MICROSENS

Network Management Software NMP

User Manual

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

Management of devices covers monitoring, configuration and administration from a remote site. The Network Management Software (NMP) is a powerful software to assist the network administrator with these tasks.

With its enhanced SNMP based features NMP provides full management access to all manageable devices. All MICROSENS devices are automatically detected by the discovery feature. Even those MICROSENS devices without IP address are listed and can be configured.

NOTE Please keep in mind that NMP is specified to work with MICROSENS devices (G7 and prior, MSP3000, MSP1000). Devices of other manufacturers may not be detected by NMP.

Due to constant product development of MICROSENS devices and the NMP software it may occasionally happen that NMP does not yet detect a MICROSENS device of the latest generation. In this case please contact the MICROSENS support for further help.

1.1. Network Management

1.1.1. Network Administration

NMP provides a discovery functionality that automatically detects all manageable MICROSENS devices in the network (SNMP Discovery, MAC Discovery, IP Based Discovery). The specific configuration can be stored to a device list file (NMP Professional) or a database (NMP Enterprise) and is used for monitoring the network status.

1.1.2. Network Monitoring

Based on the device list file used for network administration serving as a reference the current status of all active, manageable devices in the network can be retrieved automatically. The status is displayed using a graphical interface.

1.1.3. Network Configuration

The hardware configuration of a manageable device, such as port configuration of traffic prioritization, can be viewed and changed for individual devices or for all similar devices in the network simultaneously.

1.1.4. Network Visualisation with Topology Manager

NMP Professional also provides network map visualisation via the topology manager. With this tool it is possible to simply place network devices on the map, link them and monitor their actual status.

1.2. Differences between NMP Product Variants

NMP offers comprehensive tools for convenient and efficient network management.

The NMP product variants differ in the support for these tools as follows:

1.2.1. NMP Professional

NMP Professional works as stand-alone network management software. It offers a comprehensive feature set for network management like configuration of individual or grouped MICROSENS switches and lots of additional network management tools:

- Inventory list generator
- Task scheduler
- E-Mail notifications
- Automatic alarm list generation
- RMA tool
- Switch password changer
- VLAN change tool
- Device search tool
- Topology manager
- Link monitoring

NOTE For more information about these tools see Section 4.4.5.

1.2.2. NMP Enterprise

NMP Enterprise consists of two components:

- The **Server Component** provides access from the client component or a web interface. Up to 20 parallel access requests can be managed by one server instance. With two separate server instances a redundant master-slave replication mode can be implemented
- The **Client Component** is used to access a server instance on a dedicated server system in the corporate network.

Most of the NMP features are common for both NMP standalone variants and the client component of NMP Enterprise. Some of them are exclusively available with the client component, whereas other features are exclusively available for NMP Standalone variant.

NOTE To use the client for server access, no additional licence file is necessary. The client checks the valid server’s licence key file during the login procedure.

1.3. Scope of this User Manual

This user manual refers to NMP v2.10 and covers installation and use of both NMP product variants. Whereas Chapter 2 and Chapter 3 deal with both variants, Chapter 4 and Chapter 5 relate to their respective variants.

2. Install the Application

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

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

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

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

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

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

2.1. Difference between Installation Files for Windows® and Linux

While the application's functionality is identical on both Windows® and Linux operating systems the installation process differs slightly.

	Windows®	**Linux**
Installation files	1x NMP installation file, containing NMP Enterprise and NMP Professional variants	1x NMP Professional 1x NMP Server 1x NMP Client
File format	Standard Windows® `.exe` file	compressed tarball files (`.tar.gz`)
Installation process	via file explorer	via Linux CLI or archive management application

2.2. 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.

NOTE The application requires a 64-bit operating system.

Operating system	• Windows 10, Debian Linux 11 (NMP Enterprise, client component, NMP Professional) • Windows Server 2016, Debian Linux 11 (NMP Enterprise, server component)
RAM	• 8 GB (NMP Enterprise, server component) • 4 GB (NMP Enterprise, client component) • 8 GB (NMP Professional)
Free disk space	• 2 GB + 1 GB/1.000 additional managed devices (NMP Enterprise, server component) • 1 GB (NMP Enterprise, client component) • 2 GB (NMP Professional)
CPU	• 3 GHz, typically 4-6 Core CPU (current Xeon Server CPU; multi-Core i7/i5 Desktop CPU) (NMP Enterprise, server component), • 2 GHz, typically 4-6 Core CPU (multi-Core i7/i5 Desktop CPU) (NMP Enterprise, client component) • 2 GHz, typically 4-6 Core CPU (multi-Core i7/i5 Desktop CPU) (NMP Professional)
Display resolution	• at least 1280*1024 • recommended: 1920*1080

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

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

2.3. Additional Requirements for Server Access

"Client-side" refers to operations that are performed by the client in a client-server relationship in a computer network.

2.3.1. Client Component

The setup is performed by running the common NMP installer. Within the installation process the component option "Client" must be activated.

NOTE To use the client component for server access, no additional licence key file is necessary. The client component checks the valid server licence key file during the login procedure.

2.4. Port and Firewall Settings

To ensure a proper operation of all NMP variants in the corporate network the following port and firewall settings are mandatory:

Port	Protocols	Description
22	TCP/IP, SSH	SSH communication between application and device
25	TCP/IP, SNMP	Used for email notification: • can be enabled or disabled • default value, configurable
67	UDP/IP, BOOTP	Bootstrap protocol for application and device (local server port): • application listens on this port’s BootP frames
68	UDP/IP, BOOTP	Bootstrap protocol for application and device (remote client port): • application sends BootP configuration frames
161	UDP/IP, SNMP	Used by the SNMP trap receiver for application and device: • application initiates the communication with devices • application listens on this port for SNMP traps • can be enabled or disabled • default value, configurable
162	UDP/IP, SNMP	Used to forward SNMP trap to the northbound interfaces to a higher level management system: • if receiving SNMP traps is enabled, application listens on this port for SNMP Traps • can be enabled or disabled • default value, configurable

Port	Protocols	Description
514	UDP/IP, Syslog	Syslog server on server component: • used to receive Syslog messages • can be enabled or disabled • default value, configurable Syslog client on server component: • used to send Syslog messages to an external SYSLOG server • can be enabled or disabled
1025	UDP/IP, MICROSENS proprietary protocol	Used for device communication for G5 and older switches: • application initiates the communication with devices
1025	TCP/IP, HTTPS	Used for device communication with new generation switches (Micro Switch G6, Industrial Switch G6, NM3 modules): • application initiates the communication with devices
1812	UDP/IP (PAP, CHAP)	Used to communicate with a RADIUS Sever: • can be enabled/disabled • default value, configurable
4000	TCP/IP	Communication between NMP server and NMP client component: • send server-client commands in both directions • also used when replication mode is enabled • default value, configurable
4001	TCP/IP, FTPS (FTP over SSL)	Communication between server and client component: • default value, configurable
4002	TCP/IP	Used for database access: • database server on server • default value, configurable

Port	Protocols	Description
4003	TCP/IP	Communication between server and client component: • used exclusively with MSP1000 devices • forwarding data from MSP1000 platform to client via server • default value, not configurable
4177	TCP/IP	Used by master and slave servers (replication server port): • database replication mode • can be enabled or disabled • default value, configurable
5555	TCP/IP, MICROSENS proprietary protocol	Used for communication with NM1 and NM2 modules for application and device: • management modules for MSP1000 access platform
8080	TCP/IP, HTTP	Web server on server component: • can be enabled or disabled • default value, configurable
8340	UDP/IP, MICROSENS proprietary protocol	Used by IP request listener for application and device (local port): • application listens on this port for special UDP packets (IP requests) • used for device IP configuration of all generations of MICROSENS switches and NM3 modules
8341	UDP/IP, MICROSENS proprietary protocol	Used for IP configuration for application and device (remote G5 Port): • application sends IP configuration packets on this port • used for device IP configuration of all generations of MICROSENS switches and NM3 modules

Port	Protocols	Description
8342	UDP/IP, MICROSENS proprietary protocol	Listening for RING error frames for application and device (local port): • application listens on this port for special UDP packets (RING error frames)
8443	TCP/IP, HTTPS	Web server on server component: • can be enabled or disabled • default value, configurable

NOTE NMP acts as TFTP/FTP client. This means it initiates the communication. Therefore all standard TFTP and FTP ports (20, 21, 69) are used.

2.5. Installation on Windows® Operating Systems

2.5.1. Run the Install Executable

The naming convention of the installer is as follows:

- MICROSENS_`<application>`_v`<x.y.z>`_win64.exe

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

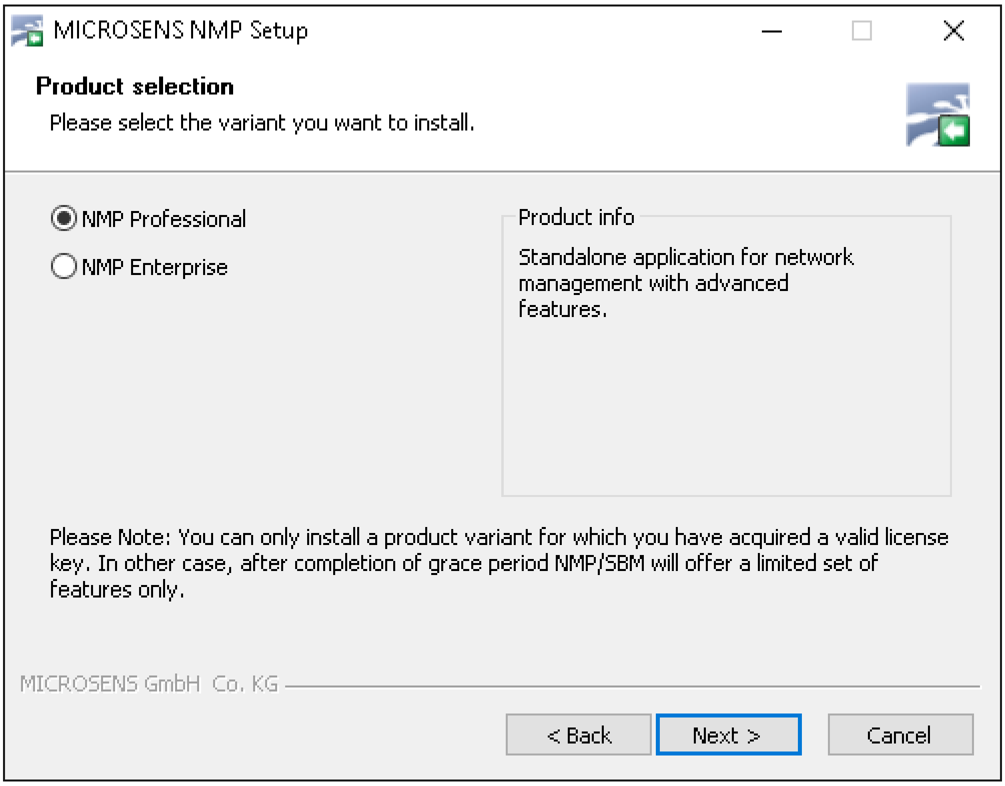
After reading the licence agreement click the button **I Agree** to go to the product selection dialogue.

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

2.5.2. Product Selection

This installer application contains all NMP variants.

NOTE If you already own a valid license key file, place it in the same folder as the installer application. In this case the NMP installer automatically selects the correct NMP variant and skips the following dialogue.



Product selection

Please select the variant you want to install.

● NMP Professional

○ NMP Enterprise

Product info

Standalone application for network management with advanced features.

Please Note: You can only install a product variant for which you have acquired a valid license key. In other case, after completion of grace period NMP/SBM will offer a limited set of features only.

Figure 1. Installation - Product Selection

Select one of the following products for installation:

- If you want to use NMP as stand-alone variant, select "NMP Professional".
- If you want to use NMP for client server installation, select "NMP Enterprise".

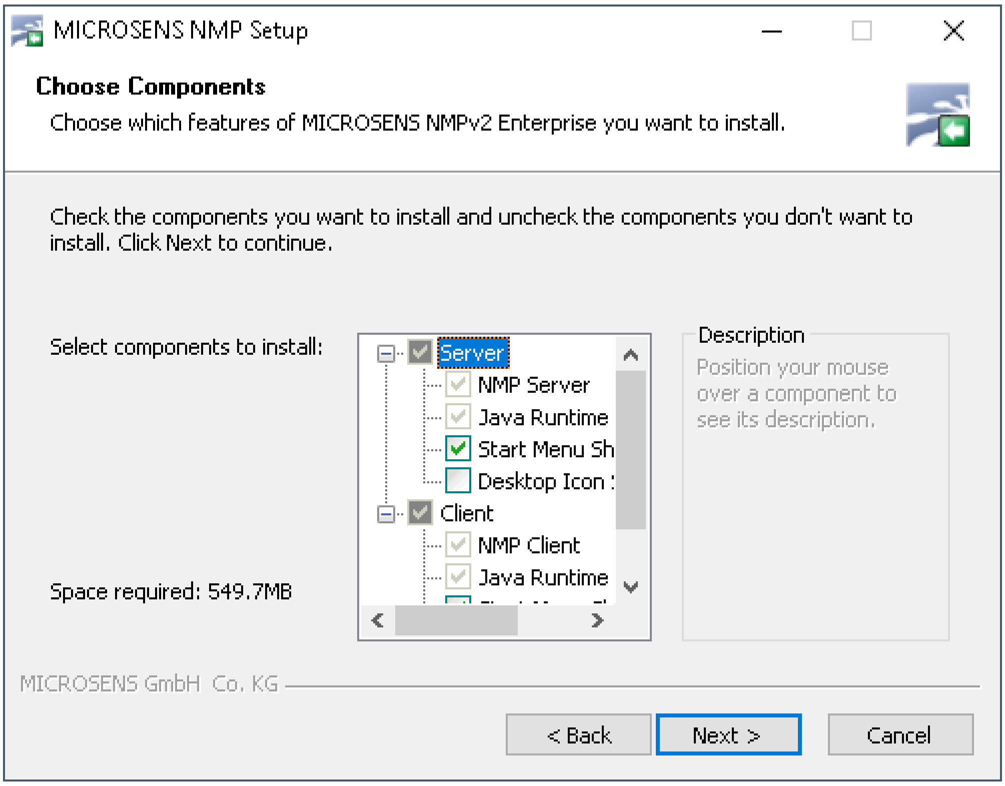
After hitting the button `Next` a confirmation dialogue appears containing information about the selected software product. Proceed with a click on the button `Next`.

NOTE The following installation dialogues show the installation process of NMP Enterprise. The dialogues of NMP Professional may slightly differ.

2.5.3. Choose Components

There are two components available for selection:

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



MICROSENS NMP Setup

Choose Components

Choose which features of MICROSENS NMPv2 Enterprise you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Server
  - ☑ NMP Server
  - ☑ Java Runtime
  - ☑ Start Menu Sh
  - □ Desktop Icon :
- ☑ Client
  - ☑ NMP Client
  - ☑ Java Runtime

Description

Position your mouse over a component to see its description.

Space required: 549.7MB

MICROSENS GmbH Co. KG

Figure 2. Choose Components

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

IMPORTANT

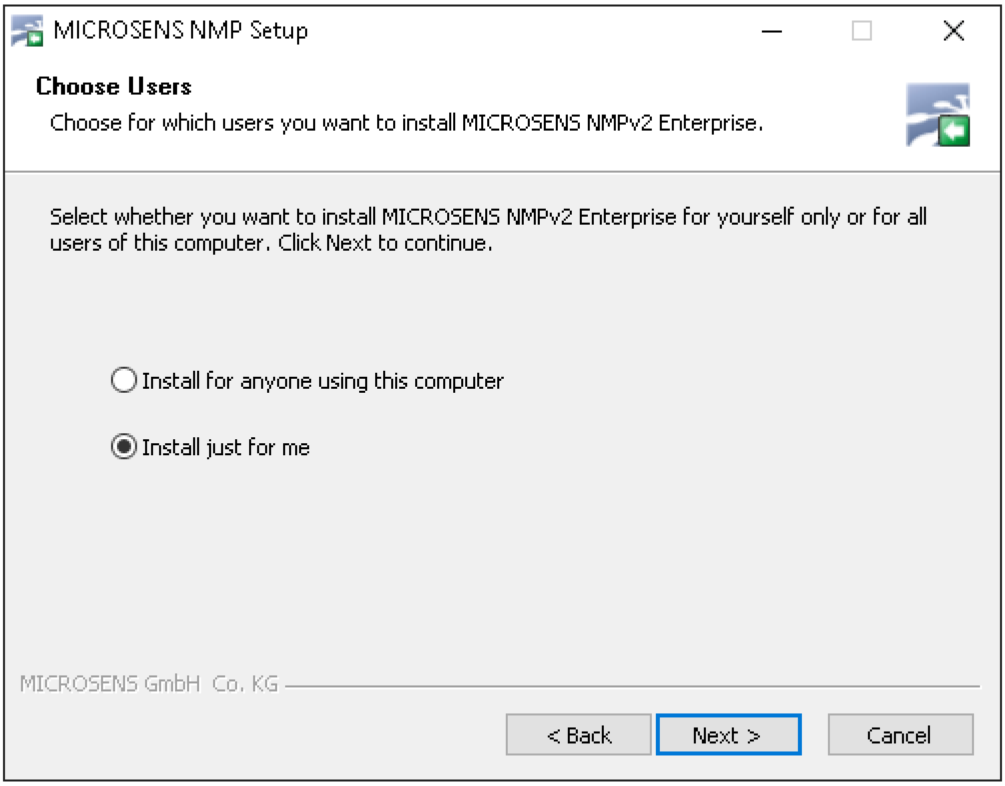
Due to further development of the application, since version v3.0 the stand-alone client component of the application will be deprecated and replaced by the web client operated by your web browser.

NOTE

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

2.5.4. Choose Users

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



MICROSENS NMP Setup

Choose Users

Choose for which users you want to install MICROSENS NMPv2 Enterprise.

Select whether you want to install MICROSENS NMPv2 Enterprise for yourself only or for all users of this computer. Click Next to continue.

○ Install for anyone using this computer

● Install just for me

MICROSENS GmbH Co. KG

Figure 3. Choose Users

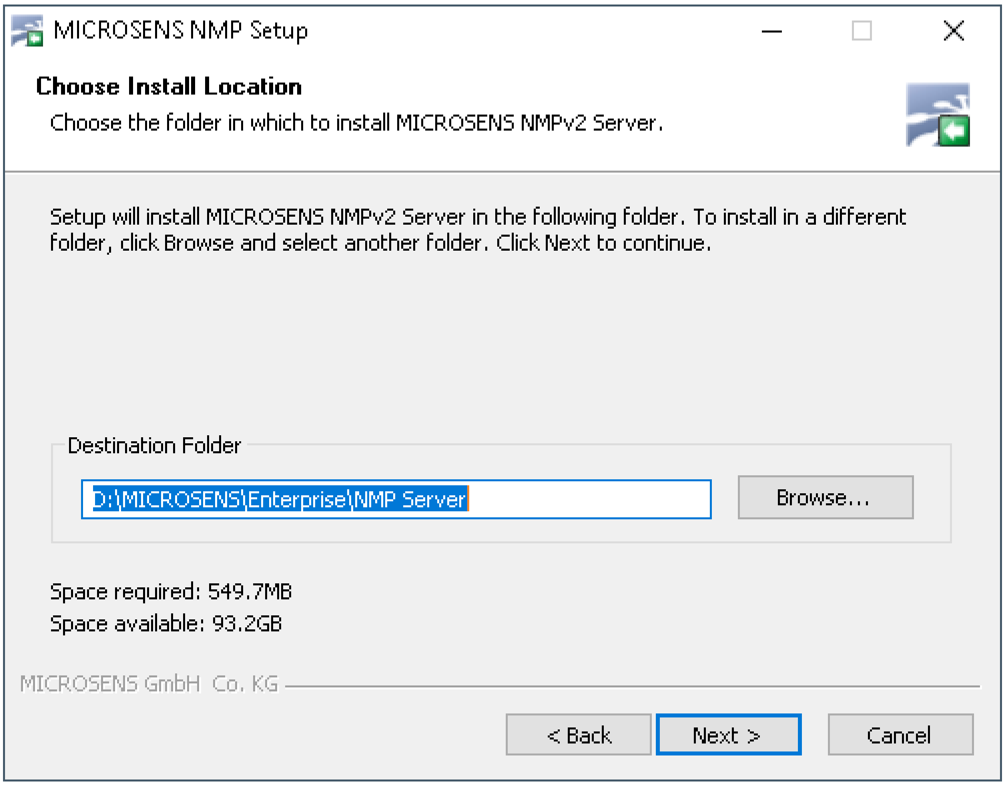
Install for anyone using this computer: Every registered user on this computer is able to use the management application after installation. This should be enabled in exceptional cases if it is ensured that only the responsible network administrator have access to this computer.

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

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

2.5.5. Choose Install Location

On the respective installation location screens determine the destination folders for Server Manager and stand-alone client component (if client installation was previously selected).



MICROSENS NMP Setup

Choose Install Location

Choose the folder in which to install MICROSENS NMPv2 Server.

Setup will install MICROSENS NMPv2 Server in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: D:\MICROSENS\Enterprise\NMP Server

Space required: 549.7MB
Space available: 93.2GB

MICROSENS GmbH Co. KG

Figure 4. Choose Install Folder

Hit the button `Next` (for stand-alone client installation folder, if applicable) and the button `Install` to start the installation process on the system.

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

The MICROSENS application is ready to be started.

2.5.6. Installation Path

During the first start up the application creates an additional folder in the user's home directory `%USERPROFILE%\NMPv2` (for NMP Professional) and `%USERPROFILE%\NMPv2 Server` (for server component of NMP Enterprise).

All configuration files (licence key file, device list, saved device configuration files, application configuration file) will be saved in the respective directory by default. Change the default location by changing the application's data directory in the application's settings.

2.6. Installation on Linux Operating Systems

NOTE For more information on how to use the CLI or the archive management application of your specific Linux distribution please refer to the respective documentation.

To install the application on Linux use the following steps:

1. Create a new directory on the local computer (for the application's client component or NMP Professional) or on a remote server (for the server component), e.g. `~/MICROSENS/NMP_Professional/` or `~/MICROSENS/NMP_Server/` . Extract the files contained in the respective tarball file into this directory, either by opening the CLI and using the tar command (e.g. `tar -zxvf microsens_nmp_professional_v2.x.x_64bit.tar.gz`) or the respective archive management application of your Linux distribution.
2. After file extraction is finished the application has to be started with root access rights.

2.7. Configuration Folder Presetting (NMP Enterprise)

By default, NMP Enterprise is using the user's home directory to find the properties file. This can be changed before starting NMP Enterprise.

On Windows®

After installing NMP Enterprise as Windows® service, edit the file `NmpServerService.ini` located at the NMP installation folder (by default `C:\Program Files\MICROSENS...`).

The following line must be added: `arg.2=--context=path_to_context_folder` (e.g.: `arg.2=--context=D:\TEST`)

On Linux OS

To change the NMP properties file directory change the script `nmps_daemon_controller.sh`.

The correct path of the folder with license and configuration files must be defined by editing the variable `SRV_CONTEXT_PATH="/path/to/server/settings"`.

Additionally, find the lines starting with `nohup` (one of them is commented out).

One of them is used to start the service with default folders, the second one uses the configured context path. The second one has to be uncommented to select the custom context folder.

In this case, the other line must be commented out.

2.8. Software Update

IMPORTANT

With **Version 2.8.8** the database file handling has changed due to an updated database version.

Therefore it is not possible to downgrade to a prior application’s version, once you have upgraded to version 2.8.8!

It is strongly recommended to backup the application’s data folder before updating from an earlier version to version 2.8.8 and newer!

NOTE

When updating from versions prior version 2.9.6 please read the information regarding using the application’s server instance as Microsoft Windows® service on Section 7.15. NOTE: When updating SBM from versions prior version 2.9.6 please read the information regarding using the application’s server instance as Microsoft Windows® service on Section 7.15.

The application is undergoing continual development in order to extend and customize it to rising and changing requirements. Therefore it is mandatory that you regularly visit the MICROSENS website to download the latest release of the application.

It is mandatory to always update both the client and server components to ensure consistency of the installed product.

IMPORTANT

Before starting the update process, the installer will evaluate the available memory on the target device. If there is no sufficient space, the update process will be canceled.

In order to update the application, proceed as follows:

1. Stop a running application.
   a. **NMP Professional:** Exit the application.
   b. **NMP Enterprise:** Stop the server instance and exit the Server Manager or stop the server service (if the server component was started as Windows service).
2. Subsequently install the updated version.
3. During the installation choose the same installation path as the path chosen for the previous version. All application files will be updated.

2.9. Installation in Silent Mode

It is possible to install the application in silent mode, which means that the installation happens automatically by passing specific parameters to the the installer.

These parameters read as follows:

`/S`

Silent installation

- No GUI
- Only message boxes are displayed if any error will occur which blocks the installation.

`/NmpProduct=[enterprise|professional]`

Selection of product to be installed

- One of `enterprise` or `professional` should be provided
- One of both must be provided in case of silent installation!

`/ProductComponentServer=true|false`

Used only if Enterprise product is selected

- Select `true` to install NMP server component of NMP Enterprise product
- Select `false` to skip installation of NMP server component.
- Parameter `true` is default if not specified.

`/ProductComponentClient=true|false`

Used only if Enterprise product is selected

- Select `true` to install NMP client component of NMP Enterprise product
- Select `false` to skip installation of NMP client component.
- Parameter `true` is default if not specified.

`/StartMenuShortcut=true|false`

Choose to create Start Menu groups during installation process

- Parameter `true` is default if not specified
- Will be applied for all components which will be installed

`/DesktopShortcut=true|false`

Choose to create desktop short cuts during installation process

- Parameter `true` is default if not specified
- Will be applied for all components which will be installed

`/AllUsers`

Install for all users

- If not specified install just for current user.

`/D=c:\override\default\installdir`

Overwrite installation path

- Use always as last parameter!
- Use without quotes, even if installation directory contains spaces!
- Will be applied for all components which will be installed.
- Components will be installed in subfolders of defined folder.

Example 1

Installation of NMP Professional with GUI, preselected options:

- install NMP Professional,
- create start menu group,
- do not create desktop shortcut,
- install for all users,
- no silent mode

```
D:\installers\MICROSENS_NMP_Installer_v2.10.0_win64.exe  /NmpProduct=professional
/StartMenuShortcut=true /DesktopShortcut=false /AllUsers
```

Example 2

Installation of NMP Enterprise Client in silent mode:

- install NMP Enterprise client only,
- create Start Menu group,
- create desktop shortcut,
- install for current user only,
- silent mode,
- installation path specified as `D:\MICROSENS` (subfolder `Enterprise\Client` will be

created for NMP Client files.

```
D:\installers\MICROSENS_NMP_Installer_v2.10.0_win64.exe         MICROSENS_NMP_Installer_v2.7.0_win64.exe /S /NmpProduct=enterprise /ProductComponentServer=false /ProductComponentClient=true     /StartMenuShortcut=true     /DesktopShortcut=true /D=D:\MICROSENS
```

3. Licensing

A licence key file is necessary to allow for usage of the application's server component and as well for operating NMP Professional .

3.1. Trial Period Licences

For testing purposes it is possible to obtain a temporary licence key file which provides a temporary right-of-use for a limited period of time (60 days). Please contact your MICROSENS representative.

NOTE After the trial period is expired, all devices except one in the device list will be set to a not managed state. Not managed devices are not polled and the context menu is not available. After installing a valid and appropriate licence key file, the application reactivates these devices.

3.2. Product Variants

Depending on the article number of the purchased usage rights a licence key file will be created and provided to the customer which enables a coverage of managed devices that differs as follows:

Product	Art. No.	Managed Devices
NMP Enterprise	MS200100	200
	MS200102	1000
NMP Professional	MS200070	50
	MS200072	100

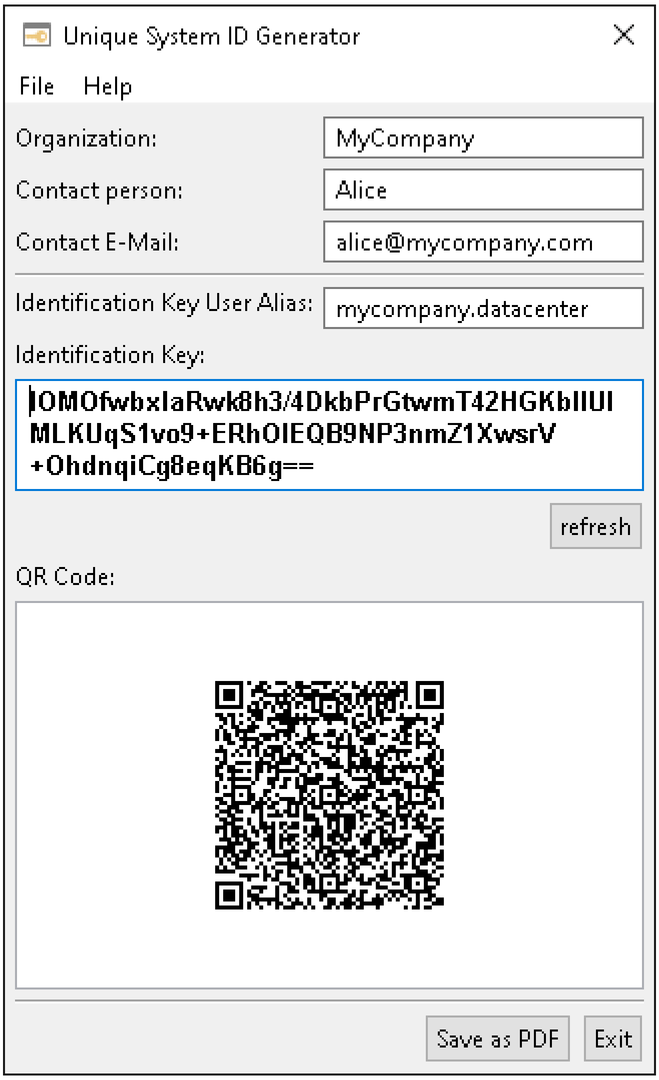
NOTE For questions regarding usage right upgrades or the prolongation of maintenance periods please contact your MICROSENS representative.

3.3. Using the Unique System ID Generator

For purchasing a valid product licence key file, the use of the MICROSENS Unique System ID Generator is mandatory.

The application is available on the MICROSENS web site (www.microsens.com) and needs to be installed on the workstation or server where the software will be used.

NOTE When using a licensed application the Unique System ID Generator is a part of the respective application. Please refer to the user manual on how to use the generator included for the purchase of for e.g. additional maintenance licence key files.



Organization: MyCompany

Contact person: Alice

Contact E-Mail: alice@mycompany.com

Identification Key User Alias: mycompany.datacenter

Identification Key:

```
OMOfwbxlaRwk8h3/4DkbPrGtwmT42HGKbIIUI
MLKUqS1vo9+ERhOIEQB9NP3nmZ1XwsrV
+OhdnqiCg8eqKB6g==
```

Figure 5. Unique System ID Generator

On start-up the application calculates the unique system ID and generates the corresponding hash sum.

NOTE The application does not scan hard disk or memory content.

- **Organization:** Name of the organization (e.g. the company name) which orders the licence key file (optional).
- **Contact person:** Name of the contact person for queries relating the purchase order (optional).
- **Contact E-Mail:** Preferred e-mail address of the the contact person (optional).
- **Identification Key User Alias:** This string can be used to assign a mnemonic identifier to the unique system ID.

  This simplifies locating the system ID in the licence manager later on instead of searching for a counterintuitive multiple-digit hash sum (optional, but recommended).

- **Identification key:** Contains the hash sum of the system ID as a string.

  This is used to protect the privacy of the machine.

- **QR Code:** The QR code is the graphical representation of the hash sum and therefore simplifies its handling.
- **Save as PDF:** After entering the additional data click on the button `Save as PDF`. This will create a PDF file containing all respective information for ordering the licence key file.
- **Exit:** Click on the button `Exit` to close the application.

IMPORTANT The system ID (and therefore the resulting hash sum) represents the actual hardware and software configuration of the system. When changing this configuration after obtaining a valid licence key file it is necessary to order a new licence key file that fits the new system configuration.

3.3.1. Steps for Ordering a Licence Key File

1. Download and install the Unique System ID Code Generator

   When using a licensed application the Unique System ID Code Generator is a part of the respective application. If you are using a valid licence key already, start the code generator from your application.

2. Enter all data (i.e. organization, contact information and alias)
3. Save the activation code as a PDF file
4. Send the PDF file to your MICROSENS representative.

   MICROSENS will generate a licence key file corresponding to this activation code.

5. After receiving the licence key file, register it with the licence manager of your application.

NOTE For more information about using the licence manager please refer to the user manual of your application.

3.4. Select Licence Key File for Server Manager

NOTE Running the Server Manager does not require any login but a valid licence key file. The licence file is necessary to use the server.

If no licence has been selected (especially after installation of the application) the following dialogue prompts to select the licence key file.

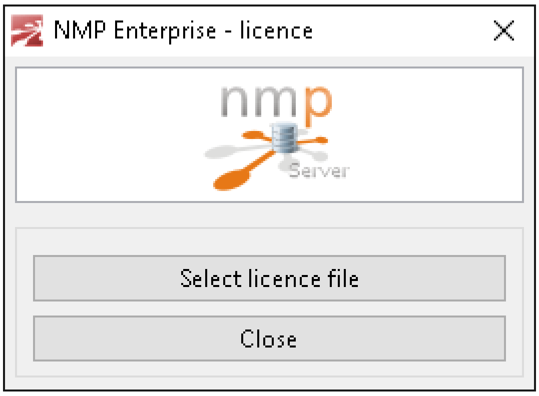


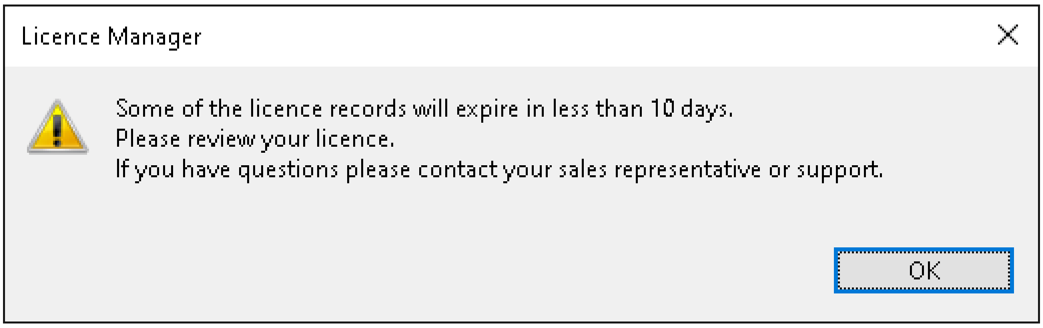
Figure 6. Licence Key Selection

NOTE The evaluation or trial licence of the application does not include a USB dongle. When starting the server manager with an evaluation or trial licence, please confirm the respective error message reporting a missing hardware USB key.

If you do not have a valid licence file, please contact MICROSENS.

3.5. Licence Key Expiry

The software checks for a valid licence key file during start-up and displays a notification, when the licence will expire in the near future.



Some of the licence records will expire in less than 10 days.
Please review your licence.
If you have questions please contact your sales representative or support.

Figure 7. Licence Key Expiry Note

For more information about your licence key file status check your registered licence key file under **Settings** › **Licence Info**.

To update your licence key files contact your sales representative or the MICROSENS support.

4. NMP Professional

This chapter describes working with NMP Professional.

NOTE The following descriptions and screenshots refer to the Windows® version of NMP. Because NMP is a Java application based on Eclipse OpenJ9, the GUI appearance does not considerably differ between Windows® and Linux operating systems. The NMP functionality is exactly the same.

NOTE In the event of technical problems with NMP, please contact the technical support of MICROSENS under the link provided within the report dialogue. For a precise and effective support save the provided report as text file and upload it to the MICROSENS ticket system when required.

4.1. Starting NMP Professional

4.1.1. Starting the Application on Windows®

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

Start › MICROSENS › MICROSENS NMPv2

or

Start › MICROSENS › MICROSENS NMPv2 (Debug mode)

The application opens with its login dialogue.

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

4.1.2. Starting on Linux Operating Systems

NOTE The application uses some ports lower than 1024. On UNIX like operating systems only applications started with root rights are able to bind those port. Therefore it is important to start the application with `sudo ./NMP` or `su root ./NMP` (or the respective super user command of your Linux distribution)

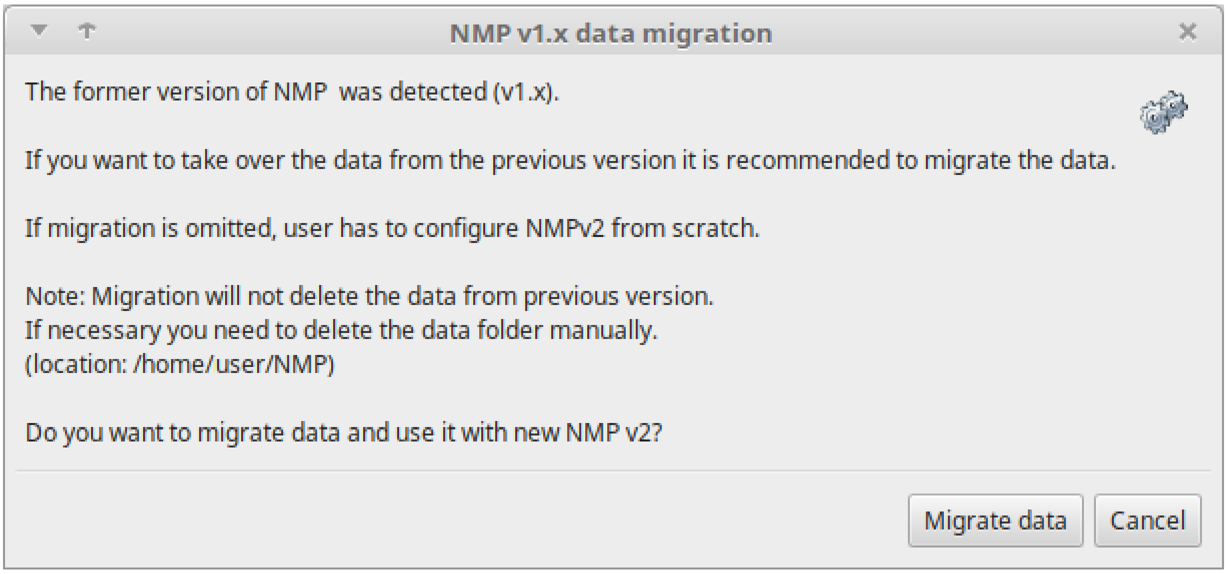
For more information please refer to the MICROSENS Knowledge Base on the website www.microsens.com/support.

1. Open a Linux CLI and change to the application's installation directory (e.g. `~/MICROSENS/NMP_Professional`).

2. Start the application as super user.

4.1.3. First Program Start

During first start the application checks whether a previous version 1 installation is available. If so, the application asks to migrate the data from this earlier version to version 2.


NMP v1.x data migration

The former version of NMP was detected (v1.x).

If you want to take over the data from the previous version it is recommended to migrate the data.

If migration is omitted, user has to configure NMPv2 from scratch.

Note: Migration will not delete the data from previous version.
If necessary you need to delete the data folder manually.
(location: /home/user/NMP)

Do you want to migrate data and use it with new NMP v2?

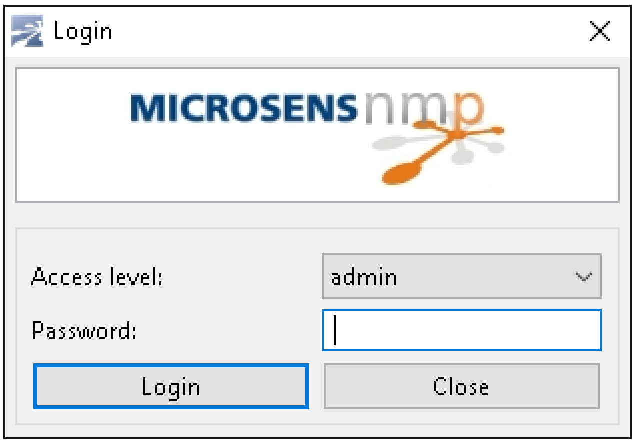
Figure 8. Data Migration from version 1

Click on the button `Migrate data` to transfer the data.

The application will create a new directory `~/NMPv2` in the user’s home directory.

The first time starting process continues with licensing of NMP Professional. For more information see Chapter 3.

4.2. Login



Access level: admin
Password:

Figure 9. NMP Professional - Login

After NMP Professional start-up entering username and password is obligatory.

Default login settings are

Administrator

- Access level: admin
- Password: admin

Standard User

- Access level: user
- Password: user

NOTE It is strongly recommended to assign a different password after using the software for the first time to prevent unauthorized access to the software!

A user with administrative privileges is able to

- configure NMP Professional,
- change device settings,
- update the firmware of devices which are managed by NMP Professional,
- monitor the state of managed devices,
- edit the device list.

A standard user is able to:

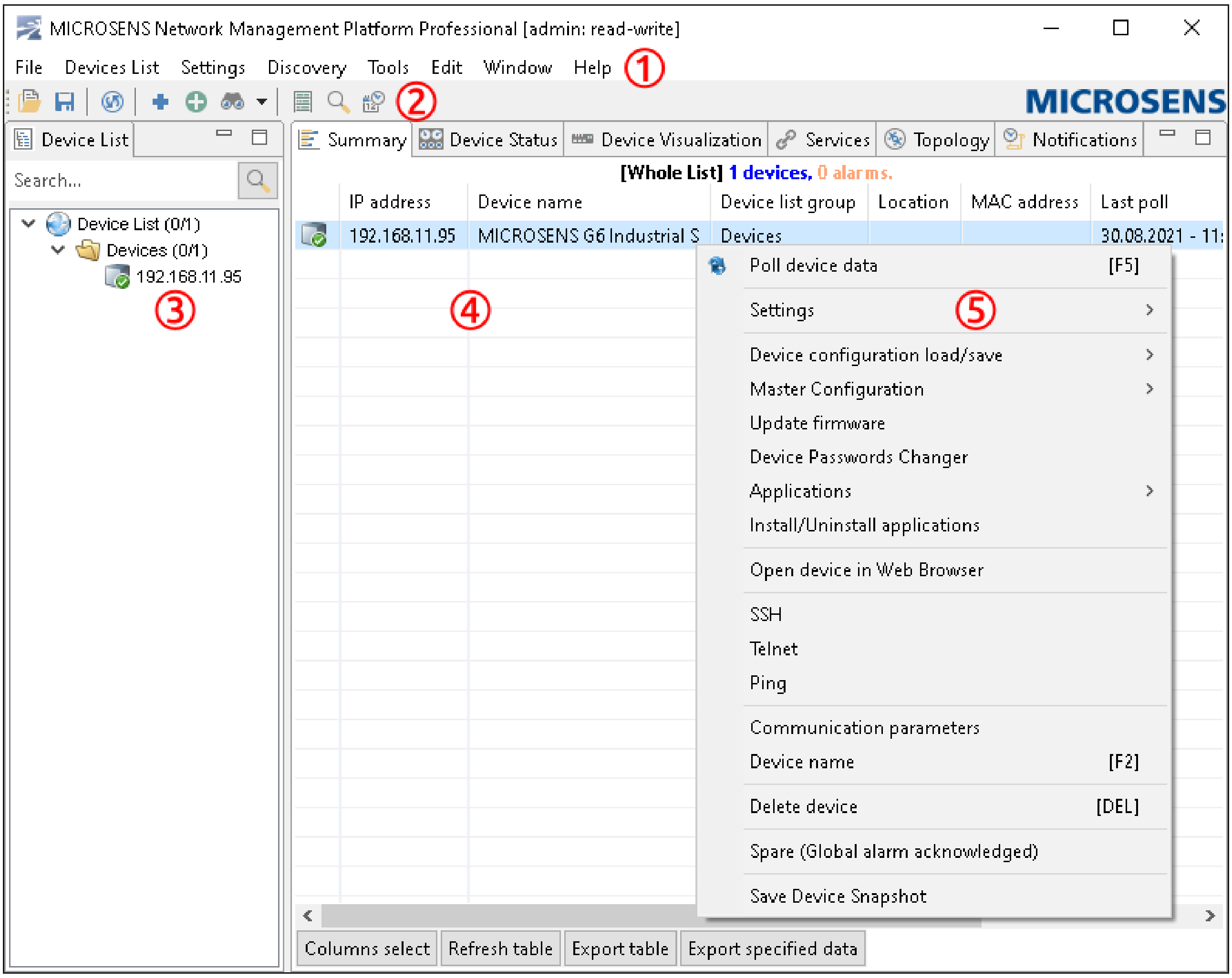
- monitor device state,
- edit device list.

User name and password can be set in the menu **Properties** › **Security Settings**.

NOTE At first start-up the user with administrative rights should configure all application settings.

NOTE After login for the first time a dialogue opens, where it is possible to upload the licence key file. For more information about licensing NMP see the MICROSENS Licensing Guide or go to the MICROSENS website (www.microsens.com/products/nmp-software).

4.3. NMP Professional Main Window



IP address	Device name	Device list group	Location	MAC address	Last poll
192.168.11.95	MICROSENS G6 Industrial S	Devices			30.08.2021 - 11:

Figure 10. NMP Professional - Main Window

The main window of NMP Professional consists of four main elements:

1. Main Menu (see Section 4.4)
2. Main Menu Toolbar (see Section 4.5)
3. Device List Tree (see Section 4.6)
4. Tabbed Data Panel with filter section (see Section 4.7)
5. Context Menu (see Section 4.8)

A detailed description of these elements is provided in the following sections.

4.4. Main Menu

The NMP main menu bar provides access to the following functions:

File	Handling device lists and exiting NMP (see Section 4.4.1)

Devices List Managing devices and groups (see Section 4.4.2)

Settings Managing application and user settings like (see Section 4.4.3)

Discovery Discovering new devices in the network (see Section 4.4.4)

Tools Several handy tools for managing the network infrastructure (see Section 4.4.5)

Edit Standard editing functions for devices and groups (see Section 4.4.6)

Window Managing the appearance of NMP (see Section 4.4.7)

Help Access to the NMP user manual and general NMP information (see Section 4.4.8)

4.4.1. File

Open (`Ctrl`+`O`)

Opens a dialogue box to select and import a device list. The following outcomes are possible:

- An existing device list (or a managed device contained therein) is highlighted in the device list tree: The imported device list is inserted as a device sub-list.
- No device list (or managed device) is highlighted in the device list tree: The imported device list is inserted as new top-level "Imported devices list".

Save (`Ctrl`+`S`)

Exports the device list into a file specified by the user (extension: `.nmpdl`). Usually, this file is automatically saved by the application on exit.

Import CSV Device List

Imports a previously saved inventory list (see Section 4.4.5.1).

Exit and force default layout

Exits NMP. Next time you start NMP its default GUI layout is selected (window maximised, icon toolbar position on top, icon size 16x16).

NMP automatically saves the current configuration in the configured NMP data directory (default is `$USER_HOME/NMPv2`).

Exit (Ctrl+Q)

Exits NMP. NMP automatically saves the current configuration in the configured NMP data directory (default is `$USER_HOME/NMPv2`).

To change the NMP data directory please refer to Section 4.4.3.1.

4.4.2. Devices List

Add new device

Used to add a new device to the device list manually. It is also possible to add a new device by right mouse clicking on a group in the tree view and choosing **Add new device** from the group context menu.

Add new subgroup

Create a new subgroup within the current group in the device list.

New groups can be added to the main group (indicated by the global network icon). It is possible to add a new empty group by choosing **Add New Subgroup** in the tree context menu.

The user can specify the group name. The length of a group name string is unlimited. The maximum number of groups is also unlimited. Each group can have an unlimited number of subgroups. The group names do not have to be unique.

Refresh selected (F5)

Use these menu items to refresh selected device(s), group(s) or all devices for data.

If a selected device is not responding, a `No response from device!` error message will be displayed in the log window and the device icon will turn red.

If logging is enabled the result of the polling process is automatically written to a log file. Logging can be enabled under **Settings › Log file/E-mail/Events**.

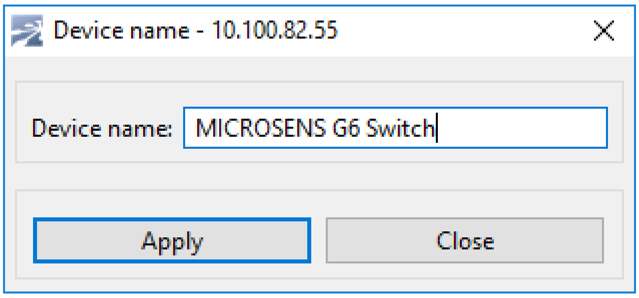
The poll task is also available in the context menu. Choose **Poll Device Data** or use the keyboard shortcut F5.

NOTE NMP is able to poll up to 100 devices at once. To avoid data loss with NMP running on computers or servers with limited processing power, highly loaded networks or slow network connections, it is recommended to reduce the number of concurrent poll threads. Configuration is available under **Settings › NMP Settings**.

Additionally, a cyclic device data refreshing function is implemented. This function can be configured per device or for all devices. For more information please refer to communication parameters option from device tree context menu (see Section 4.8).

Edit name (F2)

This dialogue dynamically depends on the selected item. If a device is selected the device name prompt will be opened:

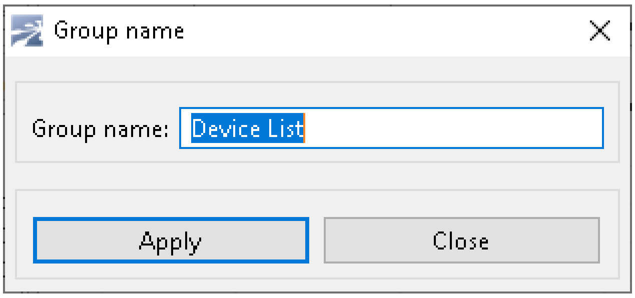

Device name - 10.100.82.55

Device name: MICROSENS G6 Switch

Figure 11. NMP - Edit Device Name

The prompt will edit the device description displayed in the NMP tree (next to IP address). The description length is limited to 25 characters. For some device types (e.g. switches) NMP will prompt to apply the new description string to the device. In this case the device description string length is limited (e.g. for switches the limit is 25 characters).

If a group in the device list is selected the group name dialogue will be opened.


Group name

Group name: Device List

Figure 12. NMP - Edit Group Name

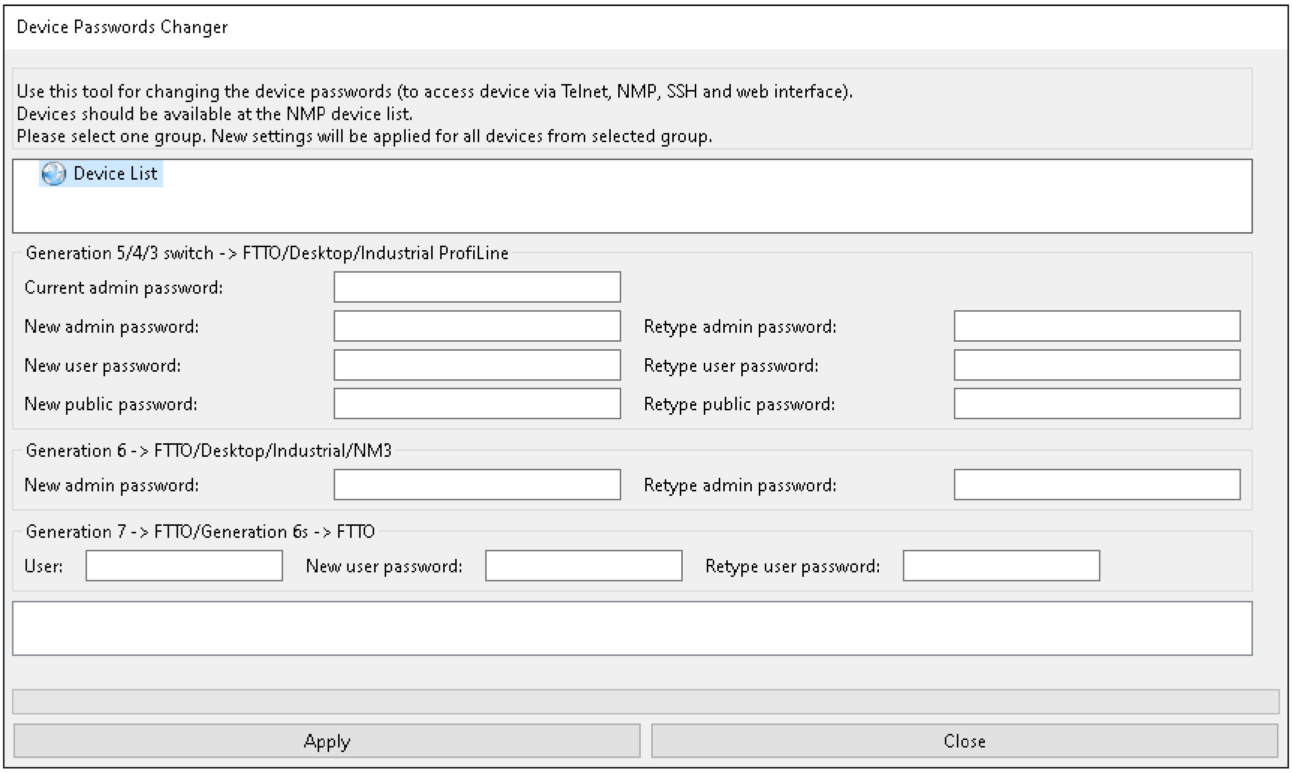
Enter the new group name in the text field and hit the button `Apply` on the keyboard. It is also possible to edit the group name by selecting the menu item from the context menu (right mouse click on the group name). The group name’s string length is unlimited.

Clear device list

Removes all items (groups and devices) from the device list. When this operation is finished, there remains one empty main group "Device List" in the left-hand pane tab **Device List**. NMP will prompt for the confirmation.

Device Password Changer

The Device Password Changer allows changing the administrator and user passwords (used also for Telnet/SSH and Web Manager login) for multiple devices. To change passwords for devices of a particular group, select a group, enter the current administrator password and new passwords for both user types and hit the button `Apply`. Below the buttons `Apply` and `Close` an operation log for all devices will be displayed afterwards.



Device Passwords Changer

Use this tool for changing the device passwords (to access device via Telnet, NMP, SSH and web interface).
Devices should be available at the NMP device list.
Please select one group. New settings will be applied for all devices from selected group.

Figure 13. NMP - Device Password Changer

NOTE

The Device Password Changer is designed for MICROSENS Switches and the NM3 management module for MSP 1000. It will not work with any other type of device.

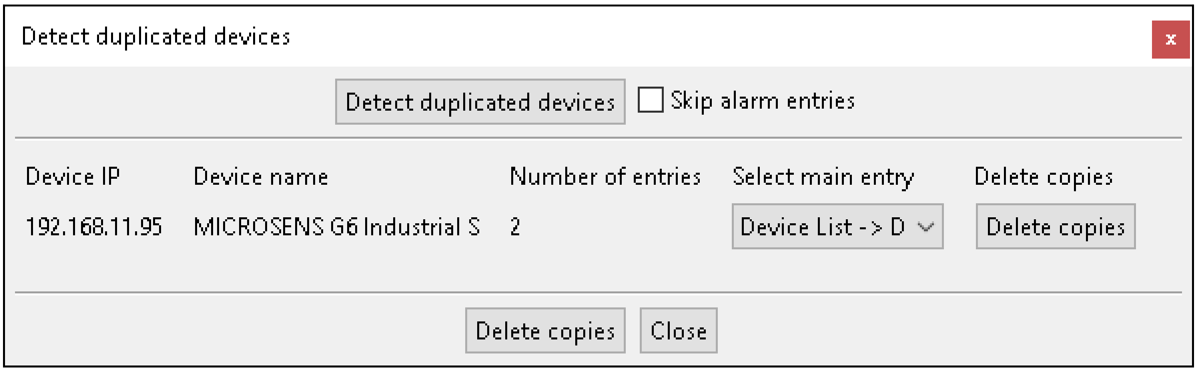
Due to constant product development of MICROSENS devices and the NMP software it may occasionally happen that NMP does not yet detect a MICROSENS device of the latest generation. In this case please contact the MICROSENS support for further help.

NOTE

To change the passwords of a single device use the **Device Password Changer** tool of the devices context menu entries in the device list tree or the **Summary** tab (see Section 4.8).

Detect Duplicated Devices

NMP allows creating a copy of an existing device. In such case two or more tree items can be assigned to one "real" device. This menu item finds all the duplicated devices and deletes them. After this "clean-up" the device list contains one tree item for one "real" device.



Device IP	Device name	Number of entries	Select main entry	Delete copies
192.168.11.95	MICROSENS G6 Industrial S	2	Device List -> D	Delete copies

Figure 14. NMP - Detect Duplicated Devices

The dialogue above shows the list of duplicated entries. The number of entries for each duplicated device is displayed. Select the "main entry" that will not be removed. There are two options to delete duplicate entries:

- Hitting the button **`Delete copies`** next to the entry deletes duplicates of the respective entry.
- Hitting the button **`Delete copies`** at the bottom of the dialogue (next to the button **`Close`**) deletes all duplicates of all entries.

Hitting the button **`Detect duplicated devices`** starts a re-scan of the device list.

By default, the tool searches for duplicates in all groups. After selecting the option "Skip alarm entries" NMP will not search for copies at the "Alarm list" group.

NOTE The "Alarm list" is created by NMP if there are any devices with "error" state at the devices list. Configure the automatic creation of the alarm list under **Settings › Log file/E-mail/Events**.

Default New Device Settings

In this dialogue specify the default communication parameters for newly added devices, such as timeout values, communication attempt retries, SNMP parameters (for SNMPv1/2/3).

For devices with FTP-based firmware updates specify a default FTP login and password.

For more information about specific device settings refer to Section 7.1.

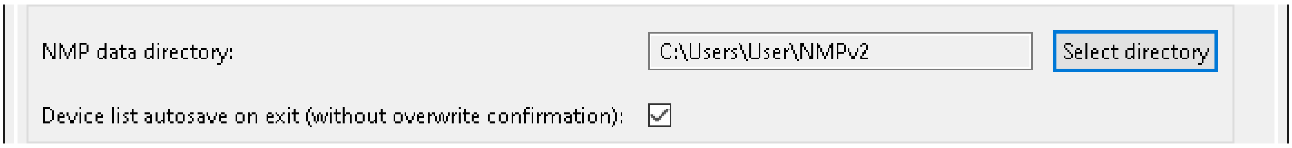
NOTE It is always possible to change the parameters for each device separately with the respective devices context menu item "Communication Parameters" (see Section 4.8).

4.4.3. Settings

NOTE Only a user with administrative rights is able to change NMP settings. A description of the sub menu items is provided in the following sections.

NMP Settings

In this dialogue specify the configuration settings for NMP application.

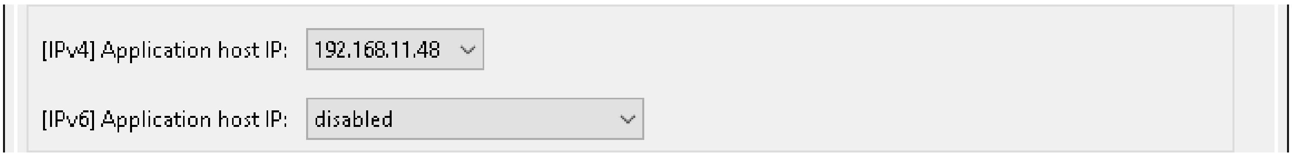


NMP data directory: C:\Users\User\NMPv2

Device list autosave on exit (without overwrite confirmation): ☑

Figure 15. NMP - Settings - Application Settings - Data Directory

- **NMP data directory:** Configure the directory where NMP saves all the configuration files. The default folder is `$USER_HOME\NMPv2`. The data folder is created at this specified location.
- **Device list autosave on exit (without overwrite confirmation):** The device list will be automatically saved on NMP exit. NMP will not prompt for confirmation.



[IPv4] Application host IP: 192.168.11.48

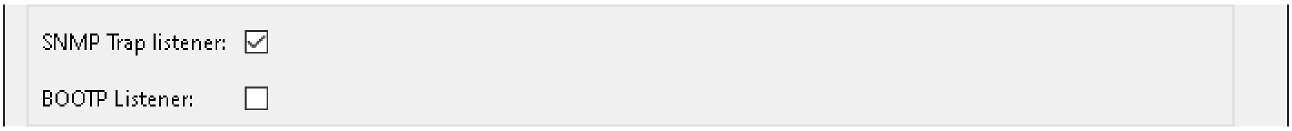
[IPv6] Application host IP: disabled

Figure 16. NMP - Settings - Application Settings - IP Settings

- **[IPv4] Application host IP:** If the NMP host system comprises more than one active IPv4 network interface card (NIC) or a number of defined interfaces then the network interface which NMP should use can be specified.

  NMP also uses this interface to:

  - Receive traps
  - Download data from devices
  - Send new configurations or update device firmware
  - Detect or scan for new devices
- **[IPv6] Application host IP:** The IPv6 address of the network interface that will be used for communication with the managed devices.

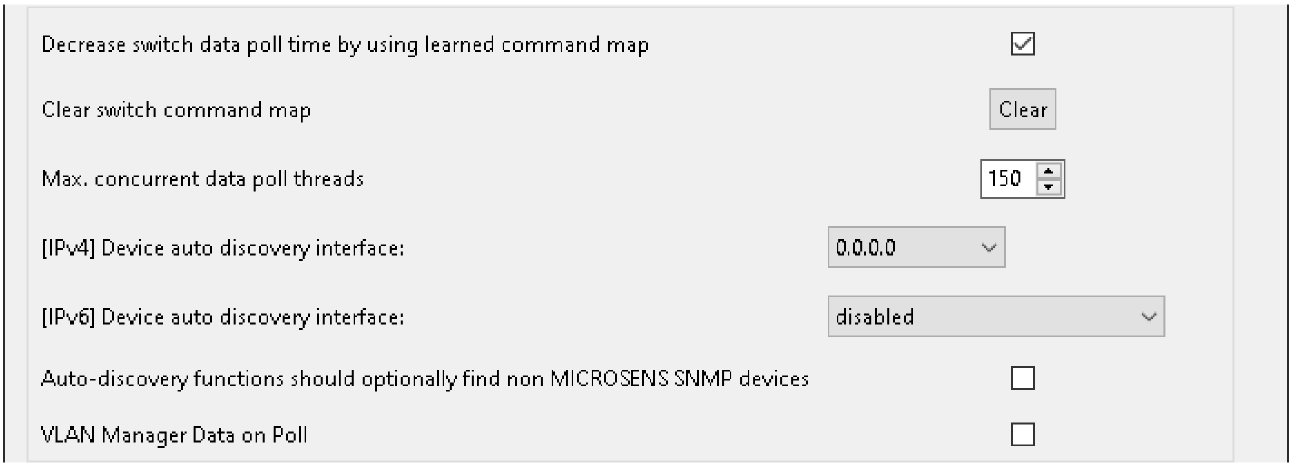


SNMP Trap listener: ☑

BOOTP Listener: □

Figure 17. NMP - Settings - Application Settings - Listeners

- **SNMP Trap listener:** NMP has a built-in SNMP trap listener to receive traps from network devices. By default, the trap listener is enabled. If a different trap receiver is already in use then it is also possible to disable this function. SNMP Trap listener uses the port `UDP 162`. NMP displays an error message during the start-up in case the port `UDP 162` is used by another SNMP trap listener or application.
- **BOOTP listener:** Activate this option to listen for BOOTP requests of MICROSENS G5 (and older) devices.



Decrease switch data poll time by using learned command map ☑

Clear switch command map

Max. concurrent data poll threads 150

[IPv4] Device auto discovery interface: 0.0.0.0

[IPv6] Device auto discovery interface: disabled

Auto-discovery functions should optionally find non MICROSENS SNMP devices ☐

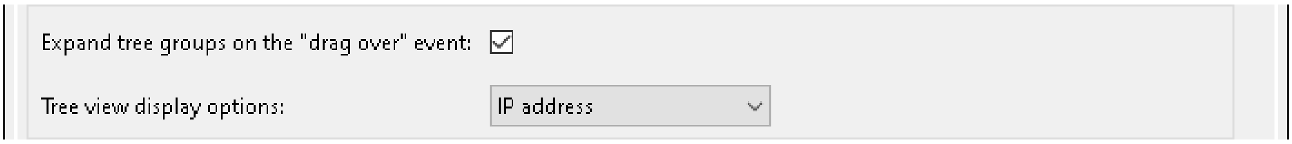
VLAN Manager Data on Poll ☐

Figure 18. NMP - Settings - Application Settings - Polling

- **Decrease switch data poll time by using learned command map:** To reduce the switch data poll time NMP uses a special command map. This feature is very useful in cases where a device does not support all the available polling features (such as RSTP). In such cases, NMP tries to load as much data as possible (included non-implemented/accessible). With this option enabled, NMP loads data that is available. The command map is created during the first device data poll. The map can be cleared (the map is then recreated if this option is enabled). This option works exclusively with MICROSENS switches generation 5 and older.
- **Clear switch command map:** Running this task will cause all switching device capabilities to be rediscovered. This function is useful if new devices are not discovered properly due to transmission problems.

NOTE This option works exclusively with MICROSENS switches generation 5 and older.

- **Max. concurrent data poll threads:** This parameter is used to define how many devices can be polled at one time. For slower servers, high loaded networks or slow network connections we recommend reducing this value for better performance.
- **[IPv4] Device auto discovery interface:** The IPv4 address of the network interface that will be used for detecting and communicating 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 instance.
- **[IPv6] Device auto discovery interface:** IPv6 Interface for device detection and communication: The IPv6 address of the network interface that will be used for communication with the managed devices.
- **Auto-discovery functions should optionally find non MICROSENS SNMP devices:** This parameter forces the SNMP-Auto discovery function to search for non MICROSENS devices also (see Section 7.2).
- **VLAN Manager Data on Poll:** When polling a device, VLAN manager data is received additionally.



