



Nexans Device Manager (NEXMAN)

Version 6.04 *or later*

Manual

KD598E21

FEATURES

- For all Nexans devices with V3.xx, V4.xx, V5.xx or V6.xx firmware
- Fast Layer-2 Autodiscovery and simple basic configuration for devices within the local segment
- Automatic Layer-2 basic configuration for devices within the local segment
- Layer-3 Autodiscovery thru three user configurable IP ranges for devices behind IP routers
- The devices are permanently polled and marked in the device list in corresponding colours
- The device list is automatically updated through polling and changes are highlighted in colour
- Devices with alarm messages are automatically shifted to the top of the list
- Devices are automatically polled and indicated in device-List in green (ok) or red (failure)
- Firmware update for one or more devices
- Scheduled firmware update in the night or at the weekend
- Reading and writing of device configurations via TFTP and SCP
- Username/password protected reading and writing of device configurations
- Automatic download of device configurations for one or more devices
- Storage of device configurations in a database on the PC or on a central server
- Storage of old device configurations via history function in the database
- Three state tabs with online indication of all state information of the device
- Reset of Error and Statistics counters for one or more devices
- Individual selection of storage locations for device lists, database, master configurations and firmware
- Creation of any number of device lists, e.g. to arrange devices into groups etc.
- Creation of any number of master configurations for distribution to one or more devices
- Each master configuration may specify different parameters for distribution
- Comprehensive information on update and progress in a log window
- Information from the log windows available for later analysis
- Sorting of device list by IP address, MAC addresses, device name and software version
- Import of device lists as CSV (comma/semicolon separated) files, e.g. from NSCM or Excel
- Import of device lists from the Nexans Basic Configurator

- Direct calling of Telnet or WEB from the configuration editor
- Easy restoration of the delivery condition
- Full IPv6 support
- Basic Configurator Features:
 - Configuration of the following basic switch parameters:
 - DHCP, IP address, network mask and gateway
 - Switch name, location und contact
 - Management VLAN-ID
 - Trunk port (Uplink)
 - User templates for quick configuration of multiple switches with similar settings
 - User templates can be saved to hard disk and recalled
 - No DHCP server and no manipulation of configuration switches required
 - Changes take immediately effect without rebooting
 - For security reasons any access via the Basic Configurator is only allowed if the switch is set to its factory default admin name/password (admin/nexans)
 - Running in (MAC Address Mode):
 - Centralized configuration, e. g. during 'Autodiscover (Layer-2)' with Nexans Device Manager
 - Configuration is done via the switch MAC address determined during Autodiscover
 - The PC and the switch to be configured must be located in the same segment or VLAN
 - Running in (Local Mode):
 - Easy on-site configuration by the installer
 - PC needs to be connected to port TP1
 - Configuration can optionally be added to a device list and imported by the NEXMAN
- Client/Controller Features:
 - Observe all devices by a server application and store relevant informaton into a SQL database
 - User Management with client capability that offers different roles and access rights
 - Zero Touch Configuration for automatic discovery, firmware updates, configuration and adding to the database
 - Log Message Server for SYSLOG, SNMP Trap and Controller Messages
 - E-Mail Notifications for all types of Log Messages
 - Time scheduled import of devices from a third-party csv-file
 - Time scheduled configuration of devices
 - Import/Export Device-Lists from or to NEXMAN Stand-Alone

CONTENTS

1. PC Software and Hardware Requirements	7
2. Installation, Update and Start of the Manager	8
2.1. Installation of NEXMAN Stand-Alone	8
2.2. Installation of NEXMAN Client / Controller	14
2.2.1. Installing NEXMAN Controller	15
2.2.2. Installing NEXMAN Client	18
2.2.3. Using an existing database	23
2.2.4. User rights for SQL Express or SQL Server	23
3. Switch Firmware Requirements	24
4. Firewall	24
5. Software Registration	24
6. Restrictions of the EVALUATION Version	25
7. Help and Documentation	25
8. Firmware Upgrade from Version V1/V2 to V3/V4/V5/V6	25
9. Integration into a Central Management System	26
10. Name and Password as Starting Parameters	28
11. Functional Description of Configuration Parameters	28
12. Quick Start	29
12.1. Starting NEXMAN Stand Alone	29
12.2. Starting NEXMAN Client.....	30
12.3. Adding Devices to Device-List.....	31
12.3.1. Adding Devices via Layer-2 Autodiscovery	31
12.3.2. Automatic Basic Configuration	38
12.3.3. Adding Devices via Layer-3 Autodiscovery	39
12.3.4. Adding Devices Manually to the Device List	40
12.4. Database Management in Client/Controller-Version	42
12.5. User Management in Client/Controller-Version	44
12.5.1. Create a new user	44
12.5.2. User roles	45
12.5.3. User Access Rights.....	46
12.6. Import Device-List from Stand-Alone version into Controller database.....	46
12.7. Export Device-List from Controller database to Stand-Alone version	47
12.8. Searching for MAC Addresses	47
12.9. Firmware Update for Devices with Firmware V1.xx / V2.xx	49
12.10. Starting the Device Editor and Configuring the Device	49
12.11. Configuration of multiple devices	52

12.11.1. Reading configuration of multiple devices.....	52
12.11.2. Enable Scheduled Configuration Download.....	54
12.11.3. Update firmware of multiple devices	55
12.11.4. Copy Configuration Templates to checked Devices	58
13. Basic Configurator	60
13.1. Functional overview.....	60
13.2. Basic Configurator in (MAC Address Mode)	61
13.2.1. Basic configuration via Autodiscovery (MAC Address Mode)	61
13.2.2. Basic configuration via Device-List (MAC Address Mode).....	61
13.3. Basic Configurator in (Local Mode)	62
13.3.1. Functioning Principle (Local Mode).....	62
13.3.2. Starting the Basic Configurator (Local Mode)	62
13.3.3. Reading the Switch Configuration (Local Mode).....	63
13.3.4. Writing the Switch Configuration (Local Mode).....	66
13.4. General Features.....	67
13.4.1. Configuring the Trunk Port and the Mgmt VLAN ID.....	67
13.4.2. Saving the Basic Configurator Settings.....	67
14. Device-Lists.....	68
14.1. Device-Category.....	68
14.1.1. Create Category.....	69
14.1.2. Allocating Category	71
14.1.3. Category Alarm	72
14.1.4. Reordering Categories via Drag&Drop	72
14.2. Automatic polling of Device-Lists	73
14.3. Saving the Device List under a New Name	74
14.4. Importing Device Lists	76
15. Master Configuration.....	77
15.1. Creating a Master Configuration.....	77
15.2. Distributing a Master Configuration	82
15.3. Distributing of Name and Location via Master Configuration	85
15.4. Distributing of IP Address via Master Configuration	87
15.5. Rebooting switches via Master Configuration	88
16. Data Backup	89
17. Multi-User capability.....	91
17.1. Terminal Server Support	91
17.2. Device-List.....	91
17.3. Device-Editor	91
18. Preferences	92
18.1. Global	93
18.1.1. Save Window Sizes	93

18.1.2. Save Device-Editor docking state	94
18.1.3. Number of retries for simultaneous reading/writing actions	94
18.1.4. Timeout for reading or writing Config (seconds)	94
18.1.5. Timeout for writing Firmware (minutes)	94
18.1.6. Timeout for status polling (seconds)	94
18.1.7. Don't save Config to Database	94
18.1.8. Maximum Number of Database History Entries	94
18.1.9. Menu language	96
18.1.10. NEXMAN Theme	96
18.1.11. Scheduled Configuration Download Time	96
18.2. Device-List	96
18.2.1. Poll interval (seconds)	96
18.2.2. Poll Controller interval (seconds)	97
18.2.3. Simultaneously polls:	97
18.2.4. Autosave Device-List (minutes)	97
18.2.5. Save columns 'Uptime' and 'Last seen' to Device-List	97
18.2.6. Adjust column size on category change	97
18.2.7. Enable custom filters:	97
18.2.8. Available Columns / Displayed Columns	98
18.2.9. Use fast scrolling	98
18.3. Device-Editor	98
18.3.1. Refresh interval for State tabs (seconds)	98
18.3.2. Refresh interval for Show buttons (seconds)	98
18.4. Access	99
18.4.1. Manager Access Mode	100
18.4.2. Protocol version	101
18.4.3. WEB Browser TCP Port	101
18.4.4. WEB Browser HTTPS TCP Port	101
18.4.5. Telnet Client	101
18.4.6. SSH Client	101
18.5. Folders	102
18.5.1. Database	102
18.5.2. Device-Lists	102
18.5.3. Master-Configs	102
18.5.4. Basic-Configs	103
18.5.5. Firmware Images	103
18.5.6. Application Data Folder	103
19. NEXMAN Controller	104
19.1. Zero Touch Configuration	104
19.2. Predefined Devices	107
19.3. Configuration Files stored on the Server	108
19.4. Log-Messages Server	108

19.5. E-Mail Notifications.....109

 19.5.1. Zero Touch Configuration Notifications.....110

 19.5.2. SYSLOG Notifications.....110

 19.5.3. SNMP Trap Notifications.....110

 19.5.4. Controller Notifications.....110

19.6. Importing Devices from file.....111

19.7. Time Scheduled Configuration.....111

19.8. Controller Settings.....112

 19.8.1. General Settings.....113

 19.8.2. Poll Settings.....115

 19.8.3. UDP Settings.....116

 19.8.4. Zero Touch Configuration Settings.....117

 19.8.5. E-Mail Notification Settings.....118

 19.8.6. Log-Messages Server Settings.....120

20. Release notes.....121

1. PC Software and Hardware Requirements

NEXMAN Stand-Alone and Client/Controller require one of the following Microsoft operations systems:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8
- Windows 10

NEXMAN Controller requires one of the following SQL Databases:

- SQL Server 2008
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

The Hardware requirements are dependent on the operation system.

2. Installation, Update and Start of the Manager

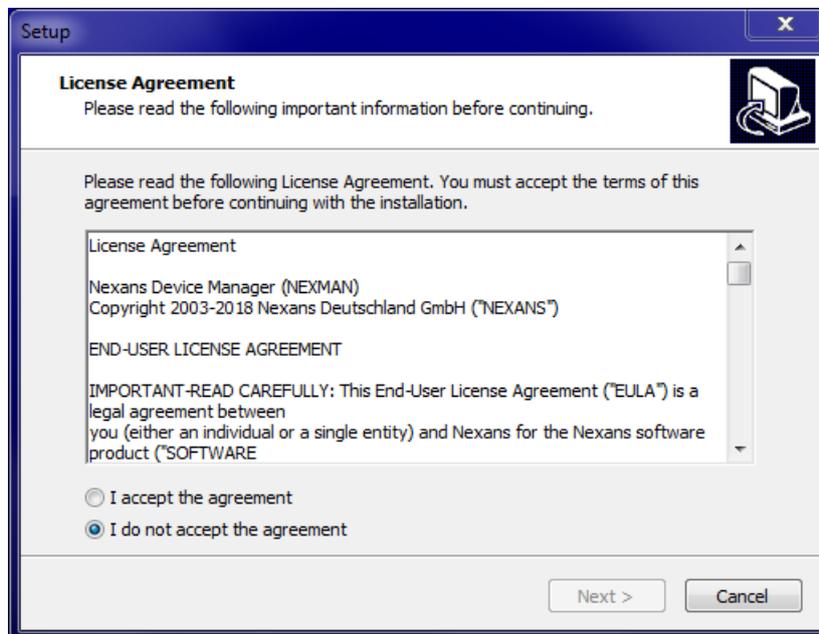
For installing the Manager, the file **NEXMAN_VX.xx_Setup.exe**, that can be downloaded from the **support portal**: www.nexans-ans.de/support needs to be executed.

If a previous Manager version is installed, this installation will only update the existing Manager. All settings and directories will be preserved.

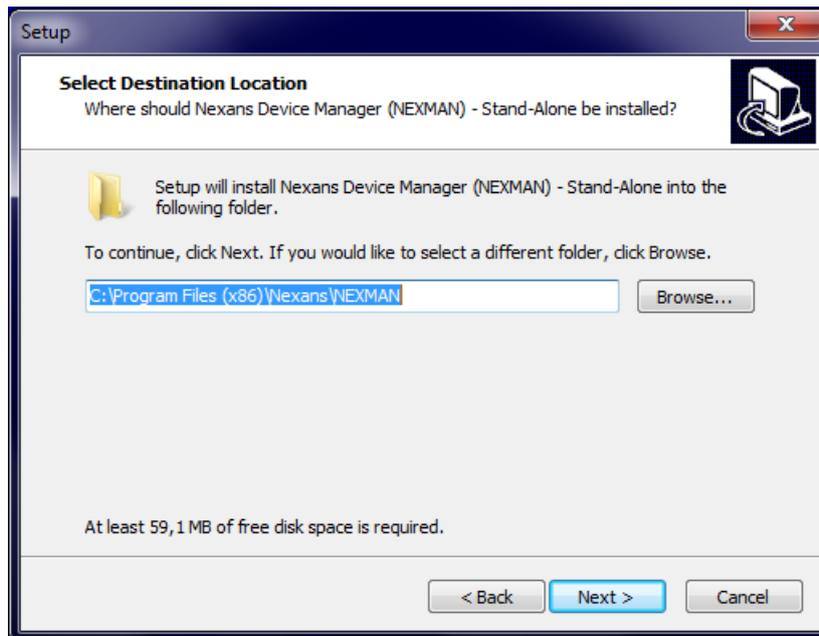
If desired, during installation a new directory can be defined in order to preserve the previous Manager version. However, a downgrade to an older version is also possible without any problem.

Depending on the PC's configuration and possible company-specific limitation of rights it might be necessary to execute the installation file with administrator rights. In this case, it might also be necessary to launch the installed Manager with administrator rights.

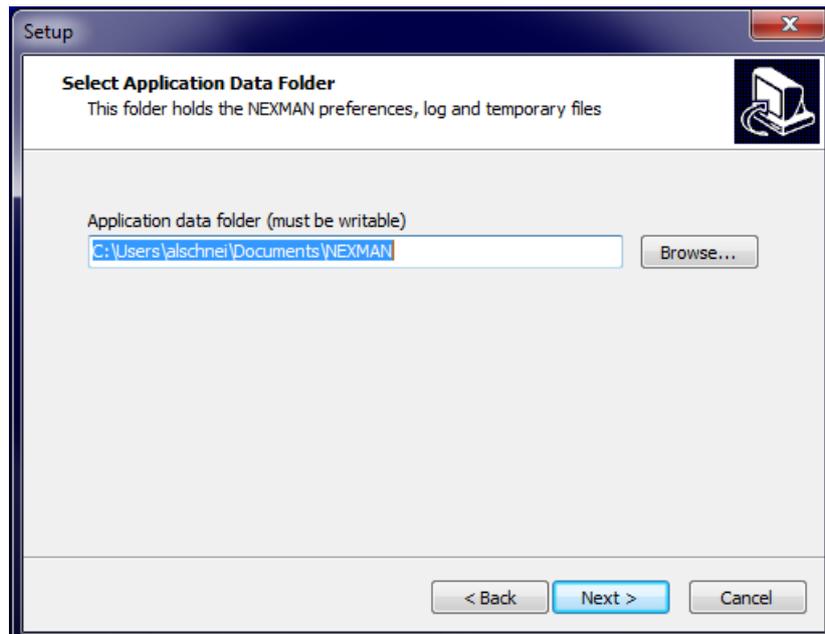
2.1. Installation of NEXMAN Stand-Alone



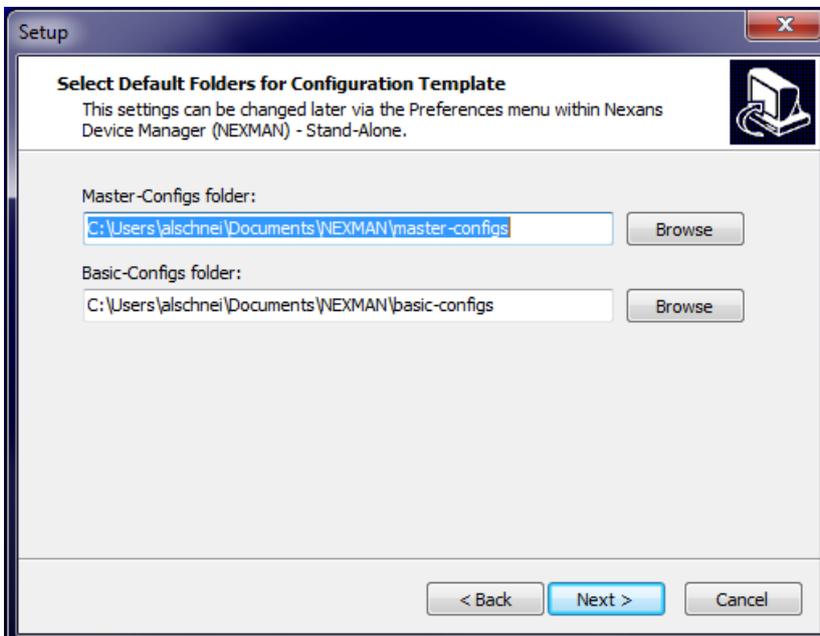
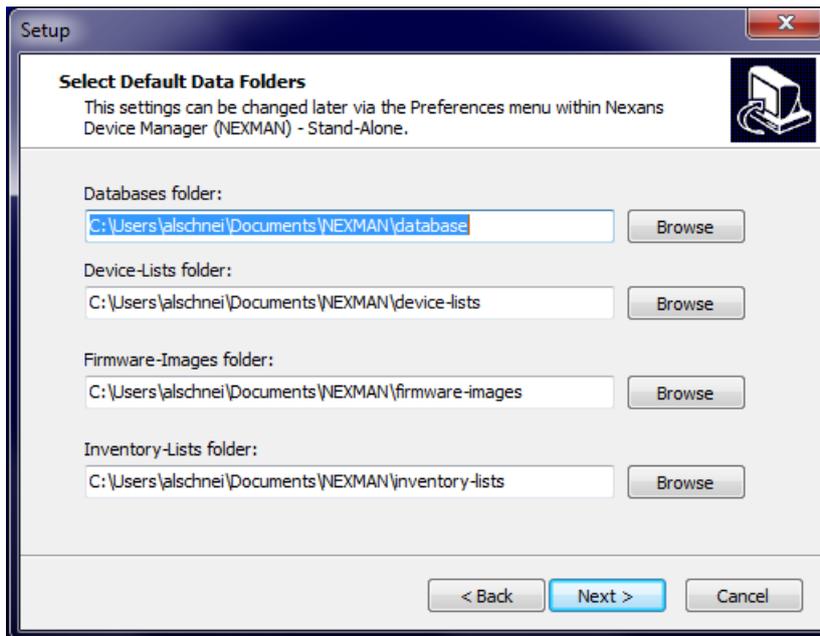
For the installation of the NEXMAN Stand-Alone version, execute the file **NEXMAN_VX.xx_Setup.exe**. First read the license agreement and then accept the agreement. Continue with clicking **Next**.



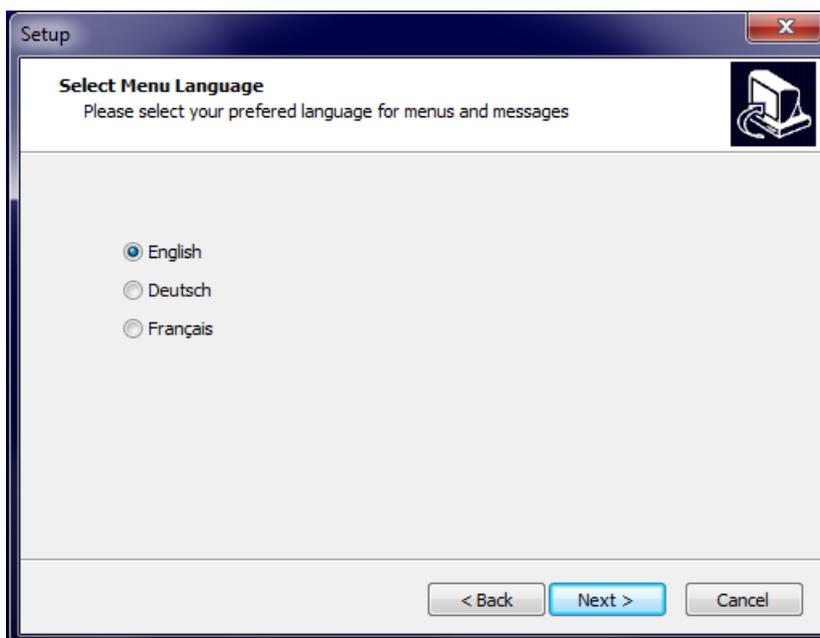
Choose the installation folder. Use **Browse...** to select a folder or just click **Next** to keep the default directory.



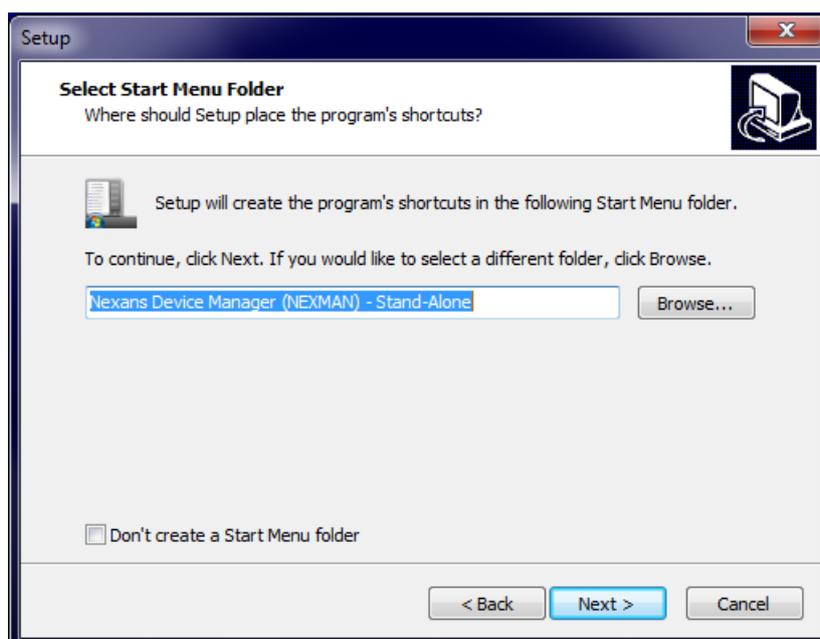
Specify the application data folder for NEXMAN. The application folder will contain the configuration files like NEXMAN.config where all preferences of the NEXMAN are stored. The folder must be writable.



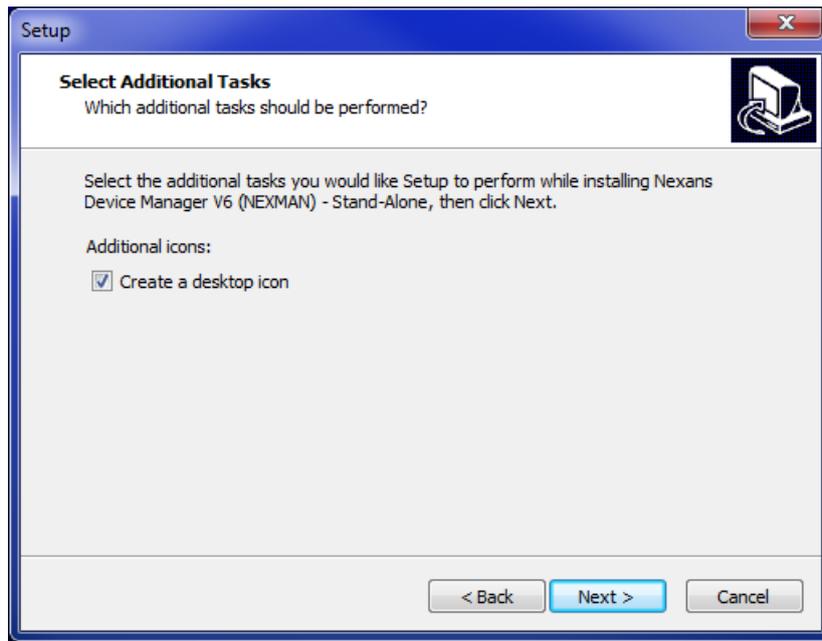
Specify the data folders for NEXMAN. Read more about the folders in chapter *18.5 Folders*.



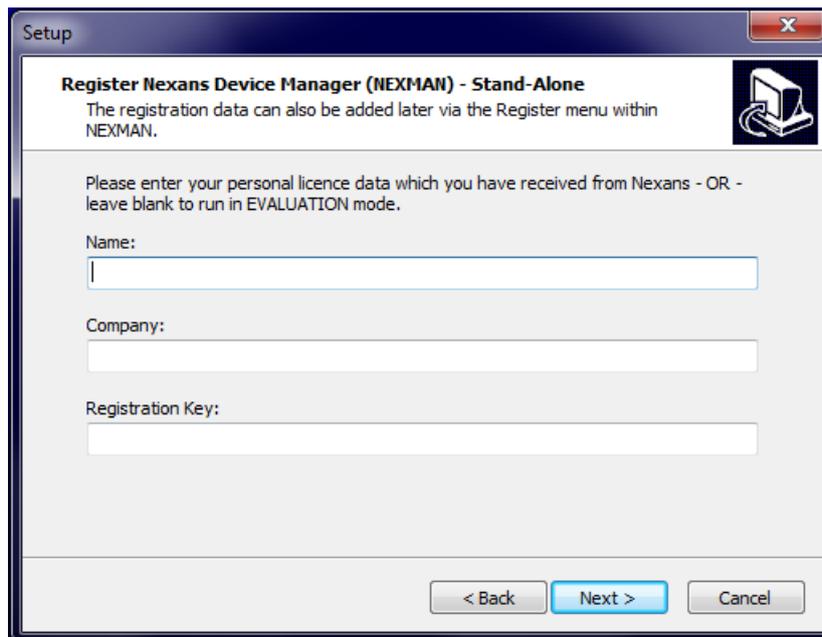
Select your preferred language. The language can also be changed via the preferences after the installation.



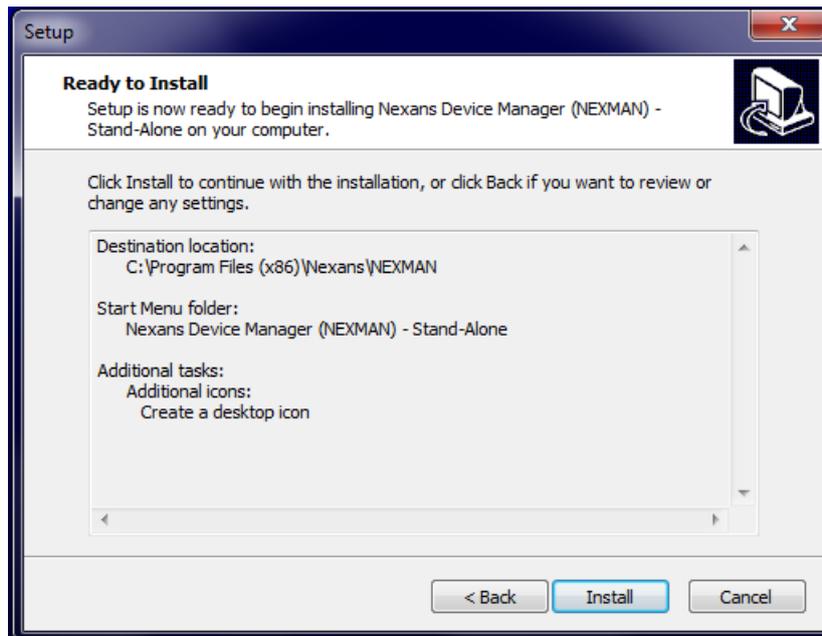
Choose a name for the start menu folder or decide not to create one.



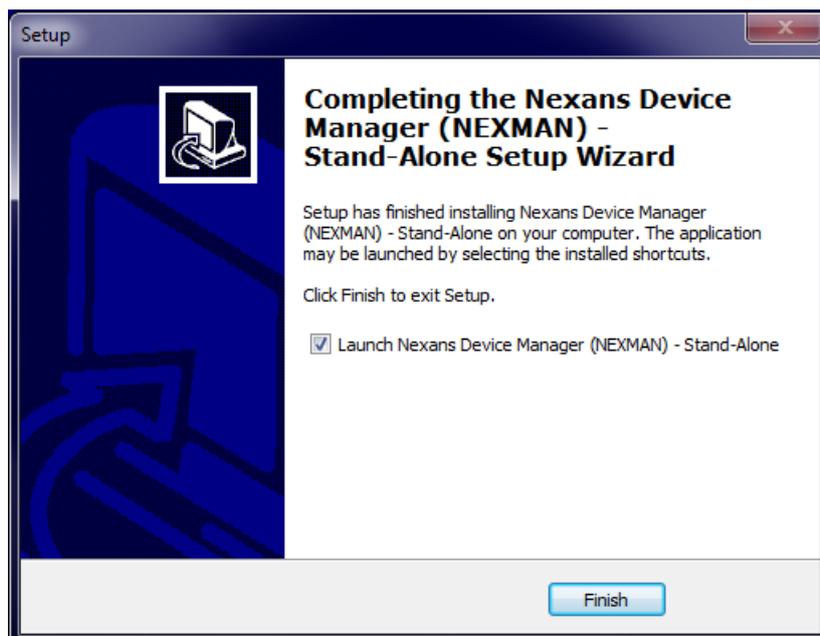
Decide, whether you want to have a shortcut created on your desktop.



Enter a registration key if available. Leave blank to use the EVALUATION version of NEXMAN. The registration key can also be entered after the installation.

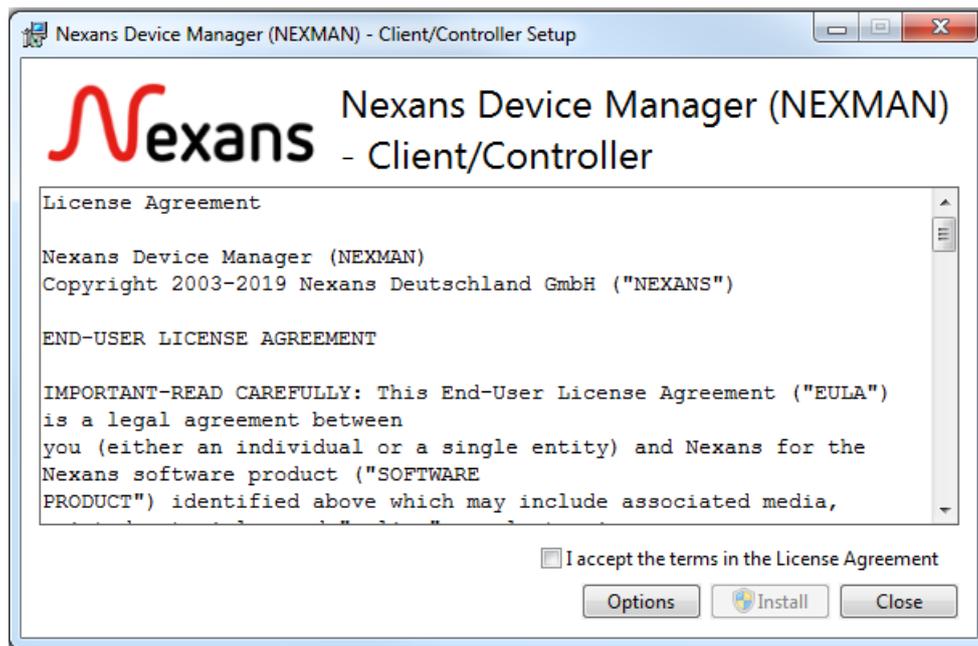


Check the summary of your settings and click on **Install** to start the installation.

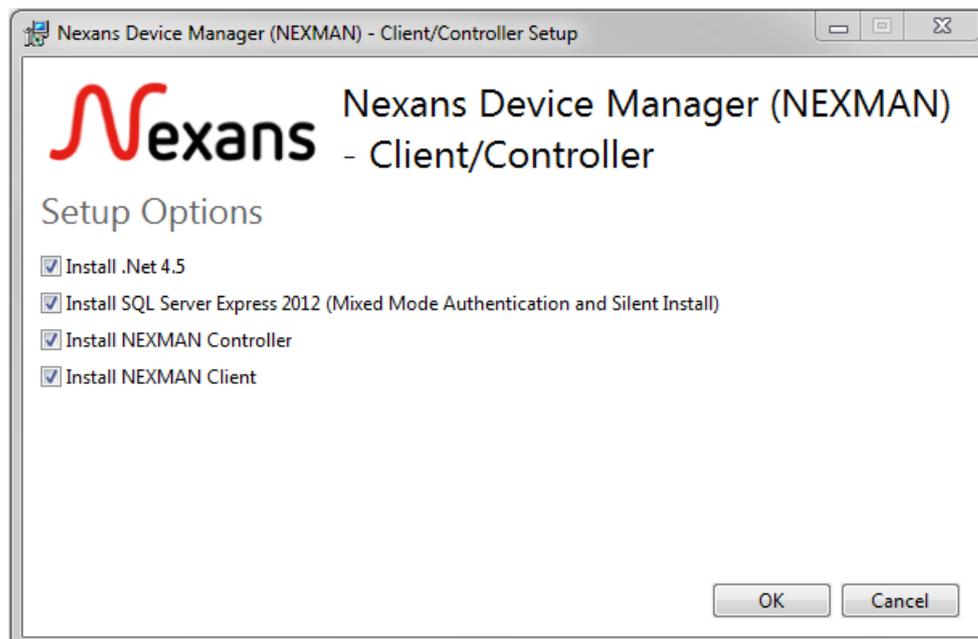


Once the installation is completed click on **Finish** to end the setup and launch NEXMAN.

2.2. Installation of NEXMAN Client / Controller



For the installation of NEXMAN Client and/or NEXMAN Controller execute the file **NEXMAN_ClientController_VX.xx_Setup.exe**. First read the license agreement carefully and accept the terms in the agreement. By clicking the button **Options**, you can choose between the different products to be installed.

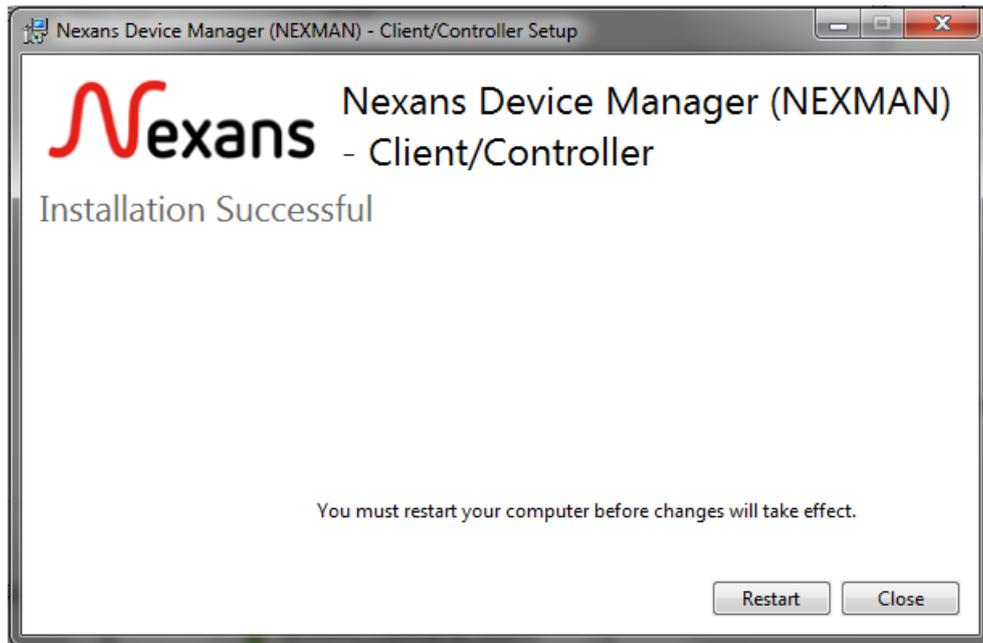


- **Install .NET 4.5:** The Microsoft .NET Framework version 4.5. Necessary for using NEXMAN Client or NEXMAN Controller. It is recommended to keep this product selected, because it will be skipped automatically if already installed.
- **Install SQL Server Express 2012:** Necessary for the NEXMAN database, must be installed together with NEXMAN Controller, if controller and database shall run on the same machine. There is no need to

install this product if you run the NEXMAN Client only or if you have SQL Server Express already installed.

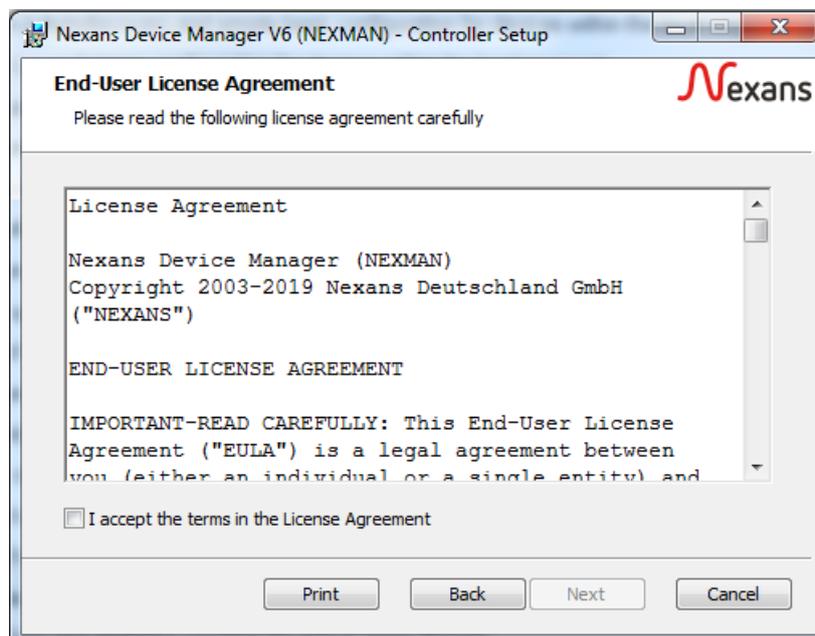
- **Install NEXMAN Controller:** The controller part of the NEXMAN application. Contains the service to collect device information and store them to the SQL database.
- **Install NEXMAN Client:** The client part to configure the Nexans devices and connect to the server.

If you choose to install NEXMAN Controller, you must reboot your computer after the setup is finished by clicking **Restart**. If you click **Close** the service is stopped until the next reboot.

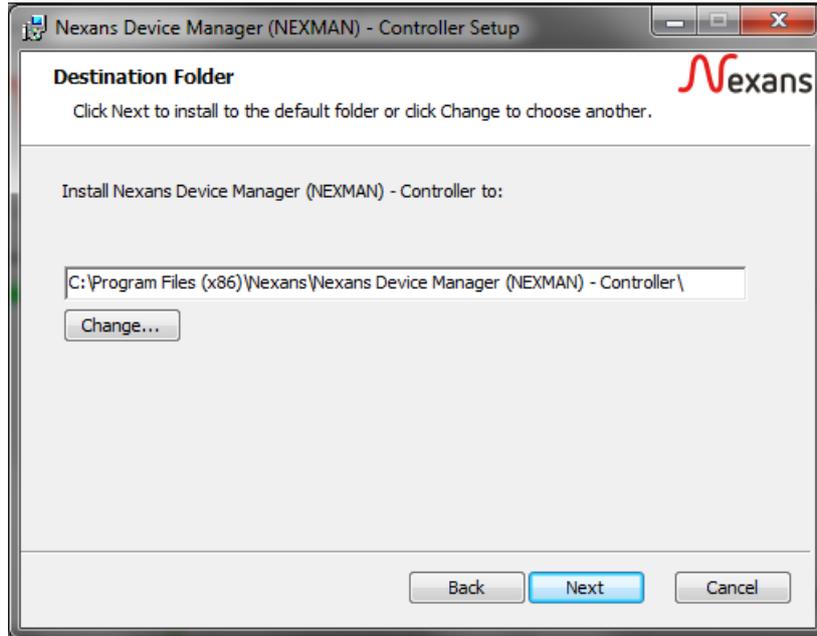


2.2.1. Installing NEXMAN Controller

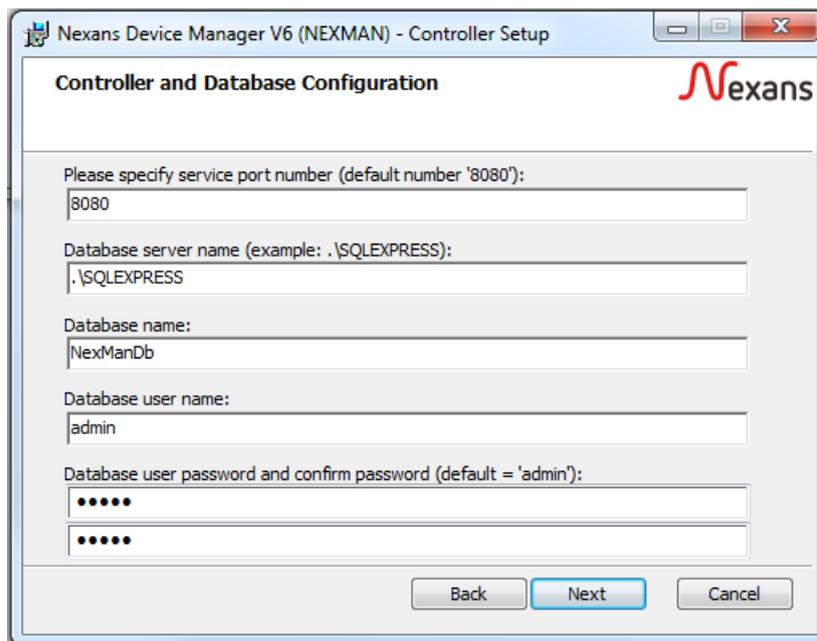
Click **Next** to start the installation of NEXMAN Controller.



Read the license agreement and accept the terms in the agreement. Continue with clicking **Next**.



Choose the installation folder. Use **Change...** to select a folder or just click **Next** to keep the default directory.

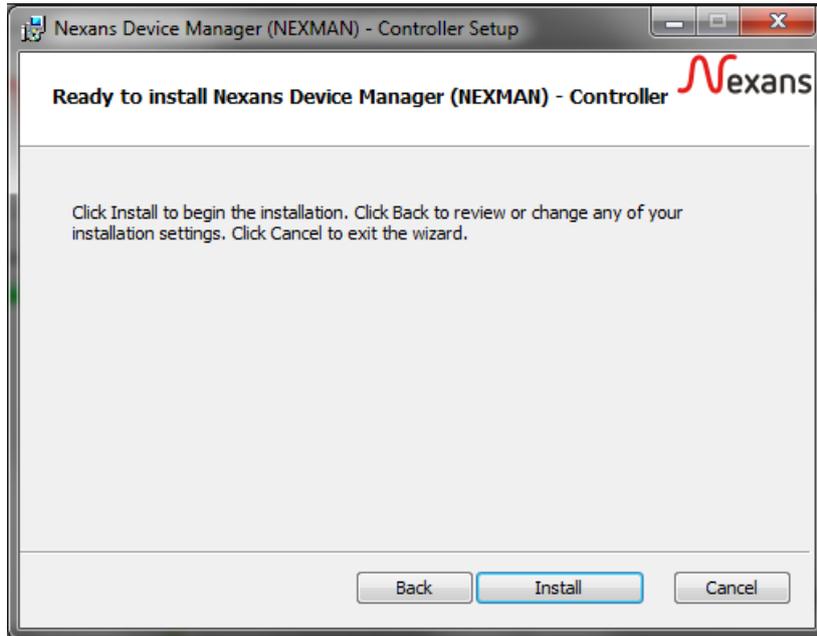


For configuring server specify the service port number first. After that, set the database server name and the name of the database itself. Use the default entry if you install the NEXMAN controller and the database on the same machine. Otherwise add the database server address or name, like 192.168.2.11\SQLEXPRESS or [DatabaseServerName]\SQLEXPRESS. Note, that in case of an external database SQL Server Express must already be installed on that machine. At last, enter the username and password needed to connect to the database. The default password is 'admin'. The 'Next'-Button will be disabled, if any value is missing or password and password confirmation do not match.

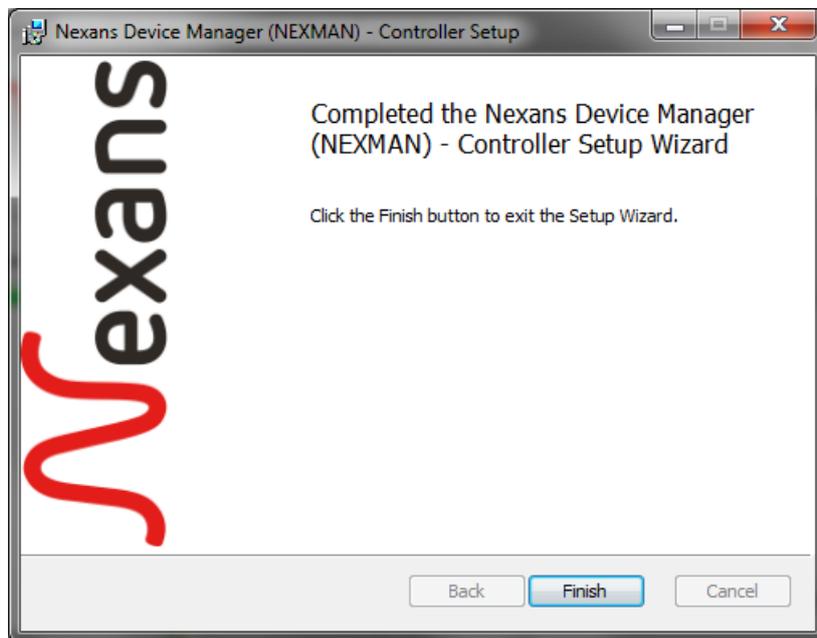
Note: If you are using IPv6 as database server address please be aware of the following rules:

- Replace colons ":" with dashes "-"

- Add the following to the end of the IPv6 address: '.ipv6-literal.net'
- Example: fe80::22a:b2ff:fe22:2bb2 → fe80-22a-b2ff-fe22-2bb2.ipv6-literal.net

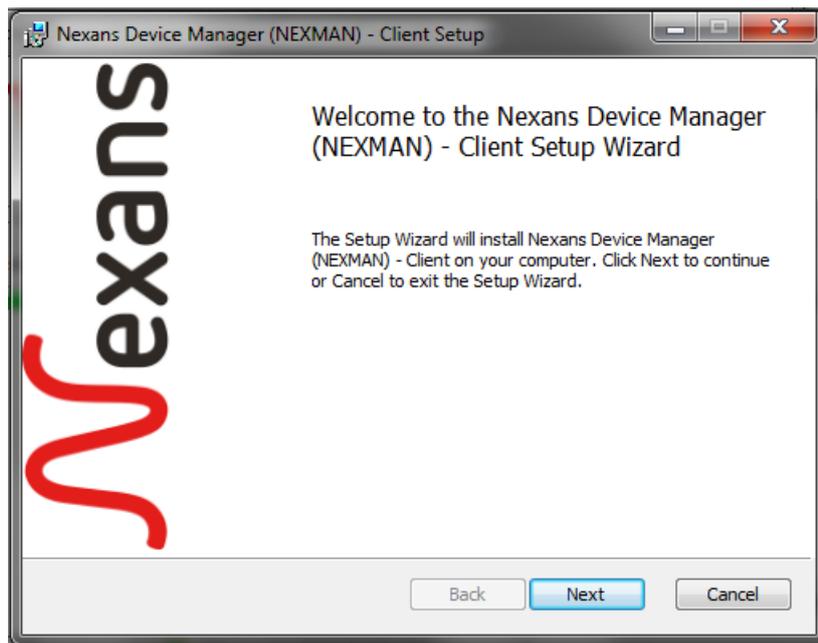


Click **Install** to start the installation.

