SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M-800 Getting Started

Getting Started

06/2015

C79000-G8976-C337-04

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
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: C79000-G8976-C337
℗ 07/2015 Subject to change

Preface

Purpose

The configuration of the SCALANCE M is shown based on 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
CP	CP 343-1 Advanced GX31, CP 443-1 Advanced GX30, CP 1628
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M874	SCALANCE M874-2 SCALANCE M874-3
M876	SCALANCE M876-3 SCALANCE M876-4
M812	SCALANCE M812-1
M816	SCALANCE M816-1
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2

Further documentation

- "Industrial Remote Communication Remote Networks - SCALANCE M874" operating instructions

  This document contains information with which you will be able to install and connect up a device of the SCALANCE M874 product line. The configuration and the integration of the device in a network are not described in these instructions

- "Industrial Remote Communication Remote Networks - SCALANCE M81x" operating instructions

  This document contains information with which you will be able to install and connect up a device of the SCALANCE M812, M816 product line. The configuration and the integration of the device in a network are not described in these instructions

- "Industrial Remote Communication Remote Networks - SCALANCE M-800 Web Based Management" configuration manual

  This document is intended to provide you with the information you require to install, commission and operate the device. It provides you with the information you require to configure the devices.

- You will find further information about working with the SCT (Security Configuration Tool) in the "Industrial Ethernet Security - Basics and Application" configuration manual. You will find this document on the Internet under the following entry ID: 56577508 (http://support.automation.siemens.com/WW/view/en/56577508)

- The "SIMATIC NET Industrial Ethernet Network Manual" contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network. There, you will find among other things optical performance data of the communications partners that you require for the installation.

  You will find this document on the Internet under the following entry ID: 27069465 (http://support.automation.siemens.com/WW/view/en/27069465)

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 (http://support.automation.siemens.com/)

  Enter the entry ID of the relevant manual as the search item.

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

  Link to the area "Industrial Communication" (http://support.automation.siemens.com/WW/view/en/10805878/133400)

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

Security messages

Note

Siemens offers IT security mechanisms for its automation and drive product portfolio in order to support the safe operation of the plant/machine. Our products are also continuously developed further with regard to IT security. We therefore recommend that you regularly check for updates of our products and that you only use the latest versions. You will find information in:

(http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en)

Here, you can register for a product-specific newsletter.

For the safe operation of a plant/machine, however, it is also necessary to integrate the automation components into an overall IT security concept for the entire plant/machine, which corresponds to the state-of-the-art IT technology. You will find information on this in: (http://www.siemens.com/industrialsecurity)

Products from other manufacturers that are being used must also be taken into account.

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

Trademarks

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

SCALANCE, SINEMA, CP 343-1, CP 443-1, CP 1628, C-PLUG, KEY-PLUG

Table of contents

Connecting SCALANCE M-800 to WAN

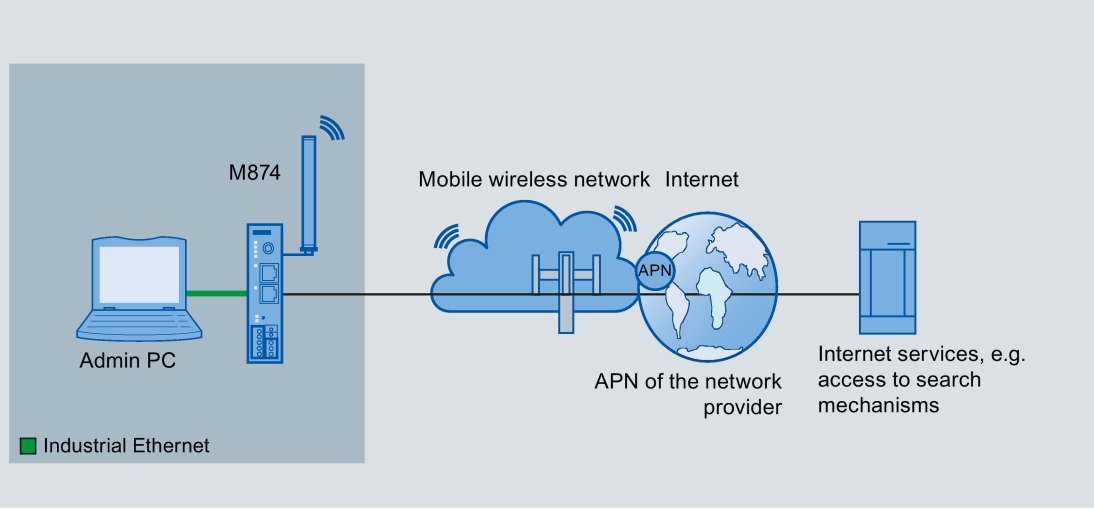
1

1.1 Connecting M874 with the mobile wireless network

1.1.1 Procedure in principle

In this example the SCALANCE M874 that is in the factory settings status is assigned an IP address. Following this, the device will be configured using Web Based Management (WBM).

Structure



Required devices/components

- 1 x M874 (additional option: a suitably installed standard rail with fittings)
- 1 x suitable antenna
- 1 x SIM card of your mobile wireless provider (the required services, for example Internet are enabled)
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuring the M874.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Note

You can also use a SCALANCE M876. The configuration described below relates specifically to the components mentioned in the section "Required devices/components".

Steps in configuration

To connect an M874 to the mobile wireless network, the following steps are necessary:

1. Setting up SCALANCE M874 and network (Page 13).
2. Launching Web Based Management (Page 13)
3. Logging in to Web Based Management (Page 16)
4. Changing the IP settings of the M874 (Page 17).
5. Configuring the SCALANCE M874.
   - Specifying device information (Page 19)
   - Configuring access parameters (Page 20)
   - Setting the time (Page 23)
   - Allowing access.

1.1.2 Setting up SCALANCE M874 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 M874 and check that it is undamaged.
2. Insert the SIM card.
3. Fit the power supply.

⚠ WARNING

Use safety extra-low voltage only

The SCALANCE M874 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 M power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

4. Fit the antenna.
5. Connect the PC to one of the two Ethernet ports (P1, P2).
6. Turn the device on. After connecting up, the fault LED (F) is lit yellow.
7. Now, turn on the PC.

1.1.3 Launching Web Based Management

In the factory settings, the SCALANCE M-800 can be reached at the following IP address:

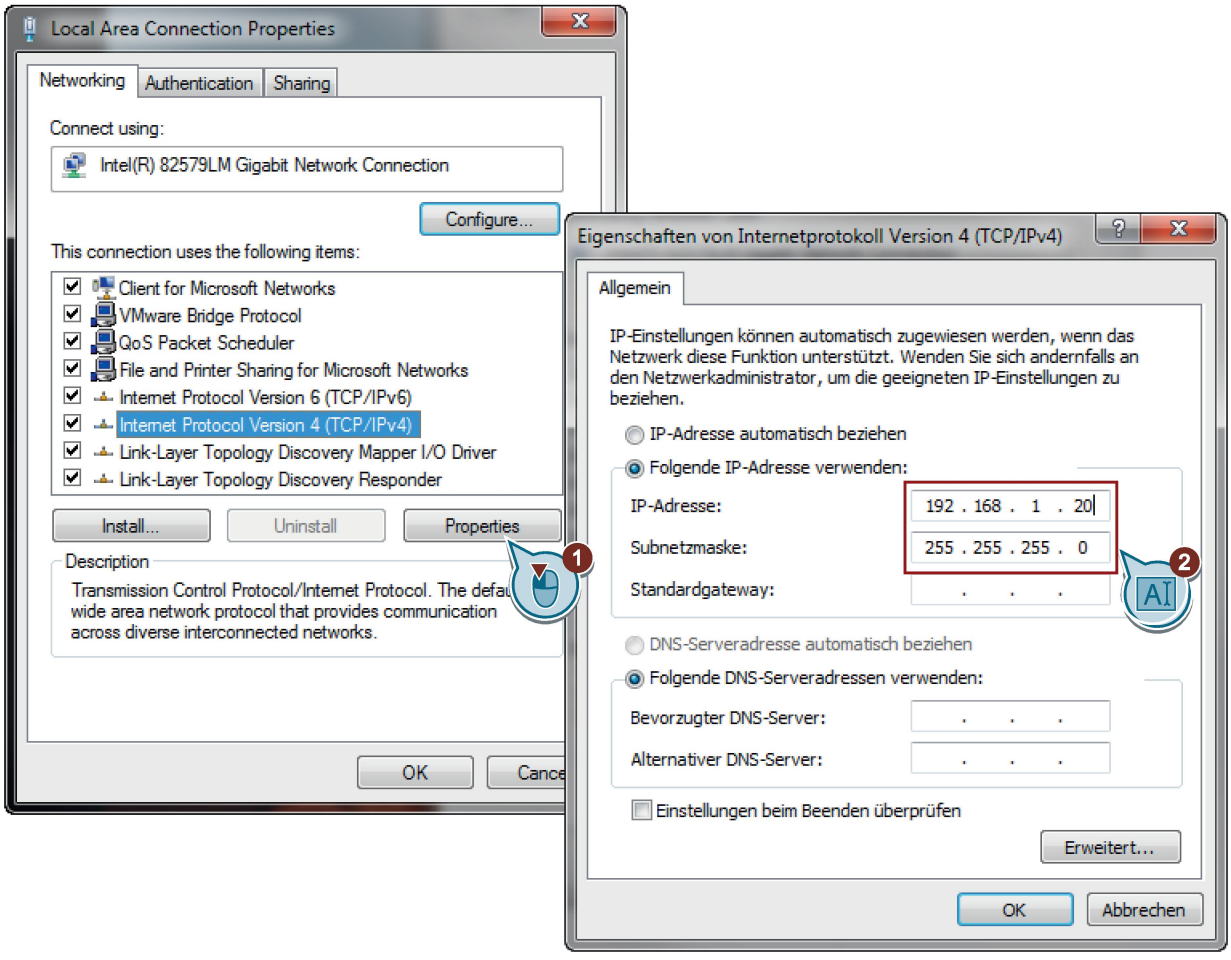
- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

In this configuration example, the Admin PC has the following IP address setting to allow it to access the Web Based Management of the M-800.

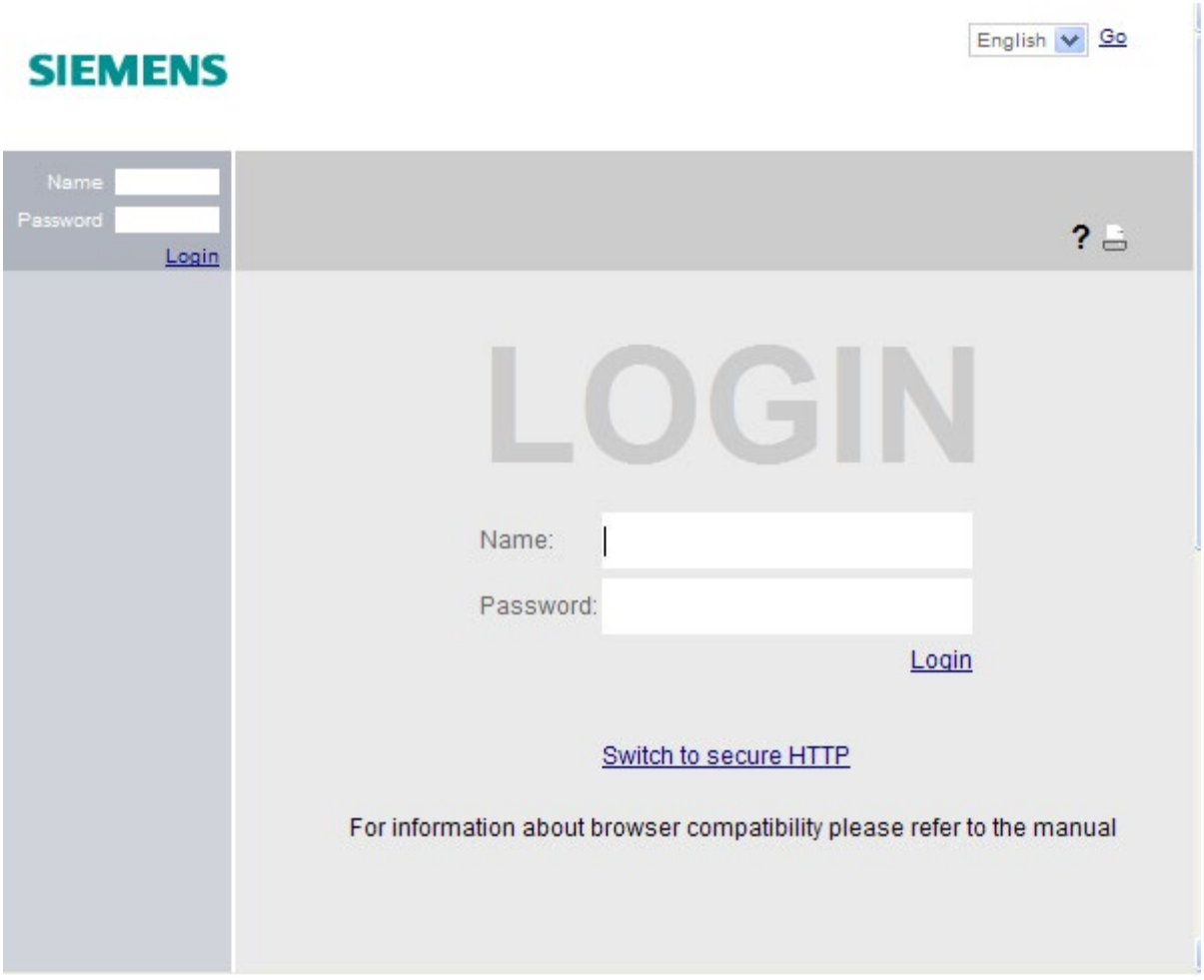
IP address	Subnet mask
192.168.1.20	255.255.255.0

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 assigned to the Admin PC from the table in the relevant boxes.



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

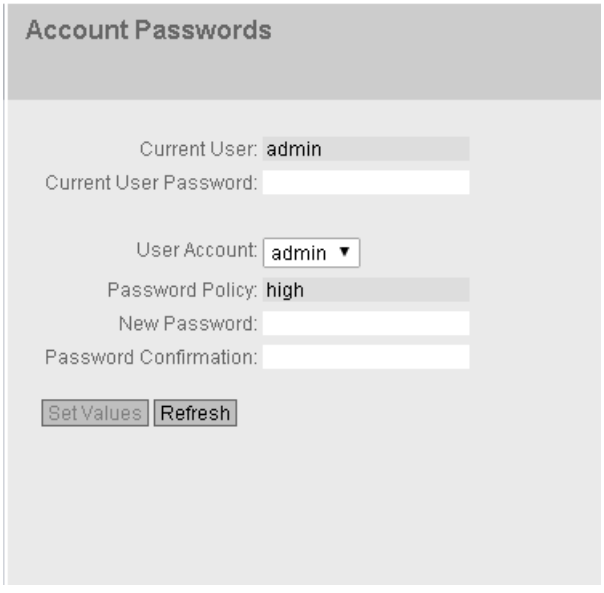


1.1.4 Logging in to Web Based Management

Procedure

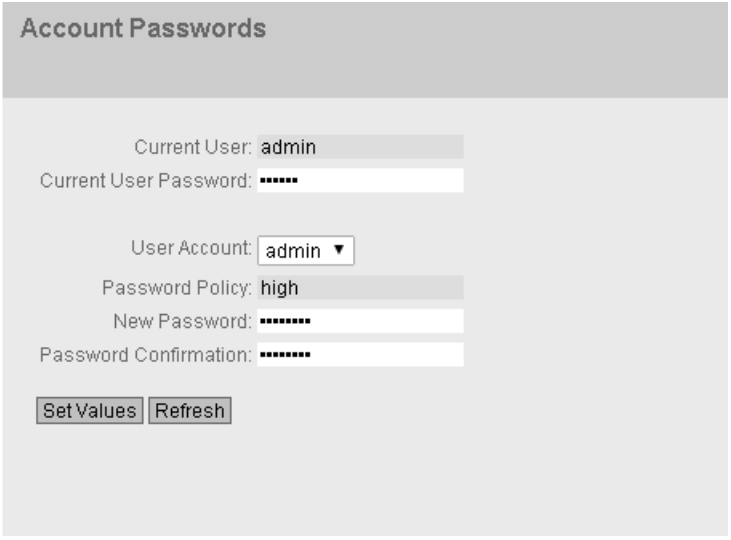
1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password.

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



3. In "Username", select the user "admin".
4. Enter the default password "admin" in "Current Admin Password".
5. Specify the new password in "New Password".

6. Repeat the password in "Password Confirmation" to confirm it. The entries must match.



7. Click the "Set Values" button.

Result

The password for the "admin" user is changed. The changes take immediate effect.

1.1.5 Changing the IP settings of the M874

The following IP address settings are made for the devices in this configuration example:

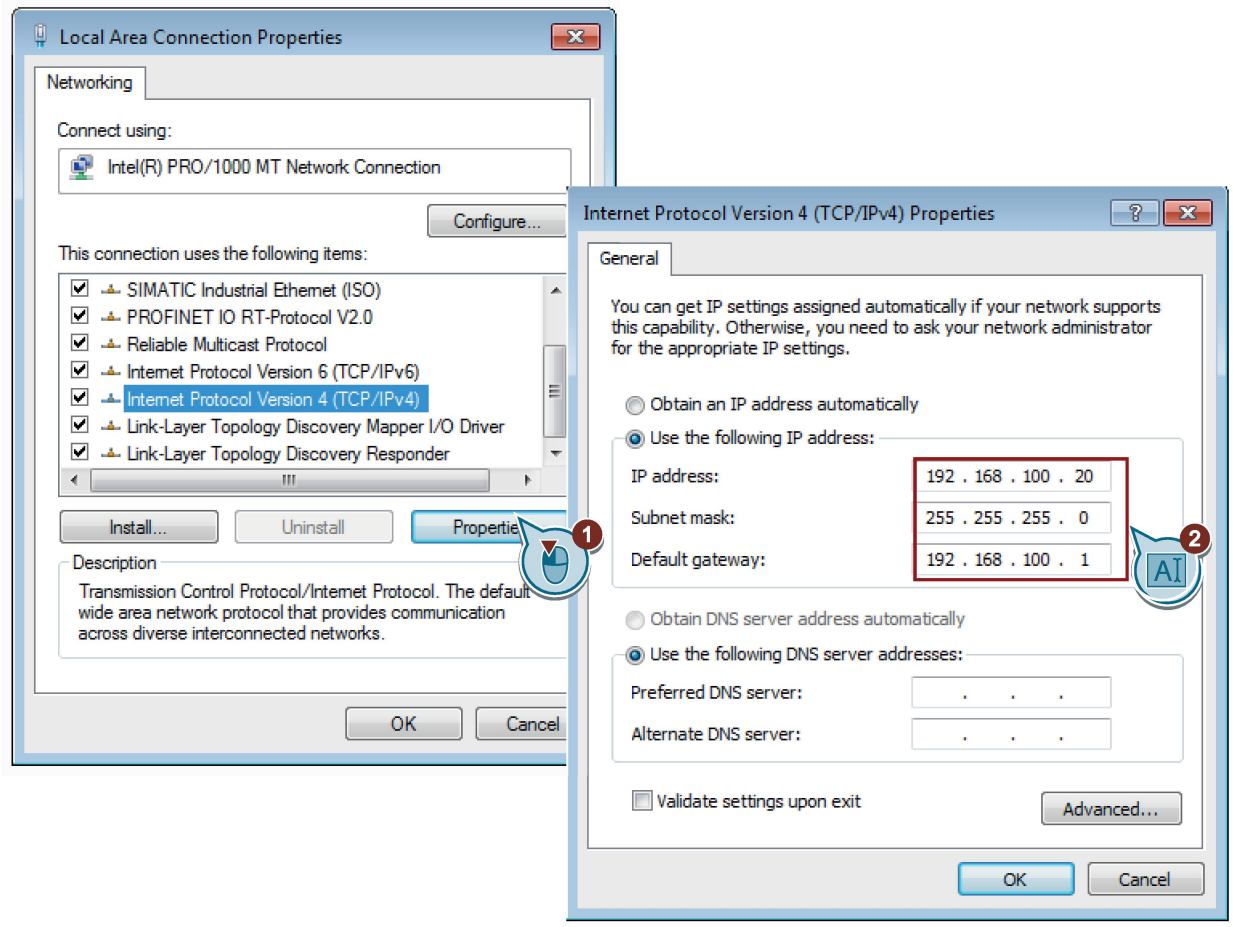
	IP address	Subnet mask
SCALANCE M-800	192.168.100.1	255.255.255.0
Admin PC	192.168.100.20	255.255.255.0

Procedure

1. Click "System" > "Agent IP" in the navigation area.
2. Enter 192.168.100.1 in "IP Address" and 255.255.255.0 in "Subnet Mask".
3. Click "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 assigned to the Admin PC from the table in the relevant boxes.



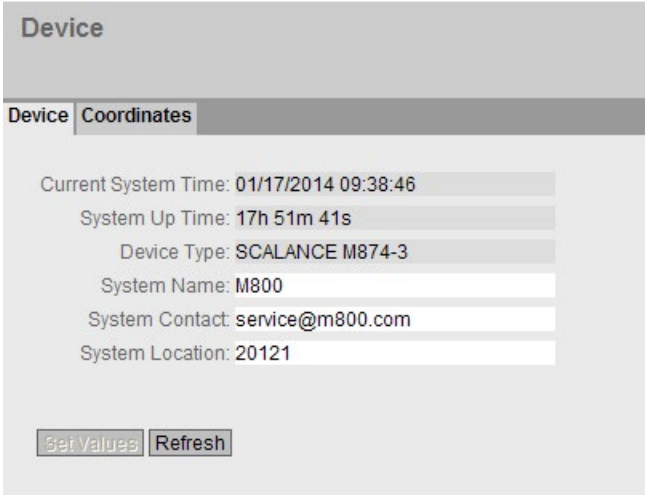
8. Confirm the dialogs with "OK" and close the Control Panel.
9. Enter the IP address "192.168.100.1" in the address box of the Web browser. If there is a problem-free connection to the device, the login page of Web Based Management (WBM)is displayed.
10. Log in with the user name "admin" and the modified password.

1.1.6 Specifying device information

To allow better identification of the SCALANCE M874, specify general device information.

Procedure

1. Click "System" > "General" in the navigation panel and on the "Device" tab in the content area.
2. In "System Name", enter M874" as the system 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 M874 has been specified.

1.1.7 Configuring access parameters

Requirement

- The services are enabled, e.g. Internet.
- The following data is available:
  - PIN number
  - APN
  - User name and password for the APN

Enter the PIN number

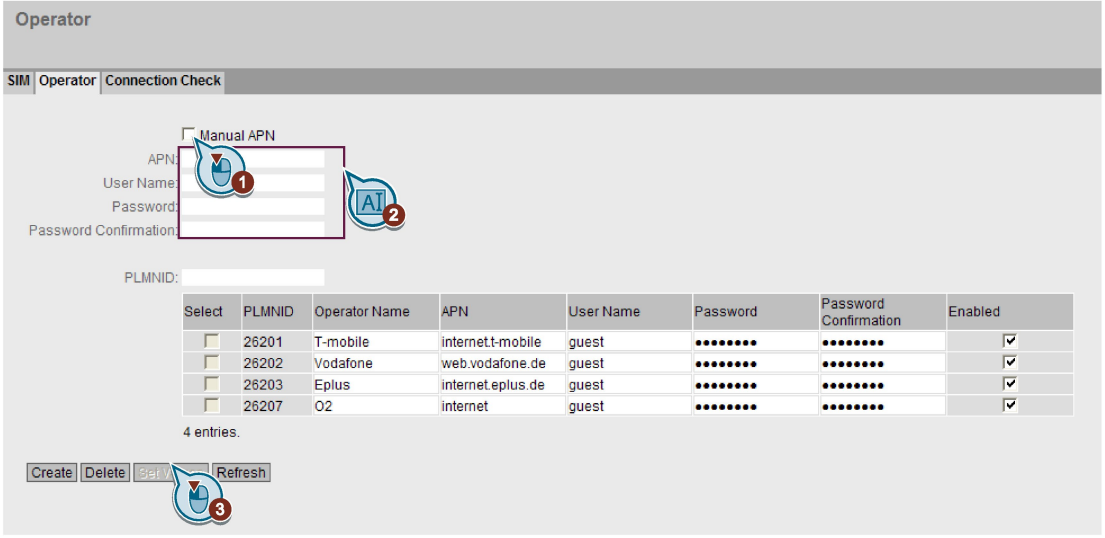
1. Click on "Interfaces" > "Mobile" in the navigation area and on the "SIM" tab in the content area.
2. In "PIN", enter the PIN number.
3. Select Enable Mobile Networks".
4. Click "Set Values".

Configure APN

1. Click on the "Operator" tab in the content area.
2. Specify the access data for the APN.
   - If your mobile wireless provider is included in the table, no further configuration is necessary.

   or

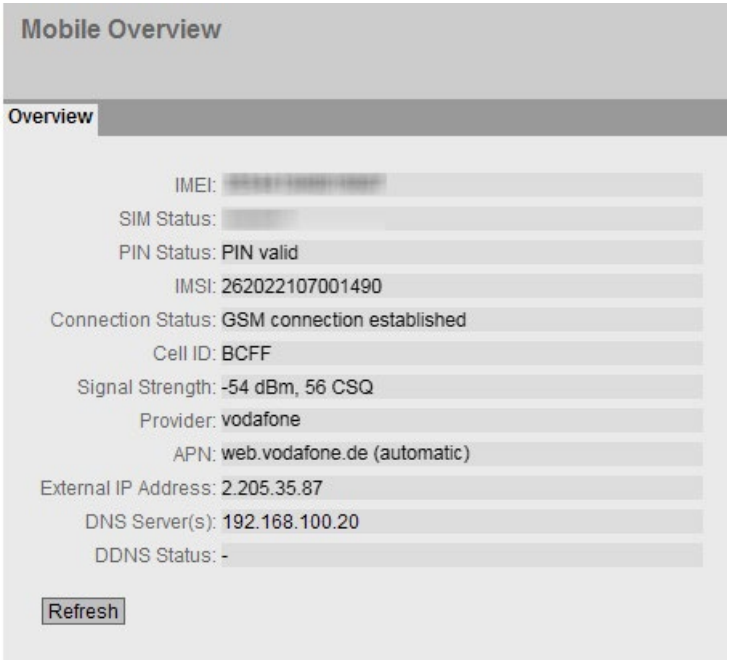
   - If your mobile wireless provider is not included in the table, enable "Manual APN".
   - Enter the APN, user name and password. Some mobile wireless providers do not use access control with a password. In this case, leave the box empty.



Result

The PIN number and the APN are configured. The M874 connects to the mobile wireless network after approximately 30 seconds. You can check whether or not the connection is established in "Information" > "Start Page".

You will find more detailed information on the connection in "Information" > "Mobile".



