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

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
 - $\,\circ\,$ 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.
- 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	tion requires a 64-bit operating system.
Operating system	 Windows 10, Linux Debian 11 (SBM, client component) Windows Server 2016, Linux Debian 11 (SBM, server component)
RAM	 8 GB (SBM, server component)
	 4 GB (SBM, client component)
Free disk space	 2 GB + 1 GB/1.000 additional managed devices (SBM, server component)
	 1 GB (SBM, client component)
CPU	 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	• at least 1280*1024
	 recommended: 1920*1080
IMPORTANT mun	start-up, the installer application verifies whether the mini- n system requirements are met. If this is not the case, the ication 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 set- ting of the operation system. It has no influence on the language set- ting of the management application.
NOTE	The following steps describe the installation process on a Microsoft Windows $^{\mbox{\tiny B}}$ 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 \mathbf{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.

MICROSENS SBM Setup	 The mathematical mathemat								
Choose Components Choose which features of MICROSENS SBM you want to install.									
Check the components you wa install. Click Next to continue.	nt to install and uncheck the comp	onents you do	n't want I	to					
Select components to install:	Server SBM Server SBM Server Java Runtime Start Menu Sh Desktop Icon : Client SBM Client	Description Position you over a comp see its desci	onent to						
Space required: 567.5MB	Java Runtime								
MICROSENS GmbH Co., KG	< Back	Next >	Cal	ncel					
	L DOCK	NOXC 2							

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:

MICROSENS SBM Setup	_		×
Choose Users Choose for which users you want to install MICROSENS SBM.			
Select whether you want to install MICROSENS SBM for yourself only or computer. Click Next to continue.	for all us	ers of th	nis
 Install for anyone using this computer Install just for me 			
MICROSENS GmbH Co. KG ———————————————————————————————————	>	Car	icel

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).

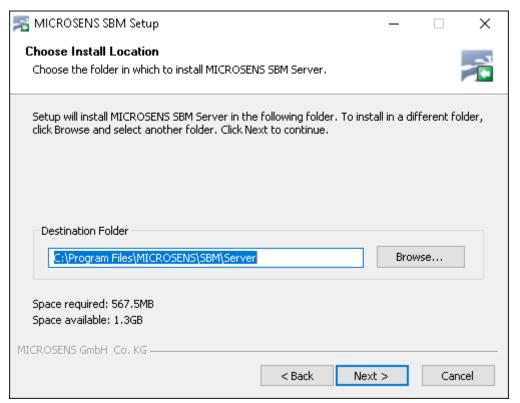


Figure 3. Choose Install Folder

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 $\mathsf{Windows}^{\texttt{®}}$ 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/L	.ogs/Events	Datab	ase backup/res	tore D	latabase re	eplication	Email n
Server data di	r path:		C:\Users\Use	er\Sen	ver			Select]
Require passw	vord on Server Manager startup:							Set Pass	word
Start server or	n Server Manager startup:								
Start Server M	anager minimized:								
IP∨4 Interface	for device communication:		127.0.0.1	~]
IP∨6 Interface	for device communication:		disabled		~]
Max. concurre	ent data poll threads:		50 🜲						
Use built-in SI	NMP Trap Listener (on port udp/	(162):							
Interface for c	lient-server communication:		127.0.0.1	~					
Port for client	-server commands:		4000						
FTPS (FTP ove	r SSL) Server port:		4001						
FTP User:			msserverftp						
FTP Password	:		•••••	••				Set Pass	word
Database Serv	er port:		4002						
Database Serv	er password:		•••••					Set Pass	word
Enable Web S	erver:]
Enable secure	d http connections (https):		🗌 HTTPS ena	bled					
Port for incon	ning 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.

