

MICROSENS

User Manual | Network Management Platform

NMP v2.6



**MICROSENS
GmbH & Co. KG**

Kueferstr. 16
59067 Hamm/Germany

Tel.	+49 2381 9452-0
FAX	+49 2381 9452-100
E-Mail	info@microsens.com
Web	www.microsens.com

Contents

1	INTRODUCTION	6
1.1	Network Management.....	6
1.1.1	Network Administration	6
1.1.2	Network Monitoring.....	6
1.1.3	Network Configuration	6
1.1.4	Network Visualisation with Topology Manager	6
1.2	Differences between NMP Product Variants	6
1.2.1	NMP Professional	6
1.2.2	NMP Enterprise	7
1.3	Scope of this User Manual.....	7
2	INSTALLATION.....	8
2.1	System Requirements.....	8
2.2	Additional Requirements for Server Access	8
2.2.1	Client Component.....	8
2.3	Port and Firewall Settings.....	9
2.4	Software Installation of NMP	11
2.4.1	Difference between Installation Files for Windows® and Linux	12
2.4.2	Starting the Installer Application on Windows®	12
2.4.3	General Pre-Installation Settings	12
2.4.4	Product Selection	13
2.4.5	Choose Components	14
2.4.6	Choose Users.....	15
2.4.7	Choose Install Location.....	16
2.4.8	Installation Path.....	16
2.4.9	Installing on Linux Operating Systems	17
2.4.10	Configuration Folder Presetting (NMP Enterprise)	17
3	LICENSING.....	18
3.1	Trial Period Licences	18
3.2	Product Variants	18
3.3	Selecting the Licence Key File.....	19
4	NMP PROFESSIONAL: GETTING STARTED	20
4.1	Starting NMP Professional	20
4.1.1	Starting on Windows®	20
4.1.2	Starting on Linux Operating Systems	20
4.1.3	First Program Start	21
4.2	Login.....	21
4.3	NMP Professional Main Window	23
4.4	Main Menu	24
4.4.1	File.....	24
4.4.2	Devices List	25
4.4.3	Settings.....	35
4.4.4	Discovery	43
4.4.5	Tools	47
4.4.6	Edit	56
4.4.7	Window	57

4.4.8	Help	58
4.5	Main Menu Toolbar	60
4.6	Device List Tree View.....	61
4.7	Tabbed Data Panel	63
4.7.1	Summary	64
4.7.2	Device Status	67
4.7.3	Device Visualization	68
4.7.4	Services.....	69
4.7.5	Topology.....	70
4.7.6	Notifications	71
4.8	Context Menu.....	71
4.8.1	Device Context Menu	72
4.8.2	Group Context Menu	77
5	WORKING WITH NMP PROFESSIONAL.....	82
5.1	Adding New Devices with Device Auto Discovery.....	82
5.2	Device Configuration in General.....	84
5.3	Device Configuration via Configuration Files.....	85
5.4	Using a Master Configuration.....	87
5.4.1	Master Configuration of MICROSENS G6 Devices.....	87
5.4.2	Master Configuration of MICROSENS G5 and older devices	91
5.5	Updating the Firmware	94
5.6	Managing Applications on G6 Devices.....	97
5.6.1	Application Basics	97
5.6.2	Device Context Menu	97
5.6.3	Group Context Menu	100
5.7	Using Services	101
5.7.1	Service Table.....	101
5.7.2	Service Manager	101
5.7.3	Cable Manager	106
5.8	Managing Topologies	108
5.8.1	Menu Icons	109
5.8.2	Topology Map Elements	111
5.8.3	Adding Map Items Manually.....	112
5.8.4	Adding Topology Connections Manually	112
5.8.5	Off-Map Connections	117
5.9	Managing Notifications	119
5.10	Events Configuration	122
5.10.1	Filtering Notifications	123
5.10.2	Acknowledging Events	124
5.11	Managing Industrial Ring Errors	125
6	NMP ENTERPRISE: GETTING STARTED WITH THE SERVER COMPONENT	126
6.1	Starting the Server Manager.....	126
6.1.1	Starting on Windows®	126
6.1.2	Starting on Linux Operating Systems	126
6.1.3	First Program Start	127
6.2	Server Manager Main Window	128
6.3	Main Menu	129
6.3.1	Server	129
6.3.2	Window	130
6.3.3	Tools.....	130

6.3.4	Help	131
6.4	Tabbed Server Configuration Panel.....	134
6.4.1	Server Settings.....	134
6.4.2	Client Authentication Settings	136
6.4.3	Syslog/Logs/Events	138
6.4.4	Database Backup/Restore	141
6.4.5	Database Replication	142
6.4.6	Email Notification	143
6.4.7	SNMP Agent	144
6.5	Server Control Buttons	146
6.6	Status Text Field	146
7	NMP ENTERPRISE: WORKING WITH THE SERVER COMPONENT ..	147
7.1	Basic Configuration.....	147
7.2	Software Update	147
7.3	Server Instance as Windows Service	147
7.3.1	Provide “Log on as a service” rights to a Windows account	147
7.3.2	Setup of Server Instance.....	149
7.3.3	Managing the Server Service	150
7.4	Server Database Replication	153
7.4.1	Starting and Running Database Replication.....	154
7.4.2	General Database Replication Procedure	157
7.4.3	Scenario 1: Failure of Master Server.....	158
7.4.4	Scenario 2: Failure of Slave Server.....	160
7.4.5	Scenario 3: Link Failure between Master and Slave Server	162
7.5	Using SNMP Traps.....	164
7.5.1	Management Information Base (MIB)	164
7.6	Switch DHCP Auto-Configuration	169
7.6.1	Switch DHCP Auto-Configuration Sequence	169
7.6.2	DHCP Server Configuration.....	170
7.6.3	Configuration of Server Instance	170
7.6.4	Creating/Editing the Master Configuration File	170
7.6.5	Sending the Files to the Server Instance	170
8	NMP ENTERPRISE: GETTING STARTED WITH THE CLIENT COMPONENT	171
8.1	Starting Client Component.....	171
8.1.1	Starting on Windows®	171
8.1.2	Starting on Linux Operating Systems.....	172
8.1.3	First Program Start	173
8.2	Login to Server Instance.....	173
8.2.1	Login Credentials	173
8.2.2	User Levels and Roles	174
8.2.3	Connection Test.....	175
8.3	Device List Synchronisation	175
8.4	Main Menu (Client Component).....	177
8.4.1	Devices List	177
8.4.2	User Management.....	178
8.4.3	Settings.....	178
8.4.4	Tools	181
8.4.5	Window	182
8.5	Tabbed Data Panel	182

8.5.1 Active Alarms.....	183
8.6 Context Menu (Client Component)	183
8.6.1 Device Context Menu	184
8.6.2 Group Context Menu	186
9 NMP ENTERPRISE: WORKING WITH THE CLIENT COMPONENT ...	188
9.1 Using DHCP Autoconfiguration of G5 Devices	188
9.1.1 Creating/Editing the Master Configuration File	188
9.1.2 Sending the DHCP Autoconfiguration Files to the Server	190
9.2 Using Perspective "User Administration"	192
9.2.1 User Manager	193
9.2.2 Access to Network Devices	194
9.2.3 Device List ACL for View Based User Model	197
9.3 Using Active Alarms.....	199
9.3.1 Prerequisites.....	199
9.3.2 Mode of Operation.....	200
10 GLOSSARY	203
11 LIST OF FIGURES	205

1 Introduction

Management of devices covers monitoring, configuration and administration from a remote site. The Network Management Platform (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 (G6 and prior, MSP3000, MSP1000). Devices of other manufacturers may not be detected by NMP.

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 easy 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 "Tools" on page 47.

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 (see page 153 for more information).
- 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 Professional and the client component of NMP Enterprise. Some of them are exclusively available with the client component, whereas others are exclusively available for NMP Professional.

Note:

To use the client for server access, no additional licence key 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 v2.6 and covers installation and use of both NMP product variants. Whereas the chapters "Installation" on page 8 and "Licensing" on page 18 deal with both variants, the following chapters relate to their respective variants:

NMP Professional	NMP Enterprise
NMP Professional: Getting started (page 20)	NMP Enterprise: Getting started with the Server Component (page 126)
Working with NMP Professional (page 82)	NMP Enterprise: Working with the Server Component (page 147)
	NMP Enterprise: Getting started with the Client Component (page 171)
	NMP Enterprise: Working with the Client Component (page 188)

2 Installation

2.1 System Requirements

NMP is designed to run on personal computers or servers with the following minimum requirements; these requirements are defined for dedicated NMP systems.

Note:

NMP requires a 64-bit operating system.

- Operating system: Windows 10, Debian Linux 9, CentOS Linux 7.6 (NMP Enterprise, client component, NMP Professional);
Windows Server 2016, Debian Linux 9, CentOS Linux 7.6 (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),
3 GHz, typically 4-6 Core CPU (multi-Core i7/i5 Desktop CPU) (NMP Enterprise, client component),
3 GHz, typically 4-6 Core CPU (multi-Core i7/i5 Desktop CPU) (NMP Professional)
- Display resolution of at least 1280*1024; recommended: 1920*1080.

Note:

Please refer also to the latest NMP Release Notes document. In case of doubt, it contains the latest installation requirements.

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

2.2 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.

2.2.1 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.

2.3 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
67	UDP, BOOTP	Bootstrap Protocol for application and device: <ul style="list-style-type: none">• application listens on this port's BootP frames
68	UDP, BOOTP	Bootstrap Protocol for application and device: <ul style="list-style-type: none">• application sends BootP configuration frames
161	UDP, SNMP	Application and device: <ul style="list-style-type: none">• application initiates the communication with devices• SNMP agent can be started on this server's port• configurable
162	UDP, SNMP	used by the SNMP Trap Receiver for application and device: <ul style="list-style-type: none">• if receiving SNMP Trap is enabled, application listens on this port for SNMP Traps
514	UDP	Syslog Server on server component: <ul style="list-style-type: none">• can be enabled or disabled• default value, configurable Syslog Client on server component: <ul style="list-style-type: none">• NMP sends syslog messages to an external SYSLOG Server• can be enabled or disabled• default value, configurable
1025	UDP, MICROSENS proprietary protocol	used for application and device communication: <ul style="list-style-type: none">• application initiates the communication with devices• used on G5 and older generation of switches
1025	TCP/IP, HTTPS	used for application and device communication <ul style="list-style-type: none">• application initiates the communication with devices• communication with new generation switches (Micro Switch G6, Industrial Switch G6, NM3 modules)

Port	Protocols	Description
4000	TCP/IP	Communication between server and client component: <ul style="list-style-type: none"> server-client commands default value, configurable
4001	TCP/IP	Communication between server and client component: <ul style="list-style-type: none"> FTPS on server default value, configurable
4002	TCP/IP	Communication between server and client component: <ul style="list-style-type: none"> database server on server default value, configurable
4003	TCP/IP	Communication between server and client component: <ul style="list-style-type: none"> forwarding data from MSP1000 platform to client via server used exclusively with MSP1000 devices default value, not configurable
4177	TCP/IP	Master and slave servers: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> management modules for MSP1000 access platform
8080	TCP/IP HTTP	Web server on server component: <ul style="list-style-type: none"> can be enabled or disabled default value, configurable
8340	UDP, MICROSENS proprietary protocol	Used by IP Request listener for application and device: <ul style="list-style-type: none"> 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, MICROSENS proprietary protocol	Used for IP Configuration for application and device <ul style="list-style-type: none"> application sends IP configuration packets on this port all generations of MICROSENS switches and NM3 modules

Port	Protocols	Description
8342	UDP, MICROSENS proprietary protocol	Listening for RING error frames for application and device <ul style="list-style-type: none">• application listens on this port for special UDP packets (RING error frames)
8443	TCP/IP HTTPS	Web server on server component: <ul style="list-style-type: none">• 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 are used.

2.4 Software Installation of NMP

This section describes the installation process of MICROSENS Network Management Platform Professional and Enterprise.

Note: Must have administrative rights are a pre-requisite to install NMP. The installer application will abort the installation when this requirement has not been met

Note: To use NMP Professional or NMP Enterprise a valid licence key file is required. For more information about licensing NMP go to the following MICROSENS website (www.microsens.com/products/nmp-software).

In order to install NMP Professional or NMP Enterprise 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.

2.4.1 Difference between Installation Files for Windows® and Linux

While the NMP 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

2.4.2 Starting the Installer Application on Windows®

On Windows® open the file explorer and navigate to the directory containing the installation file of the NMP variant. Double-click the respective file named MICROSENS_NMP_Installer_v2.x.x_win64.exe to start the installation process.

Note:

After starting the installer application Windows® may show a popup dialog asking you to confirm the installation. Click the button "Yes" to proceed.

2.4.3 General Pre-Installation Settings

On the installer's welcome screen click the button "Next" in order to enter the licence agreement dialogue.

On the licence agreement screen click the button "I Agree" to go to the product and component selection dialogue.

Note:

It is necessary to scroll down the licence agreement to the end to enable the button "I Agree".

2.4.4 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.

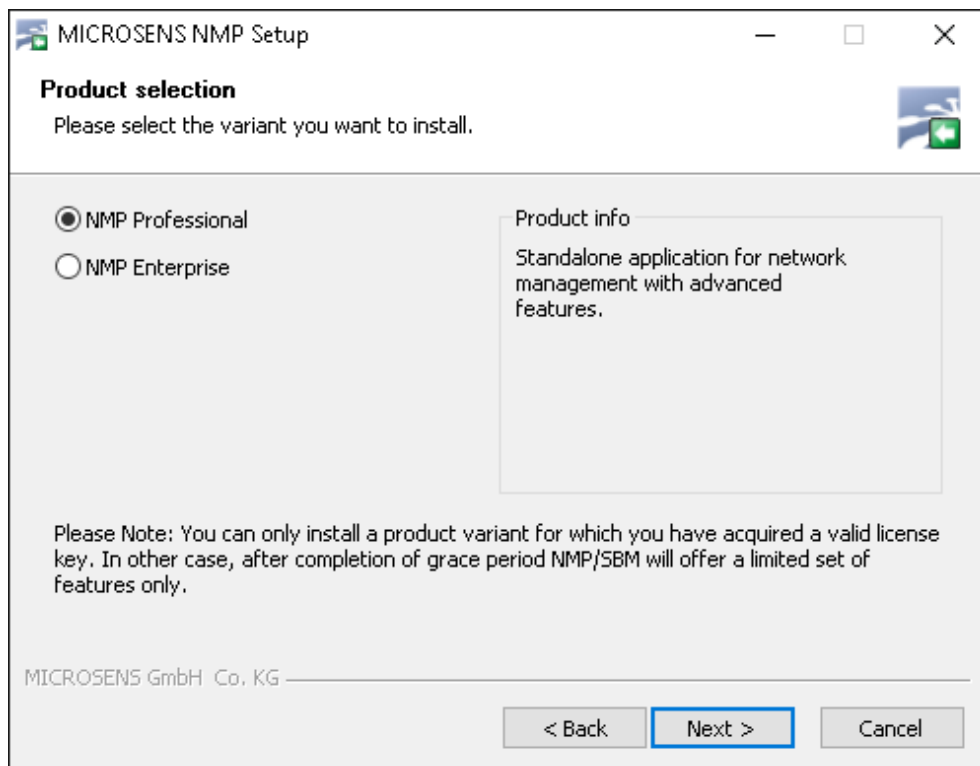


Figure 1: Installation - Product Selection

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.

2.4.5 Choose Components

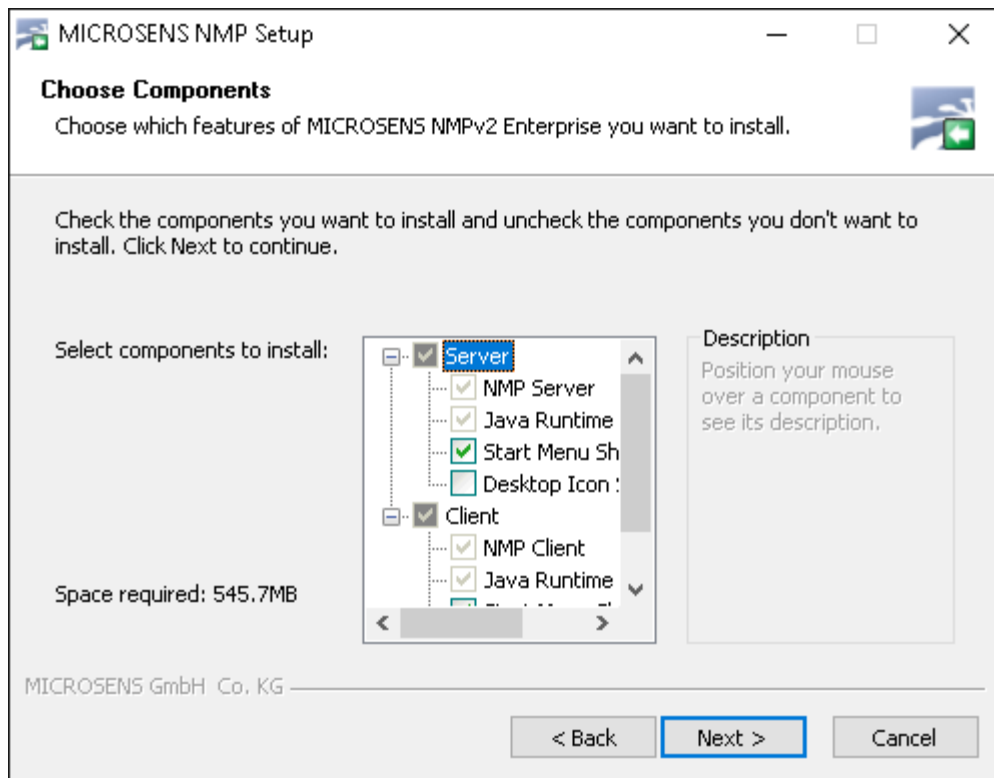


Figure 2: Installation - Choose NMP Components

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

Note:

With NMP Enterprise the installation of the client component is mandatory to access the server. For separate installations of clients on respective computers uncheck the option "Server".

Note:

When updating NMP Enterprise to a newer version, it is strongly recommended to update both the server and client components to ensure consistency of the installed software.

During the installation of the client component the installer searches for the properties file of the server component to obtain the specific values for server IP address and communication port (`%USERPROFILE%\NMPv2 Server\Settings.properties`). Otherwise the installer sets the respective default values.

2.4.6 Choose Users

On the user selection screen choose for which users the management application should be installed:

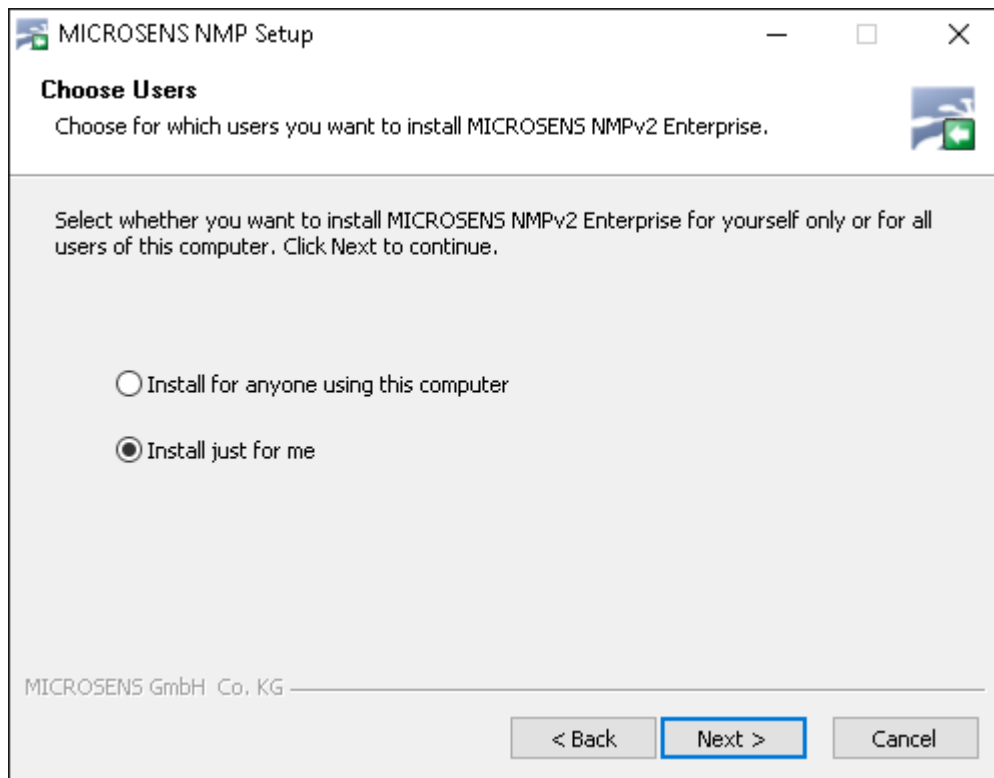


Figure 3: Installation - Choose Users

- "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 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.

2.4.7 Choose Install Location

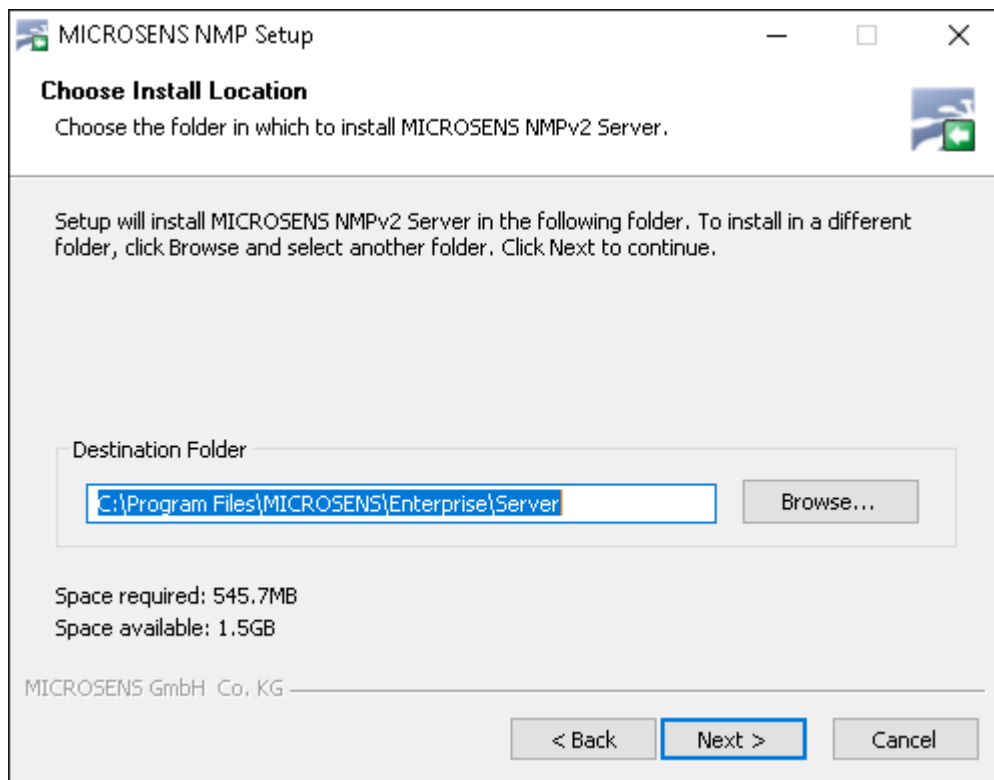


Figure 4: Installation - Choose Install Location

Now select the respective destination folders for the selected NMP variant (NMP Professional, NMP components client and server) and hit the button "Next". Afterwards hit the button "Install" to start the installation process on the system.

After finishing the installation process successfully hit the button "Finish". MICROSENS Network Management Platform is ready to be started.

Note:

Due to performance optimization NMP caches the GUI for faster display. After updating NMP it is necessary to close the application with **Exit and force default layout** (see page 24). Otherwise, based on an outdated GUI cache actual feature updates may not be visible after the next application start.

2.4.8 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 NMP 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 NMP data directory in the NMP settings (for more information please refer to page 35).

2.4.9 Installing 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 NMP Enterprise or NMP Professional on Linux use the following steps:

1. Create a new NMP directory on the local computer (for NMP Professional or NMP Client) or on a remote server (for NMP Server), e.g. `"~/MICROSENS/NMP_Professional/."` or `"~/MICROSENS/NMP_Server/."`
2. 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.
3. After file extraction is finished NMP has to be started with root access rights.

2.4.10 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 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.

On Windows® OS:

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"`)

3 Licensing

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

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, NMP 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 Selecting the Licence Key File

If no valid licence key has been selected (especially after installation of the software) this dialogue prompts to select the specific licence key file.

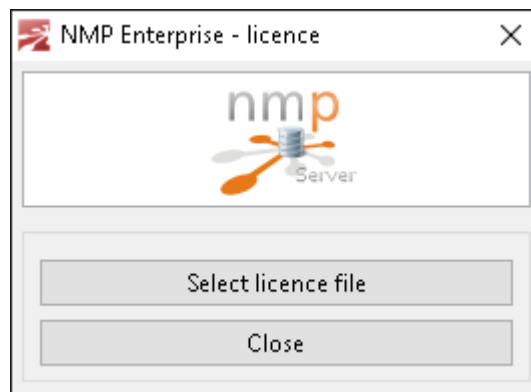


Figure 5: Licence Key File Selection

In the opening file manager dialogue of your operating system choose the specific valid licence key file and click "Open" to load the file.

After successful verification of the selected licence key file the specific NMP variant starts.

4 NMP Professional: Getting started

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.

This chapter describes the features and GUI elements of NMP Professional.

For further information about using NMP Professional please refer to the section "Working with NMP Professional" on page 82.

On how to use the client component of NMP Enterprise please refer to the chapter "NMP Enterprise: Getting started with the Client Component" on page 171.

On how to use the server component of NMP Enterprise please refer to section "NMP Enterprise: Getting started with the Server Component" on page 126.

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 on Windows®

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

Start > MICROSENS > MICROSENS NMPv2

or

Start > MICROSENS > MICROSENS NMPv2 (Debug mode)

Note:

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

NMP Professional opens with its login dialogue.

4.1.2 Starting on Linux Operating Systems

Note:

NMP 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 NMP with "sudo ./NMP" or "su root ./NMP". For more information please refer to the MICROSENS Knowledge Base on the website www.microsens.com/support.

Open a Linux CLI and change to the NMP installation directory (e.g. "~/MICROSENS/NMP_Professional").

Start NMP Professional as root user e.g. with "`sudo ./NMP`" (or the respective super user command of your Linux distribution).

4.1.3 First Program Start

During first start NMP Professional checks whether a previous NMP v1 installation is available. If so, NMP asks to migrate the data from this NMP version to NMP v2.

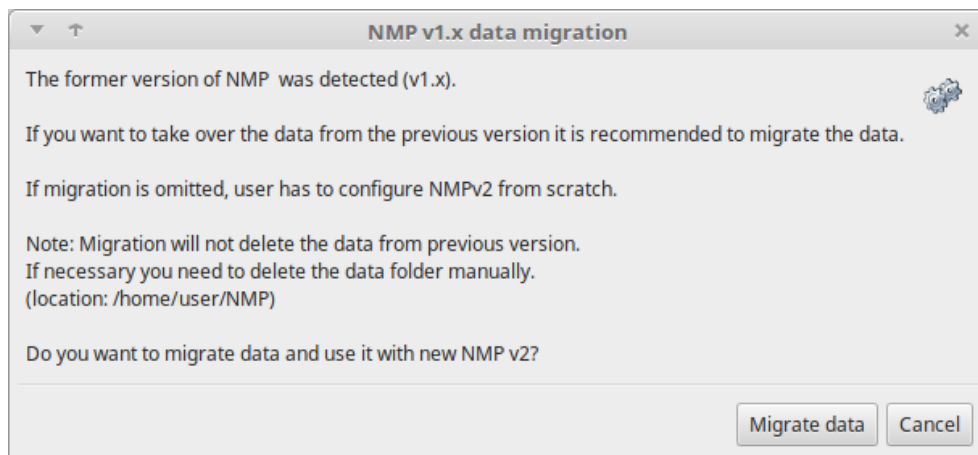


Figure 6: Data Migration from NMP v1

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

NMP Professional 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 Licensing" on page 18.

4.2 Login

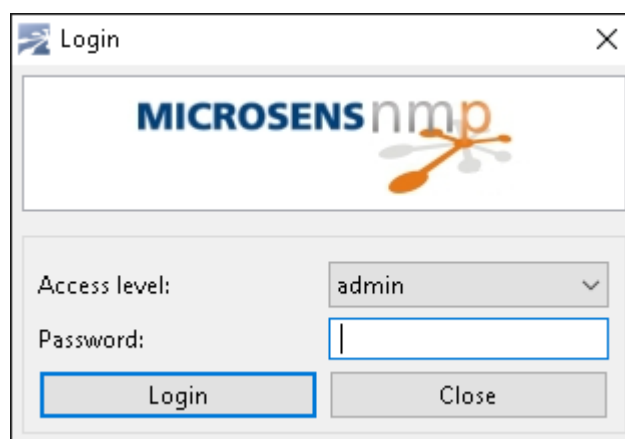


Figure 7: NMP Professional - Login

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
- change device settings
- update the firmware of devices which are managed by NMP
- 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** (see page 35).

Note:

At first start-up the user with administrative rights should configure all application settings. A detailed description is provided in section "Settings" on page 35.

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 go to the MICROSENS website (www.microsens.com/products/nmp-software).

4.3 NMP Professional Main Window

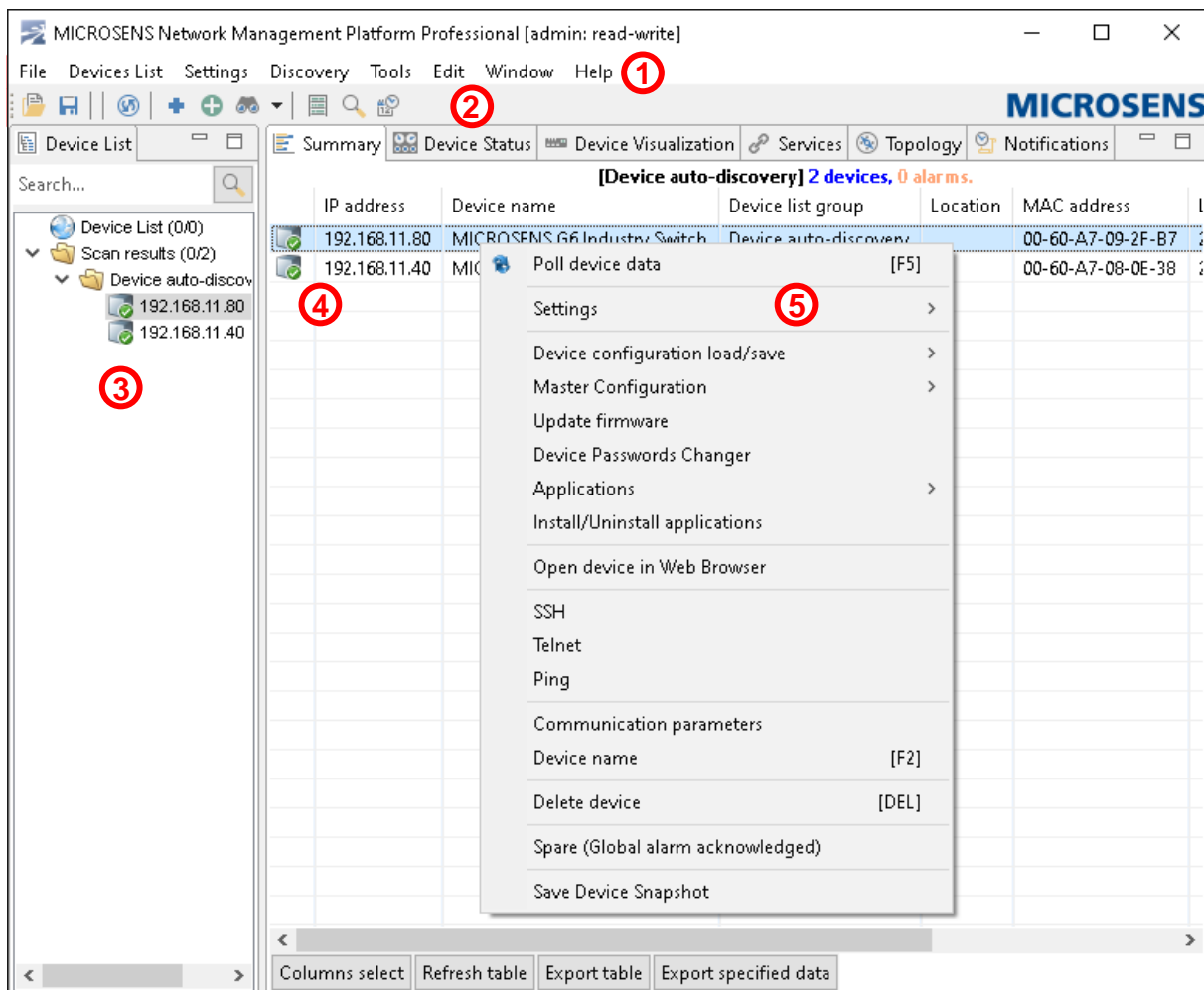


Figure 8: NMP Professional - Main Window

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

- 1** Main Menu (see page 24)
- 2** Main Menu Toolbar (see page 60)
- 3** Device List Tree (see page 60)
- 4** Tabbed Data Panel with filter section (see page 63)
- 5** Context Menu (see page 71)

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

4.4 Main Menu

The NMP main menu bar provides access to functions such as opening files, interacting with other applications and help.

4.4.1 File

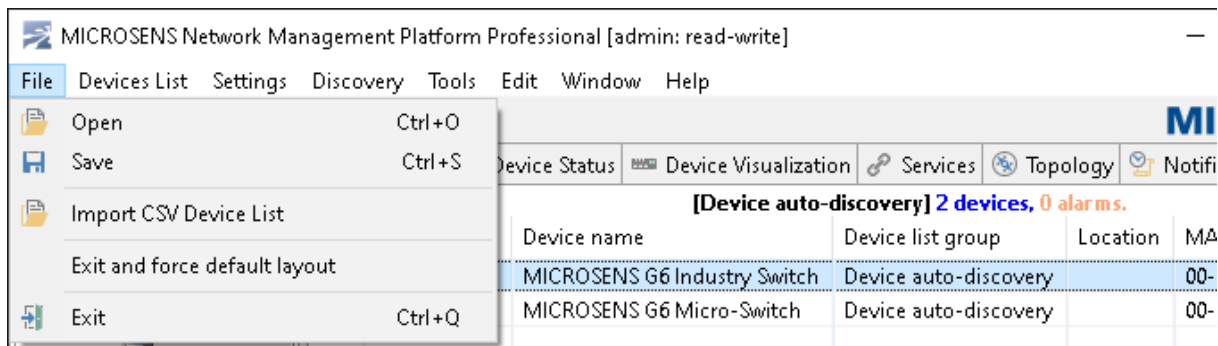


Figure 9: NMP Professional - Main Menu - File

4.4.1.1 Open (Shortcut: 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".

4.4.1.2 Save (Shortcut: Ctrl+S)

Exports the device list into a file specified by the user (extension: `.nmpd1`). Usually, this file is automatically saved by the application on exit.

4.4.1.3 Import CSV Device List (Shortcut: none)

Imports a previously saved inventory list (see page 47).

4.4.1.4 Exit and force default layout (Shortcut: none)

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`).

4.4.1.5 Exit (Shortcut: Ctrl+Q)

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

To change the NMP data directory please refer to the section "Application Settings" on page 35.

4.4.2 Devices List

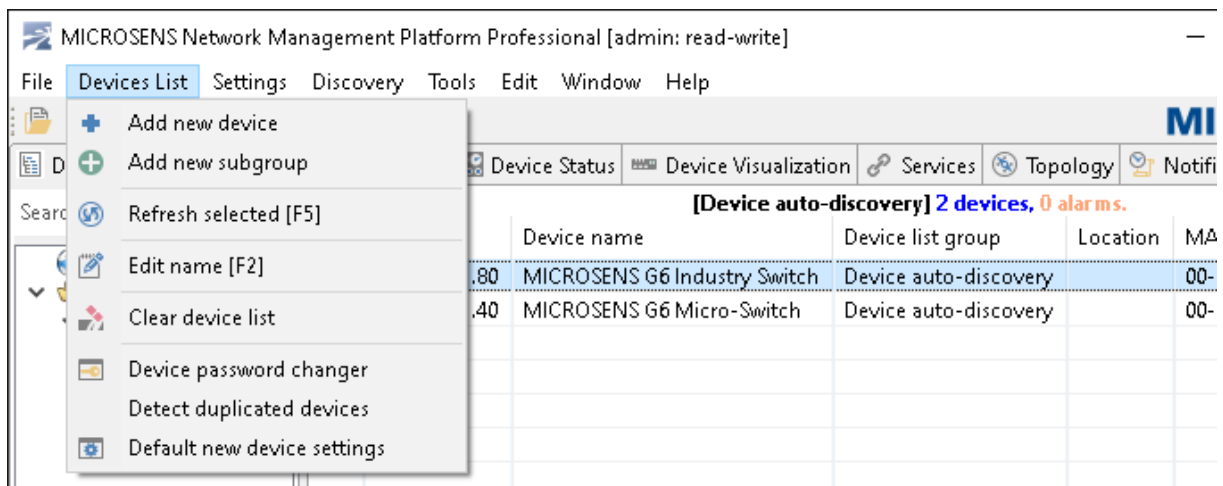


Figure 10: NMP Professional - Main Menu - Devices List

4.4.2.1 Add new device (Shortcut: None)

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 context menu.

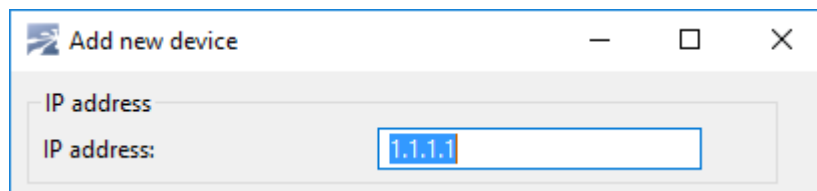


Figure 11: NMP Professional - New Device - IP Address

IP Address

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

Authorization parameters

SNMPv3

USM User:

Auth algorithm:

Auth password:

Privacy algorithm:

Privacy password:

Context name:

SNMPv1 / SNMPv2c

SNMP GET community string:

SNMP SET community string:

FTP (Access Management Module: MS416020-B)

FTP login:

FTP password:

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

Secured session user name:

Secured session password:

Generation 6 -> FTTO/Desktop/Industrial/NM3

Secured session user name:

Secured session password:

Figure 12: NMP Professional - New Device - Authorisation

Authorisation Parameters

Depending on the type of device the authorisation settings can be adapted if they differ from the defaults. The default values are defined under **Devices List -> Default New Device Settings** (see page 31).

Communication parameters

Connection TimeOut [sec]: 3

Connection retries: 2

Auto-refresh: ☒ enable

Data Auto Poll time interval [min]: 30 min

Add device Close


Figure 13: NMP Professional - New Device - Communication

Communication Parameters

The individual communication parameters can be changed for a new device if they differ from the default values. The default values are defined in **Devices List -> Default New Device Settings** (see page 31).

4.4.2.2 Add new subgroup (Shortcut: None)

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.

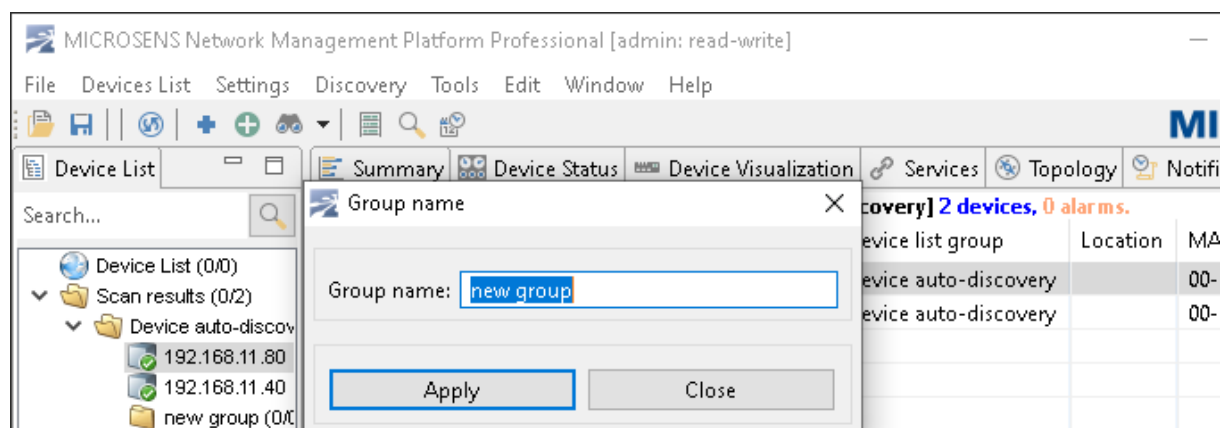


Figure 14: NMP Professional - Add New Subgroup

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.

4.4.2.3 Refresh selected (Shortcut: 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 on page 75.

4.4.2.4 Edit name (Shortcut: F2)

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

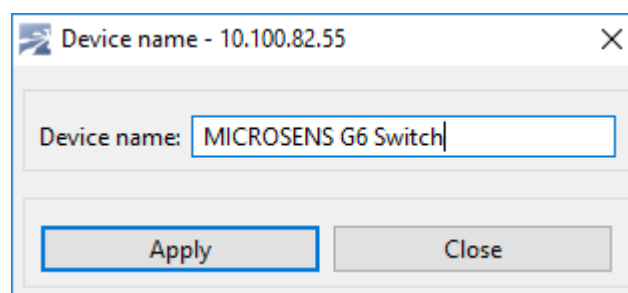


Figure 15: NMP Professional - Edit Device Name

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.

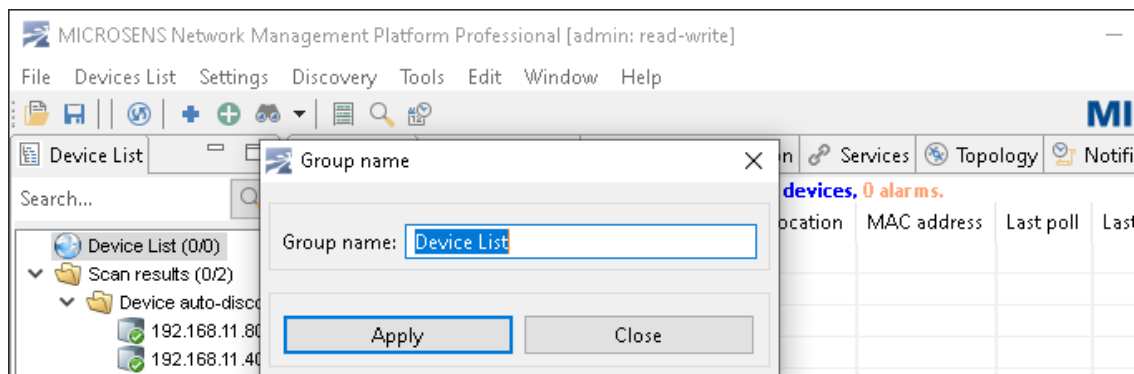


Figure 16: NMP Professional - Edit Group Name

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.

