SIEMENS

SIMATIC NET

SINEMA Server

Configuration Manual

06/2011
C79000-G8976-C241-01

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the relevant information is not taken into account.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: C79000-G8976-C241-01
℗ 06/2011

Copyright © Siemens AG 2011.
Technical data subject to change

Table of contents

Introduction 1

1.1 Information in this manual

About this manual

This manual provides you with information about monitoring devices connected to the network using the SINEMA Server application. It also contains detailed information about setting up and managing events and views as well as network administration and managing device topology.

Validity

This manual is valid for SINEMA Server - Basic V11.0 software applications.

Content of the manual

This configuration manual provides the following information that you require to work with SINEMA Server:

- Description of SINEMA Server

  This section gives you an overview of the purpose and advantages of SINEMA Server. It also lists the network devices supported by SINEMA Server. The section also outlines the software and hardware requirements for SINEMA Server.

- Installation

  In this section you will learn how to install and uninstall SINEMA Server.

- Information about the network

  This section provides standard users with valuable information on how to monitor the network with SINEMA Server.

- Network administration with SINEMA Server

  This section is intended for network administrators and describes the various network administration functions available with SINEMA Server. This information shows users how to manage the network using SINEMA Server.

- Using and filtering events

  When managing network devices, it is clear that changes in the device status or the way in which the device functions may occur. This section explains how network administrators can view all events and get a fast overview of the device status based on the type of event. Events can also be filtered to show the list of events for a particular week or month or for a specific period of time.

Required experience

To be able to put both SINEMA Server and this configuration manual to optimum use, you should be familiar with the following topics:

- Industrial Ethernet networks
- Configuring network devices

Locating information in this manual

To help you find information about specific topics of interest, the table below is intended as a guide to the manual.

Topic	Chapter, section	Location
Viewing all network devices	Configuration, viewing and monitoring the network	5.1.7
User-defined maps	Configuration, viewing and monitoring the network	5.1.6
Viewing event statistics	Configuration, using and filtering events	5.3.5
Network performance reports	Configuration, generating reports	5.4.3
Managing views	Configuration, network administration	5.5.6
Emergency license	Licensing, overview	3.2
Installing SINEMA Server	Installing the software, installing SINEMA Server	3.1

Description 2

2.1 Purpose and advantages of SINEMA Server

Purpose of SINEMA Server

In the current IT market, most of the network management tools are designed for the needs of IT enterprise networks and not for industrial networks. The standard IT network management tools cannot be used for all industrial networks, because they are expensive and too complicated for the plant and maintenance staff.

SINEMA Server is Web-enabled network management software designed by Siemens for use in Industrial Ethernet networks. SINEMA Server allows simple and efficient monitoring of network information and provides fault diagnostics and monitoring of the performance of distributed network devices in an industrial environment. The application provides accurate information based on changes occurring in the current network. This helps users to reduce the downtimes resulting from network failures during production.

Overview of SINEMA Server

SINEMA Server is a network management software application that is used to monitor and manage the devices and their statuses in Industrial Ethernet networks. SINEMA Server monitors the programmable controllers and wireless devices connected to LANs or WLANs as well as infrastructure components, such as Industrial Ethernet switches and Industrial Wireless LAN access points. SINEMA Server's "Auto discovery" functionality automatically detects not only the controllers and infrastructure components but also their parameters if these are relevant to the network. The software then calculates the network topology and statistics from this information. Users can view this information on the SINEMA Server Web interface. If they wish, users can also obtain more detailed information with additional diagnostics screens.

SINEMA Server queries the data of Ethernet nodes cyclically during operation, and reports network alarms. Changes in the network, faults and availability are logged and archived in a database. The user then has this information available to document and analyze the network with the help of report functions, each of which can be set to a specific period.

Advantages of SINEMA Server

With the various functionalities of SINEMA Server, users can improve their production capabilities and avoid unnecessary production losses in their daily routine. SINEMA Server diagnoses and visualizes Ethernet networks, such as Industrial Ethernet and PROFINET. Network activities are logged continuously and are available to users for evaluation and further processing. This helps SINEMA Server users to identify network failures before they become critical, and to react quickly to faults and critical situations.

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

The major characteristics of SINEMA Server application are as follows:

- SINEMA Server supports the following 32-bit operating systems: Windows XP Professional, Windows 2003 Server, Windows 7.
- It supports both Internet Explorer version 8.0 and Firefox version 4.0 or higher.
- Multiple instances of SINEMA Server Web interface can be opened simultaneously by different users to access the network information.
- Access to the SINEMA Server Web interface is protected by an HTTP and HTTPS protocol and can be made even more secure by password authentication.
- Remote monitoring of network operations, faults, network security and network access.
- Administration of the network and effective monitoring of the discovered network devices.
- SINEMA Server provides support for standard SNMP traps.
- You can create new users and user groups based on the different roles of the people responsible for the various network management activities. You also can create different Web interface views in SINEMA Server and assign these to different users and user groups based on their roles.
- Several users can access the same information at the same time, regardless of their locations in the network.
- The software also features an e-mail client function and an OPC server for forwarding network data and alarms to other systems.
- You can view and generate reports on network devices, as well as on their availability, configuration and performance in the network.
- You can use the export functionality to archive the SINEMA Server project data and configuration data. Similarly, you also can import configuration data into SINEMA Server.
- Users who have access to SINEMA Server also can use the OPC server to view the SINEMA Server configuration data and device properties.
- SINEMA Server can be integrated easily into HMI systems (Human Machine Interface) and visualization systems, such as SIMATIC WinCC. This allows users to monitor the communication in a process visualization system.

Supported devices

SINEMA Server provides full support for the following Siemens devices:

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

This list of supported devices is not a complete list. The devices listed here are examples of the devices supported. It should also be noted that the extent of the support varies considerably depending on the device. For devices that are detected by DCP such as SCALANCE S and other PROFINET devices, only details such as the name, type, IP address and MAC address can be displayed. SNMP-compliant devices provide additional information.

SINEMA Server also provides basic support for Siemens and non-Siemens devices that support protocols such as ICMP, SNMP V1, SNMP V2C, SNMP V3, DCP, ARP and MIBs such as MIB2, LLDP and Bridge MIB.

2.2 System requirements

Minimum hardware requirements

To install the SINEMA Server application, the computer must meet the following hardware requirements:

Parameters	Minimum requirements	Recommended requirements
Processor	Intel Dual Core CPU 2.4 GHz	Intel Quad Core CPU 2.66 GHz
RAM	2 GB	2 GB
Slots	1 PCI or PCIe	1 PCI or PCIe
Network adapters	4 (one onboard NIC) **Note:** SINEMA Server requires one network adapter that cannot be shared.	4 (one onboard NIC) **Note:** SINEMA Server supports a maximum of 4 network adapters.
Hard disk	120 GB or more	120 GB or more

Software requirements

To install the SINEMA Server application, the computer must meet the following software requirements:

Operating systems supported	- Windows XP SP3 (32-bit) - Windows 7 Professional (32-bit) - Windows 7 Ultimate (32-bit) - Windows 2003 Server (32-bit) - Windows 2003 Server R2 SP2 (32-bit)
Browser software	Internet Explorer 8.0 or higher Firefox 4.0 or higher
Java Runtime Environment (JRE)	Version 1.6.0.20 (32-bit) or higher **Note:** The Java Runtime Environment (JRE) software is supplied as part of SINEMA Server setup.

Note

If you use Windows 2003 Server and want to view the Java applet pages of the SINEMA Server Web interface, you will need to disable the Enhanced Security option in the Control Panel > Add or Remove Programs > Add/Remove Windows Components.

Note

If you use the Windows 7 operating system, the name of the computer must be a minimum of 8 characters long and should not contain the hyphen character.

Note

Java VM (JVM) and Java Runtime Environment (JRE) must be installed before you can view the SINEMA Server Web interface pages that contain Java applets. This software is provided as part of the SINEMA Server installation. However, for clients connected to the host device, JRE version 1.6.0.20 needs to be installed. This is required to view the applets correctly.

For users who access the SINEMA Server as a client, the client computer should meet the following requirements:

Browser software	Internet Explorer 8.0 or higher Firefox 4.0 or higher
Java Runtime Environment (JRE)	Version 1.6.0.20 (32-bit) or higher
Monitor resolution	1280 x 1024 pixels

SINEMA Server also supports SIMATIC Microbox IPC427C.

For SIMATIC Microbox IPC427C, the system requirements are as shown below:

Parameters	Minimum requirements
Processor	Intel Core2 Duo CPU U9300 @1.20 GHz
RAM	2 GB
Operating system	Microsoft Windows XP Professional version 2003 service pack 3

Installing the software 3

3.1 Installing SINEMA Server

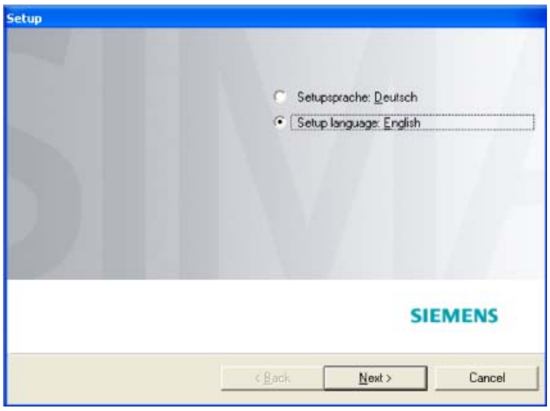
Requirement for installation

To install the SINEMA Server application on your computer, you need administrator privileges.

Installation procedure

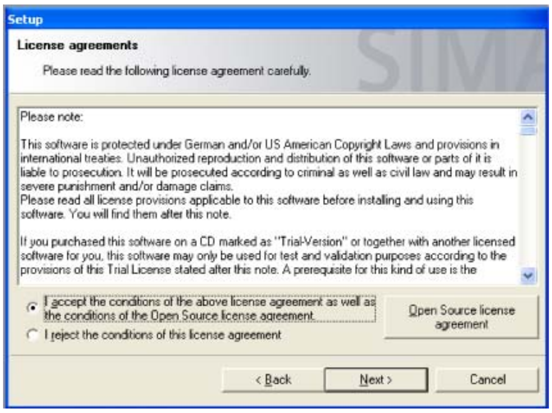
To install SINEMA Server on your computer, follow these steps:

1. Log on to the Windows OS as an administrator. Open the Windows Explorer and double-click on the "Setup.exe" file in the root directory of the installation CD or start the program from the Windows menu **Start > Run**. If the autorun function is enabled for your CD-ROM drive, setup will start automatically.
2. Select the language for the SINEMA Server Setup wizard and click "Next".



○ Setupsprache: Deutsch
● Setup language: English

3. Click the "Open source license agreement" button to view the license agreement information. After reading the license agreement, select the "I accept the conditions of the above license agreement as well as the conditions of the Open Source license agreement" option, and click "Next".



License agreements

Please read the following license agreement carefully.

Please note:

This software is protected under German and/or US American Copyright Laws and provisions in international treaties. Unauthorized reproduction and distribution of this software or parts of it is liable to prosecution. It will be prosecuted according to criminal as well as civil law and may result in severe punishment and/or damage claims.
Please read all license provisions applicable to this software before installing and using this software. You will find them after this note.

If you purchased this software on a CD marked as "Trial-Version" or together with another licensed software for you, this software may only be used for test and validation purposes according to the provisions of this Trial License stated after this note. A prerequisite for this kind of use is the

● I accept the conditions of the above license agreement as well as the conditions of the Open Source license agreement.
○ I reject the conditions of this license agreement

4. Enter the required user information and click the "Next" button.
5. A dialog box opens with the list of programs to be installed.
6. Leave the check box for the SINEMA Server component selected as shown below. To use SINEMA Server, you also require the Automation License Manager.
7. Select the check box for the Automation License Manager. Click the "Readme" button on the right hand side of the dialog box if you require more information about the ALM (Automation License Manager) software.
8. Select the "Storage space" button to view the current storage space of the computer.
9. Click the "Browse" button if you want to change the default target directory and install the application elsewhere.

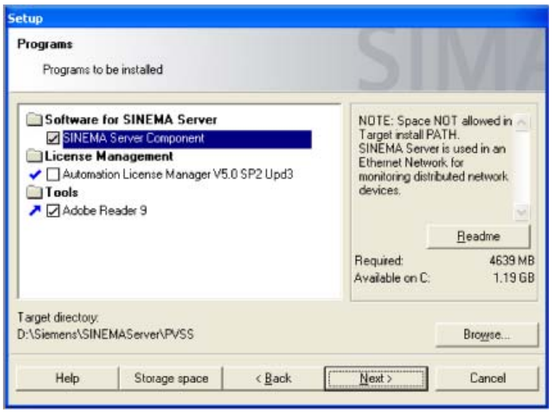
10. Select the location you require and click the "Next" button to start the installation.

Note

The space required for the full installation of SINEMA Server is 4.5 GB. If there is not enough space on the drive, click the "Browse" button and select an alternative location.

Note

If the Adobe Reader is not installed in your PC, you can select the Adobe Reader 9 check box and install it along with the SINEMA Server. Adobe Reader software is required to view the user documentation provided with the application.



Setup

Programs

Programs to be installed

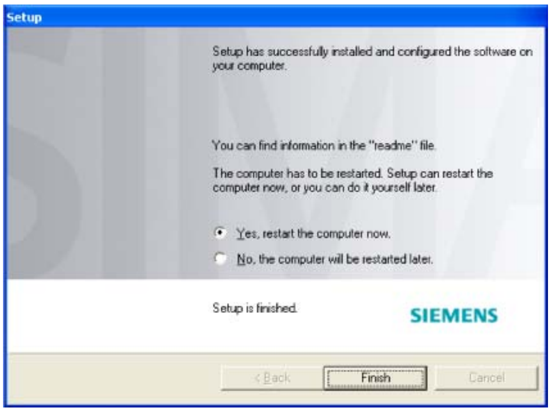
Software for SINEMA Server
☑ SINEMA Server Component
License Management
✓ □ Automation License Manager V5.0 SP2 Upd3
Tools
↗ ☑ Adobe Reader 9

NOTE: Space NOT allowed in Target install PATH.
SINEMA Server is used in an Ethernet Network for monitoring distributed network devices.

Required: 4639 MB
Available on C: 1.19 GB

Target directory:
D:\Siemens\SINEMAServer\PVSS

11. A new dialog opens that guides you right through to the completion of the installation. This may take several minutes.
12. A Setup completion window is then displayed with a status message indicating successful installation of the SINEMA Server application.



Setup

Setup has successfully installed and configured the software on your computer.

You can find information in the "readme" file.

The computer has to be restarted. Setup can restart the computer now, or you can do it yourself later.

● Yes, restart the computer now.
○ No, the computer will be restarted later.

Setup is finished.

13. In the Setup window, you have the option of restarting the computer now or later. Select the option you require and click the "Finish" button to complete the installation.

3.2 Licensing Information

Licensing information

A SINEMA Server license is required to allow you to run this application. A default trial license ships with the application. The SINEMA Server application generates a trial license automatically. This trial license can be extended by upgrading to a new license type. The following five types of license are available for SINEMA Server:

- Basic 250: This license supports a maximum of 250 monitored nodes.
- Basic 100: This license supports a maximum of 100 monitored nodes.
- Basic 50: This license supports a maximum of 50 monitored nodes.
- Emergency 50: This license supports a maximum of 50 monitored nodes.
- Trial 50: This license is a trial version and supports a maximum of 50 monitored nodes.

The Basic license is used only for production purposes. If the basic license becomes corrupted, an emergency license can be used. The emergency license provides additional validity for 14 days.

Note

With the license types listed above, the maximum number of monitored nodes does not include the management stations.

Note

The SINEMA Server V11 Trial 50 license is valid for 21 days only. Once the trial version has been activated on the computer, it cannot be used again. The trial license provides all features that are available with any other license type with support for 50 nodes.

Note

If you start SINEMA Server the first time without a valid license key, the application setup will automatically install and activate this trial license on your computer.

Automation License Manager

You can use the Automation License Manager (ALM) program to handle the SINEMA Server license. This program is used to manage the license keys. Software products requiring license keys automatically report this to the Automation License Manager. If the ALM finds a valid license key for this software, the software can be used according to the end user license agreement.

After installing SINEMA Server, you can access the documentation for this program by selecting **Start > SIMATIC > Documentation** from the Windows menu.

Storage location for license keys

You can store license keys on storage media such as license key sticks, on removable drives (but not on CD, CDRW) or USB memory sticks. License keys can be located locally on your own computer.

License upgrade

To extend the license period or to support a higher number of monitored nodes, you need to upgrade to a new license. To run a license upgrade, the upgrade license key must be available for access by the Automation License Manager.

The license types can be combined allowing you to use 2 or 3 different license types.

1. Basic 50 plus Trial 50 counts as Basic 50

- Basic 50 plus Emergency 50 counts as Basic 50
- Emergency 50 plus Trial 50 counts as Emergency 50

Additional license

1. Basic 50 plus Basic 50 counts as Basic 100
2. Basic 50 plus Basic 50 plus Basic 100 counts as Basic 200
3. Basic 100 plus Basic 100 plus Basic 100 counts as Basic 250

Note

The current version of SINEMA Server supports a maximum of 250 devices.

To upgrade a license key, follow these steps:

1. Select the View > Management menu command.
2. In the navigation area, select the location of the license key you want to upgrade.
3. In the object area, select the license key to be upgraded.
4. Select the License key > Upgrade menu command.

License downgrade

A license downgrade is possible if you have at least one license type available. To downgrade, however, you need a license type higher than Basic 50. If, for example, you have basic 50 + basic 50 (2 licenses), you can downgrade to 1 license type.

To downgrade a license type, follow these steps:

1. Stop SINEMA Server and its related services. You can do this in the Monitor panel.
2. Select the View > Management menu command.

3. In the navigation area, select the location of the license key you want to downgrade.
4. Select the License key > Transfer menu command to transfer the license key to another user.

Note

There must be at least one license type still in the navigation area after the downgrade.

3.3 Uninstalling SINEMA Server

Uninstalling

To uninstall SINEMA Server V11 Basic, follow these steps:

1. On the Windows taskbar, click **Start > Control Panel** to open the Windows Control Panel.
2. From the Control Panel window, open the Add or Remove Programs dialog box.
3. In the Add or Remove Programs dialog box, on the left pane, click Change or Remove Programs.
4. Under the "Currently installed programs" list, select SINEMA Server V11 Basic.
5. Click the Remove button. When you are prompted to confirm removal, click "Yes" to uninstall SINEMA Server from your system.

Note

When you uninstall, if you want to retain the valid license key, you can do this by opening the Automation License Manager and saving the license on a separate medium. You can, however, also transfer the license to other users.

Note

When you uninstall, setup will remove the files and folders. If the folder that is being uninstalled is still open in the Windows Explorer, an error message will be displayed. To avoid this, make sure that the folder you are uninstalling is closed.

Software user interface 4

4.1 Basic steps for operation

Starting SINEMA Server

You can start the SINEMA Server services using the following two options:

- **Using Start SINEMA Server services:**

  Use this option when the SINEMA Server is already configured.

  On the Windows taskbar, click **Start > All Programs > Siemens Automation > SINEMA Server > Start SINEMA Server** to start SINEMA Server.

- **Using SINEMA Server Monitor panel:**

  Use this option if you want to start/stop the SINEMA Server application via an interface that displays the application runtime status with status messages.

  Once SINEMA Server has started, this monitor panel will run as a tray icon. On the Windows system tray, right click on the SINEMA Server icon to access the SINEMA Server Monitor panel. A pop-up menu appears with a list of entries with which you can start a Web client, start/stop SINEMA Server and view the status and configuration information.

Note

If you are using the Windows 7 operating system, you need to run the Start SINEMA Server program with administrator privileges.

Note

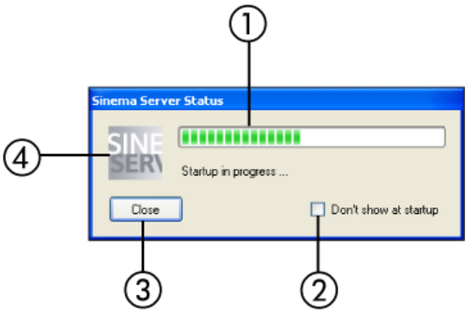
Once the SINEMA Server application has been started, you should not make any changes to the system date/time or move the date backwards to the past or forwards to the future. Such changes to the system date/time would lead to other side-effects.

Note

The computer running the SINEMA Server application is known as a management station. Make sure that the management station does not change to suspend or hibernate mode. This will result in unpredictable behavior relating to device state calculations and reachability status. If this does occur, however, remember that the application needs to be restarted.

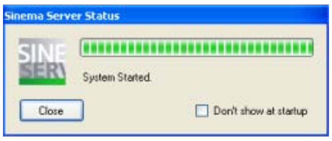
SINEMA Server Monitor panel

The SINEMA Server Monitor panel helps when monitoring the loading status and includes options for starting or stopping the SINEMA Server application. This Monitor panel is loaded by default and is a part of Windows startup. This panel starts the SINEMA Server application automatically without any user action. Initially, you will see that the SINEMA Server Status dialog box is displayed on the Windows desktop that displays a progress bar indicating the status of the application being loaded.



1. Progress bar
2. Startup - Enable/Disable option
3. Close button
4. Status icon

To hide the SINEMA Server Status window, click the "Close" button. The status window can be shown again by right clicking on the system tray icon and selecting the "Status" option from the Monitor panel shortcut menu. The SINEMA Server Monitor icon changes to green indicating that the SINEMA Server application has been started successfully.



Note

If you do not want to view the Monitor panel window the next time you start Windows, you can select the "*Do not show at startup*" check box.

SINEMA Server Monitor panel status

After starting the application, the SINEMA Server icon SINE SERV is shown in the system tray. Even after closing the Monitor panel dialog box using the "Close window" button, the application remains running in the background. The color of the icon indicates its status. The status icons and their meaning are shown below:

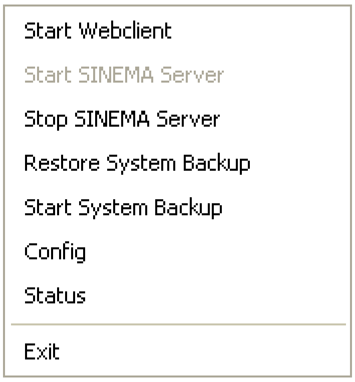
Icon	Description
SINE SERV	SINEMA Server - starting
SINE SERV 🟩	SINEMA Server has started
SINE SERV 🟥	SINEMA Server - error
SINE SERV 🟨	SINEMA Server - warning

If the application detects errors, SINEMA Server will change to an error status. This can be seen in the SINEMA Server Monitor panel system tray icon and is indicated by the color of the thin line. Before you can work any further with the application, you will need to restart it. This is possible with the Stop and Start options in the shortcut menu.

An emergency mode may occur if there are not enough computer memory resources to run the application. The emergency mode status is displayed in the SINEMA Server Monitor panel status dialog. To be able to use this application, restart SINEMA Server using the Monitor panel shortcut menu options.

SINEMA Server Monitor panel options

The SINEMA Server Monitor panel is available as an icon in the Windows system tray. To access this panel, right click on the icon and select the required option. A window containing the various options is displayed as shown below.

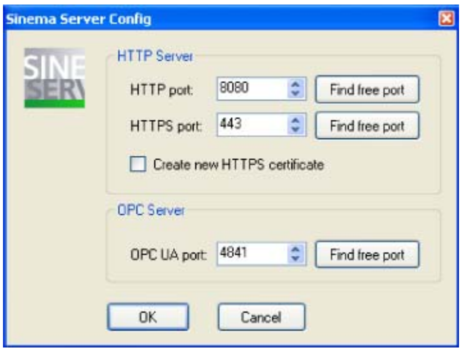


The following list of options is available with the SINEMA Server Monitor panel:

1. Start Web client:
   - Starts the local Web browser to display the SINEMA Server Web interface.
   - Tip: The menu item is disabled until SINEMA Server is started.
2. Start SINEMA Server:
   - Starts the SINEMA Server application and its related services.
   - Tip: The menu item is disabled while SINEMA Server is starting or has already been started.
3. Stop SINEMA Server:
   - Stops the SINEMA Server application and its services.
   - Tip: The menu item is disabled while SINEMA Server is stopped.
4. Restore system backup:
   - Restores the system to a previous state.
5. Start system backup:
   - Starts system backup and puts the data in a zip file.
6. Config:
   - Opens the SINEMA Server configuration dialog box. This includes HTTP server configuration options including an option for configuring UA ports. HTTP server configuration provides 3 options - HTTP, HTTPS and "Create new HTTP certificate".
7. Status:
   - Displays the Status dialog box that indicates the status of SINEMA Server.
   - While SINEMA Server is starting, the startup dialog is displayed.
   - If SINEMA Server has already been started, the dialog box will indicate that the system has been started.
8. Exit: Closes the SINEMA Server Monitor panel application and displays the Stop progress window.

Configuring a normal port, secured port and OPC UA port

To start using the SINEMA Server application in a Web browser, the port settings can be configured to use this application both in HTTP and HTTPS environments. Usually, by default the normal port settings for HTTP include port number 80 being used as the default port. This can be modified using SINEMA Server Monitor panel shortcut menu options if you do not want to use the standard settings.



Sinema Server Config

HTTP Server

HTTP port: 8080

HTTPS port: 443

☐ Create new HTTPS certificate

OPC Server

OPC UA port: 4841

The shortcut menu is accessed by right-clicking on the SINEMA Server Monitor tray icon and selecting the "Config" option. The following settings can be configured using the "Config" option:

- Reconfigure HTTP server settings
- Create new HTTPS certificate
- Configure OPC UA port

In the SINEMA Server Config window, specify the HTTP port number and HTTPS port number to reconfigure the HTTP server settings and then click OK. If the port number is already being used by another machine, click "Find free port" to locate a free port. This option automatically selects another available port number and updates the port number in the text box.

Note

When HTTP port 80 is being used by another process, a warning message "*HTTP port (80) is used by another process*" appears in the status window color-coded yellow. In this situation, it is advisable to change the port using the "Find free port" option in the SINEMA Server Config window.

Note

To obtain a list of processes using port 80, you can use the following command:

```
netstat -noa | findstr :80
```

Note

The HTTP port can be disabled by setting the port to zero in the SINEMA Server Config window. To disable the HTTP port, enter zero in the text box and click OK.

To provide further support for HTTPS connections, SINEMA Server setup also includes the generation of HTTPS certificates. Once this setup has been started on a computer, it automatically generates this certificate based on the IP address and computer name. If either the IP address or the computer name has been changed, the certificate has to be generated again. If you want to generate this certificate again, click the "Create new HTTPS certificate" check box.

The default port used for the OPC UA server is 4840. The default port can, however, be reconfigured using SINEMA Server Config. In the Config window, specify the UA port and click OK to apply the changes. Click "Find Free Port" to locate the next available port if the existing port number is already in use. Click OK to apply the changes.

Using third-party certificates

This certificate can be found in the following folder:

Siemens\SINEMAServer\PVSS\Sinema_Server\config

- certificate.pem - self-signed certificate
- privkey.pem - private key related to the certificate

To obtain a verified certificate, you will need to send the self-signed certificate to VeriSign or any other trusted organization to have it signed. This is necessary if you want to use the certificate at a later point in time. The other option is to use a certificate that has already been signed.

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

Siemens\SINEMAServer\PVSS\Sinema_Server\config

Note

The SSL certificate must be stored with the name "certificate.pem"

Reserved port numbers

SINEMA Server uses the following ports as the default ports for communication. Note, however, that two different programs cannot communicate over the same port. For example, when other SIMATIC applications or devices connect to one of the ports, this port might not be free for SINEMA Server. To avoid this problem, we recommend that you keep a track of the ports used by SINEMA Server and keep them free during such communication in the network.

This means it is important to make sure that these ports are available for SINEMA Server during startup and also while the application is running. A list of default ports used by SINEMA Server is provided below:

Default ports	Port description
80	HTTP server / Java
161	SNMP
162	SNMP traps
443	HTTPS
4897	Data
4998	Events
4999	Monitor

By default, the SINEMA Server application setup enters a list of processes in the firewall exception list. Below, you will find the list of processes that need to be opened by the application to allow the firewall ports to communicate.

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

Note

If a customized firewall is used, a system administrator will need to configure the firewall settings as outlined above.

Logging on to SINEMA Server Web interface:

Once the SINEMA Server application has started, you can use the Web browser or Monitor panel options to log on to the SINEMA Server Web interface.

This Web interface can be accessed from a host computer or using a client machine. The host computer acts as a host that includes the SINEMA Server installation. The Web interface can also be accessed from a client machine (concurrent user) using the IP address of the host computer. If you are using a port other than the default port 80, the port number has to be entered as well along with the IP address. A colon ":" separator needs to be inserted between the IP address and port number.

Note

To view the SINEMA Server Web interface pages that have Java applets, the Java Runtime Environment (JRE) version 1.6.0.20 must be installed on the client computers.

Note

Concurrent users

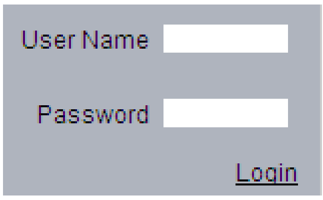
For one host computer, SINEMA Server V11 Basic supports remote access by ten concurrent users. This means that one installation of SINEMA Server can be used by a maximum of ten concurrent users for remote monitoring of network operation.

To log on to the SINEMA Server web interface, follow theses steps:

1. Open the Web browser (either Internet Explorer version 7.0 or Firefox version 3.6.8).
2. If you are accessing the SINEMA Server from the computer on which SINEMA Server is installed locally then enter **http://localhost** or **https://localhost** (if you are using secured port) in the address bar of the browser, and click "Go" to view the login page for the SINEMA Server Web interface.

   Or

   If you are accessing the SINEMA Server as a client from another computer, enter the IP address of the computer on which SINEMA Server is installed in the address bar, and click "Go" to view the login page for the SINEMA Server Web interface.
3. When you access the SINEMA Server Web interface as a client (concurrent user) from another computer, make sure that the SINEMA Server and its related services have been started on the host computer on which SINEMA Server is installed. You can check this in the "SINEMA Server Monitor status panel" window.
4. Enter the user name and password in the *Name* and *Password* text box available in the second level header and click the "Login" link.

   If the authentication is successful, you have access to the SINEMA Server Web interface. The text boxes in the second level header are replaced by the logged on user's name and the Logout link.

While SINEMA Server is running, we strongly recommended that you avoid a forced shutdown or restart of the application. If this happens, it is possible that the SINEMA Server database will be corrupted. As a result of this, the application will no longer start properly and the only way to recover is to reinstall the application. To avoid data loss in such situations, it is advisable to back up the system regularly. This data can then be retrieved using the restore function.

Selecting the language of the user interface

The language selection list box is available in the top right corner of the first level header. The SINEMA Server application is available in English and German. To change the language, click on the drop-down list box and select the language you require. The text and the user interface elements of SINEMA Server are displayed in the selected language.

Viewing SINEMA Server pages the first time

In SINEMA Server, three predefined user groups are available - Administrator, Power user and Standard user. You can log on to the SINEMA Server application using any of these three predefined user groups. The required user name and password are shown in the table below:

User group	Login information
Administrator	• User name: Administrator • Password: SinemaA
Power user	• User name: Coordinator • Password: SinemaP
Standard user	• User name: Operator • Password: SinemaS

After logging on with the system the first time, a dialog box is displayed that provides options for changing the existing password or keeping the same password for the logged-on user. **Please change the password once you have logged on to the application.**

For more information about these predefined user groups, access rights information and creating/managing users, please refer to *"User administration", section 5.5.2*

After logging on, the SINEMA server application opens specific pages within the application where you can make some of the basic settings required. These are necessary before you can work with the devices in the network. The following list of SINEMA Server application pages will be enabled in the application and their page contents will be displayed in the main window:

- Events (all sub-links)
- User admin
- Network settings
- Import/export

Note

Except for those mentioned above, the SINEMA Server pages are disabled while these pages are edited for first time.

The most important task before being able to use this application for the first time is to scan the devices in the network. This involves specifying settings in the Network settings menu - Device detection tab and Scan settings tab. The next section contains basic information about scanning the network.

For detailed information on network settings, refer to *"Network settings" section 5.5.3*.

Scanning the network

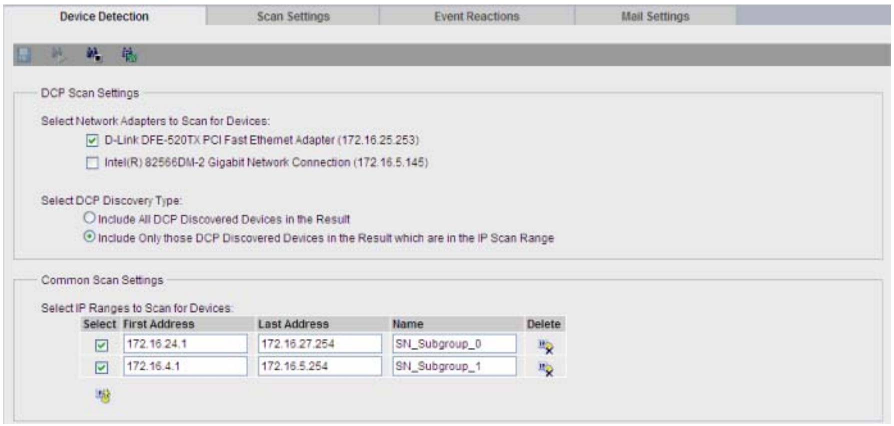
With the SINEMA Server Web interface, the information relating to detected devices in the network is displayed by various SINEMA Server Web interface pages. You can use this information to monitor and maintain the performance of distributed network devices. In the SINEMA Server application, the scan operation will detect all managed and unmanaged network devices based on the selected scan ranges.

Before starting the scan for the first time, we recommend that you modify the scan range configured in "Common scan settings" of the "Admin > Network settings > Device detection" tab. By default, SINEMA Server calculates the start and end of the IP range based on the subnet mask configured in the network interface card.

Note

The IP addresses shown in the screenshot below are simply suggestions. You should adapt the IP address ranges to suit the real network environment.

If you do not adapt the scan range and the scan range is very large, device scanning will take longer to complete. If the scan range includes more than 500 devices that need to be configured in the network, a notification message will alert you about the scan time. We therefore recommend that you specify the IP address range in small sub-groups (instead of a large single group) up to a maximum of 20 sub-groups if the IP addresses are scattered. This will help to speed up the scanning of the devices.



DCP Scan Settings

Select Network Adapters to Scan for Devices:

☑ D-Link DFE-520TX PCI Fast Ethernet Adapter (172.16.25.253)

□ Intel(R) 82566DM-2 Gigabit Network Connection (172.16.5.145)

Select DCP Discovery Type:

○ Include All DCP Discovered Devices in the Result

● Include Only those DCP Discovered Devices in the Result which are in the IP Scan Range

Common Scan Settings

Select IP Ranges to Scan for Devices:

Select	First Address	Last Address	Name	Delete
☑	172.16.24.1	172.16.27.254	SN_Subgroup_0	
☑	172.16.4.1	172.16.5.254	SN_Subgroup_1	

To scan the network, follow these steps:

1. On the SINEMA Server menu bar, click the **Admin > Network settings > Device detection** tab.
2. On the Device detection tab, select or enter the required values for the DCP scan, discovery type and IP range parameters and save the settings.
3. On the Scan settings tab, enter the values required to start the scan such as, Scan interval, DCP timeout, ICMP timeout and SNMP settings.
4. Click the "Start scan" button to begin scanning the network. The network will be scanned based on the scan ranges of the subnets selected on the **Admin > Network settings > Device detection** tab.
5. The progress of the scan is indicated by an icon on the right-hand side of the second level header.
6. After the scan has been completed, all the detected network devices are displayed along with their status on the **Network > Devices** page.

Note

In DCP Scan settings, if you choose the option "Include all devices discovered by DCP in the result", it is possible that DCP devices that are outside the IP range(s) but within the subnet(s) connected to the NIC(s) will also be discovered.

If the SINEMA Server application is stopped during scanning and if SINEMA Server is then started, there may be inconsistent responses in the application. As a result, you may find that the discovered network devices do not change to the monitored status. The information in Device details and Device topology may also not be available. To avoid this, keep to the following rules during scanning:

- Before stopping SINEMA Server, make sure that scanning has not started
- If auto scan is running, delete devices found during the scan and scan the network again

Note

While the SINEMA Server application is running, it is advisable not to modify the system date or time in any way. This will affect the application and cause unwanted side-effects.

How topology identification reacts

On completion of network scanning, the actual network topology representing management station, devices, ports, connection lines and their connection status are shown on the Actual topology page. The topology scan feature provided by the SINEMA Server application is always coupled with a network scan. Whenever a network scan is completed, the topology scan is triggered automatically. As a result, the changes in connections (new connection(s) or modified connection(s)) can be easily identified on completion of either manual network scan or a periodic auto scan of network.

Note

To scan a specific set of devices within the network for changed SNMP values, we recommend that you use the "Force read SNMP data from device" icon. This icon exists in all the tabs of the Device details page.

Network topology discovery is based on SNMP information provided by the device. If a device supports SNMP, connection lines are displayed for devices with LLDP MIB support. Hence, LLDP and bridge information will be useful to identify the topology of network.

However, if SNMP protocol support is disabled on a device, topology identification for this device will be based on neighboring devices. If neighboring device(s) support LLDP / bridge, then the connection to the relevant device can be identified. As a result, in the topology view and the device details view, the maximum number of ports will be based on the highest number of connections identified to this device.

In the case of a management station, even though it supports LLDP / bridge, this data will not be used for topology discovery. If neighboring device(s) support LLDP / bridge, then the connections to the management station can be identified.

Note

To get an accurate count of ports and connection information, it is advisable to enable the SNMP protocol for the relevant device(s).

With a device that does not support the SNMP protocol, if connections can be identified based on the neighboring devices, the value of the connection to this device will be set by default to port index 1. Even though there may be multiple ports and multiple connections to this device, a maximum of 1 connection will be identified and port index will always be 1.

Searching for a device

The "Search for device" box is in the center of the second level header. To search for a device in the network, enter any of the following parameters in the "Search for device" box and press Enter.

- IP address
- MAC address
- Subnet
- Device type
- Vendor type
- Device name

Based on the selected parameter, the device or devices will be displayed in the main window.

Quick links

Any Web page of the SINEMA Server application can be added as a quick link for fast user reference. You can add quick links to give you fast access to Web pages. To add pages as quick links, follow these steps:

1. On the SINEMA Server Web interface, browse to the page you want to have added as a quick link.
2. Type a name for the link in the text box on the right-hand side of the second level header. Click the "Add as quick link" icon to add the Web page as a quick link.