Expand tree groups on the "drag over" event: ☑

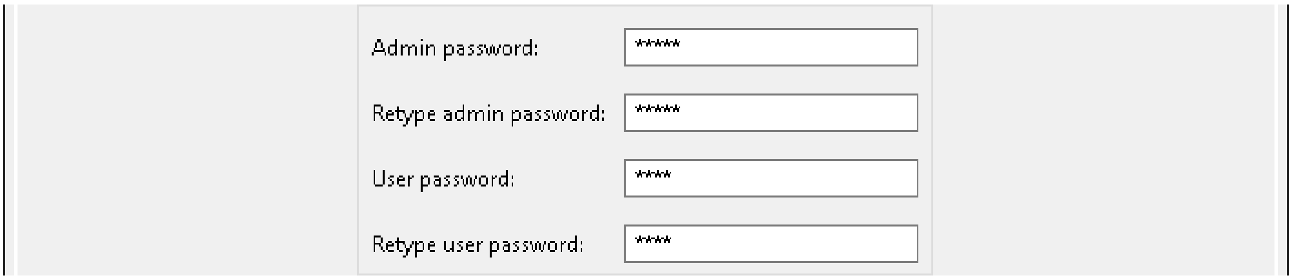
Tree view display options: IP address

Figure 19. NMP - Settings - Application Settings - Tree View Settings

- **Expand tree groups on the "drag over" event:** Expands device list tree groups during "drag & drop" operations when the mouse passes over the collapsed tree group item.
- **Tree view display options:** Configures the information shown for each device in the device list. The following options available from the drop-down list are:
  - IP address
  - Device name
  - IP address/Device name
  - Hostname
  - IP address/Hostname

Click the button `Apply` to save the respective input.

Security Settings



Admin password: ******

Retype admin password: ******

User password: ****

Retype user password: ****

Figure 20. NMP - Settings - Security Settings

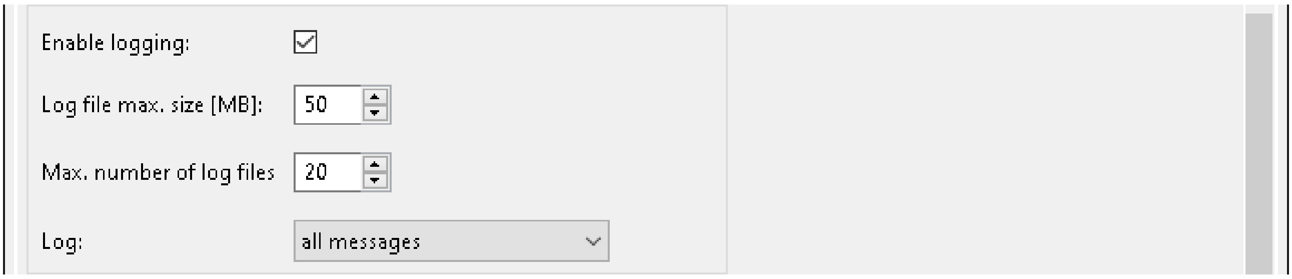
In this dialogue assign a new login name and password for the administrator and standard users to access NMP.

Click the button `Apply` to save the respective input.

NOTE For security reasons the password should be at least 8 characters long, containing a combination of letters, numbers, punctuation and symbols.

Log file/E-mail/Events

In this dialogue specify the log file handling, the e-mail configuration and how NMP has to deal with events.



Enable logging: ☑

Log file max. size [MB]: 50

Max. number of log files 20

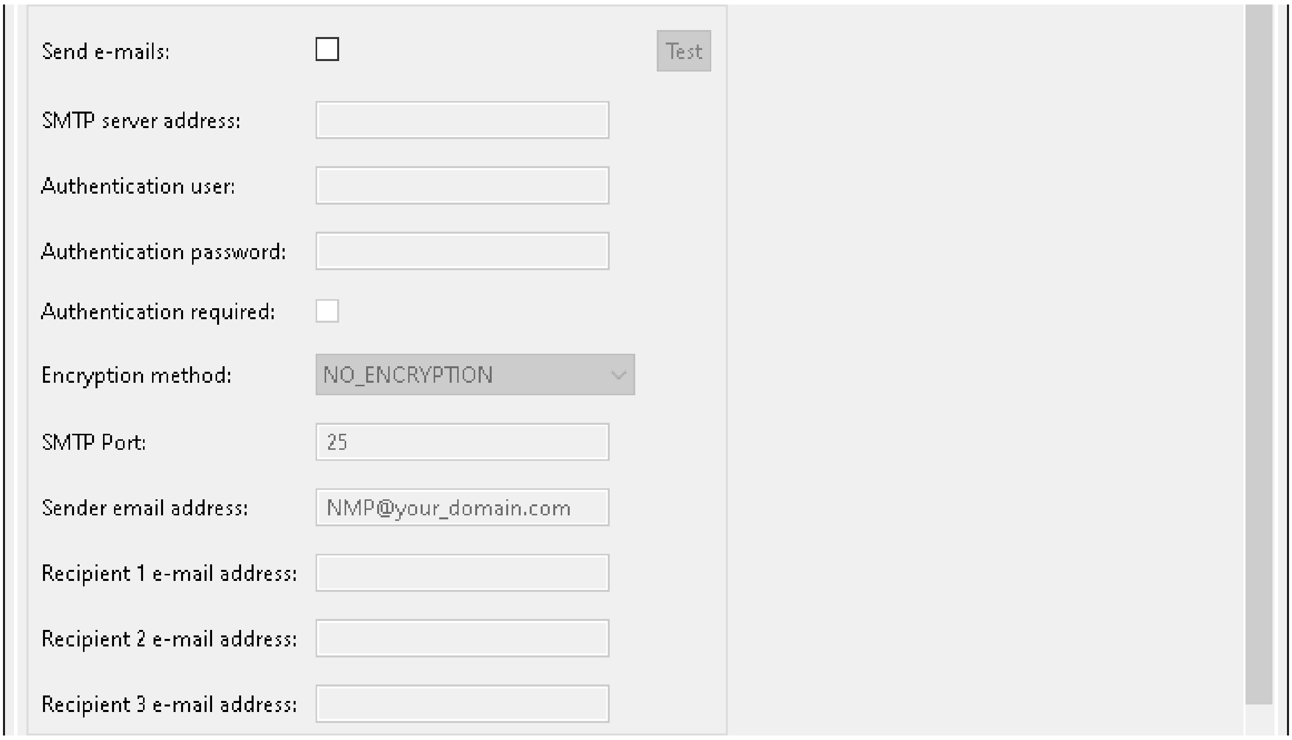
Log: all messages

Figure 21. NMP - Settings - Event Logging

- **Enable logging:** If this option is enabled, all messages displayed in the log window are written to a log file. The default file name is `messages_x.log` (x = log file number). It is automatically created in the NMP data folder. Successively older files are renamed by adding `x+0`, `x+1`, `x+2`, etc. to the base file name.
- **Log file max. size [MB]:** The maximum size of each log file in Mbytes.
- **Max. number of log files:** Specifies the maximum number of log files to be created. The maximum value is 20.

NOTE When the maximum log file size or the maximum number of log files exceeds the specified values the oldest values are overwritten and the oldest log files are deleted.

- **Log:** Specifies which information should be saved in the log file. Available options are:
  - All messages
  - Errors and SNMP traps only



Send e-mails: ☐ Test

SMTP server address:

Authentication user:

Authentication password:

Authentication required: ☐

Encryption method: NO_ENCRYPTION

SMTP Port: 25

Sender email address: NMP@your_domain.com

Recipient 1 e-mail address:

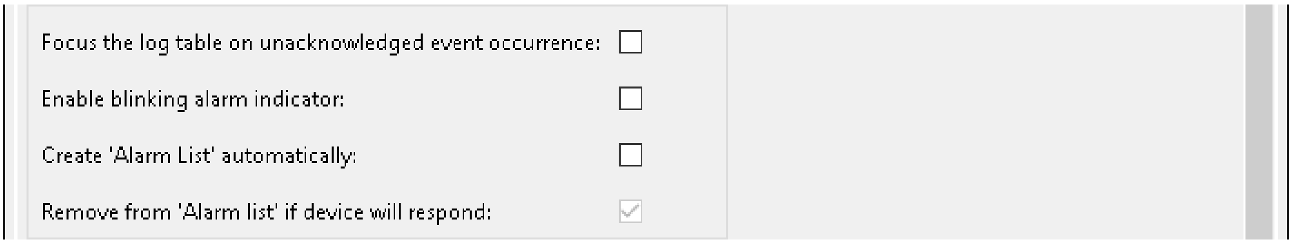
Recipient 2 e-mail address:

Recipient 3 e-mail address:

Figure 22. NMP - Settings - E-Mail Settings

- **Send e-mails:** If this option is enabled and e-mail notification is enabled for different logging options, information is forwarded by e-mail to the recipients named below. An existing e-mail account with SMTP access is required. Hit the button `Test` to verify the e-mail settings.
- **SMTP server address:** The address of the outgoing SMTP server (e.g. `smtp.<provider>.com`).
- **Authentication user and password:** User name and password for the mail account.
- **Authentication required:** Check if the SMTP server requires user authentication.
- **Encryption method:** Encryption used by the SMTP server. The following options are available from the drop-down list:
  - NO_ENCRYPTION
  - SSL
  - TLS

  NOTE NMP only supports TLS 1.2 and newer.
- **SMTP Port:** SMTP server port
- **Sender email address:** E-mail address used in "From" field of the sent message.
- **Recipient <no.> email address:** Up to 3 additional e-mail addresses



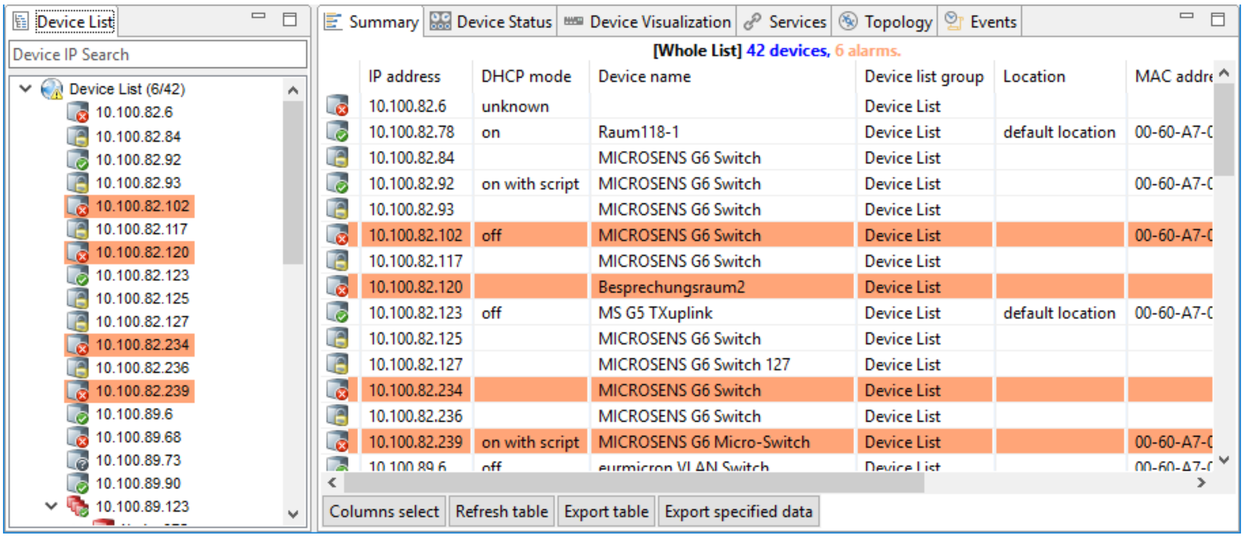
Focus the log table on unacknowledged event occurrence: □
Enable blinking alarm indicator: □
Create 'Alarm List' automatically: □
Remove from 'Alarm list' if device will respond: ☑

Figure 23. NMP - Settings - Alarm Indicators

Alarm indicators are used to notify the user about important events, such as SNMP traps or "device unavailable" errors which require network administrator attention.

- **Focus the log table on unacknowledged event occurrence:** When the new unacknowledged alarm message will be generated, the log table mask (or unpinned log window) will be automatically focused and brought to the front.

  NOTE For more information about pinned and unpinned windows please refer to Section 4.7.
- **Enable blinking alarm indicator:** Devices which have generated a new alarm will blink red in the NMP device tree list and device statistics table (see Figure 24).



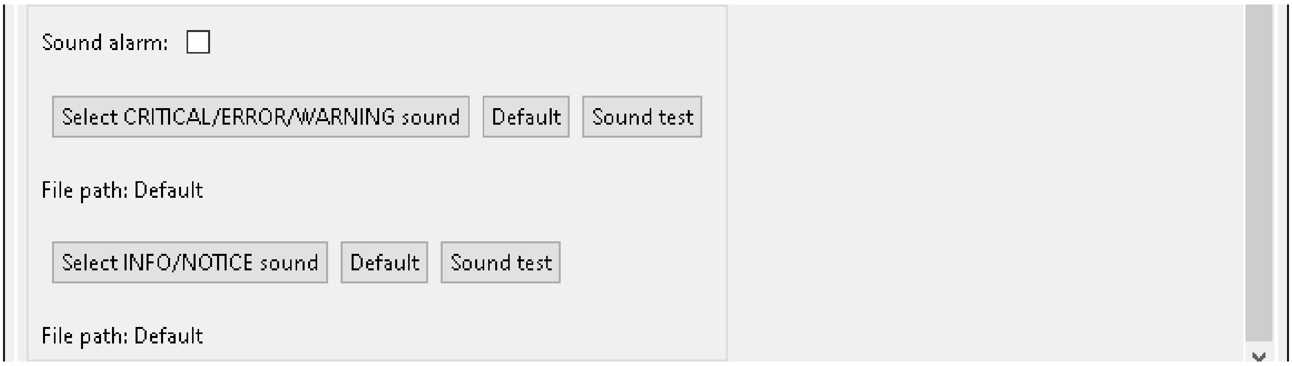
[Whole List] 42 devices, 6 alarms.

IP address	DHCP mode	Device name	Device list group	Location	MAC addre
10.100.82.6	unknown		Device List		
10.100.82.78	on	Raum118-1	Device List	default location	00-60-A7-(
10.100.82.84		MICROSENS G6 Switch	Device List		
10.100.82.92	on with script	MICROSENS G6 Switch	Device List		00-60-A7-(
10.100.82.93		MICROSENS G6 Switch	Device List		
10.100.82.102	off	MICROSENS G6 Switch	Device List		00-60-A7-(
10.100.82.117		MICROSENS G6 Switch	Device List		
10.100.82.120		Besprechungsraum2	Device List		
10.100.82.123	off	MS G5 TXuplink	Device List	default location	00-60-A7-(
10.100.82.125		MICROSENS G6 Switch	Device List		
10.100.82.127		MICROSENS G6 Switch 127	Device List		
10.100.82.234		MICROSENS G6 Switch	Device List		
10.100.82.236		MICROSENS G6 Switch	Device List		
10.100.82.239	on with script	MICROSENS G6 Micro-Switch	Device List		00-60-A7-(
10.100.89.6	off	eurmicron VLAN Switch	Device List		00-60-A7-(

Figure 24. NMP Professional - Settings - Alarm Indicator (Example)

The alarm blinks until the user acknowledges it by selecting the device in the tree or statistics table. Alarms do not blink for devices with global alarm enabled.

- **Create 'Alarm List' automatically:** All devices with alarms are automatically copied into the "Alarm List" group. The "Alarm List" group is created if it does not already exist.
- **Remove from 'Alarm List' if device responds:** Devices for which an alarm was generated and which have become available again are automatically removed from the "Alarm List" group.



Sound alarm: □

File path: Default

File path: Default

Figure 25. NMP - Settings - Sound Alarm

- **Sound alarm:** A sound will be played for alarms if this option is enabled. Different sounds are defined for critical/error/warning and info/notice event types. Specify own sounds by clicking on the respective button `Select` and choosing appropriate sound files from the file explorer (`*.wav` file format is accepted).

  A selected sound file can be tested with a click on the button "Sound test".

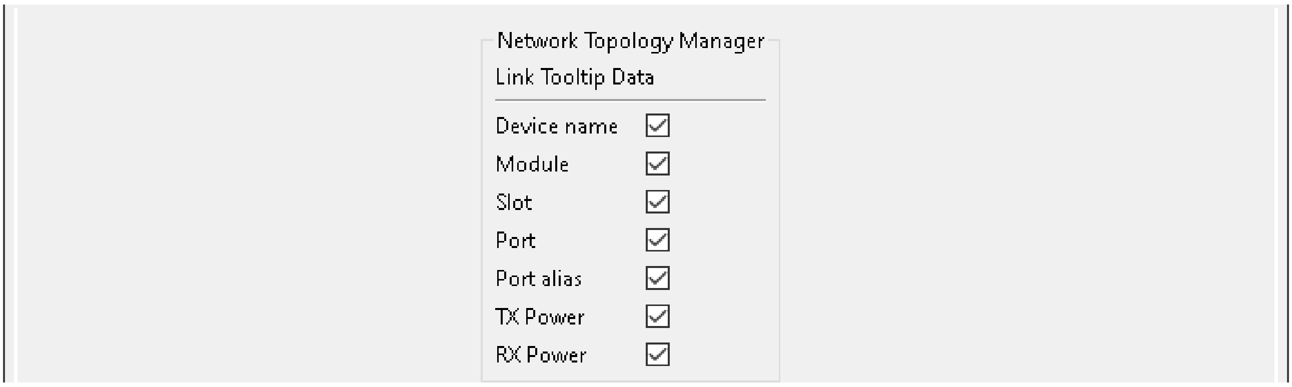
  Both alarm sounds are preset with default sounds. Hitting the button `Default` resets the respective alarm sound.

NOTE Please keep in mind that a sound card is required and speakers must be connected to the end user's client computer.

Click the button `Apply` to save the respective input.

Misc

In this dialogue specify the link tooltip data of the topology manager (see Section 7.11).



Network Topology Manager

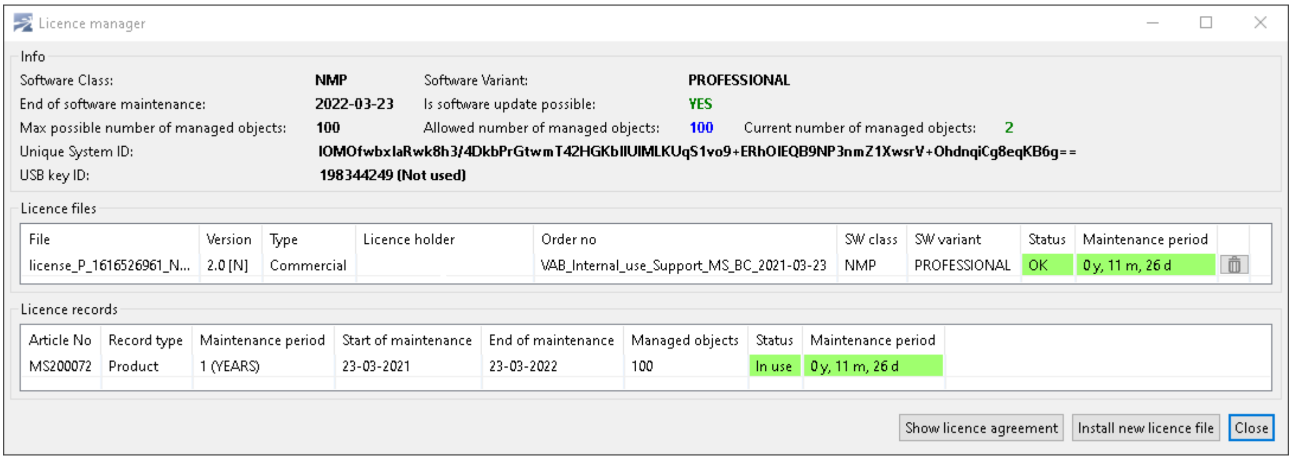
Link Tooltip Data

- Device name ☑
- Module ☑
- Slot ☑
- Port ☑
- Port alias ☑
- TX Power ☑
- RX Power ☑

Figure 26. NMP - Settings - Misc

Check or uncheck the data to enable or disable the respective tooltip information.

Licence info



Info

Software Class: **NMP** Software Variant: **PROFESSIONAL**

End of software maintenance: **2022-03-23** Is software update possible: **YES**

Max possible number of managed objects: **100** Allowed number of managed objects: **100** Current number of managed objects: **2**

Unique System ID: **IOMOfwbxlaRwk8h3/4DkbPrGtwmT42HGKbIlUIMLKUqS1vo9+ERhOIEQB9NP3nmZ1XwsrV+OhdnqiCg8eqKB6g==**

USB key ID: **198344249 (Not used)**

Licence files

File	Version	Type	Licence holder	Order no	SW class	SW variant	Status	Maintenance period
license_P_1616526961_N...	2.0 [N]	Commercial		VAB_Internal_use_Support_MS_BC_2021-03-23	NMP	PROFESSIONAL	OK	0 y, 11 m, 26 d

Licence records

Article No	Record type	Maintenance period	Start of maintenance	End of maintenance	Managed objects	Status	Maintenance period
MS200072	Product	1 (YEARS)	23-03-2021	23-03-2022	100	In use	0 y, 11 m, 26 d

Figure 27. NMP Professional - Licensing Information

This menu item opens an overview of the licensing information. The dialogue shows information e.g. about the currently installed licence key file and the entitled user. Additionally it links to the application's licence agreement.

- **Licence key files:** These are the licence key files located in the local folder `$USER_HOME/$NMP_DATA_DIR/licenses`.
- **Licence key records:** These are the licence keys included in the licence key files. One licence key file can contain one or more records with specific access rights.

Additionally this dialogue links to the application's licence agreement.

There are two options to install a new licence key file:

- A click on the button `Install new licence key file` opens the file manager. Navigate to the new licence key file to update the licence key for your application variant.
- Copy the licence key file directly into the local folder `$USER_HOME/$NMP_-DATA_DIR/licenses`.

The application scans this folder automatically to check if there are any modifications (i.e. licence key installed, licence key deleted).

NOTE To obtain a new application licence key file please contact MICROSENS.

License Activation Code Request

For purchasing a valid product licence key file the use of the MICROSENS Unique System ID Generator is mandatory.

For more information about using the Unique System ID Generator see Section 3.3.

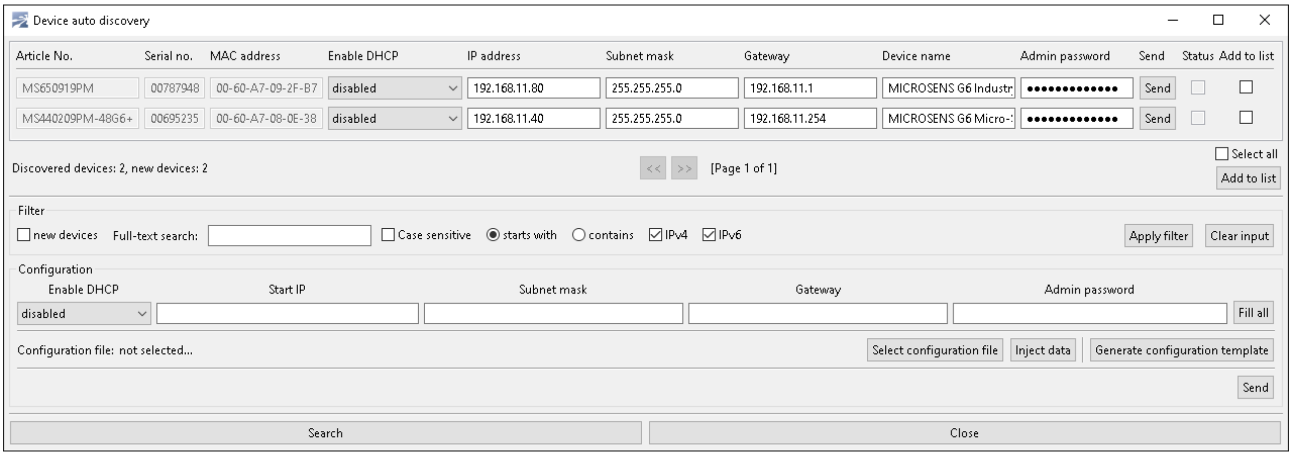
4.4.4. Discovery

Device Auto Discovery

The auto discovery features implemented in NMP allow searching for devices in the network automatically. Device lists can be generated without entering the IP address of each device.

NMP automatically creates a new group for the search results. New devices are automatically added to this group. Additionally, NMP also displays a summary of the search in the log window.

The "Switch Auto Discovery" function is a broadcast method. It detects all the devices in the current broadcast domain (i.e. the section of a network that is reachable by a network broadcast).



Device auto discovery

Article No.	Serial no.	MAC address	Enable DHCP	IP address	Subnet mask	Gateway	Device name	Admin password	Send	Status	Add to list
MS650919PM	00787948	00-60-A7-09-2F-B7	disabled	192.168.11.80	255.255.255.0	192.168.11.1	MICROSENS G6 Industr	●●●●●●●●●●●●●	Send	□	□
MS440209PM-48G6+	00695235	00-60-A7-08-0E-38	disabled	192.168.11.40	255.255.255.0	192.168.11.254	MICROSENS G6 Micro-:	●●●●●●●●●●●●●	Send	□	□

Discovered devices: 2, new devices: 2

[Page 1 of 1]

□ Select all

Filter: □ new devices Full-text search: □ Case sensitive ● starts with ○ contains ☑ IPv4 ☑ IPv6

Configuration

Enable DHCP	Start IP	Subnet mask	Gateway	Admin password
disabled				

Configuration file: not selected...

Figure 28. NMP - Device Auto Discovery

NOTE If no device is detected, the auto discovery dialogue (Figure 28) will not appear.

For more information on how to use the "Switch Auto Discovery" function, please refer to Section 7.2.

Device SNMP-based Auto Discovery (SNMP v1/v2c)

The function "Device SNMP-based Auto Discovery" allows discovering all SNMPv1/v2c capable devices in the broadcast domain (even non-MICROSENS devices) by polling newly detected devices. This function exclusively searches for SNMPv1/v2c devices with community strings matching the definitions in **Devices List › Default New Device Settings** (see section "SNMPv1/v2 Settings" in "Section 4.4.2.8).

NOTE Auto-detection of SNMPv3 devices is done via "Switch Auto Discovery" and requires the respective credentials defined under **Devices List › Default New Device Settings** (see section "SNMPv3 Settings" in Section 4.4.2.8).

The discovery window looks similar to the "Switch Auto Discovery" dialogue described above (see Figure 28). In case of SNMP-based devices, all the IP-settings input fields are disabled because configuring SNMP-based devices is not supported. This dialogue just offers adding SNMP-devices to the device list.

NOTE If no device is detected, this dialogue will not appear.

MSP 1000 platform IP discovery

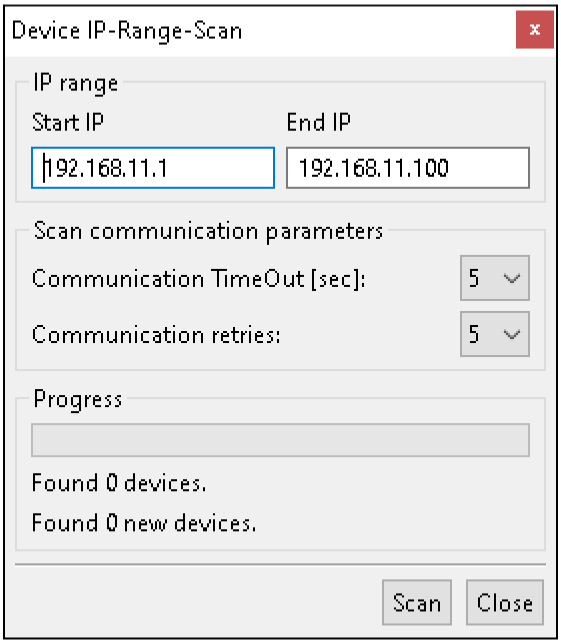
IP discovery for MSP 1000 devices allows discovering all MSP 1000 devices within a broadcast domain. All discovered devices can be added to the NMP device list.

The discovery window looks similar to the "Switch Auto Discovery" dialogue described above (see Figure 28).

In this dialogue it is possible to change the IP addresses of the discovered devices by editing the IP address text field and pressing the button `Deploy`.

NOTE | If no device is detected, this dialogue will not appear.

Device IP-Range scan


Device IP-Range-Scan

IP range

Start IP: 192.168.11.1

End IP: 192.168.11.100

Scan communication parameters

Communication TimeOut [sec]: 5

Communication retries: 5

Progress

Found 0 devices.

Found 0 new devices.

Figure 29. NMP Professional - Device IP-Range-Scan

The IP range scan method requires the following parameters to be defined in advance: * IP range with start IP and end IP * Communication parameters including timeout and retries

Device IP-Range-Scan searches for all supported devices inside the defined IP range. Community strings for the SNMP devices are defined under **Devices List › Default New Device Settings** (see section "SNMPv1/v2 Settings" in Section 4.4.2.8).

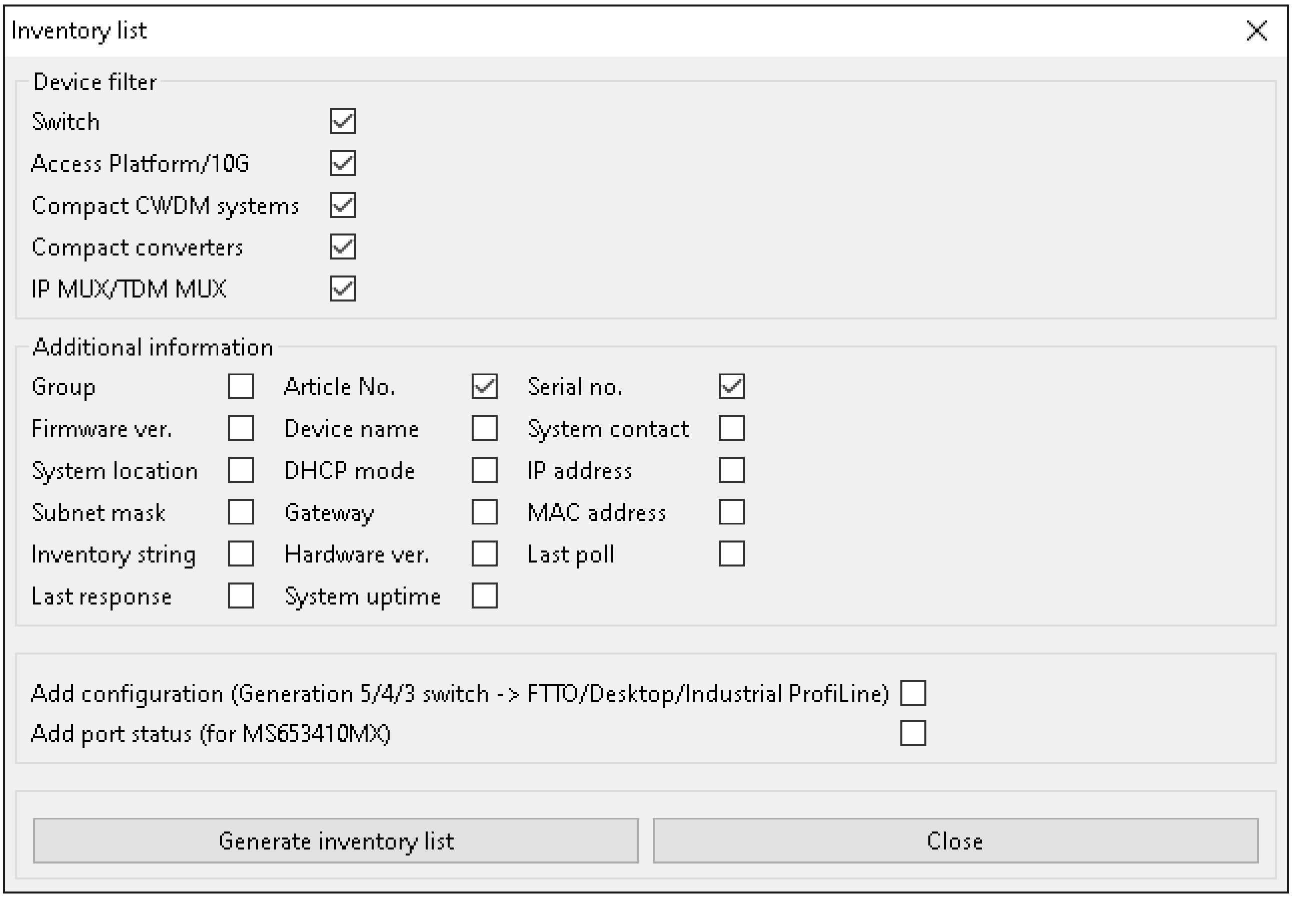
NOTE | This feature covers discovery of SNMPv1/v2c devices only. Due to the security enhancements of SNMPv3 (authentication and authorization) it is not possible to auto-discover SNMPv3 devices.

4.4.5. Tools

NOTE | Most of the tools described in this section are included with NMP Professional and the server component of NMP Enterprise. These tools are marked accordingly.

Inventory

The inventory feature allows generating an inventory list as a `.csv` file. In the respective dialogue specify the information contained in the list and which device types and their respective information will be included before generating the list.



Inventory list

Device filter

Switch ☑
Access Platform/10G ☑
Compact CWDM systems ☑
Compact converters ☑
IP MUX/TDM MUX ☑

Additional information

Group	□	Article No.	☑	Serial no.	☑
Firmware ver.	□	Device name	□	System contact	□
System location	□	DHCP mode	□	IP address	□
Subnet mask	□	Gateway	□	MAC address	□
Inventory string	□	Hardware ver.	□	Last poll	□
Last response	□	System uptime	□		

Add configuration (Generation 5/4/3 switch -> FTTO/Desktop/Industrial ProfiLine) □
Add port status (for MS653410MX) □

Figure 30. NMP - Inventory

The following options are available:

Device Filter

Different device types can be selected to become included into the inventory list:

- Switch
- Access Platform/10G
- Compact CWDM systems
- Compact converters
- IP MUX/TDM MUX

Additional Information

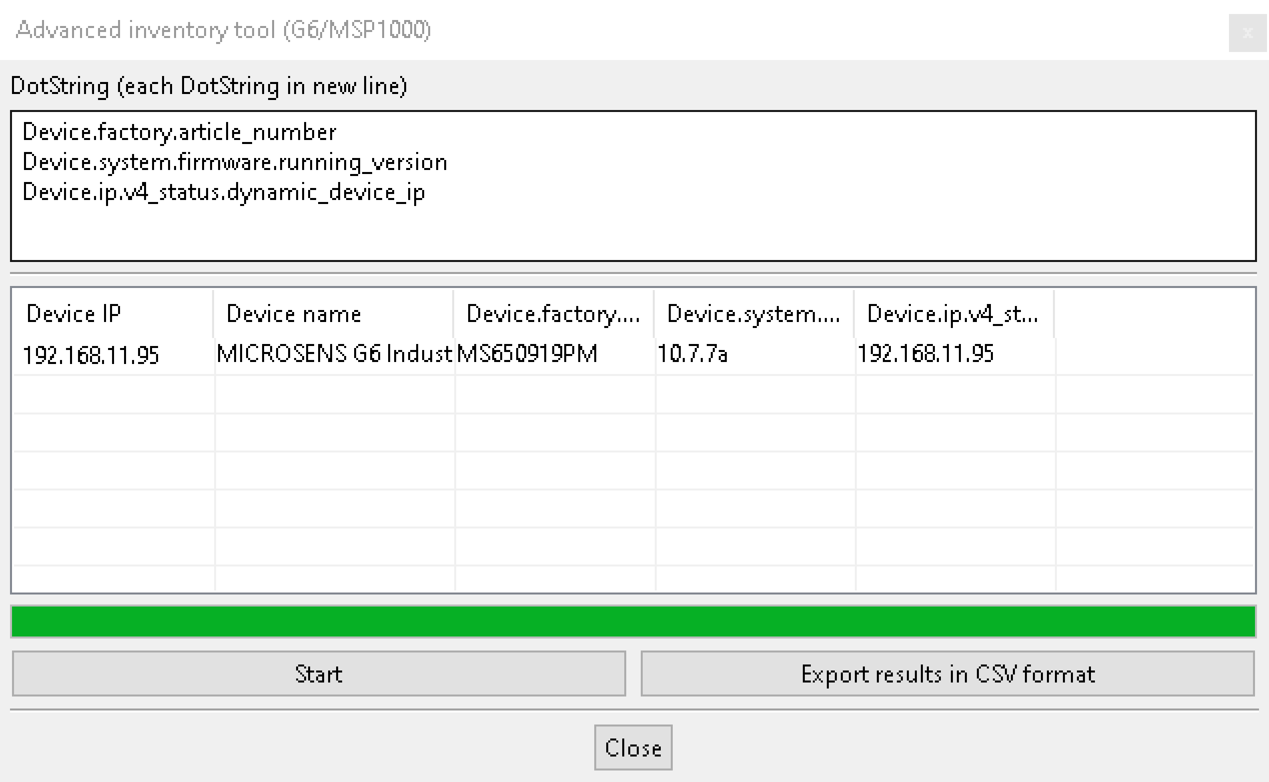
Select additional information to become included in the generated inventory list.

For Micro Switches (G5 and lower) and Industrial Switches (G5 and lower), basic configuration information can be appended to the list in addition.

If 28-port 10GBE Industrial Switches are available their port status can be appended to the list.

To import the inventory list into NMP Professional go to **File › Import CSV Device List** (see Section 4.4.1.3).

Inventory - advanced (G6/MSP1000)


Advanced inventory tool (G6/MSP1000)
x
Start
Export results in CSV format
Close

DotString (each DotString in new line)

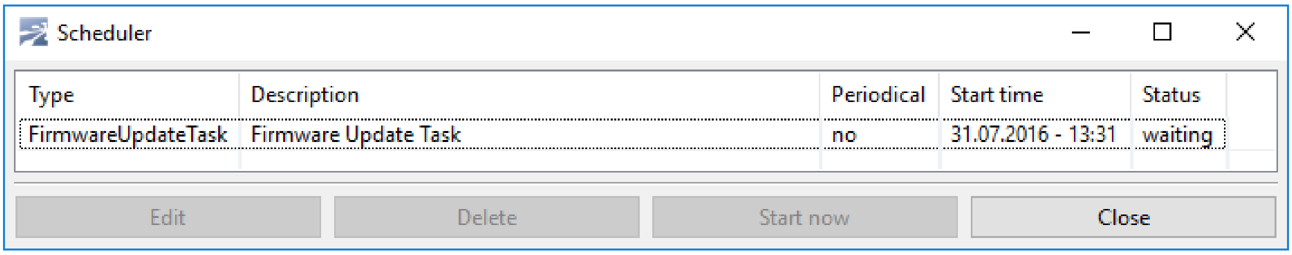
```
Device.factory.article_number
Device.system.firmware.running_version
Device.ip.v4_status.dynamic_device_ip
```

Device IP	Device name	Device.factory....	Device.system....	Device.ip.v4_st...
192.168.11.95	MICROSENS G6 Indust	MS650919PM	10.7.7a	192.168.11.95

Figure 31. NMP - Inventory advanced

The advanced inventory tool gives a quick overview of specific settings of all managed G6 and MSP1000 devices.

Scheduled tasks viewer



Type	Description	Periodical	Start time	Status
FirmwareUpdateTask	Firmware Update Task	no	31.07.2016 - 13:31	waiting

Figure 32. NMP - Scheduled Tasks Viewer

The scheduled tasks viewer dialogue is used to display planned tasks which should be performed on managed devices such as firmware updates, configuration backups and RMA IP range scans. It is possible to edit, delete or start all the tasks immediately. This tool provides information on the task name, description, start time and current status.

The tasks list is saved on NMP exit and loaded during NMP start-up.

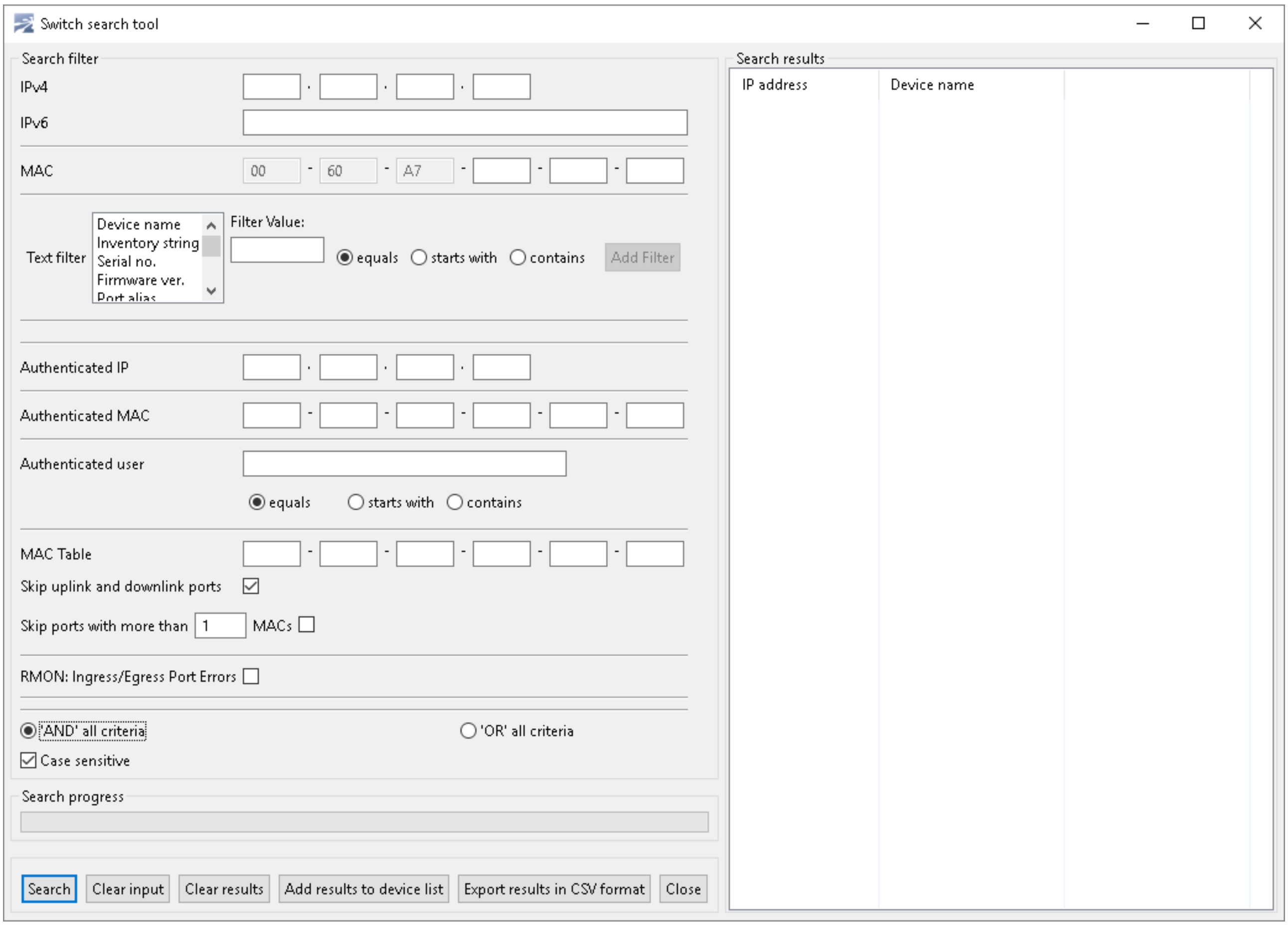
NOTE | Please keep in mind that scheduled tasks will not be started when NMP is closed.

Switch search tool

The switch search tool is a very useful feature for large networks. Thanks to this tool searching for switches in a large device list is easier and faster.

To search for a device enter some parameters such as the IP address or description and hit the button `Search`. All search results are displayed in the "Search results" table on the right hand pane. Clicking twice on any element in the table simply selects that particular device in the NMP device list tree. The tool offers the option of adding the search results as a new group in the NMP device list tree.

To export the search results into a comma-separated text file click on the button `Export results in CSV format`.



MAC 00 - 60 - A7 - - -

Text filter: ● equals

Authenticated user: ● equals

Skip uplink and downlink ports ☑

Skip ports with more than 1 MACs ☐

● 'AND' all criteria

☑ Case sensitive

Figure 33. NMP - Switch Search Tool

RMA IP Range Scanner

NOTE | "RMA" means "Return Merchandise Authorisation" and denotes the process of replacing defective devices.

The RMA scanner is used to scan a defined range of IP addresses for new devices (e.g. connected to replace identical defective devices). If any new devices are found in the defined IP range, a new group named "RMA List" and a subgroup using a range alias will automatically be created in the tree. Any devices found are placed in this group.

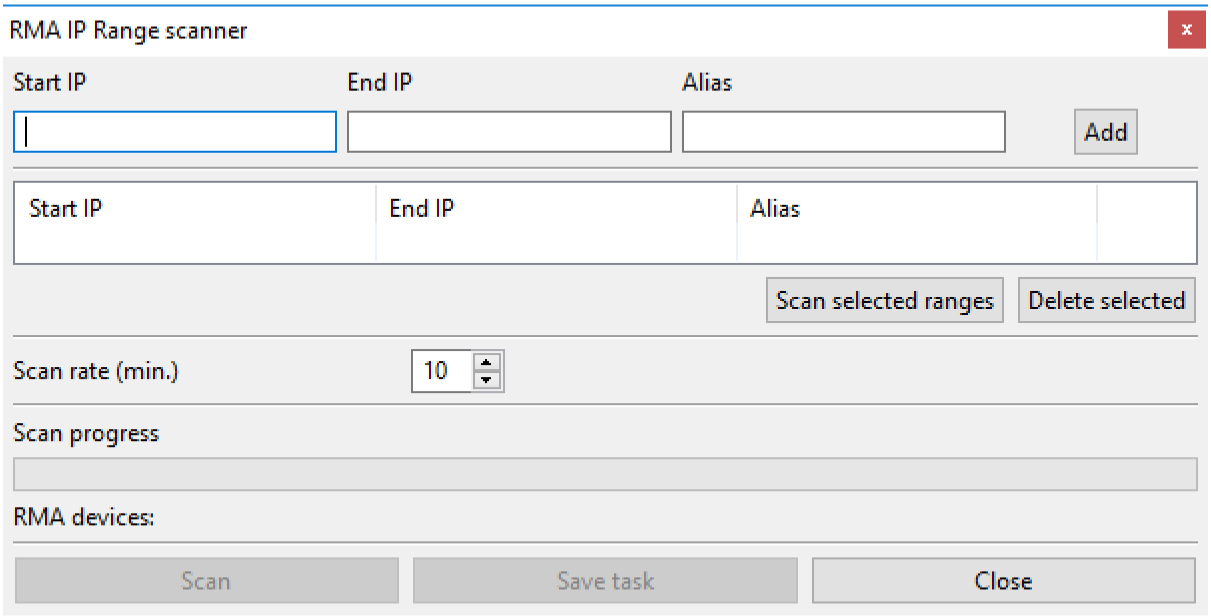


Figure 34. NMP - RMA IP Range Scanner

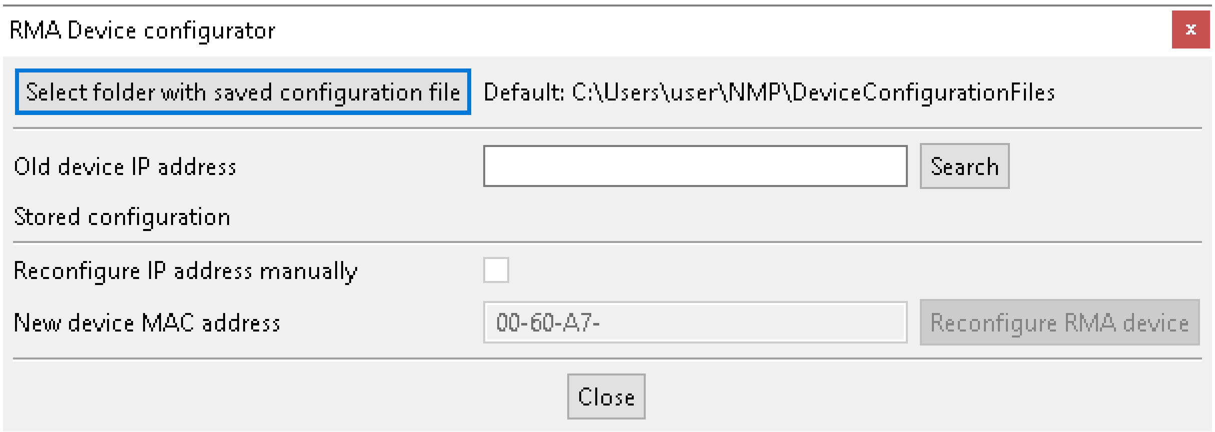
It is possible to define a number of small ranges instead of one huge range. Scanning a number of small ranges speeds up the scan process. The scan process can also be launched for a single range selected from the table.

RMA IP range scanner provides the option of scheduling the "scan task". The task is started every 10 to 120 minutes. This task can be managed under **Tools › Scheduled tasks viewer** (see Section 4.4.5.3).

RMA Device Configurator

NOTE | "RMA" means "Return Merchandise Authorisation" and denotes the process of replacing defective devices.

The "RMA Device configurator" is used to reconfigure the 'new' replacement devices (e.g. connected to replace defective devices) in the "RMA List" created by the "RMA IP range scanner".



RMA Device configurator

Select folder with saved configuration file: Default: C:\Users\user\NMP\DeviceConfigurationFiles

Old device IP address:

Stored configuration

Reconfigure IP address manually: □

New device MAC address: 00-60-A7-

Figure 35. NMP - RMA Device Configurator

To reconfigure a new device, select the folder with the saved configuration files, enter the IP address of the old (damaged) device and press the button **`Search`**. The tool then searches for the stored configuration file from the old device. If the configuration is found, the button **`Reconfigure RMA device`** and the "New device MAC address" text field are activated.

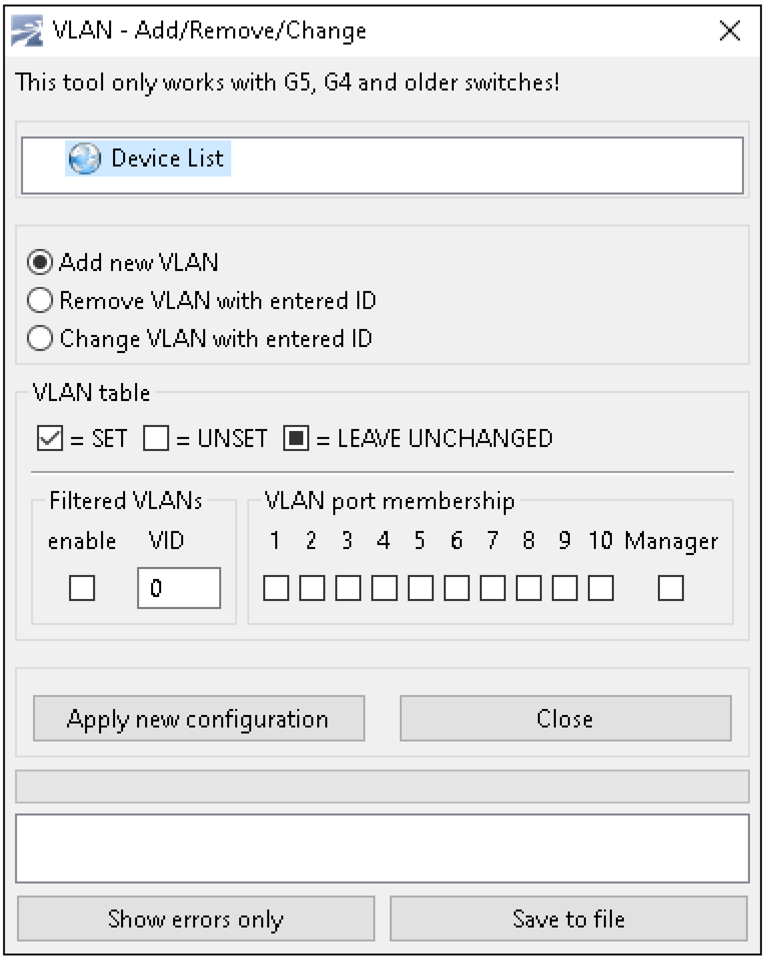
Enter the MAC address of the new device and click on the button **`Reconfigure RMA device`**. If the device is available in the "RMA List", the old device configuration (including the IP settings) is automatically transferred to the new device. The tool reports a success or failure in a message box.

NOTE The server administrator should create a scheduled task for running device configuration backups or backing up the configurations manually. It is not possible to automatically reconfigure an RMA device if the old device configuration is not available.

Switch VLAN Add/Remove/Change Tool

To add, remove or change the VLAN settings of switches in the selected group, select the respective group where to edit VLANs, select the desired operation type (add, remove or change), enter the VLAN settings and click the button **`Apply new configuration`**. Depending on the selected operation type, a VLAN will be added, removed or changed on all devices in the selected group with its respective values VLAN ID (VID) and VLAN port membership.

Log messages are displayed at the bottom of the tool window. It is possible to either display all messages or errors and then to save the log file.



This tool only works with G5, G4 and older switches!

● Add new VLAN
○ Remove VLAN with entered ID
○ Change VLAN with entered ID

☑ = SET □ = UNSET ■ = LEAVE UNCHANGED

enable	VID	1	2	3	4	5	6	7	8	9	10	Manager
□	0	□	□	□	□	□	□	□	□	□	□	□

Figure 36. NMP - VLAN Add/Remove/Change

NOTE This tool works exclusively for generation 5, 4 and older MICROSENS switches. It will not work with Micro Switches (G6 and newer) and Industrial Switches (G6 and newer)!

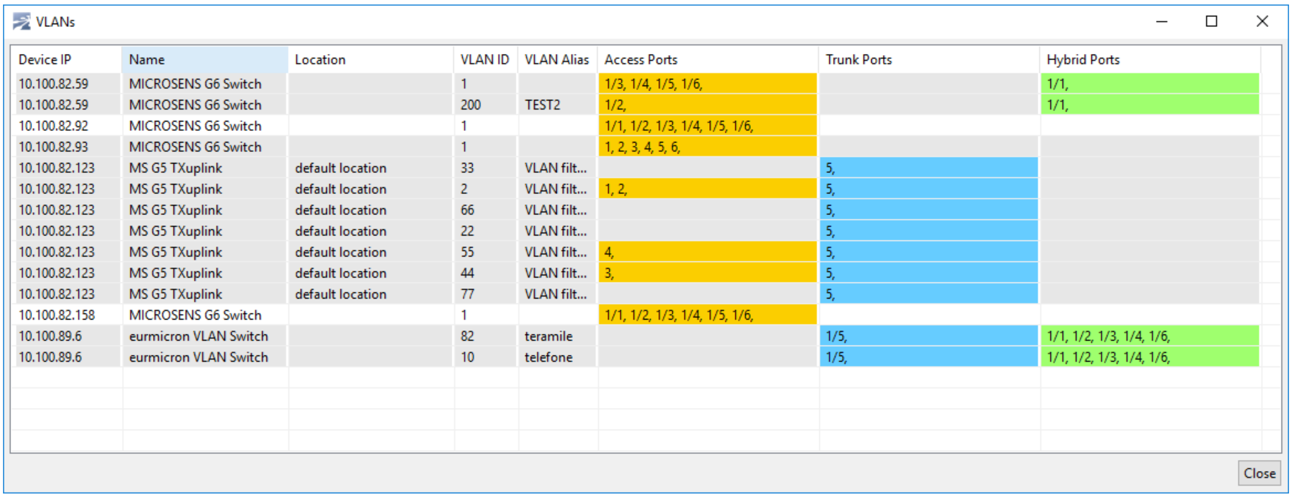
VLANs

This tool allows displaying the current VLAN configuration on all MICROSENS switches and SNMP-based devices available on the device list.

NOTE The Q-Bridge MIB enables access to non-MICROSENS devices VLAN configuration parameters via SNMP. According to this, this tool requires the Q-Bridge MIB implemented on the respective devices to work properly. For more information about Q-Bridge MIB see the respective RFC 4363.

The tool "VLANs" will scan each device from the list and create table entries for each VLAN ID (if the VLAN option is enabled). The VLANs table contains information about the device on which the VLAN is configured (IP address, device name and location) and about the configured VLAN ID.

For each configured VLAN ID, the list of member ports is created. The ports configured as "Access" are marked in orange, the trunk ports are marked in blue and the hybrid ports are marked in green.

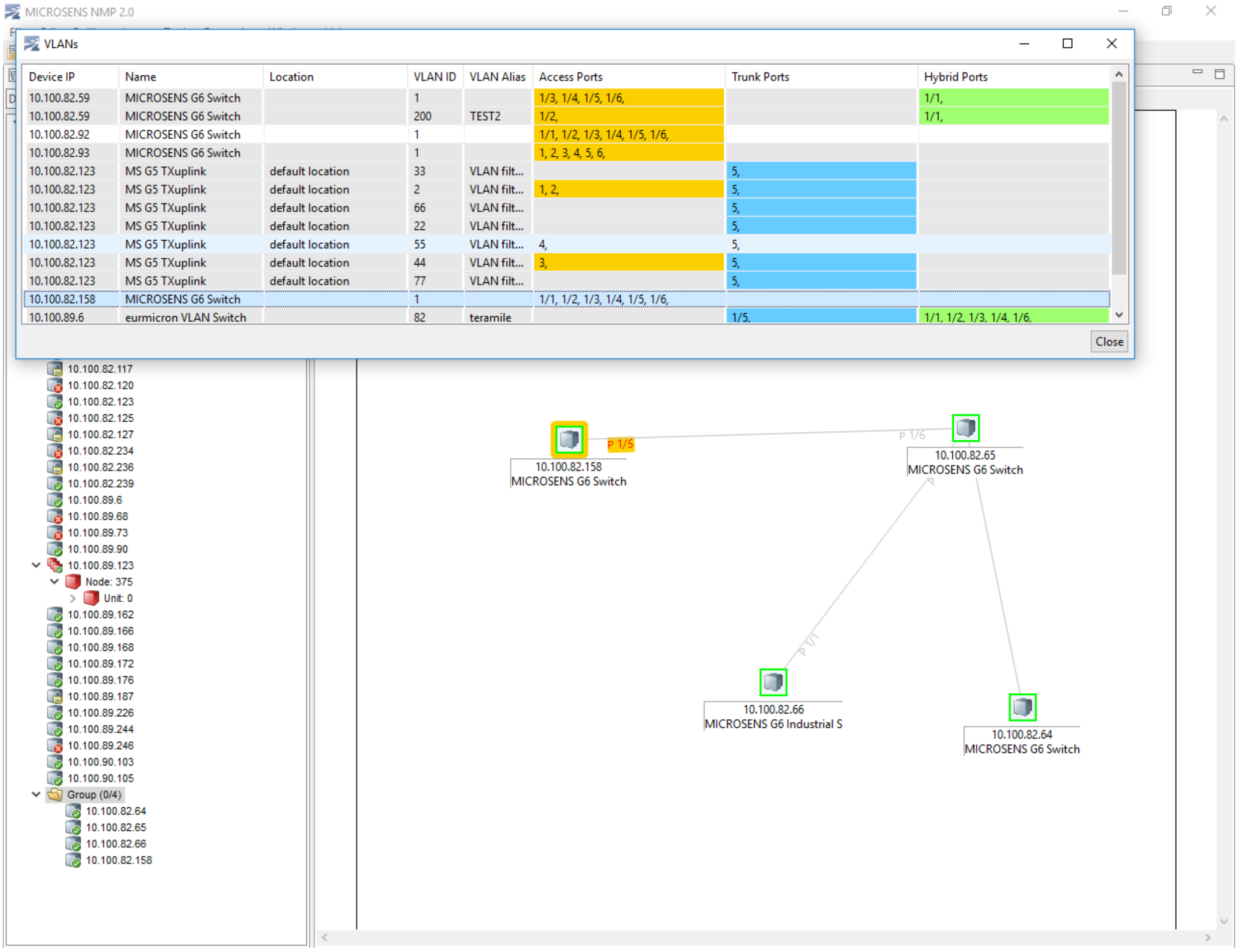


Device IP	Name	Location	VLAN ID	VLAN Alias	Access Ports	Trunk Ports	Hybrid Ports
10.100.82.59	MICROSENS G6 Switch		1		1/3, 1/4, 1/5, 1/6,		1/1,
10.100.82.59	MICROSENS G6 Switch		200	TEST2	1/2,		1/1,
10.100.82.92	MICROSENS G6 Switch		1		1/1, 1/2, 1/3, 1/4, 1/5, 1/6,		
10.100.82.93	MICROSENS G6 Switch		1		1, 2, 3, 4, 5, 6,		
10.100.82.123	MS G5 TXuplink	default location	33	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	2	VLAN filt...	1, 2,	5,	
10.100.82.123	MS G5 TXuplink	default location	66	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	22	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	55	VLAN filt...	4,	5,	
10.100.82.123	MS G5 TXuplink	default location	44	VLAN filt...	3,	5,	
10.100.82.123	MS G5 TXuplink	default location	77	VLAN filt...		5,	
10.100.82.158	MICROSENS G6 Switch		1		1/1, 1/2, 1/3, 1/4, 1/5, 1/6,		
10.100.89.6	eurmicron VLAN Switch		82	teramile		1/5,	1/1, 1/2, 1/3, 1/4, 1/6,
10.100.89.6	eurmicron VLAN Switch		10	telefone		1/5,	1/1, 1/2, 1/3, 1/4, 1/6,

Figure 37. NMP - VLANs (Example)

"VLANs" allows checking easily which VLANs are in use on which devices and which ports of which switches are assigned to particular VLANs.

"VLANs" tool in combination with "Topology Manager" (see Section 4.7.5) helps to track the current VLAN configuration at the network: When the topology view is opened, select any entry at the VLANs table and the selected VLAN will be presented on the topology.



MICROSENS NMP 2.0

VLANs

Device IP	Name	Location	VLAN ID	VLAN Alias	Access Ports	Trunk Ports	Hybrid Ports
10.100.82.59	MICROSENS G6 Switch		1		1/3, 1/4, 1/5, 1/6,		1/1,
10.100.82.59	MICROSENS G6 Switch		200	TEST2	1/2,		1/1,
10.100.82.92	MICROSENS G6 Switch		1		1/1, 1/2, 1/3, 1/4, 1/5, 1/6,		
10.100.82.93	MICROSENS G6 Switch		1		1, 2, 3, 4, 5, 6,		
10.100.82.123	MS G5 TXuplink	default location	33	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	2	VLAN filt...	1, 2,	5,	
10.100.82.123	MS G5 TXuplink	default location	66	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	22	VLAN filt...		5,	
10.100.82.123	MS G5 TXuplink	default location	55	VLAN filt...	4,	5,	
10.100.82.123	MS G5 TXuplink	default location	44	VLAN filt...	3,	5,	
10.100.82.123	MS G5 TXuplink	default location	77	VLAN filt...		5,	
10.100.82.158	MICROSENS G6 Switch		1		1/1, 1/2, 1/3, 1/4, 1/5, 1/6,		
10.100.89.6	eurmicron VLAN Switch		82	teramile		1/5,	1/1, 1/2, 1/3, 1/4, 1/6,

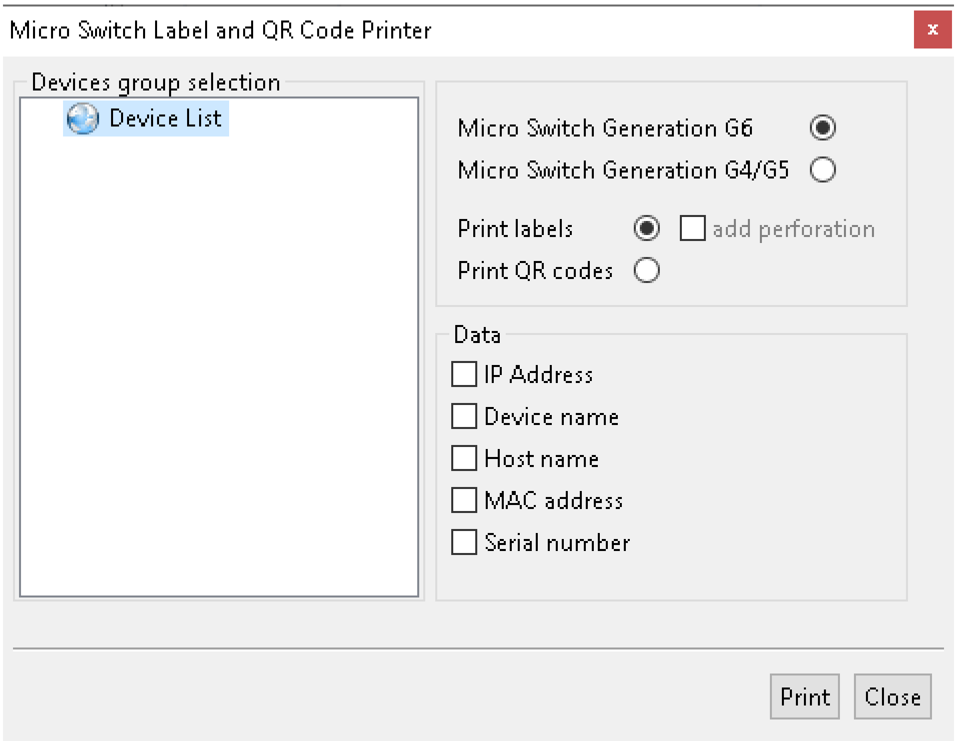
10.100.82.117
10.100.82.120
10.100.82.123
10.100.82.125
10.100.82.127
10.100.82.234
10.100.82.236
10.100.82.239
10.100.89.6
10.100.89.68
10.100.89.73
10.100.89.90
10.100.89.123
Node: 375
Unit: 0
10.100.89.162
10.100.89.166
10.100.89.168
10.100.89.172
10.100.89.176
10.100.89.187
10.100.89.226
10.100.89.244
10.100.89.246
10.100.90.103
10.100.90.105
Group (0/4)
10.100.82.64
10.100.82.65
10.100.82.66
10.100.82.158

Figure 38. NMP - VLANS tool with Topology Manager

In the example (Figure 38) the device with IP address 10.100.82.158 and VLAN with ID 1 is selected at the VLANs table. The same device is marked in the Topology Manager in orange, because the VLAN ID 1 is configured on this device and is connected via port 1/5 (also marked with orange in topology overview), which is an "ACCESS" port. The colours used in the VLANs table to mark different VLAN modes (access, trunk, hybrid) are also used in the topology overview.

Micro Switch Label and QR Code Printer

Use this feature to print housing labels for all devices contained in a device group.



Micro Switch Label and QR Code Printer

Devices group selection

Device List

Micro Switch Generation G6 ●
Micro Switch Generation G4/G5 ○

Print labels ● □ add perforation
Print QR codes ○

Data

□ IP Address
□ Device name
□ Host name
□ MAC address
□ Serial number

Figure 39. NMP - Micro Switch Label and QR Code Printer

- **Devices Group Selection:** Select the respective device group which devices data should be printed on a label (with descriptive content or as QR code).

NOTE If you want to print labels only for specific devices, create a new group and move those devices into this group. Then select this group in this dialogue. After successfully printed the label, remove the devices from this group.

- **Micro Switch Generation G6:** Check this option to select all G6 switches of this group.
- **Micro Switch Generation G4/G5:** Check this option to select all G4/G5 switches of this group.

NOTE If the selected group does not contain a specific G6, G5 or G4 switch, NMP will show a respective warning dialogue.

