SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE S615

Getting Started

01/2019

C79000-G8976-C390-03

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.

Siemens AG
Global Services Information Technology
80200 MÜNCHEN
GERMANY

C79000-G8976-C390-03
℗ 01/2019 Subject to change

Preface

Purpose

The configuration of the SCALANCE S615 is shown by means of examples.

IP settings for the examples

Note

The IP settings used in the examples were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

General naming conventions

The designation . . .	stands for . . .
SCT	Security Configuration Tool
PST	Primary Setup Tool
Device	M87x M81x M826 S615
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M804PB	SCALANCE M804PB
S615	SCALANCE S615
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2 SCALANCE M804PB
SINEMA RC	SINEMA Remote Connect

Further documentation

- Operating instructions

  These documents contain information on installing and connecting the products and on approvals for the products. The configuration and the integration of the devices in a network are not described in these instructions.

  – SCALANCE M874, M876

    Entry ID: 74518712
    (https://support.industry.siemens.com/cs/ww/de/view/109475909/en)

  – SCALANCE M812, M816

    Entry ID: 90316607
    (https://support.industry.siemens.com/cs/ww/de/view/90316607/en)

  – SCALANCE M804PB:

    Entry ID: 109759601
    (https://support.industry.siemens.com/cs/ww/en/view/109759601)

  – SCALANCE M826:

    Entry ID: 99450800
    (https://support.industry.siemens.com/cs/ww/de/view/99450800/en)

  – SCALANCE S615:

    Entry ID: 109475909
    (https://support.industry.siemens.com/cs/ww/de/view/109475909/en)

- "Web based Management" configuration manual

  This document is intended to provide you with the information you require to commission and configure devices using the Web Based Management.

  – SCALANCE M-800:

    Entry ID: 109751635
    (https://support.industry.siemens.com/cs/ww/de/view/109751635/en)

  – SCALANCE S615:

    Entry ID: 109751632
    (https://support.industry.siemens.com/cs/ww/de/view/109751632/en)

- Configuration manual Command Line Interface

  This document contains the CLI commands supported by the devices.

  – SCALANCE M-800

    Entry ID: 109751634
    (https://support.industry.siemens.com/cs/ww/de/view/109751634/en)

  – SCALANCE S615

    Entry ID: 109751633
    (https://support.industry.siemens.com/cs/ww/de/view/109751633/en)

- Industrial Ethernet Security – Basics and Application

  This document contains information about working with the SCT (Security Configuration Tool).

  Entry ID: 56577508 (https://support.industry.siemens.com/cs/ww/de/view/56577508/en)

- SIMATIC NET Industrial Ethernet Network manual

  This document contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

  Entry ID: 27069465 (https://support.industry.siemens.com/cs/ww/de/view/27069465/en)

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- using the search function:

  Link to Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps)

  Enter the entry ID of the relevant manual or the article number of the device as the search term.

- In the navigation panel on the left hand side in the area "Industrial Communication":

  Link to the area "Industrial Communication" (https://support.industry.siemens.com/cs/ww/en/ps/15247/man)

  Go to the required product group and make the following settings:
  "Entry list" tab, Entry type "manual"

Training, Service & Support

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

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary on the Internet at the following address:

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

Security information

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

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 customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

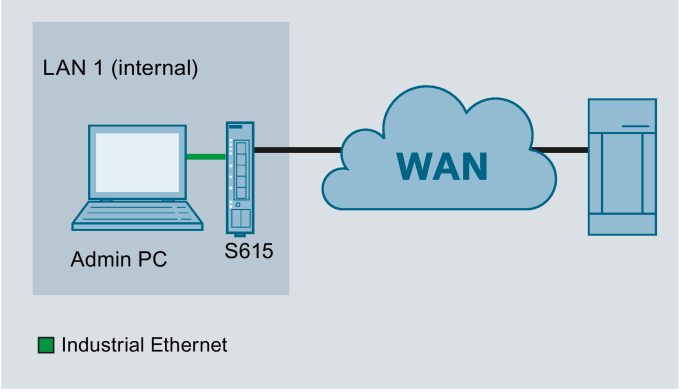
Table of contents

Connecting SCALANCE S615 to the WAN 1

1.1 Procedure in principle

In this example the SCALANCE S615 that is in the factory settings status is assigned an IP address. Following this, the device will be configured using Web Based Management (WBM). Access to the WAN via the Ethernet interface P5 of the S615 will be connected.

