

SIEMENS

Ingenuity for life

Use and Understanding of SINEC NMS

SINEC NMS V1.0 SP1

<https://support.industry.siemens.com/cs/ww/en/view/109762792>

Siemens
Industry
Online
Support



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. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

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. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

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. 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://support.industry.siemens.com>) shall also apply.

Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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 Security RSS Feed at: <https://www.siemens.com/industrialsecurity>.

Table of Contents

Legal information	2
1 Introduction	5
1.1 Overview.....	5
1.2 SINEC NMS	6
1.3 Reference System	8
2 Setting Up and Starting SINEC NMS.....	10
2.1 Installation	10
2.1.1 Useful Information about Installation	10
2.1.2 Installing SINEC NMS	11
2.2 Automation License Manager	14
2.3 Web Interface	15
2.3.1 Useful Information about the Web Interface.....	15
2.3.2 Logging On for the First Time to the Control Web Interface	17
3 Control: Perform System Administration.....	21
3.1 Operation Parameter Profile.....	21
3.1.1 Useful Information about the Operation Parameter Profile	21
3.1.2 Initial Login Data.....	22
3.2 Operation Management.....	24
3.2.1 Useful Information about Operation Management	24
3.2.2 Add Operation to System	27
3.2.3 Exporting a Certificate	30
4 Operation: Carrying Out Initial Commissioning	31
4.1 Useful Information about Initial Commissioning	31
4.2 Carrying Out Initial Commissioning	31
5 Network Monitoring	34
5.1 Detecting Devices in the Network	34
5.1.1 Useful Information about Network Scan.....	34
5.1.2 Useful Information about Monitoring on the Control	35
5.1.3 Useful Information about Monitoring on the Operations	37
5.1.4 Starting a Network scan Automatically and Manually on Control	40
6 Operation: Understanding and Filtering the Event List.....	42
6.1 Useful Information about Events	42
6.2 Adapt Event List	44
7 Operation: Understanding and Using Topology	51
7.1 Useful Information about Topology	51
7.1.1 General Information.....	51
7.1.2 Work Areas and Operation.....	51
7.1.3 Edit Mode	52
7.1.4 Online Mode	55
7.1.5 Views	55
7.1.6 Representation in Topology	56
7.2 Making Network Topology Visible	58
7.2.1 Opening and Setting Up Topology	58
7.2.2 Topology in the Online Mode	70
8 Other SINEC NMS Features	71
9 Appendix	72
9.1 Service and support	72

Table of Contents

9.2	Links and literature	73
9.3	Change documentation	73

1 Introduction

1.1 Overview

Motivation

This document assists the user and introduces them to the basic functions and settings of SINEC NMS. The chapter 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 chapters and sub-chapters are usually identical and have a modular structure. The chapters begin with the theory section “Useful information”, which explains the fundamentals and principles of the function. This chapter 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

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:

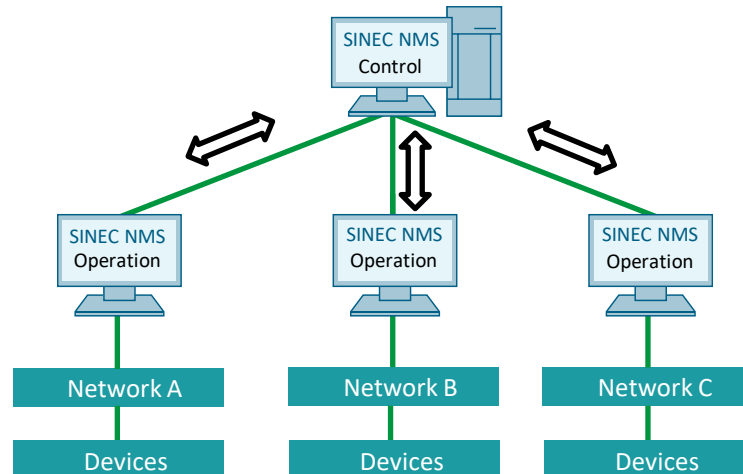
- SINEC NMS detects all devices in the network. This provides a constantly updated overview of all installed components including all essential properties in the network.
- The plant Topology is automatically read out, depicted and monitored for changes.
- Diagnostic data is collected from all network participants 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 large number of interfaces (e.g. HTTPS, OPC UA) enable network and diagnostic data to be displayed and further processed 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 rights for entire system.

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



You configure the monitoring settings to be used by the Operations centrally at the Control and then load them onto 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.

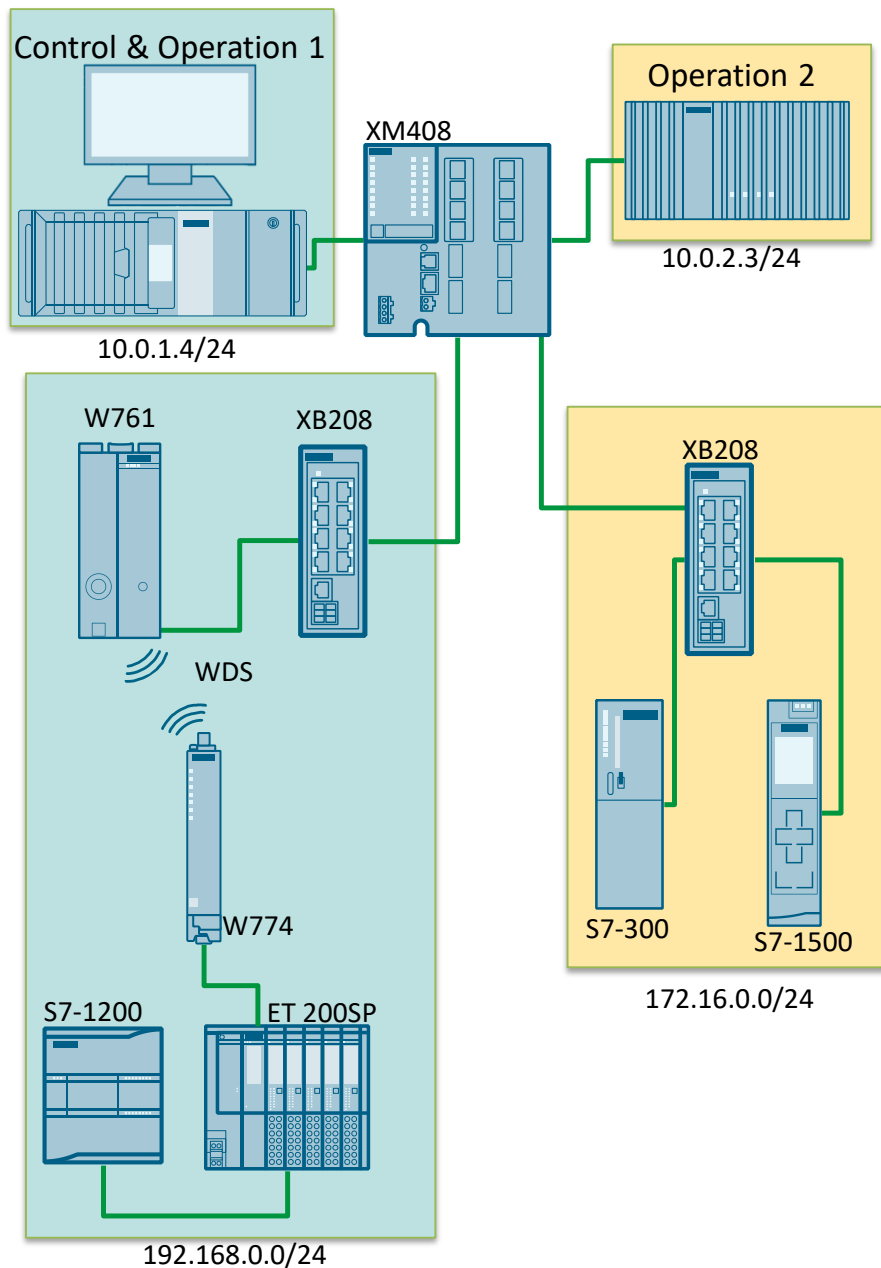
1.3 Reference System

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 facility consists of two 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 fixed 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 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.

You set up the UMC server during installation.

Note

By using UMC users, you can use 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 [Chapter 9.1](#)).

SINEC NMS test

To get to know and test SINEC NMS, there is a test license ("Trial 500"). This supports a maximum of three devices in the "Managed" management status and a maximum of 500 devices in the "Monitored" management status.

A license of this type is standard and valid for a period of 21 days. This license is activated automatically, if no other license type is found during the first commissioning of SINEC NMS by the automation license manager. A system with an expired trial license can be reactivated by adding a full license.

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.

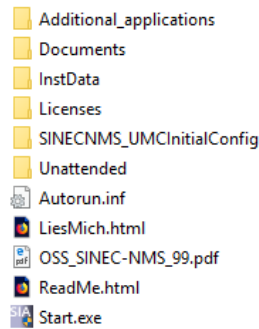
2.1.2 Installing SINEC NMS

Obtain software

The SINEC NMS software can be downloaded from Siemens Industry Online Support (see \4\ in [Chapter 9.1](#)).

The software is provided as a self-extracting archive. The directory contains the following components:

Figure 2-1



Alternatively, you can also 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

Table 2-1

Operating system	<ul style="list-style-type: none"> • Microsoft Windows 10 (Pro/Enterprise), Version 1709 or higher • Microsoft Windows Server 2016 • Microsoft Windows Server 2019
Supported operating system languages	<ul style="list-style-type: none"> • German • English
Web browser	<ul style="list-style-type: none"> • Google Chrome 78.0 or higher • Firefox 70 or later • Microsoft Edge* • Internet Explorer 11.0* <p>*The web browser is only supported to a limited extent</p>
Screen resolution	1920 x 1080 pixels

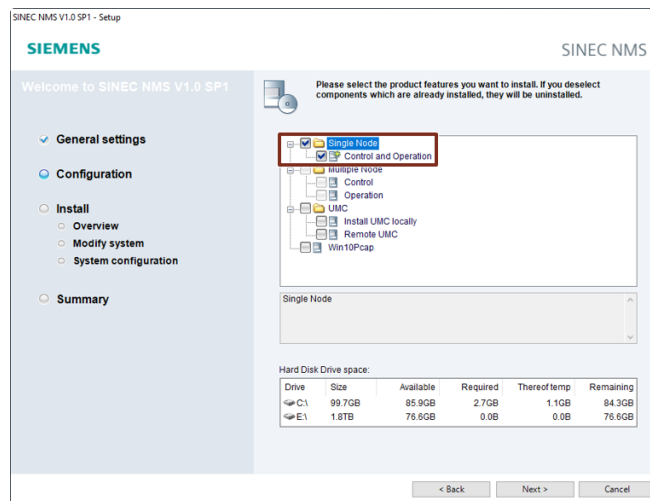
Software installation

To install a Control or Operation, proceed as follows:

1. Start the file “Start.exe” with administrator rights and select a language for the installation wizard. Then click the “Next” button.
2. Define the languages to be installed and click the “Next” button.
3. Select which components of SINEC NMS should be installed. The following options are available:

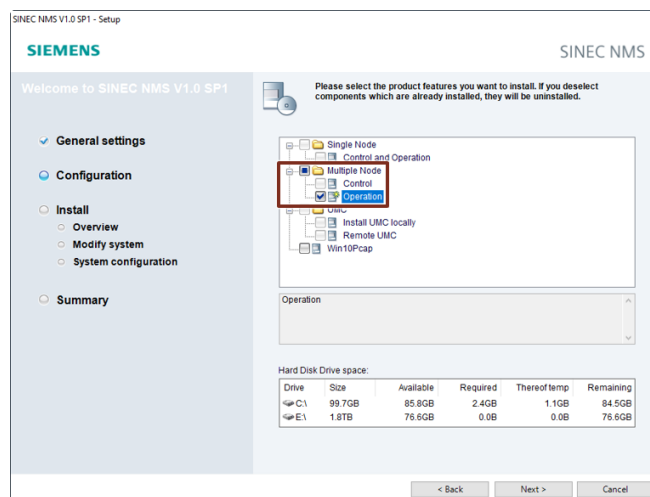
- Single Node Installation: The Control and an Operation are installed on the same PC.

