



Siemens  
Industry  
Online  
Support

APPLICATION EXAMPLE

# Using and Understanding SINEC NMS

SINEC NMS V3.0

**SIEMENS**

# Legal information

## Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. **The application examples are not subject to standard tests and quality inspections of a chargeable product and may contain functional and performance defects or other faults and security vulnerabilities. You are responsible for the proper and safe operation of the products in accordance with all applicable regulations, including checking and customizing the application example for your system, and ensuring that only trained personnel use it in a way that prevents property damage or injury to persons. You are solely responsible for any productive use.**

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. Any further use of the application examples is explicitly not permitted and further rights are not granted. You are not allowed to use application examples in any other way, including, without limitation, for any direct or indirect training or enhancements of AI models.

## Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

## Other information

Siemens reserves the right to make changes to the application examples at any time without notice and to terminate your use of the application examples at any time. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://www.siemens.com/global/en/general/terms-of-use.html>) shall also apply.

## Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit [www.siemens.com/cybersecurity-industry](https://www.siemens.com/cybersecurity-industry).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://www.siemens.com/cert>.

# Table of Contents

|           |                                                                    |           |
|-----------|--------------------------------------------------------------------|-----------|
| <b>1.</b> | <b>Introduction .....</b>                                          | <b>5</b>  |
| 1.1.      | Overview.....                                                      | 5         |
| 1.2.      | SINEC NMS.....                                                     | 6         |
| 1.3.      | Reference System .....                                             | 8         |
| <b>2.</b> | <b>Setting Up and Starting SINEC NMS.....</b>                      | <b>10</b> |
| 2.1.      | Installation.....                                                  | 10        |
| 2.1.1.    | Useful Information about Installation.....                         | 10        |
| 2.1.2.    | Installing SINEC NMS .....                                         | 11        |
| 2.2.      | SINEC NMS License Model and Automation License Manager.....        | 14        |
| 2.3.      | Web Interface.....                                                 | 16        |
| 2.3.1.    | Useful Information about the Web Interface.....                    | 16        |
| 2.3.2.    | Initial Login to the Control Web Interface .....                   | 17        |
| <b>3.</b> | <b>Control: Performing System Administration .....</b>             | <b>21</b> |
| 3.1.      | Operation Parameter Profile .....                                  | 21        |
| 3.1.1.    | Useful Information about the Operation Parameter Profile.....      | 21        |
| 3.1.2.    | Initial Credentials.....                                           | 22        |
| 3.2.      | Operation Management.....                                          | 24        |
| 3.2.1.    | Useful Information about Operation Management .....                | 24        |
| 3.2.2.    | Adding an Operation to the System .....                            | 26        |
| 3.2.3.    | Exporting Certificates.....                                        | 29        |
| <b>4.</b> | <b>Operation: Performing Initial Commissioning.....</b>            | <b>30</b> |
| 4.1.      | Useful Information about Initial Commissioning.....                | 30        |
| 4.2.      | Performing the Initial Commissioning of a Multiple Node .....      | 30        |
| <b>5.</b> | <b>Network Monitoring .....</b>                                    | <b>32</b> |
| 5.1.      | Detecting Devices in the Network.....                              | 32        |
| 5.1.1.    | Useful Information about the Network Scan.....                     | 32        |
| 5.1.2.    | Useful Information about Monitoring on the Control .....           | 33        |
| 5.1.3.    | Useful Information about Monitoring on the Operations.....         | 35        |
| 5.1.4.    | Manually or Automatically Starting a Network Scan for Control..... | 38        |
| <b>6.</b> | <b>Operation: Understanding and Filtering the Events List.....</b> | <b>40</b> |
| 6.1.      | Useful Information about Events .....                              | 40        |
| 6.2.      | Adapting the Event List.....                                       | 42        |
| <b>7.</b> | <b>Operation: Understanding and Using Topology .....</b>           | <b>48</b> |
| 7.1.      | Useful Information on Topology .....                               | 48        |

|           |                                       |           |
|-----------|---------------------------------------|-----------|
| 7.1.1.    | General Information .....             | 48        |
| 7.1.2.    | Work Areas and Operation .....        | 48        |
| 7.1.3.    | Edit Mode.....                        | 50        |
| 7.1.4.    | Online Mode .....                     | 51        |
| 7.1.5.    | Views.....                            | 51        |
| 7.1.6.    | Topological Representation .....      | 51        |
| 7.2.      | Making Network Topology Visible.....  | 53        |
| 7.2.1.    | Opening and Setting up Topology ..... | 53        |
| 7.2.2.    | Topology in the Online Mode .....     | 63        |
| <b>8.</b> | <b>Other SINEC NMS Features.....</b>  | <b>64</b> |
| <b>9.</b> | <b>Appendix .....</b>                 | <b>65</b> |
| 9.1.      | Service and support .....             | 65        |
| 9.2.      | Links and literature .....            | 66        |
| 9.3.      | Change documentation .....            | 66        |

# 1. Introduction

## 1.1. Overview

### Motivation

This document assists the user and introduces them to the basic functions and settings of SINEC NMS. The section structure guides you step-by-step through the setting options of SINEC NMS and introduces you to the necessary fundamentals.

### Guide to the documentation

In this document, we discuss the following technological key points:

- Setting up SINEC NMS
- System administration in Control
- Initial commissioning of the Operations
- Network monitoring
- Fundamentals of Events in Operations
- Explanation of topology types in Operations

The sections and sub-sections are usually identical and have a modular structure.

The sections begin with the theory section "Useful information", which explains the fundamentals and principles of the function. This section is followed by a practical section consisting of detailed instructions with screenshots.

### NOTE

To get an overview of the function, read the theory section.

If you already have basic knowledge of SINEC NMS, you can skip the theory section and start with the practical section.

## 1.2. SINEC NMS

The SINEC NMS software is a network management system for monitoring and managing industrial networks. It enables you to fully visualize and monitor networks. Using SNMP with simultaneous diagnostics via SIMATIC and PROFINET mechanisms, many aspects of plant and network diagnostics can be mapped in a single tool. The SINEC NMS distributed approach enables network infrastructure expansion at any time.

Features of SINEC NMS are among others:

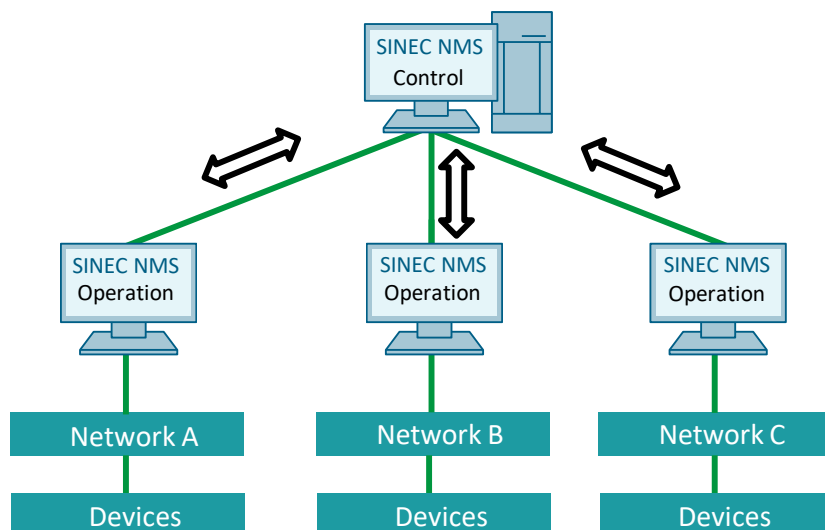
- SINEC NMS detects all devices in the network. This provides a constantly updated overview of all installed components including all essential properties in the network.
- The plant topology is automatically read out, depicted and monitored for changes.
- Diagnostic data is collected from all network stations and stored centrally. The overall state of the network is displayed via a central dashboard.
- Statistics can be displayed and evaluated over any period of time. Thus, historical Events can also be easily evaluated.
- Configurable test patterns enable essential network properties to be repeatedly checked and documented.
- A variety of interfaces (e.g., HTTPS, OPC UA, REST API) enable the visualization and further processing of network and diagnostic data in higher-level systems.
- Policy-based configuration of various network radio functions.
- Mass Operation for firmware update for single or multiple SCALANCE components.
- Central management of roles and permissions for the entire system.
- Security-relevant vulnerabilities of Siemens network devices are monitored by the Vulnerability Notification module. This functionality is optional and requires a license.

## Components

SINEC NMS is a software for monitoring and administration of networks and their devices. It consists of the "Control" component and at least one "Operation" component.

The Control is used for monitoring and administration of the entire network. An Operation is responsible for the monitoring and administration of a part of the network.

Figure 1-1



The monitoring settings to be used by the Operations are configured centrally on the Control and then synchronized to the Operations. The Operations determine the monitoring data from the devices and deliver selected data and summarized status information to the Control.

An Operation can be installed on the same PC as the Control or on another PC. The Control and each Operation has its own web interface for displaying monitoring data and administering the network.

### NOTE

Before the communication link between an Operation and the Control can be established for the first time, the Operation must authenticate to the Control with a certificate. Without this authentication, communication between this Operation and the Control and navigation in the web interface of the Operation is not possible.

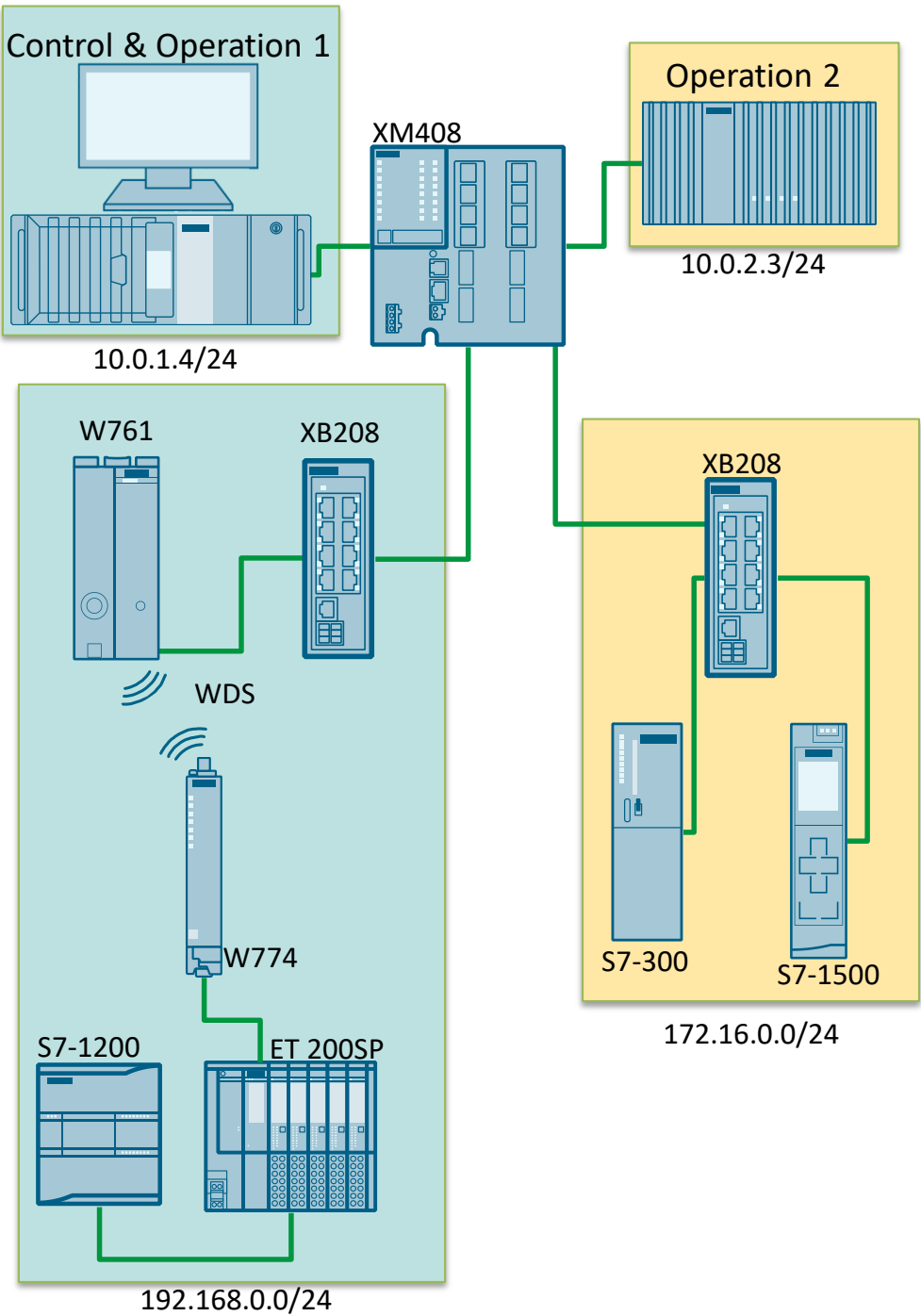
### 1.3. Reference System

**Network setup**

In order to simplify the entry into the SINEC NMS and to improve understanding of the functions, this document is based on the reference system. To demonstrate the distributed approach of SINEC NMS, the reference system consists of 2 Operations and a common Control. Each Operation has its own network with devices to be monitored and configured.

The following Figure shows you the distributed approach of the reference installation:

Figure 1-2



Network configuration

The IP addresses are defined as follows:

Table 1-1

| Module                | IP address   | Router      |
|-----------------------|--------------|-------------|
| XB208                 | 172.16.0.2   | 172.16.0.1  |
| CPU 317-2 PN/DP       | 172.16.0.5   | 172.16.0.1  |
| CPU 1513-1 PN         | 172.16.0.3   | 172.16.0.1  |
| XB208                 | 192.168.0.2  | 192.168.0.1 |
| W761                  | 192.168.0.14 | 192.168.0.1 |
| W774                  | 192.168.0.13 | 192.168.0.1 |
| CPU 1212C             | 192.168.0.10 | 192.168.0.1 |
| ET 200SP              | 192.168.0.11 | 192.168.0.1 |
| XM408-4C              | 10.0.0.1     |             |
| Control & Operation 1 | 10.0.1.4     | 10.0.1.1    |
| Operation 2           | 10.0.2.3     | 10.0.2.1    |

NOTE

The Control and Operations must be accessible via static IP addresses. Do not use IP address configuration via DHCP server. This applies to single node and multiple node installations.

SCALANCE XM408-4C

The Industrial Ethernet Switch SCALANCE XM408-4C acts as a router and connects all subnets with each other. Router ports are configured in the SCALANCE device.

The following Table shows which ports belong to which subnet:

Table 1-2

| Port | Subnet      |
|------|-------------|
| P1.2 | 10.0.1.1    |
| P1.3 | 10.0.2.1    |
| P1.4 | 172.16.0.1  |
| P1.5 | 192.168.0.1 |

## 2. Setting Up and Starting SINEC NMS

### 2.1. Installation

#### 2.1.1. Useful Information about Installation

##### SINEC NMS installation options

When installing SINEC NMS, you can select which components of SINEC NMS are to be installed:

- Single node installation: The Control and an Operation are installed on the same PC.
- Multiple node installation: The Control or an Operation is installed.

**NOTE**

SINEC NMS must be installed on each computer that is to be used as a Control or Operation.

##### Additional UMC software

In addition to installing the Control and Operation, you can also choose whether to install a UMC server or use an existing UMC server. The connection of SINEC NMS to UMC makes it possible to manage user data centrally in UMC and to integrate this user data into SINEC NMS via UMC user groups. Users and user groups can be transferred from a Microsoft Active Directory (AD). Two-factor authentication is possible using UMC.

You will set up the UMC server during installation.

**NOTE**

By using UMC users, you can employ single sign-on for Control & Operation.

##### Licensing instructions

In order to operate SINEC NMS, a license is required. Different license types are available, which differ in the number of monitored and configurable devices.

You can find an overview of the available licenses in the SINEC NMS manual (see \3\ in [Section 9.2](#)).

##### SINEC NMS test

A trial license is available to familiarize yourself with and test SINEC NMS. The trial license is included in the installation and has a usage period of 21 days. The license key is automatically activated if no other license key was found by the Automation License Manager (ALM [Section 2.2](#)) when SINEC NMS was started for the first time.

There are the following restrictions compared to the full version:

- Max. 100 devices in monitoring (management status "Monitored")
- Max. 3 devices with configuration options (management status "Managed")
- Restricted validation report
- Generating images of the topology representation is not possible

**NOTE**

It is recommended to use a valid license before the initial scanning of devices. Due to the restrictions of a trial license, the devices must be upgraded to managed status afterwards.

2.1.2. Installing SINEC NMS

Obtain software

The SINEC NMS software can be downloaded via the SiePortal (see 14\ in [Section 9.2](#)).

| Name                                                                                            | Date modified     | Type        | Size         |
|-------------------------------------------------------------------------------------------------|-------------------|-------------|--------------|
|  SINECNMS_V3.0 | 7/11/2024 2:22 PM | Application | 2,398,634 KB |

Alternatively, you can purchase the software as a software package or as an OSD (Online Software Download).

Installation overview

The reference system consists of one Control and two Operations.

For the "Control & Operation 1" unit, install the following components:

- Single node installation
- UMC server

The unit "Operation 2" is a multiple node installation and contains only the Operation. A UMC Server is not necessary.

