MICROSENS

Network Management Platform (NMP) Web+

User Manual

NMP

Web+

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

Table of Contents

Chapter 1. Introduction

Management of devices includes monitoring, configuration and administration from a remote site. The Network Management Platform (NMP) is a powerful software that assists the network administrator with these tasks.

NMP gives comprehensive management access to all manageable devices with its enhanced SNMP-based capabilities. The discovery feature detects all MICROSENS devices automatically. MICROSENS devices that do not have an IP address are also shown and can be configured.

Please bear in mind that NMP is only compatible with MICROSENS devices (G7 and prior, MSP3000, MSP1000). NMP might not be able to identify devices made by other manufacturers.

Due to the ongoing product development of MICROSENS devices and the NMP software, it is possible that NMP does not yet recognise the latest generation of a MICROSENS device. In this instance, please contact MICROSENS support for more assistance.

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 or a database and is used for monitoring the network status.

1.1.2. Network Monitoring

The current state of all active, controllable devices in the network may be automatically obtained using the device list file used for network management as a reference. The status is displayed using a graphical interface.

1.1.3. Network Configuration

The hardware configuration of a manageable device, such as port configuration or 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 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. NMP Web+ functions

NMP offers comprehensive tools for convenient and efficient network management. It offers support for these tools as follows:

NMP Web+ 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:

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

> ℹ For more information about these tools see Section 4.4.4.

NMP Web+ consists of two components:

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

> ℹ The client is **exclusively** for **server configuration**, not device management.

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

1.3. Scope of this User Manual

This user manual refers to NMP Web+ and covers its installation and use. Whereas Chapter 2 and Chapter 3 deal with installation and licensing, Chapter 4 relates to the server configuration and usage of NMP Web+.

Chapter 2. Install the Application

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

You need administrative rights as a prerequisite to install the application's Server Manager.

To use the Server Manager, a valid licence key file is required. See Chapter 3 for further information.

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

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.

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

2.1. Difference between Installation Files for Windows® and Linux

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

	Windows®	**Linux**
Installation files	1x NMP installation file	1x NMP installation file
File format	Standard Windows® `.exe` file	compressed tarball files (`.tar.gz`)
Installation process	via file explorer	via Linux CLI or archive management application

2.2. System Requirements

The application is designed to run on personal computers or servers with the following minimum requirements. These requirements are defined for dedicated systems.

The application requires a 64-bit operating system.

Operating system

- Windows 10, Debian Linux 11
  (NMP Web+)
- Windows Server 2016, Debian Linux 11
  (NMP Web+, server component)

RAM

- 8 GB (NMP Web+, server component)

Free disk space

- 2 GB + 1 GB/1.000 additional managed devices
  (NMP Enterprise, server component)

CPU

- 3 GHz, typically 4-6 Core CPU
  (current Xeon Server CPU; multi-Core i7/i5 Desktop CPU)
  (NMP Web+, server component),

Display resolution

- at least 1280*1024
- recommended: 1920*1080

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

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

2.3. Additional Requirements for Server Access

"Client-side" operations are those carried out by the client in a client-server connection in a computer network.

2.3.1. Client Component

There is no need for any special configuration; simply enter the server name and port into a web browser to access the server location.

> No additional licence key file is necessary to use the client component for server access. During the login process, the client component checks to determine whether the server licence key file is valid.

2.4. Port and Firewall Settings

To ensure proper operation of NMP Web+ in the corporate network, the following port and firewall settings are mandatory:

Port	Protocols	Description
22	TCP/IP, SSH	SSH communication between application and device
25	TCP/IP, SNMP	Used for email notification: • can be enabled or disabled • default value, configurable
67	UDP/IP, BOOTP	Bootstrap protocol for application and device (local server port): • application listens on this port’s BootP frames

Port	Protocols	Description
68	UDP/IP, BOOTP	Bootstrap protocol for application and device (remote client port): • application sends BootP configuration frames
161	UDP/IP, SNMP	Used by the SNMP trap receiver for application and device: • application initiates the communication with devices • application listens on this port for SNMP traps • can be enabled or disabled • default value, configurable
162	UDP/IP, SNMP	Used to forward SNMP trap to the northbound interfaces to a higher level management system: • if receiving SNMP traps is enabled, application listens on this port for SNMP Traps • can be enabled or disabled • default value, configurable
514	UDP/IP, Syslog	Syslog server on server component: • used to receive Syslog messages • can be enabled or disabled • default value, configurable Syslog client on server component: • used to send Syslog messages to an external SYSLOG server • can be enabled or disabled
1025	UDP/IP, MICROSENS proprietary protocol	Used for device communication for G5 and older switches: • application initiates the communication with devices
1025	TCP/IP, HTTPS	Used for device communication with new generation switches (Micro Switch G6, Industrial Switch G6, NM3 modules): • application initiates the communication with devices
1812	UDP/IP (PAP, CHAP)	Used to communicate with a RADIUS Sever: • can be enabled/disabled • default value, configurable

Port	Protocols	Description
4000	TCP/IP	Communication between NMP server and NMP client component: • send server-client commands in both directions • also used when replication mode is enabled • default value, configurable
4001	TCP/IP, FTPS (FTP over SSL)	Communication between server and client component: • default value, configurable
4002	TCP/IP	Used for database access: • database server on server • default value, configurable
4003	TCP/IP	Communication between server and client component: • used exclusively with MSP1000 devices • forwarding data from MSP1000 platform to client via server • default value, not configurable
4177	TCP/IP	Used by master and slave servers (replication server port): • database replication mode • can be enabled or disabled • default value, configurable
5555	TCP/IP, MICROSENS proprietary protocol	Used for communication with NM1 and NM2 modules for application and device: • management modules for MSP1000 access platform
8080	TCP/IP, HTTP	Web server on server component: • can be enabled or disabled • default value, configurable
8340	UDP/IP, MICROSENS proprietary protocol	Used by IP request listener for application and device (local port): • application listens on this port for special UDP packets (IP requests) • used for device IP configuration of all generations of MICROSENS switches and NM3 modules

Port	Protocols	Description
8341	UDP/IP, MICROSENS proprietary protocol	Used for IP configuration for application and device (remote G5 Port): • application sends IP configuration packets on this port • used for device IP configuration of all generations of MICROSENS switches and NM3 modules
8342	UDP/IP, MICROSENS proprietary protocol	Listening for RING error frames for application and device (local port): • application listens on this port for special UDP packets (RING error frames)
8443	TCP/IP, HTTPS	Web server on server component: • can be enabled or disabled • default value, configurable

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

2.5. Installation on Windows® Operating Systems

2.5.1. Run the Install Executable

The naming convention of the installer is as follows:

- MICROSENS_<application>Installer_v<x.y.z>_win64.exe

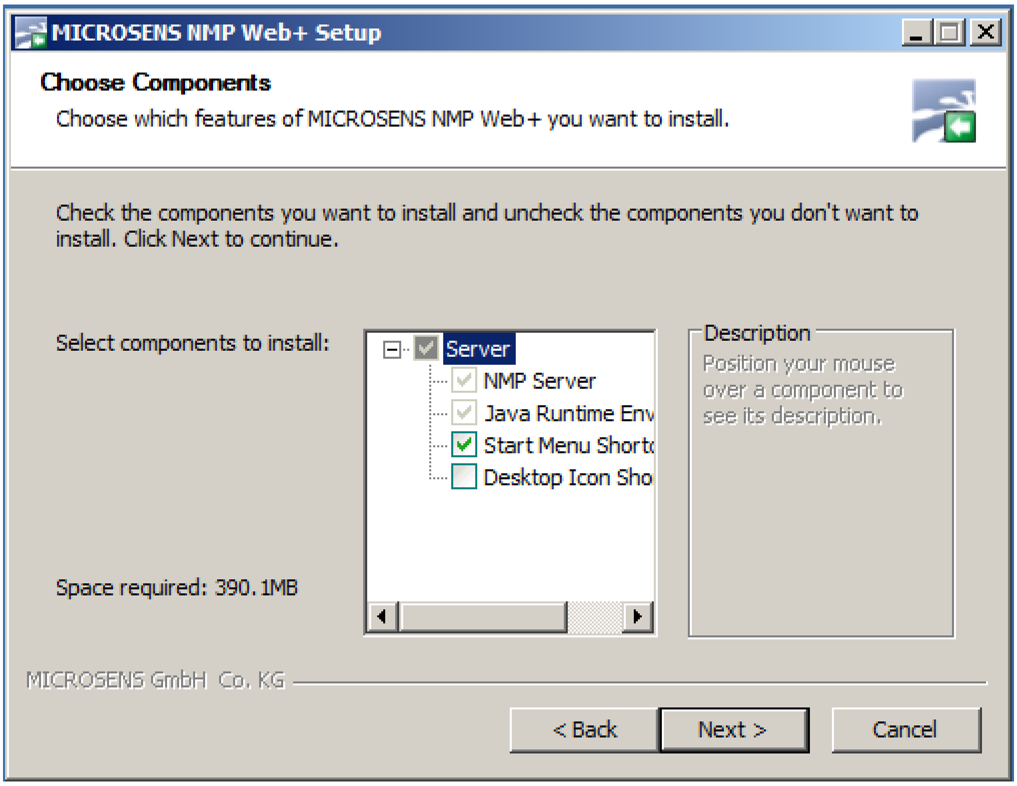
On the welcome screen click the button Next in order to enter the licence agreement dialogue.

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

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

The installation screen will show you the application to be installed. Click the button Next to continue.

2.5.2. Choose Components



MICROSENS NMP Web+ Setup

Choose Components

Choose which features of MICROSENS NMP Web+ you want to install.

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

Select components to install:

- ☑ Server
  - ☑ NMP Server
  - ☑ Java Runtime Env
  - ☑ Start Menu Shortc
  - □ Desktop Icon Sho

Space required: 390.1MB

Description

Position your mouse over a component to see its description.

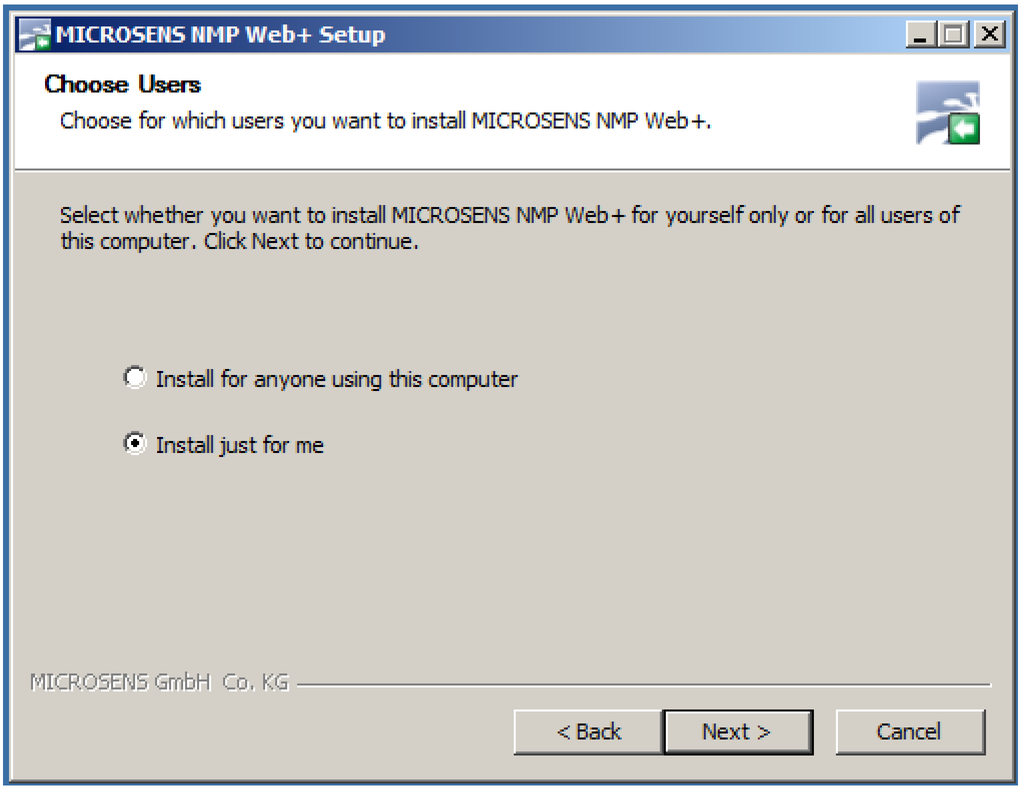
MICROSENS GmbH Co. KG

Figure 1. Choose Components

Check or uncheck the Server Manager’s supplements for installation and hit the button Next.

2.5.3. Choose Users

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



MICROSENS NMP Web+ Setup

Choose Users

Choose for which users you want to install MICROSENS NMP Web+.

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

○ Install for anyone using this computer

● Install just for me

MICROSENS GmbH Co. KG

Figure 2. Choose Users

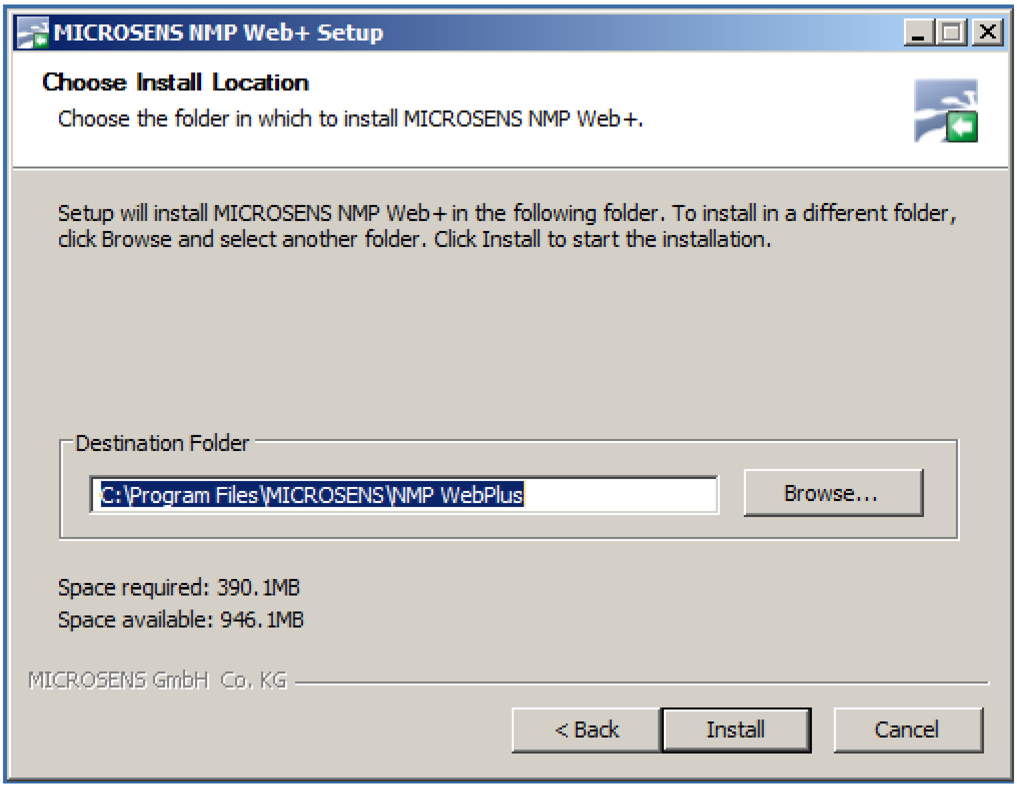
Install for anyone using this computer: Every registered user on this computer is able to use the management application after installation. This should be enabled in exceptional cases if it is ensured that only the responsible network administrator have access to this computer.

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

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

2.5.4. Choose Install Location

On the respective installation location screens determine the destination folders for Server Manager.



MICROSENS NMP Web+ Setup

Choose Install Location

Choose the folder in which to install MICROSENS NMP Web+.

Setup will install MICROSENS NMP Web+ in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\MICROSENS\NMP WebPlus

Space required: 390.1MB
Space available: 946.1MB

MICROSENS GmbH Co. KG

Figure 3. Choose Install Folder

Hit the button Next and the button Install to start the installation process on the system.

When the installation process is finished successfully click the button Next, then the button Finish.

The MICROSENS application is ready to be started.

2.5.5. Installation Path

Upon first startup, the application creates an additional folder in the user's home directory. `%USERPROFILE%\NMP WebPlus`

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

2.6. Installation on Linux Operating Systems

Please refer to the appropriate documentation for more information on how to use the CLI or the archive management application of your specific Linux distribution.

To install the application on Linux, use the following steps:

1. Create a new directory on the local computer (for the application's client compo-

nent) or on a remote server (for the server component), e.g. `~/MICROSENS/NMP_WEB/` . 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_Web-Plus_Installer_v3.2.1_RC8_win64.tar.gz`) or by using the respective archive management application of your Linux distribution.

2. After the file extraction finishes, the application must be started with root access.

2.7. Configuration Folder Presetting (NMP Web+)

By default, NMP Web+ looks for the properties file in the user's home directory. This can be changed before starting NMP Web+.

On Windows®

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

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

On Linux OS

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

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

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

The first is used to start the service with the default folders, while the second is used with the provided context path. To select a custom context folder, the second one must be uncommented.

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

2.8. Software Update

The application is always being improved in order to expand and adapt to new and evolving requirements. Therefore, it is mandatory that you regularly visit the MICROSENS website to download the latest release of the application.

In order to update the application, proceed as follows:

1. Stop a running application.
   a. **NMP Web+:** Exit the application (also applicable to the non-client NMPWeb+). Stop the server instance and exit the Server Manager or stop the server service (if the server component was started as Windows service).
2. After that, install the updated version.
3. During installation, use the same installation path as for the previous version. All

application files will be updated.

2.9. Installation in Silent Mode

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

These parameters read as follows:

`/S`

Silent installation

- No GUI
- Only message boxes are displayed if an error occurs that prevents the installation from proceeding.

`/ProductComponentServer=true|false`

Used only if Server product is selected

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

`/StartMenuShortcut=true|false`

Choose to create Start Menu groups during installation process

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

`/DesktopShortcut=true|false`

Choose to create desktop short cuts during installation process

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

`/AllUsers`

Install for all users

- If not specified, only install for the current user.

`/D=c:\override\default\installdir`	Overwrite installation path • Always use as the last parameter! • Use without quotes, even if installation directory contains spaces! • Will be applied to all the components which will be installed. • Components will be installed in subfolders of defined folder.

Example 1

Installation of NMP Web+ with GUI, preselected options:

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

```
D:\installers\MICROSENS_NMP_WebPlus_Installer_v3.2.1_RC8_win64.exe /StartMenuShortcut=true /DesktopShortcut=false /AllUsers
```

Chapter 3. Licensing

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

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). The trial license allows to manage up to 10 devices. Please contact your MICROSENS representative.

After the trial period is expired, application cannot be used anymore. User is asked to contact MICROSENS to obtain valid license file which will re-enable all the functionalities.

3.2. Licensing model

This chapter explains how the MICROSENS licensing model works.

What is a License?

A license officially grants the license owner the "right to do something" ("usage rights", for short).

What are the Usage Rights?

The following list defines the diffent types of usage rights when working with MICROSENS applications and devices:

- The right to install and update a software version
- The right to manage something

Depending on the article number of the purchased usage rights, a license key file will be created and provided to the customer. According to the type of licence, the coverage may vary as follows:

Product base license

Product license (base installation) allows the installation and use the application. This type of license never expires. The user can use and update the application to the latest version as long as it is required.

Product	Art. No.	Max device list size
NMP Web+ Enterprise	MS200500	unlimited
NMP Web+ Professional	MS200501	unlimited
NMP Web+ Standard	MS200502	unlimited

The user can add devices to the list up to the above-mentioned limit. All devices added to the list will be in READ-ONLY mode which means that their configuration cannot be modified. Only status monitoring is possible.

Important thing to notice is that only the "Enterprise" version allows remote connections with the server for multiple users at the same time. Both "Professional" and "Standard" can only be used from localhost (machine on which server is installed) by one user.

Device license

The user must purchase an extra "device licence" to allow READ-WRITE mode for devices added to the list. When such a licence is installed, it allows you to setup and manage all of the devices covered by the licence. Device licenses have their validity periods (from 1 up to 5 years). When the validity period expires, the number of devices covered by the "device licence" will be converted READ-ONLY mode without management option. To re-enable the R/W mode, the user has to purchase the "device license" again.

Art. No.	Validity period	Number of devices to be managed
MS200509-01	1 year	defined by user
MS200509-02	2 years	defined by user
MS200509-03	3 years	defined by user
MS200509-04	4 years	defined by user
MS200509-05	5 years	defined by user

When ordering, the customer should indicate the number of devices for which the licence should be generated.

It is possible to have both managed and unmanaged devices in the list at the same time. The number of managed devices depends on "device licenses" within the validity period. The application calculates the RW or RO mode for the devices based on the time they were added to the list. The oldest devices are always set to be managed in first place. All devices added later and if they are not covered by any "device license", they are always set as read only.

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

3.3. Select Licence Key File for Server Manager

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

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

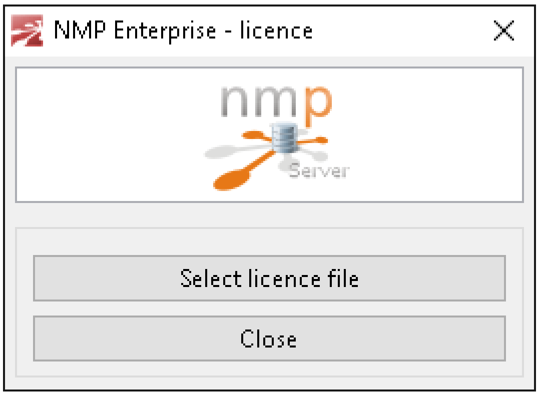
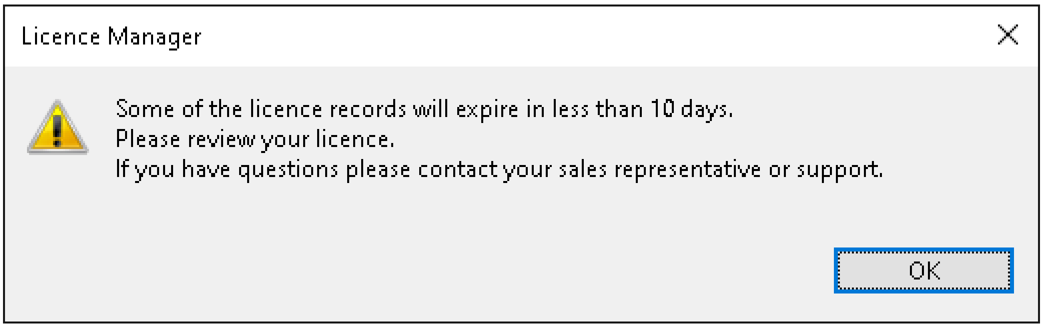


Figure 4. Licence Key Selection

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

3.4. Licence Key Expiry

During startup, the application checks for a valid licencing key file and displays a notification of when the licence will expire.



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

Figure 5. Licence Key Expiry Note

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

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

Chapter 4. NMP Web+

This chapter describes working with NMP Web+.

> 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.

> In the event of technical problems with NMP, please contact MICROSENS technical support using the link provided in the report dialogue. For 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 Web+ Server

4.1.1. Starting the Application on Windows®

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

Start › MICROSENS › MICROSENS NMP Web+

or

Start › MICROSENS › MICROSENS NMP Web+(Debug mode)

The application opens with its login dialogue.

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

4.1.2. Starting on Linux Operating Systems

> The application uses some ports lower than 1024. On UNIX-like operating systems, only applications launched with root rights can bind such ports. Therefore it is important to start the application with `sudo ./NMP` or `su root ./NMP` (or the respective super user command of your Linux distribution)

For further information, please visit the MICROSENS Knowledge Base at www.microsens.com/support.

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

4.2. Login into NMP Web+ via Web Browser

After the NMP Web+ server has been started, a user can log into the system, username and password are obligatory.

By default, 4 accounts are created with the following login settings:

System Administrator

- Login: sysadmin
- Password: sysadmin

Administrator

- Login: admin
- Password: admin

Manager

- Login: manager
- Password: manager

User

- Login: user
- Password: user

> The application provides a “User Manager” where the user accounts can be added/deleted/changed. It is strongly recommended to assign a different password after using the software for the first time to prevent unauthorized access to the software! Please keep in mind that at least one user with “System Administrator” rights must exist. The application will prevent the deletion or change of rights for the last account with "System Administrator" rights.

Access	**unauth.**	**User**	**Manager**	**Admin**	**System Admin**
Device Data	-	RO	RW (RO for IP settings)	RW	RW
Device List	-	RO	RO	RW	RW
User Data	-	-	-	-	RW
Application Data	-	-	-	-	RW

From the table above: RO - Read Only, RW - Read/Write

A user with administrative privileges is able to:

- configure NMP Web+
- change device settings
- update the firmware of devices which are managed by NMP Web+

- monitor the state of managed devices
- edit the device list

A standard user is able to:

- monitor device state
- edit device list

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

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

To access the NMP Web+ simply open a supported browser, e.g. Chrome and enter the IP address and port of the NMP Server.

The login window will be shown:

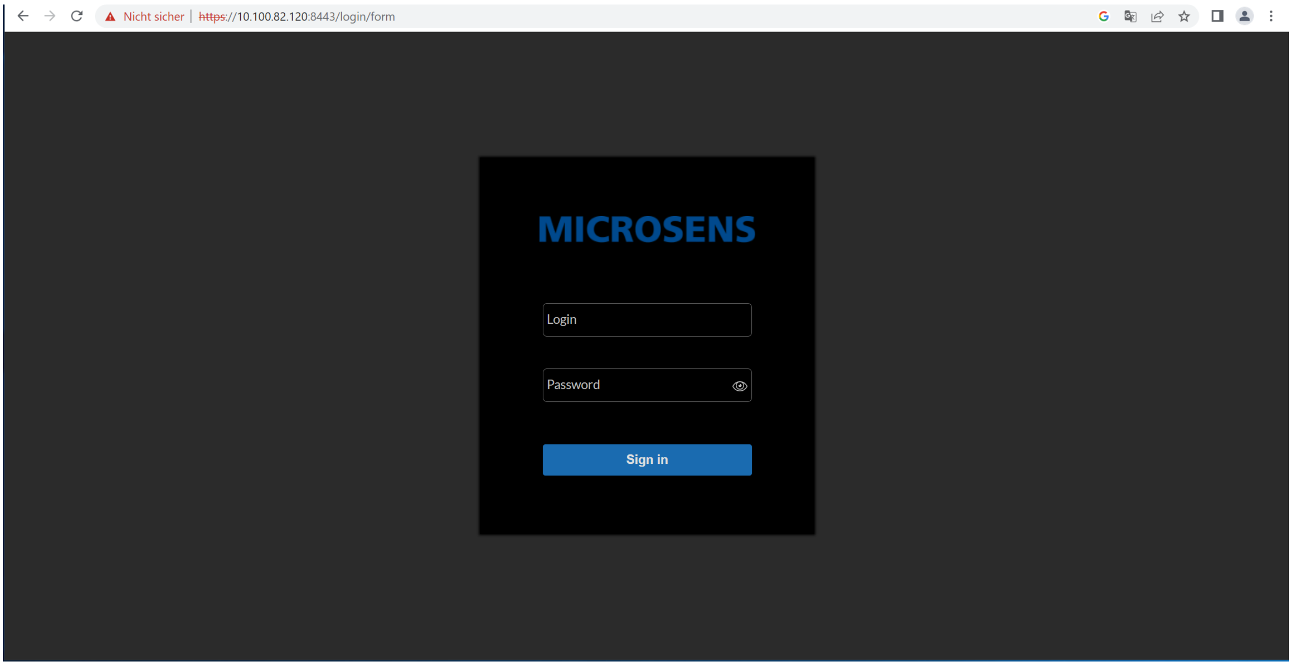


Figure 6. NMP Web+ - Login

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!

4.3. NMP Web+ Startup Window

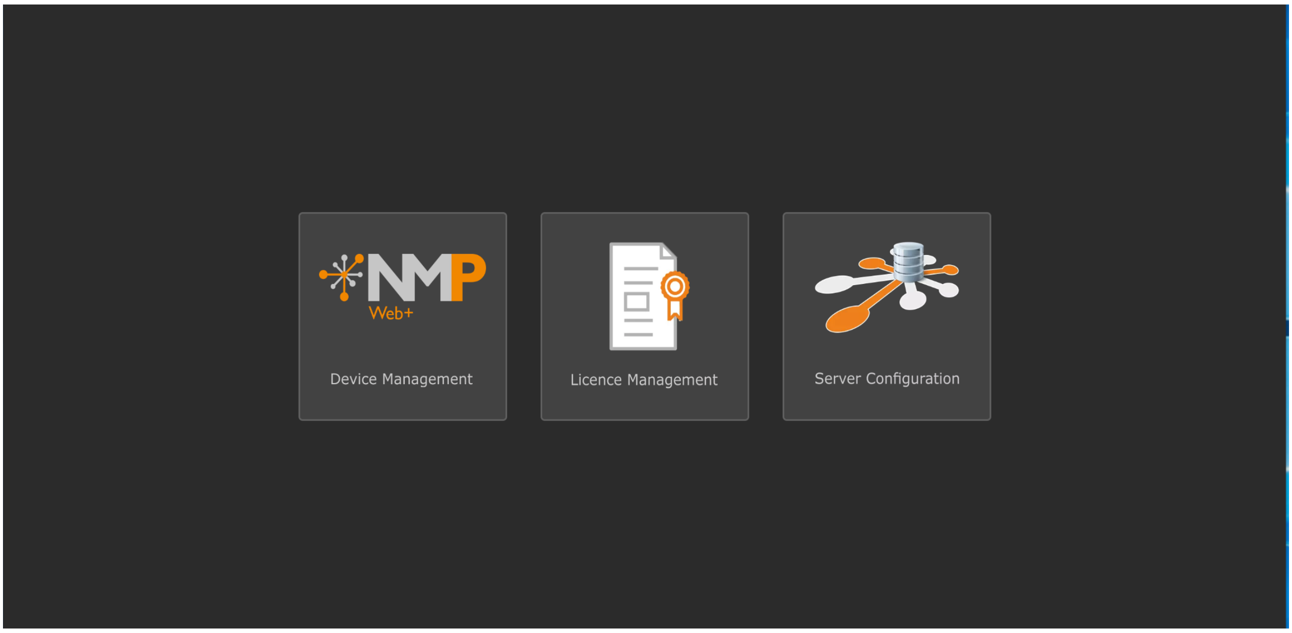


Figure 7. NMP Web+ Startup Window

The main window of NMP Web+ consists of three main elements:

1. Selection Server Configuration (see Section 4.5)
2. Selection License Management (see Chapter 3)
3. Selection Devices Management (see Section 4.4)

4.4. NMP Web+ Device Management

The Device Management application starts when Device Management is selected. The application offers the following structure and menu points.

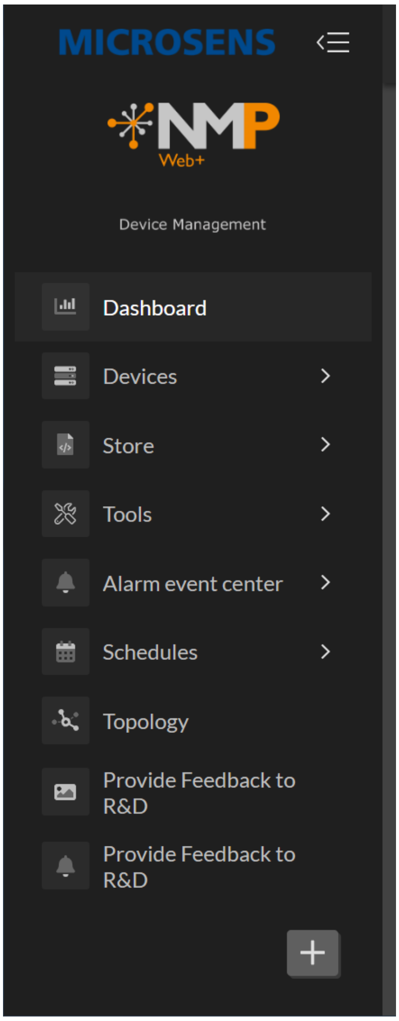


Figure 8. NMP Web+ - Device Management - Menu

4.4.1. Dashboard

The NMP Web+ Device Management Dashboard allows toggling between the **Device view** and the **Event view**. Additionally, it shows information regarding the number of active, inactive, and newly joined NMP devices in the network.

By selecting the **show devices** icon Show devices, the different device types connected to NMP, as well as their quantity, are shown.