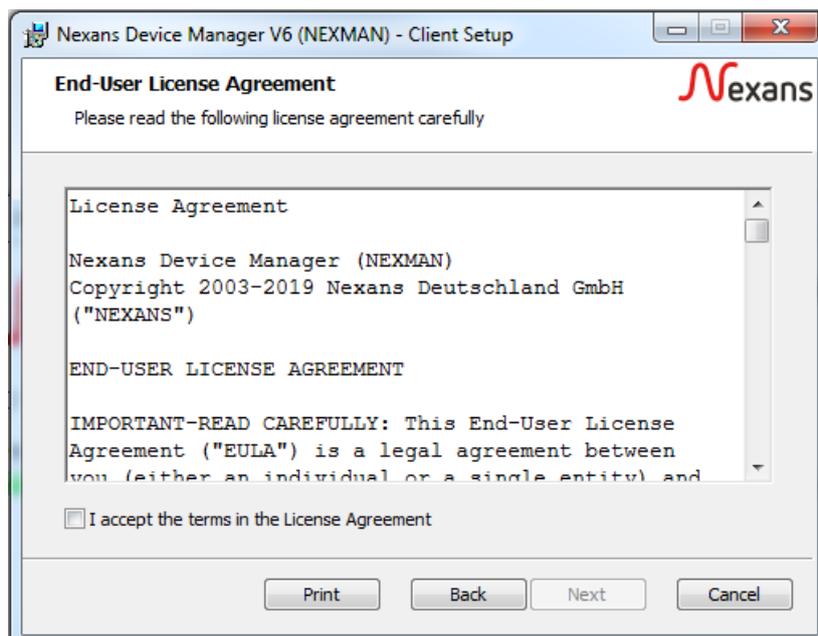


Once the installation is completed click **Finish** to end the setup of NEXMAN Controller.

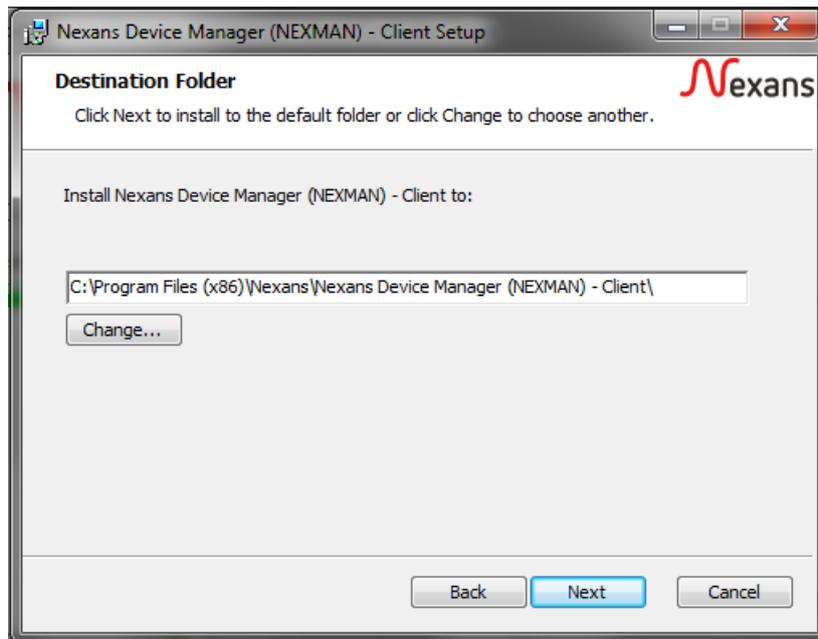
2.2.2. Installing NEXMAN Client



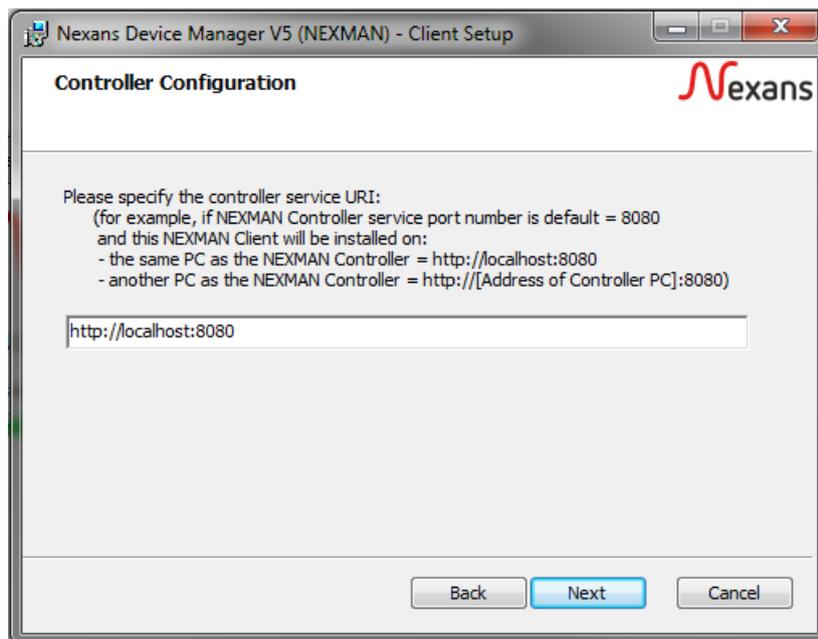
Click **Next** to start the installation of NEXMAN Client.



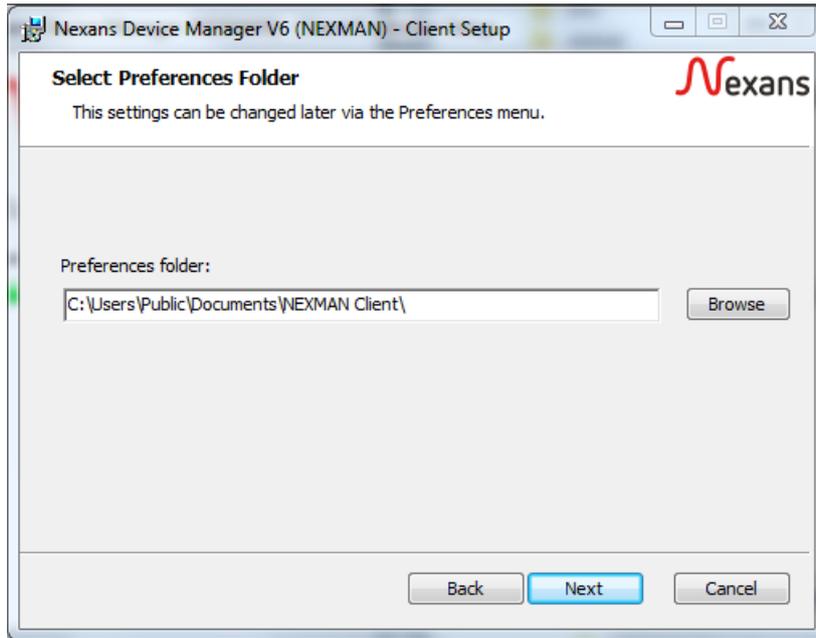
Read the license agreement and accept the terms in the agreement. Continue with clicking **Next**.



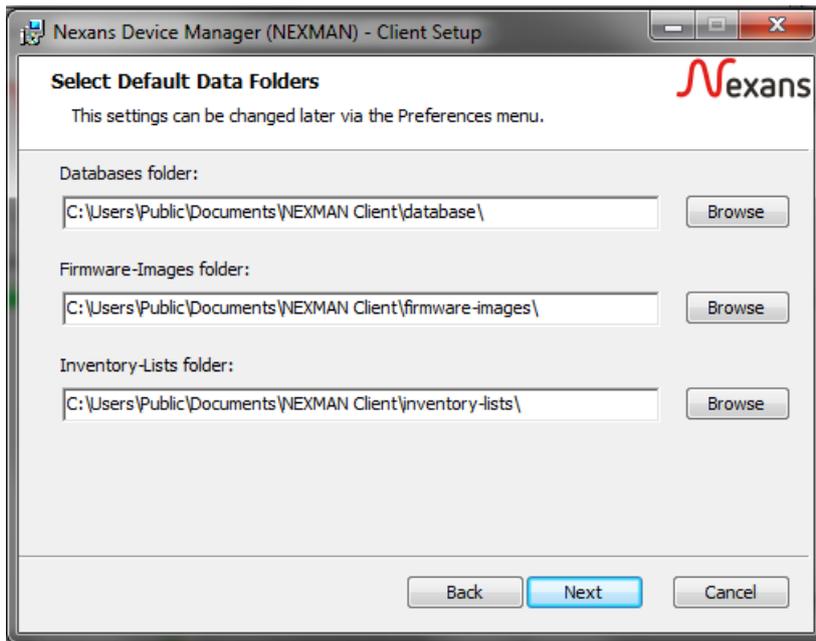
Choose the installation folder. Use **Change...** to select a folder or just click **Next** to keep the default directory.

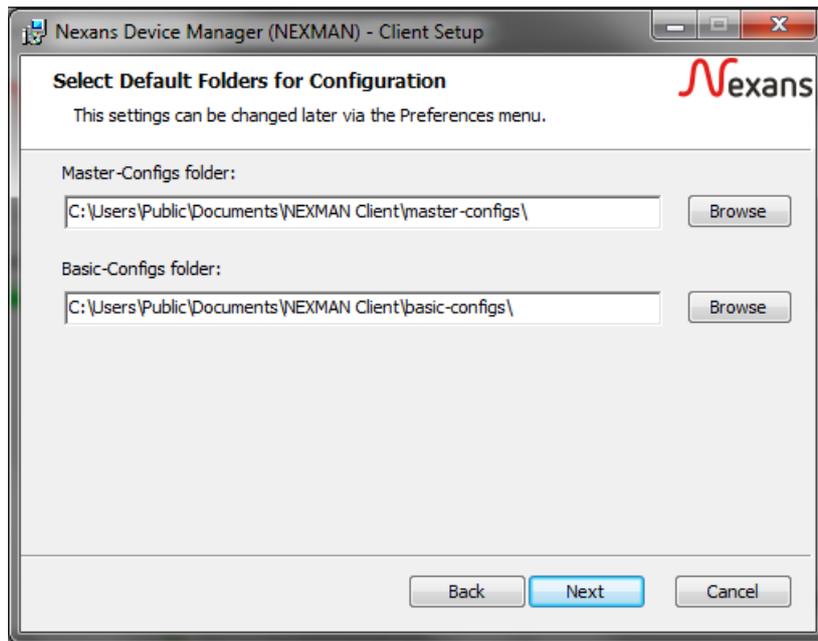


Enter the server URI the client must use to connect to the server containing the server address and the port number as you have specified it in chapter 2.2.1 *Installing NEXMAN Controller*. If you install the client on the same machine as the controller, use the “localhost” keyword or the IP address 127.0.0.1, otherwise ensure that you type in the correct IP address of your server.

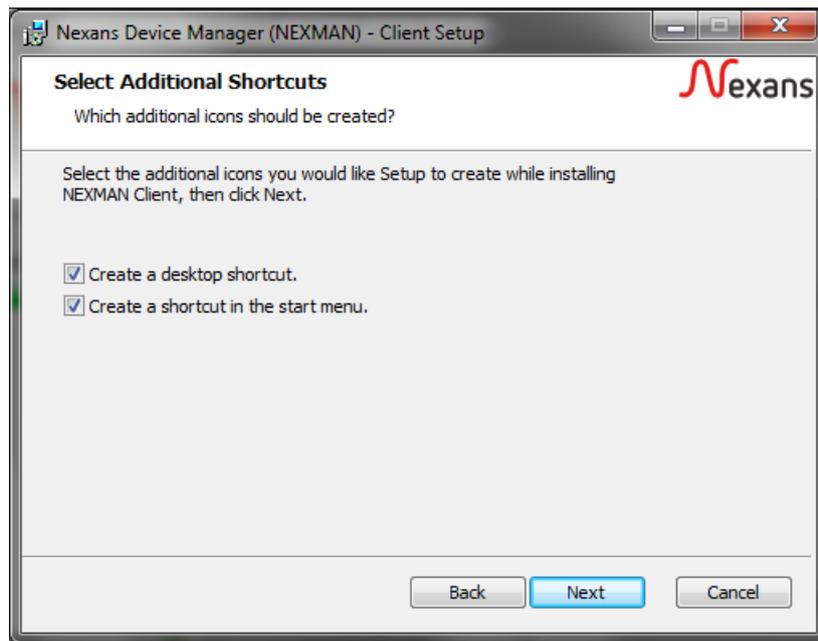


Specify the application data folder for NEXMAN. The application folder will contain the configuration files like NEXMAN.config where all preferences of the NEXMAN are stored. The folder must be writable. This path also will be the base path for the following directories.

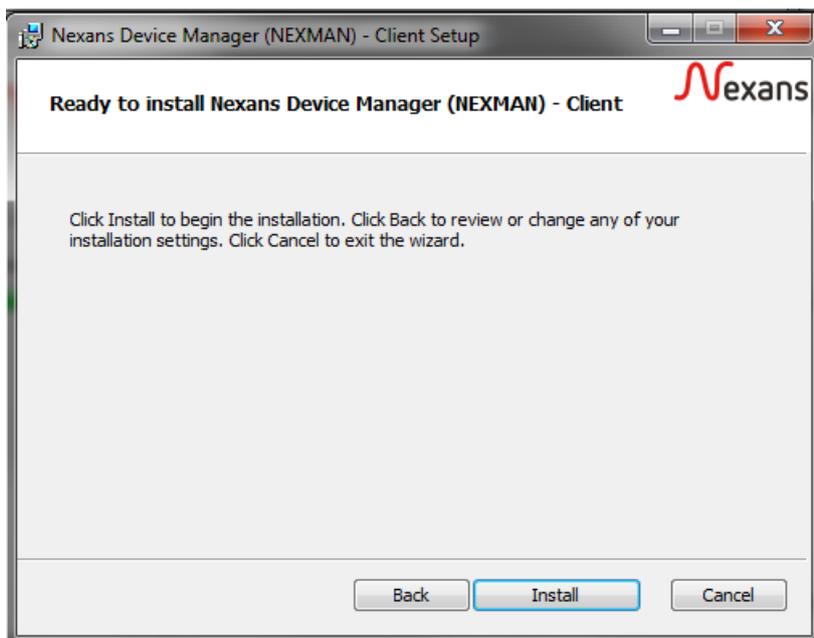




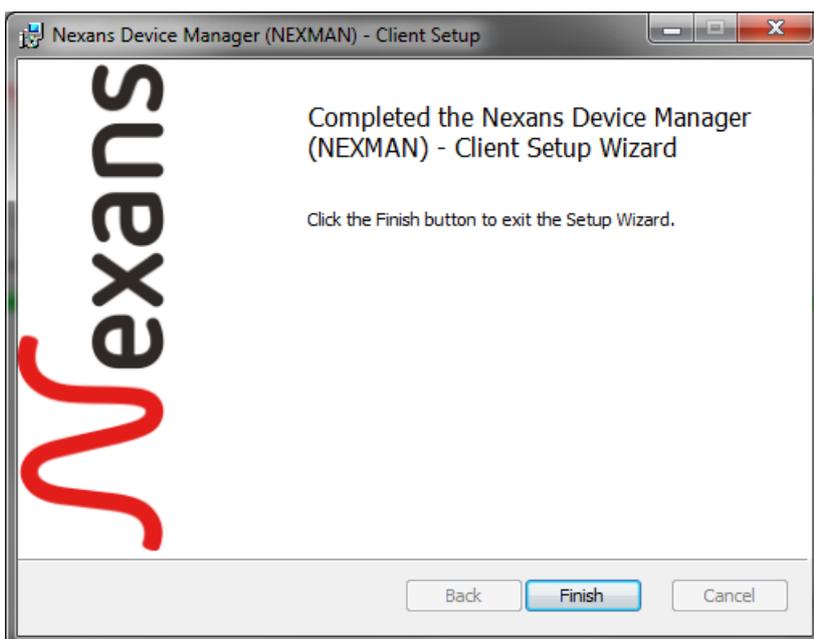
Specify the data folders for NEXMAN Client to store its data. Read more about the folders in chapter 18.5 *Folders*.



Decide, whether you want to have shortcuts created on your desktop or in your start menu.



Finally click **Install** to start the setup.



Once the installation is completed click **Finish** to end the setup of NEXMAN Client.

2.2.3. Using an existing database

To use an existing database some additional packages needs to be installed, depending of operating system and the SQL Server version which should be used:

- SQL Shared Management Objects (only for SQL Server 2014 and below)
- Microsoft System CLR Types

Both packages can be downloaded from the *Microsoft SQL Server Feature Pack*:

- SharedManagementObjects.msi
- SQLSysClrTypes.msi

If you are using Windows Server 2019 or higher please ensure that the *Microsoft Visual C++ Redistributable Package 2013* is installed. If not, this package can be downloaded from the Microsoft Home Page.

Using SQL Server Management Studio configure the existing database as follows:

- Security → Server authentication: SQL Server and Windows authentication mode
- Connections → Remote Server Connections: Allow remote connections to this server

Use the SQL Server Configuration Manager to ensure that

- Shared Memory
- TCP/IP
- Named Pipes

are enabled for your database instance.

2.2.4. User rights for SQL Express or SQL Server

To be able to install SQL Express or SQL Server the following user rights are needed:

Local Policy Object Display Name	User Right
Backup files and directories	SeBackupPrivilege
Debug Programs	SeDebugPrivilege
Manage auditing and security log	SeSecurityPrivilege

Read more at

<https://support.microsoft.com/en-us/help/2000257/sql-server-installation-fail-if-setup-account-not-have-some-user-right>

3. Switch Firmware Requirements

In order to use all features of NEXMAN, a firmware version 3.68 or higher needs to be installed on the switches:

If an older V3 firmware version is installed, any not supported parameters and status displays will be hidden or an appropriate message will be indicated.

If a firmware version 1.xx or 2.xx is installed on a device, this firmware needs first to be updated to the above version using the NEXMAN.

In case of a failed TFTP access you should check, whether it is blocked because of a too restrictively configured antivirus scanner.

For Zero Touch Configuration a firmware version V6.xx and hardware version 5 are required.

4. Firewall

For accessing the device configuration NEXMAN requires the following protocols:

- UDP - Port 50266 User authentication and device state
- UDP - Port 50268 Layer-2 Autodiscovery
- UDP - Port 50222 Zero Touch Configuration (NEXMAN Controller only)
- UDP - Port 514 SYSLOG Messages (NEXMAN Controller only)
- UDP - Port 162 SNMP Trap Messages (NEXMAN Controller only)
- TFTP - Port 69 Reading/writing of the configuration (if Manager Access Mode is set to "UDP/TFTP")
- TCP - Port 50271 Reading/writing of the configuration with SCP

If a firewall is installed on the local PC or on an installed router, you should check whether the above mentioned protocols are enabled.

For Client/Server-Communication the following protocol is needed additionally:

- TCP - Port 8080 (Default) Communication from Client to Server

5. Software Registration

To use the software without restriction a valid registration key is needed. Without a valid key the NEXMAN will work in the EVALUATION mode (see chapter 6. *Restrictions of the EVALUATION Version*).

If you have received NEXMAN on a licensed CD-ROM, there is a file named NEXMAN_Key.txt in the installation directory of the CD-ROM. This file contains the personalised key and will be automatically read during the installation procedure. Additionally the registration data is printed on a separate registration certificate.

As an alternative the key can be entered later via the **NEXMAN Help → Register NEXMAN** menu.

6. Restrictions of the EVALUATION Version

The EVALUATION version allows the management of individual devices. This version is free of charge and its run-time is unrestricted. However, all features necessary for the management of device lists have been disabled.

The EVALUATION version has the following restrictions as compared with the licensed version:

- a time-lagged start screen is shown prompting to enter the registration key.
- a maximum of five Devices can be stored and reloaded from a Device-List
- a maximum of five Devices can be selected and edited simultaneously
- Client/Controller:
 - Importing/Export Device-Lists from/to Stand-Alone version
 - Zero Touch Configuration
 - Time scheduled configuration

are limited to five devices as well.

7. Help and Documentation

The documentation on Nexans Device Manager (NEXMAN), Nexans Switch Basic Configurator and on the switch firmware can be loaded via the Manager Help menu as a PDF file.

The following documentation is available:

- Help → Manuals → Nexans Device Manager (NEXMAN)
Manual of Nexans Device Manager (the present document)
- Help → Manuals → Switch Firmware and Parameters
Detailed description of all switch functions and configuration settings
- Help → Manuals → Release Notes
Release Notes for Manager, Basic Configurator and Firmware.

8. Firmware Upgrade from Version V1/V2 to V3/V4/V5/V6

A change of firmware version V1.xx/V2.xx to V3.xx/V4.xx/V5.xx/V6.xx results in a basic functional upgrade in the firmware and in the Nexans Device Manager NEXMAN.

Because NEXMAN V6 is only able to read and write the configuration of firmware V3.xx/V4.xx/V5.xx/V6.xx, a firmware update to V3.xx/V4.xx/V5.xx/V6.xx must be performed. This update has to be performed using NEXMAN V6.

Important note:

We urgently recommend reading the Management Module and Firmware Versions chapter in the Nexans Switch Management manual and in particular the included remarks on the different firmware images prior to performing a firmware update.

9. Integration into a Central Management System

NEXMAN Stand-Alone can easily be integrated into a central management system (e. g. SNMPc, HP-Openview etc.) by entering optional parameters at the start of NEXMAN Stand-Alone. This procedure will bypass the device list and start directly the device editor.

The following two parameters are possible:

- **NEXMAN_StandAlone.exe -device -ip a.b.c.d**

The parameter "-device" will read and display the current device configuration. To do so, NEXMAN will query the Admin or User account.

Moreover the above parameter a.b.c.d has to be replaced by the device IP address. Usually management systems provide placeholders which, when called, are replaced by the IP address of the selected device. For example, with SNMPc this is "\$a", i.e. the full command would be as follows:

```
C:\Program Files\Nexans\NEXMAN\NEXMAN_StandAlone.exe -device -ip $a
```

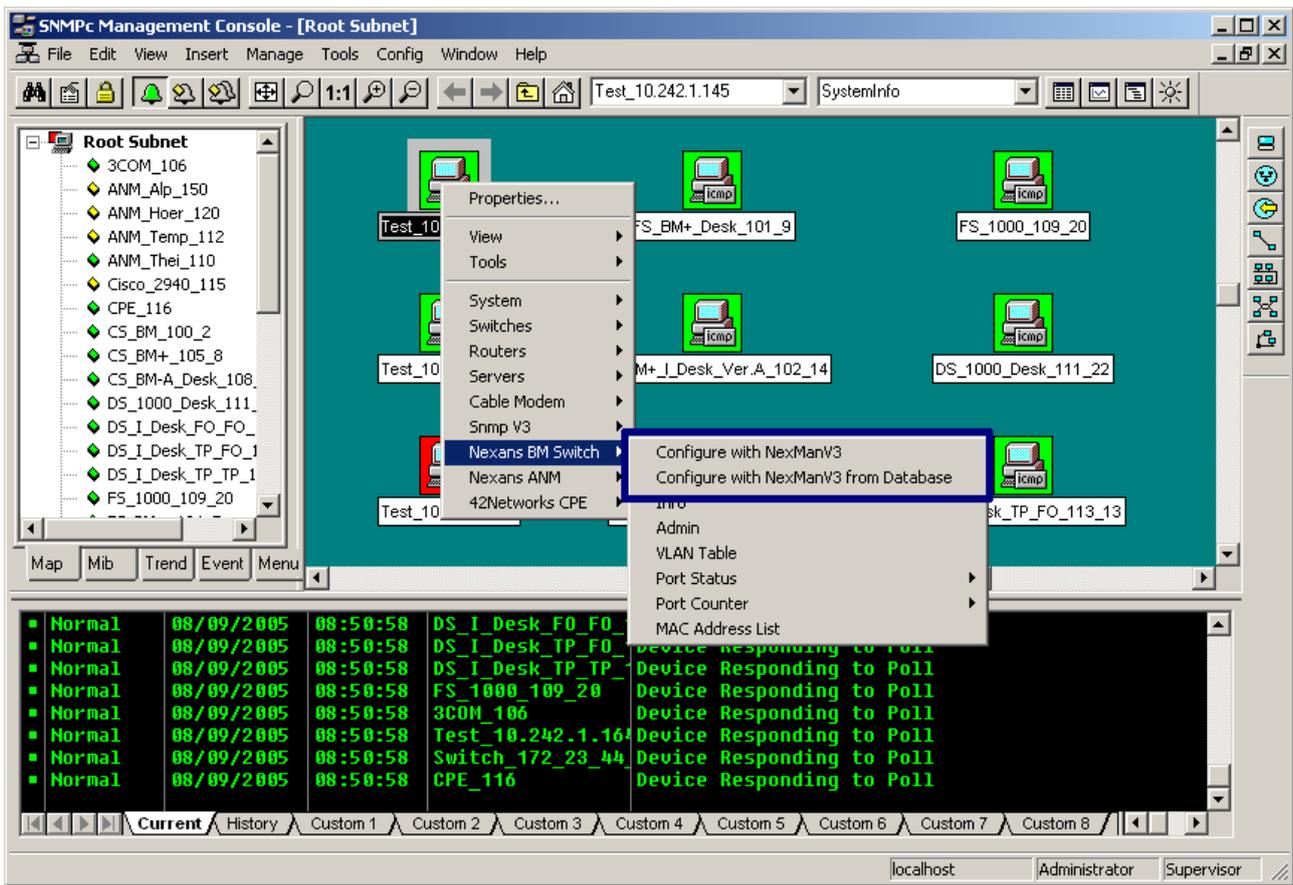
- **NEXMAN_StandAlone.exe -database -ip a.b.c.d**

The parameter "-database" will read the last configuration from the database. This is very useful, e.g. when the device cannot be reached, but the configuration needs to be consulted.

Note:

On the NEXMAN state page the current state of the device is always indicated, independent of what is stored in the database, and displayed on the appropriate configuration tabs. If the device cannot be reached, the state page remains empty.

Among others, for SNMPc a corresponding integration was created by Nexans and is available on request:



10. Name and Password as Starting Parameters

The indication of the optional parameters "-name <name>" and "-password <password>" at the start of NEXMAN Stand-Alone simplifies the manual entry of the name and password. In this case, the name and password indicated as parameters will be taken over as default into the dialog box.

Examples:

- `NEXMAN_StandAlone.exe -name admin -password Nexans`

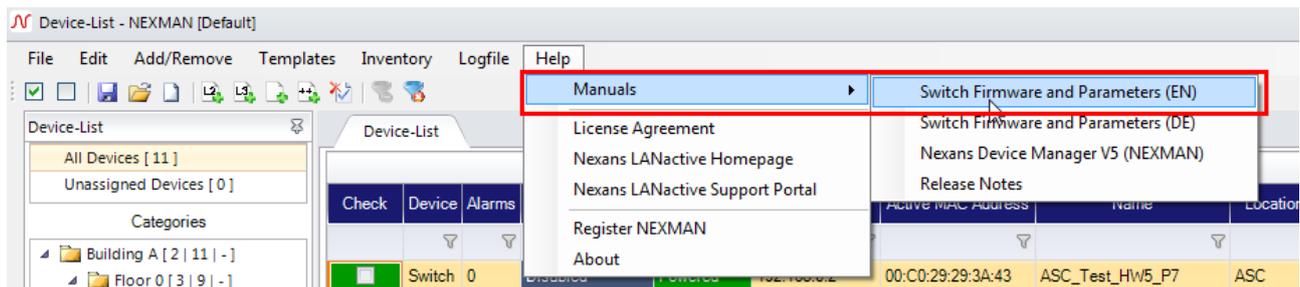
This command line will start NEXMAN and display the device list which was last loaded. As soon as the device is accessed the Authentication dialog window will be displayed with the specified name and password.

- `NEXMAN_StandAlone.exe -device -ip a.b.c.d -name admin -password Nexans`

This command line will directly start the configuration editor for the device with the IP address a.b.c.d (see chapter 9 *Integration into a Central Management System*). Here too, the Authentication dialog window will be displayed with the specified name and password.

11. Functional Description of Configuration Parameters

All configuration parameters within the Device-Editor are detailed in the "Switch Firmware" manual. This manual can be displayed via the menu **Help → Manuals → Switch Firmware and Parameters**:



12. Quick Start

12.1. Starting NEXMAN Stand Alone

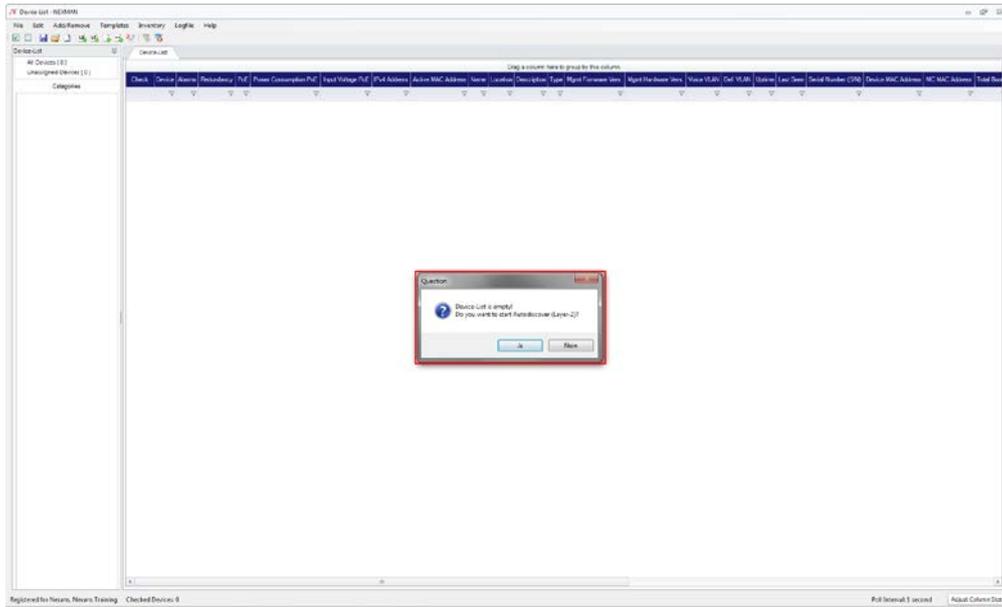
If no valid registration key was entered during the installation procedure, NEXMAN displays the following starting screen:



Please enter a valid key OR leave all fields empty. Please make sure that Name, Company and Registration Key are entered exactly as they are indicated on the Licence Sheet.

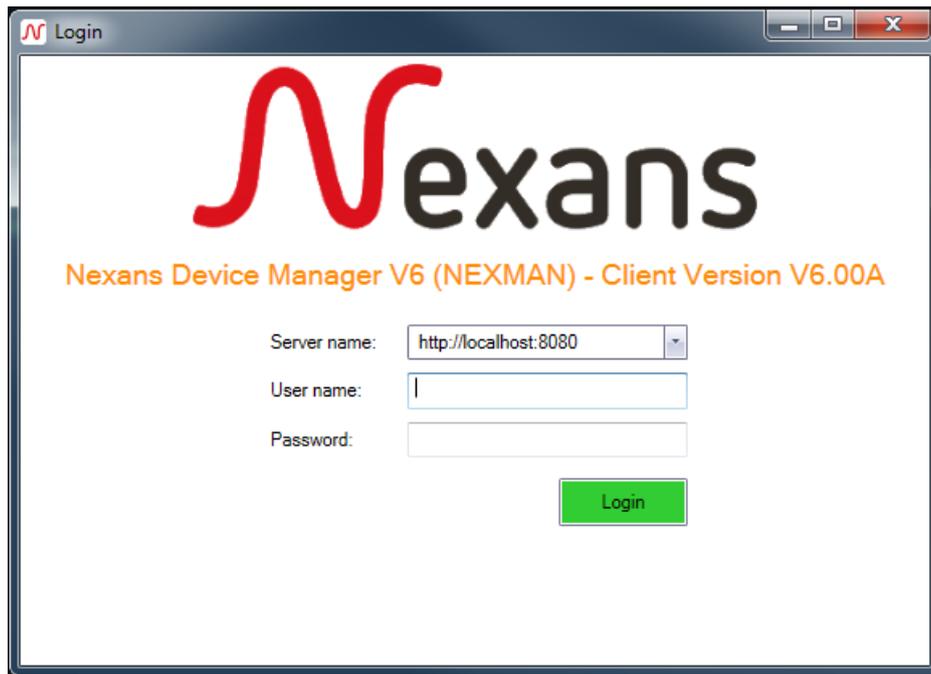
If the Registration Key field is left empty, NEXMAN will start in the EVALUATION mode (see chapter 6 *Restrictions of the EVALUATION Version*).

After pressing the **Continue** button the last device list is automatically loaded. If the device list is empty (as is the case after an initial installation), you will be asked first whether the Autodiscover (Layer-2) function shall be launched (only in Stand-Along version, more information on this topic see the next chapter):



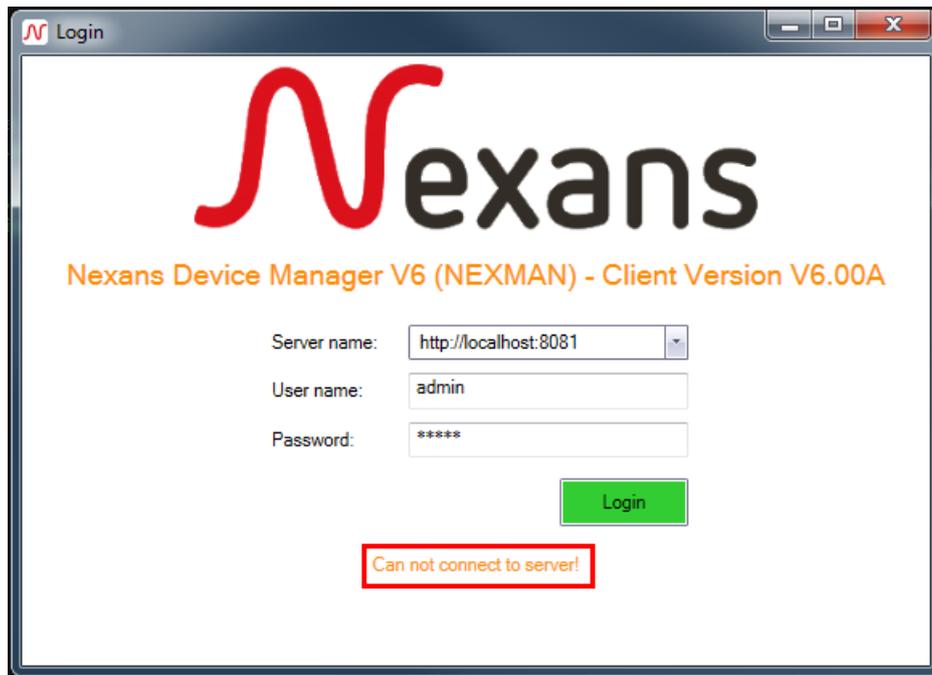
12.2. Starting NEXMAN Client

In order to use NEXMAN Client you must connect to the server:

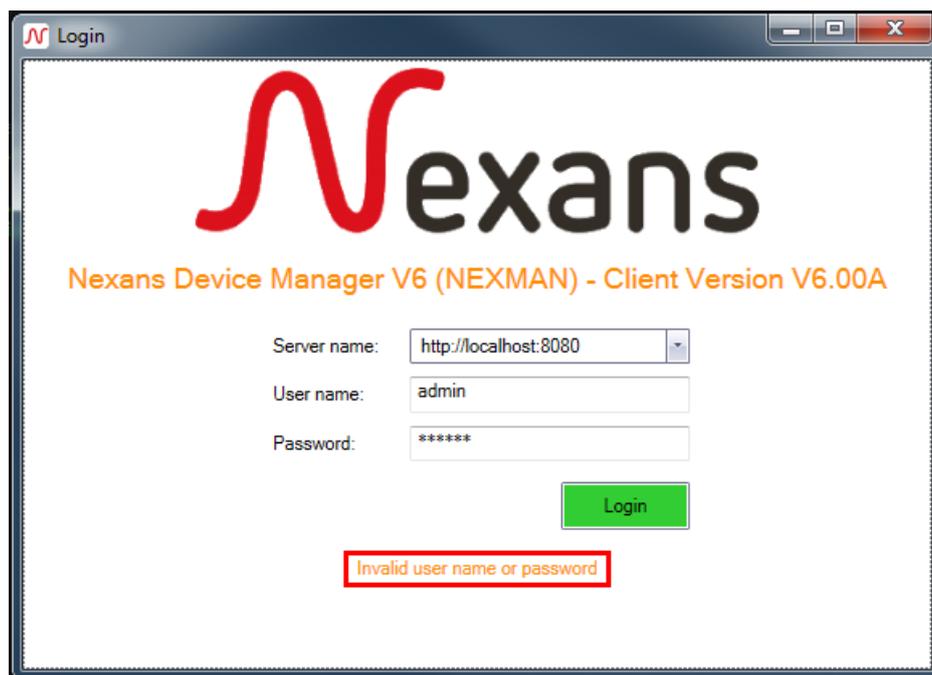


Type in the server's IP-Address or select a previously used address. Then enter your username and password to connect to the server. If you start the NEXMAN Client for the first time the default user and password are both 'admin'. Please change the default password immediately. Read more about editing a user in chapter *12.5 User Management in Client/Controller-Version*.

If you cannot connect (server is offline, wrong address...), an error message is shown:



Invalid user credentials will be notified as follows:



12.3. Adding Devices to Device-List

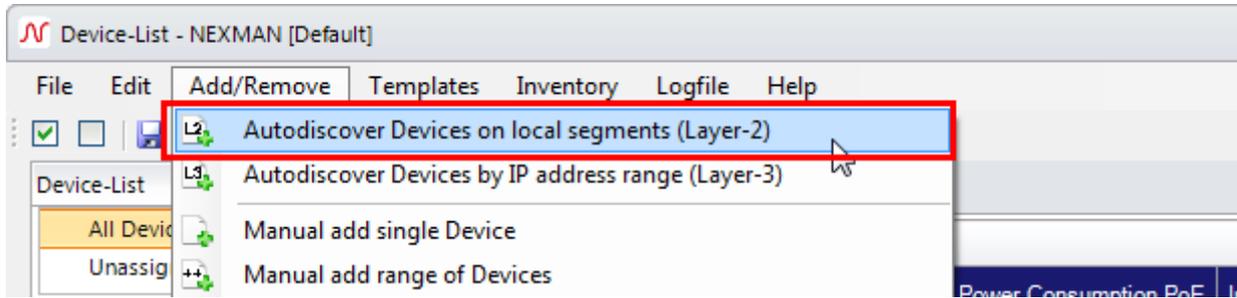
12.3.1. Adding Devices via Layer-2 Autodiscovery

The **Autodiscover Devices on local segment (Layer-2)** feature detects all devices in the network which are located in the same segment or LAN as the management PC.

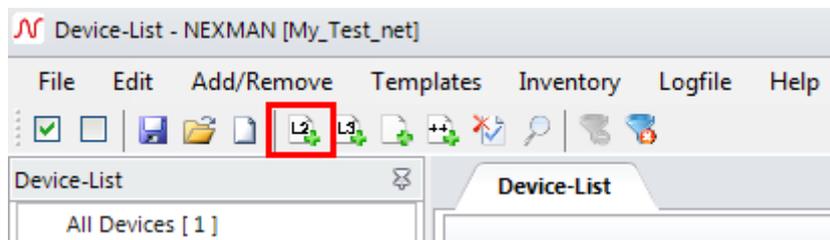
Devices, which can be addressed via a router only, can be detected automatically using the considerably slower **Autodiscover Devices by IP address range (Layer-3)** function (see next chapter).

Devices which have been detected using the Autodiscovery Layer-2 feature (also those without IP address) can be configured quite easily with their basic parameters (IP parameters, names, trunk port) in this mode. In this case the needed Basic Configurator is called directly from the Autodiscovery window.

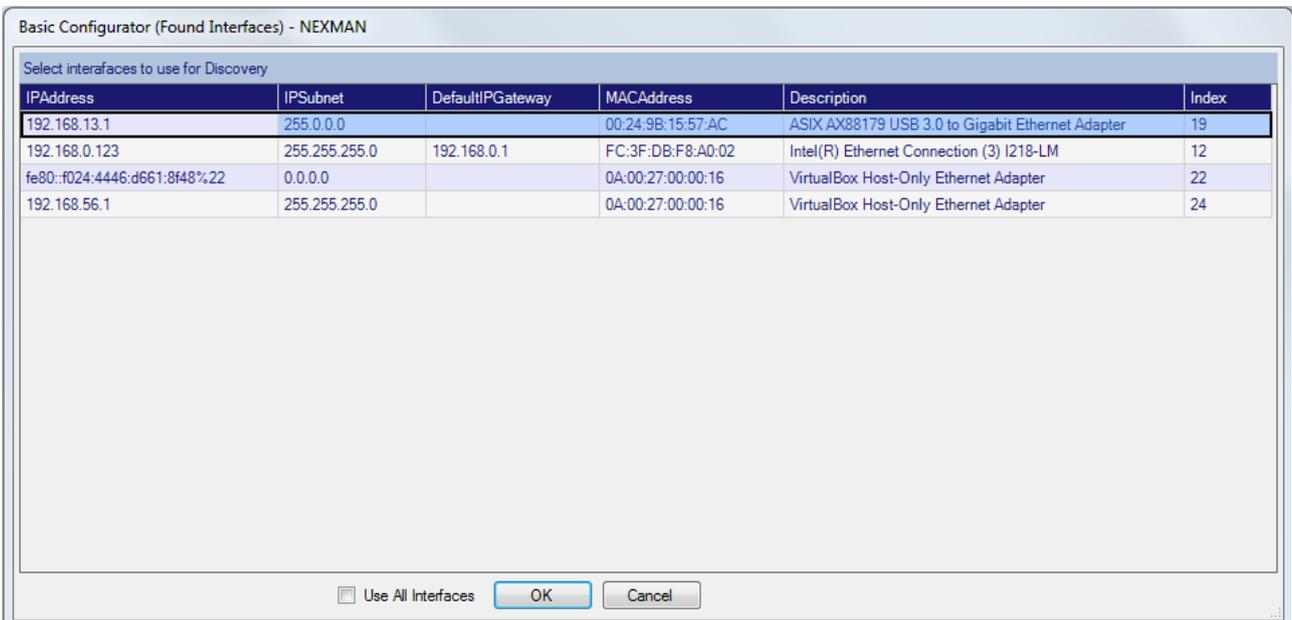
Autodiscovery can be launched either directly after launching the Manager (if the device list is empty, see previous chapter) or via the **Add/Remove** menu



or via the corresponding icon in the shortcut menu:

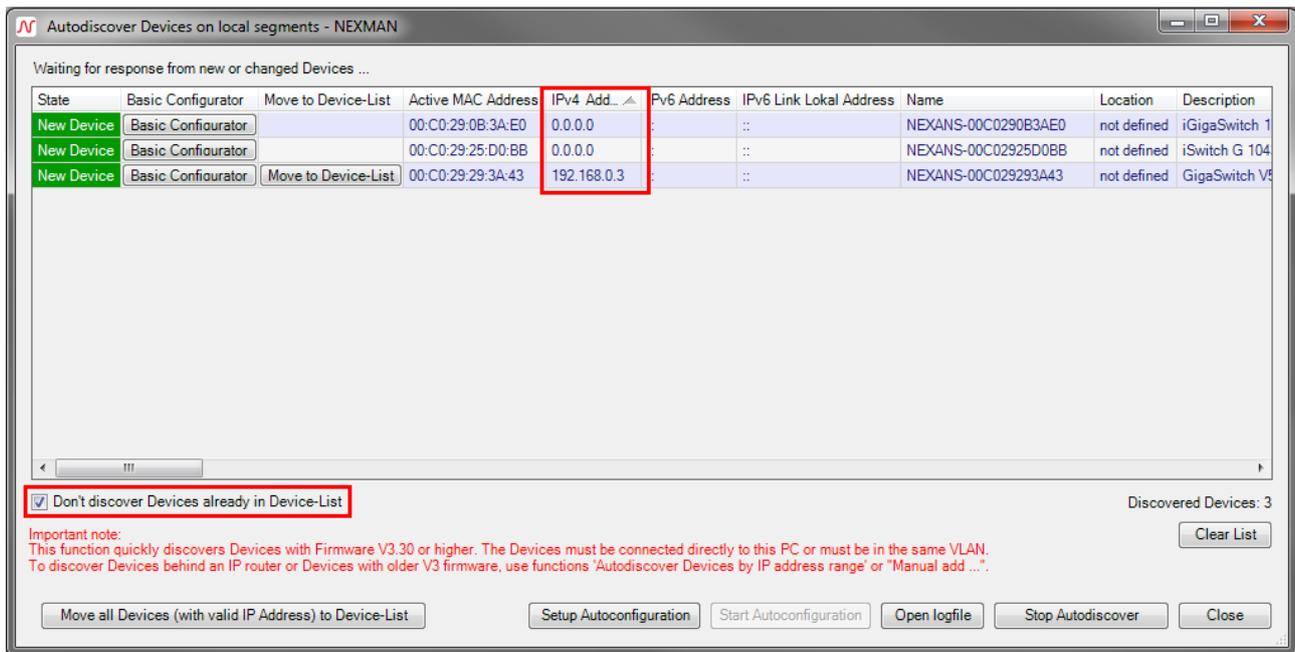


First of all, the interface to use for discovering has to be selected.