Software requirements

The following requirements apply to the SINEC NMS V3.0 software to be used:

Table 2-1

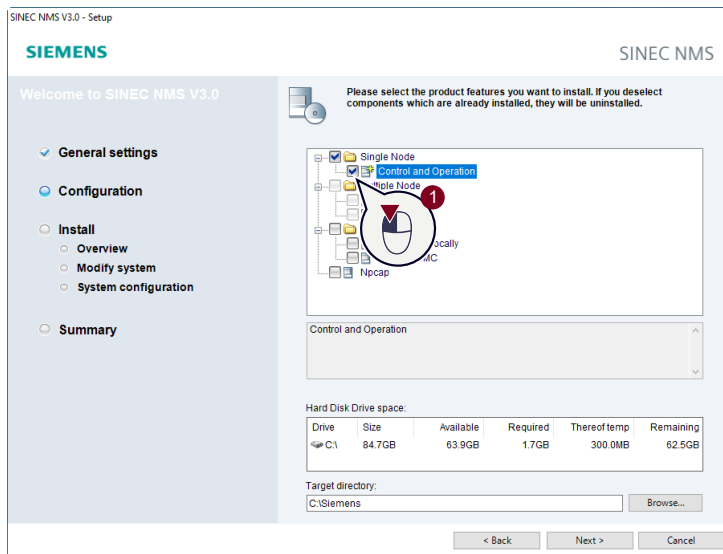
|                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating system                     | <ul style="list-style-type: none"><li>• Windows 11 Professional / Enterprise<ul style="list-style-type: none"><li>- Windows 11 23H2</li><li>- Windows 11 22H2</li></ul></li><li>• Windows 10 Professional / Enterprise<ul style="list-style-type: none"><li>- Windows 10 21H2 LTSC</li><li>- Windows 10 22H2</li></ul>Minimum build 16299</li><li>• Windows Server 2022 LTSC</li></ul> |
| Supported operating system languages | <ul style="list-style-type: none"><li>• German</li><li>• English</li><li>• French</li><li>• Spanish</li><li>• Italian</li><li>• Chinese</li></ul>                                                                                                                                                                                                                                      |
| Web browser                          | <ul style="list-style-type: none"><li>• Google Chrome 124 or higher</li><li>• Firefox 125 or later</li><li>• Microsoft Edge Chromium 124 or higher</li></ul>                                                                                                                                                                                                                           |
| Screen resolution                    | 1920 x 1080 pixels                                                                                                                                                                                                                                                                                                                                                                     |

## Software installation

To install a Control or Operation, proceed as follows:

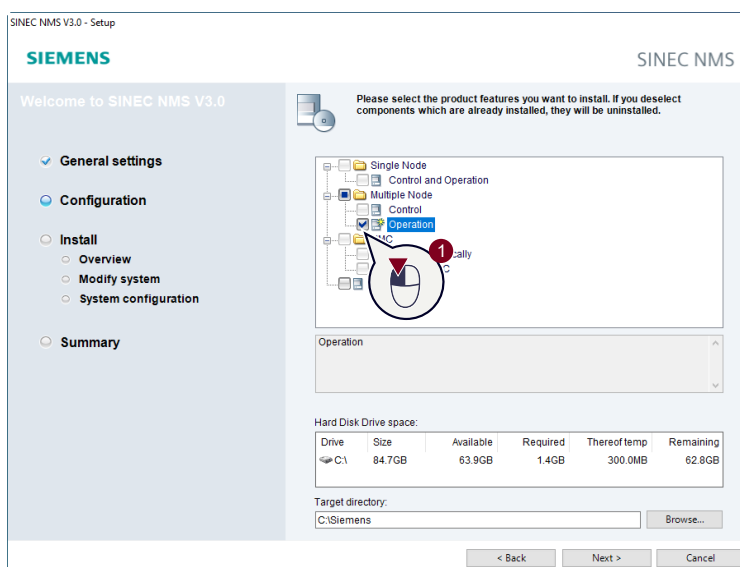
1. Start the file "SINECNMS\_V3.0.exe" with administrator permissions and select a language for the installation wizard. Then click the "Next" button.
2. Accept the license agreement. Then click the "Next" button.
3. Specify the folder to which the setup files will be extracted. Then click the "Next" button.
4. Define the languages to be installed and click the "Next" button.
5. Select which components of SINEC NMS should be installed. The following options are available:
  - Single node installation: The Control and an Operation are installed on the same PC.

Figure 2-1



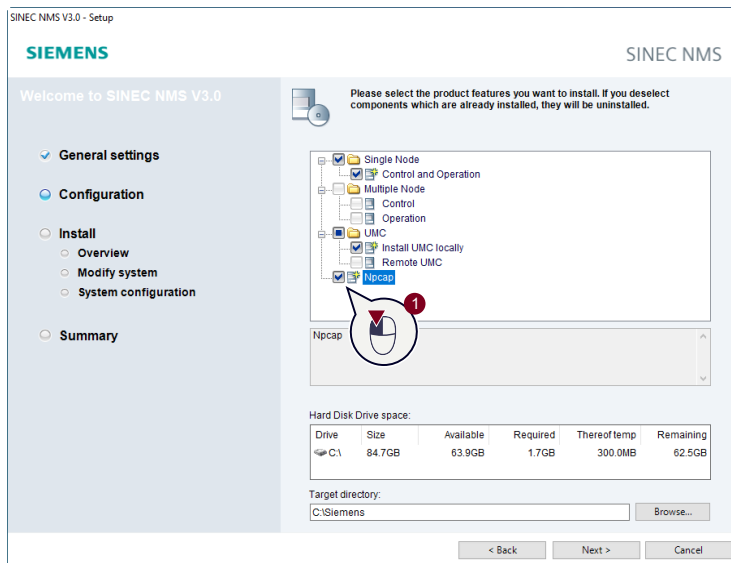
- Multiple node installation: The Control or an Operation is installed.

Figure 2-2



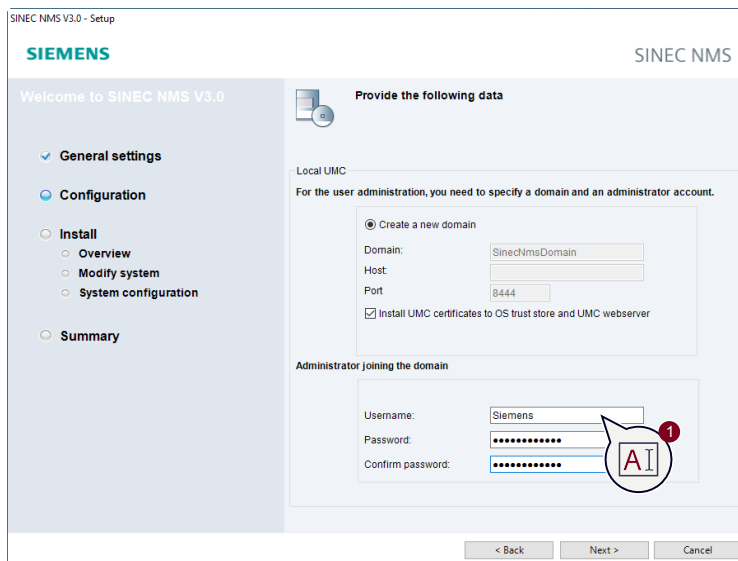
6. Select whether you want to install a UMC server or use an existing UMC server. If you do not need a UMC server, do not select either of the two options. Click on "Next".

Figure 2-3



7. Select whether a new domain is to be created or whether you want to use an existing domain. Define a name and password for the administrator to be added to this domain. To complete the configuration of UMC, click "Next".

Figure 2-4



8. Select the desired Trap service to be used.

**NOTE** For SNMPv3 traps, the SINEC NMS trap service is required.

9. Follow the instructions of the installation wizard.
10. Restart the PC after the installation is complete.
11. After restarting the PC, SINEC NMS is started automatically and you can log on to the web interface.
12. Install additional existing service packs to use the latest version of SINEC NMS.

**Result:** SINEC NMS is installed and you can log in to the web interface.

## 2.2. SINEC NMS License Model and Automation License Manager

The license model of SINEC NMS is presented below. This license model is valid from version 2.0 and is applicable to newer versions. A purchased license is time-dependent and can be used in newer versions of SINEC NMS.

Figure 2-5

### License model

#### 1. Subscription model/licenses with term

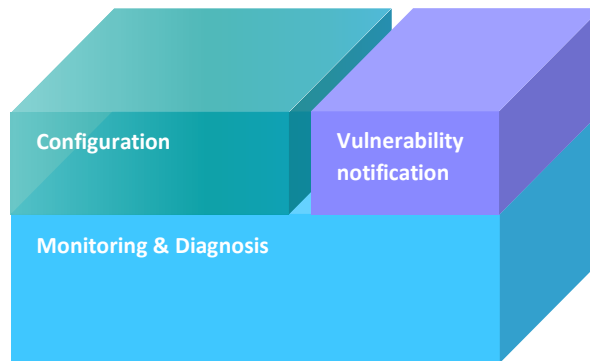
- License renews annually
- Alternatively 3 or 5 years
- Updates included

#### 2. Sizes

- from XS 100 to XXL 37500 devices

#### 3. Types

- Monitoring (necessary)
- Configuration (optional)
- Vulnerability (optional)



### Term-based licensing

Each license is limited in term. In addition to licenses with annual renewal, there are also licenses with a fixed term of 3 or 5 years. After the end of the term or if the license has not been renewed, SINEC NMS can no longer be operated productively. A new valid license is required.

### Size-based licensing

Different size options are offered. From XS (100 nodes) to S (up to 500 monitored devices), M (up to 1000), L (up to 3000) to XL (up to 10,000) and up to the maximum size of 37500 with the XXL license. If the limit of a license is reached, a larger model must be chosen.

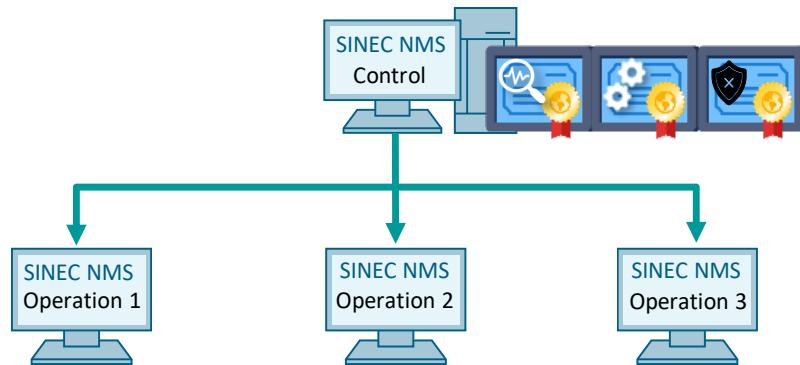
### Types of licensing

SINEC NMS offers 3 types of licenses:

- **01 – Monitoring:** A monitoring license is always necessary for monitoring. Basic functionalities are asset detection, inventory, topology, reporting, etc.
- **02 – Configuration:** If management tasks are to be possible, a configuration license is required. Basic functionalities are firmware management, configuration backups, or configuration changes.
- **03 – Vulnerability Notifications:** With the Vulnerability Notifications add-on, the connection to the vulnerability database is possible. This makes it possible to monitor the device status with regard to security-relevant vulnerabilities.

Licenses are imported centrally on the control in the ALM (Siemens Automation License Manager). The dynamic assignment of licenses to individual Operations enables low overhead and high flexibility. Up to 500 devices can be monitored per Operation. Up to 75 Operations can be connected to one control. For example, a SINEC NMS setup can monitor and manage up to 37,500 devices. If there are more devices than licenses, only the number of licensed devices is monitored, the others can only be integrated by further assigned licenses.

Figure 2-6



License keys are transferred via the supplied Automation License Manager (ALM). The term begins with the installation of the license in the ALM (not at the time of purchase).

The following section shows you how to transfer a license using a USB stick.

13. You have purchased and downloaded a license via the Online Software Delivery ([OSD](#)) internet platform. You can save the license on a USB stick or import it directly into the system. The following shows how to transfer the license to the Automation License Manager via USB stick.

14. Insert the USB stick into your PC.

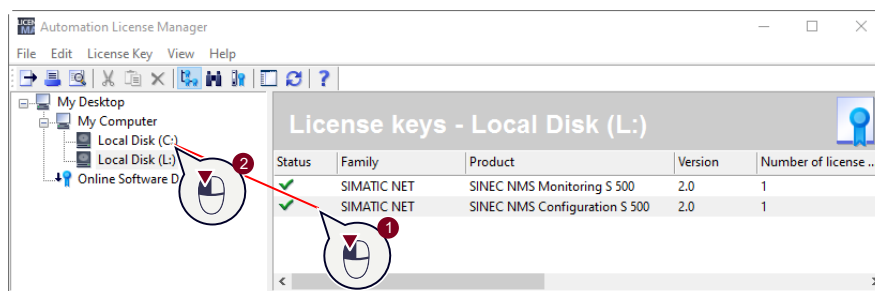
15. Close the Automation License Manager.

Figure 2-7



16. Drag and drop the license from the USB stick to a drive on your PC.

Figure 2-8



You can find more information on setting up a license server online via Article ID: [18602618](#).

## 2.3. Web Interface

### 2.3.1. Useful Information about the Web Interface

The Control and each Operation contains their own web interface. The web interface is started via the web clients of the Control and the Operation.

#### Starting Web interfaces

To open the web interface of the Control and Operations, you need a web browser. A list of supported web browsers can be found in Section [2.1.2](#).

You have the following options for opening the Operation web interface:

- Via a URL in the web browser
- Using the Operation Monitor (for UMC users only)
- Via the actions on the web interface of the Control (see [Section 5](#))
- About the desktop shortcuts

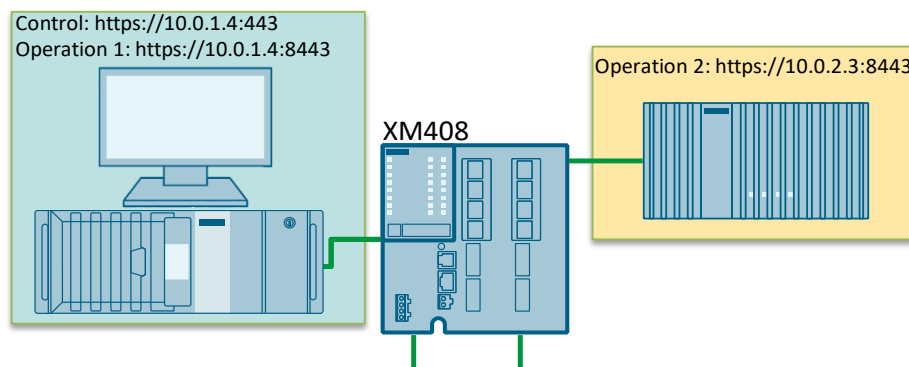
#### URLs of the web interface

If you log on to the Control or Operation with a local user, the Web interfaces of the Control and Operation can be accessed using the following URLs:

- Control: `https://<IP address or Hostname>:443`
- Operation: `https://<IP address or Hostname>:8443`

The web interfaces for the reference system are accessed as follows:

Figure 2-9



The web interface for logging into SINEC NMS can be accessed on the Control and Operation PC via the associated remote desktop connections.

#### Sign into the web interface

SINEC NMS offers two ways to log into the web interface of Control and Operation:

- Login with UMC user: If you want to use UMC users, you must define user groups and users in UMC and enter these users in SINEC NMS. A UMC user is created automatically during the installation. The first login to SINEC NMS can only be done by a local user. The UMC user created during the installation can only be used after the initial login by the local user.
- Log in with local user: If you are logging on for the first time, or if you are not using a UMC, you must log on to the Control and an Operation as a local user. By default, the following local user exists:
  - Username: SuperAdmin
  - Password: the password you have defined

### Special considerations during first log in

When you start SINEC NMS for the first time, the following special features apply:

When you log on for the first time, you must log on to the Control and an Operation as a local user. You will be prompted at Control to set the password for the user SuperAdmin. Use a secure password and remember it well. If the password is lost, it may be necessary to reinstall SINEC NMS.

You can find more information about exporting and importing the Control certificate in [Section 4](#).

### 2.3.2. Initial Login to the Control Web Interface

When you call SINEC NMS for the first time, you must use the local default "SuperAdmin" user when you first log into the Control and an Operation.

The password for this user must be set at the Control.

The first time you log on to the Control, proceed as follows:

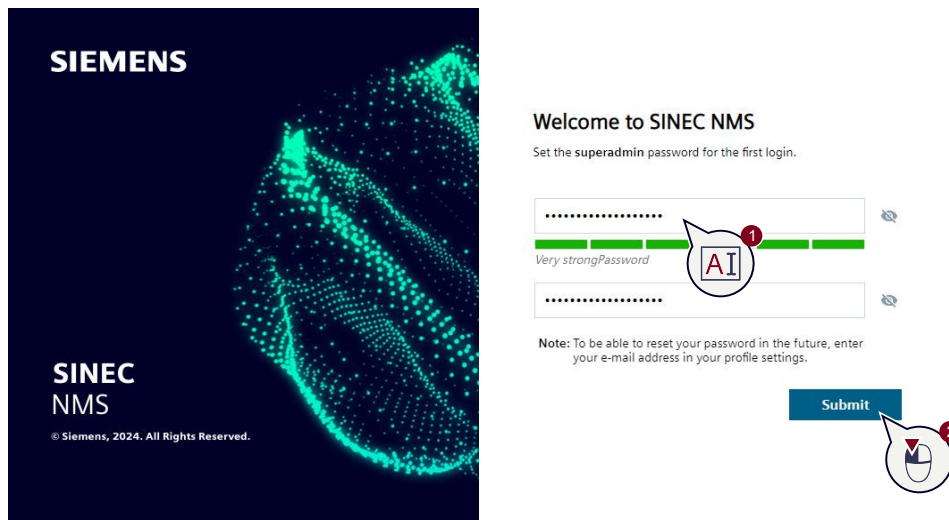
1. On the "Control & Operation 1" unit, open the web interface of the Control via URL <https://<IP address of Control>> or using the desktop shortcuts.

Figure 2-10



2. The web interface will open and you will be asked to define a new password for the user SuperAdmin. Enter the new password in the corresponding input field. Then click the "Submit" button.

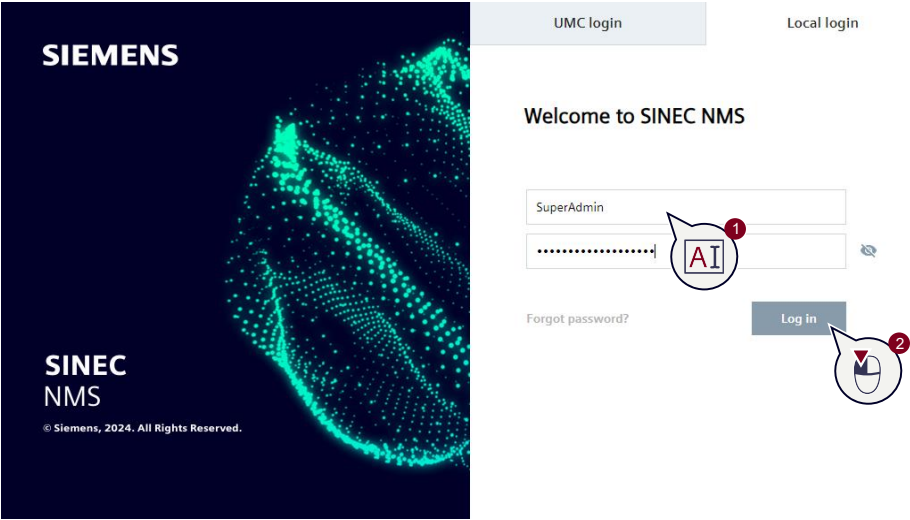
Figure 2-11



3. The password of the local user SuperAdmin has been changed. To register again, click the link.

4. Log in as SuperAdmin with your new password.  
Click "Log in".

Figure 2-12



The Start Page of the Control appears.

