

Smart Building Manager

Server Configuration 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. System Requirements	3
3. Administrative Prerequisites	4
4. General Security Recommendations	5
5. Start Server Manager	6
5.1. Server Manager Main Window	6
6. Server Configuration via Server Manager	8
6.1. Server Settings	8
6.1.1. General	8
6.1.2. Device Communication	9
6.1.3. Client-Server Communication	9
6.1.4. Web Server	10
6.1.5. Fidelio/FIAS	10
6.1.6. Device Discovery	11
6.1.7. WiFi Access Point Management Bridge	11
6.2. Client Authentication Settings	12
6.2.1. Authentication Selection	12
6.2.2. RADIUS Settings	12
6.3. Syslog/Logs/Events	14
6.3.1. Syslog Server (Receive Syslogs)	14
6.3.2. Syslog Client (Send Syslogs)	15
6.3.3. Local Logs	15
6.3.4. Event Configuration	16
6.4. Database Backup/Restore	18
6.4.1. Backup Directory	18
6.4.2. Backups Scheduler	19
6.5. Database Replication	19
6.6. Email Notification	21
6.6.1. General Settings	21
6.6.2. Additional Email Address	23
6.7. SNMP Agent	23
6.7.1. SNMP Agent Settings	23
6.7.2. SNMPv1 / SNMPv2 Community Strings	24
6.7.3. SNMPv3 Authentication Settings	24
6.7.4. SNMP Trap Destination	25
6.8. InfluxDB Client	26
6.9. MQTT	26

6.9.1. MQTT Broker	27
6.9.2. MQTT Client	28
6.9.3. MQTT Broker Topics Using SmartDirectors	28
6.10. Certificates	29
6.11. Start Server Process	30
7. Server Configuration via Web Server	31
7.1. Enable Web Server	31
7.2. Start Server Process	31
7.3. Login to Web UI	32
7.4. Start the App	33
7.5. Application "Server Configuration" Overview	35
7.6. Server Properties	36
7.6.1. General Settings	36
7.6.2. Web Server Configuration	37
7.6.3. Devices Discovery Settings	37
7.7. Communication Interfaces	38
7.7.1. Device Communication Settings	38
7.7.2. Client Server Communication Settings	39
7.8. Client Authentication	40
7.9. Syslog	42
7.9.1. Syslog Receiver Service	43
7.9.2. Syslog Forwarding Service	43
7.9.3. Local Logs	44
7.10. Database Backup	44
7.10.1. Database Backup	45
7.10.2. Schedule Database Backups	46
7.11. Database Replication	46
7.12. Email Notification	48
7.12.1. General Settings	48
7.12.2. Additional Email Address	50
7.13. SNMP Agent Communication	50
7.13.1. SNMP Receiver Service Settings	51
7.13.2. SNMPv1/SNMPv2 Communication Settings	51
7.13.3. SNMPv3 Communication Settings	52
7.14. SNMP Trap Relay	54
7.15. InfluxDB Integration	54
7.16. MQTT	55
7.16.1. MQTT Broker Service	55
7.16.2. MQTT Data Subscription Settings	56
7.17. PMS/FIAS	58
7.18. Server Startup Logs	58

7.19. Server Status 59

7.20. Server Diagnostic 60

7.21. Server Ports 60

7.22. Certificates 61

7.23. Logout from Web UI 61

Chapter 1. Summary

In this document you will learn how to configure the server component of Smart Building Manager (SBM).

Additionally, useful instructions on how to connect SBM to the following applications and protocols are specified:

- **Influx** database to store time series data for analysis purposes
- **MQTT** for IoT applications
- **Fidelio FIAS** for integration of the hotel management information protocol

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.



Make sure the browser allows the execution of scripts.



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 [Chapter 2](#))


Chapter 2. 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.

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

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

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

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

Chapter 3. Administrative Prerequisites

Before using the application for operational tasks, the prerequisites must be as follows:

- Valid login on the local computer.
- Application's server instance is started.
- User account has the right to start the application via web client.
- Valid server licence key file is uploaded to the server.

Chapter 4. General Security Recommendations

In order to work safely with the application we strongly recommend the following actions before going operational:

Passwords and Certificates

- Change all default passwords of application instances and pre-defined registered users.
- Change the default admin password of the managed devices. Refer to the respective device's user manual.
- Change the default database access password.
- Update the server certificate using a valid Root-CA.
- Update the devices certificates using a valid Root-CA.



- It is recommended to use a password management software to store all your changed passwords.
- It is recommended to use an identity management system to create and manage certificates for your server and devices.

User Management

- Create alternative admin users with appropriate permissions for daily work.
- Create different users for the different roles.
- For security reasons, only create a minimum number of users which are absolutely necessary.
- Adjust the authorisation level for each user and always select a minimum number of access permissions.

Firewall Settings

- Review necessary port numbers.
- Review necessary firewall settings.
- Adjust the port numbers of the server instance if needed.
- Take care of the dynamic port numbers as used by the server instance.
- Adjust firewall port settings for those ports which match the application's ports.

Chapter 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)



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.

5.1. Server Manager Main Window

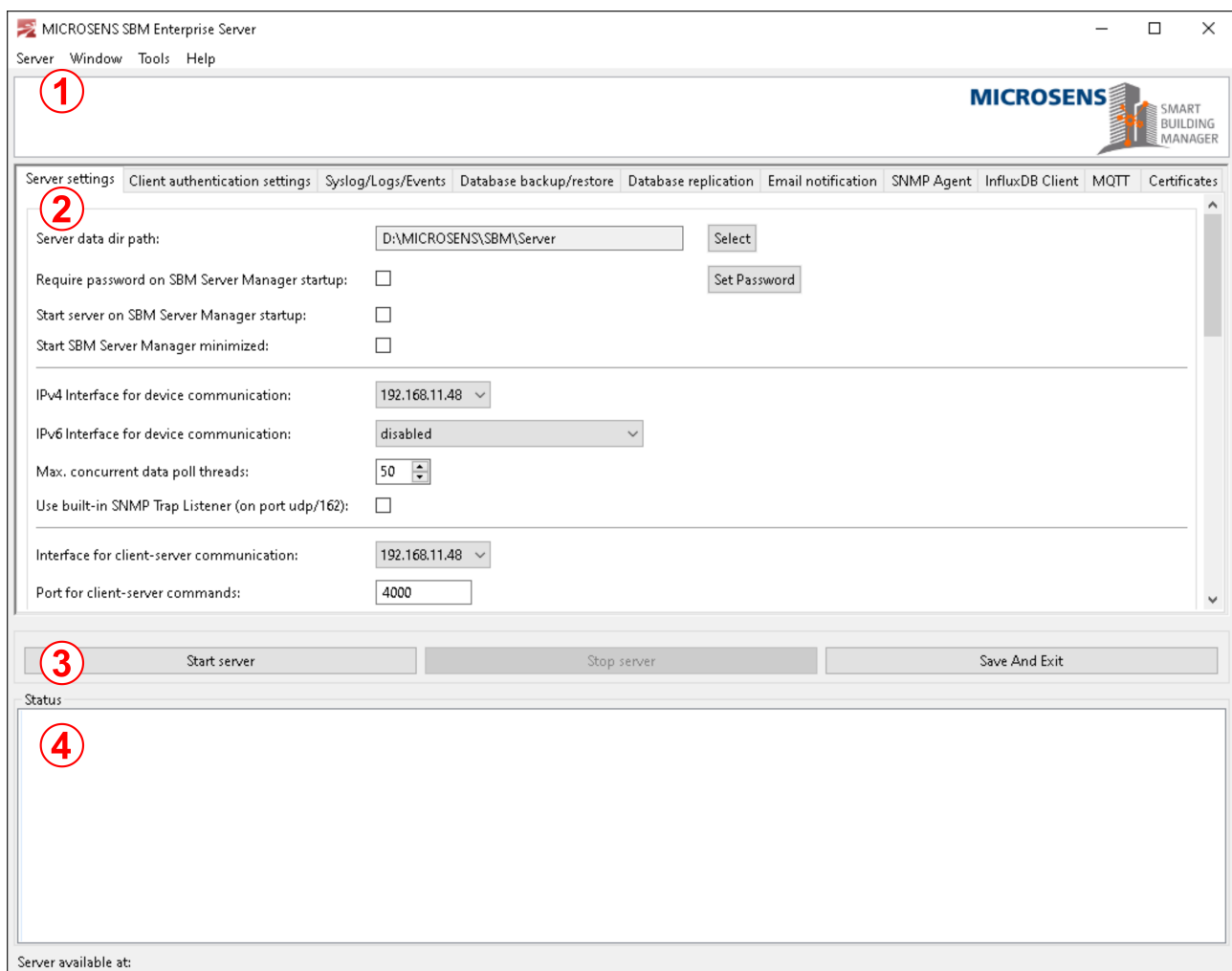


Figure 1. Server Manager - Main Window

The Server Manager's main window consists of four main elements:

1. **Main Menu:** The main menu bar provides access to functions like starting and stopping the server process, interacting with an application or help.
2. **Tabbed Server Configuration Panel:** The tabbed server configuration panel allows configuration of all the server parameters.
3. **Server Control Buttons:** The server control buttons are used to start or stop the server process or to exit the Server Manager.
4. **Status Text Field and Server IP Address:** This text box contains necessary information about the current status of the server process. All information regarding the start and stop of services is available. Additionally, the link to the web server is provided (if web server is started).

Chapter 6. Server Configuration via Server Manager

6.1. Server Settings

The tab Server Settings contains the following settings and options:

- **General:** General settings for data directory, password protection and start-up handling.
- **Device Communication:** Parameters for communication between the server instance and connected devices.
- **Client-Server Communication:** Parameters for communication between server instance and the application's client component.
- **Web Server:** Web server settings for security and ports.
- **Fidelio/FIAS:** Settings for the Fidelio/FIAS client for the management of smart devices in hotel rooms.
- **Device Discovery:** Configuration of the interfaces for device discovery in the network.
- **WiFi Access Point Management Bridge:** Settings for connecting WiFi networks of different access points.

6.1.1. General



The screenshot shows the 'General' tab of the 'Server Manager' settings. It contains four rows of settings:

Server data dir path:	<input type="text" value="C:\Users\User\ Server"/>	<input type="button" value="Select"/>
Require password on Server Manager startup:	<input type="checkbox"/>	<input type="button" value="Set Password"/>
Start server on Server Manager startup:	<input type="checkbox"/>	
Start Server Manager minimized:	<input type="checkbox"/>	

Figure 2. Server Manager - Tab "Server Settings" - General

- **Server data dir path:** Select the location where the server will save all configuration files and database data. The default location is `$USER_HOME\SBM Server`. In the selected destination folder, a respectively named folder will be created.
- **Require password on Server Manager startup:** When selected, the password prompt will be displayed before opening the Server Manager window. The password can be set by selecting the .

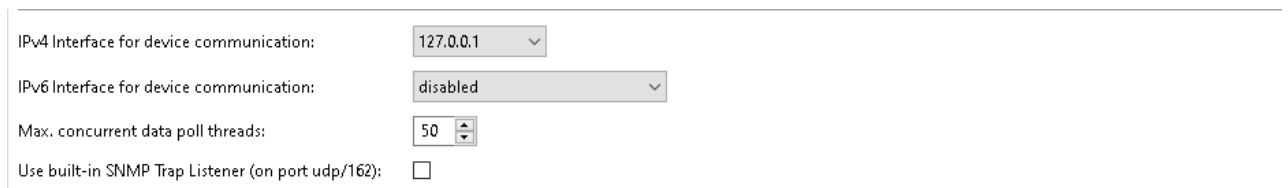
Enter the password, confirm the password to prevent typing errors and click on the button.

This function can be used to protect the server from re-configuration.

- **Start server on Server Manager startup:** Automatically starts the server instance (database engine, device data collector and, if enabled, HTTP(S) server) on start-up. If the Server Manager is added to the list of OS auto-start applications, the application's Server Manager will be started automatically and ready to use after OS boot.

- **Start Server Manager minimized:** Starts the Server Manager window in a minimized manner. The most important Server Manager features will be available via the system tray icon.

6.1.2. Device Communication

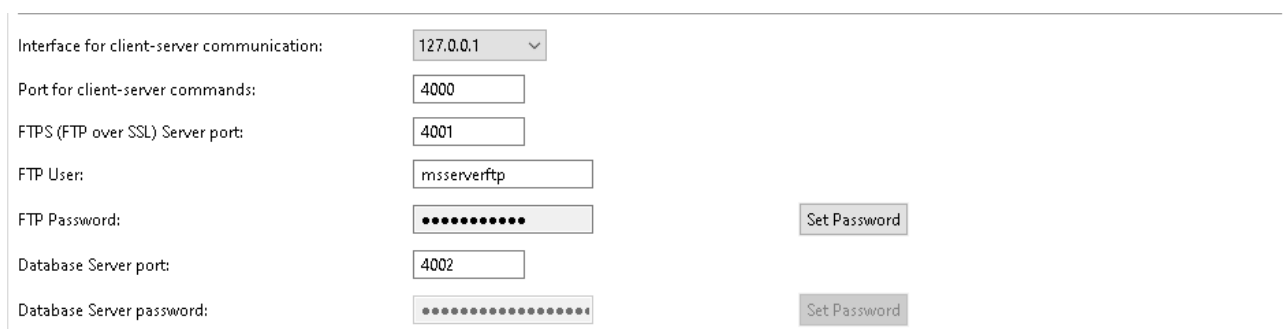


The screenshot shows the 'Device Communication' configuration window. It contains four settings: 'IPv4 Interface for device communication' set to '127.0.0.1', 'IPv6 Interface for device communication' set to 'disabled', 'Max. concurrent data poll threads' set to '50', and 'Use built-in SNMP Trap Listener (on port udp/162)' which is unchecked.

Figure 3. Server Manager - Tab "Server Settings" - Device Communication

- **IPv4 Interface for device communication:** Shows 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 network) for client access. Thanks to this function the clients do not have the direct access to managed devices. The devices can be accessed exclusively through the server process.
- **IPv6 Interface for device communication:** Shows the IPv6 address of the network interface that will be used for communication with the managed devices.
- **Max. concurrent data poll threads:** This parameter is used to define the number of devices that can be polled simultaneously. For slower servers, heavily loaded networks or slow network connections, we recommend reducing this value for better performance.
- **Use built-in SNMP Trap Listener (on port udp/162):** The server process has a built-in SNMP trap listener to receive traps from network devices. On default the trap listener is disabled. If there is no other trap receiver in use in the network it is possible to enable this function.

6.1.3. Client-Server Communication



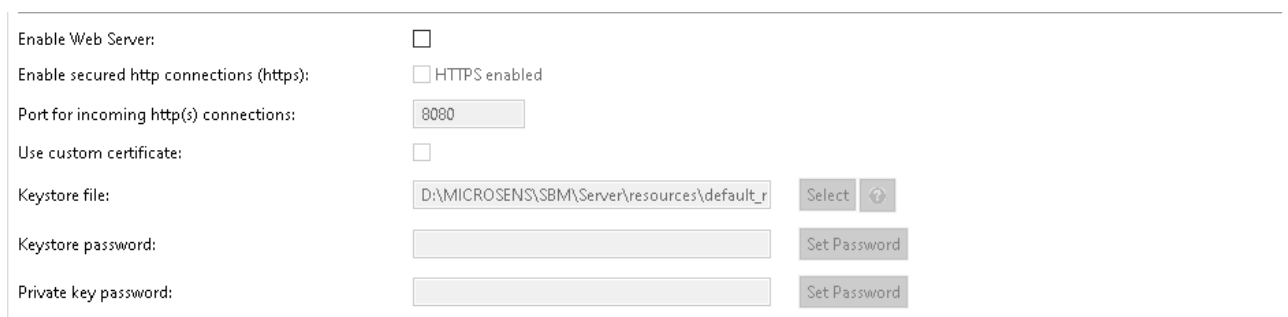
The screenshot shows the 'Client-Server Communication' configuration window. It contains seven settings: 'Interface for client-server communication' set to '127.0.0.1', 'Port for client-server commands' set to '4000', 'FTPS (FTP over SSL) Server port' set to '4001', 'FTP User' set to 'msserverftp', 'FTP Password' masked with dots with a 'Set Password' button, 'Database Server port' set to '4002', and 'Database Server password' masked with dots with a 'Set Password' button.

Figure 4. Server Manager - Tab "Server Settings" - Client-Server Communication

- **Interface for client-server communication:** The IPv4 address of the network interface that will be used for the application's client access. If the HTTP server is enabled for web client access, this interface is also used by the built-in HTTP server.

- **Port for client-server commands:** The port that is used by the application's client to communicate with the server process (4000 on default).
- **FTPS (FTP over SSL) Server port:** The built-in FTPS server is used by the application's client to synchronise device lists and firmware updates (4001 on default).
- **FTP User:** Enter the user name that is registered in the FTP server.
- **FTP Password:** Enter the user password that is registered in the FTP server.
- **Database Server port:** The port used by the built-in database server for the application's client access (4002 on default).
- **Database Server password:** To protect database access with a password. Click on the **Set Password** button. In the dialogue box that appears, enter this password.

