SIEMENS

SIMATIC NET

Network management SINEC NMS

Operating Instructions

02/2020

C79000-G8976-C489-02

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C489-02
Ⓟ 01/2020 Subject to change

Table of contents

Preface 1

Network management with SINEC NMS

In the context of digitalization and the Internet of Things, the number of components in industrial networks that communicate and therefore need to be networked is constantly increasing. Guaranteeing the security and availability of the data not only requires professional network planning and implementation, but trained personnel as well. Central network management is essential in order to reliably maintain an overview of all components and the overall status of the network around the clock.

SINEC NMS, the comprehensive network management system, monitors and manages the entire network infrastructure – everything around the clock at a glance.

Cross-industry added value:

- Monitoring and management of different device categories
- Manufacturer-independent visualization of all network nodes and comprehensive support of Siemens devices
- Highly convenient overview of the network for quick and easy determination of the overall status, without in-depth IT know-how
- Rule-based network configuration for industrial communication
- Intelligent firmware rollout based on topology expertise
- Hierarchical user/role concept for local and functional access control (role-based access control)
- Northbound interface for direct access to pre-processed network information for further processing in other systems / applications
- Distributed approach: Complete view of the network, independent of size and complexity; the network management system grows flexibly and scalably with the growing plants
- Manufacturer-independent diagnostics of NAT routers and their lower-level networks

Industry-specific added value:

- Manufacturer-independent PROFINET diagnostics
- SIMATIC Diagnostics (S7-300 and -400)
- Diagnostics of PROFINET-based PCS 7 applications
- Automatic detection and monitoring of changing PROFINET topologies (e.g. tool changer)

Purpose of this documentation

This manual supports you when installing, configuring and operating SINEC NMS. It contains information on monitoring and administration of industrial networks with SINEC NMS.

Scope of validity

The information in this document applies to SINEC NMS V1.0 SP1.

1.1 New in this product version

This product version includes the following new features and enhancements:

New functions

- Generation of firewall and NAT rules for SCALANCE S615, SCALANCE SC-600 and RUGGEDCOM ROX2 devices based on communication relations
- Configurable trust relationships with devices based on SSH/HTTPS fingerprints
- Audit trail for logging user and system activities
- Syslog client functionality for forwarding events to Syslog server
- Integrity checking of system files

Expansion of existing functions:

- Extended configuration limits for operations and devices
- Support for RUGGEDCOM ROS and ROX2 devices
- Receiving SNMPv3 informs
- Support of NAT routers between control and operations (control in external network)
- New URL calls for accessing monitoring data
- Configurable favorites for frequently used actions
- Export and import of device profiles
- Configuration of restriction lists for the network scan
- Configuration of role-based session timeouts
- New policy tasks
- Revised behavior for enabling and disabling network adapters
- Revised behavior when changing hostnames / IP addresses of control and operations
- Revised report configuration
- Revised login page
- Revised GUI design

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SINEMA, SCALANCE, SIMATIC, SINEC

License conditions

Note

Open source software

The product contains open source software. Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following document on the supplied data medium:

OSS_SINEC-NMS_99.pdf

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You can find the SIMATIC NET glossary on the Internet on our Industry Online Support pages at the following address:

Entry ID 50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

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
Link: (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 customers’ exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link: (https://www.siemens.com/industrialsecurity)

1.2 Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that this product meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software you are using up to date. Check regularly for security updates for the product.

  You can find information on this at https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)
- Only activate protocols you require for monitoring and administration of the devices.
- Whenever possible, always use the variants of protocols that provide greater security (e.g. SNMPv3).
- Connections over unsecured network areas must be secured by security mechanisms such as SSL VPN.
- Always click on the "Log off" button in the Web interface when you have finished working with SINEC NMS.
- Restrict access to the SINEC NMS to qualified personnel.
- Use the user and role administration of SINEC NMS to configure the rights of the users according to their authorizations, refer to section Authorization management (Page 272).

Users, roles and passwords

- Define rules for the use of the software and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change the user name and default password for user before you use the software.
- Create users and roles that are tailored to the scope of authorization required by each user. Do not exclusively use the "Super Admin" role that is present by default and disable the "SuperAdmin" user that is present by default after new users with corresponding rights have been created.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized persons.
- Do not use the same password for different users and systems or after it has expired.

Certificates

A secure connection between the control and operations requires authentication of the operations via certificates. Before an operation can be started, a password-protected PKCS12 container must be exported from the control and imported into the operations. Use a secure password to encrypt the PKCS12 container, refer to the "Passwords" section.

Make sure to note the password for the PKCS12 container. It is not displayed in SINEC NMS once it has been set.

For information on how to authenticate operations to the control, refer to section Operations (Page 241).

Basic information on the "Control" and "Operation" components can be found in section Components and function overview (Page 13).

Automation License Manager

If you do not require the network functions of the Automation License Manager, deny access to these functions in your firewall.

1.3 Network load due to SINEC NMS

To monitor devices, SINEC NMS uses part of the data transfer rate available in the network. This must be taken into account when planning networks in which SINEC NMS will be used.

Additional information

You can find the latest information and more on the Internet at the following address:

Link (www.siemens.com/network-management)

Components and function overview 2

2.1 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.

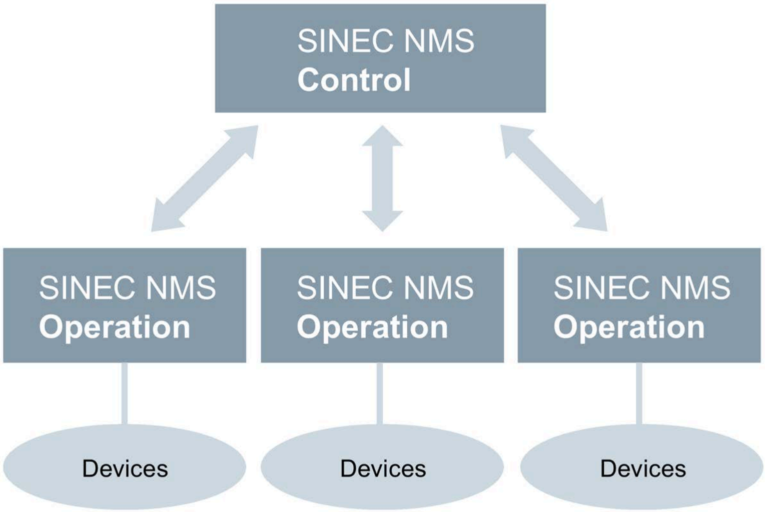


Figure 2-1 Components of SINEC NMS

The control is used for monitoring and administration of the entire network. An operation is responsible for monitoring and administering a subnetwork.

You configure the monitoring settings to be used by the operations centrally at the control and then load them onto the operations. The operations read the monitoring data from the devices and supply 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. Only one operation can be installed on a PC. The control and each operation has its own Web interface for displaying monitoring data and administering the network.

In the rest of this document, the following symbols are used at the beginning of sections to illustrate the scope of a section:

Table 2- 1 Icons for range of validity

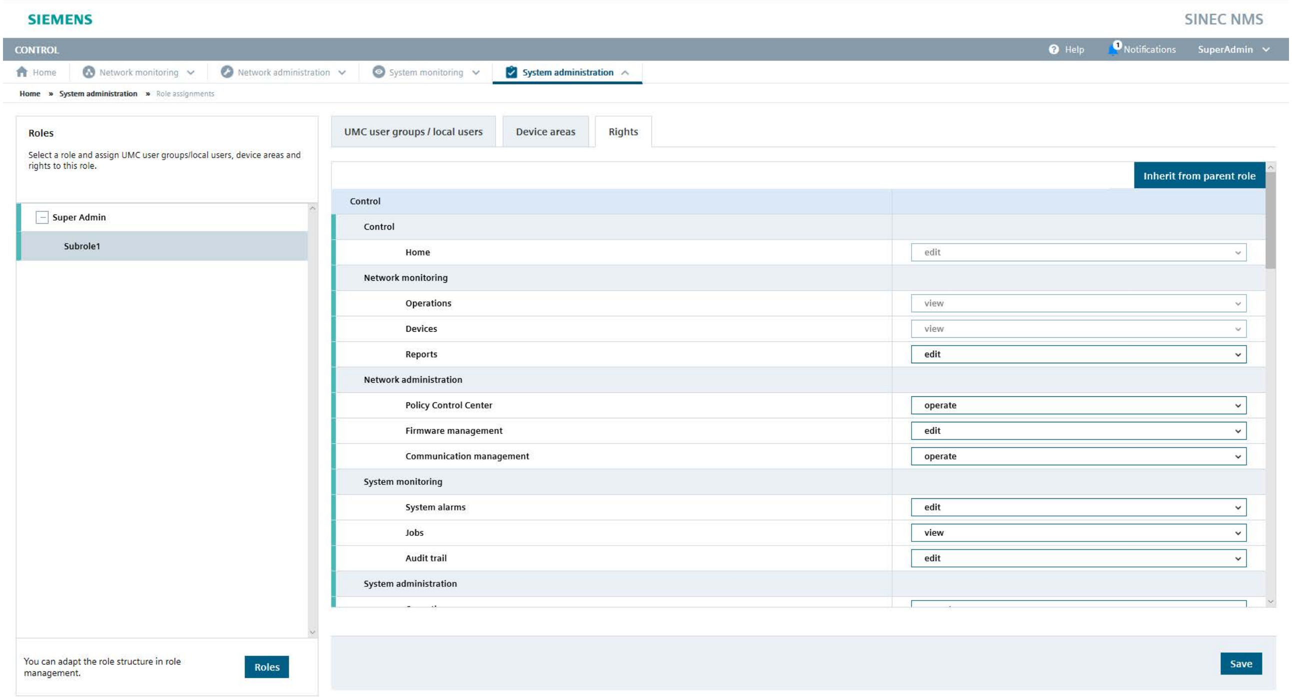
Control	The section is only relevant for the control.
Operation	The section is only relevant for operations.

Sections without any of the symbols listed above are relevant for control and operations.

2.2 Function overview

User and role management

You can define user authorizations for accessing devices and functions in user and role management. You can use definable hierarchies for roles and device areas to adapt the authorization structure of SINEC NMS to the responsibilities planned for the users.



Select a role and assign UMC user groups/local users, device areas and rights to this role.

Control	
Control	
Home	edit
Network monitoring	
Operations	view
Devices	view
Reports	edit
Network administration	
Policy Control Center	operate
Firmware management	edit
Communication management	operate
System monitoring	
System alarms	edit
Jobs	view
Audit trail	edit
System administration	

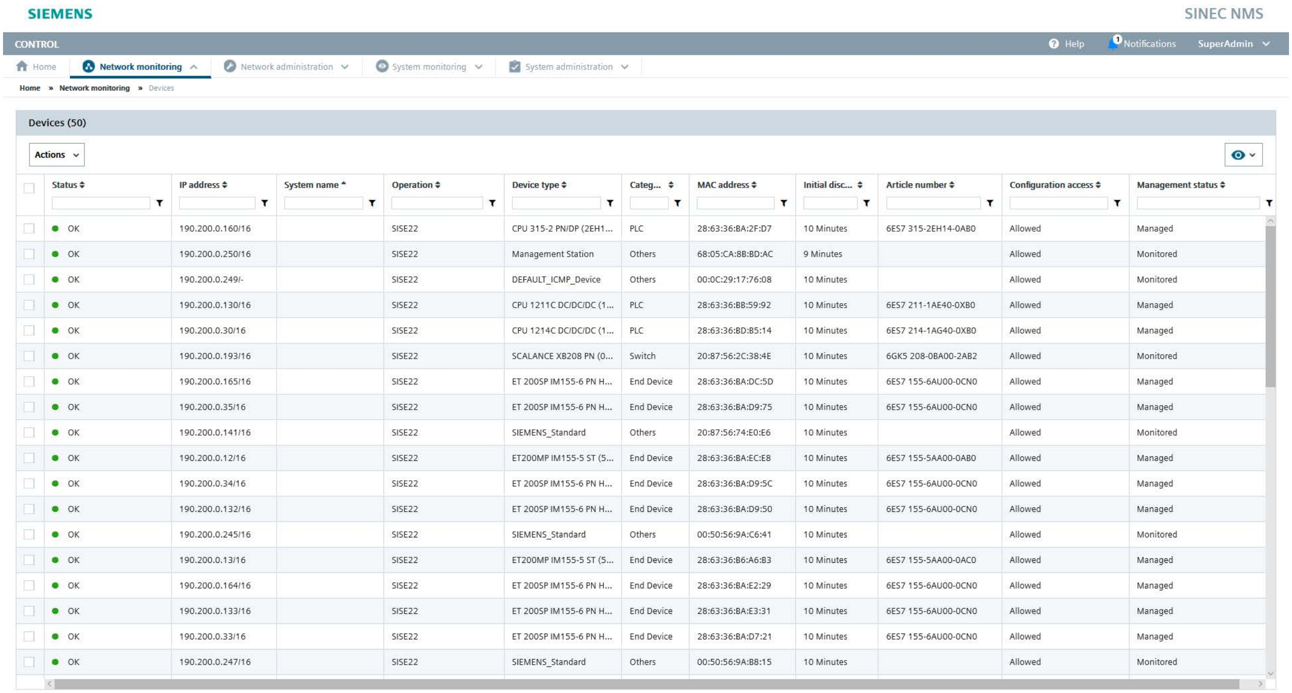
You can adapt the role structure in role management.

Figure 2-2 User and role management

For central storage of user data, SINEC NMS can be connected to UMC (User Management Component). Alternatively, user data can be stored on the control. Single sign-on is supported when using UMC users. This means that when you switch between the Web interfaces for control and operations, you do not need to log on again. UMC is set up during the installation of SINEC NMS, you can find more information in section Installation (Page 27).

Monitoring on control

The control provides an overview of the monitoring data of all operations determined by the devices.

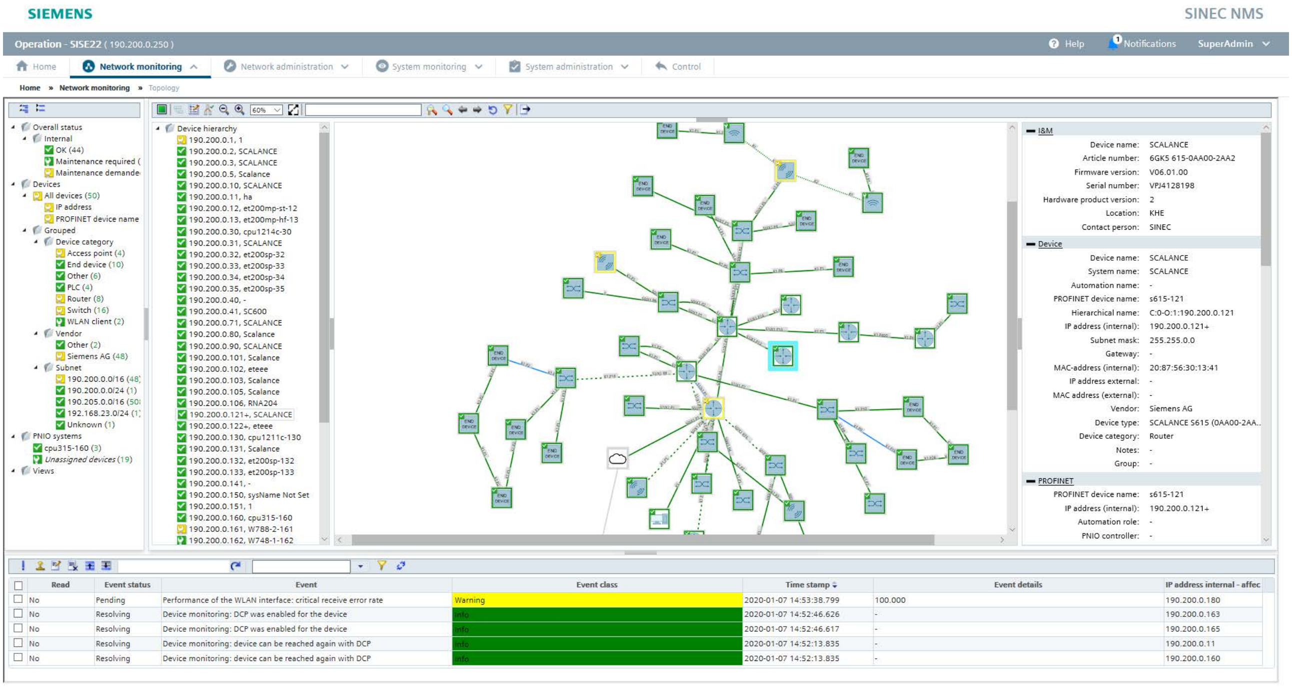


□	Status	IP address	System name	Operation	Device type	Categ...	MAC address	Initial disc...	Article number	Configuration access	Management status
□	● OK	190.200.0.160/16		SISE22	CPU 315-2 PN/DP (2EH1...	PLC	28:63:36:BA:2F:D7	10 Minutes	6ES7 315-2EH14-0AB0	Allowed	Managed
□	● OK	190.200.0.250/16		SISE22	Management Station	Others	68:05:CA:8B:BD:AC	9 Minutes		Allowed	Monitored
□	● OK	190.200.0.249/-		SISE22	DEFAULT_ICMP_Device	Others	00:0C:29:17:76:08	10 Minutes		Allowed	Monitored
□	● OK	190.200.0.130/16		SISE22	CPU 1211C DC/DC/DC (1...	PLC	28:63:36:BB:59:92	10 Minutes	6ES7 211-1AE40-0XB0	Allowed	Managed
□	● OK	190.200.0.30/16		SISE22	CPU 1214C DC/DC/DC (1...	PLC	28:63:36:BD:B5:14	10 Minutes	6ES7 214-1AG40-0XB0	Allowed	Managed
□	● OK	190.200.0.193/16		SISE22	SCALANCE XB208 PN (0...	Switch	20:87:56:2C:38:4E	10 Minutes	6GK5 208-0BA00-2AB2	Allowed	Monitored
□	● OK	190.200.0.165/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:DC:5D	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.35/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:75	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.141/16		SISE22	SIEMENS_Standard	Others	20:87:56:74:E0:E6	10 Minutes		Allowed	Monitored
□	● OK	190.200.0.12/16		SISE22	ET200MP IM155-5 ST (5...	End Device	28:63:36:BA:EC:E8	10 Minutes	6ES7 155-5AA00-0AB0	Allowed	Managed
□	● OK	190.200.0.34/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:5C	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.132/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:50	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.245/16		SISE22	SIEMENS_Standard	Others	00:50:56:9A:C6:41	10 Minutes		Allowed	Monitored
□	● OK	190.200.0.13/16		SISE22	ET200MP IM155-5 ST (5...	End Device	28:63:36:B6:A6:B3	10 Minutes	6ES7 155-5AA00-0AC0	Allowed	Managed
□	● OK	190.200.0.164/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:E2:29	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.133/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:E3:31	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.33/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D7:21	10 Minutes	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.247/16		SISE22	SIEMENS_Standard	Others	00:50:56:9A:B8:15	10 Minutes		Allowed	Monitored

Figure 2-3 Monitoring of devices on control

Monitoring on operations

Each operation displays detailed information about its monitored devices and displays the devices in network topologies, if the devices provide the neighborhood information.



- Overall status
  - Internal
    - OK (44)
    - Maintenance required (
    - Maintenance demande
- Devices
  - All devices (50)
    - IP address
    - PROFINET device name
  - Grouped
    - Device category
      - Access point (4)
      - End device (10)
      - Other (6)
      - PLC (4)
      - Router (8)
      - Switch (16)
      - WLAN client (2)
    - Vendor
      - Other (2)
      - Siemens AG (48)
    - Subnet
      - 190.200.0.0/16 (48)
      - 190.200.0.0/24 (1)
      - 190.205.0.0/16 (50
      - 192.168.23.0/24 (1)
      - Unknown (1)
- PNIO systems
  - cpu315-160 (3)
  - *Unassigned devices* (19)
- Views

- Device hierarchy
  - 190.200.0.1, 1
  - 190.200.0.2, SCALANCE
  - 190.200.0.3, SCALANCE
  - 190.200.0.5, Scalance
  - 190.200.0.10, SCALANCE
  - 190.200.0.11, ha
  - 190.200.0.12, et200mp-st-12
  - 190.200.0.13, et200mp-hf-13
  - 190.200.0.30, cpu1214c-30
  - 190.200.0.31, SCALANCE
  - 190.200.0.32, et200sp-32
  - 190.200.0.33, et200sp-33
  - 190.200.0.34, et200sp-34
  - 190.200.0.35, et200sp-35
  - 190.200.0.40, -
  - 190.200.0.41, SC600
  - 190.200.0.71, SCALANCE
  - 190.200.0.80, Scalance
  - 190.200.0.90, SCALANCE
  - 190.200.0.101, Scalance
  - 190.200.0.102, eteee
  - 190.200.0.103, Scalance
  - 190.200.0.105, Scalance
  - 190.200.0.106, RNA204
  - 190.200.0.121+, SCALANCE
  - 190.200.0.122+, eteee
  - 190.200.0.130, cpu1211c-130
  - 190.200.0.131, Scalance
  - 190.200.0.132, et200sp-132
  - 190.200.0.133, et200sp-133
  - 190.200.0.141, -
  - 190.200.0.150, sysName Not Set
  - 190.200.0.151, 1
  - 190.200.0.160, cpu315-160
  - 190.200.0.161, W788-2-161
  - 190.200.0.162, W748-1-162

I&M

Device name:	SCALANCE
Article number:	6GK5 615-0AA00-2AA2
Firmware version:	V06.01.00
Serial number:	VPJ4128198
Hardware product version:	2
Location:	KHE
Contact person:	SINEC

Device

Device name:	SCALANCE
System name:	SCALANCE
Automation name:	-
PROFINET device name:	s615-121
Hierarchical name:	C:0-O:1:190.200.0.121
IP address (internal):	190.200.0.121+
Subnet mask:	255.255.0.0
Gateway:	-
MAC-address (internal):	20:87:56:30:13:41
IP address external:	-
MAC address (external):	-
Vendor:	Siemens AG
Device type:	SCALANCE S615 (0AA00-2AA...
Device category:	Router
Notes:	-
Group:	-

PROFINET

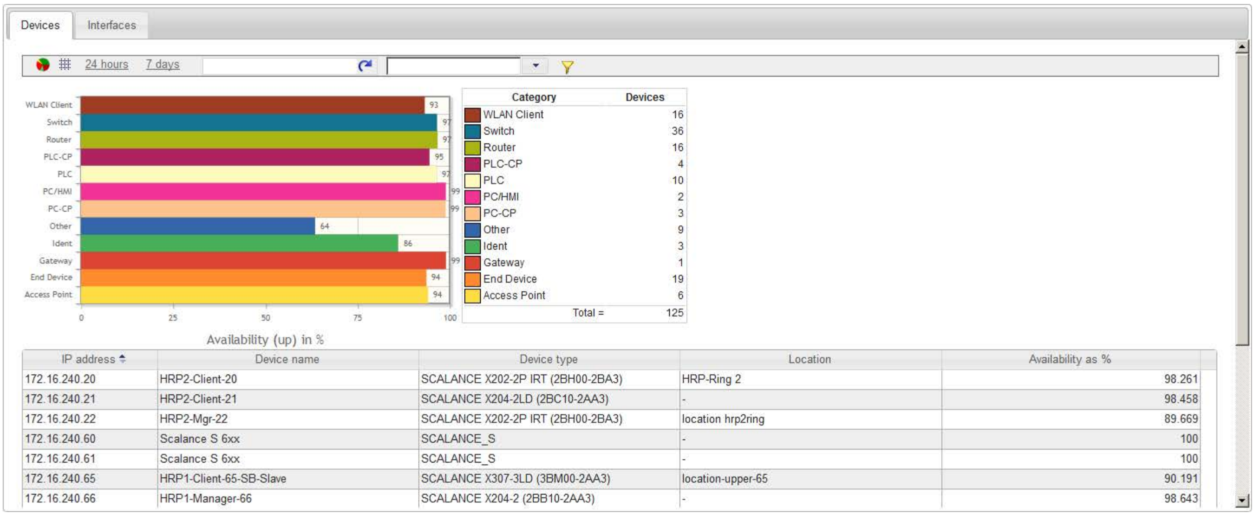
PROFINET device name:	s615-121
IP address (internal):	190.200.0.121+
Automation role:	-
PNIO controller:	-

□	Read	Event status	Event	Event class	Time stamp	Event details	IP address internal - affec
□	No	Pending	Performance of the WLAN interface: critical receive error rate	Warning	2020-01-07 14:53:38.799	100.000	190.200.0.180
□	No	Resolving	Device monitoring: DCP was enabled for the device	Info	2020-01-07 14:52:46.626	-	190.200.0.163
□	No	Resolving	Device monitoring: DCP was enabled for the device	Info	2020-01-07 14:52:46.617	-	190.200.0.165
□	No	Resolving	Device monitoring: device can be reached again with DCP	Info	2020-01-07 14:52:13.835	-	190.200.0.11
□	No	Resolving	Device monitoring: device can be reached again with DCP	Info	2020-01-07 14:52:13.835	-	190.200.0.160

Figure 2-4 Monitoring of network topologies on operation

Reports

Reports offer exportable evaluations of the network monitoring in both text and graphic form.

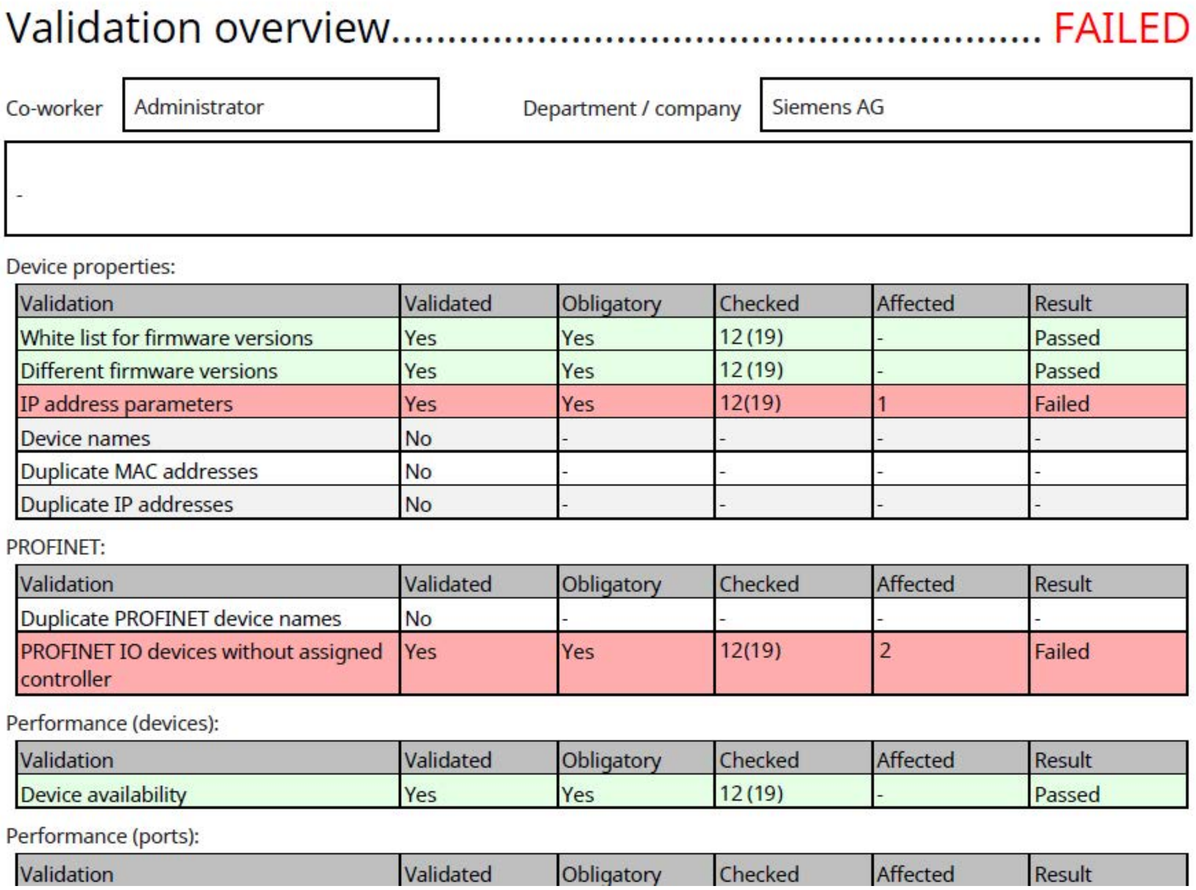


Category	Devices
🟫 WLAN Client	16
🟦 Switch	36
🟨 Router	16
🟥 PLC-CP	4
⬜ PLC	10
🟪 PC/HMI	2
🟧 PC-CP	3
🟦 Other	9
🟩 Ident	3
🟥 Gateway	1
🟧 End Device	19
🟨 Access Point	6
Total =	125

IP address	Device name	Device type	Location	Availability as %
172.16.240.20	HRP2-Client-20	SCALANCE X202-2P IRT (2BH00-2BA3)	HRP-Ring 2	98.261
172.16.240.21	HRP2-Client-21	SCALANCE X204-2LD (2BC10-2AA3)	-	98.458
172.16.240.22	HRP2-Mgr-22	SCALANCE X202-2P IRT (2BH00-2BA3)	location hrp2ring	89.669
172.16.240.60	Scalance S 6xx	SCALANCE_S	-	100
172.16.240.61	Scalance S 6xx	SCALANCE_S	-	100
172.16.240.65	HRP1-Client-65-SB-Slave	SCALANCE X307-3LD (3BM00-2AA3)	location-upper-65	90.191
172.16.240.66	HRP1-Manager-66	SCALANCE X204-2 (2BB10-2AA3)	-	98.643

Figure 2-5 Device availability report

Validation reports are available to check whether certain device properties such as firmware versions or PROFINET device names currently deviate from a specification. The validations to be performed in a validation report can be put together freely and prioritized in terms of the validation result. Validation reports are generated as PDF files and document the validation result as well as the cause of validations that are not passed.



Validation overview.. FAILED

Co-worker: Administrator

Department / company: Siemens AG

-

Device properties:

Validation	Validated	Obligatory	Checked	Affected	Result
White list for firmware versions	Yes	Yes	12 (19)	-	Passed
Different firmware versions	Yes	Yes	12 (19)	-	Passed
IP address parameters	Yes	Yes	12(19)	1	Failed
Device names	No	-	-	-	-
Duplicate MAC addresses	No	-	-	-	-
Duplicate IP addresses	No	-	-	-	-

PROFINET:

Validation	Validated	Obligatory	Checked	Affected	Result
Duplicate PROFINET device names	No	-	-	-	-
PROFINET IO devices without assigned controller	Yes	Yes	12(19)	2	Failed

Performance (devices):

Validation	Validated	Obligatory	Checked	Affected	Result
Device availability	Yes	Yes	12 (19)	-	Passed

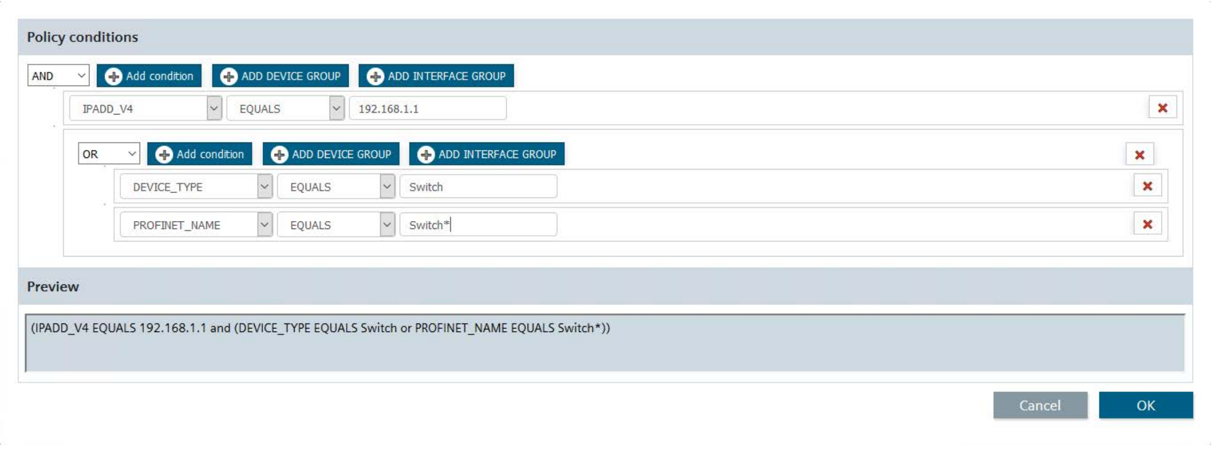
Performance (ports):

Validation	Validated	Obligatory	Checked	Affected	Result

Figure 2-6 Validation report

Policy-based device configuration

You can use a policy to schedule and perform tasks for configuring and managing devices. You can link the enforcement of policies to conditions that SINEC NMS checks against existing device properties and capabilities. Before enforcing a policy, you can use policy simulations to check which devices would be configured by the policy, and in what order, if the policy were enforced at the current time.



Policy conditions

AND

IPADD_V4 EQUALS 192.168.1.1

OR

DEVICE_TYPE EQUALS Switch

PROFINET_NAME EQUALS Switch*

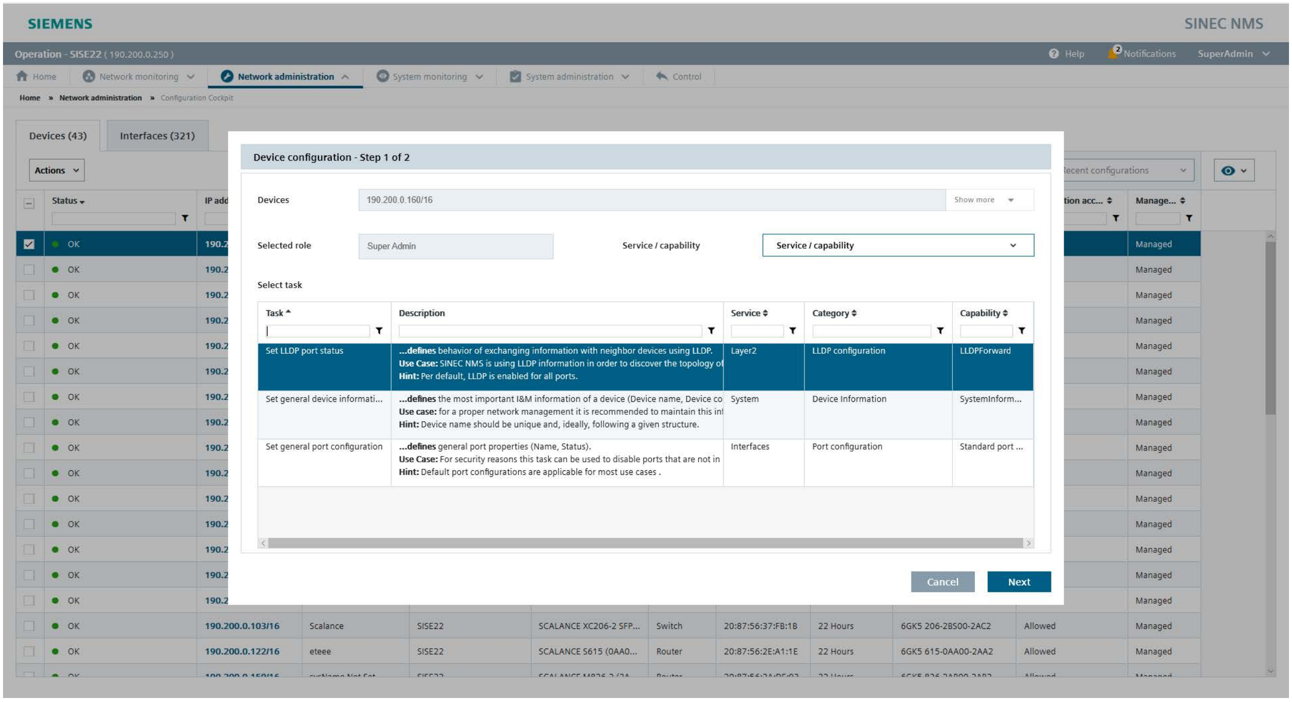
Preview

(IPADD_V4 EQUALS 192.168.1.1 and (DEVICE_TYPE EQUALS Switch or PROFINET_NAME EQUALS Switch*))

Figure 2-7 Configuration of policy conditions

Individual configuration of devices

In the Configuration Cockpit, you can directly select the devices to be configured and execute a configuration task for these devices. If required, conditions and other tasks can be added to this task in the editor for policies.



Device configuration - Step 1 of 2

Devices: 190.200.0.160/16 (Show more)

Selected role: Super Admin

Service / capability: Service / capability

Select task

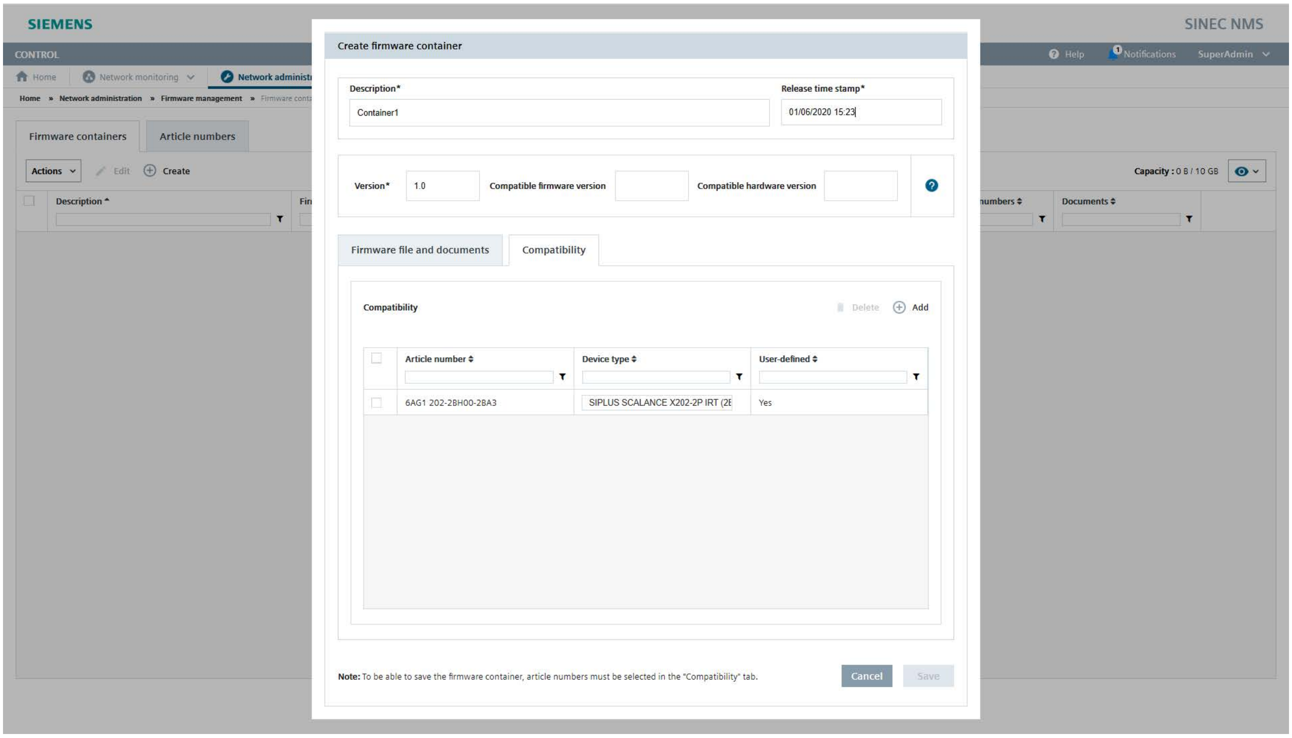
Task	Description	Service	Category	Capability
Set LLDP port status	**...defines** behavior of exchanging information with neighbor devices using LLDP. **Use Case:** SINEC NMS is using LLDP information in order to discover the topology of **Hint:** Per default, LLDP is enabled for all ports.	Layer2	LLDP configuration	LLDPForward
Set general device informati...	**...defines** the most important I&M information of a device (Device name, Device co **Use case:** for a proper network management it is recommended to maintain this int **Hint:** Device name should be unique and, ideally, following a given structure.	System	Device Information	SystemInform...
Set general port configuration	**...defines** general port properties (Name, Status). **Use Case:** For security reasons this task can be used to disable ports that are not in **Hint:** Default port configurations are applicable for most use cases .	Interfaces	Port configuration	Standard port ...

☐	OK	190.200.0.103/16	Scalance	SISE22	SCALANCE XC206-2 SFP...	Switch	20:87:56:37:FB:1B	22 Hours	6GK5 206-2BS00-2AC2	Allowed	Managed
☐	OK	190.200.0.122/16	eteee	SISE22	SCALANCE S615 (0AA0...	Router	20:87:56:2E:A1:1E	22 Hours	6GK5 615-0AA00-2AA2	Allowed	Managed

Figure 2-8 Task selection in the Configuration Cockpit

Firmware management

Firmware files for devices can be managed centrally in the firmware management on the control. Each change in the firmware management is automatically synchronized with the operations. When firmware files are uploaded to SINEC NMS, device compatibility information is automatically read out. Existing firmware files can be uploaded to the corresponding devices via policies or individual configurations.



Description*: Container1

Release time stamp*: 01/06/2020 15:23

Version*: 1.0

Compatible firmware version:

Compatible hardware version:

Compatibility

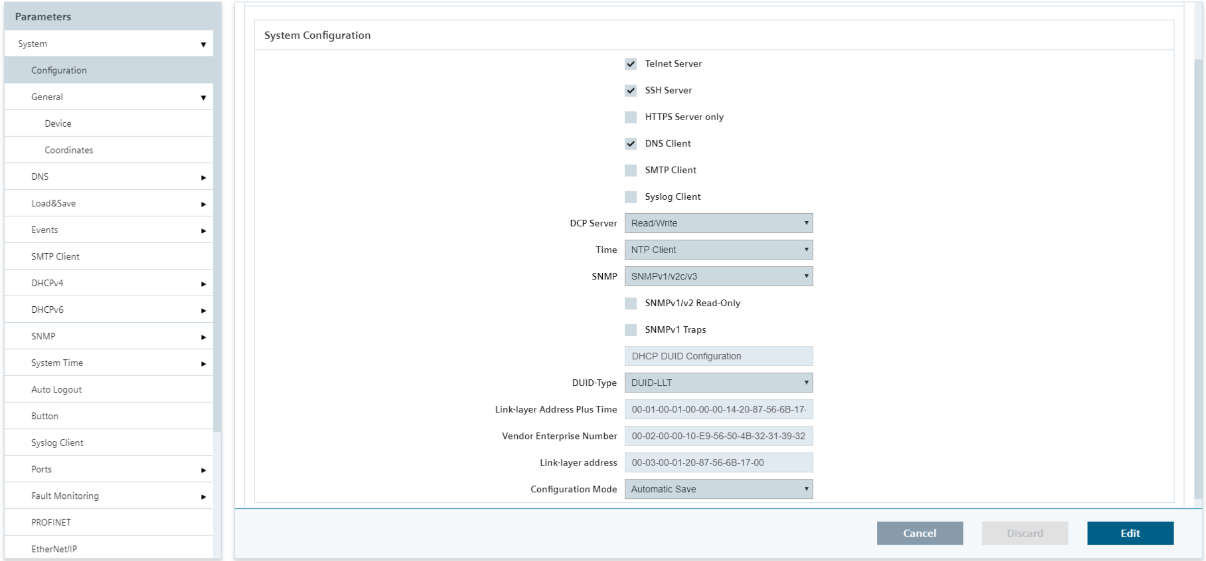
□	Article number	Device type	User-defined
□	6AG1 202-2BH00-2BA3	SIPLUS SCALANCE X202-2P IRT (2E	Yes

Note: To be able to save the firmware container, article numbers must be selected in the "Compatibility" tab.

Figure 2-9 Firmware management

Management of device configurations

Each operation contains a directory for device configurations, which you can save in the directory using policies or individual configurations and load onto the associated devices. To examine differences between device configurations, you can compare device configurations using summaries and edit the device configurations in SINEC NMS if required.



System Configuration

☑ Telnet Server
☑ SSH Server
□ HTTPS Server only
☑ DNS Client
□ SMTP Client
□ Syslog Client

DCP Server: Read/Write
Time: NTP Client
SNMP: SNMPv1/v2c/v3

□ SNMPv1/v2 Read-Only
□ SNMPv1 Traps

DHCP DUID Configuration

DUID-Type: DUID-LLT
Link-layer Address Plus Time: 00-01-00-01-00-00-00-14-20-87-56-6B-17-
Vendor Enterprise Number: 00-02-00-00-10-E9-56-50-4B-32-31-39-32
Link-layer address: 00-03-00-01-20-87-56-6B-17-00
Configuration Mode: Automatic Save

Figure 2-10 Editor for device configurations

Configuration limits

SINEC NMS can be operated with one control and up to 75 operations.

A maximum of 500 devices are supported per operation.

In total, a maximum of 37,500 devices are supported.

Installation and logon 3

3.1 License types

Each operation is licensed by the license of a certain type. The present license type determines how many devices on an operation can have the "Managed" or "Monitored" management status. Only devices with the "Managed" status can be monitored and configured by SINEC NMS. For more information on the management status, refer to section Management status (Page 54).

The following license types are available:

- Trial license: A license of this type is standard and valid for a period of 21 days. This license is automatically activated if no other license type has been found by the Automation License Manager when SINEC NMS starts the first time. The following restrictions apply as compared to the full version:
  - Max. 3 devices in the "Managed" management status, max. 500 devices with the "Monitored" management status.
  - Causes for results of validation reports are not displayed, and it is also not possible to generate pictures of the topology display.
- License type 50: Max. 50 devices with management status "Managed" or "Monitored"
- License type 100: Max. 100 devices with management status "Managed" or "Monitored"
- License type 250: Max. 250 devices with management status "Managed" or "Monitored"
- License type 500: Max. 500 devices with management status "Managed" or "Monitored"
- Power pack: This license type allows you to upgrade a SINEMA Server V13/V14 license to a SINEC NMS license. Depending on the number of devices, the following licenses are available:
  - Power pack 50: A SINEMA Server 50 license is converted into a SINEC NMS 50 license.
  - Power pack 100: A SINEMA Server 100 license is converted into a SINEC NMS 100 license.
  - Power pack 250: A SINEMA Server 250 license is converted into a SINEC NMS 250 license.
  - Power pack 500: A SINEMA Server 500 license is converted into a SINEC NMS 500 license.

Licenses of types 50/100/250 can be combined. A maximum of 500 devices per operation are supported.

On the "Network administration > Configuration Cockpit" page of the respective operation, you can use the "Allow configuration access" and "Block configuration access" actions to determine which devices should have the "Managed" status. Configuration access can only be allowed for devices that have been classified as trusted.

On the "System administration > Operation parameter profiles" page, "Discovery settings" parameter group of the control, you can use the check boxes "Trust newly discovered devices" and "Block configuration access for newly discovered devices" to define whether the newly discovered devices should be trusted and granted the "Managed" management status.

On the "Network Administration > Device credential repository" page of the respective operation, you can subsequently classify discovered devices as trustworthy or untrustworthy.

Automation License Manager

Use the Automation License Manager to manage your SINEC NMS license. Automation License Manager automatically detects your license when it is on your computer or on a removable media connected to your computer. Licenses on optical storage media such as CDs or DVDs are not recognized. For the productive operation of SINEC NMS, the license must be stored locally on your computer.

For more information on the Automation License Manager, refer to the corresponding documentation. You can open this in the Automation License Manager with the menu command "Help > Help on the Automation License Manager".

3.2 System requirements

Hardware requirements

The following hardware requirements apply to the available installation types:

Table 3- 1 Hardware requirements

Installation type	Number of operations	Number of devices	Work memory		Processor		Hard disk space		Number of network adapters per operation
			Control	Operation	Control	Operation	Control	Operation	
Single Node	1	500	32 GB[1]		4 cores with 3 GHz[3]		100 GB[4]		16
Single Node	1	100	16 GB[1]		4 cores with 2.4 GHz[3]		50 GB[4]		
Multiple Node	25	2500	32 GB[1]	8 GB[1]	4 cores with 2.4 GHz[3]	4 cores with 2.4 GHz[2]	200 GB[4]	50 GB[4]	
Multiple Node	5	2500	32 GB[1]	16 GB[1]	4 cores with 2,4 GHz[3]	4 cores with 3 GHz[3]	200 GB[4]	100 GB[4]	
Multiple Node[5]	75	37500	32 GB[1]	16 GB[1]	4 cores with 2.4 GHz[3]	4 cores with 3 GHz[3]	500 GB[4]	100 GB[4]	
Microbox IPC 427E (Single Node)	1	100	16 GB[1]		4 cores with 2.4 GHz[2]		50 GB[4]		
RUGGEDCOM APE 1808 (Operation only)[6]	1	50	8 GB[1]		4 cores with 1,6 GHz		64 GB		2

[1] The specified work memory refers only to the use of SINEC NMS. If additional programs such as STEP 7 are used, the required work memory increases accordingly.

[2] 4 physical cores, no multithreading necessary

[3] 4 physical cores, with multithreading

[4] The specified disk space also includes the estimated disk space required for archiving data. If additional programs such as STEP 7 are used, the required hard disk space increases accordingly.

[5] Installation of Control and Operations on separate PCs.

[6] No OPC UA activated

For information on the available installation types, refer to section Installation (Page 27).

Software requirements

The following requirements apply to the software to be used:

Table 3- 2 Software requirements

Operating system	• Microsoft Windows 10 (Pro / Enterprise) as of version 1709 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019
Supported operating system languages	• German • English
Web browser	• Google Chrome 78.0 or higher • Firefox 68.3 or higher • Microsoft Edge* • Internet Explorer 11.0* *The web browser is only supported to a limited extent.
Screen resolution	1920 x 1080 pixels
Virtualization	VMware ESXi V6.7; for more information, refer to the following section.

Restrictions and requirements for VMware ESXi

When SINEC NMS is used with VMware, the following restrictions and requirements apply:

- SINEC NMS is approved for VMware ESXi V6.7.
- PC must be certified for VMware ESXi V6.7.
- Distributed Switch: Not permitted
- Hard disk: Without Thin Provision
- Vmotion and Storage motion: Not supported
- Fault tolerance: Not supported
- DRS and SDRS: Not supported
- Distributed power management: Not supported
- High availability: Not supported
- VMwaretools: Must be installed, automatic update must be deactivated.
- Unused hardware should be disabled.
- Snapshots should not be created when operating SINEC NMS.

3.3 Installation

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

Proceed as follows to install the Control, Operation, or UMC:

1. Run the "Start.exe" file with administrator privileges from the installation medium.
2. Select the language for the installation wizard.
3. Click the "Read product information" button and read the content of the readme file. It contains important information on the compatibility and application of SINEC NMS. Then click the "Next" button.
4. Select which components of SINEC NMS should be installed:
   - Single Node installation: The control and an operation are installed on the same PC. This setup is used for small installations with 50 to 500 managed devices.
   - Multiple Node installation: The control or operation is installed. This distributed installation is used for larger networks where the control and multiple operations are run on individual hosts.
   - UMC: The connection of SINEC NMS to UMC makes it possible to manage user data centrally in UMC and to integrate this user data via UMC user groups in SINEC NMS. Single sign-on is supported when using UMC users. This means that when you switch between the Web interfaces for control and operations, you do not need to log on again. For information on integrating UMC user groups into SINEC NMS, refer to section UMC user groups (Page 275). If UMC has been installed on an older version of SINEC NMS, read the notes in the section Migration (Page 28). Select whether a UMC server is to be installed or an existing UMC server is to be used.

     - Install UMC locally: UMC is installed on the PC.

     - Remote UMC: An existing UMC installation is used.
5. If you want to install UMC locally, define the UMC domain settings for SINEC NMS and enter the data of an administrator user for this domain.
6. If you are working with an existing UMC installation, specify the address and port at which SINEC NMS can reach UMC and click the "Next" button.
7. Select which service you want to use for receiving SNMP traps:
   - Windows trap service: The "Automatic" start mode is set in Windows for the "RATED OPERATING DISTANCE-TRAP" service. As a result, the Windows trap service is started automatically each time an operation PC is started and SNMP trap port 162 is used together with other applications.
   - SINEC NMS trap service: SNMP trap port 162 is used exclusively by operations. Use the operation trap service when you want SINEC NMS to receive SNMPv3 traps or SNMPv3 informs.
8. Follow the instructions of the installation wizard.
9. Restart the PC once the installation is completed.

After rebooting the PC, SINEC NMS is started automatically and you can log on to the Web interface, refer to section Logon (Page 29).

Starting SINEC NMS may take some time. Until SINEC NMS is fully operational and the Web interface is available, a proxy error message may be displayed in the Web browser.

Unattended installation

If you want to install SINEC NMS without user intervention, you can run one of the three batch files in the "Unattended" directory of the installation disk with administrator rights:

- Install_SINECNMS_Complete.bat: Single Node installation
- Install_SINECNMS_Control.bat: The control is installed.
- Install_SINECNMS_Operation.bat: An operation is installed.

3.4 Uninstalling

SINEC NMS must be uninstalled from any computer that is used as a control or operation. The license key used for an operation can still be used after uninstallation. Use the Windows Control Panel to uninstall the Control and Operations. The installation wizard of SINEC NMS must not be used for uninstalling, otherwise third party products may not be fully uninstalled. You can use the SINEC NMS installation wizard to uninstall UMC and WinPcap. To launch this wizard, run the "Start.exe" file on the installation medium.

3.5 Migration

When updating the SINEC NMS installations for Control and Operations to a higher SINEC NMS version, the existing data is transferred for the most part. Note the following points before starting migration:

- Before updating to a higher SINEC NMS version, make sure that all policies, jobs and reports have been fully enforced or executed. Policies that are aborted by an update of SINEC NMS may create inconsistent states on devices and may not be continued even after an update has been performed. Jobs and reports that are aborted by an update of SINEC NMS will not be executed or will not be executed fully.
- When the migration is started, all logged-in users are automatically logged out.

UMC

The UMC version included in the SINEC NMS installation package has been updated to SINEC NMS V1 SP1. If you want to use this UMC version in SINEC NMS V1 SP1, you must reinstall and set up UMC. An existing UMC installation of SINEC NMS V1 is automatically uninstalled by SINEC NMS before installing the new UMC version. Other UMC installations must be uninstalled manually beforehand.

The UMC user groups contained in SINEC NMS are transferred to SINEC NMS V1 SP1 during the migration. UMC data is not transferred during the installation of the new UMC version.

OPC UA access

The certificate of the OPC UA Server has been updated in SINEC NMS V1 SP1. Update the certificate on the OPC UA clients according to the instructions in section Data access with OPC (UA) (Page 153) to access the OPC UA Server after the installation of SINEC NMS V1 SP1.

3.6 Logon

Logging into Control and Operations is done using the following URLs by default:

Table 3- 3 Logging in to SINEC NMS

Control	https://<IP address or host name>
Operation	https://<IP address or host name>:8443
UMC	https://<IP address or host name>:8444/umc

The port for the operation can be changed in the Operation Monitor.

On the Control and Operation PC, the web interface for logging into SINEC NMS can be opened via the corresponding desktop shortcuts. The port for accessing operations can be configured in the Operation Monitor, see section Operation Monitor (Page 37). When the port is changed, it must also be changed in the corresponding desktop shortcut. Before you log in the first time, read the notes in the "Cookies" and "Certificates" sections.

The login to SINEC NMS can be done with a user configured in UMC or with a local user. Login with a UMC user is possible if UMC was configured during the installation of SINEC NMS. The login via UMC is only possible for users from UMC user groups that are available in UMC and have been configured in SINEC NMS on the "System administration > Users" page, "UMC user groups" tab.

For information on configuring UMC user groups in SINEC NMS, refer to section UMC user groups (Page 275).

Cookies

SINEC NMS uses cookies. Ensure that the web browser you are using allows third party cookies.

Certificates

A certificate is generated during installation and signed with the SINEC NMS root CA for the control and for each operation. The created certificates are stored by SINEC NMS in the Windows certificate store of the Control and Operation PC. Web browsers such as Google Chrome, Microsoft Edge or Internet Explorer that access the Windows certificate store automatically trust the certificate presented by Control or Operation because they know its root CA certificate after installing SINEC NMS. If you want to access SINEC NMS with these web browsers from another PC, you must manually store the SINEC NMS Root CA certificate in the Windows certificate store of this PC. The Mozilla Firefox web browser uses its own certificate store, which must be manually notified of the root CA certificate issued by SINEC NMS via the web browser settings.

Initial logon

The first time you log onto a control and to an operation, you need to log on with the following local user:

Table 3- 4 User data for initial logon

User name	SuperAdmin
Password	sinecnms

After the first logon to the control, the password of this user must be changed. Use a secure password and make sure to note it. If the password is lost, it may be necessary to reinstall SINEC NMS. For more information on the safe use of users and passwords, refer to section Security recommendations (Page 10).

Login via UMC is only possible after logging in once with the user specified above. If UMC login fails after this, use the UMC administrator for the first UMC login to the control and operations. In this way, the IP address of the control/operations is included in the white list of the identity provider.

In a multiple-node installation, only the import of the control certificate is possible after the first logon to an operation. After successfully importing the certificate and authenticating the operation at the control, the user data is transferred from the control to the operation. For information on how to authenticate operations to the control, refer to section Operations (Page 241).

For more information on the default user "SuperAdmin", refer to the section Authorization management (Page 272).

Resetting the password for a local user

If a local user has forgotten a password, it can be reset using the "Forgot password?" entry on the login page of the control. The entry is only available if an e-mail server has been configured on the "System administration > Control administration" page of the control. After clicking on the entry, the user is redirected to a page where it is possible to specify the user name whose password the user wants to reset. SINEC NMS then sends an e-mail to the e-mail address from the configured e-mail account which has been set for the user on the "System administration > Users" page, "Local users" tab of the control. The user then follows the instructions in this e-mail to reset his or her password. Alternatively, users with the "Edit" right for user administration can change the password of local users on the "System administration > Users" page, "Local users" tab. This right is included in the standard role "Super Admin".

For UMC users, the password must be reset via UMC.

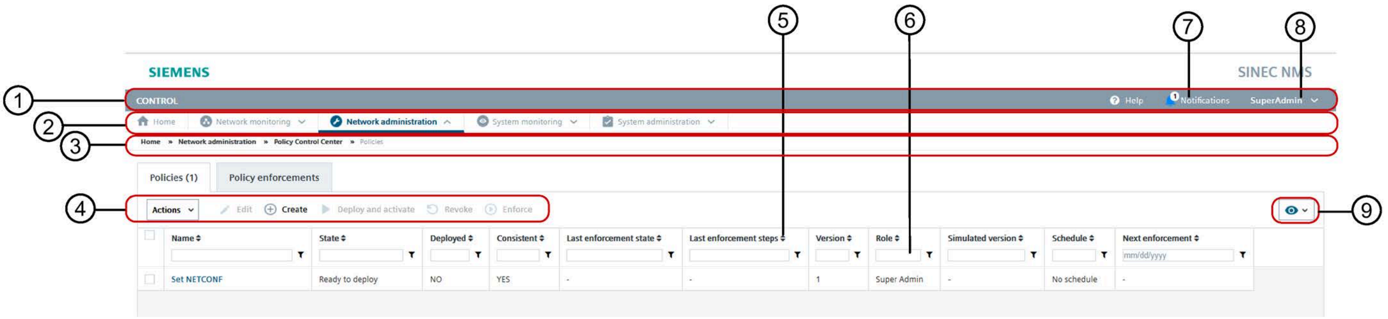
Single sign-on

Single sign-on is supported when using UMC users. This means that when you switch between the control and operations Web interfaces, you do not need to log on again. After logging off from the control or an operation, the user is logged off from all running sessions on the control and operations.

3.7 Layout of the user interface

A user interface is available for the control and each operation. The rights of a user's roles determine which monitoring and administration functions are available for this user in the user interface and which operations and devices are visible when these functions are used.

The following figure shows essential elements of the user interface of the control using the Policy Control Center. The highlighted areas and operator controls are similarly available in the user interface for operations. In the user interface of operations, the "Control" button, which can be used to navigate to the start page of the control, is also available in the navigation bar.



□	Name ≑	State ≑	Deployed ≑	Consistent ≑	Last enforcement state ≑	Last enforcement steps ≑	Version ≑	Role ≑	Simulated version ≑	Schedule ≑	Next enforcement ≑
											mm/dd/yyyy
□	Set NETCONF	Ready to deploy	NO	YES	-	-	1	Super Admin	-	No schedule	-

1 Title specifying the user interface: Control or operation

2 Navigation

3 Breadcrumb navigation

4 Action menu and buttons for quick access, refer to section below.

5 Icons for ascending/descending sorting of column contents

6 Input box for textual filtering of column contents

7 Notification menu with number of unread notifications, refer to section below

8 User menu

9 Folder list for the selection of the columns to be displayed

Figure 3-1 User interface of the control

Action menu and buttons for quick access

The action menu contains all the functions available on a page. You can use the star symbols to define frequently used actions to be displayed next to the action menu for quick access.

Notification menu

The notification menu contains notifications that provide information about completed tasks such as policy enforcement and reporting. The notification menu may also contain warnings or errors that inform about error states.

The notifications are divided into system tasks and private tasks. While system tasks contain system-relevant tasks, private tasks include tasks that the logged-on user has triggered.

The details of a notification become visible after clicking on the "Show more" button. The details of a notification include a button that allows you to navigate directly to the corresponding Web page.

Once you have read the notifications, you can mark them as read. Notifications marked as read are no longer displayed within the notification menu. After clicking on the "Show all notifications" button, all notifications that the logged-on user is allowed to see according to his or her authorizations are displayed. This includes both unread and read notifications.

User menu

The user menu displays the name of the logged on user and contains the following functions:

- Profile

  Opens a window that displays the details of the logged-on user. On the control, you can change the full name and e-mail address of the user that SINEC NMS uses if a user password is forgotten. For local users, you can use the "Change password" button on the control to change the password of the logged-on user.
- Language

  Selecting the language for the user interface
- Log out

  Logs the user off from the control/operation. When UMC is used for authentication, the user is logged off from the control and operation.

Selecting entries in tables

The first column of every table contains check boxes. The check boxes are located in the header row and in each table row.

Follow the steps outlined below to select table entries.

- Select individual entry

  Click a row in the table (excluding links). You can use this to select an individual entry and deselect other selected entries.
- Select multiple entries

  Select the check box for the first and last entry in the desired table area while holding down the Shift key.
- Select multiple entries distributed in any way

  Click in the table rows of the desired entries (excluding links). This selects the desired entries and deselects other selected entries.
- Select all entries of the same page

  Select the check box in the header.
- Deselect individual entries

  Click in the check box of the selected entry.

Specifying table contents and layout

After clicking on the eye symbol on the right above a table, you can select the columns to be displayed in the table. The arrow symbols and text cells in the column headers can be used to sort and filter their contents. The order and width of columns can be defined using drag-and-drop.

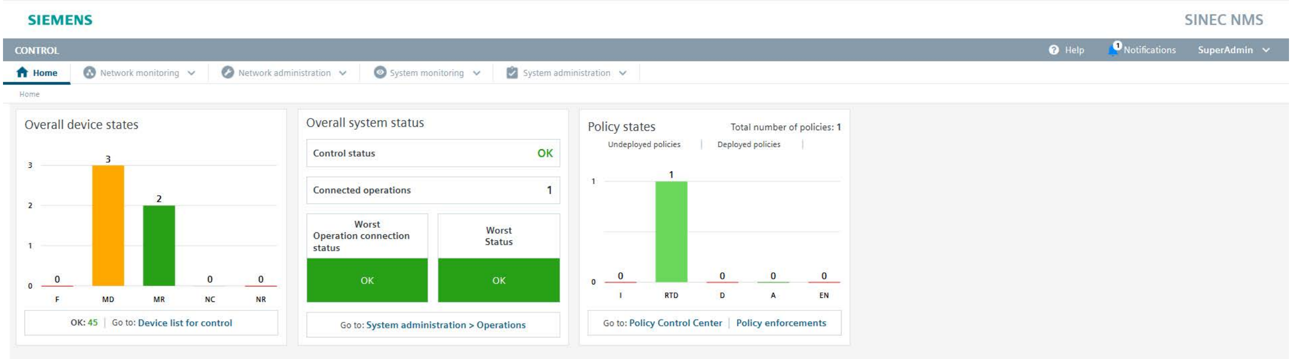
All settings for the contents and layout of tables are saved for each user on the control and all operations and are available again after logging into SINEC NMS again. The default settings for the table contents and the table layout can be restored using the "Reset" button in the dialog for selecting the columns.

3.8 Start page

3.8.1 Start page of the control

Control

You reach this page in the navigation of the control under "Home".



Control status: OK
Connected operations: 1
Worst Operation connection status: OK
Worst Status: OK
OK: 45
Total number of policies: 1

Figure 3-2 Start page of the control

The start page is the dashboard of SINEC NMS. It contains a summary of the overall status of devices as well as status information on control, operations and global policies.

The numbers of total states of monitored devices of all operations are displayed in a bar graph in the "Overall device states" area. The number of devices with the overall status "OK" is indicated below the bar graph. The overall states of the devices are indicated by the following abbreviations and colors.

Table 3- 5 Overall device states

F: Fault	🟥
MD: Maintenance demanded	🟧

MR: Maintenance required	🟩
NC: Not connected	⬜
NR: Not reachable	🟥

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

- Control status: The status of the control. This status takes into account parameters such as CPU utilization and memory management. The symbols displayed in this area have the following meanings:
  - ⚠ Synchronization required:

    Synchronization with at least one operation is required. Synchronize with the affected operations on the "System administration > Operations" page.
  - 🔄 System update required:

    The system version of an operation has not yet been updated to the system version of the control. Install the appropriate system version on the operation.
    For operations that with the "System update required" status, network scans and synchronization of parameter profiles with the control cannot be performed. No exchange of information with the control takes place for these operations, and navigation to these operations is not possible.
  - 🕓 HSP update pending:

    An HSP installed on the control could not yet be transferred to all operations. Check the connection between the control and the operations.
- Connected operations: Number of operations associated with the control.

- Worst operation connection status: Specifies whether all operations can be reached by the control. If at least one operation cannot be reached by the control, the "Not reachable" status is displayed.
- Worst operation status: This status indicates whether there are fault states on an operation. System alarm messages with the status "Pending" are used to determine operation states. For information on system alarm messages, refer to section System alarm messages (Page 237).
  The possible overall states are listed below according to their priority for the display:
  - Unknown:

    The operation cannot be reached.
  - Error

    There is a fault on an operation. Check pending system alarm messages under "System monitoring > System alarm messages" of the control.
  - Warning

    There is a warning for an operation. Check pending system alarm messages under "System monitoring > System alarm messages" of the control.
  - OK

    There are no faults or warnings.

The "Policy states" area displays the number of states of all global policies in a bar graph. This section is divided into the sub-sections "Undeployed policies" and "Deployed policies". Next to the "Deployed policies" area, the ⚠ icon is displayed 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 3- 6 Policy states

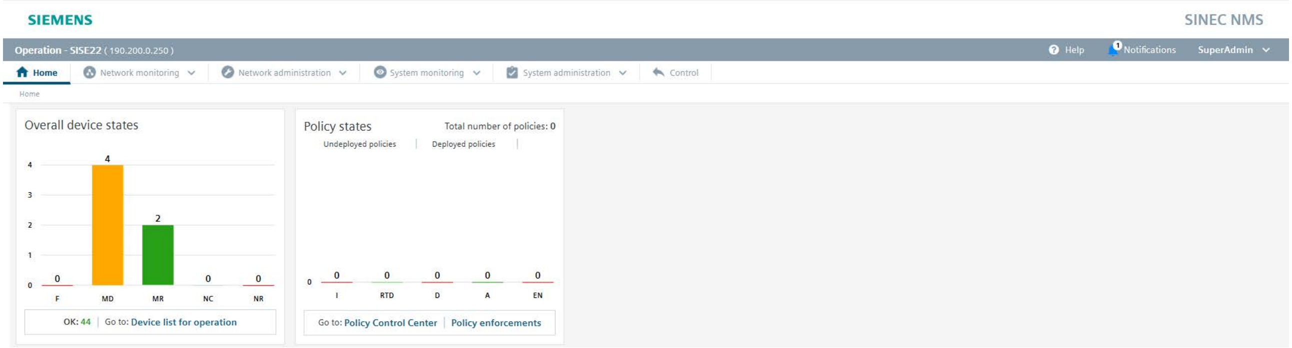
I: Inconsistent	🟥
RTD: Ready to deploy	🟩
D: Deactivated	🟩
A: Activated	🟩
EN: Enforcing	🟩

For more information on policies, refer to section Policy Control Center (Page 177).

