

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.

Preface

Purpose of this documentation

This manual will help you install, configure and operate the application, SINEMA Server. It contains basic information about devices, protocols, security mechanisms and other properties of industrial networks and provides guidance and advice on monitoring and evaluating them.

Validity of the manual

The information in this document applies to the software, SINEMA Server V12.0.

New in this edition of the manual

Compared with edition 01, this manual edition includes the following modifications:

- Structure of the manual:

To improve the clarity of the manual, it was divided into 2 main sections:

- Part 1 - Description of the concepts and procedures: Chapters 1 to 3
- Part 2 - Reference section for the program functions: Chapters 4 to 5 and appendix with "Questions and answers" and the Index

- The content of the manual:

Enhanced functions and additions in SINEMA Server compared with product version V11 were added. The essential features of this innovation in V12 are as follows:

- New innovative Web user interface
- Server overview with the overview status of other SINEMA Servers in the network
- Monitoring and display of the connection status between device groups
- Evaluation and graphic display of VLANs
- Graphic trend display for statistical data (utilization, availability, WLAN, errors etc.)
- Support of device diagnostics of third-party devices using adaptable device profiles
- Reading out and monitoring of user-specific OIDs (SNMP variables)
- Adaptation of alarm messages, alarm texts, SNMP traps, threshold values and status displays
- Central configuration of SNMP values on the devices SysContact/SysLocation and SINEMA Server as trap recipients
- Improved HMI integration: Direct access to contents using URL links
- Support of STP / RSTP, MRP
- Optimized export and printing of lists and topologies
- SINEMA Server can be operated at the same time as STEP 7 on one PC
- SINEMA Server can be operated at the same time as WinCC on one PC (64-bit Windows)
- New license for monitoring up to 500 Ethernet devices + upgrade license from V11 to V12
- User interface languages Chinese and French (other languages on request)
- 64-bit Windows 2008 Server + 64-bit Windows 7 and new service packs

Further information

You will find additional and updated information about SINEMA Server on the Internet. The Siemens Automation Customer Support Web site contains manuals, FAQs and software updates among other content. You can access this information via the following link:

SINEMA server (<http://support.automation.siemens.com/WW/news/en/35228013>)

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product. The acceptance of the disclaimers of liability and warranty it contains is a clear precondition of the use of open source software.

You will find the license conditions on the same data medium as this manual under the following file name:

DOC_OSS-S7-CM-CP_74.pdf

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection

The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)

Training, Service & Support

You will find information on Training, Service & Support in the multi-language document "DC_support_99.pdf" on the data medium supplied with the documentation.

Security messages

Note

Siemens offers IT security mechanisms for its automation and drive product portfolio in order to support the safe operation of the plant/machine. Our products are also continuously developed further with regard to IT security. We therefore recommend that you regularly check for updates of our products and that you only use the latest versions. You will find information in:

(<http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en>)

Here, you can register for a product-specific newsletter.

For the safe operation of a plant/machine, however, it is also necessary to integrate the automation components into an overall IT security concept for the entire plant/machine, which corresponds to the state-of-the-art IT technology. You will find information on this in:

(<http://www.siemens.com/industrialsecurity>)

Products from other manufacturers that are being used must also be taken into account.

Table of contents

	Preface	3
1	Network management with SINEMA Server - the concept.....	11
1.1	SINEMA Server and Web client - components for powerful network monitoring	11
1.2	Interaction of the most important functions in SINEMA Server	14
1.3	Setting up and initializing SINEMA Server.....	17
1.4	Monitoring the network with SINEMA Server.....	19
1.5	Performance characteristics of SINEMA Server.....	20
2	Installing, setting up and calling the SINEMA Server program.....	23
2.1	Installing and uninstalling software	23
2.1.1	License information.....	23
2.1.2	Installing SINEMA Server - requirements and procedure.....	26
2.1.3	Uninstalling SINEMA Server.....	29
2.2	Configuring and starting SINEMA Server	30
2.2.1	SINEMA Server Monitor.....	30
2.2.2	Configuration of the system settings.....	32
2.2.3	Start SINEMA Server	35
2.3	Archive management.....	38
2.4	Data backup and restore.....	40
2.5	Migrating a SINEMA Server V11 configuration to V12	41
2.6	Web user interface.....	43
2.6.1	Logging in to the Web interface of SINEMA Server.....	43
2.6.2	SINEMA Server user interface on the Web interface	46
3	Using SINEMA Server - the most important functions	51
3.1	Detecting devices in the network	51
3.1.1	Overview	51
3.1.2	Scanning in the network.....	51
3.2	Visualizing the network topology / monitoring network devices.....	54
3.2.1	Topology - Overview	54
3.2.2	Topology discovery	57
3.2.3	Setting up monitored topology with the reference topology.....	58
3.3	Setting up network devices individually - using the Profile editor.....	60
3.3.1	Profile concept	60
3.3.2	Setting up profiles and assigning device types.....	62
3.4	Configuring event reactions - displaying events	65
3.4.1	Events	65
3.4.2	Event list.....	68
3.4.3	Filter events.....	71

3.5	Setting up and using views	73
3.5.1	Setting up views	73
3.5.2	The View editor	76
3.5.3	Creating a view-specific topology	77
3.5.4	Configure connections	82
3.6	Users and user groups	85
3.6.1	SINEMA Server users and roles concept	85
3.6.2	Setting up users and user groups	88
4	Program functions - reference section	89
4.1	Program user interface in detail - overview of the menus.....	89
4.1.1	User interface	89
4.1.2	Quick links	94
4.1.3	Calling functions with a URL	95
4.1.4	Start window.....	99
4.1.5	Device tree	100
4.1.6	Device window	102
4.1.7	Device details.....	105
4.1.8	Device details - subcategories	110
4.1.8.1	Detailed information LAN ports	110
4.1.8.2	Detailed information WLAN.....	111
4.1.8.3	Detailed information redundant ports	113
4.1.9	Views.....	115
4.1.9.1	Views . topology	116
4.2	Topology.....	119
4.2.1	Topology - Discovered	119
4.2.1.1	Meaning and how it works.....	119
4.2.1.2	Icons and colors in the discovered topology	122
4.2.2	Topology - Monitored	126
4.2.2.1	Meaning and how it works.....	126
4.2.2.2	Icons and colors in the monitored topology	128
4.2.3	Topology - Reference.....	132
4.2.3.1	Meaning and how it works.....	132
4.2.3.2	Reference editor / how it works and modes.....	135
4.2.3.3	Reference editor / including devices	138
4.2.3.4	Reference editor / configuring connections.....	139
4.2.3.5	Reference editor - additional configuration options	142
4.2.3.6	Icons and colors in the reference topology	144
4.2.4	Topology - special features	147
4.2.5	Topology - general forms of representation	149
4.2.5.1	Topology - Device hierarchy	149
4.2.5.2	Topology - Bird's eye view	149
4.3	Reports.....	150
4.3.1	Reports - Availability	152
4.3.2	Reports - Performance.....	154
4.3.3	Reports - Inventory.....	155
4.3.4	Reports - Events	156
4.3.5	Historical data and trend charts	156
4.3.5.1	Historical data	157
4.3.5.2	Trend charts	158

4.4	Administration	161
4.4.1	Administration - Discovery / Scan	162
4.4.2	Administration - Discovery / Profiles	165
4.4.2.1	The Profile editor	166
4.4.3	Administration - Network	173
4.4.3.1	Administration - Network Time settings	173
4.4.3.2	Administration - Network SNMP	174
4.4.3.3	Administration - Network Event reactions	174
4.4.3.4	Administration - Network Polling groups	178
4.4.4	Administration - "Unmanaged" device types	181
4.4.5	Administration - Event types	183
4.4.6	Administration - OPC	187
4.4.7	Administration - User	189
4.4.7.1	Administration - User User	189
4.4.7.2	Administration - User Groups	192
4.4.7.3	Administration - User Change password	193
4.4.8	Administration - User interface	194
4.4.9	Administration - System information	194
4.4.10	Administration - System config	195
4.5	Server overview	197
5	Data exchange via OPC	199
5.1	Access via OPC server - options and concept	199
5.2	Data access with OPC (UA)	200
5.3	Data access with OPC (DA)	203
5.3.1	Configuring DCOM settings in SINEMA Server	203
5.3.2	Configuring DCOM settings for the OPC server	207
5.3.3	Accessing SINEMA Server data via an OPC server (DA)	210
A	Questions and answers	213
A.1	Topic general operator control / installation	214
A.2	Topic logging in / starting	215
A.3	Topic topology	216
A.4	Topic network monitoring / scanning / SNMP	217
A.5	Topic views	218
A.6	Topic events	219
A.7	Topic migration / import / export	220
A.8	Topic reports	221
A.9	Topic Profile editor	222
A.10	Topic administration	224
A.11	Topic Web browser	225
	Glossary	227
	Index	229

Network management with SINEMA Server - the concept

1

1.1 SINEMA Server and Web client - components for powerful network monitoring

Network monitoring with SINEMA Server

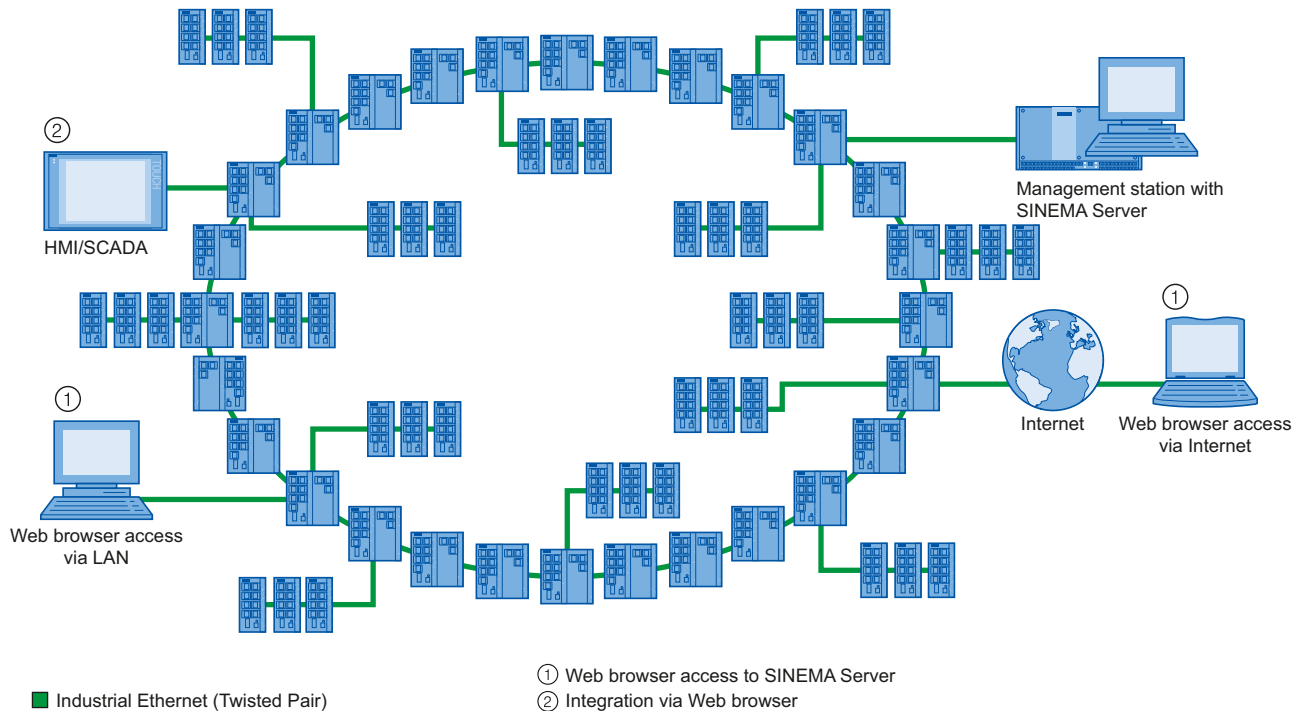
SINEMA Server is network management software. In the network, SINEMA Server monitors devices such as:

- the programmable controllers and wireless devices connected to LANs or WLANs
- the infrastructure components such as Industrial Ethernet switches or access points of industrial WLANs

With the "Autodiscovery" function of SINEMA Server, not only the controllers and infrastructure components but also their parameters are automatically detected if they are relevant for the network. Based on this information, the software then calculates the network topology and statistics.

SINEMA Server, Web client and network

A SINEMA Server application appears as follows with the Web access and the monitored network:



- Management station with SINEMA Server - "server function"

In its function as server, SINEMA Server includes configurable network management software. This is used to monitor and manage devices and their status in Industrial Ethernet/PROFINET networks.

The computer on which the SINEMA Server application runs is known as the management station.

SINEMA Server polls the status information of the Ethernet nodes during operation cyclically and reports network alarms. Changes in the network, errors and availability data are logged and archived in a database. You can call up this information.

Using the report functions that you can set to specific periods, you can document and analyze the network.

- Web user interface - access to the server functionality

SINEMA Server is accessed via the Web user interface on the Web client and in the management station:

- You configure the activities of SINEMA Server using administrative functions. You can take into account the different requirements of users by setting up user rights and specific views.
- You display the network information in the Web interface of SINEMA Server. When necessary, you can call up more detailed information with additional diagnostics displays.

- OPC server - additional interface for applications

For OPC applications, you have an additional interface available to the SINEMA Server network data. HMI systems such as SIMATIC WinCC also use this option for access to network data.

Supported devices - additional flexibility with the Profile editor

SINEMA Server can use private SNMP MIBs of Siemens devices to monitor more parameters than a generic SNMP tool. SINEMA Server also uses the DCP protocol to discover devices more quickly and to monitor devices that do not support the SNMP protocol.

SINEMA Server provides basic support for Siemens devices and devices of other vendors that support the following properties:

- Protocols such as ICMP, SNMP V1, SNMP V2C, SNMP V3, DCP, ARP etc.
- MIBs such as MIB2, LLDP and Bridge MIB.

SINEMA Server provides support for standard SNMP traps.

With the functions of the Profile editor, SINEMA Server provides a flexible instrument allowing detailed coverage of the widest range of devices in network monitoring.

As default, SINEMA Server provides full support for the following Siemens devices without any further configuration:

- The entire product spectrum of SCALANCE W, SCALANCE X and SCALANCE S
- SIMATIC NET CPs 200/300/400
- SIMATIC NET Links
- SIMATIC CPUs 300/400
- ET 200 S PN-IO
- SIMATIC PCs
- OSM and ESM switches

This list of supported devices is by no means complete. The devices listed here only represent examples of the supported devices. You should also remember that the range of support can vary considerably depending on the device. As an example, devices discovered by DCP such as SCALANCE S and other PROFINET devices are displayed only with details such as name, type, IP address and MAC address. Devices conforming with SNMP; on the other hand, provide additional information.

1.2 Interaction of the most important functions in SINEMA Server

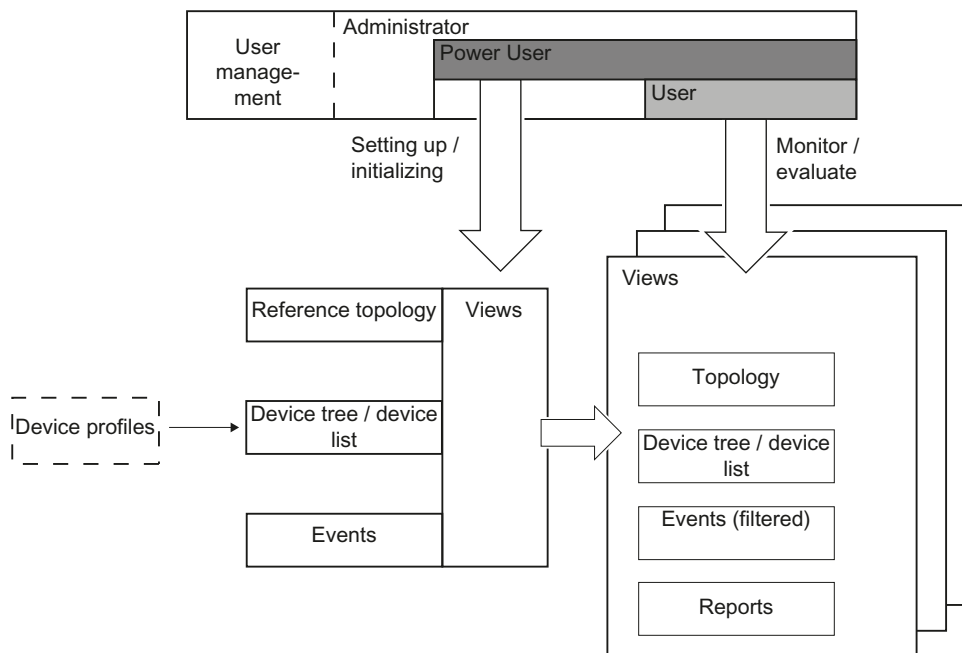
Program objects in SINEMA Server

The following diagram shows you the program objects that interact in SINEMA Server. Depending on the assigned user role in user management, you access these program objects on the Web user interface.

The following diagram also shows that the activities from your perspective as the user are essentially divided up according as follows:

- Setting up and initializing SINEMA Server
- Monitoring the network and evaluating results

The program objects shown in the diagram are described after the diagram.



Meaning and properties

- User management

The user management controls the access options for user groups. As default, the following user groups are set up:

- Administrator

Has full access to all program objects, is responsible for user management.

- Power user

Has full access to all program objects except for user management. Has unrestricted rights for network monitoring.

- User

Runs network monitoring with the assigned rights and views.

During configuration, you assign specific views to the user groups.

You can create new users and user groups oriented on the roles of users who are responsible for different network management activities. According to these roles, you can also define different views of the Web interface in SINEMA Server and assign these to different users and user groups.

- Device tree and device list

The device tree is the central navigation area for network monitoring with SINEMA Server. It is used to select higher-level views or views grouped according to certain criteria. The device list contains a table with all the devices discovered in the network along with status information.

- Device profiles (discovery / monitoring)

SINEMA Server device profiles describe the characteristics of the monitored network devices that can be displayed and evaluated. SINEMA Server reads out device information using SNMP.

By comparing this to the rules stored in the device profiles, devices can be identified and assigned to a device profile. The instructions stored in the profile then apply to the monitoring and display of the device in SINEMA Server.

You can use predefined device profiles or, when necessary, create additional profiles with the SINEMA Server Profile editor.

- Events /events list

Events are status changes in the network or system that need to be detected and require a reaction. The type of detection and the type of reaction to events can be configured in SINEMA Server.

A reaction, for example, can be to call applications that eliminate the cause of event. A further option is to trigger a notification e-mail.

- Topology and reference topology

The topology is a graphic display that shows the network components and their connections.

- Meaning when setting up:

When setting up, a reference topology is created based on an initial scan.

- Meaning when monitoring:

When monitoring, the topology shows the statuses of the network devices and the connections as well as deviations compared with the reference topology.

- Views

To be able to concentrate network monitoring on specific network sections and specific user groups, various views can be configured.

Important characteristics:

- Views contain sections of network monitoring.

- Views are shown as device lists and optionally as topology displays that need to be set up separately.

- Events can be displayed user-specific.

- Reports

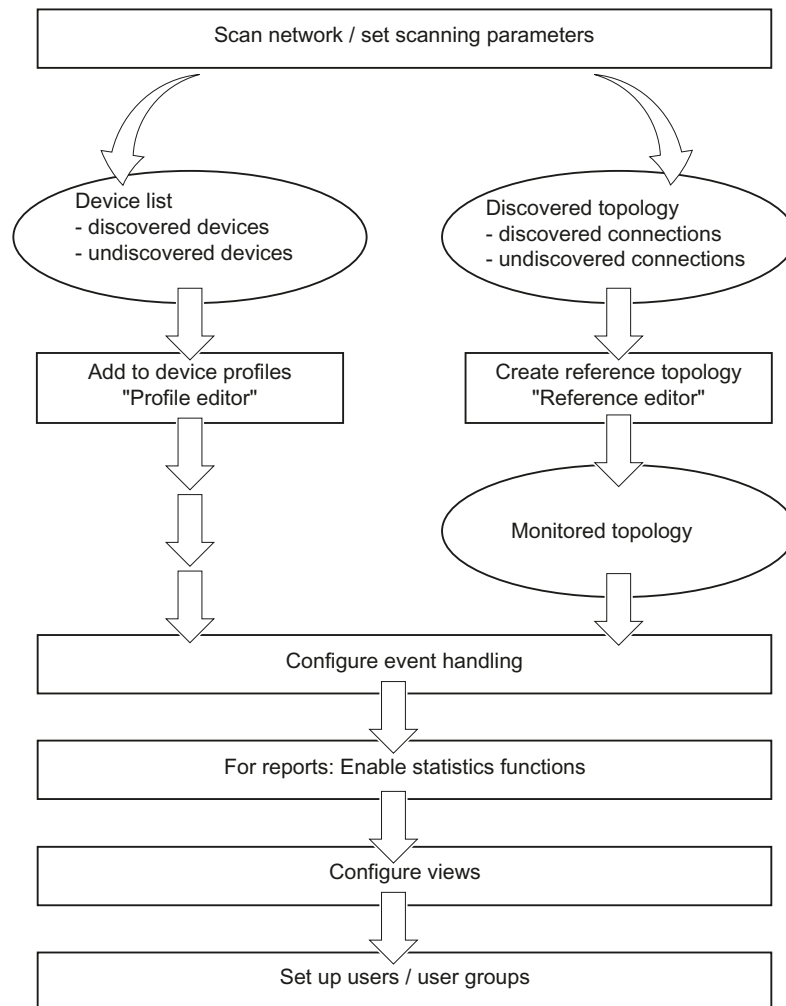
With the report function, you obtain exportable evaluations of the network monitoring in both textual and graphic form.

1.3 Setting up and initializing SINEMA Server

Action

When setting up and initializing, you basically work through the actions shown in the diagram below. The actions are described after the diagram.

Note: SINEMA Server software must be installed. Refer to the description in the section Installing, setting up and calling the SINEMA Server program (Page 23)



Description

- Action 1: Scan the network / set scanning parameters

To reduce the manual effort during setup as much as possible, first search the existing network for its components and their connections with SINEMA Server. As result, you obtain the device list and the "discovered topology".

Based on the result of this scan, you then have the following situation:

- Device list
Contains discovered devices
- Discovered topology
Contains discovered connections

- Action 2: Expand device profiles with the Profile editor

For the network devices that were not discovered or not completely, create profiles using the Profile editor to allow monitoring and display of these devices in SINEMA Server.

- Action 3: Create a reference topology with the Reference editor

Using the "Reference editor", expand undiscovered connections between network devices or those not clearly detected. This makes it possible for these to be displayed in the "monitored topology" and in specific topology displays in the "views"

- Action 4: Configuring event reactions

You specify which reactions there should be to events or status changes occurring in the network. You can specify the context to which the reaction should relate. You can choose between the views, device and system.

- Action 5: Configure reports

You enable statistics functions for the various report types.

- Action 6: Configure views

In the specific views, you specify a specific selection of devices you want to monitor in the device lists. If necessary, create suitable topology displays for the selected network sections.

- Action 7: Set up users / user groups

Based on the user groups and their roles that exist in SINEMA Server as default, set up the user management for your application. If necessary expand the default user groups by adding specific user groups.

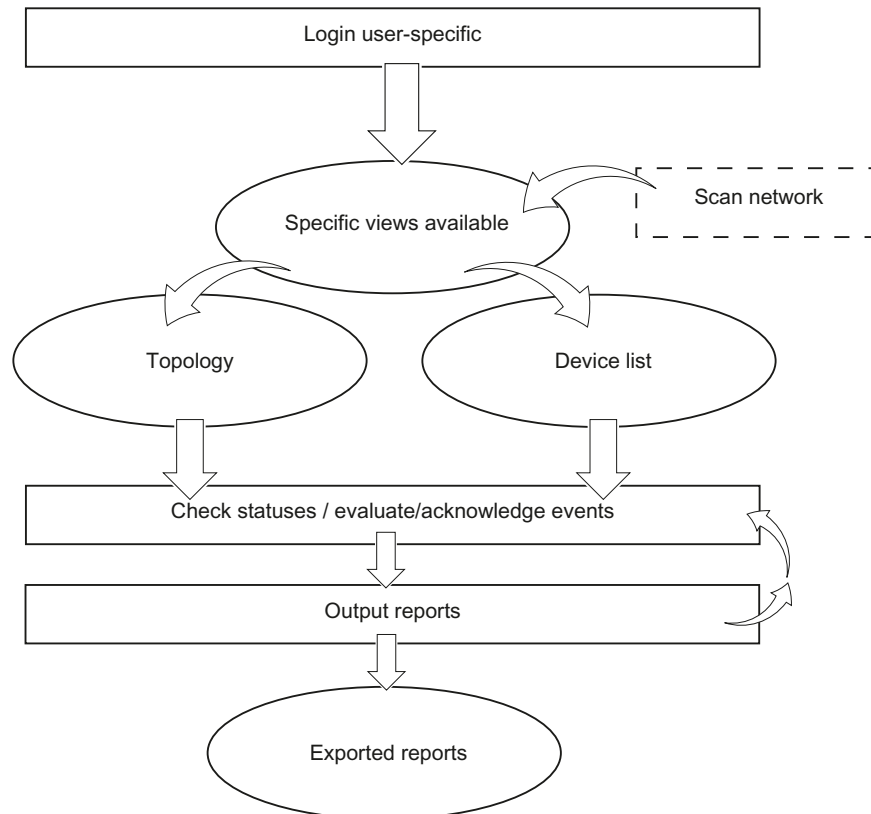
You assign views to the users.

This is the last action involved in setting up and initialization.

1.4 Monitoring the network with SINEMA Server

Monitoring the network

The following graphic shows an overview of the possible monitoring actions on the Web interface of SINEMA Server.



Description of the actions

- Action 1: User-specific login

You log in with SINEMA Server on the basis of the created users and user groups. Depending on your assignment, you have access to different views with the device lists and topology display.

The iterative actions involved in network monitoring then follow. The devices are monitored according to the polling characteristics set in SINEMA Server:

- Action 2: Check the status / evaluate and acknowledge events

User-specific events are triggered (e-mail,)

- Action 3: Output reports

Your network monitoring and network analysis is supported by the options for accessing different report types.

1.5 Performance characteristics of SINEMA Server

Supported operating systems

SINEMA Server supports the following operating systems:

- Windows XP Professional SP3 (32-bit)
- Windows 7 Ultimate Enterprise SP1 (32- / 64-bit)
- Windows 7 Professional SP1 (32- / 64-bit)
- Windows Server 2008 R2 (64-bit)

Supported Web browsers - Web interface

SINEMA Server supports the following Web browsers:

- Internet Explorer version 8.0 or higher
- Firefox version 17.0 or higher

Several instances of the Web interface of SINEMA Server Web can be opened at the same time by different users to access network information.

Access to the SINEMA Server Web interface is possible using an unencrypted HTTP connection or an encrypted HTTPS connection. User authentication using a user name and password increases the security against unauthorized access.

Regardless of their location in the network, several users can access the same information at the same time.

Configuration limits

The number of monitored network devices is limited within the framework of the licensing levels. See section License information (Page 23).

A maximum of 500 network devices can be monitored.

For each management station, SINEMA Server V12 supports remote access by ten users simultaneously. This means that an installation of SINEMA Server can be used by up to ten users at the same time for remote monitoring of network operation.

Further features

In addition to the descriptions in the previous sections, SINEMA Server also provides the following additional functions:

- Forwarding of network data and alarms to other systems using an e-mail client function and an OPC server.
- Users with access to SINEMA Server can also use the OPC server to display device data acquired by SINEMA Server.

- The export function allows the project and configuration data of SINEMA Server to be archived. Similarly, the configuration data can also be imported into SINEMA Server.
- Capability of integration in HMI systems (HMI - Human Machine Interface) and visualization systems such as SIMATIC WinCC. This makes the monitoring of communication possible in a process visualization system.

Installing, setting up and calling the SINEMA Server program

2

2.1 Installing and uninstalling software

2.1.1 License information

To use this application, you require a SINEMA Server license.

Trial license

The application ships with a standard trial license. The SINEMA Server application automatically generates a trial license. The trial license can be extended by upgrading to a new license type.

License types with limits to suit the user's needs

The following six license types are available for SINEMA Server:

- License type 500: This license supports up to 500 monitored devices
- License type 250: This license supports up to 250 monitored devices.
- License type 100: This license supports up to 100 monitored devices.
- License type 50: This license supports up to 50 monitored devices.
- Emergency: This license supports up to 500 monitored devices.

If a license type is damaged or corrupted, an emergency license can be used. The emergency license provides validity for a further 14 days.

- Trial 50: This license is a trial license and supports up to 50 monitored devices.

Note

The maximum number of monitored devices shown for the license types listed above does not include the management stations.

Note

The "Trial 50" license of SINEMA Server V12 is only valid for 21 days. Once the trial version has been activated on the computer it cannot be activated again. The trial license contains all the functions available with the other license types with support for 50 devices.

Note

If you launch SINEMA Server the first time without a valid license key, the application setup automatically installs and activates this trial license on your computer.

Automation License Manager

To manage your SINEMA Server license, you can use the Automation License Manager (ALM) program. This program is used to manage the license keys. Software products that require license keys automatically indicate this requirement to the Automation License Manager. If the ALM finds a valid license key for the software, this can be used according to the end user license agreement.

After installing SINEMA Server, you can call up the documentation for the program. To do this, select **SIMATIC > Documentation** in the Windows Start menu.

Storage location for license keys

You can store license keys on storage devices such as license key sticks, exchangeable drives (however not on CD, CD RW) or on USB sticks. License keys can be found locally on your own computer.

License upgrade

To extend the license or to expand to a higher number of monitored devices, you require an upgrade to a new license. To allow the license upgrade to be made, the Automation License Manager requires access to the license key of the upgrade license.

License types 50/100/250/500 can be combined. The license type is expanded according to the addition. However, only a maximum of 500 devices can ever be monitored.

Note

The current version of SINEMA Server supports a maximum of 500 devices.

To upgrade using a license key, follow the steps outlined below:

1. In the Automation License Manager, select the **"View > Management"** menu command.
2. In the navigation area, select the storage location of the license key with which you want to perform the upgrade.
3. In the object area, select the license key with which the upgrade will be performed.
4. Select the **"License key > Upgrade"** menu commands.

License downgrade

A license downgrade is possible if you have at least one license type available. For the downgrade, you do, however, require a license type higher than Basic 50. If, for example, you have license type 50 + license type 50 (two licenses) it is only possible to downgrade to one license type.

NOTICE
Checking the number of monitored devices Before performing the license downgrade, make sure that the number of monitored devices does not exceed the number of monitored devices that will be licensed following the downgrade. Otherwise, a login will no longer be possible following the license downgrade.

To perform a downgrade with a license type, follow the steps outlined below:

1. Stop SINEMA Server and its services. To do this, you can use the "SINEMA Server Monitor" window.
2. In the Automation License Manager, select the "**View > Management**" menu command.
3. In the navigation area, select the storage location of the license key with which you want to perform the downgrade.
4. Select the "License key > Transfer" menu command to transfer the license key to another user.

NOTICE
Checks on completion of the license downgrade Following the downgrade, there must still be at least one license type remaining in the navigation area.

2.1.2 Installing SINEMA Server - requirements and procedure

Overview

To install SINEMA Server, you do not require any special system knowledge. Most of the installation is handled automatically. The SETUP routine itself recognizes whether other programs apart from SINEMA Server need to be installed. The installation routine takes the required actions as necessary.

Successful installation and proper operation of SINEMA Server requires the following system properties:

Hardware requirements

Parameter	Minimum requirements	Recommended requirements
Processor	Intel Dual Core CPU 2.4 GHz	Intel Quad Core CPU 2.66 GHz
RAM	2 GB	4 GB
Network adapter	1 Note: SINEMA Server requires a network adapter that must not be shared by other applications.	1 Note: SINEMA Server supports up to four network adapters.
Storage requirements hard disk	<ul style="list-style-type: none">approx. 4.5 GB (with a 32-bit operating system)approx. 8.5 GB (with a 64-bit operating system)	

Software requirements

Supported operating systems	<ul style="list-style-type: none">Windows XP Professional SP3 (32-bit)Windows 7 Ultimate Enterprise SP1 (32- / 64-bit)Windows 7 Professional SP1 (32- / 64-bit)Windows Server 2008 R2 (64-bit)
Web browser	<ul style="list-style-type: none">Internet Explorer 8.0 or higherFirefox 17.0 or higher
Java Runtime Environment (JRE)	Version 1.6.0.32 (32-/64-bit) or higher Note: the Java Runtime Environment (JRE) software is made available by SINEMA Server during setup.

Note

Java VM (JVM) and Java Runtime Environment (JRE) must be installed to allow the Web interface pages of SINEMA Server that contain Java applets to be displayed. This software is made available by SINEMA Server during the installation. On clients connected to the host device, however, JRE version 1.6.0.32 or higher must be installed. This is required for the correct display of the applets.

Requirements for the Web client

For users that access SINEMA Server from client systems, the client computer must meet the following requirements:

Web browser	<ul style="list-style-type: none">• Internet Explorer 8.0 or higher• Firefox 17.0 or higher
Java Runtime Environment (JRE)	Version 1.6.0.32 (32-/64-bit) or higher
Monitor resolution	1280 x 1024 pixels

Requirements for SIMATIC Microbox IPC427C

SINEMA Server also supports SIMATIC Microbox IPC427C. The system requirements for this are as follows:

Parameter	Minimum requirements
Processor	Intel Core2 Duo CPU U9300 with 1.20 GHz
RAM	2 GB
Operating system	Microsoft Windows XP Professional service pack 3

User rights

To be able to install SINEMA Server on your computer, you require administrator privileges.

Time required

The time required is estimated to be about 10 to 20 minutes, depending on the computer class and scope of installation.

Sequence

To install SINEMA Server on your computer, follow the steps below:

1. Log in to the Windows operating system as administrator. Open the Windows Explorer and double-click on the "Setup.exe" file in the root directory of the installation CD. As an alternative, start the program from the Windows menu **Start > Run**.

If the Auto Run function is enabled for your CD-ROM drive, the installation will start automatically.

2. Select the language for the Setup wizard of SINEMA Server and click "Next".
3. Click the "Open source license agreement" button to display the license agreement. After reading the license agreement, select the option "I accept the conditions of the above license agreement as well as the conditions of the Open Source license agreement"" and then click "Next".

4. Enter the required user information and click the "Next" button.

A dialog box opens containing the list of programs to be installed. Leave the preselection of the SINEMA Server components as it stands.

To be able to use SINEMA Server, you also require the Automation License Manager.

5. Select the check box for the Automation License Manager (ALM). If you require further information about the ALM, click the "Readme" button on the right of the dialog box.
6. Select the "Storage space" button to display the current storage space of the computer.
7. Click the "Browse" button if you want to change the standard target directory and install the application somewhere else.
8. Select the required storage location and click the "Next" button to start the installation.

Note

Memory requirements

If the drive does not have enough free storage space, click the "Browse" button to select a different location for the installation.

A new dialog box opens.

9. Follow the further instructions that guide you through the entire installation. This process can take several minutes.

When it is finished, a final window is displayed for the setup. This contains a status message about the successful installation of the SINEMA Server application.

10. In the setup window, you can either restart the computer immediately or later. Select the required option and click the "Finish" button to complete the installation.

2.1.3 Uninstalling SINEMA Server

Uninstalling

To uninstall SINEMA Server V12 Basic from your computer, follow the steps below:

1. Open the Windows Control Panel by clicking **Start > Control Panel** in the Windows taskbar.
2. In the Control Panel window, open the "Add or Remove Programs" dialog box
3. In the sub window of the "Add or Remove Programs" dialog box, click on "Change or Remove Programs".
4. In "Currently installed programs", select the entry "SINEMA Server V12 Basic".
5. Click the "Remove" button. When prompted to confirm removal, click "Yes". SINEMA Server is then uninstalled from your system.

Note

After uninstalling the program, you can retain the valid license key. To do this, open the Automation License Manager and save the license on a separate data medium. You can also, however, transfer the license to other users.

Note

When uninstalling, the installation program removes the program files and folders. If one of the folders to be uninstalled is still open in the Windows Explorer, an error message is displayed. To avoid this, make sure that the folder to be uninstalled is closed.

2.2 Configuring and starting SINEMA Server

The following section describes what needs to be done to set up and start SINEMA Server on the management station.

- Configuration

Before SINEMA Server is started for the first time, system settings need to be configured. Here, configuration means the setting of basic parameters that are required for the subsequent actions for network access.

- SINEMA Server Monitor

The SINEMA Server Monitor described below is the central access point for the configuration and starting SINEMA Server as well as for several other services.

2.2.1 SINEMA Server Monitor

Overview

The SINEMA Server Monitor is the central program module that calls basic SINEMA Server functions and some additional administrative programs. The SINEMA Server Monitor runs on the PC/PG on which SINEMA Server is installed (management station).

This program loads automatically after successful installation of SINEMA Server and on each subsequent Windows startup. In addition, the following icon for accessing the user interface is integrated in the taskbar.



Note: This icon may also be colored differently indicating different statuses of SINEMA Server. You will find the significance of the different colors in the section Start SINEMA Server (Page 35)

Layout

To open the SINEMA Server Monitor, right-click on the corresponding icon in the taskbar. Following this, the menu for calling up the following functions appears:

- Start Web client
- Start SINEMA Server - see section Start SINEMA Server (Page 35)
- Exit SINEMA Server
- Restore system backup - see section Data backup and restore (Page 40)
- Start system backup - see section Data backup and restore (Page 40)
- Configuration - see section Configuration of the system settings (Page 32)
- Archive management - see section Archive management (Page 38)

- Status
- Exit

Operation / content

The functions of the individual menu items are described in the following sections. Here, some additional information on a few of the functions:

- Start Web client

The default browser (Internet Explorer or Firefox) opens and displays the user interface of SINEMA Server.

- Start SINEMA Server

SINEMA Server is loaded. The progress of this process is shown by default in the status window. If this does not happen, you can open the Status window manually using the "Status" menu command.

- Exit SINEMA Server

SINEMA Server is closed. The progress of this process is shown by default in the status window. If this does not happen, you can open the Status window manually using the "Status" menu command.

- Archive management

Historical data for creating reports is deleted in the system database and optionally swapped out and imported again if necessary.

- Status

A window appears which shows the status of SINEMA Server (server is running, starting, shutting down, etc.). In addition, a progress bar shows the progress of the respective action.

- Exit

SINEMA Server Monitor is closed. You can start it again with the "Start > Programs > Siemens Automation > SINEMA Server > SINEMA Server".

Note

The value 0 (zero) as port address disables the corresponding service.

