

## SIMATIC NET

### Network management SINEMA Server

#### Operating Instructions

#### Preface

Network management with  
SINEMA Server -  
introduction

**1**

Installing, setting up and  
calling SINEMA Server

**2**

Getting to know SINEMA  
Server - basic functions

**3**

Using SINEMA Server -  
reference section

**4**

Data exchange via OPC

**5**

Questions and answers

**A**

# Datasheet.Directory

## 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

## Trademarks

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

SINEMA, SCALANCE, SIMATIC

## 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 V13.

## New in this edition of the manual

Compared with edition 03, this manual edition includes the following modifications:

The new functions and enhanced functions of product version V13 compared with product version V12 SP1 of SINEMA Server were included:

### New functions:

- SIMATIC monitoring of SIMATIC S7-300 / S7-400 / ET 200 CPUs
- PROFINET monitoring of devices capable of PROFINET IO
- Taking into account the behavior of alternating devices, e.g. when using tool changer devices

### Expansion of existing functions:

- Expansion of the filter options for lists
- Improvement of the navigation between lists and topology representations

## 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 (<https://support.industry.siemens.com/cs/ww/en/ps/15393>)

## See also

Administration - Monitoring General (Page 182)

Alternating devices (Page 120)

Filtering data with filter templates (Page 80)

## Allowance for network utilization by SINEMA Server

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

## 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 license conditions in the following documents on the supplied data medium:

- DOC\_OSS-S7-CM-CP\_74.pdf
- 

## SIMATIC NET glossary

Explanations of many 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 or product DVD

The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should

also be considered. For more information about industrial security, visit <http://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <http://support.industry.siemens.com>.

## Security recommendations

To prevent unauthorized access, note the following security recommendations.

### General

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

You will find information on this at <http://www.siemens.com/industrialsecurity>.

- Only activate protocols you require to monitor the devices.
- Whenever possible, always use the variants of protocols that provide greater security (e.g. SNMPv3, HTTPS etc.).
- Restrict access to the SINEMA Server to qualified personnel.

### SINEMA Server clients

- It is strongly recommended that you use the HTTPS protocol for access to the Web user interface of SINEMA Server. The data is transferred encrypted and cannot be read by unauthorized third persons.
- Keep the Java Runtime Environment up to date on the clients.
- Keep the Web browser you are using up to date on the clients.

### Passwords

- Define rules for the use of the software and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you use the software.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

## Keys and passwords

This section deals with the security keys and certificates you require to set up SSL.

- We strongly recommend that you create your own SSL certificates and make them available.

How you generate HTTPS certificates is described in the following section of this manual:  
Port settings (Page 28)

- We recommend that you use certificates with a key length of 2048 bits.

## Automation License Manager

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

## Assumptions

We assume the following situation:

- SINEMA Server, monitored devices and OPC clients are protected by a firewall.
- It is certain that access to the SINEMA Server via the Internet is only possible using security mechanisms such as SSL-VPN.

# Table of contents

	<b>Preface .....</b>	<b>3</b>
<b>1</b>	<b>Network management with SINEMA Server - introduction .....</b>	<b>11</b>
1.1	Area of application and functions.....	11
1.2	Overview of the program functions .....	13
<b>2</b>	<b>Installing, setting up and calling SINEMA Server .....</b>	<b>19</b>
2.1	Performance characteristics of SINEMA Server .....	19
2.2	Installing and uninstalling software .....	20
2.2.1	License information .....	20
2.2.2	Installing SINEMA Server - requirements and procedure.....	22
2.2.3	Uninstalling SINEMA Server .....	25
2.3	Configuring and starting SINEMA Server .....	25
2.3.1	SINEMA Server Monitor.....	26
2.3.1.1	Status display .....	27
2.3.1.2	Port settings .....	28
2.3.1.3	Device profile synchronization .....	32
2.3.1.4	Archive management .....	35
2.3.1.5	Data backup and restore .....	36
2.3.2	Java applets .....	37
2.3.3	Start SINEMA Server .....	37
2.4	Migrating a SINEMA Server configuration .....	38
2.5	Web user interface .....	38
2.5.1	Logging in to the Web interface of SINEMA Server .....	38
2.5.2	SINEMA Server user interface on the Web interface .....	41
<b>3</b>	<b>Getting to know SINEMA Server - basic functions .....</b>	<b>47</b>
3.1	Detecting devices in the network .....	47
3.1.1	Overview .....	47
3.1.2	Scanning in the network .....	48
3.2	Visualizing the network topology / monitoring network devices .....	50
3.2.1	Topology - Overview .....	50
3.2.2	Topology discovery .....	52
3.2.3	Setting up monitored topology with the reference topology.....	52
3.3	Setting up network devices individually - using the Profile editor .....	53
3.3.1	Profile concept .....	53
3.3.2	Setting up profiles and assigning device types.....	55
3.4	Configuring event reactions - displaying events .....	58
3.5	Setting up and using views .....	62
3.5.1	Setting up views .....	62
3.5.2	The View editor .....	65
3.5.3	Creating a view-specific topology .....	66

3.5.4	Configure connections .....	69
3.6	Users and user groups.....	72
3.6.1	SINEMA Server users and roles concept .....	72
<b>4</b>	<b>Using SINEMA Server - reference section.....</b>	<b>75</b>
4.1	Program user interface in detail - overview of the menus .....	75
4.1.1	User interface.....	75
4.1.1.1	Filtering data with filter templates .....	80
4.1.2	Online help .....	82
4.1.3	Quick links.....	83
4.1.4	Calling functions with a URL .....	84
4.1.5	Start window.....	94
4.1.6	Device tree .....	95
4.1.7	Device window with device list.....	98
4.1.8	Device window with interface list .....	104
4.1.9	Device details.....	107
4.1.10	Device details - subcategories .....	113
4.1.10.1	Detailed information LAN ports .....	113
4.1.10.2	Detailed information WLAN.....	116
4.1.10.3	Editor for detailed information on (W)LAN ports .....	117
4.1.10.4	Detailed information redundant ports.....	118
4.1.11	Alternating devices.....	120
4.1.12	Views.....	121
4.1.12.1	Views - Overview .....	121
4.1.12.2	Views - topology / Topology editor.....	122
4.1.13	Event list.....	125
4.2	Topology .....	131
4.2.1	Topology - Discovered .....	131
4.2.1.1	Meaning and how it works .....	131
4.2.1.2	Icons and colors in the discovered topology .....	135
4.2.2	Topology - Monitored .....	136
4.2.2.1	Meaning and how it works .....	136
4.2.2.2	Icons and colors in the monitored topology .....	137
4.2.3	Topology - Reference .....	141
4.2.3.1	Meaning and how it works .....	141
4.2.3.2	Reference editor / how it works and modes.....	146
4.2.3.3	Reference editor / including devices .....	148
4.2.3.4	Reference editor / configuring connections .....	149
4.2.3.5	Reference editor - additional configuration options .....	152
4.2.3.6	Icons and colors in the reference topology .....	154
4.2.4	Topology - Unmanaged device types .....	156
4.2.5	Topology - special features.....	157
4.3	Reports.....	158
4.3.1	Reports - Availability .....	160
4.3.2	Reports - Performance.....	162
4.3.3	Reports - Inventory .....	164
4.3.4	Reports - Events .....	165
4.3.5	Historical data and trend charts .....	167
4.3.5.1	Historical data .....	168
4.3.5.2	Trend charts.....	169



4.4	Administration .....	172
4.4.1	Administration - Discovery / Scan .....	172
4.4.2	Administration - Discovery / Profiles .....	175
4.4.2.1	The Profile editor .....	177
4.4.3	Administration - Monitoring .....	182
4.4.3.1	Administration - Monitoring .....	182
4.4.3.2	Administration - Monitoring General .....	182
4.4.3.3	Administration - Monitoring SNMP settings .....	185
4.4.3.4	Administration - Monitoring Polling groups .....	186
4.4.3.5	Administration - Monitoring OPC .....	189
4.4.4	Administration - Events .....	190
4.4.4.1	Administration - Events Event types .....	190
4.4.4.2	Administration - Events Overall status groups .....	193
4.4.4.3	Administration - Events > Event reactions .....	198
4.4.5	Administration - User .....	200
4.4.5.1	Administration - User User .....	200
4.4.5.2	Administration - Users user groups .....	202
4.4.5.3	Administration - User Logon locks .....	204
4.4.6	Administration - System .....	204
4.4.6.1	Administration - System System information .....	204
4.4.6.2	Administration - System configuration .....	205
4.4.6.3	Administration - System / E-mail settings .....	205
4.4.7	Administration - My settings .....	206
4.4.7.1	Administration - My settings Password .....	206
4.4.7.2	Administration - My settings User interface .....	206
4.5	Server overview .....	207
<b>5</b>	<b>Data exchange via OPC .....</b>	<b>211</b>
5.1	Access via OPC server - options and concept .....	211
5.2	Data access with OPC (UA) .....	212
5.3	Data access with OPC (DA) .....	215
5.3.1	Configuring DCOM settings in SINEMA Server .....	215
5.3.2	Configuring DCOM settings for the OPC server .....	219
5.3.3	Accessing SINEMA Server data via an OPC server (DA) .....	221
<b>A</b>	<b>Questions and answers .....</b>	<b>225</b>
A.1	Topic general operator control / installation .....	225
A.2	Topic logging in / starting .....	226
A.3	Topic topology .....	227
A.4	Topic network monitoring / scanning / SNMP .....	228
A.5	Topic views .....	230
A.6	Topic events .....	230
A.7	Topic migration / import / export .....	231
A.8	Topic reports .....	231
A.9	Topic Profile editor .....	231
A.10	Topic Web browser .....	233

A.11      Subject SIMATIC monitoring..... 234

**Glossary .....235**

**Index .....237**

# Network management with SINEMA Server - introduction

# 1

## 1.1 Area of application and functions

The complexity and the number of nodes in Ethernet-based production networks are growing constantly due to increasing requirements. The failure of individual devices in such networks can mean loss of production and, in the worst case, bring the production chain to a standstill. To minimize unproductive times and the resulting costs, transparency of networks with continuous network monitoring is indispensable.

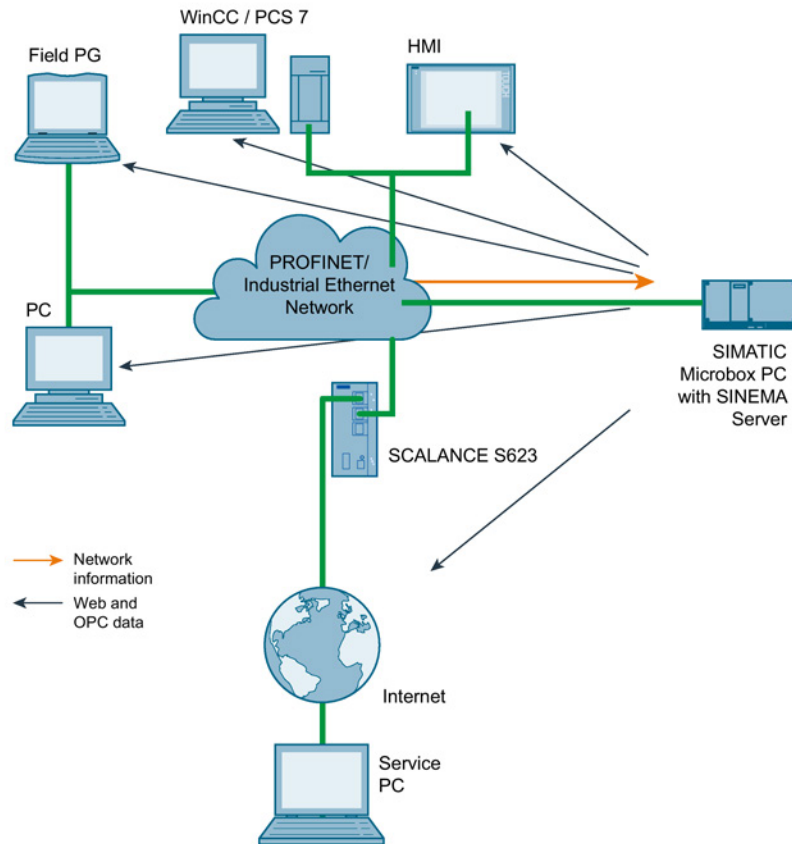
The network management software SINEMA Server is designed specifically for the requirements of industrial communication and monitors devices in the network such as:

- 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 help of extensive diagnostics and reporting functions, SINEMA Server ensures that network problems are recognized early and can be dealt with.

## Integration of SINEMA Server

The following graphic is a schematic representation of the integration of SINEMA Server in a network to be monitored.



- Management station with SINEMA Server

The SINEMA Server application runs on a SIMATIC Microbox or on a PC. The device on which the SINEMA Server runs is known as the management station. The management station is a node in the network to be monitored.

- Web client for accessing SINEMA Server

The network is monitored using Web browsers on the clients. The management station itself can also be used as a client.

- OPC server

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.

## 1.2 Overview of the program functions

### Automatic device detection

SINEMA Server discovers devices in the network automatically and obtains their device information. Cyclically, SINEMA Server polls the overall status of every discovered device and highlights this in color.

Status	IP address	PROFINET device name	Device type	MAC address	Active SIMATIC/F	SiSe receiver
	190.171.3.19	cpu319	CPU 319-3 PN/DP (3EL01-0AB0)	00:0E:8C:F8:B4:AE		Yes
	190.171.0.70	pn-io	CPU 414-3 PN/DP (3EM05-0AB0)	00:0E:8C:98:B8:79		No
	190.171.0.60	pn-io-2	CPU 315-2 PN/DP (2EH13-0AB0)	00:0E:8C:8A:68:F6		Yes
	190.171.0.65	cpu414-65	SIMATIC_S7_400_PL	00:1B:1B:AF:AE:4B		Yes
	190.171.0.88	et200pro-88	ET200PRO PN/DP CPU (8AB01-0AB0)	00:0E:8C:C9:06:95		Yes
	190.171.3.10	cpu412-3-10	CPU 412-2 PN (2EK06-0AB0)	00:1B:1B:A0:F4:45		Yes
	190.171.3.9	et200s-cpu	ET200S PN/DP CPU (8AB01-0AB0)	00:0E:8C:F6:07:2A		Yes
	190.171.3.15	cpu315-3-15	CPU 315-2 PN/DP (2EH14-0AB0)	28:63:36:0C:0E:1F		Yes
	190.171.0.150+	cpu1516-3pn-150.profinet-schnittstelllexb13b0	CPU 1516-3 PN/DP (3AN00-0AB0)	00:1B:1B:13:86:C1+		-

For more detailed information, refer to the following sections:

- Device discovery: Detecting devices in the network (Page 47)
- Detecting overall device statuses: Administration - Events Overall status groups (Page 193)

## Device display with device profiles

The display schemes for devices discovered in SINEMA Server are specified in so-called device profiles that are assigned to the devices automatically when they are discovered by SINEMA Server. If a device has been assigned to a device profile, it is displayed with the device details stored in the relevant device profile.

**Profile (ELS)**

Basic data | Discovery rules | Device types | OID sets | Thresholds

Basic data

Name: ELS ID: ELS

Device category: Switch Family: SIEMENS\_Basic


Description: Industrial Ethernet Electrical Lean Switch

Vendor: Siemens AG Use for discovery: ☐

Create on: 2014-03-13 23:06:52.00 System defined: ☒

Updated on: 2014-03-13 23:06:52.00

Default icon

 ELS.png Browse

Cancel OK

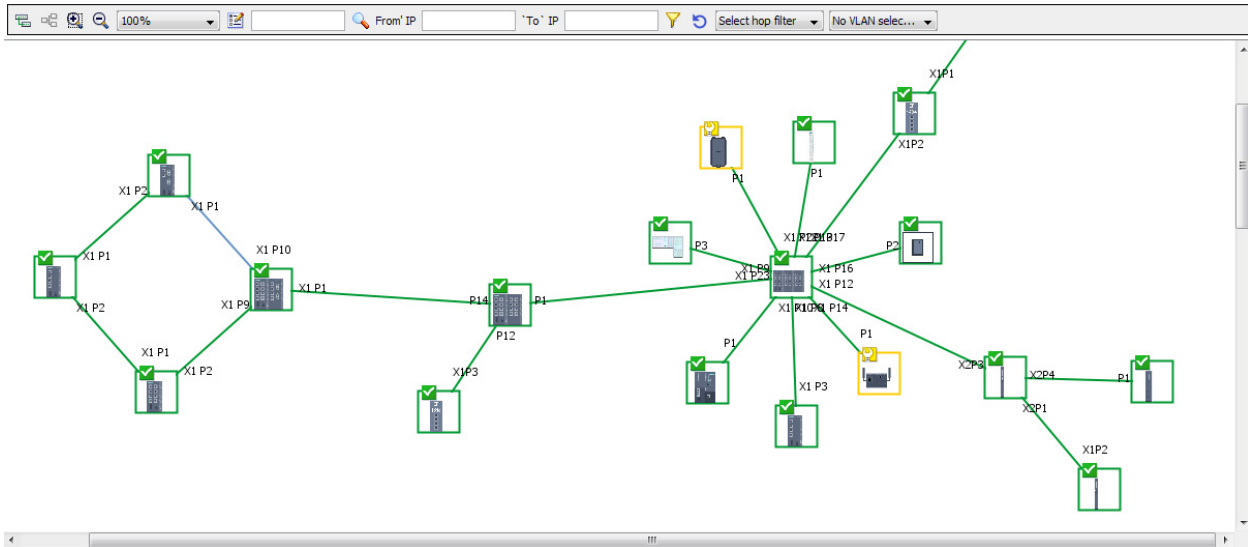
Device profiles access the information of devices via SNMP and SIMATIC / PROFINET. The devices that are supported by device profiles include SCALANCE W, SCALANCE X and SCALANCE S, SIMATIC NET CPUs 300/400/1200/1500 and SIMATIC NET CPs 200/300/400. When necessary, the Profile editor can be used to create your own device profiles based on existing device profiles.

For more detailed information on device profiles, refer to the following sections:

- Setting up network devices individually - using the Profile editor (Page 53)
- Administration - Discovery / Profiles (Page 175)

## Network monitoring with network topologies

The device information discovered by SINEMA Server also includes the position of the devices within networks. With the help of the SNMP and PROFINET protocols, SINEMA Server reads out the position information calculates a topology display using the LLDP protocol in which the detected connections between devices are shown. In the topology display, the devices can be arranged as required to improve clarity and a background image such as a plant plan can also be added. To monitor the devices, expected statuses for connectors, connections and protocol availability can be defined in the topology display. Deviations between the actual and expected statuses are then highlighted graphically.

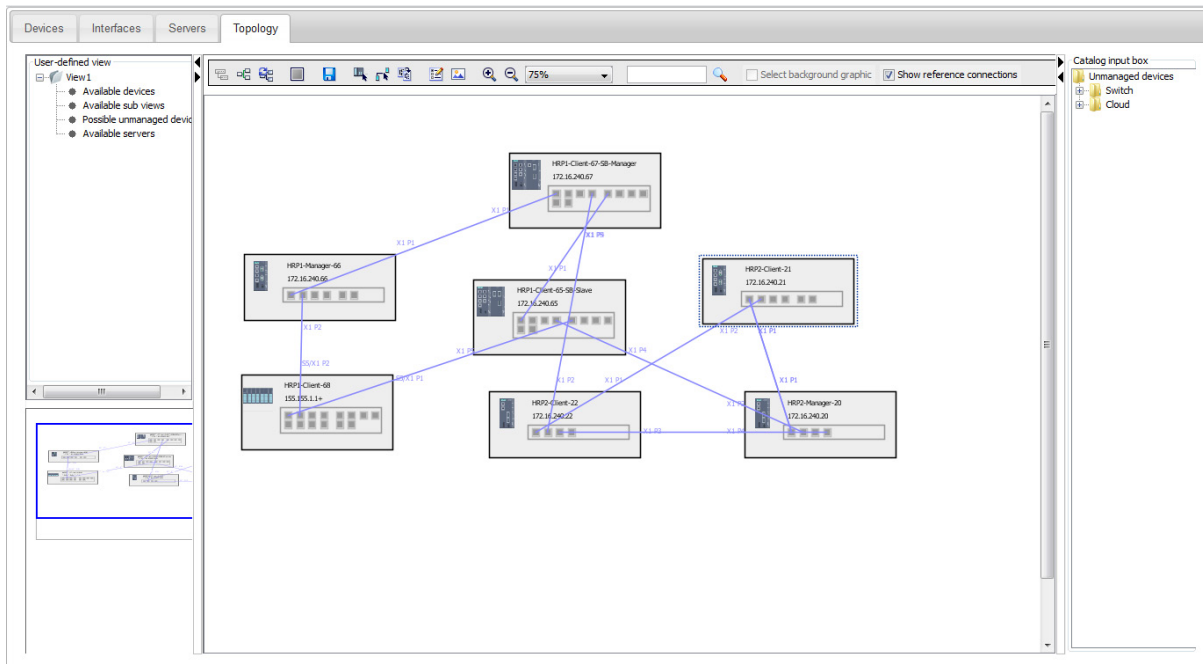


For more detailed information on the topology display, refer to the following sections:

- Visualizing the network topology / monitoring network devices (Page 50)
- Topology (Page 131)

## User-specific network monitoring

The number and appearance of the devices visible in SINEMA Server can be configured for specific users. To achieve this, you can define sections of the network monitoring as views by assigning the devices to be monitored to the views.



For each view, an additional topology display can be generated in which the assigned devices can be freely arranged. You then assign the created views to the required users.

You will find more detailed information on views and assigning users in the following sections:

- Setting up and using views (Page 62)
- Views (Page 121)
- Administration - User (Page 200)

## Events

Events such as a change in the reachability status of a monitored device are detected by SINEMA Server and recorded in an event history.

	Noted	Event status	Event	Event class	Time stamp	Event details	IP address - affected
<input type="checkbox"/>	No	-	Device monitoring: One of the devices is in the status "Disabled"	Info	2015-04-01 10:41:01.033	Name of the ID device: w2000s-8	190.171.3.8
<input type="checkbox"/>	No	-	Device monitoring: Controller reporting that a device is in the status "Disabled"	Info	2015-04-01 10:41:01.033	Name of the controller: w2000s-cpu	190.171.3.8
<input type="checkbox"/>	No	-	Discovery: network scan started	Information	2015-04-01 10:40:45.326	-	10.116.26.31
<input type="checkbox"/>	No	Resolving	Device monitoring: device can be reached again with DCP	Warning	2015-04-01 10:40:26.405	-	190.171.3.25
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET ID name detected	Warning	2015-04-01 10:40:25.342	PROFNET name: simatic-pc for IP address 190.171.0.4, 190.170.0.68, 190.171.0.4	

As default, SINEMA Server includes predefined events for important status changes in the network that can, when necessary, be expanded with new events. Apart from the event texts, the reaction to events, for example calling a program or sending an e-mail can also be configured. The influence of events on the overall statuses of monitored devices can be adapted by including them in overall status groups.

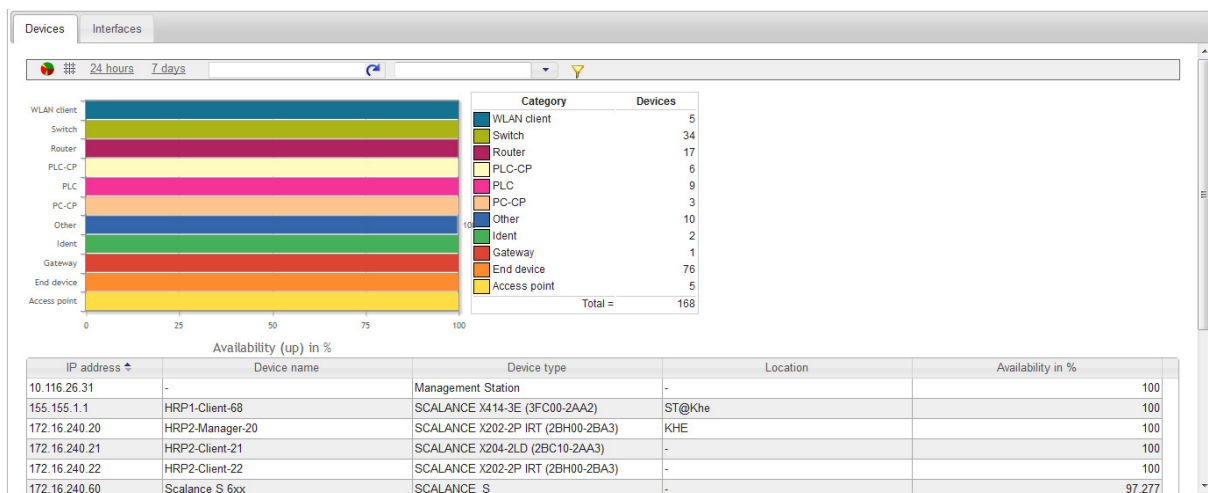


For more detailed information on event class and overall status groups, refer to the following sections:

- Events: Configuring event reactions - displaying events (Page 58)
- Overall status groups: Administration - Events Overall status groups (Page 193)

## Creating reports

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



For more detailed information on reports, refer to the section Reports (Page 158)



# Installing, setting up and calling SINEMA Server

## 2.1 Performance characteristics of SINEMA Server

### Features of the Web interface

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 of SINEMA Server

The number of monitored network devices is limited within the framework of the licensing levels. See section License information (Page 20).

A maximum of 500 network devices can be monitored.

For each management station, SINEMA Server 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.
- 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.
- Using a CSV export function (filtered) data of all lists can be downloaded, refer to the section Calling functions with a URL (Page 84)

### See also

Getting to know SINEMA Server - basic functions (Page 47)

## 2.2 Installing and uninstalling software

### 2.2.1 License information

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

#### Trial license

The application ships with a 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 and corresponding configuration limits

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 500: This license is a trial license and supports up to 500 monitored devices.

---

#### Note

The configuration limits specified by a license type do not include the network adapters of the management station.

---

---

#### Note

The "Trial 500" license of SINEMA Server V13 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.

---

---

#### 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.

---

---

#### Note

Devices in the monitoring status "Passively monitored" do not require a device license since these are monitored solely by the assigned controller.

---

## Automation License Manager

To manage your SINEMA Server license, you 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 Automation License Manager. To do this, select **Start > All Programs > Siemens Automation > Documentation** in the Windows menu.

## Storage location for license keys

You can store license keys on storage devices such as license key sticks, exchangeable drives (however not on optical memory media such as CD or DVD) or on USB memory sticks. To be able to use SINEMA Server productively, the license keys must, however, be stored locally on your computer.

## License update

To extend the license or to expand to a higher number of monitored devices, you require an update to a new license. To allow the license update to be made, the Automation License Manager requires access to the license key of the update license. The Automation License Manager or SINEMA Server then detects the update license automatically.

License types 50/100/250 can be combined. The license type is expanded according to the addition. However, only a maximum of 500 devices can be monitored. If more than 500 devices need to be monitored, these additional devices can be monitored by a separate management station. To monitor devices that are monitored by different management stations, the server overview function can be used.

---

### Note

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

---

With a license update, you can also update to a higher version of SINEMA Server. To run a license update, 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 update.
3. In the object area, select the license key with which the update 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 50. If, for example, you have license type 50 + license type 50 (two licenses) it is only possible to downgrade to one license.

### 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. In this case, run a license update with a suitable number of devices.

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 remaining in the navigation area.

## 2.2.2 Installing SINEMA Server - requirements and procedure

### Overview

Most of the installation is handled automatically. The SETUP routine itself recognizes whether other program components apart from SINEMA Server itself need to be installed. The installation routine takes the required actions as necessary.

Successful installation and problem-free operation of SINEMA Server require the following system properties:

## Hardware requirements

Parameter	Minimum requirements	Recommended requirements
Processor	Intel Core i5 with 2.4 GHz or equivalent	Intel Core i7 with 3 GHz or equivalent
RAM	4 GB	8 GB
Network adapter	1	1 <b>Note:</b> SINEMA Server supports up to four network adapters.
Storage requirements hard disk	approx. 10 GB*	approx. 50 GB*

\* The disk size also includes the capacity presumably required for archive data. When using other programs such as STEP 7, the disk requirements increase accordingly.

## Software requirements

Supported operating systems	<ul style="list-style-type: none"> <li>Windows 7 (Professional / Ultimate / Enterprise) SP1 (64-bit)</li> <li>Windows Server 2008 R2 SP1 (64-bit)</li> </ul>
Web browser	<ul style="list-style-type: none"> <li>Internet Explorer 10.0 or higher</li> <li>Firefox 26.0 or higher</li> <li>Google Chrome 30.0 or higher</li> </ul>

## 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"> <li>Internet Explorer 10.0 or higher</li> <li>Firefox 26.0 or higher</li> <li>Google Chrome 30.0 or higher</li> </ul>
Java Runtime Environment (JRE)	Version 8 update 31 or higher <b>Note:</b> The Java Runtime Environment (JRE) software is required for correct display of the Java applets. For reasons of security it is advisable to use the latest JRE version at all times.
Minimum resolution of the monitor	1280 x 1024 pixels
Recommended resolution of the monitor	1920 x 1080 pixels

### Note

Make sure that the architecture (32-bit/64-bit) of your Java plug-in matches the architecture of the Web browser you are using. You can view the architecture of the Java plug-in in the plug-in management of your Web browser.

## 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.

---

### Note

The discovery of duplicate IP addresses is only possible if you also install the "WinPcap" component.

---

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.

## 2.2.3 Uninstalling SINEMA Server

### Uninstalling

To uninstall SINEMA Server 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 relevant entry.
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.

---

## 2.3 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. Before starting SINEMA Server for the first time, basic parameters need to be set that are required for subsequent network access. 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.

## 2.3.1 SINEMA Server Monitor

### Overview

SINEMA Server Monitor is the central program module for administration of SINEMA Server. SINEMA Server Monitor runs on the PC/PG on which SINEMA Server is installed (management station).

SINEMA Server Monitor loads automatically after successful installation of SINEMA Server and on each subsequent Windows startup. In addition to this, the following icon is included in the taskbar for calling up a shortcut menu that provides the functions of SINEMA Server Monitor.



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 Status display (Page 27)

### Structure of the shortcut menu

Right-click on the icon in the taskbar. Following this, the shortcut menu for calling up the following functions appears:

- "Start web client": The standard browser is opened and SINEMA Server is called with the configured HTTPS port using the URL "https://localhost:<https-port>". If no HTTPS port is configured, SINEMA Server is called using the URL "http://localhost:<http-port>".
- "Start/Stop SINEMA Server": The progress of the action is shown in the "Status" tab of the "Settings" window.
- "Settings": The "SINEMA Server Status" window is opened. This window shows the status of SINEMA Server and provides options for making the administration settings for SINEMA Server as described in the following sections. If you change settings in SINEMA Server Monitor, the Web server is automatically exited and restarted. Open Web sessions with SINEMA Server are interrupted and you need to log in again.
- "Close": SINEMA Server Monitor is exited. You can start SINEMA Server Monitor again with "Start > Programs > Siemens Automation > SINEMA Server > SINEMA Server".

### 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 Windows 7 operating system, 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.

**See also**

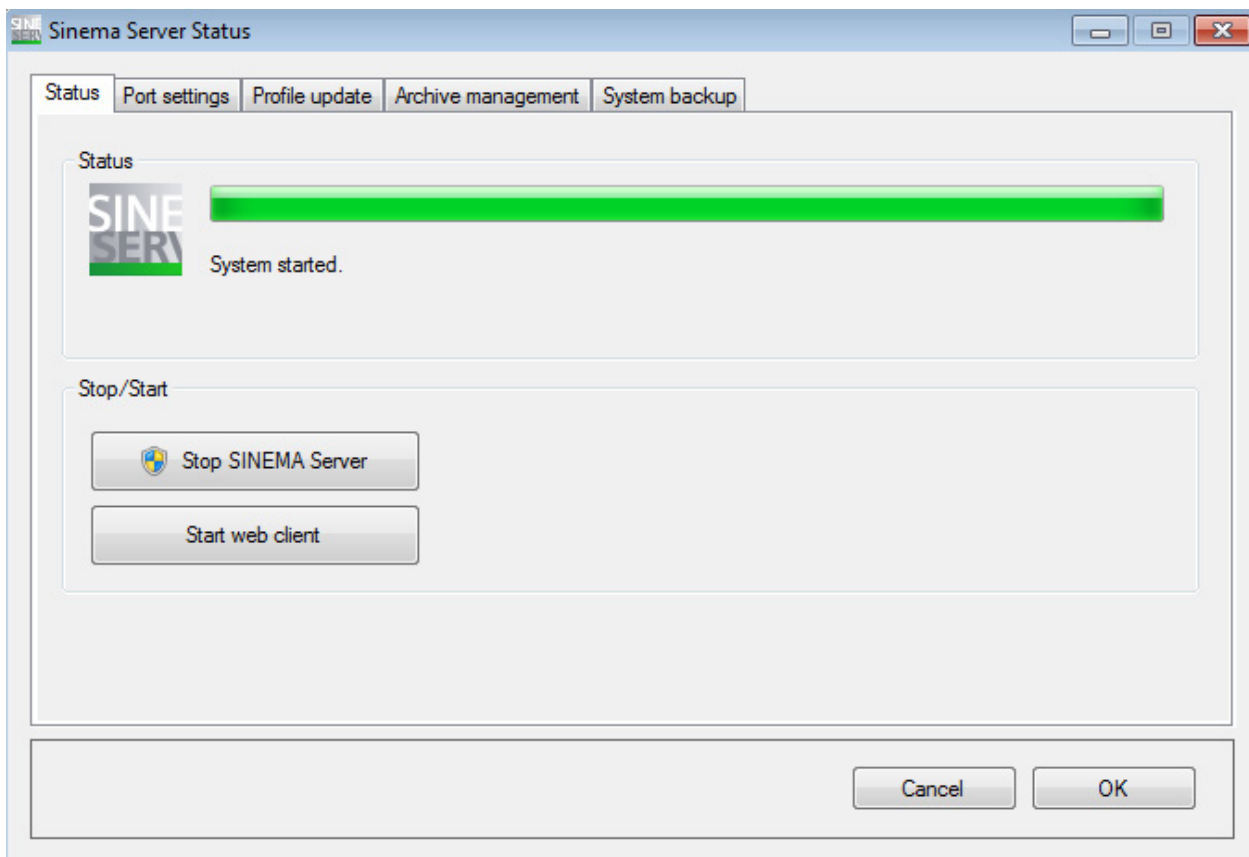
Port settings (Page 28)

Archive management (Page 35)

Device profile synchronization (Page 32)





**2.3.1.1 Status display**

The status of SINEMA Server is shown in the "Status" tab of the "SINEMA Server status" window of SINEMA Server Monitor. The tab also contains buttons for starting and stopping SINEMA Server and for calling the Web client.



## Meaning of the status displays

After starting the application, the icon for the SINEMA Server Monitor appears in the Windows taskbar. The color of the icon indicates the operating status of SINEMA Server.

Icon	Description
	SINEMA Server is stopped or is being started up
	SINEMA Server was started successfully
	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.