Structure



Required devices/components

- 1 x S615 (additional option: a suitably installed standard rail with fittings)
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuring the S615
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Settings used

For the configuration example, the devices are given the following IP address settings:

		Interface	IP address
LAN1	S615	LAN port P1 (vlan1)	192.168.100.1 255.255.255.0
		WAN port P5 (vlan2)	192.168.50.1 255.255.255.0
	PC1	LAN port	192.168.100.20 255.255.255.0 Gateway: IP address vlan1

Note

The IP settings used in the example were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

Steps in configuration

1. Setting up SCALANCE S615 and network (Page 11)
2. Launching Web Based Management (Page 12)
3. Logging in to Web Based Management (Page 15)
4. Changing the IP settings of the SCALANCE S615 (Page 17)
5. Configuring SCALANCE S615
   - Specifying device information (Page 19)
   - Setting the time (Page 20)
   - Creating IP subnet (Page 22)

1.2 Setting up SCALANCE S615 and network

Note

Familiarize yourself with the security instructions before you commission the device. You will find the security instructions in the operating instructions.

Procedure

1. First unpack the S615 and check that it is undamaged.
2. Fit the power supply.

WARNING

Use safety extra-low voltage only

The SCALANCE S615 is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/VDE0805 can be connected to the power supply terminals.

The power supply unit for the SCALANCE S615 power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

3. Wire up the S615, see Setup (Page 9).
4. Connect the device to the local network via the Ethernet ports.
5. Turn the device on. After connecting up, the fault LED (F) is lit red.
6. Now, turn on the PC.

1.3 Launching Web Based Management

In the factory settings, the SCALANCE S615 can be reached at the following IP address:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