**NOTE**

The local default administrator of SINEC NMS is now:

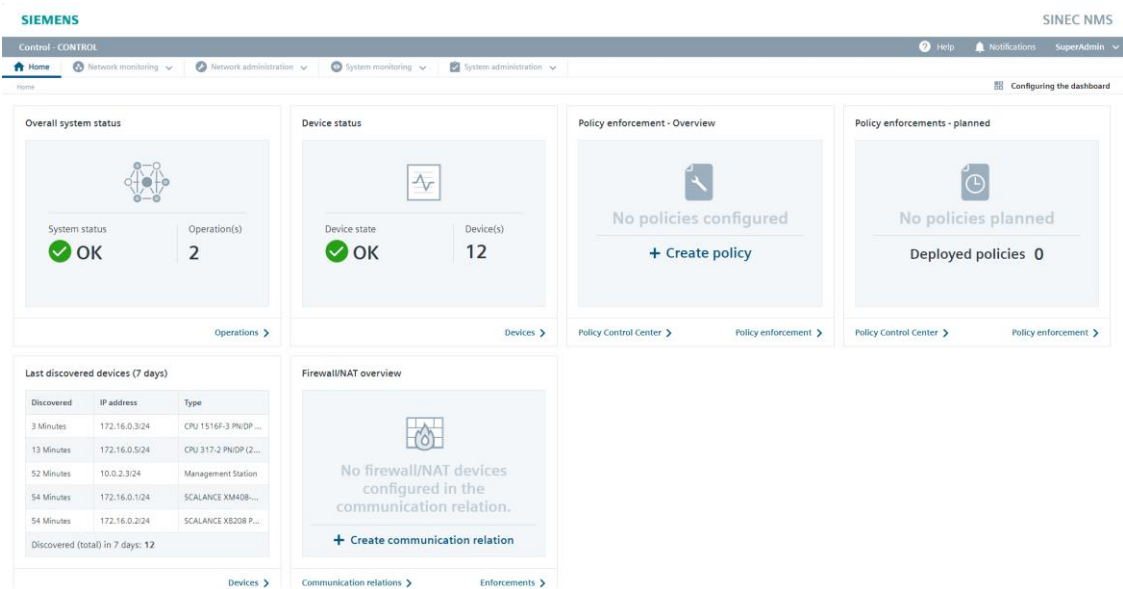
- Username: SuperAdmin
- Password: <the password you have defined>

**Start Page**

The Start Pages of Control and each Operation form the dashboard of SINEC NMS. The Start Pages are divided into several areas.

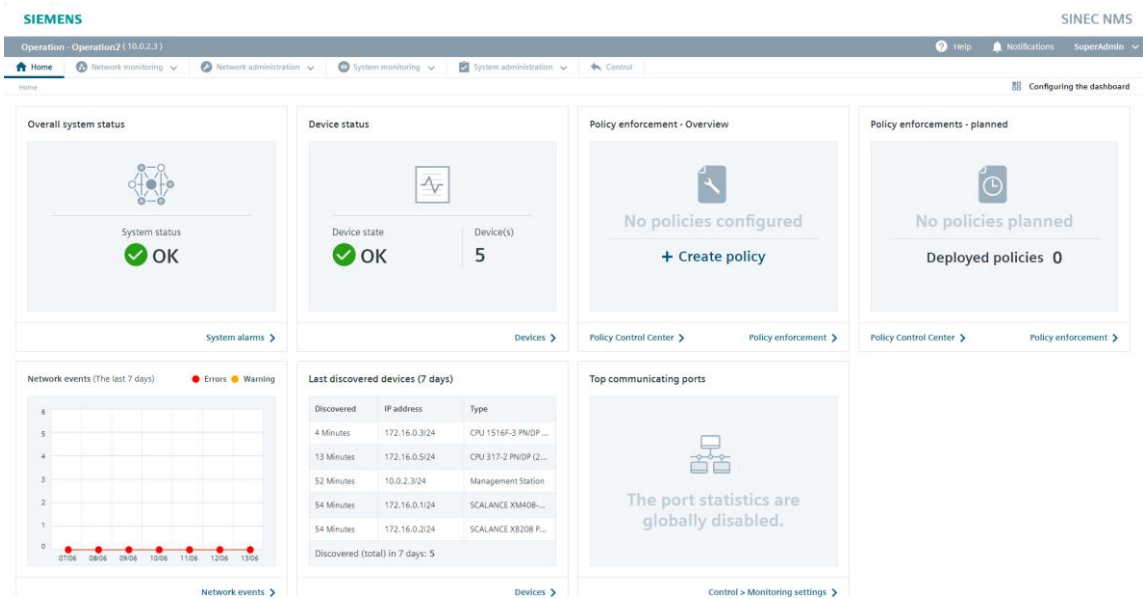
The following Figure shows the Start Page of the Control. It contains a summary of the overall status of devices as well as status information on Control, Operations, and policies.

Figure 2-13



The following Figure shows the Start Page of an Operation. It contains a summary of the overall status of devices as well as status information on policies.

Figure 2-14 Adjusting



**"Device status" area**

In the "Device status" area, the number of total statuses of monitored devices is displayed in a list. The number of devices in the overall status "OK" is given above the list. The overall status of the devices is indicated by the following abbreviations and colors.

Table 2-2

| Device status         | Color identification |
|-----------------------|----------------------|
| Error                 | <div></div>          |
| Maintenance requested | <div></div>          |
| Service necessary     | <div></div>          |
| Not accessible        | <div></div>          |

**Last discovered device (7 days)**

If new devices were found on the network during the previous scans, they will appear here.

**Network events**

The widget shows statistics about the recent daily network events, each for the event types "Error" and "Warning".

**Top communicating ports**

The widget displays up to five ports with the highest load. To view port usage, enable LAN port statistics: "Control > System administration > Operation parameter profiles > Monitoring settings > Settings for LAN port statistics".

**"Firewall/NAT overview"**

The widget provides an overview of the number and status of the configured communication relation.

### "Overall system status" pane (only visible at the Control)

The "Overall system status" pane displays the following states:

- Control state: The state of the Control. This state takes into account parameters such as CPU usage and memory management.
- Connected Operations: Number of Operations associated with the Control.

The Operation states are listed below according to their priority for display:

- Unknown: The Operation is unreachable.
- Error: There is an error on an Operation. Check pending system alarm messages on the "System monitoring > System alarms" at the Control.
- Warning: A warning message exists for an Operation. Check pending system alarm messages on the "System monitoring > System alarms" at the Control.
- OK: There are no errors or warnings.

### "Policy enforcement - Overview" pane

The "Policy enforcement - Overview" pane displays the number of states associated with every policy. The states of policies are indicated by the following abbreviations and colors.

Table 2-3

| Policy states  | Color identification                                                                |
|----------------|-------------------------------------------------------------------------------------|
| Inconsistent   |   |
| Deactivated    |  |
| Activated      |  |
| Being enforced |  |

### "Policy enforcements - planned" pane

The "Policy enforcements - planned" pane displays planned policies and loaded policies.

## 3. Control: Performing System Administration

### 3.1. Operation Parameter Profile

#### 3.1.1. Useful Information about the Operation Parameter Profile

##### Parameter profile

In a parameter profile, you can individually set all parameters, e.g. OPC and SNMP settings. The parameters that you can configure in the parameter profiles are divided into several parameter groups.

You can create and assign a separate profile for each Operation.

The "Start Profile" parameter profile is available by default and contains the default settings for all parameters.

To structure the large number of parameters that you can configure in the parameter profiles clearly, the parameters are divided into several parameter groups.

##### Configuration page in Control

On the page "System administration – Operation parameter profiles" you can centrally manage and configure profiles for all monitoring parameters of Operations.

In the "Parameter profiles" area you can create, copy, delete and rename parameter profiles. In this area you also select the parameter profile to be edited in the "Parameter groups" and "Parameter editor" areas. To copy and delete a parameter profile, the corresponding check box must be activated.

The parameter groups are displayed in the "Parameter groups" area. After selecting a parameter group, the associated parameters can be configured in the "Parameter editor" area.

##### Parameter groups

All parameters that you can edit for a parameter profile are sorted into several groups.

You can find more information on the parameter groups online in the manual via the Article ID: [109824255](#).

##### Changing parameters

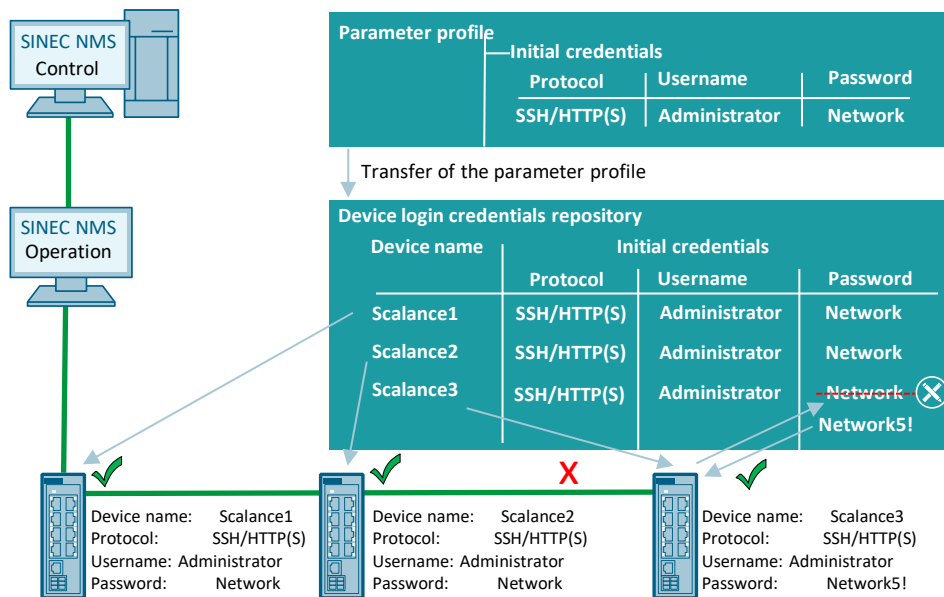
Changes in a parameter group for which the "Global" or "User global" property is displayed in the "Parameter groups" area are applied to all existing parameter profiles, including the start profile. For changes in a local parameter group, you can specify whether these changes are to be applied only to the selected parameter profile or to all parameter profiles, including the start profile.

### 3.1.2. Initial Credentials

SINEC NMS requires device login credentials to establish SNMP and SSH connections to the devices. The login data is defined in "Parameter profiles > Initial credentials". The individual Operations use the parameter profile as standard.

In addition, the login credentials can be stored and edited in the Device login credentials repository for each individual device. If no specific login data is stored in the Device login credentials repository, the initial login data is transferred to the device login data directory and used for the login.

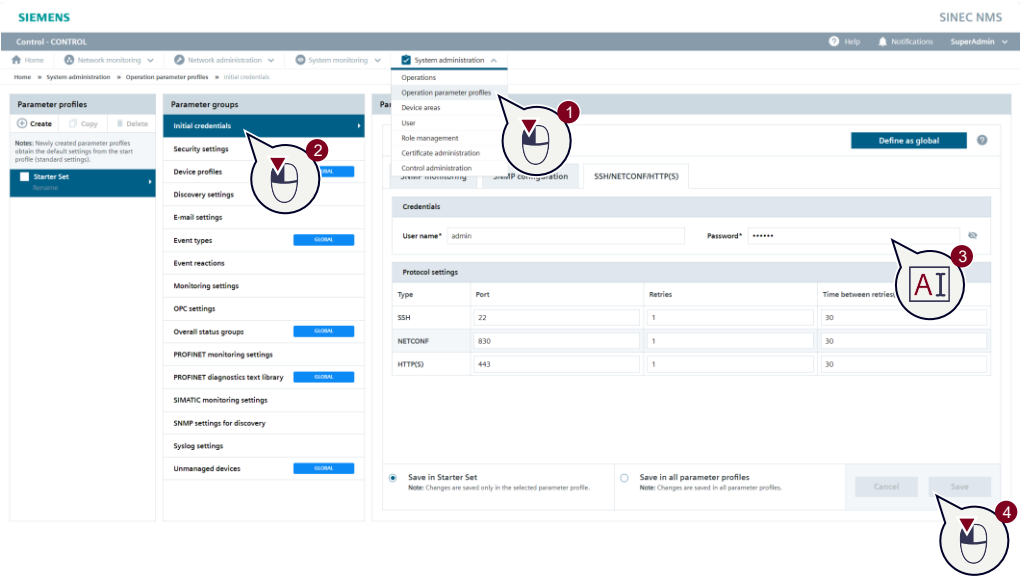
Figure 3-1



To configure the initial login data in the Control, proceed as follows.

1. Open the web interface of the Control <https://<IP address of Control>>.
2. Navigate to the configuration page "System administration > Operation parameter profiles > Initial credentials".
3. Configure your initial login credentials via SNMP and SSH/HTTP(S).
4. Save your settings. You can create additional SNMP profiles under the SNMP Discovery Settings.

Figure 3-2

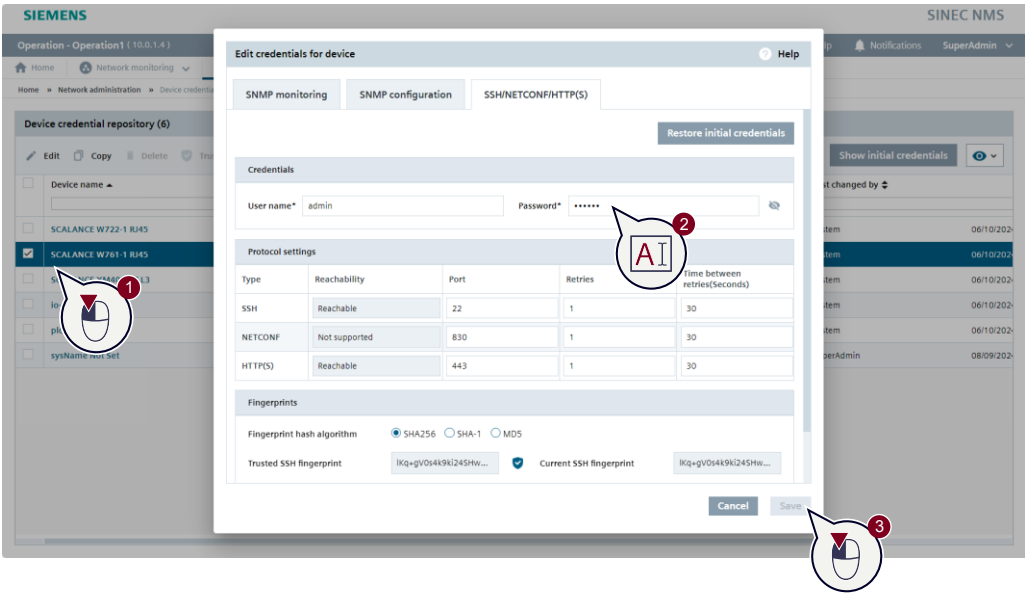


To configure the initial login credentials in the Operation, proceed as follows.

**NOTE** Please note that you can only edit the initial login data locally after a network scan (see [Section 3.2.2](#)).

1. Open the web interface of the Operation <https://<IP address of Operation>>.
2. Navigate to the configuration page "Network administration > Device credential repository".
3. Under Device name, select the device you wish to modify. Configure your initial login credentials via SNMP and SSH/HTTP(S). Save your settings.

Figure 3-3



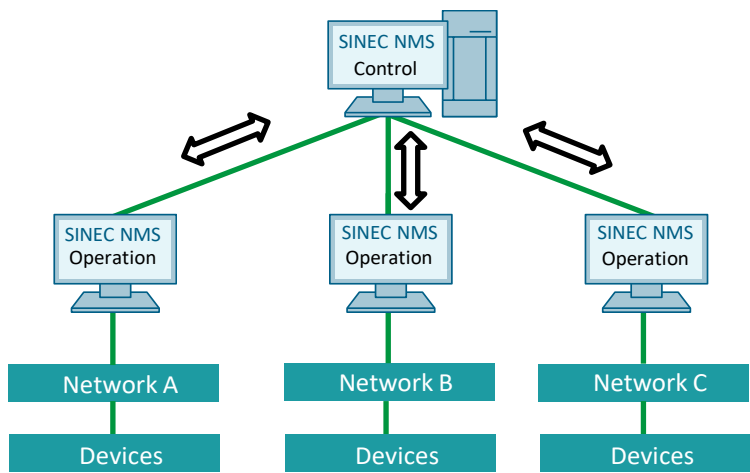
### 3.2. Operation Management

#### 3.2.1. Useful Information about Operation Management

**Overview**

SINEC NMS has a hierarchical structure. The following Figure shows the structure of SINEC NMS.

Figure 3-4



You can monitor and administer a network with one Operation. One Operation supports up to 10 network adapters. The Control is superior to the Operations and has a communication link with each Operation. The Operations determine the monitoring data from the devices and deliver selected data and summarized status information to the Control. You configure the monitoring settings to be used by the Operations centrally at the Control and then load them onto the Operations.

This bidirectional communication link allows you to monitor and administer the entire network via the Control.

**NOTE**

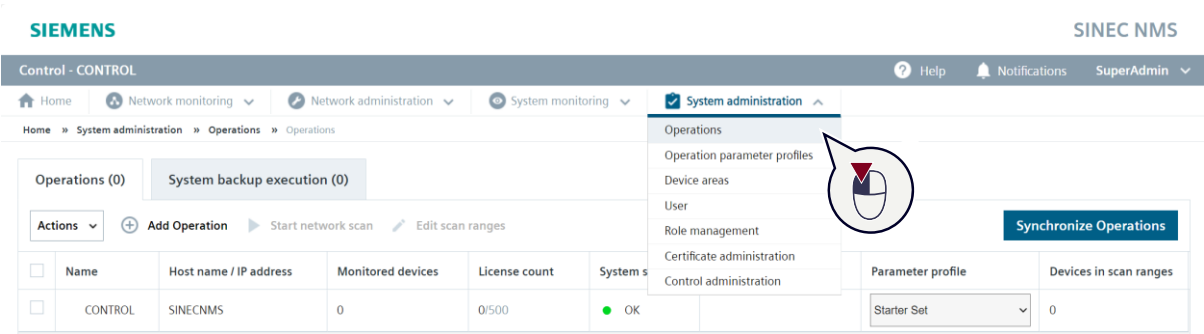
A Control only monitors and administers the Operations that you have declared in the Control and configured using an Operation parameter profile.