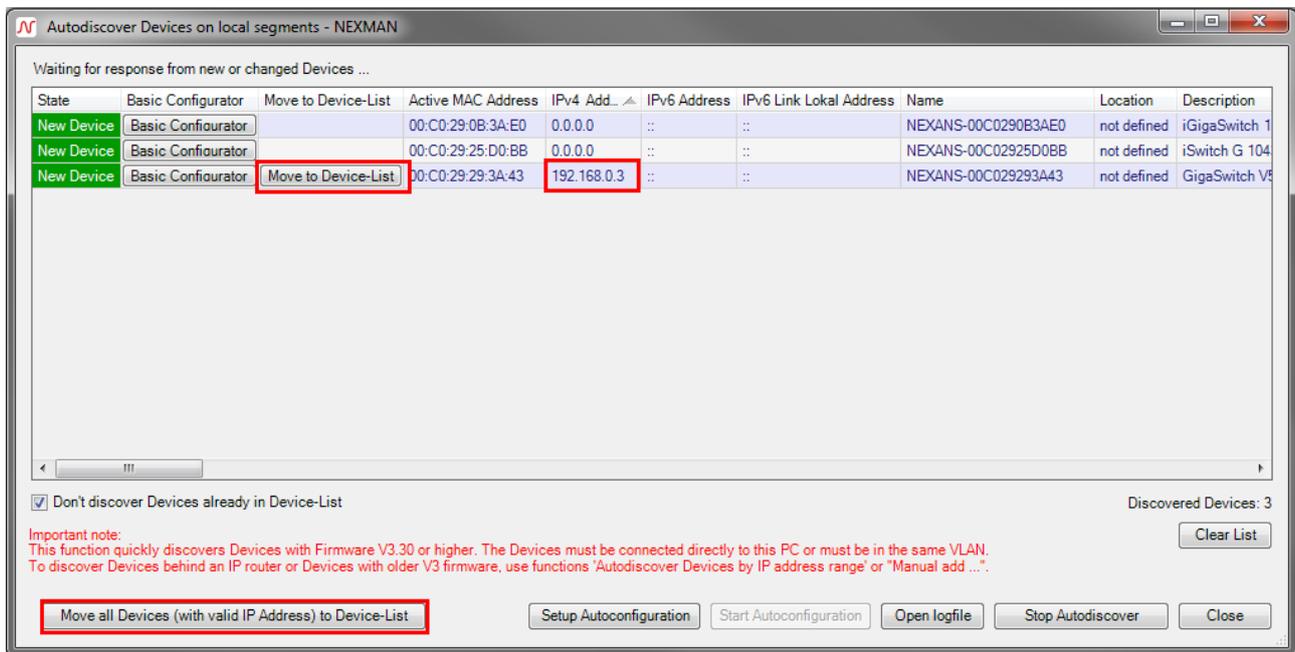
This can be achieved by selecting the desired interface and clicking **OK** afterwards or with a double click on the relevant interface. By clicking '**Use All Interfaces**' and **OK** every available interface will be used.

After starting the Autodiscovery window shows all devices answering to the periodic Layer-2 broadcast of NEXMAN. This can be devices with or without an IP address:



The box **Don't discover Devices already in Device-List** is checked by default. Responses from devices already listed in the currently open device list will be ignored.

Devices which have already received an IP address (e. g. via DHCP), can immediately be added to the device list. This is done via the **Move to Device-List** button for a single device or via **Move all Devices to Device-List** button for all devices in the list:



After being moved into the device list the devices are removed from the Autodiscovery window.

Devices without IP address cannot be moved into the device list and need to be assigned an IP address first via the **Basic Configurator**:

Autodiscover Devices on local segments - NEXMAN

Waiting for response from new or changed Devices ...

State	Basic Configurator	Move to Device-List	Active MAC Address	IPv4 Add...	IPv6 Address	IPv6 Link Lokal Address	Name	Location	Description
New Device	Basic Configurator		00:C0:29:0B:3A:E0	0.0.0.0	::	::	NEXANS-00C0290B3AE0	not defined	iGigaSwitch 1
New Device	Basic Configurator		00:C0:29:25:D0:BB	0.0.0.0	::	::	NEXANS-00C02925D0BB	not defined	iSwitch G 104
New Device	Basic Configurator	Move to Device-List	00:C0:29:29:3A:43	192.168.0.3	::	::	NEXANS-00C029293A43	not defined	GigaSwitch V5

Don't discover Devices already in Device-List Discovered Devices: 3

Important note:
This function quickly discovers Devices with Firmware V3.30 or higher. The Devices must be connected directly to this PC or must be in the same VLAN.
To discover Devices behind an IP router or Devices with older V3 firmware, use functions 'Autodiscover Devices by IP address range' or 'Manual add ...'.

Clear List

Move all Devices (with valid IP Address) to Device-List Setup Autoconfiguration Start Autoconfiguration Open logfile Stop Autodiscover Close

Afterwards the configuration of the respective device is automatically read and displayed via the Switch Basic Configurator:

Basic Configurator (MAC Address Mode) - NEXMAN

Device Info

Description: GigaSwitch V5 SFP-2VI 54VDC
Part Number (P/N): 88303953
Production Lot: 3746
Serial Number (S/N): 007783
Firmware Version: HW5-F40-P07-OFFICE-V6.01bs
Active MAC Address: 00:C0:29:29:3A:43

Device Setup

Name: NEXANS-00C029293A43
Location: not defined
Contact: not defined

IPv4 Access enabled:
DHCP IPv4 enabled:
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
IPv6 Address Mode: Disable IPv6 access
IPv6 Address: ::
Prefix Length: 0
IPv6 Gateway: ::
Trunk Port: none
Mgmt VLAN ID: 1

Write Setup to Device

User Defaults

Nicht definiert
Nicht definiert
Nicht definiert

0.0.0.0
0.0.0.0
0.0.0.0
Static IPv6 address
::
0
::
none
1

Save Defaults Load Defaults

Exit

Used network interface: [192.168.13.1] ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

If the configuration has been correctly read, the respective values will be displayed in the **Device Info** and **Device Setup** fields and can be modified. The data in the **Device Info** window is Read-Only and meant for your information only.

If multiple devices shall receive a similar configuration, a general basic setting can be defined in the **User Defaults** field and copied via the  button into the **Device Setup** field. Via the **Save Defaults** or **Load Default** buttons any template can be saved to or reloaded from hard disk.

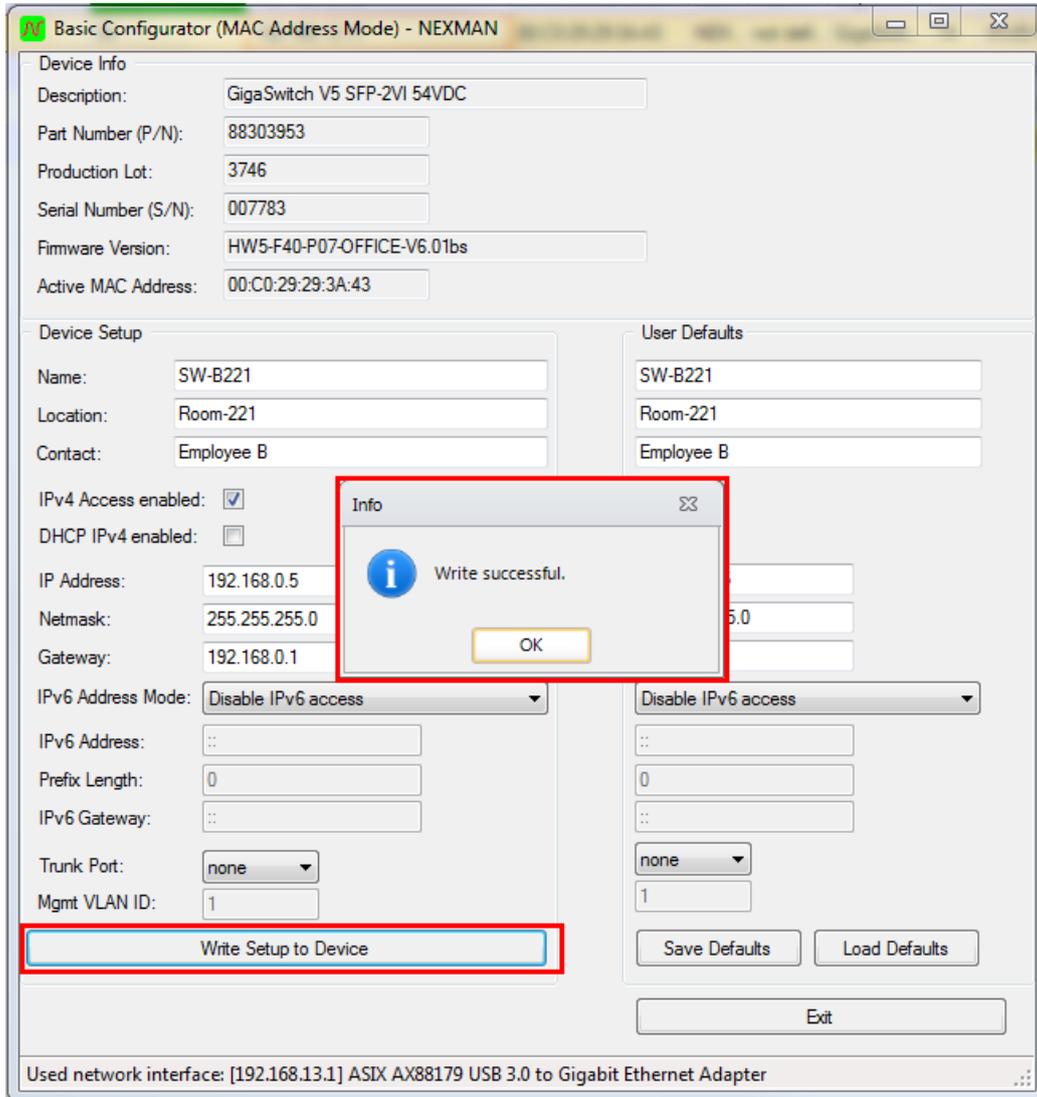
The screenshot displays two configuration panels side-by-side. The left panel, titled 'Device Setup', contains fields for Name (NEXANS-00C029293A43), Location (not defined), and Contact (not defined). It also has checkboxes for IPv4 Access enabled and DHCP IPv4 enabled, both checked. Below these are input fields for IP Address, Netmask, and Gateway, all set to 0.0.0.0. There is a dropdown for IPv6 Address Mode set to 'Disable IPv6 access', and fields for IPv6 Address, Prefix Length (0), and IPv6 Gateway. At the bottom are dropdowns for Trunk Port (none) and Mgmt VLAN ID (1), and a 'Write Setup to Device' button.

The right panel, titled 'User Defaults', is enclosed in a red border. It contains input fields for Username (SW-B221), Room (Room-221), and Employee (Employee B). It has checkboxes for 'Enable' (checked) and 'Disable' (unchecked). Below are input fields for Password (192.168.0.5), Confirm Password (255.255.255.0), and a dropdown for IPv6 Address Mode set to 'Disable IPv6 access'. There are also fields for IPv6 Address, Prefix Length (0), and IPv6 Gateway. At the bottom are dropdowns for Trunk Port (none) and Mgmt VLAN ID (1), and 'Save Defaults' and 'Load Defaults' buttons.

Between the two panels, there are two green arrow buttons pointing right. The top one is highlighted with a red box.

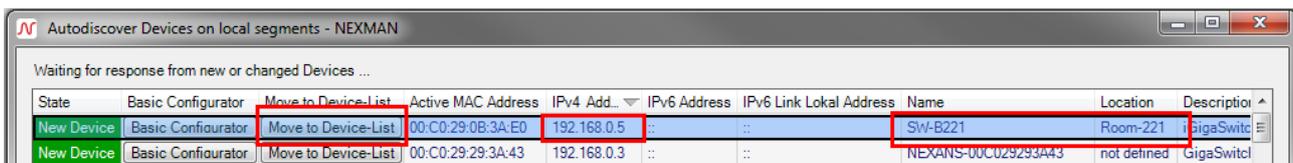
In order to write the modified configuration back into the device the Admin Name and the Admin Password should be set to Factory Default (name = admin, password = nexans). This restriction is a security feature to prevent installed devices, which have been assigned a customer-specific password, from being modified by the Basic Configurator.

After entry of the desired parameters a click on the **Write Setup to Device** button will transfer the configuration into the device. The configuration will take immediately effect without rebooting. A message informs about the successful completion of the write operation:



After confirming the Write Successful message, the **Write Setup to Device** button is disabled and the Basic Configurator can be left via the **Exit** button, in order to return to the Autodiscovery list:

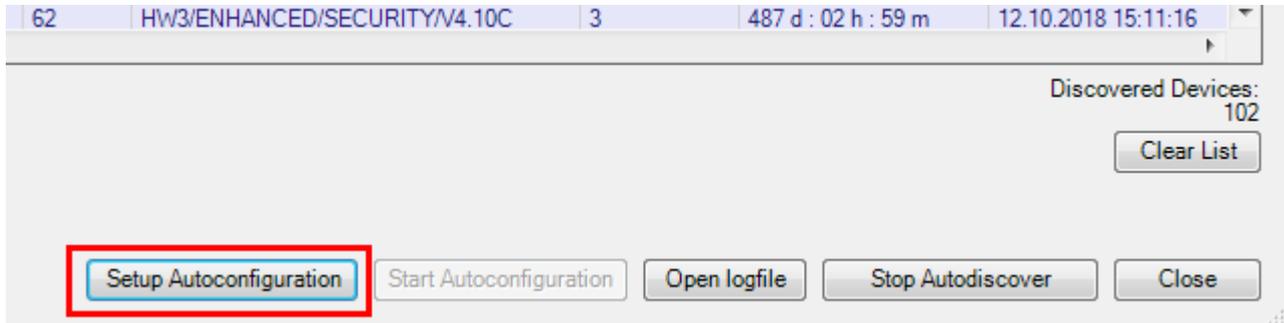
As soon as the configured device answers again, the Autodiscovery window will be updated with the new values and the device can now be moved into the device list via the **Move to Device-List** button:



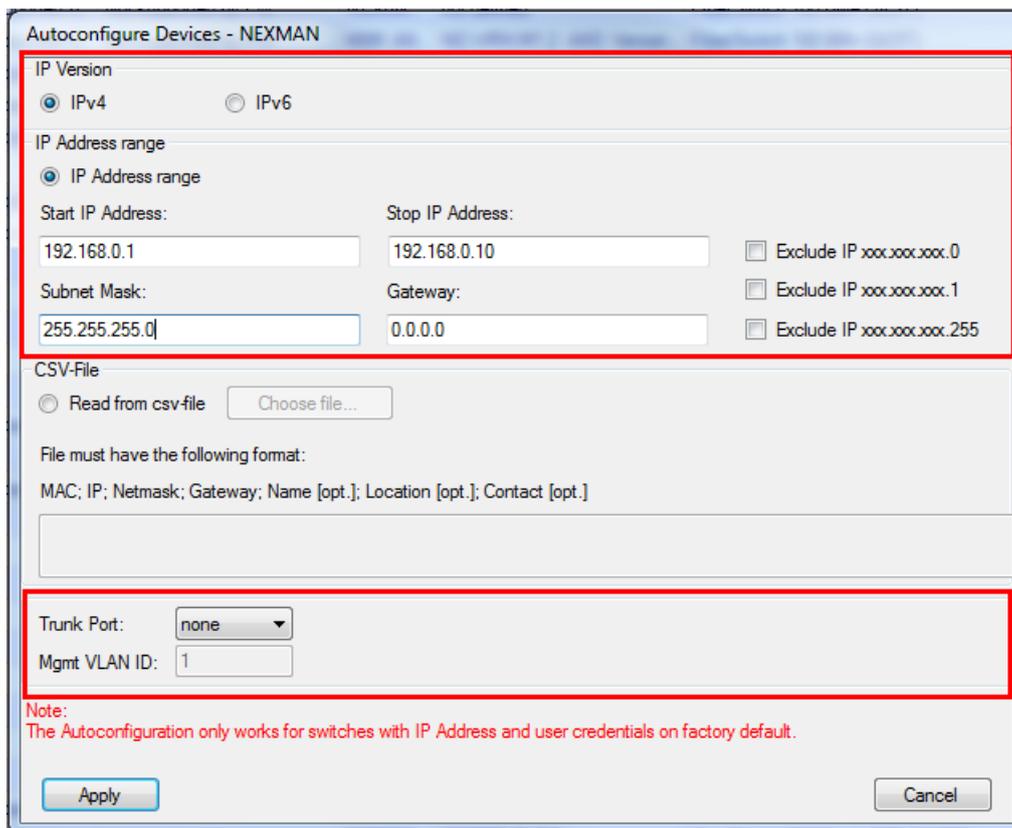
Read more about the Basic Configurator in chapter 13 Basic Configurator.

12.3.2. Automatic Basic Configuration

An easy way to apply the basic configuration to multiple device at the same time is the so called **Autoconfiguration**. All discovered devices with IP Address 0.0.0.0 and factory default username and password will automatically be configured with the pre-defined settings These settings must be prepared by clicking on **Setup Autoconfiguration**.



If you like to enter the IP Address range without additional information select **IP Address** range and fill in the necessary values. It is possible to exclude some special IP Addresses from the given range.



If your basic configuration should already contain information like name, location or contact prepare a .csv-file where these information are assigned to a specific MAC address like shown in the picture below:

	A	B	C	D	E	F	G	H
1	00:C0:29:20:33:56	10.242.1.158	255.255.252.0	10.242.0.1	NEXANS-00C029203356	testlocation	testcontact	
2	00:C0:29:0B:3A:E0	192.168.0.1	255.0.0.0	0.0.0.0	NEXANS-00C0290B3AE0	testlocation	testcontact	
3	00:C0:29:25:D0:BB	192.168.0.2	255.0.0.0	0.0.0.0	NEXANS-00C02925D0BB	testlocation	testcontact	
4	00:C0:29:29:3A:43	192.168.0.3	255.0.0.0	0.0.0.0	NEXANS-00C029293A43	testlocation	testcontact	
5								
6								
7								

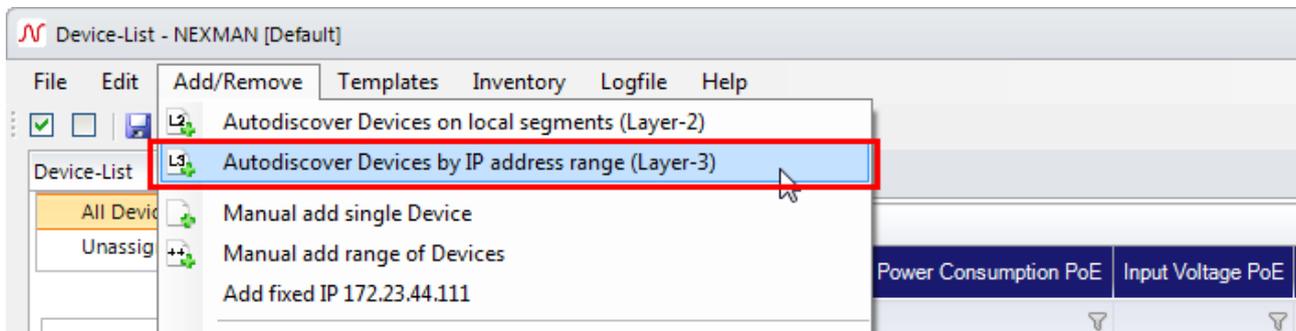
MAC address, IP address, gateway and netmask are compulsory entries.

Click **Apply** and **Start Autoconfiguration** to start. Every new device added by the Autodiscovery will also be included in the configuration process. By clicking **Stop Autoconfiguration** you can end the progress. This will also happen if no further IP addresses are available in your file or generated range. Open the logfile to have a look at the results. Note, that devices to be configured must be accessible with default username and password.

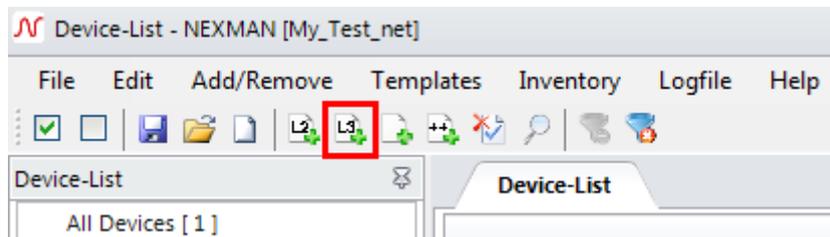
12.3.3. Adding Devices via Layer-3 Autodiscovery

Devices, which can be addressed via a router only, can be detected automatically using the **Autodiscover Devices by IP address range (Layer-3)** function. As a precondition these devices must already be configured with an IP address.

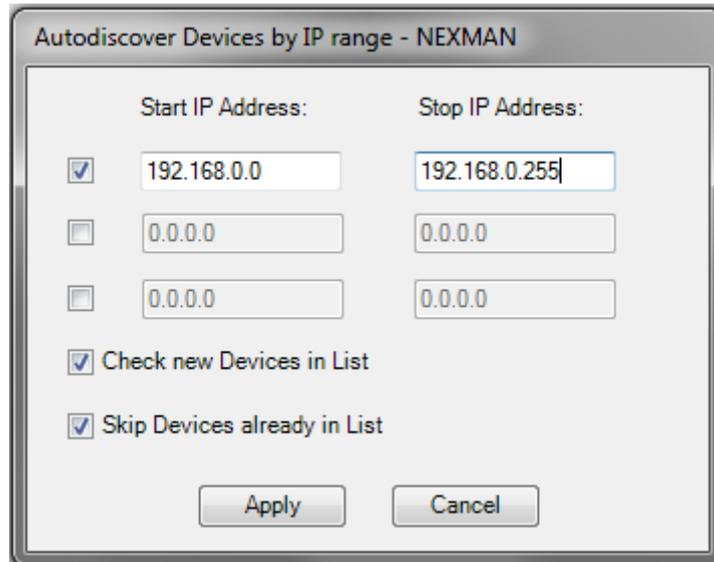
Autodiscovery can be started either via the **Add/Remove** menu



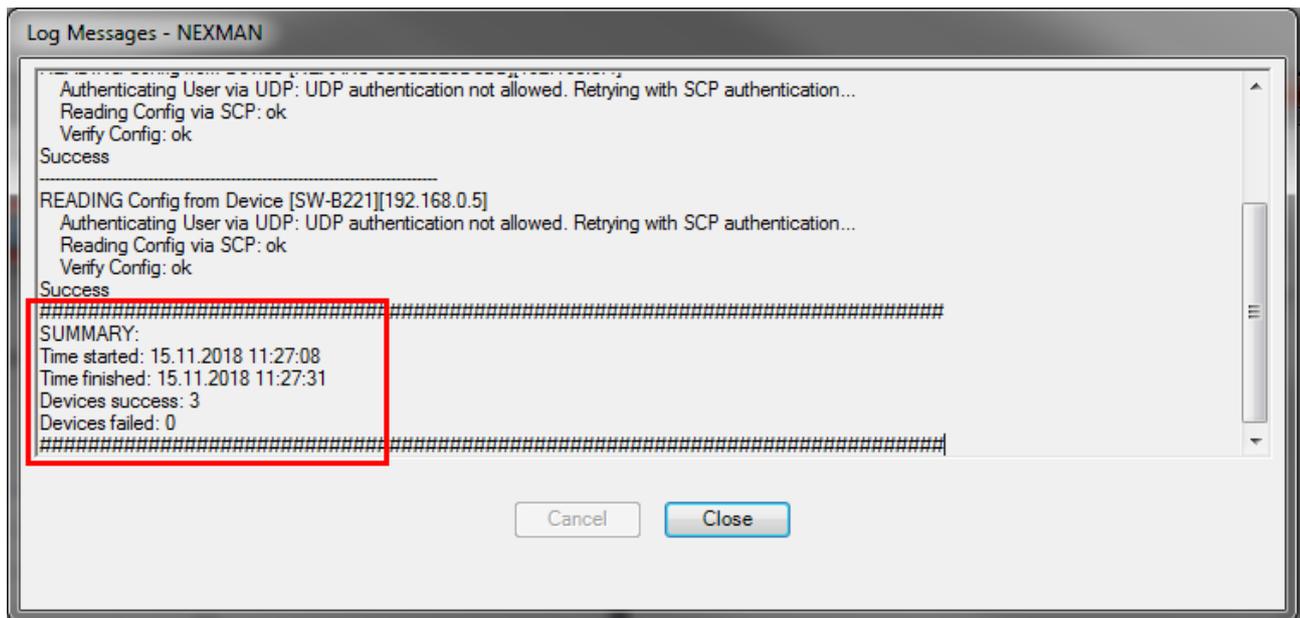
or via the corresponding icon in the shortcut menu:



In the following dialog box, up to three IP ranges can be indicated for searching for Nexans devices:



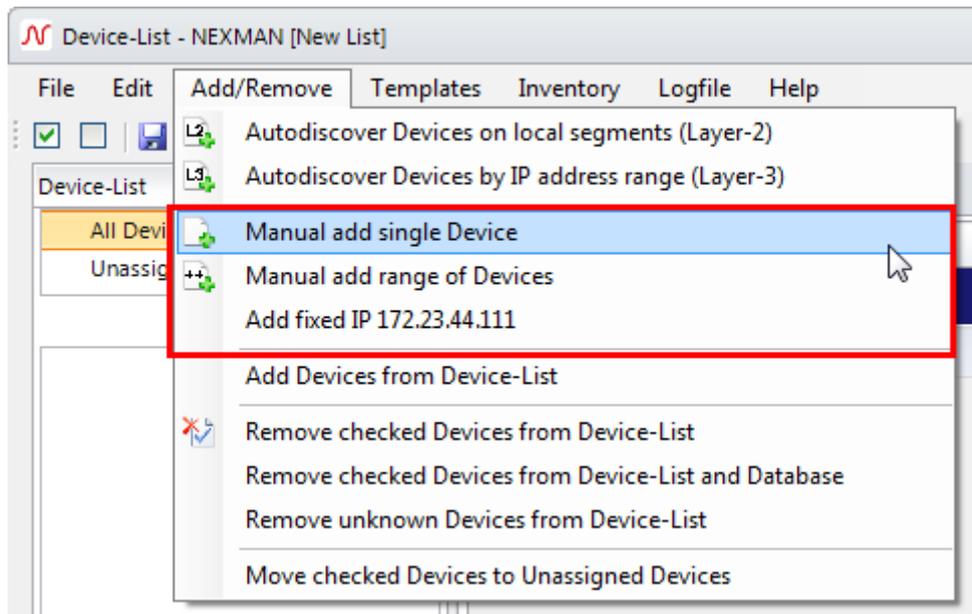
After pressing the **Apply** button and subsequent entry of the Admin Name and Admin Password all indicated IP addresses will be processed one after the other. Progress can be monitored in a log window (Note: If the required devices still have their Factory Default settings, there is no need to enter name and password):



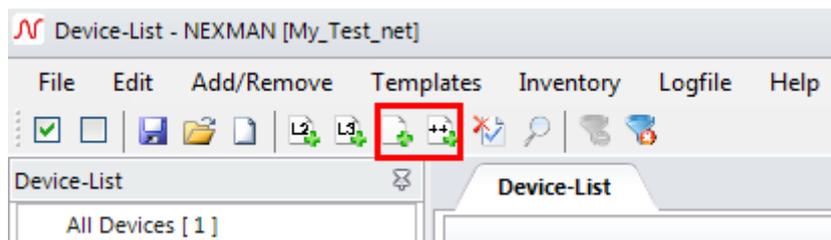
After pressing the Close button all detected devices are entered into the device list.

12.3.4. Adding Devices Manually to the Device List

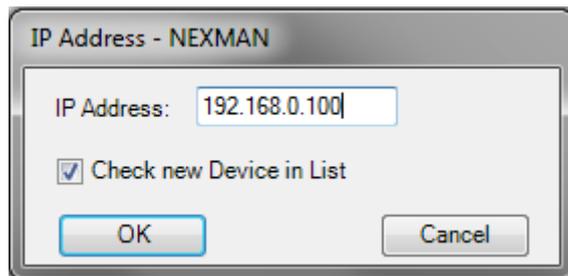
If the IP address of the respective devices is known, these devices can be added manually to the device list. This can be done via the **Add/Remove** menu



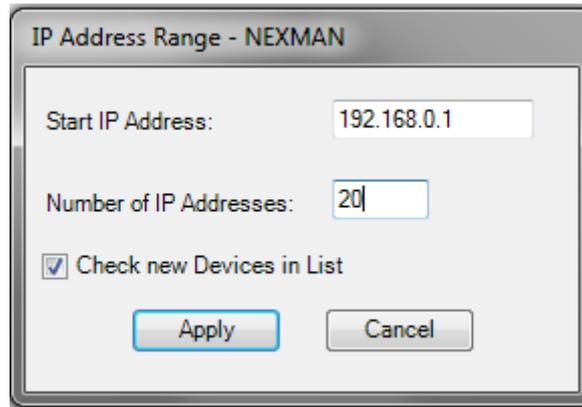
or via the corresponding icon in the shortcut menu:



As an example, you can now add a single device to the list by selecting the **Manual add single Device** menu option. Checking the **Check new Device in List** box will check the new device in the device list and select it for further actions:



Alternatively, a complete IP address range can be added to the list by selecting the **Manual add range of Devices** menu option:



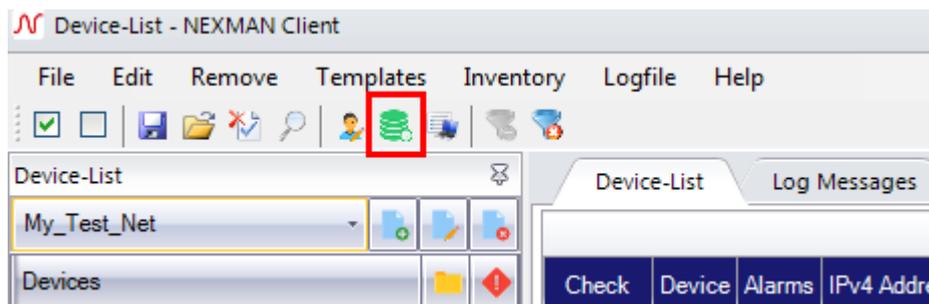
After clicking on the OK or Apply button the device is entered into the device list and most of the columns are marked with a "?" because the configuration of the device has not yet been read via automatic device polling:

Check	Device	Alarms	Redundancy	PoE	Power Consumption PoE	Input Voltage PoE	IPv4 Address	Active MAC Address	Name	Location	Description	Type	Mgmt Firmware Vers.	Mgmt Hardware Vers.	Voice VLAN	Def. VLAN	Uptime
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.20	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.19	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.18	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.17	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.16	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.15	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.14	?	?	?	?	-1	?				?
<input checked="" type="checkbox"/>	Unkn...			0	0		192.168.0.13	?	?	?	?	-1	?				?

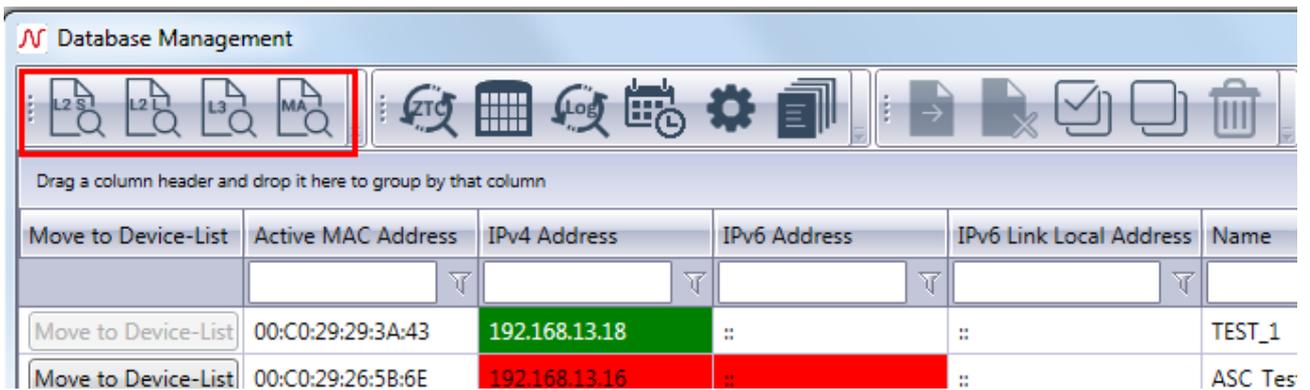
For more information regarding the automatic polling see chapter 14.2. *Automatic polling of Device-Lists.*

12.4. Database Management in Client/Controller-Version

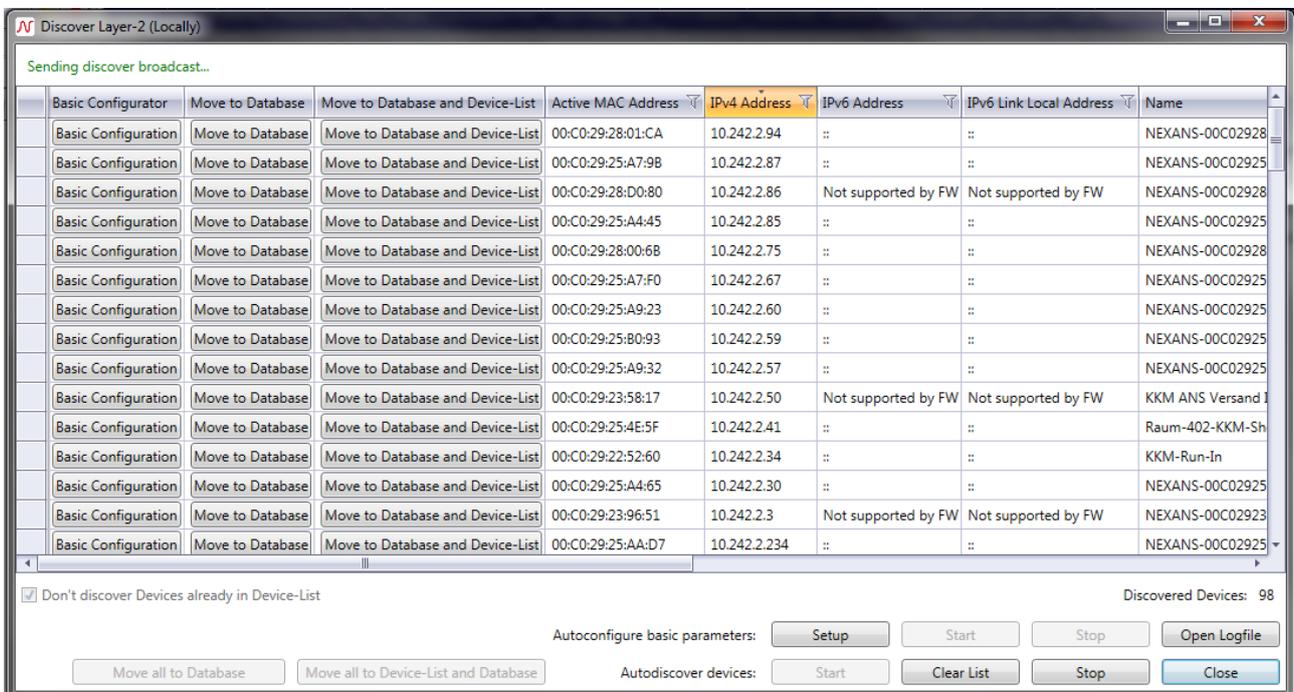
If you are using the Client/Controller-Version, all devices are handled by the controller and every device to be observed must be stored in the database. To do this open the **Database-Management** by clicking on the shortcut or using the **Edit** menu as admin-user.



On the first time entering the Database Management the database is empty. To add devices to the database the same functions as described in the chapter 12.3 *Adding Devices to Device-List* are available. The only difference is that you can start the Layer-2 Autodiscovery from server side or from client side (Locally). The basic configuration can only be done during local Autodiscovery.



Due to the fact that devices are not stored locally you can decide whether to move a discovered device to the database or to the database and to the currently opened device list on client side at once. Note, that no device can be moved to any device list without being stored in the database. Also every device can exist only once in the database and device list. However, a device still can be added to multiple device lists.

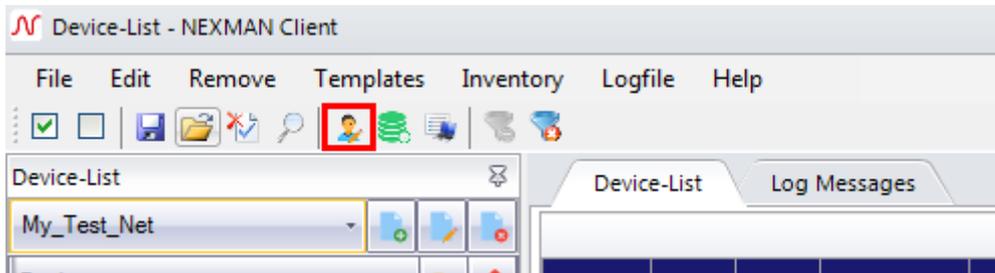


Move to Device-List	Active MAC Address	IPv4 Address	IPv6 Address	IPv6 Link Local Address	Name	Location	Description	Type	Mgmt FW	Mgmt HW
Move to Device-List	00:C0:29:0A:8E:20	192.168.13.26	2000:2000:13::26	fe80::2c0:29ff:fe0a:be20	ASC_Test_HW3_P16	Room P1.411	iGigaSwitch 1604 E+ SFP-4VI PRO3	40	HW3-F30-P16-INDUSTRIAL-V5.03hd	3
Move to Device-List	00:C0:29:25:D0:88	192.168.13.20	2000:2000:13::20	fe80::2c0:29ff:fe25:d08b	ASC_Test_HW3_P10	Room P1.411	iSwitch G 1043E+ SFP-3VI PRO3	36	HW3-F22-P10-INDUSTRIAL-V5.03he	3
Move to Device-List	00:C0:29:29:3A:43	192.168.13.17	::	::	ASC_Test_HW5_P07	Room P1.411	GigaSwitch V5 SFP-2VI 54VDC	74	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:26:3D:E1:MC	192.168.13.16	2000:2000:13::16	fe80::2c0:29ff:fe26:3de1	ASC_Test_HW3_P06_Cabel_Canal	Room P1.411	GigaSwitch V3 TP SFP-I 48V ES3	62	HW3-F21-P06-OFFICE-V6.01bn	3
Move to Device-List	00:C0:29:28:D1:04	192.168.13.15	2000:2000:13::15	fe80::2c0:29ff:fe28:d104	ASC_Test_HW3_P06_Desk	Room P1.411	GigaSwitch 641 Desk SFP-I ES3	70	HW3-F21-P06-OFFICE-V5.03he	3
Move to Device-List	00:C0:29:26:1E:C2	192.168.5.17	2000:2000:1::17	fe80::2c0:29ff:fe26:1ec2	AWR 10-Port Switch Linux	AWR Buero	iGigaSwitch 1002 E+ SFP-2VI PRO4	85	HW5-F46-P10-INDUSTRIAL-V6.01cr	5
Move to Device-List	00:C0:29:29:68:D6	192.168.0.97	2000:2000:1::97	fe80::2c0:29ff:fe29:68d6	Rack_HW5_P07	Rack	GigaSwitch V5 TP SFP-VI 54VDC	73	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:29:68:CF	192.168.0.96	2000:2000:1::96	fe80::2c0:29ff:fe29:68cf	Rack_HW5_P07	Rack	GigaSwitch V5 TP SFP-VI 54VDC	73	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:26:5D:86	192.168.0.95	2000:2000:1::95	fe80::2c0:29ff:fe26:5d86	Rack_HW5_P07	Rack	GigaSwitch V5 TP(PSE+) SFP-2VI 54VDC	72	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:26:5D:8E	192.168.0.94	2000:2000:1::94	fe80::2c0:29ff:fe26:5d8e	Rack_HW5_P07	Rack	GigaSwitch V5 TP(PSE+) SFP-2VI 54VDC	72	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:26:5D:81	192.168.0.93	2000:2000:1::93	fe80::2c0:29ff:fe26:5d81	Rack_HW5_P07	Rack	GigaSwitch V5 TP(PSE+) SFP-2VI 54VDC	72	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:29:68:B4	192.168.0.92	2000:2000:1::92	fe80::2c0:29ff:fe29:68b4	Rack_HW5_P07	Rack	GigaSwitch V5 TP SFP-VI 54VDC	73	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:26:5D:87	192.168.0.91	2000:2000:1::91	fe80::2c0:29ff:fe26:5d87	Rack_HW5_P07	Rack	GigaSwitch V5 TP(PSE+) SFP-2VI 54VDC	72	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:29:68:AD	192.168.0.90	2000:2000:1::90	fe80::2c0:29ff:fe29:68ad	Rack_HW5_P07	Rack	GigaSwitch V5 TP SFP-VI 54VDC	73	HW5-F40-P07-OFFICE-V6.01bs	5
Move to Device-List	00:C0:29:25:AA:D7	10.242.2.234	::	::	NEXANS-00C02925AAAD7	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:AC:5A	10.242.2.232	::	::	NEXANS-00C02925AC5A	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:A8:1C	10.242.2.223	::	::	NEXANS-00C02925A81C	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:28:0A:89	10.242.2.222	::	::	NEXANS-00C029280A89	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:80:8E	10.242.2.221	::	::	NEXANS-00C02925808E	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:A4:E5	10.242.2.220	::	::	NEXANS-00C02925A4E5	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:A7:79	10.242.2.219	::	::	NEXANS-00C02925A779	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:25:80:79	10.242.2.208	::	::	NEXANS-00C029258079	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:28:03:F2	10.242.2.207	::	::	NEXANS-00C0292803F2	not defined	GigaSwitch V3 TP SFP-I 48/54VDC ES3	62	HW3/ENHANCED/SECURITY/V4.14U	3
Move to Device-List	00:C0:29:26:13:2E	10.242.2.203	::	::	NEXANS-00C02926132E	not defined	GigaSwitch V3 TP SFP-I 230VAC ES3	62	HW3/ENHANCED/SECURITY/V4.10C	3

12.5. User Management in Client/Controller-Version

12.5.1. Create a new user

To create, modify or delete a user, open the **User-Management** by clicking on the shortcut or using the **Edit** menu. You must be logged in as an administrator to do so.



Click on the **Add User** button to create a new user.

Actions	First Name	Last Name	Username	Date Created	Created By	Roles
>		Administrator	admin	5/14/2018 8:14:0	system	Administrator
	Test	Test	test	9/18/2018 1:39:2	admin	User

Enter the user's credentials and assign the necessary roles. Read more about roles in chapter 12.5.2 *User roles*. Afterwards assign any device list the user should be allowed to work with.

Also, you must assign the Device-Editor pages the user should be able to edit. Click **Save** to accept your changes.

At least assign the ports the user should be able to configure. Unassigned ports will not be visible to the user in the Device-Editor.

The administrator is allowed to modify every user. He is also allowed to delete every user except his own. Additionally, the administrator can change any user's password.

There are no restrictions on Device-Editor pages or ports to administrator users, even if none are assigned to that user.

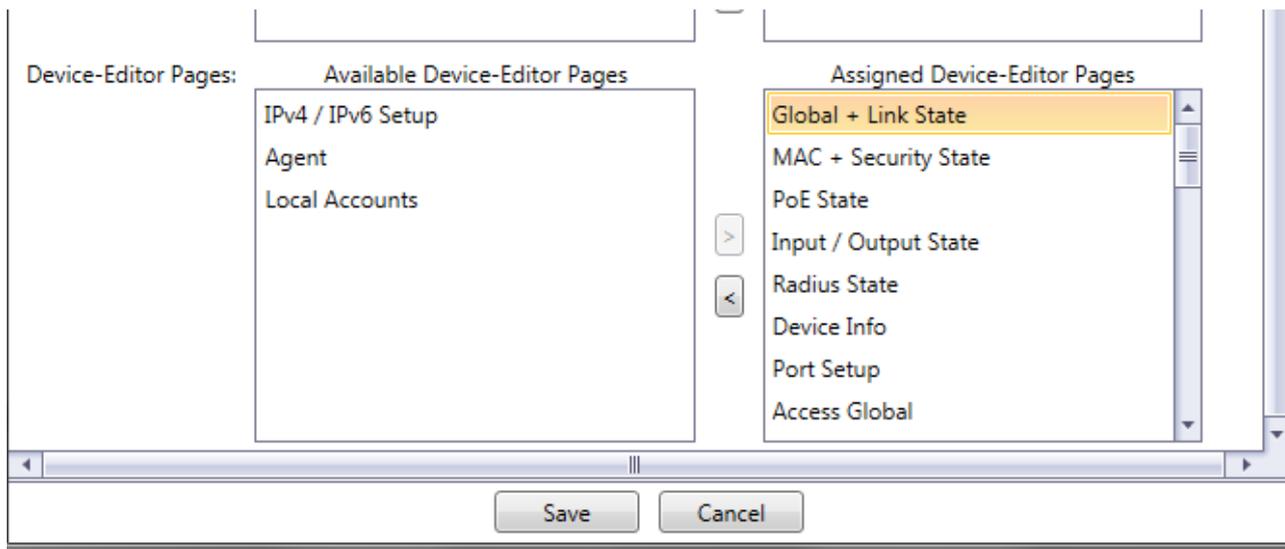
12.5.2. User roles

There are two different user roles which can be assigned to a user:

- Administrator: Has full access to the user- and database-management. Can add, modify and delete device lists. Can edit all taps of the device editor.
- User: Configure all devices that are included in the device lists, assigned to this user. Editable Device Editor pages must be assigned.

12.5.3. User Access Rights

To be able to edit device parameter the user must have access to the corresponding page in the Device Editor. The pages have to be assigned to the user by the administrator inside the Edit User window.



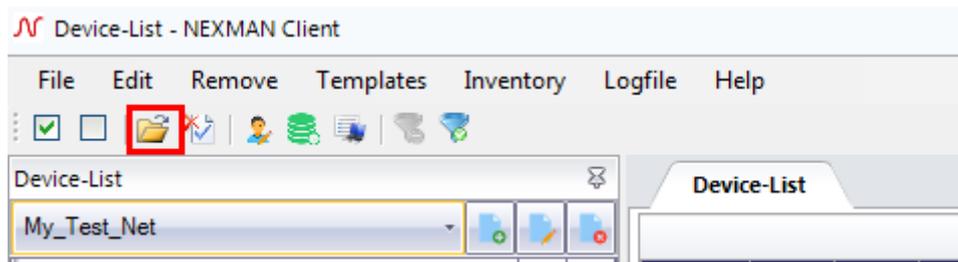
The user has read only access to any unassigned Device-Editor page.

The accessible ports have to be assigned to the user, too. Every unassigned port is not visible to the user and thereby cannot be edited.



12.6. Import Device-List from Stand-Alone version into Controller database

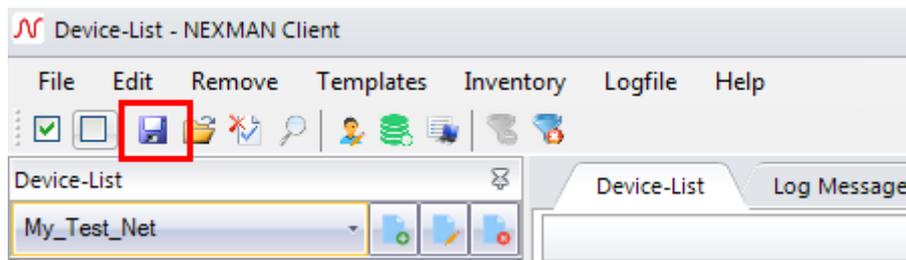
To import a Device-List stored as XML file to the database click on **Import Device-List into database** shortcut or use the **File** menu.



Choose the file to be imported. A new device list will be created named after the file name and every category and device will be added. If a device is unknown, it will be added to the database, too.