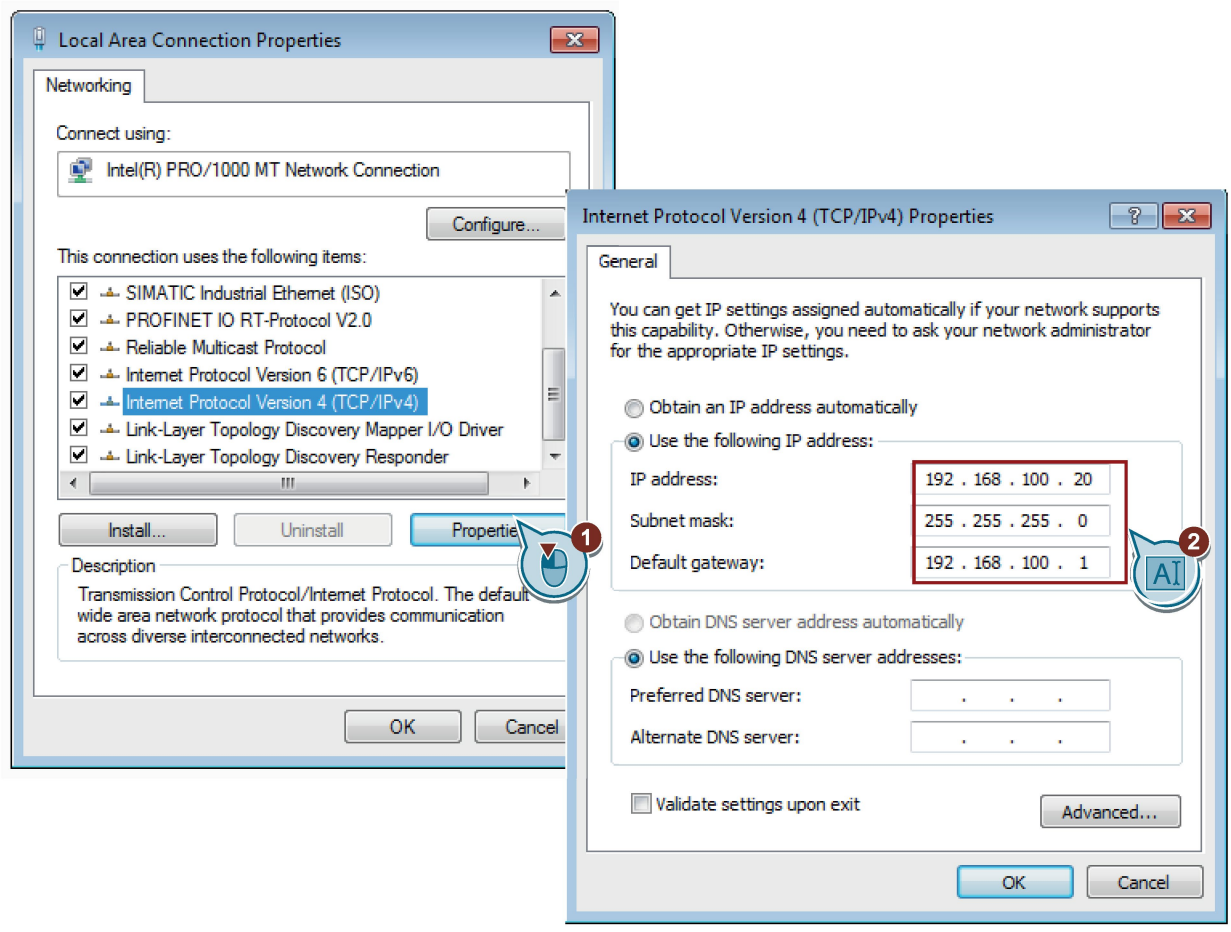
In this configuration example, the Admin PC has the following IP address setting to allow it to access the Web Based Management of the S615.

IP address	Subnet mask
192.168.1.20	255.255.255.0

Procedure

1. On the Admin PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
3. Right-click on the "LAN Connection" symbol and select the "Properties" menu command.
4. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

5. Enter the values in the table above.



6. Confirm the dialogs with "OK" and close the Control Panel.

7. Enter the IP address "192.168.1.1" in the address box of the Internet browser.

   Access via HTTPS is enabled as default. If you access the device via HTTP, the address is automatically redirected to HTTPS.

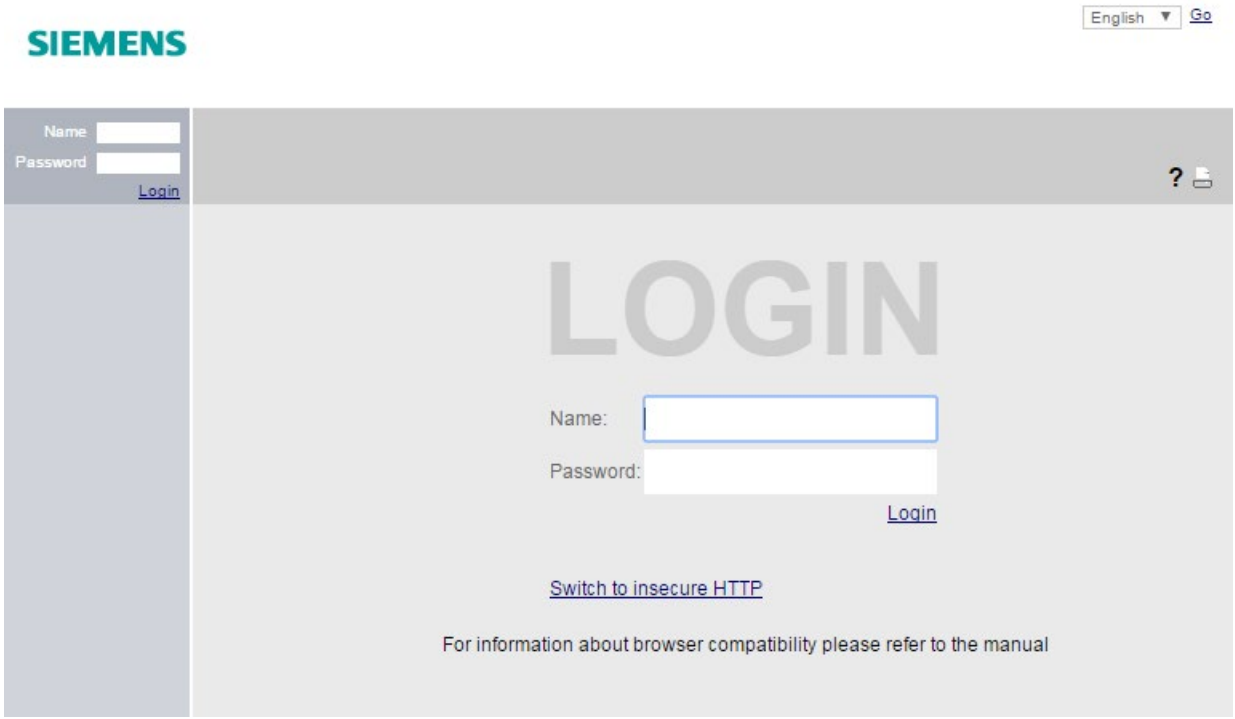
   A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

