

SIMATIC NET

Network management SINEC PNI

Operating Instructions

Preface

1

Installation and startup

2

Operation

3

Troubleshooting

4

Legal information

Warning notice system

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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1	Preface	5
1.1	Intended operational environment.....	7
1.2	Network load due to SINEC PNI	7
1.3	Security recommendations.....	7
2	Installation and startup	9
2.1	System requirements	9
2.2	Installation and startup	10
2.3	Removal	10
2.4	Structure of the user interface.....	11
2.5	Ports.....	15
3	Operation.....	17
3.1	Device list.....	17
3.1.1	Firmware Update.....	20
3.1.2	Device configuration.....	22
3.1.3	Download And Upload	26
3.2	Settings	30
3.3	Device credentials.....	32
4	Troubleshooting	35
4.1	Update of firmware failed	36
	Index.....	39

Preface

Purpose of this software

SINEC PNI (Primary Network Initialization) is used for the detection and initialization of PROFINET devices as well as the basic configuration of SCALANCE, RUGGEDCOM and RTLS devices.

In addition to IP address information, the configurable parameters include PROFINET and PROFIBUS parameters (IE/PB-Link) as well as device credentials.

Purpose of this documentation

This manual supports you in your work with SINEC PNI.

Scope of validity

The information in this document applies to SINEC PNI V1.0 Service Pack 1 Update 1

Trademarks

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

SINEC, SCALANCE, RUGGEDCOM, RTLS

License conditions

Note

Open source software

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

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

OSS_SINEC-PNI_99.pdf

SIMATIC NET glossary

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

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

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

Decommissioning

Note that personal data such as addresses or passwords can also be saved on the computer on which the software is installed.

Decommission the device properly to prevent unauthorized persons from accessing confidential data.

For decommissioning, delete all data from the device.

Ciphers

Note that, for compatibility reasons, SINEC PNI supports the weak encryption methods in addition to the strong ones.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

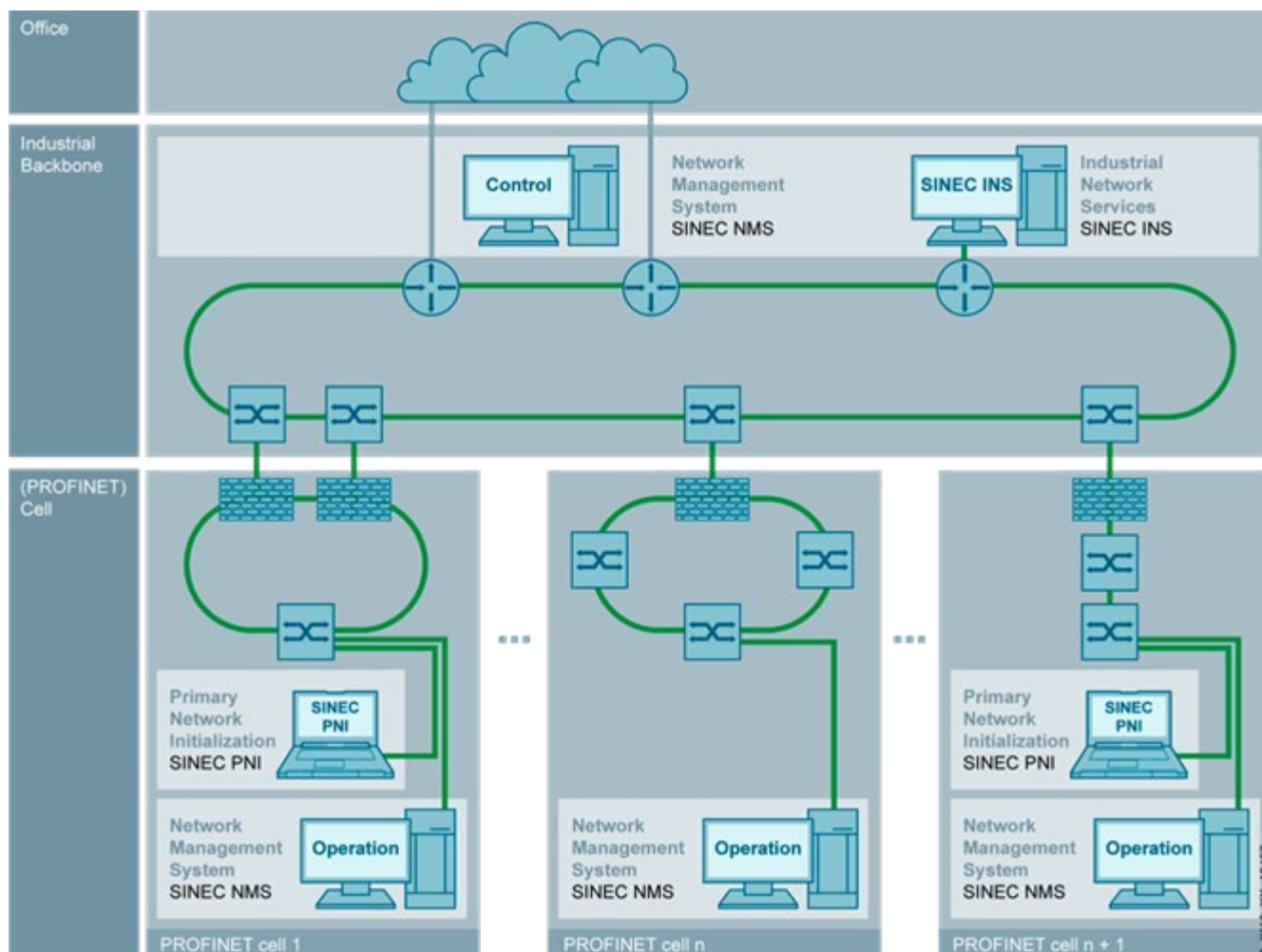
<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

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

1.1 Intended operational environment



1.2 Network load due to SINEC PNI

To initialize and commission devices, SINEC PNI uses part of the data transfer rate available in the network.