6.1.4. Web Server




Enable Web Server: ☐

Enable secured http connections (https): ☐ HTTPS enabled

Port for incoming http(s) connections:

Use custom certificate: ☐

Keystore file: **Select** 

Keystore password: **Set Password**

Private key password: **Set Password**

Figure 5. Server Manager - Tab "Server Settings" - Web Server

- **Enable HTTP Web Server:** Enables or disables the built-in HTTP server that is used for web client access.
- **Enable secured http connections (https):** The server instance offers secured HTTP connections for web access. The https connections are encrypted so the communication between clients and server is safe.
- **Port for incoming https(s) connections:** The port that will be used for the HTTP(S) server. On default the server instance uses the ports **8080** for standard HTTP and **8443** for HTTPS connections.
- **Use custom certificate:** Check this option to use your own certificate for https communication. The certificate is stored inside a Java KeyStore (JKS) repository.
- **Key store file:** Select the directory and the name of the JKS file.
- **Key store password:** Enter the password that is protecting the JKS file.
- **Private key password:** Enter the password that is protecting your private key.



For more information about creating the JKS file please refer to the application's user manual.

6.1.5. Fidelio/FIAS



The screenshot shows the 'Fidelio/FIAS' settings section. It includes a checkbox for 'Enable Fidelio/FIAS client', which is currently unchecked. Below it are two input fields: 'Fidelio/FIAS server address' with the value '0.0.0.0' and 'Fidelio/FIAS server TCP/IP port' with the value '0'.

Figure 6. Server Manager - Tab "Server Settings" - Fidelio/FIAS

- **Enable Fidelio/FIAS client:** SBM is equipped with a Fidelio/FIAS client for the management of smart devices in hotel rooms. Check this option to enable the client.
- **Fidelio/FIAS server address:** Enter the Fidelio/FIAS server IPv4 address.
- **Fidelio/FIAS server TCP/IP port:** The port used by the built-in Fidelio/FIAS client to access the server.

6.1.6. Device Discovery



The screenshot shows the 'Device discovery' section. It contains two dropdown menus: 'IPv4 Interface for device discovery' set to '192.168.11.48' and 'IPv6 Interface for device discovery' set to 'disabled'.

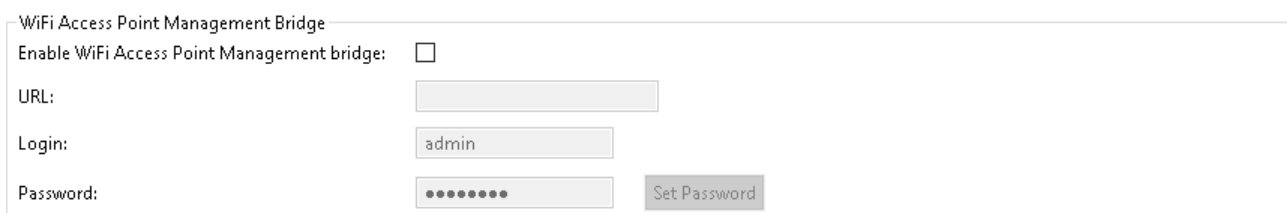
Figure 7. Server Manager - Tab "Server Settings" - Device Discovery

- **IPv4 Interface for device discovery:** Select the respective IP interface from the drop-down list.
- **IPv6 Interface for device discovery:** Select the respective IP interface from the drop-down list.



In contrast to the assigned interface for device communication it is possible to change the interface for device discovery while the server instance is running.

6.1.7. WiFi Access Point Management Bridge



The screenshot shows the 'WiFi Access Point Management Bridge' section. It includes a checkbox for 'Enable WiFi Access Point Management bridge', which is unchecked. Below it are three input fields: 'URL', 'Login' (with the value 'admin'), and 'Password' (with masked characters). A 'Set Password' button is located to the right of the password field.

Figure 8. Server Manager - Tab "Server Settings" - WiFi Access Point Management Bridge

- **Enable WiFi Access Point Management Bridge:** Check this option to enable the bridge.
- **URL:** Enter the bridged access point's URL.
- **Login:** Enter the user name that is registered on the access point.
- **Password:** Enter the user's password.

6.2. Client Authentication Settings

The tab Client Authentication Settings contains the following settings and options:

- **Authentication Selection:** Select the authentication method.
- **RADIUS Settings:** Manage the RADIUS server settings if RADIUS is the selected authentication method.

6.2.1. Authentication Selection

Use local user DB only for client authentication:	<input checked="" type="radio"/>
Use local user DB and RADIUS Server for client authentication:	<input type="radio"/>
Use RADIUS Server only for client authentication:	<input type="radio"/>

Figure 9. Server Manager - Tab "Client Authentication" - Selection

- **Use local user DB only for client authentication:** The server will use the information from its local database for user authentication.
- **Use local user DB and RADIUS Server for client authentication:** The server will use the defined RADIUS server in order to authenticate the user. A local user account (in the local server database) will be created automatically (if such an account does not exist).



The server will be able to authenticate a new user and create a local account if the number of currently existing accounts are lower than the number of allowed user accounts defined by the application's server licence. Access to the server will be granted if the RADIUS server will return the **RADIUS ACCESS ACCEPT** message and the local user's credentials exist.

- **Use RADIUS Server only for client authentication:** The server will use a RADIUS server for user authentication.

6.2.2. RADIUS Settings

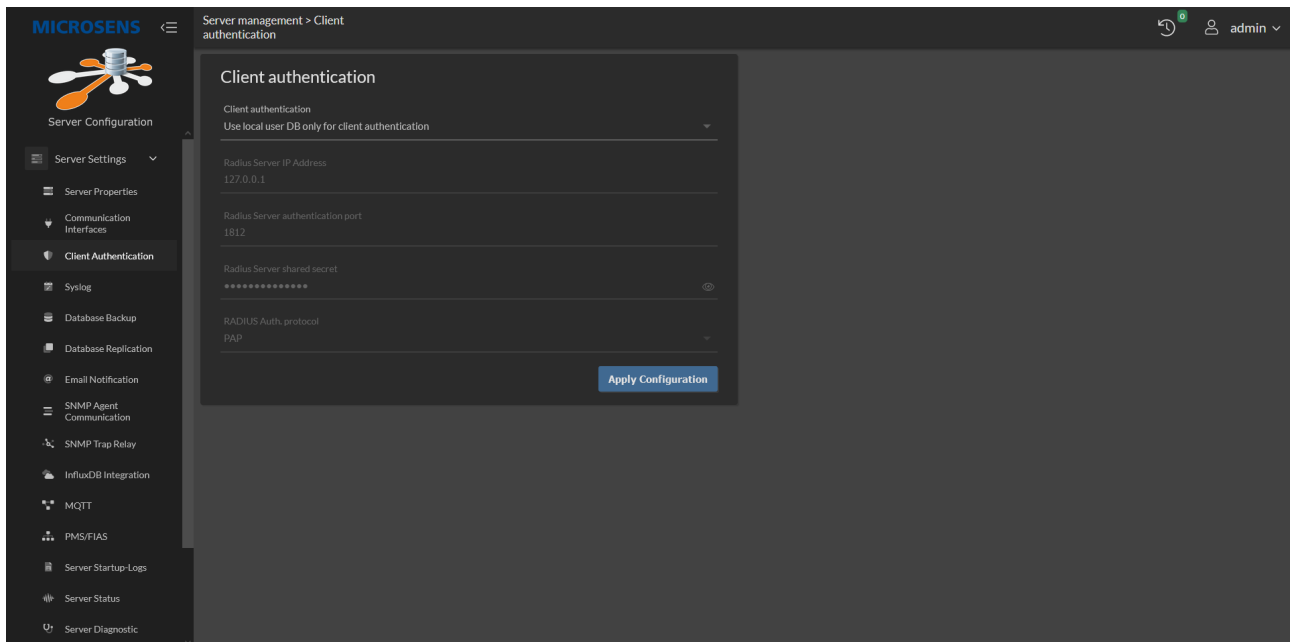


Figure 10. Server Manager - Tab "Client Authentication" - RADIUS Settings

- **RADIUS Server IP address:** The IP address of the RADIUS server.
- **RADIUS Server authentication port:** The port used by RADIUS server for authentication. Default value is 1812.
- **RADIUS Server Shared Secret:** The RADIUS server shared secret (password) used during the authentication process. Default value is default_secret.
- **RADIUS Auth protocol:** The authentication schema used by the RADIUS server (PAP or CHAP).

The user levels of RADIUS server and the application's server are mapped as follows:

RADIUS Server User Level (Value of RADIUS Service Type)	SBM Server User Level
Login-User (1)	sbmuser
Administrative-User (6)	sbmadmin
Callback-Administrative (11)	sbmsysadmin

The following example shows the mapping inside the FreeRADIUS file users:

```
sbmsysadmin    Cleartext-Password := "sbmsysadmin"
                Service-Type = Callback-Administrative-User

sbmadmin       Cleartext-Password := "sbmadmin"
                Service-Type = Administrative-User

sbmuser        Cleartext-Password := "sbmuser"
```

Service-Type = Login-User

When the authentication mode **Use local user DB and RADIUS Server for client authentication** is selected, the application's server treats the RADIUS server as the master authentication server. When the user level (Service-Type) or user password is changed on RADIUS server, the application's server will automatically update the local user account.



The local server database must contain at least one user with **Callback-Administrative** rights. The application's server will refuse to modify the user level of its local account, resulting in no local user with **Callback-Administrative** rights remaining.

After deleting a user account from RADIUS server, the local server account will not be deleted automatically. The system administrator should delete the user account from the local server database manually.



Please keep in mind that the number of application's users available on the RADIUS server should be identical to the number of user accounts allowed by the application's licence key file.

6.3. Syslog/Logs/Events

The tab Syslog/Logs/Events contains the following settings and options:

- **Syslog Server (Receive Syslogs):** Settings for the server acting as a Syslog server.
- **Syslog Client (Send Syslogs):** Settings for the server acting as a Syslog client.
- **Local Logs:** Configure the log handling.
- **Event Configuration:** Configure the type of log message and specific relevance levels.

6.3.1. Syslog Server (Receive Syslogs)

Syslog Server (receive Syslogs)

Enable Syslog Server: ☐

Syslog Server interface: (CAUTION: Always the same as the server IPv4 interface for server-devices communication)

Syslog Server port [udp]:

Figure 11. Server Manager - Tab "Syslog/Logs/Events" - Syslog Server

- **Enable Syslog server:** The application's server can act as a Syslog server. In such case, all the Syslog messages sent by devices will be saved within the application's server database.
- **Syslog server interface:** The IP address of the network interface used by the Syslog server.



This interface is always identical to the interface defined for server-devices communication.

- **Syslog server port [udp]:** The UDP port on which the Syslog server listens for incoming messages. Default value is 514.

6.3.2. Syslog Client (Send Syslogs)

Figure 12. Server Manager - Tab "Syslog/Logs/Events" - Syslog Client

- **Enable Syslog client:** Enables the Syslog client function. In this mode the application's server will send Syslog messages.
- **Syslog destination (server IP):** The IP address of the Syslog server, where the application's server sends Syslog messages.
- **Protocol/Port:** Protocol (TCP/UDP) and port which should be used by the Syslog client. This should be configured in accordance with Syslog server requirements.

6.3.3. Local Logs

Figure 13. Server Manager - Tab "Syslog/Logs/Events" - Local Logs

- **Archive logs when log count higher than or delete logs older than:** The application's server will generate a .csv file with log messages when the number of log messages in the database will be higher than the defined log count limit (25000, 50000 or 100000 messages) or older than the defined log age (1, 2, 6 or 12 months).

The archived messages will be deleted from the database to prevent unlimited growth of the database size. The server starts the archiving procedure each day at 2 a.m.. The last 500 and all unacknowledged messages are always kept in the database (i.e. they are not deleted during the archiving procedure).

- **Logs archive folder:** Choose the location where application's server should save the log archives.
- **Keep device history from last:** The application's server saves parameters like device temperature or device availability in the database which are used to create device history charts. To prevent unlimited growth of the database size, the server deletes history entries older than n` months. The maximum time for keeping the history is 12 months. The server clears the database each day at 2 a.m.
- **Clear selected log database tables:** Clear the database log tables manually by selecting the type of table that should be cleared and then clicking on the button **Clear**. This operation will remove all the log entries from the selected tables.

6.3.4. Event Configuration

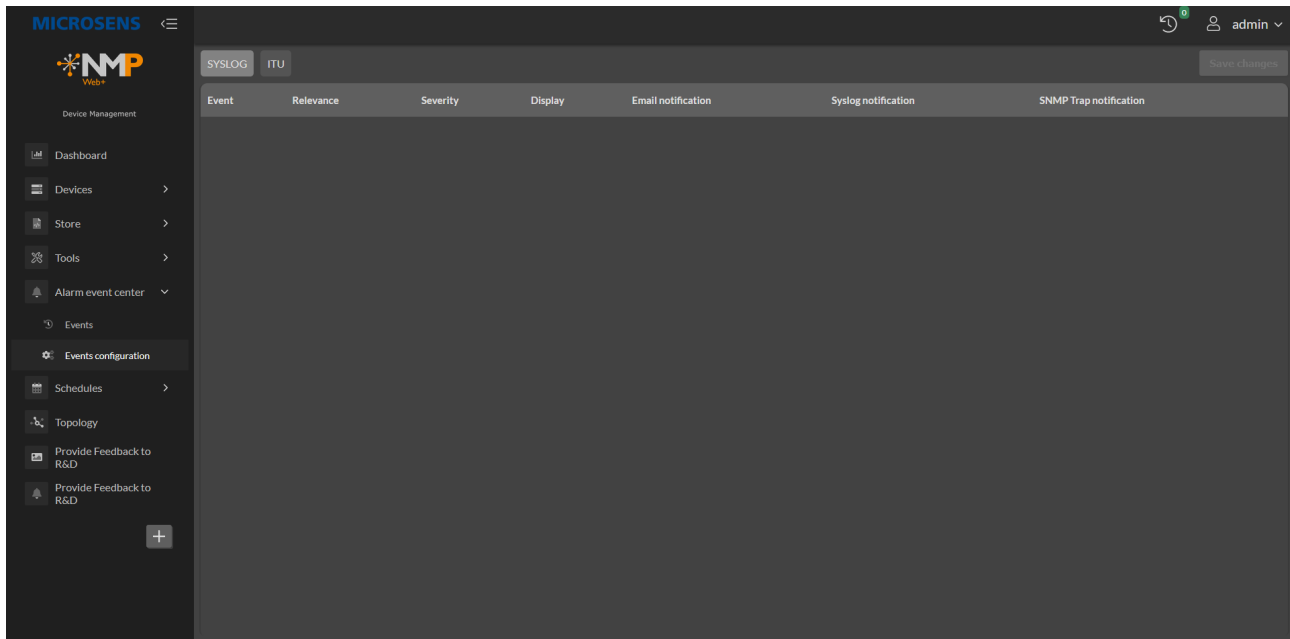


Figure 14. Server Manager - Tab "Syslog/Logs/Events" - Events Configuration

All server events can be configured here. There are several types of log messages with different relevance levels:

- **INFO:** An informational event.
- **POSITIVE:** A positive message (no error).
- **NEGATIVE:** A negative message (warning, error, critical)








Each event has an assigned relevance level according to its importance. It is not possible to change the relevance level.

Additionally, each event has an assigned severity level, which can be modified. It is possible to choose between two severity keyword styles:

- **SYSLOG:** The severity is shown as SYSLOG severity keywords according to RFC5424.
- **ITU:** The severity is shown as ITU severity keywords according to X.733.

There are nine different severity levels indicated by the formatting and the respective icon in the left column of the table:

Icon	Severity Level SYSLOG (S) ITU (I)	Meaning
	S: disabled I: disabled	The event will not generate a log entry (neither displayed nor logged). It is greyed out.

Icon	Severity Level SYSLOG (S) ITU (I)	Meaning
	S: info I: cleared	This is an informational message that does not require special attention (e.g. system messages). It is formatted with black font colour.
	S: notice I: normal	This is a success notification (e.g. configuration applied successfully). It is formatted with green font colour.
	S: WARNING I: WARNING	This is a low level warning message. It is formatted with black font colour on yellow background.
	S: ERROR I: MINOR	This is an error message that requires user attention. It is formatted with red font colour.
	S: CRITICAL I: MAJOR	This is a critical error message that requires immediate user attention. It is formatted with black font colour on red background.
	S: ALERT I: CRITICAL	This is an alert message. It is formatted with black font colour on red background.
	S: EMERGENCY I: EMERGENCY	This is an emergency message. It is formatted with black font colour on red background.
	S: debug I: debug	This message contains debugging information. It is formatted with blue font colour.

Messages are displayed differently in the application's client log table, making it easier to direct the attention to important events. How the messages are displayed depends on which severity level has been defined.