**Configuration page in Control**

To declare an Operation in the Control, use the "System administration > Operations" configuration page.

This page is divided into the "Operations" and "System backup execution" sections. In the Operations area, all existing operations are displayed and more can be added via "Add Operation". In the "System backup execution" tab, backups of the system can be initiated.

Figure 3-5



**Area "Add Operation"**

If you add a new Operation in the Control, you must specify the following information for the Operation:

- IP address of the Operations
- Parameter profile
- Certificate password, which is defined individually
- Scan range

You can find more information on the individual elements in the manual at the Article ID: [109824255](#).

**NOTE**

To speed up the network scan, the scan ranges should be limited to the IP addresses of the devices you wish to monitor. If the IP addresses of these devices do not follow each other, you can configure multiple scan ranges in which the devices to be detected are located.

**"Operation" area**

The "Operation" area lists all the Operations you have created in tabular form.

You can read status information and general settings for each Operation from the Table.

You can find more information on the individual columns in the manual at the Article ID: [109824255](#).

**Synchronize Operations/Synchronization Required**

If you have made changes to the configuration of Operations in the Control, then you must synchronize the changes with these Operations.

The button "Synchronize Operations" is used for this purpose.

If at least one Operation needs to be synchronized with the Control, the button will be labeled "Synchronization required". If no synchronization is required, the label of the button is "Synchronize Operations".

After clicking the "Synchronization required" button, SINEC NMS synchronizes all settings that differ between Control and Operation with the affected Operations. The reason for a required synchronization is indicated by the icons in the "Synchronization status" column.

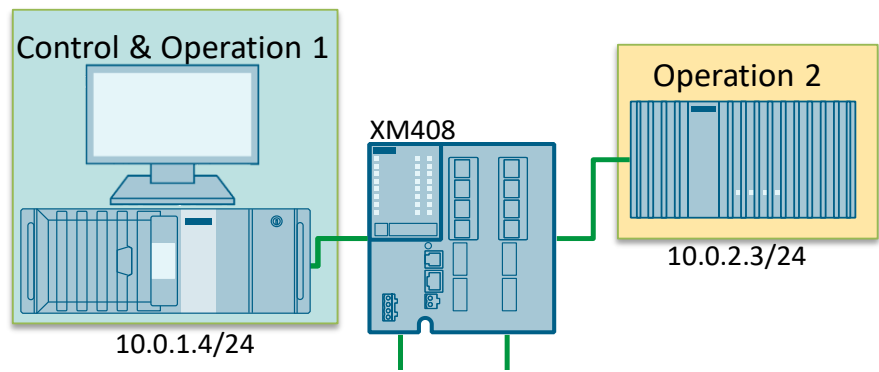
3.2.2. Adding an Operation to the System

Overview

Two Operations are used in the reference facility of this documentation.

- Operation 1: Single node installation
- Operation 2: Multiple node installation

Figure 3-6



Both Operations are inserted into the system with the parameter profile "Start profile".

Requirement

You are in the "Control & Operation 1" unit and have started the Control's web interface via the URL <https://<IP address of Control>> and are logged in as the Default Administrator.

Menu

You can find the configuration page in the Control in the navigation under "System Administration > Operations".

Figure 3-7

SIEMENS SINEC NMS

Control - CONTROL

Home Network monitoring Network administration System monitoring System administration

Home » System administration » Operations » Operations

Operations (0) System backup execution (0)

Actions Add Operation Start network scan Edit scan ranges Synchronize Operations

|                          | Name    | Host name / IP address | Monitored devices | License count | System status | Synchronization status | Parameter profile | Devices in scan ranges |
|--------------------------|---------|------------------------|-------------------|---------------|---------------|------------------------|-------------------|------------------------|
| <input type="checkbox"/> | CONTROL | SINECNMS               | 0                 | 0/500         | OK            |                        | Starter Set       | 0                      |

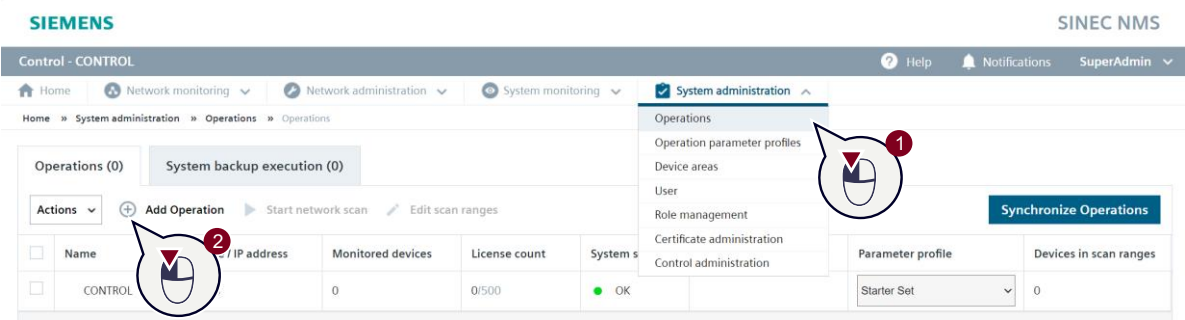
Add Operation

The following instructions show you how to add an Operation to the system. The screenshots are taken from the integration of "Operation 1".

To add an Operation to the system, proceed as follows:

- 1. Navigate to the "System administration > Operations" configuration page.

Figure 3-8



- 2. The following table shows which parameters you have to select or enter in the input fields in the "Add Operation" area:

Table 3-1

|                                | Operation 1                     | Operation 2                     |
|--------------------------------|---------------------------------|---------------------------------|
| IP address/Host name           | 10.0.1.4                        | 10.0.2.3                        |
| Position in the node structure | CONTROL                         | CONTROL                         |
| Parameter profile              | Start profile                   | Start profile                   |
| Certificate password           | <define an individual password> | <define an individual password> |
| Name of the scan range         | Operation1                      | Operation2                      |
| First IP address               | 192.168.0.1                     | 172.16.0.1                      |
| Last IP address                | 192.168.0.30                    | 172.16.0.30                     |

Specify the IP address or host name of the PC that the Operation is installed on. Enter the password for the encryption of the PKCS12 container that is used to authenticate the Operation at the Control. Select a parameter profile. In the repository hierarchy, Operations are added to a node structure that has the Control at the top. Give the Operation a name. Specify how many licenses are assigned to the Operation.

Give the scan area a name. You can define up to 500 scan ranges per Operation. Enter a scan range. Check the option "Start network scan after adding the Operation". To add the Operation to the system, click the "Add Operation" button.

Figure 3-9

Add Operation

The Operation can be added to SINEC NMS with the following settings.

Operation details

IP address/host name of the Operation \*

10.0.1.4

Certificate password \*

.....

Parameter profile \*

Starter Set

Folder hierarchy \*

CONTROL

Operation name

Operation1

Operation license count \*

30

Available licenses at Control

500/500

Scan range(s) for device identification

| Name of scan range      | First IP address                      | Last IP address                      | Devices in scan range |
|-------------------------|---------------------------------------|--------------------------------------|-----------------------|
| Operation1              | 192.168.0.1                           | 192.168.0.30                         | 30                    |
| <div>Enter a name</div> | <div>Enter the first IP address</div> | <div>Enter the last IP address</div> |                       |
| <div>Enter a name</div> | <div>Enter the first IP address</div> | <div>Enter the last IP address</div> |                       |
| <div>Enter a name</div> | <div>Enter the first IP address</div> | <div>Enter the last IP address</div> |                       |
| <div>Enter a name</div> | <div>Enter the first IP address</div> | <div>Enter the last IP address</div> |                       |

☒ Start network scan after adding the Operation  
Start a network scan if you configure "Edit discovery restriction list".

Note:

Additional steps are required for multi-node systems:  
1. Load the Operation certificate via "Download certificate".  
2. Upload the downloaded certificate to the Operation via the link under "First contact".

Cancel

Add

3. Check the initial credentials in your Device login credentials repository (see Section 3.1.2)
4. Add the second Operation to the system.

Result

The Operation appears in the "Operations" area. Since "Operation 2" has not yet authenticated to the Control ("Multi-Node Installation"), the system status displays the value "First contact".

Figure 3-10

SIEMENS

SINEC NMS

Control - CONTROL

Home

Network monitoring

Network administration

System monitoring

System administration

Home » System administration » Operations » Operations

Operations (2)

System backup execution (2)

Actions

Add Operation

Start network scan

Edit scan ranges

Synchronize Operations

|                                     | Name        | Host name / IP address | Monitored devices | License count | System status | Synchronization status | Parameter profile | Devices in scan ranges |
|-------------------------------------|-------------|------------------------|-------------------|---------------|---------------|------------------------|-------------------|------------------------|
| <input checked="" type="checkbox"/> | CONTROL (2) | SINECNMS               | 7                 | 60/500        | OK            |                        | Starter Set       | 60                     |
| <input type="checkbox"/>            | Operation1  | SINECNMS / 10.0.1.4    | 7                 | 30            | OK            |                        | Starter Set       | 30                     |
| <input type="checkbox"/>            | Operation2  | 10.0.2.3 / 10.0.2.3    | 0                 | 30            | First contact |                        | Starter Set       | 30                     |

3.2.3. Exporting Certificates

Before the communication link between an Operation and the Control can be established for the first time, the Operation must authenticate to the Control with a certificate.

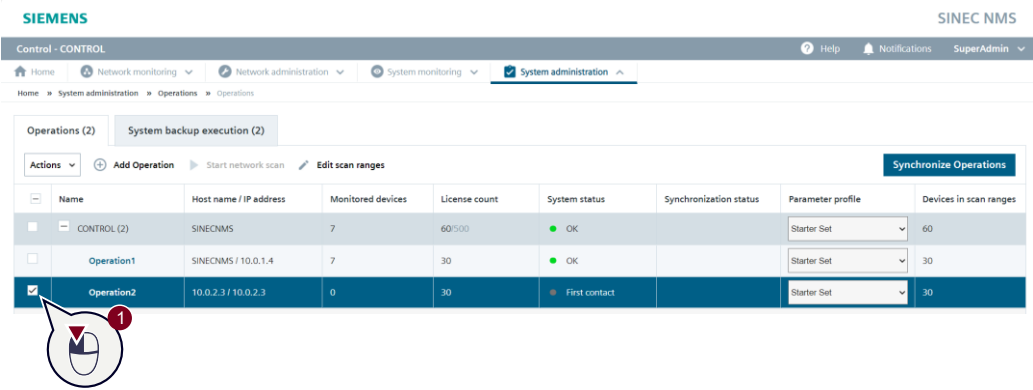
With a single node installation (here: "Operation 1"), authentication works automatically as Control and Operation are installed on the same PC.

You need a certificate so that a Multiple Node installation can authenticate itself with Control.

To download the Operation certificate, proceed as follows:

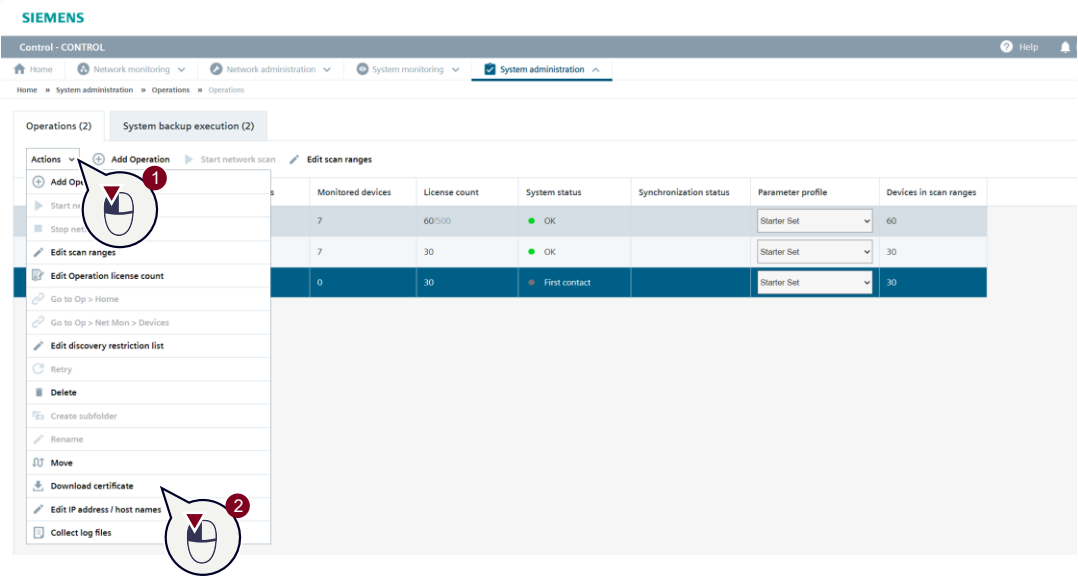
- 1. In the Operations pane, select the operation you want to authenticate.

Figure 3-11



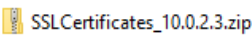
- 2. Select the menu command "Download certificate" in the context menu of the Operation. This downloads the certificate for the private key Operation as a PKCS12 container.

Figure 3-12



- 3. This downloads the certificate for the Operation with private key as a PKCS12 container.

Figure 3-13



Result

You have exported the certificate from the Control and can now import it in the Operation (see [Section 4.2](#)).

## 4. Operation: Performing Initial Commissioning

### 4.1. Useful Information about Initial Commissioning

#### Authentication at the Control

Before the communication link between an Operation and the Control can be established for the first time, the Operation must authenticate to the Control with a certificate.

With a single node installation (here: "Control & Operation 1" unit), authentication works automatically as Control and Operation are installed on the same PC.

In order for a multiple node installation (here: "Operation 2" unit) to authenticate itself to the Control, you need the certificate from the Control.

#### Network adapter

On the "Network Monitoring > Settings > Network Scan" page of an Operation, you can start the network scan and search for more suitable device profiles for devices on the Operation. You can also configure the DCP network adapters that the Operation uses for the network scan.

#### NOTE

The network scan uses the scan range configured for the Operation on the Control under "System administration > Operations".

### 4.2. Performing the Initial Commissioning of a Multiple Node

#### Requirement

You are located on the unit "Operation 2" and have started the web interface of the Operation via the URL <https://<IP address of Operation 2>:8443/local>.

#### Import certificate

You downloaded the certificate for the Operation from the Control in [Section 3.2.3](#).

#### NOTE

Authentication must only be performed once during initial commissioning. After the successful import of the certificate, the Operation has authenticated itself at the Control.

To import the certificate into the Operation, proceed as follows:

1. On the "Operation 2" unit, open the Operation web interface via the URL <https://<IP address Operation>> or the desktop shortcuts. You will automatically be redirected to the "Import Certificate" dialog.

Figure 4-1

**SIEMENS**

**SINEC NMS**  
© Siemens, 2024. All Rights Reserved.

#### Import certificate

Certificate\*

Select a certificate. ...

Password\*

Enter password

Import

Import message

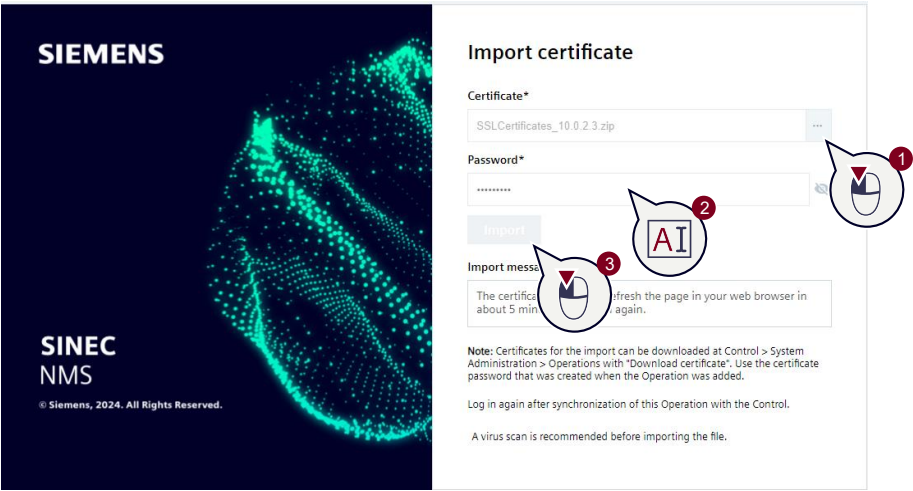
Note: Certificates for the import can be downloaded at Control > System Administration > Operations with "Download certificate". Use the certificate password that was created when the Operation was added.

Log in again after synchronization of this Operation with the Control.

A virus scan is recommended before importing the file.

- 2. In the "Certificate" section, use the context menu to navigate to the directory where the PKCS12 container (exported from the Control) is located.  
In the "Password" area, enter the certificate password (see [Section 3.2.2](#)).  
Click the "Import" button.

Figure 4-2



Result

After the successful import, the communication link between the Control and the Operation is established and all required data, including the user data and rights that can be used on the Operation, is transferred from the Control to the Operation.

It is now possible to log into the Operation with this user data.

The system status of the Operations in Control changes from "First contact" via "Initializing" to "OK". This may take a few minutes.

SIEMENS

SINEC NMS

Control - CONTROL

Help Notifications SuperAdmin

Home Network monitoring Network administration System monitoring System administration

Home » System administration » Operations » Operations

Operations (2)

System backup execution (2)

Actions Add Operation Start network scan Edit scan ranges Synchronize Operations

| <input type="checkbox"/>            | Name        | Host name / IP address | Monitored devices | License count | System status | Synchronization status | Parameter profile | Devices in sca... |
|-------------------------------------|-------------|------------------------|-------------------|---------------|---------------|------------------------|-------------------|-------------------|
| <input checked="" type="checkbox"/> | CONTROL (2) | SINECNMS               | 12                | 60/500        | OK            |                        | Starter Set       | 60                |
| <input type="checkbox"/>            | Operation1  | SINECNMS / 10.0.1.4    | 7                 | 30            | OK            |                        | Starter Set       | 30                |
| <input type="checkbox"/>            | Operation2  | 10.0.2.3 / 10.0.2.3    | 5                 | 30            | OK            |                        | Starter Set       | 30                |

NOTE

From now on, you must log in for the Default Administrator "SuperAdmin" with the password you assigned when you first logged in to the Control.

## 5. Network Monitoring

### 5.1. Detecting Devices in the Network

#### 5.1.1. Useful Information about the Network Scan

##### Network Scan

Before it is possible to monitor devices in the network, the devices must be detected by a network scan.

You will specify the scan range to be scanned when configuring the Operation on the Control (see [Section 3.2](#)).