- **Print labels:** Check this option to print descriptive labels.
- **Add perforation:** Select this option if the labels should contain a perforation print.
- **Print QR codes:** Check this option to print non-descriptive QR code labels.
- **Data:** Select the data to print on the label. Due to the limited content capacity of the label the selection is limited to three data items.

Save Selected Device as NMP Virtual Device Image

NOTE | This feature is exclusively available for MICROSENS G5 and newer switches.

This debug option allows saving a device image as `.dimg` file. In case of occurring problems, a device image can be sent to MICROSENS for debugging. Device images contain the current device status and device configuration.

NOTE | The snapshot contains all passwords encrypted for security reasons.

4.4.6. Edit

Copy (Ctrl+C)

Makes a copy of the selected item(s). It is possible to select one or more (with button `Ctrl` pressed) devices in the tree. Then select the **Copy** menu item. To insert a copy of the item use the related **Paste** menu item.

Cut (Ctrl+X)

Use this to move the selected devices from one group to another. Select one or more (with Ctrl key pressed) devices in the tree. Then select the **Cut** menu option. Now select the destination group in the tree and select the **Paste** menu option. The selected devices are moved to the selected group.

Devices which have been cut out are stored in NMP’s paste buffer. The paste buffer will be overwritten if the **Cut** function is used again.

Paste (Ctrl+V)

Pastes copied or cut out devices to the selected group. If no group is selected the devices are pasted to the main group (tree root).

Delete (Del)

Removes selected devices or groups from the device list.

- Selected device within a device list: The menu item removes the respective device from the device list. The affected group remains otherwise unchanged.
- Selected group in the device list tree: The menu item removes the respective group from the device list tree.

NOTE | Deleting a group removes all included devices of this group without requesting confirmation!

The use of the button `Del` on the keyboard or **Delete device** resp. **Delete group** from the tree context menu (by right mouse clicking on the device/group) is also possible. The dialogue prompts to confirm the deletion before the task is completed.

4.4.7. Window

This menu contains options to change the layout and appearance of the main application window.

Show View

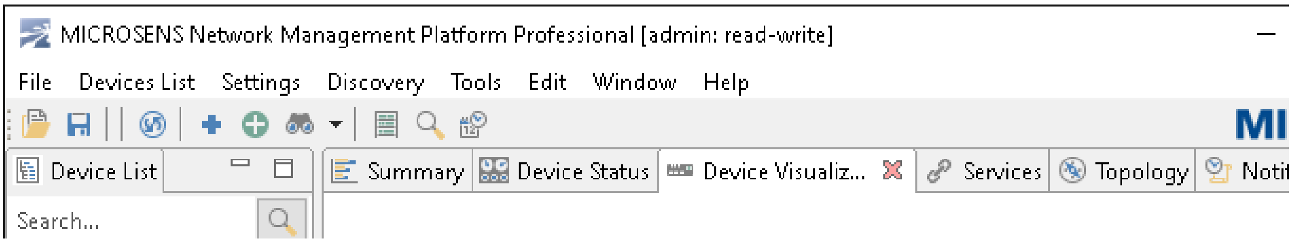


Figure 40. NMP - Tabbed Data Panel - Close Icon

NMP allows closing some of the tabbed data panels by selecting the [X] icon next to the panel name.

The closed elements can be restored by using the **Show view** menu. Currently, NMP allows closing and restoring the following views:

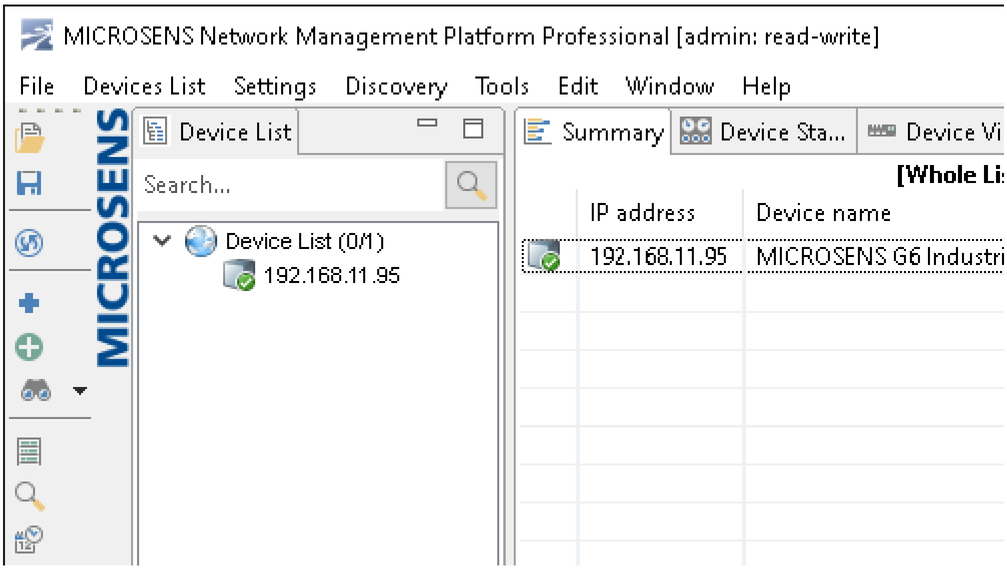
- Device visualization
- Services
- Topology

When the panel is not closed but in the background, NMP will bring it to top.

Toolbar Position

You can select the position for the main menu toolbar. The following options are possible:

- Top
- Left
- Bottom



IP address	Device name
192.168.11.95	MICROSENS G6 Industri

Figure 41. NMP - Toolbar Position Left

Toolbar Icon Size

You can choose the size for toolbar icons size. The following options are possible:

- 16x16
- 32x32

Language

Here you can chose NMP’s user interface language. The following options are possible:

- English
- German
- Polish

4.4.8. Help

This menu contains the linked NMP manuals in different languages and information about the NMP product variant.

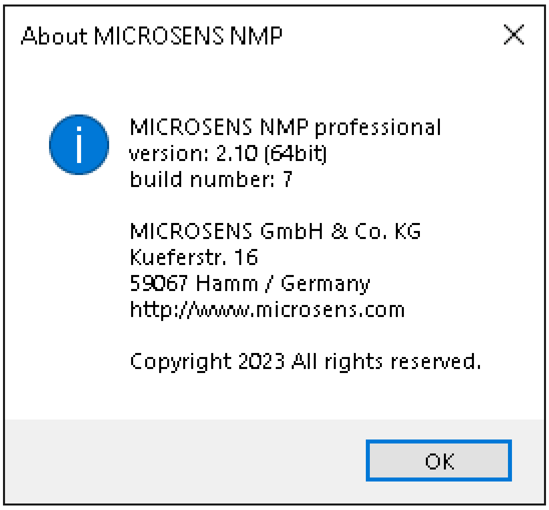
Manual

This is the link to the NMP manuals. The manuals are provided in form of PDF files and are available in the following languages:

- English

About

This dialogue shows information on the application and its version.



MICROSENS NMP professional
version: 2.10 (64bit)
build number: 7

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm / Germany
http://www.microsens.com

Copyright 2023 All rights reserved.

Figure 42. NMP - Main Menu - Help

4.5. Main Menu Toolbar

The main menu toolbar provides quick access to the most important and most used commands.

Icon	Task	Main Menu Item / Detailed Information
📂	Load device list	**File › Open**
💾	Save device list	**File › Save**
🔄	Refresh selected devices	**Device List › Refresh selected**
➕	Add new device	**Device List › Add new device**
⊕	Add new subgroup	**Device List › Add new subgroup**
🔭	Device auto discovery	**Discovery**
▤	Create Inventory List	**Tools › Inventory**
🔍	Device search tool	**Tools › Switch search tool**
📅	Scheduled tasks viewer	**Tools › Scheduled tasks viewer**

NOTE You can configure the position and icon size of the toolbar icons in the main menu under **Window › Toolbar Position** and **Window › Toolbar Icon Size**.

4.6. Device List Tree View

The left hand pane of the main window displays the device list as a tree which is a graphic representation of the device list. Devices can be assigned to different groups. The "global network" icon in the tree list is destined to be assigned to the "project group" on top of the tree view. Subgroups are easily added to this main project group.

Special groups, such as the "Alarm List", are created automatically by NMP as tree root groups.

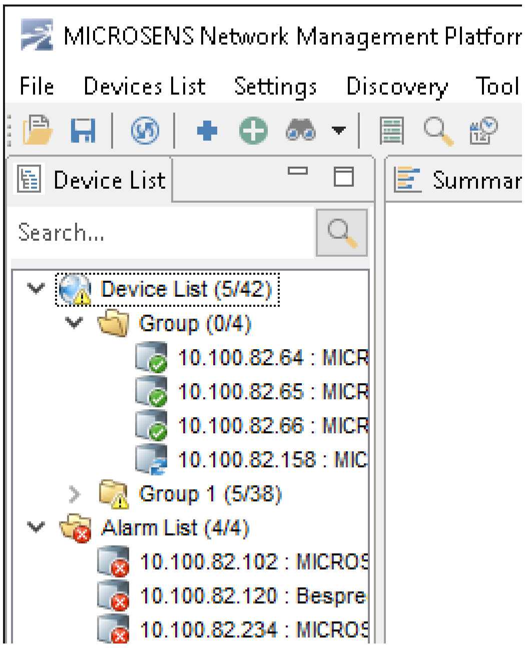


Figure 43. NMP - Device List Tree View

The number of groups and subgroups is not limited. Group names do not have to be unique.

Within the tree, devices are represented by an icon and a text identifier. Configure NMP to display the device’s IP address, device description or both next to the device icon.

Searching for list entries is possible by using an IP address or the device, host or group name (containing the search string).

It is possible to navigate through the device list using the cursor keys:

- up/down: go to the previous/next list entry (group, subgroup or device)
- left:
  - with selected device: jump to the superordinate group or subgroup
  - with selected group or subgroup: collapse group or subgroup and jump to the superordinate group or subgroup
- right: expand selected group or subgroup and jump to the first list entry

There are different icon types representing different device states:

Icon	Meaning
▣	Newly added device
?	Checking device status
⟳	Loading data from device
✓	Device available, data successfully loaded
✗	Device is not responding (not available) or data loading failed
➜	Uploading new firmware file to the device
⚙	Resetting device after firmware update
⚠	Device ring error (for switches with ring support) or user-defined alarm
✓✗	Device with acknowledged alarm
🔒	Device available, problem with authorization
▣▣	Stacked device (e.g. MSP1000)

Select a device by clicking with the mouse on its icon or by using the up/down arrow keys.

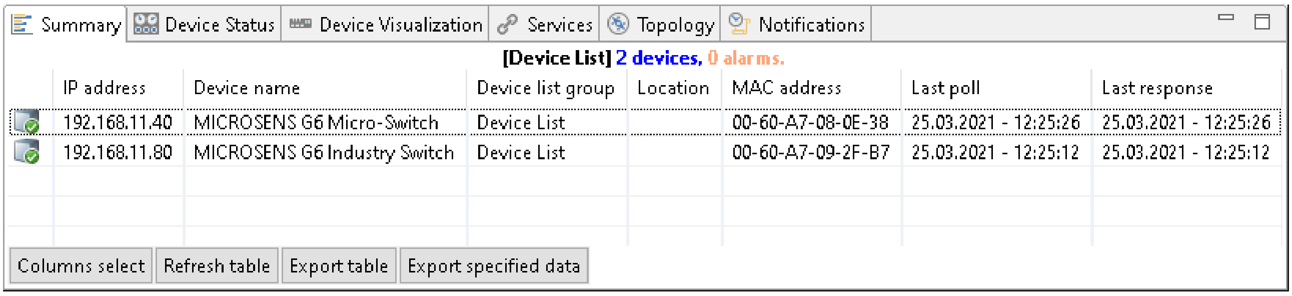
Devices can be moved to other groups. To move one or more devices between groups, use the mouse and the Drag & Drop function. Simply select a device with the mouse and drag and drop it onto the new group icon. To move several devices, select them with the mouse whilst pressing the button `Ctrl`. It is possible to drag and drop whole groups.

To edit the device list use "Copy & Paste" operation (the keys `Ctrl`+`C` and `Ctrl`+`V` on the keyboard) to create device copies or the "Cut & Paste" operation to move devices or groups (the keys `Ctrl`+`X` and `Ctrl`+`V` on the keyboard).

The device IP search field, located at the top of the device list tree view, can be used for searching the devices by well-known IP address. If NMP recognises the device within the device list, this device will be automatically selected at the tree.

4.7. Tabbed Data Panel

The tabbed data panel consists of tabs with information about the device list, the currently selected device, the topology and the log window.



[Device List] 2 devices, 0 alarms.

	IP address	Device name	Device list group	Location	MAC address	Last poll	Last response
✓	192.168.11.40	MICROSENS G6 Micro-Switch	Device List		00-60-A7-08-0E-38	25.03.2021 - 12:25:26	25.03.2021 - 12:25:26
✓	192.168.11.80	MICROSENS G6 Industry Switch	Device List		00-60-A7-09-2F-B7	25.03.2021 - 12:25:12	25.03.2021 - 12:25:12

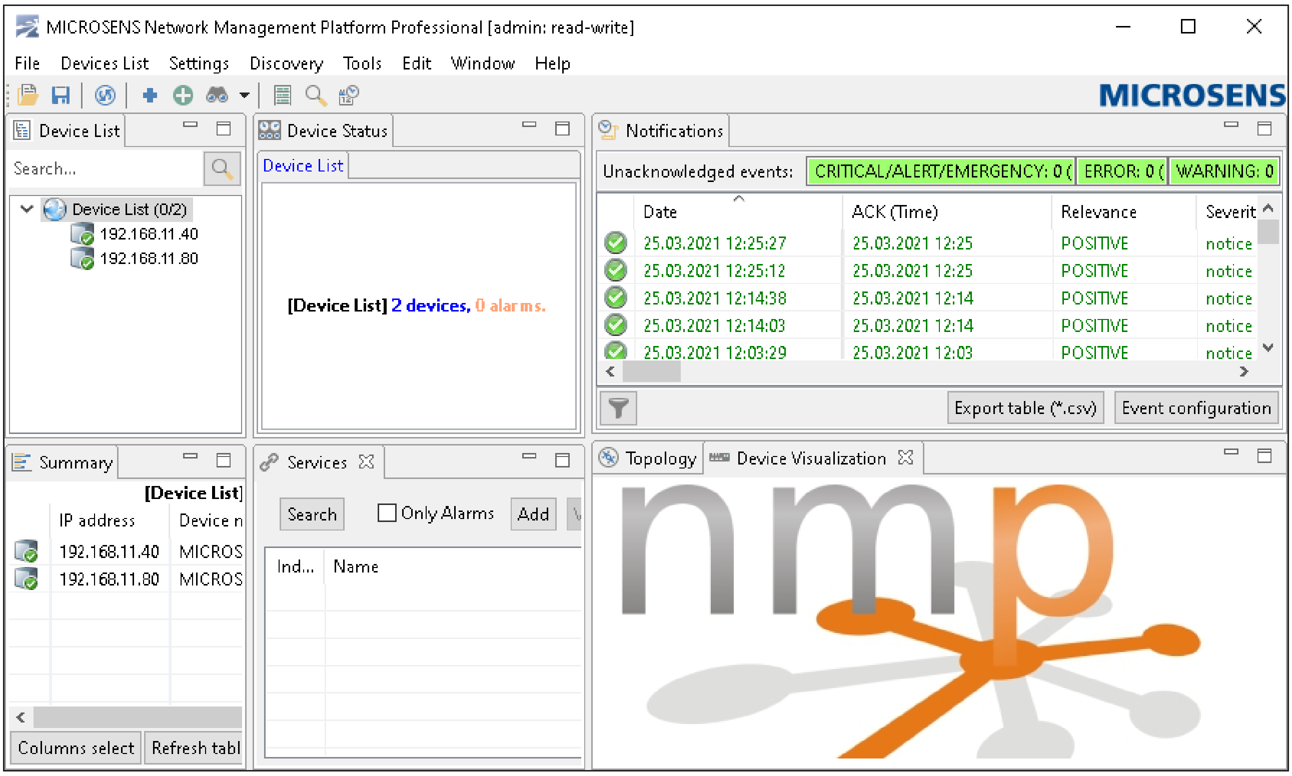
Figure 44. NMP - Tabbed Data Panel

The following tabs are available:

- **Summary** (see Section 4.7.1)
- **Device Status** (see Section 4.7.2)
- **Device Visualization** (see Section 4.7.3)
- **Services** (see Section 4.7.4)
- **Topology** (see Section 4.7.5)
- **Notifications** (see Section 4.7.6)

NOTE	Close the tabs "Device Visualisation", "Services" and "Topology" by clicking on the respective [X] icon on the right side of the tab, if the tab is active. The closed tabs can be restored by using the "Show view" menu (see Section 4.4.7.1).

It is possible to drag and drop every tab inside the NMP window. On a wide screen monitor all tabbed information can be displayed and seen at a glance.



[Device List] 2 devices, 0 alarms.

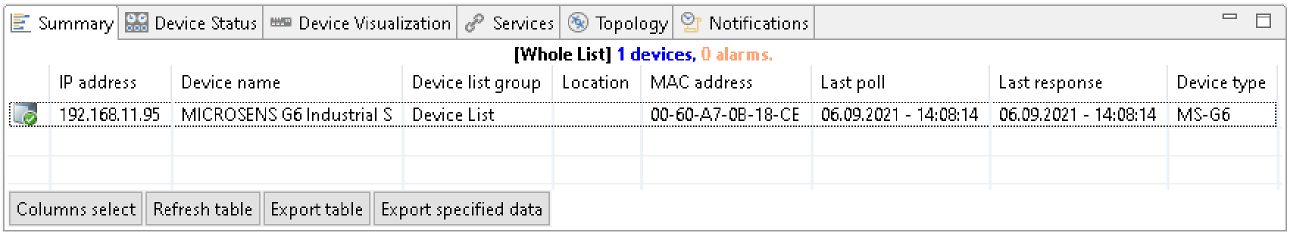
Date	ACK (Time)	Relevance	Severit
25.03.2021 12:25:27	25.03.2021 12:25	POSITIVE	notice
25.03.2021 12:25:12	25.03.2021 12:25	POSITIVE	notice
25.03.2021 12:14:38	25.03.2021 12:14	POSITIVE	notice
25.03.2021 12:14:03	25.03.2021 12:14	POSITIVE	notice
25.03.2021 12:03:29	25.03.2021 12:03	POSITIVE	notice

[Device List]

IP address	Device n
192.168.11.40	MICROS
192.168.11.80	MICROS

Figure 45. NMP - Tabbed Data Panel - Placing the Tabs

4.7.1. Summary



[Whole List] 1 devices, 0 alarms.

	IP address	Device name	Device list group	Location	MAC address	Last poll	Last response	Device type
	192.168.11.95	MICROSENS G6 Industrial S	Device List		00-60-A7-0B-18-CE	06.09.2021 - 14:08:14	06.09.2021 - 14:08:14	MS-G6

Figure 46. NMP - Tabbed Data Panel - Summary

The device summary table shows information on the currently selected sub-group in the device list or on the whole device list if nothing else has been selected. The table provides information on the current device health status. Sort the entries in ascending or descending order by clicking the respective column’s header alternately.

Select the table rows with the right mouse button to access a context menu. This context menu is identical to the respective device’s context menu in the device list tree view (see Section 4.8).

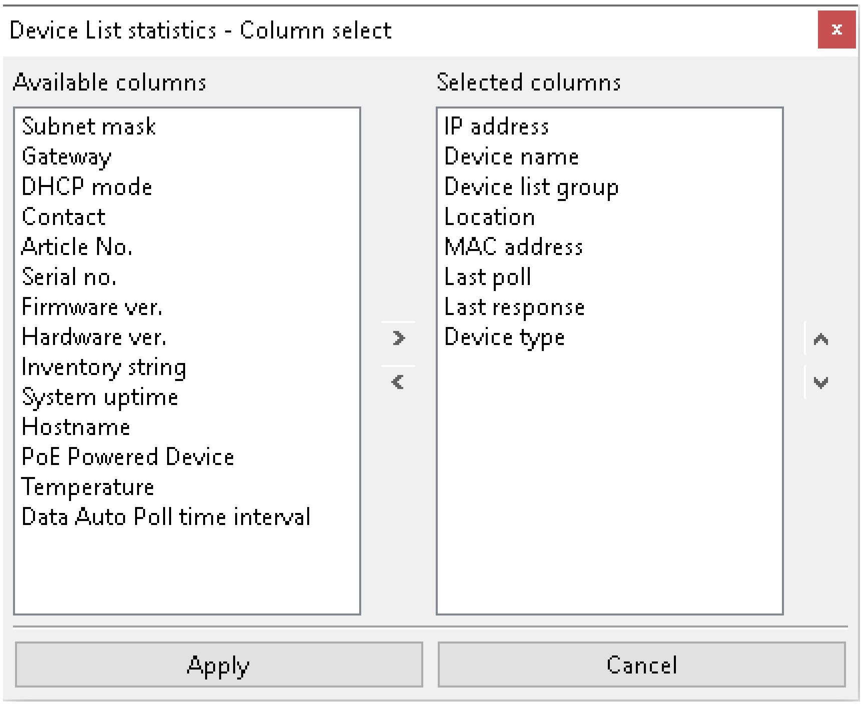
By double clicking on the selected table row the respective device status tab will be opened automatically.

It is possible to move or copy devices listed in the summary table into groups in the device tree list. Do so by using "drag & drop" (click and hold the left mouse button) or "copy & paste" (the keys Ctrl+C and Ctrl+V on the keyboard).

Mark several devices (with Ctrl button pressed) and copy or move them into the selected device list tree group.

Columns Select

By clicking the button **`Columns select`**, choose which information should be visible in the device statistics table.


Device List statistics - Column select

Available columns

- Subnet mask
- Gateway
- DHCP mode
- Contact
- Article No.
- Serial no.
- Firmware ver.
- Hardware ver.
- Inventory string
- System uptime
- Hostname
- PoE Powered Device
- Temperature
- Data Auto Poll time interval

Selected columns

- IP address
- Device name
- Device list group
- Location
- MAC address
- Last poll
- Last response
- Device type

Figure 47. NMP - Tabbed Data Panel - Summary - Column Select

Left-click the respective column with the mouse and move this column from one pane to the other by clicking on the horizontal arrow icons between the column fields.

To specify the sequence of columns mark the respective column in the "Selected columns" field with a left mouse button click and move it up or down with the vertical arrow icons on the right hand pane. To save the column and column sequence setting click on the button `Apply`.

Refresh table

The device summary table is updated automatically, e.g. after selecting a group. It is possible to refresh the current status by clicking the button `Refresh table`.

Export table

Clicking the button `Export table` exports the current table. Specify the name of the `.csv` file (default: `statistics_table.csv`) in the respective operating system's file save dialogue.

Export specified data

Clicking the button `Export specified data` opens the tool, which allows exporting additional information that is not displayed in the visible table. Select the values which should be available in the generated report.

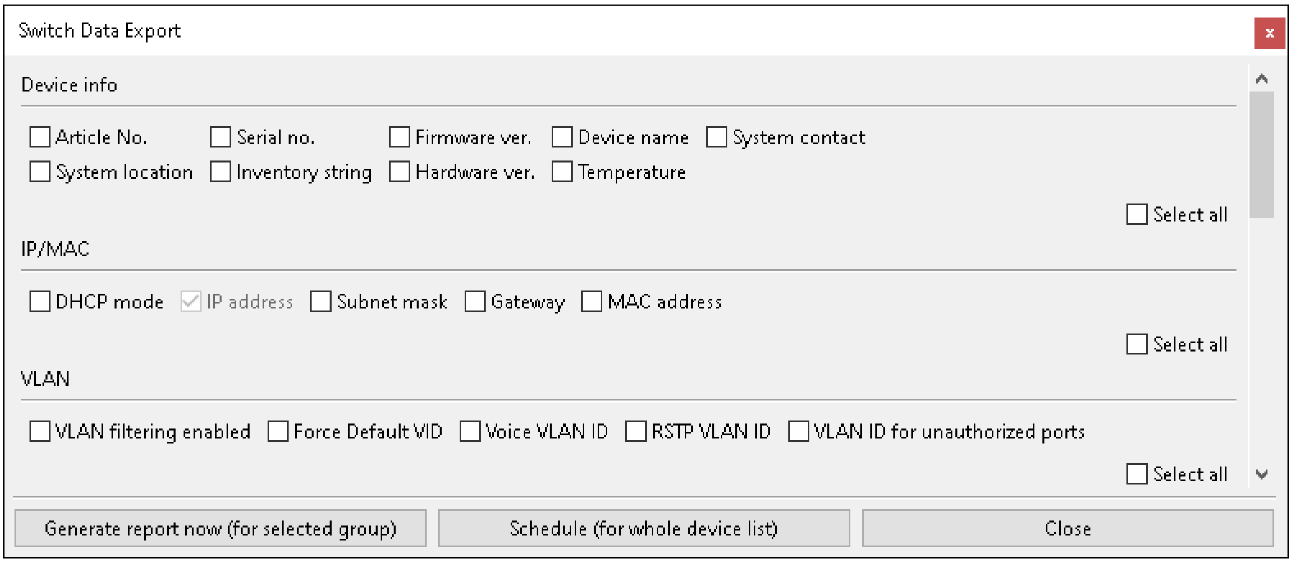


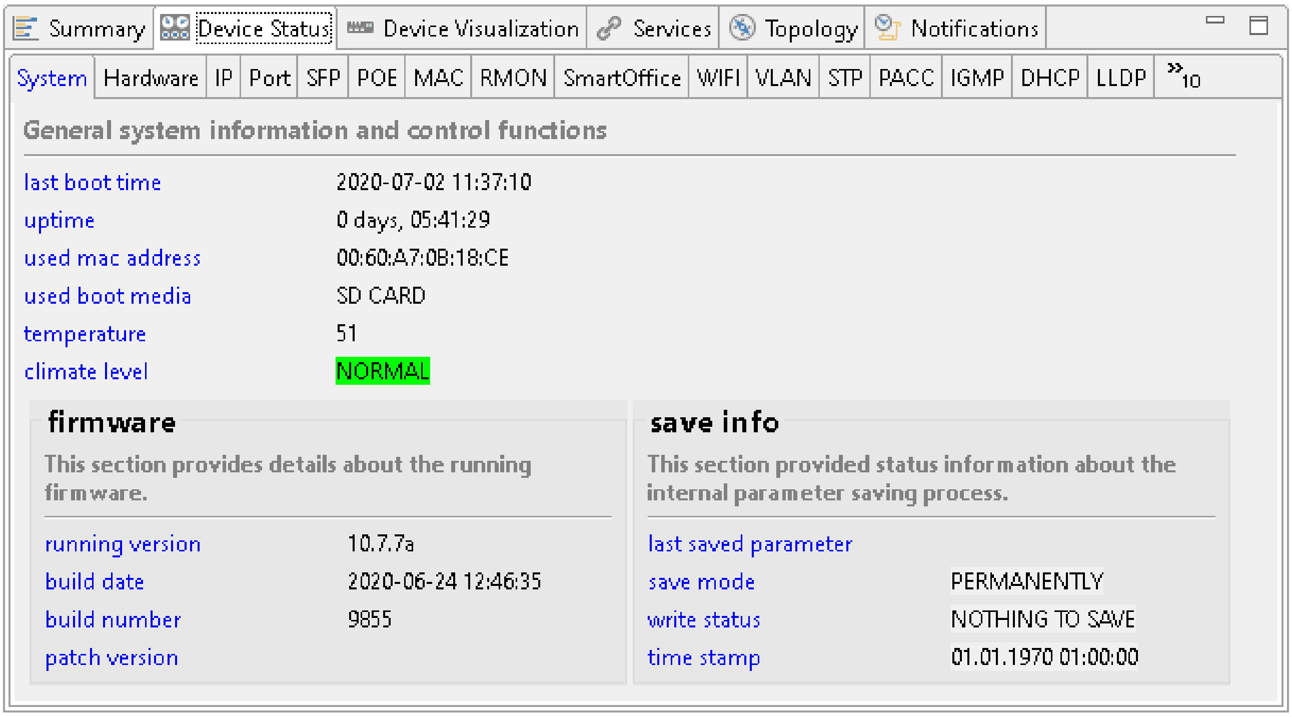
Figure 48. NMP - Tabbed Data Panel - Summary - Export Specified Data

This tool can generate the report immediately after clicking the button `Generate report now`. In such case, the report will be generated for the selected group of devices. It is also possible to schedule generation of a report. In such a case the tool generates the report for the whole device list. Reports can be generated periodically (e.g. one per day).

NOTE

Except for some information (e.g. device name, system contact and all values from IP/MAC) the reporting tool exclusively works with MICROSENS Switches.

4.7.2. Device Status



General system information and control functions

last boot time	2020-07-02 11:37:10
uptime	0 days, 05:41:29
used mac address	00:60:A7:0B:18:CE
used boot media	SD CARD
temperature	51
climate level	NORMAL

firmware

This section provides details about the running firmware.

running version	10.7.7a
build date	2020-06-24 12:46:35
build number	9855
patch version	

save info

This section provided status information about the internal parameter saving process.

last saved parameter	
save mode	PERMANENTLY
write status	NOTHING TO SAVE
time stamp	01.01.1970 01:00:00

Figure 49. NMP - Tabbed Data Panel - Device Status

The **Device Status** tab shows textual information about the selected device (current device status). Information is available on the respective subtabs.

NOTE

There are different tabs for different device types.

For some device types some additional configuration options are available which can be changed directly from the dialogue. If available, click on the button `Configure` on the lower right hand pane of the status window, which opens a configuration dialogue for the respective parameters.

4.7.3. Device Visualization

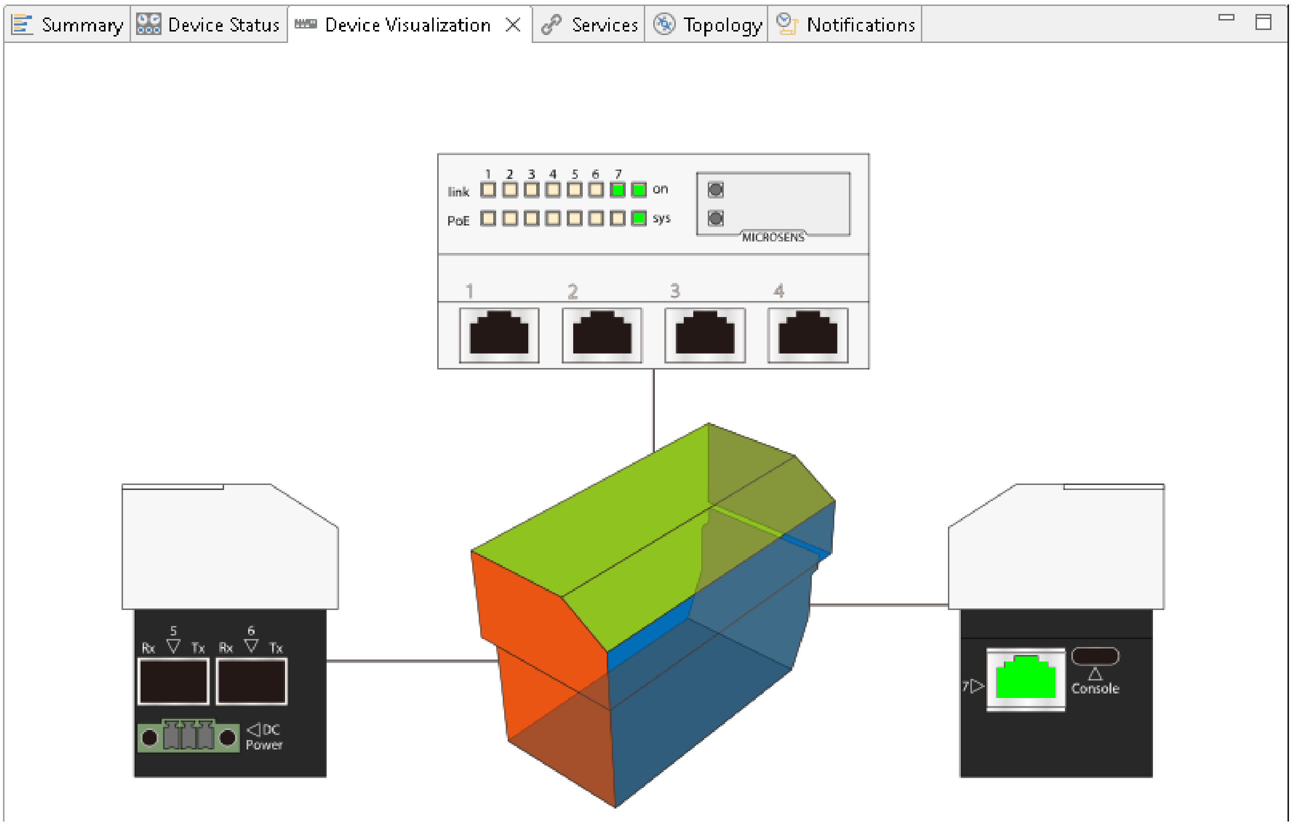


Figure 50. NMP - Tabbed Data Panel - Device Visualization (Example)

The **Device Visualisation** tab provides a symbolic representation of the current state of the managed device. The visualisation is different for different device types. In some cases it also reflects the current LED status of the managed device.

In case of MICROSENS switches, the visualisation indicates the port, link and speed status of each local copper and fibre port of the managed device.

Icon	Meaning
⬛	No link
🟧	10 Mbps link active
🟩	100 Mbps link active
🟨	1 Gbps link active
🟨	10 Gbps link active
☒	Port is off (switches)

Some device types are presented in a faithful rendition which offers additional information on mouse click.

In such cases use the mouse to select sections to access additional information or configuration options (using the left mouse button) or to access the port descriptions configuration (using the right mouse button).

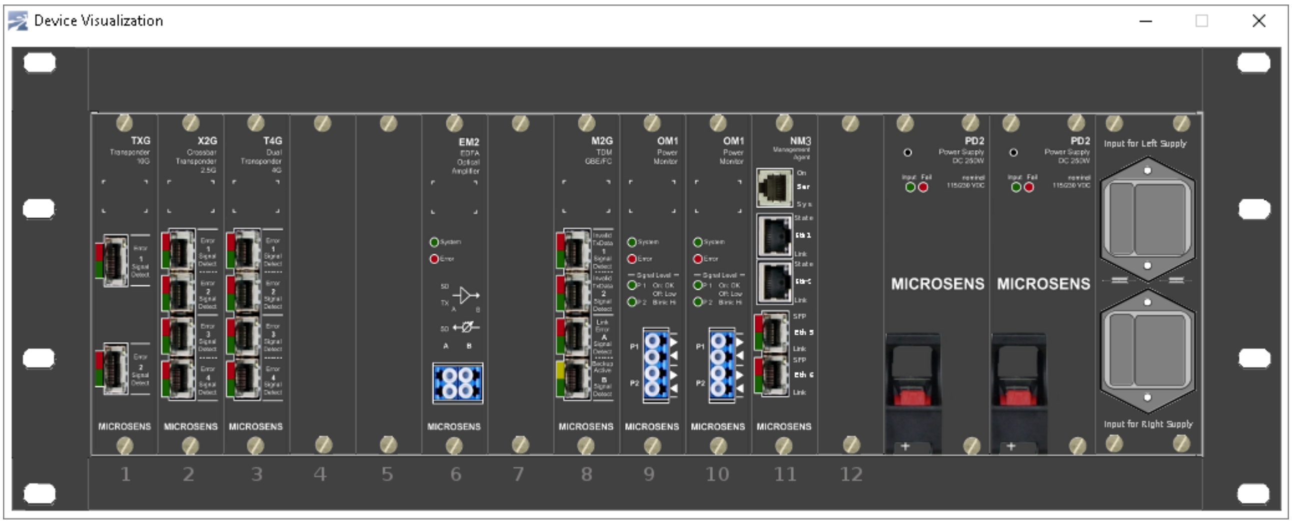
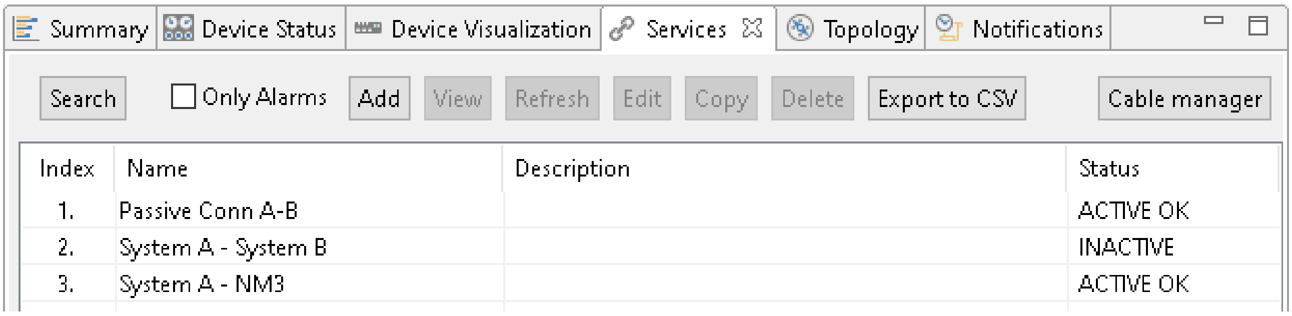


Figure 51. NMP - Tabbed Data Panel - Device Visualisation (MSP 1000)

NOTE These settings are not available for all device types.

4.7.4. Services



Index	Name	Description	Status
1.	Passive Conn A-B		ACTIVE OK
2.	System A - System B		INACTIVE
3.	System A - NM3		ACTIVE OK

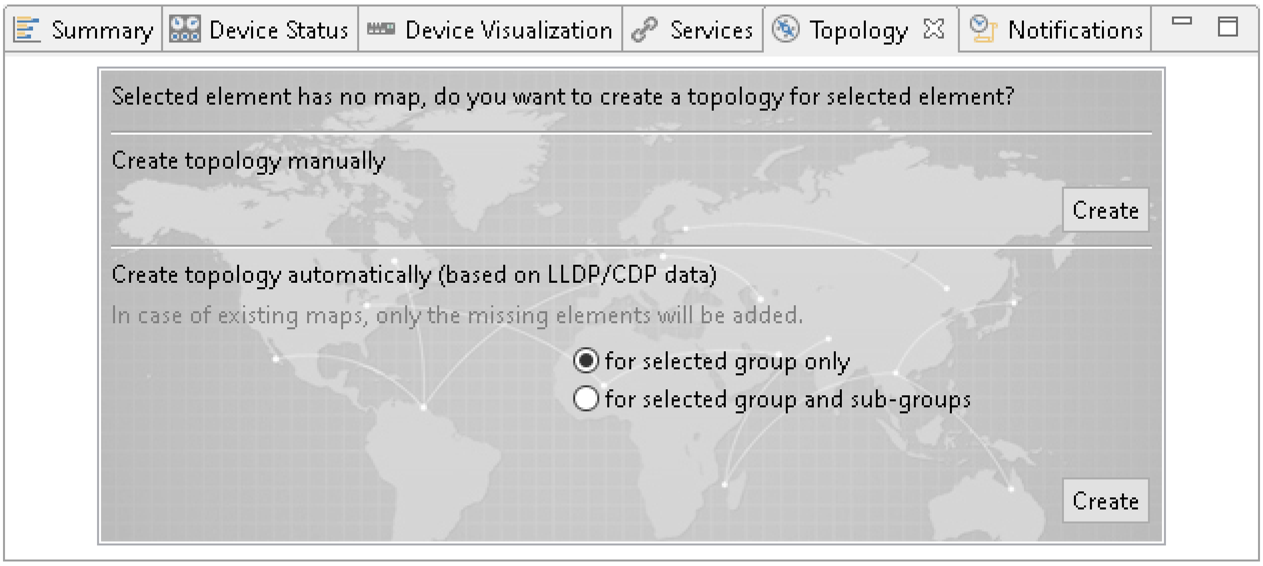
Figure 52. NMP - Tabbed Data Panel - Services

The **Services** tab can be used to define the structures of devices/ports in communication points and to monitor the status of defined active devices.

For more information on working with services please refer to Section 7.10.

NOTE After upgrading NMP from previous versions (NMP v1.x.y), defined end-to-end channels will be imported and transformed to the corresponding Services structures.

4.7.5. Topology



Selected element has no map, do you want to create a topology for selected element?

Create topology manually

Create topology automatically (based on LLDP/CDP data)

In case of existing maps, only the missing elements will be added.

● for selected group only

○ for selected group and sub-groups

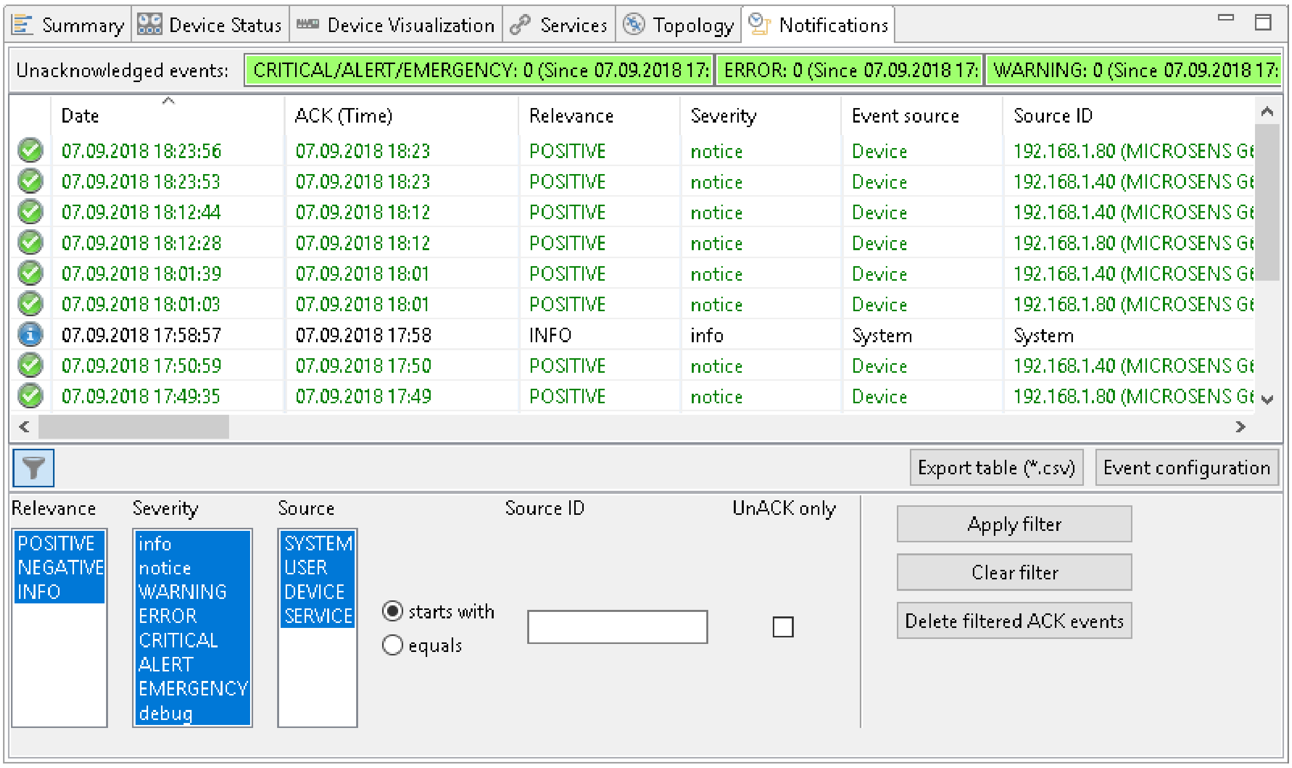
Figure 53. NMP - Tabbed Data Panel - Topology

NMP provides a network management tool for mapping the network and monitoring your devices. Maps are created based on the NMP devices which are displayed in the device list tree view on the left.

For information on how to use the Network Topology browser please refer to Section 7.11.

4.7.6. Notifications

The **Notifications** tab provides information of all the current operations and the messages from monitored devices.



Unacknowledged events: CRITICAL/ALERT/EMERGENCY: 0 (Since 07.09.2018 17: ERROR: 0 (Since 07.09.2018 17: WARNING: 0 (Since 07.09.2018 17:

	Date	ACK (Time)	Relevance	Severity	Event source	Source ID
✓	07.09.2018 18:23:56	07.09.2018 18:23	POSITIVE	notice	Device	192.168.1.80 (MICROSENS G
✓	07.09.2018 18:23:53	07.09.2018 18:23	POSITIVE	notice	Device	192.168.1.40 (MICROSENS G
✓	07.09.2018 18:12:44	07.09.2018 18:12	POSITIVE	notice	Device	192.168.1.40 (MICROSENS G
✓	07.09.2018 18:12:28	07.09.2018 18:12	POSITIVE	notice	Device	192.168.1.80 (MICROSENS G
✓	07.09.2018 18:01:39	07.09.2018 18:01	POSITIVE	notice	Device	192.168.1.40 (MICROSENS G
✓	07.09.2018 18:01:03	07.09.2018 18:01	POSITIVE	notice	Device	192.168.1.80 (MICROSENS G
ℹ	07.09.2018 17:58:57	07.09.2018 17:58	INFO	info	System	System
✓	07.09.2018 17:50:59	07.09.2018 17:50	POSITIVE	notice	Device	192.168.1.40 (MICROSENS G
✓	07.09.2018 17:49:35	07.09.2018 17:49	POSITIVE	notice	Device	192.168.1.80 (MICROSENS G

Relevance: POSITIVE, NEGATIVE, INFO

Severity: info, notice, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY, debug

Source: SYSTEM, USER, DEVICE, SERVICE

Source ID: ● starts with ○ equals

UnACK only: □

Figure 54. NMP - Tabbed Data Panel - Notifications

The different types of events are marked with different colours. With increasing importance an event's visibility in the log table will also increase. The colour code priority sequence is given by green via yellow to red. The counters for unacknowledged events are displayed on the top of the log table.

Filter extensive event lists by miscellaneous filter options and export the event table into a `.csv` file.

NOTE If the filter section is hidden click on the icon `Show filter` in the middle right hand pane of the dialogue.

For more information about working with events please refer to Section 7.12.

4.8. Context Menu

Thanks to the context menu, the access to the important features is quick and easy. Just select the tree view - or any tree element - with the right mouse button and choose one of the options from the context menu.

The context menu offers the opportunity to edit the device list (add, remove elements, sort items) or edit device parameters. The section of the menu where device settings are set may differ for different device types.

4.8.1. Device Context Menu

The device context menu opens after right-clicking on a device in the device tree list or in the **Summary** tab of the tabbed data panel. It offers various features.

NOTE For further information about device configuration via the context menu please refer to Section 7.3.

NOTE Menu items are enabled or disabled depending on the device.

Poll Device Data (F5)

Use this feature to poll information about the selected device. Please refer to Section 4.4.2.3 for more information.

Settings

The settings sub-features are device type-dependent. Please refer to the respective device manual for more details.

Device Configuration Load/Save

These options allow loading/saving the current device configuration from/to a configuration file. For more information please refer to Section 7.4.

Master Configuration

The Master Configuration editor can be used to define properties and settings which can then be applied to devices of the same type as the master device (device from which the master configuration was created). The Master Configuration editor allows changing every single parameter on all the devices in the device list.

For more information please refer to Section 7.6.1 or Section 7.6.2.

Update Firmware

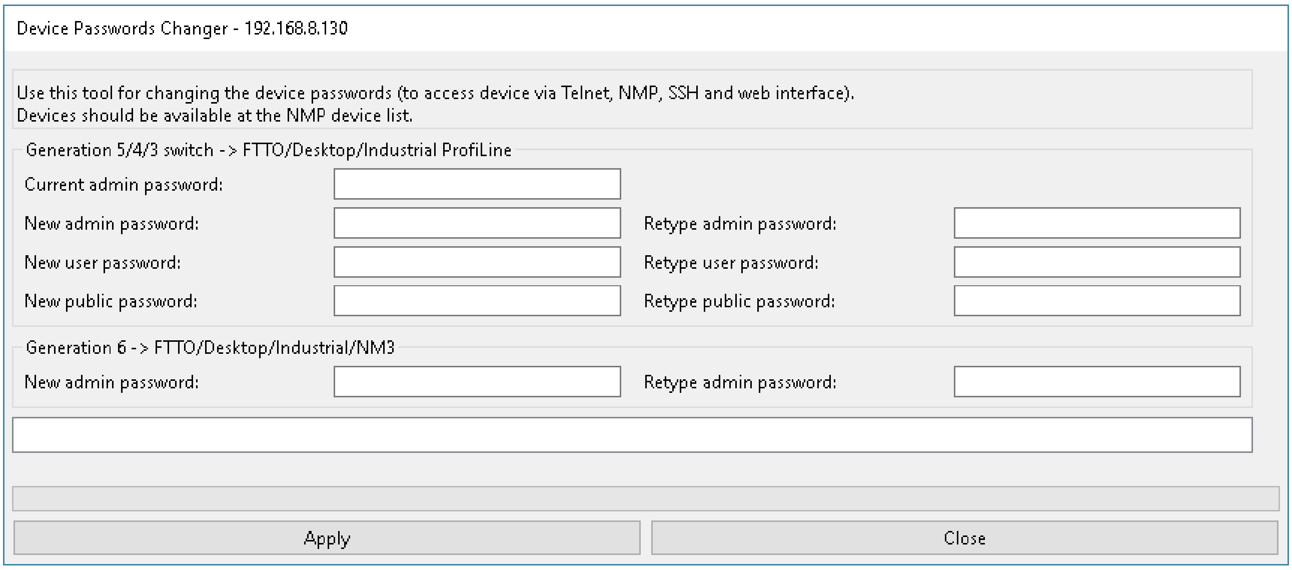
Use this menu item to update the selected device’s firmware file.

NOTE The "Update firmware" task is device type-dependent. Its dialogue may look different for different device types.

For further information on how to update the device’s firmware please refer to Section 7.8.

Device Passwords Changer

Use this tool to change the passwords of a single MICROSENS switch.



Device Passwords Changer - 192.168.8.130

Use this tool for changing the device passwords (to access device via Telnet, NMP, SSH and web interface).
Devices should be available at the NMP device list.

Generation 5/4/3 switch -> FTTO/Desktop/Industrial ProfiLine

Current admin password:

New admin password: | Retype admin password:

New user password: | Retype user password:

New public password: | Retype public password:

Generation 6 -> FTTO/Desktop/Industrial/NM3

New admin password: | Retype admin password:

Figure 55. NMP - Device Context Menu - Device Password Changer

For more information on usage please refer to Section 4.4.2.6.

NOTE

The "Device Password Changer" feature of the device’s context menu changes the password of this respective device. o change multiple passwords of grouped devices use the "Device Password Changer" tool from the "Tools" menu.

Applications

Lists all the applications currently installed on the device. After selecting an application the APP configuration window will be displayed.

For more information on managing applications please refer to Section 7.9.

Install/Uninstall Applications

This tool lists all the applications that are currently available or installed on the switch.

For more information on managing applications please refer to Section 7.9.

Open Device in Web Browser

This feature opens the IP address of the current device in the default web browser.

NOTE

For displaying the Web GUI of the specific MICROSENS G6 device correctly we recommend the use of one of the following browsers:

- Mozilla Firefox, Version 72 or better
- Google Chrome, Version 80 or better

Microsoft Internet Explorer or Microsoft Edge are not supported!

SSH

This feature opens the PUTTY tool and starts a SSH session for the selected device.

Telnet

This menu item opens the command line interface and starts a telnet session for the selected device.

Ping

This feature opens the command line interface and starts a ping command to check the availability of the selected device.

Communication Parameters

It is possible to change the communication parameters of a single device.

A detailed description of the parameters can be found in Section 4.4.2.8.

Device Name (F2)

This feature item allows changing the device’s name displayed in the device tree view. Afterwards NMP asks whether the device name stored in the device should also be changed. Usually this is recommended.

NOTE	Keep in mind that while the device name string length in the device is limited to 128 characters, the device name length in NMP is limited to 25 characters.

Copy (Ctrl+C)

This feature allows copying the selected device to another group.

NOTE	This menu item appears in the context menu of a device in the device list tree view.

Cut (Crtl+X)

This feature allows cutting out the selected device from a group and paste it (move) to another group.

NOTE	This menu item appears in the context menu of a device in the device list tree view.

Paste (Ctrl+V)

This feature allows pasting a copied/cut device to selected group.

NOTE | This menu item appears in the context menu of a device in the device list tree view.

Delete Device (`Del`)

This feature deletes the selected device from the device list. If there are any copies of the deleted device, NMP will ask whether the copies should also be removed.

Show on the Map

The selected device will be highlighted in the **Topology Manager** tab (see Section 4.7.5). The map containing the selected device will be automatically opened.

NOTE | This menu item is enabled as soon as the device is assigned to a topology map.

Spare (Global Alarm Acknowledged)

The "Global Alarm Acknowledged" task can be used for unavailable devices (the devices marked with a red icon). It confirms that a device is not responding.

The messages of faultlessly operating devices are displayed in green. A device with an acknowledged alarm will not generate any alarm information (highlighted red) in the **Notifications** tab. Additionally, a device with a confirmed alarm will not be shown in the "Alarm list" group.

4.8.2. Group Context Menu

The group context menu opens after right-clicking on a group in the device tree list.

NOTE | The menu items may vary for groups containing different types of devices.

Some features of the group context menu are reflected in the respective device context menu. The difference is that the action has an impact on all devices inside the selected group (and sub group) and not on just one respective device.

Poll Group Data (`F5`)

NMP loads the data from all the devices in the selected group (including devices from subgroups of the currently selected group).

Please refer to Section 4.4.2.3 for more information.

Device Configuration Load/Save

The availability of this feature depends on the type of devices in the current group. The feature is split into sub features.

- to save the configuration of all the devices in separate files,

- to load individual configurations from separate files to the devices and
- to load a configuration from one file to all devices in the group. In this case select which configuration components to restore.

For more information please refer to Section 7.4.

Master Configuration

The "Master Configuration" can be used to define properties and settings which can then be applied to devices of the same type as the master device (i.e. the device from which the master configuration was created). The master configuration allows changing every single parameter on all the devices in the device list.

For more information please refer to Section 7.6.1.

Update Firmware

A group can contain multiple devices of different types. So it is not possible to update the firmware for all possible device types at once.

Therefore, contrary to the device context menu, this menu item is split into sub-menu update items for

- Generation 7 (FTTO)
- Generation 6s (FTTO)
- Generation 6s+ (FTTO)
- Generation 6 switches (FTTO/Desktop/Industrial/NM3)
- Generation 5/4/3 switches (FTTO/Desktop/Industrial ProfiLine)
- MultiPort media converters

This feature can be used to update a firmware for multiple devices which are located at the same group. NMP will automatically select the devices with the same type (e.g. G6 switches, if the firmware update will be started for G6 devices).

For more information please refer to Section 7.8.

Applications Installer

With this feature it is possible to install apps on multiple grouped devices at once.

For more information on managing applications please refer to Section 7.9.

Add New Device

This feature adds a new device to the selected group. If no group is selected, the device will be added to the root of the device list.

For more information please refer to the section Section 4.4.2.1.

Add New Subgroup

A new subgroup is added to the currently selected group. The group name can be subsequently added.

Copy (`Ctrl`+`C`)

This feature can be used to create a copy of a whole group. All the devices and subgroups of the selected group will be copied too.

Cut (`Crtl`+`X`)

This feature can be used to cut the current group and paste it to another one.

Paste (`Ctrl`+`V`)

Paste the previously copied/cut group into the new selected one.

Delete Group (`Del`)

After confirming this feature the selected group is deleted, including all contained devices and subgroups.

Edit Group Name (`F2`)

Change the name of the selected group in the device list. The group name string length is unlimited.

Communication Parameters

It is possible to change the communication parameters of all devices within the selected group.

A detailed description of the parameters can be found in Section 4.4.2.8.

NOTE All these settings represent characteristics of any device in the device list. The values are stored in the device list, not in the device itself.

Open Devices in Web Browser

NMP opens all grouped devices in the default web browser.

NOTE Keep in mind that when opening a large number of web pages the system may run out of resources.

NOTE

For displaying the Web GUI of the specific MICROSENS G6 device correctly we recommend the use of one of the following browsers:

- Mozilla Firefox, Version 72 or better
- Google Chrome, Version 80 or better

Microsoft Internet Explorer or Microsoft Edge are not supported!

Group Ring Devices

This feature automatically groups all ring switches in the device list. A new group is created in the device list. This contains a subgroup named "Ring no xx" for each ring. Switches with enabled ring support are copied to the corresponding group. The ring master is highlighted with yellow background colour.

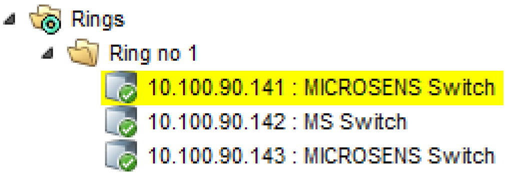

Rings
Ring no 1
10.100.90.141 : MICROSENS Switch
10.100.90.142 : MS Switch
10.100.90.143 : MICROSENS Switch

Figure 56. NMP - Device List Tree View - Ring Device Group

For more information please refer to Section 7.14.

Group Not Available Devices

This feature automatically generates a special group including a copy of all unavailable devices (marked with this icon: ☒) in the device list. This new group is called "Alarm List".

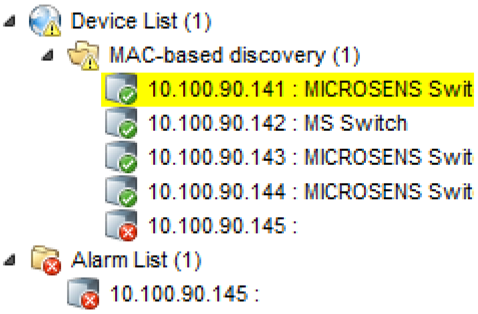

Device List (1)
MAC-based discovery (1)
10.100.90.141 : MICROSENS Swit
10.100.90.142 : MS Switch
10.100.90.143 : MICROSENS Swit
10.100.90.144 : MICROSENS Swit
10.100.90.145 :
Alarm List (1)
10.100.90.145 :

Figure 57. NMP - Device List Tree View - Alarm List

Clear Acknowledged Alarms

This function clears the "Spare (Global alarm acknowledged)" flag from all the unavailable devices in the device list.

For more information please refer to Section 4.8.1.20.

Sort By IP

All the devices in the selected group are sorted by IP address.

Sort By Description

All elements (devices and subgroups) in the selected group are sorted by device description/device name.

Rebuild Group Structure

This menu item rebuilds the device list using the device location and device group parameters. As a result, a new device list is created with all the devices grouped according to their location and group. All devices with either an unset location or group are moved to the groups with default names: "unknown location" and "unknown". Additionally, the ";" sign can be used as a separator in the location and group strings to extend the number of available tree levels.

Example 1. Example

- Current tree list group is "MAC Discovery"
- Device is "10.100.90.100" in the "MAC Discovery" tree list group
- Device Location = A;B
- Device Group = C;D;E

When the feature is applied on the "MAC Discovery" group, the new structure will be

`…\MAC Discovery\A\B\C\D\E\10.100.90.100`.

All the sub-items in "MAC Discovery" are deleted and the new structure is created in the "MAC Discovery" group.

5. NMP Enterprise

This chapter describes working with NMP Enterprise.

NOTE The following descriptions and screenshots refer to the Windows® version of NMP. Because NMP is a Java application based on Eclipse OpenJ9, the GUI appearance does not considerably differ between Windows® and Linux operating systems. The NMP functionality is exactly the same.

NOTE In the event of technical problems with NMP, please contact the technical support of MICROSENS under the link provided within the report dialogue. For a precise and effective support save the provided report as text file and upload it to the MICROSENS ticket system when required.

5.1. Starting the Server Manager

NOTE "Server Manager" is the application to operate the server component of NMP Enterprise.

After first start-up of the Server Manager the server administrator should configure all application settings. Please refer to the respective description for setting up the server in Section 5.4.1.

5.1.1. Starting the Application on Windows®

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

Start › MICROSENS › MICROSENS NMPv2 Server

or

Start › MICROSENS › MICROSENS NMPv2 Server (Debug mode)

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

5.1.2. Starting on Linux Operating Systems

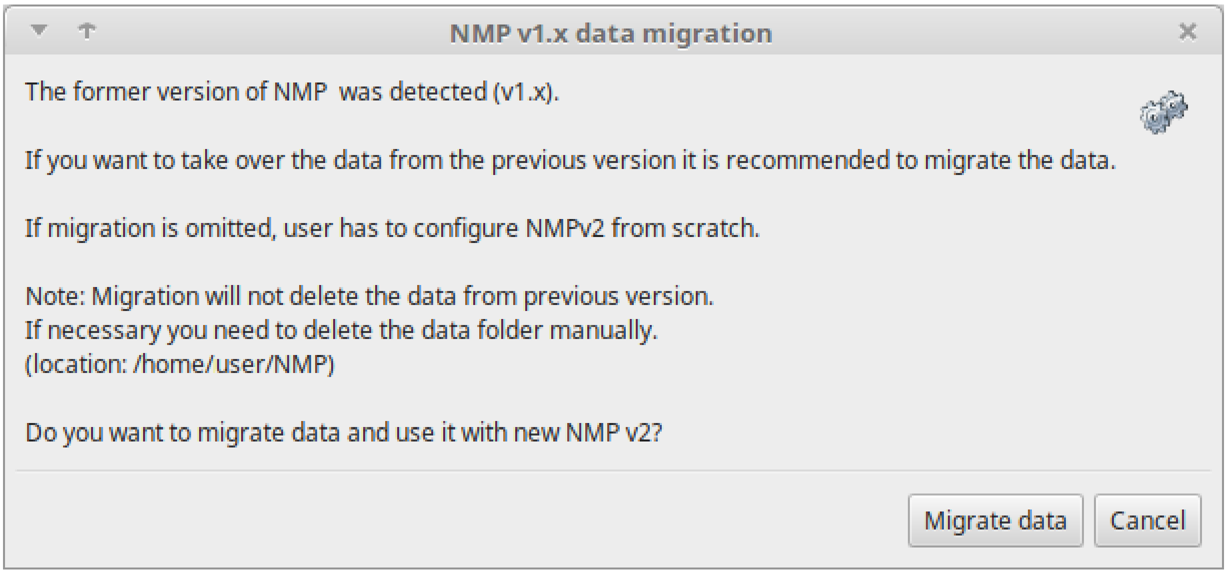
NOTE The application uses some ports lower than 1024. On UNIX like operating systems only applications started with root rights are able to bind those port. Therefore it is important to start the application with `sudo ./NMP` or `su root ./NMP` (or the respective super user command of your Linux distribution)

For more information please refer to the MICROSENS Knowledge Base on the website www.microsens.com/support.

1. Open a Linux CLI and change to the application’s installation directory (e.g. `~/MICROSENS/NMP_Server` and `~/MICROSENS/NMP_Client`).
2. Start the application as super user.

5.1.3. First Program Start

During first start the application checks whether a previous version 1 installation is available. If so, the application asks to migrate the data from this earlier version to version 2.



The former version of NMP was detected (v1.x).

If you want to take over the data from the previous version it is recommended to migrate the data.

If migration is omitted, user has to configure NMPv2 from scratch.

Note: Migration will not delete the data from previous version.
If necessary you need to delete the data folder manually.
(location: /home/user/NMP)

Do you want to migrate data and use it with new NMP v2?

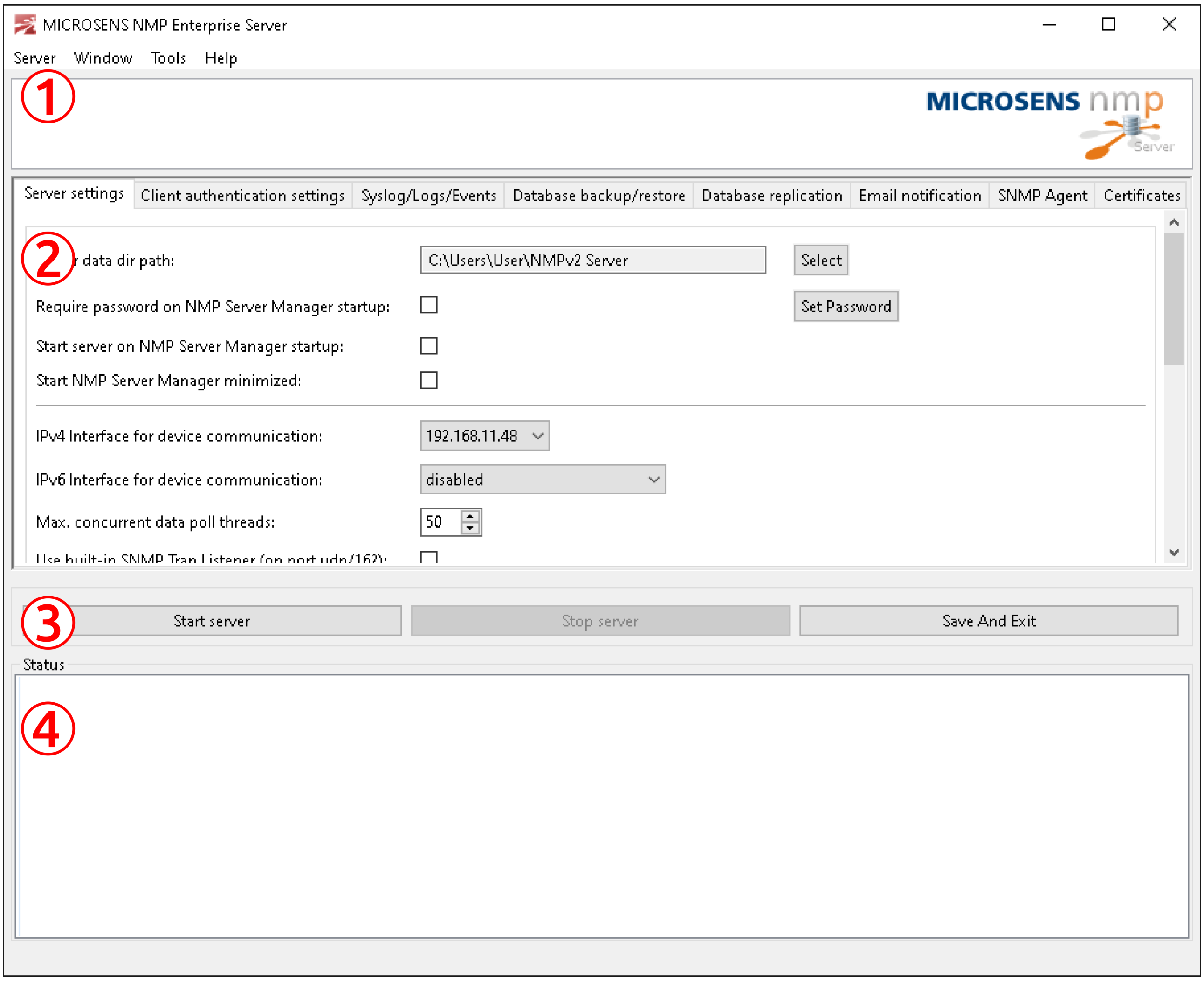
Figure 58. Data Migration from version 1

Click on the button **`Migrate data`** to transfer the data.