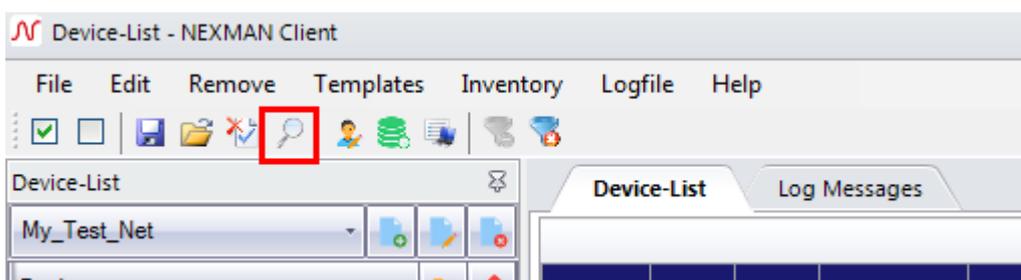
12.7. Export Device-List from Controller database to Stand-Alone version

To export a Device-List from the Controller database to a XML file that can be opened with the Stand-Alone version click on **Save Device-List as XML**.



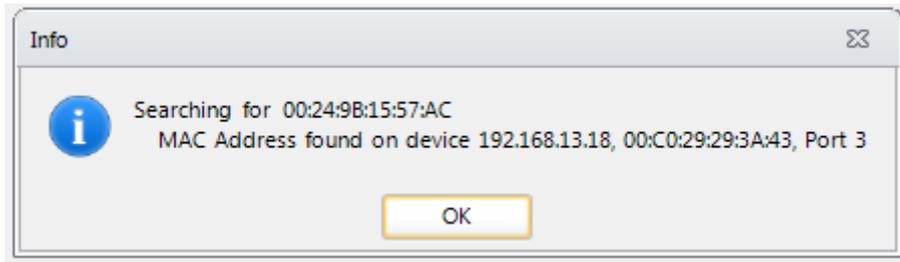
After choosing a file name the selected Device-List will be saved as XML file and can be opened by the Stand-Alone version.

12.8. Searching for MAC Addresses



With clicking **Search MAC Address in current Device-List** one or more MAC Addresses can be searched inside the neighbor tables of the devices inside the current Device-List.

When successful, a message box shows on which device and port the MAC Address can be found.



12.9. Firmware Update for Devices with Firmware V1.xx / V2.xx

If an older firmware version 1.xx or 2.xx is installed in the device, the first step is to update the firmware.

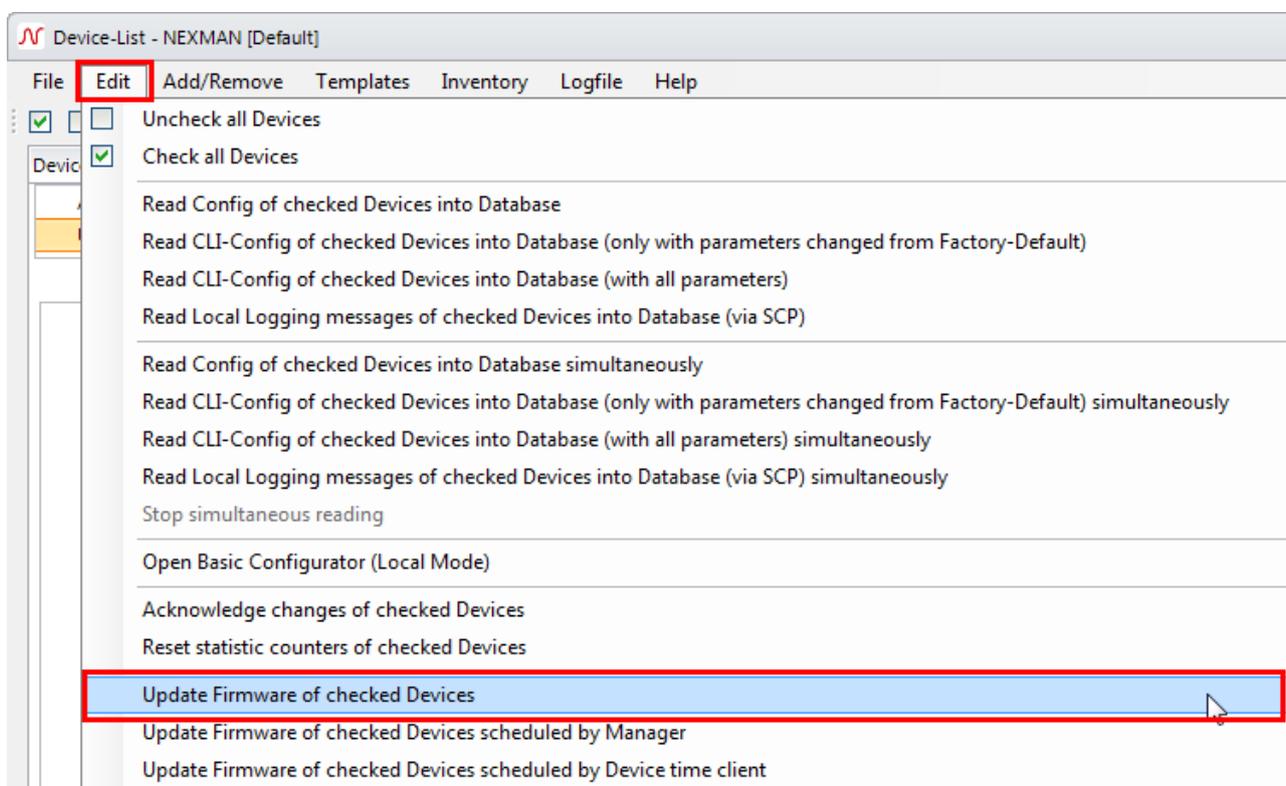
Note:

Devices with firmware version V1.xx or V2.xx are displayed in the NEXMAN Device-List as an **Unknown** Device, because firmware V1.xx and V2.xx does not deliver a status information. For this reason, in the Alarms column the device is additionally defined as **Ping Only**.

Important note:

We **urgently** recommend reading the **Management Module and Firmware Versions** chapter in the **Nexans Switch Management manual** and in particular the included remarks on the different firmware images prior to performing a firmware update.

To start the update the devices must be selected in the **Check** column and the menu option **Edit > Update Firmware of checked Devices** selected:



After selecting the appropriate firmware file the device is automatically updated.

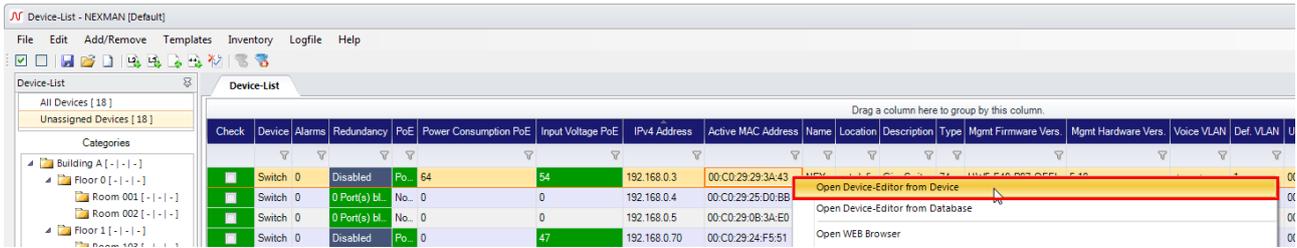
Important:

All device settings entered in firmware V1.xx or V2.xx will be retained during the update.

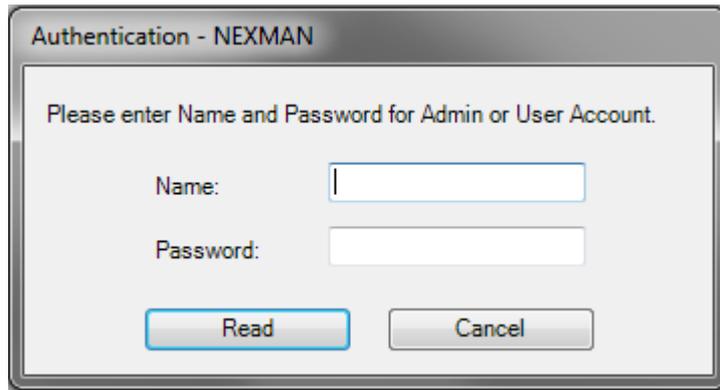
12.10. Starting the Device Editor and Configuring the Device

A double-click on the device in the device list will start the device editor.

Alternatively, this can also be done by right-clicking onto the device and subsequently selecting the **Open Device-Editor from Device** menu option:

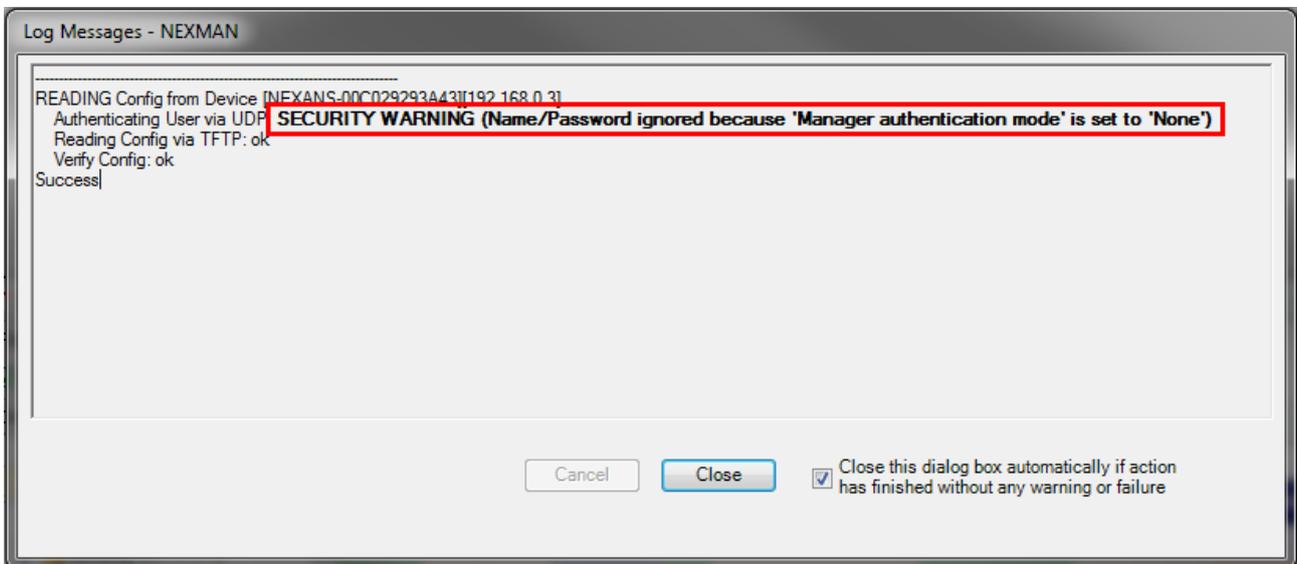


The editor first verifies the name and password in the Authentication dialog box for accessing the device (factory default is "admin" and "nexans"):

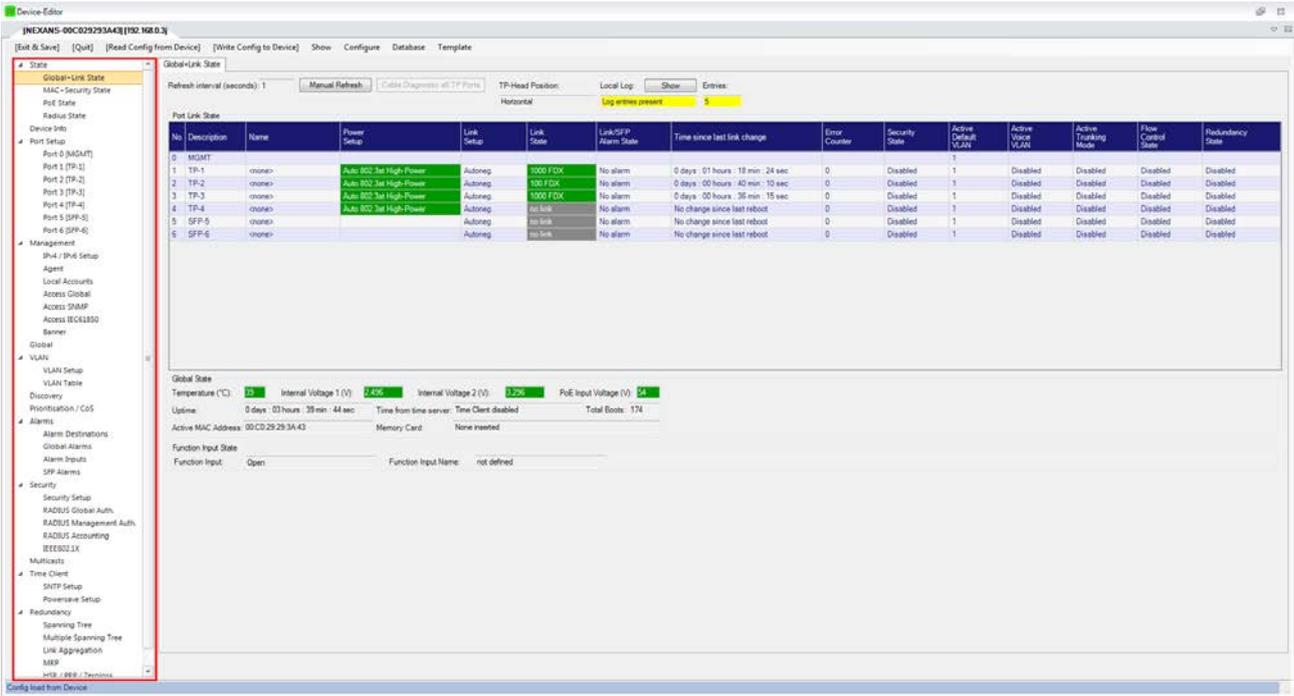


NOTE:

If the **Manager authentication mode** is set to **none** in the device, the name and password need not be entered, because the device will not perform any authentication. However, in this case a warning message is displayed in the log window informing the user on the unsecure setting of the device:



If name and password are correctly entered, the device editor state page is displayed:



On the state pages (Tabs "Global+Link State", "MAC+Security State" and "PoE State") always the current state of the device is displayed, independent of whether changes have been made in the other tabs (Agent, Access, Global, ...) and not yet transferred into the device.

Now the configuration settings of the device can be edited via the tabs (in the red box in the above figure) and transferred to the device via the **[Write Config to Device]** menu button.

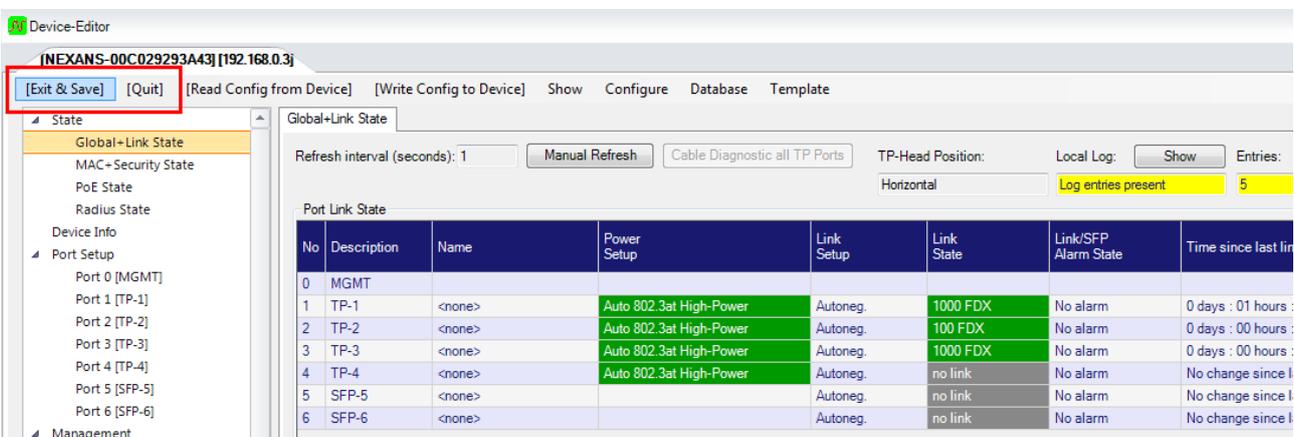
IMPORTANT:

All changes will be immediately applied by the device without rebooting.

NOTE:

The Management Module manual contains a detailed description of the device editor parameters. This manual can be opened via the help menu **Help → Manuals → Switch Firmware and Parameters**.

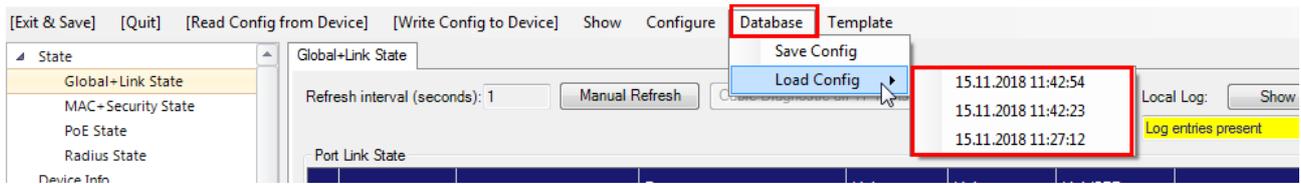
After completion of the configuration you can quit the device editor via the **[Exit & Save]** menu button. The current configuration is saved in the data base. You can leave the Device Editor without saving the configuration by pressing the **[Quit]** button:



NOTE:

Configurations already stored in the database will not be overwritten, but shifted to the History database. In

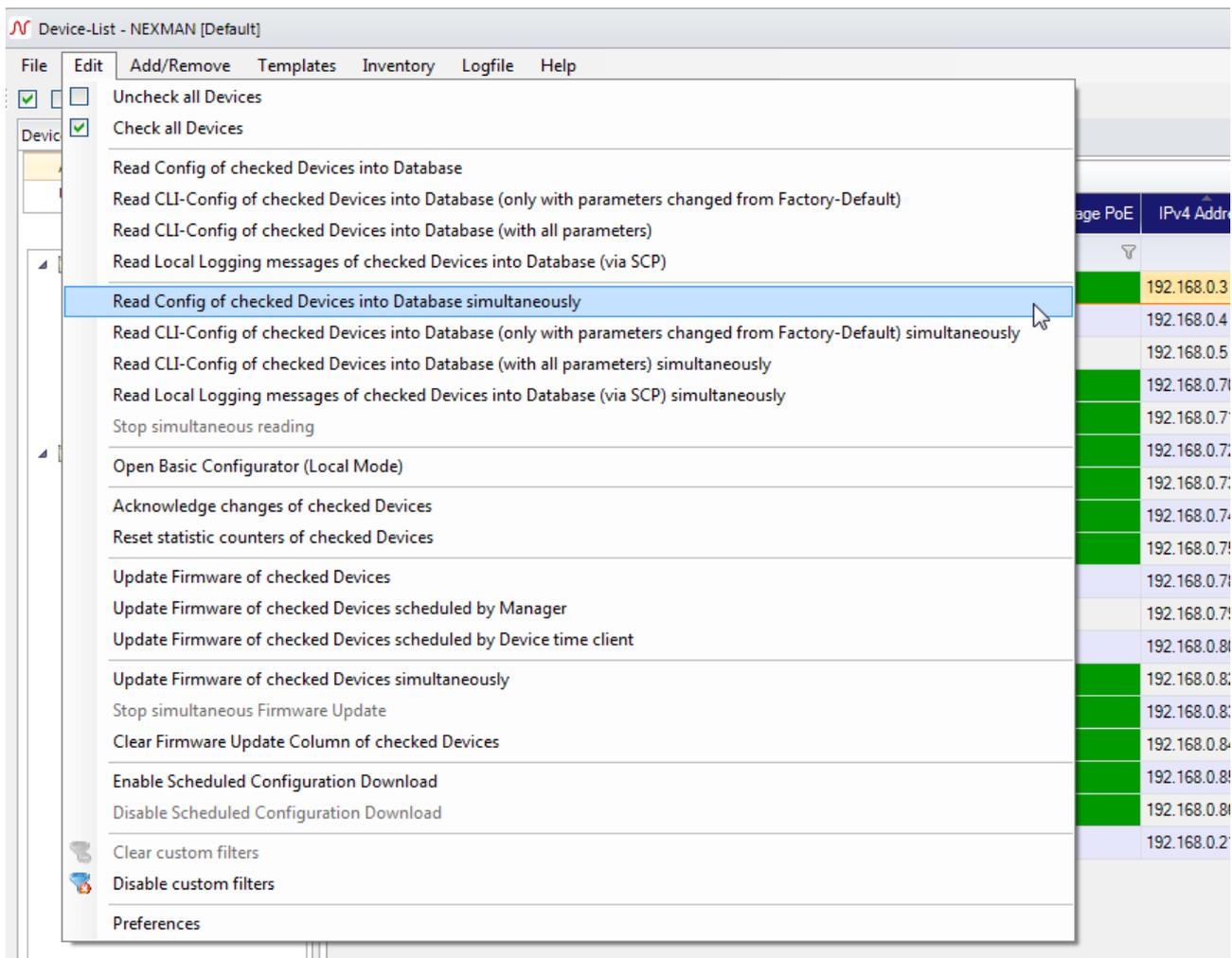
the device editor these can then be loaded into the editor via the **Database > Load Config** menu and written back into the device, if necessary:



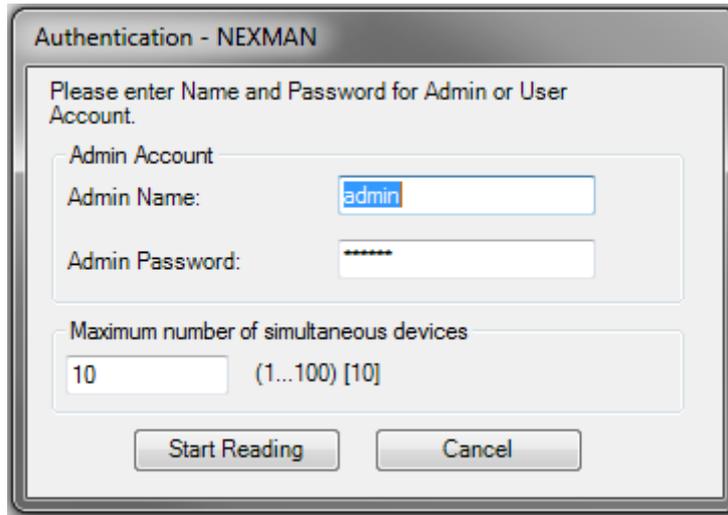
12.11. Configuration of multiple devices

12.11.1. Reading configuration of multiple devices

It is possible to read the configuration of multiple devices simultaneously. Start this action with **Edit > Read Config of checked Devices into Database simultaneously**.



Next, enter the user credentials and the maximum number of simultaneous devices.



After clicking start, a new column “File Transfer” will become visible, showing the progress of each device.

Device-List - NEXMAN [Default]

File Edit Add/Remove Templates Inventory Logfile Help

Device-List

All Devices [18]
Unassigned Devices [2]

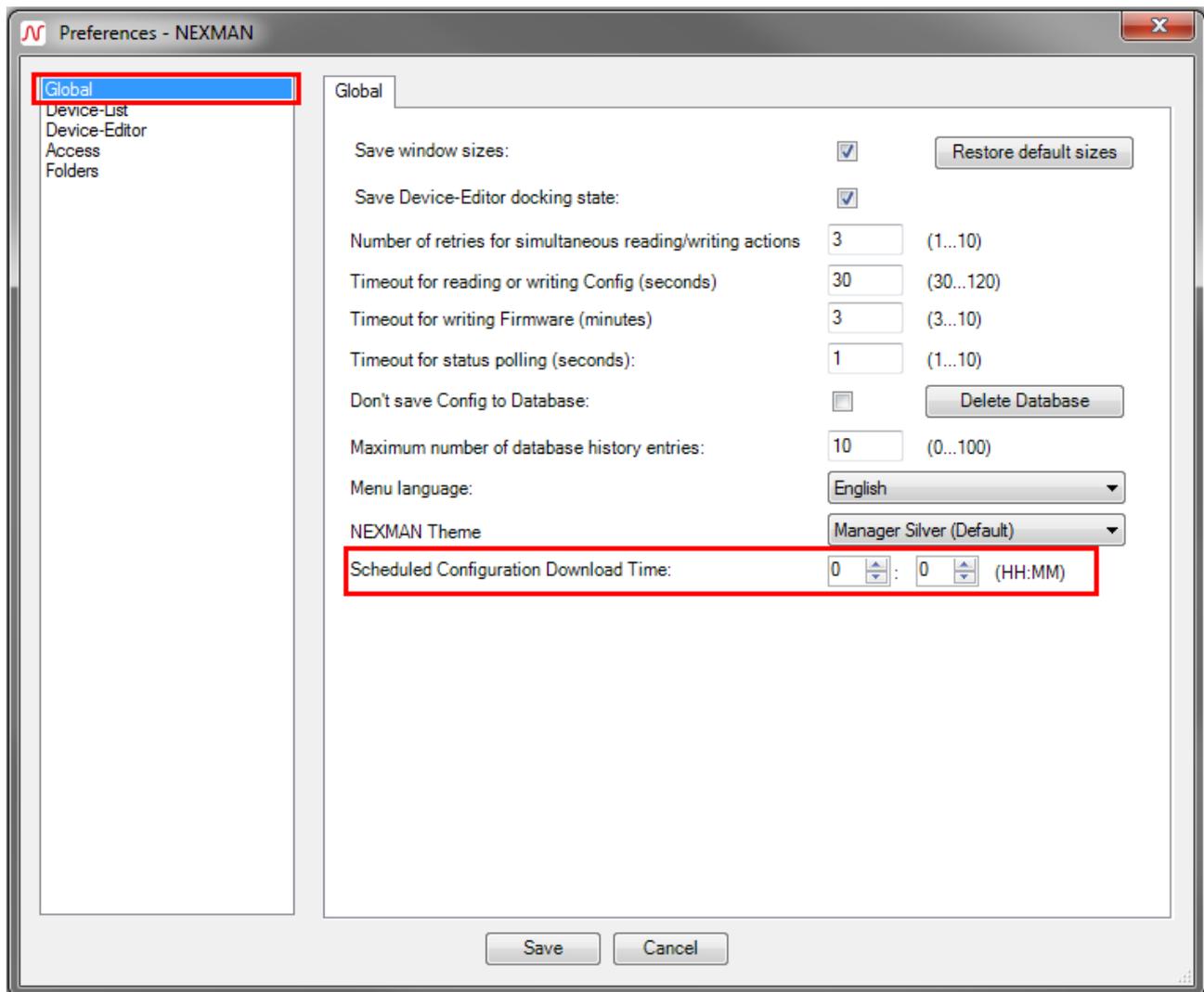
Categories

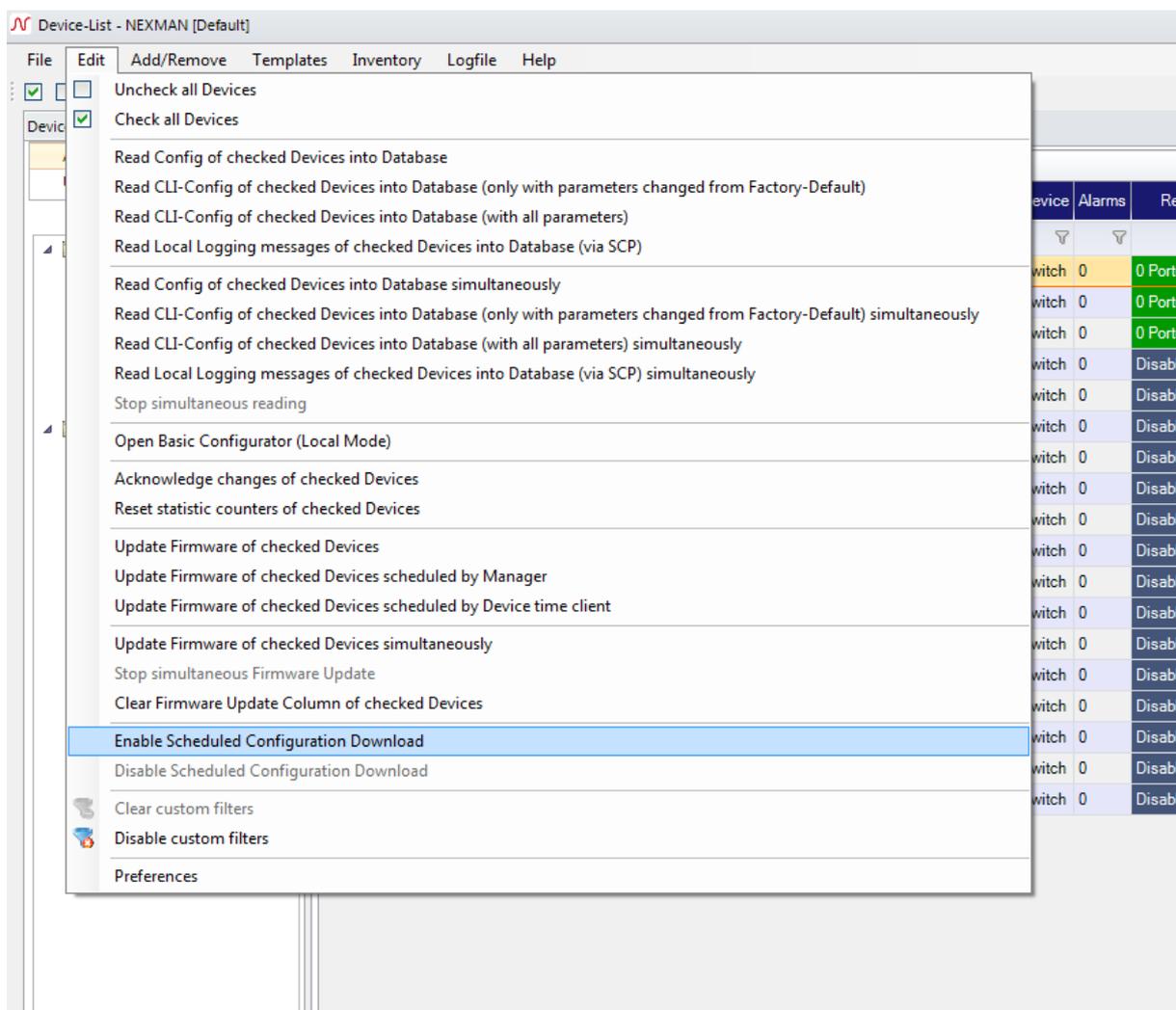
- Building A [- | 11 | -]
 - Floor 0 [2 | 7 | -]
 - Room 001 [2 | - | -]
 - Room 002 [3 | - | -]
 - Floor 1 [- | 4 | -]
 - Room 103 [2 | - | -]
 - Room 104 [2 | - | -]
- Building B [- | 5 | -]
 - Floor 0 [1 | 2 | -]
 - New Category [1 | - ...]
 - Floor 1 [1 | - | -]
 - New Category [- | - ...]
 - Floor 2 [1 | 2 | -]
 - New Category [1 | - ...]

Check	File Transfer	Device	Alarms	Redundancy
<input type="checkbox"/>	Data saved: 15.11.2018 15:23:21	Switch	0	0 Port(s) blocking
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:30	Switch	0	0 Port(s) blocking
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:46	Switch	0	0 Port(s) blocking
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:46	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:42	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:37	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:43	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:34	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:39	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:37	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:45	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:38	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:38	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:36	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:36	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:36	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:36	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:36	Switch	0	Disabled
<input checked="" type="checkbox"/>	Data saved: 15.11.2018 15:23:43	Switch	0	Disabled

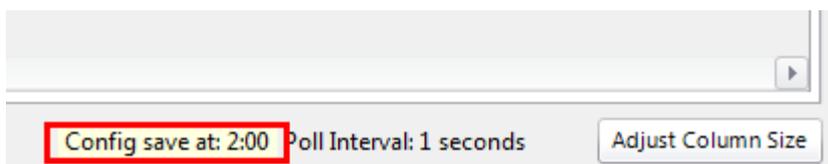
12.11.2. Enable Scheduled Configuration Download

If you want to read the configuration of your devices frequently, you can set up a time via the [Edit > Preferences](#) menu and navigate to the page “Global”.



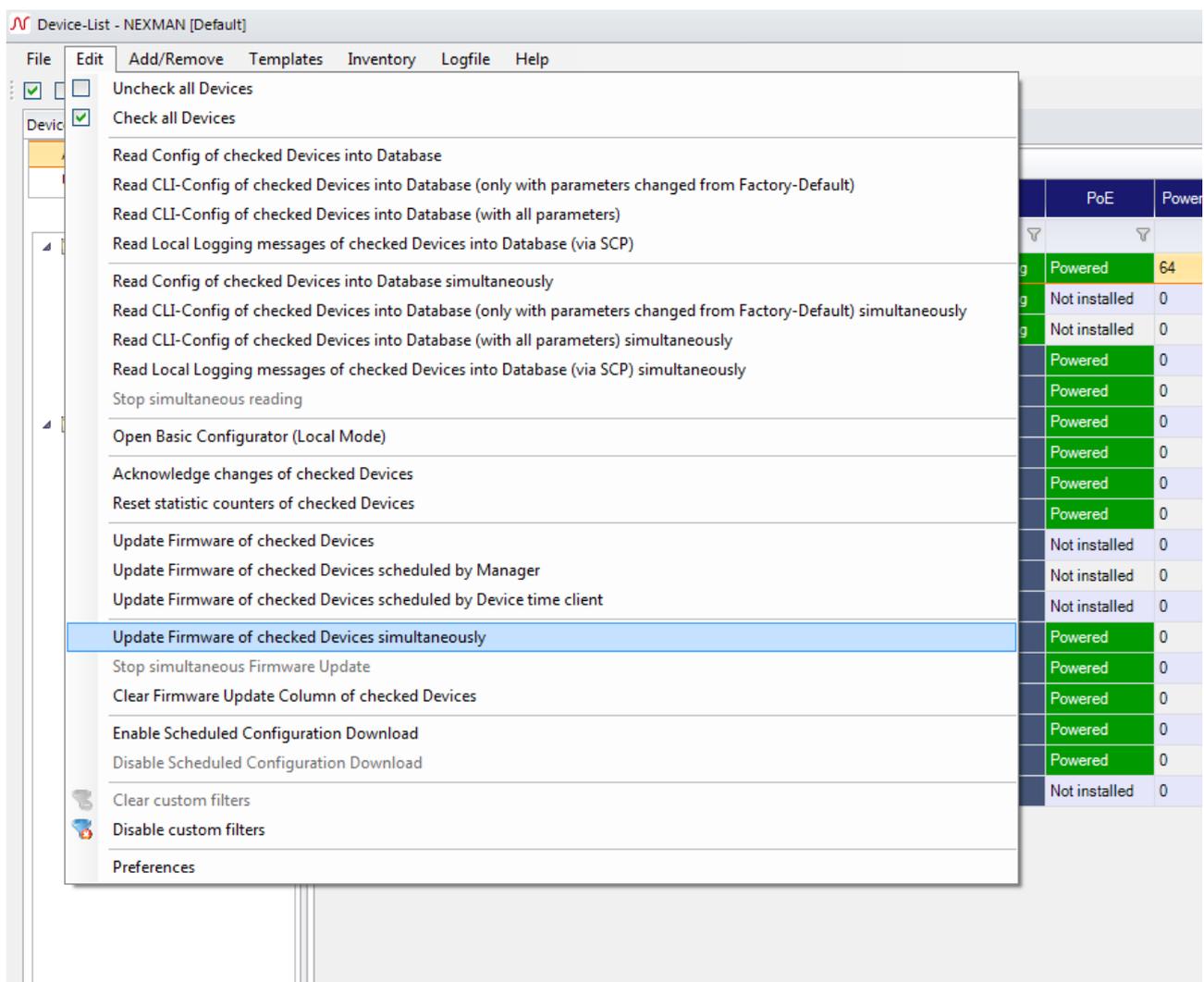


Via **Edit > Enable Scheduled Configuration Download** you can start the process. Afterwards the configuration of each device in the current device list will be read into the database at the given time each day. A notification inside the status bar shows whether the scheduled download is activated or not.



12.11.3. Update firmware of multiple devices

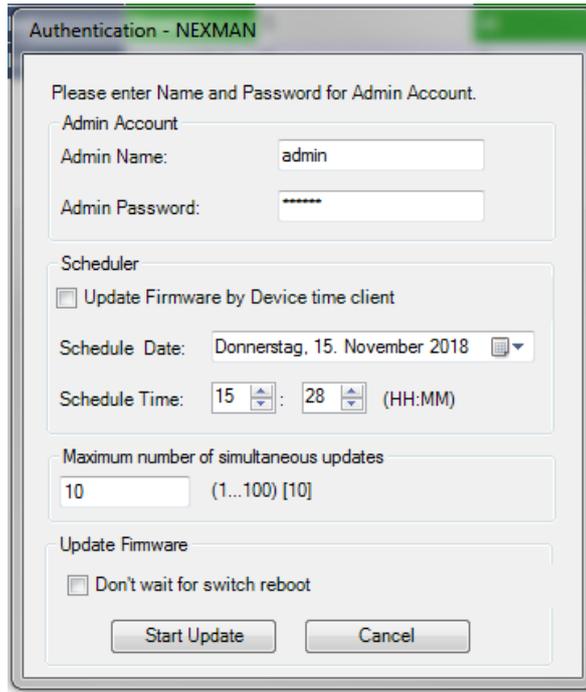
To update the firmware of multiple devices simultaneously go to **Edit > Update Firmware of checked Devices simultaneously**.



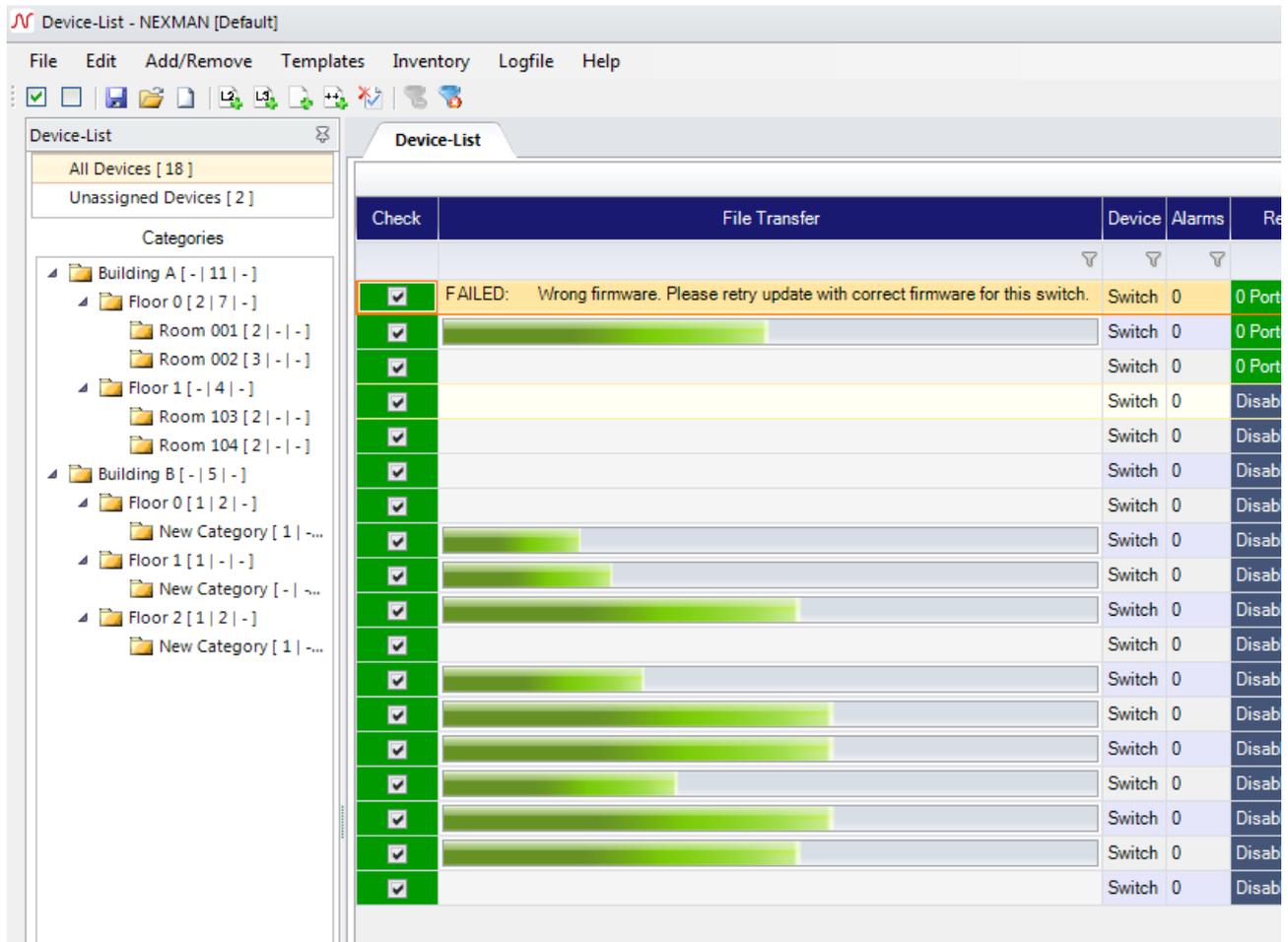
Select the firmware image you want to use. Afterwards you have to enter the user credentials and the maximum number of simultaneous updates.

If you like, you can set up a scheduler to have the update being processed at a specific time. Thereby the image file will be transferred to the switch and the update will start at the given time.

Since the switch has to reboot to finish the update you can choose whether you want to wait until the switch has rebooted or not. If you do not want to wait, the update process will be marked as finished right after the update file has been transferred to the switch. To ensure that every is able to receive the complet firmware image you should use a star topology. Otherwise a connection might get lost when a switch is rebooting.

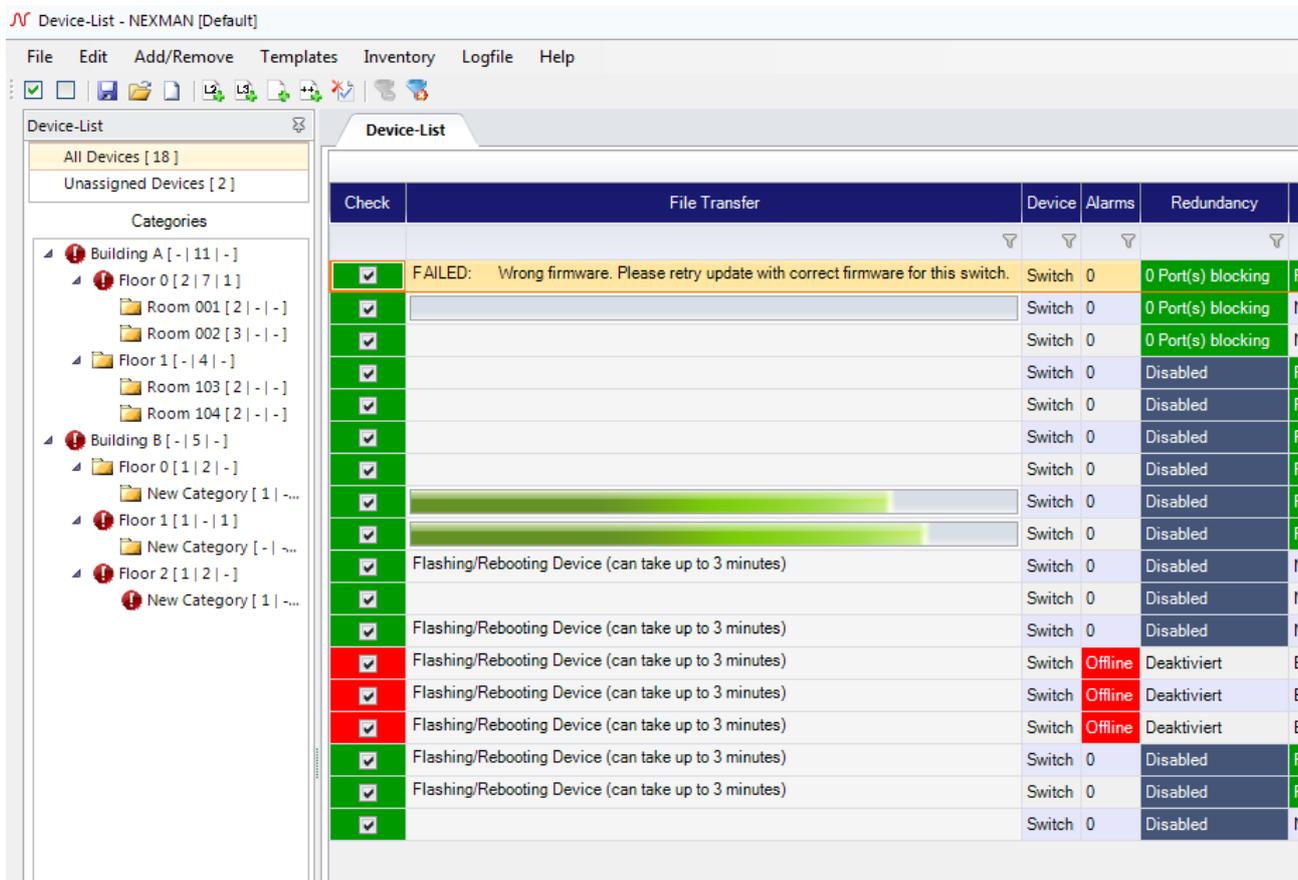


The update process is shown in the „File Transfer“ column.



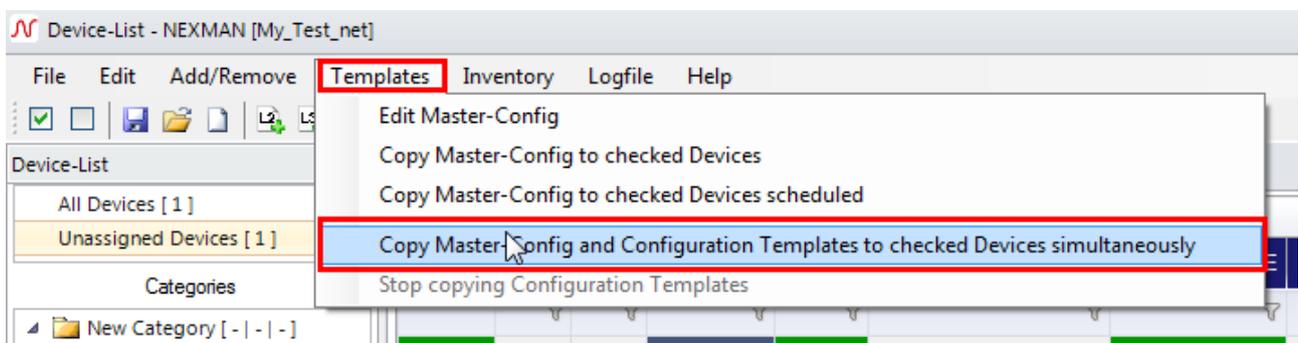
If you have decided to wait until the switch has rebooted, a message is shown while the switch is flashing and rebooting. The flashing process will be also underlined with a blinking check column. While rebooting the switch is marked as "offline".

When the update has finished a status message is shown in the same column.



12.11.4. Copy Configuration Templates to checked Devices

By clicking on the **Templates > Copy Configuration Templates to checked Devices** menu you can copy configuration templates like a master configuration to multiple devices simultaneously.