##### Time of search

The network scan is performed at the following times:

- After an initial integration of an Operation onto the Control, if the Option is activated.
- If required, by pressing a button on the "System administration > Operations" page in the Control.
- If required, press a button on the "Network monitoring > Settings > Network scan" page in Operation.
- Automatically in appropriately configured cycles. You define the time interval for starting network scans by SINEC NMS on the Control.

##### Included devices

Depending on which DCP detection type has been configured, either all devices detectable via DCP or only those devices found via ICMP in the configured IP address ranges are included in the result.

If SIMATIC controllers are found during the scan process, the IO devices assigned to this controller can also be included in the monitoring. This applies regardless of whether the IO devices are within the search area or not.

##### Device profiles and recognition rules

Based on the recognition rules of the device profiles, SINEC NMS assigns the recognized devices to a suitable device profile. Devices that cannot be assigned detection rules are assigned default profiles, provided these default profiles are activated. If the default profiles suitable for devices are not activated, these devices are not assigned to a device profile and the devices are not monitored. If PROFINET detection is active for a device profile, devices can be assigned to this device profile and the device types it contains via article numbers.

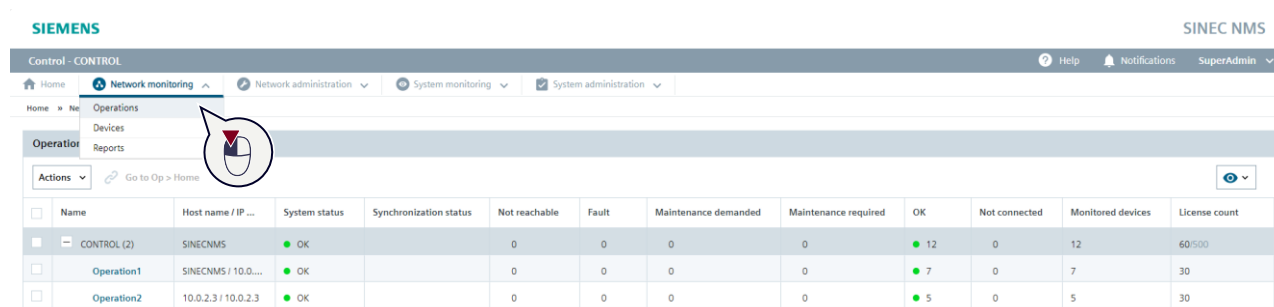
### 5.1.2. Useful Information about Monitoring on the Control

The Control allows you to monitor the Operations and the entire network.

#### Monitoring of the Operations

On the "Network monitoring > Operations" Control page, you will see the following information for each Operation:

- System state
- Synchronization status
- Number of devices with status "Not available", "Error", "Maintenance required/required", "OK", "Not connected"
- Number of devices monitored by the Operation



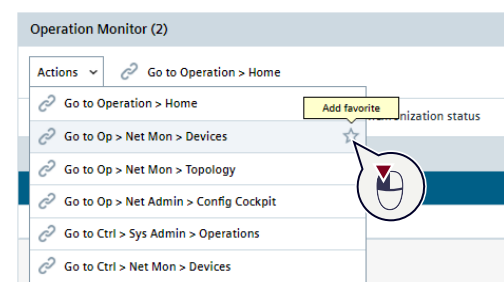
SIEMENS SINEC NMS

Control - CONTROL

Home » Network monitoring » Operations

| Name        | Host name / IP ...  | System status | Synchronization status | Not reachable | Fault | Maintenance demanded | Maintenance required | OK | Not connected | Monitored devices | License count |
|-------------|---------------------|---------------|------------------------|---------------|-------|----------------------|----------------------|----|---------------|-------------------|---------------|
| CONTROL (2) | SINECNMS            | OK            |                        | 0             | 0     | 0                    | 0                    | 12 | 0             | 12                | 60/500        |
| Operation1  | SINECNMS / 10.0.0.1 | OK            |                        | 0             | 0     | 0                    | 0                    | 7  | 0             | 7                 | 30            |
| Operation2  | 10.0.2.3 / 10.0.2.3 | OK            |                        | 0             | 0     | 0                    | 0                    | 5  | 0             | 5                 | 30            |

Use the drop-down menu to access the pages "Start", "Network Monitoring Devices", "Network Monitoring Topology", "Network Administration Configuration Cockpit", "System Administration Operations", and "Network Monitoring Devices". You can also add these pages to your favorites.



## Monitor the entire network

On the Control page "Network monitoring > Devices" the monitored devices of all Operations are displayed with their total states and determined device properties.

These include the following properties:

- State
- IP address
- System name
- Operation
- Device type
- MAC address
- Reason for overall condition

Further properties can be added via the eye icon.

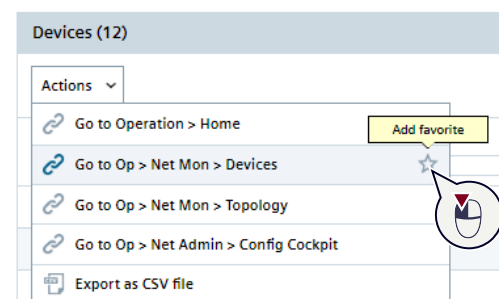
SIEMENS SINEC NMS

Control - CONTROL

Home » Network monitoring » Devices

| Status | IP address      | System name          | Operation  | Device type                         | Categ...     | MAC address       | First disc... | Article number      | Configuration access | Management ... |
|--------|-----------------|----------------------|------------|-------------------------------------|--------------|-------------------|---------------|---------------------|----------------------|----------------|
| OK     | 10.0.1.4/24     |                      | Operation1 | Management Station                  | Others       | 00:0C:29:18:86:39 | 3 Days ago    |                     | Allowed              | Monitored      |
| OK     | 192.168.0.10/24 |                      | Operation1 | CPU 1214C DC/DC/DC (1AG40-0X80)     | PLC          | 28:63:36:AF:21:9D | 3 Days ago    | 6ES7 214-1AG40-0X80 | Allowed              | Managed        |
| OK     | 192.168.0.2/24  | sysName Not Set      | Operation1 | SCALANCE SC646 (2GS00-2AC2)         | Router       | 20:87:56:82:F2:FA | 3 Days ago    | 6GKS 646-2GS00-2AC2 | Allowed              | Managed        |
| OK     | 192.168.0.1/24  | SCALANCE XM408-8C L3 | Operation1 | SCALANCE XM408-8C (8GR00-2AM2)      | Router       | 20:87:56:10:26:D7 | 3 Days ago    | 6GKS 408-8GR00-2AM2 | Allowed              | Managed        |
| OK     | 192.168.0.13/24 | SCALANCE W722-1 RJ45 | Operation1 | SCALANCE W722-1 RJ45 (1FC00-0AA0)   | WLAN Client  | 00:18:18:E6:5C:33 | 3 Days ago    | 6GKS 722-1FC00-0AA0 | Allowed              | Managed        |
| OK     | 192.168.0.14/24 | SCALANCE W761-1 RJ45 | Operation1 | SCALANCE W761-1 RJ45 (1FC00-0AA0)   | Access Point | 00:18:18:E8:61:35 | 3 Days ago    | 6GKS 761-1FC00-0AA0 | Allowed              | Managed        |
| OK     | 192.168.0.11/24 |                      | Operation1 | ET 200SP IM155-6 PN ST (6AU00-0BND) | End Device   | 00:18:18:5F:E5:81 | 3 Days ago    | 6ES7 155-6AU00-0BND | Allowed              | Managed        |
| OK     | 172.16.0.5/24   |                      | Operation2 | CPU 317-2 PN/DP (2EK14-0AB0)        | PLC          | 00:0E:8C:F8:2F:9C | 19 Minutes    | 6ES7 317-2EK14-0AB0 | Allowed              | Managed        |
| OK     | 10.0.2.3/24     |                      | Operation2 | Management Station                  | Others       | 00:0C:29:08:CA:C4 | 58 Minutes    |                     | Allowed              | Monitored      |
| OK     | 172.16.0.3/24   |                      | Operation2 | CPU 1516F-3 PN/DP (3FN0-0AB0)       | PLC          | 28:63:36:95:81:5C | 10 Minutes    | 6ES7 516-3FN01-0AB0 | Allowed              | Managed        |
| OK     | 172.16.0.2/24   | SCALANCE XB208       | Operation2 | SCALANCE XB208 PN (0BA00-2AB2)      | Switch       | 20:87:56:04:23:18 | 1 Hour        | 6GKS 208-0BA00-2AB2 | Allowed              | Managed        |
| OK     | 172.16.0.1/24   | SCALANCE XM408-8C L3 | Operation2 | SCALANCE XM408-8C (8GR00-2AM2)      | Router       | 20:87:56:10:26:08 | 1 Hour        | 6GKS 408-8GR00-2AM2 | Allowed              | Managed        |

Use the drop-down menu to access the pages "Start", "Network Monitoring Devices", "Network Monitoring Topology", "Network Administration Configuration Cockpit", "System Administration Operations", and "Export CSV File". You can also add these pages to your favorites.



### NOTE

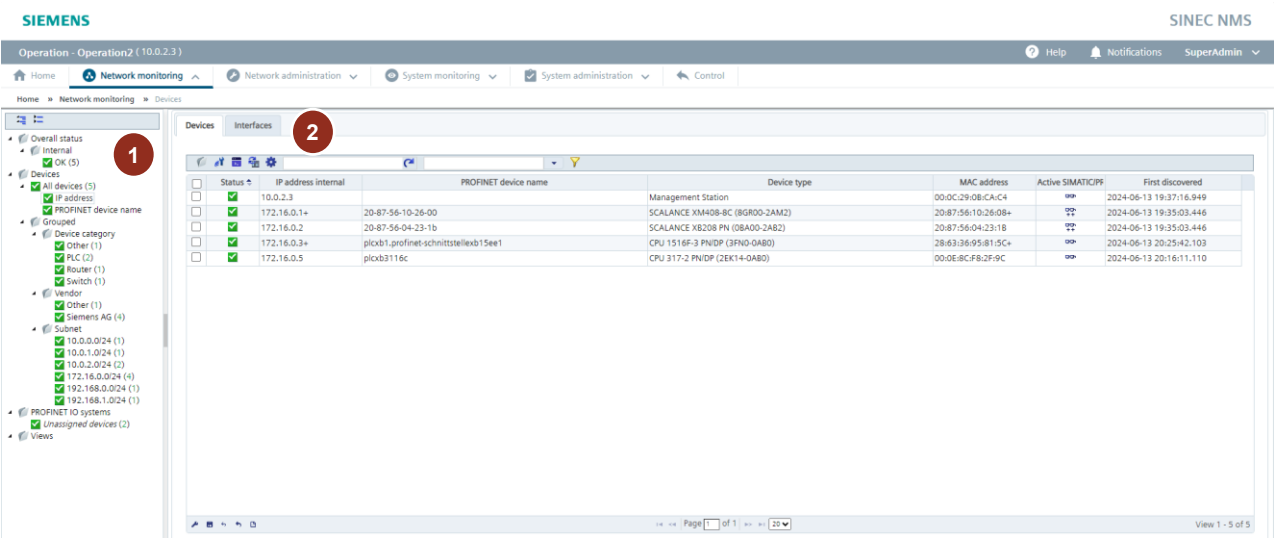
Only the Operations and their devices that you have declared to the Control are displayed.

5.1.3. Useful Information about Monitoring on the Operations

After the scan is complete, you can view the status of all network devices associated with the Operation.

Monitored devices

On the "Network Monitoring > Devices" page of an Operation, the devices of the Operation can be monitored. You see all devices that have been detected and are in the scan range of the Operation.



The following Table shows the meaning of the numbers:

Table 5-1

| No. | Area                           | Description                                                                                                                                                                           |
|-----|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Device tree                    | In the device tree, all devices monitored by the Operation are listed in groups. The different groups are used to display the devices filtered depending on the selected group topic. |
| 2   | Device window with device list | The devices that are part of the selected group topic in the device tree are listed in the device list.                                                                               |

Device tree

The device tree groups all devices that have been detected after a scan. Selecting a device group creates a filtered device list, which is displayed in the "Devices" tab of the device window. Device tree is structured as follows:

- The "Overall status" node filters the devices according to the overall status, e.g. "OK".
- The "Devices" node generates a display filtered by device property.
- The "PNIO Systems" node only displays the devices that belong to the selected PNIO system.
- The "Views" node defines user-specific views that cover only some of all existing devices.

The device tree also provides an overview of the states of the devices monitored in the network. For this purpose, the symbols in the device tree always indicate the most unfavorable current state that exists for a device node in the respective branch.

The following overall device statuses are possible:

Table 5-2

| Symbol                                                                            | Description                          |
|-----------------------------------------------------------------------------------|--------------------------------------|
|  | Device status: Not connected         |
|  | Device status: OK                    |
|  | Device status: Service necessary     |
|  | Device status: Maintenance requested |
|  | Device status: Error                 |
|  | Devices not accessible               |

### Device list

You open the device lists by selecting an entry in the device tree. The "Devices" tab in the device window is always preselected.

Depending on which entry you selected in the device tree, all devices or only a certain group are displayed in the device list.

Device lists are divided into several columns in which the device-specific data is displayed. Except in the first column, which is used to select rows, you can freely select and adjust the contents of all other columns.

### Functions of the device list

A toolbar with functions is available in the device window. You can apply these functions to a marked device in the device list.



These include the following functions:

- Device details for the selected device
- Open web-based management
- Reread device data
- Add comments
- Enabling or disabling monitoring
- Add new device manually
- Deleting a device
- Change device type
- Modify monitoring profile
- Modify device data

## Device details

For each device in the device list, you can retrieve detailed device information.

The window with the specific device details can be reached in the following ways:

- In the Device window
  - Via the corresponding symbol in the toolbar
  - By double-clicking the corresponding entry in the device list
- In the topology view
  - Via the context menu of a device
  - Double-click the device symbol

The "Device details" window consists of several tabs in which the data of a device is grouped in detail or displayed in list form.

Which registers are displayed depends on the respective device type. For example, all PROFINET-capable devices are assigned an additional "PROFINET" tab, or WLAN-capable devices are assigned the "WLAN" tab.

## 5.1.4. Manually or Automatically Starting a Network Scan for Control

### Preparation

To start the network scan of the entire system or an Operation, the following items must be completed in advance:

- All Operations whose devices are to be detected must be known to the Control (see [Section 3.2](#)).
- If you have special requirements or specifications for the network scan, you must define the monitoring settings individually in the parameter profile of the Operation (see [Section 3.1](#)).
- All Operations involved have successfully authenticated themselves at the Control and can be reached from the Control (see [Section 4](#)).

### Requirement

You are in the "Control & Operation 1" unit and have started the Control's web interface via the URL <https://<IP address of Control>> and are logged in as the Default Administrator.

### Menu

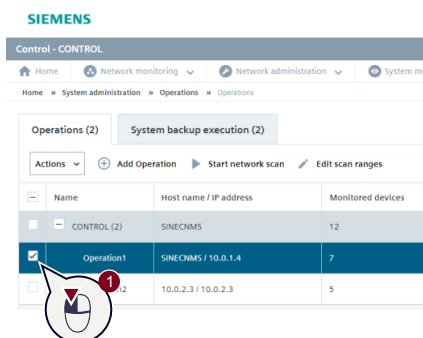
You can find the configuration page in the Control in the navigation under "System Administration > Operations".

### Start device detection manually

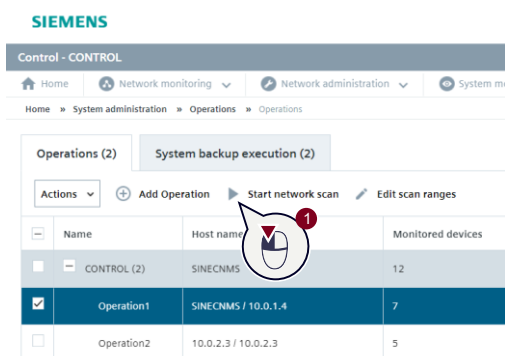
You can manually start device recognition for all or selected Operations.

To start device detection manually, proceed as follows:

1. Select the Operations over which the network scan is to run.



2. Click the "Start network scan" button.



During the network scan, the system status "Network scan in progress" will appear in the "Monitored devices" column.

Figure 5-1

| <input type="checkbox"/>            | Name        | Host name / IP address | Monitored devices                                                                                         |
|-------------------------------------|-------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>            | CONTROL (2) | SINECNMS               | 12                                                                                                        |
| <input checked="" type="checkbox"/> | Operation1  | SINECNMS / 10.0.1.4    | 7  Starting network scan |
| <input type="checkbox"/>            | Operation2  | 10.0.2.3 / 10.0.2.3    | 5                                                                                                         |

## 6. Operation: Understanding and Filtering the Events List

### 6.1. Useful Information about Events

In order to be always informed about activities in the network or at the Operation, the Event list is available on the web interface of the Operation in the "Network monitoring" area. The Event list displays all events in tabular form.

**NOTE**

Which events are displayed in the Event list depends on which views are assigned to the logged in user. This ensures that only Events related to configured views are monitored.

**Classification**

Events are divided into the following main categories:

- Network Events  
The network Events inform about occurred states and changes in the network.
- System Events  
The system Events provide information about actions, changes, and error Events in the Operation.

**Classification**

All network Events and system Events are additionally classified according to their severity.

A distinction is made between the following Event classes:

- Notification and information, e.g. user logon and logoff, "firmware version change or IP address" was detected
- Warning, e.g. "Redundant connection activated by ring manager" or "Critical rate of rejected send or receive packets"
- Error, e.g. double IP address, PROFINET diagnostics "Module missing"

Depending on the evaluation, the "Event class" column in the Event list is displayed in color-coded form. You can subsequently change the classification of any Event.

## Event state

Events can have different states. The state of an Event depends on the overall state of the network device for which the Event was triggered.

The following Table shows which states an event can assume:

Table 6-1

| Event state            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pending                | An Event triggered for a network device that is associated with a negative overall state (any overall state except OK and Not Connected) is marked Pending. The Event has been included in a list of Events pending for the instrument.                                                                                                                                                                                                                                                                                           |
| Automatically resolved | An Event that has been removed from the list of upcoming Events is marked with the Event state "Automatically resolved". Resolved Events can no longer influence the overall condition of devices. Pending Events are automatically resolved by the following Events: <ul style="list-style-type: none"> <li>Events with the assigned overall status "OK" or "Not connected" from the same overall status group</li> <li>Upcoming Events of the same overall status group (independent of the assigned overall status)</li> </ul> |
| Manually resolved      | A pending Event that was manually removed from the list of pending Events using the stamp icon in the Event list is marked with the Event state "Manually resolved".                                                                                                                                                                                                                                                                                                                                                              |
| Not available          | A triggered Event that is not assigned to an overall status group or to which no overall status is assigned there does not have an Event status.                                                                                                                                                                                                                                                                                                                                                                                  |

## Filter templates

You can filter the data displayed at the operation, such as Events, according to criteria. To avoid reconfiguring the selected filter criteria before each filter process, you can save them in a filter template and reuse the filter template.