For each event type the system administrator can enable or disable the following notification options:

- **Sound:** The client plays a sound when an event is received.
- **Email:** When an event occurs, the server sends an email to all the defined recipients.

 | Configure the SMTP server on the Email Notification tab.

- **Syslog:** The server sends a Syslog message.

 | The Syslog client has to be enabled on this tab.

- **SNMP trap notifications:** The server sends an SNMP trap notification.

 | Enable and configure the SNMP Agent on SNMP Agent tab.

6.4. Database Backup/Restore



A running server process has to be stopped before starting the backup/restore procedure.

The tab Database Backup/Restore contains the following settings and options:

- **Backup Directory:** Configure the backup folder for the database copy.
- **Backups Scheduler:** Configure periodical backups of the database.

6.4.1. Backup Directory

The server allows the creation of a backup copy of the database currently in use.

The backups will be saved as **.zip** archives. The filename contains the current date (e.g. **DB_BACKUP_2018-06-15.zip**).



If a file with the same name already exists in the backup folder, the current time in milliseconds will be appended after the current date to distinguish the files.

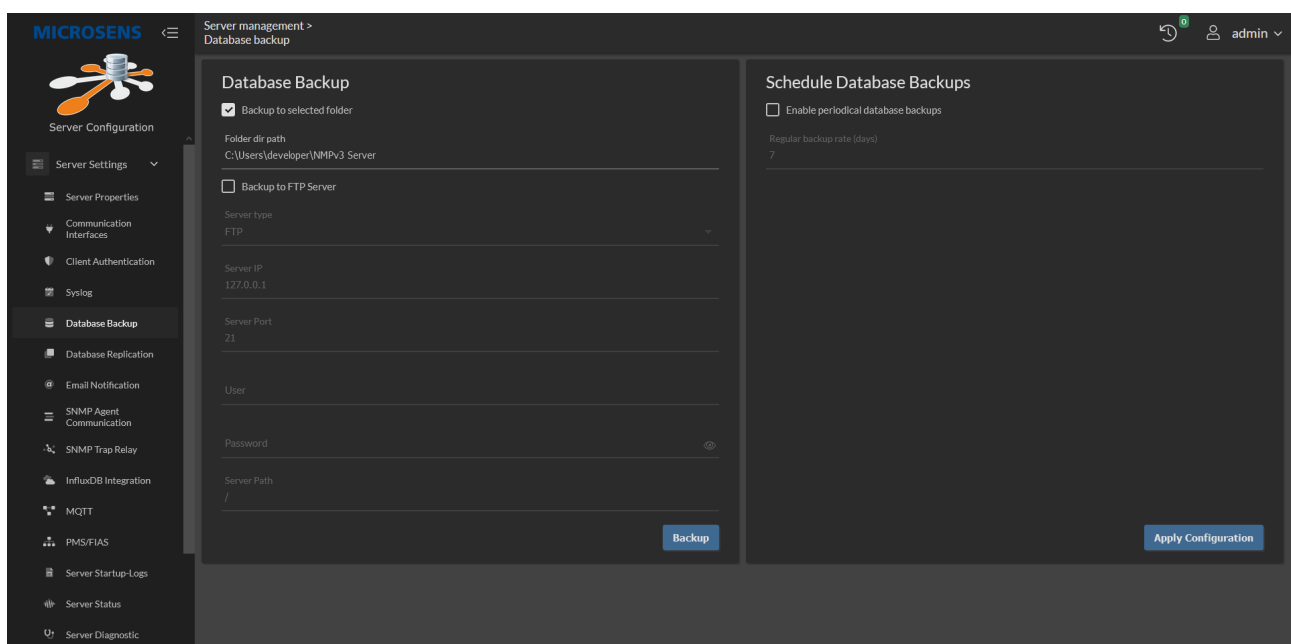


Figure 15. Server Manager - Tab "Database Backup/Restore" - Folder Selection

- **Backup to/Restore from selected folder:** A click on the button **Select folder** targets the database backup to a local directory.
- **Backup to/Restore from FTP Server:** Check this option to target the backup to an FTP server.
- **Server type:** Select the server type of the FTP server.



It is recommended to use a secure protocol like FTPS or SFTP.

- **Server IP:** Enter the IP address of the server.

- **Server Port:** Enter the server port of the server.
- **User/Password:** Enter valid credentials of the registered FTP user
- **Server Path:** Enter the server's path to the backup folder (e.g. */Some Folder/Backup*).



If the backup file should be saved in the FTP server's root directory, an empty string or "/" is required.

By clicking the button **Backup**, the backup starts automatically.

To restore the database from a backup file, click on the button **Restore**, and select the *.zip* file from which the database should be restored.



The database can only be recovered from a local backup file. When creating an FTP backup, the backup copy should first be downloaded to a local directory using an FTP client.

6.4.2. Backups Scheduler

It is possible to enable periodically scheduled backups, based on the directory settings above.

Figure 16. Server Manager - Tab "Database Backup/Restore" - Scheduler

- **Schedule periodical backups:** Enable or disable periodic database backups.
- **Periodical backups rate (days):** The server will backup the database automatically every *x* days (1 to 30).

6.5. Database Replication

This dialogue allows the configuration of two server instances in master-slave mode to replicate the current database.

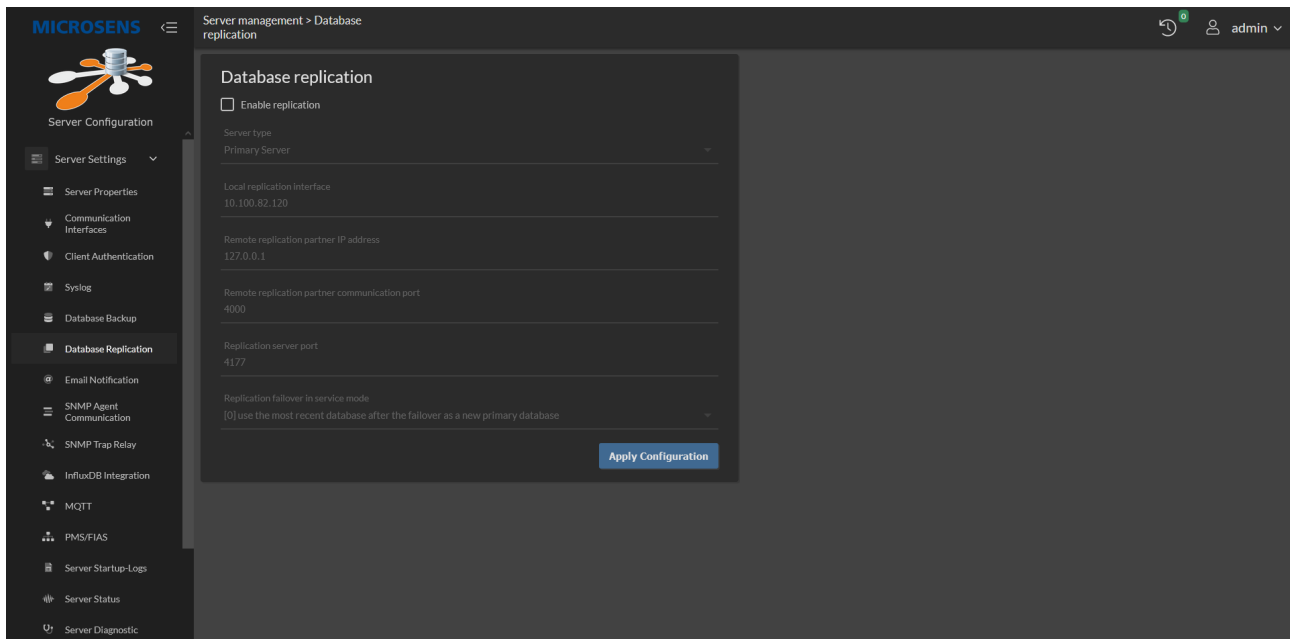


Figure 17. Server Manager - Tab "Database Replication"

- **Replication mode:** Enable or disable the replication mode.

As soon as the replication mode is enabled, select whether the respective server instance should act as a master or slave server.

- **Local replication interface:** The network interface that will be used by the local server. This interface is always identical to the interface for client-server communication (configured on tab [Server Settings](#)).
- **Remote replication partner IP address:** The IP address of the remote replication partner server. This interface must be always identical to the remote server's interface for client-server communication (configured on tab [Server Settings](#) of the remote Server Manager).
- **Remote replication partner communication port:** The port number of the remote replication partner server for client-server communication.
- **Replication server port:** The port number that will be used to replicate the database. The port on the local server must be identical to the port configured on the remote replication partner server (default: 4177).
- **Replication failover in service mode:** Select the database that will be used as a new master database after the failover.

Available options are:

- **Use the most recent database after the failover as a new master database:** The most recently used database will be used when the replication will be restored after a master or slave failure.
- **Use the master database after the failover as a new master database:** When replication is restored following a master or slave failure, the master server's database is always used.

- **Use the slave database after the failover as a new master database:**
When replication is restored following a master or slave failure, the slave server's database is always used.

In order to start the replication, configure both master and slave server:

- Both servers must have a connection via the network.
- Servers work in pairs. One of the servers should be configured as a master server, the other one should be configured as a slave server.



The replication will not be initialized when both servers will be configured as masters (or slaves). The replication will also not be initialized when the replication mode is disabled on one of the servers.

- The port used for replication should be exactly the same on both servers.
- Both servers must have access to the managed devices. In case of failure of a server (master or slave), the other one will reboot itself in no-replication mode and will continue device monitoring.

After configuring the replication options, both servers should be started by pressing the button **Start server**. From this point, the servers will automatically initialize the replication.

For more information on database replication please refer to the application's User Manual.

6.6. Email Notification

It is possible to get notified by the application via email about errors, SNMP traps and scheduled task events.

The tab Email Notification contains the following settings and options:

- **General Settings:** Configure general email settings.
- **Additional Email Address:** Assign a additional email address.

6.6.1. General Settings

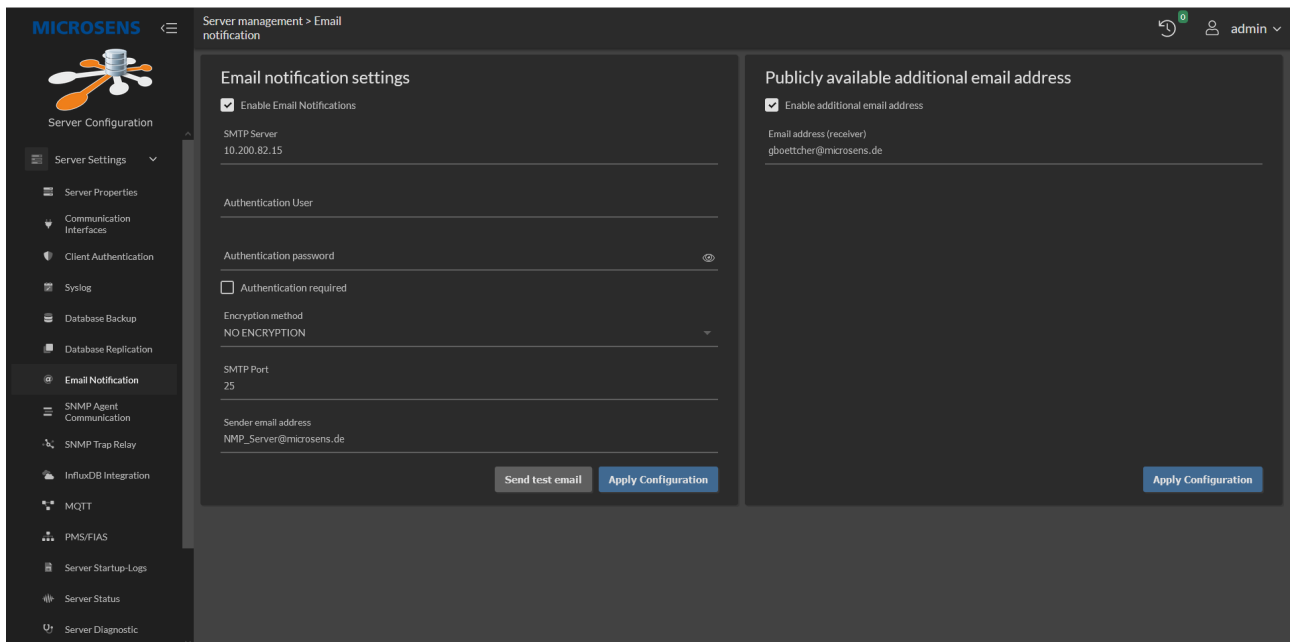




Figure 18. Server Manager - Tabbed Server Configuration Panel - Email Notification - General Settings

The server instance is able to send email notifications on events. The configured SMTP server is used as email relay server. Email notifications are sent to all registered users. The system administrator and all users should configure their proper email addresses.

- **Enable Email Notifications:** If this option is enabled, errors and SNMP trap information is forwarded by email to recipients named below.

 | A valid email account with SMTP access is required.

- **SMTP Server:** The address of the SMTP outgoing server (e.g. `smtp.gmail.com`).
- **Authentication user:** Valid user name for this email account.
- **Authentication password:** Valid user password for this email account.
- **Authentication required:** Check this option if the SMTP server requires user authentication.
- **Encryption method:** The encryption used by the SMTP Server. The following selection is possible:
 - **NO_ENCRYPTION:** Connection and communication between email server and client is not encrypted.
 - **SSL:** On first step an encrypted TLS/SSL connection between email server and client is established. Afterwards both server and client communicate secure via an encrypted channel. This selection is strongly recommended!
 - **TLS:** When using a STARTTLS encryption both server and client primarily negotiate their encryption capabilities and subsequently establish an encrypted connection if possible. All prior communication happens unencrypted.

 | Only TLS 1.2 and newer is supported.

- **SMTP Port:** The SMTP server port.
- **Sender email address:** The email address used in the field "From" of the sent message.

6.6.2. Additional Email Address

The server is able to send email notifications to an additional (publicly available) email address not related to any of the registered user accounts.



Publicly available additional email address

Enable additional email address: ☐

Email address (receiver):

Figure 19. Server Manager - Tabbed Server Configuration Panel - Email Notification - Additional Email Address

- **Enable additional email address:** Check this option to enable sending messages to an additional email address.
- **Email address (receiver):** Enter a valid email address for an additional notification receiver.

6.7. SNMP Agent

The SNMP protocol can be used to make management data available to other management systems. The application's server offers a northbound interface in the form of an SNMP Agent. A *northbound interface* is an interface that allows a particular component of a network to communicate with an upper level component.

The tab SNMP Agent contains the following settings and options:

- **SNMP Agent Settings:** Configure general SNMP agent settings.
- **SNMPv1/SNMPv2 Community Settings:** Configure SNMP v1 and SNMP v2 settings.
- **SNMPv3 Authentication Settings:** Configure SNMPv3 settings.
- **SNMP Trap Destination:** Configure multiple SNMP trap destinations.

6.7.1. SNMP Agent Settings

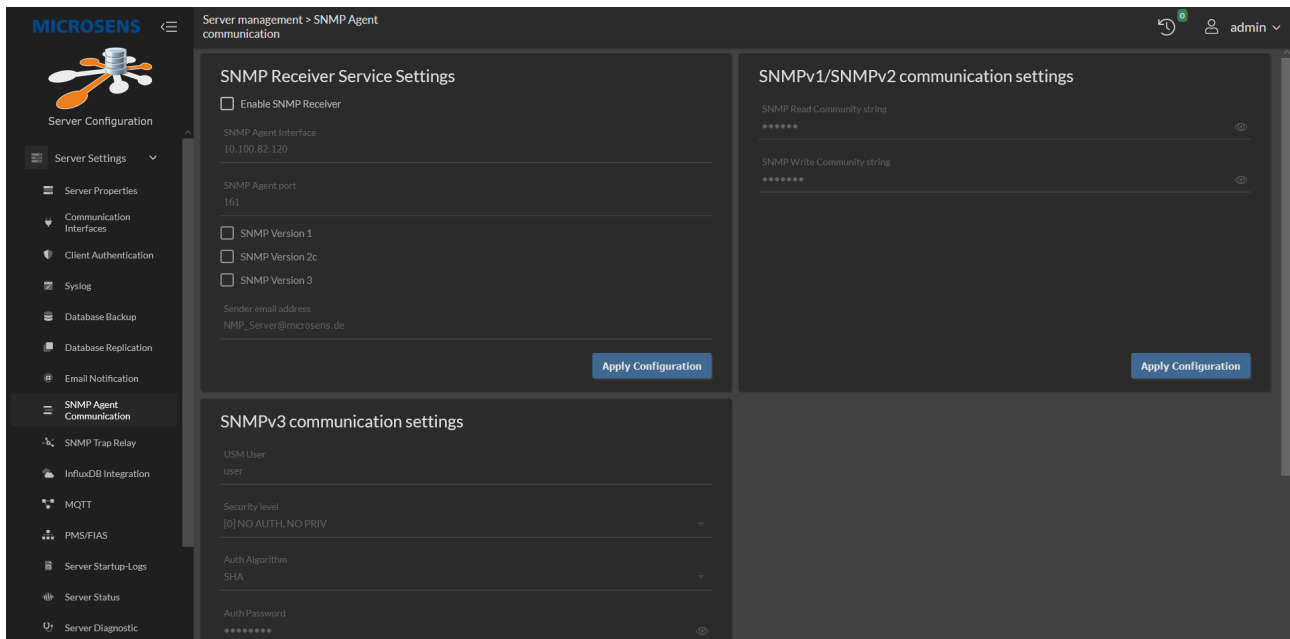


Figure 20. Server Manager - Tab "SNMP Agent" - SNMP Agent Settings

- **Enable SNMP Agent:** Enabling the SNMP agent allows the other SNMP managers to see the management data collected by the server instance.
- **SNMP Agent interface:** The IP address of the network interface used by the SNMP Agent, via which other SNMP managers can query data. The interface is configured via the tab Server Settings and is always identical to the **Interface for client-server communication**.
- **SNMP Agent port:** The port that is used by the SNMP Agent.
- **SNMP version:** Select the SNMP product variant needed to be supported by the SNMP Agent. At least one version should be enabled.