This must be taken into account when planning networks in which SINEC PNI will be used.

1.3 Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that this product meets these recommendations and/or other internal security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software you are using up to date. Check regularly for security updates of the product.
You will find information on this at <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).
- Only activate protocols you require for monitoring and administration of the devices.
- Whenever possible, always use the variants of protocols that provide greater security (e.g. SNMPv3).
- Connections over unsecured network areas must be secured by security mechanisms such as SSL VPN.
- Restrict access to SINEC PNI to qualified personnel.

Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC_support_99.pdf" on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/38652101>)

Installation and startup

2.1 System requirements

Hardware requirements

The following minimum requirements apply with respect to the hardware to be used:

- Work memory: 2 GB
- Hard disk space: 1 GB
- Network adapter: 1

Software requirements

The following requirements apply with respect to the operating system to be used:

- Microsoft Windows 7 (Pro / Enterprise) SP1
- Microsoft Windows 10 (Enterprise LTSC) Version 1607
- Microsoft Windows 10 (Enterprise LTSC) Version 1809
- Microsoft Windows 10 (Professional / Enterprise) Version 1903
- Microsoft Windows 10 (Professional / Enterprise) Version 1909
- Microsoft Windows Server 2016 Standard (LTSC) Version 1607
- Microsoft Windows Server 2019 Standard (LTSC) Version 1809

Installation of the following software is required on every operating system. On startup, SINEC PNI checks whether this software is installed. If the software is not installed, you can install it via the SINEC PNI setup:

- PCap driver: WinPcap/Win10Pcap/Npcap (programming interface to record network traffic on Layer 2)
The current Win10Pcap version is installed by SINEC PNI. SINEC PNI is compatible with the following versions:
 - WinPcap: as of 4.13
 - Win10Pcap: as of 10.2-5002
 - Npcap: as of 0.9983If the Npcap driver is already installed, it must be version 0.9983 or higher. If the version is older than 0.9983, SINEC PNI will not function properly.
- Visual C++ Redistributable 2015-2019

Unsupported devices

RUGGEDCOM ROS Non controlled devices are not supported by SINEC PNI.

2.2 Installation and startup

Installation and startup

Extract the ZIP archive of SINEC PNI. You need read and write rights for the folder created.

Click the "SinecPni.exe" file to start SINEC PNI. When SINEC PNI starts, it checks whether the PCap driver and Visual C++ Redistributable are installed; see section System requirements (Page 9). If they are not installed, they can be installed via SINEC PNI.

The "temp" directory, for which you require read and write permissions, is created for the supplied TFTP server.

At the initial start, the "Settings" page opens. On this page, you can configure the settings for the network scan; see section Settings (Page 30).

For speed and resource reasons, it is recommended that you only enable the protocols that are actually required.

Once initial configuration is complete, you can start SINEC PNI via the "SinecPni.exe" file in the unzipped file folder.

There can only be one SINEC PNI instance.

2.3 Removal

To uninstall, delete the unzipped file folder.

2.4 Structure of the user interface

The following figure shows the main operator controls of SINEC PNI. The operator controls in the header are available independent of the selected navigation entry.