1.1.8 Setting the time

The date and time are kept on the SCALANCE M-800 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. There are a number of time servers on the Internet that can be used to obtain the current time precisely. 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

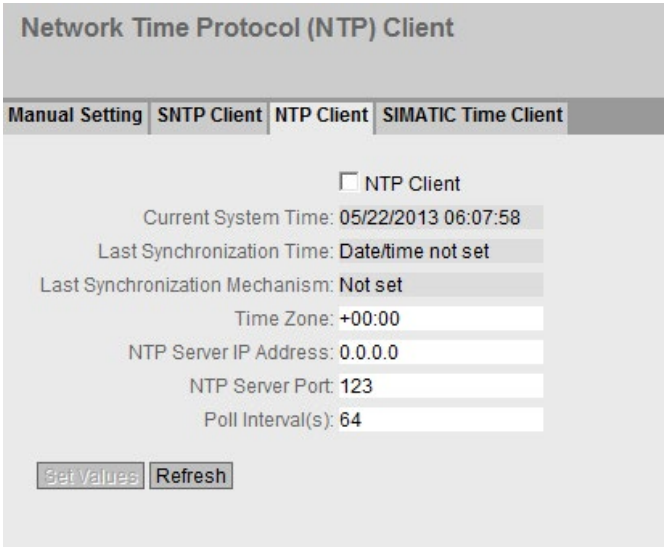
Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

Requirement

- The NTP server is reachable.
- The IP address of the NTP server is known.
  For this example, a time server (e.g. 192.53.103.108) of the Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig is used (Federal Institute of Physical and Technical Affairs - metrology institute).

Procedure

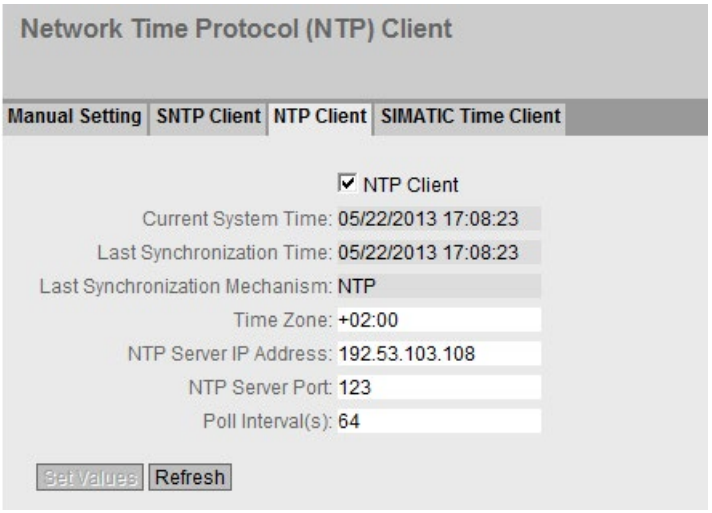
1. Click on "System" > "System Time" in the navigation area and on the "NTP Client" tab in the content area.



2. In "Time Zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. In "NTP Server IP Address", enter the IP address 192.53.103.108. It is not possible to enter the NTP address as a host name, for example timeserver.org.
4. If necessary, change the port in "NTP Server Port". As default, 123 is set.
5. In "Poll Interval (s)", enter the interval for synchronization. As default, 64 is set.
6. Select NTP Client".
7. Click "Set Values".

Result

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



1.1.9 Allow access

You have the following options for allowing access:

- Allow globally

  Here, you use simple, predefined firewall rules. The enabled services are valid for all nodes on the relevant interfaces. Full access is allowed for the specified direction.

  – vlan1: Allows access from the internal network to the device

  – ppp0 / usb0: Allows access from the external network to the device

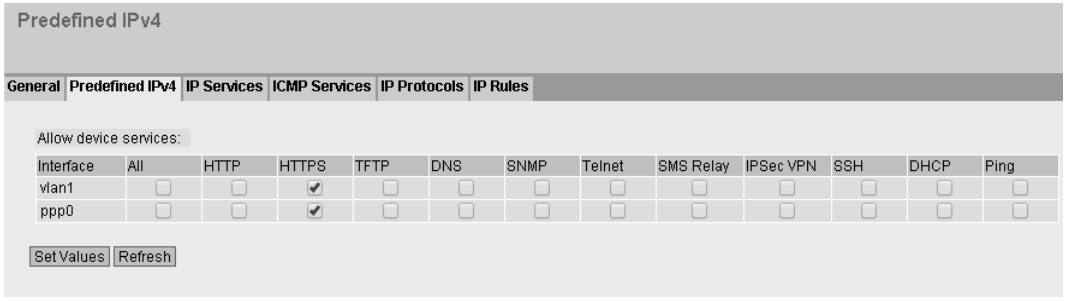
  The firewall rule for the opposite direction is permitted by stateful packet inspection.

- Allow certain services

  Here, you define firewall rules that allow individual services for a single node or all services for the node for access to the station or network.
  In this example, configure the firewall rule that only allows the device with IP address 192.168.100.20 access to the device. The service HTTP (TCP port 80) is required for access.

Example 1: Allow HTTPS access globally

1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Enable "HTTPS" for "vlan1" and "ppp0".
3. Click "Set Values".



Example 2: Allow a specific device HTTPS access

Disabling predefined firewall rules

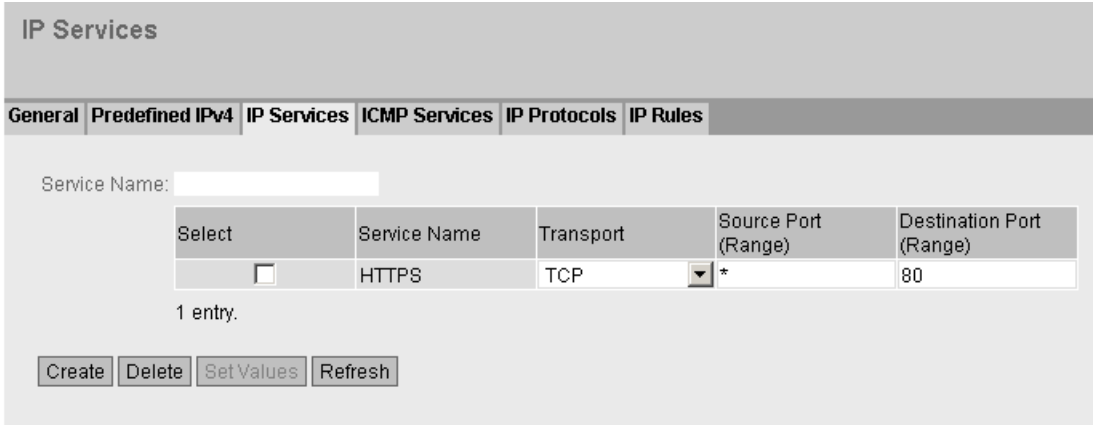
1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Deactivate all services.

Create HTTPS IP service

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. As "Service Name", enter for example "HTTPS" and click "Create". A new entry is created in the table.
3. Configure HTTPS with the following settings:

Transport	TCP
Destination Port (Range)	80 (standard port)

4. Click "Set Values".

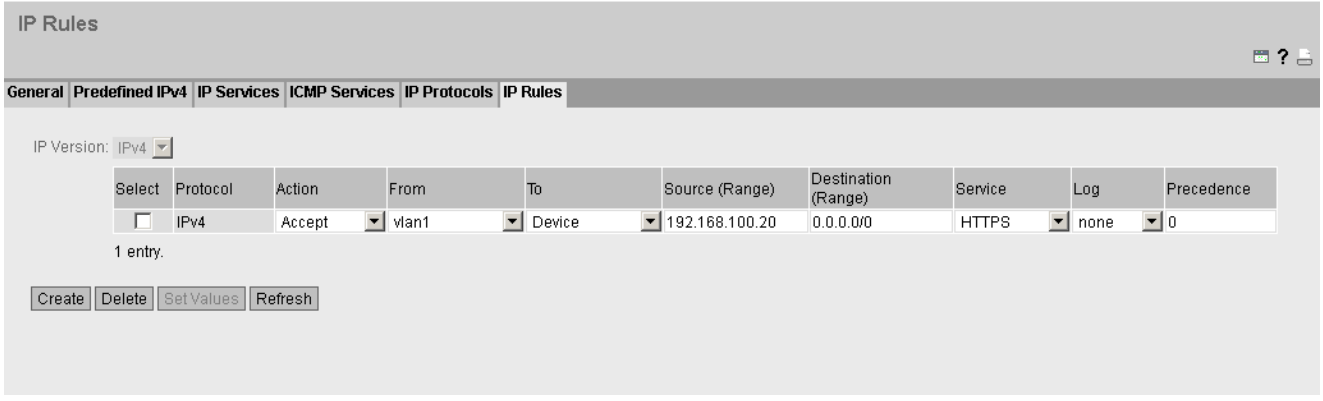


Allow only a specific device HTTPS access

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule for the created HTTPS service with the following settings:

Action	Accept
From	vlan1
To	Device
Source (Range)	192.168.100.20 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	HTTPS

4. Click "Set Values".



1.1.10 Setting up the DDNS hostname

DDNS stands for "dynamic domain name system". If you log the SCALANCE M-800 on to a DDNS service, the device can be reached from the external network under a hostname, e.g. "example.no-ip.com".

The DNS server of the DDNS service manages the assignment of IP address to hostname. The client informs the DNS server of its currently assigned IP address. The DNS name server registers the current hostname - IP address assignment and passes this on to other domain name servers in the Internet. This means that the SCALANCE M-800 can always be reached using its hostname.

Requirement

- User name and password that gives you the right to use the DDNS service
- Registered hostname, e.g. example.no-ip.com

Procedure

1. Click on "System" > "DNS" in the navigation area and on the "DDNS Client" tab in the content area.
2. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip.com
3. For "User name", enter the user name and for "Password / Password confirmation" the password that allows you to use
   the DDNS service. Your DDNS provider will give you this information.
4. Select Enable".

5. Click "Set Values".

Result

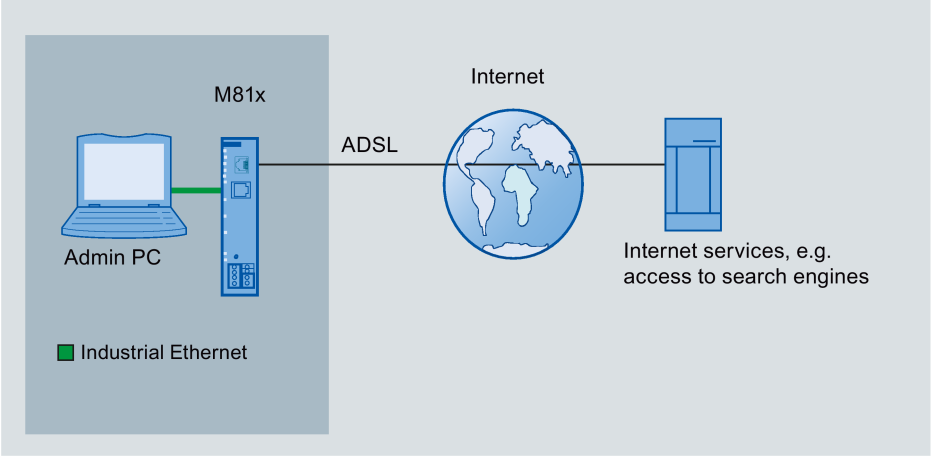
The DDNS client is activated. The DDNS client on the SCALANCE M-800 synchronizes the assigned IP address with the hostname registered in the DDNS service.

1.2 Connecting M81x to ADSL

1.2.1 Procedure in principle

In this example the SCALANCE M81x that is in the factory settings status is assigned an IP address. Following this, the device will be configured using Web Based Management (WBM).

Structure



Required devices/components

- 1 x M812 or 1 x M816 (optionally also: a suitably installed standard rail with fittings)
- ADSL is enabled
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuring the device.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Steps in configuration

To connect an M81x to the landline, the following steps are necessary:

1. Setting up SCALANCE M81x and network (Page 30).
2. Launching Web Based Management (Page 30)
3. Logging in to Web Based Management (Page 33)

4. Changing the IP settings of the M81x (Page 34).
5. Configuring the SCALANCE M81x.
   - Specifying device information (Page 36)
   - Configuring access parameters (Page 37)
   - Setting the time (Page 39)
   - Allowing access (Page 41).

1.2.2 Setting up SCALANCE M81x 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 M81x and check that it is undamaged.
2. Fit the power supply.

⚠ WARNING

Use safety extra-low voltage only

The SCALANCE M81x 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 M81x power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

3. Connect the device to the DSL socket on the splitter.
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.

1.2.3 Launching Web Based Management

In the factory settings, the SCALANCE M-800 can be reached at the following IP address:

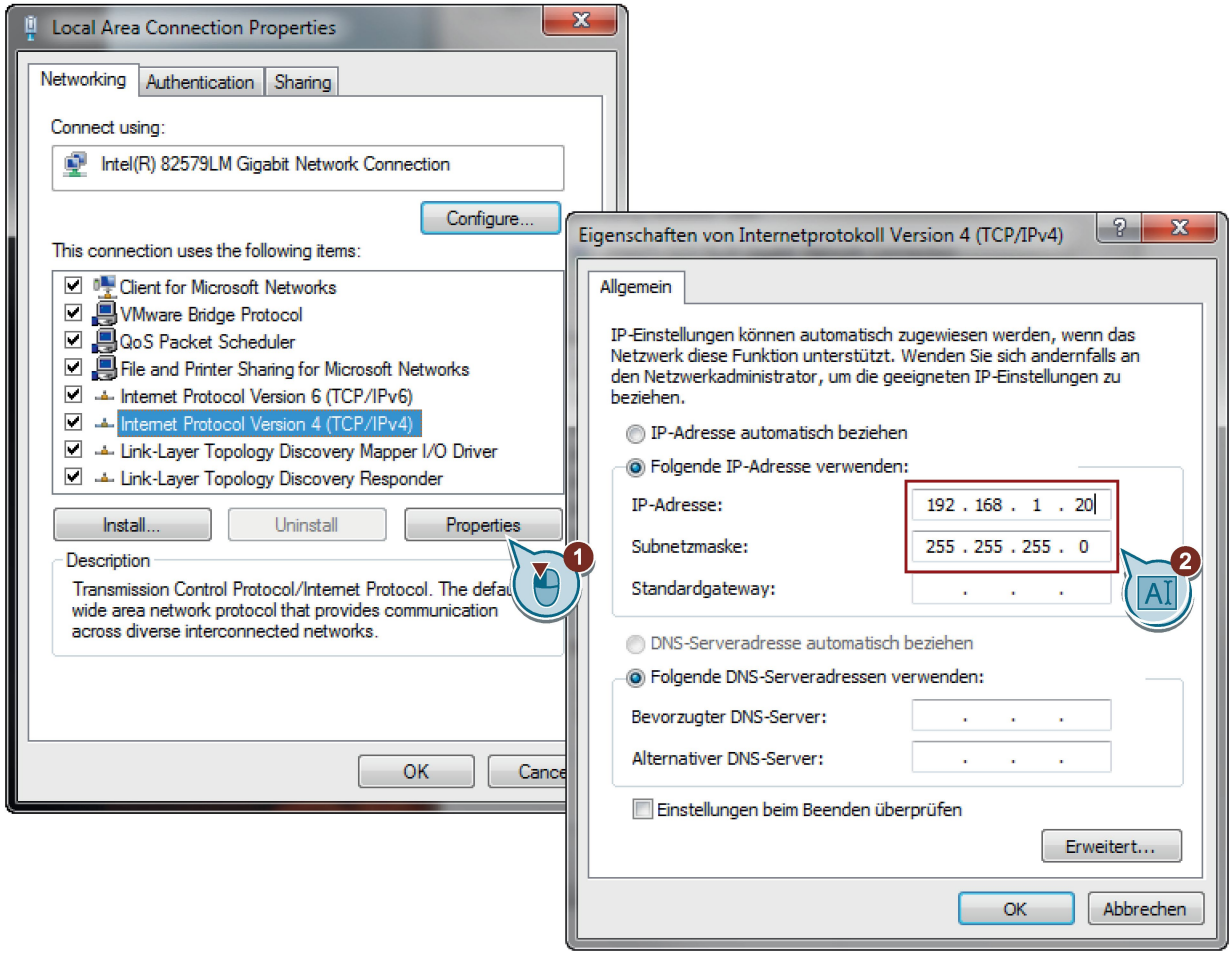
- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

In this configuration example, the Admin PC has the following IP address setting to allow it to access the Web Based Management of the M-800.

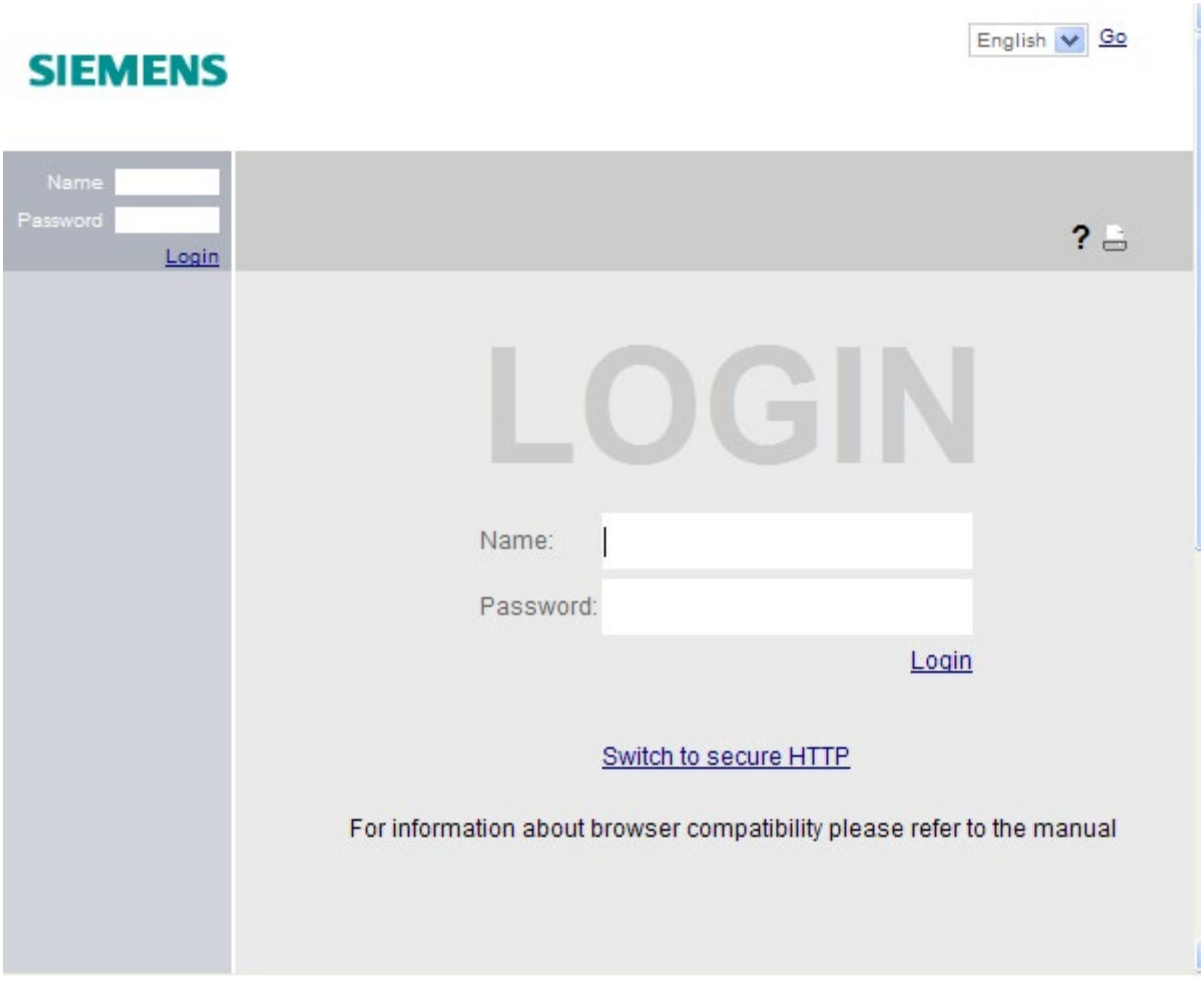
IP address	Subnet mask
192.168.1.20	255.255.255.0

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 assigned to the Admin PC from the table in the relevant boxes.



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

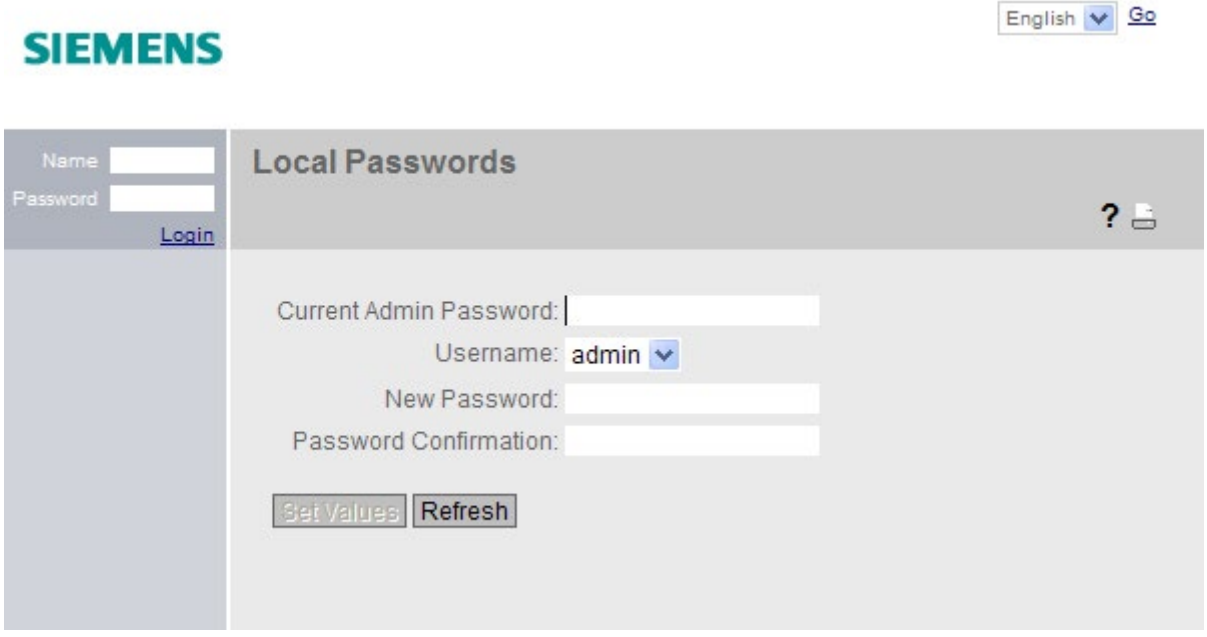


1.2.4 Logging in to Web Based Management

Procedure

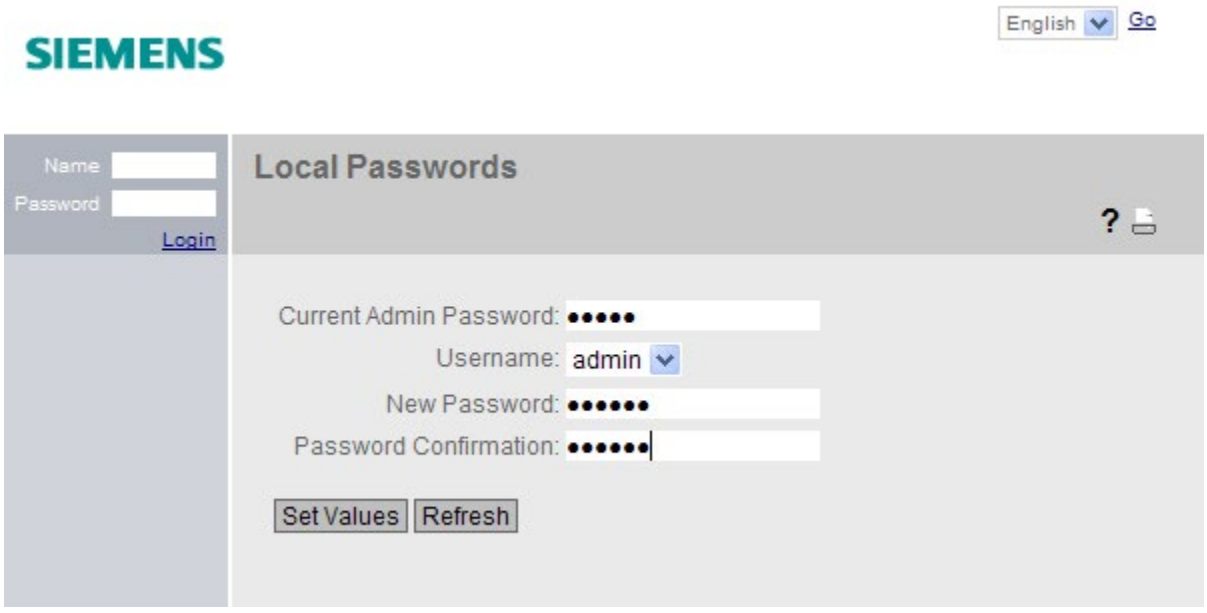
1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password.

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



3. In "Username", select the user "admin".
4. Enter the default password "admin" in "Current Admin Password".
5. Specify the new password in "New Password".

6. Repeat the password in "Password Confirmation" to confirm it. The entries must match.



7. Click the "Set Values" button.

Result

The password for the "admin" user is changed. The changes take immediate effect.

1.2.5 Changing the IP settings of the M81x

The following IP address settings are made for the devices in this configuration example:

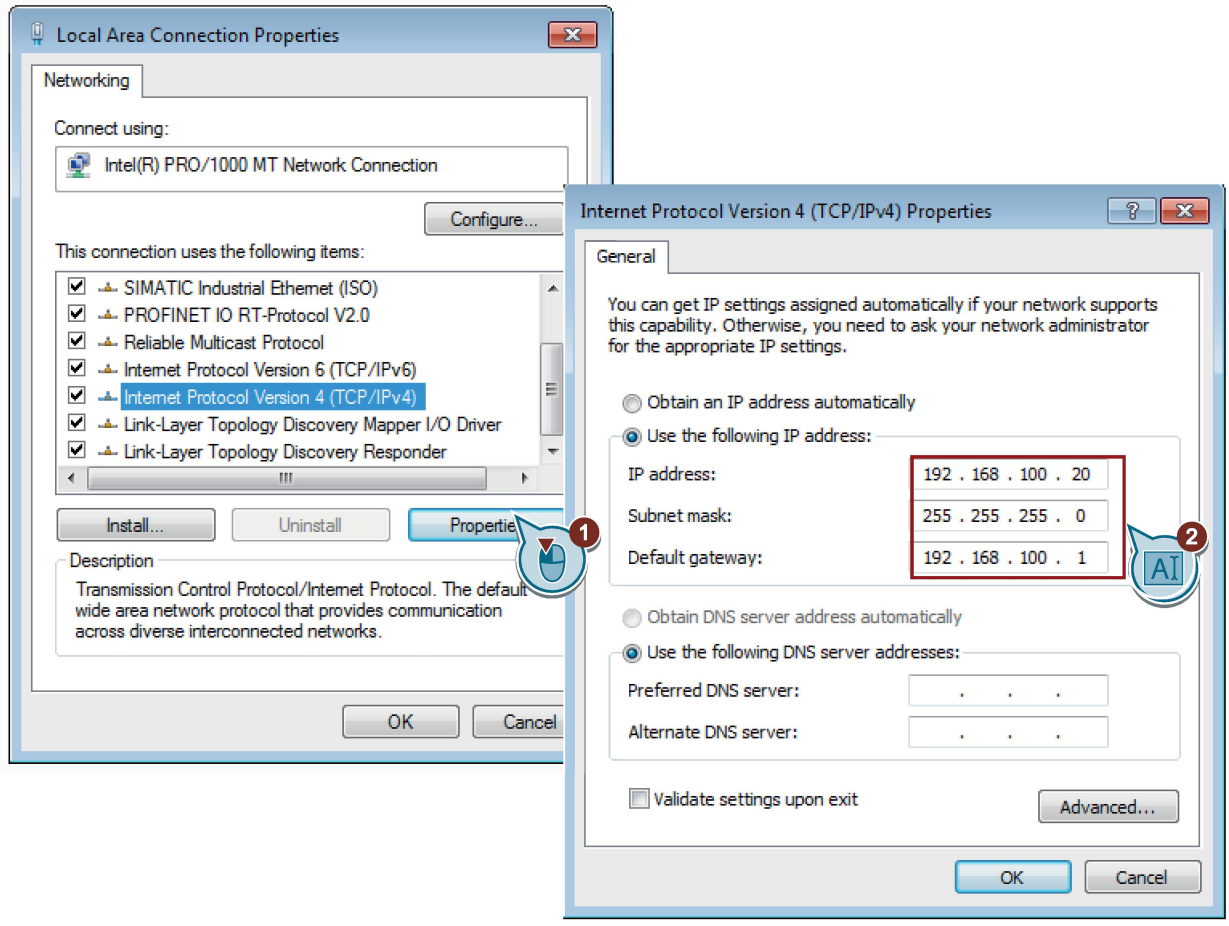
	IP address	Subnet mask
SCALANCE M-800	192.168.100.1	255.255.255.0
Admin PC	192.168.100.20	255.255.255.0

Procedure

1. Click "System" > "Agent IP" in the navigation area.
2. Enter 192.168.100.1 in "IP Address" and 255.255.255.0 in "Subnet Mask".
3. Click "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 assigned to the Admin PC from the table in the relevant boxes.