### 2.3.1.2 Port settings

With the port settings, you can configure SINEMA Server for HTTP, HTTPS, OPC UA, OPC DA and RPC connections as well as for the use of the SNMP trap port 162. For the individual connection types, the following functions are available:

- HTTP connections:
  - Specify the required HTTP port manually
  - Specify the HTTP port to be used by searching for an available port
  - Enable/disable SINEMA Server for HTTP connections
- HTTPS connections:
  - Specify the required HTTPS port manually
  - Specify the HTTPS port to be used by searching for an available port
  - Enable/disable SINEMA Server for HTTPS connections
  - Generating a new HTTPS certificate, refer to the section "Generating HTTPS certificates"

- OPC UA connections
  - Specify the required OPC UA port manually
  - Specify the OPC UA port to be used by searching for an available port
  - Enable/disable SINEMA Server for OPC UA connections
- OPC DA connections:
  - Enable/disable SINEMA Server for OPC DA connections
- RPC connections (to query the overall device statuses of remote servers, Web page "Server overview" - port can also be configured here):
  - Specify the required RPC port manually
  - Specify the RPC port to be used by searching for an available port
- SNMP traps
  - Windows trap service: If this option is enabled, the Windows trap service is used for shared use of the SNMP trap port 162 with other applications as long as the Windows trap service is enabled in Windows. The Windows trap service needs to be enabled manually to allow SINEMA Server to receive traps with this setting.
  - SINEMA Server trap service: If this option is enabled, the SNMP trap port 162 is used exclusively by SINEMA Server as long as the Windows trap service is not enabled in Windows.

Changes to the SNMP trap settings take effect only after restarting SINEMA Server.

---

**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.

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

---

**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.

---

## 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.

## 2.3 Configuring and starting 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:

Default ports	Description	Corresponding transport protocol	configurable	Firewall configuration required	Note on the response if the port is blocked
25	SMTP	TCP	yes (Web user interface)	yes	-
80	HTTP server / Java	TCP	yes (Windows taskbar)	yes	-
102	SIMATIC S7DOS	TCP	no	no	-
161	SNMP	UDP	yes (Web user interface)	yes	It is not possible to read out device information.
162	SNMP traps	UDP	no	yes	SINEMA Server does not receive any traps.
443	HTTPS	TCP	yes (Windows taskbar)	yes	-
4770	HTTPS	TCP	yes *	yes	Device overall statuses cannot be queried.
4840	OPC UA server	TCP	yes (Windows taskbar)	yes	-
4897	Data	TCP	no	no	SINEMA Server does not start.
4998	Events	TCP	no	no	SINEMA Server does not start.
4999	Monitor	TCP	no	no	SINEMA Server does not start.
5432	POSTGRESQL	TCP	no	no	Saving events / reports is not possible.

\* The port number of the old server is configured in the "Port settings" of SINEMA Server Monitor, the port number of the polling server in the Web user interface of SINEMA Server in "Server overview".

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.

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

**NOTICE****Firewall**

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

## Generating HTTPS certificates

As further support for HTTPS connections, the setup of SINEMA Server also includes the generation of HTTPS certificates. As soon as the SINEMA Server 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.

## Using third-party certificates

You will find this certificate in the following folder:

Siemens\SINEMAServer\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\Sinema\_Server\config

<b>NOTICE</b>
<b>SSL certificate</b>
The SSL certificate must be stored under the name "certificate.pem".

### 2.3.1.3 Device profile synchronization

#### Purpose of device profile synchronization

In networks with more than one SINEMA Server instance, all instances should always use the same device profiles so that the monitored devices are displayed according to uniform patterns. The device profile synchronization function allows a central file path to be specified for new device profiles or device profiles and requiring updates. The stored device profiles are automatically imported into the local SINEMA Server instance at a selectable time of day or at a selectable interval (12 hours / 24 hours). As an alternative, the device profiles stored in the configured file path can be imported manually at any time.

---

#### Note

##### Compatibility of device profiles from different SINEMA Server versions

It is possible to import device profiles from SINEMA Server version V12 into SINEMA Server  $\geq$  V12 SP1. Device profiles are migrated during the update.

Device profiles of SINEMA Server V12  $\geq$  SP1 are not compatible with SINEMA Server V12.

---

#### Rules for importing device profiles

When importing existing device profiles, the following rules apply:

- Provided device profiles whose device profile IDs do not exist in the local SINEMA Server instance are imported into the local SINEMA Server instance as new device profiles. The import of a new device profile is output as an event in the event list.
- Provided device profiles whose device profile IDs exist in the local SINEMA Server instance overwrite the corresponding device profiles in the local SINEMA Server instance. The overwriting of an existing device profile is output as an event in the event list.
- For device profiles in the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles, the response can be configured as follows:
  - Delete local device profiles without reference to provided device profiles if these local device profiles are not being used as monitoring profiles for existing devices.
  - Retain local device profiles without reference to provided device profiles (default setting).

---

#### Note

Make sure that there is only ever one device profile archive in the import folder. If the import folder contains several device profile archives at the same time, these must not have any overlaps with identical device profile IDs.

---



The table below illustrates the import rules based on examples of device profile imports. The following formatting and naming conventions are used:

- Device profiles formatted in **bold** text in the "Local device profiles" column are used as monitoring profiles for existing devices. Device profiles without this text highlighting are not used as monitoring profiles for existing devices.
- The numbers of the device profiles indicate their device profile IDs.
- The variants indicate differences in content between device profiles with the same device profile ID.

In each of the examples a distinction is made between the "Delete local device profiles without assignments" option being enabled and disabled.

Local device profiles	Provided device profiles	Local device profiles after profile import	
		"Delete local device profiles without assignments" option is enabled	"Delete local device profiles without assignments" option is disabled
<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• <b>Device profile 3, variant a</b></li> <li>• <b>Device profile 4, variant a</b></li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 3, variant a</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 3, variant a</li> <li>• Device profile 4, variant a</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• Device profile 3, variant a</li> <li>• Device profile 4, variant a</li> </ul>
<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• <b>Device profile 3, variant a</b></li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• Device profile 3, variant a</li> <li>• Device profile 4, variant a</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• Device profile 3, variant a</li> <li>• Device profile 4, variant a</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• Device profile 3, variant a</li> <li>• Device profile 4, variant a</li> </ul>
<ul style="list-style-type: none"> <li>• Device profile 1, variant a</li> <li>• Device profile 2, variant a</li> <li>• <b>Device profile 3, variant a</b></li> <li>• <b>Device profile 4, variant a</b></li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant b</li> <li>• Device profile 3, variant b</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant b</li> <li>• Device profile 3, variant b</li> <li>• Device profile 4, variant a</li> </ul>	<ul style="list-style-type: none"> <li>• Device profile 1, variant b</li> <li>• Device profile 2, variant a</li> <li>• Device profile 3, variant b</li> <li>• Device profile 4, variant a</li> </ul>

Local device profiles	Provided device profiles	Local device profiles after profile import	
		"Delete local device profiles without assignments" option is enabled	"Delete local device profiles without assignments" option is disabled
<ul style="list-style-type: none"> <li>Device profile 1, variant a</li> <li><b>Device profile 3, variant a</b></li> </ul>	<ul style="list-style-type: none"> <li>Device profile 1, variant b</li> <li>Device profile 2, variant b</li> <li>Device profile 3, variant b</li> <li>Device profile 4, variant b</li> </ul>	<ul style="list-style-type: none"> <li>Device profile 1, variant b</li> <li>Device profile 2, variant b</li> <li>Device profile 3, variant b</li> <li>Device profile 4, variant b</li> </ul>	<ul style="list-style-type: none"> <li>Device profile 1, variant b</li> <li>Device profile 2, variant b</li> <li>Device profile 3, variant b</li> <li>Device profile 4, variant b</li> </ul>

## Configuring device profile synchronization

Device profile synchronization can be configured in SINEMA Server Monitor as follows:

Operator control element	Function
Scan	Select the folder in which the device profiles to be imported will be stored.
Options	Specifying user data for access to profile update directory.
Automatic synchronization	If this check box is enabled, device profiles stored in the selected file path are imported automatically into the local SINEMA Server instance. With the "Start time" input boxes, you can configure the time at which the next automatic update is performed. With the two option buttons "12 hours" or "24 hours", the interval for the later automatic updates can be specified.
Delete local device profiles without assignments	<ul style="list-style-type: none"> <li>Check box is enabled: Device profiles of the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles are deleted in the local SINEMA Server instance during import if these device profiles are not used as monitoring profiles for existing devices. Deleting an existing device profile is output as an event in the event list.</li> </ul> <p>Note: If this check box is enabled, no import should be performed while the device profiles are being put together in the selected directory. Otherwise, this can lead to the unwanted loss of local device profiles.</p> <ul style="list-style-type: none"> <li>Check box is disabled (default): Device profiles of the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles, are retained when importing into the local SINEMA Server instance.</li> </ul>
Import manually	Manual import of the device profiles.

## Requirements for importing device profiles with user-defined parts

If the data to be imported contains a profile whose threshold is used by user-defined overall status group, all profiles must be imported into the SINEMA Server instance:

- The "Delete local device profiles without assignments" check box is enabled.
- Local device profiles without an assignment to the provided device profiles are not used by any of the monitored devices.

### 2.3.1.4 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.

#### Functions

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

- Import archives

With this function, you can read in exported archives.

- Export archives 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. The memory space that will be freed up can be calculated prior to using the function.

- Delete archives

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.

- Delete archives of deleted devices

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

---

#### Note

##### Period for historical data records

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

---

<b>NOTICE</b>
<b>Editing the ZIP file - effects</b>
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:

- Needed space

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

- Freed space

With this function, you see the storage space that became free in the SINEMA Server archive for the specified archiving period.

### 2.3.1.5 Data backup and restore

#### 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 system backup then starts. If SINEMA Server has already been started, it is closed before the backup begins and restarted after the backup is completed.

#### Restore system backup

The data from a previously created system backup is read in.

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

<b>NOTICE</b>
<b>Reading in the backup completely overwrites all existing data - project and program!</b>
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.

---

#### Note

##### Exchanging system backups between different systems is not possible

When a system backup is restored, a check is made to make sure that the computer name of the source system is identical to the computer name of the target system. If the computer names do not match, the backup cannot be restored. You should therefore avoid changing the computer name.

---

## **2.3.2 Java applets**

### **Setting required in the Java Control Panel**

SINEMA Server has been released for Java version 1.7 Update 51. After installing SINEMA Server, make the settings below in the Java Control Panel to ensure the correct integration of the Java applets in SINEMA Server.

1. In the "General" tab, click the "Settings..." button under "Temporary Internet Files". Click the "Delete Files..." button and in the dialog that opens, make sure that the "Trace and Log Files" and "Cached Applications and Applets" check boxes are selected and confirm with "OK".
2. In the "Security" tab, make sure that the security level is at least set to "High".
3. If your PC is not connected to the Internet or loading Java applets normally takes a long time, select the "Do not check" check box in the "Advanced" tab under "Perform certificate revocation checks on".
4. In the "Temporary Internet Files" section of the "General" tab, click the "Settings..." button and in the "Temporary Files Settings" dialog, make sure that the "Keep temporary files on my computer" check box is selected. In the "Advanced" tab, you should also make sure that in "Mixed Code (sandbox vs, trusted) security verification", the option "Enable - hide warning and run with protections" is selected. This avoids warnings being displayed when using the topology displays.

When you first call up one of the topology displays, the Java message "Do you want to run this application" appears in SINEMA Server. In this dialog, select the check box "Do not show this again for this publisher and location above" and click "Run".

## **2.3.3 Start SINEMA Server**

### **Automatic start**

SINEMA Server is started automatically after installation and each time the management station is restarted.

### **Manual start**

If SINEMA Server was exited, you can start the application manually as follows:

- "Start SINEMA Server" menu command in the shortcut menu of the SINEMA Server icon displayed in the taskbar
- "Start SINEMA Server" button in the "Status" tab of the "SINEMA Server status" window

<b>NOTICE</b>
<b>Avoid pauses or idle times on the management station</b>
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.

## 2.4 Migrating a SINEMA Server configuration

When installing SINEMA Server V13 no data from an already installed earlier SINEMA Server version can be adopted.

## 2.5 Web user interface

### 2.5.1 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**

For security reasons, it is strongly recommended that you use the HTTPS protocol. The data is transferred encrypted and cannot be read by unauthorized third persons.

---

---

**Note**

To allow pages of the SINEMA Server Web interface that contain Java applets to be displayed, Java Runtime Environment (JRE) version 7 Update 51 must be installed on the client computers and enabled in the browser.

---

**NOTICE****"Start Web client" function of SINEMA Server Monitor - default Web browser**

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 Installing SINEMA Server - requirements and procedure (Page 22). It is advisable to make sure that one of these Web browsers is configured as the default browser.

**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 the data is to be transferred encrypted).

If you use a port other than 80 as the HTTP standard port, 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 (e.g.: **http://192.168.0.1:8080**). This applies analogously to the HTTPS standard port 443.

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 the data is to be transferred encrypted).

If you use a port other than 80 as the HTTP standard port, 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 (e.g.: **http://192.168.0.1:8080**). This applies analogously to the HTTPS standard port 443.

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.
2. 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.

---

**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.

## Initial logon data

As default, the predefined user "Administrator" is available in SINEMA Server. This user is assigned to the predefined user group of the same name. The default user name and the password for this user are as follows:

- User name: Administrator
- Password: SinemaA

After the first logon to the system, you will be prompted to change the initial password in "Administration > My settings".

Note the mechanisms for protection against brute force attacks, refer to the section Administration - User Logon locks (Page 204)

If you have forgotten your password you can have a one-time password sent to you using the "Forgotten the password?" button. This one-time password is then sent to the e-mail address stored for the user.

---

**Note**

At least for users with administrator rights, configure the e-mail settings so that when necessary you can be sent one-time passwords.

---

You will find further information about these predefined user groups, access rights and creating/managing users in the section Users and user groups (Page 72)

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 47)

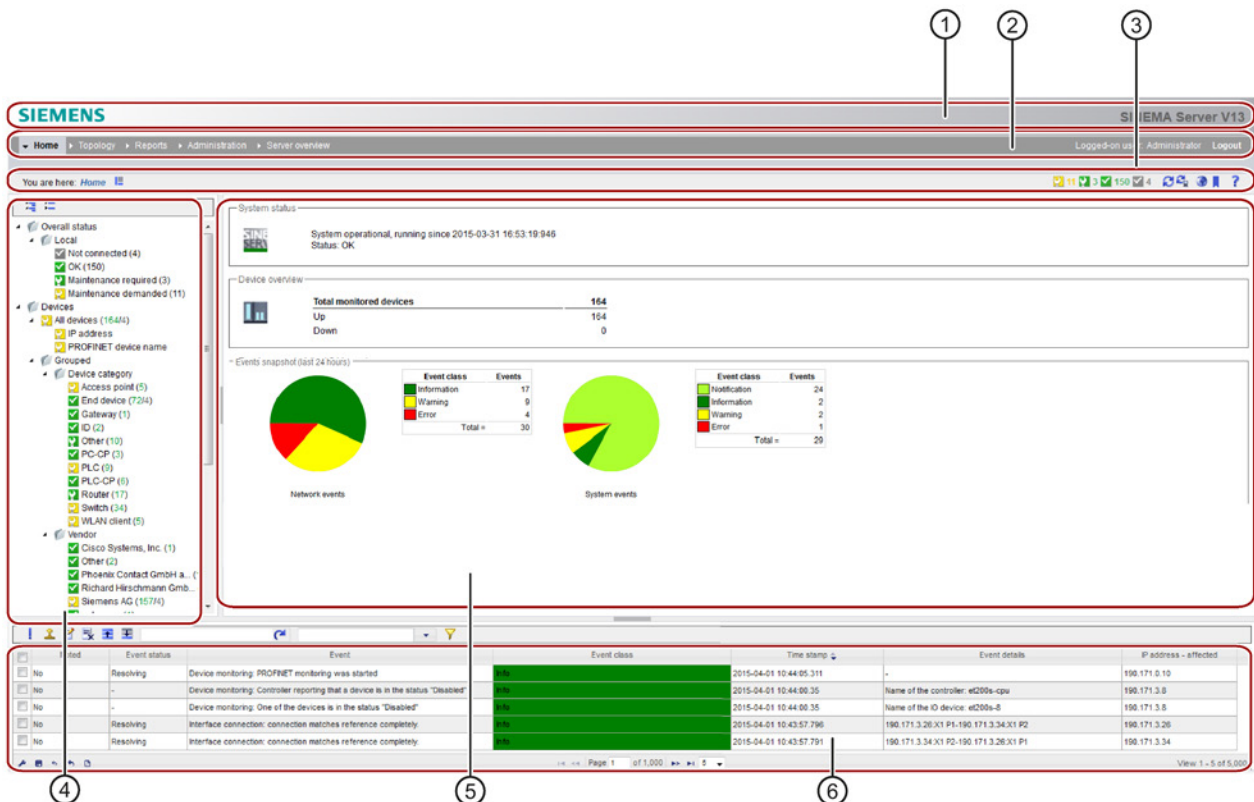


## 2.5.2 SINEMA Server user interface on the Web interface

### 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 V13).

---

**Note**

**Displaying program information**

If you click on the program name, an information window opens. It contains program information such as version number, release date and extent of the license.

---

- 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. For reasons of security, always click this button when you want to end your work with SINEMA Server. Closing browser windows and browser tabs without logging out first should be avoided for security reasons.

The content of the menu bar varies depending on the status of SINEMA Server. The "Topology" and "Reports" menu items are 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.


On the right, information texts are displayed indicating certain actions or operational statuses.

- 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): A search is made for more suitable device profiles and device types included in them for devices that were assigned standard profiles.
	(with number): Number of unreachable devices Opens the device list with the display of the unreachable devices. The number of devices involved is displayed.		(animated): Network is scanned
	Opens the device list with the display of the devices with the status "Maintenance demanded". The number of devices involved is displayed.		Opens the device list with the display of the devices with the status "Error". The number of devices involved is displayed.
	Opens the device list with the display of the devices with the status "OK". The number of devices involved is displayed.		Opens the device list with the display of the devices with the status "Maintenance required". The number of devices involved is displayed.
	Opens the device list with the display of the devices with the status "not connected". The number of devices involved is displayed.		Autorefresh on/off The content of the Web page is refreshed according to the selected "Monitoring interval".
	Refresh display SINEMA Server refreshes the content of the Web page once.		Managing and using quick links Opens the list of available quick links.
	Select language A selection dialog with the available languages is displayed. The changeover also affects the display of the online help.		Printing The print function is available on the following Web pages: <ul style="list-style-type: none"> <li>• Topology</li> <li>• Reports</li> </ul>

Icon	Display / function	Icon	Display / function
	Open help system Opens the help page for the current Web page in a separate window of the Web browser.		

- **④ Device tree and views**

The device tree contains groups of devices that are monitored by the local SINEMA Server instance or by other SINEMA Server instances. Selecting a device group below the "Overall status > Local" and "Devices" branches generates a display filtered according to the overall status or device property (type, vendor, alternating devices). Selecting an entry below the "Server overview" branch results in a display of the server overview sorted according to overall device statuses. After selecting a node under the entry "PNIO systems", only the devices that belong to the selected PNIO system are displayed. The icons in the device tree always show the worst current status of one of the device nodes in the branch.

Views are used to monitor any subareas of a network based on lists and topology displays. By assigning views to individual users, the network areas to be monitored can be restricted to specific users.

- **⑤ Main window**

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

- **⑥ Event list**

The event list shows network events that have occurred as well as system-related events. 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.

## 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.

## Updating the Web user interface

The content of the Web user interface is updated either cyclically or on demand.

This is selected using the relevant icons in the status bar.

You set the interval for cyclic operation with the menu command "Administration > My settings > User interface" in the "Monitoring interval" parameter.

**See also**

User interface (Page 75)

User interface (Page 75)



## Getting to know SINEMA Server - basic 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, reachable devices are searched for based on selectable protocols.  
Depending on the configuration in SINEMA Server, either all the devices discovered by DCP and/or ICMP or devices in preset IP address ranges are recorded.
- The devices discovered using ICMP and optionally DCP are put together in the device list. Information about the discovered devices is put together in the interface list. The discovered connections are put together in the discovered topology.
- If PROFINET IO controllers are found during the scan, the IO devices assigned to these controllers are also included in the monitoring. This is the case regardless of whether the IO devices are located in the scan range or not.
- 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. If PROFINET discovery is active, devices are assigned to the device types contained in the device profiles.
- 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 devices are detected. The device list, the interface list and the "Discovered topology" are then updated. Removed devices are no longer shown in the device and interface list or in the topology display.

#### See also

Profile concept (Page 53)

### 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.

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 covers more than 1000 addresses, a message will warn you to expect the scan to take a long time. You should therefore restrict the scan range to the devices to be monitored. To do this, it is advisable to create smaller scan groups if the IP addresses are not consecutive. This division speeds up scanning of the devices. A maximum of 40 scan groups can be created.

As default, SINEMA Server calculates the start and end of the scan range based on the subnet mask configured on the network interface adapter.


The procedure described below includes the adaptation of the scan range.

#### Network scan - procedure

To scan the network, follow the steps below:

1. Select the menu command **"Administration > Discovery"**, "Scan" tab.
2. In the section "DCP network adapter for device scan", select the function "Scanning for network adapters".

The network adapters available on the management station are displayed.

3. In the table, select the network adapters (called NIC below) via which the scan will be made and enable these using the "Enable network card for device scan" function.
4. When necessary, enter further parameters in the following Web pages:
  - **"Administration > Discovery"** in the "Profiles" tab
  - **"Administration > Monitoring > General "** in the "Time settings" area
  - **"Administration > Monitoring > SNMP settings"**
5. If applicable, select the menu command **"Administration > Discovery"** again and open the "Scan" tab.
6. Select the IP address ranges to be searched.
7. Click on the icon  ("Start scan") to start the network scan. The network is scanned according to the scan ranges for the subnets.
  - The progress of the scan is indicated by an icon in the right part of the status bar.
  - On completion of the scan, all discovered network devices and their statuses are displayed in the device lists that can be selected in the device tree.



## Special features to note

---

### Note

#### Effect of the option "Include all devices discovered with DCP 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.

---

<b>NOTICE</b>
<b>Avoid stopping/starting during the network scan</b> If SINEMA Server is stopped during the scan 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: <ul style="list-style-type: none"><li>• Before stopping SINEMA Server, make sure that the scan has not started.</li><li>• If devices were found during an aborted scan, delete these and scan the network again.</li></ul>
<b>NOTICE</b>
<b>Do not change the date or time</b> 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.



---

### Note

#### Updating device data already read in

Read device data is updated cyclically. To update immediately, it is recommended that you use the "Reread device data" icon in the device list.

---

## 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 the 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.

SINEMA Server automatically recognizes the devices reachable in the network during the discovery process and shows their topology based on the information obtained with SNMP and PROFINET. The connection lines of the topology display are also displayed between devices that support different protocols. If a device does not support SNMP or PROFINET, no connection lines are shown. The root node of the network topology is the management station.

Discovered devices that cannot be inserted in the reference topology are indicated by the  icon.

---

#### 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 - basis for the monitored topology

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 and/or PROFINET are disabled. It is also possible that unmanaged devices exist in the network that cannot be specified automatically by SINEMA Server.

The Reference editor in SINEMA Server allows manual adoption and if necessary correction and expansion of information of the discovered topology. The created reference topology is used as the basis for the monitored topology and for view-specific topologies.

The Reference editor serves the following purposes:

- Drawing/modifying reference connections
- Configuring status of the ports
  - Active port
  - Inactive port
  - Unmonitored port
  - Docking port
- Enabling / disabling references for SNMP, TCP protocols

---

**Note**

**Required rights**

To be able to edit the reference topology, users must have the "Operative monitoring settings" right.

---


## 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 of the monitored topology 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:

- Each new device that is not part of the reference topology is not shown.
- If devices were discovered that cannot be inserted in the reference topology, this is indicated in the monitor topology with the  icon in the top left corner.
- Unmonitored devices are not shown in this topology. If a device is set to "Unmonitored", it is automatically removed from the reference topology and therefore also from the monitored topology. If such a device returns to the monitored status, SINEMA Server handles this device like a new device.

---

**Note**

**The reference topology is a prerequisite**

The device hierarchy, the overall view and the topology display of the monitored topology are displayed only after the reference topology has been saved at least once.

---

## See also

Alternating devices (Page 120)

### 3.2.2 Topology discovery

#### Network scan - effect on the topology discovery

The topology scan of the SINEMA Server application is always performed after a network scan. This response applies both to a manually or automatically initiated network scan if this is enabled. The topology scan can also be performed if the network scan is disabled.

Changes to previously discovered connections or new connections are detected and displayed as being current in the discovered topology.

#### Requirements for topology discovery

The network topology discovery is based on LLDP information read out via SNMP or PROFINET. To obtain precise connection information, SNMP and/or PROFINET must therefore be enabled for the devices to be monitored.

### 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.

#### Procedure

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

This opens the reference topology with the functions of the Reference editor in which the detected devices are displayed.

2. Configure the desired status of the connections between the devices by using the "Use current connections as reference" function or the drawing tool.
3. Save the reference topology.

After completing your configuration in the Reference editor, change to the monitored topology with the "**Topology > Monitored**" menu command. The devices of the entire network are displayed here and monitored for the configured desired statuses.

---

**Note**

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

---

## 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.

#### 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. When PROFINET monitoring is active, the devices are directly assigned the device types contained in the device profiles. The assigned profile is used to classify and represent the network device.

If no suitable profile is found for a network device during the network scan, SINEMA Server assigns a standard profile to the device. With the Profile editor, SINEMA Server also supports you during necessary adaptations or additions to the profile database.

New profiles are always created based on existing profiles. To create a new profile, you must therefore always use an existing profile as the template.

To assign a profile to device types that do not correspond to any previously stored profile, you have the following alternatives:

- You assign the new device type to an existing profile.
- You create a new profile and store the new device type in it.

The assignment of devices to the new device type can then (also) be performed with the automatic new assignment of profiles, refer to the section below.

## 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 criteria based on the SNMP data of the device:

1. sysDesc (OID 1.3.6.1.2.1.1.1.0):  
A textual description of the device (system hardware type, software operating system, network software etc.).
2. lldpLocSysDesc (OID 1.0.8802.1.1.2.1.3.4.0):  
The value of the character string is required for the system description mentioned above. If the local agent supports IETF RFC 3418, the lldpLocSysDesc 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):  
This value is assigned within the "SMI enterprises sub tree" (1.3.6.1.4.1) and contains the highest OID under which the private MIB of the device manufacturer can be found.

### Automatic profile and device 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 criterion whose stored text is longest 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.

### Device discovery using PROFINET

With PROFINET discovery, devices are assigned directly to the corresponding device types based on article numbers that can be specified in the device type rules of a device profile. If PROFINET discovery is activated in "Administration > Discovery", it is handled with greater priority than the assignment to device profiles via SNMP.

### Automatic reassignment of profiles and device types

For devices that were assigned one of the standard profiles during discovery, SINEMA Server runs through the process described above for automatic profile and device type assignment again at regular intervals looking for more suitable profiles and device types they contain for these devices. The default interval for automatic reassignment is 70 minutes and this can be configured in "Administration" > "Monitoring" in the "Time settings" area. In addition to this, the automatic reassignment is always performed when a device with an assigned standard profile changes from the "Not reachable" status to the "Reachable" status.

---

#### Note

If a device has been assigned a new device profile, it is automatically removed from the reference topology and must be inserted in this again.

---

## 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. If only SNMP is used for discovery, device type rules are only taken into account after evaluating the discovery rules. In this case, and for this reason, at least one discovery rule must exist that relates to the device type to be added. In PROFINET discovery, only device type rules are taken into account.
5. Change to the "Device types" tab and select the "Add device type rule" function  
The Device type editor opens and you can enter the data for the new device type rule.
6. Follow the steps below in the Device type 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.

### 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.

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 copied:

- 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:

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.
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 175)

## 3.4 Configuring event reactions - displaying events

Events are divided into the following categories:

- Network events

Network events provide information about statuses arising and changes in the network. These also include SNMP traps and SIMATIC event and alarm messages sent to SINEMA Server by devices managed in the network.

- System events

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

Events of both categories are also divided into the following classes according to their severity:

- Notification and information:

Events of these classes 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.

Notifications and information require no action from the end user. These involve either a message about a user action performed by the application or an update due to status changes of network devices. Among others, examples are: User logins/logouts, completion of device discovery, checking of software drivers, start/end of the network scan or permissions granted by the administrator.

- 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 events of the "Warning" class include:

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

- Errors:

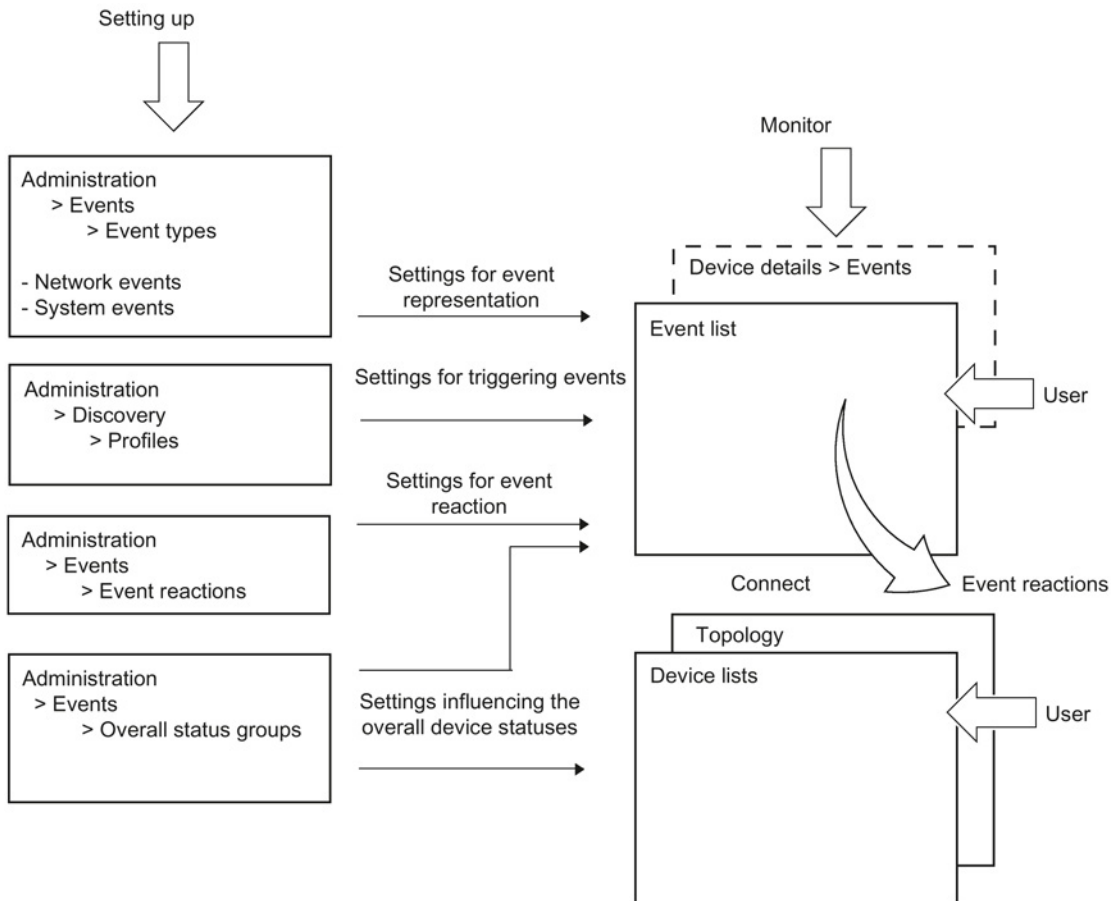
When such events occur, fast intervention is required. Depending on the content of the error message, the user must take suitable measures. The event reactions already configured for the error events simplify things.

Examples of events of the "Error" class include:

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

## 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 display

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

Here, you specify new event types and select the event types to be actively monitored. You can also adapt existing event texts and classifications.

You will find more detailed information on this function in the section Administration - Events Event types (Page 190)

- Settings for triggering events

You make the settings for triggering events with the menu command **"Administration > Discovery > Profiles"**.

In the "Threshold" tab of the profile properties of a device profile, you can use operators and threshold values to define conditions for certain event types in which

### 3.4 Configuring event reactions - displaying events

the corresponding events will be triggered. These conditions then apply to all devices to which the device profile is assigned.

User-defined network events cannot be triggered without the assignment to a threshold.

Some of the predefined events can also be triggered even without a link to a threshold.

You will find more detailed information on this function in the section The Profile editor (Page 177)

- Settings for the event reaction

You make the settings for the event reaction with the menu command **"Administration > Events > 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 - Events > Event reactions (Page 198)

- Settings influencing the overall device statuses

You make the settings for the influence of events on the overall statuses with the menu command **"Administration > Events > Overall status groups"**.

An overall status group is a group of functionally related events that can influence the overall status of devices when they are triggered by these devices. Each event within an overall status group can be assigned an overall status that the device will adopt when the corresponding event condition occurs.

You will find more detailed information on this function in the section Administration - Events Overall status groups (Page 193)

- 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.

For events that are assigned to overall status groups, their event status is important. The event status categorizes events according to the degree of effect that events have on the overall status of devices.

By connecting the event list with a topology, specific devices for which events of the event list were triggered can be displayed in a graphic network representation.

For more detailed information the events list, refer to the section Event list (Page 125)

- 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 107)

## 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 and SINEMA Server instances simplifies the management or monitoring of the devices and SINEMA Servers and their connections.

By assigning the views in the user management to individual users that do not have the right "View all devices and servers", the number of devices that can be monitored can be restricted for the specific user.

The screenshot shows the SINEMA Server V13 interface. The top navigation bar includes 'Home', 'Topology', 'Reports', 'Administration', and 'Server overview'. The 'Views' section is active, showing a list of views. The left sidebar contains a tree view of devices, with 'Views' expanded to show 'Basic views' and 'Sub views'. The main table displays a list of devices with columns for Status, IP address, PROFINET device name, Device type, MAC address, Active SIMATIC, and Views.

Status	IP address	PROFINET device name	Device type	MAC address	Active SIMATIC	Views
✗	172.16.240.60	Scalance S 6xx	SCALANCE_S	00 0E 8C D6 A7 B2	☐	View1
✓	190.171.0.70	pn-io	CPU 414-3 PN/DP (3EM05-6AB0)	00 0E 8C 98 B8 79	☐	Subview1
✓	190.171.0.67	x204in-67	SCALANCE X204IRT (0BA00-2BA3)	00 0E 8C A2 21 3D	☐	Subview1
✓	190.171.0.68	x201-3prt-68	SCALANCE X201-3P IRT (3BH00-2BA3)	00 0E 8C 81 F9 00	☐	Subview1
✓	155.155.1.1+		SCALANCE X414-3E (3FC00-2AA2)	08 00 06 97 94 5B+	☐	View1
✓	172.16.240.20		SCALANCE X202-2P IRT (2BH00-2BA3)	08 00 06 95 E3 3A	☐	View1
✓	172.16.240.21		SCALANCE X204-2LD (2BC10-2AA3)	00 0E 8C A4 9B A8	☐	View1
✓	172.16.240.22		SCALANCE X202-2P IRT (2BH00-2BA3)	08 00 06 95 E3 48	☐	View1
✓	172.16.240.65		SCALANCE X307-3LD (3BM00-2AA3)	08 00 06 CA 73 01	☐	View1
✓	172.16.240.66		SCALANCE X204-2 (2BB10-2AA3)	00 0E 8C C3 34 15	☐	View1
✓	172.16.240.67		SCALANCE X308-2LD (2FM00-2AA3)	08 00 06 CA 60 01	☐	View1

- ① View-specific device list
- ② View-specific interface list
- ③ View-specific list of SINEMA Server instances
- ④ View-specific topology
- ⑤ Basic views
- ⑥ Sub views

## Aims

From the total monitored network, you set up separate monitoring groups with the following properties and options:

- **Basic views**

Basic views provide a specific view of a section of the total monitoring.