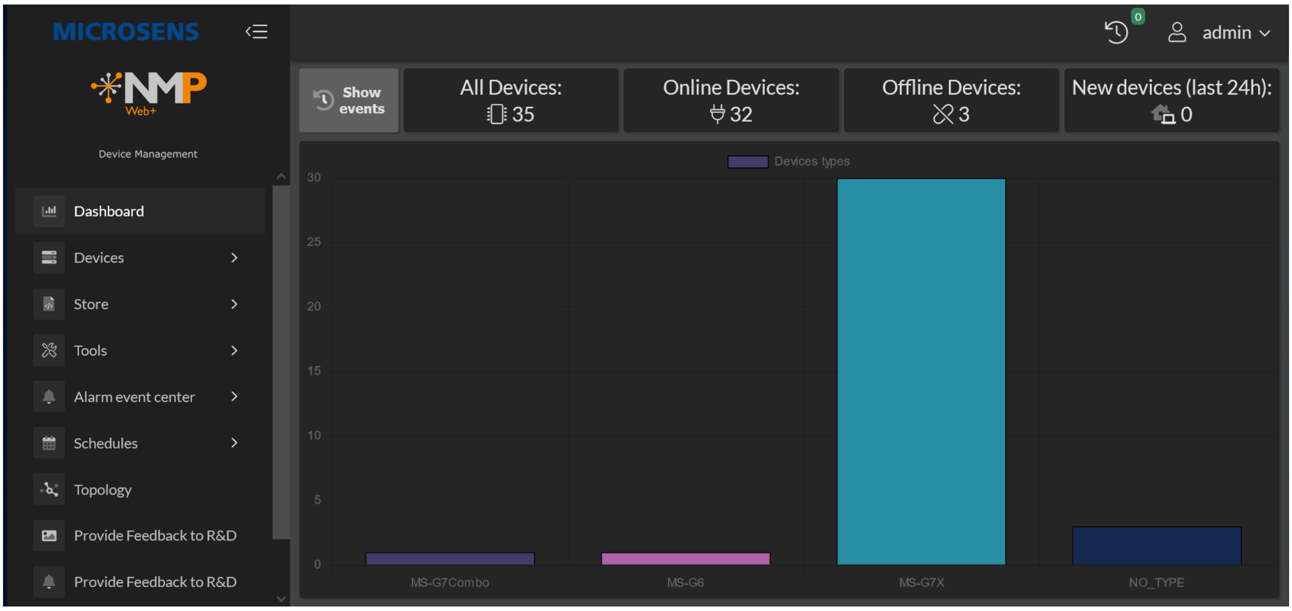


Figure 9. NMP Web+ - Dashboard - Devices

By selecting the **show events** icon Show events, the date and number of events are shown.

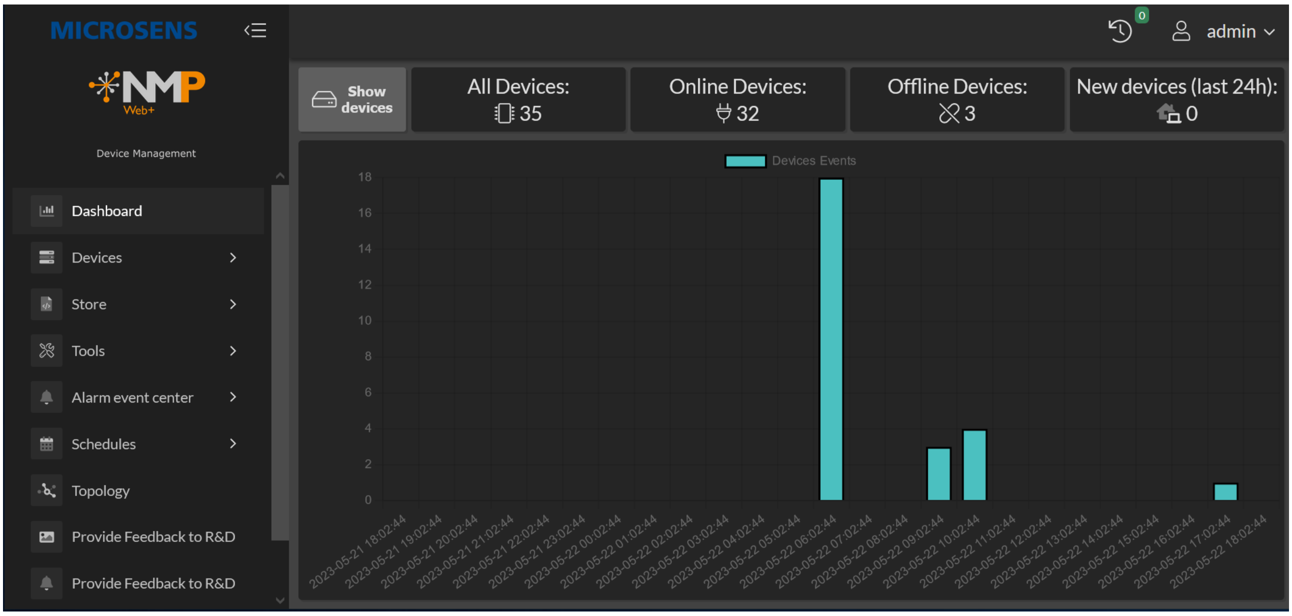


Figure 10. NMP Web+ - Dashboard - Events

4.4.2. Devices

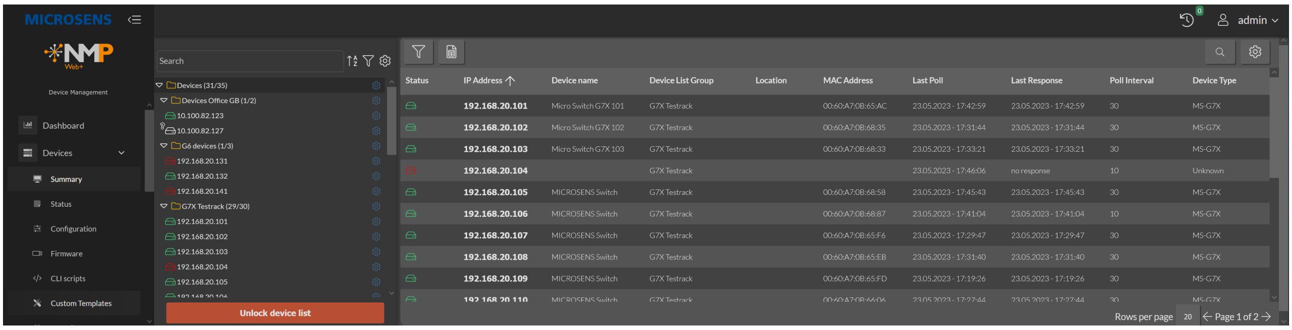
The device menu can be expanded or collapsed by clicking the [**Devices**] icon in the menu. All the functions of the [**Devices**] menu are displayed in the expanded view.

- **Summary**: Shows the summary of all devices in the system. The view can be filtered and sorted according to the device properties (see Section 4.4.2.1).

- **Status**: Shows all the details of the selected device including Maintenance and Diagnostic information (see Section 4.4.2.2).
- **Configuration**: Allows viewing and updating of device configuration (see Section 4.4.2.3).
- **Firmware**: Allows for firmware updates on individual or groups of devices (see Section 4.4.2.4).
- **CLI Scripts**: Provides the option to log the CLI status of the device and to export this information (see Section 4.4.2.5).
- **Custom Templates**: Shows all available templates and allows managing the different templates (see Section 4.4.2.6).
- **Auto discovery**: Allows network device discovery and configuration updates based on configuration files. (see Section 4.4.2.7).
- **IP range scan**: Allows scanning a certain IP range for NMP-compatible devices and generating a device list. (see Section 4.4.2.8).
- **Configuration import/export**: Allows for the search of devices and device groups, polling their status, and changing or backing up their configuration and device name. (see Section 4.4.2.9).

4.4.2.1. Summary

The [**Summary**] view consists of two main parts, the **Device Tree** and the **Summary table**, which is derived from the selected devices from the device tree.



Status	IP Address ↑	Device name	Device List Group	Location	MAC Address	Last Poll	Last Response	Poll Interval	Device Type
🟩	**192.168.20.101**	Micro Switch G7X 101	G7X Testrack		00:60:A7:0B:65:AC	23.05.2023 - 17:42:59	23.05.2023 - 17:42:59	30	MS-G7X
🟩	**192.168.20.102**	Micro Switch G7X 102	G7X Testrack		00:60:A7:0B:68:35	23.05.2023 - 17:31:44	23.05.2023 - 17:31:44	30	MS-G7X
🟩	**192.168.20.103**	Micro Switch G7X 103	G7X Testrack		00:60:A7:0B:68:33	23.05.2023 - 17:33:21	23.05.2023 - 17:33:21	30	MS-G7X
🟥	**192.168.20.104**		G7X Testrack			23.05.2023 - 17:46:06	no response	10	Unknown
🟩	**192.168.20.105**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:68:58	23.05.2023 - 17:45:43	23.05.2023 - 17:45:43	30	MS-G7X
🟩	**192.168.20.106**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:68:87	23.05.2023 - 17:41:04	23.05.2023 - 17:41:04	10	MS-G7X
🟩	**192.168.20.107**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:65:F6	23.05.2023 - 17:29:47	23.05.2023 - 17:29:47	30	MS-G7X
🟩	**192.168.20.108**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:65:EB	23.05.2023 - 17:31:40	23.05.2023 - 17:31:40	30	MS-G7X
🟩	**192.168.20.109**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:65:FD	23.05.2023 - 17:19:26	23.05.2023 - 17:19:26	30	MS-G7X
🟩	**192.168.20.110**	MICROSENS Switch	G7X Testrack		00:60:A7:0B:66:06	23.05.2023 - 17:27:44	23.05.2023 - 17:27:44	30	MS-G7X

Rows per page 20 ← Page 1 of 2 →

Figure 11. NMP Web+ - Devices - Summary

4.4.2.1.1. Device Tree

The device tree shows the devices in the network. By selecting the [**Unlock device list**] button the list can be sorted and grouped. This can be done by using "drag & drop" (click and hold the left mouse button). The changes will be saved when [**Save**] is selected at the end of the action and [**Cancel**] will discard the changes.

A new subgroup can be created by right-clicking on the settings button beside a group. The new subgroup is added at the lower end of the tree.

The devices can be renamed or removed by selecting the settings symbol beside the device identifier and selecting the corresponding menu position.

The device tree allows sorting and searching for devices by using the search box at the top of the tree. The device tree can be configured according to the customer's needs, it can be organized according to:

- IP
- IP - Device name
- Device name
- IP- Hostname
- Hostname
- Hostname - IP
- Device name - IP

4.4.2.1.2. Summary Table

The devices summary table provides information on the device or subgroup that is currently selected in the device list.

The table provides information on the device's current health status. Sort the entries in ascending or descending order by clicking on the respective header.

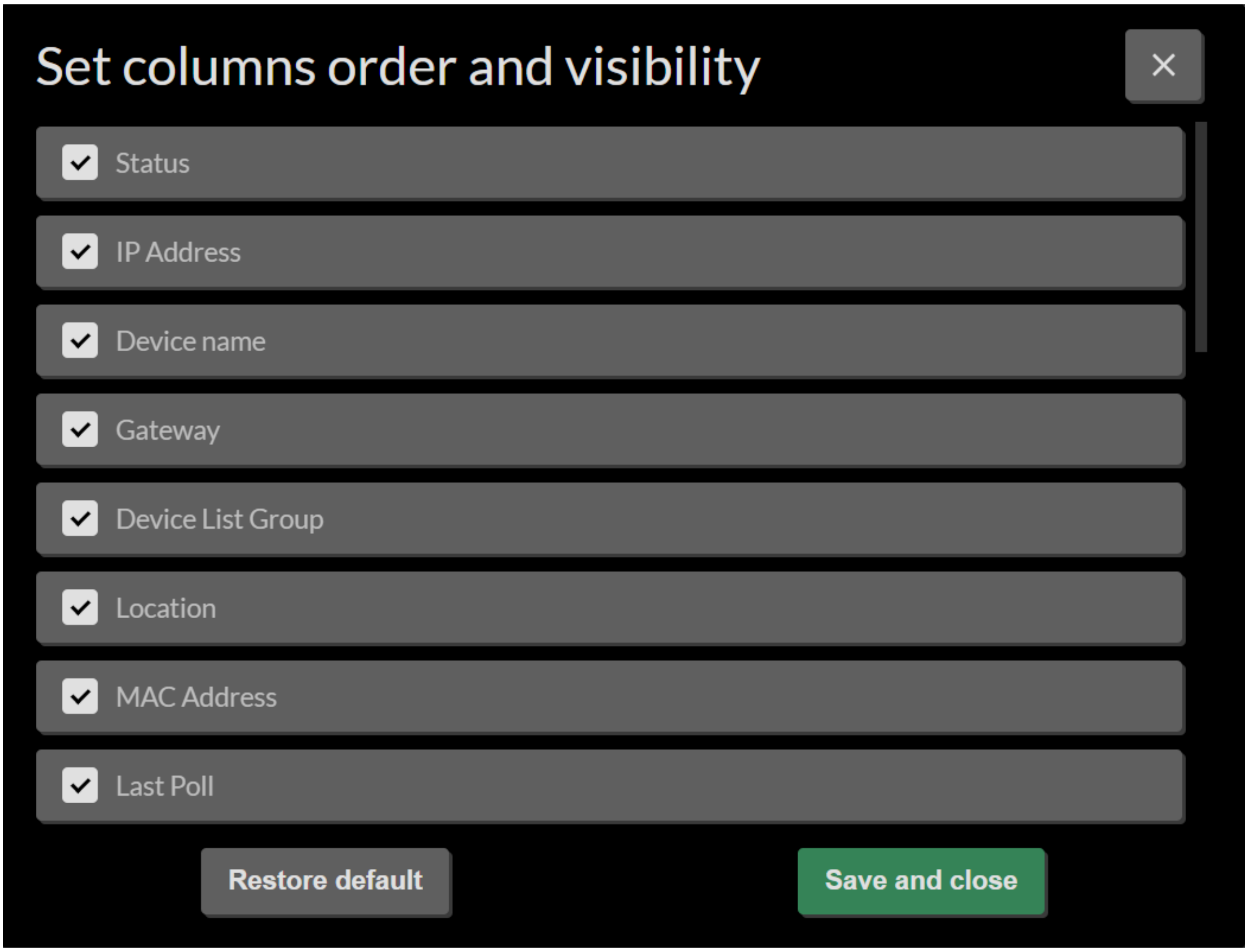
By clicking on the ⚙ button, information that should be visible in the device statistics table can be chosen.

Following information is available:

- Status
- IP Address
- Device Name
- Gateway
- Device List Group
- Location
- MAC Address
- Last Poll
- Last Response
- Poll Interval
- Device Type
- Subnet Mask
- DHCP Mode
- Contact
- Article No.

- Serial No.
- Firmware Ver.
- Inventory String
- System Uptime
- Hostname
- PoE Powered Device
- Temperature
- Free Memory
- RW/RO Mode

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 Apply button.


Set columns order and visibility

☑ Status
☑ IP Address
☑ Device name
☑ Gateway
☑ Device List Group
☑ Location
☑ MAC Address
☑ Last Poll

Figure 12. NMP Web+ - Devices - Summary - Column Select

Refresh table

The device summary table is updated automatically, e.g. after selecting a group. It is possible to refresh the current status by clicking the settings button ⚙ at the top group of the tree table and selecting [**Poll group data**].

Export table

Selecting the button ▦ opens the tool, which allows exporting the table data to a `.csv` file or `.nmpdl` file.

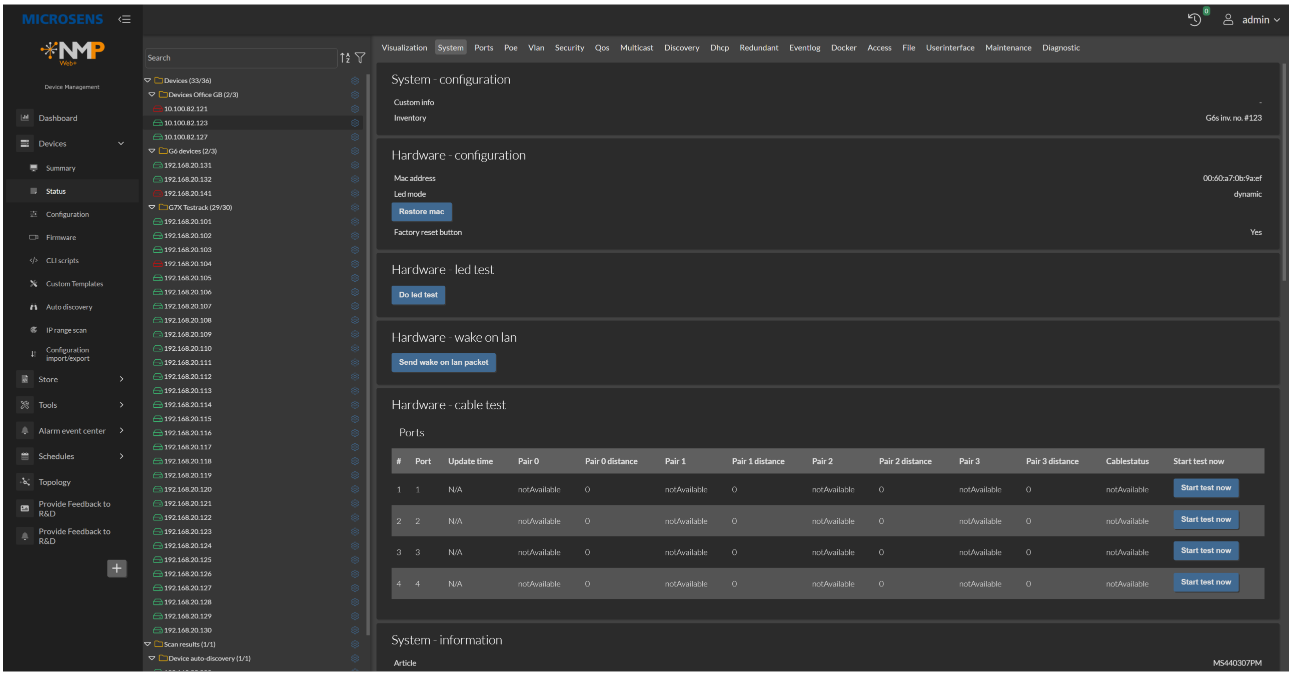
> Individual filters may be configured depending on IP address and device type by using the filter button at the top of the table.

Open Device in Web Browser

To open the device in the web browser, click on the device [**IP address**] in the summary table. This opens the IP address of the current device in a new tab in the default web browser.

4.4.2.2. Status

The Device Status tab provides information about the selected device (current device status). Information is available on the respective tabs.



System - configuration

Custom info -
Inventory G6s inv. no. #123

Hardware - configuration

Mac address 00:60:a7:0b:9a:ef
Led mode dynamic
Factory reset button Yes

Hardware - led test

Hardware - wake on lan

Hardware - cable test

Ports

#	Port	Update time	Pair 0	Pair 0 distance	Pair 1	Pair 1 distance	Pair 2	Pair 2 distance	Pair 3	Pair 3 distance	Cablestatus	Start test now
1	1	N/A	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	Start test now
2	2	N/A	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	Start test now
3	3	N/A	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	Start test now
4	4	N/A	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	0	notAvailable	Start test now

System - information

Article MS440307PM

Figure 13. NMP Web+ - Devices - Status

> There are different tabs for different device types.
>
> For some device types, some additional actions are available which can

> be initiated directly from the dialogue.

The device must first be selected from the [**Device Tree**], then the device information is shown in the table.

Following tabs may be available:

- **Visualization** this tab visualizes the device, details are described in Section 4.4.2.2.1
- **System** the tab is device dependent and displays the general device information, the device time, rebooting the device or using wake on LAN.
- **Hardware** the tab is device dependent and displays the basic configuration e.g. LEDs and port info and port names.
- **IP** the IP tab is device dependent and displays the basic IPV4 and IPV6 settings.
- **Port** the tab is device specific and displays the port specific settings.
- **SFP** the tab is device specific and displays the SFP status.
- **PoE** the tab is device specific and displays the Power over Ethernet (PoE) settings.
- **MAC** the tab is device specific and displays the MAC address monitoring settings.
- **RMON** the tab is device specific and displays the RMON remote monitoring settings and information.
- **Smart office** the tab is device specific and displays the Smart office status and settings.
- **Controller** the tab is device specific and allows configuration of SmartOffice Controller specific parameters like Smartlight config and CSLC config.
- **VLAN** the tab is device specific and displays the VLAN related status and settings.
- **Security** the tab is device specific and displays the security related settings and status. It may also allow password changes, or simple actions e.g. "Clear learned mac table".
- **QoS** the tab is device specific and displays the Quality of Service priority queues, lists and settings.
- **STP** the tab is device specific and displays the Spanning Tree (STP), Rapid STP (RSTP) protocol and Multiple STP (MSTP) protocol settings.
- **PAC** the tab is device specific and displays the Port Access Control according to 802.1X status and settings.
- **IGMP** the tab is device specific and displays the IGMP status.
- **DHCP** the tab is device specific and displays the DHCP relay agent status and statistics.
- **LLDP** the tab is device specific and displays the Link Layer Discovery Protocol configuration and status.
- **LACP** the tab is device specific and displays the Link Aggregation Control Protocol configuration and status.
- **Ring** the tab is device specific and displays the proprietary redundant ring and MRP ring related status.

- **Modbus** the tab is device specific and displays the Modbus status.
- **Access** the tab is device specific and displays the local access control status.
- **CLI** the tab is device specific and displays the Command Line Interface status and monitor.
- **SNMP** the tab is device specific and displays the Simple Network Management Protocol server setup status.
- **NTP** the tab is device specific and displays the Network Time Protocol status and settings.
- **File** the tab is device specific and displays the configuration and status of the file server and the certificate configuration.
- **Script Data** the tab is device specific and displays the scripts and variables.
- **Event** the tab is device specific and displays the event statistics, it may also allow sending e.g. test events or clear log files.
- **Logging** the tab is device specific and displays the logging statistics and logged events.
- **Redundant** the tab is device specific and displays the status, configuration and statistics of the MSRing, G8032 and STP.
- **Docker** the tab is device specific and displays the Docker general status and settings, it may also allow interaction with images or containers through simple function buttons like pull, commit, run, etc.
- **UI** the tab is device specific and displays the CLI, web, SNMP configuration and status.
- **Maintenance** the tab is device specific and displays the maintenance actions for system configuration scripts and firmware, including import and export features as well as comparison tools for configurations.

4.4.2.2.1. Device Visualization

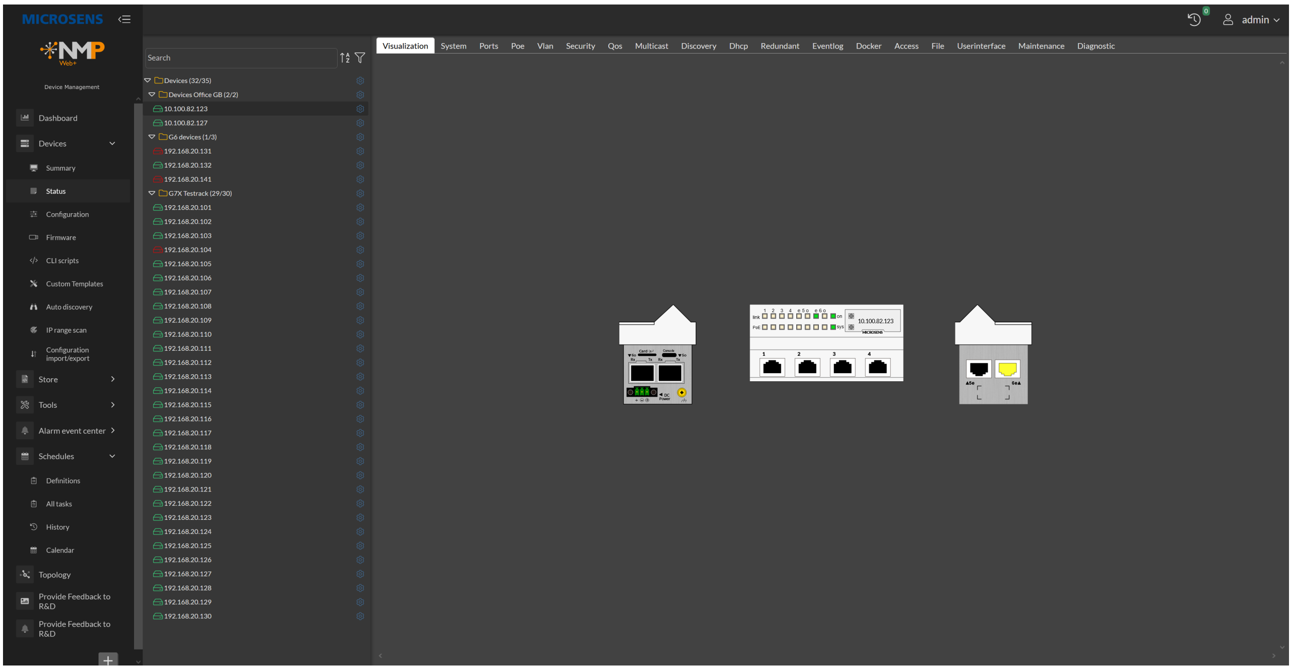


Figure 14. NMP Web+ - Devices - Device Visualization (Example)

The devices visualization tab provides a symbolic representation of the current state of the managed device. The visualization is different for different device types. In some cases, it also reflects the current LED status of the managed device.

For MICROSENS switches, the visualization indicates the port, link and speed status of each local copper and fiber port of the managed device.

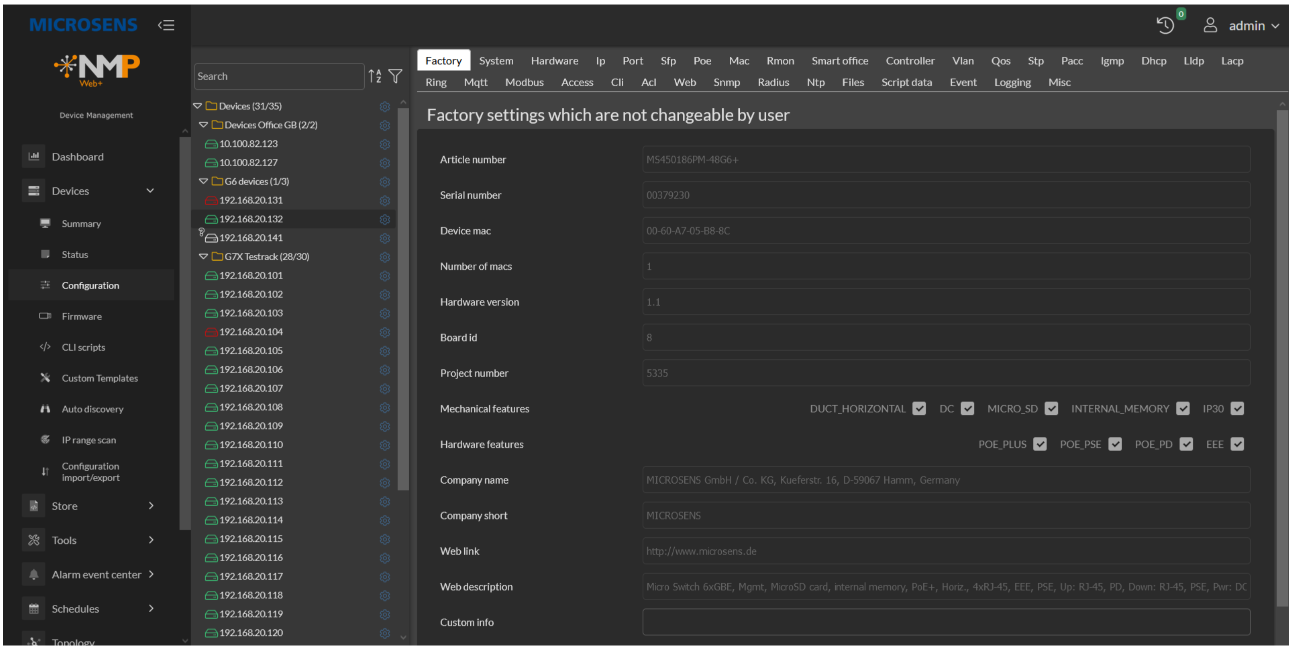
Icon	Meaning
⬛	No link
🟧	10 Mbps link active
🟩	100 Mbps link active
🟨	1 Gbps link active
🟨	10 Gbps link active
☒	Port is off (switches)

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

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

4.4.2.3. Configuration

The Configuration provides textual information about the selected device (current device status) and allows changing the configuration. Information is available on the respective tabs. At the bottom of the tabs there is the possibility to [**Apply**] configuration changes and to also save them to the SD Card.



Factory settings which are not changeable by user

Article number	MS450186PM-48G6+
Serial number	00379230
Device mac	00-60-A7-05-B8-8C
Number of macs	1
Hardware version	1.1
Board id	8
Project number	5335
Mechanical features	DUCT_HORIZONTAL ☑ DC ☑ MICRO_SD ☑ INTERNAL_MEMORY ☑ IP30 ☑
Hardware features	POE_PLUS ☑ POE_PSE ☑ POE_PD ☑ EEE ☑
Company name	MICROSENS GmbH / Co. KG, Kueferstr. 16, D-59067 Hamm, Germany
Company short	MICROSENS
Web link	http://www.microsens.de
Web description	Micro Switch 6xGBE, Mgmt, MicroSD card, internal memory, PoE+, Horiz., 4xRJ-45, EEE, PSE, Up: RJ-45, PD, Down: RJ-45, PSE, Pwr: DC
Custom info	

Figure 15. NMP Web+ - Devices - Device Configuration

The following tabs may be available:

- **Factory** this tab is device dependent and shows factory settings which are not changeable by the user.
- **System** this tab is device dependent and allows setting the device time, rebooting or showing utilization statistics. In addition, it allows setting MAC addresses, running CLI scripts, setting boot preference, detecting links, scheduling scripts and doing LED tests. After the changes have been done, the user must click on apply configuration in order to apply it.
- **Hardware** this tab is device dependent and allows doing basic tests, like LED tests, cable functionality tests, setting the IO signal, etc.
- **IP** this IP tab is device dependent and allows doing basic tests like ping, trace route, DNS lookup or ARP table, as well as IP config settings. If this is not available on the device, check for IP settings in the "system" tab.
- **Port** this tab is device specific and allows doing basic port specific settings, including but not limited to port mirroring, rate limits, restarting ports, monitoring and configuring the port settings like speed, auto negotiation and others.
- **SFP** this tab is device specific and allows configuring the SFP pluggable optical or electrical interfaces.
- **PoE** this tab is device specific and allows configuring the Power over Ethernet (PoE) settings and statistics, including the watchdog.
- **MAC** this tab is device specific and allows configuring MAC address monitoring.
- **RMON** this tab is device specific and allows configuring RMON remote monitoring, e.g. to clear all counters.
- **Smart office** this tab is device specific and allows configuring Microsens smart office settings, scanning for light controllers and configuring the director.
- **Controller** this tab is device specific and allows configuring Microsens smart office controller specific parameters like smartlight config and Cslc config.
- **VLAN** this tab is device specific and allows configuring VLAN related basic settings, VLAN ID config, port, filter, priority override lists, fabric attach and Mvrp.
- **QoS** this tab is device specific and allows configuring quality of service priority queues, enable the service, allows internal QoS settings, prio mapping, trustmode, rateshaping and port config.
- **STP** this tab is device specific and allows the configuring of spanning tree (STP), rapid STP (RSTP) protocol and multiple STP (MSTP) protocol like bridge and port configuration.
- **PAC** this tab is device specific and allows configuring port access control according to 802.1X, MAC locking and other mechanisms, filtering, supplicant, change of authorization and port config.
- **IGMP** this tab is device specific and allows configuring IGMP snooping constraints of IPv4 multicast traffic at layer 2 by configuring layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it. MLD does the same for IPv6 traffic, and also the settings may allow enabling and configuration via VLAN.
- **DHCP** this tab is device specific and allows configuring DHCP relay agent, DHCP

snooping and related ARP inspection, snooping tables and statistics.