4.4.2.5 Clear device list

(Shortcut: None)

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.

4.4.2.6 Device Password Changer

(Shortcut: None)

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.

Device List

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

Current admin password:

New admin password:

New user password:

New public password:

Retype admin password:

Retype user password:

Retype public password:

Generation 6 -> FTTO/Desktop/Industrial/NM3

New admin password:

Retype admin password:

Apply

Close

Figure 17: NMP Professional - 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.

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.

©2021 **MICROSENS** GmbH & Co. KG, Kueferstr. 16, 59067 Hamm/Germany, www.microsens.com

4.4.2.7 Detect duplicated devices (Shortcut: None)

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.

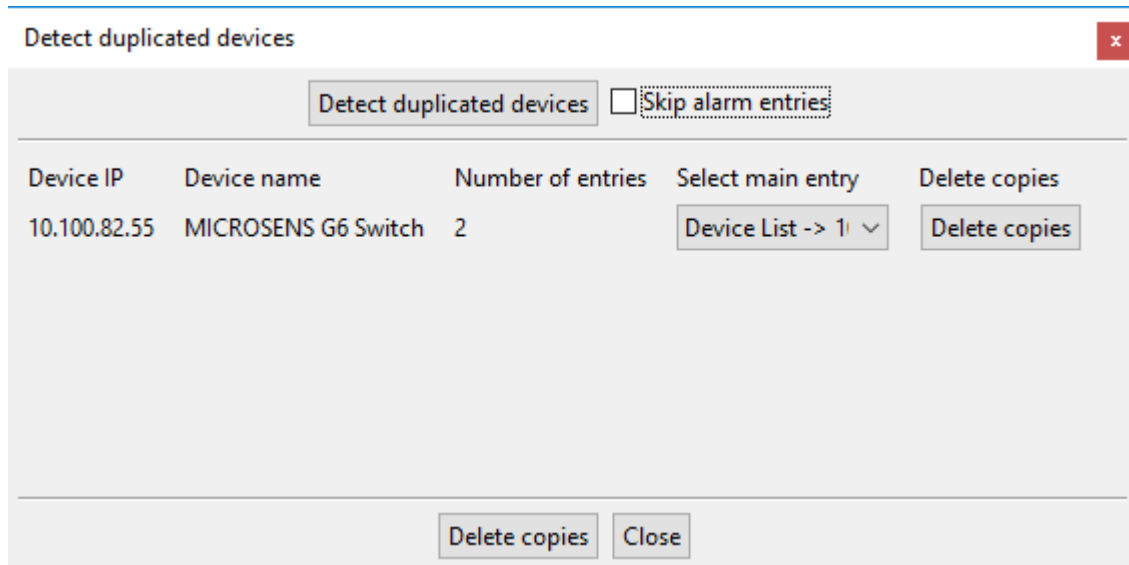


Figure 18: NMP Professional - Detect Duplicated Devices

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 "Close" button) 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 "Skip alarm entries" NMP will not search for copies at the "Alarm list" group.

Note:

The "Alarm list" is created by NMP Professional 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**.

Automatic creation of the alarm list is exclusively supported by NMP Professional and the client component of NMP Enterprise.

4.4.2.8 Default New Device Settings (Shortcut: None)

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.

Note:

It is always possible to change the parameters for each device separately with the respective devices context menu item "Communication Parameters" (see page 72).

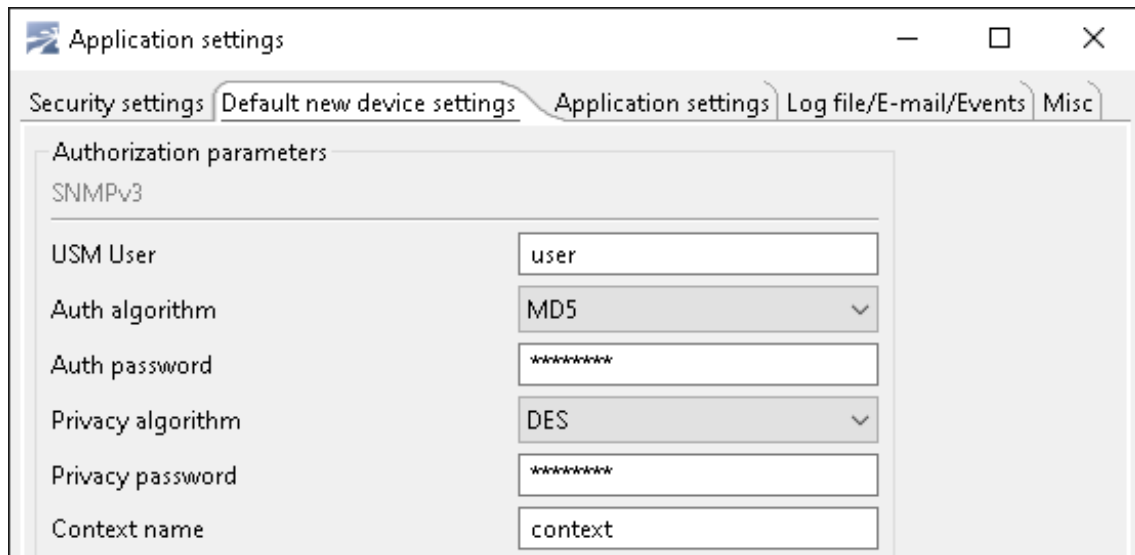
SNMPv3 Settings

Figure 19: NMP Professional - Default New Device Settings - 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	
Default SNMP GET community string:	<input type="text" value="public"/>
Default SNMP SET community string:	<input type="text" value="*****"/>

Figure 20: NMP Professional - Default New Device Settings - SNMPv1/v2c

- **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)	
Default FTP login:	<input type="text" value="admin"/>
Default FTP password:	<input type="text" value="*****"/>

Figure 21: NMP Professional - Default New Device Settings - 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	<input type="text" value="local"/>
Secured session password	<input type="text" value="*****"/>

Figure 22: NMP Professional - Default New Device Settings - Legacy Products

- **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).

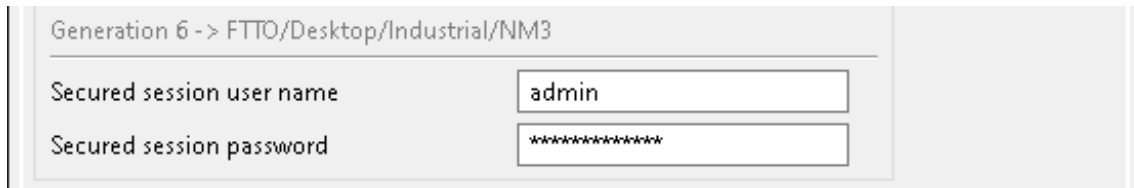


Figure 23: NMP Professional - Default New Device Settings - G6 Switches

- **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

Communication Parameters

Figure 24: NMP Professional - Default New Device Settings - Communication Parameters

- **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.

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

4.4.3 Settings

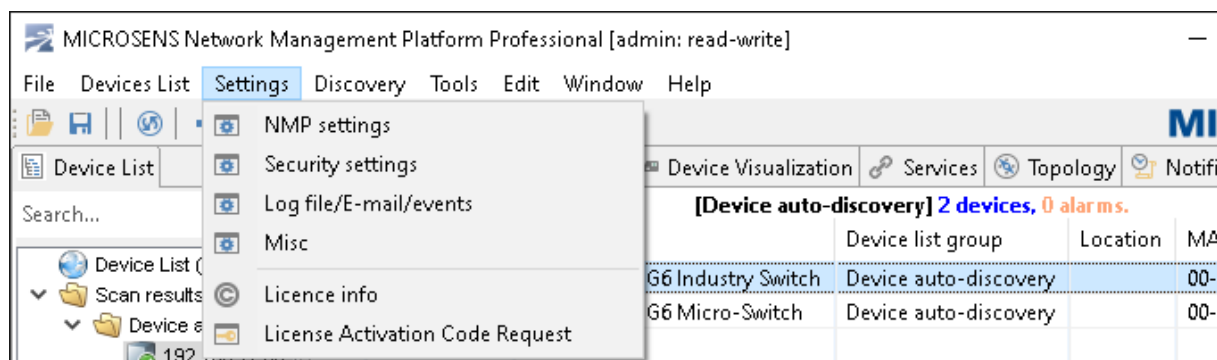


Figure 25: NMP Professional - Main Menu - Settings

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.

4.4.3.1 NMP Settings

(Shortcut: None)

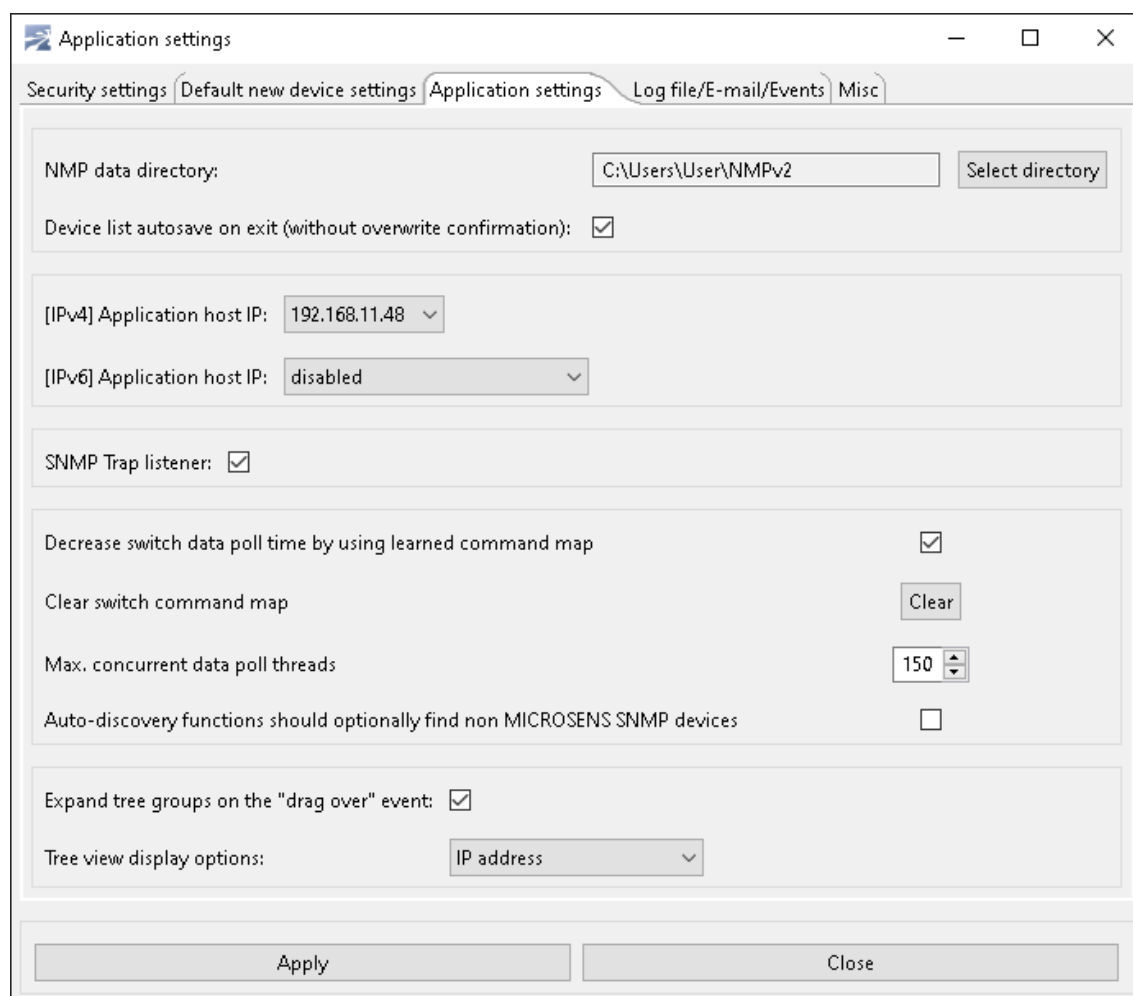


Figure 26: NMP Professional - Settings - Application Settings

In this dialogue specify the configuration settings for NMP.

- **NMP data directory:** Configure the directory where NMP saves all the configuration files. The default folder is `$USER_HOME\NMPv2`. The **NMPv2** 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:** 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:** 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.
- **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 "command map" 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.

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.
- **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 page 44).

- **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.

4.4.3.2 Security Settings

(Shortcut: None)

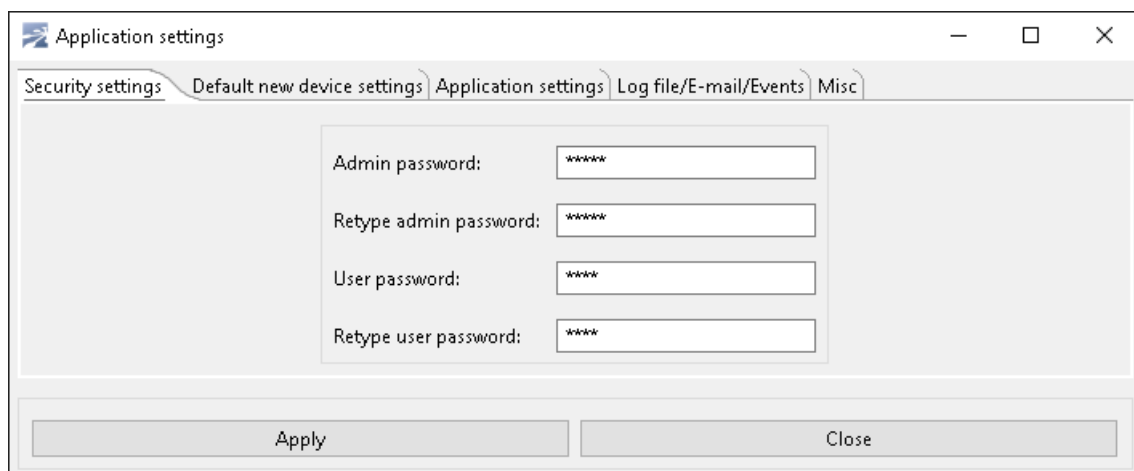


Figure 27: NMP Professional - Settings - Security Settings

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.

4.4.3.3 Log File/E-mail/Events (Shortcut: None)

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

Event Logging

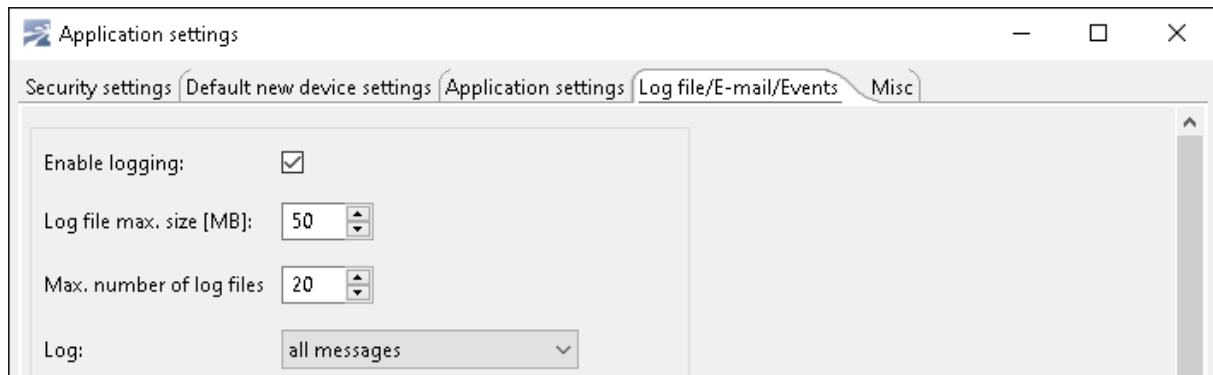


Figure 28: NMP Professional - Settings - Event Logging

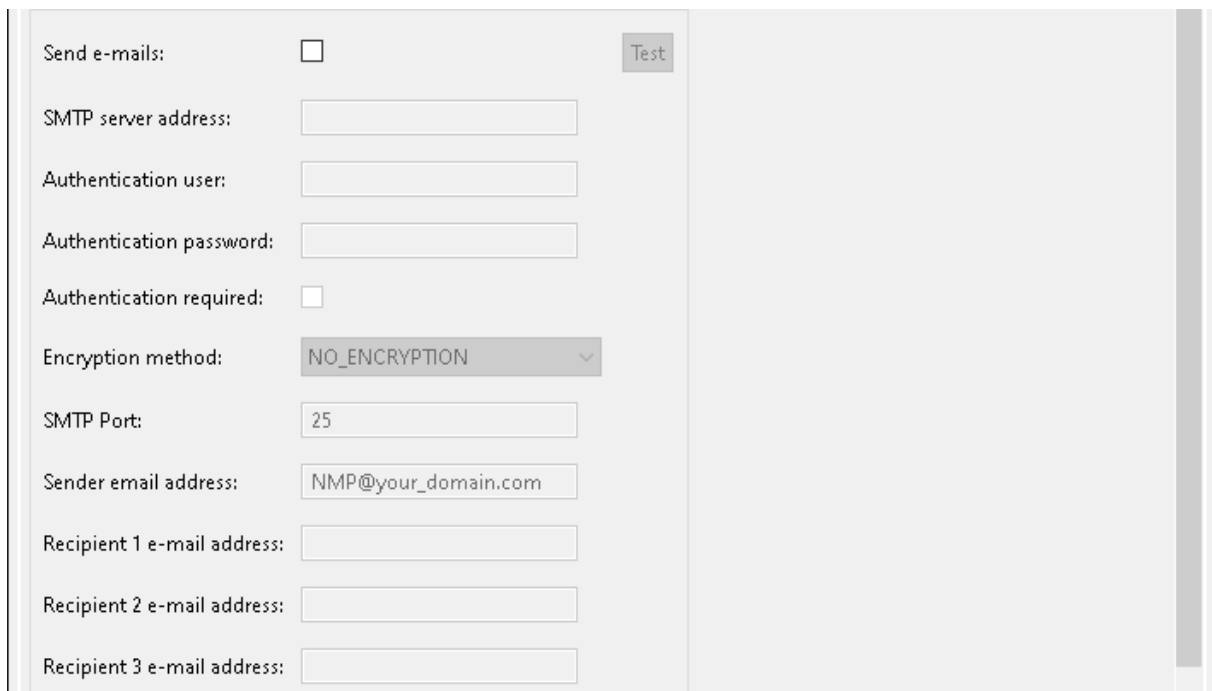
- **Enable logging:** If this option is enabled, all messages displayed in the log window are written to a log file. The default file name is "**messages_x.log**" (**x** = log file number). It is automatically created in the NMP data folder. Successively older files are renamed by adding "**x+0**", "**x+1**", "**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

E-Mail Settings



Send e-mails: ☐ Test

SMTP server address:

Authentication user:

Authentication password:

Authentication required: ☐

Encryption method: NO_ENCRYPTION ▼

SMTP Port:

Sender email address:

Recipient 1 e-mail address:

Recipient 2 e-mail address:

Recipient 3 e-mail address:

Figure 29: NMP Professional - Settings - E-Mail Settings

- **Send e-mails:** If this option is enabled and e-mail notification is enabled for different logging options (see page 38), 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
- **SMTP Port:** SMTP server port
- **Sender email address:** E-mail address used in "From" field of the sent message.
- **Recipient 1 email address:** E-mail recipient no. 1
- **Recipient 2 email address:** E-mail recipient no. 2
- **Recipient 3 email address:** E-mail recipient no. 3

Alarm Indicators

Focus the log table on unacknowledged event occurrence:	<input type="checkbox"/>
Enable blinking alarm indicator:	<input type="checkbox"/>
Create 'Alarm List' automatically:	<input type="checkbox"/>
Remove from 'Alarm list' if device will respond:	<input checked="" type="checkbox"/>

Figure 30: NMP Professional - 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 page 57.

- **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 31).

IP address	DHCP mode	Device name	Device list group	Location	MAC address
10.100.82.6	unknown	Raum118-1	Device List	default location	00-60-A7-C
10.100.82.78	on	MICROSENS G6 Switch	Device List		
10.100.82.84		MICROSENS G6 Switch	Device List		00-60-A7-C
10.100.82.92	on with script	MICROSENS G6 Switch	Device List		00-60-A7-C
10.100.82.93		MICROSENS G6 Switch	Device List		
10.100.82.102	off	MICROSENS G6 Switch	Device List		00-60-A7-C
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-C
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-C
10.100.89.6	off	rumicon VI & N Switch	Device List		00-60-A7-C

Figure 31: NMP Professional - 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 (see page 76).

- **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

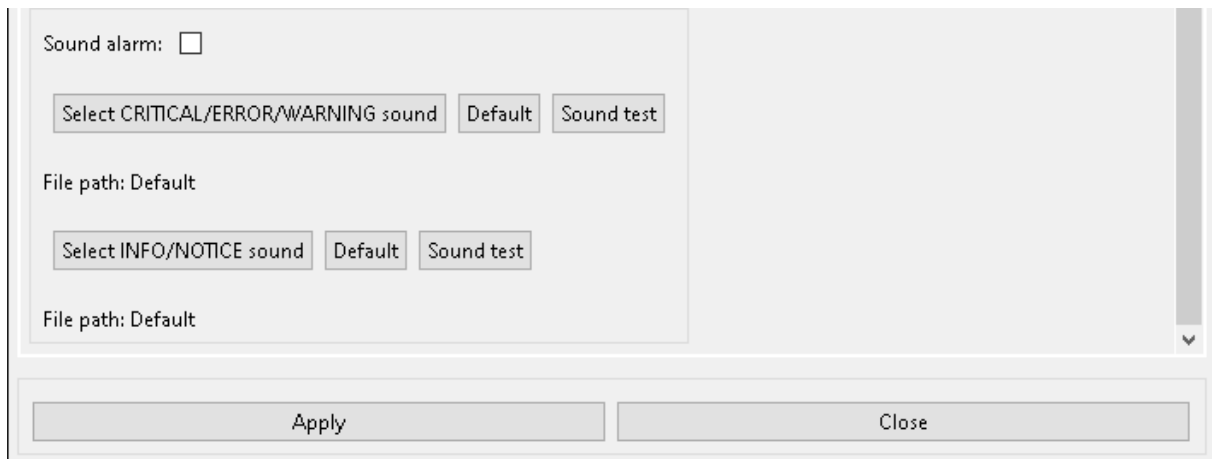


Figure 32: NMP Professional - Settings - Sound Alarm

- **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 "Select" button 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.

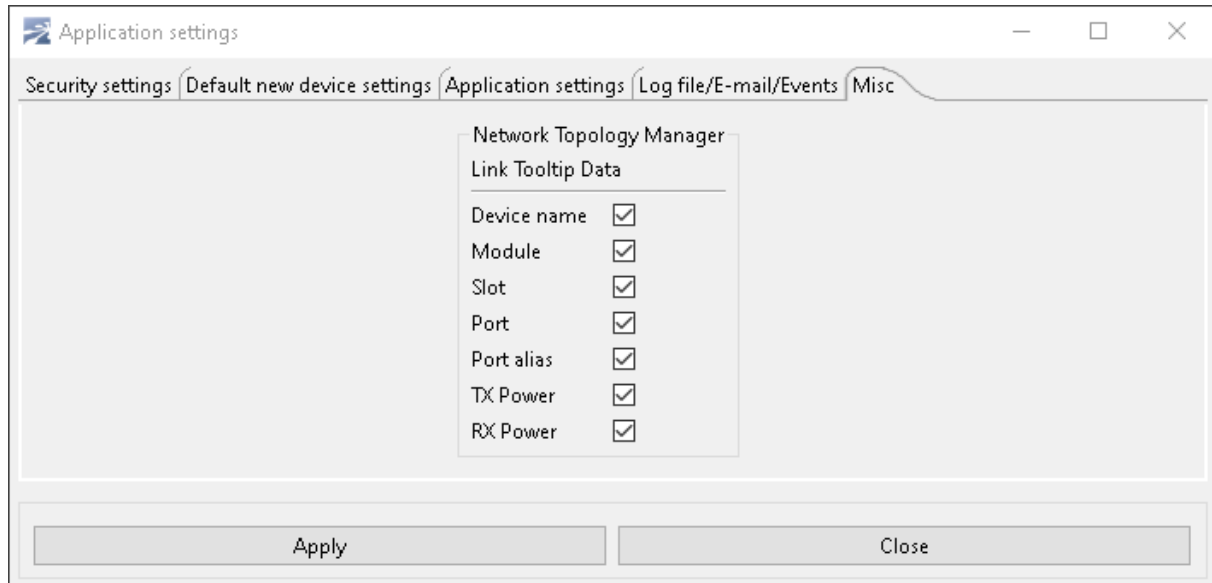
Note:

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

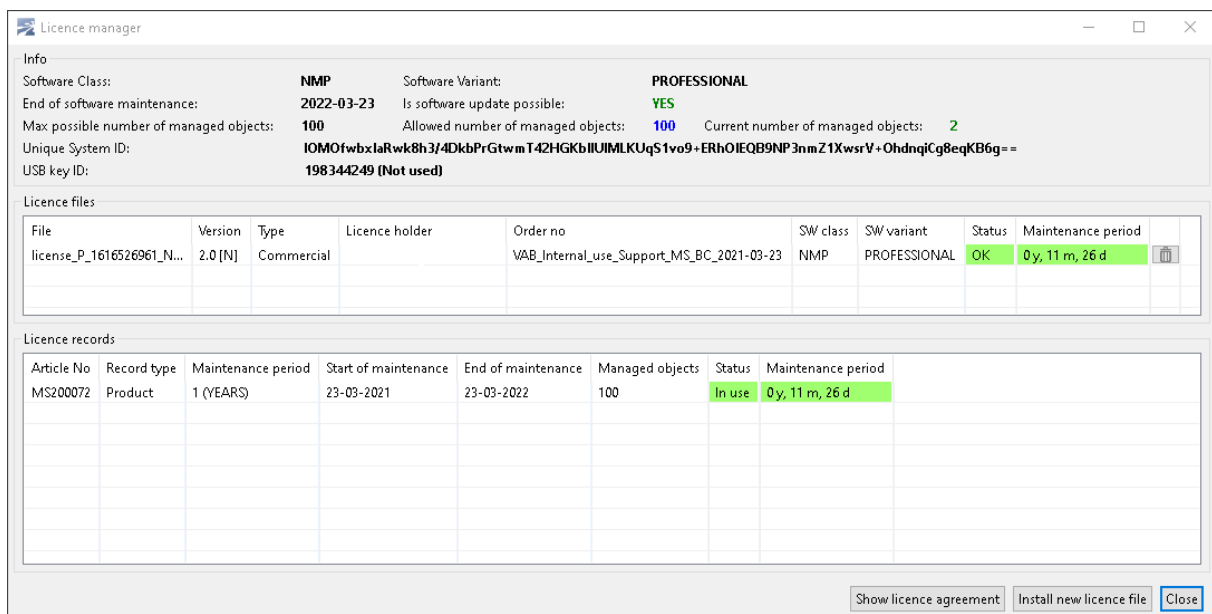
Click the button "Apply" to save the respective input.

4.4.3.4 Misc**(Shortcut: None)**

In this dialogue specify the link tooltip data of the topology manager (see page 70).

**Figure 33: NMP Professional - Settings - Misc**

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

4.4.3.5 Licence Info**(Shortcut: None)****Figure 34: 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 NMP 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 NMP 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 NMP Enterprise.
- Copy the licence key file directly into the local folder `$USER_HOME/$NMP_DATA_DIR/licenses`. NMP 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 NMP service 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 NMP Enterprise licence key folder use the licensing information dialogue of the client component.

Note:

To obtain a new NMP Enterprise licence key file please contact MICROSENS.

4.4.4 Discovery

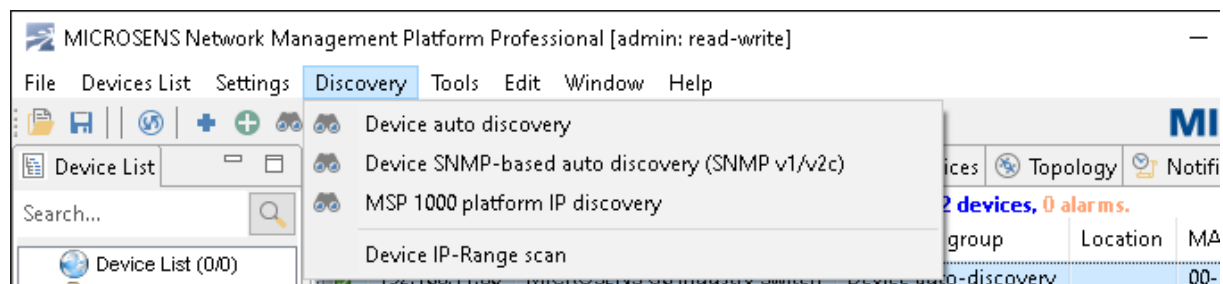


Figure 35: NMP Professional - Main Menu - Discovery

4.4.4.1 Device Auto Discovery (Shortcut: None)

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).

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	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>

Discovered devices: 2, new devices: 2 [Page 1 of 1] ☐ Select all
Add to list

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 36: NMP Professional - Device Auto Discovery

Note:

If no device is detected, the auto discovery dialogue (Figure 36) will not appear.

For more information on how to use the "Switch Auto Discovery" function, please refer to section "Adding New Devices with Device Auto Discovery" on page 82.

4.4.4.2 Device SNMP-based Auto Discovery (SNMP v1/v2c) (Shortcut: None)

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 page 31).

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 page 31).

Figure 37: NMP Professional - SNMP-based Auto Discovery

The discovery window looks similar to the “Switch Auto Discovery” dialogue described above. 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.

4.4.4.3 MSP 1000 platform IP discovery

(Shortcut: None)

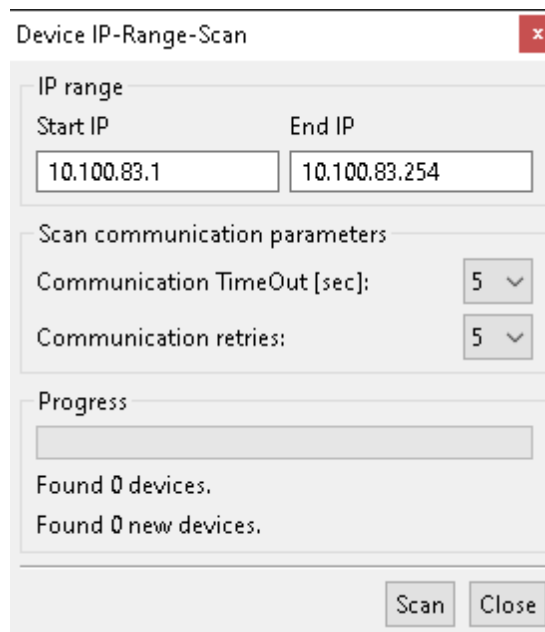
Figure 38: NMP Professional - MSP 1000 Platform IP Discovery

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.

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.

4.4.4.4 Device IP-Range scan**(Shortcut: None)**

Device IP-Range-Scan

IP range

Start IP: 10.100.83.1 End IP: 10.100.83.254

Scan communication parameters

Communication TimeOut [sec]: 5

Communication retries: 5

Progress

Found 0 devices.

Found 0 new devices.

Scan Close

Figure 39: 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 page 31).

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.

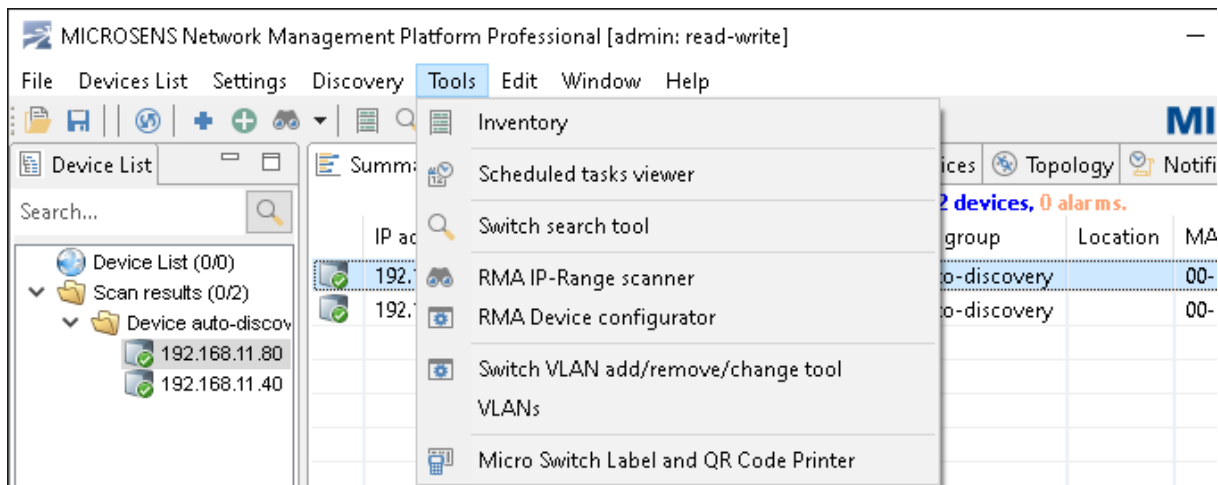


Figure 40: NMP Professional - Main Menu - Tools

4.4.5.1 Inventory

(Shortcut: None)

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 will be included before generating the list.

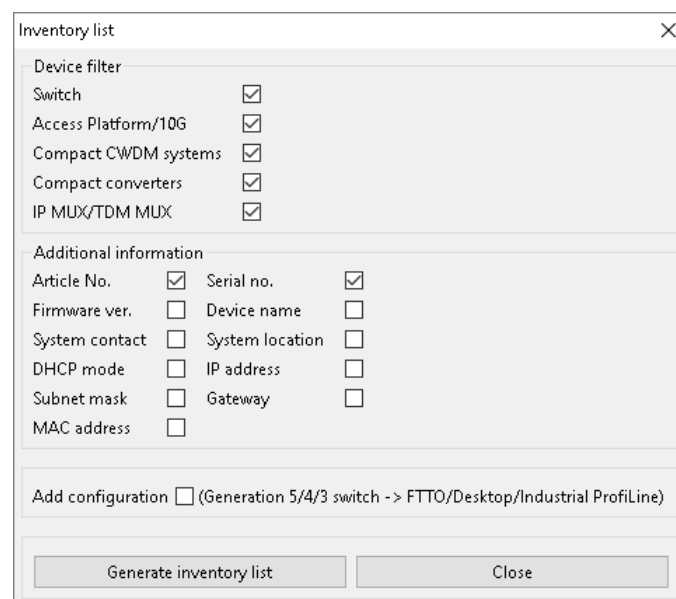


Figure 41: NMP Professional - Inventory

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

To import the inventory list into NMP Professional go to **File -> Import CSV Device List** (see page 24).

4.4.5.2 Scheduled tasks viewer

(Shortcut: None)

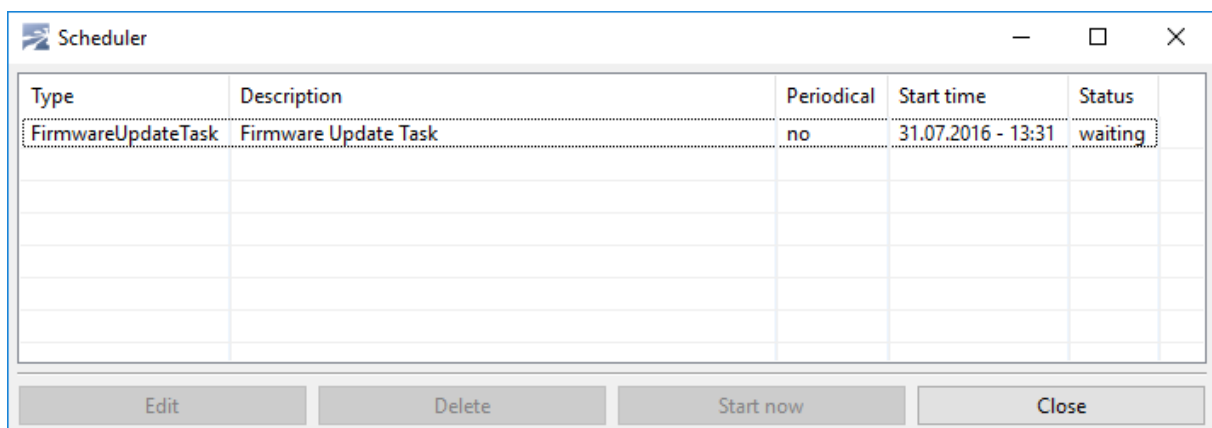


Figure 42: NMP Professional - Scheduled Task Viewer

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.

4.4.5.3 Switch search tool

(Shortcut: None)

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".

Figure 43: NMP Professional - Switch Search Tool

4.4.5.4 RMA IP Range Scanner

(Shortcut: None)

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.

RMA IP Range scanner

Start IP End IP Alias Add

Start IP	End IP	Alias
----------	--------	-------

Scan selected ranges Delete selected

Scan rate (min.) 10

Scan progress

RMA devices:

Scan Save task Close

Figure 44: NMP Professional - 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 page 48).

4.4.5.5 RMA Device configurator

(Shortcut: None)

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 Search

Stored configuration

Reconfigure IP address manually ☐

New device MAC address 00-60-A7- Reconfigure RMA device

Close

Figure 45: NMP Professional - 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 “Search” button. 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.

4.4.5.6 Switch VLAN Add/Remove/Change Tool (Shortcut: None)

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.

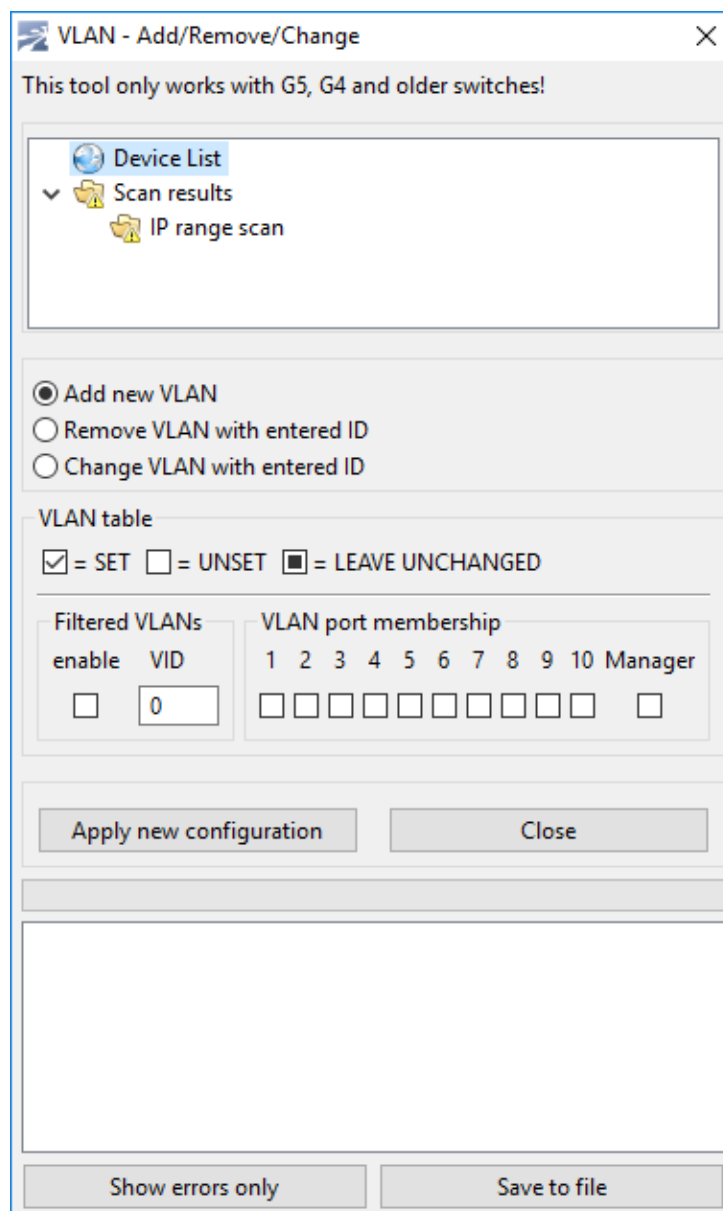


Figure 46: NMP Professional - VLAN Add/Remove/Change

Note:

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

4.4.5.7 VLANs**(Shortcut: None)**

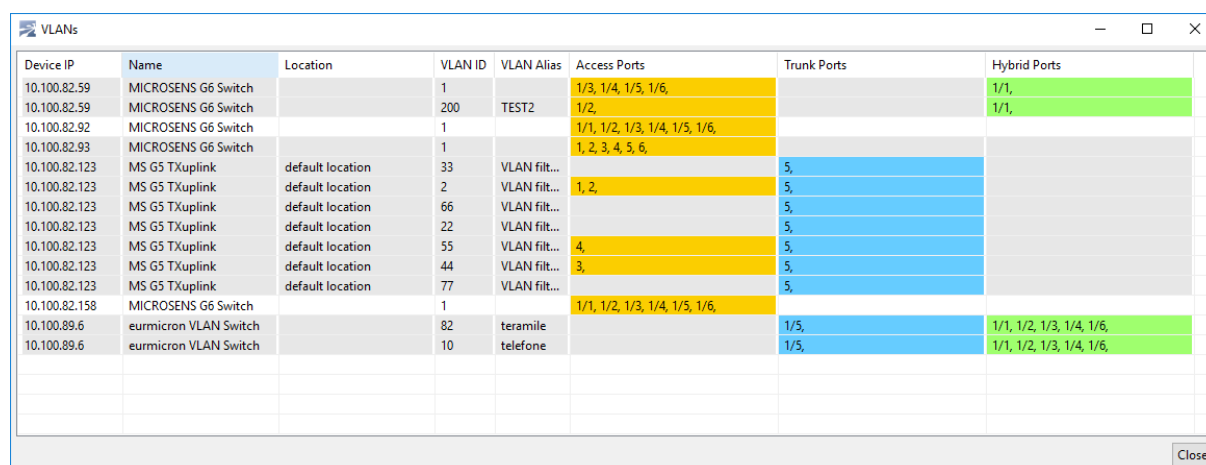
“VLANs” allows displaying the current VLAN configuration on all MICROSENS switches and SNMP-based devices available on the device list.

