MICROSENS

Smart Building Manager

Best Practices Guide

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

Table of Contents

Chapter 1. Introduction

This document summarises best practices that can be followed when using the MICROSENS SBM application. It covers the following topics:

- Common Tasks (see Chapter 2)
- Securing Your SBM Instance (see Chapter 3)
- Securing Your Network Devices (see Chapter 4)
- User Management (see Chapter 5)
- Technic Tree (see Chapter 6)
- Data Point Management (see Chapter 7)
- Customising (see Chapter 8)

We would be pleased to hear your additional best practise workflows or solutions while using MICROSENS SBM.

Chapter 2. Common Tasks

- **Keep your SBM application up to date and install the latest version as soon as it is available.**

  You will find the latest version of SBM in the download area of the MICROSENS web page.

  Please note that new versions may have new features not covering your current SBM infrastructure. To get the most out of the latest SBM version, please read the change history, the updated documentation or, if in doubt, contact your MICROSENS representative.

- **Do not customise your SBM instance directly in the productive environment!**

  Run an SBM instance in a test environment in addition to your productive SBM instance.

  This way you can test configuration changes, without putting the productive SBM instance at risk due to misconfiguration.

- **Backup your SBM database regularly by using the application's backup scheduler.**

  For more information on how to use the backup scheduler, please read the SBM Operational Guide.

- **Monitor the system you are running the SBM instance on the following:**
  - Disk space usage (free disk space)
  - CPU load
  - Network traffic (especially in a cloud environment) to detect DDoS attacks
  - User login/logout events to check for failed login attempts.

  For monitoring an SBM instance using open source solutions see the SBM System Monitoring Guide.

Chapter 3. Securing Your SBM Instance

Please perform the actions below for vulnerability assessment.

- **Keep your operating system up to date and apply the latest patch level!**

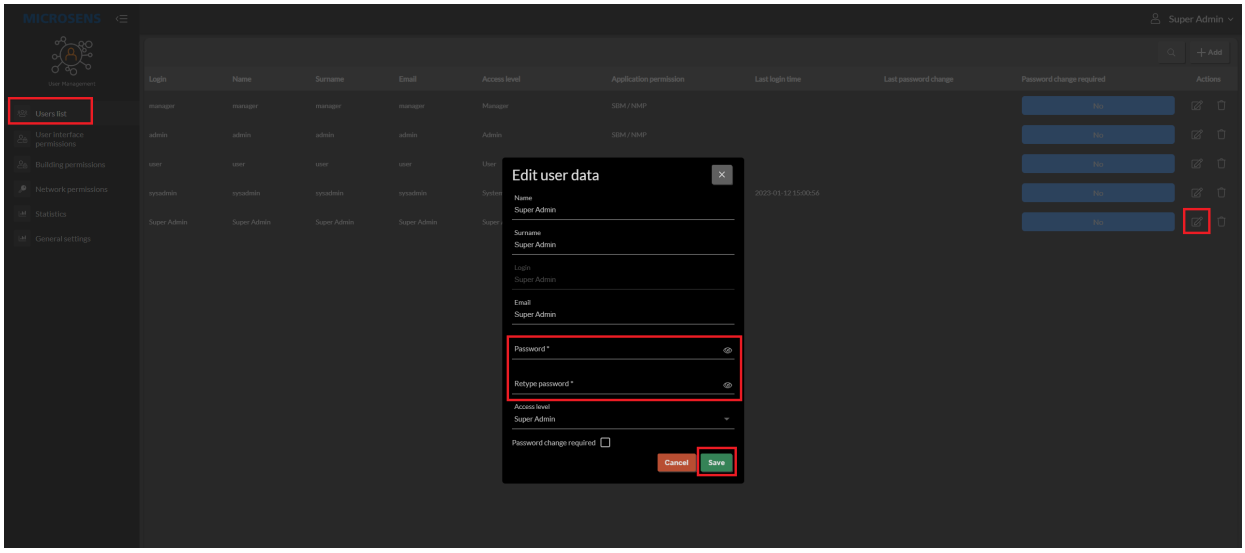
  Your SBM instance will only be as secure as your operating system!

- **Change the password for the user `Super Admin`!**

  SBM comes with several default user accounts with default passwords. At least, change the password of the user `Super Admin`, even if you do not plan to use this account.

  Never leave the default password as is!