The settings that can be defined in a filter template can be divided into three categories. The criteria of these categories are applied to the data to be displayed in the order given below:

1. Prefilter:  
The prefilter includes basic filter criteria that are applied to data to be displayed on the server side. Data that passes the prefilter is passed on to the user.
2. Complex filter:  
In the second Step, the data received from end device is filtered with a complex query, if one exists. A complex query can be used to create filter rules for individually selectable columns. These rules can be linked with logical operators and nested using rule levels.
3. Simple filter:  
In the third Step, the data that has passed the complex filter is filtered by a free text entry. In contrast to the complex filter, the simple filter includes all columns of the respective data category by default.

## Functions of the Event list

A toolbar with functions is available in the Event list. You can apply these functions to a selected Event in the Event list.

These include the following functions:

- Event noted
- Resolve Event manually
- Edit and/or delete annotations
- Maximize or minimize Event list
- Filter options

## 6.2. Adapting the Event List

### Requirement

You are in the "Control & Operation 1" unit or the "Operation 2" unit, have started the web interface of the Operation and logged on as the Default Administrator.

### Menu

You will find the configuration page in the Operation in the navigation under "Network Monitoring".

### Modifying display

The Event list shows all Events in tabular form. Each column is assigned to a device characteristics.

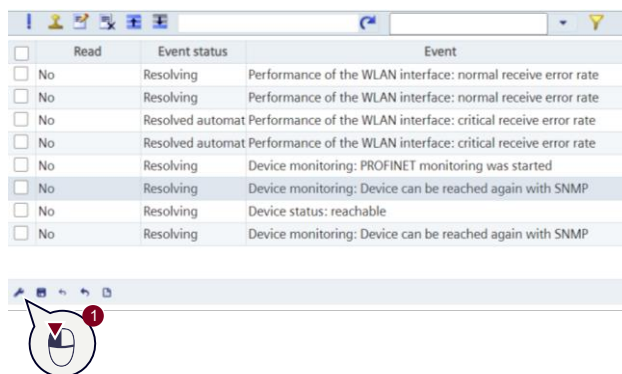
| <input type="checkbox"/> | Read | Event status     | Event                                                          | Event class | Time stamp              |
|--------------------------|------|------------------|----------------------------------------------------------------|-------------|-------------------------|
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | Info        | 2024-07-01 08:50:18.309 |
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | Info        | 2024-07-01 08:50:18.169 |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | Warning     | 2024-07-01 08:45:18.516 |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | Warning     | 2024-07-01 08:45:18.270 |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: PROFINET monitoring was started             | Info        | 2024-07-01 08:44:03.671 |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | Info        | 2024-07-01 08:44:02.695 |
| <input type="checkbox"/> | No   | Resolving        | Device status: reachable                                       | Info        | 2024-07-01 08:44:02.695 |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | Info        | 2024-07-01 08:44:02.602 |

Using the tools on the footer you can customize the entire table. You have the following options for change:

- Add columns with additional information
- Removing existing columns
- Change Column Width

To adjust the Events lists, proceed as follows:

1. Click the selected tool in the toolbar.



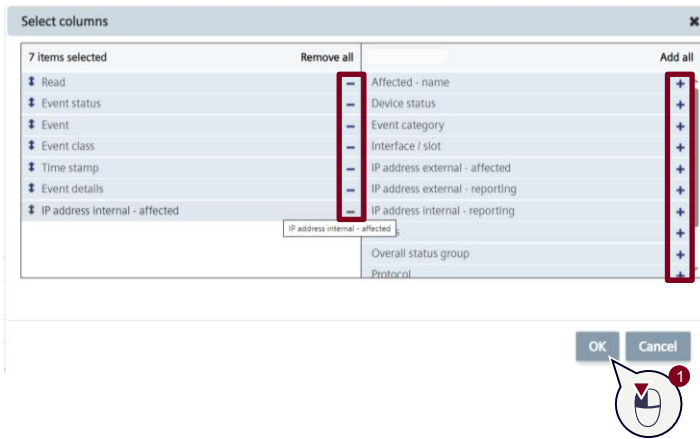
2. The column selection window opens. The breakdown is as follows:

- In the left area you can see the already displayed columns.
- In the right area you can see the free columns.

Remove existing columns using the minus sign ("-") and/or add new columns using the plus sign ("+").

You can use the Drag & Drop function to change the sort order of the columns.

Click "OK" to close the window.



3. You can edit the column width directly in the Event list.

| <input type="checkbox"/> | Read | Event status     | Event                                                          | Event details |
|--------------------------|------|------------------|----------------------------------------------------------------|---------------|
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | 1             |
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | 6             |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: PROFINET monitoring was started             | -             |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             |
| <input type="checkbox"/> | No   | Resolving        | Device status: reachable                                       | -             |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             |

4. To accept the changes, click the selected tool.

| <input type="checkbox"/> | Read | Event status     | Event                                                          | Event details | IP address internal - affected |
|--------------------------|------|------------------|----------------------------------------------------------------|---------------|--------------------------------|
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | 1.896         | 192.168.0.13                   |
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | 0.000         | 192.168.0.14                   |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        | 192.168.0.13                   |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        | 192.168.0.14                   |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: PROFINET monitoring was started             | -             | 192.168.0.11                   |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             | 192.168.0.10                   |
| <input type="checkbox"/> | No   | Resolving        | Device status: reachable                                       | -             | 192.168.0.10                   |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             | 192.168.0.11                   |

## Result

The Event list appears with the new arrangement in the device window.

## Filtering Events

Event lists can be filtered with filter templates according to various criteria.

You can filter the Events according to the following criteria:

- Event state
- Time period:
  - After Events of the last 7 days or 24 hours
  - After all Events from the current time onwards
  - After all Events within a manually entered period of time
- Event class
- Event category
- Protocol

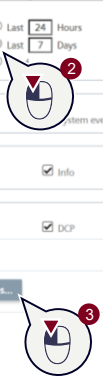
The following instructions show you how to filter Events with a prefilter:

1. Click the selected tool in the toolbar.



|                          | Read | Event status     | Event                                                          | Event details |
|--------------------------|------|------------------|----------------------------------------------------------------|---------------|
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   |               |
| <input type="checkbox"/> | No   | Resolving        | Performance of the WLAN interface: normal receive error rate   | 0.0           |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        |
| <input type="checkbox"/> | No   | Resolved automat | Performance of the WLAN interface: critical receive error rate | 50.000        |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: PROFINET monitoring was started             | -             |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             |
| <input type="checkbox"/> | No   | Resolving        | Device status: reachable                                       | -             |
| <input type="checkbox"/> | No   | Resolving        | Device monitoring: Device can be reached again with SNMP       | -             |

2. The "Events filter" dialog box appears. Change to the "Prefilter" tab. Set the filter, e.g., "Pending Last 7 Days". To save the prefilter, click "Save as...".



**Events filter**

Filter Prefilter

Note: These filter settings are applied to data to be displayed on the server. If the number of data records passing the prefilter exceeds 5000, only the last 5000 data records are forwarded to the clients.

Basic filter options

Read: All

Event status: Pending

Period:
   
☐ Last 24 Hours
   
☒ Last 7 Days
   
☐ From: To:

Event categories:
   
☒ Network events
   
☐ System events

Event classes:
   
☒ Notification
   
☒ Info
   
☒ Warning
   
☒ Error

Protocols:
   
☒ ICMP
   
☒ DCP
   
☒ ARP
   
☒ SNMP

Buttons: Delete Save **Save as...** Cancel Reset filter Use filter

3. A dialog for entering a name for the filter template opens, under which the configured filter settings are to be saved. The name must be unique and must not contain more than 25 characters. Click "Save".

Events filter

Filter template

Name Pending Last 7 Days

Cancel Save

4. A new dialog opens and confirms the successful creation of the filter template. Close the message with "OK".

Events filter

Filter template created successfully.

OK

5. To apply the filter, click the "Use filter" button.

Events filter "Pending Last 7 Days"

Filter Prefilter

Note: These filter settings are applied to data to be displayed on the server. If the number of data records passing the prefilter exceeds 5000, only the last 5000 data records are forwarded to the clients.

Basic filter options

Read All

Event status Pending

Period

☐ Last 24 Hours

☒ Last 7 Days

☐ From To

Event categories

☒ Network events

Event classes

☒ Notification ☒ Info ☒ Warning ☒ Error

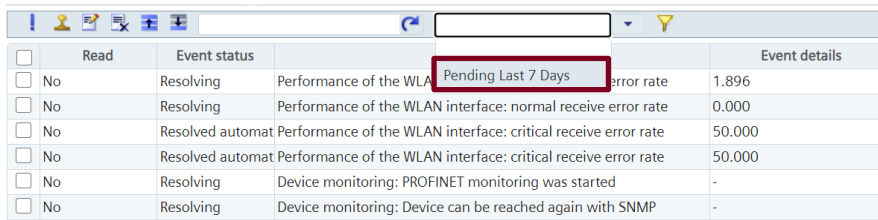
Protocols

☒ ICMP ☒ DCP ☒ ARP ☒ SNMP

Delete Save Save as...

Cancel Reset filter Use filter

6. All created filter templates are listed in a selection list. You can view the contents of this list via the toolbar. To apply a filter template from the drop-down list, select the corresponding entry in the list.



|                          | Read | Event status           | Event details                                                         |
|--------------------------|------|------------------------|-----------------------------------------------------------------------|
| <input type="checkbox"/> | No   | Resolving              | Performance of the WLAN interface: normal receive error rate 1.896    |
| <input type="checkbox"/> | No   | Resolving              | Performance of the WLAN interface: normal receive error rate 0.000    |
| <input type="checkbox"/> | No   | Resolved automatically | Performance of the WLAN interface: critical receive error rate 50.000 |
| <input type="checkbox"/> | No   | Resolved automatically | Performance of the WLAN interface: critical receive error rate 50.000 |
| <input type="checkbox"/> | No   | Resolving              | Device monitoring: PROFINET monitoring was started -                  |
| <input type="checkbox"/> | No   | Resolving              | Device monitoring: Device can be reached again with SNMP -            |

## Result

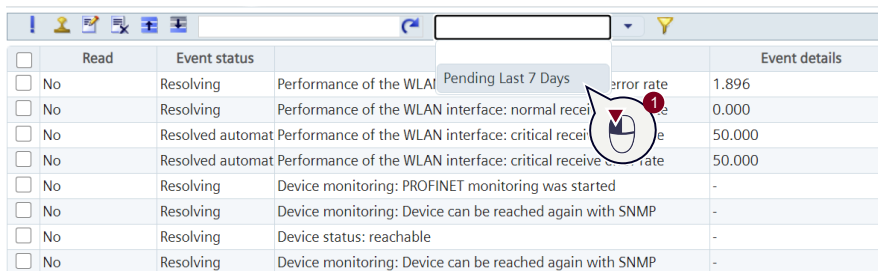
The Events are displayed in the Event list filtered according to the definition in the prefilter.

## Resolve Event manually

Events with the status "pending" can be resolved manually via the corresponding tool in the function bar. This action removes a selected pending Event from the list of Events pending for a device. The Event then enters the Event status "Manually resolved". To display only the events of the last seven days with the state "Pending", use the filter preset "Pending Last 7 Days" you just created.

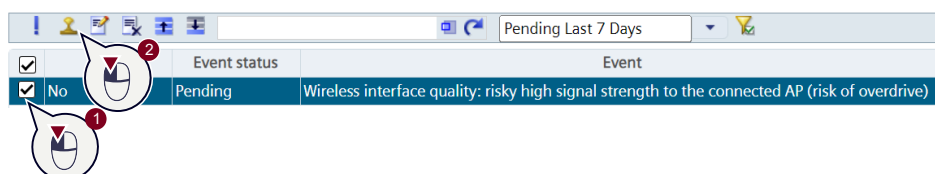
For a manual resolution, proceed as follows:

1. Select the "Pending Last 7 Days" filter preset from the drop-down list. The events are displayed in the Event list filtered according to the definition in the filter preset.



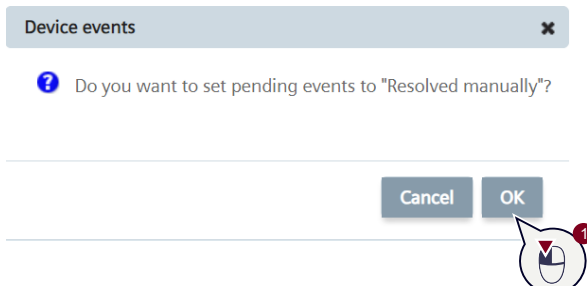
|                          | Read | Event status           | Event details                                                         |
|--------------------------|------|------------------------|-----------------------------------------------------------------------|
| <input type="checkbox"/> | No   | Resolving              | Performance of the WLAN interface: normal receive error rate 1.896    |
| <input type="checkbox"/> | No   | Resolving              | Performance of the WLAN interface: normal receive error rate 0.000    |
| <input type="checkbox"/> | No   | Resolved automatically | Performance of the WLAN interface: critical receive error rate 50.000 |
| <input type="checkbox"/> | No   | Resolved automatically | Performance of the WLAN interface: critical receive error rate 50.000 |
| <input type="checkbox"/> | No   | Resolving              | Device monitoring: PROFINET monitoring was started -                  |
| <input type="checkbox"/> | No   | Resolving              | Device monitoring: Device can be reached again with SNMP -            |
| <input type="checkbox"/> | No   | Resolving              | Device status: reachable -                                            |
| <input type="checkbox"/> | No   | Resolving              | Device monitoring: Device can be reached again with SNMP -            |

2. Select the desired event in the Event list and click the selected tool.



|                                     | Read | Event status | Event                                                                                          |
|-------------------------------------|------|--------------|------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | No   | Pending      | Wireless interface quality: risky high signal strength to the connected AP (risk of overdrive) |

3. A new dialog appears to confirm the action. Click "OK".

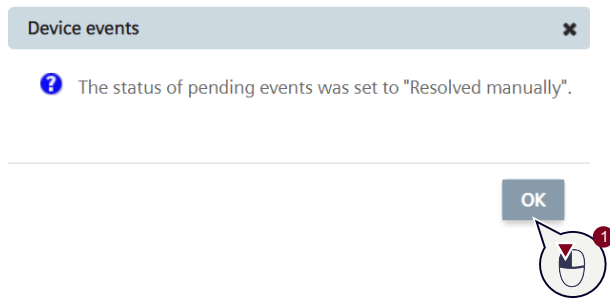


Device events

Do you want to set pending events to "Resolved manually"?

Cancel OK

4. A new dialog informs you that the selected Event has been resolved manually. Confirm the message with "OK".

**Result**

The new state of the selected Event is "Manually resolved" and is no longer listed in the Event list with the prefilter "Upcoming last 7 days" selected in the example.

## 7. Operation: Understanding and Using Topology

### 7.1. Useful Information on Topology

#### 7.1.1. General Information

##### Topology Monitoring

The device information recognizable by SINEC NMS also includes information about the respective neighboring devices. Using the SNMP and PROFINET protocols, SINEC NMS reads neighborhood information and calculates a topology representation with LLDP (Link Layer Discovery Protocol), in which the detected connections and ports between devices are displayed graphically.

##### NOTE

The network topology detection is based on LLDP information that is read out via SNMP or PROFINET. To obtain accurate connection information, SNMP and/or PROFINET monitoring for the devices to be monitored must be enabled in SINEC NMS.

The PROFINET device names of the devices are used to represent the topology. The device names must therefore be unique.

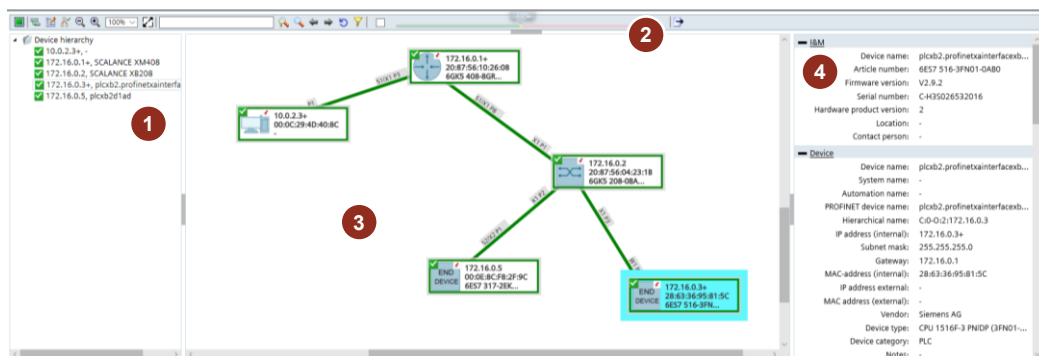
To monitor the devices, you can define SET states for connections and protocol availabilities in the topology display. The deviations between ACTUAL and SET states are then highlighted graphically.

#### 7.1.2. Work Areas and Operation

##### Work areas

The following Figure illustrates the division of the panes.

Figure 7-1



The following Table shows the meaning of the numbers:

Table 7-1

| No. | Area                                 | Description                                                                                                                                                                                                |
|-----|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Device hierarchy                     | The device hierarchy lists all devices that were determined after a search. In Edit mode, the device hierarchy in the left sidebar is initially empty; all devices determined are in the topology display. |
| 2   | Toolbar                              | The toolbar provides elements for operating the topology.                                                                                                                                                  |
| 3   | Device hierarchy in topology display | The devices in the device hierarchy are displayed topologically in the main window.                                                                                                                        |
| 4   | Detail area                          | After selecting a device in the topology view, the corresponding details for the device, ports and Events are displayed here.                                                                              |

### Topology modes

You work in SINEC NMS with different topology modes to create the requirements for device monitoring in the monitored topology.

The following modes are available in SINEC NMS:

- Edit mode (  icon)
- Online mode (  icon)

In Edit mode, you can configure a reference topology based on the topology determined by an Operation, which represents the target state of the network. The configured Reference topology forms the basis for monitoring the network.

In online mode, you can monitor the network taking into account the configured Reference topology. For connections and ports of reference devices, deviations between determined states and reference states of SINEC NMS are highlighted in color and communicated via associated Events.