- **Sub views:**

When necessary, sub views provide further specific sections of the network.

- **View-specific topology**

When necessary, set up a view-specific topology view.

- **View-specific display in the events list** (refer also to the section Event list (Page 125))

## Requirements

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

- If you want to create a view-specific topology, a reference topology must exist.
- To include SINEMA Server instances in a view-specific topology, these must be created in the "Server overview" tab.
- User rights: "Administration of devices/views/servers".

## Creating a new view

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

### Creating a basic view

1. Select the "Views" node.
2. With the right mouse button select the "Create new view" menu command; this opens the View editor.
3. Configure the new view in the Views editor by assigning the required devices and SINEMA Server instances to the view in the "Devices" and "Servers" tabs.  
  
SINEMA Server instances are only shown in the "Servers" tab if they have been created in the server overview. For more detailed information on the server overview, refer to the section Server overview (Page 207).
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 an existing view node.
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.

### 3.5 Setting up and using views

4. In the View editor, specify whether or not a specific topology display will be used.
5. If necessary, configure the topology.

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

### Positioning views later

To move a view or a sub view to a different hierarchical position after they have been created, follow the steps below:

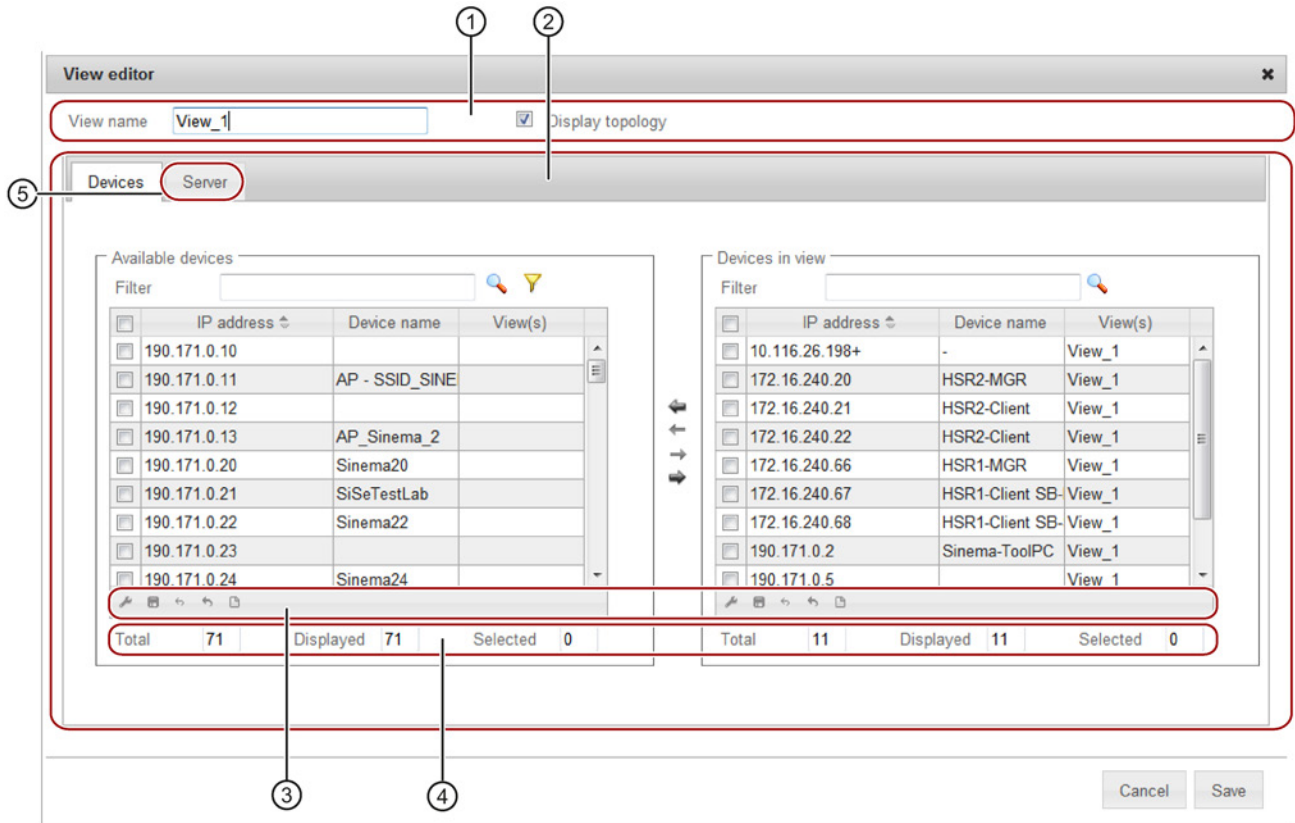
1. Select the "Views" node.
2. Right-click and select "Change view hierarchy" in the shortcut menu.
3. In the "Change view hierarchy" dialog, drag the views to the required position.

Using the arrow icon in the upper part of the dialog you can restore the last stored status.



### 3.5.2 The View editor

You open the View editor in the with the function for creating or editing a view. The way in which the Views editor works is the same for devices and SINEMA Servers instances.



- ① Header
- ② Assignment area
- ③ Settings area
- ④ Statistics
- ⑤ Views editor for SINEMA Server instances

#### How it works

In the "Devices" tab, take the devices to be included in the view from the list of "Available devices" and add them to the "Devices in view" list. Follow the same procedure in the "Servers" tab for SINEMA Server instances that were created in the server overview.

#### View filter for devices and SINEMA Server instances

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

### 3.5 Setting up and using views

The view filter provides the same filter options for devices and SINEMA Server instances. For this reason, the term "object" is used for both components in the following list:

- Show all objects (regardless of view).
- Display objects 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 objects should **not** be included in the "Available devices" or "Available servers" list box.

- Select views whose objects will be displayed.

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

Select the views whose objects should be included **exclusively** in the "Available devices" or "Available servers" list box.

### 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, SINEMA Server instances, sub views and connections between these components.

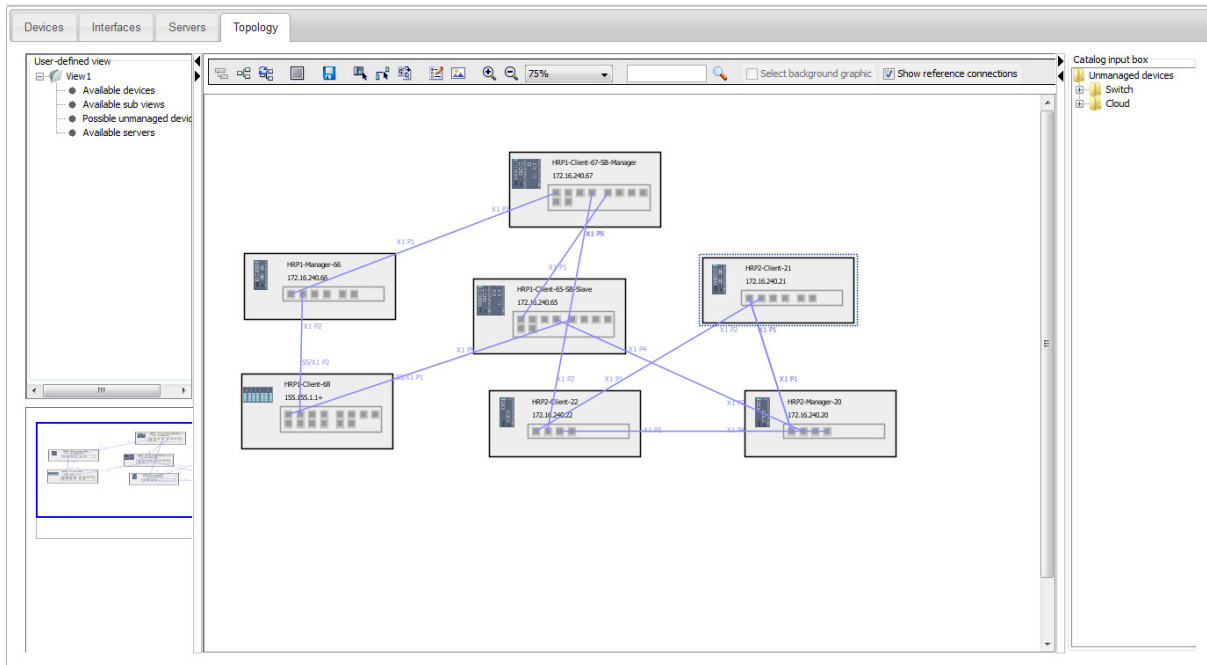
In the Topology editor, various options are available with which you can change a topology display, draw connection lines and display reference connections.

#### Requirement

The topology shown in the view area is based on the reference topology. Before you create a topology view the first time, you must first create a reference topology and save it.

## Example

The following schematic illustrates a view-specific topology.



## The editor in detail

For a description of the editor functions and icons, see section Views (Page 121)

## Creating a view-specific topology - procedure

Requirement: You have selected the "Display topology" option in the Views 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 "Available devices" subtree of the "User-defined view" 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.
2. Add the SINEMA Server instances from the "Available servers" subtree of the "User-defined view" area.  
The SINEMA Server instances are shown without connections to each other.
3. Assign the objects according to your requirements. With the selection tool enabled, position the cursor on the object while holding down the left mouse button and move it to the required position.
4. If required, add a background graphic to make the view clearer.  
See also below in "Configuring objects - background graphic".

5. Check and configure the connections between the objects, refer to the section Configure connections (Page 69).
6. To save these changes, click "Save". Then change to the "Active mode"

---

**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, device and server status - no display in draft mode**

In draft mode, the current status of ports, devices and SINEMA Server instances is displayed. They are grayed out.

---

## Configuring a background graphic

### 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.

### Change graphic position

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

1. Activate the selection tool from the toolbar and enable the option "Select background graphic" in the header.

The graphic is then displayed in a black frame with white handles.

2. Move the mouse pointer over the graphic and left-click. 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

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

1. Activate the selection tool from the toolbar and enable the option "Select background graphic" in the header.

The graphic is then displayed in a black frame with white handles.

2. Move the cursor to one of the handles and hold down the left mouse button.
3. Drag the selected handle to the required position.
4. When you release the left mouse button, the size of the background graphic changes.

#### **Deleting a background graphic**

1. Activate the selection tool from the toolbar and enable the option "Select background graphic" in the header.

The graphic is then displayed in a black frame with white handles.

2. Move the mouse pointer over the graphic and right-click.
3. In the context dialog that then opens, confirm the "Delete" function.

#### **Creating a 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 devices or SINEMA Server instances of the sub views.

Follow the steps below:

1. In the "User-defined view" area of the higher-level view under the "Available sub views" entry, select the required sub view and drag this 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.

---

### **3.5.4 Configure connections**

#### **Creating or editing user-defined connections**

To obtain a clear topological display, you can edit the arrangement of the connections with the Topology editor. Connections whose display was configured in the view-specific topology are known as user-defined connections.

### 3.5 Setting up and using views

User-defined connections are created in the draft mode in the view-specific topology as follows:

- Using and editing reference connections

Displayed reference connections are adopted as user-defined connections and their display is changed.

Note: SINEMA Server instances are not part of reference topologies. This means that connections from SINEMA Server instances can only be drawn manually.

- Drawing user-defined connections manually

New connections between device ports are created and their display specified.

---

#### Note

##### User-defined connections with SINEMA Server instances

SINEMA Server instances can only have user-defined connections to other SINEMA Server instances.

---

This procedure is described below.

### View in draft mode and in active mode

The display of the user-defined connections differs as follows:

- Draft mode
  - User-defined connections are visible as black lines with bending points.
  - Reference connections remain visible.

- Active mode

You only see the user-defined connections according to the layout configuration.

### Using and editing reference connections

If the selection tool is enabled, you have the following options:

- 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.

---

**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.

---

**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

1. In draft mode, select the tool for drawing connections from the toolbar.
2. Click on the object from which the connection will be drawn.
3. Click on the object to which the connection will be drawn.

If the objects to be connected are devices, you can select the interfaces of the devices between which the connection will be established in the "Connection Wizard" dialog.

A user-defined connection is then displayed between these two objects. The connection is displayed gray.

## 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.

## See also

Views - topology / Topology editor (Page 122)

## 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.



## Standard users and groups

In SINEMA Server, there are three predefined user groups with corresponding access rights. The control elements and options for the corresponding 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.

As default, the predefined user "Administrator" is available in SINEMA Server that is assigned to the user group of the same name.

The range of access rights when working with SINEMA Server depends on the user group to which the user belongs. The default assignment of rights to user groups is explained below:

Access right	Description	Administrator	Power user	Standard user
Server access via URL	Access right for the function call via URL As default, this right is disabled for all user groups. For security reasons, it should only be enabled for user groups with restricted access rights.	No	No	No
View discovered topology	Access right allowing display of the discovered topology	Yes	Yes	Yes
View reports	Access to the display of reports	Yes	Yes	Yes
Operative monitoring settings	Access right allowing management of devices, views and SINEMA Server instances	Yes	Yes	No
User settings	Access right allowing administration of users and user groups	Yes	No	No
Basic settings for discovery and monitoring	Access right for the basic discovery and monitoring settings	Yes	Yes	No
View monitored topology	Access right allowing display of the monitored topology	Yes	Yes	Yes
View all devices and servers	View all devices and servers regardless of the assignment to views	Yes	Yes	No
View server overview	Access right for the server overview	Yes	Yes	Yes
System settings	Access right for settings under "Administration > System"	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?
1. When necessary, create new user groups. (See also section Administration - Users user groups (Page 202))
  2. Create new users and assign these to the required user groups. (See also section Administration - User User (Page 200))

When necessary, assign views to the users. As a result, the response of the Web user interface of SINEMA Server terms of the devices and SINEMA Server instances that can be monitored depends on the specific view.

## Using SINEMA Server - reference section

### 4.1 Program user interface in detail - overview of the menus

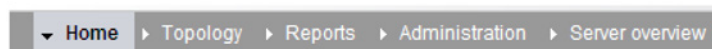
#### 4.1.1 User interface

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



Start menu command	Meaning	See section
No other sub entries	The start window of SINEMA Server provides a quick overview of the status of the network.	Start window (Page 94)

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. After selecting the "Topology" menu command, the discovered topology is displayed if no reference topology has yet been configured.	Topology - Discovered (Page 131)
...Monitored	Shows you the current status of the network based on the desired status specified in the reference topology. After selecting the "Topology" menu command, the monitored topology is displayed if a reference topology has already been configured.	Topology - Monitored (Page 136)
...Reference	Starts the Reference editor. With this tool, you configure the reference topology, i.e. the desired status of the network.	Topology - Reference (Page 141)
...Unmanaged devices	Manage devices that provide no or little opportunity for changing the way they work or the device data.	Topology - Unmanaged device types (Page 156)

## 4.1 Program user interface in detail - overview of the menus

Menu command	Tab	Meaning	See section
<b>Reports &gt;...</b>			
<b>...Availability &gt;</b>	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 160)
	Interfaces	All the interfaces of the devices are displayed individually.	
<b>...Performance &gt;</b>	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 162)
	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.	
	Discarded packets	The number of discarded incoming packets and the number of discarded outgoing packets is displayed for all LAN and WLAN interfaces.	
<b>...Inventory &gt;</b>	Vendor	Overview of the devices according to the manufacturer identifier.	Reports - Inventory (Page 164)
	IP address range	Overview of the devices according to IP address ranges.	
	Device category	Overview of the devices according to device types (switch etc.)	
	PROFINET	Overview of the devices that have a PROFINET name.	
<b>...Events &gt;</b>	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 165)
	System events		

## 4.1 Program user interface in detail - overview of the menus

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 172)
	Profiles	You can edit displayed profiles or add new profiles.	Administration - Discovery / Profiles (Page 175)
...Monitoring >	General	Set the time parameters for network monitoring and globally enable the monitoring modes for devices with SIMATIC and PROFINET capability.	Administration - Monitoring General (Page 182)
	SNMP settings	Basic settings for discovery using the SNMP protocol.	Administration - Monitoring SNMP settings (Page 185)
	Polling groups > Fast / Medium / Slow	Depending on the requirements, assign the devices to the 3 possible polling groups.	Administration - Monitoring Polling groups (Page 186)
	OPC	Select devices whose data will be sent to an OPC server.	Administration - Monitoring OPC (Page 189)
...Events	Event types	Make the settings for the display and representation of the network and system events.	Administration - Events (Page 190)
	Overall status groups	View / configure groups of functionally related events that influence the overall status of devices.	Administration - Events Overall status groups (Page 193)
	Event reactions	Define view-specific, system- and device-specific reactions to events.	Administration - Events > Event reactions (Page 198)
...User	User	Assign users to groups and views.	Administration - User User (Page 200)
	User groups	Create user groups with rights.	Administration - Users user groups (Page 202)
	Logon locks	Cancel logon locks for users and IP addresses	Administration - User Logon locks (Page 204)
...System	System information	Display information about the management station	Administration - System System information (Page 204)
	Configuration	Functions for saving, importing or resetting the configuration data of SINEMA Server and for specifying the shared secret.	Administration - System configuration (Page 205)
	E-mail settings	Specify e-mail settings required for event reactions.	Administration - System / E-mail settings (Page 205)

## 4.1 Program user interface in detail - overview of the menus

Menu command	Tab	Meaning	See section
Administration >...			
...My settings	Password	Changing your password	Administration - My settings Password (Page 206)
	User interface	Here, you specify the update interval for all user interface components relevant for monitoring.	Administration - My settings User interface (Page 206)

Server overview menu command	Meaning	Section
No other sub entries	Display of the overall statuses of devices monitored by other SINEMA Server instances in the network. These SINEMA Server instances can be called directly from the server overview.	Server overview (Page 207)

## See also








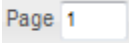



Administration - Monitoring SNMP settings (Page 185)

Administration - Events Event types (Page 190)

## General functions for the page layout

All tables have a footer with which you can specify the page layout. Other functions are used for navigation within the particular Web page.

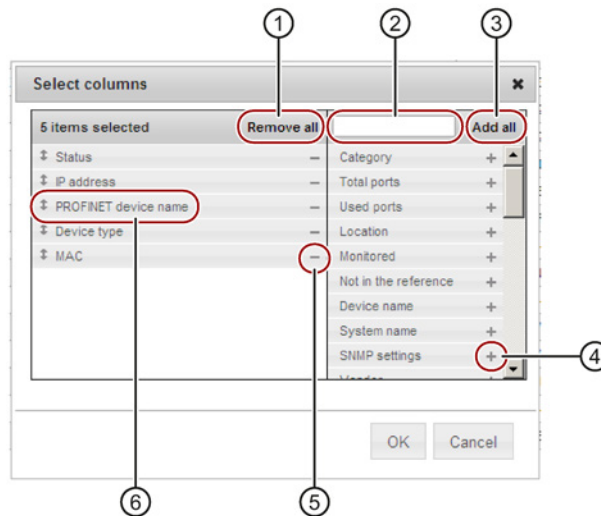
Depending on the particular Web page, you have a selection of the following functions:

Icon	Display / function	Icon	Display / function
	Select and position columns for display.		User-specific saving of the following user interface parameters: <ul style="list-style-type: none"> <li>• Column selection</li> <li>• Column order</li> <li>• Column width</li> <li>• Column sorting</li> <li>• Number of entries per page</li> <li>• Filter setting using a selection list</li> </ul>
	Select saved column layout.		Use default column layout
	Export table in CSV format		Go to first page.
	Go back one page.		Display the current page and option to scroll directly to specific page.
	Go forward one page.		Go to last page.
	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 of the same page  
Click the check box in the header.
- Deselect single entries  
Holding down the Ctrl key, click the check box of the selected entry.

#### 4.1.1.1 Filtering data with filter templates

##### Function of filter templates

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

##### Settings of filter templates

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

###### 1. Prefilters

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

###### 2. Complex filter

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

###### 3. Simple filter

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

##### Use of filter templates

Filter templates can be used to filter the following lists:

- Event list
- Device list
- Interface list
- Reports

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









## Control elements of the filter template editor

The following table explains the functions of the control elements of a filter template.

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

## Control elements of the editor for complex filters

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

Operator control element	Function
Complex filter	Textual representation of the created filter. The textual representation is updated when using the control elements of the editor.
	As an alternative to using the buttons and drop-down lists of this editor, the filter text can also be edited manually. Using the arrow icon, the modified filter text is validated and adopted for the control elements of the editor.
	Specifies whether the filter rules of the current rule level will be linked with the logical operator "AND" or "OR".
	Inserts a new rule level below the current rule level. Filter rules can be nested within each other using rule levels. Filter rules of the same rule level are shown in the query box in a common bracket.
	Inserts a new filter rule at the current rule level.  Every filter rule contains a selectable column name, a selectable operator and an input box in which the value of the selected column to be checked with the operator can be entered.
	Deletes the rule level or the filter rule.
Cancel	Discards changes to the open complex filter and closes the filter editor.

Operator control element	Function
Reset	Discards changes to the open complex filter.
Apply	Saves the settings for the complex filter and closes the filter editor. The created complex filter is now displayed in the "Complex filter" box of the filter template editor.

## 4.1.2 Online help

### Opening help pages

You have the following options:

- Opening a context-dependent page

On every Web page in SINEMA Server, you can display a page of the online help describing the current context by clicking the question mark icon in the status bar. In addition to this, in the "Device details" window, the shortcut menu command "Open help" is available to open the help page for the device details.

- Opening any help page - navigating in the online help

After you have opened a context-dependent help page, you can navigate to any help pages of SINEMA Server with the navigation panel on the left hand side.

- Opening a topic-related help page (only with Internet Explorer)

In most help pages, you can open other help pages relating to the current topic with the "Basics" menu command.

---

#### Note

##### Opening using the question mark icon - new window in the Web browser

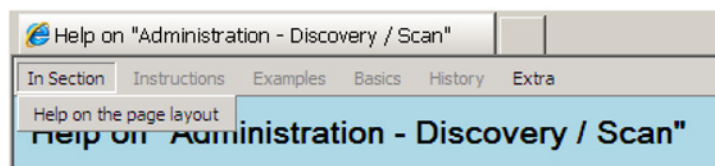
Every help page you open using the question mark icon opens in a new window of your Web browser.

This does not apply to help pages you open using the menu commands in the open online help described below.

---

### Menu commands

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




Menu command	Meaning
In Section > ...	Option for selecting sections in the open help page
Instructions	- not used -
Examples	- not used -
Basics	Option for opening help pages whose content is related to the topic of the selected help page.
History > ...	Option for selecting previously opened help pages.
Extra	Opens the navigation page of the online help. From the navigation page, you can open all the help pages of the online help of SINEMA Server.
Extra > Back	Opens the previously opened help page.
Extra > Next	Opens the next help page in the history of previously opened help pages following the currently open help page. If the currently displayed help page is the last page in the history, the menu command has no effect.

**Note****Opening help pages using "History" or "Extra"**

The history only includes help pages that have already been opened in the currently open Web browser window and only these can be selected.

### 4.1.3 Quick links

**Meaning**

With the "Quick links" function element , you can manage and use 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.

#### 4.1 Program user interface in detail - overview of the menus

4. Assign a name for the Web page that you would like entered in the list of quick links.
5. As an option, you can define one of the created direct references as the start page with 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.

#### 4.1.4 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.

The following actions are possible:

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

#### 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.

#### NOTICE

##### Recommendation

When entering the login data, we strongly advise you to use the HTTPS protocol for security reasons. The data is transferred encrypted and cannot be read by unauthorized third persons.

## Basic parameters for calling Web pages

Below there is an example of a call for a specific Web page. The parameters used in this are explained in the following table.

Example: Display of a certain device in the topology representation "Detected"

"https://sinemaserver:443?path=mnu\_network\_actual&  
ip=192.168.110.34&username=john&password=blue&topology\_view=icon\_view&onlycontent  
area=yes"

Table 4- 1 Basic parameters for the Web page call

Parameter	Meaning
path	Path of the SINEMA Server Web page to be displayed, see section below.
ip	IP address of a device. The IP address needs to be included in the URL in the following situations: <ul style="list-style-type: none"> <li>• If the device details of a specific device should be included</li> <li>• If you want a specific device to be displayed after the topology display is opened.</li> </ul>
username	Name of the user logging in
password	User-specific password

## 4.1 Program user interface in detail - overview of the menus

Parameter	Meaning
topology_view	Specifies whether or the detailed view or the icon view is displayed when calling the discovered, monitored or view-specific topology. If the parameter is not specified, the detailed view is shown. detailed_view: The detailed view is displayed. icon_view: The icon view is displayed.
onlycontentarea	Specifies whether or not only the SINEMA Server main window is displayed. YES: Only the main window is displayed.

## Parameter "path"

Path	Called Web page / corresponding menu command on the Web client
path=main_logout	The user that calls the function is logged out of the SINEMA Server instance. The function call applies only for the session in which it occurs. Other sessions remain unaffected by the function call.
path=main_kill_session&username=Administrator&password=SinemaA	End all sessions of a user. Note: The parameters for user name and password must be specified with this function call. In the example shown, the user name is "Administrator" and the password "SinemaA".
path=mnu_admin_event&tabname=admin_condition_grp	Administration > Overall status groups
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=mnu_reports_availability	Reports > Availability > Devices
path=mnu_reports_performance	Reports > Performance > LAN - Interface utilization
path=mnu_reports_inventory	Reports > Inventory > Vendor
path=mnu_reports_events	Reports > Events > Network events
path=views_tabs&params=views_{view name}	Shows the named user-specific view. The device list is displayed.
path=views_tabs&params=views_{view name}&tabname=views_topology	Shows the named user-specific view. The view-specific topology is displayed.
path=device_list&params=alldevices_ipAddress	Device list with devices that have the specified IP address.

## 4.1 Program user interface in detail - overview of the menus

Path	Called Web page / corresponding menu command on the Web client
path=device_list&params=alldevices_profinet	Device list with devices that have the specified PROFINET device name.
path=device_list&params=devicetype_WLAN Client	Device list with devices of the WLAN category
path=device_list&params=devicetype_Others	Device list with devices of the "Others" category
path=device_list&params=devicetype_Gateway	Device list with devices of the "Gateway" category
path=device_list&params=devicetype_Switch	Device list with devices of the "Switch" category
path=device_list&params=devicetype_Access Point	Device list with devices of the "Access point" category
path=device_list&params=devicetype_End Device	Device list with devices of the "End device" category
path=device_list&params=local_Not Connected	Device list with devices with the "Not connected" status
path=device_list&params=local_Ok	Device list with devices with the "OK" status
path=device_list&params=local_Fault	Device list with devices with the "Fault" status
path=device_list&params=local_Maintenance demanded	Device list with devices with the "Maintenance demanded" status
path=device_list&Params=local_Maintenance required	Device list with devices with the "Maintenance required" status
path=device_list&Params=local_Not reachable	Device list with devices with the "Not reachable" status
path=device_list&Params=local_Not Monitored	Device list with devices with the "Not monitored" status
path=device_list&params=vendor_Siemens AG	Device list with devices of the "Manufacturer / Siemens AG" category
path=device_list&params=vendor_Microsoft	Device list with devices of the "Manufacturer / Microsoft" category
path=device_list&params=vendor_ciscoSystems	Device list with devices of the "Manufacturer / Cisco systems" category
path=device_list&params=vendor_Unknown	Device list with devices of the "Manufacturer / Unknown" category
[call up a device list]&tabname=interfaces	Opening the interface list from one of the device lists mentioned above
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 "Overview" 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=simatic	Device details in the "SIMATIC" tab
path=device_details&ip={ip address}&tabname=profinet	Device details in the "PROFINET" 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 on 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

**Basic parameters for the CSV/JSON download of the content of a Web page**

Below there is an example of the download of a specific Web page. The parameters used in this are explained in the following table.

Example: CSV download of the content of the Web page "Reports > Availability > Devices" in English specifying the start and end date to be taken into account:

"https://localhost/exportTable?command=IF\_RequestReports&username=user&password=user123&report\_type=4&report\_startDate=2015-02-04 10:16:03&report\_endDate=2015-02-05 10:16:03"

Table 4- 2 Basic parameters for the Web page download

Parameter	Meaning
exportTable?	Indicates that this is a download of Web page content.
command	Indicates which Web page type should be downloaded. The following are available: <ul style="list-style-type: none"> <li>• Reports</li> <li>• Event list</li> <li>• Device list</li> <li>• Interface list</li> </ul> The values of this parameter and the filter parameters are described in the tables below.
username	Name of the user logging in
password	User-specific password
language	Display language of the content to be downloaded. Possible values: <ul style="list-style-type: none"> <li>• de</li> <li>• en</li> <li>• fr</li> <li>• zh</li> </ul> Default setting if the parameter is not used: en
download	Format for the download. Possible values: <ul style="list-style-type: none"> <li>• csv</li> <li>• json</li> </ul> Default setting if the parameter is not used: csv



## Parameters for downloading reports

Parameter	Meaning
command=Sinema_GetReports	Indicates the download of reports.
report_type	<p>Indicates the report type to be downloaded. The values of the individual report types are:</p> <ul style="list-style-type: none"> <li>• Availability &gt; Devices: 4</li> <li>• Availability &gt; Interfaces: 5</li> <li>• Performance &gt; LAN - Interface utilization: 6</li> <li>• Performance &gt; LAN - Interface error rate: 7</li> <li>• Performance &gt; WLAN - Interface error rate: 9</li> <li>• Performance &gt; WLAN - Interface data rate: 8</li> <li>• Performance &gt; WLAN - Signal strength: 10</li> <li>• Performance &gt; WLAN - Number of clients: 11</li> <li>• Performance &gt; Discarded packets: 33</li> <li>• Performance &gt; POF power budget: 39</li> <li>• Inventory &gt; Vendor: 1</li> <li>• Inventory &gt; IP address range: 2</li> <li>• Inventory &gt; Device category: 3</li> <li>• Inventory &gt; PROFINET: 38</li> <li>• Events &gt; Network events: 12</li> <li>• Events &gt; System events: 13</li> </ul> <p>The possible filter parameters for event reports are described in the table below.</p>
report_endDate	<p>End date for the report data to be downloaded</p> <p>Format: yyyy-mm-dd hh:mm:ss</p>
report_startDate	<p>Start date for the report data to be downloaded</p> <p>Format: yyyy-mm-dd hh:mm:ss</p>
period	<p>Period for the data to be downloaded. Possible values:</p> <ul style="list-style-type: none"> <li>• 24 hours: 1</li> <li>• 7 days: 2</li> <li>• Unlimited: 3</li> </ul>

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

## Filter parameters for downloading events reports

Associated reports:

- Events > Network events (report\_type: 12)
- Events > System events (report\_type: 13)

## 4.1 Program user interface in detail - overview of the menus

Parameter	Meaning
eventNoted	Filter according to the status "Noted": <ul style="list-style-type: none"> <li>• Yes: 0</li> <li>• No: 1</li> <li>• All: 2</li> </ul> Default setting if the parameter is not used: 2
eventPendingStatus	Filter according to event statuses: <ul style="list-style-type: none"> <li>• All: 0</li> <li>• Not present: 1</li> <li>• Resolving: 2</li> <li>• Resolved automatically: 3</li> <li>• Resolved manually: 4</li> <li>• Pending: 5</li> </ul> Default setting if the parameter is not used: 0
classFilter	Filter according to event classes: <ul style="list-style-type: none"> <li>• Notification: Notification</li> <li>• Information: Info</li> <li>• Warning: Warning</li> <li>• Errors: Error</li> <li>• All: All</li> </ul>
protocolFilter	Filter according to protocols: <ul style="list-style-type: none"> <li>• ICMP</li> <li>• DCP</li> <li>• ARP</li> <li>• SNMP</li> <li>• SNMP trap</li> <li>• Profinet</li> <li>• SIMATIC</li> <li>• SIMATIC Diag. Events</li> <li>• Multiple protocols: Computed</li> <li>• SIMATIC Alarms</li> <li>• All: All</li> </ul> Default setting if the parameter is not used: All

Multiple parameter values can be specified separated by commas.

### Further filter parameters for downloading reports

Associated reports:

- Availability > Interfaces (report\_type: 5)
- Performance > LAN - Interface utilization (report\_type: 6)

- Performance > LAN - Interface error rate (report\_type: 7)
- Performance > Discarded packets (report\_type: 33)

Parameter	Meaning
fromIp	Filter according to "From IP address"
toIp	Filter according to "To IP address"
deviceName	Filter according to device names
deviceType	Filter according to device types
reportsCategory	Filter according to device categories: <ul style="list-style-type: none"> <li>• End Device</li> <li>• Router</li> <li>• Switch</li> <li>• Gateway</li> <li>• Access Point</li> <li>• WLAN Client</li> <li>• PLC</li> <li>• PC/HMI</li> <li>• PC-CP</li> <li>• PLC-CP</li> <li>• Ident</li> <li>• Motion</li> <li>• Power</li> <li>• Others</li> <li>• All</li> </ul> Default setting if the parameter is not used: All
statistics	Filter according to ports on which port statistics are activated or deactivated: <ul style="list-style-type: none"> <li>• All: All</li> <li>• Port statistics enabled: Yes</li> <li>• Port statistics disabled: No</li> </ul> Default setting if the parameter is not used: All
deviceFilter	Filter according to devices: <ul style="list-style-type: none"> <li>• All devices: All</li> <li>• Existing devices: existing</li> </ul> Default setting if the parameter is not used: All This filter parameter is available for all reports.

Multiple parameter values can be specified separated by commas.

**Parameters for downloading event lists**

Parameter	Meaning
command=Sinema_GetEvents	Indicates the download of event lists.
eventNoted	Filter according to the status "Noted": <ul style="list-style-type: none"> <li>• Yes: 0</li> <li>• No: 1</li> <li>• All: 2</li> </ul> Default setting if the parameter is not used: 2
eventPendingStatus	Filter according to event statuses: <ul style="list-style-type: none"> <li>• All: 0</li> <li>• Not present: 1</li> <li>• Resolving: 2</li> <li>• Resolved automatically: 3</li> <li>• Resolved manually: 4</li> <li>• Pending: 5</li> </ul> Default setting if the parameter is not used: 0
period	Period for the data to be downloaded. Possible values: <ul style="list-style-type: none"> <li>• 24 hours: 1</li> <li>• 7 days: 2</li> <li>• Unlimited: 3</li> </ul> Default setting if the parameter is not used: 1
classFilter	Filter according to event classes: <ul style="list-style-type: none"> <li>• Notification: Notification</li> <li>• Information: Info</li> <li>• Warning: Warning</li> <li>• Errors: Error</li> <li>• All: All</li> </ul>
CategoryFilter	Filter according to event categories: <ul style="list-style-type: none"> <li>• Network events: Network</li> <li>• System events: System</li> <li>• All: All</li> </ul> Default setting if the parameter is not used: All

Parameter	Meaning
protocolFilter	Filter according to protocols: <ul style="list-style-type: none"> <li>• ICMP</li> <li>• DCP</li> <li>• ARP</li> <li>• SNMP</li> <li>• SNMP trap</li> <li>• Profinet</li> <li>• SIMATIC</li> <li>• SIMATIC Diag. Events</li> <li>• Multiple protocols: Computed</li> <li>• SIMATIC Alarms</li> <li>• All: All</li> </ul> Default setting if the parameter is not used: All
startDate	Start date for event list to be downloaded Format: yyyy-mm-dd hh:mm:ss
endDate	End date for event list to be downloaded Format: yyyy-mm-dd hh:mm:ss

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

Multiple parameter values can be specified separated by commas.