Due to data security, it may, for example, be necessary to prevent access to the system with HTTP. To do this, the service must be disabled. You achieve this by entering "0" as the HTTP port.

Requirements

To be able to use all the functions of SINEMA Server Monitor without restrictions, you should have administrator rights on the management station.

When using an operating system version Windows 7 or higher, you should assign the right "Run as administrator" to the SINEMA Server Monitor application. If you do not make this assignment, with certain functions the operating system will prompt you for confirmation that the function can be run. Confirm this prompt to allow the function to be used.

2.2.2 Configuration of the system settings

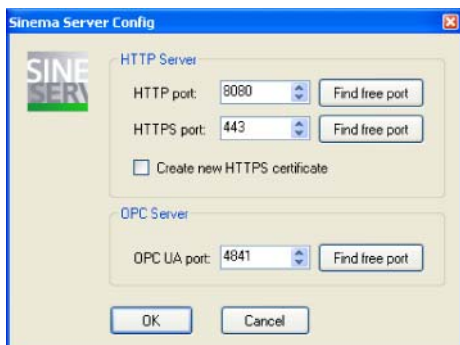
SINEMA Server Monitor - "Configuration" function

A window appears in which you can make the following communication parameter settings:

- Enter HTTP port for HTTP server / search for free HTTP port for HTTP server
- Enter HTTPS port for HTTP server / search for free HTTPS port for HTTP server
- Generate new HTTPS certificate
- Enter OPC UA port for OPC server / search for OPC UA port for OPC server

Configure normal port, protected port and OPC UA port

To be able to use the SINEMA Server application with a Web browser, the port settings for the use of the application in HTTP and HTTPS environments can be configured. The default port setting for HTTP is normally the use of port number 80 as the standard port. If you want to avoid using the default settings, change the setting using the commands in the shortcut menu of the "SINEMA Server Monitor" window.



Enter the HTTP port number and the HTTPS port number to reconfigure the HTTP server settings. Then click "OK". If the port number is already being used by a different computer, click "Find free port" to obtain a free port. With this option, a different available port number is selected automatically and the port number updated in the text box.

Note

HTTP port 80

If HTTP port 80 is being used by a different process, a warning is displayed in the status window that *HTTP port (80) is being used by different process*. This message is marked yellow. In this case, it is advisable to change the port using the "Find free port" option in the "SINEMA Server config" window.

To display a list of the processes that use port 80, you can enter the following command:
`netstat -noa | findstr :80`

The HTTP port can be disabled by setting the port to "0" in the "SINEMA Server config" window. To disable the HTTP port, enter "0" in the text box and confirm with "OK".

Reserved port numbers

SINEMA Server uses the following ports as default ports for communication. Remember, however, 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 SINEMA Server.

For this reason, make sure that these ports are available to SINEMA Server when starting up and operating the application. Below, you will find list of the default ports used by SINEMA Server:

To avoid this problem, it is advisable to note the ports used by SINEMA Server and to keep them free during network communication.

Default ports	Description	configurable	Note on the response if the port is blocked
25	SMTP	yes (Web user interface)	-
80	HTTP server / Java	yes (Windows taskbar)	-
161	SNMP	no	-
162	SNMP traps	no	SINEMA Server does not receive any traps.
443	HTTPS	yes (Windows taskbar)	-
4840	OPC UA server	yes (Windows taskbar)	-
4897	Data	no	SINEMA Server does not start.
4998	Events	no	SINEMA Server does not start.
4999	Monitor	no	SINEMA Server does not start.
5432	POSTGRESQL	no	Saving events / reports is not possible.

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

- PVSS00pmon.exe - TCP/UDP port
- PVSS00snmp.exe - TCP/UDP port

NOTICE

User-specific firewall

If a user-specific firewall is used, a system administrator needs to configure the firewall settings as shown above.

Generating HTTPS certificates

As further support for HTTPS connections, the setup of SINEMA Server also includes the generation of HTTPS certificates. As soon as this setup has been started on a computer, this certificate is generated automatically based on the IP address and the computer name. If the IP address or the computer name is changed, the certificate needs to be regenerated. To regenerate this certificate, click on the "Create new HTTPS certificate" check box.

The default port used for an OPC UA server is 4840. In the "SINEMA Server config" window, the default port can, however, be reconfigured. Enter the UA port in the configuration window and confirm the changes with "OK". Click "Find free port" to obtain the next free port if the existing port number is already being used. Apply the changes with "OK".

Using third-party certificates

You will find this certificate in the following folder:

Siemens\SINEMAServer\PVSS\Sinema_Server\config

- certificate.pem - self-signed certificate
- privkey.pem - private key for the certificate

To obtain a verified certificate, you need to send the self-signed certificate to VeriSign or another trustworthy organization to have it signed. This is necessary if you want to use the certificate later. As an alternative, you can also use a certificate that has already been signed.

In both cases, the newly generated certificate must be stored in the following folder:

- Siemens\SINEMAServer\PVSS\Sinema_Server\config

NOTICE
SSL certificate
The SSL certificate must be stored under the name "certificate.pem".

2.2.3 Start SINEMA Server

Automatic start

The following two situations must be distinguished:

- After installing SINEMA Server, SINEMA Server is started automatically after rebooting the management station.
- After restarting the management station, SINEMA Server is also automatically started.

You can recognize that SINEMA Server has started due to the following reaction:

- The "SINEMA Server status" window opens.
- The symbol for the SINEMA Server Monitor appears in the Windows taskbar.

Right-click on the SINEMA Server icon in the Windows taskbar to open the "SINEMA Server Monitor" window.

Note

Administrator rights required

If you work with the Windows 7 operating system, you need to run the program for starting SINEMA Server with administrator privileges.

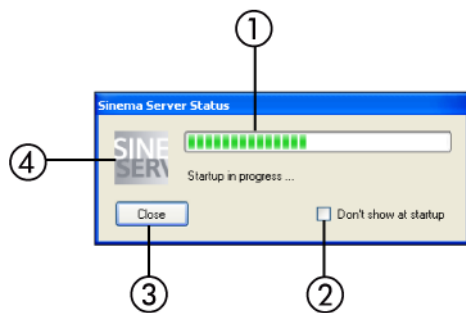
NOTICE
Do not change the date and time of the system After starting SINEMA Server, you must not change the date or time of the system. You must also not move the date into the past or the future. Changes of this type to the date or time of the system have other side-effects.

NOTICE
Avoid pauses or idle times on the management station Make sure that the management station does not change to the pause or idle status. This leads to unpredictable reactions relating to device status calculations and reachability. If such a situation does occur, the application needs to be restarted.

"SINEMA Server status" window

The "SINEMA Server Monitor" window supports you in monitoring the load status. The window includes options for starting and stopping the SINEMA Server application.

The "SINEMA Server Monitor" window is loaded as default and is part of the startup under Windows. This window starts the SINEMA Server application automatically without any user action. Initially, the dialog box is displayed with the status of the SINEMA Server on the Windows desktop. The window contains a progress bar that indicates the load status of the loaded application.



- ① Progress bar
- ② Startup - option for enabling/disabling
- ③ Button for closing
- ④ Icon for the status

To hide the "SINEMA Server status" window, click the "Close" button. The status window can be displayed again as follows:

1. Right-click on the icon in the system tray.
2. Select the "Status" command from the shortcut menu of the monitoring window.

The icon of "SINEMA Server Monitor" changes its color to green. This means that the SINEMA Server application was started successfully.

Note

Do not show the "SINEMA Server Monitor" window any more



If you do not want the "SINEMA Server Monitor" window to be displayed the next time you start Windows, select the "*Do not show at startup*" check box.



Status display in SINEMA Server Monitor

After starting the application, the icon for the SINEMA Server Monitor appears in the Windows taskbar.



Even if you close the dialog box of the "SINEMA Server status" window with the "Close window" button, the application continues to be executed in the background. The color of the icon indicates the operating status of the program.

Icon	Description
	SINEMA Server is starting
	SINEMA Server was started

Icon	Description
	SINEMA Server - error
	SINEMA Server - warning

NOTICE

Avoiding shutting down or restarting

Avoid a forced shutdown or a restart while SINEMA Server is in operation. In such situations, it is possible that the SINEMA Server database will be damaged. This means that the application no longer starts up correctly and the only remedy is to reinstall the application.

To avoid loss of data in such situations, it is advisable to back up the system regularly. The backup data can be called up when necessary using the restore function.

2.3 Archive management

Archive

Archives in SINEMA Server are data records containing historical data for creating reports. Exported data records can, when necessary, be read in again on the same management station from which they were exported.

Archive management - meaning

Historical data recorded over a long period that should remain accessible can be archived with the archive management included in SINEMA Server.

You access the functions of the archive management dialog in the management station using the SINEMA Server Monitor.

Functions

In the archive management dialog, the following options are available:

- Import archive

With this function, you can read in exported archives.

- Export archive and delete

Data records with the historical data of the specified period are exported to a ZIP file and then deleted in the database of SINEMA Server. You can calculate the storage space that will become free using the corresponding function in the archive management dialog before executing the function.

- Delete archive

Data records with the historical data of the specified period are deleted in the database of SINEMA Server. You can calculate the storage space that will become free using the corresponding function in the archive management dialog before executing the function.

- Cleaning up deleted devices in the archive

Data records with the historical data of deleted devices from the specified period are deleted in the database of SINEMA Server.

Note

Period

Historical data records can only be exported if they were recorded prior to the current month.

NOTICE
Editing the ZIP file - effects
You should not change the content of the exported ZIP file. Import is only possible using an unmodified ZIP file.

Calculating the storage space that will become free

The following functions are available in the archive management dialog:

- Calculate storage space for export

With this function, you calculate the storage space required for the ZIP file for the specified archive period.

- Calculate storage space gained

With this function, you calculate the storage space that will become free in the SINEMA Server archive.

2.4 Data backup and restore

You can access the backup functions using the "SINEMA Server Monitor".

Create system backup

All project data and program files are backed up.

You are prompted to enter the name for the backup file (<Filename>.zip). The backup then begins. If SINEMA Server has already been started, it is closed before the backup begins and restarted after the backup is completed.

- Function in "SINEMA Server Monitor": "Start system backup"

Restore system backup

The data of a previously created system backup (data backup) is read in.

To do this, you will be prompted to select the required system backup (<Filename>.zip). Following this, the system backup is started. If SINEMA Server was already started, SINEMA Server is exited before reading in the system backup and is restarted after restoring the system backup.

- Function in "SINEMA Server Monitor": "Restore system backup"

NOTICE
Restoring data from the system backup completely overwrites all existing data (project and program)!
Replacing the program data can mean the return to an older version of SINEMA Server. Version changes or program updates made in the meantime are lost and must be performed again if necessary.

2.5 Migrating a SINEMA Server V11 configuration to V12

Migration

If you install SINEMA Server V12 on a management station, on which version V11 is already installed, SINEMA Server V12 can adopt an existing database created in SINEMA Server V11. This means that you can transfer existing monitoring configurations to the powerful SINEMA Server V12 environment with little effort.

In principle, the sequence is as follows:

- The installation routine of SINEMA Server V12 detects the existing database.
- SINEMA Server proposes to adopt the database even before the actual installation starts.

Adopting data

During the migration as much existing data as possible is transferred. Due to the expanded concepts in SINEMA Server V12, it is not possible to take over all the data.

The following data records are transferred:

- Users and user groups
- Components of the system configuration with
 - Event reactions of the type "System"
 - E-mail settings
 - Discovery settings (scan settings, time settings)
- SNMP settings
- Port settings (HTTP port, HTTPS port, OPC UA port)
- HTTPS certificate

The following data records are not taken over

- Devices
- Event list
- Historical data
- "User maps"
- Reference topology
- Components of the system configuration with
 - Event reactions of the type "Device"

Sequence

Follow the installation instructions as described in the section Installing and uninstalling software (Page 23).

If the installation routine detects an existing V11 installation, you will be asked whether you want the data to be adopted.

If you confirm adoption of the data in SINEMA Server, additional information is then displayed. This information at the beginning of the installation relates to the export of the data from the V11 data management. On completion of the installation, you then receive information about importing the V11 data into the database of SINEMA Server V12.

2.6 Web user interface

2.6.1 Logging in to the Web interface of SINEMA Server

Using the Web browser or the options of SINEMA Server Monitor, you can log in to the Web interface of SINEMA Server as follows:

- On a client computer
You use a Web browser.
- On the management station
 - You use a Web browser specifying the address "localhost".or
 - You use the "Start Web client" function of SINEMA Server Monitor

Note

To allow pages of the SINEMA Server Web interface that contain Java applets to be displayed, Java Runtime Environment (JRE) version 1.6.0.32 must be installed on the client computers.

NOTICE
"Start Web client" function of SINEMA Server Monitor - default Web browser <p>When the Web client is called, the SINEMA Server Monitor uses the Web browser set as default in Windows. SINEMA Server supports the Web browsers listed in the section Performance characteristics of SINEMA Server (Page 20). It is advisable to make sure that one of these Web browsers is configured as the default browser.</p>

Logging in on a client computer

To log in to the Web interface of SINEMA Server, follow the steps below:

1. Open the Web browser.
2. Enter the IP address of the management station. In the address bar of the browser, enter **http://<IP address>** or **https://<IP address>** (if you are using a secure port).
If you use a standard port other than 80, enter the port number along with the IP address. A colon ":" must be entered between the IP address and the port number as the delimiter.
3. Enter the user name and the password in the displayed login dialog.
If authentication is successful, you will have access to the SINEMA Server Web interface.

Logging in on the management station

To log in to the Web interface of SINEMA Server on the management station, follow the steps below:

1. Open the Web browser.
2. In the address bar of the browser, enter **http://<localhost>** or **https://<localhost>** (if you are using a secure port).
3. Enter the user name and the password in the displayed login dialog.

If authentication is successful, you will have access to the SINEMA Server Web interface.

or

1. Select the "Start Web client" function in SINEMA Server Monitor.

Note

Recommendation: Use a secure port or HTTPS

When you log in to the Web interface of SINEMA Server, you should ideally use the HTTPS protocol.

NOTICE

Avoiding shutting down or restarting

Avoid a forced shutdown or a restart while SINEMA Server is in operation. In such situations, it is possible that the SINEMA Server database will be damaged. A damaged database means that the application no longer starts up correctly and the only remedy is to reinstall the application.

To avoid loss of data in such situations, it is advisable to back up the system regularly. The backup data can then be called up when necessary using the restore function.

User management - initial situation

As default, three predefined user groups are available in SINEMA Server. With these three predefined user groups, you can log in to the SINEMA Server application. You will find the default user name and the password in the following table:

User group	Login data
Administrator	<ul style="list-style-type: none">• User name: Administrator• Password: SinemaA
Power user	<ul style="list-style-type: none">• User name: Coordinator• Password: SinemaP
Standard user	<ul style="list-style-type: none">• User name: Operator• Password: SinemaS

When you first log in to the system, a dialog box is displayed with options for changing the password or retaining the password for the logged on user.

NOTICE
Recommendation - change the password Change the password after you have logged on with the application.

You will find further information about these predefined user groups, access rights and creating/managing users in the section Users and user groups (Page 85)

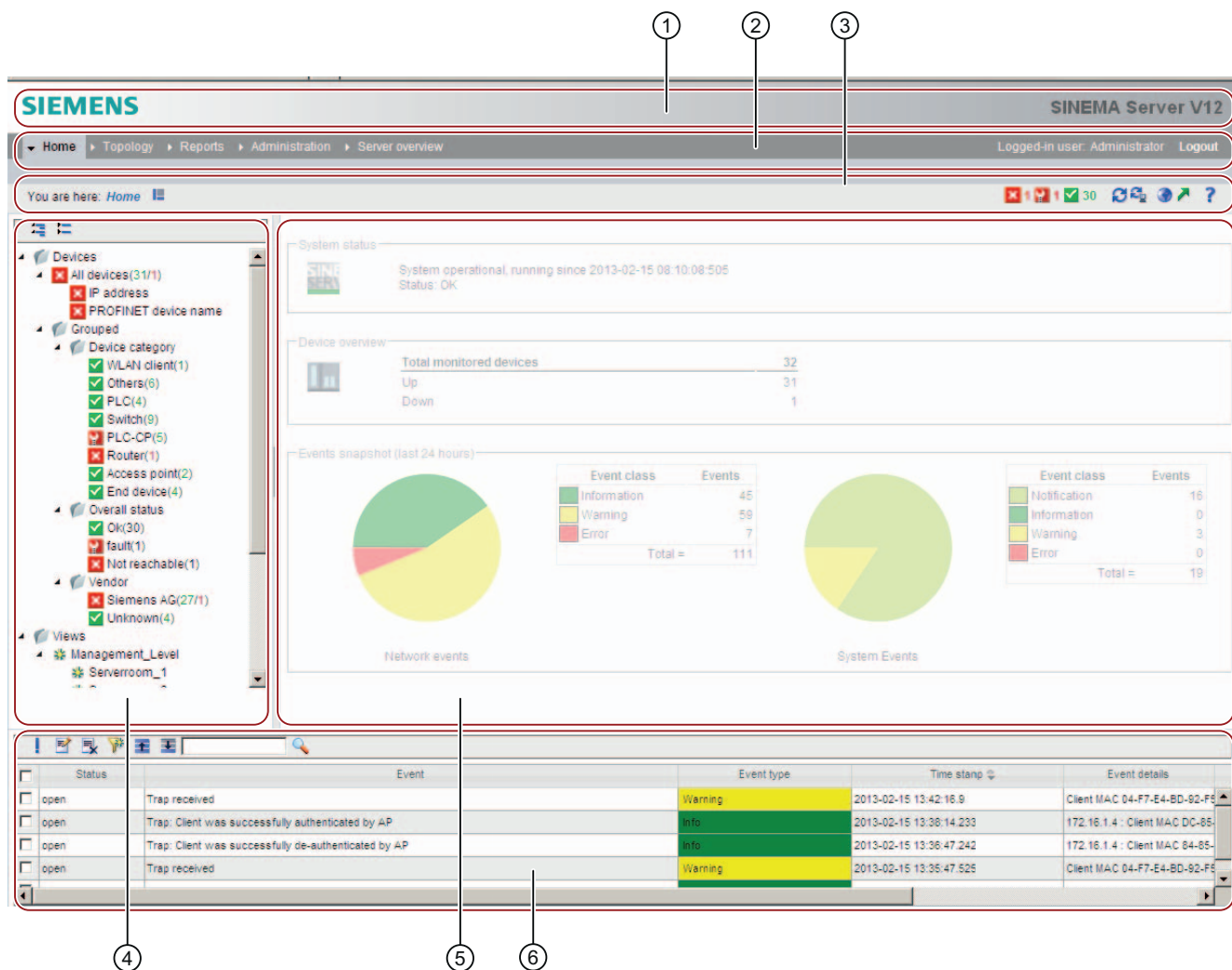
The most important action before first using the application is to scan the devices in the network. For more detailed information, refer to section Detecting devices in the network (Page 51)

2.6.2 SINEMA Server user interface on the Web interface

Program window

The program window of SINEMA Server is divided into several areas, some of which are always visible and always have the same type of content. These areas contain both general information and operator controls for performing basic program actions.

The following screenshot shows the program window with its permanent areas and the main window for the specific views.



- ① Header area
- ② Navigation bar
- ③ Status bar
- ④ Device tree
- ⑤ Main window
- ⑥ Event list

Operation / content

The individual areas of the program window are explained below in detail with their information content and the functional options.

- ① **Header area**

This area contains the SIEMENS logo and program name (SINEMA Server V12).

Note

Displaying program information

If you click on the program name, an information window opens. It contains program information such as the version number, release date, scope of the license and the type and version of the open source software used.

- ② **Navigation bar**

- 1st row:

To the left in the navigation bar is the first level of the menus, from which you can call the individual program functions. The right area displays your username and the logout button.

The content of the menu bar varies depending on the status of SINEMA Server. The "Topology" menu item is displayed only following an initial discovery.

- 2nd row:














This shows the menu commands of the second level, depending on the command you have chosen in the first level.

For detailed information on the menu commands, refer to the section section (Page 89).

- **③ Status bar**

In the left area, you see the branch of the menu tree you are in, and also the part of the program or the window that is currently open.

The right-hand section of the status bar contains the following function elements:

Icon	Display / function	Icon	Display / function
	Full screen mode on/off (hide/show the device tree and events)		(animated): Network is scanned
	(with number): Number of unreachable devices		(with number): Number of devices with error status
	(with number): Number of devices with warning status		(with number): Number of devices with information status
	(with number): Number of devices with OK status		Refresh display
	Autorefresh on/off		Select language A selection dialog with the available languages is displayed. The changeover also affects the display of the online help.
	Managing and using quick links Opens the list of available quick links.		Open help system Opens the help page for the current Web page in a separate window of the Web browser.
	Printing The print function is available on the following Web pages: <ul style="list-style-type: none"> • Topology • Reports 		

- **④ Device tree**

The device tree shows all the devices in the network as an overall list or grouped according to various properties (type, vendor).

For certain purposes, you define user-specific "Views" that include only some of the existing devices or only part of the overall network.

In the device tree, you have an overview of the statuses 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 branch.










- ⑤ **Main window**

Depending on the selected function, the main window contains specific views, for example the start window.

- ⑥ **Events list**

The events list shows the last five events (errors, warnings, messages) that have occurred in the network. Initially, the display is sorted chronologically. By clicking on the column headers, you can sort the display according to any property in ascending or descending order. Other operating options are provided by the toolbar located above.

The following table explains the function elements of this toolbar.

Icon	Display / function	Icon	Display / function
	Acknowledge the selected events. If no rows are marked, SINEMA Server acknowledges (after confirmation) all events.		Write or edit comments for the selected events.
	Delete the comments for the selected events.		Set filters for the event view. A separate window with available filter criteria opens.
	Maximize event list - over the entire program window		Minimize event list (hide) or return maximized list back to normal size. Note: A minimized window can be restored by clicking  (middle lower window frame).
	Text box for search key. The text entered is compared with all data fields compared (entire row) during the search.		Start search. All rows in which the sought after text was found remain in the list, others are hidden for a brief time.

Selecting the language of the user interface

You can change the language of the Web user interface at any time "online" by clicking the corresponding icon in the header. The changeover also affects the display of the online help.

Using SINEMA Server - the most important functions

3.1 Detecting devices in the network

3.1.1 Overview

The basic requirement for setting up network monitoring in SINEMA Server is the network scan for device discovery. You initiate this activity after first starting SINEMA Server and when necessary at the touch of the button or automatically in suitably configured cycles.

When scanning devices in the network, the following is started in SINEMA Server:

- During the first scan, devices are searched for according to selectable criteria.
Depending on the configuration in SINEMA Server, either all the devices discovered by DCP or devices in certain IP address ranges are recorded.
- The devices discovered using DCP, ICMP and SNMP are put together in the device list. The discovered connections are put together in the "Discovered topology".
Based on the discovery rules in the profile data, the devices are assigned to a suitable stored profile. Devices that cannot be assigned to any discovery rules are assigned to the available default profiles; see also section Profile concept (Page 60)
- The detected devices are changed to the "Monitored device" status in SINEMA Server. (Note: the number of devices in the "Monitored" status is limited by the SINEMA Server licensing.)
- When you scan again, newly added and removed devices are detected. The device list and the "Discovered topology" are updated accordingly.

The device discovery and the associated topology discovery are based on the protocol mechanisms of DCP and SNMP.

3.1.2 Scanning in the network

Requirements - adapting the scan range

Before you first start the scan, it is advisable to adapt the scan range.

Adapt the range using the menu command "**Administration > Discovery > Scan**" in "IP address ranges for network search". As default, SINEMA Server calculates the start and end of the IP range based on the subnet mask configured on the network interface adapter.

3.1 Detecting devices in the network

If you do not adapt the scan range, the device scan can take a very long time if there is a very large scan range. If the scan range includes more than 500 devices that need to be configured in the network, you will be notified of the expected duration of the scan. It is therefore advisable to specify the IP address range in up to 20 small subgroups instead of one large group if the IP addresses are not consecutive. This division speeds up scanning of the devices.

Network scan - procedure

To scan the network, follow the steps below:

1. Select the menu command **"Administration > Discovery"**
2. In the "Scan" tab, select the values or enter the values required for the IP address range, DCP network adapter, DCP discovery type.
3. Select the "Scan for network adapters" function
The network adapters available on the management station are displayed.
4. Select the network adapters (known as NICs below) via which the discovery will be performed.
5. When necessary, enter further parameters in the Web pages
 - **"Administration > Discovery"** in the "Profiles" tab
 - **"Administration > Network"** in the "Time settings" and in the "SNMP settings" tabs
6. Select the menu command **"Administration > Discovery"** again and open the "Scan" tab.
7. Select the IP address ranges to be searched.
8. Click "Start scan" to start the network scan. The network is scanned according to the scan ranges for the subnets.
 - The progress of the scanning is indicated by an icon on the right-hand side of the second header.
 - On completion of the scan, all discovered network devices and their status are displayed on the **"Device list"** Web page.

Special features to note

Note

Effect of the option "Include all devices discovered with TCP in the result"

If you select the option "Include all devices discovered with DCP in the result" in the DCP scan settings, note the following:

With this setting, it is possible that DCP devices that are outside the IP ranges but within the subnets connected to the NICs are also detected.

NOTICE

Avoid stopping/starting during network scanning

If SINEMA Server is stopped during the scanning and then restarted, this can lead to inconsistent responses in the application. As result of this, it is possible that the discovered network devices do not change to the monitored status. The information under "Device details" and "Device topology" may also not be available. To avoid this, keep to the following rules during scanning:

- Before starting SINEMA Server, make sure that the scan has not started.
- If the automatic scan is running, delete the devices found during the scan and scan the network again.

NOTICE

Do not change the date or time

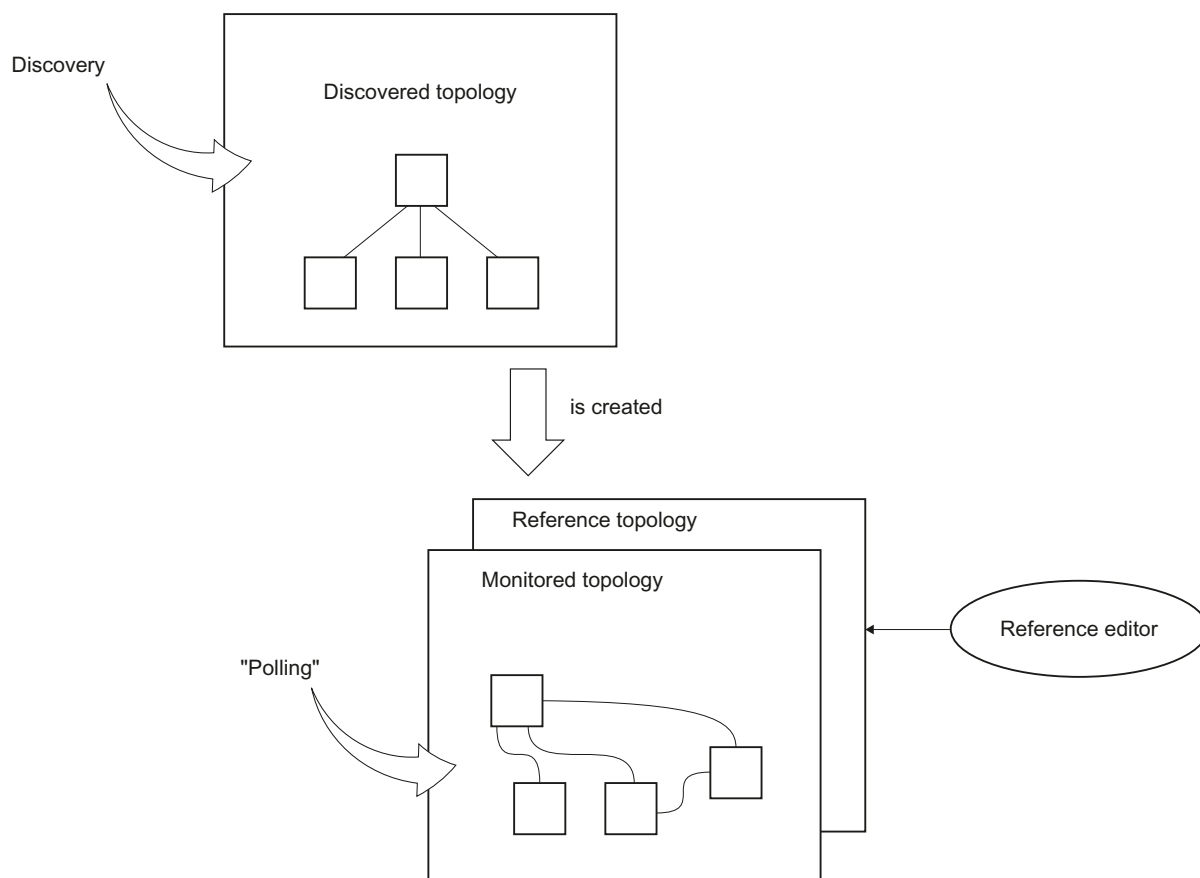
While the SINEMA Server application is running, it is advisable not to change the date or time of the system in any way. Such changes have effects on the application and cause unwanted side-effects.

3.2 Visualizing the network topology / monitoring network devices

3.2.1 Topology - Overview

SINEMA Server features the following representation forms or tools for viewing, monitoring and configuration of networks :

- Discovered topology
- Reference topology with Reference editor
- Monitored topology



Discovered topology - result of the "discovery"

The "Discovered topology" Web page is used to display the currently discovered status of the network. This shows a network topology that SINEMA Server calculates from the returned connection parameters of the discovered devices.

The "Discovered topology" Web page is the result of "discovery" alongside the device list.

New devices are also shown in this current topology. These devices are indicated by the icon for new devices. SINEMA Server automatically discovers the devices in the network and shows their topology and the connection information for the entire network based on the SNMP information. If a device does not support SNMP, no connection lines are shown. If a device supports SNMP, connection lines are shown to devices with LLDP MIB support. The root node of the network topology is the management station.

The "Current topology" includes two types of view:

- Detail view
- Icon view

The detail view is used to display the topology layout of the devices and their connections. It shows the device status, port status and connection lines. The icon view shows the topology layout with devices and their connections in the form of icons.

Note

Deviations are possible

Depending on the information provided in the network by the devices, parts of the discovered topology can deviate from the real network topology.

Reference topology / Reference editor

In a large network there may be several points at which the topology does not show all connections or at which possibly incorrect connections are discovered. One reason for this may be that devices are discovered in the network for which SNMP is disabled. It is possible that there is no LLDP MIB support available for these devices. It is also possible that unmanaged devices exist in the network that cannot be specified automatically by SINEMA Server.

To obtain complete and correct information for the reference topology and to provide the opportunity of changing this topology manually, a Reference editor is available.

The topology shown in the Reference editor is based initially on the discovered topology. In the Reference editor, you can correct the discovered topology by specifying the corrected network topology as a reference or target. The Reference editor serves the following purposes:

- Drawing/modifying reference connections
- Enabling / disabling the status of the ports
- Enabling / disabling references for SNMP, TCP protocols

Note

Administrator rights required

As default, only users with administrator rights have access to the Reference editor. If several administrators are working with the Reference editor, the last saved topology is used as the reference topology.

Monitored topology

The "Monitored topology" Web page shows the following information based on the reference topology:

- The status of the ports of the network devices
- The reference connections compared with the discovered network topology

The information on the Web page will help you to understand changes or differences in a network. These include changes to the port status, the network devices and their connections within the topology.

Further information to the response in this display:

- Layout and positions of the devices are only calculated once.
- Each new device that is not part of the reference topology is not shown.
- New devices are identified by an icon.
- Unmonitored devices are not shown in this topology. If a device is set to "unmonitored", it is automatically removed from the reference topology. If such the device is returned to the monitored status, the application handles this device like a new device.

Note

The reference topology is a prerequisite

The tree structure of the "Monitored topology" Web page is only displayed if the reference topology has been saved at least once.

3.2.2 Topology discovery

Network scan - effect on the topology discovery

On completion of the network scan, the actual network topology is displayed on the "Discovered topology" Web page. The display contains the objects management station, devices, ports and connection lines with the relevant connection status.

The topology scan of the SINEMA Server application is always performed in conjunction with a network scan. As soon as a network scan is completed, the topology scan is started automatically. This means that changes to the connections (new connections or modified connections) are detected either on completion of a manual network scan or after a regular automatic scan of the network.

Note

Forcing the discovery of modified SNMP values

To scan a specific set of devices within the network for modified SNMP values, it is advisable to use the "Force read SNMP data from device" icon. This icon exists in all tabs of the "Device details" Web page.

Principle of topology discovery

The network topology discovery is based on SNMP information of the device. If a device supports SNMP, connection lines are shown to devices with LLDP MIB support. For this reason, LLDP and bridge information is useful to detect the topology of the network.

On management stations, LLDP and bridge information are not used for the topology scan even if the station supports LLDP/bridge. If neighboring devices support LLDP/bridge, the connections to the management station can be detected.

Note

Enabling the SNMP protocol

To obtain the precise number of ports and accurate connection information, it is advisable to enable the SNMP protocol for the relevant devices.

3.2.3 Setting up monitored topology with the reference topology

Meaning

On completion of discovery, the devices can already be monitored in the device list. The topology display expands this option in a graphic view. The essential thing here is the display of the connections between the devices and the connection statuses.

By creating the reference topology, you provide the basis for the display on the "Monitored topology" Web page and in other specific views.

Reference editor

The Reference editor is used to specify the reference topology. The Reference editor provides options for manual editing of the reference topology. Initially, the Reference editor checks whether or not a reference topology exists. If no reference topology has been specified the discovered topology is used to sort the devices. This procedure continues until the reference topology has been configured.

The Reference editor provides functions for the following purposes:

- Configuration of references for port statuses
- Configuration of references for SNMP, DCP protocols
- Configuration of references for connection lines
- Adding unmanaged devices and network clouds
- Configuration of protocol-specific device availability
- Adding new devices in the editor
- Drawing reference connections

Procedure

1. Select the "**Topology > Reference**" menu command

This opens the "Reference topology" Web page with the functions of the Reference editor.

2. Enter the devices from the "Device hierarchy" area in the topology display area.

You can select several or all devices and include them in the display.

After completing your configuration in the Reference editor, change to the topology view with the "**Topology > Monitored**" menu command. In the topology view, the devices of the entire network are shown and monitored.

Note

When SINEMA Server first loads the reference topology, all ports with an unknown status are shown as having the "Not in operation" status. When you save this topology information, this "Not in operation" status is also saved.

Components of the Reference editor view

Display of nodes/connections/ports

In the Device editor area, the display of the Reference editor contains the topology information of all the devices connected in the network. An unknown device is displayed as a cloud in the Reference editor. As default, the device name and the device IP address are shown in the text display box. The content of the text display box of all devices can be configured with the "Configure nodes" button.

The connection lines in the Device editor view area have line numbers at both ends of the connection. This display is identical for the connections in the current and in the reference topology. The protocols supported by every device are displayed in the right-hand corner of the text display field. The two protocol statuses "S" and "D" indicate the status of the SNMP and DCP reachability. A scored-through icon indicates that there is no protocol support available for the specific device.

3.3 Setting up network devices individually - using the Profile editor

3.3.1 Profile concept

Profiles

Profiles give the SINEMA Server flexibility during device discovery, device monitoring and device display. Profiles describe device types in terms of common properties.

SINEMA Server distinguishes the following types of profile:

- General 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.

In addition to the general profile, a device can also be assigned a monitoring profile. As result, user-specific monitoring rules remain unaffected by changes in the general profile. This is an advantage when a vendor-specific general profile is replaced by a new profile version.

Principle of the use of profiles - expansion with the Profile editor when necessary

Based on the stored profiles, when each device is discovered the first time, SINEMA Server searches for the profiles containing suitable discovery rules. Based on this discovery, SINEMA Server can then use the properties stored in the profile for monitoring and displaying a network device.

Before running the network scan, you should check whether or not the profiles stored in SINEMA Server cover all the device types to be monitored in the network. If no suitable profile is stored for a network device, SINEMA Server supports you with the Profile editor when making the necessary adaptations and additions to the profile database.

New profiles are always created based on existing profiles.

To assign a profile to devices that do not correspond to any previously stored profile or any device type contained in the profiles, you have the following alternatives:

- You assign the new device type to an existing profile.
- You create a new profile to which the new device type is assigned.

Use of default profiles

If no assignment based on the discovery rules of profiles is possible during the discovery of a device, SINEMA Server assigns this device that has not been uniquely identified to a default profile as follows.

- Step 1:

If it is clear from the device ID that this is a Siemens device, the following profile is used:

- Siemens_Standard

- Step 2:

If no assignment is possible in step 1, a 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, SINEMA Server attempts to identify the following so-called criteria based on the SNMP data of the device:

1. sysDesc (OID 1.3.6.1.2.1.1.0):

A textual description of the device. This value should include the full name and version identification of the system hardware type, the software operating system and the network software.

2. lldpLocSysDesc (OID 1.0.8802.1.1.2.1.3.4.0):

The value of the character string is required to identify the system description of the local system. If the local agent supports IETF RFC 3418, the lldpLocSysDesc should have the same value as the sysDesc 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. DCP_ID

6. sysObjectID (OID 1.3.6.1.2.1.1.2.0):

The decisive identification of the network management subsystem is contained in the entity. This value is assigned within the "SMI enterprises sub tree" (1.3.6.1.4.1) and provides a simple and unique description for the specification "what kind of box is being managed".

Automatic profile assignment

Based on the SNMP data, for each newly discovered device, SINEMA Server searches for the profiles containing the suitable discovery rules.

- Step 1 - deciding on the profile

If more than one 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 profile, the profile with the longer name wins.

- Step 2 - using device type rules for the device within the selected profile

SINEMA Server identifies the suitable device type and uses the icon specified here for the display. If the device type cannot be identified, SINEMA Server uses the default symbol stored in the profile.

3.3.2 Setting up profiles and assigning device types

The following actions are described below:

- Add a new device type to an existing profile
- Create a new profile

Adding a new device type to an existing profile - procedure

To add a new device type to an existing profile, follow the steps below:

1. Open the "Profiles" tab with the **"Administration > Discovery"** menu command
2. Select the profile and open it with the "Edit" button or double-click on the list entry.
3. Change to the "Discovery rules" tab

4. Check the requirement for the usability of the profile. Before a device of the new device type you want to add is discovered, a suitable standard/regulation must exist.

At least one of the discovery rules of the profile must match such device. If this is not the case, add a new discovery rule to the profile.

5. Change to the "Device types" tab and select the "Add device type rule" function

The profile editor opens and you can enter the data for the new device type rule.