   Note

   Information on the security certificate

   Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

8. If there is a problem-free connection to the device, the login page of Web Based Management (WBM) is displayed.

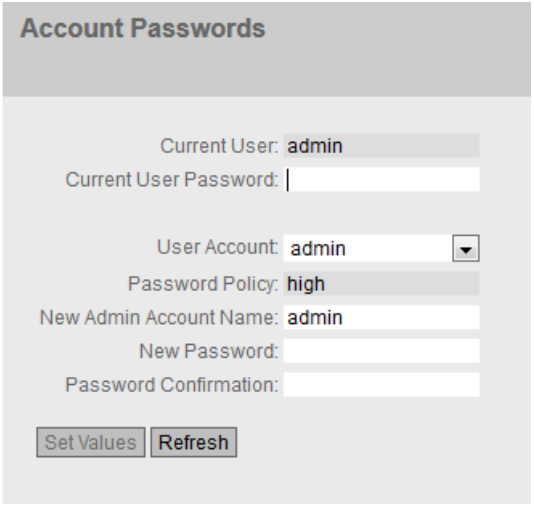


1.4 Logging in to Web Based Management

Procedure

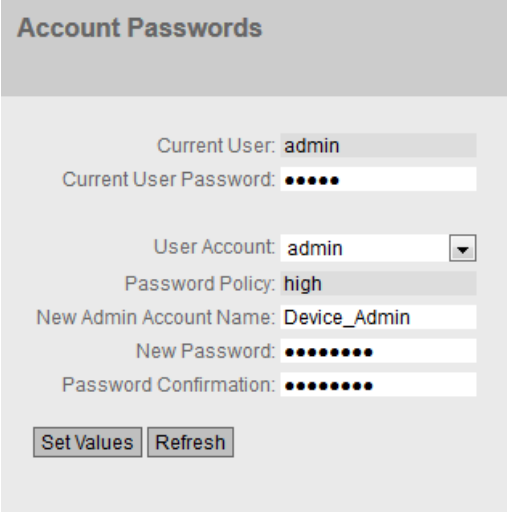
1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password. You can also rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.

2. Confirm the dialog. The "Account Passwords" WBM page is opened automatically.



3. Enter the default password "admin" in "Current User Password".
4. Change the user name for "New Admin Account Name".
5. For "New Password", enter the new password. The new password must be at least 8 characters long and contain upper case letters, lower case letters, numbers and special characters.

6. Repeat the new password in "Password Confirmation" as confirmation. The entries must match.



7. Click the "Set Values" button.

Result

The changes take immediate effect and access via DCP is write-protected.

The Basic Wizard starts to support you when configuring the device parameters.