Enable Web Server: Enable secured http Port for incoming ht	connections (https):	ATTPS enabled 8443			*			
	Start server	Stop	server	Save And Exit				
Status								
18.05.2021 - 13:17:16	Server started				^			
18.05.2021 - 13:17:16	Switch IP Request listener started							
18.05.2021 - 13:17:16	Web server started Server available	e at: https://127.0.0.1:8443						
18.05.2021 - 13:16:54	Starting web server							
18.05.2021 - 13:16:54	Starting data collector							
18.05.2021 - 13:16:54	Init Smart Office							
18.05.2021 - 13:16:54	05.2021 - 13:16:54 Loading devices list							
18.05.2021 - 13:16:54	3:16:54 Database server started							
18.05.2021 - 13:16:52	6:52 Starting database server							
18.05.2021 - 13:16:52	2021 - 13:16:52 FTP server started							
Server available at: http:	s://127.0.0.1:8443							

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>/

ΝΟΤΕ

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.

Start server	Stop server	Save And Exit

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:

	Start server	Stop server	Save And Exit
Status			
18.03.2021 - 09:00:20	Server started		
18.03.2021 - 09:00:20	Switch IP Request listener started		
18.03.2021 - 09:00:20	Starting data collector		
18.03.2021 - 09:00:13	Init Smart Office		
18.03.2021 - 09:00:13	Loading devices list		
18.03.2021 - 09:00:13	Database server started		
18.03.2021 - 09:00:05	Starting database server		
18.03.2021 - 09:00:05	FTP server started		
18.03.2021 - 09:00:04	Starting FTP server		
18.03.2021 - 09:00:04	Client-Server commands ready		

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.

MICROSE	NS
Login	
Password	0
Sign in	

Figure 8. WEB UI - Login Screen

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

- Building Management
- Device Management

NOTE • 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 dropdown menu on the top right of the web UI.

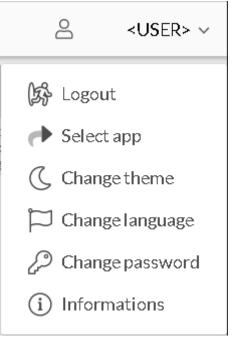


Figure 9. Web UI - User Menu

 $\,\circ\,$ The tiles of all available applications appear.

ΝΟΤΕ

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-buildingsummary.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.

MICROSENS	<=									A Super	Admin ~
-*		Y]								
Device Management						Q 🟦 Sel	ecto	onfiguration file		ය Generate te	emplate
-			Artícle no.	Seríal no.	MAC address	Enable DHCP		IP address	Subnet mask	Gateway	Device
Dashboard	~		MS650919PM	01018919	00-60- A7-0B-18- CE	Disabled	Ŧ	192.168.11.95	255.255.255.0	192.168.11.1	MICROS
📮 Summary			M5440507PM-48G7	1003278	00-60- A7-0A- EF-3B	DHCP with Script					MICROS
, Status											
‡ Configuration											
📼 Fîrmware											
CLI scripts											
🗙 Custom Templates											
Auto discovery											
Ø IP range scan											
Smart controllers		1<									

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.

```
ΝΟΤΕ
```

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.
 - $\,\circ\,$ 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-historycharts.adoc[leveloffset=+2]

6.6. Logout from Web UI

 Logout of the active application by selecting <user> > Logout from the dropdown menu.

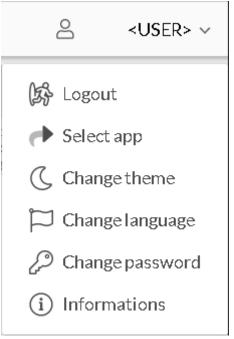


Figure 11. Web UI - User Menu

• 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 $\mathsf{Windows}^{\texttt{®}}$ 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

💈 SBM - Client 🛛 🕹 🗙							
MICROSENS							
Server IP address/DNS Name:	127.0.0.1						
Server Commands port:	4000						
Server - Replication mode:							
Slave: Server IP address/DNS Name:	127.0.0.1						
Slave: Server Commands port:	4000						
Login:							
Password:							
Connect	Close						
Connection test							

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**.