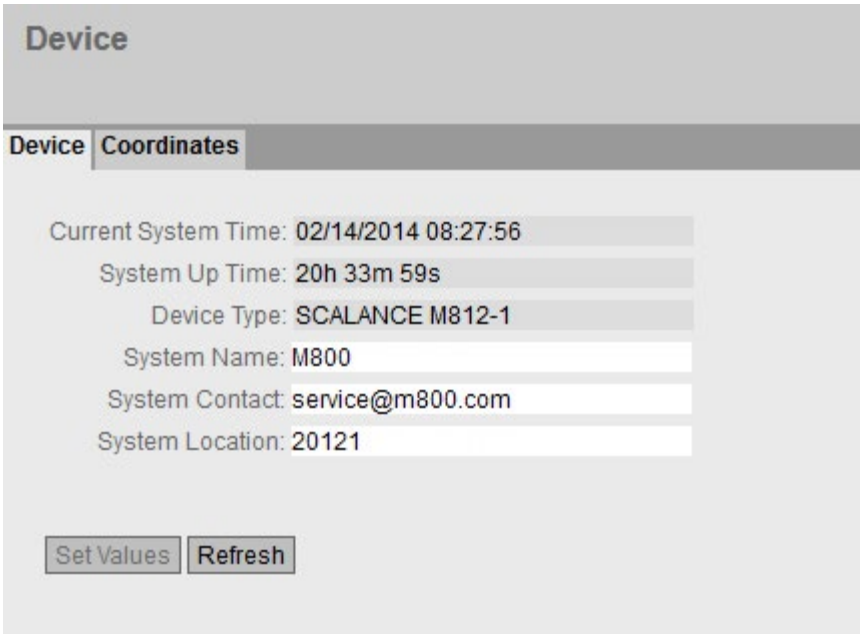
8. Confirm the dialogs with "OK" and close the Control Panel.
9. Enter the IP address "192.168.100.1" in the address box of the Web browser. If there is a problem-free connection to the device, the login page of Web Based Management (WBM)is displayed.
10. Log in with the user name "admin" and the modified password.

1.2.6 Specifying device information

To allow better identification of the SCALANCE M81x, specify general device information.

Procedure

1. Click "System" > "General" in the navigation panel and on the "Device" tab in the content area.
2. In "System Name", enter M800" as the system 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 M81x has been specified.

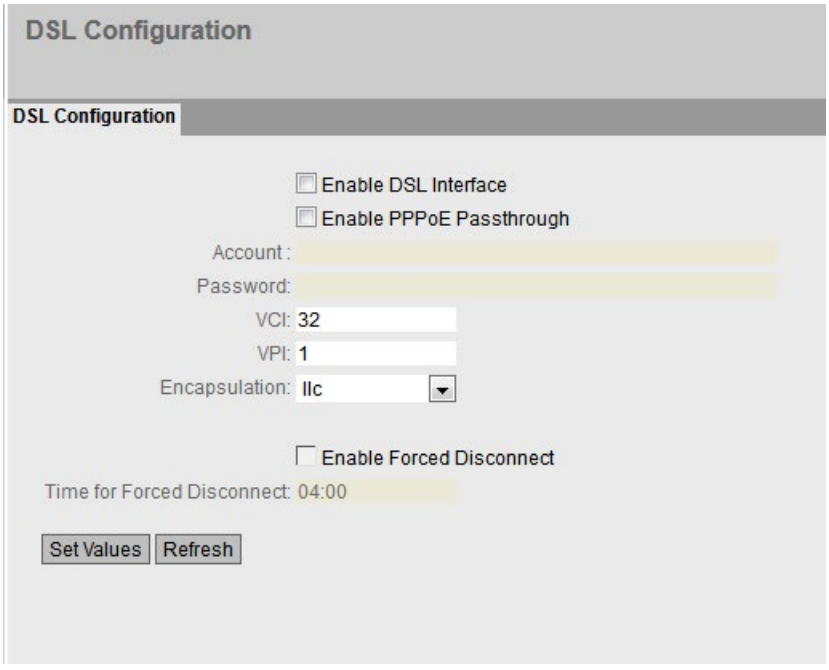
1.2.7 Configuring access parameters

Requirement

- The services are enabled, e.g. Internet.
- The following access data is known from your DSL provider:
  - User name and password for ADSL access
  - VCI / VPI
  - Encapsulation

Configuring ADSL

1. Click "Interfaces" > "DSL" in the navigation panel

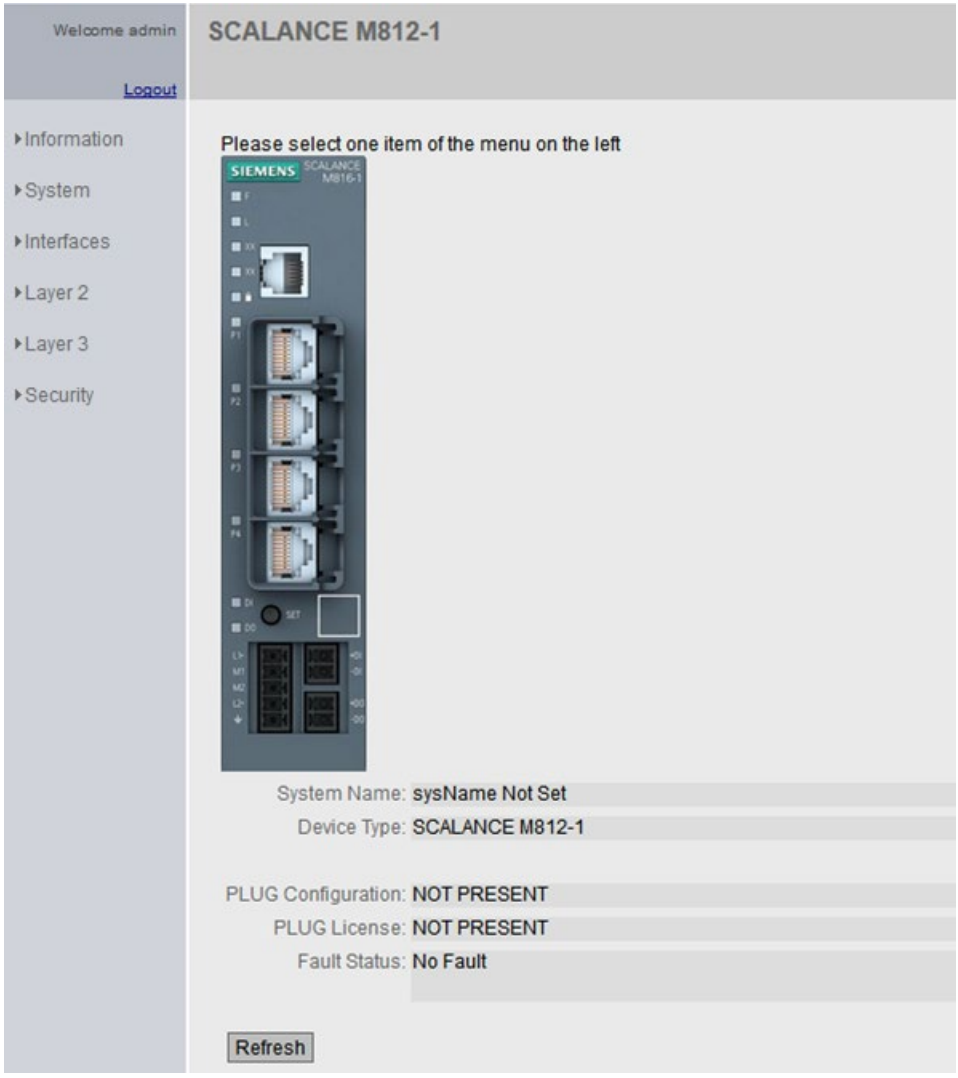


2. Select Enable DSL Interface".
3. Disable "Enable PPPoE Passthrough" to set up the access data for the SCALANCE M81x. The connected devices can use this DSL connection.

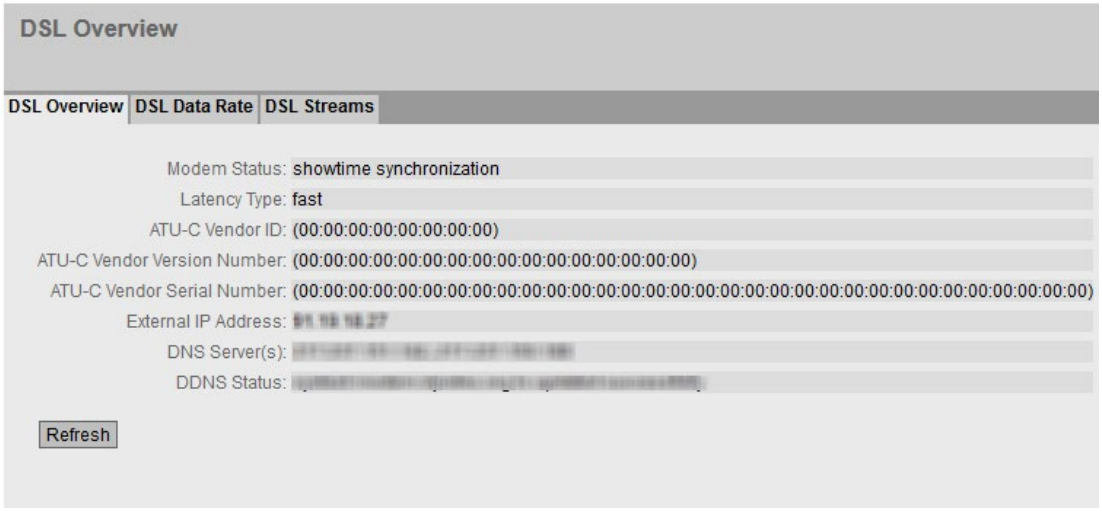
   If "Enable PPPoE Passthrough" is selected, the access data cannot be configured. In this case the SCALANCE M81x is used as a modem. Each individual connected device sends its access data to the SCALANCE M81x and establishes its own Internet connection.
4. Enter the user name and the password for the ADSL access.
5. Enter the settings for VCI / VPI. You will receive the settings from your DSL provider.
6. In "Encapsulation" select the required protocol.
7. Click "Set Values".

Result

The DSL connection is set up. The device connects to the Internet after approximately 30 seconds. You can check whether or not the connection is established in "Information" > "Start Page".



You will find more detailed information on the connection in "Information" > "DSL".



1.2.8 Setting the time

The date and time are kept on the SCALANCE M-800 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. There are a number of time servers on the Internet that can be used to obtain the current time precisely. 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

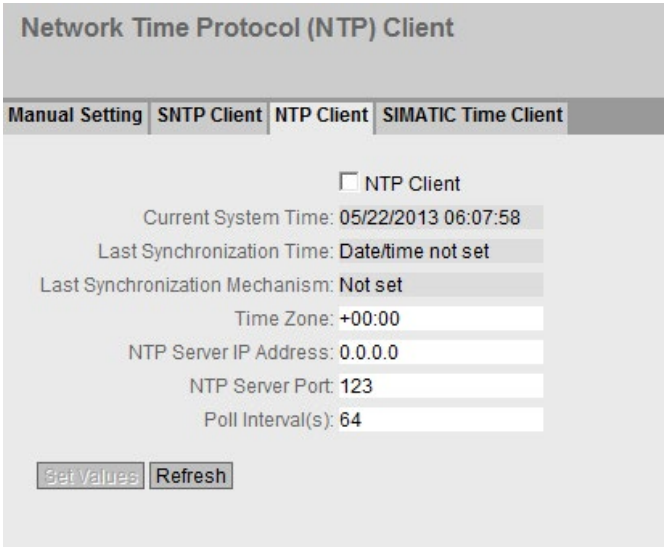
Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

Requirement

- The NTP server is reachable.
- The IP address of the NTP server is known.
  For this example, a time server (e.g. 192.53.103.108) of the Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig is used (Federal Institute of Physical and Technical Affairs - metrology institute).

Procedure

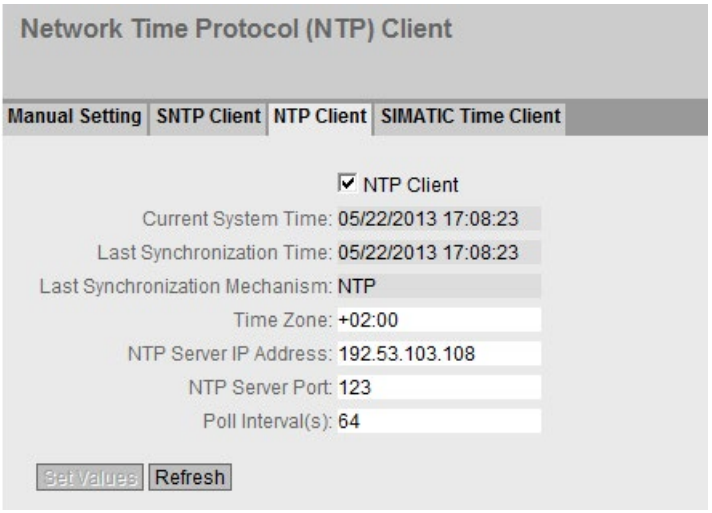
1. Click on "System" > "System Time" in the navigation area and on the "NTP Client" tab in the content area.



2. In "Time Zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. In "NTP Server IP Address", enter the IP address 192.53.103.108. It is not possible to enter the NTP address as a host name, for example timeserver.org.
4. If necessary, change the port in "NTP Server Port". As default, 123 is set.
5. In "Poll Interval (s)", enter the interval for synchronization. As default, 64 is set.
6. Select NTP Client".
7. Click "Set Values".

Result

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



1.2.9 Allow access

The firewall is enabled as default. This means that access from internal to external is not allowed.

You have the following options for allowing access:

- Allow globally

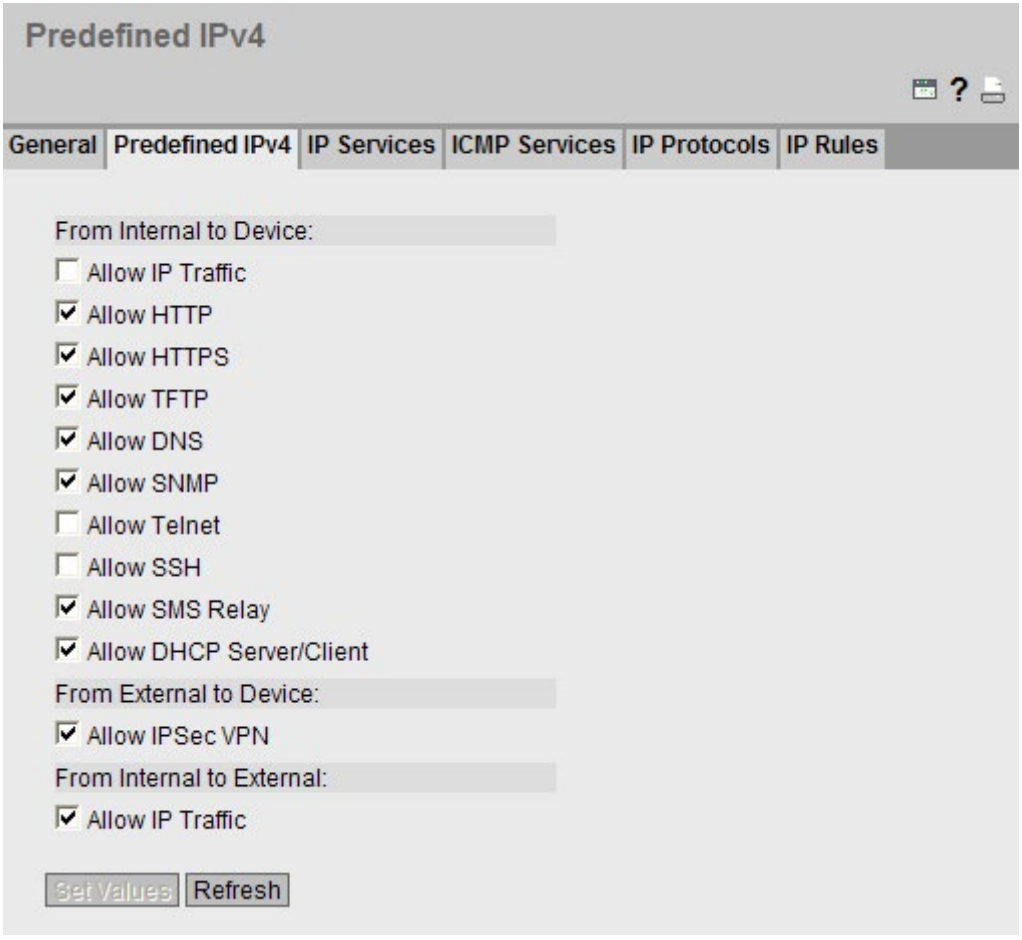
  Here, you use simple, predefined firewall rules. The enabled services are permitted for all nodes and full access is allowed in the specified direction. The firewall rule for the opposite direction is permitted by stateful packet inspection.

- Allow certain services

  Here, you define firewall rules that allow individual services for a single node or all services for the node for access to the station or network.
  In this example, configure the firewall rules that only allow the device with IP address 192.168.100.10 access to the entire Internet. For the access, the services HTTP (TCP port 80) and DNS (UDP port 53) are required.

Allow access to all

1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Under "From Internal to External", enable "Allow IP Traffic".
3. Click "Set Values".



Allow a specific device Internet access

Disabling predefined firewall rules

1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Under "From Internal to External", disable "Allow IP Traffic".

Create HTTP and DNS services

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. As "Service Name", enter for example "HTTP" and click "Create". A new entry is created in the table.
3. Configure HTTP with the following settings:

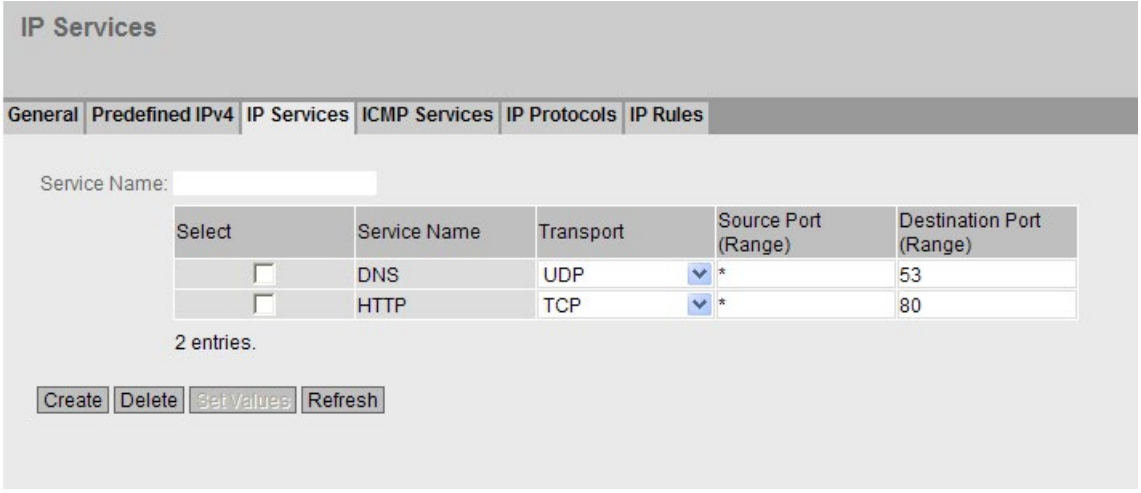
Transport	TCP
Destination Port (Range)	80 (standard port)

4. A new entry is created in the table.

   As "Service Name", enter for example "DNS" and click "Create".
5. Click "Set Values".
6. Configure DNS with the following settings:

Transport	UDP
Destination Port (Range)	53 (standard port)

7. Click "Set Values".



Only allow the IP service for a specific device

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.

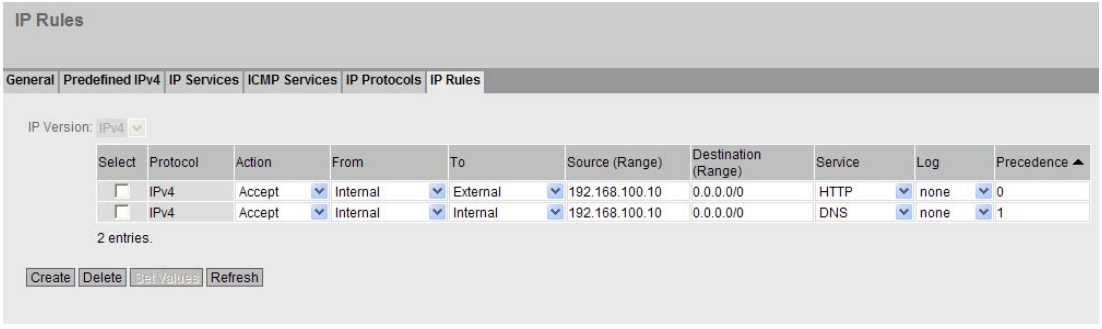
3. Configure the firewall rule for HTTP with the following settings:

Action	Accept
From	Internal
To	External
Source (Range)	192.168.100.10 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	HTTP

4. Click "Set Values".
5. Click "Create". A new entry is created in the table.
6. Configure the firewall rule for DNS with the following settings:

Action	Accept
From	Internal
To	Internal
Source (Range)	192.168.100.10 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	HTTP

7. Click "Set Values".



1.2.10 Setting up the DDNS hostname

DDNS stands for "dynamic domain name system". If you log the SCALANCE M-800 on to a DDNS service, the device can be reached from the external network under a hostname, e.g. "example.no-ip.com".

The DNS server of the DDNS service manages the assignment of IP address to hostname. The client informs the DNS server of its currently assigned IP address. The DNS name server registers the current hostname - IP address assignment and passes this on to other domain name servers in the Internet. This means that the SCALANCE M-800 can always be reached using its hostname.

Requirement

- User name and password that gives you the right to use the DDNS service
- Registered hostname, e.g. example.no-ip.com

Procedure

1. Click on "System" > "DNS" in the navigation area and on the "DDNS Client" tab in the content area.
2. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip.com
3. For "User name", enter the user name and for "Password / Password confirmation" the password that allows you to use
   the DDNS service. Your DDNS provider will give you this information.
4. Select Enable".

5. Click "Set Values".

Result

The DDNS client is activated. The DDNS client on the SCALANCE M-800 synchronizes the assigned IP address with the hostname registered in the DDNS service.

1.3 Connecting M826 with SHDSL

1.3.1 Out-of-the-box

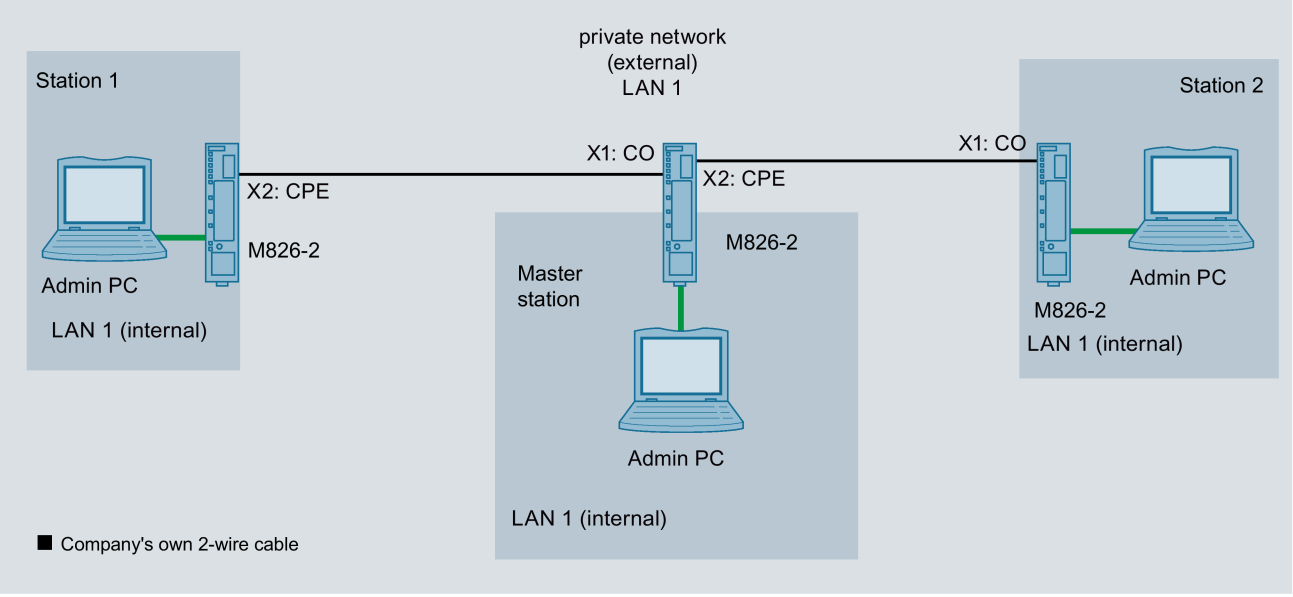
1.3.1.1 Procedure in principle

In this example three SCALANCE M826 devices that have the factory settings status are connected together directly.

As default, the SHDSL interfaces can establish a point-to-point connection with each other. For this connection, one SHDSL interface must be the CO and the other SHDSL interface the CPE.

When shipped, the SCALANCE M826 is in bridge mode. The difference between bridge and routing mode lies in the division into external and internal networks. In bridge mode there is no division. The SCALANCE M826 is a transparent bridge and connects network nodes that are in the same IP subnet. In this mode, the security features (IPsec VPN, firewall, NAT/NAPT) are not available.