6. Follow the steps below in the Profile editor:

- Enter the name of the rule in the "Name" box. This is only the name of the rule not the name of the new device type.
- Enter the name of the new device type in the "Device type" box.
- Select the icon of the new device type.

Note

Discovery rule before device type rule

A device type rule is only evaluated if a suitable discovery rule was first recognized as matching.

Creating a new profile -principle

When creating a new profile, you always base this on an existing profile. For this reason in the first step, you check which of the existing profiles represents the most suitable basis.

If you intend to create a new general profile, it is advisable to use an existing default profile as the basis. This avoids specific properties that may exist in a specific profile from being included in the new profile.

The following default profiles are available:

- Standard SNMP with DCP approval (name: DEFAULT_SNMP_DCP_Device)
- Standard SNMP (name: DEFAULT_SNMP_Device)
- Standard DCP (name: DEFAULT_DCP_Device)
- Standard ICMP (name: DEFAULT_ICMP_Device)

To be able to select the suitable profile, you should know the protocols used in the new device family.

Creating a new profile - procedure

To create a new profile, follow the steps below:

1. Open the "Profiles" tab with the **"Administration > Discovery"** menu command
2. Select the default profile and select the "Create profile" function.

This opens the "Add profile ID" dialog.

3. Now assign a unique profile ID. This is used globally in SINEMA Server as the profile ID.

As an option, decide whether or not the properties of the basic profile you are using should be included:

- Discovery rules
- Device type rules

4. Confirm your entry.

The Profile editor opens and you can enter the data for the new profile.

Follow the steps below in the Profile editor:

3.3 Setting up network devices individually - using the Profile editor

1. Enter the name of the profile in the "Basic data" tab. Select the other parameters including the required default icon for the profile.
2. Change to the "Discovery rules" tab and enter one or more rules required for the discovery of a device of this profile. You first need to clarify which rules are valid for the device.
3. Change to the "Device types" tab to specify device types individually within the profile and to assign the device type rule.

Creating a monitoring profile - principle

The procedure corresponds to the steps described earlier in "Creating a new profile". The "Discovery rules" and "Device types" tabs are omitted here.

To create a monitoring profile for a specific device in addition to a general profile, use the corresponding general profile as the base profile for creating the new monitoring profile.

You then assign this monitoring profile to the device. This separates the profiles required for device discovery and for device monitoring.

See also

Administration - Discovery / Profiles (Page 165)

3.4 Configuring event reactions - displaying events

3.4.1 Events

Each change to the operating status and every error/fault detected in the network counts as an event. Events are divided into two categories: Events at the network level and events at the system level.

The following types exist:

- **Traps**

When certain alarm events occur, devices generate trap frames that can be evaluated by management stations. The trap frames contain error messages in plain text. Which management station traps are sent to needs to be configured on the relevant devices.

- **Network events**

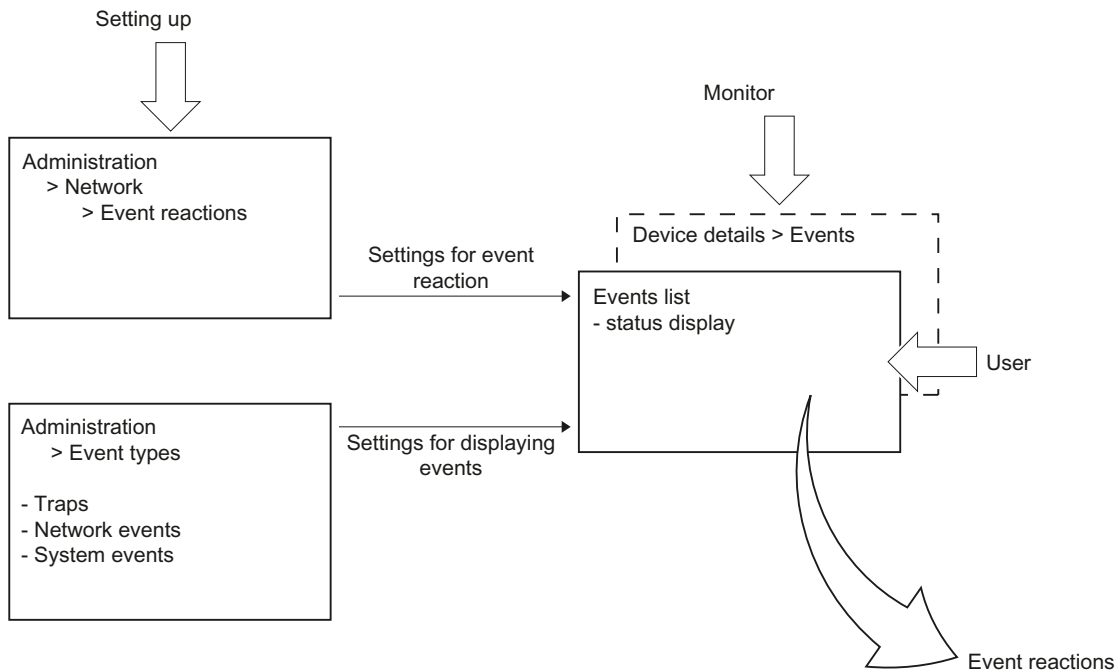
Network events provide information about changes or error events in the network.

- **System events**

System events provide information about actions, changes and error events of SINEMA Server.

Setting up and monitoring events in SINEMA Server

The following graphic illustrates the relationships of the SINEMA Server functions for setting up and monitoring network and system events.



- Setting up events

Setting up the events is part of administration.

- Settings for the event reaction

You make the settings for the event reaction with the menu command **"Administration > Network > Event reactions"**.

Here, you specify the reactions to events or status changes. You can also specify the context to which the reaction should relate. You can choose between the views, device and system.

By selecting a SINEMA Server view, you achieve the situation that the defined reaction will take place when the device affected by the event is part of the selected view. This allows you to define a view-specific event reaction.

You will find more detailed information on this function in the section Administration - Network Event reactions (Page 174)

- Settings for the event display

You make the settings for the event display with the **"Administration > Event types"** menu command.

You specify which events will be actively monitored. You can also adapt the event texts and event classifications.

You will find more detailed information on this function in the section Administration - Event types (Page 183)

- Monitoring events -

- Event list

The events list is used to monitor events. It shows the current statuses of the events enabled in SINEMA Server.

Which events are displayed also depends on the views assigned to the currently entered user. This means that events of interest are only monitored in conjunction with the configured views.

The events list is described in the following sections.

- Device details > Events

An additional option for obtaining a device-specific overview of the status of the configured events is to use the display of the device details.

You will find more detailed information on this function in the section Device details (Page 105)

3.4.2 Event list

Event list

The events list shows all the events generated in the network in the form of a table. This page provides various navigation options in the upper part of the page. For each event, specific parameters are displayed in a separate table row that are explained below.

Status	Event	Event type	Time stamp	Event details	IP address
<input type="checkbox"/> open	Trap: Überlappender Access Point gefunden	Warning	2013-03-20 17:49:44.874	172.16.1.4 : Overlap-AP aged out: AP 'CONN2'	172.16.50.5
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 17:49:33.407	Overlap-AP aged out: AP 'CONN1' [00:0E:8C:A...	172.16.50.5
<input type="checkbox"/> open	Netzwerk-Durchsuchung nach neuen Geräten	System_Notification	2013-03-20 17:48:45.39		172.16.50.5
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 17:48:33.409	Overlap-AP aged out: AP 'CONN1' [00:0E:8C:DE...	172.16.50.5
<input checked="" type="checkbox"/> open	Netzwerk-Scan gestartet	System_Notification	2013-03-20 17:48:19.189		172.16.50.5
<input type="checkbox"/> open	Netzwerk-Durchsuchung nach neuen Geräten	System_Notification	2013-03-20 17:33:53.975		172.16.50.5
<input type="checkbox"/> open	Netzwerk-Scan gestartet	System_Notification	2013-03-20 17:33:19.147		172.16.50.5
<input type="checkbox"/> open	Signalstärke zu, verbundenen AP ist gering	Warning	2013-03-20 17:33:11.16	MAC: 00:0e:8c:9b:96:18, Wert: -71	172.16.50.26
<input type="checkbox"/> open	Trap: Client erfolgreich am Access Point abgemeldet	Info	2013-03-20 17:31:28.215	172.16.1.4 : Client MAC 18-87-96-18-B8-0A on	172.16.50.5
<input type="checkbox"/> open	Signalstärke zum verbundenen AP ist wieder normal	Info	2013-03-20 17:28:12.529	MAC: 00:0e:8c:9b:96:18, Wert: -69	172.16.50.26
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 17:27:33.373	Client MAC 04-F7-E4-BD-92-F5 on VLAN 1 VA	172.16.50.25
<input type="checkbox"/> open	Signalstärke zu, verbundenen AP ist gering	Warning	2013-03-20 17:23:12.218	MAC: 00:0e:8c:9b:96:18, Wert: -70	172.16.50.26
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 17:21:29.04	Client MAC 04-F7-E4-BD-92-F5 on VLAN 1 VA	172.16.50.25
<input type="checkbox"/> open	Netzwerk-Durchsuchung nach neuen Geräten	System_Notification	2013-03-20 17:18:45.473		172.16.50.5
<input type="checkbox"/> open	Netzwerk-Scan gestartet	System_Notification	2013-03-20 17:18:19.098		172.16.50.5
<input type="checkbox"/> open	Signalstärke zum verbundenen AP ist wieder normal	Info	2013-03-20 17:18:12.608	MAC: 00:0e:8c:9b:96:18, Wert: -69	172.16.50.26
<input type="checkbox"/> open	Netzwerk-Durchsuchung nach neuen Geräten	System_Notification	2013-03-20 17:03:45.472		172.16.50.5
<input type="checkbox"/> open	Netzwerk-Scan gestartet	System_Notification	2013-03-20 17:03:19.057		172.16.50.5
<input type="checkbox"/> open	Signalstärke zu, verbundenen AP ist gering	Warning	2013-03-20 16:58:12.476	MAC: 00:0e:8c:9b:96:18, Wert: -70	172.16.50.26
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 16:53:33.342	Client MAC 04-F7-E4-BD-92-F5 on VLAN 1 VA	172.16.50.25
<input type="checkbox"/> open	Signalstärke zum verbundenen AP ist wieder normal	Info	2013-03-20 16:53:12.547	MAC: 00:0e:8c:9b:96:18, Wert: -69	172.16.50.26
<input type="checkbox"/> open	Netzwerk-Durchsuchung nach neuen Geräten	System_Notification	2013-03-20 16:48:44.972		172.16.50.5
<input type="checkbox"/> open	Netzwerk-Scan gestartet	System_Notification	2013-03-20 16:48:19.018		172.16.50.5
<input type="checkbox"/> open	Signalstärke zum verbundenen Client ist gering	Warning	2013-03-20 16:48:11.467	MAC: 04:f7:e4:bd:92:f5, Wert: -89	172.16.50.25
<input type="checkbox"/> open	Trap empfangen	Warning	2013-03-20 16:47:35.79	Client MAC 04-F7-E4-BD-92-F5 on VLAN 1 VA	172.16.50.25

Extent of the display - user management and views

Which events are displayed also depends on the views assigned to the currently entered user. This means that events of interest are only monitored in conjunction with the configured views.

Meaning

Below you will find information about the significance of the individual boxes:

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.
Status	Display of the acknowledgement status. <ul style="list-style-type: none"> "X" = acknowledged "Open" = not acknowledged
Event	Configured event information or event message.
Event type	Information on the type (weighting) of the event. The entries are color-coded with the following meaning: <ul style="list-style-type: none"> green = system information yellow = warning green/yellow = notification red = error
Time stamp	The "Time stamp" box provides information on the date and time of the generation of the event.
Event details	Shows the full information for each event.
IP address	Shows the IP address of the source device.
Interface	Provides information on the interface type being used and the interface number. This box uses a separate, unique numbering sequence for LAN and WLAN devices.
Trigger	Name of the source device.
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.








Note

Receiving SNMP traps

SINEMA Server receives SNMP traps only if the IP address of the SINEMA Server is configured on the relevant devices as the trap destination.

Operator input

The following table explains the function elements of the header.

Icon	Meaning
	Confirm events By acknowledging events, you confirm your awareness of the changed status of an active entry in the events list. No other reaction is associated with the acknowledgement. Configured event reactions are triggered solely by the status change of the event.
	Edit remark Note: If several events are selected, an edited comment is entered for all the selected events.
	Delete remark
	Filter events Note the description in the following section.
	Maximize / minimize As default, SINEMA Server shows up to 5 events in the events list. By maximizing the display, you expand the display of the events 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 events list and configuring the layout of the events list.
	Enter text for text search / filter setting
	Start text search / filter setting Result: The traps / events that match the text string specified for the text search are displayed.

See also

Administration - Network Event reactions (Page 174)

3.4.3 Filter events

Selecting events

In the filter function, you can select events for display as follows:

Meaning

- Filter: Last events

Here the following can be selected:

- All
- Open
- Acknowledged

- Displayed types and categories

The filter settings that can be selected here are a combination of event (system / network) and event type (weighting).

Information events

The following filter settings belong to this:

- System notification
- System information
- Network information

The events displayed based on this criterion are generally messages/updates relating to the network and network devices. In contrast, at the system level, these events are generated as result of changes in the performance of SINEMA Server.

Information events require no action from the end user. The event-related information relates either to a message about a user action performed by the application or to an update due to status changes of network devices. Examples of reported events on the page for information events include: User logins/logouts, completion of device discovery, checking of software drivers, start/end of the network scan or permissions granted by the administrator.

Warning events

The following filter settings belong to this:

- System warning
- Network warning

A warning indicates a status that could cause a problem in the future. After receiving the warning message, some action is necessary to ensure the problem-free operation of the devices in the network. These actions then prevent future errors/faults or traps on network devices or in the SINEMA Server application.

Examples of reported events on the page for warning events include:

- Trap(s) received
- Start of a device reply to DCP
- Link down received, link up received
- Connections activated/deactivated

Error/fault events

The following filter settings belong to this:

- System fault
- Network error

When such events occur, fast intervention is required. Depending on the content of the error message, the user must take suitable measures. The event reactions already configured for the error events simplify things.

The most important system errors generated by error events include:

- DCP subtask is not executed
- Scan manager is not run
- Memory assignment failed
- Callback address invalid

3.5 Setting up and using views

3.5.1 Setting up views

Views - purpose and use

Dividing up a large hierarchy of the network topology into small groups made up of several devices simplifies the management or monitoring of the devices and their connections.

View-specific device lists and topologies also provide options for configuring the list of monitored devices. This option can be useful for monitoring the port status of a small group of devices with user-defined connections.

The screenshot shows the SINEMA Server interface. The left sidebar displays a hierarchy of devices and views. The main area displays a table of devices with columns for Status, IP address, PROFINET device name, Device type, MAC, and Views. Annotations 1-4 point to specific elements:

- ① View-specific device list
- ② View-specific topology
- ③ Basic views
- ④ Sub views

Status	IP address	PROFINET device name	Device type	MAC	Views
❌	192.168.10.11+		CP 343-1 Adv (1GX30-0XE)	00:0E:8C:A4:AA:DA+	LineB_partA,ProductionLi
✅	192.168.20.21	Hans	SCALANCE X204IRT (0B/	08:00:06:94:7E:64	LineB_partA,ProductionLi
✅	172.16.50.58	cp-058-cp443-1-1gx30	CP 443-1 Adv (1GX30-0XE)	00:1B:1B:43:DF:95	LineB_partB1,ProductionL
✅	172.16.50.60	homer	DEFAULT_SNMP_DCP_I	00:80:63:45:03:2A	LineB_partB1,ProductionL
✅	172.16.50.61		DEFAULT_SNMP_Device	00:80:63:B8:44:F5	LineB_partB1,ProductionL
✅	172.16.50.62		DEFAULT_SNMP_Device	00:80:63:B9:12:D8	LineB_partA,ProductionLi
✅	172.16.50.64	Paulchen	SCALANCE X224 (0BA00	00:0E:8C:8B:6C:60	LineB_partA,ProductionLi
✅	172.16.50.57	cp-057-cp-443-1-1ex30	CP 443-1 (1EX30-0XE0)	00:1B:1B:45:AF:8C	LineB_partB1,ProductionL

Aims

From the total monitored network, setting up separate device groups with the following properties and options:

- Basic views: providing a specific view of a section of the total monitoring
- Sub views: when necessary set up further specific sub views
- when necessary, a view-specific topology view
- view-specific display in the events list (see also section Event list (Page 68))

Requirements

To be able to set up views, the following requirements must be met:

- Topology: The reference topology exists
- User rights: Administrator

Create a new view in the device tree

Depending on the initial situation, two variants need to be distinguished:

Creating a basic view

1. Select the "Views" node in the device tree
2. With the right mouse button select the "Create new view" function; this opens the View editor.
3. Configure the new view in the View editor by selecting the required devices from the list of possible devices.
4. In the View editor, specify whether or not a specific topology display will be used.
5. If necessary, configure the topology.

Creating a sub view

1. Select one of the existing view nodes in the device tree.
2. With the right mouse button select the "Create new view" function; this opens the View editor.
3. Configure the new view in the View editor.
4. In the View editor, specify whether or not a specific topology display will be used.
5. If necessary, configure the topology.

Note

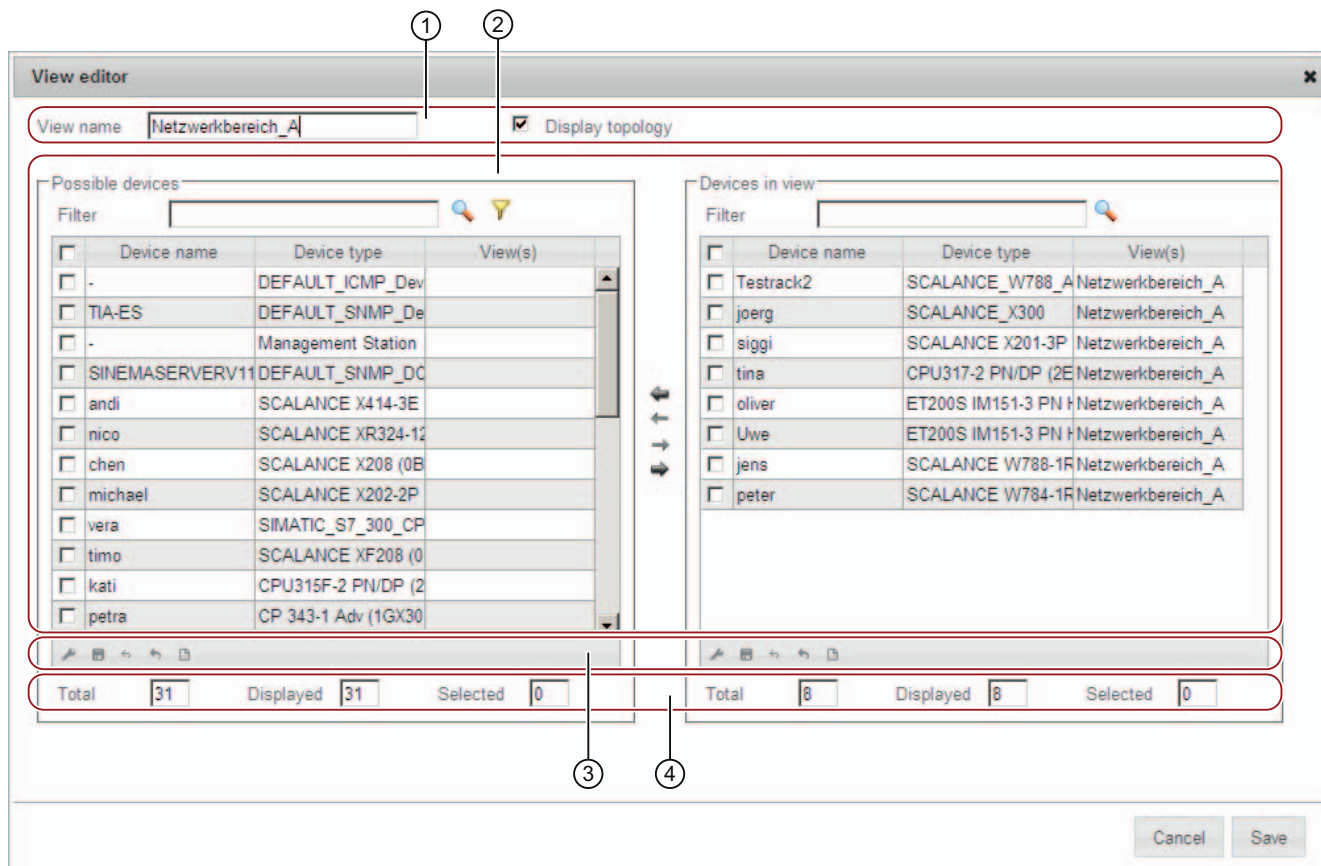
Views cannot be moved in the hierarchy

It is advisable to plan the view structure carefully prior to creating views. After a view has been created, it is not possible to move it to a different position in the hierarchy.

NOTICE
Deleting views When you delete a view, the view itself, all the sub views it contains and all assignments to users or event reactions are deleted.

3.5.2 The View editor

You open the View editor in the device tree with the function for creating or editing a view.



- ① Header
- ② Assignment area
- ③ Settings area
- ④ Statistics

How it works

In the assignment area, from the list of "Possible devices" add the devices intended for the view to the "Devices in view" list.

View filter in the View editor

The view filter allows you to preselect devices that have not yet been assigned to the current view.

The following options are available for setting the view filter:

- Show all devices (regardless of view).
- Display devices that are not part of a view (except for this view).

The node with the user-specific views is also displayed and can be selected. Select the views whose network devices should not be included in the "Possible devices" list.

- Select views whose devices will be displayed.

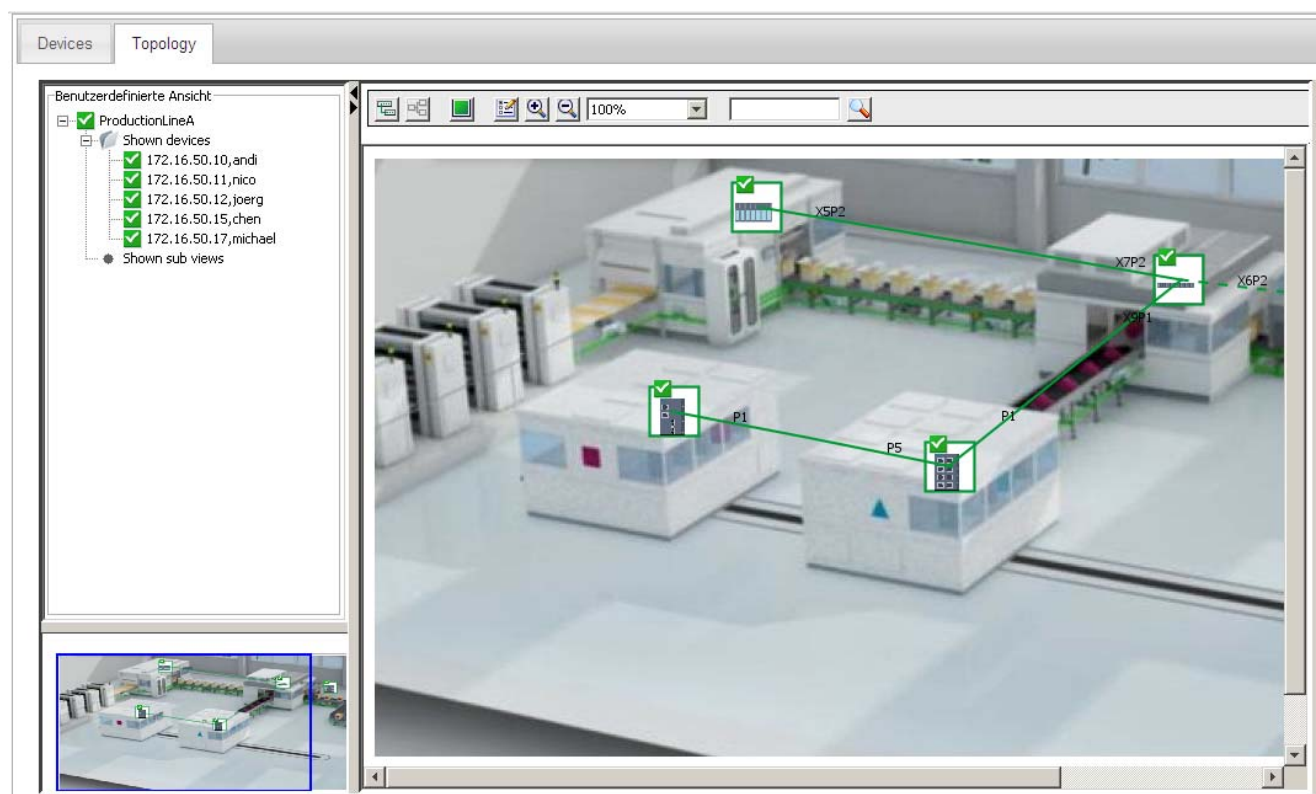
The node with the user-specific views is also displayed and can be selected.

3.5.3 Creating a view-specific topology

Overview

The topology in the views shows an area with which you can create, display and manage network devices and connections between them to be monitored. Various options are available with which you can change a topology display, draw connection lines and display reference connections. The topology shown in the view area is based only on the reference topology.

Views are used when you want to monitor a limited set of devices within the network. This makes it easier to manage user-defined connections. You have options available for displaying and identifying user-defined connections and reference connections in the relevant colors.



The editor in detail

For a description of the editor functions and icons, see section Views (Page 115)

Creating a view-specific topology

Requirement: You have selected the "Topology" option in the view editor.

A new empty page is opened. The opened page is in "Draft mode". It contains options for creating a topology

To create a view-specific topology, follow the steps below:

1. Add the devices from the "Device hierarchy" area

The devices and their connections are shown. Requirement: Connections are only displayed if they have been adopted as reference connections in the Reference editor.

Assign the devices according to your requirements. If required, add specific background graphics to make the view clearer.

2. To save these changes, click "Save". Then change to the "Active mode"

Creating the topology for sub views

You also have the option of creating topology displays for sub views. This allows you to focus the display on the connections between the device groups of the sub views.

Follow the steps below:

1. To do this, go to the left-hand area "User-defined views" in the topology display of the higher-level view. Under the "Available sub views" entry, select the required device groups and drag these to the right to the area of the topology display.
2. Here, select the sub views and configure the connections by selecting the "Draw" icon. This opens the "Select connections between views" dialog.

Note

Topology can be mixed with sub view and device display

In the topology display, you can show sub views and device views at the same time.

Editing modes in the Topology editor

Draft mode

If you create a new topology, the topology display is automatically in Draft mode or in the "Draft" status. In the draft mode, you can assign devices, define device positions and draw connections between ports of different devices.

To show all the existing reference connections, select the "Display reference connections" check box in the toolbar. This check box is selected as default. If this option is selected, the reference connections are displayed as direct light blue lines. Connections between the ports can, however, be created with a user-defined connection.

Note

Display of an empty topology

If the reference connections have not been saved at least once in the Reference editor, an empty topology is displayed in the view area. As soon as you save modifications to reference connections in the Reference editor, a view-specific topology with all reference connections is displayed.

Note

Current port status and device status - no display in draft mode

In draft mode, the current port status and device status are not displayed in the topology. They are grayed out.

The toolbar on the "User maps" page includes the following tools for access to various modes. By selecting one of these modes, various activities can be performed in the user maps.

3.5 Setting up and using views

- Selection tool
- Tool for drawing connections
- Tool for user-defined connections

With the selection tool, you activate the selection mode. This tool is enabled automatically when you open the "User maps" page. As long as the selection mode is active, a user-defined connection has a black circle that represents a bend point. Endpoints of a reference connection are shown as a circle filled in with gray. In this mode, you can perform the following editing steps:

- Change the layout or positions of devices, background graphics
- Change the layout of connections and draw additional connections
- Insert a background graphic and change its size
- Drag devices from the catalog to the device view using the mouse
- Drag devices from the "User-defined map" sub window to the device view
- Delete devices from the device view of the user map
- Specify a reference connection as a user-defined connection
- Reset the layout of a connection
- Draw new connections between ports of different devices
- Change the layout of a connection
- Create a user-defined connection based on a reference connection

Configure connections

The following points apply to user-defined connections:

- The "Create user-defined connection" button is only available if the tool for drawing connections is activated.
- This button is used to create user-defined connections for every reference connection if the ports are not used by other user-defined connections.
- User-defined connections are displayed black.

Active mode

The active mode represents a monitoring view. The view of the devices shown in this mode is similar to the devices shown in the monitored topology. The color coding of the device status, ports and connections for objects correspond to those in the monitored topology. In active mode, only the connections drawn by the user are shown.

In active mode, it is not possible to make changes to the topology. For this reason, various buttons available in the toolbar view do not exist in active mode. In this mode, only user-defined connections are displayed. The "Display reference connections" check box is therefore not available in this mode.

The following points apply to connections drawn by users and displayed in active mode:

- If there is a connection drawn by the user between two managed stations, the color of the line depends on the fill color of both ports.
- If there is a connection drawn by the user between a managed and an unmanaged device, the color of the line depends only on the port status of the managed device.
- If there is a connection drawn by the user between two managed devices that does not correspond to any reference connection, this has a cloud icon in the middle to identify a virtual connection.
- User-defined connections between unmanaged devices are always shown in gray. The port status of an unmanaged device is unknown which is why these ports are shown gray.
- A network cloud can be added from the catalog of unmanaged devices in draft mode.

Adding a background graphic

In draft mode, you can add a background graphic to the view.

Click on the "Add background graphic" icon to add a background graphic to the view.

Configuring objects

1. Change graphic position
2. Change size of the background graphic

Change graphic position

To change the position of the background graphic, follow the steps below:

1. Activate the selection tool from the toolbar and select the background graphic. The graphic is then displayed in a black frame with white handles.
2. Move the mouse pointer over the graphic. The mouse pointer then changes to four arrows pointing in all directions.
3. Now hold down the left mouse button and drag the graphic to another position.
4. When you release the left mouse button, the position of the background graphic changes.

Change size of the background graphic

You can change the size of the background graphic of a user map. To change the size of the background graphic, follow the steps below:

1. Activate the selection tool from the toolbar and select the background graphic in the view area of the user map.
2. A black frame with white handles is then displayed.
3. Hold down the left mouse button and drag the white handles to the required position.
4. When you release the left mouse button, the size of the background graphic changes.

3.5.4 Configure connections

General overview

A view contains the device list of the monitored devices along with the user-defined connections that are displayed in the topology tree.

Creating or editing user-defined connections

In the view-specific topology, you can create or modify the user-defined connections between devices. You can also specify the reference connections as being user-defined connections. With the tool for drawing connections, you can perform the following editing steps:

- Drag user-defined connections between ports of different devices manually
- By double-clicking on a reference connection, specify it as being a user-defined connection
- Create user-defined connections for all reference connections

Note

The connection lines are derived from the corresponding port status

This means the following: Even if the port is "in operation" and the user has drawn a special connection between the ports, the connection line is shown green in the active mode. These ports can, however, also be connected to other devices. You therefore need to remember that a green connection line (active mode) in a user map does not always mean that a connection actually exists.

Functions

The following option can only be configured with the selection tool:

- Using the shortcut menu, specify a reference connection as a user-defined connection

Note

"Delete device" option

The "delete device" option is displayed if you use the selection tool and the "Draw connection" tool.

Select the device you want to delete. Right click and select "Delete device" in the shortcut menu to delete the device. This option is also available in the toolbar view.

- Drawing user-defined connections manually

User-defined connections can be drawn manually by selecting the ports of the devices you want to interconnect. Follow the steps below to draw connections between devices manually:

In the map area, click on the port of the device.

Select the device you want to connect by selecting the port.

A user-defined connection is then displayed between these two devices.

In the view-specific topology, you can draw a user-defined connection line between two devices by clicking on the ports of the devices you want to connect. A dialog box is then opened in which you select the port numbers of the devices to be connected. This allows you to draw a connection between two devices that is then displayed gray.

- By double-clicking on a reference connection, specify it as being a user-defined connection

To specify an existing reference connection as a user-defined connection, double-click on the connection line that represents the reference connection. The reference connection line becomes a user-defined connection with a black circle that represents the bend point.

- Create user-defined connections for all reference connections

In the toolbar view, the "Create user-defined connections for all reference connections" icon is available. Click this icon to specify all reference connections as user-defined connections at the same time.

- Using the shortcut menu, specify a reference connection as a user-defined connection

This option is available in the shortcut menu and can only be used with the selection tool. Select the light blue connection line that represents a reference connection. Right click on the reference connection line and select the option "Set to user-defined". The reference connection line becomes a user-defined connection with a black circle that represents the bend point.

Change the layout of a connection

The user-defined connection line between two devices has a black circle in the middle of the connection line. Using this black circle, you can bend the connection line. A connection line can have up to maximum of seven bending points.

To change the layout of the connection between devices, follow the steps below:

1. Select the drawing tool for connections and select the user-defined connection line in the user map.
2. Select the black bending point in the middle of the connection line.
3. Hold down the left mouse button and drag the bending point to another location.
4. When you release the mouse button, new bending points will be shown in the middle of the relevant connection lines.
5. You can repeat steps 3 and 4 until you have created a maximum of seven bending points.
6. Drag the bending points to different locations in the user map depending on the situation.

3.6 Users and user groups

3.6.1 SINEMA Server users and roles concept

Overview

SINEMA Server has an extensive system of access rights. This system allows the administrator to grant or deny access to certain program objects individually and according to need. During configuration, you should take into account the following criteria in the role:

- Network security
- IT experience of the users
- The necessity for certain functions
- User friendliness

Note

Managing user rights is one of the main tasks of an administrator.

This should therefore be planned and configured to meet the specific requirements while taking into account security-relevant aspects. We strongly advise you to familiarize yourself with the user and roles concept of SINEMA Server. New or modified settings should always be checked in terms of their intended effect.

Basics

The access rights in SINEMA Server are specified using the following objects:

- User
- User groups
- Views

In principle, the following applies: Each user belongs to a user group. Each user group has certain rights that are transferred automatically to all its members (users). Each user can also be assigned so-called views via which the user is also granted certain rights.

3.6 Users and user groups

Standard users and groups

In SINEMA Server, there are three predefined user groups with corresponding access rights. The control elements and options for the users differ in each user group. The following table shows the predefined name of the user group as well as information on the access rights:

Name of the user group	Access rights
Administrator	The administrator has all access rights available in SINEMA Server.
Power user	A power user has all the access rights of an administrator except for the user management rights.
Standard user	The standard user has the general access rights of an operator.

The range of access rights when working with SINEMA Server depends on the user group to which the user belongs. The grading of the access rights is shown below:

Access right	Description	Administrator	Power user	Standard user
User management	Access to user and device management	Yes	No	No
Network scan	Access right for starting/stopping the scan	Yes	Yes	No
Add device type	Access right for adding a new device type	Yes	Yes	No
Delete device type	Access right for deleting a device type	Yes	Yes	No
Topology - Reference	Working in the Reference editor	yes	No	No
Topology	Access to the display of the topology	Yes	Yes	Yes
User-specific views	Access to the display of user-specific views	Yes	Yes	Yes
Network list	Access to the display of the list of network devices	Yes	Yes	Yes
Reports	Access to the display of reports	Yes	Yes	Yes
Event statistics	Access to the display of network statistics	Yes	Yes	Yes
Events	Access to the display of the event list	Yes	Yes	Yes

Access right	Description	Administrator	Power user	Standard user
Event settings	Access to the display of the event settings	Yes	Yes	No
Change event settings	Access right for changing the event settings	Yes	Yes	No
Change network settings	Access right for changing the network settings	Yes	Yes	No
Catalogs	Access to the display of catalogs	Yes	Yes	No
Change catalogs	Access right for changing catalogs	Yes	Yes	No
Views	Access to the available views	Yes	Yes	Yes
Change views	Access right for changing views	Yes	Yes	No

How it works

Whenever a user wants to execute a command, SINEMA Server checks whether or not the user has the right to do this. The following individual points are checked:

- Which user group does the user belong to?
- Does the group have the required right?

3.6.2 Setting up users and user groups

Logging on the first time

After you first log in to the system, a dialog box appears with options for changing the password.

Note**Change password**

Change the password after you log in to the application the first time.

Login data - default settings

SINEMA Server provides a default combination of user name and password for the three predefined user groups. When you first log in to the system, the following combinations of user name and password are available for these predefined user groups:

User group	Login data
Administrator	<ul style="list-style-type: none">• User name: Administrator• Password: SinemaA
Power user	<ul style="list-style-type: none">• User name: Coordinator• Password: SinemaP
Standard user	<ul style="list-style-type: none">• User name: Operator• Password: SinemaS

Note

Predefined users and user groups cannot be deleted or modified.

Principle

1. When necessary, create new user groups. (See also section Administration - User Groups (Page 192))

You then need new user groups to be able to assign functions that differ from the default settings.

2. Create new users. (See also section Administration - User User (Page 189))

When necessary, you can also assign views to the users. The Web interface of SINEMA Server then behaves according to the specific views in terms of the event list and the selection of views.

Program functions - reference section

4.1 Program user interface in detail - overview of the menus

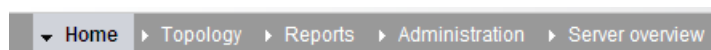
4.1.1 User interface

This section provides you with an overview of the following:

- Menu commands with a brief explanation and references to other sections
- General functions for setting the page layout and for navigation within a Web page

Menu commands

The navigation bar has the following menu commands that are explained below



Menu command Topology >...	Meaning	See section
...Discovered	Shows the network - devices and topology - in the way SINEMA Server has independently calculated it based on the discovered device data.	Topology - Discovered (Page 119)
...Monitored	Shows you the current status of the network based on the desired status specified in the reference topology.	Topology - Monitored (Page 126)
...Reference	Starts the Reference editor. With this tool, you configure the reference topology, i.e. the desired status of the network.	Topology - Reference (Page 132)

Menu command Reports >...	Tab	Meaning	See section
...Availability >	Devices	Display of all devices with information relating to their availability; in other words, how long they were reachable during the monitoring period.	Reports - Availability (Page 152)
	Interfaces	All the interfaces of the devices are displayed individually.	