Note:

The Q-Bridge MIB enables access to non-MICROSENS devices VLAN configuration parameters via SNMP. According to this “VLANs” 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 47: NMP Professional - 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 page 68) 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.

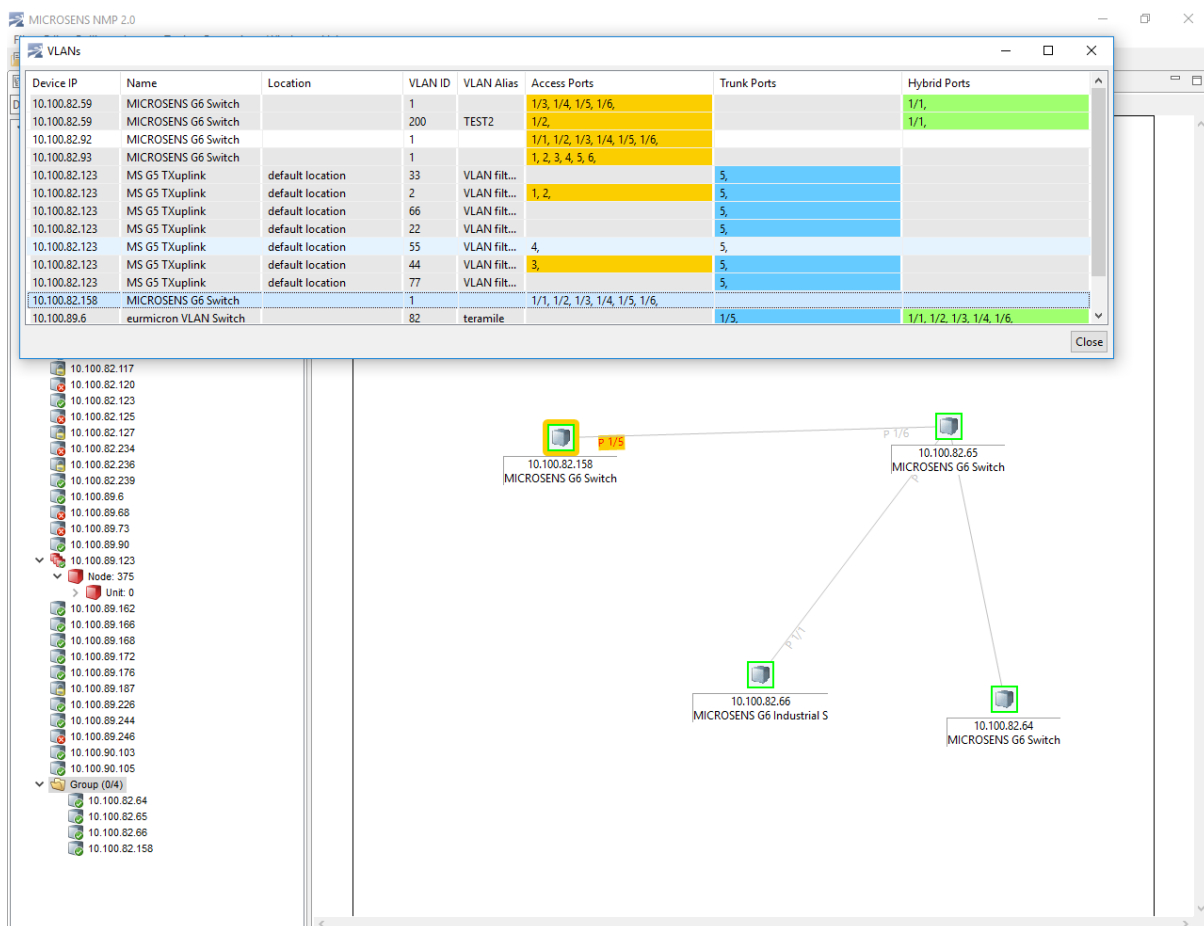


Figure 48: NMP Professional - VLANs tool with Topology Manager

In the example (Figure 48) 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.

4.4.5.8 Micro Switch Label and QR Code Printer (Shortcut: None)

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

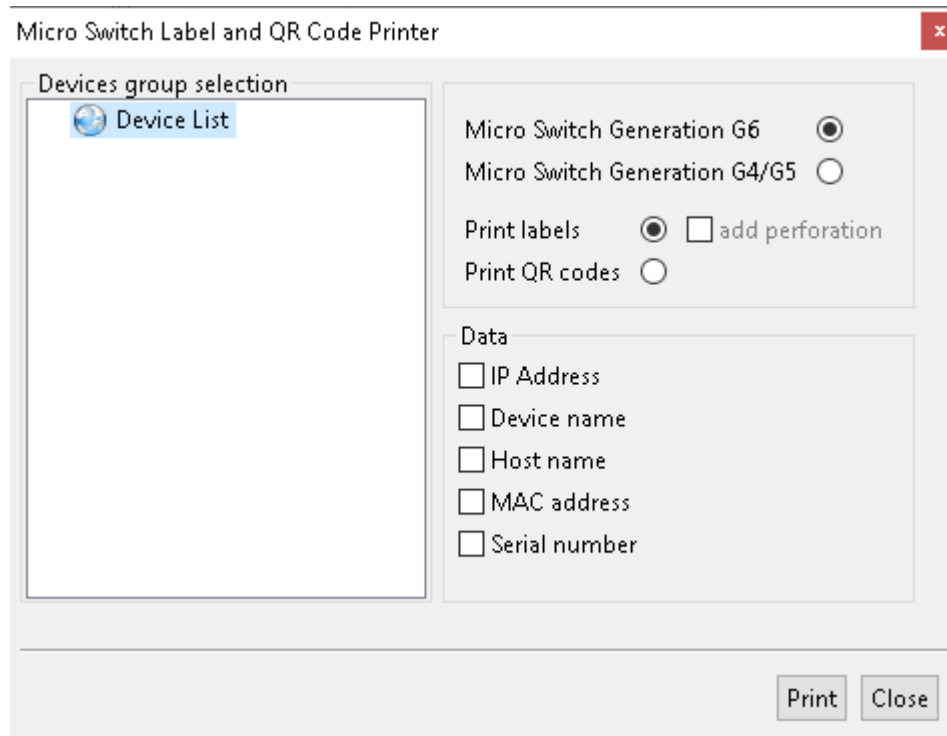


Figure 49: NMP Professional - Micro Switch Label and QR Code Printer

- **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.

4.4.6 Edit

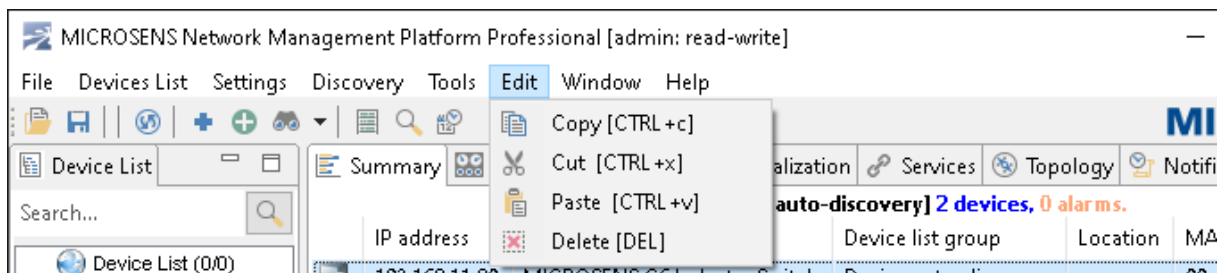


Figure 50: NMP Professional - Main Menu - Edit

4.4.6.1 Copy (Shortcut: 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.

4.4.6.2 Cut (Shortcut: 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.

4.4.6.3 Paste (Shortcut: 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).

4.4.6.4 Delete (Shortcut: 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

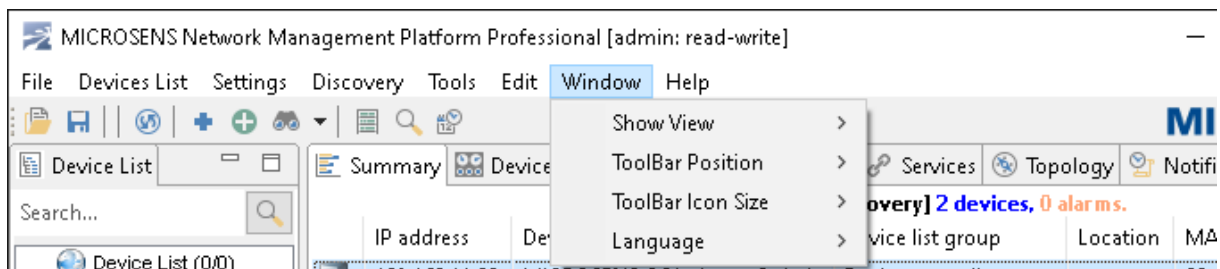


Figure 51: NMP Professional - Main Menu - Window

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

4.4.7.1 Show View

(Shortcut: None)

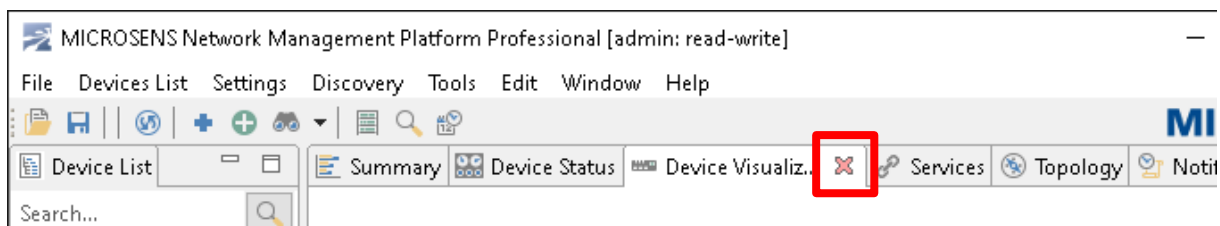


Figure 52: NMP Professional - Tabbed Data Panel - Close Icon

NMP allows closing some of the tabbed data panels by selecting the [X] icon next to the panel name. For more information about the tabbed data panels please refer to page 63.

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.

4.4.7.2 Toolbar Position (Shortcut: None)

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

- Top
- Left
- Bottom

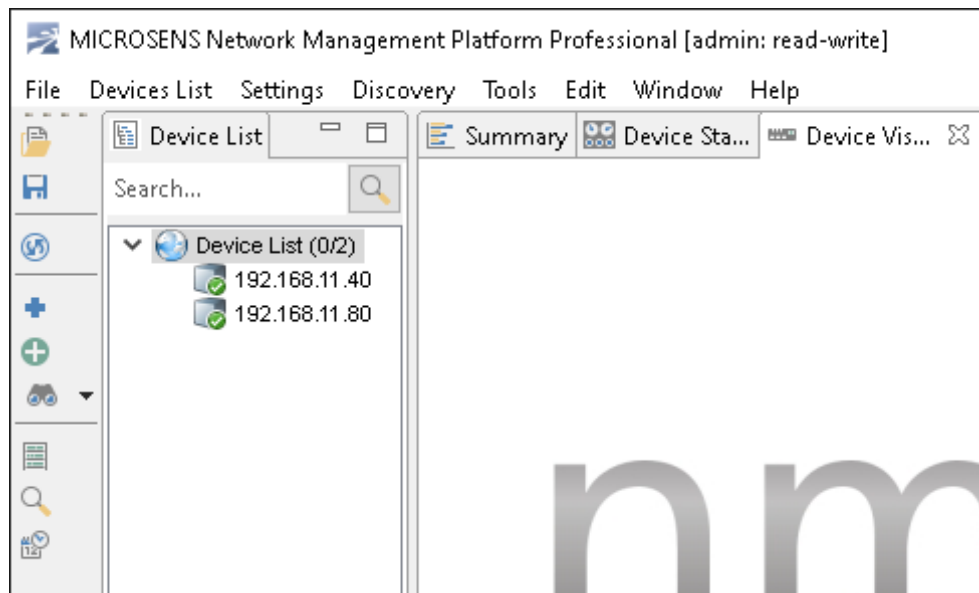


Figure 53: NMP Professional - Toolbar left

4.4.7.3 Toolbar Icon Size (Shortcut: None)

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

- 16x16
- 32x32

4.4.7.4 Language (Shortcut: None)

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

- English
- German

4.4.8 Help

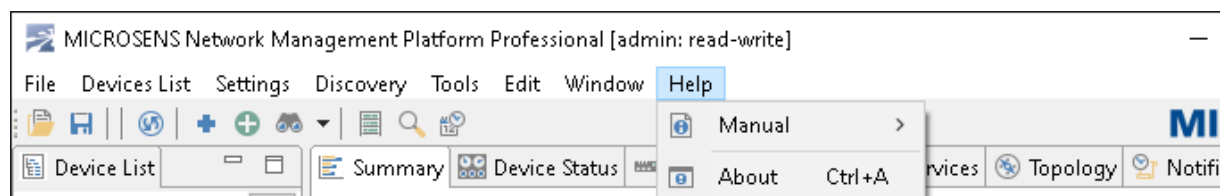


Figure 54: NMP Professional - Main Menu - Help

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

4.4.8.1 Manual (Shortcut: None)

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

4.4.8.2 About (Shortcut: None)

This dialogue shows information on the NMP version.

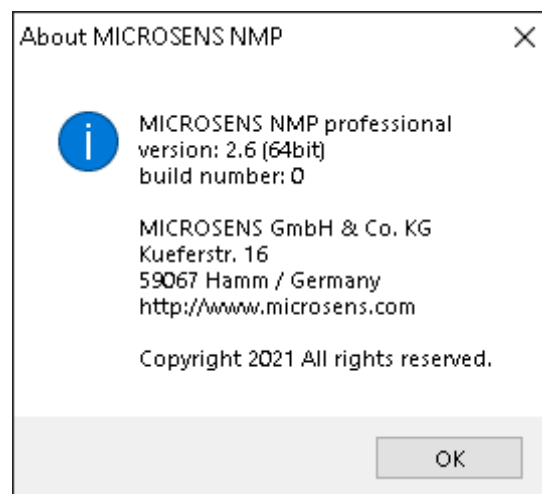


Figure 55: NMP Professional - About

4.5 Main Menu Toolbar

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

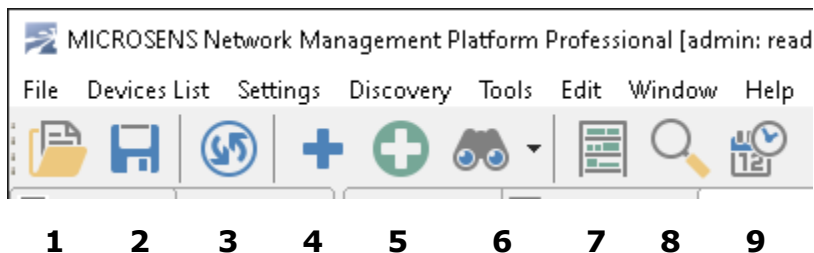


Figure 56: NMP Professional - Main Menu Toolbar

No.	Task	Main Menu Item/Detailed Information
1	Load device list	File -> Open (see page 24)
2	Save device list	File -> Save (see page 24)
3	Refresh selected devices	Device List -> Refresh selected devices (see page 28)
4	Add new device	Device List -> Add new device (see page 25)
5	Add new subgroup	Device List -> Add new subgroup (see page 27)
6	Device auto discovery	Discovery (see pages 43 to 46)
7	Create Inventory List	Tools -> Inventory (see page 47)
8	Device search tool	Tools -> Switch search tool (see page 49)
9	Scheduled tasks viewer	Tools -> Scheduled tasks viewer (see page 48)

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** (see page 58).

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.

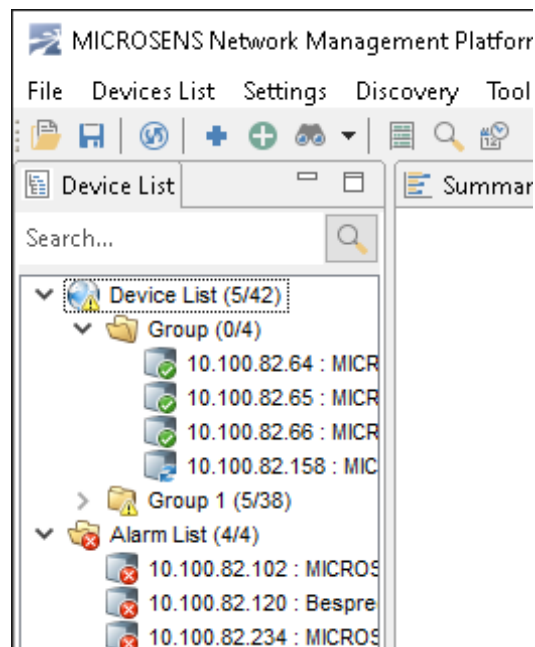


Figure 57: NMP Professional - Device List Tree View

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.

Summary	Device Status	Device Visualization	Services	Topology	Notifications	
[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
<div>Columns select</div> <div>Refresh table</div> <div>Export table</div> <div>Export specified data</div>						

Figure 58: NMP Professional - Tabbed Data Panel

The following tabs are available:

- Summary (see page 64)
- Device Status (see page 67)
- Device Visualization (see page 68)
- Services (see page 69)
- Topology (see page 70)
- Notifications (see page 71)

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 "Show View" on page 57).

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.

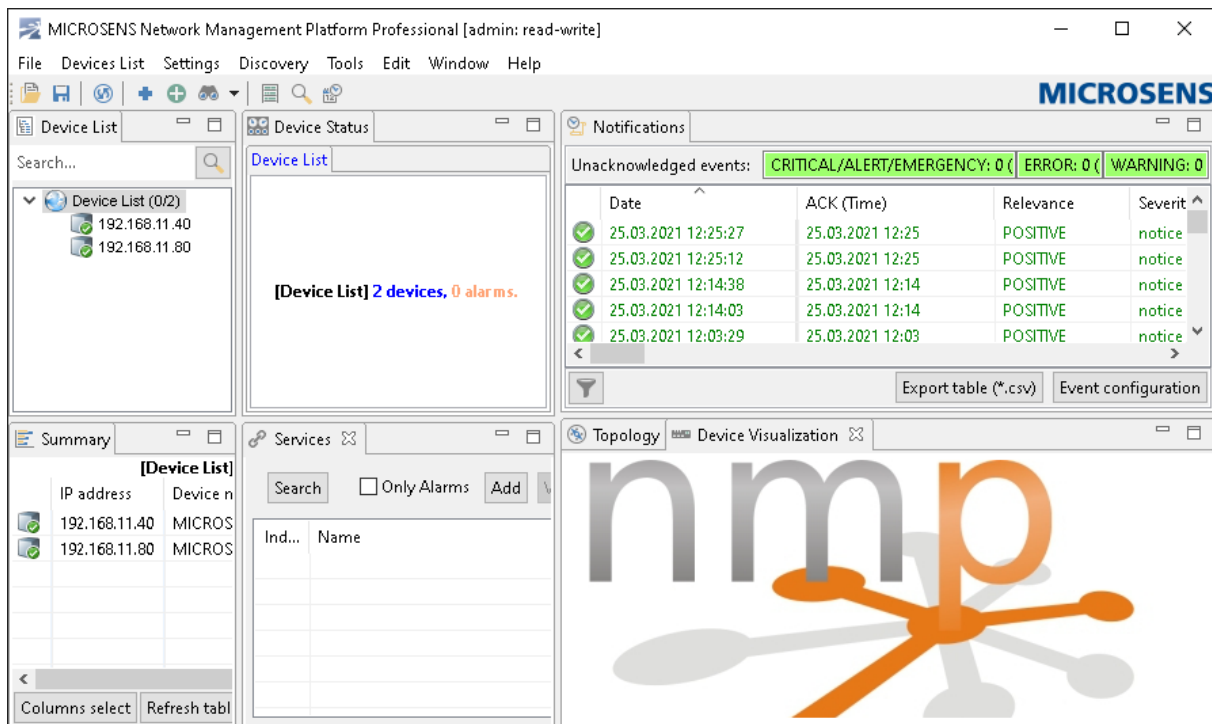


Figure 59: NMP Professional - Tabbed Data Panel - Placing the Tabs

4.7.1 Summary

Summary	Device Status	Device Visualization	Services	Topology	Notifications	Active Alarms
[Devices] 2 devices, 0 alarms.						
IP address	Device name	Device...	L...	MAC address	Last poll	Last response
192.168.11.40	MICROSENS G6 Micro-Switch	Devices		00-60-A7-08-0E-38	30.03.2021 - 17:32:00	30.03.2021 - 17:32:00
192.168.11.80	MICROSENS G6 Industry Switch	Devices		00-60-A7-09-2F-B7	30.03.2021 - 17:31:18	30.03.2021 - 17:31:18

Figure 60: NMP Professional - Tabbed Data Panel - Summary

The device summary table shows information on the currently selected subgroup 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 page 72 for more information).

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.

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

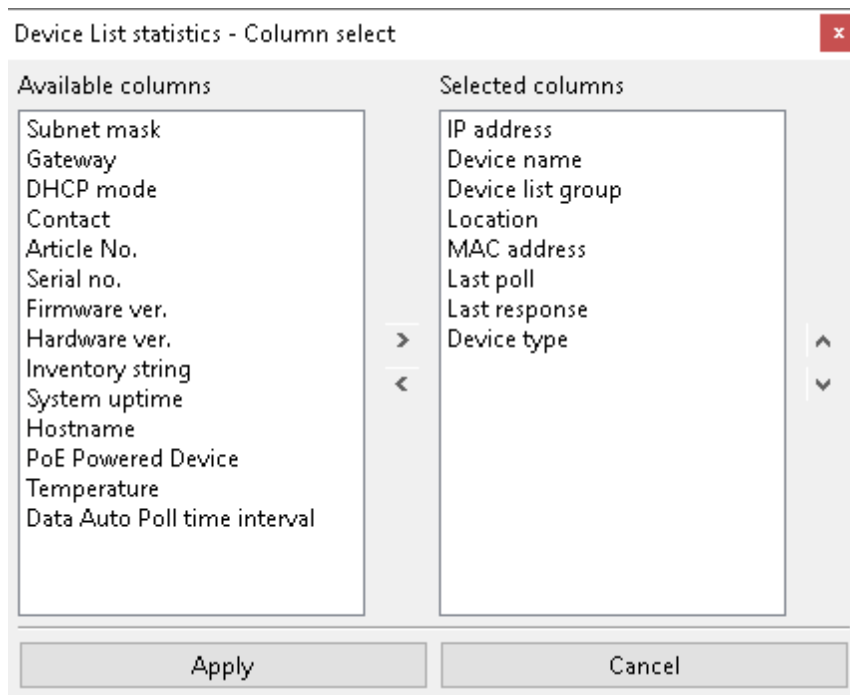


Figure 61: NMP Professional - Tabbed Data Panel - Summary - Column Select

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".

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

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.

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.

Switch Data Export

Device info

☐ Article No. ☐ Serial no. ☐ Firmware ver. ☐ Device name ☐ System contact
☐ System location ☐ Inventory string ☐ Hardware ver. ☐ Select all

IP/MAC

☐ DHCP mode ☒ IP address ☐ Subnet mask ☐ Gateway ☐ MAC address ☐ Select all

VLAN

☐ VLAN filtering enabled ☐ Force Default VID ☐ Voice VLAN ID ☐ RSTP VLAN ID ☐ VLAN ID for unauthorized ports ☐ Select all

Port

☐ Port no. ☐ Alias ☐ enabled ☐ Auto-Neg. ☐ Speed
☐ Duplex ☐ MDI-MDIX ☐ VLAN Mode ☐ Port VID ☐ Force Default VID
☐ VLAN prio. ☐ VLAN port membership ☐ Select all

PoE

☐ PoE MAX Total Input Power ☐ PoE Enable extended voltage range ☐ PoE Mode ☐ PoE PLUS ☐ Max. PSE power [W]
☐ Max. PD class ☐ PoE Priority Mode ☐ PoE Determined Class ☐ PoE Status ☐ PoE Power ☐ Select all

CDP/LLDP

☐ CDP/LLDP Device ID ☐ CDP/LLDP Device IP ☐ CDP/LLDP Device Port ID ☐ Select all

Port Access Control

☐ Entry state ☐ Authorization state ☐ Authorization mode ☐ User MAC ☐ User name
☐ PACC VLAN ID ☐ PACC VLAN Alias ☐ Login Time Stamp ☐ Select all

MAC Table

☐ MAC Table Entries
(Skip uplink and downlink ports ☐ One MAC Per Line ☐)

Generate report now (for selected group) Schedule (for whole device list) Close

Figure 62: NMP Professional - 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	2019-12-09 06:07:27
uptime	0 days, 05:37:34
used mac address	00:60:A7:08:0E:38
used boot media	INTERNAL MEMORY
temperature	39
climate level	NORMAL

firmware

This section provides details about the running firmware.

running version	10.7.4a
build date	2019-06-07 13:05:14
build number	8970
patch version	

save info

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

last saved parameter	files,scripts.execute
save mode	PERMANENTLY
write status	PROCESSING
time stamp	09.12.2019 06:07:29

Figure 63: NMP Professional - 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

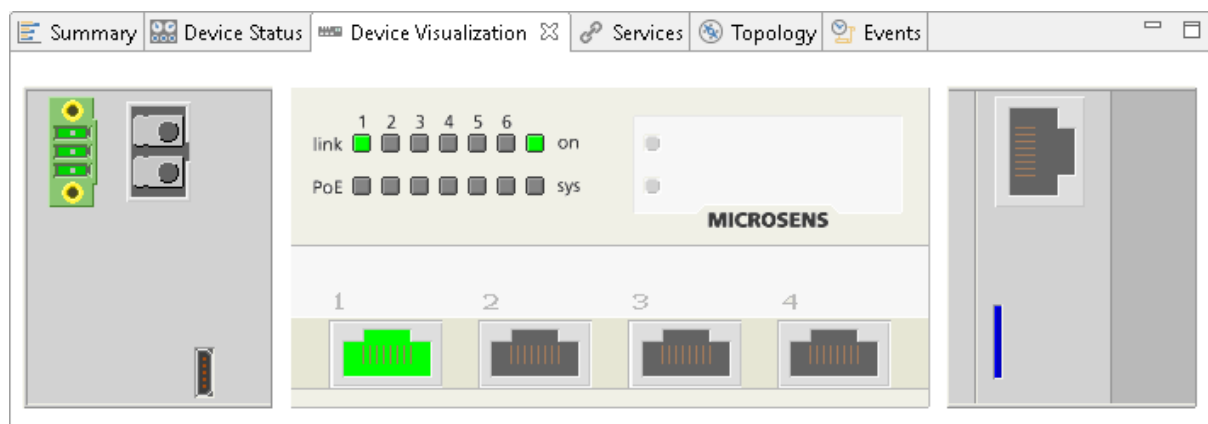







Figure 64: NMP Professional - Tabbed Data Panel - Device Visualization (Micro Switch G6)

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
	1000 Mbps 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).

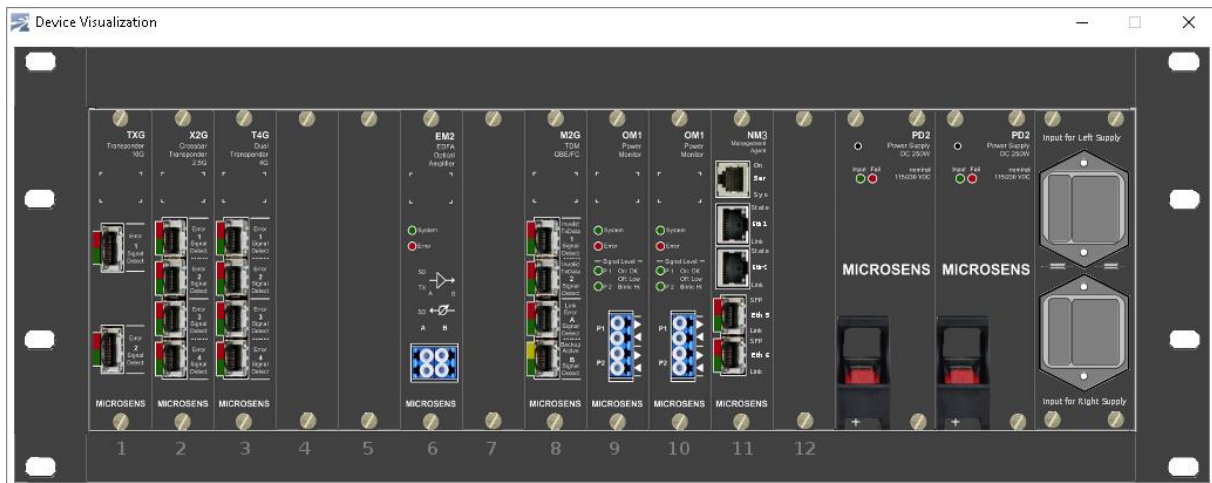


Figure 65: NMP Professional - Tabbed Data Panel - Device Visualisation (MSP 1000)

Note:

These settings are not available for all device types.

4.7.4 Services

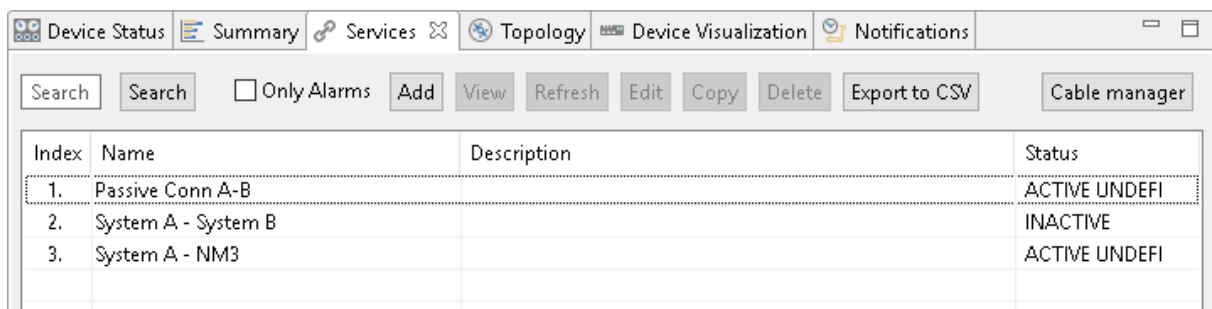


Figure 66: NMP Professional - Tabbed Data Panel - Services

The "Services" dialogue 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 the section "Using Services" on page 101.

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

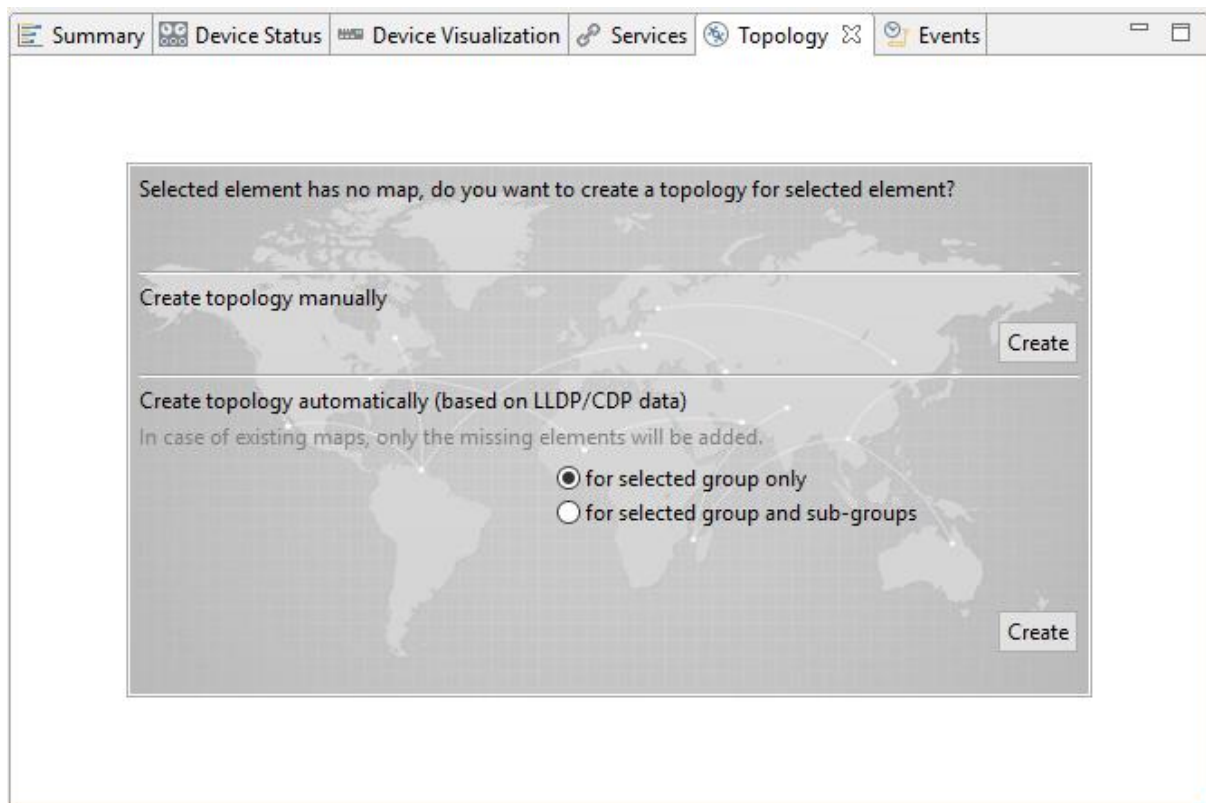


Figure 67: NMP Professional - Tabbed Data Panel - Topology

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 page 108.

4.7.6 Notifications

The notifications window provides information of all the current operations and the messages from monitored devices.

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...)
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...)

Figure 68: NMP Professional - 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 "Show filter" in the middle right hand pane of the dialogue.

For more information about working with events please refer to the section "Managing Notifications" on page 119.

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 clicking on a device in the device tree list or in the "Summary" tab of the tabbed data panel. It offers various features.

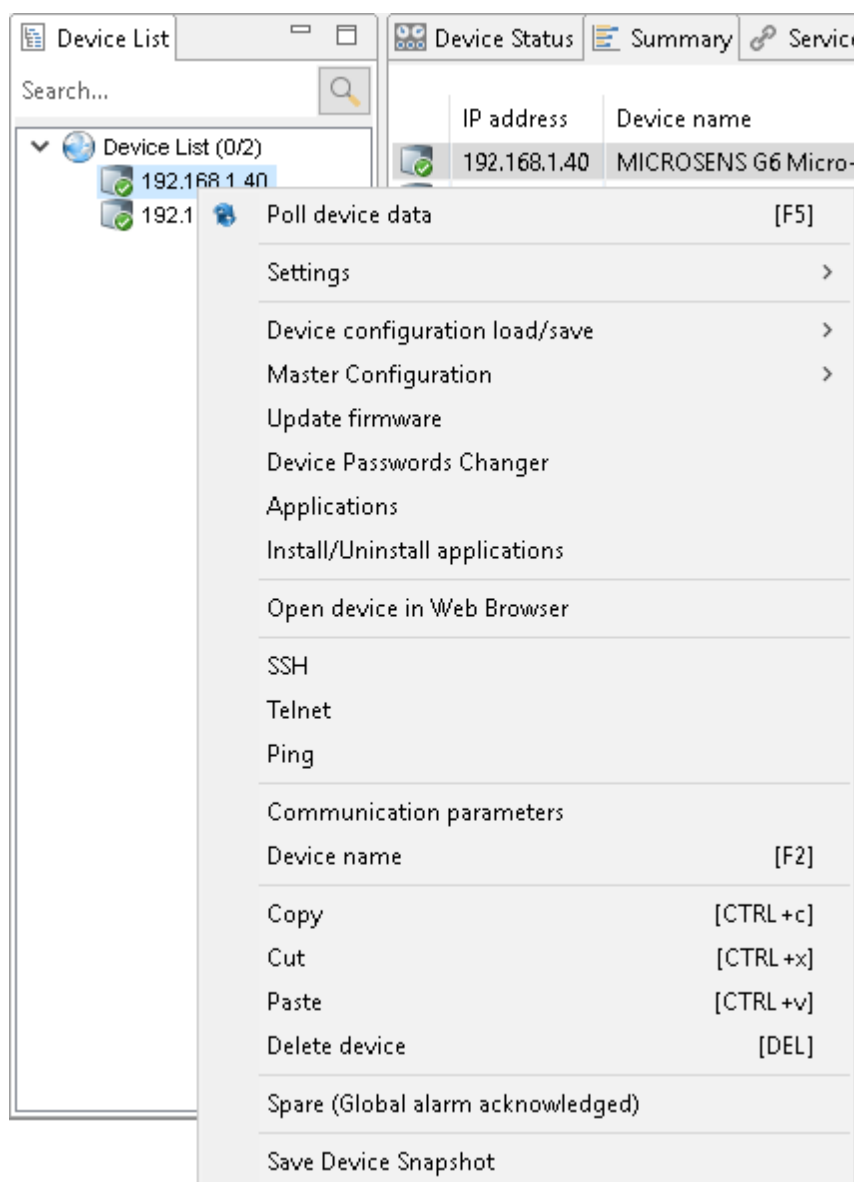


Figure 69: NMP Professional - Device Context Menu

Note:

For further information about device configuration via the context menu please refer to the section "Device Configuration in General" on page 84.

4.8.1.1 Poll Device Data (Shortcut: F5)

Use this feature to poll information about the selected device. Please refer to section "Poll selected" page 28 for more information.

4.8.1.2 Settings (Shortcut: None)

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

4.8.1.3 Device Configuration Load/Save (Shortcut: None)

These options allow loading/saving the current device configuration from/to a configuration file. For more information please refer to the section "Device Configuration via Configuration Files" on page 85.

4.8.1.4 Master Configuration (Shortcut: None)

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 the sections "Master Configuration of MICROSENS G6 Devices" on page 87 or "Master Configuration of MICROSENS G5 and older devices" on page 91.

4.8.1.5 Update Firmware (Shortcut: None)

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 page 94.

4.8.1.6 Device Passwords Changer**(Shortcut: None)**

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 70: NMP Professional - Device Context Menu - Device Password Changer

For more information on usage please refer to the "Device Password Changer" tool description on page 30.

Note:

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

4.8.1.7 Applications**(Shortcut: None)**

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 "Managing Applications on G6 Devices" on page 97.

4.8.1.8 Install/Uninstall Applications**(Shortcut: None)**

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 "Managing Applications on G6 Devices" on page 97.

4.8.1.9 Open Device in Web Browser (Shortcut: None)

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!

4.8.1.10 SSH (Shortcut: None)

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

4.8.1.11 Telnet (Shortcut: None)

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

4.8.1.12 Ping (Shortcut: None)

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

4.8.1.13 Communication Parameters (Shortcut: None)

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

A detailed description of the parameters can be found in section "Default New Device Settings" on page 31.

4.8.1.14 Device Name (Shortcut: 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.

4.8.1.15 Copy (Shortcut: 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.

4.8.1.16 Cut (Shortcut: Ctrl + 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.

4.8.1.17 Paste**(Shortcut: Ctrl + P)**

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.

4.8.1.18 Delete Device**(Shortcut: 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.

4.8.1.19 Show on the Map**(Shortcut: None)**

The selected device will be highlighted in the "Topology Manager" map (see page 68). The map containing the selected device will be automatically opened.

Note:

The "Topology Manager" is supported by NMP Professional.

4.8.1.20 Spare (Global Alarm Acknowledged)**(Shortcut: None)**

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 "Event" tab. Additionally, a device with a confirmed alarm will not be shown in the "Alarm list" group.

4.8.1.21 Save device snapshot**(Shortcut: None)****Note:**

This feature is exclusively available for MICROSENS G6 and G5 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.

4.8.2 Group Context Menu

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

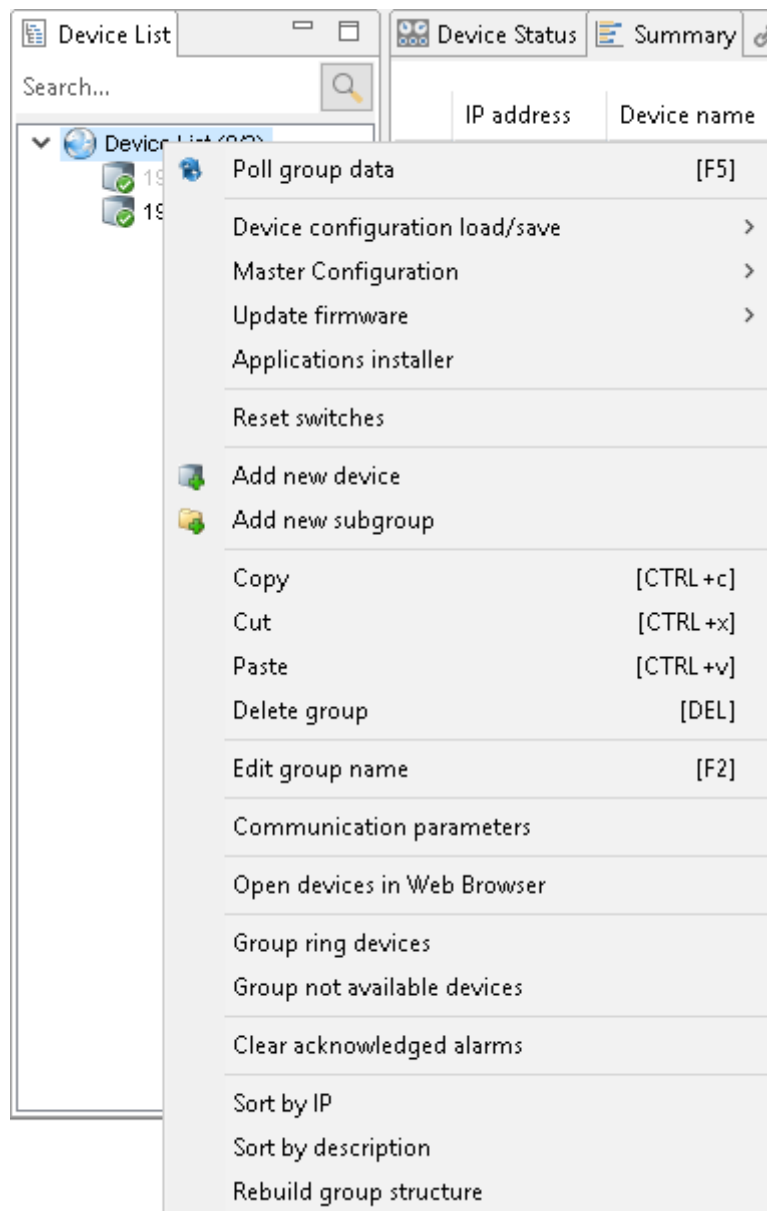


Figure 71: NMP Professional - Group Context Menu

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 subgroup) and not on just one respective device.