The application will create a new directory `~/NMPv2 Server` and `~/NMPv2 Client` in the user’s home directory.

The first time starting process continues with licensing NMP Enterprise. For more information see Chapter 3.

5.2. Server Manager Main Window



data dir path: C:\Users\User\NMPv2 Server

Require password on NMP Server Manager startup: ☐

Start server on NMP Server Manager startup: ☐

Start NMP Server Manager minimized: ☐

IPv4 Interface for device communication: 192.168.11.48

IPv6 Interface for device communication: disabled

Max. concurrent data poll threads: 50

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

Figure 59. 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).

5.3. Main Menu

The application's main menu bar provides access to the following functions:

Server	Managing the Server Manager
Window	Show and hide the Server Manager window
Tools	Several handy tools for managing the network infrastructure
Help	Access to the application’s user manual as well as licence and general information

5.3.1. Server

Start Server

This menu item starts the server component. The Server Manager subsequently starts the configured http server (if enabled) and the database engine.

If this menu item appears grey the server is running.

Stop server

This menu item stops the server component.

If this menu item appears grey the server is stopped.

IMPORTANT	Do not stop the server by terminating the server process via the task manager of your operating system or any respective CLI commands (e.g. `kill`). This can lead to data corruption or data loss in the server’s database!

Service control

This menu item installs/uninstalls the server component as a Windows service.

For detailed information, please refer to Section 7.15.

Save And Exit

This menu item saves the current configuration and closes the Server Manager window.

If this menu item appears grey the server is running. Stop the server before closing the Server Manager.

5.3.2. Window

Hide window

This menu item closes the Server Manager window. The application is accessible via the system tray icon.

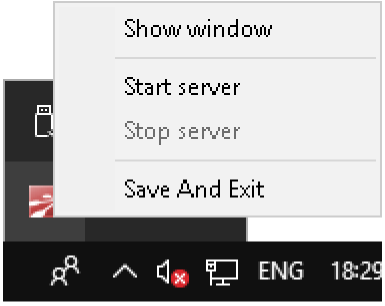


Figure 60. NMP - Server Manager - System Tray Icon

A left-click on the Server Manager’s system tray icon shows or closes the Server Manager window.

A right-click opens a context menu from where it is possible to start/stop the server or to exit the Server Manager application.

5.3.3. Tools

Generate Properties File for Client

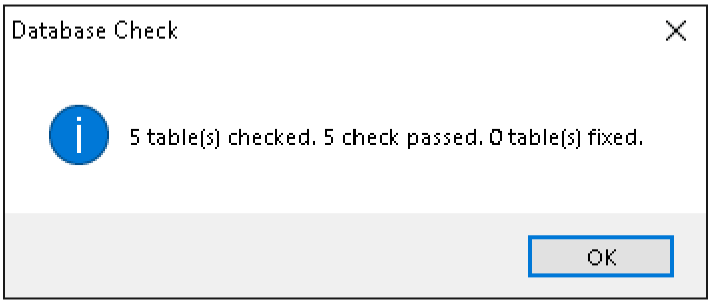
This menu item opens the operating system’s file explorer to save a text file `enterprise_server.properties` containing the server address and server port:

```
#---Enterprise Server settings---
#Fri Nov 23 12:04:26 GMT+01:00 2018
server_address=127.0.0.1
server_port=4000
```

When installing the application’s client component the installer initially searches for this file to preset the server settings for the server client communication.

Database Check

The database check makes sure that after an unintended server stop (e.g. after a system crash or `kill` command) no defective data inhibit additional configuration backups.



Database Check

5 table(s) checked. 5 check passed. 0 table(s) fixed.

Figure 61. Server Manager - Main Menu - Tools - Database Check

The opening status dialogue shows the result of this database check.

NOTE Normally, a database check should only be executed by the admin after the application was terminated in an uncontrolled way.

5.3.4. Help

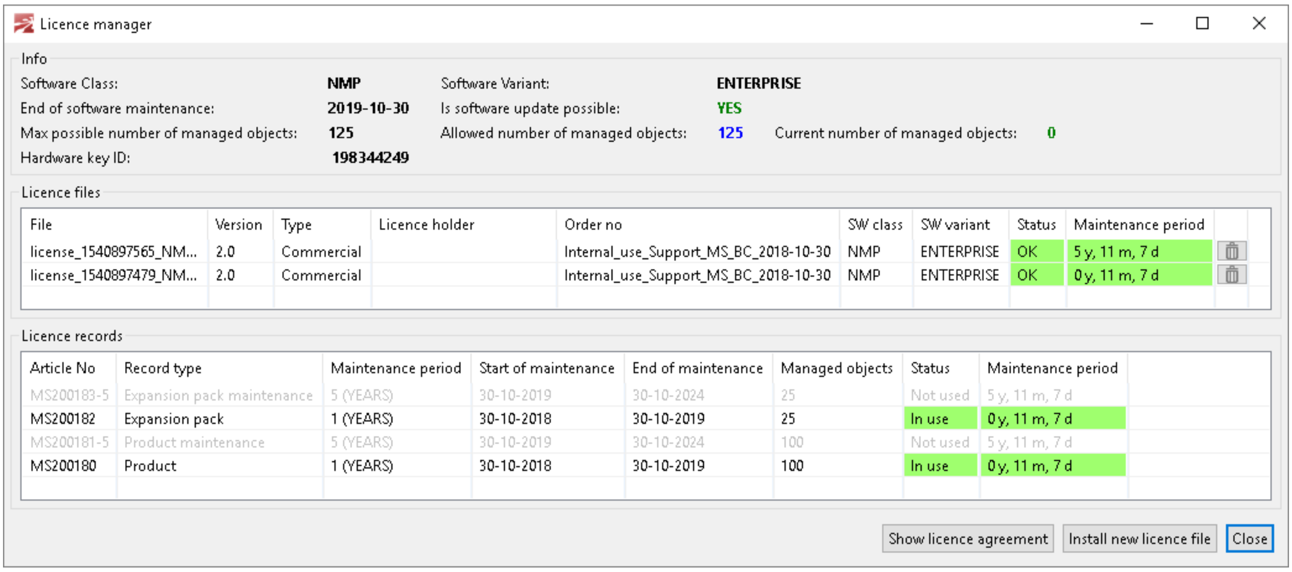
Server help

This is the link to the application’s manuals. The manuals are provided in form of PDF files and are available in the following languages:

- English

NOTE A PDF reader needs to be installed on the system in order to be able to open the manuals correctly.

Licence info



Licence manager

Info

Software Class: **NMP** Software Variant: **ENTERPRISE**
End of software maintenance: **2019-10-30** Is software update possible: **YES**
Max possible number of managed objects: **125** Allowed number of managed objects: **125** Current number of managed objects: **0**
Hardware key ID: **198344249**

Licence files

File	Version	Type	Licence holder	Order no	SW class	SW variant	Status	Maintenance period	
license_1540897565_NM...	2.0	Commercial		Internal_use_Support_MS_BC_2018-10-30	NMP	ENTERPRISE	OK	5 y, 11 m, 7 d	🗑
license_1540897479_NM...	2.0	Commercial		Internal_use_Support_MS_BC_2018-10-30	NMP	ENTERPRISE	OK	0 y, 11 m, 7 d	🗑

Licence records

Article No	Record type	Maintenance period	Start of maintenance	End of maintenance	Managed objects	Status	Maintenance period
MS200183-5	Expansion pack maintenance	5 (YEARS)	30-10-2019	30-10-2024	25	Not used	5 y, 11 m, 7 d
MS200182	Expansion pack	1 (YEARS)	30-10-2018	30-10-2019	25	In use	0 y, 11 m, 7 d
MS200181-5	Product maintenance	5 (YEARS)	30-10-2019	30-10-2024	100	Not used	5 y, 11 m, 7 d
MS200180	Product	1 (YEARS)	30-10-2018	30-10-2019	100	In use	0 y, 11 m, 7 d

Figure 62. NMP - Licensing Information

This menu item opens an overview of the licensing information. The dialogue shows information e.g. about the currently installed licence key file and the entitled user.

Additionally it links to the application's licence agreement.

- **Licence key files:** These are the licence key files located in the local folder `$USER_HOME/$NMP_DATA_DIR/licenses`.
- **Licence key records:** These are the licence keys included in the licence key files. One licence key file can contain one or more records with specific access rights.

Additionally this dialogue links to the application's licence agreement.

There are two options to install a new licence key file:

- A click on the button `Install new licence key file` opens the file manager. Navigate to the new licence key file to update the licence key for your application variant.
- Copy the licence key file directly into the local folder `$USER_HOME/$NMP_DATA_DIR/licenses`.

The application scans this folder automatically to check if there are any modifications (i.e. licence key installed, licence key deleted).

In case of using the server as service, there is no need to stop the server instance in order to install a new licence key file. Just copy the licence key file into the licence key folder and the application will install it automatically.

Without access to the local licence key folder use the licensing information dialogue of the client component.

NOTE | To obtain a new application licence key file please contact MICROSENS.

License Activation Code Request

For purchasing a valid product licence key file the use of the MICROSENS Unique System ID Generator is mandatory.

For more information about using the Unique System ID Generator see Section 3.3.

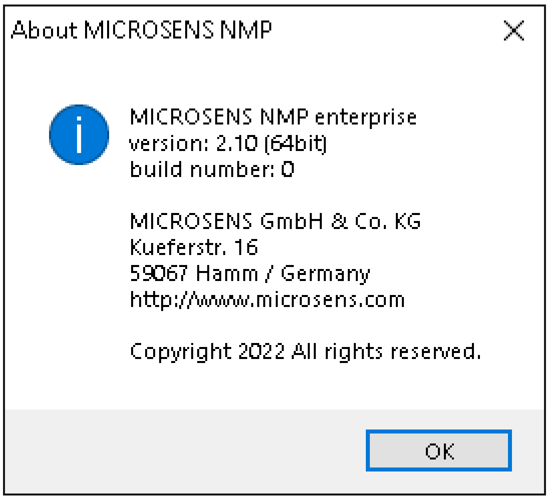
Unique System ID Generator

For purchasing a valid product licence key file the use of the MICROSENS Unique System ID Generator is mandatory.

Find more information about using this application in Section 3.3

About

This dialogue shows information on the application and its version.



About MICROSENS NMP

MICROSENS NMP enterprise
version: 2.10 (64bit)
build number: 0

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm / Germany
http://www.microsens.com

Copyright 2022 All rights reserved.

Figure 63. NMP - Main Menu - Help

5.4. Tabbed Server Configuration Panel

The tabbed server configuration panel allows configuring all the server instance’s parameters. The following tabs are available:

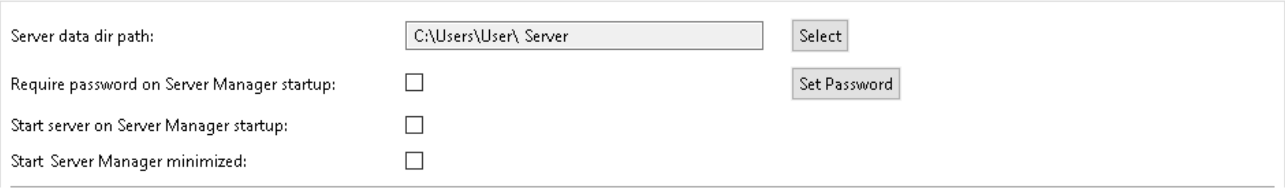
Server Settings	General server settings for data directory, IP interfaces and database configuration.
Client Authentication Settings	Configuration of authentication for registered users.
Syslog/Logs/Events	Configuration of messages, logs and events.
Database Backup/Restore	Settings on when and where the application should save database backups.
Database Replication	Configuration of the database replication feature.
Email Notification	Configuration of email addresses for notifications on errors, SNMP traps and scheduled task events.
SNMP Agent	Configuration of the SNMP Agent.
Certificates	Configuration of certificates for security and authorisation, e.g. used in SSL encryption.

5.4.1. 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.
- **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.

General



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

Require password on Server Manager startup: □

Start server on Server Manager startup: □

Start Server Manager minimized: □

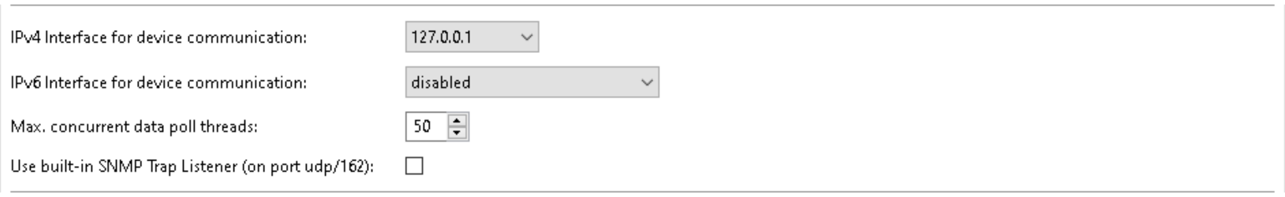
Figure 64. Server Manager - Tab "Server Settings" - General

- **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:** When selected, the password prompt will be displayed before opening the Server Manager window. The password can be set by selecting the button `Set Password`.

  Enter the password, confirm the password to prevent typing errors and click on the `Set Password` 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.

Device Communication



IPv4 Interface for device communication: 127.0.0.1

IPv6 Interface for device communication: disabled

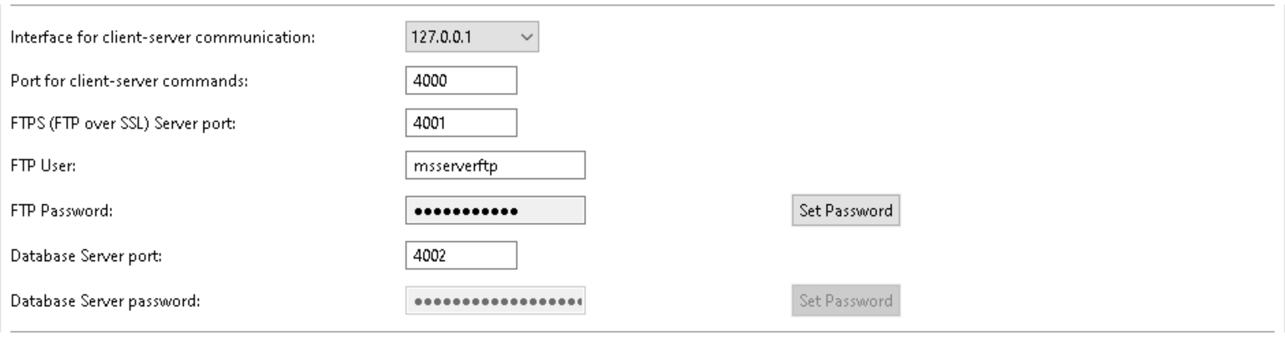
Max. concurrent data poll threads: 50

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

Figure 65. 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.

Client-Server Communication



Interface for client-server communication: 127.0.0.1

Port for client-server commands: 4000

FTPS (FTP over SSL) Server port: 4001

FTP User: msserverftp

FTP Password: ●●●●●●●●●●● Set Password

Database Server port: 4002

Database Server password: ●●●●●●●●●●●●●●●●●● Set Password

Figure 66. Server Manager - Tab "Server Settings" - Client-Server Communication

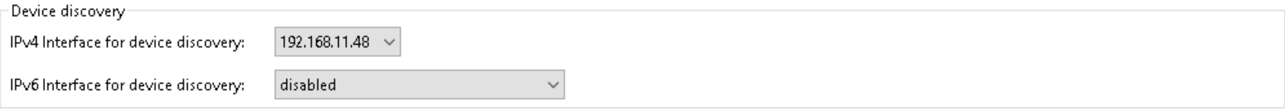
- **Interface for client-server communication:** The IPv4 address of the network interface that will be used for the application’s client access. If the HTTP server is enabled for web client access, this interface is also used by the built-in HTTP server.
- **Port for client-server commands:** The port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

As soon as the Server Manager is started, it is possible to change the database password. Administrator user rights are mandatory.

NOTE | Authorise all given port numbers in installed firewalls.

Device Discovery



Device discovery

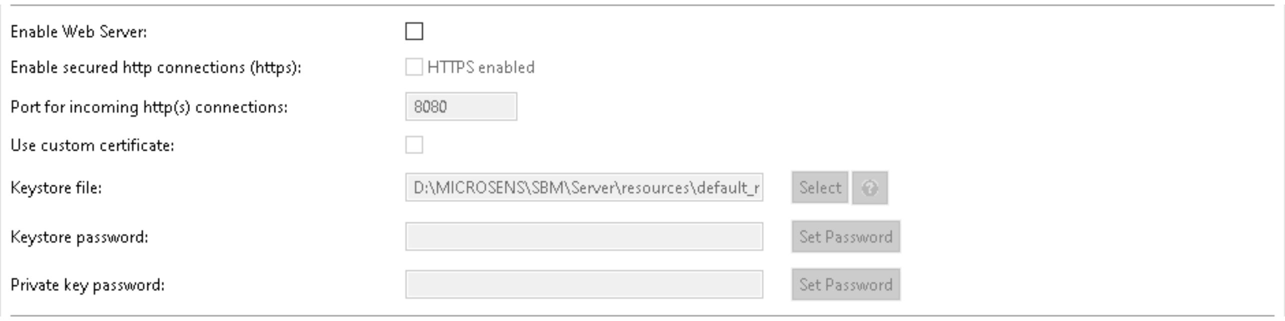
IPv4 Interface for device discovery: 192.168.11.48

IPv6 Interface for device discovery: disabled

Figure 67. Server Manager - Tabbed Server Configuration Panel - Server Settings - Device Discovery

- **IPv4 Interface for device discovery:** The IPv4 address of the network interface that will be used for detecting and communicating 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 instance.
- **IPv6 Interface for device discovery:** IPv6 Interface for device detection and communication: The IPv6 address of the network interface that will be used for communication with the managed devices.

Web Server



Enable Web Server: □

Enable secured http connections (https): □ HTTPS enabled

Port for incoming http(s) connections: 8080

Use custom certificate: □

Keystore file: D:\MICROSENS\SBM\Server\resources\default_r

Keystore password:

Private key password:

Figure 68. Server Manager - Tab "Server Settings" - Web Server

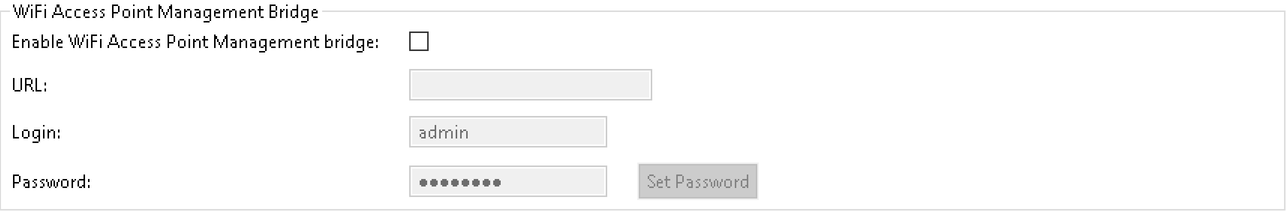
- **Enable HTTP Web Server:** Enables or disables the built-in HTTP server that is used for web client access.
- **Enable secured http connections (https):** The server instance offers secured HTTP connections for web access. The https connections are encrypted so the com-

munication 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.

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

WiFi Access Point Management Bridge



WiFi Access Point Management Bridge

Enable WiFi Access Point Management bridge:	□	
URL:		
Login:	admin	
Password:	••••••••	Set Password

Figure 69. Server Manager - Tab "Server Settings" - WiFi Access Point Management Bridge

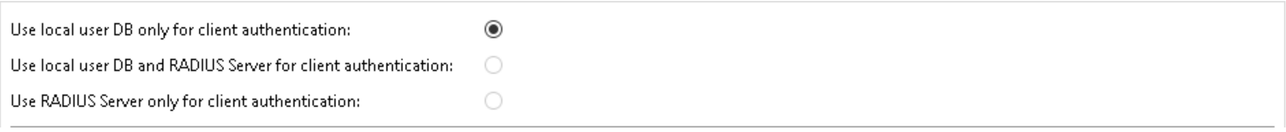
- **Enable WiFi Access Point Management Bridge:** Check this option to enable the bridge.
- **URL:** Enter the bridged access point's URL.
- **Login:** Enter the user name that is registered on the access point.
- **Password:** Enter the user's password.

5.4.2. 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.

Authentication Selection



Use local user DB only for client authentication:	●
Use local user DB and RADIUS Server for client authentication:	○
Use RADIUS Server only for client authentication:	○

Figure 70. Server Manager - Tab "Client Authentication" - Selection

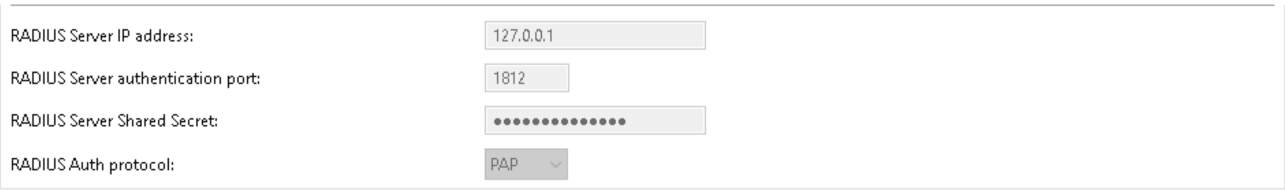
- **Use local user DB only for client authentication:** The server will use the information from its local database for user authentication.

- **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).

> **NOTE**
>
> 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 Settings



RADIUS Server IP address: 127.0.0.1
RADIUS Server authentication port: 1812
RADIUS Server Shared Secret: ••••••••••••••
RADIUS Auth protocol: PAP

Figure 71. 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)	NMP Server User Level
Login-User (1)	user
NAS-Prompt-User (7)	manager
Administrative-User (6)	admin
Callback-Administrative (11)	sysadmin

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

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

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

manager         Cleartext-Password := "manager"
                Service-Type = NAS-Prompt-User

user            Cleartext-Password := "user"
                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.

NOTE

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.

NOTE

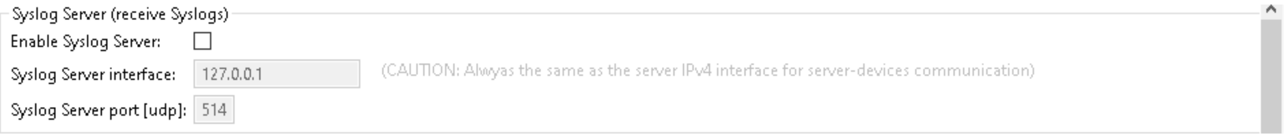
Please keep in mind that the number of application's users available on the RADIUS server should be identical to the number of user accounts allowed by the application's licence key file.

5.4.3. 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.

Syslog Server (Receive Syslogs)



Syslog Server (receive Syslogs)

Enable Syslog Server: □

Syslog Server interface: 127.0.0.1 (CAUTION: Alwyas the same as the server IPv4 interface for server-devices communication)

Syslog Server port [udp]: 514

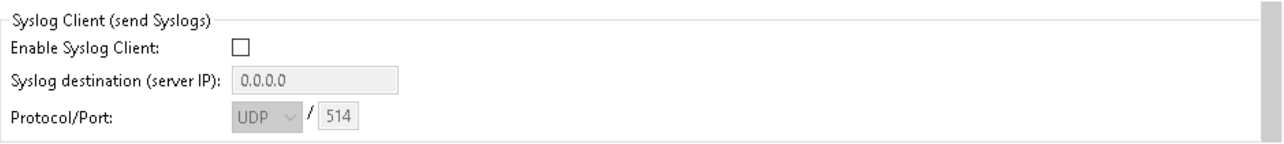
Figure 72. Server Manager - Tab "Syslog/Logs/Events" - Syslog Server

- **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.

NOTE 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.

Syslog Client (Send Syslogs)



Syslog Client (send Syslogs)

Enable Syslog Client: □

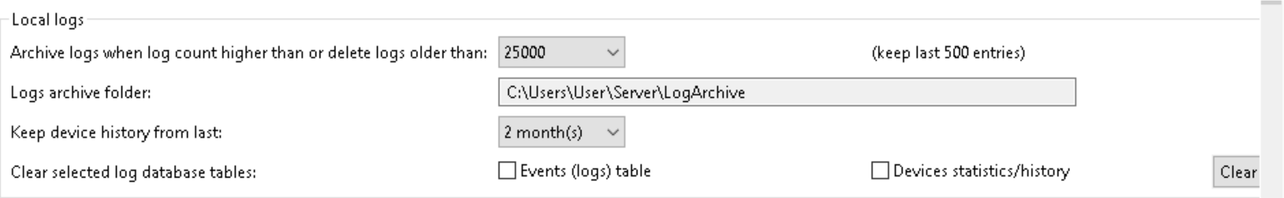
Syslog destination (server IP): 0.0.0.0

Protocol/Port: UDP / 514

Figure 73. 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.

Local Logs



Local logs

Archive logs when log count higher than or delete logs older than: 25000 (keep last 500 entries)

Logs archive folder: C:\Users\User\Server\LogArchive

Keep device history from last: 2 month(s)

Clear selected log database tables: □ Events (logs) table □ Devices statistics/history Clear

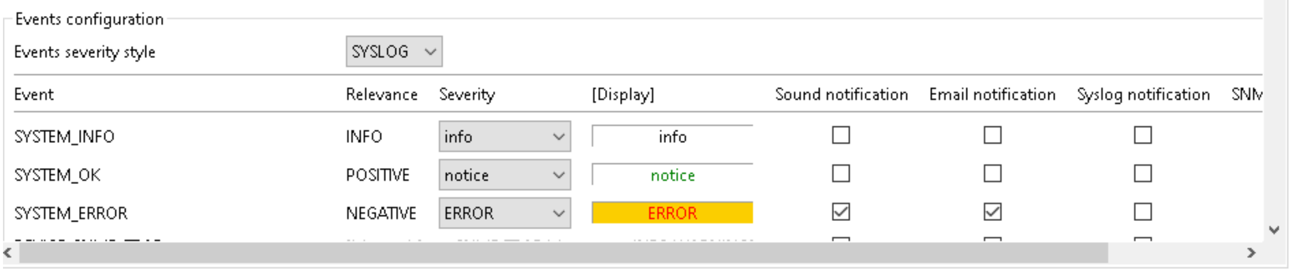
Figure 74. Server Manager - Tab "Syslog/Logs/Events" - Local Logs

- **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.

Event Configuration



Events configuration

Events severity style: SYSLOG

Event	Relevance	Severity	[Display]	Sound notification	Email notification	Syslog notification	SNM
SYSTEM_INFO	INFO	info	info	□	□	□	
SYSTEM_OK	POSITIVE	notice	notice	□	□	□	
SYSTEM_ERROR	NEGATIVE	ERROR	ERROR	☑	☑	□	

Figure 75. 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.
ℹ	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.

  NOTE | Configure the SMTP server on the **Email Notification** tab.

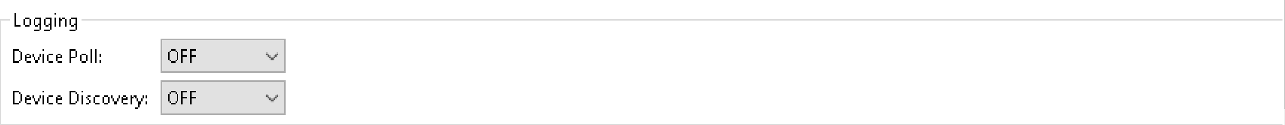
- **Syslog:** The server sends a Syslog message.

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

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

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

Logging



Logging

Device Poll: OFF

Device Discovery: OFF

Figure 76. Server Manager - Tabbed Server Configuration Panel - Syslog/Logs/Events - Logging

- **Device Poll:** From the drop-down list select the minimum log level to log messages on device poll.
- **Device Discovery:** From the drop-down list select the minimum log level to log messages on device discovery.

5.4.4. Database Backup/Restore

IMPORTANT | 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:

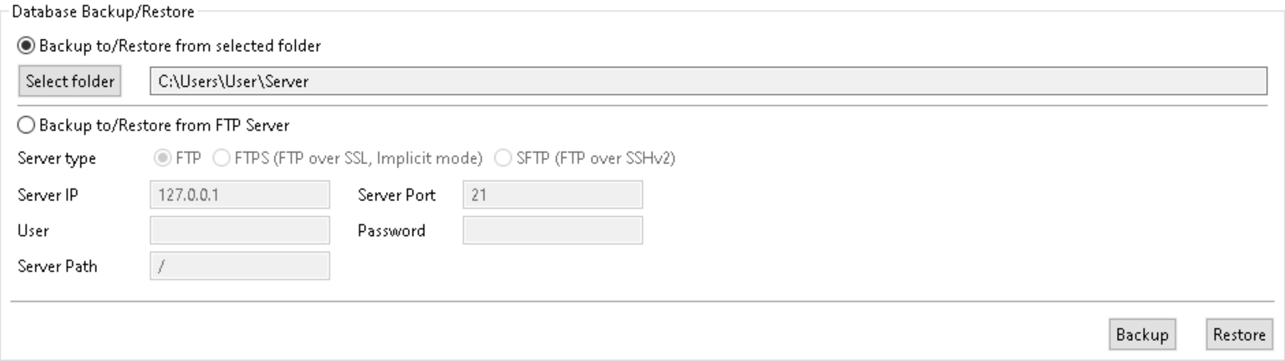
- **Backup Directory:** Configure the backup folder for the database copy.
- **Backups Scheduler:** Configure periodical backups of the database.

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`).

NOTE | 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.



Database Backup/Restore

● Backup to/Restore from selected folder

Select folder: C:\Users\User\Server

○ Backup to/Restore from FTP Server

Server type: ● FTP ○ FTPS (FTP over SSL, Implicit mode) ○ SFTP (FTP over SSHv2)

Server IP: 127.0.0.1 Server Port: 21

User: Password:

Server Path: /

Figure 77. 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.

NOTE | 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`).

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

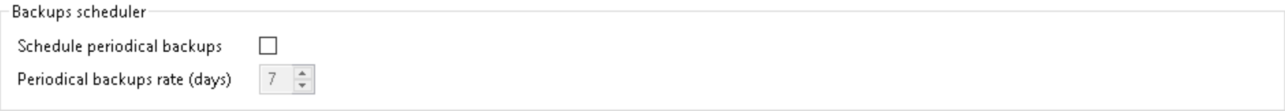
By clicking the button `Backup`, the backup starts automatically.

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.

IMPORTANT | 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.

Backups Scheduler

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



Backups scheduler

Schedule periodical backups ☐

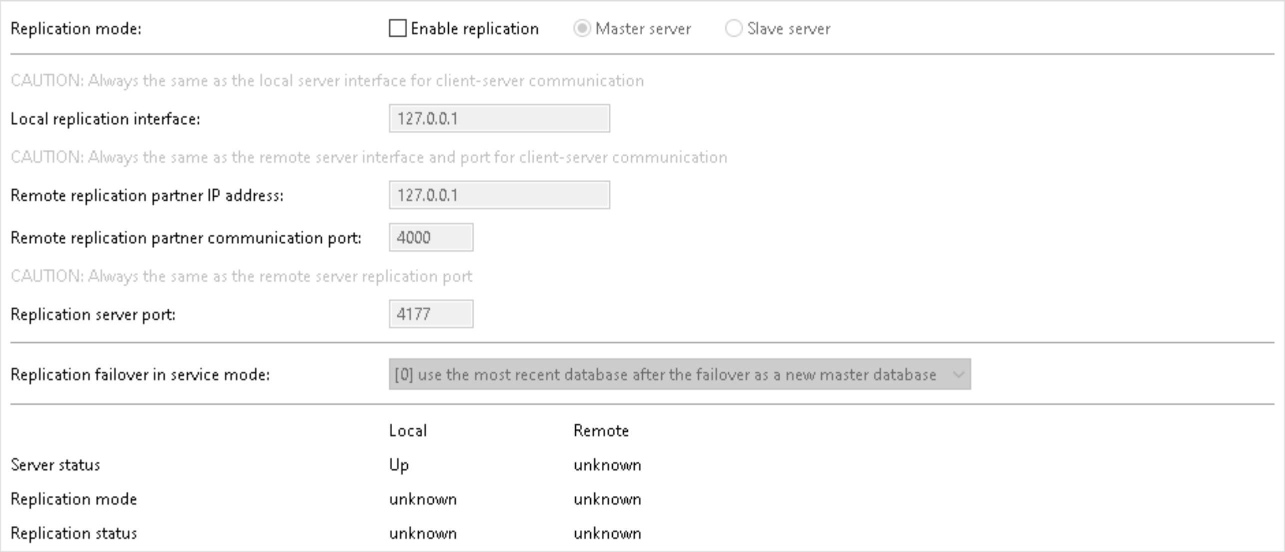
Periodical backups rate (days) 7

Figure 78. 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).

5.4.5. Database Replication

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



Replication mode: ☐ Enable replication ● Master server ○ Slave server

CAUTION: Always the same as the local server interface for client-server communication

Local replication interface: 127.0.0.1

CAUTION: Always the same as the remote server interface and port for client-server communication

Remote replication partner IP address: 127.0.0.1

Remote replication partner communication port: 4000

CAUTION: Always the same as the remote server replication port

Replication server port: 4177

Replication failover in service mode: [0] use the most recent database after the failover as a new master database

	Local	Remote
Server status	Up	unknown
Replication mode	unknown	unknown
Replication status	unknown	unknown

Figure 79. 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.

NOTE 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.

5.4.6. Email Notification

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

General Settings

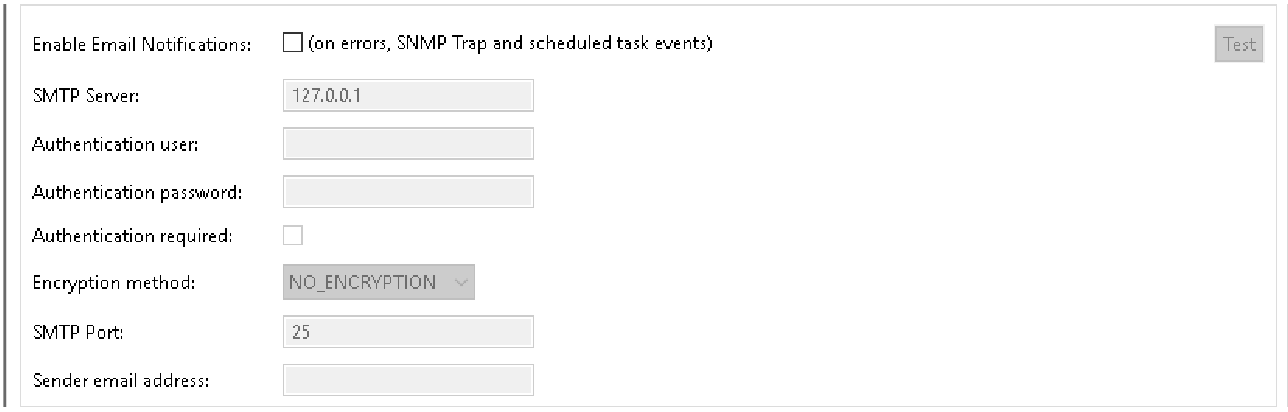

Enable Email Notifications: □ (on errors, SNMP Trap and scheduled task events)
SMTP Server: 127.0.0.1
Authentication user:
Authentication password:
Authentication required: □
Encryption method: NO_ENCRYPTION
SMTP Port: 25
Sender email address:

Figure 80. 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.

NOTE | A valid email account with SMTP access is required.

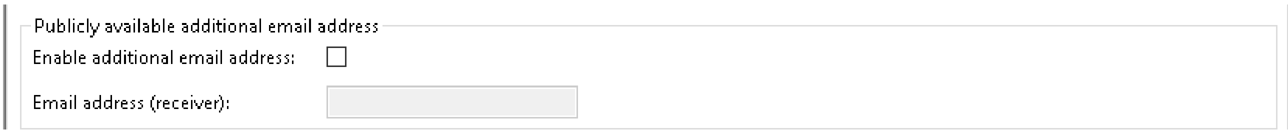
- **SMTP Server:** The address of the SMTP outgoing server (e.g. `smtp.gmail.com`).
- **Authentication user:** Valid user name for this email account.
- **Authentication password:** Valid user password for this email account.
- **Authentication required:** Check this option if the SMTP server requires 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.

  NOTE | 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.

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 81. Server Manager - Tabbed Server Configuration Panel - Email Notification - General Settings

- **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.

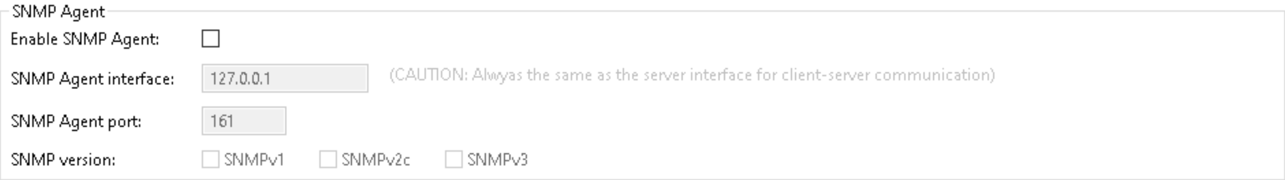
5.4.7. SNMP Agent

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.

SNMP Agent Settings



SNMP Agent

Enable SNMP Agent: ☐

SNMP Agent interface: 127.0.0.1 (CAUTION: Alwyas the same as the server interface for client-server communication)

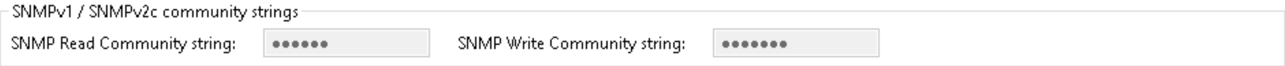
SNMP Agent port: 161

SNMP version: ☐ SNMPv1 ☐ SNMPv2c ☐ SNMPv3

Figure 82. 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.

SNMPv1 / SNMPv2 Community Strings



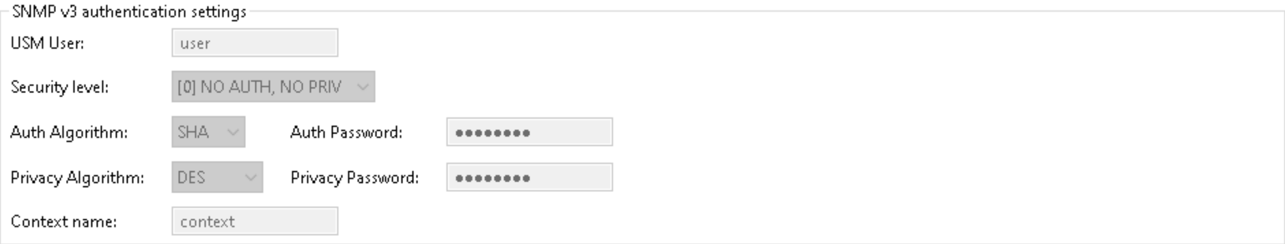
SNMPv1 / SNMPv2c community strings

SNMP Read Community string: ●●●●●● SNMP Write Community string: ●●●●●●●

Figure 83. 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.

SNMPv3 Authentication Settings



SNMP v3 authentication settings

USM User: user

Security level: [0] NO AUTH, NO PRIV

Auth Algorithm: SHA Auth Password: ●●●●●●●●

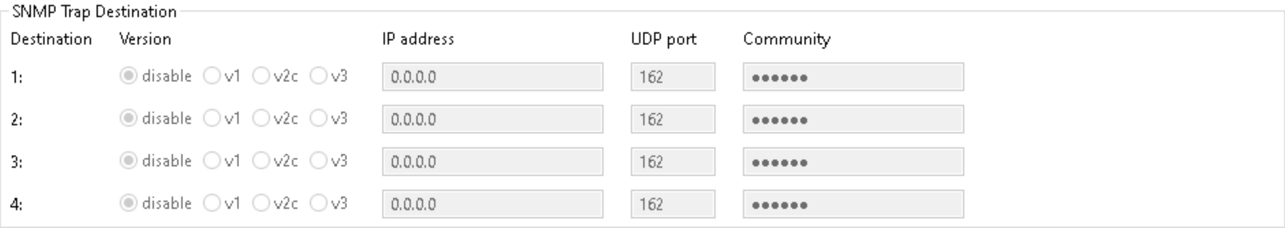
Privacy Algorithm: DES Privacy Password: ●●●●●●●●

Context name: context

Figure 84. 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.

SNMP Trap Destination



SNMP Trap Destination

Destination	Version	IP address	UDP port	Community
1:	● disable ○ v1 ○ v2c ○ v3	0.0.0.0	162	••••••
2:	● disable ○ v1 ○ v2c ○ v3	0.0.0.0	162	••••••
3:	● disable ○ v1 ○ v2c ○ v3	0.0.0.0	162	••••••
4:	● disable ○ v1 ○ v2c ○ v3	0.0.0.0	162	••••••

Figure 85. 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.

5.4.8. Certificates

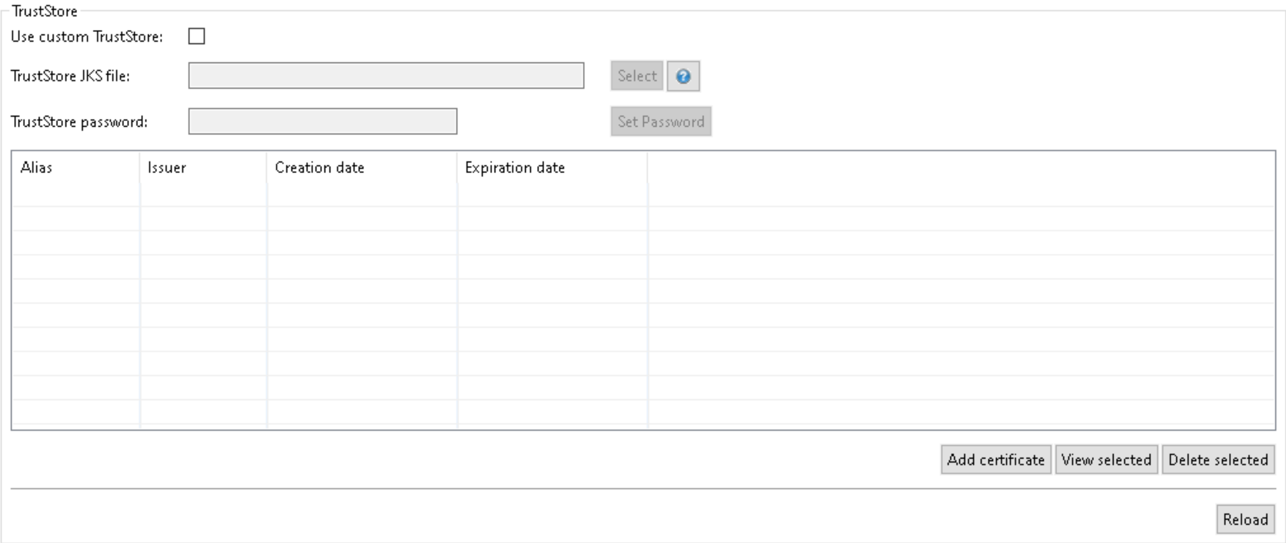


Figure 86. Server Manager - Tab "Certificates" - TrustStore

This tab allows the management of certificates. The tabular overwiew shows a list of existing certificates used for SSL/TLS communcation 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 the 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.

5.5. Server Control Buttons

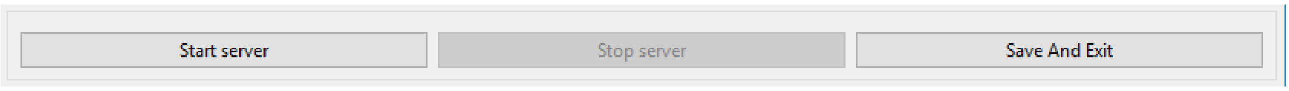


Figure 87. Server Manager - Server Control Buttons

The server control buttons serve the following functions:

Start Server

Starts the server services (HTTP Server, database engine, device data collector and trap listener if configured). After starting the server is available for client components under the configured IP address and port. All the messages from the start-up process are available at the status text field. The server component will show the respective messages if it will fail to start (e.g. if some configured ports will not be available).

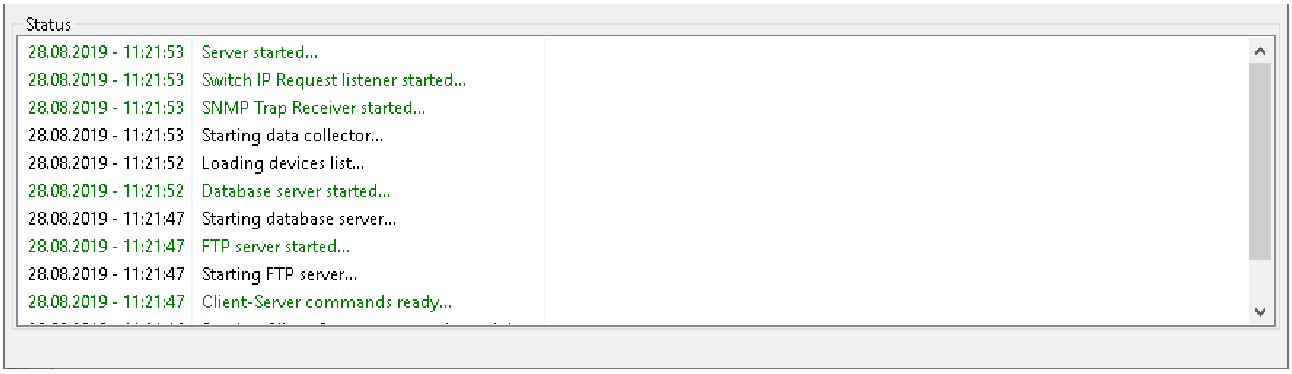
Stop server

Stops the running server instance.

Save And Exit

Saves current settings and closes the Server Manager.

5.6. Status Text Field



```
28.08.2019 - 11:21:53   Server started...
28.08.2019 - 11:21:53   Switch IP Request listener started...
28.08.2019 - 11:21:53   SNMP Trap Receiver started...
28.08.2019 - 11:21:53   Starting data collector...
28.08.2019 - 11:21:52   Loading devices list...
28.08.2019 - 11:21:52   Database server started...
28.08.2019 - 11:21:47   Starting database server...
28.08.2019 - 11:21:47   FTP server started...
28.08.2019 - 11:21:47   Starting FTP server...
28.08.2019 - 11:21:47   Client-Server commands ready...
```

Figure 88. Server Manager - Status Text Field

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

6. NMP Enterprise (Client Component)

NOTE | The client component of NMP Enterprise is available for all users who installed NMP Enterprise and choose the client component in the installation dialogue (for more information see Chapter 2).

This chapter describes the features and operation of the client component.

NOTE | The following descriptions and screenshots refer to the Windows® version of NMP. Because NMP is a Java application based on Eclipse OpenJ9 the GUI appearance does not considerably differ between Windows® and Linux operating systems. The NMP functionality is exactly the same.

Most of the NMP features are common for NMP Professional and the client component of NMP Enterprise. This chapter focuses on the tasks and features specific for the client component.

For detailed information about the features that are not described in this chapter or on how to use NMP Professional please refer to Section 1.2.1.

6.1. Starting NMP Enterprise Client

6.1.1. Starting the Application on Windows®

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

Start › MICROSENS › MICROSENS NMPv2 Client

or

Start › MICROSENS › MICROSENS NMPv2 Client (Debug mode)

The stand-alone client opens with its login dialogue.

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

6.1.2. Starting on Linux Operating Systems

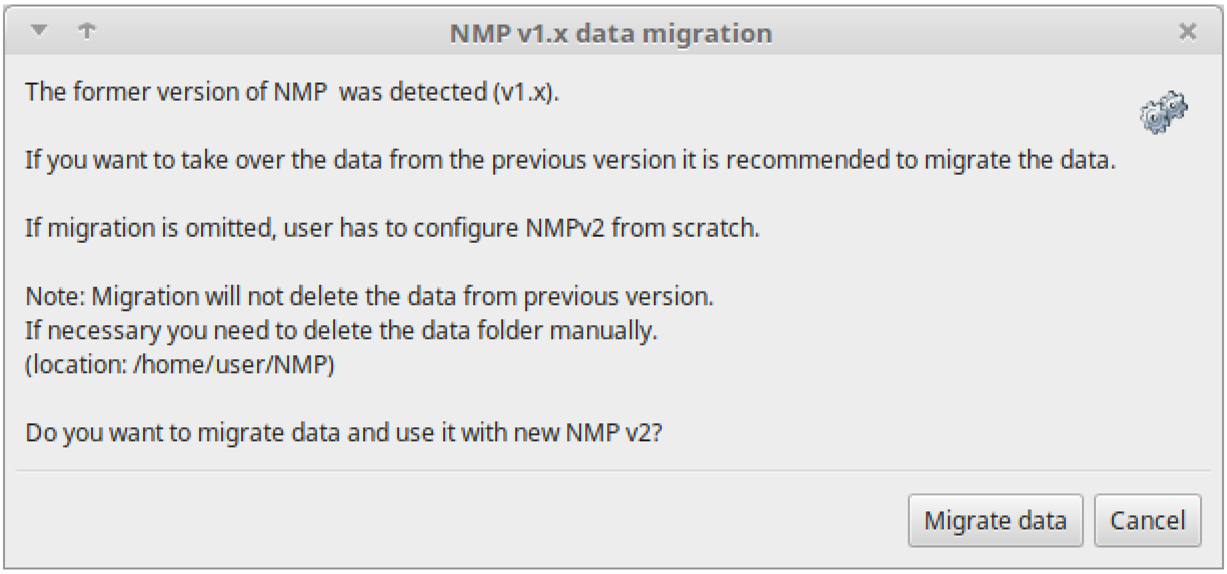
NOTE | The application uses some ports lower than 1024. On UNIX like operating systems only applications started with root rights are able to bind those port. Therefore it is important to start the application with `sudo ./NMP` or `su root ./NMP` (or the respective super user command of your Linux distribution)

For more information please refer to the MICROSENS Knowledge Base on the website www.microsens.com/support.

1. Open a Linux CLI and change to the application's installation directory (e.g. `~/MICROSENS/NMP_Server` and `~/MICROSENS/NMP_Client`).
2. Start the application as super user.

6.1.3. First Program Start

During first start the application checks whether a previous version 1 installation is available. If so, the application asks to migrate the data from this earlier version to version 2.



The former version of NMP was detected (v1.x).

If you want to take over the data from the previous version it is recommended to migrate the data.

If migration is omitted, user has to configure NMPv2 from scratch.

Note: Migration will not delete the data from previous version.
If necessary you need to delete the data folder manually.
(location: /home/user/NMP)

Do you want to migrate data and use it with new NMP v2?

Figure 89. Data Migration from version 1

Click on the button **`Migrate data`** to transfer the data.

The application will create a new directory `~/NMPv2 Server` and `~/NMPv2 Client` in the user's home directory.

6.2. Login via Stand-alone Client

After startup of the stand-alone client entering username and password is obligatory.

Additionally, for the communication with the server instance the client component must have the correct IP address and commands port number of the server instance. All additional configuration parameters (i.e. FTP port, Database Server port) will be automatically obtained from the server instance.

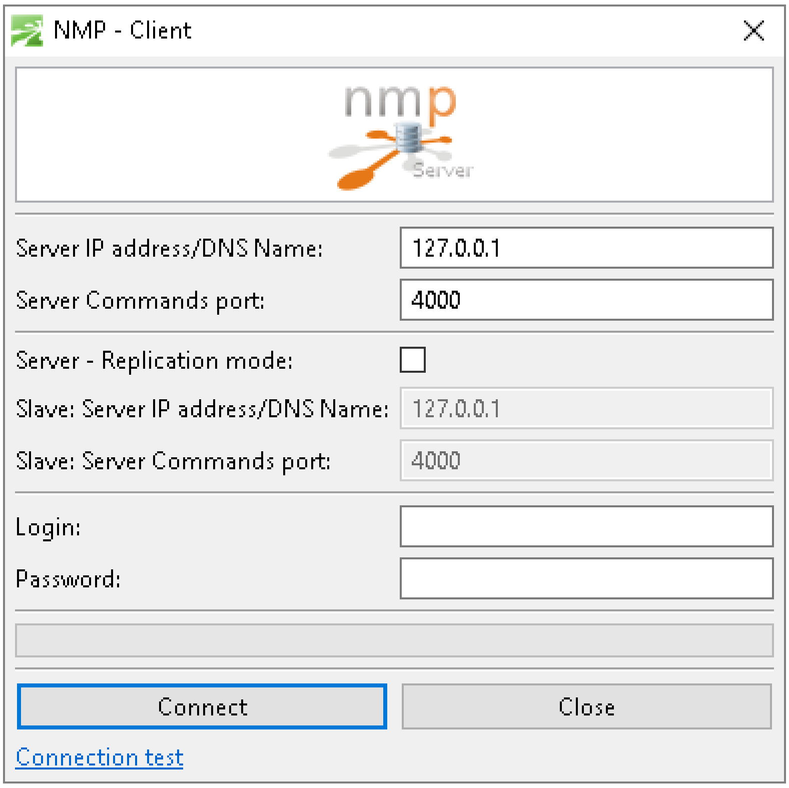
When the server instance runs in master-slave replication mode,additionally specify the slave server's IP address and its commands port number.

The stand-alone client will always try to connect with the master server. In case of a failure (e.g. master server not available) it will try to connect with the specified slave server, using the respective slave server's IP address and commands port.

Login into the client with valid user credentials.

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

- Login: sysadmin
- Password: sysadmin



Server IP address/DNS Name: 127.0.0.1

Server Commands port: 4000

Server - Replication mode: □

Slave: Server IP address/DNS Name: 127.0.0.1

Slave: Server Commands port: 4000

Login:

Password:

Figure 90. Stand-alone Client - Login

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

6.2.1. Login Credentials

A valid login name and the respective password are required to connect to the server instance. Four different default logins are available:

System Administrator

- Login: `sysadmin`
- Password: `sysadmin`

Administrator

- Login: `admin`
- Password: `admin`

Manager

- Login: `manager`
- Password: `manager`

User

- Login: `user`
- Password: `user`

IMPORTANT It is strongly recommended to assign a different password after the first use to prevent unauthorised access to the software.

NOTE Please keep in mind that at least one user with "System Administrator" rights must exist. The client will prevent deleting or changing rights for the last account with "System Administrator" rights.

When logged in with System Administrator rights the client provides a "User Management" tool where it is possible to add, delete or change user accounts.

When closing the client properly, regular logout from the server instance happens immediately. In case of not closing the client application properly (crash of client component, operating system failure), the server instance will automatically logout the respective account after 5 minutes of inactivity.

6.2.2. User Levels and Roles

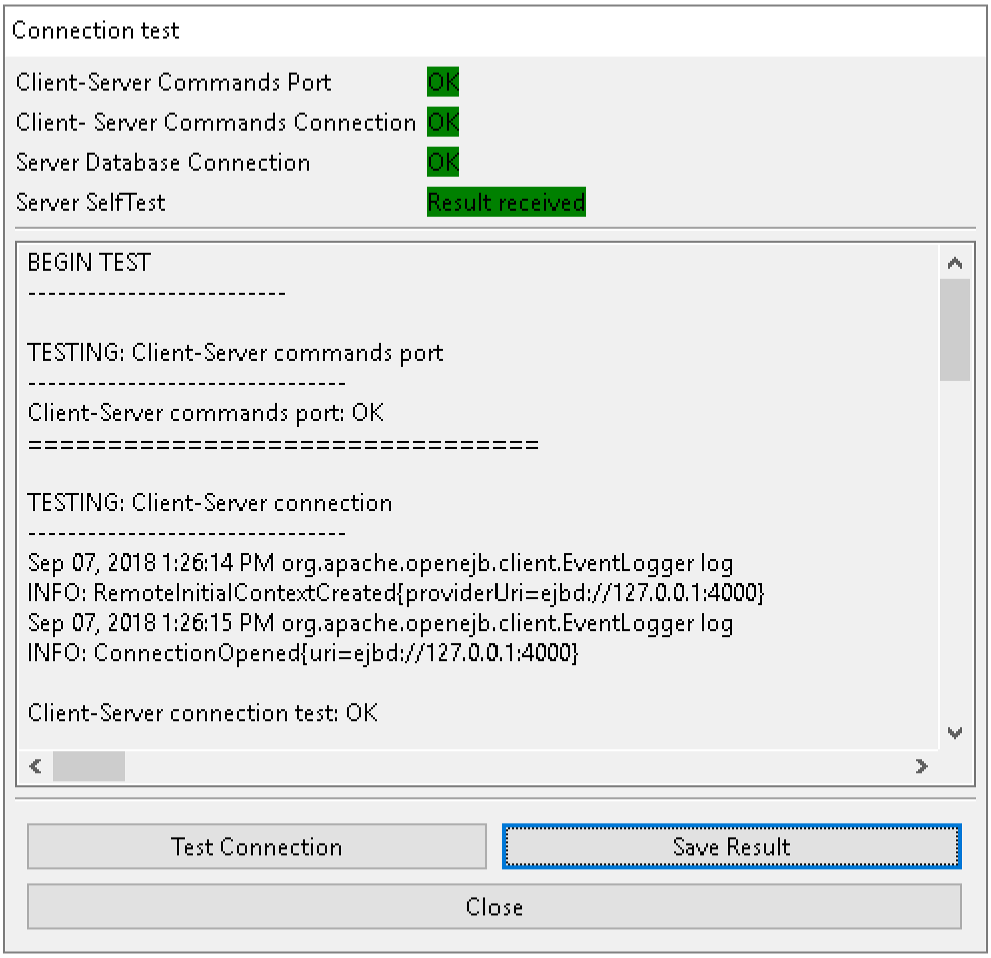
There are four different user levels which grant access to the respective scope of operation:

- **Device data:** Access to information or configuration of one respective device.
- **Device list:** Access to information or configuration of grouped devices.
- **User data:** Access to server accounts
- **Application data:** Access to client and server configuration.

Access	unauth.	User	Manager	Admin	System Admin
Device Data	-	RO	RW	RW	RW
Device List	-	RO	RO	RW	RW
User Data	-	-	-	-	RW
Application Data	-	-	-	-	RW
(RO: read-only, RW: read/write)					

6.2.3. Connection Test

The "Connection test" is available on the login dialogue below the `Connect` button. It allows checking whether the connection between stand-alone client and server instance is possible.


Connection test

Client-Server Commands Port OK
Client- Server Commands Connection OK
Server Database Connection OK
Server SelfTest Result received

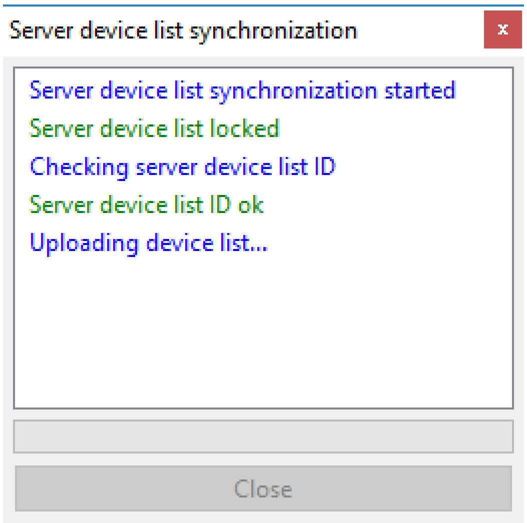
```
BEGIN TEST
-------------------------

TESTING: Client-Server commands port
-------------------------------
Client-Server commands port: OK
=================================

TESTING: Client-Server connection
-------------------------------
Sep 07, 2018 1:26:14 PM org.apache.openejb.client.EventLogger log
INFO: RemoteInitialContextCreated{providerUri=ejbd://127.0.0.1:4000}
Sep 07, 2018 1:26:15 PM org.apache.openejb.client.EventLogger log
INFO: ConnectionOpened{uri=ejbd://127.0.0.1:4000}

Client-Server connection test: OK
```

Figure 91. Stand-alone Client - Connection Test

After clicking the `Test connection` button, the client will automatically check if all necessary services and ports are available on the server instance. The result will be displayed in the dialogue and can be exported as a text file. The server’s IP address and commands port (provided at the login window) are required to perform the test.

6.3. Device List Synchronisation

After the successful login to the server instance the client will synchronise its local device list automatically with the server’s device list.



Server device list synchronization started
Server device list locked
Checking server device list ID
Server device list ID ok
Uploading device list...

Figure 92. Stand-alone Client - Device List Synchronisation

Therefore after the login each client has exactly the same device list identical to the server.

To edit the device list unlock the local device list copy first, which will automatically lock the server device list.

NOTE This operation requires the server's device list not being locked earlier by some other client. In such case a message box will appear with the name of the respective user who locked the server's device list.

To lock or unlock the local device list use **Client/Server › Unlock/Lock device list** in the client menu. It is possible to use the padlock icon on top of the client tree panel.

After applying the changes to devices in the device list, lock the local device list copy.

A dialogue appears that prompts to decide whether client shall synchronise its device list with the server's device list or not.

IMPORTANT If the device list is not synchronised, the client will reload the server's device list and all the local changes will be lost.

Otherwise, the modified device list will be sent to the server. All connected clients (client components of NMP Enterprise installations and Web Clients) will receive the updated device list within one minute subsequently and the server unlocks its device list.

NOTE Only users with administrator or system administrator rights are able to edit the device list (see Section 6.2.2).

The device list synchronisation process is automated. It is possible to synchronise the local or server device list manually. In order to perform a manual device list synchronisation, use the respective menu items via the client's menu item **Client/Server**.

It is possible to import the device list from NMP Professional. To import the respective NMP device list file unlock the client's device list and import the NMP list file using **File › Open**. Lock the local client's device list afterwards.

6.4. Main Menu

This section describes the stand-alone client's specific menu items. For all the menu items which are not described here, please refer to Section 4.4.

6.4.1. Devices List

Lock/Unlock device list

This feature unlocks the device list in order to edit it. The server's device list will be locked and no other user will be able to edit the device list at the same time. After applying the changes, lock the local device list.

The client will synchronise the device list. Afterwards the server unlocks its device list. After this operation all other connected client applications will be synchronised with the updated device list within one minute.

This menu item toggles between locking and unlocking the configuration.

Synchronize Local Client Device List

The client synchronises the local device list automatically with the server copy after every update. However, with this menu item it is possible to synchronise the local device list manually.

Synchronize Remote Server Device List

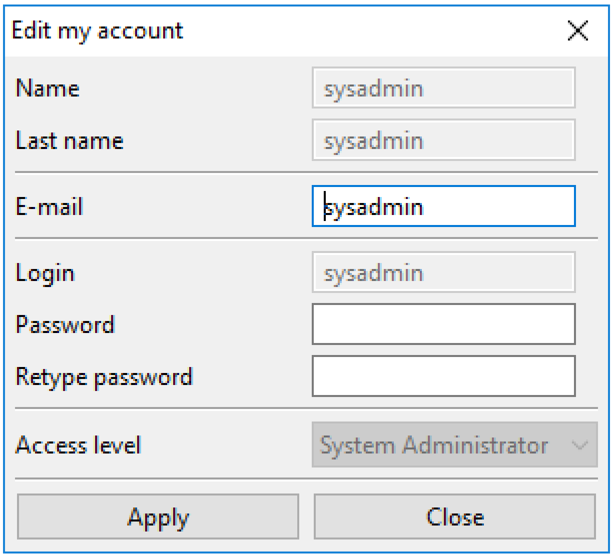
This feature manually synchronises the server's device list with a local copy.

NOTE | The local device list will be overwritten.

6.4.2. User Management

Edit My Account

This feature allows changing password and user email address of the current user.



Edit my account

Name: sysadmin

Last name: sysadmin

E-mail: sysadmin

Login: sysadmin

Password:

Retype password:

Access level: System Administrator

Figure 93. Stand-alone Client - Main Menu - User Management - Edit My Account

NOTE This option is available for all user types. It is not possible to edit accounts of other users or its own access level. If necessary, contact the system administrator.

Change User

This feature allows logging in with another user name and password. This helps to easily log in to the server instance using another account (e.g. with different access rights) without the need to restart the client. After selecting this menu item, the client’s login prompt dialogue appears.

6.4.3. Settings

NMP Settings

In this dialogue specify the configuration settings for NMP application.

Auto-lock device list: ☑

Figure 94. Stand-alone Client - Main Menu - Settings - NMP Settings - Auto-lock

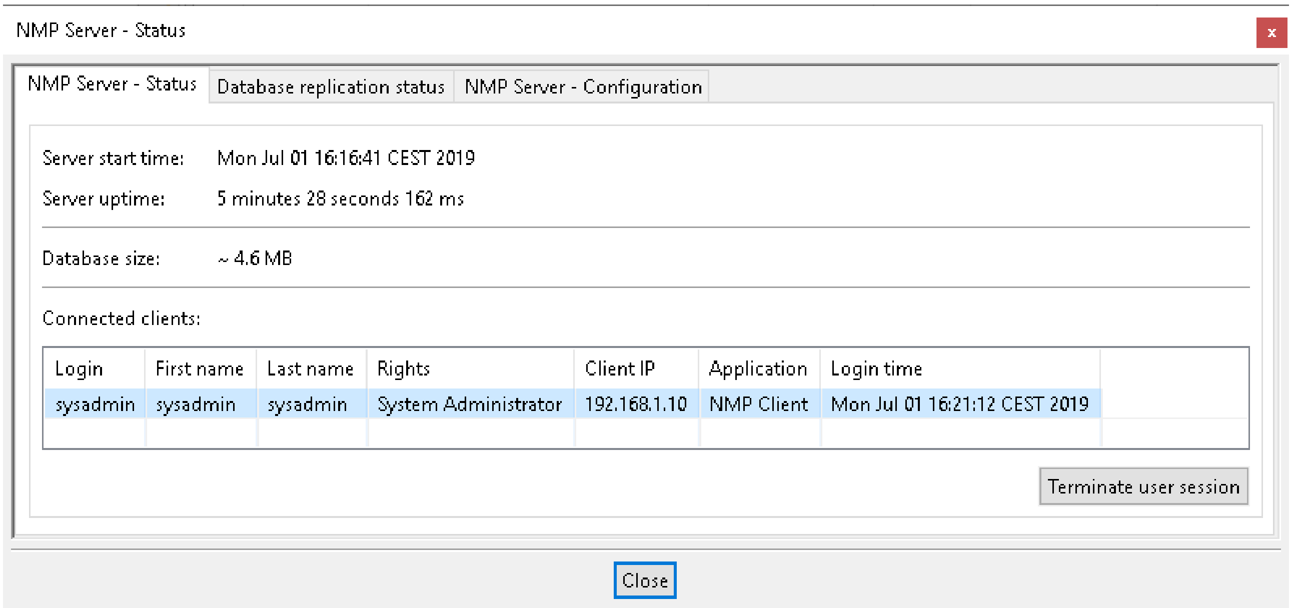
To edit the device list it is necessary to unlock the list within your client instance. This will force the server to lock the device list, so no other client can edit the devices.