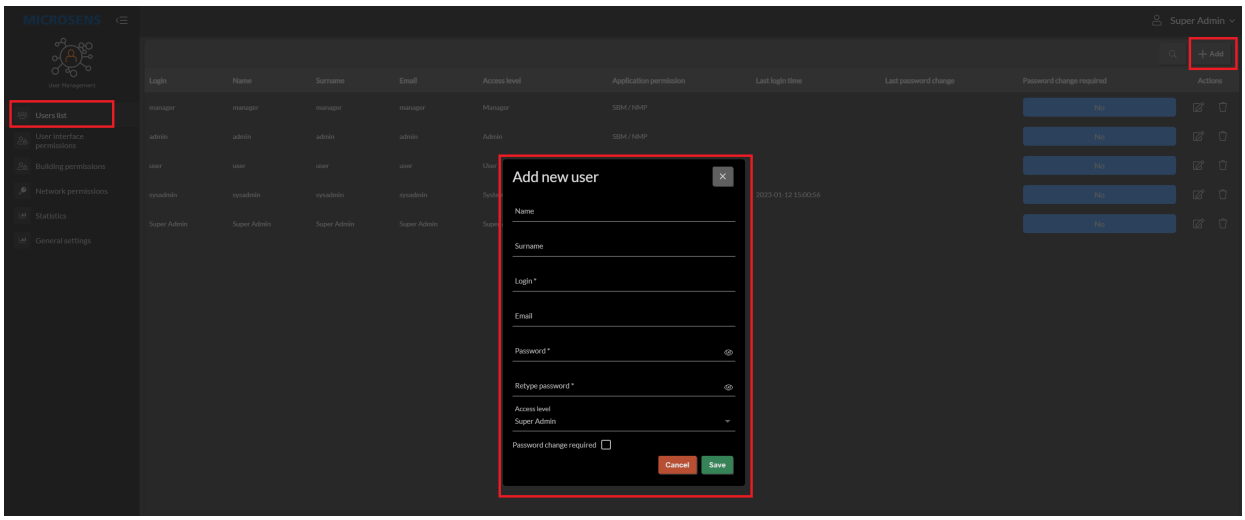
  To change the user password please use "User Management" app via Web Client.



- **Create alternative SBM admin users with Super Admin permissions for your daily work!**

  It is advised to set up a different SBM super admin account. As a result, its account settings can be changed at any time without accidentally causing a valid super admin account inactive.

  To add new user account please use "User Management" app via Web Client.



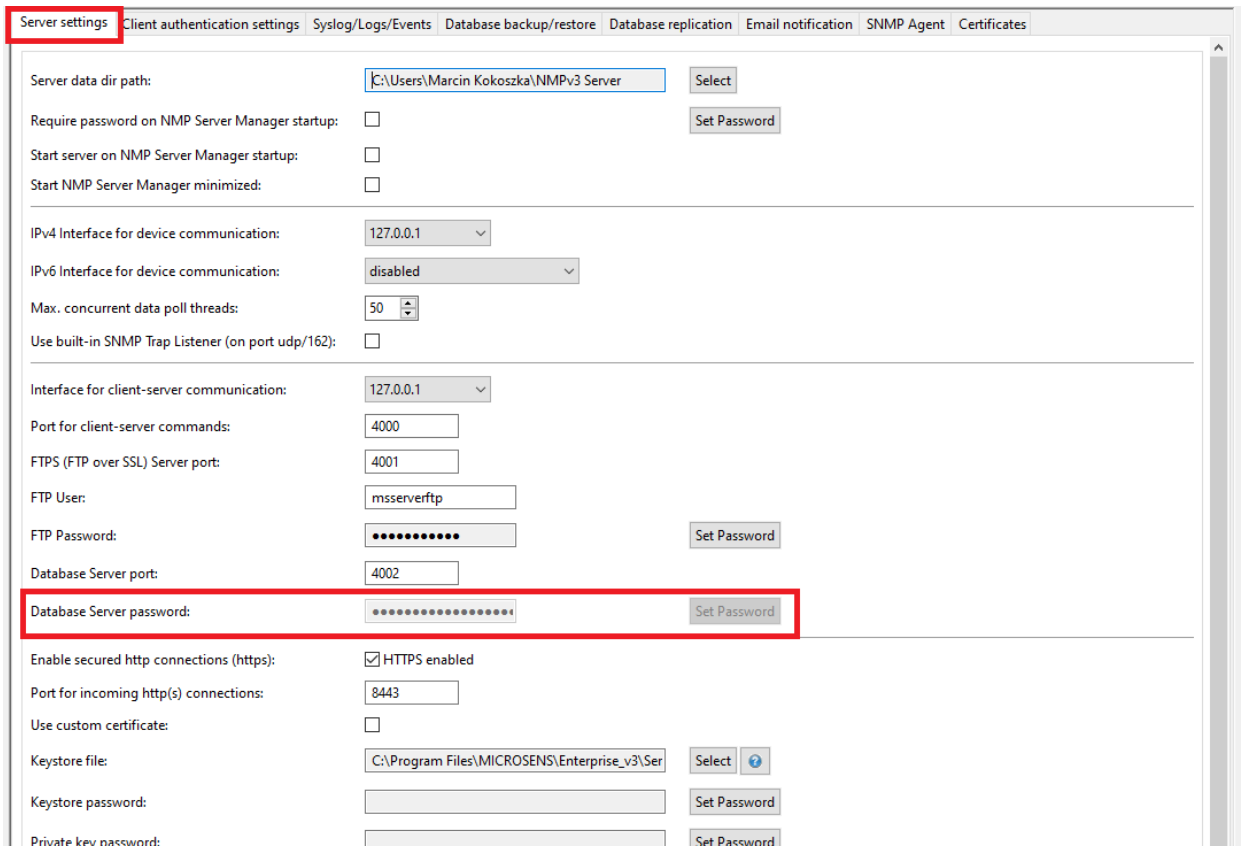
- **Change default passwords for all predefined user accounts**