6.7.2. SNMPv1 / SNMPv2 Community Strings

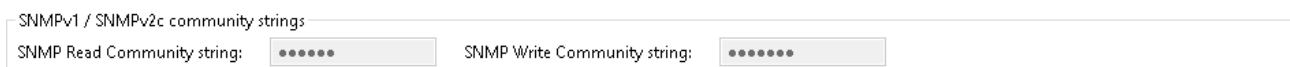


Figure 21. Server Manager - Tab "SNMP Agent" - SNMP Agent Settings

- **SNMP Read Community string:** The read-only community string allows other SNMP managers to read data values.
- **SNMP Write Community string:** The read-write community string allows other SNMP managers to read and write data values.

6.7.3. SNMPv3 Authentication Settings

SNMP v3 authentication settings

USM User:

Security level:

Auth Algorithm: Auth Password:

Privacy Algorithm: Privacy Password:

Context name:

Figure 22. Server Manager - Tab "SNMP Agent" - SNMPv3 Authentication Settings

- **USM User:** The security name of the user (typically the user name).
- **Security level:** The SNMPv3 agent supports the following security levels as defined in the USM MIB (RFC 2574):
 - **NO AUTH, NO PRIV:** Communication without authentication and privacy.
 - **AUTH, NO PRIV:** Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
 - **AUTH, PRIV:** Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA. For privacy, the DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used.
- **Auth Algorithm:** The authentication protocol ID to be associated with this user.
- **Auth Password:** The authentication passphrase.
- **Privacy Algorithm:** The privacy protocol ID to be associated with this user.
- **Privacy Password:** The privacy passphrase.
- **Context name:** An SNMP context is a collection of management information accessible by an SNMP entity.

6.7.4. SNMP Trap Destination

MICROSENS Server management > SNMP Agent forwarding

SNMP Trap Destination

Destination	Version	IP Address	UDP port	Community
0:	Disable	0.0.0.0	162
1:	Disable	0.0.0.0	162
2:	Disable	0.0.0.0	162
3:	Disable	0.0.0.0	162

Apply Configuration

Figure 23. Server Manager - Tab "SNMP Agent" - SNMP Trap Destination

The SNMP agent can send SNMP traps on different events generated by the server instance and can resend the traps received from other devices. It is possible to configure multiple different trap destinations. For each destination choose between the SNMP v1, v2c or v3 trap versions.

For more information about using SNMP traps please refer to the application's User Manual.

6.8. InfluxDB Client

Within the SBM infrastructure environment, the open source database management system *InfluxDB* enables the customer to visualise and analyse the data collected by the connected MICROSENS Smart Building controllers.

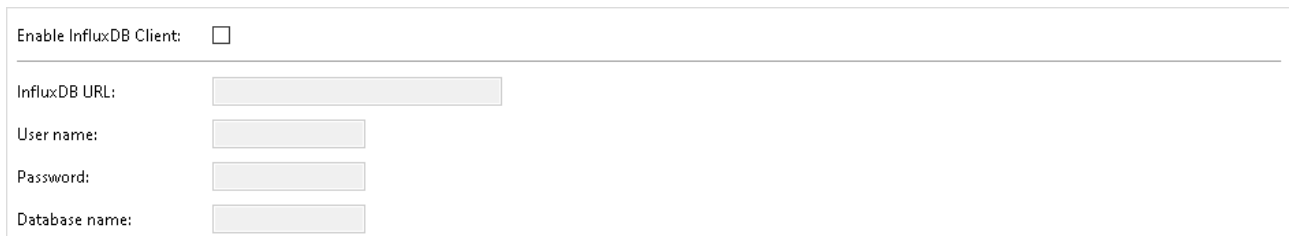


Figure 24. Server Manager - Tab "InfluxDB" - InfluxDB Settings

- **Enable InfluxDB Client:** Check this option to enable the InfluxDB client. With the InfluxDB client disabled all other fields are greyed out.
- **InfluxDB URL:** Enter the IP address of the InfluxDB server.
- **User name/password:** Enter the InfluxDB client's credentials that are stored in the InfluxDB server.
- **Database name:** Enter the InfluxDB name.

For more information about using InfluxDB please refer to the respective documentation on the [InfluxDB homepage](#).

6.9. MQTT

SBM Server can act as MQTT broker and client. This is important if you want to use SBM in automation projects with interaction between field devices.



Either activate the internal MQTT broker or the MQTT client for using an external MQTT broker. It is not recommended to enable both MQTT broker and client.

After configuring SBM as MQTT broker or client, restart SBM Server for the MQTT settings to take effect.

The tab MQTT contains the following settings and options:

- **MQTT Broker:** Configure MQTT broker address and port.
- **MQTT Client:** Configure MQTT client address, port and security settings.

6.9.1. MQTT Broker

The MQTT broker SBM Server collects and distributes all incoming MQTT data from and to managed MQTT clients, depending on the MQTT clients subscriptions.



The IPv4/IPv6 interface addresses of MQTT broker should always be identical to the **Interface for client-server communication**, configured via the tab Server settings.

MQTT Broker

[IPv4] Enable Local MQTT Broker: ☐

[IPv4] MQTT Broker Interface Address: (CAUTION: Always the same as the server IPv4 interface for server-devices communication)

[IPv4: TCP] MQTT Broker Port:

[IPv4: WebSocket] Enable WebSocket Interface: ☐

[IPv4: WebSocket] MQTT Broker Port:

[IPv4: WebSocket] Basepath:

[IPv6] Enable Local MQTT Broker: ☐

[IPv6] MQTT Broker Interface Address: (CAUTION: Always the same as the server IPv6 interface for server-devices communication)

[IPv6: TCP] MQTT Broker Port:

[IPv6: WebSocket] Enable WebSocket Interface: ☐

[IPv6: WebSocket] MQTT Broker Port:

[IPv6: WebSocket] Basepath:

Figure 25. Server Manager - Tab "MQTT" - MQTT Broker

- **[IPv4] Enable Local MQTT Broker:** Check this option to enable the MQTT broker for IPv4 network communication.
- **[IPv4] MQTT Broker Interface Address:** Enter the IPv4 address of the MQTT broker.
- **[IPv4: TCP] MQTT Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (1883) as is.
- **[IPv4 WebSocket]: Enable WebSocket Interface:** To send and receive MQTT messages via web browser and a respective MQTT JavaScript library, enable the server's WebSocket interface.
- **[IPv4 WebSocket] MQTT Broker Port:** Enter the MQTT broker's WebSocket port number.
- **[IPv4 WebSocket] Basepath:** Enter the WebSocket basepath for MQTT communication.
- **[IPv6] Enable Local MQTT Broker:** Check this option to enable the MQTT broker for IPv6 network communication.
- **[IPv6] MQTT Broker Interface Address:** Enter the IPv6 address of the MQTT broker.
- **[IPv6: TCP] MQTT Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (1883) as is.
- **[IPv6 WebSocket] Enable WebSocket Interface:** To send and receive MQTT messages via web browser and a respective MQTT JavaScript library, enable the server's WebSocket interface.

- **[IPv6 WebSocket] MQTT Broker Port:** Enter the MQTT broker's WebSocket port number.
- **[IPv6 WebSocket] Basepath:** Enter the WebSocket basepath for MQTT communication.

6.9.2. MQTT Client

When acting as MQTT client, SBM holds both the publisher and subscriber roles. Depending on the incoming or outgoing data (i.e. sensors or actuators), it serves or analyses the respective publish or subscription MQTT topics from and to the external MQTT broker.

MQTT Client

Enable MQTT Client: ☐

MQTT Remote Broker address:

MQTT Remote Broker Port:

MQTT Client ID:

Authentication required: ☐

User name:

User password:

Secured SSL/TLS communication: ☐

Subscribe Topic (@qos=2):

Figure 26. Server Manager - Tab "MQTT" - MQTT Client

- **Enable MQTT Client:** Check this option to enable the MQTT client.
- **MQTT Remote Broker Address:** Enter the IP address of the MQTT broker the client should connect to.
- **MQTT Remote Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (1883) as is.
- **MQTT Client ID:** Enter the unique MQTT client ID.
- **Authentication required:** Check this option if authentication is required for MQTT broker communication.
- **User name/password:** Enter valid MQTT clients credentials
- **Secured SSL/TLS communication:** Check this option if authentication via SSL/TLS is required for MQTT broker communication.



Configure a custom TrustStore first on tab Certificates

- **Subscribe Topic (@qos=2):** Enter the subscription topic of the MQTT client.

6.9.3. MQTT Broker Topics Using SmartDirectors

The local MQTT Broker is pre-configured corresponding with MICROSENS SmartDirectors and will subscribe to all MQTT topics for all clients.

The pattern for the subscribed topics is as follows:


```
_ { publisher_ip_address } / SmartOffice / { actorgroup | sensorgroup } / { group_name } / { attribute } _  
  
_ { publisher_ip_address } / SmartOffice / { actor | sensor } / { device_name } / { instance } / { attribute } _
```

Examples:

```
10.14.12.205 / SmartOffice / actorgroup / Valves_Climate_Zone_1_Warm / HEATING_VALVE  
  
10.14.12.213 / SmartOffice / sensor / SLC_4_1 / 1 / POWER
```

It is assumed that the topic-prefix configuration of the SmartDirector is configured as follows:

```
_ > Protocol.MQTT.publisher_config.topic_prefix = {IP4}/{SMO}_ ① ②
```

① {IP4} : IPv4 address of the device

② {SMO} : The string **SmartOffice**

6.10. Certificates

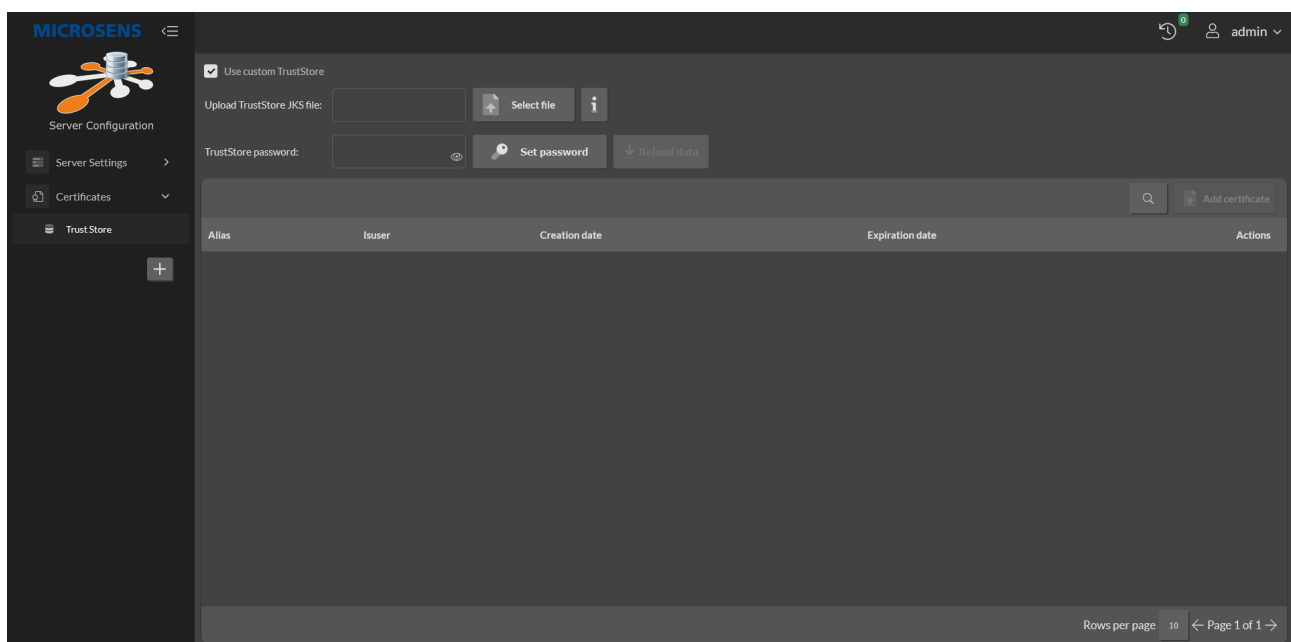


Figure 27. Server Manager - Tab "Certificates" - TrustStore

This tab allows the management of certificates. The tabular overview shows a list of existing certificates used for SSL/TLS communication of the server instance.

- **Use custom TrustStore:** Check this option to enable the use of the custom TrustStore.
- **TrustStore JKS file:** Select the necessary certificate file for SSL/TLS communication.
- **TrustStore password:** Enter the corresponding password for the selected file.
- **Add certificate:** Click on this button to store a new certificate.
- **View selected:** Left click on a table entry and click on this button to view the certificates content.
- **Delete selected:** Left click on a table entry and click on this button to delete this certificate.

6.11. Start Server Process

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

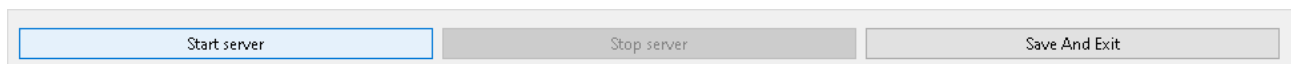


Figure 28. Server Manager - Start Server Process

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

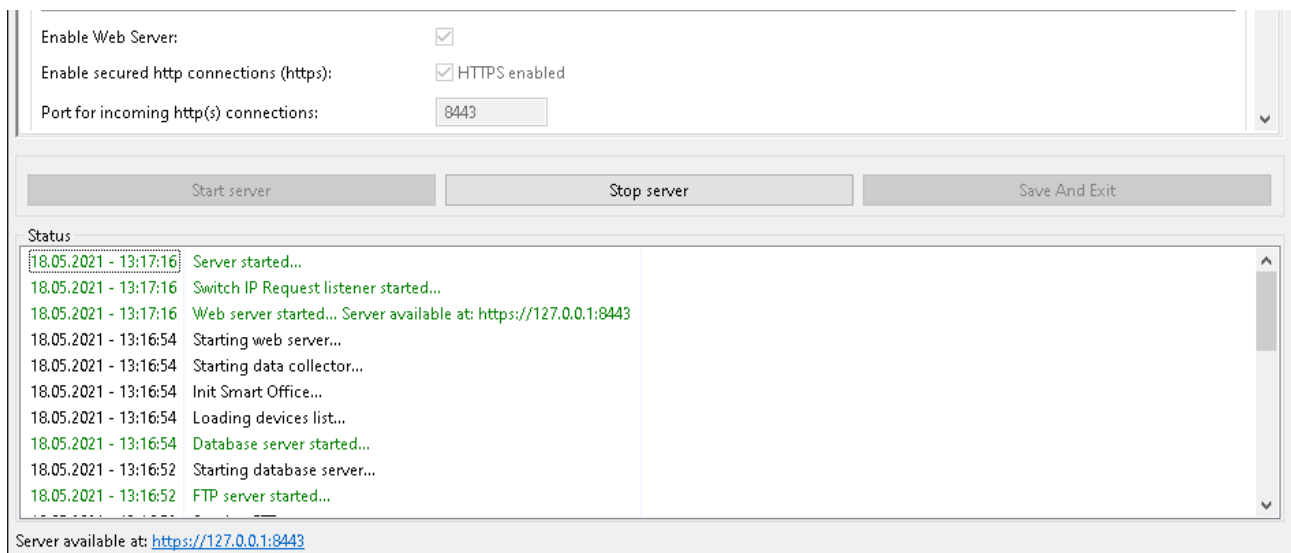


Figure 29. Server Manager - Status Field and Server URL

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

Chapter 7. Server Configuration via Web Server

7.1. 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.