After editing, the device list has to be locked again to enable editing the devices for other clients. This option controls how locking the device list happens:

- **checked:** The device list is locked automatically after 5 minutes of inactivity (default).
- **unchecked:** The device list has to be locked manually.

Server Status

This feature allows checking the current server instance status. Three different tabs show the following information:



Server start time: Mon Jul 01 16:16:41 CEST 2019

Server uptime: 5 minutes 28 seconds 162 ms

Database size: ~ 4.6 MB

Connected clients:

Login	First name	Last name	Rights	Client IP	Application	Login time
sysadmin	sysadmin	sysadmin	System Administrator	192.168.1.10	NMP Client	Mon Jul 01 16:21:12 CEST 2019

Figure 95. Stand-alone Client - Main Menu - Settings - Server Status

Server - Status

Contains information about the server’s start time and uptime, the database size and the currently connected clients. It is possible to select and terminate a user session.

NOTE It’s not possible to terminate its own user session.

Database replication status

Contains information about the database replication configuration and status.

Server - Configuration

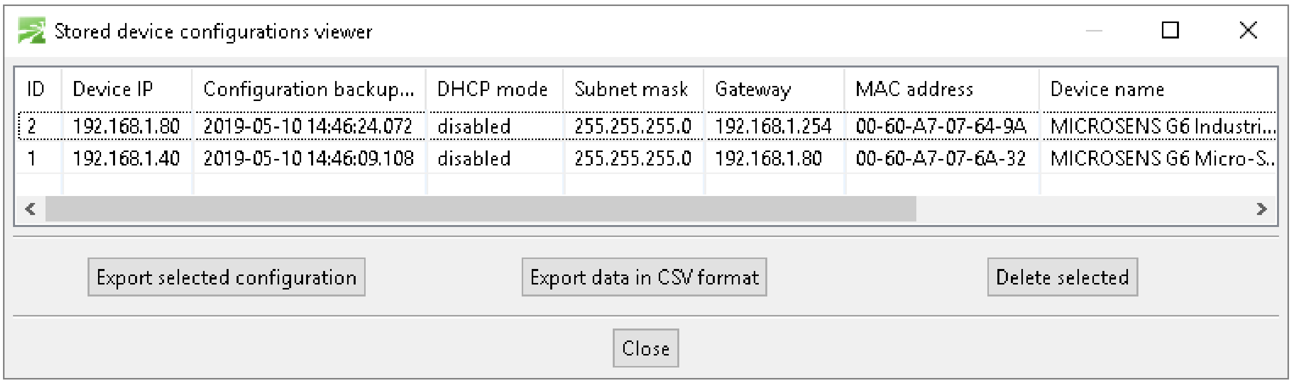
Contains extensive information about the server’s configuration.

NOTE This menu item is exclusively available for users with "System Administrator" access rights.

6.4.4. Tools

Stored Device Configurations Viewer

This tool allows viewing and deleting the previously saved device setups.



Stored device configurations viewer

ID	Device IP	Configuration backup...	DHCP mode	Subnet mask	Gateway	MAC address	Device name
2	192.168.1.80	2019-05-10 14:46:24.072	disabled	255.255.255.0	192.168.1.254	00-60-A7-07-64-9A	MICROSENS G6 Industri...
1	192.168.1.40	2019-05-10 14:46:09.108	disabled	255.255.255.0	192.168.1.80	00-60-A7-07-6A-32	MICROSENS G6 Micro-S...

Figure 96. Stand-alone Client - Main Menu - Tools - Stored Device Config Viewer

Device configurations can be saved manually by using the **Device configuration load/save** menu item from the tree context menu (see Section 4.8) or automatically by defining the "Scheduled configuration backup" task (see Section 4.4.5.3).

By clicking the button `Export selected configuration` an export of the configuration file from the database is possible for later use (e.g. to send the setup to a device with NMP Professional).

DHCP Autoconfiguration (G5)

DHCP offers the setup of a device during the DHCP Request. The firmware of MICROSENS G6 (and newer) devices already supports this function.

The DHCP Autoconfiguration tool of the client component allows using this function with MICROSENS G5 devices.

For more information about using DHCP auto-configuration please refer to Section 7.5.

NOTE DHCP auto-configuration only works with MICROSENS G5 (and prior) devices. When trying to use it with G6 devices, NMP displays a corresponding message.

6.4.5. Window

NOTE This menu item is only visible with System Administrator access rights!

Switch Perspective

With System Administrator access rights it is possible to switch between two perspectives:

- **Network Administration:** Use this perspective to configure and survey the corporate network. This is the default perspective when starting the stand-alone client.
- **User Administration:** Use this perspective to manage users. For more information about User Administration please refer to Section 7.18.

6.5. Main Menu Toolbar

The main menu toolbar provides quick access to the most important and most used commands.

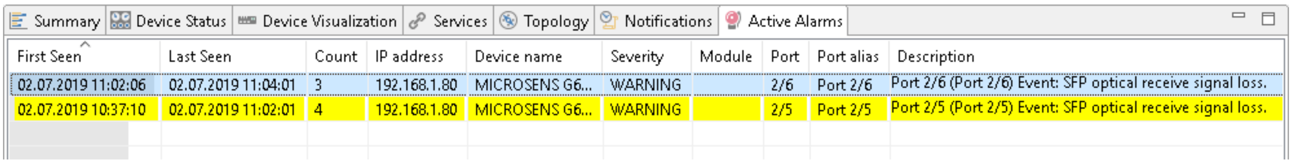
Icon	Task	Main Menu Item / Detailed Information
📂	Load device list	**File › Open**
💾	Save device list	**File › Save**
🔄	Refresh selected devices	**Device List › Refresh selected**
➕	Add new device	**Device List › Add new device**
⊕	Add new subgroup	**Device List › Add new subgroup**
🔭	Device auto discovery	**Discovery**
📋	Create Inventory List	**Tools › Inventory**
🔍	Device search tool	**Tools › Switch search tool**
📅	Scheduled tasks viewer	**Tools › Scheduled tasks viewer**
🔒	Configuration locked	**Devices List › Unlock Configuration**
🔓	Configuration unlocked	**Devices List › Lock Configuration**
🔄	Force poll selected	**Devices List › Force poll selected**

NOTE You can configure the position and icon size of the toolbar icons in the main menu under **Window › Toolbar Position** and **Window › Toolbar Icon Size**.

6.6. Tabbed Data Panel

This section describes the client component’s specific tabbed data panel items. For all the items which are not described here, please refer to Section 4.7.

6.6.1. Active Alarms



First Seen	Last Seen	Count	IP address	Device name	Severity	Module	Port	Port alias	Description
02.07.2019 11:02:06	02.07.2019 11:04:01	3	192.168.1.80	MICROSENS G6...	WARNING		2/6	Port 2/6	Port 2/6 (Port 2/6) Event: SFP optical receive signal loss.
02.07.2019 10:37:10	02.07.2019 11:02:01	4	192.168.1.80	MICROSENS G6...	WARNING		2/5	Port 2/5	Port 2/5 (Port 2/5) Event: SFP optical receive signal loss.

Figure 97. Stand-alone Client - Tabbed Data Panel - Active Alarms

This panel is helpful to view some important SNMP traps at first glance.

For more information on how to use this tab please refer to Section 7.19.

6.7. Context Menu

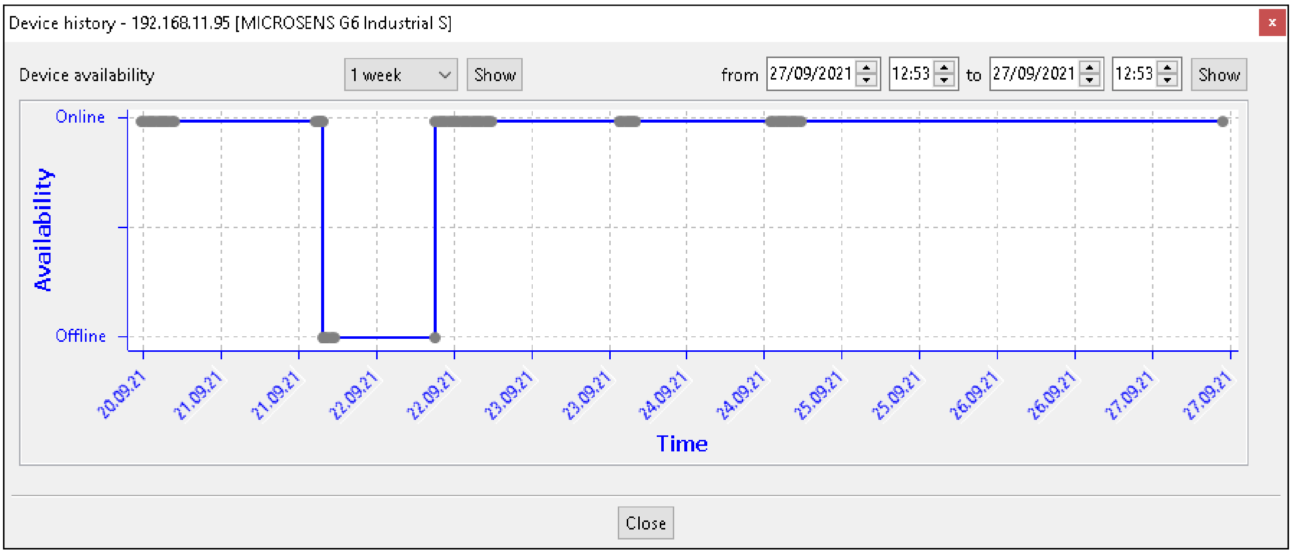
Additionally to NMP Professional the context menu of the client component offers some more menu items.

For all the context menu items which are not described here, please refer to Section 4.8

6.7.1. Device Context Menu

Device History

The server instance logs information about the managed devices' availability. To view the respective device’s availability history click on **Device history › Device history charts**. The device’s history chart appears in a separate dialogue.


Device history - 192.168.11.95 [MICROSENS G6 Industrial S]

Device availability: 1 week

from 27/09/2021 12:53 to 27/09/2021 12:53

Figure 98. Stand-alone Client - Device Context Menu - Device History Chart

The tool allows determining the history of the last (predefined) time periods between 30 minutes and one year (select specific period from drop-down list).

The time period of 24 hours is the default.

It is also possible to specify the date and time range manually to see more details within the selected range.

NOTE | The device history charts are available exclusively for MICROSENS switches.

Clear Device History

Use this menu entry to clear the device history.

NOTE | Clearing the device history requires administrator or system administrator access rights!

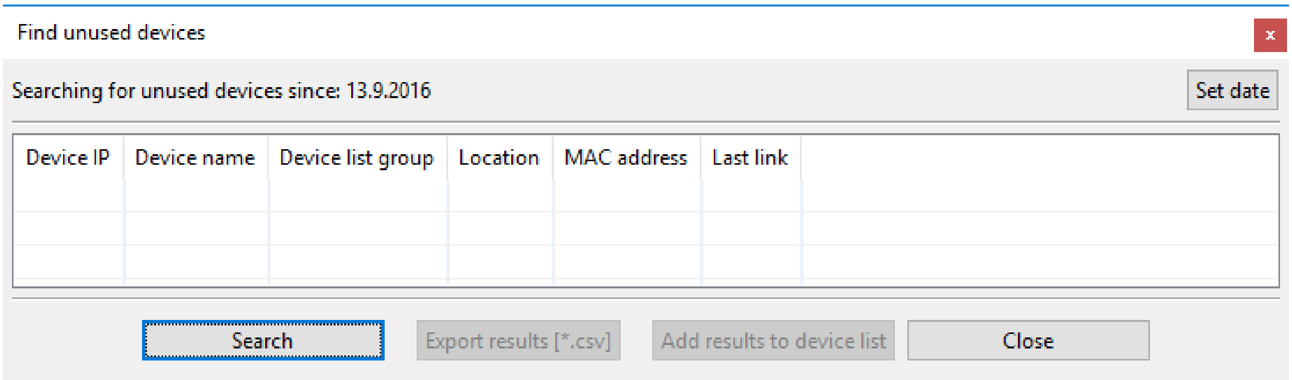
Show device logs

This feature opens the tab **Notifications** in the tabbed data panel and sets the notification filter to the IP address ("Source ID equals") of the selected device.

6.7.2. Group Context Menu

Find unused devices

This feature allows finding unused MICROSENS devices. "Unused devices" are devices without active link on client ports (no uplink/downlink port) for a specific period of time.



Searching for unused devices since: 13.9.2016

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

Figure 99. Stand-alone Client - Find Unused Devices

All found unused devices are listed in a table. To export this list to a `.csv` file click on the button **`Export results \[*.csv]`**.

To add the search results to the device list as an additional group "Unused devices" click on the button **`Add results to device list`**.

7. Application Instructions

The following sections describe how to use the application in every day tasks.

NOTE Some tasks can be executed by both NMP Professional and NMP Enterprise whereas some tasks are exclusively available by only one of the NMP variants. At the beginning of every section a respective note indicates, whether that is the case in this section.

7.1. Adding New Devices Manually

NOTE The steps for adding new devices manually is identical for both NMP Professional and NMP Enterprise.

1. Open **Devices List** › **Add new device** in the main menu. Alternatively, in the device list tree view right-click the group you want add the new device and select **Add new device** in the group context menu.
2. In the opening dialogue enter the respective device information.

   NOTE The preset values in this dialogue correspond to the default values set for new devices under **Devices List** › **Default New Device Settings**. The individual parameters can be changed for a new device if they differ from the default values.

   IP Address

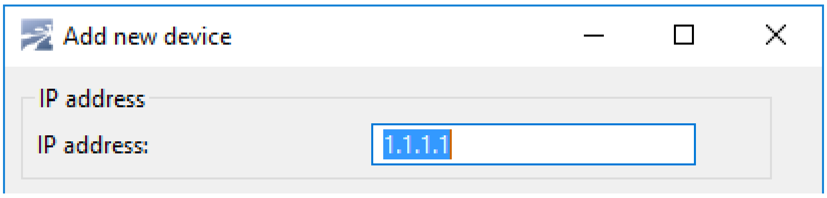
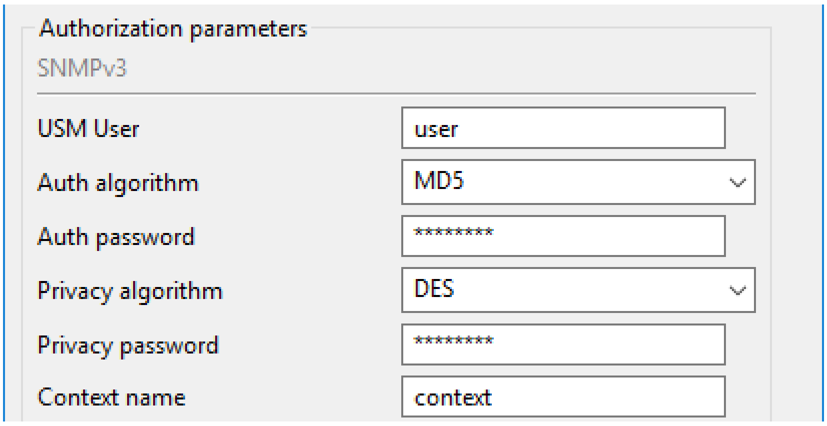
   
   Add new device
   IP address
   IP address: 1.1.1.1

   Figure 100. NMP - New Device - IP Address

   - **IP address:** The IP address of the new device is necessary for adding this device to the selected group.

   SNMPv3 Settings



Authorization parameters

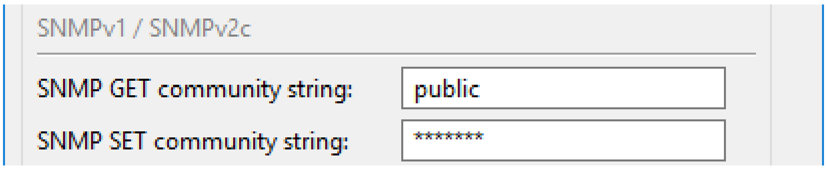
SNMPv3

USM User	user
Auth algorithm	MD5
Auth password	********
Privacy algorithm	DES
Privacy password	********
Context name	context

Figure 101. NMP - New Device - Authorisation - SNMPv3

- **USM User:** User name string for User-based Security Model (USM) device access
- **Authentication algorithm:** The type of protocol used for message authentication; available options are:
  - NoAuth – no user authentication
  - MD5 – the HMAC-MD5-96 authentication protocol
  - SHA – the HMAC-SHA-96 authentication protocol
- **Authentication password:** The authentication key for use with the authentication algorithm
- **Privacy algorithm:** The type of privacy protocol which is used for message encryption; available options:
  - NoPriv – no privacy
  - DES – the Data Encryption Standard or Algorithm
  - AES – the Advanced Encryption Standard, 128 bit key size
  - AES192 – the Advanced Encryption Standard, 192 bit key size
  - AES256 – the Advanced Encryption Standard, 256 bit key size
  - 3DES – the Triple Data Encryption Standard or Algorithm (TDEA)
- **Privacy password:** The privacy key for use with the privacy algorithm
- **Context name:** Context string requesting access

SNMPv1/v2 Settings



SNMPv1 / SNMPv2c

SNMP GET community string:	public
SNMP SET community string:	*******

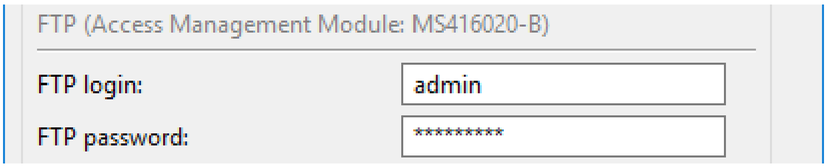
Figure 102. NMP - New Device - Authorisation - SNMPv1/2c

- **Default SNMP GET community string:** Community string for read operations

- **Default SNMP SET community string:** Community string for write operations

FTP Settings

NOTE: This section applies to the SNMP management module MS416020-B exclusively and is available for downwards compatibility with this device.



FTP (Access Management Module: MS416020-B)

FTP login: admin

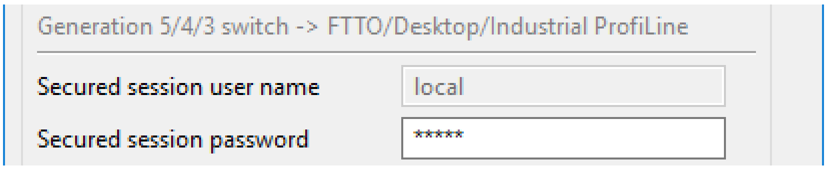
FTP password: *********

Figure 103. NMP - New Device - Authorisation - FTP

- **Default FTP login:** Login for file transfer protocol (FTP) for firmware updates
- **Default FTP password:** Password for file transfer protocol (FTP) for firmware updates

Micro Switch (G5 and older)/Industrial Switch

NOTE: This section applies only to the G5 (and older) Micro Switches and to the ProfiLine Industrial Switches.



Generation 5/4/3 switch -> FTTO/Desktop/Industrial ProfiLine

Secured session user name: local

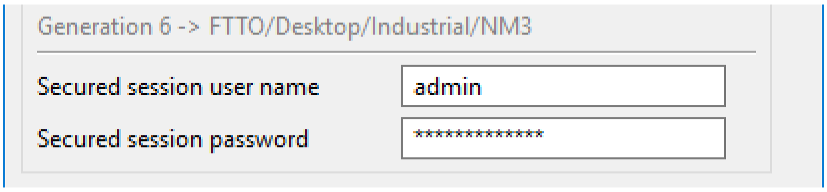
Secured session password: *****

Figure 104. NMP - New Device - Authorisation - Generation 5/4/3

- **Secured session user name:** User name needed to start the secured data exchange between NMP and device
- **Secured session password:** Password needed to start the secured data exchange between NMP and device

Micro Switch (G6)/ Industrial Switch (G6)

NOTE: This section applies to Micro Switches (G6) and to Industrial Switches (G6).



Generation 6 -> FTTO/Desktop/Industrial/NM3

Secured session user name: admin

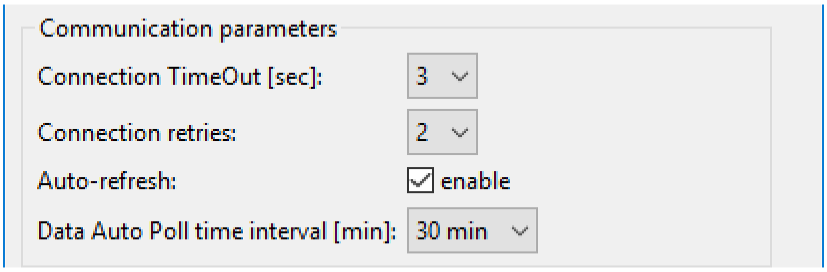
Secured session password: *************

Figure 105. NMP - New Device - Authorisation - Generation 6

- **Secured session user name:** User name needed to start the secured data exchange between NMP and device
- **Secured session password:** Password needed to start the secured data exchange between NMP and device

Depending on the type of device the authorisation settings can be adapted if they differ from the defaults.

Communication Parameters



Communication parameters

Connection TimeOut [sec]: 3

Connection retries: 2

Auto-refresh: ☑ enable

Data Auto Poll time interval [min]: 30 min

Figure 106. NMP - New Device - Communication

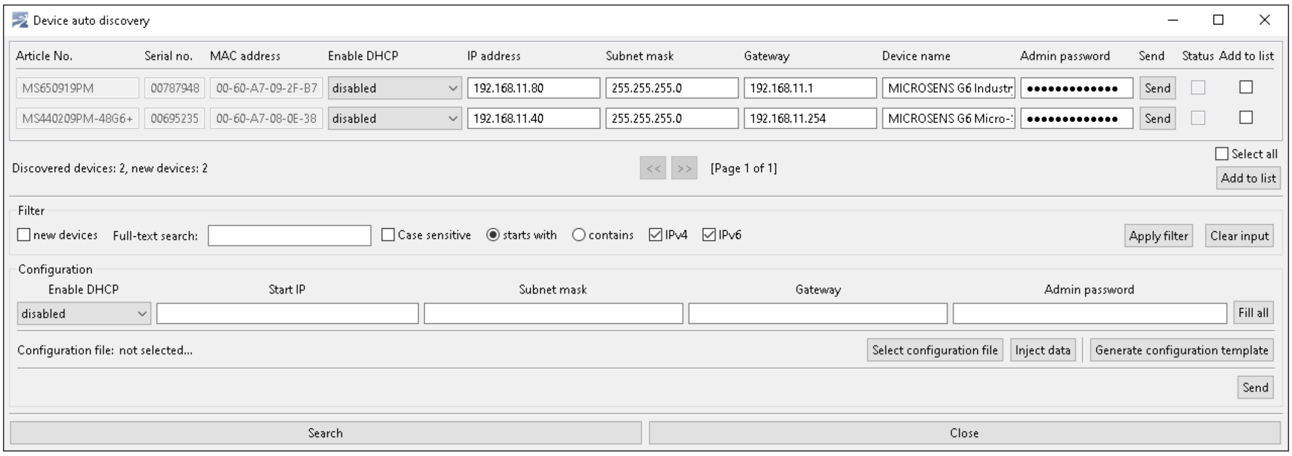
- **Connection TimeOut:** How much time in seconds NMP should wait for the device to respond.
- **Connection retries:** How many times NMP should try to reconnect with the device in the case of a failure.
- **Auto refresh:** Enables automatic data refreshing. When checked NMP polls device data of every managed device within the time interval specified in the following.
- **Data Auto Poll time interval:** The time interval NMP should wait before downloading and updating device data. Time intervals from 1 minute up to 24 hours are adjustable.

3. Click on the button `Add device` to insert the new device into the selected group. Click on the button `Close` to discard the entries.

7.2. Adding New Devices with Device Auto Discovery

> **NOTE** Auto discovery is available for both NMP Professional and NMP Enterprise.

To use "Switch Auto Discovery" start this function under **Device › Device Auto Discovery** in the main menu. The following dialogue opens:



Article No.	Serial no.	MAC address	Enable DHCP	IP address	Subnet mask	Gateway	Device name	Admin password	Send	Status	Add to list
MS650919PM	00787948	00-60-A7-09-2F-B7	disabled	192.168.11.80	255.255.255.0	192.168.11.1	MICROSENS G6 Industr	•••••••••••••	Send	□	□
MS440209PM-48G6+	00695235	00-60-A7-08-0E-38	disabled	192.168.11.40	255.255.255.0	192.168.11.254	MICROSENS G6 Micro-:	•••••••••••••	Send	□	□

Discovered devices: 2, new devices: 2 [Page 1 of 1] □ Select all

Filter
□ new devices Full-text search: □ Case sensitive ● starts with ○ contains ☑ IPv4 ☑ IPv6

Configuration
Enable DHCP: disabled Start IP Subnet mask Gateway Admin password

Configuration file: not selected...

Figure 107. *NMP Professional - Device Auto Discovery*

NOTE If no device is detected, this dialogue will not appear.

The "Switch Auto Discovery" feature allows searching for MICROSENS switches with an unknown or without an IP address. The search results contain information of a device’s Article Number, Serial Number, MAC address and the current IP settings. The editable fields allow for the configuration of the IP settings and the device’s name. The new configuration can be applied to each device by clicking the button **Send** next to the respective device entry.

The corresponding status field then changes its colour:

- yellow: The configuration is being applied.
- green: The changes have been correctly applied.
- red: In case of failure the yellow indicator will turn red. In such cases try to resend the new configuration by clicking on the button **Send**.

7.2.1. Duplicated IP addresses

The "Switch Auto Discovery" feature has the ability to detect duplicated IP addresses. In this case a "One or more duplicate IP addresses detected!" warning message will be displayed. Additionally, the duplicated IP addresses are marked red in the list.

7.2.2. Address filter

Discovered devices can also be filtered in the dialogue’s "Filter" section.

7.2.3. Automatic configuration

All parameters for all discovered devices can be filled in automatically. To do this fill in the devices' IP parameters located in the "Configuration" section (DHCP, Start IP, Subnet mask and Gateway IP). The button **`Fill all`** applies consecutive IP settings to the search results.

There is also an option to deploy a `.csv` file which contains the new configuration. Hitting the `Generate configuration template` button generates the `.csv` file which then should be filled with proper data. The `.csv` file must contain 6 columns in predefined order. The first column must contain the valid MAC address of an existing device (used as device ID), which should be re-configured. The remaining columns contain the IP settings and the name which should be assigned to the device.

An entry of the csv file should look as follows:

```
//MAC ADDRESS FORMAT: XX-XX-XX-XX-XX-XX
//DHCP = 0 -> DHCP DISABLED
//DHCP = 1 -> DHCP ENABLED
//DHCP = 2 -> DHCP WITH SCRIPT ENABLED

MAC;DHCP;IP;MASK;GATE;NAME;
00-00-00-00-00-00;0;192.168.1.100;255.255.255.0;192.168.1.1;Test Name
```

NOTE As the semicolon is used to separate the columns it is not allowed to use a semicolon as part of the device name.

When the configuration file is completed and ready for deployment, select it with `Select configuration file` and then assign the previously defined new values to devices discovered by the tool. NMP will assign the configuration to these devices by using the device MAC address as device ID.

At the end, use the button `Send` order to send the new configuration to all listed devices at once.

7.3. Device Configuration in General

NOTE Device configuration happens identically for both NMP Professional and NMP Enterprise.

The configuration of the respective device can be accessed via the respective device’s context menu and for some device types in the tabbed data panel on the tab **Device Status**.

The following device configuration actions can be performed via the device context menu:

- **Settings:** The settings sub menu items are device type-dependent. Please refer to the respective device manual for more details.
- **Device configuration load/save**
- **Master configuration**
- **Update firmware**
- **Device passwords changer**
- **Applications**

- **Install/uninstall applications**
- **Communication parameters**
- **Device name:** This feature allows changing the device’s name displayed in the device tree view. NMP then asks whether the device name stored in the device should also be changed. Usually this is recommended.

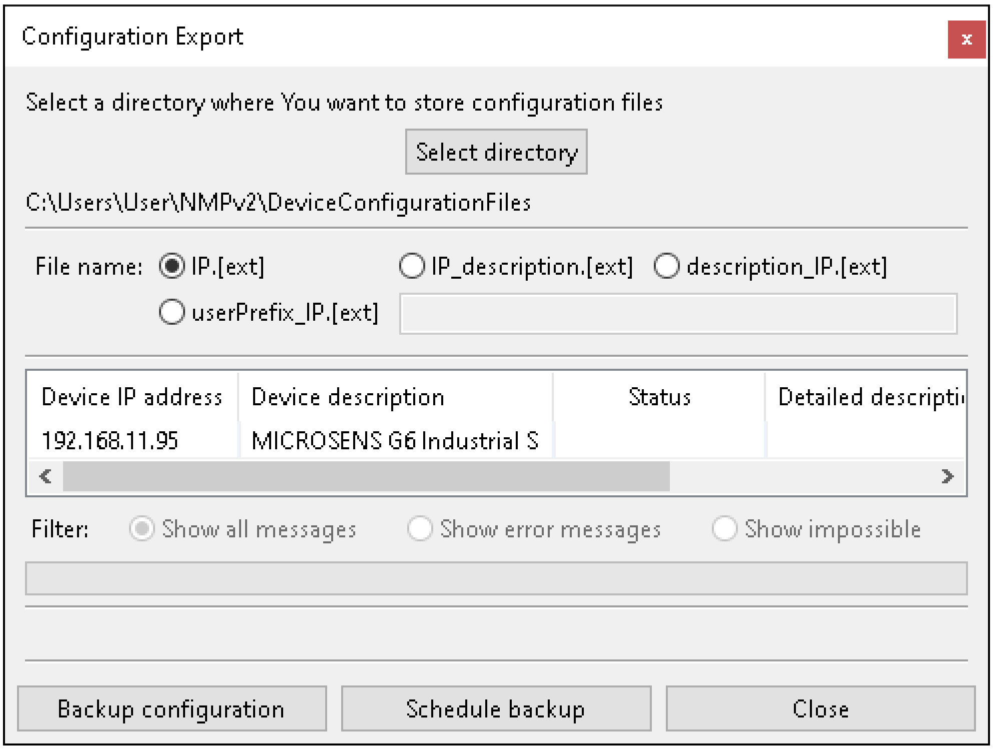
NOTE Keep in mind that the device name string length in the device is limited to 128 characters. The device name length is limited to 25 characters in NMP.

7.4. Device Configuration via Configuration Files

NOTE Device configuration happens identically for both NMP Professional and NMP Enterprise.

7.4.1. Export Configuration

It is possible to save a device’s configuration into an `.XML` configuration file for backup or device replacement purposes. For saving the device’s configuration mark the respective device in the device list tree view and choose **Device Configuration Load/Save › Save configuration settings** from the device context menu. The following dialogue opens:



Configuration Export

Select a directory where You want to store configuration files

C:\Users\User\NMPv2\DeviceConfigurationFiles

File name: ● IP.[ext] ○ IP_description.[ext] ○ description_IP.[ext] ○ userPrefix_IP.[ext]

Device IP address	Device description	Status	Detailed descripti
192.168.11.95	MICROSENS G6 Industrial S		

Filter: ● Show all messages ○ Show error messages ○ Show impossible

Figure 108. NMP - Device Context Menu - Configuration Export

Configuration files for each device are saved using the following file syntax:

- `IP.[ext]` or
- `IP_description.[ext]` or
- `description_IP.[ext]` or
- `userPrefix_IP.[ext]`,

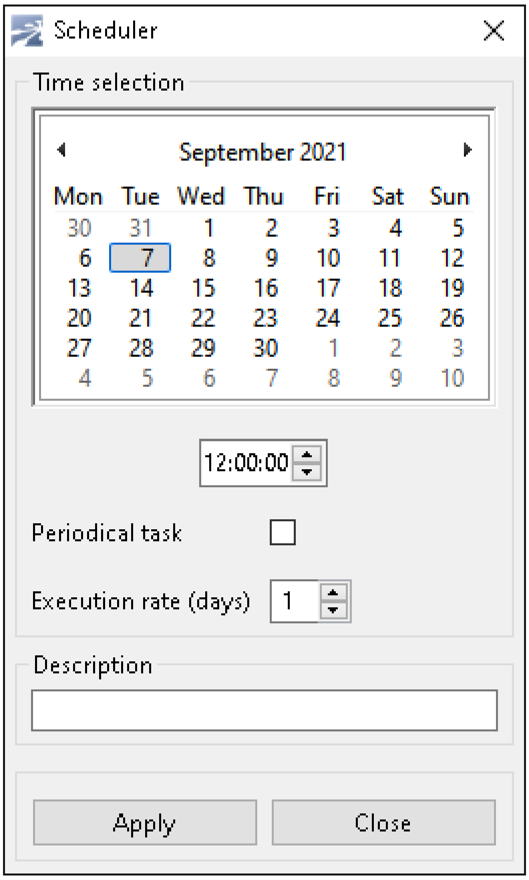
with the following substitutions:

- `IP`: The IP address of the device
- `description`: The device description
- `userPrefix`: String defined by the user

Click on the button **`Select Directory`** to specify the directory where you want to save the file.

Click on the button **`Backup configuration`** to save the configuration file.

Click on the button **`Schedule backup`** to configure a regular backup task.



Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

12:00:00

Periodical task □

Execution rate (days) 1

Description

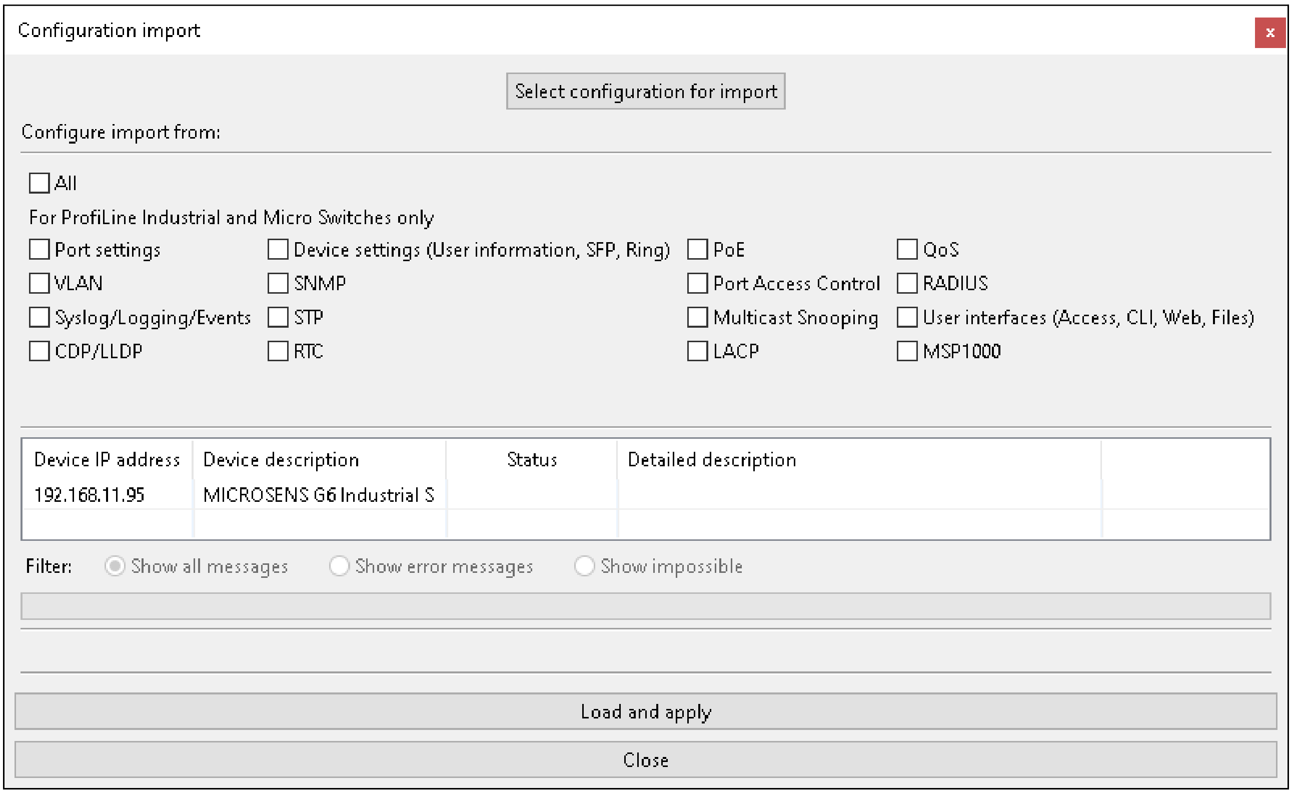
Figure 109. NMP - Scheduler - Edit Task

Define a task which will be executed once (at a defined time) or periodically at the configured execution rate.

NOTE All scheduled tasks can be deleted or modified using the "Scheduled Tasks Viewer" tool (see Section 4.4.5.3).

7.4.2. Restore Configuration

For restoring a device's configuration mark the respective device in the device list tree view and choose **Device Configuration Load/Save › Load configuration settings** from the device context menu. The following dialogue opens:



Configuration import

Select configuration for import

Configure import from:

□ All

For ProfiLine Industrial and Micro Switches only

□ Port settings
□ VLAN
□ Syslog/Logging/Events
□ CDP/LLDP
□ Device settings (User information, SFP, Ring)
□ SNMP
□ STP
□ RTC
□ PoE
□ Port Access Control
□ Multicast Snooping
□ LACP
□ QoS
□ RADIUS
□ User interfaces (Access, CLI, Web, Files)
□ MSP1000

Device IP address	Device description	Status	Detailed description
192.168.11.95	MICROSENS G6 Industrial S		

Filter: ● Show all messages ○ Show error messages ○ Show impossible

Load and apply

Close

Figure 110. NMP - Device Context Menu - Configuration Import

NOTE When loading a single configuration backup to a group of G6 devices, it is possible to select whether the SNMPv3 engine ID should be taken from this backup. Otherwise, it is generated from the MAC address of each individual target device.

Hitting the button `Load and apply` applies the imported configuration to the device.

Please refer to the device-dependent menu items in the device documentation.

7.5. Switch DHCP Auto-Configuration

NOTE DHCP Autoconfiguration is exclusively available with NMP Enterprise.

The Switch DHCP Auto-Configuration function is used to update firmware and configuration of MICROSENS Micro Switch (G5 and older) and Industrial switches.

With DHCP option and DHCP configuration request enabled, these devices are able to receive additional information from the DHCP server along with IP settings.

NOTE	The "DHCP Auto-Configuration" feature only works with MICROSENS G5 (and prior) devices. The firmware of MICROSENS G6 devices already supports this function natively. When trying to use it with G6 devices, NMP displays a corresponding error message.

7.5.1. Switch DHCP Auto-Configuration Sequence

The DHCP Server sends the server instance’s IP address, the latest firmware revision number and the name of the configuration file that will be used to reconfigure the device. After receiving this information from the DHCP server the device will send a "reconfiguration request" to the server instance. After receiving this message from the device, the server will update the device’s firmware (if necessary) and subsequently send the new configuration file to the device.

The following diagram demonstrates the principle of message and data exchange between the switch and both the DHCP server and server instance:

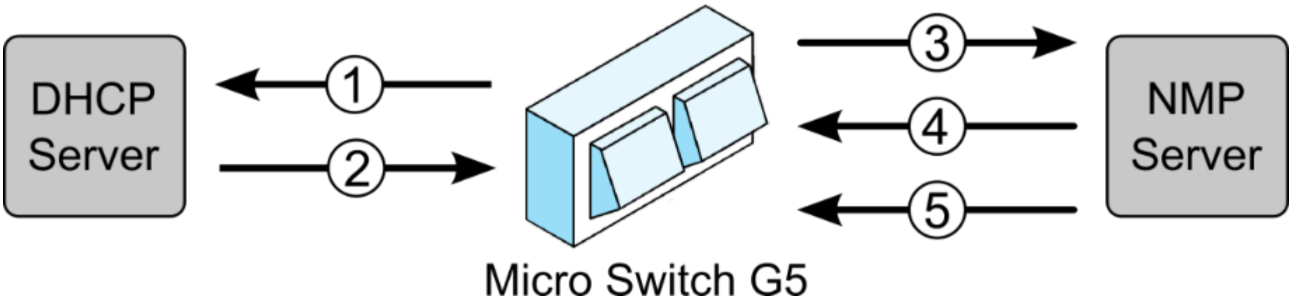


Figure 111. NMP Enterprise - Switch DHCP Auto Configuration - Sequence

Step	State	Data Exchange
1	**DHCP Discovery**	• device MAC address
2	**DHCP Offer**	• device IP address • server instance IP address • latest firmware revision number • configuration file name
3	**NMP Configuration Request**	• latest firmware revision number • configuration file name
4	**NMP Firmware Update (optional)**	• latest firmware file
5	**NMP Configuration**	• latest configuration file

7.5.2. DHCP Server Configuration

The DHCP server must be configured to deliver two additional DHCP options included in the DHCP offer frame:

Option 66 (TFTP Server Name [RFC2132])
This option must contain the IP address of the server instance because DNS is not supported by the G5 switch.

Option 67 (Boot Filename [RFC2132])
This option must contain the filename of the master configuration file (`*.nmpmc`) to be applied to the switch by the server instance.

7.5.3. Configuration of Server Instance

The server instance listens for requests on UDP port `8340`. Two files are used in order to process the "reconfiguration request" sent by the switch:

- **Master configuration file (`.nmpmc`, mandatory):** Created by the NMP Enterprise client component, includes the switch configuration and the firmware file name.

  Without this file, the server instance will not start the reconfiguration and firmware update procedure.

- **Firmware file (`.bin`, optional):** new firmware for switches.

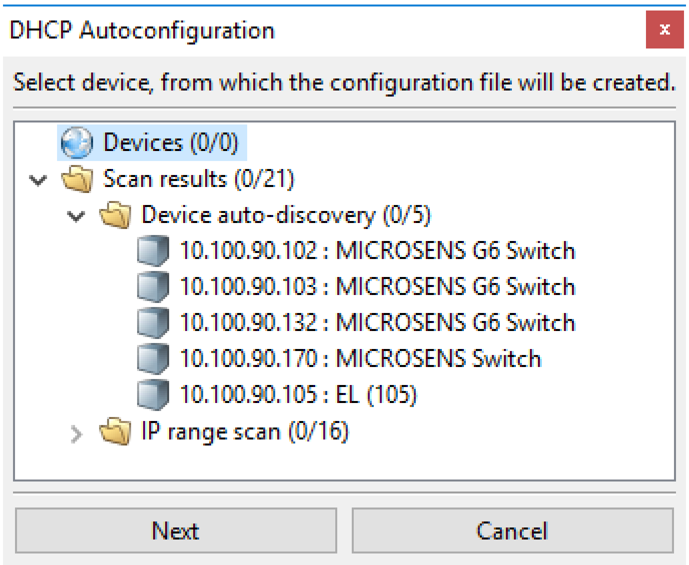
  The server instance will not update the device firmware, if the file is not available.

Place both files in the directory `<Server data directory>/FTP/DHCPAutoconfigFiles`, either manually or using the client component.

7.5.4. Creating/Editing the DHCP Autoconfiguration File

In order to create the DHCP autoconfiguration file which can be used by the server instance for DHCP Autoconfiguration procedure, open the client, connect with the server and select **Tools** › **DHCP Autoconfiguration (G5)** › **Create configuration file**.

The client opens the dialogue for selecting a device from the device list tree.



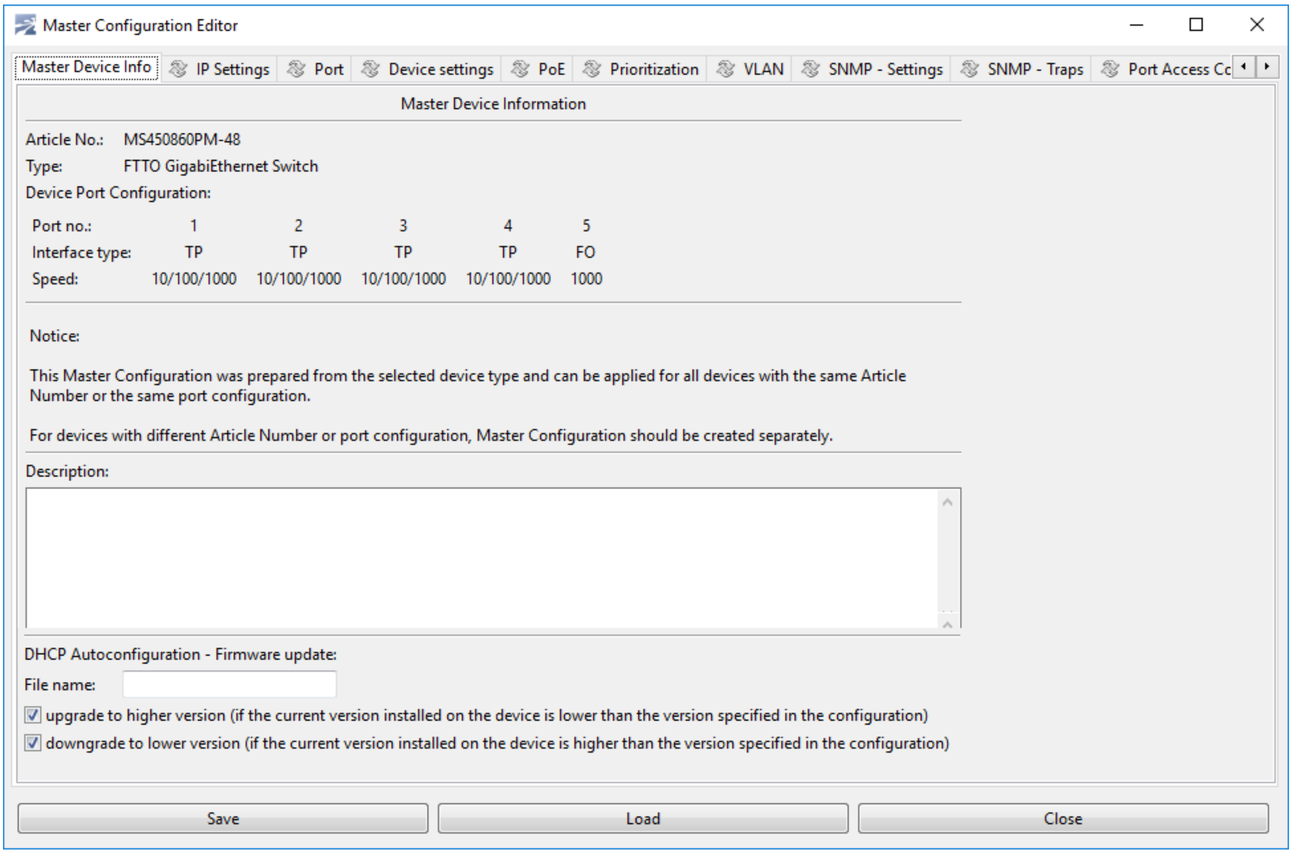
DHCP Autoconfiguration

Select device, from which the configuration file will be created.

- Devices (0/0)
- Scan results (0/21)
  - Device auto-discovery (0/5)
    - 10.100.90.102 : MICROSENS G6 Switch
    - 10.100.90.103 : MICROSENS G6 Switch
    - 10.100.90.132 : MICROSENS G6 Switch
    - 10.100.90.170 : MICROSENS Switch
    - 10.100.90.105 : EL (105)
  - IP range scan (0/16)

Figure 112. Stand-alone Client - DHCP Autoconfiguration - Select Device

Select the device, which should be used to create the DHCP autoconfiguration file ("configuration template"). After clicking the button **Next** the following "Master Configuration Editor" dialogue opens:



Master Device Information

Article No.: MS450860PM-48
Type: FTTO GigabiEthernet Switch
Device Port Configuration:

Port no.:	1	2	3	4	5
Interface type:	TP	TP	TP	TP	FO
Speed:	10/100/1000	10/100/1000	10/100/1000	10/100/1000	1000

Notice:

This Master Configuration was prepared from the selected device type and can be applied for all devices with the same Article Number or the same port configuration.

For devices with different Article Number or port configuration, Master Configuration should be created separately.

Description:

DHCP Autoconfiguration - Firmware update:

File name:

☑ upgrade to higher version (if the current version installed on the device is lower than the version specified in the configuration)

☑ downgrade to lower version (if the current version installed on the device is higher than the version specified in the configuration)

Figure 113. Stand-alone Client - DHCP Autoconfiguration - DHCP Configuration Editor

This dialogue enables editing the device configuration and selecting the setup options which should be changed (by selecting the **change** check-boxes, next to the configuration options).

Optionally, enter the firmware filename, which will be used to update the device. It is possible to determine the action that should be taken during the firmware update procedure:

- Upgrade firmware to higher version, if the current version installed on the device is lower than the version specified in the configuration file.
- Downgrade firmware to lower version, if the current version installed on the device is higher than the version specified in the configuration file.

NOTE If both actions will be disabled or the currently running firmware version is the same as the version specified in the configuration file, the firmware upload procedure will not be started.

The firmware filename that is specified in the configuration file must follow this name convention `information_ppppvxyyzzq.bin`.

The individual elements of the filename have the following meaning:

- `information_`: some additional information to the firmware (optional)
- `pppp`: project number (5313, 5324, 5331, 7018, 7014, 9135) (required)
- `v`: abbreviation for version (required)
- `x`: one digit (0…9), major version number (required)
- `yy`: two digits (00… 99), minor version number (e.g. 08) (required)
- `zz`: two digits (00… 99), project version number (e.g. 04) (required)
- `q`: one letter (a…z), project sub-version letter (optional)
- `.bin`: firmware file extension.

The following names are valid:

- `mf5324v80301.bin`
- `new_firmware_mf7014v80300d.bin`
- `10.01.2012_5331v80805a.bin`

The following names are **not** valid:

- `mf5324v8031.bin`: wrong number of digits of project version number (`1` instead of `01`).
- `new_firmware_mf7014v80300d_some_text.bin`: additional text between the project sub-version letter and `.bin` extension.
- `10.01.2012_v80805a.bin`: missing project number before the `v`.

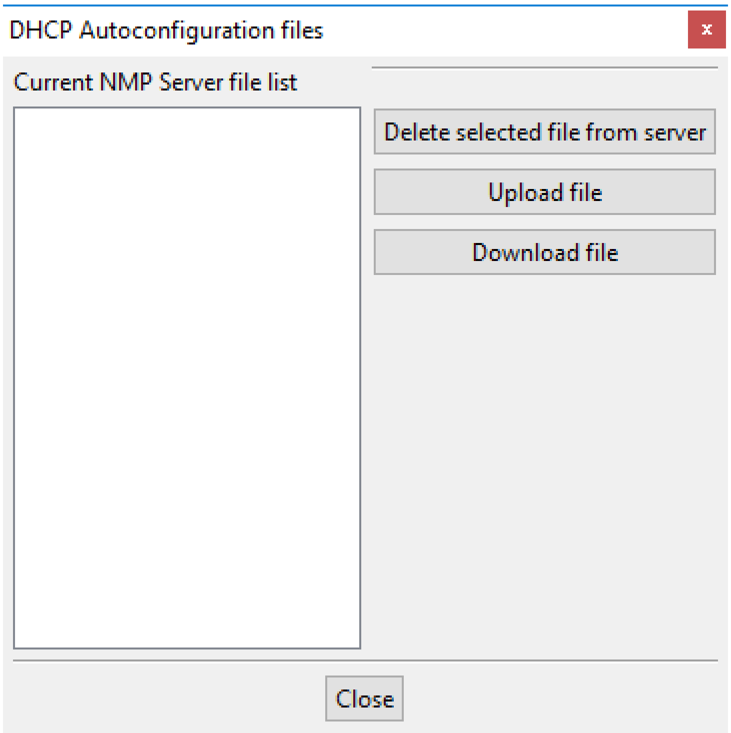
NOTE With an incorrect firmware filename the server will not be able to recognise the firmware version correctly and the update procedure will not start.

Editing a DHCP autoconfiguration file works identically, though you have to load a previously saved file from a local directory into the SHCP configuration editor.

Finally, save the edited DHCP autoconfiguration file in the directory `<Server data directory>/FTP/DHCPAutoconfigFiles`.

7.5.5. Sending the Files to the Server Instance

In order to send the DHCP Autoconfiguration and firmware file to the server select **Tools** › **DHCP Autoconfiguration (G5)** › **DHCP autoconfiguration files**. The following file transfer dialogue appears:


DHCP Autoconfiguration files

Current NMP Server file list

Figure 114. NMP Enterprise - Client - DHCP Autoconfiguration - Send File

Use this dialogue to

- upload new configuration files to server,
- download existing configuration files from the server or
- delete existing configuration files from the server.

NOTE When not using the client to upload the configuration files to the server, the necessary files must be placed in the directory `<Server data directory>/FTP/DHCPAutoconfigFiles`.

7.6. Using a Master Configuration

NOTE The use of master configuration is possible for both NMP Professional and NMP Enterprise.

Due to the continuous firmware development for MICROSENS devices and the need for NMP to operate with older firmware versions, the use of master configuration is handled differently between G6/G7 and prior devices.

7.6.1. Master Configuration of MICROSENS Devices

The "Master Configuration" can be used to define properties and settings which can then be applied to devices of the same type as the master device (i.e. the device from which the master configuration was created). The master configuration allows changing every single parameter on all the devices in the device list.

NOTE The "Master Configuration" feature is exclusively available for MICROSENS Micro Switch devices, MICROSENS Industrial ProfiLine devices and some MICROSENS desktop switches.

NOTE For master configuration of G5 and older versions please refer to the respective description in Section 7.6.2.

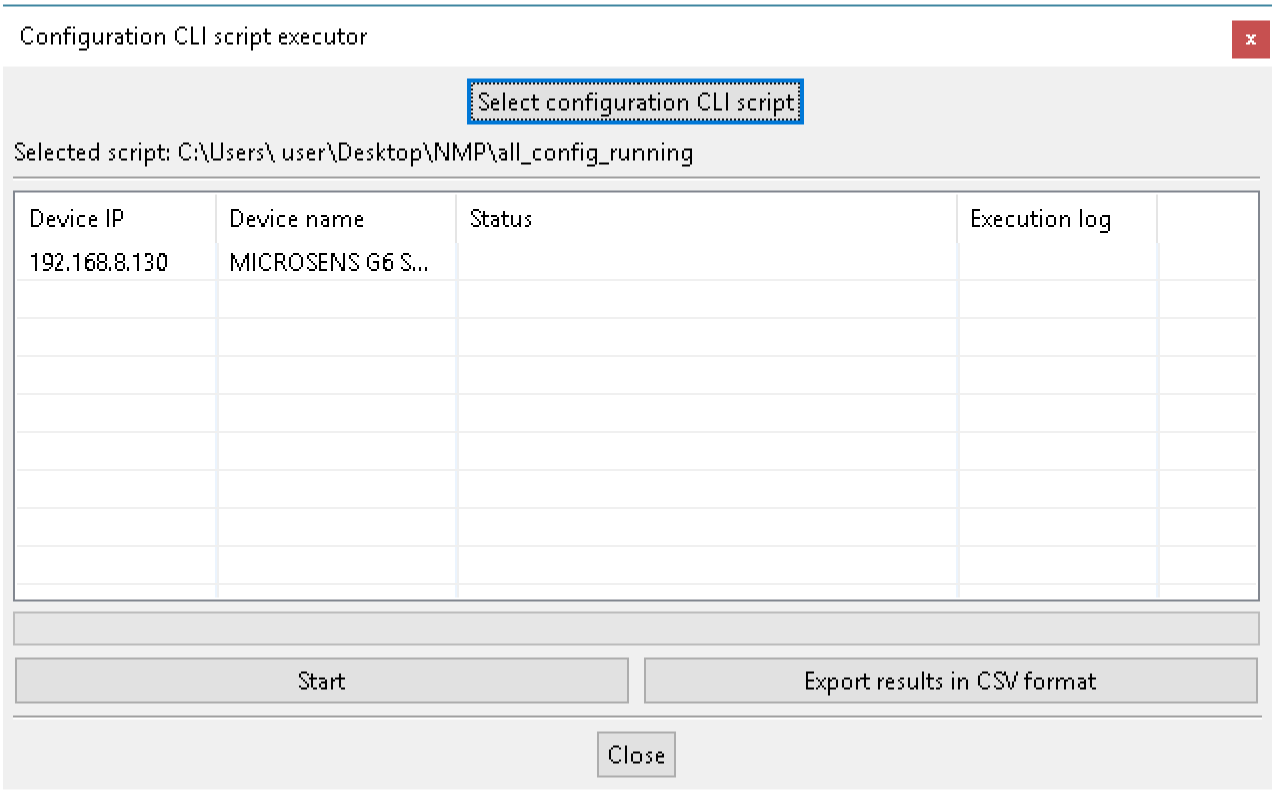
The master configuration file for MICROSENS G6 and G7 devices is in form of a CLI script (text file), which contains a list of commands that should be executed by the device. NMP offers three master configuration menu items in the device context menu:

- Apply CLI Scripts
- Generate and download CLI script
- Edit CLI script file

These context sub-menu items work as follows:

Apply CLI Script

After selecting the respective CLI script in the OS file manager dialogue, the following window appears:


Configuration CLI script executor
x
Select configuration CLI script
Start
Export results in CSV format
Close

Selected script: C:\Users\ user\Desktop\NMP\all_config_running

Device IP	Device name	Status	Execution log
192.168.8.130	MICROSENS G6 S...		

Figure 115. NMP - Device Context Menu - Master Configuration - Apply CLI Script

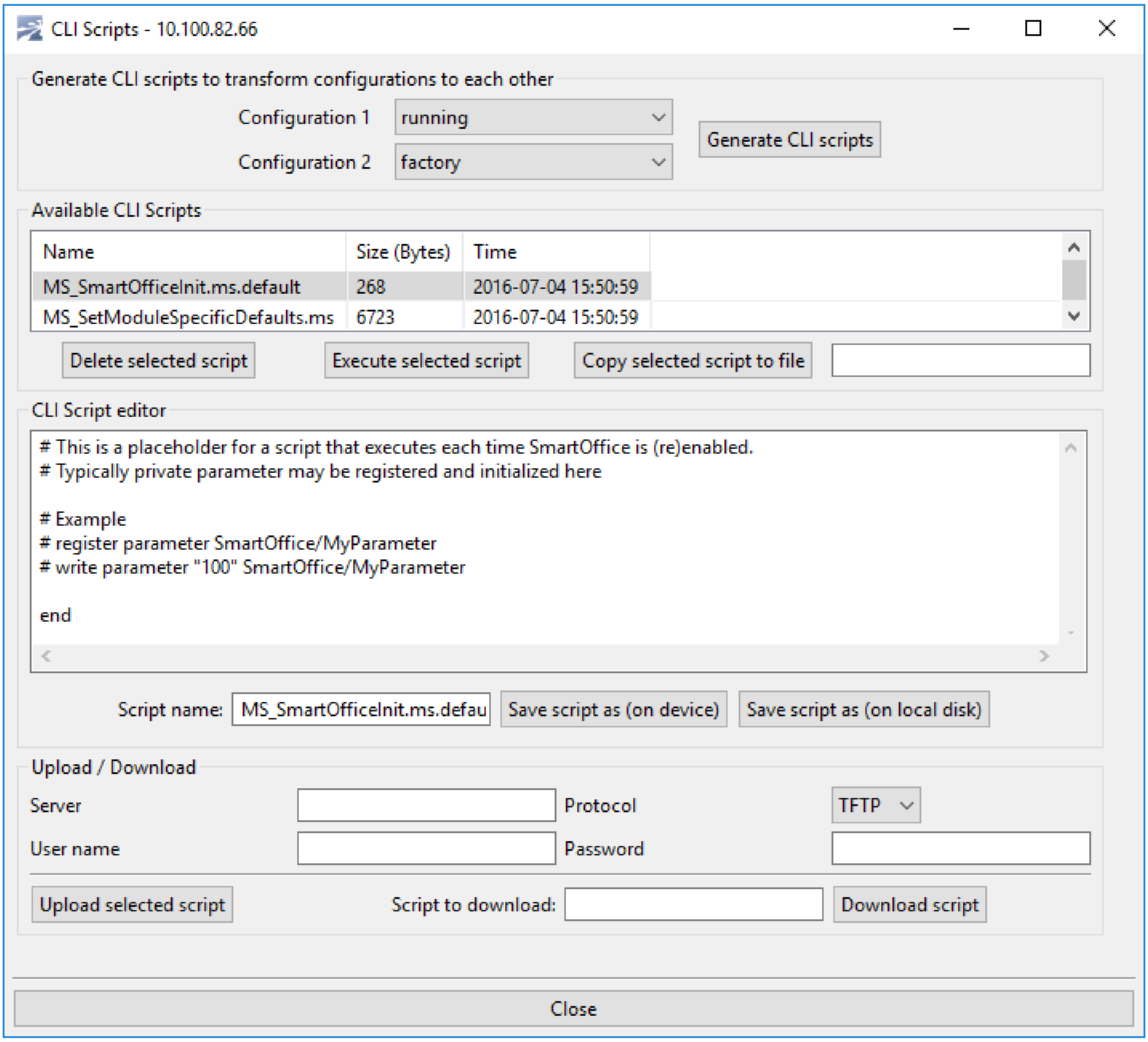
Change the selected script with the button `Select configuration CLI script`. The list shows the selected devices, for which the script will be executed and the status of operation as soon as the button `Start` is clicked.

In the "Execution log" column, the linked log file is listed as soon as the procedure will be finished for the respective device.

With the button `Export results in CSV format` an export of the procedure’s results in form of a `.csv` file is available.

Generate and Download CLI Script

This feature can be used to generate a CLI script template or edit an existing CLI script on the device before downloading it to the local disk for editing. It is possible to execute an existing CLI script on a device. By hitting this menu item the following dialogue appears:



CLI Scripts - 10.100.82.66

Generate CLI scripts to transform configurations to each other

Configuration 1: running

Configuration 2: factory

Available CLI Scripts

Name	Size (Bytes)	Time
MS_SmartOfficeInit.ms.default	268	2016-07-04 15:50:59
MS_SetModuleSpecificDefaults.ms	6723	2016-07-04 15:50:59

CLI Script editor

```
# This is a placeholder for a script that executes each time SmartOffice is (re)enabled.
# Typically private parameter may be registered and initialized here

# Example
# register parameter SmartOffice/MyParameter
# write parameter "100" SmartOffice/MyParameter

end
```

Script name: MS_SmartOfficeInit.ms.defau

Upload / Download

Server:

Protocol: TFTP

User name:

Password:

Script to download:

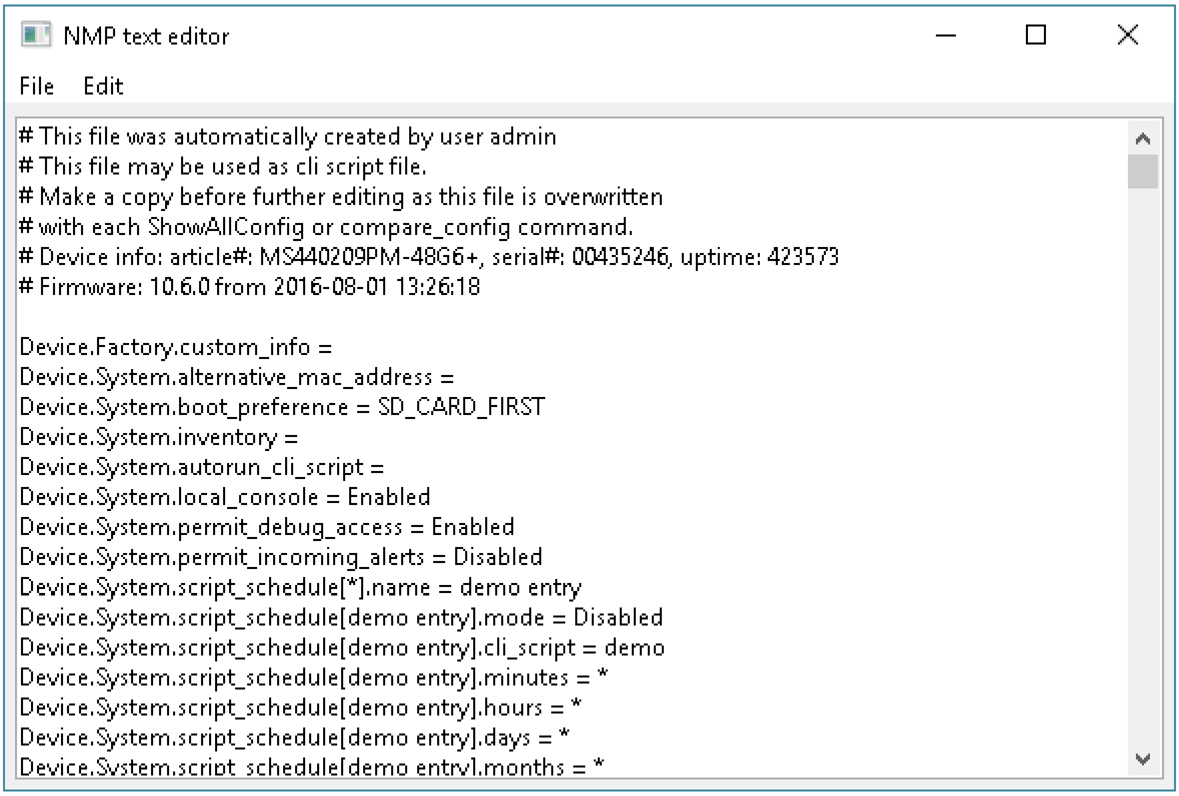
Figure 116. NMP - Device Context Menu - Master Configuration - CLI Scripts

The feature also offers a possibility to upload scripts from the device to some TFTP/FTP server or to download scripts from a TFTP/FTP server directly to the device for which the tool was opened.

Clicking on the button `Generate CLI Scripts` generates a CLI script on the device and then saves it to the local disk. Afterwards, the saved script can be locally edited (e.g. with the NMP Text Editor) and applied to many devices with the **Apply CLI Script** menu item from above.