### Parameters for downloading device lists

Parameter	Meaning
command=Sinema_GetDevices	Indicates the download of device lists.

### Parameters for downloading interface lists

Parameter	Meaning
command=Sinema_GetInterfaces	Indicates the download of interface lists.

### 4.1.5 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

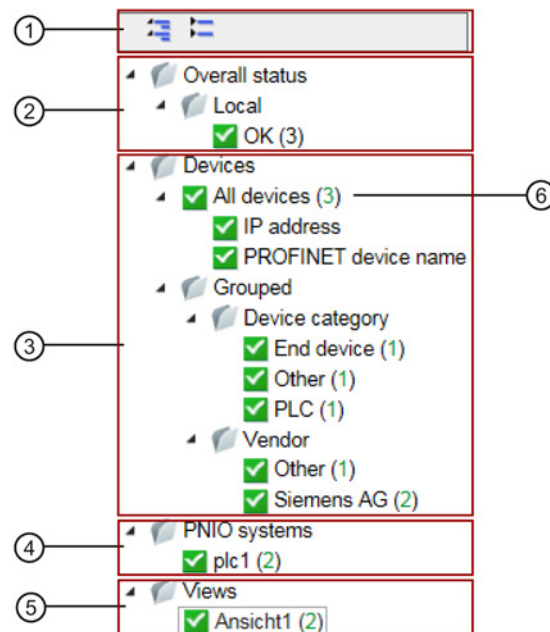
The start window provides the following information:

- 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, notification) of unnoted events, divided into network and system events.

### 4.1.6 Device tree

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

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



- ① Button for expanding or collapsing the nodes
- ② Device nodes with filters for overall statuses of devices of this and other SINEMA Server instances
- ③ Device nodes for all devices and device nodes with filters for device categories, vendor and alternating devices





- ④ Device nodes for PROFINET IO systems
- ⑤ Node for user-specific views
- ⑥ Specifies the number of nodes contained in the particular device branch

## Layout



- "Overall status" node:  
Below the "Overall status" node, the numbers of overall statuses of local devices as well as the devices monitored by other SINEMA Server instances are shown. Selecting an overall status below the "Local" entry generates a filtered display of the device or interface window according to the overall status. Selecting an overall status below the "Server overview" entry generates a display of the server overview sorted according to the overall status.
- "Devices" node:  
The entries below the "Devices" node provide the option of displaying all devices or only devices of a specific category or a specific vendor or only alternating devices in the devices and interfaces window. The colors of the numbers in brackets indicate the overall statuses of the devices.
- "PNIO systems" node:  
The entries below the "PNIO systems" node provide the option of displaying only the controller and the PROFINET IO devices of a certain PROFINET IO system. The entries below the "PNIO systems" node are named after the PROFINET IO name of the relevant controller. The colors of the numbers in brackets after the name indicate the overall statuses of the associated PROFINET devices. The requirements for displaying a PNIO system are described in the section "Options for displaying PROFINET I/O systems".
- "Views" node:  
For certain purposes, you can define user-specific views that include only some of the existing devices or only part of the overall network. For more detailed information on this topic, refer to the section "Setting up and using views (Page 62)".

## 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: Not connected See section Alternating devices (Page 120)
	Device status: OK
	Device status: Maintenance required
	Device status: Maintenance urgently required



Icon for the status	Description
	Device status: Error
	Device not reachable

**Note****Display of the status of the management station**

If changes are made to network adapters of the management station, this can influence the display of the status of the management station in SINEMA Server. Follow the steps below to restore the status display of the management station after changes to the network adapter configuration:

1. Restart the PC being used as the management station.
2. In SINEMA Server, delete the management station from the device list.
3. Run a network scan.

**Options for displaying PROFINET IO systems**

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

- Devices with SIMATIC capability:

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

- Other controller types:

The PROFINET IO system can be displayed with the aid of information that PROFINET IO devices obtain from their controller. To do this, the monitoring setting "PROFINET monitoring" must be enabled for the PROFINET IO devices to be displayed. PROFINET IO devices that cannot be assigned are displayed under the entry "Unassigned devices". If the display of the PROFINET IO system was initiated by PROFINET IO devices, the tooltip of the associated entry displays "Discovered by: IO devices".

**See also**

Server overview (Page 207)

## 4.1.7 Device window with device list

Status	IP address	PROFINET device name	Device type	MAC address	Active SIMATIC/f	SiSe receiver
	190.171.3.19	cpu319	CPU 319-3 PN/DP (3EL01-0AB0)	00:0E:8C:F8:B4:AE		Yes
	190.171.0.70	pn-io	CPU 414-3 PN/DP (3EM05-0AB0)	00:0E:8C:98:B8:79		No
	190.171.3.9	et200s-cpu	ET200S PN/DP CPU (8AB01-0AB0)	00:0E:8C:F6:07:2A		Yes
	190.171.0.60	pn-io-2	CPU 315-2 PN/DP (2EH13-0AB0)	00:0E:8C:8A:68:F6		Yes
	190.171.0.65	cpu414-65	SIMATIC_S7_400_PL	00:1B:1B:AF:AE:4B		Yes
	190.171.0.88	et200pro-88	ET200PRO PN/DP CPU (8AB01-0AB0)	00:0E:8C:C9:06:95		Yes
	190.171.3.10	cpu412-3-10	CPU 412-2 PN (2EK06-0AB0)	00:1B:1B:A0:F4:45		Yes
	190.171.3.15	cpu315-3-15	CPU 315-2 PN/DP (2EH14-0AB0)	28:63:36:0C:0E:1F		Yes
	190.171.0.150+	cpu1516-3pn-150.profinet-schnittstelllexb13b0	CPU 1516-3 PN/DP (3AN00-0AB0)	00:1B:1B:13:86:C1+		-

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

## Display

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

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

## Content






Device lists are divided into several columns in which the device-specific data is displayed. With the exception of the first column that is used to select rows, you can select any other column as required. Values that can no longer be updated because protocol reachability is not available are displayed grayed out.

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

- Status
- IP address
- PROFINET device name
- Device type
- MAC address
- Active monitoring status, see section "Possible monitoring statuses"
- Configured SIMATIC/PROFINET monitoring settings
- Automation role
- PROFINET reachability
- Assigned controller
- PROFINET channel status
- SINEMA Server is the recipient of SIMATIC event / SIMATIC alarm messages
- Total ports
- Used ports
- Deployment / installation location
- Not in the reference (yes / no)
- Device name
- System name
- SNMP settings (name)
- Vendor
- Article 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
- General profile
- Monitoring profile
- Statistical attachment data read in (yes / no)

## Possible monitoring statuses

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

Icon	Meaning
	The device is not monitored.
	<p>The PROFINET IO device becomes passive; in other words, only monitored by the CPU with SIMATIC capability assigned to the device. Passively monitored devices are shown only in the PNIO system they belong to. For passively monitored devices, no PROFINET monitoring settings can be configured.</p> <p>The passive monitoring of devices can be selected when the devices cannot be reached by SINEMA Server. Passively monitored devices do not require a device license. The requirement for passive monitoring is that the CPU with SIMATIC capability can be reached by SINEMA Server and that the monitoring setting "SIMATIC monitoring of assigned devices" is active for this CPU.</p>
	The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP.
	<p>The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring mode is also active:</p> <ul style="list-style-type: none"> <li>• PROFINET: The PROFINET monitoring of the PROFINET IO device by SINEMA Server is active.</li> <li>• SIMATIC: The SIMATIC monitoring of the CPU with SIMATIC capability by SINEMA Server is active.</li> </ul>
	<p>The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring modes are also active:</p> <ul style="list-style-type: none"> <li>• PROFINET: <ul style="list-style-type: none"> <li>– The PROFINET monitoring of the PROFINET IO device by SINEMA Server is active.</li> <li>– The PROFINET acquisition of port statistics of the PROFINET IO device by SINEMA Server is active.</li> </ul> </li> <li>• SIMATIC: <ul style="list-style-type: none"> <li>– The SIMATIC monitoring of the CPU with SIMATIC capability by SINEMA Server is active.</li> <li>– The SIMATIC monitoring of the PROFINET IO devices assigned to the controller by the CPU with SIMATIC capability is active.</li> </ul> </li> </ul> <p>The SIMATIC monitoring of SIMATIC event / alarm messages is not shown in the displayed monitoring status.</p>

## Operator input

The following table shows the functional elements of the header.

Table 4- 3 Basic settings























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

Table 4- 4 Advanced settings

Icon	Display / function	Icon	Display / function
	Add or change comment		Delete remark
	<p>Enable monitoring</p> <p>Enable monitoring for the selected devices. The PROFINET/SIMATIC monitoring that may be available for the device is performed according to the configured global and local PROFINET/SIMATIC monitoring settings.</p> <p>If the selected device is a PROFINET IO device and if the monitoring of assigned devices is activated for the controller assigned to it, as an alternative to activating monitoring by SINEMA Server, you can activate passive monitoring. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.</p>		<p>Turn off monitoring</p> <p>Disable monitoring for the selected devices. If the selected device is a monitored PROFINET IO device and if the monitoring of assigned devices is activated for the controller assigned to it, as an alternative to fully disabling monitoring, you can also enable passive monitoring. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.</p>
	<p>Change local monitoring settings</p> <p>The local PROFINET/SIMATIC monitoring settings functionally correspond to the global PROFINET/SIMATIC monitoring settings.</p> <p>When SIMATIC monitoring is activated for a device, SNMP is used to check whether the device has a firmware version that has been released for SIMATIC monitoring by the SINEMA Server. To activate SIMATIC monitoring for a device, this must therefore be reachable via SNMP and must have information about the installed firmware version.</p> <p>Local monitoring settings only take effect on devices when the global monitoring settings of the same name are active.</p> <p>Devices with PROFINET/SIMATIC capability can also be configured as alternating devices.</p>		Create new device
	<p>Delete device</p> <p>After it is deleted, the device only continues to exist in the report archive.</p> <p>When you delete a PROFINET IO device being monitored by a CPU with SIMATIC capability using the function "SIMATIC monitoring of assigned devices", this PROFINET IO device is discovered by the controller again after it has been deleted and therefore shown again in the corresponding PNIO system.</p>		Specify SNMP settings

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 profile</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"> <li>User-defined links</li> </ul> <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"> <li>Basic data</li> </ul>		Set device basic data

### Prefilters in the filter templates for device lists

Device lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for device lists.

Box group	Filter options
Basic filter	<p>Filter according to devices for which the port statistics are activated /deactivated:</p> <ul style="list-style-type: none"> <li>All</li> <li>Yes: Devices with activated port statistics</li> <li>No: Devices with deactivated port statistics</li> </ul> <p>Filter according to devices that are part / not part of the reference topology:</p> <ul style="list-style-type: none"> <li>All</li> <li>Yes: Devices that are part of the reference topology</li> <li>No: Devices that are not part of the reference topology</li> </ul>
Monitoring status	Filter according to devices with a certain monitoring status.

### Functions of the shortcut menu

The functions presented above can also be called alternatively using the shortcut menu. The shortcut menu also provides the option of calling up the discovered topology, the monitored topology, the reference topology or a view-specific topology from the device window. The device selected using the shortcut menu is shown centered and selected in the selected topology representation.

**See also**

- User interface (Page 75)
- Administration - Monitoring General (Page 182)
- Filtering data with filter templates (Page 80)
- Device details (Page 107)
- Alternating devices (Page 120)

**4.1.8 Device window with interface list**

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

- ① Header with toolbar
- ② Interface list with configurable columns
- ③ Footer with setting functions and configuration limits (identical to the footer of the device list)

**Display**

You can open interface lists of SINEMA Server by selecting an entry in the device tree. In the device window, then select the "Interfaces" tab.

Depending on the entry you select in the device tree, the interface list shows the interfaces of all devices or only the interfaces of a specific group of devices.

**Operation / content**




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









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

- IP address of the device
- Name of the device
- Name of the interface
- Alias name of the interface
- Status of the interface
- Administrated status
- MAC address of the device
- Connector type of the interface (configured by the user, otherwise the detected connector type)
- Connector type of the interface (detected)
- Speed (Mbps)
- Mode (full duplex or half duplex)
- Detected: connected to IP
- Detected: connected to port
- Detected: connected to device
- Interface statistics (enabled / disabled)
- Channel
- Connected to MAC address
- Critical clients
- Type of the device
- Discarded incoming packets
- Discarded outgoing packets
- MAC address of the interface
- Performance critical
- Interface index (unique number of the connector)
- Description of the interface
- Redundancy protocol
- Redundancy status
- Redundancy role
- Connected to IP (value from monitored topology if the reference topology is configured)
- Connected to port (value from monitored topology if the reference topology is configured)
- Connected to device (value from monitored topology if the reference topology is configured)
- Data traffic sending (Mbps)
- Data traffic receiving (Mbps)
- Transmit utilization FD (degree of utilization as a percent with full duplex)
- Transmit utilization HD (degree of utilization as a percentage with full duplex)
- HD Combined utilization (combined degree of utilization as percentage with half duplex)
- 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)
- Link aggregation
- Frequency

The following table shows the functional elements of the header.

Icon	Display / function
	Show device details Depending on whether the selected interface is a LAN or WLAN interface, the "LAN" or the "WLAN" tab of the device details is opened.
	Edit port details The dialog for editing interface information opens.
	Enable / disable interface statistics. If the interface statistics are disabled, the interface is not included in reports that can be generated with "Reports > Availability > Interfaces".

## 4.1 Program user interface in detail - overview of the menus

Icon	Display / function
	<p>Enter text to filter based on events. The entered text is searched for in all columns.</p> <p>In the input box, text is displayed when a simple query entered in the filter template editor is active.</p> <p>The  icon is displayed when a filter template with prefilter settings is active.</p> <p>The  icon is displayed when a filter template with a complex query is active.</p>
	<p>Selection of a previously created template for filtering according to interfaces. After selection, the properties of the filter template are applied to the interface list. Unsaved filter settings are indicated by the "*" character.</p> <p>As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.</p>
	<p>Open the editor for configuring filter settings that can be stored in filter templates.</p> <p>The  icon is displayed when the configured filter settings differ from the default filter settings.</p> <p>For more information, refer to the section "Prefilters in filter templates for interface lists".</p>

## Prefilters in the filter templates for interface lists

Interface lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for interface lists.

Operator control element	Filter options
From IP To IP	Filter according to interfaces that have the specified device IP addresses.
Device name and device type	Filter according to interfaces that belong to devices with the specified device name or device type.
Statistics activated	<p>Filter according to interfaces for which the port statistics are activated /deactivated:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Yes: Interfaces with activated port statistics</li> <li>• No: Interfaces with deactivated port statistics</li> </ul>

## See also

Device details (Page 107)

Editor for detailed information on (W)LAN ports (Page 117)

Filtering data with filter templates (Page 80)

### 4.1.9 Device details

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

Device details (190.171.0.65 / CPU 414-3 PN/DP)

Summary Status Description SIMATIC Config. LAN ports Events Expert

OK

Device identification

IPv4 address	190.171.0.65	Name	CPU 414-3 PN/DP
Device category	PLC	Device type	SIMATIC_S7_400_PLC
MAC	00:1B:1B:AF:AE:4B	System location	sysLocation not set

Pending events

Error	0	Warnings	0
Information	0		

Notes

-

Close

### Display

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

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

### 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.

---

#### Note

Which tabs are displayed depends on the device type.

---

## Operation / content

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

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

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

Table 4- 5 "Overview" tab

Parameter group	Display, content
-	Icon and overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Device name	IPv4 address, name, device category and type MAC and location
Pending events	Number of events pending for the device of the classes "Error", "Warning" and "Information"
Remarks	Comments, information

Table 4- 6 'Status' tab

Parameter group	Display, content
-	Overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Reachability	Information on the protocol-specific reachability of the device: Polling group, ICMP reachability ("Ping status"), SNMP reachability, overall status related to reachability, DCP reachability, SIMATIC or PROFINET reachability
PNIO system	In the "Device operational state" box, the device status obtained by SNMP is shown. For CPUs with SIMATIC capability, the Status LED and for PROFINET IO devices the PNIO Channel Status is shown. Notes on the LED status: <ul style="list-style-type: none"> <li>• BUS1F: First bus error LED</li> <li>• BUS2F: Second bus error LED</li> <li>• BUS2F: Third bus error LED</li> </ul>
Summary LAN ports	Total number of ports, used, active and inactive (differing from reference), as well as with a critical behavior

Parameter group	Display, content
Times	Information, when <ul style="list-style-type: none"> <li>• first and last time detected,</li> <li>• the last poll occurred,</li> <li>• the oldest stored data was read in and how long it was last active (up time)</li> </ul>
Miscellaneous	Information relating to C-PLUG, power supply status

Table 4- 7 'Description' tab

Parameter group	Display, content
Names	PROFINET IO, system and automation name
Location	Location according to system and automation
Identification and maintenance	Article number, serial number, vendor ID and name, firmware version, hardware revision, DCP-ID
Manual changes	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.
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
Port assignment protocol	<p>The "Port assignment" box displays whether or not the port-specific data of a device can be read out both using SNMP as well as using PROFINET and assigned to the corresponding ports. This is ensured when the data obtained via SNMP and PROFINET for the port assignment are compatible with each other. The port assignment allows SINEMA Server to switch over between SNMP and PROFINET depending on protocol availability. When there is such a protocol change, the following situations are distinguished:</p> <ul style="list-style-type: none"> <li>• All port information is compatible with the new protocol: The existing port information remains when there is a change of protocol.</li> <li>• Some port information is compatible with the new protocol: Only the information of the ports that can be read out and assigned via the new protocol are displayed. The information of the other ports is removed from the device details and from the topology.</li> <li>• No port information is compatible with the new protocol: The ports of the device are displayed grayed out in the device details and in the topology.</li> </ul> <p>In the "Protocol used" box, the protocol currently being used for reading out and for assigning port information is displayed. When using PROFINET, only the information of physical ports can be read out.</p>
Miscellaneous	Contact person and OPC name

## 4.1 Program user interface in detail - overview of the menus

Table 4- 8 'SIMATIC' tab (only active for CPUs with SIMATIC capability with active SIMATIC monitoring)

Parameter group	Display, content
SIMATIC identification	Information to identify the CPU with SIMATIC capability. If the CPU is assigned at least one PROFINET IO device and the CPU itself does not operate as a PROFINET IO device, the automation roll shown is "Controller". If the CPU operates both as a controller and PROFINET IO device at the same time (I device), "IO device" is displayed as the automation role.
Configured cycle time	Configured minimum and maximum value for the cycle time in ms.
Measured cycle time	The shortest, last read and longest cycle time read out by SINEMA Server in ms. The values for the cycle times are recalculated every 60 seconds.
SIMATIC status of assigned devices	This area shows how many of the assigned PROFINET IO devices have which status relating to the selected CPU: <ul style="list-style-type: none"> <li>Configured devices: Total number of devices configured as PROFINET IO devices in STEP 7.</li> <li>Active devices: Number of devices exchanging data with the controller.</li> <li>Deactivated devices: Number of devices deactivated by the controller.</li> <li>Faulty devices: Number of devices in the "Error" status.</li> <li>Missing devices: Number of devices configured as PROFINET IO devices in STEP 7 that have, however, not been reached by the controller.</li> </ul>
SIMATIC event / alarm messages	Date and time of the last logon (to receive SIMATIC event and alarm messages from the CPU with SIMATIC capability): Time of the last attempted logon to the CPU with SIMATIC capability Date and time of the last read out: Time of the last successful read out of the display texts from the CPU with SIMATIC capability Date and time of the last attempted read out: Time of the last attempt to read out the display texts from the CPU with SIMATIC capability

Table 4- 9 'PROFINET' tab (only active for PROFINET IO devices with active PROFINET monitoring)

Parameter group	Display, content
PROFINET identification	Information to identify and to assign the controller of the PROFINET IO device

Table 4- 10 'Config.' tab (Configuration)

Parameter group	Display, content
Ethernet	IPv4 address, router address (standard gateway), device MAC address, subnet mask and DHCP (enabled?)
Profinet	PNIO name and type
SNMP settings	Configuration name, traps enabled, SINEMA Server trap recipient (yes / no)

## 4.1 Program user interface in detail - overview of the menus

Parameter group	Display, content
General SNMP traps	Information about whether the following traps were enabled: <ul style="list-style-type: none"> <li>• Connection establishment and termination</li> <li>• Warm and cold restart</li> <li>• Authentication failed</li> </ul>
Miscellaneous	Radius server address; IP forwarding (yes / no / not supported) Alternating device (yes / no)

Table 4- 11 'LAN' tab

Parameter group	Display, content
-	Table of all LAN ports with name, status, MAC, transmission medium, data rate and other freely selectable information. The entire table can be formatted and used as described under for the device window (column width, export etc.). There are icons available above the table with following functions: <ul style="list-style-type: none"> <li>• Show port details</li> <li>• Change port details</li> <li>• Enable port statistics</li> <li>• Disable port statistics</li> </ul> If statistics is activated for a port, information about data traffic, port load and error rates is monitored using SNMP or possibly PROFINET.

Table 4- 12 '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. The "Open interface" icon provides you with more detailed information.

Table 4- 13 'Events' tab

Parameter group	Display, content
-	Table of all reported events with name, status, timestamp, status and other arbitrary information. The entire table can be formatted and used in the same way as the device window (Page 98) (column width, export etc.). There are icons available above the table with following functions: <ul style="list-style-type: none"> <li>• Mark events as "Noted"</li> <li>• Resolve pending events</li> <li>• Add / edit remark</li> <li>• Delete remark</li> <li>• Set filter for display (status, time, type)</li> </ul>

## 4.1 Program user interface in detail - overview of the menus

Table 4- 14 "IP Interfaces" Tab (IP interfaces)

Parameter group	Display, content
-	Display of all interfaces of a device with IP address data and the associated connection status. The table is displayed only for devices that can be reached via at least two IP addresses. With the button at the top left edge, the interface can be specified whose IP address will be displayed in SINEMA Server.

Table 4- 15 'VLAN' tab

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

Table 4- 16 'Redundancy' tab

Parameter group	Display, content
-	Table of all redundancy mechanisms used with the ports involved, protocol used, status, role (manager or client) along with supplementary information.  For more detailed information, the "Show port details" icon is available (refer to the section "Detailed information redundancy attachments (Page 98)").

Table 4- 17 'Expert' tab

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

Table 4- 18 'User-defined OIDs' tab

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



---

**Note****Display of the OID values**

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

---

## Functions of the shortcut menu

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

- Open WBM
- Reread data
- Enable/disable automatic update
- Add current window to quick links
- Log on again for SIMATIC event / alarm messages
- Open help
- Display selected device in a (view-specific) topology (only available for devices monitored by SINEMA Server)

## See also

Detailed information WLAN (Page 116)

Editor for detailed information on (W)LAN ports (Page 117)

Administration - Monitoring General (Page 182)


Alternating devices (Page 120)

## 4.1.10 Device details - subcategories

### 4.1.10.1 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"> <li>• Name of the connector (detected)</li> <li>• Interface index (unique number of the port)</li> <li>• MAC address</li> <li>• Transmission medium (user-defined)</li> <li>• Transmission medium (detected)</li> <li>• Status (up or down)</li> <li>• Admin status</li> <li>• Max. bandwidth (Mbps)</li> <li>• Mode (full duplex or half duplex)</li> <li>• Description</li> <li>• Alias name</li> </ul>
Topology	<ul style="list-style-type: none"> <li>• Device connection (IP address, device name)</li> <li>• Port connection</li> </ul> <p>Note: If a reference topology has been configured, the values in this section originate from the reference topology. If no reference topology has been configured, the values in this section originate from the discovered topology.</p>
Discovered topology	<ul style="list-style-type: none"> <li>• Device connection (IP address, device name)</li> <li>• Port connection</li> </ul>
Plastic Optical Fiber (POF)	<ul style="list-style-type: none"> <li>• Signal delay (ns)</li> <li>• Calculated cable length (m), according to the calculation in STEP 7</li> <li>• Power budget</li> </ul>
Data traffic	<ul style="list-style-type: none"> <li>• Transmit (transmission speed in Mbps)</li> <li>• Receive (receive speed in Mbps)</li> </ul> <p>This data is only monitored if port statistics is activated.</p>
Utilization	<ul style="list-style-type: none"> <li>• FD Transmit utilization (degree of utilization as a percent with full duplex)</li> <li>• FD Receive utilization (degree of utilization as a percent with full duplex)</li> <li>• HD Combined utilization (combined degree of utilization as percentage with half duplex)</li> </ul> <p>This data is only monitored if port statistics is activated.</p>

Group	Display, content
Error	<ul style="list-style-type: none"><li>• FD Transmit error rate (error rate as a percentage with full duplex)</li><li>• FD Receive error rate (error rate as a percentage with full duplex)</li><li>• HD Combined error rate (combined error rate as percentage with half duplex)</li><li>• FD Number of send errors (number of outgoing packets discarded with full duplex)</li><li>• FD number of receive errors (number of incoming packets discarded with full duplex)</li><li>• HD comb. number of errors (combined number of discarded packets with half duplex)</li><li>• Discarded outgoing packets</li><li>• Discarded incoming packets</li></ul> <p>This data is only monitored if port statistics is activated.</p>
Miscellaneous	Time at which connector data is saved for statistical purposes

#### 4.1.10.2 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"> <li>• Name of the connector (detected)</li> <li>• Description</li> <li>• Interface index (unique number of the port)</li> <li>• Authentication type (e.g. WEP or WPA2-PSK)</li> <li>• SSID (names of the WLANs (wireless networks) assigned to the interface)</li> <li>• BSSID (ID numbers of the WLANs assigned to the interface)</li> <li>• Mode (wireless standard acc. to IEEE: e.g. 802.11n or 802.11g)</li> <li>• Channel (wireless channel of the interface)</li> <li>• Frequency (wireless frequency of the interface)</li> <li>• Max. data rate (Mbps)</li> <li>• Mode (full duplex or half duplex)</li> </ul>
Status	<ul style="list-style-type: none"> <li>• Status (up or down)</li> <li>• Signal strength (strength of the wireless signal in dBm)</li> <li>• Transmit data rate (transmit speed in Mbps)</li> <li>• Receive data rate (receive speed in Mbps)</li> <li>• Transmit error rate (error rate as a percentage)</li> <li>• Receive error rate (error rate as a percentage)</li> <li>• Number of clients (number of clients connected via this interface)</li> </ul>

Group	Display, content
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"> <li>• Slot number (number of the connected interface)</li> <li>• Client name</li> <li>• Client IP (IP address of the connected client)</li> <li>• Client MAC (MAC address of the connected client)</li> <li>• Transmit data rate (transmit speed in Mbps)</li> <li>• Receive data rate (receive speed in Mbps)</li> <li>• Transmit error rate (error rate as a percentage)</li> <li>• Receive error rate (error rate as a percentage)</li> <li>• Critical performance (information as to whether or not the existing connection needs to be considered critical)</li> <li>• Signal (signal strength of the existing connection in dBm)</li> <li>• Signal state (indicates whether the signal strength is OK, low or high)</li> </ul>

#### 4.1.10.3 Editor for detailed information on (W)LAN ports

##### Opening the editor

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

Select the port and then click the  icon.

##### Operation / content

The following tables explain the contents of the box.

Table 4- 19 Basic data (only for LAN ports)

Parameter	Meaning
Connector type	Display of the connector type detected by SINEMA Server
Connector type (user-defined)	Selection of the connector type

Table 4- 20 Port monitoring

Parameter	Meaning
Reference port status - Up	The desired status for the port in the reference topology is "Up"
Reference port status - Down	The desired status for the port in the reference topology is "Down"

## 4.1 Program user interface in detail - overview of the menus

Parameter	Meaning
Unmonitored port (only for LAN ports)	<p>If this option is selected, the port is handled as follows:</p> <ul style="list-style-type: none"> <li>• Port connection statuses are not monitored</li> <li>• Events relating to port reference statuses are not displayed</li> </ul>
Docking port (only for LAN ports)	<p>If this option is selected, the port is handled as follows:</p> <ul style="list-style-type: none"> <li>• Port connection statuses are not monitored</li> <li>• Events relating to port reference statuses are not displayed</li> </ul>


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

**See also**

Alternating devices (Page 120)

**4.1.10.4 Detailed information redundant ports****Opening the display**

Alternatively the window with details for redundant connectors can be opened from the "Redundancy" 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. With the help of PROFINET monitoring, only MRP redundancy information can be displayed. The following table shows the possible content with a brief explanation.

Protocol	Group	Display, content
HRP	Basic data	<ul style="list-style-type: none"> <li>• Port name (e.g. X5P1)</li> <li>• Role (what is the task (client, master) of the interface within the ring?)</li> <li>• Port status (information about what the interface does with IP packets . forward or block)</li> </ul>
	Redundancy manager	<ul style="list-style-type: none"> <li>• Ring state (OK, disrupted)</li> <li>• Ring state changes (number of status changes already made due to disruptions in the ring)</li> <li>• Measured trip delay (indicates in ms how quickly the status change is made)</li> </ul>

## 4.1 Program user interface in detail - overview of the menus

Protocol	Group	Display, content
MRP	Basic data	<ul style="list-style-type: none"> <li>Name of the port (e.g. X5P2)</li> <li>Role (what is the task (client, master) of the interface within the ring?)</li> <li>Port state (information about what the interface does with IP packets . forward or block. Is only displayed via SNMP)</li> <li>Domain name</li> </ul>
	Redundancy manager	<ul style="list-style-type: none"> <li>Ring state (OK, disrupted)</li> <li>Ring state changes (number of status changes already made due to disruptions in the ring. Is only displayed via SNMP)</li> <li>Measured trip delay (indicates in ms how quickly the status change is made. Is only displayed via SNMP)</li> <li>Time ticks since (Is only displayed via SNMP)</li> <li>Domain error (Is only displayed via SNMP)</li> </ul>
STP or RSTP	Basic data	<ul style="list-style-type: none"> <li>Name of the port (e.g. X0P5)</li> <li>Port type</li> <li>Port STP state</li> <li>Port status</li> <li>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.</li> <li>Priority</li> <li>No . 'Forward transmissions'</li> <li>Big network support</li> <li>Passive Listening</li> </ul>
Standby	Basic data	<ul style="list-style-type: none"> <li>Name of the port (e.g. X6P1)</li> <li>Role (what is the task (master, master) of the interface on the "duplicate" connection?)</li> <li>Port state (information about what the interface does with IP packets . forward or block)</li> <li>Connection status (up, down)</li> <li>Topology changes (number of topology changes already made due to disruptions on the connection)</li> <li>Connection name (name of the standby connection. Required for identification since several may exist).</li> </ul>

### 4.1.11 Alternating devices

#### Meaning

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

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

#### Handling of alternating devices in SINEMA Server

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

Devices can be configured in the monitoring settings as alternating devices, refer to the section Device window with device list (Page 98)

---

#### Note

##### PROFINET IO devices configured as alternating

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

---

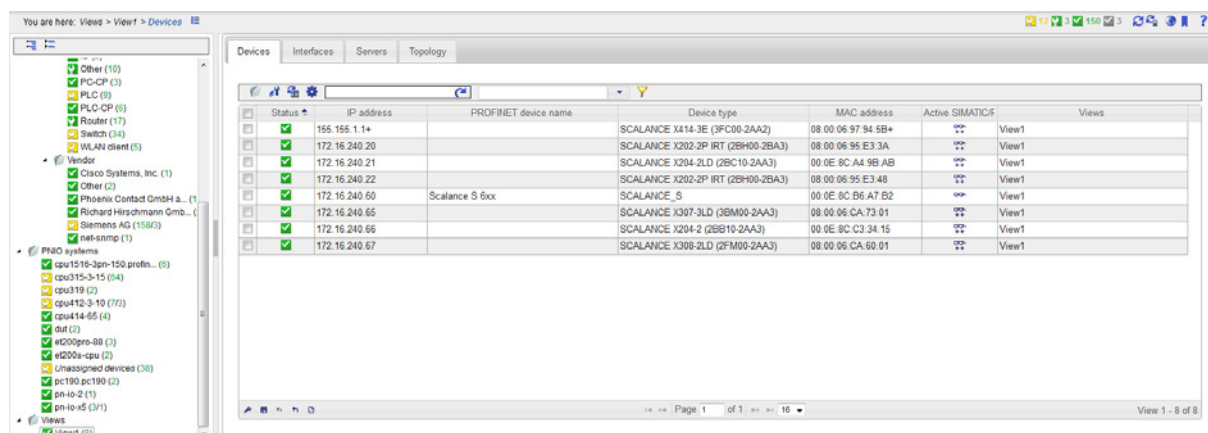
Under certain circumstances, it is useful to configure the ports to which alternating devices are connected as unmonitored or as docking ports, refer to the section Editor for detailed information on (W)LAN ports (Page 117).



## 4.1.12 Views

### 4.1.12.1 Views - Overview

The following figure shows the layout and operator controls of the "Views" window, "Devices" tab.



### Opening a view

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

The "Devices", "Interfaces" and "Servers" tabs are always present, the "Topology" tab only if this has been configured accordingly (selected).

### Working with and content of the "Devices" tab

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

### See also

Device window with device list (Page 98)

Meaning and how it works (Page 141)

Setting up and using views (Page 62)

### Working with and content of the "Interfaces" tab

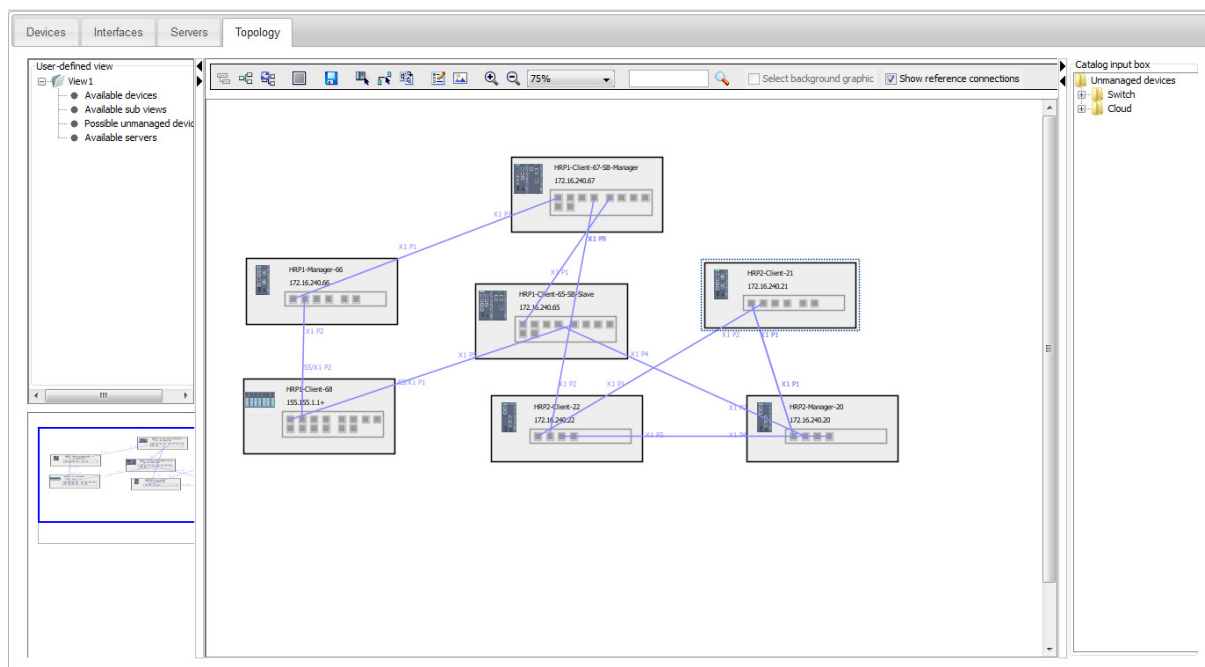
The "Interfaces" tab displays information about the interfaces of devices that were assigned to the selected view with the View editor. There is no difference compared with the interface list that is not dependent on the view.