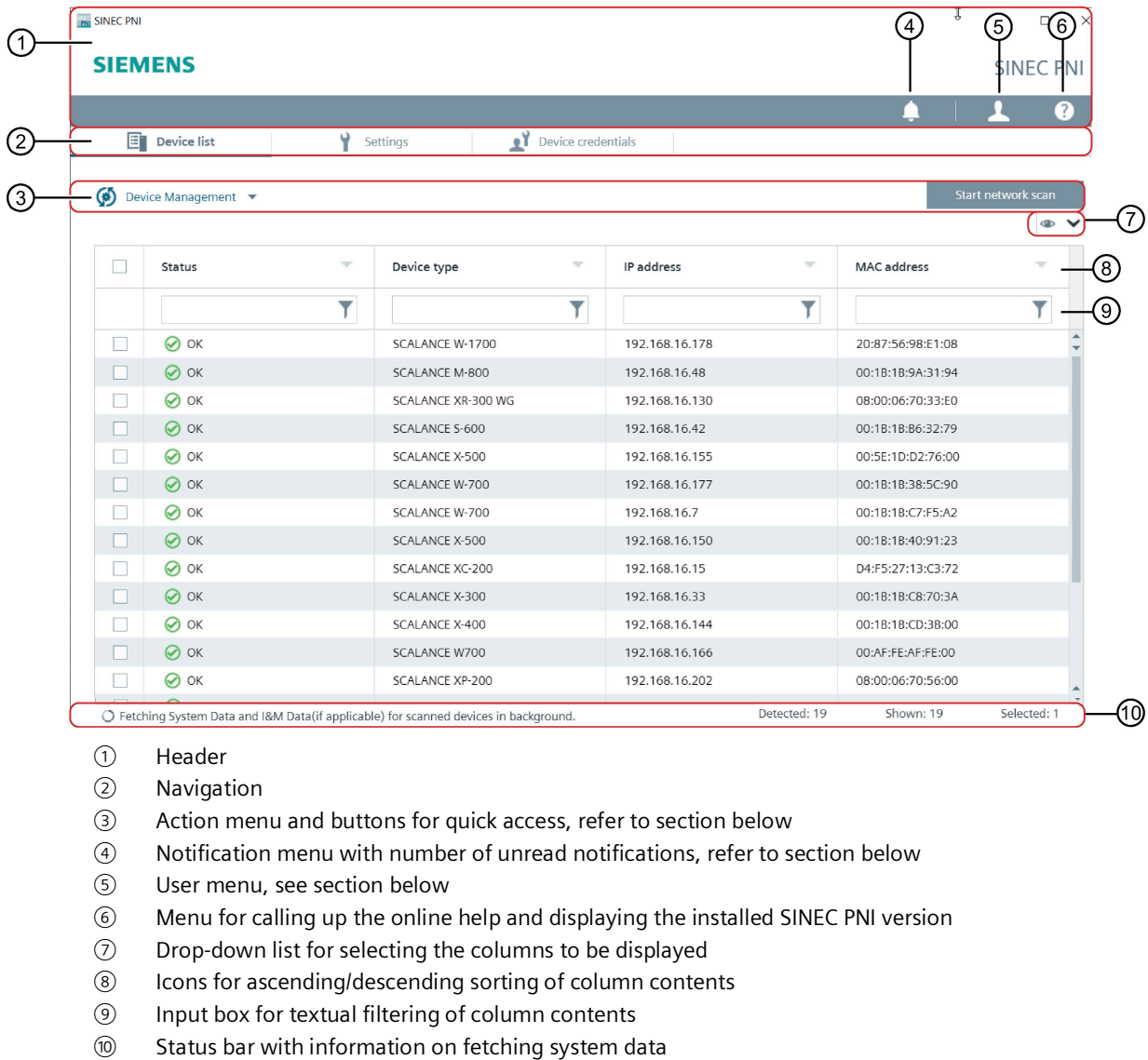


Figure 2-1 User interface of SINEC PNI

Action menu and buttons for quick access

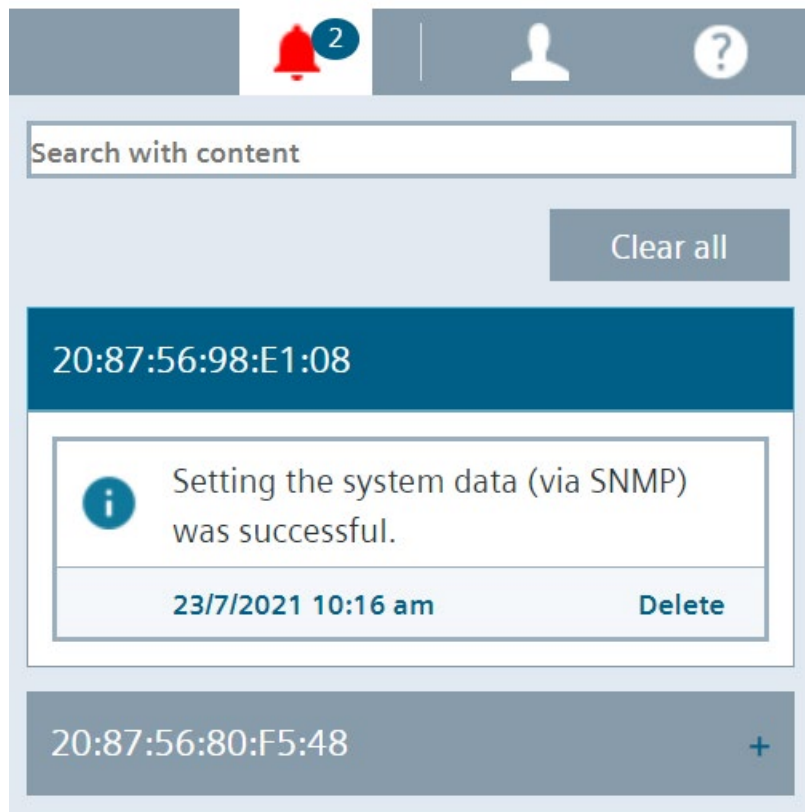
The action menu contains all the functions available on a page. You can use the star icons to define frequently used actions to be displayed next to the Action menu for quick access.

Notification menu

You can use the icon to expand the notification list. The number indicates the unread notifications. The notifications contain warnings, error messages, and notifications that provide information about completed actions. The notifications are grouped by the MAC address of the device. If you click on notifications, details are displayed.

To filter the searched content, enter a search text in the text box and confirm with the <ENTER> key.

You can remove individual notifications from the Notifications menu using the "Delete" button. The "Clear all" button removes all notifications.

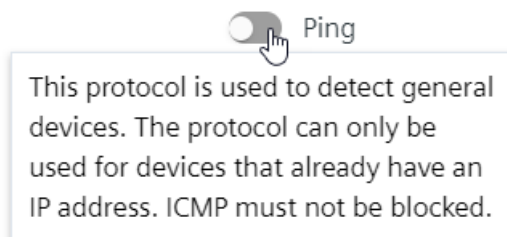


User menu

The user name contains buttons for switching the language. The supported languages are English and German.




Tooltip

If a tooltip is available at the parameter, it appears when you hover over the parameter with the mouse.



