SIEMENS
Ingenuity for life

Getting Started Understanding and Using SINEMA Server V14

SINEMA Server

https://support.industry.siemens.com/cs/ww/en/view/109746780

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

© Siemens AG 2017 All rights reserved

Table of Contents

Warranty and Liability 2

1 Introduction 4

1.1 Overview 4
1.2 Reference system 5

2 Preparing the Infrastructure 6

2.1 Installation 6
2.1.1 Valuable information on the installation 6
2.1.2 Installing SINEMA Server 6
2.2 SINEMA Server Monitor 8
2.2.1 Valuable information on SINEMA Server Monitor 8
2.2.2 Using SINEMA Server Monitor 9
2.3 SINEMA WebClient 12
2.3.1 Valuable information on SINEMA WebClient 12
2.3.2 Using and customizing SINEMA WebClient 15

3 Discovering Devices in the Network 19

3.1 Valuable information on device discovery 19
3.2 Preparing and starting device discovery 20

4 Managing and Customizing Devices 26

4.1 Device management 26
4.1.1 Valuable information on device management 26
4.1.2 Customizing the device list 28
4.1.3 Manually enabling device monitoring 31
4.2 Device profiles 35
4.2.1 Valuable information on device profiles 35
4.2.2 Creating, changing and assigning profiles 38

5 Understanding and Filtering the Event List 45

5.1 Valuable information on events 45
5.2 Customizing the event list 47

6 Understanding and Using the Topology 52

6.1 Valuable information on the topology 52
6.1.1 General information 52
6.1.2 Workspaces and how to use them 53
6.1.3 Representation in the topology 56
6.1.4 Editing mode 58
6.1.5 Online mode 59
6.1.6 Views 60
6.2 Visualizing the network topology 61
6.2.1 Opening and setting up the topology 61
6.2.2 Making corrections in the topology 67
6.2.3 Topology in Online mode 76
6.2.4 Setting up views 77

7 Appendix 83

7.1 Service and Support 83
7.2 Links and literature 84
7.3 Change documentation 84

© Siemens AG 2017 All rights reserved

1 Introduction

1.1 Overview

Reason

The SINEMA Server V14 software is a network monitoring tool that was designed specifically for industrial applications. Its diverse features and comprehensive functions allow early identification of network problems and the timely introduction of measures.

The features provided by SINEMA Server include:

- Continuous analysis and monitoring of all network components using SNMP
- Automatic topology detection
- Saving data to long-term storage
- Seamless integration of network diagnostics into HMI systems
- Comprehensive diagnostic and reporting functions.

Motivation

This document supports first-time users and familiarizes them with the basic functions and setting options of SINEMA Server. It is divided into chapters. This takes you step by step through the setting options of SINEMA Server and provides you with the necessary basics.

Guide through the documentation

This document covers the following technological key points:

- Preparing the infrastructure
- Scanning networks
- Basics of the device list
- Basics of events
- Basics of the topology
- Explanation of topology types

The chapters and subchapters normally have an identical, modular structure.

Each chapter starts with a theoretical section called “Valuable information” that explains the basics and principles of the function. This part is followed by a practical section that provides detailed instructions with screenshots.

Note

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

If you already have basic knowledge of SINEMA Server, you can skip the theoretical section and go directly to the practical section.

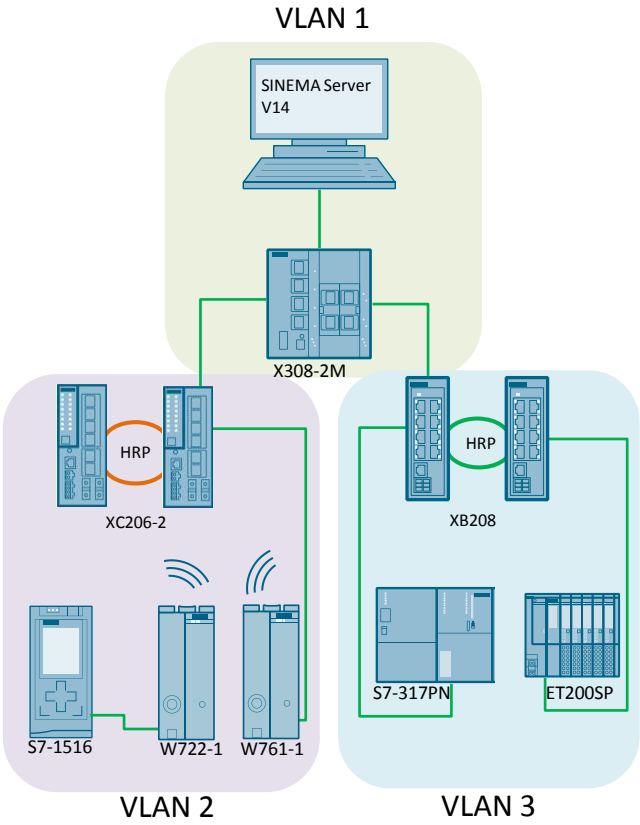
© Siemens AG 2017 All rights reserved

1.2 Reference system

Network configuration

To make it easier for you to get started with SINEMA Server and understand the functions, this document is based on a small reference system. The network configuration monitored in this document has the following structure:

Figure 1-1



Network configuration

The reference system consists of the following devices:

Table 1-1

VLAN	Device	IP address
1	Management station with SINEMA Server V14	192.168.0.1
1	SCALANCE XM308-2M	192.168.0.2
2	SCALANCE XC206-2	192.168.0.11
2	SCALANCE XC206-2	192.168.0.12
2	SCALANCE W761	192.168.0.14
2	SCALANCE W722	192.168.0.13
2	SIMATIC S7-1516-2 PN	192.168.0.15
3	SCALANCE XB208	192.168.0.21
3	SCALANCE XB208	192.168.0.22
3	ET 200SP	192.168.0.24
3	SIMATIC S7-317PN/DP	192.168.0.23

© Siemens AG 2017 All rights reserved

2 Preparing the Infrastructure

2.1 Installation

2.1.1 Valuable information on the installation

Licensing notice

Running SINEMA Server requires a SINEMA Server license. Different license types are available that differ in the number of monitored devices.

Testing SINEMA Server

A test license (“Trial 500”) is available to get to know and test SINEMA Server. This license supports up to 500 monitored devices.
However, it has restrictions compared to the full version. The “Trial 500” license is valid for 21 days.

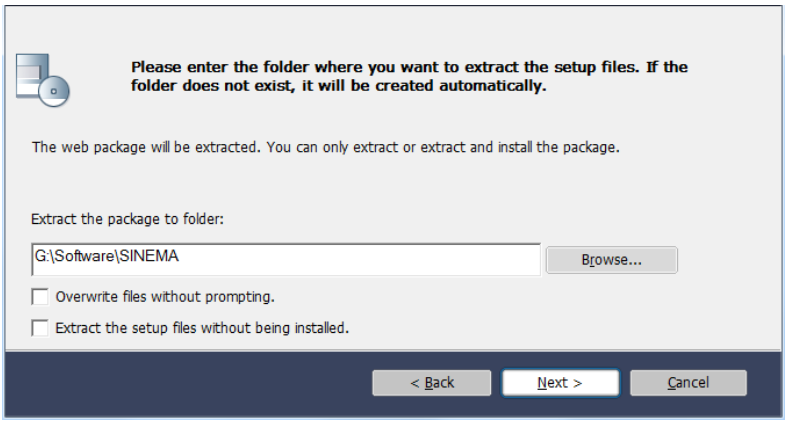
2.1.2 Installing SINEMA Server

Installing the software

The SINEMA Server software can be downloaded from Siemens Industry Online Support (see \3\, Chapter 7.2).

The software is provided to you as a self-extracting archive.

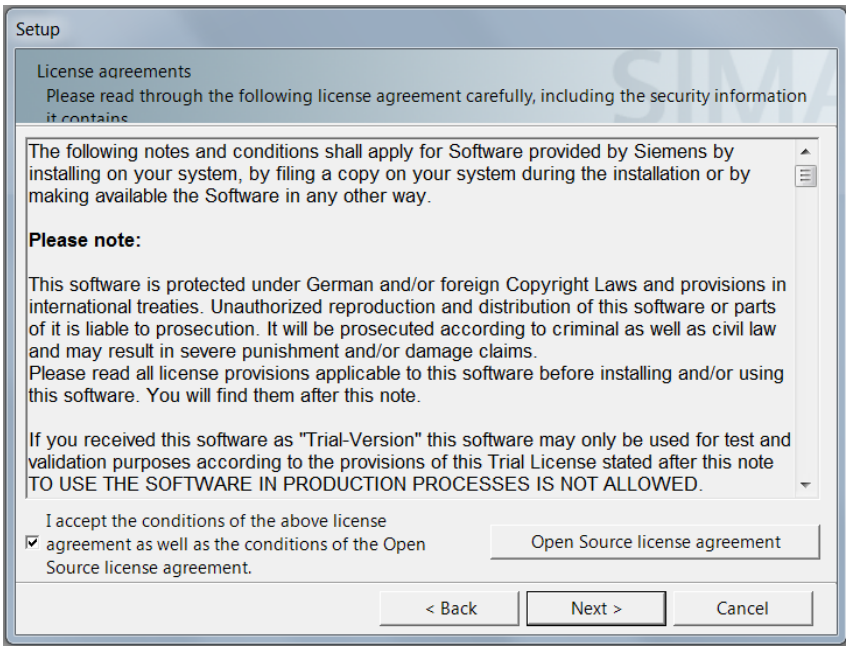
1. Log on to the Windows operating system as an administrator.
   Download the files to a directory on your computer (management station).
   Double-click the .exe file to extract the files.
   Click “Next”.



2. Select the language for the SINEMA Server setup wizard and click “Next”.

© Siemens AG 2017 All rights reserved

3. Click the “Open Source license agreement” button to view the license agreement. Accept the license agreement and click “Next”.



4. The software is installed largely automatically. The SETUP routine automatically detects whether, except for SINEMA Server itself, other program components need to be installed.

5. Follow the instructions that take you through the entire remaining installation process. This may take several minutes.

Result

When the installation process is complete, a status message appears that indicates that SINEMA Server was successfully installed.

© Siemens AG 2017 All rights reserved

2.2 SINEMA Server Monitor

2.2.1 Valuable information on SINEMA Server Monitor

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

SINEMA Server Monitor loads automatically after successful installation of SINEMA Server and with each subsequent Windows start.

The taskbar provides a button to open the SINEMA Server context menu. This context menu provides the functions of SINEMA Server Monitor.
The color of this icon may differ depending on the status of SINEMA Server.

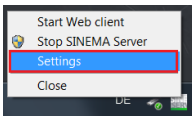
Note You need administrator rights to edit the settings in SINEMA Server Monitor.

© Siemens AG 2017 All rights reserved

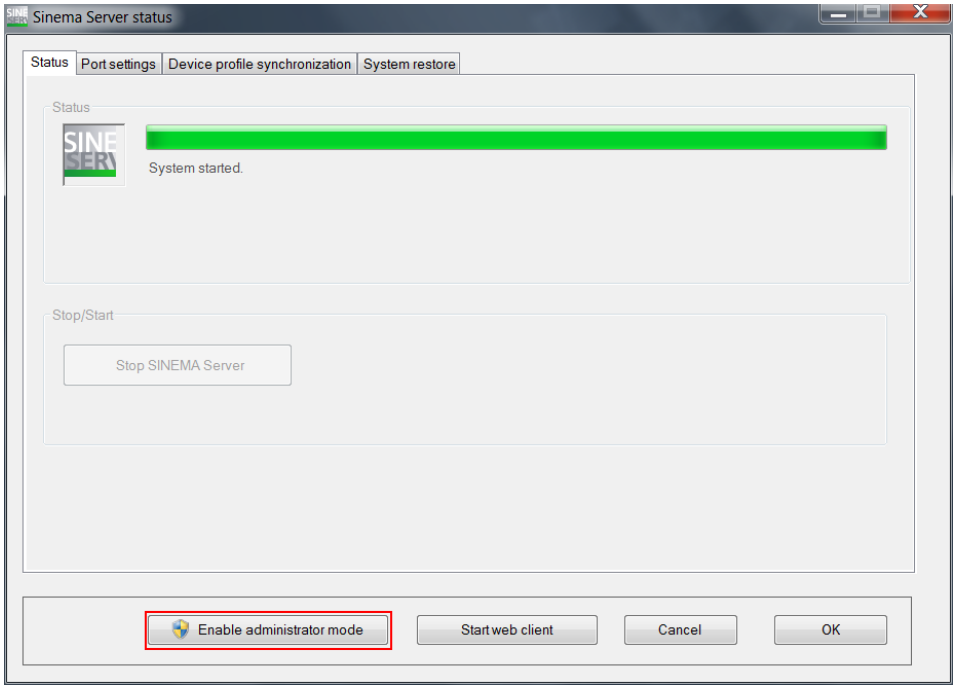
2.2.2 Using SINEMA Server Monitor

To customize SINEMA Server, proceed as follows:

1. Right-click the icon in the taskbar to open the context menu. Select “Settings”.



2. The “SINEMA Server status” window opens. The “Status” tab displays the status of SINEMA Server.
   In order to make settings in SINEMA Server, click “Enable administrator mode”.
   Note:
   If SINEMA Server has not yet started, the “Start SINEMA Server” button is visible. Click the “Start SINEMA Server” button to start SINEMA Server.

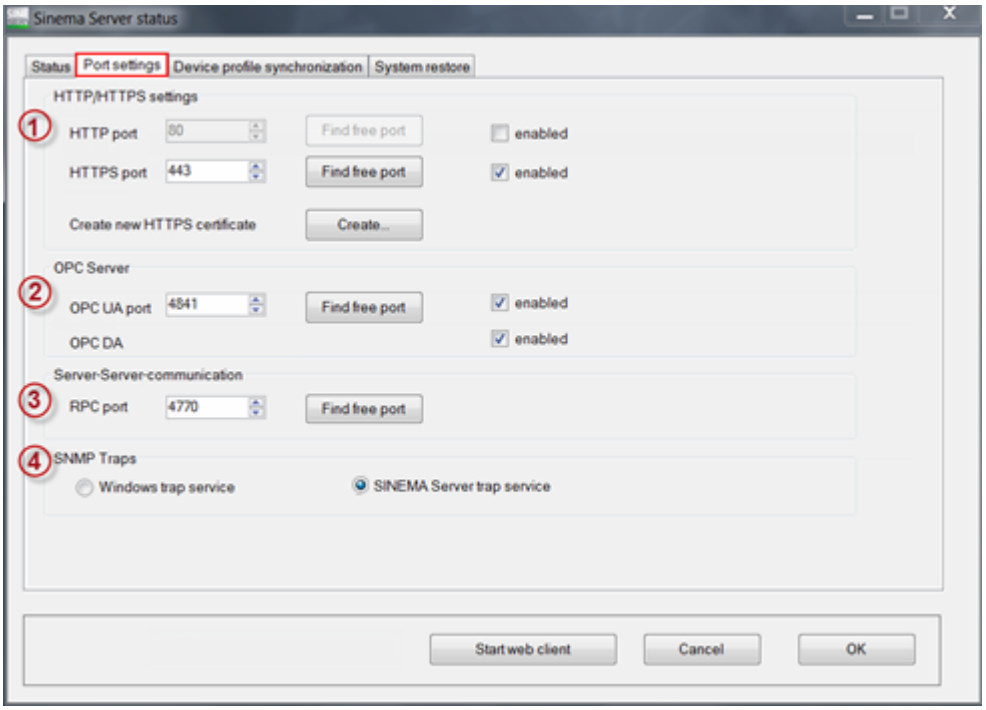


CAUTION	Avoid a forced shutdown or restart while SINEMA Server is running. This may damage the SINEMA Server database. As a result, the application no longer starts correctly. To avoid data loss in such situations, regularly back up the SINEMA Server configuration. If necessary, the backed up data can then be retrieved using the restore function. SINEMA Server features an automatic system backup function (“Job”) that is executed daily at 04:00 by default. You can change the automatic system backup settings.

© Siemens AG 2017 All rights reserved

3. Go to the “Port settings” tab. SINEMA Server uses various services for communication.
   This tab allows you to manually define the ports for the following connections and enable/disable SINEMA Server for this connection:

   - Connection using http or https (1)
   - Connection using OPC UA or OPC DA (2)
   - RPC connections (for checking device overall statuses of other SINEMA Server instances in the network) (3)
   - Use of SNMP trap service (4)



4. Customize the ports and settings to your environment or keep the default settings.
   If you have changed the SNMP trap settings, restart SINEMA Server using the “Status” tab.

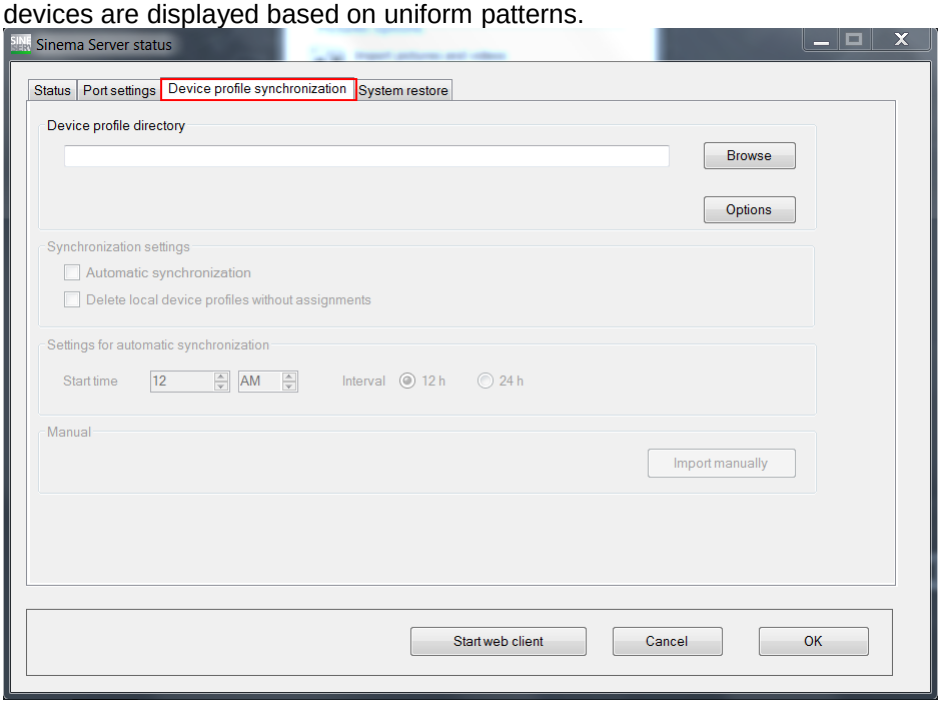
Note

If more than one SNMP application needs to receive traps, use the “SINEMA Server trap service” setting.
By default, you have to manually enable the Windows trap service in the Control Panel.

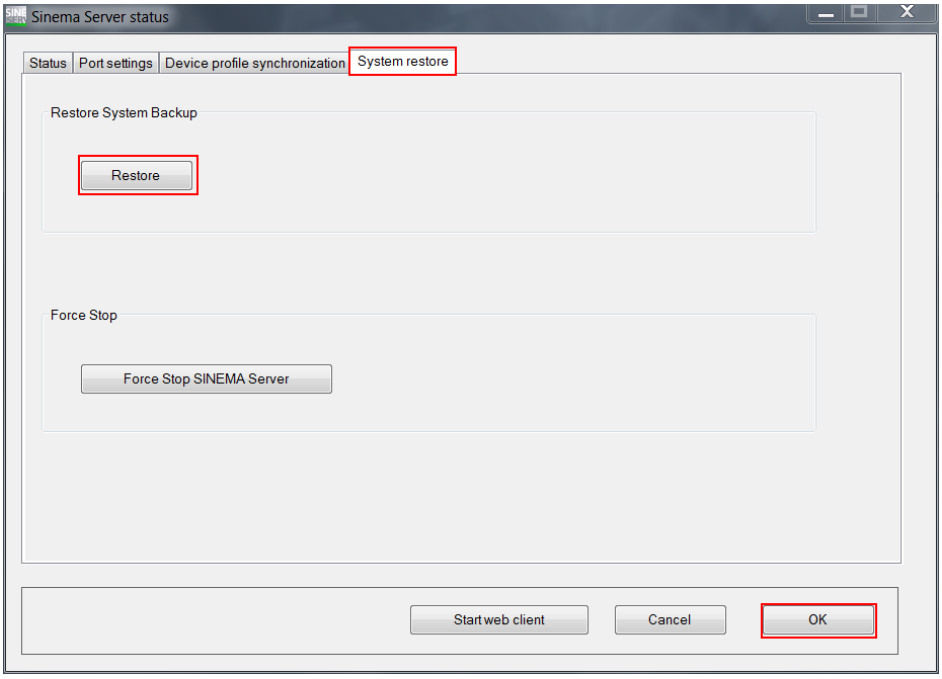
5. If you are using multiple SINEMA Server instances in your network, go to the “Device profile synchronization” tab. This tab provides the option to define a central file path for new device profiles or device profiles to be updated. Device profiles stored in this tab are automatically imported into the local SINEMA Server instance at a selectable time or after a selectable interval. With this function, all instances always use the same device profiles and the monitored

© Siemens AG 2017 All rights reserved

devices are displayed based on uniform patterns.



6. The “System restore” tab is used to restore system backups.
   If SINEMA Server can no longer be started correctly, the last created system backup is automatically restored or you can manually initiate a restore.
   Select “OK” to close SINEMA Server Monitor:



© Siemens AG 2017 All rights reserved

2.3 SINEMA WebClient

2.3.1 Valuable information on SINEMA WebClient

You access the management station using the Apache web server integrated in SINEMA Server. This allows you to directly use the SINEMA Server network monitoring software through a web browser from different client PCs.

You monitor the network using a web browser on the clients.

Web interface features

The SINEMA Server web interface can be simultaneously used by multiple clients to access network information. For each management station, SINEMA Server supports simultaneous remote access by ten users.

You can access the SINEMA Server web interface using an unencrypted HTTP connection or an encrypted HTTPS connection.

Options for login

To log in to the SINEMA Server web interface, you have the following options:

- On a client computer:
  In the browser's address bar, enter one of the following URL addresses:
  - http://<IP address of the SINEMA Server instance>
  - https://<IP address of the SINEMA Server instance>
- On the management station:
  - Use a web browser specifying the address http://localhost or https://localhost
  - Use the "Start Web client" function of SINEMA Server Monitor

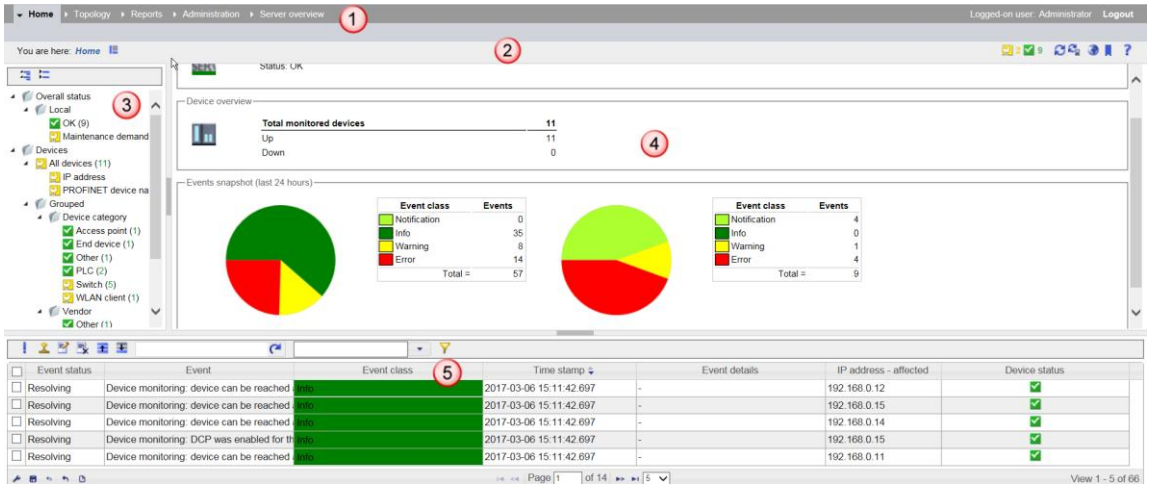
Note If you are using a port other than the HTTP default port 80, enter the port number along with the IP address. A colon " :" must be entered as a separator between the IP address and the port number, e.g.: http://192.168.0.1:8080. This rule also applies to the HTTPS default port 443.

© Siemens AG 2017 All rights reserved

The SINEMA Server user interface

The web user interface of SINEMA Server is divided into several areas, some of which are always visible and always have the same content type. These areas contain both general information and control elements for executing basic program actions.