   The created link appears as a table on the Quick links page.
3. Every link name is a hyperlink to the corresponding Web page. When you click on the link, the linked page is loaded in the main window.

Note

You can add a maximum of ten links as quick links.

Note

Refer to *section 4.3, "User interface elements"* for more information about user controls and icons shown in the second level header.

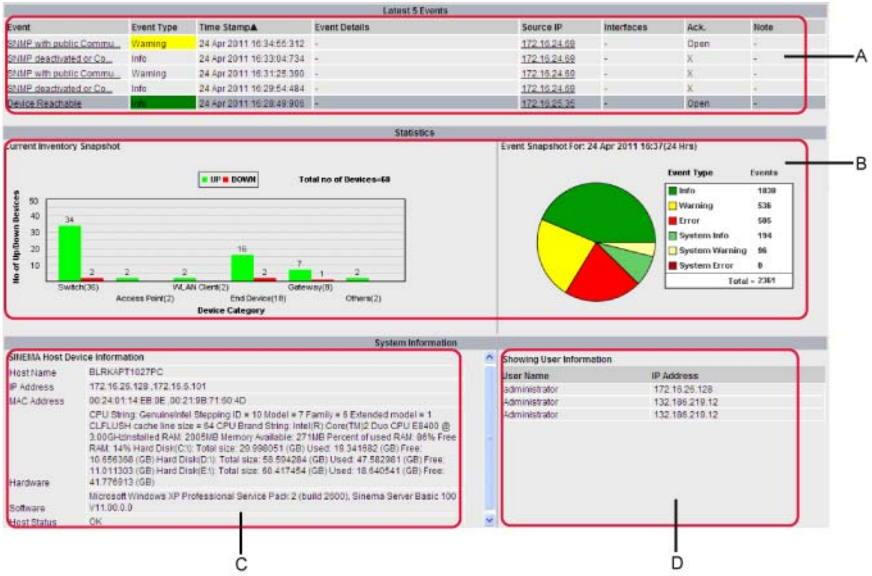
4.2 SINEMA Server home page

Overview

The SINEMA Server home page provides a quick overview of newly generated events including a graphical view of the device inventory and classification of events represented as graphs. On the SINEMA Server home page, you can also see important details about the network, such as the latest events, information about the network statistics and details of the host computer on which the SINEMA Server application is running.

The information presented on the SINEMA Server home page helps to make administrative activities more efficient. The graphs included on this home page represent a simple means of determining the number of devices based on their categories as a whole and recognizing the number of times an event occurred and the related event type.

This information is displayed in the following four sections on the SINEMA Server home page:



Latest 5 Events

Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
SNMP with public Commu...	Warning	24 Apr 2011 16:34:55:312	-	172.16.24.69	-	Open	-
SNMP deactivated or Co...	Info	24 Apr 2011 16:33:04:734	-	172.16.24.69	-	X	-
SNMP with public Commu...	Warning	24 Apr 2011 16:31:25:390	-	172.16.24.69	-	X	-
SNMP deactivated or Co...	Info	24 Apr 2011 16:29:54:484	-	172.16.24.69	-	X	-
Device Reachable	Info	24 Apr 2011 16:28:49:906	-	172.16.25.36	-	Open	-

Statistics

Current Inventory Snapshot

Event Snapshot For: 24 Apr 2011 16:37(24 Hrs)

Event Type	Events
🟩 Info	1030
🟨 Warning	536
🟥 Error	505
🟩 System Info	194
🟨 System Warning	96
🟥 System Error	0
	Total = 2361

System Information

SINEMA Host Device Information

Host Name	BLRKAPT1027PC
IP Address	172.16.25.128 ,172.15.5.101
MAC Address	00:24:01:14:EB:0E ,00:21:9B:71:60:4D
Hardware	CPU String: GenuineIntel Stepping ID = 10 Model = 7 Family = 6 Extended model = 1 CLFLUSH cache line size = 64 CPU Brand String: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHzInstalled RAM: 2005MB Memory Available: 271MB Percent of used RAM: 86% Free RAM: 14% Hard Disk(C:\): Total size: 29.998051 (GB) Used: 19.341682 (GB) Free: 10.656368 (GB) Hard Disk(D:\): Total size: 58.594284 (GB) Used: 47.582981 (GB) Free: 11.011303 (GB) Hard Disk(E:\): Total size: 60.417454 (GB) Used: 18.640541 (GB) Free: 41.776913 (GB)
Software	Microsoft Windows XP Professional Service Pack 2 (build 2600), Sinema Server Basic 100 V11.00.0.0
Host Status	OK

Showing User Information

User Name	IP Address
administrator	172.16.25.128
Administrator	132.186.219.12
Administrator	132.186.219.12

A: Last 5 events

B: Statistics

C: SINEMA host device information

D: User information

A: Last 5 events

In this section, you can view the last five events generated by SINEMA Server. For each event, you can see the event name, event type, time stamp, event details, IP address of the network device for which the event was generated, and the acknowledgement status of the event.

The event types are listed with the event type name highlighted in a separate color for each type. The system info type is shown in green, warnings in yellow and errors in red. This helps you to identify the event type immediately based on the associated color. Additional notes on each of these events provide more information about the event and these can be viewed in the last column of the table.

B: Statistics

This section provides a graphical representation of the current network statistics made available within the Inventory snapshot and Event snapshot sub-sections. In the inventory snapshot, a bar graph displays the different device categories available on the X axis and the Y axis shows the corresponding total number of devices that belong to each of these categories. The legend indicates the color code for operational and non-operational devices. The operational devices are shown in green and non-operational devices in red. For each device category, you can see the total number of operational devices and the total number of non-operational.

In the event snapshot, the pie chart representation shows the different event types in slices, each slice indicated by a different color. The legend displays each event type in a separate color and the number of events listed for the specific event type. The total of all events is also displayed in the legend. This information helps in the recognition and management of events relating to the devices in the existing network.

C: SINEMA host device information

The system information section is shown at the bottom of the SINEMA Server home page. This section provides information about the SINEMA host device and displays the IP address information of the currently logged in users. The SINEMA host device information provides additional details such as the host name, hardware and software status, host status and MAC address information

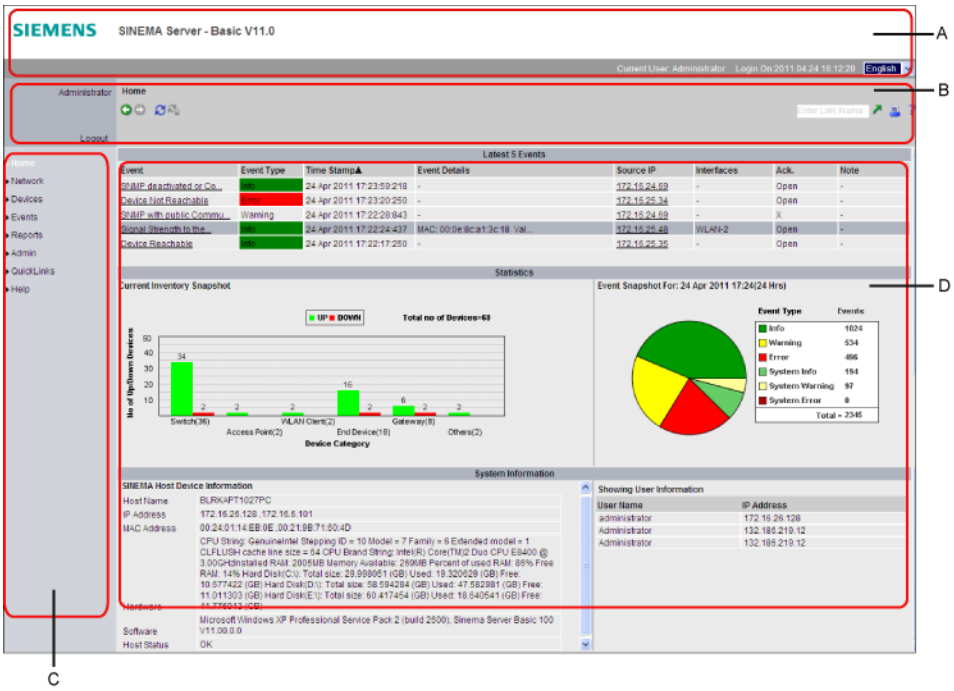
D: User information

The user information is displayed next to the SINEMA host device system information section. This section lists all the users connected to the SINEMA Server Web interface along with their IP address information.

4.3 User interface elements

User interface structure

The basic structure of the SINEMA Server application provides an easy to use Web interface that includes various options for controlling and managing the network devices. The controls for monitoring and managing these devices are well integrated in the user interface. Each of these controls has been grouped into the related areas within the user interface. The user interface screen of SINEMA Server is divided into four areas that provide different functions.



Latest 5 Events

Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
SNMP deactivated or Co...	Info	24 Apr 2011 17:23:59:218	-	172.16.24.69	-	Open	-
Device Not Reachable	Error	24 Apr 2011 17:23:20:250	-	172.16.25.34	-	Open	-
SNMP with public Commu...	Warning	24 Apr 2011 17:22:28:843	-	172.16.24.69	-	X	-
Signal Strength to the...	Info	24 Apr 2011 17:22:24:437	MAC: 00:0e:8c:a1:3c:18 Val...	172.16.25.48	WLAN-2	Open	-
Device Reachable	Info	24 Apr 2011 17:22:17:250	-	172.16.25.35	-	Open	-

Event Type	Events
🟩 Info	1024
🟨 Warning	534
🟥 Error	496
🟩 System Info	194
🟨 System Warning	97
🟥 System Error	0
Total = 2345	

System Information

SINEMA Host Device Information

Host Name	BLRKAPT1027PC
IP Address	172.16.26.128 ,172.16.6.101
MAC Address	00:24:01:14:EB:0E ,00:21:9B:71:60:4D
Hardware	CPU String: GenuineIntel Stepping ID = 10 Model = 7 Family = 6 Extended model = 1 CLFLUSH cache line size = 64 CPU Brand String: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHzInstalled RAM: 2005MB Memory Available: 269MB Percent of used RAM: 86% Free RAM: 14% Hard Disk(C:\): Total size: 29.998051 (GB) Used: 19.320629 (GB) Free: 10.677422 (GB) Hard Disk(D:\): Total size: 58.594284 (GB) Used: 47.582981 (GB) Free: 11.011303 (GB) Hard Disk(E:\): Total size: 60.417454 (GB) Used: 18.640541 (GB) Free: 41.776913 (GB)
Software	Microsoft Windows XP Professional Service Pack 2 (build 2600), Sinema Server Basic 100 V11.00.0.0
Host Status	OK

Showing User Information

User Name	IP Address
administrator	172.16.26.128
Administrator	132.186.219.12
Administrator	132.186.219.12

A: Header with language selection control

B: Second level header

C: Menu bar

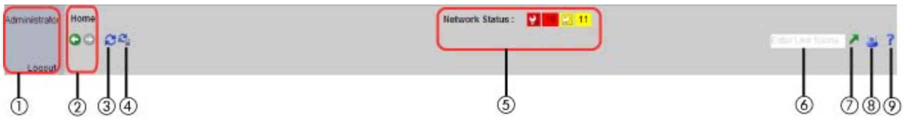
D: Main window

A: Header with language selection control

The list box at the right-hand corner of the header is used to select the language of the user interface. You can set the language to English or German. The header also includes the current user name and login date and time displayed in the right-hand corner of the screen. This information is visible only after the user has logged in successfully.

B: Second level header

The second level header or sub-header exists below the header area. It consists of the following elements:



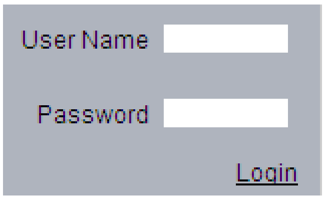
Note

The "Search for device" text box is in the center of the second level header. This is displayed only while viewing the pages in the Network, Devices, Events, Reports & admin menu items.

1. Login controls
2. Navigation controls
3. Auto refresh
4. Enable / disable auto refresh
5. Network status
6. Quick links
7. Add quick link
8. Print
9. Help

Login controls

The user name and password text box is in the left-hand corner of the sub-header area. Enter the correct user name and password to log in to the SINEMA Server Web interface. After you have logged in, the text box is replaced with the name of the logged-in user and a logout link is displayed in the login controls area as shown in the screenshot above.



Navigation controls

The navigation controls are in the top left-hand corner of the sub-header next to the login controls. These provide information indicating the current status of user navigation within the SINEMA Server application. This helps you to identify the current page name and its related hierarchy structure. You can navigate to any of the links in the hierarchy at any time by clicking on the forwards/backwards links provided.

For example, **Network > User maps** navigation indicates that you are on the User maps page. This text is displayed above the forward backward links. However, you can navigate to the link you came from by clicking the backward link.

Auto refresh

The SINEMA Server application includes options for enabling auto refresh of the Web pages. This icon is displayed in the second level header next to the "Navigation controls". The "Auto refresh" option allows you to refresh the page manually. To do this, simply click the "Refresh" button. You would normally use this "Refresh" button when the "Auto refresh" option has been disabled in the Web interface.

Enable / disable auto refresh

The "Enable / disable auto refresh" icon is next to the "Auto refresh" option. This user control is used to enable or disable the auto refresh option. If auto refresh is enabled, the screen refreshes automatically. The icon changes to "Disable" status indicated by its gray color. Click the icon again to enable the "Auto refresh" option. You can enable or disable auto refresh at any time.

Network status

The current status of the network is displayed in this second level header. The network status is indicated by icons. The red colored icon represents an error and yellow represents a warning. The total count of unacknowledged events of the types error and warning are displayed next to each icon. To view the error type or warning type events list, select the area that displays the device count, you will then go to the events list that contains unacknowledged events of the event type you selected.

Quick links

Any Web page in the SINEMA Server user interface can be added as a quick link. This provides you with fast reference options. Type in a name for the quick link in the text box and click the "Add quick link" icon to add the Web page as a quick link. Web pages added as quick links are listed on the Quick links page. You can delete quick links using controls on the Quick link page.

Add quick link

The "Add quick link" icon is located next to the "Quick link" text box. This icon is used to add a page as a quick link after typing in the quick link name in the text box.

Print

The print option allows you to print the application pages of SINEMA Server. The icon is located next to the "Quick link" text box. Once the page is loaded in the application, click the print icon to print the page. A new window containing the paper and print options is displayed. You can see a preview of the page below the print option settings. Select the required paper size and click print to open the printer dialog box. Make the required settings and click the "OK" to start printing.

Note

We strongly recommend that you select the "Print background colors and images" option in the Advanced settings tab before printing the SINEMA Server pages. This tab can be accessed from the Internet Explorer Tools menu > Internet Options > Advanced tab.

Help

Online help information is available in all Web pages of the SINEMA Server application. This can be accessed by clicking the Help button available on every Web page. The Help button is in the top right-hand corner of the sub-header area. Go to the Web page you require and click the Help button to view the online help information for the specific item. A new window pops up displaying the online help contents.

C: Menu bar

The SINEMA Server application includes a menu bar on the left-hand side of the application screen. The menu bar helps you to navigate through the various parts of the application and helps you to work more effectively with the application. Each of the links in the menu bar has related sub-links. Click on the relevant menu in the menu bar to view the sub-links available for the particular menu item. The menu items available in the application menu bar are as follows:

- Home: The home page contains the latest 5 events, statistics and system information.
- Network: This menu provides information about viewing and managing network devices.
- Devices: Contains information about devices grouped by category.
- Events: Provides options for viewing and managing events triggered by devices.
- Reports: This menu displays inventory, availability and performance reports.
- Admin: This menu is used for administration of users, groups and device settings.
- Quick links: This is used to maintain the list of favorite pages.
- Help: Contains information about the specific the pages.

D: Main window

The SINEMA Server application has a main window that is used to display the information relevant to the menu option selected. Information displayed in the main window changes when you select different menu items or their sub-links. This is the main area for viewing the SINEMA Server data and information about all the devices in the network.

Status message bar

To provide better interaction between the application and user, the SINEMA Server application supports the display of status messages based on user actions. These are displayed in the form of alert messages. The other forms of messages include validation messages, error messages and error conditions. Depending on the condition or criteria while performing actions, the related messages are generated in this message bar.

The status message can be seen at the top of the home page. The message shown in the status message bar provides more information and helps you to work with the application.

For example, when you click the "Add quick link" button without typing in the name of a quick link, a status message is displayed pointing out the omission. This message therefore provides immediate context-related support, for example when adding a quick link.

4.4 Navigation structure

Navigation overview

SINEMA Server provides enhanced navigation tools to enable you to navigate through the options. You can navigate within the application using a menu bar located to the left in the application window. Every Web page is associated with a sub-link or menu item. Based on the type of information provided, these Web pages are grouped within the corresponding menu items. For example, all event-specific Web pages are grouped under the Events menu item.

There is an arrow right symbol in front of each menu item. The arrow shown with menu item changes to an “arrow down” symbol to indicate that there are sub-links in the menu item.

General information

The navigation menu bar includes the following menu items and their sub-links:

- Home

  This menu item displays the home page of the SINEMA Server application. The home page includes information about the last five events represented at the top of a table along with an availability snapshot and SINEMA Server system information.

- Network

  The Network menu includes information specific to the network and its connected devices.

  - Devices
  - Actual topology
  - Monitoring topology
  - Reference editor
  - User maps
  - All

- Devices

  The Devices menu provides the list of devices filtered according to device category. Complete information about the device is available in the table view.

  - Switches
  - Access points
  - Clients
  - End devices
  - Gateways
  - Other devices

- Events

  The Events menu provides information about all events occurring within the application. It filters the information based on the type of event and displays this information in separate pages.

  – All events

  – Info

  – Warning

  – Error

  – Statistics

- Reports

  The Reports menu provides a detailed report relating to device inventory, availability of devices and performance of these devices.

  – Inventory

  – Availability

  – Performance

- Admin

  The Admin menu includes information that is required to manage the SINEMA Server.

  – Device list

  – User admin

  – Network settings

  – UI settings

  – Catalog

  – Views

  – Import/export

  – OPC

- Quick links

  The Quick links menu item provides options for viewing and managing the quick links.

- Help

  The Help menu includes an About page link that contains information about the SINEMA Server version including Open Source information.

Configuration 5

5.1 Viewing and monitoring the network

Overview

The **Network** menu provides various options for viewing and monitoring devices within the network. You can view all network devices in monitored/non-monitored state detected in the network. The SINEMA Server application provides information to the user by filtering these devices according to their status.

The connection topology of these devices within the network can be viewed and controlled using the "Detailed view" and "Icon view" icons. These icons are available in the toolbar view of the Actual topology and Monitoring topology pages. Reference connections can be configured and managed in the Reference topology. Support for creating and managing user-defined maps is also available in the **Network** menu and this helps you to manage a specific group of devices instead of all devices in the network.

5.1.1 Monitoring network devices

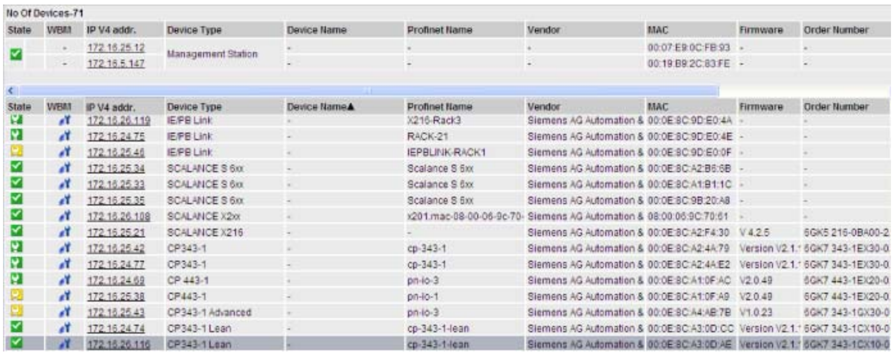
Display options

The **Network > Devices** menu item displays a list of all *monitored* network devices available in the current network.

General information

A complete list of all *monitored* network devices available in the network including the management station that is running SINEMA Server application can be viewed on this page. The management station is the system where SINEMA Server is running. The management station information is shown as separate table above the table view in Admin > Device list, Network > Devices, Network > All pages.

The IP addresses of all devices connected to the management station along with other device parameters are displayed in a table view. Below this table view, you will find a list of all monitored devices and their related device parameters. For each network device that is displayed on this page, you will see information about the device parameters such as the device name, device type, IP V4 address, vendor name, PROFINET name, MAC address, device category, first seen, etc. The total number of devices discovered in the network is displayed above this table view. Sort options are available for each field in the table view. Click the field name to sort the view based on its content. The device parameters and their descriptions are similar to the information provided in the **Network > All** page.



No Of Devices-71

State	WBM	IP V4 addr.	Device Type	Device Name	Profinet Name	Vendor	MAC	Firmware	Order Number
✓	-	172.16.25.12	Management Station	-	-	-	00:07:E9:0C:FB:93	-	-
	-	172.16.5.147		-	-	-	00:19:B9:2C:83:FE	-	-

State	WBM	IP V4 addr.	Device Type	Device Name▲	Profinet Name	Vendor	MAC	Firmware	Order Number
🟩		172.16.26.119	IE/PB Link	-	X216-Rack3	Siemens AG Automation &	00:0E:8C:9D:E0:4A	-	-
🟩		172.16.24.75	IE/PB Link	-	RACK-21	Siemens AG Automation &	00:0E:8C:9D:E0:4E	-	-
🟨		172.16.25.46	IE/PB Link	-	IEPBLINK-RACK1	Siemens AG Automation &	00:0E:8C:9D:E0:0F	-	-
✓		172.16.25.34	SCALANCE S 6xx	-	Scalance S 6xx	Siemens AG Automation &	00:0E:8C:A2:B6:6B	-	-
✓		172.16.25.33	SCALANCE S 6xx	-	Scalance S 6xx	Siemens AG Automation &	00:0E:8C:A1:B1:1C	-	-
✓		172.16.25.35	SCALANCE S 6xx	-	Scalance S 6xx	Siemens AG Automation &	00:0E:8C:9B:20:A8	-	-
✓		172.16.26.108	SCALANCE X2xx	-	x201.mac-08-00-06-9c-70-	Siemens AG Automation &	08:00:06:9C:70:61	-	-
✓		172.16.25.21	SCALANCE X216	-	-	Siemens AG Automation &	00:0E:8C:A2:F4:30	V 4.2.5	6GK5 216-0BA00-2
🟩		172.16.25.42	CP343-1	-	cp-343-1	Siemens AG Automation &	00:0E:8C:A2:4A:79	Version V2.1.'	6GK7 343-1EX30-0
🟩		172.16.24.77	CP343-1	-	cp-343-1	Siemens AG Automation &	00:0E:8C:A2:4A:E2	Version V2.1.'	6GK7 343-1EX30-0
🟩		172.16.24.69	CP 443-1	-	pn-io-3	Siemens AG Automation &	00:0E:8C:A1:0F:AC	V2.0.49	6GK7 443-1EX20-0
🟨		172.16.25.38	CP443-1	-	pn-io-1	Siemens AG Automation &	00:0E:8C:A1:0F:A9	V2.0.49	6GK7 443-1EX20-0
🟨		172.16.25.43	CP343-1 Advanced	-	pn-io-3	Siemens AG Automation &	00:0E:8C:A4:AB:7B	V1.0.23	6GK7 343-1GX30-0
✓		172.16.24.74	CP343-1 Lean	-	cp-343-1-lean	Siemens AG Automation &	00:0E:8C:A3:0D:CC	Version V2.1.'	6GK7 343-1CX10-0
✓		172.16.26.116	CP343-1 Lean	-	cp-343-1-lean	Siemens AG Automation &	00:0E:8C:A3:0D:AE	Version V2.1.'	6GK7 343-1CX10-0

The SINEMA Server application filters this information about the network devices on the **Network > Devices** page to display a device list that includes the new devices detected during the scan as well as the devices in the monitored state. SINEMA Server automatically tries to monitor the new devices as long as the total number of devices is lower than the total number of nodes supported by the license being used. This page provides complete information about the *monitored* devices. This helps you to manage the set of monitored network devices more efficiently.

Note

This list only displays devices that belong to the set of devices permitted for the logged-on user. The administrator can limit the number of devices that a user can monitor.

Note

Network devices can be set to the monitored or unmonitored state on the **Admin** > **Device list** page. Refer to "*Managing the device list", section 5.5.1* for more information about the monitoring concepts and the steps required to control the functions for monitoring these network devices.

Detailed information

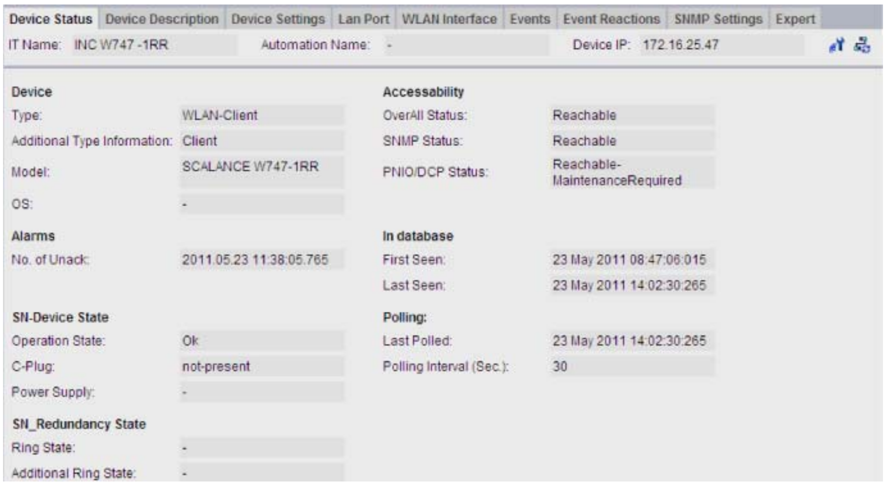
To view details of the network devices, go to the row of a device and click on the IP address link. The Device details page opens displaying information about the selected network device. The device details of all *monitored* network devices are displayed on this page.

5.1.2 View device details

Overview

The device details page is usually displayed after clicking the IP address link of the specific network device. The device details information can be easily accessed from any of the pages that contain a list of devices detected in the network.

The device details page provides complete information about the device status, device description and other related information specific to the selected network device. This makes it easy to manage and control the device information. This device-specific information is organized over several tabs on this page.



IT Name: INC W747 -1RR   Automation Name: -   Device IP: 172.16.25.47

Device		**Accessability**	
Type:	WLAN-Client	OverAll Status:	Reachable
Additional Type Information:	Client	SNMP Status:	Reachable
Model:	SCALANCE W747-1RR	PNIO/DCP Status:	Reachable-MaintenanceRequired
OS:	-		
Alarms		**In database**	
No. of Unack:	2011.05.23 11:38:05.765	First Seen:	23 May 2011 08:47:06:015
		Last Seen:	23 May 2011 14:02:30:265
SN-Device State		**Polling:**	
Operation State:	Ok	Last Polled:	23 May 2011 14:02:30:265
C-Plug:	not-present	Polling Interval (Sec.):	30
Power Supply:	-		
SN_Redundancy State			
Ring State:	-		
Additional Ring State:	-		

Device-specific controls

Apart from the device specific information organized in several tabs, the device details page includes certain controls that are available in the top row of each of these tabs.

The device parameters IT name, Automation name and Device IP are displayed at the top of each tab. These three parameters are displayed on each of these tabs. IT name is the system name. Automation name is retrieved from the Automation MIB. The device IP is the IP address of the specific network device.

The following two icons are displayed next to the three device parameters. The icons and their meaning are described below:

Icon	Description
	Web server
	Force read SNMP data from device

The "Web server" icon is available in the top row on the "Device details" page. This button exists in the top row of all tabs. When you click this icon, a Web page is opened if there is a Web page for the selected device. This page shows information and settings specific to the selected network device.

The "Force read SNMP data from device" icon is next to the "Web server" icon and is available in all tabs. You use this icon when you want to read the latest SNMP values from a specific device. When you click this icon, a request is initiated to read SNMP values of the device. The latest updated values will be shown on the user interface screen as and when the response comes from the device. This icon can be clicked any number of times in succession. However, a request within 2 minutes of the last will be ignored. This avoids increasing network traffic. You should therefore wait longer than this time before clicking the icon again.

Detailed information

The tabs on device details page are divided into the following categories:

- Device status
- Device description
- Device settings
- LAN port
- WLAN interface
- Events
- Event reactions
- SNMP settings
- Expert

Device status:

The "Device status" tab provides all the information relating to the status of selected network device. It includes information about the device type, model, accessibility, SNMP status, alarms, operating state, polling state and any other state information. This information is very helpful when handling each of the network devices in the network.

The parameters on this tab are listed below along with a description:

Parameter	Description
Device	
Type:	Describes the type of network device.
Additional type information:	Provides additional device type information.
Model:	Specifies the device family name.
OS:	Type of operating system.
Accessibility	
Overall status:	Overall status of the device response.
SNMP status:	Status of the SNMP response.
PNIO/DCP status:	Status of response specific to the PNIO/DCP request.
Alarms	
No. of unack:	Total number of unacknowledged alarms.
In database	
First seen:	Date and time when the device was detected.
Last seen:	Date and time when the device was available or last detected in the network.
SN device state	
Operating state:	Automation operating status of the component.
C-PLUG:	Current status of the C-PLUG.
Power supply:	Current status of power supply.
Polling	
Last polled:	Date when the network device was last polled.
Polling interval (sec)	Duration of the polling interval in seconds.
SN redundancy state	
Ring state:	Type of redundancy mode - HSR or MRP.
Additional ring state:	Provides the additional ring state. Ex: OK
Standby state:	Indicates redundancy state configured.
Additional standby state:	Provides the additional standby state. Ex: OK
Time	
Up time	Time when the device was started.

Device description

The Device description tab provides more information about the selected network device. You can view the IP address, LAN ports, location information, WLAN interface information, vendor identification and list of supported protocols for the specific device.

The parameters on this tab are listed below along with a description:

Parameter	Description
Network IP V4 address	 IP address of the network device.
Location Automation location: System location	 The location where a component is installed in the plant. Location name of the actual device.
LAN ports Free ports: Ports used	 No. of ports available. No. of ports used.
WLAN interface Available interfaces: Enabled interfaces:	 No. of available WLAN interfaces. No. of interfaces enabled.
Supported protocols:	List of supported protocols.
SN device identification Order number: Firmware: Serial no.: Hardware version	 Unique ID associated with the device. The firmware version of the device. Serial number of the device. Hardware version used. **Note:** SN device identification works only with Siemens devices.
Vendor identification PN/SN vendor: MIB2 vendor:	 Vendor ID of component. MIB2 vendor name.
SINEMA identification IP | MAC address:	 Provides the IP & MAC address of the system where the application is running.
Contact person Sys. Contact:	 Contact person name.
User links Link 1:	 Link URL or path of device Web server information with options to edit the link.
Link 2:	Link URL or path of device Web server information with options to edit the link.
Upload device icon	Provides the option of browsing and uploading icon images for a device.
Notes	Displays the notes, if any. Device-specific notes added in the Admin > Device list page are shown here.

A user-defined icon can be added for any managed device in the "Device description" tab. The "Upload device icon" parameter is available in the lower part of the "Device description" tab. Click the "Upload icon" button to upload the icon image to the device. The text area will change to show an empty text box with a "Browse" and "Save" button. Click the "Browse" button to select the icon image and save the changes. The saved icon image will appear on the relevant topology pages and user maps.

The minimum and recommended resolution size for the icon image is 40 x 40. The file types GIF, JPG and PNG are supported for the icon image. The icons assigned to a device can be seen in the next topology cycle. The latest topology is rebuilt every 30 seconds. This means that the changes can be seen in the SINEMA Server user interface after approximately 30 to 45 seconds depending on the user interface refresh interval.

Device settings

The Device settings tab contains various settings that are specific to the device. You can view settings related to SNMP traps, Ethernet address and PROFINET as well as Radius server information. These SNMP traps are usually configured on the device and are generated when a fault is detected in the management station.

The parameters on this tab are listed below along with a description:

Parameter	Description
SNMP traps	
Link down:	Reports status as "Checked" if verified.
Link up:	Reports status as "Checked" if verified.
Cold restart:	Reports status as "Checked" if verified.
Warm restart:	Reports status as "Checked" if verified.
Authentication fail:	Reports status as "Checked" if verified.
Ethernet address	
IP V4 address:	IP address of the network.
Subnet mask:	IP address of the subnet.
Router address:	Address of the router.
SN-SNMP traps	
Traps state:	State of traps - enabled/disabled.
PROFINET	
PNIO active:	Reports the status of PNIO active.
PNIO name:	PNIO interface name.
PNIO type:	Type of station.
Radius	
IP Radius server(s):	IP address of the radius server(s).

LAN port

The LAN port tab on the device details page provides information about the ports such as interface number, name, state, redundancy and topology. Several performance parameters related to these ports in terms of bandwidth, quality and data rates are shown on the LAN port tab. Navigation support for ports is available and helps you to navigate within each of these ports. The port numbers shown at the top as small rectangular boxes indicate individual ports available for the specific device. The color of this rectangular box indicates the status of the relevant port available within the device. The port status shown here is only for the monitored status. Clicking on the port numbers displays the parameter information available for the port or interface.

Note

For a gigabit port, the information relating to traffic, utilization and error fields is not displayed regardless of the interface status value.

The parameters on this tab are listed below along with a description:

Parameter	Description
Interface number 1 Interface index:	 Index number of the port.
Name MAC address: Interface description:	 MAC address of the port. Additional information about the port.
LAN port Media type: Mode: Max data rate (Mbps):	 Shows the supported media type. Full duplex/half duplex mode. Maximum data rate supported in Mbps.

Traffic
Transmit (Mbps):
Receive (Mbps):
	
	Transmit rate in Mbps.
	Receive rate in Mbps.

Quality Error (%):	 Signal error rate as percentage.
Redundancy Mode: State:	 Shows the mode name used. Ex: Ring port Redundancy state.
State Interface status:	 Shows port status; port is up or down.
Topology Connected to device: Connected to port:	 IP address of device to which the port is connected. Port number of the connected device.

Parameter	Description
Utilization (%)	
Transmit (full duplex):	Full duplex transmit rate as percentage.
Receive (full duplex):	Full duplex receive rate as percentage.
Combined (half duplex):	Half duplex combined rate as percentage.
Routing	
IP forwarding:	Indication of whether this device is acting as an IP gateway that forwards datagrams it receives.

WLAN interface

The WLAN Interface tab provides information specific to the wireless devices, clients or access points detected in the network. The information displayed in this tab includes data relating to client devices as well as wireless access point devices. The device interface number, interface name, state, security and other WLAN interface settings can be viewed in this tab. The WLAN interface index and WLAN interface number displayed in the WLAN interface tab are sequential and unique. The serial number, client name, MAC client address, signal state, transmit data rate and transmit/receive error rate (%) are displayed in a table view in the bottom part of the WLAN Interface tab. This table view is shown only while displaying information about wireless access point devices.

The navigation support for ports is also available in the WLAN interface tab. This simplifies navigation between each of the ports and helps to identify the port status. The port status color indicated in the rectangular box indicates the port status in the device. If you click one of the port numbers, the relevant parameter details are displayed in the page itself.

The parameters on this WLAN interface tab are listed below along with a description:

Parameter	Description
Interface number	
Interface index:	Unique interface index of the port.
Name	
Interface description:	Details of the WLAN interface.
WLAN interface	
BSSID:	Basic Service Set Identifier number.
SSID:	Indicates the associated WLAN network name.
Mode:	Indicates the WLAN network mode - 802.11b/g/a/h.
Channel/frequency (MHz):	Specifies the channel number or frequency.
State	
Interface status:	Specifies the operating state - up/down.
Interface signal strength (dBm):	Interface signal strength.
Interface error rate	
Transmit error rate (%):	Transmit error rate as a percentage.
Receive error rate (%):	Receive error rate as a percentage.
Security	
Authentication type:	Type of authentication used in the network.

Parameter	Description
SN AP (applies only to clients)	
AP BSSID:	BSSID number of the client.
AP SSID:	Specifies WLAN network name.
AP signal strength (dBm):	Specifies signal strength of AP in dBm.
AP signal strength state:	Signal strength state of AP.
AP transmit data rate (Mbps):	AP transmit data rate in Mbps.
AP transmit error rate (%):	AP transmit error rate as a percentage.
AP receive error rate (%):	AP receive error rate as a percentage.
SN clients (applies only to clients)	
Number of clients:	Number of associated WLAN clients.
Number of clients - state:	Number of clients exceeded user-defined threshold.

A table view is displayed in the lower part of the WLAN Interface tab that displays parameters specific to the client, its signal strength, signal state and error rate. A list of client-specific parameters and their meaning is shown below:

Parameter	Description
Client name	Name of the client network device.
Client IP	IP address of the client device.
Client MAC	MAC address of the client device.
Signal (dBm)	Signal strength in dBm.
Signal state	Status of the signal.
Transmit data rate (Mbps)	Transmit data rate in Mbps.
Transmit error rate (%)	Transmit error rate as a percentage.
Receive error rate (%)	Receive error rate as a percentage.

Note

The client IP address and client name are displayed in a table view only if the client device is identified or discovered by the SINEMA Server application.

Events

The Events tab provides a view of all events generated within the network. Each row in the table displays information about the event: event type, time stamp, event details, source IP, acknowledgement status, notes, etc. The Interfaces column in the table view uses separate unique sequential numbering for LAN and WLAN devices. This helps to classify the interface indicating it belongs to a LAN or WLAN device.

The list of events displayed in the table view can be customized according to specific date, event category type and recent events. To do this, you use the filters available at the top of the Events tab. There are other functions available with which you can acknowledge events, add notes, delete notes or show/hide events using the controls on the Events tab. The icons and their meaning are described below:

Icon	Description
!	Acknowledge event
≡✎	Edit notes
≡✕	Delete notes

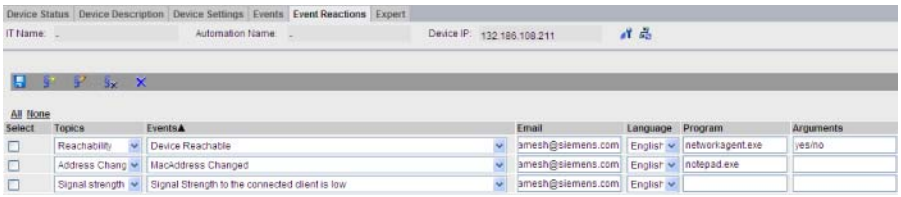
You will find more information on using these user controls and filters in "*Manage all events*" in section 5.3.1.

Event reactions

The Event reactions tab provides the required options to perform actions on each of these predefined sets of events that are generated based on the state changes. This can be achieved with the help of rules. Each rule includes a defined set of actions that will be performed on an event. The events are grouped according to specific topics. Each topic name covers a related set of events. Only the network-related topics and events can be viewed in the Event reactions tab while you are adding a rule.