Keyboard operation

Some functions can be performed via the mouse or with keyboard shortcuts.

Function		Keyboard shortcut	
Notification menu 		F3	
User menu 	Language	ALT + A	
Help menu 	Online help	F1	
	About SINEC PNI	F11	
Start network scan		F5	
Device list		CTRL + ALT + L	
Settings		CTRL + ALT + S	
Device credentials		CTRL + ALT + C	
Device management	Change device configuration		ALT + C
	Reset device		-
	Open WBM		ALT + O or F2
	Export selection		-
	Device availability	Flash LED	ALT + F
		Ping device	ALT + P
	Firmware update		-
	Restart device		ALT + R
	Download and upload	Download to computer	ALT + D
		Upload to device	ALT + U

Tables

The device list is a tabular summary of the determined device information.


Selecting entries in tables

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

Follow the steps outlined below to select table entries.

- Select individual entry
Click a row in the table. In this way, you select an individual entry and deselect other selected entries.
- Select multiple entries
Select the check box for the first and last entry in the desired table area while holding down the Shift key.
Execution starts with the first selected device.
- Select multiple entries distributed in any way
Click in the table rows of the desired entries. In this way, you select the desired entries and deselect other selected entries.
The configuration is assigned in the order in which the devices are selected in the device list.
- Select all entries of the same page
Select the check box in the header.

Showing/hiding columns

Clicking the eye icon  on the right above the table opens the drop-down list with the available columns. By selecting the check boxes, you can select the columns to be displayed in the table.

Sorting the table

By clicking on a table header, you can sort the table in ascending or descending order according to the values of this column.

Filtering entries

A search text can be entered in the text boxes of the headers in order to filter the content searched for.

2.5 Ports

SINEC PNI uses the following ports for communication with devices. These ports are not blocked for outbound data traffic in the Windows firewall by default. If problems occur during operation of SINEC PNI, check the corresponding ports in the Windows Firewall configuration.

Service	Protocol/ port number	Default port status	Confi- gurable	Authen- tication	En- ryption	Note on the response if the port is blocked
Secure Shell (SSH)	UDP/22	Open	--	✓	✓	Reading and writing configuration on devices not possible
SNMPv1/V2c	UDP/161	Open	--	--	--	Reading and writing configuration on devices not possible
SNMPv3	UDP/161	Open	--	Optional	Optional	Reading and writing configuration on devices not possible
HTTP	TCP/80	Open	✓	✓ ¹⁾	--	Default browser cannot display web pages of the unit
HTTPS	TCP/443	Open	✓	✓	✓	Default browser cannot display web pages of the unit
TFTP	UDP/69	Open	✓	--	--	The following is not possible: <ul style="list-style-type: none"> • Updating firmware on devices • Downloading files to the PC • Uploading files from the device


¹⁾ Only with external HTTP server

Operation

3.1 Device list

On the "Device list" page, you can scan the network for devices using the "Start network scan" button. The scan settings configured on the "Settings" page are used for this; see section Settings (Page 30).

You can configure the devices found via "Device Management", perform LED and ICMP reachability tests (PING), and reset the devices to PROFINET default settings or factory settings.

You can use the  button to show or hide columns in the device list and to change the order of columns.

Operation

The "Device Management" menu contains the following menu entries:

- Change Device Configuration

Calls up the editor for configuring the selected devices; see section Device configuration (Page 22).

- Reset device

Opens a dialog in which you can select one of the following options:

- Reset to PROFINET default settings: Resets the selected PROFINET devices to the respective default settings of the PROFINET IO profile. The settings that are reset depend on the functional scope of the device in question. This function is only available for devices that support the current PROFINET standard.
- Reset to factory settings: Restores the factory settings of the selected devices and removes devices from the device list. After the reset, a new network scan is required.

Note

Loss of the IP address

The IP address is also lost when you reset to PROFINET default settings or to the factory settings of the device. Following this, the device can only be addressed via a serial interface (if present), SINEC PNI (via PN-DCP), DHCP or RCDP.

SCALANCE M800 & S devices

After the factory settings are restored, the device loses its configured IP address and can be accessed again via the factory set IP address 192.168.1.1 (except M826, SC-600). Perform a network scan and adapt the IP address. After the change, you need to perform a network scan again.

The IP address is also lost with M826, SC-600. The device can then only be addressed via a any available serial interface, SINEC PNI (via PN-DCP) or DHCP.

- Open WBM

Opens the WBM (Web Based Management) of the selected devices in the Web browser.

On the "Settings" page, you configure the protocol and the port used to call the WBM.

- Export selection

Exports the selected device list entries to a CSV file.

- Device availability

- Flash LED

Performs an LED flash test (via PN-DCP or via RCDP) on the selected devices, if this is supported by the devices.

The device LEDs flash until you press the "Stop" button.

- Ping device

Performs an ICMP reachability request (PING) for the selected devices.

- **Firmware Update**
Opens the dialog in which you can select one of the following options; refer to section Firmware update (Page 20).
- **Restart Device**
Performs a restart on the selected device.
- **Download And Upload**
You can download or upload the files of the device via this menu; refer to section "Download and upload (Page 26)".
 - For SCALANCE devices, the SNMPdevice credentials (Page 32) are required.
 - For ROS and ROX2 devices, the SSH-device credentials (Page 32) are required.

Properties

Properties such as device status and IP address are shown in the table underneath the buttons for devices found during the network scan.