## Working with and content of the "Servers" tab

The "Servers" tab shows SINEMA Server instances that were created in the server overview and assigned to the current view. In the server list of a view, the columns for displaying the overall device status are not available. Similar to the "Devices" tab, the "Views" column shows the names of the views to which the SINEMA Server instances are assigned.

### 4.1.12.2 Views - topology / Topology editor

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



## "Topology" tab - modes

The input options in this tab need to be distinguished as follows:

- Draft mode

In this mode, the Topology editor is enabled.

- Active mode

The network monitoring takes place in this mode.

You select the mode with the function element in the header.

If you create a new topology, the topology display is automatically in draft mode.

## Operation / content - in draft mode

In "Draft" mode, you specify the devices, SINEMA Server instances and connections between these components to be displayed and design the required view layout. In terms of functionality, it is 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. Note that SINEMA Server instances cannot be part of reference topologies. This means that functions related to reference topologies are not available for SINEMA Server instances.

Icon	Display / function	Icon	Display / function
	Select detail view		Select icon view
	Recalculate topology		Display mode Change to the active mode to monitor the network in this view.
	Save view details (draft)		Select selection mode This tool is enabled automatically when you open the page.
	Select draw mode In this mode, you configure the connections. Note: SINEMA Server instances can only have connections to other SINEMA Server instances.		Create user-defined connections for all reference connections
	Configure topology settings		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		

### Note







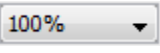


#### Moving device icons freely

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, SINEMA Server instances and connections are displayed as specified in the draft layout.

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Select detail view		Select icon view
	Display mode Change to the draft mode to specify the display layout.		Configure topology settings
	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.

## Display in 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" Web page. The color coding of the device status, ports and connections of objects correspond to those in the "Monitored topology" Web page. The following points apply to the display of SINEMA Server instances:

- The reachability status of the SINEMA Server instance is indicated by a colored line at the lower edge of the object. The meaning of the colors for the instance icon corresponds to the meaning of the colors for the SINEMA Server monitor icon.
- In the top left corner of the object, you can see the most negative overall status of one of the devices monitored by the relevant SINEMA Server instance.

In active mode, only the user-defined connections are shown. The following points apply to the display of user-defined connections:

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

## See also

Configure connections (Page 69)

Status display (Page 27)

## 4.1.13 Event list

### Event list

The event list shows all the events 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.

Noted	Event status	Event	Event class	Time stamp	Event details	IP address - affected
<input type="checkbox"/>	No	Resolving	Device monitoring: PROFNET monitoring was started	2015-04-01 11:15:03.33	-	190.171.0.10
<input type="checkbox"/>	No	Pending	Wireless interface quality: critical high signal strength to the connected AP (overdrive)	2015-04-01 11:15:01.646	MAC address: 00:0c:5a:77:a0, value: -30	190.171.0.10
<input type="checkbox"/>	No	Resolving	Device monitoring: device can reach again with SNMP	2015-04-01 11:14:59.558	-	190.171.0.10
<input type="checkbox"/>	No	Resolving	Device property: change of IP address detected	2015-04-01 11:14:45.266	Old IP address: 190.171.0.102	190.171.0.10
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET IO name detected	2015-04-01 11:14:45.219	PHIO name: simatic-pc for IP address 190.171.0.4, 190.170.0.66, 190.171.0.4	190.171.0.4
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET IO name detected	2015-04-01 11:14:45.203	PHIO name: pi-a for IP address 190.171.0.70, 190.170.0.4, 150.190.171.0.70	190.171.0.70
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET IO name detected	2015-04-01 11:14:45.188	PHIO name: scalexion s box for IP address 190.171.0.42, 172.16.2	190.171.0.42
<input type="checkbox"/>	No	Resolving	Device status: not connected	2015-04-01 11:14:21.101	-	190.171.3.29
<input type="checkbox"/>	No	Resolving	Device status: not connected	2015-04-01 11:14:21.101	-	190.171.3.28
<input type="checkbox"/>	No	-	Device monitoring: Controller reporting that a device is in the status "Disabled"	2015-04-01 11:14:20.992	Name of the controller: cpu412-3-10	190.171.3.28
<input type="checkbox"/>	No	-	Device monitoring: One of the devices is in the status "Disabled"	2015-04-01 11:14:20.992	Name of the IO device: e200ap-device29	190.171.3.29
<input type="checkbox"/>	No	-	Device monitoring: One of the devices is in the status "Disabled"	2015-04-01 11:14:20.992	Name of the IO device: e200ap-device28	190.171.3.28
<input type="checkbox"/>	No	-	Device monitoring: Controller reporting that a device is in the status "Disabled"	2015-04-01 11:14:20.992	Name of the controller: cpu412-3-10	190.171.3.29
<input type="checkbox"/>	No	Pending	Device monitoring: PROFNET monitoring was stopped	2015-04-01 11:14:11.133	-	190.171.3.29
<input type="checkbox"/>	No	Pending	Device monitoring: PROFNET monitoring was stopped	2015-04-01 11:14:09.42	-	190.171.3.28
<input type="checkbox"/>	No	-	Device monitoring: One of the devices is in the status "Disabled"	2015-04-01 11:14:00.618	Name of the IO device: e200a-8	190.171.3.8
<input type="checkbox"/>	No	-	Device monitoring: Controller reporting that a device is in the status "Disabled"	2015-04-01 11:14:00.618	Name of the controller: e200a-cpu	190.171.3.8
<input type="checkbox"/>	No	Pending	LAN: interface inactive and does not match reference	2015-04-01 11:13:59.776	-	190.171.3.34
<input type="checkbox"/>	No	Resolved automatic	Device monitoring: device is no longer reachable with SNMP	2015-04-01 11:13:45.003	-	190.171.0.10
<input type="checkbox"/>	No	Resolved automatic	Device monitoring: PROFNET monitoring was stopped	2015-04-01 11:13:10.792	-	190.171.0.10
<input type="checkbox"/>	No	Resolving	Device monitoring: Controller reporting that a device is in the status "Active"	2015-04-01 11:13:02.664	Name of the controller: e200a-cpu	190.171.3.8
<input type="checkbox"/>	No	Resolving	Device monitoring: One of the devices is in the status "Active"	2015-04-01 11:13:02.664	Name of the IO device: e200a-8	190.171.3.8
<input type="checkbox"/>	No	Resolving	Device property: change of IP address detected	2015-04-01 11:12:24.725	Old IP address: 190.171.0.10	190.171.0.10
<input type="checkbox"/>	No	-	Discovery: scan for new devices completed	2015-04-01 11:12:24.693	-	19.176.26.31
<input type="checkbox"/>	No	Resolving	Device monitoring: device can reach again with DCP	2015-04-01 11:11:37.722	-	190.171.3.28
<input type="checkbox"/>	No	Resolving	Device monitoring: device can reach again with DCP	2015-04-01 11:11:37.707	-	190.171.3.29
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET IO name detected	2015-04-01 11:11:37.613	PHIO name: pi-a for IP address 190.171.0.70, 190.170.0.4, 150.190.171.0.70	190.171.0.70
<input type="checkbox"/>	No	Pending	Device property: duplicate PROFNET IO name detected	2015-04-01 11:11:37.613	PHIO name: simatic-pc for IP address 190.171.0.4, 190.170.0.66, 190.171.0.4	190.171.0.4

## 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"	<p>The selection box is used to select an event prior to editing a particular event.</p> <p>Multiple selections are possible.</p> <p>Note:</p> <p>By double-clicking on the selected event you open the device details ("Events" tab) of the device belonging to the event.</p>
Noted	<p>Display indicating whether the event was noted by the user with the "Events noted" function.</p> <ul style="list-style-type: none"> <li>• "Yes" = Noted</li> <li>• "No" = Not noted</li> </ul>
Event status	<p>Display of the status that the event has in terms of the overall status of a device.</p> <ul style="list-style-type: none"> <li>• Pending: When an event in an overall status group that is assigned a negative overall status (every overall status except "OK") is triggered for a device, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device.</li> <li>• Resolving: An event in an overall status group that is assigned the overall status "OK" is identified by the event status "Resolving" because when it occurs, the event clears all other events of the same overall status group from the list of events pending for the device.</li> <li>• Resolved automatically: An event in an overall status group that was in the list of pending events for a device and was then removed from the list of pending events by a resolving event of the same overall status group is identified by the event status "Resolved automatically".</li> <li>• Resolved manually: An event in an overall status group that was in the list of pending events for a device and was then removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually".</li> <li>• Not present: A triggered event that is not assigned to any overall status group has no event status.</li> </ul>
Event	Configured event information or event message.
Event class	<p>Information on the class (weighting) of the event. The entries are color-coded with the following meaning:</p> <ul style="list-style-type: none"> <li>• light green = notification</li> <li>• dark green = information</li> <li>• yellow = warning</li> <li>• red = error</li> </ul>
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 (affected)	Shows the IP address of the device that triggered the event.





Column	Meaning
IP address (reporting)	Shows the IP address of the device that reported the information to trigger the event to SINEMA Server.
Remarks	Store additional information, for example, about event reactions. Note: If several events are selected, an edited comment is entered for all the selected events.
Trigger	Name of the source device.
Time stamp (reported)	Time at which the SIMATIC event / alarm message was sent by the CPU with SIMATIC capability.
Event category	Specifies whether a network event or a system event is involved.
Device status	Overall status that potentially causes the event on a device.
Overall status group	Name of the overall status group to which the event is assigned.
Affected (name)	Shows the PROFINET name of the device that triggered the event.
Affected (name)	Shows the PROFINET name of the device that reported the information to trigger the event to SINEMA Server.
Protocol	Information about which protocol supplied the event information.
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.

**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
	Noted events By marking events as "Noted", you confirm your awareness of the changed status of an active entry in the event list. No other reaction is associated with this function. Configured event reactions are triggered solely by the status change of the event.
	Removes a selected pending event from the list of events pending for a device. The event then has the event status "Manually resolved".
	Edit remark Note: If several events are selected, an edited comment is entered for all the selected events.
	Delete remark

## 4.1 Program user interface in detail - overview of the menus

Icon	Meaning
	<p>Maximize / minimize</p> <p>As default, SINEMA Server shows up to 10 events in the event list. By maximizing the display, you expand the display of the event list to the size of the full Web page. Using the functions in the footer, you also have the option of paging through the entire event list and configuring the layout of the event list.</p>
	<p>Enter text to filter based on events. The entered text is searched for in all columns</p> <p>In the input box, text is displayed when a simple query entered in the filter template editor is active.</p> <p>The  icon is displayed when a filter template with prefilter settings is active.</p> <p>The  icon is displayed when a filter template with a complex query is active.</p>
	<p>Selection of a previously created template for filtering according to events. After selection, the properties of the filter template are applied to the event list. Unsaved filter settings are indicated by the "*" character.</p> <p>As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.</p>
	<p>Open the editor for configuring filter settings that can be stored in filter templates.</p> <p>The  icon is displayed when the configured filter settings differ from the default filter settings.</p> <p>For more information, refer to the section "Prefilters in filter templates for event lists".</p>
	<p>Not connected / connected to topology</p> <p>If a topology representation is displayed in the content area, you have the option of connecting the event list with this topology representation. In the connected status, devices for which events of the event list were triggered are highlighted optically in the selected topology representation. The devices whose events are highlighted can be specified in the "Highlight only selected entries" check box:</p> <ul style="list-style-type: none"> <li>• Check box is enabled: Only the devices of the events selected in the event list are optically highlighted.</li> <li>• Check box is disabled: All devices of the current event list are optically highlighted. Using the filter settings of the event list, the number of highlighted devices can be adapted.</li> </ul> <p>The highlighted devices are listed in the "Device hierarchy" area.</p> <p>If the automatic updating is disabled, you can call up the highlighted devices one after the other with the shortcut menu in the topology display. The order in which they are called is based on the listing of the highlighted devices in the "Device hierarchy" area.</p>



## Prefilters in the filter templates for event lists

Event lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for event lists. You will find basic information on filter templates and the options of using complex filters in the section:

Filtering data with filter templates (Page 80)

Box group	Filter options
Basic filter settings	<p>Noted:</p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• All</li> </ul> <p>Event state:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• " - ": Events to which no event status is assigned</li> <li>• Resolving: Events that when they occur remove all other events of the same overall status group from the list of events pending for a device</li> <li>• Resolved automatically: Events that were removed from the list of events pending for a device by resolving events</li> <li>• Resolved manually: Events that were removed manually from the list of events pending for a device</li> <li>• Pending: Events pending for the devices</li> </ul> <p>Period:</p> <p>Filter according to events records of the last 7 days / 24 hours / all events as of the current time / period entered manually.</p>
Event categories	<p>Filter according to the origin of events:</p> <ul style="list-style-type: none"> <li>• Network events</li> <li>• System events</li> </ul>
Event classes	<p>Filter according to the severity of events:</p> <ul style="list-style-type: none"> <li>• Notification</li> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul>
Protocols	<p>Filter according to protocols by which the events were triggered:</p> <ul style="list-style-type: none"> <li>• ICMP</li> <li>• DCP</li> <li>• ARP</li> <li>• SNMP</li> <li>• SNMP trap</li> <li>• PROFINET</li> <li>• SIMATIC</li> <li>• Multiple (event was triggered by more than one protocol)</li> <li>• SIMATIC event messages</li> <li>• SIMATIC alarm messages</li> </ul>

## **Functions of the shortcut menu**

The shortcut menu provides the option of calling up the discovered topology, the monitored topology, the reference topology or a view-specific topology from the event list. In the selected topology representation, the device is selected and shown centered that triggered the event selected in the event list. This function is not available for traps that SINEMA Server has received from unknown devices.

In addition to this, you can call the overall status group to which the selected event belongs using the shortcut menu.

## **See also**

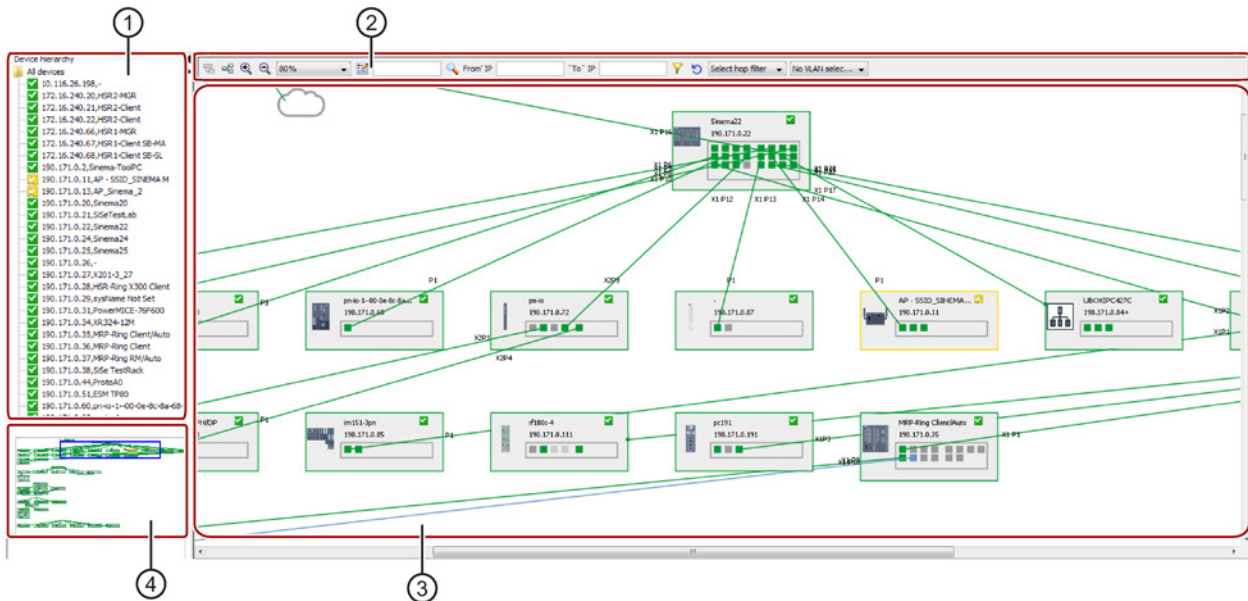
Administration - Events > Event reactions (Page 198)

## 4.2 Topology

### 4.2.1 Topology - Discovered

#### 4.2.1.1 Meaning and how it works

You can open the "Discovered topology" Web page with the functions described below with the menu command: **"Topology > Discovered"**



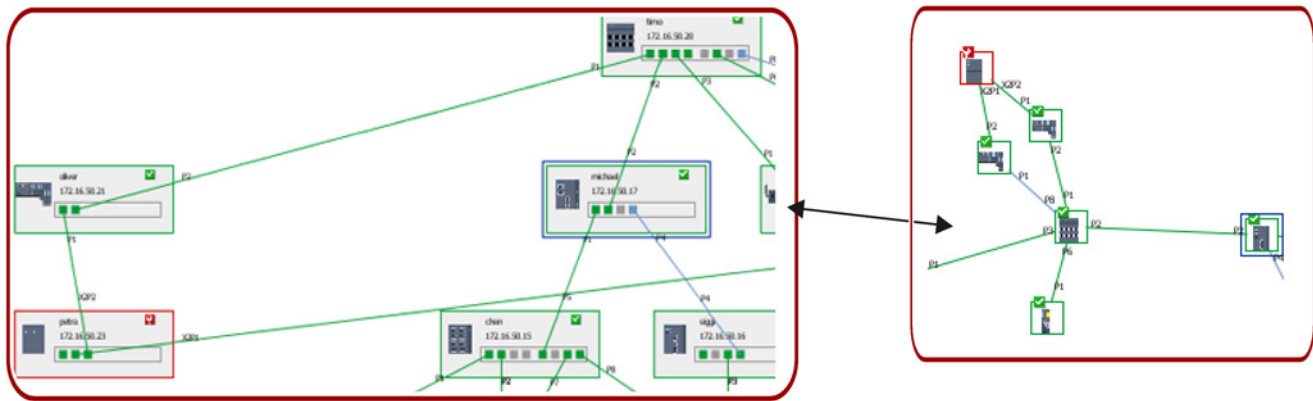
- ① Device hierarchy
- ② Toolbar
- ③ Device hierarchy in the topology display
- ④ Overall view (bird's eye view) with sliding detail selector

### Layout

The menu command "Topology > Detected" shows the network - devices and topology - in the way SINEMA Server 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.

The following figures illustrate the basic differences between the detail view (① left) and icon view (② right):

4.2 Topology



Detail view ①

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.

Icon view ②

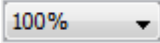







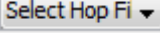
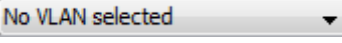
In the icon view, the devices are displayed as icons without ports. The start and end port numbers are shown on the connection line. This view shows the network structure such as ring, star and linear bus topology with the devices in the form of icons.

The devices and their connections in the current network are shown with their current status and the monitoring status.

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
	Enlarge display (zoom factor)		Reduce display (zoom factor)

Icon	Display / function	Icon	Display / function
	Select zoom factor		<p>Topology settings</p> <p>Select the from the following options in the displayed dialog:</p> <ul style="list-style-type: none"> <li>• Basic settings <ul style="list-style-type: none"> <li>– Show port names for connections</li> </ul> </li> <li>• Device labeling <ul style="list-style-type: none"> <li>– Name</li> <li>– IP address</li> <li>– Vendor</li> <li>– Category</li> <li>– Device remarks</li> <li>– PROFINET device name</li> <li>– System name</li> <li>– Name of the automation plant</li> <li>– Device type</li> <li>– MAC address</li> </ul> </li> </ul> <p>From the device names, up to 2 entries can be selected.</p>
	<p>Input box for device search</p> <p>Specify an IP address for the node scan. The found node is highlighted with a dotted frame.</p>		Start node scan
From IP 	"From" text box for IP filter	To IP 	"To" text box for IP filter
	Activate IP filter		Reset IP filter
Select Hop Fi 	<p>Select HOP filter</p> <p>Select the number of hops to be shown in the topology starting from a network node.</p> <p>If no particular node is selected you will be prompted to select a node after selecting the filter setting.</p>	No VLAN selected 	<p>Select VLAN filter</p> <p>If one or more VLANs are configured in your network structure, you can select one of these VLANs from the drop-down list. The corresponding devices and ports are then highlighted in the topology.</p>

## 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
  - Devices and their connections in the selected IP address range are displayed unchanged.
  - Devices not included in the IP address range are grayed out.
  - Connections between devices not included in the IP address range are grayed out.

## Other operator options - detail view and icon view





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
- 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

#### Interfaces

The status of the device or the color of a connection line has no effect on the interface color. The following table shows the interface colors and their significance:

Interface color	Description
	Active
	Down (with current connection)
	Down (without current connection)
	Unknown (not reachable)

#### Connection lines





##### Connection colors

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. Which of the port colors decides the color of the connection line depends on the priority of the port color:

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

##### Connection types

Wireless links, optical connections, electrical connections and unknown connections are shown in the detail view of the discovered topology and the monitored topology as follows:


Connection type	Description
	Wireless connection
	Optical connection
	Electrical connection
	Unknown connection

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

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

4.2 Topology

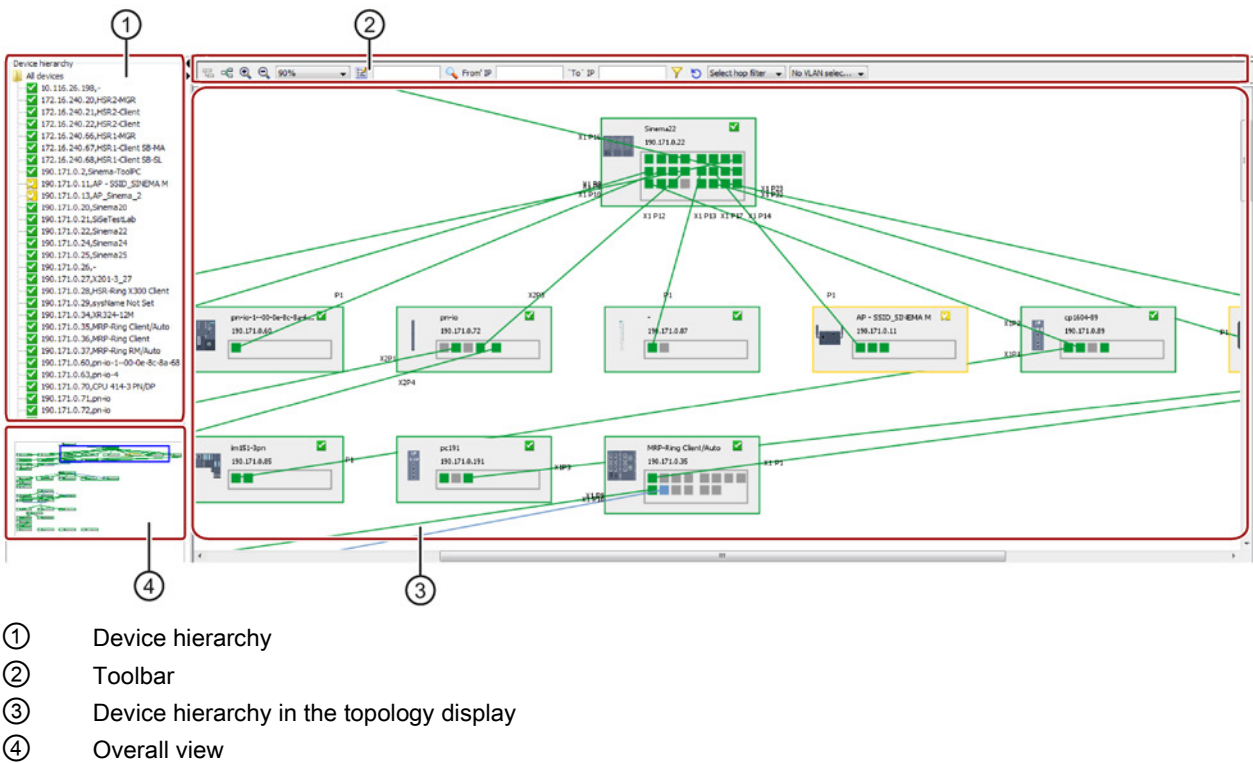
Devices not inserted in the reference topology

Discovered devices that cannot be inserted in the reference topology are indicated by the  icon.

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

**The reference topology is a prerequisite**

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



The display options are the same as those of the "Discovered topology" with detail view and icon view.

## Operator input

Operator options and functionality correspond to those of the "Discovered topology" Web page with detail view and icon view.

---

### Note

#### Differences compared with the "Discovered topology" Web page

- In the "Monitored topology" Web page, the pane 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.
  - The toolbar contains the same icons as in the discovered topology.
- 

## Content - relationship with the reference topology

The detail view of the "Monitored topology" Web page shows both the monitored devices as well as the unmanaged devices inserted extra in the reference topology, if these exist.

The following procedure is used:

- Colors  
The color of the displayed 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.
- First display  
To display the monitored topology and its status, you need to save the reference topology at least once in the Reference editor.
- Changes in the network  
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.

### 4.2.2.2 Icons and colors in the monitored topology

#### Status monitoring











- **Port / interface status:**

In the detail view of the monitored topology, two statuses are displayed for each port: the detected status and the status that results from comparing the detected port status and the reference port status.











- The detected 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.

## 4.2 Topology

The following table shows the edge and fill colors of ports depending on their detected statuses and their reference statuses:

Detected port status	Reference port status	Resulting port status		Border color / fill color
Active	Active	Active		
Active	Inactive	Active - Maintenance required		
Active	Unmonitored / Docking port	Unmonitored / docking port		
Inactive	Active	Inactive - Maintenance urgently required	With current connection	
			Without current connection	
Inactive	-	-	With current connection	
			Without current connection	
Inactive	Unmonitored / docking port	Unmonitored / docking port	With current connection	
			Without current connection	
Unknown	-	-		

- **Statuses of ring ports:**

Redundancy status (device details)	Standby port status		Fill color/border color
Up	Active		
Up	Active - Maintenance required		
Up	Inactive - Maintenance urgently required		
		With current connection	
		Without current connection	
Up	Inactive		
		With current connection	
		Without current connection	
Up	Unknown		
Passive	Active		
Passive	Active - Maintenance required		
Passive	Inactive - Maintenance urgently required		
		With current connection	
		Without current connection	
Passive	Inactive		
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 connection color is based on the fill color of the two connected ports. If, however, the reference connection between the ports does not correspond to the detected connection, the connection color is red regardless of the fill colors of the ports. In terms of the connection color unmonitored ports / docking ports behave like inactive ports; in other words, the connection color is defined by the status of the partner port.

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

Fill color port 1	Fill color port 2	Connection color
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. Which of the port colors decides the color of the active connection between client and AP depends on the priority of the port color:

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

### Devices not inserted in the reference topology

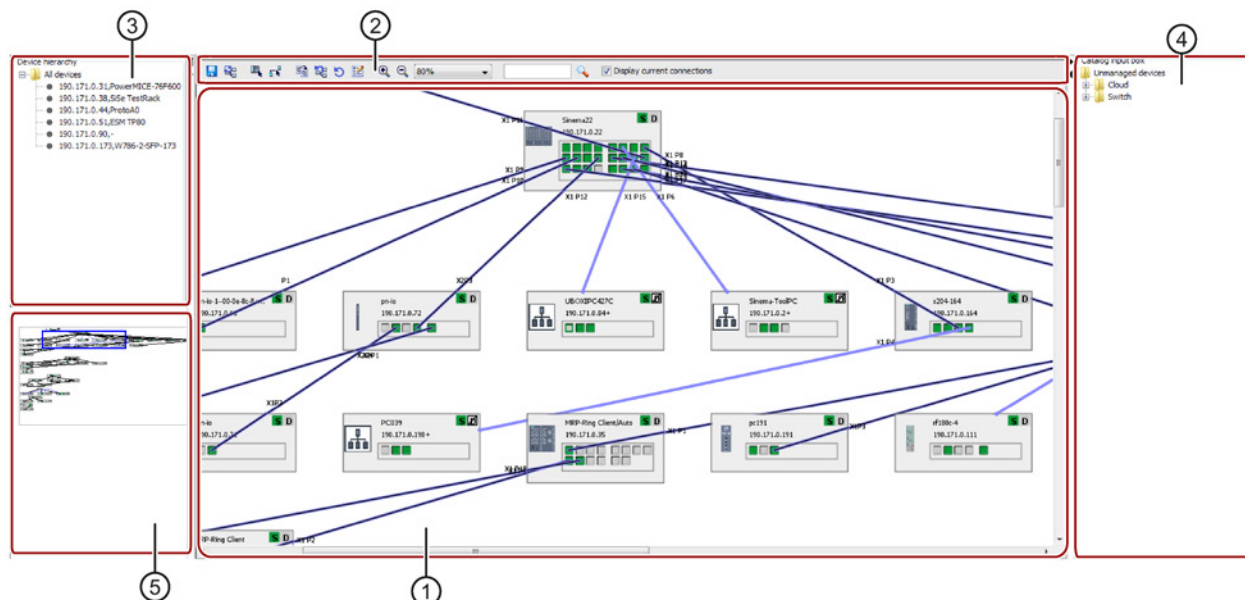
If devices were discovered that cannot be inserted in the reference topology, this is indicated in the monitor topology with the  icon in the top left corner.

## 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 areas in which the complete information on the topology of the devices discovered in the network is displayed.



- ① Reference editor
- 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"**. With this tool, you configure the reference topology; in other words the target status of the network.

### Note

SINEMA Server requires the reference topology for numerous functions. If you want to use the full functionality of SINEMA Server, you will need to configure a reference topology in advance.

## Reference editor

The Reference editor is used to specify 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
- Adding new devices in the editor
- Drawing reference connections

## Display in the Reference editor





In the Reference editor, the reference topology with reference connections and the connections between the devices discovered in the network are displayed. The device name and the device IP address of individual devices as well as the port statuses of the current topology and the reference topology are shown in the text display box. 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 suitable protocol support available for the specific device.







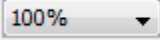


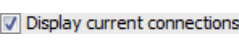
An unknown device is displayed as a cloud in the Reference editor.

The connection lines in the have port numbers at both ends of the connection. This is identical for the connections in the monitored topology and in the reference topology.

## 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 In the selection mode, functions for arranging the devices and for making settings for status information are available.		Select draw mode In the draw mode, functions are available for drawing and defining reference connections.

Icon	Display / function	Icon	Display / function
	Use current connections as reference With this function, current connections, current protocol-specific availability of devices and current port statuses are applied as 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 topology settings
	Enlarge display (zoom factor)		Reduce display (zoom factor)
	Select zoom factor		Input box for node scan
	Start node scan		Display current connections If the check box is enabled, current connections, current port statuses and current protocol-specific availability of devices are displayed.

### Working with the shortcut menus - overview

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
- Right-click on device icon  
Open the shortcut menu with the following options:
  - Remove device
  - Add comment
  - Show device details
  - Open WBM

## 4.2 Topology

- Right-click on an unconnected interface icon

Open the shortcut menu with the option of specifying the following statuses for the interface:

- Up
- Down
- Unmonitored
- Docking port

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

- 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": The definition as a reference connection is canceled / drawn connection is deleted
- Use connection as reference

- Position the mouse pointer on device icon

The following information is 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  
Specify the following statuses for the interface:
  - Up
  - Down
  - Unmonitored
  - Docking port
- 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.

**Display of connections**

The following display statuses for connections are distinguished in the Reference editor:

- Light blue line  
Connection currently discovered in the network that has not yet been defined as a reference connection.
- Black line
  - Connection currently detected in the network that has been defined as a reference connection. ("Display current connections" option is **disabled**)
  - Manually drawn connection. These connections are automatically defined as reference connections.
- black line with blue edges  
Connection currently detected in the network that has been defined as a reference connection. ("Display current connections" option is **enabled**)

### 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
- Reset reference topology
- Recalculate topology

#### Using the selection mode and drawing mode

The selection mode or the drawing mode can be selected using the corresponding icons.

- **Selection mode**

The selection mode is enabled as default when the Reference editor is called. In the selection 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 (active / inactive / unmonitored / docking port)
- Change the status of the protocol-specific device availability for the SNMP and DCP protocols
- Canceling the definition of reference connections / deleting drawn connections
- Delete unmanaged devices
- Remove managed devices and move the device to the catalog of new devices

- **Drawing mode**

In the drawing mode, you can perform the following editing steps:

- Draw a connection between ports of different devices  
In the drawing mode, you draw a connection line between two devices by clicking on the ports of the devices you want to connect.
- Specify a current connection as a reference connection (shortcut menu)
- Canceling the definition of reference connections / deleting drawn connections (shortcut menu)

#### How it works and 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 currently discovered topology will be used for the display in the "Reference topology" Web page.

The network devices are initially arranged based on the current connections in Hop layers. The Reference editor view contains several hop layers.

- For devices with current connections, the hop 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. Once the reference topology has been configured or saved, the hop layers are then based on the connections of the reference topology.

### Reset reference topology

The "Reset reference topology" button deletes the reference topology.

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

- Definitions for reference connections are canceled.
- 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 reference editor waits for the next status of the port.
- The status of the protocol-specific device availability is deleted.

### Recalculate topology

The "Recalculate topology" function results in one of the following displays in the Reference editor depending on the view:

- Icon view: The devices are displayed in the existing topology (e.g. ring topology, star topology).
- Detail view: The devices are sorted according to their hop layers.

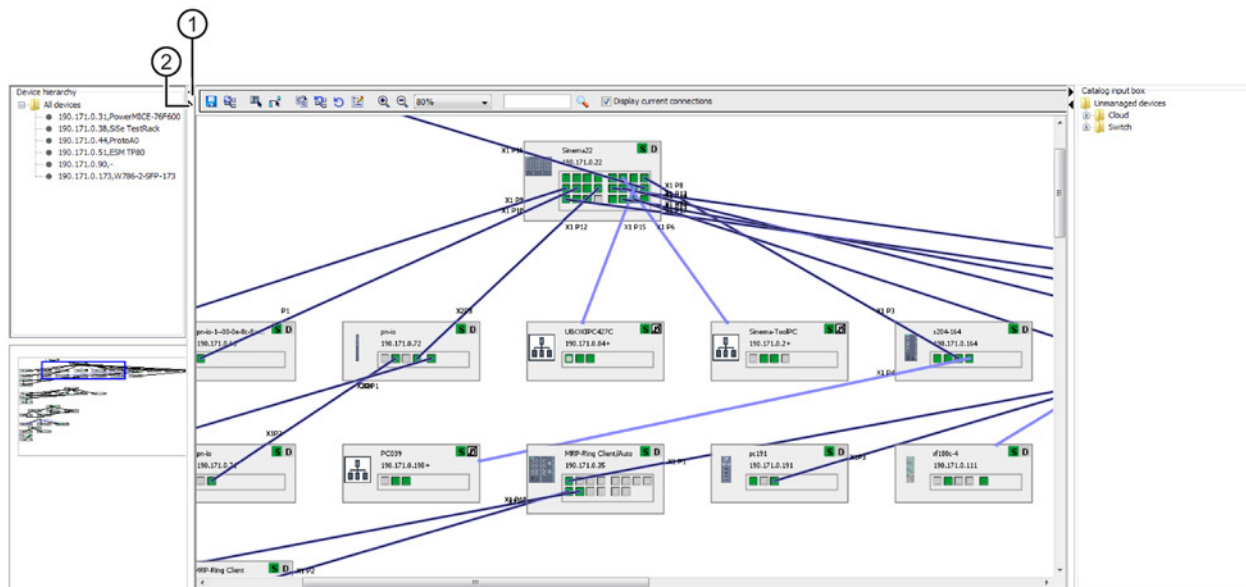
The recalculation of the topology should be performed when the discovered topology was called before the entire topology was discovered since this can lead to crossed-over connections.