### Functions of topology

The topology provides you with a toolbar with control elements.

Whether you can select a control element depends on the topology mode you are in.

Figure 7-2 Edit mode



Figure 7-3 Online mode



In Online mode, you can define the threshold value for the load on the port and view the real network load graphically. This makes it possible to investigate the network performance within the topology and detect critical states.

You can find more information on the toolbar and its buttons in the manual via the Article ID: [109824255](https://www.siemens.com/press/en/109824255)

### 7.1.3. Edit Mode

If no Reference topology has been created yet and you have the right to edit the topology, the topology will be displayed on an Operation in Edit mode after calling the page "Network monitoring > Topology".

#### Description

With the determined topology it can happen that the topology does not represent all connections or possibly recognizes wrong connections. Possible causes are that some devices are detected in the network for which SNMP and/or PROFINET is deactivated. There may also be devices in "Unmanaged" status which are not automatically detected by SINEC NMS.

In Edit mode, you can configure a Reference topology based on the topology determined by SINEC NMS that represents the target state of the network. This target state forms the basis for monitoring the network in online mode and in view-specific topology representations.

A connection wizard in Edit mode helps you to configure the Reference topology.

#### Correction and supplementation options

The Connection Wizard serves the following purposes:

- Define reference connections
- Define reference states for ports
- Define reference states for protocol-specific device availabilities
- Add new devices in the editor
- Add unmanaged devices and network clouds

Reference Connections can be configured as follows:

- Manually drawing a connection with the Draw tool
- Toggle reference state manually by double-clicking
- Changing the Reference State Using the Context Menu
- Make current/learned connection to Reference Connection

#### Define reference states for ports

Ports can have the following reference states:

- Active
- Inactive
- Not monitored
- Swap port

You can configure the reference state of a port as follows:

- Toggle reference state manually by double-clicking
- Changing the Reference State Using the Context Menu
- Accept detected state as reference state

#### NOTE

It is not possible to change the reference state of ports from which a reference connection originates.

### Adding New Devices in the Editor

In Edit mode, all determined devices are in the topology display. If these devices are deleted from the topology display via the context menu, they appear in the "Device hierarchy". You can move individual devices using drag & drop, or add all devices at once to the topology display using the context menu.

#### 7.1.4. Online Mode

If a Reference topology already exists, the topology is displayed in online mode when the "Network monitoring > Topology" page of an Operation is called up.

In online mode, you can monitor the devices and the current network topology taking into account the configured Reference topology. Deviations between determined and configured states are optically highlighted by SINEC NMS.

#### 7.1.5. Views

With a very large number of monitored devices, the monitored topology can quickly become unclear.

In SINEC NMS, you have the option of separately monitoring individual sections from the total scope of the monitored network. You can use your own monitoring groups for the following examples:

- Your reference system consists of many devices and connections and a general view is too confusing.
- They are only interested in parts of the monitored topology, e.g. ring topologies.

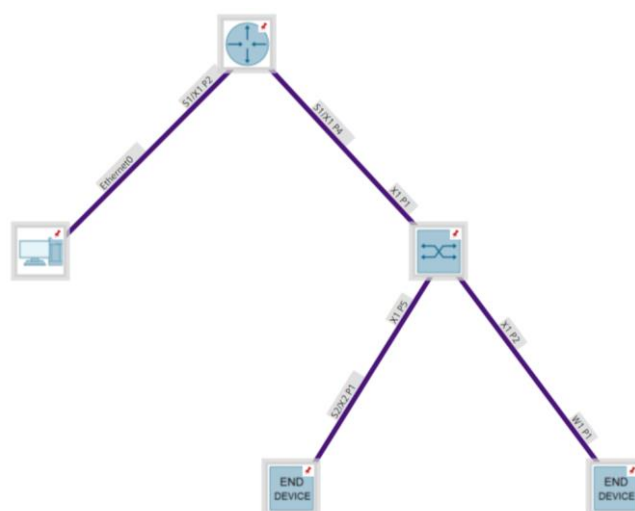
These smaller, manageable monitoring groups make it easier to manage and monitor devices and their connections.

#### 7.1.6. Topological Representation

The devices, connections and ports that SINEC NMS has detected and assigned with the protocols are automatically displayed in a topological view.

##### Devices

In both topology modes, SINEC NMS places the detected devices in the topology display and networks them with each other based on their connections. Each device is represented by a node in which the symbol of the corresponding device type is displayed.



Devices that are not part of the Reference topology are displayed with a star icon in both topology modes. Reference instruments are displayed without the star icon.

Devices whose device positions are fixed in the topology view are indicated by a pin symbol.

SINEC NMS displays devices without ascertainable connection information separately from the networked devices in the topology display. If a device without a discoverable IP address is connected to three or more devices, the device without a discoverable IP address is represented by a cloud icon.

## Connections

The connections between the devices are represented by lines in all topology modes.

In Edit mode, the lines are represented by the following color coding:

- Current connections in violet color
- Learned connections in brown color
- Reference Connections in black color

The following rules shall apply:

- If several connection types apply, the corresponding connection colors are displayed in combination.
- If the current and learned connection types apply, only the current connection is displayed.

The connection lines in online mode correspond to the connection lines in Edit mode with regard to the ports connected. Current connections that have not been defined as Reference Connections are displayed with a star icon.

If a Reference Connection between two ports does not match the current connection or one of the learned connections, the connection color is red. Otherwise the connection color depends on the fill color of the two connected ports. Wireless, optical, electrical and unknown connections are represented by different line types. If, for example, a wireless connection is involved, the connection line is displayed in a close-meshed dashed line.

The following Table shows an overview of the connection types and their representation:

Table 7-2

| Connection type                                                                     | Description           |
|-------------------------------------------------------------------------------------|-----------------------|
|  | Wireless connection   |
|  | Optical connection    |
|  | Electrical connection |
|  | Unknown connection    |

## Partial connections

If SINEC NMS cannot determine a connection port of at least one device, partial connections are formed. Partial connections can be recognized by the fact that there is no port on at least one side of the connection. This compound is referred to as a "partial compound".

The following types of partial connections are to be distinguished:

- Type A: port-to-device connection
- Type B: device-to-device connection

Partial connections are displayed according to the same rules as conventional connections. Partial connections cannot be used immediately as Reference Connections. First, the ports involved must be selected in the connection wizard.

In online mode, the color of a completed Reference Connection is formed by synchronizing it with the determined connection information. For partial connections of type A, the connection color for matching connection information is determined by the fill color of the port.

## 7.2. Making Network Topology Visible

To visually monitor the network, you can use SINEC NMS to generate a graphical representation of the network structure.

The following steps are necessary to set up the target topology of the network to be monitored:

1. Open and set up topology
2. Make optional corrections
3. Activate online mode

### 7.2.1. Opening and Setting up Topology

The topology represents the currently determined actual state of the network. It shows a network topology that SINEC NMS calculates on the basis of the information determined with SNMP and PROFINET.

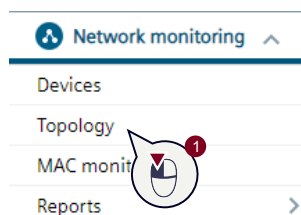
#### Requirement

You are on the Operations web interface and have logged in as the Default Administrator.

#### Open topology

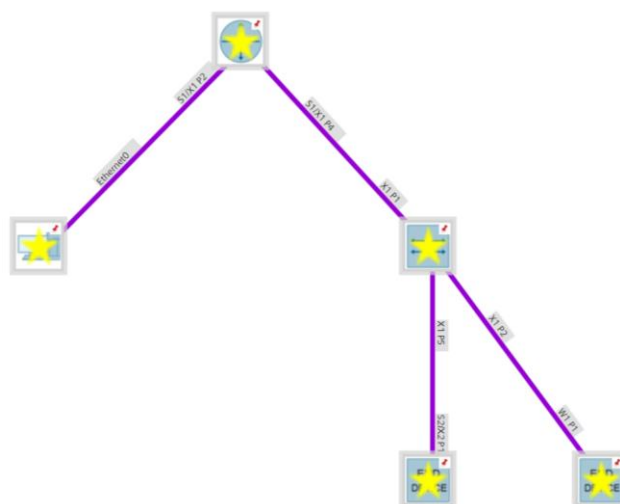
1. Click Network Monitoring > topology to open the topology.

Figure 7-4



2. The topology opens in Edit mode (🔧 icon). The view shows the topology layout of the devices, the port, and the connections. Devices that are not part of the Reference topology are displayed with a star icon.

Figure 7-5



The Edit mode allows you to make corrections and additions to the determined Actual topology and thus define a target state of the network.

The mode in which the topology opens depends on the following factors:

- If no Reference topology has yet been created and you have the right to edit the topology, the topology is displayed in Edit mode.
- If a reference topology already exists, the topology is displayed in online mode after selecting the "Topology" menu command.

### Check topology

The topology shows the physical arrangement of devices and their connections to each other, the SINEC NMS calculates on the basis of the information determined with LLDP.

Depending on the information provided by the devices in the network, the determined topology may differ from the real network topology.

If the topology does not show all devices, or if it shows the wrong devices, the following causes may be responsible:

Table 7-3

| Cause                                                                  | Remedy                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Devices are detected for which SNMP and/or PROFINET is deactivated.    | Check the accessibility of the stations via SNMP or PROFINET and activate SNMP or PROFINET in the affected devices.<br>Delete the corresponding module from the device list and run a new scan.                                           |
| Devices are detected via DCP, but the SNMP information cannot be read. | Check the SNMP settings in the device. For correct and successful device detection, the SNMP settings in the network devices and in the SINEC NMS must match.<br>Delete the corresponding module from the device list and run a new scan. |
| There are devices in the status "unmanaged" in the network.            | SINEC NMS cannot specify these devices. In the Reference topology, you can manually insert devices in the "unmanaged" status to complete the display.                                                                                     |
| Connections are not displayed or displayed incorrectly.                | Not all devices support the LLDP neighborhood detection protocol.<br>In the Reference topology, you can insert connections manually.                                                                                                      |
| Media modules in use are not recognized.                               | If new modules are inserted into a module that is already monitored by SINEC NMS, they are not immediately recognized by SINEC NMS.<br>Delete the corresponding module from the device list and run a new scan.                           |
| PROFINET devices are not recognized or displayed incorrectly.          | Check whether there are duplicate PROFINET device names in your network.                                                                                                                                                                  |

## Moving Devices in the Topology View

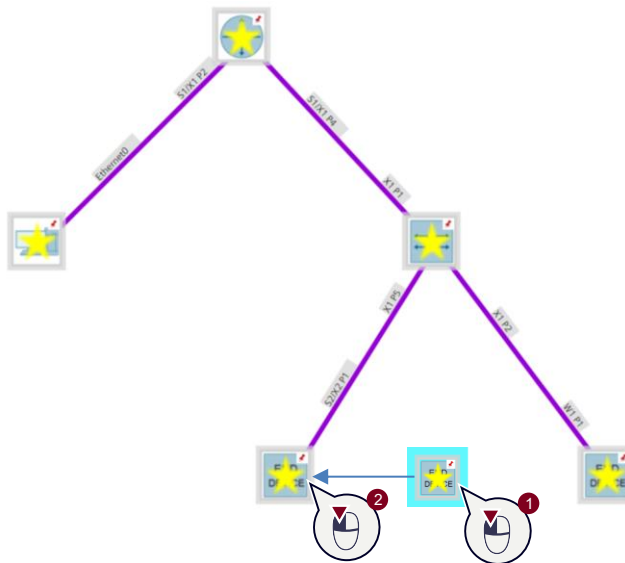
You can move devices in the topology view.

1. To do this, choose the selection tool from the toolbar.



2. Move the device to the desired position using drag & drop.

Figure 7-6



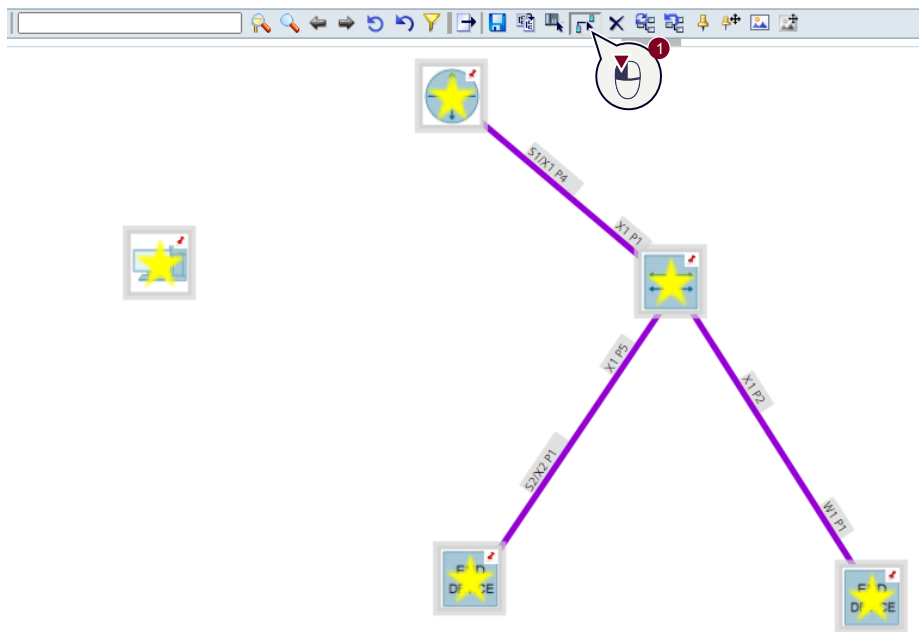
## Correct and adjust connections

If the connection information determined deviates from the reference state, you can also draw Reference Connections manually.

Proceed as follows:

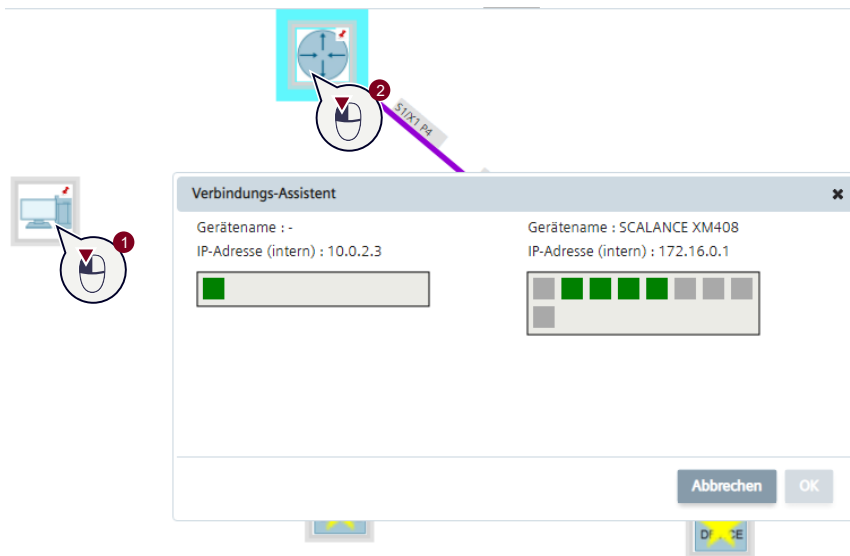
1. Use the selected tool in the toolbar to activate the Draw tool.

Figure 7-7



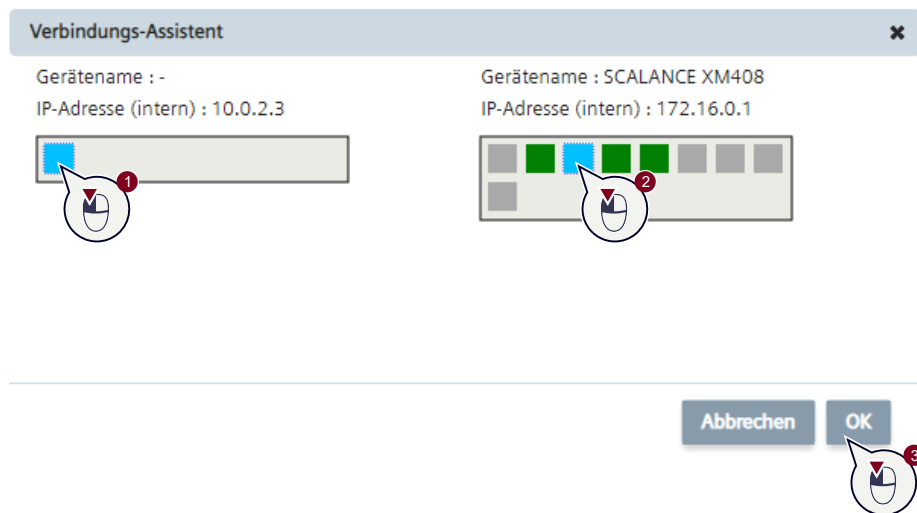
2. To draw reference connections manually, click the devices to be connected one after the other. The Connection Wizard opens.

Figure 7-8



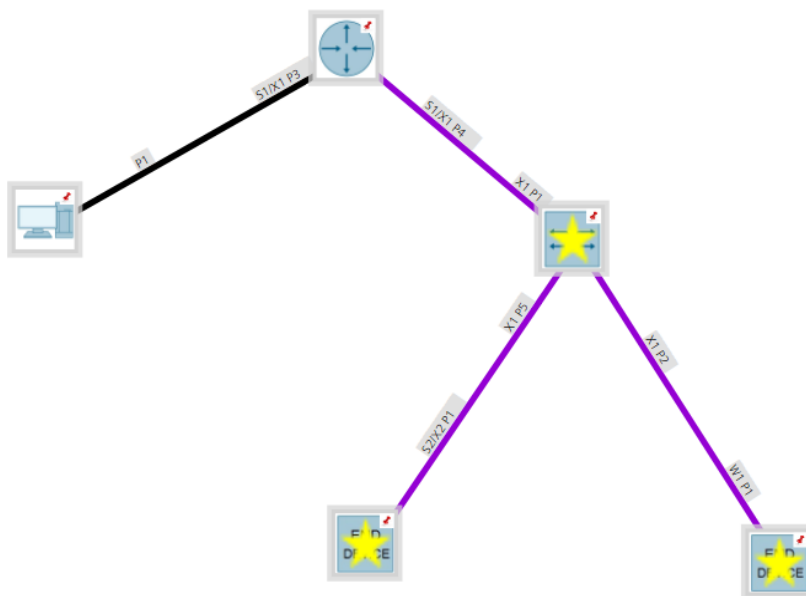
- Click one after the other on the ports of the devices to be connected. Confirm your selection with "OK".

Figure 7-9



- The reference connection (black color) between IPC and SCALANCE XM408 has been added.