Enter the user credentials and select a file to be copied to all checked devices. Change the number of maximum simultaneous actions if needed and click "Copy" to start. The status of each process is shown in the "File Transfer" column.

Copy Configuration Templates - NEXMAN

Please enter Name and Password for Admin Account.

Admin Account

Admin Name:

Admin Password:

Select Configuration Files

Master Config:	<input type="button" value="Select"/>	<input type="button" value="Deselect"/>	<input type="text"/>	
Script File:	<input type="button" value="Select"/>	<input type="button" value="Deselect"/>	<input type="text"/>	<input type="button" value="Edit"/>
Customer Default CLI Config:	<input type="button" value="Select"/>	<input type="button" value="Deselect"/>	<input type="text"/>	<input type="button" value="Edit"/>
Customer Reboot CLI Config:	<input type="button" value="Select"/>	<input type="button" value="Deselect"/>	<input type="text"/>	<input type="button" value="Edit"/>
Running CLI Config:	<input type="button" value="Select"/>	<input type="button" value="Deselect"/>	<input type="text"/>	<input type="button" value="Edit"/>

Copy Running Config without reset to factory default
Leave empty to keep current configuration

Maximum number of simultaneous updates
 (1...100) [10]

13. Basic Configurator

13.1. Functional overview

Nexans Basic Configurator is part of Nexans Device Manager (NEXMAN).

It provides the basic configuration of the switch and includes the following parameters:

- Switch description (name, location, contact)
- IP parameters (DHCP, IP address, netmask, gateway)
- Trunk uplink parameters (trunk port, mgmt VLAN-ID)

Note: By factory default the switch is set to DHCP and thus can receive its basic configuration directly from a DHCP server. Detailed information on the automatic configuration via BOOTP/DHCP can be found in the Firmware Manual.

The Basic Configurator supports two different operating modes:

- MAC Address Mode

The (MAC Address Mode) has been designed for the centralized configuration of the switch parameters within the NEXMAN 'Autodiscover Devices on local segments (Layer-2)' feature and consequently can only be called from NEXMAN.

- Local Mode

The (Local Mode) has been designed for the local on-site configuration of the switch parameters. This requires the PC to be directly connected via the network cable with the first Twisted Pair port (TP1) of the switch.

After completion of the basic settings via the Basic Configurator any further configuration can be executed via the Device-List of the Nexans Device Manager (NEXMAN).

13.3. Basic Configurator in (Local Mode)

13.3.1. Functioning Principle (Local Mode)

The (Local Mode) has been designed for the local on-site configuration of the switch parameters. This requires the PC to be directly connected via the network cable with the first Twisted Pair port (TP1) of the switch. And the Admin Name, Admin Password and the VLANs need to be set to Factory Default.

Any parameters which are written via the **Write Setup to Device** button into the switch will be immediately activated. There is no need to subsequently reboot the switch.

IMPORTANT NOTE:

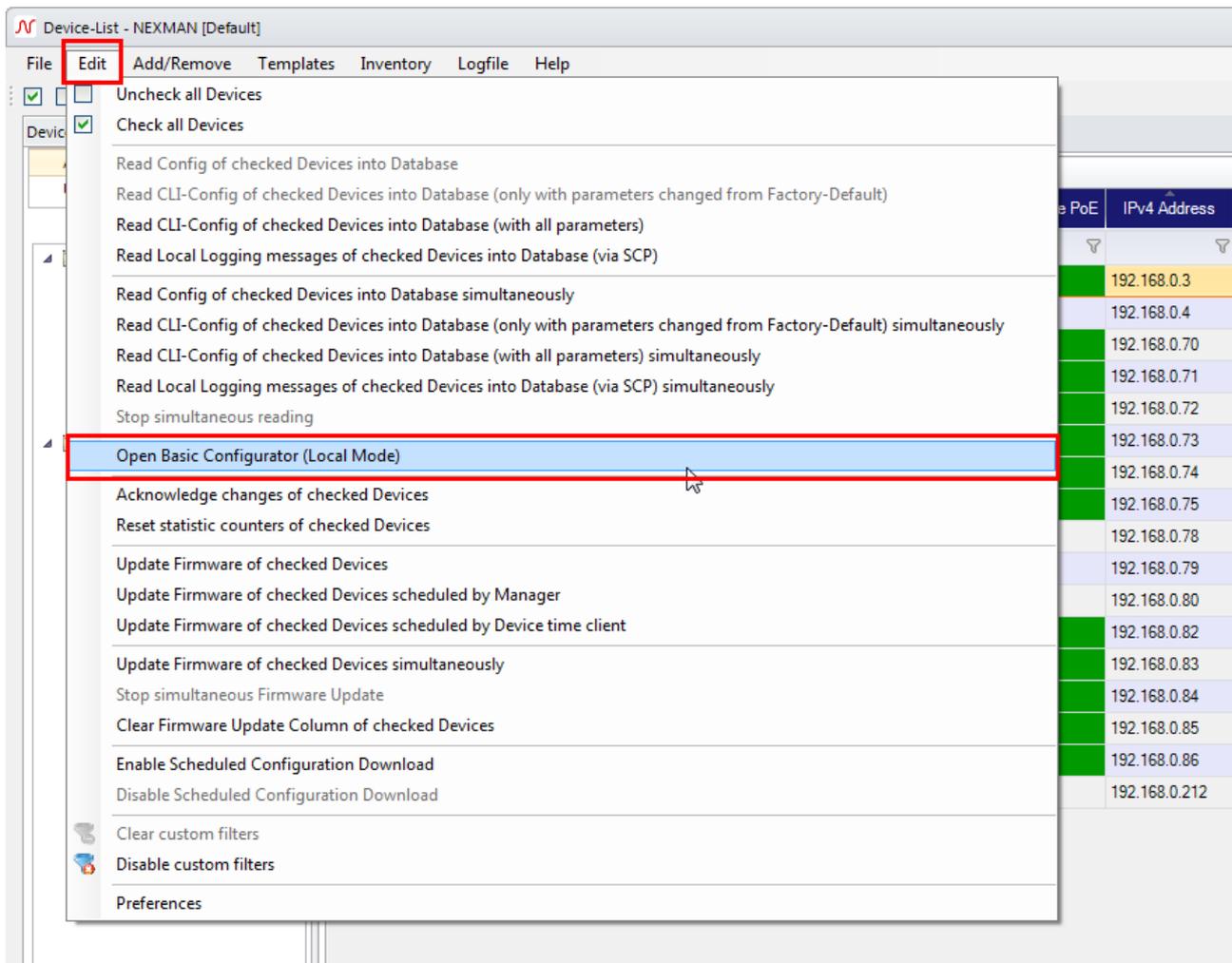
If the switch was booted (via the configuration switch) using the fixed IP address 172.23.44.111, the switch will answer to the Basic Configurator (Local Mode) queries on all switch ports (also on the Uplink Port).

Booting the switch using a fixed IP address should thus be avoided and is practicable only in exceptional cases (e. g. after modification of the VLAN settings).

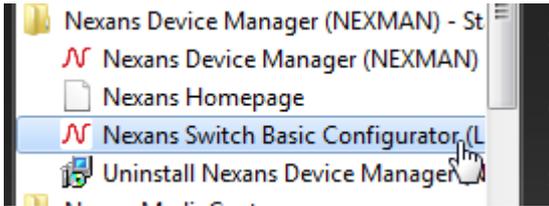
13.3.2. Starting the Basic Configurator (Local Mode)

Starting the Basic Configurator in (Local Mode) can be performed in two ways:

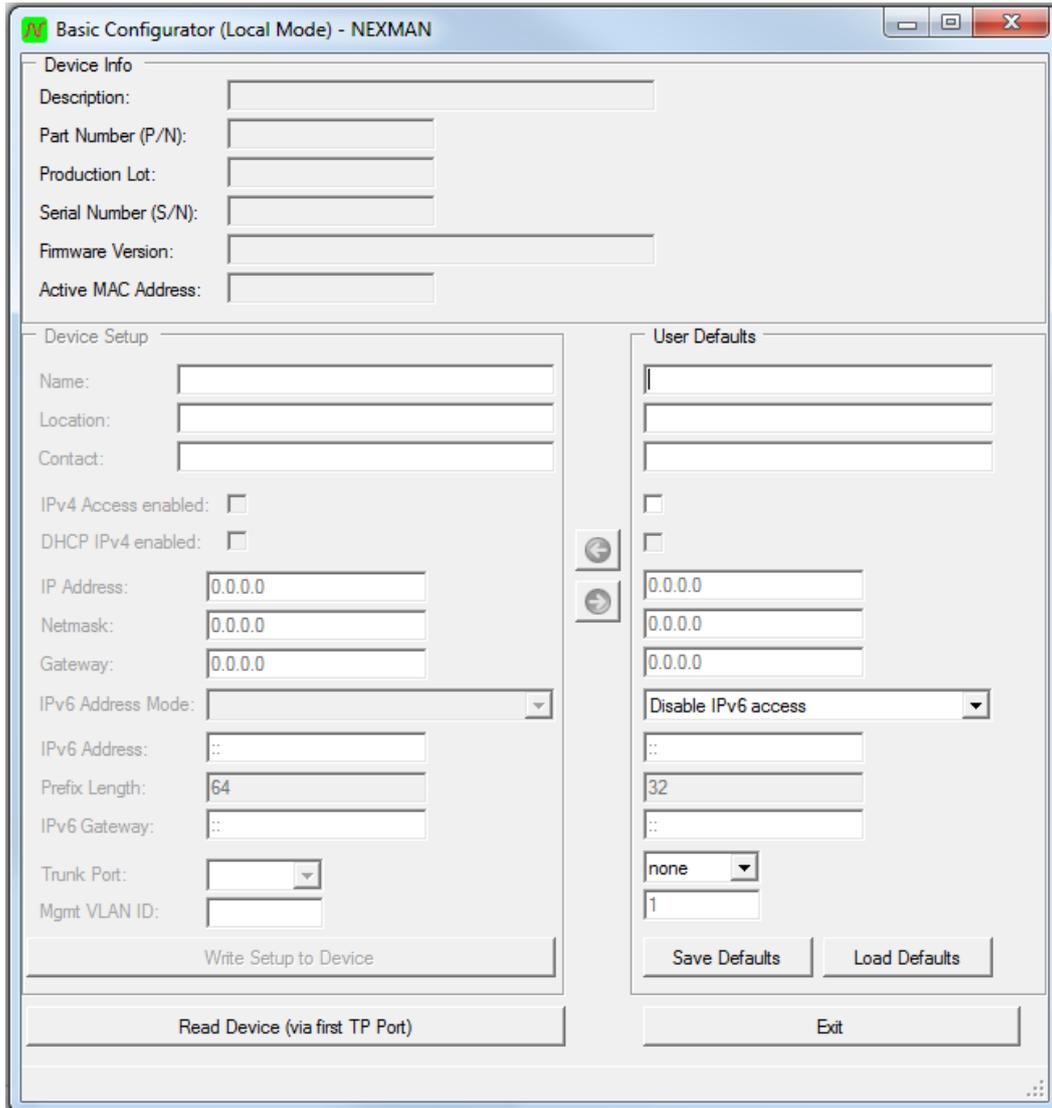
- Within NEXMAN through menu **Edit > Open Basic Configurator (Local Mode)**:



- Via the Windows start menu:



Upon the first start of the (Local Mode) an empty configuration page is displayed:



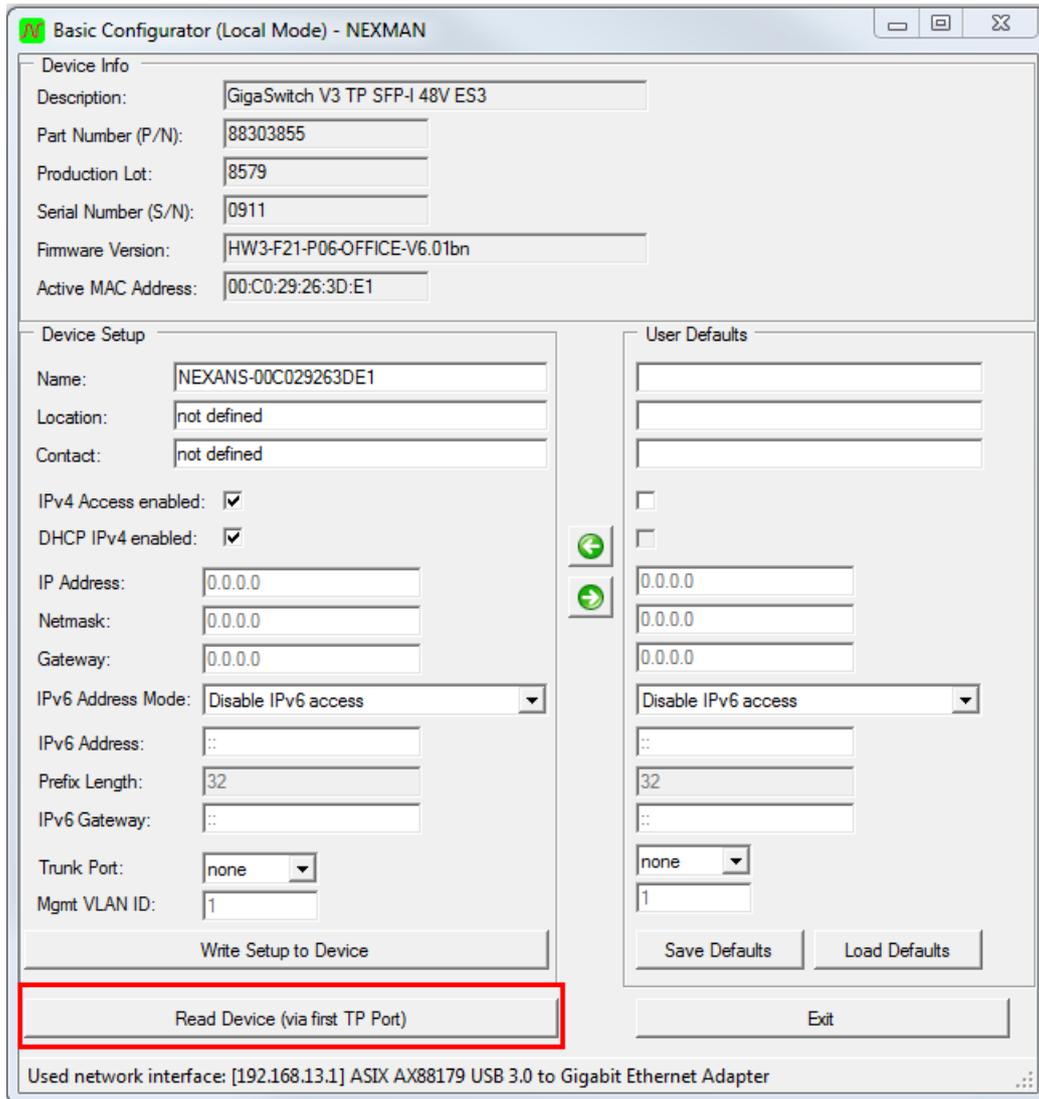
13.3.3. Reading the Switch Configuration (Local Mode)

In order to configure a switch, the currently installed configuration needs to be read first.

To do so the following requirements must be fulfilled:

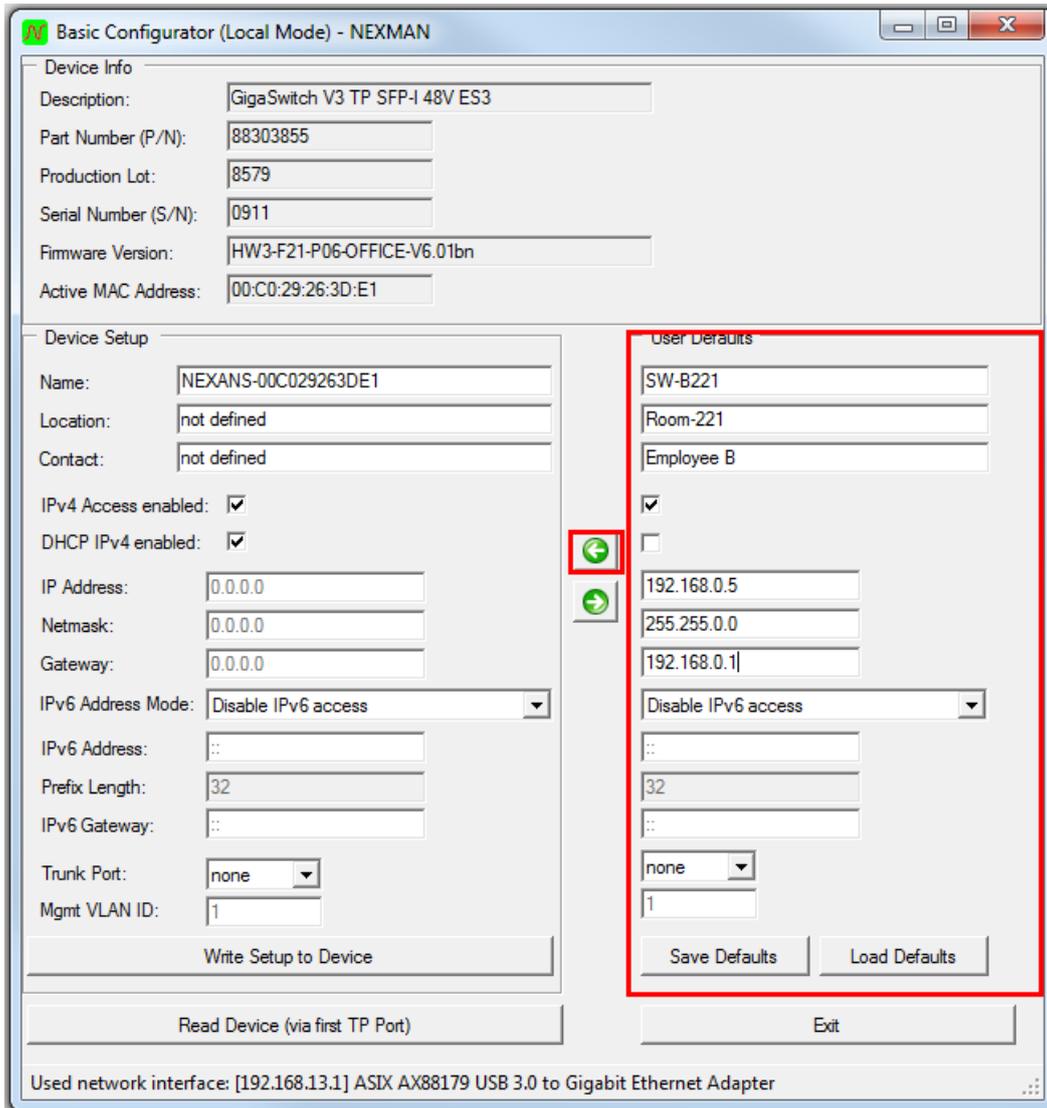
- The PC needs to be connected to the first Twisted Pair Port (TP1) of the switch.
- The switch VLANs ID need to be set to Factory Default.

To read the switch, click the **Read Device (via first TP Port)** button:



If the configuration has been correctly read, the respective values will be displayed in the **Device Info** and **Device Setup** fields and can be modified. The data in the **Device Info** window is Read-Only and meant for your information only.

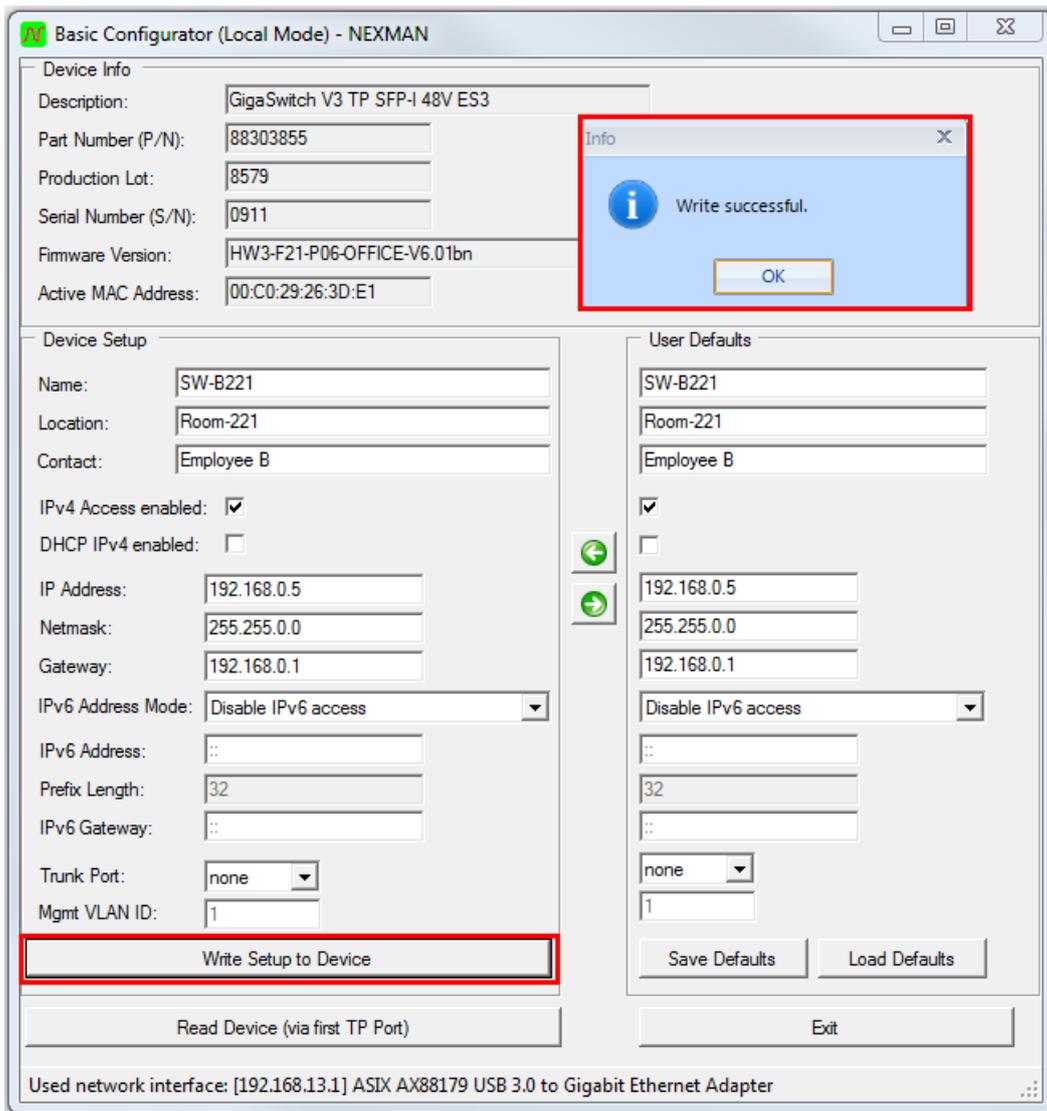
If multiple switches shall receive a similar configuration, a general basic setting can be defined in the **User Defaults** field and copied via the  button into the **Device Setup** field. Via the **Save Defaults** or **Load Defaults** buttons any template can be saved to or reloaded from the pc file system.



13.3.4. Writing the Switch Configuration (Local Mode)

In order to write the configuration after successful reading and modification back into the switch the admin name and the admin password must be set to Factory Default (name = admin, password = nexans). This restriction is a safety feature in order to prevent installed switches, which have been assigned a customer-specific password, from being modified by the Basic Configurator.

After entry of the desired parameters a click on the **Write Setup to Device** button will transfer the configuration into the switch. The configuration will take immediately effect without rebooting:



A message in the left lower corner informs about the successful completion of the write operation.

After completion of the basic settings of the switch via the Basic Configurator any further configuration can be executed using Nexans Switch Manager.

13.4. General Features

13.4.1. Configuring the Trunk Port and the Mgmt VLAN ID

If a firmware release V3.30 or higher is installed on the respective device, the Management VLAN-ID and the Trunk Port can be configured, too. If a device with an older V3 firmware release is read, the two 'Trunk Port' and 'Mgmt VLAN ID' input fields are inactive.

When writing the device setup two different cases are to be considered:

- Trunk Port = none
- Trunk Port = Port x

Trunk Port = none:



Trunk Port	none
Mgmt VLAN ID	1

If Trunk Port is set to **none**, the VLANs of the device will be set to **Factory Default**. That means that trunking is disabled on ALL ports and the 'Default VLAN ID' is set to 1 (including Management Interface).

Trunk Port = Port x:



Trunk Port	Port 5
Mgmt VLAN ID	112

If a port number has been selected for Trunk Port (normally the desired Uplink Port), the Trunking Mode for this is set to 'IEEE802.1Q Tagging'. Moreover, the Management Interface is set to the VLAN-ID indicated in the 'Mgmt VLAN ID' field.

Important:

Only the packets of the Management Interface are tagged with the configured 'Mgmt VLAN ID' to the uplink. This will ensure that at least the Management Interface can be reached via a tagged VLAN via Trunk Port. After writing the configuration using the **Write Setup to Device** button the Management Interface can only be reached via the configured 'Mgmt VLAN ID' and via the configured 'Trunk Port'.

Note:

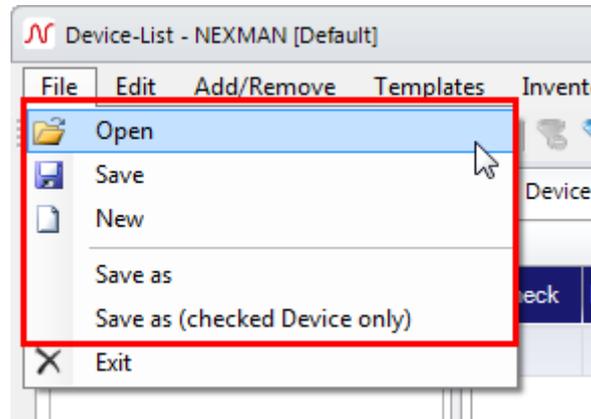
The 'Default VLAN-ID' of all Ethernet ports (including Uplink Port) is principally set to '1'. This means that the data packets of all user ports are forwarded untagged to the uplink and thus all users are located in the Default VLAN. Any configuration, if necessary, of the user ports with other VLAN-IDs can subsequently be performed via NEXMAN, WEB, Telnet or SNMP.

13.4.2. Saving the Basic Configurator Settings

All settings in the **User Defaults** field will be saved and reloaded with the next restart of the Basic Configurator.

14. Device-Lists

In a device list several devices can be combined to form a group. It is possible to create any number of lists in order to sort the devices by floors, buildings, etc. The groups are managed via the **File** menu:



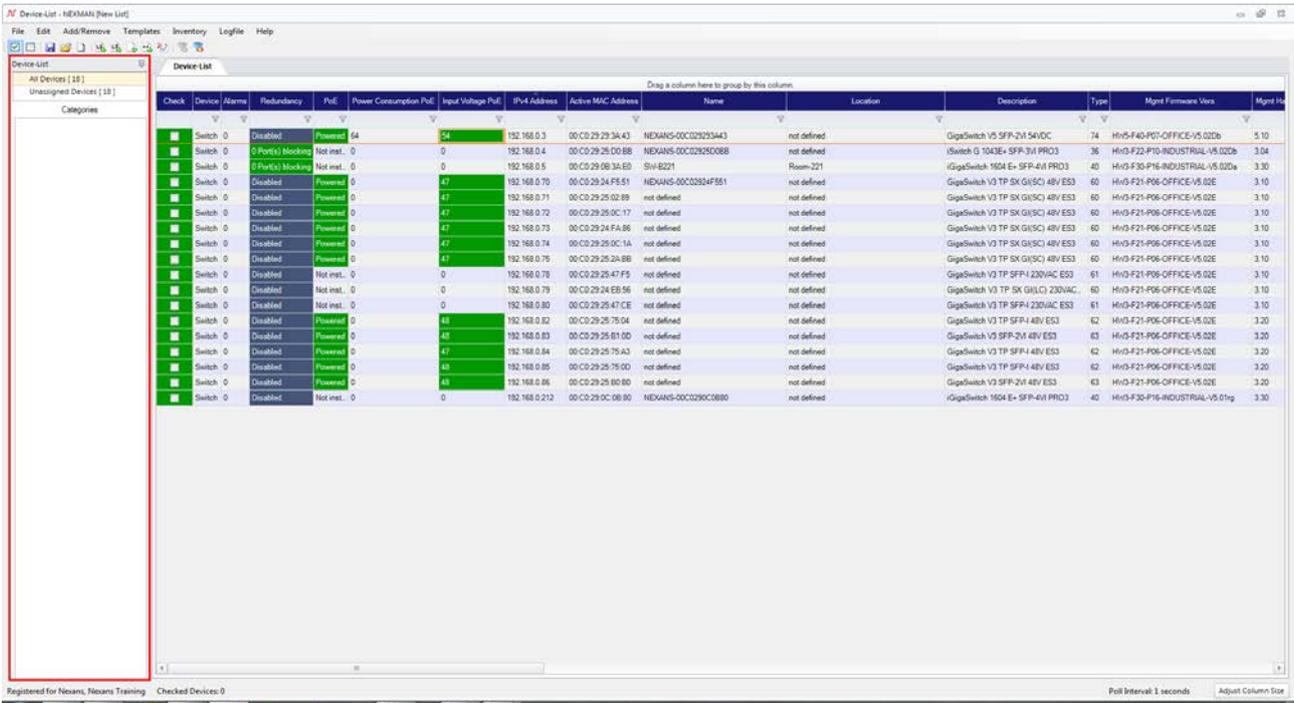
14.1. Device-Category

To the left of the device list you will find the categorization of devices. There are following categories:

- **All Devices** - List of all switches
- **Unassigned Devices** - List of all switches that have not yet categorized
- **Categories** - User Specific Categories

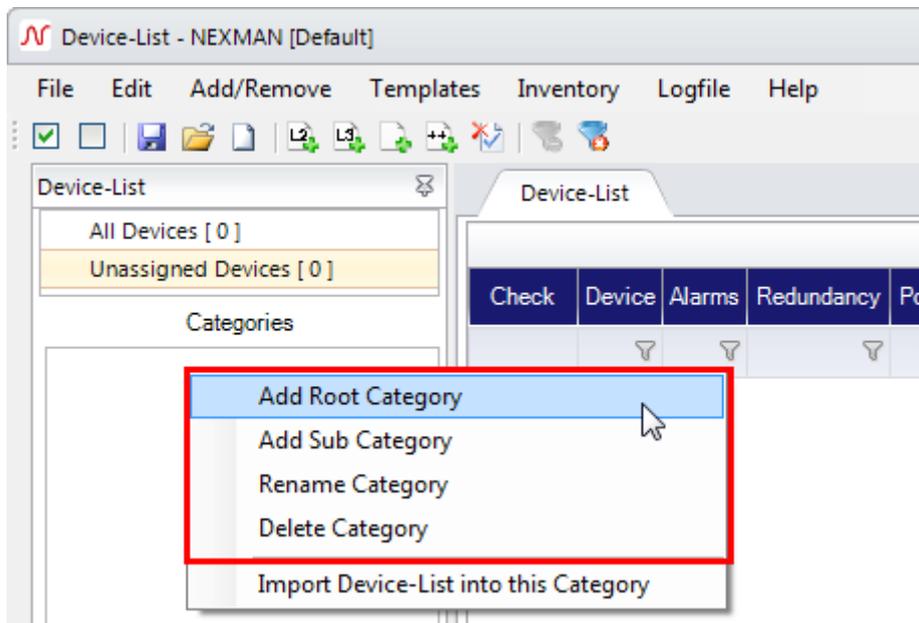
The number in brackets after **All Devices** and **Unassigned Devices** represents in each case the total number of devices in the appropriate category.

The **Categories** tree is always if new an empty list which can be created user-specifically. The user has the option to categorize their devices with their own tree structure itself.

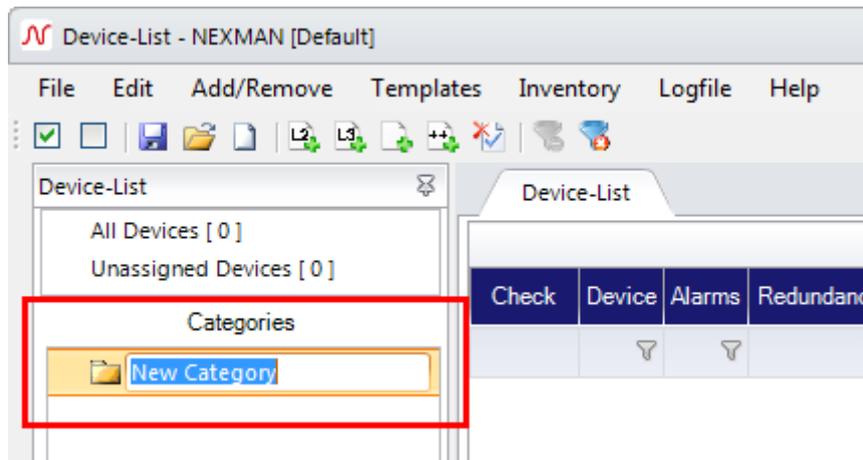


14.1.1. Create Category

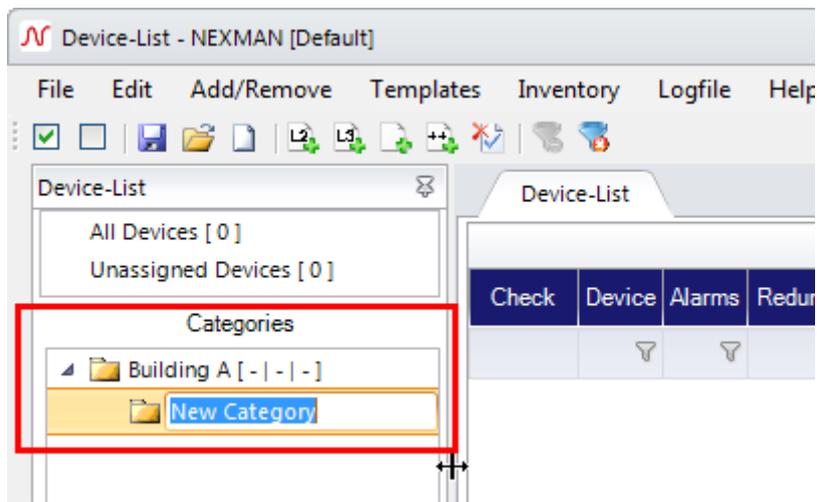
With a right click of the mouse in the "Categories" section a drop box opens to **Add Root Category**, **Add Sub Category** or Delete **Category**.



At the beginning of a new list it is only possible to create a new root category. When you **Add Root Category**, a new folder appears, which by default is called "New Category". You can rename this folder as for example "Building A". If you continue to create root categories, these are named "New Category_X". "X" represents a sequential number.

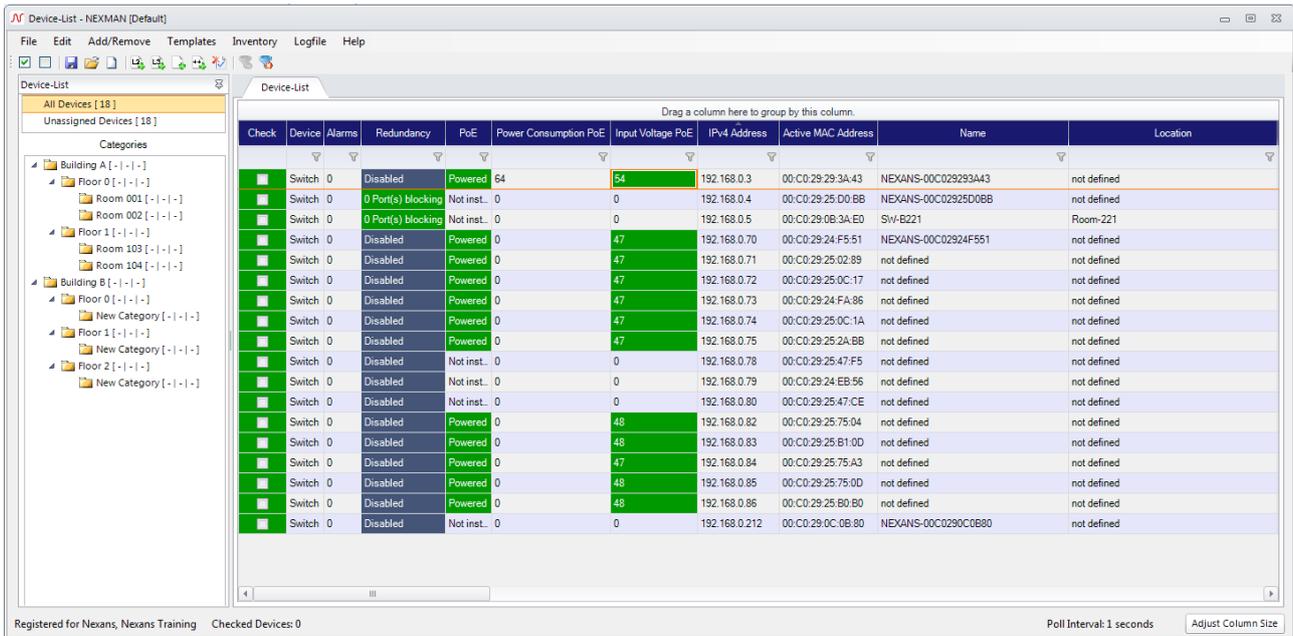


After creating a root category, it is possible to **Add Sub Category**. This will always be created in the currently selected category, with the same notation "New Category". As seen in the image, a folder has emerged, which is assigned to "Building A".



Next to the folder "Building A" a small arrow sign has appeared. When you click this sign all subcategories of the root category will hide. You can create as many sub-categories as you like, which will all depend on the context of the respective upper and subcategories.

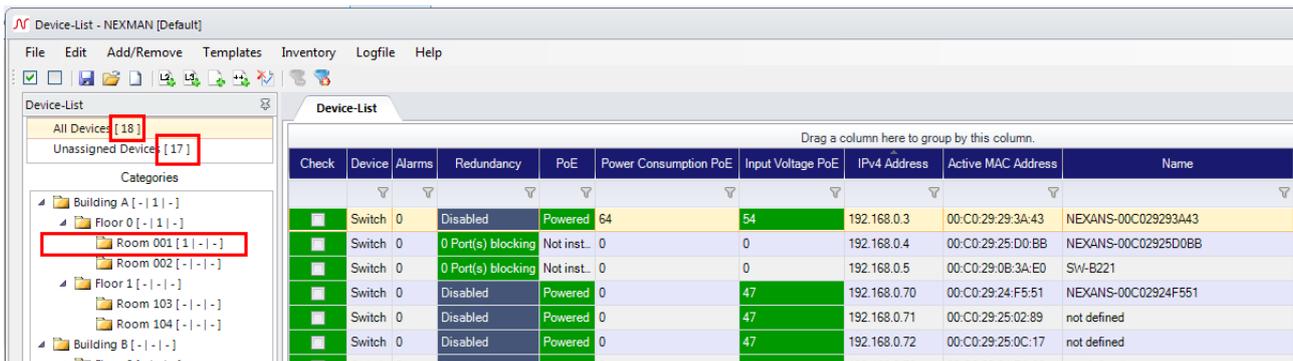
The purpose of this tree could for example be the following categorization. You have a top category "building", which has a sub-category "floor", which in turn has a sub-category of "room". Each of these categories is now able to manage devices in order to obtain an improved and simplified overview.



14.1.2. Allocating Category

After successfully creating the categories (see chapter 14.1.1 Create Category), it is now possible to associate the devices into their respective folders with drag-and-drop.

Hold the left mouse button on the device and pull it over to the folder you like to associate and release the mouse button. To associate multiple devices into a category, you have to select them each with the CTRL key and then drag them with the left mouse button over. For several following devices hold the SHIFT key, click on the first device and the last and pull the last device into the folder.

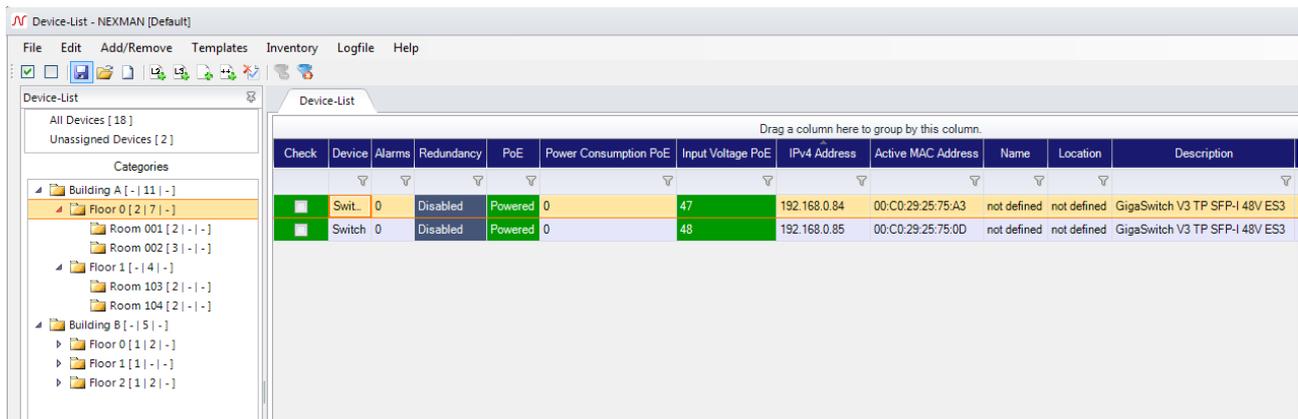


When a device is assigned to a category, the category name appears behind the statistics in brackets.

The left column represents the number of devices in this category alone.

The middle column represents the total number of devices that are included in the sub categories (added to the category of their own).

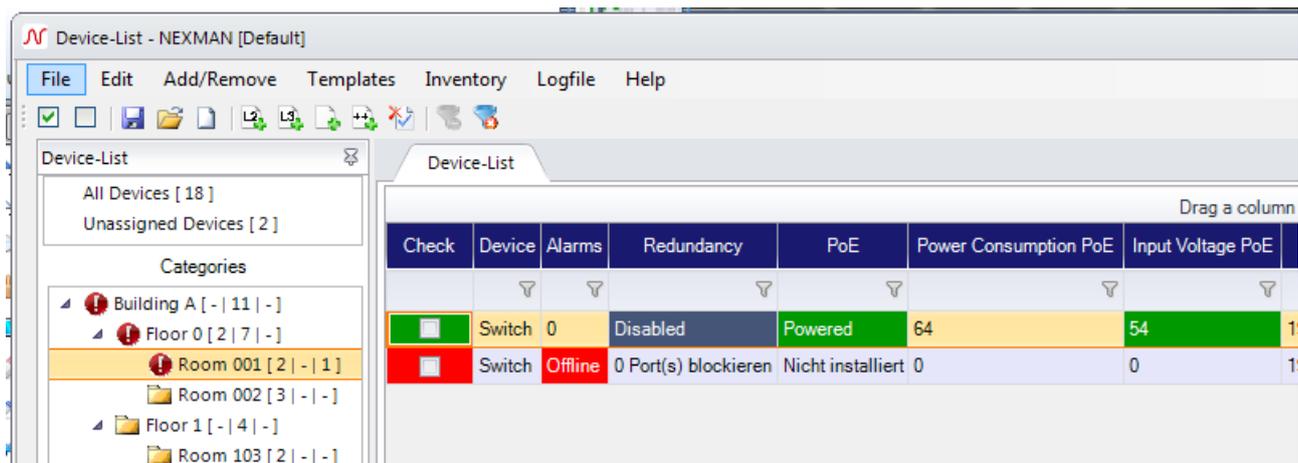
The right column shows the number of alarms available in the respective category (see next chapter 14.1.3 *Category Alarm*)



14.1.3. Category Alarm

If a device sets an alarm, it will be directly symbolically shown in the User-Defined list.

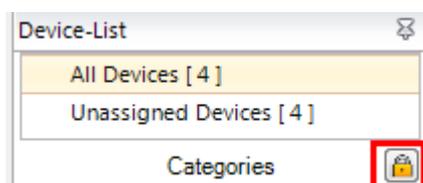
By opening the respective categories you will find that the device reports an error.



After you have corrected the error the number of errors and the symbol representing it, independently change to its normal state again.

14.1.4. Reordering Categories via Drag&Drop

Categories can be reordered by dragging them into a new position. If a Category is dragged directly onto another Category, it will become a new subcategory of that position. In order to prevent reordering by accidentally clicking on the category tree, you can lock or unlock the reordering using the 'Lock/Unlock' button.



14.2. Automatic polling of Device-Lists

Depending on the configured polling interval the contents of the device list is automatically updated in periodic intervals. If it is a Nexans device and if this device is reachable via UDP port 50266 (a firewall might block this port), the **Check** field is indicated in dark green and all fields will be updated with the corresponding values of the respective device. All fields which have changed their values will be indicated with a yellow background colour.

Check	Device	Alarms	Redundancy	PoE	Power Consumption PoE	Input Voltage PoE	IPv4 Address	Active MAC Address	Name	Location
■	Switch	0	Disabled	Powered	64	54	192.168.0.3	00:C0:29:29:3A:43	SW-B220	Room B220
■	Switch	0	0 Port(s) blocking	Not installed	0	0	192.168.0.4	00:C0:29:25:D0:BB	NEXANS-00C02925D0BB	not defined
■	Switch	0	0 Port(s) blocking	Not installed	0	0	192.168.0.5	00:C0:29:0B:3A:E0	SW-B221	Room-221

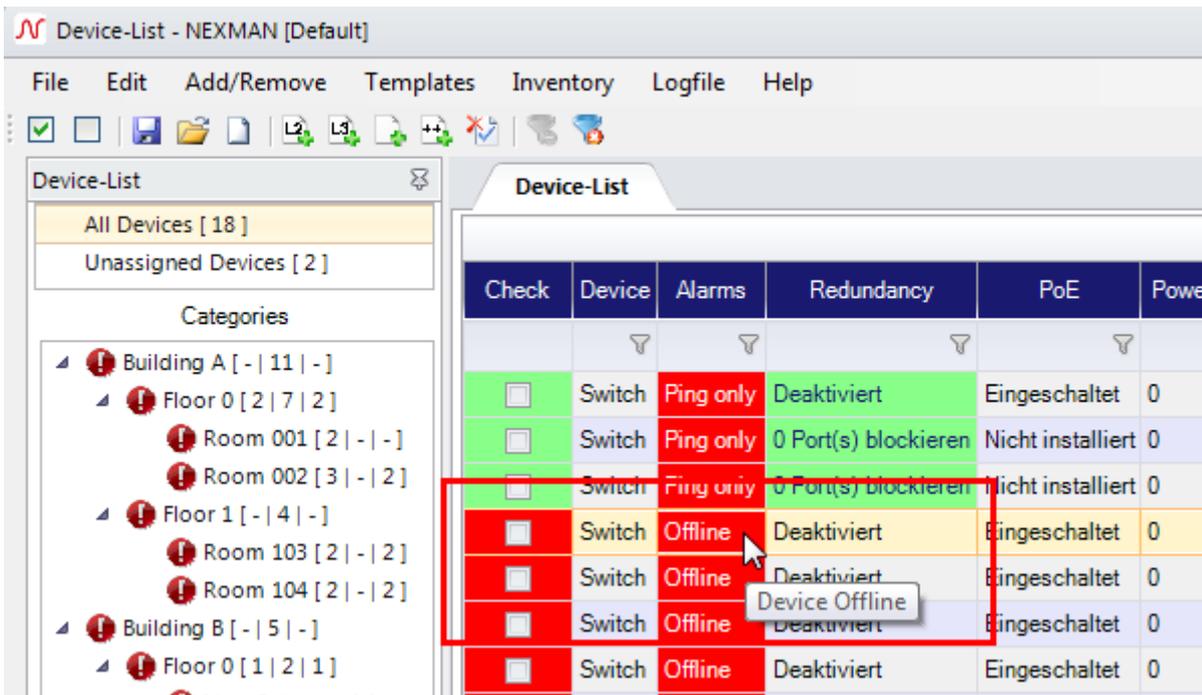
The **Edit > Acknowledge changes of checked Devices** menu can be used to remove the yellow background colour of the fields:

Note: In order to update all fields during polling, firmware version 3.64 or higher needs to be installed on the device. If an older firmware should be installed, some fields may be empty or marked with a '?'.