3.8.2 Start page of operations

Operation

You reach this page in the navigation of operations under "Home".



OK: 44

Total number of policies: 0

Figure 3-3 Start page of an operation

The start page is the dashboard of SINEC NMS. It contains a summary of the overall states of devices as well as status information about local and global policies loaded on this operation.

In the "Overall·device·states" area, the numbers of the total states of monitored devices of this operation are displayed in a bar graph. The number of devices with the overall status "OK" is indicated below the bar graph. The overall states of the devices are indicated by the following abbreviations and colors.

F:Fault	🟥
MD:Maintenance demanded	🟧
MR:Maintenance required	🟩
NC:Not connected	⬜
NR:Not reachable	🟥

The "Policy states" area displays the number of states of all policies on this operation in a bar graph. This section is divided into the sub-sections "Undeployed policies" and "Deployed policies". Next to the "Deployed policies" area, the ⚠ icon is displayed if one or more policies on the operation of SINEC NMS have been suspended due to inconsistencies. The states of policies are indicated by the following abbreviations and colors.

I:Inconsistent	🟥
RTD:Ready to deploy	🟩

D:Deactivated	🟩
A:Activated	🟩
EN:Enforcing	🟩

For more information on policies, refer to section Policy Control Center (Page 177).

3.9 Operation Monitor

Operation

The Operation Monitor is an administrative component that can be used to configure settings specifically for an operation. Operation Monitor runs on any PC on which an operation is installed and is automatically started after the operation is installed and every time the PC is started.

Calling the Operation Monitor

Operation Monitor is displayed as an icon in the taskbar and can be accessed via the "Settings" entry of the shortcut menu. If the icon is not displayed in the taskbar, the Operation Monitor can be called via "Start > Siemens Automation > SINEC NMS Operation Monitoring". The color of the symbol depends on the state of the operation. The following symbol is displayed for the "OK" state:

SINEC NMS

You can find the symbols for all possible states in the section Status (Page 38).

Calling a Web client

The Web interface of the operation can be called via the "Start Web client" button. The HTTPS port configured in the "Port settings" tab is used for this, refer to section Port settings (Page 39).

Requirement for operating the Operation Monitor

Settings in Operation Monitor can only be edited with administrator rights under Microsoft Windows. In Operation Monitor, click the "Activate administrator mode" button to make the settings of Operation Monitor editable. If you are logged in as a user with administrator rights, a Windows dialog for user account control appears that you need to confirm. If you are logged in as a user without administrator rights, you need to specify the data of a user that has administrator rights. For the response described, it is assumed that at least the second highest level "Standard" was configured for the user account control in Microsoft Windows.

Effect of changes in Operation Monitor

If you change settings in Operation Monitor, the Web server of the operation is automatically exited and restarted. Open Web sessions with the operation are aborted and users must log on again.

3.9.1 Status

The "Status" tab displays the status of the operation as well as its start and stop progress. In this tab, you can also stop and start the operation manually.

Operation Monitor states

The color of the Operation Monitor icon reflects the status of the operation. If there is a negative status, clicking on the text of the status displays its cause.

Table 3- 7 States of Operation Monitor

Icon	Meaning
SINEC NMS	OK There are no faults or warnings for the operation.
SINEC NMS	Warning There is a warning for the operation. Check pending system alarm messages under "System monitoring > System alarm messages" of the operation.
SINEC NMS	Error There is an error for the operation. Check pending system alarm messages under "System monitoring > System alarm messages" of the operation.
SINEC NMS	Operation has been stopped or is being started.

NOTICE

Avoid shutting down and restarting during operation

Do not shut down the PC and do not restart the PC while the operation is in progress. Stop the operation before shutting down the PC; otherwise, the operation database may be damaged and the operation may need to be re-installed. The operation is stopped completely as soon as the progress bar in the Operation Monitor is completely gray.

Lost monitoring data can be recovered in the "Restore" tab, refer to section Restore (Page 42).

3.9.2 Port settings

In the "Port settings" tab, you can configure the operation for HTTPS and OPC UA connections as well as for using the SNMP Trap port 162. The default port settings can be found in the "Reserved ports" section. The following settings are available:

HTTPS settings:

- HTTPS port: Specify the required HTTPS port manually
- Find free port: Specify the HTTPS port to be used by searching for an available port
- Enabled: Enable/disable the operation for HTTPS connections

Note

HTTPS port

If the HTTPS port is being used by another process, a warning to this effect appears in the "Status" tab. In this case, it is advisable to change the port using the "Find free port" button.

To display a list of the processes that use port 8443, for example, you can enter the following command: netstat -noa | findstr :8443

OPC UA settings:

- OPC UA port: Specify the required OPC UA port manually
- Find free port: Specify the OPC UA port to be used by searching for an available port
- Enabled: Enable/disable the operation for OPC UA connections
- OPC UA server authentication:
  Specify whether authentication with a user is necessary to access the OPC UA server of the operation. You configure this user on the control under "System administration > Operation parameter profiles" in the parameter group "OPC settings". With the configured user, all devices that have been added to the list of devices visible in OPC on the "Network·monitoring > Settings > OPC" page of the operation are visible, regardless of the device assignment to views. The following options are available:
  - With user authentication: Authentication with the configured user is required to access the OPC UA server.
  - Without user authentication: Authentication with the configured user is not required to access the OPC UA server.
- OPC UA security mode:
  Specify which connections are permitted for access to the OPC UA server:
  - None: The OPC USA connections do not need to signed or encrypted.
  - Signed / signed and encrypted connections: Only signed connections or signed and encrypted connections are permitted.
  - Signed and encrypted connections: Only connections that are signed and encrypted are permitted.

SNMP traps:

- Windows trap service: The "Automatic" start mode is set in Windows for the "RATED OPERATING DISTANCE-TRAP" service. As a result, the Windows trap service is started automatically each time an operation PC is started and SNMP trap port 162 is used together with other applications.

- Operation Trap service: SNMP trap port 162 is used exclusively by operations. To use the operation trap service, disable the Windows trap service in Windows. Use the operation trap service when you want SINEC NMS to receive SNMPv3 traps or SNMPv3 informs.

Changes to the SNMP trap settings take effect only after the operation is restarted.

Reserved ports

The operation uses the following ports as default ports for communication. Keep in mind that two different programs cannot communicate at the same time via the same port. If, for example, other SIMATIC applications or devices are connected to one of the ports, this port is not available for the operation.

Table 3- 8 Reserved ports

Default ports	Description	Corresponding transport protocol	Configurable	Note on the response if the port is blocked
22	Secure Shell (SSH)	TCP	Yes (Web user interface)	Policies can sometimes not be enforced.
23	Telnet	TCP	Yes (Web user interface)	Policies can sometimes not be enforced.
25	SMTP	TCP	Yes (Web user interface)	-
69	TFTP	UDP	No	No firmware and certificate download possible
102	SIMATIC S7 communication	TCP	No	-
161	SNMP	UDP	Yes (Web user interface)	It is not possible to read out device information.
162	SNMP traps	UDP	No	The operation does not receive any traps.
443	HTTPS for control	TCP	No	Web interface of the control cannot be reached.
4841	OPC UA server	TCP	Yes (Windows taskbar)	If OPC UA server and OPC UA client are separate PCs, no OPC UA communication is possible if a port is blocked.
4897	Internal communication	TCP	No	The operation does not start.

Default ports	Description	Corresponding transport protocol	Configurable	Note on the response if the port is blocked
4998		TCP	No	The operation does not start.
4999		TCP	No	The operation does not start.
5432, 5433	POSTGRESQL	TCP	No	Saving events/reports is not possible.
5671, 15671	Communication between control and operation (RabbitMQ)	TCP	No	Operation cannot be reached by control.
8443	HTTPS for operation	TCP	Yes (Windows taskbar)	Web interface of the operation cannot be reached.
8444	UMC hosting	TCP	No	Only relevant when using UMC. UMC-based authentication fails.
34964, 49152-65535	PROFINET "Read data record"	UDP	No	No PROFINET monitoring possible
49113	Heartbeat	TCP	No	Reachability check of operations (from control)
49114	Exchange of version information between control and operation	TCP	No	No exchange of version information possible
49117	HTTP port for firmware download to RUGGEDCOM ROX2 devices	TCP	No	Firmware download fails.
49131	SFTP	TCP	No	File synchronization between control and operation fails.
49133	UMC internal communication	TCP	No	Only relevant when using UMC. UMC-based authentication fails.

By default, the setup of the operation enters a series of processes in the list of firewall exceptions. Below you will find the processes that are opened by the operation so that the firewall ports can communicate.

- WCCILpmon.exe - TCP/UDP port
- WCCOAsnmp.exe - TCP/UDP port

NOTICE

Firewall

With some firewall configurations, it may be necessary for the system administrator to adapt some of the settings listed above.

3.9.3 Restore

The "Restore" tab enables you to restore monitoring backups regularly created by the system-defined backup job and force the termination of running processes. Restoring the backup restores the monitoring data on the operation. The backup job can be found on the Web interface of the operation under "Network·monitoring > Settings > System jobs", refer to section System jobs (Page 164).

Restoring monitoring backups

Using the "Restore" button, a created monitoring backup can be selected and restored manually. If the operation cannot be started correctly, the last created monitoring backup is automatically restored. The path under which the operation searches for the monitoring backup can be configured in the job type-specific settings of the backup job, refer to the section System jobs (Page 164). When restoring monitoring backups, no operations such as policy enforcements should be performed on the operation. After restoring monitoring backups, manual synchronization of the operation with the control is required on the "System administration > Operations" page.

Using the "Force stop of creating / restoring backups" function discards monitoring backups being created or stops the restoration of monitoring backups. The operation cannot be started until a monitoring backup has been completely restored.

Note

Increased memory requirements during the restoration of monitoring backups

During the restoration of a monitoring backup, due to the intermediate storage of the data in temporary directories, there is an increase in the memory requirements.

Forcing process aborts

If the operation can no longer be stopped using the "Stop operation" button in the "Status" tab, the operation can be stopped using the "Force stop" button in the "Restore" tab. However, loss of data may occur.

3.10 URL call of monitoring data

Monitoring data can also be called by specifying URLs. The following actions are possible:

- Call for a specific Web page
- CSV/JSON download of the content of a Web page

In the URL, the IP address and the port of the respective operation must be specified. The login data used is also specified in the respective URL and must originate from a local user. The local user must have the "monitoring basic" "Monitoring Access Level" right. The "monitoring standard" and "monitoring advanced" rights do not contain the authorization to call the URL. For UMC users, the URL call of monitoring data is not possible.

URL calls from Web pages by a maximum of 50 users and CSV/JSON downloads by a maximum of 10 users are supported per operation.

Note that the login information specified in the URL is also visible in your browser history. Therefore, make sure that the history is deleted when you close the browser or that it is protected from third parties.

Basic parameters for calling Web pages

The following example URL contains the basic parameters that can be used to call Web pages. They call the page "Network monitoring > Devices" on the selected operation.

https://192.168.0.200:8443/local?username=tester&password=!dt6A&path=network-monitoring/opMonDevices

The parameters have the following meanings:

- local?

  Indicates that it is a local user.
- username

  Name of the user logging on
- password

  Password of the user logging on
- path

  Path of the Web page on the operation to be displayed, see section below.

You can either specify the credentials to use directly in the URL call, as in the example above, or use a separate URL call to create the user session. If you use a separate URL call to create the user session, the credentials no longer need to be specified in subsequent URL calls by the user. Example call for creating a user session:
https://192.168.0.200:8443/local?username=tester&password=!dt6A

"path" parameter

The following parameter values are available:

- network-monitoring/opMonDevices

  Calls the page "Network monitoring > Devices" on the operation.
- network-monitoring/opMonTopology

  Calls the page "Network monitoring > Topology" on the operation.
- network-monitoring/opMonDevices&opmonpath=views_tabs&params= views_View_1&tabname=views_topology&mode=iconview

  Opens the topology of a view in the icon view.
- network-monitoring/opMonDevices&opmonpath=views_tabs&params= views_View_1&tabname=views_topology&mode=iconview_extended

  Opens the topology of a view in the extended icon view.

Basic parameters for the download of the content of a Web page

As an alternative to accessing a web page, you can download its contents in a CSV or JSON file from SINEC NMS. The following example URL contains the basic parameters that can be used to download the content of Web pages. It results in a JSON download of the content of the "Network monitoring > Devices" Web page in German.

https://localhost:8443/local?type=exportTable&command=GetDevices&username=tester &password=!dt6A&download=json

The parameters have the following meanings:

- type=exportTable

  Indicates that this is a download of Web page content.
- command

  Indicates which Web page type should be downloaded. The following are available:

  - Reports
  - Event list
  - Device list
  - Interface list

  The values of this parameter and the filter parameters are described in the sections below.
- username

  Name of the user logging on
- password

  Password of the user logging on

- language

  Display language of the content to be downloaded. Possible values:

  - de
  - en

  Default setting if the parameter is not used: en

- download

  Format for the download. Possible values:

  - csv
  - json

  Default setting if the parameter is not used: csv

Parameters for downloading reports

- command=GetReports

  Indicates the download of reports

- report_type

  Indicates the report type to be downloaded. The values of the individual report types are:

  Availability > Devices: 4

  Availability > Interfaces: 5

  Performance > LAN - Interface utilization: 6

  Performance > LAN - Interface error rate: 7

  Performance > WLAN - Interface error rate: 9

  Performance > WLAN - Interface data rate: 8

  Performance > WLAN - Signal strength: 10

  Performance > WLAN - Number of clients: 11

  Performance > Discarded packets: 33

  Performance > POF power budget: 39

  Inventory > Manufacturer: 1

  Inventory > IP address range: 2

  Inventory > Device category: 3

  Inventory > PROFINET: 38

  Events > Network events: 12

  Events > System events: 13

  The possible filter parameters for event reports are described in the table below.

- report_startDate

  Start date for the report data to be downloaded

  Format: yyyy-mm-dd hh:mm:ss

- report_endDate

  End date for the report data to be downloaded

  Format: yyyy-mm-dd hh:mm:ss

- period

  Period for the data to be downloaded. Possible values:

  - 24 hours: 1
  - 7 days: 2
  - Unlimited: 3

  Default setting if the parameter is not used: 1

  For the download of event reports, parameter values 1 and 2 indicate the unit for the period to be filtered, see below.

The parameters for the start or end date and the period should not be specified at the same time.

Filter parameters for downloading events reports

Associated reports:

- Events > Network events (report_type: 12)
- Events > System events (report_type: 13)

The parameters have the following meanings:

- eventNoted

  Filter according to the status "Read":

  - Yes: 0
  - No: 1
  - All: 2

  Default setting if the parameter is not used: 2

- eventPendingStatus

  Filter according to event states:

  - All: 0
  - Not present: 1
  - Resolving: 2
  - Automatically resolved: 3
  - Resolved manually: 4
  - Pending: 5

  Default setting if the parameter is not used: 0

- classFilter

  Filter according to event classes:

  - Notification: Notification
  - Information: Info
  - Warning: Warning
  - Error: Error

  Default setting if the parameter is not used: All event classes

- protocolFilter

  Filter according to protocols:

  - ICMP
  - DCP
  - ARP
  - SNMP
  - SNMP Trap
  - PROFINET
  - SIMATIC
  - SIMATIC Diag. Events
  - SIMATIC Alarms Filter
  - Computed

  Default setting if the parameter is not used: All protocols

- period

  Unit for the filter period:

  – Hours: 1

  – Days: 2

  – Unlimited: 3

  Default setting if the parameter is not used: 1

- periodValue

  Filter period:

  – Possible range of values for hours: 1...24

  – Possible value range for days: 1...7

  If the value 0 is specified or the "periodValue" parameter is not used, the default value for the specified unit is used.

  – Default value for unit "Hours": 24

  – Default value for unit "Days": 7

Multiple parameter values can be specified separated by commas.

Further filter parameters for downloading reports

Associated reports:

- Availability > Interfaces (report_type: 5)
- Performance > LAN - Interface utilization (report_type: 6)
- Performance > LAN - Interface error rate (report_type: 7)
- Performance > Discarded packets (report_type: 33)

The parameters have the following meanings:

- fromIp

  Filter according to "From IP address"

- toIp

  Filter according to "To IP address"

- deviceName

  Filter according to device names

- deviceType

  Filter according to device types

- reportsCategory

  Filter according to device categories:

  - End Device
  - Router
  - Switch
  - Gateway
  - Access Point
  - WLAN Client
  - PLC
  - PC/HMI
  - PC-CP
  - PLC-CP
  - Ident
  - Motion
  - Power
  - Others
  - All

  Default setting if the parameter is not used: All
- statistics

  Filter according to ports on which port statistics are activated or deactivated:

  - All: All
  - Port statistics enabled: Yes
  - Port statistics disabled: No

  Default setting if the parameter is not used: All
- deviceFilter

  Filter according to devices:

  - All devices: All
  - Existing devices: existing

  Default setting if the parameter is not used: All

  This filter parameter is available for all reports.

Multiple parameter values can be specified separated by commas.

Parameters for downloading event lists

- command=GetEvents

  Indicates the download of event lists.

- eventNoted

  Filter according to the status "Read":

  – Yes: 0

  – No: 1

  – All: 2

  Default setting if the parameter is not used: 2

- eventPendingStatus

  Filter according to event states:

  – All: 0

  – Not present: 1

  – Resolving: 2

  – Automatically resolved: 3

  – Resolved manually: 4

  – Pending: 5

  Default setting if the parameter is not used: 0

- period

  Unit for the filter period:

  – Hours: 1

  – Days: 2

  – Unlimited: 3

  Default setting if the parameter is not used: 1

- periodValue

  Filter period:

  – Possible range of values for hours: 1...24

  – Possible value range for days: 1...7

  If the value 0 is specified or the "periodValue" parameter is not used, the default value for the specified unit is used.

  – Default value for unit "Hours": 24

  – Default value for unit "Days": 7

- startDate

  Start date for event list to be downloaded

  Format: yyyy-mm-dd hh:mm:ss

- endDate

  End date for event list to be downloaded

  Format: yyyy-mm-dd hh:mm:ss
- classFilter

  Filter according to event classes:
  - Notification: Notification
  - Information: Info
  - Warning: Warning
  - Error: Error

  Default setting if the parameter is not used: All event classes
- categoryFilter

  Filter according to event categories:
  - Network: Network
  - System: System

  Default setting if the parameter is not used: All event categories
- protocolFilter

  Filter according to protocols:
  - ICMP
  - DCP
  - ARP
  - SNMP
  - SNMP Trap
  - PROFINET
  - SIMATIC
  - SIMATIC Diag. Events
  - SIMATIC Alarms Filter
  - Computed

  Default setting if the parameter is not used: All protocols

Multiple parameter values can be specified separated by commas. The parameters for the start or end date and the period should not be specified at the same time.

Parameters for downloading device lists

- command=GetDevices

  Indicates the download of device lists.

Parameters for downloading interface lists

- command=opMon_GetInterfaces

  Indicates the download of interface lists.

Network monitoring

4

4.1 Basics

Network scan

Before it is possible to monitor devices in the network, the devices must be discovered by a network scan. When configuring the operations on the page "System administration > Operations" on the control, you can define the scan ranges to be scanned by SINEC NMS. To speed up the network scan, the scan ranges should be limited to the IP addresses of the devices that are to be monitored. If the IP addresses of these devices are not in sequence, you can configure several scan ranges in which the devices to be discovered are located. The network scan can be started manually on the page "System administration > Operations" or by SINEC NMS. The time interval for starting network scans by SINEC NMS can be set on the control under "System administration > Operation parameter profiles" in the parameter group "Discovery settings".

Included devices

Depending on which DCP discovery type has been configured in the parameter group "Discovery settings", either all devices discoverable via DCP or only the devices that can be found in the configured IP address ranges via ICMP are included in the result.

If SIMATIC controllers are found during the scan, the IO devices assigned to these controllers can also be included in the monitoring. This is the case regardless of whether the IO devices are located in the scan range or not.

Device profiles and discovery rules

Based on the discovery rules of the device profiles which can be configured on the control under "System administration > Operation parameter profiles" in the parameter group "Device profiles", SINEC NMS assigns the discovered devices to a suitable device profile. SINEC NMS uses the SNMP credentials configured in the parameter group "SNMP settings for discovery" or "Initial credentials" for this purpose. Devices that cannot be assigned to any discovery rules are assigned to default profiles, provided these default profiles are enabled. If the default profiles suitable for devices are not enabled, these devices are not assigned to a device profile and the devices are not monitored, see section Disabling default profiles (Page 54). If the PROFINET discovery is active for a device profile, devices can be assigned to this device profile and the device types it contains using article numbers.

Supported capabilities

SINEC NMS detects the functions supported by the devices during the network scan to decide which devices can be configured with which tasks of a policy. These are displayed after their discovery on the page "Network administration > Configuration Cockpit" of the respective operation in the "Discovered capabilities" device details tab. In the Configuration Cockpit, the discovery of the capabilities can be re-started via the action "Discover capabilities". The detection of the capabilities of devices by SINEC NMS is a basic requirement for their configuration via policies. Only devices that meet this requirement can assume the management status "Managed", refer to section Management status (Page 54).

4.1.1 Management status

The management status of a device indicates how the device can be handled by SINEC NMS:

- Discovered: The device was discovered by SINEC NMS, but the monitoring information has not yet been fully read out.
- Monitored: The device was discovered by SINEC NMS and it is monitored, but the device cannot be configured with SINEC NMS. Either the configuration access to the device has been blocked or the functions supported by the device have not yet been discovered by SINEC NMS. Configuration access to devices can be set and the discovery of capabilities can be started on the page "Network administration > Configuration Cockpit" on the respective operation.
- Managed: The device was discovered by SINEC NMS, it is monitored and can be configured.

The number of devices with "Monitored" and "Managed" management status is limited by the existing SINEC NMS license.

4.1.2 Disabling default profiles

SINEC NMS only monitors devices that have been assigned to device profiles. If SINEC NMS does not find a suitable profile for a device, it assigns one of the following default profiles to the device to ensure that it is monitored:

- Default_ICMP_Device
- Default_SNMP_DCP_Device
- Default_SNMP_Device
- SIEMENS_Standard
- SIEMENS_Basic
- Default_DCP_Device

To deliberately exclude devices from monitoring, device profiles can be disabled on the control under "System administration > Operation parameter profiles", parameter group "Device profiles". This is also possible for default profiles.

Disabling the default profiles can have the following consequences:

- Devices that cannot be assigned to a profile (device-specific profile or default profile) are not entered in SINEC NMS and are therefore not monitored by SINEC NMS. This can occur especially with devices from third party manufacturers for which no device-specific profiles have been created.
- The topology display is incomplete because not all devices found were entered in SINEC NMS.
- If the "Topology-based" rule strategy has been configured for the rule of a policy, the processing sequence of the rule changes according to the missing devices. You can find information on this rule strategy in the section Policy strategies and error handling procedures (Page 188).
- PNIO systems may be incomplete due to missing devices.
- During the network scan, SINEC NMS detects the devices in the first step and assigns them to device profiles in the second step. Devices that were recognized are already displayed in SINEC NMS after the first step. Devices that cannot be assigned to any profiles are thereafter removed from the list.

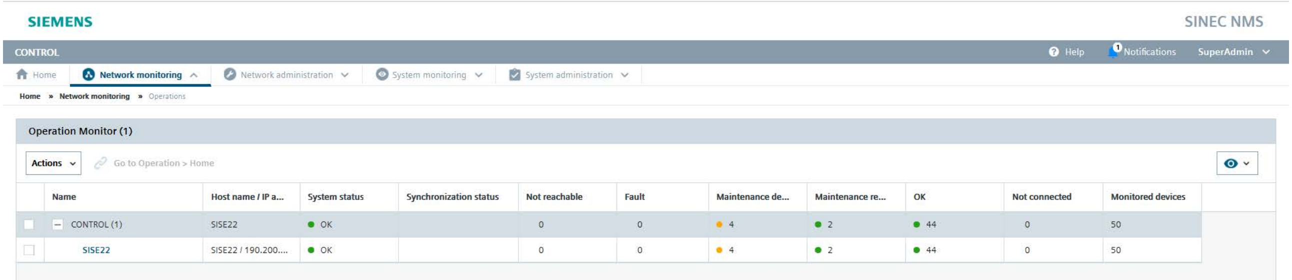
A list of all devices - both those entered in SINEC NMS and those not entered - is specified in the "scanresult_log_[time stamp].csv" log file. This log file is available in the "Siemens\SINECNMS_MON\DiscoveryLog" directory of the operation PC.

4.2 Network monitoring on control

4.2.1 Operations

Control

You reach this page in the navigation of the control under "Network monitoring > Operations".



	Name	Host name / IP a...	System status	Synchronization status	Not reachable	Fault	Maintenance de...	Maintenance re...	OK	Not connected	Monitored devices
□	⊟ CONTROL (1)	SISE22	● OK		0	0	● 4	● 2	● 44	0	50
□	SISE22	SISE22 / 190.200....	● OK		0	0	● 4	● 2	● 44	0	50

Figure 4-1 Monitoring of operations

On the page "Network monitoring > Operations", all operations are displayed which are made known to the control on the page "System administration > Operations". The "Network monitoring > Operations" page specifies the system and synchronization status of the control and the operations and displays information about the devices monitored by the operations.

Properties

The properties of the control and the operations are displayed in the following columns:

- Name

  Displays the names of the control, operations, and subfolders in a hierarchical structure. The subfolders are used to structure operations logically, for example, by location and can be configured on the "System administration > Operations" page, refer to section Operations (Page 241). The number of contained items is displayed in brackets after the name of the control and subfolders.

- Host name / IP address

  Host name / IPv4 address of the control and the operations.

- System status

  The system status specifies the communication status between the control and the operations. If there are error states in the control and the operations, this is also displayed in this column. After clicking on the column entry, information about the cause of error states is displayed. System alarm messages with the status "Pending" are used to determine the system status. For more information on system alarm messages, refer to section System alarm messages (Page 237).
  For the control and subfolders which contain multiple operations, the system status which has the highest priority is always displayed. The system statuses are listed below according to their priority:

  – Timeout

    Communication between control and operation was canceled.

  – First·contact

    The operation has not yet been authenticated at the control, see "Authentication of operations" in the section Operations (Page 241).

  – Initializing

    The communication connection is established between control and operation.

  – Error

    There is an error on the control or an operation. Check pending system alarm messages under "System monitoring > System alarm messages". For information on system alarm messages, refer to section System alarm messages (Page 237).

  – Warning

    A warning message is pending for the control or an operation. Check pending system alarm messages under "System monitoring > System alarm messages". For information on system alarm messages, refer to section System alarm messages (Page 237).

  – OK

    There are no faults or warnings.

- Synchronization status

  If the control is being synchronized with an operation, this is indicated by the character string "Synchronizing".

  If synchronization with an operation is required or has failed or there is a discrepancy between the system / HSP version of Control and Operations, this is indicated in this column by the following symbols and a corresponding message text:

  – ⚠

    A scan range or value of the parameter profile selected for the operation on the page "System administration > Operations" of the control has been changed but not yet synchronized with the operation.

  – ⚠

    The parameter profile selected for the operation on the "System administration > Operations" page of the control does not match the parameter profile active on the operation. The selected parameter profile must therefore be synchronized with the operation.

  - ⚠

    Synchronization with the operation has failed.

  - ↻ System update required:

    The system version of an operation has not yet been updated to the system version of the control. Install the appropriate system version on the operation.
    For operations that with the "System update required" status, network scans and synchronization of parameter profiles with the control cannot be performed. In addition, navigation on these operations is not possible.

  - 🕓 HSP update pending:

    An HSP installed on the control could not yet be transferred to the operation. Check the connection between the control and the operation.

- Not reachable

  Number of devices that currently have the overall status "Not reachable". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- Error

  Number of devices that currently have the overall status "Fault". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- Maintenance demanded

  Number of devices that currently have the overall status "Maintenance demanded". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- Maintenance required

  Number of devices that currently have the overall status "Maintenance required". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- OK

  Number of devices that currently have the overall status "OK". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- Not connected

  Number of devices that currently have the overall status "Not connected". For the control and subfolder that contain multiple operations, the device numbers are shown summarized.

- Monitored devices

  Number of devices that are monitored by the operation. For the control and subfolder that contain multiple operations, the device numbers are shown summarized. In addition, the status of network scans is displayed on the operations. For the control and subfolders that contain multiple operations, the scan status that has the highest priority is always displayed. The scan states are listed below according to their priority:

  – Stopping network scan

  – Stop network scan initiated

  – Executing network scan

  – Starting network scan

- License information

  Specify the type of license, the number of devices included, and the remaining validity period of the license.

- System version

  Installed version of SINEC NMS.

- HSP version

  Installed version of Hardware Support Packages (HSPs). To install HSPs, go to the page "System administration > Control administration > HSP update".

Actions

The following functions are available via the "Actions" drop-down list:

- Go to Op > Home

  Calls the "Home" page on the selected operation.

- Go to Op > Net Mon > Devices

  Calls the page "Network monitoring > Devices" on the selected operation.

- Go to Op > Net Mon > Topology

  Calls the page "Network monitoring > Topology" on the selected operation.

- Go to Op > Net Admin > Config Cockpit

  Calls the page "Network administration > Configuration Cockpit" on the selected operation.

- Go to Ctrl > Sys Admin > Operations

  Calls the page "System administration > Operations" on the control.

- Go to Ctrl > Net Mon > Devices

  Calls the page "Network monitoring > Devices" on the control.

Note

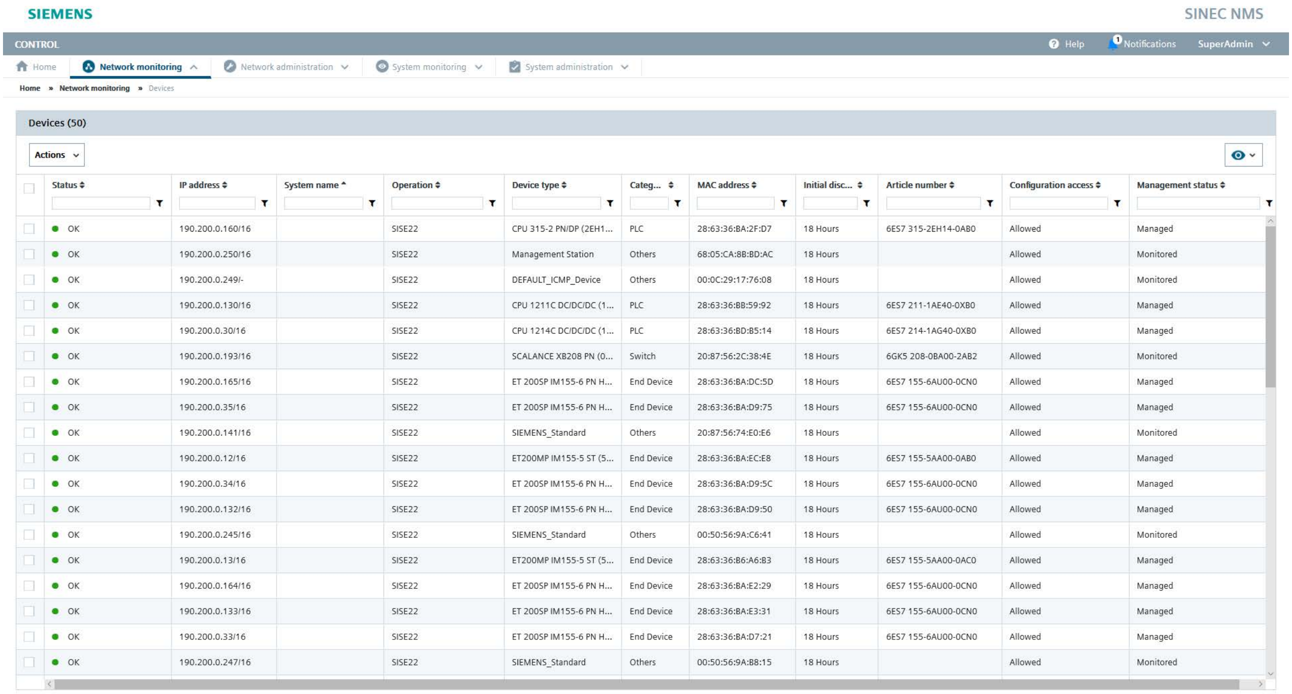
No single sign-on when using local users

When local users are used, no single-sign-on (SSO) is supported between control and operations. When the control calls a page of an operation for the first time, it is therefore necessary to log on to this operation again.

4.2.2 Devices

Control

You reach this page in the navigation of the control under "Network monitoring > Devices".



	Status	IP address	System name	Operation	Device type	Categ...	MAC address	Initial disc...	Article number	Configuration access	Management status
□	● OK	190.200.0.160/16		SISE22	CPU 315-2 PN/DP (2EH1...	PLC	28:63:36:BA:2F:D7	18 Hours	6ES7 315-2EH14-0AB0	Allowed	Managed
□	● OK	190.200.0.250/16		SISE22	Management Station	Others	68:05:CA:8B:BD:AC	18 Hours		Allowed	Monitored
□	● OK	190.200.0.249/-		SISE22	DEFAULT_ICMP_Device	Others	00:0C:29:17:76:08	18 Hours		Allowed	Monitored
□	● OK	190.200.0.130/16		SISE22	CPU 1211C DC/DC/DC (1...	PLC	28:63:36:BB:59:92	18 Hours	6ES7 211-1AE40-0XB0	Allowed	Managed
□	● OK	190.200.0.30/16		SISE22	CPU 1214C DC/DC/DC (1...	PLC	28:63:36:BD:B5:14	18 Hours	6ES7 214-1AG40-0XB0	Allowed	Managed
□	● OK	190.200.0.193/16		SISE22	SCALANCE XB208 PN (0...	Switch	20:87:56:2C:38:4E	18 Hours	6GK5 208-0BA00-2AB2	Allowed	Monitored
□	● OK	190.200.0.165/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:DC:5D	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.35/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:75	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.141/16		SISE22	SIEMENS_Standard	Others	20:87:56:74:E0:E6	18 Hours		Allowed	Monitored
□	● OK	190.200.0.12/16		SISE22	ET200MP IM155-5 ST (5...	End Device	28:63:36:BA:EC:E8	18 Hours	6ES7 155-5AA00-0AB0	Allowed	Managed
□	● OK	190.200.0.34/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:5C	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.132/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D9:50	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.245/16		SISE22	SIEMENS_Standard	Others	00:50:56:9A:C6:41	18 Hours		Allowed	Monitored
□	● OK	190.200.0.13/16		SISE22	ET200MP IM155-5 ST (5...	End Device	28:63:36:B6:A6:B3	18 Hours	6ES7 155-5AA00-0AC0	Allowed	Managed
□	● OK	190.200.0.164/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:E2:29	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.133/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:E3:31	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.33/16		SISE22	ET 200SP IM155-6 PN H...	End Device	28:63:36:BA:D7:21	18 Hours	6ES7 155-6AU00-0CN0	Allowed	Managed
□	● OK	190.200.0.247/16		SISE22	SIEMENS_Standard	Others	00:50:56:9A:B8:15	18 Hours		Allowed	Monitored

Figure 4-2 Device monitoring on the control

On the page "Network monitoring > Devices", the monitored devices of all operations are displayed with their overall states and their discovered device properties. The operations and the scan ranges in which SINEC NMS scans for devices to be monitored can be configured on the control under "System administration > Operations", refer to section Operations (Page 241).

Only monitored devices are displayed on the control. Passively monitored devices are only displayed on the respective operations.

Actions

The following functions are available via the "Actions" drop-down list:

- Go to Op > Home

  Calls the "Home" page on the operation from which the selected device is monitored.

- Go to Op > Net Mon > Devices

  Calls the page "Network monitoring > Devices" on the operation from which the selected device is monitored.

- Go to Op > Net Mon > Topology

  Calls the page "Network monitoring > Topology" on the operation from which the selected device is monitored.

- Go to Op > Net Admin > Config Cockpit

  Calls the page "Network administration > Configuration Cockpit" on the operation from which the selected device is monitored.

- Export as CSV file

  Exports the selected device list entries to a CSV file. If no entries are selected, the entire device list is exported to a CSV file.

Properties

The properties of the devices are displayed in the following columns:

- State

  The overall status of a device is formed by events that are contained in overall status groups and are pending for this device. For more information, refer to section Overall status groups (Page 265). The possible overall states are listed below:

  - 🔴
    Not reachable
  - 🔴
    Error
  - 🟠
    Maintenance demanded
  - 🟢
    Maintenance required
  - 🟢
    OK
  - ⚪
    Not connected
  - New device
    The overall state of the device could not yet be determined.

- IP address

  IP address and subnet mask in CIDR notation

- System name

  System name of the device
- Operation

  Host name of the operation from which the device is monitored
- Device type

  Device type to which the device was assigned by SINEC NMS. For information on device types, refer to section Device profiles (Page 251).
- Category

  Device category that was selected for the device in the corresponding device profile. For more information, refer to section Device profiles (Page 251).
- MAC address

  MAC address of the device
- Initial discovery

  Specifies when the device was first discovered by SINEC NMS
- Article number

  Article number of the device
- Gateway

  IP address of the gateway that is configured for the device
- PROFINET

  PROFINET device name of the device
- Serial number

  Serial number of the device
- Firmware version

  Firmware version that is active on the device
- Hardware version

  Hardware version of the device
- Place of use

  Location that is configured on the device
- Contact person

  Contact person that is configured on the device

- Configuration access

  Configuration access to devices is configured on the "Network administration > Configuration Cockpit" page of the respective operation and displayed on this page as follows:

  - Allowed

    If configuration access is allowed for a device, this device can be configured using SINEC NMS and can adopt the management status "Managed", provided the device is monitored by SINEC NMS and the capabilities of the device have been discovered.

  - Blocked

    If configuration access for a device is blocked, this device cannot be configured using SINEC NMS and the device cannot adopt the management state "Managed".

  - Blocked (untrusted)

    Configuration access is blocked for devices whose SSH/HTTPS fingerprint is not trusted. For these devices, the "Trusted" status must first be set on the "Network administration > Device credential repository" page of the respective operation. Afterwards, the configuration access to these devices can be allowed via the action "Allow configuration access" on the page "Network administration > Configuration Cockpit" of the respective operation.

- Management status

  The management status of a device indicates how the device can be handled by SINEC NMS. For information on the possible management status, refer to section Management status (Page 54).

- Assigned controller

  Controller assigned to the device

- Reason for overall status

  Event that triggered the status of the device. For more information, refer to section Overall status groups (Page 265).

- Comment

  Comment that is added to the operation under "Network monitoring > Devices".

- Last capabilities received

  Time at which the detected functions of the device were last updated.

- Updated on

  Time at which the monitoring information of the device was last updated.

- IP address external

  IP address configured on the NAT router for a device in the external subnet. Only one IP address is displayed if it is a NAT device.

- IP address internal

  IP address of the device

- MAC address external

  MAC address of the NAT router. Only one MAC address is displayed if it is a NAT device.
- NAT device

  Indicates whether the device is accessible from SINEC NMS via a NAT router.

See also

Device credential repository (Page 234)

Configuration Cockpit (Page 223)

4.2.3 Reports

4.2.3.1 Reports

Control

Reports are tabular summaries of discovered device information. Reports can be configured and executed on the "Network monitoring > Reports" page, "Reports" tab. The report status of the executions and generated reports are available on the "Report executions" tab.

Note

Do not shut down SINEC NMS while executing reports.

SINEC NMS must not be shut down during report execution. If SINEC NMS is shut down while reports are being executed, they will not be executed or will not be executed completely.

Actions

The following actions are available:

- Execute

  Executes the selected, enabled report. Once the report is executed, it is displayed in the "Report executions" tab and can be downloaded in CSV format. Disabled reports cannot be executed.
- Create

  Opens the report creation editor, see the "Editor for creating reports" section below.
- Edit

  Opens the report creation editor, see the "Editor for creating reports" section below.
- Delete

  Deletes the selected report. Optionally, the associated historical data can also be deleted.

- Enable

  Enables the selected report. Enabled reports can be executed.
- Disable

  Disables the selected report. Disabled reports cannot be executed.

Editor for creating reports

Reports can be configured using the following settings:

- Type

  Selection of the type for the report to be created:

  – Inventory: Report with detailed information on all devices discovered by operations.

  – Availability: Report with information on how long the devices were reachable in a specified time period.
- Name

  The name of the report is formed by SINEC NMS based on the selected report type and the current time stamp.
- Created by

  User who created the report.
- Send notification

  If this check box is selected, the user who created the report is notified in the Web interface as soon as the report has been completed.
- Send report as attachment

  If this check box is selected, the created report is sent as an attachment to the e-mail that is sent to the specified e-mail addresses when execution of the report has been completed. The check box can only be selected if the check box "Send e-mail" has been selected. Even if the check box is selected, it is still possible to download the report in CSV format.
- Send e-mail

  If this check box is selected, SINEC NMS sends an e-mail to the e-mail addresses specified in the text box as soon as the report has been completed. To use this function, the e-mail settings must be configured on the page "System administration > Control administration", refer to section Control administration (Page 278).

"Filters" tab:

- Role

  The selected role determines which users can work with this report. Only users who have the selected role or a role that is higher-level to the selected role are allowed to work with the report. The authorizations that a user has when working with reports are defined in the authorization management. The role also determines the device areas and the operations that can be selected for the report. The roles of the user and those roles that are subordinate to the roles of the user are available for the selection of the role.

- Device areas

  The selected device areas determine the operations to which the report refers. By default, the "All" option button is selected. With this setting, the report refers to all device areas assigned to the selected role. Device areas that are assigned to the selected role after the report is created are automatically included in the report with the "All" setting.
  The device areas that are assigned to the selected role are available for selection. You configure the device areas of roles on the "System administration > Device·areas" page of the control.

- Operations

  The selected operations determine the devices to which the report refers. The following options are available:

  – All operations of selected device areas

    With this setting, the report refers to all operations that are assigned to the selected device areas. Operations that are assigned to the selected device areas after the report has been created are automatically included in the report with this setting.

  – Select

    Selection of the operations to which the report refers. The operations that are assigned to the selected device areas are available for selection. You configure the operations of device areas on the "System administration > Device·areas" page of the control.

- Last 7 days (only for "Availability" report type)

  The last 7 days are used as the period from which the data for the report is taken.

- Last month (only for "Availability" report type)

  The last month is used as the period from which the data for the report is taken.

- Date range (only for "Availability" report type)

  Manual configuration of the time period from which the data for the report is taken.

"Schedule" tab: Configuration of the schedule for executing the report. If no schedule is configured, the report can only be executed manually.

Properties

The following properties are displayed for the configured reports:

- Name

  The name of the report is formed by SINEC NMS based on the selected report type and the current time stamp.

- Type

  Configured type of report, see section "Editor for creating reports" above.

- State

  Reports can have the following states:

  - Enabled

    The report is enabled and can be executed.

  - Disabled

    The report is disabled and cannot be executed.

  - Inconsistent (gray color)

    The report is inconsistent because it contains no role, no device area, or no operation. Reports with this status must first be supplemented with the missing components and then activated before they can be executed. Only users with the "Super Admin" role can add a role to the report.

  - Inconsistent (yellow color)

    The report is inconsistent because it comes from an older SINEC NMS version and contains no role or device area. Reports with this status can be executed, but viewing and editing the report is only possible for users who have the "Super Admin" role.

- Role

  Configured role of the report, see section "Editor for creating reports" above.

- Last edited by

  User who made the last change to the report and time stamp for the change.

- Schedule

  Configured schedule for report executions. If no schedule has been configured, the report can only be executed manually.

- Last enforcement state

  Last determined execution state for the report. The display follows the same scheme used for policies, refer to section Policy properties and actions (Page 178).

- Next enforcement

  Date and time of the next report execution according to the configured schedule.

- Start

  Date and time of the first report execution according to the configured schedule.

- End

  Date and time of the last report execution according to the configured schedule.

- Send notification

  Specifies whether the user who created the report receives notification in the Web interface when the report is executed.
- Send e-mail

  Specifies whether SINEC NMS is to send an e-mail to the e-mail addresses specified in the text box as soon as the report has been completed.
- E-mail recipient

  E-mail recipient to whom SINEC NMS sends an e-mail as soon as the report has been executed.
- Send report as attachment

  Indicates whether the generated report is to be sent as an attachment to the e-mail that is sent to the specified e-mail addresses once the report has been fully executed.

4.2.3.2 Report executions

Control

Reports created on the control that are configured and executed in the "Reports" tab are displayed on the "Network monitoring > Reports" page in the "Report executions" tab. Using the operator controls in the header, these reports can be deleted, recreated and downloaded as a CSV file. All reports created are stored in the "report" directory of the SINEC NMS installation directory on the control PC. For information on configuring and executing reports, refer to section Reports (Page 64).

4.3 Network·monitoring on operations

4.3.1 Basics of operator control

Operation

The pages for network monitoring of operations contain the following operator controls for the page and table layout as well as options for filtering the monitoring data.

4.3.1.1 Page and table layout

Functions for the page layout

On the pages for the network monitoring of the operations, all tabular displays have a footer that you can use to define the page layout. Other functions are used for navigation within the particular Web page.

Depending on the particular Web page, you have a selection of the following functions:

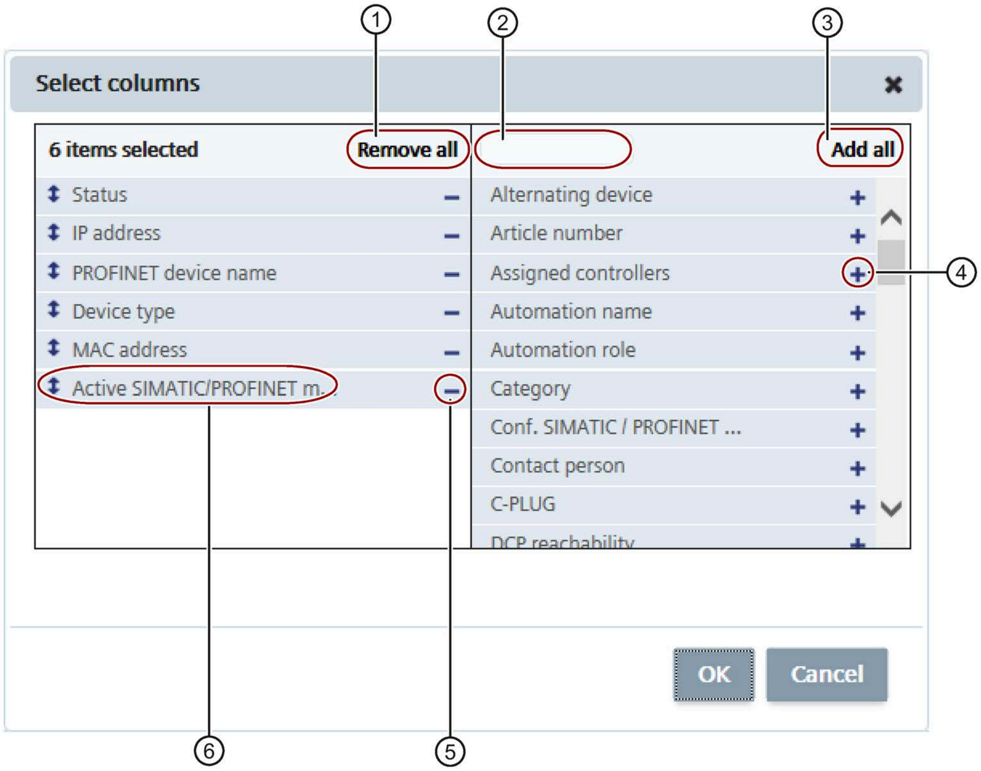
Table 4- 1 Functions for the page layout

Icon	Display / function	Icon	Display / function
🔧	Select and position columns for display.	💾	User-specific saving of the following user interface parameters: • Column selection • Column order • Column width • Column sorting • Number of entries per page • Filter setting using a selection list
↶	Select saved column layout.	↶	Use default column layout
🗋	Export table in CSV format	⏮	Go to first page.
◀◀	Go back one page.	Page 1	Display the current page and option to scroll directly to specific page.
▶▶	Go forward one page.	⏭	Go to last page.
25 ▾	Specify how many rows to display per page.		

Functions for the table layout

In a series of Web pages, information is shown in the form of a table. SINEC NMS provides functions for individual structuring of the table display.

You can see the possible settings for the display in the tables of the following graphic:



① Selection option - remove all columns from the table. At least 1 column must be selected again.

② Input option for character strings - only the elements that contain the specified character string are displayed

③ Selection option - add all columns to the table.

④ Select "+" to add an individual entry as a column in the table

⑤ Select "-" to remove an individual column from the table.

⑥ Move entries up or down using the mouse cursor to change the order of the columns and table.

Figure 4-3 Column selection

Selecting entries in tables

The first column of every table contains check boxes. The check boxes are located in the header row and in each table row.

Follow the steps outlined below to select table entries.

- Select individual entry

  Click in the check box of a table cell. You can use this to select an individual entry and deselect other selected entries.

- Select multiple entries

  Select the check box for the first and last entry in the desired table area while holding down the Shift key.

- Select multiple entries distributed in any way

  Select the check boxes of the desired entries while holding down the Ctrl key.
- Select all entries of the same page

  Select the check box in the header.
- Deselect individual entries

  Click in the check box of the selected entry while holding down the Ctrl key.

4.3.1.2 Filter templates

Operation

Function of filter templates

Data displayed in the device monitoring can be filtered according to various criteria. To avoid needing to configure the selected filter criteria again before every filtering action, you can store these in a filter template and reuse the filter template. Cross-user filter templates can be reused by all users.

Settings of filter templates

The settings that can be made 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 shown below.

1. Prefilters

   The prefilter contains basic filter criteria to be used at the server end on data to be displayed. Data that passes the prefilter is forwarded to the clients.
2. Complex filter

   The data received by the clients is filtered in the second step using a complex query if this exists. With a complex query, filter rules can be created for individually selectable columns. These rules can be logically linked using logical operators and nested in one another by using the rule levels.
3. Simple filter

   The data that has passed the complex filter is filtered in the third step by a free text entry. In contrast to the complex filter, as default the simple filter includes all columns of the relevant data category.

Use of filter templates

Filter templates can be used to filter the following lists:

- Event list
- Device list

- Interface list
- Reports

In the course of the relevant section, the prefilter settings will be described in greater detail. The operator controls of the editor for filter templates and for complex filters are described below. These are identical for all lists to be filtered.

Operator controls of the filter template editor

The following table explains the functions of the operator controls of a filter template.

Table 4- 2 Operator controls of the filter template editor

Operator control / tab name	Function
Simple filter	Filter data using a free text entry. All columns of the relevant data category are included.
Complex filter	The dialog for creating a complex filter query opens; refer to the section "Operator controls of the editor for complex filters".
Prefilters	Prefilter settings for filtering the data to be displayed at the server end. The prefilter settings are described in greater detail in the relevant sections on the event list, device list, interface list and reports.
Delete	Deletes the open filter template
Save	Saves the configured filter settings for the open filter template. System-defined filter templates can only be modified by users with full rights for the operation.
Save as	Opens a dialog for entering a name for the filter template under which the configured filter settings will be saved. The name must be unique on the operation and can contain a maximum of 25 characters. If you select the "Cross-user filter template" check box in this dialog, the filter template can be used by every user who has full rights for the operation. Per list type a maximum of 10 user-specific and 10 cross-user filter templates can be created.
Cancel	Discards changes to the open filter template and closes the filter template and template editor.
Reset filter	Discards changes to the open filter template and closes the filter template.
Use filter	Applies the configured filter settings to the list to be filtered.

Operator controls of the editor for complex filters

The editor for creating a query for the complex filter is opened with the ✏ icon. In the open filter editor, complex filters can be created with the following operator controls. Created filters are displayed in the "Complex filter" area of the filter template textually.

Table 4- 3 Operator controls for complex filters

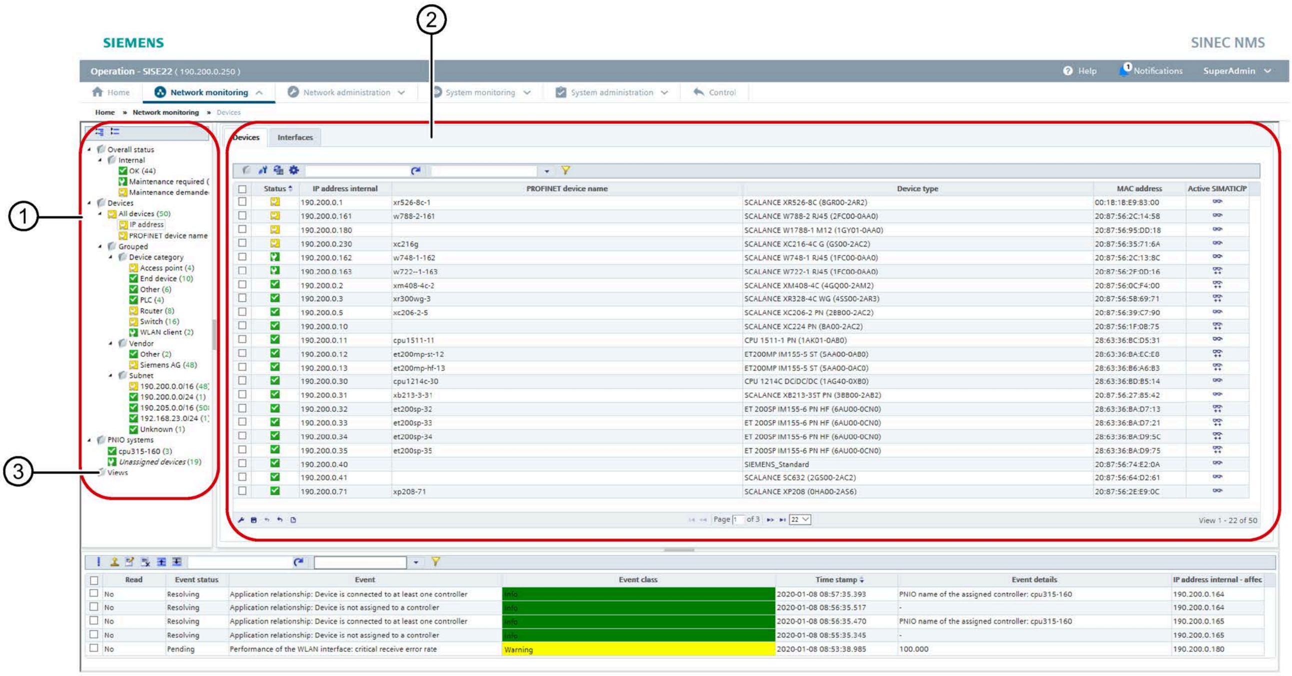
Operator control	Function
Complex filter	Textual representation of the created filter. The textual representation is updated when the operator controls of the editor are used.
↺	As an alternative to using the buttons and drop-down lists of this editor, the filter text can also be edited manually. Using the arrow icon, the modified filter text is validated and adopted for the operator controls of the editor.

Operator control	Function
AND ⌄	Specifies whether the filter rules of the current rule level will be linked with the logical operator "AND" or "OR".
+ {}	Inserts a new rule level below the current rule level. Filter rules can be nested within each other using rule levels. Filter rules of the same rule level are shown in the query box in a common bracket.
+	Inserts a new filter rule at the current rule level. Every filter rule contains a selectable column name, a selectable operator and an input box in which the value of the selected column to be checked with the operator can be entered.
-	Deletes the rule level or the filter rule.
Cancel	Discards changes to the open complex filter and closes the filter editor.
Reset	Discards changes to the open complex filter.
Apply	Saves the settings for the complex filter and closes the filter editor. The created complex filter is now displayed in the "Complex filter" box of the filter template editor.

4.3.2 Devices

Operation

The devices of the operation can be monitored on the page "Network monitoring > Devices" of an operation. The following areas are available for the operation:



- Overall status
  - Internal
    - ✓ OK (44)
    - Maintenance required (
    - Maintenance demande
- Devices
  - All devices (50)
    - IP address
    - PROFINET device name
  - Grouped
    - Device category
      - Access point (4)
      - ✓ End device (10)
      - ✓ Other (6)
      - ✓ PLC (4)
      - Router (8)
      - Switch (16)
      - WLAN client (2)
    - Vendor
      - ✓ Other (2)
      - Siemens AG (48)
    - Subnet
      - 190.200.0.0/16 (48
      - ✓ 190.200.0.0/24 (1)
      - ✓ 190.205.0.0/16 (50
      - ✓ 192.168.23.0/24 (1
      - ✓ Unknown (1)
- PNIO systems
  - ✓ cpu315-160 (3)
  - *Unassigned devices* (19)
- Views

□	Status	IP address internal	PROFINET device name	Device type	MAC address	Active SIMATIC/P
□		190.200.0.1	xr526-8c-1	SCALANCE XR526-8C (8GR00-2AR2)	00:1B:1B:E9:83:00	
□		190.200.0.161	w788-2-161	SCALANCE W788-2 RJ45 (2FC00-0AA0)	20:87:56:2C:14:58	
□		190.200.0.180		SCALANCE W1788-1 M12 (1GY01-0AA0)	20:87:56:95:DD:18	
□		190.200.0.230	xc216g	SCALANCE XC216-4C G (GS00-2AC2)	20:87:56:35:71:6A	
□		190.200.0.162	w748-1-162	SCALANCE W748-1 RJ45 (1FC00-0AA0)	20:87:56:2C:13:8C	
□		190.200.0.163	w722--1-163	SCALANCE W722-1 RJ45 (1FC00-0AA0)	20:87:56:2F:0D:16	
□	✓	190.200.0.2	xm408-4c-2	SCALANCE XM408-4C (4GQ00-2AM2)	20:87:56:0C:F4:00	
□	✓	190.200.0.3	xr300wg-3	SCALANCE XR328-4C WG (4SS00-2AR3)	20:87:56:5B:69:71	
□	✓	190.200.0.5	xc206-2-5	SCALANCE XC206-2 PN (2BB00-2AC2)	20:87:56:39:C7:90	
□	✓	190.200.0.10		SCALANCE XC224 PN (BA00-2AC2)	20:87:56:1F:0B:75	
□	✓	190.200.0.11	cpu1511-11	CPU 1511-1 PN (1AK01-0AB0)	28:63:36:BC:D5:31	
□	✓	190.200.0.12	et200mp-st-12	ET200MP IM155-5 ST (5AA00-0AB0)	28:63:36:BA:EC:E8	
□	✓	190.200.0.13	et200mp-hf-13	ET200MP IM155-5 ST (5AA00-0AC0)	28:63:36:B6:A6:B3	
□	✓	190.200.0.30	cpu1214c-30	CPU 1214C DC/DC/DC (1AG40-0XB0)	28:63:36:BD:B5:14	
□	✓	190.200.0.31	xb213-3-31	SCALANCE XB213-3ST PN (3BB00-2AB2)	20:87:56:27:85:42	
□	✓	190.200.0.32	et200sp-32	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D7:13	
□	✓	190.200.0.33	et200sp-33	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D7:21	
□	✓	190.200.0.34	et200sp-34	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D9:5C	
□	✓	190.200.0.35	et200sp-35	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D9:75	
□	✓	190.200.0.40		SIEMENS_Standard	20:87:56:74:E2:0A	
□	✓	190.200.0.41		SCALANCE SC632 (2GS00-2AC2)	20:87:56:64:D2:61	
□	✓	190.200.0.71	xp208-71	SCALANCE XP208 (0HA00-2AS6)	20:87:56:2E:E9:0C	

Page 1 of 3 22 View 1 - 22 of 50

□	Read	Event status	Event	Event class	Time stamp	Event details	IP address internal - affec
□	No	Resolving	Application relationship: Device is connected to at least one controller	Info	2020-01-08 08:57:35.393	PNIO name of the assigned controller: cpu315-160	190.200.0.164
□	No	Resolving	Application relationship: Device is not assigned to a controller	Info	2020-01-08 08:56:35.517	-	190.200.0.164
□	No	Resolving	Application relationship: Device is connected to at least one controller	Info	2020-01-08 08:56:35.470	PNIO name of the assigned controller: cpu315-160	190.200.0.165
□	No	Resolving	Application relationship: Device is not assigned to a controller	Info	2020-01-08 08:55:35.345	-	190.200.0.165
□	No	Pending	Performance of the WLAN interface: critical receive error rate	Warning	2020-01-08 08:53:38.985	100.000	190.200.0.180

1 Device tree, refer to section Device tree (Page 74)

2 Device window with device list, refer to section Device window with device list (Page 77)

Device window with interface list, refer to section Device window with interface list (Page 83)

3 Node for configurable views in the device tree, refer to section Views (Page 100)

Figure 4-4 Device monitoring on operations

4.3.2.1 Device tree

Operation

The device tree shows a navigation area for selecting device lists that are displayed after they are selected in the "Devices" tab of the device window. The "Interfaces" tab of the device window contains information about the LAN/WLAN attachments of the devices selected in the device tree.

The icons in the for the overall status in the device tree always show the worst current status of one of the device nodes in the branch.

All nodes can be expanded and collapsed using the blue symbols in the device tree header.

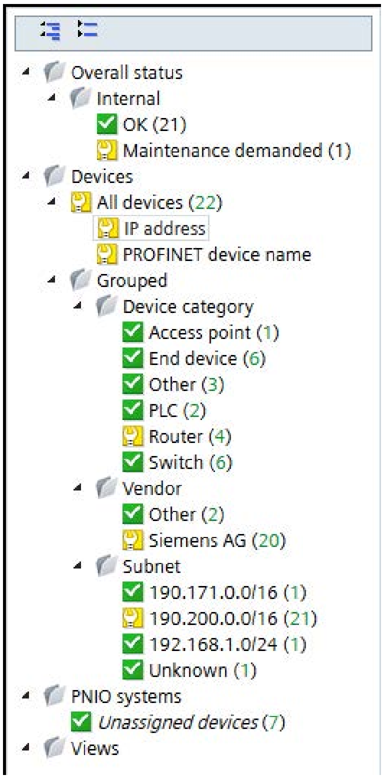


Figure 4-5 Device tree

Layout

- "Overall status" node:

  Below the "Overall status" node, the numbers of overall states of devices which are monitored by the operation are indicated. Selecting an overall status generates a filtered display of the device or interface window according to the overall status.

- "Devices" node:

  The entries below the "Devices" node provide the option of displaying all devices or only devices of a specific category, a specific vendor, a specific subnet or only alternating devices in the devices and interfaces window.
  For grouping according to subnets, the IPv4 addresses and subnet masks of the devices are used. External IP addresses configured for NAT routers are also included in the subnet grouping and after the subnet is selected they are displayed in the device list. For SCALANCE S devices, this is only possible when the operation access takes place via the external subnet. The subnet grouping with IPv6 addresses is not supported.
  The colors of the numbers in brackets indicate the reachability states of the devices.

- "PNIO systems" node:

  The entries below the "PNIO systems" node provide the option of displaying only the controller and the PROFINET IO devices of a certain PROFINET IO system.

  A CPU with SIMATIC capability that is configured as controller in multiple PROFINET IO systems is displayed in each of these PROFINET IO systems.
  The PROFINET interface modules of an HA PROFINET IO device that is integrated into

multiple PNIO systems are displayed in each of these PNIO systems. SINEC NMS treats each PROFINET interface module of an HA PROFINET IO device as a separate device.

Each PROFINET IO system is named after the PROFINET device name of the respective controller and indicates the overall states of associated PROFINET IO devices with the help of colored numbers in parentheses. The requirements for displaying a PNIO system are described in the section "Options for displaying PROFINET I/O systems".

Using the shortcut menu command "Create PNIO view", you can create a view for the devices of a PNIO system. In the views editor that opens after selecting the shortcut menu command, the devices of the PNIO system are already assigned to the view. Passively monitored devices are excluded. Changes made to the PNIO system after creating the view have no effect on the view created for the PNIO system. Changes to a PNIO view have no effect on the PNIO system.

- "Views" node:

  For certain purposes, you can define user-specific views that include only some of the existing devices or only part of the overall network. You will find additional information on this topic in the section "Views (Page 100)".

Status information

In the device tree, you have an overview of the states of the devices monitored in the network. The icons in the device tree always show the worst current status of one of the device nodes in the particular branch.

Table 4- 4 Overall device states

Icon for the status	Description
☑	Device status: Not connected See section Alternating devices (Page 107)
✅	Device status: OK
🟩🔧	Device status: Maintenance required
🟨🔧	Device status: Maintenance demanded
🟥🔧	Device status: Error
❌	Device not reachable

Options for displaying PROFINET IO systems

Depending on which controller is used in a PROFINET IO system, this can be displayed in different ways:

- Devices with SIMATIC capability:

  The PROFINET IO system can be displayed with the aid of the information that the controller obtains from assigned PROFINET IO devices. To do this, the monitoring setting "SIMATIC monitoring of assigned devices" must be enabled for the controller. In a display of the PROFINET IO system initiated by the controller, the displayed IP addresses are always IP addresses reported by the controller. In this representation, devices are also displayed that are assigned to the controller but that are themselves not SINEC NMS objects.

- Other controller types:

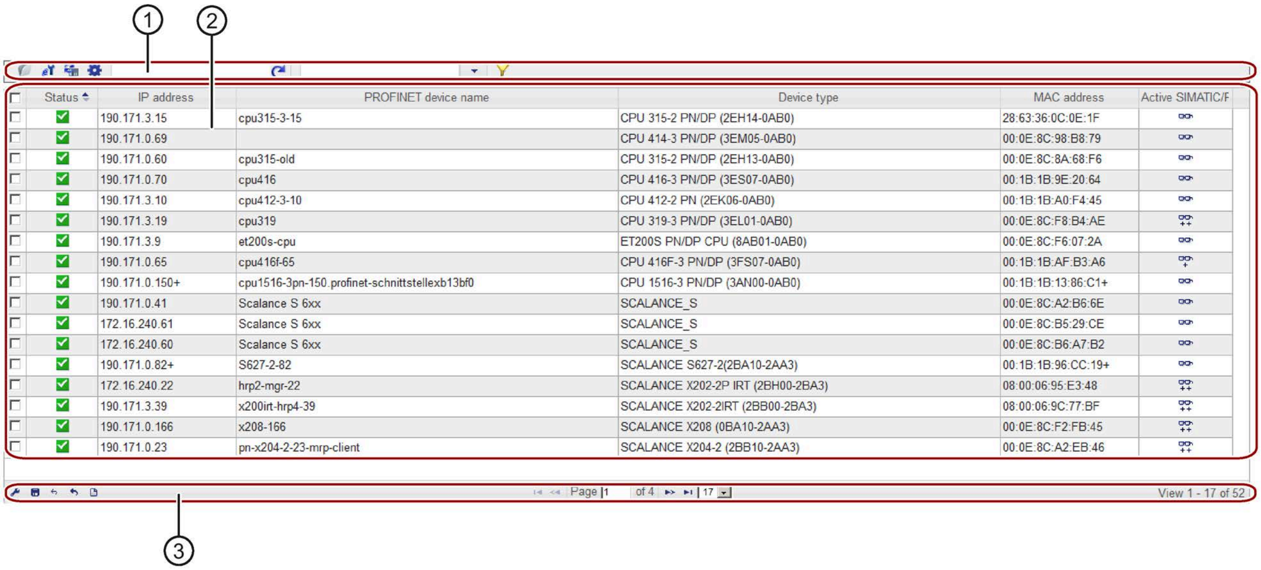
  The PROFINET IO system can be displayed with the aid of information that PROFINET IO devices obtain from their controller. To do this, the monitoring setting "PROFINET monitoring" must be enabled for the PROFINET IO devices to be displayed. If the display of the PROFINET IO system was initiated by PROFINET IO devices, the tooltip of the associated entry displays "Discovered by: IO devices".

