

NMP / SBM

Troubleshooting Guide & Knowledge Base



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. Introduction	1
2. General	3
2.1. Missing or Unstable Client Server Connection	3
2.1.1. Problem/Issue	3
2.1.2. Affected Application	3
2.1.3. Solution/Workaround	3
2.2. Do Client Components Support Multi Monitors?	4
2.2.1. Problem/Issue	4
2.2.2. Affected Applications	5
2.2.3. Solution/Workaround	5
2.3. Using Virtual Machines	5
2.3.1. Problem/Issue	5
2.3.2. Affected Application	5
2.3.3. Solution/Workaround	5
2.4. Migration from NMP 1.x to NM 2.x	6
2.4.1. Problem/Issue	6
2.4.2. Affected Application	6
2.4.3. Solution/Workaround	6
2.4.3.1. Option 1: Install with automatic migration	6
2.4.3.2. Option 2:	6
2.5. Start Application as 'sudo' on Debian 10	7
2.5.1. Problem/Issue	7
2.5.2. Affected Application	7
2.5.3. Solution/Workaround	7
2.6. Strange Application GUI Behaviour after Upgrade	8
2.6.1. Problem/Issue	8
2.6.2. Affected Application	8
2.6.3. Solution/Workaround	8
2.7. Memory dump of a running application process	9
2.7.1. Problem/Issue	9
2.7.2. Affected Applications	9
2.7.3. Solution/Workaround	9
2.8. Email notification fails	10
2.8.1. Problem/Issue	10
2.8.2. Affected Applications	10
2.8.3. Solution/Workaround	10
2.9. Migration from legacy to latest MICROSENS switches	10
2.9.1. Problem/Issue	10
2.9.2. Affected Application	10

2.9.3. Solution/Workaround	11
3. Licensing	12
3.1. Licensing Errors	12
3.1.1. Problem/Issue	12
3.1.2. Affected Applications	12
3.1.3. Solution/Workaround	12
3.2. Licence key file not working for prior application versions	13
3.2.1. Problem/Issue	13
3.2.2. Affected Applications	13
3.2.3. Solution/Workaround	13
4. Database	14
4.1. Repair server database	14
4.1.1. Problem/Issue	14
4.1.2. Affected Application	14
4.1.3. Solution/Workaround	14
4.2. Storage location of device list	15
4.2.1. Problem/Issue	15
4.2.2. Affected Application	15
4.2.3. Solution/Workaround	15
4.3. Database replication issues	15
4.3.1. Problem/Issue	15
4.3.2. Affected Application	15
4.3.3. Solution/Workaround	16
4.4. Database login not possible	17
4.4.1. Problem/Issue	17
4.4.2. Affected Application	17
4.4.3. Solution/Workaround	17
5. Device discovery and communication	19
5.1. Switch Discovery in General	19
5.1.1. Problem/Issue	19
5.1.2. Affected Application	19
5.1.3. Solution/Workaround	19
5.2. Server Side Tracing for Troubleshooting	20
5.2.1. Problem/Issue	20
5.2.2. Affected Application	20
5.2.3. Solution/Workaround	20
5.3. Presumably Low IP Range Scanner Speed	20
5.3.1. Problem/Issue	20
5.3.2. Affected Application	20
5.3.3. Solution/Workaround	21
5.4. Device is not detected	21

5.4.1. Problem/Issue	21
5.4.2. Affected Application	21
5.4.3. Solution/Workaround	21
5.5. Number of simultaneously polled devices	22
5.5.1. Problem/Issue	22
5.5.2. Affected Application	22
5.5.3. Solution/Workaround	22
5.6. 10G PLR switch not available during polling	22
5.6.1. Problem/Issue	22
5.6.2. Affected Application	23
5.6.3. Solution/Workaround	23
5.7. Devices are discovered on all interfaces, even if a single interface is selected	23
5.7.1. Problem / Symptom:	23
5.7.2. Affected Application	23
5.7.3. Solution/Workaround	23
5.8. SSH, ping, telnet terminal issues	24
5.8.1. Problem/Issue	24
5.8.2. Affected Application	24
5.8.3. Solution/Workaround	24
6. Alarm lists	25
6.1. Handling alarm list entries	25
6.1.1. Problem/Issue	25
6.1.2. Affected Application	25
6.1.3. Solution/Workaround	25
6.2. Client's alarm list is empty after server restart	25
6.2.1. Problem/Issue	25
6.2.2. Affected Application	26
6.2.3. Solution/Workaround	26
6.3. Alarm indicators in device tree vs. alarm list	26
6.3.1. Problem/Issue	26
6.3.2. Affected Application	26
6.3.3. Solution/Workaround	26
7. Managing network ring errors	27
7.1. Managing Industrial Ring Errors	27
7.1.1. Problem/Issue	27
7.1.2. Affected Application	27
7.1.3. Solution/Workaround	27
8. Working with the device list	29
8.1. Managing stacked devices	29
8.1.1. Problem/Issue	29

8.1.2. Affected Application	29
8.1.3. Solution/Workaround	29
8.1.3.1. Incorrect Device List Entries	29
8.1.3.2. Missing Alarm Trap Indicators in the Device List	30
8.2. Find a device in an extensive device list	30
8.2.1. Problem/Issue	30
8.2.2. Affected Application	30
8.2.3. Solution/Workaround	31
8.3. How to find unused switches?	31
8.3.1. Problem/Issue	31
8.3.2. Affected Application	31
8.3.3. Solution/Workaround	31
8.4. Duplicate group names	32
8.4.1. Problem/Issue	32
8.4.2. Affected Application	32
8.4.3. Solution/Workaround	32
8.5. Device type in device summary table explained	32
8.5.1. Problem/Issue	32
8.5.2. Affected Application	33
8.5.3. Solution/Workaround	33
8.6. IPv4 or IPv6 address in the device tree	33
8.6.1. Problem/Issue	33
8.6.2. Solution/Workaround	34
9. Working with VLAN	35
9.1. VLAN settings for groups?	35
9.1.1. Problem/Issue	35
9.1.2. Affected Application	35
9.1.3. Solution/Workaround	35
10. Authentication issues	36
10.1. RADIUS server and local database	36
10.1.1. Problem/Issue	36
10.1.2. Affected Application	36
10.1.3. Solution/Workaround	36
10.1.3.1. NMP 1.x	36
10.1.3.2. NMP 2.x and SBM	36
10.2. Authentication with RADIUS server fails despite valid password	37
10.2.1. Problem/Issue	37
10.2.2. Affected Application	37
10.2.3. Solution/Workaround	37
10.3. Configuration of RADIUS server attributes	37
10.3.1. Problem/Issue	37

10.3.2. Affected Application	37
10.3.3. Solution/Workaround	37
11. Device configuration	39
11.1. FW update via FTP Server does not work	39
11.1.1. Problem/Issue	39
11.1.2. Affected Application	39
11.1.3. Solution/Workaround	39
11.2. Firmware deployment from client to server not working	39
11.2.1. Problem/Issue	39
11.2.2. Affected Application	39
11.2.3. Solution/Workaround	39
11.3. Storage location of configuration backup files	40
11.3.1. Problem/Issue	40
11.3.2. Affected Application	40
11.3.3. Solution/Workaround	40
11.4. Configuration restore/update with G7x switches	40
11.4.1. Problem/Issue	40
11.4.2. Affected Application	40
11.4.3. Solution/Workaround	40
11.5. Password rules for MICROSENS G7x switches	41
11.5.1. Problem/Issue	41
11.5.2. Affected Application	41
11.5.3. Solution/Workaround	41
11.6. RMA Device Configurator ignores configuration file	41
11.6.1. Problem/Issue	41
11.6.2. Affected Application	41
11.6.3. Solution/Workaround	42
11.7. TLS v1.x support	42
11.7.1. Problem/Issue	42
11.7.2. Affected Application	42
11.7.3. Solution/ Workaround	42
12. SNMP	44
12.1. SNMP trap listener on port 162 is not working	44
12.1.1. Problem/Issue	44
12.1.2. Affected Application	44
12.1.3. Solution/Workaround	44
12.2. SNMP engine ID and configuration backups	44
12.2.1. Problem/Issue	44
12.2.2. Affected Application	44
12.2.3. Solution/Workaround	45
13. Working with SmartDirector	46

13.1. Troubleshooting SmartDirector Configuration 46

13.1.1. Problem/Issue 46

13.1.2. Affected Application 46

13.1.3. Solution/Workaround 46

Chapter 1. Introduction

MICROSENS NMP and SBM are comprehensive network management applications for complex network and smart building infrastructures.