To allow you to perform the various actions in the Event reactions page, there are controls in the form of icons. A list of the icons and their meaning is shown below:

Icon	Description
💾	Save changes to the rule
§✳	Add new rule
§✎	Edit existing rule
§✕	Delete the rule
✕	Cancel the action performed



IT Name: -   Automation Name: -   Device IP: 132.186.108.211

Select	Topics	Events▲	Email	Language	Program	Arguments
□	Reachability	Device Reachable	amesh@siemens.com	Englist	networkagent.exe	yes/no
□	Address Chang	MacAddress Changed	amesh@siemens.com	Englist	notepad.exe	
□	Signal strength	Signal Strength to the connected client is low	amesh@siemens.com	Englist		

Note

Before adding a rule, remember to set up the SMTP mail server and global mail in Admin > Network settings > Mail settings. For more information about setting up the mail server, please refer to "*Network settings*" in section 5.5.3.

To set or configure event reactions for a specific event, follow these steps:

1. Click the "Add rule" icon to add a new rule to the list of generated events.
2. Select a topic from the list and choose the associated event type from the drop-down list box.
3. Specify a valid e-mail address and select the required language - English or German.
4. Type in the program name that needs to be opened each time the event is fired. The program needs to be an application or an executable file.
5. Enter the required parameters in the arguments text box to specify arguments that need to be used while opening the specified application.
6. Repeat steps 1 to 6 to add more rules to the list of events and click the "Save" button to save the changes.
7. To edit or delete a rule, select the check box in the row containing a rule and click the appropriate button.

When you specify the program name when adding a rule, remember that the full path of the program location in the local system does not need to be entered in the "Program" text box. You only enter the program name in the text box. The environment variable must be set explicitly for the application before using the program name.

Event reactions can trigger a wide variety of programs. However, the application window is not displayed on the screen since the program runs in the background.

Example:

As an example, let us assume an event called "Network scan started". Once a network scan has been started, an e-mail is generated and sent to the corresponding e-mail ID. If the program to start a networking tool or a batch command is added, the specified application will be opened automatically once the scan is started. This allows event reactions to be set for every event type.

However, the program or application will be opened on the host computer where SINEMA Server is installed. If you are accessing SINEMA Server using a client a machine, the application cannot be seen will therefore be running in the background.

SNMP settings

The SNMP settings tab provides options for setting the SNMP parameters required for detecting and monitoring the devices in the network. The default values and the recommended range of values for the SNMP parameters are shown below:

Parameter	Default value	Range of values
Version	1	1, 2C, 3
Read community string	public	Public
Timeout	2000 ms	500 to 5000 ms
Retries	2	0 to 10
Port	161	

Expert

The Expert tab provides expert level information that helps when diagnosing or monitoring the network devices connected in the network. This tab shows a list of monitored SNMP parameters along with their corresponding monitored SNMP values.

5.1.3 Actual topology

Display options

The "**Network > Actual topology**" menu item displays a topology view page containing all discovered and monitored devices available in the current network.

General information

The "Actual topology" page is used to view the actual status of a network and contains a network topology that represents the devices and discovered connections in the network. New devices are also shown in this actual topology and are represented by a new device icon. SINEMA Server automatically detects the devices in the network, and displays the topology of the devices and connectivity across the network on the basis of the SNMP information. If devices do not support SNMP, no connection lines are displayed. If a device does support SNMP, connection lines are displayed for devices with LLDP MIB support. The root node of the topology is the management station.

The "Actual topology" includes two types of view :

- Detailed view
- Icon view

The detailed view is used to display the topology layout of devices and their connections. It displays the device status, port state and connection lines. The icon view displays the topology layout with devices and their connections represented as icons.

5.1.3.1 Detailed view

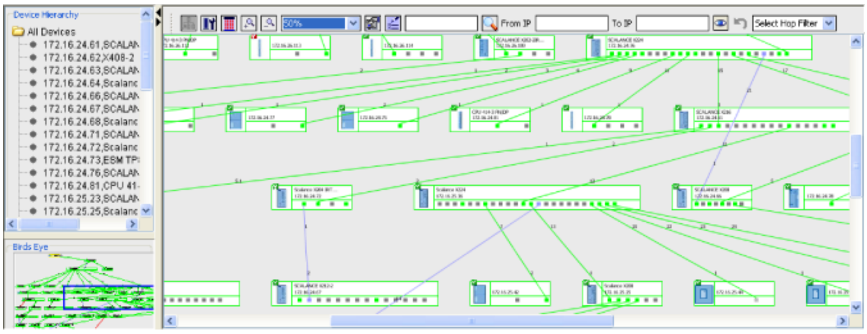
Display options

The "**Network > Actual topology**" menu item displays a topology view representing all devices discovered in the current network including new devices.

Purpose and use

The "**Network > Actual Topology**" shows the detailed topology and includes available devices, ports and connections as a tree structure. This helps you to view and manage the current network topology efficiently. This view shows a specific topology associated with a specific user. Each of these views can be customized on the Admin > Views page to display the desired number of devices within the topology.

The detailed view shows both discovered devices as well as monitored devices. Non-monitored devices are not shown in this view. When a new device is detected in the network, the actual topology displays the new device status in the top part of the device area. The color of the devices and ports depends on their current state. The connection line color, on the other hand, depends on the state of connected ports. The topology also displays the network view starting from the SINEMA Server station in a hierarchical structure.



Show / hide top pane and left pane

To obtain a larger view of the topology so that you can see all the devices, hide the top pane and left pane in the SINEMA Server application. Once the contents of the detailed view are loaded, you can see the controls for hiding the top pane and left pane.

Show / hide top pane:

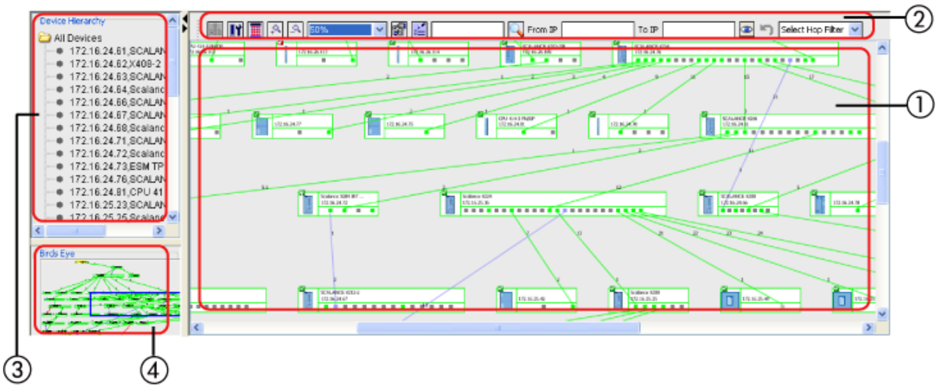
To hide the top pane, click "Hide top pane". If the top pane is hidden, the "Show top pane" option is displayed. Click "Show top pane" if you want to display the top pane again.

Show / hide left pane:

To hide the left pane, click "Hide left pane". If the left pane is hidden, the "Show left pane" option is displayed. Click "Show left pane" if you want to display the left pane again.

Parts of the detailed view

The detailed view layout consists of four separate parts containing information specifically relating to the topology of the devices detected in the network. This is the same with both the actual topology and the monitoring topology. However, the colors used to represent the topology and the device representation including toolbar options are different in these topology views.



1. Device view area
2. Toolbar
3. Device hierarchy
4. Bird's eye view

Device view area

The device view area displays the topology tree with the connections between the devices detected in the network. This topology tree is shown in the device view area immediately after selecting the "**Network > Actual topology**" menu item. This tree view includes the display of the nodes, their connection lines and the corresponding port status.

To select a device in the topology, left-click on the device. The device is selected and is highlighted in blue.

The following sections describe the parts and functions of device view area:

Display of nodes/connections/ports

In the device view area, the topology tree shows the topology information of all the devices connected in the network including new devices. Each node can have an icon as well as a text area and a port area associated with it. The default display in the text area shows the device name and IP address. The text area content of a specific device can be configured using the *Configure node* button. This button is available in the toolbar view. The ports have a rectangular shape and are usually displayed within the square box that contains the device information. The port area is located below the text display area.

Shortcut menu

A shortcut menu is available in the device view area. This can be accessed by right-clicking on the device. The options in the shortcut menu depend on the selection in the device view area. The shortcut menu includes the following two options:

- View device details
- Device-specific link

If you have not made a selection in the topology editor, the shortcut menu is shown after right-clicking in the device view area. The no selection shortcut menu includes the following options:

- Zoom in
- Zoom out
- Refresh

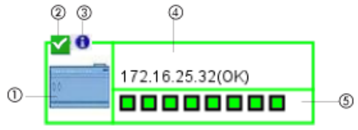
Note

The detailed view cannot be edited, so you cannot make changes to any of the devices or the topology tree structure. To customize the topology view, use the Reference editor.

Status monitoring

The status of network devices and their connections can be monitored in the detailed view with the help of various different representations of the devices; the port status indicated by a color code. Each device in the topology is represented by a device icon, a node text, and a port area. The icon represents the type of the device, the node text displays the device type information, IP address and state of the device while the port area indicates the state of the ports. The ⓘ symbol is displayed above the device icon in the node to denote a new device. The up or down status of the device is indicated by a green or red border around the rectangular box.

Below, you will see the graphical representation of a device and its contents:

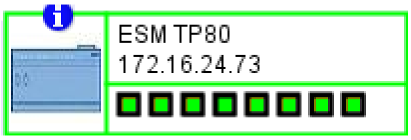
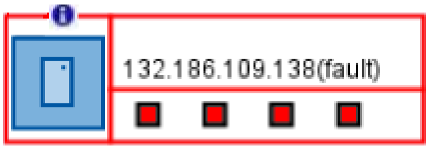
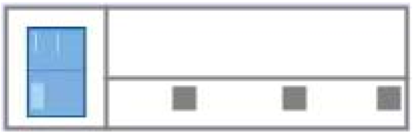
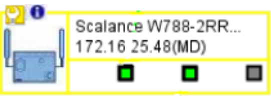


1. Device icon
2. Device status
3. New device
4. Node text
5. Port area

The different states of the devices, ports and their connection states are represented as follows:

Device state:

The color of the device depends on its general reachability. If a device is not in view, the device state will be in gray.

Device state	Description
 ESM TP80 172.16.24.73	Device in view and in "Reachable" state.
 132.186.109.138(fault)	Device is in view and it is not "Reachable".
	Device not in view or "Unknown device".
 Scalance W788-2RR... 172.16.25.48(MD)	Device in view and is "Reachable". SNMP/DCP not activated.

Status icon	Description
✓	Device in view; State: Up
🔧	Device in view; State: Up - maintenance requested
🔧	Device in view; State: "Up - maintenance demanded"
🔧	Device in view; State: Fault

Port/interface state:

The state or color of a connection has no effect on the port color. If a device is not in view, all its ports will be gray. If a device is not reachable, its port colors are light gray.

Color	Has actual connection	Description
🟩	No	Up or testing
🟩	No	Up - maintenance requested
⬛	No	Down - maintenance demanded
⬛	No	Down
⬜	No	Unknown
🟩	Yes	Up or testing
🟩	Yes	Up - maintenance requested
🟥	Yes	Down - maintenance demanded
🟥	Yes	Down
⬜	Yes	Unknown

Connection line status

The connection between the devices is represented by a line. Each line from the specific port of the device is labeled by a unique number format. Both the start point of a line and the end point of a line include their interface numbers that are displayed at both ends of the connection line. This line number is shown above the connection line in the topology view. The tooltip at the start point and the end point of a connection line shows the interface number along with the mode type used for transmission. If you move the mouse pointer to the center of the connection line, the tooltip shows the mode, transmit utilization rate and receive utilization rate.

For example, if port 2 of device A is connected to port 5 of device B, then port 2 is identified as P2 and port 5 is identified as P5. These port numbers are displayed at the start and end point of a connection line.

The LAN and WLAN devices have separate numbering sequences. If the connected devices are in view, the color of the connected ports defines the connection line color. If one of the connected devices is in view, the port of the device that is not in view is not colored but connection line color depends on both interfaces. The port color combinations and the connection line color conventions are as shown below:

Port 1	Port 2	Color
🟩	🟩	🟩
🟩	🟥	🟥
🟩	⬜	🟩
🟩	🟦	🟦
🟥	🟩	🟥
🟥	🟥	🟥
🟥	⬜	🟥
🟥	🟦	🟥
⬜	🟩	🟩
⬜	🟥	🟥
⬜	⬜	⬜
⬜	🟦	🟦
🟦	🟩	🟦
🟦	🟥	🟥
🟦	⬜	🟦

Connection types

The connection line types shown in the topology tree are classified based on the device type or the category of device. Wireless connections, optical connections and electrical connections shown in the detailed view are represented as follows:

Connection type	Description
-·-·-·-·-	Wireless connection
– – – – –	Optical connection
———————	Electrical connection

Port 1	Port 2	Line type
Electrical	Electrical	──────
Electrical	Unknown	──────
Electrical	Optical	──────
Electrical	Wireless	──────
Optical	Electrical	──────
Optical	Unknown	– – – – – –
Optical	Optical	– – – – – –
Optical	Wireless	──────
Wireless	Electrical	──────
Wireless	Unknown	-·-·-·-·-·-
Wireless	Optical	──────
Wireless	Wireless	-·-·-·-·-·-
Unknown	Electrical	──────
Unknown	Unknown	──────
Unknown	Optical	– – – – – –
Unknown	Wireless	-·-·-·-·-·-

Note

The connection lines shown above for wireless device and optical device are displayed as an active connection. The wireless or optical device connection lines can have any of the connection states as shown in the table above.

Note

It is not possible to monitor the status of the devices that are not in the set of devices permitted for the logged-on user.

Cloud state

Any unknown device discovered in the actual topology is shown as a cloud device. Connections can exist between cloud devices and ports of other devices. If a port of particular device is connected to a cloud in the actual topology, the connection color is derived from the port color. However, cloud devices without any actual connection are not displayed. The color of a connection between cloud and device (no specific port) depends on all port states.

Port state	Connection color
Up or Up - maintenance demanded	🟩
Down or Down - maintenance demanded	🟥
All unknown	⬜

Filtering the topology

You can filter the topology based on the devices available in the network or the number of hops to be shown in the topology view. The "IP filter" and "Hop filter" drop-down list boxes are available in the toolbar. To filter the topology based on the IP address, follow these steps:

1. On the topology view toolbar, enter the IP address of a network device in the IP filter search box and click the search button.
2. The network device is highlighted in the topology tree that contains the IP address.

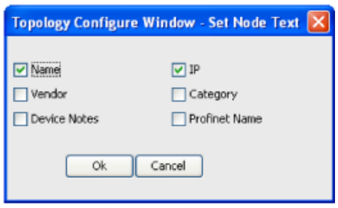
To filter the topology view based on the number of hops, follow these steps:

1. In the device view area, select the devices that need to be filtered in the topology.
2. On the toolbar, click the hop filter drop-down list and select the number of hop levels to be displayed.

The topology view now only shows the selected number of levels of the topology tree for the selected device. For example, select SWITCH 112 and then select Hop level 2 from the list, two levels of hierarchy are then displayed in the topology view for SWITCH 112.

Configure node

The Configure node option is a toolbar button in the toolbar area. This option is used to configure the node text in each node. To configure the node, select the "Configure node" icon. This change applies to all nodes in the topology tree.



Topology Configure Window - Set Node Text

☑ Name ☑ IP
□ Vendor □ Category
□ Device Notes □ Profinet Name

In the "Configure topology" window that opens. you can select any of the following items:

- Name
- IP
- Vendor
- Category
- Device notes
- PROFINET name

Select the check boxes listed in this window and click OK. You can see changes in the node text area of all nodes in the topology.

Toolbar view

The detailed view includes a toolbar that contains toolbar buttons for performing different actions on the devices in the topology tree. You can display information about each of the toolbar buttons using the Tooltip option. Move the mouse pointer over each toolbar button to view the toolbar option name. The toolbar buttons are available for the following operations:

Icon	Description
品	Opens the detailed view
▮	Opens the icon view
▦	Recalculates the topology
🔍+	Magnifies the image by the preset zoom factor.
🔍−	Reduces the image size by the preset zoom factor.
100% ▾	Provides options for selecting the zoom factor (as a percentage).
▤	Shows device details
▨	Configures the node information of the selected device.
□	Text box for entering IP address to be searched for.
🔍	Search button to search for the network device.
From IP □	Start of the IP address range.
To IP □	End of the IP address range.
👁	Filters the topology based on the IP range.
↶	Resets the filter settings.
Select Hop Fi... ▾	Filters the topology based on the selected hop level.

Device hierarchy

When you select the **Network > Actual topology** menu, the device hierarchy catalog is automatically hidden. To view the device hierarchy, drag the resize handle of this view to the right. The device hierarchy includes an "All devices" folder that contains the list of network devices shown in the device view area. To hide this view, click the left arrow. The right arrow is used to show the device hierarchy.

This pane is displayed in the left panel of the actual topology page. All the devices found during the scan are displayed in a hierarchical structure. Select any device from the list in the device hierarchy catalog and you will see that the corresponding device node text area is highlighted in blue in the device view area.

Bird's eye view

The Bird’s eye window contains an image of the entire topology tree view. This view draws a rectangle surrounding the topology tree as a border to identify the area currently shown in the device view. You can also position the rectangle at a specific location in the bird’s eye view. Positioning the rectangle in the bottom part of the bird's eye view shows the corresponding devices in the bottom part of the topology tree. When navigating across the device view area, the corresponding area is highlighted in the bird's eye view.

Recalculate topology

When you refresh, the topology layout does not change its state. The zoom level and view position remain the same. The autorefresh feature changes only the state color and connection line colors, but does not alter the device positions. Once devices are discovered and shown in the topology tree, their positions are not modified until you click the "Recalculate topology" button. If the actual topology page is accessed before the whole topology has been discovered, this may lead to crossed connections. In this case, the "Recalculate topology" button can be used to recalculate the layout and positions the devices in the device view area.

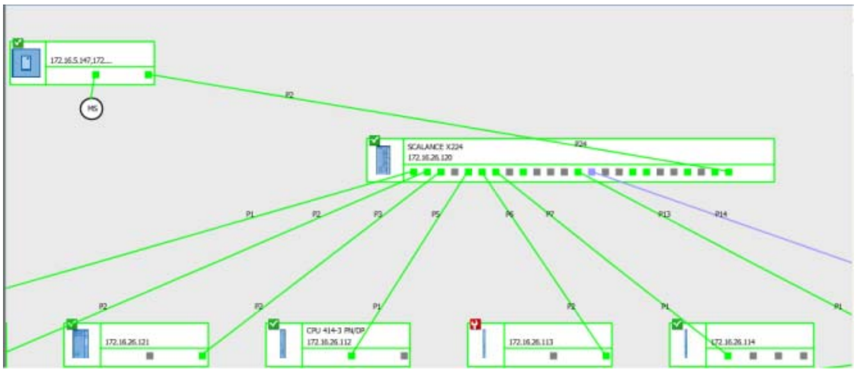
Unmanaged devices in the actual topology

In the Device view area, the unmanaged devices are not displayed in the actual topology. If an unmanaged device exists between two managed devices, this will result in the following connection:

- A cloud between ports of devices - common if more than 2 devices are connected to the unmanaged device
- A direct connection between the ports - common if only two devices are connected to the unmanaged device
- Connection between unresolved cloud and device - >If one of the managed devices has no connection, the device (not the ports) is connected to the unresolved cloud.
- No connection between the devices if port is in down state.

Unresolved ports

In the actual topology, the management station consists of one or more ports (NICs) without connection. The ports will be in Up state and displayed green, however there will not be any connection available to the device. This means that in the management station, these unresolved ports are connected through an MS bubble. The resolved ports are connected to other network devices in the topology.



If there are any unresolved devices in the topology, the application displays this information in the lower part of the topology page. The unresolved devices are therefore connected to a cloud displayed in the lower part of the actual topology. You will see a connection from this unresolved cloud to the device boundary. The unresolved cloud will also be connected to an MS bubble if there are unresolved ports in the management station. Connection endpoints can be identified easily due to the MS bubble shown in the actual topology.

Redundancy concepts

In a ring network, network devices are connected in the form of a ring and each node connects to two other nodes forming a continuous path. If the ring is closed, this would lead to circulating data packets. These data packets would greatly reduce the available bandwidth and finally lead to a breakdown of the data traffic. To avoid this situation, a redundancy manager must be configured in the ring topology.

An IE switch in the ring topology can adopt the function of redundancy manager. If the transmission path is intact, the IE switch behaves as if it were the start and end point of a linear bus topology. This prevents circulating data packets. When the IE switch operating as redundancy manager detects the failure of the transmission path, it makes the connection between its ports connected to the ring in a maximum of 200 ms. This re-establishes a connection between all components of the ring.

In a standby ring configuration, the ring network is coupled with another network and one device (switch) acts as standby master and another switch in the network acts as standby slave.

SINEMA Server provides the redundancy state details, ring status, redundancy mode information, port type and port status in Device details pages. The LAN port tab displays the redundancy mode and its corresponding status. The applications also display the corresponding device status on Network > Devices pages. The events display information about changes in the current status of the ports including information indicating the type of port.

Primary or standby port

Redundancy state (device details)	Port state
OK	Passive
Interrupted	Active

Standby status (device details)	Standby port status
Passive	Passive
Active	Active

Redundancy status	Standby port status	Color
Active	Up	🟩
Active	Up - maintenance requested	🟩
Active	Down - maintenance demanded	🟥
Active	Down	🟥
Active	Unknown	⬜
Passive	Up	🟦
Passive	Up - maintenance requested	🟦
Passive	Down - maintenance demanded	🟥
Passive	Down	🟥
Passive	Unknown	⬜

5.1.3.2 Icon view

Display options

"Network > Actual topology > Icon view" displays an icon view representing all devices discovered in the current network including new devices.

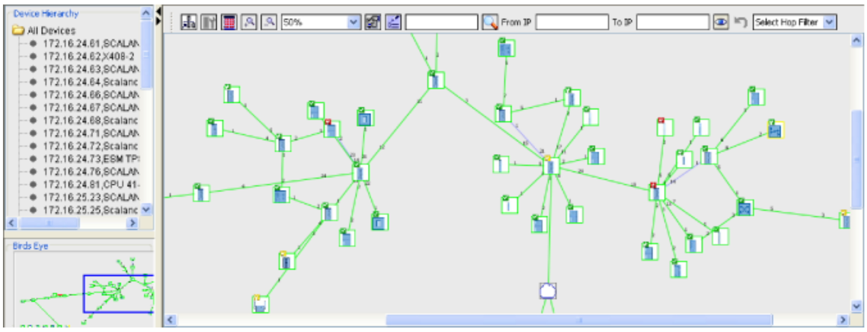
General information

The Icon view can be accessed by clicking the "Icon view" button in the toolbar of the "Actual topology" page. The icon view displays the network topology as a structured view in the form of icons. The devices and their connections in the current network along with their actual state and monitoring status are displayed as icons in this view. This view helps you to get a closer look at the network structure containing the devices and their connections represented as small icons visible in the Actual topology.

Using the icon view

To select a device in the icon view, left-click on any device listed in the device view. The device icon is then highlighted in blue. To view the device details specific to the selected device, double-click on the device icon in the device view. A tooltip text is shown both for devices that are connected and also for the set of devices that are shown as unconnected in the icon view. The tooltip displays the device information as well as the IP address of these network devices in the icon view.

The screen layout is optimized for the current detected topology. This view is helpful when you want a complete view of the devices within the network as icons. The tree view can be customized in terms of device and connection management using the Reference editor.



Icon view features

In the icon view, the devices are displayed as icons instead of ports. The start and end port number are shown on the connection line. This view displays the network structure such as ring, star and linear bus topology represented as icons. The icon view is located in the middle of device view area. The way the connections are displayed in an icon view varies according to the type of topology.

Note

The icon view layout and other show/hide options are practically the same as in the actual topology or detailed view. The parts of the detailed view including the toolbar options explained in "*Detailed view"* in section 5.1.3.1 also apply to the icon view.

Note

Modifications to the nodes or connections are not permitted in the icon view.

5.1.4 Monitoring topology

Display options

The **Network > Monitoring topology** menu item displays the reference topology that includes the reference status of the network compared to the actual network status.

General information

The Monitoring topology page displays the reference topology, the status of its ports and the reference connections compared to the actual network topology. It shows a configured topology that cannot be modified. The monitoring topology information helps in understanding the changes or differences in a network along with changes in port status, network devices and their connections within the topology.

The device layout and positions are calculated only once. Any new device that is not part of the reference topology will not be displayed on the monitoring topology page. New devices are indicated by an icon. The monitoring topology is also specific to the user view. Devices that are not in view for the user are grayed out. Non-monitored devices are not shown in this topology. If a device has been set to non-monitored, it is removed automatically from the reference topology. If the same device is set to monitored state again, this will be handled by the application as if it were a new device.

Note

The monitoring topology tree structure is not displayed in the monitoring topology page until the reference topology has been saved at least once.

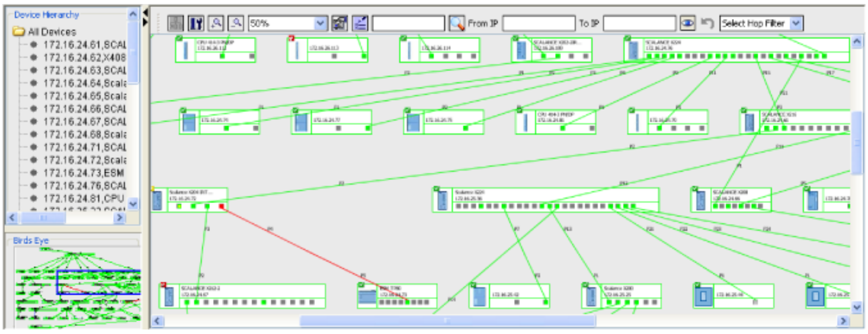
5.1.4.1 Detailed view

Display options

The **Network > Monitoring topology** menu item displays the reference status of a network. This status is based on the difference between the reference topology and the actual topology information.

Purpose and use

The detailed view displays the detailed monitoring topology and includes devices, ports and connections as a tree structure based on the reference topology. This helps you to view and manage changes within the existing network. This view shows a specific topology associated with a specific user.



To view the reference topology and its status, you need to save the reference topology in the Reference editor at least once. When you save the reference topology in the Reference editor, the network devices along with new devices added to this topology are shown in the monitoring topology. The detailed view of the monitoring topology shows both discovered devices as well as monitored devices. The color of these devices and ports depends on their current state. The connection line color, on the other hand, depends on the state of connected ports. The topology also displays the network view starting from the SINEMA Server station in a hierarchical structure.

Note

Refreshing the monitoring topology to show the latest changes takes about 3 to 5 seconds. Since the autorefresh mechanism is enabled in the monitoring topology, the changes will be shown automatically in the next user interface refresh cycle. To view the changes without waiting for this, start a manual refresh by clicking the refresh button in the monitoring topology.

Parts of the detailed view

The monitoring topology detailed view layout consists of four separate parts containing information specifically relating to the reference status of the devices discovered in the network. The parts of the monitoring topology are shown below.

1. Device view area
2. Toolbar
3. Device hierarchy
4. Bird's eye view

Note

The detailed explanation of the parts of the reference editor view "*Reference editor view*" in section 5.1.5.1 also applies to the parts of the detailed view. In the monitoring topology, the device hierarchy pane includes the "All devices" folder that contains only those devices that are shown in the device view area. The unmanaged devices "Catalog panel" is not shown in the monitoring topology detailed view.

Note

The Toolbar has the same toolbar icons as shown in "Actual topology". However, in "Monitoring topology" > "Detailed view", the "Recalculate topology" icon is not available.

Shortcut menu

A shortcut menu is available in the device view area. This can be accessed by right-clicking on the device. The options in the shortcut menu depend on the selection in the device view area. The shortcut menu includes the following two options:

- View device details
- Device-specific link

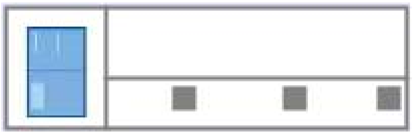
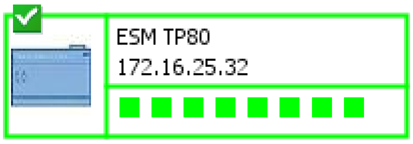
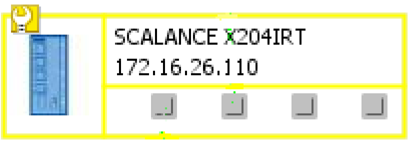
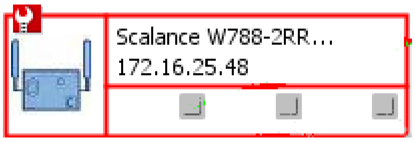
If you have not made a selection in the topology editor, the shortcut menu is shown after right-clicking in the device view area. The no selection shortcut menu includes the following options:

- Zoom in
- Zoom out
- Refresh

Status monitoring

The status of devices, ports and connections including WLAN connection changes are represented by different color codes.

Device state

Device state	Description
	Device not in view; State: Unknown
 ESM TP80 172.16.25.32	Device in view; State: SNMP/DCP reachable
 SCALANCE X204IRT 172.16.26.110	Device in view; State: Reachable; SNMP/DCP not reachable
 Scalance W788-2RR... 172.16.25.48	Device in view; State: Not reachable

Status icon	Description
✓	Device in view; State: Up
🔧	Device in view; State: Up - maintenance requested
🔧	Device in view; State: Up - maintenance demanded
🔧	Device in view; State: Fault

Port / interface state:

In the monitoring topology detailed view, the color code representation of the port status is different compared to the actual topology. Each port shown in monitoring topology displays 2 states - actual state and resulting state. This state is based on a comparison with actual and reference states.

- The actual state is shown by the border color of the port
- The resulting state is shown as the fill color of the port in the rectangle

Note

In the monitoring topology, if a device is not in view, it is displayed gray. All ports of an unreachable device are shown in light gray with a gray border around the port. As a result, all connections to another unreachable device are also shown in gray.

Port state	Fill color / border color
Up	🟩
Up - maintenance requested	🟨
Down - maintenance demanded • With actual connection • Without actual connection	🟥 🟥
Down • With actual connection • Without actual connection	◼ ◼
Unknown	⬜

Isolated port

Redundancy state (device details)	Standby port status	Fill color / border color
Active	Up	🟩
Active	Up - maintenance requested	🟨
Active	Down - maintenance demanded With actual connection Without actual connection	🟥 🟥
Active	Down With actual connection Without actual connection	▣ ■
Active	Unknown	⬜
Passive	Up	🟦
Passive	Up - maintenance requested	🟨
Passive	Down - maintenance demanded With actual connection Without actual connection	🟥 🟥
Passive	Down	▣
Passive	Unknown	⬜

LAN connection state

The connection line in the monitoring topology displays the reference topology connections. For LAN connections, the color depends on the fill colors of both connected interfaces.

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

WLAN connection state

Reference connection status - active	Line color
No	▬
Yes	▬ **Note:** The color of an active reference connection depends on the port color (green, red or light gray)
No	▬
Yes	▬ **Note:**The color of an active reference connection depends on the port color (green, red or light gray)
No	🟥

WLAN active connection state

A reference connection is treated as an active connection if one of the reference connections matches the actual WLAN connection. The active connection color depends on the color of both ports. Yellow and dark gray are used to represent an invalid port state if a reference connection is defined. All other reference connections that are not active between a client and several APs are displayed in gray.

Port 1	Port 2	Color of active connection between client and AP
🟩	🟩	🟩
🟩	🟥	🟥
🟩	⬜	🟩
🟥	🟩	🟥
🟥	🟥	🟥
🟥	⬜	🟥
⬜	🟩	🟩
⬜	🟥	🟥
⬜	⬜	⬜

5.1.4.2 Icon view

Display options

"Network > Monitoring topology > Icon view" displays an icon view representing all devices discovered in the current network including new devices.

General information

The Icon view can be accessed by clicking the "Icon view" button in the toolbar of the "Monitoring topology" page. The icon view displays the network topology as a structured view in the form of icons. The devices and their connections in the current network along with their reference status are displayed as icons in this view. This view helps you to get a closer look at the network structure containing the devices and their connections represented as small icons visible in the monitoring topology.

Note

Each time the screen is refreshed, the zoom level and view position remains the same for both the detailed view and icon view.

Using the icon view

To select a device in the icon view, left-click on any device listed in the device view. The device icon is then highlighted in blue. To view the device details specific to the selected device, double-click on the device icon in the device view. A tooltip text is shown both for devices that are connected and also for the set of devices that are shown as unconnected in the icon view. The tooltip displays the device information as well as the IP address of the network devices in the icon view.

The screen layout is optimized for the current detected topology. This view is helpful when you want a complete view of the devices within the network as icons. The tree view can be customized in terms of device and connection management using the Reference editor.

Icon view features

In the icon view, the devices are displayed as icons instead of ports. The start and end port number along the connection lines are shown in the icon view. This view displays the network structure such as ring, star and linear bus topology represented as icons. The icon view is located in the middle of device view area. The way the connections are displayed in an icon view varies according to the type of topology.

Note

Modifications to the nodes or connections are not permitted in the icon view.

5.1.5 Reference editor

Overview

The **Reference editor** displays a reference topology that includes a summary of all devices, port states and connections. The Reference editor provides options with which you can correct the discovered topology and set this corrected version as the reference topology. Only administrators have access to the Reference editor.

5.1.5.1 Reference editor view

Display options

The **Network > Reference editor** menu item displays a perfect reference topology view including all connections and representing all devices that have been discovered in the current network and so provides a complete network topology view. The Reference editor provides options with which you can correct the discovered topology and set this corrected version as the reference topology.

Purpose and use

In a large network, there may be several places where the topology does not represent all connections or false connections max be discovered. One reason might be that some devices on which SNMP is deactivated are discovered within the network. LLDP MIB support may not be available on these devices. It is also possible that unmanaged devices are discovered in the network. To obtain comprehensive and correct reference topology information and to give users the option of editing this topology manually, a reference editor is required.

The **Network > Reference editor** always displays a full reference topology. It displays all network devices including new devices. Non-monitored devices are not shown in this topology view. The topology displayed in the reference editor is based on the actual topology. The reference editor also helps you to correct the actual topology by setting the corrected network topology as the reference or target. A reference editor is used to do the following:

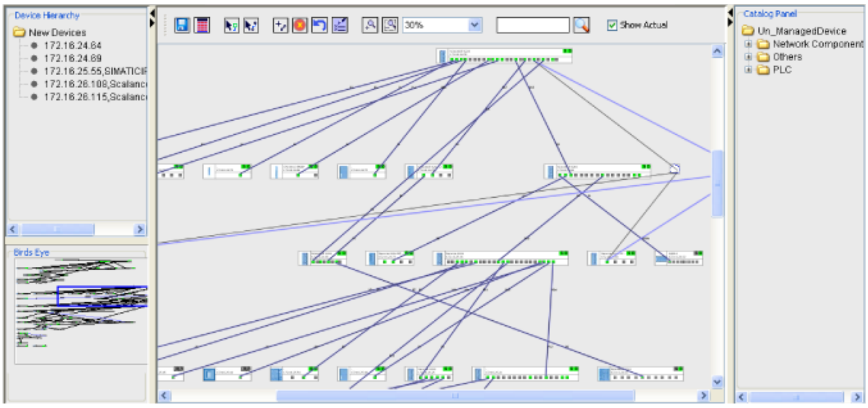
- Draw/edit reference connections
- Configure/set the status of the ports
- Configure references for SNMP, DCP protocols

Note

By default, only users with administrator permissions have access to the Reference editor. If more than one administrator works with the reference editor, the topology saved last is taken as the reference topology.

General overview

The Reference editor is used to define the reference topology. It provides options allowing you to edit the reference topology manually. Initially, the reference editor checks to whether or not a reference topology exists. If no reference topology is defined, the actual topology is used to sort the devices. This remains the situation until the reference topology is configured.



Note

When SINEMA Server first loads the reference topology, all the ports that have the unknown state are shown as having the "Down" state. When you save this topology information, this "Down" status is also saved.

Reference editor features

The reference editor provides a series of features as listed below:

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

Show / hide top pane and left pane

To obtain a larger view of the reference editor so that you can see all the devices, you can hide the top pane and left pane in the SINEMA Server application. Once the contents of the editor view are loaded, you can see the controls for hiding the top pane and left pane.

Show / hide top pane:

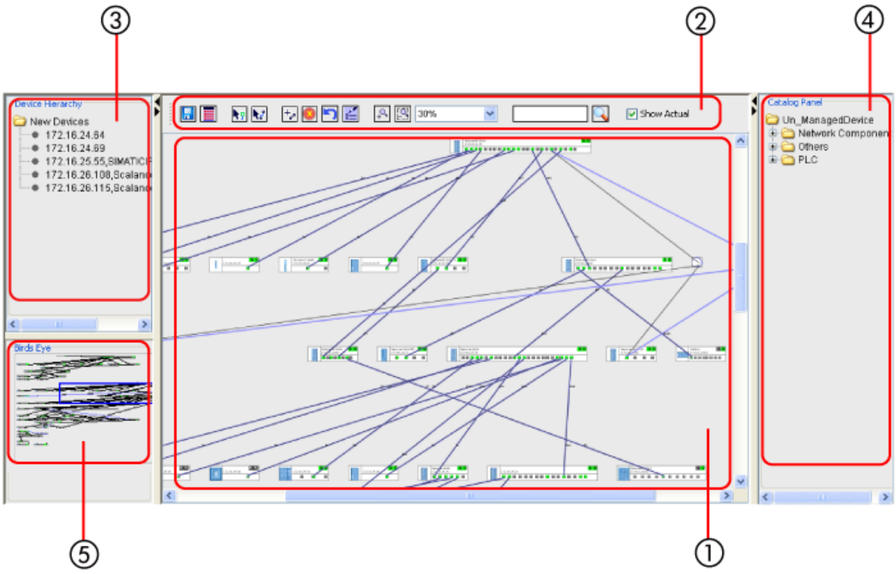
To hide the top pane, click "Hide top pane". Once the top pane is hidden, you will see that the control has changed to "Show top pane". You can click "Show top pane" if you want to display the top pane again.

Show / hide left pane:

To hide the left pane, click "Hide left pane". Once the left pane is hidden, you will see that the control has changed to "Show left pane". You can click "Show left pane" if you want to display the left pane again.

Parts of the Reference editor view

The layout of the reference editor view consists of five separate parts containing the full information specifically relating to the topology of the devices discovered in the network. It always shows a full reference topology. All monitored devices including new devices are displayed in the editor view. Non-monitored devices are not shown in the editor. The parts of the reference editor view are shown below.