The following figure shows the program window with its permanent areas and the main window for the specific views:



The following table shows the meaning of the numbers:

Table 2-1

No.	Area	Description
1	Navigation bar	The navigation bar allows you to access the individual program functions of SINEMA Server. The first row shows the main menu items. The second row displays its submenu commands depending on the menu item selected in the first row.
2	Status bar	The status bar consists of two sections: • The left area displays the menu branch you are currently in. • The right area of the status bar contains display and function elements.
3	Device tree	The device tree displays a grouped list of all devices that are monitored by SINEMA Server. The different groups are used for filtered display of the devices depending on the selected group topic.
4	Main window	Depending on the selected function, the main window contains specific views, for example the start window.
5	Event list	The event list displays network events that have occurred and system-related events.

© Siemens AG 2017 All rights reserved

SINEMA Server color scheme

SINEMA Server consistently uses a uniform color scheme to indicate device statuses or events.

The following table shows the colors and icons used:

Table 2-2

Icon	Meaning
	Device with the “Not reachable” status.
	Device with the “Maintenance demanded” status.
	Device with the “OK” status.
	Device with the “Not connected” status.
	Device with the “Fault” status.
	Device with the “Maintenance required” status.
	Event message with the “Error” event class.
	Event message with the “Information” event class.
	Event message with the “Warning” event class.

Possible monitoring statuses

SINEMA Server uses uniform icons to indicate the monitoring statuses of devices. The icons can be found in the “Active SIMATIC/PROFINET monitoring” tab.

The following table shows the icons used:

Table 2-3

Icon	Meaning
	The device is not monitored.
	The PROFINET IO device is monitored passively; this means it is monitored only by the SIMATIC-capable CPU assigned to the device.
	The device is monitored using ICMP / DCP / SNMP.
+	The device is monitored using ICMP / DCP / SNMP. Depending on whether the device is a PROFINET IO device or a SIMATIC-capable CPU, the following monitoring mode is additionally active: • PROFINET: PROFINET monitoring is active. • SIMATIC: SIMATIC monitoring is active.
++	The device is monitored using ICMP / DCP / SNMP. Depending on whether the device is a PROFINET IO device or a SIMATIC-capable CPU, the following monitoring modes are additionally active: • PROFINET: - PROFINET monitoring is active. - PROFINET collection of port statistics is active. • SIMATIC: - SIMATIC monitoring is active. - SIMATIC monitoring of the PROFINET IO devices assigned to the controller by the SIMATIC-capable CPU is active.

© Siemens AG 2017 All rights reserved

2.3.2 Using and customizing SINEMA WebClient

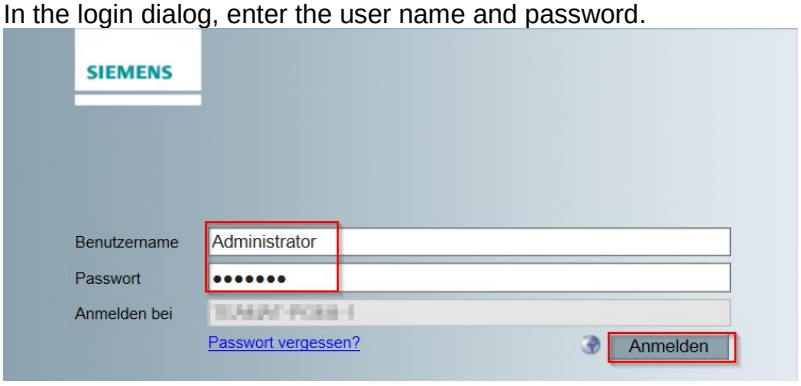
First login

To log in to the SINEMA Server web interface, proceed as follows:

1. Open a browser on a client computer or directly on the management station and enter one of the following addresses in the address bar:
   - Client computer:
     - http://<IP address of the management station>
     - https://<IP address of the management station>
   - Management station:
     - http://localhost
     - https://localhost

   You can also use the button in SINEMA Server Monitor.

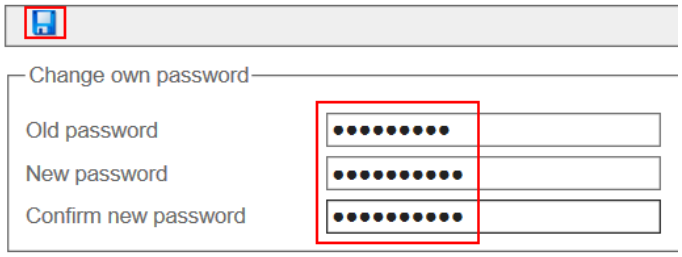
2. In the login dialog, enter the user name and password.



   When you log in for the first time, the default login data is as follows:

   - User name: “Administrator”
   - Password: “SinemaA”

3. When you have logged in to the system for the first time, you are prompted to change the initial password. Enter the old and new password. In “Confirm new password”, repeat the new password. Both entries must match.
   Save the new password.



© Siemens AG 2017 All rights reserved

4. If authentication is successful, you are given access to the SINEMA Server web interface.

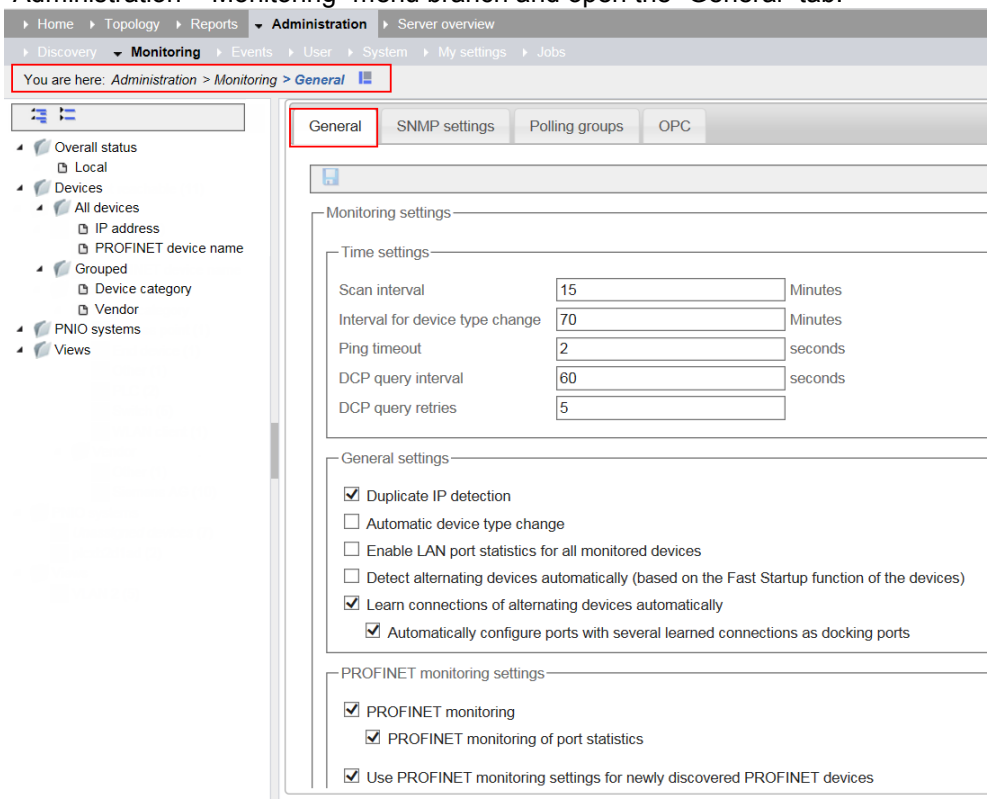
Result
The SINEMA Server user interface appears. In addition, the password for the “Administrator” user was changed after the first login. From now on, log in with the changed password.

Checking the monitoring settings

You have the option to define general parameters for monitoring in SINEMA Server. You can make the following settings:

- Time settings for the scan interval
- General settings such as Duplicate IP detection, Enable LAN port statistics for all monitored devices
- PROFINET monitoring settings
- SIMATIC monitoring settings

To view or change the general settings, use the navigation bar to go to the “Administration > Monitoring” menu branch and open the “General” tab.



It is recommended to disable automatic PROFINET monitoring for newly discovered devices in the “PROFINET monitoring settings” section.

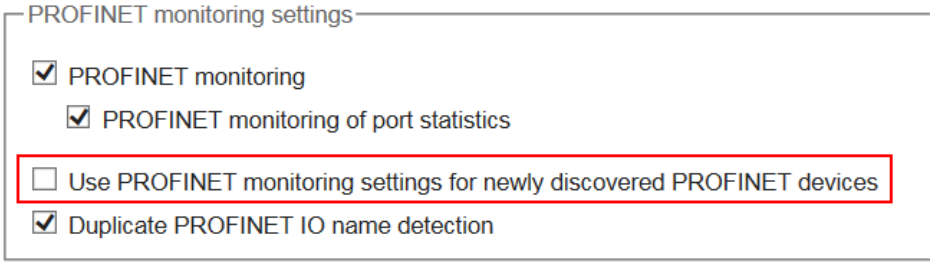
Note

You can manually enable PROFINET monitoring for the required devices at a later stage (see Chapter 4.1.3).

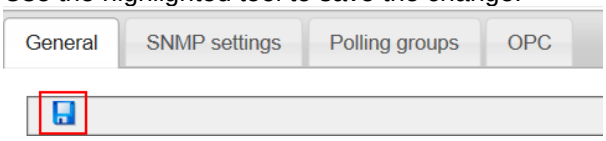
© Siemens AG 2017 All rights reserved

To do this, proceed as follows:

1. Uncheck “Use PROFINET monitoring settings for newly discovered PROFINET devices”.



2. Use the highlighted tool to save the change.



Checking the SNMP settings

SINEMA Server detects the devices using, among other things, SNMP. For correct, successful device discovery, the SNMP settings in the network devices and in SINEMA Server must match.

By default, the following SNMP settings are available and enabled in SINEMA Server:

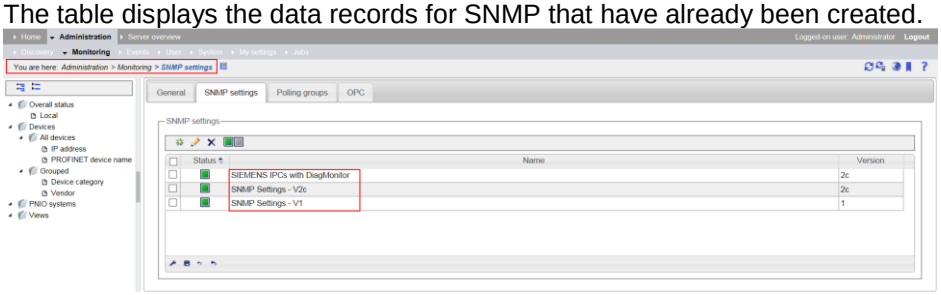
- SNMP v1 (read: public/ write: private)
- SNMP v2c (read: public/ write: private)

If there are differences between the devices and SINEMA Server regarding SNMP, you can change the SNMP settings in the devices or in SINEMA Server.

To change the SNMP settings of SINEMA Server, proceed as follows:

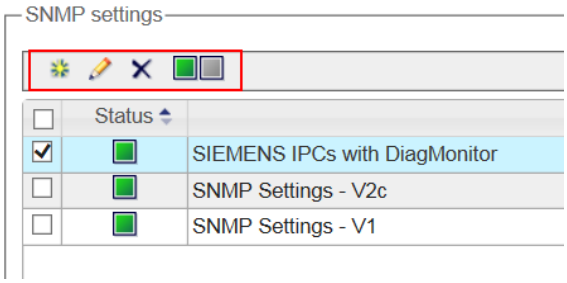
1. Use the navigation bar to go to the “Administration > Monitoring” menu branch and open the “SNMP settings” tab.

   The table displays the data records for SNMP that have already been created.



© Siemens AG 2017 All rights reserved

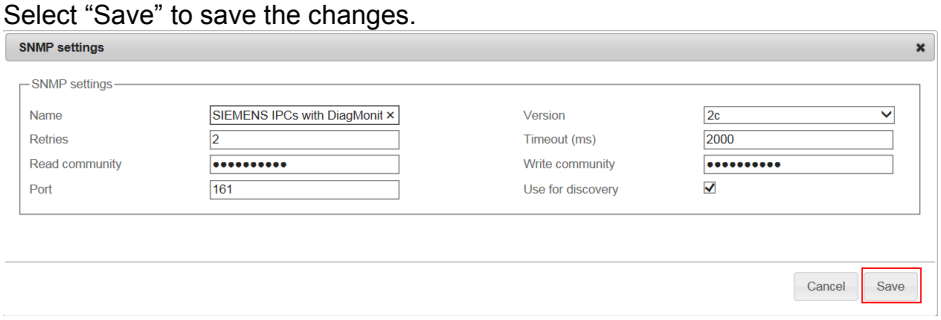
2. From the list, select the data record to be modified.



The function elements in the header allow you to change the data record or create a new data record.

Element	Description
	Create new data record for SNMP settings
	Delete SNMP settings
	Change SNMP settings
	Change status of selected (✓) SNMP settings

3. Depending on the SNMP version used (1, 2c or 3), other windows open when creating or changing a data record. In these windows, you can enter the parameters of this version such as group name and user name.
Select “Save” to save the changes.



Note

It is recommended to use SNMPv3 as this SNMP version has significantly improved security mechanisms:

- Protection against unauthorized access, i.e., check of the message’s authenticity
- Protection against data modification, i.e., check to see whether the message has been tampered with
- Protection against unauthorized interception

© Siemens AG 2017 All rights reserved

3 Discovering Devices in the Network

3.1 Valuable information on device discovery

The basic requirement for setting up network monitoring in SINEMA Server is the network scan for device discovery.

Time of the scan

The network is scanned at the following times:

- After starting SINEMA Server for the first time by pressing a button
- If required by pressing a button
- Automatically in appropriately configured cycles.

Scan characteristics

Device discovery in the network triggers the following in SINEMA Server:

1. Depending on the configuration in SINEMA Server, either all devices discovered by DCP (Discovery and Configuration Protocol) and/or, using ICMP, devices in specified IP address ranges are detected during the first scan.
   - The found devices are listed in the device list as a table.
   - Information about the interfaces of the detected devices is collected in the interface list.
   - The detected topology graphically represents the detected connections.

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

3. Based on the discovery rules in the profile data, the devices are assigned to a suitable device profile. Devices that cannot be assigned are assigned to the available default profiles (see Chapter 4.2).

4. From then on, all discovered devices are monitored in SINEMA Server.

5. If changes such as adding new devices and/or removing devices have occurred in your network, these changes are detected with a new network scan.
   If new devices have been added, the device list, the interface list and the topology are updated.
   Removed devices are no longer displayed in the device and interface list and in the topology display.

© Siemens AG 2017 All rights reserved

3.2 Preparing and starting device discovery

Before starting the scan for the first time, make the following settings:

- Customize the IP address range to minimize the device scan time
- Select the network adapter used
- Set the options

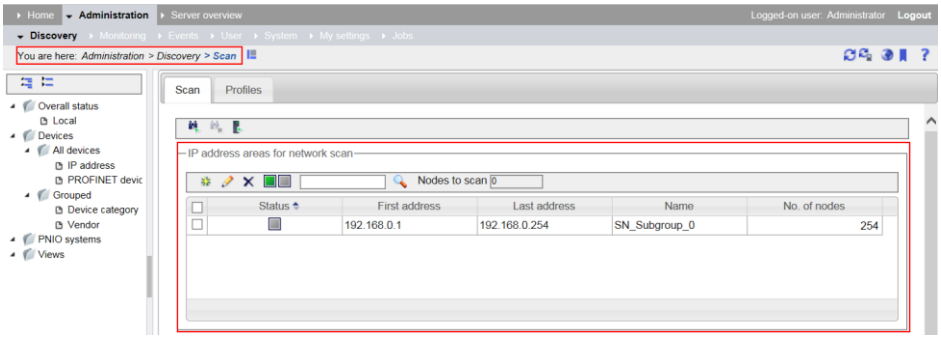
Use the “Administration > Discovery” menu command in the “Scan” tab to make all of the above settings.

Setting the scan range

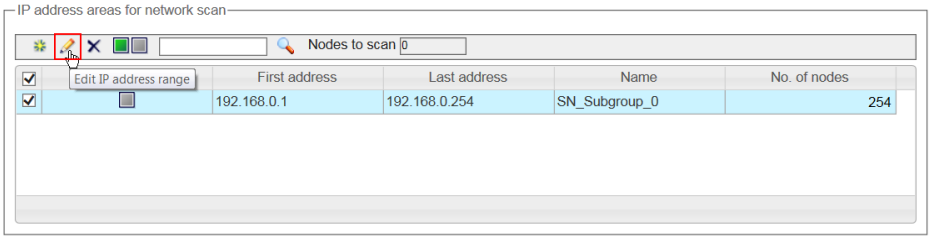
Limit the scan range to the monitored devices. To do this, it is advisable to divide the IP address range into smaller subgroups if the IP addresses are not consecutive. This division speeds up the device scan.

To set up the scan range, proceed as follows:

1. In the “Scan” tab, go to the “IP address areas for network scan” section.
   An IP address range has already been created based on the management station’s IP address.

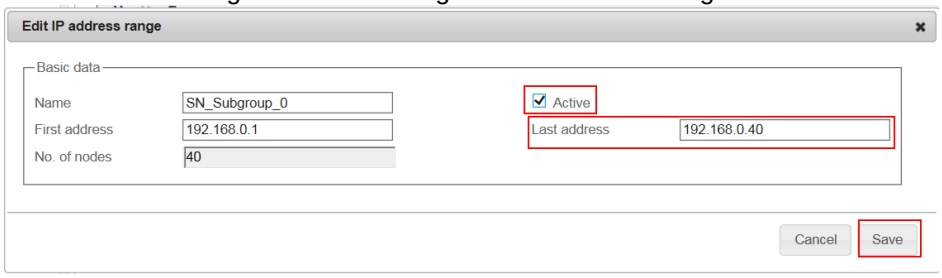


2. Select the item and use the highlighted tool to edit the IP address range.



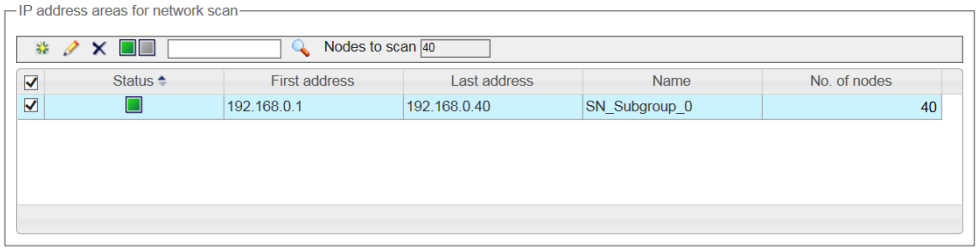
© Siemens AG 2017 All rights reserved

3. Limit the IP address range as required for your reference system and enable this IP address range for the following scan. Save the changes.



Result

The IP address range has been customized to your environment and is enabled.



Enabling the network adapter for the device scan using DCP

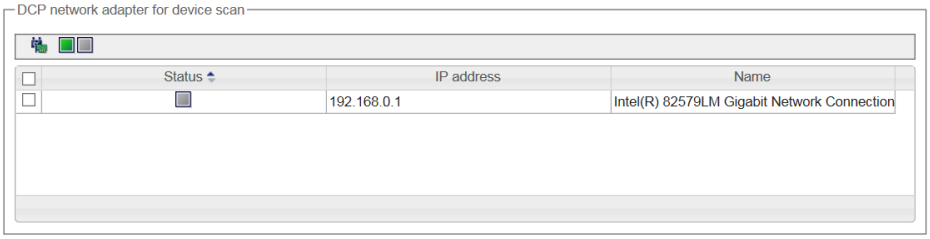
The next step is to select the network adapter of your management station. Using this network adapter, the network is scanned using DCP and then monitored.

Note The selected network adapter has no influence on where – on which network adapters – the IP address ranges are scanned.

Proceed as follows:

1. Go to the “DCP network adapter for device scan” section.

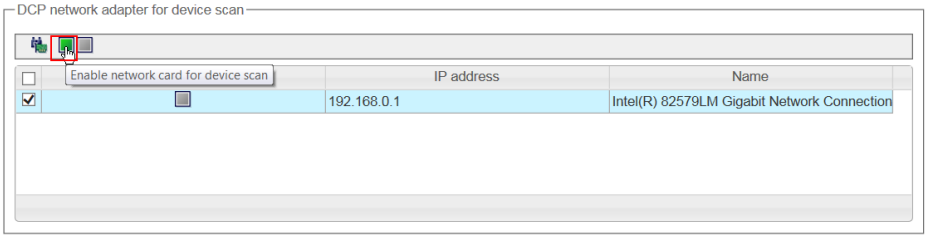
   The table displays all network adapters that are located on the management station and active.



© Siemens AG 2017 All rights reserved

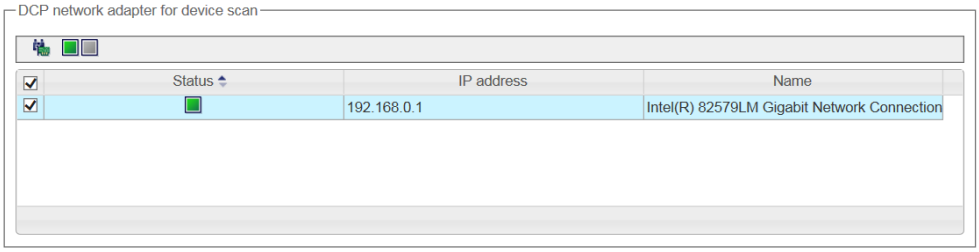
2. If no entry is visible in the table, connect your network interface to your network and select the “Scan for network adapters” function.

3. From the table, select the network adapter to be used for the scan using DCP. Use the “Enable network card for device scan” function to enable the network adapter.



Result

The network adapter is enabled for DCP discovery and monitoring.



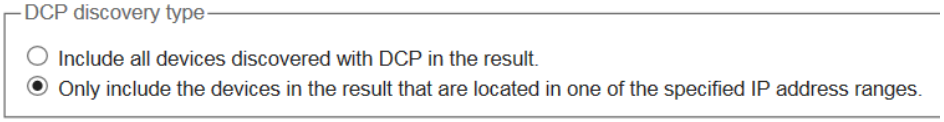
© Siemens AG 2017 All rights reserved

Setting the options

The last step is to set the device discovery options.

1. You can choose between two DCP discovery types:
   - “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”

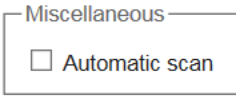
   Select the “Only include the devices in the result that are located in one of the specified IP address ranges” DCP discovery type.

Note If you select the “Include all devices discovered with DCP in the result” option in the DCP scan settings, it is possible that DCP devices are discovered that are outside the defined IP address ranges but within the subnets connected to the network adapters.

2. As an additional option, you can set the scan mode. The following options are available:
   - Automatic scan
   - Manual scan when starting for the first time or as required

   Uncheck “Automatic scan” to start a scan manually.

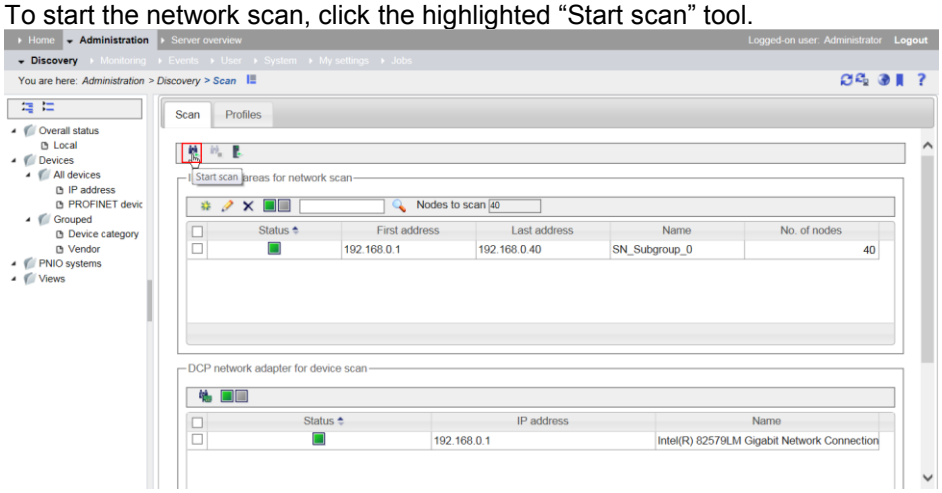
Note If you check “Automatic scan”, the “Administration > Monitoring” menu, “General” tab, allows you to set the time interval for automatic network scans.