4.1 Program user interface in detail - overview of the menus

Menu command Reports >...	Tab	Meaning	See section
...Performance >	LAN - Interface utilization	For all LAN interfaces, not only the possible speed but also their total load when sending and receiving is displayed.	Reports - Performance (Page 154)
	LAN - Interface error rate	The error quota when sending and receiving is displayed for all LAN interfaces.	
	WLAN - Interface error rate	The error quota when sending and receiving is displayed for all WLAN interfaces.	
	WLAN - Interface data rate	The transmission speed when sending and receiving is displayed for all WLAN interfaces.	
	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.	
...Inventory >	Vendor	Overview of the devices according to the manufacturer identifier.	Reports - Inventory (Page 155)
	IP address range	Overview of the devices according to IP address ranges.	
	Device category	Overview of the devices according to device types (switch etc.)	
...Events >	Network events	Display of all the events that have occurred with information relating to the status, event type and the time the event occurred.	Reports - Events (Page 156)
	System events		

Menu command Administration >...	Tab	Meaning	See section
...Discovery >	Scan	Here, you set the parameters for the network scan and start the scan.	Administration - Discovery / Scan (Page 162)
	Profiles	You can edit displayed profiles or add new profiles.	Administration - Discovery / Profiles (Page 165)
...Network >	Time settings	Set the time parameters for the network monitoring.	Administration - Network Time settings (Page 173)

4.1 Program user interface in detail - overview of the menus










Menu command	Tab	Meaning	See section
Administration >...	SNMP settings	Basic settings for discovery using the SNMP protocol.	Administration - Network SNMP (Page 174)
	Event reactions	Define view-specific, system- and device-specific reactions to events.	Administration - Network Event reactions (Page 174)
	Polling groups > Fast / Medium / Slow	Depending on the requirements, assign the devices to the 3 possible polling groups.	Administration - Network Polling groups (Page 178)
...Unmanaged devices		Manage devices that provide no or little opportunity for changing the way they work or the device data.	Administration - "Unmanaged" device types (Page 181)
...Event types >	Traps	Configure traps and events	Administration - Event types (Page 183)
	Network events		
	System events		
...OPC		Select devices whose data will be sent to an OPC server.	Administration - OPC (Page 187)
...User >	User	Assign users to groups and views.	Administration - User User (Page 189)
	Groups	Create user groups with rights.	Administration - User Groups (Page 192)
	Change password	Standard functions for managing the password	Administration - User Change password (Page 193)
...User interface		Here, you specify the interval for refreshing the monitored topology.	Administration - User interface (Page 194)
...System information		Display information about the management station	Administration - System information (Page 194)
...System configuration		Functions for saving, importing or resetting the configuration data of SINEMA Server.	Administration - System config (Page 195)

General functions for the page layout

In a series of Web pages, there are functions available in the footer with which you can specify 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:

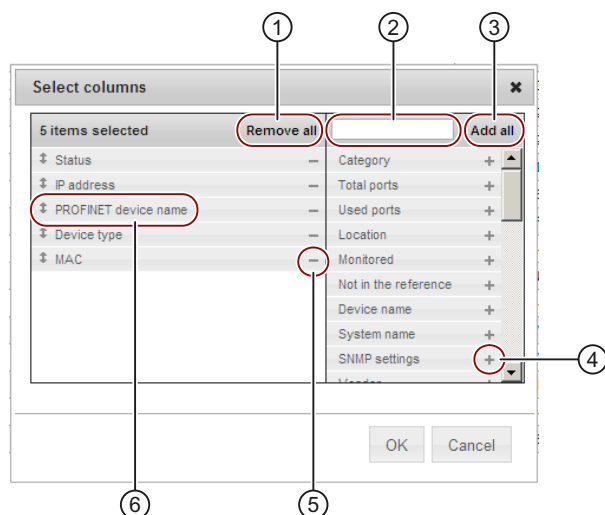
4.1 Program user interface in detail - overview of the menus

Icon	Display / function	Icon	Display / function
	Select and position columns for display.		Save column layout (content, width). Saving is user-specific.
	Select saved column layout.		Select default column layout
	Export table in CSV format		Scroll to the top of the table.
	Go back one page.	<input data-bbox="807 562 935 600" type="text" value="Page 1"/>	Display the current page and option to scroll directly to specific page.
	Go forward one page.		Scroll to the bottom of the table.
<input data-bbox="161 674 233 712" type="text" value="25"/>	Specify how many rows to display per page.		

General functions for the table layout

In a series of Web pages, information is shown in the form of a table. SINEMA Server 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 remove an individual column from the table.

⑤ Select "+" to add a individual entry as a column in the table

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

Selecting entries in tables

The first column of every table contains a check box. This check box is available in the header as well as in every row of the table.

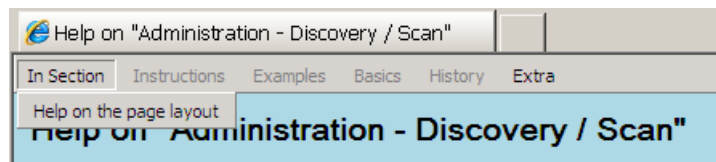
Follow the steps outlined below to select table entries:

- **Select single entry**
Click the check box in the table row. You can use this to select an individual entry and deselect other selected entries.
- **Select multiple entries (range)**
Holding down the shift key, click the check box of the first and last entry in the contiguous table range.
- **Select separate multiple entries**
Holding down the Ctrl key, click the check box of the required entry.
- **Select all entries**
Click the check box in the header.
- **Deselect single entries**
Holding down the Ctrl key, click the check box of the selected entry.

Online help


With the help icon in the status bar, you open the online help for the currently active Web page in a separate Web window.

The open online help has further menu commands in the header for navigation.



4.1.2 Quick links

Meaning

With the "Quick links" function element, you have fast access to SINEMA Server Web pages you require often. 

You can assign quick links for all standard Web pages and for view-specific Web pages.


Setting up a quick link

To assign quick links for Web pages and to specify a start page for SINEMA Server, follow the steps below:

1. Select the Web page you want to open using a quick link.
2. Select the "Quick links" function element
You open the list of available quick links.
3. Click the "New" button
This opens the "Quick links" dialog and the menu command of the currently displayed Web page is shown.
4. Assign a name for the Web page that you would like entered in the list of quick links.
5. If necessary, click the "Start page" button.

Using a quick link

To call up a Web page of SINEMA Server directly, follow the steps below:

1. Select the "Quick links" function element 
You open the list of available quick links.
2. Double-click on the required quick link.
You open the Web page.

4.1.3 Calling functions with a URL

Overview

You can call up certain functions of SINEMA Server in the Web browser by specifying the URL directly and adding the login data. In this case, you do not need to log in with SINEMA Server first. The login is made in conjunction with the call for the relevant Web page.

By specifying the URL, you control the following properties:

- the call for a specific Web page
You will find the available URLs in the following description.
- the authentication

Authentication - logging in with SINEMA Server

Requirement for access

- SINEMA Server must be running on the management station that is addressed using the URL.
- To have direct access to SINEMA Server using the URL, you need to be a member of a user group with the "Server access via URL" access right.

In the URL, enter the user name and the user-specific password. This entry is case sensitive.

You have the following options for logging in:

- You first send a separate call for the login. SINEMA Server then opens a session with the logged in user. After this, you can enter other URLs without needing to enter the login data again.

Example:

– "https://150.25.10.145:443?username=johndoe&password=hello123"

with the following significance:

IP address = 150.25.10.145

Default port = 443

Login = username=johndoe&password=hello123

- You send the login data when you call a Web page. For an example, refer to the following section "Navigation"

NOTICE
Recommendation
When entering the login data, we strongly advise you to use the HTTPS protocol.

Navigation - calling up a Web page

The Web pages listed in the following table can be called either with or without additionally entering login data. You can also select whether or not the Web page displays only the main window or also the device list, events list and navigation display in the header.

Example:

"https://sinemaserver:8080?path=network_discovered&
ip=192.168.110.34&username=john&password=blue&contentarea=yes"

The IP address needs to be included in the URL in the following situations:

- If the device details of a specific device should be included
- If you want a specific device to be displayed after the topology display is opened.

Table 4- 1 Parameters for the URL call

Parameter	Meaning
username	Name of the user logging in
password	User-specific password
path	Path of the SINEMA Server Web page to be displayed.
contentarea	Specifies whether or not only the SINEMA Server main window is displayed. YES = only the main window is displayed.

Web pages

The following table lists the Web pages available using a URL.

Path	called Web page / corresponding menu command in the Web client
path=mnu_network_actual	Topology > Discovered
path=mnu_network_actual&ip={ip}	Topology > Discovered Highlights the device selected with the IP address.
path=mnu_network_reference	Topology > Reference
path=mnu_network_reference&ip={ip}	Topology > Reference Highlights the device selected with the IP address.
path=mnu_network_monitoring	Topology > Monitored
path=mnu_network_monitoring&ip={ip}	Topology > Monitored Highlights the device selected with the IP address.
path=views_tabs¶ms=views_{view name}	Shows the named user-specific view. The device list is displayed.
path=views_tabs¶ms=views_{view name}&tabname=views_topology	Shows the named user-specific view. The view-specific topology is displayed.
path=device_list¶ms=alldevices_ip Address	Device list with devices that have the specified IP address.
path=device_list¶ms=alldevices_p rofinet	Device list with devices that have the specified PROFINET device name.

4.1 Program user interface in detail - overview of the menus

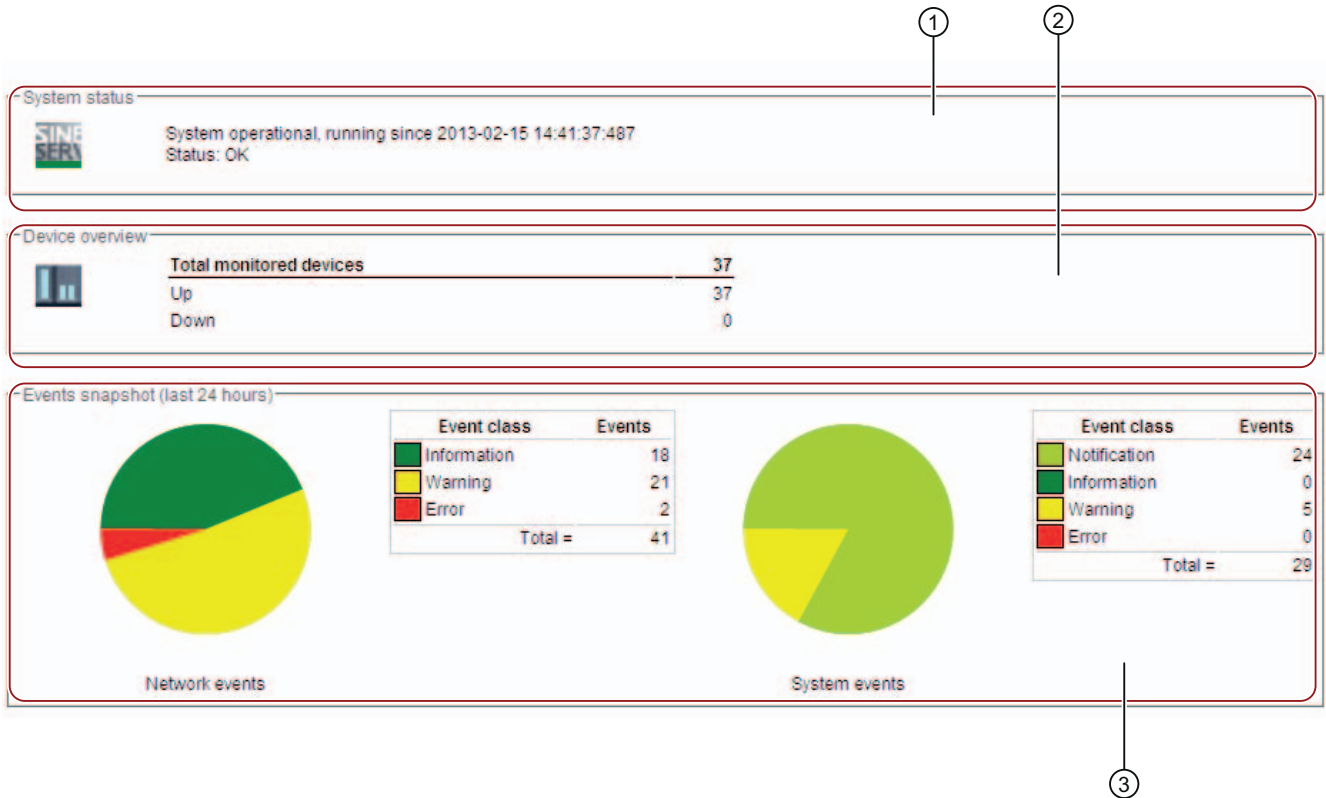
Path	called Web page / corresponding menu command in the Web client
path=device_list¶ms=device_type_WLAN Client	Device list with devices of the WLAN category
path=device_list¶ms=device_type_Others	Device list with devices of the "Others" category
path=device_list¶ms=device_type_Gateway	Device list with devices of the "Gateway" category
path=device_list¶ms=device_type_Switch	Device list with devices of the "Switch" category
path=device_list¶ms=device_type_Access Point	Device list with devices of the "Access point" category
path=device_list¶ms=device_type_End Device	Device list with devices of the "End device" category
path=device_list¶ms=overallstate_Ok	Device list with devices with the "OK" status
path=device_list¶ms=overallstate_fault	Device list with devices with the "Fault" status
path=device_list¶ms=overallstate_Maintenance demanded	Device list with devices with the "Maintenance demanded" status
path=device_list¶ms=overallstate_Maintenance required	Device list with devices with the "Maintenance required" status
path=device_list¶ms=overallstate_Not reachable	Device list with devices with the "Not reachable" status
path=device_list¶ms=vendor_Siemens AG	Device list with devices of the "Manufacturer / Siemens AG" category
path=device_list¶ms=vendor_Microsoft	Device list with devices of the "Manufacturer / Microsoft" category
path=device_list¶ms=vendor_Cisco Systems	Device list with devices of the "Manufacturer / Cisco systems" category
path=device_list¶ms=vendor_Unknown	Device list with devices of the "Manufacturer / Unknown" category
path=device_details&ip={ip address}	Details of the device with the specifies IP address
path=device_details&ip={ip address}&tabname=summary	Device details in the "Summary" tab
path=device_details&ip={ip address}&tabname=status	Device details in the "Status" tab
path=device_details&ip={ip address}&tabname=desc	Device details in the "Description" tab
path=device_details&ip={ip address}&tabname=settings	Device details in the "Settings" tab
path=device_details&ip={ip address}&tabname=lan	Device details in the "LAN port" tab
path=device_details&ip={ip address}&tabname=wlan	Device details in the "WLAN" tab
path=device_details&ip={ip address}&tabname=events	Device details in the "Events" tab
path=device_details&ip={ip address}&tabname=vlan	Device details in the "VLAN" tab

4.1 Program user interface in detail - overview of the menus

Path	called Web page / corresponding menu command in the Web client
path=device_details&ip={ip address}&tabname=redundancy	Device details in the "Redundancy" tab
path=device_details&ip={ip address}&tabname=interfaces	Device details in the "Interfaces" tab
path=device_details&ip={ip address}&tabname=expert	Device details in the "Expert" tab
path=events	Event list
path=mnu_server_overview	Server overview

4.1.4 Start window

You open the Web page using the menu command: **"Begin"**



- ① System status
- ② Device overview
- ③ Event overview - grouped according to network events and system events

Layout

The start window of SINEMA Server provides a quick overview of the status of the network. Information on the availability of the devices and statistics of the last event are supplemented by general information about SINEMA Server.

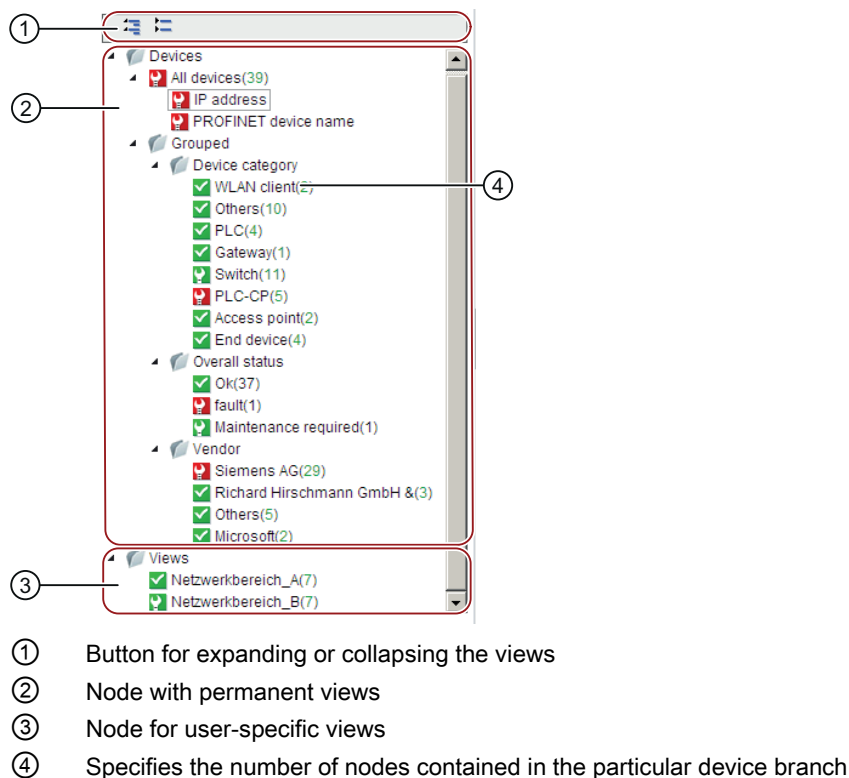
Operation / content

The start window provides the following information:

- ① System status
Information about how long (date and time) the SINEMA Server has been running.
- ② Device overview
Displays the number and status (active, inactive) of the monitored devices.
- ③ Events snapshot
Overview of the number and type (error, warning, information, display) of unacknowledged events, divided into network and system events.

4.1.5 Device tree

The device tree shows all the devices in the network as an overall list or grouped according to various properties (type, vendor).



Layout

- "Devices" node with permanently available views






The device tree allows you to view all the devices in the network as a single list or grouped by various properties (type, manufacturer).

- "Views" node with views set up specifically

For certain purposes, you can define user-specific "Views" that include only some of the existing devices or only part of the overall network. For more detailed information on this topic, refer to the section "Setting up and using views (Page 73)".

Status information

In the device tree, you have an overview of the statuses 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.

Icon for the status	Description
	Device status: In operation Meaning here: applies to all devices in the relevant branch.
	Device status: In operation - Maintenance required Meaning here: applies to at least one device in the relevant branch.
	Device status: In operation - Maintenance demanded Meaning here: applies to at least one device in the relevant branch.
	Device status: Error Meaning here: applies to at least one device in the relevant branch.
	Device not reachable Meaning here: applies to at least one device in the relevant branch.

4.1.6 Device window

Status	IP address	PROFINET device name	Device type	MAC
<input type="checkbox"/>	172.16.1.23		DEFAULT_ICMP_Device	84:85:06:2C:F4:14
<input type="checkbox"/>	172.16.1.201		DEFAULT_ICMP_Device	00:1B:1B:41:69:8F
<input type="checkbox"/>	172.16.50.23	petra	CP 343-1 Adv (1GX30-0XE0)	00:0E:8C:D6:3C:9D
<input type="checkbox"/>	172.16.50.64	Paulchen	SCALANCE X224 (0BA00-2AA3)	00:0E:8C:8B:6C:60
<input type="checkbox"/>	172.16.1.1		DEFAULT_ICMP_Device	00:1F:3F:CB:78:AF
<input type="checkbox"/>	172.16.1.4	Testrack2	SCALANCE_W788_AP_11abg	08:00:06:93:CF:6C
<input type="checkbox"/>	172.16.50.4		DEFAULT_SNMP_Device	00:30:05:C8:2A:F4
<input type="checkbox"/>	172.16.50.5		Management Station	00:19:99:80:5E:38
<input type="checkbox"/>	172.16.50.6	sinemaserverv11	DEFAULT_SNMP_DCP_Device	00:0E:8C:B3:F2:31
<input type="checkbox"/>	172.16.50.10	Andi	SCALANCE X414-3E (3FC00-2AA2)	08:00:06:93:EB:D5
<input type="checkbox"/>	172.16.50.11	Nico	SCALANCE XR324-12M (0GG00-1AR2)	00:0E:8C:C0:B8:85
<input type="checkbox"/>	172.16.50.12	joerg.mac-00-0E-8C-8B-C3-8F	SCALANCE_X300	00:0E:8C:8B:C3:8F
<input type="checkbox"/>	172.16.50.15	Chen	SCALANCE X208 (0BA10-2AA3)	00:0E:8C:8F:14:F7
<input type="checkbox"/>	172.16.50.16	Siggi	SCALANCE X201-3P IRT (3BH00-2BA3)	08:00:06:9C:70:BB
<input type="checkbox"/>	172.16.50.17	Michael	SCALANCE X202-2P IRT (2BH00-2BA3)	00:0E:8C:81:79:14

- ① Header with toolbar
- ② Device list with status display and configurable columns
- ③ Footer with setting functions and configuration limits

Display

You can open the device window of SINEMA Server by selecting an item in the device tree. Depending on the item you select, all devices or only a certain group are displayed.

Operation / content











The device window is 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.

Using the footer function "Select columns for display", the following information is available:








4.1 Program user interface in detail - overview of the menus

- Device status
- IP address
- PROFINET device name
- MAC address
- Total ports
- Used ports
- Deployment / installation location
- Monitored (yes / no)
- Not in the reference (yes / no)
- Device name
- System name
- SNMP settings (name)
- Manufacturer
- Order number
- First discovered
- Last discovered
- Remark
- Operating system
- C-plug (available?)
- Number of LAN ports
- Redundancy mode
- Redundancy status
- Standby mode
- Standby status
- Reachability
- SNMP reachability
- DCP reachability
- Uptime
- Firmware version
- Hardware version
- Automation name
- Contact person
- SINEMA Server trap recipient (yes / no)
- Device family
- Assigned profile
- Assigned monitoring profile
- Statistical attachment data read in (yes / no)

The following table shows the functional elements of the header.

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 SNMP values of the device are read out again. Note: This icon can be clicked any number of times in succession. A request within 2 minutes of the last request is, however, ignored. This avoids increased network traffic. You should therefore wait longer than two minutes before clicking the icon again.		Add or change comment
	Delete remark		Enable monitoring
	Turn off monitoring		Create new device
	Delete device After it is deleted, the device only continues to exist in the report archive.		Specify SNMP settings

4.1 Program user interface in detail - overview of the menus

Icon	Display / function	Icon	Display / function
	<p>Change device type</p> <p>Opens the "Set device type for" dialog in which a different device type can be assigned using the available profiles.</p> <p>DCP can also be enabled and the SNMP settings changed.</p>		<p>Change monitoring settings</p> <p>Opens the "Set monitoring profile for" dialog</p> <p>If necessary you can use this method to assign a monitoring profile to the device in addition to the general profile.</p>
	<p>Customize device data</p> <p>The "Adapt device" dialog opens. Here, you will find the following tabs for further entries:</p> <ul style="list-style-type: none"> User-defined links <p>When necessary, you can store links (URL) to further information that is useful in conjunction with monitoring the device.</p> <ul style="list-style-type: none"> Basic data 		<p>Set device basic data</p>
	<p>Enter text for device scan / filter setting</p>		<p>Start device scan / filter setting</p> <p>Result: The devices that match the text string specified for the text search are displayed.</p>
	<p>Select filter for display</p>		

See also

User interface (Page 89)

4.1.7 Device details

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

Gerätedetails (172.16.50.6/SINEMASERVERV11)

Zusammenfassung | Status | Beschreibung | Einstellungen | LAN-Anschlüsse | Ereignisse | Schnittstelle | Experte

Benutzerdefiniert

OK

Gerätebezeichnung

IPv4-Adresse	172.16.50.6	Name	SINEMASERVERV11
Gerätekategorie	Others	Gerätetyp	DEFAULT_SNMP_DCP_Device
MAC	00:0E:8C:B3:F2:31	Einsatzort	Microbox 427C

Unbestätigte Alarme

Fehler	0	Warnungen	0
Informationen	0		

Anmerkungen

-

Display

You can call up the "Device details" window in the following ways:

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

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. The registers that can be used depends on the device type.

4.1 Program user interface in detail - overview of the menus

Operation / content

The following table shows the tab contents of the "Device Details" window with a brief explanation.

Table 4- 2 'Summary' tab

Parameter group	Display, content
-	Device icon and status
Device name	IPv4 address, name, device category and type MAC and location
Unconfirmed alarms	Number of errors, warnings and information
Remarks	Comments, information

Table 4- 3 'Status' tab

Parameter group	Display, content
-	Overall status
Reachability	Polling group, ping status, PROFINET IO / DCP status and SNMP status
Status details	Operating state
Summary LAN ports	Total number of ports, used, active and inactive (differing from reference), as well as with a critical behavior
Times	Information, when <ul style="list-style-type: none"> • 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- 4 'Description' tab

Parameter group	Display, content
Names	PROFINET IO, system and automation name
Location	Location according to system and automation
Identification and maintenance	Order number, serial number, vendor ID and name, firmware version, hardware revision, DCP-ID
Manual changes	Manually created, migrated, device type changed?
User-defined links	Display of links 1 to 3, if entered You enter links using the "Customize device data" function, see section Device window (Page 102)
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
Miscellaneous	Contact person and OPC name

Table 4- 5 'Settings' tab

Parameter group	Display, content
Ethernet	IPv4 address, router address (standard gateway), device MAC address, subnet mask and DHCP (enabled?)
Profinet	PROFINET IO status (online / offline), PNIO name and type
SNMP settings	Configuration name, traps enabled, SINEMA Server trap recipient (yes / no)
General SNMP traps	Information about whether the following traps were enabled: <ul style="list-style-type: none"> • Connection establishment and termination • Warm and cold restart • Authentication failed
Miscellaneous	Radius server address; IP forwarding (yes / no)

Table 4- 6 'LAN ports' 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 in the same way as the device window (Page 102) (column width, export etc.). There are icons available above the table with following functions: <ul style="list-style-type: none"> • Show attachment details (see section "Detailed information LAN attachments") • Enabling connection statistics • Disabling connection statistics

Table 4- 7 'WLAN' tab

Parameter group	Display, content
-	Table of all WLAN interfaces with index, name, status, SSID and information about critical statuses. The content of the table corresponds to the "LAN ports" tab. For more detailed information, the "Open port details" icon is available (see section "Detailed information WLAN attachments").

4.1 Program user interface in detail - overview of the menus

Table 4- 8 'Events' tab

Parameter group	Display, content
-	<p>Table of all reported events with name, status, timestamp, status and other arbitrary information. The entire table can be formatted and used in the same way as the device window (Page 102) (column width, export etc.).</p> <p>There are icons available above the table with following functions:</p> <ul style="list-style-type: none"> • Acknowledge event • Add / edit remark • Delete remark • Set filter for display (status, time, type)

Table 4- 9 '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 of both selected and unselected attachments.

Table 4- 10 'Redundancy' tab

Parameter group	Display, content
-	<p>Table of all employed redundancy mechanisms with associated interfaces, protocol used, status, role (manager or client) as well as supplementary information.</p> <p>For more detailed information, the "Open port details" icon is available (see section "Detailed information redundancy attachments (Page 102)").</p>

Table 4- 11 'Expert' tab

Parameter group	Display, content
-	<p>Multi-page list of all information, as read unchanged (not translated or documented) from the device's internal memory (MIB). Shows parameters (name), OID and value.</p> <p>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.</p>

Table 4- 12 'Custom' 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.

With the shortcut menu, you can start the following actions in all tabs:

- Open WBM
- Reread data
- Disable automatic data refresh
- Add current window to quick links

See also


Device window (Page 102)

4.1.8 Device details - subcategories

4.1.8.1 Detailed information LAN ports

Opening the display

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

Operation / content

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


Group	Display, content
Basic data	<ul style="list-style-type: none">• Name of the port (e.g. P1 or X5P1)• Interface index (unique number of the port)• MAC address (not only the device itself but each port also has its own unique MAC address)• Transmission medium (copper or optical)• Status (active or inactive)• Admin status• Max. transmission speed (Mbps)• Mode (full duplex or half duplex)• Description
Topology	<ul style="list-style-type: none">• Device connections (which device is there a connection to?)• Port connections (which port is there a connection to?)
Data traffic	<ul style="list-style-type: none">• Transmit (transmission speed in Mbps)• Receive (receive speed in Mbps)
Utilization	<ul style="list-style-type: none">• Transmit utilization FD (degree of utilization as a percent with full duplex)• Transmit utilization FD (degree of utilization as a percentage with full duplex)• HD combined utilization (combined degree of utilization as percentage with half duplex)

Group	Display, content
Error rate	<ul style="list-style-type: none"> FD Transmit error rate (error rate as a percentage with full duplex) FD Receive error rate (error rate as a percentage with full duplex) HD Combined error rate (combined error rate as percentage with half duplex)
Miscellaneous	What is the starting point for saving the port data for statistical purposes?

4.1.8.2 Detailed information WLAN

Opening the display

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

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

Operation / content


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

Group	Display, content
Basic data	<ul style="list-style-type: none"> Name of the port (e.g. R1) Description Interface index (unique number of the port) Authentication type (e.g. WEP or WPA2-PSK) SSID (names of the WLANs (wireless networks) to which the interface belongs) BSSID (ID numbers of the WLANs to which the interface belongs) Mode (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	<ul style="list-style-type: none"> Status (up or down) Signal strength (strength of the wireless signal in dBm) Transmit data rate (transmit speed in Mbps) Receive data rate (receive speed in Mbps) Transmit error rate (error rate as a percentage) Receive error rate (error rate as a percentage) Number of clients
Clients	<p>Table of all clients connected to the interface. Per client, the following information can be displayed:</p> <ul style="list-style-type: none"> 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 (transmit speed in Mbps) Receive data rate (receive speed in Mbps) Transmit error rate (error rate as a percentage) Receive error rate (error rate as a percentage) Critical performance (information as to whether or not the existing connection needs to be considered critical) Signal (signal strength of the existing connection in dBm) Signal state (indicates whether the signal strength is OK, low or high)

4.1.8.3 Detailed information redundant ports

Opening the display

The details window for redundant ports can be opened 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

Operation / content

Depending on the redundancy method (protocol) being used, different information is displayed. The following table shows the possible content with a brief explanation.

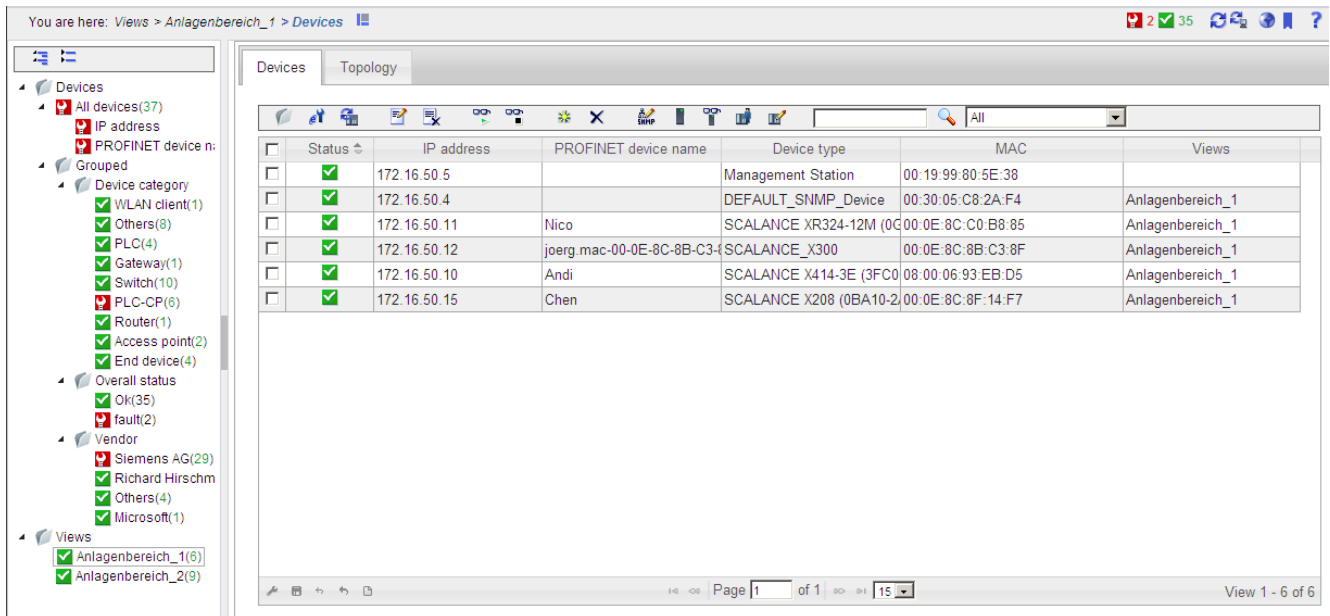
Protocol	Group	Display, content
HSR	Basic data	<ul style="list-style-type: none"> • Name of the port (e.g. X5P1) • Role (what is the task (client, master) of the interface within the ring?) • Port state (information about what the interface does with IP packets . forward or block)
	Redundancy manager	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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) • Domain name
	Redundancy manager	<ul style="list-style-type: none"> • 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) • Time ticks since • Domain error

4.1 Program user interface in detail - overview of the menus

Protocol	Group	Display, content
STP or RSTP	-	<ul style="list-style-type: none"> Name of the port (e.g. X0P5) Port type Port state (up or down) 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 (numeric value; the higher the priority, the more important the connection --> priority for transport of the data packets) No 'Forward transmissions'
Standby	Basic data	<ul style="list-style-type: none"> 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).

4.1.9 Views

The following figure shows the layout and operator controls of the "Views" window, "Devices" tab. The design is almost identical to that of the "normal" Device window.



Opening a view

You can open the "Views" window of SINEMA Server by selecting the item with this name in the device tree or one of its lower-level items.

The "Devices" tab is always present, the "Topology" tab only if this has been configured accordingly (selected).

Note

The following describes views that may be available. To learn how these objects are created, modified or deleted, and the overall purpose of views, read the section "Monitoring and managing a network - using views (Page 73)".

Operation / content

The functionality of this window also corresponds exactly to that of the Device window. There is a slight difference in the content (column assignment): In this case, the default column "Views" is included in the display. It shows the views in which the corresponding device appears.

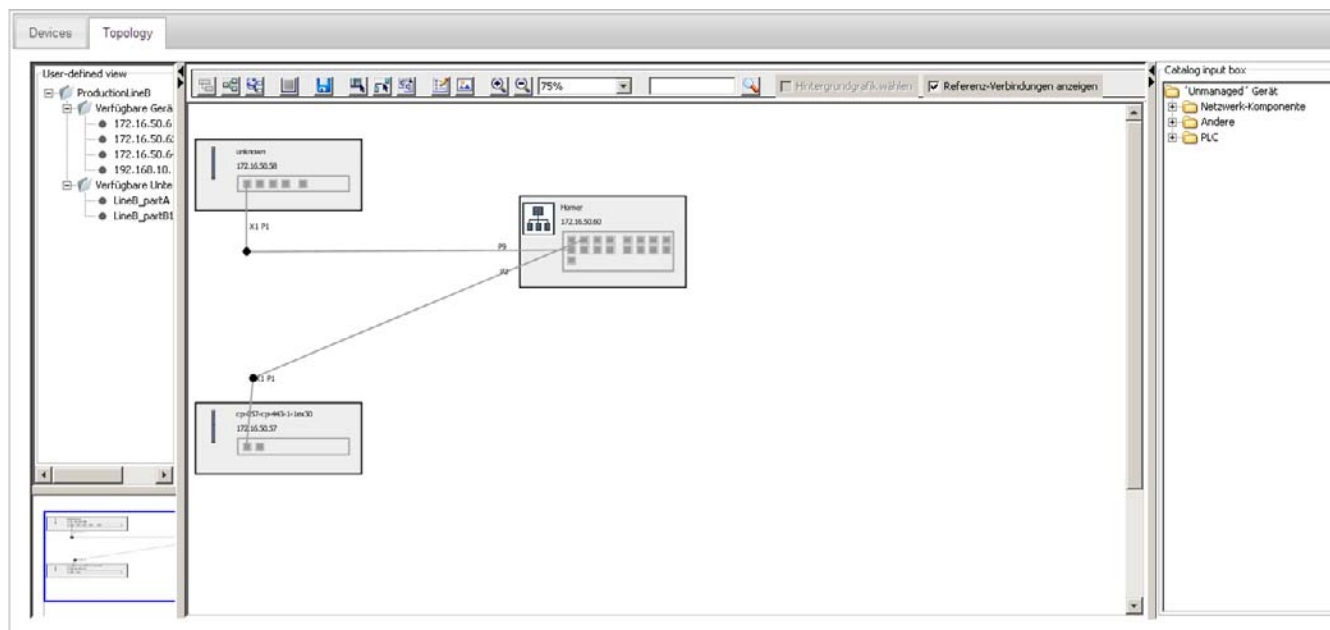
See also

Device window (Page 102)

Meaning and how it works (Page 132)

4.1.9.1 Views . topology

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



"Topology" tab - modes













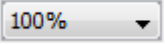


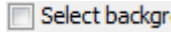
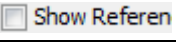
The operator options in this tab must be distinguished according to the selected topology display mode:

- Draft mode
- Active mode

Operation / content - in draft mode

In "Draft" mode, you specify the devices and connections of the network to be displayed and design the required view layout. In terms of functionality, it is very similar to the Reference editor and many of its tools and icons are also available here.

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Select detail view		Select icon view
	Recalculate topology		Change to active mode
	Save view details (draft)		Select selection mode This tool is enabled automatically when you open the page.
	Select draw mode		Create user-defined connections for all reference connections
	Configure node display		Insert background graphic Insert a background graphic and change its size.
	Enlarge display (zoom factor)		Reduce display (zoom factor)
	Select zoom factor		Input box for device scan (IP address)
	Start device scan		Select background graphic for further processing
	Show/hide reference connections		

In the data area you also have almost all the same options for opening shortcut menus with identical content as in the Reference Editor and starting further actions per mouse click or a double-click. For example "Device hierarchy" and "Bird's eye view" also are available here.

Note

Moving device icons freely

A special feature (compared with the Reference Editor) is that device icons can be freely moved and user-defined connections can be transformed in a variety of ways by moving the handles (•). This allows topologies to be represented clearly and individually.

Operation / content - in active mode



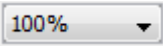


In the "active" mode, the devices and connections are displayed as specified in the draft layout. The display is however overlaid with colored identifiers and pictograms relating to reachability, connection status and detected properties.

In terms of functionality, it is very similar to the "Topology > Monitored" window and many of the same tools and icons are also available here.