Therefore, it is unavoidable that events occasionally do not go as expected.

This troubleshooting guide will assist you in resolving recognized reoccurring issues and problems on your own.

NOTE | Please make sure to follow all recommendations in the MICROSENS Best Practises Guide that is available from the MICROSENS website www.microsens.com/support.

If your specific problem is not listed or resolved in this trouble shooting guide, please contact the technical support team of MICROSENS.

Before contact, please have the following information ready:

Application version

1. Launch the respective MICROSENS application, i.e. NMP Professional, NMP Enterprise (server and client component) or SBM.
2. In the particular menu bar, click on Help > About.
 - The opening popup dialogue shows the application version.

Server and workstation settings

- Operating system and version
- RAM
- Free disk space
- CPU

NOTE | Please make sure, your server and workstation settings meet the system requirements of your application as listed in the "System Requirements" section of your application's user manual.

Debug-Log

IMPORTANT | In case of an exception error (or an application crash) on start-up, it is necessary to get a debug log file.

1. Launch the respective MICROSENS application in debug mode.
 - a. Open a command line interface (**cmd**).
 - b. Change to the local applications directory.
 - c. Search for the application with the suffix **_debug** (e.g. for Microsoft Windows®: **MICROSENS_NMP_debug.exe**).
 - d. Start the application in debug mode with the following command:
 - (for Microsoft Windows®)

`[Application]_debug.exe > [application].[version].[variant].debug.log 2>&1`

- This will open an additional command line interface (`cmd`), where all the logs and errors will be displayed.
 - Simultaneously, the pipe symbol (`>`) will force all output to be stored in the named debug text file.
2. Try to reproduce the error, then close the application via the menu File > Exit.
 3. Change to the directory where the debug file is stored and attach it to an email and send it to the MICROSENS support team.

Chapter 2. General

This chapter describes the general possible issues that could arise when working with NMP or SBM.

2.1. Missing or Unstable Client Server Connection



2.1.1. Problem/Issue

For some reason, the application client is unable to connect to the server component.

2.1.2. Affected Application

- NMP Enterprise
- SBM

2.1.3. Solution/Workaround

1. Start the server manager of the specific MICROSENS application.
2. Click on the button .
3. Wait until the message **Server started** appears in the server manager's status field.
4. Start the application's client.
5. You will find the button  on the bottom left of the login dialogue.

It allows checking whether the connection between client and server is possible.

NOTE

The correct server's IP address and command ports are required to perform the test!

- The following dialogue opens:

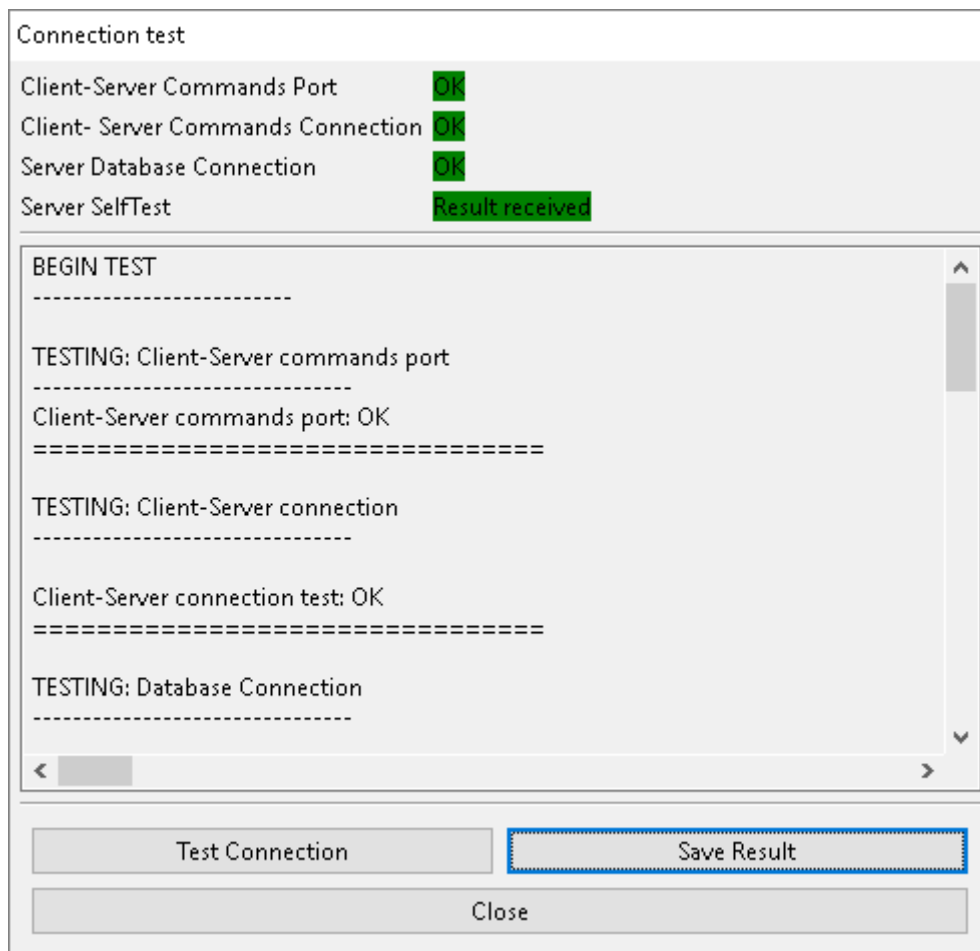


Figure 1. Connection Test

6. Click on the button **Test Connection** to start the connection test
 - The client will automatically check if all necessary services and ports are available on the server.
 - The result will be displayed in the dialogue.
7. Analyse the test result and in the event of fault, perform the corrections.
 - If corrections do not provide the desired results, click on the button **Save Result** to export the data as a text file and attach it to an email and send it to the MICROSENS support team.

2.2. Do Client Components Support Multi Monitors?

2.2.1. Problem/Issue

Since it is possible to detach tabs from the tabbed data panel and place them freely on the monitor screen:

Does the client component's UI support multiple monitors?

2.2.2. Affected Applications

- NMP Professional
- NMP Enterprise
- SBM

2.2.3. Solution/Workaround

Yes, a multiple monitor environment is supported.

Just drag & drop a tab on a second monitor screen.

You may also drag & drop the tab to the client's main window, in case you want to move it back.

2.3. Using Virtual Machines

2.3.1. Problem/Issue

What is the best way to run the application on a virtual machine?

2.3.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

2.3.3. Solution/Workaround

(Tested on Debian 9@VirtualBox and latest Ubuntu@VirtualBox)

- Configure the VM to use **Bridge Network**.

IMPORTANT

NAT (Network Address Translation) will not work because incoming messages from the host machine will not be forwarded.

E.g., device auto discovery works by broadcast messages. If broadcasts between host machine and VM are not forwarded, the application will not receive any discovery packets and therefore cannot find devices by auto discovery.

- Device auto discovery depends on the application host IP configuration. To make it work correctly, it should be set to valid OS interface or to **0.0.0.0** (default interface).
- Additionally, when the NMP is used on VM, its functionality depends on VM configuration (if the broadcasts are forwarded from host machine to guest system).