Figure 2-2



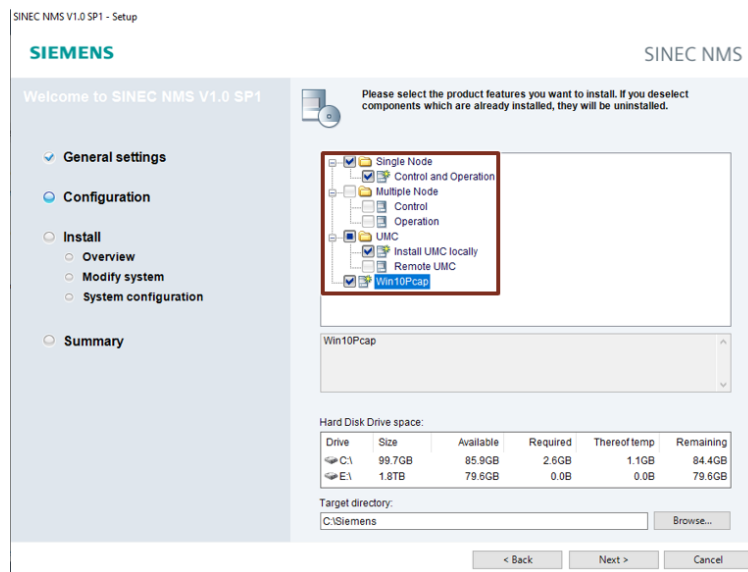
- Multiple Node Installation: The Control or Operation is installed.

Figure 2-3



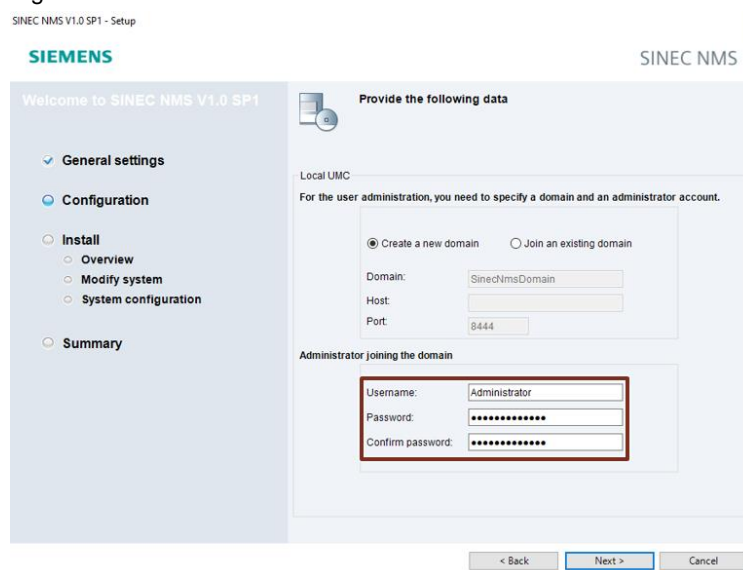
4. Select whether you want to install a UMC server or use an existing UMC server. If you do not need a UMC server, do not select either of the two options. Click the “Next” button.

Figure 2-4



5. 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 2-5

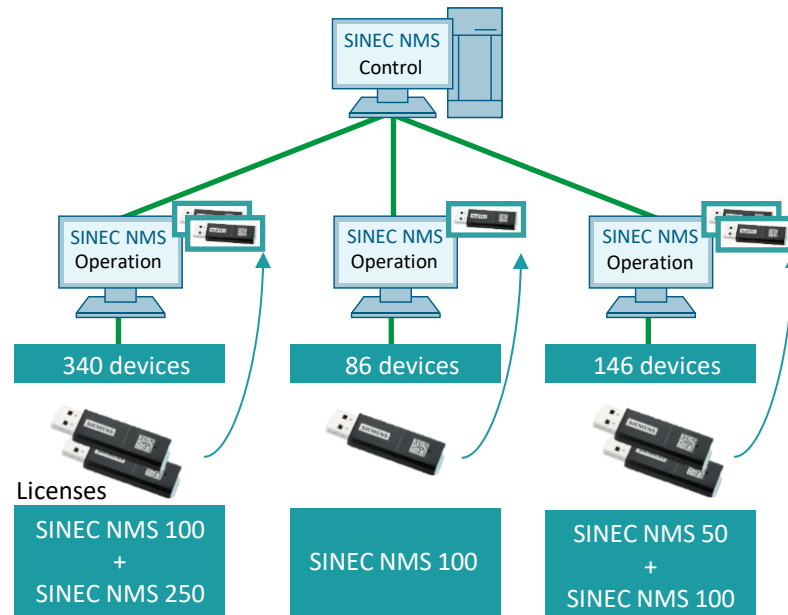


6. Select the desired Trap service to be used.
7. Follow the instructions of the installation wizard.
8. Restart the PC after the installation is complete.
9. After restarting the PC, SINEC NMS is started automatically and you can log on to the web interface.

2.2 Automation License Manager

Only the SINEC NMS Operations with the size of the devices to be monitored are licensed. The different license packages can be combined with each other so that the existing number of supported devices can be increased up to max. of 500 devices per SINEC NMS Operation.

Figure 2-6



License keys are transferred via the supplied Automation License Manager (ALM). The following steps show you how to transfer a license via a USB stick.

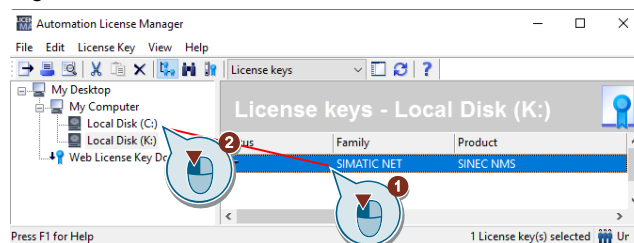
1. Insert the USB stick into your PC.
2. Close the Automation License Manager.

Figure 2-7



3. 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 at Entry 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.

For SINEC NMS V1.0 SP1, one of the following web browsers is required:

- Firefox 70 or later
- Google Chrome 78.0 or higher
- Microsoft Edge*
- Internet Explorer 11.0*

*These web browsers are only supported to a limited extent

You start the Web interface of the Control using a URL in the Web browser.

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)
- About the actions on the Web interface of the Control (see [Chapter 5](#))

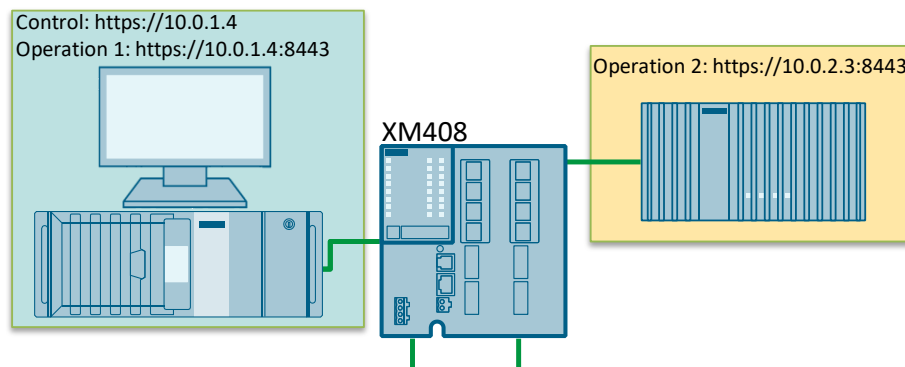
URLs of the Web interface

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

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

Figure 2-9



Signing into the web interface

SINEC NMS offers two ways to log on to 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:
 - User name: SuperAdmin
 - Password: sinecnms

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.
After logging in to the Control for the first time, you will be prompted to change the password for this user. Use a secure password and remember it well. If the password is lost, it may be necessary to reinstall SINEC NMS.

Note

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

2.3.2 Logging On for the First Time 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 on to the Control and an Operation.

After the first login to the Control, the password of this user must be changed.

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.
2. Log in with your preconfigured login data.

- User name: SuperAdmin

- Password: sinecnms

Click on “Login”.

Figure 2-10

SIEMENS
Ingenuity for life

SINEC NMS

© 2020 Siemens AG. All rights reserved.

Welcome to SINEC NMS

Default credentials are required for the first login.

SuperAdmin

.....

Forgot password?

Log in

3. You will be prompted to define a new password. Enter the old and new password in the corresponding input fields. Then click the “Submit” button.
4. The password was changed. To register again, click the link.

5. Log in as SuperAdmin with your new password.
Click on “Login”.

Figure 2-11

UMC Login Local Login

SIEMENS
Ingenueity for life

Welcome to SINEC NMS

SuperAdmin

.....

Forgot password? Log in

SINEC NMS

© 2020 Siemens AG. All rights reserved.

6. The start page of the Control appears.

Note

The default administrator of SINEC NMS is now:

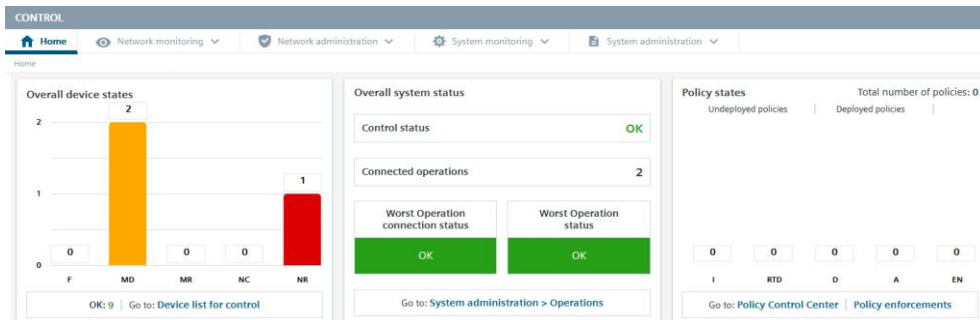
- User name: SuperAdmin
- Password: <the password you have defined>

Start page

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

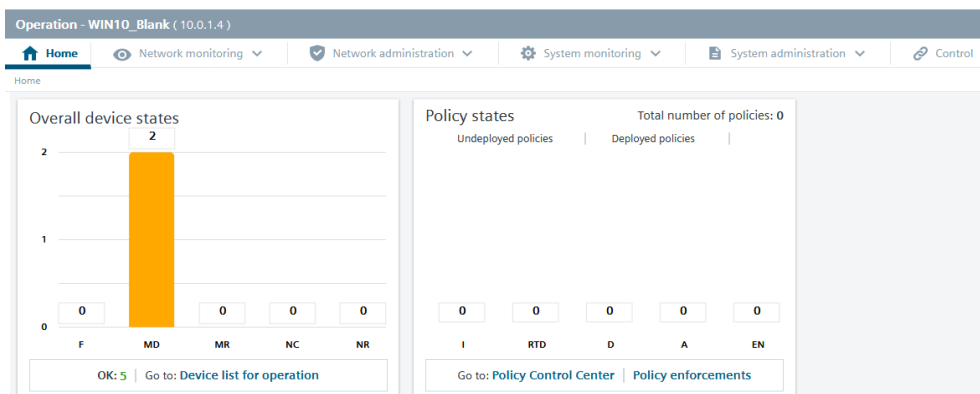
The following figure shows the start page of the Control. It contains a summary of the overall status of devices as well as status information on Control, Operations and policies.

Figure 2-12



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 2-13



Area “Overall device status”

In the “Total device states” area, the numbers of total states of monitored devices are displayed in a bar chart. The number of devices in the overall state “OK” is indicated below the bar chart. The overall status of the devices is indicated by the following abbreviations and colors.

Table 2-2

Device status	Color identification
F: Error	
WA: Maintenance requested	
WE: Service necessary	
NV: Not connected	
NE: Not accessible	

Area “Overall system status” (only visible at the Control)






The following states are displayed in the “Overall system status” area:

- 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.
- Worst Operation connection condition: Specifies whether all Operations can be reached by the Control.
- Worst Operation state: This state indicates whether there are error states on an Operation. 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.
 - Warning: A warning message exists for an Operation.
 - OK: There are no errors or warnings.

Area “Policy states”

The “Policy states” area displays the number of states of all global policies in a bar chart. This chapter is divided into the sub-chapters “Unloaded Policies” and “Loaded Policies”. A warning icon is displayed next to the Loaded Policies area if one or more policies on an Operation of SINEC NMS have been suspended due to inconsistencies. The states of policies are indicated by the following abbreviations and colors.

Table 2-3

Policy states	Color identification
I: Inconsistent	
FZL: Ready for loading	
D: Disabled	
A: Enabled	
WA: Being executed	

3 Control: Perform 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 in the manual under the Entry ID: [109777115](#).