  During the first installation SBM creates default user accounts (like Super Admin, sysadmin…) which can be also used to manage the network devices via the SBM. These user accounts are created with defualt passwords which should be changed to prevent access to "Device management" app via Web Client.

- **Change password of the SBM database!**

  SBM comes with a default password that secures the SBM database. Change this password within SBM server component.

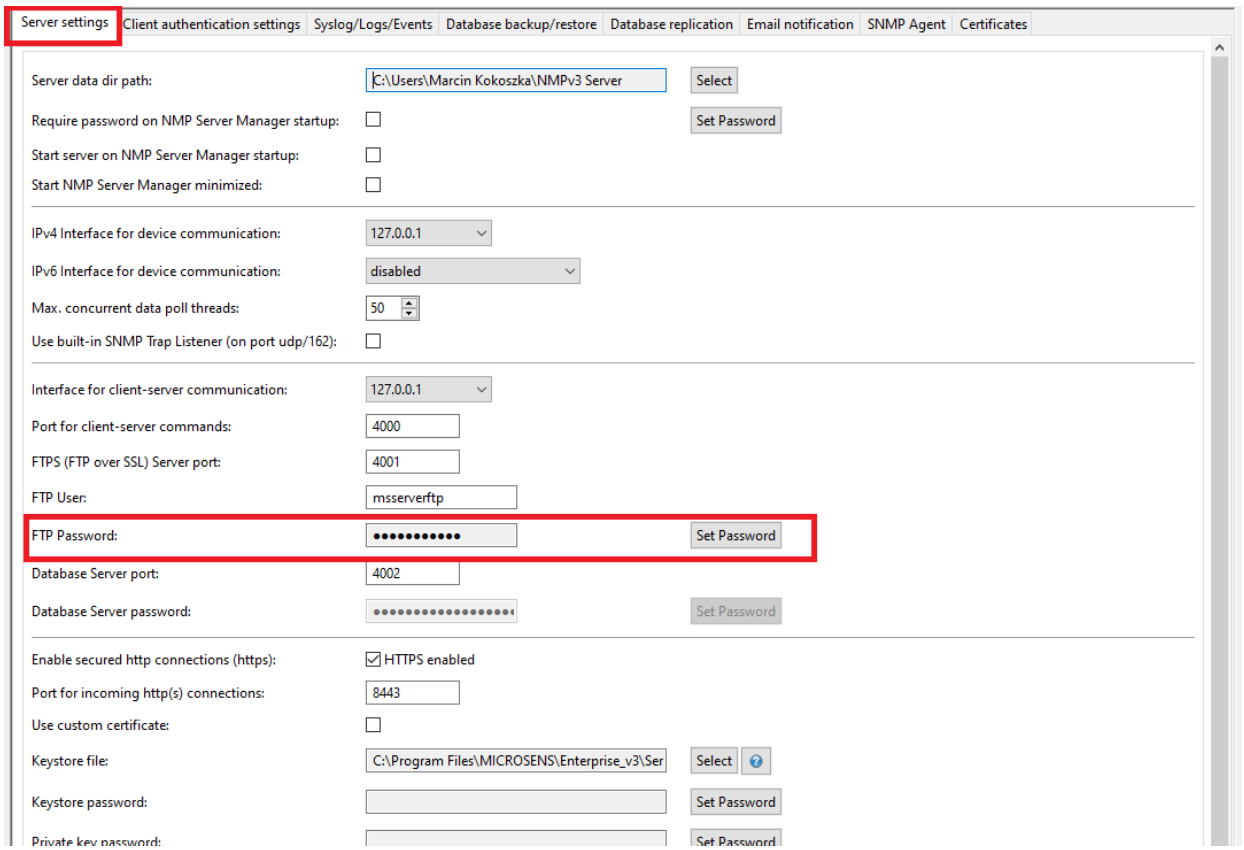
  Never leave the default password as is!