Setup



The network nodes are in the same IP subnet (LAN1)

Master station - connection to SCALANCE M826

- In the test setup, in the master station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the master station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Station 1 and 2 - connection to SCALANCE M826

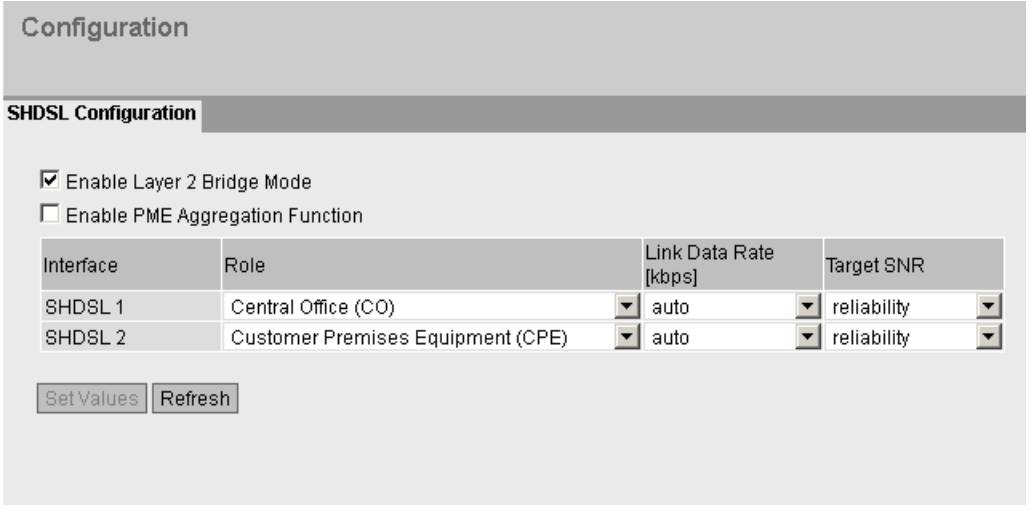
- In the test setup, in the station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Requirement

- All network nodes are in the same IP subnet.

Settings used

For the configuration example, the devices use the factory settings.



Required devices/components

Use the following components for setup:

- Connection to SHDSL
  - 3 x M826 (additional option: a suitably installed standard rail with fittings)
  - 3 x 24 V power supply with cable connector and terminal block plug
  - 2 x 2-wire cable with terminal block plugs
- 3 x PC each connected to an M826.

Configuration step

1. Setting up SCALANCE M826 and network (Page 49).

1.3.1.2 Setting up SCALANCE M826 and network

Note

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

Requirement

- All network nodes are in the same IP subnet.

Procedure

1. First unpack the M826 and check that it is undamaged.
2. Fit the power supply.

⚠ WARNING

Use safety extra-low voltage only

The SCALANCE M826 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 M826 power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

3. Wire X1 with X2, see Setup (Page 46).
4. Connect the devices to the local network via the Ethernet ports.
5. Turn the devices on. After connecting up, the fault LED (F) is lit red
6. Now, turn on the PC.

Result

The SCALANCE M826 devices are immediately operational without configuration. It may take some time before the devices have negotiated the connection parameters.

You cannot access the WBM since this requires an IP address. The IP address can be assigned by a DHCP server or with the Primary Setup Tool, see "Configuring SCALANCE M826 with PST (Page 52)".

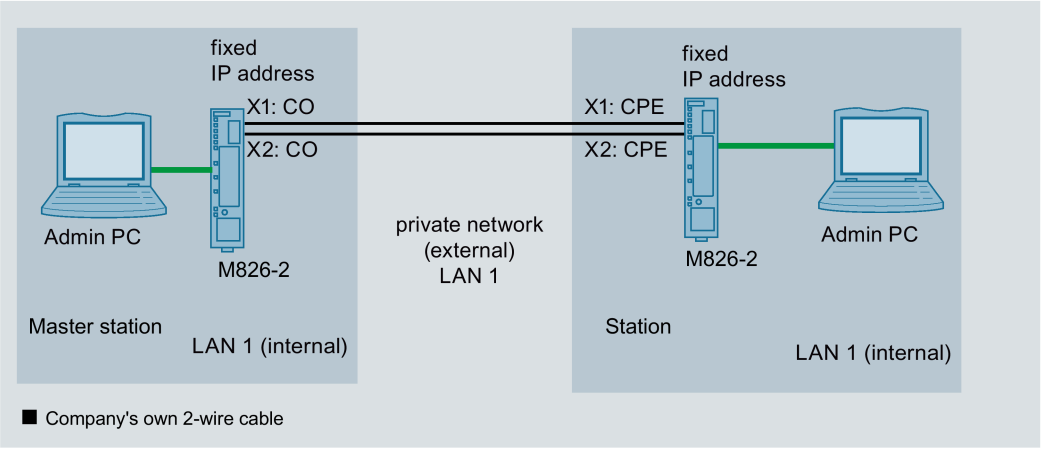
1.3.2 SHDSL in 4-wire mode

1.3.2.1 Procedure in principle

In this example, the two SHDSL interfaces will be put together to form a single connection with a higher transmission rate.

The SCALANCE M826 is in bridge mode. In this mode, the security features (IPsec VPN, firewall, NAT/NAPT) are not available.

Setup



The network nodes are in the same IP subnet

Master station - connection to SCALANCE M826

- In the test setup, in the master station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the master station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Station - connection to SCALANCE M-800

- In the test setup, in the station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Required devices/components

Use the following components for setup:

- Connection to SHDSL
  - 2 x M826 (additional option: a suitably installed standard rail with fittings)
  - 2 x 24 V power supply with cable connector and terminal block plug
- 2 x PC each connected to a SCALANCE M826.
- PST is installed on the PC.

Settings used

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

		IP address
Master station	M826	192.168.100.1 255.255.255.0
	Admin PC	192.168.100.20 255.255.255.0
Station	M826	192.168.100.10 255.255.255.0
	Admin PC	192.168.100.40 255.255.255.0

Steps in configuration

The following steps are necessary to configure the 4-wire operation

1. Setting up SCALANCE M826 and network (Page 52)
2. Configuring the SCALANCE M826 with the PST (Page 52)
3. Launching Web Based Management (Page 54)
4. Logging in to Web Based Management (Page 56)
5. Configuring SCALANCE M826

   The steps are the same for both devices, the only difference being the settings.
   - Specifying device information (Page 57)
   - Setting the time (Page 58)
   - Configuring SHDSL (Page 60)

1.3.2.2 Setting up SCALANCE M826 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 M826 and check that it is undamaged.
2. Fit the power supply.

⚠ WARNING

Use safety extra-low voltage only

The SCALANCE M826 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 M826 power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

3. Wire up the M826, see Setup (Page 50).
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.

1.3.2.3 Configuring the SCALANCE M826 with the PST

Requirement

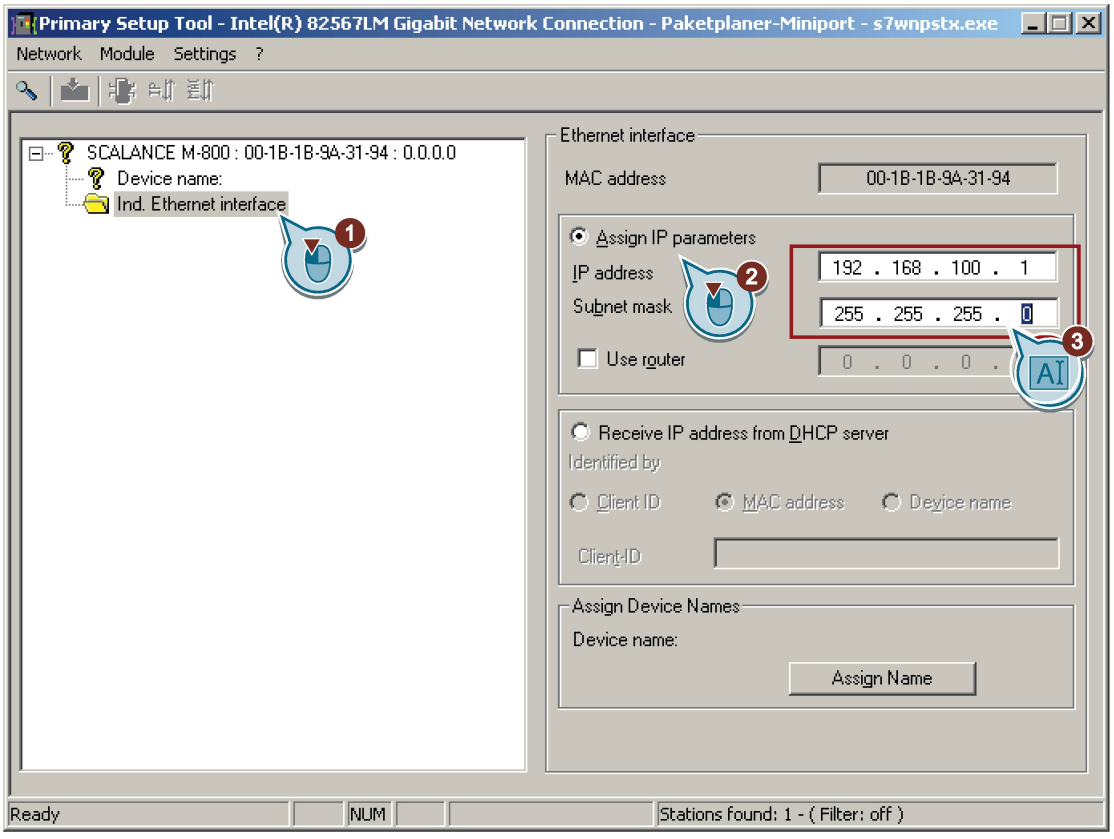
- The devices are in the same IP subnet.
- The IP addresses are unique.

Procedure

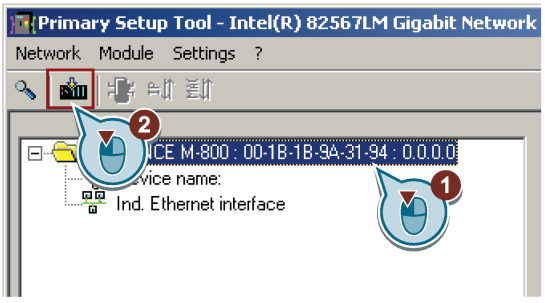
1. Start the Primary Setter Tool with "Start > SIMATIC > Primary Setup Tool".

   If several network adapters are installed in the PC, select the network adapter connected to the M826 in "Settings > Network adapter".
2. Click on the magnifier in the toolbar to start the search. Following the search, the M826 is listed in the PST.

3. Enter the values assigned to the M826 from the "Settings used (Page 50)" table.



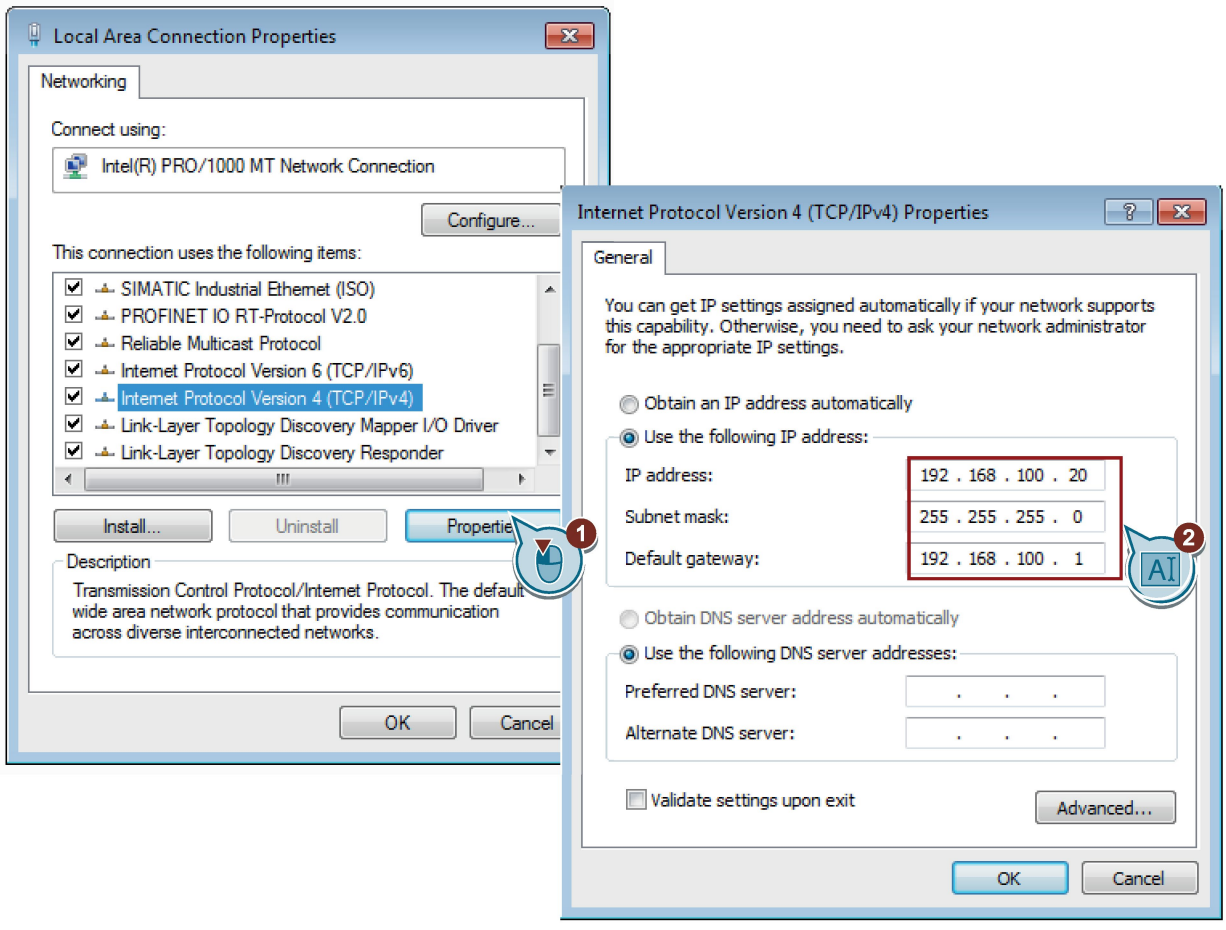
4. Transfer the IP address.



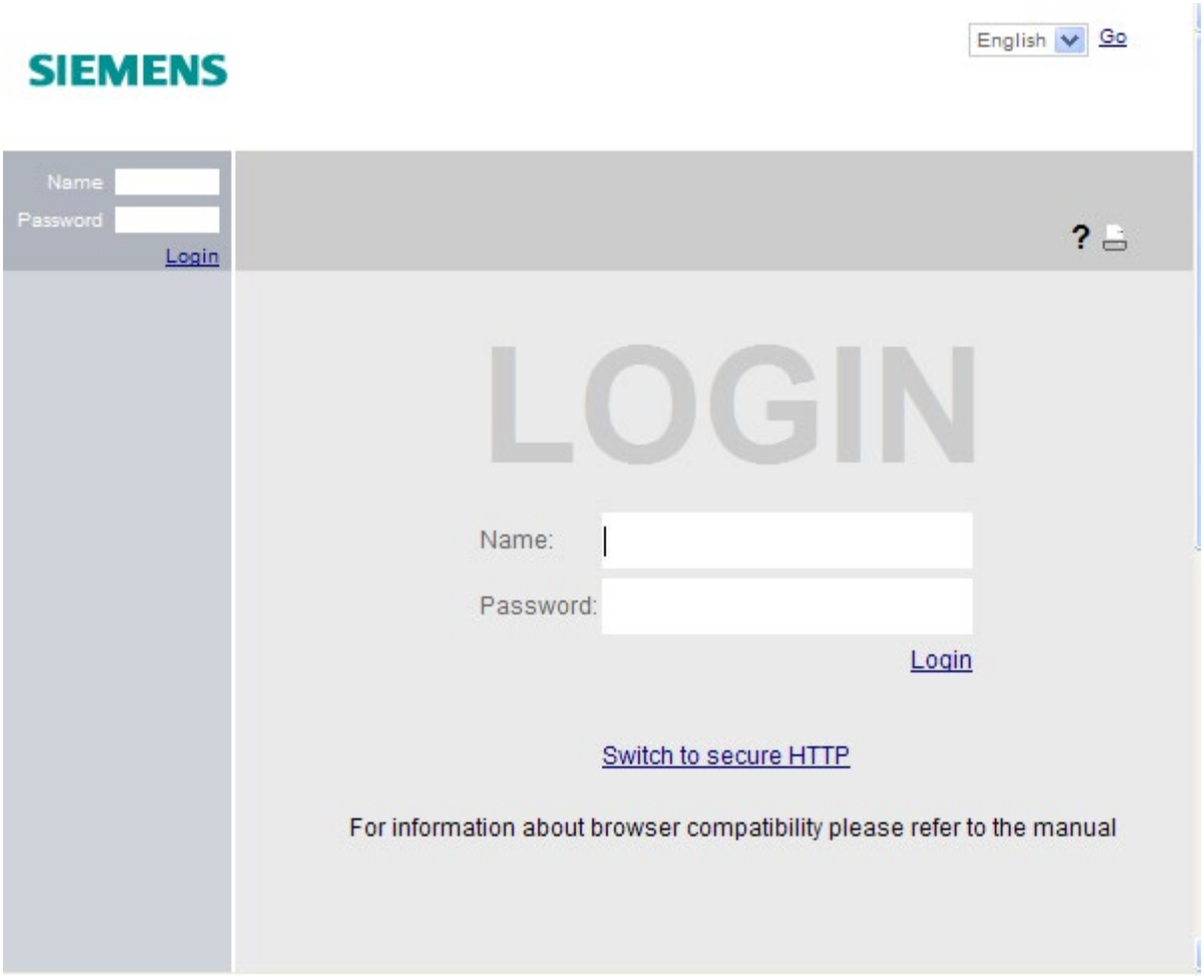
1.3.2.4 Launching Web Based Management

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 assigned to the Admin PC from the "Settings used (Page 50)" table.



6. Confirm the dialogs with "OK" and close the Control Panel.
7. Enter the IP address assigned to the M826 from the "Settings used (Page 50)" table in the address box of the Web browser. If there is a problem-free connection to the device, the login page of Web Based Management (WBM) is displayed.

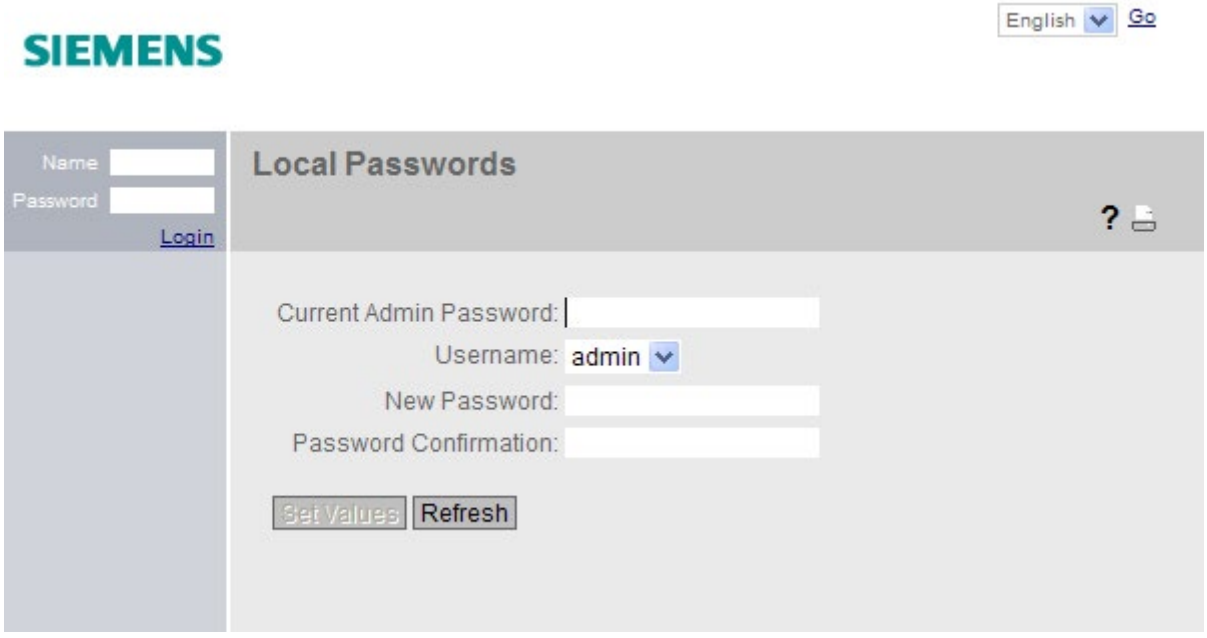


1.3.2.5 Logging in to Web Based Management

Procedure

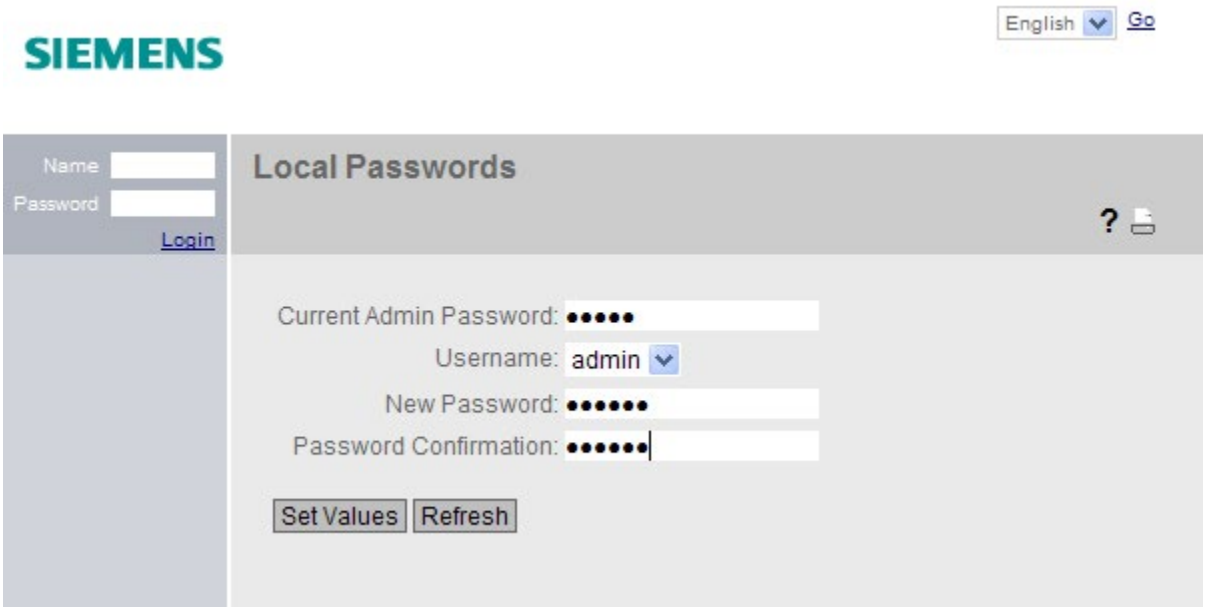
1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password.

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



3. In "Username", select the user "admin".
4. Enter the default password "admin" in "Current Admin Password".
5. Specify the new password in "New Password".

6. Repeat the password in "Password Confirmation" to confirm it. The entries must match.



7. Click the "Set Values" button.

Result

The password for the "admin" user is changed. The changes take immediate effect.

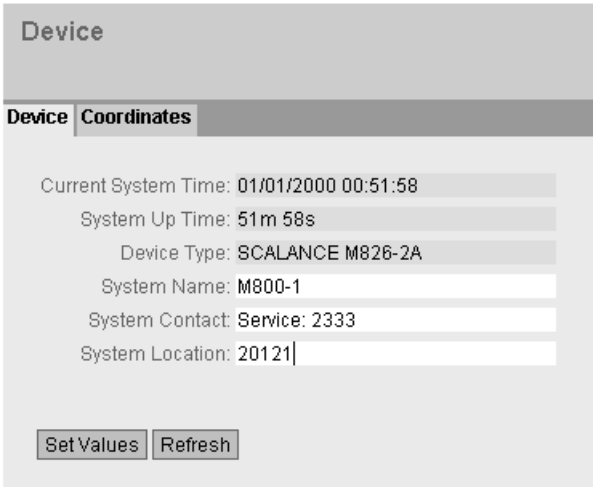
1.3.2.6 Specifying device information

To allow better identification of the SCALANCE M826, specify general device information.

Procedure

1. Click "System" > "General" in the navigation panel and on the "Device" tab in the content area.
2. For "System Name" enter a system name for the device, for example "M800-1" for the master station and "M800-2" for the station.
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 M826 has been specified.

1.3.2.7 Setting the time

The date and time are kept on the SCALANCE M-800 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

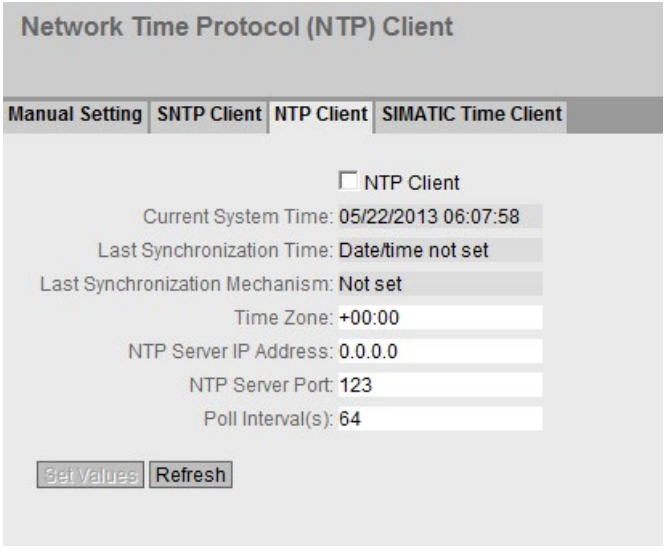
Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

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

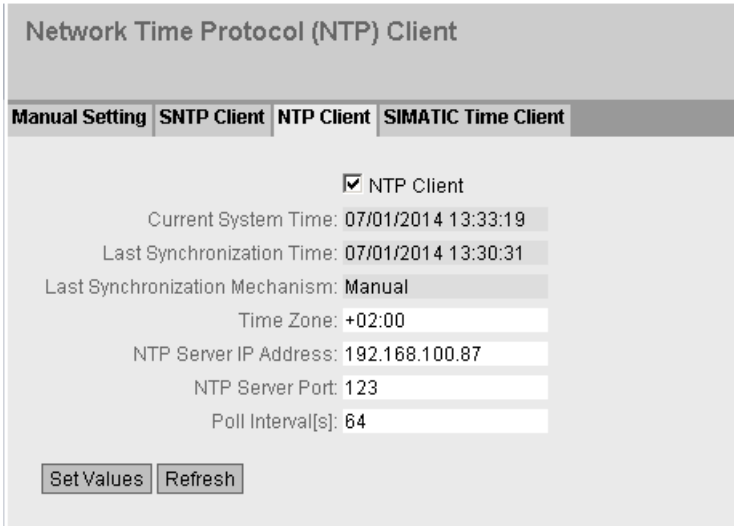
1. Click on "System" > "System Time" in the navigation area and on the "NTP Client" tab in the content area.