Edit CLI Script File

This feature opens the NMP Text Editor with a selected CLI script which can be edited before applying it to certain devices. The NMP Text Editor is comparable to various editors and offers some very basic file and text edit functions.



```
# This file was automatically created by user admin
# This file may be used as cli script file.
# Make a copy before further editing as this file is overwritten
# with each ShowAllConfig or compare_config command.
# Device info: article#: MS440209PM-48G6+, serial#: 00435246, uptime: 423573
# Firmware: 10.6.0 from 2016-08-01 13:26:18

Device.Factory.custom_info =
Device.System.alternative_mac_address =
Device.System.boot_preference = SD_CARD_FIRST
Device.System.inventory =
Device.System.autorun_cli_script =
Device.System.local_console = Enabled
Device.System.permit_debug_access = Enabled
Device.System.permit_incoming_alerts = Disabled
Device.System.script_schedule[*].name = demo entry
Device.System.script_schedule[demo entry].mode = Disabled
Device.System.script_schedule[demo entry].cli_script = demo
Device.System.script_schedule[demo entry].minutes = *
Device.System.script_schedule[demo entry].hours = *
Device.System.script_schedule[demo entry].days = *
Device.System.script_schedule[demo entry].months = *
```

Figure 117. NMP - Device Context Menu - Master Configuration - NMP Text Editor

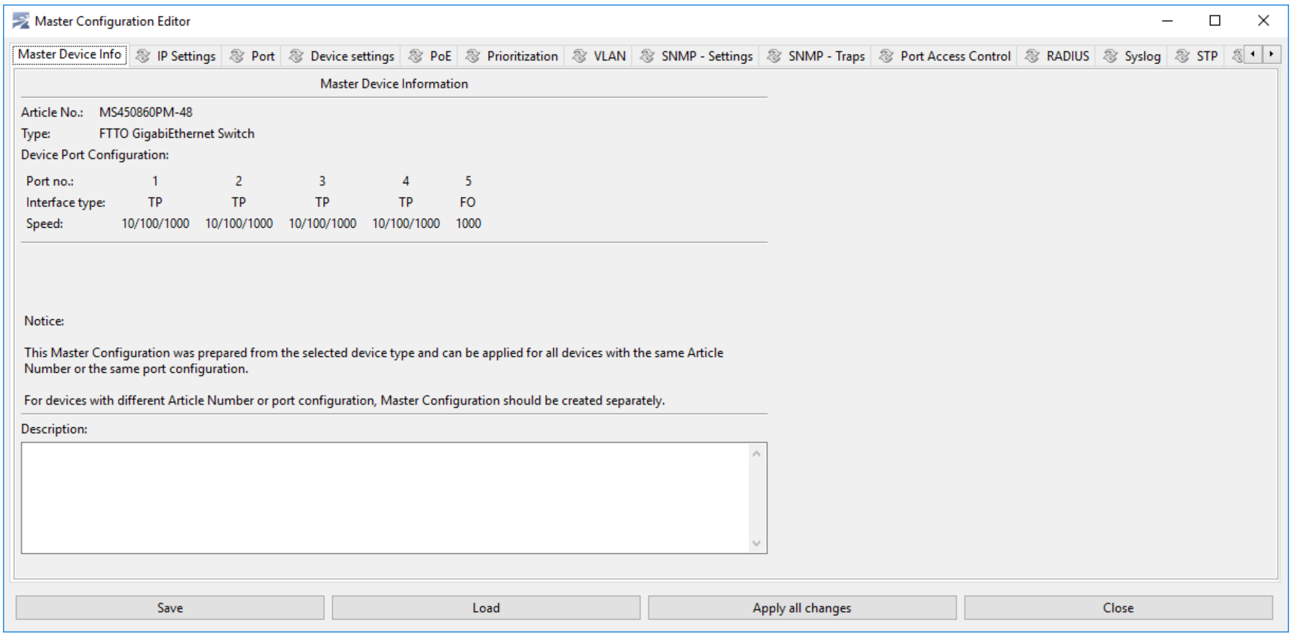
NOTE

When using the master configuration function from the group context menu the sub-menu entries are grouped by the switch model.

When selecting e.g. **[G6] Apply CLI Script** only the group contained G6 devices are affected.

7.6.2. Master Configuration of MICROSENS G5 and older Devices

To create a master configuration of a MICROSENS G5 (or older) device, select the specific switch in the NMP device tree and choose **Master Configuration** from the device context menu. The following dialogue appears:



Master Device Information

Article No.: MS450860PM-48
Type: FTTO GigabitEthernet Switch
Device Port Configuration:

Port no.:	1	2	3	4	5
Interface type:	TP	TP	TP	TP	FO
Speed:	10/100/1000	10/100/1000	10/100/1000	10/100/1000	1000

Notice:

This Master Configuration was prepared from the selected device type and can be applied for all devices with the same Article Number or the same port configuration.

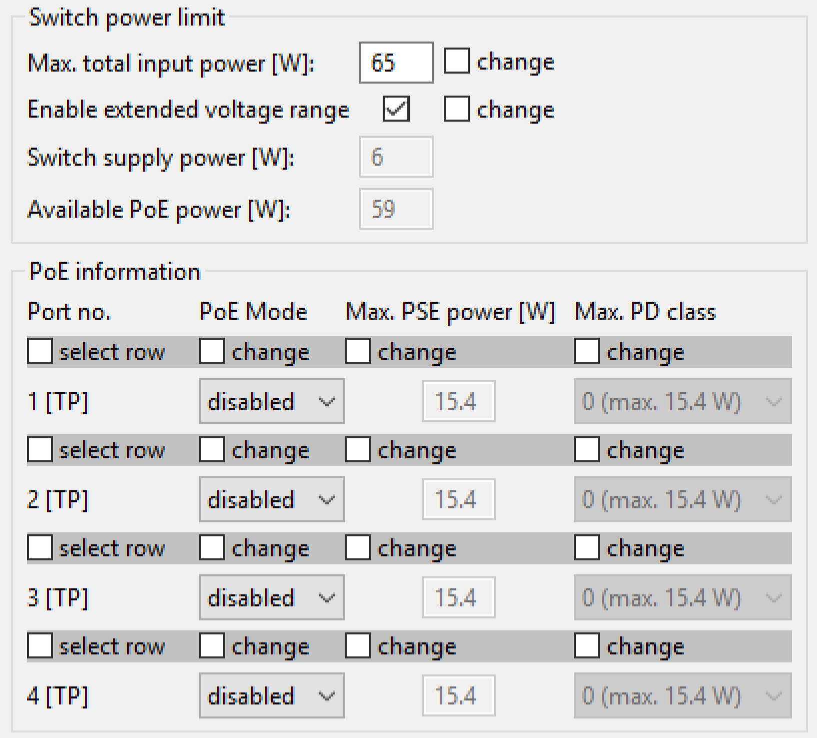
For devices with different Article Number or port configuration, Master Configuration should be created separately.

Description:

Figure 118. NMP - Device Context Menu - Master Configuration (G5 and older)

This dialogue contains several tabs with information of the "Master Device" and available configurations. Additionally, there is an option to enter the description for the master configuration which will then be saved within the file.

On each tab edit the existing settings and select which of them should be changed on the devices. The selected parameters (respective checkbox enabled) will be changed on the devices. The other parameters remain unchanged. The tabs with selected and changed settings are marked by a green icon (next to the tab name).



Switch power limit

Max. total input power [W]: 65 □ change
Enable extended voltage range ☑ □ change
Switch supply power [W]: 6
Available PoE power [W]: 59

PoE information

Port no.	PoE Mode	Max. PSE power [W]	Max. PD class
□ select row	□ change	□ change	□ change
1 [TP]	disabled	15.4	0 (max. 15.4 W)
□ select row	□ change	□ change	□ change
2 [TP]	disabled	15.4	0 (max. 15.4 W)
□ select row	□ change	□ change	□ change
3 [TP]	disabled	15.4	0 (max. 15.4 W)
□ select row	□ change	□ change	□ change
4 [TP]	disabled	15.4	0 (max. 15.4 W)

Figure 119. NMP - Device Context Menu - Master Configuration (G5 and older) - Example

On each configuration tab there is an additional button to select all the parameters. It is also possible to clear the current selection or load the original configuration from the master device (this can be done separately for all configuration pages).

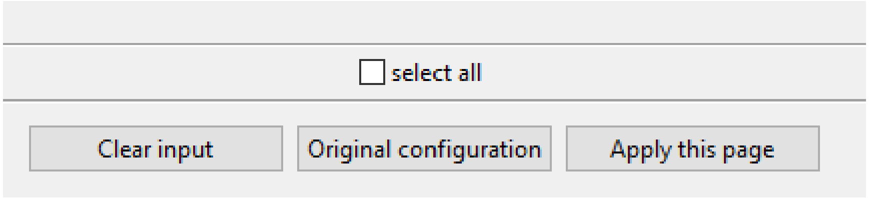
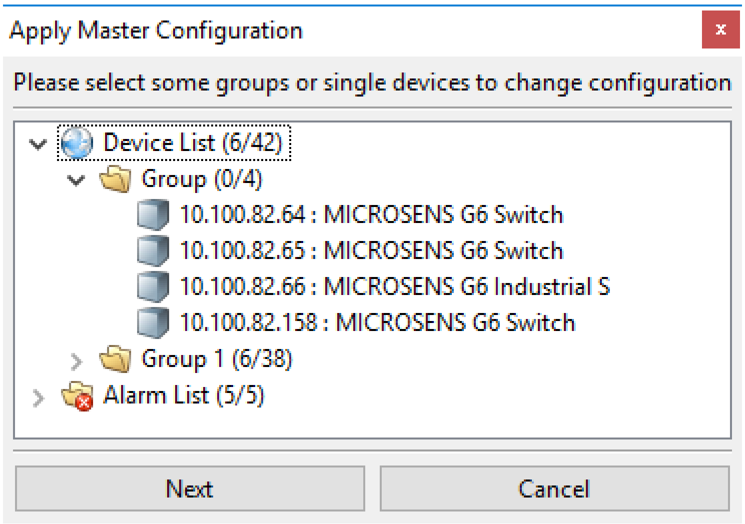


Figure 120. NMP - Device Context Menu - Master Configuration (G5 and older) - Buttons

Any change to any of the configuration pages is automatically saved. Select different tabs without having to worry about saving the changes.

To apply the configuration modifications on the current tab select the button `Apply this page`. To apply the configuration changes of all tabs select the button `Apply all changes`. After applying the changes, the dialogue containing the group/device selection opens. Select the device or group to which the changes should be applied.

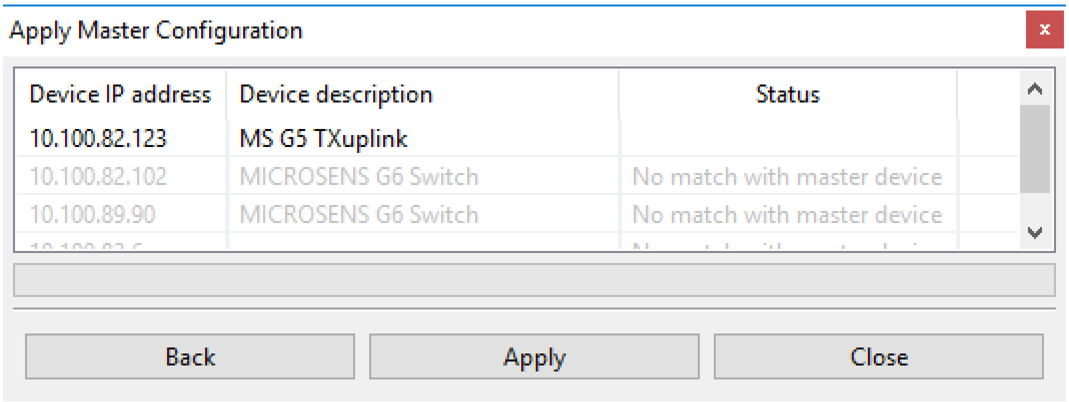

Apply Master Configuration

Please select some groups or single devices to change configuration

- Device List (6/42)
  - Group (0/4)
    - 10.100.82.64 : MICROSENS G6 Switch
    - 10.100.82.65 : MICROSENS G6 Switch
    - 10.100.82.66 : MICROSENS G6 Industrial S
    - 10.100.82.158 : MICROSENS G6 Switch
  - Group 1 (6/38)
- Alarm List (5/5)

Figure 121. NMP - Device Context Menu - Master Configuration (G5 and older) - Select Group/Device

Changes will be applied to devices with the same article number or same port configuration as the master device. For all other devices a master configuration should be created separately. After selecting a device or group in the device tree list, NMP displays a window showing the status and current progress of the operation.



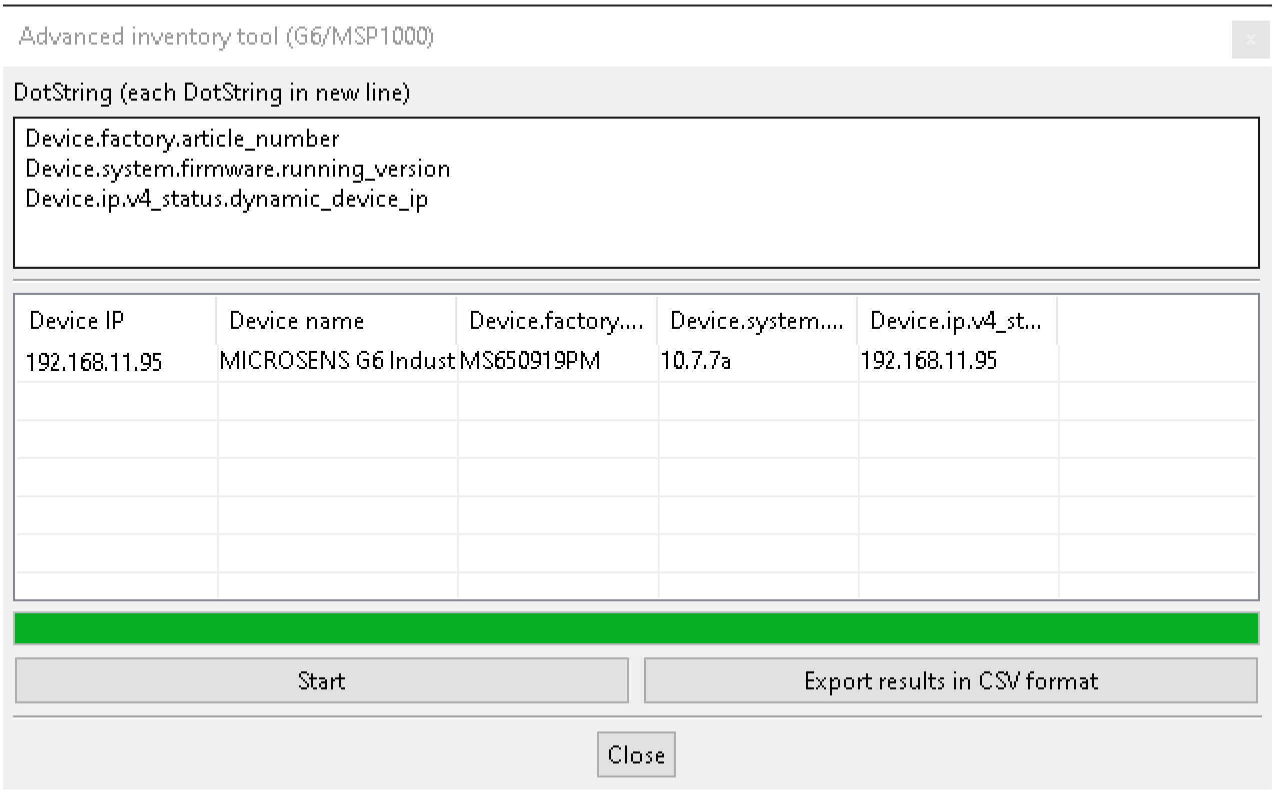
Apply Master Configuration

Device IP address	Device description	Status
10.100.82.123	MS G5 TXuplink	
10.100.82.102	MICROSENS G6 Switch	No match with master device
10.100.89.90	MICROSENS G6 Switch	No match with master device

Figure 122. NMP - Device Context Menu - Master Configuration (G5 and older) - Apply to Devices

7.7. Using Advanced Inventory Tool

NOTE The advanced inventory tool is available for both NMP Professional and NMP Enterprise.



Advanced inventory tool (G6/MSP1000)

DotString (each DotString in new line)

```
Device.factory.article_number
Device.system.firmware.running_version
Device.ip.v4_status.dynamic_device_ip
```

Device IP	Device name	Device.factory....	Device.system....	Device.ip.v4_st...
192.168.11.95	MICROSENS G6 Indust	MS650919PM	10.7.7a	192.168.11.95

Figure 123. NMP - Inventory advanced

The advanced inventory tool gives a quick overview of specific settings of all managed G6 (and newer) and MSP1000 devices as follows:

1. In the device list tree view on the left hand pane select the group that contains the devices you want to be displayed.
2. In the main menu select **Tools › Inventory - Advanced (G6/MSP1000)**

NOTE | The advanced inventory tool only functions with MICROSENS G6 and MSP1000 devices!

3. In the text area "DotString (each DotString in new line)" enter the respective DotStrings of the devices you want to display.

TIP | To quickly get the DotString, open the device’s Web Manager, change to the respective dialogue window and click on the shown parameter. The DotString will be copied to the clipboard. Paste the DotString to the text area.

4. When all wanted DotStrings are entered, click on the button `Start`.
   - The tabular overview refreshes and lists all parameters defined by the DotStrings for all devices.
5. To export the results, click on the button `Export results in CSV format`.
   - The file saving dialogue of your operating system opens.
   - Select directory and file name for the `.csv` file.
6. Click on the button `Close` to close the advanced inventory tool.

NOTE | The DotString list will be cleared after closing.

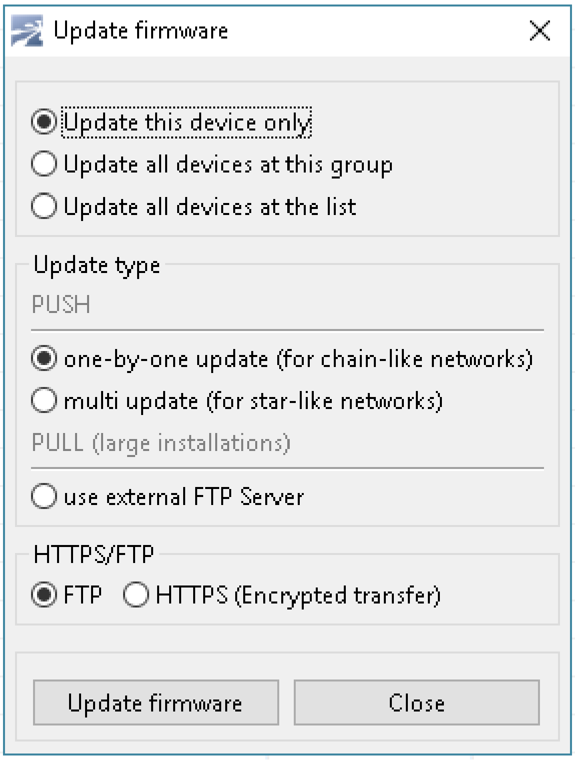
7.8. Updating the Firmware

NOTE | Updating the firmware happens identically for both NMP Professional and NMP Enterprise.

The "Update Firmware" feature is device type-dependent. It may look different for different device types. The following sections describe how to update the firmware on MICROSENS Micro Switches (G6 and newer) / Industrial Switches (G6 and newer).

NOTE | The firmware update of a device is possible if management information for the device is available. Devices with a device-polling timeout cannot be updated.

To update the firmware of one or more devices use the device context menu of the respective device or group in the device list. After clicking **Update Firmware** the following dialogue opens:


Update firmware

● Update this device only
○ Update all devices at this group
○ Update all devices at the list

Update type

PUSH

● one-by-one update (for chain-like networks)
○ multi update (for star-like networks)

PULL (large installations)

○ use external FTP Server

HTTPS/FTP

● FTP ○ HTTPS (Encrypted transfer)

Figure 124. NMP - Device Context Menu - Update Firmware

The dialogue offers several update options:

- **Update device, group or list:** It is possible to update the firmware of just one device, all devices within a group or all devices within a whole list. Opening the context menu of a device and choosing the group or list option in this dialogue, all devices that belong to the same group or list are updated too.
- **Update Type PUSH/PULL:** Choose what type of firmware update to execute and whether to use an external FTP server as the source for the firmware file.

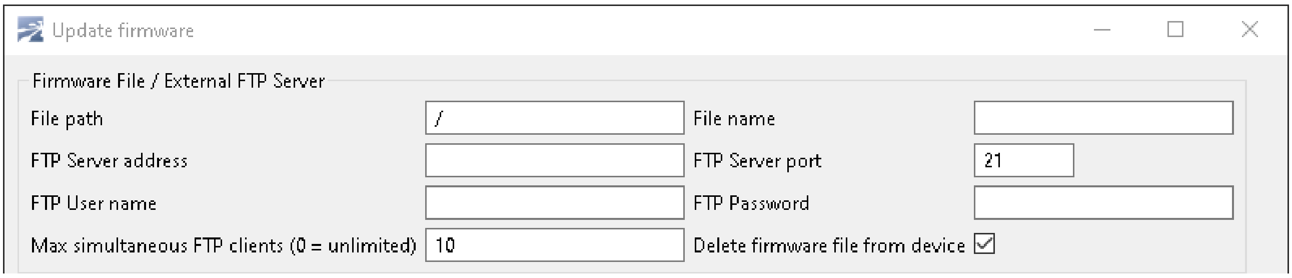
  For a star-like network topology use a "multi update". This means that up to 10 switches can be updated at the same time. In a star-like topology there is no danger of the switch's firmware failing due to another updated switch - through which the firmware file is uploaded to the following devices - being reset.

  Such a situation is, however, possible in chain-like topologies. That is why the use of the "one-by-one" update method in such topologies is mandatory.

  The "PUSH" method means, the firmware file is pushed by NMP to devices. In case of "PULL" method, which is suggested for very large installations with many switches, the device will download the firmware file itself from the provided FTP server.

- **HTTPS/FTP:** It is possible to select the protocol, which will be used during the firmware file upload (from NMP to the device). FTP or secured HTTP.

In the next step provide the FTP Server details where the firmware file is located (in case of "PULL" method) or choose the appropriate firmware file (in case of "PUSH" method).

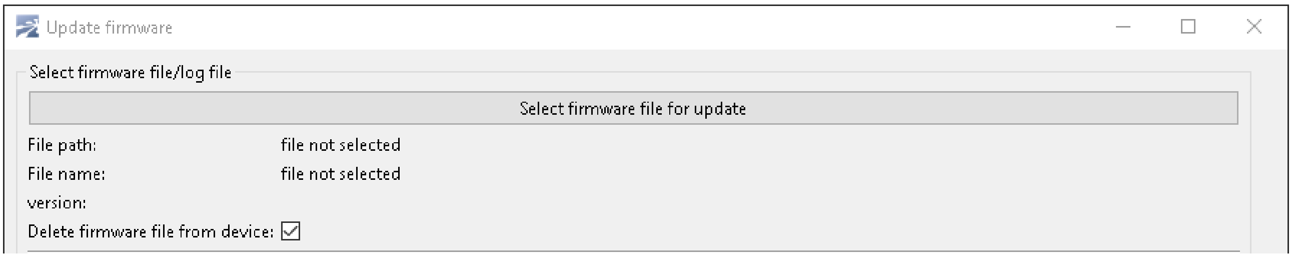


Update firmware

Firmware File / External FTP Server

File path	/	File name	
FTP Server address		FTP Server port	21
FTP User name		FTP Password	
Max simultaneous FTP clients (0 = unlimited)	10	Delete firmware file from device	☑

Figure 125. NMP - Device Context Menu - Update Firmware - Select FTP Server



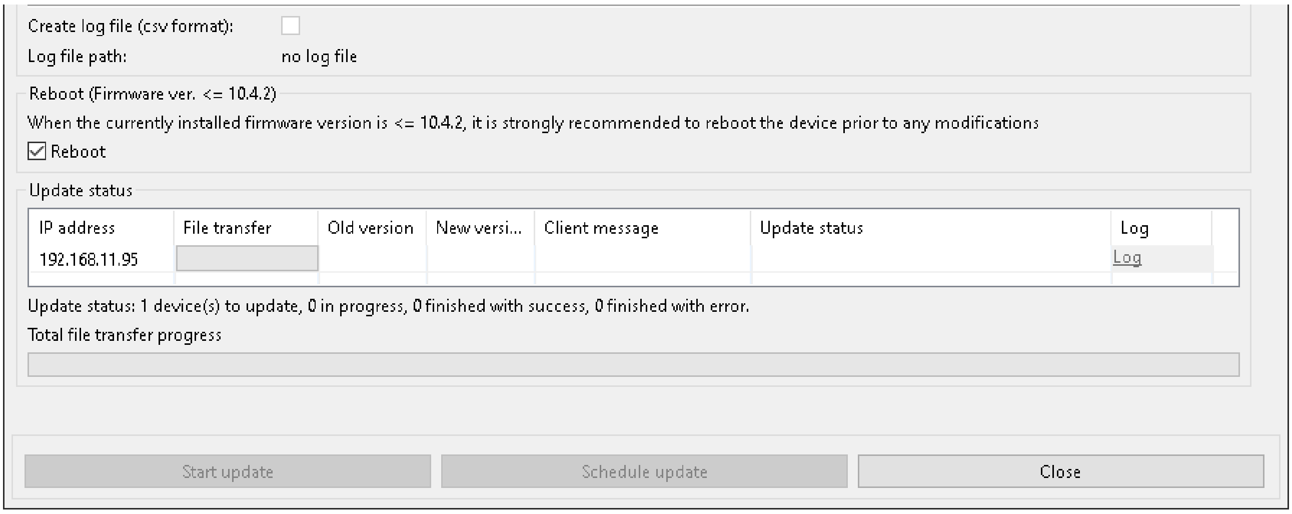
Update firmware

Select firmware file/log file

File path:	file not selected
File name:	file not selected
version:	
Delete firmware file from device:	☑

Figure 126. NMP - Device Context Menu - Update Firmware - Select File

All other settings are identical with both methods:



Create log file (csv format):	□
Log file path:	no log file

Reboot (Firmware ver. <= 10.4.2)

When the currently installed firmware version is <= 10.4.2, it is strongly recommended to reboot the device prior to any modifications

☑ Reboot

Update status

IP address	File transfer	Old version	New versi...	Client message	Update status	Log
192.168.11.95						Log

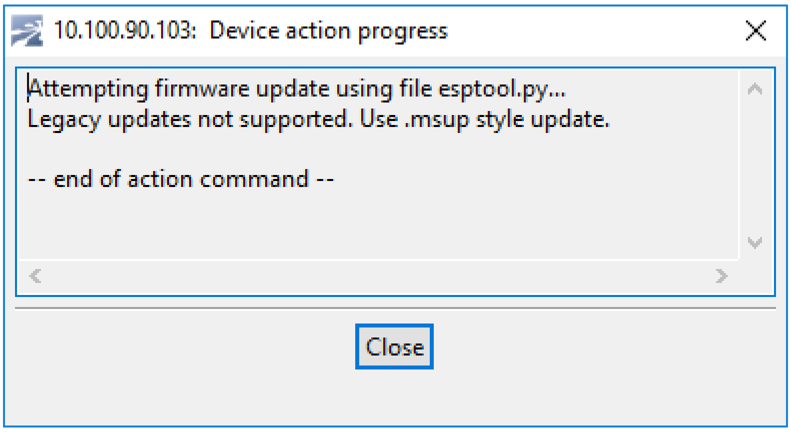
Update status: 1 device(s) to update, 0 in progress, 0 finished with success, 0 finished with error.

Total file transfer progress

Figure 127. NMP - Device Context Menu - Update Firmware - Options

With the option "Create log file" choose a path and a filename first to enable logging. After choosing the firmware file start the update immediately or schedule the update task by selecting the time when the devices are to be updated.

During the firmware update procedure, the device generates this log file, which contains the information about current update status. The log file is available under the "Log" link from "Log" column. After selecting the "Log" link, the "Device action progress" dialogue opens. This dialogue is automatically refreshed and it always displays the latest content of the log file.



```
Attempting firmware update using file esptool.py...
Legacy updates not supported. Use .msup style update.

-- end of action command --
```

Figure 128. NMP - Device Context Menu - Update Firmware - Progress

To configure a regular firmware update an option to schedule the update task is available by clicking the button `Schedule update`.

Define a task which will be executed just once (at a defined time) or periodically at the configured execution rate.

NOTE All scheduled tasks can be deleted or modified using the "Scheduled Tasks Viewer" tool (see Section 4.4.5.3).

NOTE Please keep in mind that scheduled tasks will not be started when NMP is closed.

During the update procedure NMP always displays the current update status for each device in the update status list in the column "Update status" of the firmware update dialogue. Additionally, the total progress for the whole update procedure is visible in the section "Total file transfer progress" (see Figure 127). If successful, a green message is displayed. In the case of failure NMP displays a red message.

When updates have been scheduled, the firmware update dialogue is closed and a new task is stored in NMP's memory. When NMP starts the scheduled task the "Update firmware" window is automatically opened.

NOTE After updating the firmware either by Web Manager, CLI or NMP 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.

7.9. Managing Applications on G6 Devices

NOTE Managing applications is exclusively possible on MICROSENS G6 (and newer) devices.

NOTE Managing applications happens identically for both NMP Professional and NMP Enterprise.

7.9.1. Application Basics

With NMP it is possible to manage applications on MICROSENS G6 (and newer) devices.

Applications (or in short: apps) are autonomous software modules that are running on the MICROSENS devices providing wide-ranging features.

Installation and execution of apps require no intervention in the device’s firmware. It remains unchanged. This significantly reduces the administrative workload. Several apps can run simultaneously on a device thus providing a wealth of diverse features. Rather than using existing apps, the IT department can also write scripts itself. The dynamic, event-controlled microScript programming language allows scripts to be created in any text editor and loaded onto the switch by NMP. Scripts that have been created with microScript run on a level above the operating system and adopt the access rights of the user who executes them. Possible security gaps in the operating system cannot be used by the scripts, what takes into account the increased requirements for network security.

7.9.2. Configure Applications

Open the context menu of the respective device and select **Applications**.

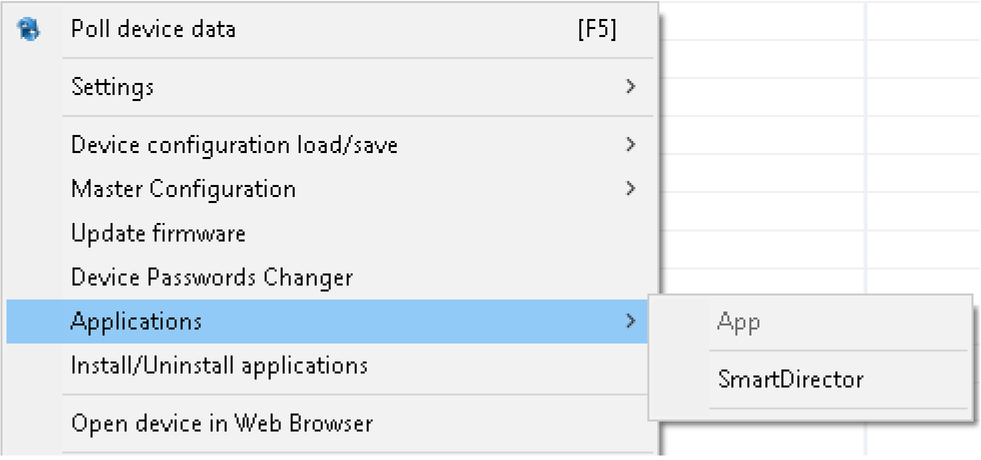


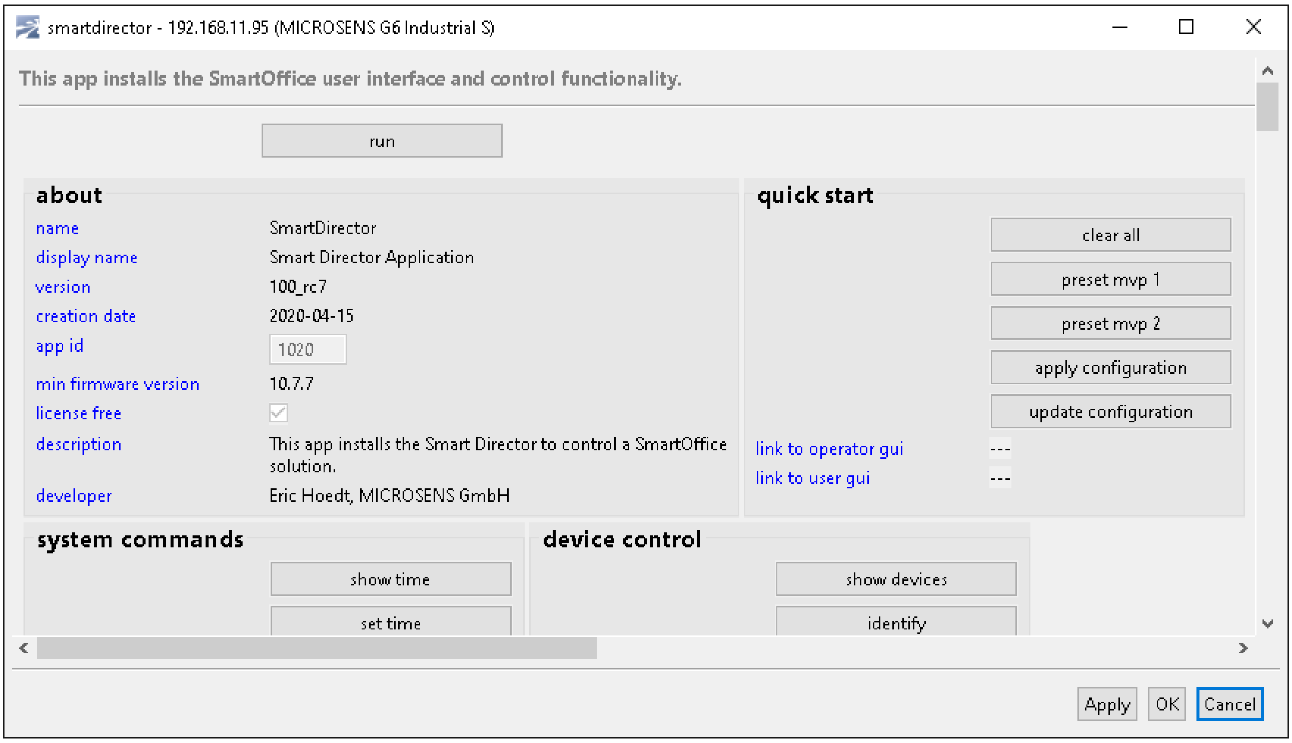
Figure 129. NMP - Device Context Menu - Applications (Example)

The sub-menu lists all applications currently installed on the device.

NOTE If NMP shows no sub menu item under **Applications** in the device’s context menu there are no applications installed on the respective device.

After selecting an application the application’s configuration dialogue opens.

NOTE Because it is possible to create applications fitting very own needs, every application has its own configuration dialogue. E.g., the application "SmartDirector" used in the example screenshot has the following structure:



smartdirector - 192.168.11.95 (MICROSENS G6 Industrial S)

This app installs the SmartOffice user interface and control functionality.

about

name	SmartDirector
display name	Smart Director Application
version	100_rc7
creation date	2020-04-15
app id	1020
min firmware version	10.7.7
license free	☑
description	This app installs the Smart Director to control a SmartOffice solution.
developer	Eric Hoedt, MICROSENS GmbH

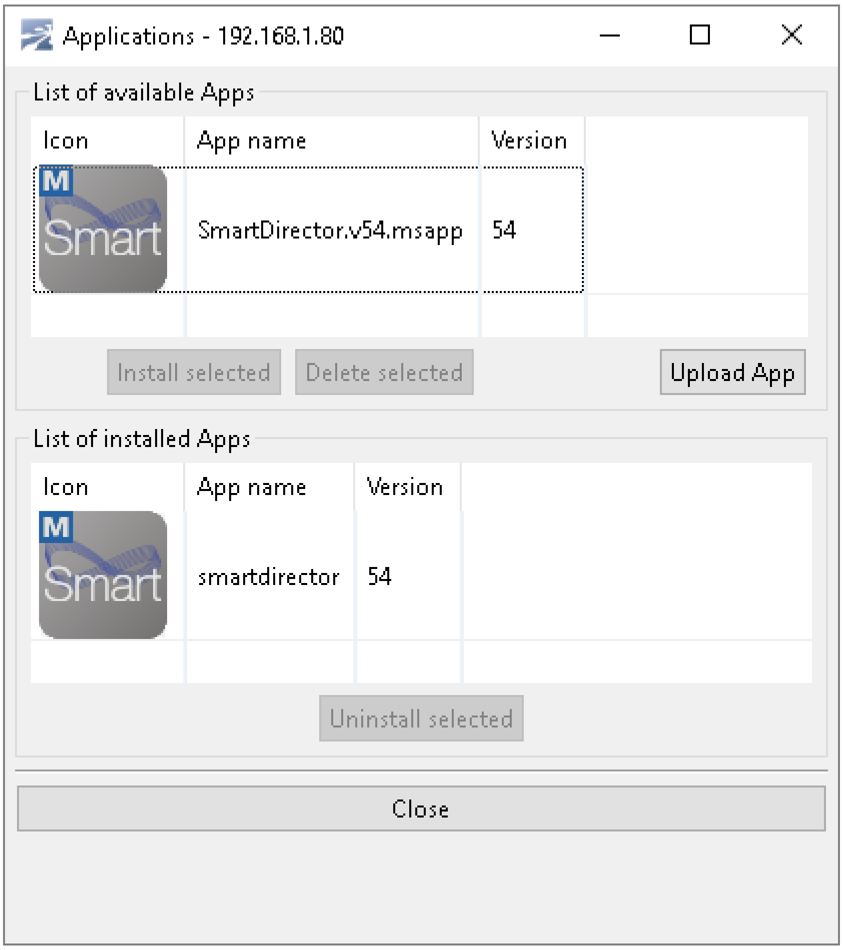
quick start

link to operator gui	---
link to user gui	---

Figure 130. NMP - Application Management - Configuration Example

7.9.3. Install/Uninstall Applications on a Single Device

In a device's context menu click on **Install/Uninstall applications**. The opening dialogue lists all applications currently installed on the selected device.



Icon	App name	Version
	SmartDirector.v54.msapp	54

Icon	App name	Version
	smartdirector	54

Figure 131. NMP - Application Management - Available Applications

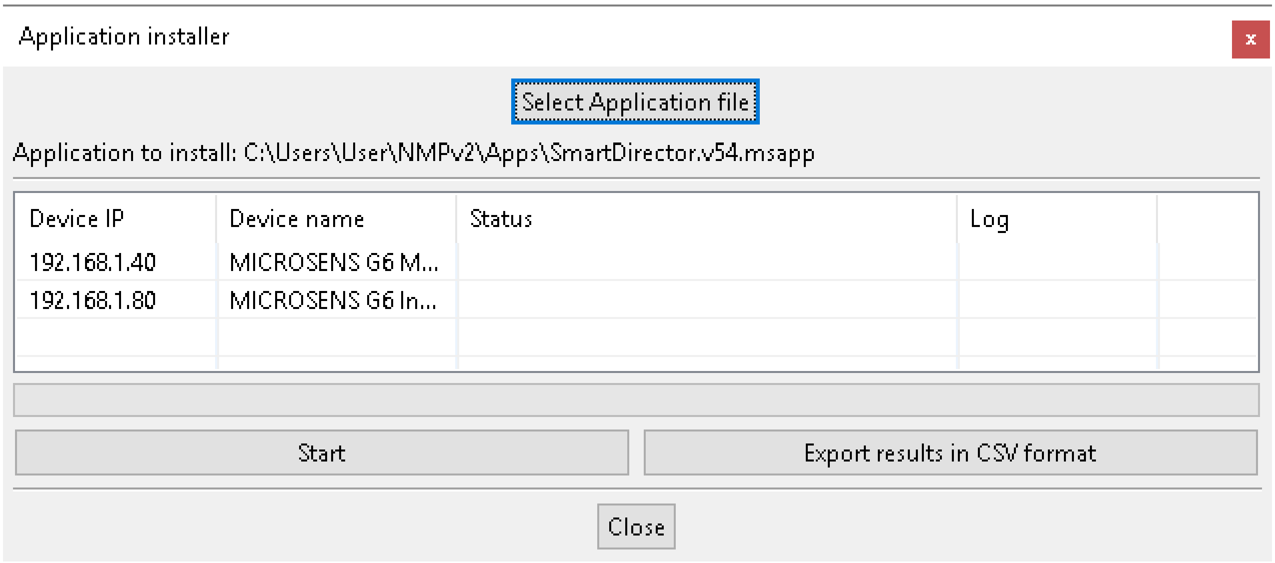
To install an application click on this app in the "List of available Apps" (or click multiple apps with the `Ctrl` key pressed). Then hit the button **`Install selected`**. The selected apps will be installed and will appear in the "List of installed Apps" after successful installation.

To uninstall an app, select it in the "List of installed Apps" and click on the button **`Uninstall selected`**.

To upload a new application into the device, click on the button **`Upload App`**. The standard file dialogue opens that prompts to choose the respective application file to upload. After the upload is finished, the respective app appears in the "List of available Apps" from where it can be selected and installed.

7.9.4. Install/Uninstall Applications on Grouped Devices

In a group’s context menu click on **Applications installer**. The file manager of your operating system opens. Browse to the locally stored application and click the button **`Open`**. NMP Professional opens the following dialogue:



Application to install: C:\Users\User\NMPv2\Apps\SmartDirector.v54.msapp

Device IP	Device name	Status	Log
192.168.1.40	MICROSENS G6 M...		
192.168.1.80	MICROSENS G6 In...		

Figure 132. NMP - Group Context Menu - Applications Installer - Select Apps

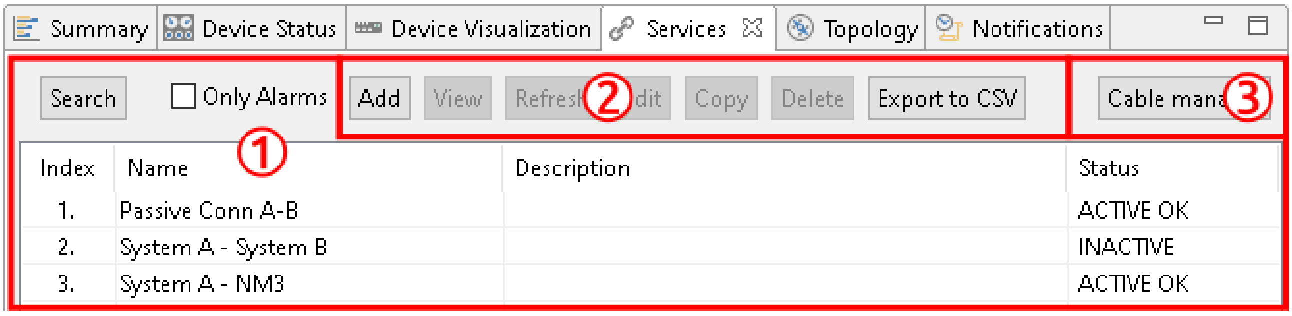
This dialogue shows a list of all the switches from the selected group. Change the selected app file with the button `Select Application file`. After clicking on the button `Start`, the selected application will be installed on all listed devices.

If the app was already installed on the switch, it will be reinstalled or updated to the newer version. After the procedure is finished, the results from the table can be exported into a `.csv` file.

7.10. Using Services

NOTE Using services is available for both NMP Professional and NMP Enterprise.

In the **Tabbed Data Panel** select the tab **Services**.



Index	Name	Description	Status
1.	Passive Conn A-B		ACTIVE OK
2.	System A - System B		INACTIVE
3.	System A - NM3		ACTIVE OK

Figure 133. NMP - Tabbed Data Panel - Services - Details

The tab offers the following sections:

1. Service table
2. Service manager
3. Cable manager

7.10.1. Service Table

The service table lists all configured services. The status of each service is presented in the column "Status". The service can hold three different states:

- Inactive (service is not used)
- Active OK (service is active, in use and its status is OK)
- Active Error (service is active and its status is ERROR; the respective row is highlighted red)

NMP checks the status of each defined service regularly and updates its state automatically. In case of any error it creates a log entry.

It is possible to search for services by entering the service name (or only a part of it) into the search field above the service table and clicking the button `Search`. NMP then hides all service entries that do not fit the search criteria.

NOTE

Hidden service list entries are recognised by their missing index entry. E.g. if the index list counts "1","2" and "4", this indicates, that the service entry with index "3" is filtered off.

To show all service entries again, just search again with an empty search phrase.

Activate the option "Only alarms" to filter for entries in alarm status.

7.10.2. Service Manager

The service manager provides configuration and management of services by clicking on the respective buttons:

- `Add`: Adds a new service.
- `View`: Opens detailed read-only view of an existing service.
- `Refresh`: refreshes an existing service’s state manually.
- `Edit`: Edits an existing service.
- `Copy`: Copy an existing service.
- `Delete`: Deletes an existing service.
- `Export to CSV`: Exports the filtered service list into a comma-separated text file.

NOTE

You can execute the commands `View`, `Refresh`, `Edit`, `Copy` and `Delete` for existing entries by opening the context menu with a right-click on the respective entry in the service table list.

After clicking the button `Add`, the service manager dialogue opens in the network view:

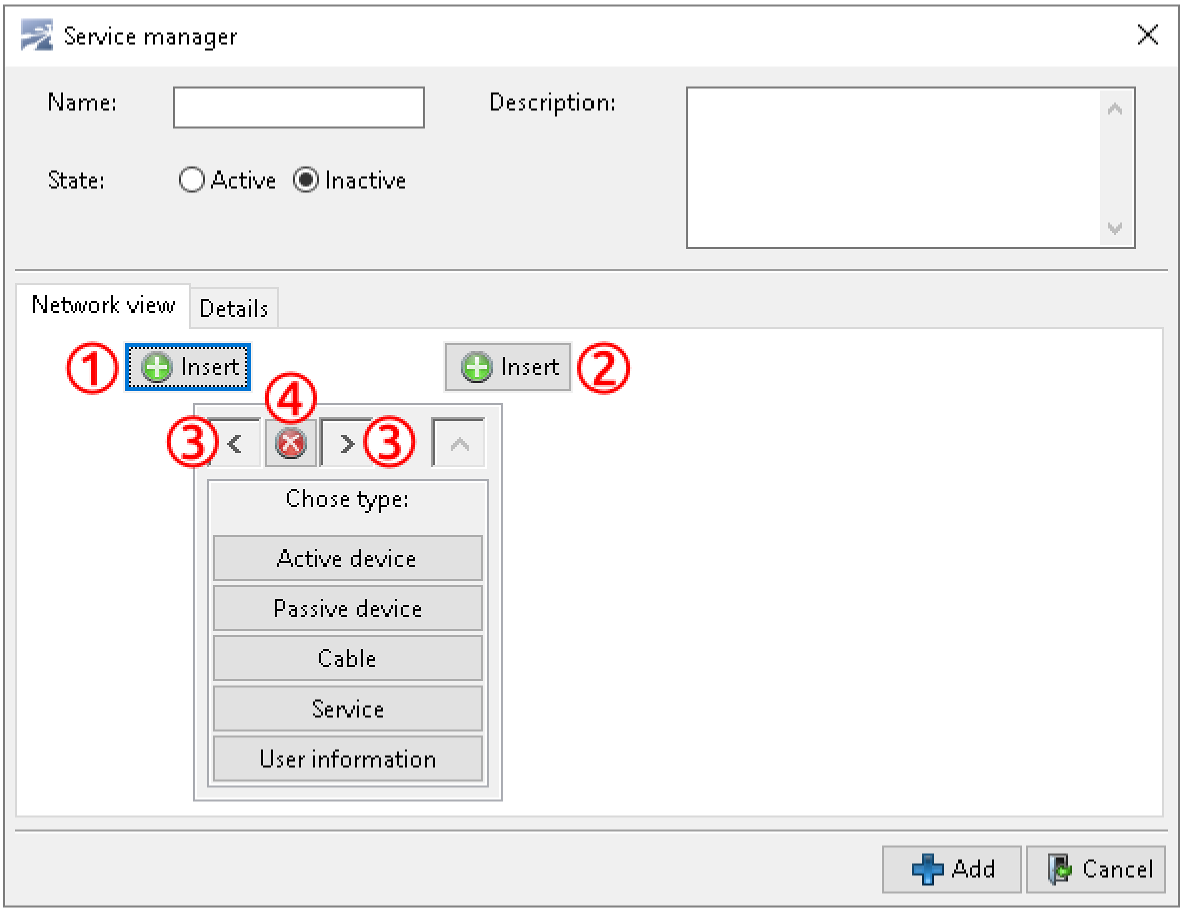

Service manager
Name:
Description:
State: ○ Active ● Inactive

Figure 134. NMP - Tabbed Data Panel - Services - Service Manager - Network View

Here you can define the service name and optionally a meaningful service description. By default, the service is created as "Inactive". To activate the service enable the option "Active".

NOTE NMP monitors the state of active services only. All the inactive services are not monitored and no log messages are generated.

By clicking the button `Insert` you can add the different elements of the service. Possible service elements are:

- **Active device:** This can be a real device or module connected to the network and shown in the device tree list. The port status has to be available.
- **Passive device:** This can be an unmonitored device, a passive module or a third party device not supported by the NMP. You can choose between the following passive device types:
    - Patch
    - Attenuator
    - Splitter
    - Passive module
    - Other

For each passive device type you can specify the respective value like loss in dB or ports of a device's passive module. Additionally you can define a meaningful description.

- **Cable:** A cable that is previously defined in the cable manager (see Section 7.10.3).
- **Service:** This can be a previously defined service.

  NOTE | It is not possible to choose the services recursively.

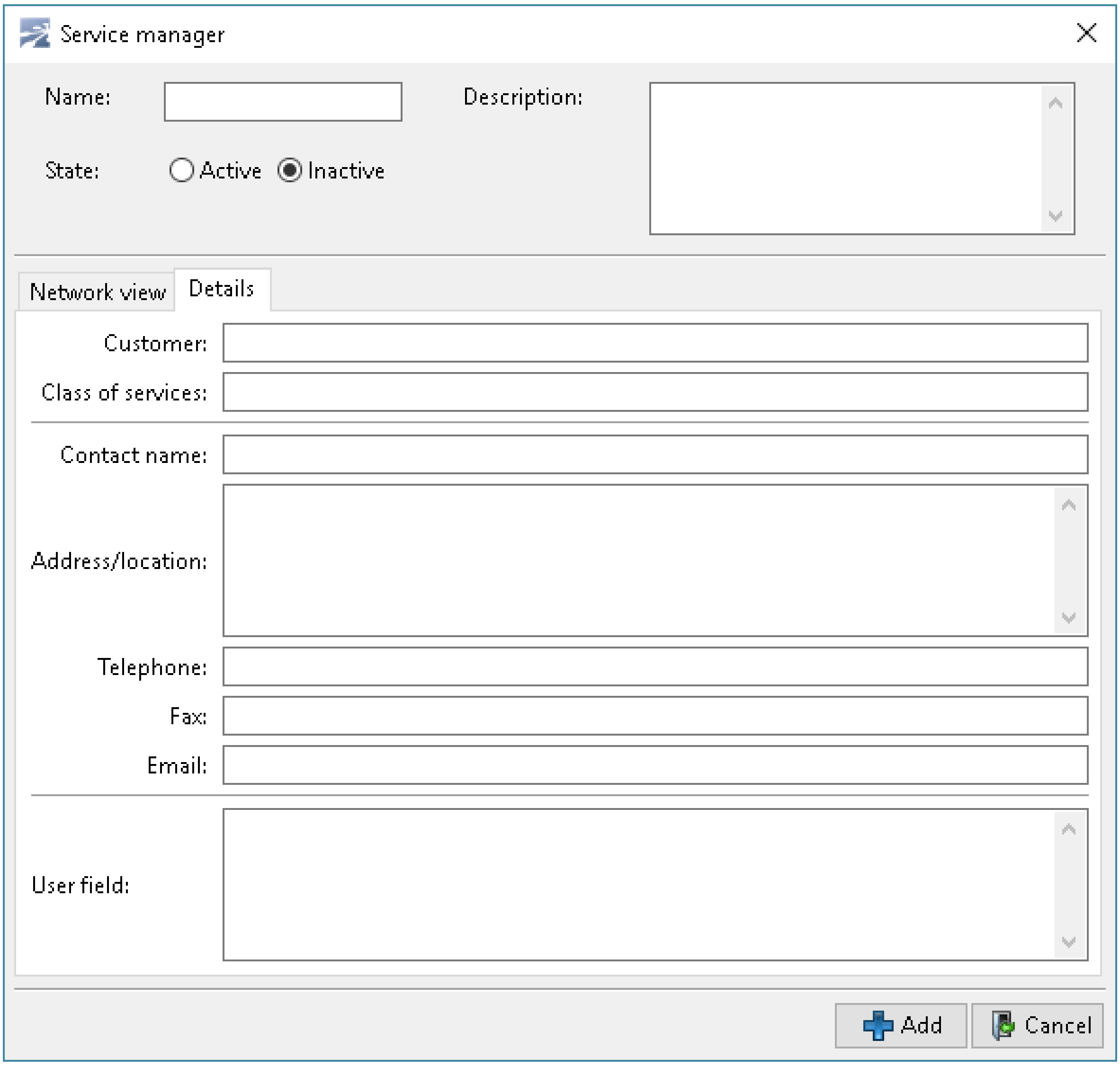
- **User Information:** This field allows adding some additional description for the respective service element.

To add an additional service element to an existing one, click the left (1) or right (2) `Insert` button on top of the respective element, depending on whether the new element should be placed before or after the existing element.

To delete an element, click on the [x] icon on top of the element (4). To change the element's order click on the respective horizontal arrows to move it left or right (3).

NOTE | It is not possible to redefine a previously determined service type. To change a service type insert another element, choose the correct service type and delete the former element.

In the "Details" view, you can add additional information, which may help to identify the service (e.g. information about the customer, some contact information and so on).



State: ○ Active ● Inactive

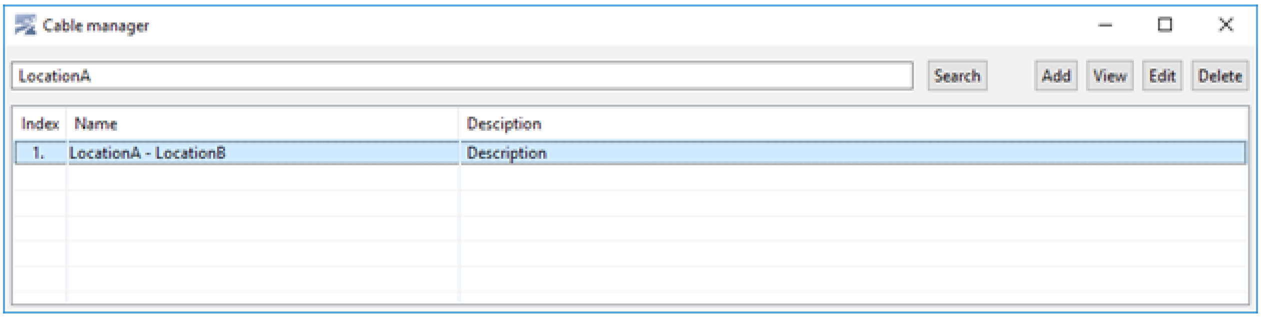
Figure 135. NMP - Tabbed Data Panel - Services - Service Manager - Details View

After clicking the button `Add`, the new service entry will be added to the list and NMP will start to monitor its state (if service in active state). NMP checks the service state by checking the status of each individual part of the service (each active/managed device).

Clicking the button `Cancel` closes the dialogue without creating the service entry.

7.10.3. Cable Manager

A click on the button `Cable Manager` opens the cable manager dialogue.



LocationA

Index	Name	Desciption
1.	LocationA - LocationB	Description

Figure 136. NMP - Tabbed Data Panel - Services - Cable Manager

You can define "virtual" fibre cables and configure descriptions and parameters. These definitions can be added as a part of a service (see Section 7.10.2).

The cable manager provides configuration and management of entries by clicking on the respective buttons:

- `Add`: Adds new cable entry
- `View`: Opens detailed read-only view of an existing cable entry
- `Edit`: Edits an existing cable entry
- `Delete`: Deletes an existing entry

NOTE

You can execute the commands `View`, `Edit` and `Delete` for existing entries by opening the context menu with a right-click on the respective entry in the cable list.

It is possible to search for entries by entering the cable name (or only a part of it) into the search field above the cable table and clicking the button `Search`. NMP then hides all cable entries that do not fit the search criteria.

NOTE

Hidden cable list entries are recognised by their missing index entry. E.g. if the index list counts "1","2" and "4", this indicates, that the cable entry with index "3" is filtered off.

To show all cable entries again, just search again with an empty search phrase.

After hitting the button `Add`, the "Cable creator" dialogue opens.

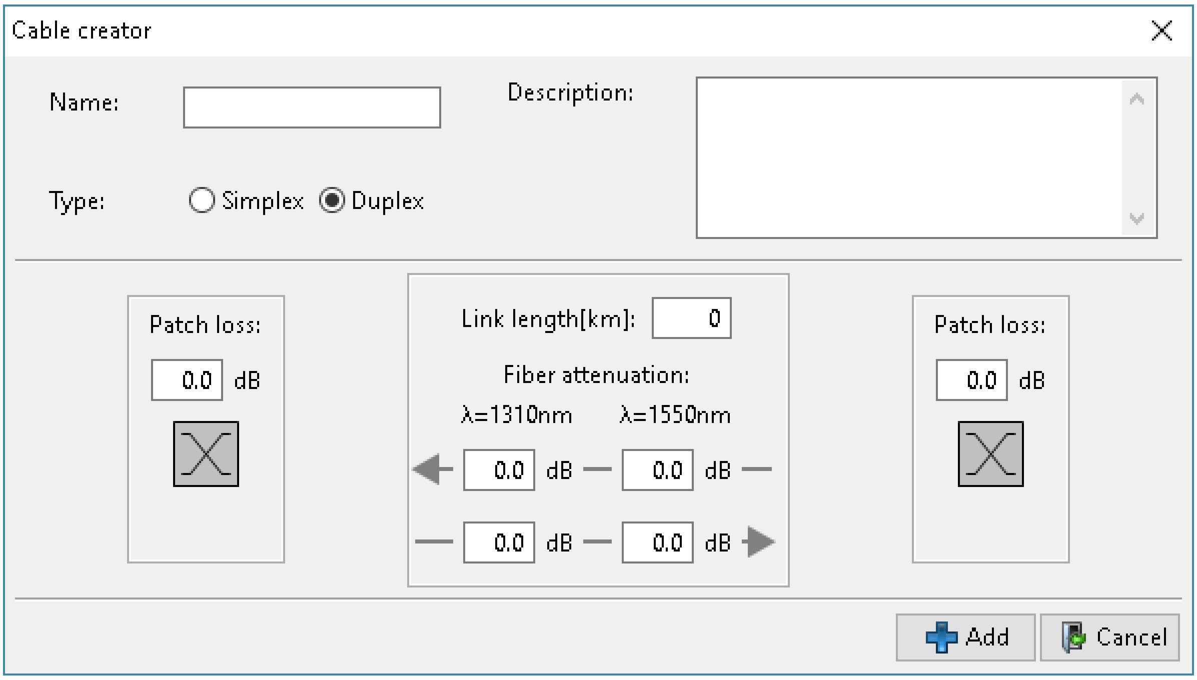


Figure 137. NMP - Tabbed Data Panel - Services - Cable Manager - Cable Creator

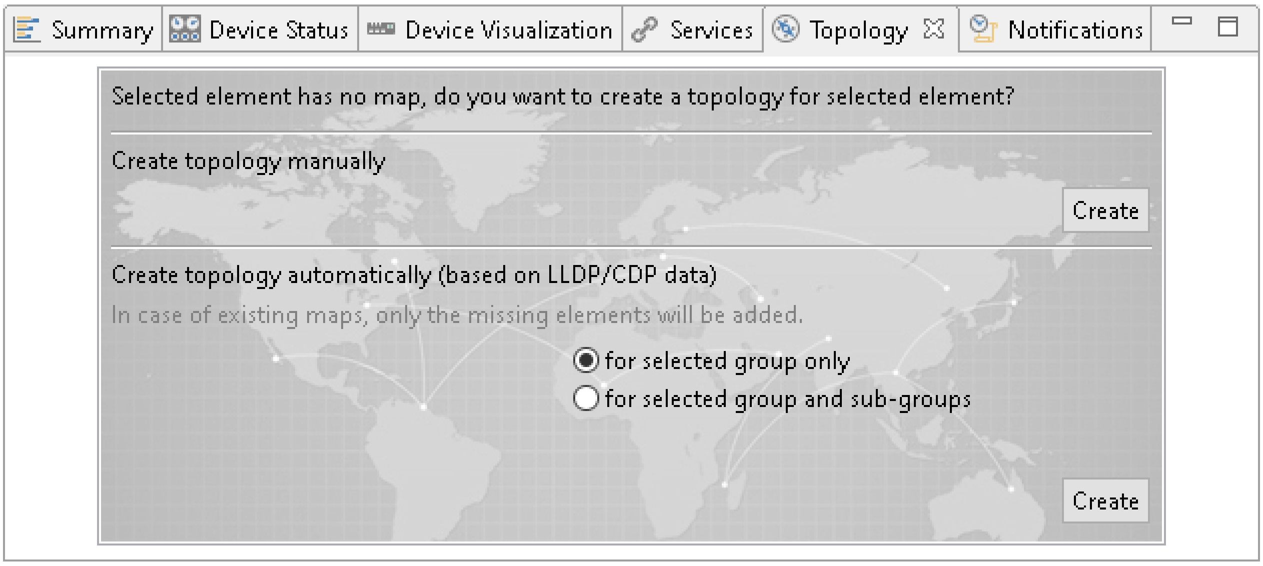
Enter the cable’s parameters, its name and optionally some meaningful description which will help to identify the cable. After selecting the button **Add**, the cable will be created and added to the list.

NOTE You will find information on patch loss, link length and attenuation in the fibre cable documentation of the cable provider. If not, you have to measure those values by yourself. Entering these values is optional. They are only used for link documentation.

7.11. Managing Topologies

NOTE Using services is available for both NMP Professional and NMP Enterprise.

To manage network topologies open the tab **Topology** in the tabbed data panel. As long as the device list is empty or no element (folder or device) is selected, the **Topology** tab will show the standard topology creation dialogue.



Selected element has no map, do you want to create a topology for selected element?

Create topology manually

Create topology automatically (based on LLDP/CDP data)

In case of existing maps, only the missing elements will be added.

● for selected group only

○ for selected group and sub-groups

Figure 138. NMP - Tabbed Data Panel - Topology - Standard Dialogue

NOTE Every group element can have its own topology. Selecting a folder or listed device inside this folder will show the respective folder topology or this topology creation dialogue.

Create a network topology manually by clicking on the button `Create` in the upper section.

In case of automated topology creation (button `Create` in the lower section), NMP will use data from the devices LLDP/CDP configuration to create the connections between these devices. For automatically created maps choose whether the map should be created just for the currently selected group or for the group and its sub-groups. If the topology already exists for a sub-group, NMP will add the missing elements automatically.

7.11.1. Menu Icons

To manage topologies the menu icons at the top of the topology area have the following functions:

Icon	Description
⚙	**Update topology** NMP will automatically check if there are any missing elements (which are available at the group and not added to the topology yet) at the current map. The missing devices or groups will be automatically added. Additionally, NMP will check if any device connections (links between devices) could be added. This works for both wired and "Optical Transport Networks" (OTN). For that purpose, NMP checks the LLDP/CDP status of each device.

Icon	Description
	Load map background image It is possible to illustrate the selected topology with a background image (e.g. floor plans). Possible file formats are `.jpg`, `.png`, `.bmp`, `.gif` and `.ico`.
	Remove map background image Click this icon to remove the topology's background image. Assigned devices are not affected.
	Hide/show map background image To concentrate on the allocated devices click this icon to turn off the background image. To show it again, click on this button a second time.
	Change map background image colour Use this function to change the colours of the map background image. Each click toggles between grey scale and original image colours.
	Hide/show device labels By default, all devices are shown with their IP address and device name. To gain a better overview in complex topologies this icon toggles the display of these device labels.
🔍	**Zoom in** Click this icon to zoom into the topology map. **NOTE** It is possible to use the mouse wheel to zoom in and out.
🔍	**Zoom out** Click this icon to zoom out of the topology map. **NOTE** It is possible to use the mouse wheel to zoom in and out.
1:1	**Zoom 1:1** Click this icon to show the topology map in its original dimensions.
	Zoom fit Click this icon to fit the topology map into the given tab area dimensions.
🖨	**Print map** Opens the print dialogue of the operating system.

Icon	Description
	Save map as image file Opens the file save dialogue of the operating system. Chose a directory and file name to exports the map as `.bmp` or `.png` file.
	Delete current topology Click this icon to delete the complete topology of the selected subgroup. All devices and background images are affected. After successful deletion the standard dialogue appears.
	Open window with unallocated map elements Opens a dialogue containing all unassigned devices and subgroups of the selected device list node. Allocate the listed elements either by drag and drop or by selecting them and clicking on the arrow icons on the right-hand side of the dialogue: > - Move selected item to the topology >> - Move all items to the topology
⇧	**Open parent map** Navigates to the topology map of the subgroup or group above the selected one. **NOTE** If the parent map does not contain a topology the standard dialogue appears.

7.11.2. Topology Map Elements

All devices and groups allocated on the map are represented by special icons and colour codes:

Icon	Description
	Represents a subgroup that could contain its own topology. **NOTE** A double-click on the icon opens the respective topology map or the standard dialogue for creating a new topology for this subgroup.
	Represents a device that is managed by NMP.

Icon	Description
✚ ✚✖	Represents a connection either to an off-map device allocated to another topology or a device not managed by NMP. A red "X" indicates a missing connection.
🟩	A green frame surrounding the map icon indicates either a properly working device or a subgroup containing properly working devices and subgroups.
🟨	Allocated map elements are surrounded by a yellow frame during polling the respective or all devices. As soon as polling has ended the respective status frame changes its colour depending on the polling result.
🟥 ⬛	A red and black blinking frame indicates a problem with the surrounded map element. The surrounded device either has a connection or configuration problem or the surrounded subgroup contains such a device. The affected connection between the respective devices blinks as well.
□	A grey frame indicates an unknown state of the device or subgroup.
☒	Button for deleting a connection between topolgy elements.