© Siemens AG 2017 All rights reserved

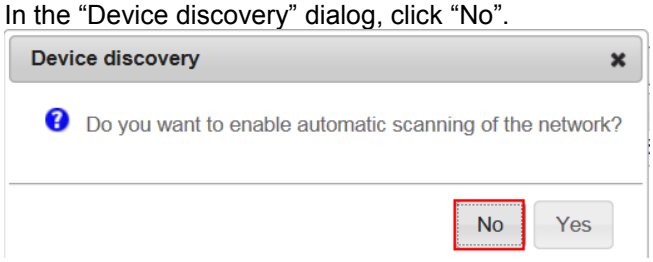
Starting device discovery

To start the network scan, proceed as follows:

1. To start the network scan, click the highlighted “Start scan” tool.



2. In the “Device discovery” dialog, click “No”.

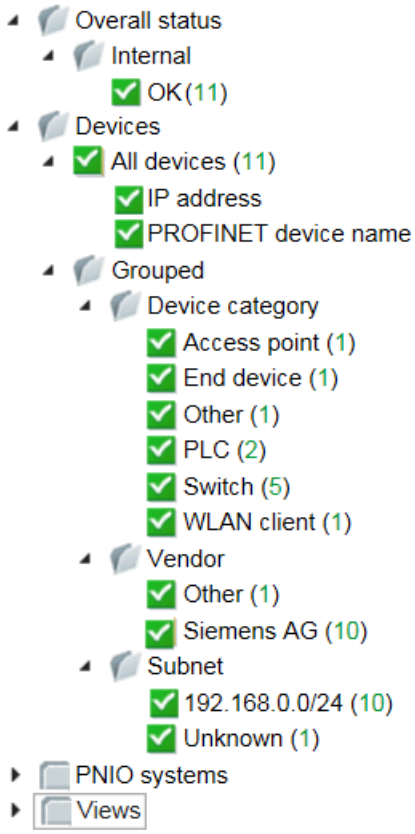


3. The network is scanned based on the scan ranges for the subnets. The scanning progress is indicated by an icon in the right section of the status bar.

© Siemens AG 2017 All rights reserved

Result

When scanning is complete, all discovered network devices, including their status, are displayed in the device lists that can be selected in the device tree.



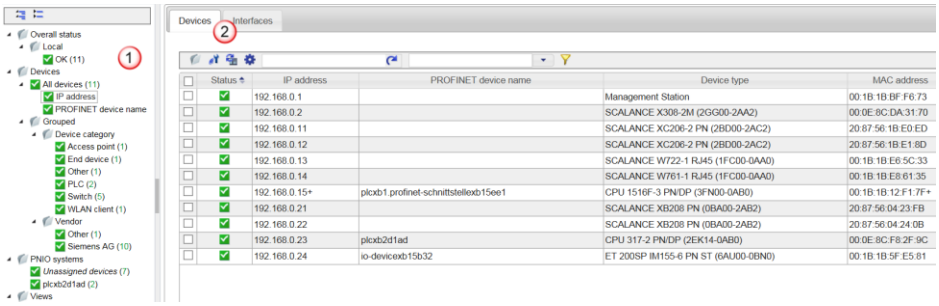
© Siemens AG 2017 All rights reserved

4 Managing and Customizing Devices

4.1 Device management

4.1.1 Valuable information on device management

When scanning is complete, all discovered network devices, including their status, are displayed in the device lists that can be selected in the device tree.



The following table shows the meaning of the numbers:

Table 4-1

No.	Area	Description
1	Device tree	The device tree displays a grouped list of all devices that are monitored by SINEMA Server. The different groups are used for filtered display of the devices depending on the selected group topic.
2	Device list	The device list lists devices that are part of the selected group topic in the device tree.

Device tree

The device tree groups all devices that were discovered after a scan.

Selecting a device group generates a filtered device list that is displayed in the “Devices” tab in the device window.

- The “Overall status > Local” group filters the devices by their overall status, e.g. “OK”.
- The “Devices” group generates a display filtered by device property.
- The “PNIO systems” group displays only devices that are part of the selected PNIO system.

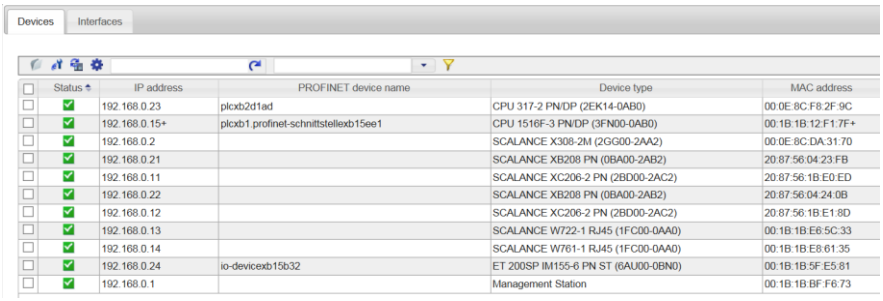
The icons for the overall status always show the worst current status of one of the device nodes included in the branch.

© Siemens AG 2017 All rights reserved

Device list

Selecting an item in the device tree opens the SINEMA Server device lists. In the device window, the “Device” tab is always the default tab.

Depending on the item selected in the device tree, the device list displays all devices or only a certain group.



Status	IP address	PROFINET device name	Device type	MAC address
✓	192.168.0.23	plcxb2d1ad	CPU 317-2 PN/DP (2EK14-0AB0)	00:0E:8C:F8:2F:9C
✓	192.168.0.15+	plcxb1.profinet-schnittstellexb15ee1	CPU 1516F-3 PN/DP (3FN00-0AB0)	00:1B:1B:12:F1:7F+
✓	192.168.0.2		SCALANCE X308-2M (2GG00-2AA2)	00:0E:8C:DA:31:70
✓	192.168.0.21		SCALANCE XB208 PN (0BA00-2AB2)	20:87:56:04:23:FB
✓	192.168.0.11		SCALANCE XC206-2 PN (2BD00-2AC2)	20:87:56:1B:E0:ED
✓	192.168.0.22		SCALANCE XB208 PN (0BA00-2AB2)	20:87:56:04:24:0B
✓	192.168.0.12		SCALANCE XC206-2 PN (2BD00-2AC2)	20:87:56:1B:E1:8D
✓	192.168.0.13		SCALANCE W722-1 RJ45 (1FC00-0AA0)	00:1B:1B:E6:5C:33
✓	192.168.0.14		SCALANCE W761-1 RJ45 (1FC00-0AA0)	00:1B:1B:E8:61:35
✓	192.168.0.24	io-devicexb15b32	ET 200SP IM155-6 PN ST (6AU00-0BN0)	00:1B:1B:5F:E5:81
✓	192.168.0.1		Management Station	00:1B:1B:BF:F6:73

Device lists are divided into several columns that display the device-specific data. With the exception of the first column that is used to select rows, you can select and customize the contents of any other column as required.

Device list functions

The device window provides a toolbar with functions. You can use these functions for a device selected in the device list.

This includes the following functions:

- Show device details for the selected device
- Open Web Based Management
- Reread device data
- Add comments
- Enable/disable monitoring
- Manually add new device
- Delete device
- Change device type

For a detailed description and list, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.1 (see \4\, Chapter 7.2).

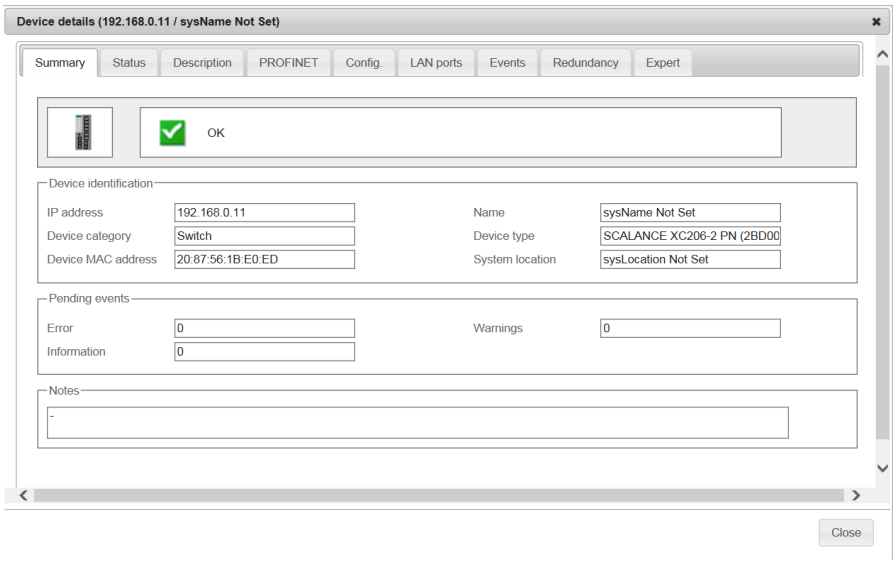
Device details

You can view detailed device information for each device in the device list. The window with the specific device details can be opened:

- In the device window
  - Using the appropriate icon in the toolbar
  - By double-clicking the appropriate item in the device list
- In the topology view
  - Using the context menu of the device
  - By double-clicking the device icon

© Siemens AG 2017 All rights reserved

The “Device details” window consists of several tabs that display the data of a device in a detailed manner, grouped or as a list.



Which tabs are displayed depends on the specific device type.

4.1.2 Customizing the device list

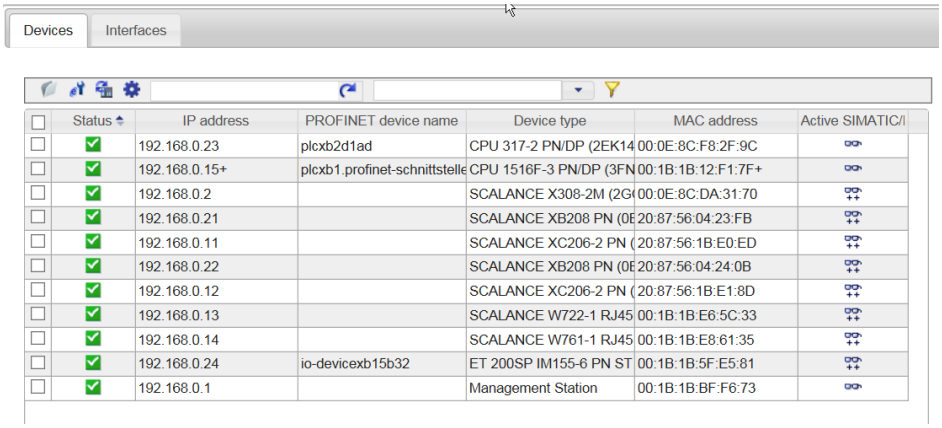
The device list provides you with a table of device-specific data of the monitored devices such as status, IP address, MAC address. Each column is assigned to a specific piece of device information.

The tools in the footer allow you to design the entire table as required. You can make the following changes:

- Add columns with more information
- Remove existing columns
- Change column width

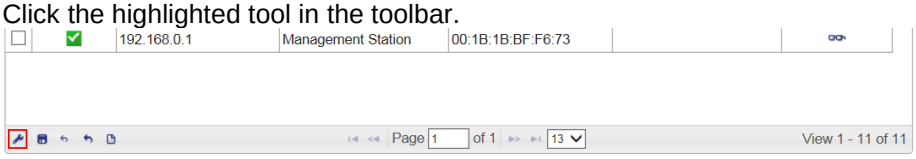
To customize the device list, proceed as follows:

1. In the device tree, select the device group whose device list you want to customize, for example all devices with the “OK” status.
   The device window displays the filtered device list.



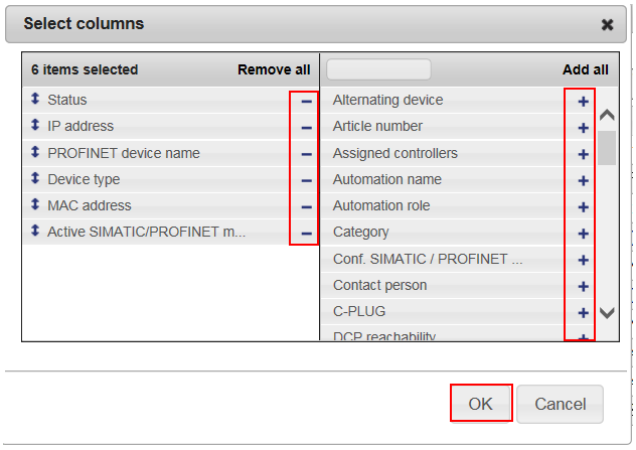
© Siemens AG 2017 All rights reserved

2. Click the highlighted tool in the toolbar.

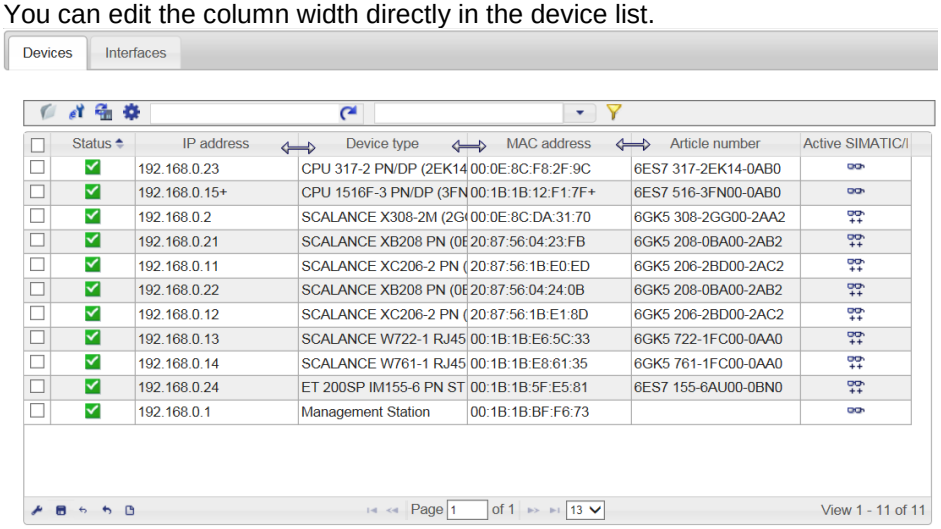


3. The window for selecting columns opens. It consists of the following parts:
   - In the left part, you can see the columns that have already been displayed.
   - In the right part, you can see the columns that are still free.

   Use the minus sign ("-") to remove existing columns and/or use the plus sign ("+") to add new columns.
   Using drag and drop, you can change the column sorting.
   Select "OK" to close the window.

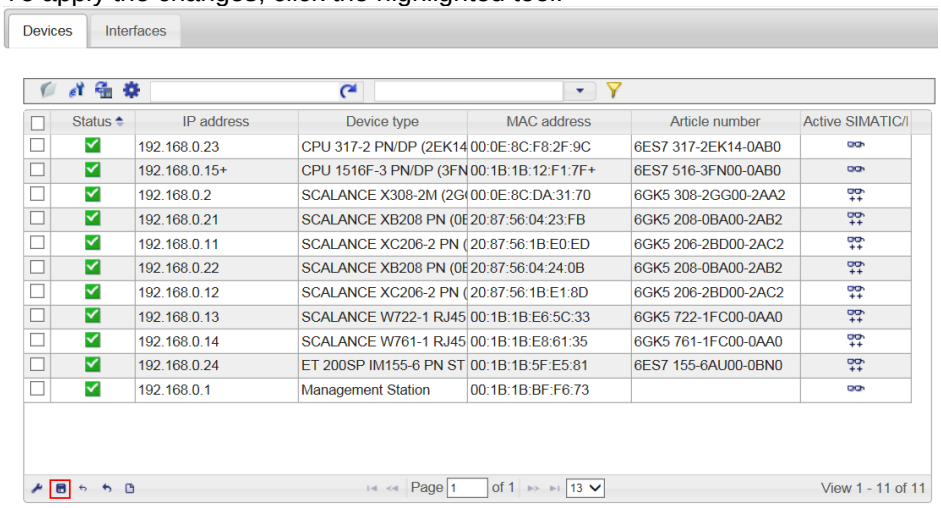


4. You can edit the column width directly in the device list.

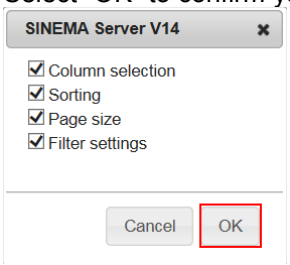


© Siemens AG 2017 All rights reserved

5. To apply the changes, click the highlighted tool.



6. In the next window, you can select the changes that will be applied to SINEMA Server.
   Select “OK” to confirm your selection.



7. If you want to customize more device lists, repeat steps 1 through 6.

Result
The modified device list appears in the device window.

© Siemens AG 2017 All rights reserved

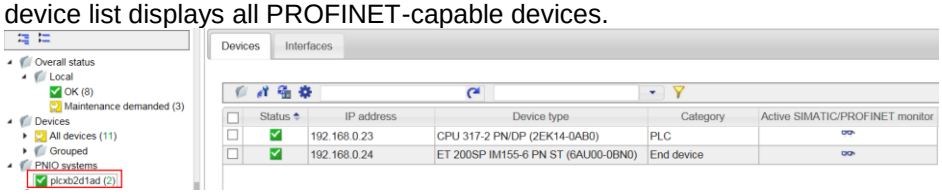
4.1.3 Manually enabling device monitoring

You can manually enable the following monitoring settings specifically for selected devices:

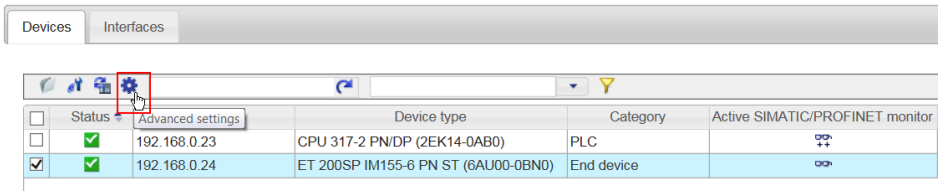
- PROFINET monitoring for PROFINET devices
- SIMATIC monitoring for SIMATIC S7-300/S7-400/ET 200 CPUs

To manually enable PROFINET monitoring, proceed as follows:

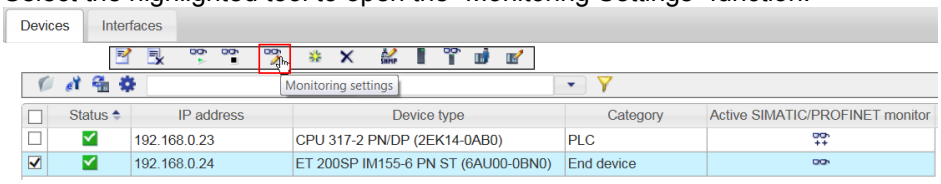
1. In the device tree, select the device list for available PROFINET devices. The device list displays all PROFINET-capable devices.



2. Select an item with a PROFINET-capable device, for example the ET 200SP of the reference system from this document. Open the highlighted tool to show more functions in the toolbar.

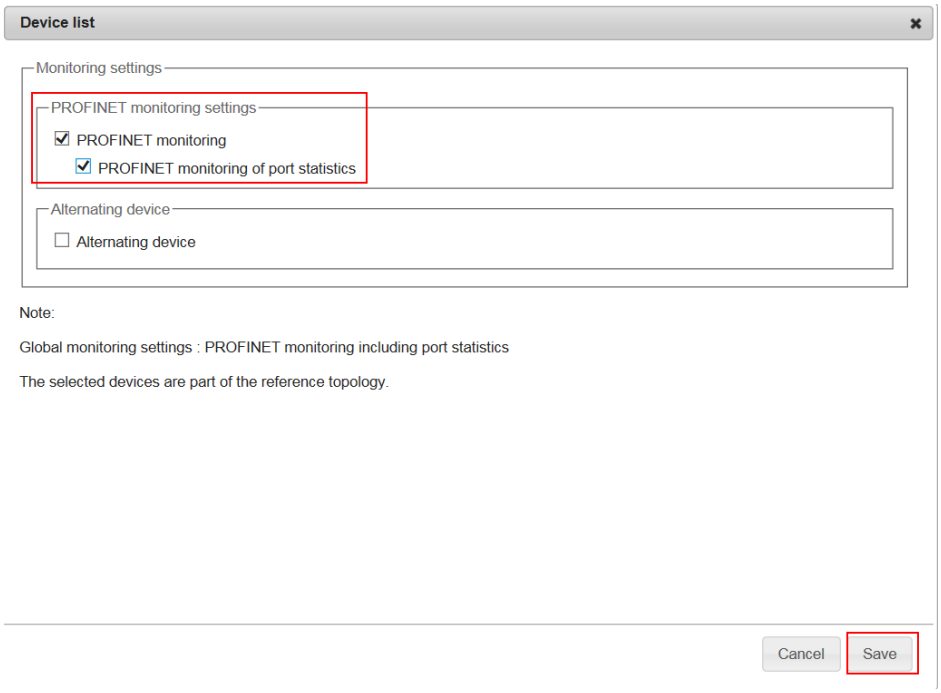


3. Select the highlighted tool to open the “Monitoring Settings” function.



© Siemens AG 2017 All rights reserved

4. In “Monitoring settings”, check “PROFINET monitoring”. To apply the change, click the “Save” button.



Note

You can only enable local PROFINET monitoring manually if you have enabled global PROFINET monitoring in the “Administration > Monitoring” menu.

Result

PROFINET monitoring of the PROFINET IO device by SINEMA Server is active. The icon in the “Active SIMATIC/PROFINET monitoring” column is displayed with glasses and two plus signs. The first plus sign indicates that PROFINET monitoring is active. The second plus sign indicates that PROFINET monitoring of port statistics is active.

	Status	IP address	Device type	Category	Active SIMATIC/PROFINET monitor
		192.168.0.23	CPU 317-2 PN/DP (2EK14-0AB0)	PLC	
		192.168.0.24	ET 200SP IM155-6 PN ST (6AU00-0BN0)	End device	

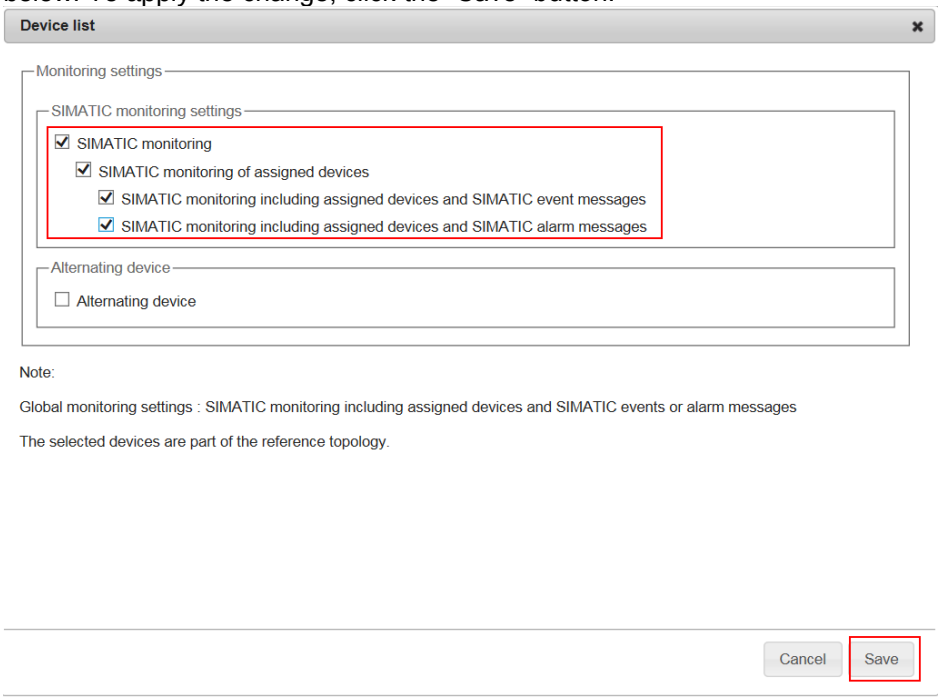
© Siemens AG 2017 All rights reserved

To manually enable SIMATIC monitoring, proceed as follows:

1. In the device tree, select the device list for available PROFINET devices. The device list displays all PROFINET-capable devices.

2. Select an item with a PROFINET controller, for example the S7-300 CPU of the reference system from this document. Open the highlighted tool in the toolbar to show more functions. Select the “Monitoring Settings” function.

3. In “Monitoring settings”, check “SIMATIC monitoring” and all the check boxes below. To apply the change, click the “Save” button.



Note

You can only enable local SIMATIC monitoring manually if you have enabled global SIMATIC monitoring in the “Administration > Monitoring” menu.