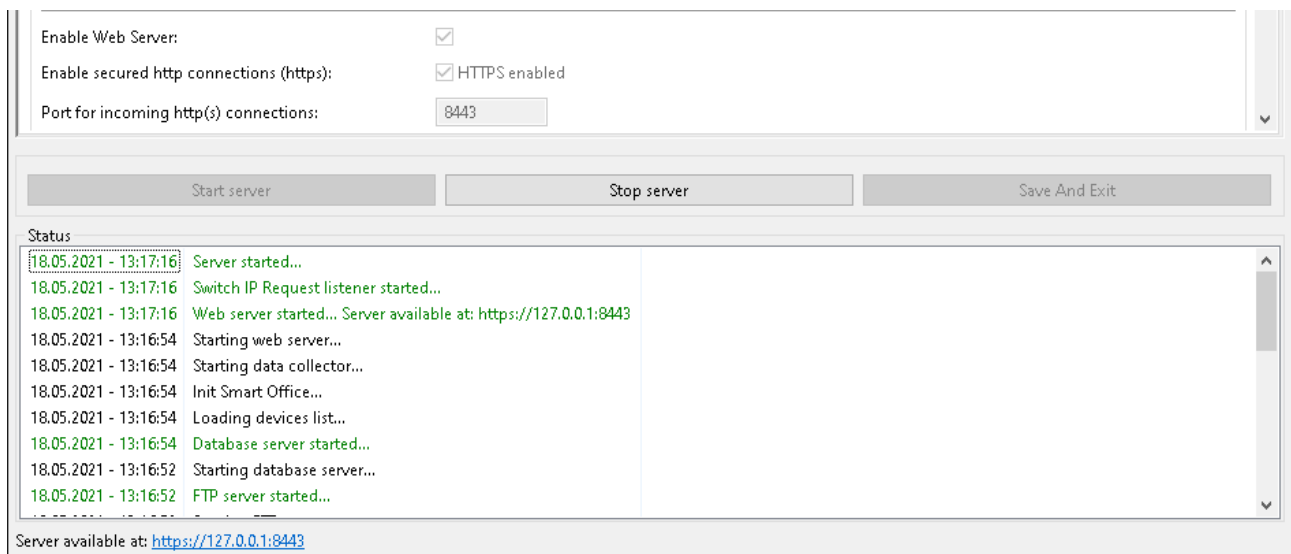


Figure 30. Server Manager - Configuring and Starting the Web Server

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>/`



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

7.2. Start Server Process

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

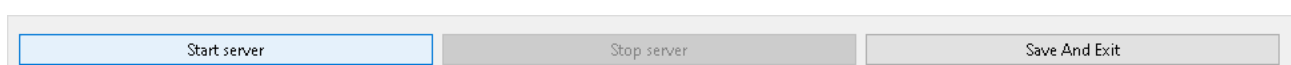


Figure 31. Server Manager - Start Server Process

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

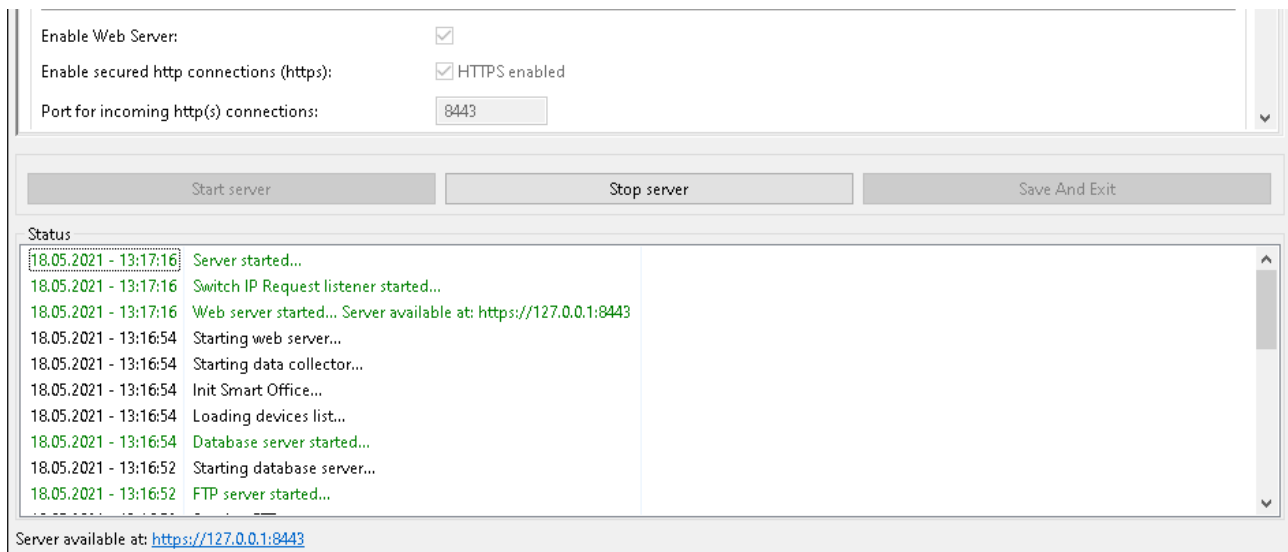


Figure 32. Server Manager - Status Field and Server URL

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

7.3. 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.

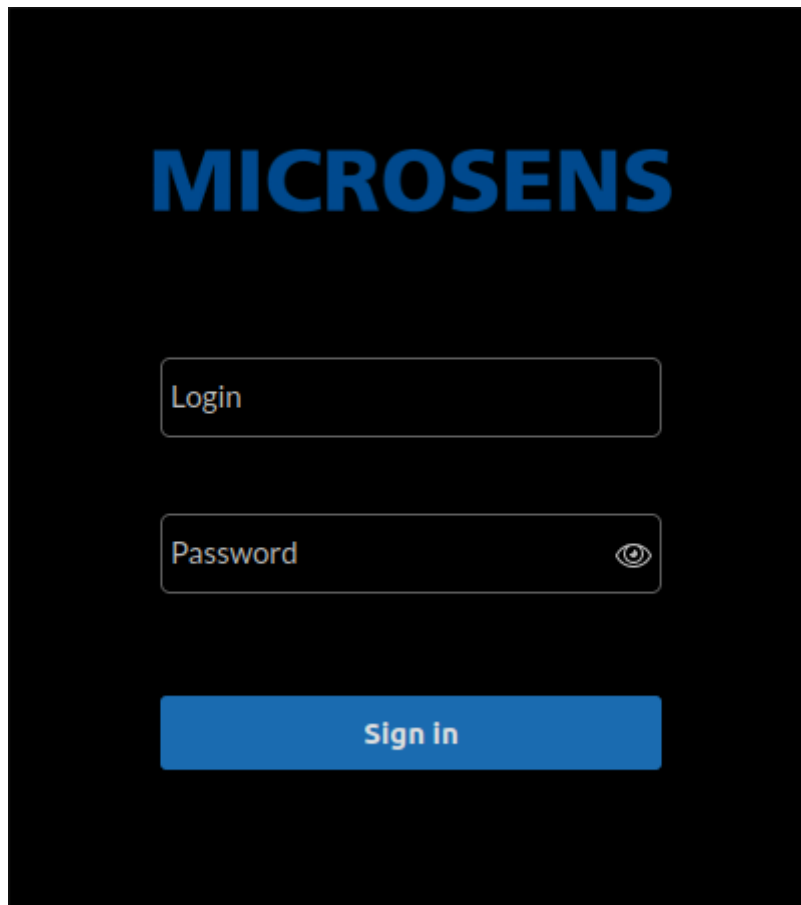


Figure 33. WEB UI - Login Screen



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.

7.4. 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 successful login into the Web UI, the tiles of all available applications appear.

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

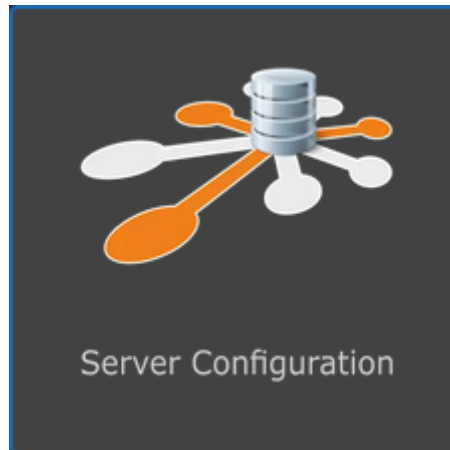


Figure 34. Web UI - Application "Server Configuration"

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.

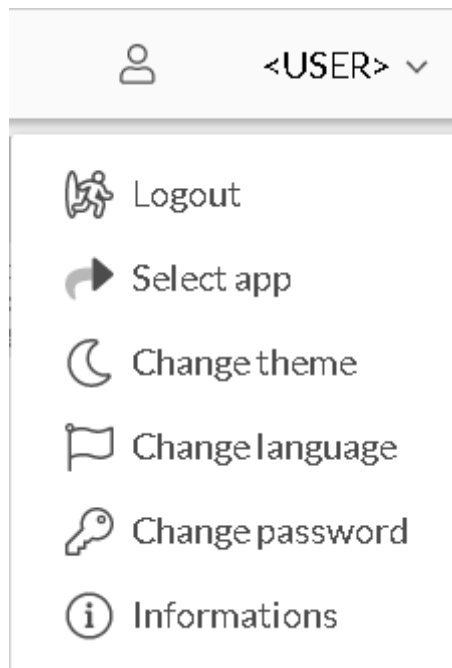


Figure 35. Web UI - User Menu

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

7.5. Application "Server Configuration" Overview

The application starts with a quick overview of the server status.

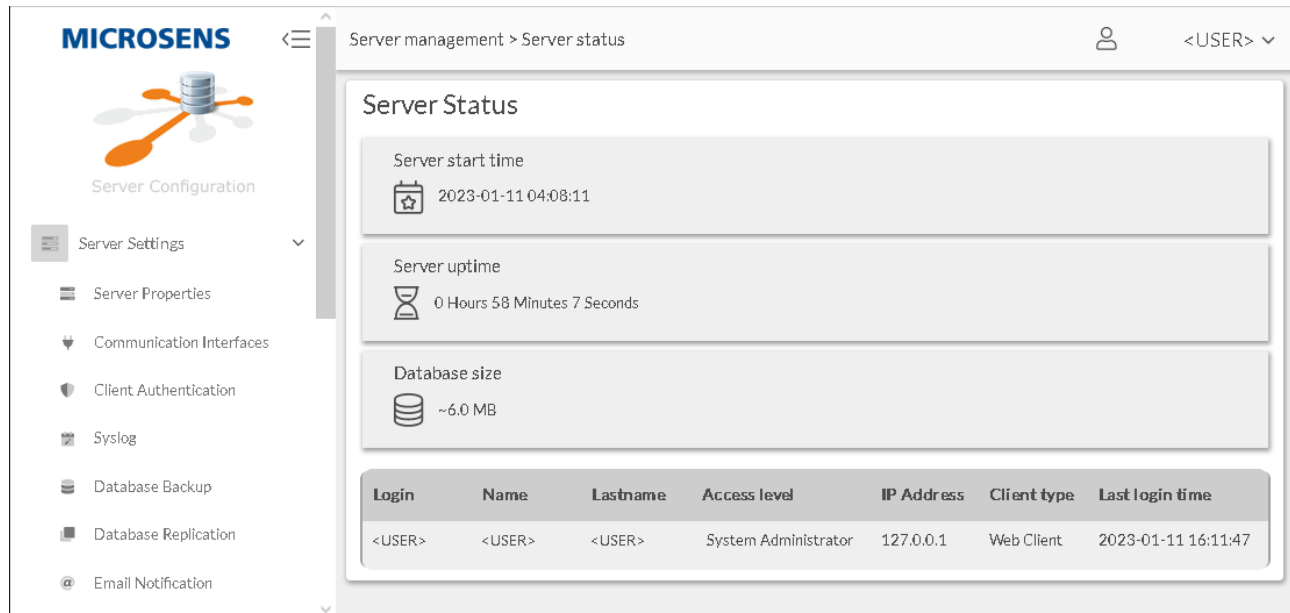


Figure 36. Web UI - Server Configuration - Start Page

In the navigation panel of the server screen click on the menu entry Server Settings to open the sub-menu entries.

The following server setting screens are available:

- Server Properties
- Communication Interfaces
- Client Authentication
- Syslog
- Database Backup
- Database Replication
- Email Notification
- SNMP Agent Communication
- SNMP Trap Relay
- InfluxDB Integration
- MQTT
- PMS/FIAS
- Server Startup-Logs
- Server Status (selected when opening the application)
- Server Diagnostic
- Server Ports

7.6. Server Properties

The menu Server Properties contains the following settings and options:

- **General Settings:** General settings for data directory, password protection and start-up handling.
- **Web Server Configuration:** Web server settings for security and ports.
- **Devices Discovery Settings:** Parameters for communication between the server process and connected devices.

Click on the button **Apply Configuration** of the respective dialogue to apply all changes to the server.

Changing the dialogue without clicking this button will discard all changes.

7.6.1. General Settings

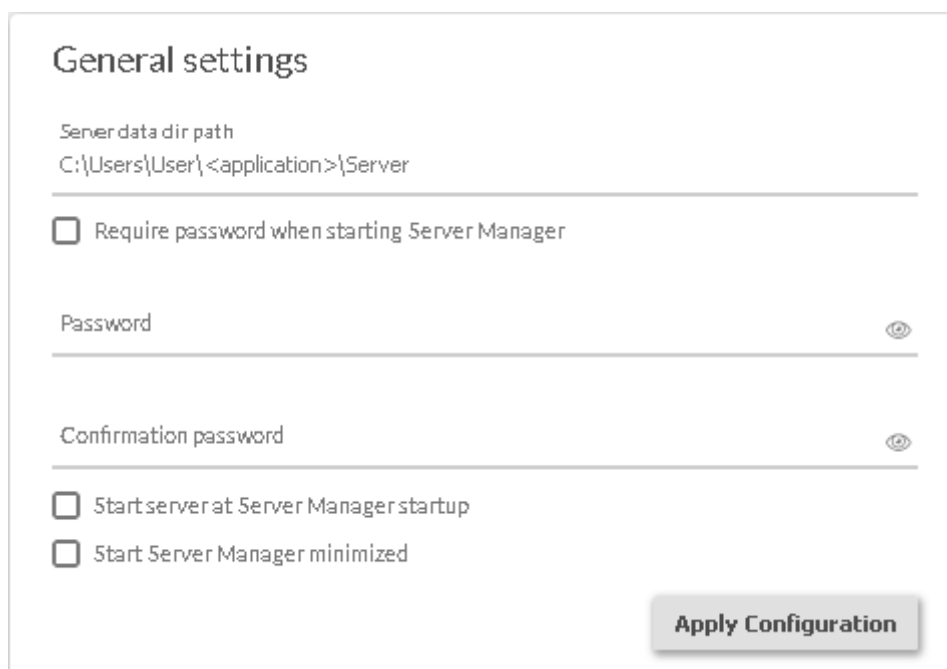
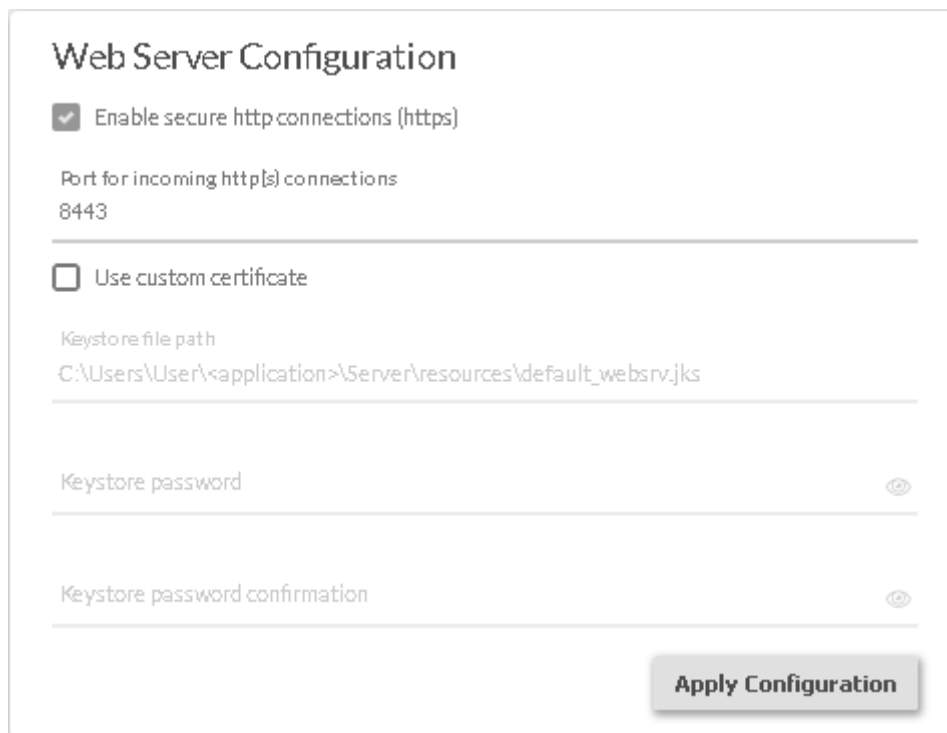


Figure 37. Web Server - Server Configuration - Server Properties - General Settings

- **Server data dir path:** Select the location where the server will save all configuration files and database data. In the selected destination folder, a respectively named folder will be created.
- **Require password on Server Manager startup:** Check this option to request a password when starting the Server Manager. Enter and confirm the password below.
- **Start server on Server Manager startup:** Automatically starts the server instance (database engine, device data collector and, if enabled, HTTP(S) server) on start-up. If the Server Manager is added to the list of OS auto-start applications, the application's Server Manager will be started automatically and ready to use after OS boot.