2. In "Time Zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. In "NTP Server IP Address", enter the IP address 192.168.100.87. It is not possible to enter the NTP address as a host name.
4. If necessary, change the port in "NTP Server Port". As default, 123 is set.
5. In "Poll Interval (s)", enter the interval for synchronization. As default, 64 is set.
6. Select NTP Client".
7. Click "Set Values".

Result

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



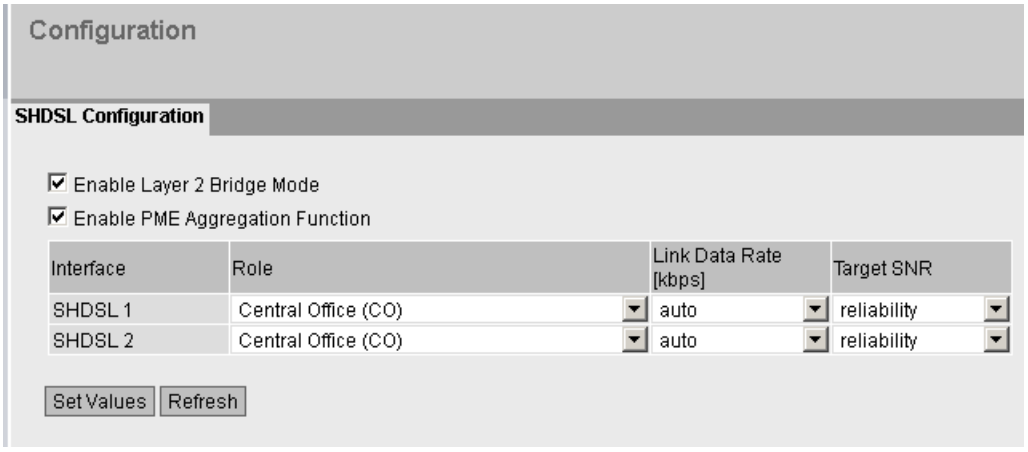
1.3.2.8 Configuring SHDSL

Procedure

1. Click "Interfaces" > "SHDSL" in the navigation panel
2. Leave "Enable Layer2 Bridge Mode" selected.
3. Select Enable PME Aggregation Function". When enabled, the SHDSL interfaces or the 2-wire cables are put together to form a single connection with a higher transmission rate.
4. Specify the role of the interfaces. The two interfaces need to have the same role on both devices.

M826 in the master station	X1	Central Office (CO)
	X2	Central Office (CO)
M826 in the station	X1	Customer Premises Equipment (CPE)
	X2	Customer Premises Equipment (CPE)

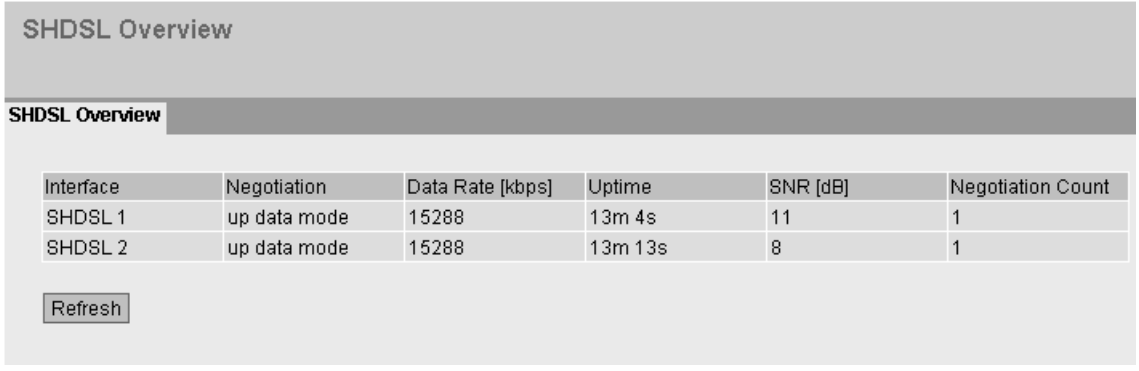
5. For "Link Data Rate" select auto" and for "Target SNR Ration" select "reliability".
6. Click "Set Values".



Result

The SHDSL connection is set up. The devices negotiate the connection parameters. This means that the devices use the transmission rate at which the data can be sent and received reliably.

You will find more detailed information on the connection in "Information" > "SHDSL".



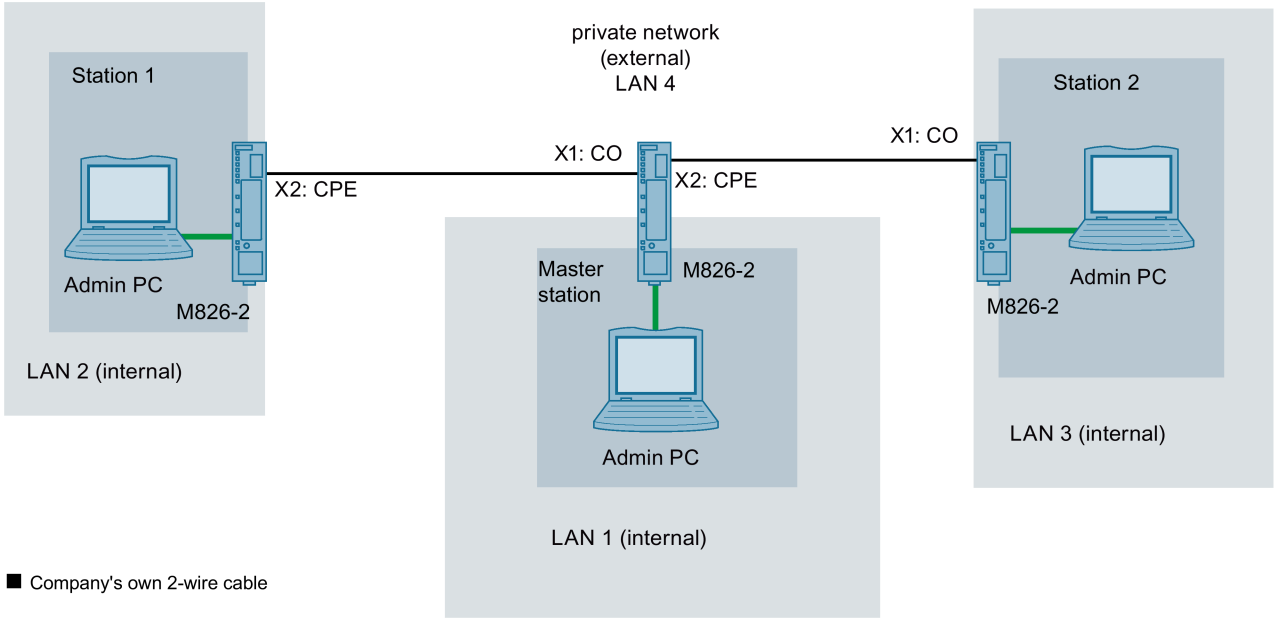
1.3.3 In routing mode

1.3.3.1 Procedure in principle

In this example, three different IP subnets will be interconnected via the SCALANCE M826. For this connection, there must be a one SHDSL interface of a device in the role of CO and the other in the role of CPE. Since the SCALANCE M826 devices operate in routing mode, there is a division into external and internal networks. This means that the SHDSL interfaces and the Ethernet interfaces are located in different IP subnets.

In this mode, the security functions (IPsec VPN, firewall, NAT/NAPT) are available.

Setup



The network nodes are in different IP subnets.

Master station - connection to SCALANCE M826

- In the test setup, in the master station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the master station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Station 1 and 2 - connection to SCALANCE M826

- In the test setup, in the station, a network node is implemented by an Admin PC connected to an Ethernet interface of the M826.
  - Admin PC: represents a node of the station
- Connection to the private network:
  - Cable connection via the SHDSL interface of the M826 on company owned 2-wire cable.

Required devices/components

Use the following components for setup:

- Connection to SHDSL
  - 3 x M876 (additional option: a suitably installed standard rail with fittings)
  - 3 x 24 V power supply with cable connector and terminal block plug
- 3 x PC each connected to an M826.
- PST is installed on the PC.

Settings used

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

		Interface		IP address
Master station	M826	SHDSL (external)	Vlan 2	192.168.184.2 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.100.1 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.100.20 255.255.255.0
Station 1	M826	SHDSL (external)	Vlan 2	192.168.184.22 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.11.2 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.11.40 255.255.255.0
Station 2	M826	SHDSL (external)	Vlan 2	192.168.184.42 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.50.2 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.50.40 255.255.255.0

Steps in configuration

1. Setting up SCALANCE M826 and network (Page 64).
2. Configuring the SCALANCE M826 with the PST (Page 65)
3. Launching Web Based Management (Page 67)
4. Logging in to Web Based Management (Page 69)
5. Configuring SCALANCE M826.

   The steps are the same for all devices, the only difference being the settings.

   – Specifying device information (Page 70)
   – Setting the time (Page 71)
   – Creating IP subnets (Page 73)
   – Configuring SHDSL (Page 75)
   – Configuring routes (Page 77)
   – Allow access (Page 78)

1.3.3.2 Setting up SCALANCE M826 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 M826 and check that it is undamaged.
2. Fit the power supply.

⚠ WARNING

Use safety extra-low voltage only

The SCALANCE M826 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 M826 power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

3. Wire up the M826, see Setup (Page 62).
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.

1.3.3.3 Configuring the SCALANCE M826 with the PST

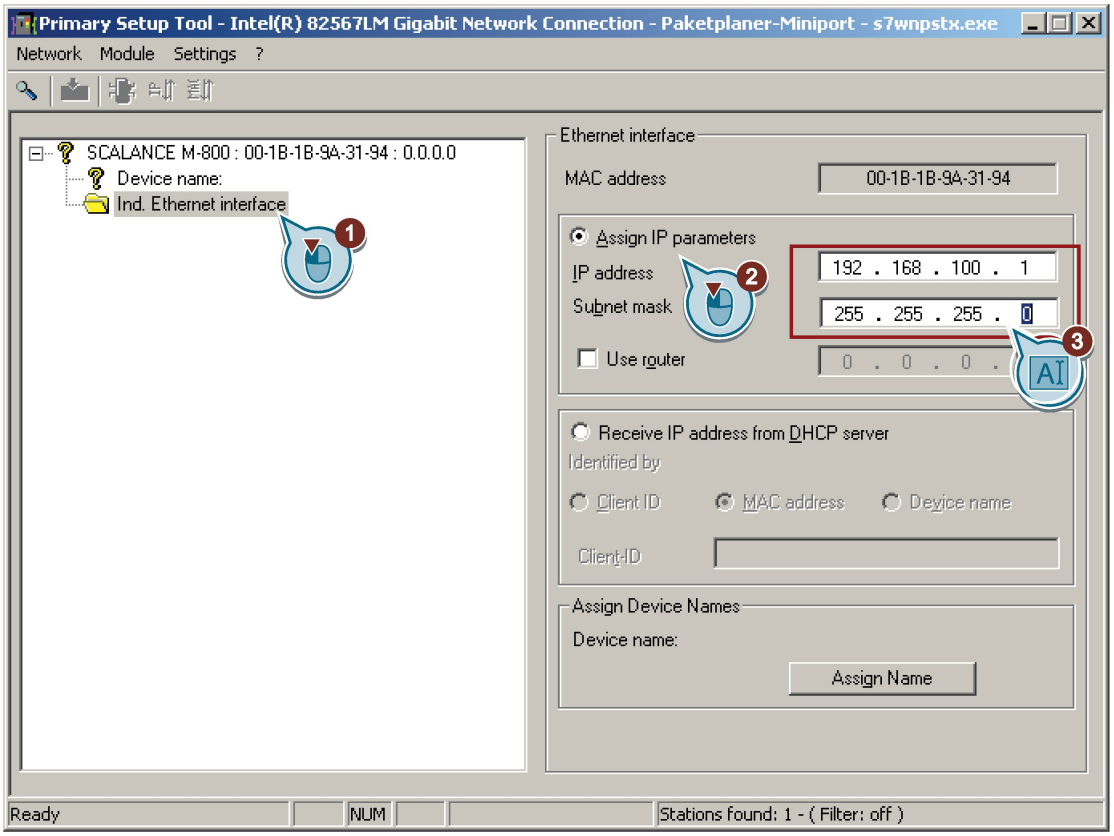
Requirement

- The IP addresses within the IP subnet are unique.

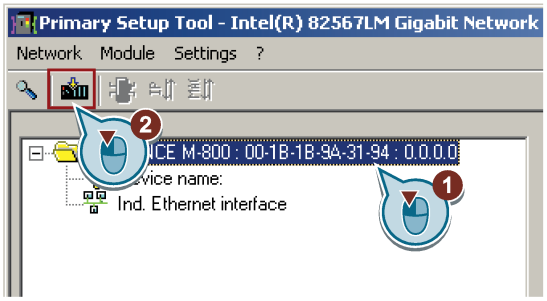
Procedure

1. Start the Primary Setter Tool with "Start > SIMATIC > Primary Setup Tool".

   If several network adapters are installed in the PC, select the network adapter connected to the M826 in "Settings > Network adapter".
2. Click on the magnifier in the toolbar to start the search. Following the search, the M826 is listed in the PST.
3. Enter the values assigned to the M826 from the "Settings used (Page 62)" table.



4. Transfer the IP address.

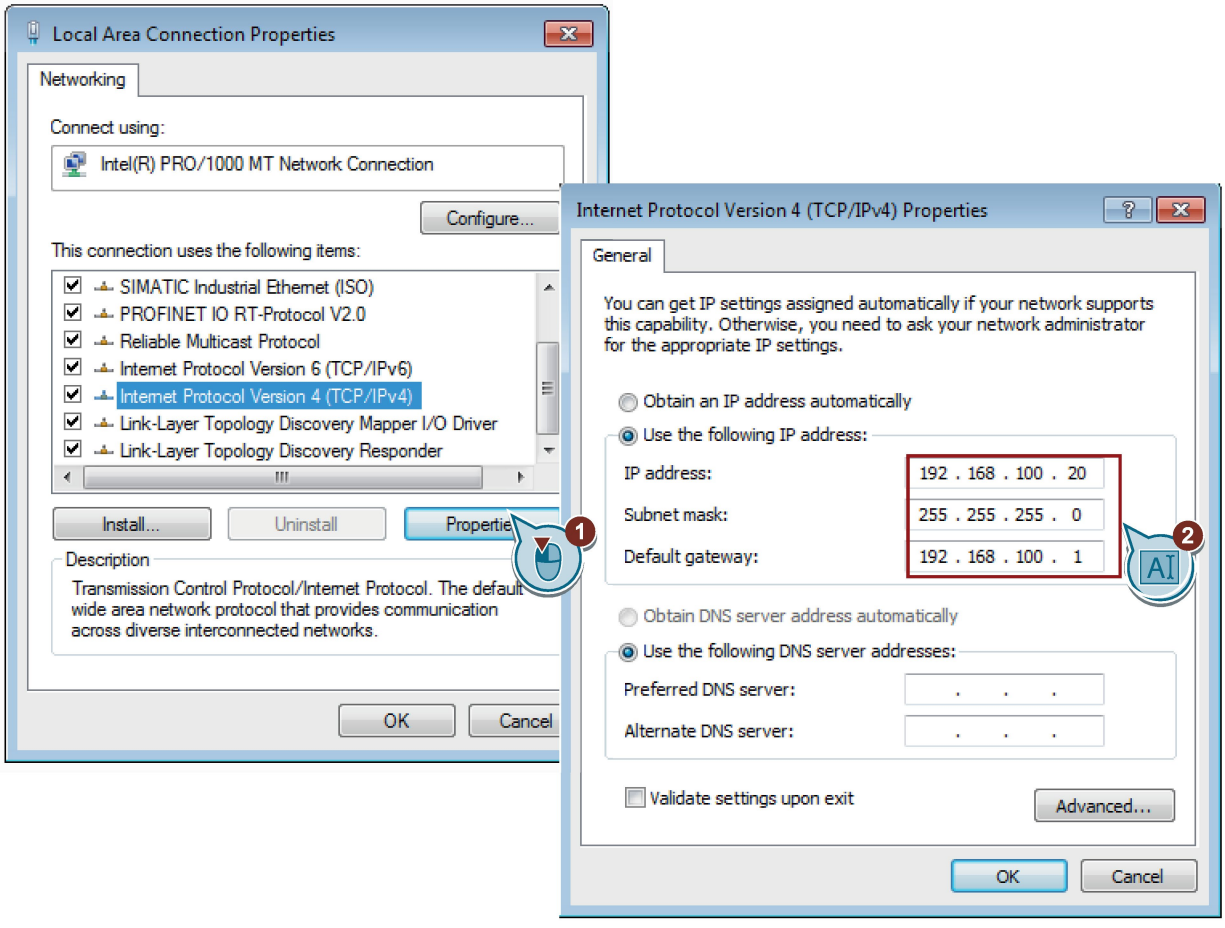


1.3.3.4 Launching Web Based Management

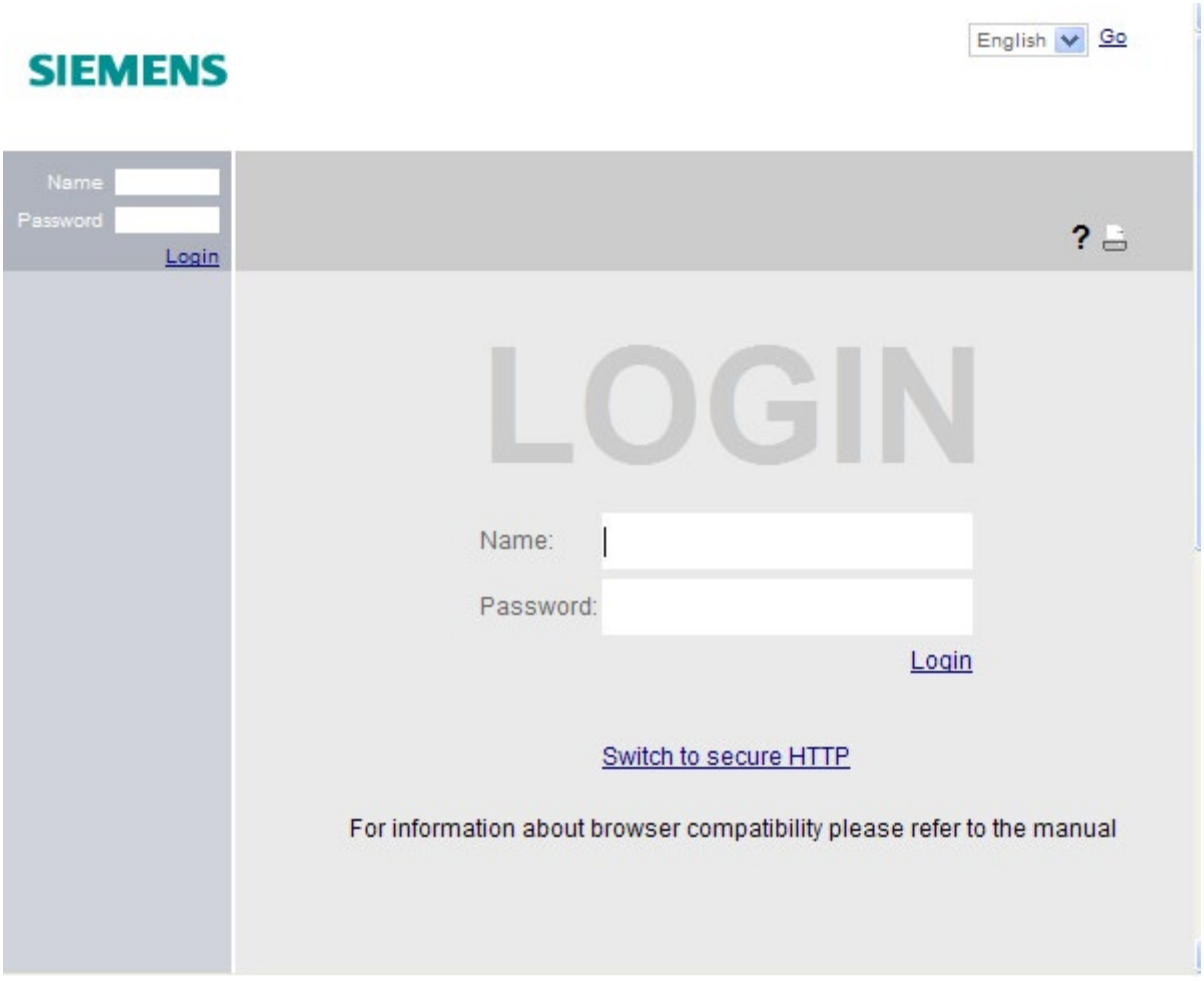
Procedure

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. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.
4. Enter the values assigned to the Admin PC from the "Settings used (Page 62)" table.

   As default gateway, enter the internal IP address (Vlan 1) of the SCALANCE M826.



5. Confirm the dialogs with "OK" and close the Control Panel.
6. Enter the IP address (vlan 1) assigned to the M826 from the table "Settings used (Page 62)" in the address box of the Web browser. If there is a problem-free connection to the device, the login page of Web Based Management (WBM) is displayed.

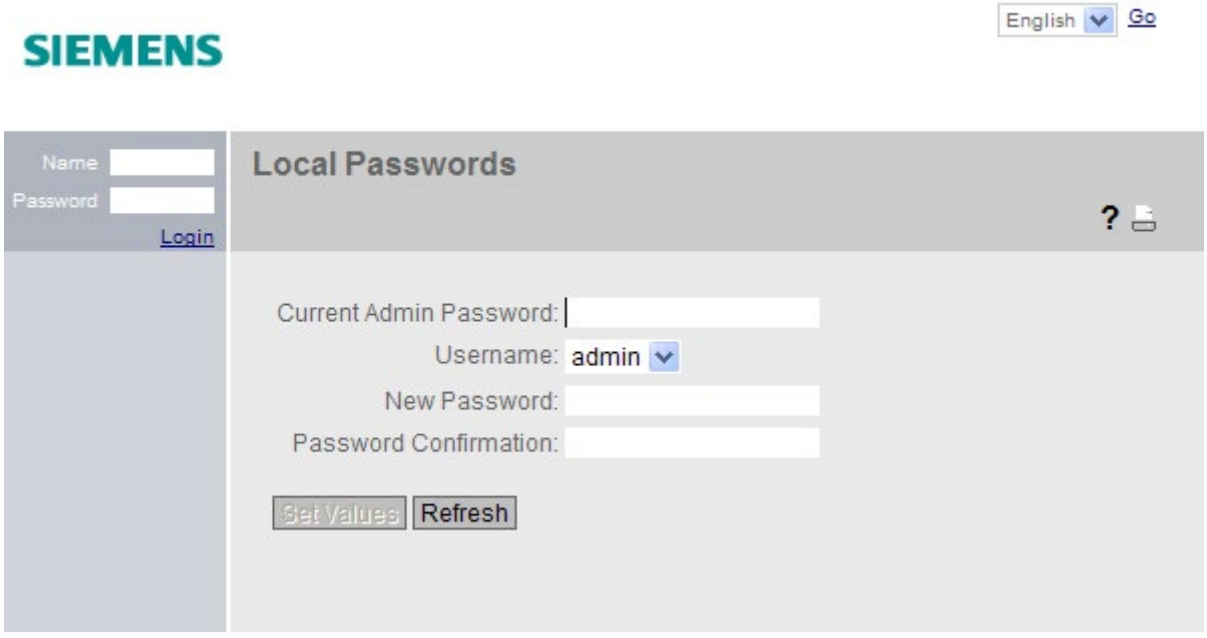


1.3.3.5 Logging in to Web Based Management

Procedure

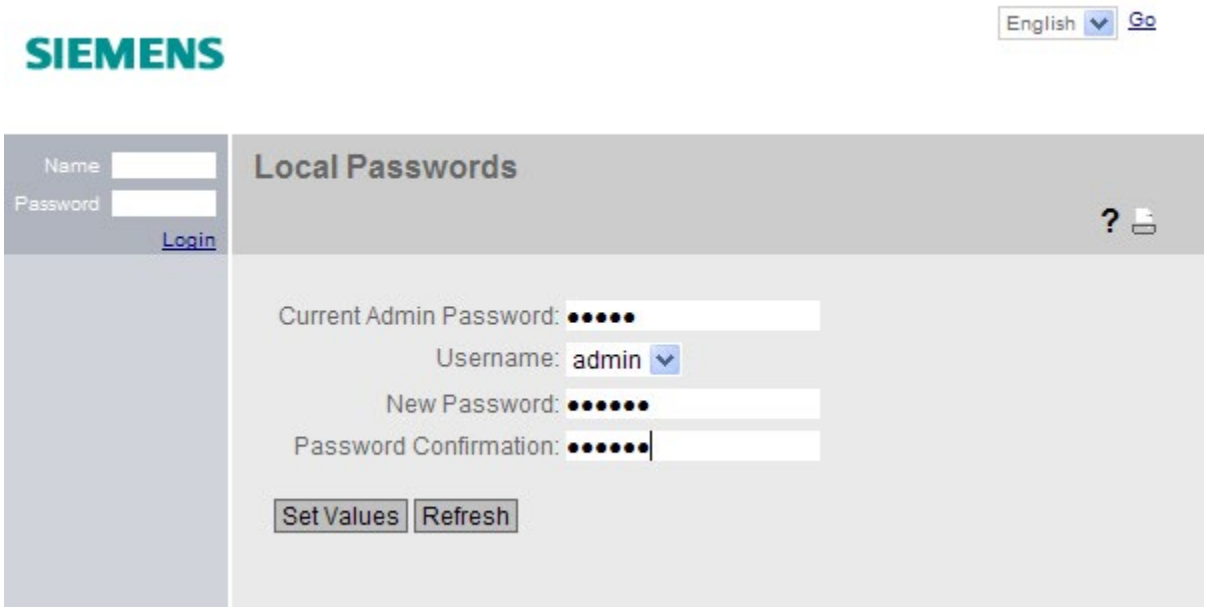
1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password.

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



3. In "Username", select the user "admin".
4. Enter the default password "admin" in "Current Admin Password".
5. Specify the new password in "New Password".

6. Repeat the password in "Password Confirmation" to confirm it. The entries must match.



7. Click the "Set Values" button.

Result

The password for the "admin" user is changed. The changes take immediate effect.

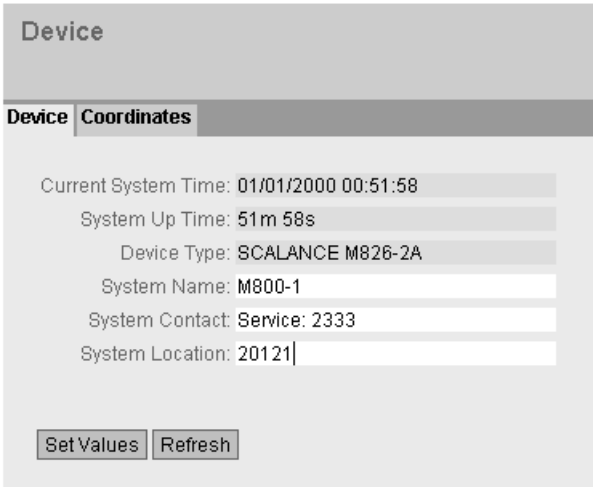
1.3.3.6 Specifying device information

To allow better identification of the SCALANCE M826, specify general device information.

Procedure

1. Click "System" > "General" in the navigation panel and on the "Device" tab in the content area.
2. For "System Name" enter a system name for the device, for example "M800-1" for the master station and "M800-2" for the station.
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 M826 has been specified.