Changing parameters

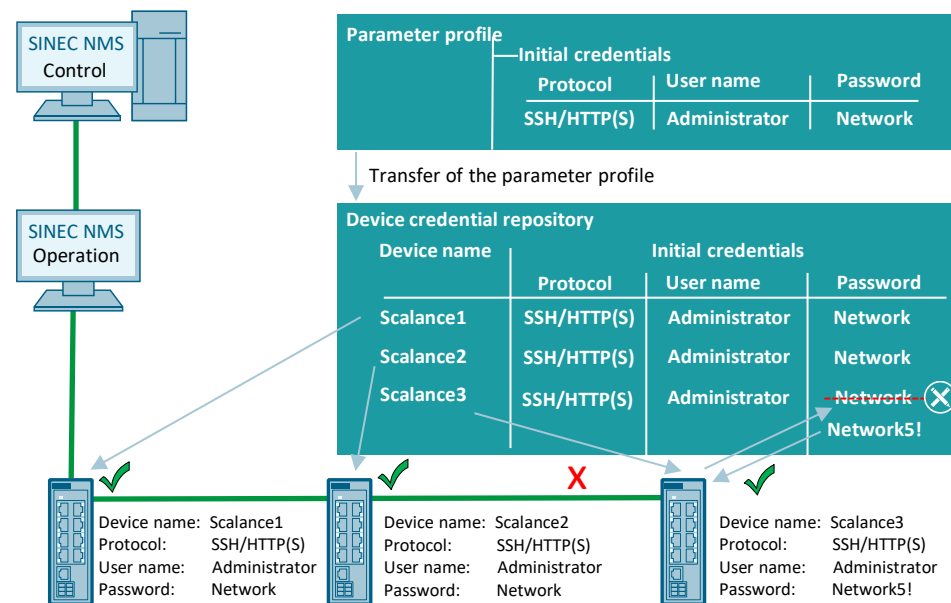
Changes in a parameter group for which the “Global” or “User global” property is displayed in the “Parameter groups” area are applied to all existing parameter profiles, including the start profile. For changes in a local parameter group, you can specify whether these changes are to be applied only to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

3.1.2 Initial credentials

SINEC NMS requires device credentials to establish SNMP and SSH connections to the devices. The login data is defined in the System administration → Operation parameter profile → Initial credentials. The individual Operations use the parameter profile by default.

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

Figure 3-1

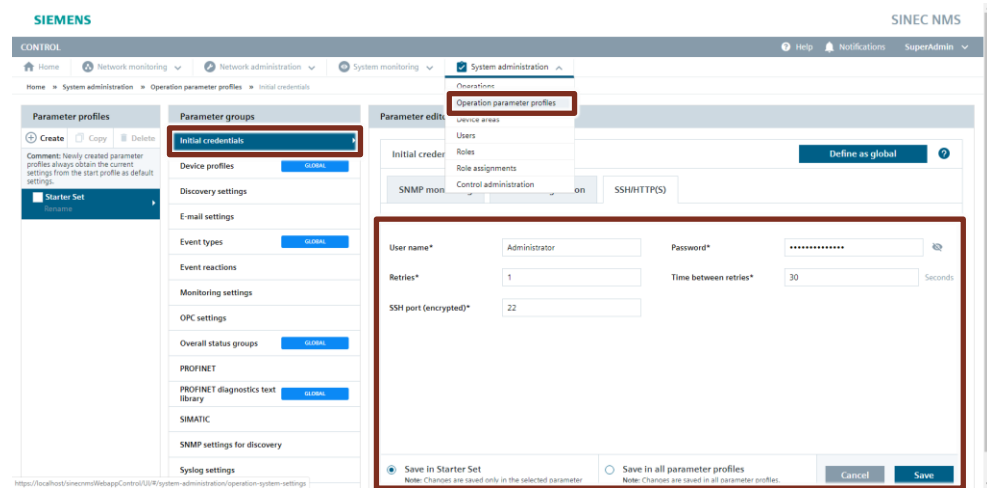


3 Control: Perform System Administration

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

Open the web interface of the Control <https://<IP address of Control>>. Navigate to the configuration page “System Administration > Operation Parameter Profile > Initial credentials”. Configure your initial credentials data via SNMP and SSH/HTTP(S). Save your settings. You can create additional SNMP profiles under the SNMP settings for discovery.

Figure 3-2



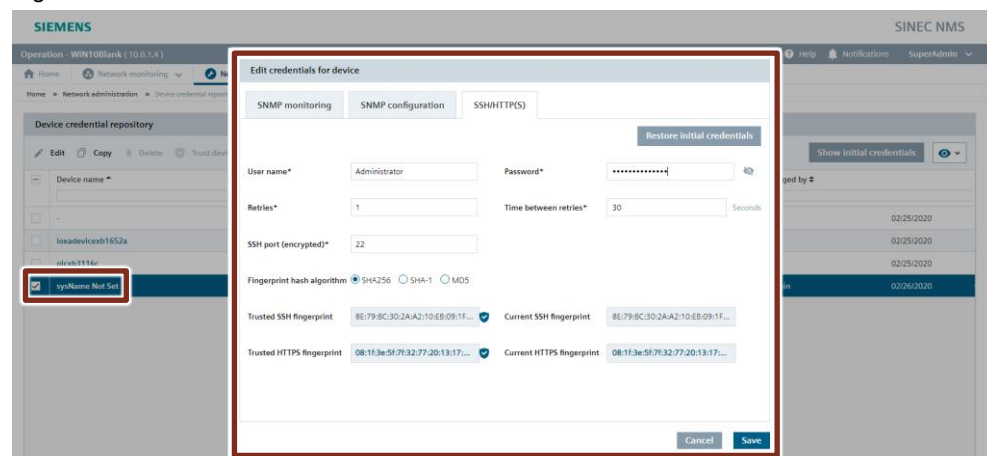
To configure the initial credentials in the Operation, proceed as follows.

Note

Please note that you can only edit the initial credentials locally after a network scan (see [Chapter 3.2.2](#)).

Open the web interface of the Operation <https://<IP address of Operation>>. Navigate to the configuration page “Network Administration > Device credential repository”. Select the device you want to edit under Device Name. Configure your initial credentials data via SNMP and SSH/HTTP(S). Save your settings.

Figure 3-3



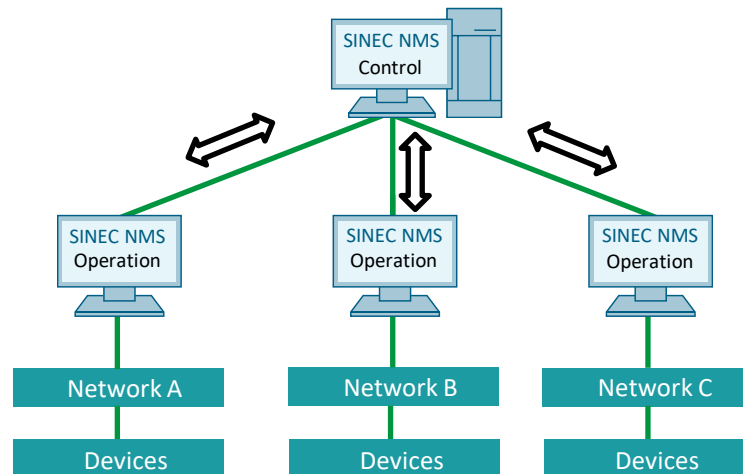
3.2 Operation Management

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

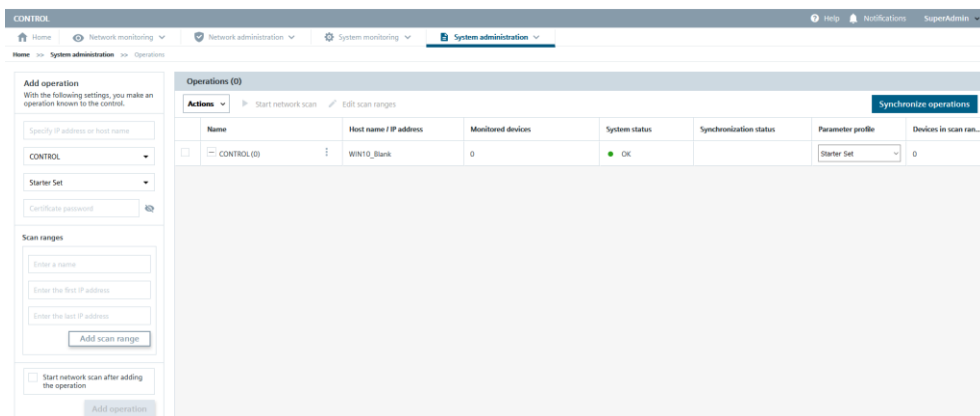
A Control only monitors and administers the Operations that you have made known in the Control and configured using an Operation parameter profile.

Configuration page in Control

To make an Operation known in the Control, use the “System Administration > Operations” configuration page.

The page is divided into the Chapters “Add Operation” and “Operations”. Operations added using the controls in the Add Operation area are displayed in the Operations area.

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
- Scan area

You can find more information on the individual elements in the manual under the Entry ID: [109777115](#).

Note

To speed up the network scan, the scan ranges should be limited to the IP addresses of the devices to be monitored. 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 under the Entry ID: [109777115](#).

Synchronize Operations/Synchronization Required

If you have made changes to the configuration of Operations in the Control, 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.

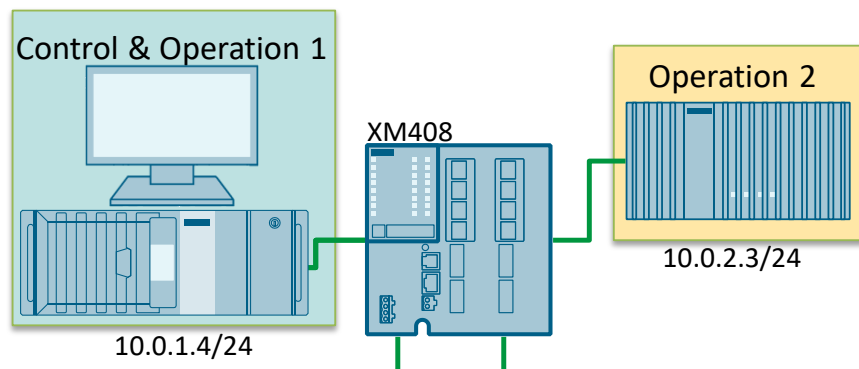
3.2.2 Add Operation to System

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”.

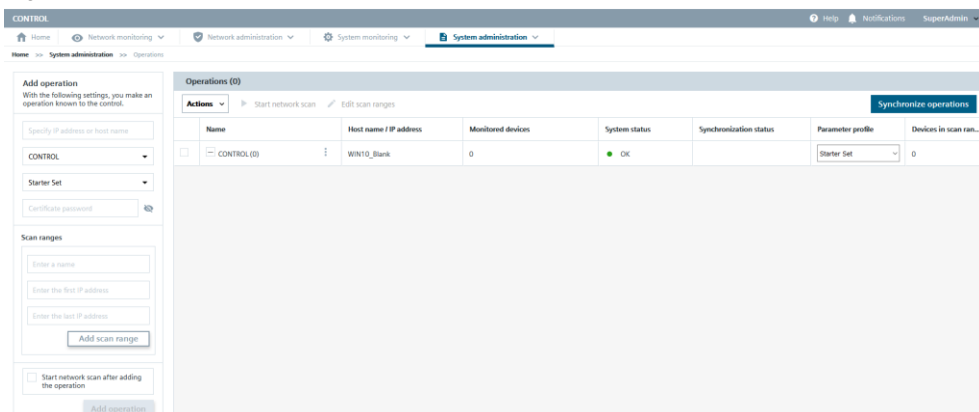
Requirement

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



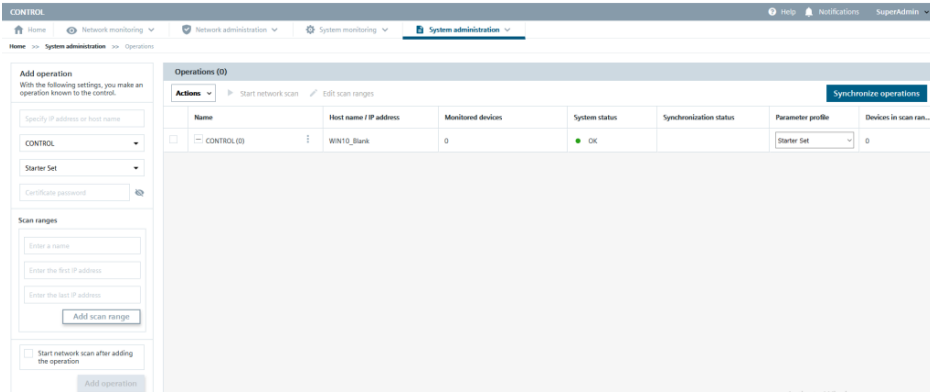
Add Operation

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 enter or select 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 area	Operation1	Operation2
First IP address	192.168.0.1	172.16.0.1
Last IP address	192.168.0.30	172.16.0.30

3. To accept the scan area, click the “Add scan range” button. You can define up to 100 scan areas per Operation.

Figure 3-9

Add operation
With the following settings, you make an operation known to the control.