PROFINET IO devices that cannot be assigned are displayed under the entry "Unassigned devices".

4.3.2.2 Device window with device list

Operation

The "Devices" tab displays information about the devices that were selected via the corresponding entry in the device tree.



□	Status	IP address	PROFINET device name	Device type	MAC address	Active SIMATIC/F
□	✓	190.171.3.15	cpu315-3-15	CPU 315-2 PN/DP (2EH14-0AB0)	28:63:36:0C:0E:1F	
□	✓	190.171.0.69		CPU 414-3 PN/DP (3EM05-0AB0)	00:0E:8C:98:B8:79	
□	✓	190.171.0.60	cpu315-old	CPU 315-2 PN/DP (2EH13-0AB0)	00:0E:8C:8A:68:F6	
□	✓	190.171.0.70	cpu416	CPU 416-3 PN/DP (3ES07-0AB0)	00:1B:1B:9E:20:64	
□	✓	190.171.3.10	cpu412-3-10	CPU 412-2 PN (2EK06-0AB0)	00:1B:1B:A0:F4:45	
□	✓	190.171.3.19	cpu319	CPU 319-3 PN/DP (3EL01-0AB0)	00:0E:8C:F8:B4:AE	
□	✓	190.171.3.9	et200s-cpu	ET200S PN/DP CPU (8AB01-0AB0)	00:0E:8C:F6:07:2A	
□	✓	190.171.0.65	cpu416f-65	CPU 416F-3 PN/DP (3FS07-0AB0)	00:1B:1B:AF:B3:A6	
□	✓	190.171.0.150+	cpu1516-3pn-150.profinet-schnittstellexb13bf0	CPU 1516-3 PN/DP (3AN00-0AB0)	00:1B:1B:13:86:C1+	
□	✓	190.171.0.41	Scalance S 6xx	SCALANCE_S	00:0E:8C:A2:B6:6E	
□	✓	172.16.240.61	Scalance S 6xx	SCALANCE_S	00:0E:8C:B5:29:CE	
□	✓	172.16.240.60	Scalance S 6xx	SCALANCE_S	00:0E:8C:B6:A7:B2	
□	✓	190.171.0.82+	S627-2-82	SCALANCE S627-2(2BA10-2AA3)	00:1B:1B:96:CC:19+	
□	✓	172.16.240.22	hrp2-mgr-22	SCALANCE X202-2P IRT (2BH00-2BA3)	08:00:06:95:E3:48	
□	✓	190.171.3.39	x200irt-hrp4-39	SCALANCE X202-2IRT (2BB00-2BA3)	08:00:06:9C:77:BF	
□	✓	190.171.0.166	x208-166	SCALANCE X208 (0BA10-2AA3)	00:0E:8C:F2:FB:45	
□	✓	190.171.0.23	pn-x204-2-23-mrp-client	SCALANCE X204-2 (2BB10-2AA3)	00:0E:8C:A2:EB:46	

① Header with toolbar

② Device list with status display and configurable columns

③ Footer with setting functions and navigation

Figure 4-6 Device window with device list

Device lists are divided into several columns in which the device-specific data is displayed. With the exception of the first column that is used to select rows, you can select any other column as required, see section Page and table layout (Page 69). For example the column for IPv4 addresses displayed as default can be removed and the column for IPv6 addresses can be added. Values that can no longer be updated because protocol reachability is not available are displayed grayed out.

Possible monitoring states

The symbol in the "Active monitoring status" column specifies whether and what type of monitoring is active for a device. In the active monitoring status, the PROFINET/SIMATIC devices also include the globally and locally configured PROFINET/SIMATIC monitoring settings.

Table 4- 5 Monitoring states of devices

Icon	Meaning
👓⊘	The device is not monitored.
👓→	The PROFINET IO device becomes passive; in other words, only monitored by the CPU with SIMATIC capability assigned to the device. Passively monitored devices are shown only in the PNIO system they belong to. For passively monitored devices, no PROFINET monitoring settings can be configured. The passive monitoring of devices can be selected when the devices cannot be reached by SINEC NMS. Passively monitored devices do not require a device license. The prerequisite for passive monitoring is that the CPU with SIMATIC capability can be reached by SINEC NMS and that the monitoring setting "SIMATIC monitoring of assigned devices" is active for this CPU.
👓	The device is monitored by SINEC NMS with the aid of the protocols ICMP / DCP / SNMP.
👓+	The device is monitored by SINEC NMS with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring mode is also active: • PROFINET: The PROFINET monitoring of the PROFINET IO device by SINEC NMS is active. • SIMATIC: The SIMATIC monitoring of the CPU with SIMATIC capability by SINEC NMS is active.
👓++	The device is monitored by SINEC NMS with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring modes are also active: • PROFINET: – The PROFINET monitoring of the PROFINET IO device by SINEC NMS is active. – The PROFINET acquisition of port statistics of the PROFINET IO device by SINEC NMS is active. • SIMATIC: – The SIMATIC monitoring of the CPU with SIMATIC capability by SINEC NMS is active. – The SIMATIC monitoring of the PROFINET IO devices assigned to the controller by the CPU with SIMATIC capability is active. The SIMATIC monitoring of SIMATIC event / alarm messages is not shown in the displayed monitoring status.

Operator input

The following table shows the functional elements of the header.

Table 4- 6 Basic settings

Icon	Display / function	Icon	Display / function
	Show details of the selected device		Call WBM (Web Based Management) If a Web page is available for the selected device, this is opened. This page displays specific information and settings for the selected network device.
	Reread device data The data of the device is read out again according to the active monitoring setting. Device data can be reread every 2 minutes.	⚙	Advanced settings Opens a menu bar in which the advanced settings are available. This is described in the table "Advanced settings", see below.
	Enter text to filter based on devices. The entered text is searched for in all columns. In the text box, text is displayed when a simple query entered in the Filter Template Editor is active. The ▣ icon is displayed when a filter template with prefilter settings is active. The () icon is displayed when a filter template with a complex query is active.		Selection of a previously created template for filtering according to devices. After selection, the properties of the filter template are applied to the device list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
▽ ▽✓	Open the editor for configuring filter settings that can be stored in filter templates. The ▽✓ icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for device lists".		

Table 4- 7 Advanced settings

Icon	Display / function	Icon	Display / function
	Add comment		Delete the selected notes
	Enable monitoring Enable monitoring for the selected devices. Any PROFINET/SIMATIC monitoring available for the device is performed according to the PROFINET/SIMATIC monitoring settings configured on the control and operation. If the selected device is a PROFINET IO device and if the monitoring of assigned devices is enabled for the controller assigned to it, as an alternative to enabling monitoring by SINEC NMS, you can enable passive monitoring for the device. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.		Turn off monitoring Disable monitoring for the selected devices. If the selected device is a monitored PROFINET IO device and if the monitoring of assigned devices is activated for the controller assigned to it, as an alternative to fully disabling monitoring, you can also enable passive monitoring. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.
	Monitoring settings The functions of the local PROFINET/SIMATIC monitoring settings correspond to the PROFINET/SIMATIC monitoring settings configured on the page "System administration > Operation parameter profiles" on the control in the parameter groups "PROFINET monitoring settings" and "SIMATIC monitoring settings". When SIMATIC monitoring is enabled for a device, SNMP is used to check whether the device has a firmware version that has been released for SIMATIC monitoring by SINEC NMS. To activate SIMATIC monitoring for a device, this must therefore be reachable via SNMP and must have information about the installed firmware version. Local monitoring settings only take effect on devices if the monitoring settings of the same name are active on the control. Devices can also be configured as alternating devices. If the property "Alternating device" is removed from a device, all the connections learned for this device are deleted.		Creating a new device Behavior when creating NAT devices: • The operation is located in the external subnet: The specified IP Address is the external IP address for the device at the NAT router • The operation is located in the internal subnet: The specified IP address is the IP address of the device.

Icon	Display / function	Icon	Display / function
✕	Delete the selected devices After it is deleted, the device only continues to exist in the report archive. When you delete a PROFINET IO device being monitored by a CPU with SIMATIC capability using the function "SIMATIC monitoring of assigned devices", this PROFINET IO device is discovered by the controller again after it has been deleted and therefore shown again in the corresponding PNIO system.		Change device type Opens the "Set device type for" dialog in which a different device type can be assigned using the available profiles. DCP can also be enabled and the SNMP settings changed.
	Adapt the monitoring profile Opens the "Set monitoring profile for" dialog If necessary you can use this method to assign a monitoring profile to the device in addition to the general profile.		Customize device data The "Adapt device" dialog opens. Here, you will find the following tabs for further entries: • User-defined links When necessary, you can store links (URL) to further information that is useful in conjunction with monitoring the device. • Basic data In this tab you can specify a device icon for the device, set the protocol and the port for calling the WBM and configure the article number of the device. The configuration of article numbers for several devices at the same time is possible only for devices that do not have a standard profile assigned to them. The article numbers configured by the user have a higher priority than article numbers discovered by the operation.

Prefilters in the filter templates for device lists

Device lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for device lists. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

Table 4- 8 Filter settings

Box group	Filter options
Basic filter	Filter according to devices for which the port statistics are activated /deactivated: • All • Yes: Devices with activated port statistics • No: Devices with deactivated port statistics Filter according to devices that are part / not part of the reference topology: • All • Yes: Devices that are part of the reference topology • No: Devices that are not part of the reference topology
Monitoring status	Filter according to devices with a certain monitoring status.

Functions of the shortcut menu

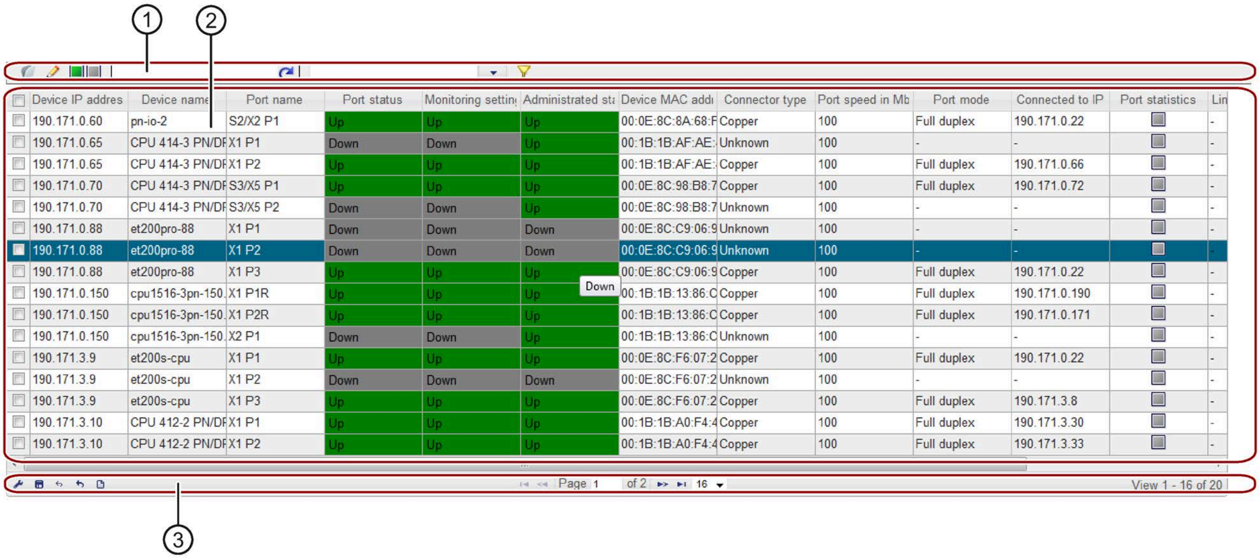
The functions presented above can also be called alternatively using the shortcut menu.

The shortcut menu also provides the option of calling up the Configuration Cockpit, the topology display or a view-specific topology display from the device window. The device selected using the shortcut menu is shown centered and selected in the topology display.

4.3.2.3 Device window with interface list

Operation

The "Interfaces" tab displays information on the interfaces of the devices that were selected via the corresponding entry in the device tree.



□	Device IP addres	Device name	Port name	Port status	Monitoring settin	Administrated sta	Device MAC addı	Connector type	Port speed in Mb	Port mode	Connected to IP	Port statistics	Lin
□	190.171.0.60	pn-io-2	S2/X2 P1	Up	Up	Up	00:0E:8C:8A:68:F	Copper	100	Full duplex	190.171.0.22	□	-
□	190.171.0.65	CPU 414-3 PN/DF	X1 P1	Down	Down	Up	00:1B:1B:AF:AE:	Unknown	100	-	-	□	-
□	190.171.0.65	CPU 414-3 PN/DF	X1 P2	Up	Up	Up	00:1B:1B:AF:AE:	Copper	100	Full duplex	190.171.0.66	□	-
□	190.171.0.70	CPU 414-3 PN/DF	S3/X5 P1	Up	Up	Up	00:0E:8C:98:B8:7	Copper	100	Full duplex	190.171.0.72	□	-
□	190.171.0.70	CPU 414-3 PN/DF	S3/X5 P2	Down	Down	Up	00:0E:8C:98:B8:7	Unknown	100	-	-	□	-
□	190.171.0.88	et200pro-88	X1 P1	Down	Down	Down	00:0E:8C:C9:06:9	Unknown	100	-	-	□	-
□	190.171.0.88	et200pro-88	X1 P2	Down	Down	Down	00:0E:8C:C9:06:9	Unknown	100	-	-	□	-
□	190.171.0.88	et200pro-88	X1 P3	Up	Up	Up	00:0E:8C:C9:06:9	Copper	100	Full duplex	190.171.0.22	□	-
□	190.171.0.150	cpu1516-3pn-150.	X1 P1R	Up	Up	Up	00:1B:1B:13:86:C	Copper	100	Full duplex	190.171.0.190	□	-
□	190.171.0.150	cpu1516-3pn-150.	X1 P2R	Up	Up	Up	00:1B:1B:13:86:C	Copper	100	Full duplex	190.171.0.171	□	-
□	190.171.0.150	cpu1516-3pn-150.	X2 P1	Down	Down	Up	00:1B:1B:13:86:C	Unknown	100	-	-	□	-
□	190.171.3.9	et200s-cpu	X1 P1	Up	Up	Up	00:0E:8C:F6:07:2	Copper	100	Full duplex	190.171.0.22	□	-
□	190.171.3.9	et200s-cpu	X1 P2	Down	Down	Down	00:0E:8C:F6:07:2	Unknown	100	-	-	□	-
□	190.171.3.9	et200s-cpu	X1 P3	Up	Up	Up	00:0E:8C:F6:07:2	Copper	100	Full duplex	190.171.3.8	□	-
□	190.171.3.10	CPU 412-2 PN/DF	X1 P1	Up	Up	Up	00:1B:1B:A0:F4:4	Copper	100	Full duplex	190.171.3.30	□	-
□	190.171.3.10	CPU 412-2 PN/DF	X1 P2	Up	Up	Up	00:1B:1B:A0:F4:4	Copper	100	Full duplex	190.171.3.33	□	-

① Header with toolbar

② Interface list with configurable columns

③ Footer with setting functions and configuration limits (identical to the footer of the device list)

Figure 4-7 Device window with interface list

Operator input

Interface lists are divided into several columns in which the data of the interfaces and their devices is displayed. With the exception of the first column that is used to select rows, you can select any other column as required.

The following table shows the functional elements of the header.

Table 4- 9 Function elements of the header

Icon	Display / function
	Show device details Depending on whether the selected interface is a LAN or WLAN interface, the "LAN" or the "WLAN" tab of the device details is opened.
✏	Edit port details The dialog for editing interface information opens. The meaning of the functions of this editor can be found in the section "Editor for detailed information on (W)LAN ports" in the operating instructions.

Icon	Display / function
🟩	Enable / disable interface statistics. If the interface statistics are disabled, the interface is not included in reports that can be generated on the operation under "Network monitoring > Reports > Availability > Interfaces".
{} ▣ ↻	Enter text to filter based on events. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The ▣ icon is displayed when a filter template with prefilter settings is active. The {} icon is displayed when a filter template with a complex query is active.
▾	Selection of a previously created template for filtering according to interfaces. After selection, the properties of the filter template are applied to the interface list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
▽ ▽✓	Open the editor for configuring filter settings that can be stored in filter templates. The ▽✓ icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for interface lists".

The shortcut menu provides the option of calling up the Configuration Cockpit, the topology display or a view-specific topology display from the device window. The device of the interface selected using the shortcut menu is shown centered and selected in the topology display.

Prefilters in the filter templates for interface lists

Interface lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for interface lists. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

Table 4- 10 Filter settings

Operator control	Filter options
From IP To IP	Filter according to interfaces that have the specified device IP addresses.
Device name and device type	Filter according to interfaces that belong to devices with the specified device name or device type.
Statistics activated	Filter according to interfaces for which the port statistics are activated /deactivated: • All • Yes: Interfaces with activated port statistics • No: Interfaces with deactivated port statistics

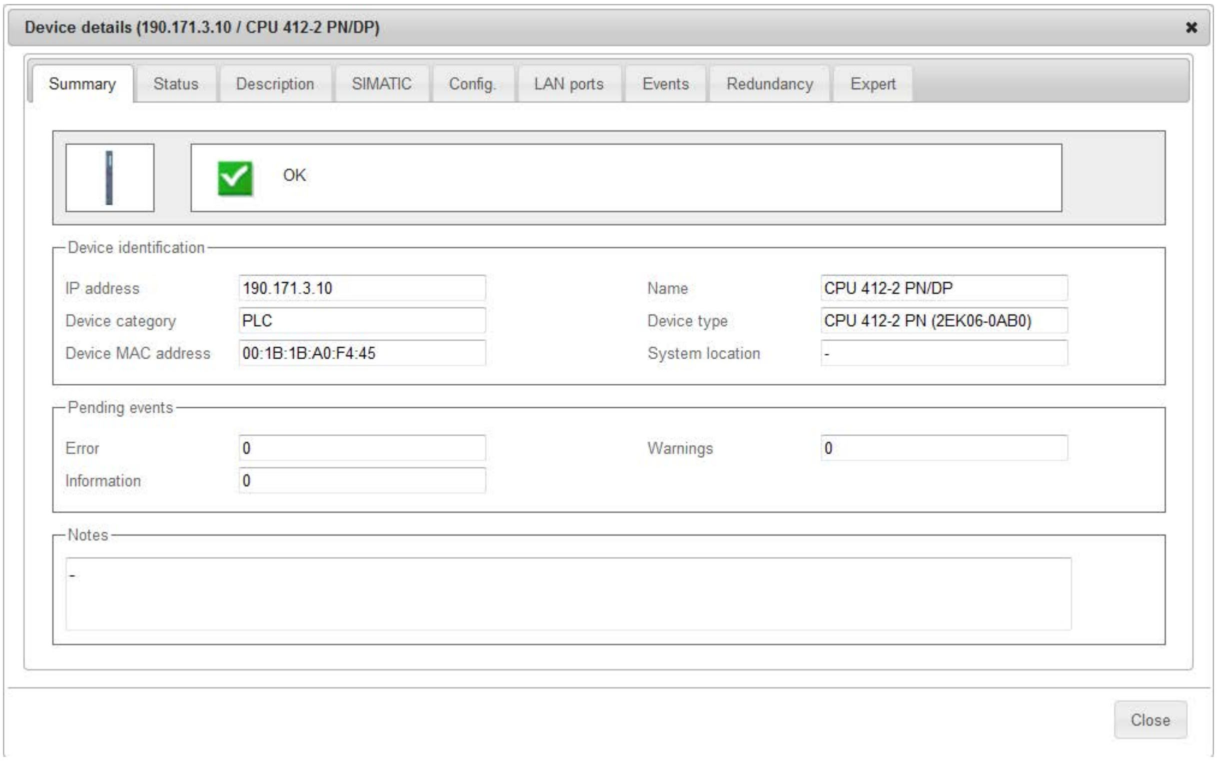
4.3.2.4 Device details

Operation

You can open the "Device details" window as follows:

- Device window
  - Icon
  - Double-click on the appropriate row
- Any topology view ("Topology > …" or "Views > …")
  - Shortcut menu of the device
  - Double-click on device icon

The following figure shows the "Overview" tab of the device details as an example of the tabs available.



Device details (190.171.3.10 / CPU 412-2 PN/DP)

✓ OK

Device identification

IP address	190.171.3.10	Name	CPU 412-2 PN/DP
Device category	PLC	Device type	CPU 412-2 PN (2EK06-0AB0)
Device MAC address	00:1B:1B:A0:F4:45	System location	-

Pending events

Error	0	Warnings	0
Information	0		

Notes

-

Figure 4-8 Device details

Overview

The "Device Details" window consists of several tabs in which the data from a device are grouped in a detailed manner or are displayed in list form.

Operator input

The following table shows the tab contents of the "Device Details" window with a brief explanation. For NAT devices, the external IP address is displayed in the window title in addition to the IP address and the name of the device. The display scheme is: Internal IP address / external IP address / device name.

Only the tabs and boxes are displayed that are relevant to the selected device. The tabs and boxes relevant for a device whose content cannot be read out by the operation due to deactivated monitoring settings or the protocol currently being used are shown grayed out. Values that can no longer be updated because protocol reachability is not available are also displayed grayed out. In the "Expert" tab, you have the option of hiding such old values. In boxes whose values cannot be displayed despite available protocol reachability, the "-" character is displayed.

For newly discovered, passively monitored devices, only the "Overview" and "Events" tabs are displayed.

Table 4- 11 "Overview" Tab

Parameter group	Display, content
-	Icon and overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Device name	IPv4 address, name, device category and type MAC address and location
NAT device identification	For devices that the operation can reach via NAT routers (1:1 NAT), instead of the parameter group "Device identification", the parameter group "Identification of NAT device" is displayed. The IP address and the MAC address of a NAT device are displayed in the boxes "Internal IP address" and "Internal MAC address". The detection of IP address changes is nor supported for NAT devices. The "External IP address" box displays the IP address configured on the NAT router for the device in the external subnet. The operation sends queries for monitoring the NAT device to this external IP address if the operation is not connected in the internal network. The "External MAC address" box displays the MAC address of the NAT router. For more detailed information on monitoring of NAT devices and NAT routers, refer to the section Monitoring of NAT devices and NAT routers (Page 104).
Pending events	Number of events pending for the device of the classes "Error", "Warning" and "Information"
Remarks	Comments, information

Table 4- 12 "Status" tab

Parameter group	Display, content
-	Overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Reachability	Information on the protocol-specific reachability of the device: Polling group, ICMP reachability ("Ping status"), SNMP reachability, overall status related to reachability, DCP reachability, SIMATIC or PROFINET reachability The overall status related to reachability is not influenced by DCP reachability.
Status details	In the "Device operational state" box, the device status obtained by SNMP is shown. For CPUs with SIMATIC capability, the Status LED and for PROFINET IO devices the PNIO Channel Status is shown. Notes on the LED status: • BUS1F: First bus error LED • BUS2F: Second bus error LED • BUS3F: Third bus error LED
Summary LAN ports	Number of ports in total, used, active and inactive (differing from reference), as well as with critical behavior
Times	Information, when • first and last time detected, • the last poll occurred, • the oldest stored data was read in and how long it was last active (up time)
Miscellaneous	Information relating to C-PLUG, power supply status

Table 4- 13 "Description" tab

Parameter group	Display, content
Names	PROFINET IO, system and automation name
Place of use	Location according to system and automation
Identification and maintenance	Article number, serial number, vendor ID and name, firmware version, hardware revision, DCP-ID
Manual changes	Information on whether the device type was changed and whether the device was migrated and created manually
User-defined links	Display of links 1 to 3, if entered You enter links using the "Customize device data" function.
Discovery and monitoring settings	Profile name and identifier, discovery and device type rule (in each case name and content), name and identifier of the monitoring profile

Parameter group	Display, content
Port assignment protocol	The "Port assignment" box displays whether or not the port-specific data of a device can be read out both using SNMP as well as using PROFINET and assigned to the corresponding ports. This is ensured when the data obtained via SNMP and PROFINET for the port assignment are compatible with each other. The port assignment allows the operation to switch over between SNMP and PROFINET depending on protocol availability. When there is such a protocol change, the following situations are distinguished: • All port information is compatible with the new protocol: The existing port information remains when there is a change of protocol. • Some port information is compatible with the new protocol: Only the information of the ports that can be read out and assigned via the new protocol are displayed. The information of the other ports is removed from the device details and from the topology. • No port information is compatible with the new protocol: The ports of the device are displayed grayed out in the device details and in the topology. In the "Protocol used" box, the protocol currently being used for reading out and for assigning port information is displayed. When using PROFINET, only the information of physical ports can be read out.
Miscellaneous	Contact, assigned filter groups for topology representation, OPC UA index, OPC DA index and information about the visibility in OPC

The "SIMATIC" tab is active for CPUs with SIMATIC capability with active SIMATIC monitoring. To detect multiple PROFINET IO systems on a CPU with SIMATIC capability, the SIMATIC monitoring of assigned devices must also be active. The CPUs for which SIMATIC monitoring is supported are listed in the readme file of SINEC NMS.

Table 4- 14 "SIMATIC" tab (only active for CPUs with SIMATIC capability with active SIMATIC monitoring)

Parameter group	Display, content
SIMATIC identification	Information to identify the CPU with SIMATIC capability.
PROFINET IO controller	This area shows the interfaces of the CPU with SIMATIC capability at which it is configured as PROFINET IO controller.
Configured cycle time	Configured minimum and maximum value for the cycle time in ms.
Measured cycle time	The shortest, last read and longest cycle time read out in ms. The values for the cycle times are recalculated every 60 seconds.
SIMATIC status of assigned devices	This area shows how many of the assigned PROFINET IO devices have which status relating to the associated controller: • Configured devices: Total number of devices configured as PROFINET IO devices in STEP 7. • Active devices: Number of devices exchanging data with the controller. • Deactivated devices: Number of devices deactivated by the controller. • Faulty devices: Number of devices in the "Error" status. • Missing devices: Number of devices configured as PROFINET IO devices in STEP 7 that have, however, not been reached by the controller.

Parameter group	Display, content
SIMATIC event / alarm messages	Date and time of the last logon (to receive SIMATIC event and alarm messages from the CPU with SIMATIC capability): Time of the last attempted logon to the CPU with SIMATIC capability Date and time of the last read out: Time of the last successful read out of the display texts from the CPU with SIMATIC capability Date and time of the last attempted read out: Time of the last attempt to read out the display texts from the CPU with SIMATIC capability
H-system	For SIMATIC S7-400-H CPUs, the operating mode of the associated H system (redundancy mode / stand-alone mode) as well as the operating mode of the modules involved (RUN / STOP) are displayed in this area. It is also specified which CPU is currently in master mode and which in standby mode. The CPU whose device details are open is highlighted in blue. Double-click the partner CPU to call up its device details. To display both CPUs of the H system, SIMATIC monitoring must be activated for both CPUs.

Table 4- 15 "PROFINET" tab (only active for PROFINET IO devices with active PROFINET monitoring)

Parameter group	Display, content
PROFINET identification	Information to identify and to assign the controller of the PROFINET IO device
High Availability	For devices with High Availability support, the High Availability operating mode (redundancy mode / stand-alone mode) is displayed in this area. The "HA device diagnostics" table shows the detected PROFINET interface modules of the device and the assigned controllers. SINEC NMS treats each PROFINET interface module of an HA device as a separate device. The PROFINET interface module whose device details are open is highlighted in blue. Double-click the partner module to call up its device details.
PROFINET diagnostics	PROFINET standard diagnostics contains status information of the PROFINET IO device at the slot and subslot level. This, for example, informs you about configured modules that do not exist in slots. PROFINET channel diagnostics collects additional status information from channels. With the "Diagnostics details" button, a table can be called which displays additional diagnostics details such as the weighting (Severity) of negative states. In the "Text" column of the PROFINET standard diagnostics and the PROFINET channel diagnostics, the texts of the PROFINET diagnostics library are shown that could be assigned to the read out raw data of the devices. If no assignment could be made the raw data is displayed in hexadecimal format. Only current data is displayed, historical data is displayed only in corresponding events.

Table 4- 16 "Config." tab (Configuration)

Parameter group	Display, content
Ethernet	MAC address of the device
IP addresses	Display of the IPv4 and IPv6 addresses of the device with standard gateway, subnet mask and origin of the IP addresses, e.g. assignment via DHCP.
PROFINET	PNIO name and type

Parameter group	Display, content
SNMP settings	Configuration name, traps enabled, SINEC NMS trap receiver (yes / no)
General SNMP traps	Information about whether the following traps were enabled: • Connection establishment and termination • Warm and cold restart • Authentication failed
Miscellaneous	Radius server address; IP forwarding (yes / no / not supported) Alternating device (yes / no)

Table 4- 17 "LAN" tab

Parameter group	Display, content
-	Table of all LAN ports with name, status, MAC, transmission medium, data rate and other freely selectable information. The entire table can be formatted and used as described for the device window (column width, export etc.). There are icons available above the table with following functions: • Show port details • Change port details, refer to the section "Editor for detailed information on (W)LAN ports" in the operating instructions • Enable port statistics • Disable port statistics If statistics is activated for a port, information about data traffic, port load and error rates is monitored using SNMP or possibly PROFINET. This information is included in reports that can be generated on the operation under "Network monitoring > Reports > Availability > Interfaces".

Table 4- 18 "WLAN" tab

Parameter group	Display, content
-	Table of all WLAN interfaces with index, name, status, SSID and information about critical states. The content of the table corresponds to the "LAN ports" tab. The "Open interface" icon provides you with more detailed information.

Table 4- 19 "Events" tab

Parameter group	Display, content
-	Table of all reported events with name, status, timestamp, status and other arbitrary information. The entire table can be formatted and used as described for the device window (column width, export etc.). There are icons available above the table with following functions: • Mark events as "Read" • Resolve pending events • Add / edit remark • Delete remark • Filter options similar to event list

Table 4- 20 "IP Interfaces" tab

Parameter group	Display, content
-	Display of all interfaces of a device with relevant IPv4 or IPv6 address and the associated connection status. The table is displayed only for devices that can be reached via at least two IP addresses. For NAT routers of the module type SCALANCE S, in addition to the IP addresses of the interfaces, the IP addresses are displayed via which the operation can reach NAT devices with 1:1 NAT. The "Define as management IP address" button can be used to define the interface with the IP address used for monitoring, configuring and identifying the device in the user interface. The accessibility of a device is determined by the IP address selected here. By default, the IP address that was used to discover the device is selected. IP addresses of interfaces that are not in use, IPv6 addresses and external IP addresses of NAT devices cannot be defined as management IP addresses.

Depending the NAT router being used, the "NAT" tab displays the configurations for static NAT (1:1 NAT), Pooled NAT and NAPT. The NAT rules are displayed regardless of whether NAT was enabled for the NAT router. The displayed NAT rules can contain IPv4 or IPv6 addresses.

You will find information on the supported NAT routers in the section Monitoring of NAT devices and NAT routers (Page 104).

For general information on NAT, refer to the Glossary.

Table 4- 21 "NAT" tab

Tab	Display, content
Static NAT (1:1 NAT)	NAT rules for static NAT (1:1 NAT)
Pooled NAT	NAT pools of the NAT router with external start and end addresses. A maximum of 20 NAT pools can be displayed. After double-clicking on a NAT pool the NAT devices are displayed that use the particular NAT pool.
NAPT	NAPT rules for IP address translations with port forwarding.

Table 4- 22 "VLAN" tab

Parameter group	Display, content
Basic data	Maximum number of possible VLANs and currently used VLANs
VLANs	Table of the currently used VLANs with identifier (VID), name and status and the "tagged" and "untagged" ports.

Table 4- 23 "Firewall" tab (only available for SCALANCE SC-600, SCALANCE S615 and RUGGEDCOM ROX2 devices with firewall support)

Parameter group	Display, content
Firewall rules	Firewall activation state and display the firewall rules present on the firewall device.

Table 4- 24 "Redundancy" tab

Parameter group	Display, content
-	Table of all redundancy mechanisms used with the ports involved, protocol used, status, role (manager or client) along with supplementary information. The "Open port details" icon provides you with incoming information.

Table 4- 25 "Expert" tab

Parameter group	Display, content
-	Listing of all the parameters read from the device with associated value, protocol and time of the last change on the device. The values of this tab are made available as raw data and are not further prepared. The data is therefore primarily for analysis by experts, for example by product support. In the box above the table, you can enter a search text that has the effect of a filter criterion for all columns of the table. Using the drop-down list, you can restrict the display to one of the protocols used to read out. If the value "All" is selected in the drop-down list and you enable the check box "Do not display value if not reachable via protocol", parameters whose values can no longer be read out via the relevant protocol are shown grayed out. If one of the protocols is selected in the drop-down list, values that can no longer be read out are hidden.

Table 4- 26 "User-def. OIDs" tab

Parameter group	Display, content
-	Table of MIB objects (see "Expert" tab) that are monitored as result of individual user settings.

Note

Display of the OID values

The correctness of the display of the OID depends on the correct selection of the data type in the profile setting.

Functions of the shortcut menu

The following functions are available in all tabs via the shortcut menu:

- Open WBM
- Reread data

  For more detailed information, refer to section Device window with device list (Page 77)
- Enable/disable automatic update
- Log on again for SIMATIC event / alarm messages (with active SIMATIC monitoring in SIMATIC tab)
- Display selected device in the (view-specific) topology (only available for devices monitored by the operation)

4.3.2.5 Device details - subcategories

Detailed information LAN ports

Operation

You can open the "LAN ports" window from the "LAN ports" tab of the device details as follows:

- Select the port and then click the 📁 icon
- Double-click on the appropriate row

Operator input

The following table explains the groups and contents of the box.

The values of the box groups "Data traffic", "Utilization" and "Error" are only monitored if port statistics is activated. All static values are delta values that are called every 5 minutes. The following symbols indicate the communication directions of the corresponding data values:

Table 4- 27 Communication directions

Icon	Communication direction
→	Send
←	Receive
↔	Half duplex (sending or receiving)

Table 4- 28 Detailed information for LAN ports

Group	Display, content
Basic data	• Name of the connection (detected) • Interface index (unique number of the port) • MAC address • Transmission medium (user-defined) • Transmission medium (detected) • Status (up or down) • Admin status • Max. bandwidth (Mbps) • Mode (full duplex or half duplex) • Description • Alias name
Topology	• Device connection (IP address, device name) • Port connection If a reference topology exists, the values in this section originate from the reference topology. If no reference topology exists, the values in this section originate from the discovered topology information.
Discovered topology	• Device connection (IP address, device name) • Port connection
Plastic Optical Fiber (POF)	• Signal delay (ns) • Calculated cable length (m), according to the calculation in STEP 7 • Power budget
Data traffic	• Transmit (transmission speed in Mbps) • Receive (receive speed in Mbps)
Utilization	Full duplex: • Transmit utilization (degree of utilization as a percentage) • Receive utilization (degree of utilization as a percentage)

Group	Display, content
	Half duplex: • HD utilization (combined degree of utilization as percentage)
Error	Full duplex: • Transmit error rate (error rate as a percentage) • Receive error rate (error rate as a percentage) • Number of send errors (number of bad outgoing packets) • Number of receive errors (number of bad incoming packets) • Number of discarded outgoing packets • Number of discarded incoming packets
	Half duplex: • HD error rate (combined error rate as percentage) • Number of errors (combined a number of bad packets) • Number of discarded packets (combined number of discarded packets)
Statistics	Time at which port statistics was enabled for the selected port.

Detailed information WLAN

Operation

You can open the window with the connection details for WLAN interfaces from the "WLAN" tab of the device details as follows:

- Select (highlight) the port and then click the icon
- Double-click on the appropriate row

Operator input

The following table explains the groups and contents of the box. All static values are delta values that are called every 5 minutes.

Table 4- 29 Detailed information WLAN

Group	Display, content
Basic data	• Name of the connection (detected) • Description • SNMP interface index (unique number of the connection) • Authentication type (e.g. WEP or WPA2-PSK) • SSID (names of the WLANs (wireless networks) assigned to the interface) • BSSID (ID numbers of the WLANs assigned to the interface) • WLAN protocol (wireless standard acc. to IEEE: e.g. 802.11n or 802.11g) • Channel (wireless channel of the interface) • Frequency (wireless frequency of the interface) • Max. data rate (Mbps) • Mode (full duplex or half duplex)
Status	• Status (Up/Down) • Signal strength (strength of the wireless signal in dBm) • Transmit data rate (Mbps) • Receive data rate (Mbps) • Transmit error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Receive error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Faulty, sent packets (in the last 5 minutes) • Faulty, received packets (in the last 5 minutes) • Number of clients (number of clients connected via this interface)

Group	Display, content
Clients	Table of all clients connected to the interface. Per client, the following information can be displayed: • Slot number (number of the connected interface) • Client name • Client IP (IP address of the connected client) • Client MAC (MAC address of the connected client) • Transmit data rate in Mbps • Receive data rate in Mbps • Transmit error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Receive error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Signal (signal strength of the existing connection in dBm) • Signal state (indicates whether the signal strength is OK, low or high)

Editor for detailed information on (W)LAN ports

Operation

You can call up the dialog for editing port information from the "LAN" and "WLAN" tab of the device details as follows:

Select (highlight) the port and then click the ✎ icon.

Operation / content

The following tables explain the contents of the box.

Table 4- 30 Basic data (only for LAN ports)

Parameter	Meaning
Connector type	Display of the connector type discovered by the operation
Connector type (user-defined)	Selection of the connector type

Table 4- 31 Port monitoring

Parameter	Meaning
Unmonitored port (only for LAN ports)	If this option is selected, the port is handled as follows: • Port connection states are not monitored • Events relating to port reference states are not displayed If this option is disabled, all reference connections of this port are deleted.
Docking port (only for LAN ports)	If this option is selected, the port is handled as follows: • Port connection states are not monitored • Events relating to port reference states are not displayed • If the check box "Learn connections of alternating devices automatically" is selected in the parameter group "PROFINET monitoring settings" on the control, connections of this port are learned. If this option is disabled, learned connections for this port and the corresponding reference connections of this port are deleted.

When a reference connection goes out from an interface, this cannot be configured as "Down".

Detailed information redundant ports

Operation

You can open the window with details for redundancy connections from the "Redundancy" tab of the device details as follows:

- Select the port and then click the ✎ icon
- Double-click on the appropriate row

Operator input

Depending on the redundancy method (protocol) being used, different information is displayed. With the help of PROFINET monitoring, only MRP redundancy information can be displayed. The following table shows the possible content with a brief explanation.

Table 4- 32 Detailed information for redundancy ports

Protocol	Group	Display, content
HRP	Basic data	• Port name (e.g. X5P1) • Role (what is the task (client, master) of the interface within the ring?) • Port status (information about what the interface does with IP packets . forward or block)
	Redundancy manager	• Ring state (OK, disrupted) • Ring state changes (number of status changes already made due to disruptions in the ring) • Measured trip delay (indicates in ms how quickly the status change is made)
MRP	Basic data	• Name of the port (e.g. X5P2) • Role (what is the task (client, master) of the interface within the ring?) • Port state (information about what the interface does with IP packets . forward or block. Is only displayed via SNMP) • Domain name
	Redundancy manager	• Ring state (OK, disrupted) • Ring state changes (number of status changes already made due to disruptions in the ring. Is only displayed via SNMP) • Measured trip delay (indicates in ms how quickly the status change is made. Is only displayed via SNMP) • Time ticks since (Is only displayed via SNMP) • Domain error (Is only displayed via SNMP)

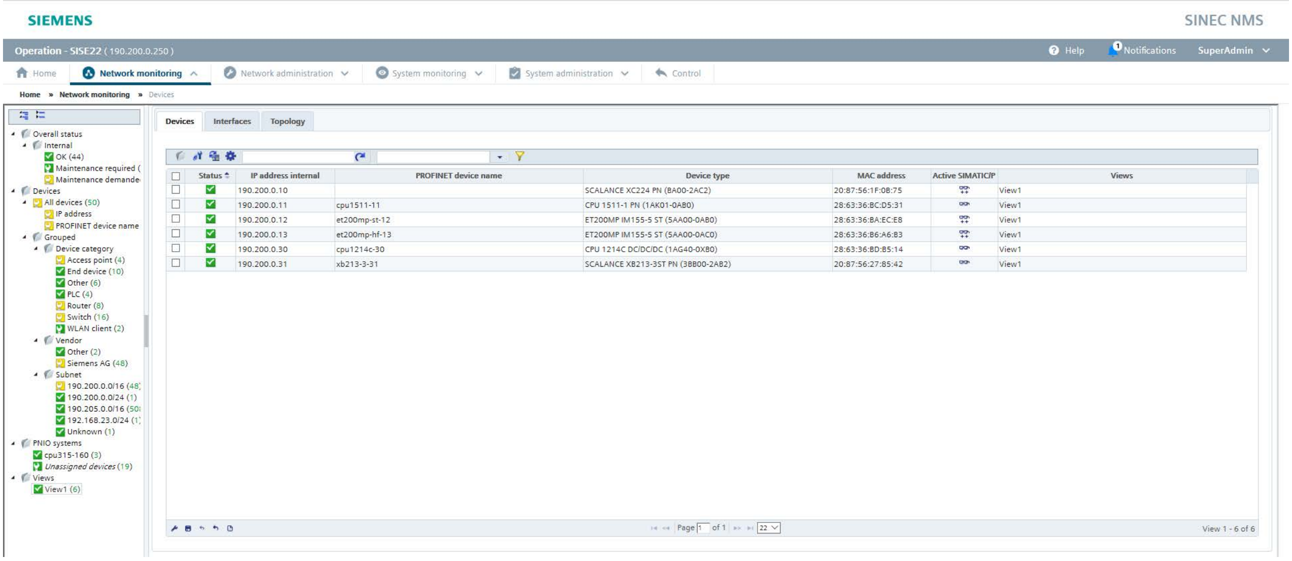
Protocol	Group	Display, content
STP or RSTP	Basic data	• Name of the port (e.g. X0P5) • Port type • Port STP state • Port status • Path costs (notional calculated costs for the current transport path of the IP packets). Path costs are used to calculate the most suitable transmission path.) • Priority • No .´Forward transmissions´ • Big network support • Passive Listening
Standby	Basic data	• Name of the port (e.g. X6P1) • Role (what is the task (master, master) of the interface on the "duplicate" connection?) • Port state (information about what the interface does with IP packets . forward or block) • Connection status (up, down) • Topology changes (number of topology changes already made due to disruptions on the connection) • Connection name (name of the standby connection. Required for identification since several may exist).

4.3.2.6 Views

Operation

You select a view by means of the desired entry below the "Views" node in the device tree.

The following figure shows the tabs "Devices", "Interfaces" and "Topology" available for views. The "Devices" and "Interfaces" tabs are always present, the "Topology" tab only if this was selected during the creation of the view.



- Overall status
  - Internal
    - OK (44)
    - Maintenance required (
    - Maintenance demande
- Devices
  - All devices (50)
    - IP address
    - PROFINET device name
  - Grouped
    - Device category
      - Access point (4)
      - End device (10)
      - Other (6)
      - PLC (4)
      - Router (8)
      - Switch (16)
      - WLAN client (2)
    - Vendor
      - Other (2)
      - Siemens AG (48)
    - Subnet
      - 190.200.0.0/16 (48
      - 190.200.0.0/24 (1)
      - 190.205.0.0/16 (50
      - 192.168.23.0/24 (1
      - Unknown (1)
- PNIO systems
  - cpu315-160 (3)
  - *Unassigned devices* (19)
- Views
  - View1 (6)

□	Status	IP address internal	PROFINET device name	Device type	MAC address	Active SIMATIC/P	Views
□	✓	190.200.0.10		SCALANCE XC224 PN (BA00-2AC2)	20:87:56:1F:0B:75		View1
□	✓	190.200.0.11	cpu1511-11	CPU 1511-1 PN (1AK01-0AB0)	28:63:36:BC:D5:31		View1
□	✓	190.200.0.12	et200mp-st-12	ET200MP IM155-5 ST (5AA00-0AB0)	28:63:36:BA:EC:E8		View1
□	✓	190.200.0.13	et200mp-hf-13	ET200MP IM155-5 ST (5AA00-0AC0)	28:63:36:B6:A6:B3		View1
□	✓	190.200.0.30	cpu1214c-30	CPU 1214C DC/DC/DC (1AG40-0XB0)	28:63:36:BD:B5:14		View1
□	✓	190.200.0.31	xb213-3-31	SCALANCE XB213-3ST PN (3BB00-2AB2)	20:87:56:27:85:42		View1

Figure 4-9 Views tab

"Devices" tab

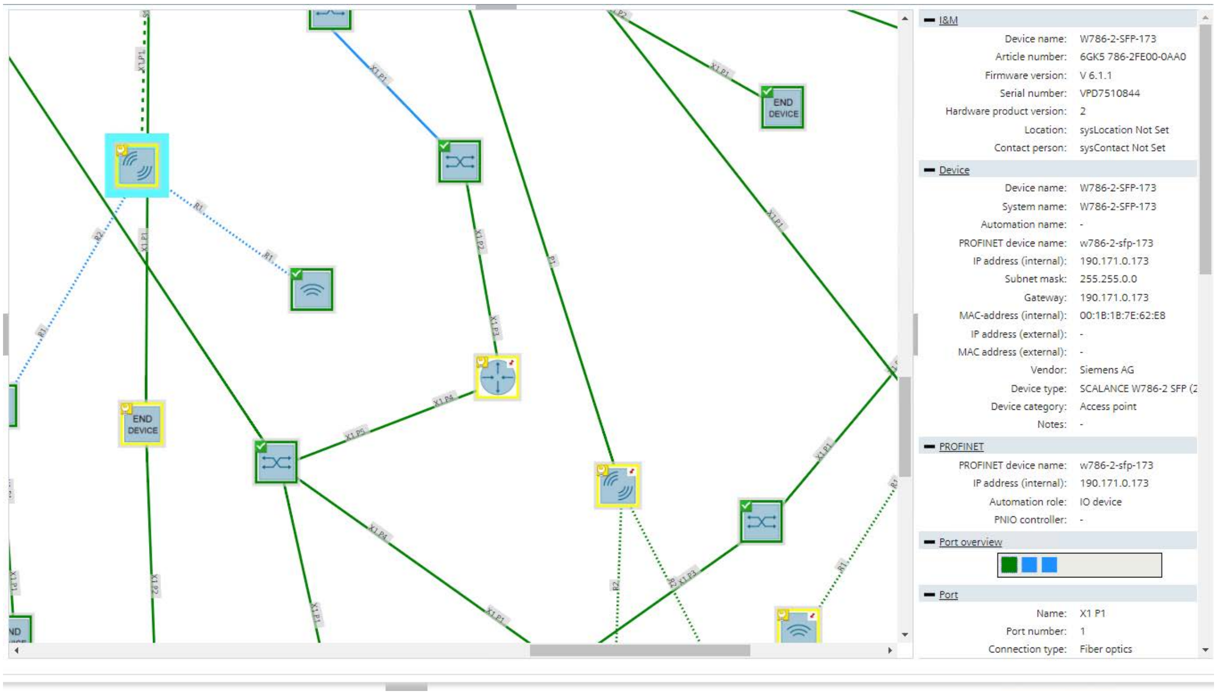
The "Devices" tab displays the devices that were assigned to the selected view with the View editor. As default, the device list of a view also includes the "Views" column. This column shows the views in which the device occurs.

"Interfaces" tab

The "Interfaces" tab displays information about the interfaces of devices that were assigned to the selected view with the View editor. There is no difference compared with the interface list that is not dependent on the view.

"Topology" tab

The following figure shows the layout and operator controls of the "Views" window, "Topology" tab in Online mode.



— I&M

Device name: W786-2-SFP-173
Article number: 6GK5 786-2FE00-0AA0
Firmware version: V 6.1.1
Serial number: VPD7510844
Hardware product version: 2
Location: sysLocation Not Set
Contact person: sysContact Not Set

— Device

Device name: W786-2-SFP-173
System name: W786-2-SFP-173
Automation name: -
PROFINET device name: w786-2-sfp-173
IP address (internal): 190.171.0.173
Subnet mask: 255.255.0.0
Gateway: 190.171.0.173
MAC-address (internal): 00:1B:1B:7E:62:E8
IP address (external): -
MAC address (external): -
Vendor: Siemens AG
Device type: SCALANCE W786-2 SFP (2
Device category: Access point
Notes: -

— PROFINET

PROFINET device name: w786-2-sfp-173
IP address (internal): 190.171.0.173
Automation role: IO device
PNIO controller: -

— Port overview

🟩 🟦 🟦

— Port

Name: X1 P1
Port number: 1
Connection type: Fiber optics

Figure 4-10 Topology of a view

To configure and display view-specific topologies a reference topology must already have been created and saved. Devices must be part of the reference topology to be able to be inserted in view-specific topologies.

Topology modes

Initially in the editing mode, the reference devices contained in the view, subviews and the unmanaged devices existing in the reference topology are contained in the left page area. They can be positioned in the topology display using drag-and-drop. Between monitored devices and unmanaged devices, the configured reference connections are shown. Between the inserted elements, you can draw in user-defined connections manually or adopt existing reference connections as user-defined connections. On user-defined connections with the shortcut menu bending points can be generated with which the course of user-defined connections can be adapted. For more information, refer to section "Operator input".

In Online mode, the elements inserted in Editing mode with their monitoring states for devices and ports and the user-defined connections drawn between them are displayed. Reference connections are not displayed in Online mode.

The colors of devices, ports and user-defined connections have largely the same meaning and formation rules as the colors of the non-specific view topology.
There are the following special features in the Editing mode of view-specific topologies:

- Reference connections are displayed in violet.
- User-defined connections are displayed in black.
- If both connection types apply, the connection color is shown in violet and black.

There are the following special features in the Online mode of view-specific topologies:

- For user-defined connections the connection color is decided by the fill color of the ports involved.
- Deviations between user-defined connections and discovered connections are not indicated in view-specific topologies.

Operator input

Operation is largely identical to the operation in the non-view-specific topology. Functions used for the configuration of the reference topology are not available in view-specific topologies. The reference states of ports can therefore not be configured. Below the operator input elements of the toolbar are explained in greater detail. For the differences to the non-view-specific topology, refer to the section Topology (Page 108).

Table 4- 33 Operator controls of view-specific topologies

Icon	Display / function	Icon	Display / function
	Topology settings The settings that are saved user-specific for the non-view-specific topologies are saved view-specific here.		Selection tool Bending points cannot be inserted for reference connections but for user-defined connectioons.
	Drawing tool With the drawing tool, user-defined connections can be drawn manually.		Showing reference connections The reference connections created in the non-view-specific topology are displayed.
	Adopt reference connections as user-defined connections Creates user-defined connections for all reference connections Individual reference connections can be adopted as user-defined connections with the shortcut menu or by double-clicking.		

4.3.2.7 Monitoring of NAT devices and NAT routers

SINEC NMS supports the monitoring of devices that can be reached via NAT routers. In addition to this, SINEC NMS shows NAT configurations of NAT routers. The term "NAT device" is used below for a device separated from an operation by a NAT router. For the discovery of NAT routers and NAT devices during the network scan, the check box "Discovery of NAT routers" must be selected in parameter profile "Discovery settings" on the control.

The monitoring of NAT devices and NAT routers by SINEC NMS is possible in the following network constellations.

Supported network constellations

An operation can be located in an external subnet and monitor devices of internal subnets that are connected to the external subnet via a NAT router. As an alternative, the operation can be separated from the external subnet by routers. In special applications (e.g. series machines) the individual internal subnets can be configured identically (same subnet mask and IP addresses).

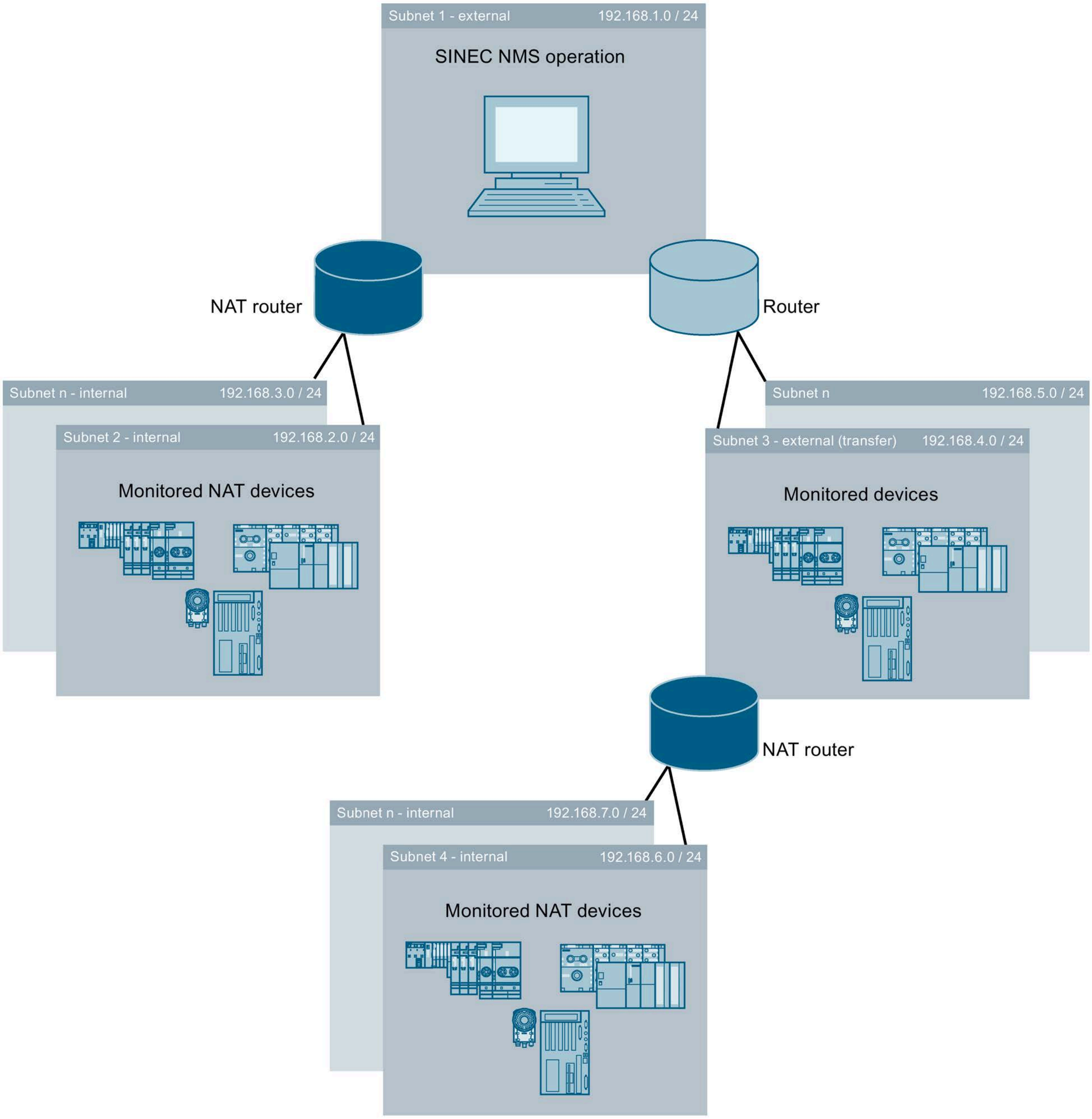


Figure 4-11 Supported network constellations

Even when the operation is located in one of the internal subnets, the devices of this subnet can be monitored. Devices can be recognized as NAT devices when the NAT router supports the NATv2-MIB (RFC7659). If the NAT router does not support this MIB, the devices are not recognized as NAT devices. The NAT procedures described below assume that operation access to the NAT devices is via the external subnet.

Supported NAT procedures

SINEC NMS can monitor NAT devices that can be reached via static NAT (1:1 NAT). For each NAT device to be monitored there must be a separate IP address configured in the external subnet on the NAT router to which the operation can send queries for monitoring the NAT device. The NAT router forwards the monitoring queries to the IP address of the NAT device in the corresponding internal subnet. 1:1 NAT rules configured for NAT routers are displayed in the device details of the operation in "NAT > Static NAT (1:1 NAT)".

NAT pools from which IP addresses are selected dynamically and used as new source IP addresses of IP packets are displayed in the device details of NAT routers in "NAT > Pooled NAT". After double-clicking on a NAT pool the NAT devices are displayed that use the particular NAT pool. NAT devices with dynamic address assignment cannot be monitored by SINEC NMS.

NAPT rules based on which a NAT router not only translates IP addresses but also TCP/UDP ports are shown in the device details in "NAT > NAPT". NAT devices that can be reached via NAPT rules cannot be monitored by SINEC NMS.

The NAT router configurations displayed in the "NAT" tab can contain IPv4 or IPv6 addresses.

Supported NAT routers

Table 4- 34 Supported NAT routers

NAT router	**SNMP is enabled for NAT devices**	**NAT device details "Identification of NAT device" are available (1:1 NAT)**	**NAT router configurations are available in device details**		
			Static NAT (1:1 NAT)	**Pooled NAT**	**NAPT**
NAT router supporting MIB NATv2 (RFC 7659), e.g. SCALANCE S615 V5.0 or higher, SCALANCE XM-400 / XR-500 V6.1 or higher	Yes	Yes	Yes	Yes	Yes
	No	As long as made available via NAT routers	Yes	Yes	Yes
SCALANCE S602 SCALANCE S612 SCALANCE S613 SCALANCE S623 SCALANCE S627-2M	Yes	Yes *	Yes	No	No
	No	As long as made available via NAT routers	Yes	No	No
NAT routers without support of the MIB NATv2 (RFC 7659) (no SCALANCE S)	Yes	Yes	No	No	No
	No	No	No	No	No

* If the operation is operated in the internal subnet, devices located in the same subnet are not displayed as NAT devices.

Access of NAT devices to the operation

It must be ensured in the configuration for the NAT devices that they can reach their associated operation. Otherwise, tasks such as firmware downloads cannot be executed.

4.3.2.8 Alternating devices

Meaning

An alternating device is a device that is deliberately not permanently connected to the network.

Alternating devices can, for example, be engineering PCs that are only connected for diagnostics. Alternating devices also occur when using tool changer devices. The PROFINET IO devices connected to tool changer devices are switched active or inactive as necessary. In both cases, alternating devices are only reachable temporarily for SINEC NMS.

Handling of alternating devices in SINEC NMS

If alternating devices cannot be reached by an operation, it is assumed that they have been deliberately deactivated or are not connected to the network. For this reason, the devices do not receive the overall status "Not reachable" but rather "Not connected". No reachability related events are displayed for devices in the "Not connected" status. As soon as the devices can be reached again, the overall device states and the reachability-related events are displayed normally again.

Devices can be recognized as alternating devices automatically if they support the "Fast startup" function and when the corresponding check box has been selected in the parameter group "PROFINET monitoring settings" on the control.

Devices can also be configured manually in the monitoring settings under "Network monitoring > Devices" as alternating devices, refer to the section Device window with device list (Page 77).

Connections from alternating devices to tool changer devices can be learned by SINEC NMS and displayed in addition to the current connections in topology displays. Learned connections remain displayed in SINEC NMS after they have been terminated.

Note

PROFINET IO devices configured as alternating

With PROFINET IO devices that are not reachable by an operation and that are monitored by controllers using the function "SIMATIC monitoring of assigned devices", the SIMATIC status reported by the corresponding controller decides the overall status of the device. If the controller reports the PROFINET IO device as being deactivated, the IO device has the overall status "Not connected". If the controller does not report the PROFINET IO device as being deactivated, the IO device has another overall status. This applies regardless of whether the PROFINET IO device is configured as alternating.

Note

Events pending for alternating devices

Events that were triggered for a device are still pending for this device even after it is configured as an alternating device and are not resolved automatically. Such events need to be resolved manually.

4.3.3 Topology

4.3.3.1 Overview

Operation

The monitored devices are displayed in a topology view on the "Network monitoring > Topology" page of an operation.

The topology display visualizes the arrangement and connection states of monitored devices based on information that SINEC NMS calls up from the devices via SNMP and PROFINET. The PROFINET device names of the devices may be required to generate the topology display and must therefore be unique. This also applies when the PROFINET monitoring is disabled in SINEC NMS.

Topology modes

Based on data obtained by an operation in the Editing mode, a reference topology can be configured in which the devices involved and target states for connections and ports can be set. Devices and connections that were defined as part of the reference topology are known below as reference devices and reference connections. Reference connections and states for ports can only be configured for reference devices.

In Online mode you can monitor the network taking into account the configured reference topology. For connections and ports of reference devices, deviations between discovered states and reference states are highlighted by SINEC NMS and communicated using corresponding events. These events can influence the overall status of the reference devices.

Display of devices and connections.

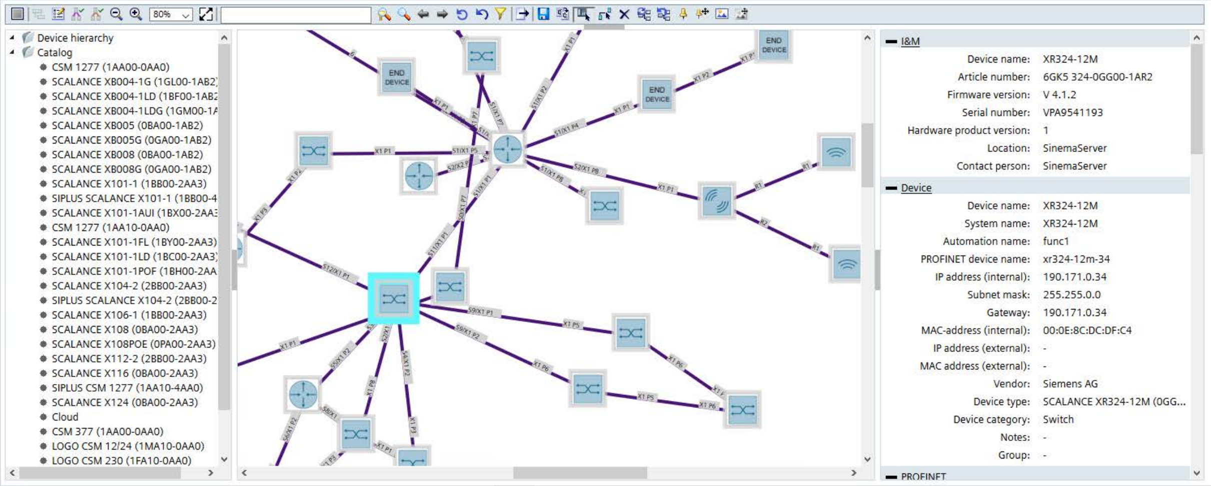
In both topology modes, SINEC NMS places discovered devices in the topology display and networks them together based on their discovered connections. SINEC NMS uses a form of display based on the equilibrium of forces between nodes and connections. The resulting device distribution can be changed in Editing mode. Each device is represented by a node with an associated device icon. In both topology modes devices that are not part of the reference topology are displayed with a star symbol, reference devices are displayed without a star symbol. In Online mode current connections that are not part of the reference topology are displayed with a star symbol.

Devices for which no connection information is discovered are displayed by SINEC NMS separately from the networked devices in the topology display. If a device without a detectable IP address is connected to three or more devices, the device without a detectable IP address is represented by a cloud symbol.

If devices are shown as overlapping in the topology, you can adjust the topology size in editing mode, see section Editing mode (Page 110).

Available work areas

The following figure illustrates the division of the work areas based on the Editing mode.



- Device hierarchy
- Catalog
  - CSM 1277 (1AA00-0AA0)
  - SCALANCE XB004-1G (1GL00-1AB2)
  - SCALANCE XB004-1LD (1BF00-1AB2
  - SCALANCE XB004-1LDG (1GM00-1A
  - SCALANCE XB005 (0BA00-1AB2)
  - SCALANCE XB005G (0GA00-1AB2)
  - SCALANCE XB008 (0BA00-1AB2)
  - SCALANCE XB008G (0GA00-1AB2)
  - SCALANCE X101-1 (1BB00-2AA3)
  - SIPLUS SCALANCE X101-1 (1BB00-4
  - SCALANCE X101-1AUI (1BX00-2AA3
  - CSM 1277 (1AA10-0AA0)
  - SCALANCE X101-1FL (1BY00-2AA3)
  - SCALANCE X101-1LD (1BC00-2AA3)
  - SCALANCE X101-1POF (1BH00-2AA
  - SCALANCE X104-2 (2BB00-2AA3)
  - SIPLUS SCALANCE X104-2 (2BB00-2
  - SCALANCE X106-1 (1BB00-2AA3)
  - SCALANCE X108 (0BA00-2AA3)
  - SCALANCE X108POE (0PA00-2AA3)
  - SCALANCE X112-2 (2BB00-2AA3)
  - SCALANCE X116 (0BA00-2AA3)
  - SIPLUS CSM 1277 (1AA10-4AA0)
  - SCALANCE X124 (0BA00-2AA3)
  - Cloud
  - CSM 377 (1AA00-0AA0)
  - LOGO CSM 12/24 (1MA10-0AA0)
  - LOGO CSM 230 (1FA10-0AA0)

I&M

Device name:	XR324-12M
Article number:	6GK5 324-0GG00-1AR2
Firmware version:	V 4.1.2
Serial number:	VPA9541193
Hardware product version:	1
Location:	SinemaServer
Contact person:	SinemaServer

Device

Device name:	XR324-12M
System name:	XR324-12M
Automation name:	func1
PROFINET device name:	xr324-12m-34
IP address (internal):	190.171.0.34
Subnet mask:	255.255.0.0
Gateway:	190.171.0.34
MAC-address (internal):	00:0E:8C:DC:DF:C4
IP address (external):	-
MAC address (external):	-
Vendor:	Siemens AG
Device type:	SCALANCE XR324-12M (0GG...
Device category:	Switch
Notes:	-
Group:	-

PROFINET

Figure 4-12 Editing mode of the topology display

In the Editing mode, the device hierarchy in the left side bar is initially empty, all detected devices are located in the topology display. If these devices are deleted from the topology display using the shortcut menu, they appear in the device hierarchy and can be dragged to the topology display again. In the Online mode, the device hierarchy displays all devices located in the topology display with their IP addresses, device names and overall states.

In the Editing mode, the left side bar contains a device catalog for adding unmanaged devices. Unmanaged devices that were added in parameter group "Unmanaged devices" on the control are available in this catalog. These are devices that cannot be monitored by SINEC NMS and that can be inserted to complete the topology display. Added unmanaged devices are displayed in the topology display of both topology modes.

After selection of a device in the topology display, the right-hand side bar shows the details of the device, ports as well as events pending for the device. In the Editing mode, the reference states for device ports can be configured in this detail area, refer to the section Editing mode (Page 110).
By double-clicking on a device in the topology display the device details of this device are called up.

The following sections describe the Editing and Online modes in detail.

4.3.3.2 Editing mode

Operator input

If no reference topology has yet been created and you have the right to edit the topology, the topology is displayed in the Editing mode after opening the page "Network monitoring > Topology" on an operation. The following sections explain how to work with the toolbar and port overview in this topology mode.

Toolbar

Table 4- 35 Operator controls in the Editing mode

Operator control	Function
■	Editing mode When you click on the operator control, SINEC NMS switches to the Online mode. If there are unsaved changes to the reference topology, you can save these in a dialog before the switchover.
⊟	Extended icon view As default the icon view is enabled in which the icon for the device type and the overall status of the device is displayed. In the extended icon view, in addition to this up to three device properties configurable in the topology settings are displayed.