7.11.3. Adding Map Items Manually

After hitting the button `Create` in the upper section of the standard dialogue, NMP prepares an empty topology area. In the menu icon bar click on **Open window with unallocated map elements** (⊞). The following dialogue opens:

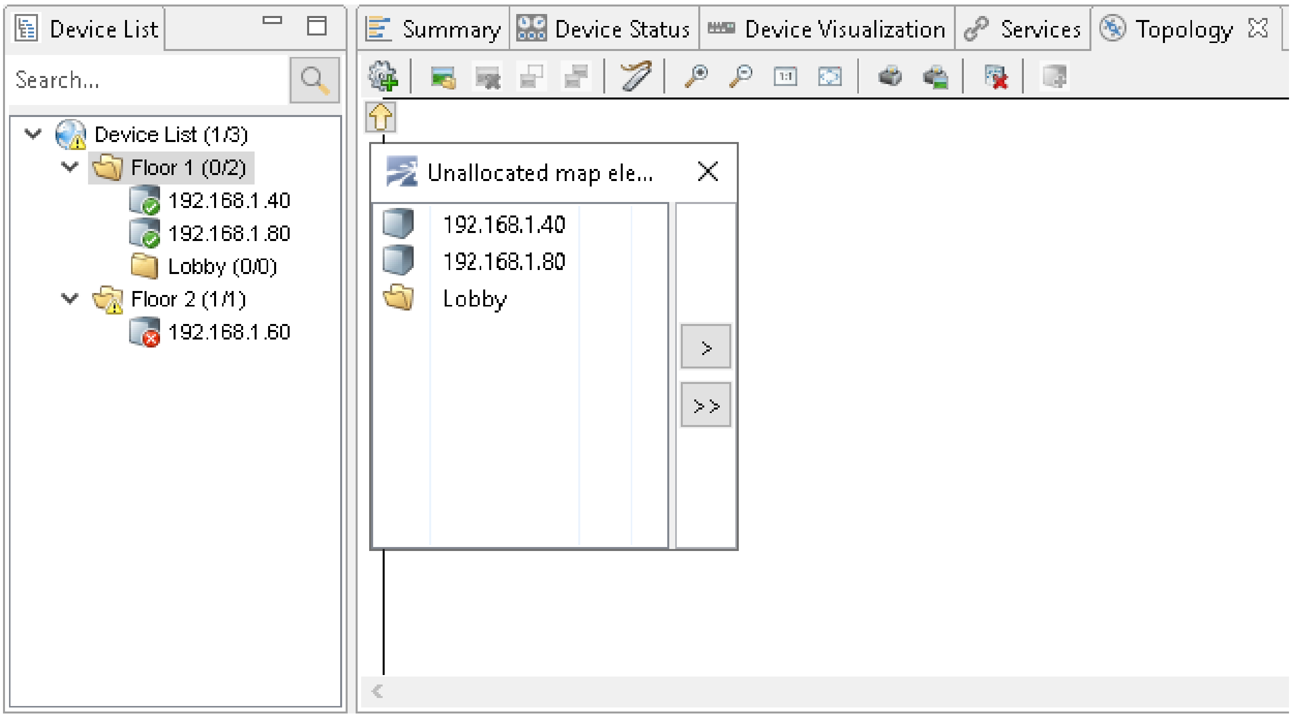


Figure 139. NMP - Tabbed Data Panel - Topology - Adding Items Manually

Allocate the listed elements either by drag and drop or by selecting them and clicking on the arrow icons on the right-hand side of the dialogue.

NMP automatically places the elements in the upper left corner of the topology area. Freely move the elements within the area as needed (drag and drop with left mouse button).

To move multiple elements (devices, folders, connections) at once hit the `Ctrl` key and click the left mouse button once. Now drag a rectangle around the respective elements. Left-click again and move the rectangle containing all elements as needed. To drop the contained elements, left-click again.

7.11.4. Adding Topology Connections Manually

After placing all the devices on the map connect them by keeping the `Shift` key pressed. Use this to draw lines (in the meaning of links) between devices.

Start with pressing the `Shift` key and left-click a device. The links between devices do not have to be straight lines, so it is possible to create multiple "link anchors" between both devices. Just click anywhere in the map to create an additional anchor. To finish the link, now select the second device.

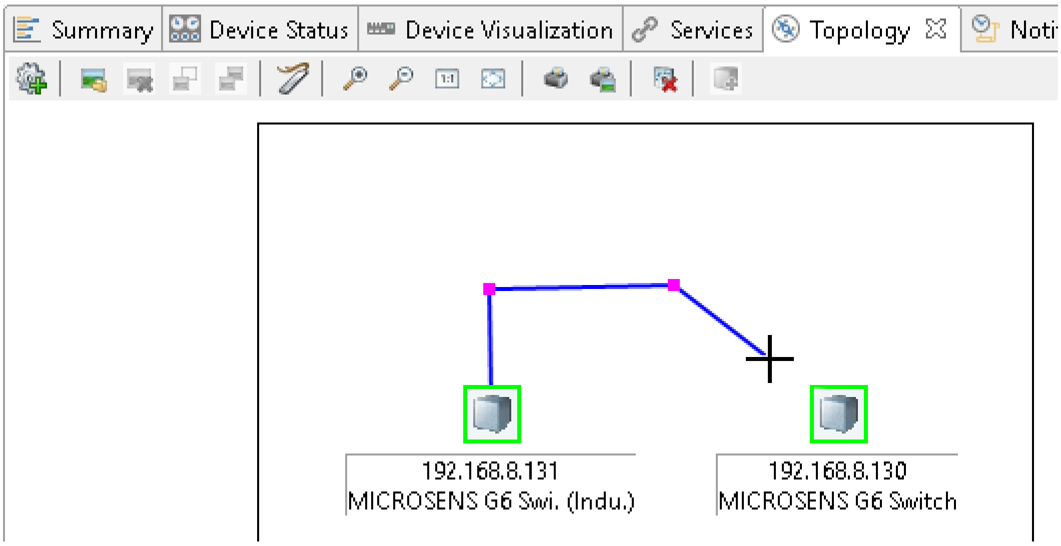


Figure 140. NMP - Tabbed Data Panel - Topology - Adding Multiple Anchors

Two devices can be connected by only one link. A connection can only be created between two different devices or between one device and one "off-map connection" element.

NOTE Keep in mind to leave the `Shift` key pressed the whole time.

As soon as the target device is connected NMP opens a connection dialogue to specify the participating ports of both devices. This dialogue contains the visualisation of both devices.

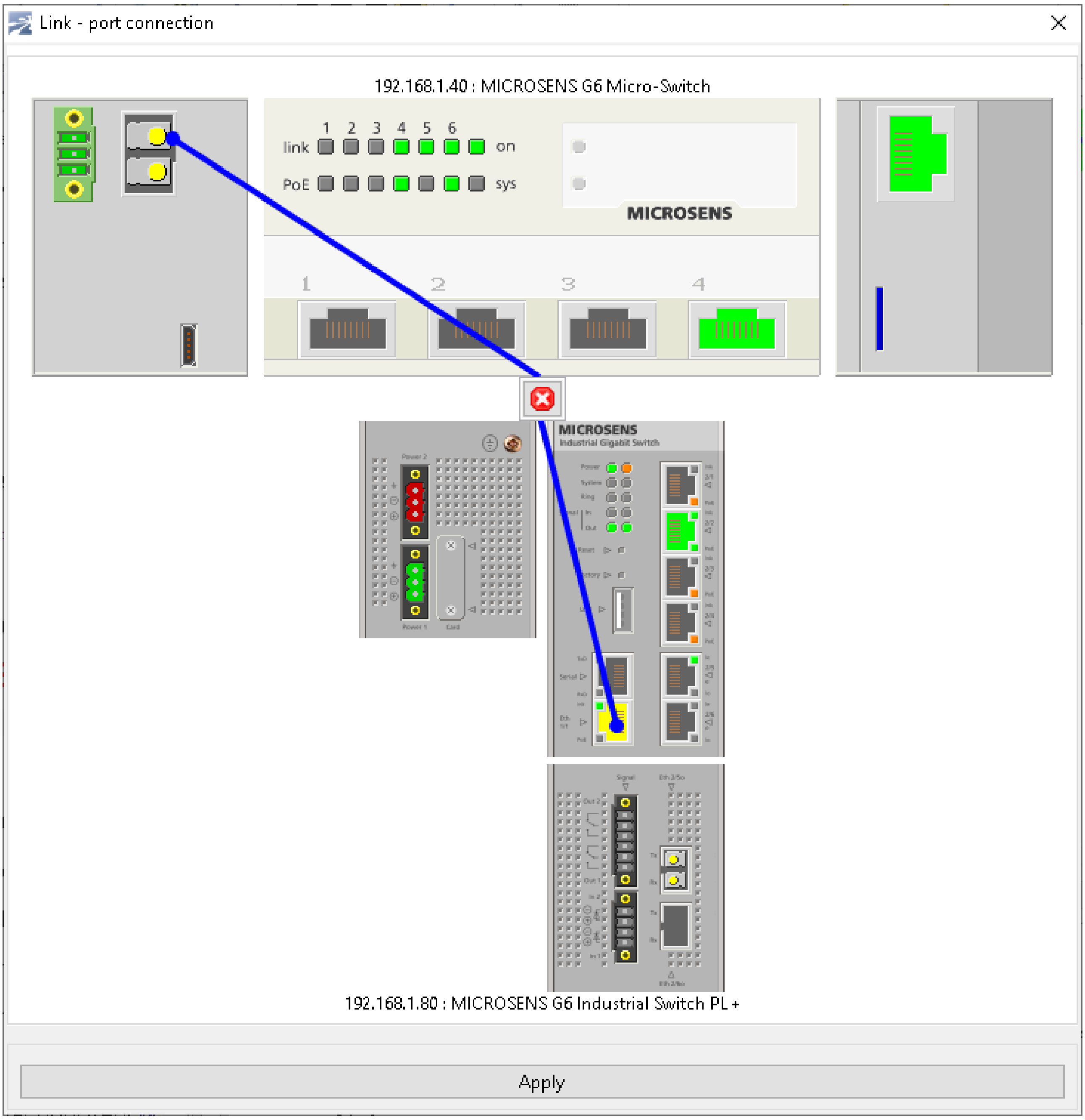
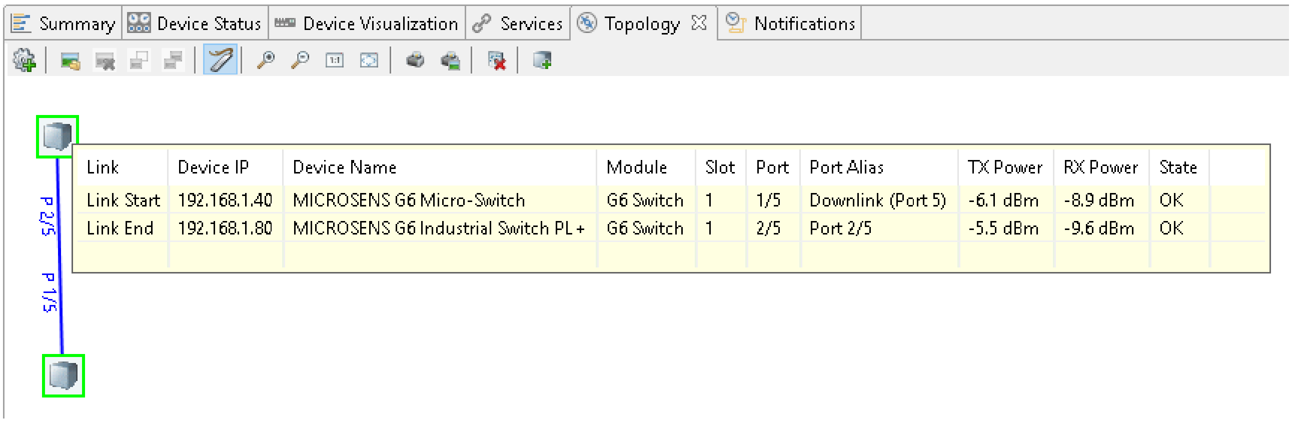

Link - port connection
192.168.1.40 : MICROSENS G6 Micro-Switch
1 2 3 4 5 6
link
on
PoE
sys
MICROSENS
1
2
3
4
MICROSENS
Industrial Gigabit Switch
192.168.1.80 : MICROSENS G6 Industrial Switch PL+
Apply

Figure 141. NMP - Tabbed Data Panel - Topology - Link Port Connection

Click on both the devices' ports which are connected. As a result the port connection is illustrated with coloured lines. Click on the button `Apply` to accept the setting. In the topology map the connection additionally shows the respective port numbers.

To delete a connection click on the respective delete icon (☒).

If the connected devices are supported by NMP and their management data is available, NMP will display a tooltip when the mouse cursor is hovering above a device, containing specific information about connections to other devices.



Link	Device IP	Device Name	Module	Slot	Port	Port Alias	TX Power	RX Power	State
Link Start	192.168.1.40	MICROSENS G6 Micro-Switch	G6 Switch	1	1/5	Downlink (Port 5)	-6.1 dBm	-8.9 dBm	OK
Link End	192.168.1.80	MICROSENS G6 Industrial Switch PL+	G6 Switch	1	2/5	Port 2/5	-5.5 dBm	-9.6 dBm	OK

Figure 142. NMP - Tabbed Data Panel - Topology - Link Parameters Tooltip

The "Topology Manager" uses queried device data to monitor the defined link state. If one or both devices are not available, or the link between some of the connected devices is down, the link will blink red and black, indicating an error.

It is possible to change the link appearance of manually created links. Just select the link anchor with the right mouse button and choose an option from the context menu.

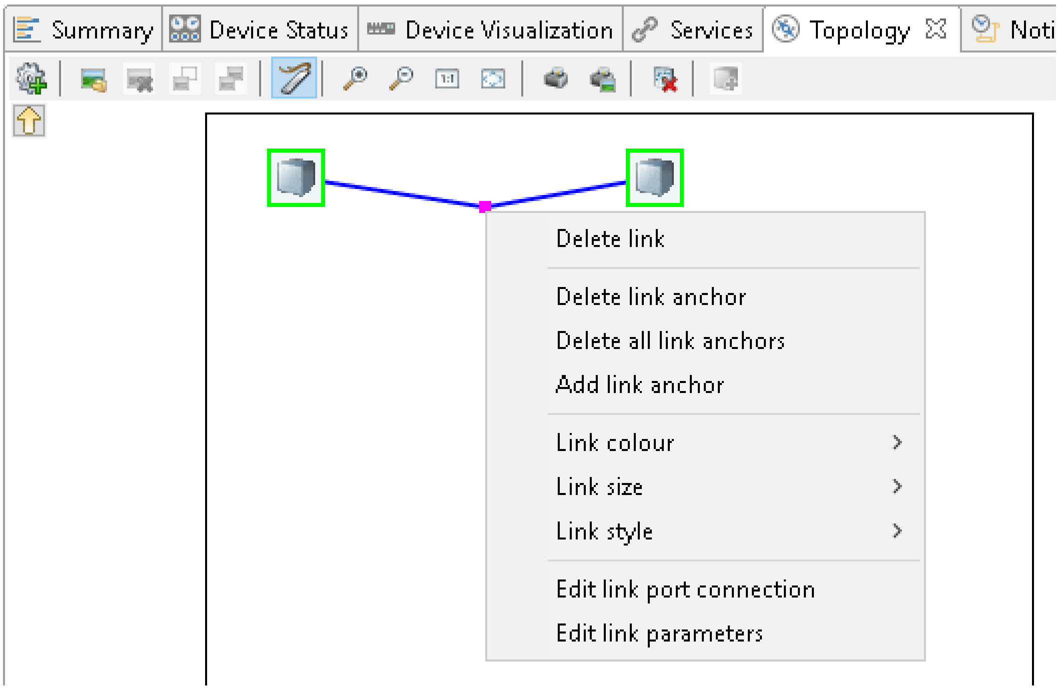


Figure 143. NMP - Tabbed Data Panel - Topology - Link Anchor Context Menu

Delete the link or change the link colour, size and style. Add or remove anchors to fit the link to the map. It is also possible to describe link parameters with a click on **Edit link port connection**.

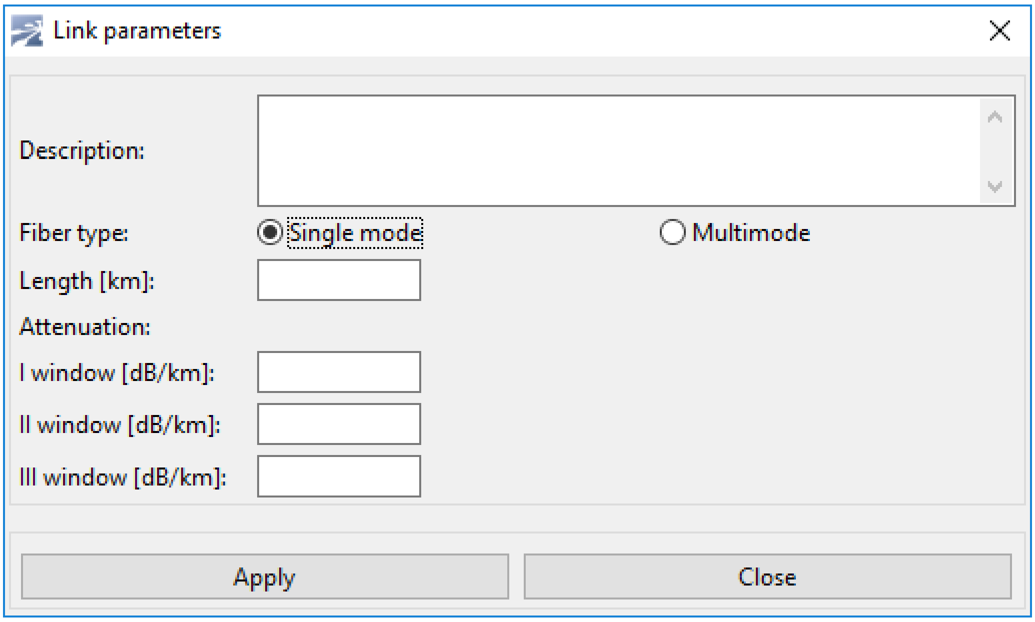


Figure 144. NMP - Tabbed Data Panel - Topology - Link Parameters

NOTE Editing link settings is only possible with manually generated connections.

7.11.5. Off-Map Connections

It is possible to add special map elements representing so-called "Off-Map connections". Such map elements are represented by special icons with a grey outline.

For adding an off-map connection right-click the respective topology and choose the **Add Off-Map connection** entry in the opening context menu.

For deleting off-map connections or assigning special descriptions right-click the respective connection and choose the desired option from the appearing context menu.

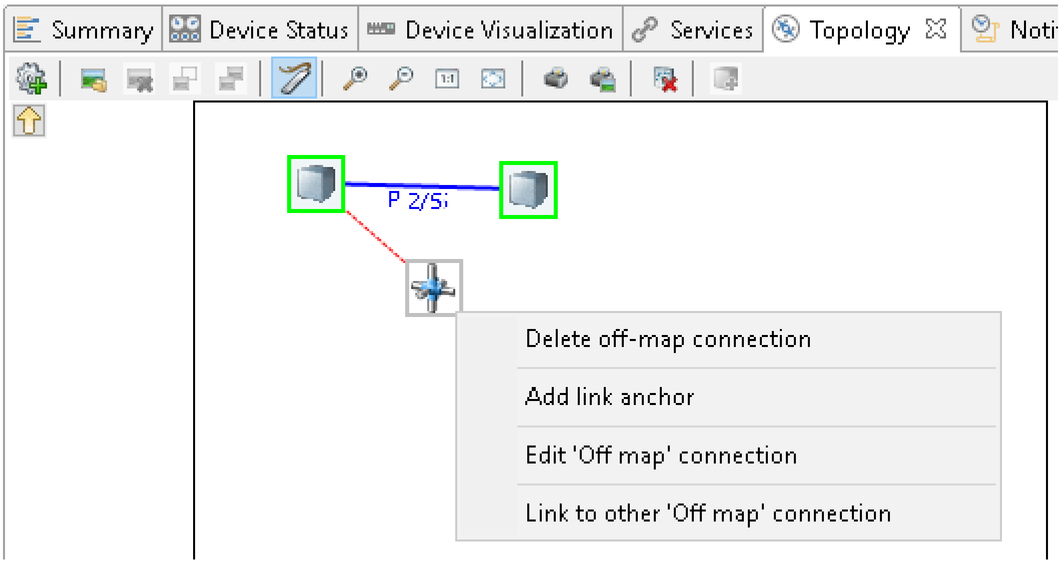

Summary
Device Status
Device Visualization
Services
Topology
Noti
P 2/S
Delete off-map connection
Add link anchor
Edit 'Off map' connection
Link to other 'Off map' connection

Figure 145. NMP - Tabbed Data Panel - Topology - Off-Map Connections - Context Menu

Off-map connections can be used to connect two different devices located on different maps. In such cases create off-map connections on two separate maps (e.g. "Map A" and "Map B"). A "Map A" device and a "Map B" device can be connected to a specific "Off-Map connection A" and "B". Then define a link between these two off-map connections using the **Link to other Off-Map connection** menu option in the context menu. If two off-map connections are linked, selecting one of them by double-clicking on it will automatically open the second map (with linked off-map connection). The link between two devices connected by an off-map connection is monitored just like two devices connected directly (on the same map).

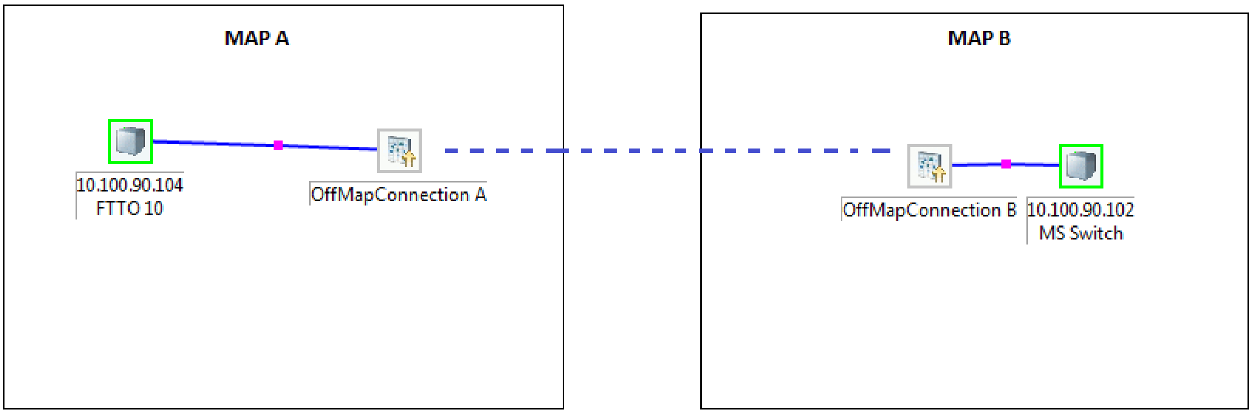


Figure 146. NMP - Tabbed Data Panel - Topology - Off-Map Connections (Example)

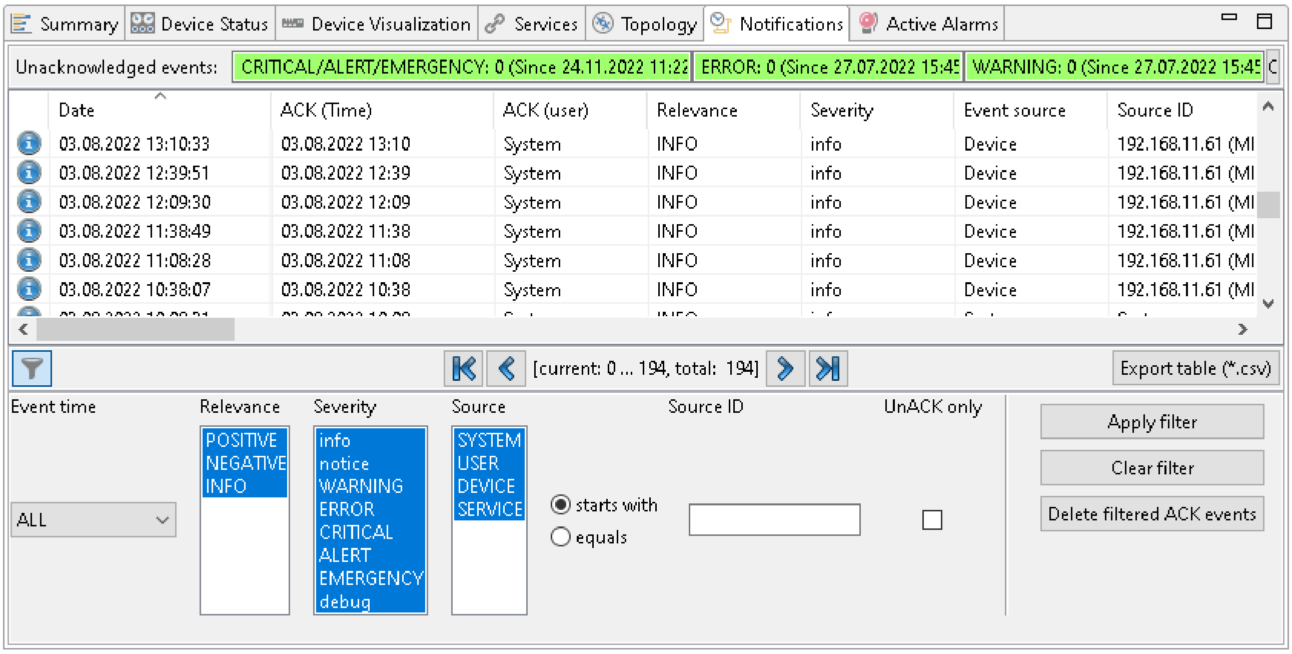
NOTE Off-map connections can also represent third party devices not supported by NMP.

7.12. Managing Notifications

NOTE Managing notifcations is available for both NMP Professional and NMP Enterprise.

If not already active, select **Window › Switch Perspective › Network Administration**.

All messages are displayed on the tab **Notifications**.



Date	ACK (Time)	ACK (user)	Relevance	Severity	Event source	Source ID
03.08.2022 13:10:33	03.08.2022 13:10	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 12:39:51	03.08.2022 12:39	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 12:09:30	03.08.2022 12:09	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 11:38:49	03.08.2022 11:38	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 11:08:28	03.08.2022 11:08	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 10:38:07	03.08.2022 10:38	System	INFO	info	Device	192.168.11.61 (MI

Figure 147. Stand Alone Client - Tabbed Data Panel - Notifications

NOTE To use events first enable event logging in the main menu under **Settings › Log File/Email/Events**.

Messages are displayed at the log table in different ways what makes it easier to pay attention to important events. The way to display messages depends on the event's predetermined relevance level and its configured severity level.

There are three different levels of relevance for an event message:

- **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.

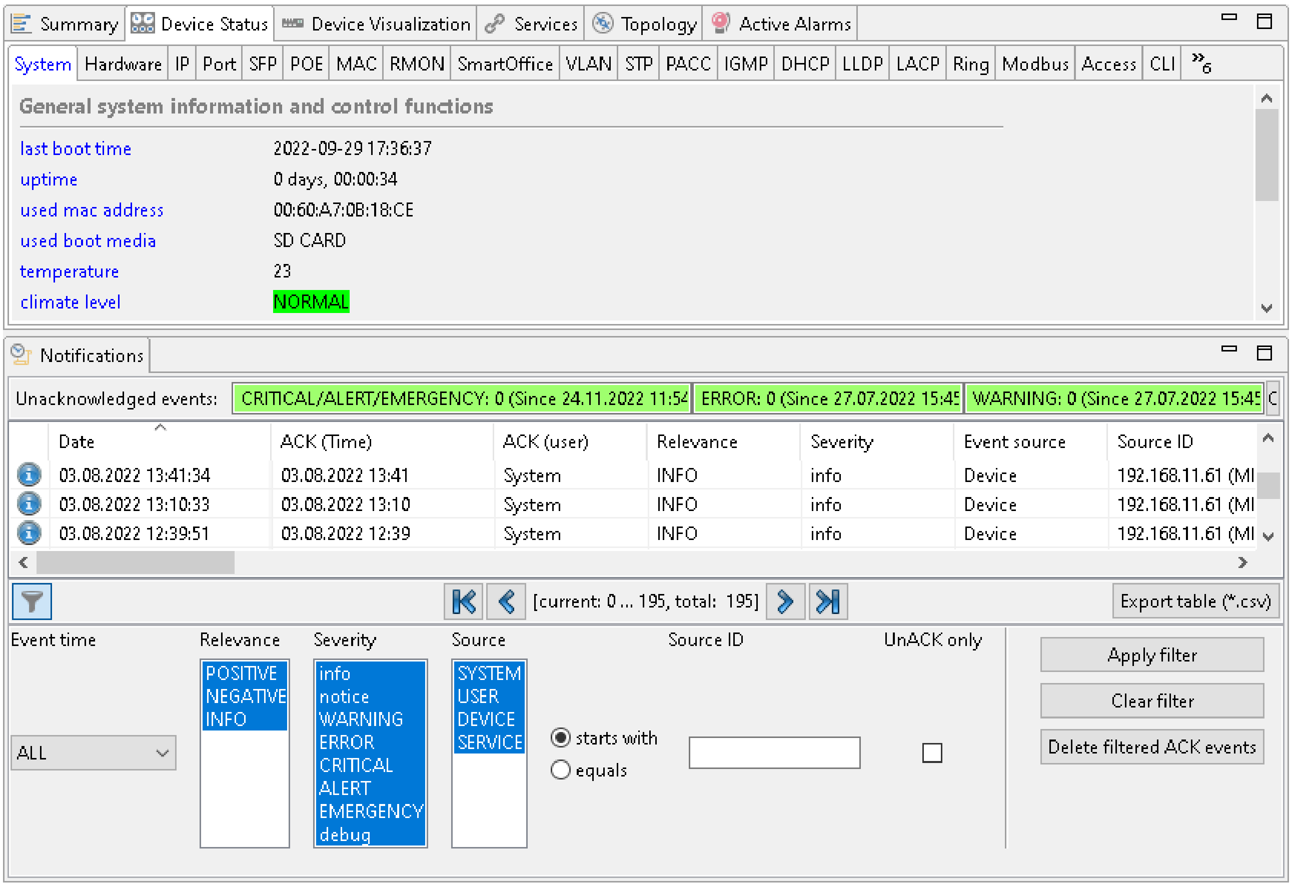
Additionally, each event has an assigned severity level, which can be modified. There are six different severity levels indicated by the formatting and the respective icon in the left column of the table:

Icon	Severity Level	Description
	DISABLED	The event will not generate a log entry (not displayed, nor logged). It is greyed out.
ℹ	NOTICE	This is an informational event that does not require special attention (e.g. system messages). It is formatted in black font colour.
✓	NO_ERROR	This is a success notification (e.g. a configuration applied successfully). It is formatted in green font colour.
⚠	WARNING	This is a low level warning message. It is formatted in black font colour on yellow background.
✖	ERROR	This is an error message that requires user attention. It is formatted in red font colour on orange background.
✖	CRITICAL	This is a critical error message that requires immediate user attention. It is formatted in black font colour on red background.

At the top of the log table, the counters for unacknowledged notifications are consolidated.

When right-clicking a log table entry and clicking on context menu entry **Show device** the respective device in the "Device List Tree View" gets activated. Opening the tab **Device Status** shows the entire device’s status values and configuration settings.

TIP When drag and drop the tab **Notifications** below the tabbed data panel choose the respective device and see the device status immediately in the tab **Device Status** above (supposed the device is available).



General system information and control functions

last boot time	2022-09-29 17:36:37
uptime	0 days, 00:00:34
used mac address	00:60:A7:0B:18:CE
used boot media	SD CARD
temperature	23
climate level	NORMAL

Unacknowledged events: CRITICAL/ALERT/EMERGENCY: 0 (Since 24.11.2022 11:54 ERROR: 0 (Since 27.07.2022 15:45 WARNING: 0 (Since 27.07.2022 15:45

Date	ACK (Time)	ACK (user)	Relevance	Severity	Event source	Source ID
03.08.2022 13:41:34	03.08.2022 13:41	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 13:10:33	03.08.2022 13:10	System	INFO	info	Device	192.168.11.61 (MI
03.08.2022 12:39:51	03.08.2022 12:39	System	INFO	info	Device	192.168.11.61 (MI

[current: 0 ... 195, total: 195]

Event time: ALL

Relevance: POSITIVE, NEGATIVE, INFO

Severity: info, notice, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY, debug

Source: SYSTEM, USER, DEVICE, SERVICE

Source ID: ● starts with ○ equals

UnACK only: □

Figure 148. Stand Alone Client - Tabbed Data Panel - Notification and Device Status

7.12.1. Filtering Notifications

Filter all the logged event messages by using the filter options available at the filter bar.

NOTE If the filter section is hidden click on `Show filter` (funnel symbol) on the bottom left of the dialogue. To toggle the filter section, click on `Hide filter` (funnel symbol) again.

The following options are available:

- **Relevance:** All messages with chosen relevance level will be displayed.
- **Severity:** All messages with chosen severity level will be displayed.
- **Source:** All messages generated by chosen source will be displayed. Messages can be generated by `SYSTEM`, `USER`, `DEVICE` or `SERVICE`.

NOTE It is possible to select one or more (with button `Ctrl` pressed) entries for Relevance, Severity and Source.

- **Source ID:** Enables filter to show the messages generated by the source with defined source ID (e.g. user name, device IP address).

- **starts with and equals:** Determine, whether the event message must fit the identical Source ID or just starts with the respective text string (e.g. to filter event messages from devices of a special IP range).
- **UnAck only:** Enables filter to show the unacknowledged messages.

All the filter options can be combined in order to display the required messages.

To execute the filter click on the following buttons:

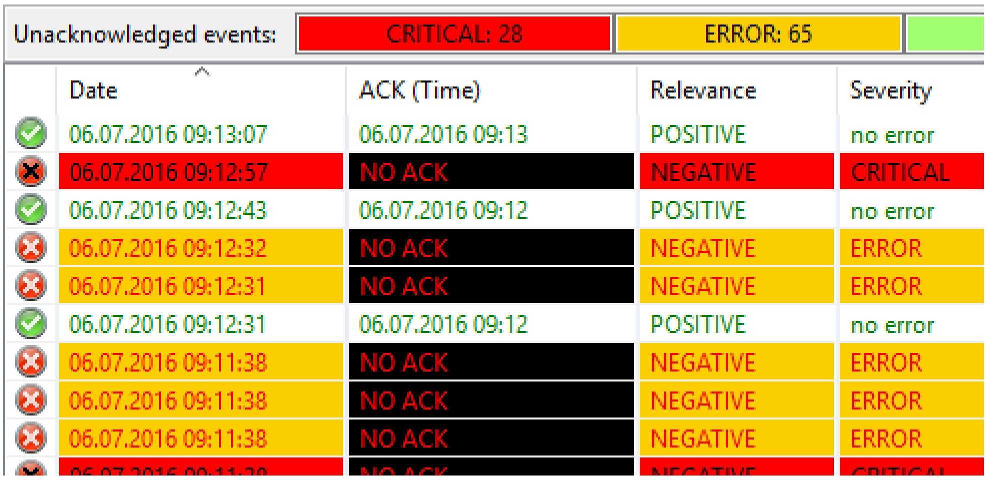
- `Apply filter`: Enables the defined filter to show the required messages.
- `Clear filter`: Resets filter.
- `Delete filtered UnACK events`Deletes the filtered messages (only the acknowledged messages can be deleted).
- `Event configuration`: Opens the "Events configuration" dialogue (see Section 7.13).
- `Export table (*.csv)`: Exports the currently filtered messages as `.csv` file.

7.12.2. Acknowledging Notifications

Notifications of events with the following severities have to be acknowledged:

Icon	Severity Level	Description
⚠	WARNING	This is a low level warning message.
⊗	ERROR	This is an error message that requires user attention.
✖	CRITICAL	This is a critical error message that requires immediate user attention.

The unacknowledged messages are marked with red "NO ACK" text on black background at the "ACK (Time)" column.



Unacknowledged events: CRITICAL: 28 ERROR: 65

	Date	ACK (Time)	Relevance	Severity
✓	06.07.2016 09:13:07	06.07.2016 09:13	POSITIVE	no error
✖	06.07.2016 09:12:57	NO ACK	NEGATIVE	CRITICAL
✓	06.07.2016 09:12:43	06.07.2016 09:12	POSITIVE	no error
⊗	06.07.2016 09:12:32	NO ACK	NEGATIVE	ERROR
⊗	06.07.2016 09:12:31	NO ACK	NEGATIVE	ERROR
✓	06.07.2016 09:12:31	06.07.2016 09:12	POSITIVE	no error
⊗	06.07.2016 09:11:38	NO ACK	NEGATIVE	ERROR
⊗	06.07.2016 09:11:38	NO ACK	NEGATIVE	ERROR
⊗	06.07.2016 09:11:38	NO ACK	NEGATIVE	ERROR
✖	06.07.2016 09:11:38	NO ACK	NEGATIVE	CRITICAL

Figure 149. Stand Alone Client - Tabbed Data Panel - Notifications - ACK Column Detail

To acknowledge one notification, double-click on the selected table entry, or choose the **ACK Event** from table context menu. As soon as the message is acknowledged, the date and time of acknowledgement is displayed instead of "NO ACK" text.

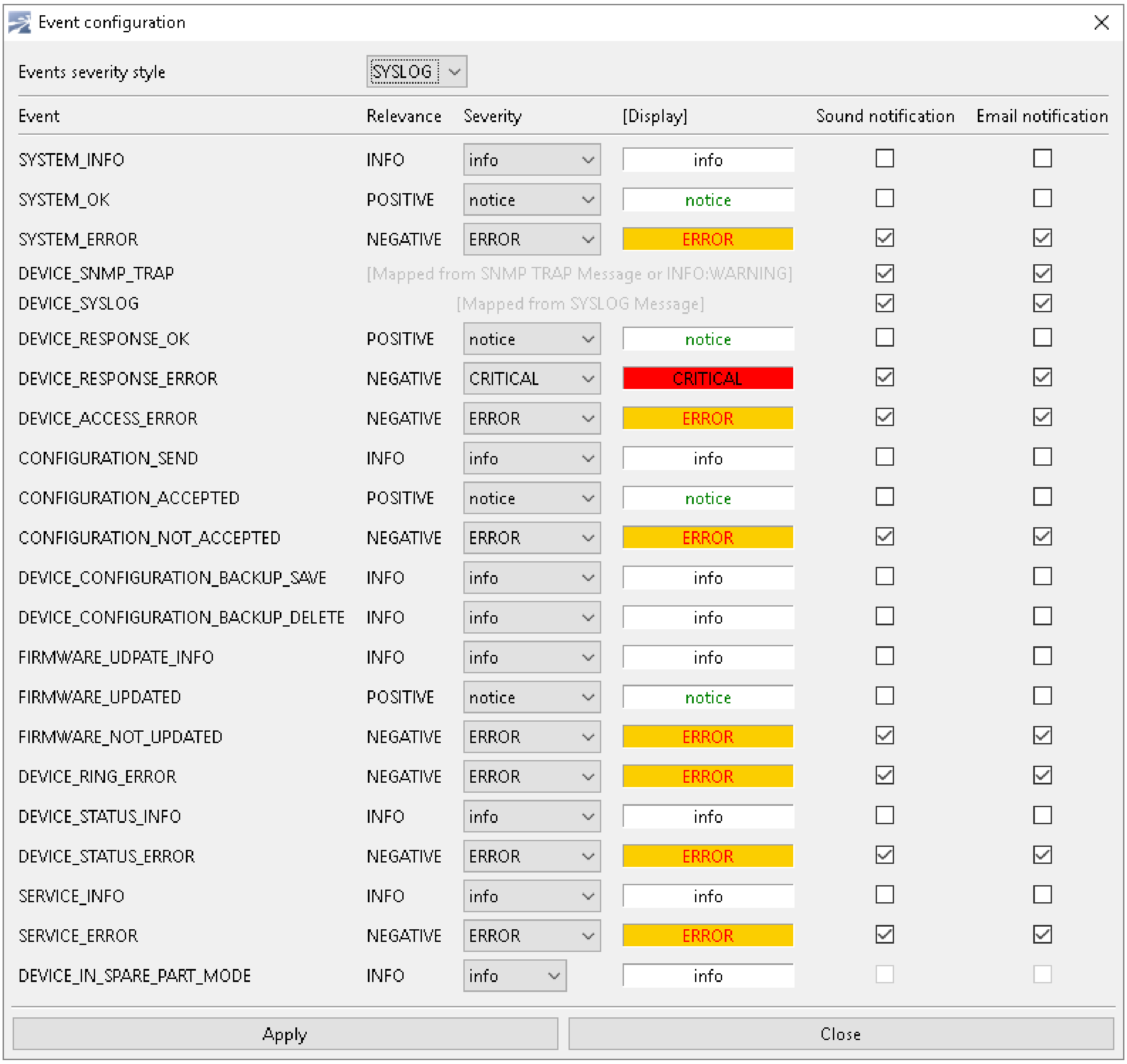
To acknowledge all notifications at once, click on the button `ACK` at the upper right hand pane of the dialogue.

NOTE The notification of events which do not require user acknowledgement are always acknowledged automatically by the system.

7.13. Configuring Events

NOTE Configuring events is available for both NMP Professional and NMP Enterprise.

To configure the events open the tab **Notifications** and select the button `Event configuration` in the filter section under the log table.



Events severity style: SYSLOG

Event	Relevance	Severity	[Display]	Sound notification	Email notification
SYSTEM_INFO	INFO	info	info	□	□
SYSTEM_OK	POSITIVE	notice	notice	□	□
SYSTEM_ERROR	NEGATIVE	ERROR	ERROR	☑	☑
DEVICE_SNMP_TRAP	[Mapped from SNMP TRAP Message or INFO:WARNING]			☑	☑
DEVICE_SYSLOG		[Mapped from SYSLOG Message]		☑	☑
DEVICE_RESPONSE_OK	POSITIVE	notice	notice	□	□
DEVICE_RESPONSE_ERROR	NEGATIVE	CRITICAL	CRITICAL	☑	☑
DEVICE_ACCESS_ERROR	NEGATIVE	ERROR	ERROR	☑	☑
CONFIGURATION_SEND	INFO	info	info	□	□
CONFIGURATION_ACCEPTED	POSITIVE	notice	notice	□	□
CONFIGURATION_NOT_ACCEPTED	NEGATIVE	ERROR	ERROR	☑	☑
DEVICE_CONFIGURATION_BACKUP_SAVE	INFO	info	info	□	□
DEVICE_CONFIGURATION_BACKUP_DELETE	INFO	info	info	□	□
FIRMWARE_UDPATE_INFO	INFO	info	info	□	□
FIRMWARE_UPDATED	POSITIVE	notice	notice	□	□
FIRMWARE_NOT_UPDATED	NEGATIVE	ERROR	ERROR	☑	☑
DEVICE_RING_ERROR	NEGATIVE	ERROR	ERROR	☑	☑
DEVICE_STATUS_INFO	INFO	info	info	□	□
DEVICE_STATUS_ERROR	NEGATIVE	ERROR	ERROR	☑	☑
SERVICE_INFO	INFO	info	info	□	□
SERVICE_ERROR	NEGATIVE	ERROR	ERROR	☑	☑
DEVICE_IN_SPARE_PART_MODE	INFO	info	info	□	□

Figure 150. NMP - Tabbed Data Panel - Notifications - Event Configuration

For each event type enable or disable the sound and email notifications.

In such case, NMP will play a sound or send an email to all defined recipients when the event will be generated.

To set the events severity style select the respective entry from the drop-down list on top of the dialogue:

- **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.

As a result the events are shown with the specific severity name, e.g.:

- MAJOR (ITU) corresponds to CRITICAL (SYSLOG)
- CRITICAL (ITU) corresponds to ALERT (SYSLOG)

NOTE Please remember to enable and configure the email and sound notifications in the main menu under **Settings › Log file/E-mail/Events**.

7.14. Managing Industrial Ring Errors

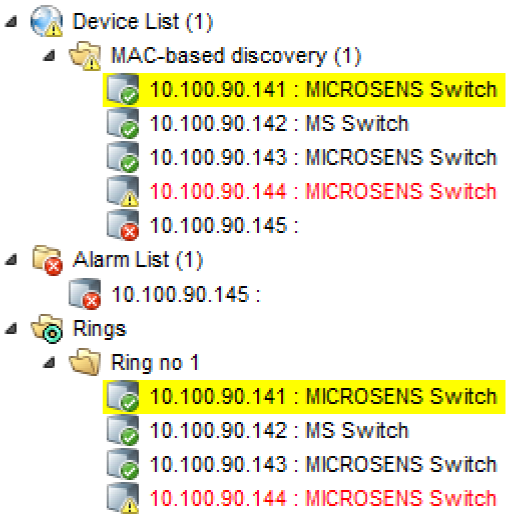
NOTE Managing ring errors is available for both NMP Professional and NMP Enterprise.

In the device tree list it is possible to group ring devices (see Section 4.8.2.15).

When ring errors happen in the network, NMP indicates the responsible devices causing the error by their entries highlighted in red text and a special "warning" icon (⚠) on the left hand pane.

NOTE In most cases errors are caused by fibre link failures between two ring switches. In such cases two switches with link failures are marked with red text and the respective icon.

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



- Device List (1)
  - MAC-based discovery (1)
    - 10.100.90.141 : MICROSENS Switch
    - 10.100.90.142 : MS Switch
    - 10.100.90.143 : MICROSENS Switch
    - 10.100.90.144 : MICROSENS Switch
    - 10.100.90.145 :
- Alarm List (1)
  - 10.100.90.145 :
- Rings
  - Ring no 1
    - 10.100.90.141 : MICROSENS Switch
    - 10.100.90.142 : MS Switch
    - 10.100.90.143 : MICROSENS Switch
    - 10.100.90.144 : MICROSENS Switch

Figure 151. NMP Professional - Device Tree List View - Industrial Ring Errors

This should lead to check the ring configuration of the responsible device or its correct connection 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 NMP.

7.15. Server Instance as Windows Service

NOTE Running the server component of NMP Enterprise as a Microsoft Windows ® service is exclusivly available with NMP Enterprise.

On Microsoft Windows® operating systems it is possible to install the server instance of the application as a Windows service. A service is a long-running executable that performs specific features and which is designed not to require user intervention. Windows services can be configured to start on operating system boot-up and to run in the background as long as the operating system is running. They can be also controlled manually.

In order to install/uninstall the server instance as a service, the Server Manager must be started with system administrator rights. Additionally, the windows user account which will be used to install the server service must have the "Log on as a service" rights.

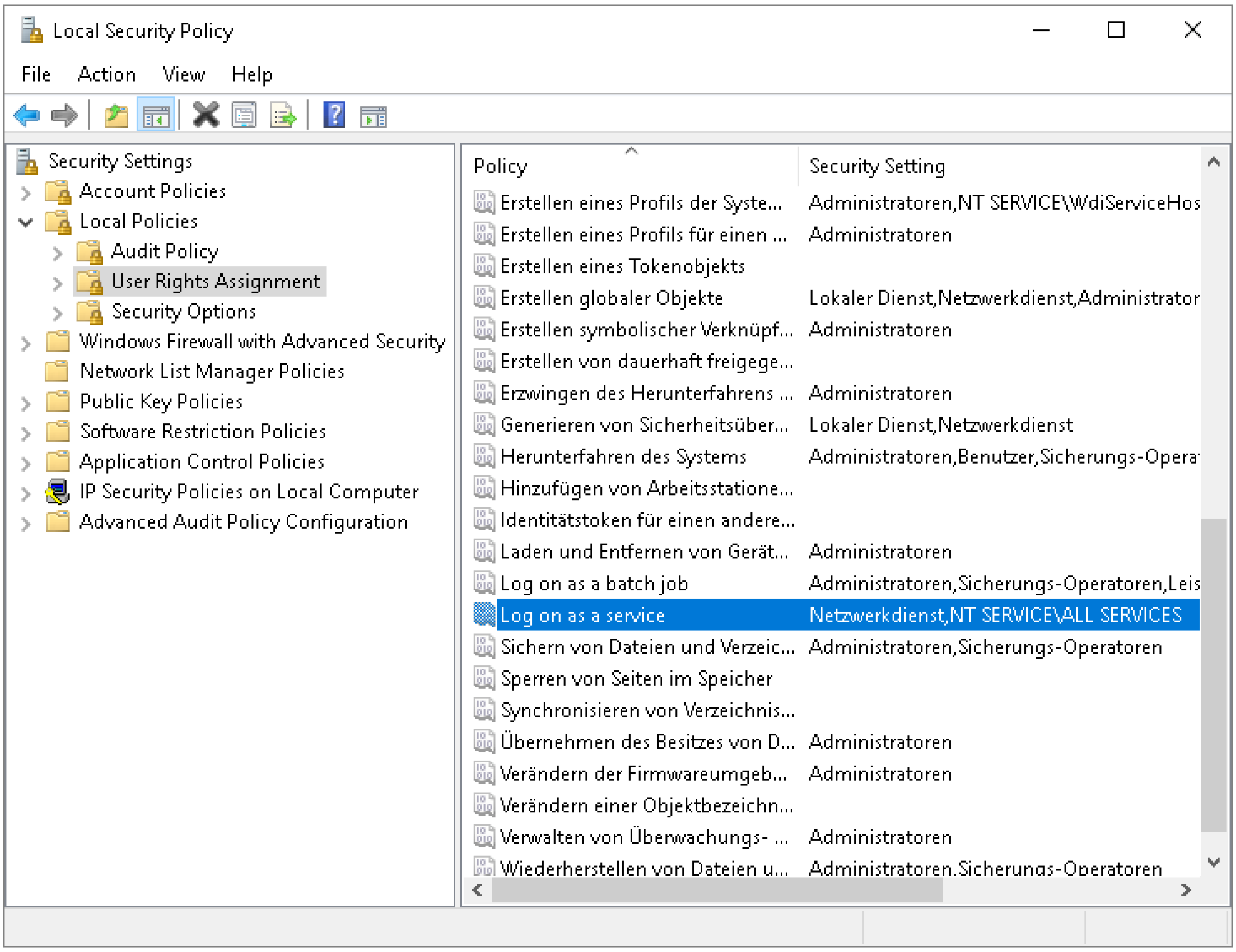
NOTE Please note the following update information:

- Updating the application from a version less or equal v2.6 to v2.9.6 or newer, the re-installation of the server instance as Microsoft Windows® service is required!
- Updating the application from version 2.9.3 to v2.9.6 or newer does not require re-installation of the server instance as Microsoft Windows® service.

7.15.1. Provide "Log on as a service" rights to a Windows account

The following steps are necessary to provide "Log on as a service" rights:

1. Open "Local Security Policy" via **Windows System** › **Windows Control Panel** › **System and Security** › **Administrative Tools**.
2. In the left-hand pane "Security Settings", select **Local Policies** › **User Rights Assignments**

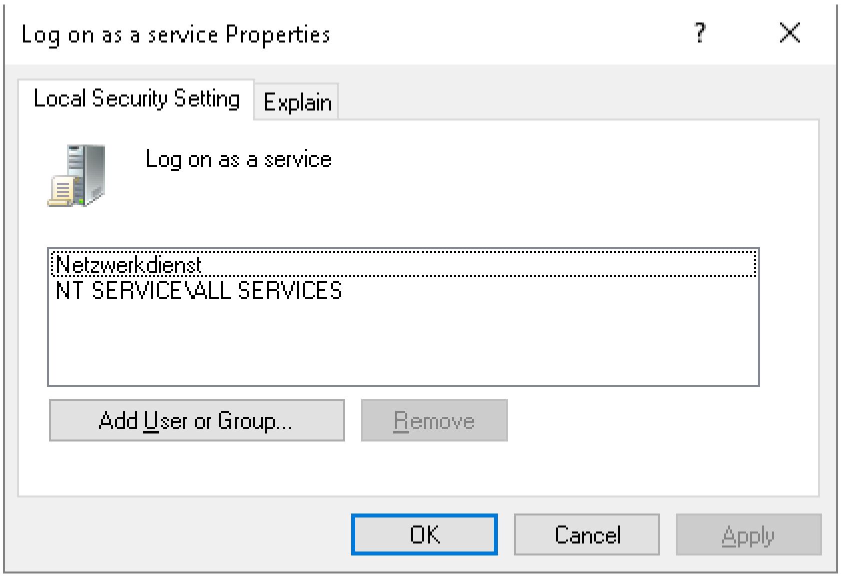


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Erstellen eines Profils der Syste...	Administratoren,NT SERVICE\WdiServiceHos
Erstellen eines Profils für einen ...	Administratoren
Erstellen eines Tokenobjekts	
Erstellen globaler Objekte	Lokaler Dienst,Netzwerkdienst,Administrator
Erstellen symbolischer Verknüpf...	Administratoren
Erstellen von dauerhaft freigege...	
Erzwingen des Herunterfahrens ...	Administratoren
Generieren von Sicherheitsüber...	Lokaler Dienst,Netzwerkdienst
Herunterfahren des Systems	Administratoren,Benutzer,Sicherungs-Opera
Hinzufügen von Arbeitsstatione...	
Identitätstoken für einen andere...	
Laden und Entfernen von Gerät...	Administratoren
Log on as a batch job	Administratoren,Sicherungs-Operatoren,Leis
Log on as a service	Netzwerkdienst,NT SERVICE\ALL SERVICES
Sichern von Dateien und Verzeic...	Administratoren,Sicherungs-Operatoren
Sperren von Seiten im Speicher	
Synchronisieren von Verzeichnis...	
Übernehmen des Besitzes von D...	Administratoren
Verändern der Firmwareumgeb...	Administratoren
Verändern einer Objektbezeichn...	
Verwalten von Überwachungs- ...	Administratoren
Wiederherstellen von Dateien u...	Administratoren,Sicherungs-Operatoren

Figure 152. Server as a Service - Local Policy

3. In the details panel, double-click on entry "Log on as service".



Log on as a service

Netzwerkdienst
NT SERVICE\ALL SERVICES

Figure 153. Server as a Service - Local Policy - Properties

4. Click on the button `Add User or Group` and add the appropriate account to the list

of accounts that should be provided with the "Logon as service" right.

Until the user account from which the server component was started will have all necessary rights, it is possible to run the server instance as a service correctly.

7.15.2. Setup of Server Instance

The server component has to be configured (interfaces, ports, backups) in GUI mode before the service is able to operate as a service.

1. Open the Server Manager window, using the Windows Start menu or desktop shortcut.
2. Configure all the necessary server options (see Section 5.4.1) and select the button **`Save and Exit`** to save the configuration file in the folder `$USER_HOME\NMPv2 Server`.

   This configuration file will be used by the server instance in service mode.

   NOTE Please bear in mind that during the server configuration the same Windows account should be used that will be used for starting the service. The server component always saves/loads its configuration file at/from the folder `$USER_HOME\NMPv2 Server`.

   If different Windows accounts are used for server configuration and for starting the service, the server component will search for its configuration file in a wrong folder. In such case a default configuration will be used.

   NOTE The server component should be configured (interfaces, ports, backups) before installing it as a service.

3. To install the server component as service use the menu item **Server › Service control** in the Server Manager main menu bar.

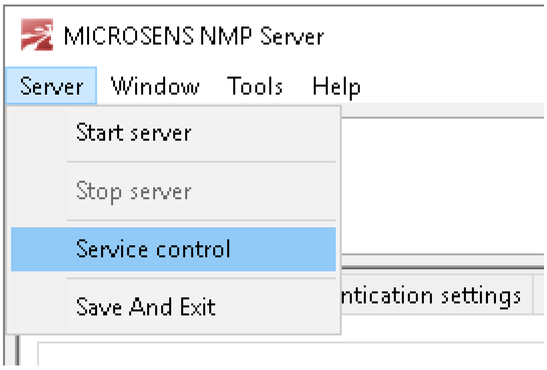
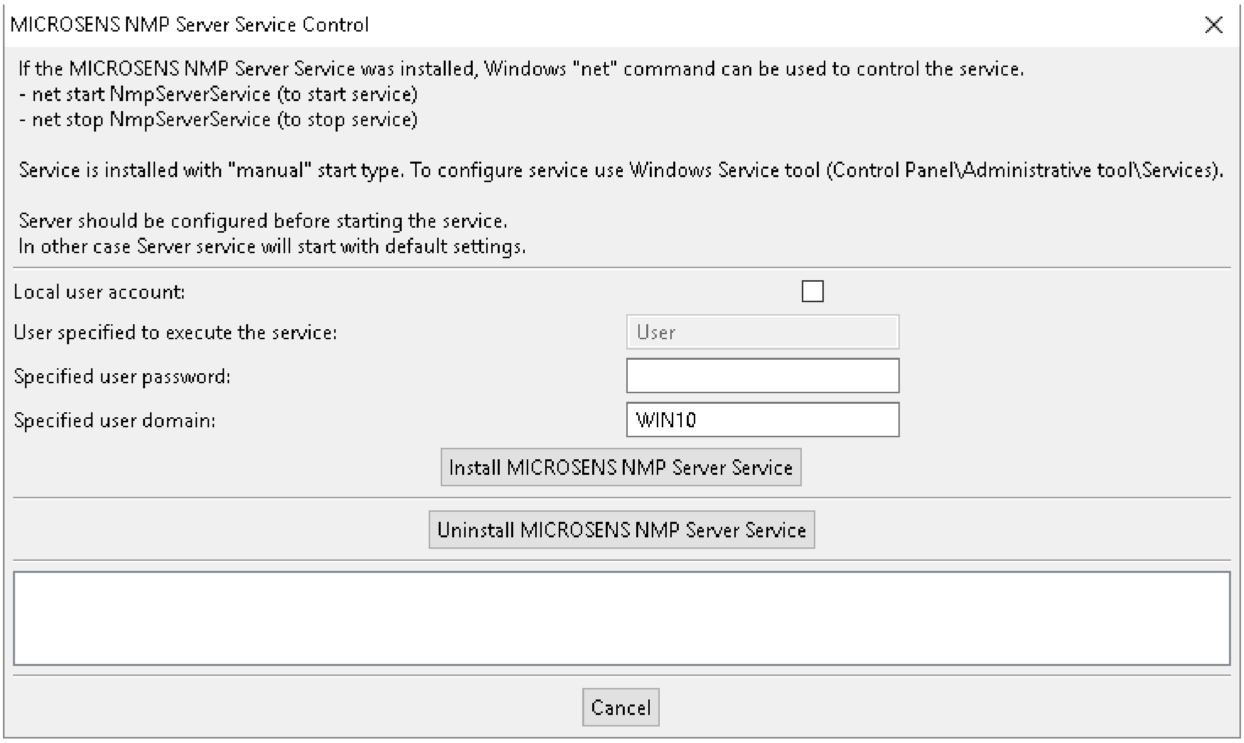


Figure 154. Server as a Service - Service Control

4. To install the service specify the password used for the Windows account and domain name (in cases where a domain account is used).



MICROSENS NMP Server Service Control

If the MICROSENS NMP Server Service was installed, Windows "net" command can be used to control the service.
- net start NmpServerService (to start service)
- net stop NmpServerService (to stop service)

Service is installed with "manual" start type. To configure service use Windows Service tool (Control Panel\Administrative tool\Services).

Server should be configured before starting the service.
In other case Server service will start with default settings.

Local user account: □

User specified to execute the service: User

Specified user password:

Specified user domain: WIN10

Install MICROSENS NMP Server Service
Uninstall MICROSENS NMP Server Service
Cancel

Figure 155. Server as a Service - Service Control - Dialogue

5. After clicking the button `Install MICROSENS Server Service` the tool will install the service.

NOTE	Please observe the logs window to check the installation result. This tool will install the service if the correct user name, password (and domain name if needed) was entered. The service will not be installed, if it was already installed before.

After clicking the button `Uninstall Server Service` the tool will remove the service from the system.

The service is always installed with start type `Auto` and with the name `NmpServerService`. That means that it will be automatically started on system boot. It is not necessary to log in to the system first.

The server service is started as non-GUI background process, so it does not appear on the desktop or taskbar.

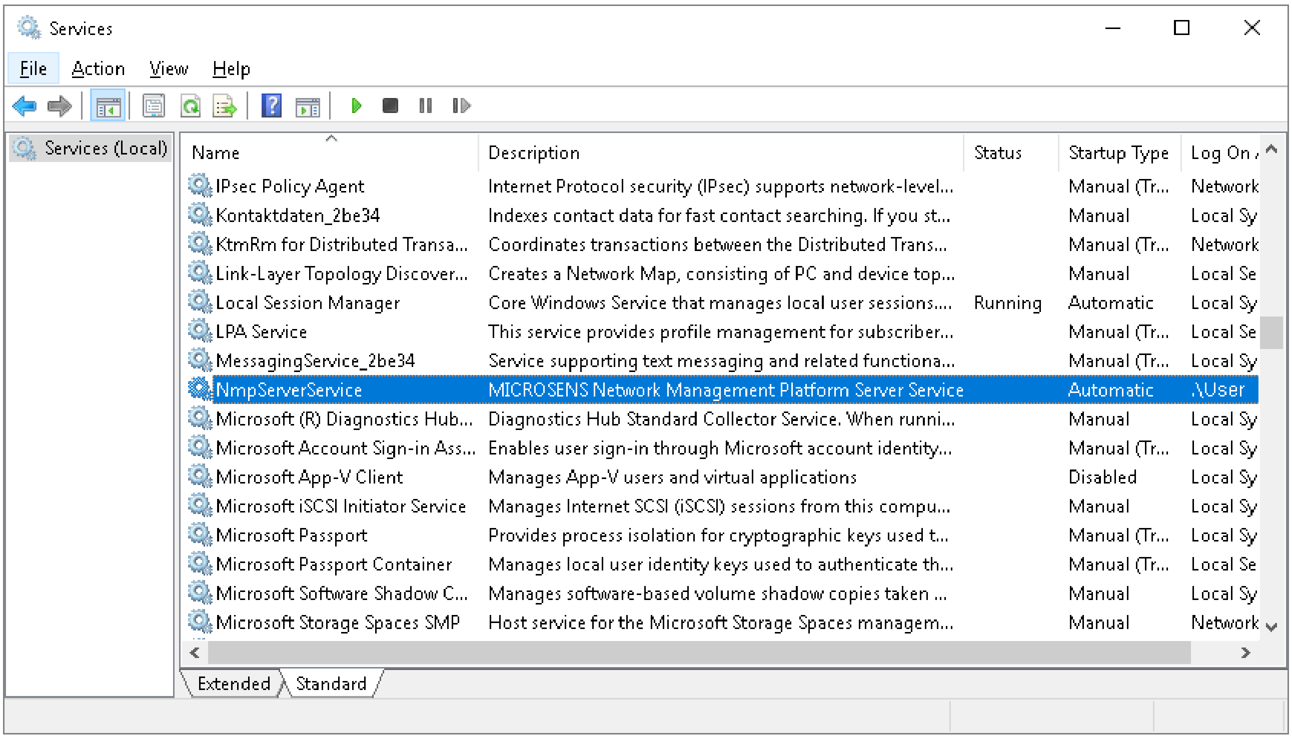
7.15.3. Managing the Server Service

To change the server configuration options it is necessary to stop the service first. Then start the Server Manager in GUI mode, change some options, close the Server Manager and start the service again (manually or reboot the system). It is also necessary to stop the service in order to update NMP Enterprise to the latest version.

Once a service is installed, it can be managed by one of the following methods:

- Launch "Services" via **Windows Control Panel › Administrative Tools**.
- Open the "Service" dialogue by typing `Services.msc` in the `Run` command on Start menu.
- Start or stop it via the Services tab in the Windows Task Manager, where its process can also be found.

The "Services" management console provides a brief description of the service features and displays the path to the specific service's executable, the current status, startup type, dependencies and the account under which the service is running.



Name	Description	Status	Startup Type	Log On A
IPsec Policy Agent	Internet Protocol security (IPsec) supports network-level...		Manual (Tr...	Network
Kontaktdaten_2be34	Indexes contact data for fast contact searching. If you st...		Manual	Local Sy
KtmRm for Distributed Transa...	Coordinates transactions between the Distributed Trans...		Manual (Tr...	Network
Link-Layer Topology Discover...	Creates a Network Map, consisting of PC and device top...		Manual	Local Se
Local Session Manager	Core Windows Service that manages local user sessions....	Running	Automatic	Local Sy
LPA Service	This service provides profile management for subscriber...		Manual (Tr...	Local Se
MessagingService_2be34	Service supporting text messaging and related functiona...		Manual (Tr...	Local Sy
NmpServerService	MICROSENS Network Management Platform Server Service		Automatic	.\User
Microsoft (R) Diagnostics Hub...	Diagnostics Hub Standard Collector Service. When runni...		Manual	Local Sy
Microsoft Account Sign-in Ass...	Enables user sign-in through Microsoft account identity...		Manual (Tr...	Local Sy
Microsoft App-V Client	Manages App-V users and virtual applications		Disabled	Local Sy
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from this compu...		Manual	Local Sy
Microsoft Passport	Provides process isolation for cryptographic keys used t...		Manual (Tr...	Local Sy
Microsoft Passport Container	Manages local user identity keys used to authenticate th...		Manual (Tr...	Local Se
Microsoft Software Shadow C...	Manages software-based volume shadow copies taken ...		Manual	Local Sy
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Spaces managem...		Manual	Network

Figure 156. Server as a Service - Windows Services Dialogue

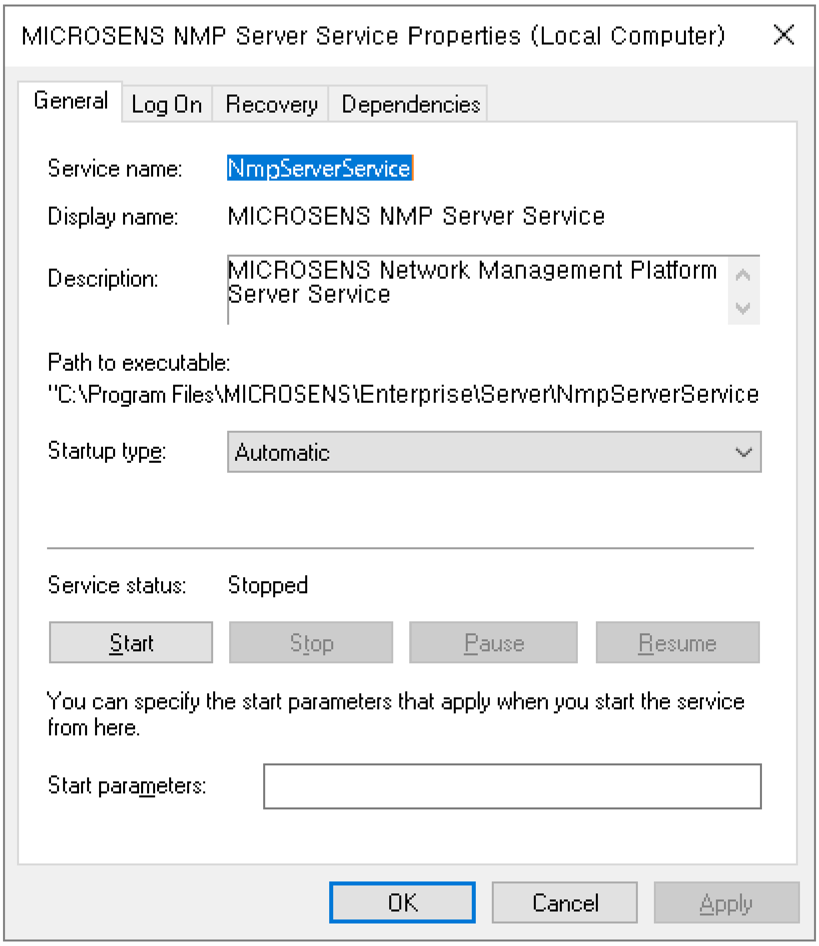
This dialogue allows the following tasks:

- Start, stop, pause or restart services.
- Specify service parameters.
- Change the following start-up types:
  - `Automatic` starts the services at system logon.
  - `Manual` starts a service as required or when called from an application (according to definition. Depending on the service this is feasible only for some services).
  - `Disabled` completely disables the service and prevents it and its dependencies from running.
  - `Automatic (Delayed)` starts the service a short time after the system has finished its booting and initial busy operations, so that the system boots faster.
- Change the account under which the service logs on.