NOTE | If the application requires a license dongle, the correct USB device has

| to be registered to the virtual machine.

2.4. Migration from NMP 1.x to NM 2.x

2.4.1. Problem/Issue

What is the best way to migrate from NMP 1.x to NMP 2.x?

2.4.2. Affected Application

- NMP Professional 1.x/2.x
- NMP Enterprise 1.x/2.x

2.4.3. Solution/Workaround

2.4.3.1. Option 1: Install with automatic migration

1. Login to the NMP 1.x Server Manager as a user with administrator rights.
2. Stop running NMP 1.x server / NMP service.
3. Exit NMP 1.x Server Manager.
4. Start NMP 2.x installer.
5. Follow the instructions of the installation wizard.
6. Select **migrate = yes**.

2.4.3.2. Option 2:

1. Login to the NMP 1.x Server Manager as a user with administrator rights.
2. Stop running NMP 1.x server / NMP service.
3. Exit NMP 1.x Server Manager.
4. Start NMP 2.x installer.
5. Follow the instructions of the installation wizard.
6. Select **migrate = no**.
7. Close the NMP 2.x installer after installation is done.
8. Change to the NMP 1.x installation folder and copy the folder **database** from NMP 1.x data directory.
9. Change to the NMP 2.x installation directory and delete the folder **database** from NMP 2.x data directory.
10. Paste the copied NMP 1.x database folder into the NMP 2.x data directory.
11. Start NMP 2.x Server Manager.

2.5. Start Application as 'sudo' on Debian 10

2.5.1. Problem/Issue

When application is started with root access rights (**sudo**) under Linux Debian 10.1, an error message occurs (example with NMP Professional):

```
user@workstation: ~/MICROSENS/NMP_Professional/$ sudo ./NMP
[sudo] password for user:
No protocol specified
Unable to init server: Could not connect: Connection refused
NMP: Cannot open display:
No protocol specified
Unable to init server: Could not connect: Connection refused
No protocol specified
Unable to init server: Could not connect: Connection refused
NMP: Cannot open display:
NMP:
An error occured. See the log file
/home/user/MICROSENS/NMP_Professional/configuration/1568815936142.log.
```

2.5.2. Affected Application

- NMP Professional
- NMP Enterprise (client component)
- SBM

2.5.3. Solution/Workaround

This is not an application error! It has to do with the Debian 10 X11 security settings.

1. Open a CLI.
2. Change to the directory **\$HOME** of the user who installed the application.
3. Create a **.bashrc** file:

```
touch .bashrc
```

4. Add the following line to the **.bashrc** file:

```
export XAUTHORITY=~/.XAuthority
```

5. Create an empty file **.XAuthority**:

```
touch .XAuthority
```

6. Run the following commands from the CLI to allow access:

```
xauth generate :0  
xauth info      # just to see whats now in .Xauthority  
xauth list      # just to see list of access permissions
```

Now you could start the application using the following command (example with NMP Professional):

```
user@workstation: ~/MICROSENS/NMP_Professional/$ sudo ./NMP
```

NOTE

For Debian 10 you may try also

```
> xauth generate :0 . trusted
```

2.6. Strange Application GUI Behaviour after Upgrade

2.6.1. Problem/Issue

After updating the application to the latest version, some of the application's GUI elements like text or menu labels show unexpected or unwanted behaviour.

Some tables or menu bar entries are missing.

2.6.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

2.6.3. Solution/Workaround

The GUI layout is saved as is, when closing the application, and reloaded on restart.

If an application upgrade affects those GUI settings (e.g. regarding new features) a restart will try to use the previously saved GUI for a prior application version and may fail to work properly.

1. In the main menu click on Windows > Restart with default layout.
2. Start the application.

Now all GUI elements are fully functional for the new application version.

2.7. Memory dump of a running application process

2.7.1. Problem/Issue

For extensive support issues, it is sometimes necessary to create a memory dump of the running application process.

NOTE | The following steps are valid for **Linux OS**.

2.7.2. Affected Applications

- NMP Professional
- NMP Enterprise
- SBM

2.7.3. Solution/Workaround

1. Start the application as user with administrator access rights.
2. Open a CLI.
3. Determine the process ID of the running application with the command `ps -ef | grep java`:

```
user@workstation: ~/MICROSENS/NMP2.Server$ ps -ef | grep java
develop+ 32168 32169 7 10:27 pts/2    00:00:50 ./jre/bin/java -Xms128m
-XX:MinHeapFreeRatio=20 -
XX:MaxHeapFreeRatio=30 -XX:+UseSerialGC -XX:MaxRAMPercentage=80 -jar
NMPServer.jar com.RunNmpServer
develop+ 52270 38653 0 10:39 pts/3    00:00:00 grep --color=auto java
```

4. Get the `<process ID>` from the command output (in the example above: `32168`).
5. Force a memory dump with the command `kill -3 <process ID>`.

NOTE

This command forces a memory dump and normally kills the respective process.

As the application server process is a JAVA process, as an exception it is not terminated and is still up and running after executing the command!

Every time a command `kill -3` is executed, a new memory dump file (i.e. `javacore` file) will be created.

- The memory dump file (e.g. `javacore.20220530.103505.38633.001.txt`) is stored to the current working folder.

6. Change to the directory where the memory dump file is stored and attach it to an email and send it to the MICROSENS support team.

2.8. Email notification fails

2.8.1. Problem/Issue

Email notification is enabled and configured but sending an email does not work. (e.g. click on button does not send any email).

2.8.2. Affected Applications

- NMP Professional
- NMP Enterprise
- SBM

2.8.3. Solution/Workaround

Please check the following issues:

- Assigned SMTP server should be working (e.g. should be reachable via web browser).
- SMTP server should be reachable via the same (sub-)network the application is communicating with.
- The SMTP hostname can be resolved via DNS.
- The assigned SMTP server address is correct.
- SMTP login credentials (i.e. username, password) are correct.
- Assigned encryption method (SSL, TLS) corresponds to server settings.
- Corporate firewall settings do not block the port for outgoing SMTP connections.

2.9. Migration from legacy to latest MICROSENS switches

2.9.1. Problem/Issue

What to consider when migrating from MICROSENS legacy switches (G3, G4, G5) to up-to-date switches (G6 and later)?

2.9.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

2.9.3. Solution/Workaround

NOTE | The scenario assumes that the legacy switches are already discovered successfully and a working part of the NMP devices list.

To migrate one or more legacy switches, proceed as follows:

1. Physically, replace the legacy switch with the new hardware.
2. Make sure the IP address of the new hardware matches the IP address of the previous switch.
3. In the application's device tree list right-click the device entry and open menu:[Communication Parameters].
 - Do not make any changes in the opening dialogue!
4. Close the dialogue.
 - This will trigger a new polling of the device.
5. Additionally, trigger polling of the device via context menu or main menu toolbar to ensure the device status will be refreshed.

The device tree list should show this switch as the replaced MICROSENS switch.

Chapter 3. Licensing

This chapter describes the licensing issues that could arise when working with NMP or SBM.

3.1. Licensing Errors

3.1.1. Problem/Issue

Application does not start but gives a error message regarding software class:

Could not determine software class (NMP/SBM). Check your installation!

3.1.2. Affected Applications

- NMP Professional
- NMP Enterprise (client component)
- SBM (client component)

3.1.3. Solution/Workaround

This error message is mainly based on licensing issues.