10.0.1.4

CONTROL

Starter Set

.....

Scan ranges

Operation1

192.168.0.1

192.168.0.30

Add scan range

4. Check the option "Start network scan after adding the Operation".

Figure 3-10

☒ Start network scan after adding the operation

5. To add the Operation to the system, click the "Add Operation" button.

Figure 3-11

Scan ranges

FIRST IP ADDRESS	LAST IP ADDRESS	
192.168.0.1	192.168.0.30	✕

Enter a name

Enter the first IP address

Enter the last IP address

Add scan range

☒ Start network scan after adding the operation

Add operation

6. Check the initial login data in your device login data directory (see Chapter [3.1.2](#))
7. 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 3-12

Operations (2)							
Actions		Start network scan		Edit scan ranges		Synchronize operations	
Name	Host name / IP address	Monitored devices	System status	Synchronization status	Parameter profile	Devices in scan ran...	
CONTROL (2)	WIN10_Blank	7	OK		Starter Set	60	
WIN10_Blank	WIN10_Blank / 10.0.1.4	7	OK		Starter Set	30	
10.0.2.3	10.0.2.3 / 10.0.2.3	0	First contact		Starter Set	30	

3.2.3 Exporting a Certificate

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.

For a single node installation (here: “Operation 1”) the authentication works automatically, because Control and Operation are installed on the same PC.

In order for a multi-node installation to authenticate itself to Control, you need the certificate.

To download the Operation certificate, proceed as follows:

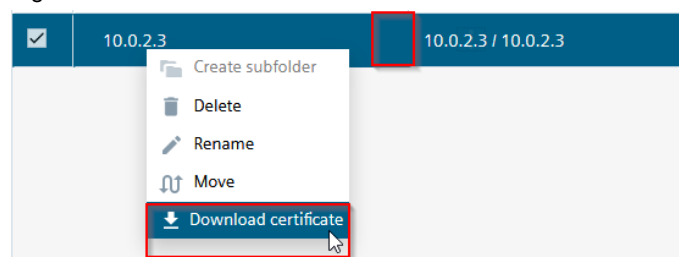
1. In the “Operations” area, select the Operation that you want to authenticate.

Figure 3-13

CONTROL (2)	WIN10_Blank	7	OK	Starter Set	60
WIN10_Blank	WIN10_Blank / 10.0.1.4	7	OK	Starter Set	30
<input checked="" type="checkbox"/> 10.0.2.3	10.0.2.3 / 10.0.2.3	0	First contact	Starter Set	30

2. Select the “Download certificate” menu command from the context menu of the Operation. This downloads the certificate for the private key Operation as a PKCS12 container.

Figure 3-14



3. Place the PKCS12 container in a directory that you can access from the Operation.

Figure 3-15

SSLCertificates_10.0.2.3.zip

Result

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

4 Operation: Carrying Out 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.

For a single node installation (here: Unit “Control & Operation 1”) the authentication works automatically, because Control and Operation are installed on the same PC.

So that a multi-node installation (here: Unit “Operation 2”) at 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 areas configured for the Operation on the Control under System Administration > Operations.

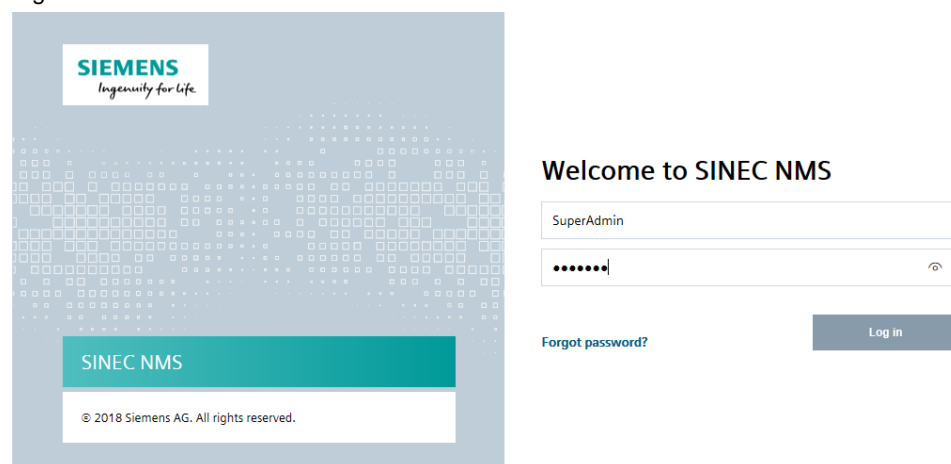
4.2 Carrying Out Initial Commissioning

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>.

The logon dialog appears.

Figure 4-1



Importing a Certificate

You have downloaded the certificate for the Operation from the Control in the [Chapter 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. Log on using the default login data:
 - User name: SuperAdmin
 - Password: sinecnmsClick "Login".
2. You will automatically be redirected to the "Import Certificate" dialog.

Figure 4-2

SINEC NMS V1.0

Import certificate

Certificate

Password

Import

Import message

Information

The user needs to log on again after synchronization of this operation with the control.

Log out

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

Figure 4-3

SINEC NMS V1.0

Import certificate

Certificate
 SSLCertificates_10.0.2.3.zip

Password

Import

Import message

Information
 The user needs to log on again after synchronization of this operation with the control.

Log out

4. Log out of Operation.

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 on to the Operation with this user data.

The system status of the Operation in the Control changes from “First Contact” to “OK”.

Figure 4-4

Operations (2)							
Actions		Start network scan		Edit scan ranges		Synchronize operations	
	Name	Host name / IP address	Monitored devices	System status	Synchronization status	Parameter profile	Devices in scan ran...
<input checked="" type="checkbox"/>	CONTROL (2)	WIN10_Blank	12	OK		Starter Set	60
<input type="checkbox"/>	WIN10_Blank	WIN10_Blank / 10.0.1.4	7	OK		Starter Set	30
<input type="checkbox"/>	10.0.2.3	10.0.2.3 / 10.0.2.3	5	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 Network Scan

Network Scan

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

You specify the scan area to be scanned when configuring the Operation on the Control (see [Chapter 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 port numbers.

5.1.2 Useful Information about Monitoring on the Control

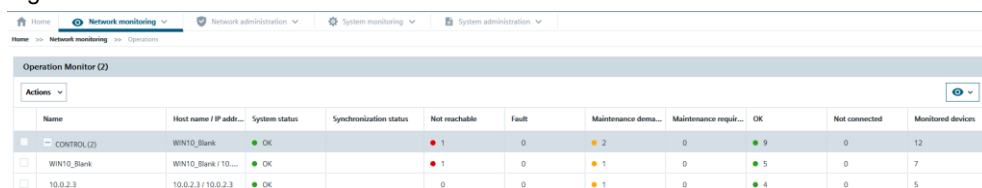
The Control allows you to monitor the Operations and the entire network.

Monitoring of the Operations

On the Network Monitoring > Operations Control page, you can 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

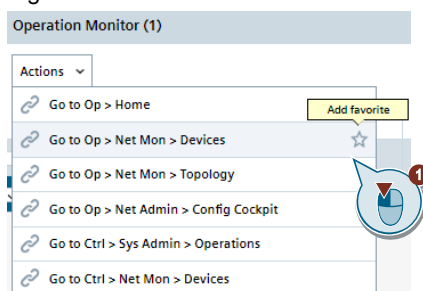
Figure 5-1



Name	Host name / IP address	System status	Synchronization status	Not reachable	Fault	Maintenance demo...	Maintenance requi...	OK	Not connected	Monitored devices
CONTROL (2)	WIN10_Blank	OK		1	0	2	0	9	0	12
WIN10_Blank	WIN10_Blank / 10...	OK		1	0	1	0	5	0	7
10.0.2.3	10.0.2.3 / 10.0.2.3	OK		0	0	1	0	4	0	5

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.

Figure 5-2



Monitoring 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:

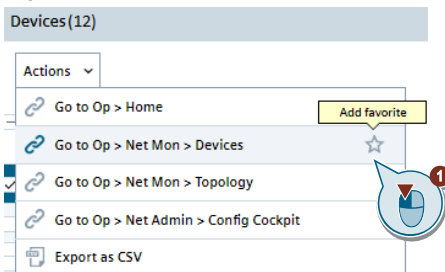
- State
- IP address
- System name
- Operation
- Device type
- MAC address
- Reason for overall condition

Figure 5-3

Status	IP address	System name	Operation	Device type	Category	MAC address	Initial discovery	Article number	Configuration
Not reachable	192.168.0.101		WIN10_Blank	CPU 1212C DCDCDC (1...	PLC		Today		Allowed
Maintenance demanded	192.168.0.2/24	sysName Not Set	WIN10_Blank	SCALANCE XB208 PN (B...	Switch	20:87:56:04:23:38	Today	6GK5 208-0BA00-2AB2	Allowed
Maintenance demanded	172.16.0.3/24	sysName Not Set	10.0.2.3	SCALANCE XB208 PN (B...	Switch	20:87:56:04:24:08	Today	6GK5 208-0BA00-2AB2	Allowed
OK	10.0.1.4/24		WIN10_Blank	Management Station	Others	00:0C:29:38:13:FD	Today		Allowed
OK	192.168.0.1/24	sysName Not Set	WIN10_Blank	SCALANCE XM408-BC (L...	Router	20:87:56:0C:4C:00	Today	6GK5 408-8GR00-2AM2	Allowed
OK	192.168.0.14/24	sysName Not Set	WIN10_Blank	SCALANCE W761-1 R4...	Access Point	00:18:18:58:61:35	Today	6GK5 761-1XC00-0AA0	Allowed
OK	192.168.0.13/24	sysName Not Set	WIN10_Blank	SCALANCE W774-1 R4...	Access Point	20:87:56:98:05:FD	Today	6GK5 774-1XC00-0AA0	Allowed
OK	192.168.0.11/24	sysName Not Set	WIN10_Blank	ET 200SP IM155-6 PN S...	End Device	28:63:36:51:18:81	Today	6ES7 155-6AU00-0BN0	Allowed
OK	172.16.0.5/24		10.0.2.3	CPU 317-2 PN0P (ZEK1...	PLC	00:05:8C:F8:2F:9C	Today	6ES7 317-2EK14-0AB0	Allowed
OK	169.254.0.104/16		10.0.2.3	Management Station	Others	02:18:18:EE:A7:00	Today		Allowed
OK	172.16.0.3/24		10.0.2.3	CPU 1513-1 PN (1AL01...	PLC	28:63:36:92:88:89	Today	6ES7 513-1AL01-0AB0	Allowed
OK	172.16.0.1/24	sysName Not Set	10.0.2.3	SCALANCE XM408-BC (L...	Router	20:87:56:0C:4C:00	Today	6GK5 408-8GR00-2AM2	Allowed

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.

Figure 5-4

**Note**

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

5.1.3 Useful Information about Monitoring on the Operations

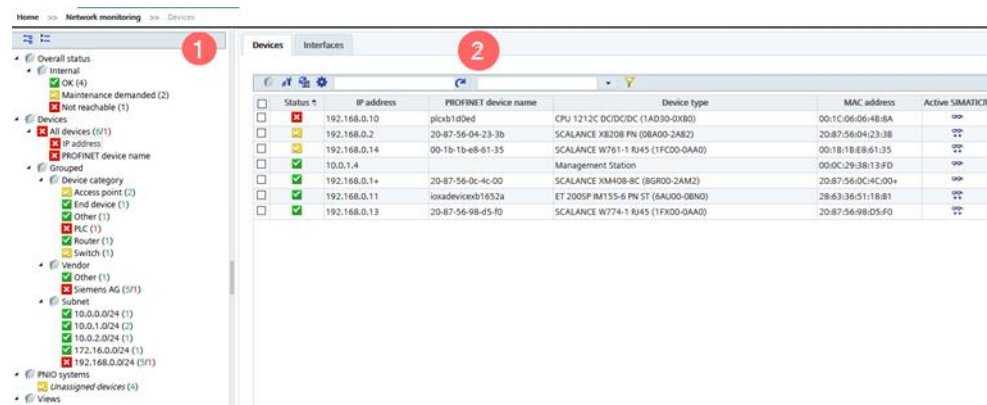
After the scan is complete, you can view the status of all network devices associated with the Operation.