The following device statuses are possible:

- **OK**
- **Warning**
The device has the IP address 0.0.0.0.
- **Error**
There is an IP/MAC address or name conflict with another device.

3.1.1 Firmware Update

You can update firmware versions on the devices via the dialog. Correct device credentials are required to load the firmware onto the device.

The settings depend on the selected device family.

The total path length of the destination folder, including the subfolder and the file name (with file extension) can be no more than 255 characters. For system reasons, some devices only support a maximum of 32 characters.

Settings with SCALANCE

Specify whether you are transferring the firmware file from a supplied or an external TFTP server to the device.

- Settings for the supplied TFTP server
 - Select NIC IP address

When there are multiple IP addresses, select the IP address of the network adapter (NIC) via which the transfer takes place.
 - Firmware file path

Navigate to the directory in which the *.sfw / *.lad firmware file is stored.
 - Port number

Enter the port number that is used for the transfer.
- Settings for the external TFTP server
 - External server path

Enter the URL, e.g. :192.168.1.10\folder\SCALANCEX400.sfw
 - Port number

Enter the port number that is used for the transfer.
- Firmware update

Click on the button to load the firmware to the device. A dialog with a confirmation prompt opens. After confirmation, the status dialog is called. This dialog shows the status of the transfer, the IP address and the MAC address.

Settings with RUGGEDCOM (ROS)

- File path

Navigate to the directory in which the destination file is stored.

- Destination name

Enter the name of the destination file.

- main.bin – The firmware image of the RUGGEDCOM ROS main application
- boot.bin – Bootloader firmware image
- fpga.xsvf – The binary FPGA firmware image

- Firmware update

Select the file that is loaded to the device and click the "Firmware Update" button. To remove the selected file, click the "Remove Selected" button.

If no file is selected, all files are transferred.

A dialog with a confirmation prompt opens. After confirmation, the status dialog is called. This dialog shows the status of the transfer, the IP address and the MAC address.

Settings with RFID

- Firmware file path

Navigate to the directory in which the *.sfw firmware file is stored.

- Firmware update

Note that you as "User" can only perform a firmware update if the communications module is in the "Ready" status.

Click on the button to load the firmware to the device. A dialog with a confirmation prompt opens. After confirmation, the status dialog is called. This dialog shows the status of the transfer, the IP address and the MAC address.

Settings with RUGGEDCOM (ROX)

Specify whether you transfer the firmware file from a supplied or an external HTTP server to the device.

Settings for the supplied HTTP server

- Select NIC IP address

When there are multiple IP addresses, select the IP address of the network adapter (NIC) via which the transfer takes place.

- Firmware file path

Navigate to the directory in which the *.zip firmware file is stored.

Once the zip file is selected, an attempt is made to determine the destination ROX version from the firmware file. If this does not succeed, you must enter the destination ROX version.

- Target ROX version

The format depends on the firmware version currently used on the device.

- Firmware version < 2.14.0

The file names have the form rrX.Y.Z.zip, where X stands for the main version number, Y for the intermediate version number and Z for the patch number, e.g. rr2.14 .0.

Enter the version in the format 'rrX.Y.Z'.

- Firmware version > = 2.14.0

Enter the following: "image.tar.bz2".

- Port number

Enter the port number that is used for the transfer.

Settings for the external HTTP server

- External server path

The setting depends on the firmware version currently used on the device.

- Firmware version < 2.14.0

http://(hostname)/(directory where the destination file is stored).

- Firmware version > = 2.14.0

http://(hostname)/(directory where image.tar.bz2 is stored)

- Target ROX version (only necessary for ROX version < 2.1.4)

The file names have the form rrX.Y.Z.zip, where X stands for the main version number, Y for the intermediate version number and Z for the patch number, e.g. rr2.14 .0.

Enter the version in the format 'rrX.Y.Z' or enter 'current' to update to the latest available firmware version on the upgrade server.

Port number

Enter the port number that is used for the transfer.

Firmware update

Click on the button to load the firmware to the device. A dialog with a confirmation prompt opens. After confirmation, the status dialog is called. This dialog shows the status of the transfer, the IP address and the MAC address.

3.1.2 Device configuration

The "Device configuration" window opens after you select one or more devices from the device list and then select the "Configure device" entry in the "Device Management" menu.

After the "Device configuration" is opened, SINEC PNI attempts to read out the data from the device and shows this with the "Spinner Icon".

Afterwards, you can configure the parameters in the tabs described below. The following buttons are available to load the changed parameters to the device:

- Load all

The parameters of all tabs are loaded to the device.

- Load

Only the parameters of the currently open tab are loaded to the device.

Changed parameters of a tab are retained after switching to another tab.

To access the devices, SINEC PNI uses the HTTPS/SSH and SNMPv1/v2c logon data set in the factory. If authentication at a device is not possible with this login data, SINEC PNI uses the login data configured on the "Device credentials" page; see section Device credentials (Page 32).

If SNMPv3 is to be used for reading and writing values, the data to be used for this must be specified on the "Device credentials" page.

IP configuration

In this tab, the following IP address parameters can be configured for the selected devices:

- IP address

IPv4 address of the device.

If you have selected multiple devices in the device list, you can specify the first IP address of an IP address range in the "Start IP address" input box, which is assigned to the selected devices during loading.

The device selected first receives the start IP address as IP address.

At most, the IP address range reaches the end of the fourth octet of the specified IP address. If the "DHCP" option is enabled, the parameter cannot be configured.