To solve the problem proceed as follows:

1. Please make sure that
 - the server is started (NMP Enterprise and SBM only)
 - the current working directory is set to the same folder where the application is located
2. Check whether the correct license file is installed (NMP Professional) or uploaded to the server (NMP Enterprise and SBM):
 - **NMP Professional**: Open Settings > Licence Info
 - **NMP Enterprise / SBM (server component)**: Open Help > Licence Information
3. Check which **LIC** files are located in the directory **\$USER_HOME/xxx_SERVER/licenses** (e.g. for Windows®: **C:\Users\admin\NMP Server\licenses**)
4. Check for file **product.ini** (hidden file!) under (for Windows ®) **C:\Program Files\MICROSENS\SBM\Server**.
 - Check for the following file entries as shown in the sample below:

```
[product]
version=v2.0.0_RC20
variant=enterprise
```

```
component=server  
class=SBM
```

3.2. Licence key file not working for prior application versions

3.2.1. Problem/Issue

As of v2.3, when installing a new license key file for a current application version, the application shows an error message, that the new license is not accepted/valid.

3.2.2. Affected Applications

- NMP Professional (v2.3 and below)
- NMP Enterprise (v2.3 and below)
- SBM (v2.3 and below)

3.2.3. Solution/Workaround

License key files created for applications (as of version 2.4) are based on a new encryption algorithm which is more secure.

So older versions of applications are not able to read it anymore.

We strongly recommend to update the application to the latest version!

Chapter 4. Database

This chapter describes the database issues that could arise when working with NMP or SBM.

4.1. Repair server database

4.1.1. Problem/Issue

Configuration backups stopped working.

4.1.2. Affected Application

- NMP Professional (prior version 2.6.3)
- NMP Enterprise (prior version 2.6.3)

4.1.3. Solution/Workaround

Occasionally, if the NMP server process is terminated or suspended while a Windows shutdown is in progress, the server's database content may become inconsistent.

In this case it is recommended to check and repair the database:

1. Launch the NMP server manager, **but do not start the server**.
2. In the main menu open Tools > Database check.
 - The NMP server manager will check the database and will repair it if necessary.
 - At the end of the check the NMP server manager will show a dialogue.

No fix necessary

In case of an error-free database the following message appears:

```
Database Check
<5> table(s) checked. <5> check passed. 0 table(s) fixed.
```

Database problem fixed

In case the server manager fixed a database problem, the following message appears:

```
Database Check
<5> table(s) checked. <4> check passed. 1 table(s) fixed.
```

Missing database connection

In case the server manager cannot connect to the database, the following message appears:

Database Check
<0> table(s) checked. <0> check passed. 0 table(s) fixed.

NOTE | This happens if another process is already connected to the database.

The Database check tool can be started multiple times.

4.2. Storage location of device list

4.2.1. Problem/Issue

What is the storage location of the device list?

Is it possible to start the application with an empty device list **or** database, but without losing the device data?

4.2.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

4.2.3. Solution/Workaround

Devices managed by the application are stored in two locations:

- In the `nmpd1` file
- In the NMP database

NOTE | Additionally, the file which is saved at the NMP Server data directory is also stored in the database.

It can be useful to remove the database and start from scratch. On launch, the application tries to load the device list from the database. If no database is found, it loads the device list from the `nmpd1` file.

4.3. Database replication issues

4.3.1. Problem/Issue

The database replication process does not work correctly.

4.3.2. Affected Application

- NMP Enterprise
- SBM

4.3.3. Solution/Workaround

Perform the following steps:

1. Stop both master and slave server processes.
2. Make a copy of both master and slave server databases.

IMPORTANT | Make sure IP addresses of master or slave server did not change in the meantime!

3. Delete the database on slave server.
4. Restart slave server.
 - Slave server will wait for master server after restart.
5. Start master server.
 - Master server will start communicating with slave server.
 - Slave server will notify master server that its own copy of database does not exist
 - Master server will send a copy of its current database to slave server

NOTE | Depending on database size, this could take some time.

- Master and slave server will initialize the replication process from scratch and both master and slave server will use the master database as main/latest database.

If the database replication issues remain, use the following debug option:

1. Stop both master and slave server processes.
2. Exit both master and slave server managers.
3. Start the server managers in debug mode with the following command:

```
~/master: [Application]_debug.exe >  
[application].[version].[variant].master.debug.log 2>&1  
~/slave: [Application]_debug.exe >  
[application].[version].[variant].slave.debug.log 2>&1
```

- This will open additional command line interfaces (**cmd**), where all the logs and errors will be displayed.
 - Simultaneously, the pipe symbol (**>**) will force all output to be stored in the named debug text file.
4. Try to reproduce the error, then close the application via the menu File > Exit.
 5. Change to the directory where the debug file is stored and attach it to an email and send it to the MICROSENS support team.

4.4. Database login not possible

4.4.1. Problem/Issue

The application's server manager does not start the database server.

The database check (Tools > Database Check) shows all counters set to 0.

4.4.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

4.4.3. Solution/Workaround

The main reasons for database authentication issues are wrong credentials or database inconsistencies.

1. Make sure to use valid database credentials with the application's server manager.
 - a. Change to tab menu:[Server Settings]
 - b. In the section menu:[Client Server Communication] make sure to assign the correct database server port and password.
2. Exit the application's server manager.
3. Restart in debug mode with the following command:
 - (for Microsoft Windows®)

```
[Application]_debug.exe > [application].[version].[variant].debug.log 2>&1
```

- This will open an additional command line interface (cmd), where all the logs and errors will be displayed.
- Simultaneously, the pipe symbol (>) will force all output to be stored in the named debug text file. This is optional for later support steps.
- If the command line shows an exception error due to failed authentication, this is the evidence that login into the database is not possible.

The application's database folder named **database** is located in the application's **data** directory and contains at least

- a folder named **nmp_server_db**
- a file named **db.properties**

IMPORTANT

Both file and folder belong together! If a database is copied manually both parts have to be copied!

It is not allowed to mix file and folders from different databases!

Follow these steps to get this fixed:

IMPORTANT

You have to use the database's password that was used when the database was created!

1. Start the application's server manager.
2. Assign a new data folder to create a new empty database.
 - a. In the main menu open menu:[General Settings].
 - b. Configure a new server data directory path.
 - c. In the section menu:[Client Server Communication] enter the database password.
3. Start the server process.
 - The server manager creates a **database** folder and a **db.properties** file in the previously configured server data directory.
4. Stop the server process.
5. Copy the previously created **db.properties** file to the original **database** folder.
6. Configure the data folder to the original server data directory.
7. Start the server process.
 - The database server should now be able to connect to the database.

Chapter 5. Device discovery and communication

This chapter describes the general device discovery and communication issues that could arise when working with NMP or SBM.

5.1. Switch Discovery in General

5.1.1. Problem/Issue

What is the simplest way to discover a switch in the network?

5.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.1.3. Solution/Workaround

NMP Professional

1. Launch the application.
2. Change to the menu menu:[Discovery]
3. Select one of the following menu entries:
 - menu:[Device Auto Discovery]
 - menu:[Device IP-Range scan]
 - menu:[Device SNMP-based Auto Discovery (SNMP v1/v2c)]
 - menu:[MSP 1000 platform IP discovery]
4. Follow the instructions of the specific entry.

Application's client

1. Launch the application's client.
2. Change to the menu:[Window].
3. Select the menu entry SelectPerspective > Network Administration.
4. Unlock the device list.
5. Select one of the following menu entries:
 - menu:[Device Auto Discovery]
 - menu:[Device IP-Range scan]
 - menu:[Device SNMP-based Auto Discovery (SNMP v1/v2c)]
 - menu:[MSP 1000 platform IP discovery]
6. Follow the instructions of the specific entry.

7. After successfully discovering and adding all available devices to the device list, lock the device list.

5.2. Server Side Tracing for Troubleshooting

5.2.1. Problem/Issue

- Connected devices are never listed as scanned/discovered devices in the client's device list.
- Some devices seem to never be polled by the client.