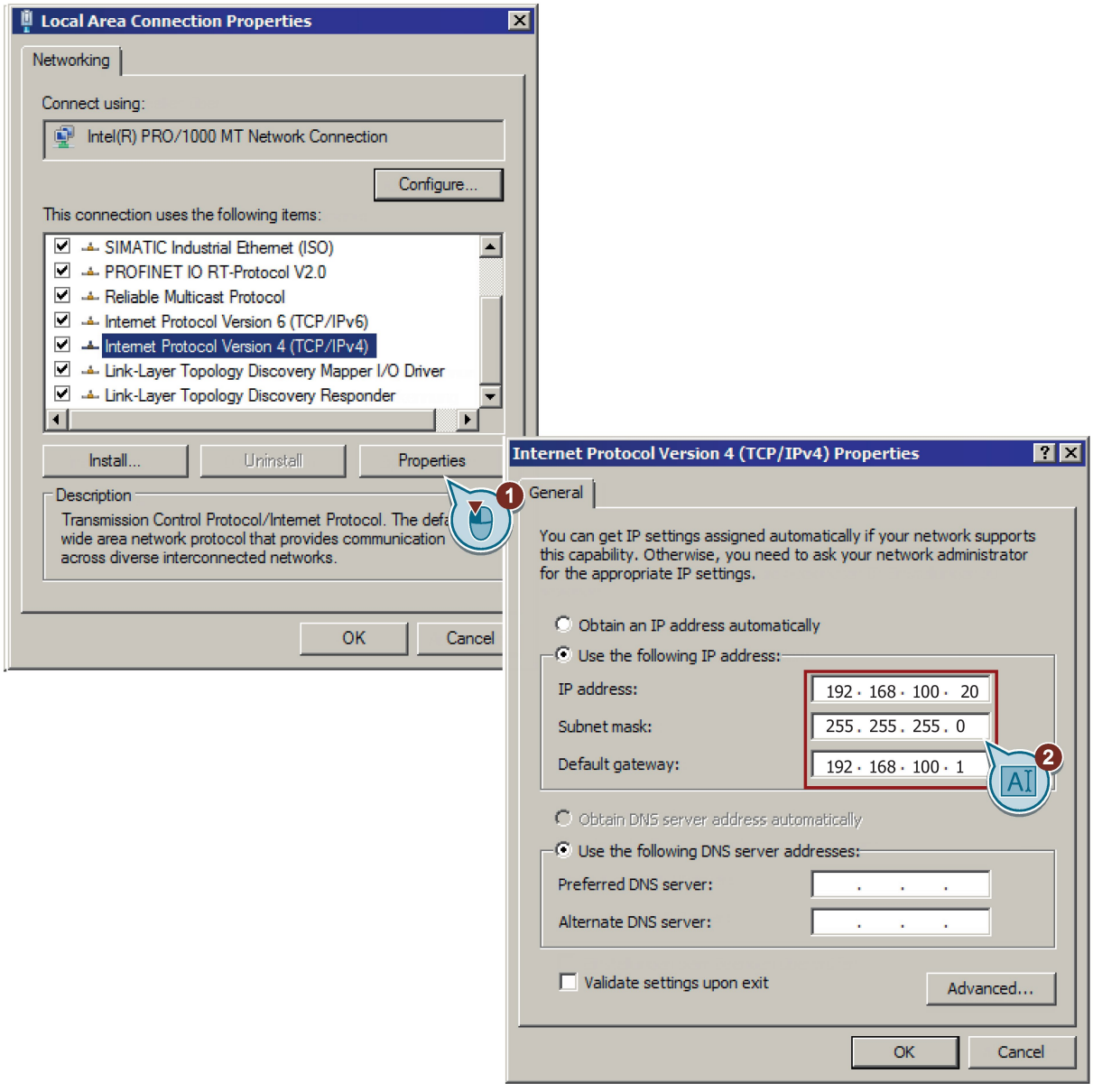
1.5 Changing the IP settings of the S615

Procedure

1. Click on "Layer 3 > Subnets" in the navigation area and on the "Configuration" tab in the content area.
2. Enter the IP address for vlan1 according to the table "Settings used (Page 9)".
3. Click on "Set Values".