Operator control	Function
📝	Topology settings • Display connections: Show/hide all connections When the check box for the connection display is disabled, the check box for displaying the port names is automatically disabled and cannot be enabled. • Display port names: In the topology display the names of the ports between which connections exist are displayed. With this option, you can show / hide these names. • Show synchronization connection between SIMATIC S7-400-H CPUs: An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system when this check box is selected. This line represents the two fiber optic (FO) cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. • Device icon style in topology: Specifies the style for the icons with which devices are shown in the topology display: – Device category: The devices are displayed with the icons of their associated device categories. Device categories can be set in the device profile editor. The assignment of icons to device categories cannot be adapted. – Device profile: The devices are displayed with icons that are assigned to the associated device types in their device profiles. If no matching icon exists for a device type, the default profile icon of the device profile is used. • Device labeling: Selection of up to three device properties that are displayed in the extended icon view for devices. • Size of the topology grid: Specifies the size of the cells of the topology grid in the Editing mode. Devices can only be moved along these grid cells. This setting does not change the existing position of devices. • Move surrounding devices When moving selected devices in the Editing mode, surrounding devices that are not fixed can also be moved automatically to maintain the device distribution. With this option you specify whether or not these surrounding devices are moved. – Do not move (Default setting): When moving selected devices, the surrounding devices are not moved. This option is recommended with large networks / topologies since there is no recalculation of the position and therefore the topology display is available more quickly. – During moving: When moving selected devices, the surrounding devices are moved to the suitable positions. – After moving After moving selected devices, the surrounding devices are moved to the suitable positions. Due to the recalculation of the position, the topology display is available after a delay. • Topology size: Specifies the clearances and the length of the connections between the devices in the Editing mode. A higher setting means greater clearances and longer device connections. The topology size should be selected according to existing number of devices. After changing the topology size, the device positions are recalculated. – Dynamic: SINEC NMS selects the topology size itself according to the existing number of devices. – Small: Up to 100 devices – Medium: 100 to 250 devices

Operator control	Function
	– Large: More than 250 devices – User-defined: You specify the topology size with a slider. By moving the slider to the right, you create greater distances between the devices, longer device connections and therefore fewer overlaps between the devices.
✓	Current connections are displayed Detected, active connections between devices are displayed. If the check box "Display connections" is disabled in the topology settings, this option cannot be enabled.
✓	Learned connections are displayed Learned connections between alternating devices and tool changer devices are displayed. If the check box "Display connections" is disabled in the topology settings, this option cannot be enabled.
⊖	Reduce topology view With each click the topology view is reduced by one zoom level.
⊕	Enlarge topology view With each click the topology view is enlarged by one zoom level.
100% ⌄	Select zoom level
⤢	Match zoom level to topology Select a zoom level that shows the entire topology without scrolling.
▭ 🔍 🔍	Device scan Searches for the entered text in the device properties of the devices in the topology display. To speed up the search, you can limit the search with the 🔍 icon to the device properties for which you want to search. You start the search with the 🔍 icon. Matching devices are displayed in a hit list and highlighted in the topology display. The device whose details are displayed in the right-hand side bar is highlighted in the topology display as well as in the hit list. To search for devices in IP address ranges, the following format must be kept to: IP address1 - IP address2 The spaces after and before the IP addresses are optional.
⇦ ⇨	Previous device / Next device If several devices were found in the device scan, the previous / next device can be selected with these operator input elements. The device details of this device are then shown in the right-hand side bar. Alternatively, the required device can be selected in the hit list of the device search.
↻	Reset device scan and scan results Deletes the input text of the device scan and deselects selected devices in the topology display.
↶	Undo last action Undo the last action in the topology.
▽	Topology filter Opens a dialog in which you can manage device groups. Monitored devices can be assigned to a device group. After selection of a device group in online mode, the associated devices are highlighted with a dark blue border. You can also manage device groups and assign devices to device groups with the device shortcut menu item "Assignment to device groups".

Operator control	Function
→	Export topology Exports the topology display as a *.PNG file ina *.ZIP archive. The set zoom level is always used. The topology display is always exported with a transparent background. The background color of the exported topology display depends on the display software used.
💾	Save Saves the configured reference topology and updates the topology display.
	Adopt detected statuses as reference statuses Adopts all the states discovered by SINEC NMS into the reference topology: • Detected devices are adopted as reference devices. The star symbols are removed from the devices. Individual devices can be adopted as reference devices using the shortcut menu. • Detected port states are adopted as reference states. The reference states of ports can be set manually in the port overview of the right-hand side bar, see section "Configuring reference states for ports". • Current / learned connections are adopted as reference connections. Partial connections are not adopted as reference connections. Individual reference connections can be adopted as reference connections with the shortcut menu or by double-clicking. The connected devices automatically become reference devices. If the connection to be adopted is a partial connection, the connection wizard is called in which you can specify the ports of the reference connection.
↖	Selection tool As default the selection tool is enabled. With the selection tool you can move devices along the configured topology grid by dragging them. As default after they have been moved devices are fixed in the topology display. When moving devices the device clearance is maintained, that is preset by the topology size configured in the topology settings. Using the shortcut menu of reference connections between fixed devices bending points can be inserted with which the course of the connections can be adapted. To do this drag the bending points to the required position. If a bending point is inserted on a reference connection between devices that are not fixed, the devices are fixed automatically. A maximum of 10 bending points per connection and 1000 bending points per topology can be created. With the shortcut menu command "Reset connection layout" the course of the connection is reset to the initial status. Individual bending points can also be deleted using the shortcut menu. If the fixing of a device is canceled, the bending points of the corresponding reference connection are deleted. Using a very large number of bending points slows down the topology display.

Operator control	Function
	Drawing tool With the drawing tool you can draw reference connections between reference devices manually. To do this, click on the devices to be connected one after the other to call the connection wizard to select the ports involved. By selecting them with the drawing tool devices automatically become reference devices. In the connection wizard, the ports of the devices to be connected are displayed with their detected and configured port states. Which of the ports are already connected is not displayed in the connection wizard but by the port names in the topology display. In the connection wizard click on the ports that are to be connected one after the other Per device one port can be selected, selected ports are highlighted in blue. If you draw a connection from an already connected port to another port of the same partner device, the connection is changed. Several connections of a port to different ports of the same device cannot be drawn. If you draw a connection from an already connected port to the port of a device to which there is not yet a connection, you can decide whether the existing connection is changed or whether an additional connection should be added. If the connection should be added, the port with more than one connection is automatically configured as a docking port. For ports already configured as docking ports in the case described the additional connection is generated as standard. Devices connected to docking ports are automatically configured as alternating devices. It is possible to draw link aggregations between devices. To do this the connection wizard must be used once per connection to be added. It is only possible to delete reference connections via the shortcut menu of the connections.
✕	Delete learned connections Deletes all learned devices from the reference topology. After deleting, the learned connections are also no longer visible in the Online mode. Individual learned connections can be deleted using the shortcut menu. If the check box "Learn connections of alternating devices automatically" is selected in the parameter group "PROFINET monitoring settings" on the control, the connections are learned again.
	Recalculate device positions Arranges all non fixed devices in the topology display with the aid of the distribution algorithm. This makes sense after adding devices step by step or after deleting devices from the topology display.
	Reset reference topology Resets the configuration of the reference topology: • All devices are removed from the reference topology and displayed with a star symbol. Individual reference devices can be removed from the reference topology using the shortcut menu. • All configured reference states for ports are reset. • All reference connections are removed. Individual reference connections can be removed using the shortcut menu.

Operator control	Function
📌	Fix selected devices As default, detected devices are not fixed. Non fixed devices are possibly repositioned automatically by moving other devices, by recalculating device positions and possibly by adding and removing devices. Fixed devices are not repositioned in these situations. Fixed devices are shown with a pin symbol. If this tool is used on devices that are already fixed, the fixing of these devices is canceled. Bending points on reference connections belonging to these devices are deleted. If there are both fixed and non fixed devices among the selected devices, using this tool fixes all devices. As an alternative the fixing can be set using the shortcut menu.
📌+	Fixing devices after moving them. As default this tool is enabled. After moving them, devices are fixed.
🖼	Insert background picture Inserts a background picture in the top left corner of the topology display. Maximum size: 50 MB Maximum resolution: 5000 x 5000 pixels An already inserted background picture can be deleted, updated and after activating the tool 🖼✥ moved with the shortcut menu.
🖼✥	Moving a background picture

Configuring reference states for ports

Reference states can only be configured for ports of reference devices. Using the shortcut menu of the ports, the following reference states can be configured in the "Port overview" area of the right-hand side bar:

- Up
- Down (cannot be selected if a reference connection exists)
- Unmonitored (only for LAN ports):
  - Port connection states are not monitored
  - Events relating to port reference states are not displayed
- Docking port (only for LAN ports):
  - Port connection states are not monitored
  - Events relating to port reference states are not displayed
  - If the check box "Learn connections of alternating devices automatically" is selected in the parameter group "PROFINET monitoring settings" on the control, connections of this port are learned.

Colors and icons

Ports

In the "Port overview" area of the right-hand side bar, the detected states and the configured reference states of the ports of the selected device are displayed. The detected states are indicated by the frame color, the reference states by the fill color of the ports. The table below shows the meaning of the possible port colors of reference devices.

Table 4- 36 Colors for port states in editing mode

Detected status	Configured reference status		
	Up	Down	Docking port / unmonitored port
Active	🟩	◼	□
Inactive	🟩	◼	□
Unknown	🟩	◼	□
Docking port / unmonitored port	🟩	◼	□

If the corresponding devices are not part of the reference topology, the fill color of the ports is white.

Connections

Current connections are shown in violet, learned connections in brown and reference connections in black. If several connection types apply, the relevant connection colors are shown as a combination. If the current and the learned connection type apply only the current connection is displayed.

So that current connections and learned connections are shown, the corresponding options in the toolbar must be selected. To display learned connections, the check box "Learn connections of alternating devices automatically" must also be enabled in the parameter group "PROFINET monitoring settings" on the Control.

Synchronization connections

An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system. This line represents the two fiber optic (FO) cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. In addition, the topology setting "Show synchronization connection between SIMATIC S7-400-H CPUs" must be enabled.

4.3.3.3 Online mode

Operator input

If a reference topology is already available, the topology is displayed in Online mode after opening the page "Network monitoring > Topology" on an operation. The majority of the operator input elements available in Online mode also exist in the Editing mode, see section Editing mode (Page 110). The operator input elements and shortcut menu commands for configuration of the reference topology are only available in the Editing mode. The following operator input elements are only available in the Online mode:

Table 4- 37 Operator controls in online mode

Operator control	Function
🟩	Online mode When you click on the operator control, SINEC NMS switches to the Editing mode.
Update interval (in topology settings)	In online mode, you can specify the interval at which the user interface of the topology is going to be updated. The following options are available: • Dynamic: For 250 devices or less, the update interval is 15 seconds. As of 251 devices, the update interval is 30 seconds. • 15 seconds • 30 seconds • 45 seconds • 60 seconds
▽	Topology filter Filter for highlighting devices and connections. The following filter categories are available: • VLAN: After selecting a VLAN ID, all associated devices and connections are highlighted in dark blue. You can only filter for one VLAN ID at a time. • Device groups: After selecting a device group, all devices that were assigned to the device group in editing mode are highlighted in dark blue and displayed in the right-hand side bar. The device groups to which a device is assigned can be seen with the shortcut menu command "Member in device groups" of this device as well as in the right-hand side bar.

Colors and icons

Devices

In the Online mode, the overall states of the devices are displayed with frame colors and state symbols. This applies regardless of whether or not the devices were added to the reference topology. The meaning of the icons fro the overall device status are described in section Device tree (Page 74).

Ports

In the "Port overview" area of the right-hand side bar for devices that were not added to the reference topology, only the detected states of the ports are displayed. The detected states determine the frame and fill colors of the ports. The same colors are used as for the detected states in the Editing mode, refer to section Colors and icons (Page 116).

For reference devices, the detected states and the states resulting from the detected states and the configured reference states are displayed. The detected states are symbolized by the frame color, the resulting states by the fill color of the ports. The table below shows the meaning of the possible port colors of reference devices:

Table 4- 38 Colors for port states in online mode

Detected port status	**Reference port status**	**Resulting port status**		**Border color / fill color**
Active	Active	Active		🟩
Active	Inactive	Active - Maintenance required		🟨
Active	Docking port / unmonitored port	Docking port / unmonitored port		□
Inactive	Active	Inactive - Maintenance required	With current connection	🟥
			Without current connection	🟥
Inactive	Docking port / unmonitored port	Docking port / unmonitored port	With current connection	□
			Without current connection	□
Inactive	Inactive	Inactive	With current connection	■
			Without current connection	■
Unknown	-	-		▨
Docking port / unmonitored port	All reference port states	Docking port / unmonitored port		□

The table below shows the meaning of the colors of redundant ports for devices that were not added to the reference topology:

Table 4- 39 Colors for states of redundancy ports in online mode (devices not in reference topology)

Current connection exists	Detected port status	Redundancy status	Port color
Yes	Active	Disabled	🟩
		Blocking / discarding	🟦
		Forwarding, listening, learning, unknown	🟩
		Not connected / broken	🟨
		Warning	🟨
Yes	Not active (can be a temporary status until the connection was calculated)	Disabled / broken / discarding	⬜
		Blocking	🟨
		Forwarding, listening, learning, unknown	🟨
		Not connected	🟨
		Warning	🟨
No	Active (can be a temporary status until the connection was calculated)	Disabled	🟩
		Blocking / discarding	🟦
		Forwarding, listening, learning, unknown	🟩
		Not connected / broken	🟨
		Warning	🟨
No	Inactive	Disabled / broken / discarding	⬜
		Blocking	🟨
		Forwarding, listening, learning, unknown	🟨
		Not connected	🟨
		Warning	🟨

The table below shows the meaning of the colors of redundant ports for devices that were added to the reference topology:

Table 4- 40 Colors for states of redundancy ports in online mode (devices in reference topology)

Resulting port status	Redundancy status	Border color / fill color
Active	Disabled	🟩
	Blocking / discarding	🟦
	Forwarding, listening, learning, unknown	🟩
	Not connected / broken	🟨
	Warning	🟨
Active - Maintenance required	Disabled	🟨
	Blocking / discarding	🟨
	Forwarding, listening, learning, unknown	🟨
	Not connected	🟨
	Warning	🟨
Inactive	Disabled / broken / discarding	⬛
	Blocking	🟨
	Forwarding, listening, learning, unknown	🟨
	Not connected	🟨
	Warning	🟨
Inactive - Maintenance required	Disabled	🟥
	Blocking / discarded	🟥
	Forwarding, listening, learning, unknown	🟥
	Not connected	🟥
	Warning	🟥

Connections

Connection colors

The connection lines in the Online mode correspond in terms of the connected ports to the connection lines in the Editing mode. Current connections that were not defined as reference connections, are shown with the star symbol. If a reference connection between two ports does not correspond to the current connection or one of the learned connections, the connection color is red regardless of the fill colors of the ports. Otherwise the connection color is based on the fill color of the two connected ports. Which of the port colors decides the color of the connection line depends on the priority of the port color:

- Red (highest priority)
- Yellow
- Blue
- Green
- Gray
- White (lowest priority)

With unmonitored ports / docking ports, the connection color is defined by the status of the partner port.

Learned connections that are not active at the time of the display between tool changer devices and alternating devices are displayed as follows regardless of the color of the connected port.

- Learned connection was not adopted as reference connection: Brown
- Learned connection was adopted as reference connection: Gray

Learned active connections are displayed in green.

Table 4- 41 Connection colors of WLAN connections

Reference connection active	Connection color
No	Light gray
Yes	The color of an active reference connection is based on the port color (green, red or light gray). Light gray: The user has specified in the reference that a connection can exist. Green: Connection discovered as active by SINEC NMS. Red: One of the interfaces belonging to the connection is down.

A reference connection is treated as an active connection if one of the reference connections corresponds to the actual WLAN connection. The color of the active connection is based on the color of both ports. Yellow and dark gray are used to indicate an invalid port status if a reference connection is defined. All other reference connections between a client and several APs that are down are shown in gray. Which of the port colors decides the color of the active connection between client and AP depends on the priority of the port color:

- Red (highest priority)
- Green
- Gray (lowest priority)

Connection types

Electrical connections, optical connections, wireless connections and unknown connections are shown in the Online mode view as follows:

Table 4- 42 Display of connection types

Connection type	Description
- - - · - · - · - - - - - - -	Wireless connection
— — — — — — — —	Optical connection
————————	Electrical connection
————————	Unknown connection
- - - - · - - - - · - - - -	Synchronization connection between SIMATIC S7-400-H CPUs, see the section "Synchronization connections" below.

The types of the connected ports decide the type of connection displayed. Which of the port types decides the type of connection depends on the priority of the port type:

- Electrical (highest priority)
- Optical
- Wireless
- Unknown (lowest priority)

Synchronization connections

An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system. This line represents the two fiber optic (FO) cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. In addition, the topology setting "Show synchronization connection between SIMATIC S7-400-H CPUs" must be enabled.

4.3.3.4 Special features

Partial connections

A partial connection is a connection in which the connection port of at least one device is unknown. The following types of partial connections must 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 adopted immediately as reference connections. First the ports involved must be selected in the connection wizard.

In Online mode, the color of an expanded reference connection is formed by comparing it with the discovered connection information. For partial connections of type A, the connection color is decided by the fill color of the port if the connection information matches up:

Table 4- 43 Representation of partial connections

Connection type	Match with the discovered connection	Fill color of the port	Connection color
A	Yes	Green	Green
A	Yes	Not green	Fill color of the port
A	No	Every fill color	Red
B	Yes	-	Gray
B	No	-	Red

High availability (HA) PROFINET IO devices

The PROFINET interface modules of an HA device are shown in the topology as device pair if the interface modules were not fixed manually to different positions. To detect HA devices, PROFINET monitoring must be activated for them.

4.3.4 Reports

Operation

SINEC NMS offers a series of reports for network monitoring and analysis on the pages under "Network monitoring > Reports" of an operation. 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

With the report types "Availability", "Performance", "Inventory" and "Events", you can select which data should be evaluated how based on the form, content and time period. The reports can be used to display statistical data in tables or graphic diagrams. Depending on the selected report type analog and digital graphs (pulse line) are displayed. You can create a preview of a report and print it out. The pages with the generated reports contain information in various boxes displayed in the table view. Optionally, this information is also shown as a pie chart or bar chart. Depending on the filter criteria the appropriate boxes are displayed with report information. The following information in the section, relates to the Web pages of the four report types mentioned.

For information on validation reports, refer to the section Validation reports (Page 133)

Note

Do not shut down SINEC NMS while executing reports.

SINEC NMS must not be shut down during report execution. If SINEC NMS is shut down while reports are being executed, they will not be executed or will not be executed completely.

Operator input

The following table shows the functional elements of the header in the tabs for reports.

The reports contain a selection of the following function elements:

Table 4- 44 Operator controls for reports

Icon	Display / function	Icon	Display / function
●	Show/hide graphic	▦	Show/hide table
24 hour	Evaluation time period: 24 hours	7 day	Evaluation time period: 7 days
() ▣ ↻	Enter text to filter based on data records. The entered text is searched for in all columns. In the text box, text is displayed when a simple query entered in the Filter Template Editor is active. The ▣ icon is displayed when a filter template with prefilter settings is active. The () icon is displayed when a filter template with a complex query is active.	▾	Selection of a previously created template for filtering according to data records. After selection, the properties of the filter template are applied to the report. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
▽ ▽✓	Open the editor for configuring filter settings that can be stored in filter templates. The ▽✓ icon is displayed when the configured filter settings differ from the default filter settings. You will find further information in the sections on the individual report types.		

Note

Validity of the filter settings

The filter settings made on these pages remain valid until you log out from the application. If you change the filter settings, these also remain valid if you change back and forth between Web pages.

Printing reports

When you select the report function, the function element for the print function appears in the status bar. 🖶

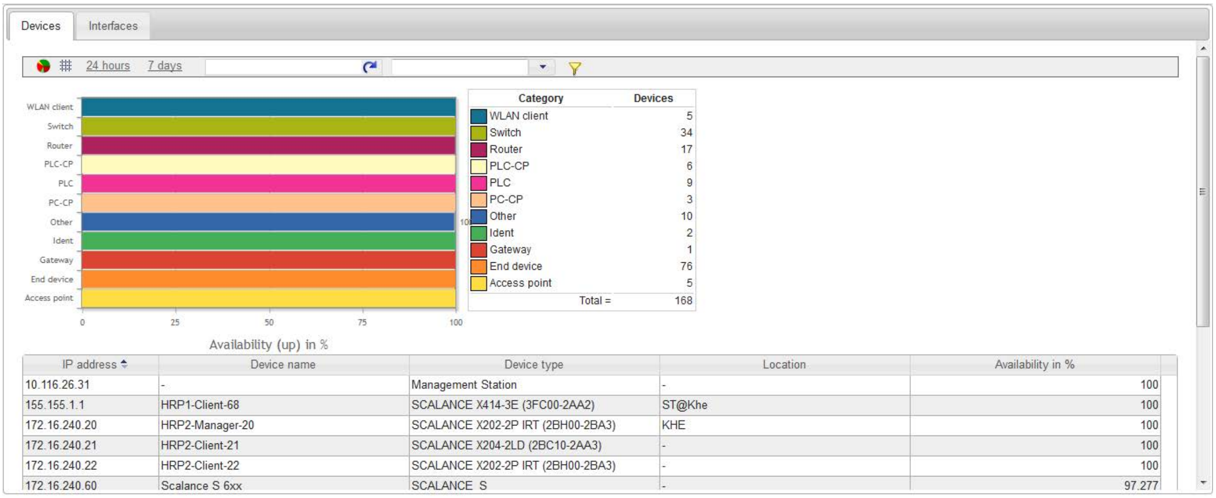
SINEC NMS outputs the content of the currently displayed report Web page in a new Web page. There, you can select further output methods with the functions available in your Web browser, for example, output to printer or to a PDF file.

Archive management

Historical data for creating reports is stored in the system database. The Operation Monitor provides a function with which you can delete, swap out or import historical data.

4.3.4.1 Availability

The report types described below can be accessed via the page "Network monitoring > Reports > Availability".



Category	Devices
WLAN client	5
Switch	34
Router	17
PLC-CP	6
PLC	9
PC-CP	3
Other	10
Ident	2
Gateway	1
End device	76
Access point	5
Total =	168

IP address	Device name	Device type	Location	Availability in %
10.116.26.31	-	Management Station	-	100
155.155.1.1	HRP1-Client-68	SCALANCE X414-3E (3FC00-2AA2)	ST@Khe	100
172.16.240.20	HRP2-Manager-20	SCALANCE X202-2P IRT (2BH00-2BA3)	KHE	100
172.16.240.21	HRP2-Client-21	SCALANCE X204-2LD (2BC10-2AA3)	-	100
172.16.240.22	HRP2-Client-22	SCALANCE X202-2P IRT (2BH00-2BA3)	-	100
172.16.240.60	Scalance S 6xx	SCALANCE S	-	97.277

Figure 4-13 Availability report

Meaning

Display of all (filtered) objects with information relating to their availability; in other words, how long they were reachable during the monitoring period. In addition to the table display, a graphic is also generated in which the monitored objects are evaluated again in groups.

"Devices" tab

The display is limited to complete devices regardless of their individual ports. The grouping in the graphic is according to device groups (routers, switches, access points etc.).

"Interfaces" tab

In this tab, the operating time of monitored interfaces is shown as a percentage. The interfaces are shown grouped according to the transmission media. When calculating the percentages for the operating time the interfaces potentially available for a device are used as the maximum value.

If a user-defined name was assigned for an interface, this is shown in the default "Name" column instead of the discovered name.

Operation / content

Although the column assignment in the data area is preset, you can arrange it any way you require (🔧 in the footer). Except for the "constant" information as it appears in the Device details, for example, you can also select the following statistical values:

- Availability (percentage)
- Number of outages
- Total uptime (period absolute)
- Total inactive (period absolute)
- Last discovered
- Initial discovery
- Average downtime (period absolute)
- Average uptime (period absolute)
- Unmonitored period (period absolute)
- Not monitored (percentage)
- Device deleted (information, whether and when deleted)

Calculations for the availability report

The availability report provides report data relating to the availability of devices in the network. To be able to calculate this information about device availability, the total operating time or the total downtime of a device must be known. The calculation of the availability report is based on the average operating time and the average downtime of devices and interfaces.

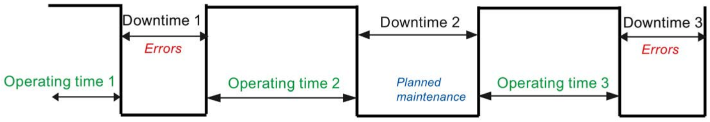


Figure 4-14 Calculations for availability report

Average operating time = total operating time / total downtimes

Total operating time = operating time 1 + operating time 2 + operating time 3 + …

Average downtime = total downtime / total failures

Total downtime = downtime 1 + downtime 2 + downtime 3 + …

The downtime can be caused by failures or planned downtimes.

% availability = average operating time * 100 / (average operating time + average downtime)

Prefilter for reports on availability

Reports on availability can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for availability reports. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

Table 4- 45 Filters for availability reports in the "Devices" tab

Operator control	Filter options
Device	Filtering according to existing or deleted devices.
Period	Filter according to data records of the last 7 days / 24 hours / period entered manually.

Table 4- 46 Filters for availability reports in the "Interfaces" tab

Operator control	Filter options
From IP To IP	Filter according to data records that have the specified IP addresses.
Device name, device type and device category	Filter according to data records for interfaces that belong to devices with the specified device name, the device type or the device category.
Statistics activated	Filter according data records for interfaces for which the port statistics are activated /deactivated: • All • Yes: Interfaces with activated port statistics • No: Interfaces with deactivated port statistics
Device	Filtering according interfaces belonging to existing or deleted devices.
Port status	Filter according to interfaces with an active connection status: • All • Only interfaces with an active connection status
Period	Filter according to data records of the last 7 days / 24 hours / period entered manually.

4.3.4.2 Performance

The report types described below can be accessed via the page "Network monitoring > Reports > Performance".

Structure and meaning

Display of the performance of monitored interfaces; in other words, how fast and reliably they have transferred and received data during the monitoring period. To display the reports the statistics for the interfaces must have been enabled in the "LAN" tab of the device details.

- LAN - Interface utilization:
  For all LAN interfaces, not only the maximum possible speed but also their total load when sending and receiving is displayed.
- LAN - Interface quality:
  The error quota when sending and receiving is displayed for all LAN interfaces.
- WLAN - Interface quality:
  The error quota when sending and receiving is displayed for all WLAN interfaces.
- WLAN - Interface data rate (transmission speed):
  For all WLAN interfaces, the bandwidth (data rate) when sending and receiving is displayed.
- WLAN - Signal strength:
  For all WLAN interfaces, the average signal strength is displayed.
- WLAN - Number of clients:
  For all access points, the number of WLAN clients to which they were connected on average is displayed.
- Discarded packets:

  The number of discarded incoming packets and the number of discarded outgoing packets is displayed for all LAN and WLAN interfaces.
- POF power budget:

  For LAN interfaces of the type "Plastic Optical Fiber (POF)", information about the power budget is displayed.

Operation / content

Although the column assignment in the data area is preset, you can arrange it any way you require (🔧 in the footer). Except for the "constant" information as it appears in the Device details, for example, you can also select the following statistical values:

- Average transmission performance (%)
- Average reception performance (%)
- Average performance (%)
- Maximum transmission performance (%)
- Maximum reception performance (%)
- Maximum performance (%)
- Average error rate (%)
- Maximum error rate (%)
- Average transmission error rate (%)
- Average reception error rate (%)
- Maximum transmission error rate (%)
- Average POF power budget
- Maximum reception error rate (%)
- Average transmit data rate (Mbps)
- Current transmission data rate (Mbps)
- Maximum transmission data rate (Mbps)
- Average signal strength (dBm)
- Maximum signal strength (dBm)
- Average client number
- Maximum client number
- Mode (WLAN default)
- Used channel
- Information if and when deleted
- Maximum POF power budget

Special feature

If the "Historical data" box is also displayed, you can use the shortcut menu of this icon to generate a further diagram in which the data that has already been recorded can be further analyzed.

Prefilter for reports on performance

Reports on performance can be filtered with the aid of filter templates. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

The meaning of the settings of the prefilter for reports on performance can be found in the section Availability (Page 125).

4.3.4.3 Inventory

The report types described below can be accessed via the page "Network monitoring > Reports > Inventory".

Layout

The Web page "Network monitoring > Reports > Inventory" has the tabs "Manufacturer", "IP address range", "Device category" and "PROFINET".

meaning / content

Inventory reports contain information relating to the vendor, IP range and device category for all the devices discovered in the network during the selected period.

Although the column assignment in the data area is preset, you can arrange it any way you require (🔧 in the footer). The following can be selected:

- IP address
- Device name
- Device type
- Location
- Name of the IP address range
- Number of interfaces (used / total)
- PROFINET device name
- MAC address
- Firmware version
- Article number
- Historical data

In the "PROFINET" tab, the following additional columns can be selected:

- PNIO name
- Device category
- PNIO role
- Subnet mask
- Router address
- Assigned PLC

Prefilter for reports on the inventory

Reports on the inventory can be filtered with the aid of filter templates. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

In the prefilter of reports on the inventory, you can filter according to monitored or unmonitored devices.

4.3.4.4 Events

The report types described below can be accessed via the page "Network monitoring > Reports > Events".

Layout

The Web page "Network monitoring > Reports > Events" has the tabs "Network events" and "System events".

Meaning

Display of all the events that have occurred (filtered) with information relating to the status, event type and the time it occurred. In addition to the table, a graphic is also generated in which the monitored events are regrouped (error, warning etc.).

Predefined report forms (tabs):

- Network events:

  All network events are displayed; in other words, messages generated by the network devices.
- System events:

  All system events are displayed; i.e. messages generated by SINEC NMS.

Prefilter for reports on events

Reports on events can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for events. For basic information on filter templates and the possibilities of complex filters, refer to section Filter templates (Page 71).

Table 4- 47 Filtering reports on events

Control element	Filter options
Basic filter settings	Read: • Yes • No • All Event state: • All • " - " • Resolved automatically • Resolved manually • Pending Period: Filter according to events • of the last 24 hours • of the last 7 days • of the next month • of a manually entered time range From device: Filter according to deleted or existing devices
Event classes	Filter according to the severity of events: • Notification • Information • Warning • Error
Protocols	Filter according to protocols by which the events were triggered: • ICMP • DCP • ARP • SNMP • SNMP trap • PROFINET • SIMATIC • Multiple (event was triggered by more than one protocol) • SIMATIC event messages • SIMATIC alarm messages

4.3.4.5 Validation reports

Overview

Function of validation reports

A validation report is the result of a configurable collection of validation is with which monitoring data of different categories can be checked based on configurable criteria. The priority can be defined for every selected validation. With the priority, you specify whether or not the result of a validation is relevant to the overall result of the validation report.

Parts of validation reports

A validation report is created in the form of a PDF file and validation report attachments and can be downloaded in the ZIP format from SINEC NMS.

The PDF file contains the overall result of the validation report, a validation overview and if applicable the results of validations that were not passed. The overall result indicates whether the validation is of the validation report were passed in total. This is the case when all validations with the validation priority "Obligatory" were passed. The validation overview indicates which validations were performed, whether these were passed, for how many devices, ports or events the relevant validation was performed and how many did not meet the criteria of this validation. In the results of validations that were not passed the data is highlighted in red due to which the relevant validation did not pass.

The validation report attachments contain all data in the .XLSX format that were used to obtain the results of the validations performed.

Required rights

Configuration of validation reports requires the "monitoring advanced" "Monitoring Access Level".

Validation report configurations

Layout of the Web page

After the Web page "Network monitoring > Reports > Validation reports" is reported, the "Validation report configurations" tab shows all configurations of validation reports stored on the operation with their status information, properties and file sizes. With the operator controls of the header, validation report configurations can be managed and the corresponding validation reports downloaded.

Operator input

The following table explains the operator controls of the header of the tab.

Table 4- 48 Operator controls for validation report configurations

Operator control	Function
✳	Adding a new validation report configuration The dialog for validation report configurations is opened, refer to the section Configuration of validation reports and validation report templates (Page 135). With the configurations of validation reports, and validation report templates, the same validations an be selected and configured.
⧉	Copying a selected validation report configuration The selected validation report configuration is copied and the configuration dialog for the new object is opened. The settings of the copied object are adopted and can be adapted.
✎	Editing a selected validation report configuration The dialog for validation report configurations is opened, refer to the section Configuration of validation reports and validation report templates (Page 135).
✕	Deleting a selected validation report configuration The selected validation report configurations are deleted. By deleting validation report configurations. the corresponding validation reports are also deleted. Validation reports with the status "In progress" cannot be deleted.
🗎	Displaying a selected validation report configuration The dialog for configuration of the validation report opens. No changes can be made.
🖶	Displaying the PDF file The PDF file for the validation report created for the selected validation report configuration is displayed in a new tab of the Web browser. Displaying PDF files is only possible for validation reports in the status "Finished". A suitable PDF reader is required to display PDF files.
⬇	Downloading validation report The validation report for the selected validation report configuration is downloaded including the validation report attachments in ZIP format. Multiple selection is possible. Downloading validation reports files is only possible for validation reports in the status "Finished". The text box "Size of the selected validation reports (MB)" shows the file size of the validation reports of all selected validation report configurations.
↷	Searches the list of validation report configurations for the entered text.

Validation report templates

Layout of the Web page

To simplify the creation of validation report configurations, in the "Validation report templates" tab, you can create templates that can be used and adapted when creating validation report configurations.

Operator input

The following table explains the operator controls of the header of the tab.

Table 4- 49 Operator controls for validation report templates

Operator control	Function
✳	Adding a validation report template The dialog for validation report templates is opened, refer to the section Configuration of validation reports and validation report templates (Page 135). With the configurations of validation reports, and validation report templates, the same validations an be selected and configured.
⧉	Copying a selected validation template configuration The selected validation report template is copied and the configuration dialog for the new object is opened. The settings of the copied object are adopted and can be adapted.
✏	Editing a selected validation template configuration The dialog for validation report templates is opened, refer to the section Configuration of validation reports and validation report templates (Page 135).
✕	Deleting selected validation template templates The selected validation report templates are deleted.
▭ ↷	Searches the list of validation report templates for the entered text.

Configuration of validation reports and validation report templates

Overview

Overview

Via the buttons for creating, editing or copying validation report configurations and validation report templates you reach the dialog in which the validation is to be made can be configured. The available validations are assigned to categories whose content you can hide and display using the PLUS and Minus sysmbols. The categories and the validations they contain are displayed in an overview tree in the left area of the configuration dialog. By selecting an entry in this tree, you come directly to the relevant position of the configuration dialog. Before a validation can be configured, the corresponding check box must be enabled. After enabling a validation, its priority can be specified by clicking the symbol in front of the check box. The symbols have the following meaning:

Table 4- 50 Validation priorities

Icon	Meaning
⚠	Validation priority "Obligatory" A validation with this priority relevant for the overall result. The validation must be passed so that the overall result "Passed" can be reached.
ℹ	Validation priority "Optional" A validation with this priority is not relevant for the overall result. Validation reports that only contain validations with this validation priority always have the overall result "Passed".

Configuration settings

For validation report configurations, you can select a validation report template in the "Configuration settings" area. For the template settings to be adopted, you need to click the "Use validation report template" button after selecting a validation report template.

Before saving a validation report template, you need to specify its name in the "Configuration settings" area.

Basic settings

In the basic settings of the configuration dialog, you can enter information about the company and the plant to which the data to be evaluated by the validation report is assigned. You can also specify the degree of trustworthiness of the validation report. The specified information appears in the PDF file generated for the validation report. For validation report configurations, the name of the validation report to be generated must be specified in the basic settings. The PDF file generated for the validation report configuration is given this name.

Generate picture of topology

In this area, you can specify whether SINEC NMS should generate a picture in PNG format from the topology display and include this in the validation report attachment. The picture is generated in the Online mode. You can choose whether the picture is generated from the icon view of the extended icon view.

The following sections explain the configurable validations. The table column "Description of the validation" always names the scenario in which a validation fails.

After configuring a validation report, its creation can be started with the "Generate validation report" button. As an alternative, the settings made can be saved as a validation report configuration or as a validation report template.

Device properties

The following validations can be configured in the "Device properties" category:

Table 4- 51 "Device properties" validations

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
White list for firmware versions	For all monitored devices a check is made whether their firmware versions differ from those of the white list. If the device type and the article number of a monitored device exist in the white list, the firmware version specified in the white list for the article number is used for the validation. If monitored devices do not exist among the devices of the white list, the validation fails.	The white list can be created manually or by importing a CSV file. The expected format of CSV files is described in the section below this table. Devices can be specified with their device type or their article number. If more than one firmware version is specified for a device these must be separated by a comma. For the validation, the firmware versions detected from the specified firmware versions are used. If the check box "Ignore devices without a firmware version" is selected, monitored devices without a firmware version detectable by SINEC NMS have no influence on the result of the validation.	The monitored devices whose firmware versions differ from the white list are listed based on their device information. Their detected firmware versions are highlighted in red.
Different firmware versions	For all monitored devices a check is made whether devices with the same device profile or of the same device type have different firmware versions.	You can select whether the validation is performed for devices with the same device profile or devices of the same device type. If the check box "Ignore devices without a firmware version" is selected, monitored devices without a firmware version detectable by SINEC NMS have no influence on the result of the validation. If the "Ignore standard profiles" check box is selected, the validation for standard profiles or the device types they contain is not performed.	The following data is specified per device profile or device type: • Number of different detected firmware versions. • Listing of these detected firmware versions • Number of devices involved
IP address parameters	A check is made whether there are currently monitored devices whose IP addresses, subnet masks and gateways do not match the information specified for the validation.	IP address ranges with the relevant subnet mask and gateway can be specified. Per row, an IP address and a subnet mask must be specified. If no gateway is specified, no validation is made. If a gateway is specified, this gateway must match the devices belonging to it. As an alternative to manual specification of the IP address ranges, the IP address ranges configured in "Administration > Discovery > Scan" can be used. In this case, the subnet masks for the relevant IP address ranges must be added manually.	The monitored devices whose IP address parameters do not match the information specified for the validation, are listed based on their device information. The deviating parameters are highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Device names	A check is made whether there are currently monitored devices whose PROFINET device names and/or system names do not match at least one of the name patterns specified for the validation.	The name pattern of the required PROFINET device names and system names can be specified in the form of regular expressions. The information specified for the validation is not case sensitive. For PROFINET device names and system names, a maximum of 10 regular expressions can be specified. It is possible to specify whether the PROFINET device name or the system name of a device needs to match the regular expressions or whether there must be a match with the PROFINET device name and system name. The following regular expressions have no effect on the validation: • \g • \k • \l • \p	The monitored devices whose PROFINET device names and/or system names do not match the regular expressions specified for the validation are listed based on their device information. The deviating names are highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate IP addresses	A check is made whether there are duplicate IP addresses in the network. The detection of duplicate IP addresses is possible only if the following requirements are met: • The check box "Detection of duplicate IP addresses" is selected on the control under "System administration > Operation parameter profiles" in the parameter group "Discovery settings". • The component "Win10Pcap" was installed during installation of SINEC NMS. • To detect duplicate IP addresses of NAT devices, the operation must be located in the same subnet as the NAT devices (internal subnet). Only the internal IP addresses of the devices are taken into account.	No configuration is necessary. A search is made for duplicate IP addresses starting with all network adapters of the operation.	The devices whose IP addresses occur more than once are listed based on their device information. IP addresses are highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate MAC addresses	A check is made whether there are duplicate MAC addresses in the network. Detection of duplicate MAC addresses for NAT devices: • The operation is located in the external subnet: In each case, the external and the internal MAC addresses of the NAT devices are compared with each other. If one of the two MAC addresses for a NAT device does not exist, no comparison is made for this NAT device. The comparison only takes place between NAT devices. • The operation is located in the internal subnet: The internal MAC addresses of all devices are compared with each other. The comparison is made between all devices of the subnet.	No configuration is necessary. A search is made for duplicate MAC addresses starting with all network adapters of the management station.	The devices whose MAC addresses occur more than once are listed based on their device information. MAC addresses are highlighted in red.

Expected format of CSV files

A white list can be created in a text editor as a CSV file and then imported into SINEC NMS. To be able to do this, the CSV file must have the following format:

- The separator between different points of a day to record is the comma.
- Each data record is noted in a row.
- At the first position of a data record, the character string "ArticleNumber" or "DeviceType" is specified. This information categorizes the information at the second position.
- At the second position of a data record, the actual article number or the actual device type is specified.
- At the third to nth position of a data record, the firmware versions are specified.

PROFINET

In the "PROFINET" category, the following validations can be configured:

Table 4- 52 "PROFINET" validations

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate PROFINET device names	A check is performed as to whether there is more than one PROFINET device name per subnet of the network.	No configuration is necessary. A search is made for duplicate PROFINET device names starting with all network adapters of the operation PC.	The devices whose PROFINET device names occur more than once in a subnet are listed based on their device information. The PROFINET device names are highlighted in red.
PROFINET IO devices without an assigned controller	A check is made whether there are PROFINET IO devices for which PROFINET monitoring is enabled and that are not assigned to a controller.	No configuration is necessary. A search is made for PROFINET IO devices without assigned controller starting with all network adapters of the operation PC.	The PROFINET IO devices without an assigned controller are listed based on the device information.

Performance (devices)

In the "Performance (devices)" category, the following validation can be configured:

Table 4- 53 "Performance (devices)" validation

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Device availability	A check is made for all monitored devices whether their availability in the specified period was below the specified limit value. The validation is performed only for devices on which the necessary information for the validation exists.	The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the availability is specified as a percentage. The default is 95%.	The monitored devices whose availability is below the specified limit value are listed based on their device information. The availability value is highlighted in red. The number of unavailable devices is also displayed.

Performance (LAN ports)

In the "Performance (ports)" category, the following validations can be configured:

Table 4- 54 "Performance (LAN ports)" validations

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Half duplex	A check is made whether there are monitored device ports in the port mode "half duplex". Only the LAN ports in operation are checked. LAN ports in operation without a detectable port mode are evaluated as errors.	No configuration is necessary.	The ports in the port mode "half duplex" are listed based on the corresponding information.
Port speed	A check is made whether there are monitored device ports that have a lower speed than the speed specified. Only the LAN ports in operation are checked. LAN ports in operation without a detectable speed are evaluated as errors.	The limit value for the speed is specified in Mbps. The default is 100 Mbps.	The ports whose speed is below the specified limit value are listed based on the corresponding information. The speed is highlighted in red.
Interface utilization	A check is made whether there are monitored device ports that had a higher receive and/or transmit utilization than that specified. Only the LAN ports in operation for which port statistics were enabled in SINEC NMS are checked.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the utilization is specified as a percentage. The default is 50%.	The ports whose receive and/or transmit utilization is higher than the specified limit value are listed based on the corresponding information. The maximum receive and/or transmit utilization is highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Interface error rate	A check is made whether there are monitored device ports that had a higher receive and/or transmit error rate than that specified. Only the LAN ports in operation for which port statistics were enabled in SINEC NMS are checked.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the error rate is specified as a percentage. The default value is 0%.	The ports whose receive and/or transmit error rate is higher than the specified limit value are listed based on the corresponding information. The maximum receive and/or transmit error rate is highlighted in red.
Discarded packets	A check is made whether there are monitored device ports that discarded more incoming and outgoing packets than specified in the period specified. Only the LAN ports in operation for which port statistics were enabled in SINEC NMS are checked.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value is specified by the number of discarded packets. The default is 0.	The ports whose number of discarded receive and/or transmit packets is higher than the specified limit value are listed based on the corresponding information. The number of discarded receive and/or transmit packets is highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Attenuation reserves of POF ports	A check is made whether there are monitored POF ports whose power margin is outside the specified range. Only the POF ports in operation for which port statistics were enabled in SINEC NMS and for which information on the power margin exists are checked. POF ports in operation without detectable values are evaluated as errors.	The range of the permitted power margin can be specified in dB. The default range is 4.5 to 99 dB.	The POF ports whose power margin is outside the specified range are listed based on the corresponding information. The power margin is highlighted in red.
Length-dependent power margin of POF ports	A check is made whether there are monitored POF ports whose attenuation reserve is outside the range specified for the cable length. Only the POF ports in operation for which port statistics were enabled in SINEC NMS and for which information on the power margin exists are checked. POF ports in operation without detectable values are evaluated as errors.	Ranges for cable lengths can be specified in m. These ranges can be assigned ranges for permitted power margin in dB.	The POF ports whose attenuation reserve is outside the range specified for the cable length are listed based on the corresponding information. The power margin is highlighted in red.

Events

In the "Events" category, the following validation can be configured:

Table 4- 55 "Events" validation

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Network events	A check is made whether more network events were triggered than specified from the selected event classes and from overall status groups if selected in the specified period.	The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. If no event classes were selected, the events of all event classes are checked. You can configure whether all events or only the events of selected overall status groups are checked.	The following data is specified per overall status group: • Number of events of the event class "Error" • Number of events of the event class "Warning" • Number of events of the event class "Information"

4.3.4.6 Historical data and trend charts

Overview

Within the Web pages for the report types "Availability", "Performance”, “Inventory" and "Events" you can call up the recorded data and trend charts. This information is shown in additional Windows.

Select a row in the table view of a report and select one of the following menu entries using the right mouse button:

- Show historical data
- Show trend charts

Note

Show historical data

In the tables of the reports, SINEC NMS provides an additional column "Historical data". This column indicates the existence of historical data.

Historical data

Meaning

The data of a device or an interface monitored in SINEC NMS is subject to change. SINEC NMS records these changes and shows them in the historical data.

Content

For the selected report entry of a device or an interface, the displayed table "Data history" has a row for each registered change. A row contains the following entries:

Table 4- 56 Historical data

Entry	Meaning
Attributes	Names the property whose status has changed. The following is displayed depending on the selected report type and the selected entry: • For devices: – IP address – MAC address – Device type – Device category – PROFINET device name – Monitoring status • For interfaces: – Interface type – Transmission rate – Interface mode
Old value	Shows the value prior to the registered change.
New value	Shows the value after the registered change.
Time of the change	Date and time of the status change

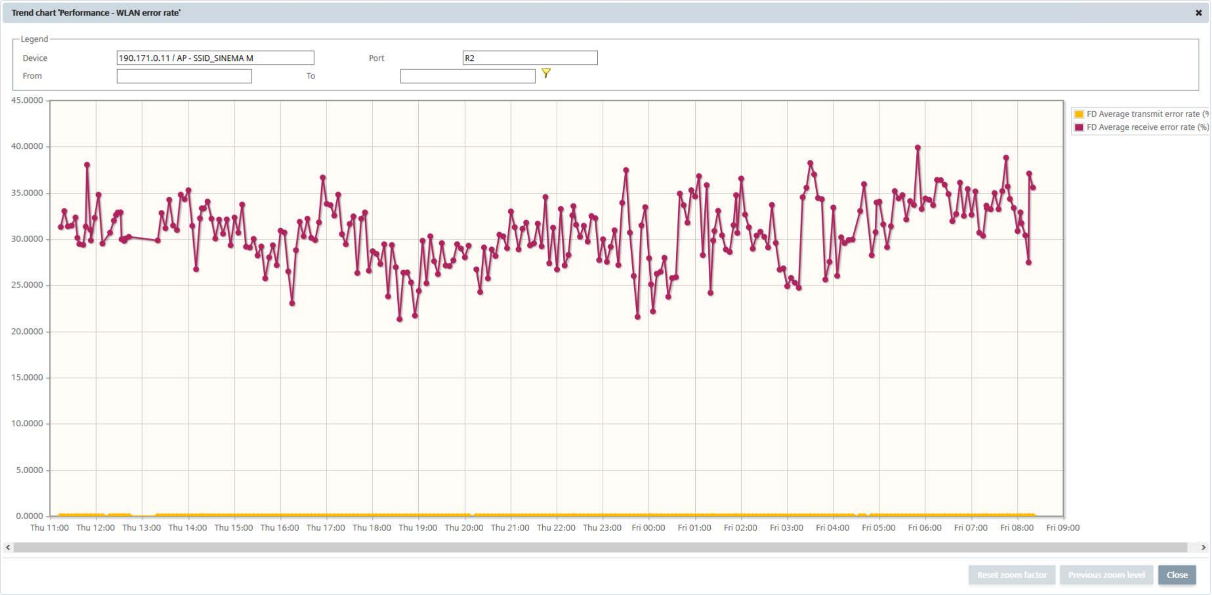
Trend charts

Meaning

Trend diagrams show certain properties of devices, interfaces and transfer parameters over time in a graphic form.

Display and content

The following figure shows the example of a possible trend chart from the "WLAN interface error rate (%)" report type with the trend of the "Average transmit error rate (%)" and "Average receive error rate (%)".



Trend chart 'Performance - WLAN error rate'

Legend

Device: 190.171.0.11 / AP - SSID_SINEMA M

Port: R2

From:

To:

Figure 4-15 Trend chart for WLAN interface error rate

In the header, you enter a display period and enable this by clicking the filter icon.

Information on the display:

- The lines of the trend have dots that mark the end of a period. By selecting the dot with the mouse pointer, you display information about the date, time and duration of the period.
- The Y axis represents the range of values of the displayed trends data.
- The X axis represents the period of time.
- If different trend data is displayed in a chart, the color distinguishes the type of data.
- If there are interruptions in a chart line, this means that there were periods in which there was no monitoring.

Reports with trend charts

The following list shows which reports record which trend data.

Table 4- 57 Reports with trend charts

Report type	Tab	Trend data
Availability	Devices	Availability in %
	Interfaces	Active time in %

Report type	Tab	Trend data
Performance	LAN - interface utilization	• Average transmit utilization in % • Average receive utilization in % • Average utilization as % For full duplex mode, the display has 3 trend lines.
	LAN interface error rate	• Average transmit error rate in % • Average receive error rate in % • Average error rate in % Display with 2 trend lines.
	WLAN interface error rate	• Average transmit error rate in % • Average receive error rate in %
	WLAN - Interface data rate (transmission speed)	Average transmit data rate (Mbps)
	WLAN - signal strength	Average signal strength (dBm)
	WLAN - number of clients	Average number of clients

Zoom function

The zoom function of the trend charts allows you to restrict the displayed period. This increases the resolution of the display and improves the clarity of the displayed times.

To use the zoom function, follow the steps below:

1. In the trend chart, click on the required starting time of the period and hold down the mouse button.
2. Drag the mouse pointer to the required end time and release the mouse button.

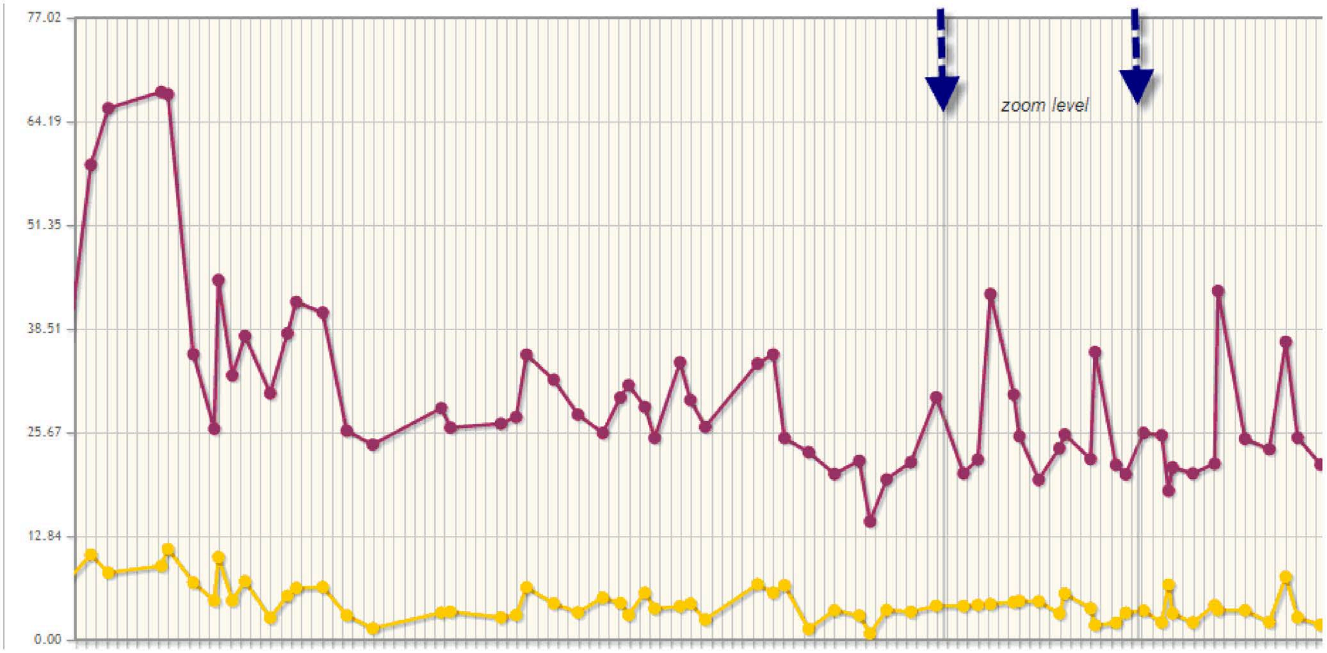


Figure 4-16 Trend chart with zoom

4.3.5 Settings

4.3.5.1 Network scan

Operation

You can scan the network and start the search for more suitable device profiles for devices on the operation on the page "Network monitoring > Settings > Network scan" of an operation. Scan ranges that are configured for the operation on the control under "System administration > Operations" are used for the network scan. You can also configure the DCP network adapter which the operation uses for the network scan.

The following operator controls are available:

Table 4- 58 "IP address ranges for network scan" area

Operator control	Function
🔍▶	Start network scan
🔍■	Stop network scan
▶	Starting automatic device type change A search is made for more suitable device profiles and device types included in them for devices that were assigned a standard profile.

Table 4- 59 Area "DCP network adapter for device scan"

Operator control	Function
	Scan LAN interfaces
🟩	Change the status of the selected (✓) interfaces green: Network adapter is used for the scan.

Note

Network adapters without DCP capability

The following network adapters cannot send DCP packets and are therefore not shown in the list "DCP network adapter for device scan".

- CP 1604
- CP 1616
- CP 1616 onboard
- CP 1613
- CP 1613-A2
- CP 1623
- CP 1626
- CP 1628

Note

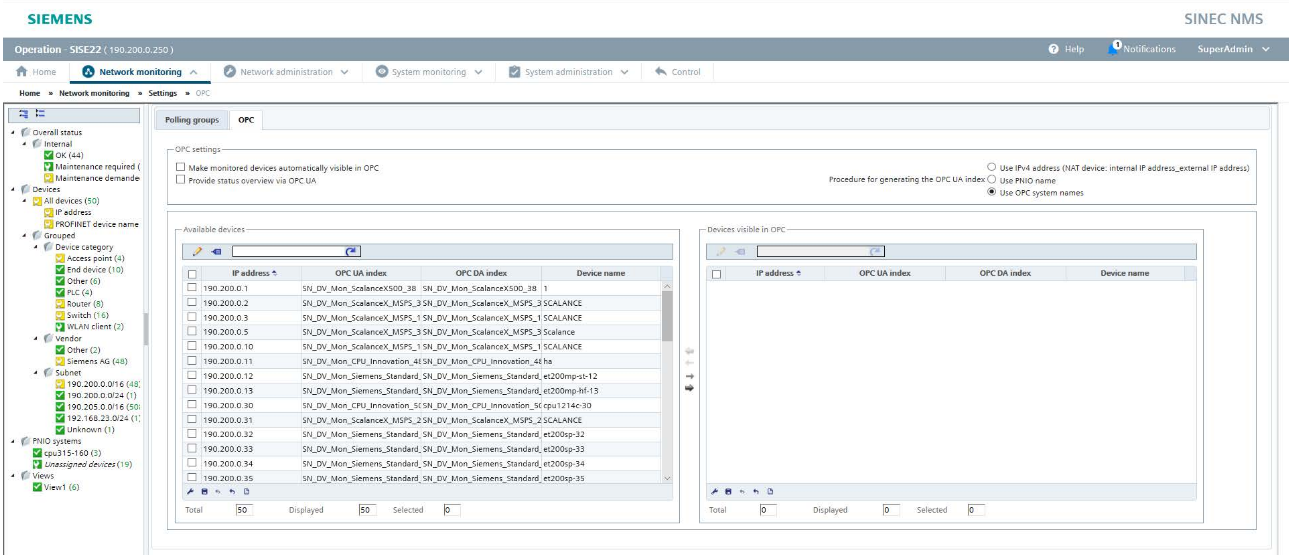
Network scan via other protocols

The network scan via other protocols is performed regardless of the settings configured in this area.

4.3.5.2 OPC

Operation

You open the Web page shown below using the menu command "Network monitoring > Settings > OPC" on an operation.



OPC settings

☐ Make monitored devices automatically visible in OPC
☐ Provide status overview via OPC UA

Procedure for generating the OPC UA index
○ Use IPv4 address (NAT device: internal IP address_external IP address)
○ Use PNIO name
● Use OPC system names

Available devices

☐	IP address	OPC UA index	OPC DA index	Device name
☐	190.200.0.1	SN_DV_Mon_ScalanceX500_38	SN_DV_Mon_ScalanceX500_38	1
☐	190.200.0.2	SN_DV_Mon_ScalanceX_MSPS_3	SN_DV_Mon_ScalanceX_MSPS_3	SCALANCE
☐	190.200.0.3	SN_DV_Mon_ScalanceX_MSPS_1	SN_DV_Mon_ScalanceX_MSPS_1	SCALANCE
☐	190.200.0.5	SN_DV_Mon_ScalanceX_MSPS_3	SN_DV_Mon_ScalanceX_MSPS_3	Scalance
☐	190.200.0.10	SN_DV_Mon_ScalanceX_MSPS_1	SN_DV_Mon_ScalanceX_MSPS_1	SCALANCE
☐	190.200.0.11	SN_DV_Mon_CPU_Innovation_48	SN_DV_Mon_CPU_Innovation_48	ha
☐	190.200.0.12	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200mp-st-12
☐	190.200.0.13	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200mp-hf-13
☐	190.200.0.30	SN_DV_Mon_CPU_Innovation_5(	SN_DV_Mon_CPU_Innovation_5(	cpu1214c-30
☐	190.200.0.31	SN_DV_Mon_ScalanceX_MSPS_2	SN_DV_Mon_ScalanceX_MSPS_2	SCALANCE
☐	190.200.0.32	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200sp-32
☐	190.200.0.33	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200sp-33
☐	190.200.0.34	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200sp-34
☐	190.200.0.35	SN_DV_Mon_Siemens_Standard_	SN_DV_Mon_Siemens_Standard_	et200sp-35

Total 50 Displayed 50 Selected 0

Devices visible in OPC

☐	IP address	OPC UA index	OPC DA index	Device name

Total 0 Displayed 0 Selected 0

Figure 4-17 Page for OPC configuration

Overview

In industrial manufacturing, devices of different manufacturers with different process controllers as well as incompatible protocols and data formats are often used. For these to be able to communicate with each other, an open communications standard (OPC --> Open Process Control) was defined. This allows plant data, alarms, events and other process data to be exchanged between all systems in real time. SINEC NMS also provides the option of making data available via OPC.

Layout

Each operation contains an OPC UA server. On the page "Network monitoring > Settings > OPC", you can configure the data of which devices will be sent to the OPC UA server of the operation. This device data is then visible for OPC UA clients and can be evaluated and monitored by them. Device data from unmonitored and passively monitored devices cannot ever be sent to the OPC UA server.

OPC settings

In the dialog area "OPC settings", the following operator controls are available:

Table 4- 60 OPC settings

Operator control	Function
Make monitored devices automatically visible in OPC	When this check box is selected, the device data of all devices monitored by the operation is visible in OPC.
Procedure for generating the OPC UA index	For monitored devices that do not yet have an OPC UA index, the operation generates an OPC UA index using one of the following procedures: • Using the Ipv4 address The OPC UA index is formed from the four digits of the IPv4 address of the device. The periods of the IPv4 address are not adopted If the digits have less than three places, the missing places are filled out with the digit "0". Example: IPv4 address: 102.23.10.4 OPC UA index: 102023010004 OPC UA index for NAT devices: <internal IP address>_<external IP address>, e.g. 192168110237_192168111237 In the case of an IP address change, the OPC UA index is not updated. • Using the PNIO name: The PNIO name of the device is used as the OPC UA index. A maximum of 64 characters of the PNIO name are adopted. If non-permitted characters occur in the PNIO name, these are replaced by the "_" character. • Using the OPC DA index (default setting): The OPC DA index of the device is used as the OPC UA index. If this setting is changed, existing OPC UA indexes are not updated.
Provide status overview via OPC UA	When this check box is selected, the following information is provided via OPC: • The numbers of devices per overall status • The worst existing overall status • The following information is provided for each view: – Name of the view – Name of the higher-level view – The worst existing overall status – Number of reachable devices – Number of unreachable devices – Number of unconnected devices The overall states are indicated by the following values: • 1: Not reachable • 2: Error • 3: Maintenance demanded • 4: Maintenance required • 5: OK • 6: Not connected • 7: Unmonitored • 8: Passively monitored

Available devices and visible in OPC

In the dialog areas "Available devices" and "Devices visible in OPC", it is possible, for example, to manually configure the data of those devices that are visible via OPC UA. If the "Make monitored devices automatically visible in OPC" check box is selected in the OPC settings, settings made relating to this are ignored and the corresponding operator controls are disabled.

The following operator controls are available:

Table 4- 61 Operator controls for visibility of devices in OPC

Operator control	Function
✏	A dialog opens in which the OPC UA index of the selected device can be changed manually. Using the button ↻ in this dialog, the existing OPC UA index is updated according to the configured procedure. The OPC UA index must be between 6 and 64 characters long and must be unique among the monitored devices. Spaces, tabs and the following characters must not occur in the OPC UA index: .:;,[]{}?*\/%!()$@
⇤	Update the OPC UA indexes of the selected devices according to the configured procedure.
□	Enter text for text search / filter
↻	Start text search / filter setting
⇦	Remove all devices from the list "Devices visible in OPC"
←	Remove all devices from the "Devices visible in OPC" list
→	Add the selected (✓) devices to the "Devices visible in OPC" list
⇨	Add all devices to the "Devices visible in OPC" list

In the footer, there is information about how many devices are in each area in total, and how many are displayed and selected.

Although the column assignment in the data area is preset, you can arrange it any way you require (🔧 in the footer). You can choose from all the device properties as those available via the device window and the device details.

Data access with OPC (UA)

The OPC UA (Unified Architecture) is based on a service-oriented architecture and manages without the components of the Microsoft COM/DCOM (Component Object Model/Distributed Object Component Model). OPC UA is a cross-platform standard with which systems and devices of different types can communicate with each other. They send messages between clients and servers via different types of network. UA supports rugged, secure communication that protects the identity of servers and clients and provides protection from attacks.

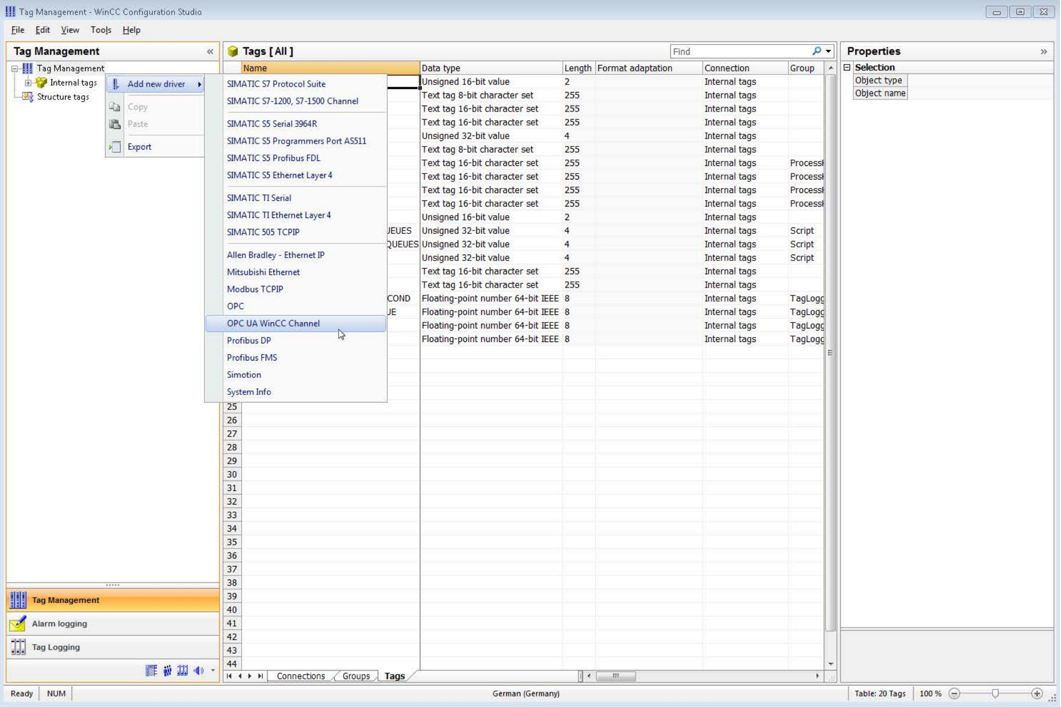
Configuring UA ports

The default port used for a UA server is 4841. This port can be configured in the Operation Monitor, see section Operation Monitor (Page 37).

If OPC UA server and OPC UA client are separate PCs, the OPC UA port used must be open in the firewall of both PCs. For more information, refer to section Port settings (Page 39).

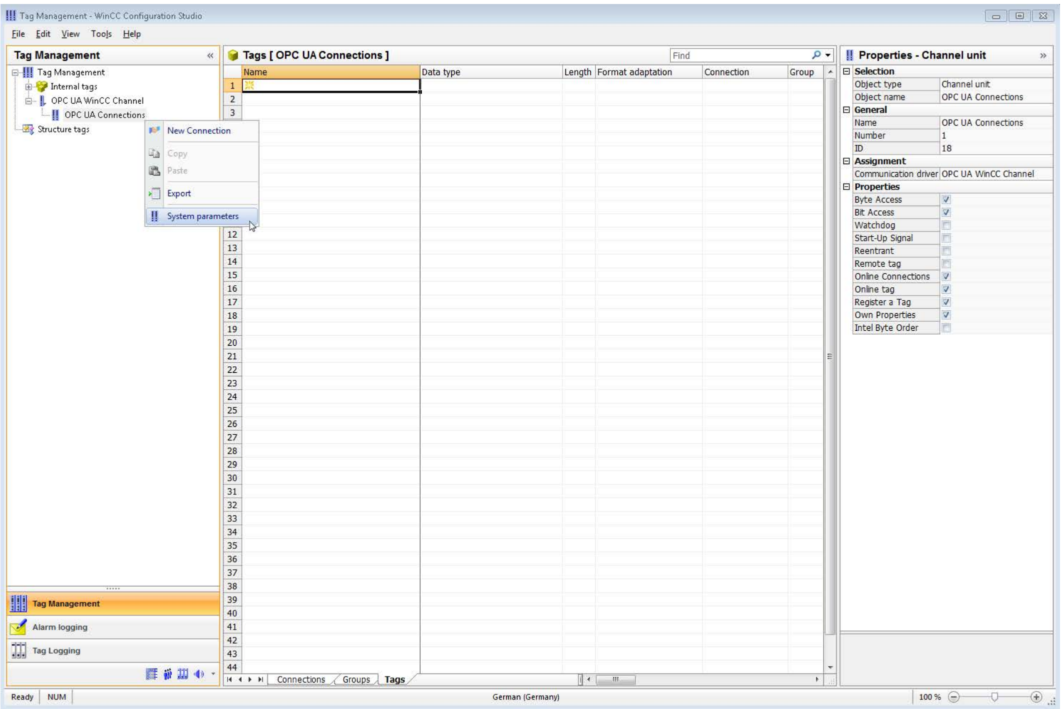
OPC UA access with WinCC Explorer 7.4

1. Start the operation whose OPC UA server you want to access.
2. Start the WinCC Explorer.
3. Open the Tag Management.
4. In the shortcut menu of the entry "Tag Management" select the menu command "Add new driver > OPC UA WinCC Channel".