4.8.2.1 Poll Group Data (Shortcut: F5)

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

For more information please refer to section "Poll all devices" on page 28.

4.8.2.2 Device Configuration Load/Save (Shortcut: None)

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 the section "Device Configuration via Configuration Files" on page 85.

4.8.2.3 Master Configuration (Shortcut: None)

This group context menu item is available for MICROSENS G6 devices exclusively.

For more information please refer to the section "Using a Master Configuration" on page 87.

4.8.2.4 Update Firmware (Shortcut: None)

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 6 switches -> Micro/Desktop/Industrial/NM3
- Generation 5/4/3 switches -> Micro/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 the section "Updating the Firmware" on page 94.

4.8.2.5 Applications installer (Shortcut: None)

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

For more information how to leverage this feature please refer to page 100.

4.8.2.6 Reset Switches (Shortcut: None)

This feature triggers a "restart" of all switches available in the selected group.

4.8.2.7 Add New Device (Shortcut: None)

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 "Add new device" on page 25.

4.8.2.8 Add New Subgroup (Shortcut: None)

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

4.8.2.9 Copy (Shortcut: 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.

4.8.2.10 Cut (Shortcut: Ctrl+X)

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

4.8.2.11 Paste (Shortcut: Ctrl+V)

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

4.8.2.12 Delete Group (Shortcut: DEL)

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

4.8.2.13 Edit Group Name (Shortcut: F2)

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

4.8.2.14 Communication Parameters (Shortcut: None)

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 "Default New Device Settings" on page 31.

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.

4.8.2.15 Open Devices in Web Browser (Shortcut: None)

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:

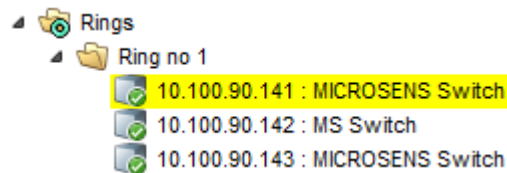
For displaying the Web GUI of the specific MICROSENS G6 device correctly we recommend the use of one of the following browsers:

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

Microsoft Internet Explorer or Microsoft Edge are not supported!


4.8.2.16 Group Ring Devices**(Shortcut: None)**

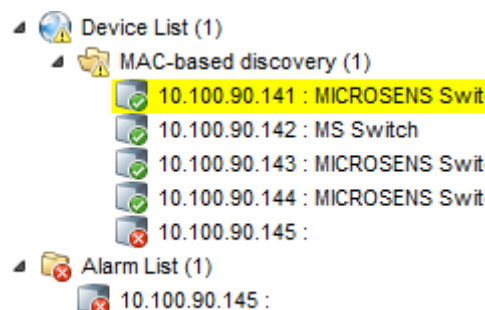
This feature automatically groups all ring switches in the device list. A new group is created in the device list. This contains a subgroup named "Ring no xx" for each ring. Switches with enabled ring support are copied to the corresponding group. The ring master is highlighted with yellow background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

**Figure 72: NMP Professional - Device List Tree View - Ring Device Group**

For more information please refer to the section "Managing Industrial Ring Errors" on page 125.

4.8.2.17 Group Not Available Devices**(Shortcut: None)**

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".

**Figure 73: NMP Professional - Device List Tree View - Alarm List****4.8.2.18 Clear Acknowledged Alarms****(Shortcut: None)**

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

For more information please refer to the section "Spare (Global Alarm Acknowledged)" on page 76.

4.8.2.19 Sort By IP**(Shortcut: None)**

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

4.8.2.20 Sort By Description**(Shortcut: None)**

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

4.8.2.21 Rebuild Group Structure**(Shortcut: None)**

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:

- 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 Working with NMP Professional

This chapter describes how to use NMP Professional. For further information about features and GUI elements please refer to the chapter "NMP Professional: Getting started" on page 20.

5.1 Adding New Devices with Device Auto Discovery

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
MS652119PM	287706	00-60-A7-05-21-14	disabled	10.100.90.103	255.255.255.0	10.100.90.3	MICROSENS G6 Swi	Send		<input checked="" type="checkbox"/>
MS652119PM	00488172	00-60-A7-06-65-02	disabled	10.100.90.102	255.255.255.0	10.100.90.3	MICROSENS G6 Swi	Send		<input type="checkbox"/>
MS440209M-G6	00000252	00-60-A7-00-00-FC	disabled	10.100.90.132	255.255.0.0	10.100.90.3	MICROSENS G6 Swi	Send		<input type="checkbox"/>
MS425523M	00463456	00-60-A7-06-47-1D	disabled	10.100.90.238	255.255.255.0	10.100.90.3	MICROSENS Optica	Send		<input type="checkbox"/>

Discovered devices: 6, new devices: 4

Filter: new devices: ☐ Full-text search: ☐ Case sensitive ☒ starts with ☐ contains

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

Configuration file: not selected...

Figure 74: NMP Professional - Device Auto Discovery

Note:

If no device is detected, the auto discovery dialogue (Figure 74) 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".

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.

Address filter

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

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.

5.2 Device Configuration in General

The configuration of the respective device can be accessed via the device context menu (see page 72) and for some device types in the tabbed data panel on the tab "Device Status" (see page 67).

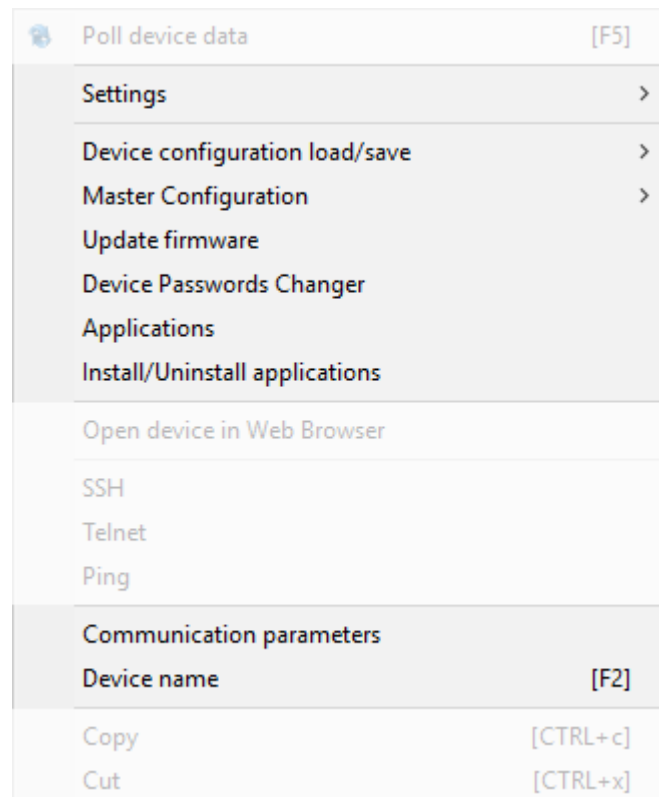


Figure 75: NMP Professional - Device Context Menu - Device Configuration

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** (see page 85)
- **Master configuration** (see page 87)
- **Update firmware** (see page 94)
- **Device passwords changer** (see page 74)
- **Applications** (see page 97)
- **Install/uninstall applications** (see page 97)
- **Communication parameters** (see page 31)

- **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.

5.3 Device Configuration via Configuration Files

It is possible to save a device's configuration into a 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:

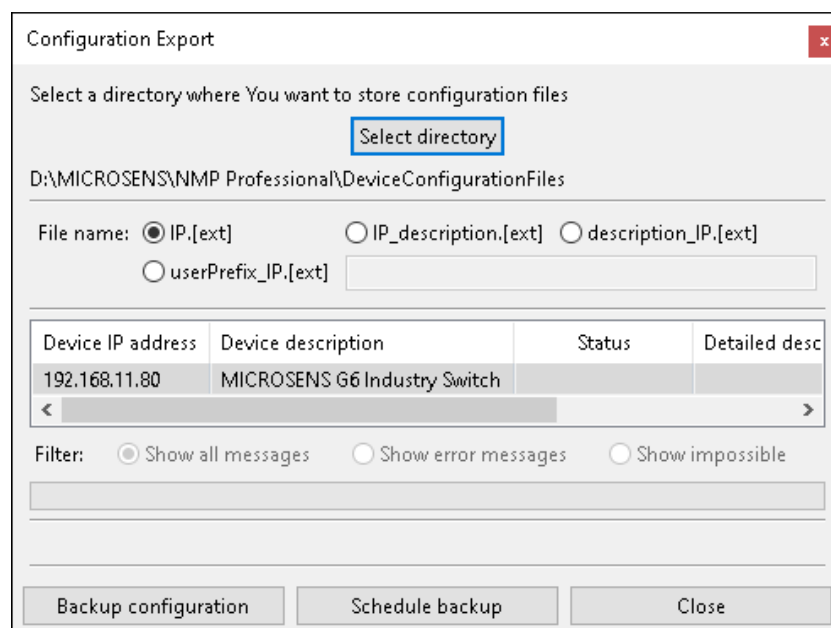


Figure 76: NMP Professional - Device Context Menu - Configuration Export

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]**,

where **IP** is substituted by the IP address of the device and **userPrefix** is a 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.

To configure a regular backup an option to schedule the backup task is available by clicking the button "Schedule backup".

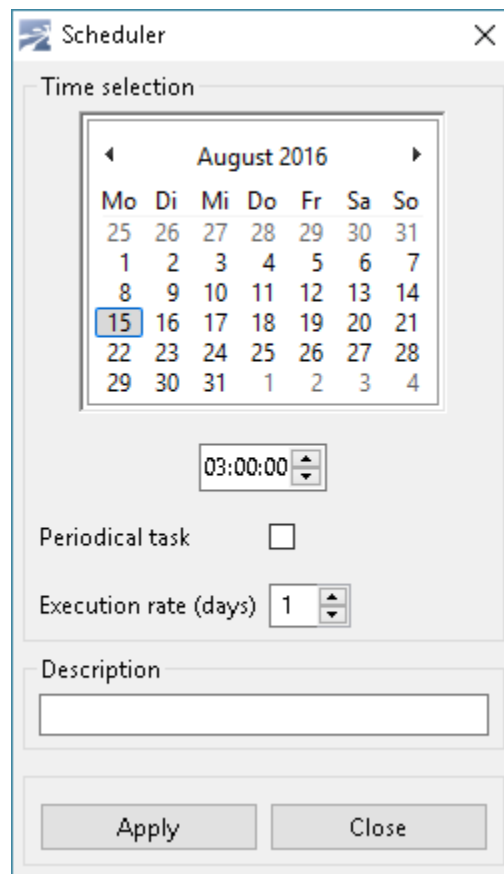


Figure 77: NMP Professional - Device Context Menu - Configuration Export - Scheduler

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 page 48).

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

Configuration will be loaded for all listed devices from previously saved backups, where available

Configuration ID

☐ All

For ProfiLine Industrial and Micro Switches only

☐ IP

☐ Port settings

☐ Device settings (User information, SFP, Ring)

☐ PoE

☐ QoS

☐ VLAN

☐ SNMP

☐ Port Access Control

☐ RADIUS

☐ Syslog/Logging/Events

☐ STP

☐ Multicast Snooping

☐ User interfaces (Access, CLI, Web, Files)

☐ CDP/LLDP

☐ RTC

☐ LACP

☐ MSP1000

Device IP address	Device description	Status	Detailed description
192.168.11.40	MICROSENS G6 Micro-Switch		
192.168.11.80	MICROSENS G6 Industry Switch		

Filter: ☒ Show all messages ☐ Show error messages ☐ Show impossible

Load and apply

Close

Figure 78: NMP Professional - 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.

5.4 Using a Master Configuration

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 and prior devices.

5.4.1 Master Configuration of MICROSENS G6 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 Micro Switch, Industrial ProfiLine devices and some desktop switches.

Note:

For master configuration of G5 and older versions please refer to the respective description on page 90.

The master configuration file for MICROSENS G6 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

This is how these context sub-menu items work:

5.4.1.1 Apply CLI Script**(Shortcut: None)**

After selecting the respective CLI script in the opening dialogue, the following dialogue appears:

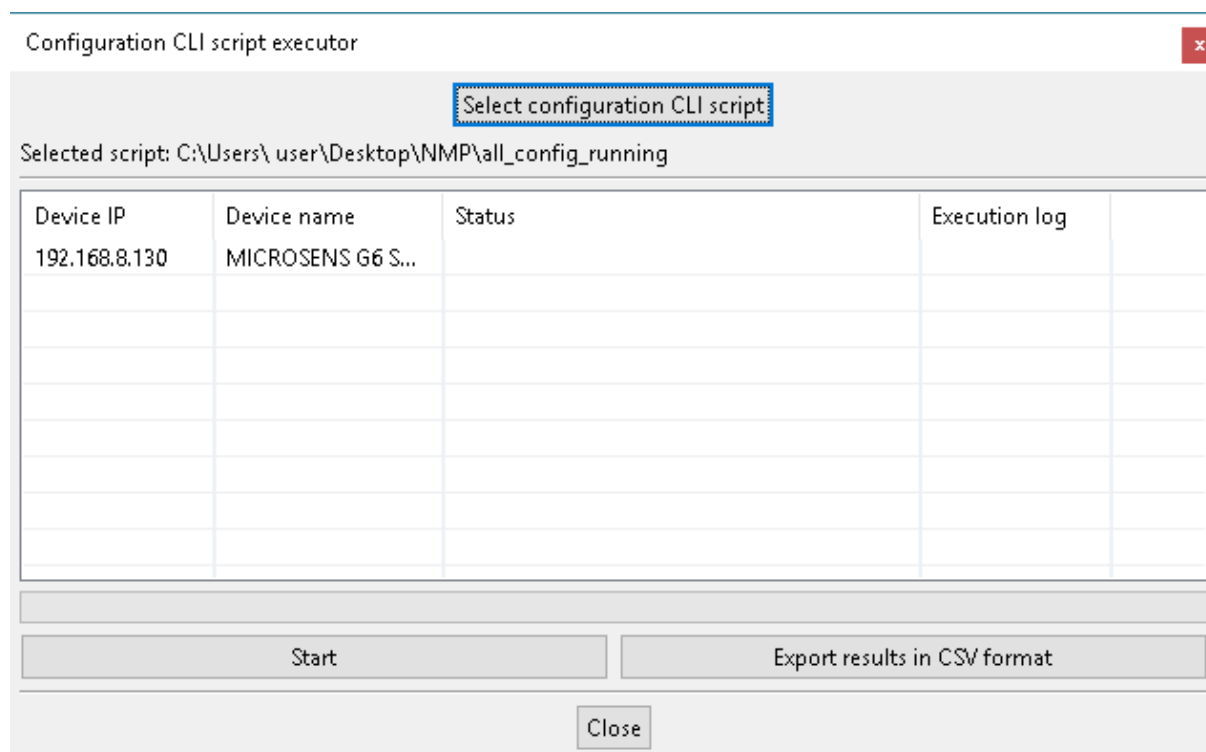


Figure 79: NMP Professional - Device Context Menu - Master Configuration - Apply CLI Script

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.

5.4.1.2 Generate and Download CLI Script (Shortcut: None)

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

Generate CLI scripts

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

Delete selected script Execute selected script Copy selected script to file

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 Save script as (on device) Save script as (on local disk)

Upload / Download

Server: Protocol: TFTP

User name: Password:

Upload selected script Script to download: Download script

Close

Figure 80: NMP Professional - 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.

5.4.1.3 Edit CLI Script File (Shortcut: None)

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.

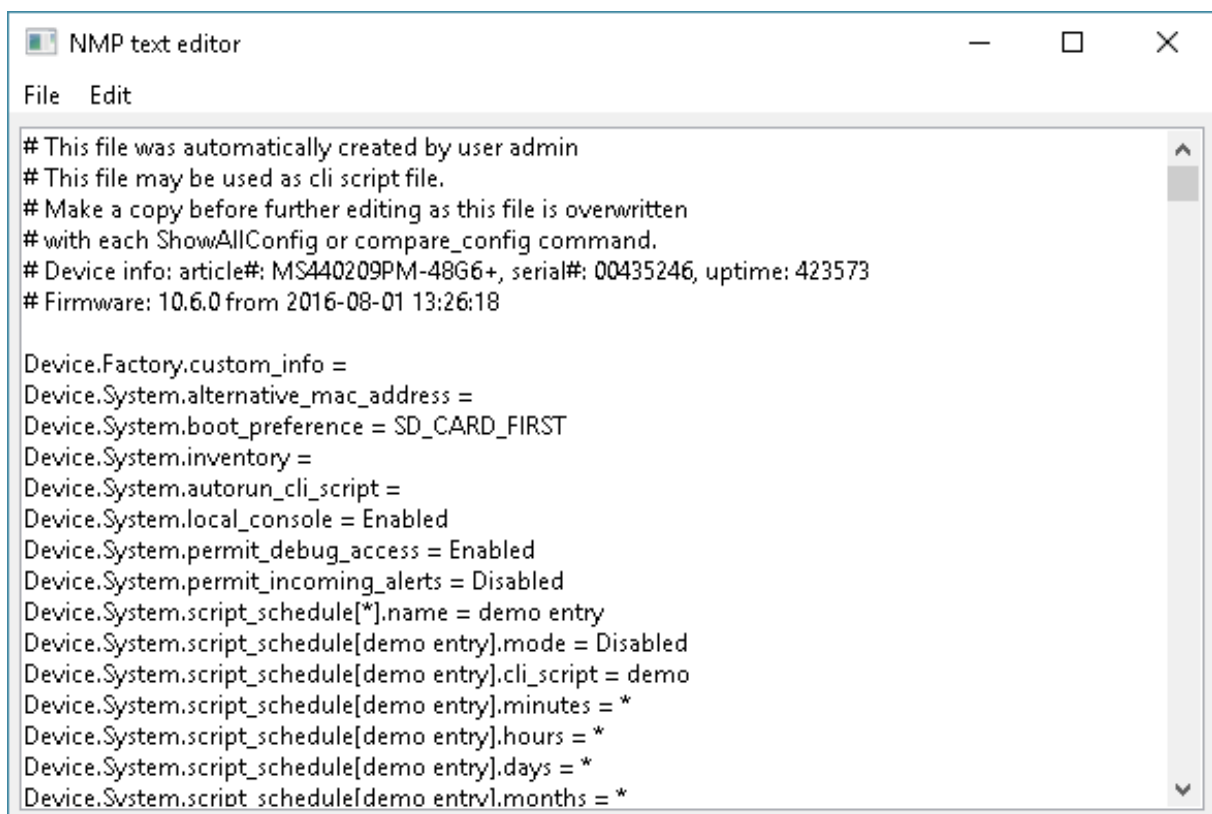


Figure 81: NMP Professional - Device Context Menu - Master Configuration - NMP Text Editor

5.4.2 Master Configuration of MICROSENS G5 and older devices

To create a master configuration select the specific switch in the NMP device tree and choose **Master Configuration** from the device context menu. The following dialogue appears:

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:

Save Load Apply all changes Close

Figure 82: NMP Professional - 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]: ☐ change

Enable extended voltage range ☒ ☐ change

Switch supply power [W]:

Available PoE power [W]:

PoE information

Port no.	PoE Mode	Max. PSE power [W]	Max. PD class
<input type="checkbox"/> select row	<input type="checkbox"/> change	<input type="checkbox"/> change	<input type="checkbox"/> change
1 [TP]	disabled ▾	<input type="text" value="15.4"/>	0 (max. 15.4 W) ▾
<input type="checkbox"/> select row	<input type="checkbox"/> change	<input type="checkbox"/> change	<input type="checkbox"/> change
2 [TP]	disabled ▾	<input type="text" value="15.4"/>	0 (max. 15.4 W) ▾
<input type="checkbox"/> select row	<input type="checkbox"/> change	<input type="checkbox"/> change	<input type="checkbox"/> change
3 [TP]	disabled ▾	<input type="text" value="15.4"/>	0 (max. 15.4 W) ▾
<input type="checkbox"/> select row	<input type="checkbox"/> change	<input type="checkbox"/> change	<input type="checkbox"/> change
4 [TP]	disabled ▾	<input type="text" value="15.4"/>	0 (max. 15.4 W) ▾

Figure 83: NMP Professional - 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).

☐ select all

Figure 84: NMP Professional - 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.

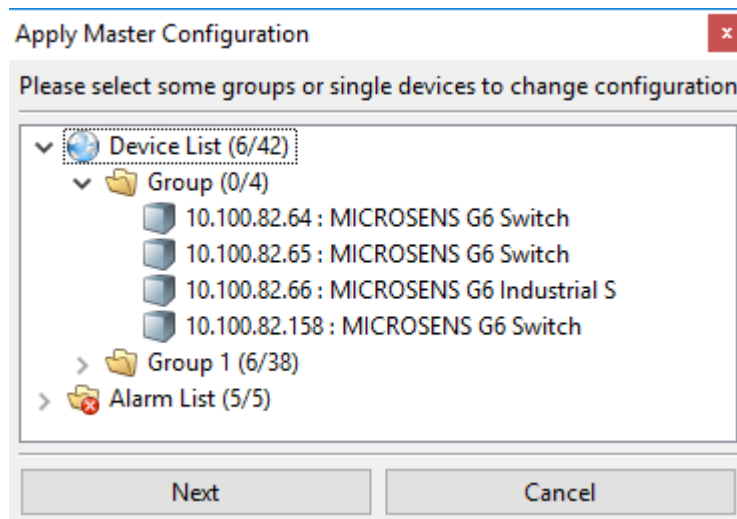


Figure 85: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Select Group/Device

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.

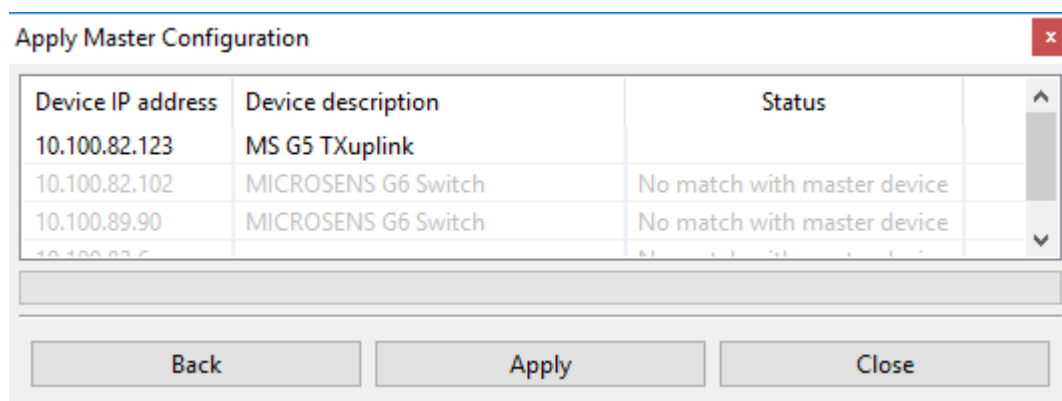


Figure 86: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Apply to Devices

5.5 Updating the Firmware

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) / Industrial Switches (G6).

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:



Figure 87: NMP Professional - 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).

Figure 88: NMP Professional - Device Context Menu - Update Firmware - Select FTP Server

IP address	File transfer	Old version	New versi...	Client message	Update status	Log
10.100.82.66						Log

Figure 89: NMP Professional - Device Context Menu - Update Firmware - Select File

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.

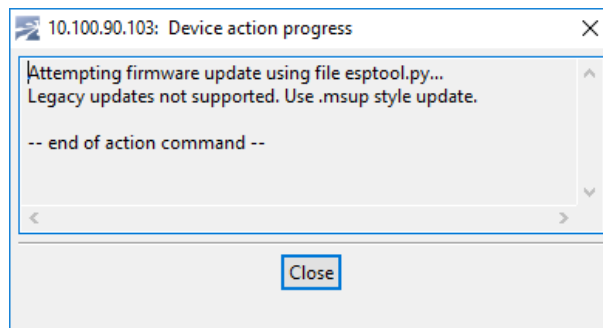


Figure 90: NMP Professional - Device Context Menu - Update Firmware - Progress

To configure a regular firmware update an option to schedule the update task is available by clicking the button "Schedule update".

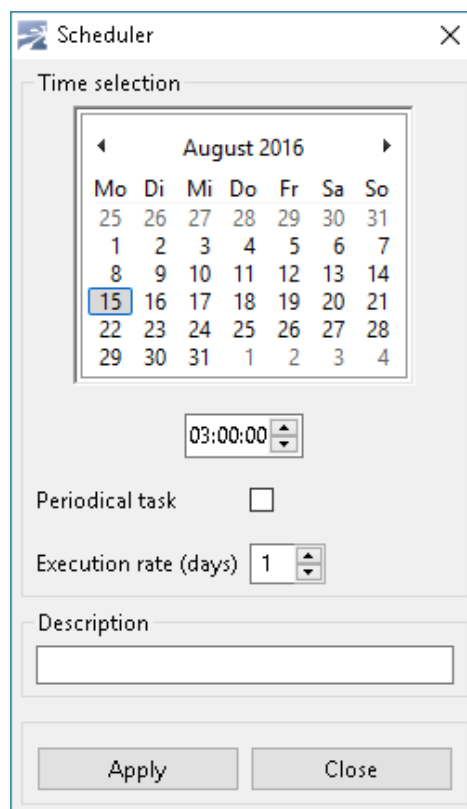


Figure 91: NMP Professional - Device Context Menu - Update Firmware - Scheduler

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 page 48).

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 89). 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.

5.6 Managing Applications on G6 Devices

5.6.1 Application Basics

With NMP it is possible to manage applications on MICROSENS G6 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 Server's own 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.

Note:

The management of applications is exclusively possible on MICROSENS G6 devices.

5.6.2 Device Context Menu

Manage applications via the context menu of the respective device (for more information about using the device context menu see page 72).

5.6.2.1 Applications

(Shortcut: None)

This feature lists in a sub menu all the applications currently installed on the device.

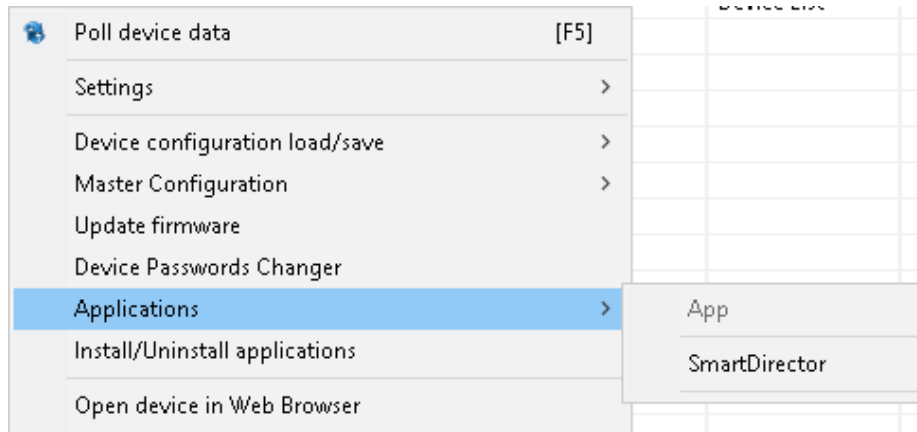


Figure 92: NMP Professional - Device Context Menu - Applications (Example)

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. The application “Smart Engine” used in the example screenshot (see Figure 92) has the following structure:

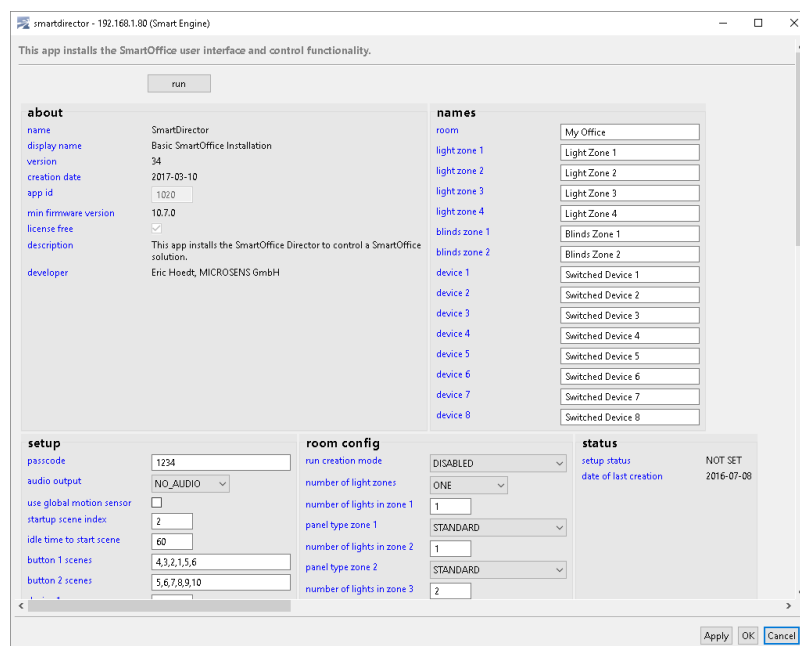


Figure 93: NMP Professional - Application Management - Configuration Example

5.6.2.2 Install/Uninstall Applications (Shortcut: None)

This feature lists all applications currently available and installed on the switch.

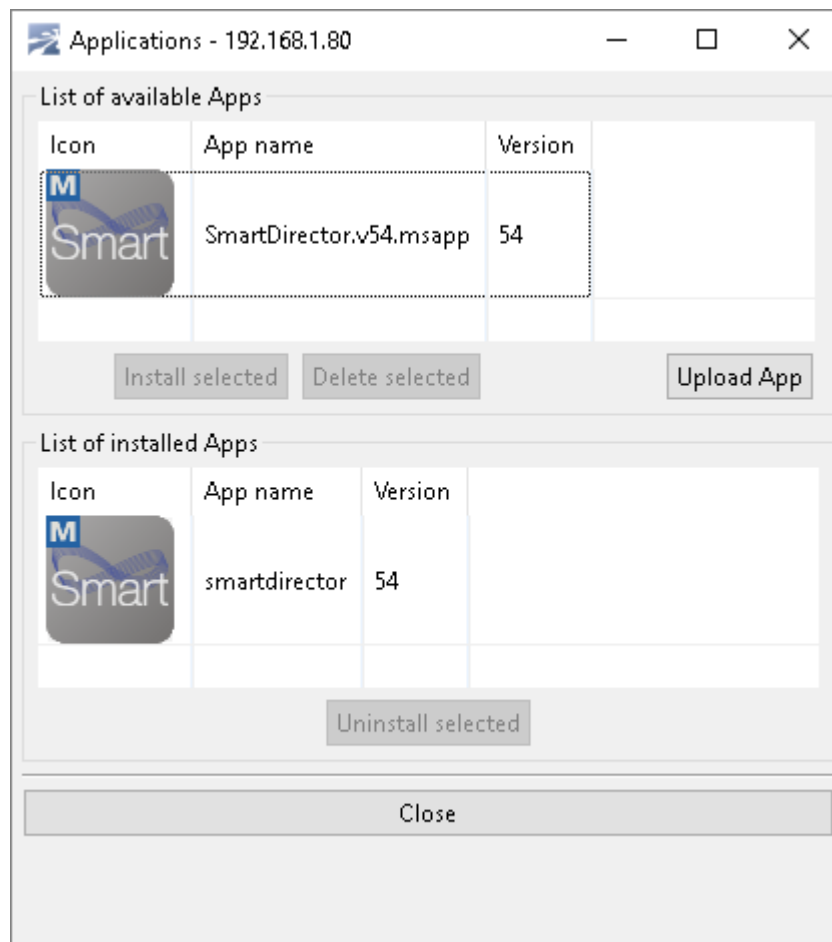


Figure 94: NMP Professional - Application Management - Available Applications

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.

5.6.3 Group Context Menu

In the group context menu it is possible to install apps on multiple grouped devices at once.

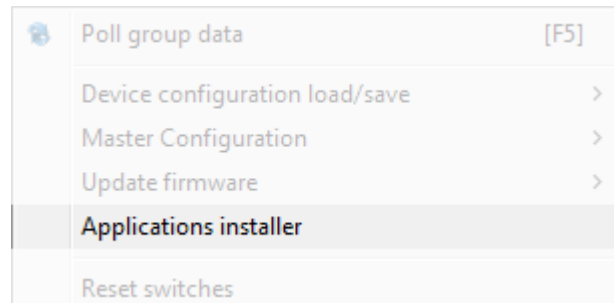


Figure 95: NMP Professional - Group Context Menu - Applications Installer

5.6.3.1 Applications Installer (Shortcut: None)

After clicking 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:

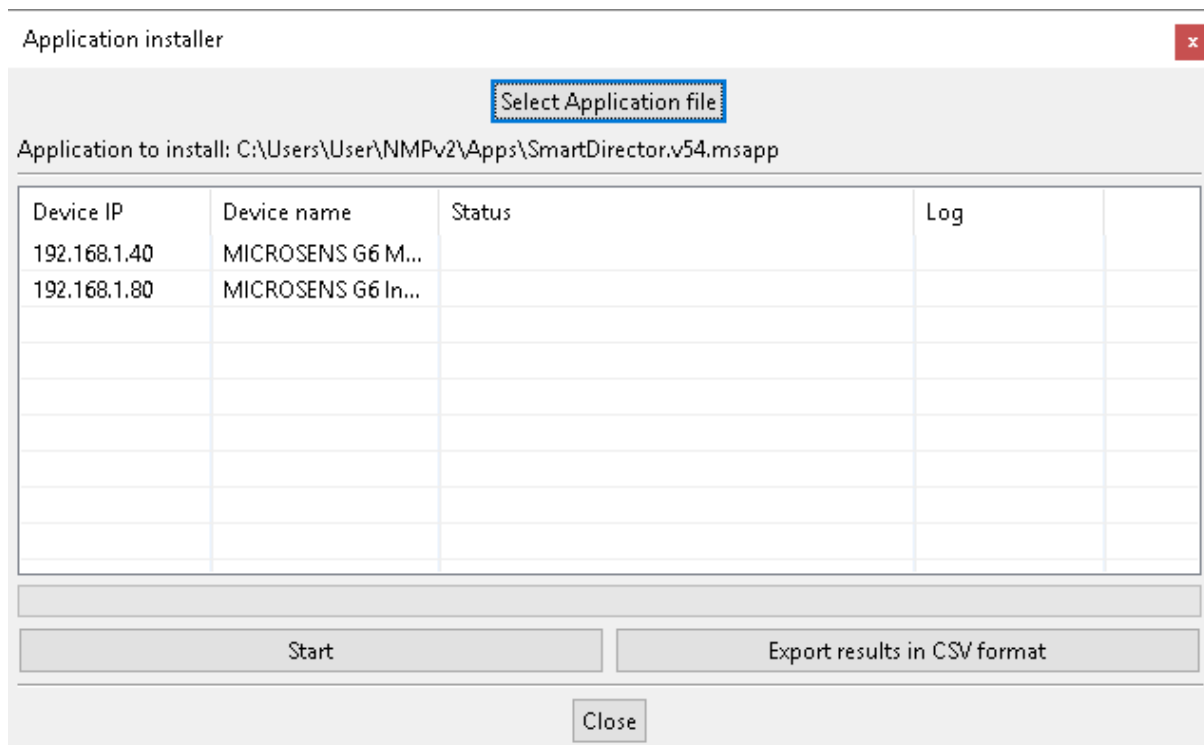


Figure 96: NMP Professional - Group Context Menu - Applications Installer - Select Apps

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. When the procedure will be finished, the results from the table can be exported in form of a **.csv** file.

5.7 Using Services

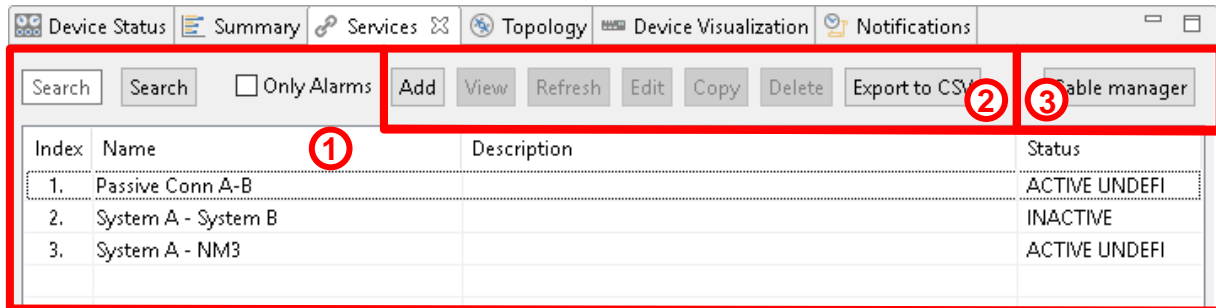


Figure 97: NMP Professional - Tabbed Data Panel - Services - Details

The tab "Services" offers three different sections:

- 1 – Service table
- 2 – Service manager
- 3 – Cable manager

5.7.1 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 (for configuration of log entries see page 38).

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.

5.7.2 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:

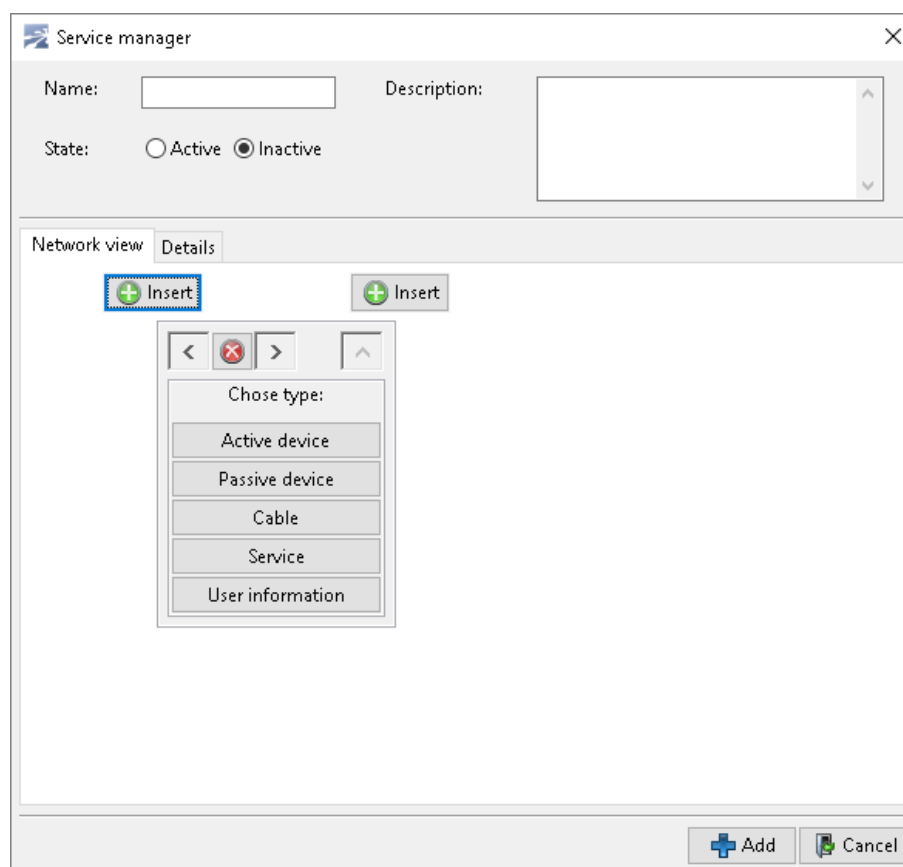


Figure 98: NMP Professional - Tabbed Data Panel - Services - Service Manager - Network View

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 page 106).
- **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).

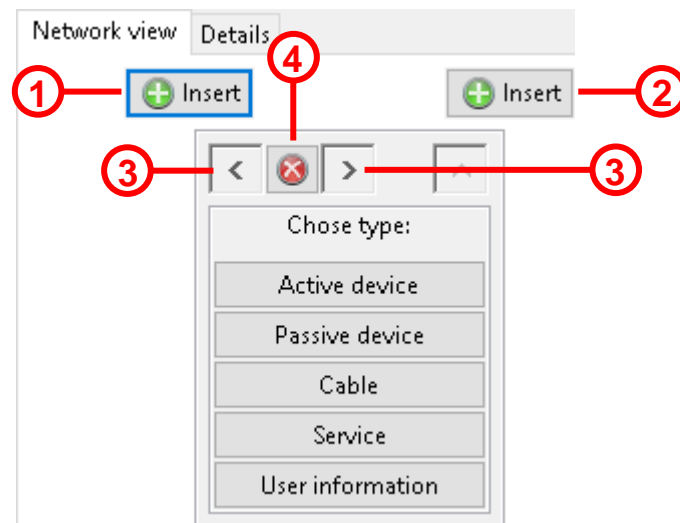


Figure 99: NMP Professional - Tabbed Data Panel - Services - Service Manager - Element

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).

The screenshot shows a window titled "Service manager" with a close button (X) in the top right corner. The window is divided into two main sections. The top section contains fields for "Name:" (a text box), "Description:" (a large text area with a scrollbar), and "State:" with two radio buttons: "Active" and "Inactive" (the "Inactive" button is selected). Below this is a tabbed interface with two tabs: "Network view" and "Details" (the "Details" tab is selected). The "Details" tab contains several input fields: "Customer:" (text box), "Class of services:" (text box), "Contact name:" (text box), "Address/location:" (large text area with a scrollbar), "Telephone:" (text box), "Fax:" (text box), "Email:" (text box), and "User field:" (large text area with a scrollbar). At the bottom right of the window are two buttons: "Add" (with a blue plus icon) and "Cancel" (with a green minus icon).

Figure 100: NMP Professional - 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.

5.7.3 Cable Manager

A click on the button "Cable Manager" opens the cable manager dialogue.

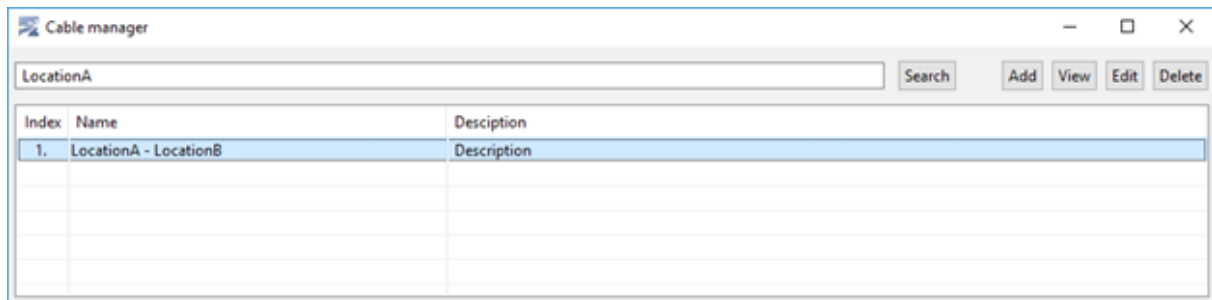


Figure 101: NMP Professional - Tabbed Data Panel - Services - Cable Manager

You can define "virtual" fibre cables and configure descriptions and parameters. These definitions can be added as a part of a service (see page 101).

