drop" with a left mouse click.

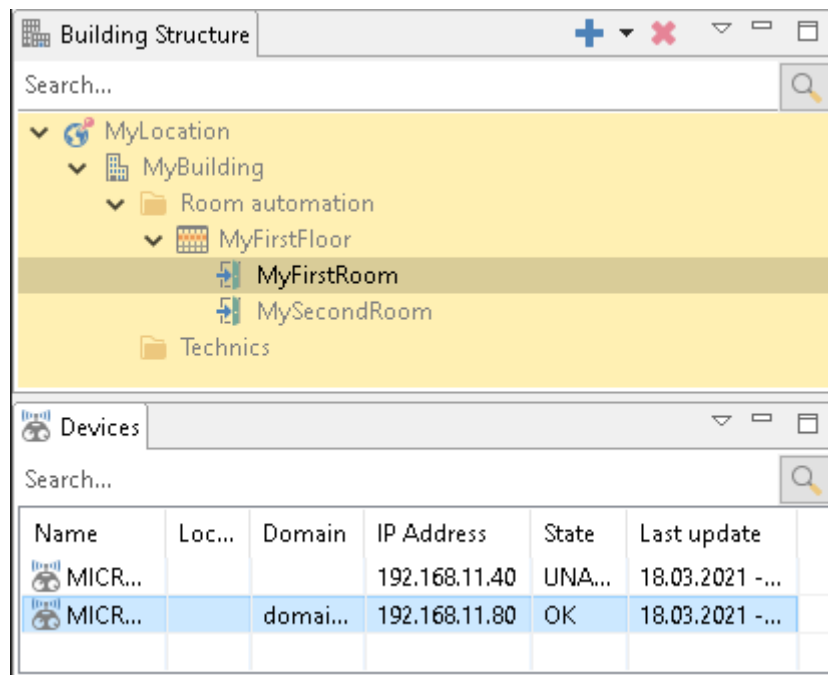


Figure 36. SBM Client - Device List with unassigned Devices

NOTE

This step is important because you need to add a context to each device. This means that you need to define which device is responsible for which building part.

If you drop the device (release the left mouse button) on a building node, the device will be assigned. The assigned device is shown as a sub-node of the building node:

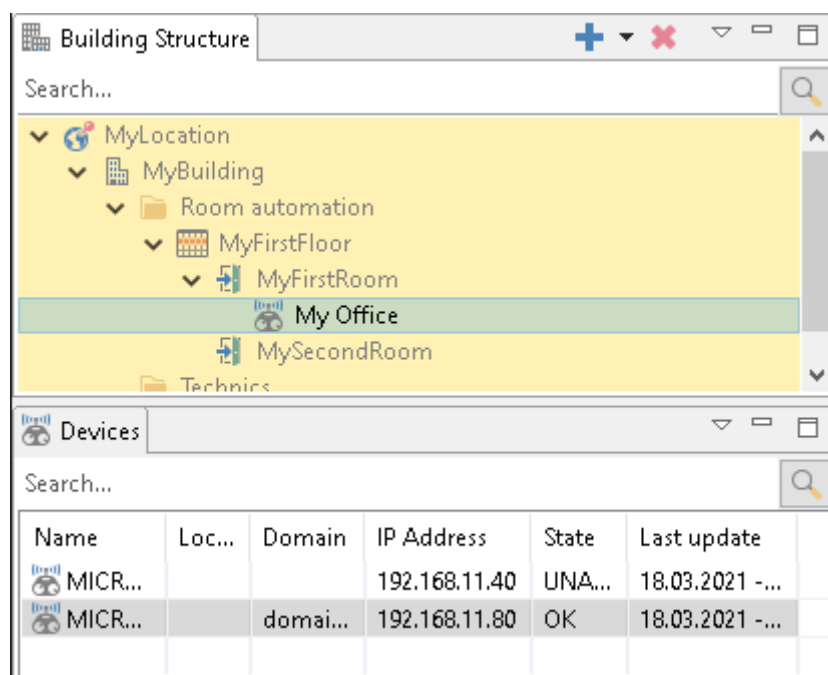


Figure 37. SBM Client - Device Assigned to Node

- Continue until all needed devices are assigned to their specific building node.

NOTE

A node can contain multiple devices but a device can only be assigned to one node.

- Finally click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

7.9. Define Data Points per Device for History Data Charts

- If the building administration is not already active change to the menu entry **Window > Switch Perspective** and click on the entry **Building Administration**.
- Click on the key lock icon (🔓) right below the main menu bar on the upper left.

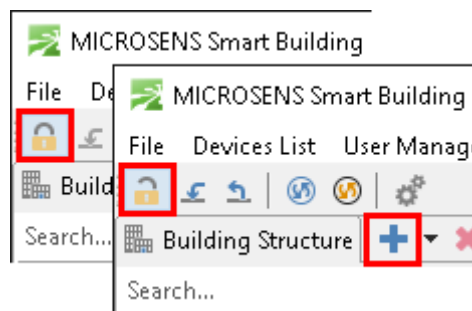


Figure 38. SBM Client - Building Administration - Unlock Configuration

- Select the device of a building tree node where you want to see history data charts.