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Select detail view		Select icon view
	Change to draft mode		Configure node display

4.1 Program user interface in detail - overview of the menus

Icon	Display / function	Icon	Display / function
	Enlarge display (zoom factor)		Reduce display (zoom factor)
	Select zoom factor		Input box for device scan (IP address)
	Start device scan		

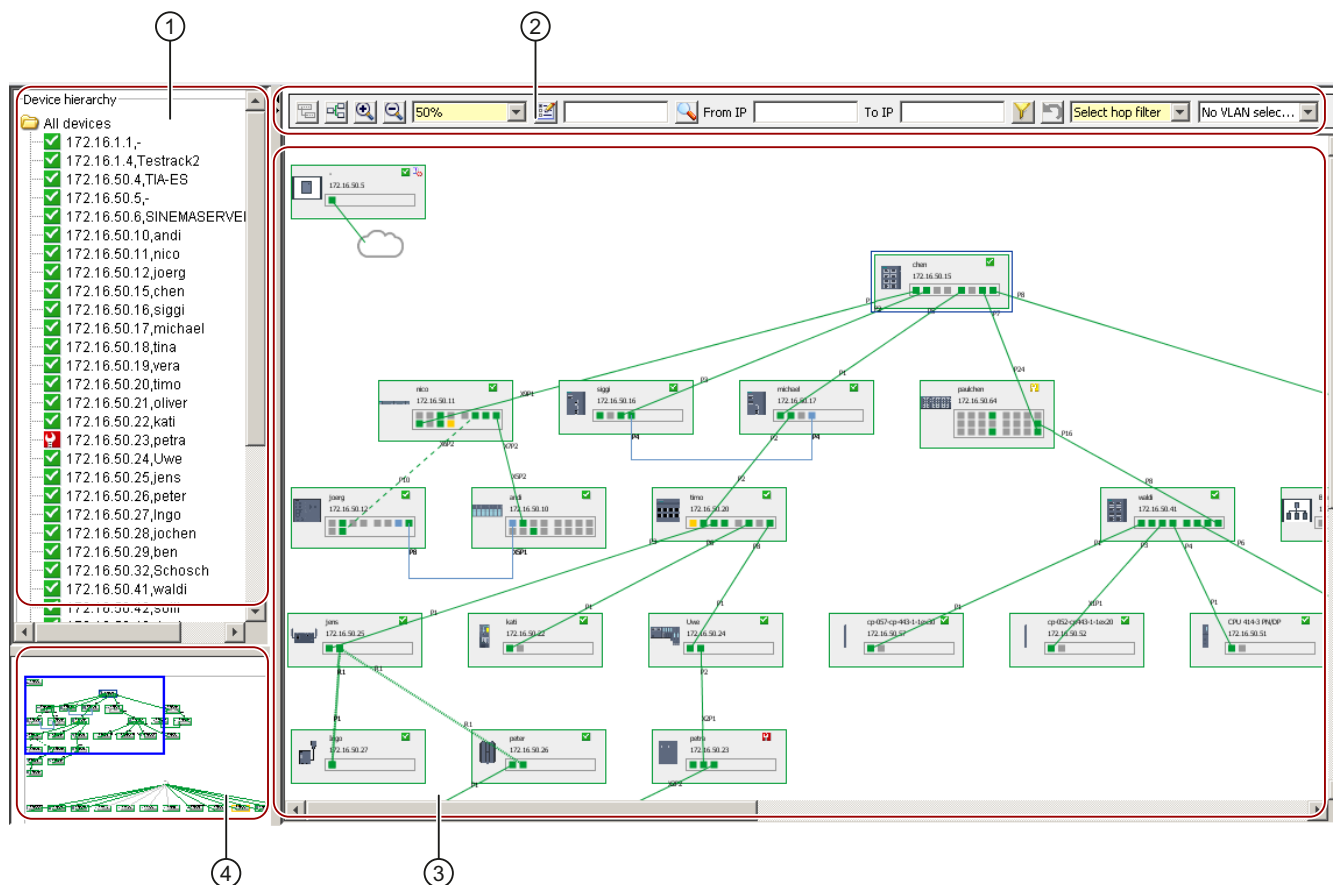
The functionality in the data area as well as in the "Device hierarchy" and "Bird's eye view " is almost identical to that of the "Topology > Monitored" window.

4.2 Topology

4.2.1 Topology - Discovered

4.2.1.1 Meaning and how it works

The functions described below are available with the menu command: **"Topology > Discovered"**



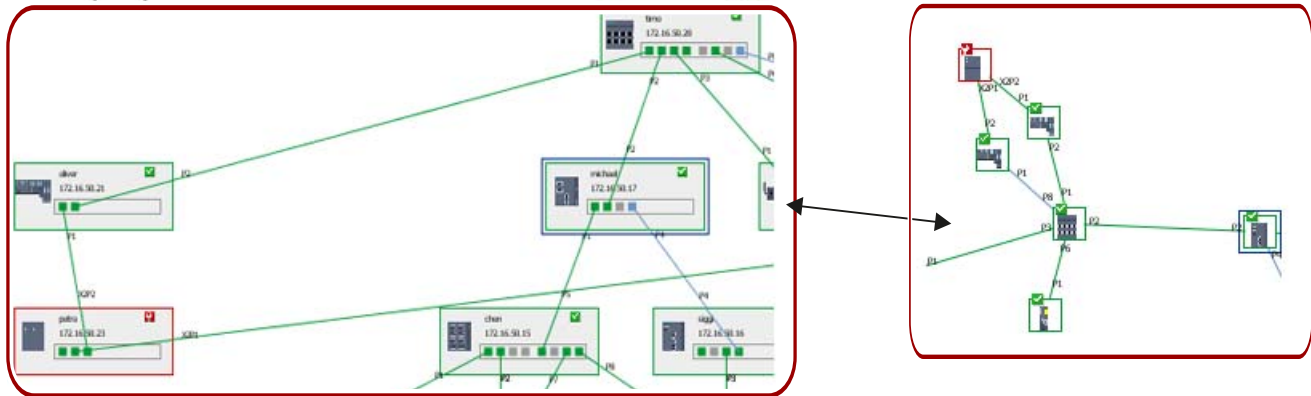
- ① Device viewing area
- ② Toolbar
- ③ Device hierarchy in the topology display
- ④ Overall view (bird's eye view) with sliding detail selector

Layout

The menu command **"Topology> Detected"** shows the network - devices and topology - in the way SINEMA Server has independently calculated it based on the detected device data. You can choose whether the topology is to be presented, as a detailed view or icon view.

4.2 Topology


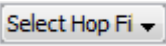

The following screenshots illustrate the basic differences between the detail view and icon view:



Operation / content

The following table explains the functions that are available on the toolbar:

Icon	Display / function	Icon	Display / function
	Select detail view		Select icon view
	Recalculate topology		Enlarge display (zoom factor)
	Reduce display (zoom factor)	<input type="text" value="100%"/>	Select zoom factor
	Configure node display Select the from the following options in the displayed dialog: <ul style="list-style-type: none"> • Basic settings <ul style="list-style-type: none"> – Port names • Device names <ul style="list-style-type: none"> – Name – IP address – Manufacturer – Category – Device notes – PROFINET device name – System name – Automation name From the device names, up to 2 entries can be selected.	<input type="text"/>	Input box for node scan Specify an IP address for the node scan. The found node is highlighted with a dotted frame.
	Start node scan	From IP <input type="text"/>	"From" text box for IP filter
To IP <input type="text"/>	"To" text box for IP filter		Activate IP filter

Icon	Display / function	Icon	Display / function
	Reset IP filter		Select HOP filter Select the number of hops to be shown in the topology starting from a network node. If no particular node is selected you will be prompted to select a node after selecting the filter setting.
	Select VLAN filter If the devices in your network structure have been assigned to a virtual network structure (VLAN), you can select these in the drop-down list of one of these VLANs. The corresponding devices are then highlighted in the topology.		

Filter settings

When making the filter settings, note the following information on the response

- Filter functions in general

The filter settings described in the table above can be put together in any combination.

- IP address filter

Nodes in the selected IP address range are displayed unchanged. Nodes not included in the IP address range are grayed out.

Other options

In addition, there are the following additional operating options:

- Mouse click on ► / ◀ (upper left, next to toolbar)

Open / close window with device hierarchy and bird's eye view.

- Right-click in the open window area

Open the shortcut menu with the following options:

- Enlarge view
- Reduce view
- Refresh view

- Right-click on device icon

Open the shortcut menu with the following options:

- Show device details
- Open WBM

4.2 Topology

- Double-click on device icon
Show device details
- Position the mouse pointer on device icon
The following information is alternatively shown:
 - Various device properties (IP, MAC, system name, PROFINET device name, etc.)
 - Interface properties (name, connection, status)
- Position the mouse pointer on connection line
Show information about connected devices
- Click a device icon or a connecting line
Name of the respective object.






4.2.1.2 Icons and colors in the discovered topology

Overview

The following sections explain the significance of the colors for devices, ports and connection lines in the discovered topology.

Devices











The color of the device is based on its general reachability. If a device is not visible in the view, the device status is shown grayed out.

Icon for the status	Description
	Device status: In operation Border color of the displayed device: green
	Device status: In operation - Maintenance required Border color of the displayed device: green
	Device status: In operation - Maintenance demanded Border color of the displayed device: yellow
	Device status: Error Border color of the displayed device: red
	Device not reachable Border color of the displayed device: red

The overall status of the device shown here depends on the partial statuses that can be configured in the profiles.

Ports / interfaces

The status or color of a connection has no effect on the port color. If a device is not visible, all ports are gray. If a device is not reachable, the port color is light gray.




























Color	Current connection exists	Description
	No	In operation or test
	No	In operation - Maintenance required
	No	Not in operation - Maintenance demanded
	No	Not in operation
	No	Unknown
	Yes	In operation or test
	Yes	In operation - Maintenance required
	Yes	Not in operation - Maintenance demanded
	Yes	Not in operation
	Yes	Unknown

Connection lines

The connection between the devices is shown by a line. If the connected devices are visible, the color of the connected ports decides the color of the connection line. If only one of the connected devices is visible, the port of the device that is not visible is not colored but the color of the connection line is based on both interfaces. The combinations of port colors and the conventions for the color of the connection line are explained below:




Port 1	Port 2	Color
		
		
		
		
		
		









4.2 Topology









Port 1	Port 2	Color
		
		
		
		
		
		
		
		
		

Connection types

The types of connection lines in the topology tree are classified according to the device type or the device category. Wireless connections, optical connections and electrical connections are shown in the detailed view as follows:

Connection type	Description
	Wireless connection
	Optical connection
	Electrical connection

Port 1	Port 2	Line type
Electrical	Electrical	
Electrical	Unknown	
Electrical	Optical	
Electrical	Wireless	
Optical	Electrical	
Optical	Unknown	
Optical	Optical	
Optical	Wireless	

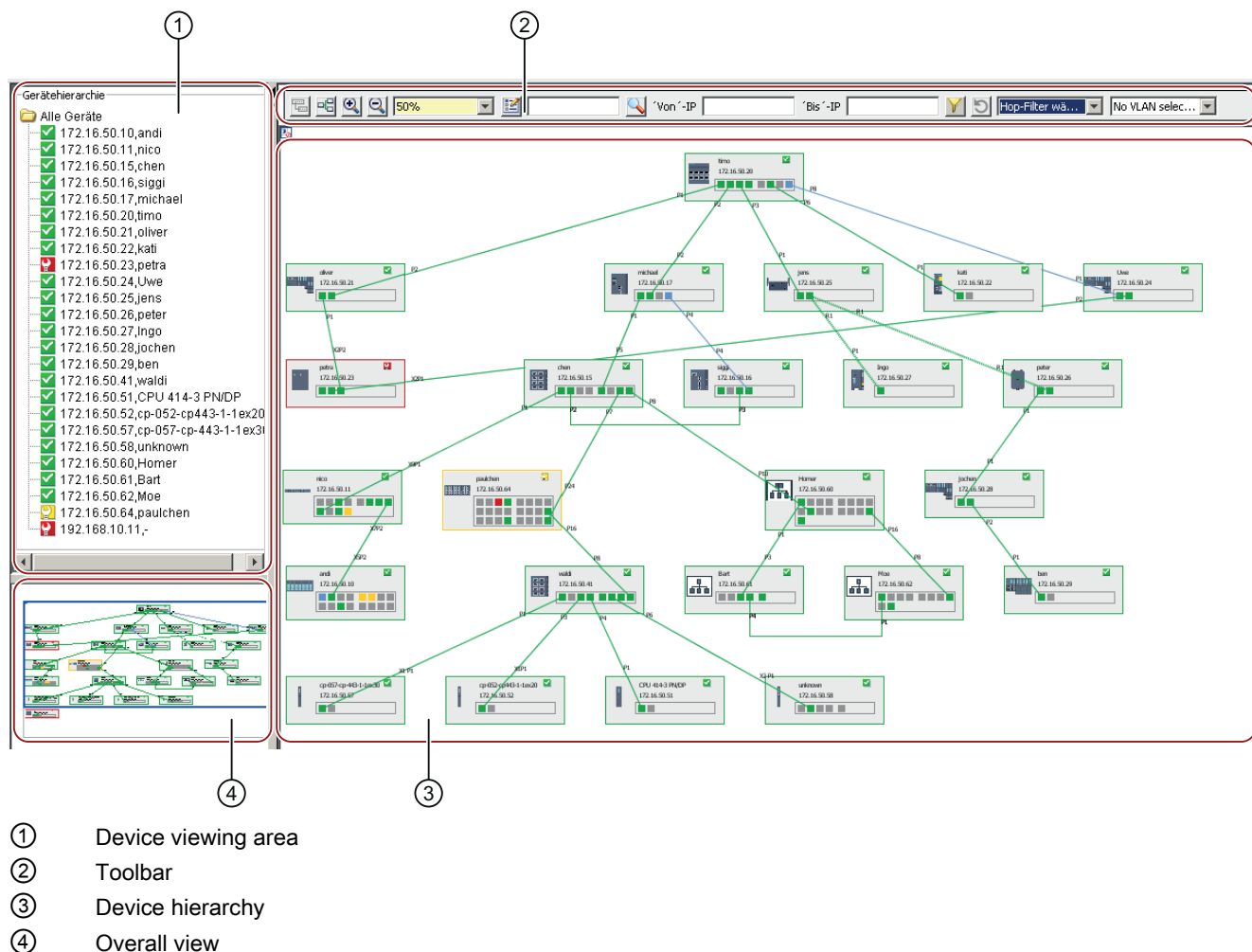
Port 1	Port 2	Line type
Wireless	Electrical	
Wireless	Unknown	
Wireless	Optical	
Wireless	Wireless	
Unknown	Electrical	
Unknown	Unknown	
Unknown	Optical	
Unknown	Wireless	

4.2 Topology

4.2.2 Topology - Monitored

4.2.2.1 Meaning and how it works

The functions described below are available with the menu command: **"Topology > Monitored"**



Layout

The menu command **"Topology> Monitored"** shows you the current status of the network based on the target status defined in the reference topology.

Note

SINEMA Server compares the current topology with the configured network. An display can therefore only occur if a reference network has been configured ("Topology > Reference").

The display options are similar to those of the "Topology > Detected" window.

Operation / content

The operability and functionality are also the same as those in the "Topology > Detected" window.

Note

In the monitored topology, the sub window of the device hierarchy includes the "All devices" folder that contains only the devices that are shown in the device view. The "Catalog window" of the unmanaged devices is shown in the detail view of the monitored topology.

Note

The toolbar contains the same icons as in the discovered topology. With "Monitored topology > Detail view", the "Create new topology" icon is, however, not available.

Shortcut menu

A shortcut menu is available in the device view area. To open this menu, right click on the device. Which options are displayed in the shortcut menu depends on the device selected in the device view area. The shortcut menu contains the following two options:

- Show device details
- Device-specific link

If you have not made a selection in the Topology editor, the shortcut menu is displayed if you right click in the device view area. The shortcut menu contains the following options:

- Enlarge
- Reduce
- Refresh

Purpose and use

To display the reference topology and its status, you must save the reference topology at least once in the Reference editor. When you save the reference topology in the Reference editor, the network devices are displayed along with the new devices added to this topology in the monitored topology.

4.2 Topology

The details view of the monitored topology shows both the monitored devices as well as the "unmanaged devices" inserted extra in the reference topology, if these exist. The color of these devices and ports depends on their current status. The color of the connection line, on the other hand, depends on the status of the connected ports. The topology also shows the network view starting from the SINEMA server station in a hierarchical structure.

Note

Refreshing the monitored topology to display the latest changes takes approximately 3 to 5 seconds. Since the automatic refresh is enabled in the monitored topology, the changes are displayed automatically following the next refresh of the user interface. To display the changes earlier, start a manual refresh by clicking the refresh button in the monitored topology.

4.2.2.2 Icons and colors in the monitored topology






Overview

The following sections explain the significance of the colors for devices, ports and connections in the monitored topology.

Status monitoring

The status changes of devices, ports and connections including WLAN connections are shown in various colors.

- **Device status**

Icon for the status	Description
	Device status: In operation Border color of the displayed device: green
	Device status: In operation - Maintenance required Border color of the displayed device: green
	Device status: In operation - Maintenance demanded Border color of the displayed device: yellow
	Device status: Error Border color of the displayed device: red
	Device not reachable Border color of the displayed device: red








- **Port / interface status:**

In the detailed view of the monitored topology, the color coding of the port status differs from that in the current topology. Each port shown in the monitored topology has two statuses: the actual status and the resulting status. This status is based on the comparison with the actual status and the reference status.





- The actual status is indicated by the border color of the port.
- The resulting status is indicated by the fill color of the port in the rectangle.

Note










In the monitored topology, a device that is not visible in the view is shown in gray. All ports of a device that is not reachable are displayed light gray with a gray border around the port. For this reason, all connections to other devices that cannot be reached are also shown in gray.

Port status	Fill color/border color
In operation	
In operation - Maintenance required	
Not in operation - Maintenance demanded <ul style="list-style-type: none"> • With current connection • Without current connection 	 
Not in operation <ul style="list-style-type: none"> • With current connection • Without current connection 	 
Unknown	

- Ring port

Redundancy status (device details)	Standby port status	Fill color/border color
Active	In operation	
Active	In operation - Maintenance required	
Active	Not in operation - Maintenance demanded <ul style="list-style-type: none"> With current connection Without current connection 	 

4.2 Topology

Redundancy status (device details)	Standby port status	Fill color/border color
Active	Not in operation With current connection Without current connection	 
Active	Unknown	
Passive	In operation	
Passive	In operation - Maintenance required	
Passive	Not in operation - Maintenance demanded With current connection Without current connection	 
Passive	Not in operation	
Passive	Unknown	

- **Status of the LAN connection**

The connection line in the monitored topology shows the connections of the reference topology. With LAN connections, the color is based on the fill color of the two connected interfaces.


















Fill color port 1	Fill color port 2	Connection color
Green	Green	Green
Green	Red	Red
Green	Light gray (unknown)	Green
Green	Light blue	Light blue (standby connection)
Red	Green	Red
Red	Red	Red
Red	Light gray (unknown)	Red
Red	Light blue (isolated)	Red
Light gray (unknown)	Green	Green
Light gray (unknown)	Red	Red
Light gray (unknown)	Light gray (unknown)	Light gray
Light gray (unknown)	Light blue (isolated)	Light blue (standby connection)
Light blue (isolated)	Green	Green
Light blue (isolated)	Red	Red
Light blue (isolated)	Light gray (unknown)	Green

- **Status of the WLAN connection**

Status of the reference connection - up	Line color / explanation
No	light gray
Yes	<p>The color of an active reference connection is based on the port color (green, red or light gray).</p> <p>light gray: The user has specified in the reference that a connection can exist.</p> <p>green: connection discovered as active by SINEMA Server.</p> <p>red: one of the interfaces belonging to the connection is down.</p>

- **Status of the active WLAN connection**

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.

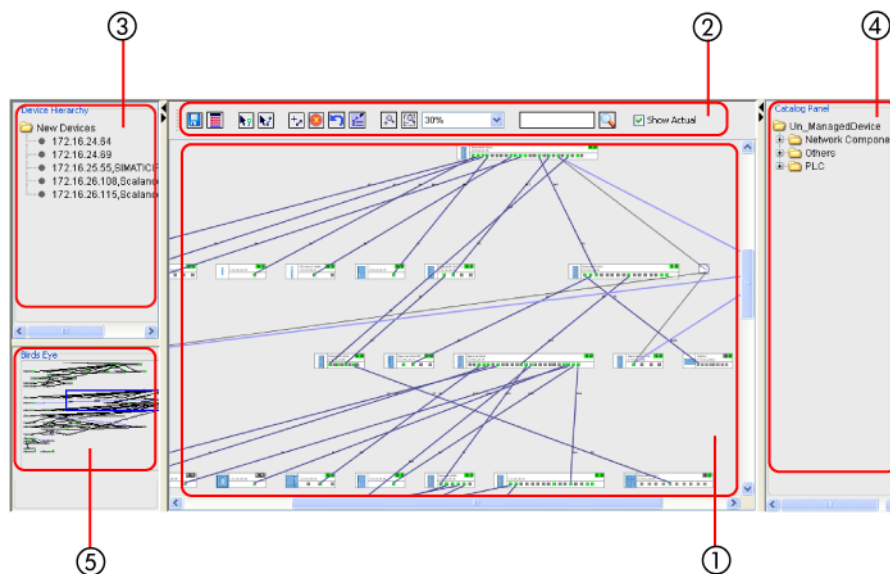
Port 1	Port 2	Color of the active connection between client and AP
		
		
		
		
		
		
		
		
		

4.2.3 Topology - Reference

4.2.3.1 Meaning and how it works

The functions described below are available with the menu command: **"Topology > Reference"**

The Reference editor consists of five individual views in which the complete information on the topology of the devices discovered in the network is displayed.



- ① Device editor - view area
- ② Toolbar
- ③ Device hierarchy (new devices)
- ④ Catalog window (unmanaged devices)
- ⑤ Overall view

Overview

You start the Reference editor with the menu command **"Topology > Reference"**. This tool enables you to configure the reference topology, i.e. the desired target state of the network.

The Reference editor provides a complete view of the reference topology with a refreshed topology in which the devices, ports and their connection status are displayed. In this editor, you can also edit connections, change the port status and configure protocols supported by the devices in the network.

A complete reference topology is always displayed. All monitored devices including the new devices are included in the editor view. Unmonitored devices are not shown in the editor. The views in the reference editor are shown below.

Note

SINEMA Server requires the reference for numerous functions. If you want to enjoy the full functionality of SINEMA Server, you therefore must configure a reference topology in advance.

Device editor - view area











In the Device editor view area, the topology tree with reference connections and the connections between the devices discovered in the network are displayed. The tree view contains the nodes, their connection lines and the corresponding port status of the current topology and reference topology.

The display of the Reference editor contains the topology information of all devices connected in the network. An unknown device is displayed as a cloud in the Reference editor. An icon and a text display box and port box can be assigned to each device node. As default, the device name and the device IP address are shown in the text display box.

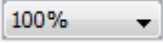


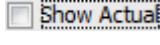
The connection lines in the Device editor view area have line numbers at both ends of the connection. This is identical for the connections in the current and in the reference topology. The protocols supported by every device are displayed in the right-hand corner of the text display field. The two protocol statuses "S" and "D" indicate the status of the SNMP and DCP reachability. A scored-through icon indicates that there is no protocol support available for the specific device.

Operation - toolbar

The following table explains the function elements of the toolbar.

Icon	Display / function	Icon	Display / function
	Save reference topology		Recalculate topology Note: During a refresh, the status of the topology layout is not changed.
	Select selection mode		Select draw mode
	Use current state as a reference		Reset reference topology Resets the changes in the reference view by discarding all changes made in the Reference topology editor.
	Discard last change		Configure node display
	Enlarge display (zoom factor)		Reduce display (zoom factor)

4.2 Topology

Icon	Display / function	Icon	Display / function
	Select zoom factor		Input box for node scan
	Start node scan		Control field for displaying the current connections

Operation - shortcut menus

By selecting objects in the view area, the following functions are available:

- Mouse click on ► / ◄ (upper left, next to toolbar)
Open / close window with device hierarchy and bird's eye view.
- Right-click in the open window area
Open the shortcut menu with the following options:
 - Enlarge view
 - Reduce view
 - Refresh view
 - Add cloud (icon for unknown device type or unknown network structure)
- Right-click on device icon
Open the shortcut menu with the following options:
 - Remove device
 - Add comment
 - Show device details
 - Open WBM
- Right-click on the interface icon
Open the shortcut menu with the option of switching the interface on or off (active / inactive):
- Right-click on protocol icons (S→SNMP / D→DCP)
Open the shortcut menu with the option of activating or deactivating the corresponding protocol:
- Right-click on connection line
Open the shortcut menu with the following alternative options:
 - Delete reference connection
 - Use connection as reference
- Position the mouse pointer on device icon
The following information is alternatively shown:
 - Various device properties (IP, MAC, system name, PROFINET device name, etc.)
 - Interface properties (name, connection, status)

- Position the mouse pointer on connection line
Show information about connected devices
- Click a device icon or a connecting line
Select the corresponding object

Operation - shortcut menus dependent on editing mode

Depending on the selected processing mode (selection / drawing), you can also use the following possibilities:

Selection mode:

- Double-click on interface icon
Switch corresponding interface on/ff (active / inactive)
- Double-click on protocol icon (S / D)
Activate / deactivate corresponding protocol

Drawing mode:

- Double-click on a connection line
Use connection as reference
- Create a reference connection
Either by clicking on the respective interfaces
or
By clicking on the devices icons involved. This opens a menu from which you can select the desired interfaces.

4.2.3.2 Reference editor / how it works and modes

Overview

The following sections explain the modes of the Reference editor and how it works:

- Using the selection mode and drawing mode
- Editing mode in the Reference editor - arrangement of the devices
- Display of the connections
- Reset reference topology
- Recalculate topology

Using the selection mode and drawing mode

The icon for the selection tool is available in the toolbar of the Reference editor. With this icon, you enable the selection mode. The icon for the selection mode is then disabled while you are working in selection mode. This mode is enabled as default when you call the reference editor. In this mode, you can perform the following editing steps:

- Drag devices from the catalog of unmanaged devices and place them in the Device editor view area with the mouse
- Drag devices from the catalog of new devices and place them in the Device editor view area with the mouse
- Change the reference status of a port (in operation/not in operation)
- Change the status of the protocol-specific device availability for the SNMP and DCP protocols
- Delete reference connections and unmanaged devices
- Remove managed devices and move the device to the catalog of new devices

Note

In selection mode, the "Remove" option is available if you right click on a device. This removes the device from the view and it is moved to the catalog of new devices. This applies only to managed devices. With unmanaged devices or user-defined device types, the "Delete" option is available.

The icon for the drawing tool is in the toolbar in the Reference editor beside the icon for the selection tool. To change to the drawing mode, click on the icon for the drawing mode. In this mode, you can perform the following editing steps:

- Draw a connection between ports of different devices
- Specify a current connection as a reference connection

In the drawing mode, you can draw a connection line between two devices by clicking on the ports of the devices you want to connect. A dialog box is then opened in which you select the port numbers of the devices to be connected. This allows you to draw connections between two devices.

Editing mode in the Reference editor - arrangement of the devices

When it starts up, the Reference editor checks whether or not a reference topology is available. If no reference topology is available, the current topology is used.

When you open the page with the Reference editor, the network devices are arranged automatically in hop layers based on the current connections. The Reference editor view contains several hop layers. The network devices are stored in a hop layer based on the connections.

- For devices with current connections, the layer is calculated automatically based on the current connections.
- Devices without current connections are stored at the end of the lowest hop layer.

This continues until the reference topology is configured. SINEMA Server saves the hop layer as long as the editor has no reference connections. Once the reference topology has been configured or saved, the hop layers are then based on the connections of the reference topology.

Display of the connections

To display the connections, the toolbar of the Reference editor includes the "Display current connections" check box that is selected as default.

As long as this option is enabled, the connections of the current topology along with the reference connections between the devices are displayed. To improve clarity or to be able to see current connections and port statuses better, with the "Display current connections" option, it is possible to display current connection lines in light blue in the Reference editor.

Reference connections are displayed in black. This means that the current connections and reference connections can be clearly distinguished. The "Display current connections" option is also used to provide color identification of the current port status and the current availability status of protocol-specific devices in the Reference editor.

The small rectangular border around ports indicates the current port status. The border around the icon for the protocol-specific availability identifies the current status of protocol-specific device availability.

Unknown devices are represented in the Reference editor by a cloud. Nevertheless, connections can exist between ports of other devices and cloud devices.

Resetting the reference

With the "Reset reference topology" button, you can reset the reference view to its original status.

Use the "Reset reference topology" button if you want to start with a new reference for all statuses except that of the connections.

The following actions are taken if you click the "Reset reference topology" button:

- All the reference connections drawn by the user and all the devices added by the user are deleted.
- The status of the reference port is reset. If the original or previous status is unknown, the editor waits for the next "In operation" or "Not in operation" status of the port.
- The status of the protocol-specific device availability is deleted.

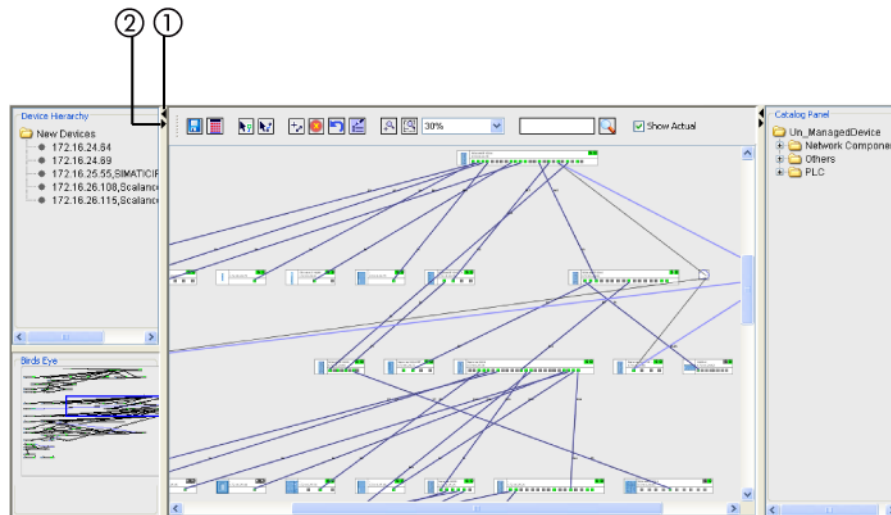
Recalculate topology

During a refresh, the status of the topology layout is not changed. The zoom level and view position remain as they are. During the automatic refresh, only the status color and the colors of the connection lines are changed but the device positions remain as they are. Once devices have been discovered and displayed in the topology tree, their positions are only changed if you click the "Recreate topology" button. If the "Current topology" page is called up before the entire topology has been discovered, this can lead to cross-over connections. In this case, you can recalculate the layout and the positions in the device view area with the "Recreate topology" button.

4.2.3.3 Reference editor / including devices

Device hierarchy (new devices)

The Reference editor includes the sub window "Device hierarchy" that displays all new devices. This sub window is on the left-hand side in the Reference editor.



New devices can be inserted in the reference topology by dragging them with the mouse. As an alternative, you can click on the new device or use the options in the shortcut menu. When you call the Reference editor, all discovered connections with current connections are automatically displayed in the center of the Device editor view area. Only unresolved devices and devices discovered the first time are entered in the list of new devices. Devices in the device hierarchy are not part of the reference and are not therefore displayed in the monitoring view.

Note

Devices in the topology tree without a current connection between the devices and ports are classified as unresolved devices.

After a new device has been added to the Reference editor area, this device is no longer available in the new devices folder. This device is only visible in the monitored topology after saving the reference topology. If a device was deleted, it is displayed again in the sub window of the device hierarchy in the new devices folder.

Adding new devices

Follow the steps below to add new devices to the Reference editor:

1. In the toolbar of the Reference editor, click "Select".
2. Select the required device in the "New devices" folder.
3. Drag the new device to the reference view with the mouse.

4. If you hold down the shift key while doing this, you can also add several new devices at the same time.
5. Once the new device has been inserted in the reference view, it disappears from the list of new devices.
6. After adding reference connections to the new devices, click the "Save" button to save the new devices.

Adding unmanaged devices

The SINEMA Server application provides options with which you can add unmanaged devices to the reference topology so that you can configure a complete topology. The unmanaged devices can be added to the reference view if you are working in selection mode. These devices cannot be monitored.

The "Catalog" sub window contains the list of categories for predefined device types. Each category consists of several predefined network devices that were not identified by SINEMA Server. Such device types can be added to the reference topology using the device types in the "Catalog" sub window. To add unmanaged devices to the reference view, go to the required folder and drag the predefined network devices to the reference topology area.

The unmanaged devices can be added to the reference view by dragging them with the mouse from the catalog of unmanaged devices on the right-hand side of view. Each unmanaged device has a unique name as soon as it is added to the reference view. This unique name is used to identify the device when creating a reference topology.

Connections between these unmanaged devices and managed devices can be created either manually or with the options in the shortcut menu. Connection lines can be drawn between any two unmanaged devices or between managed and unmanaged devices. Connection lines can also be drawn between two managed devices.

Note

Displaying the catalog

With the standard settings, if you display the "Reference topology" page, the "Catalog" sub window is not displayed. To display the "Catalog" sub window, click the arrow icon on the right-hand edge of the Web page.

4.2.3.4 Reference editor / configuring connections

Configuring reference connections - principle

In the Reference editor, the reference connections between the devices can be configured in drawing mode. The connections can be configured in different ways.

- Drawing connections between devices and ports of other devices manually
- Specifying a current connection as a reference connection by double-clicking
- Specifying a current connection as a reference connection using the shortcut menu

The following option can only be configured in selection mode:

4.2 Topology

- Specifying all or selected current connections as reference connections using the "Use current connections as reference" button.

Drawing connections between devices manually

Follow the steps below:

1. In the device editor area, click on the specific port of a device.
2. Select a specific device to which you want to draw a connection and select the port.
3. A connection line is drawn between these two devices.

As an alternative:

In the drawing mode of the Reference editor, you can draw a connection line between two devices by clicking on the ports of the devices you want to connect. A dialog box is then opened in which you select the port numbers of the devices to be connected. This allows you to draw connections between two devices.

Specify a current connection as a reference connection

- by double-clicking

To specify an existing current connection as a reference connection, double-click on the connection line representing a current connection. The line color then changes to black indicating a reference connection.

- using the shortcut menu

Select the connection line representing a current connection that is displayed light blue. Right click on the connection line and select the "*Adopt as reference*" option in the shortcut menu. The connection line is then displayed in black identifying a reference connection.

Specifying the current connections as reference connections

The "Use current connections as reference" option is available in the toolbar view and can only be used in selection mode. The icon is next to the drawing tool icon in the toolbar. Click on this icon to specify the current connections as reference connections. This opens a dialog box in which you confirm or reject the action with Yes or No. Click "Yes" if you want to specify the current connections as reference connections.

Creating connections - combinations of different media types

In the Reference editor, a maximum of 1 connection can be drawn from an unknown port to another port. If you attempt to draw several connections to an unknown port, this will be considered as a change of connection partners. The old connection is then replaced by the new one.

It is possible that there are devices with unknown media types. Connections are permitted between any media types. The precise media type, however, needs to be identified and a connection must be drawn so that the correct combination type can be selected. You will be prompted by a message on screen to check whether or not the combination is correct. This message is only displayed if you draw a connection between a specific combination of media types.

The various combinations of media types and whether these cause the message to be displayed are shown in the following table:

Combination of media types	Connection permitted	Explicit message is displayed
Copper - copper	Yes	No
Copper - glass fiber	Yes	No
Copper - wireless	Yes	Yes
Glass fiber - glass fiber	Yes	No
Glass fiber - wireless	Yes	Yes
Wireless - wireless	Yes	No
Unknown - unknown	Yes	No
Unknown - copper	Yes	Yes
Unknown - glass fiber	Yes	Yes
Unknown - wireless	Yes	Yes

Unmanaged devices in the current topology - effect on connections

In the device view area, the unmanaged devices are not displayed in the current topology. If there is an unmanaged device between two managed devices, this leads to the following connection:

- A cloud between the ports of devices
This normally happens when more than two devices are connected to the unmanaged device.
- A direct connection between the ports
This normally happens when only two devices are connected to the unmanaged device.
- Connection between unresolved cloud and device
If one of the managed devices does not have a connection, the device (not the ports) is connected to the unresolved cloud.
- No connection between the devices if the port is not an operation.

4.2.3.5 Reference editor - additional configuration options

Overview

You have further configuration options in the Reference editor for the following properties and functions:

- Status of the reference port
- Protocol-specific device availability as reference
- Cloud connections in the network

Configuring the status of the reference port

The Reference editor provides options for managing the port status. It is, however, not possible to change the reference status of ports with reference connections. The status of a reference port can be configured in selection mode to one of the following types:

- **Switching over the port status manually by double-clicking**
Double-click on the port of a specific device to switch over between the status "In operation" and "Not in operation".
- **Changing the port status using the shortcut menu**
Select the required port in the editor view and right click on it. A shortcut menu is displayed. Here, you can choose between one of the statuses "In operation" or "Not in operation".
- **Changing the port status using the "Adopt as reference" function**

Configuring the protocol-specific device availability as a reference

In the Reference editor, there are options for enabling or disabling the status of the SNMP or DCP protocol-specific device availability for a device.

If a device type supports the protocols, the status can be changed. The initial status of the device protocols can be taken from the device type. The initial protocol-specific device availability of the reference corresponds to the actually discovered protocol. The protocol-specific device availability of the reference can be configured in one of the following ways:

- **Switch over the status of the protocol-specific device availability by double-clicking**

To change the status of the protocol-specific device availability, double-click on the icon for the protocol-specific device availability. The relevant protocol is switched over between the "available" and "unavailable" status. A scored-through icon indicates the unavailable status.

Note

The availability status of the protocol cannot be configured

If the network device does not support the SNMP or DCP protocol, the availability status of the protocol cannot be configured. The unsupported protocol is identified by a scored-through icon.

- **Change the status of protocol-specific device availability**

You have the following options:

- Specify the status of the protocol-specific device availability of a device as the reference status

By selecting an individual device and clicking "Use as reference", the current status of the protocol-specific device availability is specified as the reference status.

- Specify the status of the protocol-specific device availability for several or all devices as the reference status

If you select several devices and click this button, the reaction is the same as for an individual device. This also applies if you select all devices.

Configuring cloud connections in the network

A network cloud is a special type of unmanaged device. Each device that has no IP address and that is surrounded by 3 or more LLDP devices is identified by SINEMA Server as a network cloud. Each network cloud is assigned a unique name. This name is displayed in the Reference topology editor. In contrast to other unmanaged devices, a network cloud has no ports. A network cloud can nevertheless be used as an endpoint for various connections.