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.

Cable creator

Name: Description:

Type: ☐ Simplex ☒ Duplex

Patch loss: dB

Link length(km):

Fiber attenuation:

$\lambda=1310\text{nm}$ $\lambda=1550\text{nm}$

dB dB

dB dB

Patch loss: dB

Figure 102: NMP Professional - Tabbed Data Panel - Services - Cable Manager - Cable Creator

Enter the cable 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.

5.8 Managing Topologies

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.

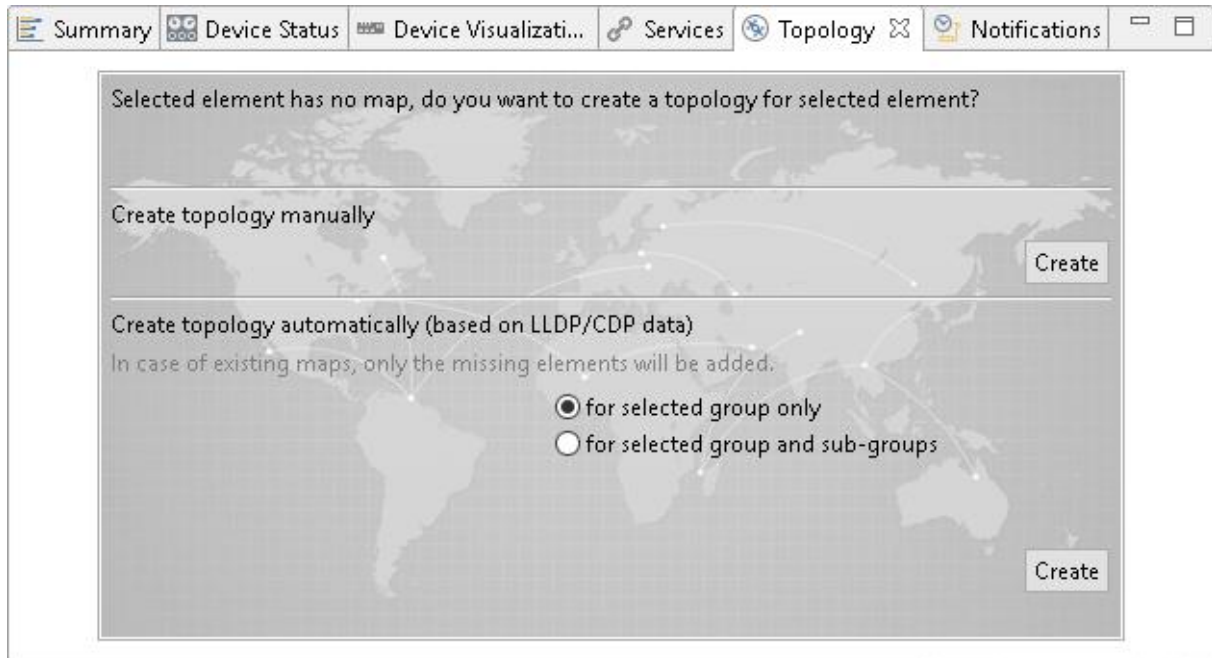


Figure 103: NMP Professional - Tabbed Data Panel - Topology - Standard Dialogue

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 group 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.

5.8.1 Menu Icons








To manage topologies the menu icons at the top of the topology area have the following functions:

Icon	Meaning
	<p>Update topology</p> <p>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.</p> <p>This works for both wired and "Optical Transport Networks" (OTN). For that purpose, NMP checks the LLDP/CDP status of each device.</p>
	<p>Load map background image</p> <p>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.</p>
	<p>Remove map background image</p> <p>Click this icon to remove the topology's background image. Assigned devices are not affected.</p>
	<p>Hide/Show map background image</p> <p>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.</p>
	<p>Change map background image colour</p> <p>Use this function to change the colours of the map background image. Each click toggles between grey scale and original image colours.</p>
	<p>Hide/show device labels</p> <p>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.</p>
	<p>Zoom in</p> <p>Click this icon to zoom into the topology map.</p> <p>Note: It is possible to use the mouse wheel to zoom in and out.</p>


Icon	Meaning
	<p>Zoom out</p> <p>Click this icon to zoom out of the topology map.</p> <p>Note: It is possible to use the mouse wheel to zoom in and out.</p>
	<p>Zoom 1:1</p> <p>Click this icon to show the topology map in its original dimensions.</p>
	<p>Zoom fit</p> <p>Click this icon to fit the topology map into the given tab area dimensions.</p>
	<p>Print map</p> <p>Opens the print dialogue of the operating system.</p>
	<p>Save map as image file</p> <p>Opens the file save dialogue of the operating system. Chose a directory and file name to exports the map as .bmp or .png file.</p>
	<p>Delete current topology</p> <p>Click this icon to delete the complete topology of the selected subgroup. All devices and background images are affected.</p> <p>After successful deletion the standard dialogue appears.</p>
	<p>Open window with unallocated map elements</p> <p>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:</p> <p>: Move selected item to the topology</p> <p>: Move all items to the topology</p>
	<p>Open parent map</p> <p>Navigates to the topology map of the subgroup or group above the selected one.</p> <p>Note: If the parent map does not contain a topology the standard dialogue appears.</p>

5.8.2 Topology Map Elements

All devices and groups allocated on the map are represented by special icons and colour codes:

Icon	Meaning
	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.
	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.

5.8.3 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" ().

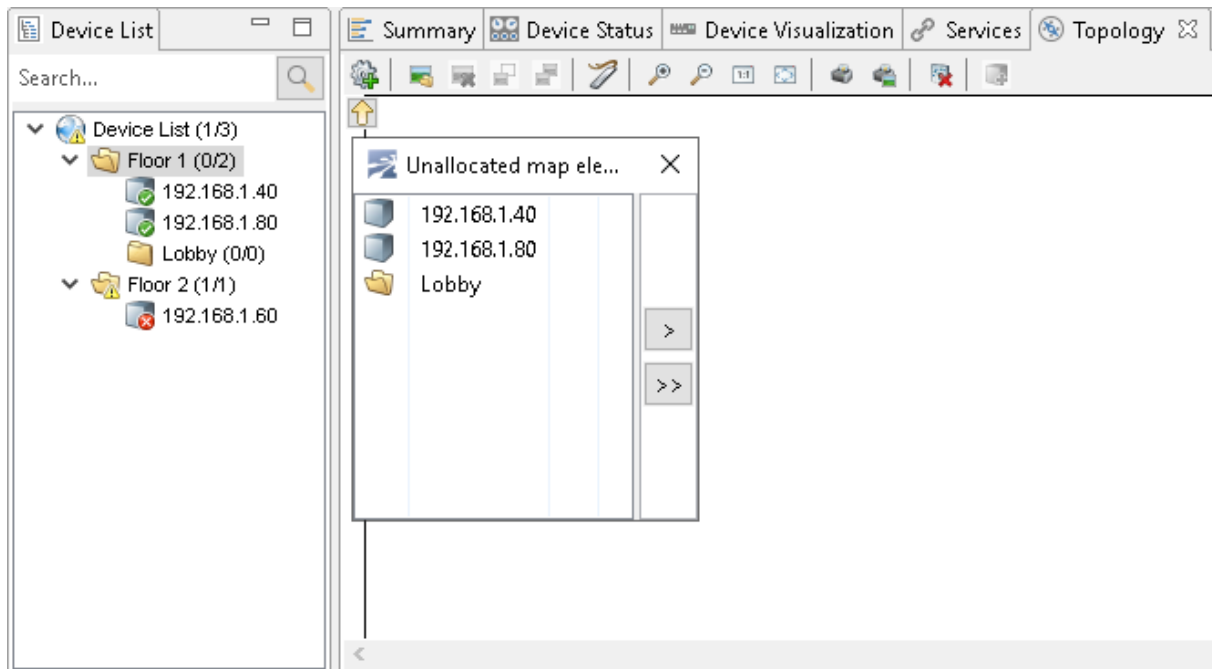


Figure 104: NMP Professional - Tabbed Data Panel - Topology - Adding Items manually

The dialogue for selecting unallocated device list elements opens (see Figure 104). 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.

5.8.4 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.

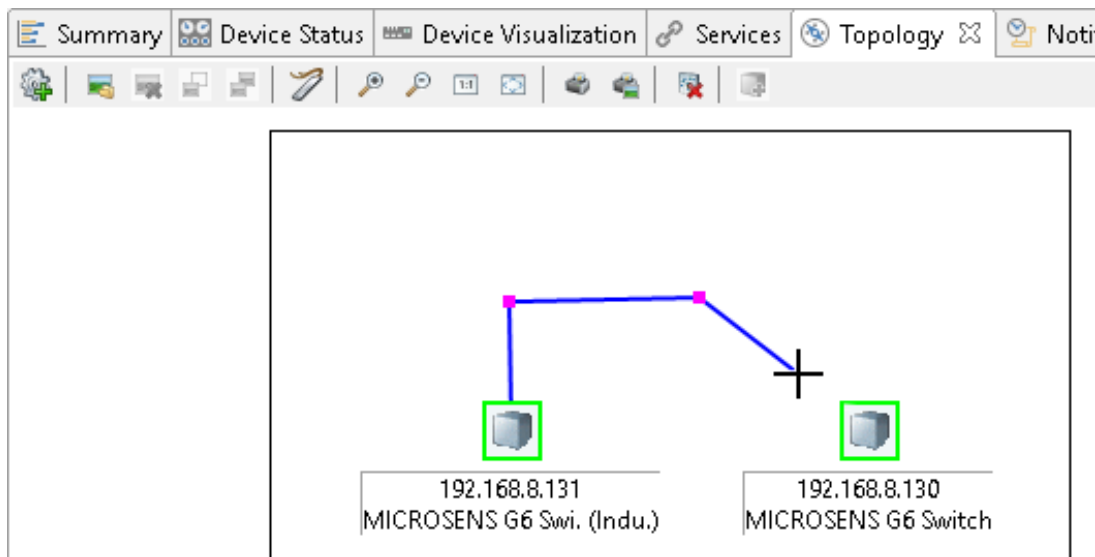


Figure 105: NMP Professional - Tabbed Data Panel - Topology - Adding Multiple Anchors

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.

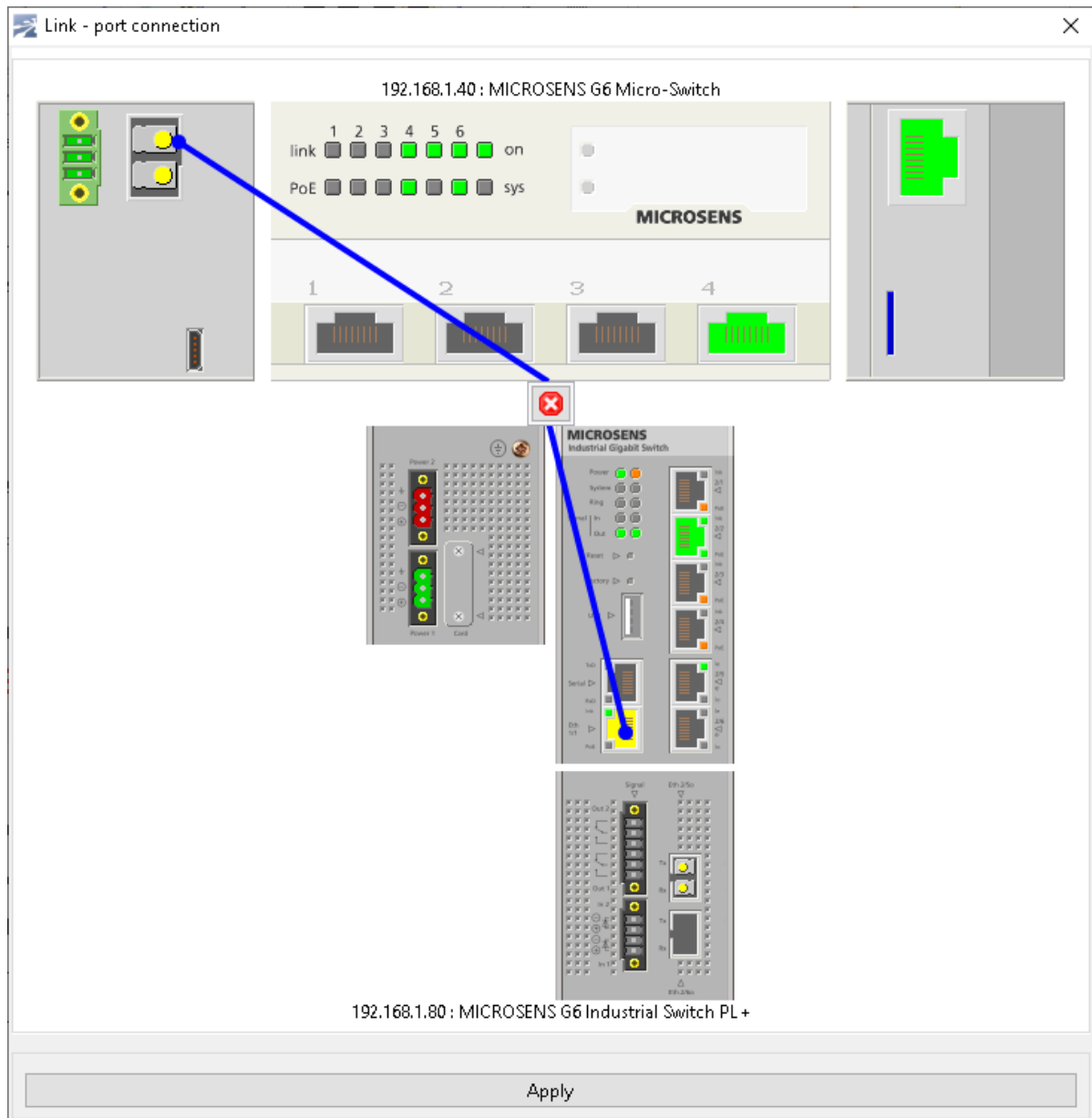

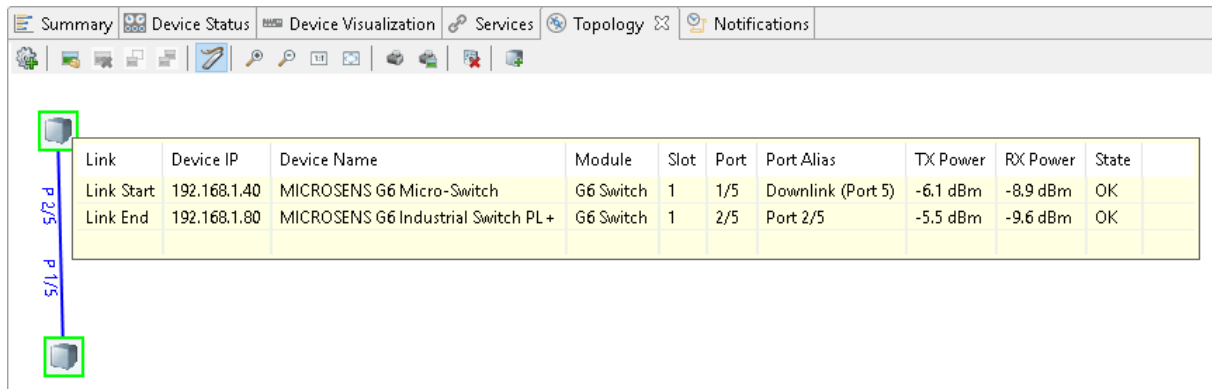


Figure 106: NMP Professional - Tabbed Data Panel - Topology - Link Port Connection

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 107: NMP Professional - 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.

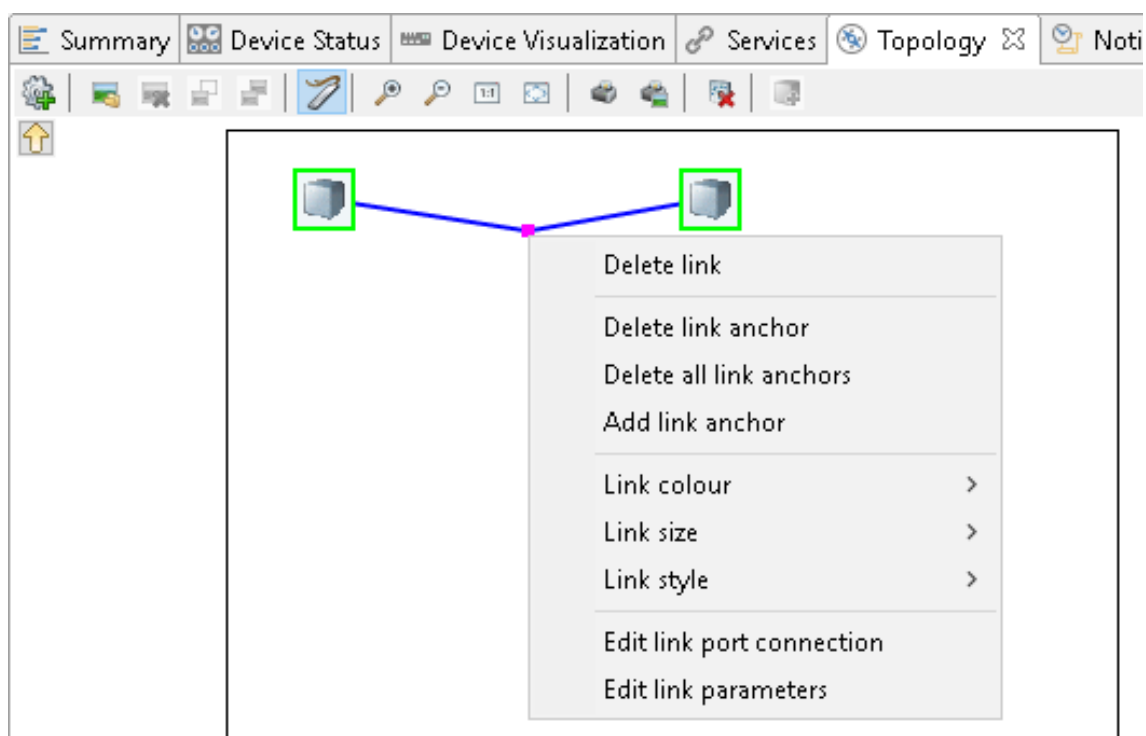
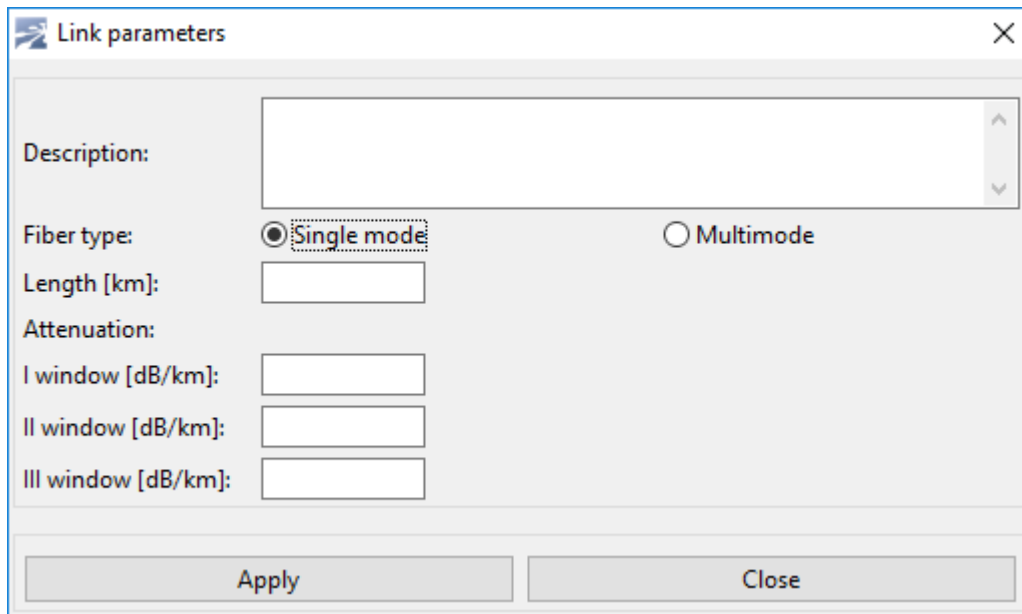


Figure 108: NMP Professional - Tabbed Data Panel - Topology - Link Anchor Context Menu

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.



The screenshot shows a 'Link parameters' dialog box. It includes a 'Description' text area, a 'Fiber type' section with 'Single mode' and 'Multimode' radio buttons, and input fields for 'Length [km]', 'Attenuation', and three optical window attenuations (I, II, III) in dB/km. 'Apply' and 'Close' buttons are at the bottom.

Figure 109: NMP Professional - Tabbed Data Panel - Topology - Link Parameters

Note:

The menu entry "Edit link port connection" opens the link port connection dialogue (see Figure 106).

Note:

Editing link settings is only possible with manually generated connections.

5.8.5 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.

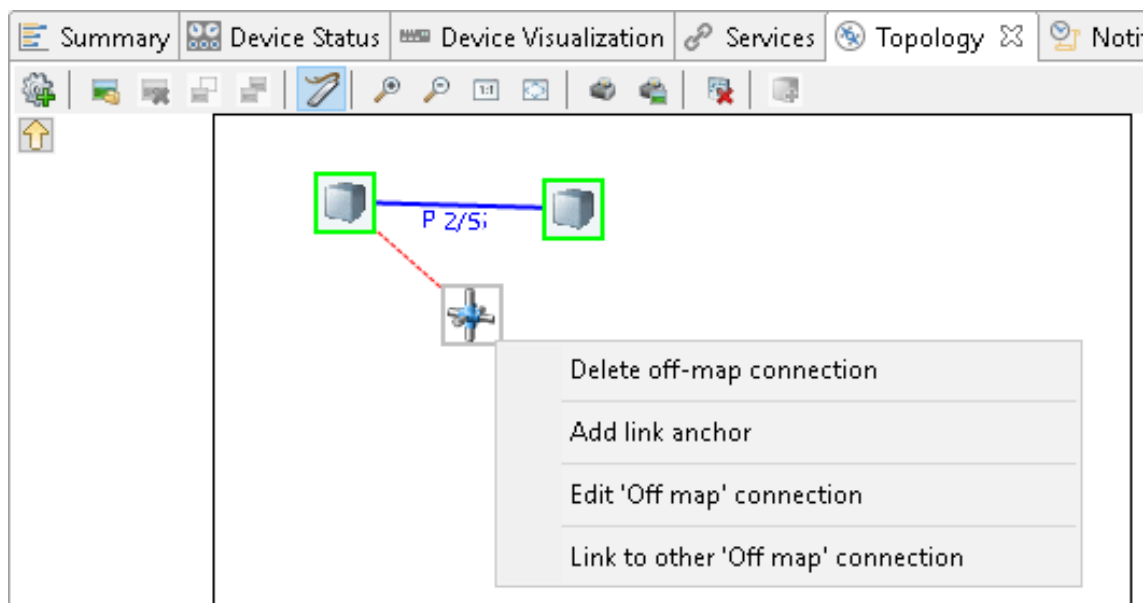


Figure 110: NMP Professional - Tabbed Data Panel - Topology - Off-Map Connections - Context Menu

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).

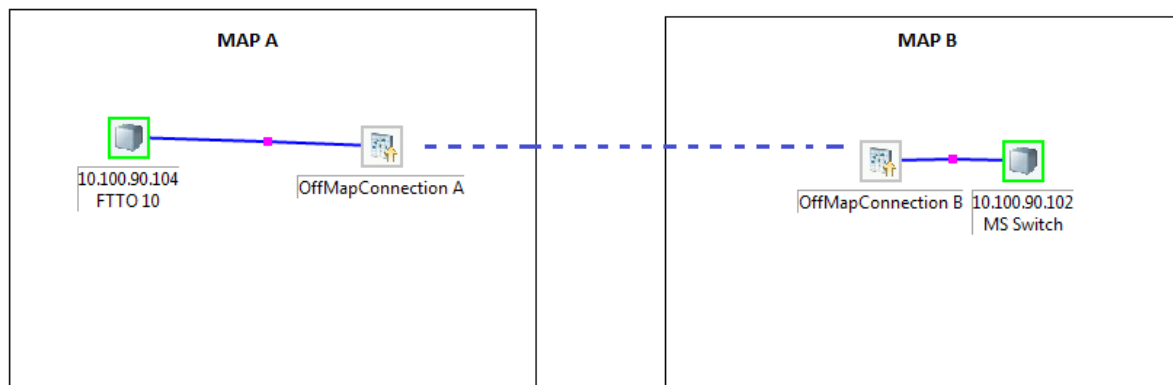


Figure 111: NMP Professional - Tabbed Data Panel - Topology - Off-Map Connections

Note:

Off-map connections can also represent third party devices not supported by NMP.

5.9 Managing Notifications

The screenshot shows the 'Notifications' tab in the NMP Professional interface. At the top, there are tabs for 'Device Status', 'Summary', 'Services', 'Topology', 'Device Visualization', and 'Notifications'. Below the tabs, a summary bar shows 'Unacknowledged events: CRITICAL/ALERT/EMERGENCY: 0 (Since 06.06.2018 16:57:31) ERROR: 4 WARNING: 0 (Since 06.06.2018 16:57:31)'. The main table displays a list of events with columns: Date, ACK (Time), Relevance, Severity, Event source, and Source ID. The table is filtered to show only 'NEGATIVE' and 'ERROR' events. Below the table, there is a filter panel with sections for 'Relevance' (POSITIVE, NEGATIVE, INFO), 'Severity' (info, notice, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY, debug), and 'Source' (SYSTEM, USER, DEVICE, SERVICE). There are also options to 'Export table (*.csv)', 'Event configuration', 'Apply filter', 'Clear filter', and 'Delete filtered ACK events'.

Date	ACK (Time)	Relevance	Severity	Event source	Source ID
06.06.2018 17:27:02	06.06.2018 17:27	INFO	info	Service	System A - Sy
06.06.2018 17:26:48	NO ACK	NEGATIVE	ERROR	Service	System A - Sy
06.06.2018 17:26:48	NO ACK	NEGATIVE	ERROR	Service	System A - Sy
06.06.2018 17:26:48	NO ACK	NEGATIVE	ERROR	Service	System A - Sy
06.06.2018 17:26:47	06.06.2018 17:26	INFO	info	Service	System A - Sy
06.06.2018 17:26:00	06.06.2018 17:26	INFO	info	Service	Passive Conn
06.06.2018 17:19:43	06.06.2018 17:19	POSITIVE	notice	Device	192.168.1.80 (
06.06.2018 17:19:33	06.06.2018 17:19	INFO	info	Device	192.168.1.40 (
06.06.2018 17:09:08	06.06.2018 17:09	INFO	info	Device	192.168.1.40 (
06.06.2018 17:08:56	06.06.2018 17:08	POSITIVE	notice	Device	192.168.1.80 (
06.06.2018 16:58:21	06.06.2018 16:58	POSITIVE	notice	Device	192.168.1.80 (
06.06.2018 16:58:03	06.06.2018 16:58	INFO	info	Device	192.168.1.40 (
06.06.2018 16:57:31	06.06.2018 16:57	INFO	info	System	System

Figure 112: NMP Professional - Tabbed Data Panel - Notifications

All NMP messages are displayed on the tab "Notifications".

Note:

To use events first enable event logging in the main menu under **Settings -> Log File/Email/Events**. For more information please refer to page 38.






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

Additionally, each NMP 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	Meaning
	DISABLED	The event will not generate a log entry (not displayed, nor logged). It is greyed out.
	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 events 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).

The screenshot shows the NMP Professional interface with the 'Device Status' tab selected. Below it, the 'Notifications' tab is active, displaying a table of unacknowledged events. The table has columns for Date, ACK (Time), Relevance, Severity, Event source, and Source ID. The events listed are all 'POSITIVE' with 'notice' severity, originating from the 'Device' source. Below the table, there are filter options for Relevance (POSITIVE, NEGATIVE, INFO), Severity (info, notice, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY, debug), and Source (SYSTEM, USER, DEVICE, SERVICE). There are also checkboxes for 'starts with' and 'equals' search methods, and buttons for 'Export table (*.csv)', 'Event configuration', 'Apply filter', 'Clear filter', and 'Delete filtered ACK events'.

Date	ACK (Time)	Relevance	Severity	Event source	Source ID
25.03.2021 12:57:11	25.03.2021 12:57	POSITIVE	notice	Device	192.168.11.80
25.03.2021 12:57:06	25.03.2021 12:57	POSITIVE	notice	Device	192.168.11.40
25.03.2021 12:46:51	25.03.2021 12:46	POSITIVE	notice	Device	192.168.11.80
25.03.2021 12:46:26	25.03.2021 12:46	POSITIVE	notice	Device	192.168.11.40
25.03.2021 12:36:02	25.03.2021 12:36	POSITIVE	notice	Device	192.168.11.80

Figure 113: NMP Professional - Tabbed Data Panel - Notification and Device Status

5.10 Events Configuration

Configure the events by selecting the button “Event configuration” from the filter section under the log table.

Event	Relevance	Severity	[Display]	Sound notification	Email notification
SYSTEM_INFO	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
SYSTEM_OK	POSITIVE	notice	notice	<input type="checkbox"/>	<input type="checkbox"/>
SYSTEM_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_SNMP_TRAP	[Mapped from SNMP TRAP Message or INFO:WARNING]			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_SYSLOG	[Mapped from SYSLOG Message]			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_RESPONSE_OK	POSITIVE	notice	notice	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_RESPONSE_ERROR	NEGATIVE	CRITICAL	CRITICAL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_ACCESS_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CONFIGURATION_SEND	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
CONFIGURATION_ACCEPTED	POSITIVE	notice	notice	<input type="checkbox"/>	<input type="checkbox"/>
CONFIGURATION_NOT_ACCEPTED	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_CONFIGURATION_BACKUP_SAVE	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_CONFIGURATION_BACKUP_DELETE	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
FIRMWARE_UPDATE_INFO	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
FIRMWARE_UPDATED	POSITIVE	notice	notice	<input type="checkbox"/>	<input type="checkbox"/>
FIRMWARE_NOT_UPDATED	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_RING_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_STATUS_INFO	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_STATUS_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SERVICE_INFO	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>
SERVICE_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE_IN_SPARE_PART_MODE	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Apply, Close

Figure 114: NMP Professional - 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 (SYSLOG, ITU) click on the button 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** (see page 38).

5.10.1 Filtering Notifications

Filter all the logged event messages by using the filter options available at the filter bar.

Figure 115: NMP Professional - Tabbed Data Panel - Notifications - Filter

Note:

If the filter section is hidden click on "Show filter" (.) on the bottom of the dialogue. To toggle the filter section, click on "Hide filter".

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 page 122).
- **Export table (*.csv):** Exports the currently filtered messages as .csv file.

5.10.2 Acknowledging Events

Events configured with the following severities have to be acknowledged:

Icon	Severity Level	Meaning
	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 events 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 116: NMP Professional - Tabbed Data Panel - Events - ACK Column Detail

To acknowledge one event, double-click on the selected table entry, or choose the "ACK Event" from table context menu. When the event is acknowledged, the date and time of acknowledgement is displayed instead of "NO ACK" text.

To acknowledge all events at once, click on the button "ACK" at the upper right hand pane of the dialogue.

Note:

The events which do not require user acknowledgement are always acknowledged automatically by the system.

5.11 Managing Industrial Ring Errors

In the device tree list it is possible to group ring devices (see page 80).

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 (Figure 117) 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.

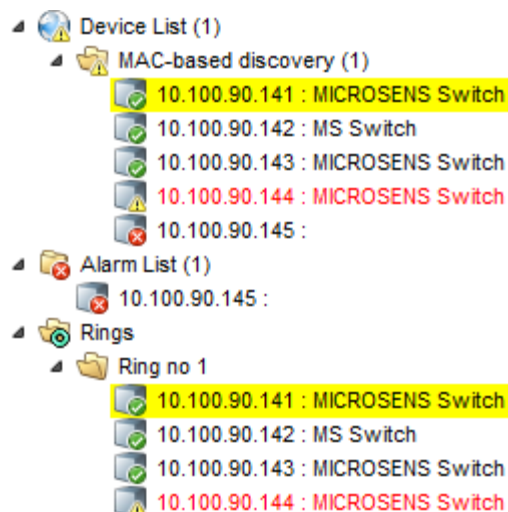


Figure 117: NMP Professional - Device Tree List View - Industrial Ring Errors

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.

6 NMP Enterprise: Getting started with the Server 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.

This chapter describes the features and operation of the server component of NMP Enterprise.

On how to use the client component of NMP Enterprise please refer to chapter "NMP Enterprise: Getting started with the Client Component" on page 171.

On how to use NMP Professional please refer to chapter "NMP Professional: Getting started" on page 20.

Note:

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

Note:

Running the Server Manager does not require any login.

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.

6.1 Starting the Server Manager

6.1.1 Starting on Windows®

In order to start the Server Manager 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 server in debug mode will open an additional Microsoft Windows® command line interface ('cmd'), where all the logs and errors will be displayed.

The Server Manager opens with its main window.

6.1.2 Starting on Linux Operating Systems

Note:

NMP 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 NMP with "sudo bash start_NMPS.sh" or "su root start_NMPS.sh", depending on your Linux operating system. For more

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

Open a Linux CLI and change to the NMP installation directory (e.g. "`~/MICROSENS/NMP_Server`").

Start NMP Server as root user e.g. with "`sudo sh ./start_NMPS.sh`" (or the respective super user command of your Linux distribution for starting a bash script).

6.1.3 First Program Start

During first start the NMP Server checks whether a previous NMP v1 installation is available. If so, NMP asks to migrate the data from this NMP version to NMP v2.

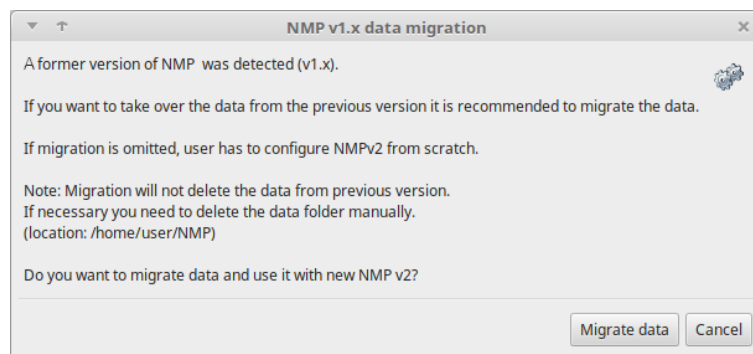


Figure 118: Data Migration from NMP v1

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

NMP Server will create a new directory "`~/NMPv2 Server`" in the user's home directory.

The first time starting process continues with licensing NMP Server. For more information see chapter "3 Licensing" on page 18.

6.2 Server Manager Main Window

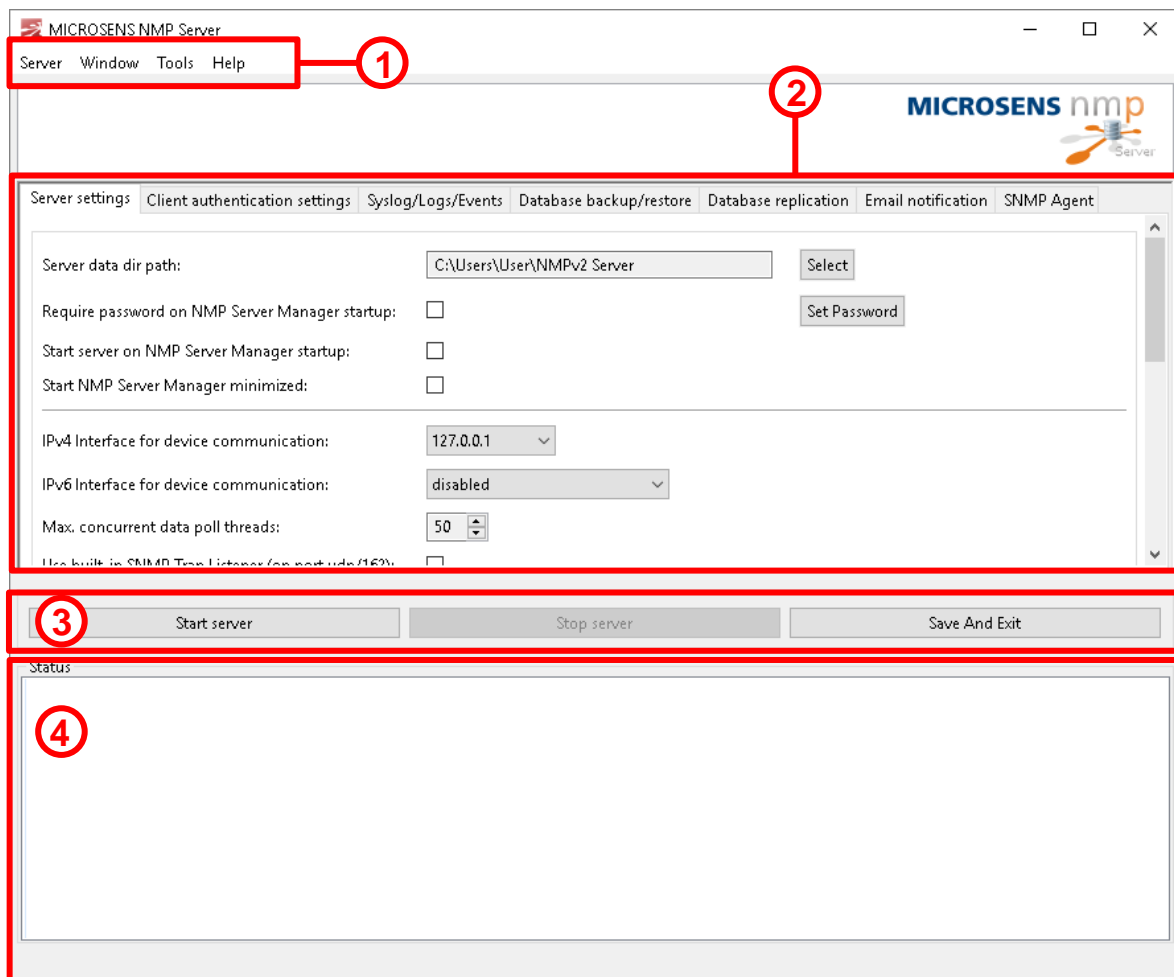


Figure 119: Server Manager - Main Window

The main window of the Server Manager consists of four main elements:

- 1** - Main Menu (see page 129)
- 2** - Tabbed Server Configuration Panel (see page 134)
- 3** - Server Control Buttons (see page 136)
- 4** - Status Text Field and Server IP address (see page 146)

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

6.3 Main Menu

The main menu bar provides access to functions like starting and stopping server, interacting with an application or help.

6.3.1 Server

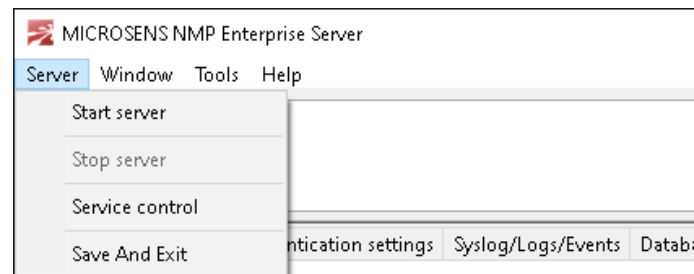


Figure 120: Server Manager - Main Menu - Server

6.3.1.1 Start server (Shortcut: None)

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.

6.3.1.2 Stop server (Shortcut: None)

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!

6.3.1.3 Service control (Shortcut: None)

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

For detailed information, please refer to the section "Server Instance as Windows Service" on page 147.

6.3.1.4 Save And Exit (Shortcut: None)

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.

6.3.2 Window

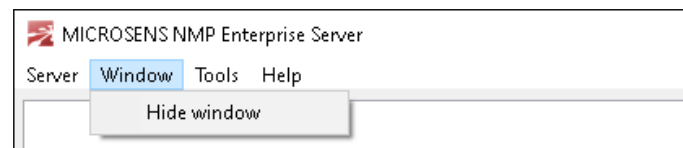


Figure 121: Server Manager - Main Menu - Window

6.3.2.1 Hide window

(Shortcut: None)

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

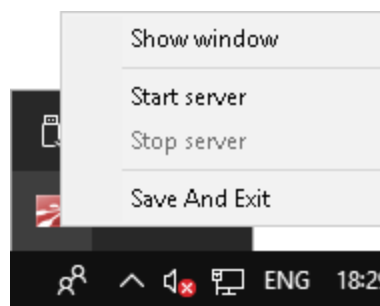


Figure 122: Server Manager - System Tray Icon

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.

6.3.3 Tools

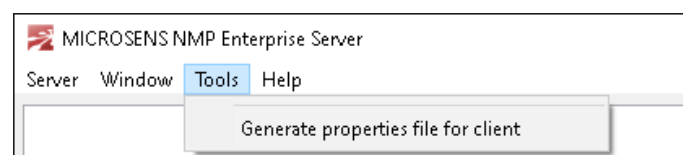


Figure 123: Server Manager - Main Menu - Tools

6.3.3.1 Generate Properties File for Client

(Short-Cut: None)

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 client component of NMP Enterprise the installer initially searches for this file to preset the server settings for the server client communication.

6.3.4 Help

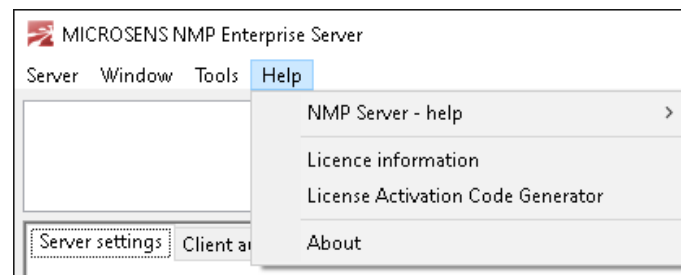


Figure 124: Server Manager - Main Menu - Help

6.3.4.1 NMP Server help (Shortcut: None)

This is the link to the NMP variant 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.