1.3.3.7 Setting the time

The date and time are kept on the SCALANCE M-800 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

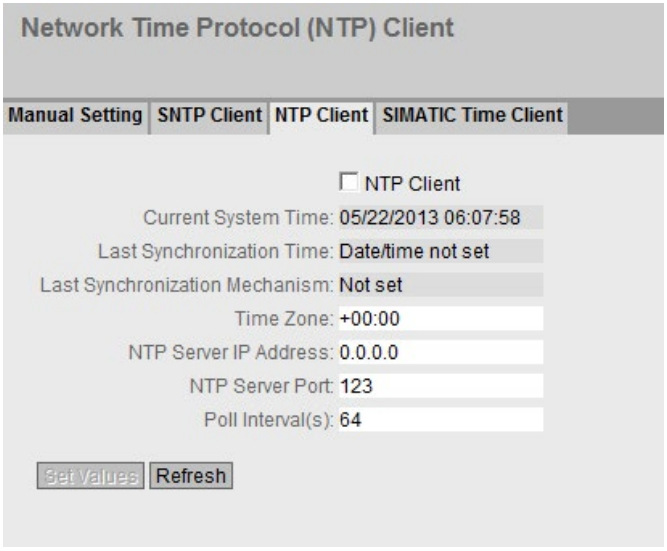
Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

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

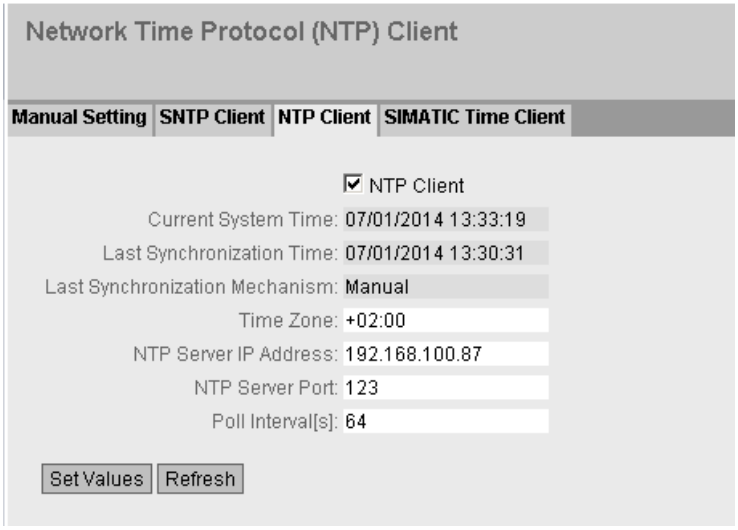
1. Click on "System" > "System Time" in the navigation area and on the "NTP Client" tab in the content area.



2. In "Time Zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. In "NTP Server IP Address", enter the IP address 192.168.100.87. It is not possible to enter the NTP address as a host name.
4. If necessary, change the port in "NTP Server Port". As default, 123 is set.
5. In "Poll Interval (s)", enter the interval for synchronization. As default, 64 is set.
6. Select NTP Client".
7. Click "Set Values".

Result

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



1.3.3.8 Creating IP subnet

In routing mode, the interfaces are handled differently.

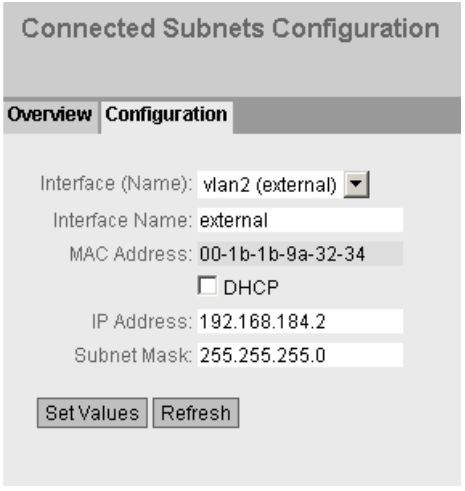
- Ethernet interface: Connection of the internal IP subnet (vlan 1)
- SHDSL interface: Connection of the external IP subnet (vlan 2)

The Ethernet interface or internal IP subnet has already been configured with the PST. For this configuration example, only the IP subnet for the SHDSL interface or for the external IP subnet needs to be configured. The same steps need to be taken on all devices.

Procedure

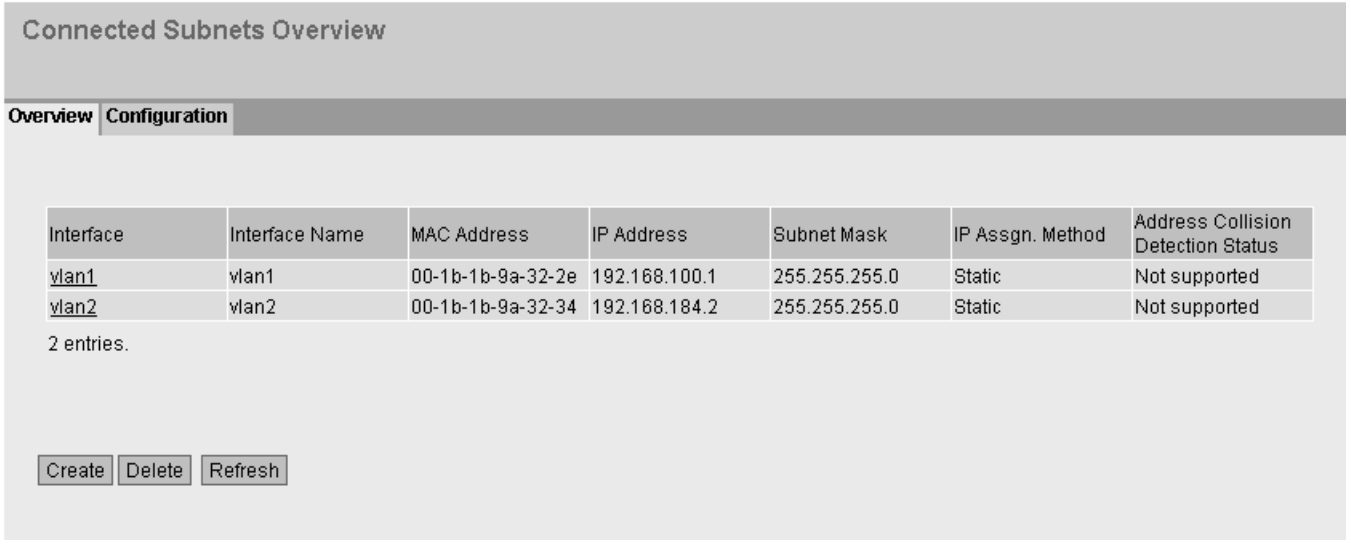
1. Click on "Layer 3" > "Subnets" in the navigation area and on the "Configuration" tab in the content area.
2. For "Interface" select "vlan 2".
3. For "Interface Name" you can enter a name.

4. Enter the value assigned to the M826 from the "Settings used (Page 62)" table.
5. Click "Set Values".



Result

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



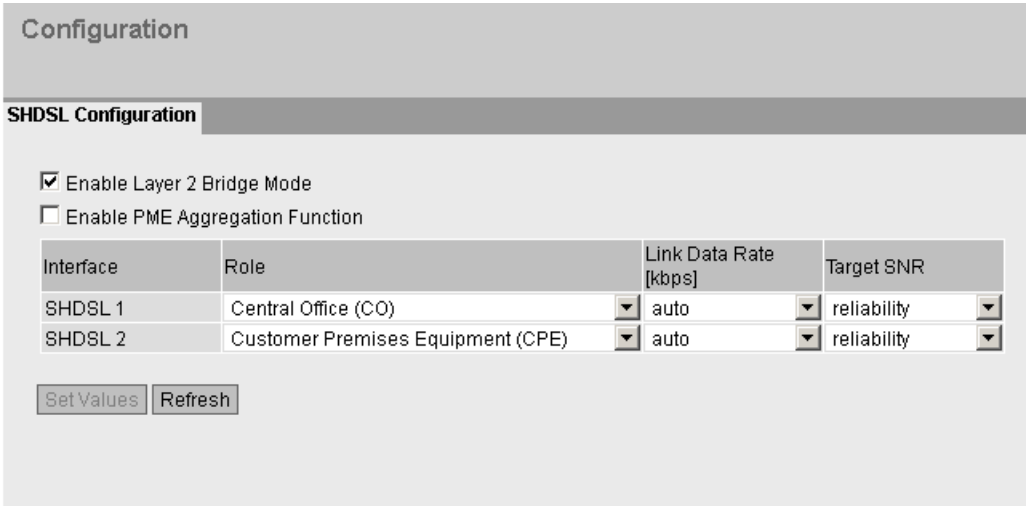
1.3.3.9 Configuring SHDSL

Procedure

1. Click "Interfaces" > "SHDSL" in the navigation panel
2. Specify the role of the interfaces

SHDSL 1 (X1)	Central Office (CO)
SHDSL 2 (X2)	Customer Premises Equipment (CPE)

3. For "Link Data Rate" select auto" and for "Target SNR Ration" select "reliability".
4. Click "Set Values".



5. Deselect "Enable Layer2 Bridge Mode" to set the routing mode. In this mode, the security functions (IPsec VPN, firewall, NAT/NAPT) are available again.

Result

The SHDSL connection is set up. The devices negotiate the connection parameters. This means that they use the transmission rate at which the data can be sent and received reliably. You will find more detailed information on the connection in "Information" > "SHDSL".

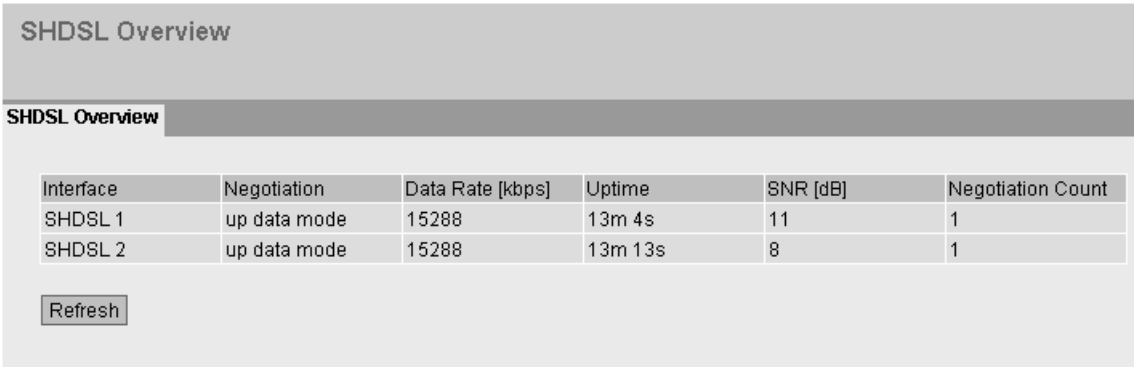


Figure 1-1 Overview of M826 in the master station

You can protect the data transfer additionally using the firewall and IPsec VPN.

1.3.3.10 Configuring routes

The master station and the stations are in different IP subnets. To allow the master station to communicate with the stations, the appropriate routes need to be created on the M826.

M826 in the master station: Configuring routes

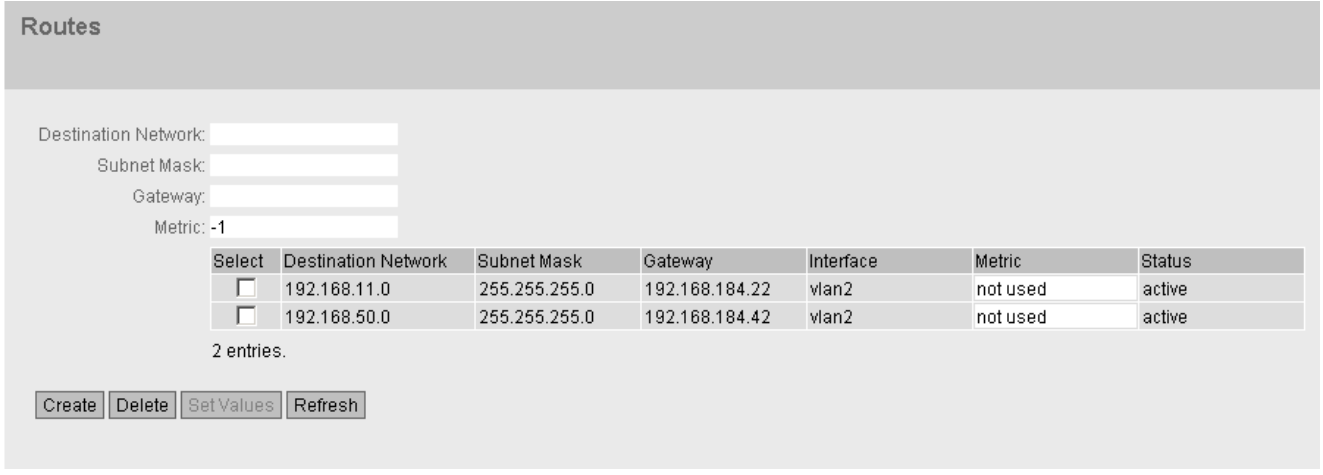
1. Click "Layer 3" > "Routes" in the navigation panel.
2. Configure the routes with the following settings:
   - Route to station 1

Destination Network	192.168.11.0
Subnetmask	255.255.255.0
Gateway	192.168.184.22 external IP address of the M826 in station 1
Metric	-1

   - Route to station 2

Destination Network	192.168.50.0
Subnetmask	255.255.255.0
Gateway	192.168.184.42 external IP address of the M826 in station 2
Metric	-1

3. When you have entered the values, click "Create".
4. To update the display, click "Refresh".



M826 in the stations: Configuring routes

1. Click "Layer 3" > "Routes" in the navigation panel.
2. Configure the route to the master station with the following settings:

Destination Network	192.168.100.0
Subnetmask	255.255.255.0
Gateway	192.168.184.2 external IP address of the M826 in the master station
Metric	-1

3. When you have entered the values, click "Create".
4. To update the display, click "Refresh".

Result

The routes have been created. The SCALANCE M826 in the master station can communicate with the stations.

Using the ping function, the communications connection can be tested. For example, can the Admin PC in station 1 be reached by the Admin PC in the master station?

1.3.3.11 Allow access

You have the following options for allowing access:

- Allow globally

  Here, you use simple, predefined firewall rules. The enabled services are valid for all nodes on the relevant interfaces. Full access is allowed for the specified direction.

  – vlan1: Allows access from the internal network to the device

  – vlan2: Allows access from the external network to the device

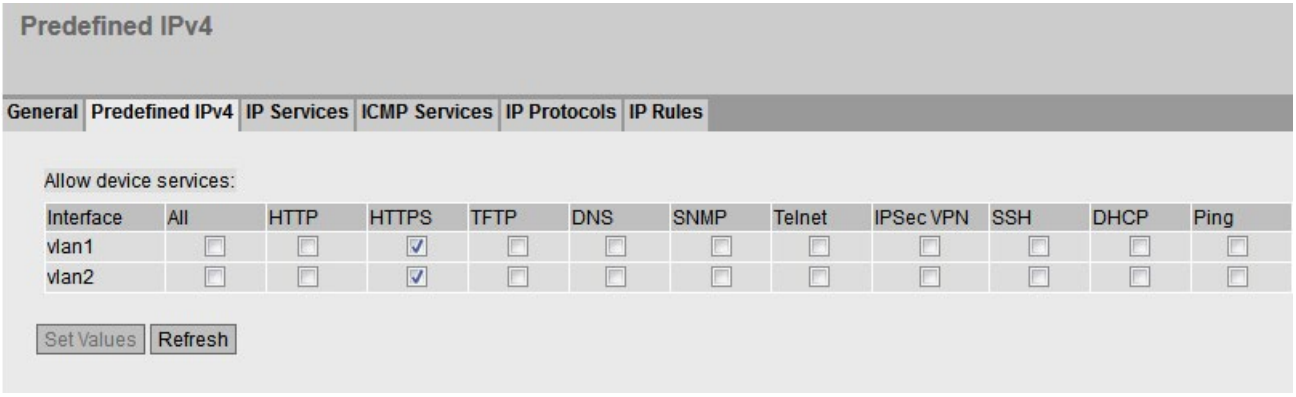
  The firewall rule for the opposite direction is permitted by stateful packet inspection.

- Allow certain services

  Here, you define firewall rules that allow individual services for a single node or all services for the node for access to the station or network.
  In this example, configure the firewall rule that only allows the device with IP address 192.168.100.20 access to the device. The service HTTP (TCP port 80) is required for access.

Example 1: Allow HTTPS access globally

1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Enable "HTTPS" for "vlan 1" and "vlan 2".
3. Click "Set Values".



Example 2: Allow a specific device HTTPS access

Disabling predefined firewall rules

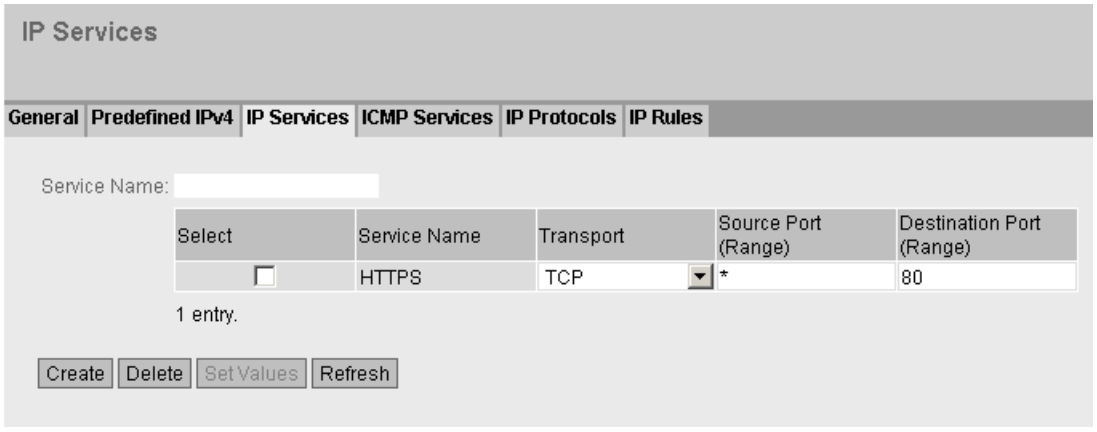
1. Click on "Security" > "Firewall" in the navigation area and on the "Predefined IPv4" tab in the content area.
2. Deactivate all services.

Create HTTPS IP service

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. As "Service Name", enter for example "HTTPS" and click "Create". A new entry is created in the table.
3. Configure HTTPS with the following settings:

Transport	TCP
Destination Port (Range)	80 (standard port)

4. Click "Set Values".

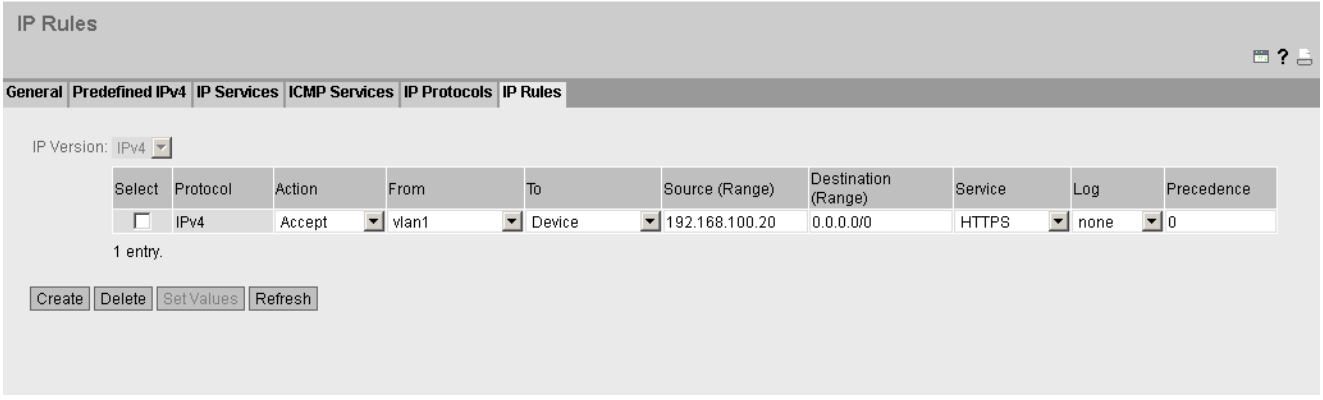


Allow only a specific device HTTPS access

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule for the created HTTPS service with the following settings:

Action	Accept
From	vlan1
To	Device
Source (Range)	192.168.100.20 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	HTTPS

4. Click "Set Values".



SCALANCE M-800 as DHCP server

2

If you want to use the device to manage the network configuration, you can use the device as a DHCP server. This allows IP addresses to be assigned automatically to the devices connected to the internal network.

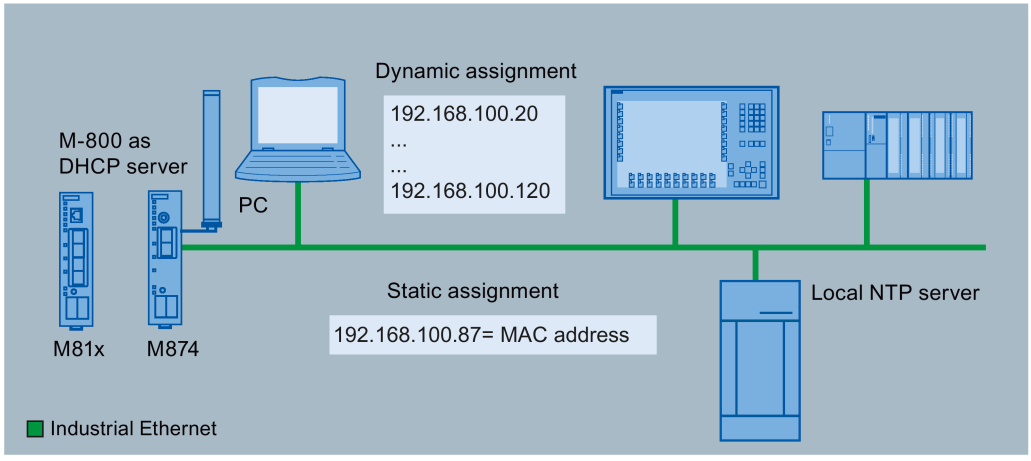
In this example, both static and dynamic IP address assignments are configured.

Note

DHCP client and DHCP server

The device can either be only a DHCP client or only a DHCP server.

SCALANCE M-800 as DHCP server



Required devices/components

- SCALANCE M-800 as DHCP server

  1 x M874, 1 x M812 or M816 (optionally also: a suitably installed standard rail with fittings)

- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC with which the SCALANCE M-800 is connected.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Setting used

In the configuration example, the SCALANCE M-800 has the following IP address setting:

- IP address 192.168.100.1
- Subnet mask: 255.255.255.0

Requirement

- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

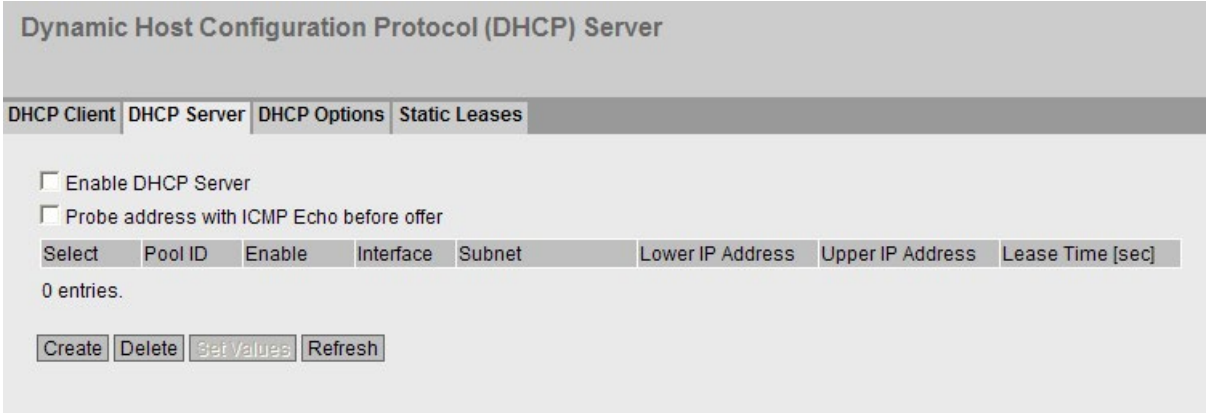
1. Configuring dynamic IP address assignment (Page 83)
2. Specifying DHCP options (Page 85)
3. Configuring static IP address assignment (Page 87)

2.1 Configuring dynamic IP address assignment

The devices whose MAC address or whose client ID was not specified specifically, are assigned a random IP address from a specified address range.

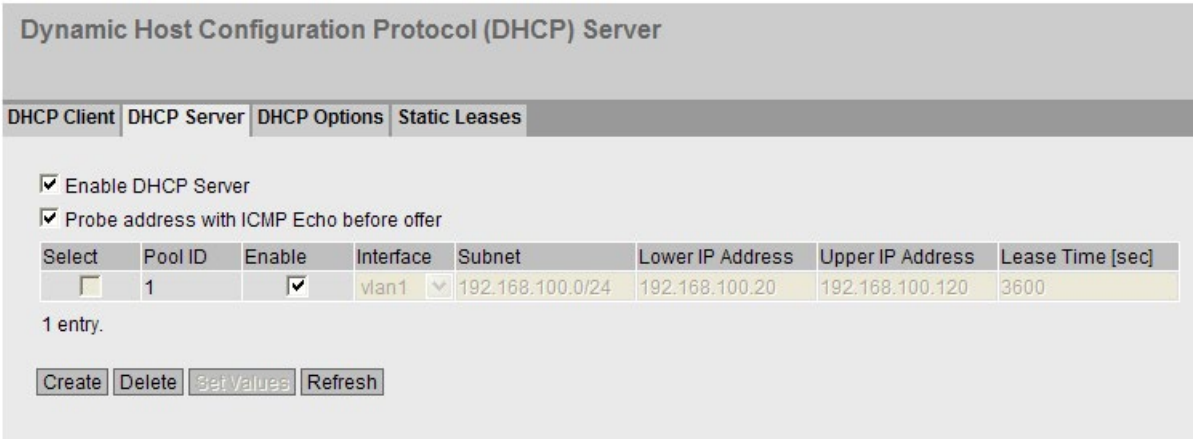
Procedure

1. Click on "System" > "DHCP" in the navigation area and on the "DHCP Server" tab in the content area.



2. Click "Create". A new row with a unique number (pool ID) is created in the table.
3. Enter the network address range in "Subnet". Since the device being used is operating both as a gateway and a DNS relay, the IP address 192.168.100.1 must be in the network address range. In this example the network address: 192.168.100.0/24 (= 192.168.100.0 / 255.255.255.0) is used.
4. In "Lower IP Address", enter the IP address 192.168.100.20 that specifies the start of the dynamic address band and that is located within the network address range.
5. In "Upper IP Address", enter the IP address 192.168.100.120 that specifies the end of the dynamic address band and that is located within the network address range.

6. Select the following:
   - "Enable" to use the address band
   - "Probe address with ICMP Echo before offer to activate the ping function. With this ping, the DHCP server checks whether or not the IP address has already been assigned.
   - "Enable DHCP Server to activate the DHCP server.
7. Click "Set Values".