Name	Data type	Length	Format adaptation	Connection	Group
	Unsigned 16-bit value	2		Internal tags	
	Text tag 8-bit character set	255		Internal tags	
	Text tag 16-bit character set	255		Internal tags	
	Text tag 16-bit character set	255		Internal tags	
	Unsigned 32-bit value	4		Internal tags	
	Text tag 8-bit character set	255		Internal tags	
	Text tag 16-bit character set	255		Internal tags	Processi
	Text tag 16-bit character set	255		Internal tags	Processi
	Text tag 16-bit character set	255		Internal tags	Processi
	Text tag 16-bit character set	255		Internal tags	Processi
	Unsigned 16-bit value	2		Internal tags	
JEUES	Unsigned 32-bit value	4		Internal tags	Script
QUEUES	Unsigned 32-bit value	4		Internal tags	Script
	Unsigned 32-bit value	4		Internal tags	Script
	Text tag 16-bit character set	255		Internal tags	
	Text tag 16-bit character set	255		Internal tags	
COND	Floating-point number 64-bit IEEE	8		Internal tags	TagLogg
JE	Floating-point number 64-bit IEEE	8		Internal tags	TagLogg
	Floating-point number 64-bit IEEE	8		Internal tags	TagLogg
	Floating-point number 64-bit IEEE	8		Internal tags	TagLogg

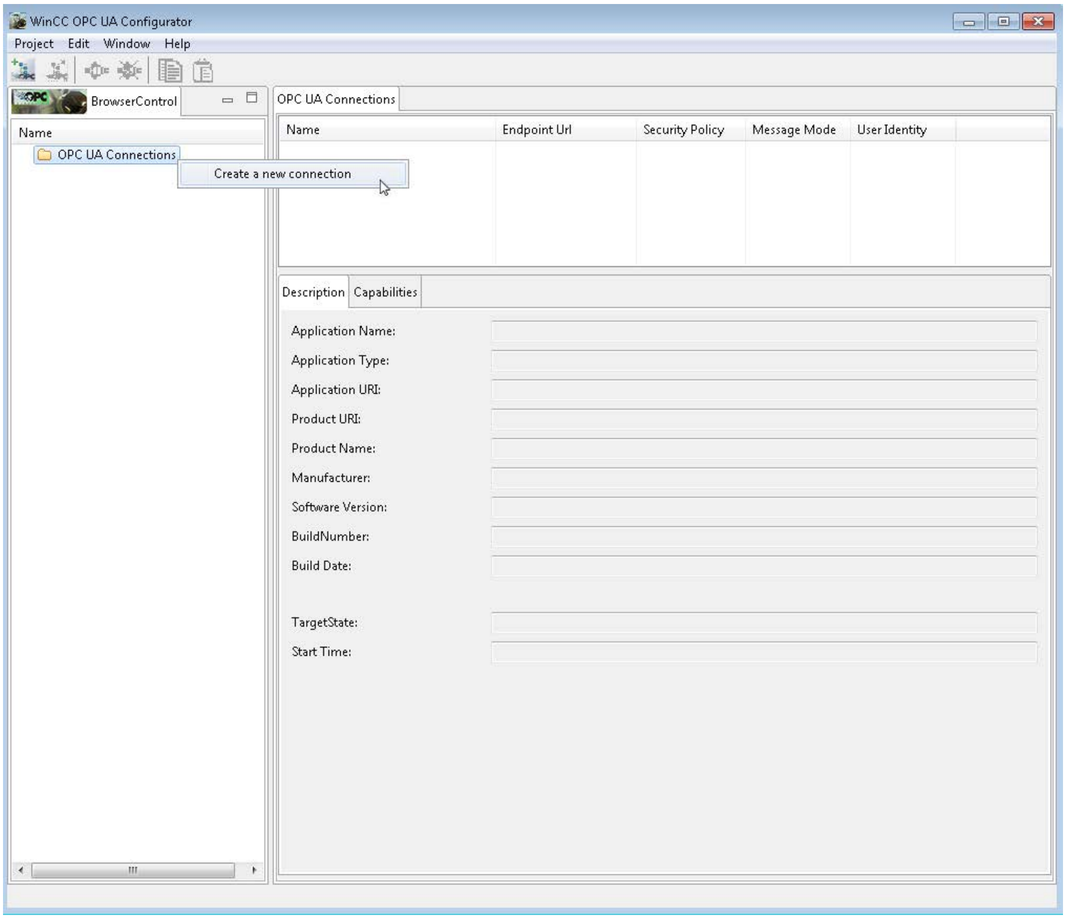
5. In the shortcut menu of the entry "OPC UA Connections" select the entry "System parameters".



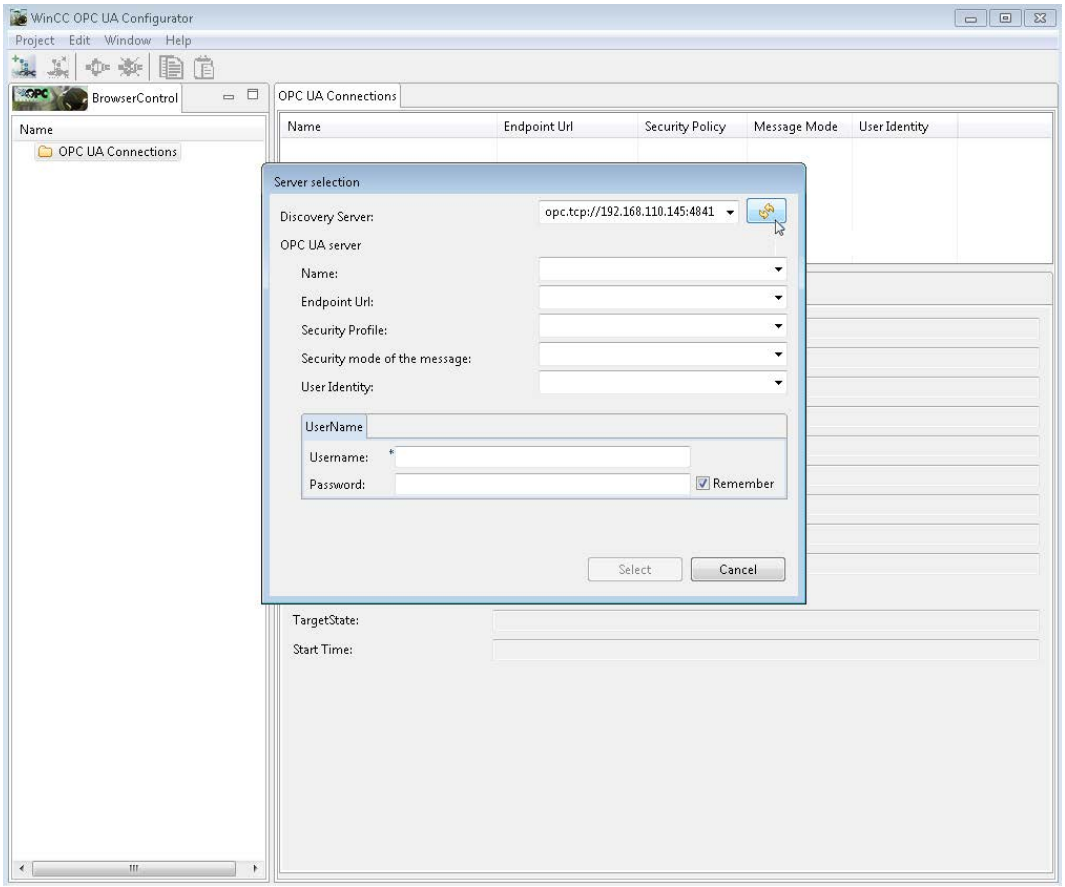
Properties - Channel unit

Selection	
Object type	Channel unit
Object name	OPC UA Connections
General	
Name	OPC UA Connections
Number	1
ID	18
Assignment	
Communication driver	OPC UA WinCC Channel
Properties	
Byte Access	☑
Bit Access	☑
Watchdog	☐
Start-Up Signal	☐
Reentrant	☐
Remote tag	☐
Online Connections	☑
Online tag	☑
Register a Tag	☑
Own Properties	☑
Intel Byte Order	☐

6. In the WinCC OPC UA Configurator in the shortcut menu of the entry "OPC UA Connections" select the menu command "Create a new connection".

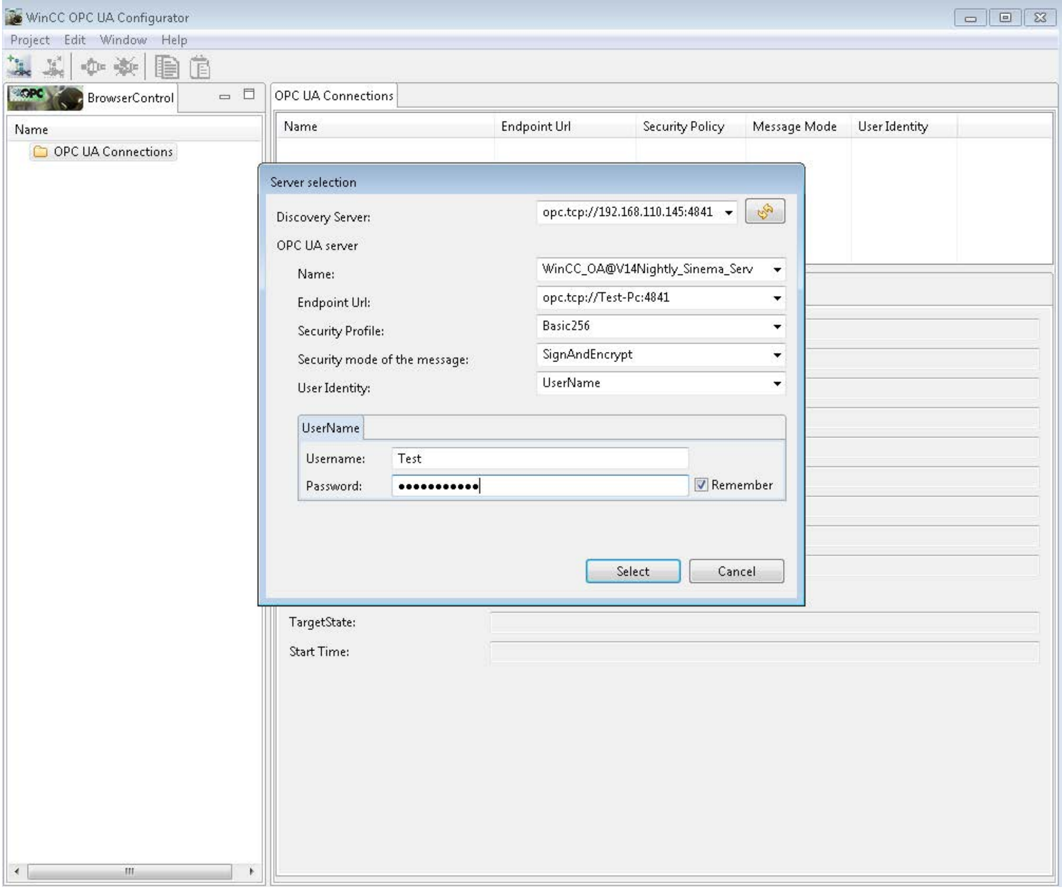


7. In the window "Server selection" enter the data of the OPC UA server in the input box "Discovery Server" and click on the button to update the window.



Discovery Server: opc.tcp://192.168.110.145:4841

8. As default, access to the OPC UA server is only possible with user authentication. Therefore, select the "UserName" entry for the "User Identity" parameter and enter the data of an available user in SINEC NMS.



Server selection

Discovery Server: opc.tcp://192.168.110.145:4841

OPC UA server

Name: WinCC_OA@V14Nightly_Sinema_Serv

Endpoint Url: opc.tcp://Test-Pc:4841

Security Profile: Basic256

Security mode of the message: SignAndEncrypt

User Identity: UserName

UserName

Username: Test

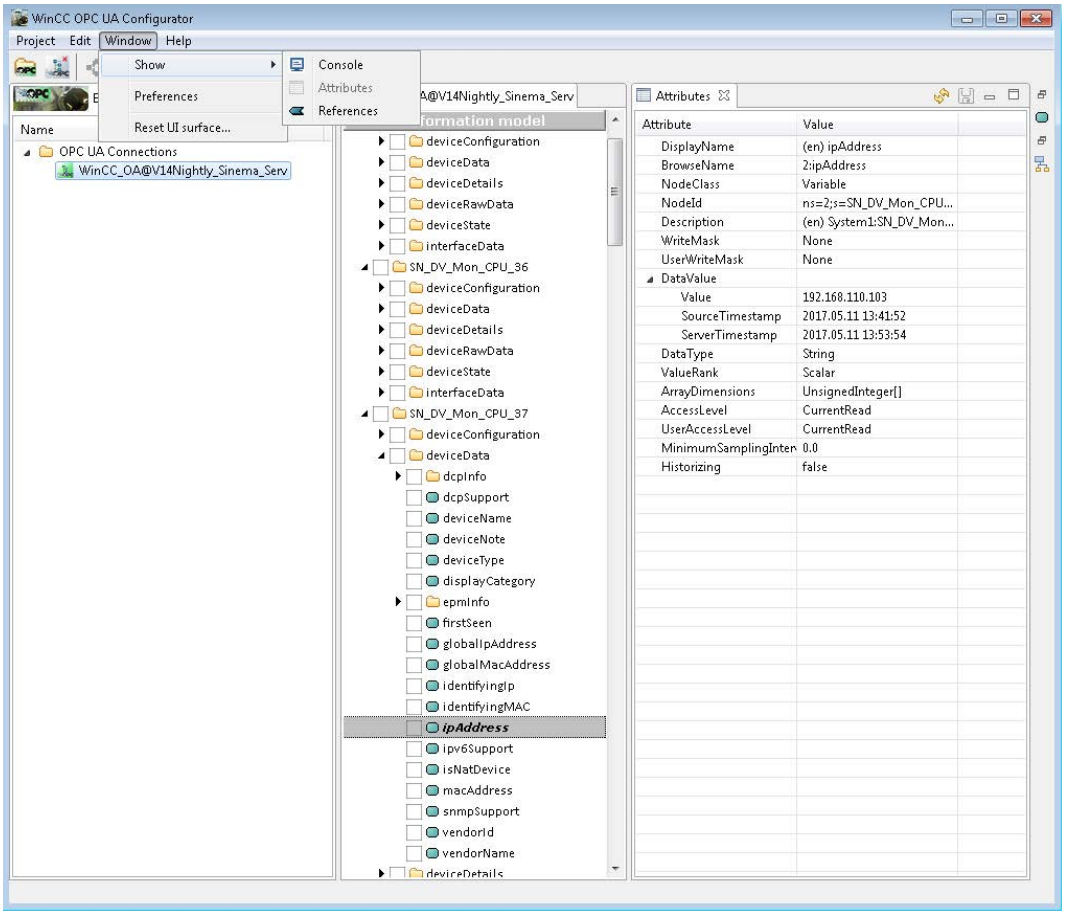
Password: ●●●●●●●●●●● ☑ Remember

You can disable this default for user authentication when accessing the OPC UA server in the operation monitor.

Result: The connection establishment initially fails, because created certificates are rejected as default by the OPC UA server. The entry for the OPC UA connection turns red.

9. Move the rejected certificates on the OPC UA server from the directory "C:\Siemens\SINECNMS_MON\WinCC_OA\[Version]\data\opcua\server\PKI\CA\rejected" into the directory "C:\Siemens\SINECNMS_MON\WinCC_OA\[Version]\data\opcua\server\PKI\CA\certs".

Result: Youi have set up a connection to the OPC UA server. You can use the menu command "Window > Show > Attributes" to display SINEC NMS data.

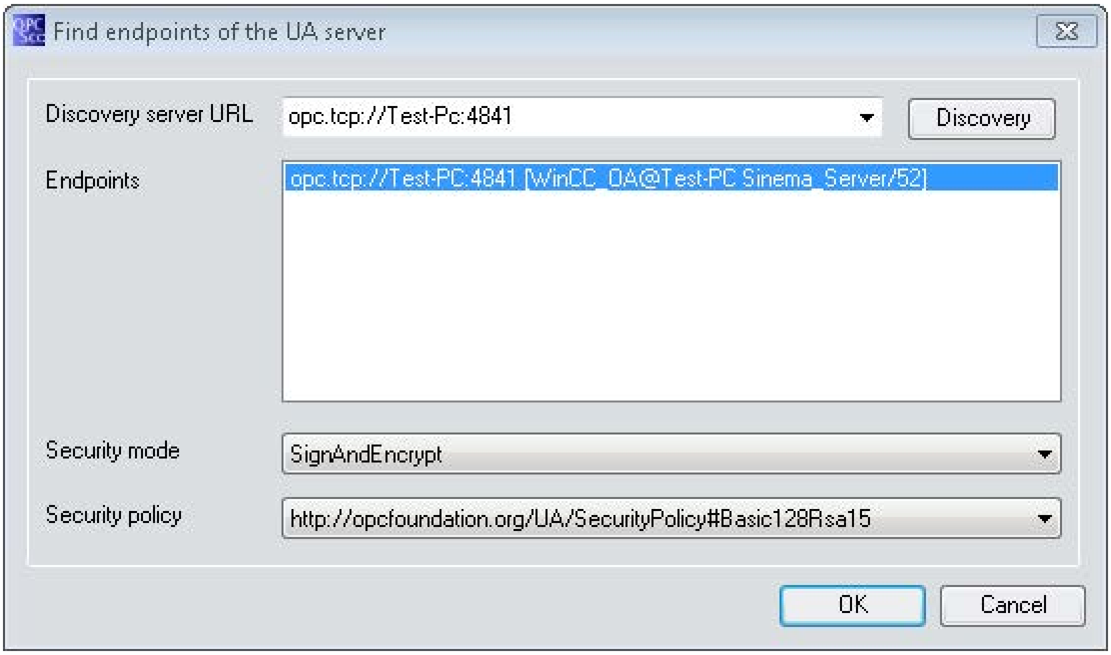


Attribute	Value
DisplayName	(en) ipAddress
BrowseName	2:ipAddress
NodeClass	Variable
NodeId	ns=2;s=SN_DV_Mon_CPU...
Description	(en) System1:SN_DV_Mon...
WriteMask	None
UserWriteMask	None
DataValue	
Value	192.168.110.103
SourceTimestamp	2017.05.11 13:41:52
ServerTimestamp	2017.05.11 13:53:54
DataType	String
ValueRank	Scalar
ArrayDimensions	UnsignedInteger[]
AccessLevel	CurrentRead
UserAccessLevel	CurrentRead
MinimumSamplingInter	0.0
Historizing	false

OPC UA access with OPC Scout

1. Start the operation whose OPC UA server you want to access.
2. Start OPC Scout V10.

3. Create a signed and encrypted UA server connection in OPC Scout V10 (opc.tcp://pcname:port).



Find endpoints of the UA server

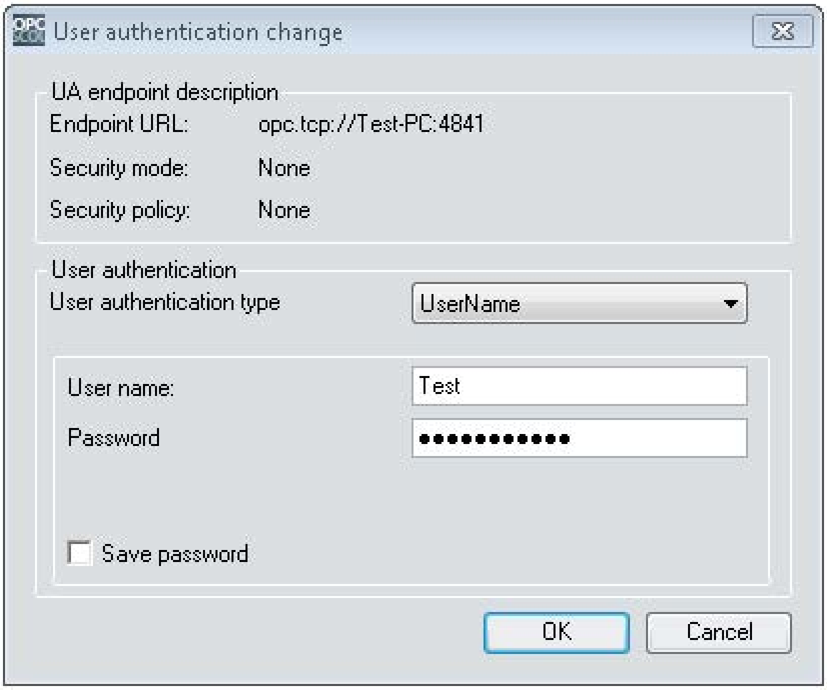
Discovery server URL: opc.tcp://Test-Pc:4841

Endpoints: opc.tcp://Test-PC:4841 [WinCC_OA@Test-PC Sinema_Server/52]

Security mode: SignAndEncrypt

Security policy: http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15

4. As default, access to the OPC UA server is only possible with user authentication. For this reason right-click on the server, select the menu command "Change user authentication", from the drop-down list "User authentication type" select the entry "UserName" and enter the data of a user that exists in SINEC NMS.



User authentication change

UA endpoint description

Endpoint URL: opc.tcp://Test-PC:4841

Security mode: None

Security policy: None

User authentication

User authentication type: UserName

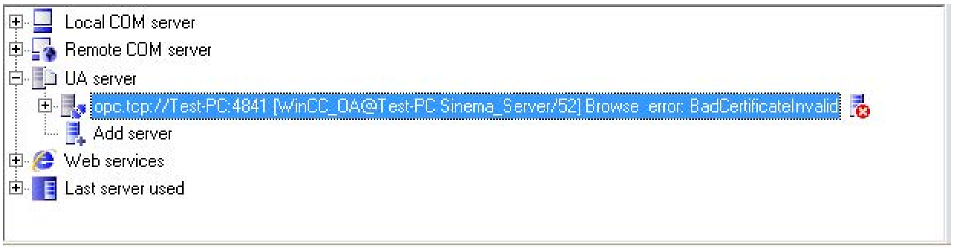
User name: Test

Password: ●●●●●●●●●●●

□ Save password

You can disable this default for user authentication when accessing the OPC UA server in the operation monitor.

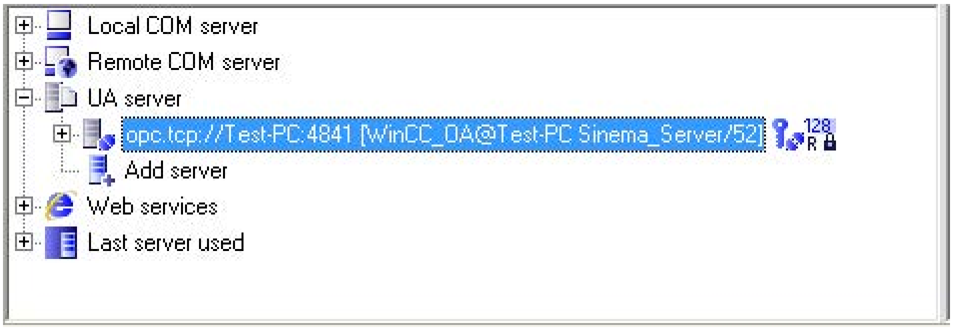
5. Double-click on the server so that the error message "Bad certificate error" appears.



Local COM server
Remote COM server
UA server
opc.tcp://Test-PC:4841 [WinCC_OA@Test-PC Sinema_Server/52] Browse error: BadCertificateInvalid
Add server
Web services
Last server used

6. You will now find the rejected OPC Scout V10 certificate in the directory "C:\Siemens\SINECNMS_MON\WinCC_OA\[Version]\data\opcua\server\PKI\CA\rejected" .

7. Move this certificate to the directory "C:\Siemens\SINECNMS_MON\WinCC_OA\[Version]\data\opcua\server\PKI\CA\certs".
8. Now double-click on the server again for a signed and encrypted connection.



4.3.5.3 Polling groups

Operation

The page "Network monitoring > Settings > Polling groups" shows the three polling groups "Fast", "Medium" and "Slow" each in a separate tab, together with their assigned network devices.

Meaning

A polling group is a device group whose UP/DOWN status is queried at a certain interval (polling rate) via the ICMP protocol. The polling rate can be specified for each group within a certain range. The number of devices per group is limited. The division into 3 polling groups is defined for the relevant bandwidth of their polling rate. The following groups are distinguished

- Fast
- Medium
- Slow

Network devices that are not monitored or that can be ignored or are classified as non-critical can be moved to lower-level polling groups. This means that such devices are polled at a longer interval. This technique allows you to control the network load when lots of devices need to be polled.

Polling groups

The 3 polling groups appear in the form of tabs within the polling dialog. These polling groups are divided up based on the polling rate measured in seconds.

- Fast

  This group is intended for all devices that need to be polled frequently.

  - The default setting is 30 seconds.
  - The minimum polling interval is 10 seconds; the maximum polling interval is 60 seconds.
  - As default, the group can contain up to 100 devices. Up to 250 devices can be assigned.
- Medium

  This group is intended for all devices that need to be polled with medium frequency.

  - The default setting is 150 seconds.
  - The minimum polling interval is 90 seconds; the maximum polling interval is 150 seconds.
  - As default, the group can contain up to 200 devices. Up to 500 devices can be assigned.
- Slow

  This group is intended for all devices that need to be polled less frequently.

  - The default setting is 300 seconds.
  - The minimum polling interval is 180 seconds; the maximum polling interval is 300 seconds.
  - As default, the group can contain up to 200 devices. Up to 1000 devices can be assigned.

Note

Number of devices

The number of devices shown in the medium and slow tabs is the number of devices remaining until the maximum possible number of devices is reached.

Operator input

The following table shows the functional elements of the header:

Table 4- 62 Operator controls for polling groups

Icon	Display / function	Icon	Display / function
Rate (in sec.): 30 ▼	Polling rate in seconds	Fast (150)	Transfer selected (✓) devices to the "Fast" polling group *
Slow (120)	Transfer selected (✓) devices to the "Slow" polling group *****	Medium (50)	Transfer selected (✓) devices to the "Medium" polling group *
□	Enter text for text search	🔍	Start text search
41/250	Display the used / available table entries		

*****) The number after the group name indicates how many table entries are still available.

The table below this shows the network devices assigned to this group, in each case with

- Status
- IP address
- Name
- Device type
- Location

Setting up polling groups - procedure

To move devices from one group to another, follow the steps below:

1. Select the device or the devices you want to move to another group.
2. Click the appropriate icon in the header. Result: The selected devices are moved to the required group.

4.3.5.4 System jobs

Operation

The system-defined jobs for system backups of monitoring and archive data as well as for database cleaning of archive data are displayed on the page "Network monitoring > Settings > System jobs". On this page, both jobs can be controlled, configured and scheduled for time-driven execution. The jobs cannot be deleted.

The "Online system backup of monitor and archive data" job must not be executed while the "Database cleanup of archive data" job is being executed. The reverse also applies. There must be at least 10 minutes between the end of the job execution of the database cleanup for archive data and the start of the execution of the job "Online system backup of monitor and archive data". These restrictions apply both to manual and planned job executions.

System backup of monitoring and archive data

By default, this job is executed every day at 4:00 a.m. and backs up the monitoring and archive data of devices and events of the operation. A created system backup can be manually restored via Operation Monitor, "Restore" tab. If the operation cannot be started correctly, the last created system backup is transferred back automatically. The path on which the operation searches for this system backup can be configured in the job type-specific settings of the job, refer to the section Job type-specific settings for the job type "System backup" (Page 167).

Database cleanup of archive data

This job cleans the operation database of archive data for reports and events. Prior to deletion, the archive data can be exported for reports. It is also possible to import this archive data. The effects of a database cleanup take effect only after the operation has been restarted.

Operator input

The following table explains the operator controls of the header:

Table 4- 63 Operator controls for jobs

Operator control	Function
✏	Edit selected job The dialog for configuring jobs is opened, refer to section Configuration of jobs (Page 166).
▶	Run selected jobs The selected job is started from the beginning and changed to the "In progress" status. Multiple selection is possible. The execution started with this button has no influence on executions planned for the job.
■	Stop selected jobs A job with the status "In progress" is stopped with this button and cannot be continued at the same position. If the "Manual" execution type was configured for the job, it is given the status "Stopped". Multiple selection is possible.
🟥	Stop / suspend all jobs The function of this button depends on the status of the job: • Job status "In progress": Refer to the description of the "Stop selected jobs" function. • Job status "Pending / Finished / Stopped / Failed partly / Failed": Jobs in one of these states and not configured with the "Manual" execution type are set to the state "Suspended". For jobs in the "Suspended" status, planned executions are not performed and changes to their configuration are not possible. Regardless of the jobs involved, the buttons "Run selected jobs" and "Stop selected jobs" are disabled. When the "Stop / suspend all jobs" button is clicked again, the buttons are re-enabled and planned executions of jobs are performed again.
□ {} ↷	Enter text to filter based on jobs. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The {} icon is displayed when a filter template with a complex query is active.

Operator control	Function
	Selection of a previously created template for filtering according to jobs. After selection, the properties of the filter template are applied to the list of jobs. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
▽ ▽✓	Open the editor for configuring filter settings that can be stored in filter templates. The ▽✓ icon is displayed when the configured filter settings differ from the default filter settings.

Task states

The "Task" column displays the total number of tasks of a job. Behind the total number, it is displayed how many tasks have which status. The states are indicated by colors:

Color	Task status
Green	Task was executed successfully.
Red	An error occurred when executing the task.
Gray	Task status is unknown.

Configuration of jobs

Overview

Overview

You reach the dialog for configuring jobs via the button for editing a job. In this dialog, you can make basic settings not dependent on the job type and job type specific settings. The settings cannot be changed for jobs that are currently being executed.

Basic settings

The "Basic settings" tab contains the following parameters:

Table 4- 64 Operator controls in the "Basic settings" tab

Parameter	Function
ID	ID of the job. The ID cannot be changed.
Status	Current status of the job. A job with "pending" status can be executed. For information on other job states, refer to the section Operator input (Page 165).
Description	Freely selectable description of the job.
Tasks	Display of the total number of tasks contained in the job. Behind this, the states of the tasks during the last job execution are shown, see section Operator input (Page 165).

Parameter	Function
Type of execution	With this drop-down list, the type of execution of the job can be specified: • Manual: The job can only be executed using the buttons "Run selected jobs" in the header of the job list and "Save and execute" in the configuration dialog for jobs. • Once: The job is executed once at a selectable time. The job can also be executed with the "Run selected jobs" button. • Every n hours: As of a selectable point in time the job is executed at a selectable interval of hours. The minimum value is 1, the maximum value 24. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n hours" option is not available for the job type "Database cleanup of archive data". • Every n days: As of a selectable point in time the job is executed at a selectable interval. As the interval, the options "Daily", "Weekly", "Monthly" or a user-defined number of days can be selected. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n days" option is not available for the job type "Database cleanup of archive data". • Every n months: As of a selectable point in time the job is executed at a selectable interval. As the interval, the options "Monthly", "Yearly" or a user-defined number of months can be selected. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n months" option is only available for the job type "Database cleanup of archive data". No logon to SINEC NMS is necessary for jobs configured with an execution type other than "Manual".
Job type	Display of the job type. For information on the available job types, refer to section System jobs (Page 164).

Job type-specific settings for the job type "System backup"

For the job type "System backup of monitoring and archive data", the "Job type specific settings" tab contains the following parameters:

Table 4- 65 Job type-specific settings for the job type "System backup"

Parameter	Function
Number of system backups to keep available	Number of system backups stored under the configured path on the operation. If the specified number is reached, the next system backup automatically deletes the system backup with the oldest time stamp. The minimum value is 1, the maximum value 10.
Path for system backups on management station	Path on the operation under which system backups are stored and under which the operation searches for the most recently created system backup. Paths to network drives are not permitted.

Job type-specific settings for the job type "Database cleanup"

For the job type "Database cleanup of archive data", the "Job type specific settings" tab contains the following parameters:

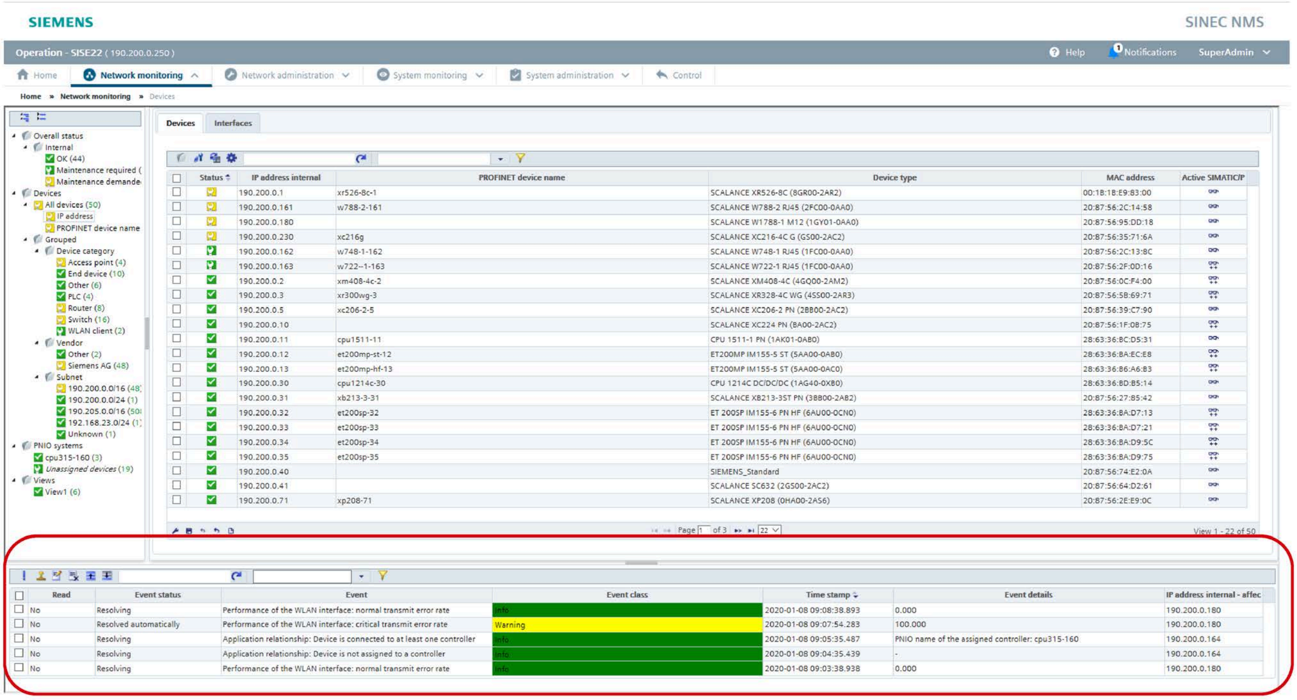
Table 4- 66 Job type-specific settings for the job type "Database cleanup"

Parameter	Function
Entries to be deleted	If you have selected the type of execution "Manual" or "Single", the following options are available: • Entries older than Entries before the specified month and year are deleted. The specified month must be before the current month. • Entries for events between Entries between the specified start and end date are deleted. With this option, only event-relevant archive data can be deleted. If you have selected the type of execution "Every n months", you can specify a number of months. Entries that are older are deleted. Permitted range of values: 1 ... 120 months.
Event categories / event classes	Selection of event categories and event classes whose events will be deleted. Events in the status "Pending" cannot be deleted.
Report archives	• None: No action is taken. • Delete archives: Archive data relevant for reports is deleted • Delete archives of deleted devices: Archive data relevant for reports of all deleted devices is deleted regardless of the specified time frame for entries to be deleted. • Export archives and delete: Report-relevant archive data is exported to a specified directory on the operation as a ZIP file and then deleted from the operation. It is not possible to export to network drives. • Import archives - path on management station (only for the types of execution "Manual" and "Single"): Report-relevant archive data is imported from the specified directory on the operation. If no path is specified, there is no import. Importing from network drives is not possible. ZIP files generated by SINEC NMS should not be edited prior to import. It is not possible to import edited ZIP files.

4.3.6 Event list

Operation

The event list shows all the events in the form of a table.



☐	Status	IP address internal	PROFINET device name	Device type	MAC address	Active SIMATIC/IP
☐	🟨	190.200.0.1	xr526-8c-1	SCALANCE XR526-8C (8GR00-2AR2)	00:1B:1B:E9:83:00	
☐	🟨	190.200.0.161	w788-2-161	SCALANCE W788-2 RJ45 (2FC00-0AA0)	20:87:56:2C:14:58	
☐	🟨	190.200.0.180		SCALANCE W1788-1 M12 (1GY01-0AA0)	20:87:56:95:DD:18	
☐	🟨	190.200.0.230	xc216g	SCALANCE XC216-4C G (GS00-2AC2)	20:87:56:35:71:6A	
☐	🟩	190.200.0.162	w748-1-162	SCALANCE W748-1 RJ45 (1FC00-0AA0)	20:87:56:2C:13:8C	
☐	🟩	190.200.0.163	w722--1-163	SCALANCE W722-1 RJ45 (1FC00-0AA0)	20:87:56:2F:0D:16	
☐	✓	190.200.0.2	xm408-4c-2	SCALANCE XM408-4C (4GQ00-2AM2)	20:87:56:0C:F4:00	
☐	✓	190.200.0.3	xr300wg-3	SCALANCE XR328-4C WG (4SS00-2AR3)	20:87:56:5B:69:71	
☐	✓	190.200.0.5	xc206-2-5	SCALANCE XC206-2 PN (2BB00-2AC2)	20:87:56:39:C7:90	
☐	✓	190.200.0.10		SCALANCE XC224 PN (BA00-2AC2)	20:87:56:1F:08:75	
☐	✓	190.200.0.11	cpu1511-11	CPU 1511-1 PN (1AK01-0AB0)	28:63:36:BC:D5:31	
☐	✓	190.200.0.12	et200mp-st-12	ET200MP IM155-5 ST (5AA00-0AB0)	28:63:36:BA:EC:E8	
☐	✓	190.200.0.13	et200mp-hf-13	ET200MP IM155-5 ST (5AA00-0AC0)	28:63:36:B6:A6:B3	
☐	✓	190.200.0.30	cpu1214c-30	CPU 1214C DC/DC/DC (1AG40-0XB0)	28:63:36:BD:B5:14	
☐	✓	190.200.0.31	xb213-3-31	SCALANCE XB213-3ST PN (3BB00-2AB2)	20:87:56:27:85:42	
☐	✓	190.200.0.32	et200sp-32	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D7:13	
☐	✓	190.200.0.33	et200sp-33	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D7:21	
☐	✓	190.200.0.34	et200sp-34	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D9:5C	
☐	✓	190.200.0.35	et200sp-35	ET 200SP IM155-6 PN HF (6AU00-0CN0)	28:63:36:BA:D9:75	
☐	✓	190.200.0.40		SIEMENS_Standard	20:87:56:74:E2:0A	
☐	✓	190.200.0.41		SCALANCE SC632 (2GS00-2AC2)	20:87:56:64:D2:61	
☐	✓	190.200.0.71	xp208-71	SCALANCE XP208 (0HA00-2AS6)	20:87:56:2E:E9:0C	

☐	Read	Event status	Event	Event class	Time stamp	Event details	IP address internal - affec
☐	No	Resolving	Performance of the WLAN interface: normal transmit error rate	Info	2020-01-08 09:08:38.893	0.000	190.200.0.180
☐	No	Resolved automatically	Performance of the WLAN interface: critical transmit error rate	Warning	2020-01-08 09:07:54.283	100.000	190.200.0.180
☐	No	Resolving	Application relationship: Device is connected to at least one controller	Info	2020-01-08 09:05:35.487	PNIO name of the assigned controller: cpu315-160	190.200.0.164
☐	No	Resolving	Application relationship: Device is not assigned to a controller	Info	2020-01-08 09:04:35.439	-	190.200.0.164
☐	No	Resolving	Performance of the WLAN interface: normal transmit error rate	Info	2020-01-08 09:03:38.938	0.000	190.200.0.180

Figure 4-18 Event list

The events in the event list that are displayed also depend on the views assigned to the logged-on user. This means that events are only monitored if they are associated with the configured views.

Properties

For each event in the event list, specific parameters are displayed in a table row that are explained below.

Table 4- 67 Properties in the event list

Column	Meaning
"Check box"	The selection box is used to select an event prior to editing a particular event. Multiple selections are possible. Note: By double-clicking on the selected event you open the device details ("Events" tab) of the device belonging to the event.
Read	Display indicating whether the event was read by the user with the "Events read" function. • "Yes" = Read • "No" = Not read
Event status	Display of the status that the event has in terms of the overall status of a device. • Pending: When an event that is assigned a negative overall status (every overall status except "OK" and "Not connected") is triggered for a device, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device. • Resolved automatically: An event was removed from the list of pending events is identified by the event status "Resolved automatically". Resolved events can no longer influence the overall status of devices. Pending events are automatically resolved by the following events: – Events assigned the "OK" or "Not connected" overall status from the same overall status group – Pending events of the same overall status group (regardless of the assigned overall status) • Resolved manually: A pending event that was removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually". • Not present: A triggered event that is not assigned to any overall status group or is not assigned any overall status in the group has no event status.
Event	Configured event information or event message.
Event class	Information on the class (weighting) of the event. The entries are color-coded with the following meaning: • light green = notification • dark green = information • yellow = warning • red = error
Time stamp	The "Time stamp" box provides information on the date and time of the generation of the event.

Column	Meaning
Event details	Shows the full information for each event.
IP address (affected)	Shows the IP address of the device that triggered the event.
IP address (reporting)	Shows the IP address of the device that reported to the operation the information to trigger the event.
External IP address (affected)	Shows the IP address of the NAT router for the device that triggered the event.
External IP address (reporting)	Shows the IP address of the NAT router for the device that reported the information to trigger the event to the operation.
Remarks	Store additional information, for example, about event reactions. Note: If several events are selected, an edited comment is entered for all the selected events.
Trigger	Name of the source device.
Time stamp (reported)	Time at which the SIMATIC event / alarm message was sent by the CPU with SIMATIC capability.
Event category	Specifies whether a network event or a system event is involved.
Device status	Overall status that potentially causes the event on a device.
Overall status group	Name of the overall status group to which the event is assigned.
Affected (name)	Shows the PROFINET name of the device that triggered the event.
Reporting (name)	Shows the PROFINET name of the device that reported to the operation the information to trigger the event.
Protocol	Information about which protocol supplied the event information.
Interface / slot	Provides information on the interface type being used and the interface number or on the slot, subslot and channel of the PROFINET device.

Note

Receiving SNMP traps

The operation receives SNMP traps only if the IP address of the operation is configured on the relevant devices as the trap destination.

Operator input

The following table explains the function elements of the header.

Table 4- 68 Operator controls of the header

Icon	Meaning
!	Events read By marking events as "Read", you confirm your awareness of the changed status of an active entry in the event list. No other reaction is associated with this function. Configured event reactions are triggered solely by the status change of the event.
⊥	Removes a selected pending event from the list of events pending for a device. The event then has the event status "Manually resolved".
✎	Edit remark Note: If several events are selected, an edited comment is entered for all the selected events.
✗	Delete remark
↑ ↓	Maximize / minimize By default, SINEC NMS shows up to 10 events in the event list. By maximizing the display, you expand the display of the event list to the size of the full Web page. Using the functions in the footer, you also have the option of paging through the entire event list and configuring the layout of the event list.
() ▣ ↷	Enter text to filter based on events. The entered text is searched for in all columns In the input box, text is displayed when a simple query entered in the filter template editor is active. The ▣ icon is displayed when a filter template with prefilter settings is active. The () icon is displayed when a filter template with a complex query is active.
▾	Selection of a previously created template for filtering according to events. After selection, the properties of the filter template are applied to the event list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.

Icon	Meaning
▽ ▽✓	Open the editor for configuring filter settings that can be stored in filter templates. The ▽✓ icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for event lists".
🔗 🔗	Not connected / connected to topology If the topology display is shown in the content area, you have the option of connecting the event list to this topology display. In the connected status, devices for which events of the event list were triggered are highlighted optically in the selected topology representation. The devices whose events are highlighted can be specified in the "Highlight only selected entries" check box: • Check box is enabled: Only the devices of the events selected in the event list are optically highlighted. • Check box is disabled: All devices of the current event list are optically highlighted. Using the filter settings of the event list, the number of highlighted devices can be adapted. The highlighted devices are listed in the left side area. If the automatic updating is disabled, you can call up the highlighted devices one after the other with the shortcut menu in the topology display. The order in which they are called is based on the listing of the highlighted devices in the left side area.

Prefilters in the filter templates for event lists

Event lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for event lists. You will find basic information on filter templates and the options of using complex filters in the section:
Filter templates (Page 71)

Table 4- 69 Filter settings

Box group	Filter options
Basic filter settings	Read: • Yes • No • All Event state: • All • " - " • Resolved automatically • Resolved manually • Pending Period: Filter according to events • of the last 24 hours • of the last 7 days • of the next month • of a manually entered time range
Event categories	Filter according to the origin of events: • Network events • System events

Box group	Filter options
Event classes	Filter according to the severity of events: • Notification • Information • Warning • Error
Protocols	Filter according to protocols by which the events were triggered: • ICMP • DCP • ARP • SNMP • SNMP trap • PROFINET • SIMATIC • Multiple (event was triggered by more than one protocol) • SIMATIC event messages • SIMATIC alarm messages

Functions of the shortcut menu

The shortcut menu provides the option of calling up the topology display or a view-specific topology display from the event list. In the topology display, the device is selected and shown centered that triggered the event selected in the event list. This function is not available for traps that the operation has received from unknown devices.

In addition to this, you can call the overall status group to which the selected event belongs using the shortcut menu.

Network administration 5

5.1 Policy Control Center

5.1.1 Policies

Function overview

Tasks for configuring and managing devices can be planned and enforced using a policy. The devices and tasks of a policy can be freely compiled within the framework of the existing authorizations. Before enforcing a policy and based on the available capabilities, SINEC NMS determines which tasks can actually be enforced for which of the devices. Using policy simulations, this information can also be determined without enforcing the policy. The results of policy enforcements and policy simulations are displayed in the Web interface.

Note

Do not shut down SINEC NMS while enforcing policies.

SINEC NMS must not be shut down during policy enforcement. If SINEC NMS is shut down during policy enforcement, the devices configured with these policies may become inconsistent and the aborted policies may not continue. Therefore, you should revoke or deactivate all policies before shutting down SINEC NMS.

Global and local policies

Global policies are configured in the control, then deployed to all involved operations and then enforced on these operations. Global policies are visible on the control and on the operations involved.

Local policies are configured directly on the operations on which they are to be enforced. Local policies are only visible on their associated operation, this also applies to single-node installations.

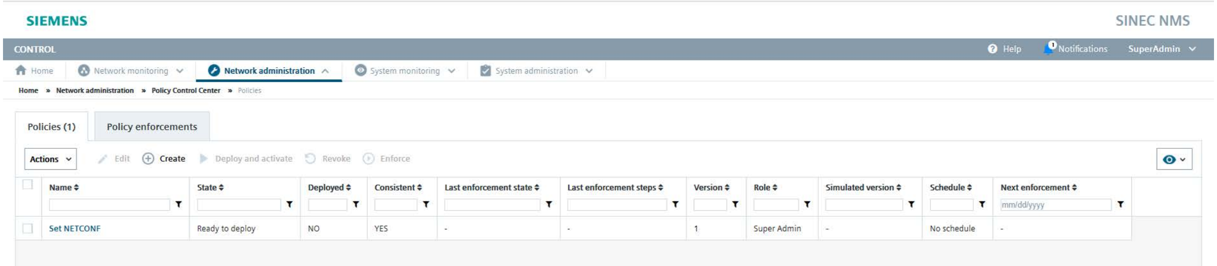
Local system-defined policies are created for tasks configured in the Configuration Cockpit.

Unlike local policies, global policies only need to be configured once centrally and can then be used for all affected operations. You set via the device areas of the policy the operations for which a global policy is used, refer to section Policy editor (Page 183).

5.1.2 User interface of the Policy Control Center

Control

The Policy Control Center is available on the page "Network administration > Policy Control Center". Global policies can be managed and enforced in the Policy Control Center.



□	Name	State	Deployed	Consistent	Last enforcement state	Last enforcement steps	Version	Role	Simulated version	Schedule	Next enforcement
											mm/dd/yyyy
□	Set NETCONF	Ready to deploy	NO	YES	-	-	1	Super Admin	-	No schedule	-

Figure 5-1 Policy Control Center on control

5.1.2.1 Policies

Policies can be configured in the "Policies" tab.

Policy properties and actions

Policy properties

The following policy properties are displayed in the columns of the Policy Control Center:

- ID

  Policy identifier assigned by SINEC NMS.

- Name

  Unique name of the policy assigned in the Policy Editor.

- State

  Displays one of the policy states described below. The tooltip of the column entry shows which state the policy has on how many operations. The ⚠ symbol is displayed for inconsistent policies.

  - Enforcing

    The policy is being enforced. Which rules are enforced for which devices is determined at the time of enforcement based on the conditions and tasks of the policy, refer to section Policy decision (Page 193).

  - Ready to deploy

    The policy has been configured with all necessary information and can be deployed to operations.

  - Activated

    The policy has been deployed to the associated operations and activated there. In this state, the policy can be enforced on the operations manually or according to a configured schedule. The simulation of the policy is also possible.

  - Deactivated

    The policy has been deployed to the associated operations and deactivated there. In this state, the policy can be neither enforced or simulated.

  - Inconsistent

    A policy that cannot be enforced or simulated because of inconsistencies in the configuration of roles, device areas, and tasks is assigned the "Inconsistent" state and must be corrected in the Policy Editor. Inconsistencies can occur, for example, if the authorizations of a policy role are subsequently changed or a selected device area no longer contains any devices. The reason for the inconsistent state of the policy is displayed in the tooltip of the ⚠ icon that appears in the Policy Editor for the affected tasks.

  - Suspended (display in tooltip)

    The "Suspended" state is displayed in a tooltip for a policy that was recognized as inconsistent by SINEC NMS. If the policy has the "Activated" or "Deactivated" state, the policy must be deleted from the affected operations using the "Revoke" action. It is then given the state "Inconsistent" and can be corrected in the Policy Editor. Policies in the "Suspended" state that have not yet been loaded on an operation do not have to be revoked and can be edited directly in the Policy Editor.

  - Unknown (display in tooltip)

    The state of the policy could not be determined.

- Deployed

  Indicates whether the policy has been deployed on at least one operation.

- Consistent

  Indicates whether the policy is consistent, refer to the "Inconsistent" state. The reason for the inconsistent state of the policy is displayed in a tooltip.

- Last enforcement state

  Indicates the last detected enforcement state of the policy on operations. The enforcement state with the highest priority is always displayed. The enforcement states are listed below according to their priority:

  - Enforcing

    The policy is being enforced. The progress of policy enforcement is expressed as a percentage in parentheses. Which rules are enforced for which devices is determined at the time of enforcement based on the conditions and tasks of the policy, refer to section Policy decision (Page 193).

  - Failed

    The policy could not be fully enforced due to a fault.

  - Skipped

    The policy could not be enforced because enforcement of the same policy was not yet complete.

  - Success

    The policy has been fully enforced.

  - Waiting

    Multiple policies cannot be enforced simultaneously on a single operation. Policies that cannot currently be enforced are in the "Waiting" state.

  The numbers in brackets indicate how many operations have the displayed enforcement state.
  Example: "Enforcing (1/5)" means that the policy will be enforced on one of five operations.

- Last enforcement steps

  Specifies the number of steps of the last policy enforcement. The numbers in brackets indicate the number of execution steps for each state:

  - Existing (light green)

    All parameters to be configured with the execution step already exist.

  - Success (dark green)

    The execution step was successfully performed.

  - Failed (red)

    The execution step has failed.

  - Skipped (black)

    The execution step was skipped.

- Version

  The current version of the policy. It is automatically increased on each saving of changes to the policy.

- Role

  Configured policy role, refer to section Policy editor (Page 183).

- Simulated version

  Version and date of the last policy simulation. If you click on the entry in the column, the simulation report is displayed, refer to section Policy reports (Page 194).

- Schedule

  Configured schedule for policy enforcements. Without scheduling, the policy can only be enforced manually.

- Next enforcement

  Date and time of the next policy enforcement according to configured policy planning.

- Description

  Description of the policy, supplementing the policy name.

- Last enforcement

  Date, time, and version of the last enforcement.

- Last change

  Name of the user who made the last change to the policy and the associated date and time.

- Duration of last enforcement

  Duration of last enforcement of the policy on an operation.

- Average enforcement time

  The average duration of policy enforcements on the operations, based on the last policy version.

- Type

  Global, local or local system-defined policy, refer to section Policies (Page 177).

- Strategy

  Specifies whether the policy enforcement is coordinated between the devices of an operation time-wise. For more detailed information, refer to section Policy strategies and error handling procedures (Page 188).

- Number of rules

  Number of rules configured in the Policy Editor.

Policy actions

The following functions are available via the "Actions" drop-down list:

- Edit

  Opens a policy in "Ready to deploy" or "Inconsistent" state for editing in the Policy Editor, refer to section Policy editor (Page 183). Policies in the "activated" and "deactivated" states are opened read-only in the Policy Editor. These can only be edited after being revoked.

- Create

  Creates a new policy and opens the Policy Editor, refer to section Policy editor (Page 183). Once a policy has been saved with all necessary information, it is given the state "Ready to deploy". The policy must now be deployed to operations and activated before it can be enforced or simulated on these.

- Copy

  Copies the properties of the selected policy to a new policy. The Policy Editor will then be opened to enter the name for the new policy. The name of the policy must be unique.

  When you copy a policy, some properties such as the device areas or the schedule are reset.

- Delete

  Deletes the selected policy. Only policies in the states "Ready to deploy" and "Inconsistent" can be deleted. When a policy is deleted, all historical data of this policy is also deleted.

- Deploy and activate

  Deploys a policy with the state "Ready to deploy" to the operations assigned to the device areas selected in the policy and sets the policy to the state "Activated". In this state, the policy can be enforced according to a configured schedule or manually. The simulation of the policy is also possible.

- Deploy and deactivate

  Deploys a policy with the state "Ready to deploy" to the operations assigned to the device areas selected in the policy and sets the policy to the state "Deactivated". In this state, the policy can be neither enforced or simulated.

- Activate

  Sets a policy that is deployed to operations and has the state "Deactivated" to the state "Activated". In this state, the policy can be simulated and/or enforced.

- Deactivate

  Sets a policy that is deployed to operations and has the state "Activated" to the state "Deactivated". In this state, the policy can be neither enforced or simulated.

- Revoke

  Sets a policy with the state "Activated" or "Deactivated" to the state "Ready to deploy" and deletes the policy from operations so that the policy can be edited again or deployed to operations. A policy with the "Enforcing" state cannot be revoked.

- Enforce

  Manually starts the enforcement of a policy in "Activated" state. There must be at least 1 minute between the start of policy enforcements.

  Note that the devices affected by the policy and the enforced rules depend on the time stamp of the policy enforcement, refer to section Policy decision (Page 193).

- Simulate

  Creates a simulation report for the current version of the selected policy. The generated report can be accessed via the entry in the "Simulated version" column. Only policies with the status "Activated" can be simulated. There must be at least 1 minute between the start of policy simulations.

  For information on simulation reports, refer to section Policy reports (Page 194).

- Show historical data

  Calls the tab "Policy enforcements" and displays information about already performed enforcements of the policy selected in the "Policies" tab.

Policy editor

The Policy Editor opens when you create, open for editing or copy a policy in the Policy Control Center. Configure a policy in the Policy Editor.

Basic settings

Configure the following basic settings in this area of the editor:

- Name

  Unique name of the policy.

- Description

  Optional description of the policy, in addition to the policy name.

- Role

  The selected policy role decides which users are allowed to work with this policy. Only users who have the selected policy role or a role that is superior to the policy role are allowed to work with the policy. The authorizations a user has when working with policies are defined in the authorization management.
  The policy role also defines the device areas and the configurable tasks of the policy. Only tasks for which the necessary rights for the device configuration are available in the policy role can be selected during the rule configuration. Furthermore, after selection of the policy role, the policy only applies to device areas that are assigned to this role. The roles of the user and those roles that are subordinate to the roles of the user are available for the selection of the policy role.

- Version

  The current version of the policy. It is automatically increased on each saving of changes to the policy.

- Last edited by

  User who made the last policy change and time stamp for when the change was made.

- Device areas

  By default, the policy refers to the device areas assigned to the selected policy role. You can further restrict these device areas with the setting "Device areas". The device areas cannot be extended beyond the device areas of the selected policy role. During the loading of the policy, SINEC NMS uses the selected device areas to determine the operations to which the policy is loaded. If you select no device areas, the policy relates to the device areas of the policy role. You configure the device areas of roles on the "System administration > Device·areas" page of the control.

- Conditions

  With policy conditions, you select devices from the configured device areas based on properties such as IP addresses or article numbers. If you do not configure any policy conditions, the policy relates to all devices of the configured device areas.

  Wildcards can be used in some conditions. The following wildcards can be used in these conditions:

  – * (Any number of characters including spaces)

  – ? (The character preceding this wildcard can occur not at all or once, including spaces)

  – . (Exactly any one character including spaces)

  If the characters above are not to be used as wild cards they must follow a "\" e.g. "\?".

Note

IP addresses in policy conditions

In order to identify devices in policy conditions via IP addresses, the IP addresses through which SINEC NMS can reach the devices must always be specified. If there is a NAT router between an operation and a device, the external IP address of the device that is present on the NAT router for the device must be specified. This is displayed on the "Network monitoring > Devices" page of the control as well as on the "Network administration > Configuration·Cockpit" page of the operation.

Note

Using the "IPV4_CIDR" policy condition

Policy conditions of "IPV4_CIDR" type are specified in CIDR format. Using such a condition, you can check whether the portion of the specified IP address determined by the number of bits matches that of the checked IP addresses.

Example:

IPV4_CIDR EQUALS 192.168.1.1 / 16: Devices and interfaces whose IP addresses begin with 192.168 meet the policy condition.

Note

Using the "CONNECTED_TO_MAC" policy condition

The "CONNECTED_TO_MAC" policy condition can be used to identify an interface connected to a specific device. To specify this device, use the MAC address of the device and not the MAC address of one of the device's interfaces.

- Strategy

  The policy strategy is used to specify whether the enforcement of the policy is synchronized between the devices of an operation. For more detailed information, refer to section Policy strategies and error handling procedures (Page 188).

- Schedule

  Sets a schedule for policy enforcements. If you do not configure a schedule, the policy can only be enforced manually with the "Enforce" action.

Rule configuration

In the rule configuration, you can define rules whose tasks are applied to the devices during policy enforcement. A policy contains at least one rule, a rule contains at least one task. Using the "Add rule" button, a rule can be configured based on the following settings:

- Rule name

  Entering the name for the rule. Rule names must be unique within a policy.

- Rule description

  Description of the rule, supplementing the rule name.

- Rule type

  Configuration as rule for devices or as rule for interfaces. Depending on the selected rule type, tasks are available for devices or for device interfaces.

- Rule strategy

  If the "Synchronized" policy strategy has been selected in the basic settings, you can define the processing sequence of the devices for each rule using the rule strategy. For more detailed information, refer to section Policy strategies and error handling procedures (Page 188).

- Device conditions

  The devices or interfaces to which the rule is to be applied are identified by the device properties specified here.

- Interface conditions

  The interfaces to which the rule is to be applied are identified by the device properties specified here. This setting is only available for interface rules.

- Capabilities required for rule

  Display of all capabilities that a device must support for the execution of all tasks of the rule. The capabilities that are required for the individual tasks are displayed in the task selection dialog.
  The functions supported by a device are displayed in the "Discovered capabilities" tab of the device details in the Configuration Cockpit of the relevant operation. The capabilities are discovered in the context of the network scan and can be re-discovered via the action "Discover capabilities" in this tab.

- Rule error handling

  Specifies how to proceed in case of an error in the execution of a task for a device. For more detailed information, refer to section Policy strategies and error handling procedures (Page 188).

- Add task

  When adding a task, first select the desired setting and then the parameter to be configured for it, for example "Set RADIUS server" setting, IP address "192.168.1.1". Mandatory parameters are preselected, optional parameters can also be selected if required. The available tasks depend on the configured policy role and the selected rule type. In the dialog for selecting the tasks, the "Capability" column displays which capability a device must support for the execution of the individual tasks. Function descriptions of the individual tasks are displayed in the "Description" column.

Note

Policy task "Load config file to device"

When the "Load config file to device" policy task is enforced, the SNMP/CLI login data of the user used in the configuration file are overwritten by the login data available in the device credential repository of the respective operation for these devices before they are loaded onto the device. This ensures that devices remain accessible by SINEC NMS even after older device configurations have been restored. When working with device configurations, note the information in the readme file concerning the compatibility with different devices.

Note

Policy task "Set CLI commands"

You can create CLI scripts in a CLI editor and execute them for devices using the "Set CLI commands" policy task. The following parameters can be used in the CLI editor:

- $User: user that is configured for the device in the device credential repository.
- $Pass: password configured for the device in the device credential repository.
- $IP: IP address of the device
- $Name: Name of the device.
- $MAC: MAC address of the device
- $Date-Time: Current date and current time of day.

Note

Password configuration in policy tasks "Set local user", "Set SNMP v3 user" and "Set SNMP v3 user password"

In the password parameters of the "Set local user", "Set SNMP v3 user" and "Set SNMP v3 user password"policy tasks, you can alternatively generate a password using the character string "Random([password length])" from SINEC NMS, e.g. with "Random(12)". The password is generated randomly based on the following password guidelines:

- Minimum length: 8 characters (default setting)
- Maximum length: 19 characters
- At least 1 uppercase letter
- At least 1 special character
- At least 1 number
- Permitted special characters: !#$%^&*()_+-={}[]',<.>/`~@.

If no password length or a password length smaller than 8 characters is specified, 8 characters are used as the password length. If a password length greater than 19 characters is specified, 19 characters will be used as the password length. The passwords are loaded onto the devices after the policy tasks have been executed and updated in the SINEC NMS device credential repository for the devices.

Note

Policy task "Load HTTPS certificate to device"

With the "Load HTTPS certificate to device" policy task, you can load HTTPS certificates onto devices that are automatically classified as trusted by SINEC NMS if the "Trust device after certificate download" parameter has been set to "YES" in the policy task. If you are not using the Control or Operation PC for device access, the SINEC NMS root CA certificate and the issuing CA certificate of the respective operation must be stored on the PC from which the device is accessed. You can find the certificates in the installation directory of the control under "SINECNMS\public_certificates". The root CA certificate must be stored in the Windows Certificate Manager under "Trusted Root Certification Authorities > Certificates", the issuing CA certificate under "Intermediate Certification Authorities > Certificates".

The configured conditions and tasks of the policy as well as the time of policy enforcement determine which rules are applied to which devices. The procedure according to which SINEC NMS compiles policy rules for devices can be found in section Policy decision (Page 193).

Policy structure

The policy structure is displayed in the left pane of the Policy Editor and provides an overview of all configured rules and the tasks they contain. Tasks that cannot be performed due to missing authorizations, for example, are marked with the symbol ⚠ as inconsistent.

The order in which the rules and tasks of the policy are executed can be changed in the policy structure using a drag-and-drop operation. Tasks can be moved within their rule.
The Policy Editor must be updated after a change to the rule or task sequence. A dialog with the button "Refresh" is displayed for this purpose. If you do not click the "Refresh" button in

this area but instead the "Discard" button, the state that existed before the changes were made is restored.

5.1.2.2 Policy enforcements

The "Policy enforcements" tab displays information about the policy enforcements created in the "Policies" tab. If you click on the entry in the "Enforcement report" column, the Policy Enforcement report is displayed, refer to section Policy reports (Page 194).

5.1.3 Policy strategies and error handling procedures

Policy strategies

The policy strategy is used to specify whether the enforcement of the policy is coordinated between the devices of an operation time-wise.

Note

Enforcement of policies, rules and tasks

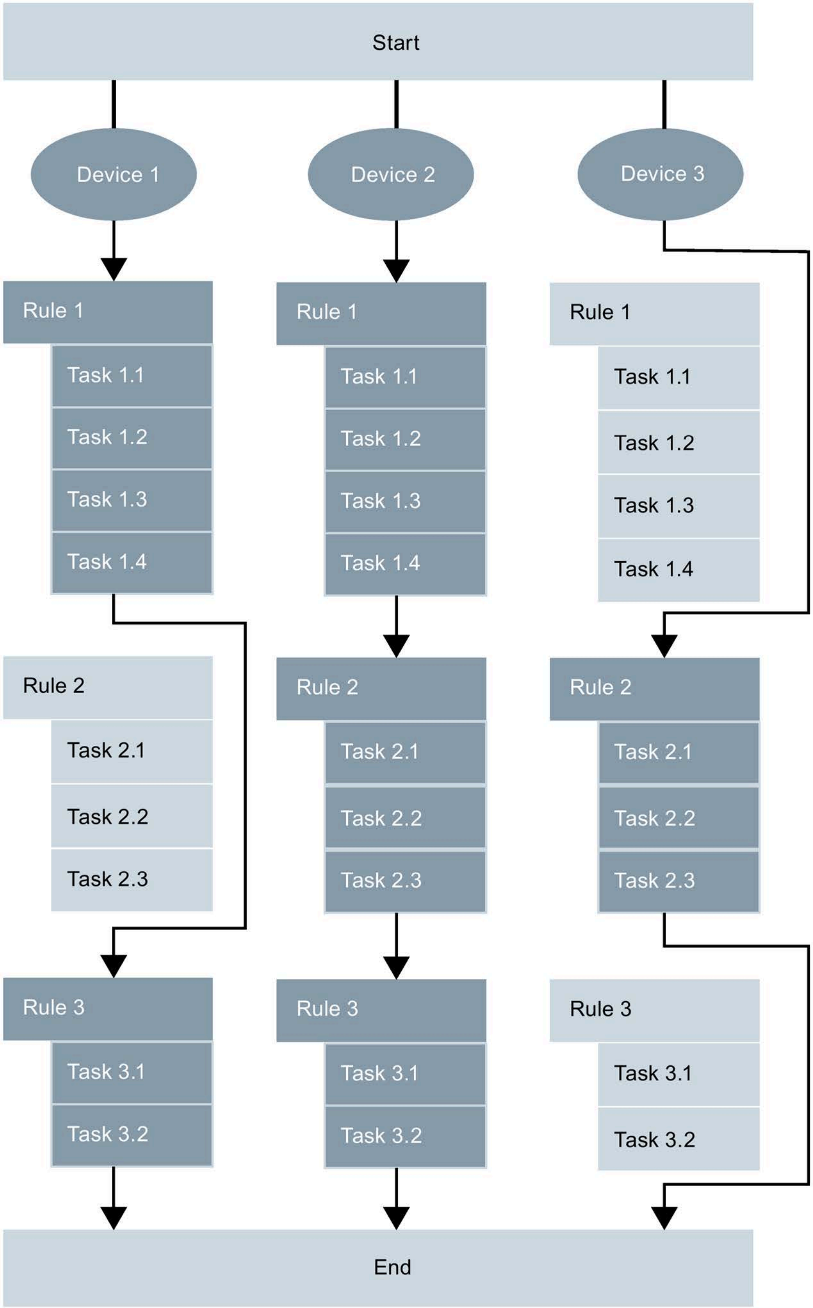
The policies on one operation are enforced independently of the policies on other operations. This applies to both policy strategies.

The rules of a policy and the tasks of a rule are executed sequentially for a device.

One of the following policy strategies may be selected for a policy:

- Not synchronized

  The policy is enforced simultaneously for all devices of the operation. As soon as all tasks of a rule have been executed for a device, the next rule of the policy is executed for the device. This strategy can shorten the enforcement duration of policies, but depending on the tasks at hand, the functionality of the network can be temporarily impaired. This is the case, for example, if the firmware update for a switch is performed at an unfavorable time and the device must then be restarted.