Note

IP address bulk configuration

After the IP bulk configuration of devices with the same IP address, the order of the IP addresses shown in the device list changes after the scan process.

With RUGGEDCOM ROS devices, the IP addresses may not be assigned in the order in which the devices were selected in the device list. It depends on which device responds first.

- Subnet mask

Subnet mask of the device.

If the "DHCP" option is enabled, the parameter cannot be configured.

- Use router

When this check box is selected, the device uses a router to address devices in a different subnet. An IPv4 address can be specified for the router to be used.

If the "DHCP" option is enabled, the parameter cannot be configured.

- DHCP

If this option is enabled, the IP address configuration of the device is performed by a DHCP server. DHCP mode defines the parameter based on which the IP address for the device is reserved by the DHCP server.

- MAC address

The IP address is reserved by the DHCP server based on the MAC address of the device.

- Client ID

The IP address is reserved by the DHCP server based on the specified client ID of the device. If you have selected multiple devices in the device list, you can specify a number in the Counter field in addition to the client ID. This number is used as a suffix to the client ID and assigned to the first device during loading. The counter is incremented by 1 for each additional device.

- Device name

The IP address is reserved by the DHCP server based on the device name.

If this option is set together with other data on the device, setting this data can fail if the device does not receive an IP address from the DHCP server in time.

After assignment via DHCP, a new network scan is necessary to display the addresses currently distributed by the DHCP server for the device.

System

In this tab, the following system parameters can be configured for the selected devices:

- System name

Description of the device. If you have selected multiple devices in the device list, you can select one of the following values from the drop-down list:

- Sequence: Enter a number that is used as a suffix to the system name and assigned to the first device during loading. The counter is incremented by 1 for each additional device.
- Last octet of IP address: The number of the last IP octet that the IP address of the respective device has is used as suffix to the system name.

- System location

Location for the device, e.g. a room number.

- System contact

Name of a contact person who is responsible for managing the device.

PROFINET

In this tab, the following PROFINET parameters can be configured for the selected devices:

- PROFINET device name
PROFINET device name that can be specified for the device. If you have selected multiple devices in the device list, you can select one of the following values from the drop-down list:
 - Sequence: Enter a number that is used as a suffix to the PROFINET device name and assigned to the first device during loading. The counter is incremented by 1 for each additional device.
 - Last octet of IP address: The number of the last IP octet that the IP address of the respective device has is used as suffix to the PROFINET device name.
- Converted name
PROFINET device name that is generated by SINEC PNI from the specified name if it does not comply to the rules of IEC 61158-6-10. In this case, the converted device name is loaded to the device.
- Plant designation
Unique designation of the device within the plant.
- Location identifier
Unique designation of the device location.
- Installation date
Date on which the device was installed.
- Additional information
Entry of additional information.

Device credentials

The password of an existing user can be changed in this tab.

- User name
User name for which the password is to be changed.
- Current password
Password currently used by the user to log onto the device. The display of the password in plain text can be enabled and disabled using the button next to the text box.
- New password
New password to be used by the user to log onto the device. The display of the password in plain text can be enabled and disabled using the button next to the input box.

3.1 Device list

- Confirm password

Confirmation of the entered password. Both password entries must match, otherwise a message is displayed. The display of the password in plain text can be enabled and disabled using the button next to the input box.

Note

Device credentials

The devices apply the login data configured on the "Device credentials" page. If authentication at a device is not possible with this login data, you can adapt the login data here.

PROFIBUS

You can configure PROFIBUS parameters for IE/PB-Link devices in this tab.

RTLS

In this tab, you can configure the IP address of the Locating Manager server.

3.1.3 Download And Upload

After you have selected one or more devices from the device list, you can select the "Download And Upload" entry in the "Device Management" menu to upload and download files.

The total path length of the destination folder, including the subfolder and the file name (with file extension) can be no more than 255 characters. For system reasons, some devices only support a maximum of 32 characters. In the case of very long folder names or deeply nested folder structures, files can no longer be renamed, edited or moved.

Download to computer

When you click on "Download to computer", the "Download" dialog opens with the following options:

- Device family

The scope of the file list depends on this.

- External or internal TFTP server (only available with SCALANCE)

Specify whether you transfer the files to a supplied or an external TFTP server.

Settings for the supplied TFTP server

- Select NIC IP address

When there are multiple IP addresses, select the IP address of the network adapter (NIC) via which the transfer takes place.

- Port number

Enter the port number that is used for the transfer.

- Destination folder

Specify the destination folder in which the file is stored.

Settings for the external TFTP server

- External server path

Specify the directory in which the files are stored. The specification is: IP address\

- Port number

Enter the port number that is used for the transfer.

- Folder/File name

The selected option is added to the file name, separated by an underscore (_). The file name then has the following structure:

<Option>_<File> e.g. 192.168.16.1_config.conf

There is a setting "Create subfolder" with the supplied TFTP server. If the setting is enabled, the selected option is used as the name for the subfolder and the file name is not extended.

If the option cannot be retrieved, "Unknown" is used as name.

If there is already a file with the same name in the destination folder, the file name is extended by the suffix "(1)". This also applies to the name of the subfolder.

With the external TFTP server, this depends on the settings of the TFTP server. If the setting is not supported, the existing file is overwritten and the file name is shortened if the generated file name exceeds the character limit.