🗾 MICROSENS Smart Building Manager Client [user: Super Admin@127.0.0.1 -> Super Admin]								
File Devices List User Manage	ement Settings	Discovery	Tools	Edit	Window	Help		
🗎 🗛 🛛 🚳 🐼 🛛 🕈 🚭) 🛲 🗕 🗐 C	L			Swite	h Perspective	>	Network Administration
🗄 Device List		Summary 🔛	Device	Statu:	Shov	v View	>	Building Administration
Search	Q				Tooll	Bar Position	>	Building Web Dashboard
N. S. PALAT		IP address	Devic	e name	Tooll	Bar Icon Size	>	User Administration
Device list locked Oevices (0/0)					Lang	uage	>	
Eiguro 12 Cl	DM Cliant	Minda		C :	hab Day	an a ativa	1100	r 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.



🗾 МІС	NICROSENS Smart Building								
File U	🗾 MICROSENS Smart Building								
6	File User Management Settir								
🏭 User	<u></u>								
Search, 🌉 User manager 🖉 Acces									
	Search								

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.

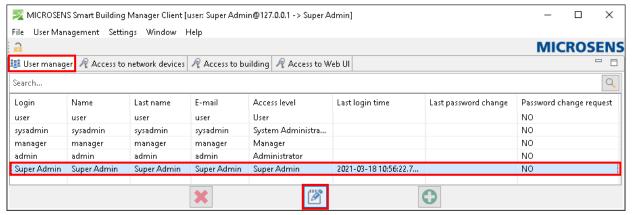


Figure 15. SBM Client - User Administration - Select User

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

🗾 Edit my account	×
User name	Super Admin
User last name	Super Admin
E-mail	Super Admin
Login	Super Admin
Password	•••••
Retype password	•••••
Password change request	
Access level	Super Admin \sim
Apply	Close

Figure 16. SBM Client - User Administration - Edit User

MICROSENS

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.

7.4. Create additional Admin Users



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

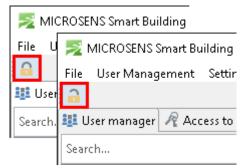


Figure 17. SBM Client - User Administration - Unlock User List

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

File User Mar	nagement S	ettings Window Help				
<u>_</u>		🗾 Add new user	×			MICROSEN
🔢 User manag	jer 🧖 Acces	User name	Alice	veb UI		- 6
Search		User last name	Smith			Q
Login	Name			Last login time	Last password change	Password change request
user	user	E-mail	a.smith@mycompany.c			NO
sysadmin	sysadmin	Login	alice			NO
manager	manager	-				NO
admin	admin	Password	•••••			NO
Super Admin	Super Adm	Retype password	•••••	2021-03-18 10:56:22.7		NO
		Password change request		-	-	
		Access level	~	-	0	
			System Administrator			
		Add	Administrator			
			Manager	μ		
			User Smart Office Admin			
			Smart Office User			
			Smart Office Sysadmin			
			Super Admin			
			Smart Office Web User			

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

- Enter name, last name and e-mail address.
- $\,\circ\,$ 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 (a) 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**.

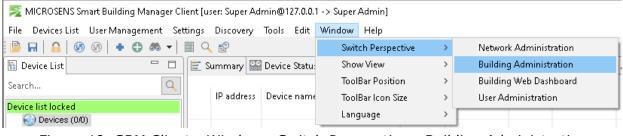


Figure 19. SBM Client - Window - Switch Perspective - Building Administration

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

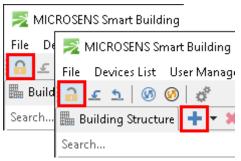


Figure 20. SBM Client - Building Administration - Unlock Smart Office Configuration

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.



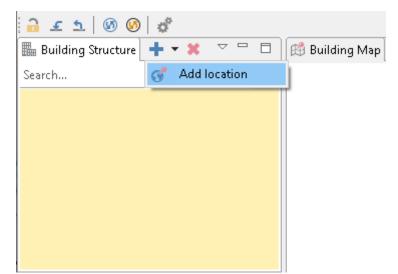


Figure 21. SBM Client - Building Administration - Add Location

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

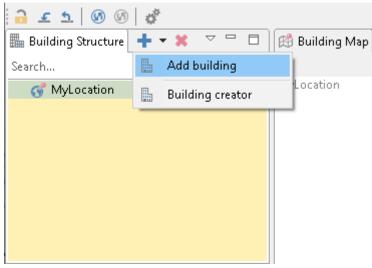


Figure 22. SBM Client - Building Administration - Add Building

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.