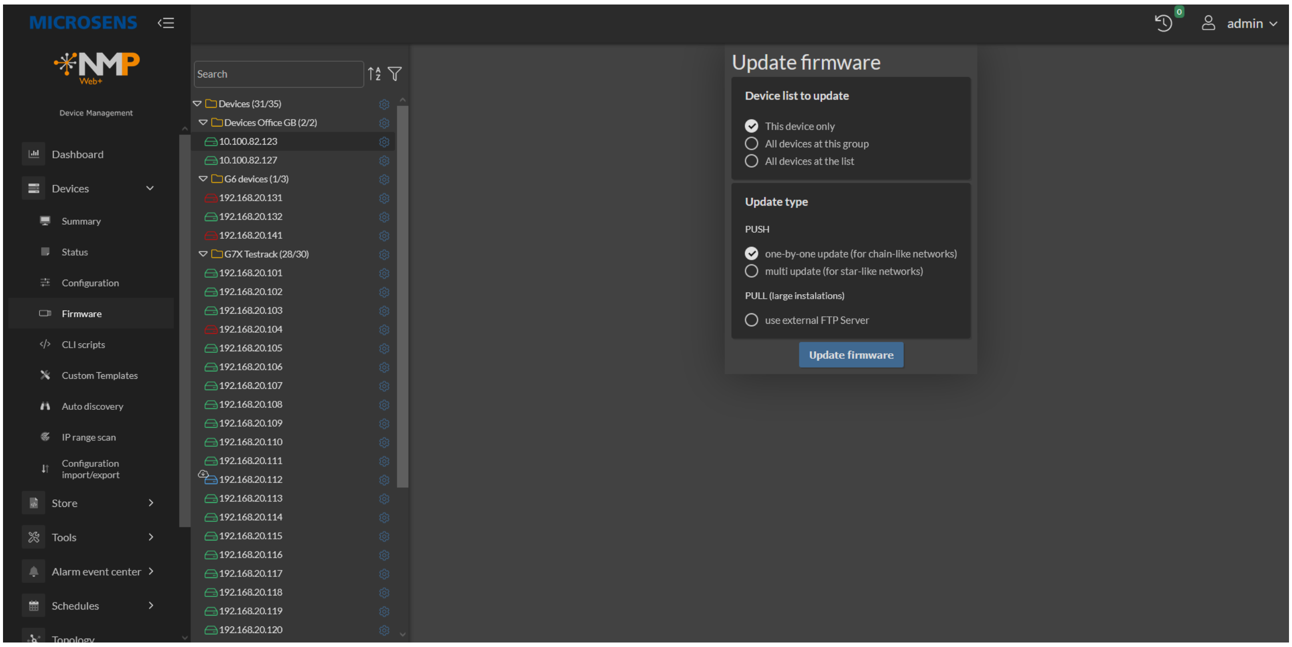
- **LLDP** this tab is device specific and allows configuring link layer discovery protocol, local coordinates and civic location.
- **LACP** this tab is device specific and allows configuring link aggregation control protocols, port and trunk.
- **Ring** this tab is device specific and allows configuring proprietary redundant ring and MRP ring related settings and status values.
- **MQTT** this tab is device specific and allows configuring MQTT Internet of Things protocol settings like publisher and subscriber, broker, topic and broker user.
- **Modbus** this tab is device specific and allows configuring Modbus industrial communications protocols often used with SCADA and PLC applications like device config and element map.
- **Access** the tab is device specific and allows configuring local access control for user login and authentication and element access limitation. It allows defining the authentication method, e.g. LOCAL, and the settings for radius server and TACAS as well as the enabled access methods for the different user groups.
- **ClI** this tab is device specific and allows configuring the command line interface settings, like enabling/disabling from telnet and ssh, setting timeouts, script filters and all other options.
- **ACL** this tab is device specific and allows configuring the access control lists of the device, like enabling and disabling filtering, setting the active filter port config and listing the group and individual rules for easier reference.
- **Web** this tab is device specific and allows configuring web interface settings, smart office web gui definitions and restarting the server.
- **SNMP** this tab is device specific and allows configuring simple network management protocol server setup for all supported versions, provides details on the device and allows using browser actions.
- **Radius** this tab is device specific and allows configuring RADIUS server definitions, for example address, UDP port and shared secret.
- **NTP** this tab is device specific and allows configuring network time protocols and defining servers, sync intervals, time zone and formats.
- **Files** this tab is device specific and allows storing and loading configurations, scripts, certificates and log files and for software upgrades.
- **File** this tab is device specific and allows changing the configuration of the file server.
- **Script Data** this tab is device specific and allows to configure scripts may define and use configuration and status parameters for their own use.
- **Event** this tab is device specific and allows configuring event definitions for traps, syslogs, log files, severity levels etc.
- **Logging** this tab is device specific and allows configuring logging which is used to write event notifications to a server for collection. SYSLOG, SNMP traps or the CLI may be specified as destinations. Additionally, local log files are written to the SD card and status data can be specified to create long term history data.
- **Misc** this tab is device specific and allows configuring miscellaneous network man-

agement related parameters like terminal server and speaker.

- **Multicast** this tab is device specific and allows configuring multicast settings like IGMP and MLD snooping and groups.
- **Discovery** this tab is device specific and allows configuring LLDP settings like Tx delay and ports.
- **Redundant** this tab is device specific and allows configuring STP bridge basic functions, ports, loop config, MSTP groups.
- **Eventlog** this tab is device specific and allows configuring logs general settings, targets and severities.
- **Docker** this tab is device specific and allows configuring docker general settings, import/ export images and containers.
- **UI** this tab is device specific and allows configuring CLI, Web, SNMP settings.
- **Maintenance** this tab is device specific and allows several maintenance actions for system configuration scripts and firmware, including import and export features as well as comparison tools for configurations.

4.4.2.4. Firmware

The [**Firmware**] menu allows you to update the firmware of the currently selected device. The options shown are device dependent.



Update firmware

Device list to update

● This device only
○ All devices at this group
○ All devices at the list

Update type

PUSH

● one-by-one update (for chain-like networks)
○ multi update (for star-like networks)

PULL (large instalations)

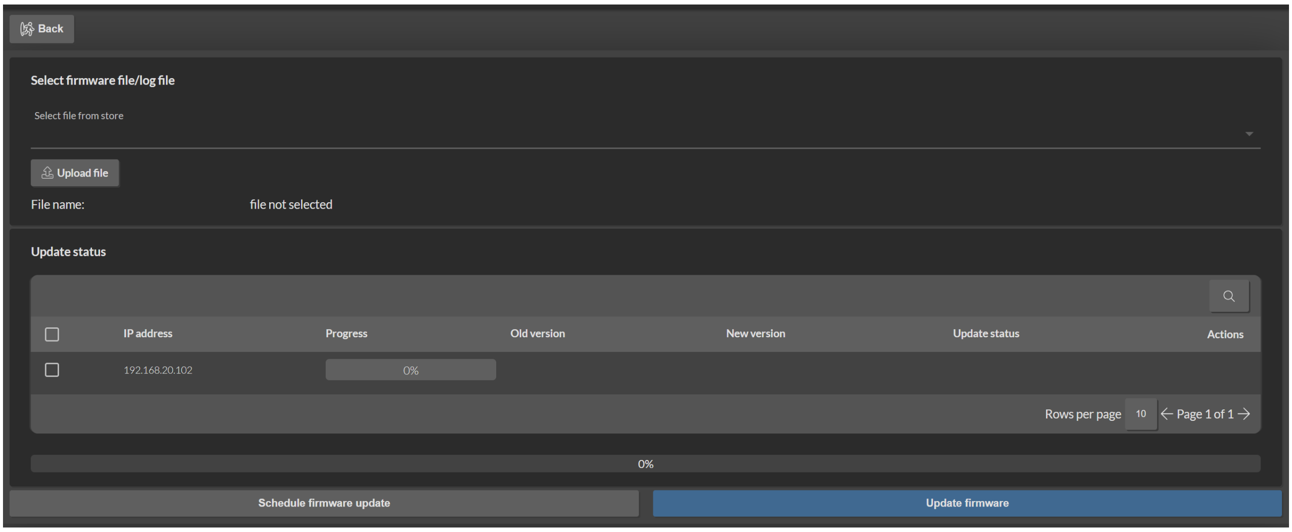
○ use external FTP Server

Figure 16. NMP Web+ - Devices - Firmware

Select the device from the search list to update it. In general, the option allows updating either the single selected device, the entire group of devices, or the entire list of devices. The user has the option of pushing updates to individual devices in chain networks or to all devices in star-like networks. Additionally, it is also feasible to make an update per pull request. Some devices additionally provide users the choice of transferring updates through FTP or HTTPS with encryption.

4.4.2.4.1. Update Firmware

The menu for updating the firmware opens when [**Update firmware**] is selected.



File name: file not selected

□	IP address	Progress	Old version	New version	Update status	Actions
□	192.168.20.102	0%				

Figure 17. NMP Web+ - Devices - Firmware - Select firmware file/log file

The menu allows the selection of a FW from the [**Store**] [see Section 4.4.3]. It offers several options like

- deleting the firmware file from device or
- rebooting before the firmware is modified
- scheduling firmware update in order to open the scheduler configuration to define a one - time or repeated task
- updating firmware

The **Update status** window shows the update status of each device individually.

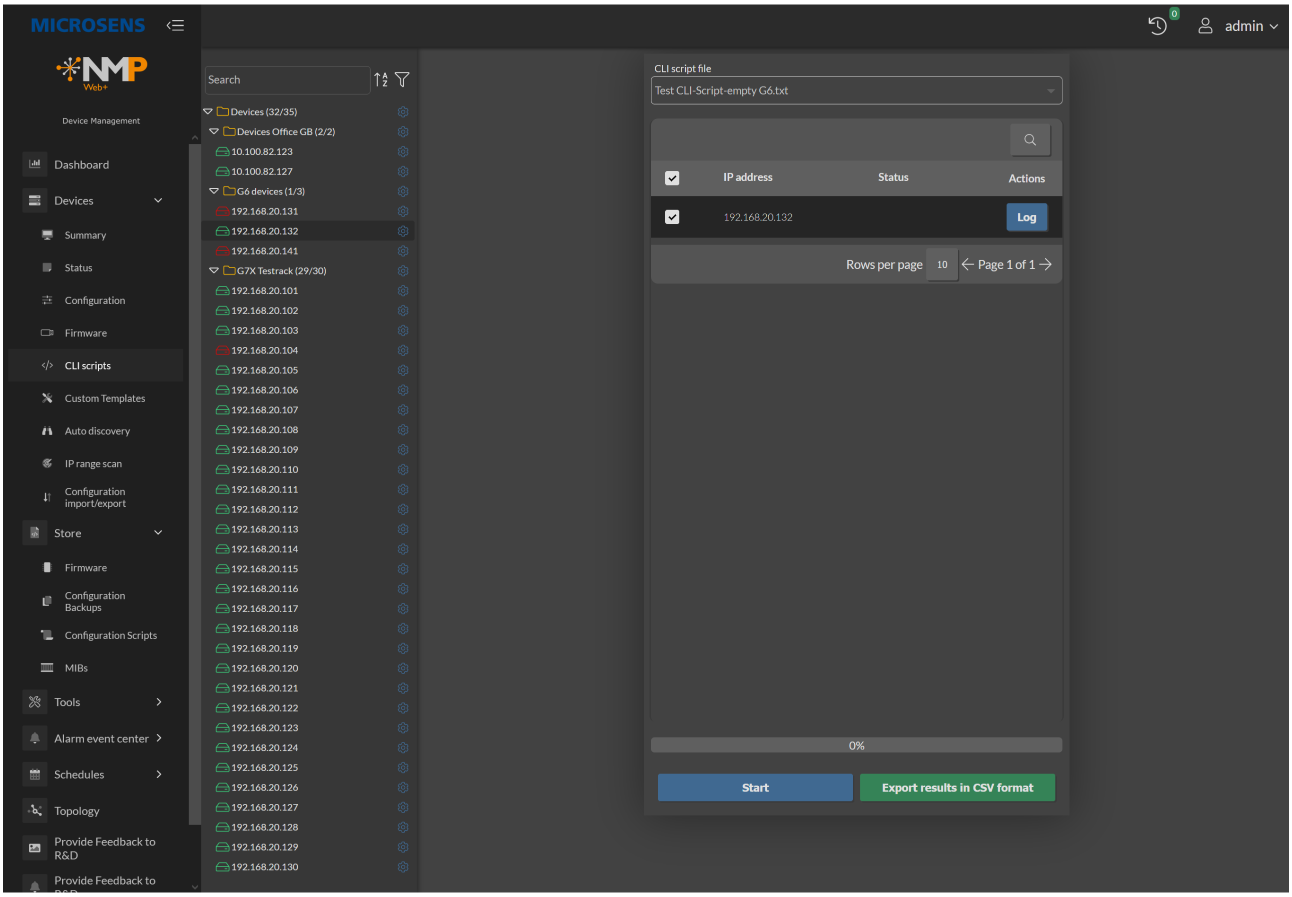
Selecting Back will lead to the firmware main window, any changed settings will be discarded.

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

For further information on how to update the device's firmware, please refer to Section 5.1.

4.4.2.5. CLI Scripts

The CLI Scripts menu allows the selection of CLI scripts from the [**Store**] [see Section 4.4.3] and to send them to a device or a group of devices.



CLI script file: Test CLI-Script-empty G6.txt

☑	IP address	Status	Actions
☑	192.168.20.132		Log

Rows per page 10 ← Page 1 of 1 →

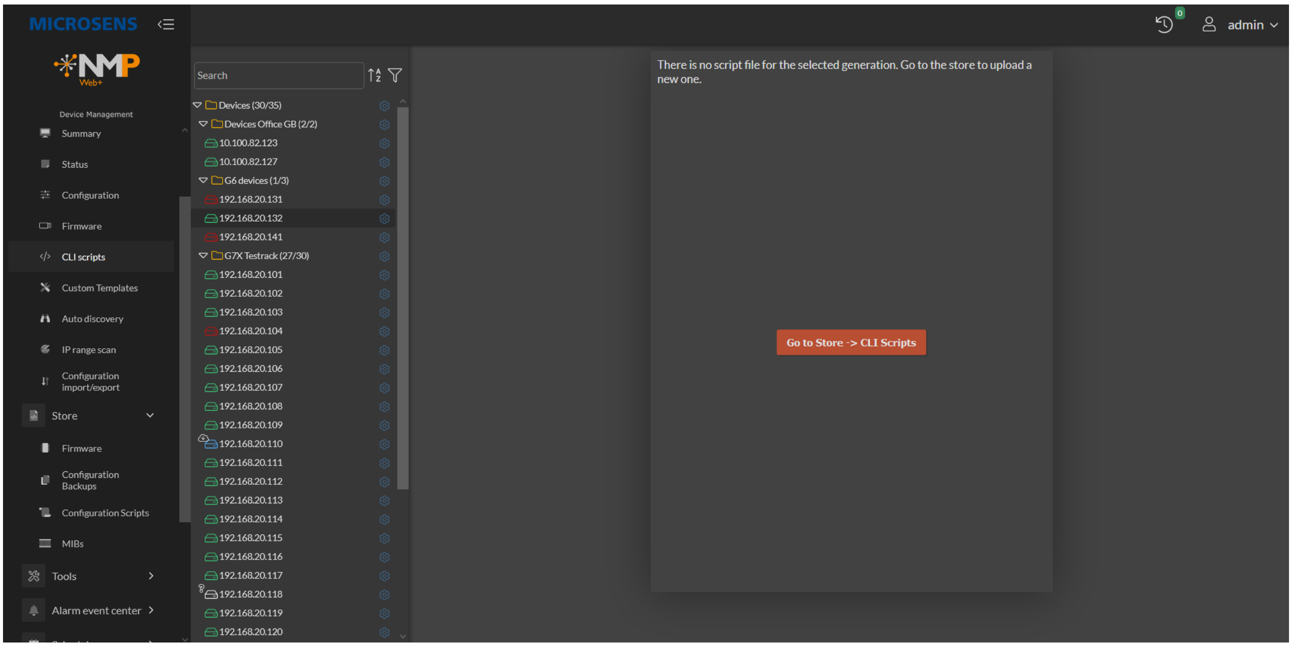
0%

Figure 18. NMP Web+ - Devices - CLI Scripts

To send a CLI script to the device, select the CLI script file via the drop-down menu at the top of the configuration window. The script is transferred when the [**Start button**] is selected. The results can be exported to a `.csv` file.

> Before a CLI script file can be selected, it needs to be saved in the "Store". For more details see chapter Section 4.4.3.

If no CLI script is available, the customer will get the following information:



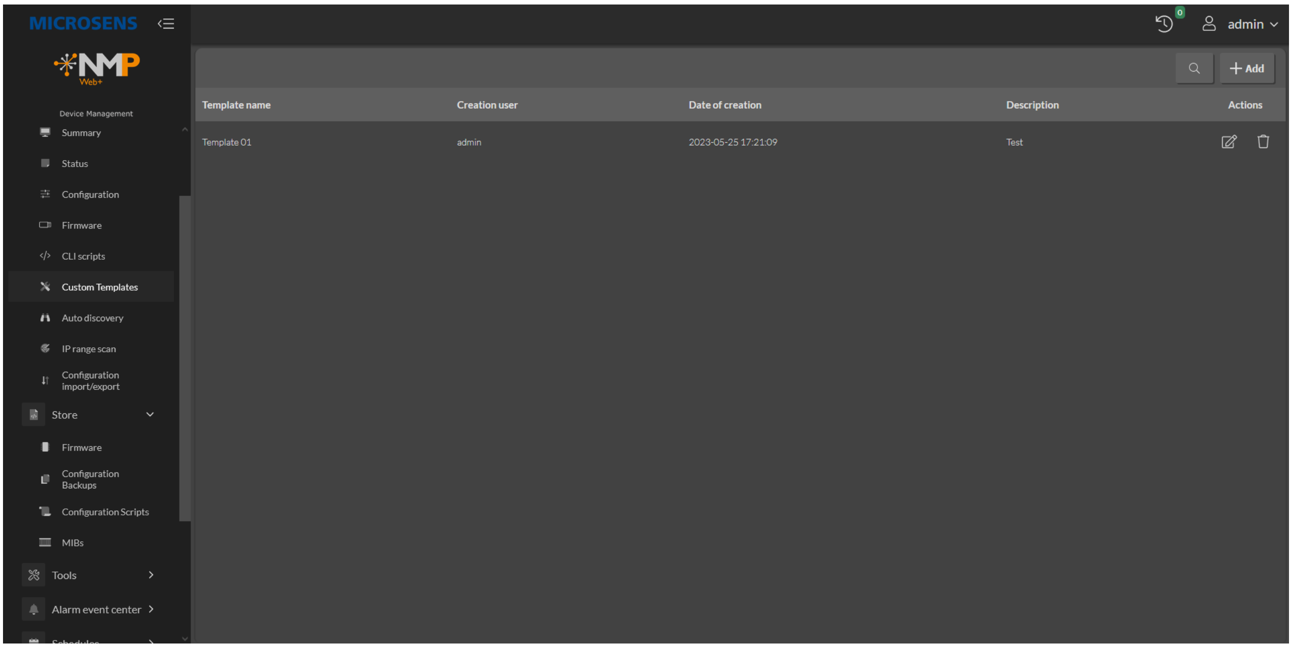
There is no script file for the selected generation. Go to the store to upload a new one.

Figure 19. NMP Web+ - Devices - CLI Scripts - No script

NMP Web+ ensures that the selected CLI file fits in to the selected device, when the parameters have been correctly set.

4.4.2.6. Custom Templates

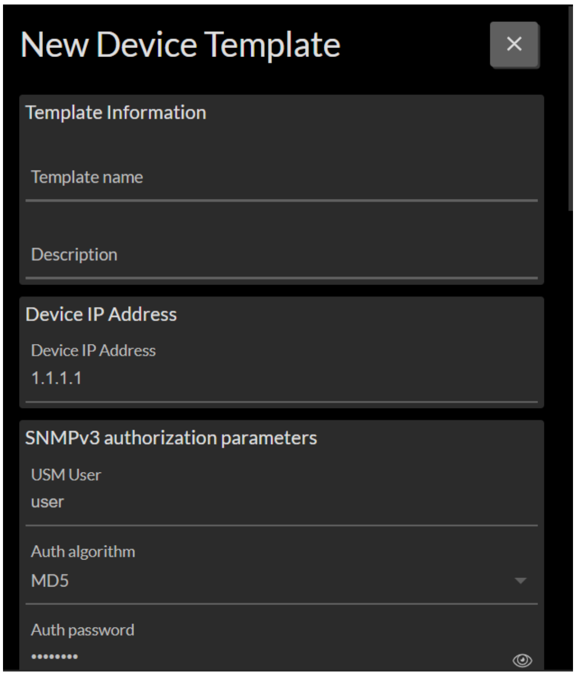
A custom template can be created by selecting the +Add button in the top right corner of the window. An existing template can be changed via selecting the editing tool.



Template name	Creation user	Date of creation	Description	Actions
Template 01	admin	2023-05-25 17:21:09	Test	

Figure 20. NMP Web+ - Devices - Custom Templates

The [**New device template**] window allows the creation or modification of a custom template.



New Device Template
×

Template Information

Template name

Description

Device IP Address

Device IP Address
1.1.1.1

SNMPv3 authorization parameters

USM User
user

Auth algorithm
MD5

Auth password
••••••••

Figure 21. NMP Web+ - Devices - Custom Templates - New device template

The parameters that can be altered are:

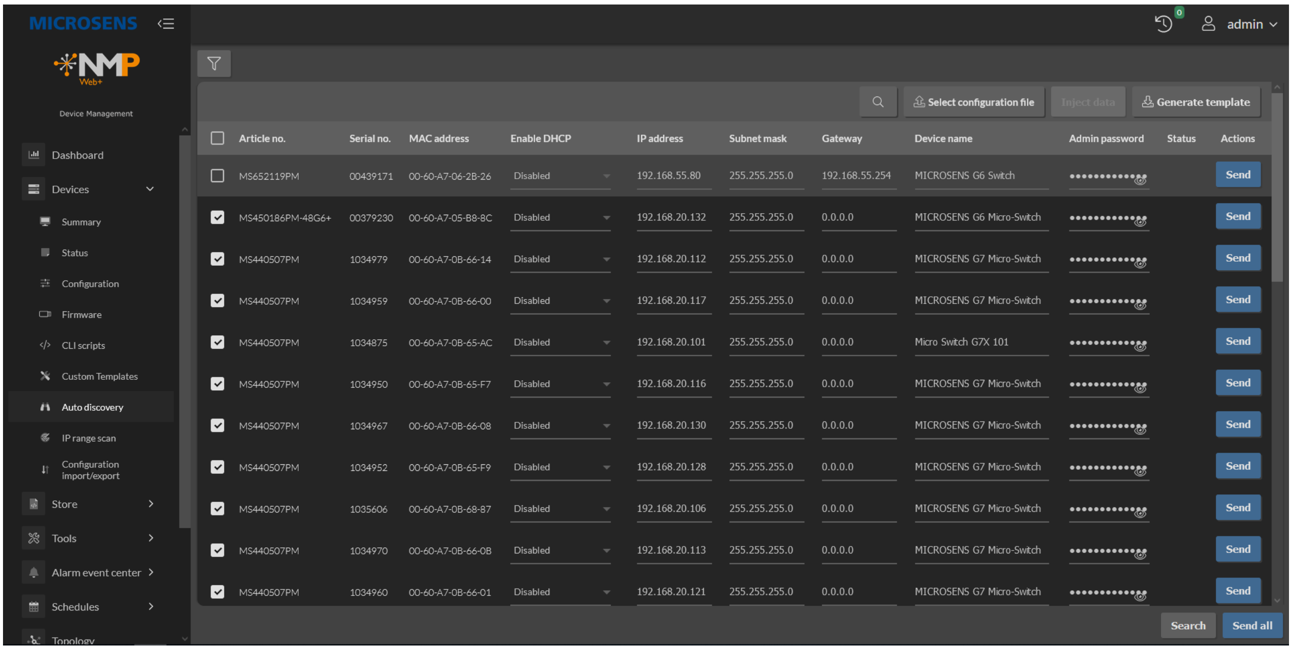
- Template information
- Device IP address
- SNMPv3 authorization parameters
- SNMPv1/SNMPv2c authorization parameters
- FTP access Management Module MS416020-B parameters
- G3/G4/G5 switch FTTO/Desktop/Industrial Profi Line parameters
- G6/G7 Combo/G7 MacSec/G7X/Desktop/Industrial Profi Line parameters
- Communication parameters

4.4.2.7. Auto discovery

NMP’s auto discovery features make it possible to automatically look for devices on a network. 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	Status	Actions
□	MS652119PM	00439171	00-60-A7-06-2B-26	Disabled	192.168.55.80	255.255.255.0	192.168.55.254	MICROSENS G6 Switch	••••••••••••		Send
☑	MS450186PM-48G6+	00379230	00-60-A7-05-B8-8C	Disabled	192.168.20.132	255.255.255.0	0.0.0.0	MICROSENS G6 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034979	00-60-A7-0B-66-14	Disabled	192.168.20.112	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034959	00-60-A7-0B-66-00	Disabled	192.168.20.117	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034875	00-60-A7-0B-65-AC	Disabled	192.168.20.101	255.255.255.0	0.0.0.0	Micro Switch G7X 101	••••••••••••		Send
☑	MS440507PM	1034950	00-60-A7-0B-65-F7	Disabled	192.168.20.116	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034967	00-60-A7-0B-66-08	Disabled	192.168.20.130	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034952	00-60-A7-0B-65-F9	Disabled	192.168.20.128	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1035606	00-60-A7-0B-68-87	Disabled	192.168.20.106	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034970	00-60-A7-0B-66-0B	Disabled	192.168.20.113	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send
☑	MS440507PM	1034960	00-60-A7-0B-66-01	Disabled	192.168.20.121	255.255.255.0	0.0.0.0	MICROSENS G7 Micro-Switch	••••••••••••		Send

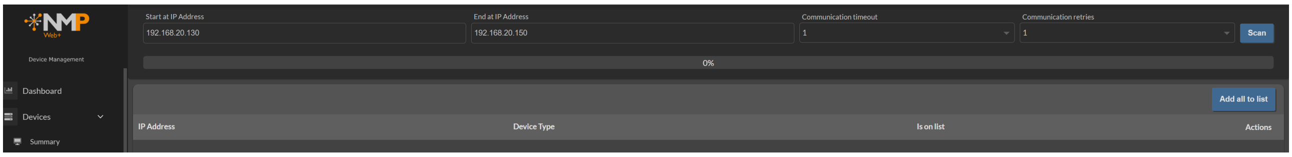
Figure 22. NMP Web+ - Devices - Auto Discovery

If no device is detected, the auto discovery dialogue (Figure 22) will not appear.

4.4.2.8. IP range scan

The following parameters need to be defined in advance for the IP range scan method:

- IP range with start IP and end IP
- Communication parameters including timeout and retries



Start at IP Address: 192.168.20.130
End at IP Address: 192.168.20.150
Communication timeout: 1
Communication retries: 1
0%

IP Address	Device Type	Is on list	Actions

Figure 23. NMP Web+ - Devices - IP-Range-Scan

Device IP range scan searches for all supported devices inside the defined IP range. Community strings for the SNMP devices are defined under menu [**Devices Configuration**] see tab [SNMP].

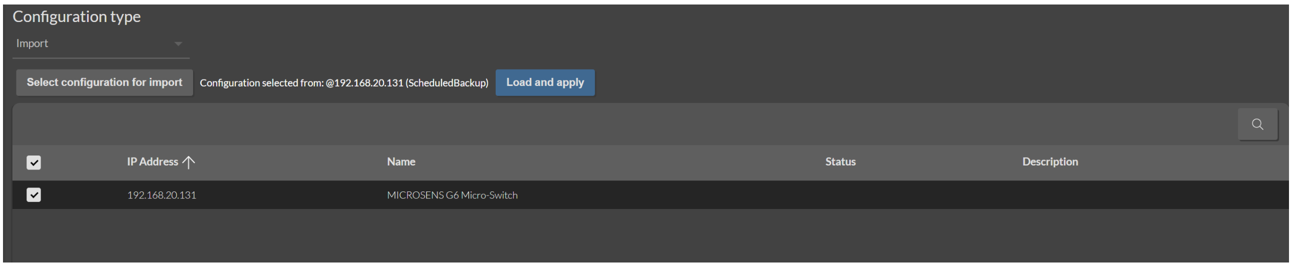
This feature covers discovery of SNMPv1/v2c devices only. Due to the security enhancements of SNMPv3 (authentication and authorization), it is not possible to auto-discover SNMPv3 devices.

4.4.2.9. Configuration import/export

4.4.2.9.1. Import Configuration

To import a configuration to a device, pick the device in the device list tree view, then choose the option [**Import**] from the import/export selection box in the [**Configura-**

tion type] window.

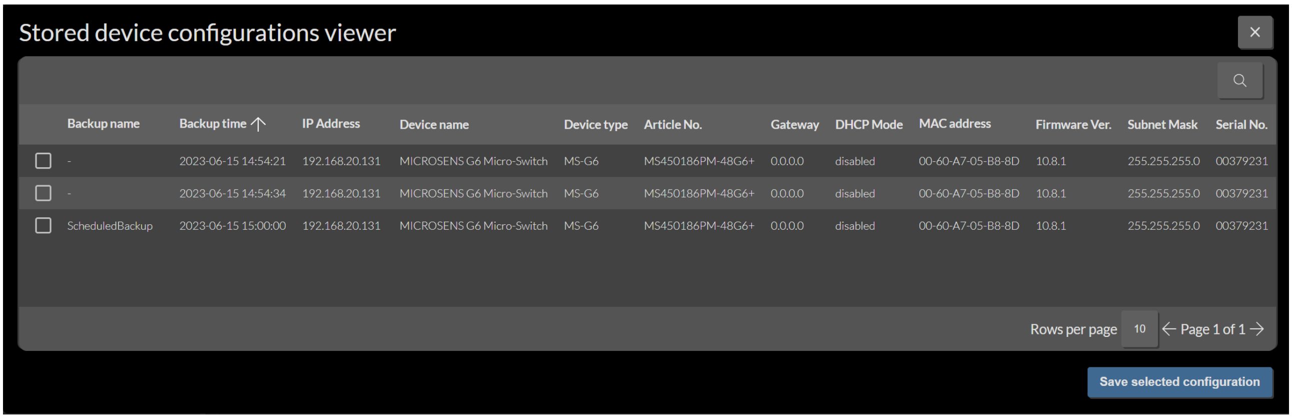


Configuration selected from: @192.168.20.131 (ScheduledBackup)

☑	IP Address ↑	Name	Status	Description
☑	192.168.20.131	MICROSENS G6 Micro-Switch		

Figure 24. NMP Web+ - Devices - Configuration import/export - Configuration import

The checkbox for the relevant device(s) can now be selected, and the best suited saved configuration can be selected by using the **Select configuration for import** button.


Stored device configurations viewer
×
Save selected configuration

	Backup name	Backup time ↑	IP Address	Device name	Device type	Article No.	Gateway	DHCP Mode	MAC address	Firmware Ver.	Subnet Mask	Serial No.
☐	-	2023-06-15 14:54:21	192.168.20.131	MICROSENS G6 Micro-Switch	MS-G6	MS450186PM-48G6+	0.0.0.0	disabled	00-60-A7-05-B8-8D	10.8.1	255.255.255.0	00379231
☐	-	2023-06-15 14:54:34	192.168.20.131	MICROSENS G6 Micro-Switch	MS-G6	MS450186PM-48G6+	0.0.0.0	disabled	00-60-A7-05-B8-8D	10.8.1	255.255.255.0	00379231
☐	ScheduledBackup	2023-06-15 15:00:00	192.168.20.131	MICROSENS G6 Micro-Switch	MS-G6	MS450186PM-48G6+	0.0.0.0	disabled	00-60-A7-05-B8-8D	10.8.1	255.255.255.0	00379231

Rows per page 10 ← Page 1 of 1 →

Figure 25. NMP Web+ - Devices - Configuration import/export - Stored Configuration

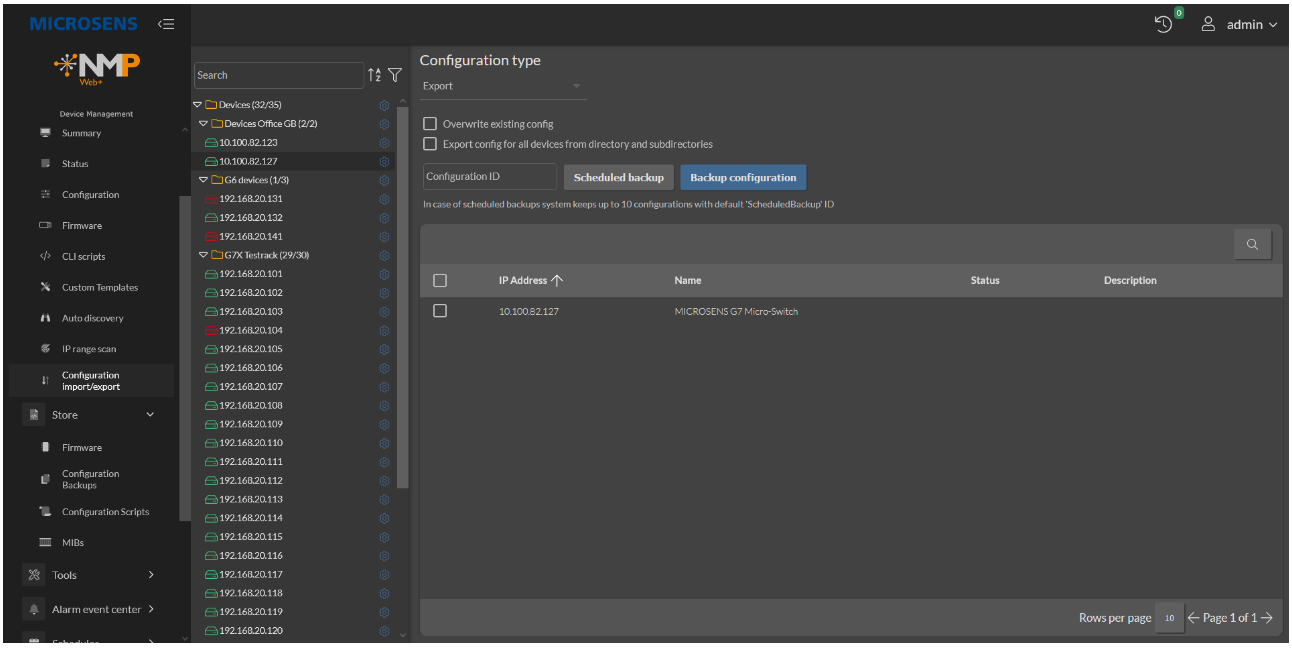
Selecting the button Load and apply applies the imported configuration to the device.