© Siemens AG 2017 All rights reserved

Result

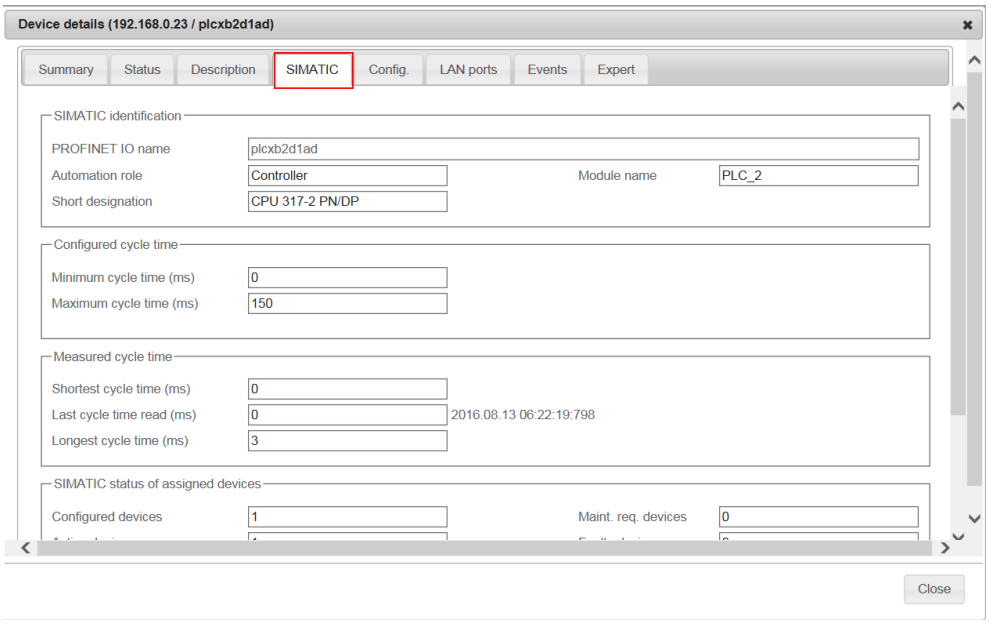
SIMATIC monitoring

- of the SIMATIC-capable CPU by SINEMA Server is active.
- of the PROFINET IO devices assigned to the controller by the SIMATIC-capable CPU is active.

The icon in the “Active SIMATIC/PROFINET monitoring” column is displayed with glasses and two plus signs. The first plus sign indicates that SIMATIC monitoring is active. The second plus sign indicates that SIMATIC monitoring of port statistics is active.

	Status	IP address	Device type	Category	Active SIMATIC/PROFINET monitor
☐	✅	192.168.0.23	CPU 317-2 PN/DP (2EK14-0AB0)	PLC	
☐	✅	192.168.0.24	ET 200SP IM155-6 PN ST (6AU00-0BN0)	End device	

In the device details, a new tab, “SIMATIC”, is active. This tab allows you to view more information such as cycle time, SIMATIC event messages and SIMATIC alarm messages.



© Siemens AG 2017 All rights reserved

4.2 Device profiles

4.2.1 Valuable information on device profiles

Profiles give SINEMA Server flexibility during device discovery, device monitoring and device display. They describe one or more device types that have common properties.

Profile management

During device discovery, SINEMA Server uses SNMP to determine details about newly discovered devices such as system hardware type, firmware version, article number.

Based on this SNMP data, the first step performed by SINEMA Server is to select, for the device, the profile with suitable discovery rules from the profile database. In the second step, SINEMA Server determines the suitable device type within the selected profile and uses the icon defined here for the display.

If no suitable profile is found for a network device during the network scan, SINEMA Server assigns a default profile to this device.

The assigned profile is used to classify and represent the network device.

Using default profiles

If an assignment based on the discovery rules of profiles is not possible when discovering a device, SINEMA Server assigns a default profile to this device that has not been uniquely identified:

- If the device ID indicates that the device is a Siemens device, the “SIEMENS_Standard” profile is used.
- If the device cannot be assigned as a Siemens device, a default profile is assigned based on the protocols supported by the device, e.g. “DEFAULT_SNMP_DCP_Device”.

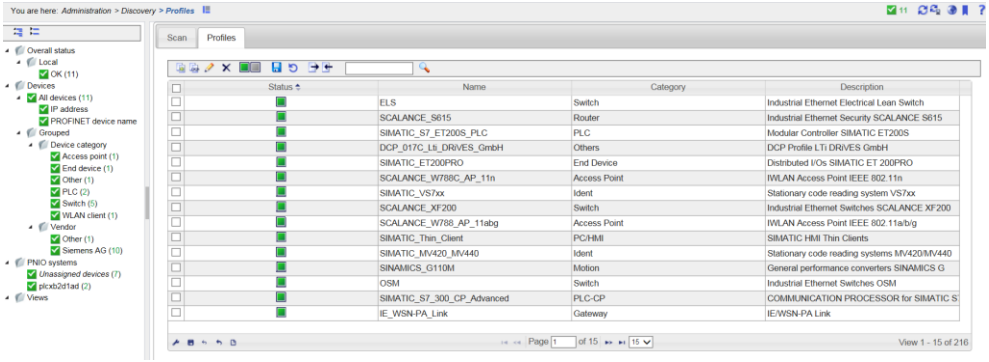
You can manually assign a profile to a device with a default profile. You can do the following:

- Assign the new device type to an existing profile.
- Create a new profile and store the new device type in this profile.
  New profiles are always created based on existing profiles.

© Siemens AG 2017 All rights reserved

Profile database

The profiles of the SINEMA Server profile database are listed in the “Profiles” tab. To go to this list, select the “Administration > Discovery” menu command.

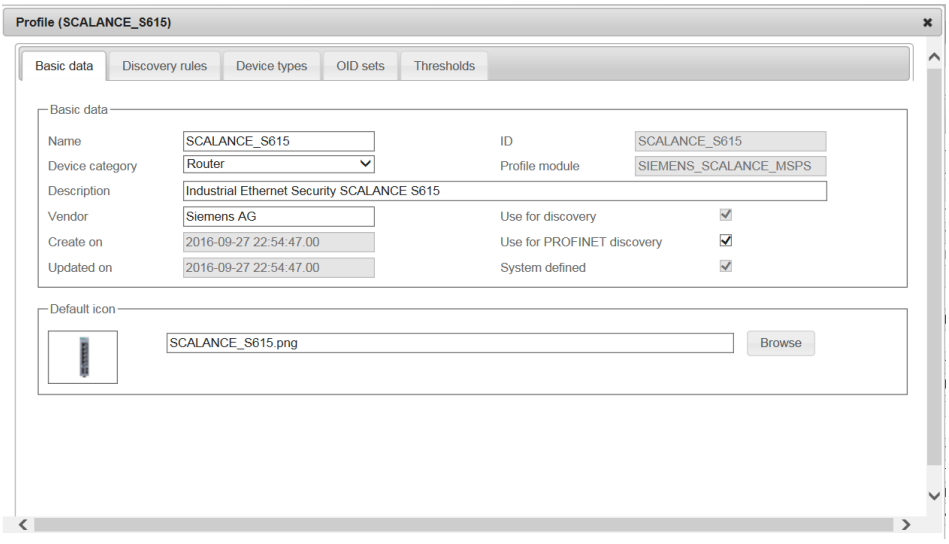


Profile details

You can view detailed information for each profile in the profile database. The window with the profile details can be opened:

- Using the appropriate icon in the toolbar
- By double-clicking the appropriate item in the device list

The “Profile details” window consists of several tabs that display the stored profile data in a detailed manner, grouped or as a list.



© Siemens AG 2017 All rights reserved

Profile database functions

The profile database provides a toolbar with functions. You can use these functions for a selected profile.

This includes the following functions:

- Create new profile
- Create monitoring profile
- Edit profile
- Delete profile

For a detailed description and list, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.4.2 (see \4\, Chapter 7.2).

© Siemens AG 2017 All rights reserved

4.2.2 Creating, changing and assigning profiles

Creating a new profile

The following instructions show you how to monitor a previously unknown device using SINEMA Server. A “Brother” printer is used as an example of the unknown device. Create a new profile to make the printer known to SINEMA Server.

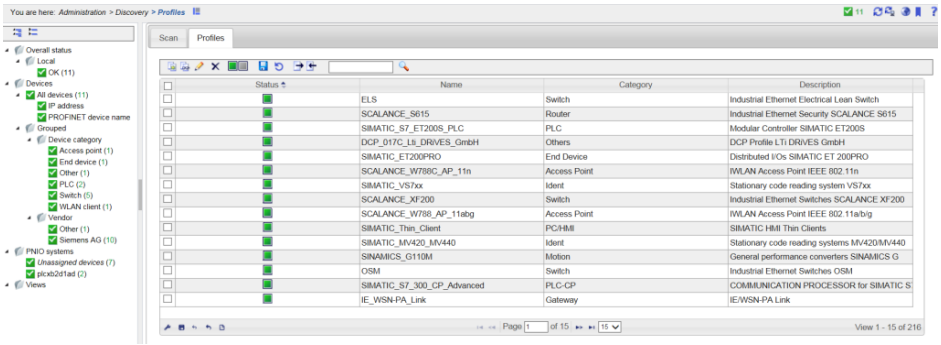
When you create a profile for a new device, you first need more detailed information about the device. This information includes:

- How can you identify the device?
- Does the device support the Automation MIB or can the I&M data be read elsewhere?
- Are there useful values you can monitor?
- Can you determine the status of the device?

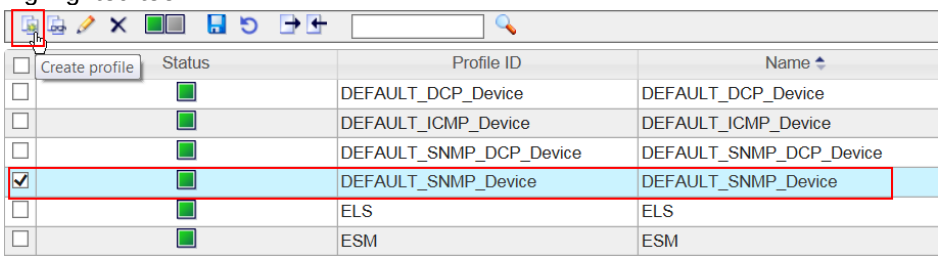
When creating a new profile, you always use an existing one. This existing profile therefore forms the basis of your new profile. As a basis for the Brother profile, use the “DEFAULT_SNMP_Device” default profile. This default profile is the best possible basis as the printer supports only SNMP.

To create a new profile, proceed as follows:

1. Select the “Administration > Discovery” menu command to open the “Profiles” tab.

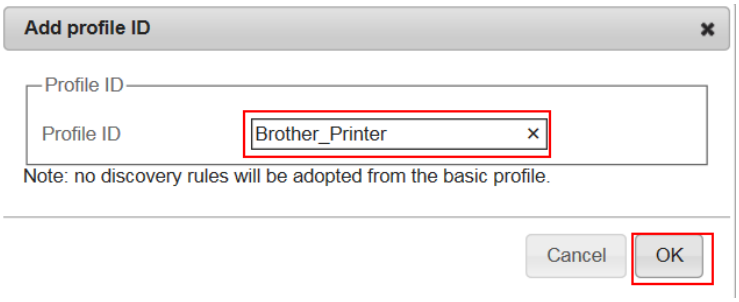


2. From the list, select the profile that is the most favorable basis for your new profile. For the Brother printer example, the “DEFAULT_SNMP_Device” default profile is the best possible choice.
   Select the “DEFAULT_SNMP_Device” profile. To create a new profile, click the highlighted tool.



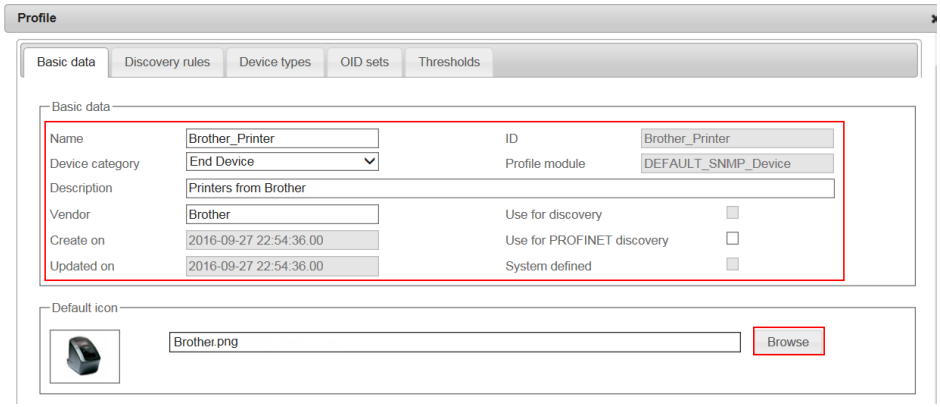
© Siemens AG 2017 All rights reserved

3. This opens the “Add profile ID” dialog. Assign a unique “Profile ID”. This name is used globally in SINEMA Server as the profile ID. Select “OK” to confirm the name.

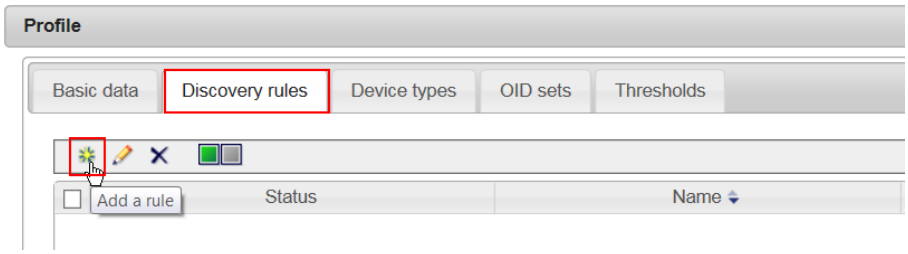


4. The Profile editor opens. You can enter data for the new profile. In the “Basic data” tab, define the following parameters:
   - Name of the profile
   - Device category
   - Vendor
   - Device icon
   - PROFINET discovery

   For a detailed description of the input options, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.4.2 (see \4\, Chapter 7.2).

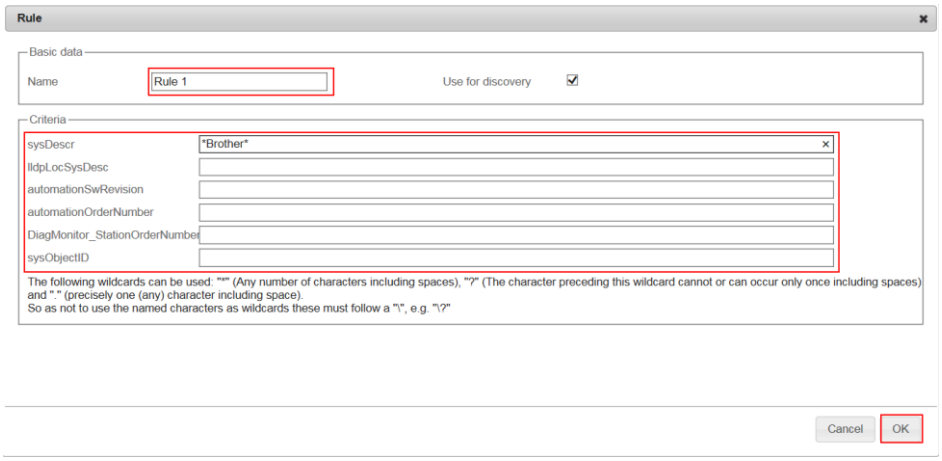


5. Go to the “Discovery rules” tab. In this tab, you define strings that are used to discover the new device family.
   To add a new rule, click the highlighted tool.



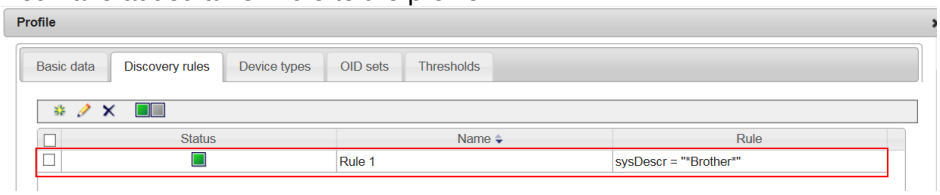
© Siemens AG 2017 All rights reserved

6. A new dialog appears. Define the discovery criteria in the appropriate fields. Select the strings such that all associated devices are discovered while no unwanted devices can be assigned to the profile.
   For a detailed description of the input options, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.4.2 (see \4\, Chapter 7.2).
   Click “OK” to close the dialog.

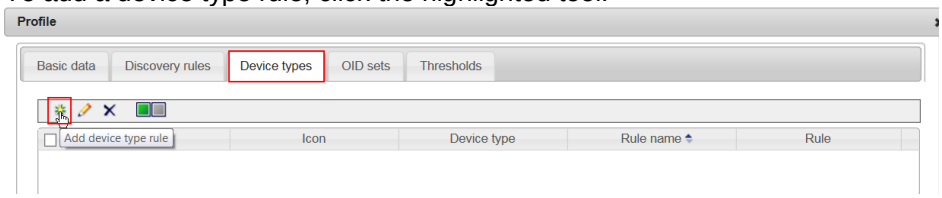


Result

You have added a new rule to the profile.

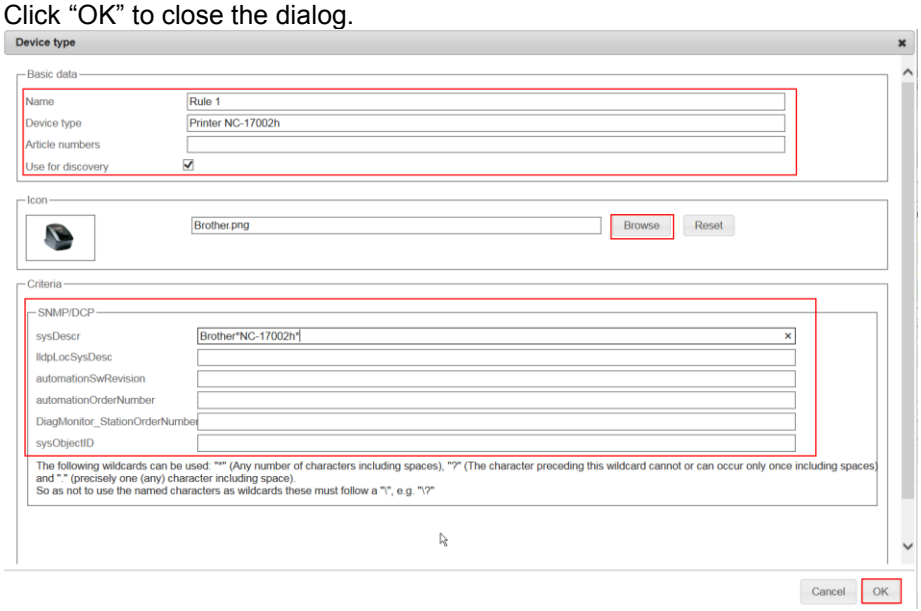


7. If an applicable profile was found for the found device, the second step tries to determine the correct device type.
   To specify single device types within the profile, go to the “Device types” tab.
   To add a device type rule, click the highlighted tool.



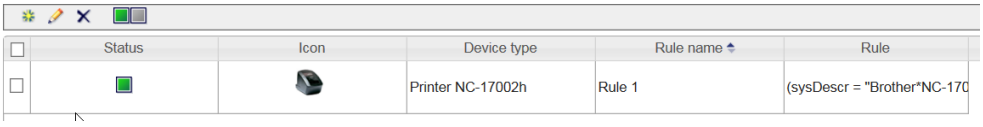
© Siemens AG 2017 All rights reserved

8. The Device type editor opens. Define the discovery criteria for the device type in the appropriate fields.
   For a detailed description of the input options, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.4.2 (see \4\, Chapter 7.2).
   Click “OK” to close the dialog.

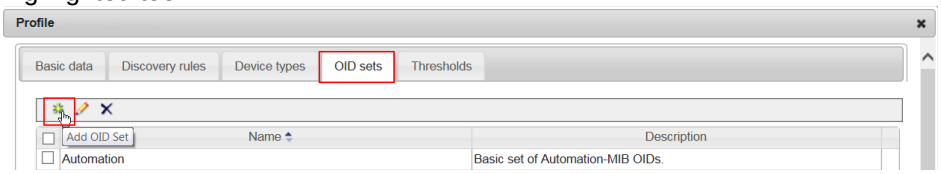


Result

You have added a new device type rule for the new printer device, “Brother NC-17002h”.

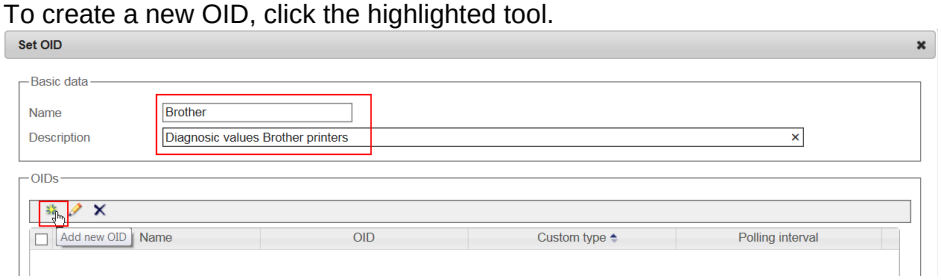


9. SINEMA Server tries to read the I&M data such as firmware version, order number, serial number in the Automation MIB. As the printer does not support this MIB, a new OID set has to be created.
   To do this, go to the “OID sets” tab. To create a new OID set, click the highlighted tool.



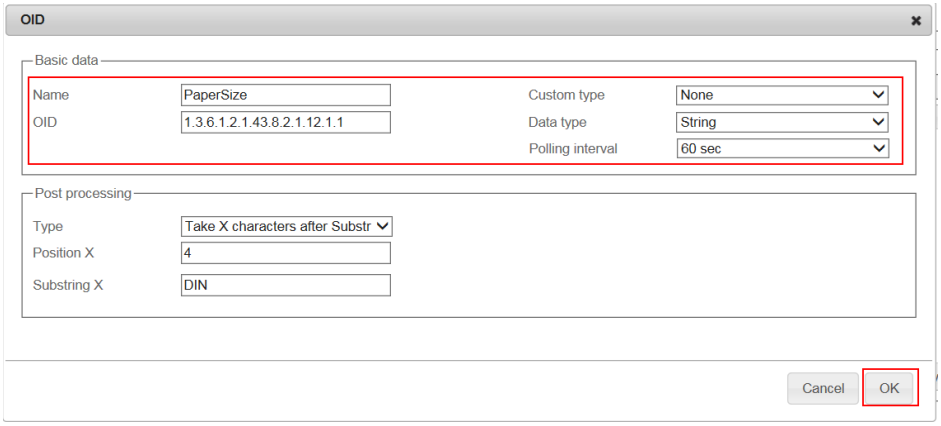
© Siemens AG 2017 All rights reserved

10. Enter a name and, optionally, a description of the new OID set.
    To create a new OID, click the highlighted tool.



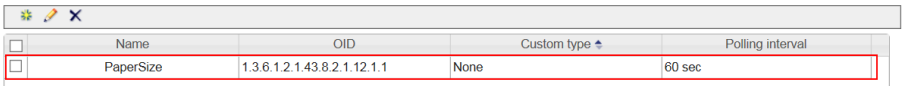
11. The OID editor opens. The following example creates an OID to display the currently set paper size.
    In the dialog's input fields, enter the following data:
    - Enter a name for the OID, for example PaperSize.
    - Enter the associated OID.
    - From the "Data type" drop-down list, select the data type that matches your OID.
    - If you select the "String" data type, the "Post processing" section allows you to define rules to edit the string, for example: use only the four characters following the "DIN" string.

    Click "OK" to close the dialog.



Result

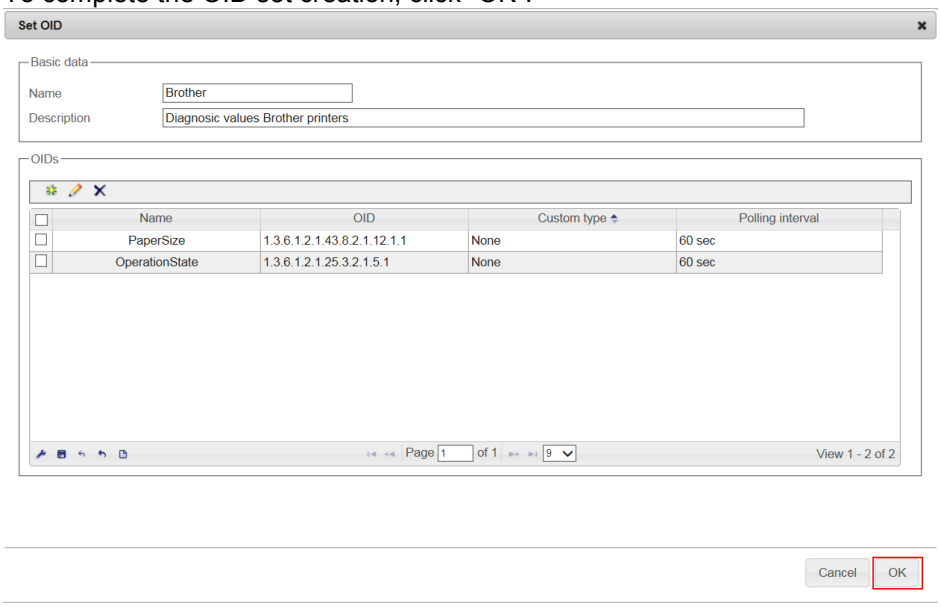
You have added a new OID for the Brother printer.