If the device does not answer on UDP port 50266, but only to a ping (e. g. because a firewall is blocking Port 50266), the **Check** field will be displayed in light green:

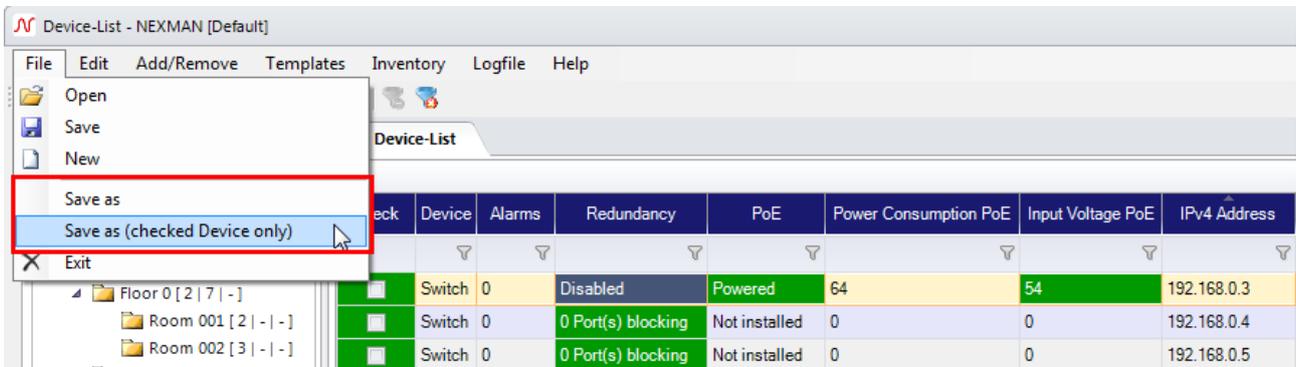
Check	Device	Alarms	Redundancy	PoE	Power Consumption PoE	Input Voltage PoE	
■	Switch	Ping only	Deaktiviert	Eingeschaltet	0	0	
■	Switch	Ping only	0 Port(s) blockieren	Nicht installiert	0	0	
■	Switch	Ping only	Device only responding to Ping! Possible reasons: > UDP Port 50266 blocked by firewall > Device runs not V3 firmware > Unkown third-party Device > Firmware damaged. Please retry update.				0
■	Switch	Offline			0	0	
■	Switch	Offline			0	0	
■	Switch	Offline			0	0	
■	Switch	Offline			0	0	

If the device answers neither on port 50266 nor to a ping, the **Check** and **Alarm** fields will be displayed with red background:

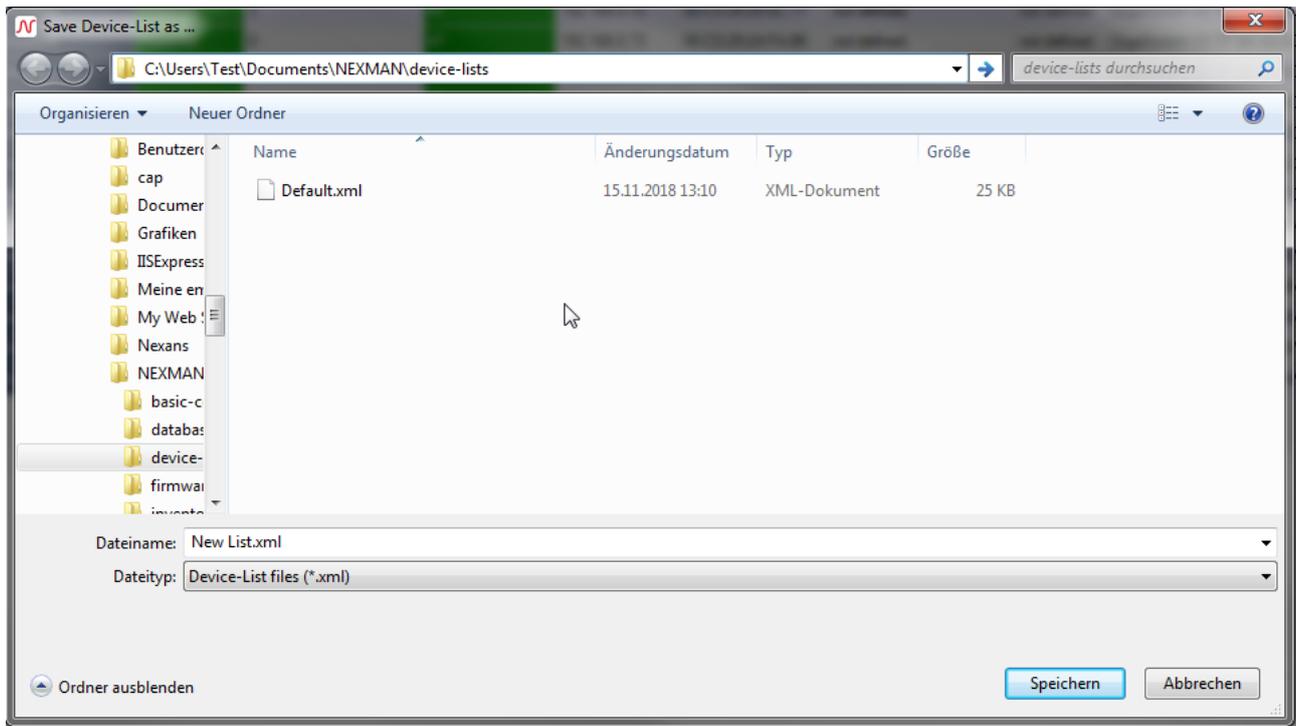


14.3. Saving the Device List under a New Name

After the first start of NEXMAN the device list "Default.xml" is created by default. If you want to save the device list under a new name, select the **File** menu:

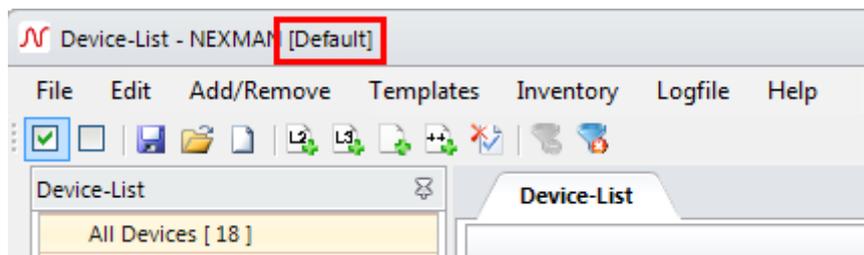


In the subsequent file browser window, the desired name for the Device List can be entered:

**NOTE:**

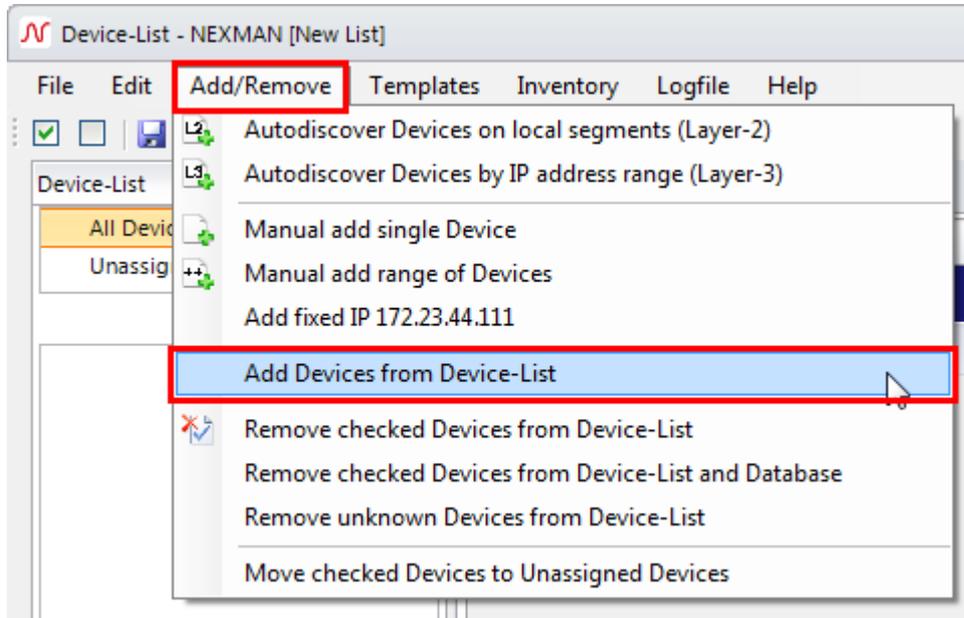
The directory shown for **Save as** or **Open** has been specified during the installation procedure and is set to "C:\Program Files\Nexans\NEXMAN\device-lists" by default. You can modify this directory via the **Edit → Preferences** menu and for example enter a server directory.

After the device list was stored under a new name, this list will be loaded as the current device list and indicated in the header:



14.4. Importing Device Lists

The **Add/Remove** menu allows you to import existing device lists. The imported device lists are added to the device list which is currently open:



The following import functions are available:

- **Add Devices from Device-List**

This function allows you to load device lists which have been created using NEXMAN.

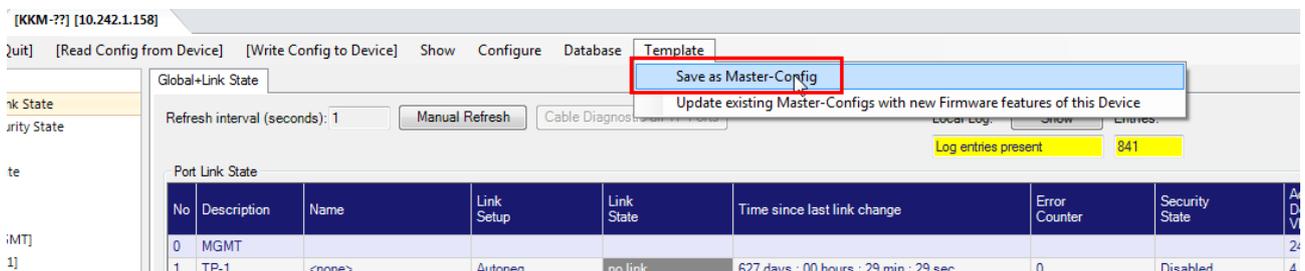
15. Master Configuration

A master configuration is used for distributing uniform basic settings to one or more devices of a device list. The master configuration offers the advantage that the administrator can choose which parameters to distribute. For example, you would be able to create one master configuration where only the SNMP settings are modified and another where only the RADIUS parameters are set. You could also create a master configuration for each department, if they require different settings.

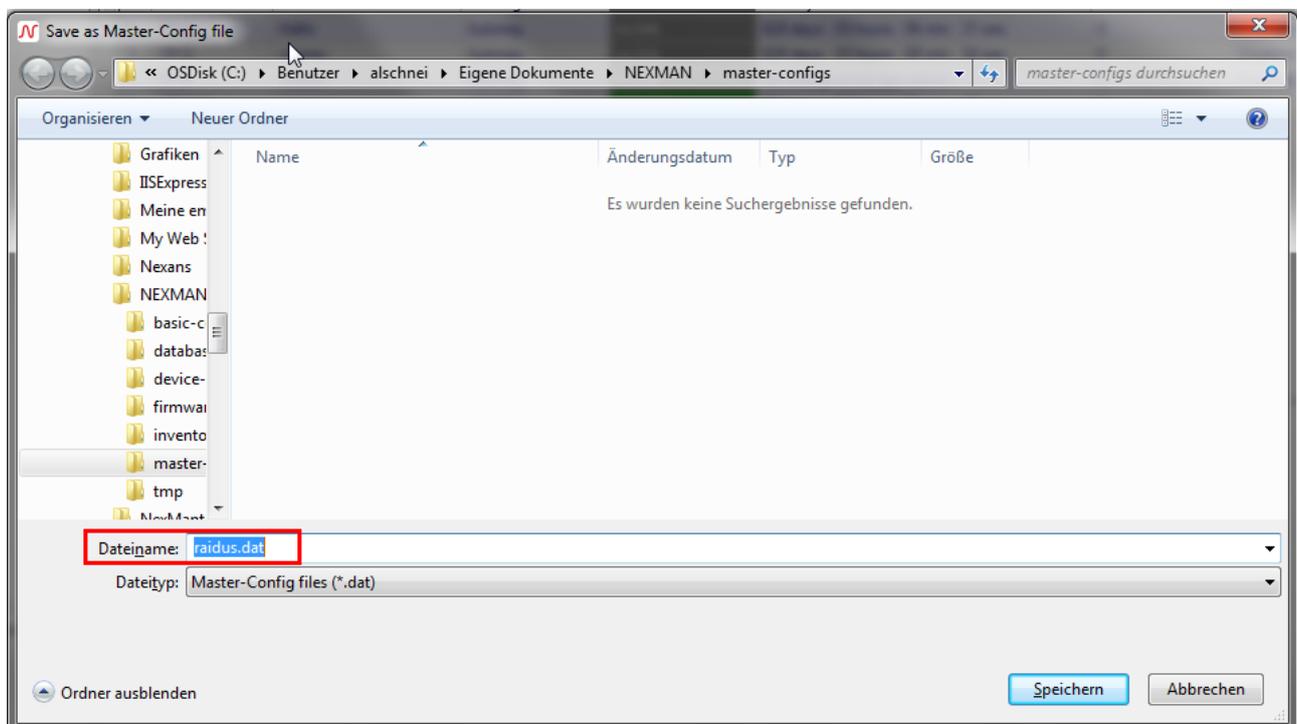
15.1. Creating a Master Configuration

Before distributing a master configuration, a template has to be created and edited. To do so, a device of the corresponding device type needs to be loaded into the device editor, e.g. by selecting a device from the device list by double-clicking on it.

Afterwards select the **Templates > Save as Master Config** menu option:



In the file browser window, which opens afterwards, a name for the master configuration needs to be entered. You should choose a mnemonic name describing the function of the master configuration:

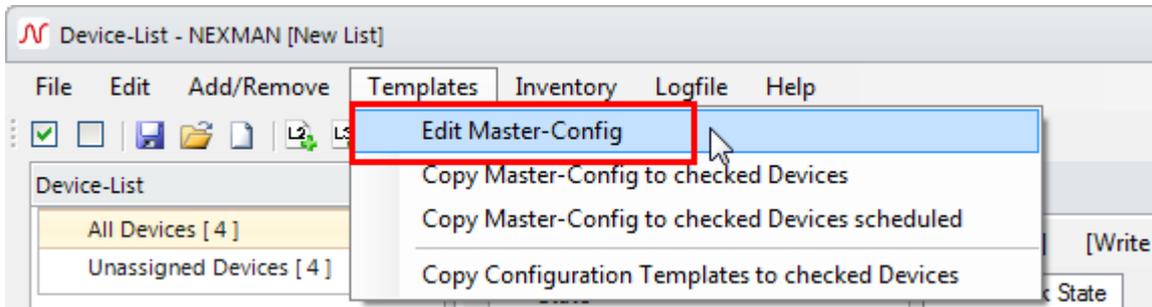


NOTE:

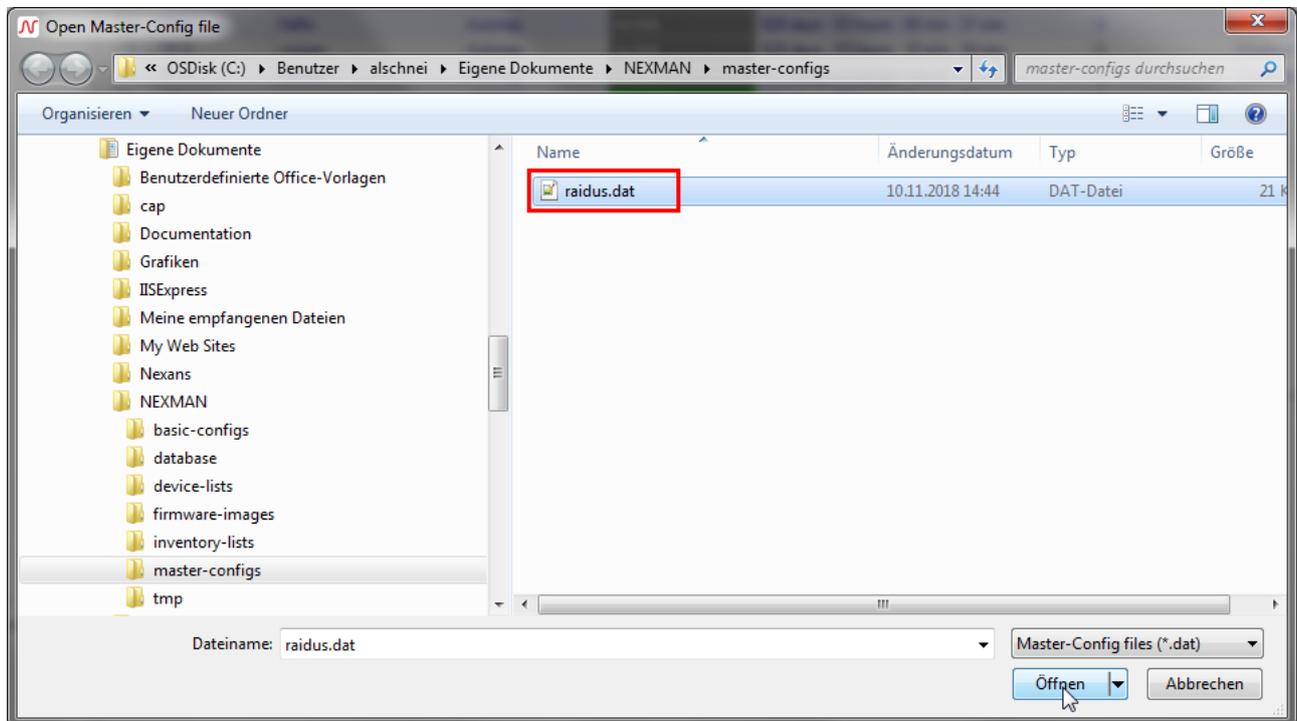
The directory shown has been specified during the installation procedure and is set to "C:\Program

Files\Nexans\NEXMAN\masters" by default. You can modify this directory via the **Edit > Preferences** menu and for example indicate a server directory.

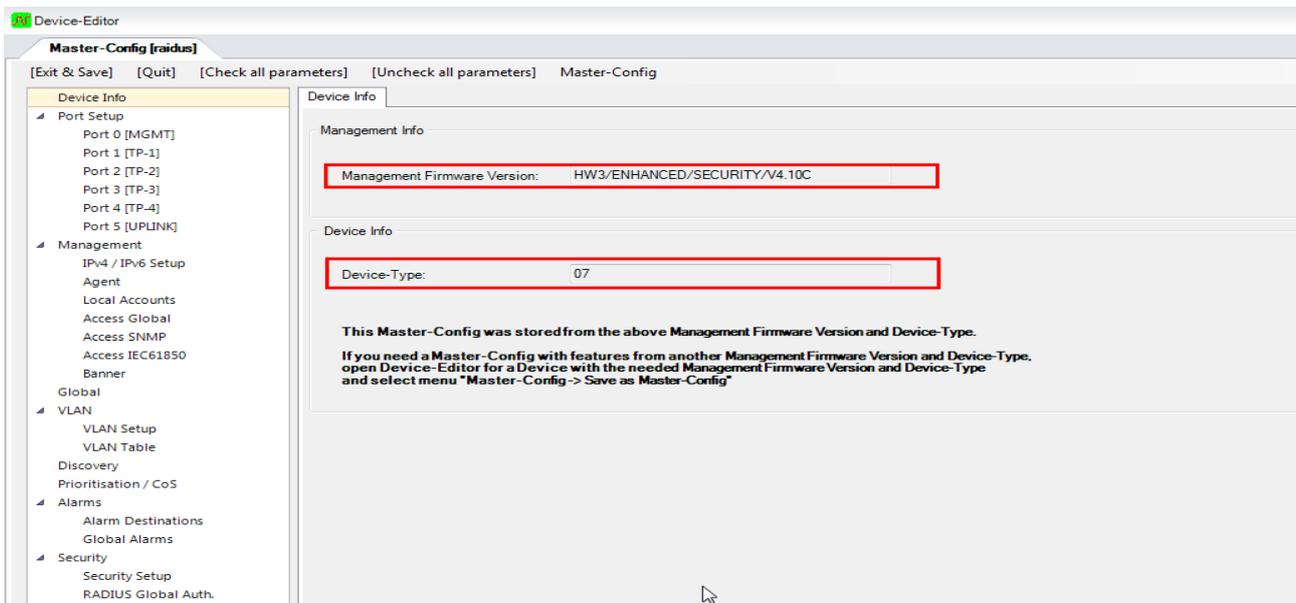
If you want to edit the master template you need to exit the device editor and select the **Templates → Edit Master-Config** menu option:



Select the previously stored master configuration in the next file browser window:



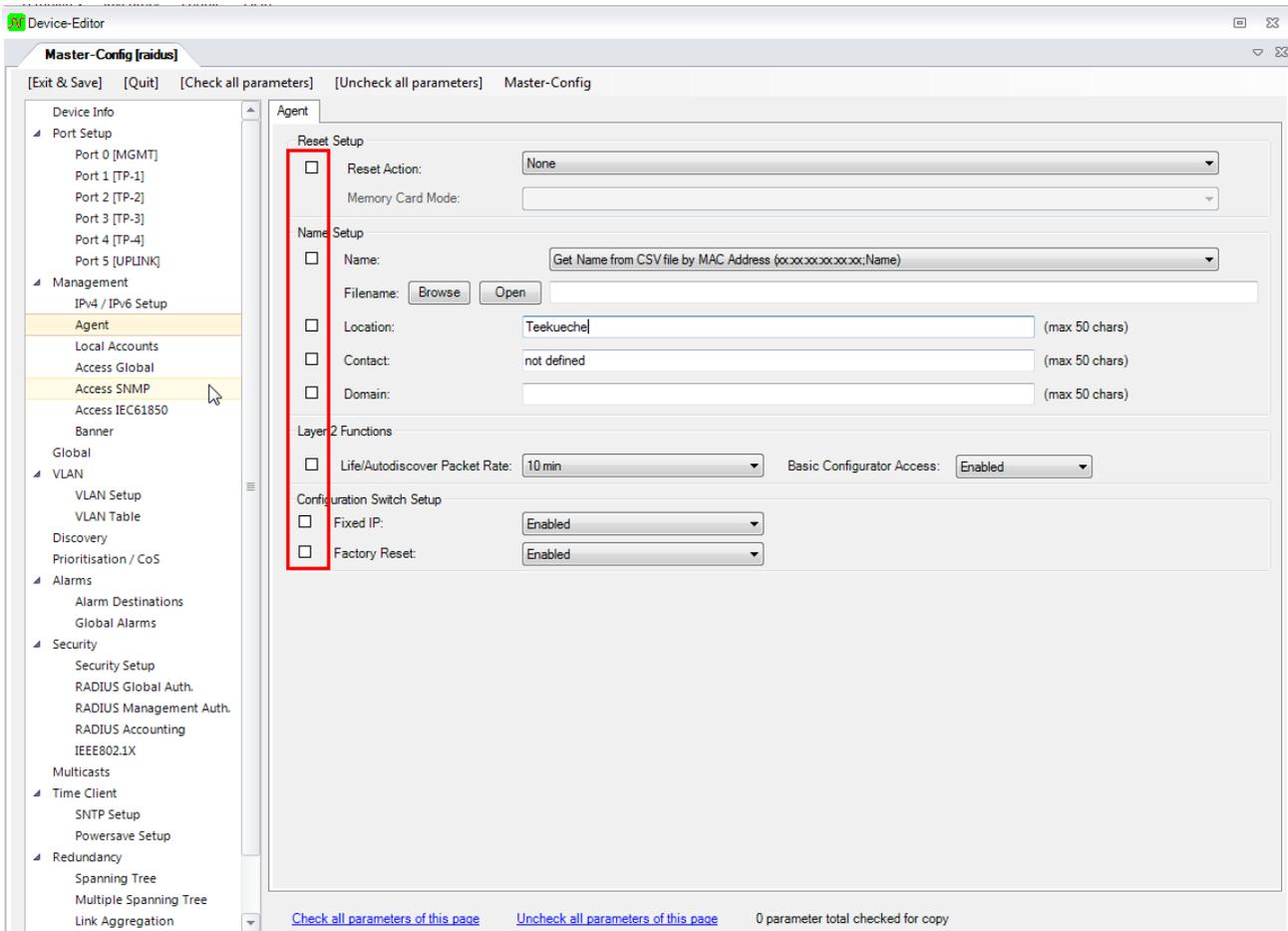
After selection of the master configuration a message is displayed first:



This message reminds you that the master configuration was created for a particular device type (in this example for Device Type 34; the respective device type is indicated on the Info tab).

Although this master was stored for device type 34 (as an example), it nevertheless can be transferred to other device types, if all device types contain the selected parameters (e. g. SNMP parameter). However, if you want to distribute special settings, such as Speed/Duplex, you have to consider, that these are different for each device type, since each device type has a different number of ports and/or port arrangement.

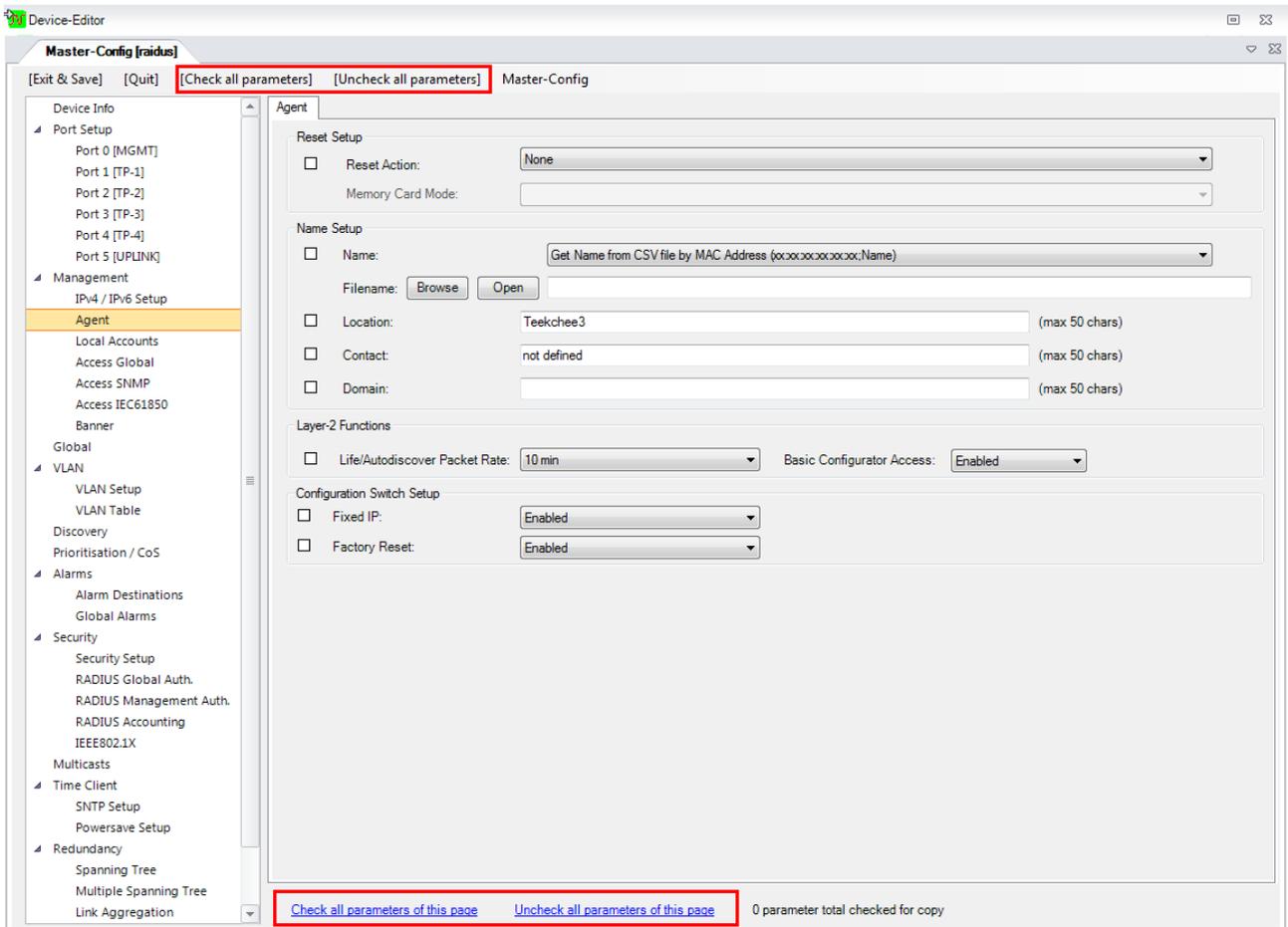
The master editor differs from a normal device editor in that it has no state page and that it offers additional check boxes preceding the individual parameters:



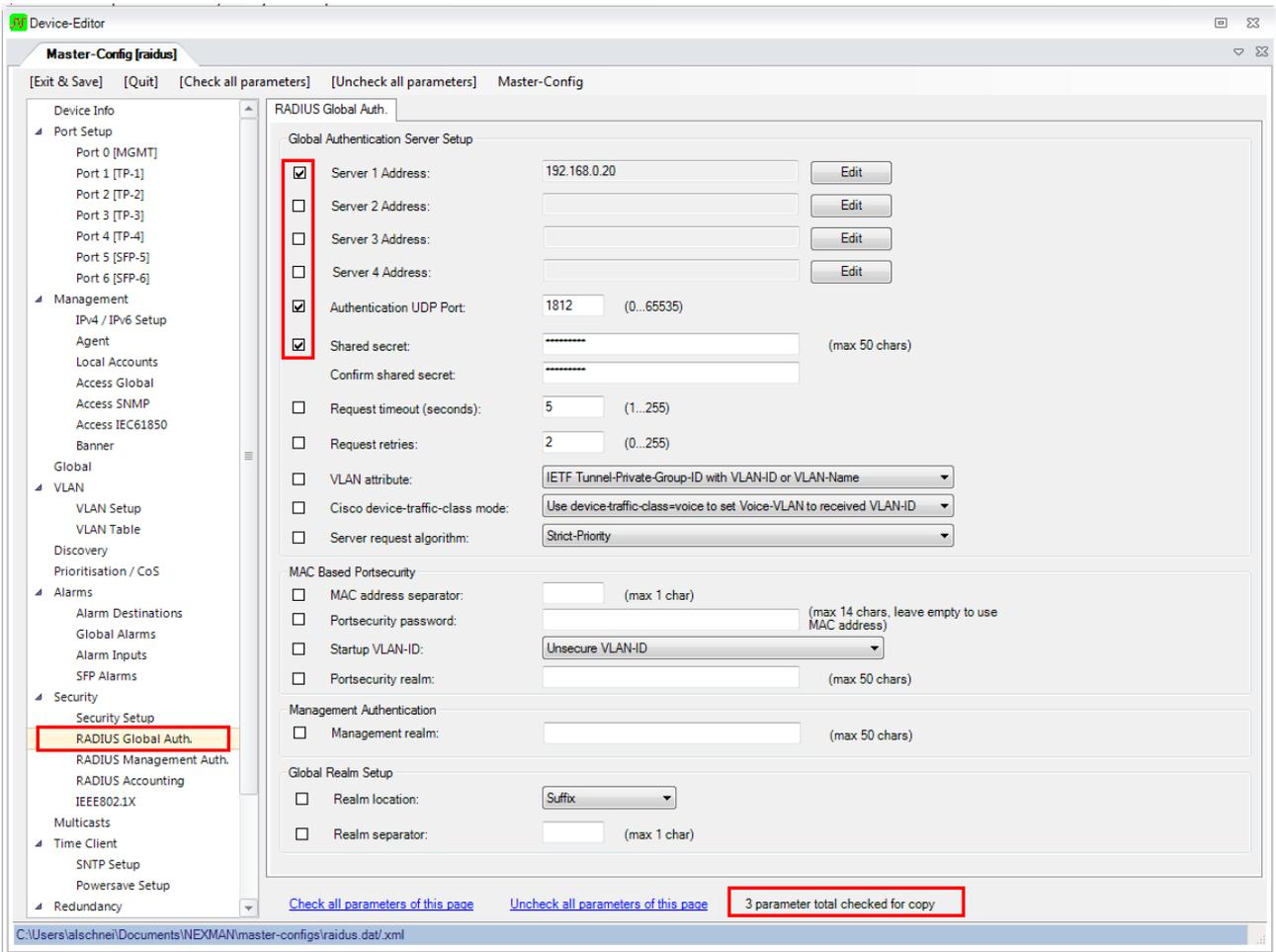
These check boxes allow you to choose which parameters are to be distributed to other devices. No other parameters will be changed in the target devices, i.e. the settings for these parameters are irrelevant as long as the respective box is not checked.

When you first open the master configuration no parameters are selected. This is confirmed by the counter in the left lower corner which indicates: "0 parameters checked for copy".

If you want to select/deselect all parameters for the whole switch or a single page you can do that simply via the menu options **Check all parameters**, **Uncheck all parameters**, **Check all parameters of this page** or **Uncheck all parameters of this page** respectively:



In the following example we want to create a master for the RADIUS settings. So we select the RADIUS Global Auth. tab and check the relevant boxes:



NOTE:

Some settings, i.e. some tables, can only be selected as a whole. For that reason the check mark will apply to the whole table.

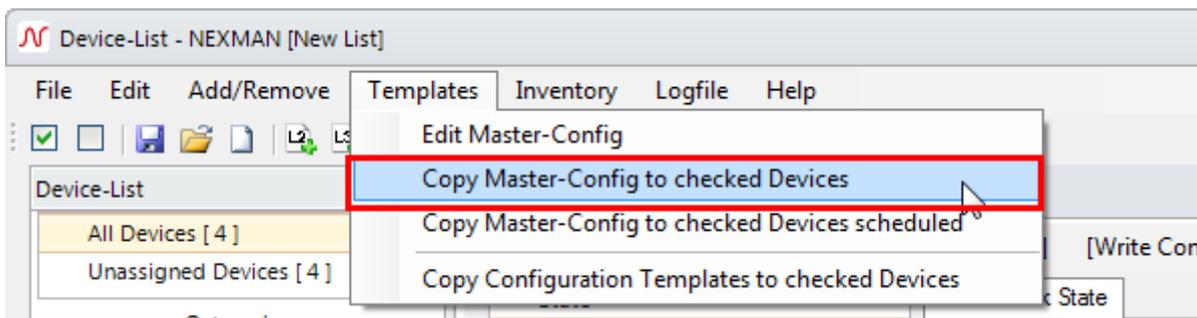
At the bottom you can see that 4 parameters have been selected.

Exit the master editor and save the configuration via the **[Exit & Save]** menu option.

15.2. Distributing a Master Configuration

You can only distribute a master configuration, if you have first created and edited the respective master (see previous chapter).

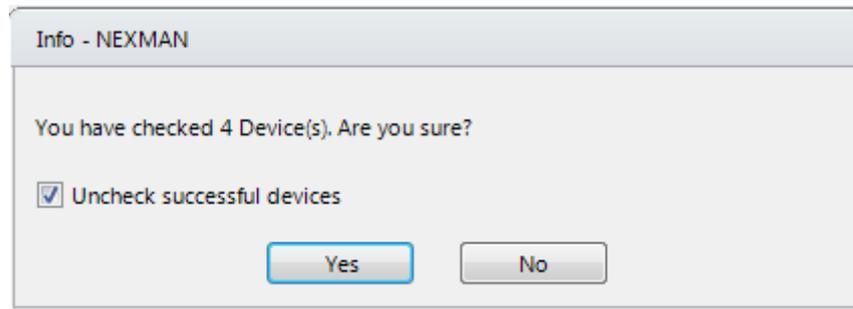
All devices, which shall receive the master configuration, must be selected in the **Check** column of the device list. Distribution is started by selecting the menu option **Templates > Copy Master to checked Devices**:



Note:

By selecting the menu option **Templates > Copy Master to selected Devices scheduled** a scheduled distribution is possible.

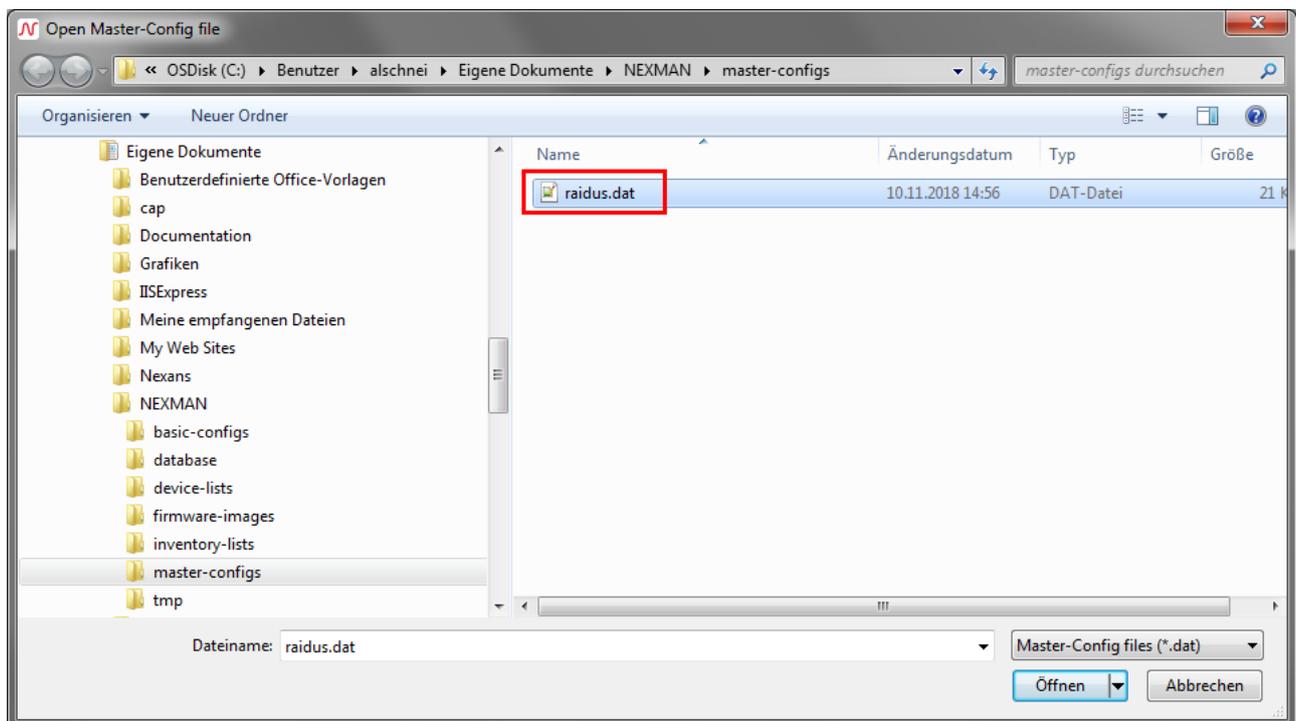
After selecting the desired menu option a confirmation query is displayed indicating the selected devices:



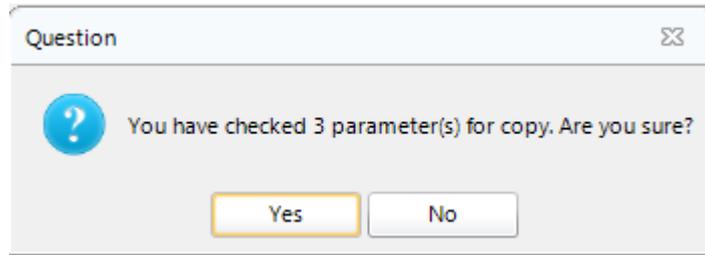
Note:

By checking the box **Uncheck successful Devices** the check mark in the **Check** column will be removed for all devices, to which the master has been successfully copied. Thus after completion of the distribution only those devices still have their check mark in the device list, for which the distribution has failed. So you do not need to look for them in the log book. By clicking on the **Check** column title these devices are moved to the top of the device list.

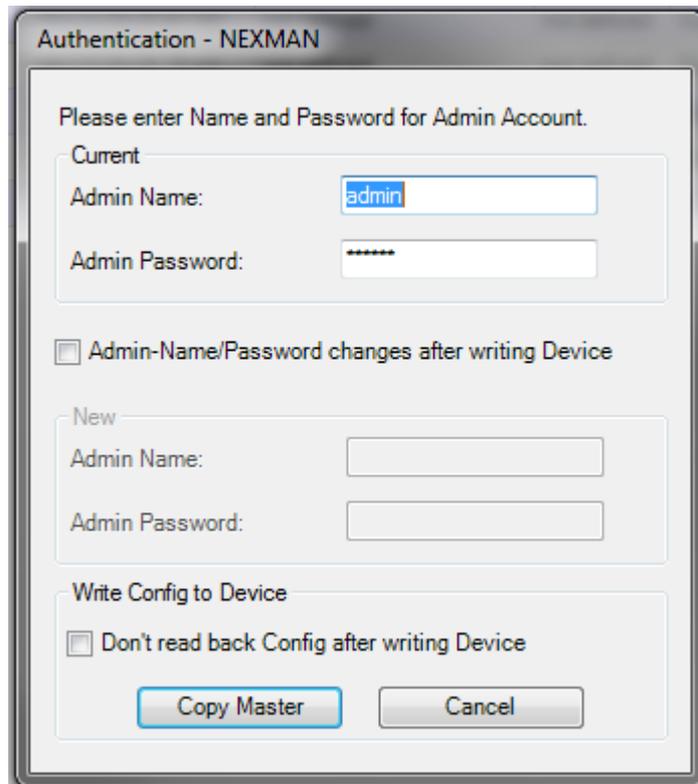
When you have answered the query with Yes a file browser window opens for selecting the previously created master configuration:



Now there is again a confirmation request displayed indicating the selected parameters:



Prior to the distribution the name and password of the Admin account have to be entered:

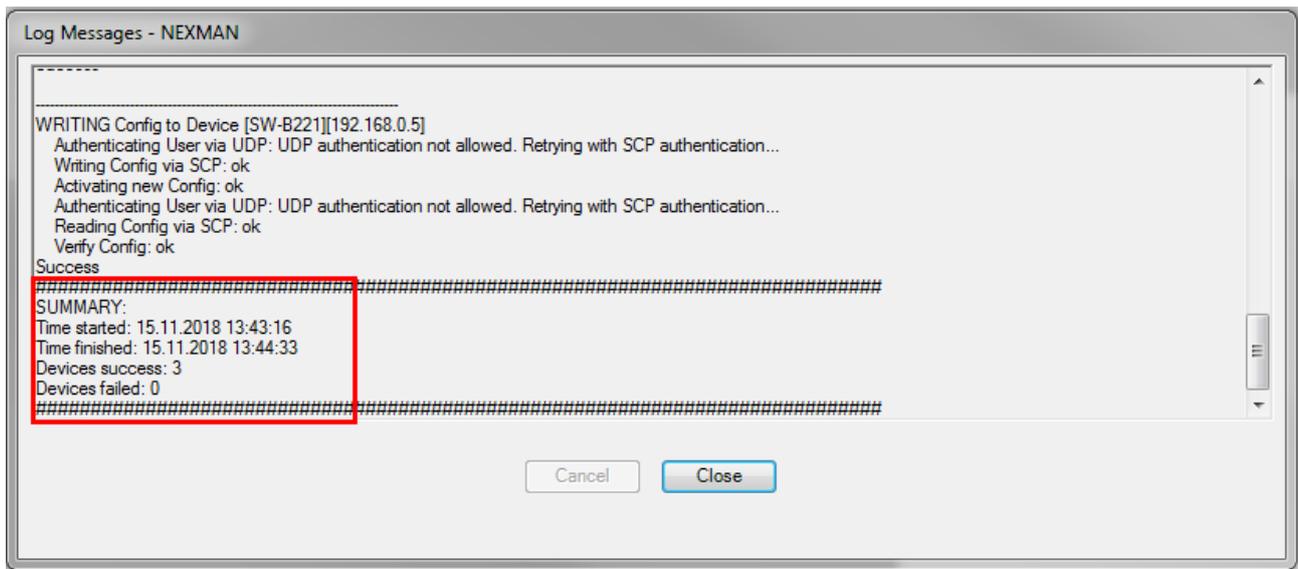


Note:

If the master configuration changes the Admin account, both the current Admin account and the new Admin account must be entered. In this case the box "Admin-Name/Password changes after writing Device" must be checked.

After pressing **Copy Master** the distribution is started.

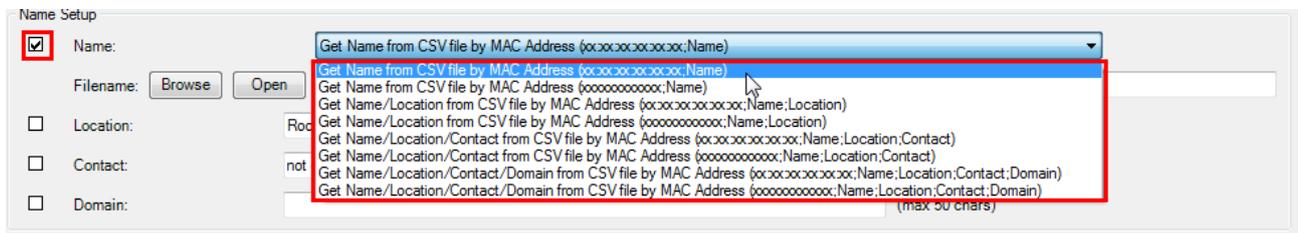
The progress can be monitored in the log window. After completion of all devices a summary is displayed at the end of the log book:



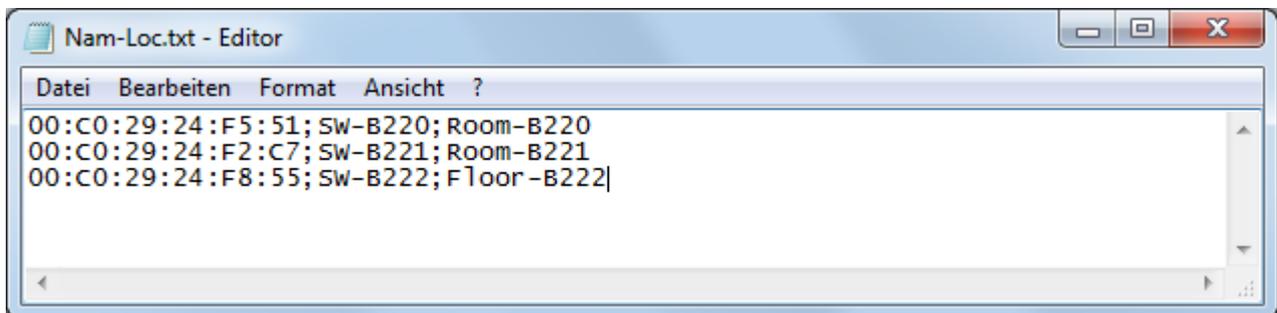
15.3. Distributing of Name and Location via Master Configuration

The name and the location of a device are typically assigned individually. That is why the standard procedure (as described above) with direct indication of a name or a location in the Master Editor cannot be used. Instead, in the Master configuration a reference can be made to an external CSV file from which the name and the location, if required, can be derived from the MAC address.