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.

The [**Alarm and event center**] now shows this at the menu events.

4.4.2.9.2. Export Configuration

It is possible to save a device’s configuration for backup or for device replacement purposes. To save the device’s configuration, mark the respective device in the **device list tree** view and mark the checkbox in the **Configuration type** menu. The device backups are generated and saved by selecting [**Backup configuration**].



Configuration type: Export

□ Overwrite existing config

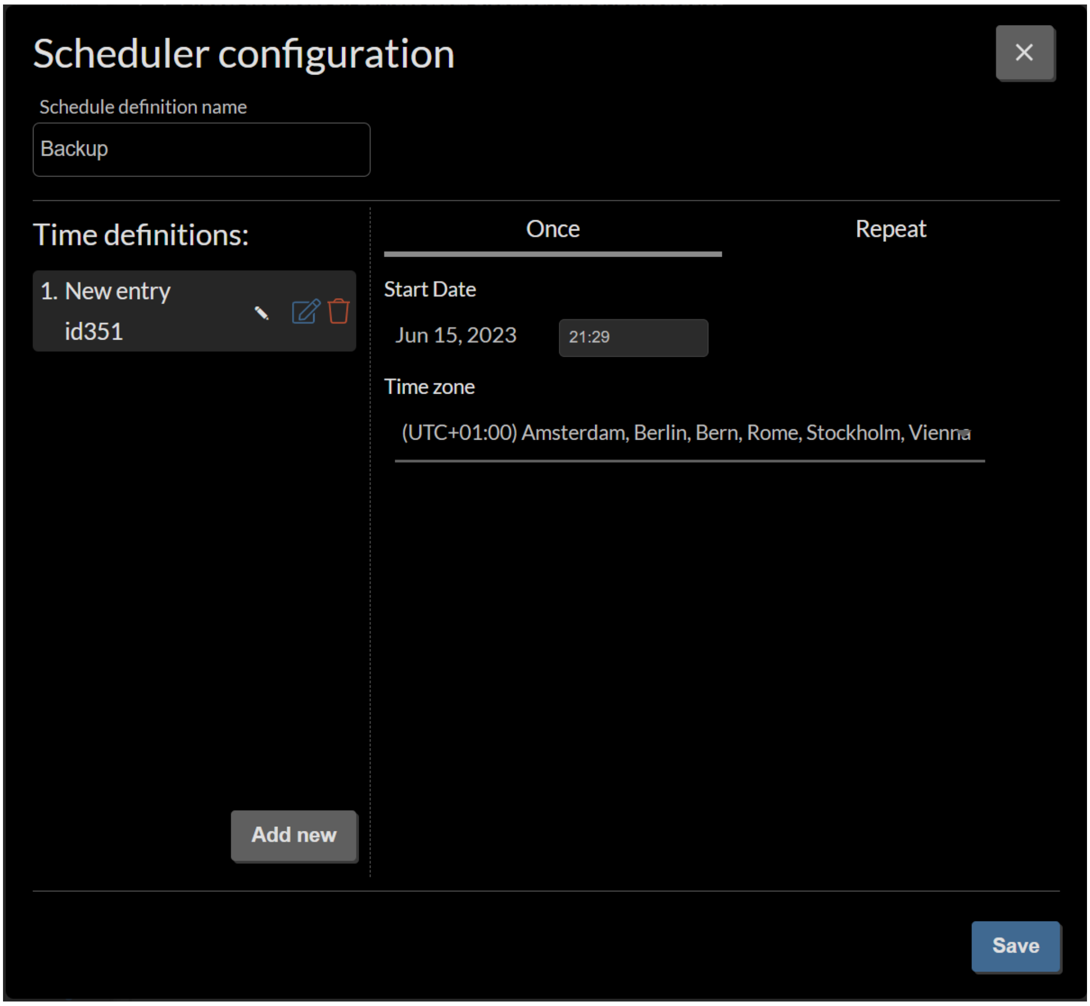
□ Export config for all devices from directory and subdirectories

In case of scheduled backups system keeps up to 10 configurations with default 'ScheduledBackup' ID

□	IP Address	Name	Status	Description
□	10.100.82.127	MICROSENS G7 Micro-Switch		

Figure 26. NMP Web+ - Devices - Configuration import/export - Configuration export

In addition, it is possible to schedule a backup for the selected device(s) either as a one-time backup, or as a repeated event. This can be configured by selecting [**Scheduled backup**].



Scheduler configuration

Schedule definition name: Backup

Time definitions:

1. New entry id351

Once | Repeat

Start Date: Jun 15, 2023 21:29

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Figure 27. NMP Web+ - Devices - Configuration import/export - Scheduler

Define a task which will be executed once (at a defined time) or periodically at the configured execution rate.

All scheduled tasks can be deleted or modified using the "Schedules" menu (see Section 4.4.6).

4.4.3. Store

The Store menu can be expanded or collapsed by selecting the Store icon in the menu. In the expanded view, all functions of the store menu are shown.

Firmware

Shows where which firmware version is saved in NMP (see Section 4.4.2.4)

Configuration Backups

Shows where in NMP each backup for each device type is saved (see Section 4.4.3.2)

Configuration Scripts

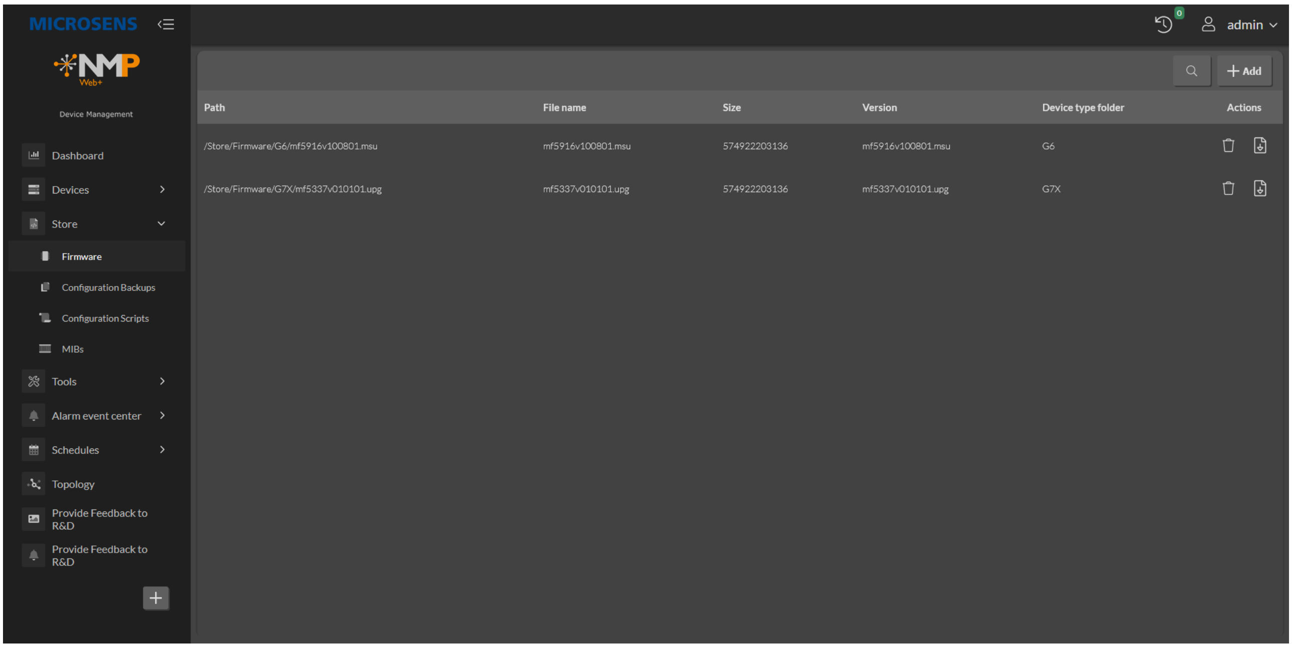
Shows where in NMP each Configuration Script is saved (see Section 4.4.3.3)

MIBs

> The MIBs store is used to store the MIB files provided by the user in order to support any SNMP-based device. Therefore, if a user has a device that can be managed using the SNMP protocol but not the NMP, they can upload the MIB files for that device, add it to the list using its IP address, and then choose the MIB file that should be used for that device from the Store/MIBs section (the one that was just uploaded). As a result, we can now add basic support for any SNMP-based device that NMP does not already support. (see Section 4.4.3.4)

4.4.3.1. Firmware

New firmware can be added by selecting the +Add button. This will allow the selection of the correct DestinationFolder based on the device type of the file. By selecting [**upload file**], the OS specific file selection and upload menu will be opened, and the correct file can be selected.



Path	File name	Size	Version	Device type folder	Actions
/Store/Firmware/G6/mf5916v100801.msu	mf5916v100801.msu	574922203136	mf5916v100801.msu	G6	
/Store/Firmware/G7X/mf5337v010101.upg	mf5337v010101.upg	574922203136	mf5337v010101.upg	G7X	

Figure 28. NMP Web+ - Devices - Store - Firmware

> The selected device DestinationFolder will be used to update the devices. Selecting the wrong device DestinationFolder for the firmware may lead to inconveniences when updating a device with its firmware. For example, a G6 device can only be updated with firmware files in the G6 DestinationFolder.

The uploaded Firmware images can be deleted or downloaded using the corresponding symbol. The overview always shows [**Device type folder**] to avoid confusion.

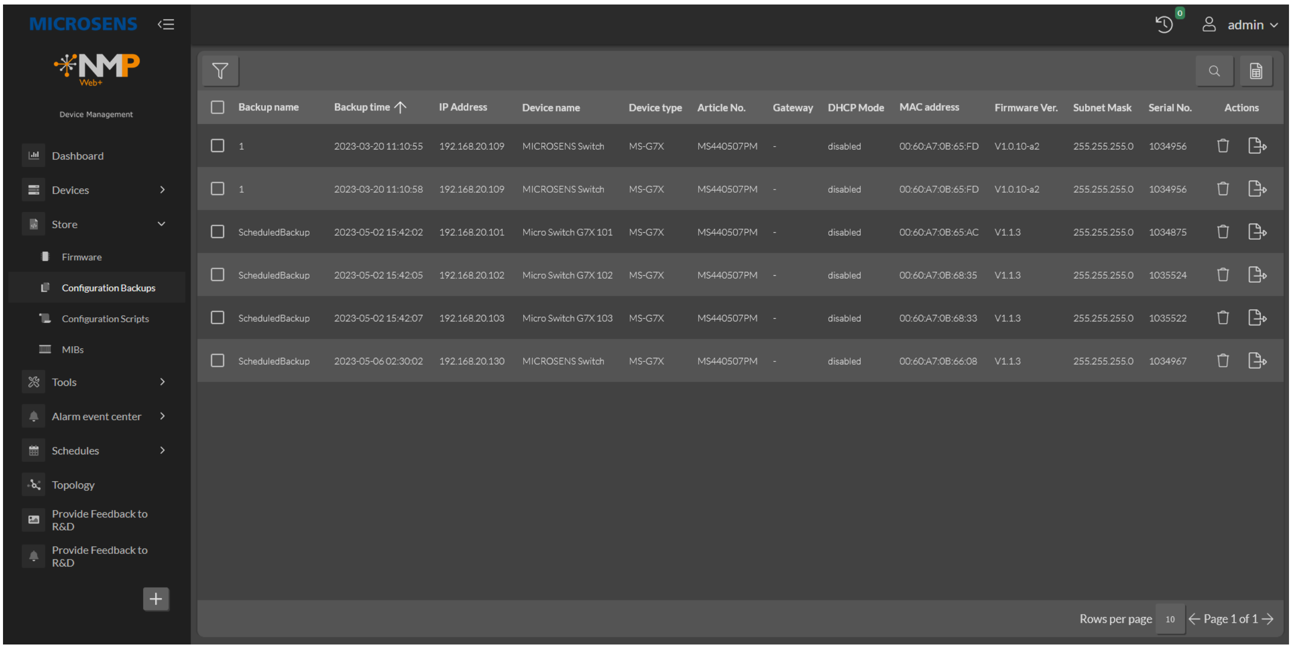
4.4.3.2. Configuration backups

This menu provides an overview of the archived backups including:

- Backup name

- Backup time
- IP address
- Device name
- Device type
- Article Number
- Gateway
- DHCP Mode
- MAC address
- Firmware Version
- Subnet Mask
- Serial Number

The table can be sorted in ascending and descending order for each criteria by clicking on the name of the criteria.



□	Backup name	Backup time ↑	IP Address	Device name	Device type	Article No.	Gateway	DHCP Mode	MAC address	Firmware Ver.	Subnet Mask	Serial No.	Actions
□	1	2023-03-20 11:10:55	192.168.20.109	MICROSENS Switch	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:65:FD	V1.0.10-a2	255.255.255.0	1034956	
□	1	2023-03-20 11:10:58	192.168.20.109	MICROSENS Switch	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:65:FD	V1.0.10-a2	255.255.255.0	1034956	
□	ScheduledBackup	2023-05-02 15:42:02	192.168.20.101	Micro Switch G7X 101	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:65:AC	V1.1.3	255.255.255.0	1034875	
□	ScheduledBackup	2023-05-02 15:42:05	192.168.20.102	Micro Switch G7X 102	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:68:35	V1.1.3	255.255.255.0	1035524	
□	ScheduledBackup	2023-05-02 15:42:07	192.168.20.103	Micro Switch G7X 103	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:68:33	V1.1.3	255.255.255.0	1035522	
□	ScheduledBackup	2023-05-06 02:30:02	192.168.20.130	MICROSENS Switch	MS-G7X	MS440507PM	-	disabled	00:60:A7:0B:66:08	V1.1.3	255.255.255.0	1034967	

Rows per page 10 ← Page 1 of 1 →

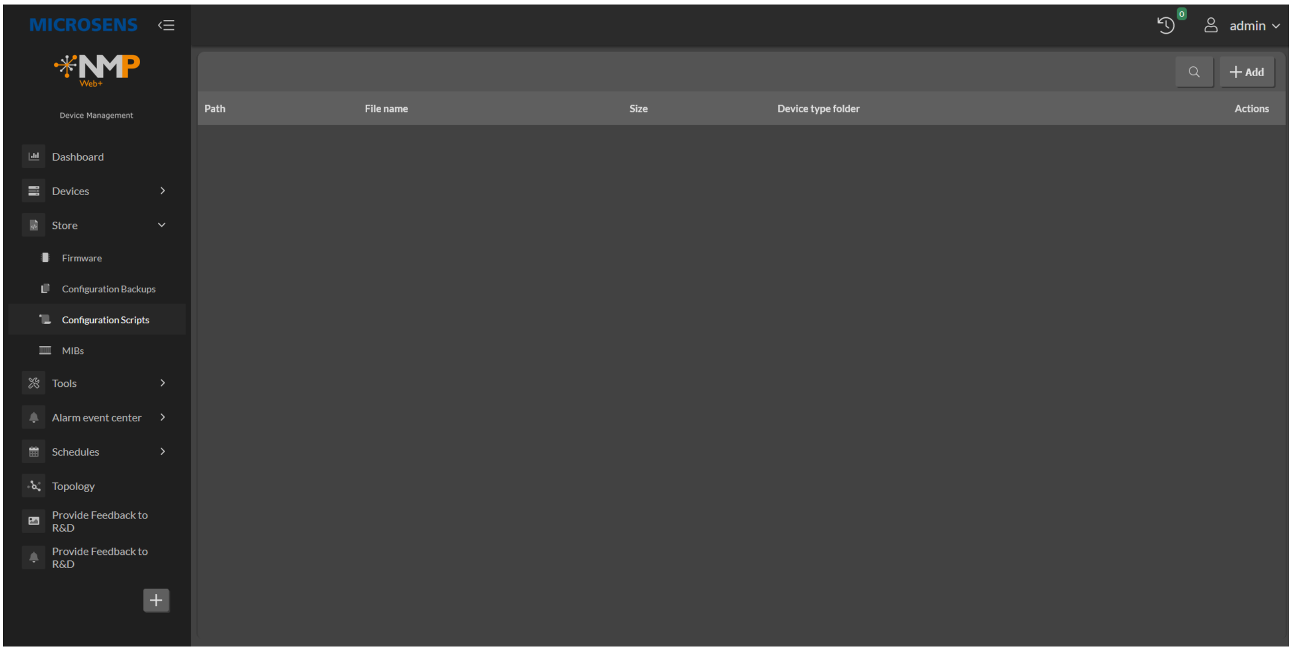
Figure 29. NMP Web+ - Devices - Store - Configuration backups

Each Backup can be deleted or exported in the `.yaml` format.

Selecting the export button on top of the table will export the complete list in the `.csv` format.

4.4.3.3. Configuration scripts

A configuration script can be added by selecting the +Add button. This will allow the selection of the correct DestinationFolder based on the device type of the file. By selecting [**upload file**], the OS specific file selection and upload menu will be opened, and the correct file can be selected.



Path	File name	Size	Device type folder	Actions

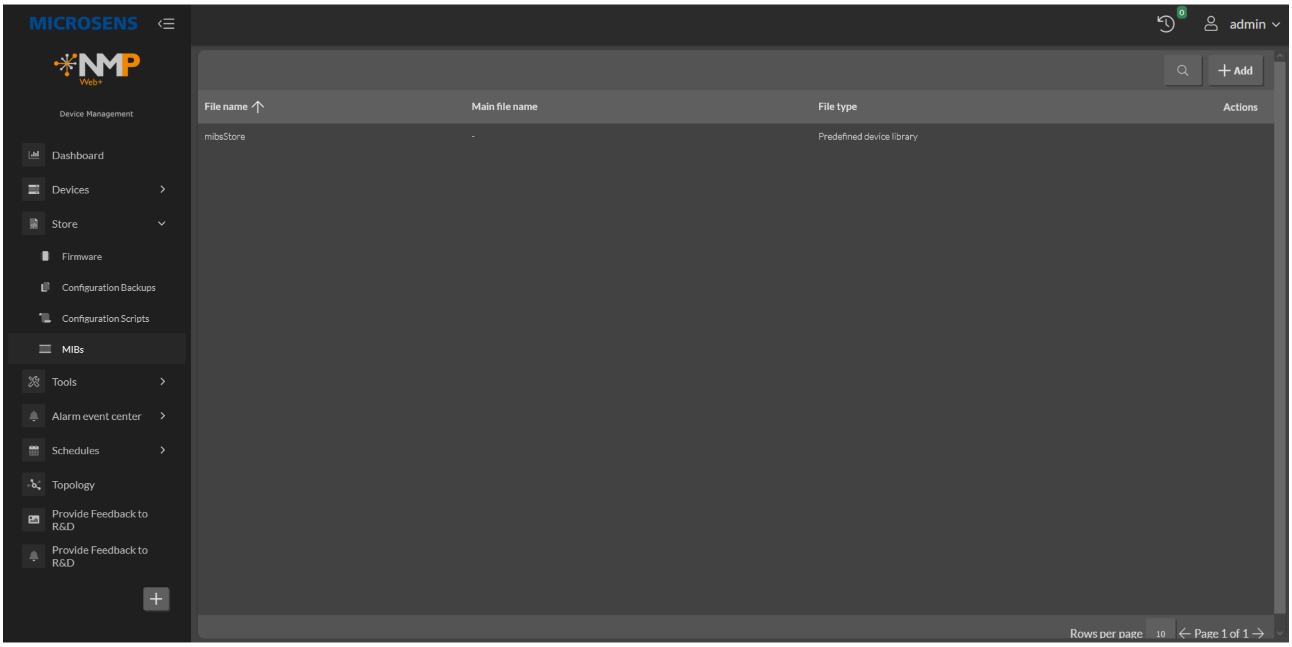
Figure 30. NMP Web+ - Devices - Store - Configuration scripts

The selected device DestinationFolder will be used to upload scripts to the devices. Selecting the wrong device DestinationFolder for the configuration script may lead to inconveniences when updating a device with this configuration script. For example, a G6 device can only be updated with configuration script files in the G6 DestinationFolder.

The uploaded configuration script can be deleted using the corresponding symbol. The overview always shows [**Device type folder**] to avoid confusion.

4.4.3.4. MIBs

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).



File name	Main file name	File type	Actions
mibsStore	-	Predefined device library	

Figure 31. NMP Web+ - Devices - Store - MIB

The MIB file for the server component’s SNMP agent is always installed together with NMP. The server component’s MIB file (`NMP_SERVER_MIB.mib`) (`SBM_SERVER_MIB.mib`) can be found in the folder `SERVER_INSTALLATION_PATH\mib\`.

The MIB contains several groups which provide information on the managed devices and the server instance status:

- **serverInfo:** Information of the server component’s version and status
- **deviceList:** Information of all the devices (modules, ports) managed by the server instance (available in the server’s devices list)
- **servicesList:** Information on configured services (defined port-to-port connections, links)
- **nmpServerTrap:** Traps sent by the server instance, including the following subgroups:
  - **nmpServerNotifications:** Information about server notifications
  - **eventData:** Information about the occurring event
- **nmpsConformance**

> For clarity, the following OIDs are skipped and substituted in the OID table below by "[…]":
>
> | OID | Name | Access |
> |---|---|---|
> | `1.3.6.1.4.1.3181` | `microsens` | RO |
> | `1.3.6.1.4.1.3181.5909` | `nmpServer` | RO |

OID	Name	Access	Description
[⋯].1	**serverInfo**		
[⋯].1.1	serverName	RO	Server name
[⋯].1.2	serverManufacturer	RO	Server manufacturer
[⋯].1.3	serverVersion	RO	Server version
[⋯].1.4	serverLicenseArticleNumber	RO	Server licence key file article number
[⋯].1.5	serverLicenseHolder	RO	Entitled user
[⋯].1.6	serverMaintenancePeriod	RO	Server maintenance period
[⋯].1.7	serverMaxActiveUsers	RO	Maximum number of active users supported
[⋯].1.8	serverCurrentActiveUsers	RO	Current number of active users
[⋯].1.9	serverStartTime	RO	Server start time
[⋯].1.10	serverUptime	RO	Server uptime
[⋯].1.11	serverReplicationMode	RO	Server replication mode
[⋯].1.12	serverReplicationStatus	RO	Server replication status
[⋯].2	**deviceList**		
[⋯].2.1	deviceListSize	RO	Server device list size
[⋯].2.2	deviceListTable	NA	Server device list
[⋯].2.2.1	deviceListTableEntry	NA	Entry in the device list table
[⋯].2.2.1.1	deviceIp	NA	Device IP address (table index)
[⋯].2.2.1.2	deviceSubnetMask	RO	Device subnet mask
[⋯].2.2.1.3	deviceGateway	RO	Device gateway
[⋯].2.2.1.4	deviceDhcpMode	RO	Device DHCP mode
[⋯].2.2.1.5	deviceMac	RO	Device MAC address
[⋯].2.2.1.6	deviceName	RO	Device name
[⋯].2.2.1.7	deviceLocation	RO	Device location
[⋯].2.2.1.8	deviceContact	RO	Person who is responsible for the device
[⋯].2.2.1.9	deviceGroup	RO	Device list group
[⋯].2.2.1.10	deviceInventoryString	RO	Device inventory string

OID	Name	Access	Description
[…].2.2.1.11	deviceStatus	RO	Device status: - noStatus (1) - downloadingData (2) - unavailable (3) - available (4) - resetting (5) - firmwareUpdate (6) - checking (7) - userDefinedAlarm (8)
[…].2.3	deviceModulesTable	NA	List of device modules
[…].2.3.1	deviceModulesTableEntry	NA	Device modules table
[…].2.3.1.1	moduleDeviceIp	NA	Device IP address (table index)
[…].2.3.1.2	moduleId	NA	Module position in the following syntax: nodeId:unitId:slotId (table index)
[…].2.3.1.3	moduleArticleNumber	RO	Module article number
[…].2.3.1.4	moduleSerialNumber	RO	Module serial number
[…].2.3.1.5	moduleFirmwareVersion	RO	Module firmware version
[…].2.3.1.6	moduleHardwareVersion	RO	Module hardware version
[…].2.3.1.7	moduleTemperature	RO	Module temperature
[…].2.3.1.8	moduleStatus	RO	Module status: - ok (1) - spareMode (2) - inactive (3) - warning (4) - alarm (5) - unknown (255)
[…].2.4	deviceModulePortsTable	NA	List of device module ports
[…].2.4.1	deviceModulePortsTableEntry	NA	Entry in the device module ports table
[…].2.4.1.1	portModuleDeviceIp	NA	Device IP address (table index)
[…].2.4.1.2	portModuleId	NA	Module position in the following syntax: nodeId/unitId/slotId (table index)
[…].2.4.1.3	portId	NA	Module port id (table index)
[…].2.4.1.4	portAlias	RO	Module port alias
[…].2.4.1.5	portStatus	RO	Module port state

OID	Name	Access	Description
[…].3	**servicesList**		
[…].3.1	servicesListSize	RO	Number of defined services
[…].3.2	servicesOk	RO	Number of services in the ok state
[…].3.3	servicesWarning	RO	Number of services in the warning state
[…].3.4	servicesError	RO	Number of services in the error state
[…].3.5	servicesListTable	NA	List of defined services
[…].3.5.1	servicesListTableEntry	NA	Entry in the services list table
[…].3.5.1.1	serviceId	NA	ID of service (table index)
[…].3.5.1.2	serviceName	RO	Name of service
[…].3.5.1.3	serviceDescription	RO	Detailed service description
[…].3.5.1.4	serviceState	RO	Service status
[…].100	**nmpServerTrap**		
[…].100.0	nmpServerNotifications		
[…].100.0.1	nmpServerSystemInfo		Event type =System Info
[…].100.0.2	nmpServerSystemOk		Event type =System OK
[…].100.0.3	nmpServerSystemError		Event type =System ERROR
[…].100.0.4	nmpServerDeviceSnmpTrap		Event type =SNMP Trap from device
[…].100.0.5	nmpServerDeviceResponseOk		Event type =Device Response OK
[…].100.0.6	nmpServerDeviceResponseError		Event type =No response from device
[…].100.0.7	nmpServerDeviceAccessError		Event type =Device access error (e.g. authentication issue)
[…].100.0.8	nmpServerDeviceConfigSend		Event type =New configuration sent to device
[…].100.0.9	nmpServerDeviceConfigAccepted		Event type =New configuration accepted by device
[…].100.0.10	nmpServerDeviceConfigError		Event type =New configuration not accepted by device
[…].100.0.11	nmpServerDeviceConfigBackupSave		Event type =Device configuration saved at the database

OID	Name	Access	Description
[…].100.0.12	nmpServerDeviceConfigBackupDelete		Event type =Device configuration deleted from database
[…].100.0.13	nmpServerDeviceFirmwareInfo		Event type =Device firmware update info
[…].100.0.14	nmpServerDeviceFirmwareOk		Event type =Device firmware update ok
[…].100.0.15	nmpServerDeviceFirmwareError		Event type =Device firmware update error
[…].100.0.16	nmpServerDeviceRingError		Event type =RING Error
[…].100.0.17	nmpServerDeviceStatusInfo		Event type =Device status info
[…].100.0.18	nmpServerDeviceStatusError		Event type =Device status error
[…].100.0.19	nmpServerServiceInfo		Event type =Service info
[…].100.0.20	nmpServerServiceError		Event type =Service error
[…].100.0.21	nmpServerSparePartMode		Event type =Spare Part mode
[…].100.0.22	nmpServerDeviceSyslog		Event type:Syslog from device received
[…].100.0.100	nmpServerShutdownTrap		Trap indicating that the server instance is shut down
[…].100.1	eventData		
[…].100.1.1	eventTime	AFN	Event time
[…].100.1.2	eventRelevance	AFN	Event relevance
[…].100.1.3	eventSeverity	AFN	Event severity
[…].100.1.4	eventSource	AFN	Event source like device, user or system
[…].100.1.5	eventSourceId	AFN	Event source ID like device IP address or user name
[…].100.1.6	eventMessage	AFN	
[…].200	**nmpsConformance**		
[…].200.1	nmpsGroups		
[…].200.1.1	nmpsServerInfoGroup		Information about server version and status
[…].200.1.2	nmpsDeviceListGroup		Information about devices at the server list

OID	Name	Access	Description
`[…].200.1.3`	`nmpsDeviceModulesListGroup`		Information about device modules
`[…].200.1.4`	`nmpsDeviceModulePortsListGroup`		Information about device module ports
`[…].200.1.5`	`nmpsServicesListGroup`		Information about defined services (end to end connections)
`[…].200.1.6`	`nmpsNotificationsGroup`		Server notifications
`[…].200.1.7`	`nmpsEventDataGroup`		Server trap objects
`[…].200.2`	`nmpsCompliances`		
`[…].200.2.1`	`nmpsCompliance`		Server compliance information

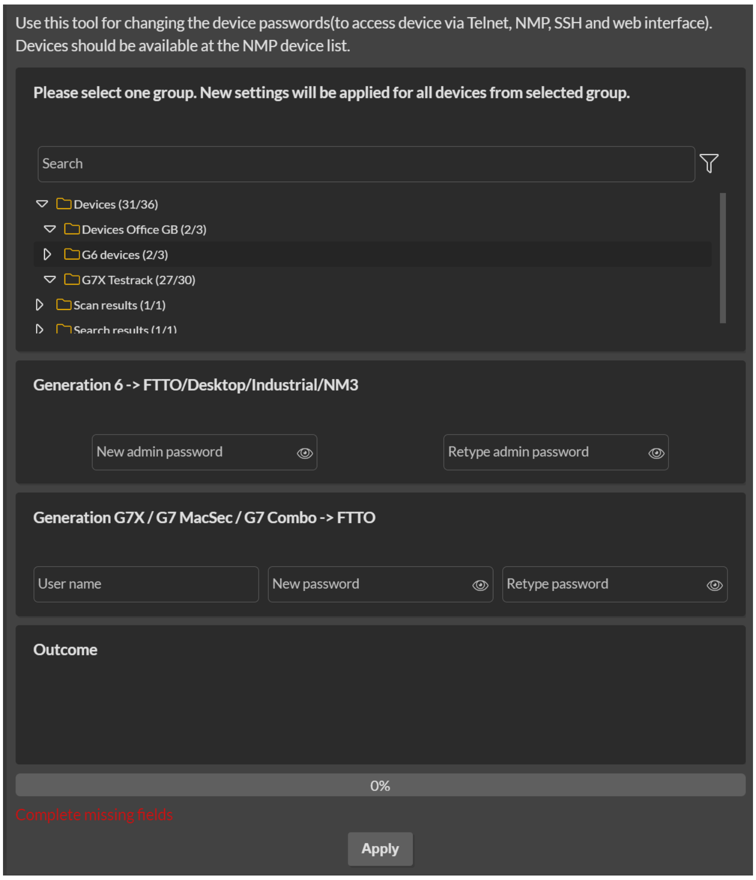
A MIB file can be added by selecting the +Add button. By selecting [**upload MIB files**], the OS specific file selection and upload menu will be opened, and the correct file can be selected. Afterwards, the main MIB file needs to be defined, then the upload can be carried out.

4.4.4. Tools

4.4.4.1. Device Passwords Changer

Use this tool to change the passwords of a group of switches (to access device via Telnet, NMP, SSH and web interface).

Devices should be available at the NMP device list.



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.