6.3.4.2 Licensing Information (Shortcut: None)

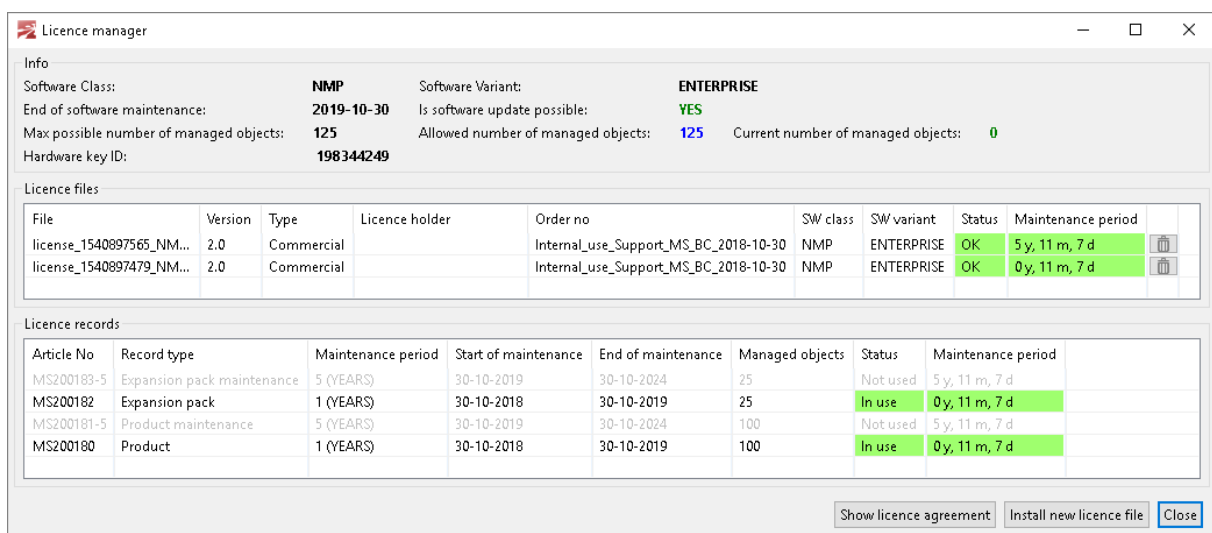


Figure 125: Server Manager - Licensing Information

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

A click on the button "Install new licence key file" opens the file manager. Navigate to the new licence key file to update the NMP Enterprise licence key.

Note:

To obtain a new NMP Enterprise licence key file please contact MICROSENS.

6.3.4.3 Usage Right Activation Code Generator

This menu item opens the Licence Activation Code Generator.

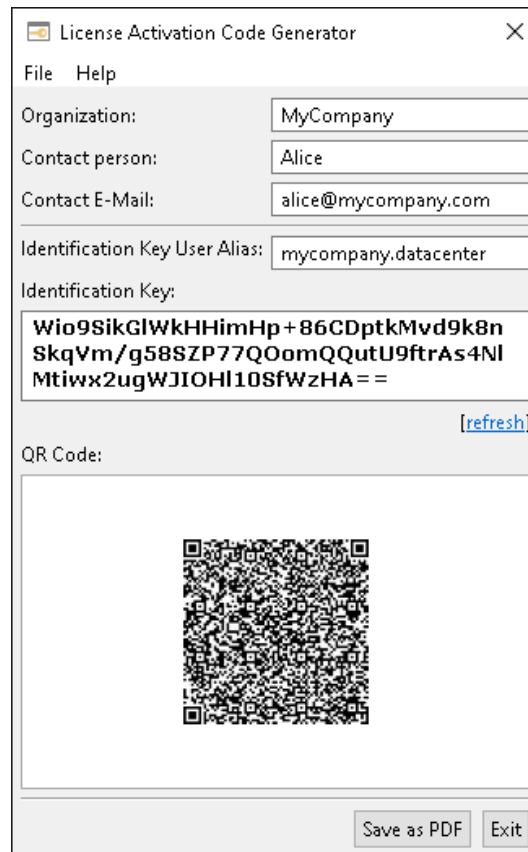


Figure 126: Licence Activation Code Generator

The code generator determines a unique system ID and generates the respective hash code for an identification key.

This identification key is necessary to apply for a valid licence key file from MICROSENS.

The input fields are optional.

Using a user alias for the identification key simplifies the licence key file handling when using multiple key files.

Click on the button "Save as PDF" to save the generated identification key file and send it to MICROSENS sales.

6.3.4.4 About**(Shortcut: None)**

This menu item shows information about NMP Enterprise software version.

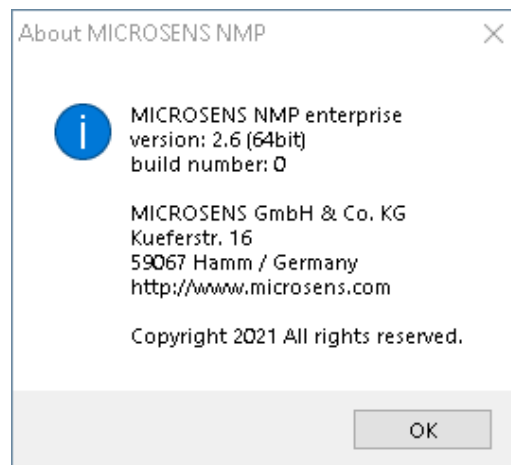


Figure 127: Server Manager - About

6.4 Tabbed Server Configuration Panel

The tabbed server configuration panel allows configuring all the server component's parameters.

6.4.1 Server Settings

Figure 128: Server Manager - Tabbed Server Configuration Panel - Server Settings

- **Server data dir path:** Configure the directory where the server component will save all necessary configuration files and database data. The default folder is: `$USER_HOME\NMPv2 Server`. In the selected destination folder a new folder 'NMPv2 Server' will be created.

- **Require password on NMP 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".

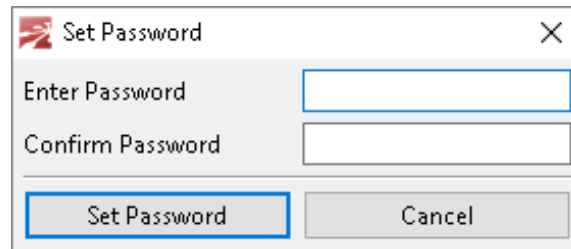


Figure 129: Server Manager - Tabbed Server Configuration Panel - Server Settings - Set Password

Enter the password, confirm the password to prevent typing errors and click the button "Set Password".

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

- **Start server on NMP Server Manager startup:** Automatically starts the server component (database engine, device data collector and, if enabled, HTTP server) on start-up. If the Server Manager will be added to the list of OS auto-start applications, the server component will be started automatically and ready to use after OS boot.
- **Start NMP Server Manager minimized:** Starts the Server Manager window minimized. The most important Server Manager features will be available via the system tray icon (see page 130).
- **IPv4 Interface for device communication:** The IPv4 address of the network interface that will be used for communication with the managed devices. In a more complex network infrastructure where the server hardware has more than one network adapter, it is possible to use one interface (accessible exclusively from secured local network) for device communication and another one (accessible from external 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 communication:** 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 at one time. For slower servers, heavy loaded networks or slow network connections we recommend reducing this value for a better performance.
- **Use built-in SNMP Trap Listener (on port udp/162):** The server component 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.
- **Interface for client-server communication:** The IPv4 address of the network interface that will be used for the specific client component access. If

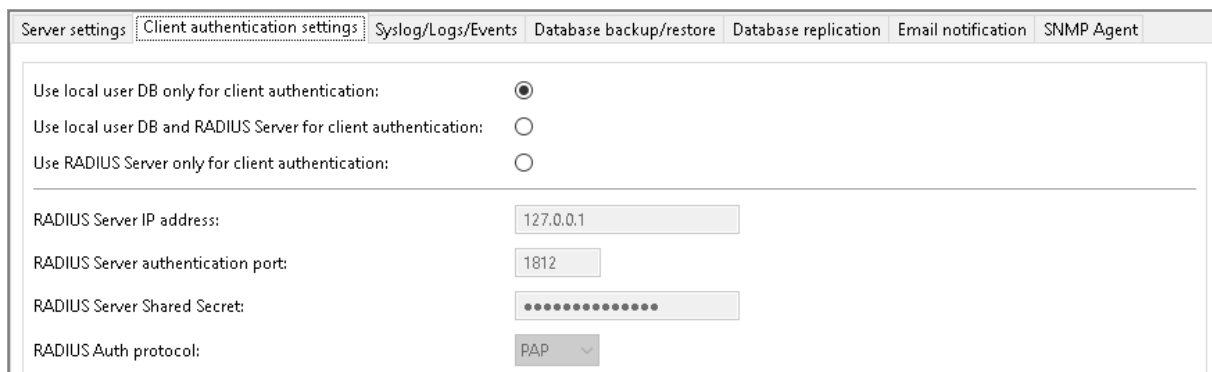
the HTTP server is enabled for Web Client access, the interface is also used by the built-in HTTP server.

- **Port for client-server commands:** The port that is used by the client component to communicate with the server component (4000 on default).
- **FTPS (FTP over SSL) Server port:** The built-in FTPS server is used by the client component to synchronise device lists and firmware updates (4001 on default).
- **FTP User / FTP Password:** Enter the credentials for the FTP user.
- **Database Server port:** The port used by the built-in database server for client component access (4002 on default).
- **Database Server password:** As soon as the server component is started, it is possible to change the database password. Administrator user rights are mandatory.

Note:

Authorise all given port numbers in installed firewalls.

6.4.2 Client Authentication Settings



Server settings | **Client authentication settings** | Syslog/Logs/Events | Database backup/restore | Database replication | Email notification | SNMP Agent

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: ☐

RADIUS Server IP address:

RADIUS Server authentication port:

RADIUS Server Shared Secret:

RADIUS Auth protocol:

Figure 130: Server Manager - Tabbed Server Configuration Panel - Client Authentication Settings

- **Use local user DB only for client authentication:** The server will use the information from his 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. The local user account (in the local server database) will be created automatically (if such an account does not exist).

Note:

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

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

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

The user levels of RADIUS server and the server component are mapped as follows:

RADIUS Server User Level (Value of RADIUS Service Type)	NMP Enterprise User Level
Login-User (1)	User
NAS-Prompt-User (7)	Manager
Administrative-User (6)	Administrator
Callback-Administrative (11)	System Administrator

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 server component treats the RADIUS server as the master authentication server. When the user level (Service-Type) or user password will be changed on RADIUS Server, the server component will automatically update the local user account.

Note:

At least one user with "sysadmin" rights has to exist at the local server database. The server component will deny to change the user level of its local account resulting there would be no local user left with "sysadmin" rights.

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 server users available on the RADIUS

server should be identical to the number of NMP Enterprise user accounts allowed by the licence key file.

6.4.3 Syslog/Logs/Events

The screenshot displays the 'Syslog/Logs/Events' configuration tab in the Server Manager. It is divided into several sections:

- Syslog Server (receive Syslogs):** Includes an 'Enable Syslog Server' checkbox, a 'Syslog Server interface' field (192.168.1.10) with a caution note, and a 'Syslog Server port [udp]' field (514).
- Syslog Client (send Syslogs):** Includes an 'Enable Syslog Client' checkbox, a 'Syslog destination (server IP)' field (0.0.0.0), and a 'Protocol/Port' dropdown set to UDP/514.
- Local logs:** Includes an 'Archive logs when log count higher than' dropdown (25000), a 'Logs archive folder' field (C:\Users\User\NMPv2 Server\LogArchive) with a 'Select folder' button, a 'Keep device history from last' dropdown (2 month(s)), and a 'Clear selected log database tables' section with checkboxes for 'Events (logs) table' and 'Devices statistics/history', and a 'Clear' button.
- Events configuration:** Includes an 'Events severity style' dropdown (SYSLOG) and a table for event configurations.

Event	Relevance	Severity	[Display]	Sound notification	Email notification	Syslog notification	SNMP Trap notification
SYSTEM_INFO	INFO	info	info	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SYSTEM_OK	POSITIVE	notice	notice	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SYSTEM_ERROR	NEGATIVE	ERROR	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_SNMP_TRAP	[Mapped from SNMP TRAP Message or INFO:WARNING]			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_SYSLOG	[Mapped from SYSLOG Message]			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_RESPONSE_OK	POSITIVE	disabled		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE_RESPONSE_ERROR	NEGATIVE	CRITICAL	CRITICAL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 131: Server Manager - Tabbed Server Configuration Panel - Syslog/Logs/Events

Syslog Server (receive Syslogs)

- **Enable Syslog server:** The server component can act as a syslog server. In such case, all the syslog messages sent by devices will be saved at the 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)

- **Enable Syslog client:** Enables the syslog client function. In this mode the server component will send syslog messages.
- **Syslog destination (server IP):** The IP address of the syslog server, where the server should send 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

- **Archive logs when log count higher than:** The server will generate a `.csv` file with log messages when the number of log messages in the database will be higher than the defined limit (25000, 50000 or 100000 messages). 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 o'clock AM. Always the last 500 and all unacknowledged messages are kept in the database (i.e. they are not deleted during the archiving procedure).
- **Logs archive folder:** Choose the location where the server should save the log archives.
- **Keep device history from last:** The 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 6 months. The server clears the database each day at 2 o'clock AM.
- **Clear selected log database tables:** Clear the database log tables manually by selecting the respective type of table that should be cleared and clicking the button "Clear". This operation will remove all the log entries from the selected tables.

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

Additionally, each NMP 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 (not displayed, nor logged). It is greyed out.
	S: info I: cleared	This is an informational message that does not require special attention (e.g. system messages). It is formatted in black font colour.
	S: notice I: normal	This is a success notification (e.g. a configuration applied successfully). It is formatted in green font colour.
	S: WARNING I: WARNING	This is a low level warning message. It is formatted in black font colour on yellow background.
	S: ERROR I: MINOR	This is an error message that requires user attention. It is formatted in red font colour.
	S: CRITICAL I: MAJOR	This is a critical error message that requires immediate user attention. It is formatted in black font colour on red background.
	S: ALERT I: CRITICAL	This is an alert message. It is formatted in black font colour on red background.
	S: EMERGENCY I: EMERGENCY	This is an emergency message. It is formatted in black font colour on red background.
	S: debug I: debug	This message contains debugging information. It is formatted in blue font colour.

Messages are displayed differently in the 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 tab "Email Notification" (see page 143).

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

Note:

The syslog client has to be enabled on this tab.

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

Note:

Enable and configure the SNMP Agent on tab "SNMP Agent" (see page 144).

6.4.4 Database Backup/Restore

Figure 132: Server Manager - Tabbed Server Configuration Panel - Database Backup/Restore

The server component allows creating a backup copy of the currently used database. The system administrator is able to back up the database manually by clicking the button "Backup". Depending on the determined option the database copy will be:

- saved at the selected folder or
- sent to the configured FTP server.

In case of "Backup to FTP Server" option, the path to the backup folder should be defined (e.g. `"/Some Folder/Backup"`).

Note:

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

The backups will be saved as **.zip** archives. The filename contains the current date (e.g. "**NMPS_DB_BACKUP_2018-06-15.zip**"). If a file with this name already exists in the backup folder, the current time in milliseconds will be added after the current date to differ the files.

It is possible to enable scheduled backups. In such case the server will automatically create a database copy every x days (1...30). The scheduler will use the currently selected backup option to create the backup (i.e. "Backup to selected folder" or "Backup to FTP server").

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

Note:

The server has to be stopped before starting the backup restore procedure.

Note:

The server instance has to be stopped before starting the backup restore procedure.

6.4.5 Database Replication

Server settings | Client authentication settings | Syslog/Logs/Events | Database backup/restore | **Database replication** | Email notification | SNMP Agent

Replication mode: ☐ Enable replication ☒ Master server ☐ Slave server

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

Local replication interface:

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

Remote replication partner IP address:

Remote replication partner communication port:

CAUTION: Always the same as the remote server replication port

Replication server port:

Replication failover in service mode:

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

Figure 133: Server Manager - Tabbed Server Configuration Panel - Database Replication

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

For more information on database replication please refer to the chapter "Server Database Replication" on page 153.

6.4.6 Email Notification

Server settings Client authentication settings Syslog/Logs/Events Database backup/restore Database replication **Email notification** SNMP Agent

Enable Email Notifications: ☐ (on errors, SNMP Trap and scheduled task events) Test

SMTP Server:

Authentication user:

Authentication password:

Authentication required: ☐

Encryption method:

SMTP Port:

Sender email address:

Publicly available additional email address

Enable additional email address: ☐

Email address (receiver):

Figure 134: Server Manager - Tabbed Server Configuration Panel - Email Notification

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 NMP Enterprise 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.

- **SMTP Port:** The SMTP server port.
- **Sender email address:** The email address used in the field "From" of the sent message.
- **Enable 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.
- **Email address (receiver):** Enter the email address for an additional notification receiver.

6.4.7 SNMP Agent

Server settings | Client authentication settings | Syslog/Logs/Events | Database backup/restore | Database replication | Email notification | **SNMP Agent**

SNMP Agent

Enable SNMP Agent: ☐

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

SNMP Agent port:

SNMP version: ☐ SNMPv1 ☐ SNMPv2c ☐ SNMPv3

SNMPv1 / SNMPv2c community strings

SNMP Read Community string: SNMP Write Community string:

SNMP v3 authentication settings

USM User:

Security level: ▼

Auth Algorithm: ▼ Auth Password:

Privacy Algorithm: ▼ Privacy Password:

Context name:

SNMP Trap Destination

Destination	Version	IP address	UDP port	Community
1:	<input checked="" type="radio"/> disable <input type="radio"/> v1 <input type="radio"/> v2c <input type="radio"/> v3	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="*****"/>
2:	<input checked="" type="radio"/> disable <input type="radio"/> v1 <input type="radio"/> v2c <input type="radio"/> v3	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="*****"/>
3:	<input checked="" type="radio"/> disable <input type="radio"/> v1 <input type="radio"/> v2c <input type="radio"/> v3	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="*****"/>
4:	<input checked="" type="radio"/> disable <input type="radio"/> v1 <input type="radio"/> v2c <input type="radio"/> v3	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="*****"/>

Figure 135: Server Manager - Tabbed Server Configuration Panel - SNMP Agent

The SNMP protocol can be used to make management data available to other management systems. The server instance offers a northbound interface in 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.

SNMP Agent

- **Enable SNMP Agent:** Enabling the SNMP agent reveals the management data collected by the server component to the other SNMP managers.

- **SNMP Agent interface:** The IP address of the network interface used by the SNMP Agent through which the 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 version needed to be supported by the SNMP Agent. At least one version should be enabled.

SNMPv1/SNMPv2c community strings

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

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

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

For more information about using SNMP traps please refer to the section "Using SNMP Traps" on page 164.

6.5 Server Control Buttons

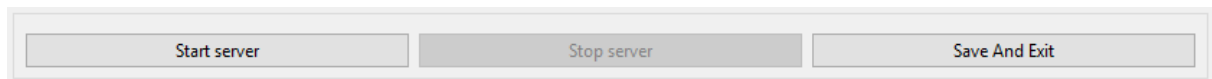


Figure 136: Server Manager - Server Control Buttons

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.

Note:

This button is available if the server instance is stopped.

6.6 Status Text Field

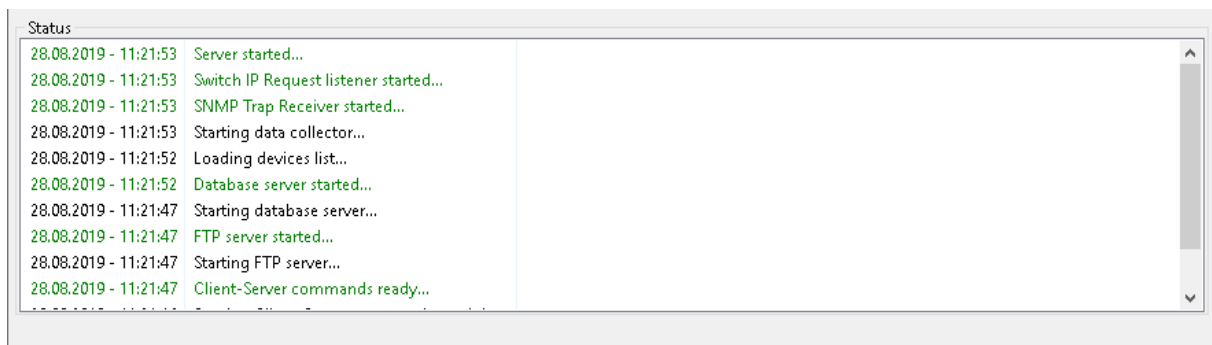


Figure 137: Server Manager - Status Text Field

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

7 NMP Enterprise: Working with the Server Component

This chapter contains appliance concepts of the server component of NMP Enterprise.

7.1 Basic Configuration

At 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 on page 134.

7.2 Software Update

NMP 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 NMP.

In order to update the application, stop a running server instance and exit the Server Manager or stop the server service (if the server component was started as Windows service). Subsequently install the updated version.

During the installation choose the same installation path as the path chosen for the previous version. All application files will be updated.

7.3 Server Instance as Windows Service

On Microsoft Windows® operating systems it is possible to install the server instance 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.

7.3.1 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**

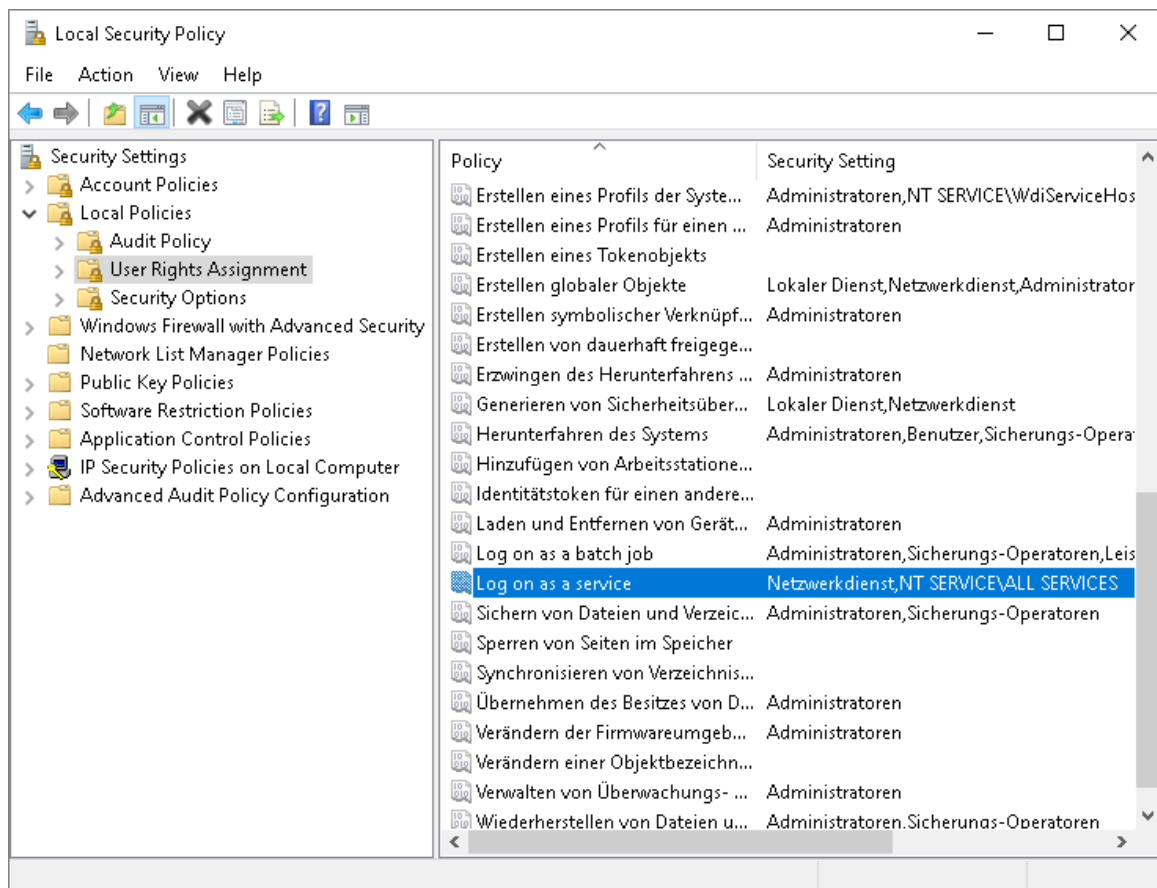


Figure 138: Server as a Service - Local Policy

3. In the details panel, double-click **Log on as service**

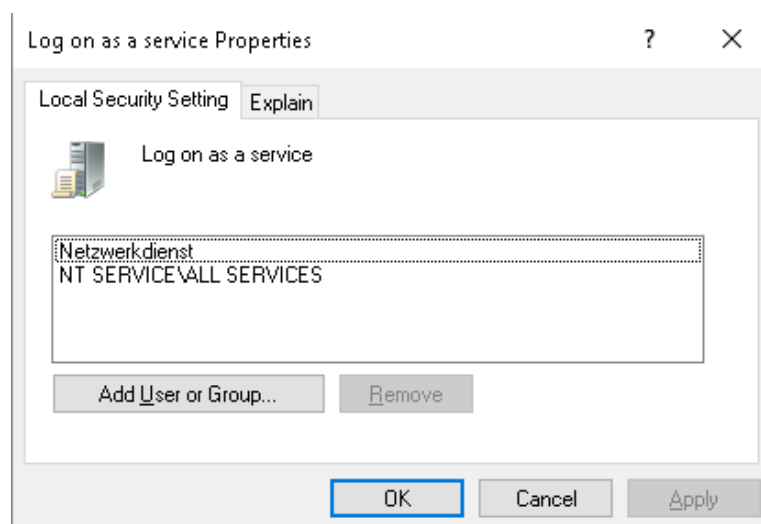


Figure 139: Server as a Service - Local Policy - Properties

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.

7.3.2 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 page 134) and then 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 submenu item **Service control** that is available via the menu item **Server** in the Server Manager main menu bar.

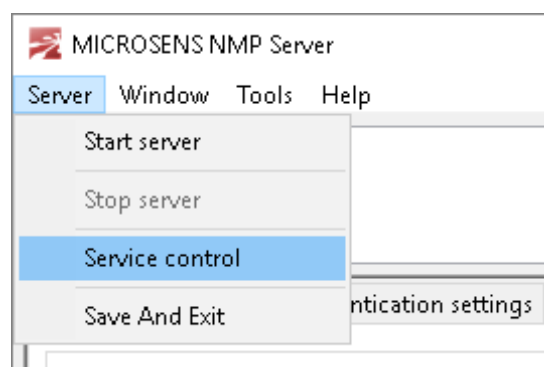


Figure 140: Server Manager - Main Menu - Server - Service Control

4. To install the service specify the password used for the Windows account and domain name (in cases where a domain account is used).

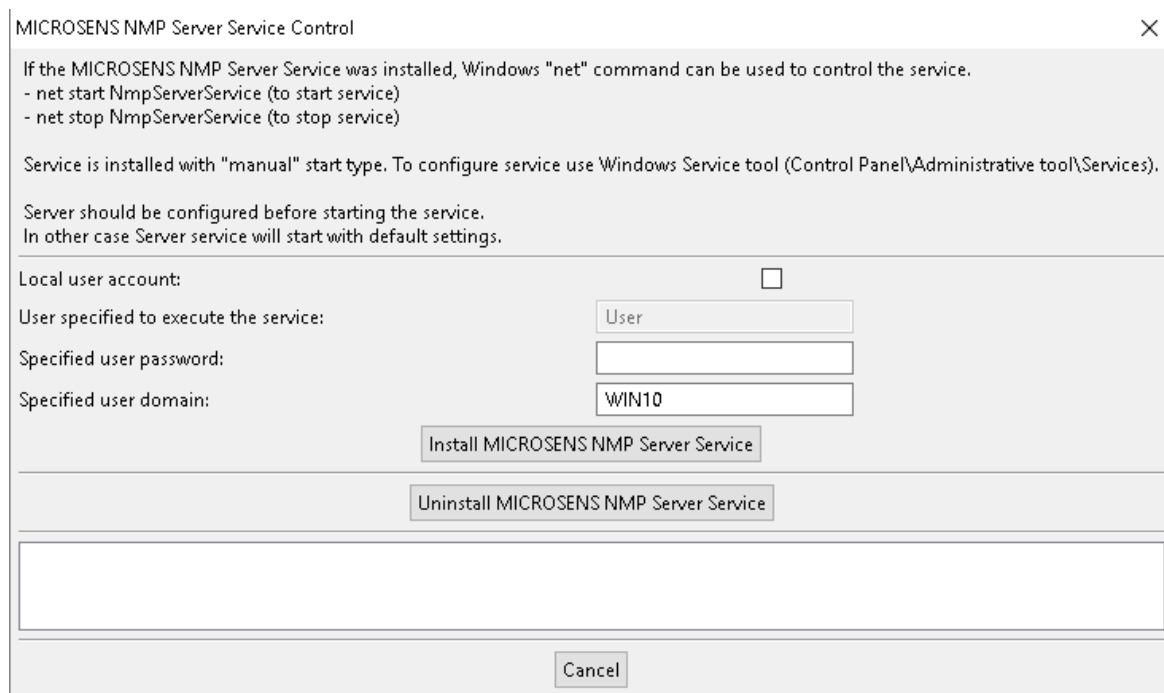


Figure 141: Server Manager - Service Control

5. After clicking the button "Install MICROSENS NMP Server Service" the tool will try to 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 NMP Server Service" the tool will try to remove the service from the system.

The service is always installed with "Auto" start type 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.

7.3.3 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 launching "Services" via **Windows Control Panel > Administrative Tools**.

Alternatively, open the "Service" dialogue by typing **Services.msc** in the Run command on Start menu.

Alternatively, "Services" can be started or stopped 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.

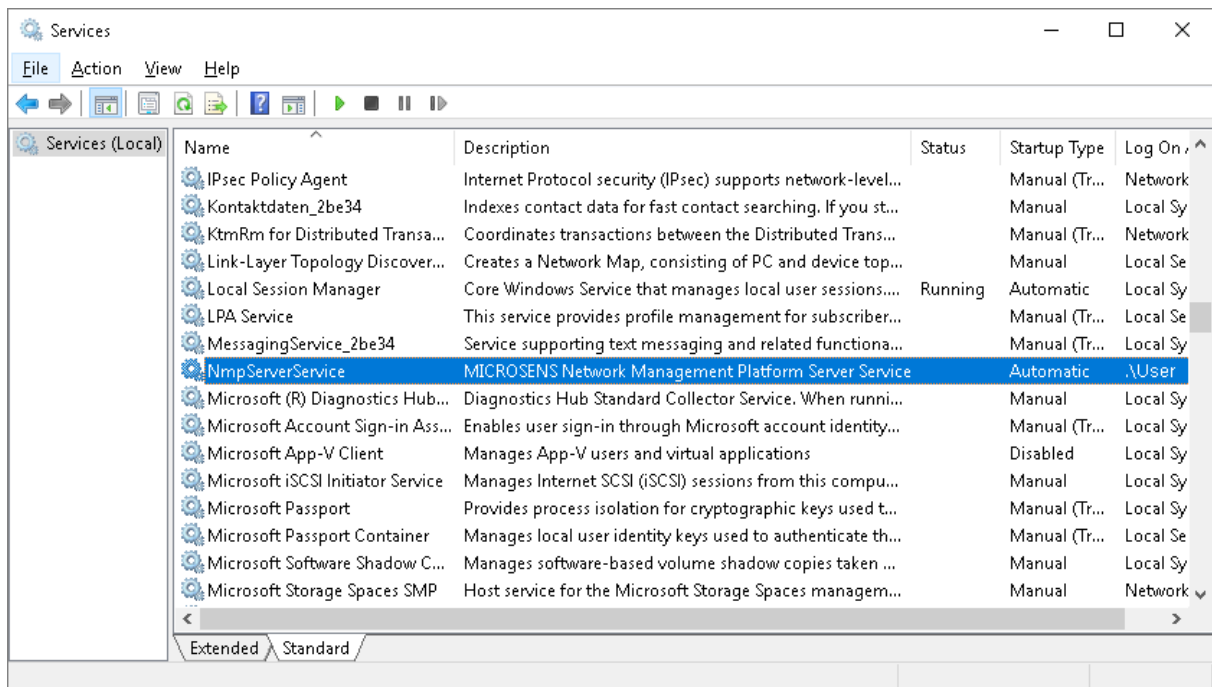


Figure 142: Server as a Service - Windows Services Dialogue

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)** is a new start-up type introduced in Windows Vista®, that 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" to manage the service.

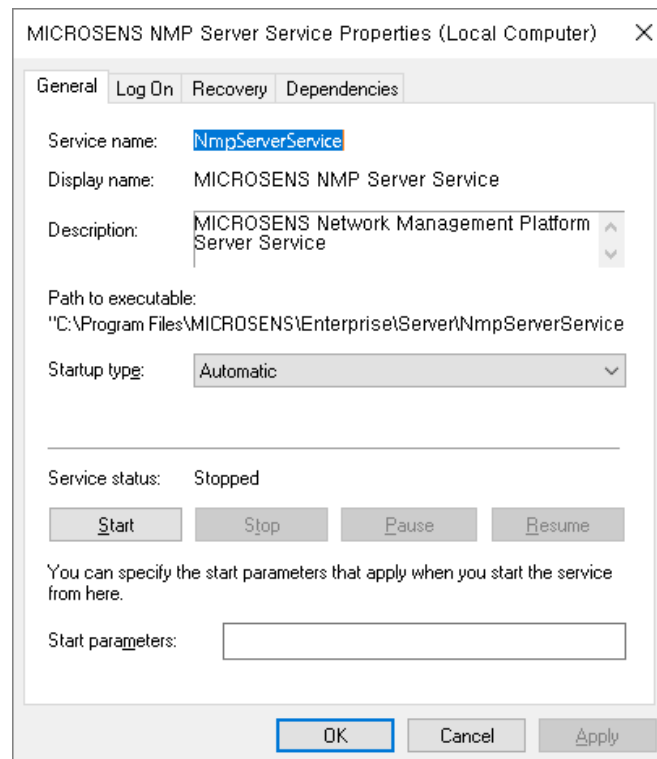


Figure 143: Server as a Service - General

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, user can 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 **NmpServerService.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.

7.4 Server Database Replication

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.

7.4.1 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".

	Local	Remote
Server status	Up	Unknown
Replication mode	Disabled	Unknown
Replication status	Disabled	Unknown

Figure 144: Server Manager - Database Replication Setting

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 "Server settings" tab)
- **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 "Server settings" page)
- **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.

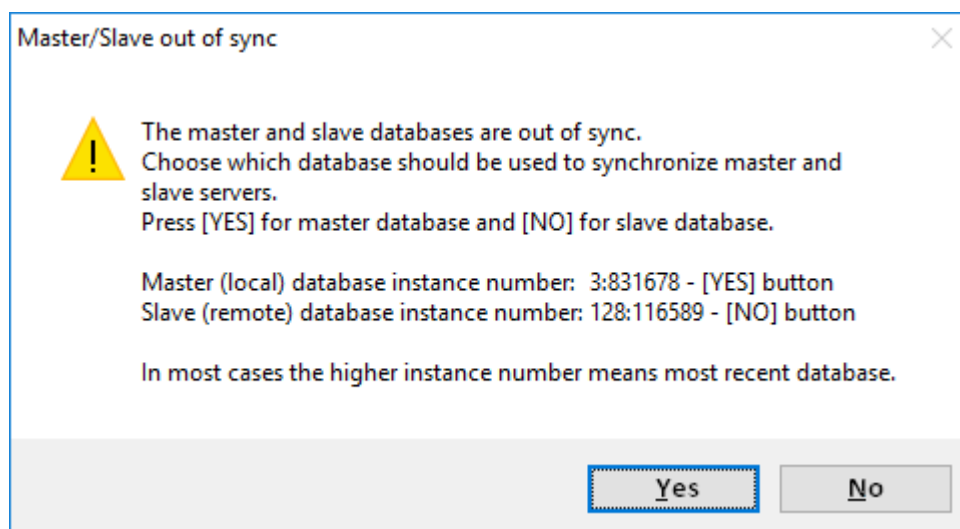


Figure 145: Server Manager - Database Replication - Out of Sync Message

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 NMP Enterprise). 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 the section "General Database Replication Procedure" on page 157).

When the database replication is started, it is possible to use a client application (i.e. client component or NMP Web Client) 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:

- NMP Web Client 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.

7.4.2 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.

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.

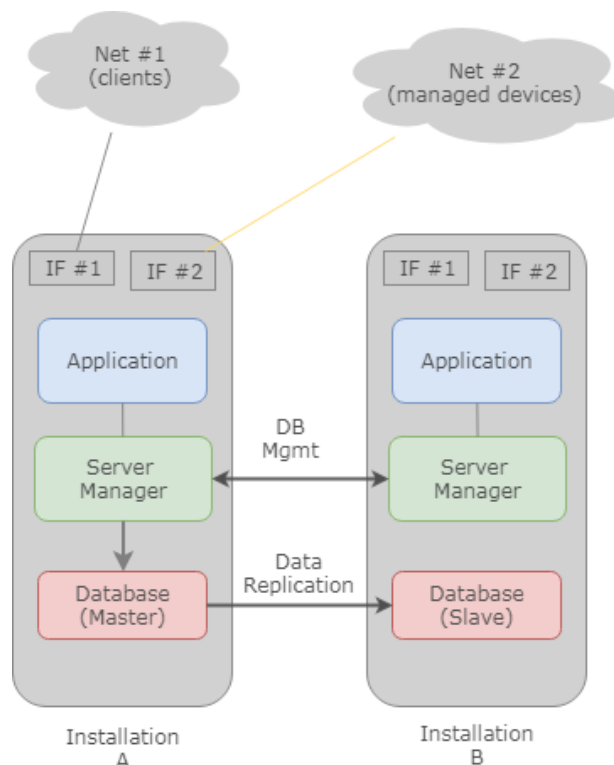


Figure 146: Database Replication - Redundant Operation

7.4.3 Scenario 1: 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 146).
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 147).

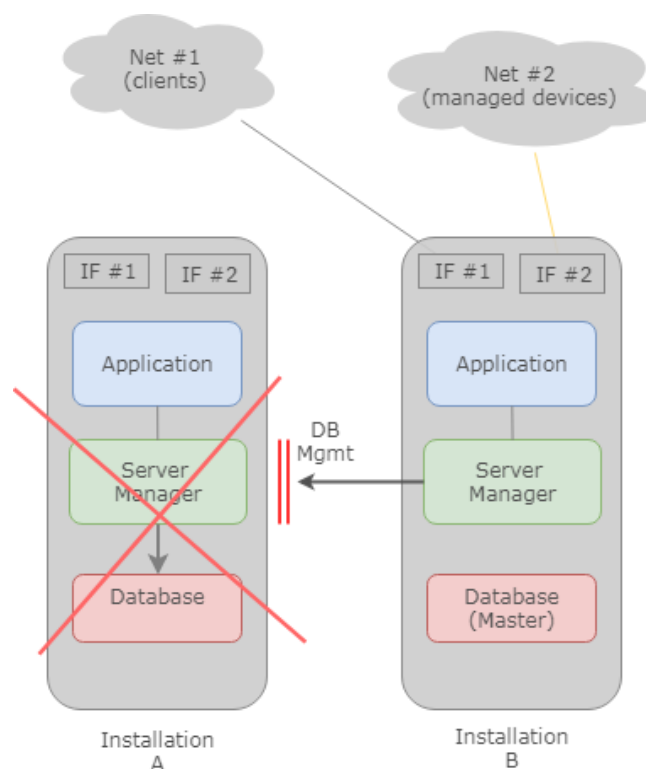


Figure 147: Database Replication - Master Server Failure

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'.

Instance 'B' notices that its replication partner server is available again and reboots in replication mode. Both servers synchronise their databases.

The replication process is re-initialised and both master and slave server operate in their previously determined replication modes (Figure 148).

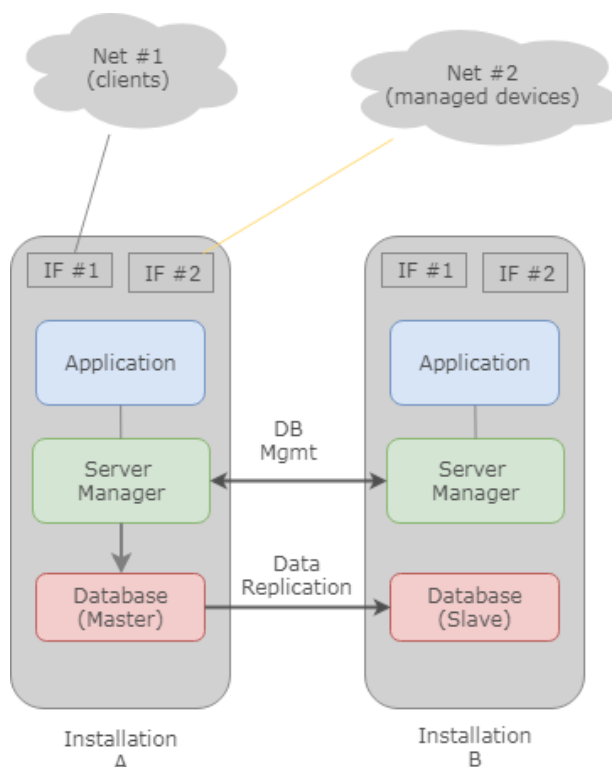


Figure 148: Database Replication - Master Server Restart

7.4.4 Scenario 2: 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 146 on page 157).
2. Due to a failure instance 'B' (slave) is not available. 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 instance 'B' to show up again (Figure 149).

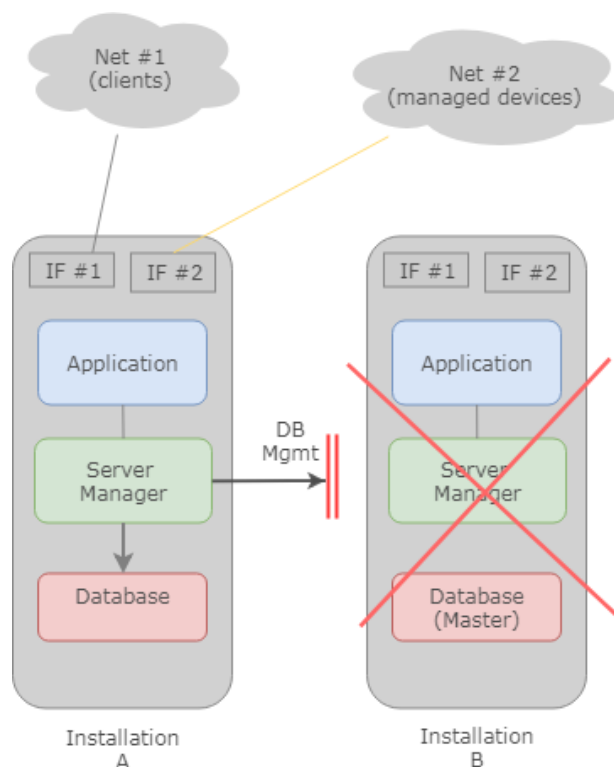


Figure 149: Database Replication - Slave Server Failure

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'.

Instance 'A' notices that its replication partner server is available again and reboots in replication mode. Both servers synchronise their databases.

The replication process is re-initialised and both master and slave server operate in their previously determined replication modes (Figure 150).