Result

The DHCP server can assign up to 100 IP addresses from a set address band. This is only possible if the connected devices are configured so that they obtain the IP address from a DHCP server.

2.2 Specifying DHCP options

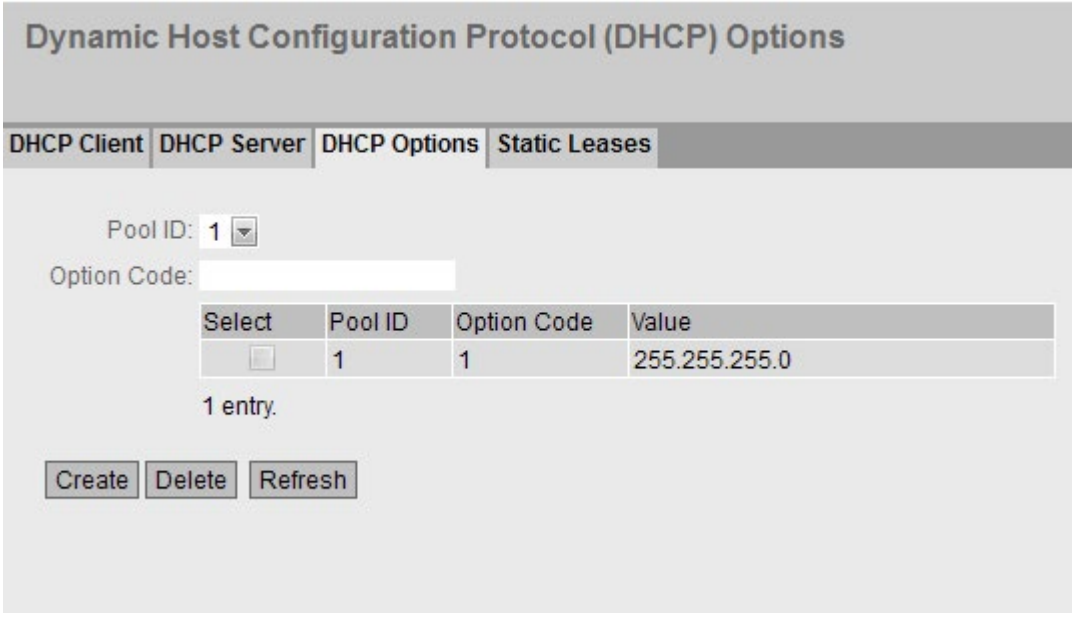
Further information can be transferred to the DHCP client using DHCP options. The various DHCP options are defined in RFC 2132.

In this example, the following DHCP options are created.

DHCP option		Information contained
1	Netmask	The subnet mask to match the IP address For this example the subnet mask is: 255.255.255.0
3	Default gateway	IP address of the default gateway Without this information, the DHCP client is only assigned an IP address by the DHCP server and it can only communicate with the nodes in the internal network.
6	DNS server	IP address of the DNS server Without this information, the DHCP client is not automatically assigned a DNS server. To allow name resolution, a DNS server must be known to the DHCP client. This can also be configured manually.
42	NTP server	IP address of the NTP server. In this example, the IP address of the NTP server (192.168.100.87) is transferred to the DHCP clients. The IP address is entered in hexadecimal notation. The IP address 192.168.100.87 corresponds to "C0A86457". So that the NTP server can always be reached at this IP address, the IP address is assigned to the MAC address, see section "Configuring static IP address assignment (Page 87)".

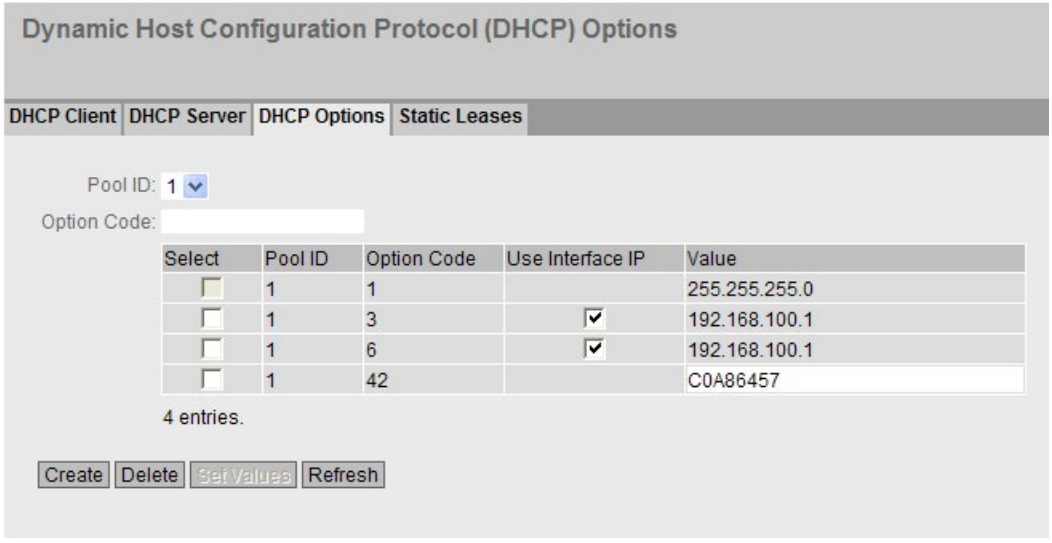
Procedure

1. Click on "System" > "DHCP" in the navigation area and on the "DHCP Options" tab in the content area.



2. In "Pool ID", select "1". Enter "1" in "Option Code".
3. Click "Create". A new row is created in the table. The subnet mask 255.255.255.0 is entered automatically.
4. Click "Set Values".
5. Enter "3" in "Option Code". Click "Create". A new row is created in the table.
6. Since the device will be used as a gateway, enable "Use Interface IP". Click "Set Values". The IP address of the device is entered automatically as the value.
7. Enter "6" in "Option Code". Click "Create". A new row is created in the table.
8. Since the device will be used as a DNS relay, enable "Use Interface IP". Click "Set Values". The IP address of the device is entered automatically as the value.
9. Enter "42" in "Option Code".
10. Click "Create". A new row is created in the table.
11. In "Set Values", enter the IP address of the NTP server in hexadecimal notation.

Result



The DHCP options are configured. If a DHCP client requests an IP address, in addition to the host IP address, it also receives the information entered in the DHCP options.

2.3 Configuring static IP address assignment

For nodes in permanent operation, static IP address assignment should be preferred, for example for a local NTP server. The IP address of the NTP server is used in the DHCP option.

As long as the NTP server can be reached at the same IP address, the DHCP option will work correctly. If the IP address changes, the DHCP option contains incorrect information.

For the example, the IP address is assigned to the MAC address of the NTP server. This means that the NTP server always has the same IP address.

In this configuration example, the NTP server can be reached with the following IP address setting:

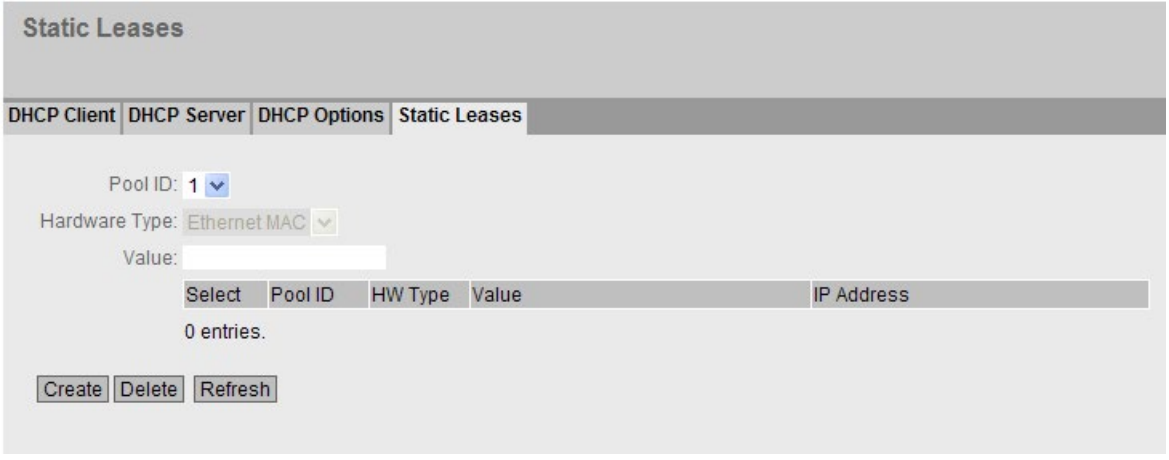
IP address	Subnet mask
192.168.100.87	255.255.255.0

Requirement

- The NTP server obtains the IP address from a DHCP server and identification is based on the MAC address.

Procedure

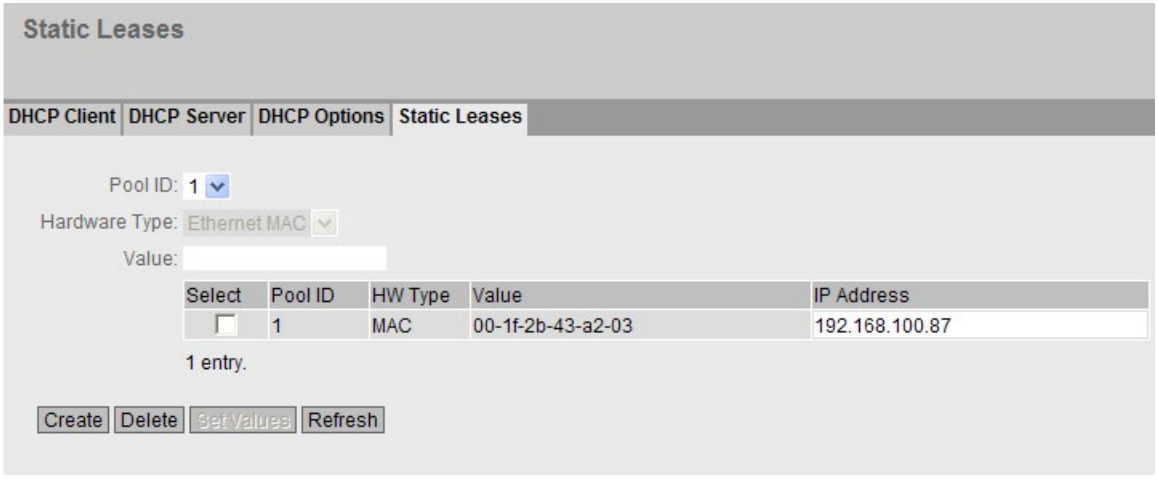
1. Click on "System" > "DHCP" in the navigation area and on the "Static Leases" tab in the content area.



2. In "Pool ID", select "1".
3. For "Hardware Type", select "Ethernet MAC".
4. In "Client ID", enter the MAC address of the NTP server.
5. Click "Create". A new row is created in the table.
6. In "IP Address", enter the IP address of the NTP server.
7. Click "Set Values".

Result

The NTP server always has the IP address 192.168.100.87.



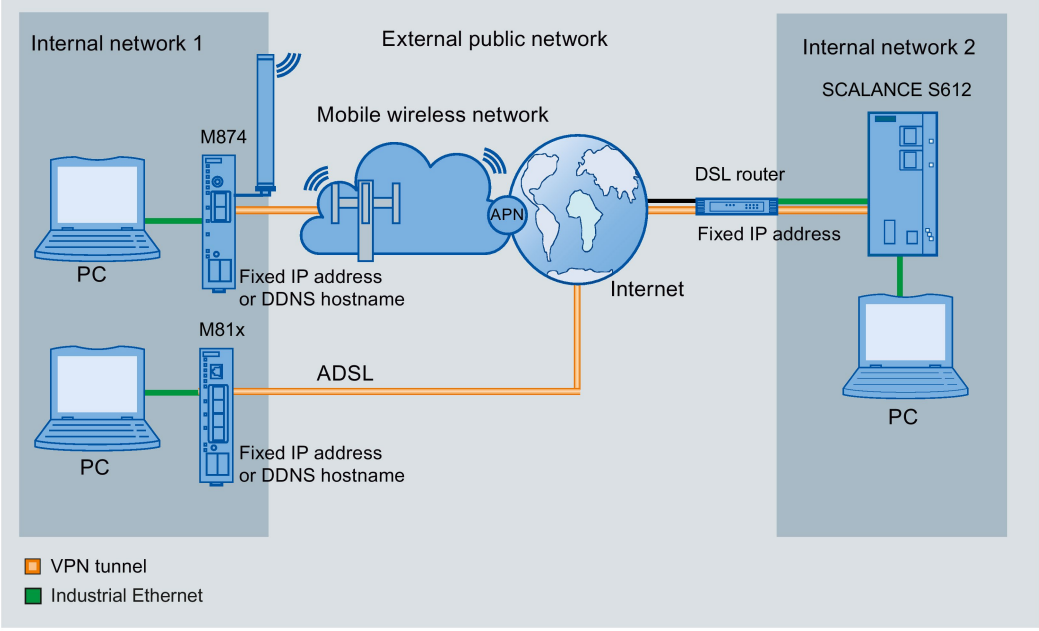
VPN tunnel between SCALANCE M-800 and S612 3

3.1 Procedure in principle

In these examples, a secure VPN tunnel is configured between a SCALANCE M-800 and a SCALANCE S.

- Example 1: Secure VPN tunnel with pre-shared keys (PSK)
- Example 2: Secure VPN tunnel with certificates

Structure



Internal network 1 - connection to SCALANCE M-800

- In the test setup, in the internal network, a network node is implemented by an Admin PC connected to an Ethernet interface of the SCALANCE M-800.
  - Admin PC: Represents a node in the internal network
  - M-800: SCALANCE M module for protection of the internal network
- Connection to the external, public network:
  - Wireless via the antenna of the M874 to the mobile wireless network.
  - Wired via the RJ-45 jack of the M81x to ADSL.

Internal network 2 - attachment to an internal port of the SCALANCE S

- In the test setup, in the internal network, each network node is implemented by one PC connected to the internal port of the security module.
  - PC: Represents a node in the internal network
  - S612: Security module for protection of the internal network
- Connection to the external, public network via DSL router

  Access to the Internet is via a DSL modem or a DSL router connected to the external port of the security module.

Required devices/components

Use the following components for setup:

- Connection to the mobile wireless network
  - 1 x M874 (additional option: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - 1 x suitable antenna
  - 1 x SIM card of your mobile wireless provider. Suitable services are enabled, e.g. Internet.
- Connecting to ADSL
  - 1 x M812 or 1 x M816 (optionally also: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - ADSL access is enabled
- 1 x SCALANCE S612, (additional option: a suitably installed DIN rail with fittings)
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC with which the SCALANCE M-800 is connected.
- 1 x PC with which the SCALANCE S612 is connected and on which the "Security Configuration Tool" is installed.
- 1 x DSL modem or DSL router
- 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

		Internal address	External address
Internal network 1	M-800	192.168.100.1 255.255.255.0	Fixed IP address, e.g. 90.90.90.90 Provider dependent As an alternative, the DDNS host-name can also be used.
	Admin PC	192.168.100.20 255.255.255.0	
Internal network 2	DSL router	192.168.184.254 255.255.255.0	Fixed IP address (WAN IP address), e.g. 91.19.6.84
	S612	Internal port 192.168.11.2 255.255.255.0	External port 192.168.184.2 255.255.255.0
	PC	192.168.11.100 255.255.255.0	

Requirement

- SCALANCE S612 is connected to the Internet via the DSL router.

  On the DSL router, the PORT forwarding must be set so that the UDP packets from the Internet addressed to ports 500 and 4500 of the router are sent to ports 500 and 4500 of the connected SCALANCE S612 (passive module).
- The SCALANCE M-800 is connected to the WAN , refer to "Connecting SCALANCE M-800 to the WAN (Page 11)".
- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

Example 1: Secure VPN tunnel with PSK

Configuring a VPN tunnel with the SCT V3.x

1. Creating the project and modules (Page 96)
2. Configuring a tunnel connection (Page 98)
3. Configuring the properties of the S612 (Page 100)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 101)

Configuring a VPN tunnel with the SCT V4.x

1. Creating the project and modules (Page 103)
2. Configuring a tunnel connection (Page 106)
3. Configuring the properties of the S612 (Page 107)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 108)

Configuring the SCALANCE M-800

1. Activating VPN (Page 109)
2. Configuring the VPN remote end (Page 110)
3. Configuring a VPN connection (Page 111)
4. Configuring VPN authentication (Page 112)
5. Configuring phase 1 and phase 2 (Page 113)
6. Establishing the VPN connection (Page 114)

Example 2: Secure VPN tunnel with certificates

Configuring a VPN tunnel with the SCT V3.x

1. Creating the project and modules (Page 116)
2. Configuring a tunnel connection (Page 118)
3. Configuring the properties of the S612 (Page 120)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 121)

Configuring a VPN tunnel with the SCT V4.x

1. Creating the project and modules (Page 123)
2. Configuring a tunnel connection (Page 126)
3. Configuring the properties of the S612 (Page 127)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 128)

Configuring the SCALANCE M-800

1. Loading a certificate (Page 129)
2. Activating VPN (Page 131)
3. Configuring the VPN remote end (Page 132)
4. Configuring a VPN connection (Page 132)
5. Configuring VPN authentication (Page 133)
6. Configuring phase 1 and phase 2 (Page 134)
7. Establishing the VPN connection (Page 135)

3.2 Secure VPN tunnel with PSK

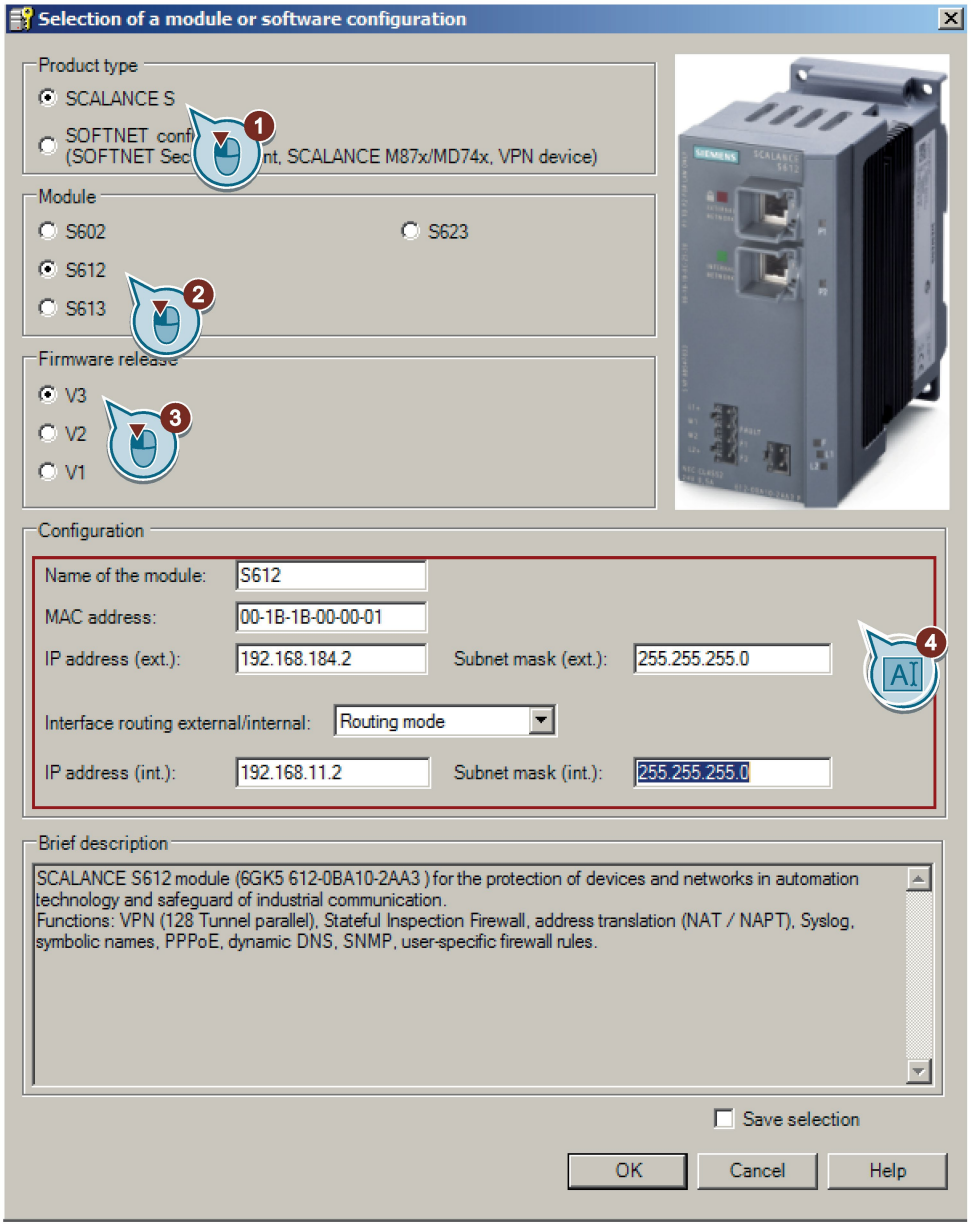
3.2.1 Configuring a VPN tunnel with the SCT V3.x

3.2.1.1 Creating the project and modules

Procedure

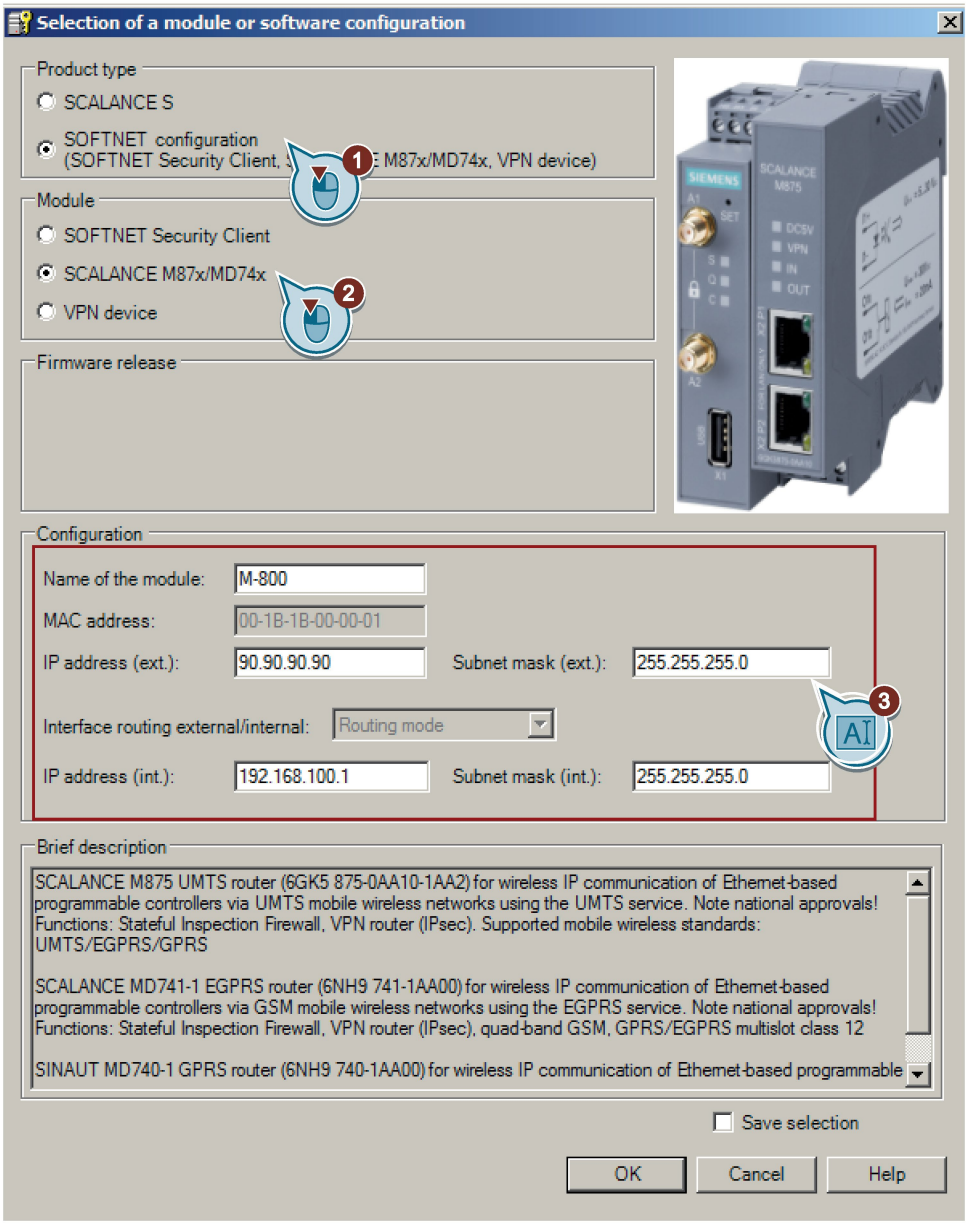
1. Start the Security Configuration Tool V3.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new project has been created and the "Selection of a module or software configuration" dialog is open.

5. Enter the values assigned to the S612 from the "Settings used (Page 91)" table. In addition to this, enter the MAC address printed on the front of the security module



6. Close the dialog with "OK".
7. Generate a second module with the "Insert" > "Module" menu command

8. Enter the values assigned to the M-800 from the "Settings used (Page 91)" table.



9. Close the dialog with "OK".

Result

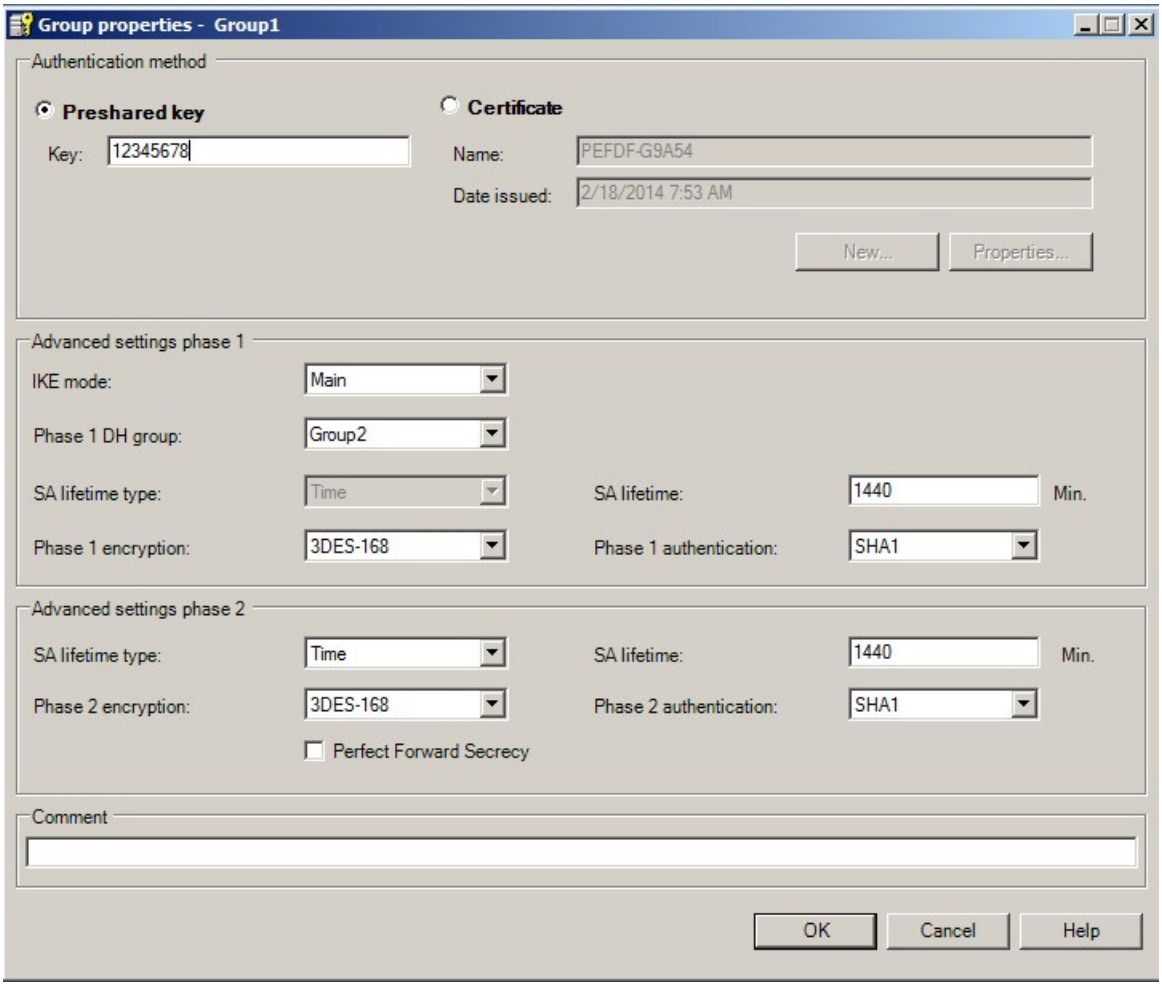
The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

3.2.1.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the S612 are assigned to the same VPN group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the M-800 and the S612 in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu.
6. For this configuration example, configure the group properties with the following settings.