Search

- Devices (31/36)
  - Devices Office GB (2/3)
  - G6 devices (2/3)
  - G7X Testrack (27/30)
- Scan results (1/1)
- Search results (1/1)

Generation 6 -> FTTO/Desktop/Industrial/NM3

New admin password

Retype admin password

Generation G7X / G7 MacSec / G7 Combo -> FTTO

User name

New password

Retype password

Outcome

0%

Complete missing fields

Figure 32. NMP Web+ - Device - Tools - Device Password Changer

> To change the password of a single device, please use the The menu:[**Devices - Configuration**] menu and the tab [**Access**]*.

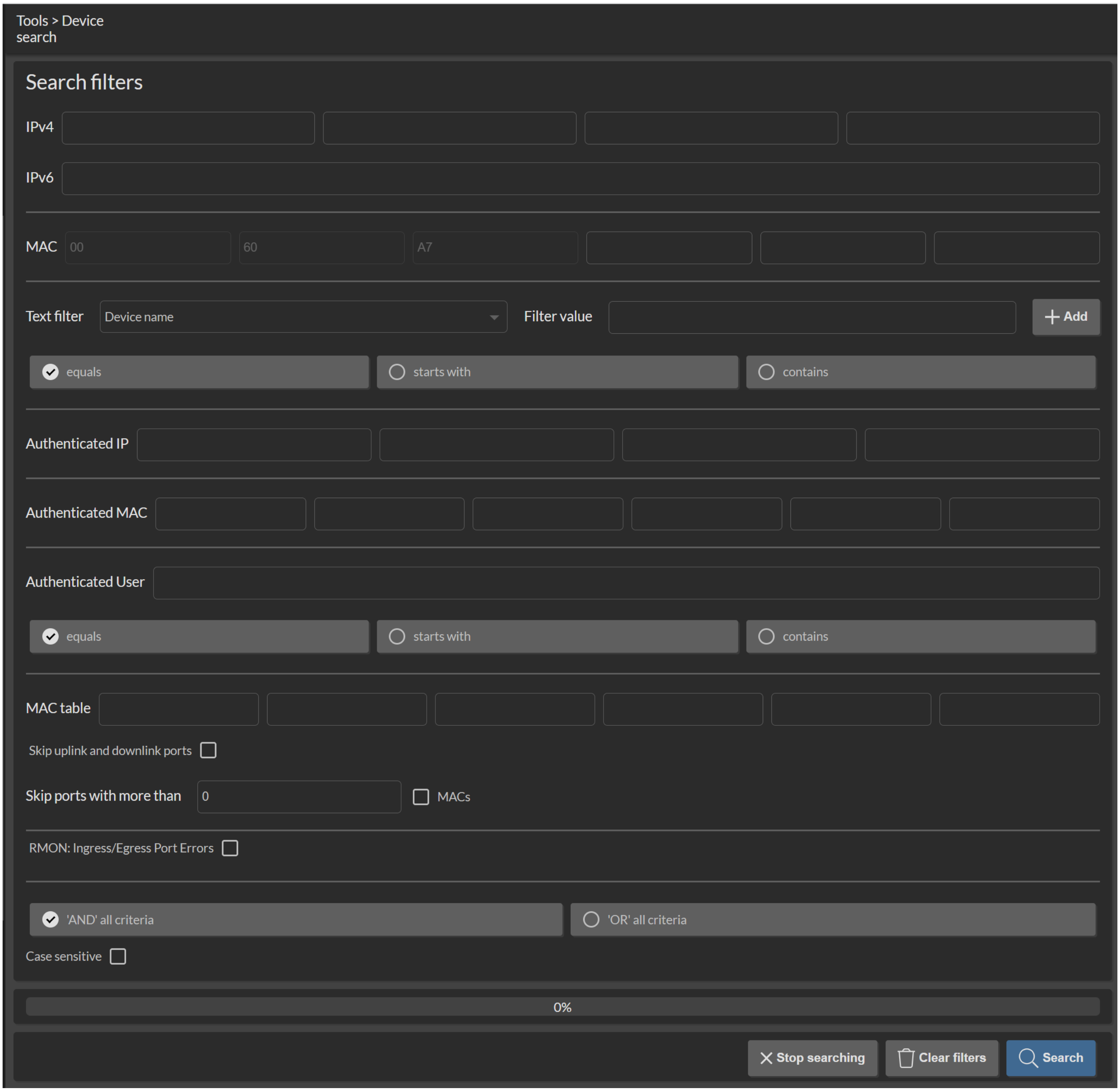
4.4.4.2. Device Search

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 Search button. All search results are displayed in the "Search results" table on the right-hand pane. Clicking on the [**+Add results to device list**] selects the identified device(s) and adds 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. This export includes the IP address and the deviceName.



Tools > Device search

Search filters

IPv4

IPv6

MAC: 00 : 60 : A7

Text filter: Device name — Filter value

☑ equals ○ starts with ○ contains

Authenticated IP

Authenticated MAC

Authenticated User

☑ equals ○ starts with ○ contains

MAC table

Skip uplink and downlink ports □

Skip ports with more than 0 □ MACs

RMON: Ingress/Egress Port Errors □

☑ 'AND' all criteria ○ 'OR' all criteria

Case sensitive □

0%

Figure 33. NMP Web+ - Device - Tools - Device Search Tool

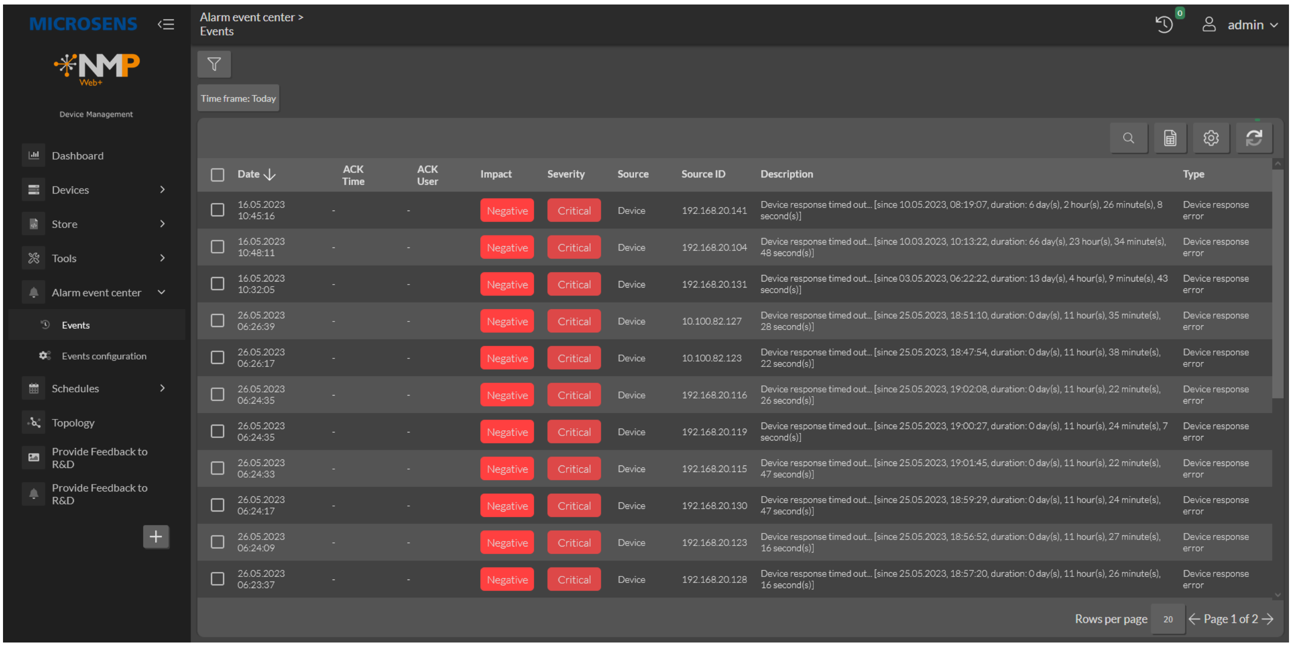
You can exit the [**Device search tool**] by selecting a different menu.

4.4.5. Alarm event center

The alarm event center shows the device alarms and allows the configuration of events.

4.4.5.1. Events

This panel is helpful to view some important SNMP traps at a first glance. It gives you a complete overview of the configured events within the defined timeframe and whether they have been acknowledged or not.



☐	Date ↓	ACK Time	ACK User	Impact	Severity	Source	Source ID	Description	Type
☐	16.05.2023 10:45:16	-	-	Negative	Critical	Device	192.168.20.141	Device response timed out... [since 10.05.2023, 08:19:07, duration: 6 day(s), 2 hour(s), 26 minute(s), 8 second(s)]	Device response error
☐	16.05.2023 10:48:11	-	-	Negative	Critical	Device	192.168.20.104	Device response timed out... [since 10.03.2023, 10:13:22, duration: 66 day(s), 23 hour(s), 34 minute(s), 48 second(s)]	Device response error
☐	16.05.2023 10:32:05	-	-	Negative	Critical	Device	192.168.20.131	Device response timed out... [since 03.05.2023, 06:22:22, duration: 13 day(s), 4 hour(s), 9 minute(s), 43 second(s)]	Device response error
☐	26.05.2023 06:26:39	-	-	Negative	Critical	Device	10.100.82.127	Device response timed out... [since 25.05.2023, 18:51:10, duration: 0 day(s), 11 hour(s), 35 minute(s), 28 second(s)]	Device response error
☐	26.05.2023 06:26:17	-	-	Negative	Critical	Device	10.100.82.123	Device response timed out... [since 25.05.2023, 18:47:54, duration: 0 day(s), 11 hour(s), 38 minute(s), 22 second(s)]	Device response error
☐	26.05.2023 06:24:35	-	-	Negative	Critical	Device	192.168.20.116	Device response timed out... [since 25.05.2023, 19:02:08, duration: 0 day(s), 11 hour(s), 22 minute(s), 26 second(s)]	Device response error
☐	26.05.2023 06:24:35	-	-	Negative	Critical	Device	192.168.20.119	Device response timed out... [since 25.05.2023, 19:00:27, duration: 0 day(s), 11 hour(s), 24 minute(s), 7 second(s)]	Device response error
☐	26.05.2023 06:24:33	-	-	Negative	Critical	Device	192.168.20.115	Device response timed out... [since 25.05.2023, 19:01:45, duration: 0 day(s), 11 hour(s), 22 minute(s), 47 second(s)]	Device response error
☐	26.05.2023 06:24:17	-	-	Negative	Critical	Device	192.168.20.130	Device response timed out... [since 25.05.2023, 18:59:29, duration: 0 day(s), 11 hour(s), 24 minute(s), 47 second(s)]	Device response error
☐	26.05.2023 06:24:09	-	-	Negative	Critical	Device	192.168.20.123	Device response timed out... [since 25.05.2023, 18:56:52, duration: 0 day(s), 11 hour(s), 27 minute(s), 16 second(s)]	Device response error
☐	26.05.2023 06:23:37	-	-	Negative	Critical	Device	192.168.20.128	Device response timed out... [since 25.05.2023, 18:57:20, duration: 0 day(s), 11 hour(s), 26 minute(s), 16 second(s)]	Device response error

Figure 34. NMP Web+ - Alarm event center - Events

The [**Reload**] button will reload the table and provide a notification saying: **Events: data up to date**.

The [**Settings**] button allows you to add or delete rows, change their position via drag and drop, and configure different colours for each severity level. By pressing [**Save and Close**] the changes will be saved, by selecting [**Restore Default**] they will be discarded.

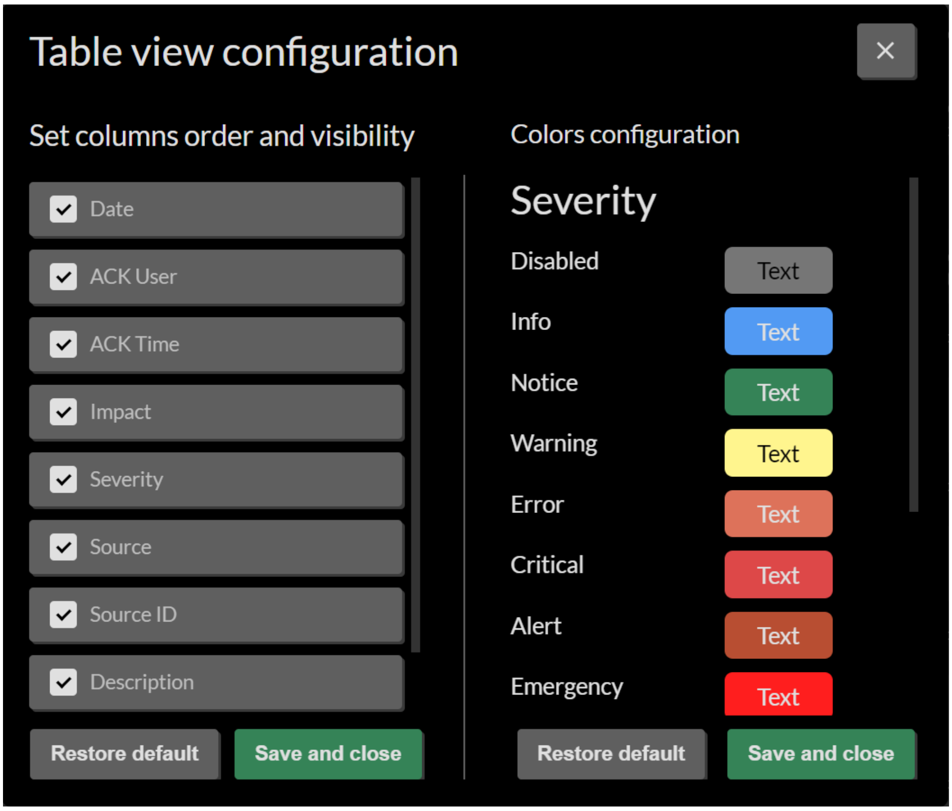


Table view configuration

Set columns order and visibility

- ☑ Date
- ☑ ACK User
- ☑ ACK Time
- ☑ Impact
- ☑ Severity
- ☑ Source
- ☑ Source ID
- ☑ Description

Colors configuration

Severity

Disabled	Text
Info	Text
Notice	Text
Warning	Text
Error	Text
Critical	Text
Alert	Text
Emergency	Text

Figure 35. NMP Web+ - Alarm event center - Events - Table view configuration

Sorting can be done by clicking on the row header, which toggles between ascending and descending order with each click.

It is possible to display the following information in the table:

- Date
- ACK User
- ACK Time
- Impact
- Severity
- Source
- Source ID
- Description
- Type

The table can be exported as a `.csv` file with the export button.

> The export file is arranged according to the table, so changes on the table will influence the export file as well.

By selecting the filter icon, you may filter the table based on the criteria listed:

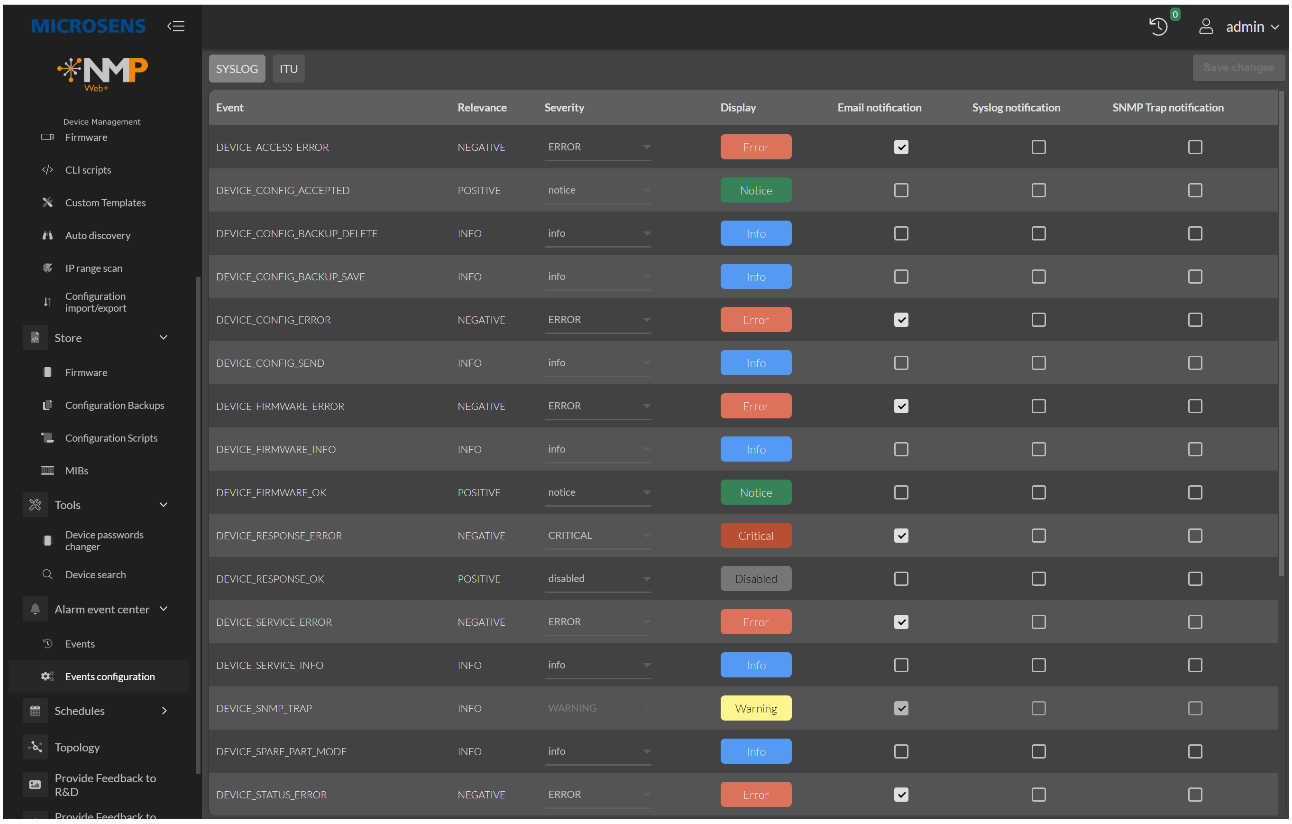
- severity

- Impact
- Source
- Time frame
- Acknowledged
- Types

And all the possible parameters.

The events can be selected with the checkbox, selecting the event allows to [**Acknowledge**] the selected, which will also set the ACK time parameter. [**Delete selected**] will delete the selected elements.

4.4.5.2. Events configuration



Event	Relevance	Severity	Display	Email notification	Syslog notification	SNMP Trap notification
DEVICE_ACCESS_ERROR	NEGATIVE	ERROR	Error	☑	☐	☐
DEVICE_CONFIG_ACCEPTED	POSITIVE	notice	Notice	☐	☐	☐
DEVICE_CONFIG_BACKUP_DELETE	INFO	info	Info	☐	☐	☐
DEVICE_CONFIG_BACKUP_SAVE	INFO	info	Info	☐	☐	☐
DEVICE_CONFIG_ERROR	NEGATIVE	ERROR	Error	☑	☐	☐
DEVICE_CONFIG_SEND	INFO	info	Info	☐	☐	☐
DEVICE_FIRMWARE_ERROR	NEGATIVE	ERROR	Error	☑	☐	☐
DEVICE_FIRMWARE_INFO	INFO	info	Info	☐	☐	☐
DEVICE_FIRMWARE_OK	POSITIVE	notice	Notice	☐	☐	☐
DEVICE_RESPONSE_ERROR	NEGATIVE	CRITICAL	Critical	☑	☐	☐
DEVICE_RESPONSE_OK	POSITIVE	disabled	Disabled	☐	☐	☐
DEVICE_SERVICE_ERROR	NEGATIVE	ERROR	Error	☑	☐	☐
DEVICE_SERVICE_INFO	INFO	info	Info	☐	☐	☐
DEVICE_SNMP_TRAP	INFO	WARNING	Warning	☑	☐	☐
DEVICE_SPARE_PART_MODE	INFO	info	Info	☐	☐	☐
DEVICE_STATUS_ERROR	NEGATIVE	ERROR	Error	☑	☐	☐

Figure 36. Server Manager - Tab "Syslog/Logs/Events" - Events configuration

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

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

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

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

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

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

ℹ | The color defined for the events in the [**Events**} menu will be used.

Icon	Severity Level SYSLOG (S) ITU (I)	Meaning
	S: disabled I: disabled	The event will not generate a log entry (neither displayed nor logged). It is greyed out.
ℹ	S: info I: cleared	This is an informational message that does not require special attention (e.g. system messages). It is formatted with black font color.
✓	S: notice I: normal	This is a success notification (e.g. configuration applied successfully). It is formatted with green font color.
⚠	S: WARNING I: WARNING	This is a low level warning message. It is formatted with black font color on a yellow background.
✖	S: ERROR I: MINOR	This is an error message that requires user attention. It is formatted with red font color.
✖	S: CRITICAL I: MAJOR	This is a critical error message that requires immediate user attention. It is formatted with black font color on a red background.
✖	S: ALERT I: CRITICAL	This is an alert message. It is formatted with black font color on a red background.
✖	S: EMERGENCY I: EMERGENCY	This is an emergency message. It is formatted with black font color on a red background.
	S: debug I: debug	This message contains debugging information. It is formatted with blue font color.

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

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

- **Sound notification:** When an event occurs, the server rings a sound.
- **Email notification:** When an event occurs, the server sends an email to all the defined recipients.

> ℹ | Configure the SMTP server on the Email Notification tab.

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

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

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

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

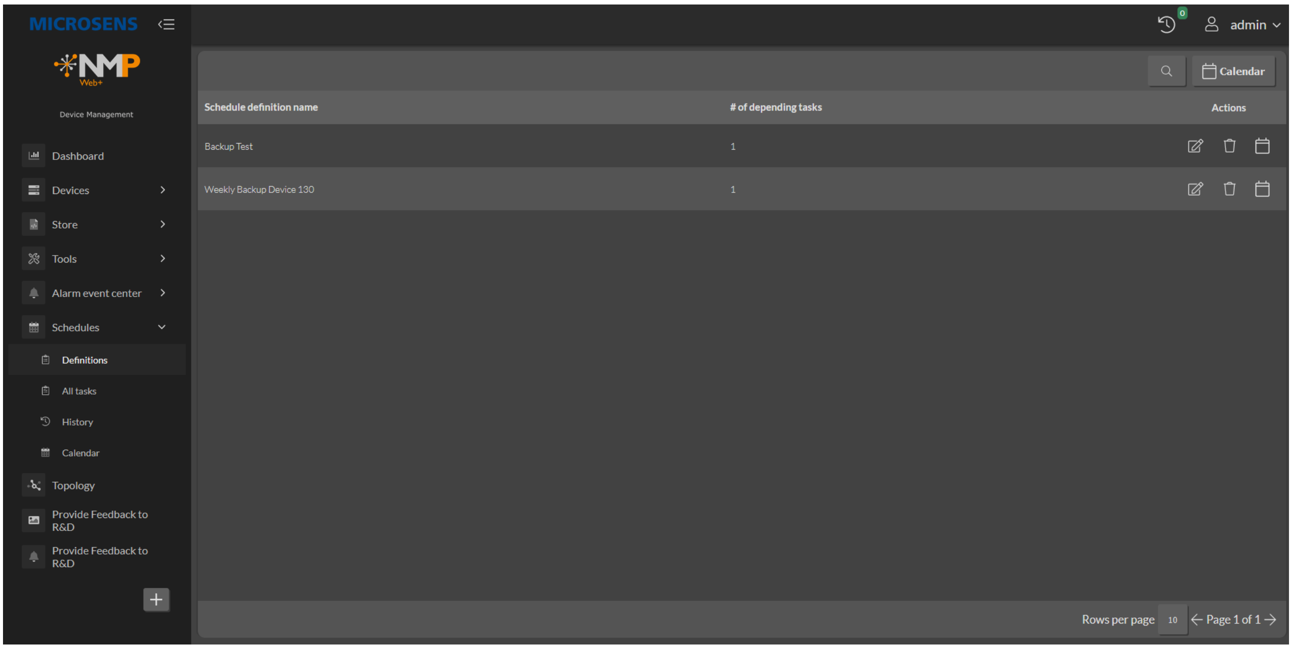
4.4.6. Schedules

Within the schedules' menu, the following settings can be done:

- **Definitions** allows seeing and altering defined scheduled events Section 4.4.6.1
- **All tasks** provides information about the events and their execution status Section 4.4.6.2
- **History** provides information about the event history Section 4.4.6.3
- **Calendar** provides a calendar view about executed and upcoming events Section 4.4.6.4

4.4.6.1. Definitions

Definitions shows scheduled device events generated by NMP, for example by scheduling firmware updates via the [**Devices Firmware**] menu or backup events via the [**Devices Configuration import/export**] menu.



Schedule definition name	# of depending tasks	Actions
Backup Test	1	
Weekly Backup Device 130	1	

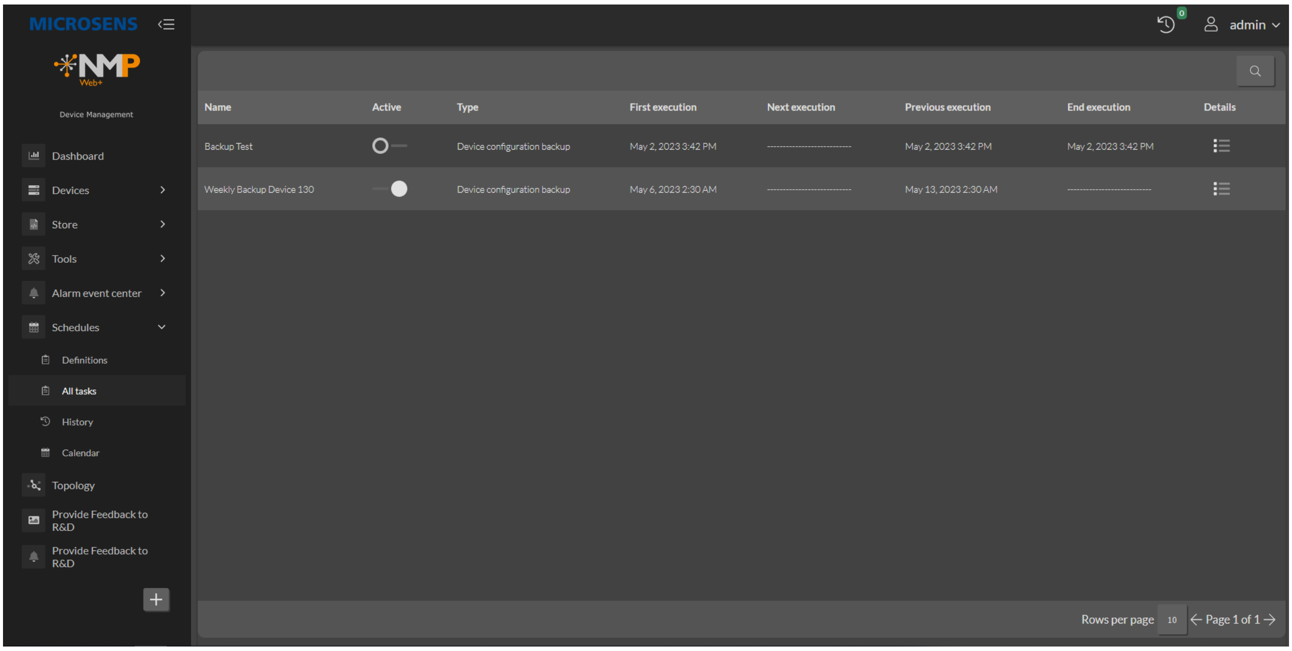
Figure 37. NMP Web+ - Schedules - Definitions

The [**Definitions**] menu allows the configuration of all the events in one place. By selecting the edit symbol, all settings of the events can be changed:

- Schedule definition name
- Time definitions
- Start Date
- End Date
- Time Zone
- Frequency

4.4.6.2. All tasks

The [**All tasks**] menu provides information about the events and their execution status.



Name	Active	Type	First execution	Next execution	Previous execution	End execution	Details
Backup Test	○	Device configuration backup	May 2, 2023 3:42 PM	------------------------	May 2, 2023 3:42 PM	May 2, 2023 3:42 PM	☰
Weekly Backup Device 130	●	Device configuration backup	May 6, 2023 2:30 AM	------------------------	May 13, 2023 2:30 AM	------------------------	☰

Rows per page 10 ← Page 1 of 1 →

Figure 38. NMP Web+ - Schedules - All tasks

Sorting can be done by clicking on the row header, which toggles between ascending and descending order with each click.

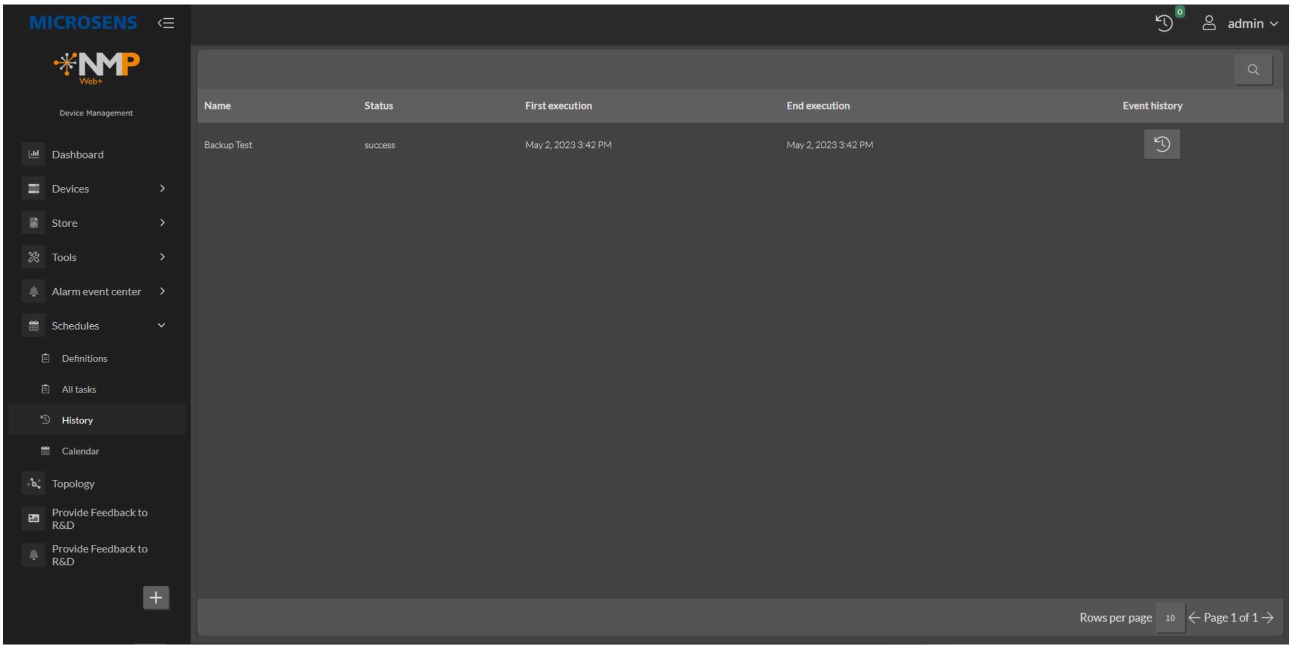
The menu makes it easily visible if a

- task is active or not,
- when it was first executed,
- when it will be executed the next time,
- when it was executed the last time and
- when the scheduled task ends.

Details about the device’s IP addresses are shown, when [**details**] ☰ is selected.

4.4.6.3. History

History provides information about the event history.