1. Device editor view area
2. Toolbar
3. Device hierarchy (new devices)
4. Catalog panel (unmanaged devices)
5. Bird's eye view

1. Device editor view area

The area of the device editor view displays the topology tree including actual and reference connections with the connections between the devices discovered in the network. This topology tree is shown in the device editor view after selecting the "**Network > Reference editor**" menu item. This tree view includes the display of nodes, their connection lines and the corresponding port status of the actual and reference topology displayed in the reference editor.

To select a device in the device editor view, left-click on the device. The device is selected and is highlighted in blue.

The following sections describe the parts and functions of device editor view:

Display of nodes/connections/ports

In the device editor view area, the reference editor screen shows the topology information of all the devices connected in the network. An unknown device in the reference editor is shown as a cloud. Each device node can have an icon as well as a text area and a port area associated with it. The default display in the text area shows the device name and IP address. The content of the text area of a specific device can be configured using the *Configure node* button. This button is available in the toolbar.

The connection lines in the device editor view area contain line numbers at both ends of the connection. This is the same for both actual and reference topology connections. The protocol support available on each device is shown in the right-hand corner of the text area. The two protocol states "S" and "D" indicate SNMP and DCP reachability status. A strike through icon is used to indicate that protocol support is unavailable for the specific device.

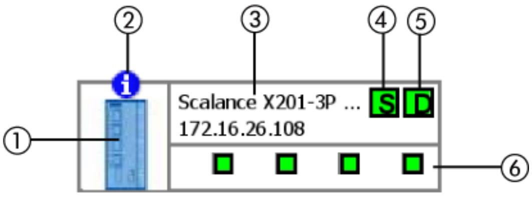
Shortcut menu

A shortcut menu is available in the device editor view area. This can be accessed by right-clicking on the Reference editor. The options available in the shortcut menu depend on the selection in the device editor view.

Mode	Selection area	Shortcut menu options
Select	Device port	• Up • Down
Select	Device protocol	• Activate • Deactivate
Draw	Actual connection line	• Change to reference
Select or draw mode	No selection	• Zoom in • Zoom out • Refresh

Status monitoring

You can monitor the status of the network devices, their ports and connections in the Reference editor view with the help of various representations of ports, connection lines and protocol-specific device availability status. Each device in the editor is represented by a device icon, a node text area, protocol options and a port area. The ℹ symbol is displayed above the device icon in the node to denote a new device. Below, you will see the graphical representation of a device and its contents:



1. Device icon
2. New device icon
3. Node text area
4. SNMP protocol
5. DCP protocol
6. Device ports

Note

For device ports, the border color around the rectangular area is used to indicate the status in the actual topology. The inner color of the port indicates the reference or monitoring status.

The different port states and protocol-specific device availability are represented as follows:

Port state:

Target state	Show actual	Border color	Up	Down
Up / Testing / Up - maintenance requested	Enabled	Green	🟩	◼
Up / Testing / Up - maintenance requested	Disabled	Black	🟩	◼
Down / Down - maintenance demanded	Enabled	Gray (dark)	🟩	◼
Down / Down - maintenance demanded	Disabled	Black	🟩	◼
Unknown	Enabled	Gray	🟩	◼
Unknown	Disabled	Black	🟩	◼

Protocol-specific device availability status:

State	Show actual	Color of rectangle around SNMP icon
reachable	Enabled	S
reachable	Disabled	S
not reachable	Enabled	S
not reachable	Disabled	S
not activated	Enabled	S
not activated	Disabled	S

State	Show actual	Color of rectangle around DCP icon
reachable	Enabled	D
reachable	Disabled	D
not reachable	Enabled	D
not reachable	Disabled	D
not activated	Enabled	D
not activated	Disabled	D

Note

The "not reachable" state depends on the target state of the device. SNMP may or may not be supported on the device. If SNMP support is available for the device, the inner color is green otherwise it is gray.

Using select mode and draw mode

The Select tool icon is available in the Reference editor toolbar. This icon is used to enable select mode. The Select tool icon is then disabled while you are working in Select mode. This mode is enabled by default once you access the Reference editor. In this mode, the following actions can be performed:

- Drag and drop devices from the unmanaged devices catalog to the Device editor view area
- Drag and drop devices from the new devices catalog to the Device editor view area
- Change the reference status of the port to Up / Down
- Modify the protocol-specific device availability status for SNMP and DCP protocols
- Delete reference connections and unmanaged devices
- Remove managed devices and move the device to the new device catalog

Note

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

The Draw tool icon is available next to the Select tool icon in the Reference editor toolbar. To change to Draw mode, select the Draw icon. In this mode, the following actions can be performed:

- Draw a connection between ports belonging to different devices
- Change the actual connection to a reference connection

In draw mode, a connection line can be drawn between two devices by clicking on the ports of the devices to be connected. A dialog box is displayed where you select the port numbers of the devices to be connected. This allows connections to be drawn between two devices.

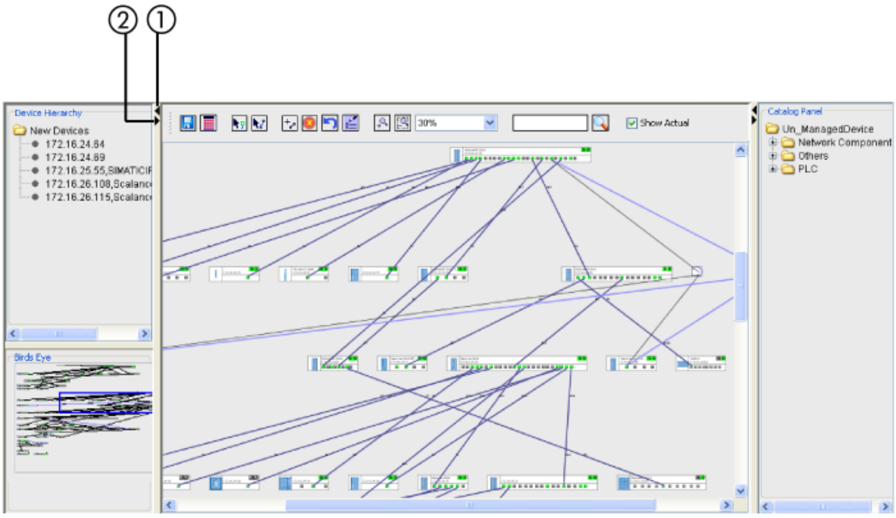
2. Toolbar

The Reference editor includes a toolbar that contains toolbar icons for performing different actions when configuring ports and managing actual and reference connections between devices. You can display information about each of the toolbar buttons using the Tooltip option. The toolbar buttons are available for the following operations:

Icon	Description
💾	Save the changes to the Reference editor.
▦	Recalculate topology based on reference connections
↖	Select mode
↖	Draw mode
✚	Use actual as reference
⊗	Reset reference topology
↶	Discard changes
▨	Configure node
🔍+	Zoom-in topology: Magnifies the image by the preset zoom factor.
🔍−	Zoom-out topology: Reduces the image size by the preset zoom factor.
100% ▾	Set zoom percentage: Provides options for selecting the zoom factor (as a percentage).
▭	Text box for entering IP address to be searched for.
🔍	Search button to search for the network device.
☑ Show Actual	Shows actual connections between devices including the actual port status.

3. Device hierarchy (new devices)

The Reference editor includes the "Device hierarchy" pane that consists of all new devices. This pane is shown on the left-hand side of the Reference editor view. When you select the "Network > Reference editor" menu, the device hierarchy area is automatically hidden. To view the device hierarchy pane, drag the resize handle of this view to the right so that the network device list is visible. To hide the device hierarchy pane, click the control (1). Click the control (2) in the upper-left corner of the main window and the device hierarchy pane appears.



New devices can be added to the reference topology by dragging and dropping the devices. You can also do this either by double-clicking on the new device or using shortcut menu option. When the Reference editor is accessed, all discovered connections with actual connections are displayed automatically in the center of the device editor view area. Only unresolved devices and devices that have been newly discovered are included in the new devices list. Devices in the Device hierarchy pane are not part of the reference and are therefore not shown in the monitoring view.

Note

Devices with no actual connection between the devices and ports in the topology tree are classified as unresolved devices.

After the new device has been added to the Reference editor area, this device is no longer available in the New devices folder. This device will be visible in the monitoring topology only after the reference topology has been saved. If a device is deleted, it will be shown again in the New devices folder in the Device hierarchy pane.

4. Catalog panel (unmanaged devices)

The Catalog panel includes a list of categories for predefined device types. Each category consists of several predefined network devices that have not been identified by SINEMA Server. Such device types can be added to the reference topology using the device types in the catalog panel. To add unmanaged devices to the reference view, go to the required folder and drag the predefined network devices to the reference topology area.

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

Note

If you display the Reference topology page, the Catalog panel will be hidden by default. To view the Catalog panel, drag the resize handle of this view to the left so that the unmanaged device categories are visible.

5. Bird's eye view

The bird's eye view is located below the New devices catalog. This view includes a display of the complete topology tree structure represented as a bird's eye view. The entire viewing area of the topology tree is shown in this window. The sliding frame available in this view helps you to place the focus on a specific area within the topology. When the frame is placed over the area containing network devices in this view, the control in the Device editor view displays the area containing these network devices.

Reference editor edit mode

In the center of the the Reference editor, there is a device editor that displays a reference view. This first checks whether or not a reference topology is available. If no reference topology is available, the actual topology is used. After you access the Reference editor page, the network devices will be automatically sorted into hop layers based on the actual connections. Several hop layers exist in the Reference editor view. The network devices are placed in a hop layer based on the connections.

- For devices that have actual connections, the location is calculated automatically based on the actual connections.
- For devices that do not have actual connections, the devices are placed at the end of lowest hop layer.

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

The Reference editor toolbar includes a "Show actual" check box that is selected by default. While this option is enabled, the actual topology connections are displayed along with reference connections between the devices. To allow better identification or to view actual connections and port status, the "Show actual" option allows actual connection lines to be displayed in light blue in the Reference editor. Reference connections are displayed in black. This means that actual and reference connections are clearly distinguished. The "Show actual" option also provides color coding for the actual port status and actual protocol-specific device availability status in the Reference editor. The small rectangular border around ports indicates the actual port status. The border around the protocol-specific device availability icon indicates the actual protocol-specific device availability status.

Unknown devices in the reference editor are represented by a cloud. Connections can nevertheless exist between ports of other devices and the cloud devices.

Recalculate topology

In the reference editor, whenever the reference topology is loaded, the device hop levels are based on the actual topology. To base the hop levels on on reference connection, you can use the "Recalculate topology" icon. When you click the "Recalculate topology" icon, the devices with reference connection(s) will be layered based on the corresponding reference connections.

Note

When the recalculation of the topology is based on reference connection(s), the device positions will be based on the reference connection(s) of the relevant device(s) each time the reference editor is loaded.

5.1.5.2 Working with the Reference editor

General overview

The Reference editor provides a complete reference topology view that includes an updated topology representing devices, ports and their connection status. This editor also allows you to edit connections, change port status and configure protocols supported by devices in the network.

Configuring reference connections

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

- Draw connections manually between devices and ports of other devices
- Change an actual connection to a reference connection by double-clicking
- Change an actual connection to a reference connection using the shortcut menu

The following option can be configured only in Select mode:

- Change all or selected actual connections to reference connections using the "Use actual as reference" button

Drawing connections manually between devices

1. In the Device editor area, click the specific port of a device using the mouse.
2. Choose a specific device to which you want to draw a connection and select the port.
3. You will see that a connection line is drawn between these two devices.

In Reference editor draw mode, a connection line can be drawn between two devices by clicking on the ports of the devices to be connected. A dialog box is displayed where you select the port numbers of the devices to be connected. This allows connections to be drawn between two devices.

Changing an actual connection to a reference connection by double-clicking

To change an existing actual connection to a reference connection, double click on the connection line representing an actual connection. The line color changes to black indicating a reference connection. In the background, you will see a light blue color appear.

Changing an actual connection to a reference connection using the shortcut menu

Select the connection line that represents an actual connection shown in light blue. Right click on the connection line and select the "*Change to reference*" option in the shortcut menu. The connection line changes to black indicating a reference connection.

Changing all actual connections to reference connections using the "Use actual as reference" button

This option is available in the toolbar view and can be used only in "Select" mode. This icon resembles the shape of a funnel and is located next to the "Draw tool" icon in the toolbar. Click this icon to convert all actual connections to reference connections. A dialog box is displayed with Yes/No options prompting you to decide whether to continue. Select "Yes" if you want to convert all actual connections to reference connections.

Configuring the reference port status

The Reference editor provides options for managing the port status. It is, however, not possible to change the reference status of ports with reference connections. The reference port status can be configured in "Select" mode using any of these options:

- Toggle port status manually by double-clicking
- Change port status using the shortcut menu
- Change port status using "Use actual as reference"

Toggle port status manually by double-clicking

Double-click on the port of a specific device to toggle the state between "Up" and "Down"

Change port status using the shortcut menu

Select the required port in the editor view and right-click with the mouse. A shortcut menu appears with options to select the "Up" or "Down" state or the port.

Configuring reference protocol-specific device availability

The Reference editor provides options with which you can enable or disable the SNMP or DCP protocol-specific device availability status in a device. If a device type supports the protocols, the status can be modified. The initial status of the device protocols is taken from the device type. Initial reference protocol-specific device availability is the protocol actually discovered. The reference protocol-specific device availability can be configured using any of these options:

- Toggle protocol-specific device availability status by double-clicking
- Changing protocol-specific device availability status
  - Change the protocol-specific device availability status of one device to reference status
  - Change the protocol-specific device availability status of several devices to reference status
  - Change the protocol-specific device availability status of all devices to reference status

Toggling protocol-specific device availability status by double-clicking:

To change the protocol-specific device availability status, double click the protocol-specific device availability icon. The relevant protocol toggles between available and unavailable status. A strike through icon is used to represent the unavailable status.

Note

If the network device does not support the SNMP or DCP protocol, it will not be possible to configure the reachability status of the protocol. The unsupported protocol will be indicated by a strike through icon.

Changing protocol-specific device availability status:

if you select a single device and click "Use actual as reference", the actual protocol-specific device availability status will be converted to the reference status. if you select more than one device and click this button, the response is the same as with a single device. This also applies if you select all devices.

Configuring network cloud connections

A network cloud is a special type of unmanaged device. Any device that does not have an IP address and is surrounded by 3 or more LLDP devices is identified by SINEMA Server as a network cloud. Each network cloud is assigned a unique name. This name is displayed in the reference topology editor. In contrast to other unmanaged devices, a network cloud has no ports. A network cloud can, however, act as an end point for several connections.

Clouds identified by SINEMA Server have the name "VirtualDevice *XXX" (XXX represents the index number 1 or 2 or 3, etc). Let us assume that we have a cloud in the actual topology. Conversion of this actual cloud (including all connections) to the reference cloud results in the following set of actions:

- The connection line changes to black indicating a reference connection.
- A replica of the actual cloud is created (Reference Cloud*1) after reloading the reference topology.
- The same set of connection partners is available just as for the actual cloud.
- This reference cloud is displayed in the monitoring topology and will continue to exist in the application until the cloud is deleted.
- Both the actual and reference cloud are always displayed in the reference editor.
- If the actual cloud is converted to a reference cloud (Reference Cloud*2), a new reference cloud is created. The old reference cloud becomes orphaned.

Note

The orphan clouds can be either deleted manually or the application itself deletes this reference cloud when the reference topology is reloaded. To display a reference cloud, at least one reference connection needs to be available in the editor.

Reset reference

The "Reset reference" button is used to reset the reference view to its original status. This option resets the changes in the reference view by discarding any changes that are made in the reference topology editor. Use the "Reset reference" button when you want to start with a fresh reference for all statuses other than connections.

The following actions are performed when the "Reset reference" button is used:

- All the reference connections drawn and the devices added by the user are deleted.
- The reference port status is reset. If the original or previous status is unknown, the editor waits for the next "Up" or "Down" status of the port.
- The protocol-specific device availability status is deleted.

Add new devices

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

1. Click "Select mode" in the Reference editor toolbar.
2. Select the required device listed in the "New devices" folder.
3. Drag the new device to the reference view.
4. Similarly, a set of new devices can be added by holding down the Shift key and dragging and dropping them.
5. Once the new device is added to the reference view, the device disappears from the New devices list.
6. Click the "Save" button to save these changes after adding the reference connections with new devices.

Add unmanaged devices

SINEMA Server application provides options with which you can add unmanaged devices to the reference topology to allow you to configure a complete topology. When you are in "Select" mode, the unmanaged devices can be added to the reference view and these devices cannot be monitored. The unmanaged devices can be added to the reference view by dragging them from the unmanaged device catalog available on right-hand side of the view. Each unmanaged device is assigned a unique name when the device is added to the reference view. This unique name helps to identify the device while creating a reference topology.

Save reference topology

The "Save" button is located in the Reference editor toolbar. This option saves the existing reference topology status and its connections. After relevant changes are made in the Reference editor if you do not save, the changes will not be present if you change to any other pages in the application. Click the "Save" button to save the changes made in the reference topology.

Note

Whenever the reference topology is saved, the corresponding changes can be seen in the monitoring topology. Refreshing the monitoring topology to show the latest changes takes about 3 to 5 seconds. To view the changes without waiting for this, you can perform a manual refresh by clicking the refresh button in the monitoring topology.

Port type resolution when using different combinations

In the reference editor, a maximum of 1 connection can be drawn from an unknown port to any other port. If you attempt to draw more connections on a single unknown port, this will be considered as a change of connection partners. The old connection will then be replaced by the new one.

It is possible that there are many devices with unknown medium types and connections are permitted between any medium types. The exact medium type must, however, be identified and a connection drawn so that the correct combination type is selected. The popup message "Please make sure that port types of both ends are connectable to each other" prompts you to check that the combination is correct. This popup message is displayed only while drawing a connection between a specific combination of medium types. The various combinations of medium types and whether or not they cause a prompt to be displayed can be seen in the table below:

Combination of medium types	Connection allowed	Explicit prompt displayed
Copper - Copper	Yes	No
Copper - Fiber	Yes	No
Copper - Wireless	Yes	Yes
Fiber - Fiber	Yes	No
Fiber - Wireless	Yes	Yes
Wireless - Wireless	Yes	No
Unknown - Unknown	Yes	No
Unknown - Copper	Yes	Yes
Unknown - Fiber	Yes	Yes
Unknown - Wireless	Yes	Yes

5.1.6 User-defined maps

Overview

A **user-defined map** displays a map area that helps you to create, view and manage network devices and connections to be monitored between these devices. It provides various options with which you can modify a user map, draw connection lines and view reference connections. The topology displayed in a user map is based on the reference topology only.

User-defined maps are used when you want to monitor a limited set of devices within the network. This makes it easier to manage user-defined connections and provides options for viewing and identifying both user-defined connections and reference connections in their specific colors.

5.1.6.1 User-defined maps view

Display options

The **Network > User maps** menu item is used to create, view and manage user-defined maps. The connections between these devices include reference connections as well as user-defined connections. This page provides options for creating a map, deleting a map, renaming a map, editing a user map, activating a user map and editing or deleting notes.

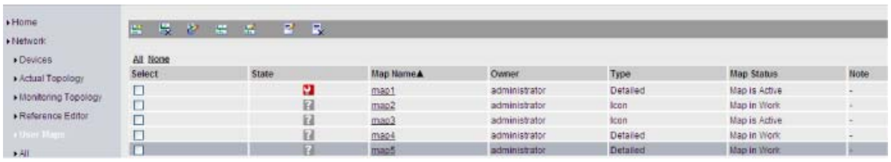
Purpose and use

Dividing a very large network topology hierarchy into small groups made up of a set of devices helps you when managing or monitoring the devices and their connections. This is the main reason for using user maps. User maps also provide options that allow you to configure the list of monitored devices displayed in a user map. This can be used to monitor the port status of a small set of devices with user-defined connections.

When you select the **Network > User maps** menu, the User maps page is displayed. This page includes a table view that contains the map name, name of the owner, state of the map, the type and its status. All maps belonging to the current user are listed in this table view. Each map includes a hyperlink that helps you to view the user map containing the list of network devices. If the user has not created any maps, this table view will be empty.

To allow you to work with user maps, the user maps page provides certain controls in the form of icons. The icons and their meaning are described below:

Icon	Description
	Create map
	Delete map
	Rename map
	Activate map
	Edit map
	Edit note
	Delete note



Select	State	Map Name▲	Owner	Type	Map Status	Note
□	✓	map1	administrator	Detailed	Map is Active	-
□	?	map2	administrator	Icon	Map in Work	-
□	?	map3	administrator	Icon	Map is Active	-
□	?	map4	administrator	Detailed	Map in Work	-
□	?	map5	administrator	Detailed	Map in Work	-

User map features

User maps provide a series of features as listed below:

- Configure user-defined connections
- Draw user-defined connection
- Change connection layout
- Add unmanaged or managed devices
- Add link to another user map
- Create user map as a copy

Creating a user map

To create a user map, follow these steps:

1. On the User maps page, click the "Create map" icon to create a user map.
2. A new page is displayed that contains the options for creating a user map.
3. Enter a unique name for the user map in the "Map name" text box.
4. Select the "Map type" (icon / detailed) for the user map by selecting the appropriate option.
5. Select "Map mode" (Empty / Reference topology) from the table view options to specify the content of the user map.
6. Empty view creates a blank view and does not contain any network devices.
7. Click the Save button to save these changes. You then go to the table view that lists the new user map.

Note

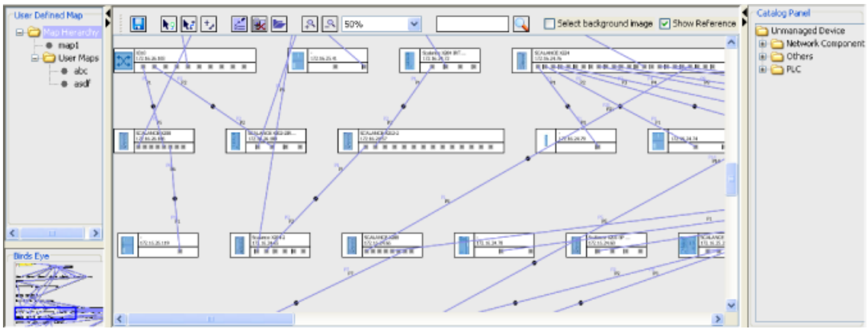
Existing user maps will be listed in the "Map mode" table view only when the user map is in the "Active" state. The Map mode displays the corresponding maps based on the radio button selected for the "Map type".

Note

The user who creates the user map is automatically its owner. The user has full rights to modify, rename or delete the user map. The administrator can only view the user map.

Viewing user maps

A user map can be viewed on the **Network > User maps** page. On this page, a table view is shown with multiple rows. Each row corresponds to a user map consisting of the "Select" check box, map name, owner name, user map type and status information relating to the user map. To view a user map, click the map name hyperlink in the table view. The user map is then displayed as shown in the screenshot below. The map contains either an icon view or detailed view depending on the "Map type" selected when the user map was created.



If you selected an empty view, you will see a blank view without any devices or connections. You can, however, add devices to a user map by dragging them, double-clicking or using the shortcut menu option "Add to map". If a reference topology map name is selected while creating a new user map, you will see that all reference devices along with their connections and status are copied to the user map device view area. Any new devices found in the network or devices recently added to the reference editor can be seen in the map hierarchy folder in the "User-defined map" pane.

User map status

A user map can have one of two statuses - *Design* and *Active*. When a user map is created, it has the "Design" status indicating the draft mode. The map status is shown in the table view visible when viewing user maps. The "Design" status refers to the actual working status of the user map and means that the user can make modifications to the map. Changes can only be made to the user map when it is in the "Design" status.

Note

To change a map with the active status to the design status directly and at the same time open the user map for editing, use the "Edit map" button. This button changes the the status of map to the design status and opens the user-defined map.

The "Active" status indicates that a user map is ready to use. It signifies that user map design has been completed. You cannot make any changes to the user map when it is in the active status. You will, however, see that the existing user maps are displayed in the "Create user map" page if the user map is in the Active status. This allows you to copy the existing user map to a new user map.

The State column displays the icons indicating the user map status. The status icons and their meaning are shown below:

Icon	Description
?	User map in the "Design" status
🔧	User map in the "Active" status

Activate map

When it is created, the map automatically has the "Design" status. To change the "Design" status to "Active", select the user map and click the "Activate map" icon.

The following points apply to the map when in the "Active" status.

- User maps can be associated with specific users.
- The user map cannot be edited. You cannot make any changes to the map.
- The actual monitoring status of the device can be seen while the map is active.
- Maps cannot be renamed while they are in the "Active" status.

The following points apply to the map when in the "Design" status.

- The user map can be edited. Changes to the user map are permitted.
- Monitoring of the status of devices is not possible.

Renaming user maps

The list of existing user maps can be viewed in a table when you open the "User maps" menu. Select the check box belonging to the required user map and select the "Rename map" icon. The map name is cleared from the text box allowing you to enter a new name for the selected user map. Enter the new name for the user map and click the "Save" icon to save the changes. The selected user map now has a new name.

Modifying user maps

The administrator or the owner of the user map can modify existing maps. Click on the map name to view the contents of the user map. You can make changes to the user map in the user map device view. Below, you will find a list of the options available when modifying an existing map.

- Add devices from the user-defined map pane
- Add unmanaged devices from the catalog panel
- Delete device
- Reset connection layout
- Create or edit a user-defined connection
- Change a reference connection to a user-defined connection
- Delete a user-defined connection

Note

After you have made the changes to the user map design and before closing the user map, it is a good practice to save the current map. To save the user map, click the "Save" icon in the toolbar.

Deleting user maps

To delete the user map, select the user map by clicking the "Select" check box and then clicking the "Delete" icon. The user map is then deleted.

If the map is deleted by the owner, the user map is completely deleted and all reference links are removed. However, if an administrator or other users delete the user map, only the references will be deleted. The user map still exists and may not be visible to them. The owner will still be able to view the user map.

Associating users with a map

To associate a user with a map, follow these steps:

1. Firstly, make sure the user map has been created and the devices are present in the map.
2. Save the content of the user map.
3. Go to **Admin** > **User admin** and click the "Add new user" icon.
4. Specify the required details on the New user page.
5. Select the specific user group you want the map to be associated with.

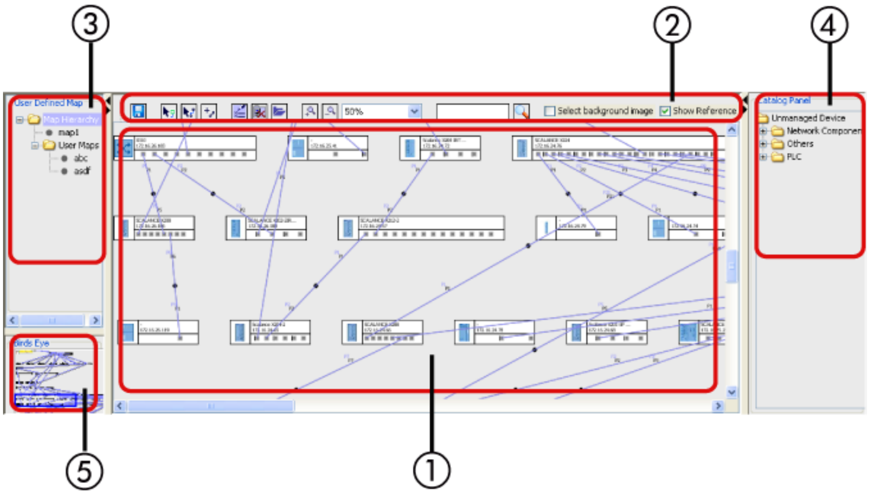
6. In the "Associate maps" row, you will see a list of the user maps in the "Active" status.
7. Select the check box belonging to the required user map and select the "Save" option.

Note

User maps can be associated with a user only if the map is in the "Active" state.

Parts of the user map

The user map layout consists of five separate parts containing information specifically relating to the topology of the devices detected in the network.



1. Device view
2. Toolbar view
3. User-defined map pane
4. Catalog panel
5. Bird's eye view

1. Device view

The user map device view area displays the tree structure with the connections between the devices detected in the network. This depends on the map type and map name selected when you created the user map. This topology tree containing reference devices and reference connections is shown in the device view area after opening the user map. This tree view includes the display of the reference topology nodes, reference connection lines and the corresponding reference port status displayed in the user map view. Each node in the tree includes the device icon, node text area and port area. New devices are displayed in the user defined map pane. In the user map, the reference connections are shown in light blue and user-defined connections are gray.

if you create an empty view, you will not initially see any topology information in the user map device view area. You can drag available devices from the user-defined map pane.

Note

Connection lines can be drawn between unmanaged devices, managed devices or between managed devices and unmanaged devices.

Shortcut menu

A shortcut menu is available in the user map view that provides you with options for creating or managing devices in the map. The options available in the shortcut menu depend on the objects selected in the user map.

Note

This shortcut menu is available only when the user map is in the "Design" status.

Note

The shortcut menu options shown in following table are displayed using the "Select" tool. The "Delete device" option is displayed when you are using the "Select" tool and "Draw connection" tool.

Selection area	Shortcut menu options	Notes
Reference connection	• Change to user-defined	• Changes a reference connection to a user-defined connection
User-defined connection	• Delete connection • Reset connection layout	• Deletes the connection • Resets the layout of the connection
Background image	• Delete image	• Deletes the background image
Network device	• Delete device	• Deletes the device from the user map and all connections that are connected to the deleted device
User map link icon	• Delete map • Properties	• Deletes the user map link icon • View user map properties
Association link	• Delete map connection	• Deletes the map connection line

Status monitoring

A user map has two modes - active mode and draft mode. In draft mode, you can position devices in the layout. You can also redefine the layout of user-defined connections and draw unmanaged devices and connections to managed devices.

In active mode, the user map displays the color code indicating the device state, interfaces and connections similar to the monitoring topology connections.

Note

The status of device icons, the port state and connection line shown in the section **Monitoring topology > Detailed view** is also applicable to the topology tree view shown in user maps.

---

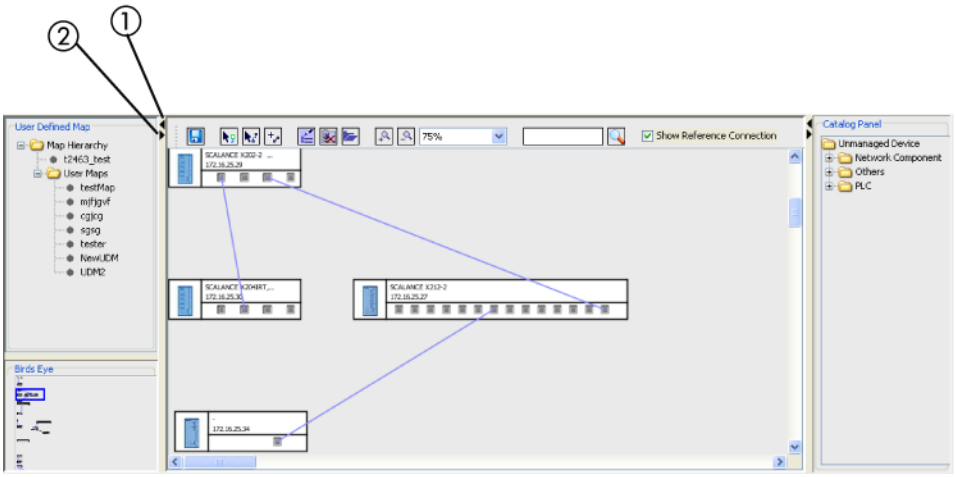
2. Toolbar view

In user maps, a toolbar is available at the top of the user map view window that provides various options for viewing the network devices and controlling them. The toolbar icons and their meaning are shown below:

Icon	Description
💾	Save map details
↖	Select tool
↖	Draw connection tool
↖	Create user-defined connections for all reference connections
▨	Configure node
☒	Delete device
📂	Add a background image to a user-defined map
🔍	Zoom-in topology
🔍	Zoom-out topology
100% ▾	Set zoom percentage
▭	Enter IP to search for
🔍	Search for device
□ Select background image	Select background image
☑ Show Reference Connection	Show reference connection

3. User-defined map pane

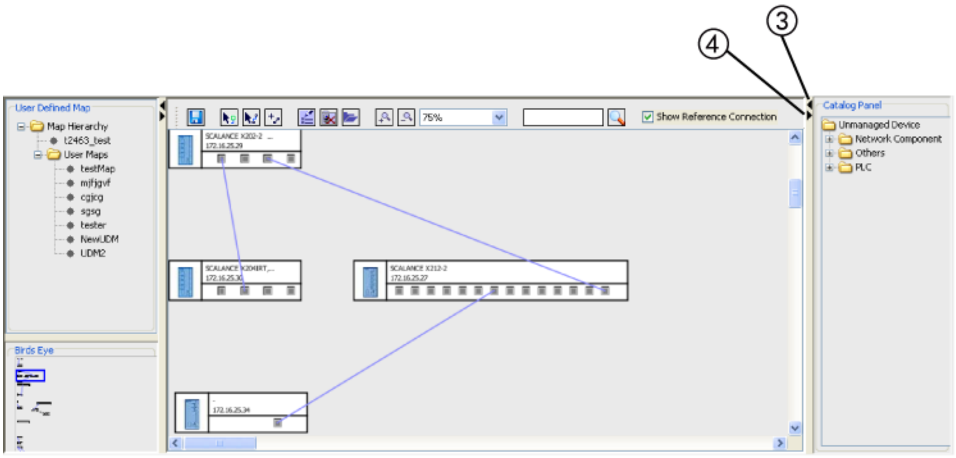
To open the user map, select the relevant map by clicking on the user map name in the **Network > User maps** page. In the user map, you will see that the "User-defined map" pane is hidden by default. To view the user-defined map pane, drag the resize handle of this view to the right so that the network device list is visible in the "User-defined map" pane. To hide the "User-defined map" pane, click the control (1). Click control (2) in the upper-left corner of the main window and the user-defined map pane reappears.



This pane is displayed in the left panel of the user-defined map. All the devices found during the scan are displayed in a hierarchical structure. The user map name itself is used as the subfolder name that contains the list of devices. The subfolders are grouped together in the Map hierarchy folder. The devices in the subfolder can be moved to the device view by dragging them or by double-clicking on the network device in the "User-defined map" pane.

4. Catalog panel

The Catalog panel is shown on right-hand side of the topology applet. This is only possible while the user map is in the "Draft" mode. When you display the user map, the catalog panel is automatically hidden. To view the catalog panel, click control (3) in the upper right-hand corner of the main window. To hide the catalog panel, click the control (4).



The catalog panel includes a folder list with categories for predefined device types. Each category consists of several predefined network devices that cannot be identified by SINEMA Server. Such device types can be added to the user map using the device types in the catalog panel. The catalog panel lists three types of unmanaged device categories in the Unmanaged device folder. The "Network component", "Others" and "PLC" folders are displayed in the catalog and consist of several predefined device types under each category. Go to the required folder and drag the predefined network devices to the topology area to add them to the user map.

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

5. Bird's eye view

The bird's eye view shows an image of the entire device view area. It displays the currently selected map. This view is located below the user-defined map pane. A blue rectangular box is usually shown to indicate the currently displayed area in the device view. Options are available in this view for positioning the rectangle at a specific location within the bird's eye view.

User defined map modes

Draft mode

When a user map is created on the **Network > User maps** page, the user map is automatically in draft mode or design status. In draft mode, you can place devices, define device positions in a map and draw connections between ports of various devices. To view all the existing reference connections, the "Show reference connections" check box is available in the toolbar. This check box is enabled by default. When this option is selected, the reference connections are shown as direct light blue lines. Connections between the ports can, however, be drawn using a user-defined connection.

Note

An empty map will be displayed in the Device view area of user maps if the reference connections have not been saved at least once in the Reference editor. When you save the changes to reference connections in the Reference editor, a user map containing all reference connections is displayed.

Note

In draft mode, the actual port status and device status are not shown in user maps. These are displayed gray.

The toolbar in the "User maps" page includes the following tools for accessing different modes. Several tasks can be performed in the user maps by selecting one of these modes.

- Select tool
- Draw connection tool
- User-defined connection tool

The Select tool is used to enable the Select mode. This tool is enabled automatically when open the user maps page. While Select mode is active, a user-defined connection includes a black circle that represents a bend point. End points of a reference connection are shown as a circle with a gray filling. In this mode, the following actions can be performed:

- Change layout or positions of devices, background images
- Change layout of connections and draw additional connections
- Add background image and change its size
- Drag and drop devices from the catalog to the device view
- Drag and drop devices from the User-defined map pane to the device view
- Delete device from the user map device view
- Change a reference connection to a user-defined connection
- Reset the layout of a connection

The Draw connection tool is available in the toolbar view. To change to Draw connection mode, select the Draw connection tool. In this mode, the following actions can be performed:

- Draw new connections between ports of various devices
- Change the layout of a connection
- Create a user-defined connection based on a reference connection
- Create user-defined connections for all reference connections

Note

The connection lines are derived from the corresponding port status. This means that even if port is "Up" and the user has drawn a special connection between these ports, the connection line will be displayed green in the active mode. These ports may, however, be connected to other devices as well. You should therefore remember that a green connection line (active mode) in user maps does not always mean that a connection exists in reality.

The following points apply to user-defined connections:

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

Note

The connection line with an end point containing a circle with a gray filling indicates that the user cannot change a reference connection to another port.

Active mode

In user maps, the active mode represents a monitoring view. The view of devices displayed in this mode is similar to the devices shown in the monitoring topology. The color codes used for the device state, ports and connections for objects that are part of the reference topology are similar to those in the monitoring topology. Active mode displays only the connections drawn by the user. Devices that are not in the view are shown as disabled.

It is not possible to make any changes to the user map while in active mode. For this reason, various mode buttons available in the toolbar view are not present in active mode. Only user-defined connections are displayed in this mode. The "Show reference connection" check box is therefore not available in this mode.

The following points apply to connections drawn by a user and shown in active mode:

- If a user-drawn connection is between two managed devices, the color of the line depends on the fill colors of both ports
- If a user-drawn connection is between a managed and an unmanaged device, the line color depends only on the color of the managed device port status
- If a user-drawn connection between two managed devices does not match any reference connection it has a small cloud icon in the middle to indicate a virtual connection
- User-drawn connections between unmanaged devices are always shown in gray. The port status of an unmanaged device will be unknown and these ports are therefore shown in gray
- The network cloud is a special type of unmanaged device that is added to the unmanaged device catalog

5.1.6.2 Working with user-defined maps

General overview

A user map includes the list of monitored devices along with user-defined connections displayed in the topology tree. With user maps, you can create or edit user-defined connections, add new devices and unmanaged devices, add a background image and change the connection layout.