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 area of the Operation.

Figure 5-5



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 total device states are possible:

Table 5-2

Icon	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.

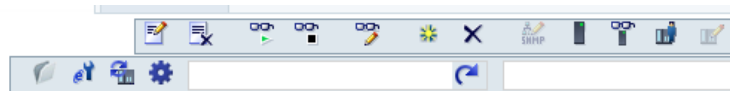
Depending on which entry you selected in the device tree, all devices or only a certain group are displayed in the device list.

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.

Figure 5-6



These include the following functions:

- Show device details for the selected device
- Open Web based Management
- Reread device data
- Adding comments
- Enable/disable monitoring
- Add new device manually
- Deleting a device
- Change device type

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.

Figure 5-7

Device details (192.168.0.1 / sysName Not Set)

Summary Status Description Config. LAN ports Events VLAN Redundancy IP Interfaces Expert

OK

Device identification

IP address	192.168.0.1	Name	sysName Not Set
Device category	Router	Device type	SCALANCE XM408-8C (8GR00-2AM)
Device MAC address	20:87:56:0C:4C:00	System location	sysLocation Not Set
		Hierarchical name	C:0-0:1:192.168.0.1

Pending events

Error	0	Warnings	0
Information	0		

Notes

-

Close

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

5.1.4 Starting a Network scan Automatically and Manually on 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 [Chapter 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 [Chapter 3.1](#)).
- All Operations involved have successfully authenticated themselves at the Control and can be reached from the Control (see [Chapter 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”.

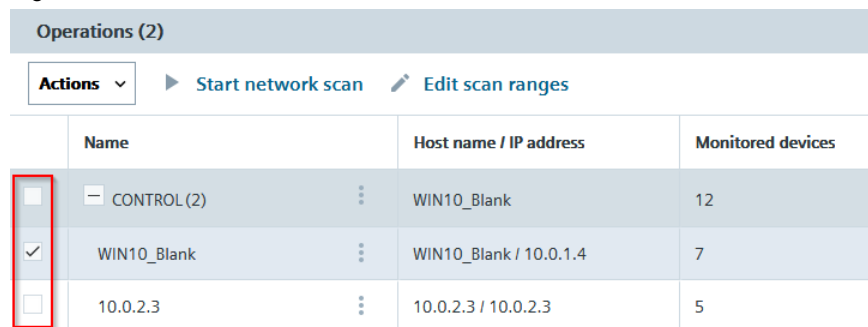
Start device detection manually

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.

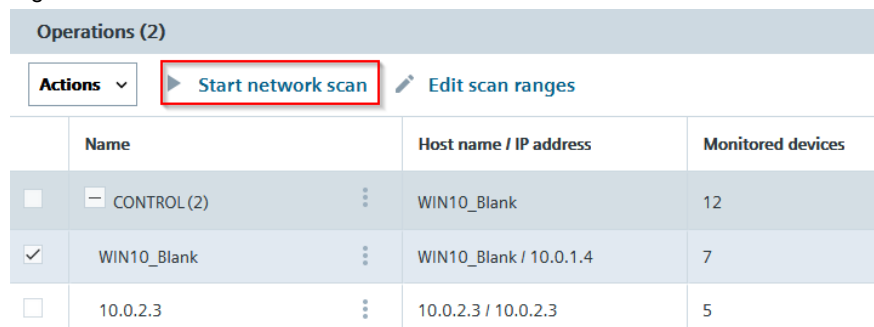
Figure 5-8



Operations (2)			
Actions ▾ ▶ Start network scan ✎ Edit scan ranges			
	Name	Host name / IP address	Monitored devices
<input type="checkbox"/>	CONTROL (2)	WIN10_Blank	12
<input checked="" type="checkbox"/>	WIN10_Blank	WIN10_Blank / 10.0.1.4	7
<input type="checkbox"/>	10.0.2.3	10.0.2.3 / 10.0.2.3	5

2. Click the “Start network scan” control element.


Figure 5-9



Operations (2)			
Actions ▾ ▶ Start network scan ✎ Edit scan ranges			
	Name	Host name / IP address	Monitored devices
<input type="checkbox"/>	CONTROL (2)	WIN10_Blank	12
<input checked="" type="checkbox"/>	WIN10_Blank	WIN10_Blank / 10.0.1.4	7
<input type="checkbox"/>	10.0.2.3	10.0.2.3 / 10.0.2.3	5

- During the network scan, the system status “Network scan in progress” is displayed in the Monitored Devices column.

Figure 5-10

	Name		Host name / IP address	Monitored devices
<input type="checkbox"/>	CONTROL (2)	⋮	WIN10_Blank	12
<input checked="" type="checkbox"/>	WIN10_Blank	⋮	WIN10_Blank / 10.0.1.4	7  Executing network scan
<input type="checkbox"/>	10.0.2.3	⋮	10.0.2.3 / 10.0.2.3	5

6 Operation: Understanding and Filtering the Event 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 rating, 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"> Events with the assigned overall status "OK" or "Not connected" from the same overall status group Upcoming Events of the same overall status group (independent of the assigned overall status)
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 Clients.
2. Complex filter:
In the second Step, the data received from Clients 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 Adapt 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 information.

Figure 6-1

	Read	Event status	Event	Event class	Time stamp
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	Info	2019-01-16 13:04:41.949
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	Warning	2019-01-16 12:59:41.919
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	Info	2019-01-16 12:44:41.972
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	Warning	2019-01-16 12:39:41.926
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	Info	2019-01-16 10:49:41.872
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	Warning	2019-01-16 10:44:41.935
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	Info	2019-01-16 10:04:41.925

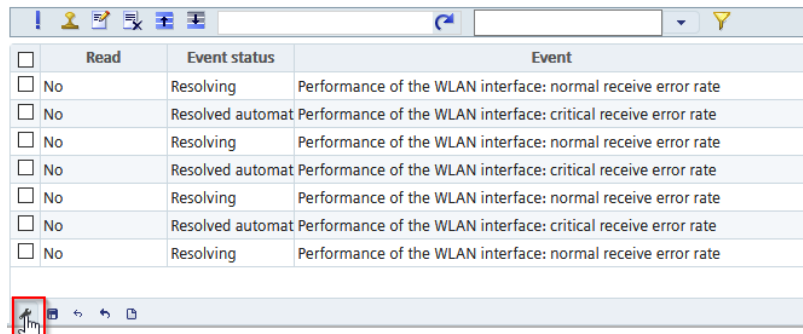
With the tools on the footer you can freely design the entire Table. You have the following options for change:

- 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.

Figure 6-2



<input type="checkbox"/>	Read	Event status	Event
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate

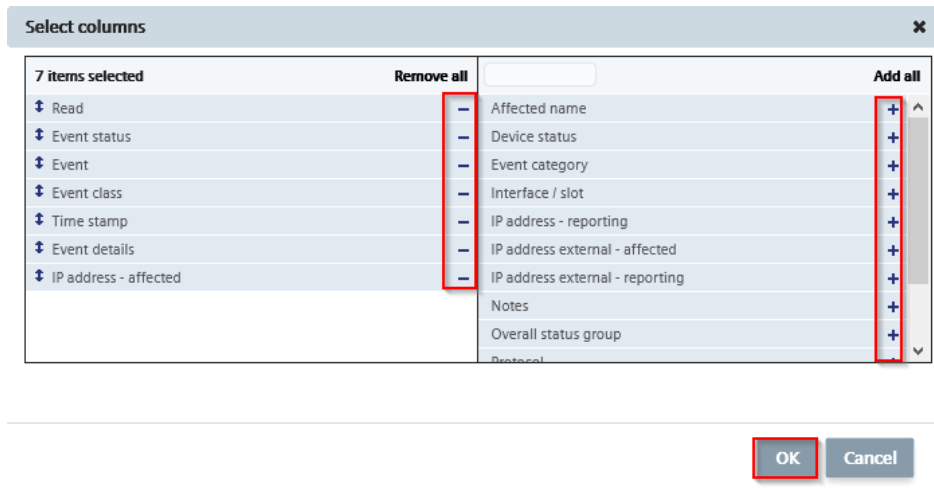
2. The column selection window opens. The breakdown is as follows:

- 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.

Figure 6-3



Select columns

7 items selected

Remove all

+

-

Read

Event status

Event

Event class

Time stamp

Event details

IP address - affected

Affected name

Device status

Event category

Interface / slot

IP address - reporting

IP address external - affected

IP address external - reporting

Notes

Overall status group

Protocol

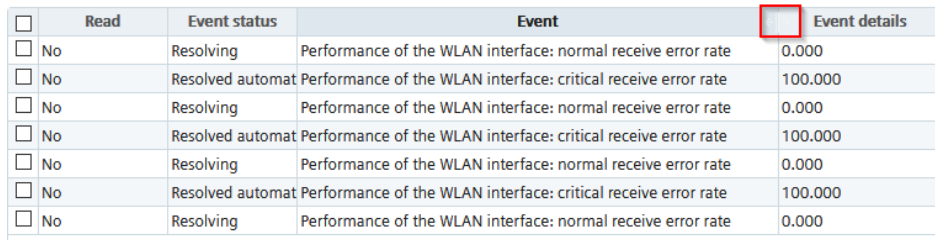
Add all

OK

Cancel

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

Figure 6-4



<input type="checkbox"/>	Read	Event status	Event	Event details
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000

© Siemens AG 2020 All rights reserved

SINEC NMS
Entry ID: 109762792, V1.1, 03/2020

45

- To accept the changes, click the selected tool.

Figure 6-5

<input type="checkbox"/>	Read	Event status	Event	Event details
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000

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.

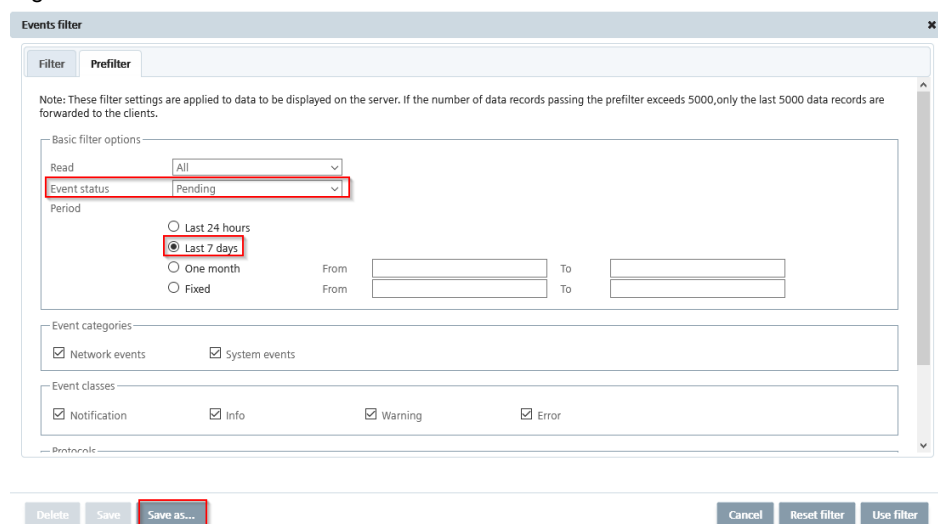
Figure 6-6



<input type="checkbox"/>	Read	Event status	Event	Event details
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000
<input type="checkbox"/>	No	Resolved automat	Performance of the WLAN interface: critical receive error rate	100.000
<input type="checkbox"/>	No	Resolving	Performance of the WLAN interface: normal receive error rate	0.000

2. The “Event Filter” dialog box appears. Change to the “Prefilter” tab. Set the filter, e.g. “The last 7 days pending”. To save the prefilter, click “Save as...”.

Figure 6-7



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

☐ One month

☐ Fixed

From: To:

Event categories

☒ Network events ☒ System events

Event classes

☒ Notification ☒ Info ☒ Warning ☒ Error

Protocol:

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".