Name	Status	First execution	End execution	Event history
Backup Test	success	May 2, 2023 3:42 PM	May 2, 2023 3:42 PM	

Rows per page 10 Page 1 of 1

Figure 39. NMP Web+ - Schedules - History

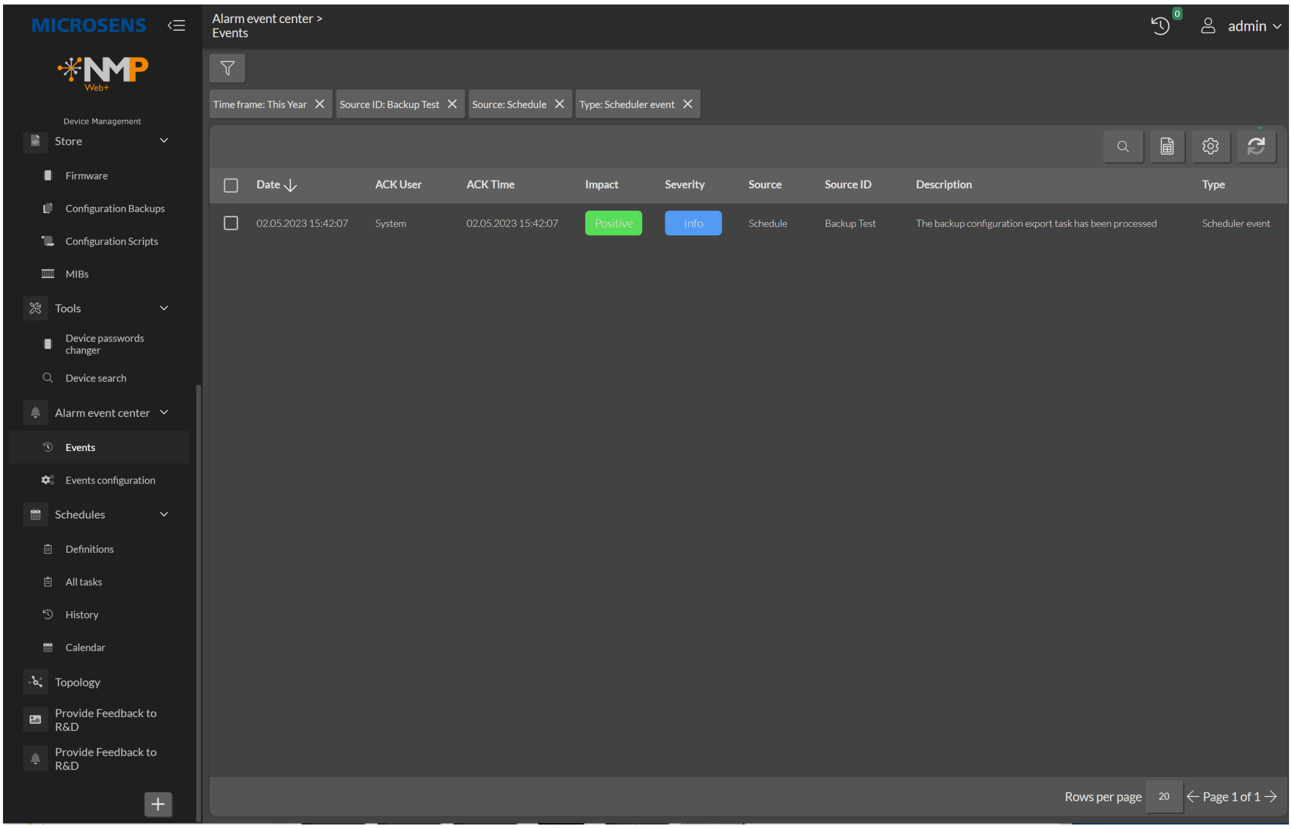
Sorting can be done by clicking on the row header, which toggles between ascending and descending order with each click.

The menu makes it easily visible if a

- task was successful,
- when the task was first executed,
- when it was executed the last time and
- provides an overview of the history of the event.

4.4.6.3.1. Historic event view

The historic view of the event is opened when the customer selects the button. This will open a specific view in the [**Alarm and event center**].



Time frame: This Year ✕ Source ID: Backup Test ✕ Source: Schedule ✕ Type: Scheduler event ✕

□	Date ↓	ACK User	ACK Time	Impact	Severity	Source	Source ID	Description	Type
□	02.05.2023 15:42:07	System	02.05.2023 15:42:07	Positive	Info	Schedule	Backup Test	The backup configuration export task has been processed	Scheduler event

Figure 40. NMP Web+ - Schedules - History - Historic event view

The [**Reload**] button will reload the table and provide a notification saying: **Events: data up to date**.

The [**settings**] button allows changing, add or delete rows, change their position via drag and drop and configure the colors for each severity level different. By selecting [**Save and Close**] the changes will be saved, by selecting [**Restore default**] they will be discarded.

With the [**export button**], the table is being exported as `.csv`.

The export file is arranged according to the table, so changes on the table will influence the export file as well.

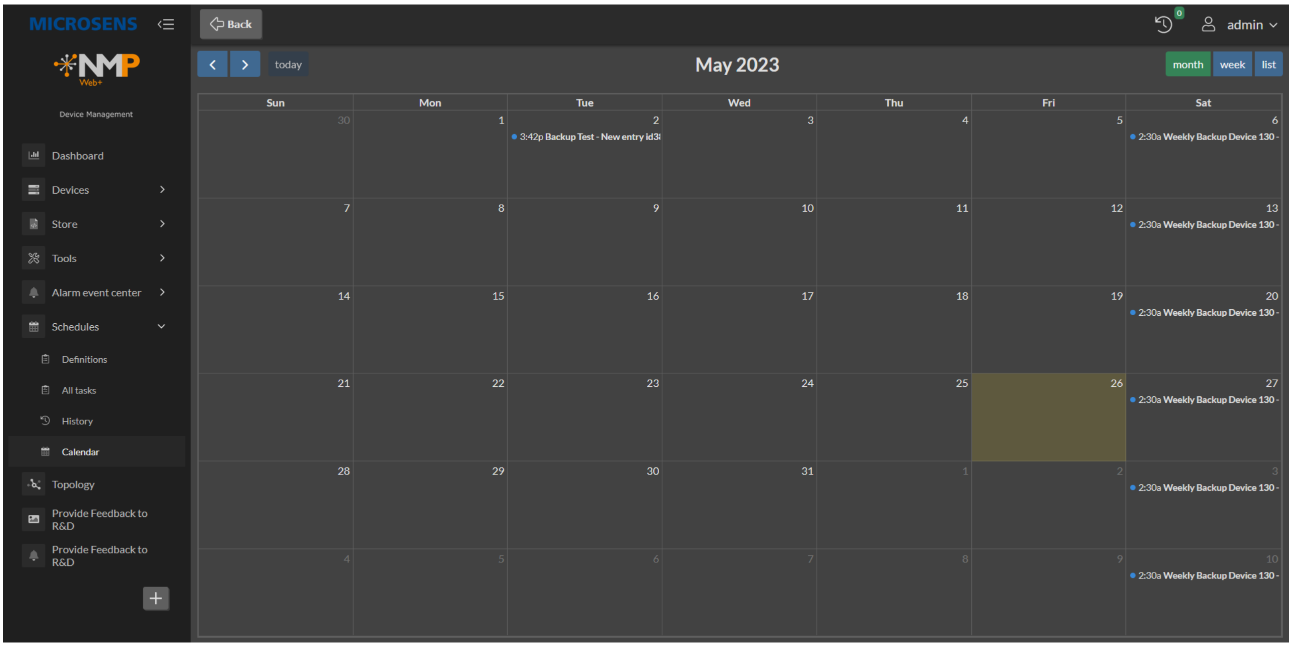
By selecting the [**filter**] icon, you may filter the table based on the criteria listed:

- severity
- Impact
- Source
- Time frame
- Acknowledged
- Types

And all the possible parameters.

The historic events can be selected with the checkbox, selecting the event allows to [**Acknowledge**] the selected, which will also set the ACK time parameter. [**Delete selected**] will delete the selected elements.

4.4.6.4. Calendar



May 2023

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2 3:42p Backup Test - New entry id3	3	4	5	6 2:30a Weekly Backup Device 130 -
7	8	9	10	11	12	13 2:30a Weekly Backup Device 130 -
14	15	16	17	18	19	20 2:30a Weekly Backup Device 130 -
21	22	23	24	25	26	27 2:30a Weekly Backup Device 130 -
28	29	30	31	1	2	3 2:30a Weekly Backup Device 130 -
4	5	6	7	8	9	10 2:30a Weekly Backup Device 130 -

Figure 41. NMP Web+ - Schedules - Calendar

The calendar is used to display planned tasks performed on managed devices such as firmware updates, configuration backups and RMA IP range scans. The calendar is filled automatically. It is possible to edit, delete or start all the tasks immediately, by selecting them and setting the desired action. This tool provides information on the task name, description, start time.

The view can be changed between month, week and list view.

4.4.7. Topology

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

The standard view is the all devices view, which shows a map of the devices:

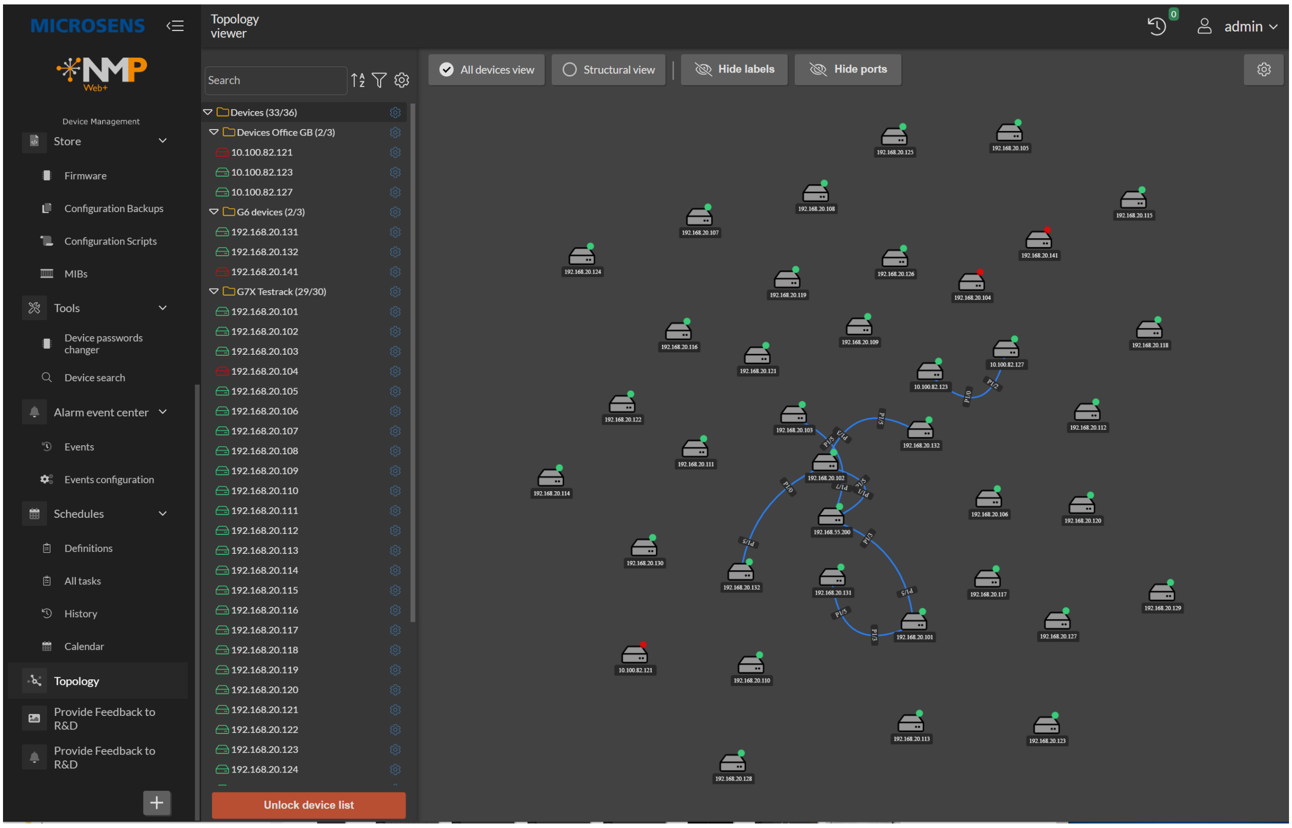
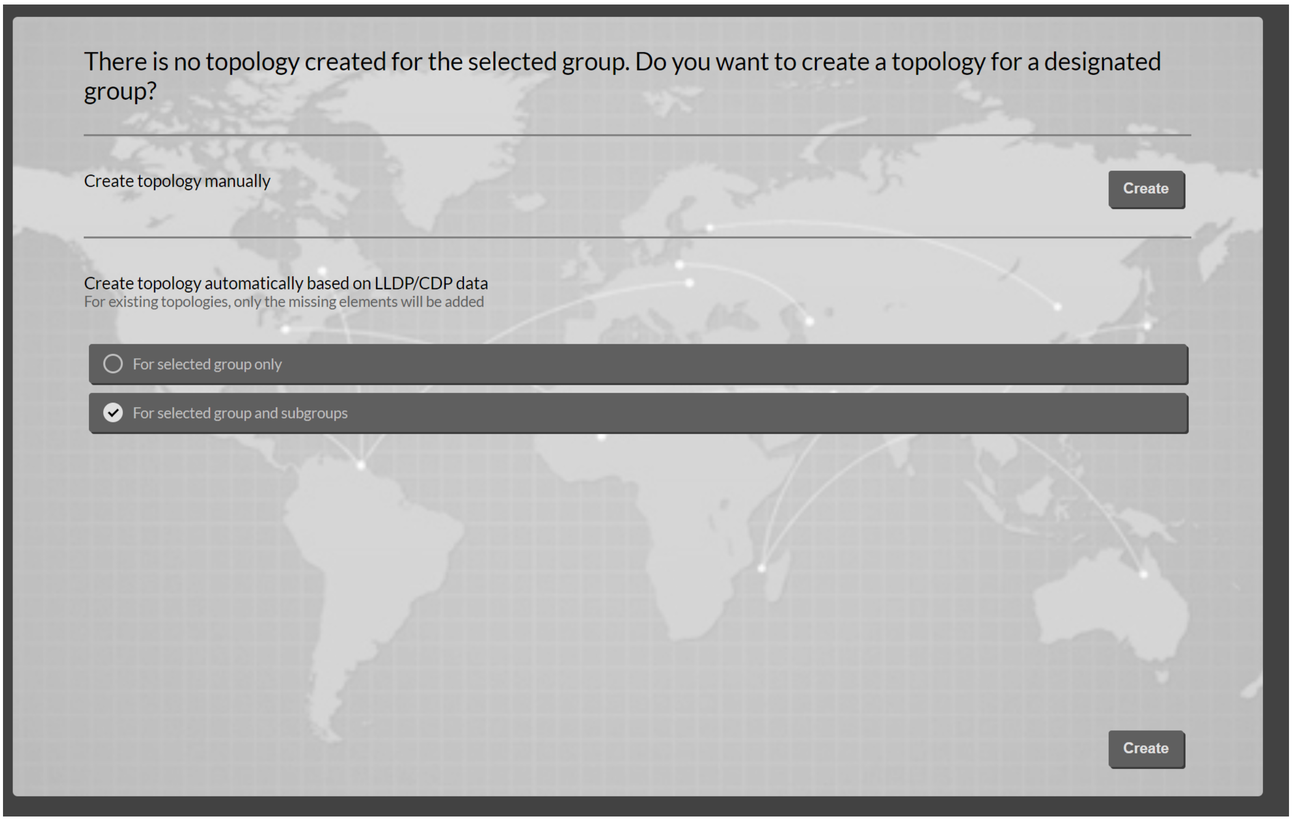


Figure 42. NMP Web+ - Devices - Topology

Selecting [**Structural view**] for the first time will allow configuration of the structural view:



There is no topology created for the selected group. Do you want to create a topology for a designated group?

Create topology manually

Create topology automatically based on LLDP/CDP data
For existing topologies, only the missing elements will be added

○ For selected group only

✓ For selected group and subgroups

Figure 43. NMP Web+ - Devices - Topology - Structural view assistant

Once the suitable option has been selected and the view has been created, the device list can be unlocked, and the Editor can be used in order to provide an easily readable view. The editor also allows the addition of pictures in the background, for example a map, to show the physical position of the device.

> If the customer wants to return to the view, the topology must first be deleted. This is possible when the [**Editor**] is used to change the structural view and the [**Delete topology**] button is selected.

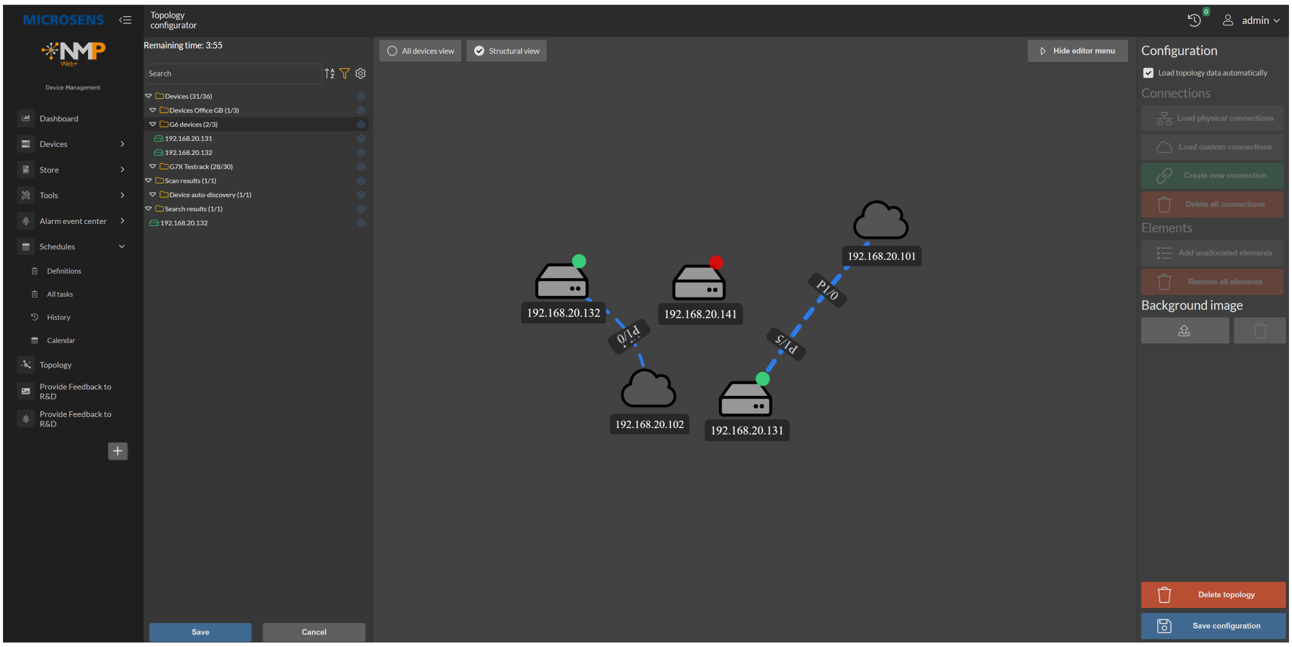


Figure 44. NMP Web+ - Devices - Topology - Topology Editor

By selecting the link between the devices, a device view is shown, displaying the connection ports for the connected devices. This also works on the "all devices" view

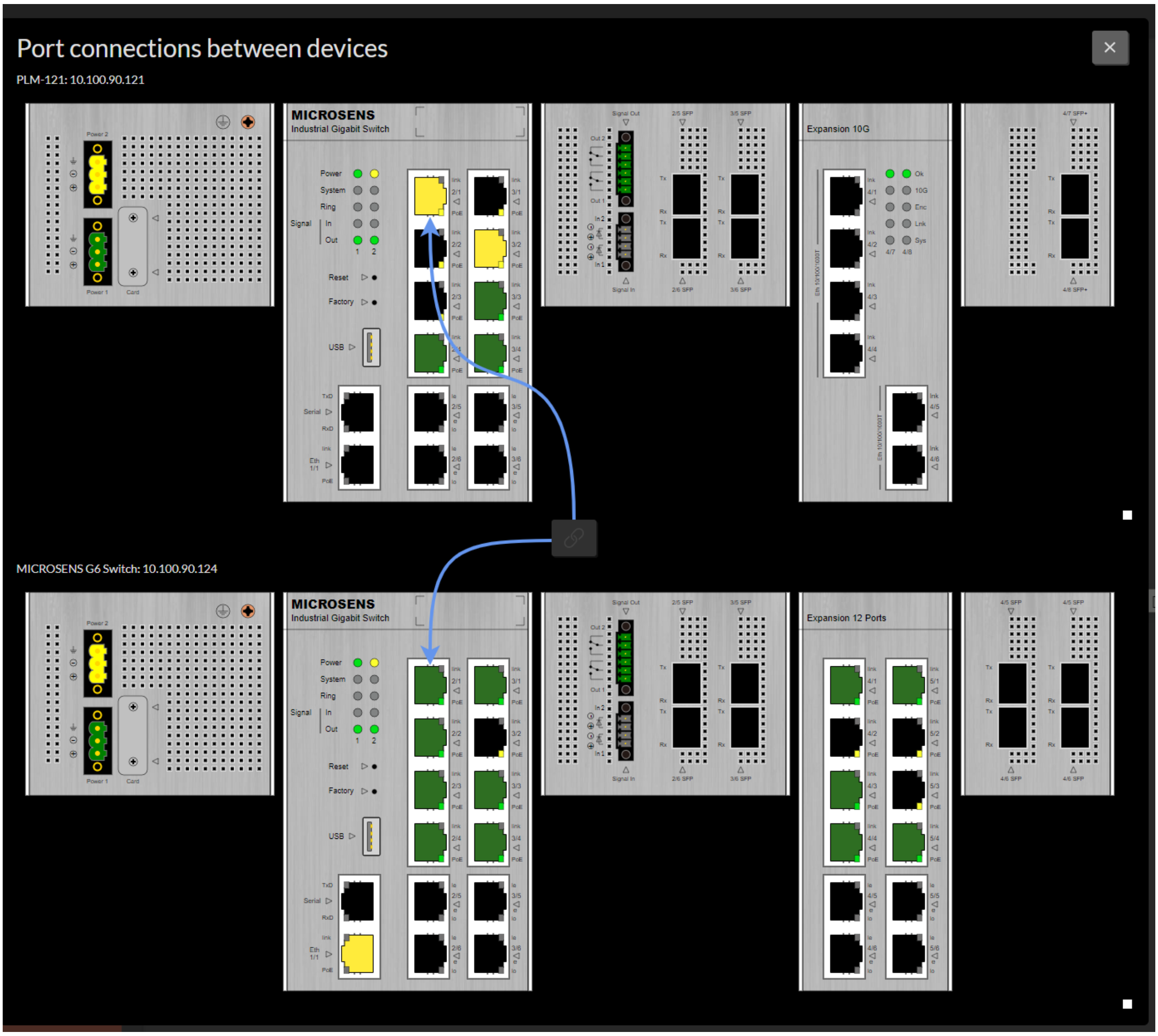

Port connections between devices
PLM-121: 10.100.90.121
MICROSENS
Industrial Gigabit Switch
Expansion 10G
MICROSENS G6 Switch: 10.100.90.124
MICROSENS
Industrial Gigabit Switch
Expansion 12 Ports

Figure 45. NMP Web+ - Devices - Topology - Port connection view

The user can select if labels and ports need to be shown on the overview, by clicking on the Show/Hide labels and Show/Hide ports symbol.

4.5. Server Configuration

With the new NMP Web+, the server can be managed and configured as it was with previous NMP versions via the server manager window and by using the new Web Interface. This gives a possibilty to change some server parameters without a need to stop the server when it runs as a Windows service or Linux daemon in the background. It also gives the admin a possibility to check the current server configuration without stopping the service/daemon in order to use the server manager window or analyze the configuration files.

4.5.1. Server Settings

The server settings menu allows configuring all the server instance’s parameters.
The menu options that are available are:

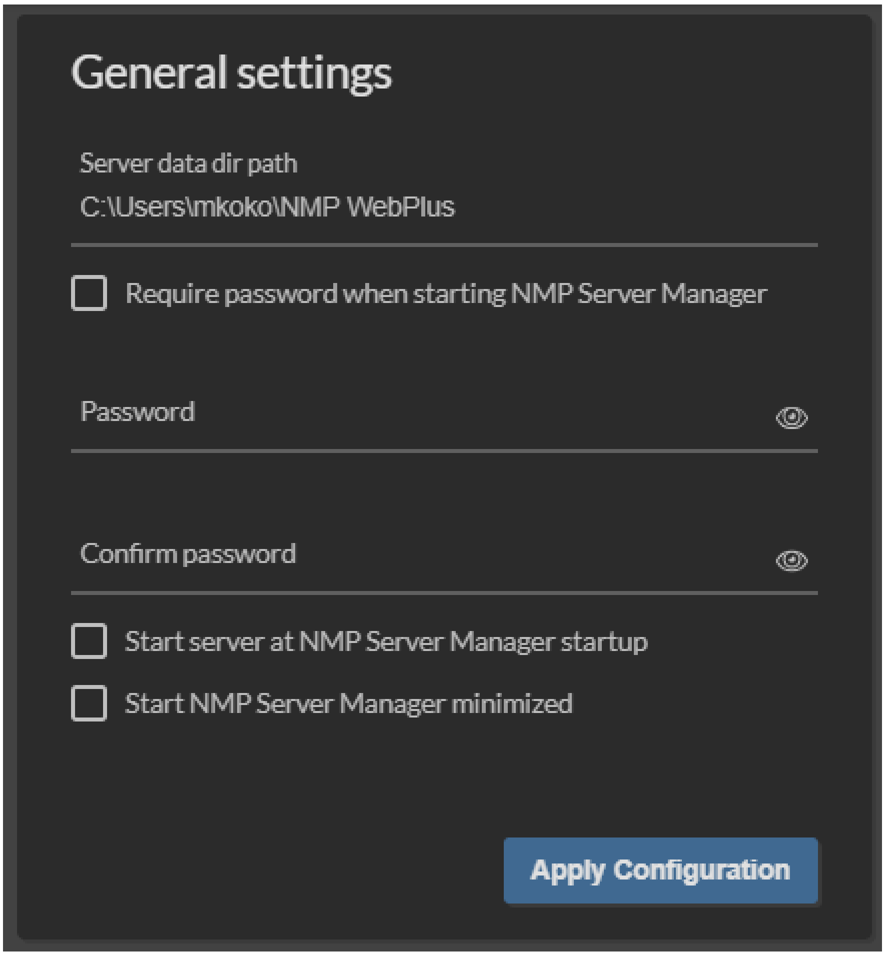
- **Server Properties**: General server settings for data directory and Web Client access.
- **Communication Interfaces**: IP interfaces for device communication, device discovery and client access.
- **Client Authentication**: Configuration of authentication for registered users.
- **Syslog**: Configuration of Syslog client/server service.
- **Database Backup**: Settings on when and where the application should save database backups.
- **Database Replication**: Configuration of the database replication feature.
- **Email Notification**: Configuration of email addresses for notifications on errors, SNMP traps and scheduled task events.
- **SNMP Agent Communication**: Configuration of the SNMP Agent.
- **SNMP Trap Relay**: Configuration of SNMP Trap relay feature.
- **Server Startup-Logs**: Server startup information.
- **Server Status**: Server statistics. Information about logged in users.
- **Server Diagnostic**: Configuration of logging.
- **Server Ports**: Information about ports used by server for firewall configuration.

4.5.1.1. Server Properties

The **Server Properties** panel contains the following settings and options:

- **General settings**: General settings for data directory, password protection and start-up handling.
    - **Server data dir path**: Select the location where the server will save all the configuration files and database data. In the selected destination folder, a respectively named folder will be created.
    - **Require password when starting NMP Server Manager**: When selected, the password prompt will be displayed before opening the Server Manager window. This function can be used to protect the server from re-configuration.

- **Start server on Server Manager Startup**: Automatically starts the server instance (database engine, device data collector and, if enabled, HTTP(S) server) on start-up. If the Server Manager is added to the list of OS auto-start applications, the application’s Server Manager will be started automatically and ready to use after OS boot.
- **Start Server Manager minimized**: Starts the Server Manager and runs it in a minimized window. The important Server Manager features will be available for access via the system tray icon.



General settings

Server data dir path
C:\Users\mkoko\NMP WebPlus

□ Require password when starting NMP Server Manager

Password

Confirm password

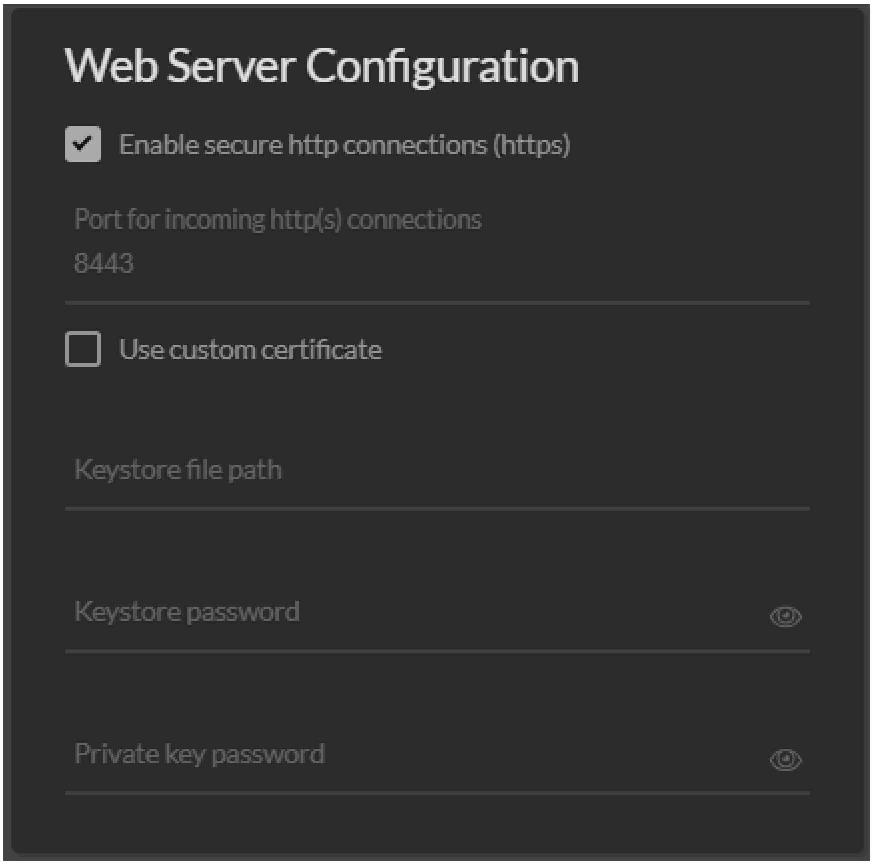
□ Start server at NMP Server Manager startup

□ Start NMP Server Manager minimized

Figure 46. NMP Web+ - Server Configuration - Server Settings - Server Properties - General Settings

- **Web Server Configuration**: Web server settings for security and ports.
  - **Enable secure http connections (https)**: The server instance offers secured HTTP connections for web access. The https connections are encrypted so the communication between clients and server is safe.
  - **Port for incoming https(s) connections**: The port that will be used for the HTTP(S) server. On default the server instance uses the ports 8080 for standard HTTP and 8443 for HTTPS connections.
  - **Use custom certificate**: Check this option to use your own certificate for https communication. The certificate is stored inside a Java KeyStore (JKS) repository.

  - **Keystore file path**: Select the directory and the name of the JKS file.
  - **Keystore password**: Enter the password that is protecting the JKS file.
  - **Private key password**: Enter the password that is protecting your private key.



Web Server Configuration

☑ Enable secure http connections (https)

Port for incoming http(s) connections: 8443

□ Use custom certificate

Keystore file path

Keystore password

Private key password

Figure 47. NMP Web+ - Server Configuration - Server Settings - Server Properties - Web Server Configuration

All options are read-only via the web client as any changes here requires server restart.