- **Start Server Manager minimized:** Starts the Server Manager window in a minimized manner. The most important Server Manager features will be available via the system tray icon.

7.6.2. Web Server Configuration



The image shows a 'Web Server Configuration' dialog box. It has a title bar and a main area with several settings. At the top, there's a checkbox labeled 'Enable secure http connections (https)' which is checked. Below this is a text field for 'Port for incoming http(s) connections' with the value '8443'. Further down is another checkbox labeled 'Use custom certificate' which is unchecked. Below that is a text field for 'Keystore file path' with the value 'C:\Users\User\<application>\Server\resources\default_websrv.jks'. There are two more text fields: 'Keystore password' and 'Keystore password confirmation', both with eye icons to the right. At the bottom right is a button labeled 'Apply Configuration'.

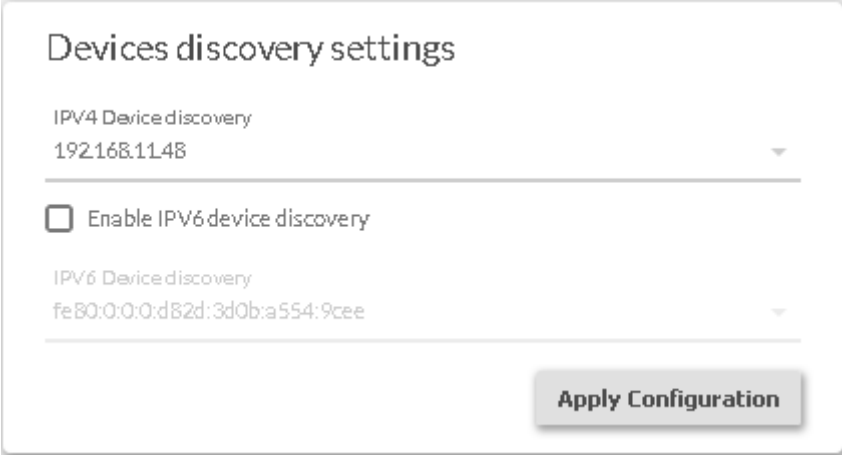
Figure 38. Web Server - Server Configuration - Server Properties - Web Server Configuration

- **Enable secured http connections (https):** The server instance offers secured HTTP connections for web access. The https connections are encrypted so the communication between clients and server is safe.
- **Port for incoming https(s) connections:** The port that will be used for the HTTP(S) server. On default the server instance uses the ports **8080** for standard HTTP and **8443** for HTTPS connections.
- **Use custom certificate:** Check this option to use your own certificate for https communication. The certificate is stored inside a Java KeyStore (JKS) repository.
- **Key store file path:** Select the directory and the name of the JKS file.
- **Key store password:** Enter and confirm the password that is protecting the JKS file.



For more information about creating the JKS file please refer to the application's user manual.

7.6.3. Devices Discovery Settings



Devices discovery settings

IPv4 Device discovery
192.168.11.48

☐ Enable IPv6 device discovery

IPv6 Device discovery
fe80:0:0:0:d82d:3d0b:a554:9cee

Apply Configuration

Figure 39. Web Server - Server Configuration - Server Properties - Devices Discovery Settings

- **IPv4 device discovery:** Shows 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 network) for client access. Thanks to this function the clients do not have the direct access to managed devices. The devices can be accessed exclusively through the server process.
- **Enable IPv6 device discovery:** Check this option to enable device discovery via IPv6.
- **IPv6 device discovery:** Shows the IPv6 address of the network interface that will be used for communication with the managed devices.

7.7. Communication Interfaces

The menu Communication Interfaces contains the following settings and options:

- **Device Communication Settings:** Parameters for communication between the server instance and connected devices.
- **Client Server Communication Settings:** Parameters for communication between server instance and the application's client component.

Click on the button Apply Configuration of the respective dialogue to apply all changes to the server.

7.7.1. Device Communication Settings

Device communication settings

IPv4 interface for device communication
192.168.11.48

☐ Enable IPv6 Interface for device communication

IPv6 interface for device communication
0:0:0:0:0:0:1

☐ Use built in SNMP Trap Listener (UDP port 162)

Max. concurrent data poll threads
50

Apply Configuration

Figure 40. Web Server - Server Configuration - Communication Interfaces - Device Communication Settings

- **IPv4 Interface for device communication:** The IPv4 address of the network interface that is 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 network) for client access. Thanks to this function, clients do not have the direct access to managed devices. The devices can be accessed exclusively through the server instance.
- **Enable IPv6 Interface for device communication:** Check this option, if one or more managed devices of your infrastructure are using IPv6.
- **IPv6 Interface for device communication:** The IPv6 address of the network interface that is used for communication with the managed devices.
- **Use built-in SNMP Trap Listener (on port udp/162):** The server has a built-in SNMP trap listener to receive traps from network devices. On default the trap listener is disabled. If there is no other trap receiver in use in the network, it is possible to enable this function.
- **Max. concurrent data poll threads:** This parameter is used to define the number of devices that can be polled simultaneously. For slower servers, heavy loaded networks or slow network connections, we recommend reducing this value for a better performance.

7.7.2. Client Server Communication Settings

Client Server communication settings

Interface for client-server commands
127.0.0.1

Port
4000

FTPS (FTP over SSL) Server port
4001

FTP User
msserverftp

FTP Password
●●●●●●●●●●

FTP Password confirmation

Database Server port
4002

Apply Configuration

Figure 41. Web Server - Server Configuration - Communication Interfaces - Client Server Communication Settings

- **Interface for client-server communication:** The IPv4 address of the network interface that is used for the application's client access. If the HTTP server is enabled for web client access, the interface is also used by the built-in HTTP server.
- **Port:** The port that is used by the application's client to communicate with the server instance (4000 on default).
- **FTPS (FTP over SSL) Server port:** The built-in FTPS server is used by the application's client to synchronise device lists and firmware updates (4001 on default).
- **FTP User:** Enter the user name that is registered in the FTP server.
- **FTP Password/confirmation:** Enter and confirm the user password that is registered in the FTP server.
- **Database Server port:** The port used by the built-in database server for the application's client access (4002 on default).

7.8. Client Authentication

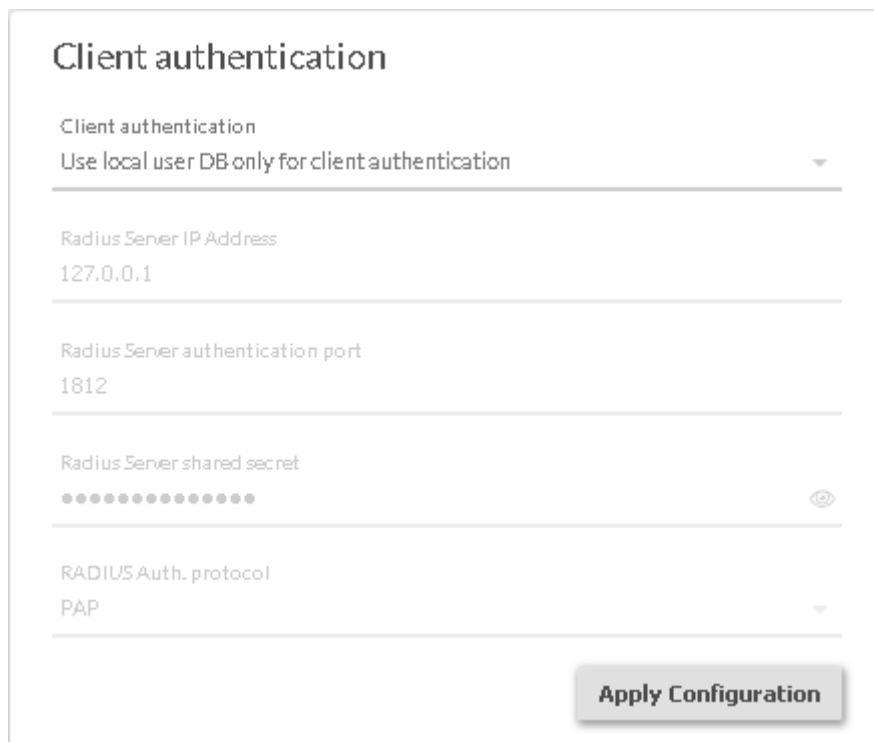


Figure 42. Web Server - Server Configuration - Client Authentication

- **Client authentication:** Select the authentication mode from the drop-down list:
 - Use local user DB only for client authentication: The server will use the information from its local database for user authentication.
 - Use local user DB and RADIUS Server for client authentication: The server will use the defined RADIUS server in order to authenticate the user. A local user account (in the local server database) will be created automatically (if such an account does not exist).



The server will be able to authenticate a new user and create a local account if the number of currently existing accounts are lower than the number of allowed user accounts defined by the application's server licence. Access to the server will be granted if the RADIUS server will return the **RADIUS ACCESS ACCEPT** message and the local user's credentials exist.

- Use RADIUS Server only for client authentication: The server will use a RADIUS server for user authentication.
- **RADIUS Server IP address:** The IP address of the RADIUS server.
- **RADIUS Server authentication port:** The port used by RADIUS server for authentication. Default value is **1812**.
- **RADIUS Server Shared Secret:** The RADIUS server shared secret (password) used during the authentication process. Default value is **default_secret**.
- **RADIUS Auth protocol:** The authentication schema used by the RADIUS server (PAP or CHAP).

The user levels of RADIUS server and the application's server are mapped as follows:

RADIUS Server User Level (Value of RADIUS Service Type)	SBM Server User Level
Login-User (1)	sbmuser
Administrative-User (6)	sbmadmin
Callback-Administrative (11)	sbmsysadmin

The following example shows the mapping inside the FreeRADIUS file `users`:

```
sbmsysadmin    Cleartext-Password := "sbmsysadmin"  
               Service-Type = Callback-Administrative-User  
  
sbmadmin       Cleartext-Password := "sbmadmin"  
               Service-Type = Administrative-User  
  
sbmuser        Cleartext-Password := "sbmuser"  
               Service-Type = Login-User
```

When the authentication mode **Use local user DB and RADIUS Server for client authentication** is selected, the application's server treats the RADIUS server as the master authentication server. When the user level (Service-Type) or user password is changed on RADIUS server, the application's server will automatically update the local user account.



The local server database must contain at least one user with **Callback-Administrative** rights. The application's server will refuse to modify the user level of its local account, resulting in no local user with **Callback-Administrative** rights remaining.

After deleting a user account from RADIUS server, the local server account will not be deleted automatically. The system administrator should delete the user account from the local server database manually.



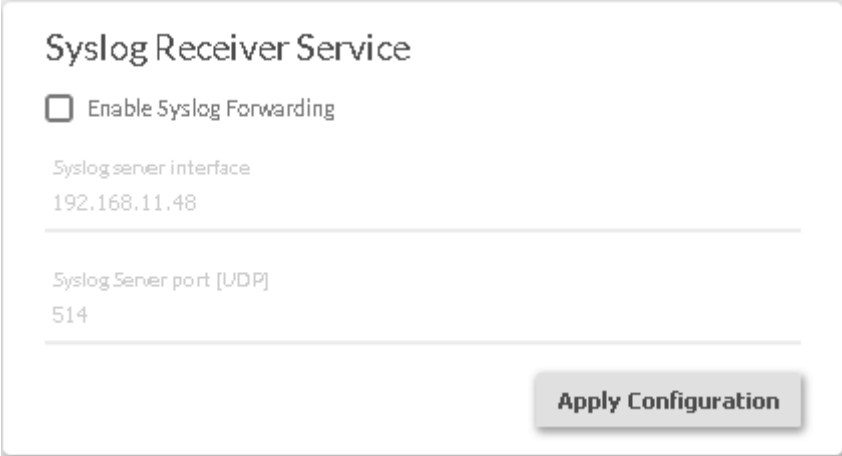
Please keep in mind that the number of application's users available on the RADIUS server should be identical to the number of user accounts allowed by the application's licence key file.

7.9. Syslog

The menu Syslog contains the following settings and options:

- **Syslog Receiver Service:** Settings for the server acting as a Syslog server.
- **Syslog Forwarding Service:** Settings for the server acting as a Syslog client.
- **Local Logs:** Configure the log handling.

7.9.1. Syslog Receiver Service



Syslog Receiver Service

☐ Enable Syslog Forwarding

Syslog server interface
192.168.11.48

Syslog Server port [UDP]
514

Apply Configuration

Figure 43. Web Server - Server Configuration - Syslog - Syslog Receiver Service

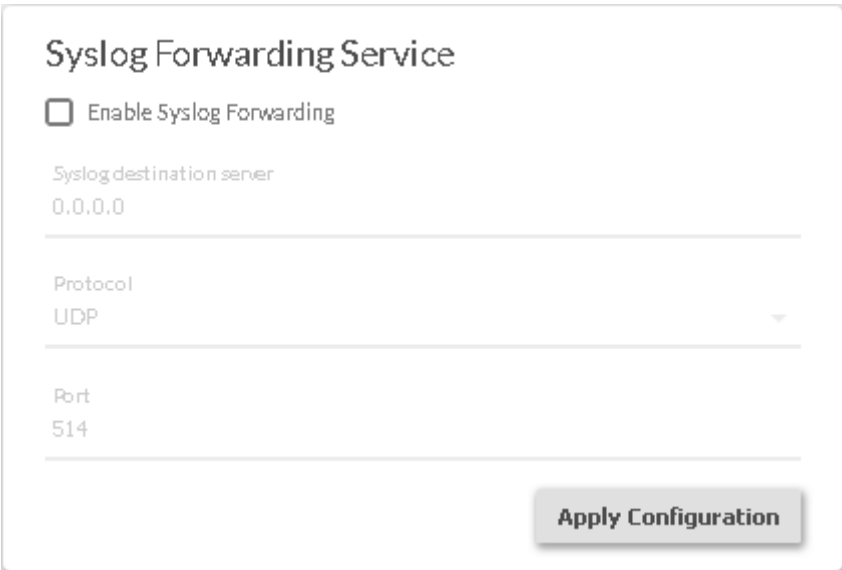
- **Enable Syslog Receiver:** The application's server can act as a Syslog server. In such case, all the Syslog messages sent by devices will be saved within the application's server database.
- **Syslog server interface:** The IP address of the network interface used by the Syslog server.



This interface is always identical to the interface defined for server-devices communication.

- **Syslog server port [udp]:** The UDP port on which the Syslog server listens for incoming messages. Default value is 514.

7.9.2. Syslog Forwarding Service



Syslog Forwarding Service

☐ Enable Syslog Forwarding

Syslog destination server
0.0.0.0

Protocol
UDP

Port
514

Apply Configuration

Figure 44. Web Server - Server Configuration - Syslog - Syslog Forwarding Service

- **Enable Syslog Forwarding:** Enables the Syslog client function. In this mode the

application's server will send Syslog messages.

- **Syslog destination server:** The IP address of the Syslog server, where the application's server sends Syslog messages.
- **Protocol/Port:** Protocol (TCP/UDP) and port which should be used by the Syslog client. This should be configured in accordance with Syslog server requirements.

7.9.3. Local Logs

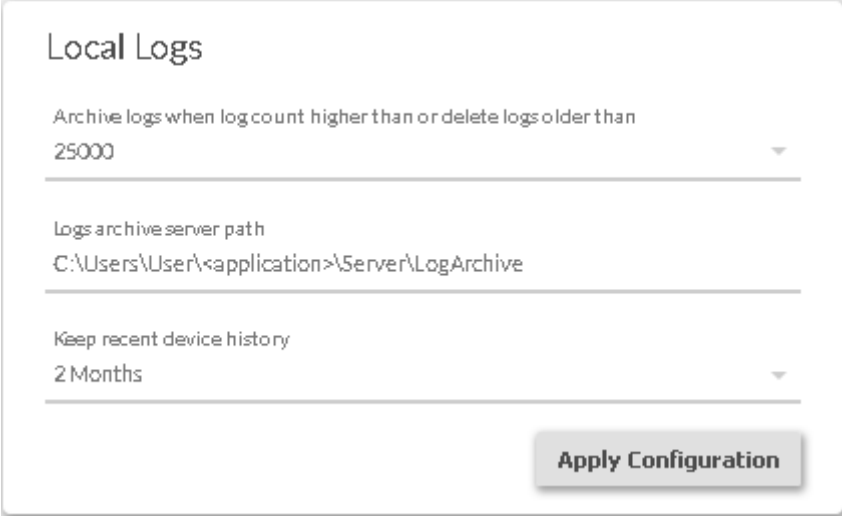


Figure 45. Web Server - Server Configuration - Syslog - Local Logs

- **Archive logs when log count higher than or delete logs older than:** The application's server will generate a **.csv** file with log messages when the number of log messages in the database will be higher than the defined log count limit (25000, 50000 or 100000 messages) or older than the defined log age (1, 2, 6 or 12 months).