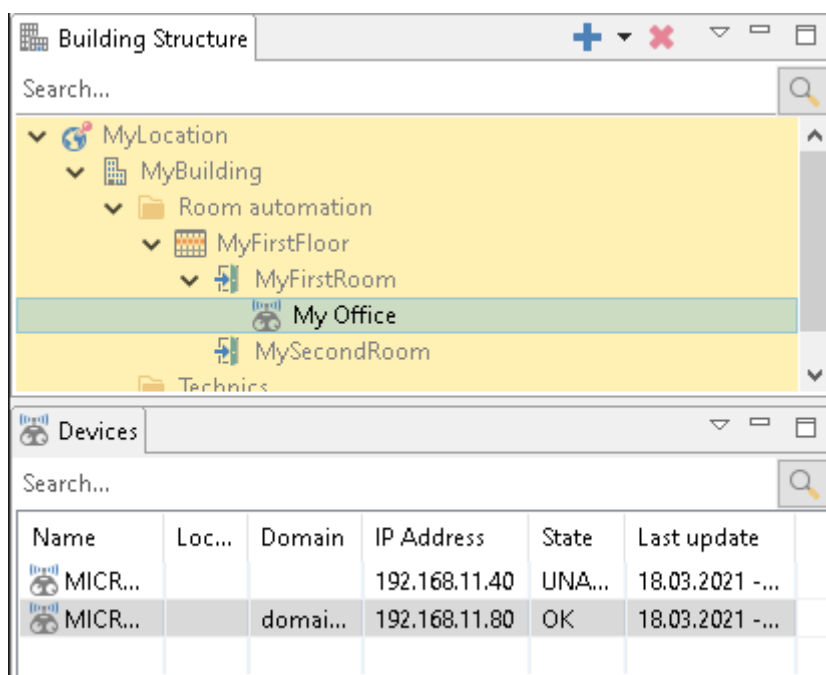


Figure 39. SBM Client - Select Device for Monitoring History Data

- Go to the Tab **Data points** at the right hand side to see a list of all data points of a

single device. You should see a list like in the following figure:

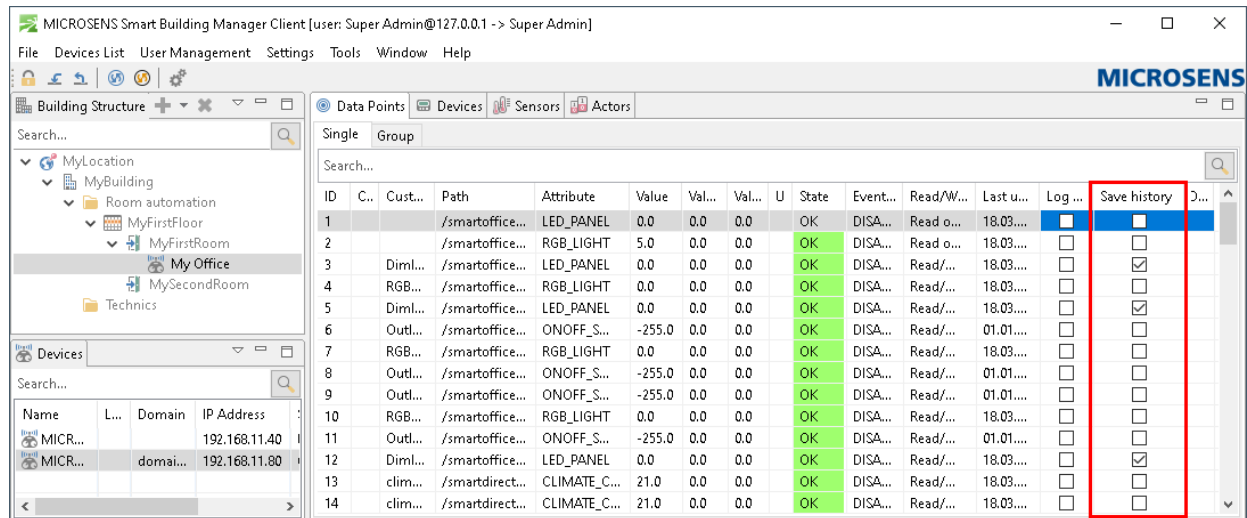


Figure 40. SBM Client - Building Administration - Data Points

5. To mark specific data points for history data double-click the respective checkbox in the column Save history.
6. Click on the "open lock" icon (🔓) on the upper left to submit the changes to SBM Server. The lock icon changes to a "closed lock" symbol.

Our [General Terms and Conditions of Sale \(GTCS\)](https://www.microsens.com/fileadmin/files/downloads/Impressum/MICROSENS_AVB_EN.pdf) 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.

©2022 MICROSENS GmbH & Co. KG, Kueferstr. 16, 59067 Hamm, Germany.

All rights reserved. This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG.

Document ID: QSG-EN-20008_Smart-Building-Manager_v1.3