Figure 6-8

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

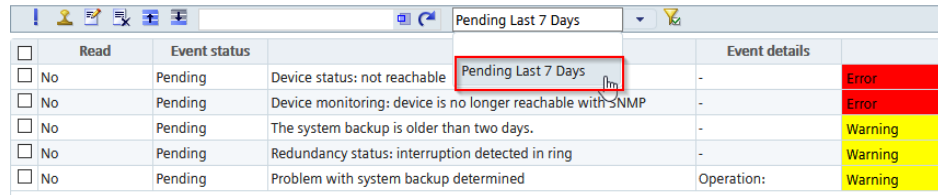
Figure 6-9

5. To apply the filter, click the "Apply Filter" button.

Figure 6-10

- 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 and press <ENTER>.

Figure 6-11



	Read	Event status	Event	Event details	
<input type="checkbox"/>	No	Pending	Device status: not reachable	Pending Last 7 Days	Error
<input type="checkbox"/>	No	Pending	Device monitoring: device is no longer reachable with SNMP	-	Error
<input type="checkbox"/>	No	Pending	The system backup is older than two days.	-	Warning
<input type="checkbox"/>	No	Pending	Redundancy status: interruption detected in ring	-	Warning
<input type="checkbox"/>	No	Pending	Problem with system backup determined	Operation:	Warning

Result

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

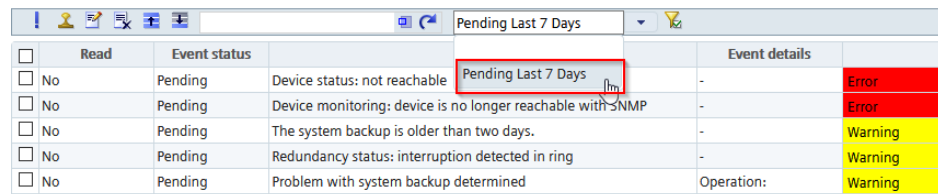
Resolve Event manually

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 prefilter “Pending Last 7 Days” you just created.

For a manual resolution, proceed as follows:

- Select the “Pending Last 7 Days” prefilter from the drop-down list. The Events are displayed in the Event list filtered according to the definition in the prefilter.

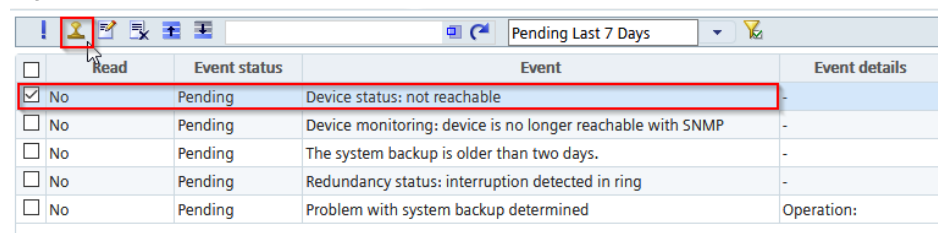
Figure 6-12



	Read	Event status	Event	Event details	
<input type="checkbox"/>	No	Pending	Device status: not reachable	Pending Last 7 Days	Error
<input type="checkbox"/>	No	Pending	Device monitoring: device is no longer reachable with SNMP	-	Error
<input type="checkbox"/>	No	Pending	The system backup is older than two days.	-	Warning
<input type="checkbox"/>	No	Pending	Redundancy status: interruption detected in ring	-	Warning
<input type="checkbox"/>	No	Pending	Problem with system backup determined	Operation:	Warning

- Select the desired Event in the Event list and click the selected tool.

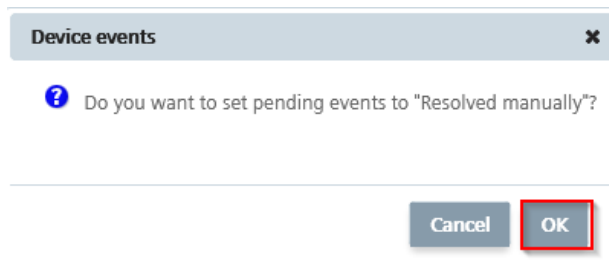
Figure 6-13



	Read	Event status	Event	Event details
<input checked="" type="checkbox"/>	No	Pending	Device status: not reachable	-
<input type="checkbox"/>	No	Pending	Device monitoring: device is no longer reachable with SNMP	-
<input type="checkbox"/>	No	Pending	The system backup is older than two days.	-
<input type="checkbox"/>	No	Pending	Redundancy status: interruption detected in ring	-
<input type="checkbox"/>	No	Pending	Problem with system backup determined	Operation:

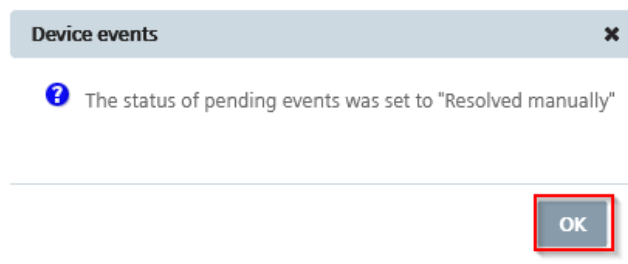
3. A new dialog appears to confirm the action. Click "OK".

Figure 6-14



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

Figure 6-15



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 about Topology

7.1.1 General Information

Monitoring with Topology

The device information recognizable by SINEC NMS also includes information about the respective neighboring devices. Using the SNMP and PROFINET protocols, SINEC NMS reads out neighborhood information and calculates a Topology representation using the LLDP protocol (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.

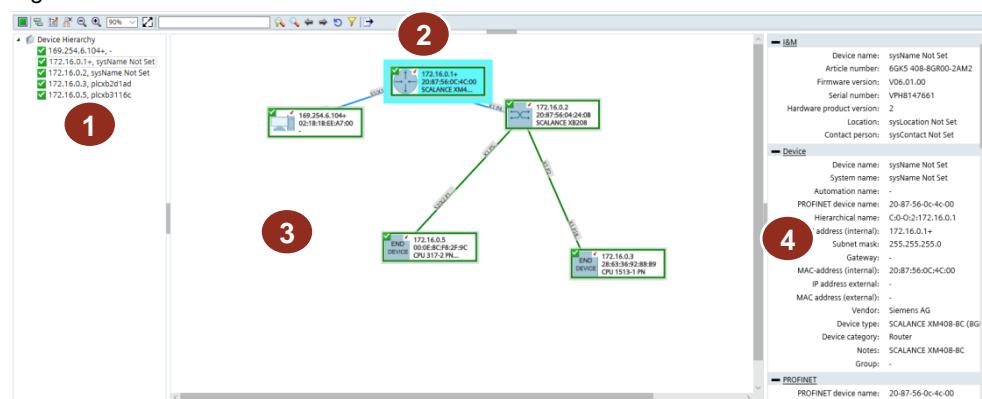
To monitor the devices, you can define SET states for connections, connections and protocol availabilities in the Topology display. The deviations between ACTUAL and SET states are then highlighted graphically.

7.1.2 Work Areas and Operation

Work areas

The following Figure illustrates the division of the work areas.

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



You can find more information on the toolbar with operating elements in the manual under the Entry ID: [109777115](#)

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
- Defining reference states for protocol-specific device availabilities
- Adding new devices in the Editor
- Add unmanaged devices and network clouds

Note

To display learned connections, the check box “Automatically learn connections from alternating devices” in the parameter group “PROFINET monitoring settings” on the Control must also be activated.

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 determined 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.

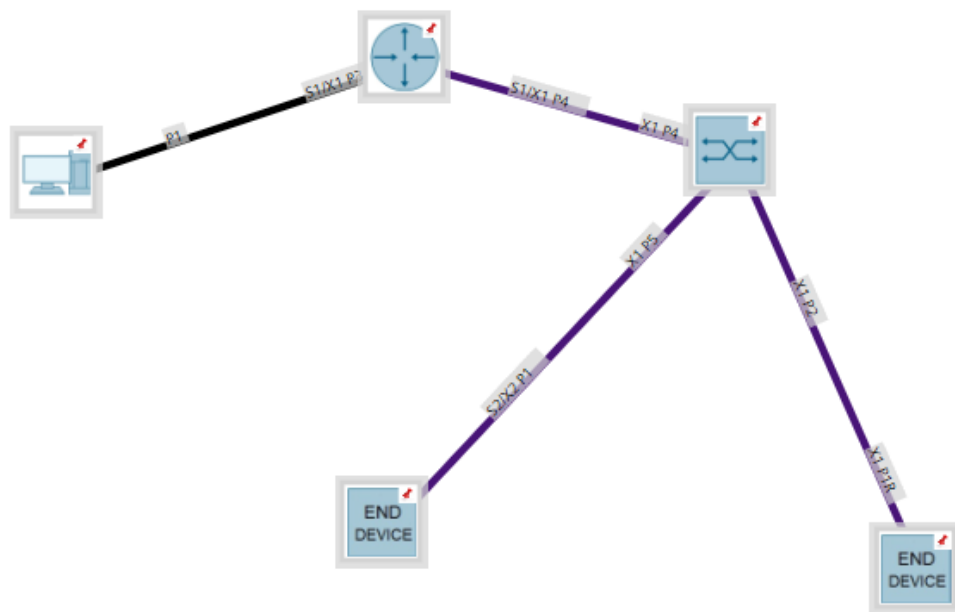
7.1.6 Representation in Topology

The devices, connections and ports that SINEC NMS has detected and assigned with the protocols are automatically displayed topologically.

Devices

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

Figure 7-4



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.

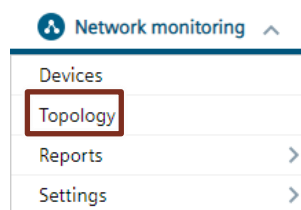
Requirement

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

Open Topology

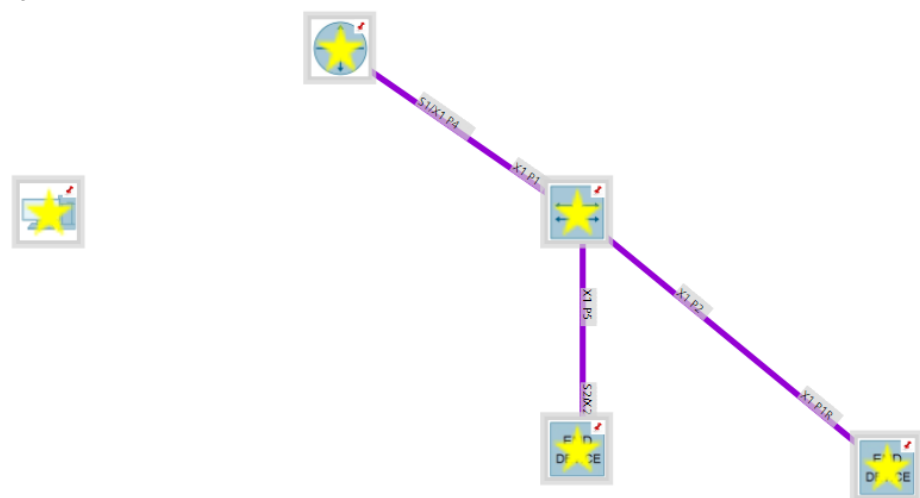
1. Click Network Monitoring > Topology to open the Topology.

Figure 7-5



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 7-6



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 represent all or incorrect devices or connections, the following causes may be present:

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. 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. 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. 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. 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 Topology

You can move devices in the Topology view.

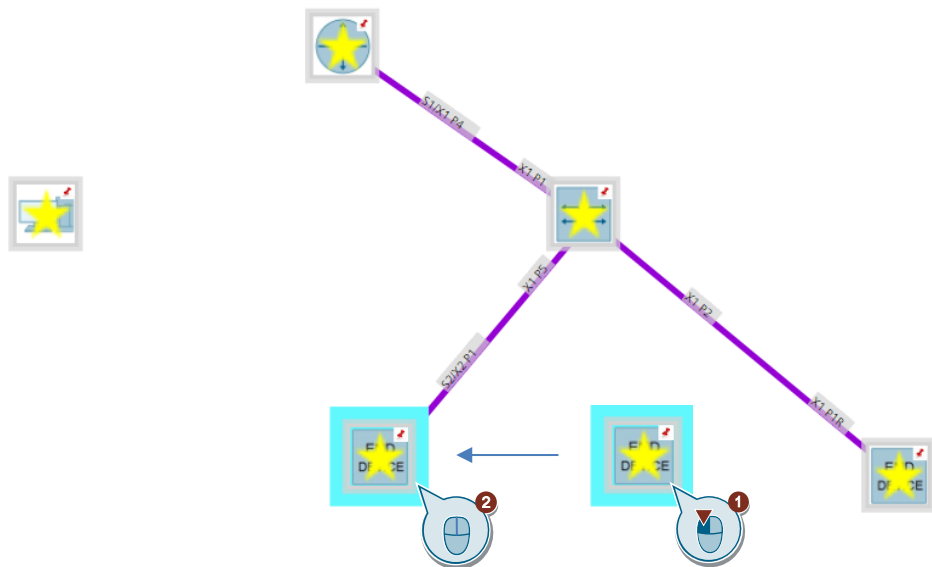
1. To do this, choose the selection tool from the toolbar.