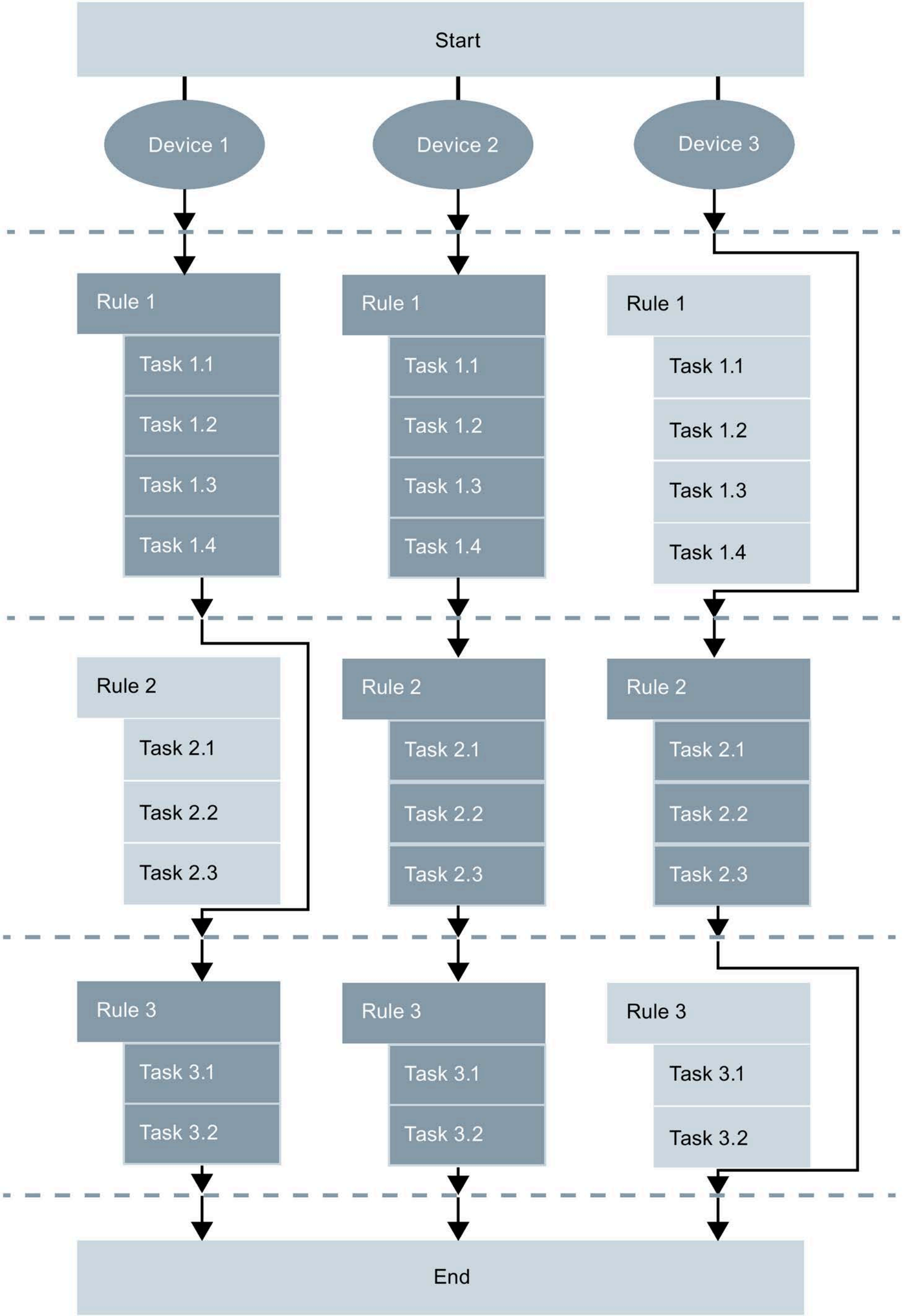
Dark grey	Enforcing

Light gray Not enforcing

Figure 5-2 "Not synchronized" policy strategy

- Synchronized

  The policy enforcement only continues with the next rule after a rule has been enforced for all devices.



Dark grey Enforcing

Light gray	Not enforcing

Figure 5-3 "Synchronized" policy strategy

With the "Synchronized" policy strategy, the Rule strategy to be used can be configured for each rule. The order in which the rule is applied to the devices is specified using the rule strategy:

– Topology based

  The rule is applied to the devices based on the arrangement of the devices in the topology. Devices that are more device hops away from the operation are processed before devices that are fewer device hops away from the operation. Devices with the same distance to the operation are processed simultaneously. To use this option, the reference topology must be created on the operation.

– Sequential

  The rule is applied to the devices one after the other.

– Parallel

  The rule is applied in parallel to the devices.

Method for Rule error handling

For each rule, it is also determined how to proceed in case of an error in the execution of a task for a device. The selected error handling procedure is related to the selected policy and rule strategy.

- On error stop policy enforcement for device

  The enforcement of the policy is completed for the device after the task in which the error occurred.

- On error continue with next rule for device

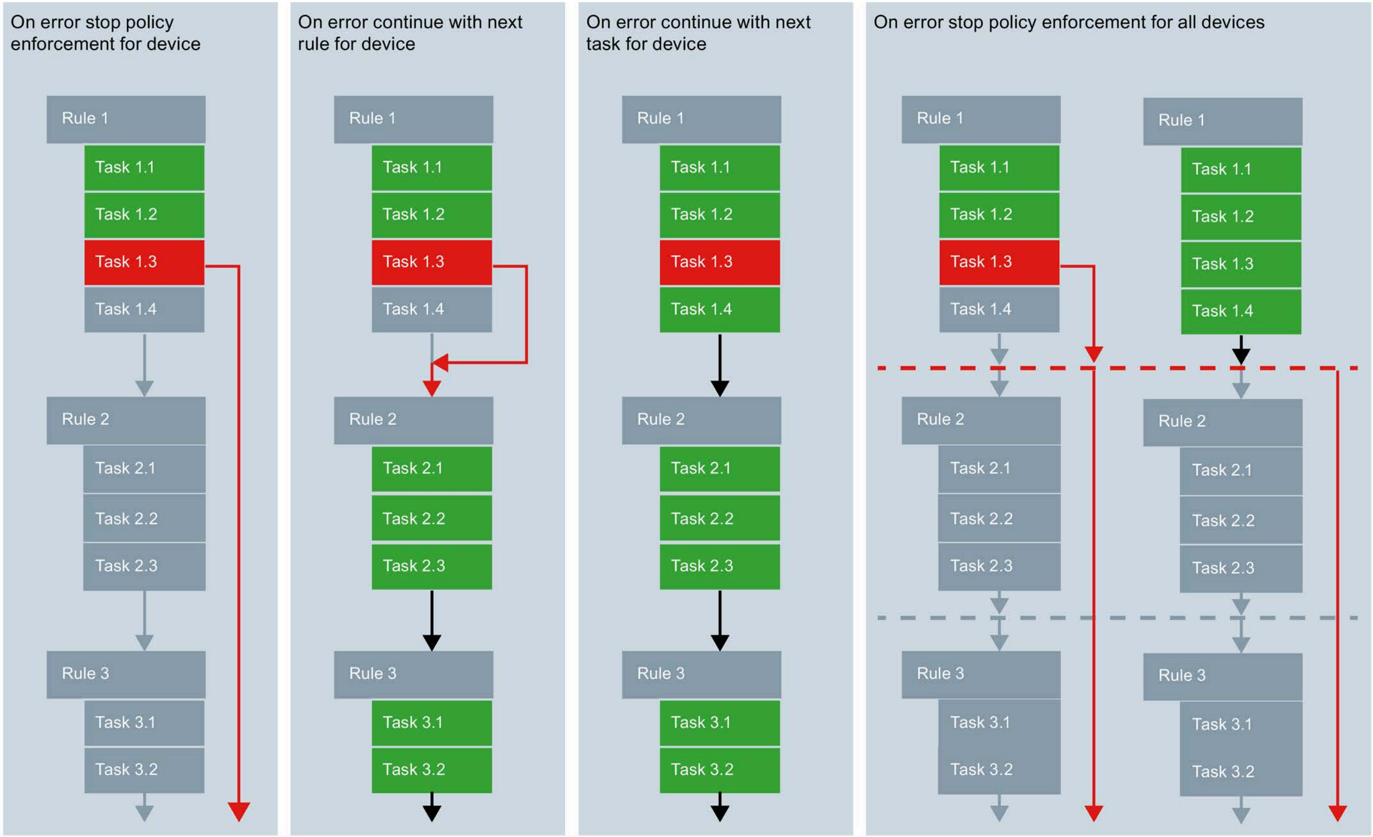
  The enforcement of the policy for this device continues with the next rule. Additional tasks of the rule in which the error occurred are no longer processed for the device.

- On error continue with next task for device

  The enforcement of the policy for this device continues with the next task. If no other task is available in the rule, the policy enforcement continues with the task of the next rule.

- On error stop policy enforcement for all devices (only for policies with the "Synchronized" policy strategy)

  The enforcement of the policy is stopped for the device for which the error occurred after the affected task. For all other devices of the operation, the policy is stopped after enforcement of the rule.


On error stop policy enforcement for device
On error continue with next rule for device
On error continue with next task for device
On error stop policy enforcement for all devices
Rule 1
Task 1.1
Task 1.2
Task 1.3
Task 1.4
Rule 2
Task 2.1
Task 2.2
Task 2.3
Rule 3
Task 3.1
Task 3.2

Green	Fully enforced
Red	Fault in enforcement

Figure 5-4 Method for Rule error handling

5.1.4 Policy decision

At the time at which the enforcement of a policy is initiated on an operation, SINEC NMS decides which rules of the policy are relevant for which devices of the operation. Only devices for which configuration access is allowed and that originate from the configured device areas and meet the policy conditions are included in the policy decision. For these devices, SINEC NMS checks per rule whether the device and interface conditions contained in the rule are fulfilled and whether these devices have the capabilities required for the execution of all tasks of the rule. Devices that meet these conditions are assigned the rule for enforcement.

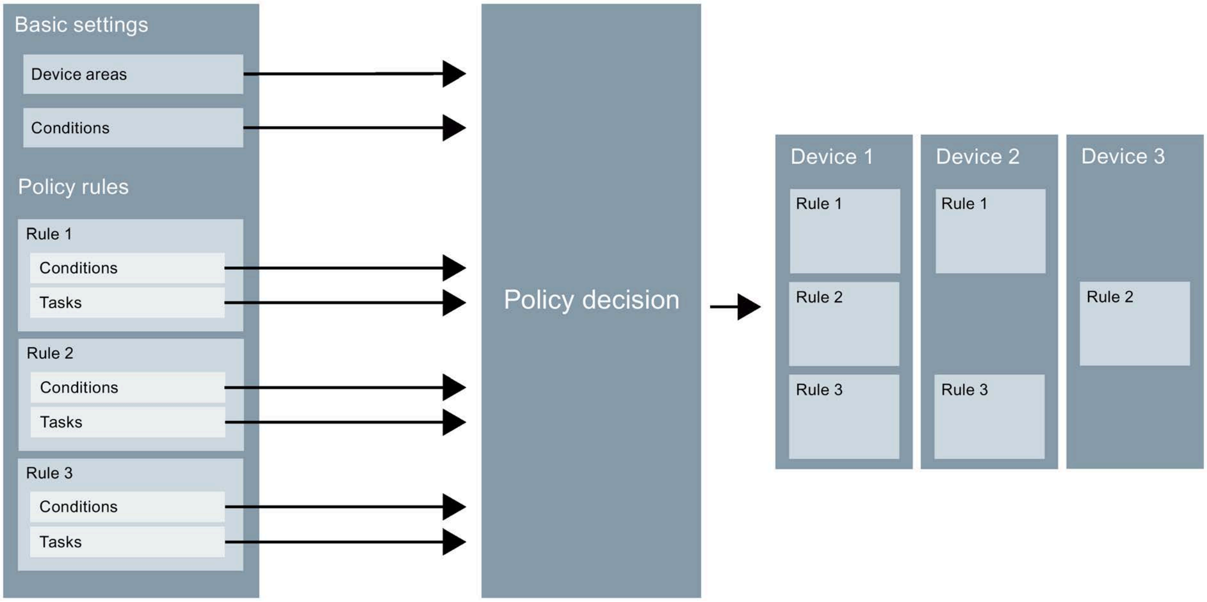


Figure 5-5 Policy decision process

The capabilities supported by a device are discovered during the network scan, for example, and displayed in the "Discovered capabilities" tab of the device details in the Configuration Cockpit of the affected operation. The discovery of the capabilities may be started using the action "Discover capabilities" in the Configuration Cockpit.

The result of the compilation of rules for devices may vary depending on the time of the policy decision.

5.1.5 Policy reports

Enforcement reports

Enforcement reports document the result of the policy enforcements.

Enforcement reports are automatically generated during the enforcement of policies and can be opened in the "Policy enforcements" tab by clicking on the text in the "Enforcement report" column.

The enforcement report of a policy is divided into the "General" and "Enforcement report" areas.

The "General" area contains a summary of the configured policy properties, times for enforcing the policy and the number of devices to which the policy was applied. The policy editor with all configured policy properties is displayed write-protected using the button "Display policy configuration".

The "Enforcement report" area documents the achieved enforcement result of the policy per rule. The meaning of the table columns is as follows:

- Device: Device name and IP address of the device to which the task of the rule was applied.
- Device type: Device type of the device to which the task of the rule was applied.
- Enforcement order: The order in which the rule was applied to the devices.
- Port: Port to which the task of the rule was applied.
- Task: Name of the task that was applied to the device or interface.
- Parameter: Parameter that was configured according to the task.
- Value: Value set according to the task on the device. Internal values such as created keywords for a device configuration are not displayed in the enforcement report.
- Enforcement result: Indication of whether the parameter value could be successfully set on the device according to the task. If a value to be set is already available on a device, it is not set again on the device. If a value could not be set successfully, a corresponding fault text is displayed.

Simulation reports

The result of the policy can vary depending on the time at which it is enforced, refer to section Policy decision (Page 193). Simulation reports allow you to predict the outcome of policy enforcements without having to enforce the policy itself. Simulation reports indicate which tasks would be applied to which devices or interfaces if the policy were executed at the time the policy simulation was started.

Simulation reports are almost identical in content to enforcement reports. In contrast to enforcement reports, simulation reports contain no information about the enforcement result.

Simulation reports can be created in the "Policies" tab via the "Simulate" action. To open the simulation report, click on the entry in the "Simulated version" column.

5.1.6 Policy Control Center on operations

Operation

The Policy Control Center on Operations allows local policies to be managed and enforced. The configuration options and mechanisms for compiling policy rules for devices described for the Policy Control Center on the control applies analogously to the Policy Control Center on operations.

Local policies are only visible on the associated operations and not in the control. This also applies to single-node installations.

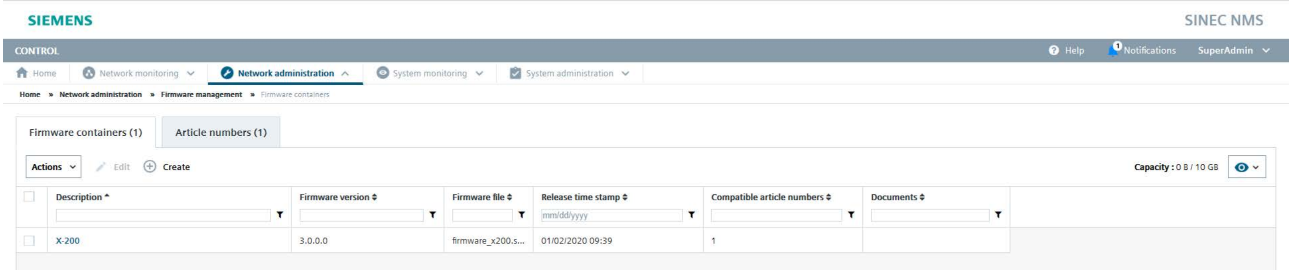
Global policies which are loaded on an operation are visible in the Policy Control Center of this operation and their enforcement can be stopped there. No additional actions are available for global policies on operations.

The type of this policy is displayed in the optional "Type" column of the Policy Control Center.

5.2 Firmware management

Control

Firmware management is available on the "Network administration > Firmware management" page.



□	Description	Firmware version	Firmware file	Release time stamp	Compatible article numbers	Documents
□	X-200	3.0.0.0	firmware_x200.s...	01/02/2020 09:39	1	

Figure 5-6 Firmware management

In the firmware management, you can manage firmware files and mark them with tags. The tags can be used in the configuration of 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 made available to operations automatically. Each change to the firmware containers in the control is automatically synchronized with the operations. For larger changes to the firmware containers, synchronization with the operations may take some time.

Structure of firmware containers

Firmware containers are set up as follows:

- Firmware file
  Firmware file that can be uploaded to SINEC NMS and transferred to devices there. For RUGGEDCOM ROS devices, one firmware file consists of several files. Several firmware files can be added to a firmware container for these devices.
- Properties
  Firmware version, article numbers of compatible devices, compatible firmware and hardware version, release date and time, etc. For SCALANCE devices of the current generation (with firmware files in .sfw format) as well as for RUGGEDCOM ROS devices and for RUGGEDCOM ROX2 devices, SINEC NMS automatically reads all specified properties from the firmware files when uploading the firmware files, with the exception of the compatible firmware and hardware versions, if these are available in the firmware files. For RUGGEDCOM ROS devices, SINEC NMS reads the properties from the "Main.zb" file.
- Documentation

  Documents such as version information that can be uploaded to SINEC NMS and added to the firmware container.

5.2.1 Firmware containers

All firmware containers available in SINEC NMS are displayed on the page "Network administration > Firmware management > Firmware containers". Firmware containers can be managed, imported and exported on this Web page.

Note

Firmware management for RUGGEDCOM ROS devices

When importing firmware files for RUGGEDCOM ROS devices, SINEC NMS reads the board type IDs and derives the devices compatible with the firmware files. Make sure that these board type IDs correspond to the RUGGEDCOM ROS devices with which the firmware files are to be compatible.

Properties

The properties of firmware containers are displayed in the following columns:

- Description

  Description assigned in the editor for firmware containers.

- Firmware version

  The firmware version is read by SINEC NMS when uploading firmware files. When reading out, SINEC NMS normalizes the firmware version to make it comparable with other firmware versions. The firmware version can be adapted manually in the editor for firmware containers, see paragraph "Editor for firmware containers". If a device has more than one firmware container for firmware download, the firmware container with the latest firmware version is used.

- Firmware file

  File name of the contained firmware files.

- Release time stamp
  Date and time of the firmware release. The release time stamp is read out by SINEC NMS when uploading the firmware files and can be changed in the editor for firmware containers, refer to section "Editor for firmware containers".

- Compatible article numbers

  Number of article numbers of the devices with which the firmware files of the firmware container are compatible. The compatible article numbers are read out by SINEC NMS when the firmware files are uploaded and can be edited manually in the editor for firmware containers, refer to section "Editor for firmware containers".

- Documents

  The number of documents such as version information added in the editor for firmware containers, see the "Editor for firmware containers" section.

Actions

The following functions are available via the "Actions" drop-down list:

- Edit

  Opens the editor for the selected firmware container, see the "Editor for firmware containers" section.

- Copy

  Opens the editor for copying the selected firmware container. The firmware version must be changed in the opened editor and must be unique for the article numbers of the firmware container.

- Create

  Opens the editor for creating a new firmware container, see the "Editor for firmware containers" section.

- Download documents

  Downloads the document of the selected firmware container. If several documents are stored in a firmware container, you can select the document to be loaded.

- Edit article number repository

  The article number repository contains the article numbers available for assignment in the editor for firmware containers, refer to section "Editor for firmware containers". When uploading firmware files to SINEC NMS, SINEC NMS reads the article numbers compatible with the firmware file and adds them to the article number repository. Once the article number repository has been opened, article numbers can also be added manually. In the "Device type" text box, you can specify the name of the device to which the article number refers.

- Import

  Opens a dialog for importing firmware containers that were exported from SINEC NMS.

- Export

  Exports the selected firmware containers as ZIP file.

- Delete

  Deletes the selected firmware containers from the firmware management.

Editor for firmware containers

The editor for firmware containers opens when you create or edit a firmware container. In this editor, you select the firmware files, configure the properties of the firmware container and add any existing documents to the firmware container.

- Description

  Description of the firmware files of the firmware container.

- Release time stamp

  Date and time of the firmware release. The release time stamp is read out by SINEC NMS when uploading the firmware files and can be changed manually in this field.

- Version

  The firmware version is read by SINEC NMS when uploading firmware files. When reading out, SINEC NMS normalizes the firmware version to make it comparable with other firmware versions. The firmware version can also be entered and changed manually in this field. If a device has more than one firmware container for firmware download, the firmware container with the latest firmware version is used.

- Compatible firmware version

  Firmware version that must be installed on devices at the least in order for the firmware version of the firmware container to be installed. The compatible firmware version can be manually configured by the user in this field.

- Compatible hardware version

  Firmware version that must be installed on devices at the least in order for the firmware version of the firmware container to be installed. The compatible hardware version can be manually configured by the user in this field.

In the "Firmware file and documents" tab, you select the firmware files and optional documents such as version information.

- "Firmware file" area:

  You can select the firmware files for the firmware container in this area. When firmware files are uploaded, the firmware version, the article numbers of compatible devices and the release time stamp, if available, are read out. The order of the firmware files in the list determines the order in which they are loaded to the devices. You can adjust the order of the firmware files using the "Move up" and "Move down" buttons.

  A maximum of 3 firmware files can be added per firmware container. Files in *.exe, *.bat, *.vbs and *.com formats cannot be added.

  If a firmware file is added to a firmware container where article numbers are already available, you can use one of the following options to decide how to handle the article numbers for the firmware container:

  – Keep: Keeps the article numbers and device types of the firmware container. The article numbers and device types read from the firmware file are ignored.

  – Replace: Removes all article numbers and device types from the firmware container and adds the article numbers and device types read from the firmware file to the firmware container.

  – Merge: Adds to the firmware container the article numbers and device types that are not yet included in the firmware container. Article numbers and device types already present in the firmware container are not affected by this action.

- "Documents" area:

  In this area, you can select documents such as release notes for the firmware container. A maximum of 10 documents can be added for each firmware container. Files in *.exe, *.bat, *.vbs and *.com formats cannot be added. The maximum permitted file size per document is 10 MB. The names of the added documents must be unique within a firmware container.

In the "Compatibility" tab, the article numbers of the devices that are compatible with the selected firmware file are displayed. These article numbers are read by SINEC NMS from the uploaded firmware files. For the article numbers, the device types configured in the

article number repository are displayed. Device types configured for article numbers in this tab are stored in the article number repository.
The following operator controls can be used to manually configure the assignment of article numbers to the firmware file:

- Add

  Opens the article number repository from which you can use check boxes to select article numbers of the devices that are compatible with the firmware files of the firmware container. If the desired article number is not available in the article number repository, you can add the article number to the article number repository and then assign it to the firmware file.

- Delete

  Deletes the selected article numbers and device types from the firmware container. The article numbers and their device types are then still available in the article number repository.

5.2.2 Article numbers

The Web page "Network administration > Firmware management > Article numbers" contains an article number-based list of the available firmware containers. Firmware containers without assignment to article numbers are not displayed. Using tags you can, for each article number, mark firmware versions that are relevant for devices with this article number.

Operator controls

In the header, the following operator controls are available:

- Edit tags

  Opens a dialog in which you can assign user-defined tags to the available firmware versions of the article number. The user-defined tags can be used in policies and in the Configuration Cockpit to determine the firmware versions to be loaded.

- Set reference version

  Opens a dialog where you can select the reference firmware version for the selected article numbers. Only firmware versions that are available for all selected article numbers are available for selection.

- Export as CSV file

  Exports the selected entries to a CSV file.

Properties

The following properties are displayed:

- Article number

  Article number of the devices with which the firmware containers of the table row are compatible. The compatibility of firmware containers with article numbers is defined in the editor for firmware containers, refer to section Firmware containers (Page 197).

- Device type

  Designation of the devices to which the article number refers. Device types are assigned to article numbers in the article number repository, refer to section Firmware containers (Page 197).

- Available firmware versions

  Listing of firmware versions of all firmware containers with which the article number is compatible. The compatibility of firmware containers with article numbers is defined in the editor for firmware containers, refer to section Firmware containers (Page 197).

  If a device (article number) has more than one firmware container for firmware download, the firmware container with the latest firmware version is used.

- Latest firmware version

  Firmware version that has the highest version identifier among the firmware versions available for the article number. If the option to select the most recent firmware version is selected to configure the firmware tasks in policies or in the Configuration Cockpit, the firmware version displayed here is loaded to devices. The latest firmware version will also be used if several firmware container are possible for a device.

- Reference firmware version

  Select the reference firmware version for one or more article numbers. If the option to select the reference firmware version is selected to configure firmware tasks in policies or in the Configuration Cockpit, the firmware version that was selected for these devices in the present tab as the reference firmware version is loaded to devices.

- User-defined tags

  Specification of user-defined tags for the available firmware versions. If a user-defined tag is used to configure firmware tasks in policies or in the Configuration Cockpit, the firmware version that was selected for devices in the present tab with this user-defined tag is loaded to the devices. A maximum of 10 user-defined tags can be assigned to an article number.

5.3 Communication management

Control

You can create communication relations in Communication Management. A communication relation describes which communication partners may communicate via which services and which security devices are used to secure this communication. Communication relations are used by SINEC NMS to generate firewall rules, which you can then load onto the security devices involved. For information on creating communication relations, refer to section Communication relations (Page 202).

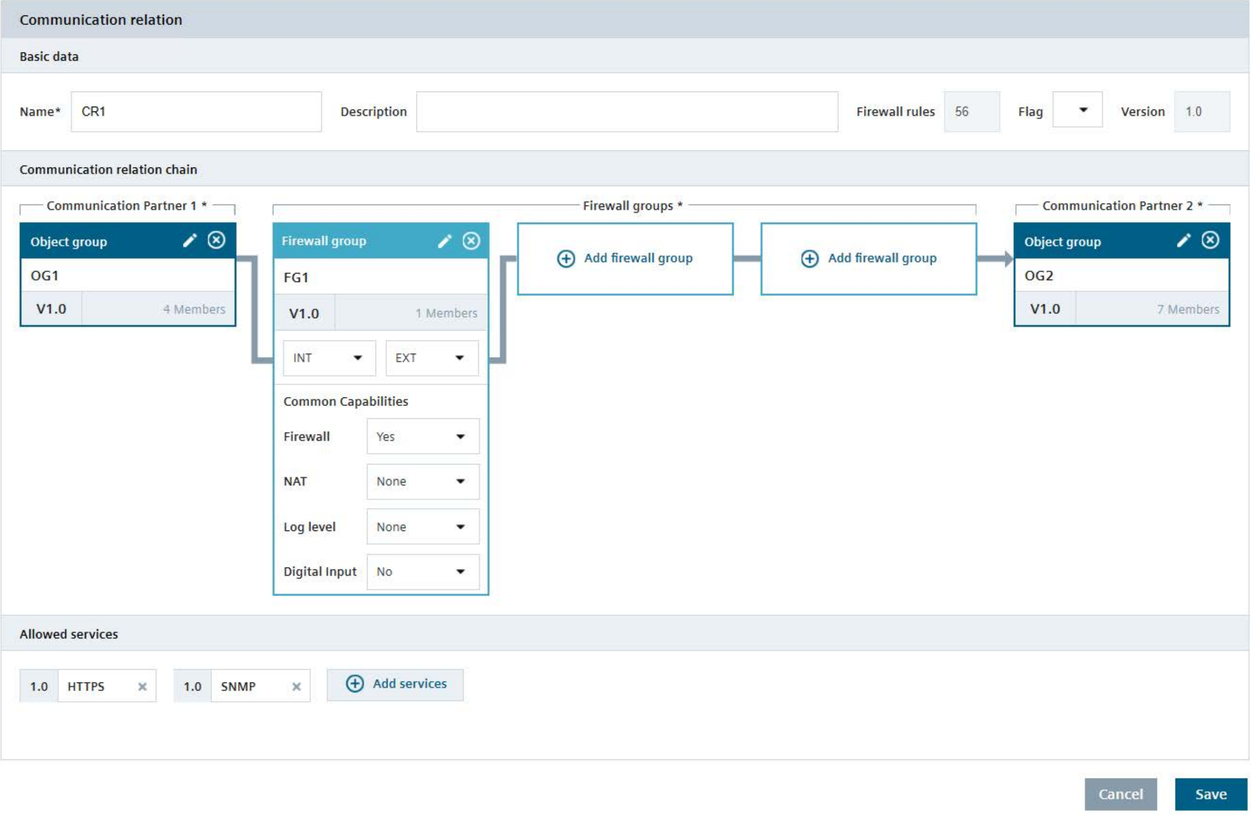
Communication parties are grouped into object groups. This makes it possible to describe the communication between several partners using a single communication relation. For information on creating object groups, refer to section Object groups (Page 211).

Firewall devices that are to receive the same firewall rules are grouped into firewall groups. For information on creating firewall groups, refer to section Firewall groups (Page 214).

5.3.1 Firewall/NAT

5.3.1.1 Communication relations

You reach this page in the navigation of the control under "Network administration > Communication management > Firewall/NAT > Communication relations". The following figure shows the editor for communication relations.



Communication relation

Basic data

Name* CR1 | Description | Firewall rules 56 | Flag | Version 1.0

Communication relation chain

Communication Partner 1 *
Object group
OG1
V1.0 4 Members

Firewall groups *
Firewall group
FG1
V1.0 1 Members
INT | EXT

Common Capabilities
Firewall: Yes
NAT: None
Log level: None
Digital Input: No

Communication Partner 2 *
Object group
OG2
V1.0 7 Members

Allowed services

1.0 HTTPS | 1.0 SNMP

Figure 5-7 Communication Relation Editor

All communication relations that been created are shown on the page "Network administration > Communication management > Firewall/NAT > Communication relations". Communication relations can be managed, enabled and disabled via the operator controls of the header. SINEC NMS generates firewall/NAT rules from activated communication relations, which can be displayed on the page "Network administration > Communication management > Firewall/NAT > Relation enforcements" and loaded on the firewall devices involved, see section Relation enforcements (Page 208).

Properties

The properties of communication relations are displayed in the following columns:

- Flag

  Color coding for visual categorization and differentiation from other communication relations. The coding has no effect on the functionality and the generated rule set of a communication relation.

- Enabled

  Indicates whether the communication relation is enabled or disabled. Communication relations can be enabled and disabled via the operator controls of the header.
  SINEC NMS only generates firewall rules from enabled communication relations.

- Name

  Unique name of the communication relation assigned in the editor for communication relations.

- State

  The status of the communication relation is formed from the states of contained object groups and firewall groups and determines whether a communication relation can be executed. The status with the highest priority determines the status of the communication relation. In the following, the states are listed according to their priority:

  - Outdated

    There is a higher version available for a contained object or firewall group. No firewall rules can be generated from a communication relationship in this state. Open the communication relation and click on the "Update" button in the editor to transfer the higher version to the communication relation.

  - Inconsistent

    A contained object or firewall group is in the "Inconsistent" state. No firewall rules can be generated from a communication relationship in this state. Follow the instructions in the following sections to set the "OK" status in the affected object or firewall group.

    Object groups: See section Object groups (Page 211).

    Firewall groups: See section Firewall groups (Page 214).

  - Update

    A contained object or firewall group is in the "Update" state. Firewall rules can be generated from the communication relationship. Follow the instructions in the following sections to set the "OK" status in the affected object or firewall group.

    Object groups: See section Object groups (Page 211).

    Firewall groups: See section Firewall groups (Page 214).

  - OK

    All contained objects or firewall groups are in the "OK" state. Firewall rules can be generated from the communication relationship.

- Communication partner 1

  Name of the object group whose devices establish communication to Communication partner 2. The "ANY" communication partner means that every device may establish communication. Even devices that are not members of an object or firewall group. Communication partner 1 can be selected in the editor for communication relations.

- Firewall groups

  Names of the firewall groups whose devices are used for communication between the communication partners. The firewall groups can be selected in the Communication Relation Editor.

- Communication partner 2

  Name of the object or firewall group to whose devices the communication is established. The "ANY" entry means that the communication to every device may be established. Even to devices that are not members of an object or firewall group. Communication partner 2 can be selected in the editor for communication relations.

- Firewall rules

  Number of firewall rules generated by SINEC NMS for the communication relation and loaded onto the security devices of the firewall group.

- Services

  Services that are used for communication between the communication partners. The services can be selected in the Communication Relation Editor. The "ANY" entry means that there is no restriction for the services used for communication.

- Version

  The version indicates the processing status of a communication relation. After a major change, the number before the dot is incremented and the number after the dot is set to 0, after a minor change, the number after the dot is incremented. SINEC NMS distinguishes between major and minor changes as follows:

  – Major changes:

    The communication partners of the communication relation have changed.

    The configuration of the common interfaces or capabilities in the Communication Relation Editor has changed.

    The services of the communication relation have changed.

    The version ID before the dot of a contained object or firewall group has changed.

  – Minor changes:

    The description of a communication relation has changed.

    The version ID after the dot from a contained object or firewall group has changed.

- Direction

  Display of the communication direction. Communication is always established from communication partner 1 to communication partner 2. To establish communication in the opposite direction, a separate communication relation must be configured.

- Description

  Description of the communication relation assigned in the editor for communication relations.

- Last change

  Name of the user who made the last change to the communication relation and the associated date and time.

- Reason for change

  Reason given by the user for the last major or minor change to the communication relation.

Actions

The following functions are available via the "Actions" drop-down list:

- Create

  Creates a communication relation for editing in the editor, see section below.
- Edit

  Opens a communication relation for editing in the editor, see section below.
- Copy

  Copies the properties of the selected communication relation to a new communication relation. The Policy Editor will then be opened to enter the name for the new policy. The name of the communication relation must be unique. The version of the communication relation is reset during copying.
- Delete

  Deletes the selected communication relation. The contained object groups, firewall groups and services are still available in the object library and can be used in communication relations.
- Enable

  Enables the selected communication relation. SINEC NMS generates firewall/NAT rules from activated communication relations, which can be displayed on the page "Network administration > Communication management > Firewall/NAT > Relation enforcements" and loaded on the firewall devices involved, see section Relation enforcements (Page 208).
- Disable

  Disables the selected communication relation. Firewall rules can only be generated from enabled communication relations.

Communication Relation Editor

The Communication Relation Editor opens when you create, open for editing, or copy a communication relation. In this editor, you define the communication partners involved by selecting the object groups. By selecting firewall groups, you determine the firewall devices that are used between the communication partners. When you execute the communication relation, the generated firewall rules are loaded on all firewall devices in these firewall groups. Communication takes place in the direction of the arrow from left to right.

The "Communication relation chain" dialog area is used to select the object and firewall groups involved. It is divided into the following sub-sections:

- Communication partner 1
  - Add object group

    Opens a dialog for selecting the object group whose devices establish the communication. Only object groups with the "OK" status can be selected. Object groups can also be managed in this dialog.
  - Add any device

After selecting this option, each device may establish communication. Even devices that are not members of an object or firewall group.

- Firewall groups
  - Add firewall group

    Opens a dialog for selecting a firewall group whose firewall devices are used between the communication partners. Firewall groups can be added after both communication partners have been specified. Only firewall devices with the "OK" status can be selected. Firewall groups can also be managed in this dialog.

    Up to 3 firewall groups can be selected in the "Firewall groups" area section, each of which can influence communication. Firewall groups can only be added to this area after both communication partners have been selected.

    The incoming and outgoing communication interfaces can be defined for each firewall group. Only the common interfaces that have been activated in the Firewall Group Editor are available for selection.
    The shared capabilities to be used can also be selected for each firewall group. The following options are available:

    Firewall: Specifies whether the firewall should be activated on the firewall devices.
    NAT: Specifies whether and which type of IP address translations with NAT are to be performed by the firewall devices. For information on the selectable NAT types, refer to the "NAT" section.
    Log level: Specifies the log level up to which events are recorded by the security devices. For example, if the "Warning" log level is selected, events of the "Critical" and "Warning" log levels are recorded, but no events of the "Info" log level.
    Digital input: If you select "Yes" for this option, the rules generated for the communication relation can be enabled and disabled via the digital input of the firewall devices.
- Communication partner 2
  - Add object group

    Opens a dialog for selecting the object group to whose devices the communication is established. Only object groups with the "OK" status can be selected. Object groups can also be managed in this dialog.
  - Add any device

    After selecting this option, the communication to each device may be established. Even to devices that are not members of an object or firewall group.
  - Add firewall group

    Opens a dialog for selecting a firewall group to whose devices the communication is established. Only firewall devices with the "OK" status can be selected. Firewall groups can also be managed in this dialog.

    The interface for incoming communication can be selected for a firewall group as Communication partner 2. The firewall cannot be disabled and IP address translations with NAT are not possible.

In the "Allowed services" dialog area, you can select the services through which the two communication partners may communicate. Communication via services other than those selected is not permitted by the firewall devices. Pre-defined services or user-defined services can be selected.

NAT

The following NAT conversion types are available in a communication relation:

- 1:1 SRC NAT (internal network on the left)

  The NAT router replaces the source IP address of a data packet with another source IP address during the transition from the internal to the external network. SINEC NMS treats the network to the left of the NAT router as an internal network. The assignment of old to new source IP addresses is unique. A source IP address in the internal network is assigned exactly one source IP address in the external network. You must specify the source IP address in the external network in the "Translation IP address (external)" column on the "Network administration > Communication management > Object library > NAT" page.

- 1:1 DST NAT (internal network on the right)

  The destination IP address of a data packet is replaced by the NAT router with a different destination IP address during the transition from the external to the internal network. SINEC NMS treats the network to the right of the NAT router as an internal network. The assignment of old to new destination IP addresses is unique. A destination IP address in the external network is assigned exactly one destination IP address in the internal network. You must specify the destination IP address in the external network in the "Translation IP address (external)" column on the "Network administration > Communication management > Object library > NAT" page.

- n:1 SRC NAT (internal network on the left)

  The source IP addresses of all data packets are replaced by the NAT router with another common source IP address at the transition from the internal to the external network. The new source IP address in the external network is identical for all data packets. SINEC NMS treats the network to the left of the NAT router as an internal network. SINEC NMS always uses the IP address of the interface that was selected as the external interface in the associated communication relation as the new source IP address in the external network.

5.3.1.2 Relation enforcements

The "Network administration > Communication management > Firewall/NAT > Relation enforcements" shows all monitored firewall devices. SINEC NMS generates associated firewall/NAT rules for each firewall device that is part of at least one enabled communication relation. The firewall rules allow communication according to the communication relations in which the firewall device is involved. You can compare the generated rules on the "Relation enforcements" page with the rules that are on the firewall device. If there are differences between the rules, you can load the rules generated by SINEC NMS onto the firewall devices. This deletes existing rules on the firewall devices. Before loading rules to a firewall device, you need to select a role from the corresponding drop-down list. After selecting the role, only the firewall devices assigned to the device areas of this role are available.

Properties

The properties of firewall devices are displayed in the following columns:

- Device Name

  Name of the firewall device
- IP address

  IP address of the firewall device
- Device type

  Device type of the firewall device.
- Operation

  Name of the operation from which the firewall device is monitored.
- Reference counter

  Specifies how often this firewall group is used in communication relations.
- Number of firewall rules

  Number of firewall rules generated by SINEC NMS for the firewall device.
- Device status

  The following device states are possible:

  – Device not configured

    The firewall device is not part of an active communication relation.

  – Configuration inconsistent

    At least one of the communication relations of the firewall device must in the "Outdated" or "Inconsistent" state, or rules or more have been generated for the firewall device by SINEC NMS 2000.

  – Device not reachable

    The firewall device is not accessible from SINEC NMS.

  – Enforcement required

    The firewall/NAT rules generated by SINEC NMS for the firewall device differ from the firewall/NAT rules on the firewall device. Use the "Enforce on device" action to load the rules generated by SINEC NMS onto the firewall device. This deletes existing rules on the firewall device.

  – Synchronized

    The firewall/NAT rules generated by SINEC NMS for the firewall device match the firewall/NAT rules on the firewall device.
- Firewall state

  Indicates whether the firewall is enabled on the firewall device and whether the firewall device is accessible. The firewall of a firewall device can be disabled using the "Disable firewall" action.

- NAT router

  Specifies whether NAT has been configured for the firewall device in at least one of its communication relations.
- Configuration access

  Specifies whether the firewall device may be configured by SINEC NMS. The configuration access to a firewall device can be set on the "Network administration > Configuration Cockpit" page of the corresponding operation.
- Last enforcement state

  Specifies the last determined state of the execution of communication relations on the firewall device.
- Enforced on

  Time and date at which the last execution was performed on the firewall device.
- Enforced by

  User who performed the last execution on the firewall device.

Operator controls

In the header, the following operator controls are available:

- Actions
  - Device details

    Retrieves the device details for the selected firewall device. In the device details, you can compare the rules generated by SINEC NMS with the rules that exist on the firewall device. Differences between these rules are highlighted in yellow. Some device-specific properties are not explicitly displayed on the firewall devices. In this case, SINEC NMS merely indicates that there are differences as compared to the generated rules. If execution is required, this is indicated in the tab title of the firewall and NAT rules.

    The rules in the "Firewall" tab are sorted according to their priority. The priority of the firewall rules is relevant when logging data packets that pass the firewall device according to these firewall rules. It is not derived from the order of configured communication relations, but instead from the source and destination IP addresses contained in the firewall rules. The scheme for prioritizing the firewall rules is as follows:

    1. Source IP address: Single IP address, Destination IP address: Individual IP address
    2. Source IP address: Single IP address, Destination IP address: IP address range
    3. Source IP address: IP address area - Destination IP address: Individual IP address
    4. Source IP address: IP address area - Destination IP address: IP address range
  - Enforce on device

    This action allows you to run the portions of the communication relations that the selected firewall devices are involved in on the firewall devices. The firewall/NAT rules that are relevant for the firewall devices are loaded onto the firewall devices. This action can only be performed for devices with the "Enforcement required" status. You need to select a role from its drop-down list before performing the action. The roles assigned to your user and the roles subordinate to these roles are available for selection. After selecting the role, only the firewall devices assigned to the device areas of the selected role are available for execution.

Note

Accessibility after execution on firewall devices

The communication relations of the selected firewall devices should be configured so that the firewall devices can still be reached by SINEC NMS after execution. After selecting the action for firewall devices, a dialog opens in which you must confirm this before execution via an associated check box.

– Disable firewall

Disables the firewall for the selected firewall devices. The firewall can be enabled again by performing the "Enforce on device" action for the firewall devices.

- Role

  A role must be selected before taking the "Enforce on device" action. The roles assigned to your user and the roles subordinate to these roles are available for selection. After selecting the role, only the firewall devices assigned to the device areas of the selected role are available for execution.

See also

Configuration Cockpit (Page 223)

5.3.2 Object library

5.3.2.1 Object groups

The "Network administration > Communication management > Object library > Object groups" page shows all the object groups that have been created. Object groups can be managed via the operator controls of the header.

Properties

The properties of object groups are displayed in the following columns:

- Name

  Unique name of the object group assigned in the editor for object groups.

- Members

  Number of devices belonging to the object group.

- Version

  The version indicates the processing status of an object group. After a major change, the number before the dot is incremented and the number after the dot is set to 0, after a minor change, the number after the dot is incremented. You can find information on categorizing changes in the "Major and minor changes" section.

- State

  The status of the object group is formed from the states of the group members. The status with the highest priority determines the status of the object group. In the following, the states are listed according to their priority:

  – Inconsistent

    A major change has been made to a group member. Use the "Apply member changes" button in the Object Group Editor to apply the change to the object group and set the status of the group member to "OK". If a group member that has been added to the object group as a monitored device is no longer accessible by SINEC NMS, this group member must be deleted from the object group so that the object group can be set to the "OK" status. You can find information on categorizing changes in the "Major and minor changes" section.

  – Update

    A minor change was made to a group member. Use the "Apply member changes" button in the Object Group Editor to apply the change to the object group and set the status of the group member to "OK". You can find information on categorizing changes in the "Major and minor changes" section.

  – OK

    All group members have the "OK" status.

- Reference counter

  Specifies how often this object group is used in communication relations.

- Description

  Description of the object group assigned in the editor for object groups.

- Last change

  Name of the user who made the last change to the object group and the associated date and time.

- Reason for change

  Reason given by a user for the last major or minor change to the object group.

Minor and minor changes

SINEC NMS distinguishes between major changes and minor changes to object groups and group members. The type of change determines the versioning and the status of group members, object groups and communication relations. Major changes to object groups influence the status of communication relations in which these object groups are used. SINEC NMS categorizes changes to object groups as follows:

- Major changes
  - The number of members of an object group has changed.
  - The IP address of a group member has changed.
  - A group member of an object group can no longer be reached from SINEC NMS.
- Minor changes
  - The name or description of an object group has changed.
  - The device name, the device type or the description of a group member has changed.

Actions

The following functions are available via the "Actions" drop-down list:

- Create

  Creates an object group for editing in the Object Group Editor, see section below.
- Edit

  Opens an object group for editing in the Object Group Editor, see section below.
- Copy

  Copies the properties of the selected object group to a new object group. The Object Groups Editor then opens to enter the name for the new object group. The name of the object group must be unique. The version of the object group is reset during copying.
- Delete

  Deletes the selected object group. Only object groups that are not used in any communication relation can be deleted. The number of communication relations in which an object group is used is specified in the "Reference counter" column.

Object Groups Editor

The Object Group Editor opens when you create, open for editing, or copy an object group. In the Object Group Editor, you configure an object group and obtain information about the status of each group member. If a group member have the status "Inconsistent" or "Update", the reason for this status is displayed in a tooltip.

The following operator controls are available:

- Add monitored devices

  Opens a dialog in which you can add monitored devices to the object group. For devices that can be reached via several IP addresses, you can select the IP address to be used in the object group in the "Internal IP address" column. Unlike devices added to the object group via the "Add device IP addresses" button, SINEC NMS displays discovered monitoring information for added monitored devices in the object group and automatically detects changes made to the device outside SINEC NMS.

- Add device IP addresses

  Opens a dialog in which you can add devices to the object group via their IP addresses. With this variant of adding, you can also include devices in the creation of firewall rules that are not monitored by SINEC NMS. However, SINEC NMS does not display monitoring information in the object group for these devices and cannot detect changes made to the device outside SINEC NMS.

- Delete

  Deletes the selected group member from the object group.

- Apply member changes

  If members of the object group have the "Update" or "Inconsistent" status as a result of changes, you can apply the changes to the object group with this button. The members and the object group then receive the "OK" status. The acceptance of changes to members is only possible if no member of the object group has been selected and the group members of SINEC NMS can be reached. If a group member that has been added to the object group as a monitored device is no longer accessible by SINEC NMS, this group member must be deleted from the object group so that the object group can be set to the "OK" status. If the IP address of the device is to remain included in the creation of firewall rules, you can add it to the object group using the "Add device IP addresses" button.

5.3.2.2 Firewall groups

The "Network administration > Communication management > Object library > Firewall groups" page shows all the firewall groups that have been created. Firewall groups can be managed using the controls in the header.

Properties

The properties of firewall groups are displayed in the following columns:

- Name

  Unique name of the firewall group assigned in the editor for firewall groups.

- Members

  Number of devices belonging to the firewall group.

- Active interfaces

  Number of common interfaces of the firewall group that have been enabled in the Firewall Group Editor. See the Firewall Group Editor section for information about common interfaces.

- Version

  The version indicates the processing status of the firewall group. After a major change, the number before the dot is incremented and the number after the dot is set to 0, after a minor change, the number after the dot is incremented. You can find information on categorizing changes in the "Major and minor changes" section.

- State

  The status of the firewall group is formed from the states of the group members. The status with the highest priority determines the status of the firewall group. In the following, the states are listed according to their priority:

  - Inconsistent

    A major change has been made to a group member. Use the "Apply member changes" button in the Firewall Group Editor to apply the change to the object group and set the status of the group member to "OK". If a group member that has been added to the object group as a monitored device is no longer accessible by SINEC NMS, this group member must be deleted from the firewall group so that the firewall group can be set to the "OK" status. You can find information on categorizing changes in the "Major and minor changes" section.

  - Update

    A minor change was made to a group member. Use the "Apply member changes" button in the Firewall Group Editor to apply the change to the object group and set the status of the group member to "OK". You can find information on categorizing changes in the "Major and minor changes" section.

  - OK

    All group members have the "OK" status.

- Reference counter

  Specifies how often this firewall group is used in communication relations.

- Description

  Description of the firewall group assigned in the Firewall Group Editor.

- Last change

  Name of the user who made the last change to the firewall group and the associated date and time.

- Reason for change

  Reason given by a user for the last major or minor change to the firewall group.

Minor and minor changes

SINEC NMS distinguishes between major and minor changes in firewall groups and group members. The type of change determines the versioning and status of group members, firewall groups and communication relations. Major changes to firewall groups affect the state of communication relations in which these firewall groups are used. SINEC NMS categorizes changes to firewall groups as follows:

- Major changes
  - The number of group members in a firewall group has changed.
  - The IP address or device type of a group member has changed.
  - An enabled common interface has been removed from a firewall group.
  - A shared capability has been removed from a firewall group.
  - A common interface of a firewall group has been disabled.
  - A group member of a firewall group can no longer be reached from SINEC NMS.
- Minor changes
  - The name or description of a firewall group has changed.
  - A disabled common interface has been removed from a firewall group.
  - The firewall group contains a new shared capability.
  - The firewall group contains a new common interface.
  - A common interface of a firewall group has been enabled.
  - The device name of a group member has changed.

Actions

The following functions are available via the "Actions" drop-down list:

- Create

  Creates a firewall group for editing in the Firewall Group Editor, see section below.
- Edit

  Opens a firewall group for editing in the Firewall Group Editor, see section below.
- Copy

  Copies the properties of the selected firewall group to a new firewall group. The Firewall Group Editor then opens to enter the name of the new firewall group. The name of the firewall group must be unique. The version of the firewall group is reset during copying.
- Delete

  Deletes the selected firewall group. Only firewall groups that are not used in any communication relation can be deleted. The number of communication relations in which a firewall group is used is specified in the "Reference counter" column.

Firewall Groups Editor:

The Firewall Group Editor opens when you create, open for editing, or copy a firewall group. In the Firewall Group Editor, you configure a firewall group and get information about the status of each group member. If a group member have the status "Inconsistent" or "Update", the reason for this status is displayed in a tooltip.

The "Common interfaces" area displays the interfaces that all members of the firewall group have. You can use the check boxes next to the interface names to enable them for use in communication relations. At least one common interface must be activated in each firewall group.

The "Common capabilities:" area shows the capabilities that all members of the firewall group have. If all members of the firewall group have a capability, this is marked with "Yes" and can be used in communication relations.

The following operator controls are available:

- Add members

  Opens a dialog where you can add monitored firewall devices to the firewall group. Only SCALANCE S615, SCALANCE SC-600 and RUGGEDCOM ROX2 devices can be added.

- Delete

  Deletes the selected group member from the firewall group.

- Apply member changes

  If members of the firewall group have the "Update" or "Inconsistent" status as a result of changes, you can apply the changes to the firewall group with this button. The members of the user group and firewall group then receive the "OK" status. It is only possible to apply changes to group members if no member of the firewall group has been selected and the SINEC NMS group members can be reached. If a group member that has been added to the object group as a monitored device is no longer accessible by SINEC NMS, this group member must be deleted from the firewall group so that the firewall group can be set to the "OK" status.

5.3.2.3 NAT

All NAT rules generated by SINEC NMS for the firewall devices of all activated communication relations are displayed on the "Network administration > Communication management > Object library > NAT" page.

Using the buttons in the header, you can export the NAT rules as XLS files and import them into SINEC NMS.

Properties

The properties of NAT rules are displayed in the following columns:

- NAT

  Type of NAT implementation. For information on the possible NAT implementation types, refer to the "NAT" section of the Communication relations (Page 202) chapter.
- Firewall device name

  Name of the firewall device that performs the NAT.
- Firewall IP address

  IP address of the firewall device that performs the NAT that can be reached by SINEC NMS.
- Operation

  Name of the operation that monitors and configures the firewall device.
- Firewall device type

  Device type of the firewall device that performs the NAT.
- Internal interface

  Name of the interface of the firewall device that was selected as the internal interface in the associated communication relation.
- Physical IP address (internal)

  IP address of the device in the internal network. Depending on the NAT implementation, this IP address has one of the following meanings:
  - For NATs "1:1 SRC NAT" and "n:1 SRC NAT": Source IP address of data packets, which is replaced by another source IP address during the transition from the internal network to the external network.
  - For NAT "1:1 DST NAT": IP address in the internal network to which data packets from the external network are forwarded.
- Physical device name

  Name of the device in the internal network.
- Physical device type

  Type of device in the internal network.
- Physical device description

  Description of the device in the internal network.

- External interface

  Name of the interface of the firewall device that was selected as the external interface in the associated communication relation.
- Translation IP address (external)

  External IP address for the device on the NAT router Depending on the NAT implementation, this IP address has one of the following meanings:

  – For NAT "1:1 SRC NAT": Specify the IP address in the external network to be used as the new source IP address.

  – For NAT "1:1 DST NAT": Specify the IP address on the external network from which data packets are to be forwarded to the internal network.

  – For NAT "n:1 SRC NAT": SINEC NMS always uses the IP address of the interface that was selected as the external interface in the associated communication relation as the new source IP address.
- Comment

  Enter a comment for the NAT rule.
- Last change

  Name of the user who made the last change to the NAT rule and the associated date and time.

5.3.2.4 Services

The "Network administration > Communication management > Object library > Services" page shows all available services. Services define the protocols the partners of communication relations that may be used to communicate. User-defined services can be managed via the operator controls of the header. System-defined services cannot be edited or deleted. A service is displayed in the Service Editor after clicking on an entry in the "Name" column.

Properties

The properties of services are displayed in the following columns:

- Name

  Unique name of the services. After clicking on an entry in this column, the service is displayed in the Service Editor.
- System-defined

  Indicates whether the service is pre-defined by SINEC NMS. System-defined services cannot be edited or deleted.
- IP Version

  IP protocol version
- IP protocol

  Name of the protocol.

- Protocol number

  Number of the IP protocol.
- Protocol restrictions

  Specifies the restrictions of the service on source (SRC) and destination (DST) ports or on ICMP types and codes.
- SRC port

  Specifies the restriction of the service to the source (SRC) port.
- DST port

  Specifies the restriction of the service to the destination (DST) port.
- ICMP type

  Specifies the restriction of the service to the ICMP type.
- ICMP code

  Specifies the restriction of the service to the ICMP code.
- Version

  The version indicates the processing status of the service. After a major change, the number before the dot is incremented and the number after the dot is set to 0, after a minor change, the number after the dot is incremented. System-defined services always have version 1.0. You can find information on categorizing changes in the "Major and minor changes" section.
- Reference counter

  Specifies how often this service is used in communication relations.
- Description

  Description of the service.
- Last change

  The name of the user who made the last change to the service and the associated date and time.
- Reason for change

  Reason given by a user for the last major or minor change to the service.

Major and minor changes

SINEC NMS distinguishes between major and minor changes when changing services. The type of change determines the versioning of the service. In addition, major changes to services influence the state of communication relations in which these services are used. SINEC NMS categorizes changes to services as follows:

- Major changes
  - The IP protocol has changed.
  - A parameter of the IP protocol has changed.
- Minor changes
  - The name of a service has changed.
  - The description of a service has changed.

Actions

The following functions are available via the "Actions" drop-down list:

- Create

  Creates a service for editing in the Service Editor, see section below.
- Edit

  Opens a service for editing in the Service Editor, see section below. System-defined services cannot be edited.
- Copy

  Copies the properties of the selected service to a new service. The service for entering the name for the new service is then opened. The name of the service must be unique. The version of the service is reset during copying.
- Delete

  Deletes the selected service. Only services that are not used in any communication relation and that are not system-defined can be deleted. The number of communication relations in which a service is used is specified in the "Reference counter" column.

Service editor

The Services Editor opens when you create, open for editing, copy, or click an entry in the "Name" column. You configure the service in the Service Editor. System-defined services cannot be edited.

The following operator controls are available:

- Name

  Unique name of the services.
- Description

  Description of the service.

- Version

  The version indicates the processing status of the service. After a major change, the number before the dot is incremented and the number after the dot is set to 0, after a minor change, the number after the dot is incremented. System-defined services always have version 1.0. You can find information on categorizing changes in the "Major and minor changes" section.

- IPv4 protocol

  Selection of the protocol:

  – User-defined

    IP protocol is selected from the IANA list.

  – 1 (ICMP)

    The ICMP protocol and the specified ICMP type and code are used.

  – 6 (TCP)

    The TCP protocol and the specified source and destination ports are used.

  – 17 (UDP)

    The UDP protocol and the specified source and destination ports are used.

5.4 Configuration Cockpit

Operation

The Configuration·Cockpit is available on the "Network·administration > Configuration Cockpit" page.

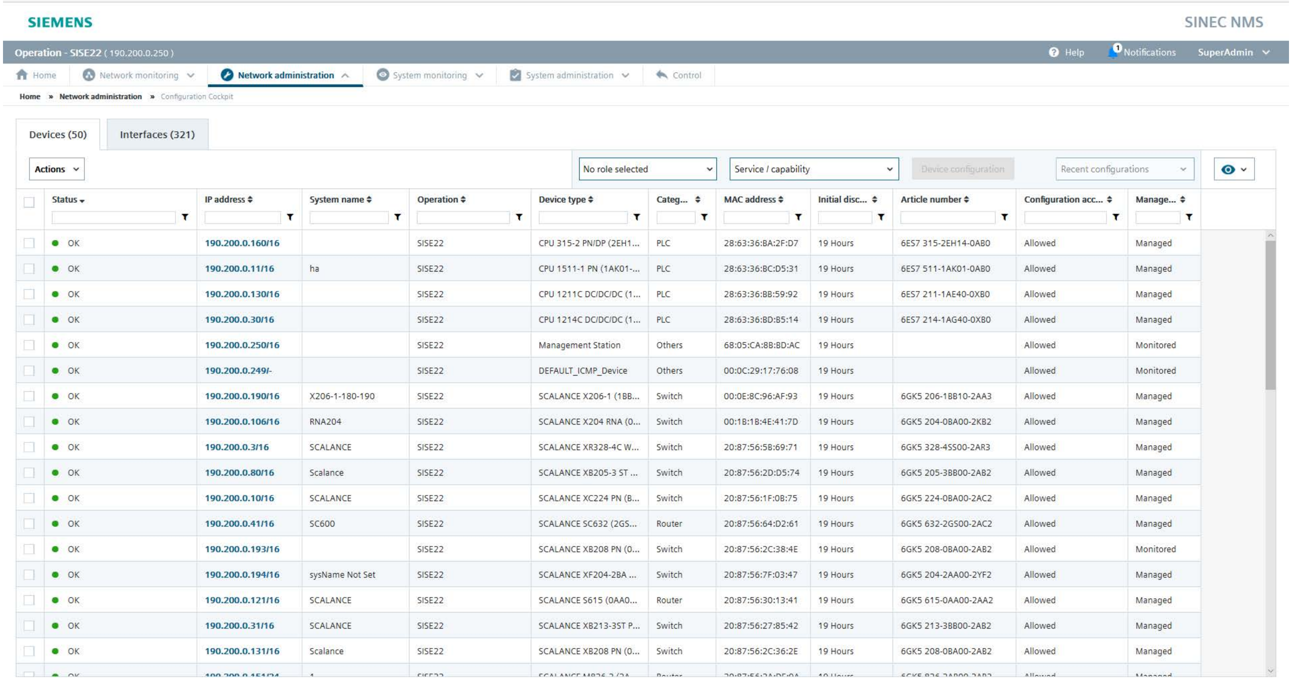
Individual configuration tasks for devices and device interfaces can be executed in the Configuration Cockpit. In contrast to configuration via the Policy Control Center, in the Configuration Cockpit you directly select the devices or interfaces to be configured and then always select a task to be executed for the devices or interfaces. This task is then executed immediately. Each executed task is treated as a local policy and is visible in the Policy Control Center of the associated operation. The type of such policies is "System local".

To view enforcement reports for policies configured in the Configuration Cockpit, at least the "view" permission for the Policy Control Center is required.

5.4.1 Devices

Operation

You reach this page in the navigation of operations under "Network administration > Configuration Cockpit", "Devices" tab.



☐	Status	IP address	System name	Operation	Device type	Categ...	MAC address	Initial disc...	Article number	Configuration acc...	Manage...
☐	● OK	190.200.0.160/16		SISE22	CPU 315-2 PN/DP (2EH1...	PLC	28:63:36:BA:2F:D7	19 Hours	6ES7 315-2EH14-0AB0	Allowed	Managed
☐	● OK	190.200.0.11/16	ha	SISE22	CPU 1511-1 PN (1AK01-...	PLC	28:63:36:BC:D5:31	19 Hours	6ES7 511-1AK01-0AB0	Allowed	Managed
☐	● OK	190.200.0.130/16		SISE22	CPU 1211C DC/DC/DC (1...	PLC	28:63:36:BB:59:92	19 Hours	6ES7 211-1AE40-0XB0	Allowed	Managed
☐	● OK	190.200.0.30/16		SISE22	CPU 1214C DC/DC/DC (1...	PLC	28:63:36:BD:B5:14	19 Hours	6ES7 214-1AG40-0XB0	Allowed	Managed
☐	● OK	190.200.0.250/16		SISE22	Management Station	Others	68:05:CA:8B:BD:AC	19 Hours		Allowed	Monitored
☐	● OK	190.200.0.249/-		SISE22	DEFAULT_ICMP_Device	Others	00:0C:29:17:76:08	19 Hours		Allowed	Monitored
☐	● OK	190.200.0.190/16	X206-1-180-190	SISE22	SCALANCE X206-1 (1BB...	Switch	00:0E:8C:96:AF:93	19 Hours	6GK5 206-1BB10-2AA3	Allowed	Managed
☐	● OK	190.200.0.106/16	RNA204	SISE22	SCALANCE X204 RNA (0...	Switch	00:1B:1B:4E:41:7D	19 Hours	6GK5 204-0BA00-2KB2	Allowed	Managed
☐	● OK	190.200.0.3/16	SCALANCE	SISE22	SCALANCE XR328-4C W...	Switch	20:87:56:5B:69:71	19 Hours	6GK5 328-4SS00-2AR3	Allowed	Managed
☐	● OK	190.200.0.80/16	Scalance	SISE22	SCALANCE XB205-3 ST ...	Switch	20:87:56:2D:D5:74	19 Hours	6GK5 205-3BB00-2AB2	Allowed	Managed
☐	● OK	190.200.0.10/16	SCALANCE	SISE22	SCALANCE XC224 PN (B...	Switch	20:87:56:1F:0B:75	19 Hours	6GK5 224-0BA00-2AC2	Allowed	Managed
☐	● OK	190.200.0.41/16	SC600	SISE22	SCALANCE SC632 (2GS...	Router	20:87:56:64:D2:61	19 Hours	6GK5 632-2GS00-2AC2	Allowed	Managed
☐	● OK	190.200.0.193/16		SISE22	SCALANCE XB208 PN (0...	Switch	20:87:56:2C:38:4E	19 Hours	6GK5 208-0BA00-2AB2	Allowed	Monitored
☐	● OK	190.200.0.194/16	sysName Not Set	SISE22	SCALANCE XF204-2BA ...	Switch	20:87:56:7F:03:47	19 Hours	6GK5 204-2AA00-2YF2	Allowed	Managed
☐	● OK	190.200.0.121/16	SCALANCE	SISE22	SCALANCE S615 (0AA0...	Router	20:87:56:30:13:41	19 Hours	6GK5 615-0AA00-2AA2	Allowed	Managed
☐	● OK	190.200.0.31/16	SCALANCE	SISE22	SCALANCE XB213-3ST P...	Switch	20:87:56:27:85:42	19 Hours	6GK5 213-3BB00-2AB2	Allowed	Managed
☐	● OK	190.200.0.131/16	Scalance	SISE22	SCALANCE XB208 PN (0...	Switch	20:87:56:2C:36:2E	19 Hours	6GK5 208-0BA00-2AB2	Allowed	Managed
☐	● OK	190.200.0.151/24	1	SISE22	SCALANCE M826-2 (2A...	Router	20:87:56:2A:DF:0A	19 Hours	6GK5 826-2AB00-2AB2	Allowed	Managed

Figure 5-8 Device·configuration in the Configuration Cockpit

In the "Devices" tab, you can configure tasks for devices and device interfaces.

To do this, follow the steps outlined below:

1. Select a role from the drop-down list titled "No role selected" and optional capabilities from the "Service / capability" drop-down list according to which the selectable devices and tasks are to be filtered. Selected filter settings are also in effect in the "Interfaces" tab. For more detailed information, refer to the "Filter settings" section.
2. Select the devices that are to be configured from the list of devices.

   Note

   IP addresses of the devices

   The devices are displayed in the Configuration Cockpit with the IP addresses through which SINEC NMS can reach the devices. If there is a NAT router between an operation and a device, the external IP address of the device that is set for the device on the NAT router is displayed. This should be taken into account when selecting the devices to be configured.

   ---

3. You can select the task to be executed from all available tasks or select a task from the history of the most recently executed tasks:
   – To select the task to be executed from all available tasks, click the "Device configuration" button.

     The selected devices, the selected role as well as the tasks available according to the selected devices and active filters are displayed in the "Device configuration" dialog. Before selecting a task, you can further restrict the filter setting for capabilities by clearing the check boxes next to unneeded capabilities. Filter settings that you made in step 1 cannot be removed in this dialog.

     Function descriptions of the individual tasks are displayed in the "Description" column. Select the task to be performed and click the "Next" button.

   – If you want to run a task that you have already executed, you can alternatively select this task from the drop-down list "Recent configurations". The drop-down list contains the 10 most recent tasks performed by the logged-in user. If the logged-in user has not used the recent configurations list for longer than three months, the list for this user will be deleted.
     If the rights of the selected role have been changed since the recent executions, the list of available tasks may be reduced. If filter settings for capabilities are active, only those tasks that can be performed with these capabilities are available in the drop-down list.
4. Select the parameters that are to be configured according to the selected task.
5. To add more tasks and devices, click on the "Edit as policy" button. The settings made are then opened in the Policy Editor. For information on configuring policies in the Policy Editor, refer to section Policy editor (Page 183). Policies configured based on configuration cockpit settings are executed once and then automatically set to "Ready to deploy". This also applies if a schedule with multiple enforcements has been configured for these policies in the Policy Editor.

   To execute the task immediately for the selected devices, click the "Execute" button. The task is then executed as a local policy and displayed in the Policy Control Center of the operation with the name of the selected task and the associated time stamp. As soon as the policy has been executed, it is automatically disabled by SINEC NMS. After clicking the "Enforce" button, a dialog appears showing the progress of policy enforcement with the following options:

– Go to Policy Control Center: Opens the page "Network administration > Policy Control Center", "Policies" tab on the operation. After the policy has been enforced, you can use the entry to open the "Policy enforcements" tab.

– Close: Closes the dialog.

– Close and notify: Closes the dialog and informs the user with a notification as soon as the policy has been enforced.

If a task was selected in the "Device configuration" dialog for which the required capabilities are not available for all selected devices, a dialog with the following options is displayed:

– Cancel: The execution of the task is canceled for all devices.

– Continue: The task is executed for all devices that have the capabilities required for the task. The task is not executed for the other devices.

Filter settings

With the filters for roles and capabilities, you define a preselection for the selectable devices and for the tasks that are available for the device configuration. Before selecting a task for devices, the list of devices must be filtered by roles; filtering by capabilities is optional. Regardless of the filter settings selected, the available tasks always depend on the capabilities that the selected devices support.

- Roles: After selecting a role from the drop-down list titled "No role selected", only devices with the "Managed" management status that are assigned to the device areas of the selected role are displayed. After selecting a role, only tasks for which the necessary device configuration rights are available in the role can be selected in the device configuration dialog.
  Roles for device areas are authorized on the "System administration > Role assignments" page, in the "Device areas" tab. Authorization of roles for the configuration of devices is performed on this page in the "Rights" tab.
  Only those roles can be selected that are assigned to the logged-in user and subordinate to these roles.

- Capabilities: In the drop-down list for capabilities, the capabilities are displayed grouped by services (level 1) and categories (level 2). After selecting a capability, only those devices with the management status "Managed" that have the selected capability are displayed. In the dialog for device configuration, only tasks that can be executed with this capability can be selected after a capability has been selected.
  Only those capabilities can be selected that belong to categories for which the roles of the logged-in user are authorized. If a role has been selected in the role filter, only the capabilities of the categories for which this role is authorized can be selected.
  Roles for configuring device services are authorized on the page "System administration > Role assignments", "Rights" tab in the "Device configuration" area.

Actions

- Block configuration access

  If configuration access for a device is blocked, this device cannot be configured using SINEC NMS and the device cannot adopt the management status "Managed". For more information on the management status, refer to section Management status (Page 54).

- Allow configuration access

  If configuration access is allowed for a device, this device can be configured using SINEC NMS and can adopt the management status "Managed", provided the device is monitored by SINEC NMS and the capabilities of the device have been discovered. This action is not possible for devices with the "Blocked (untrusted)" access status, see section below. For more information on the management status, refer to section Management status (Page 54).