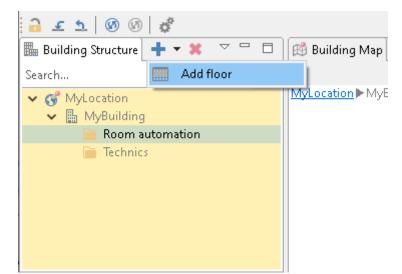


Figure 23. SBM Client - Building Administration - Structure

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.

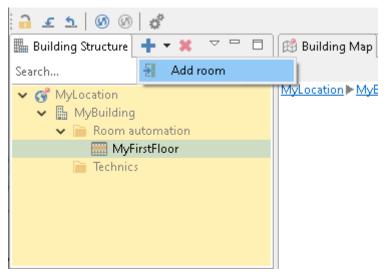


Figure 24. SBM Client - Building Administration - Add Room

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

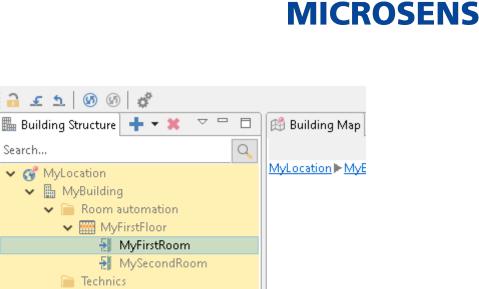


Figure 25. SBM Client - Building Administration - Structure

8. Finally click on the "open lock" icon (a) 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**.

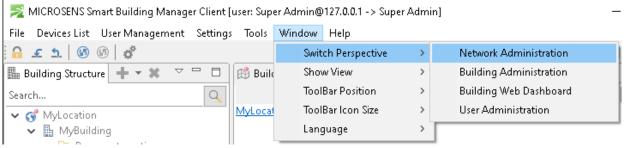


Figure 26. SBM Client - Window - Switch Perspective - Network Administration

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

🗾 MICROSENS Smart Building							
File Devices Li	🗾 MICROSENS Smart Building						
🖹 🖻 🖬 🔒	File Devices List User Manag						
🗄 Device List	🗎 🖬 🔒 🚳 🖉 + (
Search	🗄 Device List						
	Search						

Figure 27. SBM Client - Network Administration - Unlock Configuration

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



🗾 Device auto discovery	×
Executing command, please wait!	

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

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

```
ΝΟΤΕ
```

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

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

Article No.	Serial no.	MAC address	Enable DHCP		IP address	Subnet mask	Gateway	Device name	Admin password	Send	Statu	s Add to lis
MS440209PM-48G6+	00695235	00-60-A7-08-0E-38	disabled	~	192.168.11.40	255.255.255.0	192.168.11.254	MICROSENS G6 Micro-:	•••••	• Send		
MS650919PM	00787948	00-60-A7-09-2F-B7	disabled	~	192.168.11.80	255.255.255.0	192.168.11.1	MICROSENS G6 Industr	•••••	• Send		
												□ Select a
Discovered devices: 2, r	ew devices:	2				<< >> [Page 1 of 1]					Select a
	ew devices: :	2				<< >> [Page 1 of 1]					
Filter		2	Case	sensitiv	e () starts with (<< >>> [⊃contains ☑IPv4 ☑	-			Apply fil	lter	
)iscovered devices: 2, r Filter □ new devices Full- Configuration		2	Case	sensitiv	e () starts with (-			Apply fil	lter	Add to lis
Filter Prew devices Full- Configuration Enable DHCP	text search:	2 	Case	sensitiv	e () starts with () Subnet mas) contains	-		Admin pase		lter	Add to li: Clear input
Filter new devices Full- Configuration Enable DHCP			Case	sensitiv) contains	 IP∨6		Admin pass		lter	Add to lis
Filter new devices Full- Configuration Enable DHCP disabled	text search:		Case	sensitiv) contains	 IP∨6	Select configuration file				Add to lis
Filter new devices Full- Configuration Enable DHCP	text search:		Case	sensitiv) contains ☑ IPv4 ☑	 IP∨6	Select configuration file		word		Add to lis

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

- Review the list of detected devices.
- $\circ\,$ 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.
- 6. Finally click on the "open lock" icon (a) 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 (\bigcirc) right below the main menu bar on the upper left:

🗾 MICROSENS Smart Building							
File Devices List	🗾 MICROSENS Smart Building						
🖻 🖬 🔒 🎯	File Devices List User Manag						
🗄 Device List	🕒 🖬 🔒 🐼 🐼 + 🤅						
Search	🗄 Device List 📃 🗖						
	Search						

MICROSENS

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**.