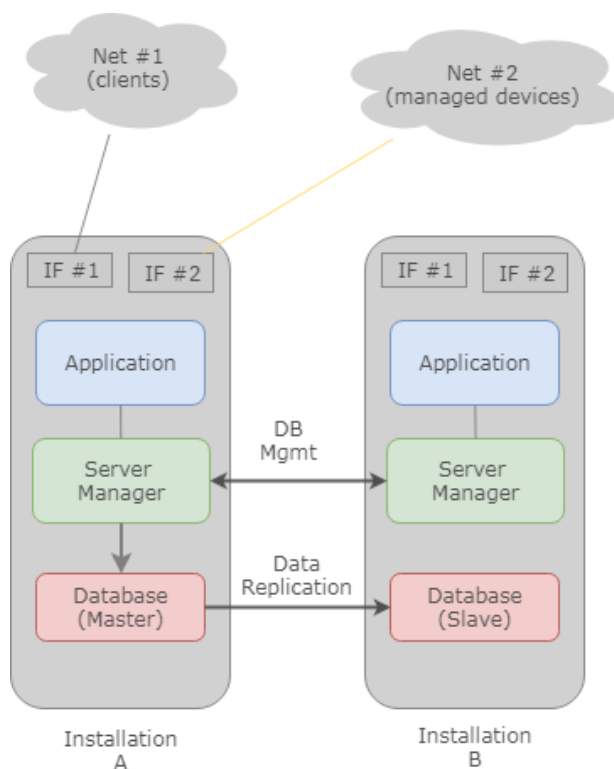


Figure 150: Database Replication - Slave Server Restart

7.4.5 Scenario 3: 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 146 on page 157).
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.

Note:

The replication of databases is not possible.

Both servers wait for their respective replication partner to show up again (Figure 151).

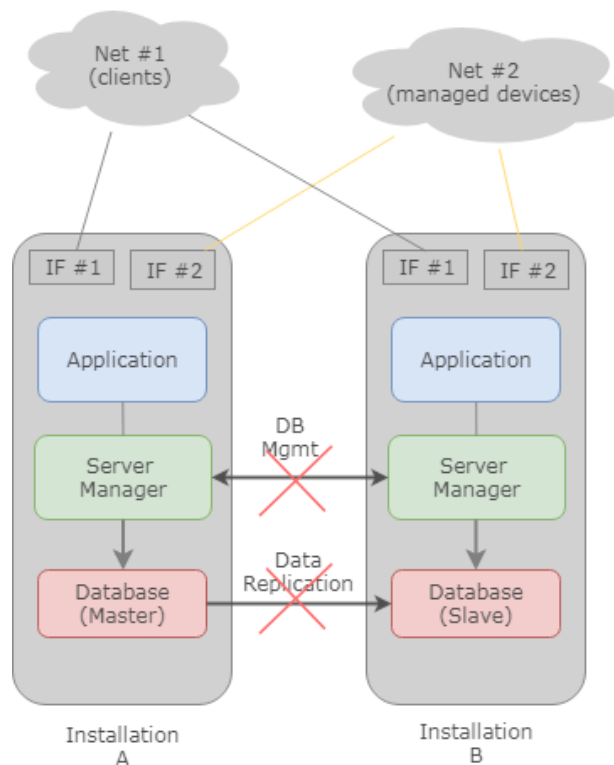


Figure 151: Database Replication - Link Failure

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.

The replication process is re-initialised and both master and slave server operate in their previously determined replication modes. They synchronise their databases (Figure 152).

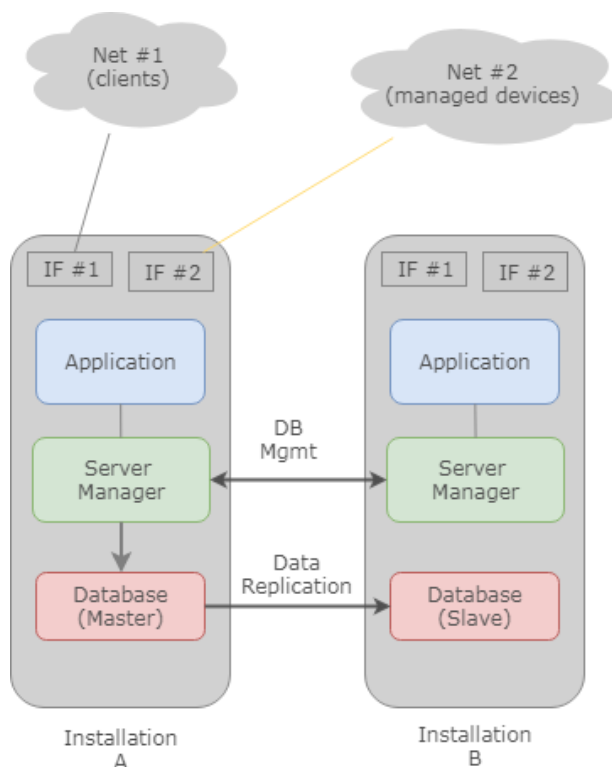


Figure 152: Database Replication - Link Restored

7.5 Using SNMP Traps

Note:

For configuration of SNMP traps please refer to the section "SNMP Agent" on page 144.

7.5.1 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 "**NMP_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 sub-groups:
 - **nmpServerNotifications**
 - **eventData:** Information about the occurring event
- **nmppsConformance**

The available OIDs of the server's MIB are listed in the following table:

OID	Name	Access	Description
.1.3.6.1.4.1.3181	microsens		
.1.3.6.1.4.1.3181.5909	nmpServer		
.1.3.6.1.4.1.3181.5909.1	serverInfo		
.1.3.6.1.4.1.3181.5909.1.1.0	serverName	R	Server name
.1.3.6.1.4.1.3181.5909.1.2.0	serverManufacturer	R	Server manufacturer
.1.3.6.1.4.1.3181.5909.1.3.0	serverVersion	R	Server version
.1.3.6.1.4.1.3181.5909.1.4.0	serverLicenseArticleNumber	R	Server licence key file article number
.1.3.6.1.4.1.3181.5909.1.5.0	serverLicenseHolder	R	Entitled user
.1.3.6.1.4.1.3181.5909.1.6.0	serverMaintenancePeriod	R	Server maintenance period
.1.3.6.1.4.1.3181.5909.1.7.0	serverMaxActiveUsers	R	Maximum number of active users supported
.1.3.6.1.4.1.3181.5909.1.8.0	serverCurrentActiveUsers	R	Current number of active users

OID	Name	Access	Description
.1.3.6.1.4.1.3181.5909.1.9.0	serverStartTime	R	Server start time
.1.3.6.1.4.1.3181.5909.1.10.0	serverUptime	R	Server uptime
.1.3.6.1.4.1.3181.5909.1.11.0	serverReplicationMode	R	Server replication mode
.1.3.6.1.4.1.3181.5909.1.12.0	serverReplicationStatus	R	Server replication status
.1.3.6.1.4.1.3181.5909.2	deviceList	R	
.1.3.6.1.4.1.3181.5909.2.1.0	deviceListSize	R	Server device list size
.1.3.6.1.4.1.3181.5909.2.2	deviceListTable	NA	Server device list
.1.3.6.1.4.1.3181.5909.2.2.1	deviceListTableEntry	NA	Entry in the device list table
.1.3.6.1.4.1.3181.5909.2.2.1.1	deviceIp	NA	Device IP address (table index)
.1.3.6.1.4.1.3181.5909.2.2.1.2	deviceSubnetMask	R	Device subnet mask
.1.3.6.1.4.1.3181.5909.2.2.1.3	deviceGateway	R	Device gateway
.1.3.6.1.4.1.3181.5909.2.2.1.4	deviceDhcpMode	R	Device DHCP mode
.1.3.6.1.4.1.3181.5909.2.2.1.5	deviceMac	R	Device MAC address
.1.3.6.1.4.1.3181.5909.2.2.1.6	deviceName	R	Device name
.1.3.6.1.4.1.3181.5909.2.2.1.7	deviceLocation	R	Device location
.1.3.6.1.4.1.3181.5909.2.2.1.8	deviceContact	R	Person who is responsible for the device
.1.3.6.1.4.1.3181.5909.2.2.1.9	deviceGroup	R	Device list group
.1.3.6.1.4.1.3181.5909.2.2.1.10	deviceInventoryString	R	Device inventory string
.1.3.6.1.4.1.3181.5909.2.2.1.11	deviceStatus	R	Device status: <ul style="list-style-type: none"> • noStatus (1) • downloadingData (2) • unavailable (3) • available (4) • resetting (5) • firmwareUpdate (6) • checking (7) • userDefinedAlarm (8)
.1.3.6.1.4.1.3181.5909.2.3	deviceModulesTable	NA	List of device modules
.1.3.6.1.4.1.3181.5909.2.3.1	deviceModulesTableEntry	NA	Device modules table
.1.3.6.1.4.1.3181.5909.2.3.1.1	moduleDeviceIp	NA	Device IP address (table index)
.1.3.6.1.4.1.3181.5909.2.3.1.2	moduleId	NA	Module position in the following syntax: nodeId:unitId:slotId (table index)
.1.3.6.1.4.1.3181.5909.2.3.1.3	moduleArticleNumber	R	Module article number
.1.3.6.1.4.1.3181.5909.2.3.1.4	moduleSerialNumber	R	Module serial number

OID	Name	Access	Description
.1.3.6.1.4.1.3181.5909.2.3.1.5	moduleFirmwareVersion	R	Module firmware version
.1.3.6.1.4.1.3181.5909.2.3.1.6	moduleHardwareVersion	R	Module hardware version
.1.3.6.1.4.1.3181.5909.2.3.1.7	moduleTemperature	R	Module temperature
.1.3.6.1.4.1.3181.5909.2.3.1.8	moduleStatus	R	Module status: <ul style="list-style-type: none"> • ok (1) • spareMode (2) • inactive (3) • warning (4) • alarm (5) • unknown (255)
.1.3.6.1.4.1.3181.5909.2.4	deviceModulePortsTable	NA	List of device module ports
.1.3.6.1.4.1.3181.5909.2.4.1	deviceModulePortsTableEntry	NA	Entry in the device module ports table
.1.3.6.1.4.1.3181.5909.2.4.1.1	portModuleDeviceIp	NA	Device IP address (table index)
.1.3.6.1.4.1.3181.5909.2.4.1.2	portModuleId	NA	Module position in the following syntax: nodeId/unitId/slotId (table index)
.1.3.6.1.4.1.3181.5909.2.4.1.3	portId	NA	Module port id (table index)
.1.3.6.1.4.1.3181.5909.2.4.1.4	portAlias	R	Module port alias
.1.3.6.1.4.1.3181.5909.2.4.1.5	portStatus	R	Module port state
.1.3.6.1.4.1.3181.5909.3	servicesList	R	
.1.3.6.1.4.1.3181.5909.3.1.0	servicesListSize	R	Number of defined services
.1.3.6.1.4.1.3181.5909.3.2.0	servicesOk	R	Number of services in the ok state
.1.3.6.1.4.1.3181.5909.3.3.0	servicesError	R	Number of services in the error state
.1.3.6.1.4.1.3181.5909.3.4	servicesListTable	NA	List of defined services
.1.3.6.1.4.1.3181.5909.3.4.1	servicesListTableEntry	NA	Entry in the services list table
.1.3.6.1.4.1.3181.5909.3.4.1.1	serviceId	NA	ID of service (table index)
.1.3.6.1.4.1.3181.5909.3.4.1.2	serviceName	R	Name of service
.1.3.6.1.4.1.3181.5909.3.4.1.3	serviceDescription	R	Detailed service description
.1.3.6.1.4.1.3181.5909.3.4.1.4	serviceStatus	R	Service status
.1.3.6.1.4.1.3181.5909.100	nmpServerTrap		
.1.3.6.1.4.1.3181.5909.100.0	nmpServerNotifications		

OID	Name	Access	Description
.1.3.6.1.4.1.3181.5909.100.0.1	nmpServerSystemInfo		
.1.3.6.1.4.1.3181.5909.100.0.2	nmpServerSystemOk		
.1.3.6.1.4.1.3181.5909.100.0.3	nmpServerSystemError		
.1.3.6.1.4.1.3181.5909.100.0.4	nmpServerDeviceSnmpTrap		
.1.3.6.1.4.1.3181.5909.100.0.5	nmpServerDeviceResponseOk		
.1.3.6.1.4.1.3181.5909.100.0.6	nmpServerDeviceResponseError		
.1.3.6.1.4.1.3181.5909.100.0.7	nmpServerDeviceAccessError		
.1.3.6.1.4.1.3181.5909.100.0.8	nmpServerDeviceConfigSend		
.1.3.6.1.4.1.3181.5909.100.0.9	nmpServerDeviceConfigAccepted		
.1.3.6.1.4.1.3181.5909.100.0.10	nmpServerDeviceConfigError		
.1.3.6.1.4.1.3181.5909.100.0.11	nmpServerDeviceConfigBackup Save		
.1.3.6.1.4.1.3181.5909.100.0.12	nmpServerDeviceConfigBackup Delete		
.1.3.6.1.4.1.3181.5909.100.0.13	nmpServerDeviceFirmwareInfo		
.1.3.6.1.4.1.3181.5909.100.0.14	nmpServerDeviceFirmwareOk		
.1.3.6.1.4.1.3181.5909.100.0.15	nmpServerDeviceFirmwareError		
.1.3.6.1.4.1.3181.5909.100.0.16	nmpServerDeviceRingError		
.1.3.6.1.4.1.3181.5909.100.0.17	nmpServerDeviceStatusInfo		
.1.3.6.1.4.1.3181.5909.100.0.18	nmpServerDeviceStatusError		
.1.3.6.1.4.1.3181.5909.100.0.19	nmpServerChannelInfo		
.1.3.6.1.4.1.3181.5909.100.0.20	nmpServerChannelError		
.1.3.6.1.4.1.3181.5909.100.0.21	nmpServerSparePartMode		
.1.3.6.1.4.1.3181.5909.100.0.22	nmpServerDeviceSyslog		
.1.3.6.1.4.1.3181.5909.100.0.100	nmpServerShutdownTrap		Trap indicating that the server instance is shut down
.1.3.6.1.4.1.3181.5909.100.1	eventData		
.1.3.6.1.4.1.3181.5909.100.1.1.0	eventTime		Event time
.1.3.6.1.4.1.3181.5909.100.1.2.0	eventRelevance		Event relevance
.1.3.6.1.4.1.3181.5909.100.1.3.0	eventSeverity		Event severity
.1.3.6.1.4.1.3181.5909.100.1.4.0	eventSource		Event source like device, user or system
.1.3.6.1.4.1.3181.5909.100.1.5.0	eventSourceId		Event source ID like device IP address or user name
.1.3.6.1.4.1.3181.5909.100.1.6.0	eventMessage		
.1.3.6.1.4.1.3181.5909.200	nmpsConformance		
.1.3.6.1.4.1.3181.5909.200.1	nmpsGroups		
.1.3.6.1.4.1.3181.5909.200.1.1	nmpsServerInfoGroup		Information about server version and status

OID	Name	Access	Description
.1.3.6.1.4.1.3181.5909.200.1.2	nmpsDeviceListGroup		Information about devices at the server list
.1.3.6.1.4.1.3181.5909.200.1.3	nmpsDeviceModulesListGroup		Information about device modules
.1.3.6.1.4.1.3181.5909.200.1.4	nmpsDeviceModulePortsListGroup		Information about device module ports
.1.3.6.1.4.1.3181.5909.200.1.5	nmpsServicesListGroup		Information about defined services (end to end connections)
.1.3.6.1.4.1.3181.5909.200.1.6	nmpsNotificationsGroup		Server notifications
.1.3.6.1.4.1.3181.5909.200.1.7	nmpsEventDataGroup		Server trap objects
.1.3.6.1.4.1.3181.5909.200.2	nmpsCompliances		
.1.3.6.1.4.1.3181.5909.200.2.1	nmpsCompliance		Server compliance information

7.6 Switch DHCP Auto-Configuration

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:

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

7.6.1 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:

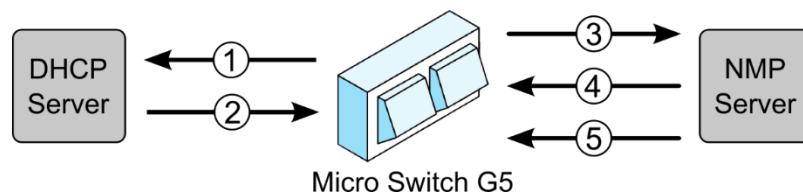


Figure 153: Server Component- Switch DHCP Auto Configuration

①	DHCP Discovery <ul style="list-style-type: none"> - Device MAC Address
②	DHCP Offer <ul style="list-style-type: none"> - Device IP address - Server instance IP Address - Latest Firmware Revision Number - Configuration Filename
③	NMP Configuration Request <ul style="list-style-type: none"> - Latest Firmware Revision Number - Configuration Filename
④	NMP Firmware Update (optional) <ul style="list-style-type: none"> - Latest Firmware File
⑤	NMP Configuration <ul style="list-style-type: none"> - Latest Configuration File

7.6.2 DHCP Server Configuration

The DHCP server must be configured to deliver two additional DHCP options included in the DHCP offer frame:

- **Option 66: Server Name (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 (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.

7.6.3 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, required): created by the client component, includes the switch configuration and the firmware filename
- Firmware file (*.bin, optional): new firmware for switches.

The configuration file is mandatory. Without this file, the server instance will not start the reconfiguration and firmware update procedure.

The firmware file is optional. The server instance will not update the device firmware, if the file is not available.

Place both files in the following directory, either manually or using the client component:

<Server data directory>/FTP/DHCPAutoconfigFiles

7.6.4 Creating/Editing the Master Configuration File

Use the client component to create and edit the master configuration file.

For more information about creating and editing the master configuration file please refer to the section "Creating/Editing the Master Configuration File" on page 188.

7.6.5 Sending the Files to the Server Instance

Use the client component to send the master configuration file and the firmware file to the server instance.

For more information about sending the files to the running server instance please refer to the section "Sending the DHCP Autoconfiguration Files to the Server" on page 190.

Note:

After updating the firmware either by Web Manager or CLI be sure to clear the cache of the browser you are using to open the Web Manager of the respective device. This will force the browser to reload the device's updated web GUI data instead of using the outdated data from its cache.

8 NMP Enterprise: Getting started with the 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 page 12).

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 chapter "NMP Professional: Getting started" on page 20.

8.1 Starting Client Component

8.1.1 Starting on Windows®

In order to start the client use one of the links which are provided in the Microsoft Windows® Start menu:

Start > MICROSENS > MICROSENS NMPv2 Client

or

Start > MICROSENS > MICROSENS NMPv2 Client (Debug mode).

Note:

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

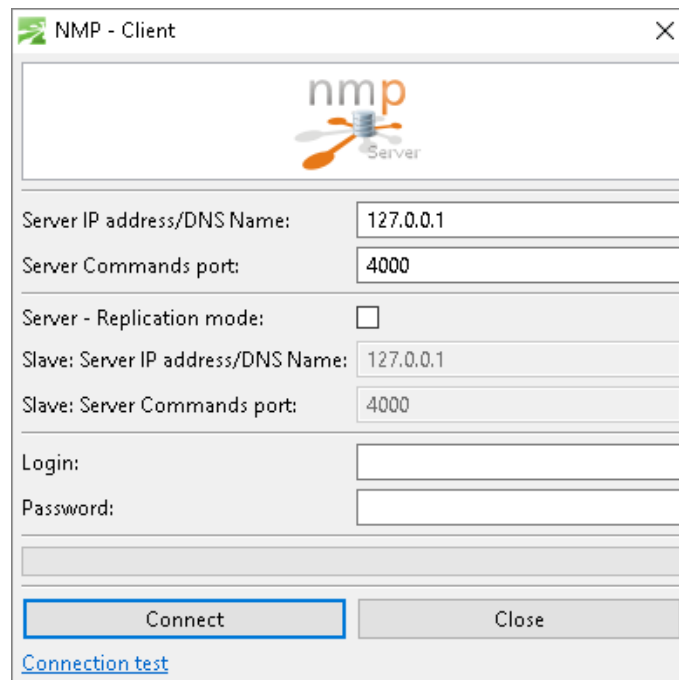


Figure 154: Client Component - Login Dialogue

8.1.2 Starting on Linux Operating Systems

Note:

NMP 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 NMP with "sudo ./NMPCClient" or "su root ./NMPCClient", depending on your Linux operating system. For more information please refer to the MICROSENS Knowledge Base on the website www.microsens.com/support.

Open a Linux CLI and change to the NMP installation directory (e.g. "~/MICROSENS/NMP_Client").

Start NMP Client as root user e.g. with "sudo NMPCClient" (or the respective super user command of your Linux distribution for starting a bash script).

8.1.3 First Program Start

During first start the NMP Client checks whether a previous NMP v1 installation is available. If so, NMP asks to migrate the data from this NMP version to NMP v2.

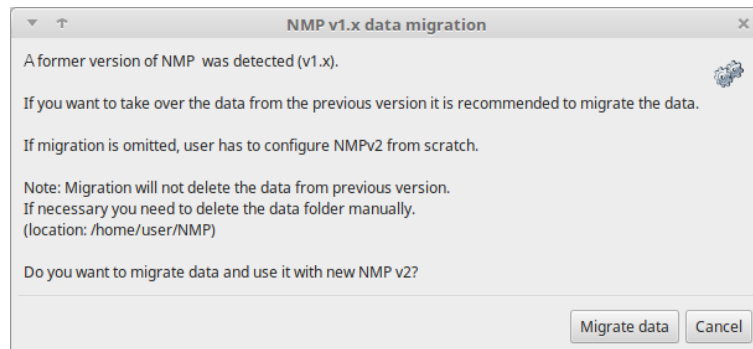


Figure 155: Data Migration from NMP v1

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

NMP Client will create a new directory "`~/NMPv2 Client`" in the user's home directory.

8.2 Login to Server Instance

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 (FTP port, Database Server port) will be automatically obtained from the server instance.

When the server instance runs in master-slave replication mode (see page 153 for more information), additionally specify the slave server's IP address and its commands port number.

The client component 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.

8.2.1 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

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 Manager" 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.

8.2.2 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)

8.2.3 Connection Test

The "Connection test" is available on the Login dialogue below the "Connect" button. It allows checking whether the connection between client component and server instance is possible.

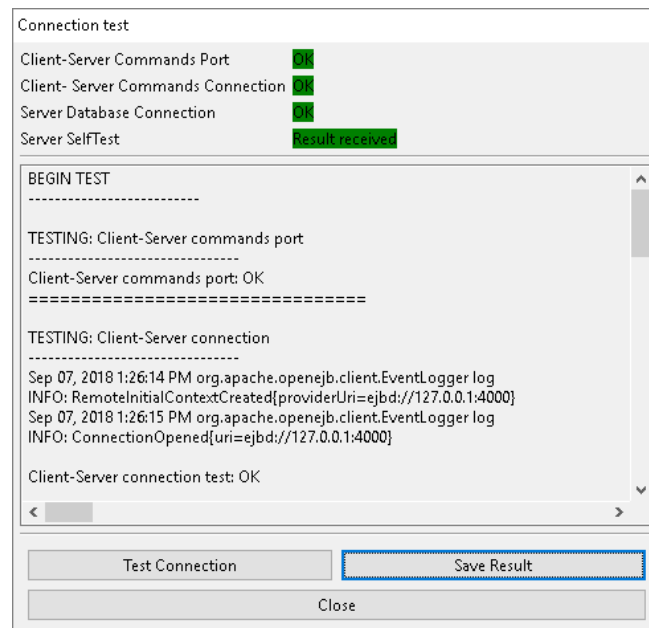


Figure 156: Client Component - Connection Test

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.

8.3 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.

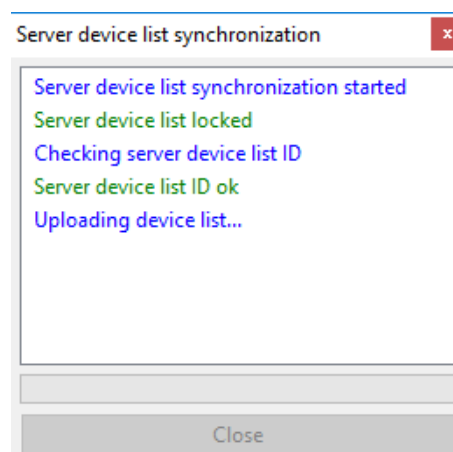


Figure 157: Client Component - Device List Synchronisation

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 "Unlock/Lock device list" via the menu item "Client/Server" in the client menu (see page 177). It is possible to use the padlock icon on top of the client tree panel.

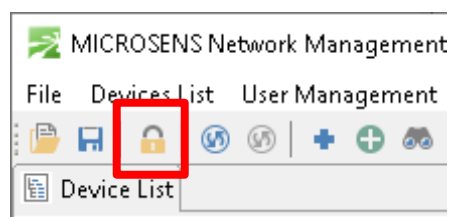


Figure 158: Client Component - Lock/Unlock Configuration

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.

Note:

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 "User Levels" on page 174).

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" (see page 177).

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 the "Open" menu item in the client menu. Lock the local client's device list afterwards (see page 177).

8.4 Main Menu (Client Component)

This chapter describes the client component's specific menu items. For all the menu items which are not described here, please refer to the chapter "NMP Professional: Getting started" on page 23.

8.4.1 Devices List

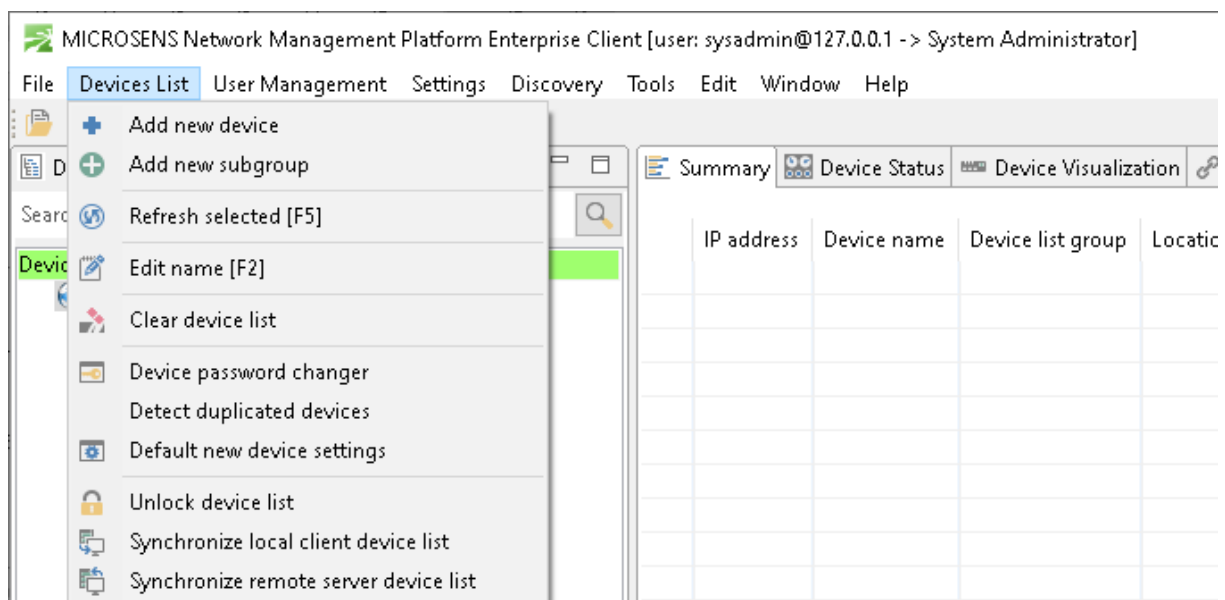


Figure 159: Client Component - Main Menu - Devices List

8.4.1.1 Lock/Unlock device list (Shortcut: None)

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.

8.4.1.2 Synchronize Local Client Device List (Shortcut: None)

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.

8.4.1.3 Synchronize Remote Server Device List (Shortcut: None)

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

Note:

The local device list will be overwritten.

8.4.2 User Management

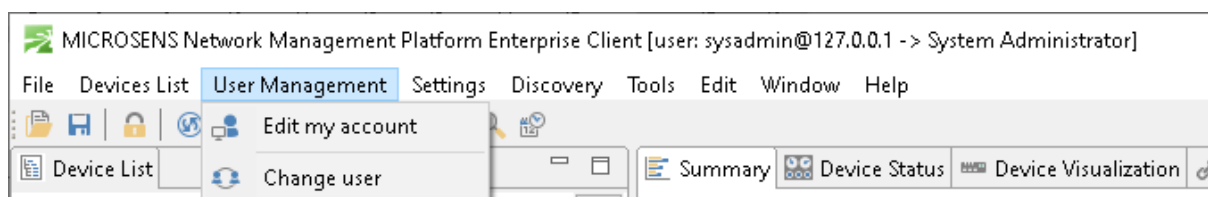


Figure 160: Client Component - Main Menu - User Management

8.4.2.1 Edit My Account (Shortcut: None)

This feature allows changing password and user email address of the current user. This option is available for all user types.

Figure 161: Client Component - Main Menu - User Management - Edit My Account

8.4.2.2 Change User (Shortcut: None)

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.

8.4.3 Settings

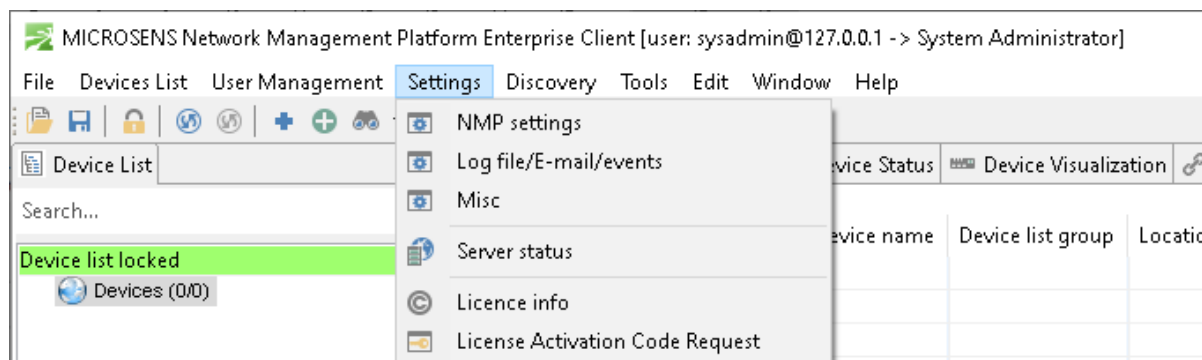


Figure 162: Client Component - Main Menu - Settings

8.4.3.1 Server Status

(Shortcut: None)

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

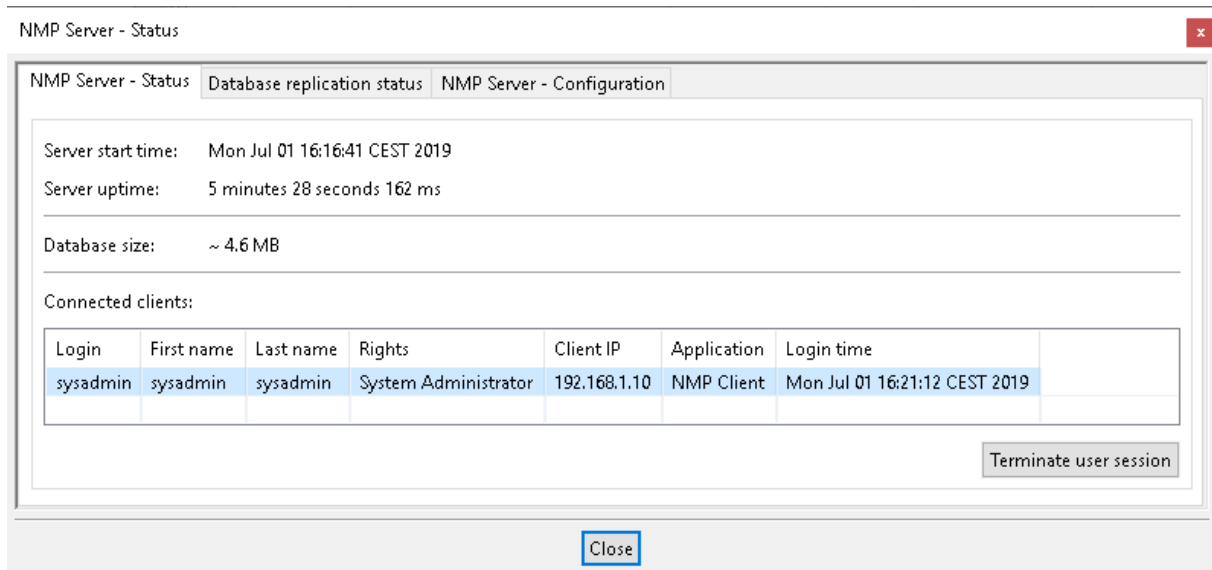


Figure 163: Client Component - Server Status

- "NMP 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.
- "Database replication status" contains information about the database's replication configuration and status.
- "NMP Server - Configuration" contains extensive information about the server's configuration.

Note:

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

8.4.3.2 Usage Right Activation Code Generator

This menu item opens the Licence Activation Code Generator.

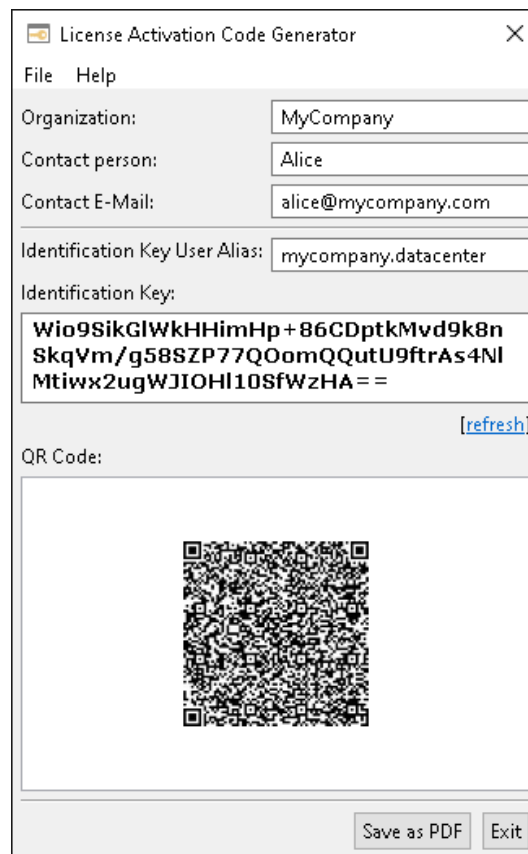


Figure 164: Licence Activation Code Generator

The code generator determines a unique system ID and generates the respective hash code for an identification key.

This identification key is necessary to apply for a valid licence key file from MICROSENS.

The input fields are optional.

Using a user alias for the identification key simplifies the licence key file handling when using multiple key files.

Click on the button "Save as PDF" to save the generated identification key file and send it to MICROSENS sales.

8.4.4 Tools

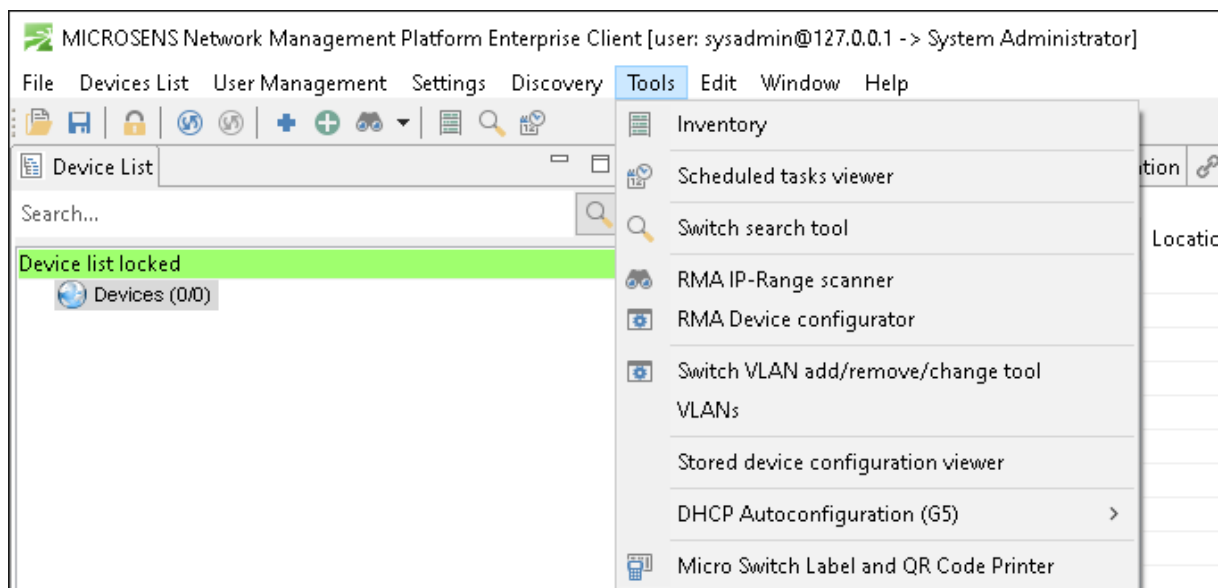


Figure 165: Client Component - Main Menu - Tools

8.4.4.1 Stored Device Configurations Viewer (Shortcut: None)

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

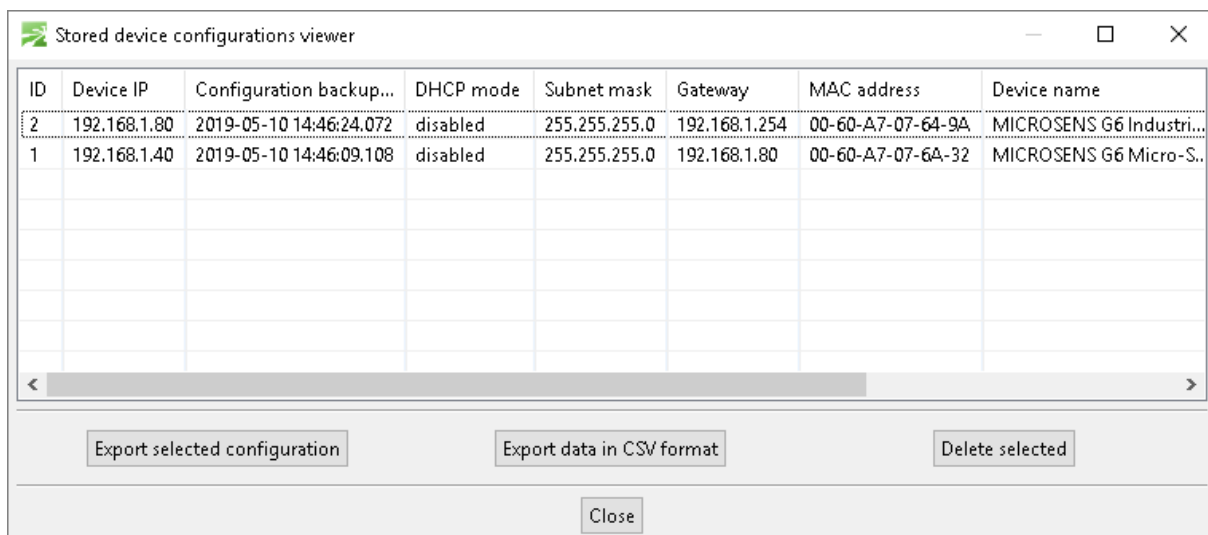


Figure 166: Client Component - Main Menu - Tools - Stored Device Configuration Viewer

Device configurations can be saved manually by using the "Device configuration load/save" menu item from the tree context menu (see page 73) or automatically by defining the "Scheduled configuration backup" task (see page 85).

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).

8.4.4.2 DHCP Autoconfiguration (G5) (Shortcut: None)

DHCP offers the setup of a device during the DHCP Request. The firmware of MICROSENS G6 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 page 188.

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.

8.4.5 Window

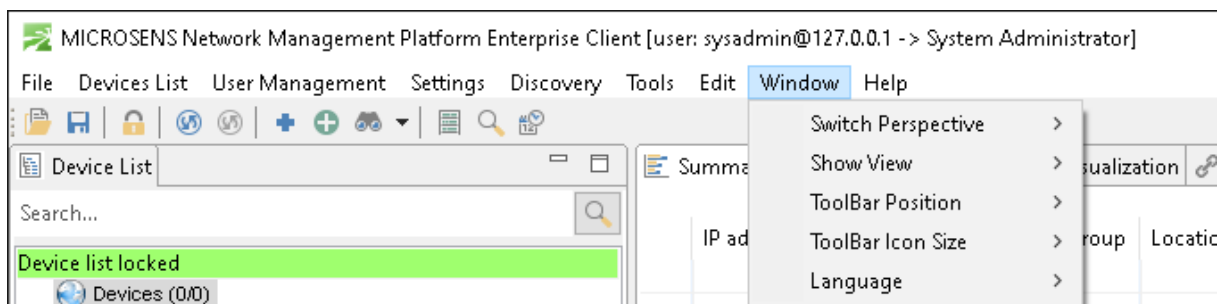


Figure 167: Client Component - Main Menu - Window

Note:

This menu item is visible with System Administrator access rights.

8.4.5.1 Switch Perspective (Shortcut: None)

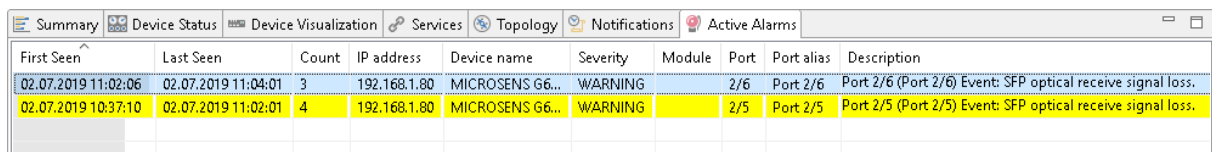
With System Administrator access rights it is possible to switch between two perspectives:

- **Network Administration:** Use this perspective to configure and survey the corporate network.
- **User Administration:** Use this perspective to manage NMP users. For more information about User Administration please refer to page 192.

8.5 Tabbed Data Panel

This chapter describes the client component's specific tabbed data panel items. For all the items which are not described here, please refer to the chapter "NMP Professional: Getting started" on page 23.

8.5.1 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 168: Client Component – 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 page 199.

8.6 Context Menu (Client Component)

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 the chapter "NMP Professional: Getting started" on page 71.