   The IP address is adjusted automatically in the address bar of the Web browser. The Web browser on the Admin PC can no longer access Web Based Management because its IP settings no longer match.
4. On the Admin PC, open the Control Panel with the menu command "Start" > "Control Panel".
5. Click "Network and Sharing Center" and select the "Change Adapter Settings" option in the navigation menu on the left.
6. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

7. Enter the values for the PC from the "Settings used (Page 9)" table.



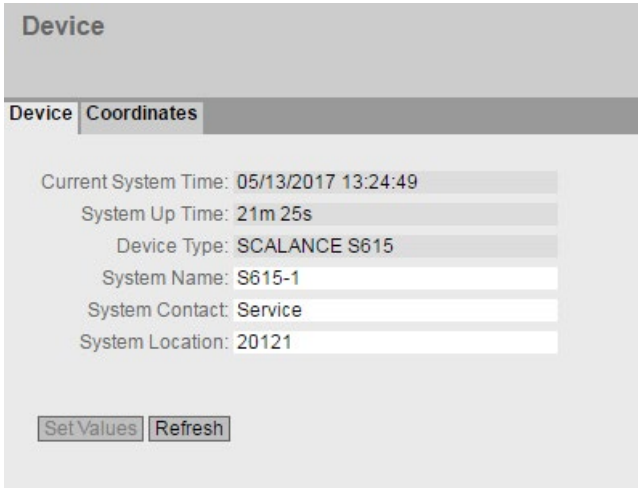
8. Confirm the dialogs with "OK" and close the Control Panel.
9. In the address box of the Web browser, enter the IP address for vlan1, see table "Settings used (Page 9)". If there is a problem-free connection to the device, the login page of Web Based Management (WBM) is displayed.
10. Log in with the user name "admin" and the modified password.

1.6 Specifying device information

To allow better identification of the SCALANCE S615, specify general device information.

Procedure

1. In the navigation area click on "System > General" and in the content area on the "Device" tab.
2. In "System Name", enter a name for the device.
3. Enter the contact person responsible for the device in "System Contact".
4. Enter the identifier for the location at which the device is installed in "System Location", for example the room number.



5. Click the "Set Values" button.

Result

The general device information for the SCALANCE S615 has been specified.

1.7 Setting the time

The date and time are kept on the SCALANCE S615 to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. For this example, the time server is configured using NTP.

Note

Manual time setting - reaction after interrupting the power supply

Note that the time is reset to the factory setting if the power supply is interrupted. On return of the power, you need to set the system time again. As result, certificates can lose their validity.

Synchronization using a time server

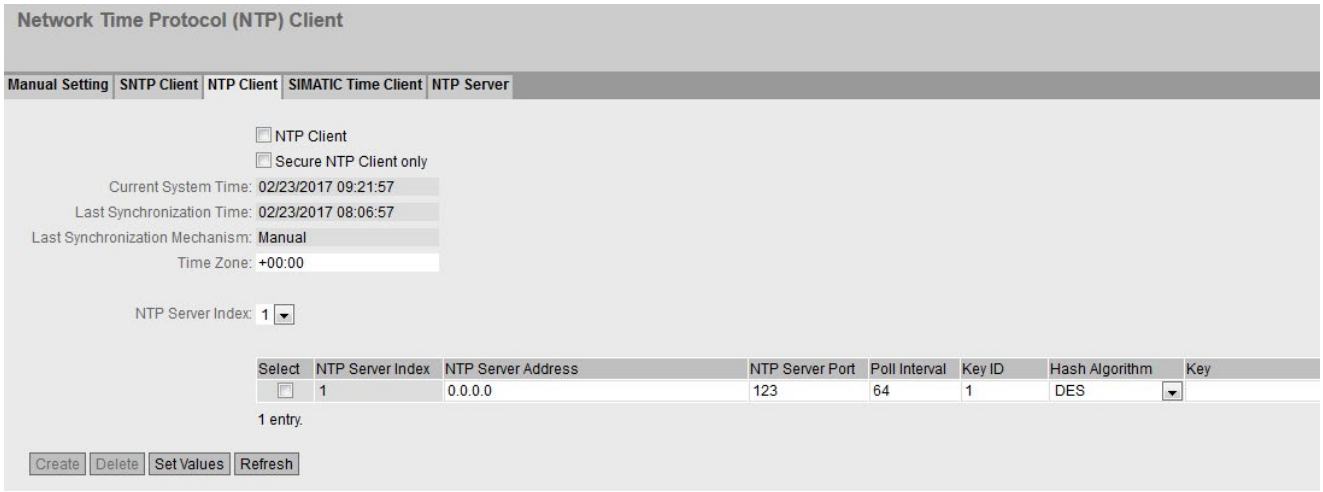
Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