Name	OID	Custom type	Polling interval
PaperSize	1.3.6.1.2.1.43.8.2.1.12.1.1	None	60 sec

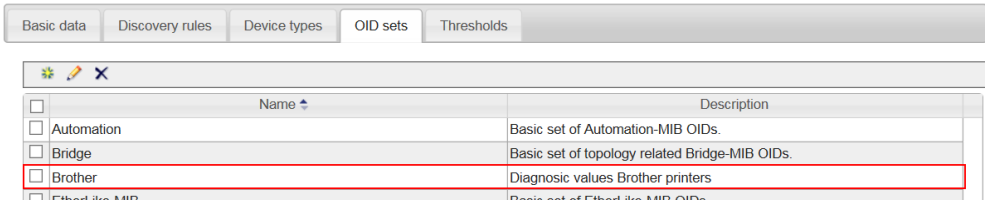
© Siemens AG 2017 All rights reserved

12. To add more OIDs to the “Brother” OID set, repeat steps 10 through 12.
    To complete the OID set creation, click “OK”.

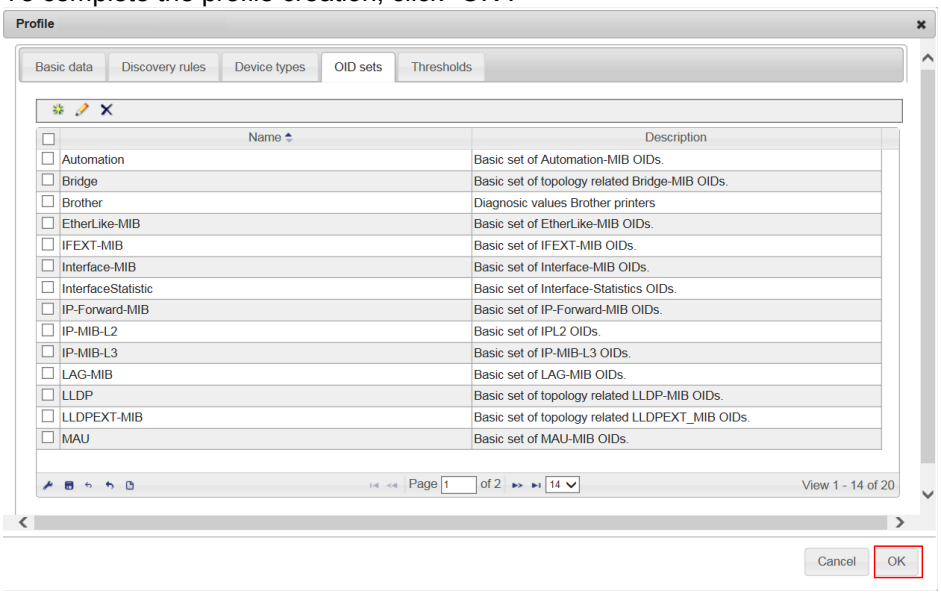


Result

You have created a new OID set, “Brother”.

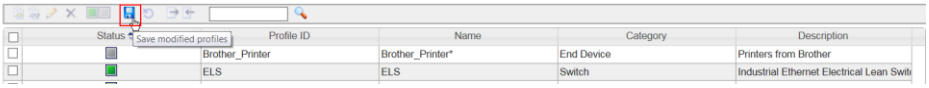


13. To complete the profile creation, click “OK”.

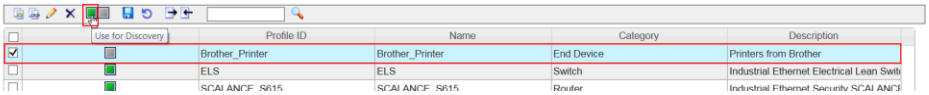


© Siemens AG 2017 All rights reserved

14. The new profile appears in the profile database. Select the new profile and use the highlighted tool to save the new item

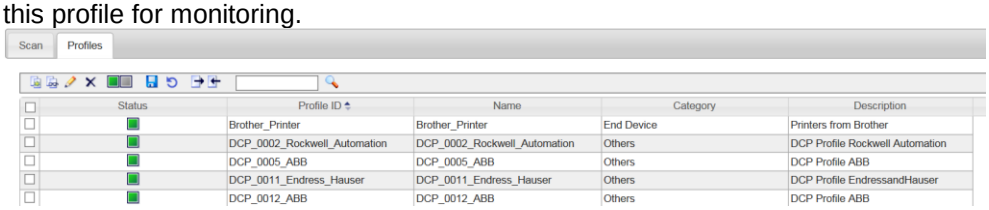


15. To use the new profile for monitoring, select the newly created profile. To activate the new profile, click the highlighted tool.



Result

You have added the new profile to the profile database. SINEMA Server uses also this profile for monitoring.

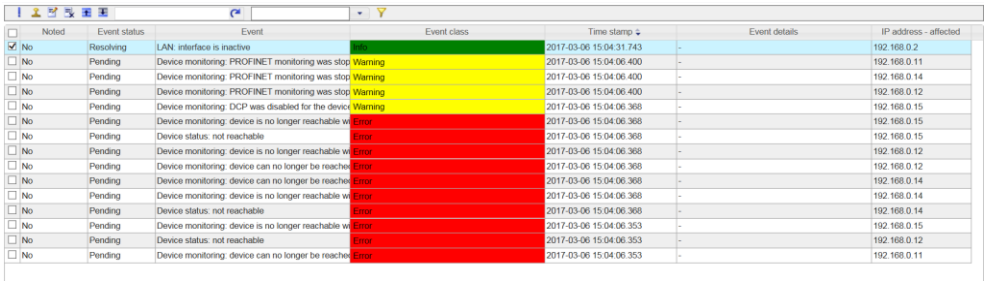


© Siemens AG 2017 All rights reserved

5 Understanding and Filtering the Event List

5.1 Valuable information on events

The program user interface of SINEMA Server provides the event list that keeps you constantly informed about activities in the network or SINEMA Server. The event list displays all events in a table.



Noted	Event status	Event	Event class	Time stamp	Event details	IP address - affected
No	Resolving	LAN: interface is inactive	Info	2017-03-06 15:04:31.743	-	192.168.0.2
No	Pending	Device monitoring: PROFINET monitoring was stop	Warning	2017-03-06 15:04:06.400	-	192.168.0.11
No	Pending	Device monitoring: PROFINET monitoring was stop	Warning	2017-03-06 15:04:06.400	-	192.168.0.14
No	Pending	Device monitoring: PROFINET monitoring was stop	Warning	2017-03-06 15:04:06.400	-	192.168.0.12
No	Pending	Device monitoring: DCP was disabled for the device	Warning	2017-03-06 15:04:06.368	-	192.168.0.15
No	Pending	Device monitoring: device is no longer reachable w	Error	2017-03-06 15:04:06.368	-	192.168.0.15
No	Pending	Device status: not reachable	Error	2017-03-06 15:04:06.368	-	192.168.0.15
No	Pending	Device monitoring: device is no longer reachable w	Error	2017-03-06 15:04:06.368	-	192.168.0.12
No	Pending	Device monitoring: device can no longer be reache	Error	2017-03-06 15:04:06.368	-	192.168.0.12
No	Pending	Device monitoring: device can no longer be reache	Error	2017-03-06 15:04:06.368	-	192.168.0.14
No	Pending	Device monitoring: device is no longer reachable w	Error	2017-03-06 15:04:06.368	-	192.168.0.14
No	Pending	Device status: not reachable	Error	2017-03-06 15:04:06.368	-	192.168.0.14
No	Pending	Device monitoring: device is no longer reachable w	Error	2017-03-06 15:04:06.353	-	192.168.0.15
No	Pending	Device status: not reachable	Error	2017-03-06 15:04:06.353	-	192.168.0.12
No	Pending	Device monitoring: device can no longer be reache	Error	2017-03-06 15:04:06.353	-	192.168.0.11

Classification

Events are divided into the following main categories:

- Network events
  Network events provide information about statuses and changes that have occurred in the network.
- System events
  System events provide information about actions, changes and error events of SINEMA Server.

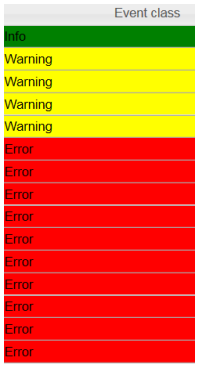
Classification

All network and system events are additionally classified by their severity.

The different event classes are listed below:

- Notification and information such as user login and logout
- Warning such as link down or link up received
- Error such as memory assignment failed

Depending on the classification, the “Event class” column is color-coded in the event list.



Event class
Info
Warning
Warning
Warning
Warning
Error
Error
Error
Error
Error
Error
Error
Error
Error
Error

© Siemens AG 2017 All rights reserved

Event status

Events can have different statuses. The status of an event depends on the overall status of the network device for which this event was triggered.

An event can have the following statuses:

- Pending
  An event triggered for a network device to which a negative overall status (each overall status except “OK” and “Not connected”) is assigned is labeled as “Pending”. The event was included in a list of events pending for the device.
- Resolved automatically
  An event that was removed from the list of pending events is labeled as “Resolved automatically”. Pending events are automatically resolved, for example, when the device changes to a positive overall status (overall status: “OK” and “Not connected”).
- Resolved manually
  A pending event that was manually removed from the list of pending events using the appropriate tool (“Stamp”) in the event list is labeled as “Resolved manually”.
- <blank>
  A triggered event that is not assigned to an overall status has no event status. Normally, these are system events.

Note

Chapter 4.4.4 (see \4\, Chapter 7.2) of the “SIMATIC NET network management SINEMA Server” operating instructions provides you with more information about the overall status of a device.

Filter templates

You can filter the data displayed in SINEMA Server, for example events, by criteria. To avoid having to reconfigure the selected filter criteria before each filter operation, you can save them in a filter template and reuse the filter template. Cross-user filter templates can be reused by all users of the SINEMA Server instance.
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 below order:

1. Prefilter:
   The prefilter includes basic filter criteria that are applied, on the server side, to data to be displayed. Data that passes the prefilter is forwarded to the clients.
2. Complex filter.
   In the second step, the data received by clients is filtered using any complex query. With a complex query, filter rules can be created for individually selectable columns. These rules can be connected using logical operators and nested within one another using rule levels.
3. Simple filter:
   In the third step, the data that has passed the complex filter is filtered by entering free text. In contrast to the complex filter, the simple filter, by default, includes all columns of the appropriate data category.

© Siemens AG 2017 All rights reserved

Event list functions

The event list provides a toolbar with functions. You can use these functions for an event selected in the event list.

This includes the following functions:

- Event noted
- Manually resolve event
- Edit and/or delete remark
- Maximize/minimize event list
- Filter options

For a detailed description and list, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.1.14 (see \4\, Chapter 7.2).

5.2 Customizing the event list

Customizing the display

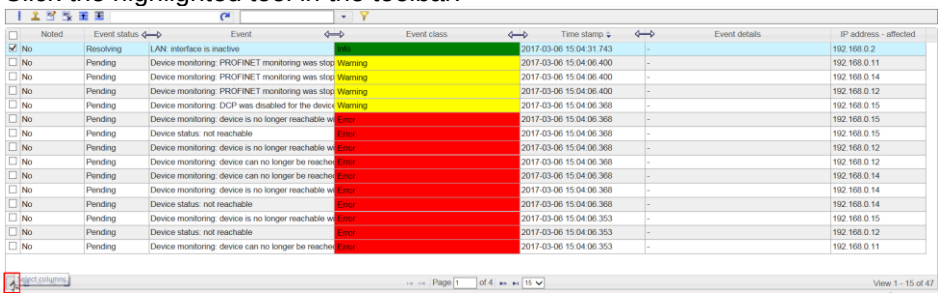
The event list displays all events in a table. Each column is assigned to a specific piece of information.

The tools in the footer allow you to design the entire table as required. You can make the following changes:

- Add columns with more information
- Remove existing columns
- Change column width

To customize the event list, proceed as follows:

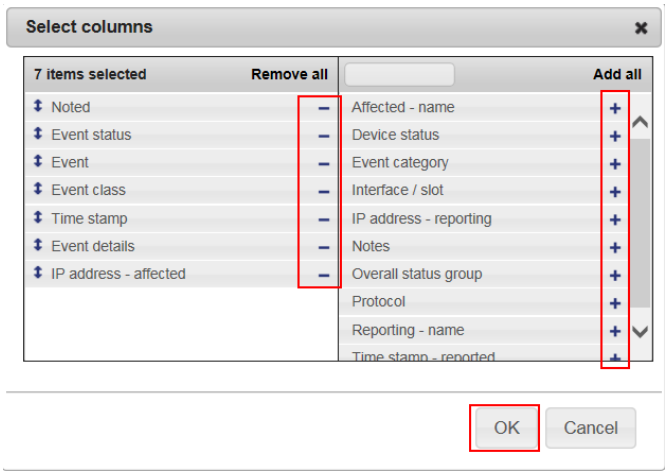
1. Click the highlighted tool in the toolbar.



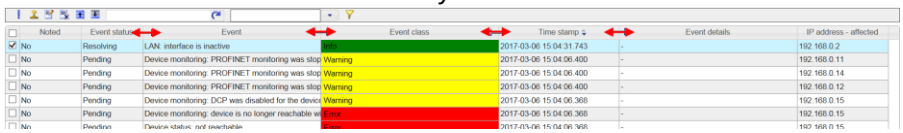
© Siemens AG 2017 All rights reserved

2. The window for selecting columns opens. It consists of the following parts:
   - In the left part, you can see the columns that have already been displayed.
   - In the right part, you can see the columns that are still free.

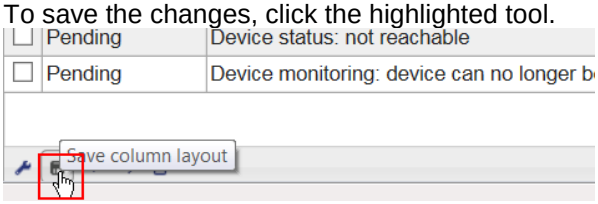
   Use the minus sign ("-") to remove existing columns and/or use the plus sign ("+") to add new columns.
   Using drag and drop, you can change the column sorting.
   Select "OK" to close the window.



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



4. To save the changes, click the highlighted tool.



Result
The modified event list appears in the device window.

© Siemens AG 2017 All rights reserved

Filtering events

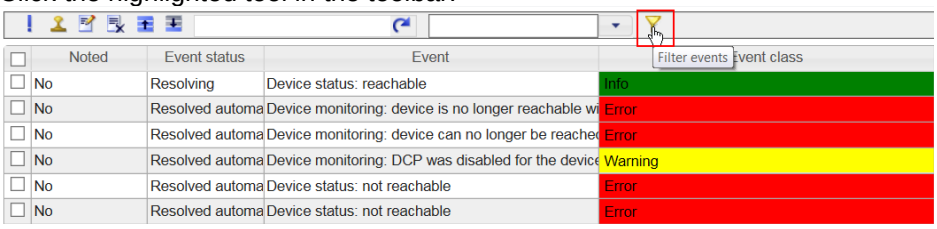
Using filter templates, event lists can be filtered by various criteria.

You can filter events by the following criteria:

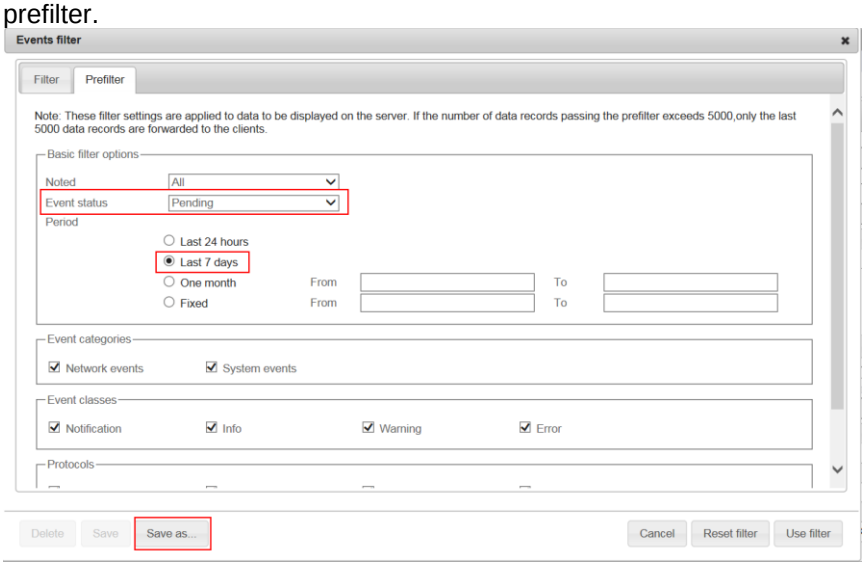
- Event status
- Period:
  - By events in the last 7 days/24 hours
  - By all events starting with the current time
  - By all events within a manually entered period
- Event class
- Event category
- Protocols

The following instructions show you how to filter events using a prefilter:

1. Click the highlighted tool in the toolbar.

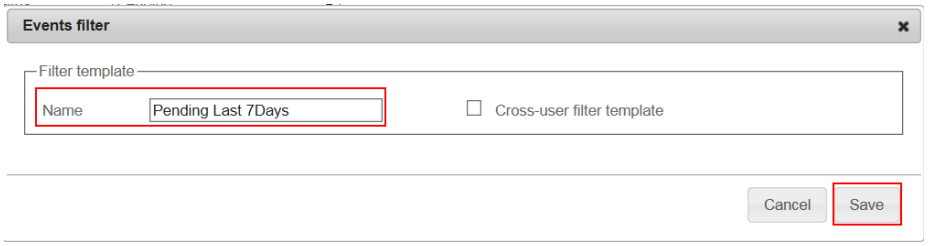


2. The “Events filter” dialog appears. Go to the “Prefilter” tab.
   Set the filter, for example “Pending last 7 days”. Click “Save as…” to save the prefilter.

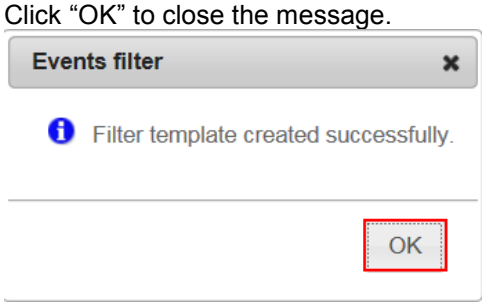


© Siemens AG 2017 All rights reserved

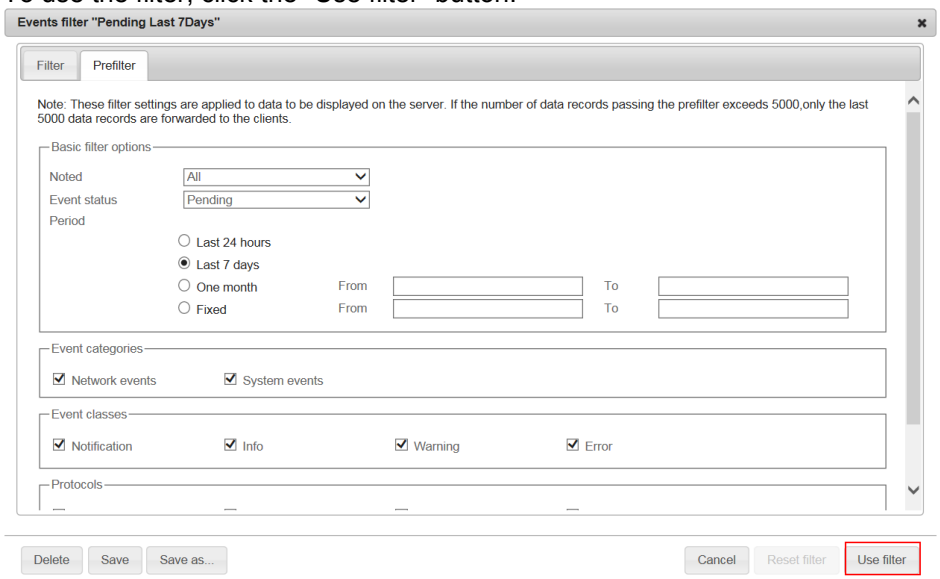
3. A dialog opens where you can enter a filter template name under which you want to save the configured filter settings. The name must be unique within the SINEMA Server instance and not contain more than 25 characters. Click “Save”.



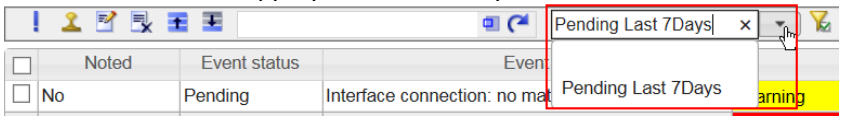
4. A new dialog opens and confirms the successful creation of the filter template. Click “OK” to close the message.



5. To use the filter, click the “Use filter” button.



6. All created filter templates are listed in a drop-down list. You can view the contents of this list using the toolbar. To use a filter template from the drop-down list, select the appropriate item and press <ENTER>.



© Siemens AG 2017 All rights reserved

Result

Filtered display of events in the event list based on the definition in the prefilter. The screenshot shows events filtered by the “Pending” event status within a period of seven days.

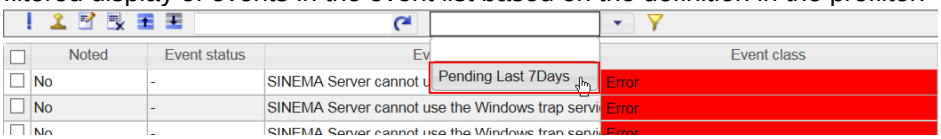
Event status	Event	Event class
Pending	Device status: not reachable	Error
Pending	Interface connection: no match with reference.	Warning
Pending	Interface connection: no match with reference.	Warning
Pending	LAN: interface inactive and does not match referen	Error
Pending	Redundancy status: redundant connection activate	Warning

Manually resolving events

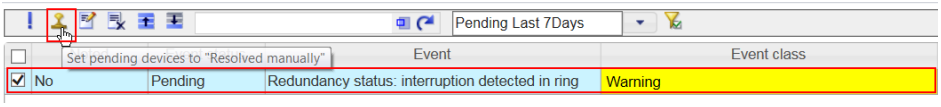
You can manually resolve events with the “Pending” status using the appropriate tool (“Stamp”) in the toolbar. This action removes a selected pending event from the list of events pending for a device. Then the device is assigned the “Resolved manually” event status. To view only events with the “Pending” status, use the “Pending Last 7 Days” prefilter you have just created.

To manually resolve an event, proceed as follows:

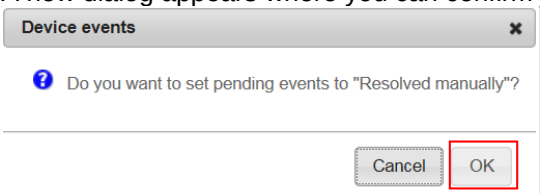
1. From the drop-down list, select the “Pending Last 7 Days” prefilter. You get a filtered display of events in the event list based on the definition in the prefilter.



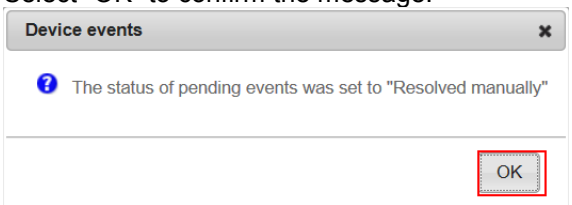
2. From the event list, select the desired event and click the highlighted tool (“Stamp”).



3. A new dialog appears where you can confirm the action. Click “OK”.



4. A new dialog informs you that the selected event was manually resolved. Select “OK” to confirm the message.



Result

The new status of the selected event is “Resolved manually” and it is no longer listed in the event list.

© Siemens AG 2017 All rights reserved

6 Understanding and Using the Topology

6.1 Valuable information on the topology

6.1.1 General information

Monitoring using the topology

The device information that can be detected by SINEMA Server includes information about neighboring devices. Using the SNMP and PROFINET protocols, SINEMA Server reads neighborhood information and uses LLDP to calculate a topology display that graphically represents the discovered connections between devices.