8.6.1 Device Context Menu

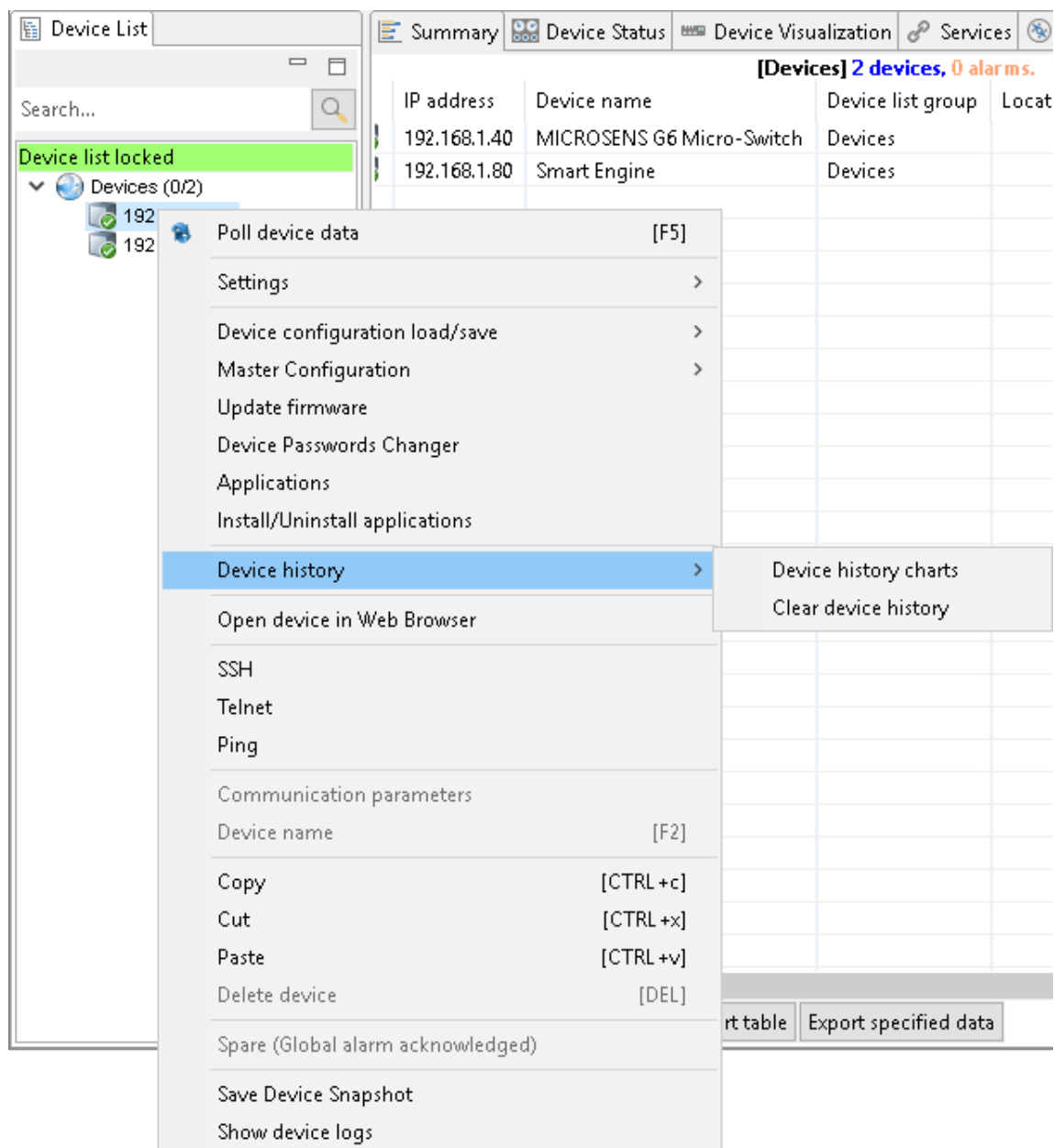


Figure 169: Client Component - Device Context Menu

8.6.1.1 Device History

(Shortcut: None)

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

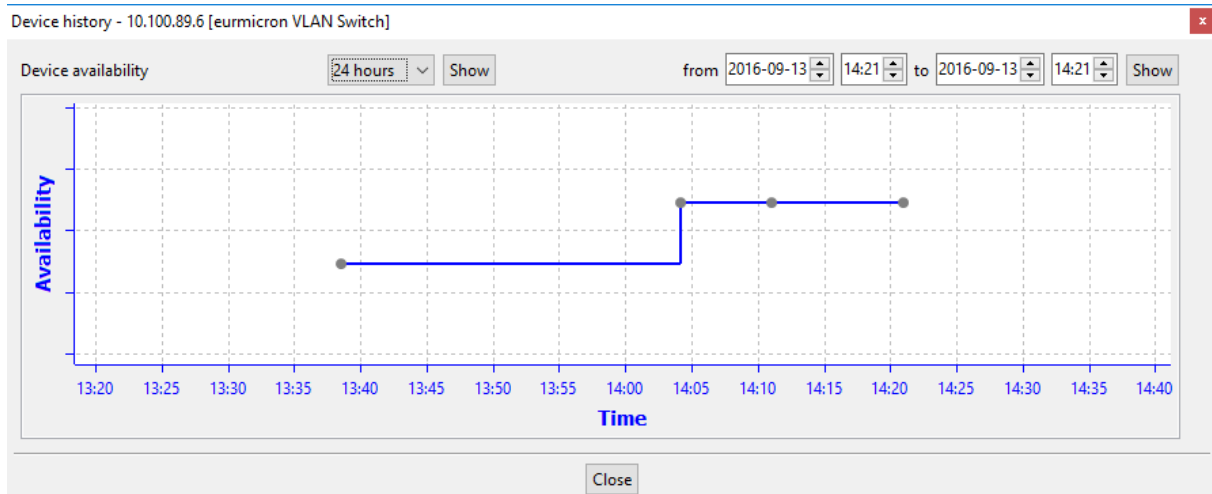


Figure 170: Client Component - Device History Chart

The tool allows determining the history of the last (predefined) time periods:

- 30 min.
- 1 hour
- 12 hours
- 24 hours (default)
- 1 week
- 1 moth
- 6 months
- 1 year
- All

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

To clear the device history click on the submenu item "Clear device history".

Note:

Clearing the device history requires login as administrator or system administrator.

Note:

The device history charts are available exclusively for MICROSENS Switches.

8.6.1.2 Show device logs (Shortcut: None)

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.

8.6.2 Group Context Menu

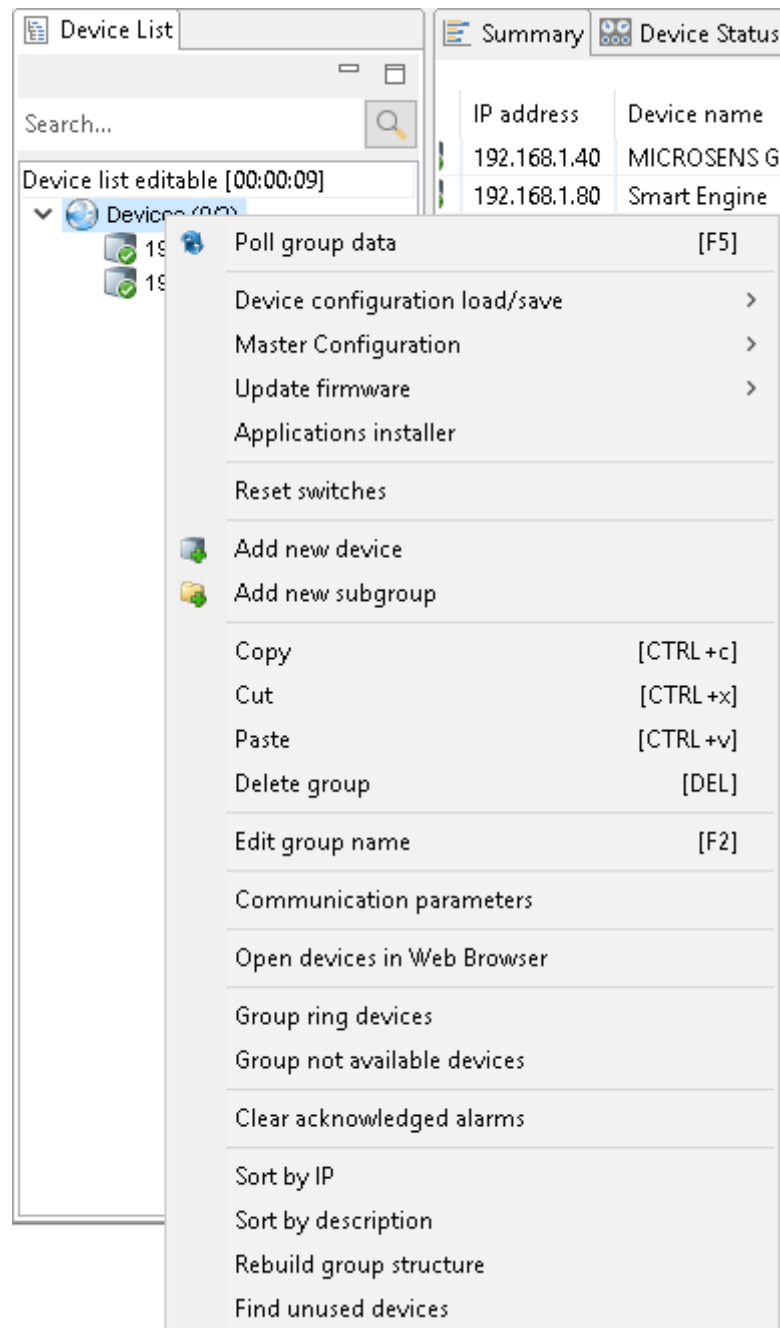
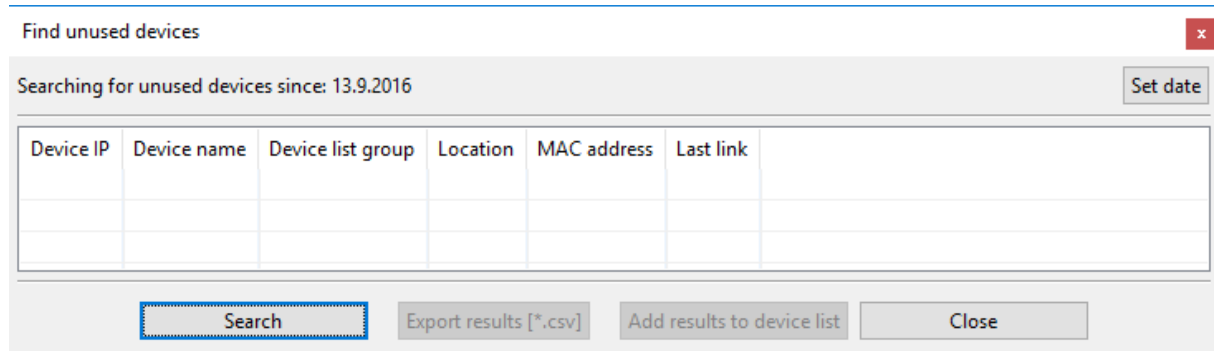


Figure 171: Client Component - Group Context Menu

8.6.2.1 Find unused devices**(Shortcut: None)**

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.



Find unused devices

Searching for unused devices since: 13.9.2016 Set date

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

Search Export results [*.csv] Add results to device list Close

Figure 172: Client Component- Find Unused Devices

All found "unused devices" are listed in a table which can be exported to a *.csv file.

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

9 NMP Enterprise: Working with the Client Component

This chapter contains appliance concepts of the client component.

9.1 Using DHCP Autoconfiguration of G5 Devices

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

The DHCP Autoconfiguration tool of NMP Client component allows using this function with MICROSENS G5 devices.

The DHCP Autoconfiguration is available via the main menu item "Tools" (see page 182).

9.1.1 Creating/Editing the Master Configuration File

In order to create the master configuration file, which can be used by the server instance for DHCP Autoconfiguration procedure, open the client, connect with the server and select the "Create configuration file" menu item. The client opens the dialogue for selecting a device from the device list tree.

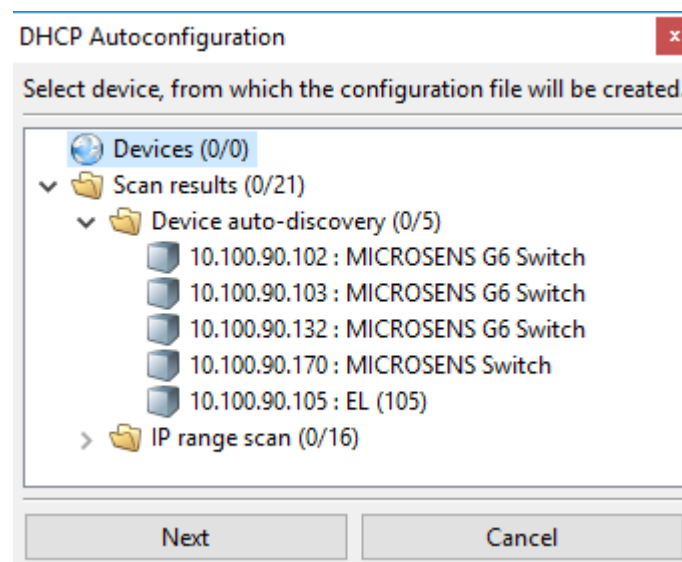


Figure 173: Client Component - DHCP Autoconfiguration - Device Selection

Select the device, which should be used to create the master configuration file ("configuration template"). After clicking the button "Next" the following "Master Configuration Editor" dialogue opens:

Master Configuration Editor

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:

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)

Save Load Close

Figure 174: Client Component - Master 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.

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_ppppvxyzzq.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.

9.1.2 Sending the DHCP Autoconfiguration Files to the Server

In order to send the DHCP Autoconfiguration and firmware file to server select "DHCP Autoconfiguration files" via "DHCP Autoconfiguration (G5)" under the main menu item "**Tools**".

The following file transfer dialogue appears:

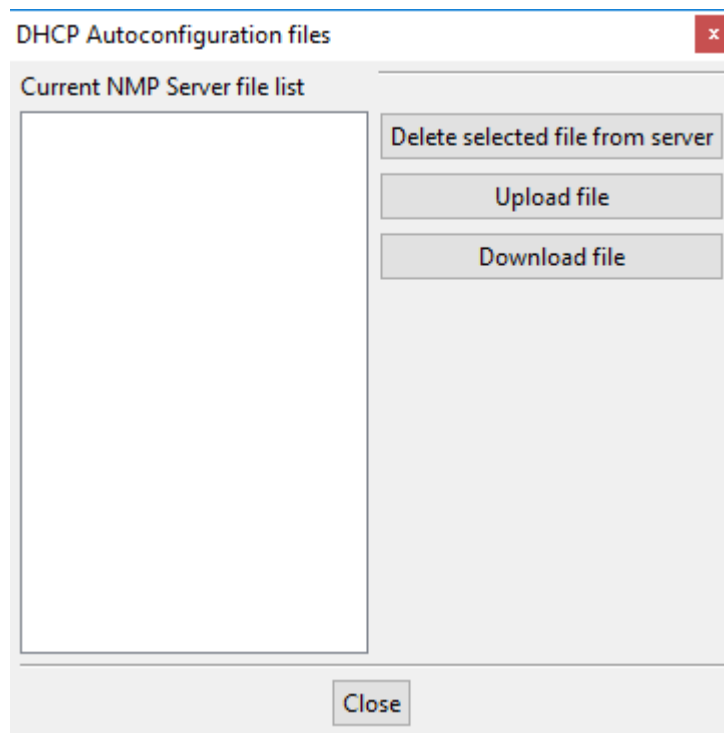


Figure 175: Client Component - DHCP Autoconfiguration Files

Use this window to

- upload new configuration files to server,
- download existing configuration files from the server or
- delete existing configuration files from the server.

Note:

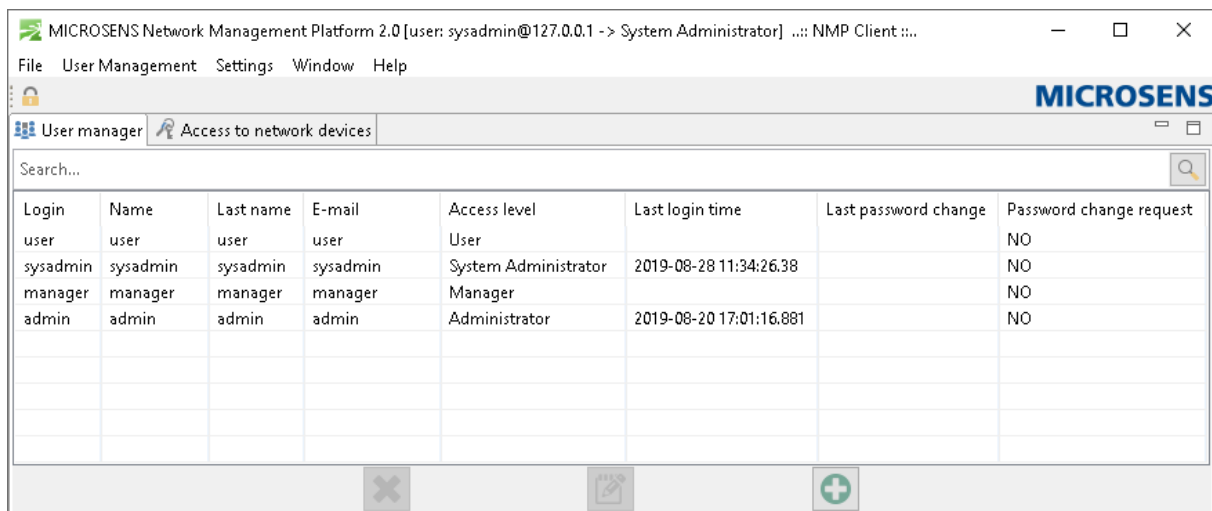
When not using the client to upload the configuration files to the server, the necessary files must be placed in the directory "**Server Data Directory/FTP/DHCPAutoconfigFiles**".

9.2 Using Perspective "User Administration"

Note:

The perspective "User Administration" is visible with System Administrator access rights.

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**.



The screenshot shows the MICROSENS Network Management Platform 2.0 Client Component window. The title bar indicates the user is 'sysadmin@127.0.0.1 -> System Administrator'. The menu bar includes File, User Management, Settings, Window, and Help. The 'User manager' tab is active, showing a table of user accounts. A search bar is located above the table. The table has columns for Login, Name, Last name, E-mail, Access level, Last login time, Last password change, and Password change request. The data shows three users: 'user' (User), 'sysadmin' (System Administrator), and 'manager' (Manager). The 'admin' user is also listed with an 'Administrator' access level.

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	2019-08-28 11:34:26.38		NO
manager	manager	manager	manager	Manager			NO
admin	admin	admin	admin	Administrator	2019-08-20 17:01:16.881		NO

Figure 176: Client Component - Perspective "User Administration"

Note:

All menu items are described in the section "Main Menu (Client Component)" on page 177.


To return to the perspective "Network Administration" click on **Window -> Switch Perspective -> Network Administration** in the main menu.

The User Administration dialogue contains three tabs:

- **User Manager:** Use this view to add, modify or delete NMP user accounts.
- **Access to Network Devices:** Use this view to assign access rights for the respective NMP user account.

9.2.1 User Manager

Adding a new user account

To add a new user account click on the icon "New user" () at the bottom pane.

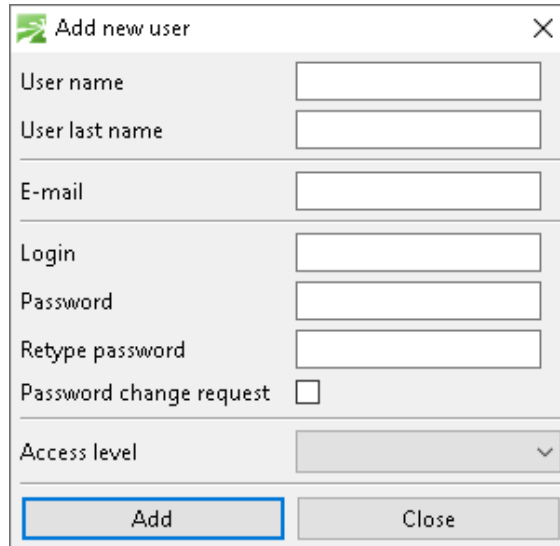
A dialog box titled "Add new user" with a close button (X) in the top right corner. It contains several input fields: "User name", "User last name", "E-mail", "Login", "Password", "Retype password", and a checkbox for "Password change request". Below these is a dropdown menu for "Access level". At the bottom are two buttons: "Add" (highlighted with a blue border) and "Close".

Figure 177: Client Component - 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.

Editing and deleting an existing user account

To edit an existing user account select the respective table entry and click on the button "Edit user" ().

To delete an existing user account select the respective table entry in the view "User Manager" and click on the button "Remove user" ().

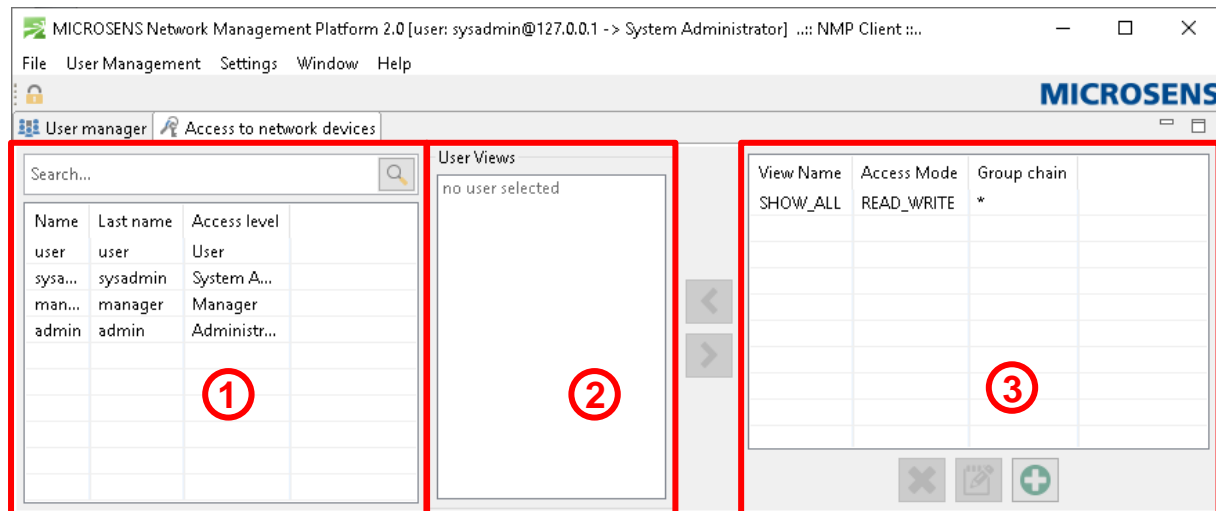
Note:

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.

9.2.2 Access to Network Devices

Change to the view "Access to Network Devices" to define and assign network access rights.

Figure 182: Client Component - Perspective "User Administration" -






Access to Network Devices

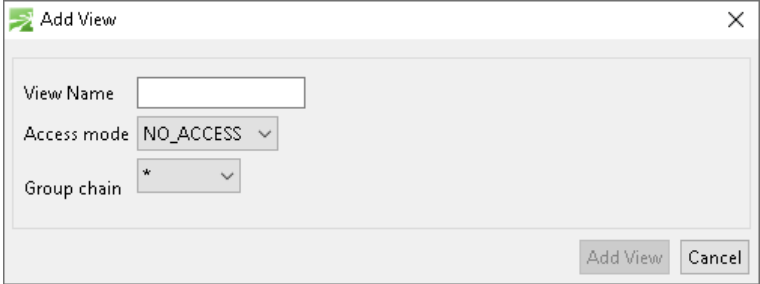
The "Access to Network Devices" view consists of three main elements:



1. List of existing NMP user accounts.
2. Assigned access view for the account selected in the left-hand pane.
3. List of defined access views.

Creating New Access View

To create a new access view, follow these steps:




Step	Description
1	<p>In the main menu toolbar click on the "lock" symbol to unlock the NMP configuration.</p> <p> - Configuration is locked.</p> <p> - Configuration is unlocked.</p> <p>Confirm the upcoming notice dialogue.</p>
2	<p>Click on the button "Define New View" () at the bottom of the right-hand pane.</p>


Step	Description
3	<p data-bbox="300 365 1185 398">In the opening dialogue enter the specific access view data.</p> <div data-bbox="472 439 1235 721">  </div> <p data-bbox="300 745 1406 813">Figure 178: Client Component - Perspective "User Administration" - Access to Network Devices - Add Access View</p> <ul data-bbox="300 848 1406 1301" style="list-style-type: none"> • 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: <ul data-bbox="347 1021 1406 1178" style="list-style-type: none"> • 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. <p data-bbox="347 1323 1406 1391">The access mode is applied for the last node of the group chain. The group chain can end with one of the following entries:</p> <ul data-bbox="347 1406 1406 1637" style="list-style-type: none"> • "" (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). <p data-bbox="395 1653 1406 1794">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]".</p> <p data-bbox="300 1816 1406 2018">Note: The view "SHOW_ALL" with "READ_WRITE" access to the complete device list is predefined, non-erasable and by default associated with all NMP 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.</p>

Step	Description
	Note: For more information about dealing with group chains please refer to page 197.
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.

Assigning Access View to NMP User Account

To assign an existing access view to an NMP user account, follow these steps:

Step	Description
1	In the main menu toolbar click on the "lock" symbol to unlock the NMP configuration.  - Configuration is locked.  - Configuration is unlocked. Confirm the upcoming notice dialogue.
2	In the left-hand pane select an existing NMP 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.

Step	Description
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.

9.2.3 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 NMP 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:

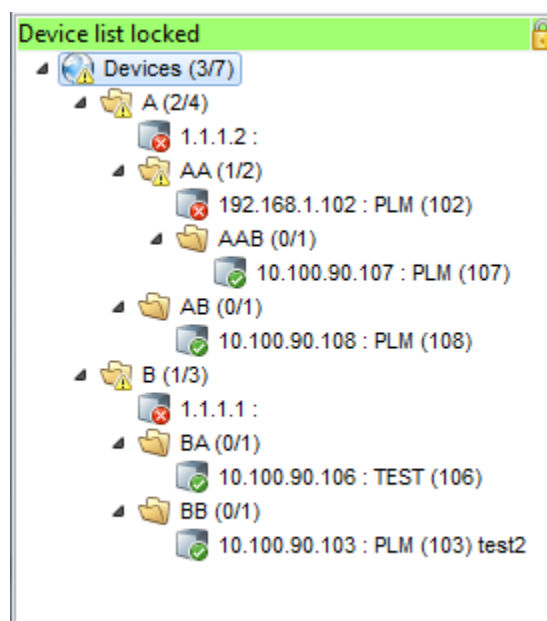


Figure 179: Client Component - Basic Tree View

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 180: Client Component - Perspective "User Administration" - Access to Network Devices - Access Views

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:

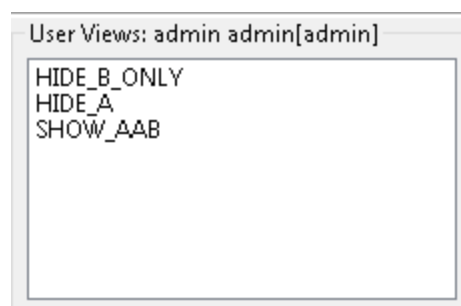


Figure 181: Client Component - Perspective "User Administration" - Access to Network Devices - User Views (Administrator)

After closing this dialogue the administrator gets the following device list tree view with restricted node access:

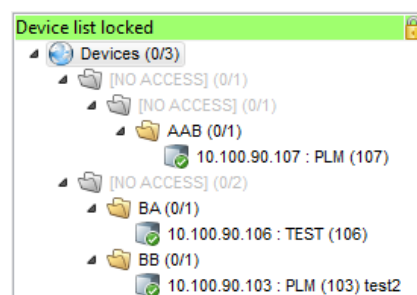


Figure 182: Client Component - Restricted Tree View

With restricted access to the device tree list it is not possible to delete restricted nodes or even visible nodes with restricted children. NMP 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 sysad
	03.06.2015 08:45:35	03.06.2015 08:45	System	INFO	notice	User	sysadmin sysad
	03.06.2015 08:45:35	03.06.2015 08:45	System	INFO	notice	User	sysadmin sysad
	03.06.2015 08:42:07	03.06.2015 08:42	System	INFO	notice	User	sysadmin sysad
	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 sysad
	03.06.2015 08:40:06	03.06.2015 08:40	System	INFO	notice	User	admin admin

Figure 183: Client Component - Restricted Notification Tab

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.

9.3 Using Active Alarms

The tab "Active Alarms" is helpful to view some important SNMP traps of managed devices at first glance.

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 184: Client Component – Tabbed Data Panel – Active Alarms

Note:

The tab "Active Alarms" shows notifications of MICROSENS G6 devices as well as of MSP1000 and MSP3000 devices.

9.3.1 Prerequisites

To use "Active Alarms" with NMP client component the following conditions are a must have:

- The managed device is a MICROSENS MSP1000 with NM3 module or a G6 switch with firmware version 10.7.4 and above. If the managed devices do

not include one of these device types, the NMP client component hides the tab "Active Alarms".

- The managed device is configured to send SNMP traps to the connected NMP server 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).

#	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	<input checked="" type="checkbox"/>
	log debug events only	<input type="checkbox"/>

add table entry unique value for alias +

Figure 185: Web Manager - SNMP Target for Active Alarms

Note:

Be sure to enter the IP address of the NMP server component as SNMP target's host address (see page 134).

- The SNMP trap listener has to be enabled on the NMP server component (see page 134).

9.3.2 Mode of Operation

When all prerequisites are met "Active Alarms" operate as follows:

- Every MSP1000 or G6 device contains pre-defined SNMP events with i.e. name, event, group, relevance, severity, trap options etc.
- 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 NMP server component receives this trap and saves it in its database.
4. At a regular interval the NMP client component 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.

Note:

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.

10 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.

11 List of Figures

Figure 1: Installation - Product Selection	13
Figure 2: Installation - Choose NMP Components.....	14
Figure 3: Installation - Choose Users	15
Figure 4: Installation - Choose Install Location	16
Figure 5: Licence Key File Selection	19
Figure 6: Data Migration from NMP v1.....	21
Figure 7: NMP Professional - Login.....	21
Figure 8: NMP Professional - Main Window.....	23
Figure 9: NMP Professional - Main Menu - File	24
Figure 10: NMP Professional - Main Menu - Devices List.....	25
Figure 11: NMP Professional - New Device - IP Address	25
Figure 12: NMP Professional - New Device - Authorisation	26
Figure 13: NMP Professional - New Device - Communication	27
Figure 14: NMP Professional - Add New Subgroup.....	27
Figure 15: NMP Professional - Edit Device Name.....	28
Figure 16: NMP Professional - Edit Group Name	29
Figure 17: NMP Professional - Device Password Changer	30
Figure 18: NMP Professional - Detect Duplicated Devices	31
Figure 19: NMP Professional - Default New Device Settings - SNMPv3	32
Figure 20: NMP Professional - Default New Device Settings - SNMPv1/v2c.....	33
Figure 21: NMP Professional - Default New Device Settings - FTP	33
Figure 22: NMP Professional - Default New Device Settings - Legacy Products.....	33
Figure 23: NMP Professional - Default New Device Settings - G6 Switches	34
Figure 24: NMP Professional - Default New Device Settings - Communication Parameters	34
Figure 25: NMP Professional - Main Menu - Settings.....	35
Figure 26: NMP Professional - Settings - Application Settings	35
Figure 27: NMP Professional - Settings - Security Settings.....	37
Figure 28: NMP Professional - Settings - Event Logging	38
Figure 29: NMP Professional - Settings - E-Mail Settings.....	39
Figure 30: NMP Professional - Settings - Alarm Indicators.....	40
Figure 31: NMP Professional - Alarm Indicator (Example)	40
Figure 32: NMP Professional - Settings - Sound Alarm.....	41
Figure 33: NMP Professional - Settings - Misc.....	42
Figure 34: NMP Professional - Licensing Information	42
Figure 35: NMP Professional - Main Menu - Discovery	43
Figure 36: NMP Professional - Device Auto Discovery	44
Figure 37: NMP Professional - SNMP-based Auto Discovery	45
Figure 38: NMP Professional - MSP 1000 Platform IP Discovery	45
Figure 39: NMP Professional - Device IP-Range-Scan	46
Figure 40: NMP Professional - Main Menu - Tools	47
Figure 41: NMP Professional - Inventory	47
Figure 42: NMP Professional - Scheduled Task Viewer	48
Figure 43: NMP Professional - Switch Search Tool	49
Figure 44: NMP Professional - RMA IP Range Scanner	50
Figure 45: NMP Professional - RMA Device configurator	51
Figure 46: NMP Professional - VLAN Add/Remove/Change	52
Figure 47: NMP Professional - VLANs (Example)	53
Figure 48: NMP Professional - VLANS tool with Topology Manager	54
Figure 49: NMP Professional - Micro Switch Label and QR Code Printer	55
Figure 50: NMP Professional - Main Menu - Edit.....	56
Figure 51: NMP Professional - Main Menu - Window	57
Figure 52: NMP Professional - Tabbed Data Panel - Close Icon	57
Figure 53: NMP Professional - Toolbar left.....	58

Figure 54: NMP Professional - Main Menu - Help	58
Figure 55: NMP Professional - About	59
Figure 56: NMP Professional - Main Menu Toolbar	60
Figure 57: NMP Professional - Device List Tree View.....	61
Figure 58: NMP Professional - Tabbed Data Panel	63
Figure 59: NMP Professional - Tabbed Data Panel - Placing the Tabs	64
Figure 60: NMP Professional - Tabbed Data Panel - Summary	64
Figure 61: NMP Professional - Tabbed Data Panel - Summary - Column Select	65
Figure 62: NMP Professional - Tabbed Data Panel - Summary - Export Specified Data	66
Figure 63: NMP Professional - Tabbed Data Panel - Device Status.....	67
Figure 64: NMP Professional - Tabbed Data Panel - Device Visualization (Micro Switch G6).....	68
Figure 65: NMP Professional - Tabbed Data Panel - Device Visualisation (MSP 1000)	69
Figure 66: NMP Professional - Tabbed Data Panel - Services	69
Figure 67: NMP Professional - Tabbed Data Panel - Topology	70
Figure 68: NMP Professional - Tabbed Data Panel - Notifications.....	71
Figure 69: NMP Professional - Device Context Menu.....	72
Figure 70: NMP Professional - Device Context Menu - Device Password Changer.....	74
Figure 71: NMP Professional - Group Context Menu.....	77
Figure 72: NMP Professional - Device List Tree View - Ring Device Group	80
Figure 73: NMP Professional - Device List Tree View - Alarm List	80
Figure 74: NMP Professional - Device Auto Discovery	82
Figure 75: NMP Professional - Device Context Menu - Device Configuration.....	84
Figure 76: NMP Professional - Device Context Menu - Configuration Export.....	85
Figure 77: NMP Professional - Device Context Menu - Configuration Export - Scheduler...86	
Figure 78: NMP Professional - Device Context Menu - Configuration Import	87
Figure 79: NMP Professional - Device Context Menu - Master Configuration - Apply CLI Script	88
Figure 80: NMP Professional - Device Context Menu - Master Configuration - CLI Scripts	89
Figure 81: NMP Professional - Device Context Menu - Master Configuration - NMP Text Editor	90
Figure 82: NMP Professional - Device Context Menu - Master Configuration (G5 and older).....	91
Figure 83: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Example	92
Figure 84: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Buttons.....	92
Figure 85: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Select Group/Device.....	93
Figure 86: NMP Professional - Device Context Menu - Master Configuration (G5 and older) - Apply to Devices.....	93
Figure 87: NMP Professional - Device Context Menu - Update Firmware.....	94
Figure 88: NMP Professional - Device Context Menu - Update Firmware - Select FTP Server	95
Figure 89: NMP Professional - Device Context Menu - Update Firmware - Select File	95
Figure 90: NMP Professional - Device Context Menu - Update Firmware - Progress	96
Figure 91: NMP Professional - Device Context Menu - Update Firmware - Scheduler.....	96
Figure 92: NMP Professional - Device Context Menu - Applications (Example)	98
Figure 93: NMP Professional - Application Management - Configuration Example	98
Figure 94: NMP Professional - Application Management - Available Applications.....	99
Figure 95: NMP Professional - Group Context Menu - Applications Installer	100
Figure 96: NMP Professional - Group Context Menu - Applications Installer - Select Apps.....	100
Figure 97: NMP Professional - Tabbed Data Panel - Services - Details.....	101
Figure 98: NMP Professional - Tabbed Data Panel - Services - Service Manager - Network View	102
Figure 99: NMP Professional - Tabbed Data Panel - Services - Service Manager - Element.....	104
Figure 100: NMP Professional - Tabbed Data Panel - Services - Service Manager - Details View	105

Figure 101: NMP Professional - Tabbed Data Panel - Services - Cable Manager.....	106
Figure 102: NMP Professional - Tabbed Data Panel - Services - Cable Manager - Cable Creator	107
Figure 103: NMP Professional - Tabbed Data Panel - Topology - Standard Dialogue	108
Figure 104: NMP Professional - Tabbed Data Panel - Topology - Adding Items manually	112
Figure 105: NMP Professional - Tabbed Data Panel - Topology - Adding Multiple Anchors	113
Figure 106: NMP Professional - Tabbed Data Panel - Topology - Link Port Connection....	114
Figure 107: NMP Professional - Tabbed Data Panel - Topology - Link Parameters Tooltip	115
Figure 108: NMP Professional - Tabbed Data Panel - Topology - Link Anchor Context Menu	115
Figure 109: NMP Professional - Tabbed Data Panel - Topology - Link Parameters.....	116
Figure 110: NMP Professional - Tabbed Data Panel - Topology - Off-Map Connections - Context Menu	117
Figure 111: NMP Professional - Tabbed Data Panel - Topology - Off-Map Connections ...	118
Figure 112: NMP Professional - Tabbed Data Panel - Notifications	119
Figure 113: NMP Professional - Tabbed Data Panel - Notification and Device Status	121
Figure 114: NMP Professional - Tabbed Data Panel - Notifications - Event Configuration	122
Figure 115: NMP Professional - Tabbed Data Panel - Notifications - Filter.....	123
Figure 116: NMP Professional - Tabbed Data Panel - Events - ACK Column Detail	124
Figure 117: NMP Professional - Device Tree List View - Industrial Ring Errors.....	125
Figure 118: Data Migration from NMP v1	127
Figure 119: Server Manager - Main Window	128
Figure 120: Server Manager - Main Menu - Server.....	129
Figure 121: Server Manager - Main Menu - Window	130
Figure 122: Server Manager - System Tray Icon.....	130
Figure 123: Server Manager - Main Menu - Tools.....	130
Figure 124: Server Manager - Main Menu - Help.....	131
Figure 125: Server Manager - Licensing Information	131
Figure 126: Licence Activation Code Generator.....	132
Figure 127: Server Manager - About	133
Figure 128: Server Manager - Tabbed Server Configuration Panel - Server Settings.....	134
Figure 129: Server Manager - Tabbed Server Configuration Panel - Server Settings - Set Password	135
Figure 130: Server Manager - Tabbed Server Configuration Panel - Client Authentication Settings	136
Figure 131: Server Manager - Tabbed Server Configuration Panel - Syslog/Logs/Events	138
Figure 132: Server Manager - Tabbed Server Configuration Panel - Database Backup/Restore	141
Figure 133: Server Manager - Tabbed Server Configuration Panel - Database Replication	142
Figure 134: Server Manager - Tabbed Server Configuration Panel - Email Notification ...	143
Figure 135: Server Manager - Tabbed Server Configuration Panel - SNMP Agent	144
Figure 136: Server Manager - Server Control Buttons	146
Figure 137: Server Manager - Status Text Field.....	146
Figure 138: Server as a Service - Local Policy	148
Figure 139: Server as a Service - Local Policy - Properties	148
Figure 140: Server Manager - Main Menu - Server - Service Control	149
Figure 141: Server Manager - Service Control	150
Figure 142: Server as a Service - Windows Services Dialogue	151
Figure 143: Server as a Service - General	152
Figure 144: Server Manager - Database Replication Setting	154
Figure 145: Server Manager - Database Replication - Out of Sync Message	155
Figure 146: Database Replication - Redundant Operation	157
Figure 147: Database Replication - Master Server Failure	158
Figure 148: Database Replication - Master Server Restart	159
Figure 149: Database Replication - Slave Server Failure	160
Figure 150: Database Replication - Slave Server Restart	161

Figure 151: Database Replication - Link Failure	162
Figure 152: Database Replication - Link Restored	163
Figure 153: Server Component- Switch DHCP Auto Configuration	169
Figure 154: Client Component - Login Dialogue	172
Figure 155: Data Migration from NMP v1	173
Figure 156: Client Component - Connection Test	175
Figure 157: Client Component - Device List Synchronisation	175
Figure 158: Client Component - Lock/Unlock Configuration	176
Figure 159: Client Component - Main Menu - Devices List.....	177
Figure 160: Client Component - Main Menu - User Management	178
Figure 161: Client Component - Main Menu - User Management - Edit My Account	178
Figure 162: Client Component - Main Menu - Settings.....	178
Figure 163: Client Component - Server Status	179
Figure 164: Licence Activation Code Generator.....	180
Figure 165: Client Component - Main Menu - Tools	181
Figure 166: Client Component - Main Menu - Tools - Stored Device Config Viewer	181
Figure 167: Client Component - Main Menu - Window	182
Figure 168: Client Component - Tabbed Data Panel - Active Alarms.....	183
Figure 169: Client Component - Device Context Menu	184
Figure 170: Client Component - Device History Chart.....	185
Figure 171: Client Component - Group Context Menu	186
Figure 172: Client Component- Find Unused Devices.....	187
Figure 173: Client Component - DHCP Autoconfiguration - Device Selection.....	188
Figure 174: Client Component - Master Configuration Editor	189
Figure 175: Client Component - DHCP Autoconfiguration Files.....	191
Figure 176: Client Component - Perspective "User Administration"	192
Figure 177: Client Component - User Administration - Add User	193
Figure 178: Client Component - Perspective "User Administration" - Access to Network Devices - Add Access View	195
Figure 179: Client Component - Basic Tree View	197
Figure 180: Client Component - Perspective "User Administration" - Access to Network Devices - Access Views	198
Figure 181: Client Component - Perspective "User Administration" - Access to Network Devices - User Views (Administrator).....	198
Figure 182: Client Component - Restricted Tree View.....	198
Figure 183: Client Component - Restricted Notification Tab.....	199
Figure 184: Client Component - Tabbed Data Panel - Active Alarms.....	199
Figure 185: Web Manager - SNMP Target for Active Alarms	200

Disclaimer

All information in this document is provided 'as is' and 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 consecutive damage.

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

©2021 MICROSENS GmbH & Co. KG, Kueferstr. 16, 59067 Hamm, Germany.

NMP is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

All rights reserved. This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG.

Document ID: PM-19002_2021-05-20