Figure 7-7



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

Figure 7-8



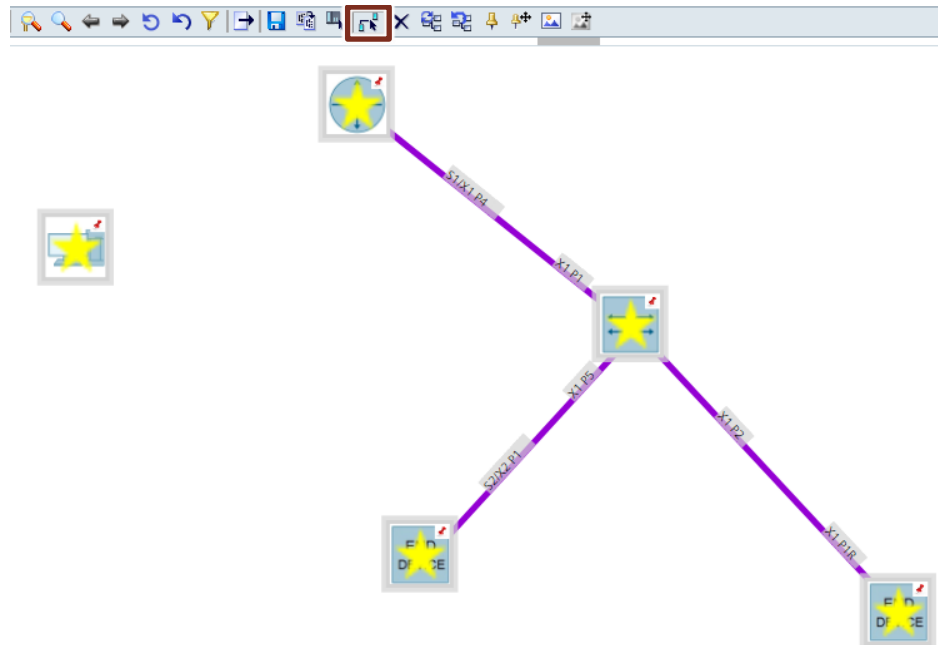
Correcting and adjusting connections

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

Follow these steps:

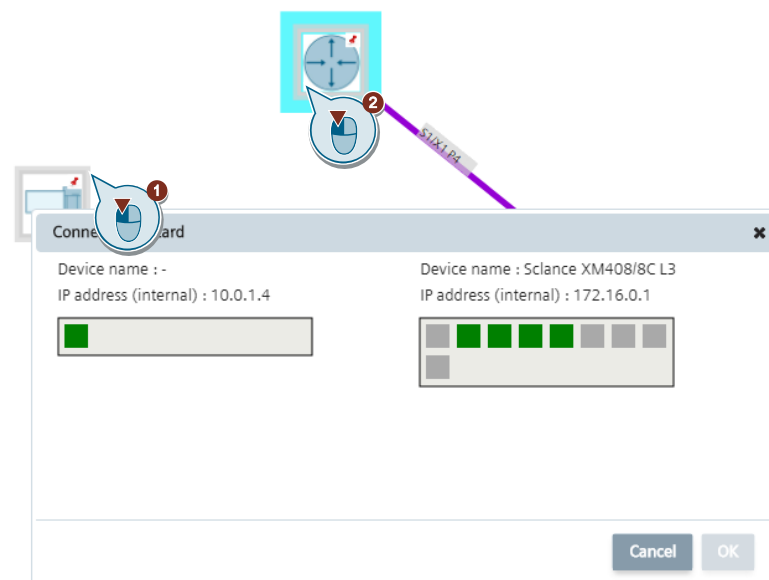
1. Use the selected tool in the toolbar to activate the Draw tool.

Figure 7-9



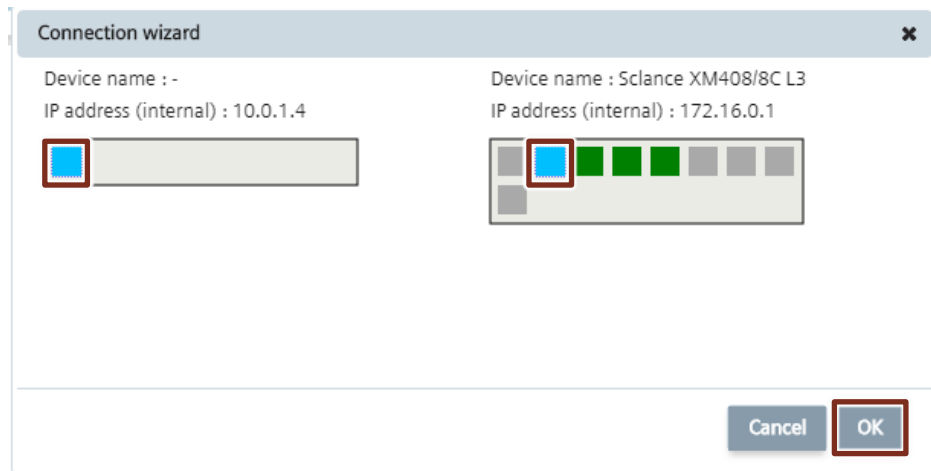
2. To draw Reference Connections manually, click the devices to be connected one after the other. The Connection Wizard opens.

Figure 7-10



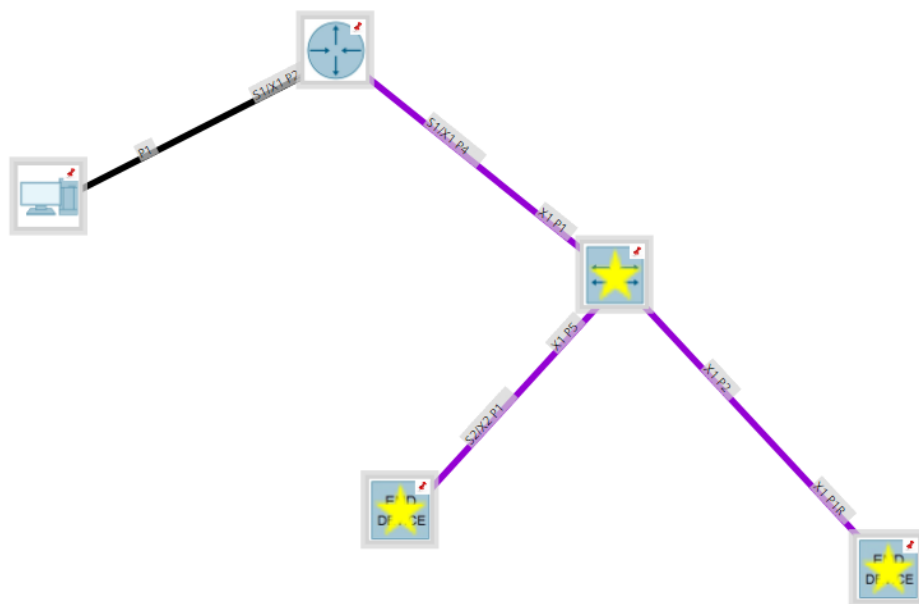
- Click one after the other on the ports of the devices to be connected. Confirm your selection with "OK".

Figure 7-11



- The Reference Connection (black color) between IPC and Scalance XM408 was added.

Figure 7-12



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:

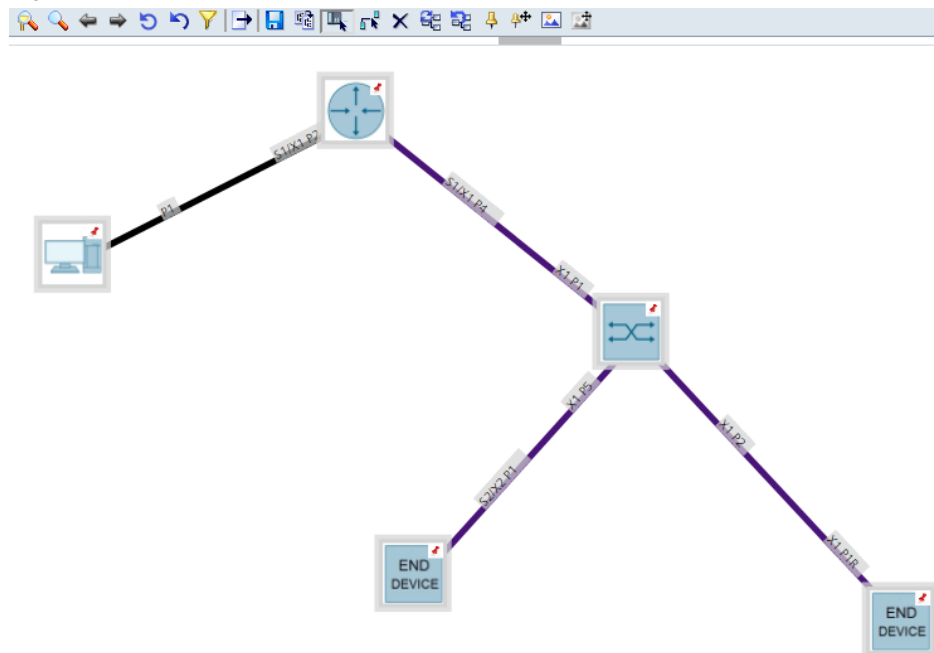
1. Click the selected tool in the toolbar. With the function “Use determined states as reference states” you can define the Topology determined by SINEC NMS as a whole as a reference.

Figure 7-13



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

Figure 7-14



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

Figure 7-15



Result

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

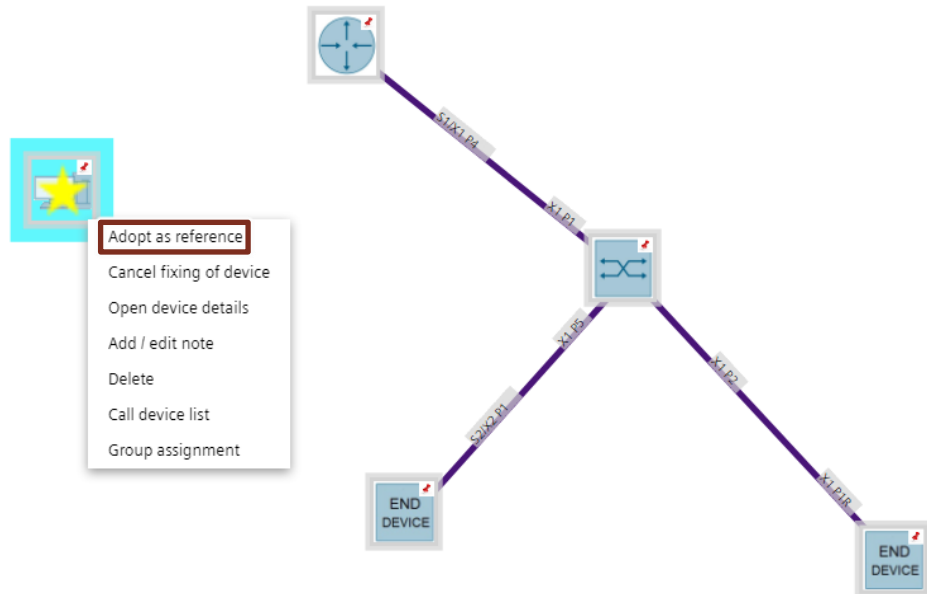
Accepting individual devices and connections as references

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.