Figure 7-10



### Transfer reference without correction

If the determined topology already matches your desired target configuration, you can transfer the determined states to the monitored topology without making any changes.

This applies to the following states:

- Determined devices are accepted as reference devices.
- Determined port states are accepted as reference states.
- Current and learned connections are accepted as Reference Connections.

Follow these steps for this purpose:

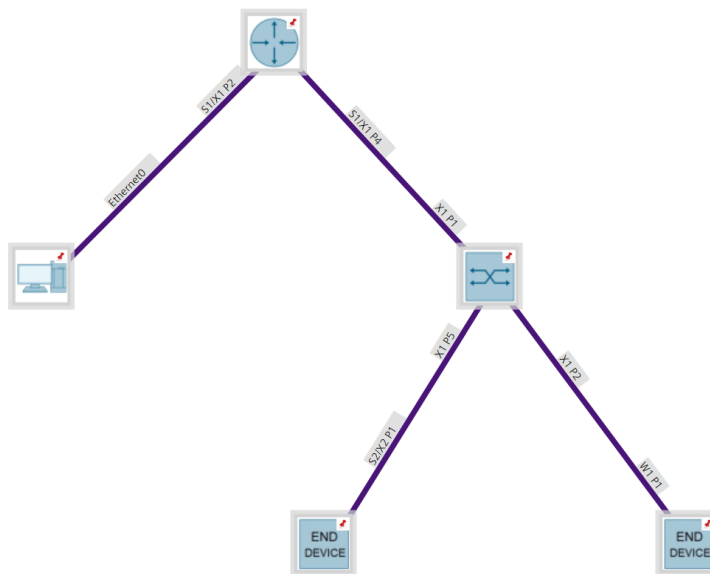
1. Click the selected tool in the toolbar. With the function "Adopt determined statuses as reference statuses" you can define the topology determined by SINEC NMS as a whole as a reference.

Figure 7-11



2. The colored compounds of the determined topology now appear as black-violet Reference Connections. The star icons are removed from the devices.

Figure 7-12



3. To save the Reference topology, click the selected tool.

Figure 7-13



### Result

The Reference topology is the basis for displaying the topology in online mode.

### Accepting individual devices and connections as references

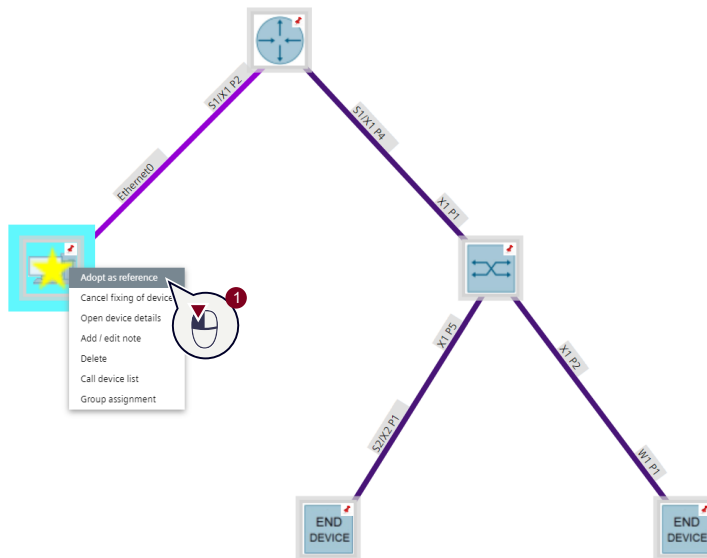
You can also use individual devices and connections as references. Devices that are not part of the Reference topology are displayed with a star icon in both topology modes. Current connections that are not part of the Reference topology are displayed in online mode with a star icon.

Proceed as follows:

1. For devices:

Click with the right mouse button on the device and select the corresponding entry in the context menu.

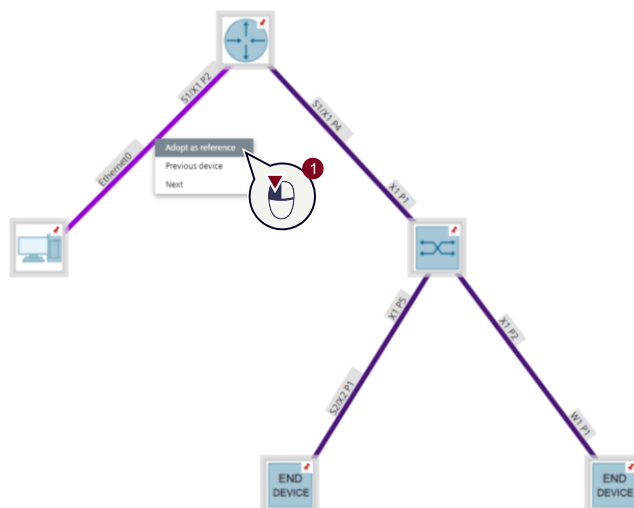
Figure 7-14



2. For Connections:

Right-click the connection and select the corresponding entry from the context menu. Alternatively, you can change the reference state by double-clicking the connection.

Figure 7-15

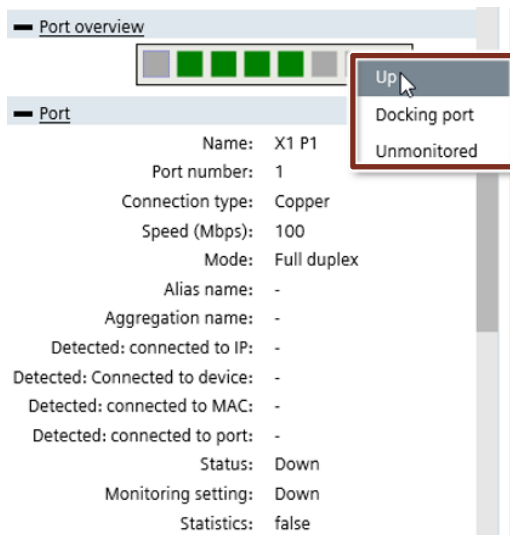


## Correcting and adjusting ports

The "Port Overview" area in the sidebar displays the determined states and the configured reference states of the ports of the selected device.

If the port information determined deviates from the reference state, right-click the port and select the desired reference state.

Figure 7-16



## Extended icon view and topology settings

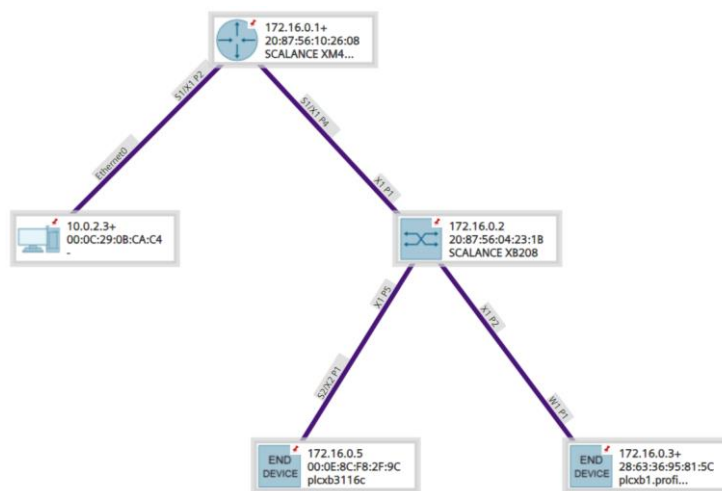
1. To select the extended Icon view, click the selected tool.

Figure 7-17



2. The topology appears in the extended Icon view.  
In the extended Icon view, up to three additional device properties are displayed that can be configured in the topology settings.  
To return to the symbol view, click the corresponding tool.

Figure 7-18



To define the topology settings, you must be in Edit mode. Proceed as follows:

1. Click the selected tool in the toolbar.

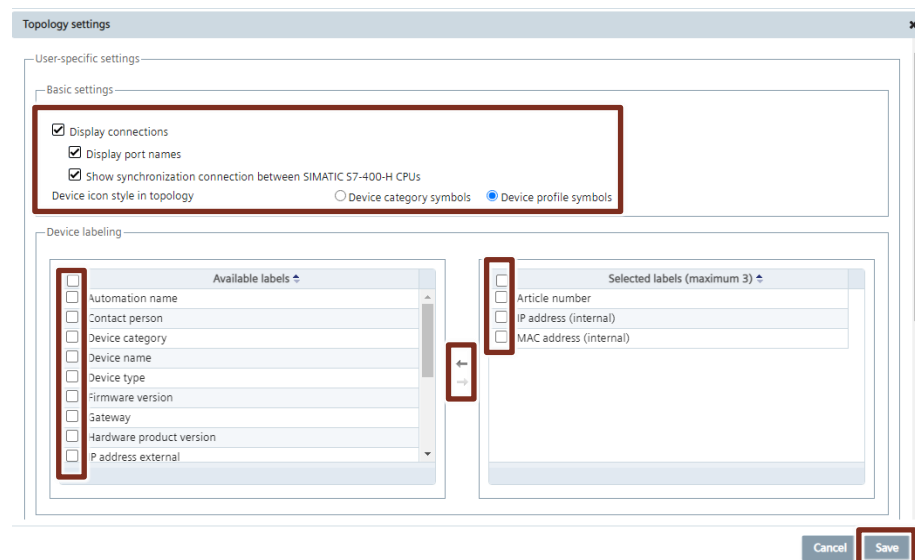
Figure 7-19



2. Select the desired options in the dialog that appears. Two columns are visible for the device label. The left pane shows the available device properties that can be displayed. All currently displayed device properties are listed in the right area.

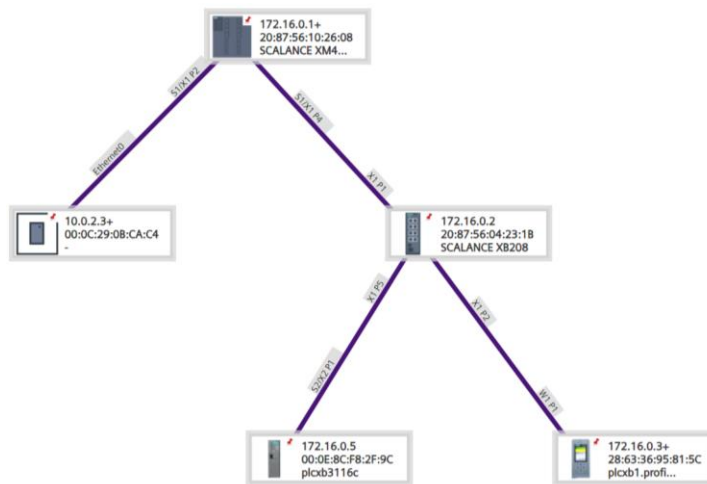
Select the device properties to be displayed in the topology from the left column. Use the arrows to move the selection to the right column. You can select up to three device properties. Close the dialog with the "Save" button.

Figure 7-20



3. The topology displays the information based on the new settings.

Figure 7-21



### Activate or deactivate Edit mode and Online mode

To switch to Online mode, proceed as follows:

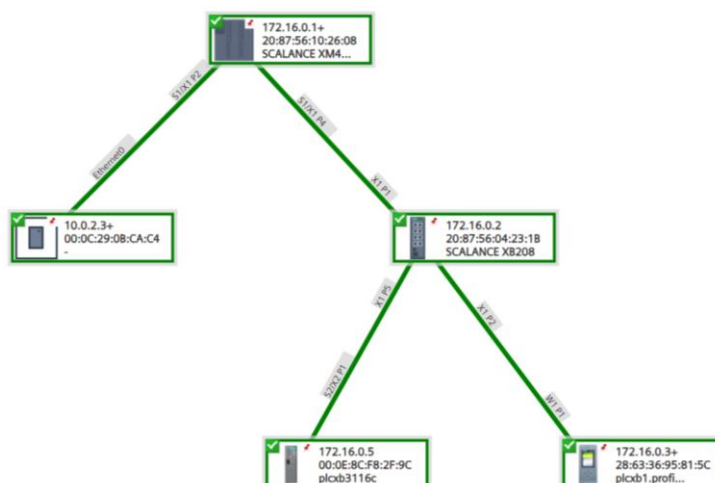
1. To switch to Online mode, click the selected tool

Figure 7-22



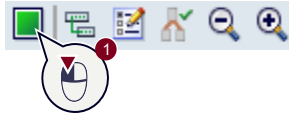
2. The topology appears in Online mode.

Figure 7-23



- To return to Edit mode, click the selected tool.

Figure 7-24



### 7.2.2. Topology in the Online Mode

The topology in online mode is the result of the synchronization between the determined Actual Topology and the adjustments from the Reference topology.

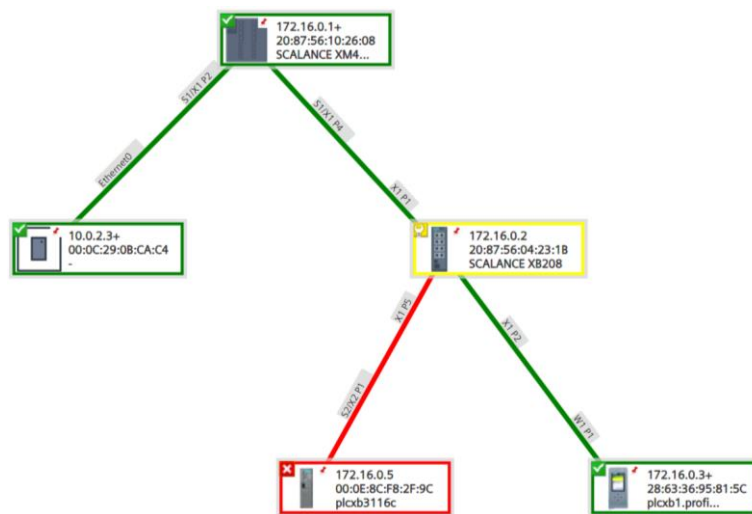
The following information is displayed in the monitored topology:

- Port states resulting from the determined topology and the Reference topology.
- Port connections resulting from the determined topology and the Reference topology. The resulting states of the ports involved are also included in the representation of the port connections.

#### Testing the monitored topology

The monitored topology helps you to monitor your network. In the following screenshot the connection to the CPU 317-2 PN/DP was removed in the reference system for testing purposes. SINEC NMS detects the status change and displays the error.

Figure 7-25



#### Result

SINEC NMS detects faulty connections and displays them graphically and port granularly.

## 8. Other SINEC NMS Features

This document is intended to support the first user and to give him an understanding of the basic functions and setting options of SINEC NMS.

SINEC NMS offers you even more features:

### UMC users

UMC (User Management Component) is a database for the central administration of user data. In SINEC NMS, the UMC users can be used after the UMC user groups have been included by specifying the UMC user group names. An Editor is available for integrating the UMC user groups.

### Policy Control Center

A policy can be used to plan and perform tasks for configuring and managing devices. The devices and tasks of a policy can be freely combined within the scope of the existing permissions. Before executing a policy, SINEC NMS uses the available device functions to determine for which of the devices which tasks can actually be executed.

### Firmware management

In firmware management you can manage firmware files and label them with keywords. The keywords can be used when configuring tasks in policies and in the configuration cockpit to determine the firmware files to be loaded to devices.

Firmware files are managed on the Control in firmware containers and automatically provided to the Operations. Each change to the firmware containers in the Control is automatically synchronized with the Operations. When major changes are made to the firmware containers, synchronization with the Operations can take some time.

### Configuration cockpit

Individual configuration tasks for devices and device interfaces can be performed in the configuration cockpit. In contrast to configuration via the Policy Control Center, you select the devices or interfaces to be configured directly in the configuration cockpit and then always select a task that is to be executed for the devices or interfaces. This task is then executed immediately.

### Reports

SINEC NMS offers a range of reports for network monitoring and analysis. The data for the reports is obtained exclusively from the Operation on which the report is created. The following report types are available:

- Availability
- Performance
- Inventory
- Events
- Validation reports
- In the Control there are the reports "Stock" and "Availability", which can be executed time-Controlled and regularly, e.g. monthly. You can download the reports as CSV files or send them automatically by email.

## 9. Appendix

### 9.1. Service and support

#### SiePortal

The integrated platform for product selection, purchasing and support - and connection of Industry Mall and Online support. The SiePortal home page replaces the previous home pages of the Industry Mall and the Online Support Portal (SIOS) and combines them.

- **Products & Services**  
In Products & Services, you can find all our offerings as previously available in Mall Catalog.
- **Support**  
In Support, you can find all information helpful for resolving technical issues with our products.
- **mySieportal**  
mySiePortal collects all your personal data and processes, from your account to current orders, service requests and more. You can only see the full range of functions here after you have logged in.

You can access SiePortal via this address: [sieportal.siemens.com](https://sieportal.siemens.com)

#### Industry Online Support

Industry Online Support is the previous address for information on our products, solutions and services.

Product information, manuals, downloads, FAQs and application examples - all information is available with just a few mouse clicks: [support.industry.siemens.com](https://support.industry.siemens.com)

#### Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form: [support.industry.siemens.com/cs/my/src](https://support.industry.siemens.com/cs/my/src)

#### SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page: [siemens.com/sitrain](https://siemens.com/sitrain)

#### Industry Online Support app

You will receive optimum support wherever you are with the "Industry Online Support" app. The app is available for iOS and Android:



## 9.2. Links and literature

| No. | Topic                                                                                                                                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11\ | SiePortal<br><a href="https://sieportal.siemens.com/en-ww/">https://sieportal.siemens.com/en-ww/</a>                                                                                           |
| 12\ | Link to the article page of the application example<br><a href="https://support.industry.siemens.com/cs/ww/en/view/109762792">https://support.industry.siemens.com/cs/ww/en/view/109762792</a> |
| 13\ | SINEC NMS manual<br><a href="https://support.industry.siemens.com/cs/ww/en/view/109973629">https://support.industry.siemens.com/cs/ww/en/view/109973629</a>                                    |
| 14\ | SINEC NMS V3.0<br><a href="https://support.industry.siemens.com/cs/ww/en/view/109973059">https://support.industry.siemens.com/cs/ww/en/view/109973059</a>                                      |

## 9.3. Change documentation

| Version | Date    | Change                                         |
|---------|---------|------------------------------------------------|
| V1.0    | 03/2019 | First edition                                  |
| V1.1    | 03/2020 | Changes for the new version SINEC NMS V1.0 SP1 |
| V2.0    | 01/2022 | Changes for the new version SINEC NMS V1.0 SP2 |
| V3.0    | 09/2024 | Changes for the new version SINEC NMS V3.0     |
| V3.1    | 01/2026 | Formatting updated                             |