Note

Network topology detection is based on LLDP information read via SNMP or PROFINET. To obtain detailed connection information, SNMP and/or PROFINET monitoring must be enabled in SINEMA Server for the devices to be monitored.

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

To monitor the devices, you can define DESIRED states for connectors, connections and protocol availability in the topology display. Deviations between ACTUAL and DESIRED states are then highlighted graphically.

Topology modes

In a previous version of SINEMA Server V14, you used different topology display types for viewing, monitoring and configuring networks:

- “Detected topology”
- “Monitored topology”
- “Reference topology”.

In SINEMA Server V14, you will only find a single topology for viewing, monitoring and configuring networks. In SINEMA Server V14, you work with different topology modes to create the conditions for device monitoring in the monitored topology.

SINEMA Server V14 provides the following modes:

- Editing mode
- Online mode

Based on the topology detected by SINEMA Server, Editing mode allows you to configure a reference topology that represents the desired state of the network. The configured reference topology forms the basis for monitoring the network.

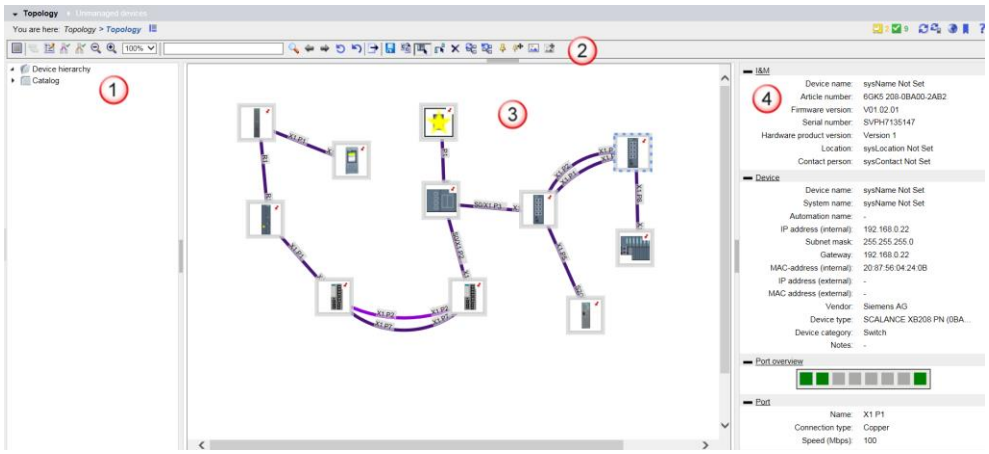
Online mode allows you to monitor the network considering the configured reference topology. For connections and ports of reference devices, deviations between determined statuses and reference statuses are highlighted by SINEMA Server and communicated through associated events.

© Siemens AG 2017 All rights reserved

6.1.2 Workspaces and how to use them

Workspaces

The following figure uses Editing mode to illustrate the individual workspaces.



The following table shows the meaning of the numbers:

Table 6-1

No.	Workspace	Description
1	Device hierarchy	The device hierarchy lists all devices that were detected after a scan. In Editing mode, the device hierarchy in the left-hand sidebar is initially blank, all detected devices are in the topology display.
2	Toolbar	The toolbar provides elements for using the topology.
3	Device hierarchy in the topology display	The main window displays the devices of the device hierarchy in a topology.
4	Detail area	After selecting a device in the topology display, this area displays associated details about the device, ports and events.

Functions of the topology

The topology provides a toolbar with control elements.
Whether or not you can select a control element depends on the topology mode you are in.

The following tables provide information about the specific functions of the control elements and specify in which topology mode the control element is available.

For a detailed description and list, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.2 (see \4\, Chapter 7.2).

General control elements

The following table shows the control elements that can be selected in the two topology modes.

© Siemens AG 2017 All rights reserved

Table 6-2

Control element	Function
	Enable Editing/Online mode.
	Reduce/enlarge topology view.
100%	Select zoom level.
	Search device properties of devices in topology display for entered text.
	Select previous/next device if device scan finds multiple devices.
	Reset device scan and scan results.
	Export topology display as *.PNG file in *.ZIP archive.
	Save configured reference topology and update topology display.

Control elements in Editing mode

The following table shows the control elements that can only be selected in Editing mode.

Table 6-3

Control element	Function
	Extended icon view
	Allows you to make topology settings. These settings include: • Show connections/port names • Define device labeling • Set size of topology grid • Define topology size
	Show detected, active connections between devices.
	Show learned connections between alternating devices and tool changer devices.
	Adopt detected statuses as reference statuses.
	Selection tool; use drag and drop to move devices along the configured topology grid.
	Drawing tool; manually draw reference connections between reference devices.
	Delete learned connections.
	Recalculate device positions.
	Reset reference topology.
	Fix selected devices.
	Fix devices after moving.
	Insert background image.
	Move background image.

© Siemens AG 2017 All rights reserved

Control elements in Online mode

The following table shows the control elements that can only be selected in Online mode.

Table 6-4

Control element	Function
No VLAN Selected	After selecting a VLAN ID, highlight all the devices and connections associated with it in blue.

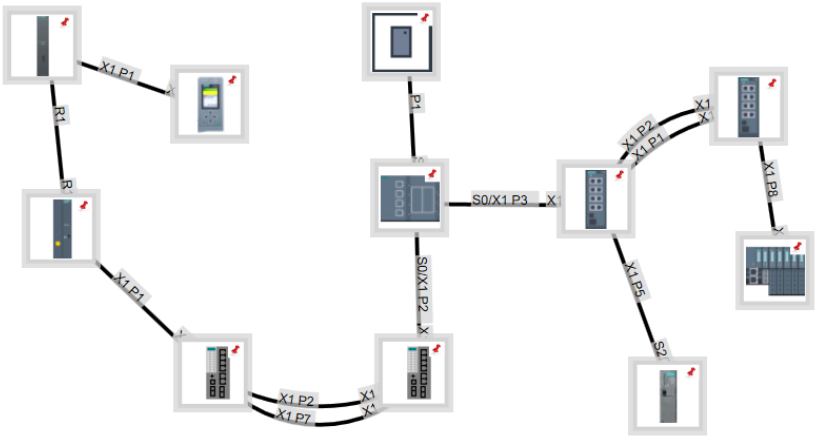
© Siemens AG 2017 All rights reserved

6.1.3 Representation in the topology

The devices, connections and ports discovered and assigned by SINEMA Server using the protocols are automatically displayed in a topology.

Devices

In both topology modes, SINEMA Server places the detected devices in the topology display and connects them using their detected connections. Each device is represented by a node that displays the icon of the associated device type.



In both topology modes, devices that are not part of the reference topology are displayed with a star icon. Reference devices are displayed without a star icon.

Devices whose device position is fixed in the topology view are displayed with a pin icon.

In the topology display, SINEMA Server shows devices without detectable connection information separated from the networked devices. If a device without a detectable IP address is connected to three or more devices, the device without the detectable IP address is indicated by a cloud icon.

Note The device distribution based on the equilibrium of forces between nodes and connections can be changed in Editing mode.

Connections

In all topology modes, the connection between the devices is represented by a line.

In Editing mode, the lines are represented using the following color coding:

- Current connections are purple,
- learned connections are brown and
- reference connections are black.

The following rule applies:

- If several connection types apply, the specific connection colors are combined.
- If the current and the learned connection type apply, only the current connection is displayed.

© Siemens AG 2017 All rights reserved

With regard to the connected ports, the connection lines in Online mode correspond to the connection lines in Editing mode. Current connections that were not defined as reference connections are displayed with a star icon.

If a reference connection between two ports does not correspond to the current connection or one of the learned connections, the connection color is red. Otherwise, the connection color is based on the fill color of the two connected ports. Wireless, optical, electrical and unknown connections are represented by different dash types. If the connection is, for example, a wireless connection, the connection line is shown as a closely spaced dashed line.
The following table provides an overview of the connection types and the way they are displayed:

Table 6-5

Connection type	Description
	Wireless connection
	Optical connection
	Electrical connection
	Unknown connection

Note

For a detailed description of possible colors and dash types, please refer to the “SIMATIC NET network management SINEMA Server” operating instructions, Chapter 4.2 (see \4\, Chapter 7.2).

Note

For current connections and learned connections to be displayed, the associated options must be enabled in the toolbar. For learned connections to be displayed, additionally check the “Detect alternating devices automatically” check box in “Administration > Monitoring > General”.

© Siemens AG 2017 All rights reserved

Partial connections

If SINEMA Server cannot detect a connection port of at least one device, partial connections are created. Partial connections are indicated by a missing port on at least one side. This connection is referred to as a “partial connection”.

The following different types of partial connections exist:

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

Partial connections are displayed based on the same rules as conventional connections. Partial connections cannot be directly adopted as reference connections. It is first necessary to select the ports involved in the connection wizard.

In Online mode, the color of an added reference connection is created by comparing it to the detected connection information. For type A partial connections, the connection color is specified by the port’s fill color if the connection information matches.

6.1.4 Editing mode

Description

In the detected topology, it is possible that the topology does not show all connections or possibly detects incorrect connections. One possible cause is that some devices are detected in the network for which SNMP and/or PROFINET are disabled. Another possible cause is that “unmanaged” devices exist that cannot be automatically discovered by SINEMA Server.

Based on the topology detected by SINEMA Server, Editing mode allows you to configure a reference topology that represents the desired state of the network. This DESIRED state forms the basis for monitoring the network in Online mode and in view-specific topology displays.

In Editing mode, a connection wizard helps you configure the reference topology.

Options for correcting and adding

The connection wizard is used for the following purposes:

- Setting reference connections
- Setting reference statuses for ports
- Setting reference statuses for protocol-specific device availability
- Adding new devices in the editor
- Adding unmanaged devices and network clouds

Setting reference connections

The following rule applies to the colors used for the connections in Editing mode:

- Current connections are purple,
- learned connections are brown and
- reference connections are black.

Reference connections can be configured as follows:

- Manually draw the connection using the “drawing” tool
- Manually change the reference status by double-clicking
- Change the reference status using the context menu
- Use the current/learned connection as the reference connection

© Siemens AG 2017 All rights reserved

Setting reference statuses for ports

Ports can have the following reference statuses:

- Active
- Inactive
- Unmonitored
- Docking port

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

- Manually change the reference status by double-clicking
- Change the reference status using the context menu
- Use the determined status as the reference status

Note It is not possible to change the reference status of ports that have a reference connection.

Adding new devices in the editor

In Editing mode, all detected devices are in the topology display. If these devices are deleted from the topology display using the context menu, they appear in the “Device hierarchy” and can be added to the topology display using drag and drop.

6.1.5 Online mode

Online mode allows you to monitor the devices and the current network topology considering the configured reference topology. Deviations between determined statuses and configured statuses are highlighted by SINEMA Server.

© Siemens AG 2017 All rights reserved

6.1.6 Views

Purpose and use

In the monitored topology, a very large hierarchy of the network topology can become cluttered.

SINEMA Server allows you to separately monitor individual parts of the total monitored network. You can use the separate monitoring groups for the following examples:

- Your reference system consists of a very large number of devices and connections and the overall view is cluttered.
- You are only interested in parts of the monitored topology, for example ring topologies.

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

Note

In user management, you can assign the views to individual users who do not have the “View all devices and servers” right. This allows you to limit the number of monitorable devices on a user-specific basis.
To do this, enable the “View user-specific topology” function in the User groups editor in “Administration > User > User groups”.

Requirements

If you want to set up views, the following requirements must be met:

- If you create a view-specific topology, a reference topology must exist.
- If you integrate SINEMA Server instances into a view-specific topology, these instances must be known to SINEMA Server.
- If you have created additional users, these users must have the “Operative monitoring settings” right. Users need this right to view and edit views.

© Siemens AG 2017 All rights reserved

6.2 Visualizing the network topology

For visual monitoring of the network, SINEMA Server allows you to generate a graphical representation of the network structure.

To get the DESIRED topology of the network to be monitored, perform the following steps:

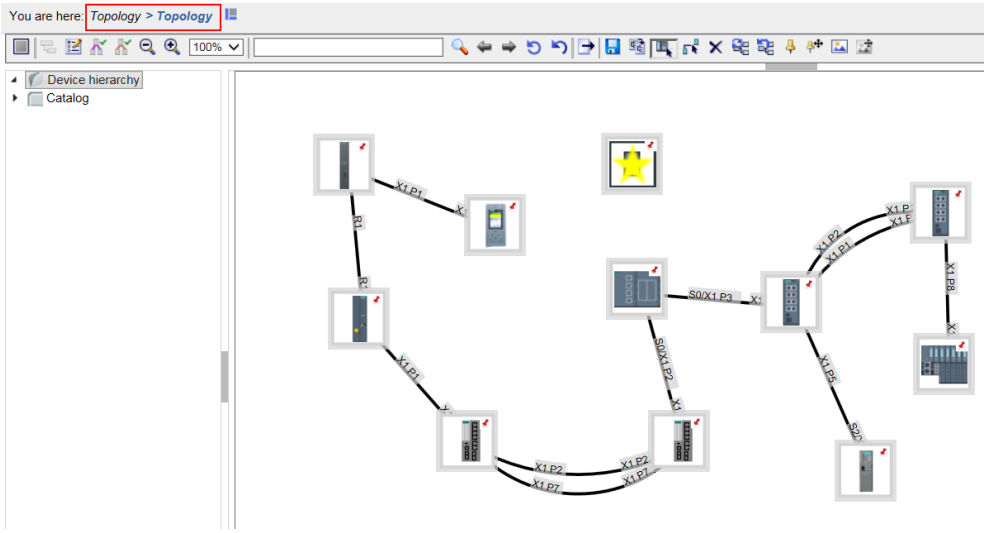
1. Open and set up topology
2. Make optional corrections
3. Enable Online mode

6.2.1 Opening and setting up the topology

The topology displays the currently detected ACTUAL state of the network. It shows a network topology calculated by SINEMA Server based on the information determined using SNMP and PROFINET.

Opening the topology

The “Topology” menu command opens the topology.



In which mode the topology opens depends on the following factors:

- If a reference topology has not yet been created and you have the “Operative monitoring settings” right, the topology is displayed in Editing mode.

- If a reference topology exists, the topology is displayed in Online mode once the “Topology” menu command has been selected.

Note The status of the “Operative monitoring settings” right can be viewed in the User groups editor in “Administration > User > User groups”.

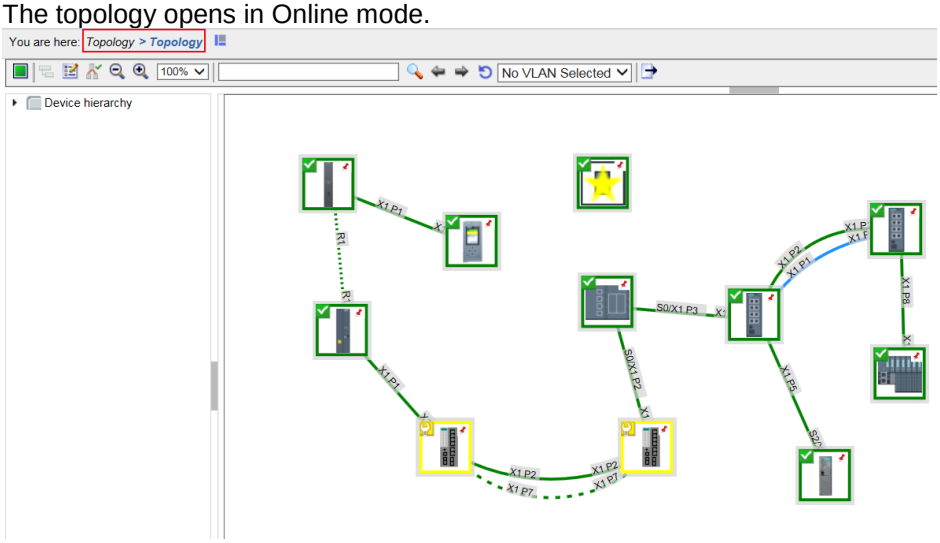
The view displays the topology layout of the devices and their connections. It shows the device status, port status and connection lines.

© Siemens AG 2017 All rights reserved

To change the mode and view, proceed as follows:

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

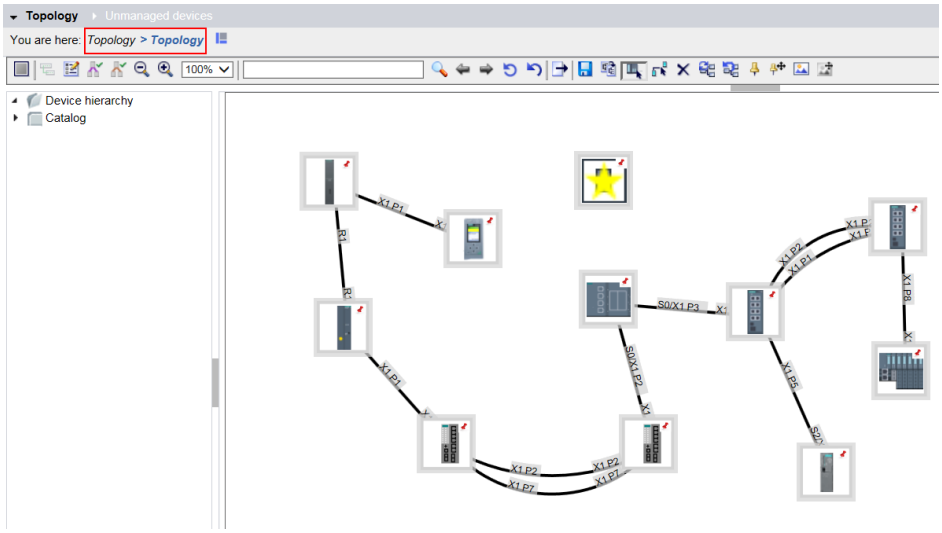
2. The topology opens in Online mode.



3. To switch to Editing mode, click the highlighted tool.

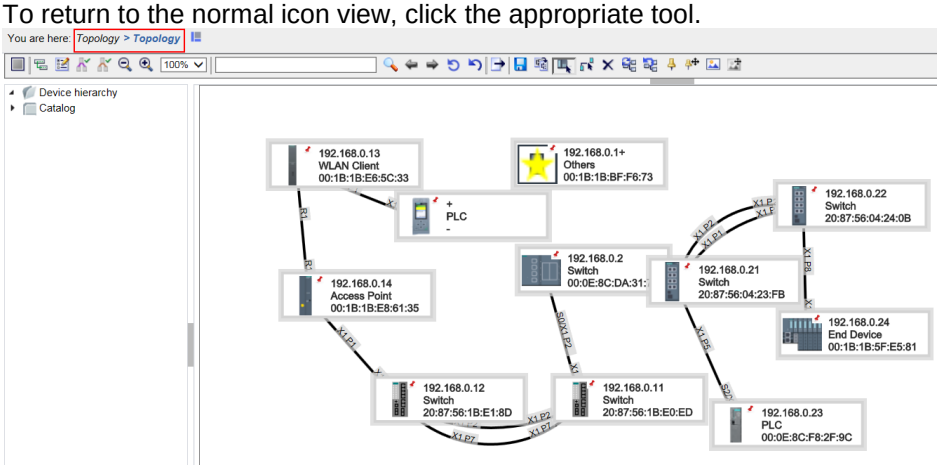
© Siemens AG 2017 All rights reserved

4. The topology opens in Editing mode.



5. To select the extended icon view, click the highlighted tool.

6. The topology opens in the extended icon view.
   The extended icon view additionally displays up to three device properties that can be configured in the topology settings.
   To return to the normal icon view, click the appropriate tool.



© Siemens AG 2017 All rights reserved

Topology settings

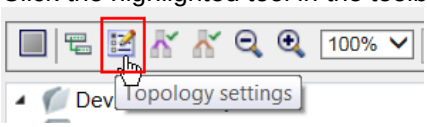
You can make various topology settings. The settings relate to the way the topology and the devices are displayed.

You can make the following settings:

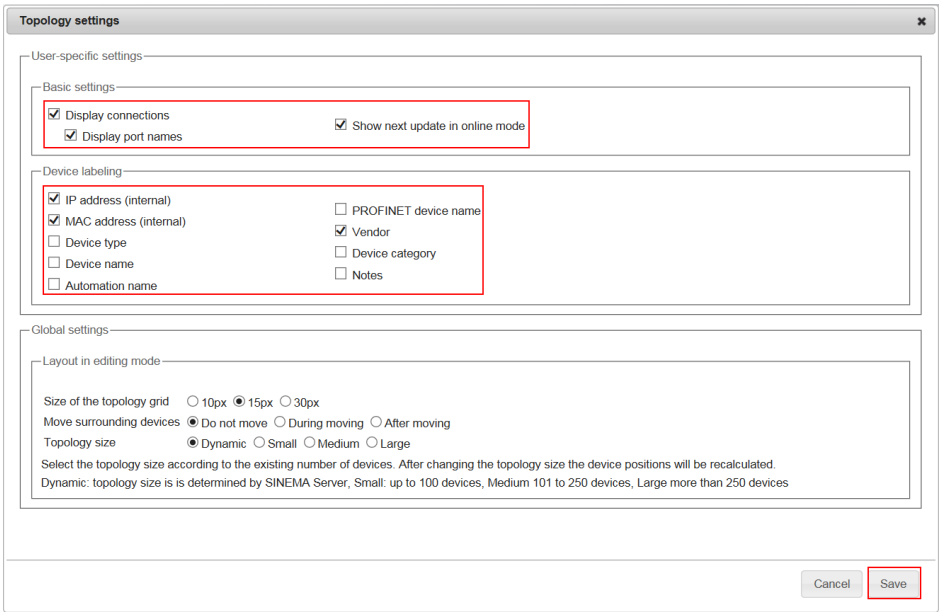
- Show/hide all connections.
- Show/hide port names.
- Show/hide circle icon for automatic update progress of topology display in Online mode. The circle icon indicates when the automatic update interval has expired.
- Select up to three device properties that are displayed in the extended icon view.
- Set the size of the topology grid cells in Editing mode. Devices can only be moved along these grid cells.
- Define the moving behavior for the surrounding devices when selected devices are moved.
- Set the spacing and lengths of the connections between the devices in Editing mode.

You must be in Editing mode to make topology settings. Proceed as follows:

1. Click the highlighted tool in the toolbar.



2. In the displayed dialog, select the desired options.
   In “Device labeling”, you can select up to three items. Select “Save” to close the dialog.



Result

The topology displays the information based on the new settings.

© Siemens AG 2017 All rights reserved

Checking the topology

The topology shows the physical arrangement of devices and their connections calculated by SINEMA Server based on the information determined using LLDP.

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

If the topology does not display all of the devices/connections or incorrect ones, this could be caused by the following:

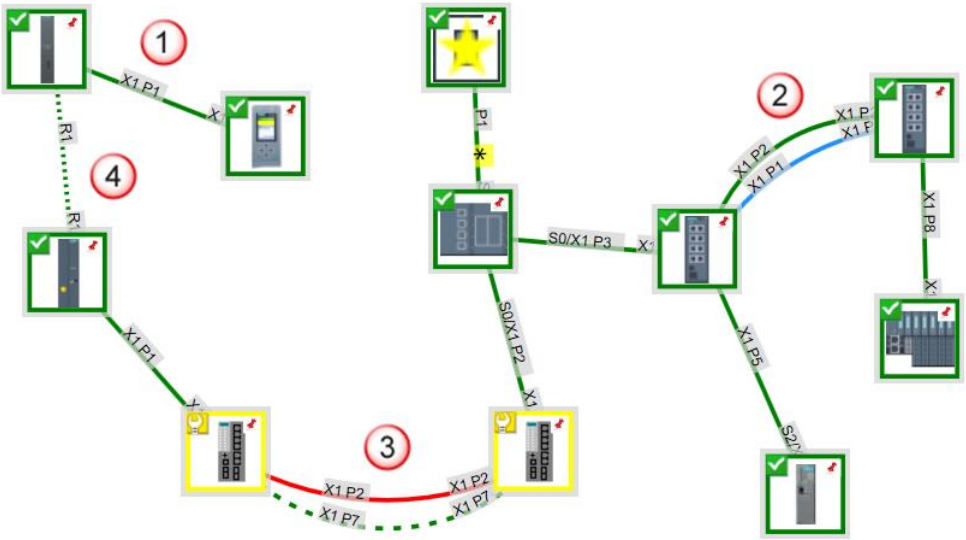
Table 6-6

Cause	Remedy
Discovery of devices for which SNMP and/or PROFINET are disabled.	Make sure that the nodes can be reached via SNMP or PROFINET and enable SNMP or PROFINET in the relevant devices. Delete the relevant module from the SINEMA Server device list and run a new scan.
Discovery of devices via DCP, but the SNMP information cannot be read.	Check the SNMP settings in the device. For correct, successful device discovery, the SNMP settings in the network devices and in SINEMA Server must match (see Chapter 2.3.2). Delete the relevant module from the SINEMA Server device list and run a new scan.
“Unmanaged” devices in the network.	SINEMA Server cannot specify these devices. In the reference topology, you can manually add “unmanaged” devices to complete the display (see Chapter 6.2.2).
No or incorrect display of connections.	Not all devices support the LLDP neighborhood discovery protocol. The reference topology allows you to manually insert connections (see Chapter 6.2.2).
No discovery of inserted media modules.	If new modules are inserted into a module that has already been monitored by SINEMA Server, these modules are not immediately discovered by SINEMA Server. Delete the relevant module from the SINEMA Server device list and run a new scan.