Note

A user-drawn connection is only visible on the User maps page. A user-drawn connection does not represent a reference connection.

Configuring user maps

User maps can be configured to perform several actions. The list of actions is shown below:

1. Add devices from the user-defined map pane
2. Add unmanaged devices
3. Create or edit user-defined connections
4. Create a link to another user map
5. Add background image

Add devices from the user-defined map pane

Devices can be added to the user map device view from the user-defined map pane using any of the methods shown below:

- By right-clicking with the mouse
  - Select the device in the User-defined map pane, right-click and select "Add to current map". You will see that the device is added to the current user map.
- By double-clicking on the device
  - In the "User-defined map" pane, double-click on the device you want to add to the user map. The device will be moved to the user map.
- By drag and drop
  - Select the desired device in the "User-defined map" pane. Press the left mouse button and move the device to the required position in the user map. Release the left mouse button once you have positioned the device in the correct place.

Add unmanaged devices

In user maps, there are options for adding certain predefined device types to the map. These devices are grouped in the Unmanaged devices folder in the Catalog panel. The Catalog panel is shown on the right-hand side of the user map. Unmanaged devices can be added to the map by dragging the devices from the Catalog panel. Each unmanaged device displays a unique name once it is added to the map. This name helps to identify the device.

Create or edit user-defined connections

In user maps, you can create or change the user-defined connections between devices. The reference connections can also be changed to user-defined connections. The following list of actions can be performed in user maps using the Draw connection tool:

- Draw user-defined connections manually between ports belonging to various devices
- Change a reference connection to a user-defined connection by double-clicking
- Create user-defined connections for all reference connections

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

- Change a reference connection to a user-defined connection using the shortcut menu

Note

The "Delete device" option is displayed when you are using the "Select" tool and "Draw connection" tool. Select the device you want to delete. Right-click and select "Delete device" in the shortcut menu to delete the device. This option is also available in the toolbar view.

- Draw user-defined connection manually

  User-defined connections can be drawn manually by selecting the ports of devices that need to be connected. Follow the steps below to draw connections between devices manually:

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

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

  A user-defined connection can be seen between these two devices.

  In user maps, a user-defined connection line can be drawn between two devices manually by clicking on the ports of the devices to be connected. A dialog box is displayed where you select the port numbers of the devices to be connected. This allows connections to be drawn between two devices and these are displayed gray.

- Change a reference connection to a user-defined connection by double-clicking

  To change an existing reference connection to a user-defined connection, double click on the connection line representing a reference connection. The reference connection line changes to a user-defined connection that includes a black circle representing a bend point.

- Create user-defined connections for all reference connections

  The "Create user-defined connections for all reference connections" icon is available in the toolbar view. Click this icon to convert all reference connections to user-defined connections at once.

- Change a reference connection to a user-defined connection using the shortcut menu

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

Create a link to another user map

In user maps, a link can be created from one user map to another. The list of user maps created is shown in "Map hierarchy folder > User maps". To create a link to another user map, follow these steps:

1. In the "User-defined map" pane, browse through the user maps in the Map hierarchy folder.
2. Select the user map and drag the user map to an existing map.
3. The user map is displayed as a small rectangular box containing an icon representing as a globe. The status of this user map is displayed above this rectangular box.
4. Multiple associations can be drawn between this user map link and other devices.

To view the contents of the user map link, double click on the user map icon available in the existing user map. To go back to the main user map, use the back arrow button. The user map link only defines a logical relation to other objects. It does not display any device status information. It helps to determine the status of the devices within a linked user map by showing the linked user map status icon. If the devices within the user map link are in a fault state, then the user map link will be displayed with a fault state icon.

Create user map as a copy

At times it may be necessary to create a copy of a user map that is based on the reference topology. A copy of a user map can be created in the "Create user pap" page. Follow the steps below to create a user map as a copy.

1. On the User maps page, select the "Create map" icon to create a new user map.
2. In the "Create user map" page, enter the map name and select the required map type.
3. In Map mode, select the map name as reference topology and select "Save" option.
4. A copy of the user map is then available that is based on the reference topology.

The copy of user map is based on the reference topology and will not be created on the basis of the actual topology. Positions will only be taken from the reference topology. It is important to note that user-defined connections will not be created automatically.

Add background image

A background image can be added to user map while in Draft mode. This is done using the "Add background image" icon. This icon is available in the toolbar view. Click the "Add background image" icon to add a background image to the user map. The image will be placed in the background in the user map view area.

Configuring objects

1. Change image position
2. Change background image size
3. Change the layout of a connection

Change image position

To change the background image position, follow these steps:

1. Activate the Select tool on the toolbar and select the background image. A black border rectangle with white handles is visible around the image.
2. Move the cursor over the image, the cursor now changes to a four directional arrow.
3. Next, hold down the left mouse button and drag the image to another location.
4. Once the left mouse button is released, you will see that the background image position has changed.

Change background image size

The background image size can be altered in the user map. To change the background image size, follow these steps:

1. Activate the Select tool and select the background image in the user map view area.
2. A black border rectangle with white handles is visible.

3. Drag the desired white handle to another position by holding down the left mouse button.
4. Once the left mouse button is released, you will see that the background image is now resized.

Change the layout of a connection

The user-defined connection line drawn between two devices includes a black circle at the center of the connection line. With this black circle, you can bend a connection line. A maximum of seven bending points can be created in a single connection line. Creating bending points on a connection line can be helpful when working with a complex user map tree structure especially when the line spans several devices.

Follow the steps below to change the layout of the connection between devices:

1. Activate the Draw connection tool and select the user-defined connection line in the user map.
2. Select the black bending point at the center of the connection line.
3. Hold down the left mouse button and drag the bending point to another location.
4. When you release the left mouse button, new bending points are drawn in the center of the corresponding connection line.
5. Steps 3 and 4 above can be repeated until a maximum of seven bending points have been created.
6. Drag the bending points to different locations depending on the situation in the user map area.

5.1.7 Viewing all network devices

Display options

The **Network >All** menu item displays a list of devices detected in the network.

General information

The **Network > All** menu item displays information specific to the management station and the devices discovered within the network. This information is displayed in the form of a table. The management station device type provides a list of IP addresses of devices connected to the management device along with other device parameters. Each row of the table displays information about the detected device such as state, WBM, device type, device state, device name, PROFINET name, device category, MAC address, order number of the device.

The total number of devices discovered in the network is displayed above this table. Sort options are available for each field in the tabular view. Click the field name to sort the view based on its content. To view detailed information specific to each of the devices listed in the table view, select the IP address or state field to navigate to the Device details page.

The SINEMA Server application filters this information about network devices on the **Network > All** page to display a device list that includes new devices detected during the scan as well as the devices in either monitored or non-monitored state.

Note

To view the list of devices in the **Network > All** page, the device scan should have been run at least once. The device scan settings are made in the **Admin** > **Network settings** > **Device detection** tab and the **Scan settings** tab. Refer to "*Network settings*" in section 5.5.3 for more information about making the device scan settings.

Device parameters

The device parameters and their description can be found both on the **Network > All** and **Network > Devices** pages. The various device parameters and their descriptions are explained below:

Parameter	Description
State	The current state of the device.
WBM	Opens the Web based management site for the device.
IP V4 addr.	IP address of the device.
Device type	Type of device (for example SCALANCE X 200).
Device name	Unique name assigned to the device.
PROFINET name	PNIO name.
Vendor	The device vendor.
MAC	The MAC address
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.
Device category	The device category (for example Client Devices).
First seen	The time since the device was discovered for the first time. Represented as DD:MM:YYYY Hours:Minutes:Seconds:Milliseconds

Description of status icons

The "State" parameter provides information about the device status. Each row listing a device on this page contains information about the device status as an icon.

The status icons along and their meaning are shown below:

Icon	Description
✅	Good state
🟥	Fault state
🟨	Maintenance demanded
🟩	Maintenance required
?	Diagnostics not supported

Detailed information

To obtain details of the network device, go to the row of the device and click on the IP address field. The classified device details can be seen on different tabs on the device details page. The information displayed is specific to the selected network device. Please note that the device details information displayed is the same on both the **Network > All** and **Network > Devices** pages.

For a detailed overview of each of the tab options available on the Device details page, please refer to section 5.1.2 "*View device details*".

5.2 View network devices by category

5.2.1 View switches

Display options

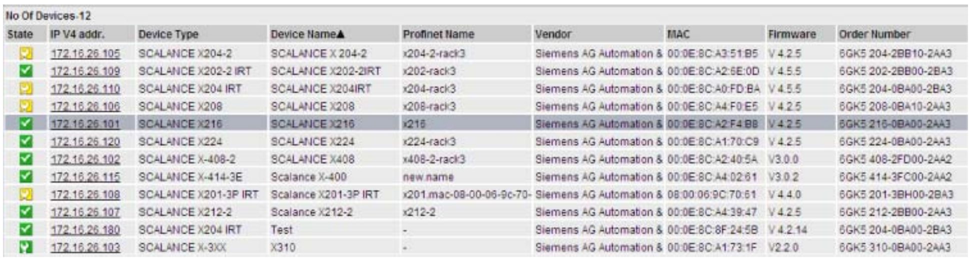
The **Devices > Switches** menu item displays a list of all switches detected in the network. The devices are filtered so that only devices of the type switch in the list of network devices are displayed.

General information

The **Devices > Switches** menu filters the list of devices so that only switches in the network are shown. This information is displayed in the form of a table. Each row of the table contains information about the device type, PROFINET name, IP address, device name, vendor name, MAC address and other details relating to the ports used.

The total number of devices of the type switch available in the current network is displayed above the table. The view can be sorted according to any of these fields in the table view. Click the field name in the view to sort the list of devices.

The State and IP V4 address column fields include a hyperlink to the Device details page. The other fields provided in this table view do not contain any hyperlinks.



No Of Devices-12

State	IP V4 addr.	Device Type	Device Name▲	Profinet Name	Vendor	MAC	Firmware	Order Number
🟨	172.16.26.105	SCALANCE X204-2	SCALANCE X 204-2	x204-2-rack3	Siemens AG Automation &	00:0E:8C:A3:51:B5	V 4.2.5	6GK5 204-2BB10-2AA3
✓	172.16.26.109	SCALANCE X202-2 IRT	SCALANCE X202-2IRT	x202-rack3	Siemens AG Automation &	00:0E:8C:A2:6E:0D	V 4.5.5	6GK5 202-2BB00-2BA3
🟨	172.16.26.110	SCALANCE X204 IRT	SCALANCE X204IRT	x204-rack3	Siemens AG Automation &	00:0E:8C:A0:FD:BA	V 4.5.5	6GK5 204-0BA00-2BA3
🟨	172.16.26.106	SCALANCE X208	SCALANCE X208	x208-rack3	Siemens AG Automation &	00:0E:8C:A4:F0:E5	V 4.2.5	6GK5 208-0BA10-2AA3
✓	172.16.26.101	SCALANCE X216	SCALANCE X216	x216	Siemens AG Automation &	00:0E:8C:A2:F4:B8	V 4.2.5	6GK5 216-0BA00-2AA3
✓	172.16.26.120	SCALANCE X224	SCALANCE X224	x224-rack3	Siemens AG Automation &	00:0E:8C:A1:70:C9	V 4.2.5	6GK5 224-0BA00-2AA3
✓	172.16.26.102	SCALANCE X-408-2	SCALANCE X408	x408-2-rack3	Siemens AG Automation &	00:0E:8C:A2:40:5A	V3.0.0	6GK5 408-2FD00-2AA2
✓	172.16.26.115	SCALANCE X-414-3E	Scalance X-400	new.name	Siemens AG Automation &	00:0E:8C:A4:02:61	V3.0.2	6GK5 414-3FC00-2AA2
🟨	172.16.26.108	SCALANCE X201-3P IRT	Scalance X201-3P IRT	x201.mac-08-00-06-9c-70-	Siemens AG Automation &	08:00:06:9C:70:61	V 4.4.0	6GK5 201-3BH00-2BA3
✓	172.16.26.107	SCALANCE X212-2	Scalance X212-2	x212-2	Siemens AG Automation &	00:0E:8C:A4:39:47	V 4.2.5	6GK5 212-2BB00-2AA3
✓	172.16.26.180	SCALANCE X204 IRT	Test	-	Siemens AG Automation &	00:0E:8C:8F:24:5B	V 4.2.14	6GK5 204-0BA00-2BA3
✓	172.16.26.103	SCALANCE X-3XX	X310	-	Siemens AG Automation &	00:0E:8C:A1:73:1F	V2.2.0	6GK5 310-0BA00-2AA3

The device parameters and their meaning are shown below:

Parameter	Description
State	Current state of the device represented as an icon.
IP V4 addr.	IP address of the device.
Device type	Type of device (example: SCALANCE X 200)
Device name	Name of the device.
PROFINET name	PNIO name.
Vendor	Vendor name.
MAC	The MAC address.
Firmware	The firmware version of the device.
Order number	Unique ID associated with the specific device.
Total ports	Total number of ports available.
Ports used	Number of ports used.
Last seen	The time stamp when the device was most recently available.
Uptime	Total time the device was up and running. Represented as Days Hours:Minutes:Seconds.Milliseconds

5.2.2 View access points

Display options

The **Devices > Access points** menu item displays a list of all access points detected in the network. The devices are filtered so that only the access points in the list of network devices are displayed.

General information

The **Devices > Access points** menu filters the list of devices so that only access points detected in the network are shown. This information is displayed in the form of a table. Each row of the table contains information about the device type, IP address, device name, PROFINET name, vendor name, MAC address, up time, SSID and other details relating to the wireless access points. You can view information specific to the access points such as the number of radios, number of clients, SSID details, etc.

The total number of access points available in the current network is displayed above this table. The device parameters and their meaning are shown below:

Parameter	Description
State	Current state of the device represented as an icon.
IP V4 addr.	IP address of the device.
Device type	Type of device (example: SCALANCE W 788-2RR)
Device name	Name of the device.
PROFINET name	PNIO name.
Vendor	Vendor name.
MAC	The MAC address of the device.
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.
No. of radios	Number of wireless radios available
No. of clients	Number of wireless clients available
Last seen	The time stamp when the device was most recently available.
Uptime	Total time when the device was up and running.
SSID1	Public name of wireless network 1 for communication.
SSID2	Public name of wireless network 2 for communication.
SSID3	Public name of wireless network 3 for communication.

5.2.3 View client devices

Display options

The **Devices > Clients** menu item displays a list of all client devices detected in the network. The devices are filtered so that only devices of the type client in the list of network devices are displayed.

General information

The **Devices > Clients** menu filters the list of devices so that only client devices in the network are shown. This information is displayed in the form of a table. Each row of the table contains information about the device state, IP address, device name, PROFINET name, device type, vendor name, MAC address and other details relating to the client devices discovered in the network.

The total number of client devices available in the current network is displayed above this table.

The device parameters and their meaning are shown below:

Parameter	Description
State	Current state of the device represented as an icon.
IP V4 addr.	IP address of the device.
Device type	Type of device (example: SCALANCE W4747 - 1)
Device name	Unique name assigned to the device.
PROFINET name	PNIO name.
Vendor	The device vendor.
MAC	The MAC address.
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.
Connected	Access point to which the device is connected.
Signal	Client device signal information.
Security	Type of security mechanism available for the device.
Last seen	The time stamp when the device was most recently available.
Up time	Total time when the device was up and running.

5.2.4 View end devices

Display options

The **Devices > End devices** menu item displays a list of all end devices detected in the network. The devices are filtered so that only end devices in the complete list of network devices are displayed.

General information

The **Devices > End devices** menu filters the list of devices so that only end devices in the network are shown. This information is displayed in the form of a table. Each row of the table contains information about the device type, STATE; IP address, device name, PROFINET name, vendor name, MAC address, security, connected AP and other details relating to the end devices discovered in the network.

The total number of end devices available in the current network is displayed above this table.

The device parameters and their meaning are shown below:

Parameter	Description
State	Current state of the device represented as an icon.
IP V4 addr.	IP address of the device.
Device type	Type of device (example: IM151 - 3xx)
Device name	Unique name assigned to the device.
PROFINET name	PNIO name.
Vendor	Vendor name.
MAC	MAC address of the device.
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.
Operating system	Operating system used.
Last seen	The time stamp when the device was most recently available.
Uptime	Total time when the device was up and running.

5.2.5 Gateway devices view

Display options

The **Devices > Gateways** menu item displays a list of all gateway devices discovered in the network. The devices are filtered so that only gateway devices in the list of network devices are displayed.

General information

The **Devices > Gateways** page displays the gateway devices existing in the network as a table view. Each row of the table contains information about the state, IP address, device name, device type, PROFINET name, vendor name, MAC address and other details relating to port usage.

The total number of devices of the type gateway available in the current network is displayed above this table.

The device parameters and their meaning are shown below:

Parameter	Description
State	The current state of the device.
IP V4 addr.	IP address of the device.
Device type	Type of device (for example SCALANCE X 200).
Device name	Unique name assigned to the device.
PROFINET name	PNIO name.
Vendor	Device vendor name.
MAC	The MAC address.
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.
No. of subnets	Total number of subnets in which the device is used.
Connected	Displays the name of a connected router, if any.
Total ports	Total number of ports available.
Ports used	Number of ports used.
Last seen	The time stamp when the device was most recently available.
Uptime	Total time the device was up and running.

5.2.6 View other devices

Display status

The **Devices > Other devices** menu item displays the list of devices that cannot be grouped into any specific device category. The devices that are not classified as belonging to any of the network device categories in the **Devices** menu can be viewed here.

General information

The **Devices > Other devices** menu filters the list of devices so that only non-categorized devices in the network are shown. These devices do not belong to any category of devices and are therefore classified as other devices.

The **Devices > Other devices** page displays information about the management station that is currently running the SINEMA Server application. The IP addresses of devices that belong to the management station device type are grouped together and displayed along with other device parameters in a table view. The other devices existing in the network are displayed below this Management station view. This information is displayed in the form of a table. Each row of the table contains information about the state, device type, IP address, device name, PROFINET name, vendor name, MAC address and other details relating to the "other" devices discovered in the network.

The total number of other devices available in the current network is displayed above this table.

The device parameters and their meaning are shown below:

Parameter	Description
State	The current state of the device.
IP V4 addr.	IP address of the device.
Device type	Type of device (for example SCALANCE X 200).
Device name	Unique name assigned to the device.
PROFINET name	PNIO name
Vendor	The device vendor.
MAC	The MAC address.
Firmware	The firmware version of the device.
Order number	The unique ID associated with the specific device.

5.3 Using and filtering events

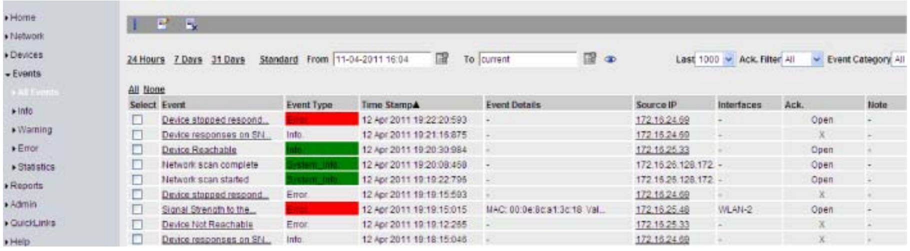
5.3.1 Managing all events

Display status

The **Events** > **All events** menu item displays the list of all types of events generated in the network.

General information

Any changes to the operational state or any fault detected in the network is considered as an event. The events are classified in two categories - network level events and system level events. The network level events relate to the changes detected within the existing network, whereas the system level events display event information specific to the performance of the SINEMA Server application as a whole. This page provides navigation options at the top of the page and a table view that lists all the events generated in the network.



From 11-04-2011 16:04 To current Last 1000 Ack. Filter All Event Category All

Select	Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
☐	Device stopped respond...	Error	12 Apr 2011 19:22:20:593	-	172.16.24.69	-	Open	-
☐	Device responses on SN...	Info	12 Apr 2011 19:21:16:875	-	172.16.24.69	-	X	-
☐	Device Reachable	Info	12 Apr 2011 19:20:30:984	-	172.16.25.33	-	Open	-
☐	Network scan complete	System_Info	12 Apr 2011 19:20:08:458	-	172.16.26.128.172	-	Open	-
☐	Network scan started	System_Info	12 Apr 2011 19:19:22:796	-	172.16.25.128.172	-	Open	-
☐	Device stopped respond...	Error	12 Apr 2011 19:19:15:593	-	172.16.24.69	-	X	-
☐	Signal Strength to the...	Error	12 Apr 2011 19:19:15:015	MAC: 00:0e:8c:a1:3c:18 Val...	172.16.25.48	WLAN-2	Open	-
☐	Device Not Reachable	Error	12 Apr 2011 19:19:12:265	-	172.16.25.33	-	X	-
☐	Device responses on SN...	Info	12 Apr 2011 19:18:15:046	-	172.16.24.69	-	X	-

Event parameters

You can view the various event parameters for each event. The various event parameters and their descriptions are explained below:

Parameter	Description
Select	Displays a check box to select an event to acknowledge, add notes or delete notes.
Event	Displays event information.
Event type	Type of event.
Time stamp	Time of the last occurrence of the event.
Event details	Displays complete details of the event.
Source IP	IP address of the source device.
Interfaces	Displays the interface type number used.

Parameter	Description
Ack.	Displays 'X' if the event has been acknowledged and 'Open' if the event has not been acknowledged yet.
Note	Displays the notes.

Viewing all events

The **All events** page provides a complete list of all events generated in the network in a table view. This page consists of various navigation options provided at the top of the page. For each event displayed as a separate row, the parameters such as event, event type, time stamp, event details, source IP and notes can be viewed in this table view. Below, you will find information about the significance of each of these fields:

- The "Select" field is used to select the event prior to performing an action for the specific event.
- The "Event" field provides the event information or event message.
- The "Event type" field provides information about the type of event. Open events are highlighted in a unique color format. This helps to identify the unacknowledged events when the complete list is displayed. The system info type is shown in green, warnings in yellow and errors in red.
- The "Time stamp" field provides information about the date and time when the event was generated.
- The "Event details" field displays the complete information about each event.
- The "Source IP" field provides the IP address of the source device.
- The "Interfaces" field displays information about the interface type and interface number used. This field uses unique numbering sequences for LAN and WLAN devices separately.
- The "*Ack.*" column of all the acknowledged events displays the status as "X" and all the unacknowledged events are indicated by "Open".
- Additional information about the notes can be managed and viewed in the "Notes" column.

Note

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

Note

The recently updated list of the last 1000 events is displayed on the All events page. Scroll down further to view the complete list of events.

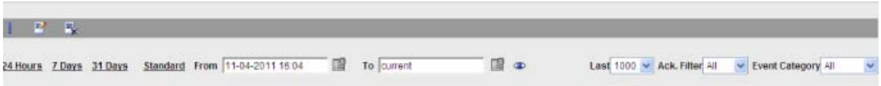
Navigation options

To view, filter or manage the list of events, SINEMA Server provides several filtering options and user controls as icons in the Events menu. These options help you to manage and view the required list of events effectively. The icons and their meaning are described below:

Icon	Description
!	Acknowledging events
✎	Edit notes
✗	Delete notes
👁	Show icon

Note

The navigation options provided on the **Events** > **All events** page are the same on all Events pages.



From 11-04-2011 16:04 To current

Last 1000 Ack. Filter All Event Category All

You will find a description and information about each of these filters in the following sections:

- Acknowledging events
- Adding notes
- Deleting notes
- Filtering events for a period
- Viewing all recent events
- Using the acknowledge filter
- Using the event category filter

Acknowledging events

All events generated by the SINEMA Server application can be acknowledged. Acknowledging the events that have event reactions configured for the event helps to deal with or rectify critical events.

To acknowledge an event, follow these steps:

1. From the list of events, select the check box for the event you want to acknowledge.
2. Click the Acknowledge icon at the top of the page.
3. You can check that the acknowledgment was made. The Status box displays 'X' in the column for the specific event indicating that the event has been acknowledged.

If you try to acknowledge an already acknowledged event, the alert "Selected event already acknowledged" is displayed. If you have selected a combination of acknowledged and unacknowledged events, if you try to acknowledge, you will see that only the unacknowledged events are acknowledged.

Note

To acknowledge all the events displayed in the table in a single action, select the "All" link above the table and then select the "All" option in the "Acknowledge filter" list box. The unacknowledged event(s) will be acknowledged.

Adding notes

You can add notes to an event relating to the current status of the event. This will allow you to manage the events better. If multiple events are selected for adding notes, an empty edit box will be opened. The text entered in this box will be updated for the selected events.

To add notes to an event, follow these steps:

1. From the list of events, select the check box for the event to which you want to add a note.
2. Click the Add notes icon.

   A pop-up window appears.
3. Type the note in the text box and click the OK button.

   The note is added to the event.

Notes written for the specific event will be shown in the table view. When adding notes, it is important to remember that the existing notes will be overwritten if you add notes to an event that already contains notes.

Deleting notes

You can delete the notes that have been added to an event.

To delete the notes, follow these steps:

1. On the All events page, select the check box for the events for which the note will be deleted.

   Note

   If you want to delete the notes of all events, select the "All" check box at the top of the Select column in the event table.

2. Click the "Delete notes" icon to delete the note for the selected events.

Filtering events for a period

The links 24 hours, 7 days, and 31 days located on the second-level header are used to filter the events that occurred in the last 24 hours, the last 7 days and the last 31 days.

- Click the 24 hours link to view the list of events that occurred in the last 24 hours.
- Click the 7 days link to view the list of events that occurred in the last 7 days.
- Click the 31 days link to view the list of events that occurred in the last 31 days.

You also can filter the events that occurred during a specific period by following the steps outlined below:

1. Select the start date of a specific period from the calendar in the "From" box.

   For example, if you want to view the events that took place between 25-03-2010 and 10-05-2010, select 25-03-2010 in the From box.

2. Select the end date for the period from the calendar in the "To" box, and click "Show".

   All the events that occurred during the specified period are displayed in a table.

   Note

   When you filter events for a specific period, the event list shows all the acknowledged and unacknowledged events. Unacknowledged events are displayed as "Open" and acknowledged events as "X".

   Note

   If filter settings are modified for the display of the list of recent events, acknowledge filter and event category filter, you will see that the color of these list boxes changes to light orange indicating changes to these settings. To switch back to the default settings, click the "Standard" link.

Viewing all recent events

Events can be filtered to view only the last 50, 100, 200 or 1000 events. This helps you to keep track of the last 50 events triggered in the network instead of having to view the complete list of events. This can be achieved by selecting the drop-down list next to the "Show" icon on this page.

For example, select the 50 option from the drop-down list to view only the latest 50 events. This saves time and is more productive since you do not need to search through the entire list of events if you are only interested in recent events that have occurred in the network.

Using the acknowledge filter

You can filter the events based on their acknowledged status. Events can be listed on this page based on their acknowledged or unacknowledged status. The "Acknowledge filter" list box provides three options: 'All', 'Open', 'X'. By default, the 'All' option is selected in the Ack. filter list box.

To filter the events based on their acknowledged status, follow these steps:

1. In the "Acknowledge filter" list box, select the required option from the list box.
2. The list of events displayed in the table changes depending on the selected option.
3. Select 'Open' to view only the list of unacknowledged events.
4. Select 'X' to view a complete list of acknowledged events.

Using the event category filter

The "Event category filter" option is located next to the "Ack.". filter list box. This filter provides options for filtering the events based on the event category type or you can also view all the events. There are two event categories supported - network events and system events. Network events list all the events relating to the devices supported in the network. System events list the events specific to changes within the SINEMA Server application as a whole. Select the desired category type to view the list of events belonging to the category you require.

Configure events

In SINEMA Server, events can be acknowledged by the user. This helps you to rectify critical events before they become more serious. Event reactions help you to handle such situations effectively. For more information about configuring event reactions, refer to "*Network settings*" in section 5.5.3.

5.3.2 View information events

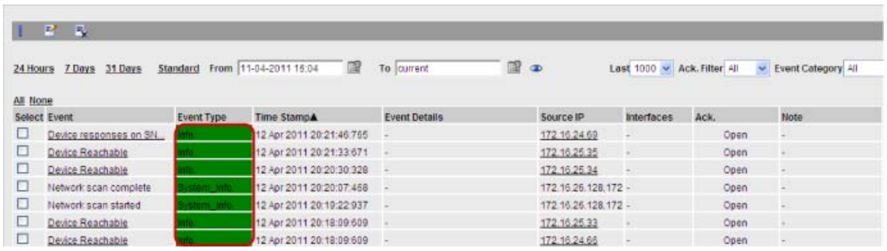
Display status

The **Events > Info** menu item displays a list of events that contain only event messages or information specific to the events. The events causing warnings or errors will not be listed on this page.

General information

The SINEMA Server application filters the list of events displayed based on the type of event generated within the network. The **Events > Info** page displays only the events that contain some kind of information specific to the event and does not identify a warning/error or a system trap. You can view information about the event, event type, event details, time stamp, source IP, acknowledgment status and notes on this page.

The "Event" field provides the name of the event. The information events are distinguished by a specific color code. This helps to identify the events when the complete list is displayed. The information events are displayed in green. The "Source IP" field provides the IP address of the source device.



From 11-04-2011 15:04 To current Last 1000 Ack. Filter All Event Category All

Select	Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
☐	Device responses on SN...	Info	12 Apr 2011 20:21:46:765	-	172.16.24.69	-	Open	-
☐	Device Reachable	Info	12 Apr 2011 20:21:33:671	-	172.16.25.35	-	Open	-
☐	Device Reachable	Info	12 Apr 2011 20:20:30:328	-	172.16.25.34	-	Open	-
☐	Network scan complete	System_Info	12 Apr 2011 20:20:07:468	-	172.16.26.128,172	-	Open	-
☐	Network scan started	System_Info	12 Apr 2011 20:19:22:937	-	172.16.26.128,172	-	Open	-
☐	Device Reachable	Info	12 Apr 2011 20:18:09:609	-	172.16.25.33	-	Open	-
☐	Device Reachable	Info	12 Apr 2011 20:18:09:609	-	172.16.24.66	-	Open	-

Note

The options for acknowledging events, filtering the date, adding or deleting notes and viewing the event list based on the category are the same on all Events pages. These user controls and filters are available on all pages in the **Events** menu.

Understanding information events

As explained above, an event occurs whenever there are changes in a device state or when a fault is detected in the network. The events displayed on this page are generally messages/updates specific to the network and the network devices. System level events, on the other hand, are generated whenever there are changes in the performance of the application.

With information events, no action is required of the end user. The event signifies either a message displayed based on a user action performed in the application or an update resulting from network device state changes. For example, user account logins/logouts, device discovery completion, software driver verification, start/end of network scan or permissions granted by the administrator are usually reported as events on the information events page.

5.3.3 View warning events

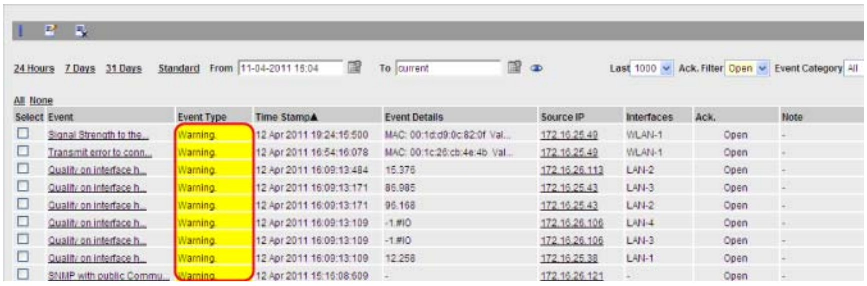
Display status

The **Events > Warning** menu item displays the list of events that contain warning messages for the user. The events resulting from errors or faults detected in the network devices are not listed on this page.

General information

On the **Events > Warning** page, the SINEMA Server application filters the list of events displayed based on the type of event generated in the network. The **Events > Warning** page displays only the events that contain warnings and does not identify errors or system traps. You can view information about the event, event type, event details, time stamp, source IP, acknowledgment status and notes on this page.

The "Event" field provides the name of the event. The warning events are distinguished by a specific color code. This helps to identify the events when the complete list is displayed. The warning events are displayed in yellow. The "Source IP" field provides the IP address of the source device.



24 Hours 7 Days 31 Days Standard From 11-04-2011 15:04 To current Last 1000 Ack. Filter Open Event Category All

All None

Select	Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
□	Signal Strength to the...	Warning	12 Apr 2011 19:24:15:500	MAC: 00:1d:d9:0c:82:0f Val...	172.16.25.49	WLAN-1	Open	-
□	Transmit error to conn...	Warning	12 Apr 2011 16:54:16:078	MAC: 00:1c:26:cb:4e:4b Val...	172.16.25.49	WLAN-1	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:484	15.376	172.16.26.113	LAN-2	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:171	86.985	172.16.25.43	LAN-3	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:171	96.168	172.16.25.43	LAN-2	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:109	-1.#IO	172.16.26.106	LAN-4	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:109	-1.#IO	172.16.26.106	LAN-3	Open	-
□	Quality on interface h...	Warning	12 Apr 2011 16:09:13:109	12.258	172.16.25.38	LAN-1	Open	-
□	SNMP with public Commu...	Warning	12 Apr 2011 15:15:08:609	-	172.16.26.121	-	Open	-

Note

The options for acknowledging events, filtering the date, adding or deleting notes and viewing the event list based on the category are the same on all Events pages. These user controls and filters are available on all pages in the Events menu.

Understanding warning events

The events displayed on this page are generally warnings specific to the network and the network devices. A warning alerts the user of a condition that might cause a problem in the future. Based on such warning messages, some level of action is required to ensure the smooth functioning of the devices within the network. These actions will prevent further errors or traps in the network devices or in the SINEMA Server application.

For example, traps received, maintenance requests, device started responding on DCP, link down received, link up received and activation/deactivation of connections are usually reported on the warning events page.

5.3.4 View error events

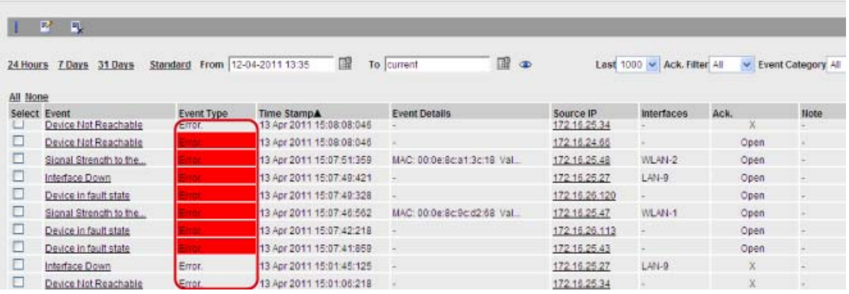
Display status

The **Events > Error** menu item displays the events that contain error messages. The events involving warnings or information are not listed on this page.

General information

The SINEMA Server application filters the list of events displayed based on the type of event generated within the network. The **Events > Error** page displays only events that contain error messages. This event type is important to the user and requires quick action to be taken because it indicates an error on devices, in the network or in the system. You can view information about the event, event type, event details, time stamp, source IP, acknowledgment status and notes on this page.

The "Event name" field provides the name of the event. The error events are distinguished by a specific color code. This helps to identify the events when the complete list is displayed. The error events are displayed in red. The "Source IP" field provides the IP address of the source device.



24 Hours 7 Days 31 Days Standard From 12-04-2011 13:35 To current Last 1000 Ack. Filter All Event Category All

All None

Select	Event	Event Type	Time Stamp▲	Event Details	Source IP	Interfaces	Ack.	Note
□	Device Not Reachable	Error.	13 Apr 2011 15:08:08:046	-	172.16.25.34	-	X	-
□	Device Not Reachable	Error	13 Apr 2011 15:08:08:046	-	172.16.24.66	-	Open	-
□	Signal Strength to the...	Error	13 Apr 2011 15:07:51:359	MAC: 00:0e:8c:a1:3c:18 Val...	172.16.25.48	WLAN-2	Open	-
□	Interface Down	Error	13 Apr 2011 15:07:49:421	-	172.16.25.27	LAN-9	Open	-
□	Device in fault state	Error	13 Apr 2011 15:07:49:328	-	172.16.26.120	-	Open	-
□	Signal Strength to the...	Error	13 Apr 2011 15:07:46:562	MAC: 00:0e:8c:9c:d2:68 Val...	172.16.25.47	WLAN-1	Open	-
□	Device in fault state	Error	13 Apr 2011 15:07:42:218	-	172.16.26.113	-	Open	-
□	Device in fault state	Error	13 Apr 2011 15:07:41:859	-	172.16.25.43	-	Open	-
□	Interface Down	Error.	13 Apr 2011 15:01:45:125	-	172.16.25.27	LAN-9	X	-
□	Device Not Reachable	Error.	13 Apr 2011 15:01:06:218	-	172.16.25.34	-	X	-

---

Note

The options for acknowledgments, filtering the date, adding or deleting notes and viewing events based on the event category are the same on all pages in the **Events** menu.

Understanding error events

How events are handled is very important if faults are detected or any of the devices in the network are malfunctioning. The error events include error messages that can occur either in the network or in the system. Fast action is required from the user when such events occur. The user then needs to take appropriate action depending on the error information. If event reactions are configured in advance for these events, this makes it easier because an event reaction can be configured so that an e-mail is sent to a specified address and this invokes the application specified on the event reactions configuration page. For more information about configuring event reactions, refer to "*Network settings*" in section 5.5.3.

Examples of some of the key system errors generated by the error events include DCP subtask not running, Scan Manager not running, memory allocation failed, invalid callback address .

5.3.5 Viewing event statistics

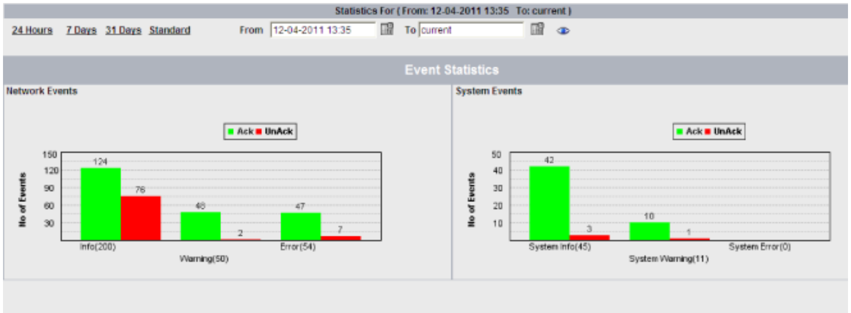
Display status

The **Events** > **Statistics** menu item provides a graphic view of the number of network level events and system level events generated in the application.