Requirement

- An NTP server can be reached in the local network.
- The IP address of the NTP server is known.
  For this example, a local time server with the IP address 192.168.100.87 is used.

Procedure

1. In the navigation area click on "System > System Time" and in the content area on the "NTP Client" tab.

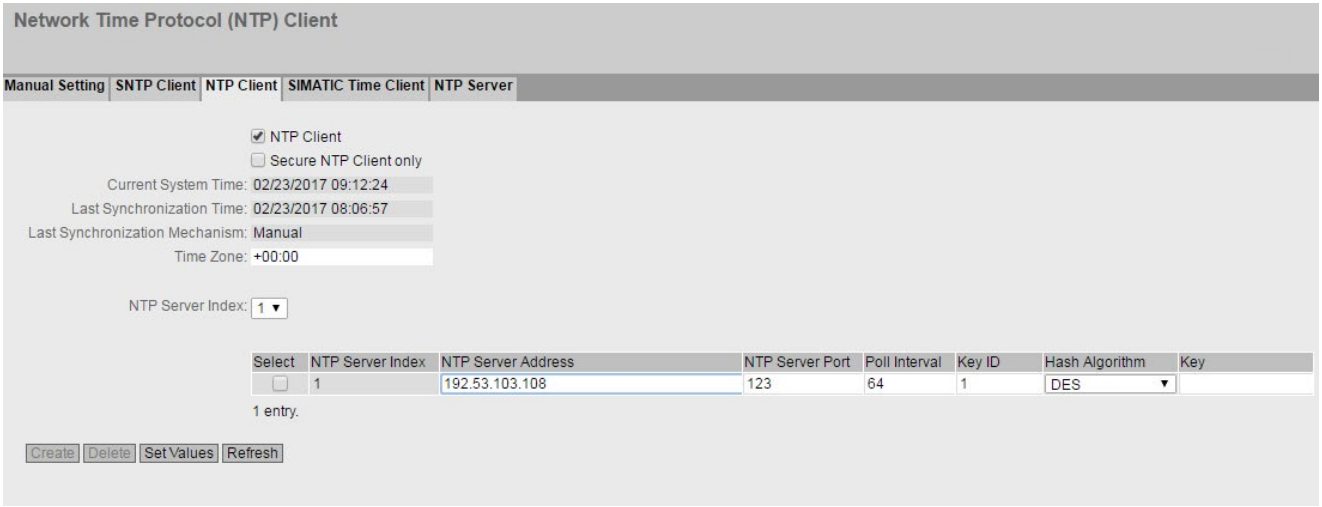


2. In "Time zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. Click "Create". A new entry is created in the table.

4. In "NTP Server Address", enter the IP address 192.53.103.108.
5. If necessary, change the port in "NTP Server Port". As default, 123 is set.
6. In "Poll Interval", enter the interval for synchronization. As default, 64 is set.
7. Enable "NTP Client".
8. Click on "Set Values".

Result

System time using NTP is set. Click "Refresh" to refresh the WBM page.