- Discover capabilities

  Detects the functions supported by the selected devices and displays them in the "Capabilities" device details tab of the Configuration Cockpit. SINEC NMS uses the functions discovered by a device, among other things in the context of the policy decision, to determine the policy rules that are enforced for the device. During the network scan and after the change of credentials in the device credential repository, SINEC NMS always automatically performs a discovery of capabilities.

- Export as CSV file

  Exports the data of the table to a CSV file.

- Show device details

  Retrieves the device details for the selected device. For more information on the displayed device details, refer to section Device details (Page 232).

Properties

The properties of the devices are displayed in the following columns:

- State

  The status of a device is formed by events that are contained in overall status groups and are pending for this device. The possible overall states are listed below according to their priority for the display:

  - 🔴

    Not reachable
  - 🔴

    Error
  - 🟠

    Maintenance demanded
  - 🟢

    Maintenance required
  - 🟢

    OK
  - ⚪

    Not connected
- IP address

  IP address and subnet mask in CIDR notation. The details of the device are displayed by clicking on the entry in this column, refer to section Device details (Page 232).
- System name

  System name of the device
- Operation

  Operation from which the device is monitored
- Device type

  Device type to which the device was assigned by SINEC NMS.
- Category

  Device category that was selected for the device in the corresponding device profile.
- MAC address

  MAC address of the device
- Initial discovery

  Specifies when the device was first discovered by SINEC NMS
- Article number

  Article number of the device

- Gateway

  IP address of the gateway that is configured for the device

- PROFINET

  PROFINET device name of the device

- Serial number

  Serial number of the device

- Firmware version

  Firmware version that is active on the device

- Hardware version

  Hardware version of the device

- Place of use

  Location that is configured on the device

- Contact person

  Contact person that is configured on the device

- Configuration access

  The following values are possible:

  - Allowed

    If configuration access is allowed for a device, this device can be configured using SINEC NMS and can adopt the management status "Managed", provided the device is monitored by SINEC NMS and the capabilities of the device have been discovered.

  - Blocked

    If configuration access for a device is blocked, this device cannot be configured using SINEC NMS and the device cannot adopt the management status "Managed".

  - Blocked (untrusted)

    Configuration access is blocked for devices whose SSH/HTTPS fingerprint is not trusted. Configuration access to these devices cannot be allowed using the "Allow configuration access" action. Prior to this, the "Trusted" status must be set on the "Network administration > Device credential repository" page of the respective operation for these devices.

- Management status

  The management status indicates how the device can be handled by SINEC NMS. For detailed information on the possible management status, refer to section Management status (Page 54).

- Assigned controller

  Controller assigned to the device

- Reason for overall status

  Event that triggered the status of the device.

- Comment

  Comment that is added to the operation under "Network monitoring > Devices".
- Last capabilities received

  Time at which the detected functions of the device were last updated.
- Updated on

  Time at which the device data was last updated.
- IP address external

  IP address configured on the NAT router for a device in the external subnet. Only one IP address is displayed if it is a NAT device.
- IP address internal

  IP address of the device
- MAC address external

  MAC address of the NAT router. Only one MAC address is displayed if it is a NAT device.
- NAT device

  Indicates whether the device is accessible from SINEC NMS via a NAT router.

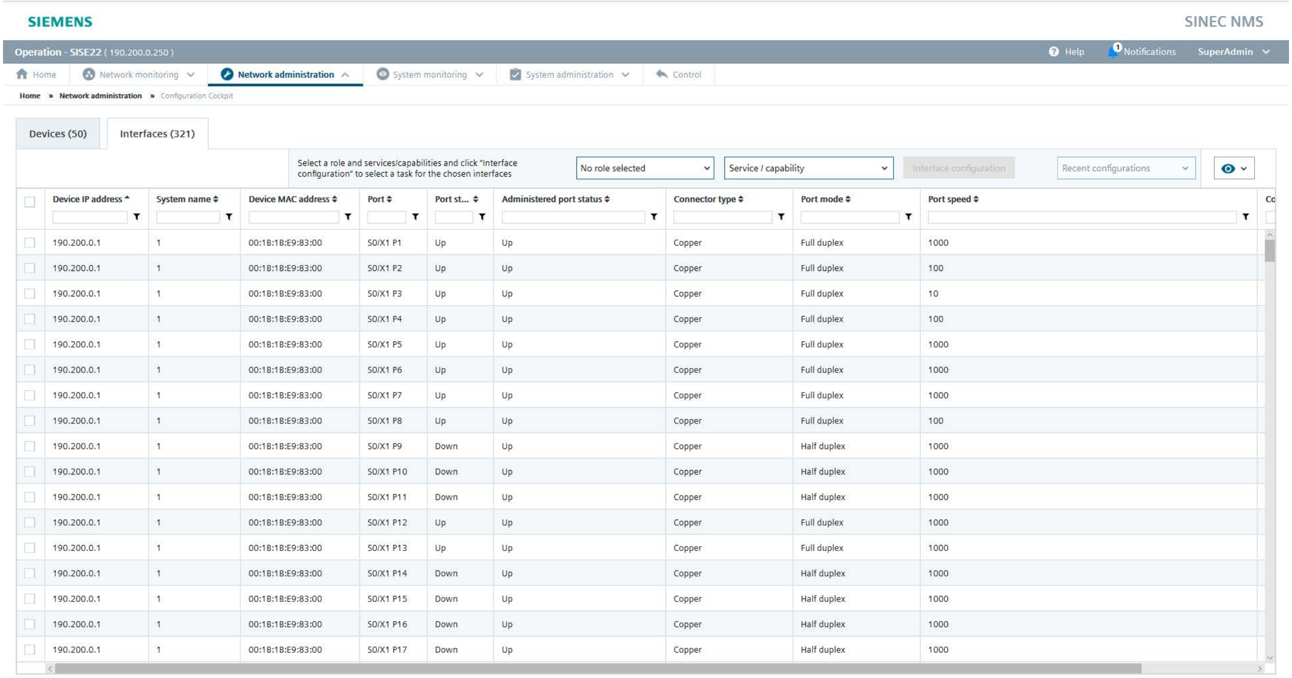
See also

Device credential repository (Page 234)

5.4.2 Interfaces

Operation

You reach this page in the navigation of operations under "Network administration > Configuration Cockpit", "Interfaces" tab.



Select a role and services/capabilities and click "Interface configuration" to select a task for the chosen interfaces

□	Device IP address	System name	Device MAC address	Port	Port st...	Administered port status	Connector type	Port mode	Port speed	Co
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P1	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P2	Up	Up	Copper	Full duplex	100	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P3	Up	Up	Copper	Full duplex	10	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P4	Up	Up	Copper	Full duplex	100	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P5	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P6	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P7	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P8	Up	Up	Copper	Full duplex	100	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P9	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P10	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P11	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P12	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P13	Up	Up	Copper	Full duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P14	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P15	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P16	Down	Up	Copper	Half duplex	1000	
□	190.200.0.1	1	00:1B:1B:E9:83:00	S0/X1 P17	Down	Up	Copper	Half duplex	1000	

Figure 5-9 Interface configuration in the Configuration Cockpit

Tasks for device interfaces can be configured in the "Interfaces" tab.

To do this, follow the steps outlined below:

1. Select a role from the drop-down list titled "No role selected" and optional capabilities from the "Service / capability" drop-down list according to which the selectable interfaces and tasks are to be filtered. Selected filter settings are also in effect in the "Devices" tab. For more detailed information, refer to the "Filter settings" section.
2. Select the interfaces that are to be configured from the list of interfaces.

Note

IP addresses of the interfaces

The device interfaces are displayed in the Configuration Cockpit with the IP addresses through which SINEC NMS can reach the corresponding devices. If there is a NAT router between an operation and a device, the external IP address of the device that is set for the device on the NAT router is displayed. This should be taken into account when selecting the interfaces to be configured.

3. You can select the task to be executed from all available tasks or select a task from the history of the most recently executed tasks:
   - To select the task to be executed from all available tasks, click on the "Interface configuration" button.

     The selected interfaces, the selected role and the tasks available according to the selected interfaces and active filters are displayed in the "Interface configuration" dialog. Before selecting a task, you can further restrict the filter setting for capabilities by clearing the check boxes next to unneeded capabilities. Filter settings that you made in step 1 cannot be removed in this dialog.

     Function descriptions of the individual tasks are displayed in the "Description" column. Select the task to be performed and click the "Next" button.
   - If you want to run a task that you have already executed, you can alternatively select this task from the drop-down list "Recent configurations". The drop-down list contains the 10 most recent tasks performed by the logged-in user. If the logged-in user has not used the recent configurations list for longer than three months, the list for this user will be deleted.
     If the rights of the selected role have been changed since the recent executions, the list of available tasks may be reduced. If filter settings for capabilities are active, only those tasks that can be performed with these capabilities are available in the drop-down list.
4. Select the parameters that are to be configured according to the selected task.
5. To add more tasks and interfaces, click on the "Edit as policy" button. The settings made are then opened in the Policy Editor. For information on configuring policies in the Policy Editor, refer to section Policy editor (Page 183). Policies configured based on configuration cockpit settings are executed once and then automatically set to "Ready to deploy". This also applies if a schedule with multiple enforcements has been configured for these policies in the Policy Editor.

   To execute the task immediately for the selected interfaces, click the "Execute" button. The task is then executed as a local policy and displayed in the Policy Control Center of the operation with the name of the selected task and the associated time stamp. As soon as the policy has been executed, it is automatically disabled by SINEC NMS. After clicking the "Enforce" button, a dialog appears showing the progress of policy enforcement with the following options:
   - Go to Policy Control Center: Opens the page "Network administration > Policy Control Center", "Policies" tab on the operation. After the policy has been enforced, you can use the entry to open the "Policy enforcements" tab.
   - Close: Closes the dialog.
   - Close and notify: Closes the dialog and informs the user with a notification as soon as the policy has been enforced.

   If a task was selected in the "Interface configuration" dialog for which the required capabilities are not available for all selected Devices, a dialog with the following options is displayed:
   - Cancel: The execution of the task is canceled for all interfaces.
   - Continue: The task is executed for all interfaces whose associated devices have the capabilities required for the task. The task is not executed for the other interfaces.

Filter settings

You use the filters for roles and capabilities to create a preselection for the selectable interfaces and for the tasks available for the interface configuration. Before selecting a task for interfaces, the list of interfaces must be filtered by roles; filtering by capabilities is optional. Regardless of the filter settings selected, the available tasks always depend on the capabilities that the selected interfaces support.

- Roles: After selecting a role from the drop-down list titled "No role selected", only the interfaces whose associated devices have the "Managed" management status and which are assigned to the device areas of the selected role are displayed. After selecting a role, only tasks for which the necessary device configuration rights are available in the role can be selected in the interface configuration dialog.
  Roles for device areas are authorized on the "System administration > Role assignments" page, in the "Device areas" tab. Authorization of roles for the configuration of devices is performed on this page in the "Rights" tab.
  Only those roles can be selected that are assigned to the logged-in user and subordinate to these roles.
- Capabilities: In the drop-down list for capabilities, the capabilities are displayed grouped by services (level 1) and categories (level 2). After selecting a capability, only those interfaces whose associated devices have the management status "Managed" and the selected capability are displayed. In the interface configuration dialog, only tasks that can be executed with this capability can be selected after a capability has been selected.
  Only those capabilities can be selected that belong to categories for which the roles of the logged-in user are authorized. If a role has been selected in the role filter, only the capabilities of the categories for which this role is authorized can be selected.
  Roles for configuring device services are authorized on the page "System administration > Role assignments", "Rights" tab in the "Device configuration" area.

5.4.3 Device details

The "Device details" window opens when an entry in the "IP address" column of the Configuration Cockpit is clicked or when the "Show device details" action is selected. The window contains the following tabs:

Device details

This tab contains the device information displayed in the columns of the "Devices" tab, refer to section Devices (Page 223).

Capabilities discovered

This tab specifies the capabilities that have been discovered by SINEC NMS for the device and the policy tasks that can be enforced for the device. In addition, it is specified which protocols were used to recognize the individual capabilities. The protocols used to detect a capability may differ from the protocols used to perform the capability. SINEC NMS uses the information about the policy tasks that can be performed for a device as part of the policy decision to determine the policy rules to be performed for the device, see section Policy decision (Page 193).

During the network scan and after the change of credentials in the device credential repository, SINEC NMS always automatically performs a discovery of capabilities. The discovery of the capabilities can be initiated manually via the "Discover capabilities" action in the "Devices" tab, refer to section Devices (Page 223).

Configuration history

The tab displays all parameters that were configured with the last 5 policies for the device.

Device parameters

The tab displays all tasks and parameters that can be configured by policies on the device based on the detected capabilities. If one of these tasks has already configured a value on the device, it is displayed in the "Value" column.

5.5 Device configuration repository

Operation

The device configuration repository is available on the "Network administration > Device configuration repository" page.

The Device configuration repository contains backups from configurations that were created by devices of the operation with policies. Up to 10 device configurations are stored in a ring buffer for each device. Subsequent device configurations overwrite device configurations with the oldest time stamp.

The properties of the devices from which the respective configuration originates are displayed for each existing device configuration.

In order to save, view, edit or restore the configuration of a device, the "SINEMA Configuration Interface" device property must be enabled on the respective devices. This property can be activated by the policy task "Set SINEMA Configuration Interface enabled".

Read the notes on the compatibility of devices with the functions described in this section. You can find these notes in the readme file of SINEC NMS.

Actions

The following operator controls are available in the "Actions" drop-down list:

- Displays

  Displays the device configuration parameters in write-protected mode. After a click on the "Edit" button, the device configuration parameters can be edited.
  Changes that are made cannot be saved in the original device configuration, but must be saved as a separate device configuration. Changes in the separate device configuration can either be transferred to this device configuration or saved in another device configuration.
  When new device configurations are saved, these can be marked with tags. Tags can be used in policies to select the desired device configuration. Tags are separated from each

other by the character ";". The tag "Custom" must not be used. It is used by SINEC NMS for device configurations in which parameters were manually changed and in which it is possible to overwrite parameters. Alternatively to the manual creation of tags, tags can be generated by policies, refer to section Policy Control Center (Page 177).

- Compare: Opens a dialog in which two selected device configurations are compared in places. Deviations between both configurations are highlighted in red.
- Lock: Locks the selected device configuration. Locked device configurations are not removed from the ring buffer when new device configurations are added.
- Unlock: Unlocks the selected device configuration. Unlocked device configurations are removed from the ring buffer when new device configurations are added.
- Edit tags: Opens a dialog to add or edit tags. Tags can be used in policies to select the desired device configuration. Tags are separated from each other by the character ";". The tag "Custom" must not be used. It is used by SINEC NMS for device configurations in which parameters were manually changed and in which it is possible to overwrite parameters. Alternatively to the manual creation of tags, tags can be generated by policies, refer to section Policy Control Center (Page 177).
- Delete: Deletes the selected device configuration.
- Restore: Restores the selected device configuration on the device whose properties are displayed for the device configuration.
- Export: Exports the selected configuration file and stores it locally on the client PC. This action is only available for RUGGEDCOM ROS and RUGGEDCOM ROX2 devices.

5.6 Device credential repository

Operation

The device credential repository· is available on the "Network administration > Device credential repository" page.

In the Device credential repository you can manage for each monitored device the data with which SINEC NMS logs in to the devices for reading and writing device information with SNMP and CLI.

Initially, the credentials for each device are available in the Device credential repository, which was configured on the control under "System administration > Operation parameter profiles" in the parameter group "Initial credentials". If SINEC NMS was able to discover a device with the SNMP settings from the parameter group "SNMP settings for discovery", these SNMP settings are taken over for the device in the Device credential repository and overwrite the initial credentials in the "SNMP monitoring" tab of the corresponding edit dialog.

The logon data to be used for devices can be changed manually in the Device credential repository.

Operator controls

The following operator controls are available:

- Edit

  Opens the editor for login information for the selected device, see the "Editor for login information" section.

- Copy

  You can copy the logon information of a selected device to other devices. After clicking on this operator control, a dialog opens in which you can enter the credentials to be copied and select the devices to which this information is to be copied.

- Delete

  Deletes the credentials for the selected device from the Device credential repository. Logon information of monitored devices cannot be deleted.

- Trust device

  Classifies the current SSH/HTTPS fingerprint of a device as trusted. The device receives the "Trusted" status and the fingerprint that was trusted is displayed in the "Trusted SSH fingerprint (SHA-256)" / "Trusted HTTPS fingerprint (SHA-256)" column. Configuration access to the device is allowed and can be changed on the "Network administration > Configuration Cockpit" page of operations.
  When SINEC NMS reads a fingerprint from a device that differs from the currently trusted fingerprint, the fingerprint and the device are automatically classified as untrusted.
  Devices that have an HTTPS certificate loaded with the "Load HTTPS certificate to device" policy task are automatically classified as trusted by SINEC NMS, if the "Trust device after certificate download" parameter has been set to "YES" in the policy task.

- Untrust device

  Classifies the SSH/HTTPS fingerprint of a device as untrusted. The device receives the "Untrusted" status and the current untrusted fingerprint is displayed in the "Current SSH fingerprint (SHA-256)" / "Current HTTPS fingerprint (SHA-256)" column. Configuration access to the device by SINEC NMS is blocked.

- Show initial credentials

  Shows the credentials which were configured on the control under "System administration > Operation parameter profiles" in the parameter group "Initial credentials".

Editor for logon information

The editor for logon information can be opened by selecting a device and clicking the "Edit" button. In this editor, you configure the data with which SINEC NMS logs in to the device for reading and writing device information with SNMP and SSH/HTTP(S).

Using the button "Restore initial credentials" you can, in each tab, restore the settings that were configured on the control under "System administration > Operation parameter profiles" in the parameter group "Initial credentials".

In the tabs "SNMP monitoring" and "SNMP configuration", you can take over the SNMP settings of the other tabs via the buttons "Use SNMP Write settings" and "Use SNMP Read settings".

In the "SSH/HTTP(S)" tab, the currently trusted SSH/HTTPS fingerprint and the last SSH/HTTPS fingerprint read are displayed in addition to the login data. These fingerprints are identical for trusted devices. After clicking on an HTTPS fingerprint, the properties of the corresponding certificate are displayed. The option fields above the text boxes can be used to select the hash algorithm used to display the fingerprints. SINEC NMS always uses the hash algorithm SHA-256 for the internal comparison of certificates due to the high collision security. It is possible that SINEC NMS classifies a device as untrustworthy due to a modified SHA-256 fingerprint and the SHA-1 and/or MD5 hash algorithms cannot detect any changes to the certificate.

See also

Configuration Cockpit (Page 223)

System monitoring 6

6.1 System alarm messages

On the page "System monitoring > System alarm messages", system alarm messages are displayed which are reported by the control and by operations. Only the system alarm messages reported by this operation are displayed on an operation.

Status of system alarm messages

System alarm messages influence the system status of control and operations, which is displayed under "System administration > Operations". The status of alarm messages, which is displayed under "System monitoring > System alarms" in the "Alarm status" column, is important for influencing this system status:

- Pending

  The problem triggered by the system alarm message has not yet been resolved. Pending system alarm messages flow into the system status of the control and operations, which is displayed under "System administration > Operations".

- Automatically resolved

  SINEC NMS has marked the system alarm message as no longer pending because the underlying problem has been resolved.

- Resolved manually

  A user has manually marked the system alarm message as no longer pending.

- Not applicable

  System alarm messages with this alarm status are for information only and do not require user interaction.

Operator controls

You can execute the following actions using the operator controls of the header:

- Read

  Mark the system alarm message as read. This selection has no influence on the system status of control and operations.

- Unread

  Mark the system alarm message as unread. This selection has no influence on the system status of control and operations.

- Resolve manually

  Sets the system alarm message to the status "Resolved manually", see above.

- Comment

  Adding a comment to the system alarm message.

6.2 Jobs

6.2.1 Jobs

SINEC NMS runs processes such as the creation of reports internally via jobs. Status information for these jobs is displayed on the "System monitoring > Jobs" page.

The available job types include:

- Adding an operation
- Running a network scan
- Enforcing a policy
- Creating a report
- Legacy data cleanup

Similar to policies, the scope of jobs determines their visibility. Global jobs are visible on the control and on all involved operations, while local jobs are only visible on the affected operation.

The numbers in brackets in the "State" column indicate the number of operations on which the specified job state could be restored.

The following functions are available via the operator controls of the header:

- Show historical data

  Shows information on executions of the selected job already performed. You can find more information in the section Historical data (Page 239)

- Export as CSV file

  Exports the information about the selected jobs to a CSV file. If no jobs are selected, the information of all listed jobs is exported to a CSV file.

A maximum of 200 simultaneously executed jobs are supported on the control and on operations.

Note

Do not shut down SINEC NMS while executing jobs.

SINEC NMS must not be shut down during job execution. If SINEC NMS is shut down while jobs are being executed, they will not be executed or will not be executed completely.

6.2.2 Historical data

If you click on the "Show historical data" button on the "System monitoring > Jobs" page, the "Historical data" page displays information about the executions of the selected jobs that has already taken place. If no jobs have been selected before clicking the "Show historical data" button, historical data is displayed for all jobs.

You can filter the displayed historical data by job type, date and time, and execution states. These filter settings are available after clicking the "Add filter" button.

6.3 Audit Trail

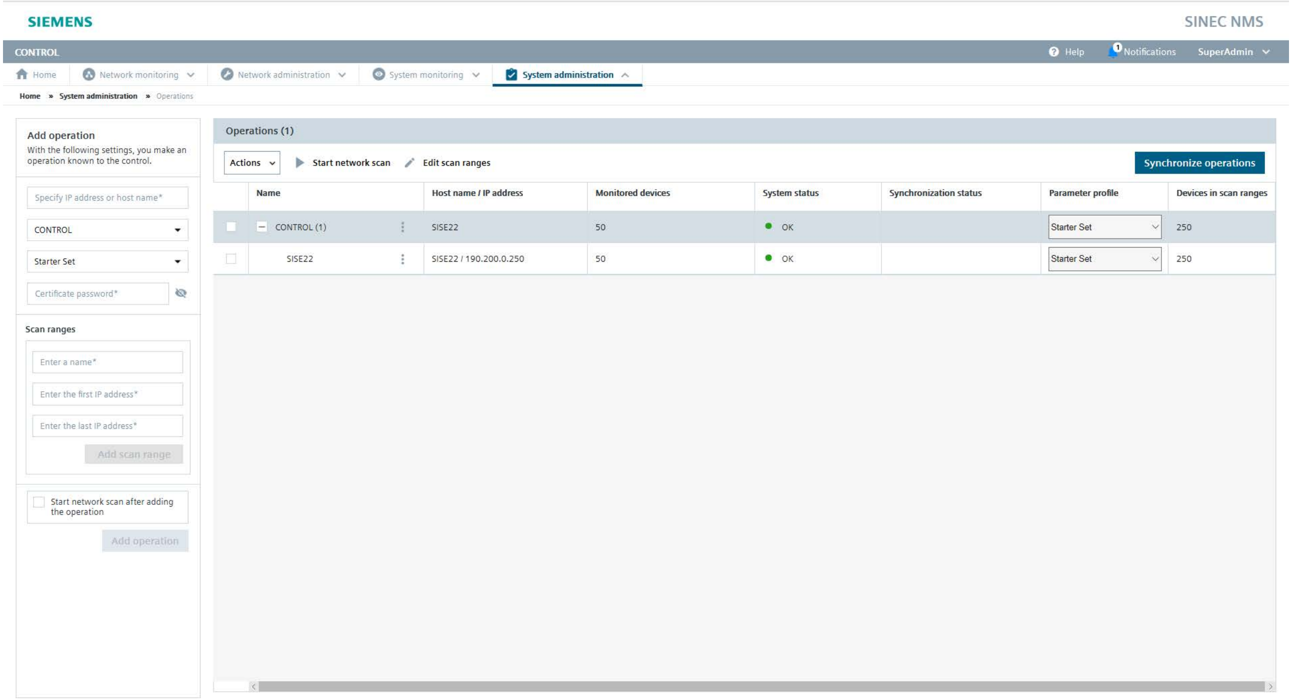
The "System monitoring > Audit trail" page displays audit log events for logging user and system activities. The audit log events can be exported as a CSV file. They are automatically deleted from SINEC NMS after 90 days.

System Administration 7

7.1 Operations

Control

You reach this page in the navigation of the control under "System administration > Operations".



Add operation

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

Specify IP address or host name*

CONTROL

Starter Set

Certificate password*

Scan ranges

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

Operations (1)

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 ranges
□	− CONTROL (1)	SISE22	50	● OK		Starter Set	250
□	SISE22	SISE22 / 190.200.0.250	50	● OK		Starter Set	250

Figure 7-1 Operation configuration on control

On the page "System administration > Operations", operations can be made known in the system and configured using parameter profiles.

For all operations, the scan ranges can be set centrally and network scans can be started. For information on the management and configuration of parameter profiles, refer to section Operation parameter profiles (Page 249).

The page is divided into the areas "Add operation" and "Operations". Operations added using the operator controls of the "Add operation" area are displayed in the "Operations" area.

Add operation

The following operator controls are available in the "Add operation" area:

- Hostname/IP address

  IPv4 address / hostname of the PC on which the operation is installed. When using IPv6, a host name must be specified. Make sure that SINEC NMS can reach the operation at the specified address. Addressing via localhost or via the IP address 127.0.0.1 is not permitted. If there is a NAT router between the control and the operation, refer to the "NAT" section below.

- Position in node structure

  During adding, operations are integrated into a hierarchical node structure, headed by the control. You can use the positioning setting to specify the node under which the operation is inserted. Operations can be inserted under the control node or under a subfolder. Subfolders can be created using the shortcut menu of the control and operations.

- Parameter profile

  Selection of the parameter profile to be used for the operation to be added. The parameter profiles available on the "System administration > Operation parameter profiles" page of the control are available for selection. For more information, refer to section Operation parameter profiles (Page 249).

- Certificate password

  Password for encrypting the PKCS12 container used to authenticate the operation at the control. For more information, refer to the "Authentication of operations" section.

- Name of the scan range

  Name for an IP address range in which the operation searches for devices. The names of the scan ranges must be unique within an operation.

- First IP address

  First IP address of a scan range in which the operation searches for devices. Make sure that the operation can reach the IP addresses of the specified scan range and that the scan ranges do not overlap within an operation.

  If a scan range is to contain only a single IP address, the same value can be specified as the first and last IP address.

- Last IP address

  Last IP address of a scan range in which the operation searches for devices. Make sure that the operation can reach the IP addresses of the specified scan range and that the scan ranges do not overlap within an operation.

  If a scan range is to contain only a single IP address, the same value can be specified as the first and last IP address.

- Add scan range

  Adds the scan range to the operation. Each operation can contain a maximum of 100 scan ranges.

- Start network scan after adding the operation

  Starts the network scan for the operation as soon as this is added. The search status of the operation is then displayed in the "Monitored devices" column. You configure the network adapter that uses an operation for the network scan on the respective operation under "Network monitoring > Settings > Network scan".

- Add operation

  Adds the operation with the configured properties. The connection between the control and the operation is then established first and after this the selected parameter profile is synchronized with the operation. A network scan is then performed if required. A maximum of 25 operations can be added.

  The first time you establish a connection between an operation and the control, follow the instructions under the "Authentication of operations" heading.

Operations

The following operator controls are available above the table:

- Actions
  - Start network scan

    Starts the network scan for the selected operation. When the action is executed for a subfolder, the network scan is started for all operations located below that subfolder. The network scan cannot be performed for operations that are currently being synchronized with the control. During the network scan, the system status "Executing network scan" is displayed in the "Monitored devices" column. You configure the network adapter that uses an operation for the network scan on the respective operation under "Network monitoring > Settings > Network scan". The network scan for the operation can also be started directly here.
  - Stop network scan

    Stops the network scan for the selected operation. When the action is executed for a subfolder, the network scan is stopped for all operations located below that subfolder.
  - Edit scan ranges

    Calls a dialog for managing the scan ranges for the selected operations. The network scan searches through all scan ranges that are enabled in this dialog.
  - Go to Op > Home

    Calls the "Home" page on the selected operation.
  - Go to Op > Net Mon > Devices

    Calls the page "Network monitoring > Devices" on the selected operation.

- – Edit discovery restriction list

  Opens a dialog in which the IP addresses of the devices for which PROFINET discovery is not to be performed can be specified. In each configured restriction, the devices can be specified via IP addresses, IP address areas or using CIDR notation. The IP addresses that SINEC NMS can use to access these devices must be specified for the devices. To exclude the devices of a configured restriction from PROFINET discovery, the restriction must be activated.

- – Retry

  If an operation is in the "Not reachable" system status, this action can be used to attempt to re-establish the connection between the control and the operation.

- – Delete

  Deletes the selected operations or subfolders. Only subfolders that contain no operations or subfolders can be deleted.

- – Collect log files

  Starts the collection of log files for the control and selected operations. Once the collection of log files is complete, a notification is displayed. Operation backups are not part of the generated log files.

- Synchronize operations / Synchronization required

  Changes made in the control to the configuration of operations must be synchronized with these operations by means of this button.
  If at least one operation has to be synchronized with the control, the button contains the labeling "Synchronization required". If no synchronization is required, the button is labeled "Synchronize operations".
  After a click on the button "Synchronization required", SINEC NMS synchronizes all deviating settings between control and operation with the affected operations. The operations to be synchronized do not need to be selected via the check boxes.
  The reason for required synchronization is indicated by the icons in the "Synchronization status" column.
  No synchronization is required after renaming an operation.
  The synchronization of an operation cannot be performed while a network scan is running for that operation.

The following properties are displayed in the table:

- Name

  Displays the names of the control, operations, and subfolders in a hierarchical structure. The subfolders are used to structure operations logically, for example, by location. The number of contained items is displayed in brackets after the name of the control and subfolders.

  Options in the shortcut menu, which can be called via the icon ⋮

  - – Create subfolder (available for control and subfolders)

    Creates a subfolder below the control or a folder under which operations can be inserted or subsequently positioned.

  - – Delete (available for operations and subfolders)

    Deletes the selected operation or subfolder. Only subfolders that contain no operations or subfolders can be deleted.

  If an operation has the "Not reachable" system status, you can force the deletion of this operation by selecting the corresponding check box in the confirmation dialog for the deletion of the operation. The data of the operation is removed from the control. Operations deleted in this way must be reinstalled before they can be added to a control again.

  - Rename (available for operations and subfolders)

    Opens a dialog in which you can rename the operation or subfolder. Transferring the new name to the system can take some time.

  - Move (available for operations and subfolders)

    Calls a dialog in which you can specify the desired position for the selected operation or subfolder. The operation or subfolder can only be positioned below the control or a subfolder.

  - Download certificate (available for operations)

    Downloads the certificate and the private key for the operation in a PKCS12 container, see the "Authentication of operations" section.

  - Edit IP address / hostnames (available for operations)

    Opens a dialog where you can change the IP address / hostname of the selected operation. To change the external IP address of an operation configured for operation on a NAT router, this IP address must also be changed in the "NATIPConfig.properties"configuration file, see "NAT" section below. In order to change the IP address / hostname, the certificate of the operation must be renewed, therefore you need to also specify a password for the new certificate in the dialog. If a multiple node installation is involved, you then need to import the new certificate on the operation, see section "Authenticating operations".

- Host name / IP address

  Hostname / IPv4 address of the control and the operations. The hostname/IP address for operations can be changed via the shortcut menu. SINEC NMS automatically detects a change in the hostname / IP address of the control. The PC on which the control is installed must be restarted for the new hostname/IP address to be adopted for the control.

- Monitored devices

  Number of devices that are monitored by the operation. For the control and subfolder that contain multiple operations, the device numbers are shown summarized. In addition, the status of network scans is displayed on the operations. For the control and subfolders that contain multiple operations, the scan status that has the highest priority is always displayed. The scan states are listed below according to their priority:

  - Stopping network scan
  - Stop network scan initiated
  - Executing network scan
  - Starting network scan

- System status

  The system status specifies the communication status between the control and the operations. If there are error states in the control and the operations, this is also

displayed in this column. After clicking on the column entry highlighted in blue, information about the cause of error states is displayed. System alarm messages with the status "Pending" are used to determine the system status. For more information on system alarm messages, refer to section System alarm messages (Page 237).
For the control and subfolders which contain multiple operations, the system status which has the highest priority is always displayed. The system statuses are listed below according to their priority:

– Not reachable

  The control or operation is not accessible. For an operation, this status is displayed as soon as the control receives no feedback from the operation for a certain time.

– First·contact

  The operation has not yet been authenticated at the control, see the "Authentication of operations" section.

– Initializing:

  The communication connection is established between control and operation.

– Error

  There is an error on the control or an operation. Check pending system alarm messages under "System monitoring > System alarm messages". For information on system alarm messages, refer to section System alarm messages (Page 237).

– Warning

  A warning message is pending for the control or an operation. Check pending system alarm messages under "System monitoring > System alarm messages". For information on system alarm messages, refer to section System alarm messages (Page 237).

– OK

- Synchronization status

  If the control is being synchronized with an operation, this is indicated by the "Synchronizing" message.

  If synchronization with an operation is required or has failed or there is a discrepancy between the system / HSP version of Control and Operations, this is indicated in this column by the following symbols and a corresponding message text:

  – ⚠

    A scan range or value of the parameter profile selected for the operation in the "Parameter profile" column has been changed but not yet synchronized with the operation.

  – ⚠

    The parameter profile selected in the"Parameter profile" column does not correspond to the parameter profile that is active on the operation or a scan range for the operation has been changed. The parameter profile must therefore be synchronized with the operation.

  – ⚠

    Synchronization with the operation has failed.

  – 🔄 System update required:

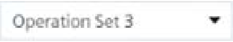
    The system version of an operation has not yet been updated to the system version of the control. Install the appropriate system version on the operation.
    For operations that with the "System update required" status, network scans and synchronization of parameter profiles with the control cannot be performed. In addition, navigation on these operations is not possible.

  – 🕒 HSP update pending:

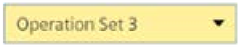
    An HSP installed on the control could not yet be transferred to the operation. Check the connection between the control and the operation.

- Parameter profile

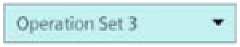
  Selection of the parameter profile for an operation. If the parameter profile for a subfolder is changed, this selection applies to all operations that are subordinate to this subfolder. If the selection in the drop-down list for an operation or subfolder is changed or the value of a selected parameter profile is changed on the "System administration > Operation parameter profile" page on the control, the parameter profile must be synchronized with this operation using the "Synchronization required" button. When no synchronization with an operation is required, the button label is "Synchronize operations".
  The reason for which synchronization is required is indicated by the color of the drop-down list.

  – 

    The selected parameter profile ("Operation Set 3" in this case) and all values of the parameter profile are synchronous between the control and the operation. No synchronization is required.

  – 

    For the operation, a new parameter profile ("Operation Set 3" in this case) was selected in the drop-down list that is not yet used on the operation, or a scan range for the operation was changed. The parameter profile must therefore be synchronized with the operation.

– 

Operation Set 3

The parameter profile selected in the drop-down list corresponds to the parameter profile that is active on the operation, but at least one value of this parameter profile has been changed on the page "System administration > Operation parameter profiles" on the control. The parameter profile must therefore be synchronized with the operation.

- Devices in scan ranges

  Number of devices that were found in the active scan ranges of the operation.

Authentication of operations

Before the communication connection between an operation and the control can be established for the first time, the operation must authenticate itself at the control with a certificate. Without this authentication, no communication is possible between this operation and the control and navigation in the Web interface of the operation. Make sure that the control and the operation do not have too large a deviation in the system time. Otherwise, the certificate may be rejected on the operation.

For a multiple-node installation, follow these steps to perform the authentication of an operation on the control: The steps described below are not required for a single-node installation.

Requirement: You have already added the operation to the control and configured a password for the operation, see the "Adding an operation" section.

1. Call the page "System administration > Operations" on the control.
2. In the shortcut menu of the operation you want to authenticate to the control, select the menu command "Download certificate".

   This downloads the certificate for the operation with private key as a PKCS12 container.
3. Place the PKCS12 container in a directory that you can access from the operation.
4. Log in to the operation with a user that has been assigned the "Super Admin" role.
5. Import the PKCS12 container and enter the password that was specified when the operation was added to the control.
6. Log out of the operation.

After the successful import, the communication connection between 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 in to the operation using this user data. On the control, the system status "OK" is displayed for the operation on the "System administration > Operations" page.

NAT

SINEC NMS supports the use of a NAT router between control and operations. In this case, the control must be in the external network and the operations must be in the internal network. The operations must then be added to SINEC NMS with their external IP address. The external IP addresses of the operations must also be assigned to their internal IP addresses in the NAT configuration file "NATIPConfig.properties" as follows:

<External IP address of the operation>=<Internal IP address of the operation>

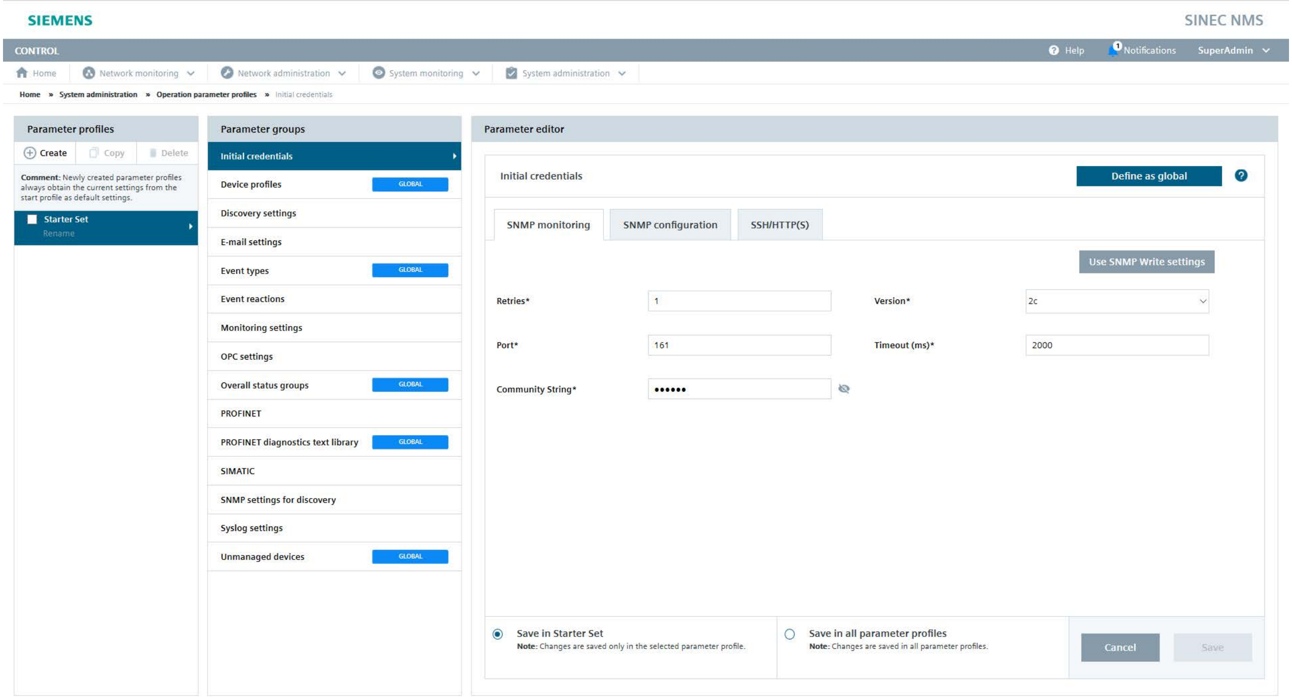
Example: 10.201.0.240=10.101.0.240

You can find this configuration file on the control in the SINEC NMS installation directory under "SINECNMS/config".

7.2 Operation parameter profiles

Control

You reach this page in the navigation of the control under "System administration > Operation parameter profiles".



Comment: Newly created parameter profiles always obtain the current settings from the start profile as default settings.

Retries*	1	Version*	2c
Port*	161	Timeout (ms)*	2000
Community String*	••••••		

● Save in Starter Set
Note: Changes are saved only in the selected parameter profile.

○ Save in all parameter profiles
Note: Changes are saved in all parameter profiles.

Figure 7-2 Configuration of operation parameter profiles on control

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

Select the configured parameter profiles on the "System administration > Operations" page of the control and synchronize them with the desired operations.

Note

Synchronization is required after every change to the parameter profiles

Note that parameter profiles must be synchronized with the operations after each change. For information on synchronizing parameter profiles with operations, refer to section Operations (Page 241).

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

The parameter profile "Start profile" is available by default and contains the default settings of all parameters. When a new parameter profile is created, the current settings of the start profile are always used as default settings. After changes have been made to the start profile, the changed settings are used as default settings for new parameter profiles.

The parameters that can be configured in parameter profiles are divided into several parameter groups. These parameter groups are displayed in the "Parameter groups" area. After selecting a parameter group, the associated parameters are configurable in the "Parameter editor" area. For information on the configurable parameter groups, refer to section Parameter groups (Page 250).

Changes in a parameter group for which the property "Global" or "Custom global" is displayed in the area"Parameter groups" 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 only to be applied to the selected parameter profile or to all parameter profiles, including the start profile. For this purpose, the option boxes "Save in [Selected parameter profile]" and "Save in all parameter profiles" are available.
For the parameter groups "Device profiles", "Event types", "Overall status groups", "Unmanaged devices" and "PROFINET diagnostics text library", the property "Global" is preselected and cannot be removed. The property can be set user-defined for all other parameter groups. The buttons "Define as global" and "Remove property "global"" are available in the "Parameter editor" for this purpose.

7.2.1 Parameter groups

7.2.1.1 Initial credentials

In the parameter group "Initial credentials", you configure the SNMP and CLI settings which are used by default for devices in the Device credential repository on the operations under "Network administration > Device credential repository". The configured initial credentials for devices can be restored after manual changes have been made in the Device credential repository.

SINEC NMS initially tries to detect devices with the settings from the parameter group "SNMP setting for discovery". If this is successful, the initial credentials in Device credential repository will be overwritten by the settings from the parameter group "SNMP settings for discovery".

7.2.1.2 Device profiles

Profiles give SINEC NMS flexibility during device discovery, device monitoring and device display. Profiles describe device types in terms of common properties.

SINEC NMS distinguishes between the following profile types:

- Device profile

  This profile type contains information required for discovery and monitoring of a network device.

- Monitoring profile

  This profile type contains information that is only required for monitoring a network device.

The term "Device profile" is used to represent both profile types when the "Monitoring profile" is not explicitly used.

Based on the stored profiles, SINEC NMS searches for those device profiles that contain the appropriate discovery rules for each newly discovered device. The assigned device profile is used to classify and display the network device. SINEC NMS can only monitor devices to which device profiles have been assigned. If no suitable device profile is found for a network device during the network scan, SINEC NMS assigns a default profile to the device. To intentionally exclude devices from monitoring by SINEC NMS, you can disable the default profiles. Refer also to the information in the section Disabling default profiles (Page 54).

Create new profiles

New profiles are always created based on existing profiles. To create a new profile, you must therefore always select an existing profile as the template.

Default profiles

If no assignment based on the discovery rules of profiles is possible on the discovery of a device, SINEC NMS assigns an enabled default profile to this device that has not been uniquely identified. You cannot assign devices to disabled profiles.

- Step 1:

  If it is clear from the device ID that this is a Siemens device, one of the following enabled default profiles is used:

  – SIEMENS_Standard

  – SIEMENS_Basic

- Step 2:

  If no assignment is possible in step 1, an enabled default profile is assigned based on the protocols supported by the device.

  – DEFAULT_SNMP_DCP_Device

  – DEFAULT_SNMP_Device

  – DEFAULT_DCP_Device

  – DEFAULT_ICMP_Device

Device discovery using SNMP

During discovery, SINEC NMS attempts to identify the following criteria based on the SNMP data of the device:

1. sysDescr (OID 1.3.6.1.2.1.1.1.0):

   A textual description of the device (system hardware type, software operating system, network software etc.).

2. lldpLocSysDesc (OID 1.0.8802.1.1.2.1.3.4.0):

   The value of the character string is required for the system description mentioned above. If the local agent supports IETF RFC 3418, the lldpLocSysDesc object should have the same value as the sysDescr object.

3. automationSwRevision (OID 1.3.6.1.4.1.4329.6.3.2.1.1.5.0)

4. automationOrderNumber (OID 1.3.6.1.4.1.4329.6.3.2.1.1.2.0)

5. DiagMonitor_StationOrderNumber (OID 1.3.6.1.4.1.4196.1.2.2.13.0)

   Article numbers of SIMATIC IPCs on which the software "DiagMonitor" was installed (only for SIMATIC IPC device profiles)

6. DCP_ID

7. sysObjectID (OID 1.3.6.1.2.1.1.2.0):

   This value is assigned within the "SMI enterprises sub tree" (1.3.6.1.4.1) and contains the highest OID under which the private MIB of the device manufacturer can be found.

Automatic device profile and device type assignment

Based on the SNMP data, SINEC NMS searches for the device profiles that contain the appropriate discovery rules for each newly discovered device.

- Step 1 - Determine device profile

  If more than one device profile has a rule that suits the device, the priority of the rule decides which is used.

  If the same criterion exists in more than one device profile, the profile with the criterion whose stored text is longest wins.

- Step 2 - Use device type rules for the device within the selected device profile

  SINEC NMS identifies the suitable device type and uses the icon specified here for the display. If the device type cannot be identified, SINEC NMS uses the default symbol stored in the device profile.

Device discovery using PROFINET

The PROFINET discovery can be enabled in the "Basic data" tab of a device profile. This activates device profile and device type rules for this device profile that contain the article numbers of the devices identifiable via PROFINET as assignment criteria. The article numbers of device type rules can be edited after the check box in the "SNMP/DCP criteria" area has been selected. The corresponding device profile and device type rules are then updated automatically.

Automatic reassignment of profiles and device types

For devices that were assigned one of the standard profiles during discovery, SINEC NMS runs through the process described above for automatic profile and device type assignment again at regular intervals looking for more suitable profiles and device types they contain for these devices. The default interval for automatic reassignment is 70 minutes and is configurable in the parameter group "Monitoring settings". In addition to this, the automatic reassignment is always performed when a device with an assigned standard profile changes from the "Not reachable" status to the "Reachable" status.

Note

Effect of assignment of the reference topology

If a device has been assigned a new device profile, it is automatically removed from the reference topology and must be adopted again as a reference device.

"Device profiles" parameter group

The existing device and monitoring profiles are displayed in the parameter group "Device profiles". The profiles can be managed, enabled and disabled using the "Actions" drop-down list.

Actions

The following functions are available via the "Actions" drop-down list:

- Create device profile

  Opens a dialog via which a new device profile can be created based on a selected device profile. In this dialog, you can select whether the discovery rules and/or the device type rules of the selected device profile should be transferred to the new device profile.
  No new device profile can be created without the selection of a base profile.

- Create monitoring profile

  Opens a dialog via which a new monitoring profile can be created based on a selected monitoring profile.
  No new device profile can be created without the selection of a base profile.

- Edit

  Opens the dialog for editing the properties of the selected profile, refer to section Device profile properties (Page 254).

- Delete

  Deletes the selected device profile. If a device profile to which devices are assigned is deleted, these devices are no longer monitored by SINEC NMS. Default profiles cannot be deleted. For more information on default profiles, refer to section Basics (Page 53).

- Enable

  Enables the selected device profile. SINEC NMS assigns devices exclusively to activated profiles. Devices that cannot be assigned to any profiles are not monitored by SINEC NMS. For more information, refer to section Device profiles (Page 251).

- Disable

  Disables the selected device profile. SINEC NMS assigns devices exclusively to activated profiles. Devices that cannot be assigned to any profiles are not monitored by SINEC NMS. For more information, refer to section Device profiles (Page 251).

- Restore

  Restores the factory settings of system-defined device profiles.

- Export profiles

  Exports the selected device profiles to a ZIP file.

- Import profiles

  Imports device profiles from a ZIP file exported from SINEC NMS. After selecting the ZIP file, you can determine which device profiles are to be imported. Existing device profiles are overwritten during import.

Device profile properties

By selecting a device profile with the action "Edit", the properties of the device profile are displayed in the following tabs.

Basic data

The following properties are available in the "Basic data" tab:

- Name

  Name of the device profile.

- ID

  ID of the device profile.

- Device category

  Categorization of devices of this device profile.

  If the "Device category" device icon style is selected in the topology settings of the operation, the selection of the device category determines the icon with which devices of this device profile are displayed in the topology representations.

- Profile module

  Display of the device family name. The entry is relevant if you want to modify the monitoring profile of the device. The monitoring profile of a device must always belong to the same profile module as the device profile.

- Vendor

  Manufacturer of the devices of the device profile. If a device is assigned a device profile without a vendor ID, the DCP ID is used to identify the vendor.

- Use for discovery

  When this check box is selected, the device profile is enabled and used for device discovery.

- Created on

  Date and time the profile was created.

- Use for PROFINET discovery

  When this check box is selected, devices can be assigned to this device profile and the device types contained can be assigned using article numbers. When the check box is selected, device profile and device type rules are activated for this device profile that contain the article numbers of the devices identifiable via PROFINET as assignment criteria. The article numbers of device type rules can be edited after the check box in the "Criteria" area has been selected. The corresponding device profile and device type rules are then updated automatically.

- Updated on

  Date and time of the last profile update.

- System-defined

  When this check box is selected, the device profile is set by the system and was not created by the user. System-defined profiles can be reset to the factory settings and restored after deleting. The setting cannot be changed.

- Description

  Description of the device profile.

- Device category and standard profile icon

  Icon of the selected device category and selected default profile icon

  In the topology settings of the operation, you can specify which of these two icons is used to represent devices in topologies. The device category icon is used when the "Device category" option is selected in the topology settings. The default profile icon is used when the "Device profile" option is selected in the topology settings and no suitable icon was found for the respective device type.

  The assignment of icons to device categories cannot be adapted.

Discovery rules

The "Discovery rules" tab contains all the rules to be checked through during the assignment of devices to device profiles. The table must contain at least one rule so that the profile for monitoring can be enabled. Each rule must be unique within an operation and may only occur once.

Discovery rules for the PROFINET discovery using article numbers are derived from device type rules and cannot be changed in the "Discovery rules" tab. Such discovery rules can be edited by editing the article numbers in the "Criteria" area of device type rules. The corresponding device profile and device type rules are then updated automatically.

The following wildcards can be used to specify the discovery rules for SNMP / DCP:

- * (Any number of characters including spaces)
- ? (The character preceding this wildcard can occur not at all or once, including spaces)
- . (Exactly any one character including spaces)

If the characters above are not to be used as wild cards they must follow a "\" e.g. "\?".

The "Discovery rules" tab is not available for monitoring profiles.

Device types

In the "Device types" tab, names, symbols and rules can be configured for the devices of the device profile.

If no rule is suitable for the type of a discovered device, the profile name will be used as the name of the device type and the default icon of the profile will be used to display the device.

The rules for device types are specified using the following protocol-specific criteria:

- PROFINET:
  Specifying the article numbers. Several article numbers are separated by commas. The use of the wildcard character (*) is not permitted.

  It is only possible to specify article numbers in the device type criteria if the check box "Use for PROFINET discovery" has been selected in the "Basic data" tab. The specified article numbers are also used as device profile criteria.

- SNMP / DCP:

  Specifies the SNMP value. The use of the following wild cards is possible:

  – * (Any number of characters including spaces)

  – ? (The character preceding this wildcard can occur not at all or once, including spaces)

  – . (Exactly any one character including spaces)

  So as not to use the named characters as wildcards these must follow a "\\", e.g. "\\?"

The "Device types" tab is not available for monitoring profiles.

OID sets

The "OID sets" tab displays the sets of the OIDs which are read out from devices of the device profile. Per device profile, a maximum of 90 OIDs can be created in user-defined OID sets, 30 OIDs each for the data types "Integer32", "Uinteger32" and "String". The OIDs are then displayed in the Configuration Cockpit in the details of corresponding devices.

Only user-specific OID sets and OIDs from the system-defined OID set "Automation" can be modified. For OIDs from the OID set "Automation", an alternative OID can be specified or a fixed display value defined. In addition to this, rules can be specified for extracting partial values from the individual OIDs. Other OID sets that are read by SINEC NMS are displayed and cannot be modified.

Thresholds

The "Thresholds" tab contains thresholds for monitored data. Thresholds are linked to operators and trigger events if values are exceeded for example. You can only define new thresholds for OIDs from user-defined OID sets. Create user-defined OID sets in the "OID sets" tab.

Creating or editing thresholds opens an editor with the following parameters:

- Name

  Name of the threshold.

- Source

  For user-defined thresholds you can select the OID to be checked from a user-defined OID set. No selection option is available for system-defined thresholds.

- Data type

  Data type of the threshold. The data type selected here decides the operators that can be used for the check. No selection option is available for system-defined thresholds.

- System-defined
  - Check box is enabled: It is not possible to create new value checks. The values and events of existing value checks can be adapted.
  - Check box is disabled: It is possible to create new value checks. All the values and events of existing value checks can be adapted.
- Overall status group

  Selection of the overall status group from where the triggering event originates.
- Use binary format for the threshold check

  When this check box is selected, integer values to be checked are interpreted as binary values. In the "Values" area, the match with bit patterns, which are specified as follows, can be checked:
  - Order of notation: LSB (from right to left)
  - Usable characters: 0, 1, ?. The placeholder ? allows both binary values.
  - Maximum length: 32 characters
  - Leading 0s do not need to be noted
  - The bit pattern must not consist only of the placeholder ?.
- "Values" area

  In this area, you specify value checks with the aid of operators and events that should be triggered when check conditions are met.

System-defined thresholds can be copied to other device profiles using the "Copy" button of the "Thresholds" tab. Copying is only possible when thresholds with the same names exist in the target profiles. If a threshold to be copied does not exist in the target profile, this threshold is skipped during copying. User-defined thresholds cannot be copied to other device profiles. A maximum of 10 system-defined thresholds can be copied to a maximum of 10 target profiles.

7.2.1.3 Discovery settings

Basic settings

The following basic settings are available in the "Basic settings" area:

- Automatic network scan

  If this check box is selected, the network scan is started automatically at the set interval.
- Interval

  The scan interval for the automatic network scan.

- Start

  Date and time at which the automatic network scan is performed the first time.
- End

  Date and time at which the automatic network scan is performed the last time. If no end date and no end time are specified, the automatic network scan is performed without any limit in the configured scan interval.

Advanced settings

The following basic settings are available in the "Advanced settings" area:

- Discovery of NAT / routers

  Select this check box so that NAT routers and devices in switched / routed networks are correctly discovered during the network scan. Selecting the check box increases the time required for the network scan, depending on the existing network constellation. This setting does not influence the monitoring of NAT routers and NAT devices. If it is not known whether there are NAT routers in the network, the check box should be selected and the longer time for the network scan must simply be accepted.
- Trust newly discovered devices
  - Check box selected: SINEC NMS classifies the SSH/HTTPS fingerprints of devices discovered during the network scan as trustworthy. The corresponding devices are displayed on the "Network administration > Device credential repository" page of the respective operation with the "Trusted" trust status. Whether configuration access to these devices is allowed by default can be defined via the "Block configuration access for newly discovered devices" check box. Configuration access for discovered devices can be set manually on the "Network administration > Configuration Cockpit" page.
  - Check box is cleared: SINEC NMS classifies the SSH/HTTPS fingerprints of devices discovered during the network scan as not trustworthy. The corresponding devices are displayed on the "Network administration > Device credential repository" page of the respective operation with the "Untrusted" status. Configuration access to these devices is blocked by default and cannot be configured manually.
- Block configuration access for newly discovered devices (can only be enabled when the "Trust newly discovered devices" check box is active)

  If you select this check box, newly discovered devices cannot be configured via SINEC NMS. If the "Trust newly discovered devices" check box is selected, configuration access for discovered devices can be set manually on the "Network administration > Configuration Cockpit" page of the respective operation.

DCP discovery type:

- Enable DCP network adapters dynamically

  If this option button is enabled, all DCP network adapters on the operation whose subnets overlap with an enabled scan area are automatically enabled. The DCP network adapters can be manually disabled or enabled on the operation using this setting. If a DCP network adapter has been manually disabled on an operation, it will no longer be automatically enabled afterwards.

  The following setting determines which devices are included in the network scan:

  – Include all devices discovered with DCP in the result: Devices outside the specified IP address ranges are also discovered and monitored.

  – Only include the devices in the result that are located in one of the specified IP address ranges

- Disable all DCP network adapters

  If this option button is enabled, all DCP network adapters on the operation are disabled. The DCP network adapters cannot be manually enabled on the operation using this option.

7.2.1.4 E-mail settings

In the parameter group "E-mail settings", you configure the data of the e-mail account that SINEC NMS uses for sending e-mails which inform recipients about events that have occurred. If you want the operation to use the same e-mail settings as the control, select the "Use e-mail settings of Control administration" check box. Reactions to events that have occurred are configured in the parameter group "Event reactions", refer to section Event reactions (Page 261).

On the page "System administration > Control administration", configure the data of the e-mail account that SINEC NMS uses for sending the following e-mails:

- E-mails notifying users about the completion of reports.
- E-mails to locally configured users who have forgotten their password.

For information on the "System administration > Control administration" page, refer to section Control administration (Page 278).

If communication with the e-mail server used is to be encrypted, the certificate of the e-mail server must be stored in the Windows certificate manager of the operation.

7.2.1.5 Event types

Events are divided into Network events and System events. Network events provide information on status changes in the network or contain device traps. System events contain system-related status information.

In this parameter group, you can by default disable existing event types of both categories, enable them and adjust their display in multiple languages. You can also create new network event types and trap types. For network events of a created network event type to be triggered, the network event type must be assigned to an overall status group and then assigned to a threshold in the profiles of the required devices. When creating a trap type, you must specify the OID to which the traps to be received relate.

For information on overall status groups, refer to section Overall status groups (Page 265).

For information on configuring thresholds for device profiles, refer to section Device profiles (Page 251).

7.2.1.6 Event reactions

SINEC NMS can send e-mails to configured recipients as reactions to triggered events. For SINEC NMS to be able to send e-mails, the e-mail settings must be configured in the parameter group "E-mail settings"; refer to section E-mail settings (Page 260).

Operator controls

The following operator controls are available in the header:

- Create

  Opens the editor to create event reactions, see the "Editor for event reactions" section.

- Edit

  Opens the editor for editing the selected event reactions, refer to section "Editor for event reactions".

- Delete

  Deletes the selected event reactions.

- Enable

  Enables the selected event reactions. When an associated event occurs, only enabled event reactions are executed.

- Disable

  Disables the selected event reactions. Disabled event reactions are not executed.

- Default e-mail recipient

  Specification of e-mail addresses to which e-mails are sent if no specific e-mail recipient was configured for an event reaction.

  If multiple e-mail recipients are specified, these need to be separated from each other by a semicolon.

Properties

The properties of created event reactions are displayed in the following columns:

- State

  Shows whether the event reactions are enabled or disabled. When an associated event occurs, only enabled event reactions are executed.

- Event type

  Event type for which the event reactions are configured. When events of this type occur, the configured event reactions are executed.

- E-mail recipient

  E-mail addresses to which e-mail notifications are sent when events of the configured event type occur. The e-mail notifications are only sent if the event reactions have been enabled.

- Devices

  The event reactions are executed if the devices specified here trigger an event of the configured event type.

Editor for event reactions

The event reactions editor opens when you create or edit an event reaction. The following operator controls are available for configuring event reactions:

- Event types

  Events of the event types selected via the check box trigger the event reactions. You can search for the desired event types using the input box. All event types from the parameter group "Event types" are available, refer to section Event types (Page 260).

- E-mail recipient

  Specify the e-mail recipients who are to be informed by e-mail when an event of the configured event type occurs. The e-mail can be sent either to specific e-mail recipients or to configured default e-mail recipients.

  If multiple e-mail recipients are specified, these need to be separated from each other by a semicolon (there must be no spaces).

- Devices

  In this area, you can specify that the event reactions are only executed if the associated event is triggered by selected devices.

  The following options are available:

  – Devices in views: The event reactions are only executed when the devices of the specified views have triggered the associated event.

  – All devices: The event reactions are executed regardless of which devices have triggered the associated event.

7.2.1.7 Monitoring settings

The following settings are available in the parameter group "Monitoring settings":

Reachability via ICMP (Ping)

- ICMP retries
  Number of retries for ICMP polling after a device has not responded to the first ICMP polling. After this, the device receives the overall status "Not reachable" or "Not connected".
- ICMP timeout
  Specification of time in seconds after which ICMP polling is considered failed.
- ICMP query interval

  Specification of the time between ICMP queries in seconds if ICMP retry attempts were specified.

Reachability via DCP (PROFINET)

- DCP query interval
  Specification of the time between DCP polling in seconds if DCP retry attempts were specified.
- DCP retries
  Number of retries for DCP polling after a device has not responded to the first DCP polling. After this, the device receives the overall status "Not reachable". If this is an alternating device, it receives the status "Not connected".
- PROFINET reachability retries

  Number of retries for PROFINET reachability queries after a device has not responded to the first query. After this, the device receives the state "Not reachable" via PROFINET.

General monitoring settings

In the general monitoring settings, you can select one of the following option buttons for the configuration of LAN port statistics.

- Detection of duplicate IP addresses

  If this check box is selected, SINEC NMS checks whether the same IP address exists more than once in the network.
- Permanently disable LAN port statistics for all monitored devices

  When this option box is enabled, no port statistics of LAN ports are monitored, not even for newly discovered devices. The setting cannot be changed manually for individual LAN ports.
- Permanently enable LAN port statistics for all monitored devices

  When this option box is enabled, information about data traffic, port load and error rates is monitored using SNMP or possibly PROFINET for the LAN ports of all monitored devices. If devices are newly discovered and monitored, the port statistics for their LAN ports are enabled automatically. The setting cannot be changed manually for individual LAN ports.

Note

For gigabit ports with SNMP V1 monitoring, port statistics cannot be enabled due to the protocol.

Note

Enabling port statistics for all LAN ports can lead to high network load.

- Configure LAN port statistics manually for all monitored devices

  The current settings for LAN port statistics are retained and can be changed manually for the individual ports.
  When you select this option box, you can optionally select the following check box:

  – Disable LAN port statistics for all monitored devices once

    If this check box is selected, the LAN port statistics for all monitored devices are disabled. The settings for the LAN port statistics can then be changed manually for the individual ports.

Device profile changes

- Automatic device type change
  If this check box is selected, for devices that were assigned default profiles, an automatic search is made for more suitable device profiles and the device types contained in them.
- Interval for device type change
  For devices that have been assigned to standard profiles, a search is made for more suitable device profiles and device types contained therein at specified intervals. The default interval for automatic device type change is 70 minutes and is configurable. In addition to this, the automatic device type change is always performed when a device with an assigned standard profile is reachable.

7.2.1.8 OPC settings

If the "With user authentication" option is selected for an operation in the "Port settings" tab of the Operation Monitor, access to the OPA UA server of this operation requires authentication for the user whose data is configured in this parameter group.

7.2.1.9 Overall status groups

Function of overall status group

An overall status group is a group of functionally related events that influence the overall status of a device. Each event within an overall status group can be assigned an overall status that the device will adopt when the corresponding event condition occurs.

Conventions for events in the overall status groups

The following conventions apply to events in the overall status groups:

- An overall status group must contain at least one event.
- An event can only belong to one overall status group.
- Only events assigned to an overall status group can influence the overall status of a device.

States of events in overall status groups

To form the overall status of devices, various states that events from overall status groups can adopt are significant. These event states are displayed in the "Event status" column of the event list on the pages for network monitoring of operations.

Table 7- 1 Meaning of event states

Event status	Meaning
Pending	When an event that is assigned a negative overall status (every overall status except "OK" and "Not connected") is triggered for a device, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device.
Resolved automatically	An event that was removed from the list of pending events by SINEC NMS is identified by the event status "Resolved automatically". Resolved events can no longer influence the overall status of devices. Pending events are automatically resolved by the following events: • Events assigned the "OK" or "Not connected" overall status from the same overall status group • Pending events of the same overall status group (regardless of the assigned overall status)
Resolved manually	An event that was removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually".
-	A triggered event that is not assigned to any overall status group or is not assigned any overall status in the group has no event status.

Rules for forming the overall status

The overall status of devices is formed by events from the overall status groups according to the following rules:

- The event with the most negative overall status pending for the device decides the overall status of the device. The classification as the most negative overall status applies to all the overall status groups.
- After the automatic or manual resolution of pending events, the device receives the most negative overall status assigned to one of the remaining pending events. If there is no further event pending for the device, the device receives the overall status "OK" or "Not connected".

Example of forming overall states

In the following example, various events are triggered by a device that belong to different overall status groups.

The overall status groups are made up of the following events:

- Overall status group "A":
  - Event "A1": Warning - Overall status "Maintenance demanded"
  - Event "A2": Warning - Overall status "Maintenance required"
  - Event "A3": Info - Overall status "OK"
- Overall status group "B":
  - Event "B1": Warning - overall status "Error"
  - Event "B2": Info - Overall status "OK"
- Overall status group "C":
  - Event "C1": Warning - Overall status "Maintenance demanded"

The following table shows the changes in the device overall status based on the occurrence of these events and the events pending for the device. Initially there are no pending events for the device and the device has the overall status "OK".

Table 7- 2 Example trend of overall device states

Triggered event / user action	Overall status of the device	Events pending for the device
A1	Changes from "OK" to "Maintenance demanded".	• A1 - "Maintenance demanded"
A3	Changes from "Maintenance demanded" to "OK".	None
C1	Changes from "OK" to "Maintenance demanded".	• C1 - "Maintenance demanded"
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None
A1	Changes from "OK" to "Maintenance demanded".	• A1 - "Maintenance demanded"

Triggered event / user action	Overall status of the device	Events pending for the device
A2	Changes from "Maintenance demanded" to "maintenance required".	• A2 - "Maintenance required"
B1	Changes from "Maintenance required" to "Error".	• A2 - "Maintenance required" • B1 - "Error"
C1	"Error", no change.	• A2 - "Maintenance required" • B1 - "Error" • C1 - "Maintenance demanded"
A3	"Error", no change.	• B1 - "Error" • C1 - "Maintenance demanded"
B2	Changes from "Error" to "Maintenance demanded".	• C1 - "Maintenance demanded"
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None

Types of overall status groups

A distinction must be made between system-defined and user-defined overall status groups.

In system-defined overall status groups, the assignments of overall states to event types belonging to the overall status group can be adapted. Event types of the overall status group can also be enabled/disabled. Existing event types cannot, however, be removed from a system-defined overall status group. It is also not possible to add an event type to a system-defined overall status group.

Note

System-defined overall status group "POF Power Margin - Cable length"

The event types of the system-defined overall status group "POF Power Margin - Cable length" are disabled by default. If these event types should be included in the device monitoring, they need to be enabled.

Event types available in the "Event types" parameter group can be included in user-defined overall status groups. Overall states can be freely assigned to these event types. It is also possible to remove event types from user-defined overall status groups. A maximum of 100 overall status groups can be created.

Structure of the parameter group

In the parameter group "Overall status groups", system-defined and, if necessary, user-defined overall status groups are displayed.

The overall status groups can be managed and reset to factory settings using the operator controls of the header.

The event types of the overall status group are displayed in the dialog for configuring an overall status group. Assigned event types can be enabled or disabled for triggering or assigned to overall states which devices are to adopt when the associated events are triggered. User-defined overall status groups can be assigned event types that are available in the parameter group "Event types".

7.2.1.10 PROFINET

PROFINET monitoring and PROFINET diagnostics are only supported for devices with PROFINET IO capability. The PROFINET monitoring settings listed below only affect monitored devices.

- PROFINET discovery

  If this check box is selected, PROFINET is used to detect devices. You can configure which devices are excluded from PROFINET discovery on the "System administration > Operations" page, see section Operations (Page 241).

- PROFINET monitoring
  If this check box is selected, PROFINET monitoring and PROFINET standard diagnostics as well as PROFINET channel diagnostics of PROFINET devices are enabled globally. This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations. Events relevant for diagnostics can only be triggered when PROFINET monitoring is enabled. They are displayed in the event list of the operations.