General information

A brief overview of events, the event type and its status helps to understand the complete list of events generated in the application. To simplify this, the SINEMA Server application prepares statistics of all acknowledged and unacknowledged events. The event statistics page displays graphs for the following event categories:

- Network events
- System events



Statistics For (From: 12-04-2011 13:35 To: current)

From: 12-04-2011 13:35

To: current

The Network events graph shows the number of acknowledged events for each event type indicated in green while red is used for unacknowledged events. The event types information, warning and error are shown on the X-axis and the Y-axis indicates total number of events for each of these event types. The bar graph shows bars for both unacknowledged and acknowledged events for a specific event type.

The System events graph provides information about the number of events generated for SystemInfo, SystemWarning and SystemError events. This is indicated by the X-axis. The Y-axis shows the number of events for each of system event of a specific type. Just as in the network events graph, the green bar indicates acknowledged events whereas red is used for unacknowledged events.

Filtering events

The graphs can be filtered to display events that occurred in a particular date/time range or in a specific week/month. The hours/day filters are used to filter the events for a specified number of days or hours. Date filters are available to restrict the display of events in the graph to a specific date range. Select the date by clicking the calendar icon to display the information in the "From" and "To" text boxes. Then, click the "Show" button to view events within the graph for the specified range.

5.4 Report generation

Overview

The SINEMA Server application includes a "Reports" menu with which you can display specific reports relating to the network devices. You can view reports based on the network devices inventory, availability of devices in the network and the performance of the devices in the network. These reports can be used to generate network related statistical information in an interpretable format. It is also possible to create a preview of these reports and print them.

The generated report pages include information classified within several fields available as a table view. This information is also depicted by pie charts or bar charts. Based on the filtered criteria, the corresponding fields containing report information are displayed in the Inventory, Availability and Performance reports.

5.4.1 Network devices inventory

Display status

The **Reports > Inventory** menu item generates and displays reports based on the vendor, IP range and device category of all devices detected in the network.

General information

The inventory report provides device related information. After selecting the **Reports > Inventory** menu item, you can view the full report relating to devices in the current network based on the device vendor, IP range and device category for a specified date/time period. This information can be viewed as a table and as charts.

The **Reports > Inventory** page contains three tabs:

- Vendor
- IP range
- Device category

These tabs can be seen at the top of the Inventory page. Click on any tab to view the corresponding report. By default, the Vendor tab is selected when you click the **Reports > Inventory** menu.

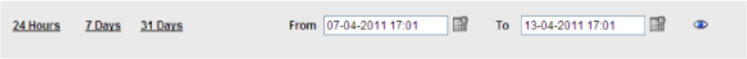
Note

When you view the Reports page for the first time, you may see that the reports do not display any information. The report data is displayed only after filtering the report information for a certain time.

Filtering report information for a period

To allow you to view, filter or manage the reports displayed, SINEMA Server provides several filtering options in the Reports menu. These controls will help you to manage and view the required list of events effectively. The Show icon is used to filter and display the reports for the specified date / time range. You will find a description of the icon and its meaning below:

Icon	Description
👁	Show icon



From 07-04-2011 17:01 To 13-04-2011 17:01

Note

The filter options in the **Reports** menu are the same on all Report pages.

Note

When filtering the report based on a specified period, the time in the From and To fields should be at least 10 minutes.

Note

The filter settings made on these pages are retained until you log out of the application. If the filter settings have been changed, the settings will be remain valid even after navigating back and forth between other Web pages.

The links 24 hours, 7 days, and 31 days located at the top of the page are used to filter the reports created in the last 24 hours, the last 7 days and the last 31 days.

- Click the 24 hours link to view the reports created in the last 24 hours.
- Click the 7 days link to view the reports created in the last 7 days.
- Click the 31 days link to view the reports created in the last 31 days.

You also can filter the reports created during a specific period by following the steps outlined below:

1. Select the start date of a specific period from the calendar in the "From" box.

   For example, if you want to view the reports between 25-03-2010 and 10-05-2010, select 25-03-2010 in the From box.
2. Select the end date for the period from the calendar in the "To" box, and click "Show".

All the reports created for the specified period are displayed in a table.

Device state

The current state of a device is represented as an icon on each of the report pages in the table view. You will find the icon representation and the description of each device state in the table below:

Icon	Description
✓	Good state
🔧	Fault state
🔧	Maintenance demanded
🔧	Maintenance required
?	Unknown state

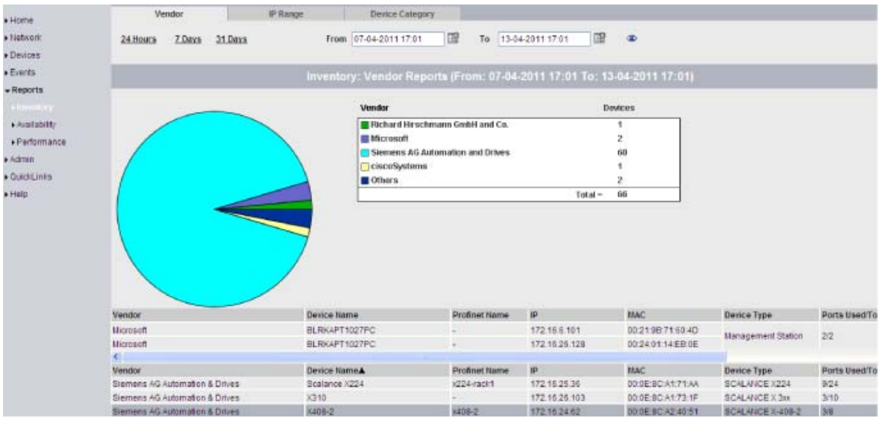
Note

The device state icon representation in the table view is the same on all report pages.

Vendor tab

The Vendor tab displays reports based on vendor information relating to all devices discovered in the network. The management station information is shown as a table. The management station device type provides a list of IP addresses of devices connected to the management station along with other device parameters. This report contains information about the vendor, device name, PROFINET name, IP, MAC address, device type,ports uses/total, location and the current state of the device. This information is displayed as a table and as a pie chart.

The pie chart slices shown below give you a quick overview of the proportion of devices from different vendors in the network. A common set of 3 standard vendors have been identified and are depicted in this chart. All other devices, however, that do not belong to these standard vendors are grouped in "Others". The chart legend displays color-coded vendor names and the number of network devices belonging to each vendor. The total number of devices in the network is also displayed in this chart legend.



From 07-04-2011 17:01 To 13-04-2011 17:01

Inventory: Vendor Reports (From: 07-04-2011 17:01 To: 13-04-2011 17:01)

Vendor	Devices
🟩 Richard Hirschmann GmbH and Co.	1
🟪 Microsoft	2
🟦 Siemens AG Automation and Drives	60
🟨 ciscoSystems	1
🟦 Others	2
Total =	66

Vendor	Device Name	Profinet Name	IP	MAC	Device Type	Ports Used/To
Microsoft	BLRKAPT1027PC	-	172.16.6.101	00:21:9B:71:60:4D	Management Station	2/2
Microsoft	BLRKAPT1027PC	-	172.16.26.128	00:24:01:14:EB:0E		

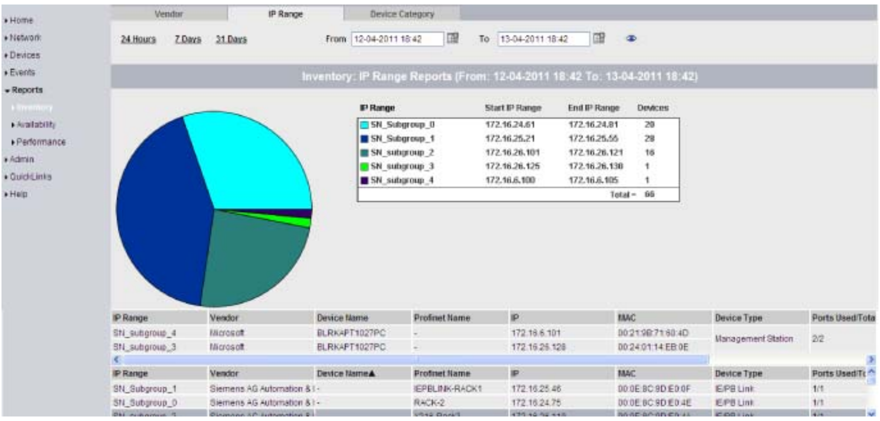
Vendor	Device Name▲	Profinet Name	IP	MAC	Device Type	Ports Used/To
Siemens AG Automation & Drives	Scalance X224	x224-rack1	172.16.25.36	00:0E:8C:A1:71:AA	SCALANCE X224	9/24
Siemens AG Automation & Drives	X310	-	172.16.26.103	00:0E:8C:A1:73:1F	SCALANCE X 3xx	3/10
Siemens AG Automation & Drives	X408-2	x408-2	172.16.24.62	00:0E:8C:A2:40:51	SCALANCE X-408-2	3/8

The report in table form is displayed at the bottom of the page. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Vendor	Name of the device vendor.
Device name	Name of the device connected.
PROFINET name	PNIO name.
IP	IP address of the device.
MAC	MAC address of the device.
Device type	Type of network device.
Ports used/total	Number of ports in use / total number of ports.
Location	System location (SNMP parameter)
Current state	Current state of the device represented as an icon.

IP range tab

The IP range tab displays reports based on the selected IP ranges set when scanning devices. This report contains information about the selected IP range, vendor name, device name, PROFINET name, IP address, MAC address, current state, device type ports used/total and state information. The information on this tab is displayed as a table and as a pie chart. The pie chart provides a quick overview of the different IP ranges used indicated by a color code representing each slice. The chart legend shows the different IP ranges indicated by a separate color, the IP start range, end range and the the number of network devices in each IP range including the total number of displayed devices..



From 12-04-2011 18:42 To 13-04-2011 18:42

Inventory: IP Range Reports (From: 12-04-2011 18:42 To: 13-04-2011 18:42)

IP Range	Start IP Range	End IP Range	Devices
SN_Subgroup_0	172.16.24.61	172.16.24.81	20
SN_Subgroup_1	172.16.25.21	172.16.25.55	28
SN_subgroup_2	172.16.26.101	172.16.26.121	16
SN_subgroup_3	172.16.26.125	172.16.26.130	1
SN_subgroup_4	172.16.6.100	172.16.6.105	1
		Total =	66

IP Range	Vendor	Device Name	Profinet Name	IP	MAC	Device Type	Ports Used/Tota
SN_subgroup_4	Microsoft	BLRKAPT1027PC	-	172.16.6.101	00:21:9B:71:60:4D	Management Station	2/2
SN_subgroup_3	Microsoft	BLRKAPT1027PC	-	172.16.26.128	00:24:01:14:EB:0E		

IP Range	Vendor	Device Name▲	Profinet Name	IP	MAC	Device Type	Ports Used/T
SN_Subgroup_1	Siemens AG Automation & I	-	IEPBLINK-RACK1	172.16.25.46	00:0E:8C:9D:E0:0F	IE/PB Link	1/1
SN_Subgroup_0	Siemens AG Automation & I	-	RACK-2	172.16.24.75	00:0E:8C:9D:E0:4E	IE/PB Link	1/1

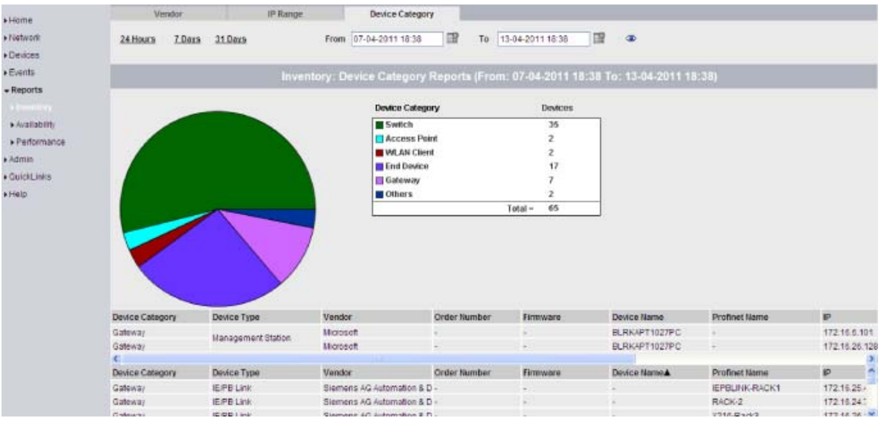
The report in table form is displayed at the bottom of the page. This report contains various device parameters. The various device parameters on the IP range tab and their meaning are shown below:

Parameter	Description
IP range	IP range name.
Vendor	Name of the device vendor.
Device name	Name of the device connected.
PROFINET name	PNIO name.
IP	IP address of the network device.
MAC	MAC address of the device.
Device type	Type of network device.
Ports used/total	Number of ports in use / total number of ports.
Location	System name.
Current state	Current state of the device represented as an icon.

Device category tab

The Device category tab provides reports based on the associated device categories discovered in the network. General device types that are identified in the network are access point, switch, WLAN client, end device, gateway and others.

The management station information is shown as a table. The management station device type provides a list of IP addresses of devices connected to the management station along with other device parameters. This report contains the device category, device type, vendor name, order number, firmware, PROFINET name, IP address, MAC address and the state of these devices. This information is shown as a table and as a pie chart. The pie chart provides an overview of the number of devices belonging to a specific device category identified by a unique color code and each device category is represented as a slice. The chart legend as shown in the screenshot below indicates the device category type with a color code and the number of devices in the specified device category.



From 07-04-2011 18:38 To 13-04-2011 18:38

Inventory: Device Category Reports (From: 07-04-2011 18:38 To: 13-04-2011 18:38)

Device Category	Devices
🟩 Switch	35
🟦 Access Point	2
🟥 WLAN Client	2
🟪 End Device	17
🟪 Gateway	7
🟦 Others	2
Total =	65

Device Category	Device Type	Vendor	Order Number	Firmware	Device Name	Profinet Name	IP
Gateway	Management Station	Microsoft	-	-	BLRKAPT1027PC	-	172.16.6.101
Gateway		Microsoft	-	-	BLRKAPT1027PC	-	172.16.26.128

Device Category	Device Type	Vendor	Order Number	Firmware	Device Name▲	Profinet Name	IP
Gateway	IE/PB Link	Siemens AG Automation & D	-	-	-	IEPBLINK-RACK1	172.16.25.
Gateway	IE/PB Link	Siemens AG Automation & D	-	-	-	RACK-2	172.16.24.

The report in table form is displayed at the bottom of the page. This report contains various device parameters. The various device parameters on the device type tab and their meaning are shown below:

Parameter	Description
Device category	Device family name.
Device type	Category type to which the device belongs.
Vendor	Name of the vendor.
Order number	Order number.
Firmware	Firmware version of the device.
Device name	Name of the device.
PROFINET name	PNIO name.
IP	IP address of the device.
MAC	MAC address of the device.
Ports used/total	No. of ports in use / maximum number of ports.
Current state	Current state of the device represented as an icon.

5.4.2 Network device availability

Display status

The **Reports > Availability** menu item generates and displays reports that provide information relating to the availability of devices in the network.

General information

The Availability report displays the statistics of the total uptime of devices, the total downtime of devices, devices that are operational for the longest time on a specific day, devices that are not operational for the longest time and the percentage availability of devices for all the devices detected in the network during the scan. This information is displayed as a table with bar graph representation.

Note

When you view the Reports page for the first time, you may see that the reports do not display any information. The report data is displayed only after filtering the report information for a certain time.

The **Reports > Availability** page consists of two tabs.

- Devices
- Interfaces

These tabs can be seen at the top of the Availability reports page. Click on any tab to view the corresponding report. By default, the devices tab is selected with the report displaying information about all available devices in the network filtered for the current day.

Note

The filter options in the Reports menu are the same on all Report pages.

Note

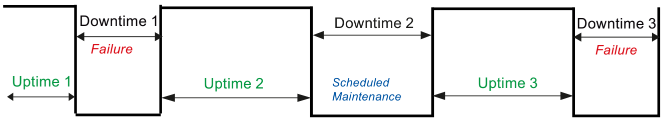
When filtering the report based on a specified period, the time in the From and To fields should be at least 10 minutes.

Note

The availability reports do not explicitly take into account the time when the SINEMA Server application is not running. The time during which the application was shut down is excluded from any calculations.

Availability report calculations

The Availability report provides report data specifically relating to the availability of devices in the network. To calculate this device availability information, the total up time or down time of a device needs to be known. The availability report calculation is based on the mean up time (MUT) and mean down time (MDT) of devices and interfaces.



Mean up time (MUT) = total up time / total outages

Total up time = uptime 1 + uptime 2 + uptime 3 + ...

Mean down time (MDT) = total down time / total outages

Total down time = downtime 1 + downtime 2 + downtime 3 + ...

Downtime can be due to failure or a scheduled downtime.

%Availability = MUT * 100 / (MUT + MDT)

Data representation

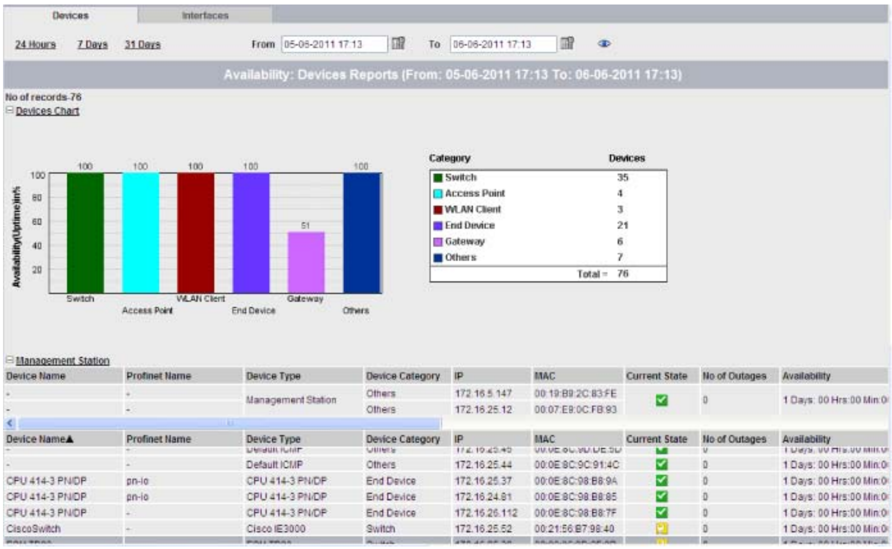
The Availability reports contain standard data representation for some of the report fields shown in the table view. The report field column name along with the representation format is shown the table below:

Report parameter	Data format
Availability Total downtime Mean up time Mean down time	days: hours: minutes: seconds Example: 2 days: 01 hours: 30 minutes: 00 seconds Example: 0 days: 00 hours:00 minutes: 00 seconds Example: 0 days: 00 hours:00 minutes: 00 seconds
First seen Last seen	dd-month-yyyy hours:minutes:seconds:milliseconds Example: 13 Jan 2011 16:50:30:218
Availability (%)	Example: 98.131

Devices tab

The Devices tab provides reports based on the devices available in the network. To determine device availability, the overall reachability factor is taken into account. If devices are reachable, then they are considered available.

The management station information is shown as a table. The management station device type provides a list of IP addresses of devices connected to the management station along with other device parameters. In this page, you can view device availability reports that contain information about the device, device name, device type, device model, IP, MAC address, device state, number outages, total downtime and availability of the devices as a percentage. The bar chart displays each device category on the X-axis. The total number of devices representing each category is shown above each of these bars in this graph. The Y-axis indicates the availability (uptime) of devices as a percentage. The chart legend shows the different device categories indicated by a separate color and the number of network devices in each category.



From 05-06-2011 17:13 To 06-06-2011 17:13

Availability: Devices Reports (From: 05-06-2011 17:13 To: 06-06-2011 17:13)

No of records-76

Category	Devices
🟩 Switch	35
🟦 Access Point	4
🟥 WLAN Client	3
🟪 End Device	21
🟪 Gateway	6
🟦 Others	7
Total =	76

Device Name	Profinet Name	Device Type	Device Category	IP	MAC	Current State	No of Outages	Availability
-	-	Management Station	Others	172.16.5.147	00:19:B9:2C:83:FE	✓	0	1 Days: 00 Hrs:00 Min:0
-	-		Others	172.16.25.12	00:07:E9:0C:FB:93			

Device Name▲	Profinet Name	Device Type	Device Category	IP	MAC	Current State	No of Outages	Availability
-	-	Default ICMP	Others	172.16.25.45	00:0E:8C:9D:DE:5D	✓	0	1 Days: 00 Hrs:00 Min:0
-	-	Default ICMP	Others	172.16.25.44	00:0E:8C:9C:91:4C	✓	0	1 Days: 00 Hrs:00 Min:0
CPU 414-3 PN/DP	pn-io	CPU 414-3 PN/DP	End Device	172.16.25.37	00:0E:8C:98:B8:9A	✓	0	1 Days: 00 Hrs:00 Min:0
CPU 414-3 PN/DP	pn-io	CPU 414-3 PN/DP	End Device	172.16.24.81	00:0E:8C:98:B8:85	✓	0	1 Days: 00 Hrs:00 Min:0
CPU 414-3 PN/DP	-	CPU 414-3 PN/DP	End Device	172.16.26.112	00:0E:8C:98:B8:7F	✓	0	1 Days: 00 Hrs:00 Min:0
CiscoSwitch	-	Cisco IE3000	Switch	172.16.25.52	00:21:56:B7:98:40	⚠	0	1 Days: 00 Hrs:00 Min:0

The report in table form is displayed at the bottom of the page. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	Category of the device.
IP	IP address of the device.
MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
No. of outages	Number of times when the device was not reachable.
Availability	Sum of all the times when the device was reachable.
Total downtime	Sum of all the times when the device was not reachable.
Availability (%)	Shows device availability - days: hours: mins.
Last seen	The time and date when the device was last seen.
First seen	The time and date when the device was first seen.
Mean down time	Time during which the device was not reachable. Total downtime / number of outages
Mean up time	The time during which the device was reachable. Total up time / number of outages.

Interfaces tab

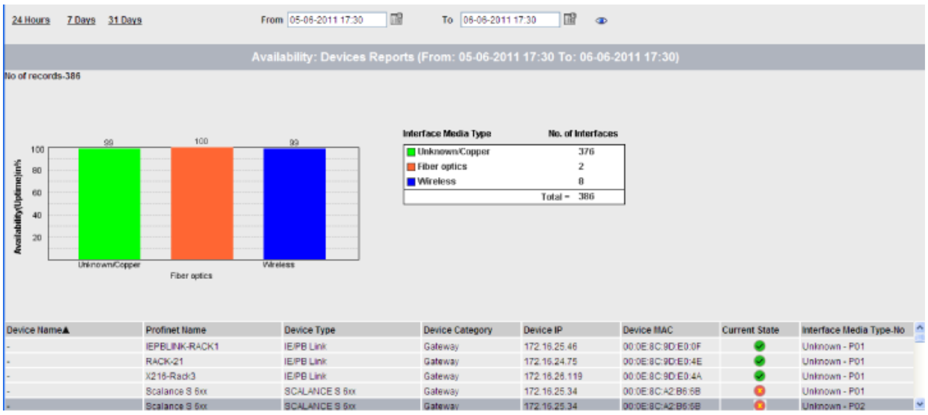
The Interfaces tab provides reports based on the interface media type available for the devices in the network. The interface availability report contains the device name, device type, device IP address, device MAC address, current state, no. of outages, total downtime and availability of the devices as a percentage. The report fields containing device-specific information are provided in the report view only for reference purposes. They do not contain refreshed or actual information about the network devices available at a particular time. This device-specific information helps to relate other report parameters to establish for which device or IP address the change might be applicable. The report information in this tab is shown as a table.

Note

When you click on the Interfaces tab, a new pop-up window is displayed that contains the Availability Interfaces report information.

Note

The report fields Device name, Device type, Device category, Device IP, Device MAC, Current state and Interface media type no. do not provide actual or updated device information available at that point in time. This information is provided as reference for other report field parameters.



From 05-06-2011 17:30 To 06-06-2011 17:30

Availability: Devices Reports (From: 05-06-2011 17:30 To: 06-06-2011 17:30)

No of records-386

Interface Media Type	No. of Interfaces
🟩 Unknown/Copper	376
🟥 Fiber optics	2
🟦 Wireless	8
Total =	386

Device Name▲	Profinet Name	Device Type	Device Category	Device IP	Device MAC	Current State	Interface Media Type-No
-	IEPBLINK-RACK1	IE/PB Link	Gateway	172.16.25.46	00:0E:8C:9D:E0:0F	✓	Unknown - P01
-	RACK-21	IE/PB Link	Gateway	172.16.24.75	00:0E:8C:9D:E0:4E	✓	Unknown - P01
-	X216-Rack3	IE/PB Link	Gateway	172.16.26.119	00:0E:8C:9D:E0:4A	✓	Unknown - P01
-	Scalance S 6xx	SCALANCE S 6xx	Gateway	172.16.25.34	00:0E:8C:A2:B6:5B	✗	Unknown - P01
-	Scalance S 6xx	SCALANCE S 6xx	Gateway	172.16.25.34	00:0E:8C:A2:B6:5B	✗	Unknown - P02

A bar chart is displayed at the top of the page indicating the interface availability. This bar chart displays the interface availability (up time) as a percentage grouped according to the LAN interface type. The chart legend shows the names of the different interface types such as copper, wireless, fiber-optic and the number of interfaces existing for these interface types.

The report in table form is displayed at the bottom of the page. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	Category of the device.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Interface media type no.	Type of interface used and interface number.
No. of outages	Number of times when the device was not reachable.
Interface availability	Sum of all the times when the interface was reachable.
Interface total downtime	Sum of all the times when the interface was not reachable.
Interface availability (%)	Shows device availability - days: hours: mins.
Interface last seen	The time and date when the device was last seen.
Interface first seen	The time and date when the device was first seen.
Mean down time	Time during which the interface was down. MDT = total down time / number of outages
Mean up time	The time during which the interface was up as indicated by "OperState". MUP = total up time / number of outages.

5.4.3 Network performance

Display status

The **Reports > Performance** menu item generates performance reports based on interface utilization and the quality of these interfaces.

General information

The Performance report provides performance-related information. This report provides complete information about device-specific parameters and various other interface quality and signal strength parameters. This information is displayed as a table on the Performance reports page.

Note

When you view the Reports page for the first time, you may see that the reports do not display any information. The report data is displayed only after filtering the report information for a certain time.

The Reports > Performance page contains six tabs:

- LAN interface utilization
- WLAN interface data rate
- LAN interface quality
- WLAN interface quality
- WLAN signal strength
- WLAN number of clients

These tabs can be seen at the top of the Performance reports page. Click on any of these tabs to view the corresponding report. By default, the LAN interface utilization tab is selected when you click the **Reports > Performance** menu.

Note

The filter options in the Reports menu are the same on all Report pages.

Note

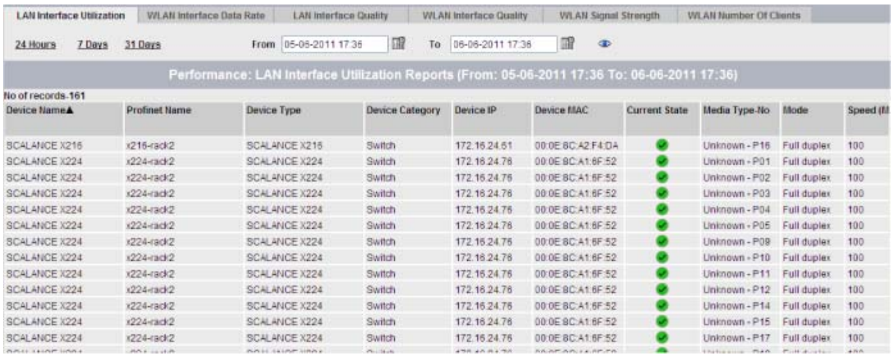
When filtering the report based on a specified period, the time in the From and To fields should be at least 10 minutes.

Note

The report fields Device name, Device type, Device category, Device IP, Device MAC, Current state and Interface media type no. do not provide actual or updated device information available at that point in time. This information is provided as reference for other report field parameters.

LAN interface utilization

The LAN interface utilization tab provides reports based on the interface use in the current network. This report helps you to analyze the performance, efficiency and utilization percentages of the interfaces. The report includes a table view containing device- and interface-specific information including full duplex utilization information. The device names can be sorted either in ascending or descending order by clicking on the arrow in the column header of the table view.



From 05-06-2011 17:36 To 06-06-2011 17:36

Performance: LAN Interface Utilization Reports (From: 05-06-2011 17:36 To: 06-06-2011 17:36)

No of records-161

Device Name▲	Profinet Name	Device Type	Device Category	Device IP	Device MAC	Current State	Media Type-No	Mode	Speed (M
SCALANCE X216	x216-rack2	SCALANCE X216	Switch	172.16.24.61	00:0E:8C:A2:F4:DA	✓	Unknown - P16	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P01	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P02	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P03	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P04	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P05	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P09	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P10	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P11	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P12	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P14	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P15	Full duplex	100
SCALANCE X224	x224-rack2	SCALANCE X224	Switch	172.16.24.76	00:0E:8C:A1:6F:52	✓	Unknown - P17	Full duplex	100

The report in table form is displayed on the Performance reports > LAN interface utilization tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	Category of the device.
Device IP	IP address of the device.
Device MAC	MAC address.
Current state	Current state of the device represented as an icon.
Media type no.	Type of interface used and interface number
Mode	Full duplex or half duplex mode.
Speed (Mbps)	Speed of interface in Mbps.
Average transmit utilization (%)	Average of archived interface (transmit) utilization over selected time span as a percentage.
Maximum transmit utilization (%)	Maximum archived interface transmit utilization over selected time span as a percentage.
Average receive utilization (%)	Average archived interface (receive) utilization over selected time span as a percentage.
Maximum receive utilization (%)	Maximum archived interface receive utilization over selected time span as a percentage.
Average utilization (%)	Average archived interface utilization over selected time span as a percentage.
Maximum utilization (%)	Maximum archived interface utilization over selected time span as a percentage.

WLAN interface data rate

The WLAN interface data rate tab provides reports specifically about the interface data rate and the transmission capabilities within the current network. This report determines the data transmission rates, the interface mode and interface channel speed for each of these devices within the network.

This report provides a table view that contains information about the device-specific parameters and other WLAN interface transmission rate information.

The report in table form is displayed on the Performance reports > WLAN interface data rate tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	Category of the device.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Interface no.	Interface number.
Device mode	Current mode of the device.
Mode	Interface mode used.
Channel (GHz)	Speed of interface in GHz.
Current transmit data rate (Mbps)	Transmit data rate in Mbps.
Average transmit data rate (Mbps)	Average transmit data rate over selected time period.
Maximum transmit data rate (Mbps)	Maximum transmit data rate over selected time period.

LAN interface quality

The LAN interface quality tab provides reports based on the quality of LAN interfaces used in the current network. Various interface modes, their interface speeds and error percentages of LAN interfaces are displayed in this report. The quality factor of these LAN interfaces is measured based on the error rate. This report determines the quality aspects of LAN interfaces provides a basis for measures to improve network efficiency.

This report provides a table view that contains information about the device-specific parameters and other quality-related interface parameters.

The report in table form is displayed on the Performance reports > LAN interface quality tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	WLAN device category.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Media type no.	Type of interface and interface number.
Mode	Mode - 802.11 a/b/g
Speed (Mbps)	Speed of the interface channel in GHz.
Average error (%)	Average error rate over a selected time period as a percentage.
Maximum error (%)	maximum error rate over a selected time period as a percentage.

WLAN interface quality

The WLAN interface quality tab provides reports based on the quality of WLAN interfaces used in the current network. Various interface modes supported for WLAN interfaces including transmit data rate and transmit error rate are shown in this report. This report determines the quality aspects of WLAN interfaces.

This report provides a table view that contains information about device-specific parameters, interface mode, interface speed including information about transmit data rate and error rate as a percentage.

The report in table form is displayed on the Performance reports > WLAN interface quality tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	WLAN device category.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Interface no.	Interface number.
Device mode	Current mode of the device.
Mode	Interface mode used.
Channel (GHz)	Speed of interface in GHz.
Current transmit data rate (Mbps)	Transmit data rate in Mbps.
Average transmit error (%)	Average transmit error rate as a percentage.
Maximum transmit error (%)	Maximum transmit error rate as a percentage.
Average receive error (%)	Average receive error rate as a percentage.
Maximum receive error (%)	Maximum receive error rate as a percentage.

WLAN signal strength

The WLAN signal strength tab provides information about the transmit data rate and signal strength for each specific device in the network. This report helps to determine the wireless data transmission rates and signal strength efficiency. The current device mode, interface mode, interface channel speed and its interface number can also be seen in this report.

The table view contains information about the device-specific parameters, transmit data rate and signal strength parameters.

The report in table form is displayed on the Performance reports > WLAN signal strength tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	WLAN device category.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Interface no.	Interface number.
Device mode	Current mode of the device.
Mode	Interface mode used.
Channel (GHz)	Speed of interface in GHz.
Current transmit data rate (Mbps)	Transmit data rate in Mbps.
Average signal strength (dBm)	Average signal strength in dBm.
Maximum signal strength (dBm)	Maximum signal strength in dBm.

WLAN number of clients

The WLAN number of clients tab provides information about the number of clients connected to each of these wireless devices, their transmit data rate, interface channel speed, mode of transmission and other device-specific details. This report helps to determine the number of clients connected and their transmission rates.

The table view provides device-specific information, current state, interface mode, interface number, interface channel speed, current transmit data rates and the number of clients connected to each of these wireless devices.

The report in table form is displayed on the Performance reports > WLAN signal strength tab. This report contains various device parameters. The device parameters and their meaning are shown below:

Parameter	Description
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of network device.
Device category	WLAN device category.
Device IP	IP address of the device.
Device MAC	MAC address of the device.
Current state	Current state of the device represented as an icon.
Interface no.	Interface number.
Mode	Interface mode used.
Channel (GHz)	Speed of interface in GHz.
Current transmit data rate (Mbps)	Transmit data rate in Mbps.
Average (no. of clients)	Average total number of clients available during a selected time.
Maximum (no. of clients)	Maximum number of clients available during a selected time.

5.5 Network administration

5.5.1 Manage device list

Display status

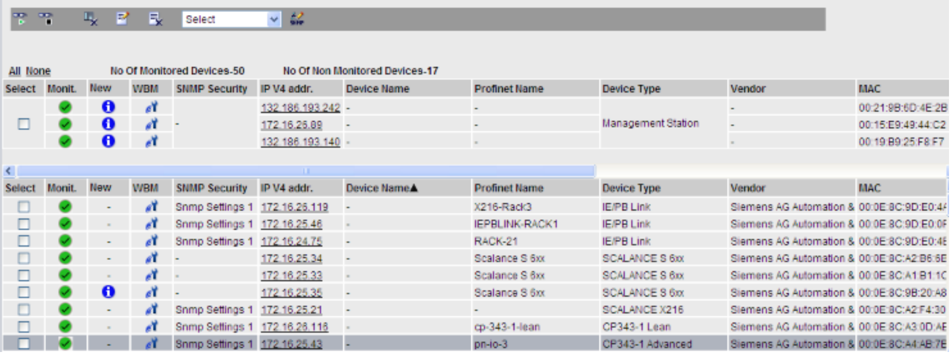
The **Admin** > **Device list** menu item displays the list of devices along with options for administering and managing the device list. With this page, you can display and manage information specific relating to the management station and the list of devices detected in the network.

General information

The **Admin** > **Device list** menu item lists the management station device type along with devices discovered in the network. This page provides options for managing the device list settings. You can enable or disable device monitoring, delete a device, add notes and make SNMP settings for the list of devices available in the network. These controls are available as icons at the top of the page. The icons and their meaning are described below:

Icon	Description
	Start monitoring
	Stop monitoring
	Delete device
	Add notes
	Delete notes
SNMP	Modify SNMP settings

The list of devices displayed in the **Network** and **Devices** menu can be easily managed from the **Admin** > **Device list** page.



All None   No Of Monitored Devices-50   No Of Non Monitored Devices-17

Select	Monit.	New	WBM	SNMP Security	IP V4 addr.	Device Name	Profinet Name	Device Type	Vendor	MAC
□	✓	ℹ	🔧	-	132.186.193.242	-	-	Management Station	-	00:21:9B:6D:4E:2B
	✓	ℹ	🔧		172.16.26.89	-	-		-	00:15:E9:49:44:C2
	✓	ℹ	🔧		132.186.193.140	-	-		-	00:19:B9:25:F8:F7

Select	Monit.	New	WBM	SNMP Security	IP V4 addr.	Device Name▲	Profinet Name	Device Type	Vendor	MAC
□	✓	-	🔧	Snmp Settings 1	172.16.26.119	-	X216-Rack3	IE/PB Link	Siemens AG Automation &	00:0E:8C:9D:E0:4
□	✓	-	🔧	Snmp Settings 1	172.16.25.46	-	IEPBLINK-RACK1	IE/PB Link	Siemens AG Automation &	00:0E:8C:9D:E0:0
□	✓	-	🔧	Snmp Settings 1	172.16.24.75	-	RACK-21	IE/PB Link	Siemens AG Automation &	00:0E:8C:9D:E0:4
□	✓	-	🔧	-	172.16.25.34	-	Scalance S 6xx	SCALANCE S 6xx	Siemens AG Automation &	00:0E:8C:A2:B6:6E
□	✓	-	🔧	-	172.16.25.33	-	Scalance S 6xx	SCALANCE S 6xx	Siemens AG Automation &	00:0E:8C:A1:B1:1C
□	✓	ℹ	🔧	-	172.16.25.35	-	Scalance S 6xx	SCALANCE S 6xx	Siemens AG Automation &	00:0E:8C:9B:20:A8
□	✓	-	🔧	Snmp Settings 1	172.16.25.21	-	-	SCALANCE X216	Siemens AG Automation &	00:0E:8C:A2:F4:30
□	✓	-	🔧	Snmp Settings 1	172.16.26.116	-	cp-343-1-lean	CP343-1 Lean	Siemens AG Automation &	00:0E:8C:A3:0D:A
□	✓	-	🔧	Snmp Settings 1	172.16.25.43	-	pn-io-3	CP343-1 Advanced	Siemens AG Automation &	00:0E:8C:A4:AB:7E

The total number of monitored and non-monitored devices that exist in the current network is shown at the top of this page. The management station device type is shown in a separate table that contains a list of devices. Even if there are several devices in the management station, a single check box is available for selection. For stations with other device types, a Select check box is available for each of the network devices. You can select all the devices in the list in one action using the "All" option. Selecting the option "None" deselects all the devices if you do not want to perform operations on all the devices.