- **Change password for the FTP Server!**

  SBM comes with a default FTP user and a default password. At least, change the FTP user's password.

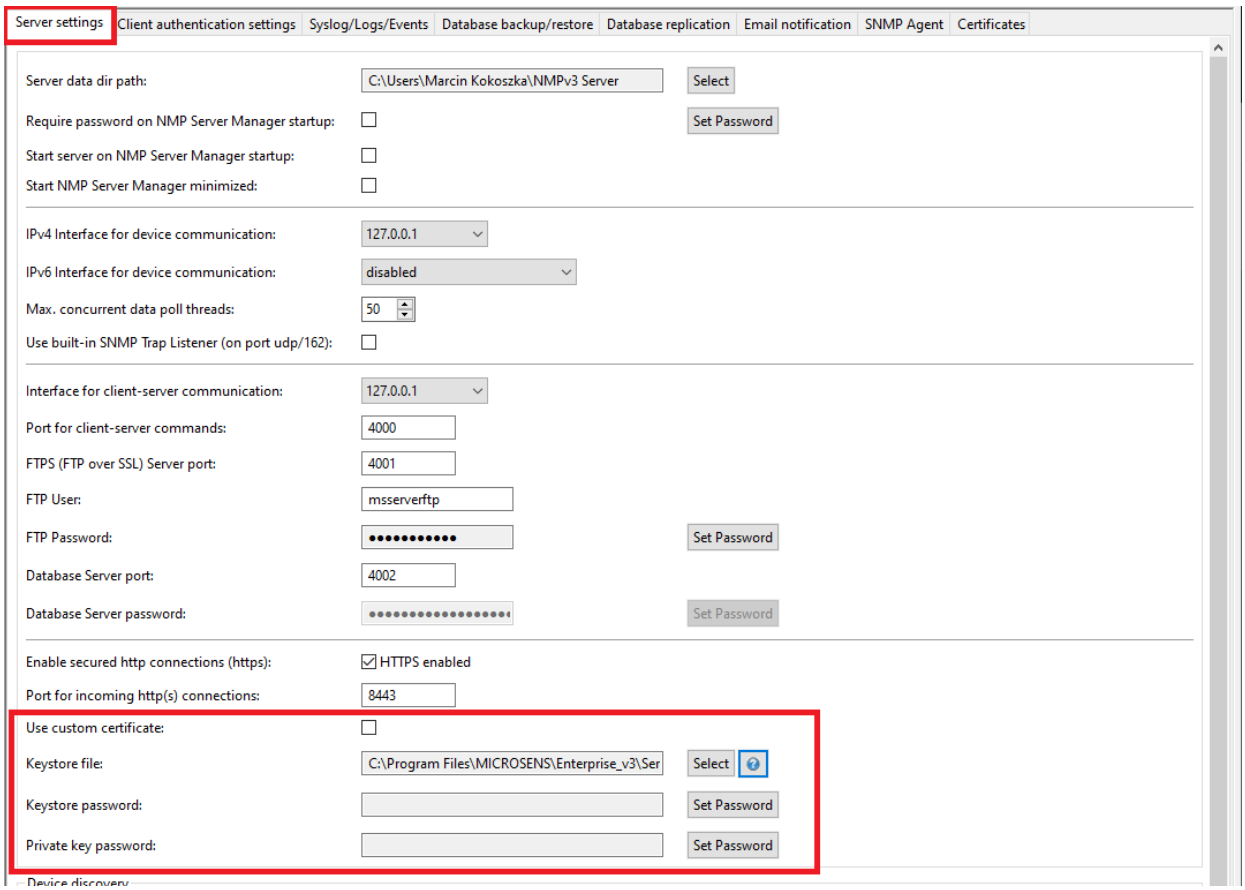
  Never leave the default password as is!



- **Update the SBM Server certificate to avoid Man-in-the-Middle attacks!**

  SBM Server comes with default self-signed certificate for web server. Please update it with valid certiicate in Java KeyStore (JKS) format. A Java KeyStore (JKS) is a repository of security certificates either authorization certificates or public key certificates plus corresponding private keys, used for instance in SSL encryption.

  Detailed help/description how to create JKS certificate for SBM can be found at the Server manager window.