© Siemens AG 2017 All rights reserved

Topology of the reference system in Online mode

The following figure shows the topology automatically created by SINEMA Server for the reference system of this description (see Chapter 1.2).
To show you different colors and statuses in the topology view, the ring between the two XC-200 modules was opened in the reference system.



Note

The colors used in the topology are based on the device statuses of the real network devices. As a result, it is possible that your detected topology is displayed with different colors.

The following table provides a description of the reference system's detected topology.

Table 6-7

No.	Description
1	The display of the devices, connections and interfaces is color-coded based on their status. Green means that everything is "OK". Yellow indicates a maintenance request.
2	SINEMA Server has discovered the redundant ring connection between the two XB-200 modules. As one connection is blocked and therefore passive, the passive connection and the associated ring port are shown in blue.
3	A ring connection is configured between the two XC-200 modules; however, this connection is physically interrupted. SINEMA Server detects the ring configuration and the open connection. The device status of the redundancy master and the affected ring ports are therefore labeled with "Maintenance request" (yellow). The uninterrupted connection is shown in red. The connection type between the two XC-200 modules is optical. As a result, the connection line appears as a dashed line.
4	The SCALANCE W modules set up a WLAN and thus enable the CPU S7-1500 to participate in the network. SINEMA Server detects the WLAN. The connection line appears as a closely spaced dashed line. Due to the "Own" MAC mode setting in the SCALANCE W722, the WLAN client, too, is visible in SINEMA Server.

© Siemens AG 2017 All rights reserved

6.2.2 Making corrections in the topology

In Editing mode, you can make corrections and additions to the detected ACTUAL topology, thus defining a DESIRED state of the network.

Opening Editing mode

If a reference topology does not yet exist and you have the “Operative monitoring settings” right, the topology is automatically displayed in Editing mode.

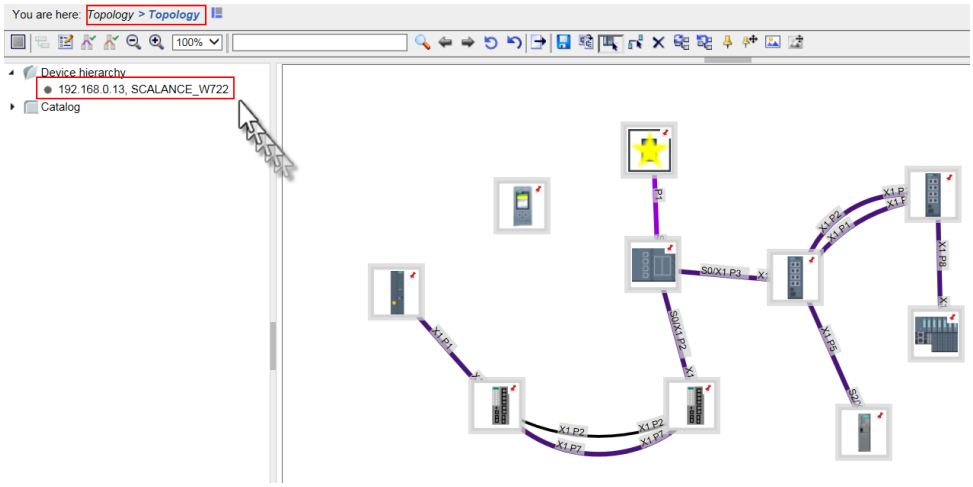
The mode you are currently in is indicated by the associated control element in the toolbar.

- Editing mode is indicated by the icon.
- Online mode is indicated by the icon.

When you click the control element, SINEMA Server switches to Editing mode.

Inserting devices

In Editing mode, the device hierarchy in the left-hand sidebar is initially blank and all detected devices are in the topology display. If these devices are deleted from the topology display using the context menu, they appear in the “Device hierarchy” and can be added to the topology display using drag and drop.



Devices that are newly discovered while a reference topology exists are displayed in the “Device hierarchy” dialog area. When selection mode is enabled, you have to add such devices in the Reference editor using drag and drop. This also applies to devices whose connections are unknown.

© Siemens AG 2017 All rights reserved

Using the reference without corrections

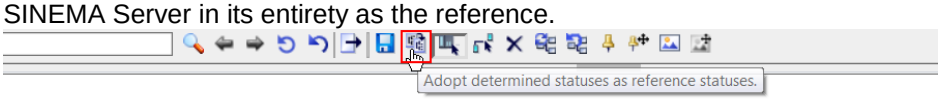
If the detected topology matches your DESIRED configuration, you can use the determined statuses for the monitored topology without any changes.

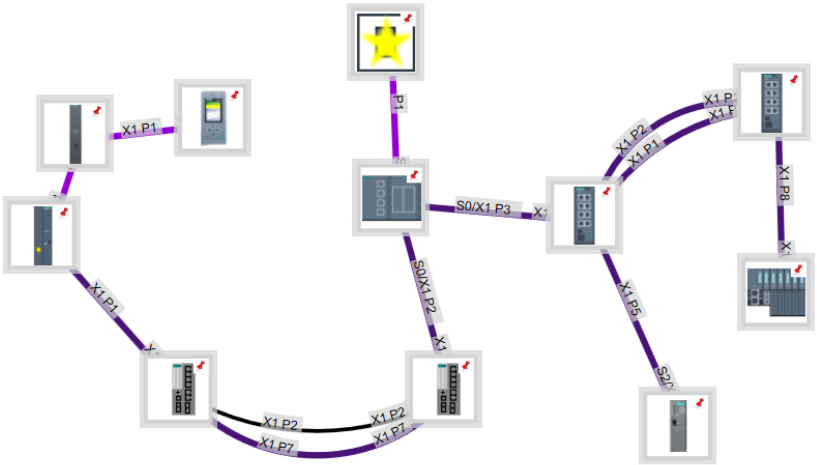
This applies to the following statuses:

- Adopting detected devices as reference devices.
- Adopting detected port statuses as reference statuses.
- Adopting current and learned connections as reference connections.

To do this, proceed as follows:

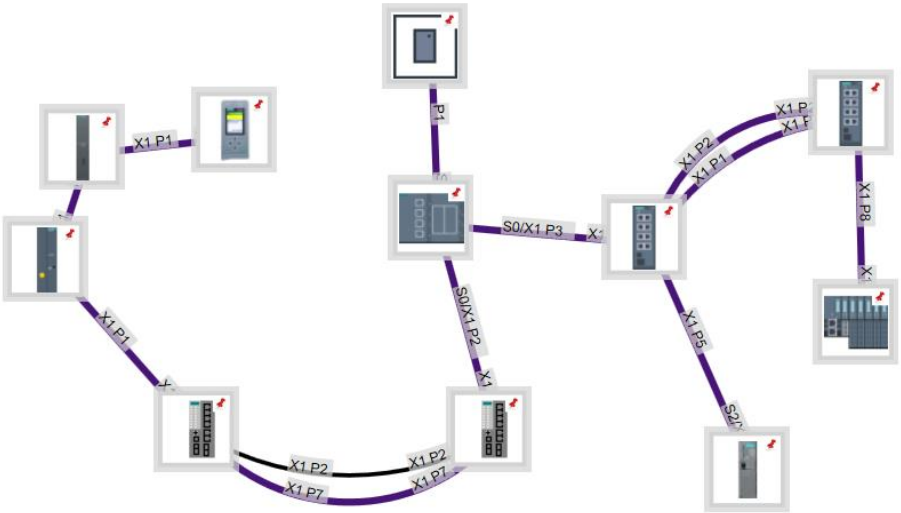
1. Click the highlighted tool in the toolbar. The “Adopt determined statuses as reference statuses” function allows you to define the topology detected by SINEMA Server in its entirety as the reference.



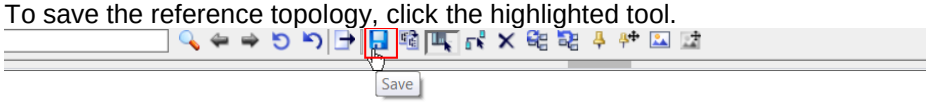


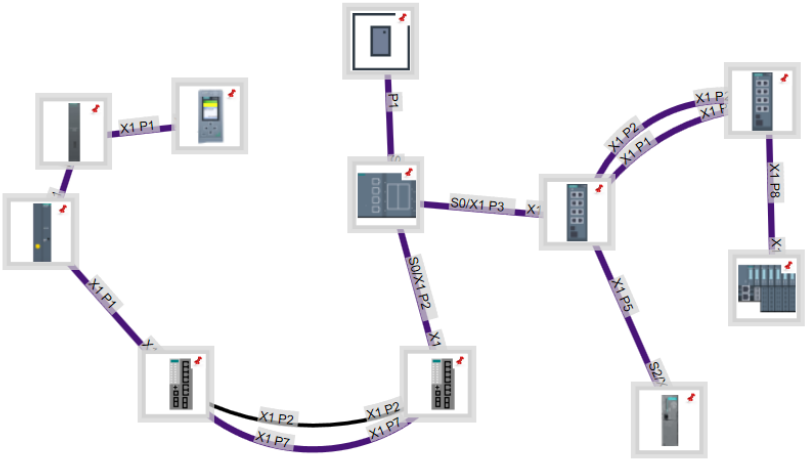
© Siemens AG 2017 All rights reserved

2. Now the colored connections of the detected topology are displayed as black reference connections. The star icons are removed from the devices.



3. To save the reference topology, click the highlighted tool.





Result

The reference topology is the basis for the topology display in Online mode.

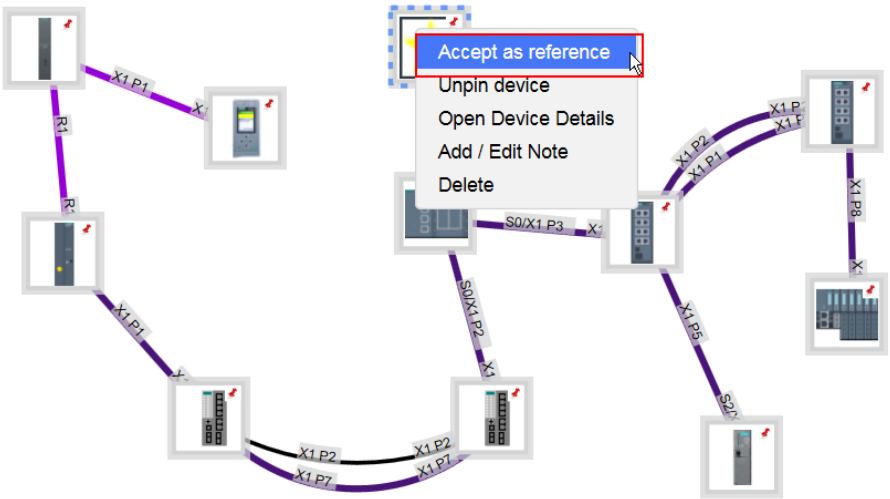
© Siemens AG 2017 All rights reserved

Accepting single devices and connections as the reference

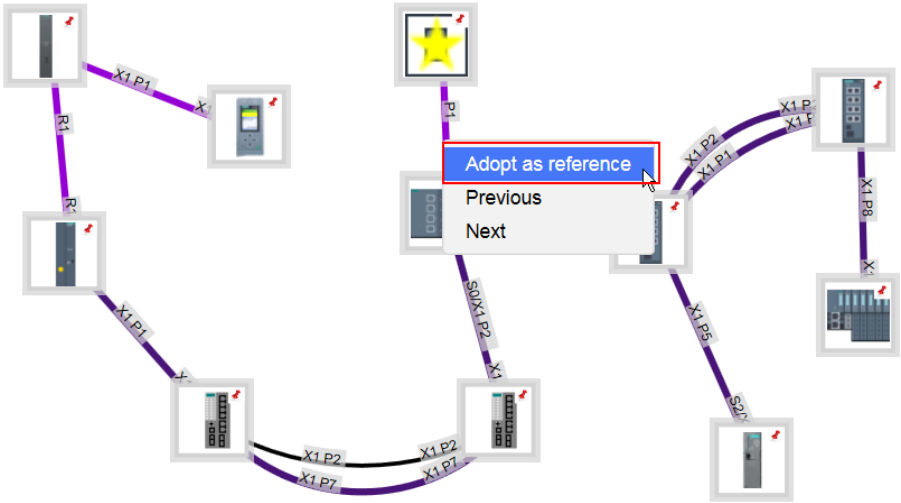
You can also accept single devices and connections as the reference. In both topology modes, devices that are not part of the reference topology are displayed with a star icon. In Online mode, current connections that are not part of the reference topology are displayed with a star icon.

Proceed as follows:

1. For devices:
   Right-click the device and select the appropriate item from the context menu.



2. For connections:
   Right-click the connection and select the appropriate item from the context menu. Alternatively, you can change the reference status by double-clicking the connection.

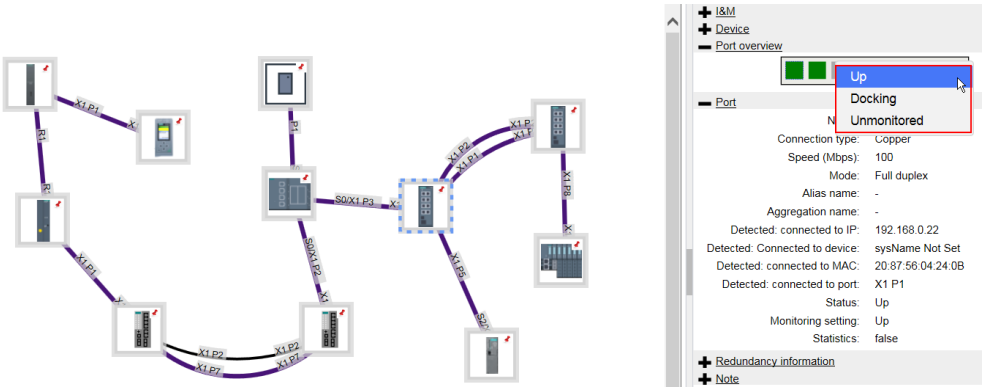


© Siemens AG 2017 All rights reserved

Correcting and customizing ports

The “Port overview” area in the sidebar displays the determined statuses and the configured reference statuses of the ports of the selected device.

If the detected port information differs from the reference status, right-click the port and select the desired reference status.



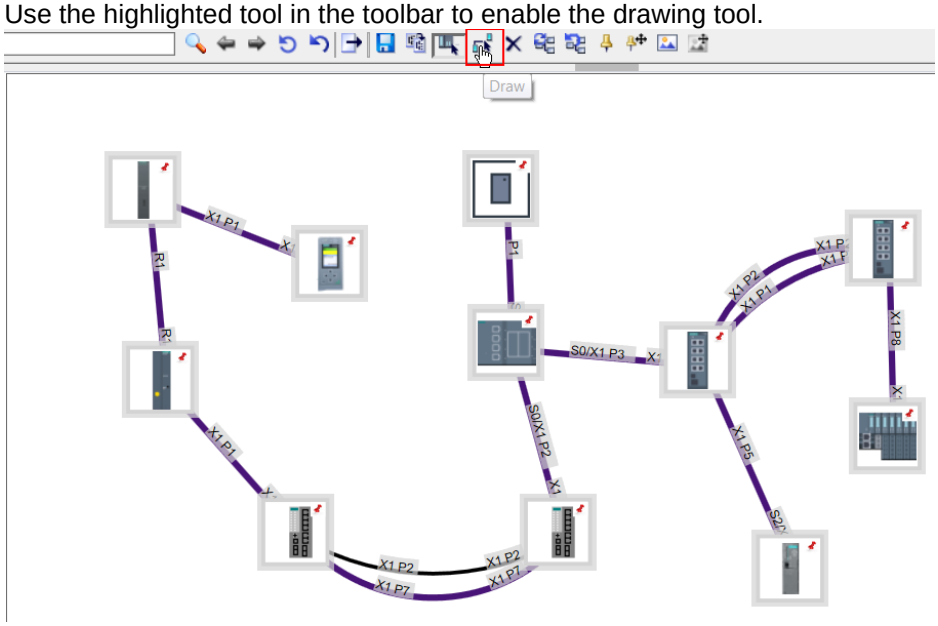
© Siemens AG 2017 All rights reserved

Correcting and customizing connections

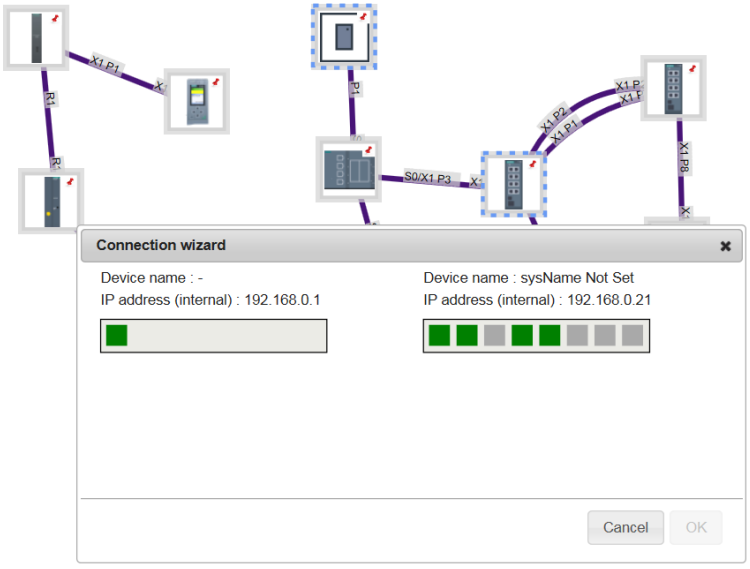
If the detected connection information differs from the reference status, you can also draw reference connections manually. The selected ports to be connected are shown in blue.

Proceed as follows:

1. Use the highlighted tool in the toolbar to enable the drawing tool.

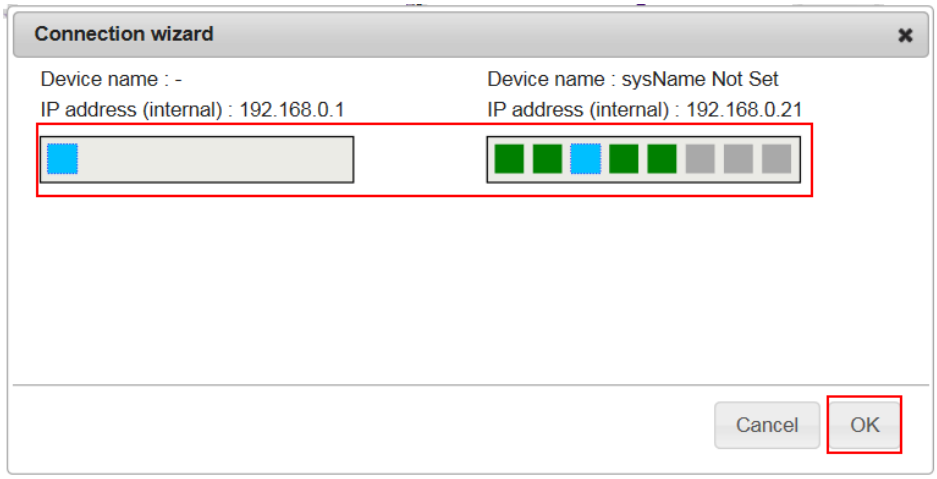


2. To draw reference connections manually, click the devices to be connected one after the other. This opens the connection wizard.

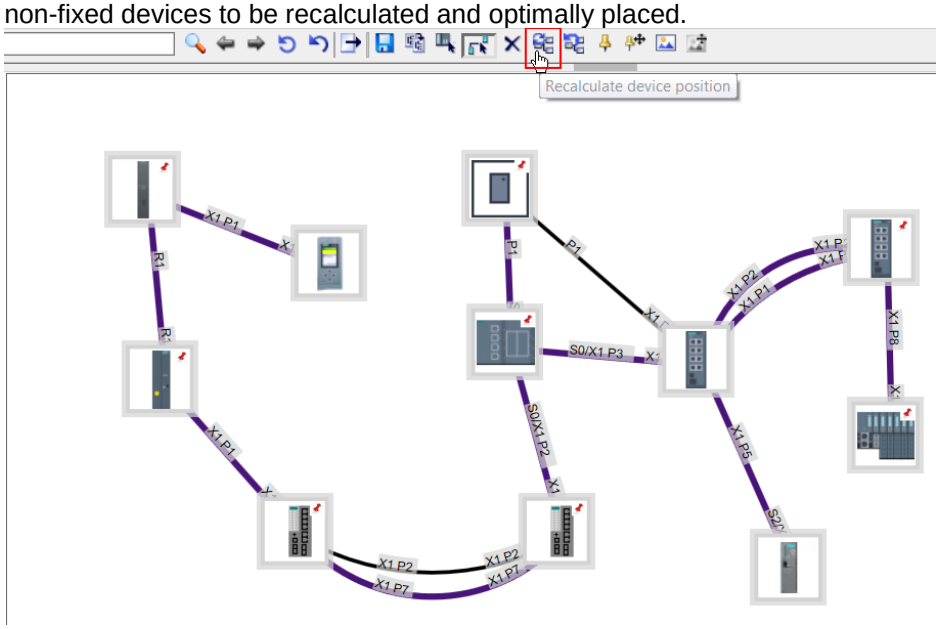


© Siemens AG 2017 All rights reserved

Click the device ports to be connected one after the other. Select “OK” to confirm your selection.

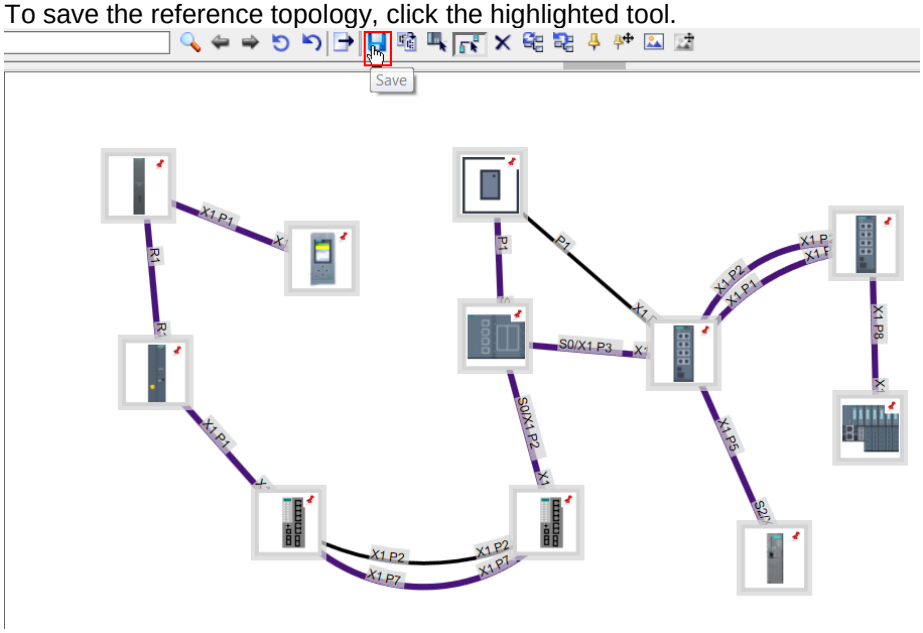


3. To recalculate the topology based on your newly drawn connections, click the highlighted tool during the process. This function causes the device position for non-fixed devices to be recalculated and optimally placed.



© Siemens AG 2017 All rights reserved

4. To save the reference topology, click the highlighted tool.



Result

You have manually created reference connections. Now these connections are included in the monitored topology.

Moving devices

You have the option to move devices in the topology view. The selection tool allows you to move devices along the configured topology grid using drag and drop. By default, devices are fixed when they have been moved in the topology view. When moving devices, the device spacing specified by the topology size configured in the topology settings is complied with.

To move devices, enable the “Select” icon in the toolbar.

Note

In the topology settings, you can define the moving behavior for the surrounding devices when selected devices are moved.