The name of the subfolder and the file name depend on the following options:

- IP address
- MAC address
- System name
- PROFINET device name (only available for SCALANCE)

If the PROFINET device names are empty or the system names are the same for multiple selected devices, the file is overwritten.

- Add date and time

The date and time are appended to the file name, separated by an underscore (_).

- File list

The scope depends on the selected device family.

- "Close" button

Closes the dialog.

- "Download" button

Click on the button to download the desired file. The status dialog opens. This dialog shows the status of the transfer, the IP address and the MAC address.

After all downloads are complete, you can either close the dialog or jump directly to the destination folder with the "Open folder" button.

Upload to device

Via the dialog, you can restore a previously backed up configuration, for example. The device takes on the configuration from the selected file and continues working with these settings. All settings made up to this point that have not been saved in a file are lost.

Setting with SCALANCE

- External or internal TFTP server

Specify whether you transfer the files to a supplied or an external TFTP server.

Settings for the supplied TFTP server

- Select NIC IP address

When there are multiple IP addresses, select the IP address of the network adapter (NIC) via which the transfer takes place.

- Config File Path

Navigate to the directory in which the configuration file is stored.

- Port number

Enter the port number that is used for the transfer.

Settings for the external TFTP server

- File path

Specify the directory in which the file is stored.

The specification is: IP address\directory\file e.g.
192.168.16.1\folder\config_Scalance_700.conf

- Port number

Enter the port number that is used for the transfer.

- "Close" button

Closes the dialog.

- "Upload" button

Click on the button to load the configuration file to the device. The status dialog opens. This dialog shows the status of the transfer, the IP address and the MAC address.

The user sees the "Restart pending" message in the status dialog for devices for which the "Restore" was successful but which have not been restarted.

Settings with RUGGEDCOM (ROS)

- Config File Path

Specify the directory in which the file is stored.

- Banner File Path

Select the bannert.txt to be uploaded.

- "Close" button

Closes the dialog.

- "Upload" button

Click on the button to load the configuration file to the device. The status dialog opens. This dialog shows the status of the transfer, the IP address and the MAC address.

Status dialog

The following statuses are possible:

- In progress
- Done

The file was successfully downloaded.

- Connection lost
- Not supported

The selected device is not supported.

- Invalid login information (only with RUGGEDCOM ROS / ROX)
- Login error
- Restart pending

Device must be restarted. If no restart is performed and you execute another action, the status is overwritten.

3.2 Settings

The "Settings" page is displayed after SINEC PNI is started for the first time. On this page, you make the settings that are used for the network scan. Before configuring these settings, make sure that the following requirements have been met:

- The network adapter to be used is active.
- An IP address is assigned to the network adapter to be used.
- The software required for SINEC PNI is installed, see section System requirements (Page 9).

The following parameters are available:

Network adapter

Network adapter used for the network scan.

Note

Do not change the network adapter configuration during runtime of SINEC PNI

The network adapter used must not be disabled in the operating system or changed in its configuration during runtime of SINEC PNI.

Restart of SINEC PNI

Values configured on this page are reset after every restart of SINEC PNI. This does not include the setting of the network adapter.

Multiple network adapters

The ICMP reachability request (PING) goes over all network adapters.

Discovery

Finding configurable devices in the network.

- PROFINET devices (DCP)

Protocol DCP (Discovery Configuration Protocol) for detecting PROFINET devices.

- Fetch additional information (not recommended for S7-1200 V2.2 CPUs)

When you select this check box, I&M data (e.g. article number, firmware version and serial number) of detected devices is read out in addition. The detection of I&M data may take some time during the network scan. In addition, I&M data (e.g. plant designation and location designation) can be edited in the device configuration dialog if the check box is selected.

- RUGGEDCOM ROS devices (RCDP)

Protocol RCDP (RUGGEDCOM Discovery Protocol) for detecting RUGGEDCOM ROS devices.

- RTLS

For detecting RTLS devices.

- Ping

Protocol ICMP echo for reachability request of devices in the IP address range configured below.

In addition, the Timeout and Retries parameters can be configured.

Without device selection, you can only open the WBM on the device, but not configure the device. Only use this protocol if the devices cannot be reached via any of the other protocols.

With device selection, you can also configure the device. The following devices are available for selection:

- SCALANCE devices

Protocol ICMP echo for detecting SCALANCE devices.

- RUGGEDCOM ROS devices

Protocol ROS ICMP for detecting RUGGEDCOM ROS devices.

- RUGGEDCOM ROX2 & WIN devices

Protocols ICMP echo and SSH for detecting RUGGEDCOM ROX2 and WIN devices.

- Timeout

Specification of time in seconds after which an ICMP reachability request (PING) is considered failed.

- Retries

Number of retries for ICMP reachability requests (PING) after a device has not responded to the first ICMP request.

- IP address ranges
IP address ranges in which devices will be searched for. The IP address ranges can be specified using the following notations.

192.168.11.12 - 192.168.11.120

172.16.2.2

192.168.3.0/24

192.168.6.34 - *

Multiple entries are separated by commas (,) or semicolons (;). The duration of the network scan depends on the number of devices to be detected.

- Import IP address ranges

Imports the IP address ranges that are defined in a csv or txt file.

Multiple entries are separated by commas (,) or semicolons (;). The duration of the network scan depends on the number of devices to be detected.

Example: 192.168.16.50,192.168.16.52;192.168.1.1 - 192.168.1.20

- Open WBM

Protocol and port used to call the WBM of devices in the Web browser.