Clouds identified by SINEMA Server have the name "Virtual Device *XXX" (where XXX stands for the index number 1 or 2 or 3 etc.).

Assuming there is a cloud in the current topology. Specifying this current cloud (including all connections) as a reference cloud causes the following actions:

- The connection line is displayed in black identifying a reference connection.
- After reloading the reference topology a simulation of the discovered cloud is created (reference cloud*1).
- The same connection partners are available as for the current cloud.
- This reference cloud is displayed in the monitored topology and remains in the application until the cloud is deleted.
- Both the current and the reference cloud are always displayed in the Reference editor.
- If the discovered cloud is specified as a reference cloud (reference cloud*2), a new reference cloud is created. The old reference cloud is orphaned.

Note

Deleting orphaned clouds - creating a reference cloud

The orphaned clouds can either be deleted manually or the application deletes them itself when the reference topology is reloaded. To display a reference cloud at least one reference connection must be available in the editor.

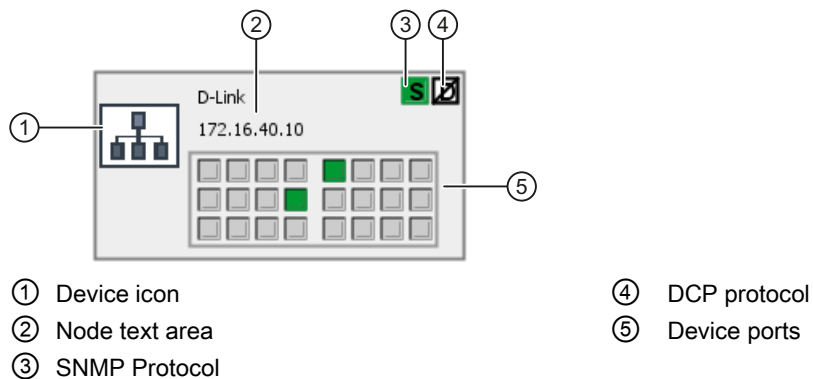
4.2.3.6 Icons and colors in the reference topology

Overview

The following sections explain the significance of the colors for devices, ports and connection lines in the reference topology.

Status monitoring

In the Reference editor, you can monitor the status of the network devices, their ports and connections. This monitoring is based on the various displays of ports, connection lines and the statuses of the protocol-specific availability of devices. Each device in the editor is represented by a device icon, a node text, protocol options and a port area. Below you can see the graphic representation of a device and its content:



Note

With device ports, the color of the border around the rectangular area indicates the status in the current topology. The fill color of the port shows the reference or monitored status.





Port status

The various ports statuses and the protocol-specific device availability are shown as follows:



Target status	Display current connections	Border color	In operation	Not in operation
In operation/test/in operation - Maintenance required	Enabled	Green		
In operation/test/in operation - Maintenance required	Disabled	Black		
Not in operation/not in operation - Maintenance demanded	Enabled	Gray (dark)		
Not in operation/not in operation - Maintenance demanded	Disabled	Black		
Unknown	Enabled	Gray		
Unknown	Disabled	Black		

Status of protocol-specific device availability







The protocol-specific device availability is shown as follows in the SNMP icon:

Status	Display current connections	Color of the rectangle around the SNMP icon
reachable	Enabled	
reachable	Disabled	
Unreachable	Enabled	
Unreachable	Disabled	

4.2 Topology

Status	Display current connections	Color of the rectangle around the SNMP icon
not activated	Enabled	
not activated	Disabled	

The protocol-specific device availability is shown as follows in the DCP icon:

Status	Display current connections	Color of the rectangle around the DCP icon
reachable	Enabled	
reachable	Disabled	
Unreachable	Enabled	
Unreachable	Disabled	
not activated	Enabled	
not activated	Disabled	

Note

The "unavailable" status depends on the target status of the device. SNMP is either supported by the device or not. If the device supports the SNMP protocol, the fill color is green, otherwise gray.

4.2.4 Topology - special features

Overview

- Unresolved ports
- Redundancy concepts

Unresolved ports - display in the topology

If the discovered topology includes devices with unresolved ports, SINEMA Server shows these devices in the lower area of the topology page with a connection to a cloud. The connections out of this cloud end at device boundaries since no port assignment is possible.

On the management station, this status is indicated by a connection to a cloud icon.

In terms of a device, the following two situations must be distinguished for unresolved ports:

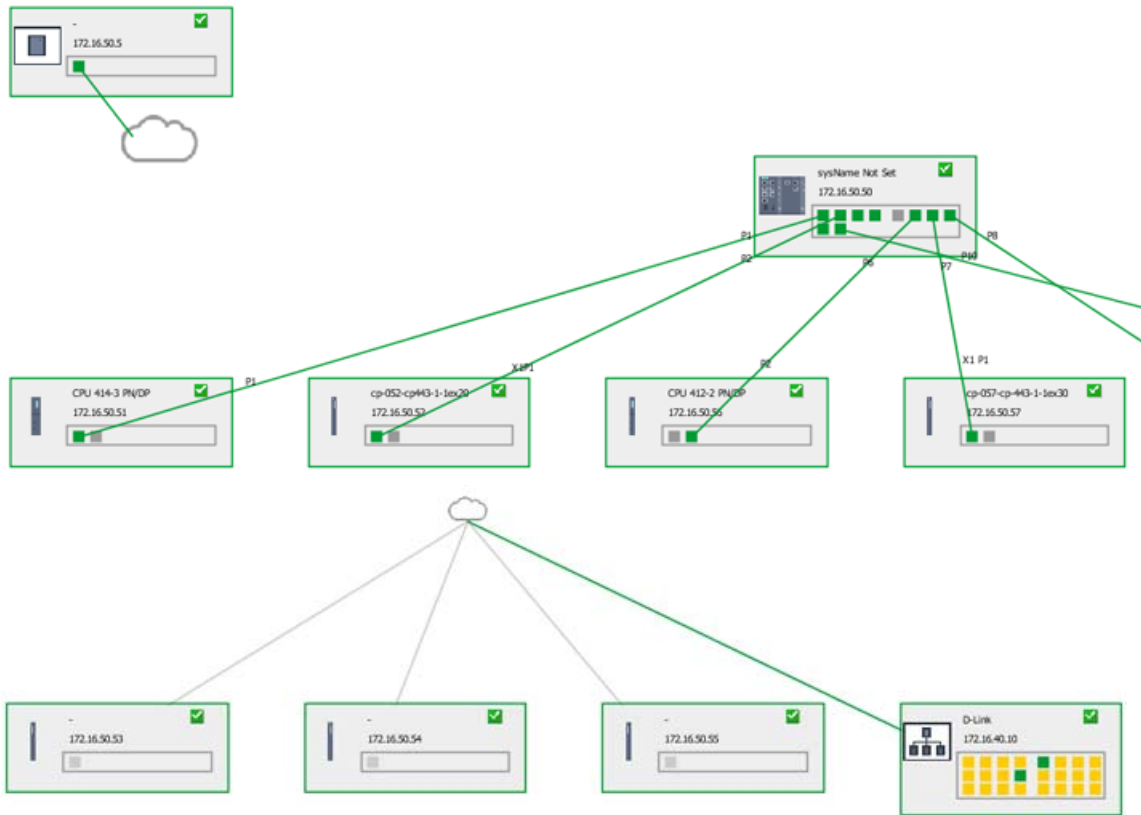
- Case a)

At least one port of the device has a connection to a device discovered in SINEMA Server. In this case the device is shown in the topology with its resolved ports. Active ports are shown in green without a connection.

- Case b)

No port of a discovered device has a connection to a device discovered in SINEMA Server. In this case, the device is connected to the cloud in the lower display area.

4.2 Topology



Redundancy concepts

In a ring network, the network devices are connected together in the form of a ring. Each node is connected to two other nodes so that a continuous path is achieved.

In a standby ring configuration, the ring network is linked to another network and a device (switch) serves as the standby master and another switch in the network serves as the standby slave.

On the pages with the device details, SINEMA Server shows the following properties:

- Details of the redundancy status
- Ring status
- Information on the redundancy mode
- Port type
- Port status

The redundancy mode and its corresponding status are shown in the "LAN port" tab. On the "Network > Devices" pages, the applications also show the corresponding device status. The events show information on changes to the current status of the ports including information on the type of port.

4.2.5 Topology - general forms of representation

4.2.5.1 Topology - Device hierarchy

Layout

You can open the "Device hierarchy" window from the three topology views by clicking on the ► icon in the upper left corner of the window.

Operation / content

It differs in content and function depending on where you open the window.

- **"Topology > Discovered / Monitored"** Web page

In this use, the window displays all devices, which are also visible in the topology.

If you double-click on an item, a search is made for the corresponding device in the topology view, the device is selected and the window focuses accordingly.

- **"Topology > Reference"** Web page

In this use, the window displays all devices, which are not visible in the topology.

If you double-click on an item, the corresponding device is transferred to the topology view, i.e. it is included in the reference. The same result can also be achieved by using the mouse to drag the device item from the device overview into the topology view.

4.2.5.2 Topology - Bird's eye view

Layout

You can open the "Bird's eye view" window from the three topology views by clicking on the ► icon in the upper left corner of the window.

Operation / content

The "Bird's eye view" window shows the entire topology view in a highly reduced form. The blue frame indicates the section that is currently displayed on the screen.

4.3 Reports

Types of report

SINEMA Server provides a set of reports for network monitoring and analysis. Specifically, the following properties and criteria are analyzed:

- Availability
- Performance
- Inventory
- Events

In each of these types of reports, you can precisely select the data to be evaluated based on the form, content and time period.











The reports can be used to display meaningful statistical data. In addition to this, 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 fields are displayed with report information in the Inventory, Availability or Performance report.

Operation / content

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:

Icon	Display / function	Icon	Display / function
	Show/hide graphic		Show/hide table
	Evaluation time period: 24 hours		Evaluation time period: 7 days
	Evaluation time period: Start time By clicking in the input box, you open the calendar function,		Evaluation time period: End time By clicking in the input box, you open the calendar function,
	Start text search / filter setting Result: The elements that match the text string specified for the text search are included.		Enter text for text search / filter setting
	Apply text filter, show data		Filtering according to existing or deleted devices

Note**Filter options**

The filter options in the **Reports** menu are identical for all report pages.


Note**Minimum period 10 minutes**

When filtering the report according to a specific period, the period entered in the "From" and "To" boxes must be at least 10 minutes.

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. 

SINEMA Server 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. In the management station, the SINEMA Server Monitor provides a function with which you can delete, swap out or import historical data.

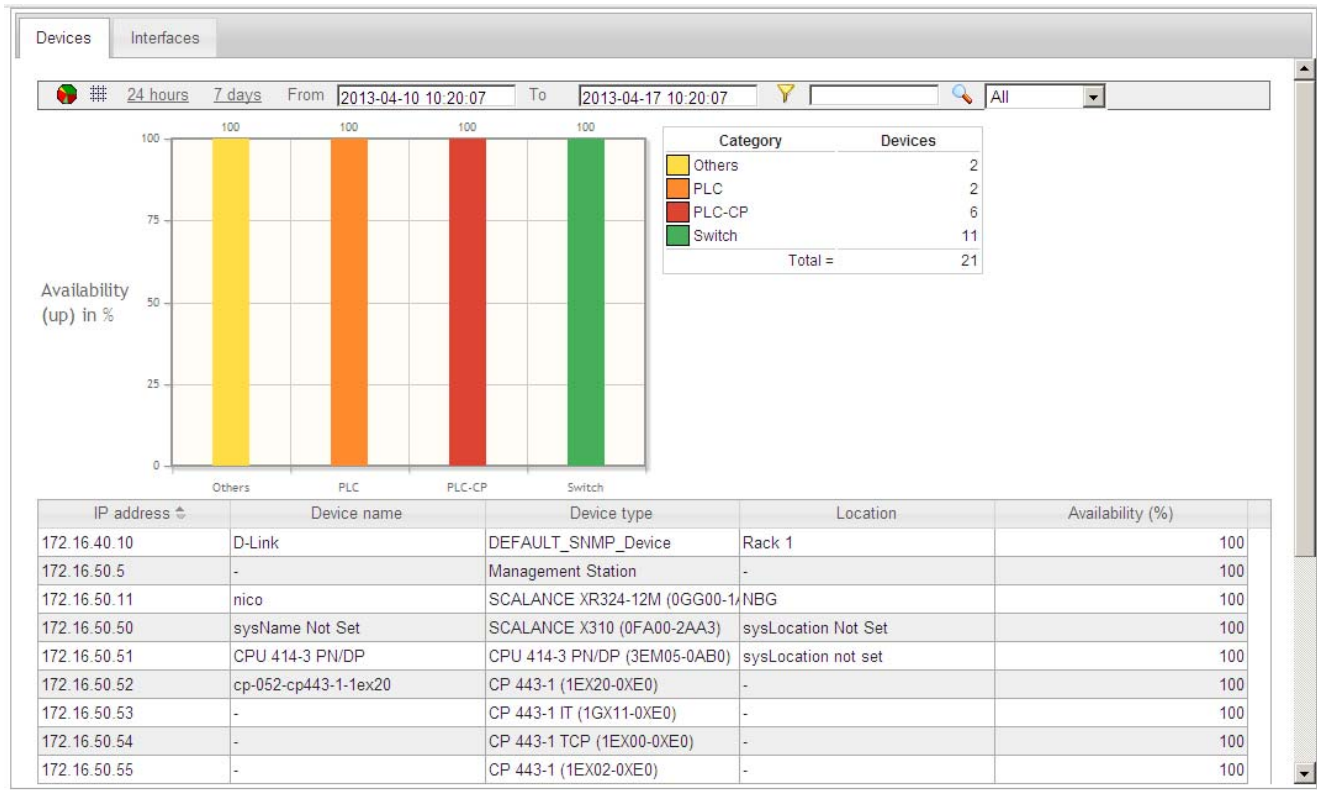
See also

Device details (Page 105)

4.3 Reports

4.3.1 Reports - Availability

The report types described below are available with the menu command: **"Reports > Availability"**



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 (for details see 'Tab').


"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

All the interfaces of the devices are displayed individually. The grouping in the graphic is according to the transmission media (copper, glass fiber, wireless).

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:

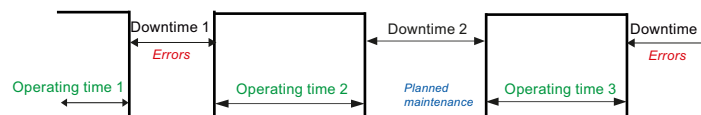
- Availability (percentage)
- Number of outages
- Total uptime (period absolute)
- Total inactive (period absolute)
- Last discovered
- First discovered
- Average downtime (period absolute)
- Average uptime (period absolute)
- Unmonitored period (period absolute)
- Not monitored (percentage)
- Device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

Special feature - "Historical data" column

If the "Historical data" box is displayed as well, two further diagrams can be generated using the shortcut menu of this icon. These diagrams either analyze data that has already been acquired or make predictions in trend diagrams.

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.



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)

4.3.2 Reports - Performance

The report types described below are available with the menu command: **"Reports > Performance"**


Structure and meaning

Display of all (filtered) objects with information relating to their performance; in other words, how fast and reliably they have transferred and received data during the monitoring period.

The "Reports > Performance" window has the following tabs:

- LAN - Interface utilization:
For all LAN interfaces, not only the 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.

Operation / content

Although the column assignment in the data area is preset, you arrange it any way you wish ( 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 (%) | • Maximum reception error rate (%) |
| • Average reception performance (%) | • Average transmission data rate (%) |
| • Average performance (%) | • Current transmission data rate (Mbps) |
| • Maximum transmission performance (%) | • Maximum transmission data rate (Mbps) |
| • Maximum reception performance (%) | • Average signal strength (dBm) |
| • Maximum performance (%) | • Maximum signal strength (dBm) |
| • Average error rate (%) | • Average client number |
| • Maximum error rate (%) | • Maximum client number |
| • Average transmission error rate (%) | • Mode (WLAN default) |
| • Average reception error rate (%) | • Used channel |
| • Maximum transmission error rate (%) | • Information if and when deleted |

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.

See also

Device details (Page 105)

4.3.3 Reports - Inventory


The report types described below are available with the menu command: **"Reports > Inventory"**

Layout

The **"Reports > Inventory"** Web page contains the "Vendor", "IP address range" and "Device category" tabs.

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 arrange it any way you wish ( in the footer). The following can be selected:

- IP address
- Device name
- Device type
- Location
- Name of the IP address range (Page 173)
- Number of interfaces (used / total)
- PROFINET device name
- MAC address
- Firmware version
- Order number

4.3 Reports

4.3.4 Reports - Events

The report types described below are available with the menu command: **"Reports > Events"**

Layout

The **"Reports > Events"** Web page contains the "Network events" and "System events" tabs.

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; in other words, the messages generated by SINEMA Server.

4.3.5 Historical data and trend charts

Within the report pages, you can call up 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, SINEMA Server provides an additional column "Historical data".

4.3.5.1 Historical data

Meaning

The data of a device or an interface monitored in SINEMA Server is subject to change. SINEMA Server 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:

Entry	Meaning
Attributes	<p>Names the property whose status has changed.</p> <p>The following is displayed depending on the selected report type and the selected entry:</p> <ul style="list-style-type: none">• For devices:<ul style="list-style-type: none">– IP address– MAC address– Device type– Device category– PROFINET device name– Monitoring status• For interfaces:<ul style="list-style-type: none">– 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

4.3 Reports

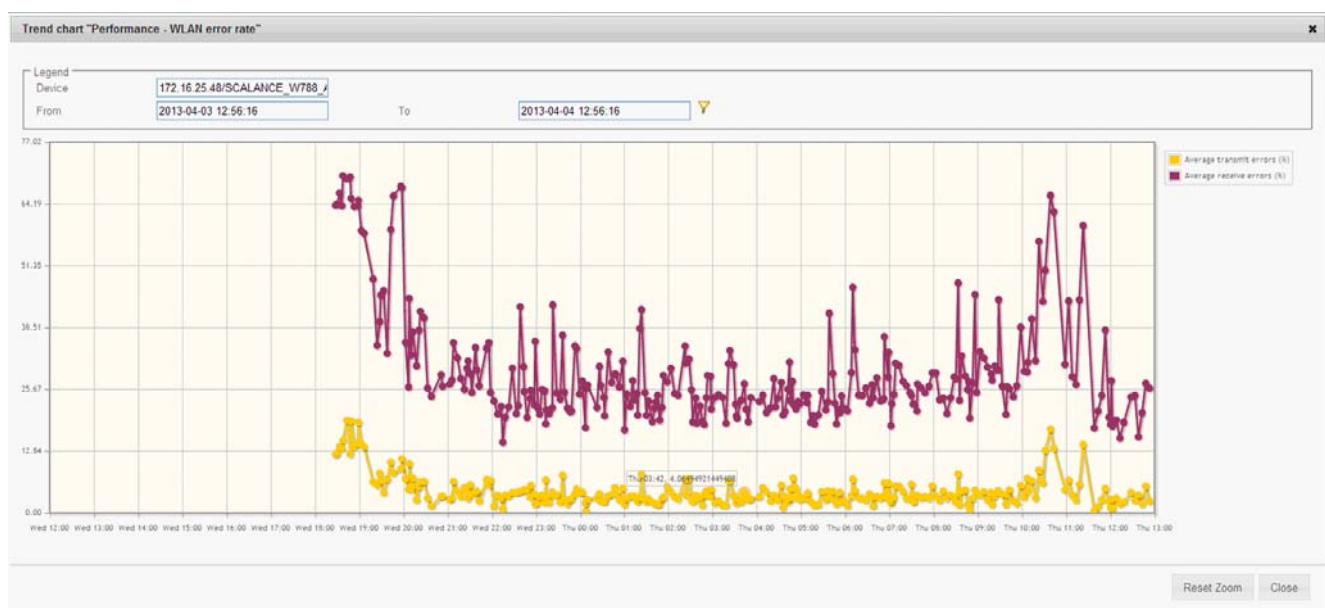
4.3.5.2 Trend charts

Meaning

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 (%)" with the trend of the "Average transmit error rate (%)" and "Average receive 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.

Report type	Tab	Trend data
Availability	Devices	Availability in %
	Interfaces	Active time in %
Performance	LAN - interface utilization	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Average transmit error rate in % Average receive error rate in % Average error rate in % Display with 2 trend lines
	WLAN interface error rate	<ul style="list-style-type: none"> Average transmit error rate in % Average receive error rate in %
	WLAN - Interface data rate (transmission speed)	Average transmission data rate (Mbps)
	WLAN - signal strength	Average signal strength (dBm)
	WLAN - number of clients	Average number of clients

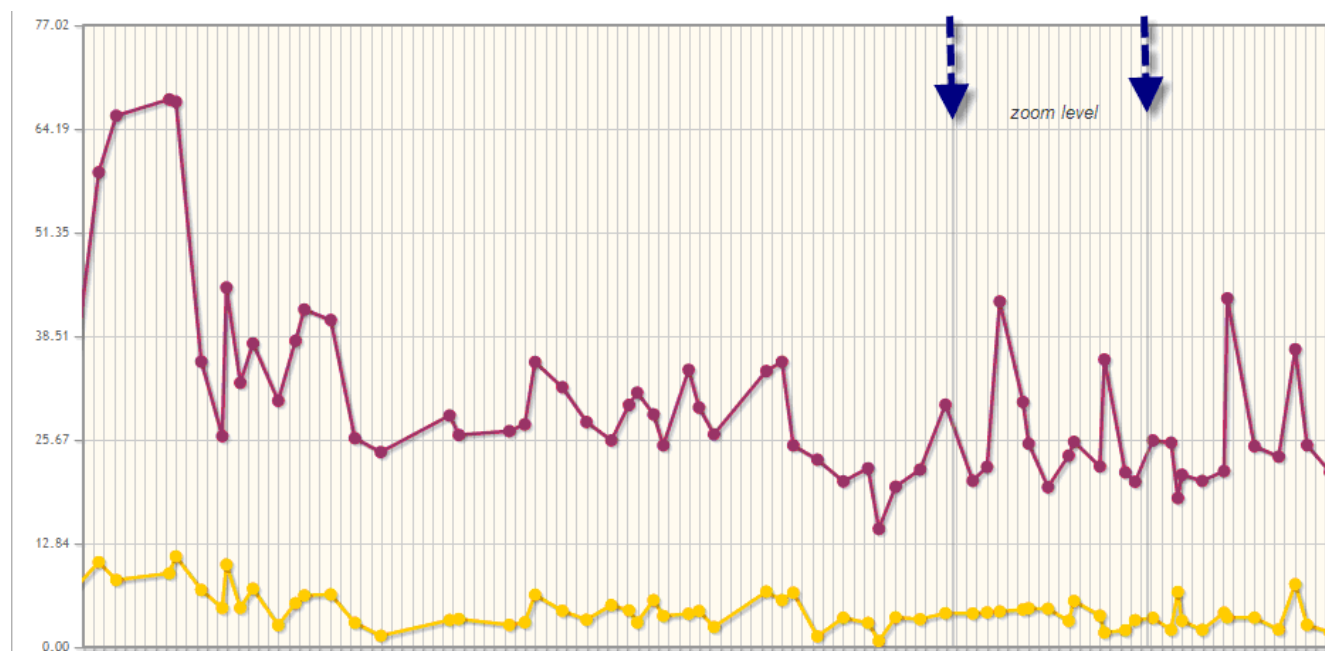
Zoom function

The zoom function of the trend charts allows you to spread 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 the required starting time of the period to be spread and hold down the mouse button.
2. Drag the mouse pointer to the required end time and release the mouse button.

4.3 Reports



4.4 Administration

SINEMA Server includes various tools for managing the network, program, users and other objects. You can open the tools in the following Web pages using the menu commands with the same names:

"Administration > ..."

- Discovery
- Network
- 'Unmanaged' device types
- Event types
- OPC
- User
- User interface
- System information
- Import / Export

4.4.1 Administration - Discovery / Scan

The functions described below are available with the menu command: **Administration > Discovery** "Scan" tab

Scan

Profiles

IP address ranges for network search

Nodes to scan

285

	Status	First address	Last address	Name	No. Nodes
<input type="checkbox"/>		172.16.50.1	172.16.50.254	Rack	254
<input type="checkbox"/>		192.168.10.1	192.168.10.20	10er	20
<input type="checkbox"/>		192.168.20.20	192.168.20.30	20ger	11

DCP network adapter for device scan

	Status	IP address	Name
<input type="checkbox"/>		172.16.50.5	Intel(R) 82578DM Gigabit Network Connection

DCP detection type

☐ Include all devices discovered with DCP in the result.
 ☒ Only include the devices in the result that are located in one of the specified IP address ranges.

Scan



On this Web page, you set the parameters for the network scan and start the scan.

You have the option of specifying the IP address range for the scan in the network and the DCP network adapter of the management station used for the scan.

Other setting options relate to whether or not detected devices are taken into account and the execution of the scan.

- **Header area**





The following table shows the function elements of the header area.

Icon	Display / function
	Start network scan When a scan is running, you can recognize this due to the appearance of the scan icon in the status bar of SINEMA Server.
	Stop network scan

- **IP address areas for network scan**

Here you specify which IP addresses SINEMA Server should limit itself to for the network scan. With the green status icon, the corresponding range will be included in the scan, and all else excluded.



The following table shows the functional elements of the header.

Icon	Display / function
	Create a new address range
	Change address range
	Delete address range
	Change the status of the selected (✓) ranges green: Network range is included in the scan. gray: Network range is defined but not included in the scan.

- **"DCP network adapter for device scan" area**

Here you specify the LAN interface of the management station to be used for the network scan (green status icon).

The following table shows the functional elements of the header.

Icon	Display / function
	Scan LAN interfaces
	Change the status of the selected (✓) interfaces green: Network adapter is used for the scan.

- **"DCP detection type" area**

To take discovered devices into account, select from the following options:

- Include all devices discovered with DCP in the result.
- Only include the devices in the result that are located in one of the specified IP address ranges.

- **"Miscellaneous" area**

Here, you can select functions using the check boxes:

- Automatic scan

If this option is selected, the scan is started automatically at the set interval. You set the interval with the **"Administration > User interface"** menu command.

The check box is deselected as default.

- Duplicate IP detection

If this option is selected, SINEMA Server checks whether or not the IP address exists more than once in the network.

- Duplicate PROFINET IO name detection

If this option is selected, SINEMA Server checks whether or not the same PROFINET IO device name exists more than once in the network.

Adapting the scan range

If you do not adapt the scan range, the device scan can take a very long time if there is a very large scan range.

Refer to the description in the section Detecting devices in the network (Page 51)

4.4.2 Administration - Discovery / Profiles

The functions described below are available with the menu command: **"Administration > Discovery" "Profiles" tab**

Displaying and editing profiles

The "Profiles" tab shows the device profiles that exist in SINEMA Server in the form of a table. Via this table, you have access to all the functions of profile editing.

You can edit the displayed profiles or add new profiles. The following types of profile must be distinguished:

- General profile

This profile type contains information required for discovery and monitoring of network devices.








- Monitoring profile





This profile type contains information that is only required for monitoring network devices.

This difference is shown in the selectable table column Profile type.

Controlling the profile display and editing profiles - function elements

The following table explains the function elements of the header area.

Icon	Display / function
	Create new profile <ul style="list-style-type: none"> • Requirement: A general profile must be selected. • The Profile editor is opened with the "Add profile ID" dialog.
	Create new monitoring profile <ul style="list-style-type: none"> • Requirement: A general profile or monitoring profile must be selected. • The Profile editor is opened with the "Add profile ID" dialog.
	Edit selected profile <ul style="list-style-type: none"> • The Profile editor is opened with the "Profile" dialog with the selected profile data.
	Delete the selected profiles <ul style="list-style-type: none"> • Profiles are deleted following a further prompt for confirmation. • Default profiles cannot be deleted.
	Enable / disable selected profiles <ul style="list-style-type: none"> • Enabled profiles are used during discovery and scanning.
	Save modified profiles <ul style="list-style-type: none"> • The profiles marked with "*" are stored in SINEMA Server.
	Restore selected profiles <ul style="list-style-type: none"> • The function can be used with the profiles supplied with SINEMA Server following modification

Icon	Display / function
	Export profiles <ul style="list-style-type: none"> The selected profile data is added to a ZIP archive. You are prompted to specify a storage location for downloading the ZIP archive.
	Import profiles The dialog box for selecting the profile file is displayed. <ul style="list-style-type: none"> File type: ZIP file Note: Profiles that exist in SINEMA Server and have the same profile identifier are overwritten by the imported profile.
	Enter text for text search / filter setting
	Start profile search Result: The profiles that contain the specified text string in one of the displayed columns.

See also

Profile concept (Page 60)

4.4.2.1 The Profile editor

Displaying and editing profiles

With the Profile editor, you can perform one of the following actions:

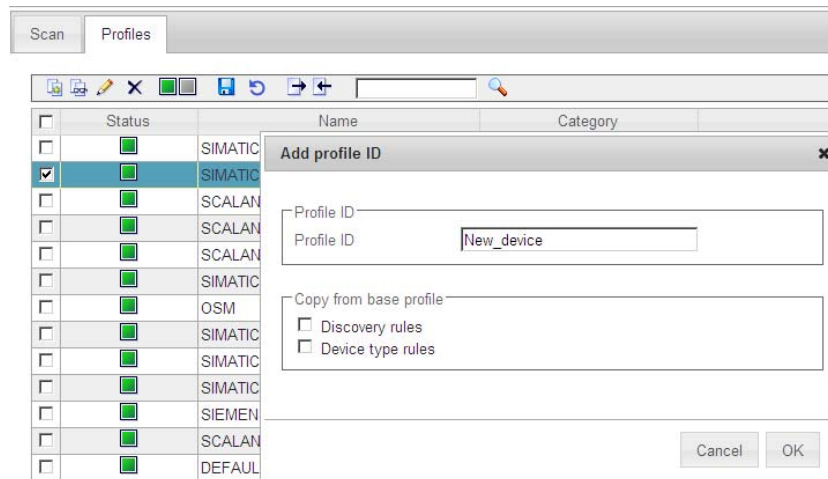
- Add a new device type to an existing profile
- Create a new profile
- Edit / modify an existing profile

The dialogs and tabs are described below.

For information on the procedure, you should also refer to the section Setting up profiles and assigning device types (Page 62)

Create new profile

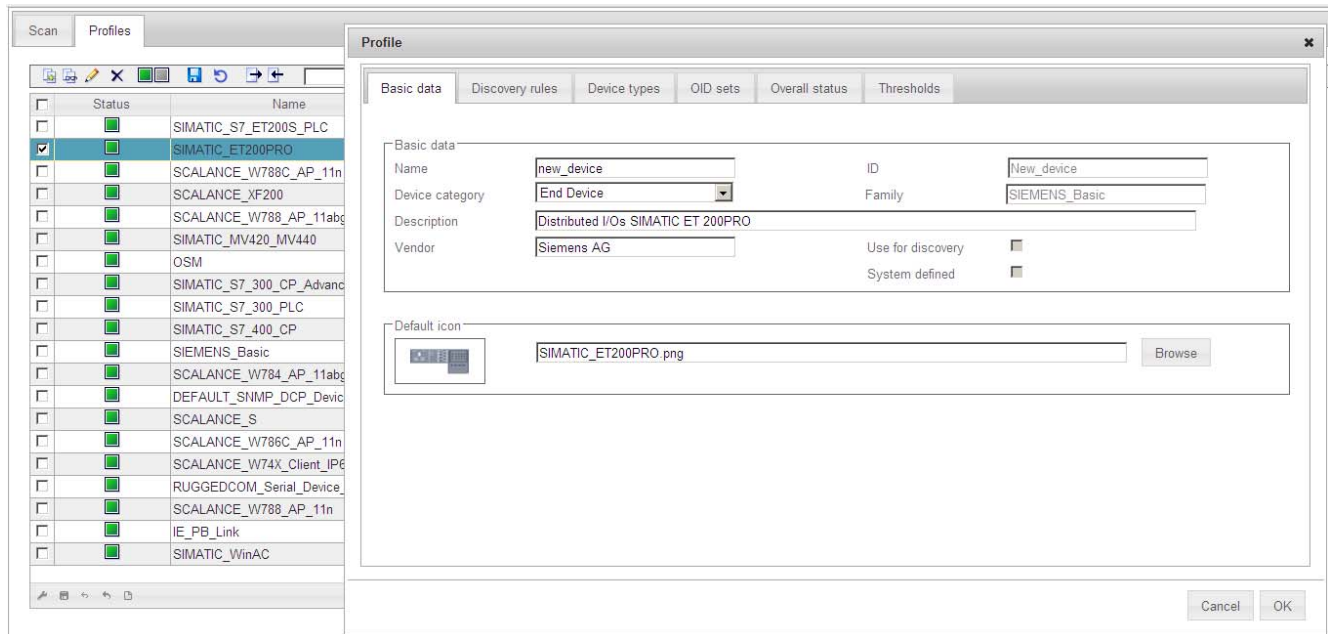
If, after selecting a basic profile, you create a new profile with the "Create profile" function element, you open the "Add profile ID" dialog.



When you confirm your entries with OK, you open the following dialogs of the Profile editor.

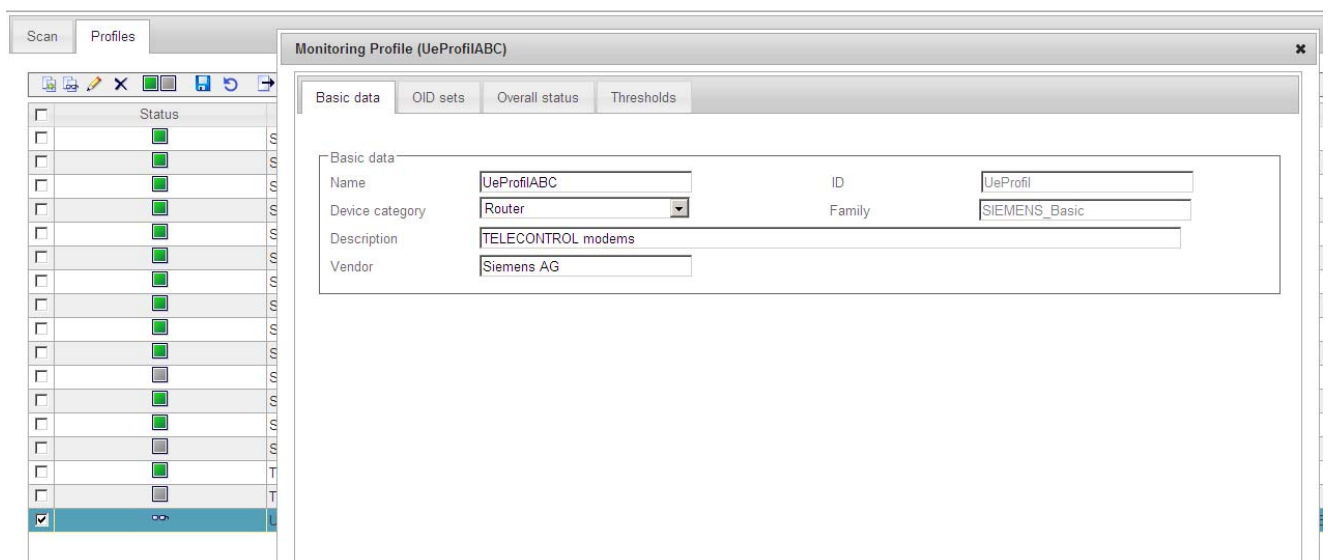
General profile - entering profile details with the Profile editor

If you edit or create a general profile, you open the dialog with the tabs required for discovery and monitoring of a network device.









Monitoring profile - entering profile details with the Profile editor

If you edit or create a new monitoring profile, you open the dialog with the tabs required for monitoring a network device.



Function elements

Some of the tabs described below also have function elements available. For information on the entries, refer to the tabs described below.

Icon	Display / function	Icon	Display / function
	Add an entry You open a further input dialog.		Edit selected entry You open a further input dialog.
	Delete selected entry The selected entry is deleted (only after you have confirmed this).		Change between "Use for discovery" / "Do not use for discovery"
	Enter text for text search / filter setting		Start search for entry Result: The entries that contain the specified text string in one of the displayed columns are displayed.

"Basic data" tab (general profile and monitoring profile)

Input box / parameters	Description
Name	Profile name
Device category	The device category is assigned to all devices discovered using this profile.
ID	Profile ID
Family	Display of the family name. The entry cannot be changed here. 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 family as the general profile.
Description	Option for entering a technologically suitable profile description.
Vendor	Vendor name (can be entered)
Use for discovery	Option selected: The profile is used for the device discovery. The setting cannot be changed here, the profile is initially disabled. Reason: If a time-consuming check (comparison with all other profiles) was required for activation, this would be impractical and annoying in this situation. You can enable the profiles later after you have saved them using the corresponding icon in the toolbar.
System defined	Option selected: Shows that the 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 here.
Default icon	Here, you assign a default icon to the profile for display in the topology. If no other icon is defined in the device types for a device that belongs to this profile, this default icon is used in the topology display.

"Discovery rules" tab (general profile)

The tab contains all the rules to be checked through during discovery. The table must contain at least one rule to be able to enable the profile for monitoring.

Each rule must be unique within a management station and may only occur once.

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Status	Display of the status selected in the header or in the dialog. green: Rule is used for discovery.
Name	Name of the discovery rule.
Rule	Rule as a text string with the following content: "Criteria"-name + values + operators Example: <ul style="list-style-type: none"> sysDescr = <code>"SIMATIC HMI*ThinClient*646"</code>

"Device types" tab (general profile)

The tab is used to define a name and an icon and to specify rules for the device assignment that will be used for the discovered devices.

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 entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Status	Display of the status selected in the header or in the dialog. green: Rule is used for discovery.
Icon	Icon that will be used instead of the default icon specified in the profile.
Device type	Name of the device type
Rule name	Name of the device type rule
Rule	Rule as a text string with the following content: "Criteria"-name + values + operators Example: <ul style="list-style-type: none"> sysDescr = <code>*6AV6 646-0AA21-2AX0*</code>
Icon name	File name of the icon used
Order numbers	Order number according to the conventions of the manufacturer

"OID sets" tab (general profile and monitoring profile)

Contains SNMP OID sets

To enter or edit the values and descriptions of the OID sets, you open a extra dialog.

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Name	Name of the OID set
Description	Text as description
System defined	System defined as opposed to user defined. Refer to the note on "Editable" in the next line.
Editable	Display "yes / no" Only the Automation MIB and OID sets for specific users can be modified. Other OID sets that are read by SINEMA Server are displayed and cannot be modified.