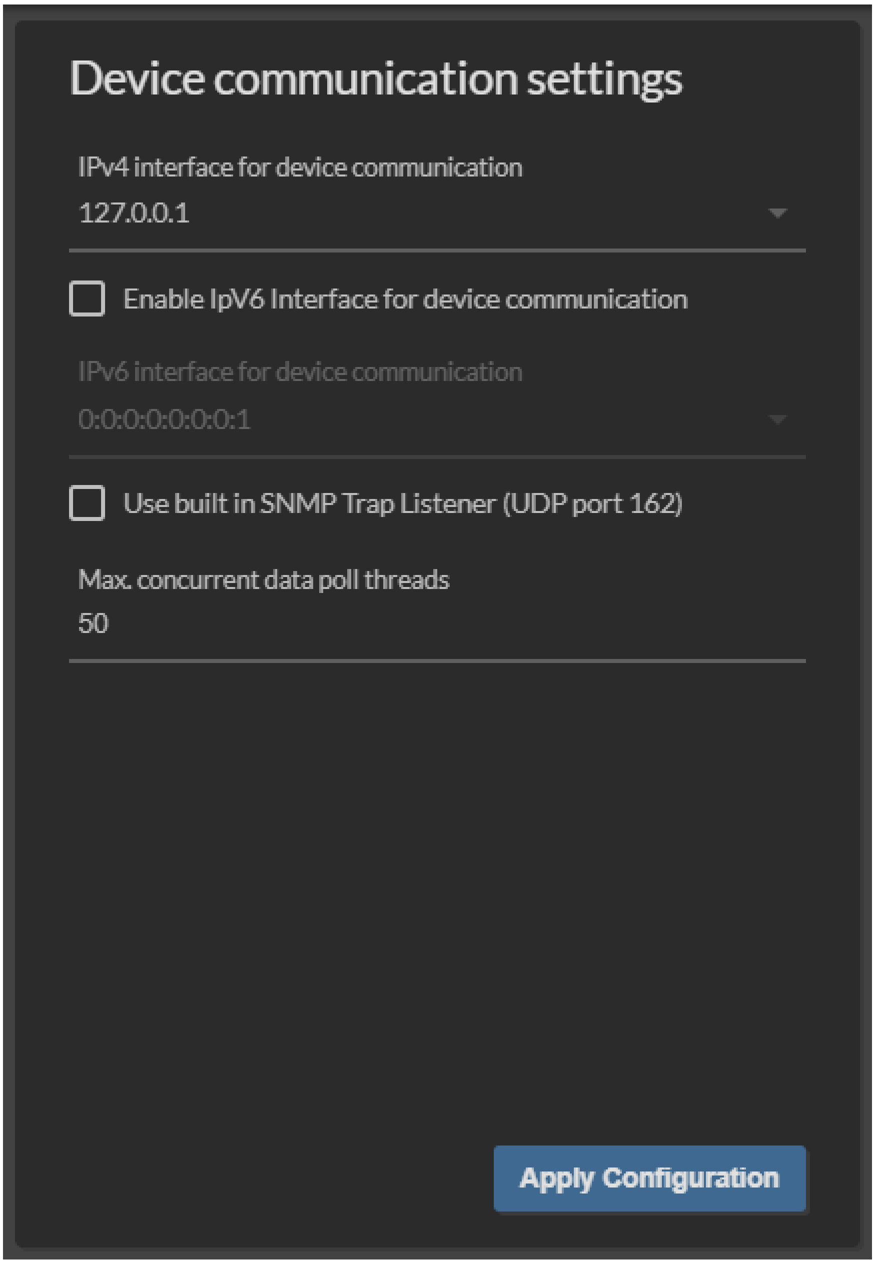
4.5.1.2. Communication Interfaces

The **Communication Interfaces** panel contains the following settings and options:

- **Device Communication Settings**: Parameters for communication between the server instance and connected devices.
  - **IPv4 Interface for device communication**: Shows the IPv4 address of the network interface that will be used for communication with the managed devices. In a more complex network infrastructure where the server hardware has more than one network adapter, it is possible to use one interface (accessible exclusively from secured local network) for device communication and another one (accessible from external network) for client access. Thanks to this function the clients do not have the direct access to managed devices. The devices can be accessed exclusively through the server process.
  - **Enable IPv6 Interface for device communication**: Enables the possibility to

use IPv6 interface for communication with devices.

- **IPv6 Interface for device communication**: Shows the IPv6 address of the network interface that will be used for communication with the managed devices.
- **Use built-in SNMP Trap Listener (UDP port 162)**: The server process has a built-in SNMP trap listener to receive traps from network devices. On default the trap listener is disabled. If there is no other trap receiver in use in the network it is possible to enable this function.
- **Max. Concurrent data poll threads**: This parameter is used to define the number of devices that can be polled simultaneously. For slower servers, heavily loaded networks or slow network connections, we recommend reducing this value for better performance.



Device communication settings

IPv4 interface for device communication
127.0.0.1

□ Enable IpV6 Interface for device communication

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

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

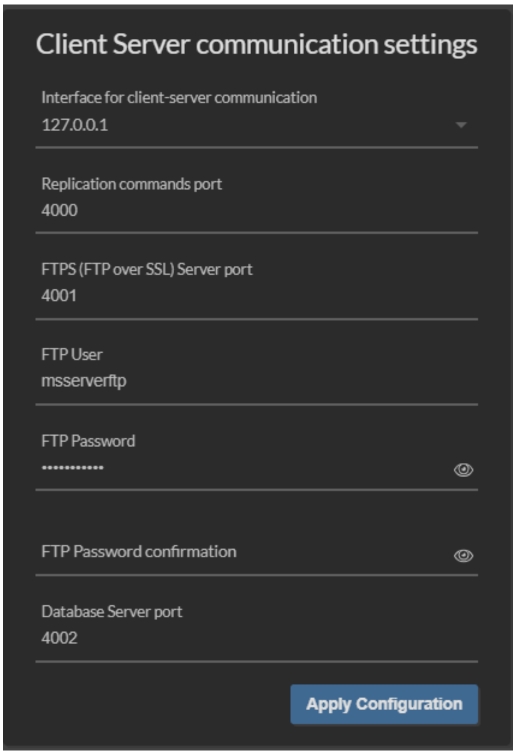
Max. concurrent data poll threads
50

Figure 48. NMP Web+ - Server Configuration - Server Settings - Communication Interfaces - Device Communication Settings

- **Client-Server Communication settings**: Parameters for communication between server instance and the application's client component.
  - **Interface for client-server communication**: The IPv4 address of the network interface that will be used for the application's client access. If the HTTP server is enabled for web client access, this interface is also used by the built-in HTTP server.
  - **Replication commands port**: The port that is used by the master and slave server to communicate when the replication function is enabled (4000 on default).
  - **FTPS (FTP over SSL) Server port**: The built-in FTPS server is used by the application's client to synchronize device lists and firmware updates (4001 on

default).

- **FTP User**: Enter the user name that is registered in the FTP server.
- **FTP Password**: Enter the user password that is registered in the FTP server.
- **Database Server port**: The port used by the built-in database server for the application’s client access (4002 on default).



Client Server communication settings

Interface for client-server communication
127.0.0.1

Replication commands port
4000

FTPS (FTP over SSL) Server port
4001

FTP User
msserverftp

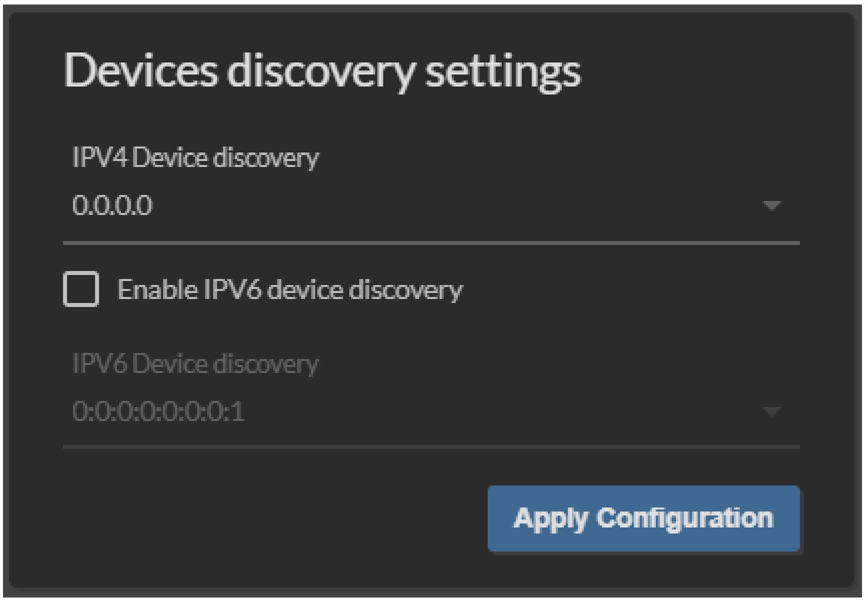
FTP Password
•••••••••••

FTP Password confirmation

Database Server port
4002

Figure 49. NMP Web+ - Server Configuration - Server Settings - Communication Interfaces - Client Server Communication Settings

- **Device Discovery settings**: Configuration of the interfaces for device discovery in the network.
  - **IPv4 Interface for device discovery**: The IPv4 address of the network interface that will be used for detecting and communicating with the managed devices. In a more complex network infrastructure where the server hardware has more than one network adapter, it is possible to use one interface (accessible exclusively from secured local network) for device communication and another one (accessible from external network) for client access. Thanks to this function the clients do not have the direct access to managed devices. The devices can be accessed exclusively through the server instance.
  - **Enable IPv6 device discovery**: Enables the possibility to use IPv6 interface for device discovery.
  - **IPv6 Interface for device discovery and communication**: The IPv6 address of the network interface that will be used for communication with the managed devices.



Devices discovery settings

IPV4 Device discovery
0.0.0.0

☐ Enable IPV6 device discovery

IPV6 Device discovery
0:0:0:0:0:0:0:1

Figure 50. NMP Web+ - Server Configuration - Server Settings - Communication Interfaces - Devices Discovery Settings

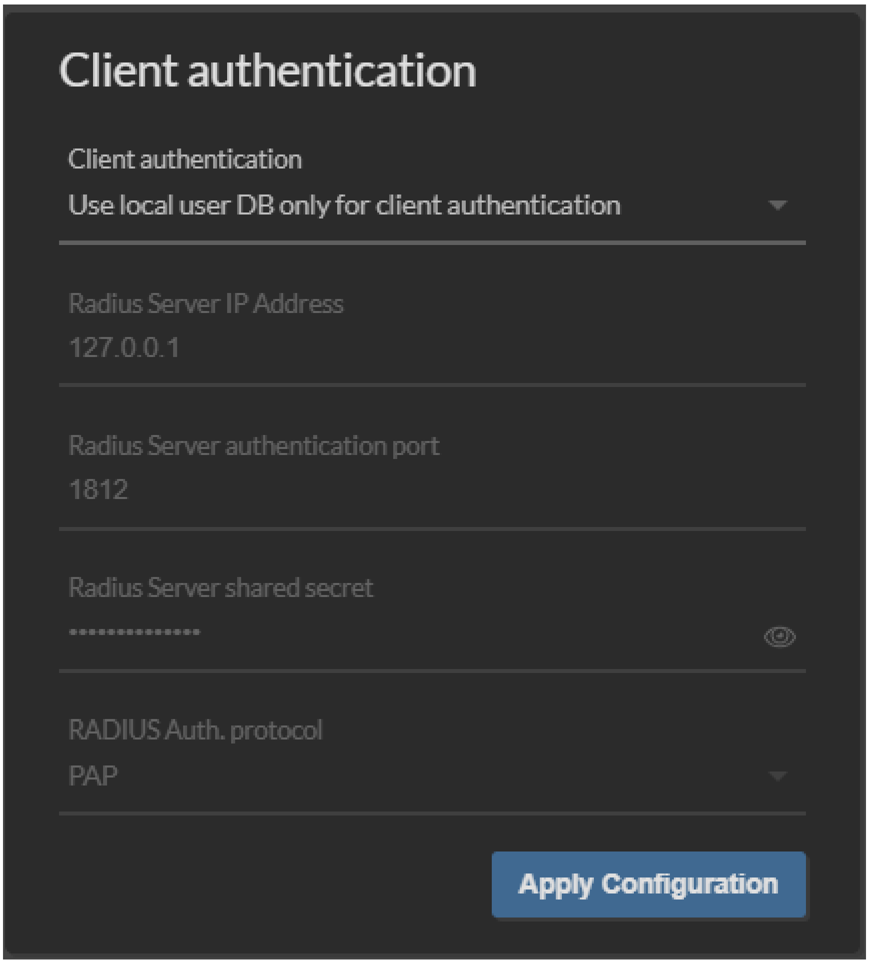
4.5.1.3. Client Authentication

The **Client Authentication** panel contains the following settings and options:

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

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

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



Client authentication

Client authentication: Use local user DB only for client authentication

Radius Server IP Address: 127.0.0.1

Radius Server authentication port: 1812

Radius Server shared secret: ••••••••••••••

RADIUS Auth. protocol: PAP

Figure 51. NMP Web+ - Server Configuration - Server Settings - Client Authentication

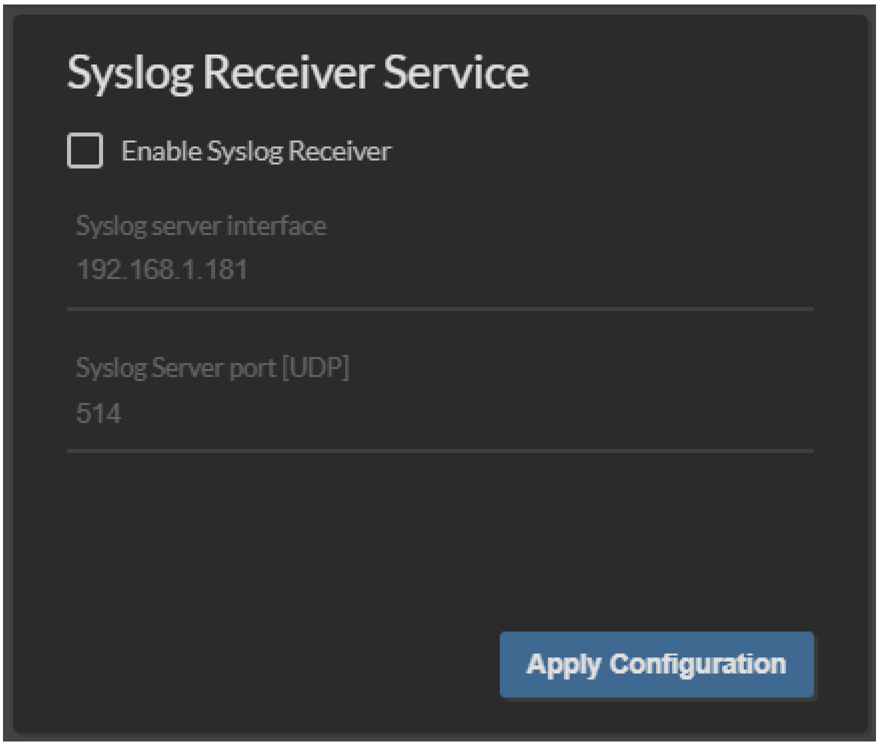
4.5.1.4. Syslog

The **Syslog** panel contains the following settings and options:

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

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

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



Syslog Receiver Service

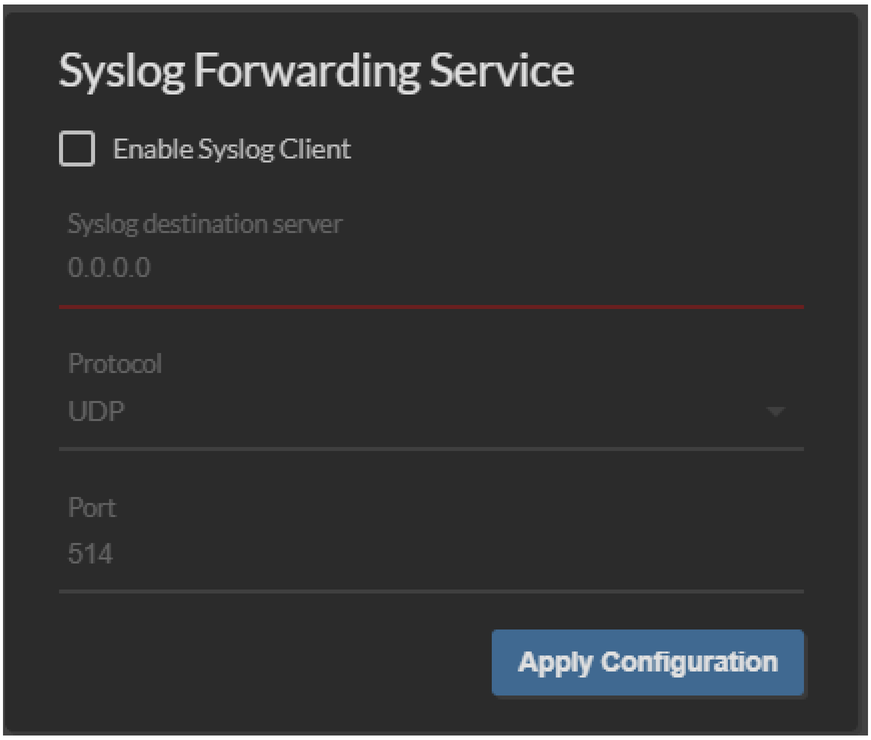
□ Enable Syslog Receiver

Syslog server interface
192.168.1.181

Syslog Server port [UDP]
514

Figure 52. NMP Web+ - Server Configuration - Server Settings - Syslog - Syslog Receiver Service

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



Syslog Forwarding Service

□ Enable Syslog Client

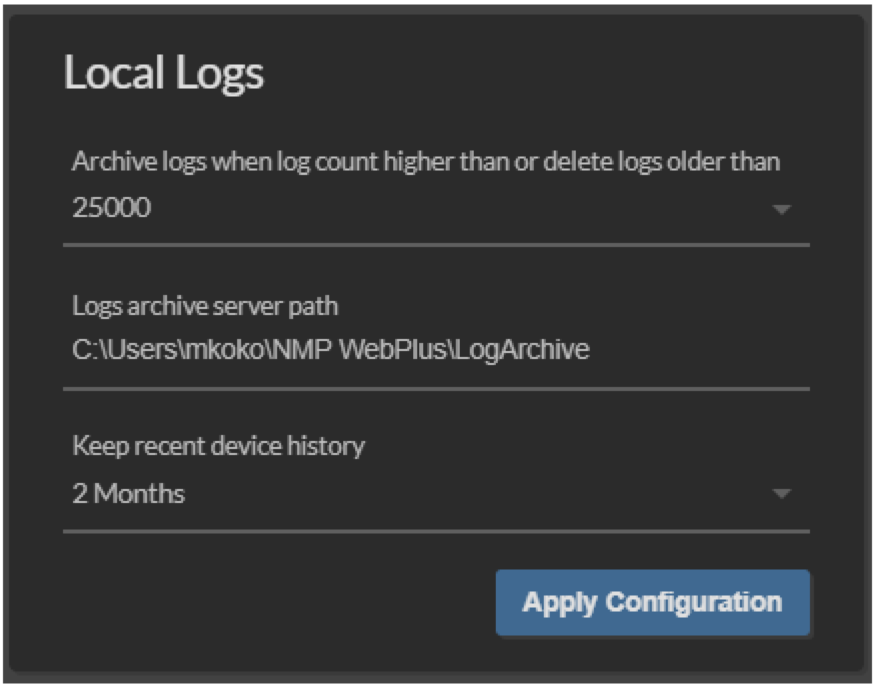
Syslog destination server
0.0.0.0

Protocol
UDP

Port
514

Figure 53. NMP Web+ - Server Configuration - Server Settings - Syslog - Syslog Forwarding Service

- **Local Logs**: Configure the log handling.
  - **Archive logs when log count higher than or delete logs older than**: The application's server will generate a .csv file with log messages when the number of log messages in the database will be higher than the defined log count limit (25,000, 50,000 or 100,000 messages) or older than the defined log age (1, 2, 6 or 12 months). The archived messages will be deleted from the database to prevent unlimited growth of the database size. The server starts the archiving procedure each day at 2 a.m. The last 500 and all unacknowledged messages are always kept in the database (i.e. they are not deleted during the archiving procedure).
  - **Logs archive server path**: Choose the location where application's server should save the log archives.
  - **Keep recent device history**: The application's server saves parameters like device temperature or device availability in the database which are used to create device history charts. To prevent unlimited growth of the database size, the server deletes history entries older than n` months. The maximum time for keeping the history is 12 months. The server clears the database each day at 2 a.m.



Local Logs

Archive logs when log count higher than or delete logs older than
25000

Logs archive server path
C:\Users\mkoko\NMP WebPlus\LogArchive

Keep recent device history
2 Months

Figure 54. NMP Web+ - Server Configuration - Server Settings - Syslog - Local Logs

4.5.1.5. Database Backup

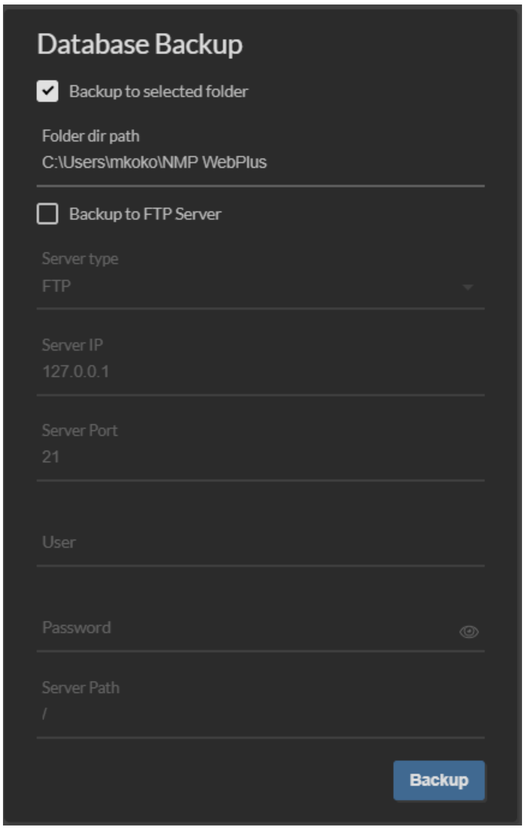
The **Database Backup** panel contains the following settings and options:

- **Database Backup**: Configure the backup folder for the database copy.
  - **Backup to selected folder**: Creates a database backup at the folder specified by “Folder dir path” parameter.
- **Backup to FTP Server**: Check this option to target the backup to an FTP server.
  - **Server type**: Select the server type of the FTP server.

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

  - **Server IP**: Enter the IP address of the server.
  - **Server Port**: Enter the server port of the server.
  - **User/Password**: Enter valid credentials of the registered FTP user
  - **Server Path**: Enter the server’s path to the backup folder (e.g. /Some_-Folder/Backup). NOTE: If the backup file should be saved in the FTP server’s root directory, an empty string or "/" is required.

By clicking the button Backup, the backup starts automatically.



Database Backup

☑ Backup to selected folder

Folder dir path
C:\Users\mkoko\NMP WebPlus

□ Backup to FTP Server

Server type
FTP

Server IP
127.0.0.1

Server Port
21

User

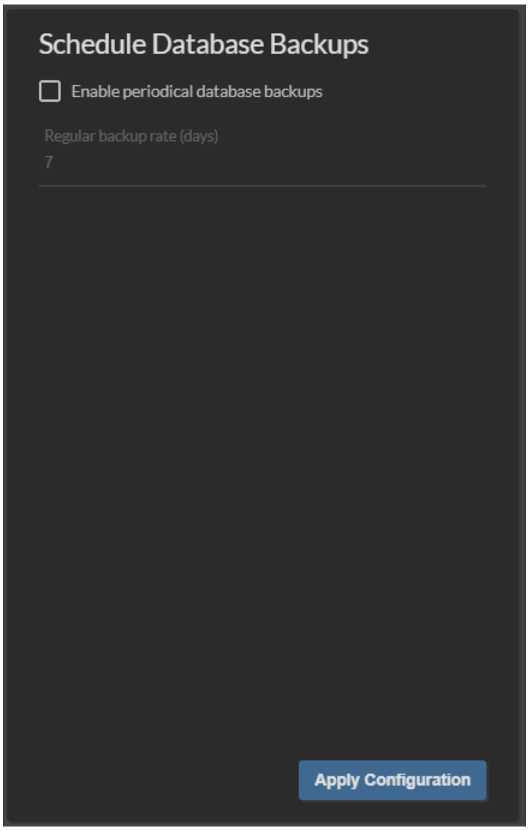
Password

Server Path
/

Figure 55. NMP Web+ - Server Configuration - Server Settings - Database Backup - Database Backup

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

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



Schedule Database Backups

□ Enable periodical database backups

Regular backup rate (days)
7

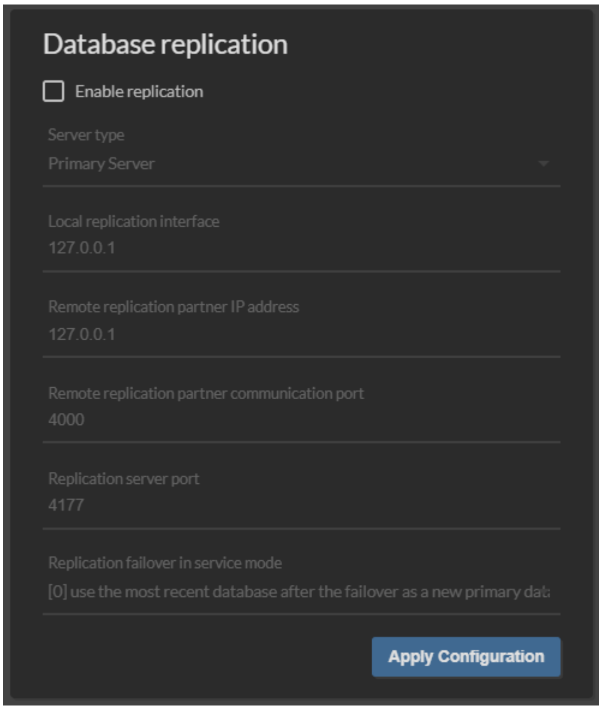
Figure 56. NMP Web+ - Server Configuration - Server Settings - Database Backup - Schedule Database Backups

4.5.1.6. Database Replication

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

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

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



Database replication

□ Enable replication

Server type: Primary Server

Local replication interface: 127.0.0.1

Remote replication partner IP address: 127.0.0.1

Remote replication partner communication port: 4000

Replication server port: 4177

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

Figure 57. NMP Web+ - Server Configuration - Server Settings - Database Replication

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

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

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

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

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

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

4.5.1.7. Email Notification

It is possible to get notified by the application via email about errors, SNMP traps and scheduled task events. The server instance is able to send email notifications on events. The configured SMTP server is used as email relay server. Email notifications are sent to all registered users. The system administrator and all users should configure their proper email addresses.

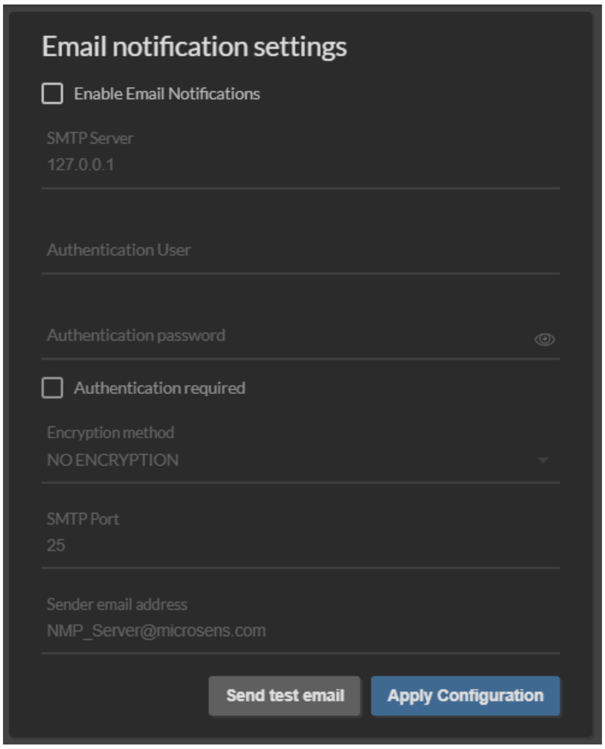
- **Enable Email Notifications**: If this option is enabled, errors and SNMP trap information is forwarded by email to recipients named below.

  ℹ | 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.

    ℹ | Only TLS 1.2 and newer is supported.

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



Email notification settings

□ Enable Email Notifications

SMTP Server
127.0.0.1

Authentication User

Authentication password

□ Authentication required

Encryption method
NO ENCRYPTION

SMTP Port
25

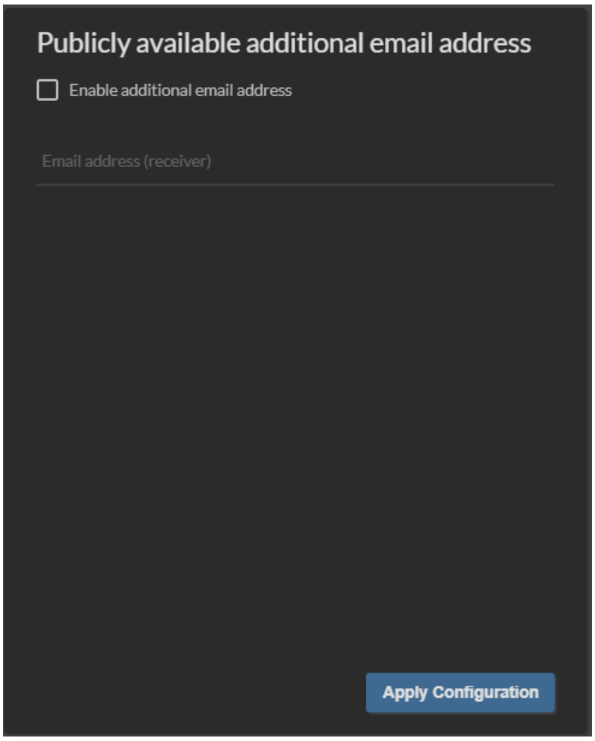
Sender email address
NMP_Server@microsens.com

Figure 58. NMP Web+ - Server Configuration - Server Settings - Email Notification - Email Notification Settings

4.5.1.7.1. 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.

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



Publicly available additional email address

□ Enable additional email address

Email address (receiver)

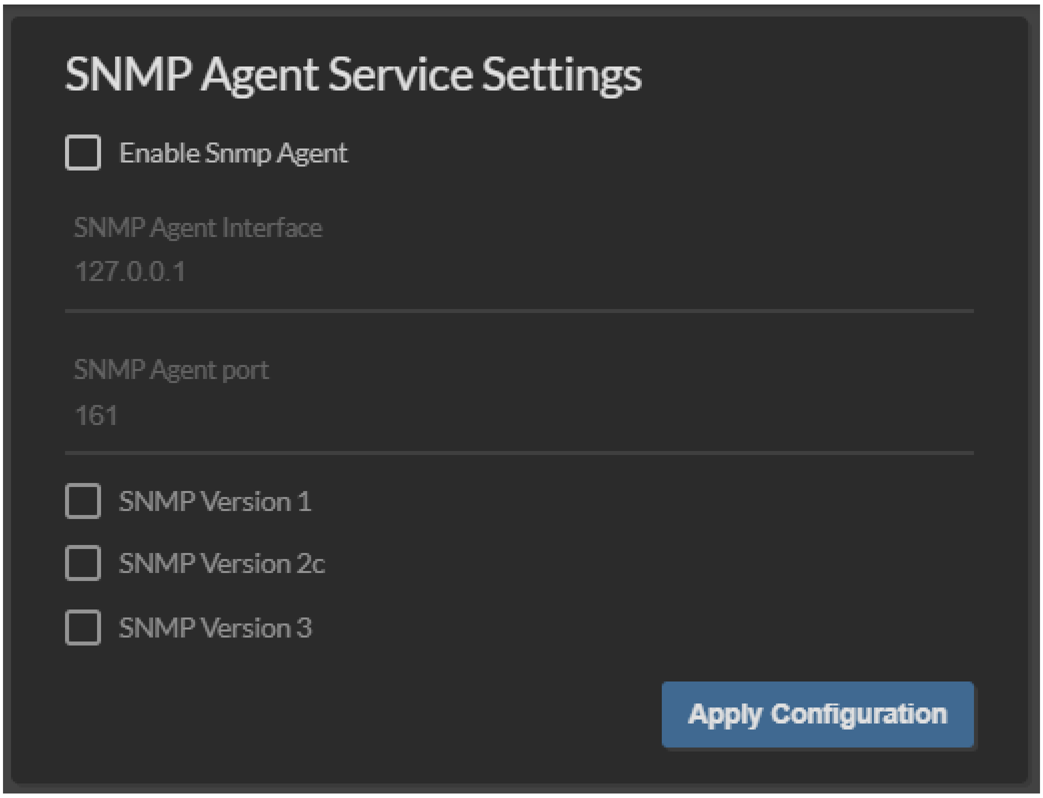
Figure 59. NMP Web+ - Server Configuration - Server Settings - Email Notification - Additional Email Address

4.5.1.8. SNMP Agent Communication

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

The **SNMP Agent Communication** panel contains the following settings and options:

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



SNMP Agent Service Settings

□ Enable Snmp Agent

SNMP Agent Interface
127.0.0.1

SNMP Agent port
161

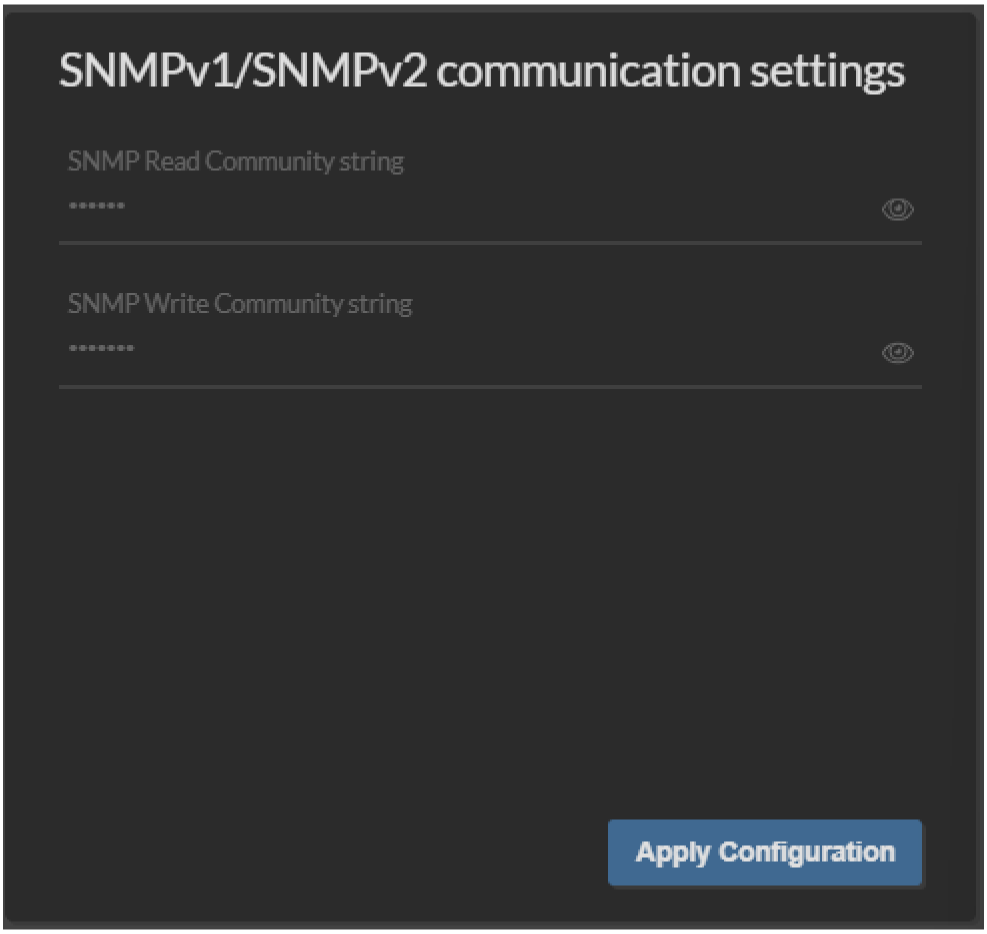
□ SNMP Version 1

□ SNMP Version 2c

□ SNMP Version 3

Figure 60. NMP Web+ - Server Configuration - Server Settings - SNMP Agent Communication - SNMP Agent Service Settings

- **SNMPv1/SNMPv2 Communication Settings**: Configure SNMP v1 and SNMP v2 settings.
  - **SNMP Read Community string**: The read-only community string allows other SNMP managers to read data values.
  - **SNMP Write Community string**: The read-write community string allows other SNMP managers to read and write data values.