- **Use an API-Gateway software to avoid DDoS attacks**

  This is important especially for the cloud instances!

- **Restrict connections to HTTPS only!**

  SBM web server can be accessed via HTTP or HTTPS. For secure data communication enable HTTPS. This will disable HTTP access to the web server.

- **Make sure that the TLS version is 1.2 or higher is used everywhere!**
- **Make sure that you are using an MQTT broker which allows TLS connections only!**

  SBM comes with MQTT broker functionality. If you plan to use an external MQTT broker, make sure it allows secure TLS connections!

- **Use clean MQTT logs!**

  Ensure that the MQTT logs do not contain any information leaks that would allow attackers to misconfigure SBM or the devices.

- **Make sure that all IoT data are encrypted!**
- **Make sure that every edge device implements at least the basic authentication with user name, password and client ID.**

- Client ID should be its MAC-Address or serial number.
- It is much more secure to use X.509 certificates for the edge device identification.

Chapter 4. Securing Your Network Devices

Please perform the actions below for vulnerability assessment.

- **Change the default passwords of all your switches and edge devices!**

  There are still network devices available containing widely known default user accounts and passwords. At least, change the passwords of existing user accounts.

  Never leave the default passwords as is!

- **Follow the guidelines in the MICROSENS Security Guide to make your MICROSENS switch and SmartDirector as secure as possible!**

  You will find the latest version of the Security Guide in the download area of the MICROSENS web page.

- **Use an identity management system to create certificates for your switches!**

  Secure and stable identity management is a complex work load with high potential for errors and carelessness. An identity management system will support this task.

- **Do not forget to update the trust-store of the SBM instance so that the certificates of the switches are accepted!**

  What's the use of secure network devices if the SBM does not recognise them?

- **Consider the use of VLANs to make your network more secure through the micro-segmentation approach!**

  Micro-segmentation minimises the effect of attacks on the infrastructure, by containing the consequences to the affected segments only.

Chapter 5. User Management

Please perform the actions below to control user access to your SBM instance.

- **For security reasons, just a minimum number of users that are actually required should be created!**

  User management will become increasingly complex and error-prone with every new user account.

- **Adjust the authorisation level for each user!**

  A user should have the minimum authorisation and access level to be able to perform his or her current responsibilities.

- **Create different users for the different roles!**

  Assigning roles to users will help in managing users conveniently.

- **Make sure that a user must change the login password after the very first login!**

  They will not do it on their own, but must be pushed to do so on their first login.

- **Take care of the user's settings, e.g.:**
  - Account locking
  - Session timeouts

Chapter 6. Technic Tree

The SBM technic tree provides the possibility to manage technical services (i.e. devices, sensors, activators) that have not been assigned to a specific building infrastructure element (i.e. rooms or floors).

- Clarify which of the services from your infrastructure have to be assigned to the technic tree.

  It is not possible to use the same entry for both device and technic tree!

- Define the nodes and hierarchy structures based on the end users' needs.
- For usability reasons keep the tree hierarchy as flat as possible (recommendation: max. depth 2-3 levels).

Chapter 7. Data Point Management

7.1. MQTT Topic Scheme

- **Define your MQTT topic scheme first before creating the MQTT data point sheet.**
  - Use a tree diagram or dendrogram to visualise the hierarchical MQTT structure.
  - This diagram will help in the use of wildcards (e.g. + for single level, # for multiple levels) for grouped MQTT topic subscriptions.

7.2. MQTT Data Point Sheet

- **Do not forget to review the following items after importing the MQTT data point sheet:**
  - Data point configuration list
  - Data point assignments
- **Use an IoT simulation software.**

  This will help to publish MQTT data to SBM so you can verify whether the published data points match your expectation through the use of the SBM charts and dashboards.

- **Define alarm rules for the most critical data point values**

  This will force SBM to send an alarm notification in case a data point value exceeds a certain value range.

Chapter 8. Customising

- **Start with the data point design as follows:**
  - Define the data point IDs/names
  - Define MQTT topic names based on your defined topic scheme
  - Assign the correct DataPointClass
- **Make sure the access mode assigned to each data point is correct.**
  - `READONLY` means the data point can only be used for visualisation
  - `READWRITE` means the data point value can be written to implement control functions
- **Make sure the correct context information is assigned to each data point.**
- **Use an SVG which is as simple as possible to visualise the data points in order to avoid visual noise.**

  This will help to get a quick overview of all the data point states.

- **Use room types and assign it to rooms to avoid the workload spent in defining room status cards for each room individually.**

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

Disclaimer

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

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

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

Document ID: DEV-EN-SBM-Best-Practice_v0.3