5.2.2. Affected Application

- NMP Enterprise
- SBM

5.2.3. Solution/Workaround

1. Start the application's server manager.
2. In the tabbed server configuration panel change to the tab menu:[Sys-log/Logs/Events]
3. Scroll down to the section menu:[Logging].
4. If you are going to send the log files to the MICROSENS support team, select **DEBUG** from menu:[Device Poll] and menu:[Device Discovery] from the respective drop-down list.

NOTE | It is not necessary to restart the server. Logging starts as soon as the option is enabled.

The log files are located in the application server's data directory (sub-folder **LOG**) under the administrator's home directory.

The file is named **Application_log.log**.

5.3. Presumably Low IP Range Scanner Speed

5.3.1. Problem/Issue

The IP range scanner takes a long time to detect a large number of devices. (e.g. approx. 45-50 minutes for 8000 devices).

5.3.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.3.3. Solution/Workaround

The time period for completely detecting available devices by their IP addresses depends on several aspects:

- Available network bandwidth and actual network load
- Specific response time of the available switches (G3, G4, G5, G6)
- Performance of the workstation on which the application is running

NOTE

Please make sure, your server and workstation settings meet the system requirements of your application according to the "System Requirements" section of your application's user manual.

The following data may serve as a rough guidance for IP scanner performance:

- 300 ms / device * 8000 Devices: approx. 40 minutes
- 200 ms / device * 8000 Devices: approx. 26 minutes
- 100 ms / device * 8000 Devices: approx. 14 minutes

5.4. Device is not detected

5.4.1. Problem/Issue

A device is not discovered by the application.

5.4.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.4.3. Solution/Workaround

- Device might be not supported by the application.

For more information about supported devices please refer to the application's user manual.

- Is the device switched on?
 - Is the power LED on?
 - Is it connected to a properly working and sufficient power supply?
 - Does the device have a separate power switch and is it switched on?
- Is the device plugged to the network?
 - Does the **ping** command receive an answer from the device?
 - Is the network cable generally connected to the network (i.e. edge device)?

- Is the network cable and its plug intact (e.g. no bends, loose contact etc.)
- Is the network cable connected to the correct port of the device?
- Is the device configured for and connected to the correct sub-network (i.e. the same sub-network the application is communicating with)?

If all of the above-mentioned steps fail, enable server-side tracing of device discovery and send the log file to the MICROSENS support team.

5.5. Number of simultaneously polled devices

5.5.1. Problem/Issue

How much devices can be polled simultaneously?

5.5.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.5.3. Solution/Workaround

The application is able to poll up to 200 devices at once. To avoid data loss with slower PCs, highly loaded networks or slow network connections (e.g. slow VPN), reducing the number of concurrent poll threads is highly recommended.

NMP Professional

1. In the main menu open Settings > NMP Settings.
2. Scroll down to parameter menu:[Max. concurrent data poll threads].
3. Enter a value less than 200.

NMP Enterprise / SBM (server component)

1. In the main window change to the tab menu:[Server settings].
2. Scroll down to section menu:[Device Communication].
3. Enter a value of less than 200.

Additionally, a cyclic device data refreshing functionality is also implemented. This functionality can be configured for each device or for all devices. For more information please refer to communication parameters option from the device tree context menu.

5.6. 10G PLR switch not available during polling

5.6.1. Problem/Issue

10G PLR devices are unavailable when polling a group of devices.

5.6.2. Affected Application

- NMP Professional
- NMP Enterprise

5.6.3. Solution/Workaround

There may be two different reasons for the unavailability of 10G PLR devices:

Device's response time exceeds time limit due to device issues or network performance problems

NMP loads only a very basic set of data, nevertheless this device responds very slowly. If devices become unavailable, it may help to change the communication parameters as follows:

- Set the connection timeout to the maximum value.
- Set the maximum retries to the maximum value.

Non-unique SNMPv3 Engine ID in the 10G PLR devices within your administrative domain

It may be that, the same SNMP engine ID is configured on multiple devices. By default, the engine ID is unique and derived from the MAC address of the device.

- Use the CLI command `snmp-server engineID local default` on the affected 10G PLR devices to set the engine ID to its default value.

IMPORTANT

This command additionally erases the SNMPv3 database. SNMP users must be configured again.

5.7. Devices are discovered on all interfaces, even if a single interface is selected

5.7.1. Problem / Symptom:

Application server discovers devices on all available network interfaces, even if only one specific interface is selected.

5.7.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.7.3. Solution/Workaround

This was an issue in an earlier version of the application caused by a request to send broadcast discovery messages and listen on all interfaces.

Otherwise, it's possible that a misconfigured or improper interface would prevent the

application's client from displaying any results.

This behaviour has been fixed.

5.8. SSH, ping, telnet terminal issues

5.8.1. Problem/Issue

When selecting a device in the device list and starting a **ping**, **ssh** or a **telnet** session via the device's context menu, the terminal opens but is not operational.

5.8.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

5.8.3. Solution/Workaround

The main reason for the device not responding to terminal communication (and obviously any other communication) is that it is generally not accessible via the network.

- Please perform all steps described in section **Device is not detected** to make sure the device is accessible via network.
- Make sure **ssh** and **telnet** access are enabled in the device.
- Make sure to use valid credentials (username, password) for **ssh** and **telnet** access.

If **ping**, **ssh** or **telnet** are generally working via separate OS CLI commands but not via application, contact the MICROSENS support team.

Chapter 6. Alarm lists

This chapter describes the general issues with alarm lists that could arise when working with NMP or SBM.

6.1. Handling alarm list entries

6.1.1. Problem/Issue

What are the rules to add or remove entries in the alarm list?

How to handle entries with severity equal or higher than **WARNING**?

6.1.2. Affected Application

- NMP Professional (as of version 2.1)
- NMP Enterprise (as of version 2.1)
- SBM (as of version 2.1)

6.1.3. Solution/Workaround

- If the application receives an event with the severity equal or higher than **WARNING** and is marked as **negative**, an entry in the alarm list is created.

NOTE	Events with WARNING might indicate a problem that might appear in the future. So take WARNINGS as an indicator for upcoming alarms.
-------------	---

- If the application receives an event with the severity equal or higher than **WARNING** and is marked as **positive**, the corresponding entry will be deleted from the alarm list.
- If an event is received where a corresponding alarm is already created, the counter in the alarm list is incremented.

If you see e.g. an entry "port disabled" in the alarm list with the severity **WARNING** and you know this is done on intention, you can delete this entry from the alarm list manually as follows:

1. Select the entry
2. Open the entry's context menu with a right-click
3. Select the context menu item menu:[Delete] to delete the entry.

6.2. Client's alarm list is empty after server restart

6.2.1. Problem/Issue

The alarm list of application client shows a couple of alarms but after restarting the application server the client's alarm list is empty.

6.2.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

6.2.3. Solution/Workaround

Alarm messages are not persistently stored on the workstation's or server's hard disk but only handled in the volatile memory.

Therefore, if the application server is restarted, the active alarm list is always empty as its entries depend on receiving SNMP traps from the devices.

Devices do not resend traps on server restart so prior alarms are not added to the alarm list.

6.3. Alarm indicators in device tree vs. alarm list

6.3.1. Problem/Issue

A device has reported an event, which is displayed as an entry in the alarm list.

The same device does not show any alarm indicators for this alarm in the device tree.

6.3.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

6.3.3. Solution/Workaround

The application works as expected:

The icon indicator in the device tree is meant to show basic communication errors only (e.g. device not responding, ring error, authorisation failed etc.).

There is even a general indicator for devices with acknowledged alarms, but this indicator is not mapped to a specific alarm.

There is no indicator for alarms in the device tree.

NOTE

For more information about device icons please refer to the application's user manual.

Chapter 7. Managing network ring errors

This chapter describes the general issues with network rings that could arise when working with NMP or SBM.

7.1. Managing Industrial Ring Errors

7.1.1. Problem/Issue

How to detect a ring error when using industrial switches?