1.8 Creating IP subnet

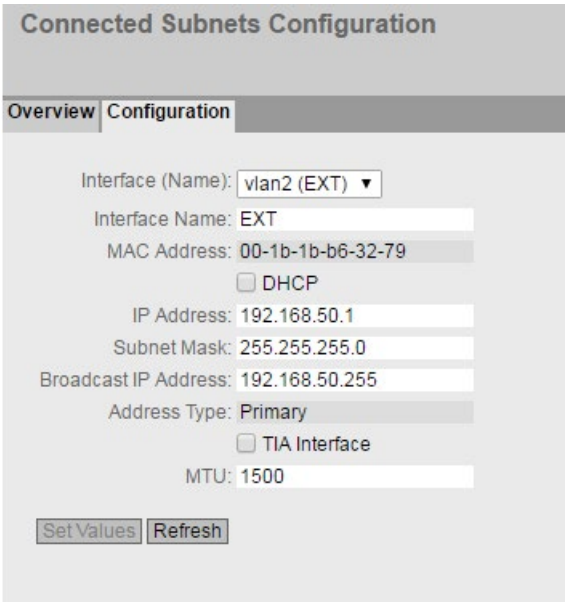
The interfaces are handled differently.

- Ethernet interface P1 (vlan1): Connection to LAN
- Ethernet interface P5 (vlan2): Connection to WAN

For this configuration example, only the IP subnet for the Ethernet interface P5 needs to be configured. The IP subnet for the Ethernet interface P1 is already configured.

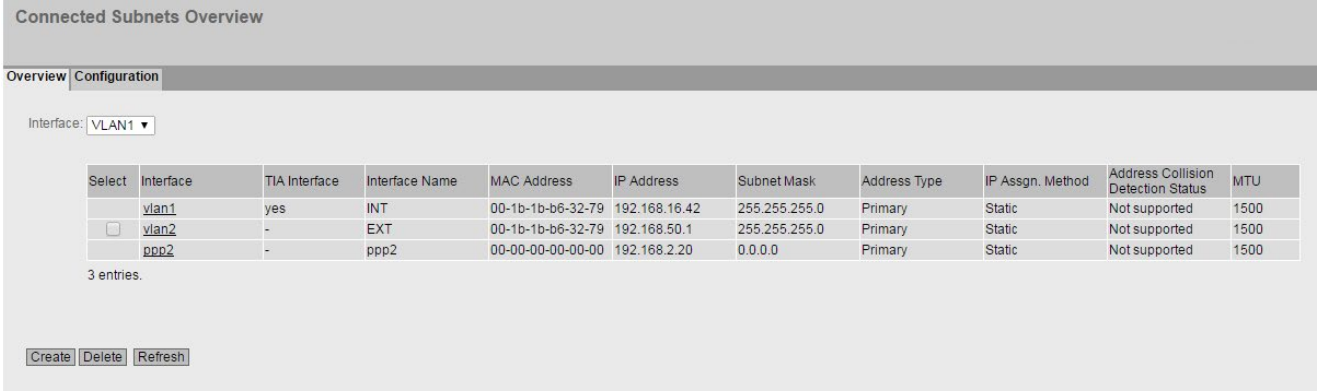
Procedure

1. Click on "Layer 3 > Subnets" in the navigation area and on the "Configuration" tab in the content area.
2. For "Interfaces" select "vlan2".
3. For "Interface Name" you can enter a name.
4. Enter the IP address for vlan2, see table "Settings used (Page 9)"
5. Click on "Set Values".



Result

The IP subnets have been created. The IP subnets are displayed in the "Overview" tab.



Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status	MTU
	vlan1	yes	INT	00-1b-1b-b6-32-79	192.168.16.42	255.255.255.0	Primary	Static	Not supported	1500
	vlan2	-	EXT	00-1b-1b-b6-32-79	192.168.50.1	255.255.255.0	Primary	Static	Not supported	1500
	ppp2	-	ppp2	00-00-00-00-00-00	192.168.2.20	0.0.0.0	Primary	Static	Not supported	1500

3 entries.