NOTE Please bear in mind, that after changing the account, the server service will search for its configuration file in the folder `$USER_HOME\NMPv2 Server`.

If the configuration file will not be available, the default configuration will be used. * Configure recovery options upon service failure.

Open the "NmpServerService" with a double-click to manage the service.



MICROSENS NMP Server Service Properties (Local Computer)

Service name: NmpServerService

Display name: MICROSENS NMP Server Service

Description: MICROSENS Network Management Platform Server Service

Path to executable:
"C:\Program Files\MICROSENS\Enterprise\Server\NmpServerService

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 157. Server as a Service - General

- On the tab **General** change the service status of the service.
- On the tab **Log on** change the account that is used to log on for this service.

To stop or start the server service, use the Windows "net" command. In order to start or stop the service, open the Windows command line interface by typing `cmd.exe` in the `Run` command on **Start** menu:

- To start the service type `net start NmpServerService`
- To stop the service type `net stop NmpServerService`

With a firewall enabled, the `NmpServerServcie.exe` application, that is available in the

NMP Enterprise installation folder, should be added to the firewall exception list. Otherwise the server service may not be accessible.

7.16. Server Database Replication

NOTE | Server database replication is exclusively available with NMP Enterprise.

Database replication is an important feature of a robust database management system. The server component allows starting a database replication easily by using the Server Manager.

The replication capability of the server database has the following options:

One master, one slave

A replicated database resides in two locations and is managed by two different server instances. One of these server instances has the master role for this database, and the other one has the slave role. Together, the master and its associated slave represent a "replication pair".

Roll-forward shipped log

The replication is based on shipping the server database transaction log from the master to the slave, and then rolling forward the operations described in the log to the slave database.

Asymmetry

Only the master processes transactions. The slave processes no transactions, not even read operations. Only the master server can accept client connections. The slave server redirects all incoming client connections to the master server.

Asynchronicity

All transactions are committed on the master without waiting for the slave. The shipping of the transaction log to the slave is performed regularly and is completely decoupled from the transaction execution at the master server. This may lead to lost transactions on master malfunctions (e.g. system crash).

Shared nothing

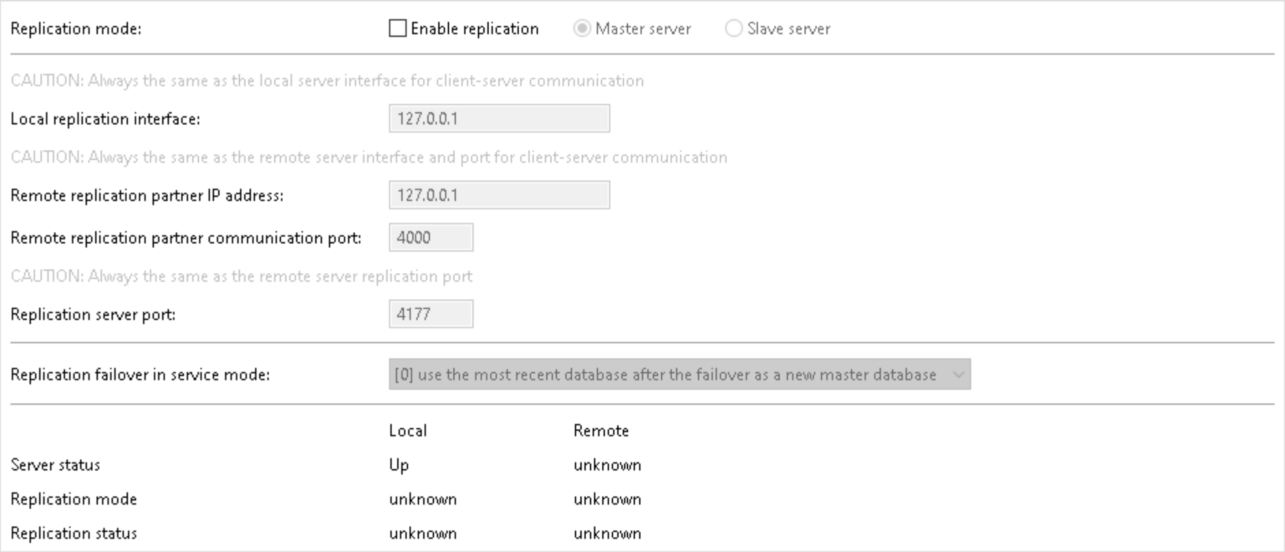
Apart from the network line, no hardware is assumed to be shared.

The replication process builds on the server component’s ability to recover from a crash by starting with a backup and rolling forward the server’s transaction log files. The master sends his log records to the slave using a network connection. The slave subsequently writes these log records to its local log and reproduces them to its own database.

If the master fails, the slave completes the recovery by reproducing the log that has not already been processed. The state of the slave server after this recovery is close to the master’s state shortly before it crashed. However, some of the last transactions performed on the master server may not have been sent to the slave and therefore may not be reflected. When the slave has completed the database recovery work, it is transformed into usual server mode (no replication mode) that enables processing transactions. From this point the (former) slave server can accept client connections and waits for the master server to show up after the repair.

7.16.1. Starting and Running Database Replication

Before a replication starts, configure the two server instances on two servers. After the Server Manager start-up switch to the tab **Database replication**.



Replication mode: □ Enable replication ● Master server ○ Slave server

CAUTION: Always the same as the local server interface for client-server communication

Local replication interface: 127.0.0.1

CAUTION: Always the same as the remote server interface and port for client-server communication

Remote replication partner IP address: 127.0.0.1

Remote replication partner communication port: 4000

CAUTION: Always the same as the remote server replication port

Replication server port: 4177

Replication failover in service mode: [0] use the most recent database after the failover as a new master database

	Local	Remote
Server status	Up	unknown
Replication mode	unknown	unknown
Replication status	unknown	unknown

Figure 158. Server Manager - Tabbed Server Configuration Panel - Database Replication

The replication dialogue elements have the following meaning:

Replication mode
: Enables or disables database replication and defines server role (master or slave) (default = replication disabled).

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**, see Section 5.4.1).

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**, see Section 5.4.1).

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 actual 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:**

  The master server's database will always be used when the replication will be restored after the master or slave failure.

- **Use the slave database after the failover as a new master database:**

  The slave server's database will be always used when the replication will be restored after the master or slave failure.

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 master server, the other one should be configured as slave server.

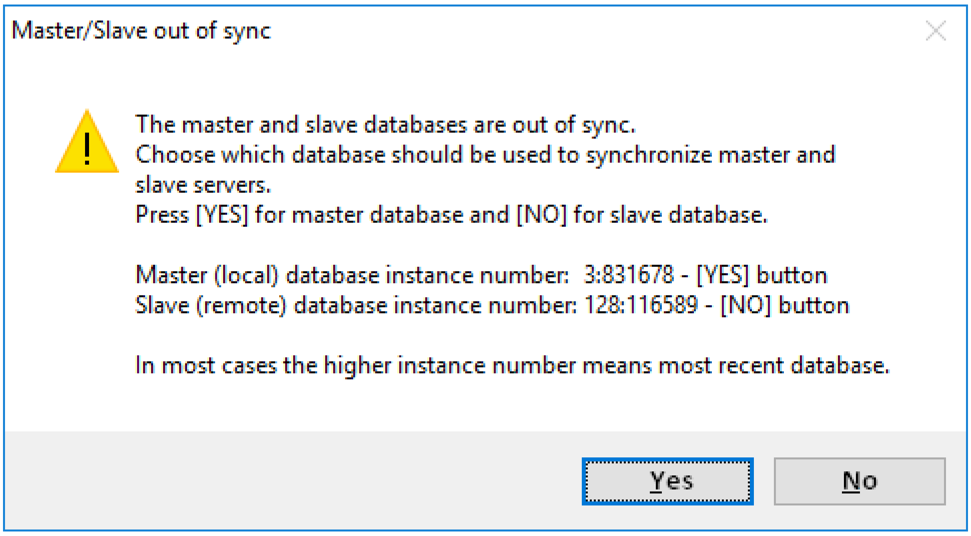
NOTE The replication will not be initialized when both servers will be configured as masters (or slaves). The replication will also not be initialized when the replication mode is disabled on one of the servers.

- The port used by the 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` on the tab **Server settings**. From this point, the servers will automatically initialize the replication.

NOTE

Observe the Server Manager log windows of both servers, where all the operations will be displayed.



Master/Slave out of sync

The master and slave databases are out of sync.
Choose which database should be used to synchronize master and slave servers.
Press [YES] for master database and [NO] for slave database.

Master (local) database instance number: 3:831678 - [YES] button
Slave (remote) database instance number: 128:116589 - [NO] button

In most cases the higher instance number means most recent database.

Figure 159. Server Manager - Database Replication - Out of Sync Message

When the replication is started with an existing database, the master server (which acts like the replication controller) will display the question box and ask which database should be chosen as the master database. Both databases must be synchronised.

The database with the higher number is the most recent one. Decide which database should be used as a new master database for the replication. The above window will not be displayed, when the database does not exist (i.e. first installation of the application's Server Manager). The database that will not be chosen as the master database for the replication will be replaced by the new master database.

In case of starting the replication when server instances are started as Windows services, configure both servers using the Server Manager dialogue. After configuration both Server Managers should be closed by clicking the button `Save and Exit`. When the server services will be started they will automatically initialise the replication. When the replication is started in server service mode, the master server will automatically choose the new master database for database synchronisation. The master server will use the option that is determined by the administrator (see Section 7.16.2). When the database replication is started, it is possible to use a client application (i.e. stand-alone-client or application's web UI) to connect with the master server. The slave server cannot accept client connections. On the attempt to connect to the slave server then the following may happen:

- The web UI will be redirected automatically to the master server.

NOTE

This happens when the web servers of both server instances are enabled.

- The client component will display a warning message, that the slave server cannot accept client connections.

In order to stop the server replication, the master server should be stopped first and subsequently the slave server. It is not possible to stop the slave server first if the master server and the database replication operate correctly.

7.16.2. General Database Replication Procedure

The server database replication has the ability to automatically recover a database after the failure of one of the server instances. In case of failure of one of the replication server partners, the other one will automatically reboot itself in no-replication mode and will continue monitoring the corporate network. In this case a server will always accept client connections (no matter if the server was configured as master or slave). When the replication partner server will show up again (e.g. after a repair), both servers will connect to each other and the replication will be re-initialized automatically.

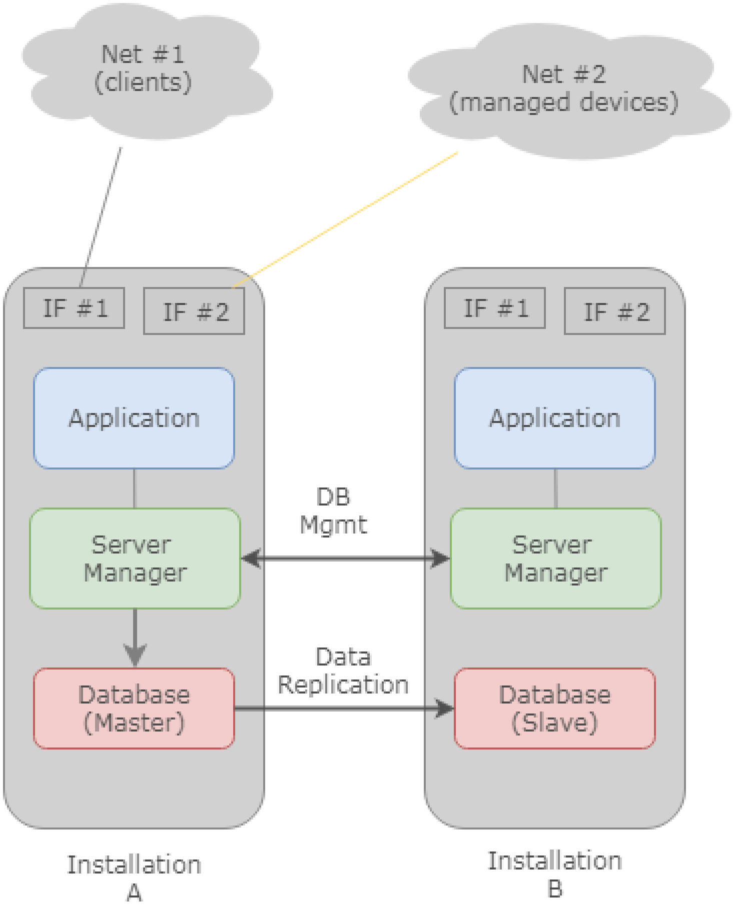


Figure 160. Database Replication - General Operation

During the replication failover procedure, both servers will have to synchronise their databases. When the servers will be started in GUI mode (via Server Manager), the administrator has to choose manually which database should be used as a new master database for the replication. When the servers will be started in Windows service mode, the master server will automatically decide which database will be used as a new master database.

NOTE | The other database will be replaced by the new master database.

7.16.3. Scenario: Failure of Master Server

1. Server instance 'A' acts as replication master for the database, server instance 'B' acts as replication slave. New data is stored in the master server’s database and subsequently replicated into the slave server’s database (Figure 160).
2. Due to a failure server instance 'A' (master) is not available. Server instance 'B' (slave) is turning into single operation mode. It takes over the tasks of instance 'A' and stores monitoring data in its own database. Therefore server instance 'B' maintains its database with the most recent data.

   Meanwhile it waits for server instance 'A' to show up again (Figure 161).

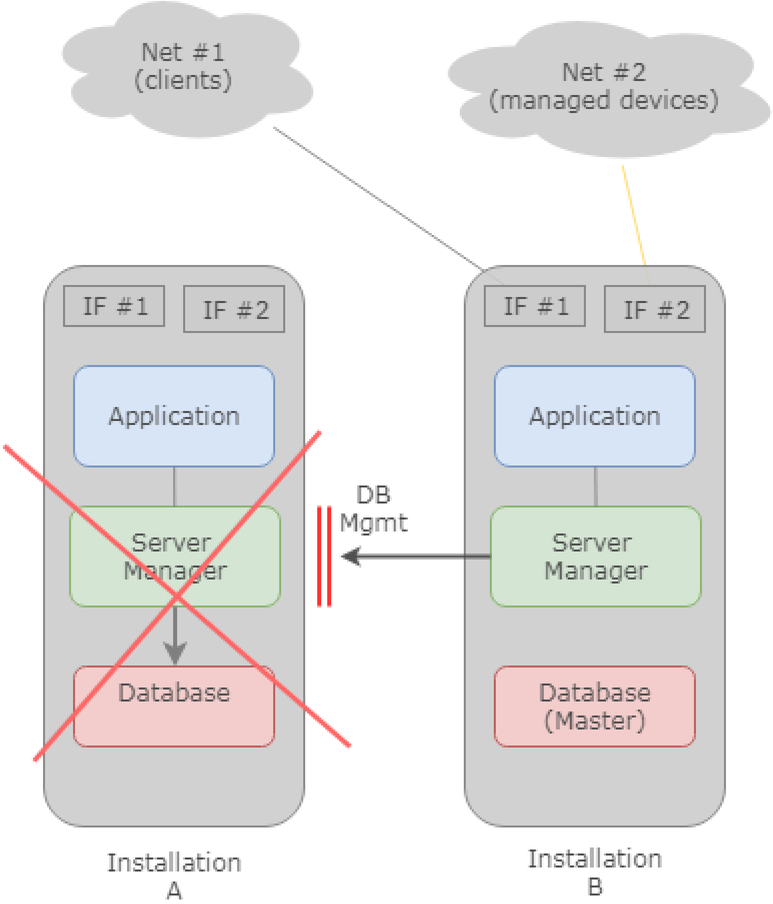


Figure 161. Database Replication - Master Server Failure

3. After the failure is corrected, server instance 'A' restarts. It initialises the replication procedure and waits for connection to its replication partner server instance 'B'.
4. Instance 'B' notices that its replication partner server is available again and reboots in replication mode. Both severs synchronise their databases.
5. The replication process is re-initialised and both master and slave server operate in their previously determined replication modes (Figure 160).

7.16.4. Scenario: Failure of Slave Server

1. Server instance 'A' acts as replication master for the database, server instance 'B' acts as replication slave. New data is stored in the master server’s database and subsequently replicated into the slave server’s database (Figure 160).
2. Due to a failure server instance 'B' (slave) is not available. Server instance 'A' (master) is turning into single operation mode and continues the regular network monitoring operation. Therefore server instance 'A' maintains his database with the most recent data.

   Meanwhile it waits for server instance 'B' to show up again (Figure 162).

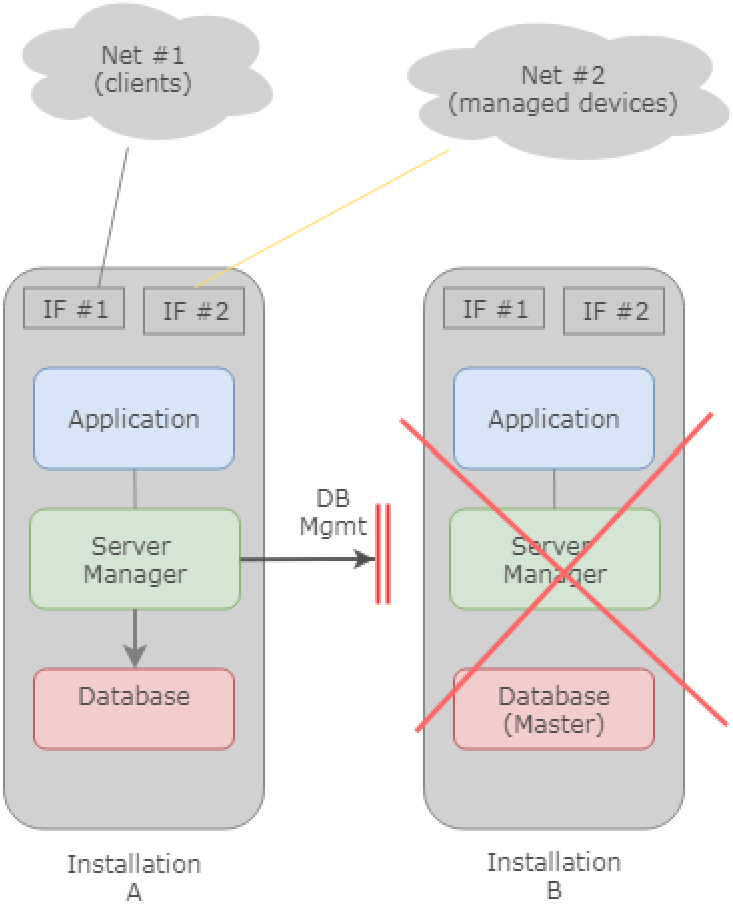


Figure 162. Database Replication - Slave Server Failure

3. After the failure is corrected, server instance 'B' restarts. It initialises the replication procedure and waits for connection to its replication partner server instance 'A'.
4. Instance 'A' notices that its replication partner server is available again and reboots in replication mode. Both severs synchronise their databases.
5. The replication process is re-initialised and both master and slave server operate in their previously determined replication modes (Figure 160).

7.16.5. Scenario: Link Failure between Master and Slave Server

1. Server instance 'A' acts as replication master for the database, server instance 'B' acts as replication slave. New data is stored in the master server's database and subsequently replicated into the slave server's database (Figure 160).
2. Due to a link failure the connection between instances 'A' and 'B' is broken. Both servers reboot in single operation mode. Therefore they both continue monitoring the network and accept client connections.

IMPORTANT	With loss of connection the replication of databases is not possible.

Both servers wait for their respective replication partner to show up again (Figure 163).

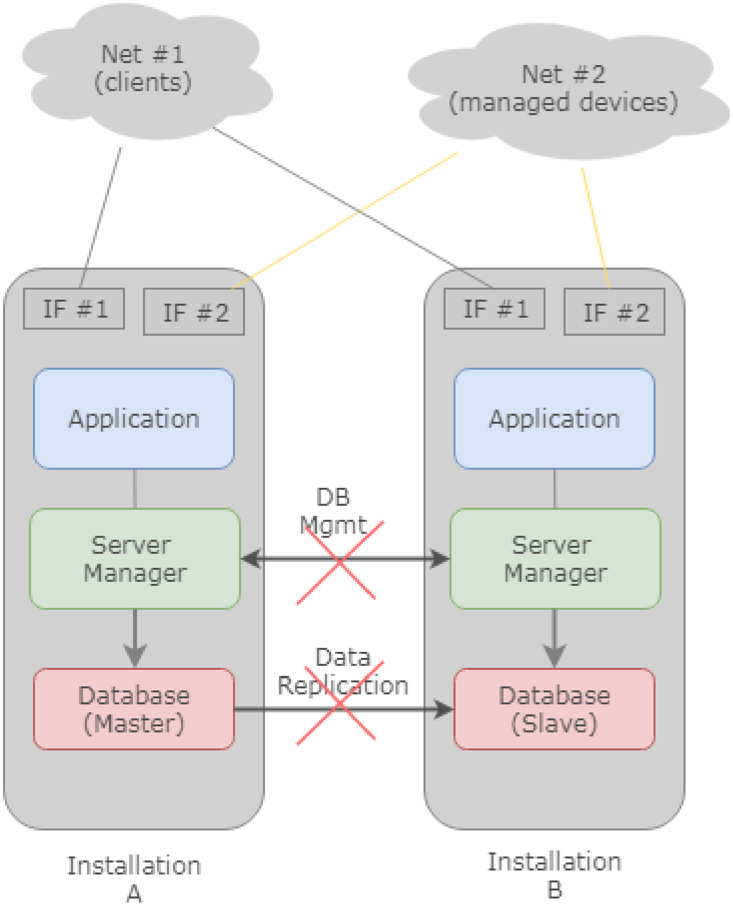


Figure 163. Database Replication - Link Failure

3. After the link failure is corrected both master and slave server notice that the respective replication partner is available again and reboot in replication mode.
4. The replication process is re-initialised and both master and slave server operate in their previously determined replication modes (Figure 160).

7.17. Using SNMP Traps

NOTE Using SNMP traps is exclusivly available with NMP Enterprise.

For general information on configuring the SNMP agent refer to Section 5.4.7.

7.17.1. Management Information Base (MIB)

A Management Information Base (MIB) is a database used for managing the entities in a communications network. The database is hierarchical (tree-structured) and each entity is addressed through an object identifier (OID).

The MIB file for the server component's SNMP agent is always installed together with NMP Enterprise. The server component's MIB file (`NMP_SERVER_MIB.mib`) can be found in the folder `SERVER_INSTALLATION_PATH\mib\`.

The MIB contains several groups which provide information on the managed devices and the server instance status:

- **serverInfo:** Information of the server components version and status
- **deviceList:** Information of all the devices (modules, ports) managed by the server instance (available in the server's devices list)
- **servicesList:** Information on configured services (defined port-to-port connections, links)
- **nmpServerTrap:** Traps sent by the server instance, including the following subgroups:
  - **nmpServerNotifications:** Information about server notifications
  - **eventData:** Information about the occurring event
- **nmpsConformance**

NOTE For reasons of clarity the following OIDs are skipped in the OID table below and replaced by "[…]":

OID	Name	Access
1.3.6.1.4.1.3181	microsens	RO
1.3.6.1.4.1.3181.5909	nmpServer	RO

OID	Name	Access	Description
[…].1	serverInfo		
[…].1.1	serverName	RO	Server name
[…].1.2	serverManufacturer	RO	Server manufacturer
[…].1.3	serverVersion	RO	Server version

OID	Name	Access	Description
[…].1.4	serverLicenseArticleNumber	RO	Server licence key file article number
[…].1.5	serverLicenseHolder	RO	Entitled user
[…].1.6	serverMaintenancePeriod	RO	Server maintenance period
[…].1.7	serverMaxActiveUsers	RO	Maximum number of active users supported
[…].1.8	serverCurrentActiveUsers	RO	Current number of active users
[…].1.9	serverStartTime	RO	Server start time
[…].1.10	serverUptime	RO	Server uptime
[…].1.11	serverReplicationMode	RO	Server replication mode
[…].1.12	serverReplicationStatus	RO	Server replication status
[…].2	**deviceList**		
[…].2.1	deviceListSize	RO	Server device list size
[…].2.2	deviceListTable	NA	Server device list
[…].2.2.1	deviceListTableEntry	NA	Entry in the device list table
[…].2.2.1.1	deviceIp	NA	Device IP address (table index)
[…].2.2.1.2	deviceSubnetMask	RO	Device subnet mask
[…].2.2.1.3	deviceGateway	RO	Device gateway
[…].2.2.1.4	deviceDhcpMode	RO	Device DHCP mode
[…].2.2.1.5	deviceMac	RO	Device MAC address
[…].2.2.1.6	deviceName	RO	Device name
[…].2.2.1.7	deviceLocation	RO	Device location
[…].2.2.1.8	deviceContact	RO	Person who is responsible for the device
[…].2.2.1.9	deviceGroup	RO	Device list group
[…].2.2.1.10	deviceInventoryString	RO	Device inventory string

OID	Name	Access	Description
[…].2.2.1.11	deviceStatus	RO	Device status: - noStatus (1) - downloadingData (2) - unavailable (3) - available (4) - resetting (5) - firmwareUpdate (6) - checking (7) - userDefinedAlarm (8)
[…].2.3	deviceModulesTable	NA	List of device modules
[…].2.3.1	deviceModulesTableEntry	NA	Device modules table
[…].2.3.1.1	moduleDeviceIp	NA	Device IP address (table index)
[…].2.3.1.2	moduleId	NA	Module position in the following syntax: nodeId:unitId:slotId (table index)
[…].2.3.1.3	moduleArticleNumber	RO	Module article number
[…].2.3.1.4	moduleSerialNumber	RO	Module serial number
[…].2.3.1.5	moduleFirmwareVersion	RO	Module firmware version
[…].2.3.1.6	moduleHardwareVersion	RO	Module hardware version
[…].2.3.1.7	moduleTemperature	RO	Module temperature
[…].2.3.1.8	moduleStatus	RO	Module status: - ok (1) - spareMode (2) - inactive (3) - warning (4) - alarm (5) - unknown (255)
[…].2.4	deviceModulePortsTable	NA	List of device module ports
[…].2.4.1	deviceModulePortsTableEntry	NA	Entry in the device module ports table
[…].2.4.1.1	portModuleDeviceIp	NA	Device IP address (table index)
[…].2.4.1.2	portModuleId	NA	Module position in the following syntax: nodeId/unitId/slotId (table index)
[…].2.4.1.3	portId	NA	Module port id (table index)
[…].2.4.1.4	portAlias	RO	Module port alias
[…].2.4.1.5	portStatus	RO	Module port state

OID	Name	Access	Description
[⋯].3	**servicesList**		
[⋯].3.1	servicesListSize	RO	Number of defined services
[⋯].3.2	servicesOk	RO	Number of services in the ok state
[⋯].3.3	servicesWarning	RO	Number of services in the warning state
[⋯].3.4	servicesError	RO	Number of services in the error state
[⋯].3.5	servicesListTable	NA	List of defined services
[⋯].3.5.1	servicesListTableEntry	NA	Entry in the services list table
[⋯].3.5.1.1	serviceId	NA	ID of service (table index)
[⋯].3.5.1.2	serviceName	RO	Name of service
[⋯].3.5.1.3	serviceDescription	RO	Detailed service description
[⋯].3.5.1.4	serviceState	RO	Service status
[⋯].100	**nmpServerTrap**		
[⋯].100.0	nmpServerNotifications		
[⋯].100.0.1	nmpServerSystemInfo		Event type =System Info
[⋯].100.0.2	nmpServerSystemOk		Event type =System OK
[⋯].100.0.3	nmpServerSystemError		Event type =System ERROR
[⋯].100.0.4	nmpServerDeviceSnmpTrap		Event type =SNMP Trap from device
[⋯].100.0.5	nmpServerDeviceResponseOk		Event type =Device Response OK
[⋯].100.0.6	nmpServerDeviceResponseError		Event type =No response from device
[⋯].100.0.7	nmpServerDeviceAccessError		Event type =Device access error (e.g. authentication issue)
[⋯].100.0.8	nmpServerDeviceConfigSend		Event type =New configuration sent to device
[⋯].100.0.9	nmpServerDeviceConfigAccepted		Event type =New configuration accepted by device
[⋯].100.0.10	nmpServerDeviceConfigError		Event type =New configuration not accepted by device
[⋯].100.0.11	nmpServerDeviceConfigBackup-Save		Event type =Device configuration saved at the database

OID	Name	Access	Description
[⋯].100.0.12	nmpServerDeviceConfigBackupDelete		Event type =Device configuration deleted from database
[⋯].100.0.13	nmpServerDeviceFirmwareInfo		Event type =Device firmware update info
[⋯].100.0.14	nmpServerDeviceFirmwareOk		Event type =Device firmware update ok
[⋯].100.0.15	nmpServerDeviceFirmwareError		Event type =Device firmware update error
[⋯].100.0.16	nmpServerDeviceRingError		Event type =RING Error
[⋯].100.0.17	nmpServerDeviceStatusInfo		Event type =Device status info
[⋯].100.0.18	nmpServerDeviceStatusError		Event type =Device status error
[⋯].100.0.19	nmpServerServiceInfo		Event type =Service info
[⋯].100.0.20	nmpServerServiceError		Event type =Service error
[⋯].100.0.21	nmpServerSparePartMode		Event type =Spare Part mode
[⋯].100.0.22	nmpServerDeviceSyslog		Event type:Syslog from device received
[⋯].100.0.100	nmpServerShutdownTrap		Trap indicating that the server instance is shut down
[⋯].100.1	eventData		
[⋯].100.1.1	eventTime	AFN	Event time
[⋯].100.1.2	eventRelevance	AFN	Event relevance
[⋯].100.1.3	eventSeverity	AFN	Event severity
[⋯].100.1.4	eventSource	AFN	Event source like device, user or system
[⋯].100.1.5	eventSourceId	AFN	Event source ID like device IP address or user name
[⋯].100.1.6	eventMessage	AFN	
[⋯].200	**nmpsConformance**		
[⋯].200.1	nmpsGroups		
[⋯].200.1.1	nmpsServerInfoGroup		Information about server version and status
[⋯].200.1.2	nmpsDeviceListGroup		Information about devices at the server list

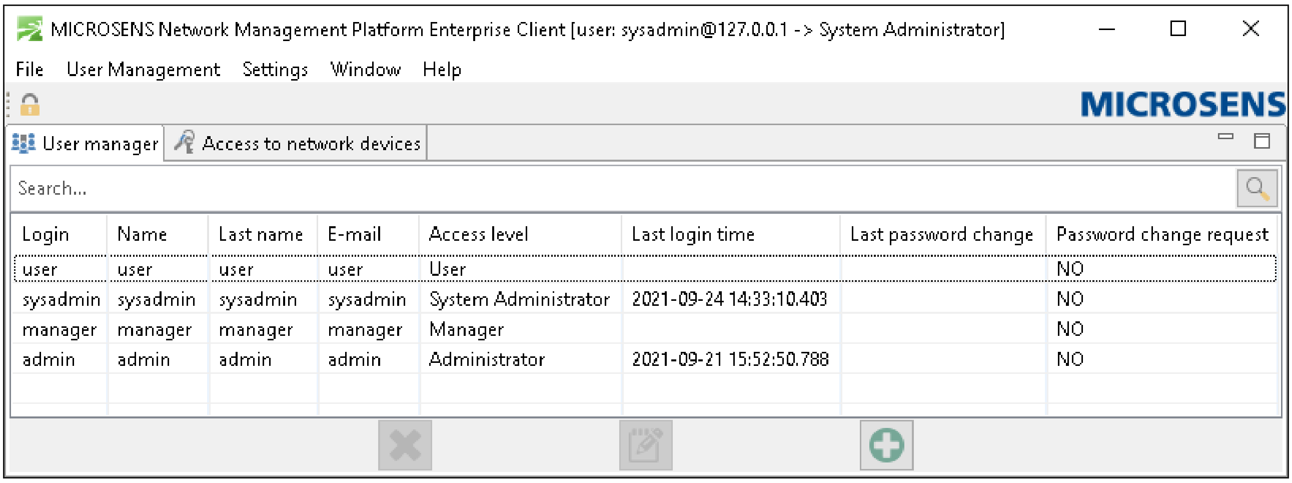
OID	Name	Access	Description
[⋯].200.1.3	nmpsDeviceModulesListGroup		Information about device modules
[⋯].200.1.4	nmpsDeviceModulePortsListGroup		Information about device module ports
[⋯].200.1.5	nmpsServicesListGroup		Information about defined services (end to end connections)
[⋯].200.1.6	nmpsNotificationsGroup		Server notifications
[⋯].200.1.7	nmpsEventDataGroup		Server trap objects
[⋯].200.2	nmpsCompliances		
[⋯].200.2.1	nmpsCompliance		Server compliance information

7.18. User Administration

NOTE While NMP Professional simply offers changing the passwords of both users "admin" and "user" (see Section 4.4.3.2), NMP Enterprise comes with comprehensive user administration options.

With the User Administration tool it is possible to add, delete or edit user accounts on the server. The number of possible user accounts is unlimited. Open the perspective **User Administration** under the main menu **Window › Switch Perspective › User Administration**.

NOTE The perspective **User Administration** is visible with System Administrator access rights.


MICROSENS Network Management Platform Enterprise Client [user: sysadmin@127.0.0.1 -> System Administrator]

Login	Name	Last name	E-mail	Access level	Last login time	Last password change	Password change request
user	user	user	user	User			NO
sysadmin	sysadmin	sysadmin	sysadmin	System Administrator	2021-09-24 14:33:10.403		NO
manager	manager	manager	manager	Manager			NO
admin	admin	admin	admin	Administrator	2021-09-21 15:52:50.788		NO

Figure 164. Stand-alone Client - Perspective "User Administration"

> **NOTE** To return to the perspective **Network Administration** click on **Window › Switch Perspective › Network Administration** in the main menu.

The **User Administration** dialogue contains the following tabs:

- **User Manager:** Use this view to add, modify or delete user accounts.
- **Access to Network Devices:** Use this view to assign access rights for the respective user account.

7.18.1. User Manager

Use this dialogue to add, edit or delete user accounts

Add a New User Account

To add a new user account click on the icon "New user" (⊕) at the bottom pane. The following dialogue opens:

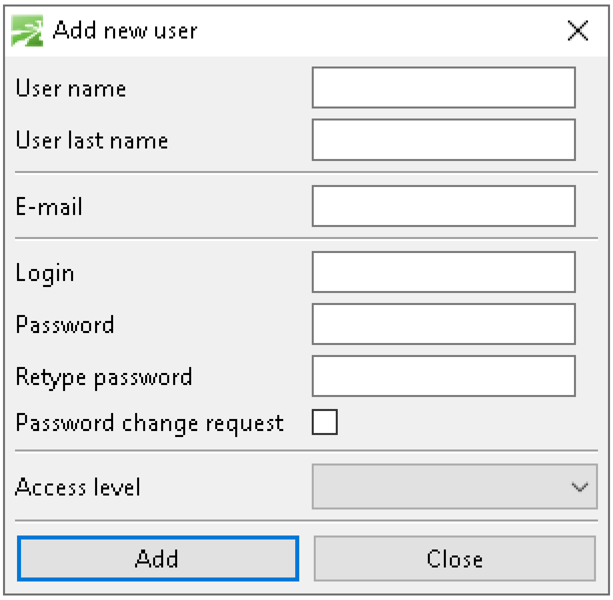


Figure 165. Stand-alone Client - User Administration - Add User

Fill all the fields (name, last name, e-mail, login and password), define the new user's access level and click on the button **Add**.

It is strongly recommended to activate the option "Password change request" so the user have to change the determined password to a private password on first login.

> **NOTE** The login credentials have to be unique. The client will warn if the new login already exists in the database.

Edit and Remove an Existing User Account

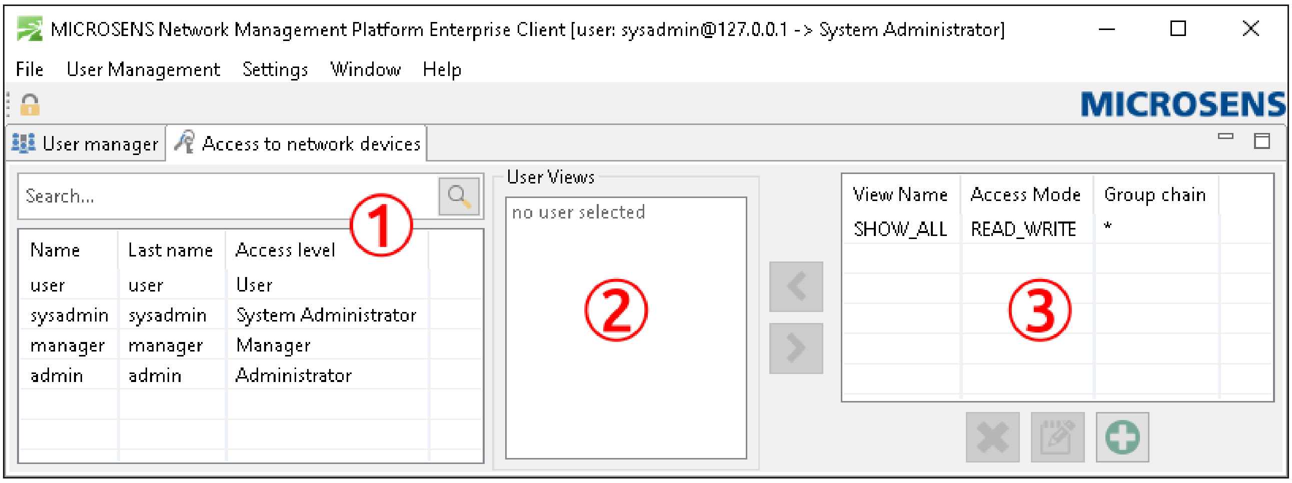
To edit an existing user account select the respective table entry and click on the icon "Edit user (✎).

To remove an existing user account select the respective table entry and click on the icon "Remove user" (✖).

NOTE Keep in mind that at least one user account with access level "System Administrator" has to exist (because only a system administrator can edit user accounts). The client will warn on the attempt to delete or change rights for the last "System Administrator" account.

7.18.2. Access to Network Devices

Change to the view **Access to Network Devices** to define and assign network access rights.


MICROSENS Network Management Platform Enterprise Client [user: sysadmin@127.0.0.1 -> System Administrator]
File
User Management
Settings
Window
Help
MICROSENS
User manager
Access to network devices
Search...
1
User Views
no user selected
2
3

Name	Last name	Access level
user	user	User
sysadmin	sysadmin	System Administrator
manager	manager	Manager
admin	admin	Administrator

View Name	Access Mode	Group chain
SHOW_ALL	READ_WRITE	*

Figure 166. Stand-alone Client - User Administration - Access to Network Devices

This view consists of three main elements:

1. List of existing user accounts (with possibility to search for accounts).
2. Assigned access view for the account selected in the left-hand pane.
3. List of defined access views.

Create, Edit and Remove Access Views

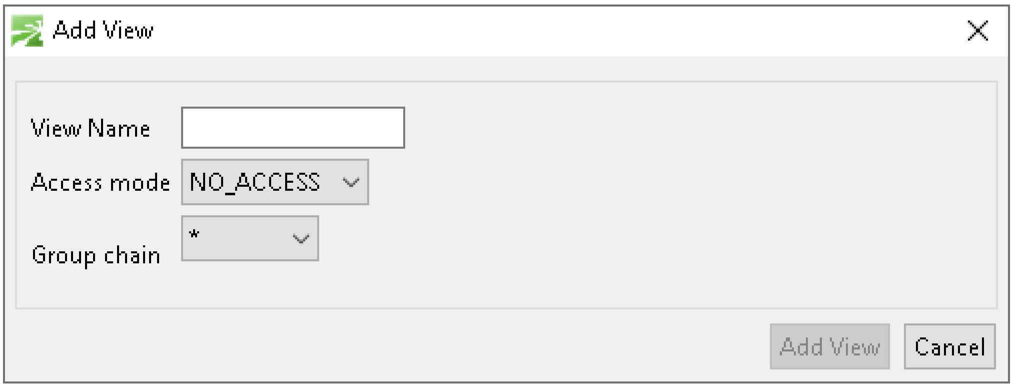
To create a new access view, follow these steps:

1. In the main menu toolbar click on the "lock" symbol to unlock the application’s configuration.
   - 🔒 - Configuration is locked.
   -

🔓 - Configuration is unlocked.

Confirm the upcoming notice dialogue.

2. Click on the button "Define New View" (⊕) at the bottom of the right-hand pane.
3. In the opening dialogue enter the specific access view data.



View Name

Access mode NO_ACCESS

Group chain *

Figure 167. Stand-alone Client - User Administration - Access to Network Devices - Add Access View

- **View Name:** Enter a name for a new device list view or click on a previously defined view in the view list table. This entry has to be unique.
- **Access mode:** Select one of the following access modes:
  - **NO_ACCESS:** This mode blocks the access to the respective group chain.
  - **READ_WRITE:** This mode allows access to the respective group chain.
- **Group chain:** The drop-down list combo mirrors the node structure of the device list tree. After selecting the first node subsequently the next drop-down lists appear for further selection.

  The access mode is applied for the last node of the group chain. The group chain can end with one of the following entries:

  - **"" (empty):** If the group chain ends with "", it means that the devices at this group should be hidden. All its subgroups are visible to the user.
  - **"*" (asterisk):** If the group chain ends with "*", it means that the same access mode is applied also to subgroups of this node (inheritance).

    It is also possible to hide some group and its subgroups ("*") and to show one of the subgroups with another view. In such a case, the group in the device list tree is visible to the user marked with a grey icon and the name of group replaced with "[NO ACCESS]".

NOTE

The view "SHOW_ALL" with "READ_WRITE" access to the complete device list is predefined, non-erasable and by default associated with all users. Additionally the system administrator's list view association cannot be deleted. Therefore it is not possible for the system administrator to accidentally block his comprehensive device list view.

NOTE

For more information about dealing with group chains please refer to Section 7.18.3.

4. Click the button `Add view` to apply the new access view. The new entry appears in the list of defined access views in the right-hand pane.
5. To **edit an existing access view**, select an entry and click on the button `Edit selected view` (✎) at the bottom of the right-hand pane.

   To **delete an existing access view**, select an entry and click on the button `Remove selected view` (✖) at the bottom of the right-hand pane.

6. In the main menu toolbar click on the "lock" symbol to lock the NMP configuration.

   The client component synchronises its configuration with the server.

Assign/Remove Access View to/from User Account

To assign an existing access view to an user account, follow these steps:

1. In the main menu toolbar click on the "lock" symbol to unlock the application's configuration.

   - 🔒 - Configuration is locked.
   - 🔓 - Configuration is unlocked.

   Confirm the upcoming notice dialogue.

2. In the left-hand pane select an existing user account from the list.
3. In the right-hand pane select an existing access view.
4. To assign the selected access view click on the horizontal arrow pointing left (‹).

   The access view appears in the list of assigned views for the selected NMP user account in the middle pane.

5. To remove the access view from a selected NMP user account, select the assigned view and click on the horizontal arrow pointing right (›).

   The entry disappears from the access view list.

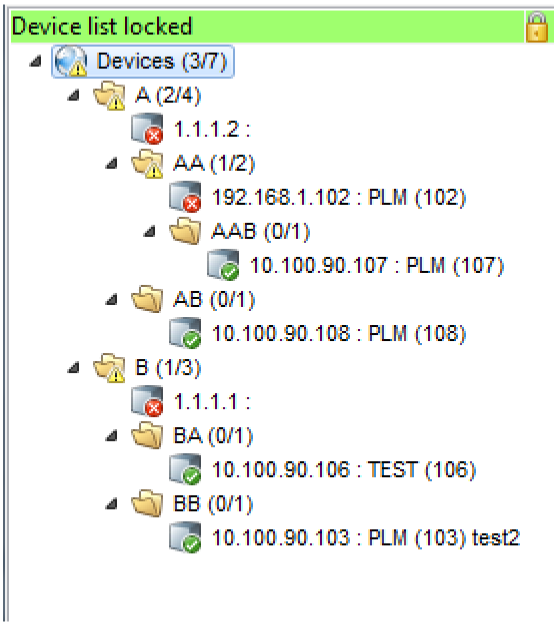
6. In the main menu toolbar click on the "lock" symbol to lock the NMP configuration.

The client component synchronises its configuration with the server.

7.18.3. Device List ACL for View Based User Model

It is possible to limit the scale of the device list due to user access rights. Therefore the system administrator can see all the devices managed by the application while the user with restricted access rights can see some respective devices to which e.g. he has management access.

Assuming the device list is as follows:



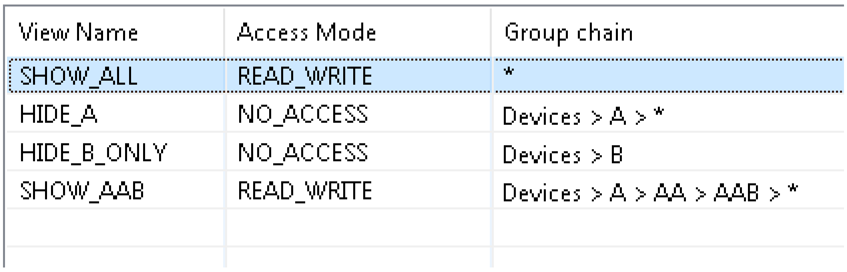
Device list locked

- Devices (3/7)
  - A (2/4)
    - 1.1.1.2 :
    - AA (1/2)
      - 192.168.1.102 : PLM (102)
      - AAB (0/1)
        - 10.100.90.107 : PLM (107)
    - AB (0/1)
      - 10.100.90.108 : PLM (108)
  - B (1/3)
    - 1.1.1.1 :
    - BA (0/1)
      - 10.100.90.106 : TEST (106)
    - BB (0/1)
      - 10.100.90.103 : PLM (103) test2

Figure 168. Stand-alone Client - User Administration - Device List ACL - Example: Basic Tree View

There are two top level nodes "A" and "B" with several child nodes. With the predefined list view "SHOW_ALL" all nodes and devices are visible to all users by default.

To restrict the view to nodes and devices the following list views are created:



View Name	Access Mode	Group chain
SHOW_ALL	READ_WRITE	*
HIDE_A	NO_ACCESS	Devices > A > *
HIDE_B_ONLY	NO_ACCESS	Devices > B
SHOW_AAB	READ_WRITE	Devices > A > AA > AAB > *

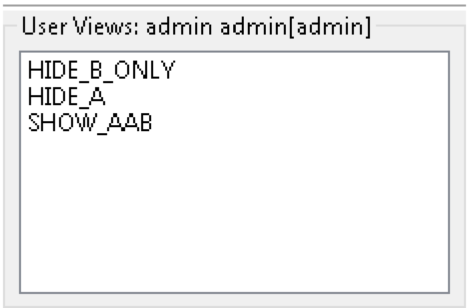
Figure 169. Stand-alone Client - User Administration - Device List ACL - Example: List View

The additionally defined list views have the following restriction or allowance function:

- **HIDE_A:** Node "A", all its children ("AA", "AB") and the respective devices are not visible (set via "*" for child nodes).

- **HIDE_B_ONLY:** Node "B" is not visible and its child nodes ("BA", "BB") and their respective devices are visible.
- **SHOW_AAB:** Node "AAB" (child of "AA") and the respective devices should be visible even if they are in hidden node "A" (see list view "HIDE_A" from above).

These list views are associated to the administrator while the "SHOW_ALL" list view is dissociated:

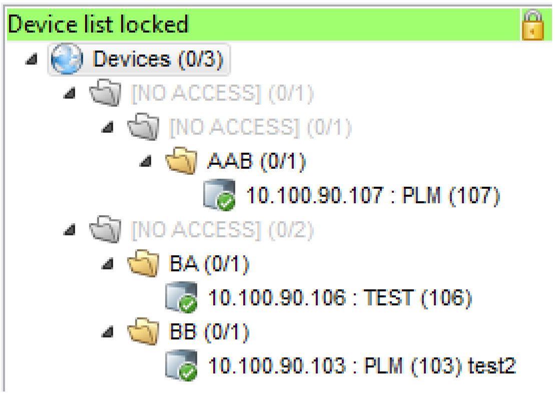


User Views: admin admin[admin]

HIDE_B_ONLY
HIDE_A
SHOW_AAB

Figure 170. Stand-alone Client - User Administration - Device List ACL - Example: User View (Administrator)

After closing this dialogue the administrator gets the following device list tree view with restricted node access:



Device list locked

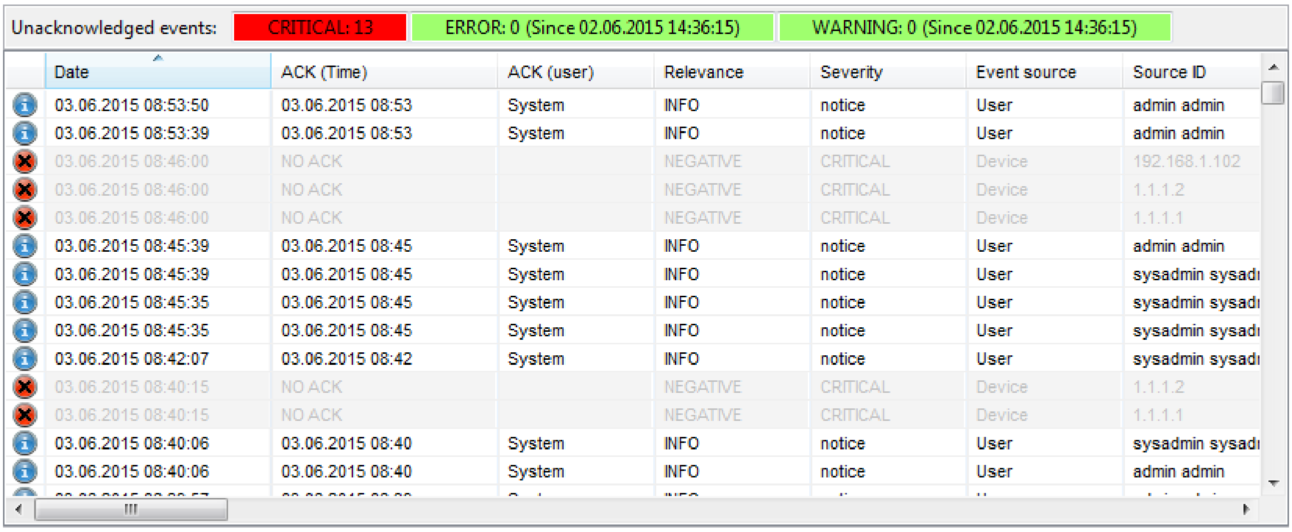
- Devices (0/3)
  - [NO ACCESS] (0/1)
    - [NO ACCESS] (0/1)
      - AAB (0/1)
        - 10.100.90.107 : PLM (107)
  - [NO ACCESS] (0/2)
    - BA (0/1)
      - 10.100.90.106 : TEST (106)
    - BB (0/1)
      - 10.100.90.103 : PLM (103) test2

Figure 171. Stand-alone Client - User Administration - Device List ACL - Example: Restricted Tree View

With restricted access to the device tree list it is not possible to delete restricted nodes or even visible nodes with restricted children. The application will open a respective warning message.

If the administrator would e.g. move or copy the accessible device "PLM (107)" from node "AAB" to the restricted node "AA", the device would be placed inside this node and would be hidden.

With restricted access to device tree nodes and devices the **Notification** tab would look like this:



Unacknowledged events: CRITICAL: 13 | ERROR: 0 (Since 02.06.2015 14:36:15) | WARNING: 0 (Since 02.06.2015 14:36:15)

	Date	ACK (Time)	ACK (user)	Relevance	Severity	Event source	Source ID
ⓘ	03.06.2015 08:53:50	03.06.2015 08:53	System	INFO	notice	User	admin admin
ⓘ	03.06.2015 08:53:39	03.06.2015 08:53	System	INFO	notice	User	admin admin
✖	03.06.2015 08:46:00	NO ACK		NEGATIVE	CRITICAL	Device	192.168.1.102
✖	03.06.2015 08:46:00	NO ACK		NEGATIVE	CRITICAL	Device	1.1.1.2
✖	03.06.2015 08:46:00	NO ACK		NEGATIVE	CRITICAL	Device	1.1.1.1
ⓘ	03.06.2015 08:45:39	03.06.2015 08:45	System	INFO	notice	User	admin admin
ⓘ	03.06.2015 08:45:39	03.06.2015 08:45	System	INFO	notice	User	sysadmin sysadı
ⓘ	03.06.2015 08:45:35	03.06.2015 08:45	System	INFO	notice	User	sysadmin sysadı
ⓘ	03.06.2015 08:45:35	03.06.2015 08:45	System	INFO	notice	User	sysadmin sysadı
ⓘ	03.06.2015 08:42:07	03.06.2015 08:42	System	INFO	notice	User	sysadmin sysadı
✖	03.06.2015 08:40:15	NO ACK		NEGATIVE	CRITICAL	Device	1.1.1.2
✖	03.06.2015 08:40:15	NO ACK		NEGATIVE	CRITICAL	Device	1.1.1.1
ⓘ	03.06.2015 08:40:06	03.06.2015 08:40	System	INFO	notice	User	sysadmin sysadı
ⓘ	03.06.2015 08:40:06	03.06.2015 08:40	System	INFO	notice	User	admin admin

Figure 172. Stand-alone Client - User Administration - Device List ACL - Example: Restricted Notifications

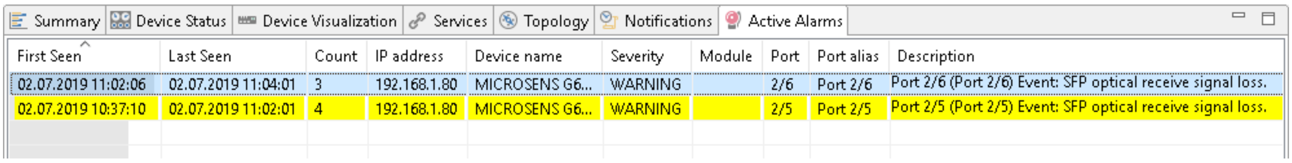
The events generated by hidden devices are visible. They are greyed out and cannot be acknowledged.

The user with restricted access can see, whether there are failures on hidden devices, so he optionally can inform the system administrator about malfunctioning devices.

7.19. Using Active Alarms

NOTE | Active alarms is exclusively available with NMP Enterprise.

To use active alarms change to the tab **Active Alarms** in the stand-alone client.



First Seen	Last Seen	Count	IP address	Device name	Severity	Module	Port	Port alias	Description
02.07.2019 11:02:06	02.07.2019 11:04:01	3	192.168.1.80	MICROSENS G6...	WARNING		2/6	Port 2/6	Port 2/6 (Port 2/6) Event: SFP optical receive signal loss.
02.07.2019 10:37:10	02.07.2019 11:02:01	4	192.168.1.80	MICROSENS G6...	WARNING		2/5	Port 2/5	Port 2/5 (Port 2/5) Event: SFP optical receive signal loss.

Figure 173. Stand-alone - Tabbed Data Panel - Active Alarms

It is helpful to view some important SNMP traps of managed devices at first glance.

NOTE | The tab **Active Alarms** shows notifications of MICROSENS G6 (and newer) devices as well as of MSP1000 and MSP3000 devices.

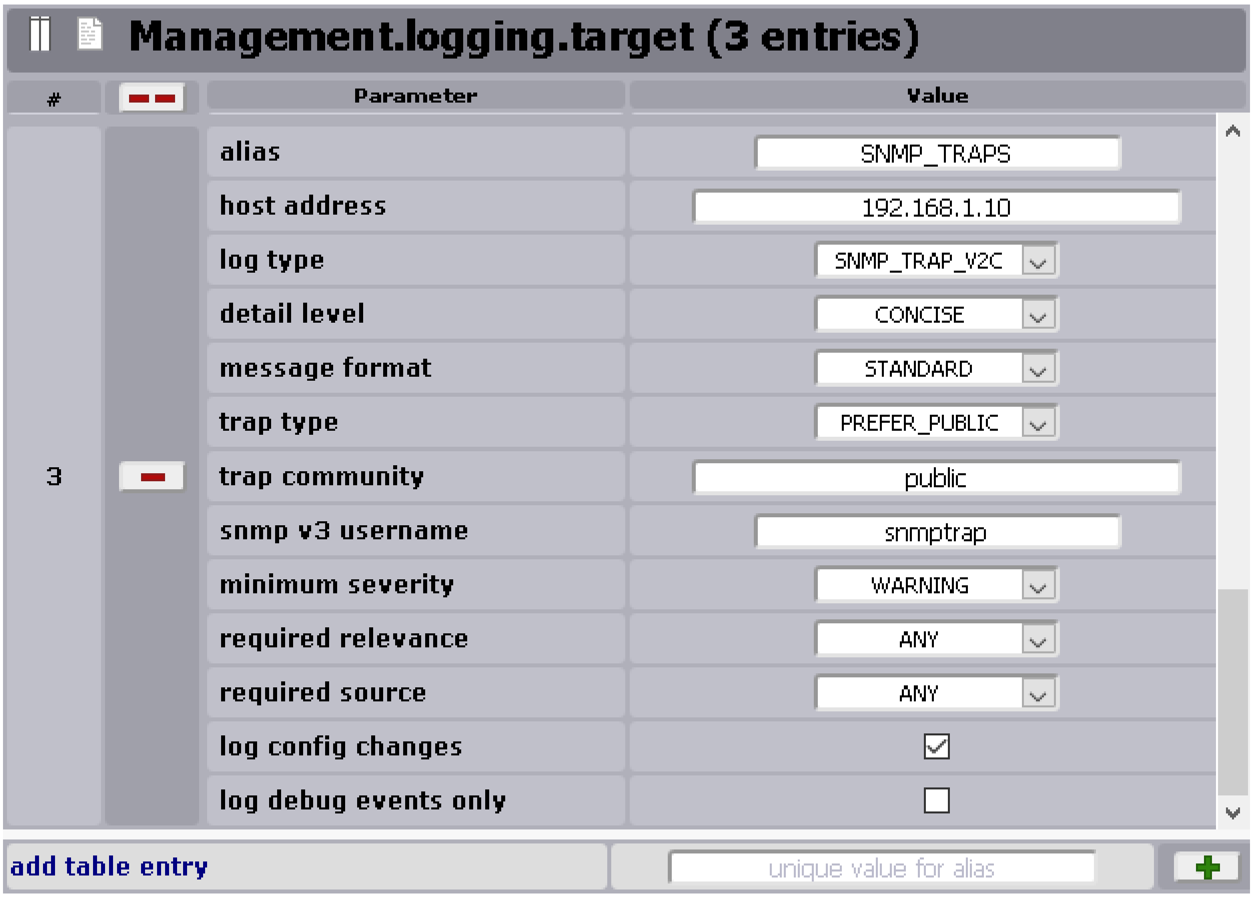
7.19.1. Prerequisites

To use Active Alarms with the stand-alone client the following conditions are a must have:

- The managed device is a MICROSENS MSP1000 with NM3 module or a G6 (and newer) switch with firmware version 10.7.4 and above. If the managed devices do not include one of these device types, the stand-alone client hides the tab **Active**

Alarms.

- The managed device is configured to send SNMP traps to the connected server instance component. E.g. with a G6 switch the configuration is done via view **Logging** on tab **Targets** in the section **Management.Logging.Target** (with Web Manager, CLI command accordingly).



Management.logging.target (3 entries)

#	▬▬	Parameter	Value
3	▬	alias	SNMP_TRAPS
		host address	192.168.1.10
		log type	SNMP_TRAP_V2C
		detail level	CONCISE
		message format	STANDARD
		trap type	PREFER_PUBLIC
		trap community	public
		snmp v3 username	snmptrap
		minimum severity	WARNING
		required relevance	ANY
		required source	ANY
		log config changes	☑
		log debug events only	☐

Figure 174. Device - Web Manager - SNMP Target for Active Alarms

NOTE Be sure to enter the IP address of the Server Manager as SNMP target's host address (see Section 5.4.1).

- The SNMP trap listener has to be enabled on the Server Manager (see Section 5.4.1).

7.19.2. Mode of Operation

When all prerequisites are met, Active Alarms operate as follows:

1. Every MSP1000 or G6 (and newer) device contains pre-defined SNMP events with i.e. name, event, group, relevance, severity, trap options etc.
2. If an SNMP event is enabled as a trap and the minimum severity of the event is sufficient for a notification, the SNMP agent of the device sends this event to the determined SNMP trap listener.
3. The SNMP trap listener of the Server Manager receives this trap and saves it in its

database.

4. At a regular interval the stand-alone client polls the database to collect new information about SNMP events of managed devices.
5. If a new occurring SNMP trap is part of one of the following event groups, it is listed on the tab **Active Alarms**:
    - FIRMWARE (5)
    - POWER (10)
    - TEMPERATURE (11)
    - LINK (12)
    - SFP (13)
    - SIGNALS (17)
    - CABLE (22)
    - MSP 1000 (24)
    - FAN (26)

    The tab "Active Alarms" shows the following entries:

    - "First Seen": Time and date of the first occurrence of this SNMP trap.
    - "Last Seen": Time and date of the last occurrence of this SNMP trap.
    - "Count": Number of SNMP traps received since first occurrence.
    - "IP Address": IP address of the device which has sent the SNMP trap.
    - "Device Name": Name of the specific device (`sys info` in SNMP device info).
    - "Severity": Severity of the SNMP trap.
    - "Module": NM3 module of a managed MSP1000 device.
    - "Port/Port Alias": Port and port alias of the SNMP trap if the SNMP trap source is a port, otherwise empty.
    - "Description": Information about what causes the SNMP trap.

    The list entries appear or disappear as follows:

    - An event with negative relevance adds a new entry in the list.
    - If this event did not happen before, a new entry with identical "First/Last Seen" data and "Count" equals 1 appears in the list.
    - If this event already exists in the list, the "Last Seen" entry is updated and the "Count" is increased by 1.
    - If this event has happened before but due to an alarm reset or an identical SNMP trap with positive relevance was deleted from the list earlier, it reappears in the list with the "Last Seen" entry updated and the "Count" increased by 1.
    - An event with positive relevance deletes a corresponding entry in the list. So the tab **Active Alarm** operates as dynamic alarm list, only showing actual SNMP traps.

Click on the header of a column to sort the table for the respective value in ascending or descending order.

A right-click of one of the list entries opens the context menu:

- **Show device:** Opens the tab **Device Status** of the respective device which has sent the SNMP trap.
- **Remove active alarm:** Deletes the respective entry from the active alarm list and resets all data. An identical event with negative relevance will force a new list entry with identical "First/Last Seen" data and "Count" equals 1.

8. Glossary

The glossary provides detailed information and definitions of terms used in this documentation.

Micro Switch

The MICROSENS Micro Switch concept is based on the dimensions of 45 x 45 mm (system 45x45). This is a widespread design throughout the world that facilitates the use in national and international installation systems.

The advantage of the system 45x45 is its cost efficiency compared to the classic systems, with a 50% reduction in the time and cost expenditure required for installation. Components are no longer screwed but are simply snapped into place in the device carrier or installation sockets provided. This enables the requisite installation time to be considerably reduced.

The installation components of MICROSENS are offered as horizontal and vertical versions. The equipment is delivered in a suitable form so that no conversion or time consuming assembly is necessary on site. This means that installation time is reduced and the robustness of components is greatly increased.

Desktop Switch

The MICROSENS desktop switches offer a cost effective way to realise modern fibre base networks in the LAN area (FTTO).

There are versions with Fast Ethernet or Gigabit Ethernet with different port numbers available. For high demanding applications the switches are available with management and the PoE option allows the simple implementation of VoIP applications.

The fan-less design of the devices guarantees a noiseless and reliable operation.

Industrial Switch

The MICROSENS Industrial Switches have been designed for specific applications that are prone to failure. An open firmware concept means that these devices can be adapted flexibly in order to suit individual customer and market requirements. Extremely challenging applications such as those related to use in the utility and railway sector as well as in potentially explosive underground environments are underpinned by special certifications.

NM3

According to the modular concept of the MSP 1000 platform, MICROSENS offers two variants in the context of the network management modules: The NM3 module with a 4-port Gigabit Ethernet switch allocates one slot in the chassis. The NM3+ accommodates six Gigabit Ethernet ports in total, one USB extension port, and two potential-free digital inputs and outputs. Due to the additional interfaces, it allocates two module slots. Both modules can be connected to a console over a serial RS-232 connection.

In addition to the protection against manipulation, MICROSENS modules also offer a high degree of failsafe performance. Both the NM3 and NM3+ modules offer two

SFP slots. As a particularly advantageous feature, they permit the combination of the management systems of several MSP 1000 platforms. They can be interconnected in cascaded mode and also in a fail-safe ring topology. If a node breaks down, the network management re-routes the traffic and ensures that all other nodes remain reachable in an almost uninterrupted mode. On the hardware end, an integrated protection mechanism additionally detects and prevents undesired network loops (loop protection).

Industrial ProfiLine

MICROSENS offers a 25-port Gigabit Ethernet switch in 19" design. The ProfiLine rack switch was developed for use in harsh industrial environments and offers a total of 25 Gigabit Ethernet ports of which eight can be expanded to fibre optic connections as combo ports with SFP modules. A total of 16 copper ports offer PoE/PoE+ functionality with which the terminal devices connected can be supplied with electricity economically and without additional cabling work.

Industrial ring structures can be established either via SFP ports or via copper connections. In the event of failure, a special mechanism detects a fault on a network node or interruption of the line and ensures automatic reconfiguration of the network within milliseconds.

The switch operating system, firmware and configuration data are saved on a SD card. If a switch needs to be replaced, the existing SD card is simply inserted in the new device which automatically accepts all the settings.

MultiPort media converter

With the media converter it is possible to realise the media conversion of up to 12 ports in 1 height unit (1 HU). This port density can be reached also with the standard optical connectors such as ST- and SC-duplex.

Beside this high port density the actual 12 port converter has several additional features such as SNMP/web-based management, optional redundant power supply and auto-crossing integrated. The MICROSENS converters are designed for the installation into 19" racks. With this compact design it is possible to reach very high port densities in the central distribution racks.

The connection to the central switch is done, depending on the version, by Telco or RJ-45 cable. The Telco cables are having an RJ-21 connector with a capacity of 12 twisted-pair connections and offer flexibility and simple installation.

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: PM-EN-19002_User-Manual-NMPv2(10)_v2.10.7