Monitoring concept

In SINEMA Server, whenever devices are newly discovered, the status is displayed as "Enable monitoring in progress". This indicates an intermediate status before the device is moved to the final status "Enable monitoring" or "Disable monitoring" status. Depending on the license type, these network devices will be changed to the monitored status by the application. When the devices are in the non-monitored status, only a few details about the device are shown on the relevant pages. The following points apply to devices in the non-monitored status:

- If errors occur, the application cannot display generated events for the device.
- The non-monitored devices are identified by an "x".
- The device details page is not displayed after clicking the IP address link of an unmonitored device.
- The non-monitored devices will not be shown in user defined maps or in the Reference Editor.

If devices are in the monitored state, complete details of the network device including events and device parameters can be displayed. In monitored state, the devices within the network can be managed and monitored. Any changes to the device in the network can be tracked easily when the devices are in the monitored state.

The number of devices that will be changed to the monitored state in the network depends on the license type. For example, with a Basic 250 license, if there are 300 network devices, then only a set of 250 nodes will be monitored. The remaining 50 devices will be unmonitored. If SINEMA Server is running with a trial license, a maximum of 50 devices will be in the monitoring state, the rest of the devices will be in the unmonitored state.

Device list parameters

The device list parameters and their meaning are shown below:

Parameter	Description
Select	Selects the device before performing actions.
Monit.	Displays a green icon if the device is monitored.
New dev.	Displays status of the new device.
WBM	Provides settings specific to the device.
SNMP security	Type of SNMP settings used. For example SNMP settings1, SNMP settings 2, etc.
IP V4 addr.	IP address of the network device.
Device name	Name of the device.
PROFINET name	PNIO name.
Device type	Type of the device.
Vendor	The device vendor.
MAC	The MAC address.
Firmware	The firmware version of the device.
Order number	Unique ID associated with the specific device.
Device category	Device category type.
Notes	Displays notes.

Enabling or disabling monitoring

The **Admin > Device list** page includes options for enabling or disabling device monitoring. To enable or disable monitoring of network devices, follow these steps:

1. From the list of devices displayed, select the device by clicking the check box in the same row.
2. Click the "Enable monitoring" icon to enable monitoring for the specific network device.
3. If the device is already being monitored, you can disable monitoring. To disable monitoring, select the device using the Select check box in the device row and click the Disable monitoring icon.

In the Monitoring column, the various device states are represented using icons to indicate the final or intermediate status. The status icons and their meaning are shown below:

Status icon	Description
✓	Enable monitoring (possible final status)
✗	Disable monitoring (possible final status)
🖧	Possible intermediate status • Enable monitoring is in progress • Disable monitoring is in progress • Delete device is in progress

Note

If one or more devices is selected for the Enable or Disable or Delete operation, the device will first be changed to the relevant intermediate status. Once the required operation is complete, the device will be changed to the relevant final status. You will see that while a device is in an intermediate status, the entire row for the device is disabled. Wait until the device is changed to a final status before performing any other operation on the device.

The number of monitored devices depends on the license type available. With a Basic 100 license, a total of 100 devices or less can be monitored easily.

Scenario:

A user has a Basic 100 license type and is monitoring 70 devices in the network. The user downgrades to Basic 50. This results in a mismatch where the number of monitored devices is greater than the present license allows. In this case, all the links in the Web client will have the disabled status except the Admin > Device list link.

To solve this problem, the monitored devices need to be disabled or deleted in keeping with the license type available. A logout-login session is also required to ensure that all the links in the Web client are in the enabled status.

Delete device

The monitored or unmonitored devices displayed in the device list can be deleted using the "Delete device" icon. This user control is available as an icon at the top of the Device list page. To delete a device from the list, follow these steps:

1. Select the check box in the row of the device you want to delete.
2. This check box is below the "Select" box for each row.
3. Click the "Delete device" icon to delete the device from the device list.

Add notes

You can add notes to any device with information about the specific device or its default settings. Adding notes to the devices in the device list helps you to manage the devices better.

To add notes to a device in the device list, follow these steps:

1. From the list of devices, select the check box of the device to which you want to add a note.
2. Click the Add notes icon.

   A pop-up window appears.
3. Type the note in the text box and click the Add button.

   The note is added to the device.

If you add notes to a device that already contains notes, the previous notes will be overwritten.

Modify SNMP settings

The SNMP settings are required when discovering and monitoring devices in the network. The SNMP settings for the network devices displayed on the **Admin** > **Device list** page can be modified using the "Modify SNMP settings" icon. This is used only when the SNMP settings have been set for the device and you want to change the SNMP settings from from the currently used SNMP settings 1. The drop-down list next to the modify SNMP settings icon lists each of the activated SNMP settings.

Note

The SNMP settings on the **Network settings > Scan settings** tab and **Admin > Device list** should be the same as the settings available for the specific network device. If any SNMP settings are modified on the network device, the change needs to be included in the SINEMA Server application using the *Web server* icon on the **Device details > SNMP settings** tab.

Note

To use different SNMP settings for the network device, SNMP settings 2 or SNMP settings 3 must be activated on the **Admin > Network settings**, **Scan settings** tab.

To modify the SNMP settings, follow these steps:

1. From the list of devices, select the check box of the device for which you want to change the SNMP settings.
2. Select the desired SNMP settings from the drop down list; for example, SNMP settings 2.
3. Click the "Modify SNMP icon" button next to the drop-down list box.
4. The network device now starts to use SNMP settings 2 instead of SNMP settings 1.

5.5.2 User administration

Introduction

Managing users and groups in the network becomes critical in a network-based environment when access rights and permissions need to be controlled and managed. SINEMA Server provides a user administration interface with which you can view and manage users and groups in the network. The various configurations required for network administration can only be created by users with administrator privileges.

The various configuration options available in SINEMA Server are as follows:

- Creating and managing users and groups
- Configuring event reactions for predefined network events
- Creating and managing views
- Creating and managing user-defined maps
- Configuring network settings
- Configuring views
- Configuring user interface settings
- Configuring scan settings
- Configuring report settings
- Importing and exporting SINEMA Server project data

User groups

SINEMA Server provides three predefined groups with appropriate access rights. The controls and options available to users differ for each user group. The following table shows the predefined user group name along with access rights information:

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

The access rights within the SINEMA Server application vary according to the type of user. The list of access rights is shown below:

Access right	Description	Administrator	Power	Standard user
User administration	Access to manage users & devices	Yes	No	No
Network scan	Access to start/stop scan	Yes	Yes	No
Add device type	Access to add new device type	Yes	Yes	No
Delete device type	Access to delete device type	Yes	Yes	No
Topology	Access to view topology	Yes	Yes	Yes
User maps	Access to view user maps	Yes	Yes	Yes
Network list	Access to view list of network devices	Yes	Yes	Yes
Reports	Access to view reports	Yes	Yes	Yes
Event statistics	Access to view network statistics	Yes	Yes	Yes
Events	Access to view events list	Yes	Yes	Yes
Event settings	Access to view event settings	Yes	Yes	No
Modify event settings	Access to modify event settings	Yes	Yes	No
Modify network settings	Access to modify network settings	Yes	Yes	No
Catalogs	Access to view catalogs	Yes	Yes	No
Modify catalogs	Access to modify catalogs	Yes	Yes	No
Views	Access to the available views	Yes	Yes	No
Modify quick links	Access to modify quick links	Yes	Yes	No

Login information

A default combination of user name and password is provided by the SINEMA Server application for the three predefined user groups. When logging in to the system for the first time, the following user name and password combinations need to be used for these predefined user groups:

User group	Login information
Administrator	• User name: administrator • Password: SinemaA
Power user	• User name: coordinator • Password: SinemaP
Standard user	• User name: operator • Password: SinemaS

After logging on with the system the first time, a dialog box is displayed that provides options for changing the existing password or keeping the same password for the logged-on user.

Please change the password once you have logged on to the application.

Note

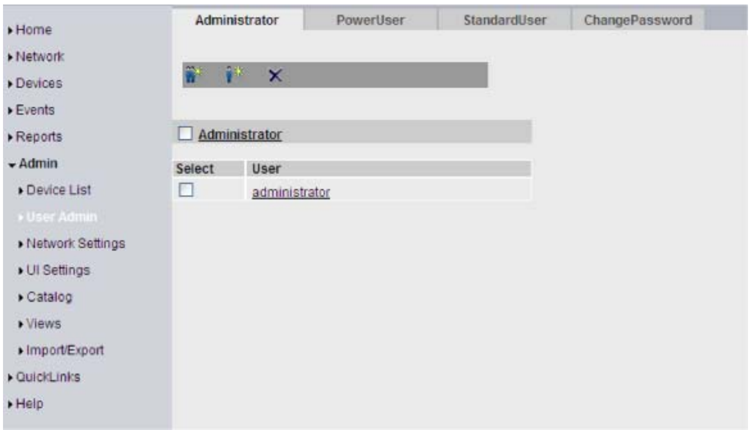
Predefined users and user groups cannot be deleted or modified.

Display options

The **Admin > User admin** menu item displays the list of users available along with the selected user group. The available predefined user groups each have tabs at the top of this page. By default, the Administrator tab, Power user tab, and Standard user tab are available. When the User admin page is opened, the Administrator tab is displayed. Click on the relevant tab to view the users in the selected user group.

Users and groups can be managed easily within these tabs with help of user controls available in the form of icons. The icons and their meaning are described below:

Icon	Description
👥	Add new group
👤	Add user
✕	Delete user/ group
💾	Save
📝	Edit users list
⬅	Navigate back
✏	Edit user group



□ Administrator

Select	User
□	administrator

Creating new user groups

Only a user with administrator rights can create new user groups. With administrator privileges, you can create new user groups in addition to the three predefined user groups. You can assign different access rights to each user group you create.

To create a new user group, follow these steps:

1. On the SINEMA Server menu, click **Admin > User admin**.
2. Click the "Add new group" icon.
3. In the table that appears, enter the name of the new user group in the "User group" text box at the beginning of the list.
4. Select the check boxes next to the access rights you want to assign to the created user group and click the "Save" icon.

   The created user group appears as a tab at the top of the main window.

Creating new users

Only a user with administrator rights can create new users.

To create a new user, follow these steps:

1. On the SINEMA Server menu, click **Admin > User admin**.
2. Click on any user group tab in the main window. By default, three predefined user groups are available - Administrator, Power user and Standard user. Apart from the predefined user groups, you can also have user group tabs for the user-defined user groups.
3. Click the "Add new user" icon on the selected user group tab.

   A table appears with various user parameters listed in the left-hand column and text boxes in the right-hand column.
4. Enter the following details for the new user:
   - Type in the login name of the user in the "User name" text box.
   - Type the name of the user in the "Full user name" text box.
   - Type the login password of the user in the "Password" text box.
   - Type the password again to confirm the password in the "Confirm password" text box.
   - Type the mail ID of the user in the "E-mail ID" text box.
   - Select the group to which the user will belong in the "User group" list box.
   - Select a view for the user from the "View name" list box.
   - Select the required active user map to be associated with a user.
5. Click the "Save" icon.

   The created user is added to the list of users in the selected user group.

Note

The created users will have the access rights assigned to the user group to which they belong.

Note

When a new view is created using Admin > Views, this view can be assigned to a user from the "Add new user" screen. If this user logs on to the application to view the topology, the network topology can be viewed only after a delay of maximum 30 seconds from the time this view was created.

Changing the password for a user

Users can change their password on the "Change password" tab at any time.

To change the password, follow these steps:

1. Select the **Admin > User admin > Change password** tab.

   This tab displays all parameter names along with a text box for editing.

   In the text box for the user name, you can view the user ID used to log in to the SINEMA Server Web interface. This text box cannot be edited.
2. In the Old password text box, enter the old password.
3. Enter the new password in the text box labeled Password.
4. Confirm the new password by entering the new password in the text box.
5. Click the "Save" button to save the new password.

Modifying users

To modify a user's details, follow these steps:

1. Click on the user group tab containing the details of an existing user.
2. Click on the name of the user you want to modify in the displayed list of users.

   A table appears displaying all the parameters of the selected user.
3. Click the User list edit icon.

   The text field of each parameter changes to an editable text box.
4. Make the required changes and click "Save" to save the changes.

Deleting users

You can only delete users you created earlier.

To delete a user from a user group, follow these steps:

1. Go to the user group tab on which you want to delete a user.

   A table appears listing the users available in the selected user group. The left-hand column of the table has check boxes for each user.

2. Select the check box for the user name you want to delete and click the "Delete" icon.

   A status message "Selected group/user deleted successfully" is displayed in the status bar at the top of the page.

3. The user is no longer in the user list.

Modifying user groups

You can modify the access rights for the user-defined user groups. To modify a user group, follow these steps:

1. Click on the tab of the user group you want to modify.

   A table appears listing the users available in the selected user group.

2. Click the name of the user group displayed in the table header.

   A table appears displaying the name and all the access rights of the user group.

3. Click the Edit user group icon.

   The table can now be edited.

4. Make the necessary changes and click the "Save" icon.

Deleting user groups

To delete a user group, follow these steps:

1. Go to the tab of the user group you want to delete.
2. Select the check box belonging to the user group displayed in the table header.
3. Click the Delete icon.

   If any users exist in the user group, a message "Please delete all users belonging to the group before deleting the group" is displayed in the message status bar.

4. Delete the users in the group first and then delete the user group.

Note

When you delete a user group, any users in the user group are not deleted automatically.

5.5.3 Network settings

Display options

The **Admin** > **Network settings** menu item is used to manage and control the settings used by SINEMA Server for a specific network.

General information

The "Network settings" page is used to configure and manage the network settings in the current network. The various network settings such as device detection, scan settings, event reactions and e-mail settings can be configured on the Admin > Network settings page.

Detailed information

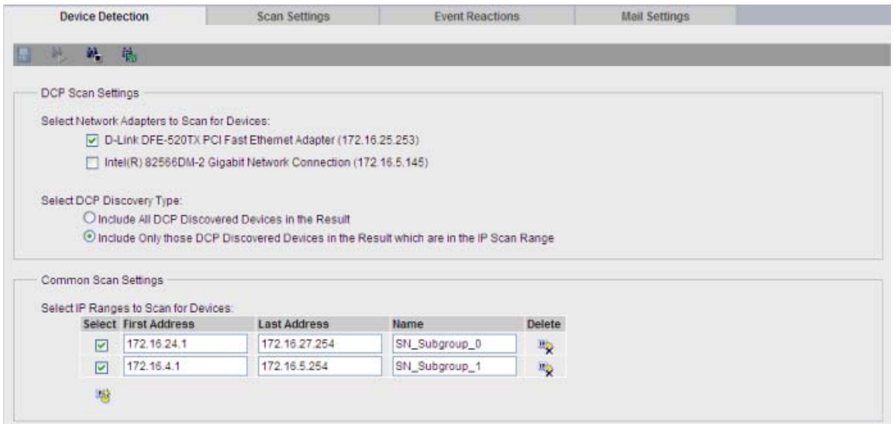
The "Network settings" page includes the following tabs for managing various settings in the network:

- Device detection
- Scan settings
- Event reactions
- Mail settings

Device detection

The most important part of the activities involved in managing the network devices is specifying the device detection settings. The Device detection tab includes the following 2 sections as shown in the screenshot below. It includes options for setting the DCP scan, discovery type and common scan settings including several user controls available in the form of icons. The icons and their meaning are described below:

Icon	Description
💾	Save
	Start scan
■	Stop scan
	Scan NIC
IP	Add IP range
IP	Delete IP range



DCP Scan Settings

Select Network Adapters to Scan for Devices:

☑ D-Link DFE-520TX PCI Fast Ethernet Adapter (172.16.25.253)

□ Intel(R) 82566DM-2 Gigabit Network Connection (172.16.5.145)

Select DCP Discovery Type:

○ Include All DCP Discovered Devices in the Result

● Include Only those DCP Discovered Devices in the Result which are in the IP Scan Range

Common Scan Settings

Select IP Ranges to Scan for Devices:

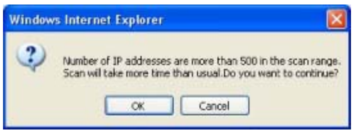
Select	First Address	Last Address	Name	Delete
☑	172.16.24.1	172.16.27.254	SN_Subgroup_0	
☑	172.16.4.1	172.16.5.254	SN_Subgroup_1	

1. In the "DCP scan settings" section, select the list of network adapters by clicking the check box.
2. Click the "Scan NIC" button if you cannot see the list of network adapters.
3. Select the "DCP discovery type" option by choosing the relevant setting to include the devices discovered with DCP in the scan.
4. In the "Common scan settings" section, select the IP ranges available to scan for devices by clicking the "Select" check box next to each defined IP range.
5. If the IP range does not exist, click the "Add IP range" icon to add a new IP range and specify the "First address", "Last address" and a unique subgroup name for the IP range. The subgroup name cannot be written as "Others" while entering subgroup name in the text box.
6. To delete an existing IP range, select the IP range and click the "Delete" icon.
7. Click the "Save" icon to save the current settings. Next, click the "Start scan" icon to start device scanning. The "Start scan" icon is disabled out indicating that scanning is in progress.
8. To stop an active scan, click the "Stop scan" icon.

Note

In DCP Scan settings, if you choose the option "Include all devices discovered by DCP in the result", it is possible that DCP devices that are outside the IP range(s) but within the subnet(s) connected to the NIC(s) will also be discovered.

The network device scan takes much longer to complete if the scan range is large. If the scan range includes more than 500 devices that need to be configured in the network, a notification message as shown in the screenshot below will alert you about the scan time. Click OK to continue or Cancel to stop the current operation so that you can specify a different scan range.



Windows Internet Explorer

Number of IP addresses are more than 500 in the scan range. Scan will take more time than usual.Do you want to continue?

We therefore recommend that you specify the IP address range in small sub-groups (instead of a large single group) up to a maximum of 20 sub-groups if the IP addresses are scattered. This will help to speed up the scanning of the devices.

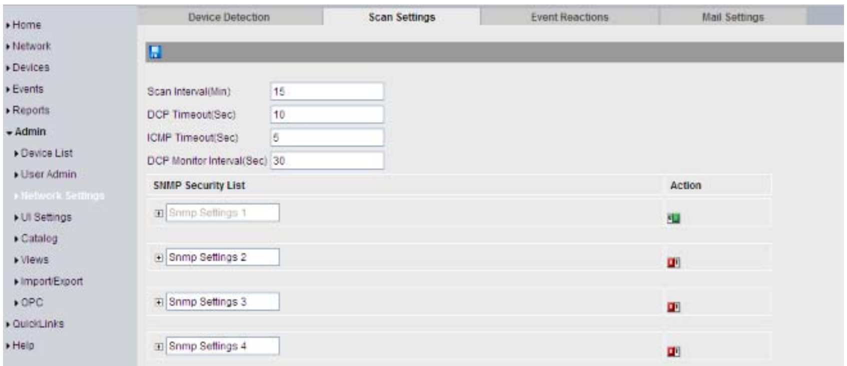
Note

For the DCP protocol to function correctly, DCP binaries can be loaded by only one application at a time. If DCP binaries are loaded by application(s) such PST, SINEMA Server will not be able to run the DCP protocol. If this happens, an alert will be triggered in the application.

Scan settings

The Scan settings tab includes time-related parameters and SNMP parameter settings required for device discovery within the network. This tab consists of various options for setting these parameters including several user controls available as icons. The icons and their meaning are described below:

Icon	Description
0 I	Activate
0 I	Deactivate



Scan Interval(Min) 15
DCP Timeout(Sec) 10
ICMP Timeout(Sec) 5
DCP Monitor Interval(Sec) 30

SNMP Security List	Action
Snmp Settings 1	
Snmp Settings 2	
Snmp Settings 3	
Snmp Settings 4	

Time-related parameters: The time-related settings required for discovery by SINEMA Server are displayed in the text boxes. These text boxes are displayed at the top of the "Scan settings" tab below the "Save" button. The time-related parameters are described below:

Parameter	Description
Scan interval (min)	The time interval between each successive scan. Resolution in minutes.
DCP timeout (sec)	The maximum time allowed for a DCP discovery. Represented in seconds.
ICMP timeout (sec)	The maximum time allowed for an ICMP discovery. Represented in seconds.

SNMP settings: The SNMP settings on the "Scan settings" tab are listed with the column headings "SNMP security list" and "Status". The SNMP parameters required for discovering and monitoring the devices in the network are displayed in SNMP settings 1, SNMP settings 2 up to SNMP settings 10. The SNMP parameters can be displayed by clicking the ‘+’ symbol. Once the required changes are made to the parameters, click the "Activate" button to save the changes for each SNMP setting. If you do not want to use the setting, select the "Deactivate" button.

Note

The SNMP settings on the "Scan settings" tab should be the same as the settings available for the specific network device. If any SNMP settings are modified on the network device, the change needs to be included in the SINEMA Server application using the Web server button on the **Device details** > **SNMP settings** tab.

The default values and the recommended range of values for the SNMP parameters are shown below:

Parameter	Default value	Range of values
Version	1	1, 2C, 3
Read community string	public	
Timeout	2000 ms	2000 to 5000 ms
Retries	2	0 to 10
Port	161	

Note

After making the changes, click the "Start scan" button to initiate a scan with the new values. To stop an active scan at any time, click the "Stop scan" button.

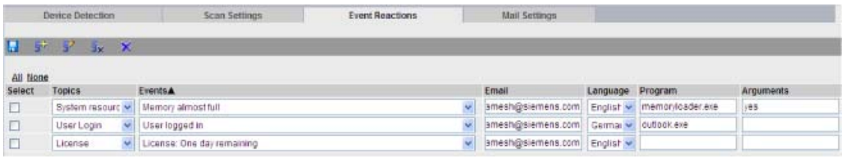
Event reactions

The Event reaction tab includes options for adding actions or rules for each of the predefined events. The required level of action to be taken each time an event occurs can be controlled by adding rules. For example, whenever a user logs into the SINEMA Server application, notifications need to be sent to the user automatically in the form of an e-mail.

Each rule includes a defined set of actions that will be performed on an event. The events are grouped into specific topic areas where every topic name consists of a related set of events. Only the system-related events can be viewed in the Event settings tab while you are adding a rule.

To allow you to perform the various actions in the Event reactions page, there are controls in the form of icons. A list of the icons and their meaning is shown below:

Icon	Description
💾	Save changes to the rule
§✳	Add new rule
§✎	Edit existing rule
§✕	Delete the rule
✕	Cancel the action performed



Select	Topics	Events▲	Email	Language	Program	Arguments
□	System resourc	Memory almost full	amesh@siemens.com	Englist	memoryloader.exe	yes
□	User Login	User logged in	amesh@siemens.com	Germa	outlook.exe	
□	License	License: One day remaining	amesh@siemens.com	Englist		

Note

Event rules work only if the mail settings are configured for the user. Event reactions can trigger a wide variety of programs. However, the application window is not displayed on the screen since the program runs in the background.

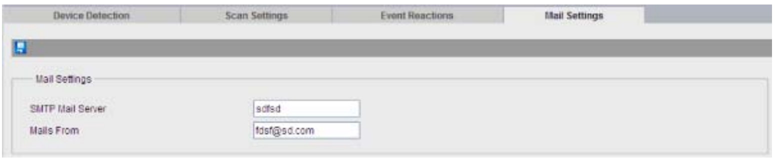
Follow the steps below to set or manage rules for the events generated within the SINEMA Server application:

1. Click the "Add rule" icon to add a new rule to the list of generated events.
2. Select a topic from the list and choose the associated event type from the drop-down list box.
3. Specify a valid e-mail address and select the required language - English or German.

4. Type in the program name that needs to be opened each time the event is fired. The program needs to be an application or an executable file.
5. Enter the required parameters in the arguments text box to specify arguments that need to be used while opening the specified application.
6. Repeat steps 1 to 6 to add more rules to the list of events and click the "Save" icon to save the changes.
7. To edit or delete a rule, select the check box in the row containing a rule and click the appropriate button.

Mail settings

The "Mail settings" tab mainly contains the SMTP mail server settings. The SMTP mail server is used for mail server configuration. These settings are used by Event settings whenever an e-mail address is configured for an event. In this tab, you can configure the SMTP mail server name and e-mail address.



SMTP Mail Server: sdfsd
Mails From: fdsf@sd.com

To make the generic settings, follow these steps:

1. Enter the SMTP mail server address in the "SMTP mail server" text box.
2. Type a valid e-mail address in the "Mails from" text box.
3. Next, click the "Save" icon to save the generic settings.

5.5.4 UI settings

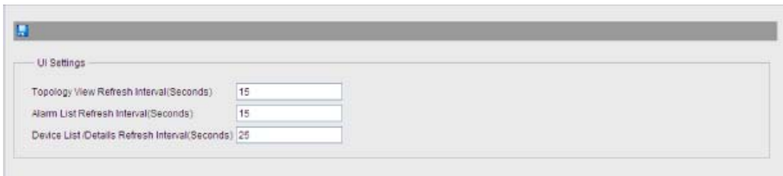
Display options

The **Admin > UI settings** menu item is used to view or manage the refresh time interval settings in the SINEMA Server application.

General information

The UI settings page provides options for specifying the refresh time interval settings in seconds. Based on the time interval specified on the UI settings page, the contents of the page are refreshed as configured. For example, if the topology view refresh Interval is set to 15 seconds, this topology view is refreshed every 15 seconds.

On the UI settings page, there is a text box for each user interface setting where you can modify these settings. Once these UI settings have been made, you can save the user interface changes with the "Save" button. The settings controlled in the UI settings page will override the default automatic refresh setting. This is only applies to the user interfaces listed below.



UI Settings

Topology View Refresh Interval(Seconds) 15
Alarm List Refresh Interval(Seconds) 15
Device List /Details Refresh Interval(Seconds) 25

The refresh time interval settings can be modified for the following user interfaces:

- Topology view: Topology view refresh interval in seconds; default value: 15 seconds.
- Alarm list: Alarm list refresh interval in seconds; default value: 15 seconds.
- Device list / details: Device list / details refresh Interval in seconds; default value: 25 seconds.

5.5.5 Device catalog

Display options

The **Admin > Catalog** menu item is used to add or manage device types containing devices that cannot be identified by SINEMA Server.

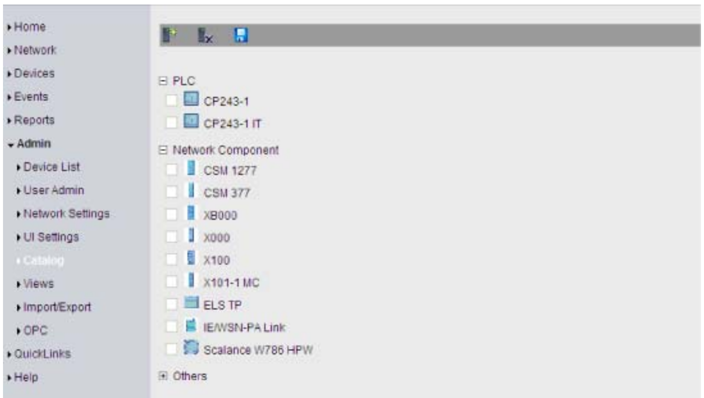
General information

In general, SINEMA Server scans the devices within the network and monitors those devices that can be identified in the current network. However, there are some devices that cannot be identified by SINEMA Server. Such devices can be managed on the Catalog page. As the name suggests, a catalog is used to manage the list of device types. These device types exist in the following three types of device family.

1. PLC
2. Network component
3. Others

The Catalog page includes user controls for adding, saving and deleting user-defined device types. The icons and their meaning are described below:

Icon	Description
✱	Add device type
✕	Delete device type
💾	Save changes



The Catalog page includes options for viewing or managing the device types. There are two kinds of device type available.

- Predefined device types:

  These are device types built into SINEMA Server. The predefined device types in each device family can be viewed on the Catalog page. The properties or values of these predefined device types cannot be modified. However, you can view the properties or values by clicking the device type.

- User-defined device types:

  These device types are defined by the user and they can be created at any point in time. You can create a user-defined device type within any of the device families using the "Add device type" icon.

Each device type contains information about the device type, number of ports, device icon image, device type family, vendor information and protocol support. Each device type acts as a profile. In the user maps, you can create devices of these device types. Such devices are called unmanaged or user-defined devices. By default, there are 21 predefined devices types provided by the SINEMA Server application.

Note

The user-created devices belonging to these device types can only be viewed in the **Network > User maps** page.

Adding or deleting a user-defined device type

To add a new device type, follow these steps:

1. Click the "Add" button to add a new device type.
2. Enter the device type in the "Device type" text box.
3. To insert a device icon, click the "Browse" button and select the icon image you want to use for the device.
4. Specify the vendor name in the empty text box.
5. Select the device family name from the drop-down list and specify the number of ports of the new device.
6. Select the protocols to be supported by the new device by clicking the check box.
7. Click the "Save" button to save these changes.

To delete a device type you created earlier, follow these steps:

1. Click the '+' symbol next to the device family.
2. Select the user-defined device type by clicking the check box.
3. Click the "Delete device type" button to delete a device type.

Note

Once a device has been added to the Device catalog, the number of ports cannot be modified. To modify ports, delete the device and add the device again using the "Add" button.

Note

Predefined device types on the Catalog page cannot be deleted. You will see that the check box is disabled for the predefined device types.

5.5.6 Managing views

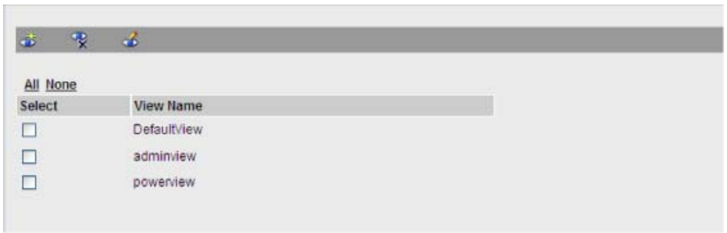
Display options

The **Admin > Views** menu item is used to create and manage views. The views help in the effective management and tracking of a set of network devices available in the network.

General information

The views provided in SINEMA Server help you to customize a list of network devices displayed on the page. Views can be created and managed to suit your particular requirements. You may, for example, only want to to view a set of 10 network devices in the network. A user-defined view can then be created to view only these 10 devices. It is easier to manage these devices with the help of a view. The Views page provides user controls for adding a view, deleting a view and modifying the views that have already been created. The icons and their meaning are described below:

Icon	Description
	Add view
	Delete view
	Modify view
💾	Save changes
⬅	Navigate back



All None

Select	View Name
□	DefaultView
□	adminview
□	powerview

Default views

A pre-defined view is available in the **Admin > Views** page. This is created by default and can be seen when you open the Views page:

- Default view

  The default view is a predefined view available on the Views page. This view contains all monitored devices displayed in a table. This view cannot, however, be modified or deleted by the user.

Adding user-defined views

To add a new user-defined view, follow these steps:

1. Click the "Add view" icon displayed at the top of the Views page.
2. A list of devices will be shown in a table containing device-related information.
3. Specify a name for this view in the "View name" text box.
4. In the table view, click the check box for each device you want to add to the view.
5. Click the "Save" icon to save the changes to your view.
6. The newly created view will then be displayed on the Views page.

Modifying or deleting a view

To modify a view you created earlier, follow these steps:

1. On the Views page, select the user-defined view you want to modify. You can do this by selecting the check box next to the name of the view.
2. Click the "Modify view" icon to modify the content of the view.
3. Select the devices you want to include in the view and click the "Save" icon.

To delete a user-defined view, select the check box next to the view name and click the "Delete view" button. A status message is displayed in the message bar at the top of Views page once the view has been deleted.

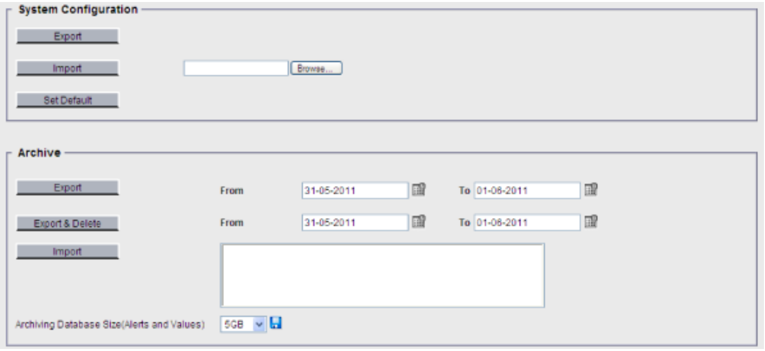
5.5.7 Import/export

Display options

The **Admin > Import / export** menu item helps you to handle the SINEMA Server system configuration and provides options for archiving its data.

General information

Using the SINEMA Server application, you may at times need to manage system configuration information or archive the data. These tasks can be handled with the **Admin > Import / export** menu item.



From 31-05-2011 To 01-06-2011

From 31-05-2011 To 01-06-2011

Archiving Database Size(Alerts and Values) 5GB

The Import/export page includes import/export options for the following operations:

1. System configuration
2. Archiving

System configuration

At times, it may be necessary to save the system configuration on the client machine or import a previously used system configuration or set a particular system configuration as the default. To handle these tasks, the Import/export page provides the "Export", "Import" and "Set default" buttons.

Export:

Click the "Export" button to export the system configuration. A dialog box opens providing you with options for saving or opening the system configuration.

Import:

To import an existing system configuration, click the "Import" button and select the .dpl file using the "Browse" button.

Set default:

To set a specific system configuration as the default, click the "Set default" button. The existing system configuration is then set as default and a message is displayed in the message status bar at the top of the page to indicate the success or failure of this operation.

Archiving

Data is archived in SINEMA Server when it may be necessary to retrieve historical data. If there is a lack of storage space or a hardware failure on the host computer, this will result in loss of data. Archiving helps to avoid loss of data and allows data to be retained over longer periods of time. To handle these archive operations, the Import/export page provides "Export", "Export & delete" and "Import" buttons.

The Archive section includes an option for setting the archive database size (alerts and values) and allows the changes to be saved. A minimum of 3.0 GB is required for storing archived data. This includes both installation space and space for archived data. 2 GB is required for the SINEMA Server installation. The remaining space is available for archiving. The table below will help you to decide how much space you will require on the computer and the approximate number of files that can be stored on hard disk. After a specified number is reached, the oldest files are deleted to make space for new files.

Space required for SINEMA Server (GB)	Approximate number of files
3	130
4	270
5	410
6	550
7	690
8	830
9	970
10	1110
11	1250
21	2660

Note

These calculations are approximate and based on test data. It is not possible to predict exact values that might occur in runtime in an real environment.

Note

It is advisable to export the archive files before they are deleted.

Export:

The historical data to be archived needs to be exported from the online system. This can be done using the "Export" button. Click the "Export" button to export the historical data. A dialog box opens providing you with options for saving or opening the compressed data.

Export & delete:

This option provides the same functionality as the "Export" button. Additionally, this option checks whether this archived data is stored in any other locations on the SINEMA Server and then deletes the archive.

Import:

Once the archived data has been exported using the Export option, this data will be made available as a zip file and this is shown in the file list next to the Import button. Select the required file from the file list and click the "Import" button to begin importing the archive.

5.5.8 OPC

Display options

The **Admin > OPC** menu item provides an OPC view that is used to manage and view the list of network devices displayed on the OPC client.

General information

This OPC view is available as default on the **Admin > OPC** page. This page provides a list of network devices along with device-related information. The devices shown on this page can be modified to show only a specific set of devices on the OPC server. In the "Visible in OPC" column, select the check box available for each of these devices and select the "Save" icon. While accessing the OPC server, you will be able to view only the devices that are filtered in the OPC page. This view cannot be deleted by the user.

The Device index column in the table view shows the index number for each network device. This information is useful to map the corresponding device when it is monitored through an OPC client and makes identification of devices easier. For example, if the device name on the OPC client is listed as *SN_DV_MON_ScalanceX200_45*, the corresponding device index on the OPC page will be shown as *ScalanceX200_45*.

Viewing SINEMA Server data using an OPC server 6

OPC

Open Process Control (OPC) is used in industrial automation devices to communicate real-time plant data, alarms and events, historical data and batch process data between control devices of different manufacturers. The OPC interface is a standard for interoperability of different systems for the data exchange at runtime. Third party systems can have OPC clients to connect to the OPC server and read or monitor the data.

Using an OPC server to access SINEMA server data

Only users who have access to SINEMA Server can access SINEMA Server project data using an OPC server. You can use the OPC client to access an OPC server. Through an OPC server, you can access SINEMA Server configuration data and the properties of the network devices.

Any OPC client can be used to interact with an OPC server. You can use the OPC server to view the runtime data and properties of a SINEMA Server project and can also modify the values for the runtime data.

Note

If you want remote access to SINEMA Server data, the OPC client must be installed locally on your computer.

Note

An OPC view with a list of network devices is required before setting up OPC connections. You can create an OPC view on the **Admin > OPC** page. Whenever the OPC view changes (new devices identified or existing devices deleted), all the connected OPC clients need to be disconnected and reconnected to the OPC Server to browse the latest devices in the OPC view.

OPC Data Access (UA)

OPC Unified Architecture is based on service-oriented architecture and removes the Microsoft COM/DCOM parts. OPC UA is a cross-platform standard through which various kinds of systems and devices can communicate by sending messages between clients and servers over various types of networks. UA supports robust, secure communication that secures the identity of clients and servers and resists attacks.

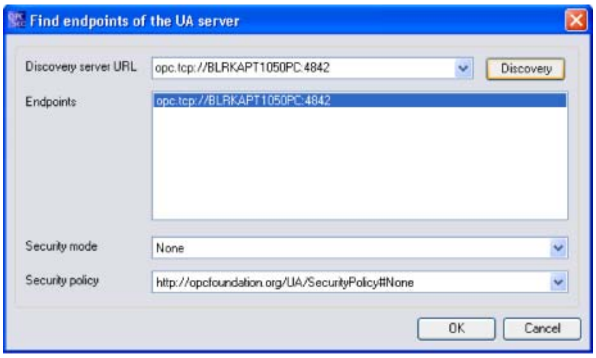
Configuring UA ports

The default port used for a UA server is 4840. These ports can be configured using the Config option available in the SINEMA Server Monitor panel shortcut menu. To access this shortcut menu, right click on the SINEMA Server Monitor panel tray icon. A window opens providing you with a list of options.

For more information about configuring a UA port, refer to "*Basic steps in operation*" in section 4.1.

Accessing SINEMA Server data using an OPC server (OPC UA)

1. In Windows, click Start > All Programs > SIMATIC > SIMATIC NET > OPC Scout to open the OPC Scout client.
2. In the Server Explorer window, expand the UA server folder in the navigation area.
3. Click on the Add server entry. The "Find endpoints of the UA server" dialog opens.
4. Enter the Discovery URL and IP address or the computer name and port number of the discovery server in the "Discovery server URL" input box.
5. Specify the security options as shown in the screenshot below and click OK.