The archived messages will be deleted from the database to prevent unlimited growth of the database size. The server starts the archiving procedure each day at 2 a.m.. The last 500 and all unacknowledged messages are always kept in the database (i.e. they are not deleted during the archiving procedure).

- **Logs archive server path:** Choose the location where application's server should save the log archives.
- **Keep device history from last:** The application's server saves parameters like device temperature or device availability in the database which are used to create device history charts. To prevent unlimited growth of the database size, the server deletes history entries older than **n`** months. The maximum time for keeping the history is 12 months. The server clears the database each day at 2 a.m.

7.10. Database Backup

The menu Database Backup contains the following settings and options:

- **Database Backup:** Configure the backup folders for the database copy.

- **Schedule Database Backups:** Configure periodical backups of the database.

Click on the button **Apply Configuration** of the respective dialogue to apply all changes to the server.

7.10.1. Database Backup

The server allows the creation of a backup copy of the database currently in use.

The backups will be saved as **.zip** archives. The filename contains the current date (e.g. **SBMS_DB_BACKUP_2018-06-15.zip**).




If a file with the same name already exists in the backup folder, the current time in milliseconds will be appended after the current date to distinguish the files.

The image shows a 'Database Backup' configuration window. It has two main sections. The first section, 'Backup to selected folder', is selected with a checked checkbox. It contains fields for 'Folder dir path' (C:\Users\User\Server), 'Server type' (FTP), 'Server IP' (127.0.0.1), 'Server Port' (21), 'User', 'Password' (with a toggle icon), and 'Server Path' (/). The second section, 'Backup to FTP Server', is unselected. A 'Backup' button is located at the bottom right of the dialog.


Figure 46. Web Server - Server Configuration - Database Backup - Database Backup

- **Backup to selected folder:** Check this option to target the backup to a local folder.

- **Folder dir path:** Enter the local path.
- **Backup to FTP Server:** Check this option to target the backup to an FTP server.
- **Server type:** Select the server type of the FTP server.

 | It is recommended to use a secure protocol like FTPS or SFTP.

- **Server IP:** Enter the IP address of the server.
- **Server Port:** Enter the server port of the server.
- **User/Password:** Enter valid credentials of the registered FTP user
- **Server Path:** Enter the server's path to the backup folder (e.g. */Some Folder/Backup*).

 | If the backup file should be saved in the FTP server's root directory, an empty string or "/" is required.

By clicking the button **Backup**, the backup starts automatically.

7.10.2. Schedule Database Backups

It is possible to enable periodically scheduled backups, based on the directory settings above.

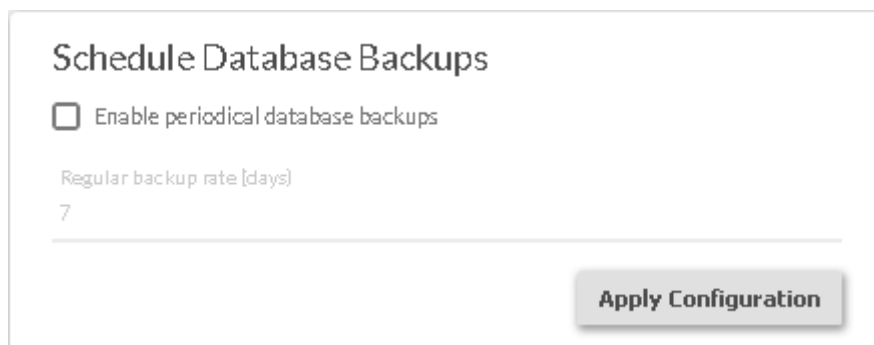


Figure 47. Web Server - Server Configuration - Database Backup - Schedule Database Backups

- **Enable periodical database backups:** Enable or disable periodic database backups.
- **Regular backup rate (days):** The server will backup the database automatically every *x* days (1 to 30).

7.11. Database Replication

This dialogue allows the configuration of two server instances in master-slave mode to replicate the current database.

The screenshot shows a web form titled "Database replication". It contains the following fields and options:

- ☐ Enable replication
- Server type: Primary Server (dropdown menu)
- Local replication interface: 127.0.0.1
- Remote replication partner IP address: 127.0.0.1
- Remote replication partner communication port: 4000
- Replication server port: 4177
- Replication failover in service mode: [Q] use the most recent database after the failover as a new primary database (dropdown menu)
- Apply Configuration button

Figure 48. Web Server - Server Configuration - Database Backup

- **Enable replication:** Enable or disable the replication mode.
- **Server type:** Select whether the respective server instance should act as master or as slave server.
- **Local replication interface:** The network interface that will be used by the local server. This interface is always identical to the interface for client-server communication (configured in menu Server Properties).
- **Remote replication partner IP address:** The IP address of the remote replication partner server. This interface must be always identical to the remote server's interface for client-server communication.
- **Remote replication partner communication port:** The port number of the remote replication partner server for client-server communication
- **Replication server port:** The port number that will be used to replicate the database. The port on the local server must be identical to the port configured on the remote replication partner server (default: 4177)
- **Replication failover in service mode:** Select the database that will be used as a new master database after the failover.

Available options are:

- **Use the most recent database after the failover as a new master database:** The most recently used database will be used when the replication will be

restored after a master or slave failure.

- **Use the master database after the failover as a new master database:**
When replication is restored following a master or slave failure, the master server's database is always used.
- **Use the slave database after the failover as a new master database:**
When replication is restored following a master or slave failure, the slave server's database is always used.

In order to start the replication, configure both master and slave server:

- Both servers must have a connection via the network.
- Server instances work in pairs. One of the servers should be configured as a master server, the other one should be configured as a slave server.



The replication will not be initialized when both servers will be configured as masters (or slaves). The replication will also not be initialized when the replication mode is disabled on one of the servers.

- The port used for replication should be exactly the same on both servers.
- Both servers must have access to the managed devices. In case of failure of a server (master or slave), the other one will reboot itself in no-replication mode and will continue device monitoring.

After configuring the replication options, both servers should be started by pressing the **Start server** button in the respective Server Manager. From this point, the servers will automatically initialize the replication.

7.12. Email Notification

The menu Email Notification contains the following settings and options:

- **General Settings:** Configure general email settings.
- **Additional Email Address:** Assign a additional email address.

7.12.1. General Settings

Email notification settings

☒ Enable Email Notifications

SMTP Server

Authentication User

Authentication password

☐ Authentication required

Encryption method
NO ENCRYPTION

SMTP Port
25

Sender email address
NMP_Server@microsens.com

Send test email Apply Configuration

Figure 49. Web Server - Server Configuration - Email Notification - General Settings

The server instance is able to send email notifications on events. The configured SMTP server is used as email relay server. Email notifications are sent to all registered users. The system administrator and all users should configure their proper email addresses.


- **Enable Email Notifications:** If this option is enabled, errors and SNMP trap information is forwarded by email to recipients named below.

| A valid email account with SMTP access is required.

- **SMTP Server:** The address of the SMTP outgoing server (e.g. `smtp.gmail.com`).
- **Authentication user:** Valid user name for this email account.
- **Authentication password:** Valid user password for this email account.
- **Authentication required:** Check this option if the SMTP server requires user authentication.
- **Encryption method:** The encryption used by the SMTP Server. The following selection is possible:
 - **NO_ENCRYPTION:** Connection and communication between email server and client is not encrypted.
 - **SSL:** On first step an encrypted TLS/SSL connection between email server and

client is established. Afterwards both server and client communicate secure via an encrypted channel. This selection is strongly recommended!

- **TLS:** When using a STARTTLS encryption both server and client primarily negotiate their encryption capabilities and subsequently establish an encrypted connection if possible. All prior communication happens unencrypted.

 | Only TLS 1.2 and newer is supported.

- **SMTP Port:** The SMTP server port.
- **Sender email address:** The email address used in the field "From" of the sent message.

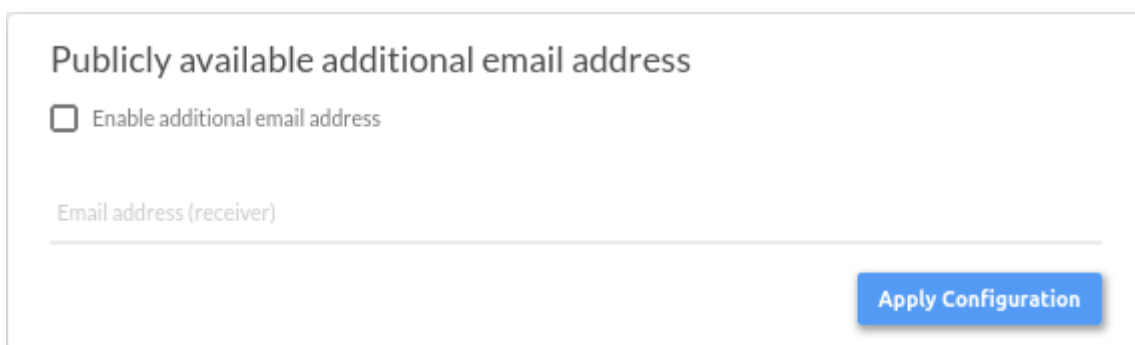
Click on [Send test email](#) to send an email to the assigned email address.



Check the email account's spam folder if the email is not received after a short while.

7.12.2. Additional Email Address

The server is able to send email notifications to an additional (publicly available) email address not related to any of the registered user accounts.



Publicly available additional email address

☐ Enable additional email address

Email address (receiver)

Apply Configuration

Figure 50. Web Server - Server Configuration - Email Notification - Additional Email Address

- **Enable additional email address:** Check this option to enable sending messages to an additional email address.
- **Email address (receiver):** Enter a valid email address for an additional notification receiver.

7.13. SNMP Agent Communication

The SNMP protocol can be used to make management data available to other management systems. The server instance offers a northbound interface in the form of an SNMP Agent. A *northbound interface* is an interface that allows a particular component of a network to communicate with an upper level component.

The menu SNMP Agent Communication contains the following settings and options:

- **SNMP Receiver Service Settings:** Configure general SNMP settings like enable or

disable specific SNMP protocols.

- **SNMPv1/SNMPv2 communication settings:** Configure settings for SNMPv1 and SNMPv2 protocol.
- **SNMPv3 communication settings:** Configure settings for SNMPv3 protocol.

Click on the button **Apply Configuration** of the respective dialogue to apply all changes to the server.

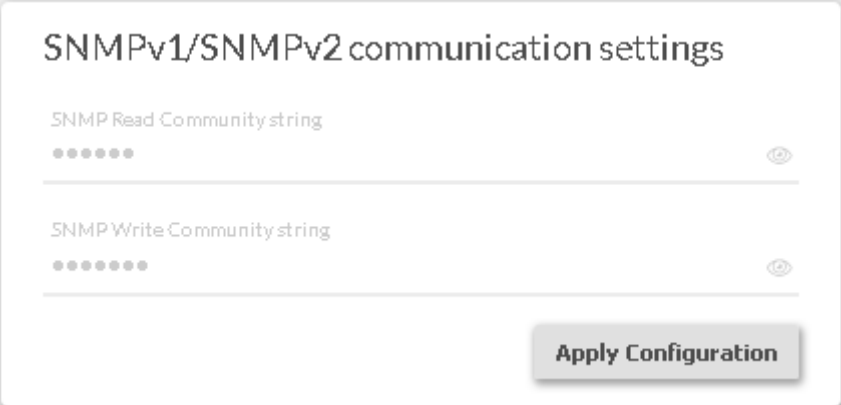
7.13.1. SNMP Receiver Service Settings



Figure 51. Web Server - Server Configuration - SNMP Agent Communication - SNMP Receiver Service Settings

- **Enable SNMP Agent:** Enabling the SNMP agent allows the other SNMP managers to see the management data collected by the server instance.
- **SNMP Agent interface:** The IP address of the network interface used by the SNMP Agent, via which other SNMP managers can query data. The interface is configured via the Server Properties and is always identical to the **Interface for client-server communication**.
- **SNMP Agent port:** The port that is used by the SNMP Agent.
- **SNMP version:** Select the SNMP product variant needed to be supported by the SNMP Agent. At least one version should be enabled.
- **Sender email address:** Enter the sender's email address.

7.13.2. SNMPv1/SNMPv2 Communication Settings

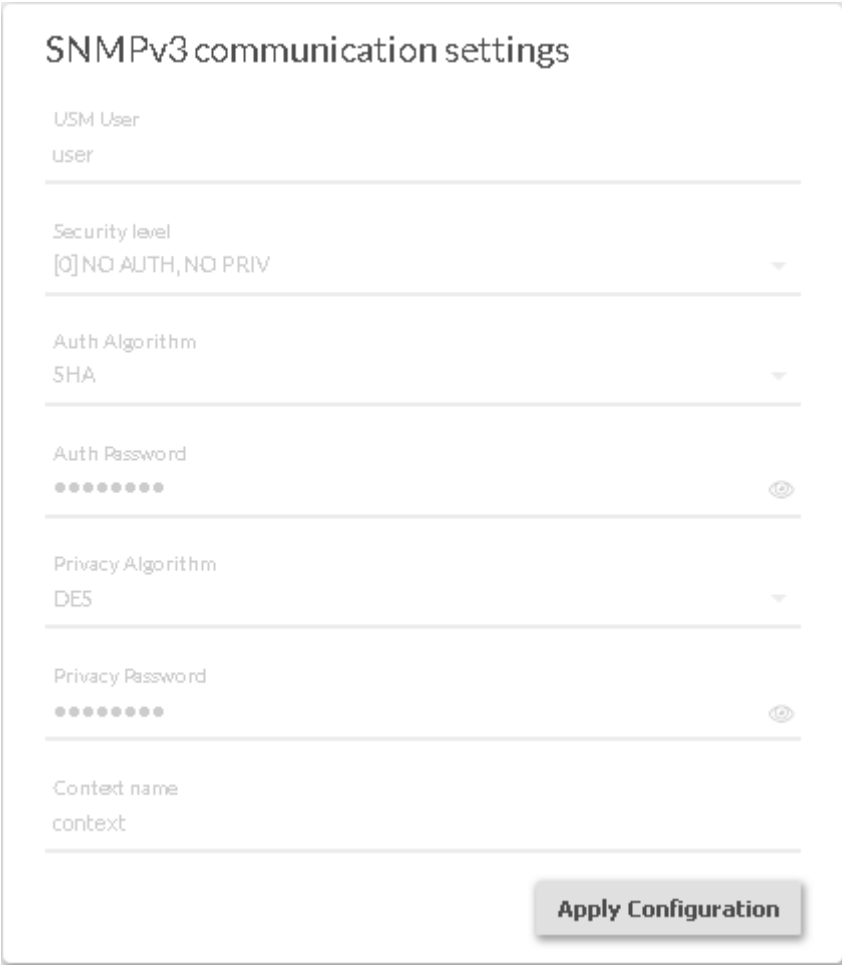


The screenshot shows a web interface titled "SNMPv1/SNMPv2 communication settings". It contains two text input fields. The first field is labeled "SNMP Read Community string" and has a password mask of seven dots. The second field is labeled "SNMP Write Community string" and has a password mask of eight dots. To the right of each field is a small eye icon for toggling visibility. At the bottom right of the form is a button labeled "Apply Configuration".

Figure 52. Web Server - Server Configuration - SNMP Agent Communication - SNMP Receiver Service Settings

- **SNMP Read Community string:** The read-only community string allows other SNMP managers to read data values.
- **SNMP Write Community string:** The read-write community string allows other SNMP managers to read and write data values.

7.13.3. SNMPv3 Communication Settings



The image shows a web form titled "SNMPv3 communication settings". It contains several input fields and dropdown menus. The fields are: "USM User" with the value "user"; "Security level" with a dropdown menu showing "[0] NO AUTH, NO PRIV"; "Auth Algorithm" with a dropdown menu showing "SHA"; "Auth Password" with a masked password field (dots) and an eye icon; "Privacy Algorithm" with a dropdown menu showing "DES"; "Privacy Password" with a masked password field (dots) and an eye icon; and "Context name" with the value "context". At the bottom right of the form is a button labeled "Apply Configuration".

Figure 53. Web Server - Server Configuration - SNMP Agent Communication - SNMP Receiver Service Settings

- **USM User:** The security name of the user (typically the user name).
- **Security level:** The SNMPv3 agent supports the following security levels as defined in the USM MIB (RFC 2574):
 - **NO AUTH, NO PRIV:** Communication without authentication and privacy.
 - **AUTH, NO PRIV:** Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
 - **AUTH, PRIV:** Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA. For privacy, the DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used.
- **Auth Algorithm:** The authentication protocol ID to be associated with this user.
- **Auth Password:** The authentication passphrase.
- **Privacy Algorithm:** The privacy protocol ID to be associated with this user.
- **Privacy Password:** The privacy passphrase.
- **Context name:** An SNMP context is a collection of management information accessible by an SNMP entity.