🗄 Device List		💽 Summary		Device S		Dev	
Search		IP add	ress	Device nar	ne	Dev	
Device list editable [00:	04:02]						
 Oevices (0/0) ✓ ¹/₂ Scan results 	Poll group	Poll group data [
✓ ⁽) Device a ⁽) 192. ¹	Device con	Device configuration load/save					
	Master Cor	Master Configuration Update firmware					
	Update firn						
	Application	Applications installer					
	Reset switc	Reset switches					
	Add new d	evice					
	🖡 Add new si	ibgroup					

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.



📓 Device List			💽 S	ummary 🔛 De	evice S	📟 Device \	
						٩]	
Search		Q		IP address	Device	name	
Device list editable (00:00	Device list editable [00:00:54]			192.168.11.40	MICRO:	SENS G6 Micr	
V R Devices (1/2)	7.04j		6	192.168.11.80	MICRO:	SENS G6 Indu	
🗸 🦏 MyGroup (1/2		Poll gro	up dat	а		[F5]	
🛣 192.168.1		Device	onfig	uration load/sav	'e	>	
		Master	Config	uration		>	
		Update firmware				>	
		Applications installer					
		Reset switches					
	4	Add new device					
	i	Add new subgroup					
		Сору	Сору			[CTRL+c]	
		Cut			[CTRL+x]	
		Paste			[CTRL+v]	
	D	Delete g	group		[DEL]		
		Edit gro	oup name			[F2]	
		Commu	unicati	on parameters			

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

7. 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.

I.	Communication parameters		
	Connection TimeOut [sec]:	2 🗸	
	Connection retries:	1 ~	
	Auto refresh:	🗹 enable	
	Data Auto Poll time interval:	1 min 🗸 🗸	
	Apply		Close

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



8. Finally click on the "open lock" icon (a) 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**.

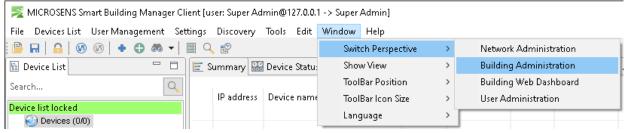


Figure 34. SBM Client - Switch Perspective - Building Administration

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

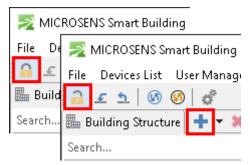


Figure 35. SBM Client - Building Administration - Unlock Configuration

- $^\circ\,$ 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.



闘 Building S	tructure			+ •	• 🗶 🔻 🗖					
Search	Search									
 ✓ Image MyLocation ✓ Image MyBuilding ✓ Image Room automation ✓ Image MyFirstFloor 										
		MyFirstRo								
	72) Techni	MySecond cs	IKOOM							
器 Devices					~					
Search					Q					
Name	Loc	Domain	IP Address	State	Last update					
😹 MICR			192.168.11.40	UNA	18.03.2021					
😹 MICR		domai	192.168.11.80	ОК	18.03.2021					

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:

🏨 Building S	Structure			+ -	• 🗶 🗢 🗖							
Search												
 ✓ Image MyLocation ✓ Image MyBuilding ✓ Image MyFirstFloor ✓ Image MyFirstFloor ✓ Image MyFirstRoom 												
My Office MySecondRoom Units of the second se												
Devices												
Search												
Name 🚟 MICR	Loc	Domain	IP Address 192.168.11.40	State UNA	Last update 18.03.2021							
😹 MICR		domai	192.168.11.80	ОК	18.03.2021							

Figure 37. SBM Client - Device Assigned to Node



4. 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.