"Overall status" tab (general profile and monitoring profile)

In this tab, you define how the overall status of a device is formed. To do this, you store data records containing certain triggers and trigger conditions along with a weighting. The overall status for the device shown in SINEMA Server then represents the trigger with the highest priority that was detected.

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Trigger	In conjunction with the selected device, possible property that can be relevant for a status display. Examples: ICMP, SNMP
Trigger condition	Possible status in conjunction with the trigger in which the data record and its weighting will be taken into account for the overall status.
Overall status	Status information used in SINEMA Server.
Severity	Numeric priority that correlates with the overall status.

"Thresholds" tab (general profile and monitoring profile)

Here, in data records, you specify limit values for data values that are read by the device or calculated by the system. With these limit values, you link events that are triggered if the value exceeds all falls below the limit value.

The operator used for the limit value check has a specific data type that is specified in the OID set. The limit values must be specified accordingly.

Requirement: You can only define new data records for data values for user-specific OID sets.

4.4 Administration

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Rule name	Name of the data record
Source	Relates to a user-defined or system-defined OID set.
System defined	Yes: The limit values are linked to a system-specific OID set. The limit value and event can be edited.

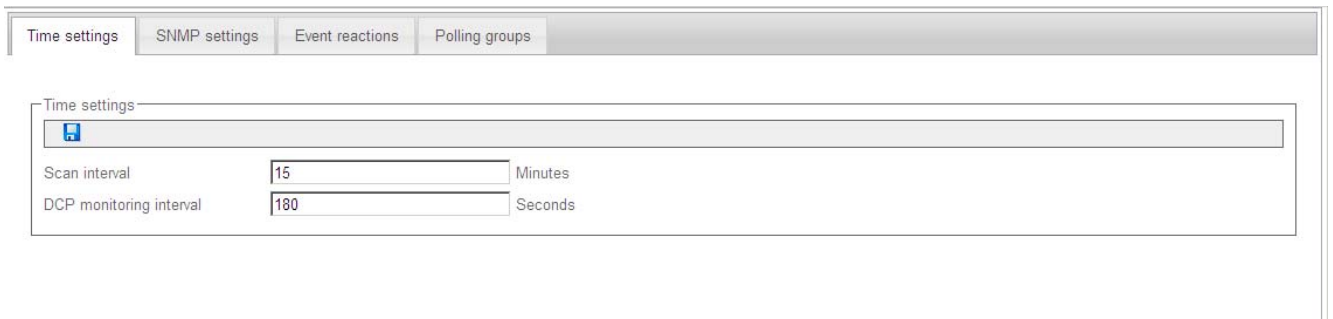
4.4.3 Administration - Network

Overview

The functions described below are available with the menu command: **"Administration > Network"**

The Web page contains the following tabs:

- Time settings
- SNMP settings
- Event handling
- Polling groups



The tabs with their layout and contents, as well as the operating options in detail:

4.4.3.1 Administration - Network Time settings

Time settings

The icon for saving the settings () is located in the header.





The following values are shown below this:

- The time interval for automatic network scans
- The DCP monitoring interval

4.4.3.2 Administration - Network SNMP

SNMP settings

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Create new record for SNMP settings		Change SNMP settings
	Delete SNMP settings		Change the status of the selected (✓) SNMP settings

The table below this shows the existing data records with SNMP settings.

Depending on the SNMP version (1, 2c, 3), when you create or change a record, another window opens in which you can enter the parameters of this version, for example

- Retries
- Timeout
- Group name
- Security level
- User name
- Authentication algorithm
- Authentication password
- Encryption algorithm
- Encoding password

4.4.3.3 Administration - Network Event reactions

The dialogs described below are available with the menu command: **"Administration > Network"**

Configuring event reactions

Event reactions can be defined for the following context types:

- for a specific view

This allows you to define a view-specific event reaction. The views already configured in SINEMA Server are available.

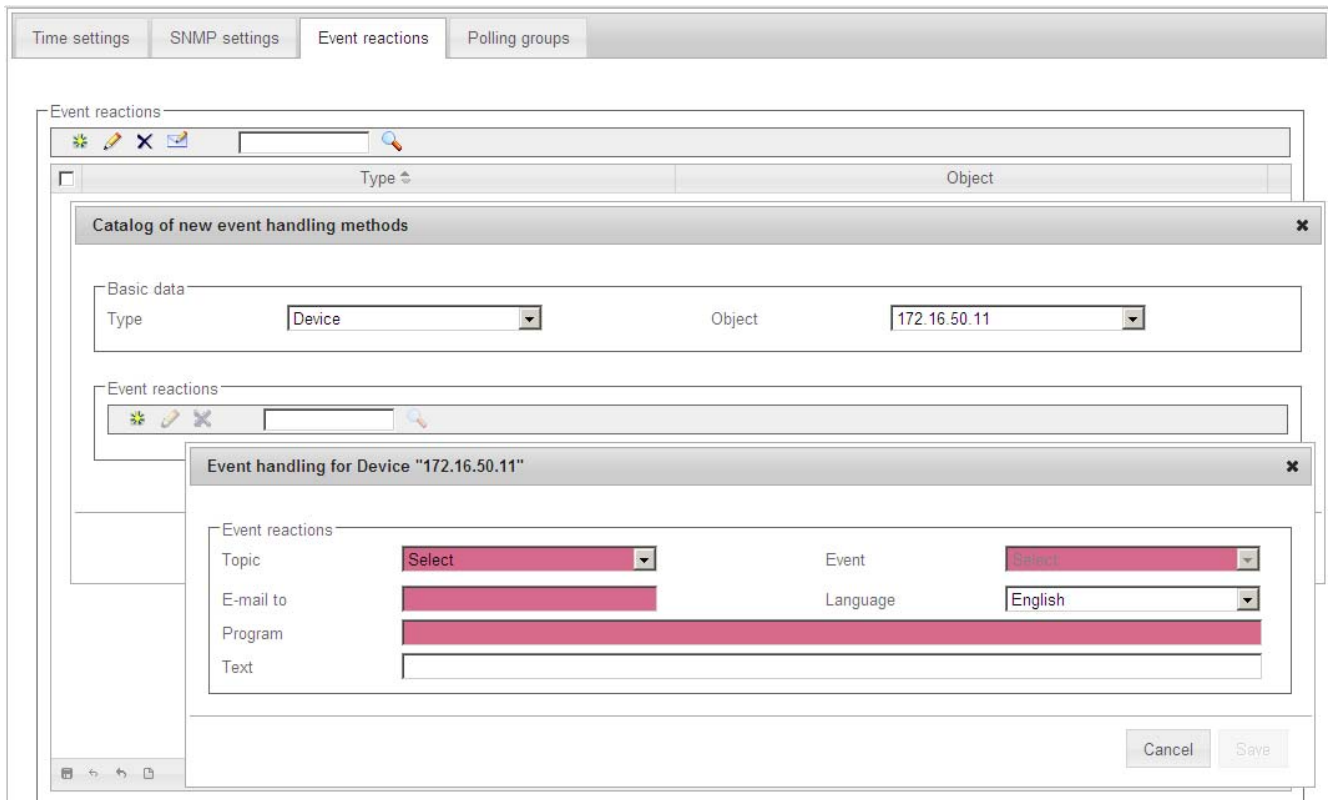
- for the system
- for network devices

All the devices discovered by SINEMA Server are available.

This type selection followed by selection of the relevant object is made in the "Catalog of new event handling methods" dialog that then opens.

In a further dialog "Event handling", you configure the actual event reaction.

The following figure shows the dialog sequence for specifying an event reaction for a network device.



The last dialog to be displayed "Event handling" also shows the selected context type and the selected object in the title bar.







Requirement - e-mail settings

Before you can configure an event reaction, you will be prompted to configure the e-mail settings. The following needs to be specified:

- SMTP server IP
- SMTP port
- Email address of the sender
- User name (optional)
- Password / password confirmation (optional)
- Encryption (selection from drop-down list)

Working with "Event reactions" and the "Catalog of new event handling methods"

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Add new event reaction. With this function, you open a new dialog "Catalog of new event handling methods" The information in this table reflects that in the opened dialog. Depending on the selected type, in the "Catalog of new event handling methods", you open a further dialog "Event reactions".		Change event handling
	Delete event handling		Make e-mail settings
	Enter text for text search		Start text search

"Catalog of new event handling methods" dialog

In this dialog, the following settings can be configured:

- Basic data / Type

From the drop-down list, you can select the following:

- Views
- System
- Device

- Basic data / Object

Depending on the selection you make for "Type", the available views or devices are listed in the drop-down list. If no views have yet been configured in the system, the selection is empty.

- Event reactions

Operator input, see table above.

Note

One event reaction per type / object

You can configure an event reaction for each selected combination of "Type" / "Object". Assigning multiple event reactions is not possible.

"Event reactions for device / System / View x" dialog

In this dialog, the following settings can be configured:

Parameter	Meaning
Topic	Here, various predefined topics can be assigned depending on the type "View / Device / System".
Event	Here, various predefined events names can be assigned depending on the type "View / Device / System".
E-mail address	Specifies an e-mail recipient to be notified when the event occurs.
Language	The sent e-mail contains an event-specific information text. Here, select the language to be used for output.
Program	<p>Here, enter the name of an executable program that will bring about a specific reaction to the event.</p> <p>You can also specify the transfer parameters for program execution.</p> <p>Example: <i>mail.exe \$i \$m \$n</i></p> <p>These transfer parameters are interpreted and replaced by SINEMA Server as follows when the executable program is called.</p> <p>Syntax and meaning</p> <ul style="list-style-type: none"> • \$i - placeholder for IP address • \$m - placeholder for MAC address • \$n - placeholder for device name
Text	Specifies an additional text to be transferred by e-mail (see also information relating to the "Language" parameter).

See also

Administration - Event types (Page 183)

4.4.3.4 Administration - Network Polling groups

This window shows the three polling groups "Fast", "Medium" and "Slow" each in a separate tab, together with their assigned network devices.

You are here: Administration > Netzwerk > Abfragegruppen

Zeiteinstellungen SNMP-Einstellungen Ereignisbehandlung Abfragegruppen

Schnell Mittel Langsam

Rate (in Sek.): 30 Verschieben Langsam(1000) Mittel(500) 17/250

<input type="checkbox"/>	Zustand	IP-Adresse	Name	Gerätetyp	Einsatzort
<input type="checkbox"/>		172.16.50.11	Nico	SCALANCE XR324-12M (0GG00-1AR2)	NBG
<input type="checkbox"/>		172.16.40.10		DEFAULT_SNMP_Device	Rack 1
<input type="checkbox"/>		172.16.51.11	pn-name-scalance-x204irt	SCALANCE X204IRT (0BA00-2BA3)	front 2 from right
<input type="checkbox"/>		172.16.50.56	cpu-056-cpu-412-2pn-2ek06	CPU 412-2 PN (2EK06-0AB0)	sysLocation not set
<input type="checkbox"/>		172.16.50.51	cpu-051-cpu414-3-pndp-3em05	CPU 414-3 PN/DP (3EM05-0AB0)	sysLocation not set
<input type="checkbox"/>		172.16.50.64	Paulchen	SCALANCE X224 (0BA00-2AA3)	
<input type="checkbox"/>		172.16.51.2	X308-2M-ip110-10	SCALANCE X308-2M POE (2QG00-2AA)	sysLocation Not Set
<input type="checkbox"/>		172.16.51.1	oben-mitte	SCALANCE X308-2M POE (2QG00-2AA)	sysLocation Not Set
<input type="checkbox"/>		172.16.51.3		SCALANCE X308-2M (2GG00-2AA2)	sysLocation Not Set
<input type="checkbox"/>		172.16.50.5		Management Station	
<input type="checkbox"/>		172.16.50.53		CP 443-1 IT (1GX11-0XE0)	
<input type="checkbox"/>		172.16.50.54		CP 443-1 TCP (1EX00-0XE0)	
<input type="checkbox"/>		172.16.50.55		CP 443-1 (1EX02-0XE0)	
<input type="checkbox"/>		172.16.50.57	cp-057-cp-443-1-1ex30	CP 443-1 (1EX30-0XE0)	
<input type="checkbox"/>		172.16.50.52	cp-052-cp443-1-1ex20	CP 443-1 (1EX20-0XE0)	

Page 1 of 2 View 1 - 15 of 17

Meaning

A polling group is a device group whose UP/DOWN status is polled at a certain interval (polling rate). 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 your 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.




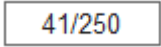
Note

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:

Icon	Display / function	Icon	Display / function
	Polling rate in seconds	Fast (150)	Transfer selected (✓) devices to the "Fast" polling group *
Slow (120)	Enter selected (✓) devices in the "Slow" polling group *	Medium (50)	Transfer selected (✓) devices to the "Medium" polling group *
	Enter text for text search		Start text search
	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

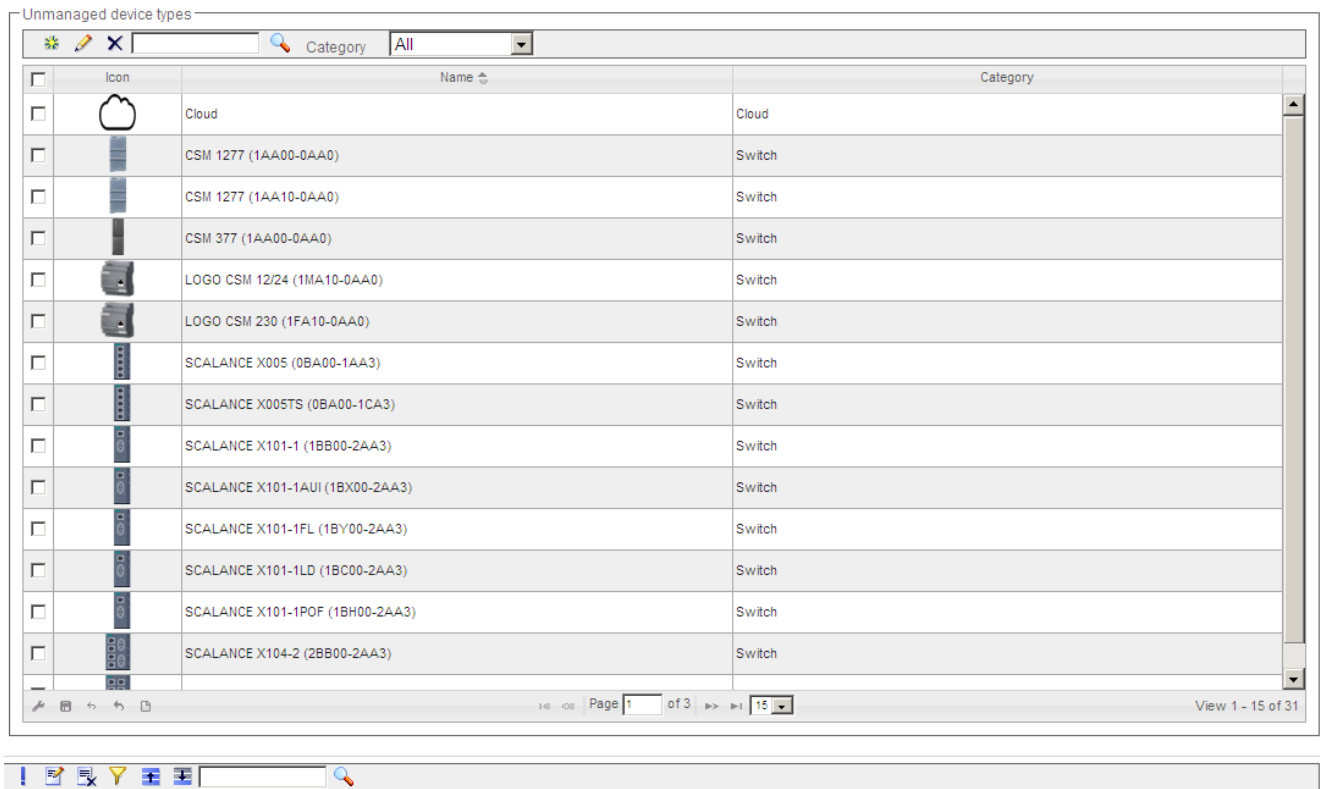
Setting up polling groups - procedure

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.

4.4.4 Administration - "Unmanaged" device types

You open the Web page shown below using the menu command: **"Administration > Unmanaged devices"**







Layout



The **"Administration > 'Unmanaged' device types"** Web page allows you to manage devices that offer no or only minor options to change the behavior or characteristics of the devices.

Content / operation

The following table explains the function elements of the header:

Icon	Display / function
	Create new device
	Change device data
	Delete device
	Enter text for text search

4.4 Administration

Icon	Display / function
	Start text search
	Filter display based on device category (All, switch, access point, client, terminal, gateway, other device)

In the table below this, the previously known devices are displayed with the their icon, name, device family and category.

4.4.5 Administration - Event types

You open the Web page shown below using the menu command: **"Administration > Event types"**

The Web page contains the following tabs:

- "Traps",
- "Network events"
- "System events".

In these tabs, you can configure traps and events.

As soon as there are status changes or error events in the network, these appear as traps or events in the tabs described here.

The three tabs are nearly identical in the form and content. Therefore, the "Traps" tab is used in the following figure as an example of all other tabs.

The editing dialog for a trap entry is also shown.

4.4 Administration

The screenshot shows the 'Traps' management interface. The main window displays a table of traps with columns for Status, OID, and Trap description. A modal dialog titled 'Traps' is open, showing the configuration for a selected trap. The dialog has fields for Basic data (OID, Class, Text) and an Enable checkbox. The 'Traps' tab is selected in the main window.

Status	OID	Trap description	Info
<input type="checkbox"/>	1.3.6.1.6.3.1.1.5.5	Trap: Authentication	
<input type="checkbox"/>	1.3.6.1.6.3.1.1.5.1	Trap: Cold start re	
<input type="checkbox"/>	1.3.6.1.6.3.1.1.5.2	Trap: Warm start	
<input type="checkbox"/>	1.3.6.1.6.3.1.1.5.3	Trap: Link down r	
<input type="checkbox"/>	1.3.6.1.6.3.1.1.5.4	Trap: Link up rec	
<input type="checkbox"/>	*	Trap received	
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.11	Trap: Redundancy	
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.12	Trap: Redundancy	
<input checked="" type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.13	Trap: Redundancy	
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.21	Trap: Standby manager entered active state	Info
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.22	Trap: Standby manager entered passive state	Info
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.23	Trap: Standby manager lost its partner	Warning
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.24	Trap: Standby manager found again his partner	Info
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.25	Trap: Standby manager partner has wrong version	Warning
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.26	Trap: Standby manager found more than one partne	Warning
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.31	Trap: Power is not redundant	Warning
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.32	Trap: Power supply is redundant	Info
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.2.100.2.1.0.41	Trap: Device entered fault state	Warning
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.4.0.11	Trap: Redundancy manager entered active state	Info
<input type="checkbox"/>	1.3.6.1.4.1.4196.1.1.5.4.0.12	Trap: Redundancy manager entered passive state	Info

Event types - meaning

- "Traps" tab

When certain alarm events occur, devices generate trap frames that can be evaluated by management stations. The trap frames contain error messages in plain text.

- "Network events" tab

Network events provide information about changes or error events in the network.







- "System events" tab

System events provide information about actions, changes and error events of SINEMA Server.

Operator input


The following table explains the function elements of the header.

Icon	Display / function
	Add new trap / event type (only traps and network event) The input dialog is displayed (see above)
	Edit trap / events The input dialog is displayed (see above)

Icon	Display / function
	Delete trap / event (only traps and network event) Note: Traps /network events created by "System" cannot be deleted.
	Change the status of the selected (✓) traps / events (enabled / disabled) Note: Disabled traps / events move to the end of the table.
	Restore the default settings for selected traps / events Note: Traps / events created by "User" cannot be reset.
	Enter text for text search / filter setting
	Start text search / filter setting Result: The traps / events that match the text string specified for the text search are displayed.
	Filter the display according to the following criteria: <ul style="list-style-type: none"> • All • Enabled • Disabled

Content

The events are shown in the form of a table.

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

Parameter	Meaning
"Check box"	Select this option to select all the displayed entries.
Status	Shows the event status (enabled / disabled)
OID (only for "Traps") *)	Object identification The OID is set by the particular network device. If traps are received and the OID is unknown, the OID box in the display remains empty.
Text *)	Contains the configurable event text.
Class *)	Contains the configurable classification.
Original text *)	Contains the text entry specified the first time the trap / event was detected.
Original class *)	Contains the classification that was specified the first time the trap / event was detected.
Originator (only for "Traps")	Specifies the instance that made the initial definition. The following are possible: <ul style="list-style-type: none"> • System • User

*) Can be edited by double-clicking in the input dialog.

Input dialog - special features

The entry in the text boxes is language specific. If you write to the text box directly, the text is stored under the currently set language.

If you click the globe symbol beside the text box, you open an additional dialog in which you can make the entries for the permitted languages.

See also

Administration - Network Event reactions (Page 174)

4.4.6 Administration - OPC

You open the Web page shown below using the menu command: **"Administration > OPC"**

Possible devices

Device index	Device name	Device type
SN_DV_Mon_CPU_28	kati	CPU315F-2 PN/DP (2FJ14-0AB0)
SN_DV_Mon_CPU_29	CPU 412-2 PN/DP	CPU412-2 PN (2EK06-0AB0)
SN_DV_Mon_CPU_30	CPU 414-3 PN/DP	CPU414-3 PN/DP (3EM05-0AB0)
SN_DV_Mon_CP_22	-	CP 343-1 Adv (1GX30-0XE0)
SN_DV_Mon_CP_23	vera	SIMATIC_S7_300_CP_Advance
SN_DV_Mon_CP_24	cp-052-cp443-1-1ex20	CP 443-1 (1EX20-0XE0)
SN_DV_Mon_CP_25	petra	CP 343-1 Adv (1GX30-0XE0)
SN_DV_Mon_CP_26	unknown	CP 443-1 Adv (1GX30-0XE0)
SN_DV_Mon_CP_27	cp-057-cp-443-1-1ex30	CP 443-1 (1EX20-0XE0)
SN_DV_Mon_CP_39	-	CP 443-1 (1EX02-0XE0)
SN_DV_Mon_CP_40	-	CP 443-1 TCP (1EX00-0XE0)
SN_DV_Mon_CP_41	-	CP 443-1 IT (1GX11-0XE0)
SN_DV_Mon_DefaultDevice_1	-	Management Station
SN_DV_Mon_DefaultSnmpDevic	Moe	DEFAULT_SNMP_Device
SN_DV_Mon_DefaultSnmpDevic	Bart	DEFAULT_SNMP_Device
SN_DV_Mon_DefaultSnmpDevic	TIA-ES	DEFAULT_SNMP_Device
SN_DV_Mon_OSM_ESM_6	desire	OSM
SN_DV_Mon_ScalanceX200_13	siggi	SCALANCE X201-3P IRT (3BH0
SN_DV_Mon_ScalanceX200_15	timo	SCALANCE XF208 (0BA00-2A
SN_DV_Mon_ScalanceX200_16	michael	SCALANCE X202-2P IRT (2BH0
SN_DV_Mon_ScalanceX200_42	solli	SCALANCE X204-2LD (2BC00-

Total: 36 Displayed: 36 Selected: 0

Devices visible in OPC

Device index	Device name	Device type
SN_DV_Mon_CPU_31	tina	CPU317-2 PN/DP (2EJ10-0AB0)
SN_DV_Mon_DefaultSnmpAndC	Homer	DEFAULT_SNMP_DCP_Device

Total: 2 Displayed: 2 Selected: 0

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. SINEMA Server also provides the option of making data available using OPC.

For more information on the topic of OPC in SINEMA Server, see also the section Data exchange via OPC (Page 199)

Layout






In the **"Administration > OPC"** window, you can select devices whose data is to be sent to an OPC server. This allows this information to be evaluated and monitored by (any) OPC clients.

Operation / content

The window contains two areas next to each other, each with the same basic layout. When you first open the window, the left-hand area contains all the devices discovered in the network. The right-hand area (initially empty) contains all the devices intended to make data available via the OPC.


With a toolbar between the two areas, you can move devices from one window at the other.

The following table explains the function elements of this toolbar.

Icon	Display / function
	Move all devices from the right area to the left area
	Move all selected (✓) devices from the right area to the left area
	Move all selected (✓) devices from the left area to the right area
	Move all devices from the left area to the right area
	Save settings (device lists)

The headers of both areas contain a text box for a text filter. It is sufficient to enter a text fragment of any kind and press Return (<Enter> / <Return>). SINEMA Server then displays only the devices in which this fragment occurs in any field (even if it not displayed).

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 arrange it any way you wish ( in the footer). You can choose from all the device properties as those available via the device window and the device details.

See also

Device details (Page 105)

4.4.7 Administration - User

Overview

The "**Administration > User**" Web page has the following tabs:

- "User"
- "Groups"
- "Change password".

The following explains the form, content and functionality of these tabs.

4.4.7.1 Administration - User User

You open the Web page shown below using the menu command: "**Administration > User > User**"

The figure shows the Web page with the User editor opened.

4.4 Administration

User

Groups

Change password

All

<input type="checkbox"/>	User name	Full user name	E-mail	View name	User group	Logged in
<input type="checkbox"/>	Administrator	Sinema Administrator	administrator@siemens.com	user1.user2.user3.user4.Anlage1	Administrator	172.16.50.5, 194.138.39.60
<input type="checkbox"/>	Coordinator	Sinema Coordinator	coordinator@siemens.com	user1.user2.user3.user4.Anlage1	Power User	-
<input type="checkbox"/>	Operator	Sinema Operator	operator@siemens.com		Standard User	-
<input type="checkbox"/>	user1	user1	user1@w.dew	user1	Standard User	-
<input type="checkbox"/>	user2	user2	user2@w.dew	user2	Standard User	-
<input type="checkbox"/>	user3	user3	user3@dede.sw	user3	Standard User	-
<input type="checkbox"/>	user4	user4	user4@ad.de	user4	Standard User	-

User editor

User data

Views

View selection

views

user1

user2

user3

user4

Anlage1

Select all




Deselect all



Cancel

Save

Functions

The following table explains the function elements of the header.

Icon	Display / function
	Create a new user This opens the User editor.
	Change user This opens the User editor.
	Delete user
<input data-bbox="354 1597 486 1608" type="text"/>	Enter text for text search / filter

Icon	Display / function
	Start text search / enable filter The user groups containing the specified text in their names are displayed.
	Filter display: <ul style="list-style-type: none">• All• Logged in• Logged off

The data area contains the user data with the following columns:

- User name
- Full user name
- E-mail address
- View name (assigned views)
- User group
- Logged in as (IP address)

If you create or change a user, another window opens with two tabs in which you can enter the user-specific data.

User editor

When you create or modify a user, a further window opens in which you can enter the user data and select the views.

See also

Users and user groups (Page 85)

4.4.7.2 Administration - User Groups

The following figure shows the "Administration > User > Groups" window with the User groups editor opened.

Functions

The following table explains the function elements of the header.

Icon	Display / function
	Create a new user group This opens the User groups editor.
	Change user group This opens the User groups editor.
	Deleting user group
	Enter text for text search / filter
	Start text search / enable filter The user groups containing the specified text in their names are displayed.

All user groups are displayed in the data area.

User group editor

When you create or change a group, another window opens in which you can select the user rights of the respective group. These rights include:

- View all devices
- Administer devices
- Views of the detected topology
- Views of the monitored topology
- Access to network settings
- Use of all reports
- Views of the system information
- Administer users and user groups

Procedure

To create a user group and to assign one or more functions to the user group, follow the steps below in the opened User groups editor:

1. Enter a name for the new user group.
2. Select one or more entries in the table.
3. Select the "Activating..." button to assign the selected functions to the user group.
4. Select the "Deactivating..." button to remove the selected functions from the user group.
5. Select the "Save" button to apply the settings.

See also


Users and user groups (Page 85)

4.4.7.3 Administration - User Change password

Changing the password


The window contains the usual fields for changing a password:

- Previous password
- New password
- Confirm new password

You can save the change using the  icon in the header.

4.4.8 Administration - User interface

The "**Administration > User interface**" Web page includes the "Monitoring refresh interval" box. With the monitoring interval, you specify the number of seconds after which the monitored topology is updated again.

You can save the value using the  icon in the header.

4.4.9 Administration - System information

The "**Administration > System information**" Web page shows you the following information about the management station in the form of a table:

- Computer
 - Processor
 - Main memory
 - Hard disk
 - MAC address
 - IP address(es)
- Operating system
 - Type and version
 - Computer name
 - Computer status
 - Time zone
- SINEMA server
 - License type
 - Version number
 - Revision

4.4.10 Administration - System config

Meaning

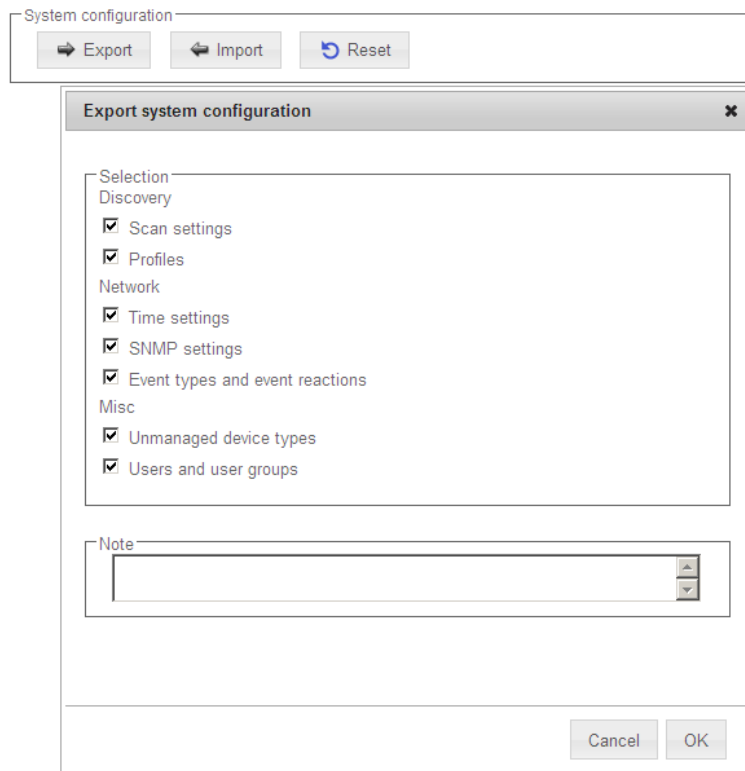
In some cases, it is necessary to save the system configuration, to import a previously used system configuration or to reset the system configuration to the initial values.

Note

Sequence on the management station

The functions described here can only be executed completely on the management station.

With the **"Administration > System config"** menu command, you obtain the following buttons and functions:



- "Export" button

To export the system configuration, click the "Export" button. A dialog box with options is opened (see above) with which you can save the system configuration using a selected path name.

- "Import" button

To import an existing system configuration, click the "Import" button and select the file *.dpl in the dialog that opens.

The function is available before the first network scan.

- "Reset" button

To reset certain settings of the system configuration, click the "Reset" button. A dialog box with options opens (see above) in which you can make your selections.

The function is available before the first network scan.

Note

Windows XP

When using Windows XP it is possible that the system configuration cannot be exported or imported if other programs (e.g. "Computer", "Editor" or "Command prompt") are loaded. In this case, you will need to close these programs before being able to take the required action.

Behavior of read-in profiles

Profiles that have been read in, both those saved earlier as well as "third-party" profiles, are always disabled initially. If a time-consuming check (comparison with all other profiles) was required for activation, this would be impractical and annoying in this situation. You can enable the profiles later after you have saved them using the corresponding icon in the toolbar.

4.5 Server overview

You open the Web page shown below using the menu command: **"Server overview"**

<input type="checkbox"/>	Name	IP	System status					
<input checked="" type="checkbox"/>	Production	172.16.50.5	NO_RESPONSE	-	-	-	-	-
<input type="checkbox"/>	Office	172.16.50.5	NO_RESPONSE	-	-	-	-	-
<input type="checkbox"/>	ServerRoom	172.16.50.5	NO_RESPONSE	-	-	-	-	-
<input type="checkbox"/>	Maintenance	172.16.50.5	NO_RESPONSE	-	-	-	-	-
<input type="checkbox"/>	Infrastructure	172.16.50.5	NO_RESPONSE	-	-	-	-	-

SINEMA Server editor

Hint: User needs to install certificate manually to work with HTTPS.

Basic data

Name:
Protocol:

IP address:
Port:

Authentication

User name:
Password:

Confirm password:

Meaning

On the **"Server overview"** Web page, SINEMA Server provides the option of collecting information about other SINEMA servers in the network.

The possible statuses are each shown in a separate column in the table.

You can set up access to the monitored servers using the functions on this Web page.

Operator input

The following table shows the tab contents of the "Server overview" window with a brief explanation.

Icon	Display / function	Icon	Display / function
	Add new server This function opens a dialog called "SINEMA Server editor".		Edit selected server With this function you open the "SINEMA Server editor" dialog in which you can edit the existing entries.
	Deleting servers	<input type="text"/>	Set polling interval.
<input type="text"/>	Enter text for text search / filter		Start text search / filter setting

Displaying the server overview using HTTPS - requirement

The use of the HTTPS protocol normally prevents the display of the server data (status display: NO RESPONSE). To be able to access the server, you first need to install the server certificate on your client.

Follow these steps:

1. In your Web browser, click the "Certificate error" notification.

This opens a dialog with a message regarding the non-trustworthy certificate.

2. Click the "Show certificate" button.

The certificate window opens.

3. Select the "Install certificate" option and follow the instructions to install the certificate of the relevant server on your client computer.

Data exchange via OPC

5.1 Access via OPC server - options and concept

OPC

The OPC standard (Open Process Control) is used for devices in industrial automation to transfer plant data, alarms and events, historical data and data from batch processes between control devices of different manufacturers in real time. The OPC interface is a standard for the co-operation of differing systems when exchanging data at runtime. Systems of other manufacturers can be connected to the OPC server via OPC clients and read out or monitor the data.

When accessing data, the following types of access must be distinguished:

- 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).

- Data access with OPC (DA)

OPC DA is a standard with specifications for real-time data transfer from data acquisition devices such as PLCs. It is used to provide a display and interface for devices such as HMI devices. SINEMA Server supports the range of functions of OPC DA.

With OPC DA remote access, the DCOM settings must be configured in SINEMA Server.

Accessing SINEMA Server data via an OPC server

Only users with access to SINEMA Server can access project data of SINEMA Server via an OPC server. The OPC server can be accessed via the OPC client. Via the OPC server, in turn, the configuration data of SINEMA Server and the properties of the network devices can be accessed. For interaction with an OPC server, any OPC client can be used. With the help of the OPC server, you can display runtime data and properties of a SINEMA Server project and also change the values of runtime data.

Note

For remote access to SINEMA Server data, the OPC client must be installed locally on your computer. Before OPC connections can be set up, an OPC view with a list of network devices is required. You can create an OPC view on the Administration > OPC page. Whenever the OPC view changes (when new devices are detected or existing devices are deleted), all connected OPC clients must be disconnected and then reconnected to the OPC server so that the latest devices are displayed in the OPC view.

5.2 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.

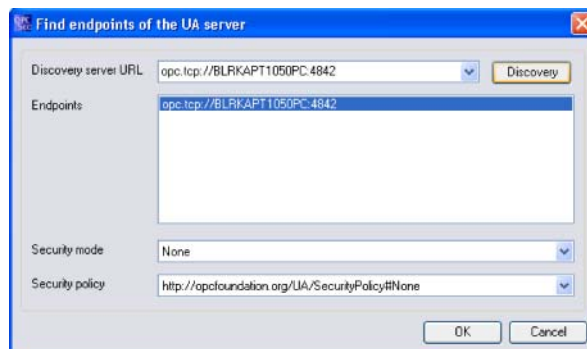
Configuring UA ports

The default port used for a UA server is 4840. This port can be configured using the configuration option in the shortcut menu of the "SINEMA Server Monitor" sub window. To access this shortcut menu, right click on the icon for the sub window "SINEMA Server Monitor" in the Windows system tray. A window with a list of options is then displayed.

You will find more detailed information on configuring a UA port in "*Basic steps in operation*" in section 4.1.

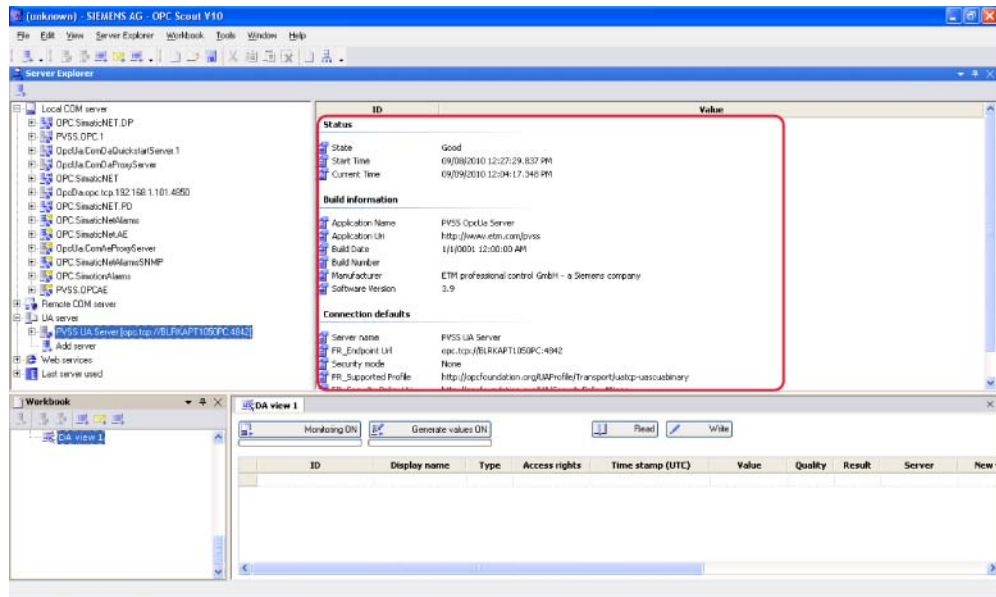
Accessing SINEMA Server data via an OPC server (OPC UA)

1. To start the OPC Scout client, click Start > Programs > SIMATIC > SIMATIC NET > OPC Scout in Windows.
2. Expand the folder of the UA server in the navigation area of the Server Explorer window.
3. Click on the "Add server" entry. The "Find endpoints of the UA server" dialog opens.
4. In the "Discovery server URL" input box, enter the discovery URL and IP address or the computer name and port number of the discovery server.
5. Enter the security options as shown below and click OK.