- PROFINET monitoring of port statistics (can only be selected if the "PROFINET monitoring" check box is enabled)
  If this check box is selected, PROFINET monitoring of LAN port statistics for PROFINET devices is enabled globally. This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations. On this page, the port statistics must also be enabled in the device details for the desired LAN port.

- Use PROFINET monitoring settings for newly discovered PROFINET devices
  If this check box is enabled, the configuration of the two options named above is used for newly discovered devices.

- Duplicate PROFINET IO name detection
  If this check box is selected, the operations check whether the same PROFINET IO device name exists more than once in the network.

  Note

  Duplicate PROFINET IO device names are not permitted as per the PROFINET standard.

- Detect alternating devices automatically (based on the Fast Startup function of the devices)
  When this check box is selected, devices that support the "Fast Startup" function are automatically discovered by the operations as alternating devices when they start up and they are included in the monitoring.

- Learn connections of alternating devices automatically
  When this check box is selected, the operations learn all connections of alternating devices and show these in the topology display on the page "Network monitoring > Topology". Learned connections are historical connections that remain displayed after they have been terminated.
- Automatically configure ports with several learned connections as docking ports (can only be selected if the "Learn connections of alternating devices automatically" check box is also selected)
  When this check box is selected, the operations automatically configure ports with more than one learned connection as docking ports.

7.2.1.11 PROFINET diagnostics text library

The PROFINET diagnostics text library contains all texts that SINEC NMS displays in the "Text" column of the PROFINET channel diagnostics as well as details in the corresponding events on the operation. The PROFINET channel diagnostics is available in the "PROFINET" device detail tab, which can be accessed on the "Network monitoring > Devices" page of an operation for a device. The event list is available on all pages for network monitoring of operations.

The PROFINET diagnostics texts can be made available to SINEC NMS by importing files in the XML language GSDML. In channel diagnostics, SINEC NMS assigns the raw data read out from the devices to the texts from the PROFINET diagnostics text library. If there are no texts for the raw data, the raw data is displayed in hexadecimal format. A maximum of 10 XML files can be imported at one time. English and German are the languages supported for the texts of the PROFINET diagnostics text library. When the"Overwrite existing diagnostics texts" check box is selected, existing texts are overwritten during import. If texts to be imported do not exist in a language, the English versions are used when the texts of this language are overwritten. Standardized PROFINET texts and standardized texts for Siemens devices are available by default in SINEC NMS. Each text can be enabled, disabled or deleted in the PROFINET diagnostics text library. After disabling texts, the corresponding events are no longer triggered and the data belonging to them is not displayed in the PROFINET channel diagnostics. When a text is deleted from the PROFINET diagnostics text library, the raw data belonging to it is displayed in hexadecimal format in the PROFINET channel diagnostics and in the event details.

7.2.1.12 SIMATIC

Devices for which SIMATIC monitoring is supported are referred to in this document as "with SIMATIC capability". These devices are listed in the readme file of SINEC NMS. The following SIMATIC monitoring settings are available:

- SIMATIC monitoring
  If this check box is set, SIMATIC monitoring of CPUs with SIMATIC capability is enabled globally. This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations.
- SIMATIC monitoring of assigned devices (can only be selected when the "SIMATIC monitoring" check box is enabled)
  When this check box is selected, the SIMATIC monitoring of device data that is available on CPUs with SIMATIC capability via higher level PROFINET IO devices is enabled

globally. This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations.

- SIMATIC monitoring including assigned devices and SIMATIC event messages (can only be selected if the check box "SIMATIC monitoring of assigned devices" is selected)
  If this check box is selected, the operations log on to CPUs with SIMATIC capability to receive SIMATIC event messages.
  In the Web interface of the operations, the received event messages are displayed in the global and in the device-specific event list of the CPU and are marked with the status "Incoming" (for active status) or "Outgoing" (for no longer active status). This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations. The logon to receive SIMATIC event messages from CPUs with SIMATIC capability can be restarted in this Web interface by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".
- SIMATIC monitoring including assigned devices and SIMATIC alarm messages (can only be selected if the check box "SIMATIC monitoring of assigned devices" is selected)
  If this check box is selected, the operations log on to CPUs with SIMATIC capability to receive SIMATIC alarm messages.
  In the Web interface of the operations, the received alarm messages are displayed in the global and in the device-specific event list of the CPU and are marked with the status "Incoming" (for active status) or "Outgoing" (for no longer active status). This monitoring on the device level is enabled using device parameters of the same name on the "Network monitoring > Devices" page of operations. The logon to receive SIMATIC alarm messages from CPUs with SIMATIC capability can be restarted in this Web interface by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".

Note

Requirements for receiving and displaying SIMATIC event messages / alarm messages

In order for the operations to be able to receive and display SIMATIC event messages / alarm messages from a CPU with SIMATIC capability, the following requirements must be met:

- In the STEP 7 configuration of the CPU, SIMATIC event messages / alarm messages must be enabled so that end devices can log on to the CPU to receive the messages. Enabling the messages for operations is based on the same principle as for HMI devices.
- To assign the messages to message texts, the option "Enable Web server on module" must be enabled in the STEP 7 configuration of the CPU. Alternatively, the option "Generate and load Web server configuration" can be enabled in STEP 7 as of V5.5.4. However, this is not available for all CPUs with SIMATIC capability.

For more information, refer to the Siemens Industry Online Support:
Link (https://support.industry.siemens.com/cs/ww/en/ps/13828)

7.2.1.13 SNMP settings for discovery

In the parameter group "SNMP settings for discovery", you configure profiles for SNMP settings with which SINEC NMS logs on to devices in order to detect devices with SNMP. SINEC NMS hereby uses all enabled SNMP profiles in descending order of their SNMP versions. Disabled SNMP profiles are not used for device discovery.

If SINEC NMS was able to detect a device with one of the SNMP profiles, the device's settings are transferred to the Device credential repository on the corresponding operation under "Network administration > Device credential repository" for the device and the device is then monitored with these settings. If this does not work, SINEC NMS tries to detect the device with the initial SNMP settings. You configure these in the parameter group "Initial credentials" of the control.

With SNMP versions 1 and 2c, only community strings for read and write access can be used to secure the communication. With SNMP V3, authentication via MD5 / SHA1 hashes and encrypted communication can also be used.

Note

SNMP settings for writing to devices

The SNMP settings for writing to devices can be configured in the control in the parameter group "Initial credentials" and in the operations under "Network administration > Device credential repository".

Note

Using SNMP V3

For security reasons, it is advisable to use SNMP settings in which SNMP V3 is used. Select only secure passwords with a high password strength.

Note

Limit the number of SNMP profiles used

SNMP access is blocked by some devices after 10 failed authentication attempts. Therefore, if possible, use a limited number of SNMP profiles.

7.2.1.14 Syslog settings

SINEC NMS can operate as a Syslog client and send triggered system events, network events, system alarm messages, and audit trail events of the operation to a Syslog server. You can specify the address and port of this Syslog server in the "Syslog settings" parameter group. The system events are sent to the Syslog server in RFC 5424 format in English. If you want the operation to use the same Syslog settings as the control, select the "Use Syslog settings of Control administration" check box.

The appendix to the manual describes the general structure and the meaning of the Syslog messages.

7.2.1.15 Unmanaged devices

In the parameter group "Unmanaged devices" you can manage devices which cannot be monitored and which can be inserted into the topology display on the "Network monitoring > Topology" page of operations for completion. The devices available in the parameter group "Unmanaged devices" are available on the operations in editing mode of the topology page in the left side bar. Inserted unmanaged devices are also displayed in online mode.

7.3 Authorization management

Control

7.3.1 Components

The authorizations for monitoring and configuring devices and for using the system functions of SINEC NMS are configured in the control and automatically transferred to the operations. The following components are important for configuring authorizations:

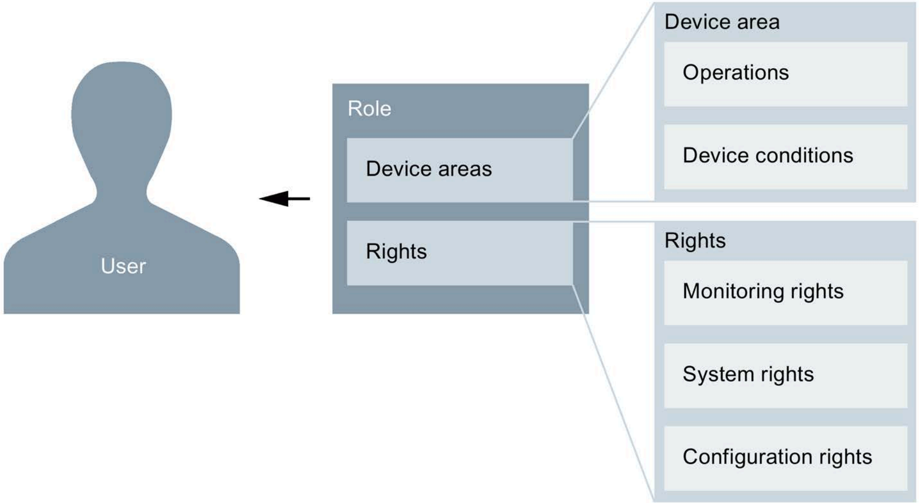


Figure 7-3 Authorization management components

One or more roles are assigned to each user. Each role consists of device areas and rights.

The settings of the displayed components are automatically synchronized between control and operations.

Users

Users can be centrally managed in User Management Component (UMC) and then used in SINEC NMS or configured locally in SINEC NMS, refer to section User (Page 275).

The "SuperAdmin" user with the "Super Admin" role is available by default after the installation of SINEC NMS. This role includes the device area "All devices" as well as all rights. The role and the device area cannot be deleted. At least one user with the "Super Admin" role must always be present and enabled.

Roles

A role uses included device areas and rights to specify what users can do and where they can do it. The device areas and rights that can be assigned to a role are determined by the position of the role in the role hierarchy, refer to section Roles (Page 276).

Device areas

Operations and optional device conditions are assigned to a device area. The assigned operations determine which devices are visible in this device area. The device conditions determine which devices of the assigned operations is configurable in the device area. Configured device conditions have no effect on the visibility of devices. If no device conditions are configured, all devices of the operations assigned to the device area are configurable. Device areas are configured on the "Device areas" page, refer to section Device areas (Page 274).

Rights

The rights of a role consist of monitoring rights, system rights and configuration rights.

The monitoring rights define which monitoring functions a user may use. Therefore, a user may be prohibited from using reports but, for example, allowed, to monitor based on the device list. The operations and devices that are visible to users when using the monitoring functions depend on the operations that are assigned to the device areas of their role.

System rights can be used to configure the authorizations for using the system functions of SINEC NMS. System functions include, for example, adding operations to the control and editing the user administration.

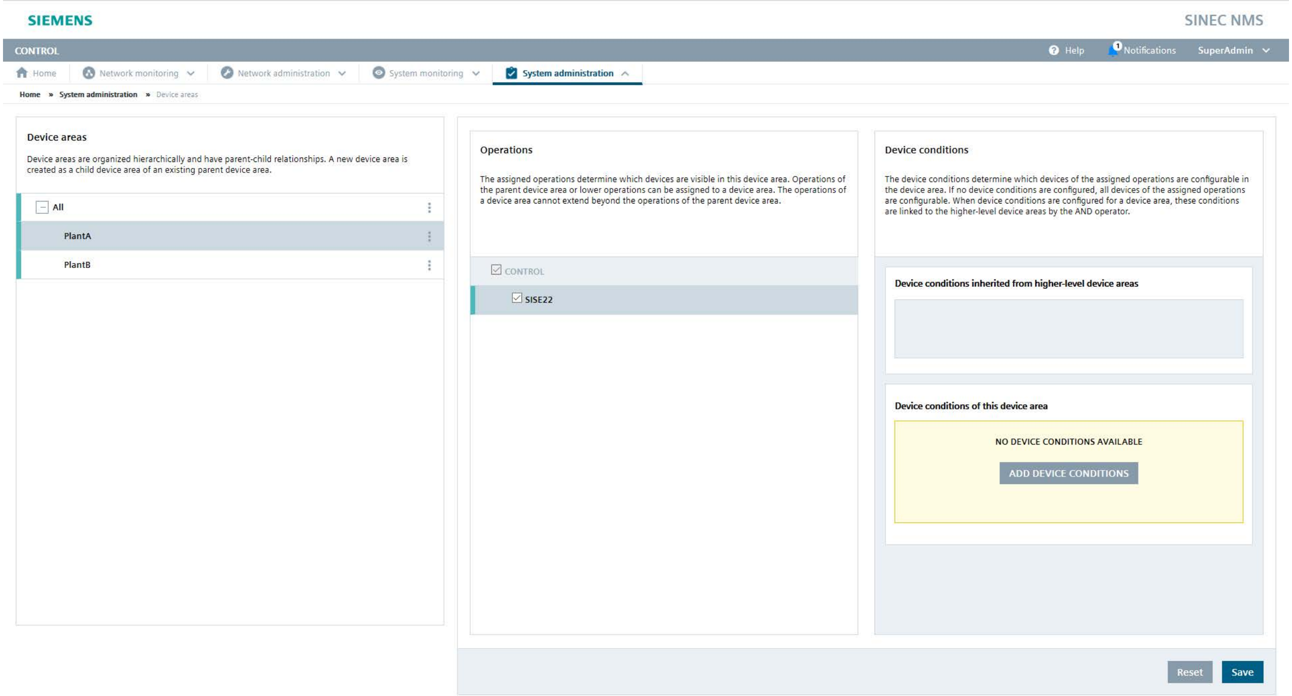
The configuration rights define which capabilities can be configured with policies and the Configuration Cockpit. The devices that are configurable for users depend on the device areas of their role.

Rights are assigned to roles on the "System administration > Role assignments" page, refer to section Role assignments (Page 277).

7.3.2 Device areas

Control

You reach this page in the navigation of the control under "System administration > Device areas".



Device areas

Device areas are organized hierarchically and have parent-child relationships. A new device area is created as a child device area of an existing parent device area.

Operations

The assigned operations determine which devices are visible in this device area. Operations of the parent device area or lower operations can be assigned to a device area. The operations of a device area cannot extend beyond the operations of the parent device area.

Device conditions

The device conditions determine which devices of the assigned operations are configurable in the device area. If no device conditions are configured, all devices of the assigned operations are configurable. When device conditions are configured for a device area, these conditions are linked to the higher-level device areas by the AND operator.

Device conditions inherited from higher-level device areas

Device conditions of this device area

Figure 7-4 Configuration of device areas

Under "System administration > Device areas", device areas can be created, deleted and the operations and device conditions of a device area can be defined.

Device areas are organized hierarchically and have parent-child relationships to each other. A new device area is created as a child device area of an existing parent device area.

The operations of the parent device area or fewer operations can be assigned to a device area. Only operations that have been added to the control and can be accessed by the control are available.

If device conditions are configured for a device area, these device conditions are linked to those of higher-level device areas by the AND operator.

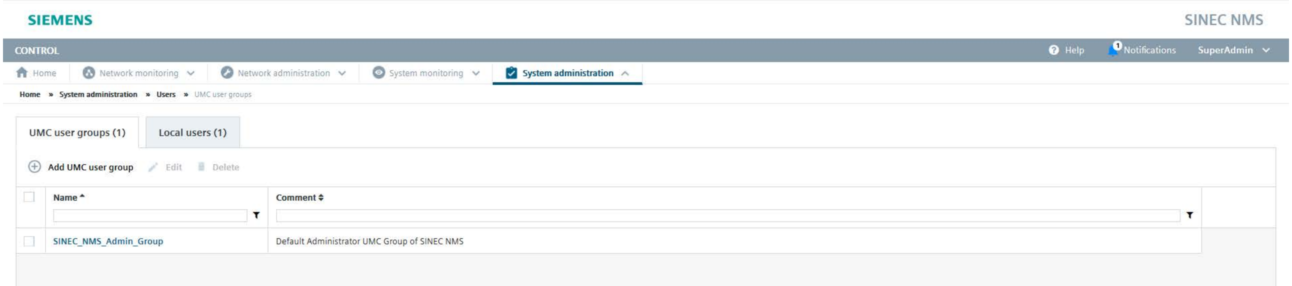
Device areas are assigned to roles on the "System administration > Role assignments" page, refer to section Role assignments (Page 277).

7.3.3 User

7.3.3.1 UMC user groups

Control

You reach this page in the navigation of the control under "System administration > Users", "UMC user groups" tab.



□	Name	Comment
□	SINEC_NMS_Admin_Group	Default Administrator UMC Group of SINEC NMS

Figure 7-5 Configuration of UMC user groups

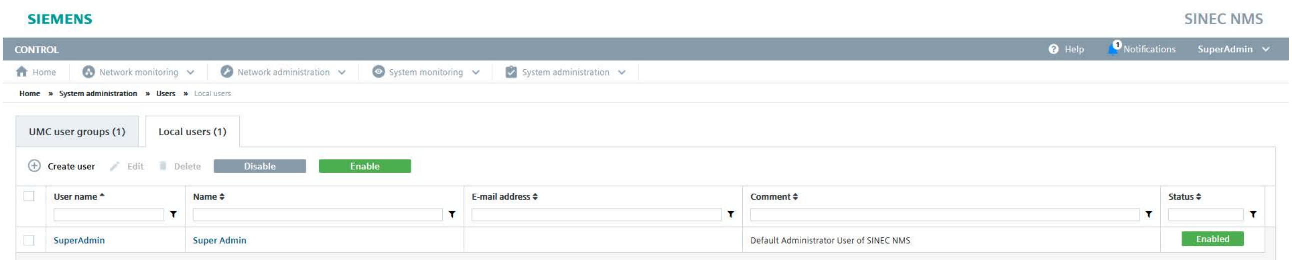
UMC (User Management Component) is a database for the central administration of user data. In SINEC NMS, the UMC users can be used after the UMC user groups have been included by specifying the UMC user group names. The editor under "System administration > Users > UMC user groups" can be used to integrate the UMC user groups. The names of the UMC user groups in SINEC NMS must match exactly the names of the UMC user groups in UMC.

UMC can be configured during the installation of SINEC NMS.

7.3.3.2 Local users

Control

You reach this page in the navigation of the control under "System administration > Users", "Local users" tab.



□	User name	Name	E-mail address	Comment	Status
□	SuperAdmin	Super Admin		Default Administrator User of SINEC NMS	Enabled

Figure 7-6 Configuration of local users

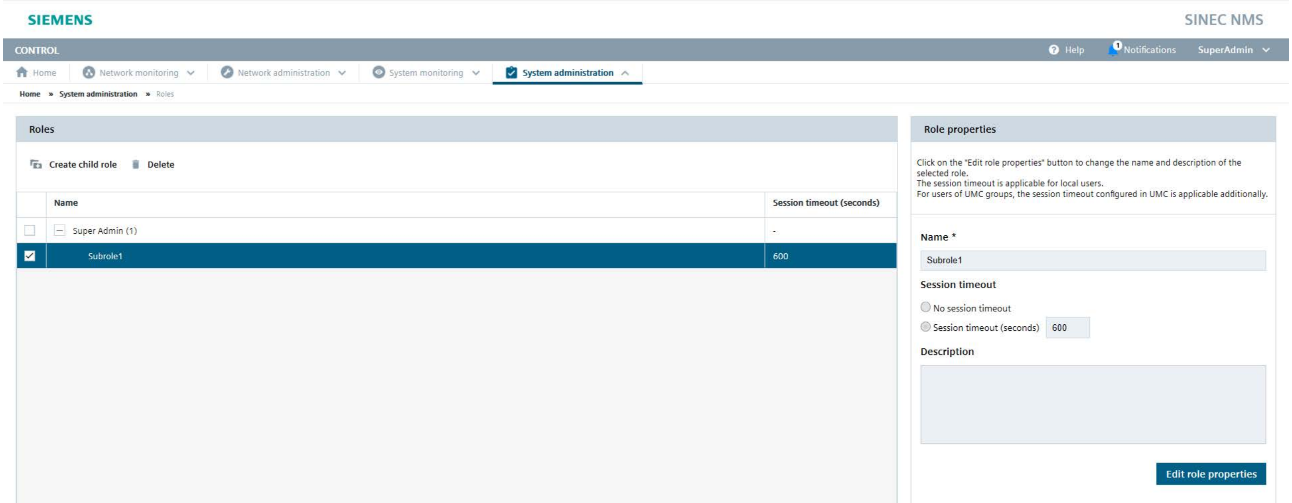
As an alternative to employing users from UMC, users can be configured under "System administration > Users > Local users". Users that are to be used must be enabled. At least one user with the "Super Admin" role must always be present and enabled.

Single-sign-on is not supported for local users. When switching between the Web interface of the control and the Web interface of an operation, you must log on again.

7.3.4 Roles

Control

You reach this page in the navigation of the control under "System administration > Roles".



	Name	Session timeout (seconds)
□	⊟ Super Admin (1)	-
☑	Subrole1	600

Click on the "Edit role properties" button to change the name and description of the selected role.
The session timeout is applicable for local users.
For users of UMC groups, the session timeout configured in UMC is applicable additionally.

Name *: Subrole1

Session timeout

○ No session timeout
○ Session timeout (seconds) 600

Description

Figure 7-7 Configuration of roles

On the "System administration > Roles" page, roles can be created and deleted, and the description as well as the session timeout of roles can be changed.

The session timeout of a role determines the number seconds of inactivity after which a user with this role is automatically logged out. A user with multiple roles does not have a session timeout if session timeout is configured for at least one of the user's roles. Otherwise, the role with the shortest duration determines the session timeout of the user.

Roles are organized hierarchically and have parent-child relationships to each other. A new role is created as a child role of an existing parent role. Users can only edit or delete roles that are subordinate to their own roles.

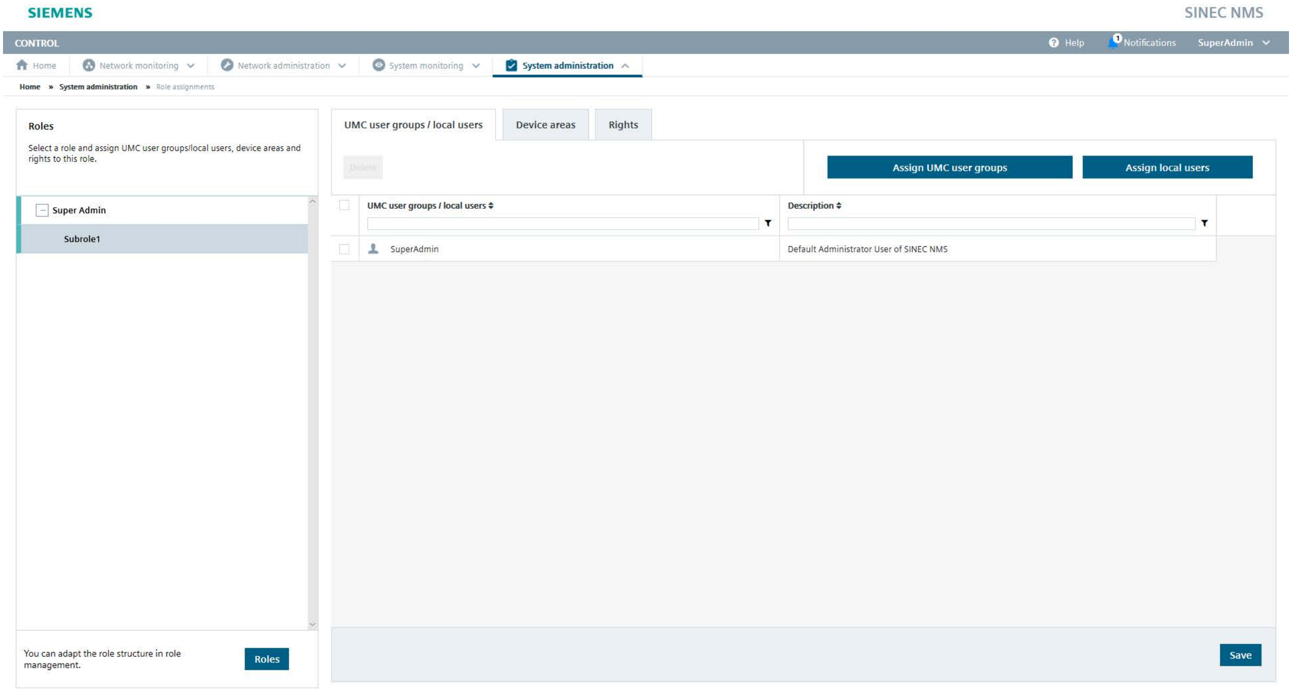
When a child role is created, it inherits the device areas, the operations and device conditions, and the rights of its parent role. The inherited properties can be restricted on the "System administration > Role assignments" page, but not extended beyond the properties of the parent role. For more information, refer to section Role assignments (Page 277).

At the top of the role hierarchy is the pre-defined role "Super Admin", to which the pre-defined "All" device area and all rights are assigned. This role has no session timeout and is assigned to the default user "SuperAdmin".

7.3.5 Role assignments

Control

You reach this page in the navigation of the control under "System administration > Role assignments".



Select a role and assign UMC user groups/local users, device areas and rights to this role.

UMC user groups / local users	Description
SuperAdmin	Default Administrator User of SINEC NMS

You can adapt the role structure in role management.

Figure 7-8 Role assignments

On the page "System administration > Role assignments", UMC user groups and users as well as device areas and rights can be assigned to the roles created in the role administration.

Users can only edit the assignment of roles that are subordinate to their own roles. The selected role is assigned all device areas or all parent role rights via the button "Inherit from parent role" in the "Device areas" and "Rights" tabs.

In the "UMC user groups / local users" tab, the desired UMC user groups and users are assigned to a role via the "Assign UMC user groups" or "Assign local users" buttons.

In the "Device areas" tab, the desired device areas are assigned to a role by selecting the corresponding check boxes. The device areas of the parent role or fewer device areas can be assigned to a role.

The authorizations for the use of functions are assigned to a role, e.g. to view or edit policies, in the "Rights" tab. In the "Device configuration" section, device services are selected which may be configured on devices. This determines which tasks can be selected for device configuration in policies and in the Configuration Cockpit when this role is used.

The rights of the parent role or fewer rights can be assigned to a role.

The role hierarchy is defined on the "System administration > Roles" page, refer to section Roles (Page 276).

7.4 Control administration

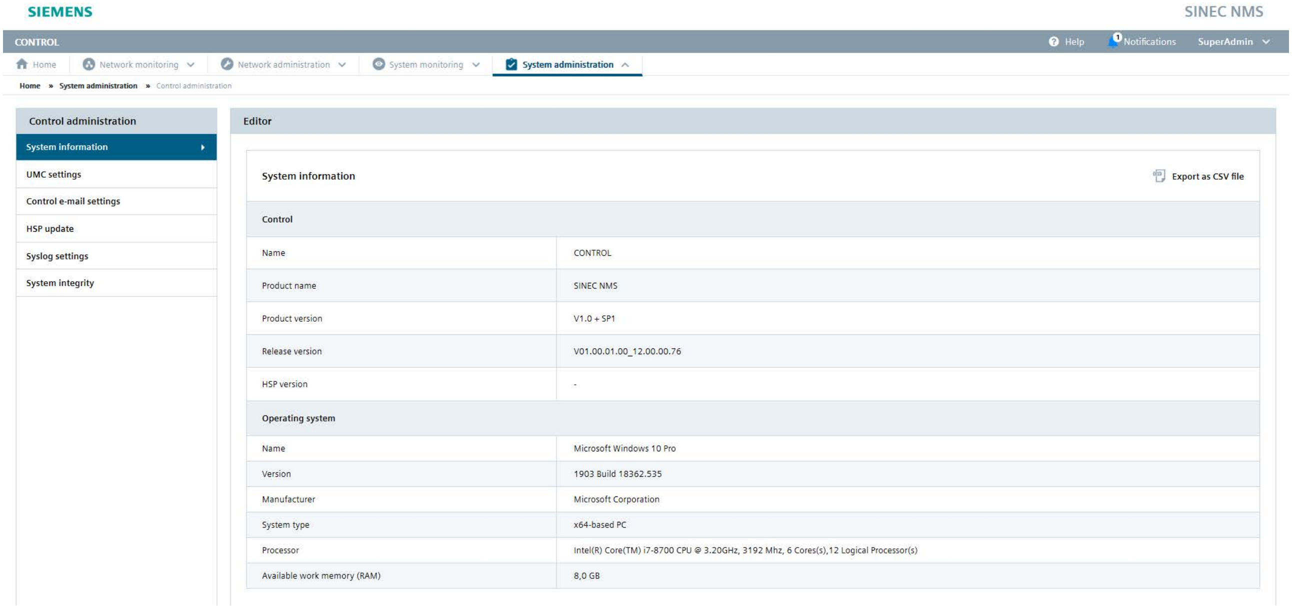
Control

The control administration is available under "System administration > Control administration". The control administration contains information about the installed SINEC NMS version and about the PC on which the control was installed. The control administration is also used for the configuration of UMC and e-mail settings as well as the installation of HSPs.

7.4.1 System information

Control

You reach this page in the navigation of the control under "System administration > Control administration > System information".



System information

Control	
Name	CONTROL
Product name	SINEC NMS
Product version	V1.0 + SP1
Release version	V01.00.01.00_12.00.00.76
HSP version	-
Operating system	
Name	Microsoft Windows 10 Pro
Version	1903 Build 18362.535
Manufacturer	Microsoft Corporation
System type	x64-based PC
Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz, 3192 Mhz, 6 Cores(s),12 Logical Processor(s)
Available work memory (RAM)	8,0 GB

Figure 7-9 Display of system information

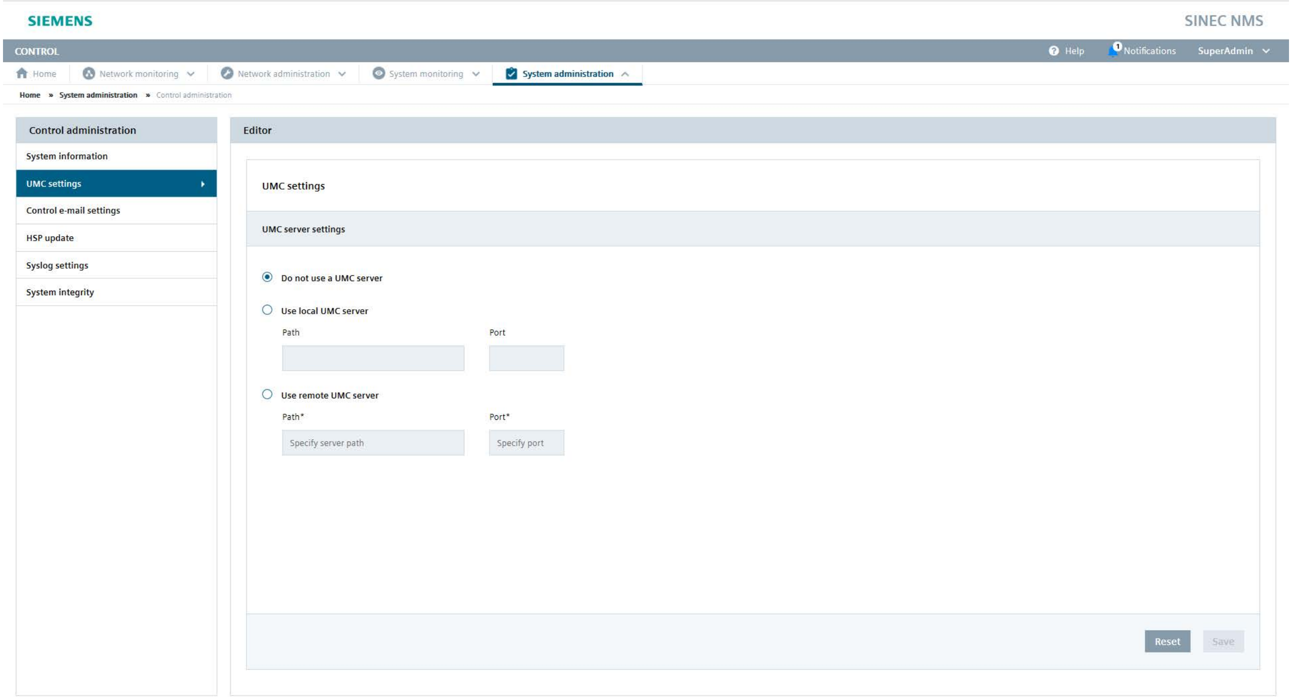
The page "System administration > Control administration > System information" contains information about the installed SINEC NMS version and about the PC on which the control was installed.

The displayed system information can be exported as CSV file using the button "Export as CSV file".

7.4.2 UMC settings

Control

You reach this page in the navigation of the control under "System administration > Control administration > UMC settings".



UMC settings

UMC server settings

● Do not use a UMC server

○ Use local UMC server

Path | Port

○ Use remote UMC server

Path* Specify server path | Port* Specify port

Figure 7-10 UMC settings

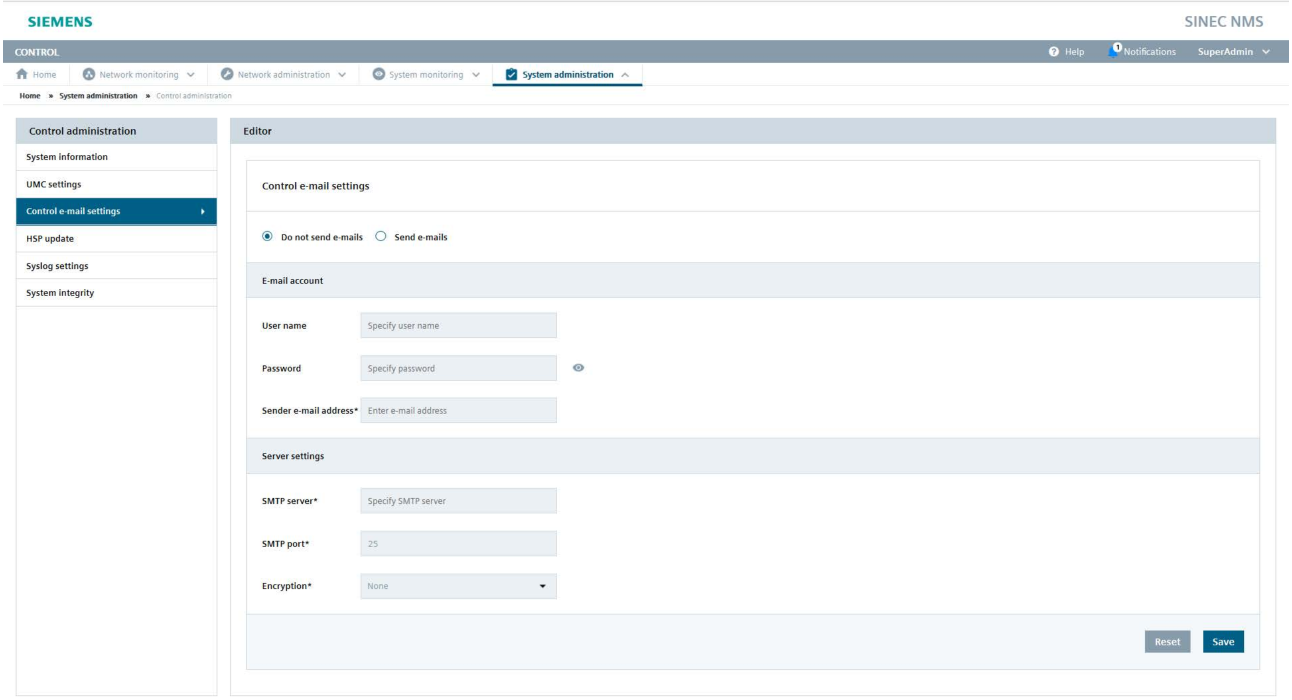
On the page "System administration > Control administration > UMC settings", you can specify whether SINEC NMS should be connected to UMC.

The connection to UMC makes it possible to manage user data centrally in UMC and to integrate this user data via UMC user groups in SINEC NMS. On the page "UMC settings" you can specify at which address and via which port SINEC NMS can reach UMC. By default, the page contains the settings that were configured for UMC during the installation of SINEC NMS. For information on integrating UMC user groups into SINEC NMS, refer to section UMC user groups (Page 275).

7.4.3 Control e-mail settings

Control

You reach this page in the navigation of the control under "System administration > Control administration > Control e-mail settings".



Control e-mail settings

● Do not send e-mails ○ Send e-mails

E-mail account

User name: Specify user name

Password: Specify password

Sender e-mail address*: Enter e-mail address

Server settings

SMTP server*: Specify SMTP server

SMTP port*: 25

Encryption*: None

Figure 7-11 Control e-mail settings

On the page "System administration > Control administration > Control e-mail settings", you configure the data of the e-mail account that SINEC NMS uses for sending the following e-mails:

- E-mails notifying users about the completion of reports. For information on creating reports, refer to section Reports (Page 123).
- E-mails to local users who have forgotten their password.

If communication with the e-mail server used is to be encrypted, the certificate of the e-mail server must be stored in the certificate manager of the control. You can use the supplied batch file with the following structure for the call. The command prompt for this call must be run by an administrator.

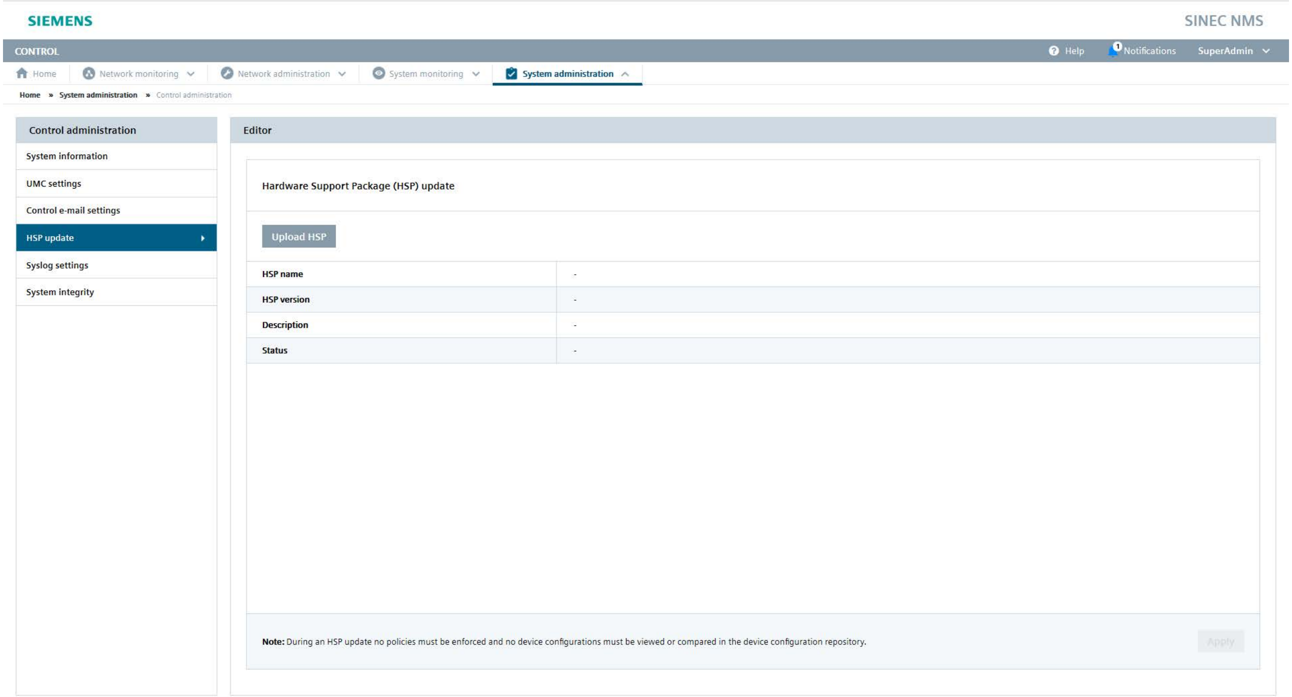
- %SINECNMS_HOME%\bin\importKey.bat <path to certificate> <aliasName>
- Example call: C:\Siemens\SINECNMS\SINECNMS\bin\importKey.bat C:\tmp\mycert.pem mymailcertificate

The data of the e-mail account that SINEC NMS uses for sending e-mails to inform about events that have occurred can be configured on the page "System administration > Operation parameter profiles" in the parameter group "E-mail settings" of the control, refer to section Operation parameter profiles (Page 249).

7.4.4 HSP update

Control

You reach this page in the navigation of the control under "System administration > Control administration > HSP update".



Hardware Support Package (HSP) update

HSP name	-
HSP version	-
Description	-
Status	-

Note: During an HSP update no policies must be enforced and no device configurations must be viewed or compared in the device configuration repository.

Figure 7-12 HSP update

7.4.4.1 HSP update

On the "System administration > Control administration > HSP update" page, you can install Hardware Support Packages (HSPs), extend the SINEC NMS with supported devices and unlock functions such as additional policy actions. You can obtain HSPs in zip format from Siemens Industry Online Support on request.

During the installation of HSPs, no policies may be enforced and no device configurations may be displayed or compared in the device configuration repository.

To install an HSP, proceed as follows:

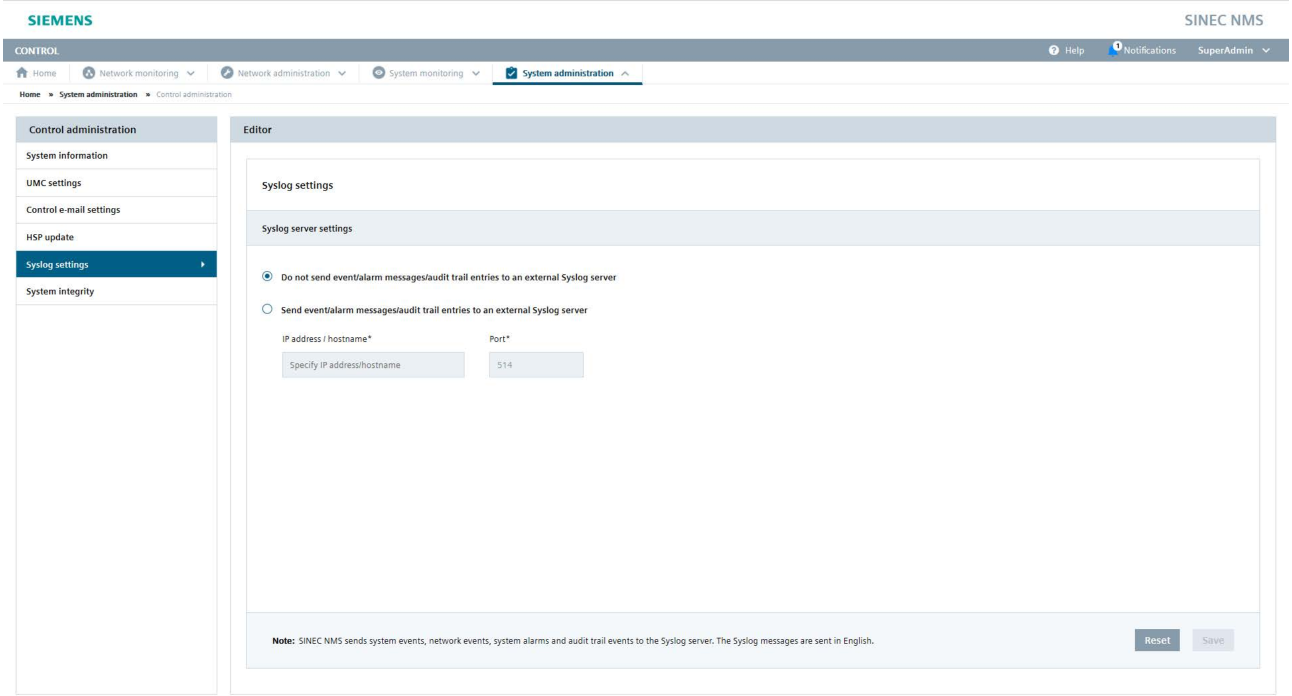
1. Click on the "Upload HSP" button and select the desired HSP file.
2. Once the HSP upload is complete, click the "Apply" button.

The HSP will now be installed on the control and on all connected operations.

7.4.5 Syslog settings

Control

You reach this page in the navigation of the control under "System administration > Control administration > Syslog settings".



Syslog settings

Syslog server settings

● Do not send event/alarm messages/audit trail entries to an external Syslog server

○ Send event/alarm messages/audit trail entries to an external Syslog server

IP address / hostname*: Specify IP address/hostname

Port*: 514

Note: SINEC NMS sends system events, network events, system alarms and audit trail events to the Syslog server. The Syslog messages are sent in English.

Figure 7-13 Syslog settings

SINEC NMS can operate as a Syslog client and send triggered system events, network events, system alarm messages and audit trail events from the control to a Syslog server. You can specify the address and port of this Syslog server on the "Syslog settings" page. The system events are sent to the Syslog server in RFC 5424 format in English.

The appendix to the manual describes the general structure and the meaning of the Syslog messages.

7.4.6 System integrity

Control

You reach this page in the navigation of the control under "System administration > Control administration > System integrity".

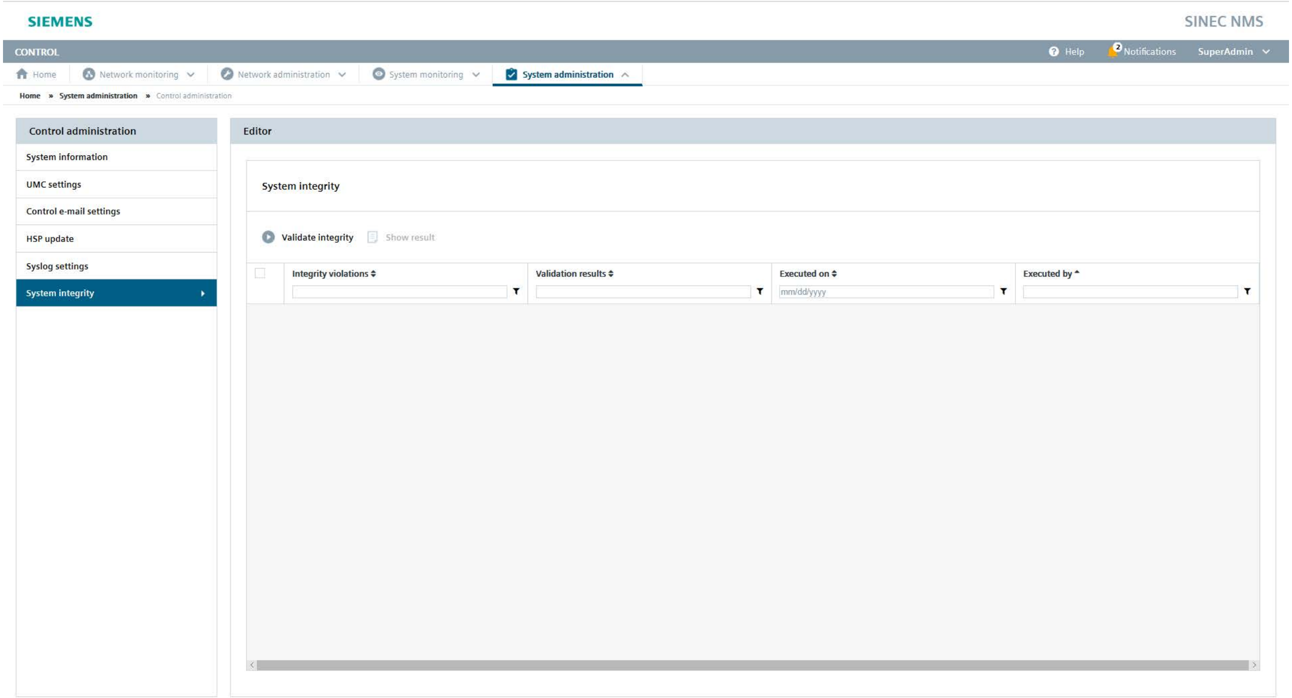


Figure 7-14 System integrity

You can verify the integrity of the control's system files on the "System administration > Control administration > System integrity" page. The result of an integrity check indicates whether system files have been modified without authorization. If this is the case, we recommend re-installing SINEC NMS to restore the original state of the system files.

7.5 Operation administration

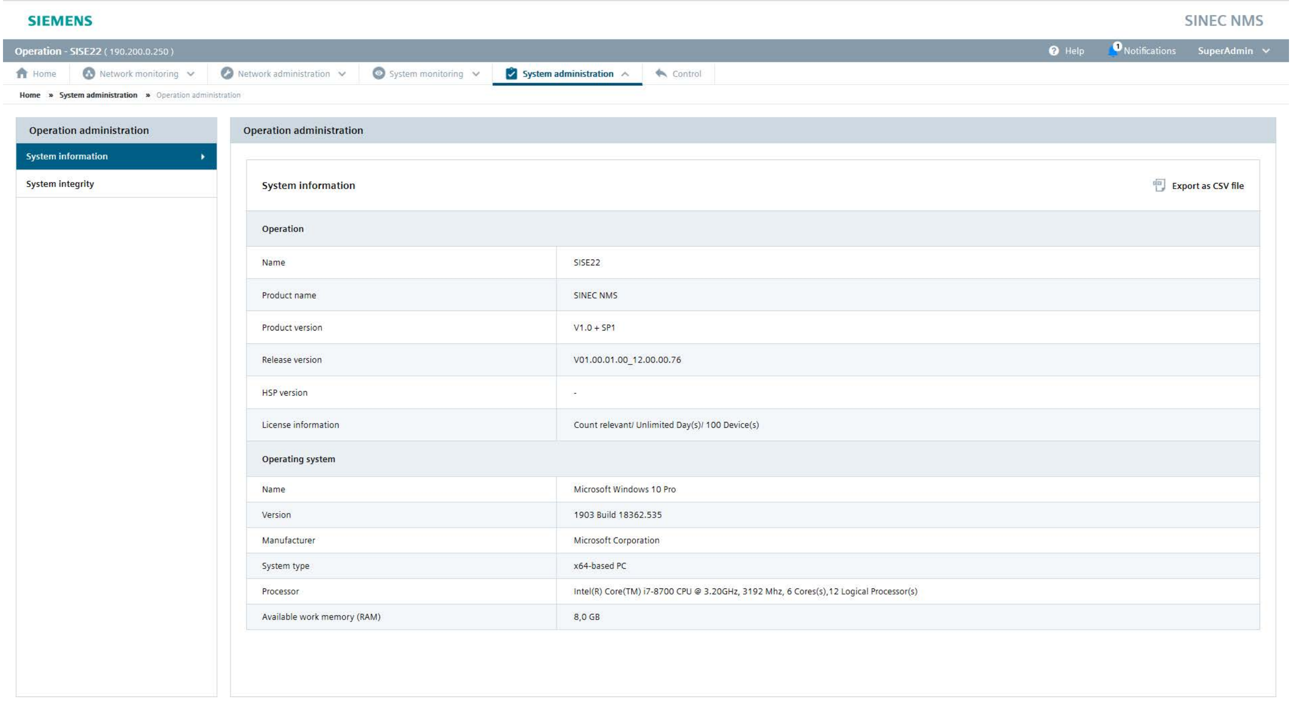
Operation

The operation administration is available under "System administration > Operation administration". Operation administration contains information about the respective operation and the PC on which the operation is installed. Operation administration is also used to check the integrity of system files of the operation.

7.5.1 System information

Operation

You reach this page in the navigation of operations under "System administration > Operation administration > System information".



System information

Operation	
Name	SISE22
Product name	SINEC NMS
Product version	V1.0 + SP1
Release version	V01.00.01.00_12.00.00.76
HSP version	-
License information	Count relevant/ Unlimited Day(s)/ 100 Device(s)
Operating system	
Name	Microsoft Windows 10 Pro
Version	1903 Build 18362.535
Manufacturer	Microsoft Corporation
System type	x64-based PC
Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz, 3192 Mhz, 6 Cores(s),12 Logical Processor(s)
Available work memory (RAM)	8,0 GB

Figure 7-15 Display of system information

The field for the operation name on the "System information" page indicates the computer name of the operation and contains information about the installed SINEC NMS version, as well as the license used for the operation. In addition, the page contains information on the operating system and the hardware configuration of the PC on which the operation is installed.

The displayed system information can be exported as CSV file using the button "Export as CSV file".

7.5.2 System integrity

Operation

You reach this page in the navigation of Operations under "System administration > Operation administration > Integrity check".

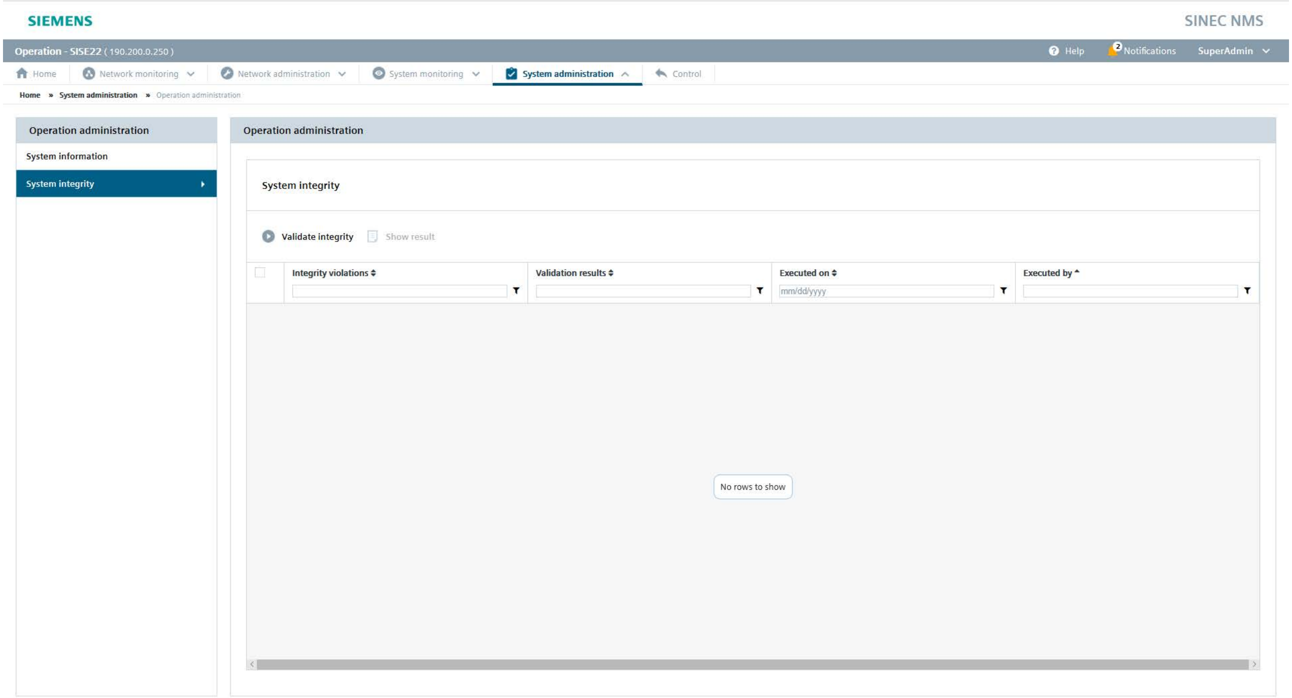


Figure 7-16 System integrity

You can verify the integrity of the operations' system files on the "System administration > Operation administration > System integrity" page. The result of an integrity check indicates whether system files have been modified without authorization.

Troubleshooting 8

The network scan is not performed after an operation is added.

If the check box "Start network scan after adding the operation" is selected on the "System administration > Operations" page before adding an operation, a network scan will be performed after the connection and synchronization between the control and the operation have been successfully established. If these steps bring no success, the operation can be reconnected to the control using the "Retry" button. If adding the operation was successful, the network scan will not be performed automatically and must be triggered manually for the operation via the "Start network scan" action.

Devices are monitored even though they are not in scan ranges

If existing scan ranges of an operation are changed or deleted, this has no effect on the devices monitored by the operation. Devices that are no longer within a scan range after changing or deleting a scan range will continue to be monitored by the operation. To disable monitoring for a device, use the "Delete selected devices" operator control on the "Network·monitoring > Devices" page of the associated operation, refer to section Device window with device list (Page 77).

It is not possible to save, display or restore a device configuration

In order to save, view, edit or restore the configuration of a device, the "SINEMA Configuration Interface" device property must be enabled on the respective devices. This property can be activated by the policy task "Set SINEMA Configuration Interface enabled".

The devices that are currently released for backing up and restoring device configurations can be found in the readme file of SINEC NMS.

OPC UA access to the data of an operation is not possible

Port 4841, which is used by default for OPC UA, is not automatically opened in Windows Firewall when an operation is installed. If you want to access the operation via OPC UA, enable this port in the firewall of the operation PC or configure another port to be used in the Operation Monitor, see section Operation Monitor (Page 37).

Policy enforcement or simulation contains no devices or the wrong devices

Check the following points:

- Check whether the capabilities required to perform the policy tasks have been discovered by SINEC NMS. If the device capabilities could not be discovered correctly, the device login data that SINEC NMS uses to read the devices may have to be checked, or the detection may have to be performed again.
- Check whether the devices have the "Managed" management status.

Policy fails

The present error type is displayed in the "Policy enforcements" tab of the Policy Control Center:

- Incorrect value: The value to be set is not supported by the device.
- Authentication failure: It is possible that "SNMP V1/V2 Read only" is activated on the device. Deactivate this read-only mode with a policy or use SNMP V3 for device access.

If your policy contains the "Set commit changes" task, drag-and-drop this task onto the end of the policy rule in the policy structure. You should generally pay attention to the logical sequence of tasks when configuring the policy rules.

Error message 503 "Service unavailable" appears when the Web interface is called

After starting the PC, the Web server may be accessible before the SINEC NMS components are ready for operation. In this case, wait until the SINEC NMS components are ready for operation.

Historical data is no longer available

Historical data is automatically deleted by control and operations after 3 months.

The enforcement of a policy, report or job has been skipped.

If a policy, report or job has a "Skipped" status, this may be caused by the following:

- There is a license problem on the associated operation.
- The time of execution is in the past.
- A previous enforcement of the same policy or execution of the same report or job is still running.

Device capabilities are not discovered after restoring a monitoring backup

After restoring a monitoring backup, manual synchronization of the operation with the control is required on the "System administration > Operations" page. If the capabilities of devices are not detected correctly afterwards, perform a manual discovery of the device capabilities on the page "Network Administration > Configuration Cockpit" of the respective operation.

Syslog messages A

A.1 Structure of the Syslog Messages

SINEMA NMS can forward events to a Syslog server. The events are transferred to the Syslog server in accordance with RFC 5424 or RFC 5426.

A Syslog message is composed of the following parameters:

Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message). The following values are used for audit trail events that are sent as Syslog messages: • Severity: Class of the event displayed in the "Class" column on the "System monitoring > Audit trail" page. • Facility: 13 (log audit)
VERSION	Version number of the Syslog specification.
TIMESTAMP	SINEC NMS sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as the local time including the time zone and correction for daylight saving / standard time if needed.
HOSTNAME	References the source computer with its name and the IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX "-" is output if information is missing.
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time. Example: [timeQuality tzKnown="0" isSynced="0"] The "tzKnown" parameter indicates whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter indicates whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
MSG	
MESSAGE	Message as ASCII string (English) For audit trail events that are sent as Syslog messages, the message is structured as follows. The values of the columns mentioned are displayed on the "System monitoring > Audit trail" page. Initiatedby: <value of the column "Initiated by"> fromIP: <value of the column "Initiated by IP address"> Message: <value of the column "Message"> Details: <value of the column "Details"> Item Path: <value of the column "Item path">

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs 5424 and 5426.

https://tools.ietf.org/html/rfc5424 (https://tools.ietf.org/html/rfc5424)

https://tools.ietf.org/html/rfc5426 (https://tools.ietf.org/html/rfc5426)

A.2 Tags in Syslog Messages

The "MESSAGE" parameter contains tags that are filled dynamically with the data of the respective event. These tags are displayed within curly brackets {variable} in the "Message text" field in section List of Syslog Messages (Page 293).

The following tags occur in the "MESSAGE" parameter of the Syslog messages:

Tag	Description	Format	Possible values or example
{IP address}	Source or destination IP address according to RFC1035 or RFC4291 section 2.2	%d.%d.%d.%d	192.168.1.105
{Dest mac}	Destination MAC address	%02x:%02x:%02x; %02x:%02x:%02x	00:0C:29:2F:09:B3
{Src mac}	Source MAC address	%02x:%02x:%02x; %02x:%02x:%02x	00:0C:29:2F:09:B3
{Src port}	Source port (0 to 65535)	%d	2345
{Dest port}	Destination port (0 to 65535)	%d	80
{Protocol}	Layer 4 protocol or service used that generated the event.	%s	Possible values: • WBM • UDP • TCP • Telnet • SSH • Console • PNIO • PB • OPC • WebSSO
{User name}	String without spaces that identifies the authenticated user by his or her name.	%s	SuperAdmin
{Group}	String without spaces that identifies the user group based on the user group's name.	%s	Operators
{Local interface}	Symbolic name of the local interface	%s	Console (login using Operation Monitor)

Tag	Description	Format	Possible values or example
{Destination user name}	String without spaces that identifies the destination user based on the user's name.	%s	Testuser
{Role}	Symbolic name of a role	%s	Administrator
{Time minute} {Timeout}	Number of minutes	%d	44
{Time second}	Number of seconds	%d	44
{Failed login count}	Number of failed login attempts	%d	10
{Max sessions}	Maximum number of sessions	%d	10
{vap}	Symbolic name of the virtual access point	%s	VAP1.1
{status} {reason}	Additional status information as a readable string that can contain multiple words. Must begin with "(" and end with ")".	(%s)	(Invalid group cipher) (Unknown peer)
{Wlan interface}	Symbolic name of the WLAN interface	%s	WLAN1
{ssid}	SSID in ASCII representation; any number of spaces.	%s	MyWLAN
{ssid_Hex}	SSID in Hex representation	%02x%02x%02x %02x%02x	050E081234
{Channel}	Name of the channel	%d	12
{Signal strength}	Signal strength	%d	12
{Version}	Name of the version without spaces	%s	V1.0.3SP1
{Resource}	Resource name protected by the protection level concept without spaces.	%s	FullReadAccess
{Trigger condition}	String without spaces for a trigger condition with which the respective function is activated.	%s	E/A-Pin FB-88
{Trigger pin}	String without spaces for an IO pin that triggered the event.	%s	DI1
{Firewall rule}	String with or without spaces for a set of firewall rules.	%s	Rule1
{Subject}	String with or without spaces for subject in the certificate. Used as part of the certificate-based authentication and must include Unicode characters.	(%s) or (%s %s) etc. With UTF8 code: (%S), (%S %S)	
{Config detail}	String with or without spaces for the designation of a configuration.	%s	OpenVPN
{Url}	String without spaces for identification of the that is requested on the Web server.	%s	https://webserver:8443/page1/subpage2?postdata
Patch information	String without spaces that identifies the patch version.	%s	HSPV1.0
Source	String without spaces for designating the source of change details.	%s	Possible values: • Control • Operation

Tag	Description	Format	Possible values or example
Component	String without spaces for designating the affected components of change details.	(%s) or (%s %s) etc.	Possible values: • OperationMgmt • PolicyMgmt • DiscoveryMgmt • PurgeMgmt • JobMgmt • ReportMgmt • HSPMgmt • LicenseMgmt • SystemIntegrity • FirewallMgmt • CredentialMgmt • Monitoring
MessageDetail	String with or without spaces for a message from SINEC NMS.	(%s) or (%s %s) etc.	
EventDetails	String with or without spaces for the description of an event.	%s	Example 1: 7.587 Example 2: 10.10.2.127:X1 P1-10.10.2.125:X1 P1 Example 3: C:\Siemens\SINECNMS_MON \DiscoveryLog\
IPaffected	IP address of the device that triggered the event.	%d.%d.%d.%d	192.168.1.105
IPreporting	IP address of the device that reported the information to trigger the event to SINEMA NMS.	%d.%d.%d.%d	192.168.1.105
IPaffectedExternal	IP address of the NAT router for the device that triggered the event.	%d.%d.%d.%d	192.168.1.105
IPreportingExternal	IP address of the NAT router for the device that reported the information to trigger the event to the SINEC NMS.	%d.%d.%d.%d	192.168.1.105
Interface	String with or without spaces for the name of the interface or the slot on the device.	%s	Example 1: R1 Example 2: X1 P4
Hsp information	Name of the HSP.	%s	HSP name

A.3 List of Syslog Messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

Identification and authentication of human users

Message text	{Protocol}: User {User name} logged in from {IP address}.
Example	WBM: User SuperAdmin logged in from 192.168.1.105.
Explanation	A user has successfully logged in.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} failed to login from {IP address}.
Example	WBM: User SuperAdmin failed to login from 192.168.1.105.
Explanation	The login of a user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} logged out from {IP address}.
Example	WBM: User SuperAdmin logged out from 192.168.1.105.
Explanation	A user has logged out successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: Default user {User name} logged in from {IP address}.
Example	WBM: Default user SuperAdmin logged in from 192.168.1.105.
Explanation	A default user has successfully logged in.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

User account management

Message text	{Protocol}: User {User name} has changed the password.
Example	WBM: User Tester has changed the password.
Explanation	A user has changed the user's own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has changed the password of user {Destination user name}.
Example	WBM: User SuperAdmin has changed the password of user Tester.
Explanation	A user has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has requested One-Time-Password.
Example	WBM: User Tester has requested One-Time-Password.
Explanation	A user has requested a one-time password for his user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} disabled user-account {Destination user name}.
Example	WBM: User SuperAdmin disabled user-account Tester.
Explanation	An authenticated user has disabled the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} enabled user-account {Destination user name}.
Example	WBM: User SuperAdmin enabled user-account Tester.
Explanation	An authenticated user has enabled the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} created user-account {Destination user name}.
Example	WBM: User SuperAdmin created user-account Tester.
Explanation	A user has created a user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} changed user-account {Destination user name}.
Example	WBM: User SuperAdmin changed user-account Tester.
Explanation	A user has changed an existing user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} deleted user-account {Destination user name}.
Example	WBM: User SuperAdmin deleted user-account Tester.
Explanation	A user has deleted an existing user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Management of the identifiers

Message text	{Protocol}: User {User name} created role {Role}.
Example	WBM: User SuperAdmin created role Testers.
Explanation	A user has created a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 1.4

Message text	{Protocol}: User {User name} deleted role {Role}.
Example	WBM: User SuperAdmin deleted role Testers.
Explanation	A user has deleted a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 1.4

Message text	{Protocol}: User {User name} assigned user {Destination user name} to role {Role}.
Example	WBM: User SuperAdmin assigned user Tester to role Testers.
Explanation	A user has assigned another user to a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 1.4

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login sessions exceeded.
Example	WBM: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of simultaneous sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Protection of check information

Message text	{Protocol}: User {User name} has deleted the monitoring event logging buffer.
Example	WBM: User SuperAdmin has deleted the monitoring event logging buffer.
Explanation	The user or system has deleted the event log memory.

Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

Message text	{Protocol}: User {User name} has deleted the monitoring report logging buffer.
Example	WBM: User SuperAdmin has deleted the monitoring report logging buffer.
Explanation	The user or system has deleted the report log memory.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

Message text	{Protocol}: Exported the monitoring report logging buffer and deleted.
Example	WBM: Exported the monitoring report logging buffer and deleted.
Explanation	The user or system exported and deleted the report log memory.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

Message text	{Protocol}: Deleted the monitoring report logging buffer of deleted devices.
Example	WBM: Deleted the monitoring report logging buffer of deleted devices.
Explanation	The user or system deleted the report log memory of deleted devices.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

Software and information integrity

Message text	Software integrity verification failed.
Example	Software integrity verification failed.
Explanation	The software integrity check has detected an integrity error.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

System resources

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	A critical resource problem has occurred in the system. No user action is required.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	A resource problem has occurred in the system. No user action is required.
Severity	Warning

Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	A resource anomaly has occurred in the system.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	Normal utilization of system resources.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	Critical state of the system resources. User action is required.
Severity	Critical
Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Message text	Source: {Source} Resource: {Component} detected {MessageDetail}.
Explanation	Alarm status of the system resources. A user action is required immediately.
Severity	Alert
Facility	local0
Standard	IEC 62443-3-3: SR 7.2

Index