Follow these steps:

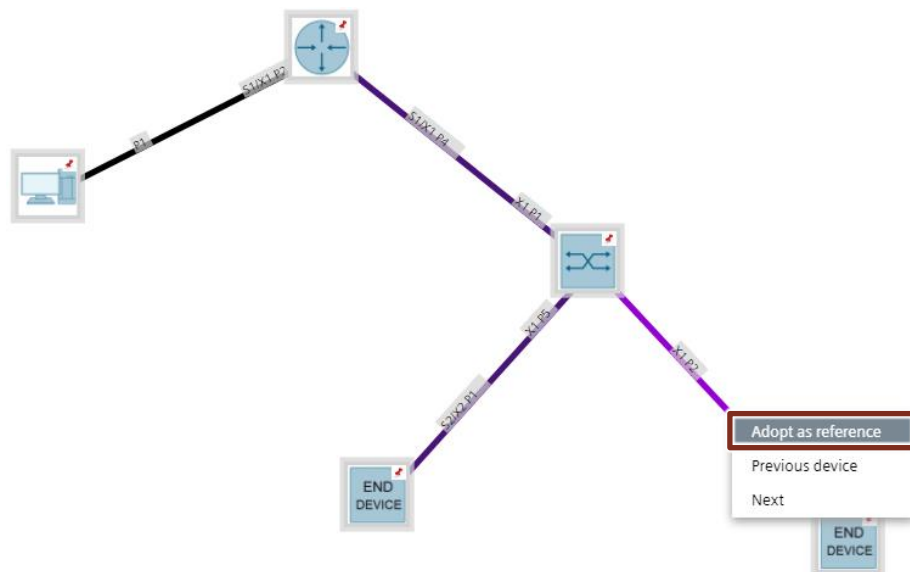
1. For devices:
Click with the right mouse button on the device and select the corresponding entry in the context menu.

Figure 7-16



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 7-17

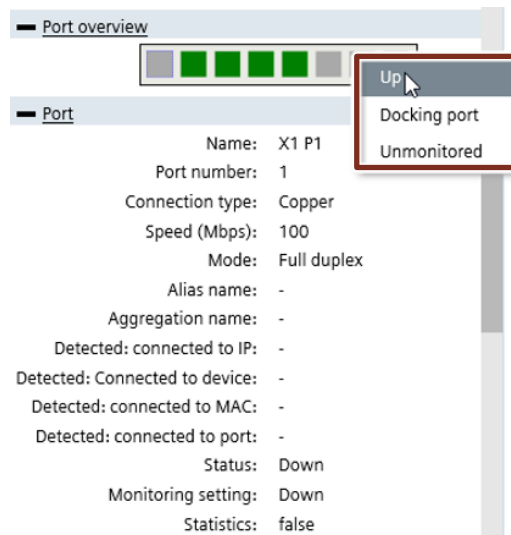


Correcting and adjusting ports

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 7-18



Extended icon view and Topology settings

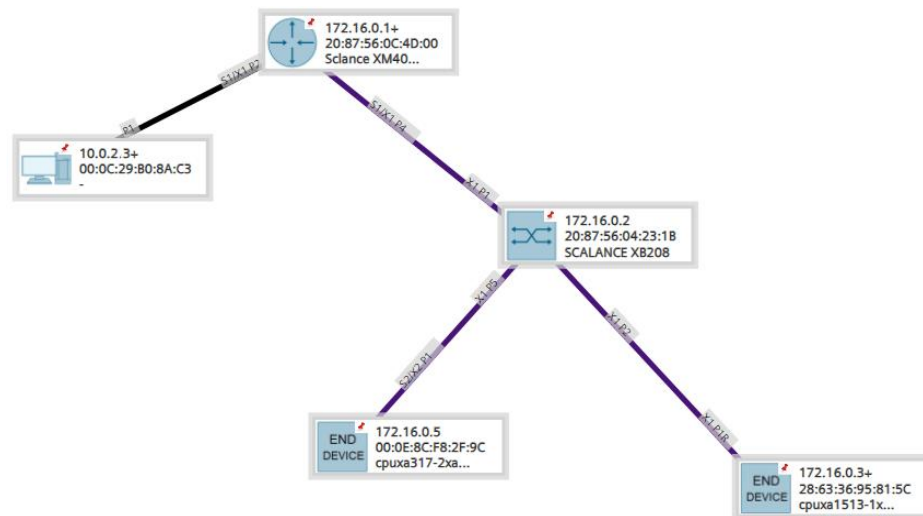
1. To select the extended Icon view, click the selected tool.

Figure 7-19



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 7-20



To define the Topology settings, you must be in Edit mode. Follow these steps:

1. Click the selected tool in the toolbar.

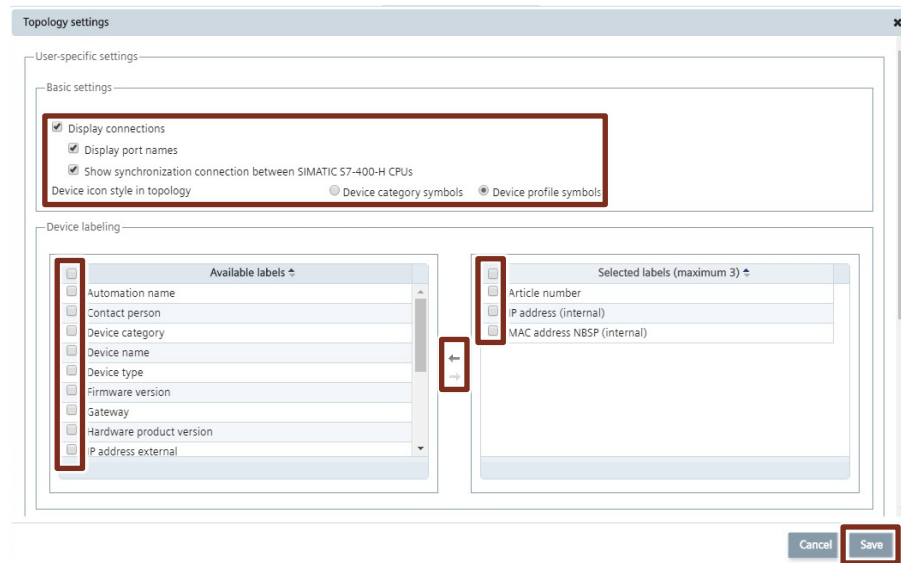
Figure 7-21



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.

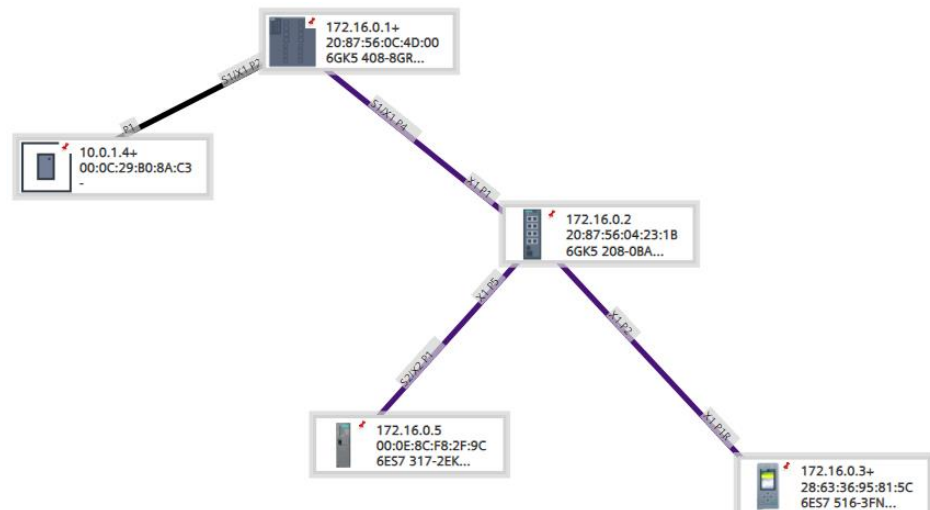
Select the device properties to be displayed in the Topology from the left column. Use the arrows to move the selection to the right column. You can select up to three device properties. Close the dialog with the "Save" button.

Figure 7-22



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

Figure 7-23



Activate or deactivate Edit mode and Online mode

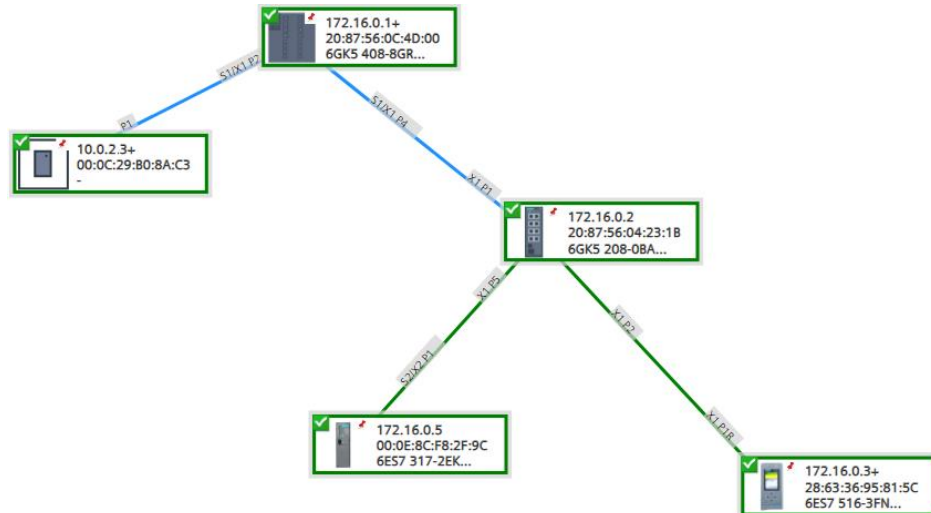
To switch to Online mode, proceed as follows:

1. To switch to online mode, click the selected tool
Figure 7-24



2. The Topology appears in online mode.

Figure 7-25



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

Figure 7-26



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:

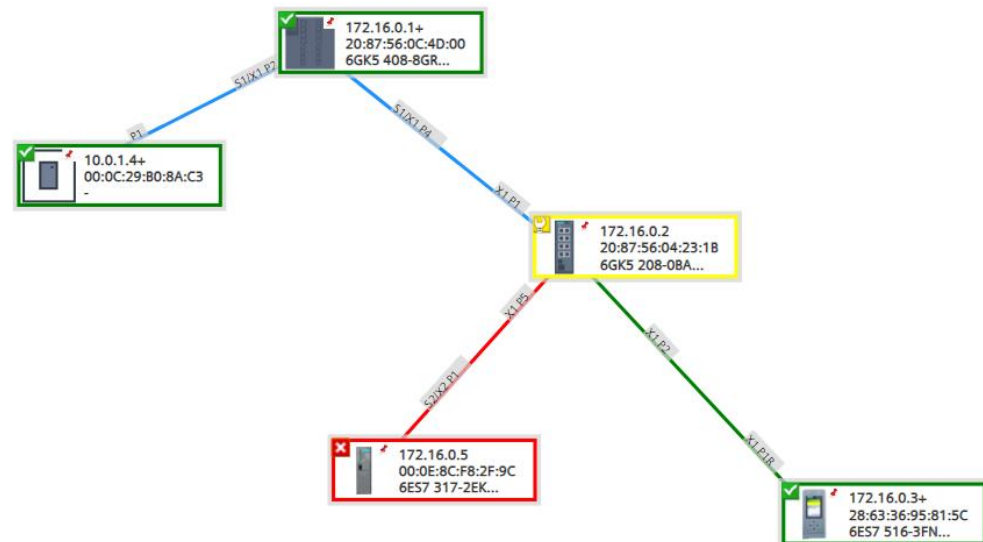
- Port states resulting from the determined Topology and the Reference Topology.
- Port connections resulting from the determined Topology and the Reference Topology. The resulting states of the ports involved are also included in the representation of the port connections.

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 7-27



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 e-mail.

9 Appendix

9.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

<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:

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

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:

www.siemens.com/sitrain

Network Management SINEC NMS with SCALANCE

<https://www.sitrain-learning.siemens.com/DE/en/rw70417/Netzwerkmanagement-SINEC-NMS-mit-SCALANCE>

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support app

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

<https://support.industry.siemens.com/cs/ww/en/sc/2067>

9.2 Links and literature

Table 9-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109762792
\3\	SINEC NMS manual https://support.industry.siemens.com/cs/ww/en/view/109762749
\4\	SINEC NMS V1.0 SP1 Software (incl. 21-day trial license) download https://support.industry.siemens.com/cs/ww/en/view/109776939

9.3 Change documentation

Table 9-2

Version	Date	Modifications
V1.0	03/2019	First edition
V1.1	03/2020	Adjustments to the new version of SINEC NMS V1.0 SP1