SNMPv1/SNMPv2 communication settings

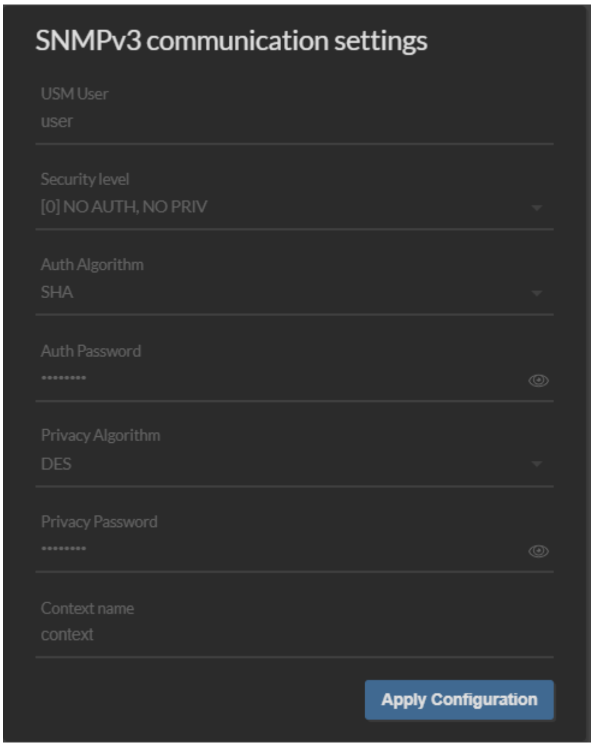
SNMP Read Community string
••••••

SNMP Write Community string
•••••••

Figure 61. NMP Web+ - Server Configuration - Server Settings - SNMP Agent Communication - SNMPv1/SNMPv2 Communication Settings

- **SNMPv3 Communication Settings**: Configure SNMPv3 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.



SNMPv3 communication settings

USM User: user

Security level: [0] NO AUTH, NO PRIV

Auth Algorithm: SHA

Auth Password: ••••••••

Privacy Algorithm: DES

Privacy Password: ••••••••

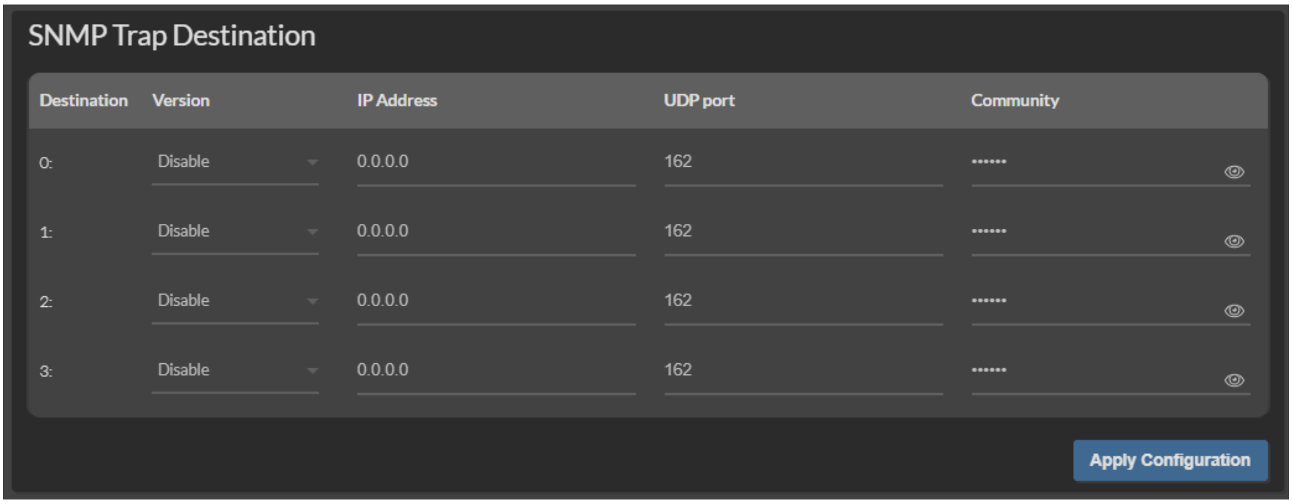
Context name: context

Figure 62. NMP Web+ - Server Configuration - Server Settings - SNMP Agent Communication - SNMPv3 Communication Settings

4.5.1.9. SNMP Trap Relay

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

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



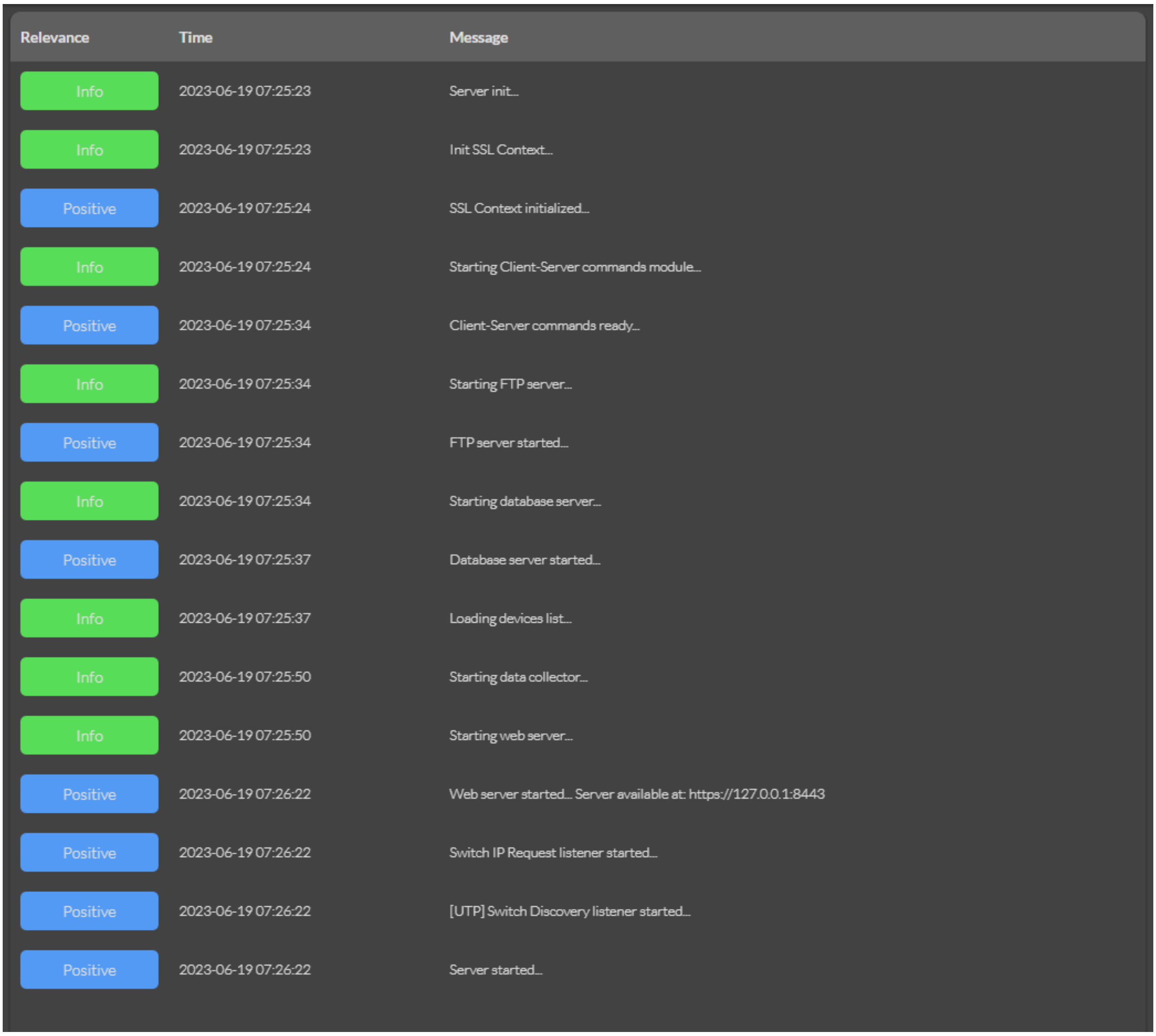
SNMP Trap Destination

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

Figure 63. NMP Web+ - Server Configuration - Server Settings - SNMP Trap Relay - SNMP Trap Destination

4.5.1.10. Server Startup-Logs

Server startup logs contains all the messages which normally are displayed at the server manager window when started in GUI mode. However, when the server is started in Windows service or Linux daemon mode, the manager window is not available so there is no easy possibility to check the startup logs, except investigating the log files. Thanks to this panel, user can easily diagnose server startup process.



Relevance	Time	Message
Info	2023-06-19 07:25:23	Server init...
Info	2023-06-19 07:25:23	Init SSL Context...
Positive	2023-06-19 07:25:24	SSL Context initialized...
Info	2023-06-19 07:25:24	Starting Client-Server commands module...
Positive	2023-06-19 07:25:34	Client-Server commands ready...
Info	2023-06-19 07:25:34	Starting FTP server...
Positive	2023-06-19 07:25:34	FTP server started...
Info	2023-06-19 07:25:34	Starting database server...
Positive	2023-06-19 07:25:37	Database server started...
Info	2023-06-19 07:25:37	Loading devices list...
Info	2023-06-19 07:25:50	Starting data collector...
Info	2023-06-19 07:25:50	Starting web server...
Positive	2023-06-19 07:26:22	Web server started... Server available at: https://127.0.0.1:8443
Positive	2023-06-19 07:26:22	Switch IP Request listener started...
Positive	2023-06-19 07:26:22	[UTP] Switch Discovery listener started...
Positive	2023-06-19 07:26:22	Server started...

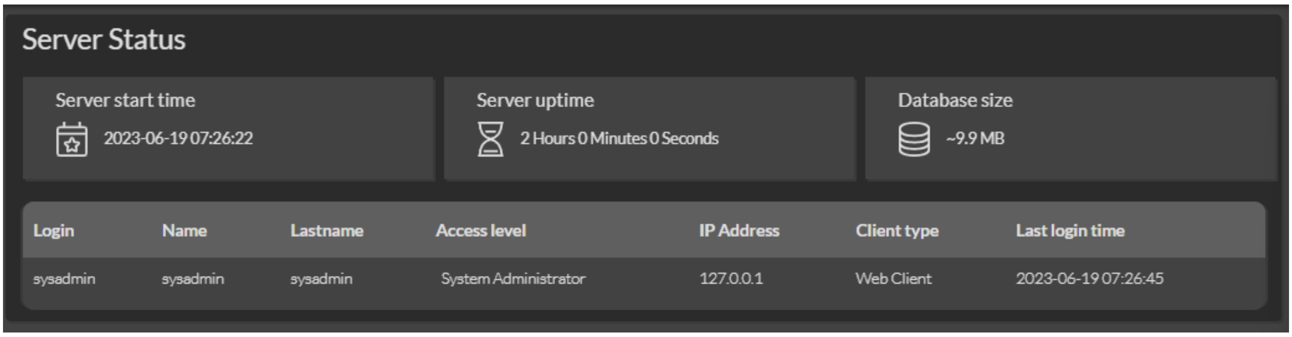
Figure 64. NMP Web+ - Server Configuration - Server Settings - Server Startup-Logs

4.5.1.11. Server Status

Server status panel contains basic informations about server status:

- **Server start time**: When the server was booted up.
- **Server uptime**: How long the server is running for.
- **Database size**: The current database size.

Additionally, the list of currently logged in users is available.



Server Status

Server start time: 2023-06-19 07:26:22

Server uptime: 2 Hours 0 Minutes 0 Seconds

Database size: ~9.9 MB

Login	Name	Lastname	Access level	IP Address	Client type	Last login time
sysadmin	sysadmin	sysadmin	System Administrator	127.0.0.1	Web Client	2023-06-19 07:26:45

Figure 65. NMP Web+ - Server Configuration - Server Settings - Server Status

4.5.1.12. Server Diagnostic

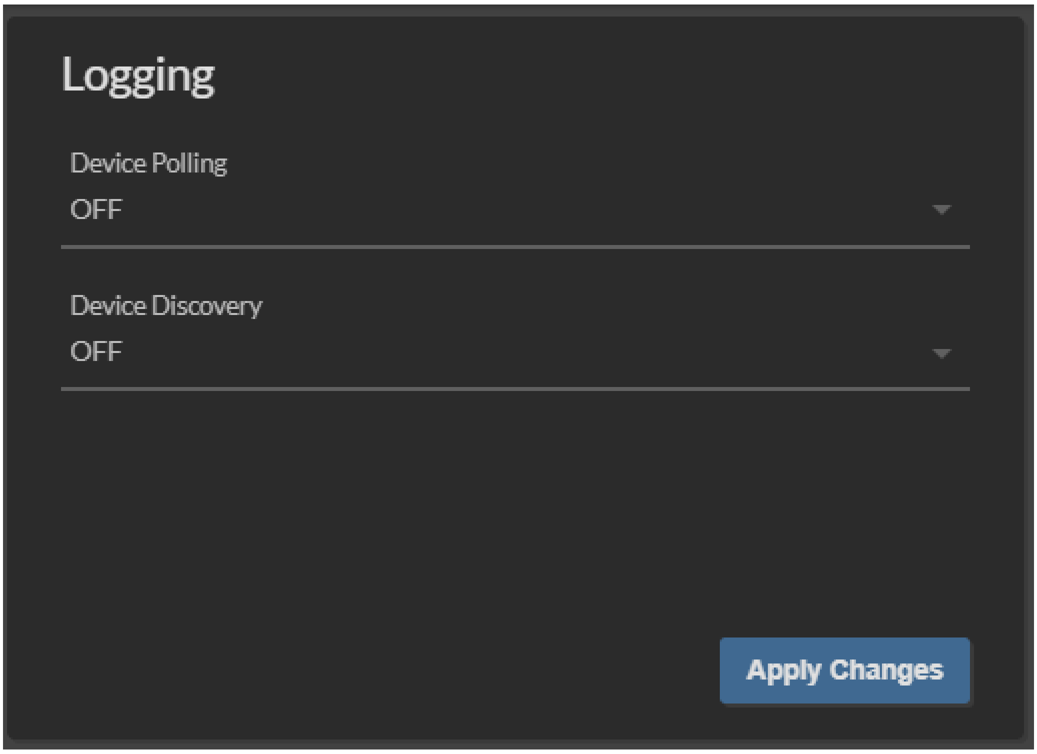
The server diagnostic panel enables additional loggers to use the device data polling and device discovery feature. It can be useful to detect the root cause of some problems, such as when something related to device communication does not work properly. For each logger, the user can define what kind of messages should be logged. The logging levels in descending order are:

- SEVERE (highest value)
- WARNING
- INFO
- CONFIG
- FINE
- FINER
- FINEST (lowest value)

In addition there is a level OFF that can be used to turn off logging, and a level ALL that can be used to enable logging of all messages.

Generated log files can be found at the NMP Server data folder which by defualt is `$USER_HOME/NMP Web+/LOG`.

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



Logging

Device Polling
OFF

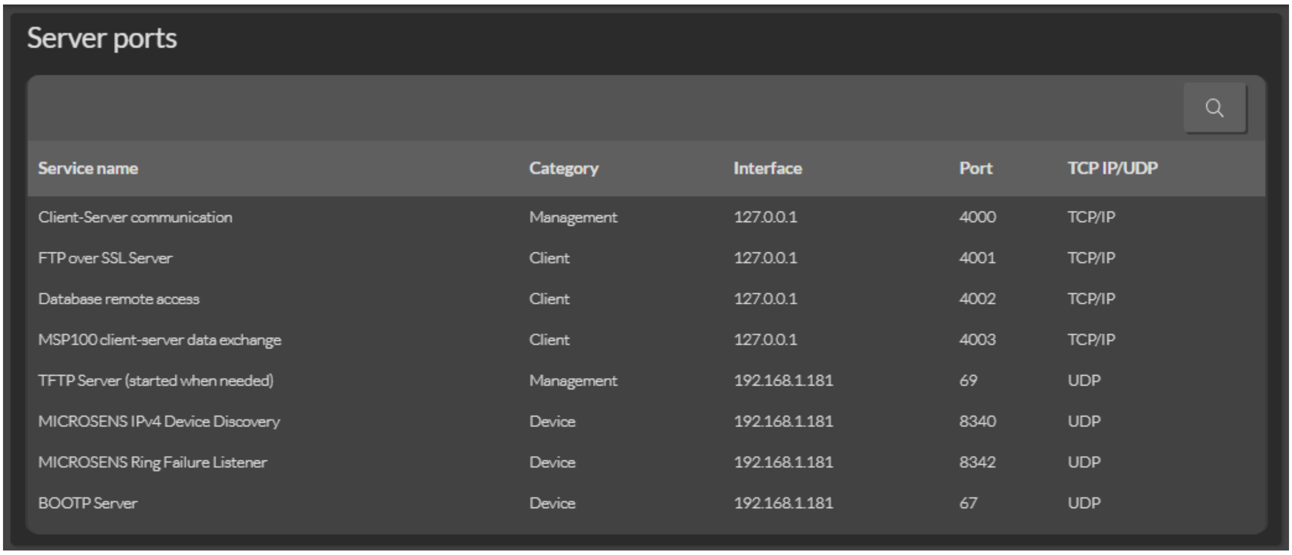
Device Discovery
OFF

Figure 66. NMP Web+ - Server Configuration - Server Settings - Server Diagnostic - Logging

4.5.1.13. Server Ports

It contains a list of ports used by the server. This information can be used to configure system firewall properly to establish communication between:

- server and devices
- server and client
- master and slave server in replication mode



Server ports

Service name	Category	Interface	Port	TCP IP/UDP
Client-Server communication	Management	127.0.0.1	4000	TCP/IP
FTP over SSL Server	Client	127.0.0.1	4001	TCP/IP
Database remote access	Client	127.0.0.1	4002	TCP/IP
MSP100 client-server data exchange	Client	127.0.0.1	4003	TCP/IP
TFTP Server (started when needed)	Management	192.168.1.181	69	UDP
MICROSENS IPv4 Device Discovery	Device	192.168.1.181	8340	UDP
MICROSENS Ring Failure Listener	Device	192.168.1.181	8342	UDP
BOOTP Server	Device	192.168.1.181	67	UDP

Figure 67. NMP Web+ - Server Configuration - Server Settings - Server Ports

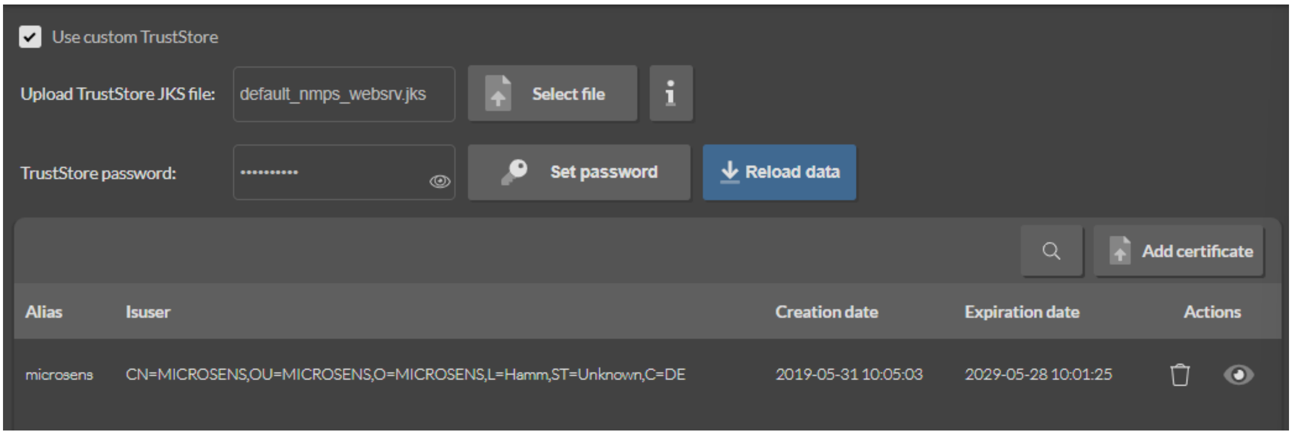
4.5.2. Certificates

Configuration of certificates for security and authorization, e.g. used in SSL encryption.

4.5.2.1. Trust Store

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

- **Use custom TrustStore**: Check this option to enable the use of the custom TrustStore.
- **Upload TrustStore JKS file**: Select the necessary certificate file for SSL/TLS communication.
- **TrustStore password**: Enter the corresponding password for the selected file.
- **Reloald data**: refresh the list of certificates after uplaoding
- **Add certificate**: Click on this button to store a new certificate.
- **View selected (table action)**: Click on this button to view the certificates content.
- **Delete selected (table action)**: Click on this button to delete this certificate.



☑ Use custom TrustStore

Upload TrustStore JKS file: default_nmps_websrv.jks

TrustStore password: ••••••••••

Alias	Isuser	Creation date	Expiration date	Actions
microsens	CN=MICROSENS,OU=MICROSENS,O=MICROSENS,L=Hamm,ST=Unknown,C=DE	2019-05-31 10:05:03	2029-05-28 10:01:25	

Figure 68. NMP Web+ - Server Configuration - Certificates - Trust Store

Chapter 5. Application Instructions

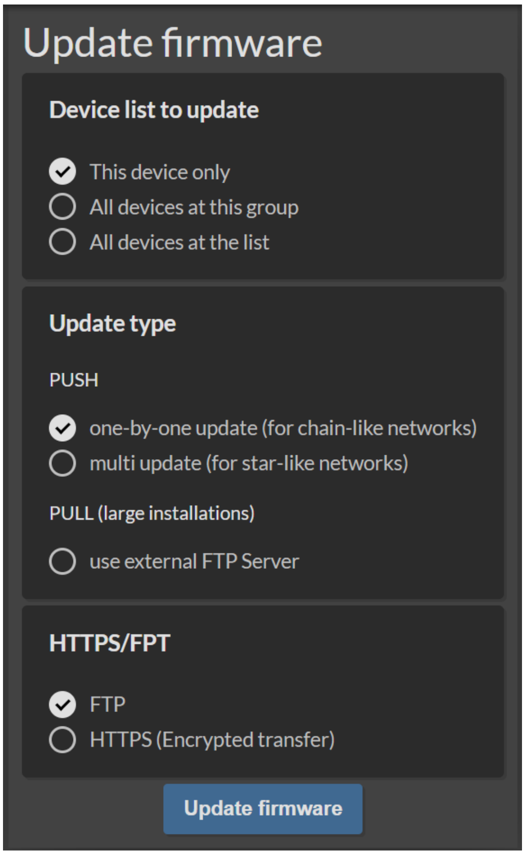
The following sections describe how to use the application in every day tasks.

5.1. 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 and newer) / Industrial Switches (G6 and newer).

> The firmware update of a device is possible if management information for the device is available. Devices with a device-polling timeout cannot be updated.

To update the firmware of one or more devices use the device context menu of the respective device or group in the device list. After clicking Update Firmware the following dialogue opens:



Update firmware

Device list to update

✓ This device only
○ All devices at this group
○ All devices at the list

Update type

PUSH

✓ one-by-one update (for chain-like networks)
○ multi update (for star-like networks)

PULL (large installations)

○ use external FTP Server

HTTPS/FPT

✓ FTP
○ HTTPS (Encrypted transfer)

Figure 69. NMP - Device Context Menu - Update Firmware

The dialogue offers several update options:

- **Update device, group or list:** It is possible to update the firmware of just one device or all devices within a group or all devices within a whole list. When the context menu of a device is opened and the group or list option in this dialogueis chosen, 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.

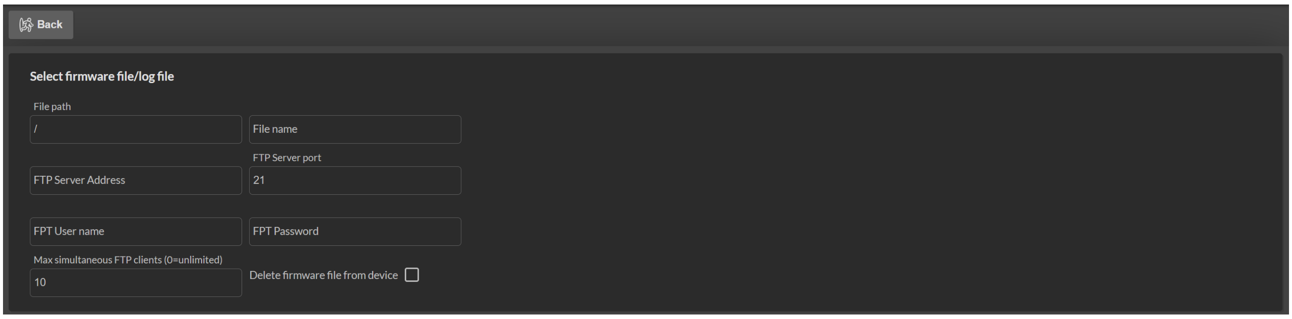
  For a star-like network topology use a "multi update". This means that up to 10 switches can be updated at the same time. In a star-like topology there is no danger of the switch’s firmware failing due to another updated switch - through which the firmware file is uploaded to the following devices - 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.

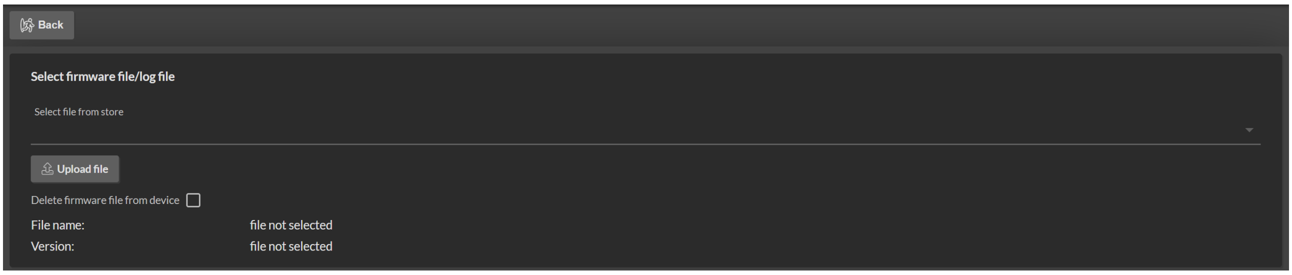
In the next step provide the FTP Server details where the firmware file is located (in case of "PULL" method) or choose the appropriate firmware file (in case of "PUSH" method).


Back

Select firmware file/log file

File path: /
File name
FTP Server Address
FTP Server port: 21
FPT User name
FPT Password
Max simultaneous FTP clients (0=unlimited): 10
Delete firmware file from device □

Figure 70. NMP - Device Context Menu - Update Firmware - Select FTP Server


Back

Select firmware file/log file

Select file from store

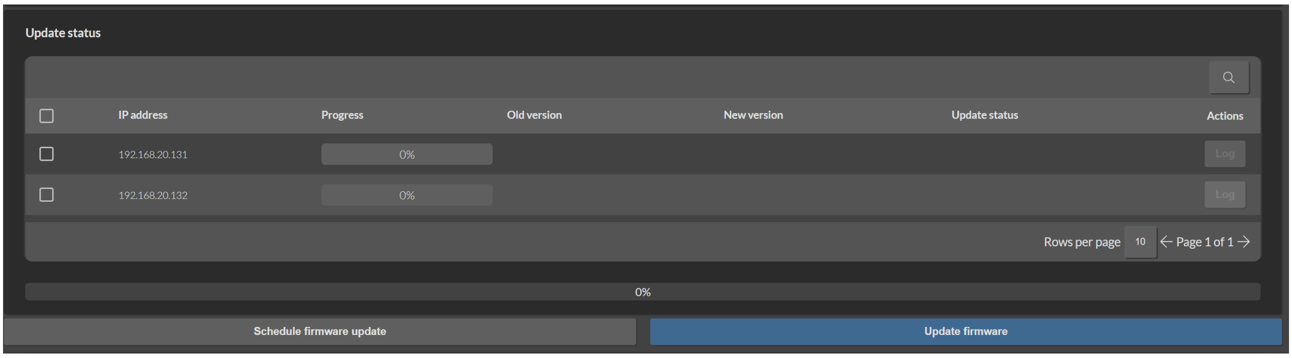
Upload file

Delete firmware file from device □

File name: file not selected
Version: file not selected

Figure 71. NMP - Device Context Menu - Update Firmware - Select File

All other settings are identical with both methods:



Update status

□	IP address	Progress	Old version	New version	Update status	Actions
□	192.168.20.131	0%				Log
□	192.168.20.132	0%				Log

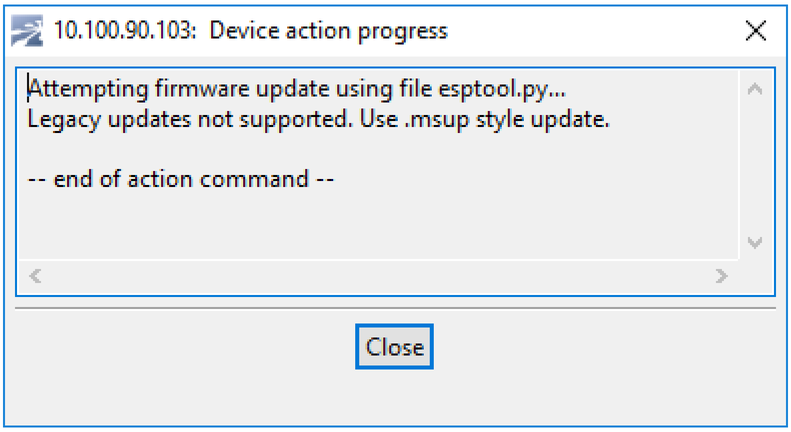
Rows per page 10 ← Page 1 of 1 →

0%

Figure 72. NMP - Device Context Menu - Update Firmware - Options

The "Create log file" option requires choosing 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.



10.100.90.103: Device action progress

```
Attempting firmware update using file esptool.py...
Legacy updates not supported. Use .msup style update.

-- end of action command --
```

Figure 73. NMP - Device Context Menu - Update Firmware - Progress

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

Define a task which will be executed just once (at a defined time) or periodically according to the configured execution rate.

All scheduled tasks can be deleted or modified using the menu:[Schedules] menu (see Section 4.4.6.1).

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 72). 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.

> 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.

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

Disclaimer

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

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

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

Document ID: PM-EN-19002_User-Manual-NMPv3_v3.2.3