## 4.2 Topology

## 4.2.3.3 Reference editor / including devices

## Device hierarchy

The Reference editor includes the sub window "Device hierarchy" that displays all devices that are not in the reference topology. This sub window is on the left-hand side in the Reference editor.



- ① Hide the device hierarchy
- ② Show the device hierarchy

New devices can be inserted in the reference topology by dragging them with the mouse. 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.

After a new device has been added to the reference topology, this device is no longer available in the new devices folder. This device is visible in the monitored topology after saving the reference topology.

If a device was deleted from the reference topology, it is displayed again in the sub window of the device hierarchy.

## Adding new devices

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

1. In the toolbar of the Reference editor, click the "Select" icon.
2. Select the required device in the "Device hierarchy" folder and drag it to the reference view. To add several devices at the same time, hold down the shift key when selecting and placing the devices.

Alternatives:

- As an alternative, you can click on the new device or use the options in the shortcut menu.

Once the new device has been inserted in the reference view, it disappears from the "Device hierarchy" list.

3. After adding reference connections to the new devices, click the "Save" button to save the new devices.

## Adding unmanaged devices to the topology view

In the selection mode, the SINEMA Server application provides the option of adding unmanaged devices to the reference topology. This makes it possible to configure a complete topology view. The unmanaged devices cannot, however, be monitored in the network.

The Catalog box contains the list of categories for predefined device types. Each category consists of several predefined network devices.

The unmanaged devices can be added to the reference topology by dragging them to it. Each unmanaged device is given a unique name as soon as it is added to the reference view.

Connections between unmanaged devices and managed devices can be created either manually or with the options in the shortcut menu. Refer to the information on connections in the next section.

---

### Note

#### Displaying the catalog

When the reference topology is displayed, the Catalog input box is hidden as default. To display the Catalog input box, 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 their ports manually
- Specifying a current connection as a reference connection by double-clicking.

## 4.2 Topology

The following option can only be configured in selection mode:

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

### Drawing connections between devices manually

To draw a reference connection between the ports of devices, you can use the following alternative methods:

1. Click on the port of a device.
2. Click on the required port of the target device.

A black connection line is then drawn between these two devices. Implicitly, a connection created in this way has the status of a reference connection.

As an alternative:

1. In drawing mode, click on 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.

2. Select the ports for both devices from the drop-down lists.
3. Confirm the dialog.

A black connection line is then drawn between these two devices. Implicitly, a connection created in this way has the status of a reference connection.

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

### Specify a current connection as a reference connection

Currently detected connections in the network are initially displayed highlighted light blue in the topology view.

To define a currently detected connection as a reference connection you can use one of the following two methods:

- By double-clicking in the drawing mode

In the drawing mode, double-click on the connection line representing a current connection. A thin black line then appears above the blue line of the connection indicating a reference connection.

- Using the shortcut menu in the selection mode

Right click on the connection line in selection mode 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

It is possible to define all currently detected connections as reference connections.

Follow the steps below:

Then change to the Selection mode

Click on the "Use current connections as reference" icon and confirm the displayed dialog.

The line colors of the connections then change to black indicating a reference connection.

### Creating connections - combinations of different media types

The creation of connections between different media types is always permitted in the topology view.

The precise media type, however, needs to be identified and when drawing a connection, the correct combination type must 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 following table shows the various combinations of media types and their relevance for a message display.

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

Unmanaged devices are not automatically displayed in the reference topology. If there is an unmanaged device between two monitored 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 only two devices are connected to the unmanaged device.

#### 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 port in the reference topology (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. The port status knows the following modes:

- Up
- Down
- Unmonitored
- Docking port

You will find information on the significance of these ports statuses in the section Editor for detailed information on (W)LAN ports (Page 117)

It is not possible to change the reference status of ports if they have a reference connection. The status of a port in the reference topology can be configured in selection mode in one of the following ways:

- **Switching over the port status manually by double-clicking**

Double-click on the port of a specific device to switch over between the status "Up" and "Down".

- **Changing the port status using the shortcut menu**

Right-click on the port. A shortcut menu with the port modes listed above is displayed:

- **Adopting the detected port status as the reference status**

With the "Use current connections as reference" function, the detected port statuses are also defined as reference statuses.

##### 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 is 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:

- **Switching over 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.

---

- **Adopting protocol-specific device availability from the current status**

With the "Use current connections as reference" function, the protocol-specific availability statuses of the devices are defined as reference statuses.

## 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 three 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 "ActualCloud \*XXX" in the discovered topology and the name "ReferenceCloud \*XXX" in the reference topology (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 (ReferenceCloud \*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 (ReferenceCloud\*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.

---

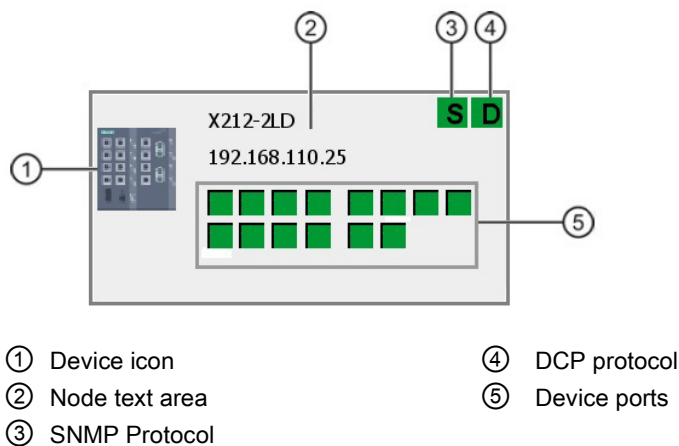
## 4.2.3.6 Icons and colors in the reference topology

### Overview

The following sections explain the significance of the colors for devices, ports and connection lines in the "Reference topology" Web page.

### 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 selected reference status.

---










## Port status

The detected and configured port statuses are displayed in the reference topology. These are shown as follows:

Detected port status	Display current connections	Setting in the reference topology			
		Up	Down	Unmonitored	Docking port
Active	Enabled				
Active	Disabled				
Inactive	Enabled				
Inactive	Disabled				
Unknown	Enabled				
Unknown	Disabled				

## Status of protocol-specific device availability

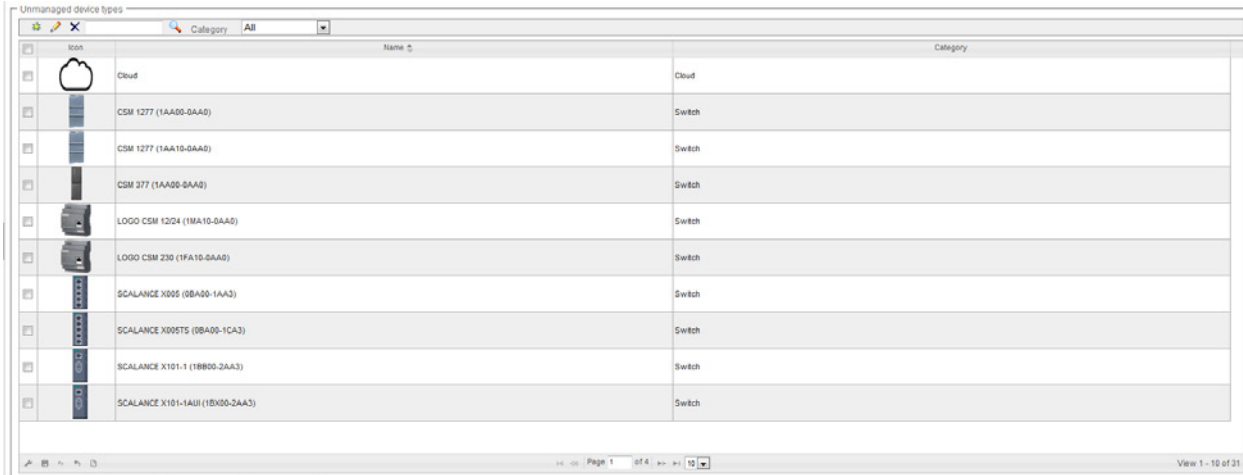
The detected and configured protocol statuses are displayed in the reference topology. The display of the SNMP protocol statuses uses the same scheme as the display of TCP protocol statuses. The SNMP protocol statuses are shown as follows:

Detected protocol status	Display current connections	Setting in the reference topology	
		Reachable	Not reachable
Reachable	Enabled		
Reachable	Disabled		
Not reachable	Enabled		
Not reachable	Disabled		
Protocol is not supported	Enabled		
	Disabled		

## 4.2 Topology

## 4.2.4 Topology - Unmanaged device types

You open the Web page shown below using the menu command: **"Topology > Unmanaged devices"**



## Layout

The **"Topology > Unmanaged devices"** 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
	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.

## 4.2.5 Topology - special features

### Partial connections

A partial connection is a connection in which the connection port of at least one device is unknown. The following types of partial connections must be distinguished:

- Type A: Port-to-device connection
- Type B: Device-to-device connection

In the topology displays, the connection lines end at the frames of device symbols if the connection port is unknown for the corresponding devices.

### Display of partial connections in the discovered topology

Type A: The color of the connection line depends on the color of the port from which connection information is available.

Type B: The color of the connection is always gray.

### Display and handling of partial connections in the reference topology

Partial connections are displayed in the reference topology based on the same scheme as in the discovered topology.

Partial connections cannot be included in the reference. Instead, partial connections can be expanded by drawing connections to connection ports that were not discovered. Connections created in this way then serve as reference for the monitored topology.

### Display of partial connections in the monitored topology

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

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

### Link aggregations

With a link aggregation, several parallel physical connections with the same transmission speed are grouped together to form a logical connection with a higher transmission speed. This method based on IEEE 802.3ad is also known as port trunking or channel bundling.

### Display of link aggregations in the discovered topology

In the discovered topology, all the connections of a link aggregation are represented by one connection line.

### Display and handling of link aggregations in the reference topology

Link aggregations are displayed in the reference topology based on the same scheme as in the discovered topology and can be expanded by connections that are not displayed.

### Display of link aggregations in the monitored topology

SINEMA Server checks the connections drawn in the reference topology to establish whether they belong to the link aggregation. If they do belong and if the ports involved with the connections are active, the connections are displayed in gray. If the ports involved are inactive, the general rules of the monitored topology for deciding the color of connection lines apply.

## 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 statistical data in tables or graphic diagrams. You can create a preview of a report and print it out.

The pages with the generated reports contain information in various boxes displayed in the table view. Optionally, this information is also shown as a pie chart or bar chart. Depending on the filter criteria the appropriate boxes are displayed with report information.

### 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
	Enter text to filter based on data records. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The  icon is displayed when a filter template with prefilter settings is active. The  icon is displayed when a filter template with a complex query is active.		Selection of a previously created template for filtering according to data records. After selection, the properties of the filter template are applied to the report. Unsaved filter settings are indicated by the "*" character.  As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The  icon is displayed when the configured filter settings differ from the default filter settings. You will find further information in the sections on the individual report types.		

### Note

#### Validity of the filter settings

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

## Printing reports

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

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.

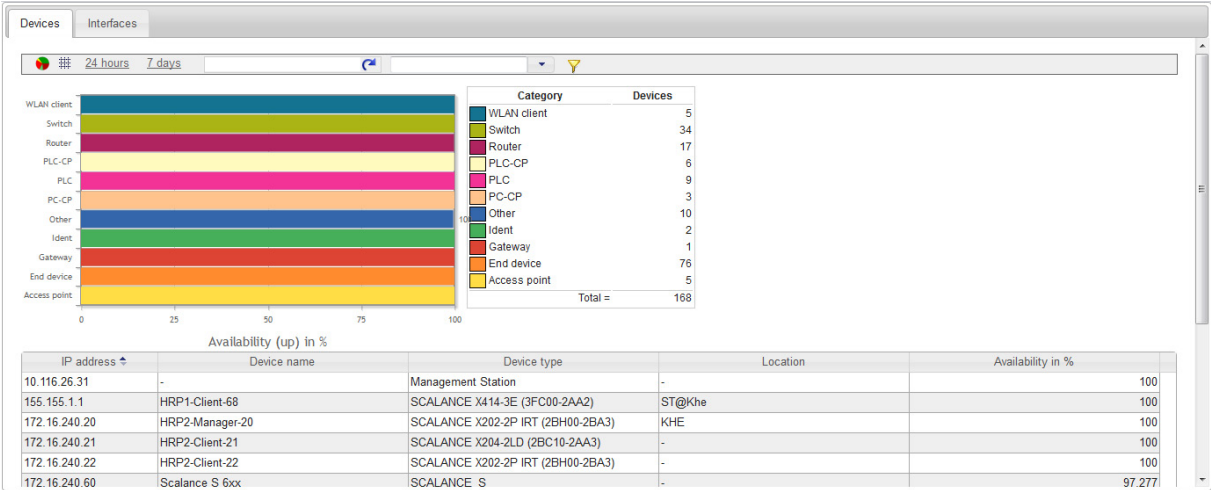
4.3 Reports

See also

Device details (Page 107)

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, unknown).

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



## Operation / content

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

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

## Calculations for the availability report

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



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 Reports

#### Prefilter for reports on availability

Reports on availability can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for availability reports.

Table 4- 21 Filters for availability reports in the "Devices" tab

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

Table 4- 22 Filters for availability reports in the "Interfaces" tab

Operator control element	Filter options
From IP To IP	Filter according to data records that have the specified IP addresses.
Device name, device type and device category	Filter according to data records for interfaces that belong to devices with the specified device name, the device type or the device category.
Statistics activated	Filter according data records for interfaces for which the port statistics are activated /deactivated: <ul style="list-style-type: none"> <li>• All</li> <li>• Yes: Interfaces with activated port statistics</li> <li>• No: Interfaces with deactivated port statistics</li> </ul>
Device	Filtering according interfaces belonging to existing or deleted devices.
Port status	Filter according to interfaces with an active connection status: <ul style="list-style-type: none"> <li>• All</li> <li>• Only interfaces with an active connection status</li> </ul>
Period	Filter according to data records of the last 7 days / 24 hours / period entered manually.

#### See also

Filtering data with filter templates (Page 80)

#### 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 maximum possible speed but also their total load when sending and receiving is displayed.
- LAN - Interface quality:  
The error quota when sending and receiving is displayed for all LAN interfaces.
- WLAN - Interface quality:  
The error quota when sending and receiving is displayed for all WLAN interfaces.
- WLAN - Interface data rate (transmission speed):  
For all WLAN interfaces, the bandwidth (data rate) when sending and receiving is displayed.
- WLAN - Signal strength:  
For all WLAN interfaces, the average signal strength is displayed.
- WLAN - Number of clients:  
For all access points, the number of WLAN clients to which they were connected on average is displayed.
- Discarded packets:  
The number of discarded incoming packets and the number of discarded outgoing packets is displayed for all LAN and WLAN interfaces.
- POF power budget:  
For LAN interfaces of the type "Plastic Optical Fiber (POF)", information about the power budget is displayed.

## Operation / content

Although the column assignment in the data area is preset, you 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       |
| • Average POF power budget             | • Maximum POF power budget              |

## 4.3 Reports

### Special feature

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

### Prefilter for reports on performance

Reports on performance can be filtered with the aid of filter templates. The meaning of the settings of the prefilter for reports on performance can be found in the section on the "Availability" report type.

### See also

Device details (Page 107)

Reports - Availability (Page 160)

Filtering data with filter templates (Page 80)

## 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", "Device category" and "PROFINET" 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
- Number of interfaces (used / total)
- PROFINET device name
- MAC address
- Firmware version

- Article number
- Historical data

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

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

### Prefilter for reports on the inventory

Reports on the inventory can be filtered with the aid of filter templates. In the prefilter of reports on the inventory, you can filter according to monitored or unmonitored devices.

### See also

Filtering data with filter templates (Page 80)

Reports - Availability (Page 160)

## 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.

**Prefilter for reports on events**

Reports on events can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for availability reports.

Table 4- 23 Filtering reports on events

Operator control element	Filter options
Basic filter settings	<p>Noted:</p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• All</li> </ul> <p>Event state:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• " - ": Events to which no event status is assigned</li> <li>• Resolving: Events that when they occur remove all other events of the same overall status group from the list of events pending for a device</li> <li>• Resolved automatically: Events that were removed from the list of events pending for a device by resolving events</li> <li>• Resolved manually: Events that were removed manually from the list of events pending for a device</li> <li>• Pending: Events pending for the devices</li> </ul> <p>Period: Filter according to data records of the last 7 days / 24 hours / all events as of the current time / period entered manually.</p> <p>From device: Filter according to deleted or existing devices</p>

Operator control element	Filter options
Event classes	Filter according to the severity of events: <ul style="list-style-type: none"> <li>• Notification</li> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul>
Protocols	Filter according to protocols by which the events were triggered: <ul style="list-style-type: none"> <li>• ICMP</li> <li>• DCP</li> <li>• ARP</li> <li>• SNMP</li> <li>• SNMP trap</li> <li>• PROFINET</li> <li>• SIMATIC</li> <li>• Multiple (event was triggered by more than one protocol)</li> <li>• SIMATIC event messages</li> <li>• SIMATIC alarm messages</li> </ul>

**See also**

Filtering data with filter templates (Page 80)

### 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". This column indicates the existence of 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"><li>• For devices:<ul style="list-style-type: none"><li>– IP address</li><li>– MAC address</li><li>– Device type</li><li>– Device category</li><li>– PROFINET device name</li><li>– Monitoring status</li></ul></li><li>• For interfaces:<ul style="list-style-type: none"><li>– Interface type</li><li>– Transmission rate</li><li>– Interface mode</li></ul></li></ul>
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



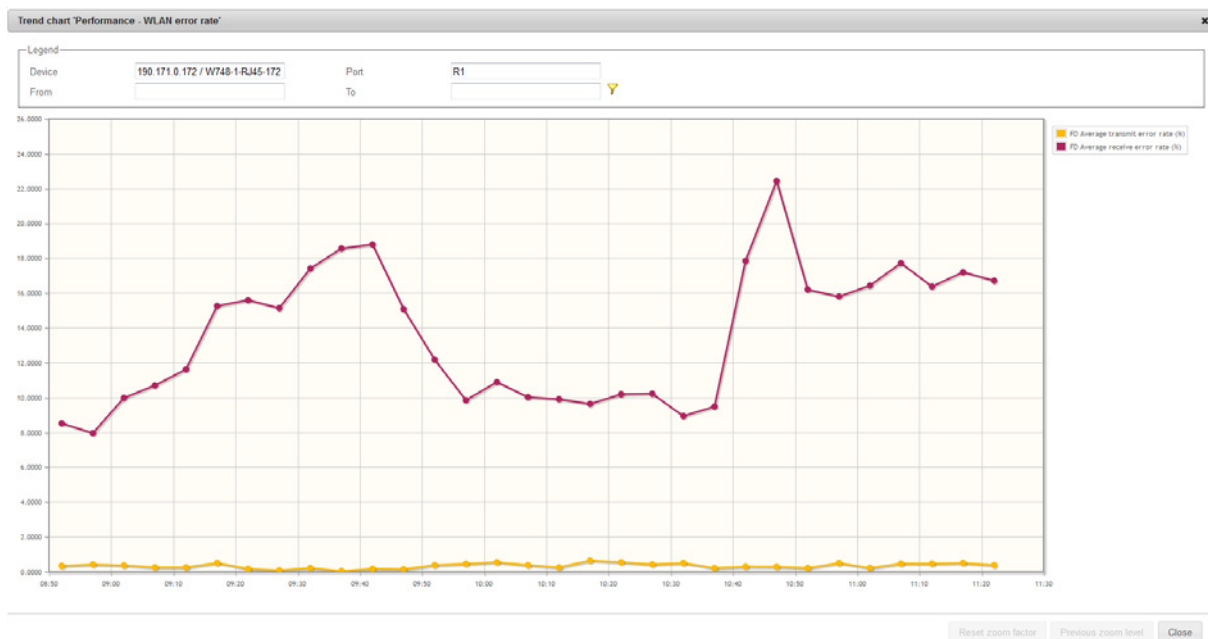
### 4.3.5.2 Trend charts

#### Meaning

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

#### Display and content

The following figure shows the example of a possible trend chart from the "WLAN interface error rate (%)" 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.

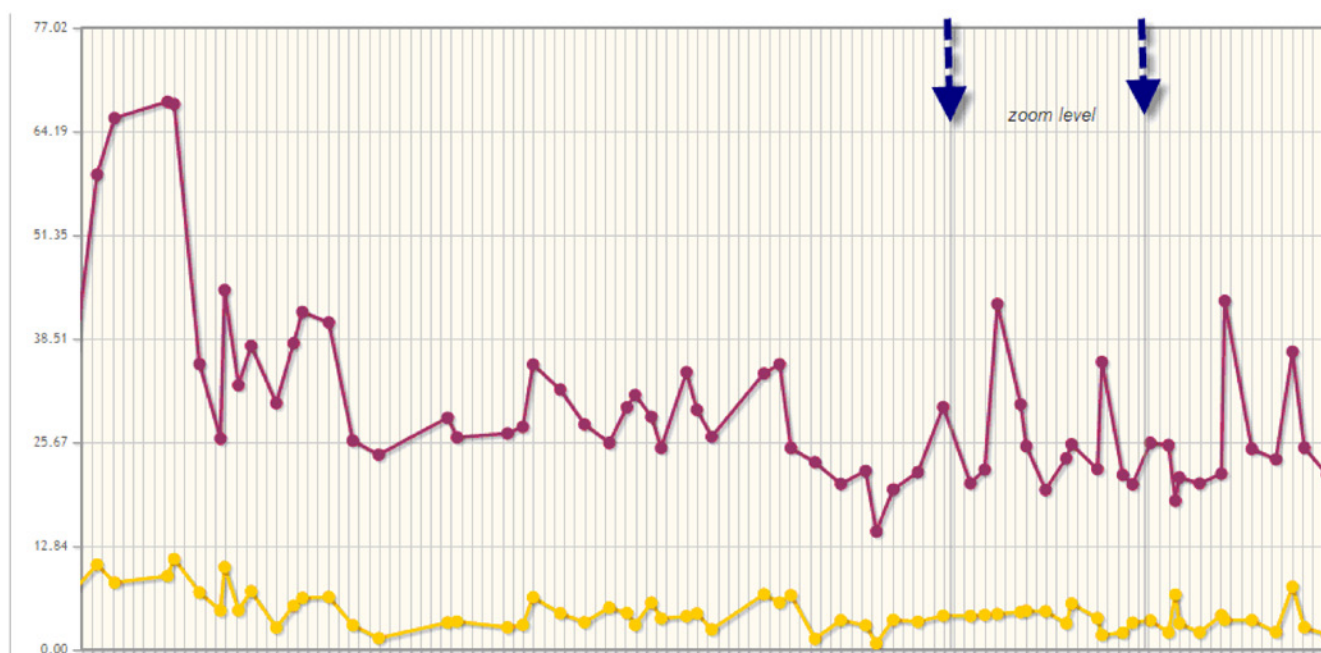
Report type	Tab	Trend data
Availability	Devices	Availability in %
	Interfaces	Active time in %
Performance	LAN - interface utilization	<ul style="list-style-type: none"> <li>• Average transmit utilization in %</li> <li>• Average receive utilization in %</li> <li>• Average utilization as %</li> </ul> For full duplex mode, the display has 3 trend lines.
	LAN interface error rate	<ul style="list-style-type: none"> <li>• Average transmit error rate in %</li> <li>• Average receive error rate in %</li> <li>• Average error rate in %</li> </ul> Display with 2 trend lines.
	WLAN interface error rate	<ul style="list-style-type: none"> <li>• Average transmit error rate in %</li> <li>• Average receive error rate in %</li> </ul>
	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 restrict the displayed period. This increases the resolution of the display and improves the clarity of the displayed times.

To use the zoom function, follow the steps below:

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



## 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
- Monitoring
- Events
- User
- System
- My settings

### 4.4.1 Administration - Discovery / Scan

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

Scan Profiles

IP address areas for network scan

Nodes to scan: 595

Status	First address	Last address	Name	No. of nodes
<input checked="" type="checkbox"/>	190.171.3.1	190.171.3.255	PNIO	255
<input checked="" type="checkbox"/>	190.171.0.1	190.171.0.255	Rack 1 und 2	255
<input checked="" type="checkbox"/>	190.172.0.60	190.172.0.70	Rack 1 PLC-CPs	11
<input checked="" type="checkbox"/>	172.16.240.10	172.16.240.80	HRP and Standby Rack	71
<input checked="" type="checkbox"/>	155.155.1.0	155.155.1.2	Router HRP-SB Rack	3

DCP network adapter for device scan

Status	IP address	Name
<input checked="" type="checkbox"/>	190.171.0.144	Intel(R) Gigabit CT Desktop Adapter #2
<input checked="" type="checkbox"/>	169.254.106.195	Intel(R) Gigabit CT Desktop Adapter
<input checked="" type="checkbox"/>	10.116.26.31	Intel(R) Ethernet Connection (2) I218-V

DCP discovery 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.

Miscellaneous

### 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
	Starting automatic device type change A search is made for more suitable device profiles and device types included in them for devices that were assigned a standard profile. If the check box "Use PROFINET discovery in network search" is enabled, more suitable device types are searched for using PROFINET tools for devices with PROFINET capability that were assigned a standard profile.

- **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 Note: A maximum of 40 IP address ranges can be created.
	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 DCP network scan (green status icon).



---

**Note**

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

---

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.

---

**Note****Effect of the option "Include all devices discovered with DCP 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.

---

- **"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 > My settings"** menu command.

The check box is deselected as default.

- Use PROFINET discovery in network search

For the device discovery and profile assignment the article numbers of the devices obtained via PROFINET are used. The devices are assigned to the device types contained in the profiles.

PROFINET discovery is useful when the PROFINET devices to be discovered are not reachable using SNMP or there are no suitable discovery rules in the required device profiles. If PROFINET and SNMP data is available for device discovery, the PROFINET data is given preference.

## 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. If the scan range covers more than 1000 addresses, a message will warn you to expect the scan to take a long time. You should therefore restrict the scan range to the devices to be monitored. To do this, it is advisable to create smaller scan groups if the IP addresses are not consecutive. This division speeds up scanning of the devices. A maximum of 40 scan groups can be created.

## See also

Detecting devices in the network (Page 47)

### 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.

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.

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"> <li>Requirement: A general profile must be selected.</li> <li>The Profile editor is opened with the "Add profile ID" dialog.</li> </ul>
	Create new monitoring profile <ul style="list-style-type: none"> <li>Requirement: A general profile or monitoring profile must be selected.</li> <li>The Profile editor is opened with the "Add profile ID" dialog.</li> </ul>
	Edit selected profile <ul style="list-style-type: none"> <li>The Profile editor is opened with the "Profile" dialog with the selected profile data.</li> </ul>
	Delete the selected profiles <ul style="list-style-type: none"> <li>Profiles are deleted following a further prompt for confirmation.</li> <li>Default profiles cannot be deleted.</li> </ul>
	Enable / disable selected profiles <ul style="list-style-type: none"> <li>Enabled profiles are used during discovery and scanning.</li> </ul>
	Save modified profiles <ul style="list-style-type: none"> <li>The profiles marked with "*" are stored in SINEMA Server.</li> </ul>
	Restore selected profiles <ul style="list-style-type: none"> <li>The function can be used with the profiles supplied with SINEMA Server following modification</li> </ul>
	Export profiles <ul style="list-style-type: none"> <li>The selected profile data is added to a ZIP archive. You are prompted to specify a storage location for downloading the ZIP archive.</li> </ul> <p>Note: If the data to be exported contains a profile whose limit value uses a user-defined overall status group, all profiles of the SINEMA Server instance must be exported.</p>
	Import profiles <p>The dialog box for selecting the profile file is displayed.</p> <ul style="list-style-type: none"> <li>File type: ZIP file</li> </ul> <p>Note: Profiles that exist in SINEMA Server and have the same profile identifier are overwritten by the imported profile.</p> <p>If the data to be imported contains a profile whose limit value uses a user-defined overall status group, all profiles must be imported into the SINEMA Server instance.</p>
	Enter text for text search / filter setting
	Start profile search <p>Result: The profiles that contain the specified text string in one of the displayed columns.</p>

### See also

Profile concept (Page 53)



### 4.4.2.1 The Profile editor

#### Displaying and editing profiles

With the Profile editor, you can perform one of the following actions:

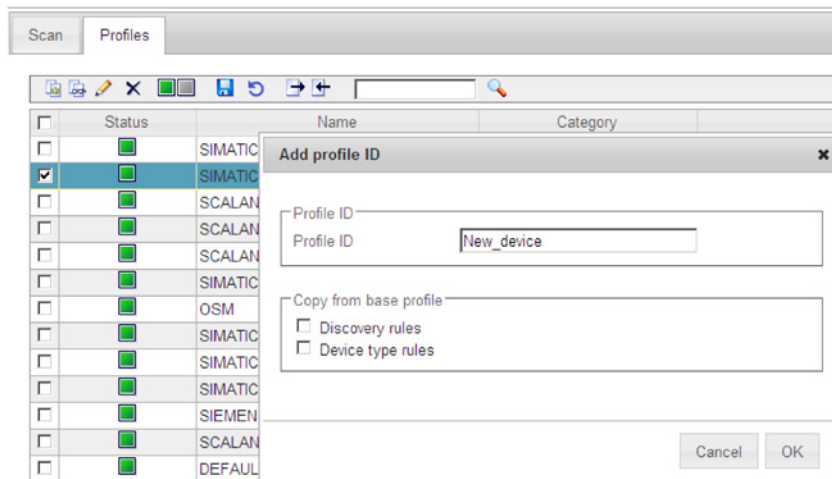
- Add a new device type to an existing profile
- Create a new profile
- Edit / modify an existing profile

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 55)

#### Create new profile

If, after selecting a profile as template, 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.

The screenshot shows the 'Profile' dialog box with the 'Basic data' tab selected. The fields are as follows:

- Name: [Redacted]
- Device category: Switch
- ID: SCALANCEX300
- Family: SIEMENS\_SCALANCE\_X200
- Description: Industrial Ethernet Switches SCALANCE XF200
- Vendor: Siemens AG
- Create on: 2014-03-13 23:07:0.00
- Updated on: 2014-03-13 23:07:0.00
- Default icon: SCALANCE\_XF200.png

On the right, a list of device descriptions is shown, with 'Industrial Ethernet Switches SCALANCE XF200' highlighted.

## 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.







The screenshot shows the 'Monitoring Profile' dialog box with the 'Basic data' tab selected. The fields are as follows:

- Name: [Redacted]
- Device category: Switch
- ID: SCALANCEX300
- Family: SIEMENS\_SCALANCE\_X200
- Description: Industrial Ethernet Switches SCALANCE XF200
- Vendor: Siemens AG
- Create on: 2014-03-13 23:07:0.00
- Updated on: 2014-03-13 23:07:0.00

The 'OID sets' and 'Thresholds' tabs are also visible at the top of the dialog.

## 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). Note: If a device is assigned a profile without a vendor ID, the DCP ID is used to identify the vendor.
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 assignment of devices to device profiles.

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"> <li>sysDescr = "**SIMATIC HMI*ThinClient*646**"</li> </ul>

**"Device types" tab (general profile)**

The tab is used to define a name and an icon and to specify rules for the device type 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	Specifying rules with protocol-specific criteria: <ul style="list-style-type: none"> <li>PROFINET: Specifying the article numbers. Several article numbers are separated by commas. The use of wildcards (*) is not allowed.</li> <li>SNMP/DCP: Specifies the SNMP value. The use of wildcards (*) is allowed.</li> </ul>
Icon name	File name of the icon used
Article numbers	Article 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 an extra dialog.

The entries are made in an additional dialog. Use the function elements described above to create a new data record. Per device profile, a maximum of 10 OIDs can be created in user-defined OID sets. These OIDs are then displayed in the device detail tab "User-defined OIDs" of the corresponding devices.

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 user-specific OID sets and OIDs from the system-defined OID set "Automation" can be modified. For OIDs from the OID set "Automation", an alternative OID can be specified or a fixed display value defined. In addition to this, rules can be specified for extracting partial values from the individual OIDs. Other OID sets that are read by SINEMA Server are displayed and cannot be modified.

**"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. You select the events to be linked to the thresholds from the overall status groups. Overall status groups are formed based on the functional relationship of their events and make it easier for you to locate the required event.

The operator used for the threshold check has a specific data type that is specified in the OID set. The thresholds must be specified accordingly.

Requirement: You can only define new data records for data values for user-specific OID sets.

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 threshold is linked to a system-specific OID set. The threshold and event can be edited.

### 4.4.3 Administration - Monitoring

#### 4.4.3.1 Administration - Monitoring

##### Overview

The functions described below are available with the menu command: **"Administration - Monitoring"**

The Web page contains the following tabs:

- General
- SNMP settings
- Polling groups
- OPC

#### 4.4.3.2 Administration - Monitoring General

##### Administration - Monitoring General

##### Time settings

- Scan interval  
The time interval for automatic network scans
- The DCP monitoring interval  
The DCP monitoring interval
- Interval for device type change  
At the specified interval, a search is made for more suitable device profiles and device types included in them for devices that were assigned standard profiles.
- Ping timeout  
Specifies the time after which a device is classified as being unreachable using ICMP

##### General settings

- Duplicate IP address detection  
If this check box is set, SINEMA Server checks whether or not the IP address exists more than once in the network.

---

##### Note

The discovery of duplicate IP addresses is only possible if you have also installed the "WinPcap" component.

---

- Automatic device type change  
If check box is set, a search is made for more suitable device profiles and the device

types in them for devices that were assigned standard profiles. The default interval for automatic device type change is 70 minutes and can be configured in the "Time settings" area. In addition to this, the automatic device type change is always performed when a device with an assigned standard profile changes from the "Not reachable" status to the "Reachable" status.

## PROFINET monitoring settings

PROFINET monitoring is only supported for devices with PROFINET IO capability. The PROFINET monitoring settings listed below only affect monitored devices.

- **PROFINET monitoring**  
If this check box is enabled, PROFINET monitoring of PROFINET devices is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name.
- **PROFINET monitoring of port statistics (can only be selected when the "PROFINET monitoring" check box is enabled)**  
If this check box is set, PROFINET monitoring of LAN port statistics for PROFINET devices is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name.  
In addition to this, the port statistics must be enabled in the device details for the required LAN port.
- **Use PROFINET monitoring settings for newly discovered PROFINET devices**  
If this check box is enabled, the configuration of the two options named above is used for newly discovered devices.
- **Duplicate PROFINET IO name detection**  
If this check box is set, SINEMA Server checks whether or not the PROFINET IO device name exists more than once in the network.