Fixing devices

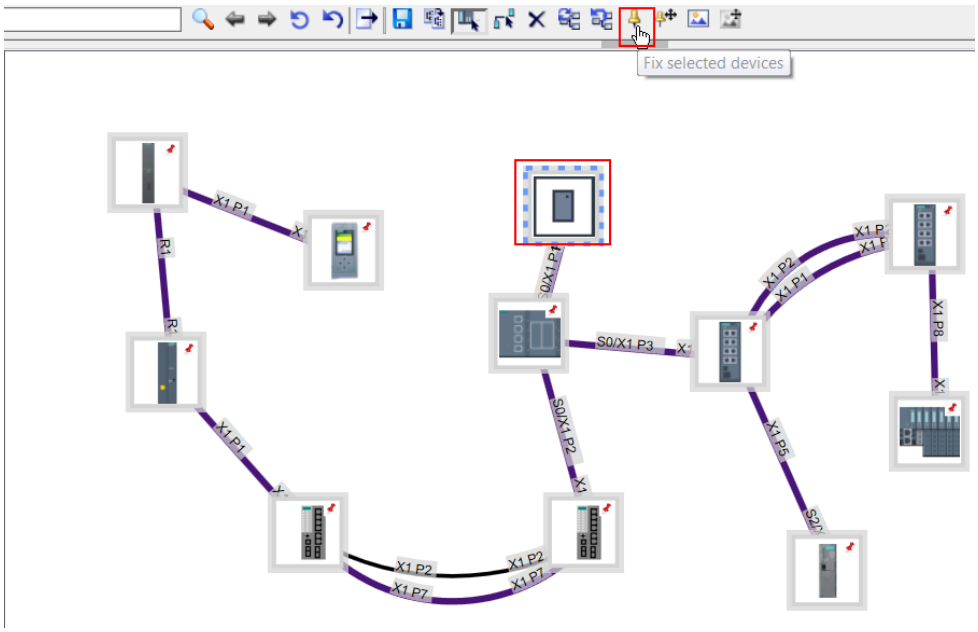
By default, detected devices are not fixed. Automatic repositioning of non-fixed devices can be caused by:

- Moving other devices
- Recalculating device positions
- Adding and removing devices

In these cases, fixed devices are not repositioned. Fixed devices are displayed with a pin icon.

To fix a device, select the appropriate device and select the “pin” icon from the toolbar.

© Siemens AG 2017 All rights reserved



You can also select multiple devices at a time: Press and hold down the <Ctrl> key and click the devices you want to select.

<Ctrl> + A allows you to select and move all the devices at once.

Note

Using this tool for devices that have already been fixed unfixes these devices.

If the selected devices include both fixed and non-fixed devices, using this tool fixes all devices.

© Siemens AG 2017 All rights reserved

6.2.3 Topology in Online mode

The topology in Online mode is the result of comparing the detected ACTUAL topology with the customizations from the reference topology.
The monitored topology displays the following information:

- Port statuses resulting from the detected topology and the reference topology.
- Port connections resulting from the detected topology and the reference topology. The ‘port connections’ display also includes the resulting statuses of the ports involved.

Opening Online mode

If a reference topology exists, the topology is displayed in Online mode once the “Topology” menu command has been selected.

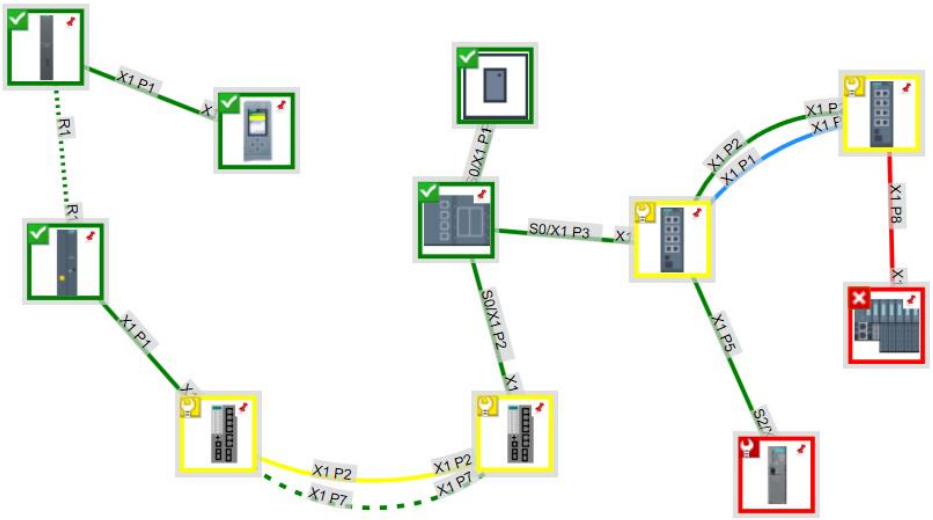
The mode you are currently in is indicated by the associated control element in the toolbar.

- Editing mode is indicated by the icon.
- Online mode is indicated by the icon.

When you click the control element, SINEMA Server switches to Online mode.

Testing the monitored topology

The monitored topology helps you monitor your network. In the following screenshot, the connection to the ET 200SP was removed in the reference system for test purposes.
SINEMA Server detects the status change and displays the error.



© Siemens AG 2017 All rights reserved

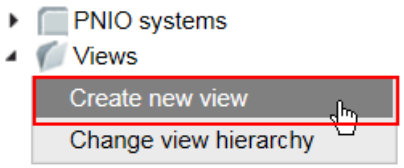
6.2.4 Setting up views

In the monitored topology, a very large hierarchy of the network topology can become cluttered.

SINEMA Server allows you to separately monitor individual parts of the total monitored network, for example VLAN 2 from the reference system of this description (see Chapter 1.2).

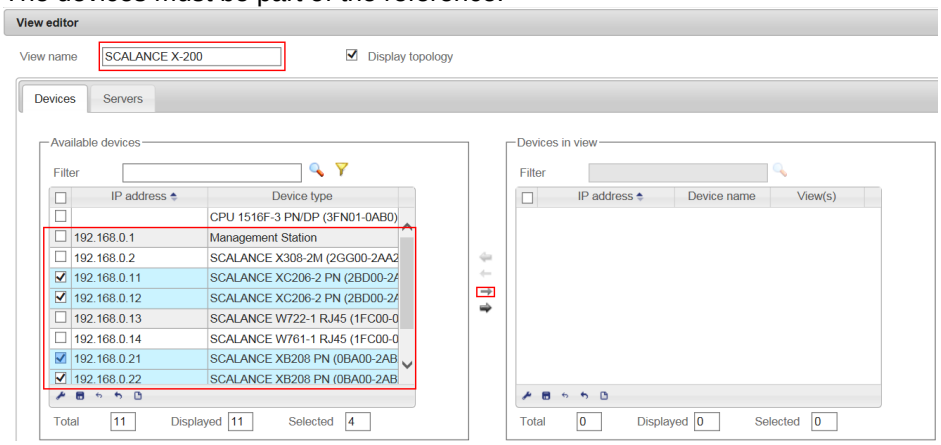
To create a view-specific topology, proceed as follows:

1. In the device tree, select the “Views” node. Right-click to select the “Create new view” menu command.



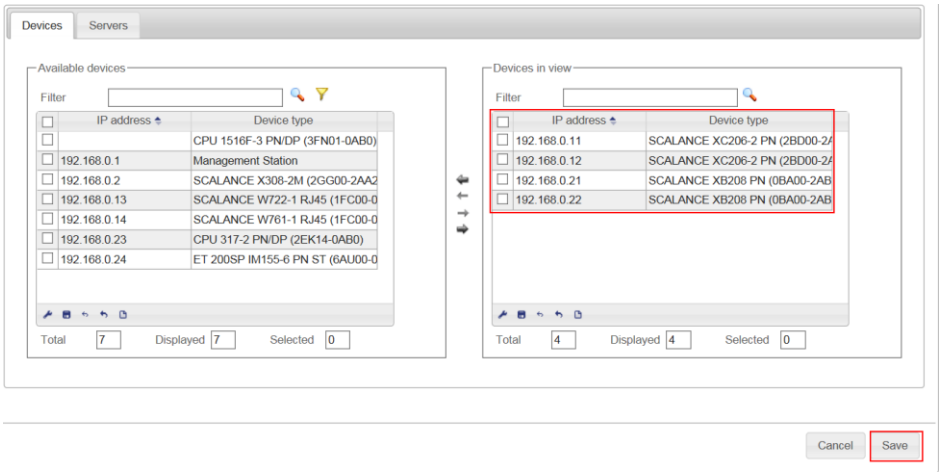
2. The View editor opens. Assign a name to the new view.
   The left column displays all available devices. As an example, select all SCALANCE X-200 devices. Use the arrow to transfer your selection to the right column. This adds the selected devices to the user-defined view.

   Note:
   The devices must be part of the reference.



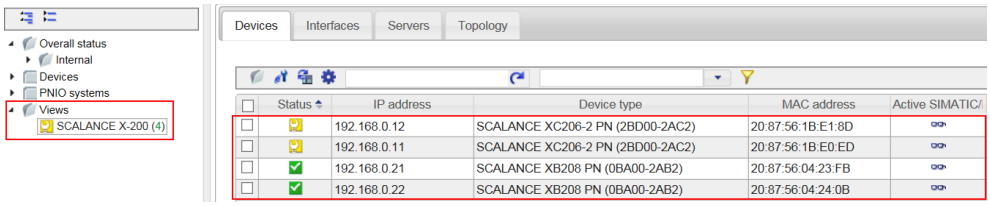
© Siemens AG 2017 All rights reserved

3. When you have applied all devices that belong to the SCALANCE X-200 family to the right column, select “Save” to save the view.

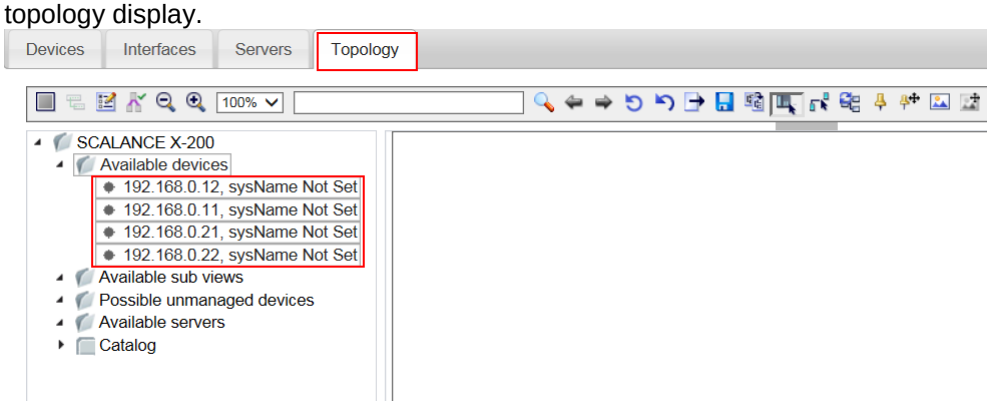


Result

You have created a new view, “SCALANCE X-200”. The “Devices” tab lists all devices that belong to this view.

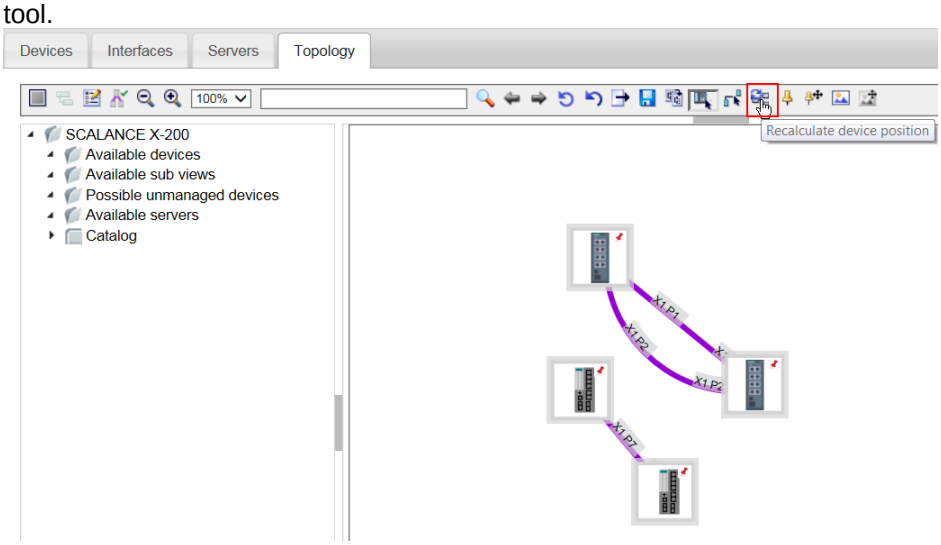


4. Go to the “Topology” tab. The “Device hierarchy” dialog area displays all devices of this view. Use drag and drop to insert these devices into the topology display.

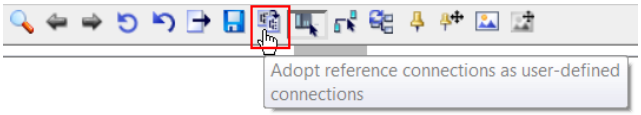


© Siemens AG 2017 All rights reserved

5. The devices appear in the view area in Editing mode.
   To get a structured display, click the highlighted “Recalculate device position” tool.



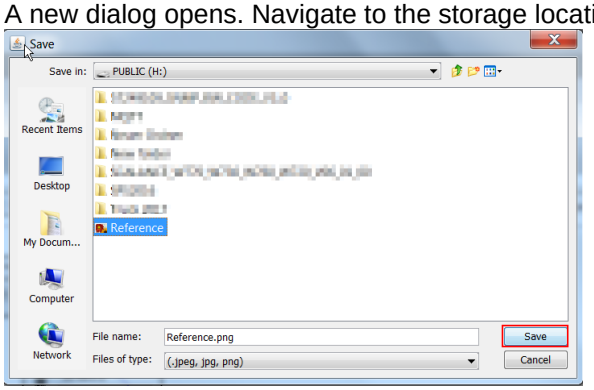
6. The connections from the reference are automatically applied to each view, provided that the connections exist. In each view, you can choose whether or not to display the reference connection in active mode. You can also redraw a connection or edit an existing connection.
   To apply all existing reference connections to the user-specific view, click the highlighted “Adopt reference connections as user-defined connections” tool in the toolbar.



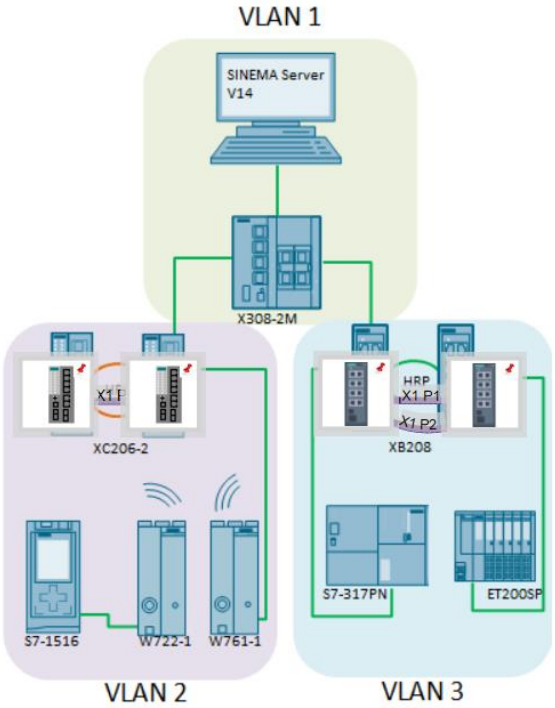
© Siemens AG 2017 All rights reserved

7. You can select a background image for the view. Click the highlighted “Insert background picture” tool.

8. A new dialog opens. Navigate to the storage location of the image and open it.

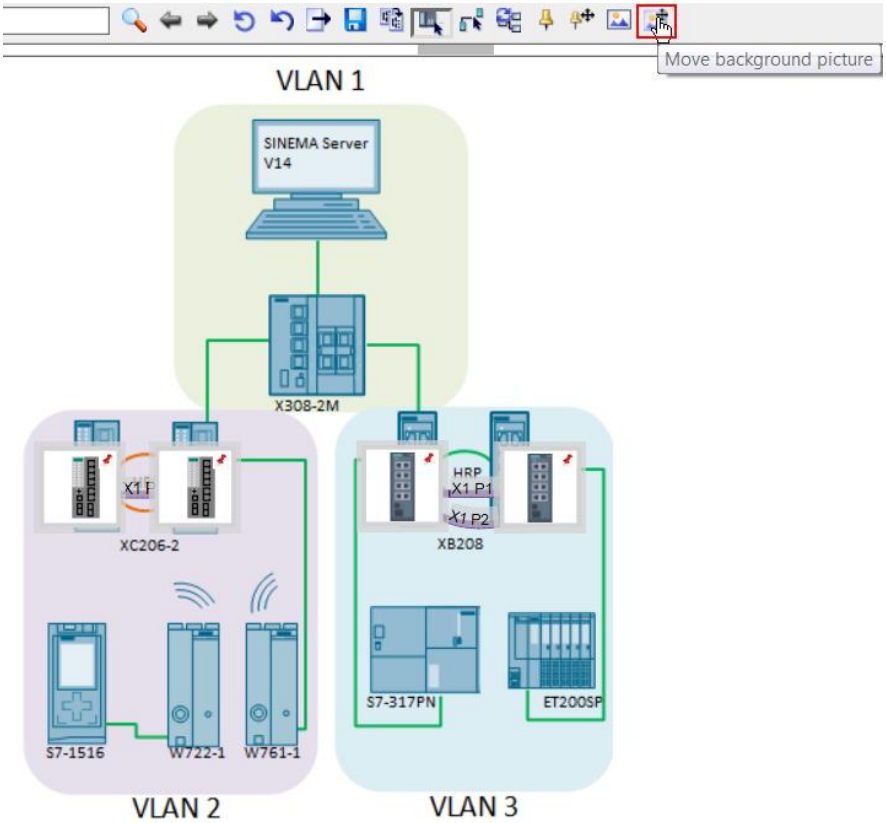


9. The image is inserted into the view. Rearrange the devices as needed. To do this, enable the “Select” tool. While holding down the left mouse button, position the cursor on the device and move it to the desired position.
Place, for example, the SCALANCE devices on the corresponding background image icon.

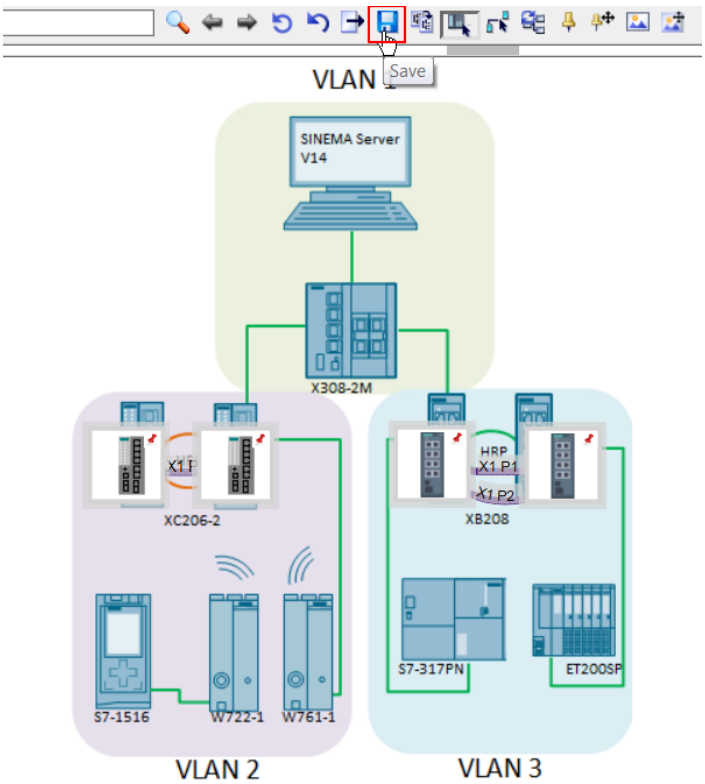


© Siemens AG 2017 All rights reserved

10. The “Move background picture” tool allows you to move the background image.

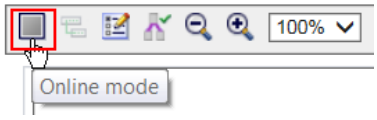


11. Use the highlighted tool to save the view.



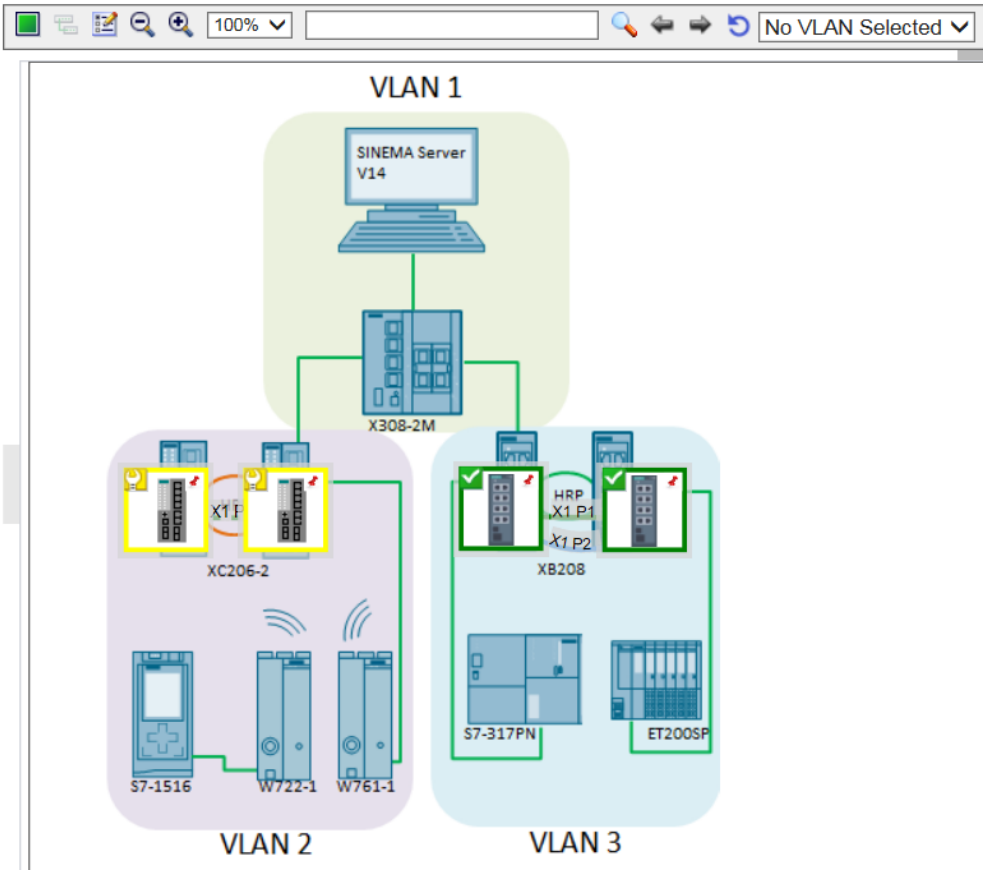
© Siemens AG 2017 All rights reserved

12. To use the view for monitoring, click the highlighted “Online mode” tool. Online mode displays the items inserted in Editing mode with their monitoring statuses for devices and ports and the user-defined connections drawn between them. Online mode does not display reference connections.



Result

You have created a new view, “SCALANCE X-200”, and enabled it for monitoring.



© Siemens AG 2017 All rights reserved

7 Appendix

7.1 Service and Support

Industry Online Support

Do you have any questions or do you need support?

With Industry Online Support, our complete service and support know-how and services are available to you 24/7.

Industry Online Support is the place to go to for information about our products, solutions and services.

Product Information, Manuals, Downloads, FAQs and Application Examples – all the information can be accessed with just a few clicks:
https://support.industry.siemens.com

Technical Support

Siemens Industry's Technical Support offers you fast and competent support for any technical queries you may have, including numerous tailor-made offerings ranging from basic support to custom support contracts.

You can use the web form below to send queries to Technical Support:
www.siemens.com/industry/supportrequest.

Service offer

Our service offer includes the following services:

- Product Training
- Plant Data Services
- Spare Part Services
- Repair Services
- Field & Maintenance Services
- Retrofit & Modernization Services
- Service Programs & Agreements

For detailed information about our service offer, please refer to the Service Catalog:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

The "Siemens Industry Online Support" app provides you with optimum support while on the go. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

© Siemens AG 2017 All rights reserved

7.2 Links and literature

Table 7-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109746780
\3\	SINEMA Server V14 software (including 21-day trial license) download https://support.industry.siemens.com/cs/ww/en/view/109749138
\4\	SINEMA Server Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109748925

7.3 Change documentation

Table 7-2

Version	Date	Modifications
V1.0	08/2017	First version

© Siemens AG 2017 All rights reserved