In the Master Editor you can choose among the following four procedures:

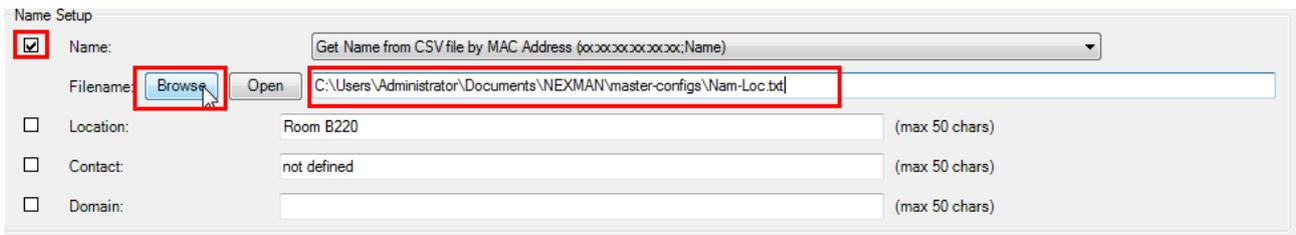


The corresponding format of the CSV file is indicated in brackets. A file for the selection of "Get Name/Location from CSV file by MAC Address (xx:xx:xx:xx:xx:xx;Name;Location)" could look as follows:



Note: Possible letters in the MAC address are accepted as upper- and lower-case letters.

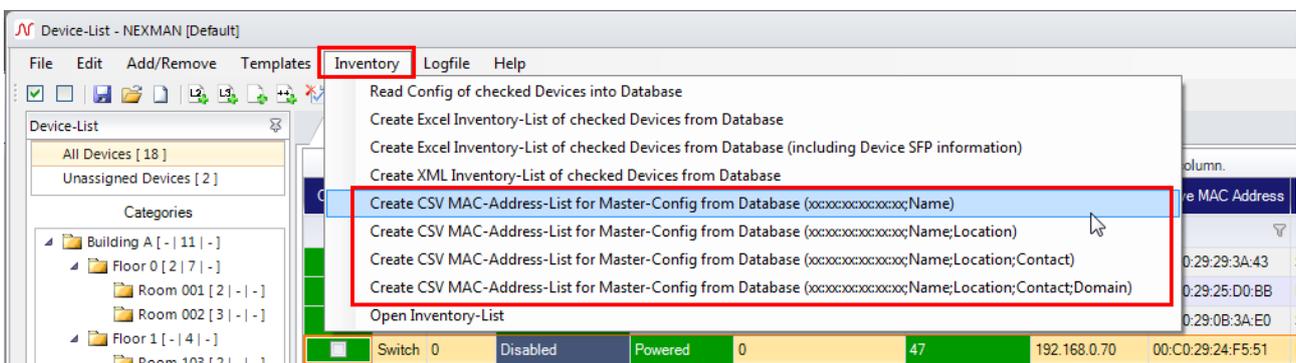
Afterwards the created CSV file must be selected in the Master Editor via the **Browse** button and the Master check mark be set:



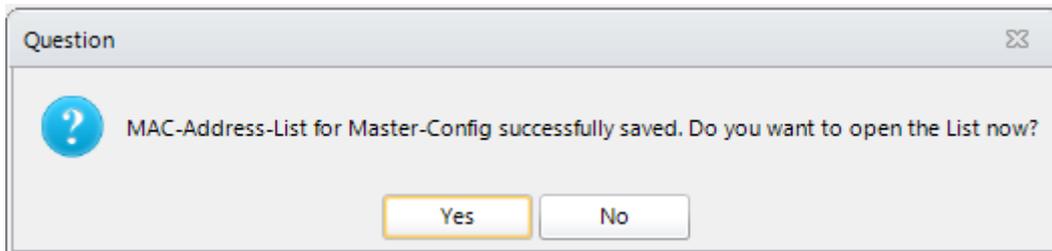
A template for the CSV file can be automatically created using the Manager. To do so select the desired devices in the **Check** column of the Device List and then select the menu item

Inventory → Create CSV MAC-Address-List for Master-Config from Database

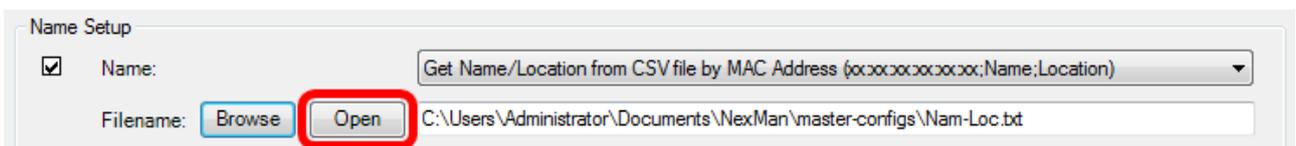
(xx:xx:xx:xx:xx:xx;Name) or **Inventory → Create CSV MAC-Address-List for Master-Config from Database (xx:xx:xx:xx:xx:xx;Name;Location):**



Now you can directly edit the created CSV file:



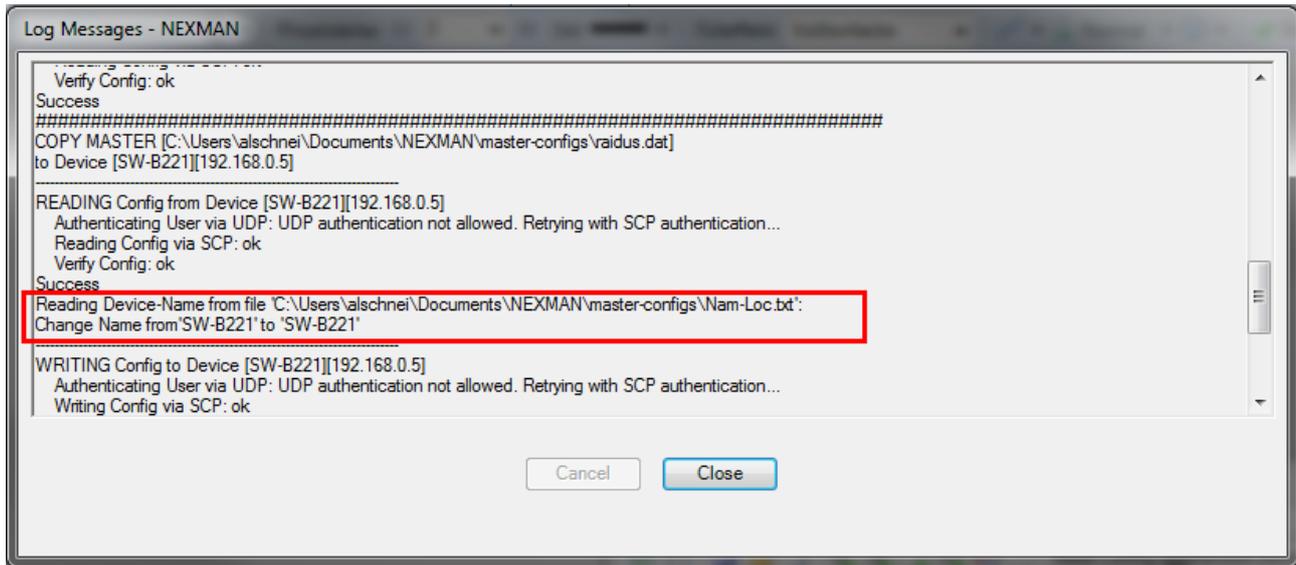
Alternatively, the CSV file can also be opened directly from the Master Editor via the Open button:



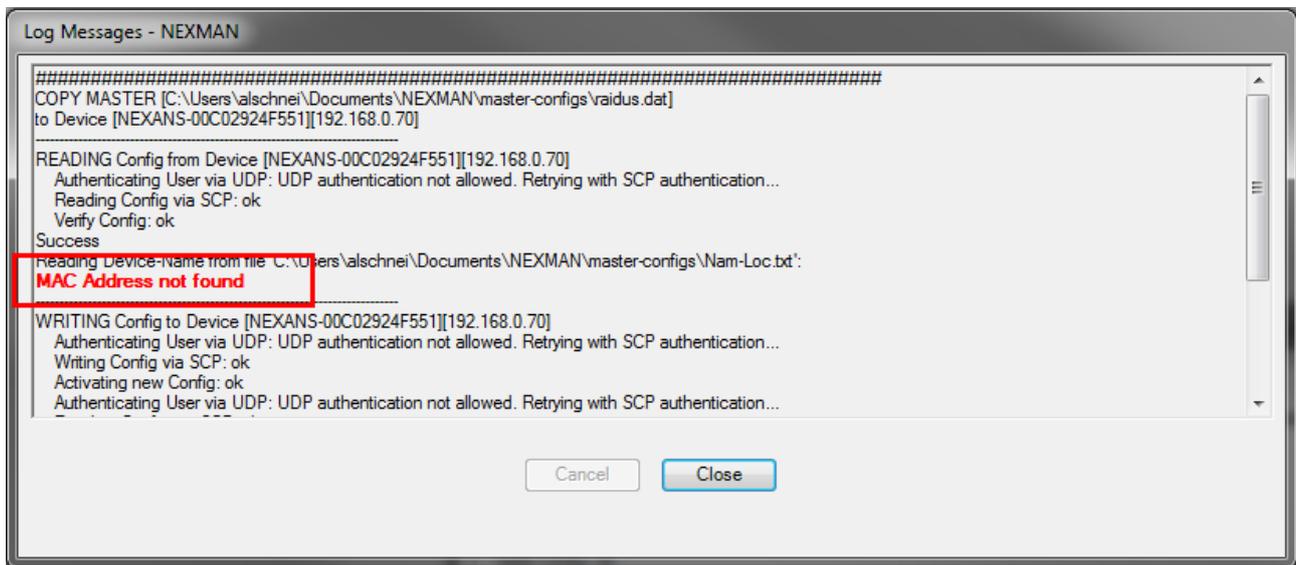
After saving the Master configuration can be distributed (see previous chapter).

Note:

The log book shows whether the Manager has found the respective MAC address of the device during the distribution of the Master configuration. The executed changes are documented:



If the respective MAC address is not found in the CSV file, a corresponding error message is returned and the name or location Device will not be changed. However, all other parameters of the Master configuration, which have been selected by Master check marks, will be accepted:



15.4. Distributing of IP Address via Master Configuration

In the same way as described in the previous chapter you can distribute the IP Address, Netmask and Gateway by using a .csv file. Therefore, click the check box next to the IP Address on tab 'IPv4 / IPv6 Setup' in the Master Editor.

IPv4 Address: Get IP-Address/Netmask/Gateway from CSV file by MAC Address
(xxxxxxxxxxxx;IP-Address;Netmask;Gateway)

Netmask:

Gateway Address:

The checkboxes for netmask and gateway will become disabled after selecting the IP Address, because these values are also taken from the .csv file. In this case, the file must have the following format:
MAC Address ; IP Address ; Netmask ; Gateway

Use the **Browse** button to select an existing file and the **Open** button to modify it.

15.5. Rebooting switches via Master Configuration

A reboot of single or all switches without changing the configuration can be performed via the Master configuration.

To do so, the Master check mark is set on the **Agent** tab and the Parameter check mark for **Reboot**. Please take care that this is the only Master check mark set (see indication in the footer):

Agent

Reset Setup

Reset Action: None
None
Reboot (Cold Start)
Reboot with Factory Default (Except IP Parameters)
Reset Total Boots Counter
Reset Port Counters
Reset Total Operation Time
Reset Local Logging
Reset Total Boots Counter, Port Counters, Total Operation Time and Local Logging
Reboot without customer reboot settings
Reboot with customer default settings
Room BZZU (max 50 chars)

Memory Card Mode:

Name Setup

Name:

Filename:

Location:

Contact: (max 50 chars)

Domain: (max 50 chars)

Layer-2 Functions

Life/Autodiscover Packet Rate: Basic Configurator Access:

Configuration Switch Setup

Fixed IP:

Factory Reset:

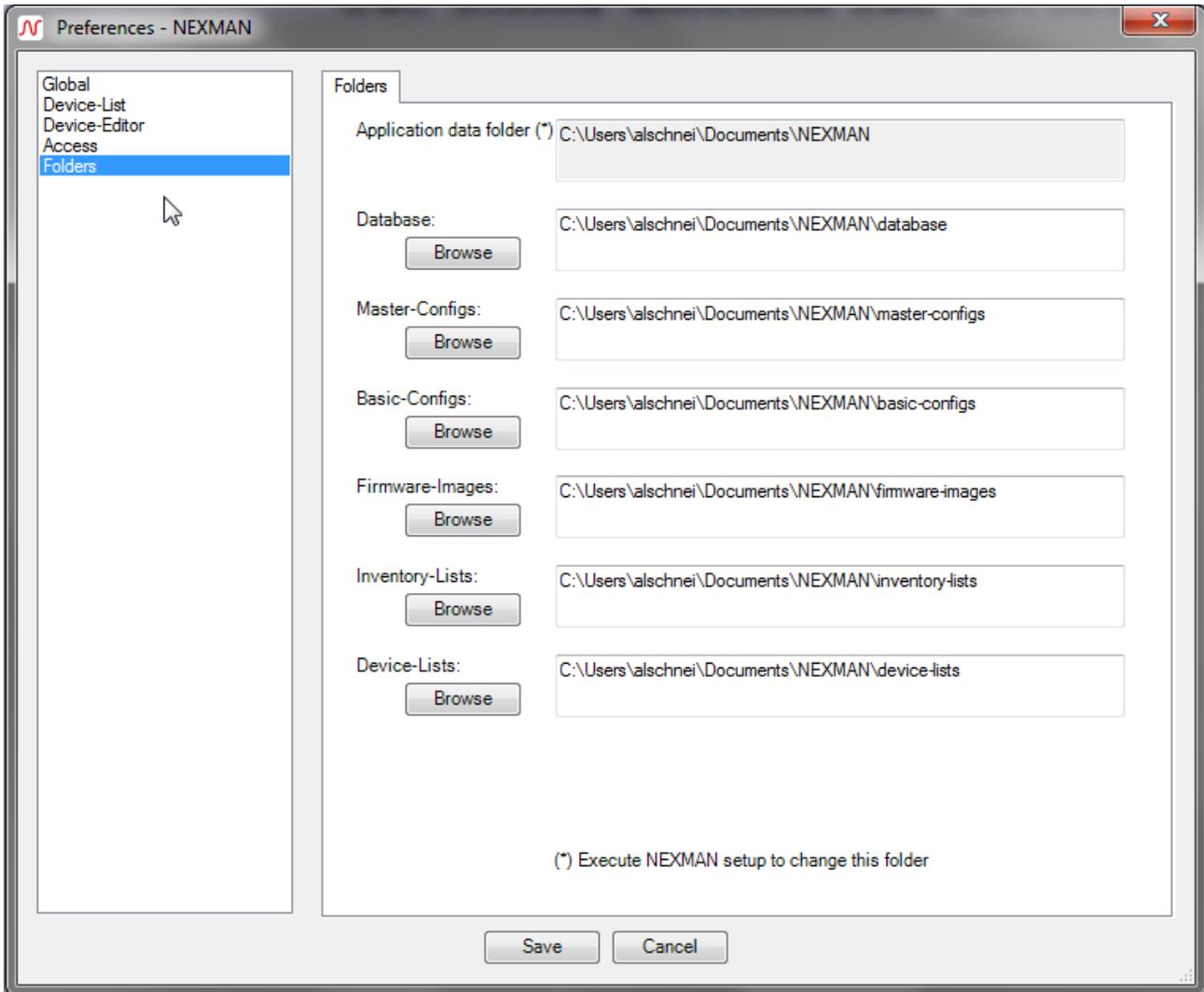
When this Master configuration is distributed, a single switch is rebooted at a time and then the process is paused until this switch is online again, before the next switch is addressed. The current configuration of the switches (after rebooting) is saved to the database so that possible changes in the configuration are recorded by DHCP/BOOTP.

16. Data Backup

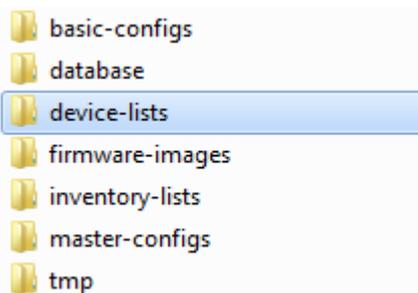
In order to perform a data backup, the folders indicated during installation must be saved. By default these folders are created in the following path:

C:\Users\[your username]\Documents\NEXMAN

If these folders were modified during installation, the paths can be verified in the Device-List in the “Edit > Preferences > Folders” menu.



For a data backup the following folders should be saved:



For a new installation or transfer of data to a new computer the existing folders can be replaced by the saved ones.

In order to import all settings made under Preferences, the NEXMAN configuration file must be saved. This file is located in the main directory, where also the folders are placed.

 NEXMAN.config	10.11.2018 14:56	CONFIG-Datei	17 KB
---	------------------	--------------	-------

This file contains the paths of the configuration folders. It might be necessary to modify them.

17. Multi-User capability

Multi-user capability is particularly useful if the Manager is installed on different computers and these access the same server directories for database and device lists. Another application would be launching the Manager several times on the same computer.

17.1. Terminal Server Support

All common terminal servers are supported. This allows several users to execute the Manager simultaneously on a computer.

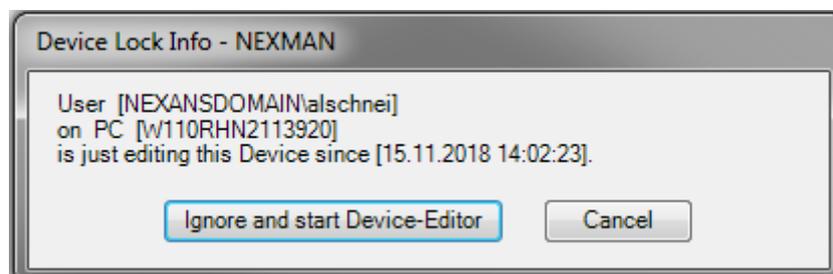
17.2. Device-List

As precondition an interval should be configured for automatically saving the device list under menu item Edit > Preferences > Device-List using the Autosave Device-List configuration setting. Here the device list is only saved, if changes have been performed on the list. If a second Manager has opened the same device list in parallel and wants to add or remove devices, it will recognize the changed and automatically saved device list of the first Manager and issue an appropriate warning:



17.3. Device-Editor

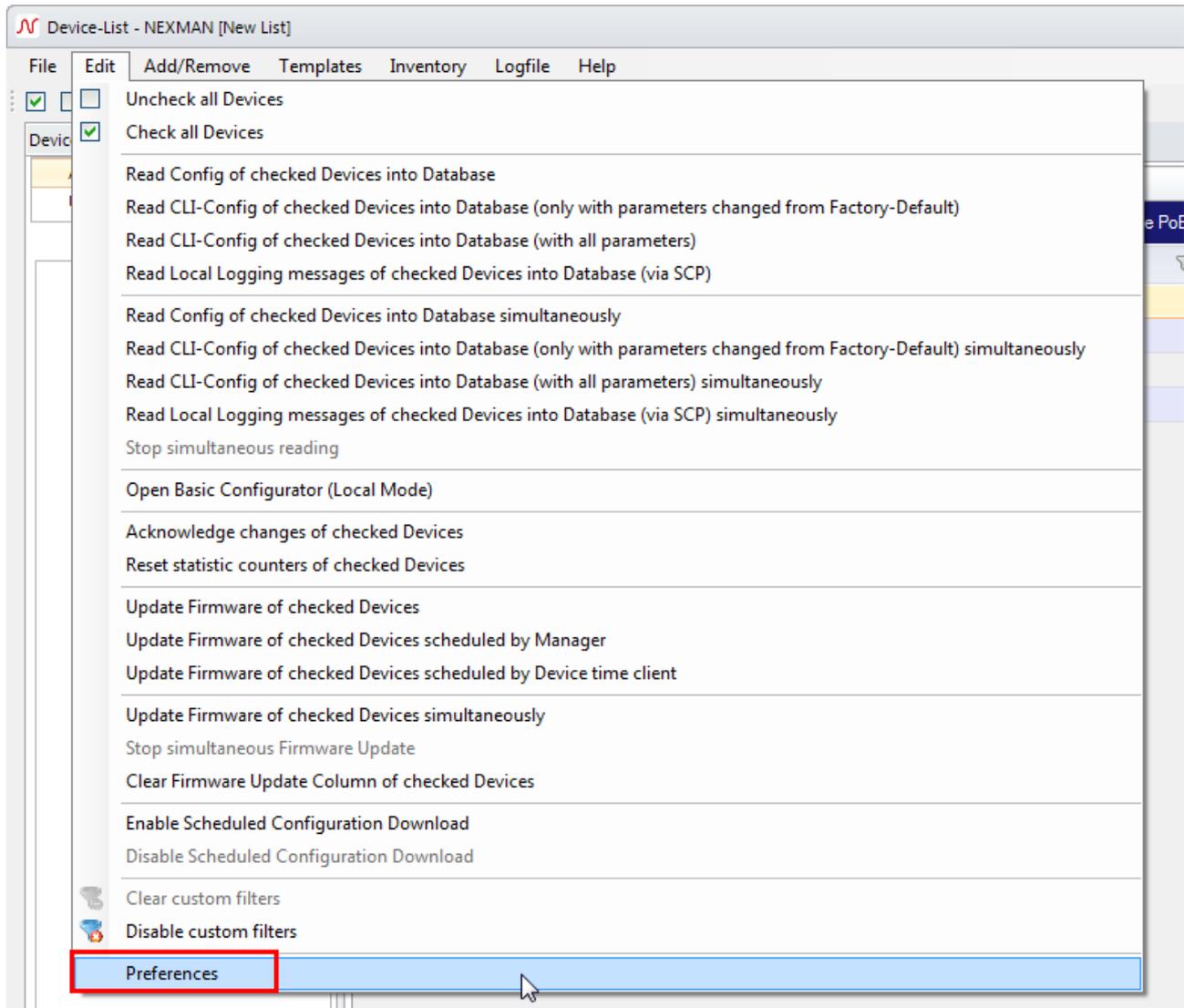
As soon as a device is opened in the Device-Editor for editing, the Manager creates a Lock file for this device in the Database directory. If then a second Manager tries to edit the same device in parallel, an appropriate warning is issued indicating user name, PC name, date and time:



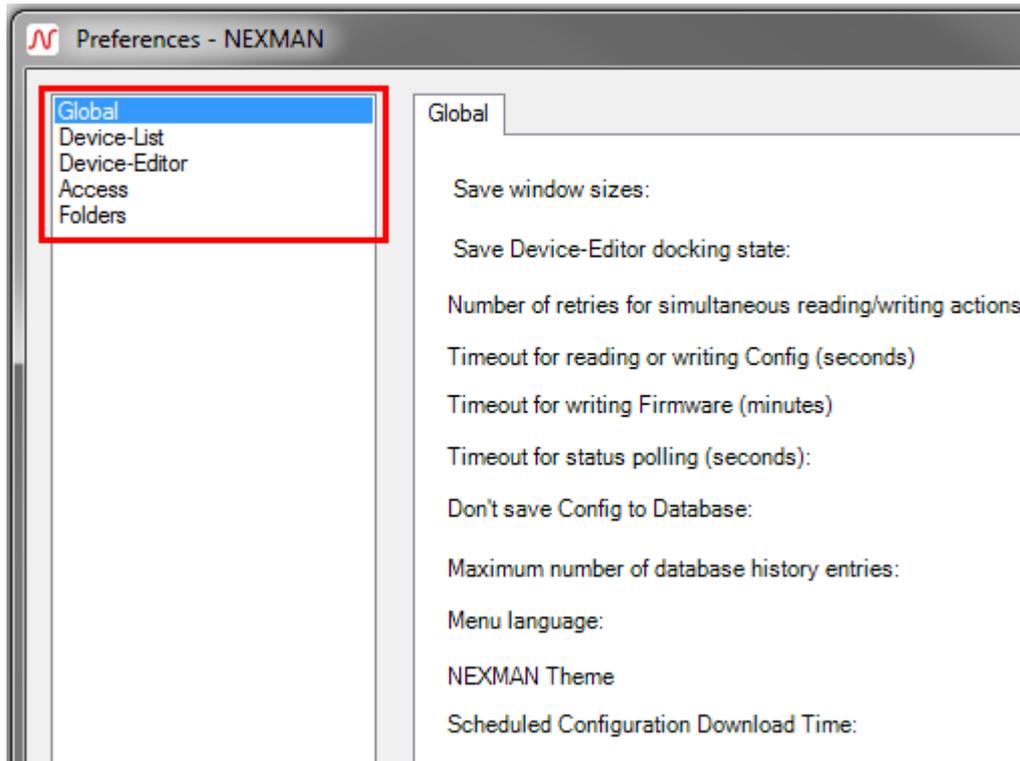
After leaving the editor the Lock file is deleted again.

18. Preferences

The basic settings for NEXMAN can be entered via the **Edit > Preferences** menu:

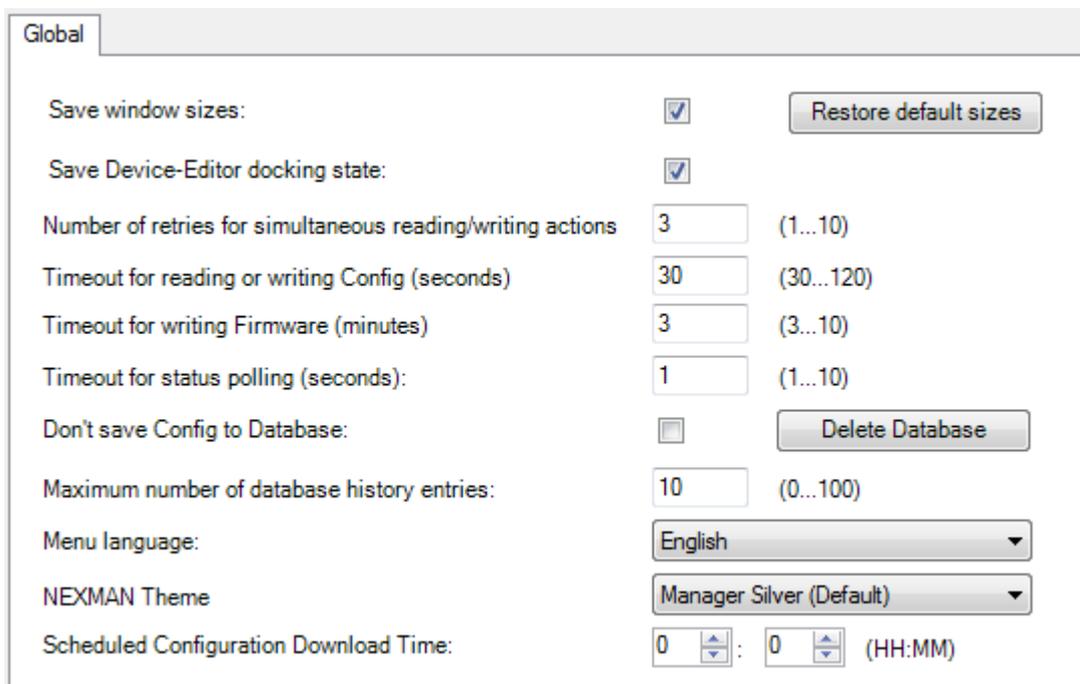


In the displayed dialogue box you can now select an appropriate category in the selection menu on the left side:



18.1. Global

The global settings are defined in this category:



18.1.1. Save Window Sizes

If this box is checked, the window positions and sizes of the device list, the device editor and the master editor are saved and reloaded with each call. If this box is not checked, the default size and positions will be used for each start. Pressing the Restore default sizes button will reset the saved values to the default values.

18.1.2. Save Device-Editor docking state

If this box is checked, the docking state of the device editor and the master editor is saved. That means, depending on the state of the last closed editor new editors will be opened as floating windows or tabbed to the main window. If this box is not checked, new editors will be tapped to the main window. In this case, saved window sizes have also no effect on new editors.

18.1.3. Number of retries for simultaneous reading/writing actions

This value defines how often the NEXMAN retries to connect to the switch during any simultaneous action if any connection error occurs.

These actions are described in chapter *12.9 Configuration of multiple devices*.

18.1.4. Timeout for reading or writing Config (seconds)

While reading or writing a configuration to the device, NEXMAN is waiting for the indicated period of time, until the device activates the configuration. The default value is 30 seconds. This default value should be changed in exceptional cases only (e. g. if after a reboot of the device and the related link loss a very long dead time would be added by the core device).

18.1.5. Timeout for writing Firmware (minutes)

While updating the firmware, NEXMAN is waiting for the indicated period of time, until the device has booted with the new firmware. The default value is 3 minutes. This default value should be changed in exceptional cases only (e. g. if after a reboot of the device and the related link loss a very long dead time would be added by the core device).

18.1.6. Timeout for status polling (seconds)

This is the period of time used for waiting for an answer from the device during status polling until it is considered offline. This applies both to polling the devices in the Device List (Stand-Alone version) and to polling within the Device Editor. The default value is one second. This value should be changed in exceptional cases only (e. g. if the connection to the device is made via a very slow dial-up connection).

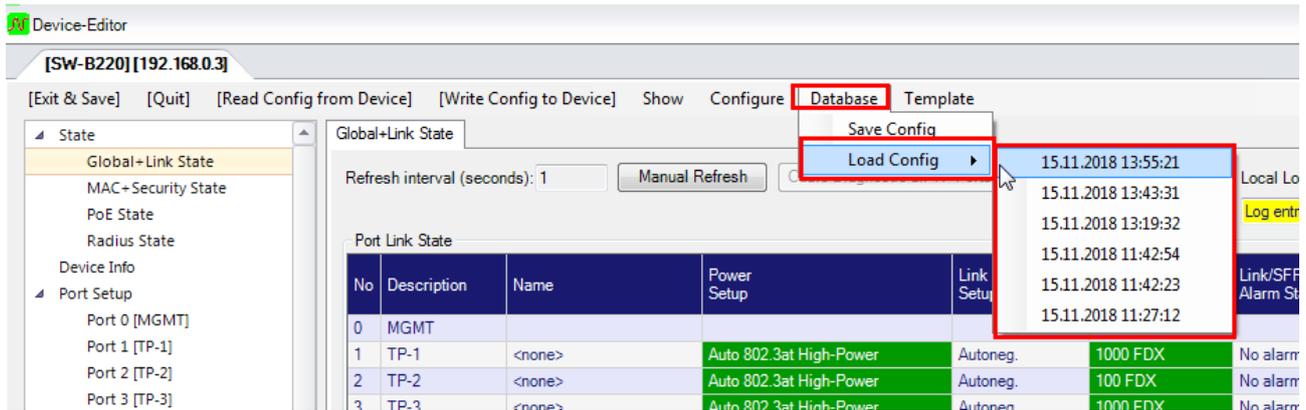
18.1.7. Don't save Config to Database

If this setting is enabled, binary and CLI configurations are prevented from being saved in the database. This makes particular sense, if for reasons of security the switch configuration must not be saved to a data storage medium.

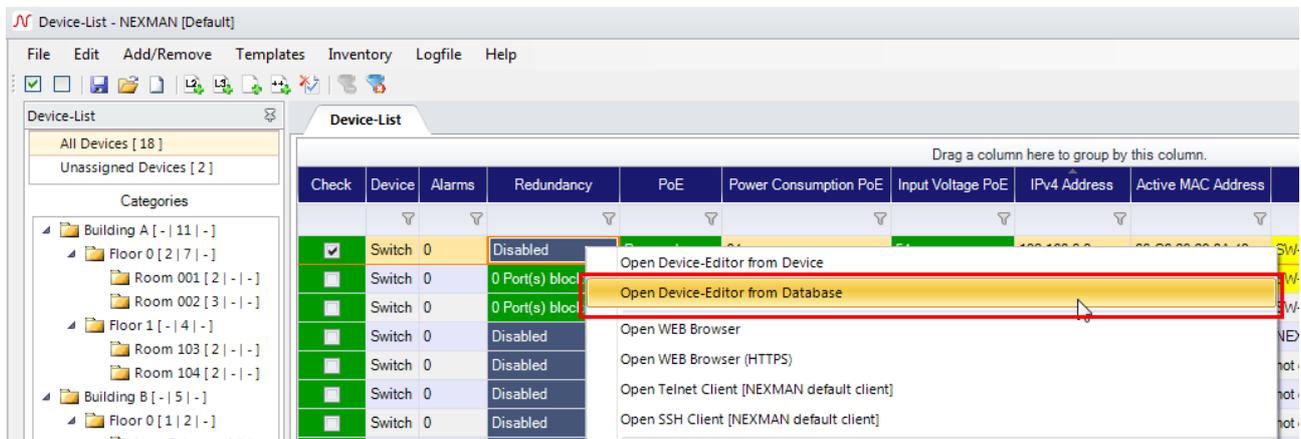
18.1.8. Maximum Number of Database History Entries

This value defines the maximum number of configurations which can be archived for each individual device in the database folder. After each save operation of a modified configuration to the database a new archive

entry is created and excess entries, if any, deleted. These archived configurations can be loaded into the device editor via the **Database > Load Config** menu:

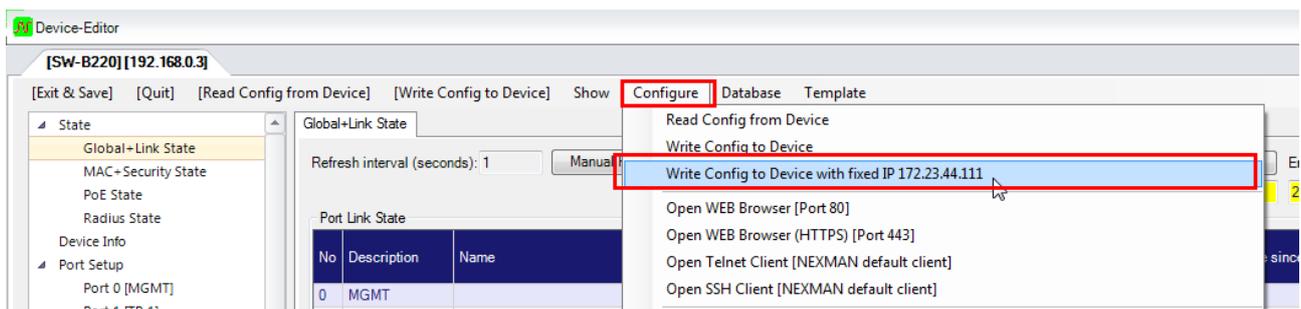


Moreover, the most current configuration in the database can be loaded into the device editor by selecting the **Open Device-Editor from Database** menu option from the right-click menu:



Any configuration, which has been loaded in such a way, can be written back to the device using the **Write Config to Device** function.

Another possibility of using the database is the simple replacement of a device. For example: The replacement device can receive the configuration of the old device prior to installation without having to be activated with its final IP address in the network. To do so, you just have to boot the device with the fixed IP address and subsequently write back the configuration, which was loaded into the device editor via the **Open Device-Editor from Database** menu option, via the **Configure Device > Write Config to Device with fixed IP 172.23.44.111** menu:



18.1.9. Menu language

You can here change the language of NEXMAN. The following languages can be selected:

- English
- Deutsch
- Français

18.1.10. NEXMAN Theme

The following themes can be chosen:

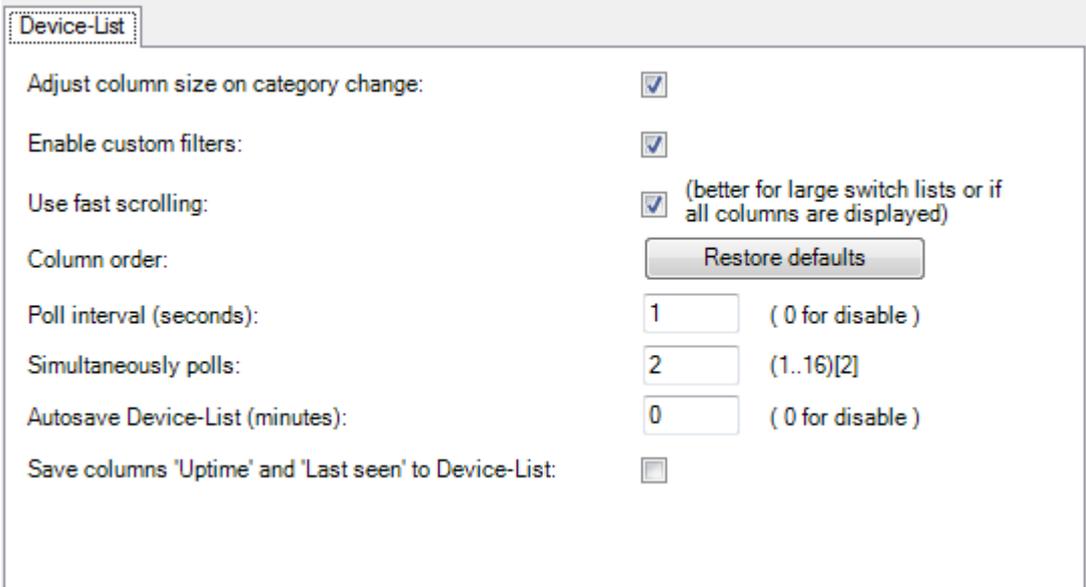
- NEXMAN Silver (Default)
- Windows 7
- Desert
- Metro Blue
- Metro

18.1.11. Scheduled Configuration Download Time

Set the time for frequent configuration download. See chapter *12.9.2 Enable Scheduled Configuration Download* for details.

18.2. Device-List

These basic settings only apply to the behaviour and the appearance of the device list:



The screenshot shows a configuration window titled "Device-List" with the following settings:

Adjust column size on category change:	<input checked="" type="checkbox"/>
Enable custom filters:	<input checked="" type="checkbox"/>
Use fast scrolling:	<input checked="" type="checkbox"/> (better for large switch lists or if all columns are displayed)
Column order:	<input type="button" value="Restore defaults"/>
Poll interval (seconds):	<input type="text" value="1"/> (0 for disable)
Simultaneously polls:	<input type="text" value="2"/> (1..16)[2]
Autosave Device-List (minutes):	<input type="text" value="0"/> (0 for disable)
Save columns 'Uptime' and 'Last seen' to Device-List:	<input type="checkbox"/>

18.2.1. Poll interval (seconds)

This period of time defines the intervals at which the devices in the device list are polled via UDP port 50266. This setting does not exist in Client/Server version.

18.2.2. Poll Controller interval (seconds)

This period of time defines the intervals at which the client polls the controller for any new information, for example Device-List updates or new log messages.

This setting does not exist in the Stand-Alone version.

18.2.3. Simultaneously polls:

Here the number of parallel queries of several switches contained in the Device List is set. In particular for a large number of devices this provides the advantage that the switch status will be refreshed more quickly.

This setting does not exist in Client/Server version.

18.2.4. Autosave Device-List (minutes)

Here an interval for automatically saving the Device List can be configured. The device list is only saved, if changes have actually been performed on the list.

This setting does not exist in Client/Server version.

18.2.5. Save columns 'Uptime' and 'Last seen' to Device-List

In the Device List the **Uptime** column shows the time since the last booting of the device. Moreover, in the **Last seen** column the date and time of the last received response of the device is listed. By default these two columns are not saved in the Device List file.

If the Device List shall display the current values for these two columns immediately after opening, the **Save columns 'Uptime' and 'Last seen' to Device-List** option is to be checked. However, now with **each** change of the Device List and **each** shut down of the Manager a message will be displayed reporting the change in the Device List and asking, whether it shall be saved or not. Since both columns are principally updated with **each** polling run of the Device List and thus the Device List contents is changed, the above message is bound to be displayed.

18.2.6. Adjust column size on category change

If the check mark is set for this function, the sizes of the columns in the device list will be automatically adjusted to the contents of the fields, when the category is changed. However, for the first polling run of the devices in the device list the sizes of the columns are principally determined automatically. If this function is disabled, the size of the column can be changed by drawing the column header after the first polling run, or by selecting "Adjust Column Size" below the device-list.

18.2.7. Enable custom filters:

When this function is disabled, the Custom Filter line is removed from the Device List.

18.2.8. Available Columns / Displayed Columns

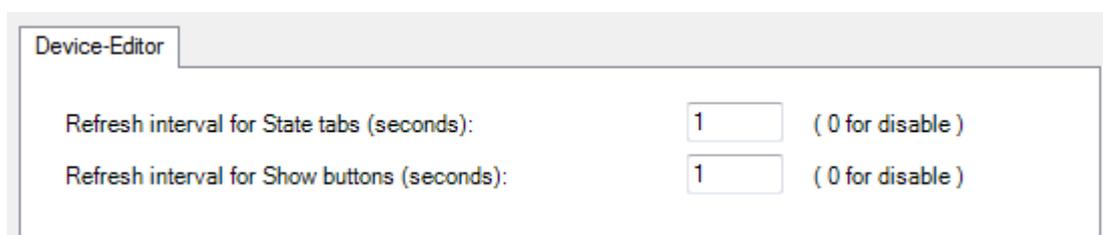
These two selection fields allow you to define which columns shall appear in the device list. Only those columns will be shown which are indicated in the 'Displayed Columns' field. Via the 'Add' and 'Remove' buttons you can then add or remove columns. Moreover, the two green buttons enable you to configure the order of the columns.

18.2.9. Use fast scrolling

Selecting this function will enable fast scrolling.

18.3. Device-Editor

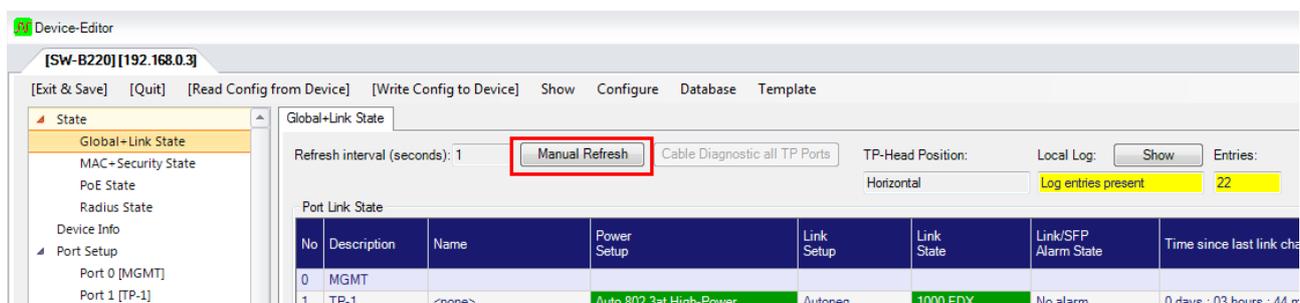
These basic settings determine the behaviour of the device editor:



The screenshot shows the 'Device-Editor' settings window. It contains two input fields for refresh intervals, both set to '1' second. The first field is labeled 'Refresh interval for State tabs (seconds):' and the second is 'Refresh interval for Show buttons (seconds):'. Both fields have a note '(0 for disable)' next to them.

18.3.1. Refresh interval for State tabs (seconds)

This period of time defines the intervals at which the 'State' tabs in the device editor are automatically updated. If this value is set to '0', no automatic update will be made. Pressing the **Manual Refresh** button will initiate an immediate update:



The screenshot shows the 'Device-Editor' interface for a device named '[SW-B220] [192.168.0.3]'. The 'State' tab is selected in the left sidebar. The main area shows the 'Global+Link State' configuration. A 'Manual Refresh' button is highlighted with a red box. Below the configuration, there is a table for 'Port Link State'.

No	Description	Name	Power Setup	Link Setup	Link State	Link/SFP Alarm State	Time since last link cha
0	MGMT						
1	TP-1	<none>	Auto 802.3at High-Power	Autoneg.	1000 FDX	No alarm	0 days : 03 hours : 44 m

18.3.2. Refresh interval for Show buttons (seconds)

This time period defines at which intervals the windows appearing after pressing a 'Show' button will be automatically refreshed. If this value is set to '0', no automatic refreshing will take place. In this case pressing the **Manual Refresh** button will trigger an update:

Spanning Tree State

```

Bridge Addr./Prio:          00c029293a43/32768 (32768 sysid 0)
Root Bridge Address/Priority: 00c0290b3ae0/32768 (32768 sysid 0)
Cost to Root:              20000
Max Age configured [Oper.]: 20 [50]
Hello Time configured [Oper.]: 2 [2]
Fwd Delay configured [Oper.]: 15 [30]
Topology Changes (Time):    1 (0 days : 0 hours : 0 min : 15 sec)
    
```

If	No	State	Role	Cost	Prio.	Design. Cost	P2P	Category
1	Forwarding	Designated	20000	128/1	20000	Yes	Edge	
2	Forwarding	Designated	200000	128/2	20000	Yes	Edge	
3	Forwarding	Root	20000	128/3	0	Yes	RSTP	
4	[no Link]							
5	[no Link]							
6	[no Link]							

Refresh interval (seconds):

Manual Refresh Close

18.4. Access

This category summarizes basic settings for access via external programs:

Access

Manager access mode: UDP/TFTP first, then SCP

Protocol version: IPv4 only

WEB browser TCP port: 80 (1...65535) [80]

WEB browser HTTPS TCP port: 443 (1...65535) [443]

Telnet client: NEXMAN default client

Browse

SSH client: NEXMAN default client

Browse

18.4.1. Manager Access Mode

The Manager Access Mode defines which protocols the Manager uses to read or write the switch configuration.

This includes the following actions:

- Reading the binary configuration
- Writing the binary configuration
- Reading the CLI configuration
- Firmware update

UDP/TFTP only:

Here file transfer of the configuration or firmware is performed via the switch-integrated TFTP server. Access to the TFTP server generally requires prior authentication, which is performed using a proprietary protocol via UDP port 50266. After successful authentication only one single Get or Put TFTP transfer may be performed. After successful completion of the TFTP transfer, access to the TFTP server is locked again.