## SIMATIC monitoring settings

The SIMATIC monitoring is supported only for SIMATIC S7-300 / S7-400 / ET 200 CPUs. SIMATIC monitoring is not supported for S7-400/S7-400 H CPUs with the following firmware versions:

- S7-400 CPUs: Firmware V5.0.0 to V6.0.3
- S7-400 H CPUs: Firmware V5.0.0. to V6.0.4, V8.1.0

Devices for which SIMATIC monitoring is supported are known in this document as being "with SIMATIC capability". The following SIMATIC monitoring settings are available:

- **SIMATIC monitoring**  
If this check box is set, SIMATIC monitoring of CPUs with SIMATIC capability is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name.
- **SIMATIC monitoring of assigned devices (can only be selected when the "SIMATIC monitoring" check box is enabled)**  
When this check box is enabled, the SIMATIC monitoring of device data about assigned PROFINET IO devices and that is available on CPUs with SIMATIC capability is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name.

- SIMATIC monitoring including assigned devices and SIMATIC event messages (can only be selected when the "SIMATIC monitoring of assigned devices" check box is enabled)  
When this check box is enabled, SINEMA Server logs on to CPUs with SIMATIC capability to receive SIMATIC event messages. The received event messages are displayed in the global and in the device-specific event list of the CPU and are indicated as having the status "Incoming" (for active statuses) or "Outgoing" (for no longer active statuses). Activating this monitoring at the device level is achieved using device parameters with the same name.  
The logon to receive SIMATIC event messages from CPUs with SIMATIC capability can be restarted by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".
- SIMATIC monitoring including assigned devices and SIMATIC alarm messages (can only be selected when the "SIMATIC monitoring of assigned devices" check box is enabled)  
When this check box is enabled, SINEMA Server logs on to CPUs with SIMATIC capability to receive SIMATIC alarm messages. The received alarm messages are displayed in the global and in the device-specific event list of the CPU and are indicated as having the status "Incoming" (for active statuses) or "Outgoing" (for no longer active statuses). Activating this monitoring at the device level is achieved using device parameters with the same name.  
The logon to receive SIMATIC alarm messages from CPUs with SIMATIC capability can be restarted by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".

---

#### Note

##### Requirements for receiving and displaying SIMATIC event messages / alarm messages

To allow SINEMA Server to receive and display SIMATIC event messages / alarm messages from a CPU with SIMATIC capability, the following requirements must be met:

1. In the STEP 7 configuration of the CPU, SIMATIC event messages / alarm messages must be enabled so that end devices can log on to the CPU to receive the messages. Enabling the messages for SINEMA Server is based on the same principle as for HMI devices.
  2. To assign the messages to message texts, the option "Enable Web server on module" must be enabled in the STEP 7 configuration of the CPU. As an alternative in STEP 7 as of V5.5.4 the option "Generate and load Web server configuration" can be enabled. This is, however, not available for all CPUs with SIMATIC capability.
- 

#### See also





Device window with device list (Page 98)



### 4.4.3.3 Administration - Monitoring SNMP settings

#### 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. As default, SNMP settings with versions 1 and 2c are available and enabled. During the network scan, SINEMA Server searches through all devices capable of SNMP in descending order of the active SNMP versions. If an SNMP setting with version 3 is available and enabled, this setting is used by SINEMA Server during the scan.

#### Note

##### Using SNMP V3

For reasons of security, it is advisable to use SNMP settings in which SNMP V3 is used. Select only secure passwords with a high password strength.

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

#### 4.4.3.4 Administration - Monitoring Polling groups

This window shows the three polling groups "Fast", "Medium" and "Slow" each in a separate tab, together with their assigned network devices.

General | SNMP settings | **Polling groups** | OPC

Fast | Medium | Slow

Rate (in sec.): 30 Move to: Slow(1000) Medium(497) 2/250

Status	IP address	Name	Device type	Location
<input checked="" type="checkbox"/>	192.168.0.58	plc1	CPU 315-2 PN/DP (2EH13-0AB0)	
<input checked="" type="checkbox"/>	192.168.0.51	et200s	ET200S IM151-3 PN HF (3BA22-0AB0)	

Page 1 of 1 View 1 - 2 of 2

#### 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
Rate (in sec.): <input type="text" value="30"/> 	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 *
<input type="text"/>	Enter text for text search		Start text search
<input type="text" value="41/250"/>	Display the used / available table entries		

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

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

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

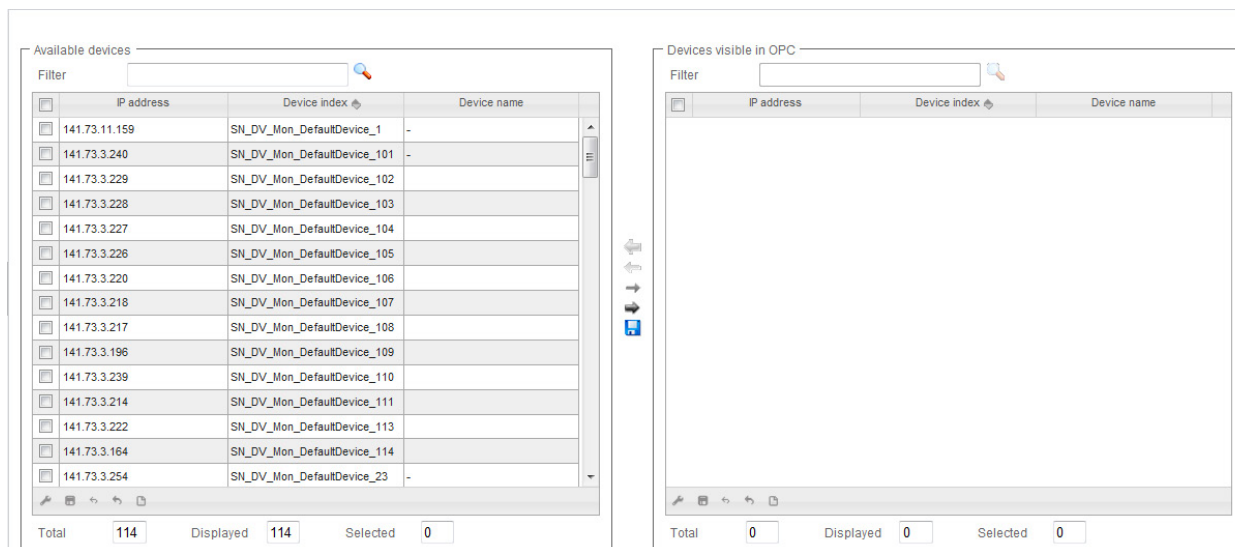
## Setting up polling groups - procedure

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

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

### 4.4.3.5 Administration - Monitoring OPC

You open the Web page shown below using the menu command: **"Administration > Monitoring > OPC"**



## 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 211)

## Layout






In the **"Administration > Monitoring > 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 107)

## 4.4.4 Administration - Events

### 4.4.4.1 Administration - Events Event types

You open the Web page shown below using the menu command: **"Administration - Events > Event types"**

The Web page contains the following tabs:

- "Network events"
- "System events".

In these tabs you have the option of configuring the display of network- and system-relevant 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 tabs are nearly identical in the form and content. Therefore, the following figure serves as an example for both tabs.

Event types

Overall status groups

Event reactions

Network events

System events

All

	Status	Text	Class	Trap OID
		Duplicate IP address found.	Error	
		Monitored SINEMA Server: change to overall status number	Info	
		Device monitoring: Device is not configured as a controller	Info	
		Device status: PNIO status: Maintenance requested	Error	
		Device status: reachable	Info	
		Device status: Not connected	Info	
		Device status: PNIO status: Error	Error	
		Device monitoring: device can reached again with DCP	Info	
		Device monitoring: DCP was enabled for the device	Info	
		Device monitoring: DCP was disabled for the device	Warning	
		Device monitoring: device is no longer reachable with SNMP	Error	
		Device monitoring: device can reached again with SNMP	Info	
		Device properties: SNMP was enabled for the device	Info	
		Device properties: SNMP was disabled for the device	Warning	
		Device status: PNIO status: Maintenance required	Warning	
		Device status: PNIO status OK	Info	
		Device monitoring: SNMPv3 authentication failed.	Error	
		Device monitoring: successful SNMP access	Info	
		Trap: SNMP authentication error detected.	Warning	1.3.6.1.6.3.1.1.5.5
		Trap: device cold restart detected.	Warning	1.3.6.1.6.3.1.1.5.1
		Trap: device warm restart detected.	Warning	1.3.6.1.6.3.1.1.5.2
		Trap: Link down received	Warning	1.3.6.1.6.3.1.1.5.3
		Trap: Link up received	Info	1.3.6.1.6.3.1.1.5.4

Page 1

of 11

23

View 1 - 23 of 247

## Event types - meaning

- "Network events" tab

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

- "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
	Create a new event type (only network event) The input dialog is displayed. If you enable the "Trap" check box, you can specify the OID that will trigger the trap network event (see representation above).
	Edit event type The input dialog is displayed (see above)
	Delete event type (only network event) Note: Network events created by "System" cannot be deleted.
	Change the status of the selected (✓) event type (activated / deactivated) Note: Deactivated event types move to the end of the table.

## 4.4 Administration

Icon	Display / function
	Restore the default settings for selected event types Note: Event types 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"> <li>• All</li> <li>• Enabled</li> <li>• Disabled</li> </ul>

## 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 status of the events (enabled / disabled)
Text	Contains the configurable event text.
Class	Contains the configurable classification.
Trap OID (only with "network events")	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.
Original text	Contains the text entry specified the first time the event type was detected.
Original class	Contains the classification that was specified the first time the event type was detected.
Originator (only for "network events")	Specifies the instance that made the initial definition. The following are possible: <ul style="list-style-type: none"> <li>• System</li> <li>• User</li> </ul>
Overall status group	Specifies the overall status group to which the event belongs. The following are possible: <ul style="list-style-type: none"> <li>• Name of the overall status group</li> <li>• None</li> </ul>

## 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 - System / E-mail settings (Page 205)

### 4.4.4.2 Administration - Events Overall status groups

#### Function of overall status group

An overall status group is a group of functionally related events that influence the overall status of a device. Each event within an overall status group can be assigned an overall status that the device will adopt when the corresponding event condition occurs.

#### Conventions for events in the overall status groups

The following conventions apply to events in the overall status groups:

- An overall status group must contain at least one event. A maximum of 20 events can be assigned to an overall status group.
- An event can only belong to one overall status group.
- Only events assigned to an overall status group can influence the overall status of a device.

#### Statuses of events in overall status groups

To form the overall status of devices, various statuses are significant that events from overall status groups can adopt. These event statuses are displayed in the "Event status" column of the event list.

Event status	Meaning
Pending	When an event that is assigned a negative overall status (every overall status except "OK") is triggered for a device, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device.
Resolving	An event that is assigned the overall status "OK" or "Not connected" is identified by the event status "Resolving" because when it occurs, the event clears all other events of the same overall status group from the list of events pending for the device.
Resolved automatically	An event that was in the list of pending events for a device and was then removed from the list of pending events by a resolving event of the same overall status group is identified by the event status "Resolved automatically".
Resolved manually	An event that was in the list of pending events for a device and was then removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually".
-	A triggered event that is not assigned to any overall status group or is not assigned any overall status in the group has no event status.

## Rules for forming the overall status

The overall status of devices is formed by events from the overall status groups according to the following rules:

- The event with the most negative overall status pending for the device decides the overall status of the device. The classification as the most negative overall status applies to all the overall status groups.
- If a resolving event is triggered, the event status "Pending" is removed for all events of the corresponding overall status group. The device then falls back to the most negative overall status assigned to one of the remaining pending events. If there is no further event pending for the device, the device receives the overall status "OK" or "Not connected".
- As an alternative, the "Pending" status can also be removed manually using the stamp icon in the event list. The device then falls back to the most negative overall status assigned to one of the remaining pending events. If there is no further event pending for the device, the device receives the overall status "OK" or "Not connected".

## Example of forming overall statuses

In the following example, various events are triggered by a device that belong to different overall status groups.

The overall status groups are made up of the following events:

- Overall status group "A":
  - Event "A1": Warning - Overall status "Maintenance demanded"
  - Event "A2": Info - Overall status "Maintenance required"
  - Event "A3": Info - Overall status "OK" (resolving event)
- Overall status group "B":
  - Event "B1": Warning - overall status "Error"
  - Event "B2": Info - Overall status "OK" (resolving event)
- Overall status group "C":
  - Event "C1": Warning - Overall status "Maintenance demanded"

The following table shows the changes in the device overall status based on the occurrence of these events and the events pending for the device. Initially there are no pending events for the device and the device has the overall status "OK".

Triggered event / user action	Overall status of the device	Events pending for the device
A1	Changes from "OK" to "Maintenance demanded".	<ul style="list-style-type: none"> <li>• A1 - "Maintenance demanded"</li> </ul>
A3	Changes from "Maintenance demanded" to "OK".	None.
C1	Changes from "OK" to "Maintenance demanded".	<ul style="list-style-type: none"> <li>• C1 - "Maintenance demanded"</li> </ul>
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None

Triggered event / user action	Overall status of the device	Events pending for the device
A2	Changes from "OK" to "Maintenance required".	<ul style="list-style-type: none"> <li>A2 - "Maintenance required"</li> </ul>
A1	Changes from "Maintenance required" to "Maintenance demanded".	<ul style="list-style-type: none"> <li>A1 - "Maintenance demanded"</li> <li>A2 - "Maintenance required"</li> </ul>
B1	Changes from "Maintenance demanded" to "Error".	<ul style="list-style-type: none"> <li>B1 - "Error"</li> <li>A1 - "Maintenance demanded"</li> <li>A2 - "Maintenance required"</li> </ul>
C1	"Error", no change.	<ul style="list-style-type: none"> <li>C1 - "Maintenance demanded"</li> <li>B1 - "Error"</li> <li>A1 - "Maintenance demanded"</li> <li>A2 - "Maintenance required"</li> </ul>
A3 (resolving event for overall status group "A")	"Error", no change.	<ul style="list-style-type: none"> <li>C1 - "Maintenance demanded"</li> <li>B1 - "Error"</li> </ul>
B2 (resolving event for overall status group "B")	Changes from "Error" to "Maintenance demanded".	<ul style="list-style-type: none"> <li>C1 - "Maintenance demanded"</li> </ul>
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None

## Types of overall status groups

A distinction must be made between system-defined and user-defined overall status groups.

In system-defined overall status groups, the assignments of overall statuses to events belonging to the overall status group can be adapted. Events of the overall status group can also be enabled / disabled. Existing events cannot, however, be removed from a system-defined overall status group. It is also not possible to add an event to a system-defined overall status group.

In user-defined overall status groups events can be included that are visible in the entry "Event types". Overall statuses can be freely assigned to these events. It is also possible to remove events from user-defined overall status groups. A maximum of 100 overall status groups can be created.

The following figure shows the events of the system-defined overall status group "SNMP Reachability" and the properties dialog of an assigned event:

Overall status group "SNMP Reachability"

Basic data

Name: SNMP Reachability      System defined: ☒

Events

Event status	Name	Class
<input checked="" type="checkbox"/>	Device properties: SNMP was enabled for the device	Info

Event dialog details:

Basic data

Events: Device properties: SNMP was enabled for the device

Class: Info      Resolving: ☒

Device status: OK

Buttons: Cancel, OK, Cancel, Save



## Layout of the Web page

On the "Administration > Events > Overall status groups" Web page, system-defined and, if they exist; user-defined overall status groups are displayed.

## Operator input

The following table explains the function elements of the header.

Icon	Display / function
	Create new overall status group The dialog for configuring overall status groups is displayed (see description below).
	Edit overall status group The dialog for configuring overall status groups is displayed (see description below).
	Delete overall status group Note: System-defined overall status groups cannot be deleted.
	Reset selected overall status groups The selected system-defined overall status groups are reset to the default settings.


Icon	Display / function
	Enter text for text search / filter setting
	Start text search / filter setting Result: The overall status groups that match the text string specified for the text search are displayed.

## Content

The overall status groups are shown in the form of a table.


Parameter	Meaning
"Check box"	Select this option to select all the displayed entries.
Name	Name of the overall status group
System-defined	Specifies whether the overall status group is system-defined or user-defined. In system-defined overall status groups, the assignments of overall statuses to events belonging to the overall status group can be adapted. Events of the overall status group can also be enabled / disabled. Existing events cannot, however, be removed from a system-defined overall status group. It is also not possible to add an event to a system-defined overall status group. In user-defined overall status groups, any events created in "Event types" can be included. Overall statuses can be freely assigned to these events. It is also possible to remove events from user-defined overall status groups. A maximum of 100 overall status groups can be created.

## Dialog for configuring overall status groups

This dialog shows the name of the overall status group and its events. Assigned events can be enabled or disabled for triggering. User-defined overall status groups can be assigned events that are visible in the entry "Administration" > "Events" > "Event types". After selecting an assigned event or the icon , the dialog for assigning events opens.

## Dialog for assigning events

This dialog is used to select an assigned event and to select the overall status that the event will cause if it is triggered. The following functions are available:

- Event: Name of the assigned event. In user-defined overall status groups, the dialog for selecting the assigned event can be opened using the icon . In this dialog, you can select the network event to be assigned. The OIDs are displayed as default in the selection dialog for trap network events.
- Event class: Categorization of the assigned event.
- Overall status: Overall status that the device will adopt when the event occurs.
- Resolving: Specifies whether or not an event resolves (removes) all other events pending in the list for a device in the same overall status group. Only events assigned the "OK" overall status are resolving events.
- OID: Display of the OID of a selected trap network event.

#### 4.4.4.3 Administration - Events > Event reactions

The dialogs described below are available with the menu command: **"Administration - Events > Event reactions"**

#### 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.

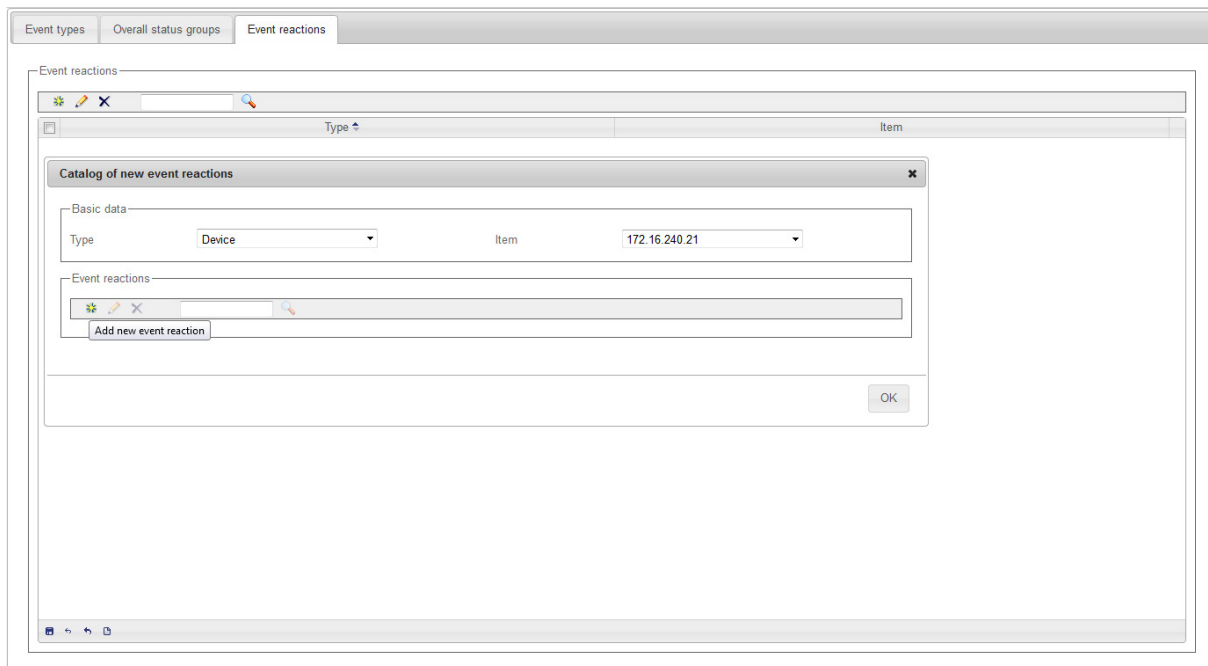
- for the system
- for network devices

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.

## 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		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 e-mail recipients to be notified when the event occurs. Note: If multiple e-mail recipients are specified, these need to be separated from each other by a semicolon (there must be no spaces).
Language	The sent e-mail contains an event-specific information text. Here, select the language to be used for output.
Program	Here, enter the name of an executable program that will bring about a specific reaction to the event.
Text	Specifies an additional text to be transferred by e-mail (see also information relating to the "Language" parameter). You can also specify the transfer parameters for program execution. Example: <i>mail.exe \$i \$m \$n</i> These transfer parameters are interpreted and replaced by SINEMA Server as follows when the executable program is called. Syntax and meaning <ul style="list-style-type: none"> <li>• \$i - placeholder for IP address</li> <li>• \$m - placeholder for MAC address</li> <li>• \$n - placeholder for device name</li> </ul>

**4.4.5 Administration - User****Overview**

The **"Administration > User"** Web page has the following tabs:

- "User"
- "Groups"
- "Logon locks"

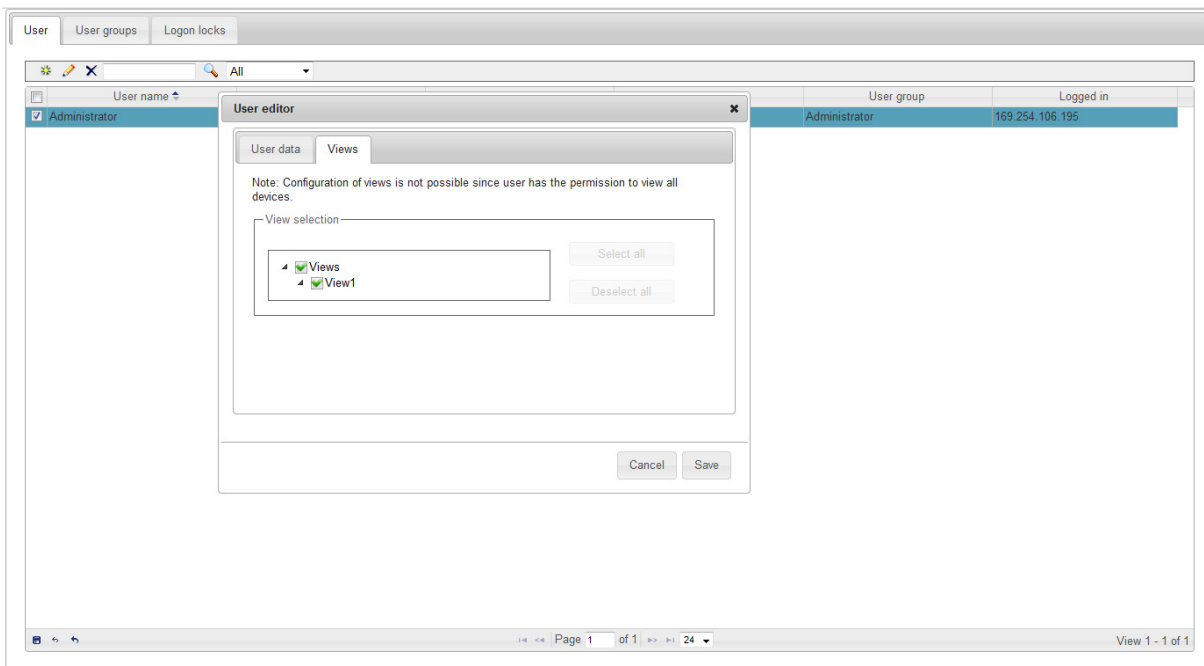
The following explains the form, content and functionality of these tabs.

**4.4.5.1 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.





## 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
	Enter text for text search / filter
	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"> <li>• All</li> <li>• Logged in</li> <li>• Logged off</li> </ul>

The data area contains the user data with the following columns:

- User name
- Full user name
- E-mail
- View(s) (assigned views)

- User group
- Logged in (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

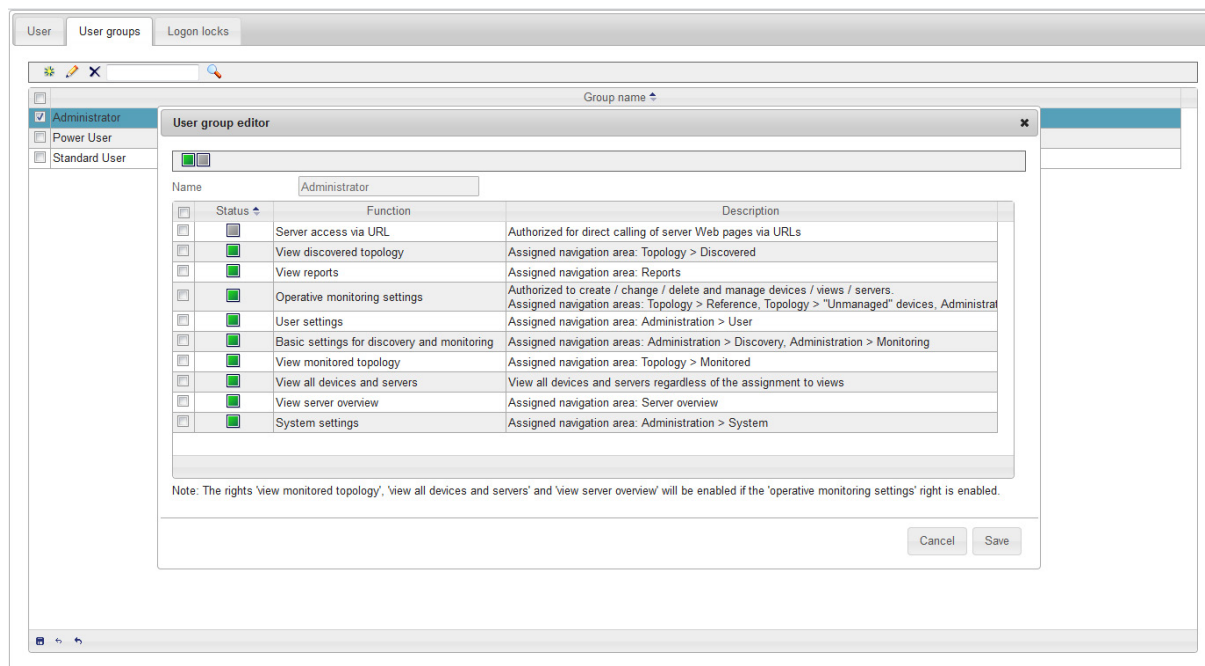
When you create or modify a user, a further window opens in which you can enter the user data and select the views. If the user does not have the right "View all devices and servers", after the user is logged on only the devices and SINEMA Server instances are displayed that are assigned to the view of the user. A PNIO system is only displayed for this user when the corresponding controller is assigned to at least one view of this user.

## See also

Users and user groups (Page 72)






### 4.4.5.2 Administration - Users 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. Note: The "User settings" right in the "Administrator" user group cannot be disabled.
	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:

- Server access via URL
- View discovered topology
- View reports
- Operative monitoring settings
- User settings
- Basic settings for discovery and monitoring
- View monitored topology
- View all devices and servers
- View server overview
- System settings

## 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 "Activate" button to assign the selected functions to the user group.
4. Select the "Deactivate" 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 72)

### 4.4.5.3 Administration - User Logon locks

#### Protection from brute force attacks

To protect against brute force attacks, after five failed logon attempts the IP address of a user or a user the logon to SINEMA Server is rejected for one hour assuming that there was less than five minutes between the logon attempts.

#### Locked IP addresses / unlocking users

Locked IP addresses are displayed under "Administration > User > Logon locks" and can be unlocked by users who have the "User settings" right.

### 4.4.6 Administration - System

#### 4.4.6.1 Administration - System System information

The "Administration > System > 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

#### 4.4.6.2 Administration - System configuration

##### Meaning

In this dialog, you can export your system configuration, import an exported system configuration and reset your system configuration to initial values.

In this dialog, you also specify the shared secret for access to data of other SINEMA Server instances. Before a SINEMA Server instance can query device data of another SINEMA Server instance and display it in the server overview, the same shared secret must be configured for both of them.

With the **"Administration > System > Configuration"** menu command, you obtain the following buttons and functions:

"System configuration" dialog area:

- "Export" button

To export the system configuration, click the "Export" button. The following settings can be saved on a specified path:

- Scan settings
- Device profiles
- General monitoring settings
- Event types / event reactions / overall status groups
- "Unmanaged" device types
- Filter templates

- "Import" button

To import an existing system configuration, click the "Import" button and select the file \*.dpl in the dialog that opens.

Importing a system configuration is only possible when there are currently no devices in the system.

- "Reset" button

To reset certain settings of the system configuration, click the "Reset" button. A dialog box with options opens in which you can make your selection.

Resetting a system configuration is only possible when there are currently no devices in the system.

"Server overview" dialog area: Entry of the shared secret.

#### 4.4.6.3 Administration - System / E-mail settings

Before you can configure an event reaction in "Administration > Event reactions" you need to configure e-mail settings in "Administration > System > 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)

## See also

Administration - Events Event types (Page 190)

## 4.4.7 Administration - My settings

### 4.4.7.1 Administration - My settings Password

#### 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.

### 4.4.7.2 Administration - My settings User interface

The "**Administration > My settings > User interface**" Web page includes the "Monitoring refresh interval" box. With the monitoring interval, you specify the number of seconds after which the data in the user interface is updated. The minimum value is 15 seconds.

You can save the value using the  icon in the header.

## 4.5 Server overview


You can open the "Server overview" Web page in one of the following ways:

- Entry in the navigation bar
- Entry below the "Server overview" node in the device tree

Name	IP/Host	System status	Red	Yellow	Green	Other
Sinema Server 1	192.168.110.145	OK	0	0	15	0
Sinema Server 2	192.168.110.150	OK	0	0	0	0

### Meaning







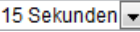

On the "**Server overview**" Web page, SINEMA Server provides an overview of the overall statuses of devices monitored by other SINEMA Server instances in the network. To do this, the Web page shows how many devices have which overall status for each SINEMA Server. To increase and decrease the number of devices, there are system events that can be enabled or disabled for each device overall status.

Before SINEMA Server instances are displayed on this Web page, they must be created and configured using the  button, refer to the section "Configuring a SINEMA Server instance".

Configured SINEMA Server instances can be called directly from the server overview. When they are called up, there is an automatic authentication with the user data with which the calling user is logged in for the local SINEMA Server instance. To do this, the user needs the "Server access via URL" right.







## Operator input

The following table shows the operator control elements of the "Server overview" Web page with a brief explanation.

Icon	Display / function
	Open server in new tab With this function, you open the selected SINEMA Server instance and are automatically logged in with the user data configured for the instance in the server overview.
	Add new server This function opens the "SINEMA Server editor" dialog. In this dialog, you configure the data for the reachability of the SINEMA Server instance; refer to the section "Configuring a SINEMA Server instance".
	Edit selected server With this function you open the "SINEMA Server editor" dialog in which you can edit the existing entries, refer to the section "Configuring a SINEMA Server instance".
	Delete servers
	Create report With this function, you open the dialog for configuring a report containing the number of reachability statuses of a selected SINEMA Server instance over a selected period. The following parameters can be configured in this dialog: <ul style="list-style-type: none"> <li>The period the report will cover.</li> <li>The types of reachability status to be included in the report.</li> </ul>
	Enter text for text search / filter
	Set polling interval. The default setting is 15 seconds.
	Start text search / filter setting

## Content

The following information is available in the columns of the server overview:

Parameter	Meaning
Name	Name of the SINEMA Server instance
IP/host	IP address of the SINEMA Server instance
System status	Reachability status of the SINEMA Server instance
	Number of devices that currently have the overall status "Not reachable".
	Number of devices that currently have the overall status "Error".
	Number of devices that currently have the overall status "Maintenance demanded".
	Number of devices that currently have the overall status "Maintenance required".
	Number of devices that currently have the overall status "OK".
	Number of devices that currently have the overall status "Not connected".



Parameter	Meaning
Port Web UI	Port used to call the SINEMA Server instance from the server overview.
Protocol	Protocol used to call the SINEMA Server instance from the server overview.
Port server poll	Port used to poll the overall device statuses from the SINEMA Server instance.

**Note****User-specific display of the SINEMA Server instances**

SINEMA Server instances that were created in the server overview can be part of views that can be assigned to specific users. If you are logged in as a user whose user group has restricted user rights and to which such a view was assigned, you will only see the SINEMA Server instances of the corresponding view in the server overview.

**Configuring a SINEMA Server instance**

The "Basic settings" tab of the "SINEMA Server editor" window contains the following operator control elements:

Operator control element	Function
Name	Name of the SINEMA Server instance to be displayed in the server overview
IP/host	IP address of the SINEMA Server instance
Protocol	Protocol used to call the SINEMA Server instance from the server overview.
Port	Port used to call the SINEMA Server instance from the server overview.

In the "Advanced settings" tab, the port used to poll the device overall statuses from the SINEMA Server instance can be configured.

**Calling up a SINEMA Server instance - requirement**

SINEMA Server instances are called up from the server overview using the HTTPS protocol. To be able to call up SINEMA Server instances, 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.

**See also**

SINEMA Server users and roles concept (Page 72)



## 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. In turn, the configuration data of SINEMA Server and the properties of the network devices can be accessed via the OPC server. For the interaction with an OPC server, any OPC client can be used. Using the OPC server, you can display the runtime data and properties of a SINEMA Server project.

---

#### 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 > Monitoring > 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.

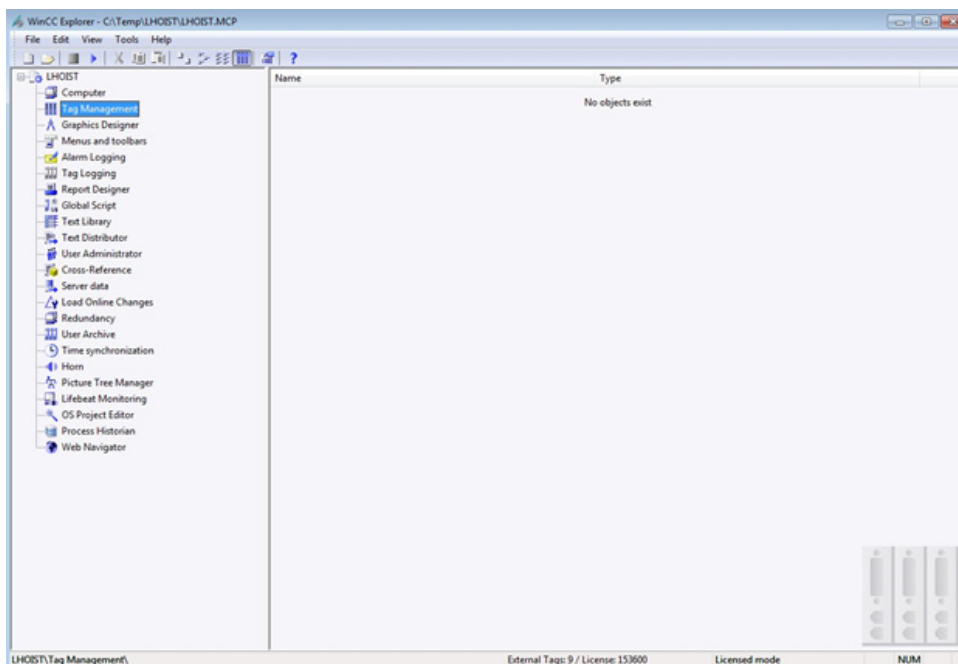
### Configuring UA ports

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.