Discovery server URL: opc.tcp://BLRKAPT1050PC:4842

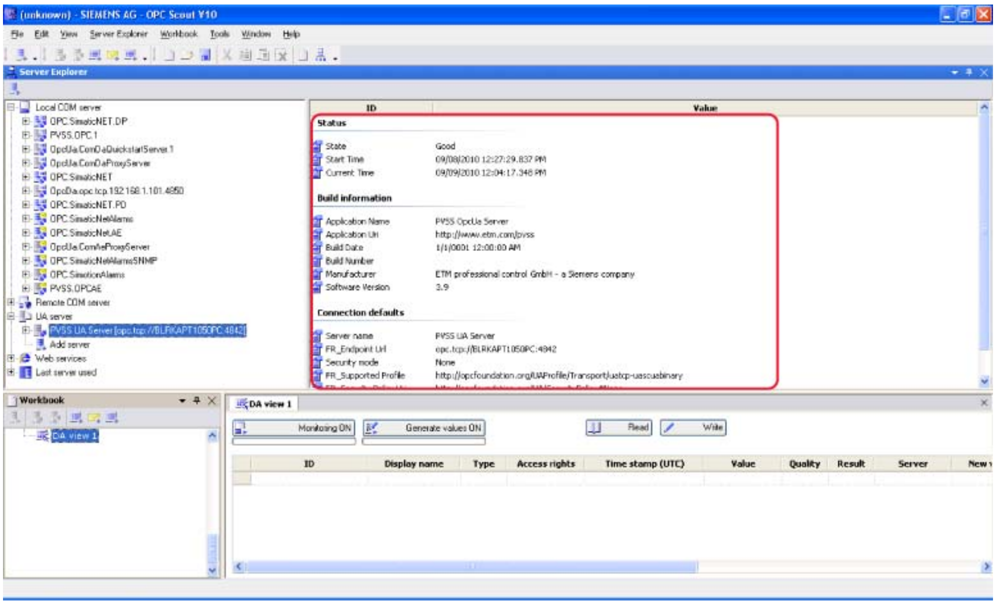
Endpoints: opc.tcp://BLRKAPT1050PC:4842

Security mode: None

Security policy: http://opcfoundation.org/UA/SecurityPolicy#None

6. The connected UA server will now be listed in the UA server folder in the navigation tree.

7. Click on the server to view the connection status and connection defaults information. This information is displayed on the right-hand side in the Server Explorer window.



ID	Value
Status	
State	Good
Start Time	09/08/2010 12:27:29.837 PM
Current Time	09/09/2010 12:04:17.348 PM
Build information	
Application Name	PVSS OpcUa Server
Application Uri	http://www.etm.com/pvss
Build Date	1/1/0001 12:00:00 AM
Build Number	
Manufacturer	ETM professional control GmbH - a Siemens company
Software Version	3.9
Connection defaults	
Server name	PVSS UA Server
FR_Endpoint Url	opc.tcp://BLRKAPT1050PC:4842
Security mode	None
FR_Supported Profile	http://opcfoundation.org/UAProfile/Transport/uatcp-uasc-uabinary

ID	Display name	Type	Access rights	Time stamp (UTC)	Value	Quality	Result	Server	New v

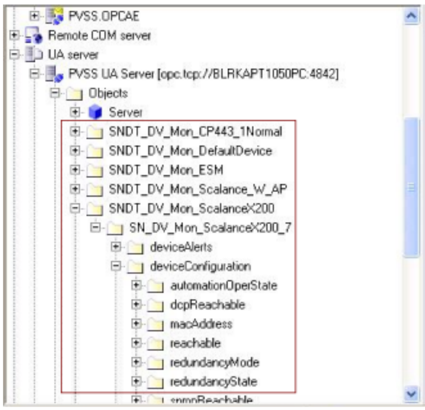
8. Expand the connected UA server to view the list of network devices. The folder name beginning with SNDT_DV_Mon identifies the network device name.

Note

Only objects that have been added to the OPC view are displayed in the navigation pane.

---

9. The fields displayed in **Network > All** correspond to the device property names available as folders in the "Device configuration" folder.



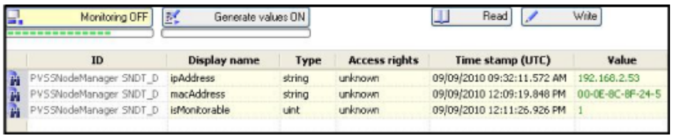
10. In the workbook area, you will see that a view has already been created for the UA server.

11. Drag and drop the required device elements to the view space below.

12. Click the "Read" button at the top of the view space. This will start reading the values of each of these device properties for the selected device as shown below.

13. As an example, you can see the values for the "IP address", "MAC address" and "Is monitorable" device properties in the screenshot below. Since the device is in the monitored status, the value for this property will be listed as 1.

14. Click the "Monitoring ON" button to view or track the changes to these devices. Any changes to these devices or device properties are updated synchronously in the value field.



ID	Display name	Type	Access rights	Time stamp (UTC)	Value
PVSSNodeManager SNDT_D	ipAddress	string	unknown	09/09/2010 09:32:11.572 AM	192.168.2.53
PVSSNodeManager SNDT_D	macAddress	string	unknown	09/09/2010 12:09:19.848 PM	00-0E-8C-8F-24-5
PVSSNodeManager SNDT_D	isMonitorable	uint	unknown	09/09/2010 12:11:26.926 PM	1

15. If the network device containing the IP 192.168.2.53 is set to the non-monitored status in SINEMA Server from the **Admin** > **Device list** page, then this value automatically changes to 0 indicating a non-monitored status for the network device.

16. Similarly, these steps can be used to display other device properties and you will be able to view the data of all the network devices discovered by the SINEMA Server application.

OPC Data Access (DA)

OPC DA is a standard that provides specifications for communicating real-time data from data acquisition devices such as PLCs to display and interface devices such as human machine interfaces (HMI). SINEMA Server supports OPC DA functionality.

Configuring DCOM settings in SINEMA Server

For remote OPC DA access, the DCOM settings need to be configured in SINEMA Server. The information in this section outlines steps for configuring the DCOM settings in SINEMA Server.

Requirements

- Data Execution Prevention (DEP) option settings:

  By default, DEP option is enabled for all programs. If this option is disabled, change the option to "Turn on DEP for essential Windows programs and service only" by selecting the radio button. The DEP tab is part of the "Performance options" window and can be accessed from the "System properties > Advanced" tab. Right click on the My Computer icon and select the "Properties" option to view system properties.

Note

The steps shown for configuring DCOM settings in SINEMA Server apply to the Windows Server 2003R2 operating system.

Note

In Windows XP, it is advisable to disable the Windows firewall temporarily while setting the DCOM configuration and testing the OPC server for remote connectivity. Once connectivity is established, the Windows firewall needs to be enabled again with exceptions to allow OPC server connectivity.

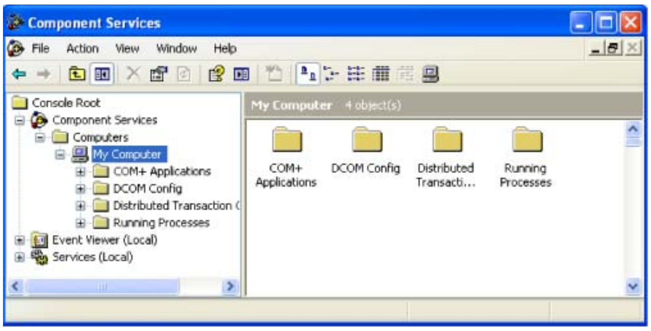
Setting the properties in the DCOM configuration for OPC DA communication

The settings that need to be made in DCOM configuration for OPC DA communication include the following steps:

- Configure default DCOM settings
- Configure OPC server DCOM settings
- Configure OPC server browser DCOM settings
- Restart the system

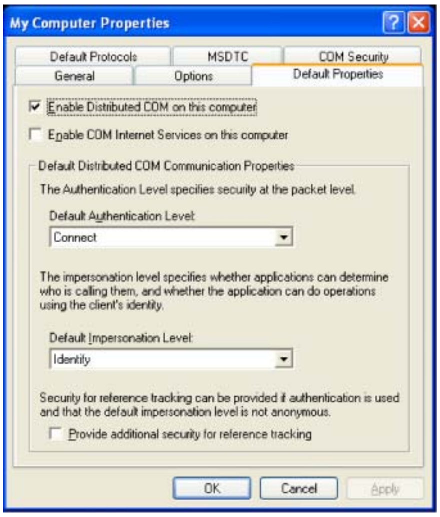
Configure default DCOM settings

1. In Windows, select Start > Run. In the Open list box, type "dcomcnfg" and click OK.
2. The component services window opens containing the folder hierarchy structure.



3. Go to the Component Services, Computers, "My Computer" branch.
4. Right click on "My Computer" and select the "Properties" option to open the "My Computer Properties" window.
5. Enter a short description for your computer and click OK.

6. In the "Default Properties" tab, specify the default authentication level by selecting the option "Connect" from the drop-down list.



☑ Enable Distributed COM on this computer

□ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level: Connect

The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level: Identity

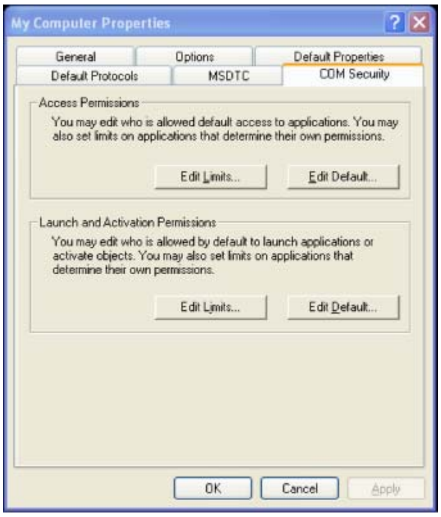
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

□ Provide additional security for reference tracking

7. Select "Identify" in the drop-down list box for the default impersonation level and select OK.

8. In the "Default Protocols" tab in the DCOM protocols section, move "Connection oriented TCP/IP" to the top of list and remove other unused protocols.

9. Next, select the "COM Security" tab. In the "COM Security" tab, go to the "Access Permissions" section.



Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

10. In "Access Permissions", click the "Edit Default" button to open the "Access Permissions" window. Here you select the list of users that will have access to OPC servers and OPC server browsers on the computer.

11. Configure the access permissions depending according to your requirements by selecting any of the following options and click OK.

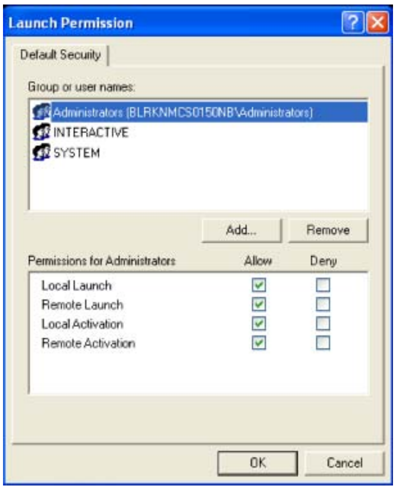
    - To provide access to everyone, add the domain group "Everyone".

    - If both server and client are in same network domain, add the list of users who will access the OPC server. You should also allow local and remote access for these users.

    - To block access to everyone, create a domain group and add the logins that will be allowed to access the OPC server and OPC server browser. Then, add the group to the "Group or user names" list.

12. Make sure that the "SYSTEM" group is listed in the "Group or user names" list and that the "Allow" check box is selected for local access and remote access. If the group has not been added, you can add the group using the "Add" button. Next, click the OK button.

13. In the "Launch and Activation Permissions" section, click the "Edit Default" button to open the "Launch Permission" window. Here you set the list of users that can launch OPC servers and OPC server browsers on this computer.



Group or user names:

- Administrators (BLRKNMCS0150NB\Administrators)
- INTERACTIVE
- SYSTEM

Permissions for Administrators	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

14. Configure the launch permissions by selecting any of the following options and click OK.

    - To provide access to everyone, add the domain group "Everyone".

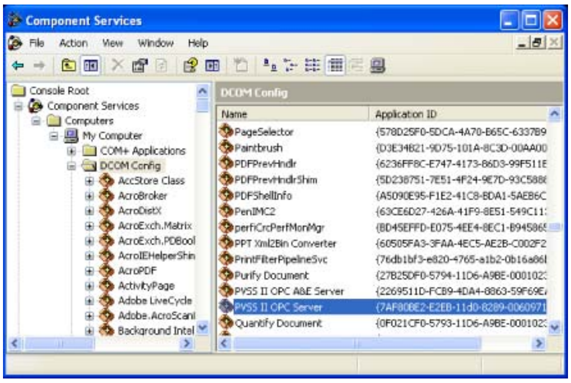
    - If both server and client are in same network domain, add the list of users who will access the OPC server. You should also allow local and remote access for these users.

    - To block access to everyone, create a domain group and add the logins that will be allowed to access the OPC server and OPC server browser. Then, add the group to the "Group or user names" list.

15. Make sure that the "SYSTEM" group is listed in the "Group or user names" list and that the "Allow" check box is selected for local access and remote access. If the group has not been added, you can add the group using the "Add" button. Next, click the OK button.

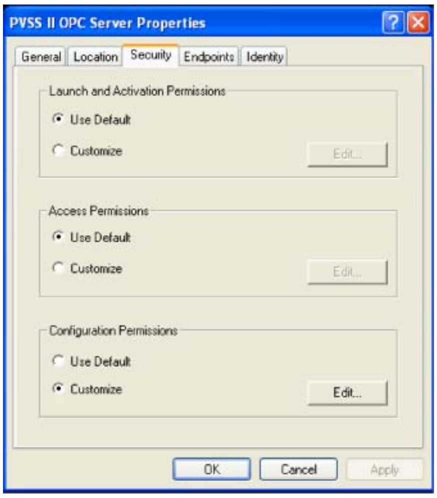
Configure OPC server DCOM settings

1. In the Component Services window, expand My Computer to view the folder structure.
2. Select the DCOM Config folder. The objects it contains are displayed on the right-hand side.



Name	Application ID
PageSelector	{578D25F0-5DCA-4A70-B65C-633789
Paintbrush	{D3E34B21-9D75-101A-8C3D-00AA00
PDFPrevHndlr	{6236FF8C-E747-4173-86D3-99F511E
PDFPrevHndlrShim	{5D238751-7E51-4F24-9E7D-93C588(
PDFShellInfo	{A5090E95-F1E2-41C8-BDA1-5AEB6C
PenIMC2	{63CE6D27-426A-41F9-8E51-549C11:
perfiCrcPerfMonMgr	{BD45EFFD-E075-4EE4-8EC1-B94586!
PPT Xml2Bin Converter	{60505FA3-3FAA-4EC5-AE2B-C002F2
PrintFilterPipelineSvc	{76db1bf3-e820-4765-a1b2-0b16a86I
Purify Document	{27B25DF0-5794-11D6-A9BE-000102:
PVSS II OPC A&E Server	{2269511D-FCB9-4DA4-8863-59F69E/
PVSS II OPC Server	{7AF80BE2-E2EB-11d0-8289-0060971
Quantify Document	{0F021CF0-5793-11D6-A9BE-000102:

3. Select "PVSS II OPC Server" in the list view. Right-click on this object and select Properties.
4. The "PVSS II OPC Server Properties" window is displayed.
5. In the "General" tab, set the authentication level to "Default" by selecting this in the drop-down list.
6. The authentication level will nevertheless change to "Connect" because we set the default connection level to "Connect" earlier.
7. In the "Location" tab, select the "Run application on this computer" check box. Deselect all other check box options and click OK.
8. In the "Security" tab, we recommend that you select "Use Default" for the "Launch and Activation Permissions". If you select "Customize", make sure that suitable OPC server users and/or groups are added.



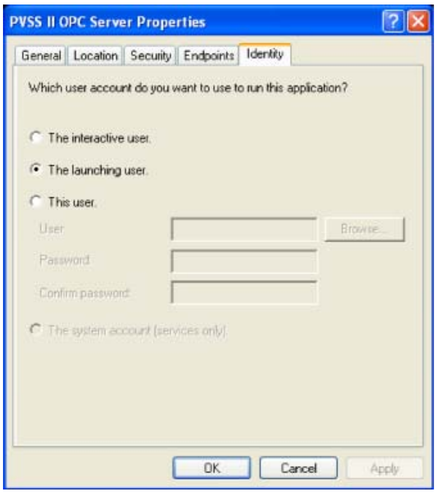
Launch and Activation Permissions
● Use Default
○ Customize

Access Permissions
● Use Default
○ Customize

Configuration Permissions
○ Use Default
● Customize

9. We recommend that you select "Use Default" for the "Access Permissions". If you select "Customize", make sure that suitable OPC server users and/or groups are added.

10. We recommend that you select "Use Default" for the "Configuration Permissions". If you select "Customize", make sure that suitable OPC server users and/or groups are added.
11. After making these settings, click OK.
12. In the "Default Protocols" tab in the DCOM protocols section, move "Connection oriented TCP/IP" to the top of list and remove other unused protocols.
13. In the "Identity" tab, the settings you select depend on the intended use of the OPC server PC. Use the settings shown below for unattended or attended operation.



Which user account do you want to use to run this application?

○ The interactive user.

● The launching user.

○ This user.

User

Password

Confirm password

○ The system account (services only)

– If there are no users configured for the computer on which OPC server is running, we recommend that you select the "This user" option and specify a user name and password. This setting will allow the OPC server to start even if nobody has logged on to the computer.
– This option can be used if somebody has logged on the computer.
– Let us assume, for example, that the user name is "Captain" and the user domain name is "XYZ". If this option is selected and the server is started locally, the user account must have Admin privileges to make OPC server configuration changes.

Configure OPC server browser DCOM settings

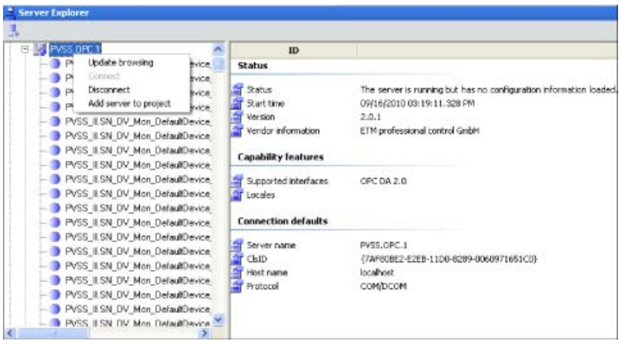
1. In the DCOM Config list view, select the "OpcEnum" object.
2. Right-click on this object and select the "Properties" option.
3. Then, follow the steps 5 to 13 as shown above in the section "Configure OPC server DCOM settings".

Restart the system

1. After working through these steps, restart the system.

Accessing SINEMA Server data using an OPC server (OPC DA)

1. In Windows, click Start > All Programs > SIMATIC > SIMATIC NET > OPC Scout to open the OPC Scout client.
2. In the navigation tree displayed on left hand-side of the screen, expand the local COM server.
3. Then, expand the OPC DA server listed below in the tree hierarchy.
4. The connection to the server is established automatically and the complete list of devices along with the device properties is displayed.



Status

Status	The server is running but has no configuration information loaded.
Start time	09/16/2010 03:19:11.328 PM
Version	2.0.1
Vendor information	ETM professional control GmbH

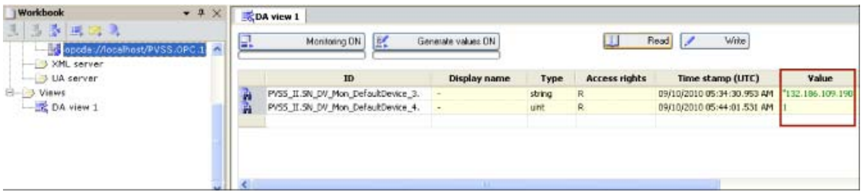
Capability features

Supported interfaces	OPC DA 2.0
Locales	

Connection defaults

Server name	PVSS.OPC.1
ClsID	{7AF80BE2-E2EB-11D0-8289-0060971651C0}
Host name	localhost
Protocol	COM/DCOM

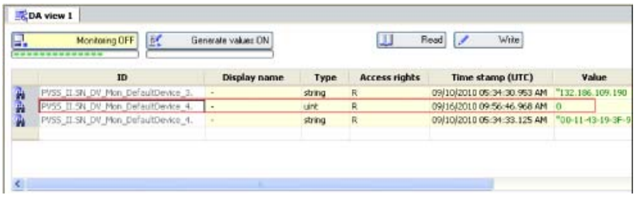
5. The connection status, server capability features and connection defaults are displayed on right-hand side of the Server Explorer window.
6. In the Workbook area, you will see that the "DA view1" has been created for the DA server.
7. Drag the required device elements to the "DA view1" area.
8. Click the "Read" button at the top of the area. This will start reading the values of each of these device properties for the selected device as shown below.
9. As an example, you can see the values displayed for the "IP address", "MAC address" and "Is monitorable" device properties in the screenshot below. Since the device is in the monitored status, the value for this property will be listed as 1.



ID	Display name	Type	Access rights	Time stamp (UTC)	Value
PVSS_II.SN_DV_Mon_DefaultDevice_3.	-	string	R	09/10/2010 05:34:30.953 AM	"132.186.109.190
PVSS_II.SN_DV_Mon_DefaultDevice_4.	-	uint	R	09/10/2010 05:44:01.531 AM	1

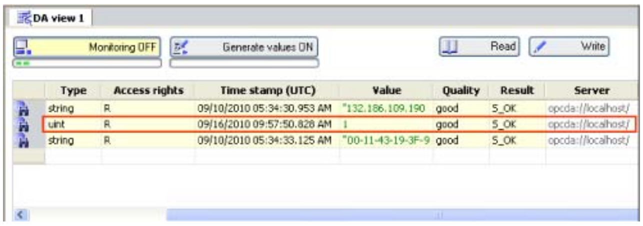
10. Click "Generate values ON" and select the "Read" button to start reading the data from SINEMA Server.
11. Click the "Monitoring ON" button to view or track the changes to these devices. Any changes to these devices or device properties are updated synchronously in the value field.

12. If the network device containing the IP is set to the non-monitored status in SINEMA Server, this value automatically changes to 0 indicating a non-monitored status for the network device.



ID	Display name	Type	Access rights	Time stamp (UTC)	Value
PVSS_II.SN_DV_Mon_DefaultDevice_3.	-	string	R	09/10/2010 05:34:30.953 AM	"132.186.109.190
PVSS_II.SN_DV_Mon_DefaultDevice_4.	-	uint	R	09/16/2010 09:56:46.968 AM	0
PVSS_II.SN_DV_Mon_DefaultDevice_4.	-	string	R	09/10/2010 05:34:33.125 AM	"00-11-43-19-3F-9

13. When the device containing the specific IP is set back to the monitored status in SINEMA Server, you will see that the value switches to 1 indicating the monitored status for the device.



Type	Access rights	Time stamp (UTC)	Value	Quality	Result	Server
string	R	09/10/2010 05:34:30.953 AM	"132.186.109.190	good	S_OK	opcda://localhost/
uint	R	09/16/2010 09:57:50.828 AM	1	good	S_OK	opcda://localhost/
string	R	09/10/2010 05:34:33.125 AM	"00-11-43-19-3F-9	good	S_OK	opcda://localhost/

14. Similarly, these steps can be used to display other device properties and you will be able to view the data of all the network devices discovered by the SINEMA Server application.

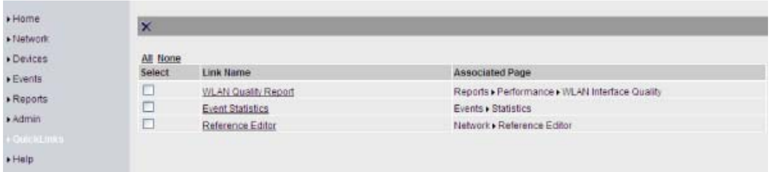
Quick Links 7

Fast access to pages

The **Quick links** menu provides fast access to pages you require often. Instead of working through the usual menus, browse to the required page and then add a quick link to it. The newly added quick link appears in the table view of the Quick links page and contains a select check box, link name and associated page information. The quick link in the table view includes a hyperlink to the relevant page. The associated page column provides the complete path information for the page added as a quick link.

There are user controls on the application pages with which you can add or delete quick links. The "Add quick link" icon along with a text box for the quick link name is available in the second level header on all pages of SINEMA Server application. The "Delete quick link" icon is available on the Quick links page. The icons and their meaning are described below:

Icon	Description
↗	Add quick link
✕	Delete quick link



Select	Link Name	Associated Page
□	WLAN Quality Report	Reports ▸ Performance ▸ WLAN Interface Quality
□	Event Statistics	Events ▸ Statistics
□	Reference Editor	Network ▸ Reference Editor

Detailed information

Apart from using quick links at page level, the SINEMA Server application provides additional options of adding quick links to individual user maps or views, all tabs in the Device details, Reports, User Admin and Network settings pages. This feature allows easy access to specific parts of the pages provided by the application and therefore allows information to be viewed or monitored faster.

To add a quick link to the user map or view, go to the relevant user map or view and select the "Add quick link" icon. The user map or view selected will then be available as a quick link on the quick links page. If the user map is deleted from the User maps page, the hyperlink for the quick link will also be deleted. A tooltip will be displayed to indicate that the quick link is invalid and does not exist. This same applies to quick links for various views.

On the User admin page, user-defined groups exist as separate tabs in addition to the predefined groups. Each tab or group can be added as a quick link. The following points apply to the use of quick links on the user admin page:

1. If the specific group created by the user is deleted, the hyperlink associated with the quick link is also deleted making the quick link invalid.
2. With new users, quick links can be created only if access to the page is allowed by the owner of group. If access is not allowed, the quick link icon is not be displayed in the second level header.
3. If access to view the quick links page is allowed, quick links can be created by the user for specific pages provided the user has access rights for these pages. If quick link is created for the Admin > Device list page, the corresponding quick link name will be listed on the Quick links page. For security reasons, if the administrator or owner of group cancels access to the Admin > Device list page, a quick link created by user will be shown as invalid on the Quick links page.

Quick links can be added for all tabs of the Reports, Device details and Network settings pages. Navigate to the desired tab of the page in the application and select the "Add as quick link" icon to add the tab as a quick link. If a quick link is created for the WLAN interface tab of the Device details page, the corresponding quick link name with the hyperlink along with associated page information is displayed on the Quick links page. If the specific WLAN device is changed to non-monitoring status or if the device is deleted, a quick link added for that particular device will become invalid. You will see that the hyperlink is not displayed for the quick link in the Quick links table view. The quick link will, however, still exist on the Quick links page.

Adding quick links

To add quick links, follow these steps:

1. In SINEMA Server, browse to the page or area for which you want to add a quick link.
2. Type a name for the link in the text box next to the "Add quick links" button on the second level header.
3. Click the "Add quick link" button. The created link appears as an entry in the table view displayed on the Quick links page.

Note

Quick links can be added for individual user maps or views and all tabs of the Device details, Reports, User admin and Network settings pages.

Example

Follow the steps outlined below to add a quick link with the name "Network load report" to view a performance report based on network load:

1. In the navigation bar on the left, click the **Reports > Performance** menu item and then select the WLAN interface quality tab.

   The WLAN interface quality reports for the selected date and time range are displayed.

2. Type "WLAN quality report" in the Quick link text box in the second level header and click the "Add as quick link" icon.

   The "WLAN quality report" link appears as an item in the table view on the **Quick links** page. The associated page navigation path is also listed in one of the columns in the table view. Select the "WLAN quality report" link to access the WLAN interface quality report page directly.

Deleting quick links

Follow the steps below to delete quick links from the list of quick links:

1. Select the "Quick links" menu item in the menu bar on the left-hand side.
2. On the Quick links page, a list of quick links is displayed in the table view.
3. Select the check box for the link you want to delete and click the "Delete" button.
4. The quick link will now be deleted and will disappear from the list of quick links shown on the page.

Help 8

Viewing help information

The **Help** menu is on the left-hand side of the menu bar in the SINEMA Server application. This menu item is listed below the **Quick links** menu.

The help menu provides specific help for each of the pages in the SINEMA Server application. When you click the Help menu, the Topics sub-link is displayed containing a list of help topics. Each help topic corresponds to a page available in SINEMA Server. Click on the topic name to call up the help information. This help information is displayed on the same page in the main window.

For example, the user maps help page provides you with general information about user maps and explains the steps required for various actions within a user map.

FAQs 9

9.1 FAQs

FAQs

- **How many concurrent users can access the SINEMA Server Web interface as client?**

  Ten users can access the SINEMA Server Web interface concurrently.

- **How to view the login page for the SINEMA Server Web interface**

  The SINEMA Server monitor panel loads automatically as part of Windows startup. This panel is responsible for starting SINEMA Server. The monitor panel is available as an icon in the Windows system tray. Right-click on the system tray icon to view the list of options. Enter **http://localhost** in the address bar of the browser, and click "Go" to view the login page for the SINEMA Server Web interface.

- **How many quick links I can add to the menu bar?**

  You can add a maximum of ten links as quick links.

- **How do I print a specific topology view?**

  Click the Printer icon on the Topology view toolbar.

- **How can I change the size of the topology view?**

  Use the Zoom factor drop-down list box on the Topology view toolbar to view the topology in different sizes.

- **How do I change the configuration for the node display in the Topology view?**

  Use the Configure nodes toolbar button in the Topology view to change the node display in the Topology view area.

- **What is the purpose of the Icon view button on the Topology view toolbar?**

  The Icon view button allows you to view the device icons of the network devices that are displayed in the Topology view area. If you activate the icon view, you can view more network devices in the topology view than in the default view. In the Icon view, you can view the IP details such as IP address and MAC address for the devices.

- **Where do I set up the time interval for refreshing the topology view?**

  You can set up the time interval for refreshing the topology view on the UI settings tab (**Admin** > **UI settings**).

- **What is the purpose of user-defined maps?**

  User defined maps are created to monitor and manage a specific group of devices instead of all the devices in the network.

- What is an unresolved device in the topology view?

  In the topology view of a user-defined map, if the displayed device has a connection to a device that is not included in the selected user-defined map or is not associated with a logged-on user, the connection line is displayed with an unknown device (represented by a cloud). In the topology of user-defined maps, these unknown devices are called unresolved devices. There can be unresolved devices in the detailed view and in the icon view.

- Can I change the parameter settings for a network device?

  You can only change the name of a network device, the other parameters cannot be edited.

- How many event reactions can I add for a particular event?

  You can add a maximum of ten event reactions for a particular event.

- What is the purpose of the event acknowledgement functionality in SINEMA Server?

  Acknowledging an event helps you to rectify critical events before they become more serious. This can be achieved by configuring the event reactions. Acknowledge the events for which event reactions have been configured in the application.

- How do I define events in SINEMA Server?

  In SINEMA Server, network events and system events are predefined in the software application. Users do not have the option of defining them manually.

- How do I change the password?

  On the SINEMA Server Web interface menu bar, click the Admin > User administration > Change password tab to change the password.

- How do I split large scan ranges into smaller scan ranges?

  If you know the IP addresses of the devices available in the network, you can add ranges to split large scan ranges into smaller ranges. This helps to reduce the total scan time in the current network.

  You can add a scan range on the Device detection tab (**Admin > Network settings > Device detection** tab), and assign a start IP address and end IP address to split up a scan range.

- Which SNMP security levels are available for SINEMA Server?

  The following SNMP security levels are available for SINEMA Server:

  - noAuthnoPriv: No authentication, no encryption.
  - authNoPriv: Authentication with the MD5 or SHA algorithm, no encryption.
  - authPriv: Authentication with the MD5 or SHA algorithm, encryption with the DES / AES / AES 128 algorithm.
  - Maximal. Authentication with the MD5 or SHA algorithm, encryption with the DES / AES / AES 128 algorithm.

- **How do I apply the configuration settings from one SINEMA Server system to another SINEMA Server system?**

  You can use the Export and Import functionality in SINEMA Server to apply the configuration settings from one SINEMA Server system to another SINEMA Server system. The configuration details are stored in the SINEMA Server database. You can export these configuration details from the database to a configuration file in ASCII file (.dpl) format. For ease of use you can import the configuration settings of an existing SINEMA Server system to another SINEMA Server system that needs to be configured.

- **How can I view the exported SINEMA Server database?**

  The SINEMA Server database is exported in the ASCII format and you can view the file using Microsoft Word.

- **How does SINEMA Server handle the reports when a device is replaced in the network?**

  The reports display only the information belonging to the new device; the data of the old device is not shown. However, the IP address remains the same and a new MAC address is assigned to the new device. If a device is deleted, then the link to its entire history is lost and the reports will not generate any data relating to the deleted device.

- **How can I be sure that SINEMA Server and its related services have started up?**

  SINEMA Server provides a Status monitor panel that is loaded during Windows startup. This panel displays the status of the SINEMA Server application; the loading of its related services is indicated by a progress bar. This also provides options for starting/stopping the SINEMA Server application including options for starting the Web client.

- **Unable to login to SINEMA Server in the Firefox browser after the network cable is disconnected**

  This problem occurs when network cable of the computer running the SINEMA Server application is disconnected. This is because the browser checks whether the "Work offline" is set and assumes it is offline making a login to the SINEMA Server application impossible. To access the application if the network cable is disconnected, deselect the "Work offline" option in the File menu of the Firefox browser. This situation will not occur while working with Internet Explorer.

- **What to do if there are setup errors when you install the SINEMA Server application on drive "D:".**

  Even though you install the SINEMA Server application on drive "D:" drive, only certain SINEMA Server components will be installed in this drive. Other components are nevertheless installed on the Windows volume (drive "C:"). To avoid setup errors, make sure that you have a minimum of 800 MB of free space on drive "C:" even though you have adequate free space on on the drive "D:".

- **Will the SINEMA Server application detect a new device if the existing IP address of a device is changed to a new IP address?**

  In this situation, SINEMA Server will discover the device again with the new IP address during the next scan. This is the case only if the IP address is in the scan range; the old instance of the device with the old IP address will be shown as unreachable. The application ensures that a new instance of monitored device is not created in this case. In SINEMA Server, this monitored device will have the same MAC address as the device whose IP was changed.

- **Database crashes during a forced shut down while SINEMA Server is running**

  If there is a forced shut down while SINEMA Server is running, it is possible that the SINEMA Server database may be corrupted. The application will then not start up properly. The only way to recover from this situation is to reinstall SINEMA Server. To avoid this data loss, we recommend that back up the system periodically. This data can then be retrieved using the restore function.

- **What happens when no reference connections are defined in the reference topology editor**?

  If a user does not define any reference connections but saves a reference, all the devices that are shown in the editor window become part of the reference but do not have any reference connections. As a result, the devices will be displayed as unresolved devices in the monitoring view. The next time you open the Topology editor, the devices are still in the hop layers they were in when you last saved. The application does not recalculate the hop layers based on the actual topology.

Glossary

ARP

The Address Resolution Protocol is used for address resolution. Its task is to find the corresponding network hardware address (MAC address) for a given protocol address.

BOOTP

In computer networking, the Bootstrap Protocol, or BOOTP is a network protocol used by a network client to obtain an IP address from a configuration server.

DCP

Discovery and basic Configuration Protocol is a protocol suitable for obtaining address parameters from PROFINET components.

Discovery

The process by which SINEMA Server scans the network and automatically detects the managed objects in the network.

Dummy devices

Dummy devices are the user-defined devices that do not support any protocol. In SINEMA Server, the dummy devices are not identified automatically by the scan operation.

FTP

File Transfer Protocol is a network protocol for exchanging and manipulating files over a TCP computer network. An FTP client can connect to an FTP server to manipulate files on that server.

HTTP

Hypertext Transfer Protocol is used mainly for communication between Web servers and Web browsers (such as Internet Explorer).

HTTPS

Hypertext Transfer Protocol Secure is a combination of the hypertext transfer protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network Web server.

ICMP

Internet Control Message Protocol is one of the main protocols of the Internet Protocol family. It is used to exchange information and error messages.

IP address

The IP address consists of 4 bytes. Each byte is represented in decimal form and separated from the previous byte by a period. This results in the following structure, where XXX stands for a number between 0 and 255 (dotted decimal notation): XXX.XXX.XXX.XXX

The IP address consists of two parts, the network ID and the host ID. This makes it possible to create different subnets. Depending on the bytes of the IP address used for the network ID and the bytes used for the host ID, the IP address can be assigned to a specific address class:

Address class	Address class identifier	The network ID and the host ID
A	Byte 1 (possible value 1 to 126) (Byte 1 the byte furthest left.)	Byte 2 to byte 4 Possible value for each 0 to 255. 0.0.0 should not be assigned, 255.255.255 is the broadcast address.
B	Byte 1 (possible value 128 to 191) Byte 2 (possible value 0 to 255)	Byte 3 and byte 4 Possible value for each 0 to 255. 0.0. should not be assigned, 255.255 is the broadcast address.
C	Byte 1 (possible value 192 to 223) Byte 2 and byte 3 (possible value for each 0 to 255)	Byte 4 Possible value 1 to 254. 0 should not be assigned, 255 is the broadcast address.
D	Byte 1 (possible value 224 to 239) Multicast addresses	Byte 2 to byte 4 Possible value for each 0 to 255. 0.0.0 should not be assigned. Some multicast addresses have a special meaning, for example 224.0.0.1 All systems of the subnet 224.0.0.2 All routers of the subnet

LLDP

Link Layer Discovery Protocol is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network.

Managed objects

Devices that can be detected automatically by SINEMA Server while scanning the network.

Management station

The management station is the system on which SINEMA Server is running.

MIB

Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol.

MTBF

Mean Time Between Failures is the average time between failures of a device.

MTTR

Mean Time To Recovery is the average time taken by a device to recover from any failure.

NIC

Network Interface Card is a piece of computer hardware used to connect a computer to an Ethernet network.

PING

A test protocol belonging to the Internet Protocol family. This protocol exists on every MS Windows computer under the same name as a console application (command prompt level). With "Ping," you can prompt a reply (sign of life) from an IP network node within a network as long as you know its IP address.

PNIO

PROFINET Input Output allows direct interfacing of distributed field devices via Ethernet. This supports flat communication hierarchies in automation.

Polling

The process of checking the managed devices periodically to know the status of the devices.

PROFIBUS

PROFIBUS is a standard for fieldbus communication in automation technology.

RFC

In computer network engineering, a Request For Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SNMP

Simple Network Management Protocol is a standardized protocol for exchanging network management information.

SNMP community

An SNMP community is a group to which devices and management stations running SNMP belong.

Subnet mask

The subnet mask specifies which parts of an IP address are assigned to the network number. The bits in the IP address whose corresponding bits in the subnet mask have the value "1" are assigned to the network number.

Telnet

Telecommunication **net**work is a network protocol used on the Internet or local area network (LAN) connections.

TFTP

Trivial File Transfer Protocol is a simple protocol for transferring files.

Topology

The topology describes the network structure. It describes how a network (the transmission medium) and the devices or computers are interconnected.

Unmanaged objects

Devices that cannot be detected automatically by SINEMA Server when it scans the network.

Index