7.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

7.1.3. Solution/Workaround

In the device tree list it is possible to group ring devices.

In most cases ring errors are caused by fibre link failures between two ring switches. When ring errors happen in the network, the application identifies the devices responsible for these errors by their entries highlighted in red text and a special **WARNING** icon on the left hand pane.

The following image shows the ring's master switch (with IP address **10.100.90.141** and yellow background) as "Ring no 1". There is also a ring error caused by the device with the IP address **10.100.90.144**.

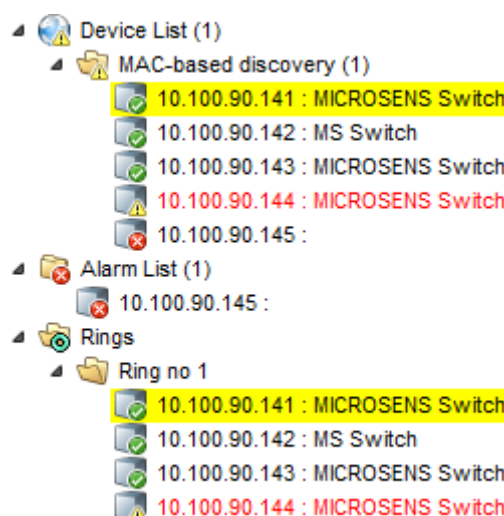


Figure 2. Device Tree List View - Industrial Ring Errors

This should lead to the check of the ring configuration of the responsible device and whether it's connected correctly to the network.

NOTE

Sometimes it is necessary to poll ring devices manually after repairing the ring error to get the proper status of the ring devices in the application.

Chapter 8. Working with the device list

This chapter describes the general device list issues that could arise when working with NMP or SBM.

8.1. Managing stacked devices

8.1.1. Problem/Issue

- How are stacked devices (i.e. MICROSENS MSP1000) created in the device tree list?
- The device tree list acts in an unexpected manner.
- The sub-tree icon of a contained module is missing.
- Active alarms are not shown in the device list.

8.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

8.1.3. Solution/Workaround

8.1.3.1. Incorrect Device List Entries

Stacked devices are organised in trees and sub-trees. A sub-tree contains all modules of the specific device in the form of nodes.

Even when the tree node is collapsed, if one of the sub-tree nodes is marked as **RED** (error state), this state will propagate to the matching parent tree node to signal a module error.

The current color code of the node (i.e. the device's module) has one of the following meanings:

- **Green**: OK
- **Yellow**: TEST
- **Red**: ERROR

The tree for a stacked device is created by the messages sent by every (NM3) module. Each message contains the module's **NODE ID**, **UNIT ID** and **MODULE ID**. These unique values identify the specific module.

The application does not check whether a sent message is valid or not. As soon as it receives a module message it creates the corresponding sub-tree. Sometimes a module can send a message containing wrong or missing **NODE ID** or **UNIT ID**.

NOTE | This problem is not yet solved but currently subject to close investigation.

This unwanted behaviour has two essential implications:

- Incorrect device list entry
- Missing device list icon

For stacked devices the application offers no option to remove or add a single sub-tree node. Only the module itself is responsible for adding or removing its node IDs, by sending the message. The application is only triggered to action by these incoming module messages.

To this day, the only way to repair incorrect entries or entries without icons from the list, is as follows:

1. Unlock the device list.
2. Delete the affected device node from the list.
3. Lock the device list in order to sync it with the server.
4. Unlock device list and add the previously removed device to the list.
5. Lock the device list in order to sync it with the server.

8.1.3.2. Missing Alarm Trap Indicators in the Device List

Modules of stacked devices are responsible for managing and providing alarm messages.

The application receives both the modules' status message for managing the device tree list and the modules' trap message with alarm cause and severity for managing the alarm list.

To this today, the application handles both message types separately and does not acquire an alarm state for a device list node.

This issue may be addressed in an upcoming version of the application.

8.2. Find a device in an extensive device list

8.2.1. Problem/Issue

How can I search for a device in an extensive (e.g. several hundred or even thousand devices) device list?

8.2.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

8.2.3. Solution/Workaround

On top of the device list tree, enter a name or IP address into the search field.

NOTE | For application versions prior to 2.2.0 only searching for IP addresses is allowed.

8.3. How to find unused switches?

8.3.1. Problem/Issue

How can I find unused switches in my network?

8.3.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

8.3.3. Solution/Workaround

The application provides a function to search for unused devices.

The following algorithm is used to detect unused switches:

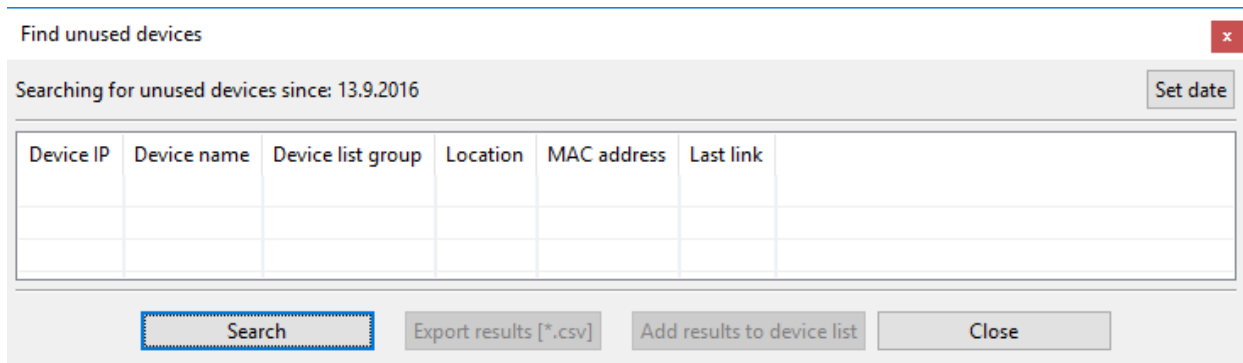
- Every time a device is polled the application creates a port list and checks if links are up.
- If a link is up, the timestamp is saved.

When the search is started, the application checks if any port of the device were up (link up) within the assigned time range. If this is the case, it means that the device was used (i.e. something was connected to it). Otherwise, it means the device was not used (i.e. nothing was connected to it, no link up on ports).

Therefore, the term "unused" refers to a device where no connections were made to any ports other than the uplink port within the allotted time period.

The steps to find those devices are as follows:

1. Select a group of nodes or the root node in the device list.
2. Open the context menu with a right-click.
3. Select the menu item menu:[Find unused devices] to open the search dialog.



Device IP	Device name	Device list group	Location	MAC address	Last link

Figure 3. Find Unused Devices

4. Hit **Set date** and set the time range in which to search for unused devices.
5. Hit **Search** to start the search
 - The dialogue shows a tabular overview of unused devices in the assigned time range.
6. Hit **Add results to device list** to create a new device list node named menu:[Unused devices] containing the devices in the search result.

8.4. Duplicate group names

8.4.1. Problem/Issue

Is it allowed to create multiple device group names with the same name?

8.4.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

8.4.3. Solution/Workaround

Apart from the fact, that we highly recommend using unique group names for better allocation of devices and infrastructure, it is allowed to use duplicate group names.

The application uses internal IDs to manage groups.

8.5. Device type in device summary table explained

8.5.1. Problem/Issue

When selecting a group in the device tree list, the right hand tabbed data panel shows information of all the contained devices.

What is the meaning of the entry in the column "device type" in the tabular overview of a particular device?