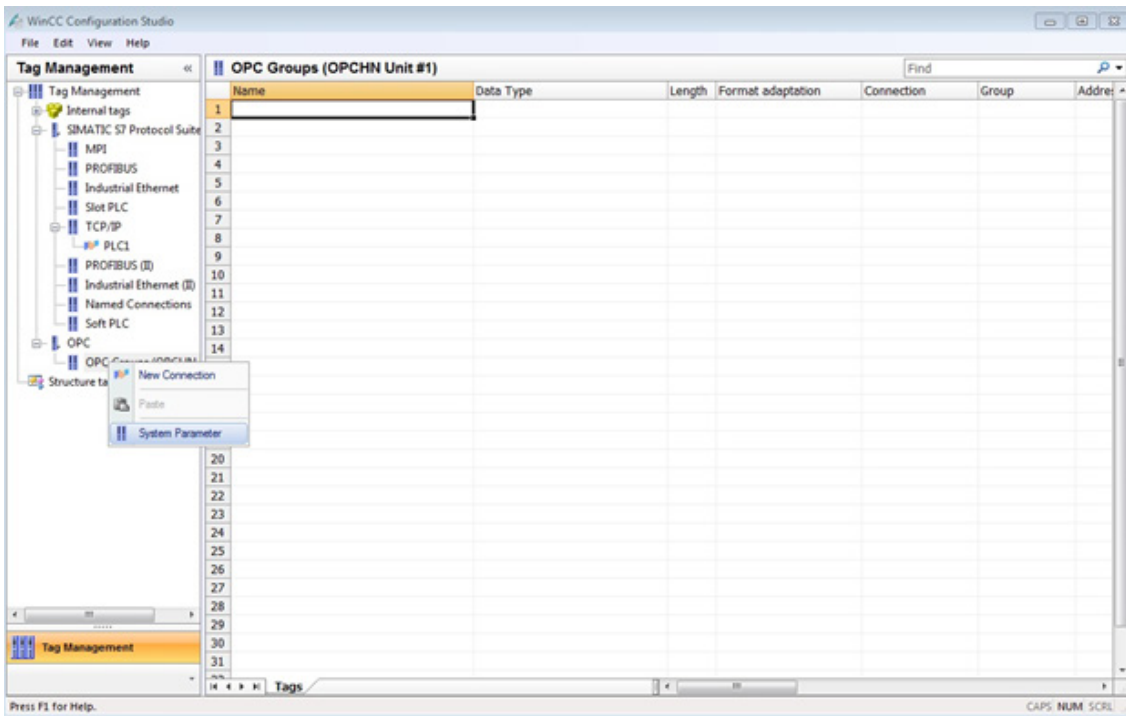
For more detailed information on configuring a UA port, refer to the section Port settings (Page 28).

### Creating a secure OPC connection in WinCC Explorer 7.2

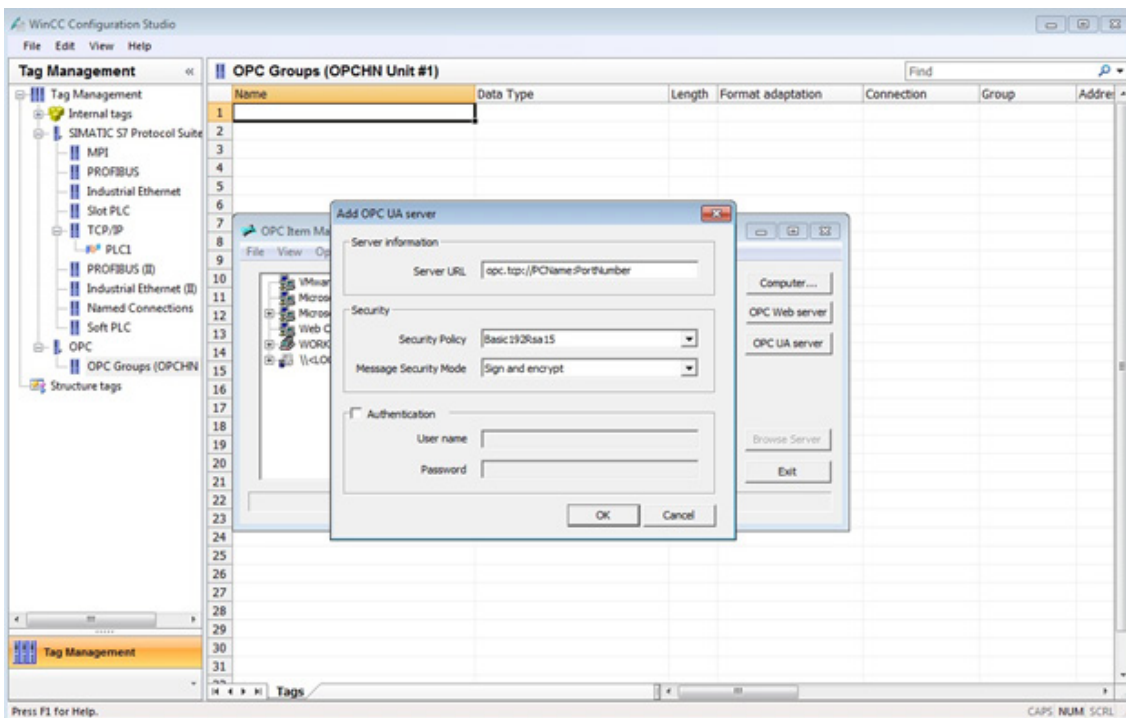
1. You will find the WinCC client certificate "Siemens OPC UA Client for WinCC.der" in the path "C:\Program Files\SIEMENS\WinCC\OPC\UAWrapper\PKI\CA\certs". Copy this certificate to the folder "C:\Siemens\SINEMAServer\Sinema\_Server\WinCC\_OA\3.13\data\opcua\server\PKI\CA\certs".
2. Start the WinCC Explorer.
3. Open the Tag Management.



4. In OPC Groups , open System Parameter.



5. Create a new OPC UA connection.

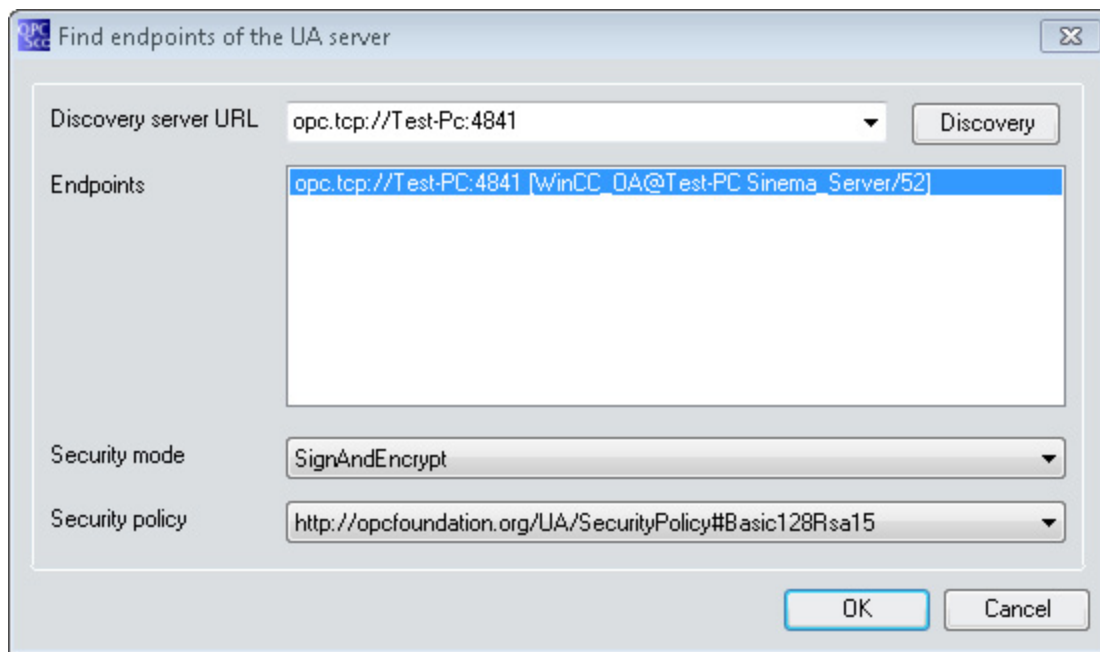


Result: The error message "This OPC Server does not support a browser interface" appears.

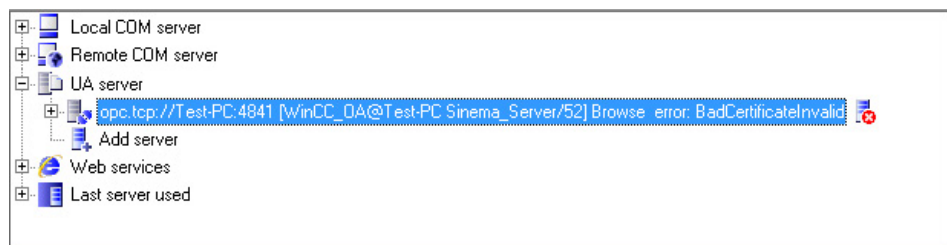
6. Copy the rejected certificate from the folder "C:\Program Files\SIEMENS\WinCC\OPC\UAWrapper\PKI\CA\rejected\certs" to the folder "C:\Program Files\SIEMENS\WinCC\OPC\UAWrapper\PKI\CA\certs".
7. Create a new OPC UA connection again to have full secure access (Basic 192RSA 15).

### Accessing (OPC Scout) SINEMA Server data via an OPC server (OPC UA)

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



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



5. You will now find the rejected OPC Scout V10 certificate in the directory  
"C:\Siemens\SINEMAServer\WinCC\_OA\3.13\data\opcua\server\PKI\CA\rejected".



6. Move this certificate to the folder  
"C:\Siemens\SINEMAServer\WinCC\_OA\3.13\data\opcua\server\PKI\CA\certs".
7. Now double-click on the server again for a signed and encrypted connection.

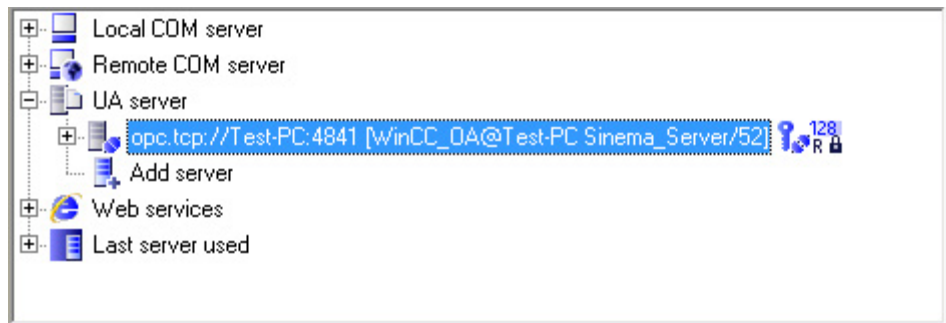


Figure 5-1 Scout\_4

## 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 setting is disabled, enable as follows:

1. Right click on the "My Computer" icon and select the "Properties" option to view the system properties.
2. In "Advanced", open the "Performance" options.
3. Select the "Data Execution Prevention" tab.

---

**Note**

The steps involved in configuring the DCOM settings in SINEMA Server apply to the Windows Server 2008 R2 operating system.

---

**Note**

Before settings can be made for DCOM, you may need to configure exceptions in the Windows firewall.

---

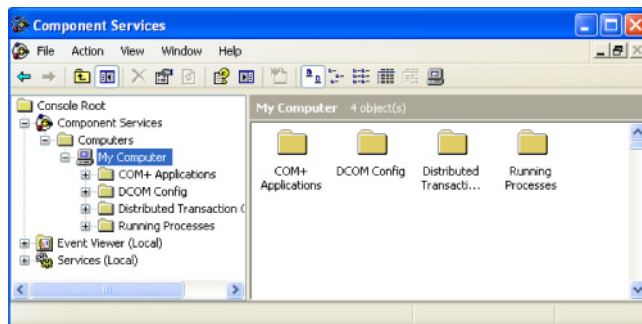
### Setting up the properties of the DCOM configuration for OPC DA communication

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

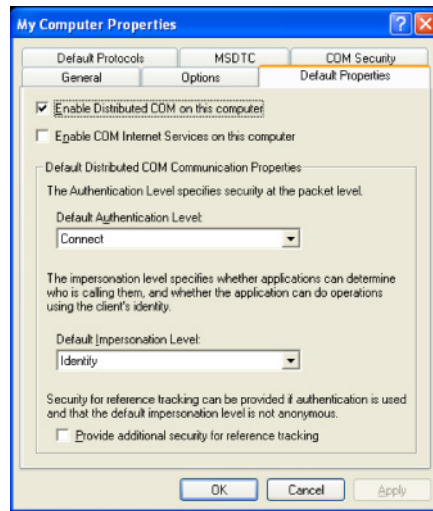
1. In Windows, select the command "Start > Run". In the "Open" list box, enter the command "dcomcnfg" and confirm with OK.
2. The "Component Services" window then opens with the folder hierarchy.



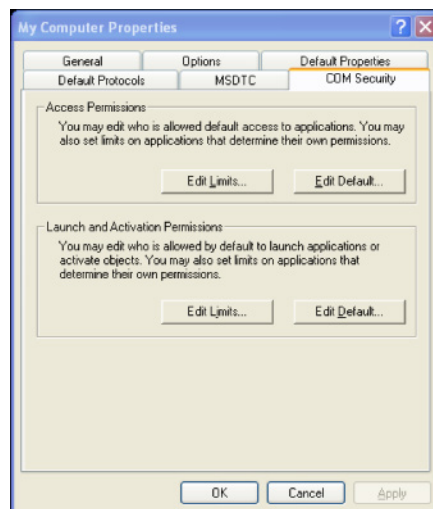
3. Go to the component services, Computers, My Computer.
4. Right click on "My Computer" and select the "Properties" option to open the "My Computer Properties" window.
5. Enter a brief description for your computer and confirm with "OK".



6. Go to the "Default Properties" tab and enter the default authentication level by selecting the "Connect" option in the drop-down list.

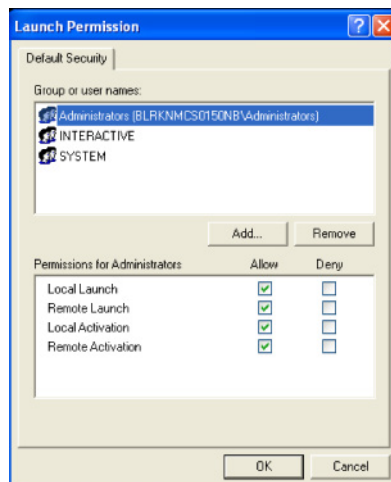


7. In the drop-down list for the default impersonation level, select the "Identify" option and confirm with "OK".
8. In the "Default Protocols" tab, move the "Connection-oriented TCP/IP protocol" entry to the first position in the list under "DCOM Protocols" and remove other protocols that are not being 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.

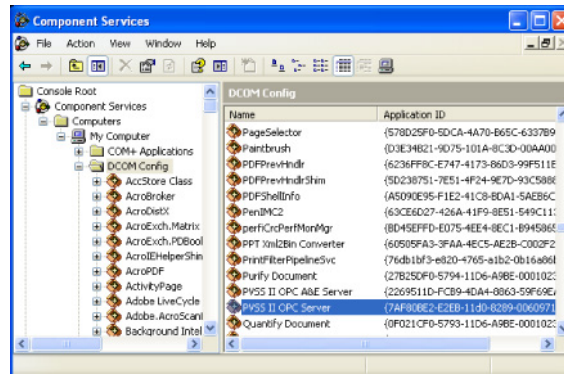


14. Configure the launch permissions by selecting the required options and confirming with "OK".
  - To allow all users access, add the domain group "Everyone".
  - If the server and client are in the same network domain, add the list of users who will access the OPC server. You should also allow these 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

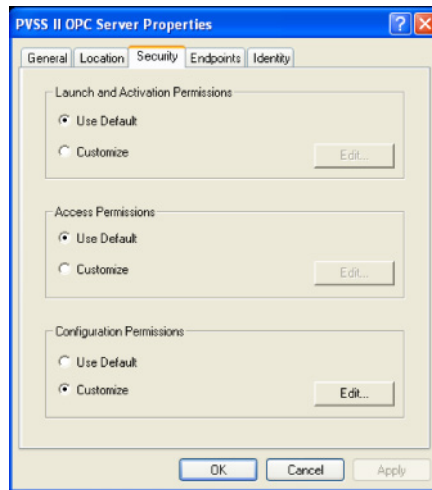
### Procedure

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.

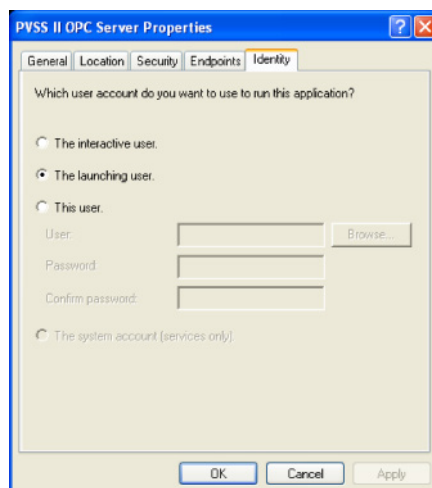


3. In the list view, select "PVSS II OPC Server". Right click on this object and select "Properties".
4. The "PVSS II OPC Server Properties" window is displayed.
5. In the "General" tab, enter "Default" as the authentication level by selecting this option in the drop-down list.
6. The authentication 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.

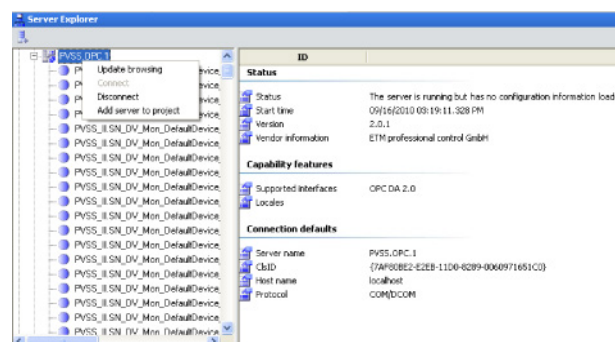
### Configuring DCOM settings for the OPC server browser

1. In the DCOM Config list view, select the "OpcEnum" 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".
4. After working through these steps, restart the system.

## 5.3.3 Accessing SINEMA Server data via an OPC server (DA)

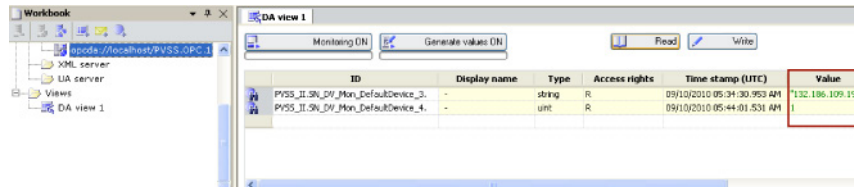
### Procedure

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.

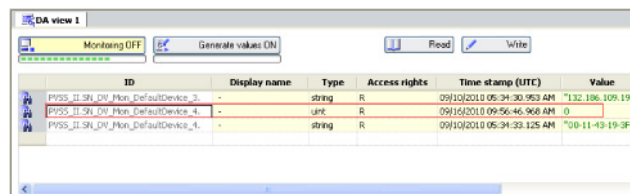


5. The connection status, performance features and connection defaults of the server are displayed on the right-hand side of the Server Explorer window.
6. Note that a view "DA view1" for the DA server has already been created in the workbook area.
7. Drag the required device elements to the "DA view1" area.

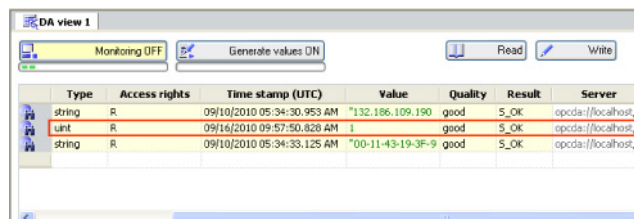
8. Click the "Read" button at the top edge of the area. This starts reading out of the values for the individual device properties of the selected device (see below).
9. As an example, in the figure below, you can see the values displayed for the device properties "IP address", "MAC address" and "Is 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.



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.









## 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 > My settings > Password" 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 disk space on "C:" even if there is enough free disk space on drive "D:".

### **What can I do if the Web browser has long reaction times?**

If the SINEMA Server application is open in the Web browser for a longer period of time (more than 3 days), this can lead to long loading times for Web pages.

Remedy:

Close and reopen the browser.

### **Why is it useful to create system backups?**

Since the volume of project data in the SINEMA Server application grows over time, it is advisable to make a regular system backup of the project data in the SINEMA Server application.

### **How can I change the background color for printing out?**

The print function of SINEMA Server is configured as default so that printouts have a gray background. This setting is advantageous when printing charts.

If you want a white printout background when printing pages and do not require charts to be printed out, follow the steps below:

Go to **"Tools > Internet Options > Advanced"** and disable the **"Print background colors and images"** option.

## **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.

**Why doesn't SINEMA Server start up?**

There is possibly an IP address conflict. The IP address of the management station with SINEMA Server must be unique in the network. If the IP address of the management station has been assigned to another network device in the network, it is not possible to start SINEMA Server.

**SINEMA Server Monitor indicates a system error in the "WCCOADddManager" component. What can I do?**

It is possible that the WinPCap software is not correctly installed. Follow the steps outlined below:

1. Exit SINEMA Server.
2. Install WinPCap manually from the SINEMA Server product DVD.
3. Start SINEMA Server.

**When do sessions become invalid in SINEMA Server?**

If the PC on which the SINEMA Server Web user interface is running changes to the "Hibernate" or "Standby" status, the current session becomes invalid and the current user is automatically logged out.

Remedy:

Make sure that an adequate interval for changing to "Hibernate" is selected in the operating system.

## **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 icon view, the device icon and the status of the device are shown.

### What happens if there are no reference connections defined in the Reference topology editor?

If a user does not define any reference connections in a reference topology and saves the reference topology, 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.

## 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 "Administration > My settings > User interface".

#### How can scanning be speeded up?

You should restrict the scan range to the devices to be monitored. To do this, it is advisable to divide the IP address range into smaller subgroups if the IP addresses are not consecutive. This division speeds up scanning of the devices.

Specify the IP address ranges to be scanned in "**Administration > Discovery**" in the "Scan" tab.

#### Which security settings are available for SNMPv3?

The following security levels are available for SNMPv3:

- 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 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.

**Why are network devices with SNMP capability not correctly discovered?**

If SNMP is disabled for the device during discovery, it is possible that the device will be identified as a standard ICMP device. If SNMP is enabled later, the SINEMA Server starts to monitor the SNMP data of the device.

A deviation can also result from the following:

- The SNMP settings stored in SINEMA Server are incorrect.
- The SNMP function is disabled on the network device.
- The network device does not reply within the expected time window.

Remedy:

- If necessary, adapt the SNMP parameters.
- If necessary, enable the SNMP function in the network device.
- Delete the network device in SINEMA Server and then run network discovery again.

**Why are media modules not discovered?**

If new submodules are added to a module that is already being monitored by SINEMA Server, it is possible that SINEMA Server will not detect these immediately.

Remedy:

1. Delete the module in question from the SINEMA Server device list.
2. Run the scan again.

Following this, the display is correct.

**Is it possible to run the network scan with VLAN network adapters?**

A network scan with VLAN network adapters is basically possible; however devices can then not be reached using the DCP protocol. The following device properties can therefore not be detected:

- DCP status (reachable / not reachable)
- DCP ID
- PROFINET IO name
- PROFINET IO type

### **Why are incorrect device statuses shown for SCALANCE S devices?**

Due to the implementation of DCP in SCALANCE S devices, these devices do not reply deterministically to a DCP request. The reply to the DCP request may arrive late or not at all. This response is not dependent on the firmware version.

## **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?**

With the event acknowledgment function, you can specify that you have noted an event.

## 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. You can import the configuration data of a system into another SINEMA Server system if no devices have yet been created in the target system.

## A.8 Topic reports

### Frequently asked questions

**How does SINEMA Server create reports if a device in the network is replaced?**

When you delete a device, you can use the "Delete historical data" check box to specify whether the device you are deleting will be included in future reports. If you select the check box, reports created after the device is deleted contain no information about 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?**

The list of profiles can be opened with the menu command **"Administration > Discovery > Profiles"**.

The display of this function depends on the rights of the user.

### **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. You should therefore check whether new device types can be assigned to existing device profiles. For example, can the device type SCALANCE X499 be assigned to 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 device type due to an error in the rules?**

You have 3 options:

- Alternative 1:  
With the function for automatic profile reassignment, SINEMA Server regularly searches for a more suitable device profile for a device that was assigned a standard profile.
- Alternative 2:  
Change the assignment of the device type in the device list using the "Change device type" function.
- Alternative 3
  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?**

Changes to the following device profile properties affect devices that are already using the device profile:

- All the profile properties of the "Basic data" properties tab
- User-defined OID configurations created in the "OID sets" tab
- Parameters for new thresholds
- Changes to existing threshold parameters

**See also**

Setting up network devices individually - using the Profile editor (Page 53)

Administration - Discovery / Profiles (Page 175)

## **A.10 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.

## A.11 Subject SIMATIC monitoring

### Frequently asked questions

#### Why can I not activate SIMATIC monitoring for my CPU? Which CPUs support SIMATIC monitoring?

SINEMA Server V13 supports SIMATIC monitoring of SIMATIC S7-300 / S7-400 / ET 200 CPUs. SIMATIC monitoring can only be activated for these modules.

#### Which settings need to be made on a CPU so that SINEMA Server can receive SIMATIC event messages / alarm messages?

In the STEP 7 configuration of the CPU, SIMATIC event messages / alarm messages must be enabled so that end devices can log on to the CPU to receive the messages. Enabling the messages for SINEMA Server is based on the same principle as for HMI devices.

#### Why do the received SIMATIC event messages / alarm messages contained no texts?

The SIMATIC event messages / alarm messages must be assigned to their corresponding message texts. You achieve this by enabling the option "Enable Web server on module " in the STEP 7 configuration of the CPU. As an alternative in STEP 7 as of V5.5.4 you can enable the option "Generate and load Web server configuration". This is, however, not available for all supported CPUs.

#### When does a PNIO system become visible in the device tree?

Depending on the CPU being used, a PNIO system can result from the following procedures:

- **SIMATIC S7-300 / S7-400 / ET 200 CPUs:**  
The PROFINET IO system can be displayed with the aid of the information that the controller obtains from assigned PROFINET IO devices. To do this, the monitoring setting "SIMATIC monitoring of assigned devices" must be enabled for the controller. In a display of the PROFINET IO system initiated by the controller, the displayed IP addresses are always IP addresses reported by the controller. In this representation, devices are also displayed that are assigned to the controller but that are themselves not SINEMA Server objects.
- **Other controller types:**  
The PROFINET IO system can be displayed with the aid of information that PROFINET IO devices obtain from their controller. To do this, the monitoring setting "PROFINET monitoring" must be enabled for the PROFINET IO devices to be displayed. PROFINET IO devices that cannot be assigned are displayed under the entry "Unassigned devices". If the display of the PROFINET IO system was initiated by PROFINET IO devices, the tooltip of the associated entry displays "Discovered by: IO devices."

# 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.



# Index

## A

- Access rights, 73
- Adapting the scan range, 48, 48, 175
- Add new server, 208
- Administrator, 73
- Archive, 35
- Archive management, 159
  - Meaning, 35
- Assigned monitoring profile, 99
- Assigned profile, 99
- Automation License Manager, 21

## B

- Background graphic, 68
  - Adding, 68
  - Changing the size, 68
  - Deleting, 69
- Basic view, 63

## C

- Calculating the storage space that will become free, 36
- Calculations for the availability report, 161
- Calling functions with a URL, 84
  - Authentication, 84
  - Navigation, 85
  - Web pages, 86
- Calling up a SINEMA Server instance using HTTPS, 209
- Catalog of new event reactions, 199
- Change monitoring profile, 103
- Change the layout of a connection, 71
- Changing the password, 206
- Client computer
  - Logging in, 39
- Cloud, 151
- Configuration limits, 19
- Configure topology settings, 124
- Configuring cloud connections in the network, 153
- Configuring the status of the reference port, 152
- Confirm events, 127
- Controlling the profile display and editing profiles, 176
- Create new device, 102
- Create system backup, 36

- Creating or editing user-defined connections, 69
- Customize device data, 103

## D

- Date and time of day, 49
- DCP, 153
- DCP detection type, 174
- DCP icon, 155
- DCP monitoring interval, 182
- DCP reachability, 99
- Default ports, 30
- Default profiles, 54
- Delete archive, 35
- Delete archives of deleted devices, 35
- Deleting views, 64
- Device discovery using SNMP, 54
- Device hierarchy, 148
- Device list, 48, 98
- Device overview, 95
- Device status, 96
- Device tree, 41, 48, 98, 104
- Device type rule, 56
- Devices
  - Number of monitored, 22
- Discovered topology, 50
- Discovery, (Topology)
- Discovery rule, 56
- Display in the Reference editor, 142
- Display of an empty topology, 68

## E

- Editing the ZIP file, 35
- E-mail client function, 19
- Enable monitoring, 102
- Event, 126
- Event class, 126
- Event details, 126
- Event list, 41, 60, 125
- Event overview, 95
- Event reaction, 60
- Event reactions, 199
  - Create new, 199
- Event types, 191

Events, 111  
    Filter, 80  
    Setting up and monitoring in SINEMA Server, 59  
Expert, 112  
Export archive and delete, 35  
Export table in CSV format, 78

## G

General profile, 175, 178  
Generating HTTPS certificates, 31  
Glossary, 4

## H

Hardware requirements, 23  
Historical data, 167  
HMI systems, 19  
Hop layer, 147  
HTTP port, 28  
HTTP port 80, 29  
HTTPS certificate, 28  
HTTPS port, 28

## I

ICMP, 47  
Icon view, 131  
Import archives, 35  
Import profiles, 176  
Importing a system configuration, 205  
Initial logon data, 40  
Installation  
    Sequence, 24  
    Time required, 24  
Interface list, 104  
IP address, 99  
IP interfaces, 112

## L

LAN ports, 111  
License downgrade, 22  
License key  
    Storage location, 21  
License types and corresponding configuration limits, 20  
License update, 21

## M

MAC address, 99  
Main window, 41  
Management station, 25  
    Logging in, 39  
Media types, 151  
    Combination, 151  
    Explicit message, 151  
Menu commands, 75  
Minimum requirements, 23  
Monitor resolution, 23  
Monitored topology, 50  
Monitoring interval, 206  
Monitoring profile, 53, 175, 178

## N

Navigation bar, 41  
Network adapter, 23  
Network clouds, 142  
Network events, 58, 58, 166  
Network monitoring, 47  
Network scan, 47  
    Effect on the topology discovery, 52  
    Interval, 182  
    Procedure, 48  
Network topology, 62  
Number of LAN ports, 99  
Number of monitored devices, 22

## O

OPC, 189  
OPC UA port, 29  
Open WBM, 113  
Operating system, 23, 99, 204

## P

Page layout  
    General functions, 78  
Polling, 50  
Polling group, 186  
Port address  
    Value 0 (zero), 29  
Port numbers  
    Reserved, 29  
Port status, 155  
Power user, 73  
Printing reports, 159

Processor, 23  
 Profile, 53  
   Add a new device type to an existing profile, 56  
   Creating new, 56, 177  
   Displaying and editing, 175  
   Exporting, 176  
   General, 53  
   Principle of the use of profiles, 53  
 Profile editor, 57  
   "Basic Data" tab, 179  
   "Device types" tab, 180  
   "Discovery rules" tab, 180  
   "OID sets" tab, 181  
 Profile search, 176  
 Profiles  
   Displaying and editing, 177  
 PROFINET device name, 99  
 Program window, 41

## Q

Quick link, 83  
   Setting up, 83  
   Using, 84

## R

RAM, 23  
 Reachability, 99  
 Recalculate topology, 123, 147  
 Receiving SNMP traps, 127  
 Recommended requirements, 23  
 Redundancy, 112  
 Redundancy mode, 99  
 Redundancy status, 99  
 Reference connections, 142  
 Reference editor, 50, 146, 149  
   Adding new devices, 149  
   Adding unmanaged devices, 149  
   Display of the connections, 145  
   Drawing connections between devices manually, 150  
   References for connection lines, 142  
   References for port statuses, 142  
   References for SNMP, DCP protocols, 142  
   Resetting the reference, 147  
   Selection mode and drawing mode, 146  
   Specify a current connection as a reference connection, 150  
   Specifying the current connections as reference connections, 150

Reference port, 152  
 Reference topology, 50, 137  
 Report type  
   Availability, 158  
   Events, 158  
   Inventory, 158  
   Performance, 158  
 Reports  
   Evaluation time, 159  
   Inventory, 164  
 Reports with trend charts, 170  
 Requirements for the Web client, 23  
 Reread device data, 101  
 Reserved port numbers, 29  
 Restore system backup, 36  
 RPC port, 29

## S

Scan, (Network scan), 172  
 Scan LAN interfaces, 174  
 Scanning  
   Procedure, 48  
 Selecting entries in tables, 79  
 Server overview, 207  
 Set device basic data, 103  
 Setting up polling groups, 188  
 SIMATIC NET glossary, 4  
 SNMP, 153  
 SNMP icon, 155  
 SNMP reachability, 99  
 SNMP settings, 99, 185  
 SNMP version, 185  
 Software requirements, 23  
 Specify SNMP settings, 102  
 SSL certificate, 31  
 Standard user, 73  
 Standby mode, 99  
 Start network scan, 173  
 Start SINEMA Server, 26  
 Start Web client, 26  
 Start window, 95  
 Statistical port data, 99  
 Status, 99  
 Status bar, 41  
 Status display  
   in SINEMA Server Monitor, 28  
 Status monitoring, 154  
 Status of protocol-specific device availability, 155  
 Stop network scan, 173  
 Storage requirements hard disk, 23  
 Sub view, 63

- Subnet mask, 48
- System configuration
  - Exporting, 205
  - Importing, 205
- System events, 166
- System information, 204
- System status, 95

## T

- Table layout
  - General functions, 79
- Time stamp, 126
- Topology
  - Active mode, 122
  - Can be mixed with sub view and device display, 69
  - Creating for sub views, 69
  - Detail view, 131
  - Discovery, 50
  - Draft mode, 122
  - Icon view, 131
  - Modes, 122
  - Monitored, 136
  - Operation in active mode, 123
  - Operation in draft mode, 123
  - Reference, 141
  - Unmanaged devices, 151
- Topology discovery
  - Principle, 52
- Topology editor
  - Editing modes, 124
- Topology in the views, 66
- Topology scan, 52
- Topology settings, 133
- Trend charts, 167
  - Zoom function, 170
- Trial license, 20
- Turn off monitoring, 102
- Types of report, 158

## U

- Uninstalling, 25

,

- 'Unmanaged' device types, 156

## U

- UP/DOWN status, 186
- User, 72, 74
- User editor, 202
- User group, 72, 202, 203
- User group editor, 203
- User groups, 74
- User interface
  - Language selection, 44
- User rights, 24
- Using third-party certificates, 31

## V

- View filter in the View editor, 65
- Views, 62, 72, 121
- VLAN, 112

## W

- WBM (Web Based Management), 101
- Web browser, 23
- Web client, 26
- Web interface, 19
- WLAN, 111