After the settings specified above have been configured, you can perform network scans on the "Device list" page; see section Device list (Page 17).

3.3 Device credentials

Note

Restart of SINEC PNI

Values configured on this page are reset after every restart of SINEC PNI.

To access the devices, SINEC PNI uses the HTTPS/SSH and SNMPv1/v2c logon data set in the factory. If authentication at a device is not possible with this login data, SINEC PNI uses the login data configured on the "Device credentials" page. If SNMPv3 is to be used for reading and writing values, the data to be used for this must be specified on this page.

- User name

User name with which SINEC PNI logs onto the device. The user name is required to create new users on devices.

Value used by default: admin

- Password

Password with which SINEC PNI logs onto the device. The password is required to create new users on devices.

Value used by default: admin

- SNMP version

Selection of the SNMP version whose login data you want to specify.

- Read SNMPv1/v2c community string
Password used by SINEC PNI for read SNMPv1/v2c access to devices.
Value used by default: public
- Read/write SNMPv1/v2c community string
Password used by SINEC PNI for read and write SNMPv1/v2c access to devices.
Value used by default: private
- SNMPv3 user name
User name used by SINEC PNI for read and write SNMPv3 access to devices.
- SNMPv3 authentication
Selection of the hash algorithm and password for authenticating the used SNMPv3 user.
- SNMPv3 encryption
Selection of the encryption algorithm and password for encrypting SNMPv3 communication.

Troubleshooting

Setting of parameters fails

When the IP address is set together with other parameters on the device, setting of these parameters can fail if the device cannot be reached with the new IP address in time. Configure the parameters separately from the IP address in this case.

When the system name is configured together with the PROFINET device name on the device, setting of these parameters can fail if the device cannot be reached in time. Configure the system name separately from the PROFINET device name in this case.

SINEC PNI can no longer be started

If error messages such as "The action cannot be performed. Please restart the application." or "An unexpected error occurred." appear during the execution of SINEC PNI, system files of SINEC PNI may be corrupt. Restart SINEC PNI in this case. If SINEC PNI can still not be started afterward, download SINEC PNI from the associated Siemens website again and use this SINEC PNI version immediately.

RUGGEDCOM ROX2: Same/lower firmware version

If the error message "No differences were detected in the target version. Nothing to update." appears after the firmware is updated, this can also mean that the device cannot establish a connection to the server. A firmware downgrade for RUGGEDCOM ROX2 devices is not supported. As of firmware version $\geq 2.14.0$, the error message "File transfer is unsuccessful" is displayed instead.

RUGGEDCOM ROS: IP address bulk configuration

In the IP bulk configuration of devices with the same IP address, the order of the IP addresses shown in the device list changes after the scan process.

With RUGGEDCOM ROS devices, the IP addresses may not be assigned in the order in which the devices were selected in the device list. It depends on which device responds first.

RUGGEDCOM ROS: After the banner.txt is imported, ssh fails

The size range of the banner file: $< 4 \text{ KB} \leq 8 \text{ KB}$.

After uploading a file with this size range, access via SSH is no longer possible. Load Telnet and an empty version of the banner.txt file to the device to replace the existing file.

4.1 Update of firmware failed

Protection from brute force attacks on devices

If the device credentials stored in SINEC PNI, e.g. for SNMP or HTTPS/SSH, do not match the device and SINEC PNI attempts to access the device using them, the affected user account or the IP address is blocked by the PNI host for a specific period after several failed login attempts. After this period has expired, the device can be accessed again.

The number of failed login attempts after which the user account is locked is generally preset to 10 via HTTPS/SSH and 3 with SNMP.

4.1 Update of firmware failed

If the firmware update fails, it may be due to several reasons.

Firmware file

- The firmware file is not valid.
- The configured folder structure is incorrect or invalid.
Check if the folder exists. Adapt the configuration accordingly.
- There is no firmware file in the folder
Copy the appropriate firmware file into the folder.

Device

Device is not accessible.

- The IP address has changed.
Use the PING function to check whether the device is accessible.
Perform a network scan.
- Cable break, network cable pulled
Check the cable connection
- Network problems
The device is accessible, but the firmware could not be transferred in full due to low bandwidth.
Try again later. If the problem persists, contact the network administrator.
- Netconf lock
Netconf lock is activated in the device.

SNMP

Access using SNMP is not possible:

- The stored device credentials for SNMP do not match the device.
Adapt the device credentials.
- SNMP is disabled or write-protected on the device.
Check the SNMP configuration on the device.
- Access via SNMP is prevented by a firewall on the device.
Configure an appropriate firewall rule on the device.

TFTP/HTTP server

Communication between the device and TFTP/HTTP server is not possible:

- The port configured in SINEC PNI and the port of the external TFTP/HTTP server are different.
- No firewall rule is configured on the PC for the TFTP/HTTP port.
Configure an appropriate firewall rule on the PC.
- The external TFTP/HTTP server has not started.
- The address of the TFTP/HTTP server is not correct.
- Access via TFTP/HTTP is prevented by a firewall on the device.
Configure an appropriate firewall rule on the device.

SSH

Access via SSH is not possible:

- The stored device credentials for SSH do not match the device.
Adapt the device credentials.
- SINEC PNI does not support a TLS version < 1.2
Check the TLS version used on the device.
- Access via SSH is prevented by a firewall on the device.
Configure an appropriate firewall rule on the device.

Index

G

Glossary, 6

S

Service & Support, 8

SIMATIC NET glossary, 6

T

Training, 8