8.5.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

8.5.3. Solution/Workaround

The table below contains a list of possible device types that can be managed by the application:

Device Type	Comment
OEM	SNMP Based OEM device (with very basic support)
AccessPlatform	
CwdmSystem	
MediaConverter	
MSP3000	MSP300 Device
MSP1000	MSP1000 Devivce
RAMAN	
IPMux	
GbTdmMux	
SmartIOModule	Smart IO Controller
FM100	
ModbusController	It is a Modbus controller
MS-G6	Any kind of MICROSENS G6 switch
MS-GL	Any kind of legacy switch generations like G5 or older
	NOTE No mechanism exists to check if it is a G5 or G4 model
MS-Ox	It is an OEM switch built by MICROSENS
	x is a number between 1 to 8

8.6. IPv4 or IPv6 address in the device tree

8.6.1. Problem/Issue

How to manage different IP address protocols (i.e. IPv4 or IPv6) in the device list tree?

8.6.2. Solution/Workaround

The device is added manually, therefore, it depends on the IPv4 or IPv6 address entered by the user.

Chapter 9. Working with VLAN

This chapter describes the general VLAN issues that could arise when working with NMP or SBM.

9.1. VLAN settings for groups?

9.1.1. Problem/Issue

How can I set the VLAN settings for a group of devices?

9.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

9.1.3. Solution/Workaround

Change the VLAN settings for a group of devices as follows:

1. In the device tree list, select the respective group.
2. In the main menu open Tools > Switch VLAN Add/Remove/Change Tool.

This tool allows to add, remove or change the VLAN settings of all switches in the selected group.

3. Check the desired option (add, remove or change), enter the VLAN settings and click on **Apply new configuration**.

Depending on the selected operation type, a VLAN with the provided settings will be added, removed or changed on all devices in the selected group. Log messages are displayed at the bottom of the dialogue. It is possible to display all messages or only errors, after which the messages can be saved to a log file.

Chapter 10. Authentication issues

This chapter describes the general authentication issues that could arise when working with NMP or SBM.

10.1. RADIUS server and local database

10.1.1. Problem/Issue

User authentication is possible via three options:

- Local database only
- Local database and RADIUS server
- RADIUS server only

The operations "Local database only" and "RADIUS server only" should be clear.

How is user authentication organised when both local database as well as RADIUS server are enabled?

10.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

10.1.3. Solution/Workaround

The functioning differs from application version.

10.1.3.1. NMP 1.x

The local NMP database is used only to create a copy of user accounts from the RADIUS server. If the RADIUS server is not available, the user is able to restart the server with local authentication only and use it with all accounts.

10.1.3.2. NMP 2.x and SBM

The application initially tries to authenticate a user via the determined RADIUS server. If the RADIUS server is not available, the application will try to use its local database to authenticate the user.

If a user's credentials are stored on both the RADIUS server and the local database, only the credentials stored in the RADIUS server are considered.

On failing login attempts via RADIUS, ensure that the credentials saved in the RADIUS server are valid. Transfer the currently valid credentials from the local database to the RADIUS server to overwrite the user's outdated RADIUS credentials.

10.2. Authentication with RADIUS server fails despite valid password

10.2.1. Problem/Issue

Despite using a correct and valid password, authentication with RADIUS fails.

10.2.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

10.2.3. Solution/Workaround

This problem is caused by a limitation in how RADIUS 1.0 handles passwords when the PAP authentication protocol is enabled:

With RADIUS 1.0 and PAP enabled a **password length of max. 16 characters** is allowed.

The application allows RADIUS passwords longer than 16 characters. During authentication with the RADIUS 1.0 server, the application transmits the longer password to the server correctly, but with PAP enabled the RADIUS server cannot decode passwords longer than 16 characters.

Apart from the fact, that we highly recommend using long passwords and RADIUS 2.0 server, use a password with maximum 16 characters, if there is no other option.

Alternatively switch to CHAP authentication, if possible.

10.3. Configuration of RADIUS server attributes

10.3.1. Problem/Issue

How should the RADIUS server configuration look like, especially in regards to RADIUS attributes?

10.3.2. Affected Application

- NMP Enterprise
- SBM

10.3.3. Solution/Workaround

The following RADIUS attributes are important for the application server:

Attribute	Type	Comment
6	Service-Type	<p>Value for e.g. "sysadmin" user</p> <p>It is used by application's server to check the user rights</p> <p>(Callback-Administrative = 11 is for sysadmin user account type).</p>
18	Reply-Message	<p>Value is a string which must be in the following format:</p> <p><code>UserData:UserName UserLastname UserEmail</code></p> <p>where <code>UserName</code>, <code>UserLastname</code> and <code>UserEmail</code> must be replaced with real user data.</p> <p>It is used by the application's server to get additional information about the user, such as name, last name and email address which can be used for logging or for sending notifications.</p>

NOTE

You have to configure/add the two attributes as listed above in the RADIUS server because the application server expects both values at the RADIUS reply message in order to work properly.

Chapter 11. Device configuration

This chapter describes the general device configuration issues that could arise when working with NMP or SBM.

11.1. FW update via FTP Server does not work

11.1.1. Problem/Issue

Firmware update does not work when using an FTP server.

11.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

11.1.3. Solution/Workaround

Please check for the following:

- FTP server is active and connected to the network.
- FTP server's IP address is ping-able via CLI.
- If a firewall is used, please check whether the FTP server can be reached through the firewall using FTP protocol (e.g. using an FTP client).
- Check for valid FTP settings (i.e. IP address, credentials) in the application.

11.2. Firmware deployment from client to server not working

11.2.1. Problem/Issue

Uploading a firmware file from application's client to application's server component for deployment results in an error message "Firmware upload is failed".

11.2.2. Affected Application

- NMP Enterprise
- SBM

11.2.3. Solution/Workaround

The main reason for failing firmware upload is an interface misconfiguration between client and server component.

- Make sure, the client server communication happens via the correct interface.

NOTE | In the server settings, the interface for client communication should match the client's IP address, not `localhost` or `127.0.0.1`.

11.3. Storage location of configuration backup files

11.3.1. Problem/Issue

Where are the configuration backup files stored?

11.3.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

11.3.3. Solution/Workaround

- **NMP Professional:** The configuration backup files are stored in the local file system.
- **NMP Enterprise/SBM:** The configuration backup files are stored in the applications database.

11.4. Configuration restore/update with G7x switches

11.4.1. Problem/Issue

How does the application handle configuration backup, restore and update procedures with MICROSENS G7x switches?

11.4.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

11.4.3. Solution/Workaround

G7x switches do not accept configuration files which are incomplete! A configuration restore file must always contain all the parameters.

Therefore, the application replaces the IP settings from the configuration backup file with the current IP settings of the destination switch.

This is valid for both the IPv4 as well as the IPv6 settings

NOTE | The G7x switch configuration works as follows (as of FW Version 1.x.y)

- YAML configuration file import/export:
 - partial config is not supported
 - requires a reboot after import
- CLI script file import/export:
 - supports all CLI commands so that you can do the partial set up
 - effective immediately
- **G7x devices can not produce a full config in form of a CLI script!**

11.5. Password rules for MICROSENS G7x switches

11.5.1. Problem/Issue

Is there a set length or minimum character requirement for passwords used with MICROSENS G7x switches?

11.5.2. Affected Application

- NMP Professional (Version ≥ 2.6)
- NMP Enterprise (Version ≥ 2.6)
- SBM (Version ≥ 2.6)

11.5.3. Solution/Workaround

Please note the following rules:

- At least 8 characters (the more characters, the better)
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Include at least one special character (e.g. ! @ # ?)

11.6. RMA Device Configurator ignores configuration file

11.6.1. Problem/Issue

RMA device configurator can not find the configuration file of a MICROSENS G6 switch, even if the correct configuration folder is specified.

The error message reads that the configuration file could not be found.

11.6.2. Affected Application

- NMP Professional
- NMP Enterprise

- SBM

11.6.3. Solution/Workaround

The RMA tool goes back to early versions of NMP and therefore is a little bit outdated.

Since there was no further development in the meantime, the RMA tool does not support G6 switches actually.