In detail the process is as follows:

- The user enters his/her account data (name/password) into the Manager's authentication dialogue.
- The Manager encrypts name and password using a proprietary procedure.
- The encrypted account data are transmitted via UDP port 50266 to the switch. At the same time the UDP packet informs whether a TFTP Put or Get access is requested.
- The switch receives the packet and decrypts name and password.
- Depending on the "Manager Authentication Mode" setting the switch compares the data with the local Read/Write and Read/Only account or sends them to a Radius server.
- Depending on whether name, password and the access request (Get or Put) match a Read/Write or Read/Only account, the switch answers per UDP packet on port 50266 with a positive or negative acknowledgement to the Manager.

- In case of a positive acknowledgement the switch simultaneously enables access to the TFTP server. Depending on whether a Get or Put access has been authenticated, TFTP access is unlocked exclusively for Get or Put.
- Now the Manager performs the requested Get or Put access via TFTP.
- After successful completion of the TFTP file transfer, the TFTP server is locked again.

Note: The server is locked also in case of a transfer failure.

UDP/TFTP first, then SCP

This is a Manager's default setting. First, an authentication via UDP is attempted. If this attempt is successful, file transfer via TFTP will be performed.

If the switch rejects the UDP authentication, because no matching account was found, access to the switch will be aborted.

If the switch rejects the UDP authentication due to the "Manager Authentication Mode" is set to SNP, another authentication attempt via SNP will be initiated. If this attempt is successful, file transfer via SCP will be performed.

If the switch also rejects the SNP authentication, because no matching account was found, access to the switch will be aborted.

18.4.2. Protocol version

Defines which protocol version should be used to access the switch.

18.4.3. WEB Browser TCP Port

This setting defines which TCP port is used when selecting the Open WEB Browser menu option. The default port for WEB is 80.

18.4.4. WEB Browser HTTPS TCP Port

This setting defines which TCP port is used when selecting the **Open WEB Browser (HTTPS)** menu option. The default port for WEB is 443.

18.4.5. Telnet Client

This setting defines which Telnet client is started when selecting the **Open Telnet Client** menu option. If the **Use Windows default client** box is checked, the Windows-registered Telnet Client is called. If this box is not checked, you can select any Telnet application to be started instead by pressing the **Browse** button.

18.4.6. SSH Client

Here you can configure, which SSH client is launched upon selection of the **Open SSH Client** menu option. The **Browse** button allows you to select an SSH client which already has to be installed on the PC. It is called with the selected file name and the attached IP address of the device.

18.5. Folders

In the Folders category several default directories are defined. These directories will then be offered to the user as defaults when opening directories:

Application data folder (*) C:\Users\alschnei\Documents\NEXMAN

Database: C:\Users\alschnei\Documents\NEXMAN\database

Master-Configs: C:\Users\alschnei\Documents\NEXMAN\master-configs

Basic-Configs: C:\Users\alschnei\Documents\NEXMAN\basic-configs

Firmware-Images: C:\Users\alschnei\Documents\NEXMAN\firmware-images

Inventory-Lists: C:\Users\alschnei\Documents\NEXMAN\inventory-lists

Device-Lists: C:\Users\alschnei\Documents\NEXMAN\device-lists

(*) Execute NEXMAN setup to change this folder

18.5.1. Database

The configurations of the individual devices are stored in this folder. For each device a file of the name a_b_c_d.dat is created (a_b_c_d is the IP address a.b.c.d of the device). Within the folder another folder called 'history' is created containing the archived configuration.

18.5.2. Device-Lists

The device lists are stored in this folder. If several PCs are used to access this folder (e. g. because it references a network drive), NEXMAN checks whether the currently loaded device list has been modified by another PC and returns a corresponding message, if necessary.

This folder does not exist in Client/Server version.

18.5.3. Master-Configs

The master configurations are stored in this folder.

18.5.4. Basic-Configs

User-Default templates of the Basic Configurator are stored in this folder.

18.5.5. Firmware Images

The firmware images are stored in this folder.

18.5.6. Application Data Folder

The basic configuration (above Preferences) and several temporary files of NEXMAN are stored in this folder. Consequently, this folder can only be defined during installation of NEXMAN. If the position of this folder shall be changed at a later stage, this can be done by recalling the NEXMAN Setup Program.

19. NEXMAN Controller

19.1. Zero Touch Configuration

Zero Touch Configuration is a feature, which allows the Controller to do firmware updates, to copy config files and to add new devices to the database automatically.

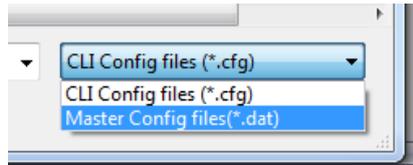
To start and stop this feature click Start **Zero Touch Configuration** in the button in the **Database Management** (see Chapter 12.4 Database Management in Client/Controller-Version).



After starting, the Controller will listen for packets sent by any device to register itself. Therefore, corresponding devices must have a **firmware version V6.xx** or above, belong to one of the **device family F40, F46 or F47** and have Zero Touch Configuration enabled, like it is at factory default. Also, all new devices must receive their IP Address from a DHCP Server first. This DHCP Server must have the Option 43 configured, to tell the device the Controllers IP Address. After that, the device will repetitive send a message to the controller until the Controller itself or any user disables Zero Touch Configuration on the switch.

When receiving a message, the Controller checks whether this device (means this MAC Address) already exists in the database. In this case, the message will be ignored. Otherwise, depending on the settings, the controller will update the firmware, copy the config file to the switch and add the switch to the database. Additionally, the switch will be added to the device list '**New Devices [system]**', which can only be seen by administrator users and not be edited manually, except removing switches from this list. Last, the switch will be added to a category describing the result of the progress and the Controller sends a notification E-Mail, if enabled.

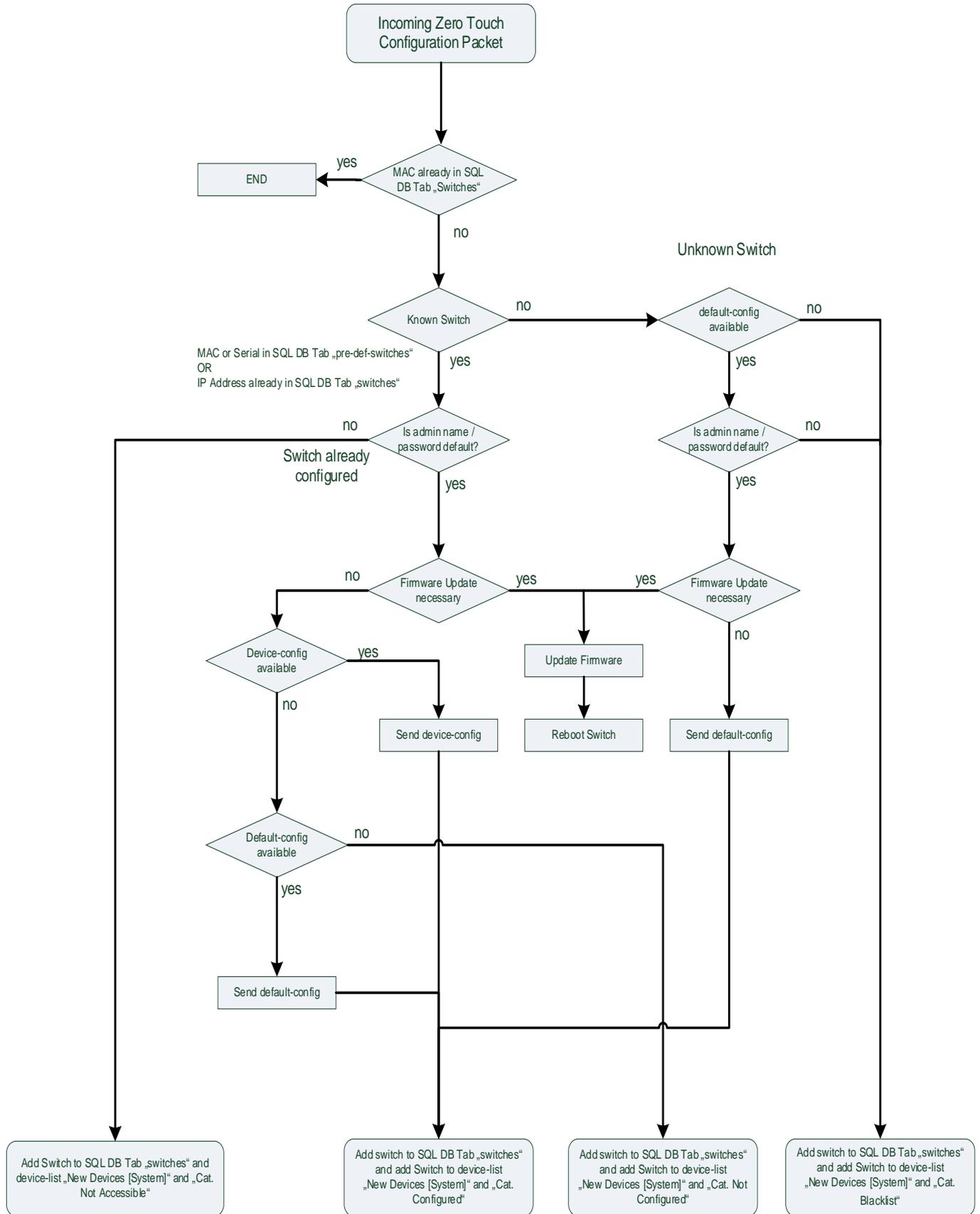
The firmware the device should be updated to can be set in the settings menu. One firmware for every device family which supports Zero Touch Configuration. Also updating the firmware can be enabled or disabled. The default CLI configuration file which should be copied to the device can be set up in the same way. This file will be taken if nothing else is specified. If there is any need to copy individual configurations to different devices, the **Predefined Device List** should be preferred. If the device to configure is listed here, the corresponding configuration file will be copied to the device, otherwise the default configuration fill will be used. Enabling or disabling the copying of configuration files will have impact on both, default configuration and Predefined Device List. It is also possible to use master configurations for Zero Touch Configuration. To select a master config, change the file type after clicking the upload button.



The corresponding xml-file containing the parameters which should be copied to the device must exist in the same directory as the master config and will be uploaded automatically.

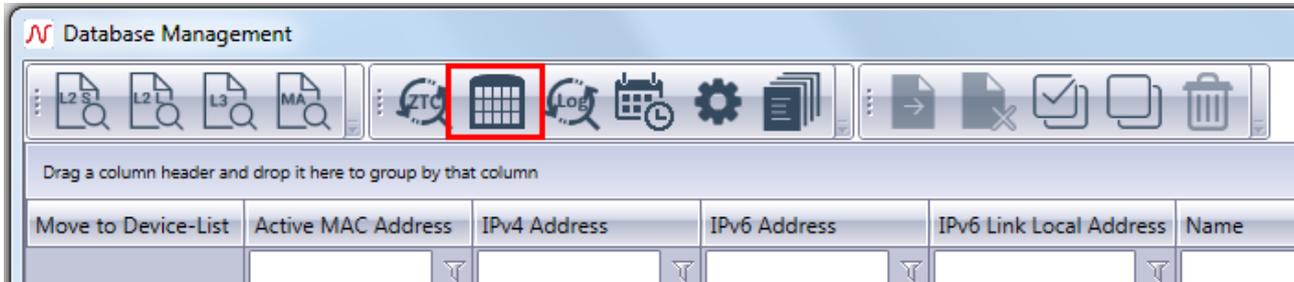
Read chapter *19.3.4 Zero Touch Configuration Settings* for more information about setting up Zero Touch Configuration.

The following picture shows the workflow of Zero Touch Configuration.

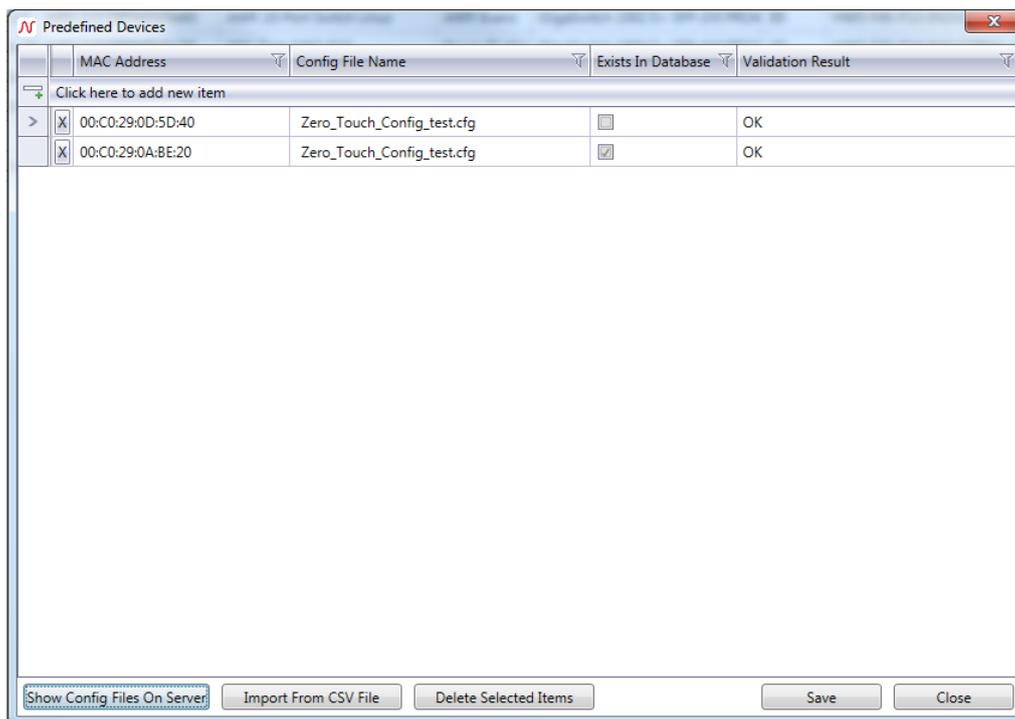


19.2. Predefined Devices

If nothing else is specified, the default configuration file set up in the Controller settings will be used for every new device depending on the device family. For an individual configuration the MAC Addresses of the devices which should be configured can be added to the **Predefined Devices List**. Click **'Predefined Devices'** to open that list.



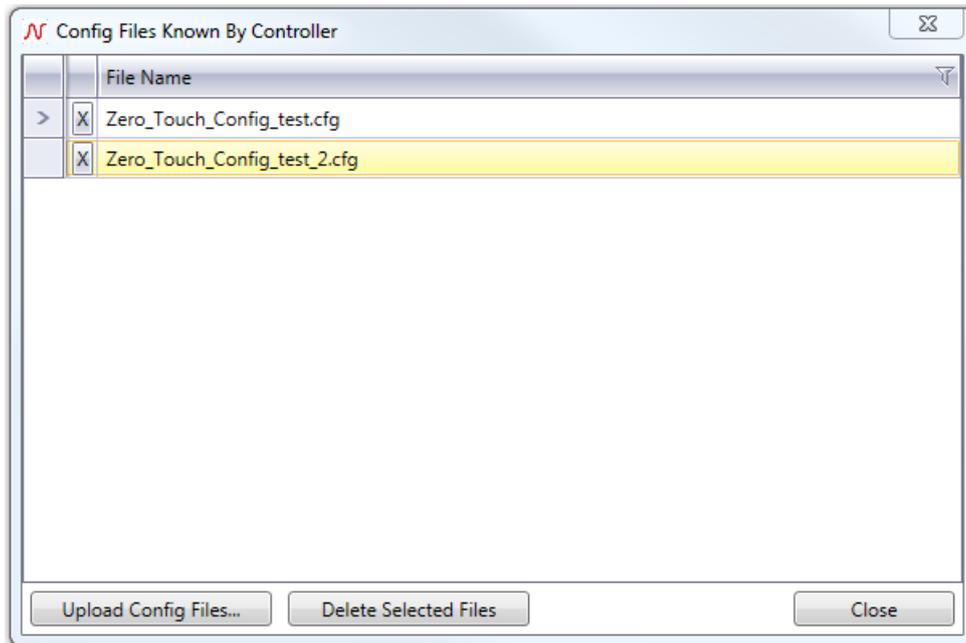
To add a new device, click on the row **'Click here to add new item'**. Add the MAC Address and select a config file from the drop-down box in column **'Config File Name'**. Only already uploaded files can be selected. The column **'Exists In Database'** indicates whether this MAC Address already has been added to the database. Validation Result shows any error possibly made during adding a new item. Click **'Save'** to store the items in the database if no error is listed.



To add multiple MAC Addresses and config files at once, click **'Import From CSV File'**. This file should only contain the MAC Address and the name of the configuration file. If the configuration file is not known to the Controller (not uploaded yet), the corresponding cell remains blank and an error is listed.

To add new files to the server, click **'Show Config Files On Server'** button. Use **'Upload Config Files...'** to select and upload new files, **'Deleted Selected Files'** to delete every selected item or the **'X'** button to delete

a specific file. Please have in mind, that only **CLI config files** or **Master Configurations** can be used for Zero Touch Configuration.



19.3. Configuration Files stored on the Server

To handle the configuration files, which are stored on the server like described in the previous chapter, the button **Config File On Server** can also be used.



19.4. Log-Messages Server

The Controller can receive different kinds of messages and store them into the database. These messages are

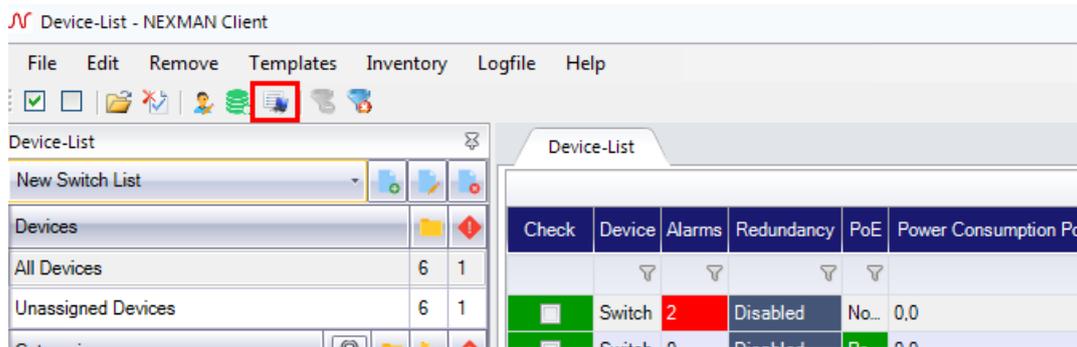
- SYSLOG Messages
- SNMP Trap Messages
- Zero Touch Configuration Messages
- Controller Notifications

To enable the listening to SYSLOG and SNMP Trap messages, click '**Start Log-Messages Listening**' inside the Database Management. Messages sent by the controller itself, like Zero Touch Config or Controller Notifications will be stored anyway.

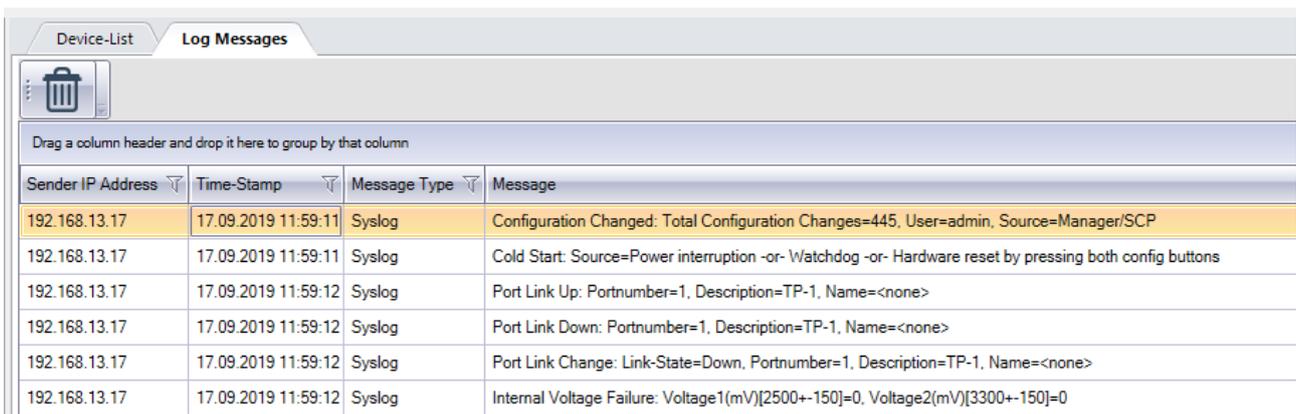


To receive SYSLOG and SNMP Trap messages, the controller’s IP Address must be entered into the device’s configuration using the Device-Editor.

To have a look at the received messages click **‘Show/Hide Log-Message’** in the main window.



The new tab page lists all types of messages concerning devices inside the current Device-List. Administrators will see all messages. The **‘Delete’** button allows the deleting of any message. The page can also be moved anywhere inside the main window and the new position will be stored until the **‘Show/Hide Log-Message’** button is clicked again.

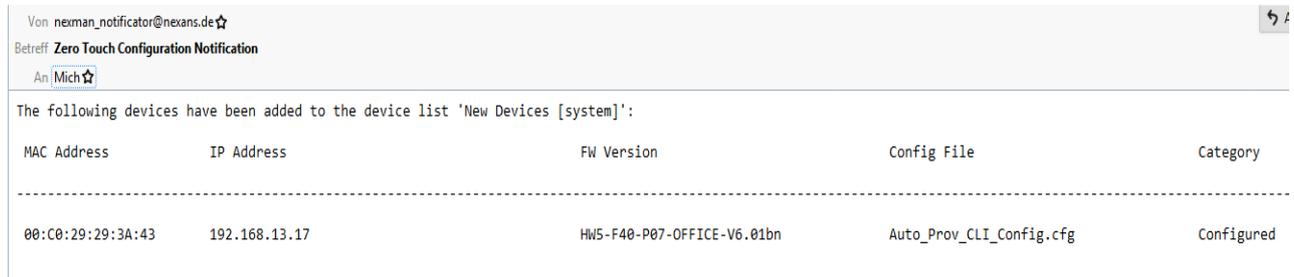


19.5. E-Mail Notifications

The Controller is able to send notifications via E-Mail to inform the user about special events. The different types of notifications can be activated in the Controller Settings menu (see chapter *19.4.5 E-Mail Notifications*).

19.5.1. Zero Touch Configuration Notifications

If activated, the controller will send an E-Mail after a specific amount of time containing the information about the devices which have been updated, configured and added to the database since the last notification. Also, it tells about the current firmware version, the used configuration file and the category the device has been moved to. The E-Mail will look like the following:



19.5.2. SYSLOG Notifications

When receiving a SYSLOG messages with a severity level equal or lower than specified in the settings the Controller will send an E-Mail like the following:



19.5.3. SNMP Trap Notifications

When receiving a SNMP Trap message, the Controller will send an E-Mail like the following:



To decrypt SNMPv3 message username, authentication password and privacy password must be entered in the Controller Settings (see chapter 19.4.6 *Log-Messages Server Settings*) and the device's SNMP protocol version must be set to 'SNMPv3 [Auth.-SHA][Priv.-AES-128]' with same SNMPv3 Trap Account credentials.

19.5.4. Controller Notifications

The Controller is also able to send notifications on its own, every time a known switch goes offline. The corresponding E-Mail will look like the following:

Von nexman_notifier@nexans.de ☆		
Betreff Switch Went Offline Notification		
An Mich ☆		
The following Controller Notifications have been received:		
Sender IP Address	Time Stamp	Message
-----	-----	-----
10.242.2.65	02.09.2019 14:46:21	Switch is offline: 10.242.2.139!

19.6. Importing Devices from file

To avoid adding Devices to the database manually or the network is scanned by any third-party tool it is possible to schedule an import process which will read and import Devices from a csv-file at a specific time. The Devices will be added to a Device-List which has to be selected in the general settings and if possible to new categories which are created like it is written in the device's location. Therefore, the csv-file must have the following format:

IP Address; Location

If the categories inside the location are separated with the same character as the IP Address and Location, the Location should be enclosed in quotation marks. The separators can be set in the settings menu, like the maximum category level, which means how many subcategories should be created.

The following picture demonstrates how the file could look like:

```

1 192.168.13.26;BuildingA\RoomB\A101
2 192.168.13.20;BuildingA\RoomB\A105
3 192.168.13.17;BuildingA\RoomB\A102
4 192.168.13.16;BuildingA\RoomB\A103
5 192.168.13.15;BuildingA\RoomB\A104
6 192.168.13.5 ;BuildingB\RoomA\B105
7 192.168.6.200;BuildingB\RoomA\B106
8 192.168.6.120;BuildingB\RoomC\B107

```

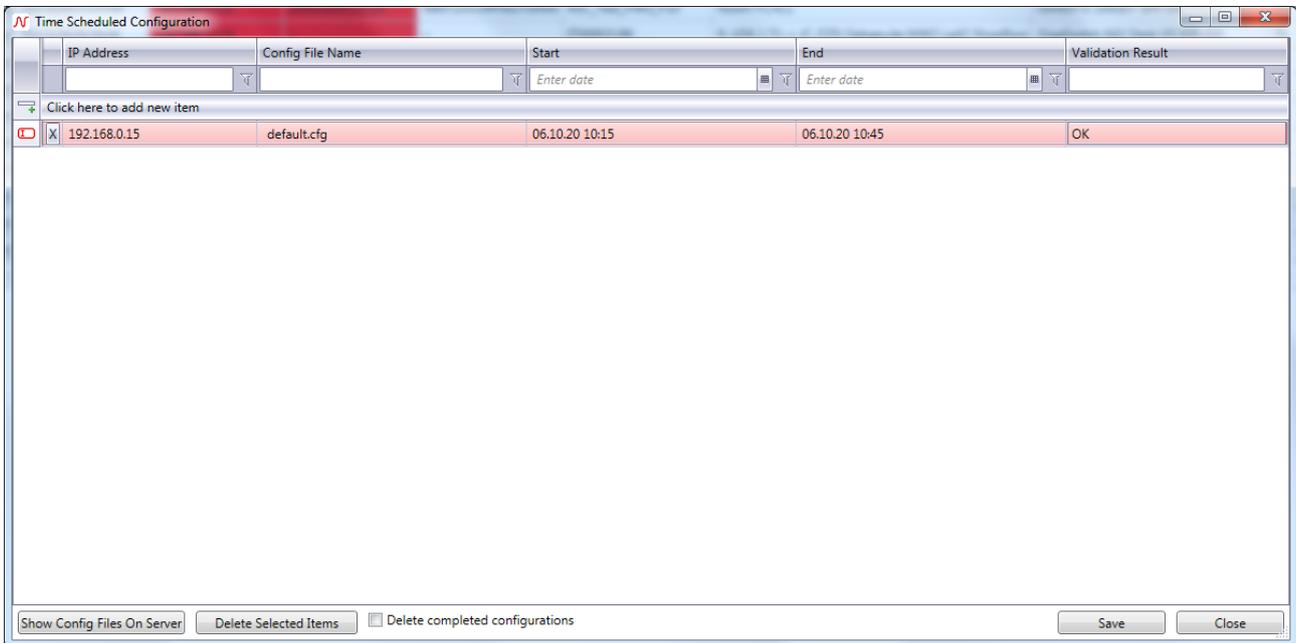
To read more about setting up time scheduled device import see chapter *19.6.1 General Settings*.

19.7. Time Scheduled Configuration

The Controller is able to copy specific configurations to devices at a given point of time. When this feature is enabled and that point of time is reached, the Controller will first read the current configuration of the target device and save it. Afterwards the new configuration will be copied to the devices. This configuration will last until the end time is reached. Then the old configuration will be copied back to the device. To enable this feature use the **Settings** menu as described in chapter *19.8.1 General Settings*. For setting up the configuration files and the corresponding devices open the **Time Scheduled Configuration** dialog by clicking the **Open Time Scheduled Configuration** button.



In this dialog several IP addresses of devices to be configured can be entered. The configuration file can be chosen in column “Config File Name”. The dropdown list shows every configuration file stored on the server. To add or remove files see chapter 19.3 *Configuration Files stored on the Server*. The start time tells the Controller when the new configuration should be copied to the device. At the end time the old configuration is copied back to the device. Both points of time must lay in the future.

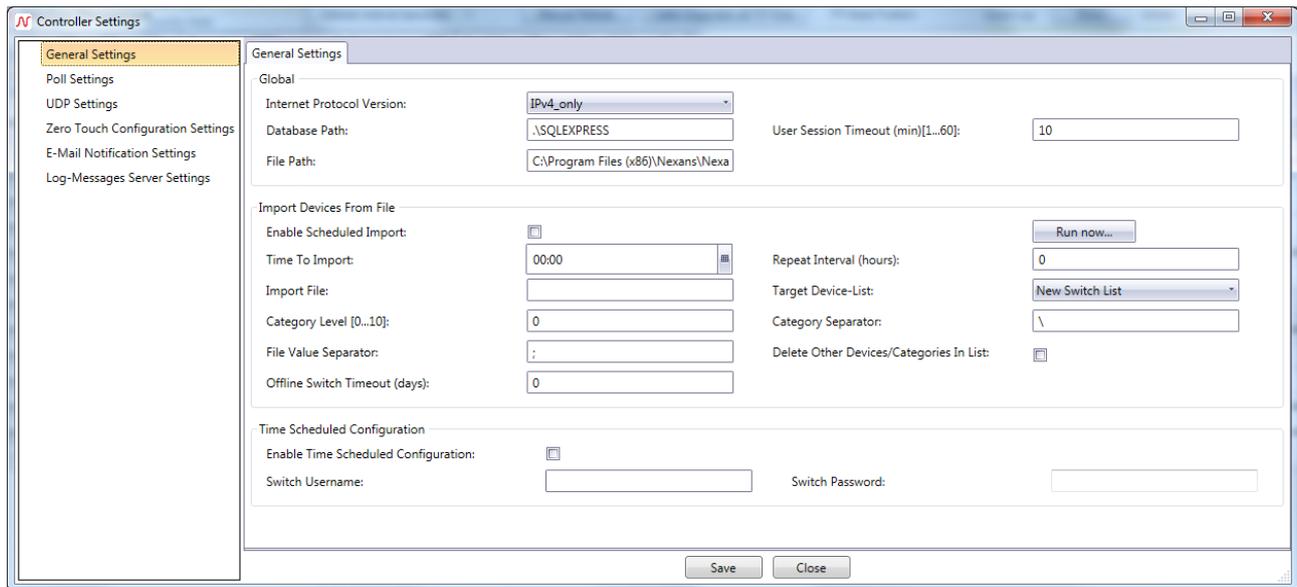


19.8. Controller Settings

To open and configure the Controller Settings click on the **Settings** button in the **Database Management** (see Chapter 12.4 *Database Management in Client/Controller-Version*).



19.8.1. General Settings



19.8.1.1. Internet Protocol Version

Defines which protocol version should be used to access the switch. Possible values are

- IPv4
- IPv6
- Both (IPv6 will be preferred)

19.8.1.2. User Session timeout

User will be automatically logged out if the controller does not receive any messages from the client for this amount of time. This setting works together with the one described in chapter *18.2.2 Poll Controller interval (seconds)*.

19.8.1.3. File Path

This directory will be used by the controller to store all of its files, like configuration or firmware files.

19.8.1.4. Database path

Changes the path to the NEXMAN Database. The Controller must be restarted if this setting is changed. Ensure that this path is correct and that the database already exists. Otherwise the Controller is not able to start anymore.

19.8.1.5. Enable scheduled import

Enable/Disable the time scheduled import of Devices from a csv-file.

19.8.1.6. Run now...

This button starts the file import immediately.

19.8.1.7. Time To Import

The time at which the Devices should be imported daily.

19.8.1.8. Repeat interval

If this value is greater than zero, the file import will be repeated after the given amount of hours. If set to zero, the import will be processed only at the 'Time To Import'.

19.8.1.9. Import File

The full path and name of the csv file which should be used for import. This file must be accessible by the Controller. Use the 'Select' button to browse inside the directories. Note, that this will happen from Client side.

19.8.1.10. Target Device List

The Device-List the switches will be imported into.

19.8.1.11. Category Level

The maximum number of subcategories created out of the location given by the csv-file.

19.8.1.12. Category Separator

The character used to separate different categories inside the csv-file.

19.8.1.13. File Value Separator:

The character used to separate different values (IP Address | Location) inside the csv-file.

19.8.1.14. Delete Other Devices/Categories In List

When checked, all devices and categories which exist in the target Device-List, but not in the csv-file will be deleted.

19.8.1.15. Offline Switches Timeout (days):

If a Device inside the target device list is offline for than the given amount of days, it will be deleted from this list. If this value is equal to '0', this function is deactivated.

19.8.1.16. Enable Time Scheduled Configuration

Enable/Disable time scheduled configuration if Devices.

19.8.1.17. Switch Username

The username to access the devices which should be configured.

19.8.1.18. Switch Password

The password to access the devices which should be configured.

19.8.2. Poll Settings

Setting	Value
Poll Interval (sec)	1
Poll Threads Count (0...16)	16
Ping Retries (0...10)	2
Ping Interval (sec)[1...3]	1
Ping Timeout (sec)[1...10]	2

19.8.2.1. Poll Interval

Time to wait until the Poll Engine restarts polling known switches. If it takes more time to poll all switches in database, the Poll Engine will restart immediately.

19.8.2.2. Ping Threads Count

Number of simultaneous poll threads.

19.8.2.3. Ping Retries

Number of retries if a poll fails, for example if device is offline.

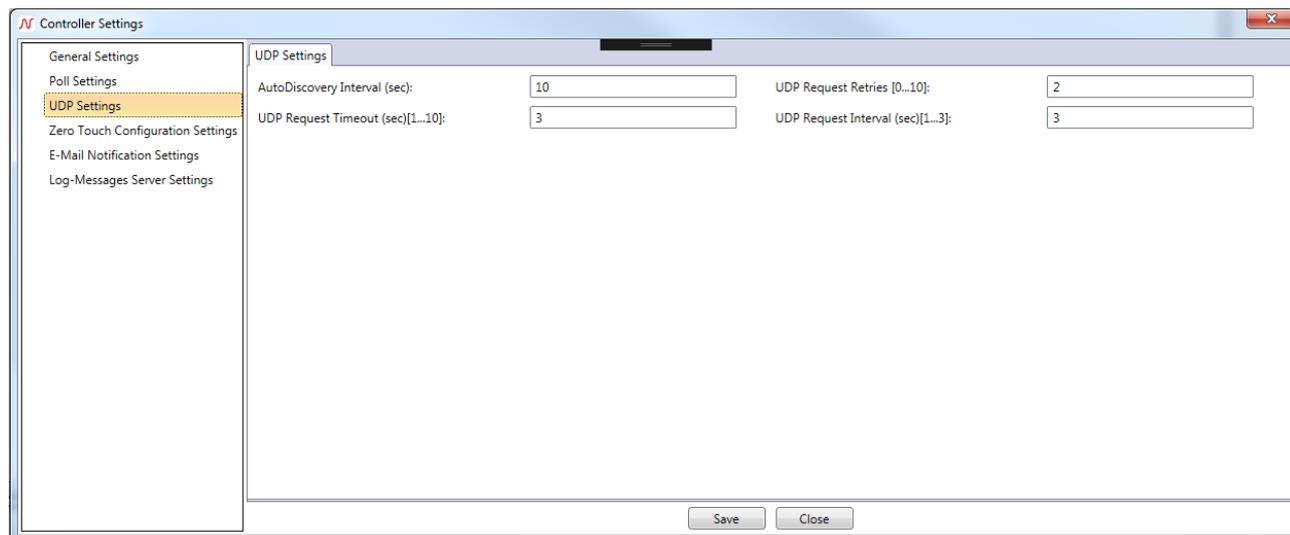
19.8.2.4. Ping Interval

Time to wait before retrying to poll a device.

19.8.2.5. Ping Timeout

Timeout for a poll action.

19.8.3. UDP Settings



19.8.3.1. Autodiscovery Interval

Time to send a discovery broadcast message in Discovery Mode.

19.8.3.2. UDP Request Timeout

Timeout to cancel the receiving of any UDP message.

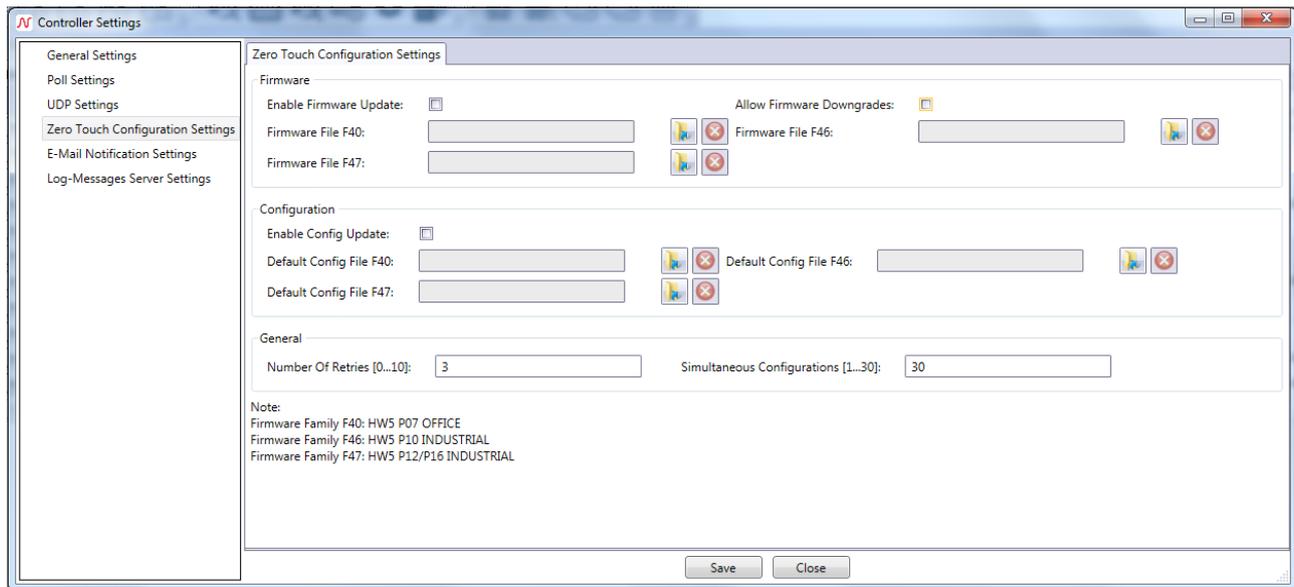
19.8.3.3. UDP Request Retries

Number of retries if any UDP request fails.

19.8.3.4. UDP Request Interval

Time to wait before retrying a UDP request.

19.8.4. Zero Touch Configuration Settings



19.8.4.1. Enable Firmware Update

Allows the controller to update the firmware of new devices automatically if Zero Touch Configuration is active.

19.8.4.2. Allow Firmware Downgrades

Allows the controller to downgrade the firmware of new devices.

19.8.4.3. Firmware File F40

The firmware file to be taken by the controller to update devices of family F40 in Zero Touch Configuration mode (HW5 P07 Office Switch).

19.8.4.4. Firmware File F46

The firmware file to be taken by the controller to update devices of family F46 in Zero Touch Configuration mode (HW5 P10 Industrial Switch).

19.8.4.5. Firmware File F47

The firmware file to be taken by the controller to update devices of family F47 in Zero Touch Configuration mode (HW5 P12/P16 Industrial Switch).

19.8.4.6. Enable Config Update

Allows the Controller to copy a configuration file (default config or from predefined list) to new devices if Zero Touch Configuration is active.

19.8.4.7. Default Config File F40

The config file to be copied to devices of family F40 in Zero Touch Configuration mode if device is not specified in Predefined List (HW5 P07 Office Switch).

19.8.4.8. Default Config File F46

The config file to be copied to devices of family F46 in Zero Touch Configuration mode if device is not specified in Predefined List (HW5 P10 Industrial Switch).

19.8.4.9. Default Config File F47

The config file to be copied to devices of family F47 in Zero Touch Configuration mode if device is not specified in Predefined List (HW5 P12/P16 Industrial Switch).

19.8.4.10. Number of Retries

Number of retries if firmware update or configuration failed.

19.8.4.11. Simultaneous Configurations

Number of simultaneously updated or configured devices.

19.8.5. E-Mail Notification Settings

The screenshot shows the 'Controller Settings' window with the 'E-Mail Notification Settings' tab selected. The window is divided into a left sidebar and a main content area. The sidebar lists various settings categories, with 'E-Mail Notification Settings' highlighted. The main content area contains several sections of configuration options:

- E-Mail Server:** Includes fields for 'Send From E-Mail Address', 'Password', 'Recipient E-Mail Address 1', 'Recipient E-Mail Address 2', 'Recipient E-Mail Address 3', 'SMTP Server', and 'SMTP Server Port Number [1...65535]' (set to 1). There is also a checkbox for 'Use SSL'.
- Syslog / SNMP Trap Messages:** Includes a checkbox for 'Send Syslog / SNMP Trap Notifications' and a text input for 'Syslog Notifications Severity Level [0..7]' (set to 1).
- Zero Touch Configuration:** Includes a checkbox for 'Send Zero Touch Configuration Notifications'.
- Controller Notifications:** Includes checkboxes for 'Send Switch Is Offline Notifications' and 'Send Settings Changed Notifications'.
- General Settings:** Includes a text input for 'Send Notifications Every x Minutes' (set to 1).

At the bottom of the window are 'Save' and 'Close' buttons.

19.8.5.1. Send From E-Mail Address

This E-Mail address is used to send notifications to the recipients.

19.8.5.2. Password

The password of the 'Send From' E-Mail account.

19.8.5.3. Recipient E-Mail Address 1

First E-Mail address which should receive any kind of notification.

19.8.5.4. Recipient E-Mail Address 2

Second E-Mail address which should receive any kind of notification.

19.8.5.5. Recipient E-Mail Address 3

Third E-Mail address which should receive any kind of notification.

19.8.5.6. SMTP Server

The name or IP Address of the SMTP Server which should be used to send E-Mail notifications.

19.8.5.7. SMTP Server Port Number

The Remote TCP/IP Port number of the SMTP Server.

19.8.5.8. Use SSL

Use SSL for sending E-Mails.

19.8.5.9. Send Syslog / SNMP Trap Notifications

Enable sending of Syslog and SNMP Trap notifications via E-Mail.

19.8.5.10. Syslog Notifications Severity Level

Syslog notifications will only be send if their severity level is lower or equal to this number.

19.8.5.11. Send Zero Touch Configuration Notifications

Enable sending of notifications about new devices which have been automatically configured and added to the database by Zero Touch Configuration.

19.8.5.12. Send Switch Is Offline Notifications

Enable sending of notifications if the controller recognizes that a switch went offline.

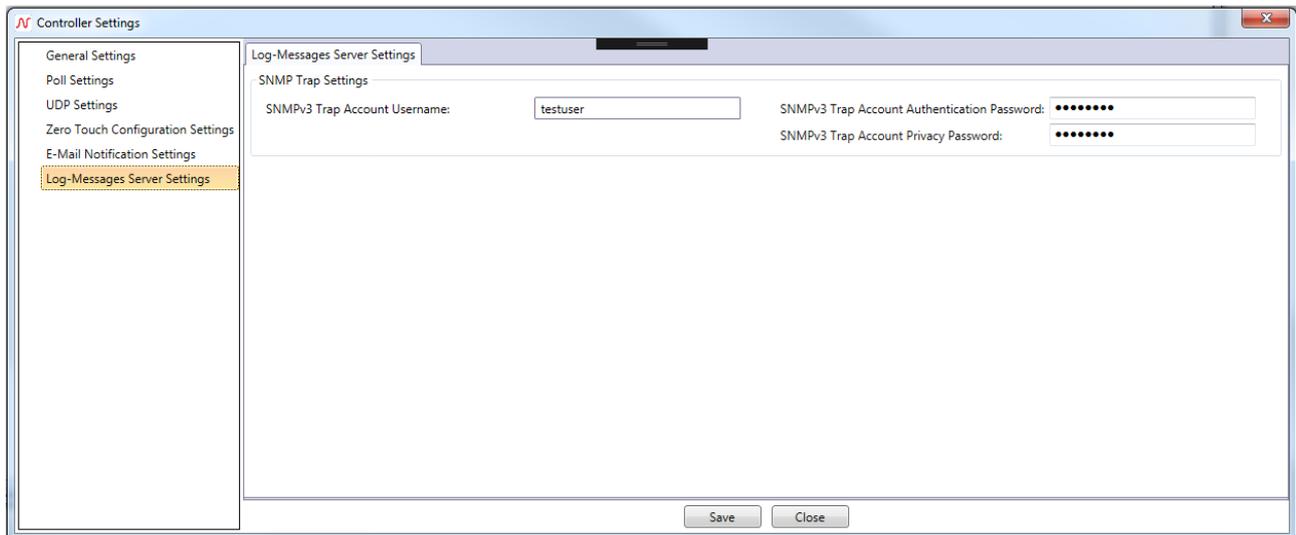
19.8.5.1. Send Settings Changed Notifications

Enable sending of notifications if the settings like starting Zero Touch Configuration or listening to SYSLOG messages have changed.

19.8.5.1. Send Notifications Every x Minutes

If this value is greater than zero, the notifications of Zero Touch Configuration or offline switches will be collected for this timespan and send in one E-Mail altogether. If this value is equal to zero, E-Mails are send immediately.

19.8.6. Log-Messages Server Settings



The screenshot shows the 'Controller Settings' window with the 'Log-Messages Server Settings' tab selected. The left sidebar lists various settings categories, with 'Log-Messages Server Settings' highlighted. The main area contains the following fields:

- SNMP Trap Settings
- SNMPv3 Trap Account Username:
- SNMPv3 Trap Account Authentication Password:
- SNMPv3 Trap Account Privacy Password:

At the bottom of the window, there are 'Save' and 'Close' buttons.

19.8.6.1. SNMPv3 Trap Account Username

The username to decrypt SNMPv3 Trap messages. (SNMPv3 [Auth.-SHA] [Priv.-AES-128] only)

19.8.6.2. SNMPv3 Trap Account Authentication Password

The authentication password to decrypt SNMPv3 Trap messages. (SNMPv3 [Auth.-SHA] [Priv.-AES-128] only)

19.8.6.3. SNMPv3 Trap Account Privacy Password

The privacy password to decrypt SNMPv3 Trap messages. (SNMPv3 [Auth.-SHA] [Priv.-AES-128] only)

20. Release notes

From release V3.64 all release notes (switch manager, switch basic configurator and the switch firmware) are located in a separate manual called **Nexans Switch Management - Release Notes**.

Subject to modifications.



Nexans networking solutions are employed all over the world and have demonstrated their reliability in a variety of applications. Our references include leading companies of the world, universities, industrial enterprises, hospitals, government authorities and banks. A LAN system which can grow with the requirements of its users must be designed from the very beginning in such way that it is flexible enough to support frequent moves, adds and changes, in particular.

With more than 25 years of experience in the development and production of optical solutions, the systems from Nexans provide the reliability and the security you can expect from your network.



Nexans Deutschland GmbH • Advanced Networking Solutions

Bonnenbroicher Str. 2-14 • 41238 Mönchengladbach • Tel +49(0)2166272985 • Fax +49(0)2166272499