7.14. SNMP Trap Relay

SNMP Trap Destination

Destination	Version	IP Address	UDP port	Community
0:	Disable ▾	0.0.0.0	162	*****
1:	Disable ▾	0.0.0.0	162	*****
2:	Disable ▾	0.0.0.0	162	*****
3:	Disable ▾	0.0.0.0	162	*****

Apply Configuration

Figure 54. Web Server - Server Configuration - SNMP Trap Relay - SNMP Trap Destination

The SNMP agent can send SNMP traps on different events generated by the server instance and can resend the traps received from other devices. It is possible to configure up to 4 different trap destinations. For each destination choose between the SNMP v1, v2c or v3 trap versions.

7.15. InfluxDB Integration

Within the SBM infrastructure environment, the open source database management system *InfluxDB* enables the customer to visualise and analyse the data collected by the connected MICROSENS Smart Building controllers.

Influx Database Integration Settings

☐ Enable InfluxDB Integration

InfluxDB URL

User name

Password

Database name

Apply Configuration

Figure 55. Web Server - Server Configuration - InfluxDB Integration - InfluxDB Integration Settings

- **Enable InfluxDB Integration:** Check this option to enable the InfluxDB client. With the InfluxDB client disabled all other fields are greyed out.
- **InfluxDB URL:** Enter the IP address of the InfluxDB server.
- **User name/password:** Enter the InfluxDB client's credentials that are stored in the InfluxDB server.
- **Database name:** Enter the InfluxDB name.

For more information about using InfluxDB please refer to the respective documentation on the [InfluxDB homepage](#).

7.16. MQTT

SBM Server can act as MQTT broker and client. This is important if you want to use SBM in automation projects with interaction between field devices.



Either activate the internal MQTT broker or the MQTT client for using an external MQTT broker. It is not recommended to enable both MQTT broker and client.

After configuring SBM as MQTT broker or client, restart SBM Server instance for the MQTT settings to take effect.

The menu MQTT contains the following settings and options:

- **MQTT Broker Service:** Configuring the MQTT settings for the server instance acting as MQTT broker.
- **MQTT Data Subscription Settings:** Configuring the MQTT settings for the server instance acting as MQTT client.

Click on the button Apply Configuration of the respective dialogue to apply all changes to the server.

7.16.1. MQTT Broker Service

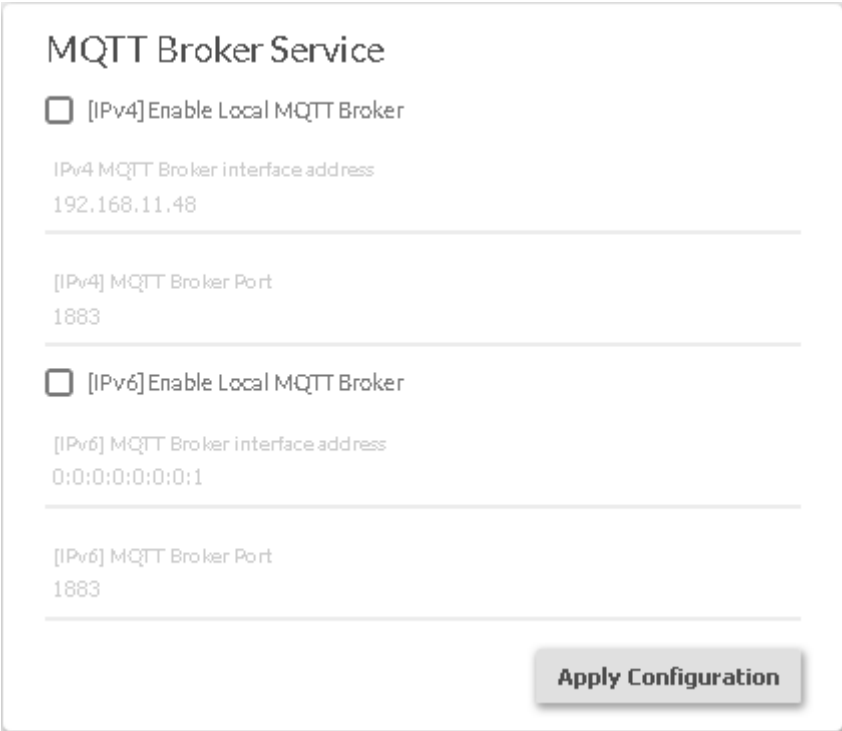


Figure 56. Web Server - Server Configuration - MQTT - MQTT Broker Service

The MQTT broker SBM Server collects and distributes all incoming MQTT data from and to managed MQTT clients, depending on the MQTT clients subscriptions.

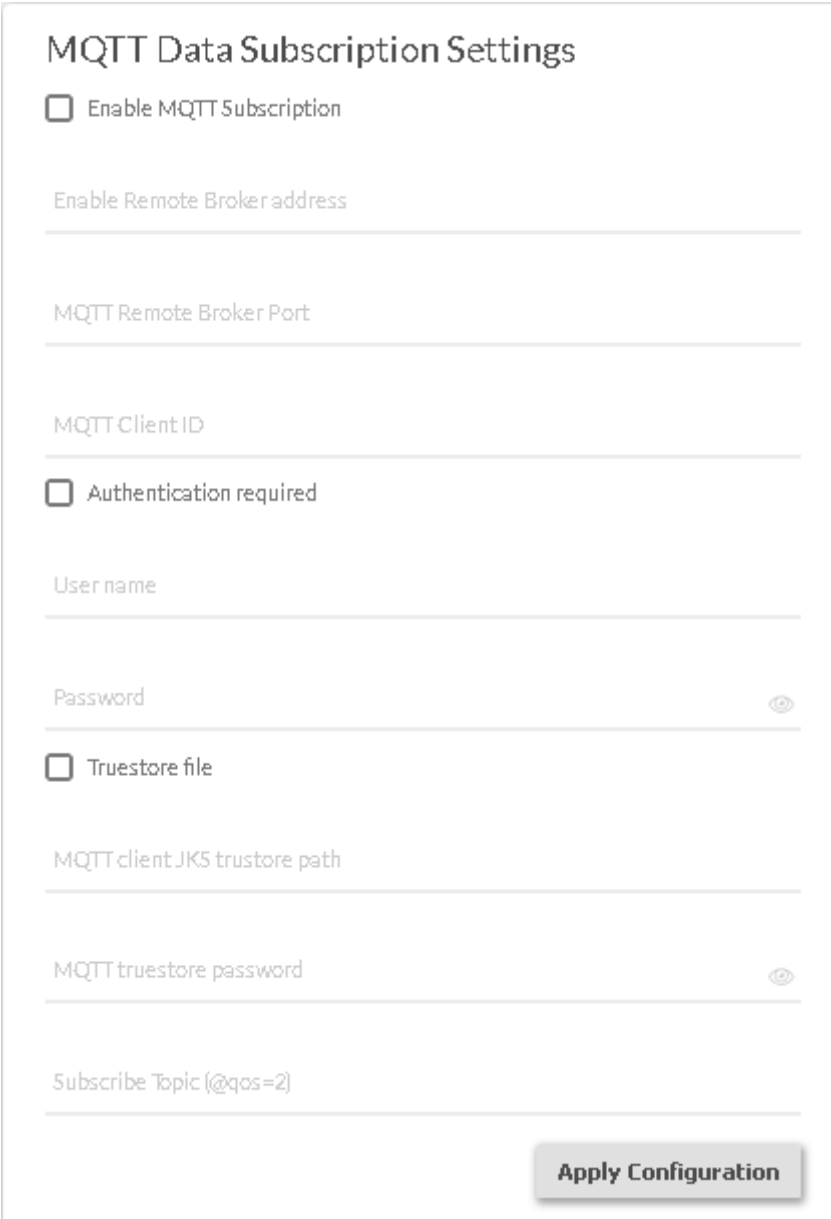


The IPv4/IPv6 interface addresses of MQTT broker should always be identical to the **Interface for client-server communication**, configured via the menu Server Properties.

- **[IPv4] Enable Local MQTT Broker:** Check this option to enable the MQTT broker for IPv4 network communication.
- **[IPv4] MQTT Broker Interface Address:** Enter the IPv4 address of the MQTT broker.
- **[IPv4] MQTT Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (**1883**) as is.
- **[IPv6] Enable Local MQTT Broker:** Check this option to enable the MQTT broker for IPv6 network communication.
- **[IPv6] MQTT Broker Interface Address:** Enter the IPv6 address of the MQTT broker.
- **[IPv6] MQTT Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (**1883**) as is.

7.16.2. MQTT Data Subscription Settings

When acting as MQTT client, SBM holds both the publisher and subscriber roles. Depending on the incoming or outgoing data (i.e. sensors or actuators) it serves or analyses the respective publish or subscription MQTT topics from and to the external MQTT broker.



The screenshot shows a web form titled "MQTT Data Subscription Settings". It contains several configuration options and input fields:

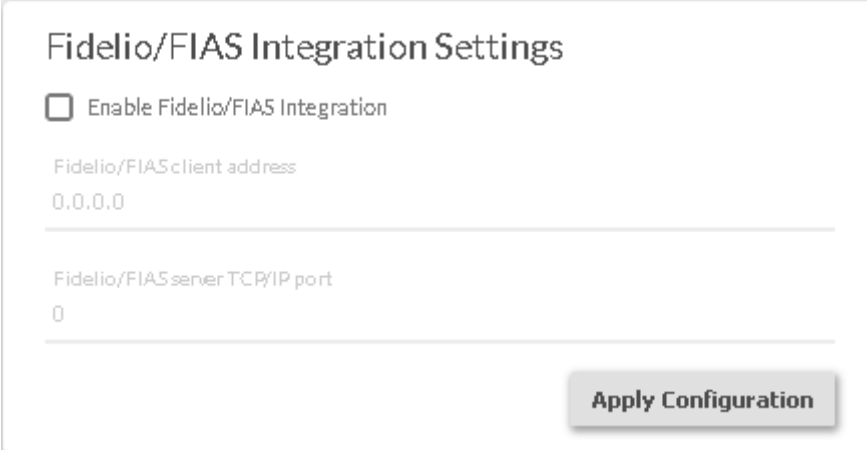
- ☐ Enable MQTT Subscription
- Enable Remote Broker address (text input field)
- MQTT Remote Broker Port (text input field)
- MQTT Client ID (text input field)
- ☐ Authentication required
- User name (text input field)
- Password (password input field with an eye icon for toggling visibility)
- ☐ Truststore file
- MQTT client JKS trustore path (text input field)
- MQTT trustore password (password input field with an eye icon for toggling visibility)
- Subscribe Topic (@qos=2) (text input field)
- An "Apply Configuration" button at the bottom right.

Figure 57. Web Server - Server Configuration - MQTT - MQTT Broker Service

- **Enable MQTT Subscriptions:** Check this option to enable the MQTT client.
- **Enable Remote Broker Address:** Enter the IP address of the MQTT broker the client should connect to.
- **MQTT Remote Broker Port:** Enter the MQTT broker port number. As long as it does not prove necessary, leave the default port (1883) as is.
- **MQTT Client ID:** Enter the unique MQTT client ID.
- **Authentication required:** Check this option if authentication is required for MQTT broker communication.
- **User name/password:** Enter valid MQTT clients credentials
- **TrustStore file:** Check this option if authentication via SSL/TLS is required for MQTT broker communication.

- **MQTT client JKS TrustStore path:** Select the necessary certificate file for SSL/TLS communication.
- **MQTT Truststore password:** Enter the corresponding password for the selected file.
- **Subscribe Topic (@qos=2):** Enter the subscription topic of the MQTT client.

7.17. PMS/FIAS



The screenshot shows a web form titled "Fidelio/FIAS Integration Settings". It contains a checkbox labeled "Enable Fidelio/FIAS Integration". Below this are two text input fields: "Fidelio/FIAS client address" with the value "0.0.0.0" and "Fidelio/FIAS server TCP/IP port" with the value "0". An "Apply Configuration" button is located at the bottom right of the form.

Figure 58. Web Server - Server Configuration - PMS/FIAS - Fidelio/FIAS Integration Settings

- **Enable Fidelio/FIAS Integration:** SBM is equipped with a Fidelio/FIAS client for the management of smart devices in hotel rooms. Check this option to enable the client.
- **Fidelio/FIAS server address:** Enter the Fidelio/FIAS server IPv4 address.
- **Fidelio/FIAS server TCP/IP port:** The port used by the built-in Fidelio/FIAS client to access to the server.

7.18. Server Startup Logs

Server Startup Logs		
Relevance	Time	Message
Info	2023-03-23 01:26:36	Server init...
Info	2023-03-23 01:26:36	Init SSL Context...
Positive	2023-03-23 01:26:38	SSL Context initialized...
Info	2023-03-23 01:26:38	Starting Client-Server commands module...
Positive	2023-03-23 01:27:30	Client-Server commands ready...

Figure 59. Web Server - Server Configuration - Server Startup Logs

This window provides useful information about the current server instance status. All information about starting and stopping the services are available.

7.19. Server Status




Server Status						
<div>Server start time</div> <div>  2023-03-23 01:29:17 </div>						
<div>Server uptime</div> <div>  1 Hours 45 Minutes 28 Seconds </div>						
<div>Database size</div> <div>  ~6.1 MB </div>						
Login	Name	Lastname	Access level	IP Address	Client type	Last login time
Super Admin	Super Admin	Super Admin	System Administrator	192.168.11.64	Web Client	2023-03-23 13:31:36


Figure 60. Web Server - Server Configuration - Server Status

This window provides useful information about the current server instance status:

- Server start time
- Server uptime
- Actual database size

- Login information about all current users which are logged in.

7.20. Server Diagnostic



Logging

Device Polling
OFF

Device Discovery
ALL

Apply Changes

Figure 61. Web Server - Server Configuration - Server Diagnostic

This window enables the use of logging several information.

- Device Polling
- Device Discovery

7.21. Server Ports

Service name	Category	Interface	Port	TCP IP/UDP
Client-Server communication	Management	192.168.11.48	4000	TCP/IP
FTP over SSL Server	Client	192.168.11.48	4001	TCP/IP
Database remote access	Client	192.168.11.48	4002	TCP/IP
NMP / SBM Web Server	Client	192.168.11.48	8443	TCP/IP
MSP100 client-server data exchange	Client	192.168.11.48	4003	TCP/IP
TFTP Server (started when needed)	Management	192.168.11.48	69	UDP
MICROSENS IPv4 Device Discovery	Device	192.168.11.48	8340	UDP
MICROSENS Ring Failure Listener	Device	192.168.11.48	8342	UDP
BOOTP Server	Device	192.168.11.48	67	UDP

Figure 62. Web Server - Server Configuration - Server Ports

This window shows a tabular overview of all used interfaces and ports.

💡 | Use this list for configuring the firewall correctly.

7.22. Certificates

This view allows the management of certificates. The tabular overview shows a list of existing certificates used for SSL/TLS communication of the server instance.

Figure 63. Web Server - Server Configuration - Certificates

- **Use custom TrustStore:** Check this option to enable the use of the custom TrustStore.
- **Upload TrustStore JKS file:** Click on the button **Select file** to select the necessary certificate file for SSL/TLS communication.
- **TrustStore password:** Click on the button **Set password** to enter the corresponding password for the selected file.
- **Add certificate:** Click on this button to store a new certificate.
- **View selected:** In the column Actions click on the button **View** to view the content of the specific certificate.
- **Delete selected:** In the column Actions click on the button **Delete** to delete this certificate.

7.23. Logout from Web UI

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

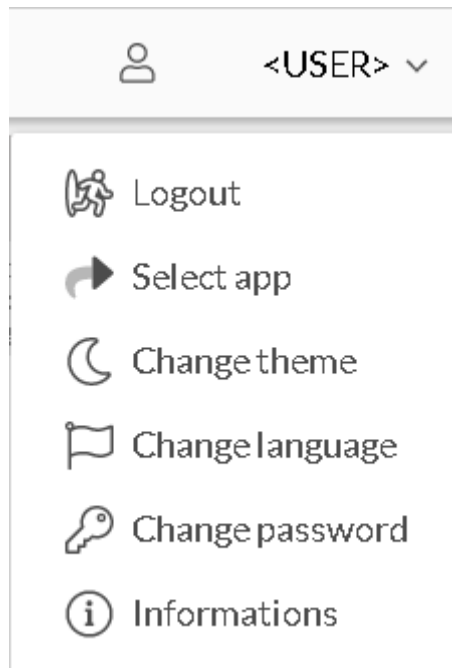


Figure 64. Web UI - User Menu

- The login dialogue appears.

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.

©2023 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: CONF-EN-22001_Smart-Buidling-Manager_Server_v1.4