11.7. TLS v1.x support

11.7.1. Problem/Issue

The application requires TLS communication only based on TLS v1.2.

How to integrate devices which support TLS v1.1?

11.7.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

11.7.3. Solution/ Workaround

It is possible for users with administrator access rights to enable version TLS 1.0 and 1.1 manually.

To enable TLS v1.0 and v1.1 support proceed as follows:

1. First, locate `java.security` configuration file located in the folder `$INSTALLATION_FOLDER\jre\conf\security`

JRE is installed by NMP/SBM installer and is located here by default (e.g. for NMP Enterprise server on Windows®):

`C:\Program Files\MICROSENS\Enterprise\Server\jre`

2. Edit `java.security` file directly and remove the `TLSv1.1` and/or `TLSv1` entries.

Search for the property `jdk.tls.disabledAlgorithms`. Its contents will be similar to:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, \ +
DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ +
include jdk.disabled.namedCurves
```

By removing the 'TLSv1.1' and/or 'TLSv1' entries, you can add those versions to the list of useable versions.

Should look like the sample below:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, RC4, DES, MD5withRSA, \ +  
DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ +  
include jdk.disabled.namedCurves
```

Chapter 12. SNMP

This chapter describes the general SNMP issues that could arise when working with NMP or SBM.

12.1. SNMP trap listener on port 162 is not working

12.1.1. Problem/Issue

The application shows an error message that the SNMP port 162 cannot be used.

12.1.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

12.1.3. Solution/Workaround

This behaviour is mainly caused by insufficient process permissions.

If you start the application as regular user with limited access rights, the application's process has no access to ports lower than 1024.

So NMP/SBM cannot start SNMP Trap listener on port 162 as it is not accessible so it cannot listen for incoming messages.

You need to run the application as **administrator**, **root** or **sudo** user with administrator access rights!

If the application is started with root permissions it has access to port 162. The SNMP trap listener is started properly and can catch SNMP traps from devices.

12.2. SNMP engine ID and configuration backups

12.2.1. Problem/Issue

The configuration backup of a device contains the unique SNMP engine ID of the specific device.

Given that each of these devices would receive the same SNMP engine ID, could this be a problem if this configuration backup was to be deployed to other devices?

12.2.2. Affected Application

- NMP Professional
- NMP Enterprise
- SBM

12.2.3. Solution/Workaround

NOTE | The following solution applies for MICROSENS G6 switches only!

The application takes care of the SNMP engine ID. When deploying the configuration to a device, it will replace the SNMP engine ID of the configuration with the MAC address of the target switch to make sure the ID is always unique.

Chapter 13. Working with SmartDirector

This chapter describes the general Smart Director issues that could arise when working SBM.

13.1. Troubleshooting SmartDirector Configuration

13.1.1. Problem/Issue

- SmartDirector does not work as expected.
- Devices, actors or sensors seem to show wrong data or no data at all.

How to solve SmartDirector issues?

13.1.2. Affected Application

- SBM

13.1.3. Solution/Workaround

For SmartDirector issues, SBM provides the SmartDirector Configuration Check.

To start the SmartDirector Configuration Check, proceed as follows:

1. Launch SBM client component.
2. In the main menu select Tools > Check Smart Director Configuration

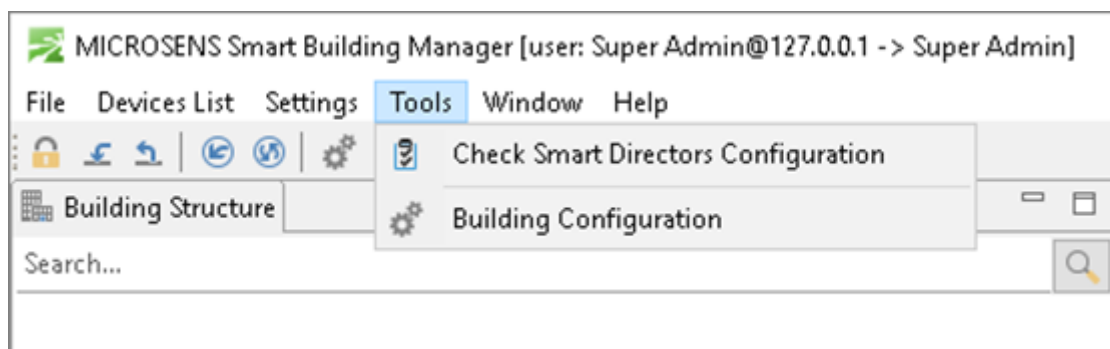


Figure 4. SBM Client Component - Main Menu - Tools

- The SmartDirector Configuration Check opens a dialogue for scanning the configuration of all assigned SmartDirectors.

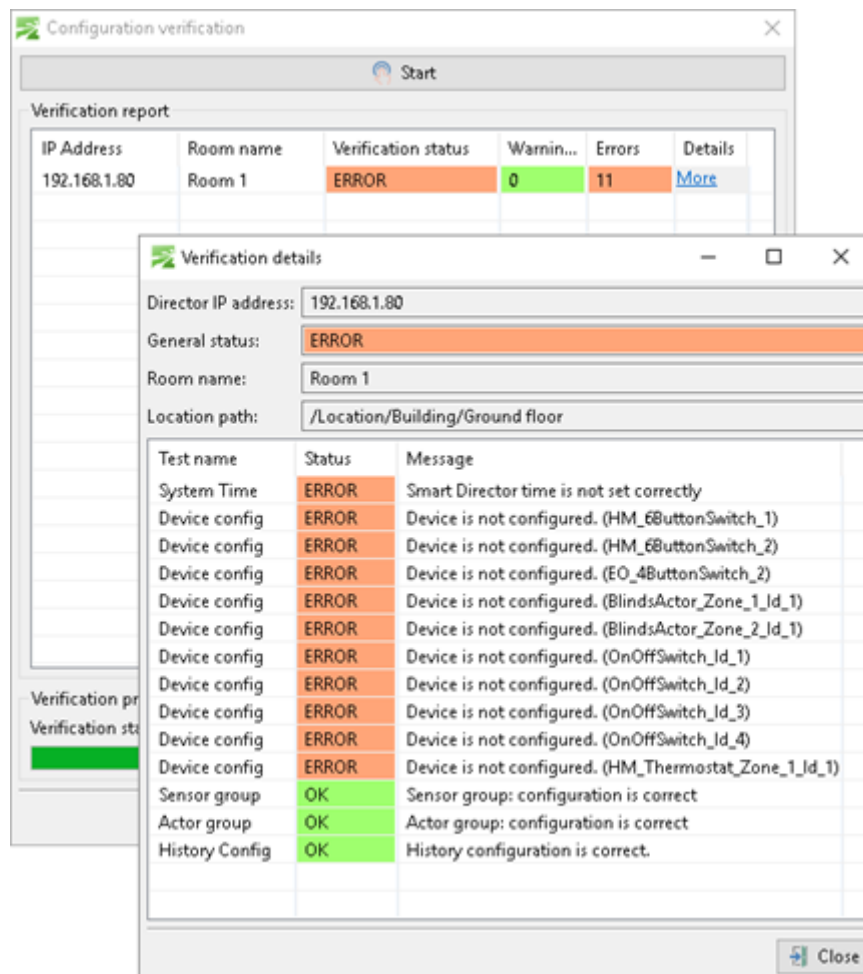


Figure 5. SBM Client Component - Main Menu - Tools - Check SmartDirectors Configuration

3. Click on **Start** to start the scanning process.
 - SBM then lists the status data of all found SmartDirectors.
 - A click on **More** in the column "Details" opens a detailed list of status data of the respective SmartDirector.
4. Click on **Close** to close the dialogue.
5. In the client component, select the affected device, actor or sensor and fix the specific error.

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: DEV-EN-NMP-troubleshooting-kb_v0.6