6. The connected UA server is now listed in the navigation tree structure in the UA server folder.

7. Click on the server to display the connection status and the default settings of the connection. This information is displayed in the right half of the Server Explorer window.

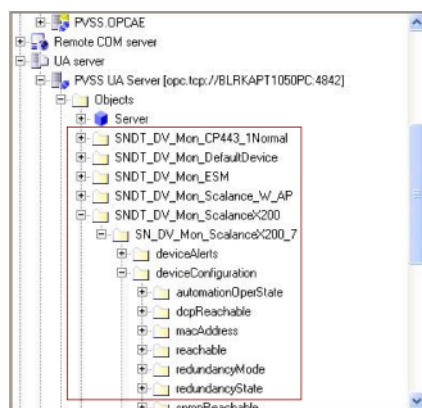


8. Expand the connected UA server to display the list of network devices. The folder name beginning with "SNDT_DV_Mon", specifies the name of the network device.

Note

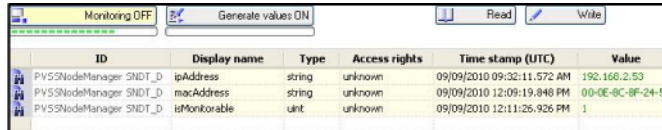
In the navigation pane, only objects added to the OPC view are displayed.

9. The boxes displayed under **Network > All**, correspond to the names of the device properties available as folders in the "Device configuration" folder.



10. Note that a view for the UA server has already been created in the workbook area.
11. Drag the required device elements to the view area below.
12. Click the "Read" button at the top edge of the view area. This starts reading out of the values for the individual device properties of the selected device (see below).
13. As an example, in the map below, you can see the values for the device properties "IP address", "MAC address" and "Is monitorable". Since the device is in the monitored status, the value for this property is listed as "1".

14. By clicking "Monitoring ON", you can display or track changes to these devices. All the changes to these devices or device properties are updated at the same time in the value box.



ID	Display name	Type	Access rights	Time stamp (UTC)	Value
PVSSNodeManager SMDT_D	ipAddress	string	unknown	09/09/2010 09:32:11.572 AM	192.168.2.53
PVSSNodeManager SMDT_D	macAddress	string	unknown	09/09/2010 12:09:19.848 PM	00-0E-8C-8F-24-5
PVSSNodeManager SMDT_D	isMonitorable	uint	unknown	09/09/2010 12:11:26.926 PM	1

15. If the network device with IP 192.168.2.53 was changed to the non-monitored status using the **Administration > Event list** page, the value for the monitoring status changes to "0" for "not monitored".
16. The steps for displaying other device properties are similar to those described here. This means that you can call up the data of all network devices detected by the SINEMA Server application.

5.3 Data access with OPC (DA)

OPC DA is a standard with specifications for real-time data transfer from data acquisition devices such as PLCs. It is used to provide a display and interface for devices such as HMI devices. SINEMA Server supports the range of functions of OPC DA.

5.3.1 Configuring DCOM settings in SINEMA Server

With OPC DA remote access, the DCOM settings must be configured in SINEMA Server. The explanations in this section describe how to configure the DCOM settings in SINEMA Server.

Requirements

- Data execution prevention (DEP) settings:

By default, data execution prevention is enabled for all programs. If this option is disabled, change the option to "Turn on DEP for essential Windows programs and service only" by selecting the radio button. The "DEP" tab is part of the "Performance options" window. It can be accessed from the "System properties > Advanced" tab. Right click on the "My Computer" icon and select the "Properties" option to view the system properties.

Note

The steps involved in configuring the DCOM settings in SINEMA Server apply to the Windows Server 2003R2 operating system.

Note

In Windows XP, it is advisable to disable the Windows firewall briefly while making the settings for the DCOM configuration and testing the remote connection of the OPC server. Once the connection is established, the Windows firewall must be re-enabled with exceptions to allow the connection to the OPC server.

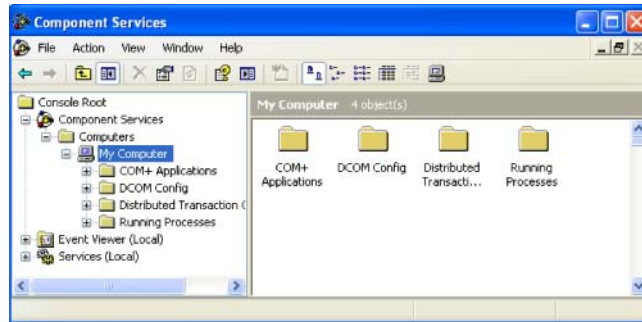
Setting up the properties of the DCOM configuration for OPC DA communication

The settings required in the DCOM configuration for OPC DA communication involve the following steps:

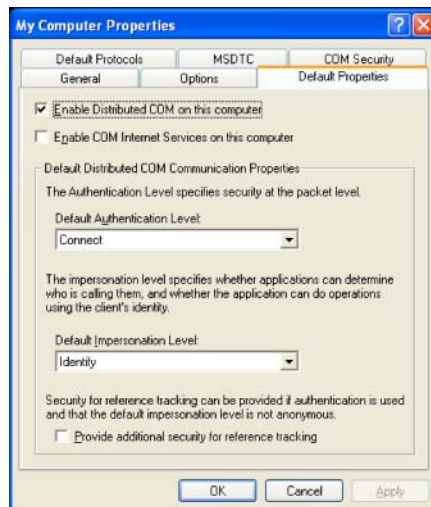
- Configuring default DCOM settings
- Configuring DCOM settings for the OPC server
- Configuring DCOM settings for the OPC server browser
- Restarting the system

Configuring default DCOM settings - procedure

1. In Windows, select the command "Start > Run". In the "Open" list box, enter the command "dcomcnfg" and confirm with OK.
2. The "Component Services" window then opens with the folder hierarchy.

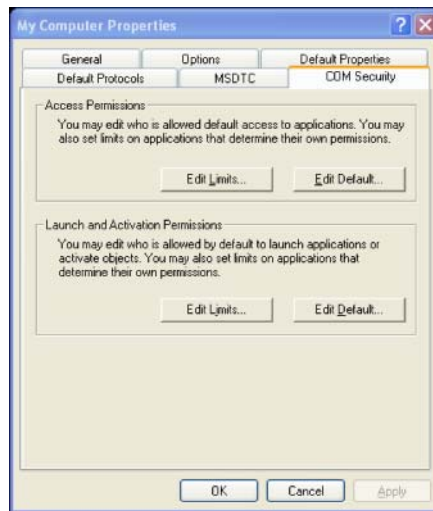


3. Go to the component services, Computers, My Computer.
4. Right click on "My Computer" and select the "Properties" option to open the "My Computer Properties" window.
5. Enter a brief description for your computer and confirm with "OK".
6. Go to the "Default Properties" tab and enter the default authentication level by selecting the "Connect" option in the drop-down list.



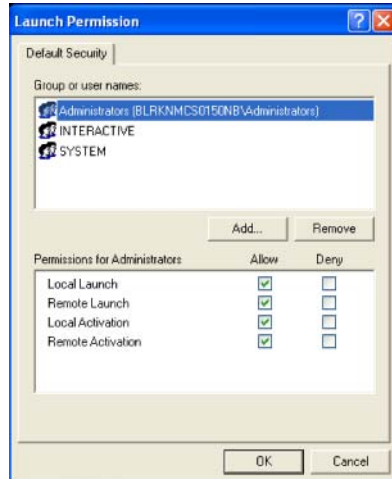
7. In the drop-down list for the default impersonation level, select the "Identify" option and confirm with "OK".
8. In the "Default Protocols" tab, move the "Connection-oriented TCP/IP protocol" entry to the first position in the list under "DCOM Protocols" and remove other protocols that are not being used.

9. Then open the "COM Security" tab. Here, go to the "Access Permissions" section.



10. Under "Access Permissions", click the "Edit Default" button to call the "Launch and Activation Permissions" window. Here, select the list of users on the computer that have access to the OPC server and OPC server browser.
11. Configure the access permissions according to your requirements by selecting the required options and confirming with "OK".
- To allow all users access, add the domain group "Everyone".
 - If the server and client are in the same network domain, add the list of users who will access the OPC server. You should also allow these users both local and remote access.
 - To deny access for all users, create a domain group and add the users for whom access to the OPC server and the OPC server browser is allowed. Then add the group to the "Group or user names" list.
12. Make sure that the "SYSTEM" group is shown in the "Group or user names" list and that the "Allow" check box is selected for local and remote access. If the group has not been added, you can add it with the "Add" button. Next, click the "OK" button.

13. Under "Launch and Activation Permissions", click the "Edit Default" button to open the "Launch Permission" window. Here, select the list of users that can start the OPC servers and OPC server browsers on this computer.

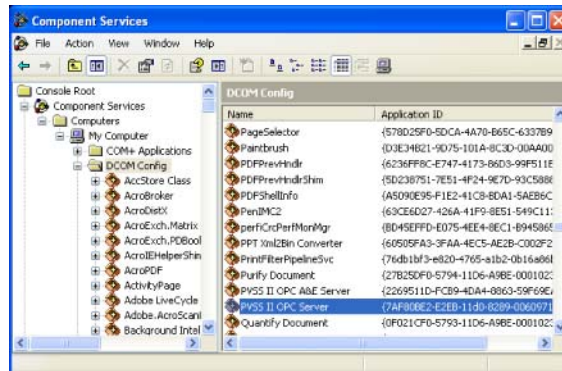


14. Configure the launch permissions by selecting the required options and confirming with "OK".
- To allow all users access, add the domain group "Everyone".
 - If the server and client are in the same network domain, add the list of users who will access the OPC server. You should also allow these users both local and remote access.
 - To deny access for all users, create a domain group and add the users for whom access to the OPC server and the OPC server browser is allowed. Then add the group to the "Group or user names" list.
15. Make sure that the "SYSTEM" group is shown in the "Group or user names" list and that the "Allow" check box is selected for local and remote access. If the group has not been added, you can add it with the "Add" button. Next, click the "OK" button.

5.3.2 Configuring DCOM settings for the OPC server

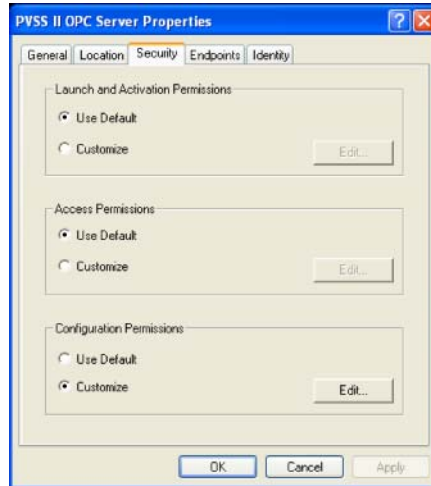
Procedure

1. Expand the "My Computer" entry in the "Component Services" window to show the folder structure.
2. Select the "DCOM Config" folder. The objects this contains are displayed on the right.



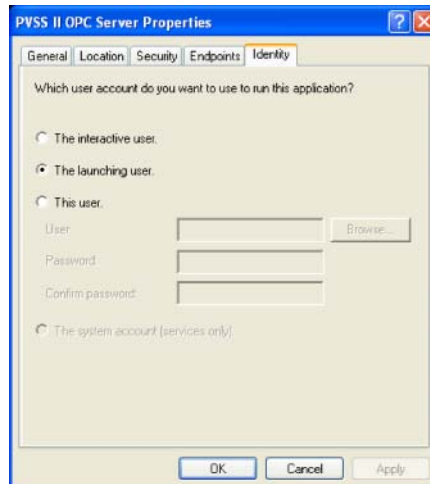
3. In the list view, select "PVSS II OPC Server". Right click on this object and select "Properties".
4. The "PVSS II OPC Server Properties" window is displayed.
5. In the "General" tab, enter "Default" as the authentication level by selecting this option in the drop-down list.
6. The authentication level is nevertheless set to "Connect" because you set this earlier as the default level.
7. In the "Location" tab, select the "Run application on this computer" check box. Deselect all the other check boxes and confirm with "OK".

8. In the "Security" tab, it is advisable to select the option "Use Default" under "Launch and Activation Permissions". If you enable "Customize", you must make sure that suitable OPC server users and/or groups are added.



9. Under "Access Permissions", it is advisable to select the "Use Default" option. If you enable "Customize", you must make sure that suitable OPC server users and/or groups are added.
10. Under "Configuration Permissions", it is advisable to select the "Use Default" option. If you enable "Customize", you must make sure that suitable OPC server users and/or groups are added.
11. Once you have made these settings, click "OK".

12. In the "Default Protocols" tab, move the "Connection-oriented TCP/IP protocol" entry to the first position in the list under "DCOM Protocols" and remove other protocols that are not being used.
13. In the "Identity" tab, the settings you select depend on the intended use of the PC with the server OPC server. Use the settings shown below for unattended or attended operation.



- If there are no users configured for the computer on which OPC server is running, it is advisable to select the "This user" option and specify a user name and password. This setting will allow the OPC server to start even if nobody has logged on to the computer.
- This option can be used if somebody has logged on to the computer.
- Assuming, for example, that the user name is "Captain" and the user domain name is "XYZ", if this option is selected and the server is started locally, the user account must have administrator privileges to make changes to the OPC server configuration.

Configuring DCOM settings for the OPC server browser

1. In the DCOM Config list view, select the "OpEnum" object.
2. Right click on this object and select "Properties".
3. Then, follow the steps 5 to 13 as shown above in the section "Configuring DCOM settings for the OPC server".

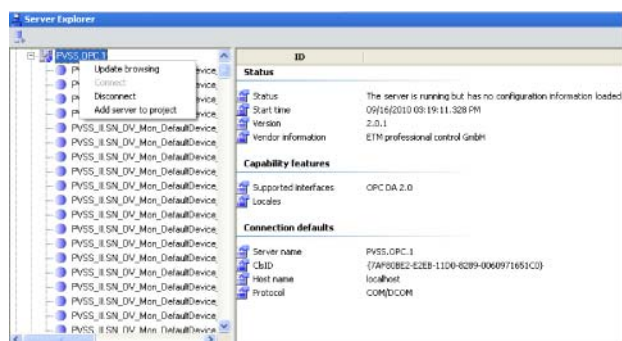
Restarting the system

1. After working through these steps, restart the system.

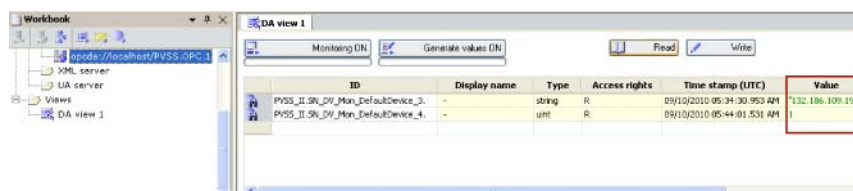
5.3.3 Accessing SINEMA Server data via an OPC server (DA)

Procedure

1. To start the OPC Scout client, click Start > Programs > SIMATIC > SIMATIC NET > OPC Scout in Windows.
2. In the navigation tree displayed on left hand-side of the screen, expand the local COM server.
3. Then, expand the OPC DA server listed further below in the tree hierarchy.
4. The connection to the server is established automatically. The complete list of devices along with the device properties is displayed.



5. The connection status, performance features and connection defaults of the server are displayed on right-hand side of the Server Explorer window.
6. Note that a view "DA view1" for the DA server has already been created in the workbook area.
7. Drag the required device elements to the "DA view1" area.
8. Click the "Read" button at the top edge of the area. This starts reading out of the values for the individual device properties of the selected device (see below).
9. As an example, in the figure below, you can see the values displayed for the device properties "IP address", "MAC address" and "Is monitorable". Since the device is in the monitored status, the value for this property is listed as "1".



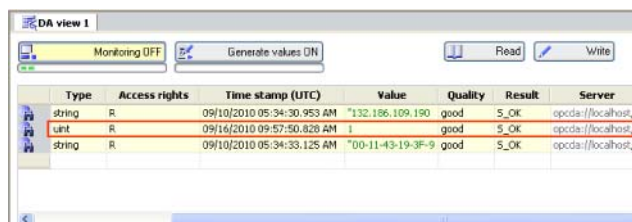
10. Click "Generate values ON" and select the "Read" button to start reading the data from SINEMA Server.
11. By clicking "Monitoring ON", you can display or track changes to these devices. All the changes to these devices or device properties are updated at the same time in the value box.

12. If the network device containing the IP is set to the non-monitored status in SINEMA Server, this value automatically changes to "0" indicating a "non-monitored" status for the network device.



ID	Display name	Type	Access rights	Time stamp (UTC)	Value
PYSS_II_SH_OP_Hna_DefaultDevice_3	-	string	R	09/10/2010 05:34:30.953 AM	"132.186.109.190"
PYSS_II_SH_OP_Hna_DefaultDevice_4	-	uint	R	09/16/2010 09:56:46.968 AM	0
PYSS_II_SH_OP_Hna_DefaultDevice_4	-	string	R	09/10/2010 05:34:33.125 AM	"00-11-43-19-3F-9"

13. When the device containing the specific IP is set back to the monitored status in SINEMA Server, you will see that the value changes to "1" indicating the "monitored" status for the device.



Type	Access rights	Time stamp (UTC)	Value	Quality	Result	Server
string	R	09/10/2010 05:34:30.953 AM	"132.186.109.190"	good	S_OK	opcda://localhost/
uint	R	09/16/2010 09:57:50.828 AM	1	good	S_OK	opcda://localhost/
string	R	09/10/2010 05:34:33.125 AM	"00-11-43-19-3F-9"	good	S_OK	opcda://localhost/

14. The steps for displaying other device properties are similar to those described here. This allows you to view the data of all the network devices discovered by the SINEMA Server application.

Questions and answers

The following sections are intended to give you an additional opportunity to find answers to typical questions relating to the use of SINEMA Server.

A.1 Topic general operator control / installation

Frequently asked questions

How many users can access the Web interface of SINEMA Server as clients at the same time?

Ten users can access the Web interface of SINEMA Server at the same time.

How do I change the password?

To change the password, click "Administration > User > Change password" (tab) in the menu bar of the Web interface of SINEMA Server.

How can I be sure that SINEMA server and the corresponding services have started?

SINEMA server has a status monitoring window that is loaded when Windows is started. This window shows the status of the SINEMA Server application. The loading of the corresponding services is indicated by a progress bar. This window also contains options for starting/stopping the SINEMA Server application as well as options for starting the Web clients.

How can I log in to SINEMA Server in Firefox after disconnecting the network cable?

This problem occurs if the network cable of the computer on which the SINEMA Server application is running is disconnected. The reason is that the browser checks whether "Work Offline" is set. It assumes that the connection is offline so that no login to the SINEMA Server application is possible. To access the application when the network cable is disconnected, deselect the "Work Offline" option in the "File" menu of the Firefox browser. This situation does not occur when working with Internet Explorer.

What do I do if there are setup errors during installation of the SINEMA Server on drive "D:"?

Even if you install the SINEMA Server application on drive "D:", only certain components of SINEMA Server will be installed on this drive. Other components will nevertheless be installed on the Windows drive (drive "C:"). To avoid setup errors, make sure that you have at least 800 MB of free storage space on drive "C:" even if there is enough storage space on drive "D:".

A.2 Topic logging in / starting

Frequently asked questions

What can I do if there is a database crash during forced shutdown of SINEMA Server?

If there is a forced shutdown while working with SINEMA Server, it is possible that the SINEMA Server database will be damaged. The application then no longer starts up correctly. The only remedy in this situation is to reinstall SINEMA Server. To avoid loss of data, it is advisable to back up the system regularly. The backup data can then be called up when necessary using the restore function.

A.3 Topic topology

Frequently asked questions

How do I print out a specific topology view?

Click on the printer icon in the status bar.

How do I change the size of the topology view?

To change the size of the topology view, use the box with the "Select zoom factor" drop-down list in the toolbar of the topology view.

What is the function of the "Symbol view" button in the toolbar of the topology view?

With the "Symbol view" button, you can display network devices in the topology view as icons. If the symbol view is enabled, you can see a larger number of network devices in the topology view compared with the default view. In the symbol view, the IP details such as the IP address and MAC address are shown.

What happens if there are no reference connections defined in the Reference topology editor?

If a user does not define any reference links, but saves a reference, all the devices shown in the editor window become part of the reference but do not have any reference connections. As a result, the devices in the monitored view are displayed as unresolved devices. The next time the Topology editor is called, the devices are still in the hop layers in which they were the last time you saved. The application does not recalculate the hop layers based on the current topology.

When are ring topologies displayed badly in the topology display?

In views, when displaying the topology in the icon view, the following optical malfunction can occur: If you repeatedly recalculate the topology, SINEMA Server represents a ring topology so badly that it is difficult to recognize as a ring.

Remedy: In this case, the positions of the devices involved should be corrected manually.

A.4 Topic network monitoring / scanning / SNMP

Frequently asked questions

How do I specify the interval for refreshing the topology view?

The interval for refreshing the topology view is set in the "UI settings" tab (menu command **"Administration > User interface"**).

How can I divide large scan ranges into smaller scan ranges?

If you know the IP addresses of the devices available in the network, you can divide a large scan range into several smaller ranges by specifying IP address ranges. This reduces the total time required for scanning in the current network.

To specify a scan range, open the "Scan" tab (menu command **"Administration > Discovery"**) and assign a first and last address for the scan using an IP sub range.

Which SNMP security levels are available for SINEMA Server?

The following SNMP security levels are available for SINEMA Server:

- noAuthNoPriv: No authentication, no encryption.
- authNoPriv: Authentication with the MD5 or SHA algorithm, no encryption.
- authPriv: Authentication with the MD5 or SHA algorithm, encryption with the DES/AES/AES 128 algorithm.
- Maximum: Authentication with the MD5 or SHA algorithm, encryption with the DES/AES/AES 128 algorithm.

Does the SINEMA Server application detect a new device if the existing IP address of the device is changed to a new IP address?

In this case, SINEMA Server rediscovers the device during the next scan with the new IP address. This is only the case if the IP address is within the scan range. The old instance of the device with the old IP address is shown as being unreachable. In this case, the application makes sure that no new instance of the monitored device is created. In SINEMA Server, the monitored device has the same MAC address as the device whose IP address was changed.

Speeding up the display / refresh of the performance data

If you enable the port statistics during operation, you will be able to observe the display / refresh of the performance data in the device details initially with a considerable delay (up to ten minutes). To speed up this process (approximately three minutes), you need to execute the "Reread data" command twice (icon in the device list) within two minutes.

A.5 Topic views

Frequently asked questions

What are the user-specific views used for?

With user-specific views, you have the option of monitoring and managing only a specific group of devices instead of all the devices in the network.

A.6 Topic events

Frequently asked questions

How many event reactions can I add for an event?

You can add up to ten event reactions for a specific event.

What purpose does the event acknowledgement function have in SINEMA Server?

By acknowledging an event, you can detect critical events and in some situations deal with them before they become serious. Correcting the situation can be achieved using configured event reactions. In this case, you acknowledge the event for which event reactions were configured in the application.

A.7 Topic migration / import / export

Frequently asked questions

How can I transfer the configuration settings from one SINEMA Server system to another SINEMA Server system?

To adopt the configuration settings of a SINEMA Server system in another SINEMA Server system, you can use the export and import functions of SINEMA Server. The configuration information is stored in the SINEMA Server database. You can export this configuration information from the database to a configuration file in ASCII format (*.dpl). This configuration data of the existing system can then be imported easily into another SINEMA Server system you want to configure.

How can I display the exported SINEMA Server system?

The exported SINEMA Server database is available in ASCII format. You can display the file with Microsoft Word.

A.8 Topic reports

Frequently asked questions

How does SINEMA Server create reports if a device in the network is replaced?

The reports in SINEMA Server contain only the information relating to the new device. The data of the old device is not displayed. The IP address, however, remains unchanged; the device is assigned a new MAC address. If a device is deleted, all the historical data of the device is lost. The subsequent reports then no longer contain data relating to the deleted device.

Windows 2008 Server R2 64-bit: How can I set a date from the past?

If you use Windows 2008 Server R2 64-bit, you cannot normally select a day from the past when specifying a date (e.g. reports).

To be able to do this, you must first enable "Active scripting" in the Internet Explorer.

A.9 Topic Profile editor

Frequently asked questions

Where do I find the profiles in SINEMA Server V12?

The list of profiles can be opened with the menu command **"Administration > Discovery > Profiles"**.

If you cannot find the relevant navigation node, ask your SINEMA Server administrator to assign you the required rights.

What is the difference between general profiles and monitoring profiles?

General profiles are used for discovery and monitoring. Monitoring profiles are used only for monitoring.

In addition to the general profile, a device can also be assigned a monitoring profile. As result, user-specific monitoring rules remain unaffected by changes in the general profile. This is an advantage, for example, when a vendor-specific general profile is replaced by a new profile version.

When should I create a new profile and when should I use an existing profile?

It is advisable to keep the number of profiles as small as possible to retain clarity. To be sure that the system is capable of discovering a new device type, you should first check whether or not a profile already exists to which you can add the new device type. A very simple example might be that a SCALANCE X499 would fit perfectly in an existing SCALANCE X4xx profile.

When are the functions in the "Profiles" tab disabled?

During a network scan, several functions are disabled to avoid inconsistencies.

To avoid an interruption by a network scan when editing a profile, you should temporarily increase the refresh interval or turn off the automatic scan temporarily.

Remember to set the scan parameters again when the action is completed.

How can I recognize which profile is used for a discovered device?

You will find this information in the device details in the "Description" tab. The information required is in the "Discovery and monitoring settings" parameter box

What do I do if a discovered device has been assigned an incorrect data type due to an error in the rules?

You have 2 options:

- **Alternative 1:**

Change the assignment of the device type in the device list using the "Change device type" function.

- **Alternative 2**

1. Correct the rule in the profile you are using.
2. Delete the incorrectly discovered device in the device list in SINEMA Server
3. Start a new discovery.

Does changing the profile have effects on devices that have already been discovered and that use this profile?

No, changes to the profile do not affect devices that have already been discovered.

If you want a modified profile to be used, you will need to delete these devices in SINEMA Server and start a new discovery.

Note, however, that the historical data of a deleted device is not assigned to the newly discovered device.

See also

Setting up network devices individually - using the Profile editor (Page 60)

Administration - Discovery / Profiles (Page 165)

A.10 Topic administration

Frequently asked questions

The server overview cannot be displayed using HTTPS - how do I access the server?

The use of the HTTPS protocol normally prevents the display of the server data (status display: NO RESPONSE). To be able to access the server, you first need to install the server certificate on your client.

Follow the steps below (Internet Explorer):

1. In your Web browser, click the "Certificate error" notification.

This opens a dialog with a message regarding the non-trustworthy certificate.

2. Click the "Show certificate" button.

The certificate window opens.

3. Select the "Install certificate" option and follow the instructions to install the certificate of the relevant server on your client computer.

A.11 Topic Web browser

Frequently asked questions

How can I display path information in the Internet Explorer?

When searching for files (for example uploading icons), the Internet Explorer displays "fakepath" in the path information. If instead of this, you want to see the correct path (all folders), you will need to change the following settings in the Internet options:

- In the Internet Explorer, under "Tools - Internet options - Security - Custom level":
Enable the entry "Include local directory path when uploading files to a server".

How can I display applets in the Internet Explorer?

When using the Internet Explorer 9, 64-bit applets (e.g. graphics in the server overview) are not displayed in newly opened Windows (tabs). To allow these to be displayed, you need to make the following settings in the Internet options:

- In the Internet Explorer under "Tools - Internet options - Security - Trusted sites":
Enter the IP address of the server as a trusted site.

Glossary

SIMATIC NET glossary - note

Below you will find explanations of terminology that are relevant to the product described here or the contents of this document.

Further explanations of the specialist terms used in this documentation can be found in the SIMATIC NET glossary. Refer to the information and the additional links in the preface.

Archive

Archives in SINEMA Server are data records containing historical data for creating reports. Exported data records can, when necessary, be read in again on the same management station from which they were exported.

Discovery

The process in which SINEMA Server scans the network and detects the managed objects in the network automatically.

Dummy devices

Dummy devices are user-defined devices that do not support any protocol. With SINEMA Server, dummy devices are not detected automatically during scanning.

Managed device

Device that can be detected automatically by SINEMA Server when scanning the network.

Management station

The management station is the system on which SINEMA Server is installed.

MIB

MIB (**M**anagement **I**nformation **B**ase) is a formal description of a group of network objects that can be managed using the SNMP protocol (Simple Network Management Protocol).

MTTR

The MTTR time (**M**ean **T**ime **T**o **R**ecovery) is the average recovery time for a device following a failure.

Network device

In SINEMA Server, network devices have certain properties. With this in mind, in the descriptions, terms are used whose meaning in SINEMA Server is defined as follows:

- **Reachable device**
A device that can be reached during discovery and when polling.
- **Monitored device**
A device found during discovery that is monitored.
- **Unmonitored device**
A device found during discovery that is not yet monitored.
- **Discovered device**
The device was found during discovery and could be assigned to a profile.
- **Not uniquely identified device**
The device was found during discovery and could be assigned to a default profile. If necessary, profiles can be adapted or the device settings should be checked.
- **Deleted device**
A device deleted in SINEMA Server that only remains known in conjunction with report data.

Polling

The querying of the status of the managed devices performed at regular intervals.

SNMP community

An SNMP community is group of devices and management stations on which SNMP is run.

Unmanaged device

Device that physically exists but does not support any protocol so that it cannot be discovered during the SINEMA Server scan.

Index

A

- Access rights, 86
- Adapting the scan range, 164
- Add new server, 197
- Adding a background graphic, 81
- Administrator, 86
- Administrator privileges, 35
- Adopting data, 41
- Archive, 38
- Archive management, 151
 - Meaning, 38
- Assigned monitoring profile, 103
- Assigned profile, 103
- Autodiscovery function, 11
- Automatic start, 35
- Automation License Manager, 24

B

- Backup functions, 40
- Basic view, 74
- Bird's eye view, 149

C

- Calculating the storage space that will become free, 39
- Calculations for the availability report, 153
- Calling functions with a URL, 95
 - Authentication, 95
 - Navigation, 96
 - Web pages, 96
- Catalog of new event reactions, 176
- Change monitoring settings, 104
- Change password, 88
- Change the layout of a connection, 84
- Changing the password, 193
- Cleaning up deleted devices in the archive, 38
- Client computer
 - Logging in, 43
- Cloud, 141
- Configuration, 32
- Configuration limits, 20
- Configure node display, 120

- Configure reports, 18
- Configure views, 18
- Configuring cloud connections in the network, 143
- Configuring event reactions,
- Configuring the port, 32
- Configuring the status of the reference port, 142
- Confirm events, 70
- Controlling the profile display and editing profiles, 165
- Create a reference topology with the Reference editor, 18
- Create new device, 103
- Create system backup, 40
- Creating or editing user-defined connections, 82
- Customize device data, 104

D

- Date and time of day, 53
- DCP, 143
- DCP detection type, 164
- DCP icon, 146
- DCP monitoring interval, 173
- DCP reachability, 103
- Default ports, 33
- Default profiles, 61
- Delete archive, 38
- Deleting views, 75
- Details of the redundancy status, 148
- Device discovery using SNMP, 61
- Device editor - view area, 133
- Device hierarchy, 149
- Device hierarchy (new devices), 138
- Device list
 - View-specific, 73
- Device overview, 100
- Device profiles, 18
- Device status, 103
- Device tree, 100
- Device tree and device list, 15
- Device type rule, 62
- Devices
 - Number of monitored, 25
- Discovered topology, 54
- Discovery rule, 62
- Display of an empty topology, 79
- Displaying the server overview using HTTPS, 198

- E**
 - Editing the ZIP file, 39
 - E-mail client function, 20
 - E-mail settings, 175
 - Enable monitoring, 103
 - Error/fault events, 72
 - Evaluating and acknowledging events, 19
 - Event, 69
 - Event details, 69
 - Event list, 68
 - Event overview, 100
 - Event reaction, 66
 - Event reactions, 176
 - Create new, 176
 - Event types, 184
 - Events, 108
 - Filter, 71
 - Setting up and monitoring in SINEMA Server, 66
 - Events /events list, 15
 - Exit SINEMA Server, 30
 - Expert, 108
 - Export archive and delete, 38
 - Export table in CSV format, 92
- G**
 - General profile, 168
 - Generating HTTPS certificates, 34
 - Glossary, 5
- H**
 - Hardware requirements, 26
 - Historical data, 156
 - HMI systems, 21
 - Hop layer, 136
 - HTTP port, 32
 - HTTP port 80, 32
 - HTTPS certificate, 32
 - HTTPS port, 32
- I**
 - ICMP, 51
 - Icon view, 120
 - Import archive, 38
 - Import profiles, 166
 - Importing a system configuration, 196
 - Information events, 71
 - Installation
 - Sequence, 28
 - Time required, 27
 - IP address, 103
 - Duplicate detection, 164
- J**
 - Java Runtime Environment (JRE), 26
- L**
 - LAN ports, 107
 - License downgrade, 25
 - License key
 - Storage location, 24
 - License types with limits to suit the user's needs, 23
 - License upgrade, 24
 - Login, 19
 - First time, 88
 - Login data - default settings, 88
- M**
 - MAC address, 103
 - Main window, 46
 - Management station, 30
 - Logging in, 44
 - Media types, 140
 - Combination, 141
 - Explicit message, 141
 - Menu commands, 89
 - Migration, 41
 - Sequence, 42
 - Minimum requirements, 26
 - Monitor resolution, 27
 - Monitored topology, 54
 - Refreshing, 128
 - Monitoring interval, 194
 - Monitoring profile, 168
- N**
 - Navigation bar, 46
 - Network adapter, 26
 - Network clouds, 58
 - Network events, 156
 - Network monitoring, 51
 - Network scan, 51
 - Effect on the topology discovery, 57
 - Interval, 173

Procedure, 52
 Network topology, 73
 Number of LAN ports, 103
 Number of monitored devices, 25

O

Online help, 93
 OPC, 187
 OPC server, 20
 OPC UA port, 32
 Open WBM, 109
 Operating system, 194
 Supported, 20
 Output reports, 19

P

Page layout
 General functions, 91
 Password, 44
 Polling group, 178
 Port address
 Value 0 (zero), 31
 Port numbers
 Reserved, 33
 Port status, 145
 Power user, 86
 Printing reports, 151
 Processor, 26
 Product range, 13
 Profile, 60
 Add a new device type to an existing profile, 62
 Creating new, 167
 Displaying and editing, 165
 Exporting, 166
 General, 60
 Principle of the use of profiles, 60
 Profile editor, 63
 "Basic Data" tab, 169
 "Device types" tab, 170
 "Discovery rules" tab, 170
 "OID sets" tab, 171
 "Overall status" tab, 171
 Profile search, 166
 Profiles
 Behavior of read-in, 196
 Displaying and editing, 166
 PROFINET device name, 103
 Program objects in SINEMA Server, 14
 Program window, 46

Q

Quick link, 94
 Setting up, 94
 Using, 94

R

RAM, 26
 Reachability, 103
 Recalculate topology, 137
 Receiving SNMP traps, 69
 Recommended requirements, 26
 Redundancy, 108
 Redundancy concepts, 147
 Redundancy mode, 103
 Information, 148
 Redundancy status, 103
 Reference connections, 58
 Reference editor, 138
 Adding new devices, 138
 Adding unmanaged devices, 139
 Display of the connections, 137
 Drawing connections between devices manually, 140
 References for connection lines, 58
 References for port statuses, 58
 References for SNMP, DCP protocols, 58
 Resetting the reference, 137
 Specify a current connection as a reference connection, 140
 Specifying the current connections as reference connections, 140
 Using the selection mode and drawing mode, 136
 Reference port, 142
 Reference topology, 133
 Report type
 Availability, 150
 Events, 150
 Inventory, 150
 Performance, 150
 Reports, 16
 Evaluation time, 150
 Inventory, 155
 Reports with trend charts, 159
 Requirements for SIMATIC Microbox IPC427C, 27
 Requirements for the Web client, 27
 Reread device data, 103
 Reserved port numbers, 33
 Restore system backup, 40
 Ring status, 148

S

- Scan, 162
 - Procedure, 52
- Scan LAN interfaces, 163
- Scanning the network, 18
- Selecting entries in tables, 93
- Server overview, 197
- Service & Support, 5
- Set device basic data, 104
- Set up users / user groups, 18
- Setting scanning parameters, 18
- Setting up polling groups, 180
- SIMATIC NET glossary, 5
- SINEMA Server Monitor, 30
- SINEMA Server status, 35
- SNMP, 143
- SNMP icon, 145
- SNMP reachability, 103
- SNMP settings, 174
- SNMP version, 174
- Software requirements, 26
- Specify SNMP settings, 103
- SSL certificate, 34
- Standard user, 86
- Standby mode, 103
- Start network scan, 163
- Start SINEMA Server, 30
- Start system backup, 30
- Start Web client, 30
- Start window, 100
- Statistical port data, 103
- Status bar, 46
- Status display
 - in SINEMA Server Monitor, 36
- Status monitoring, 144
- Status of protocol-specific device availability, 145
- Stop network scan, 163
- Storage requirements hard disk, 26
- Sub view, 74
- Subnet mask, 51
- System configuration, 195
 - Exporting, 196
 - Importing, 196
- System events, 156
- System information, 194
- System settings, 30
- System status, 100

T

- Table layout

- General functions, 92
- Time stamp, 69
- Topology
 - Active mode, 116
 - Can be mixed with sub view and device display, 79
 - Creating for sub views, 79
 - Detail view, 120
 - Detected / Monitored, 149
 - Draft mode, 116
 - Icon view, 120
 - Modes, 116
 - Monitored, 126
 - Operation in active mode, 117
 - Operation in draft mode, 116
 - Reference, 149
 - Unmanaged devices, 141
- Topology and reference topology, 16
- Topology discovery, 51
 - Principle, 57
- Topology editor
 - Editing modes, 79
- Topology in the views, 77
- Topology scan, 57
- Topology tree, 133
- Training, 5
- Trap frame, 65
- Trend charts, 156
 - Zoom function, 159
- Trial license, 23
- Turn off monitoring, 103
- Types of report, 150

U

- Uninstalling, 29

,

- 'Unmanaged' device types, 181

U

- Unresolved ports, 147
- UP/DOWN status, 178
- User, 88
- User editor, 191
- User group, 192
- User group editor, 193
- User groups, 88
- User interface
 - Language selection, 49

User management, 86
User rights, 27
Using third-party certificates, 34

V

View filter in the View editor, 76
Views, 115
VLAN, 108

W

Warning events, 72
WBM (Web Based Management), 103
Web browser, 26
 Supported, 20
Web client, 30
Web interface, 20
WLAN, 107