5. Finally click on the "open lock" icon (a) 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.
- 2. Click on the key lock icon (\bigcirc) right below the main menu bar on the upper left.

\mathbb{N}	міс	ROSENS Smart Building
File	De	🗾 MICROSENS Smart Building
	£	File Devices List User Manag
🖩 В	uild	
Sear	ch	🌆 Building Structure 📑 🔫 🕷
		Search

Figure 38. SBM Client - Building Administration - Unlock Configuration

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

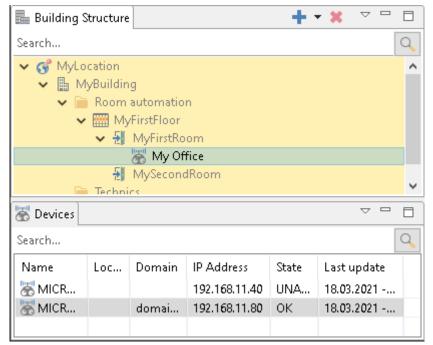


Figure 39. SBM Client - Select Device for Monitoring History Data

4. 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:

🗾 MICROSENS Smart Building Manager Client [user: Super Admin@127.0.0.1 -> Super Admin]												- 0	×							
File Devices List User Management Settings Tools Window Help																				
🔒 🖌 💁	6	60 🖉																	MICRO	SENS
🌆 Building	Struct	ure 🕂 🔻	X \bigtriangledown \square		💿 Da	ata P	oints 🚍	Devices 🔊 Ser	nsors 👪 Actor:	s										- 8
Search					Single Group															
✓ G ^o MyLocation					Sear	Search														
 MyBuilding Room automation 				ID	C	Cust	Path	Attribute	Value	Val	Val	U	State	Event	Read/W	Last u	Log	Save history	D 🔨	
V IIII MyFirstFloor				1			/smartoffice	LED_PANEL	0.0	0.0	0.0		OK	DISA	Read o	18.03				
✓ ₩ MyFirstRoom				2			/smartoffice	RGB_LIGHT	5.0	0.0	0.0		ОК	DISA	Read o	18.03				
🚟 My Office				3		Diml	/smartoffice	LED_PANEL	0.0	0.0	0.0		ОК	DISA	Read/	18.03		\checkmark		
🛃 MySecondRoom				4		RGB	/smartoffice	RGB_LIGHT	0.0	0.0	0.0		OK	DISA	Read/	18.03				
📄 Technics				5		Diml	/smartoffice	LED_PANEL	0.0	0.0	0.0		OK	DISA	Read/	18. 0 3		\checkmark		
				6		Outl	/smartoffice	ONOFF_S	-255.0	0.0	0.0		ОК	DISA	Read/	01.01				
품 Devices	evices 🗸 🖓 🗖				7		RGB	/smartoffice	RGB_LIGHT	0.0	0.0	0.0		ОК	DISA	Read/	18.03			
Search			Q	8		Outl	/smartoffice	ONOFF_S	-255.0	0.0	0.0		ОК	DISA	Read/	01.01				
				~	9		Outl	/smartoffice	ONOFF_S	-255.0	0.0	0.0		ОК	DISA	Read/	01.01			
Name	L	Domain	IP Address		10		RGB	/smartoffice	RGB_LIGHT	0.0	0.0	0.0		ОК	DISA	Read/	18.03			
🚟 MICR			192.168.11.4	0 1	11		Outl	/smartoffice	ONOFF_S	-255.0	0.0	0.0		ОК	DISA	Read/	01.01			
😹 MICR		domai	192.168.11.8	0 1	12		Diml	/smartoffice	LED_PANEL	0.0	0.0	0.0		ОК	DISA	Read/	18.03		\checkmark	
					13		clim	/smartdirect	CLIMATE_C	21.0	0.0	0.0		ОК	DISA	Read/	18.03			
<	< >			>	14		clim	/smartdirect	CLIMATE_C	21.0	0.0	0.0		OK	DISA	Read/	18.03			~

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 (a) 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) apply to all orders (see https://www.microsens.com/fileadmin/files/downloads/Impressum/MICROSEN-S_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