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

Result

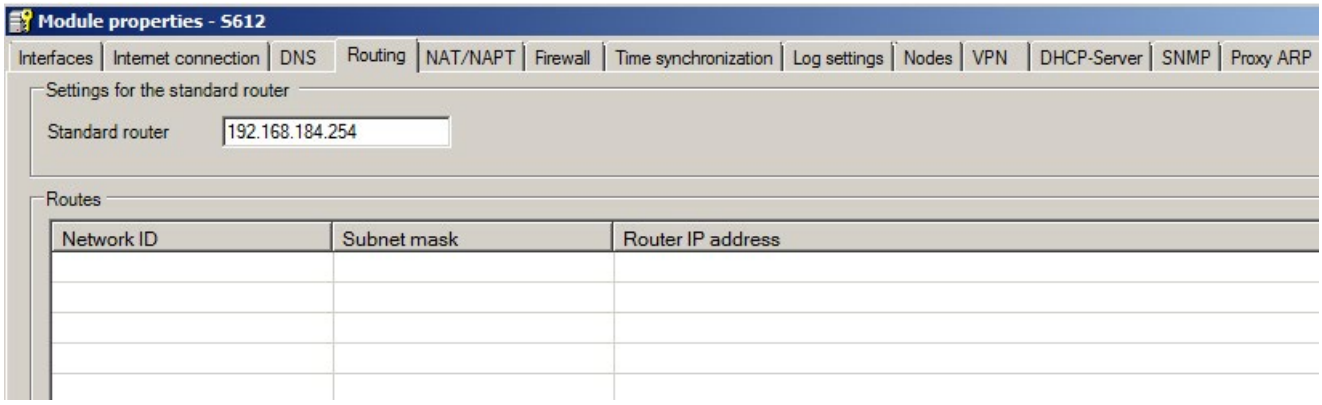
The configuration of the tunnel connection is complete.

3.2.1.3 Configuring the properties of the S612

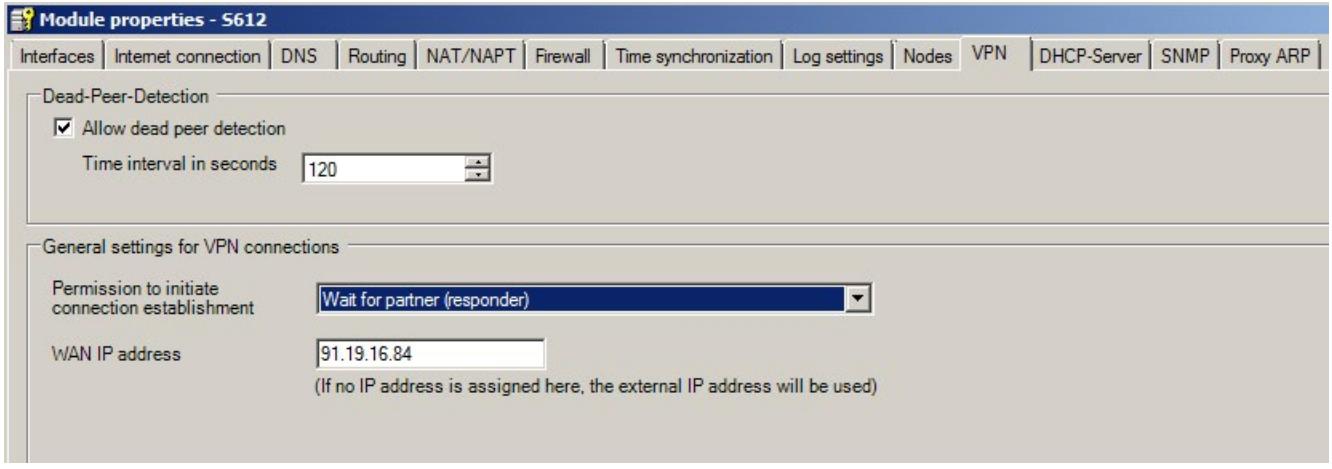
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

Procedure

1. Select the "S612" in the content area.
2. Select the menu command "Edit" > "Properties". Click the "Routing" tab.
3. For "Default router", enter the internal IP address of the default router "192.168.184.254". Click "Apply"



4. Click the "VPN" tab.
5. For "Permission to initiate connection establishment", select the "Wait for partner (responder)" entry.
6. Enter the WAN IP address of the DSL router, e.g. 91.19.6.84



7. Click "Apply" and close the dialog with "OK".
8. Select the "Project" > "Save" menu command. Save the security project under the required name.

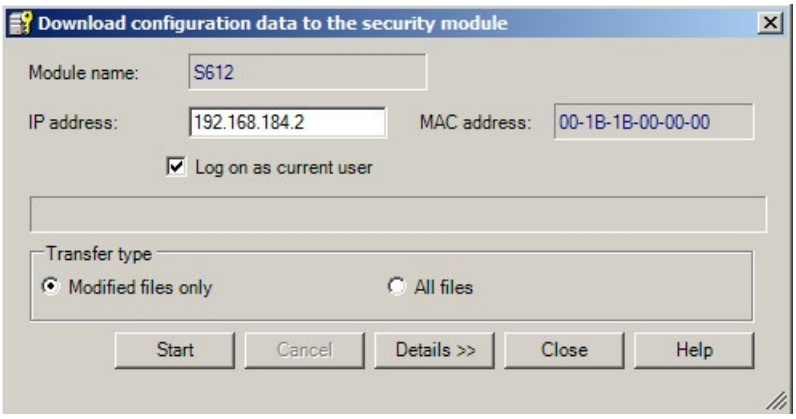
Result

The security project is configured. The settings are saved in the configuration file:

3.2.1.4 Downloading the configuration to the S612 and saving the M-800 configuration

Downloading the configuration to the S612

1. In the content area, select the "S612" security module and select the menu command "Transfer" > "To module(s) …". The following dialog opens.



2. Click the "Start" button to start the download.

   If the download was completed free of errors, the security module is restarted automatically and the new configuration activated.

Saving the SCALANCE M-800 configuration

1. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project directory.

Result

The following file will be saved in the project directory:

- Configuration file: projectname.M-800.txt

The configuration file contains the exported configuration information for the SCALANCE M-800.

Configuration file	Settings in WBM
IPsec VPN > Connections > VPN Standard Mode - Edit Settings	Security > IPSec VPN > Remote End > Remote Mode: Standard
Address of the remote site's VPN gateway: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentication method: Pre Shared Key	Security > IPSec VPN > Authentication > Authentication: PSK

Configuration file	Settings in WBM
Pre Shared Key: 12345678	Security > IPSec VPN > Authentication > PSK und PSK Confirmation: 12345678
Remote ID: U28098881@GEA32	Security > IPSec VPN > Authentication > Remote ID not required. The external IP address of the S612 is entered in the WBM. In this example, this is 192.168.184.2
Local ID: U269159D5@GEA32	Security > IPSec VPN > Authentication > Local ID not required. The entry remains empty in the WBM.
Remote net address: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Remote subnet mask: 255.255.255.0	
Local net address: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Local subnet mask: 255.255.255.0	
IPsec VPN > Connections > Edit IKE	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA encryption: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA mode: Main mode	--
ISAKMP-SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPsec SA encryption: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPsec SA hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPsec SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 2 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--
DH/PFS group: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: On	--
DPD delay (seconds): 150	--
DPD timeout (seconds): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD maximum failures: 5	--

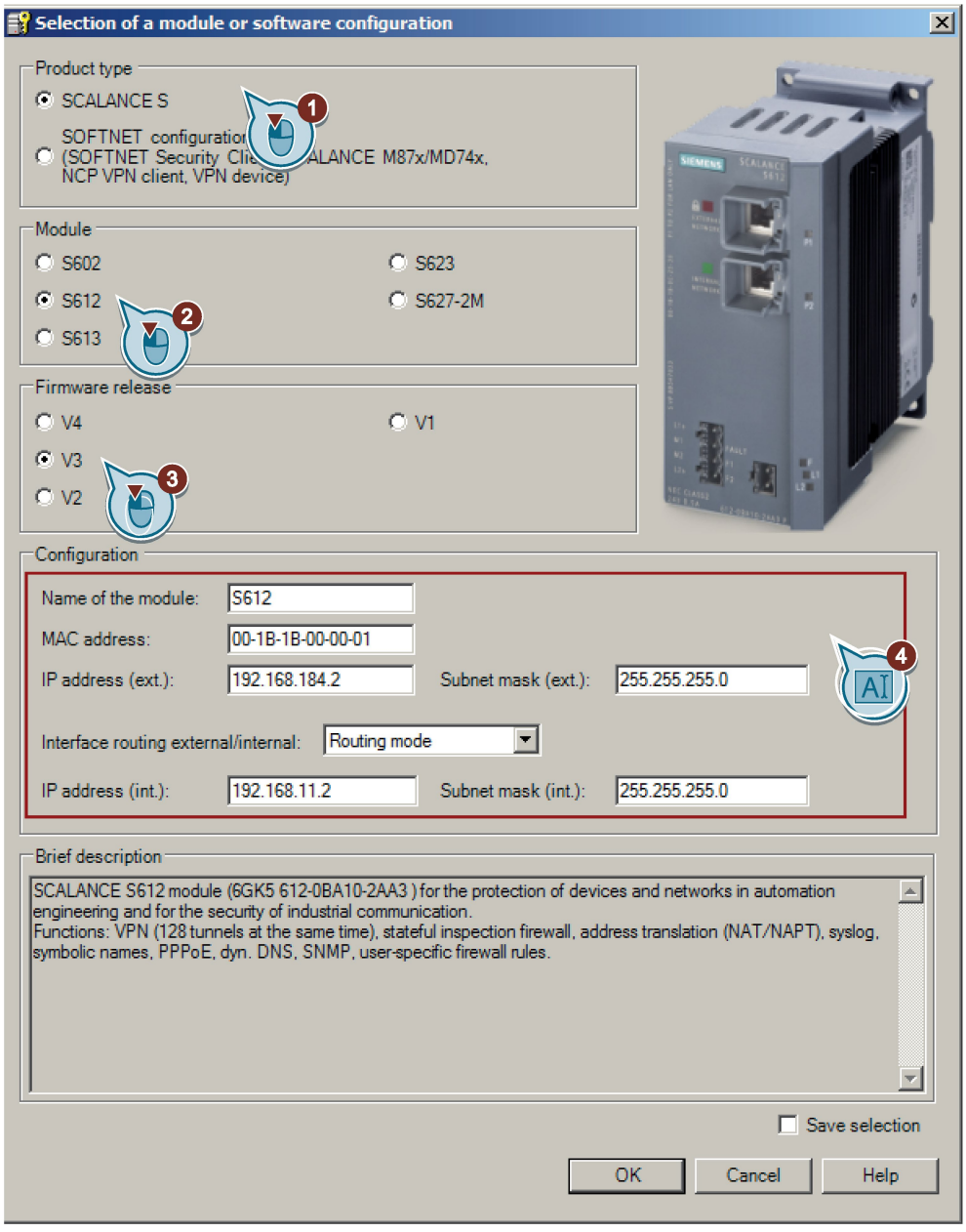
3.2.2 Configuring a VPN tunnel with the SCT V4.x

3.2.2.1 Creating the project and modules

Procedure

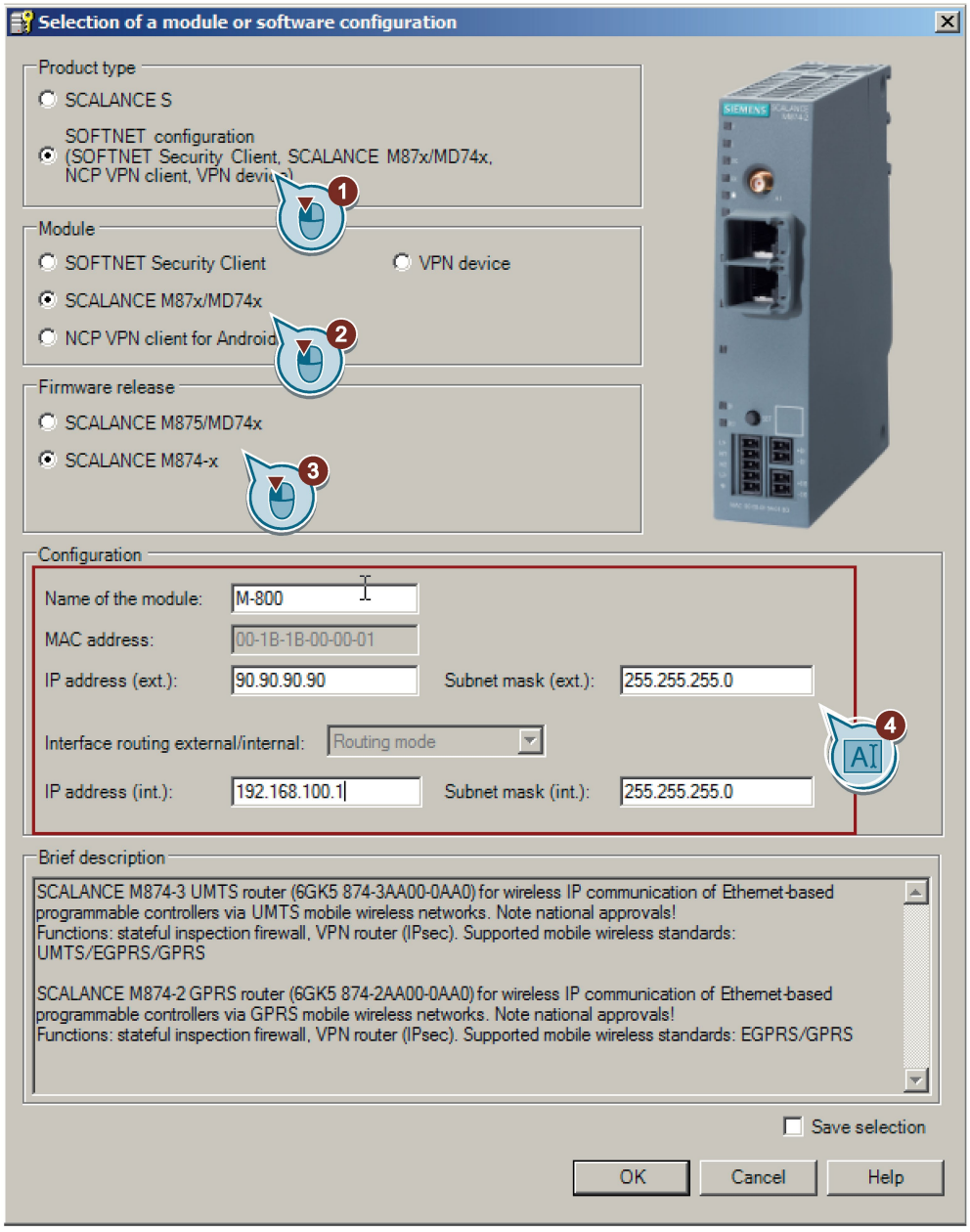
1. Start the Security Configuration Tool V4.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new project has been created and the "Selection of a module or software configuration" dialog is open.

5. Enter the values assigned to the S612 from the "Settings used (Page 91)" table. In addition to this, enter the MAC address printed on the front of the security module



6. Close the dialog with "OK".
7. Generate a second module with the "Insert" > "Module" menu command

8. Enter the values assigned to the M-800 from the "Settings used (Page 91)" table.



9. Close the dialog with "OK".

Result

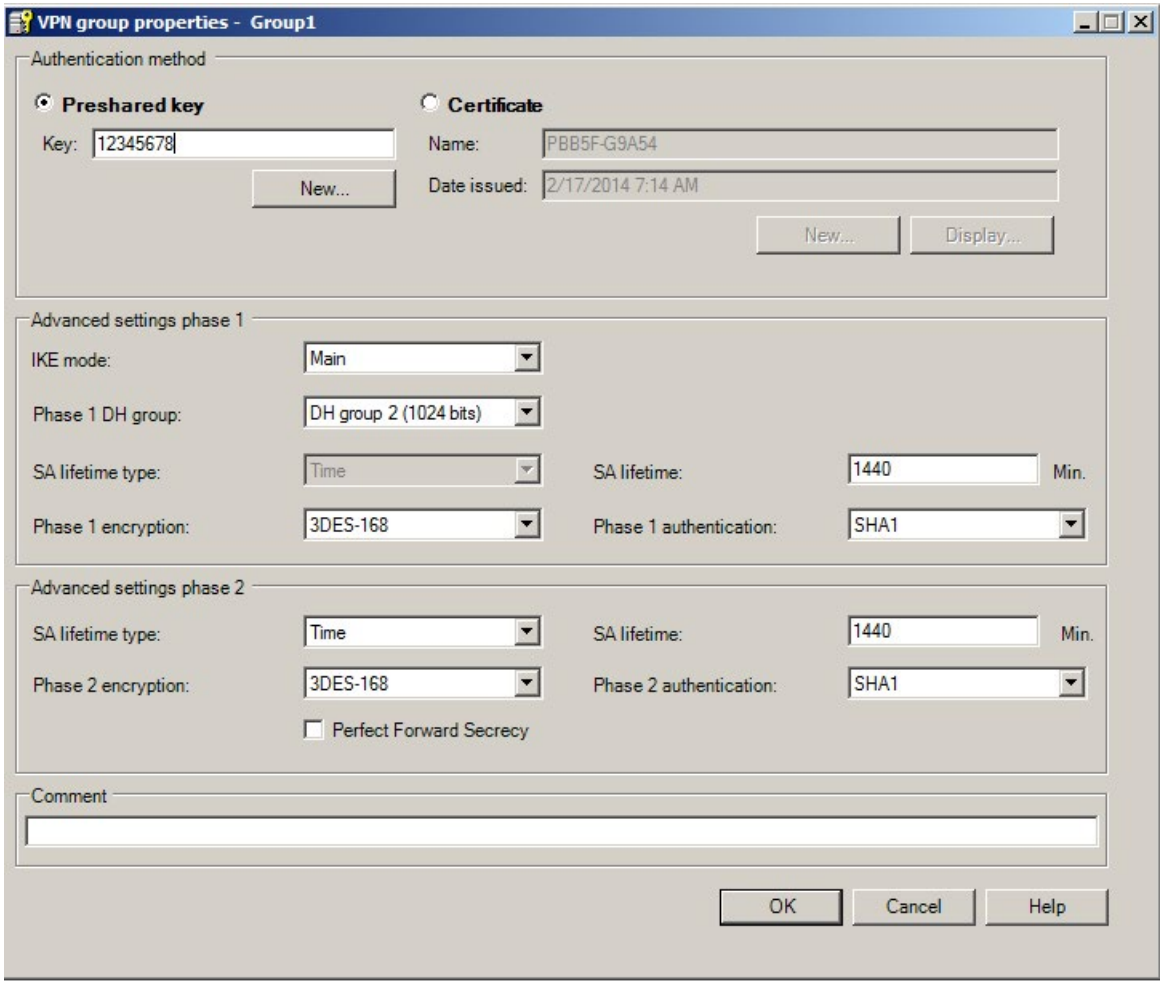
The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

3.2.2.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the M-800 and the S612 are assigned to the same VPN group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation panel.
3. Select the SCALANCE M-800 and the S612 in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu.
6. For this configuration example, configure the group properties with the following settings.



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

Result

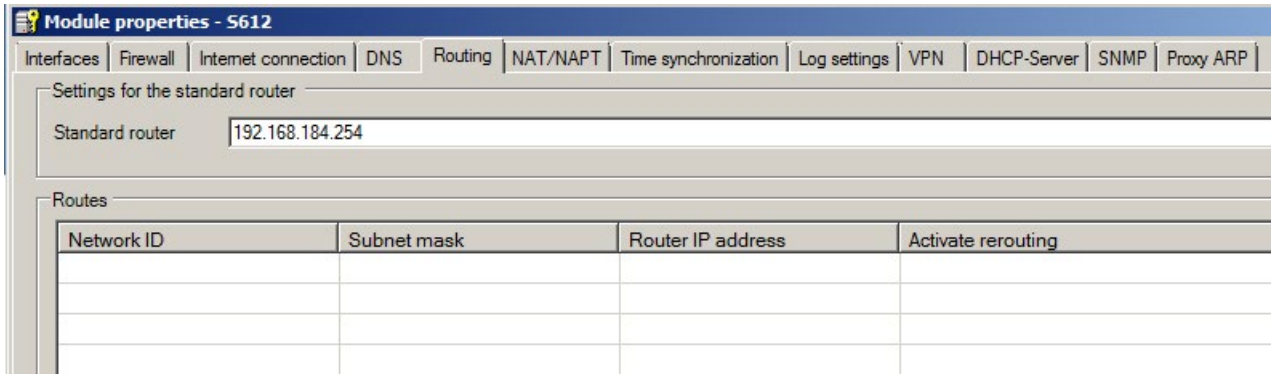
The configuration of the tunnel connection is complete.

3.2.2.3 Configuring the properties of the S612

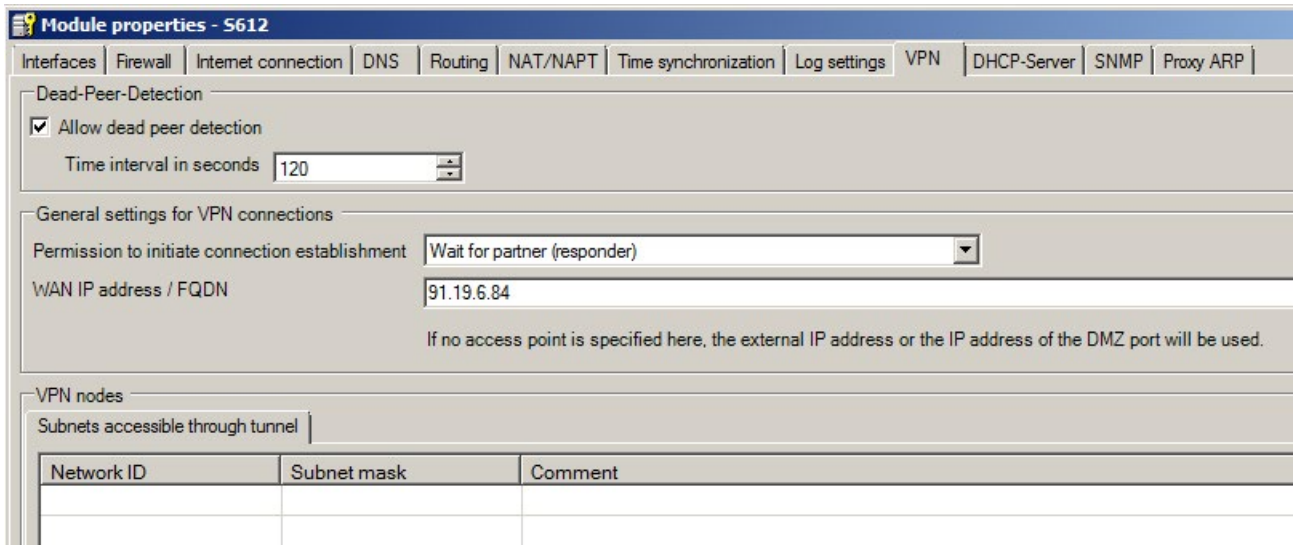
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

Procedure

1. Select the "S612" in the content area.
2. Select the menu command "Edit" > "Properties". Click the "Routing" tab.
3. For "Default router", enter the internal IP address of the default router "192.168.184.254". Click "Apply"



4. Click the "VPN" tab.
5. For "Permission to initiate connection establishment", select the "Wait for partner (responder)" entry.
6. Enter the WAN IP address of the DSL router, e.g. 91.19.6.84



7. Click "Apply" and close the dialog with "OK".
8. Select the menu command "Project" > "Save". Save the security project under the required name.

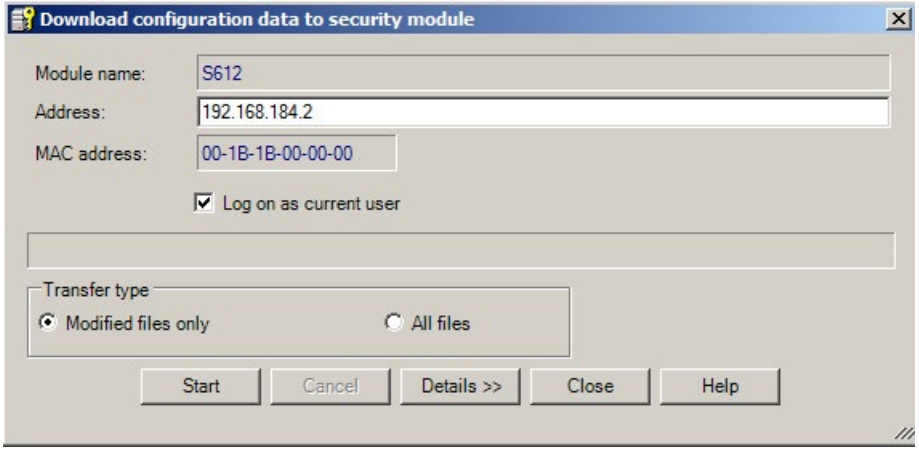
Result

The security project is configured. The settings are saved in the configuration file.

3.2.2.4 Downloading the configuration to the S612 and saving the M-800 configuration

Downloading the configuration to the S612

1. In the content area, select the "S612" security module and select the menu command "Transfer" > "To module(s) …". The following dialog opens.



2. Click the "Start" button to start the download.

   If the download was completed free of errors, the security module is restarted automatically and the new configuration activated.

Saving the SCALANCE M-800 configuration

1. In the content area, select the SCALANCE M-800 and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project directory.

Result

The following file will be saved in the project directory:

- Configuration file: projectname.M-800.txt

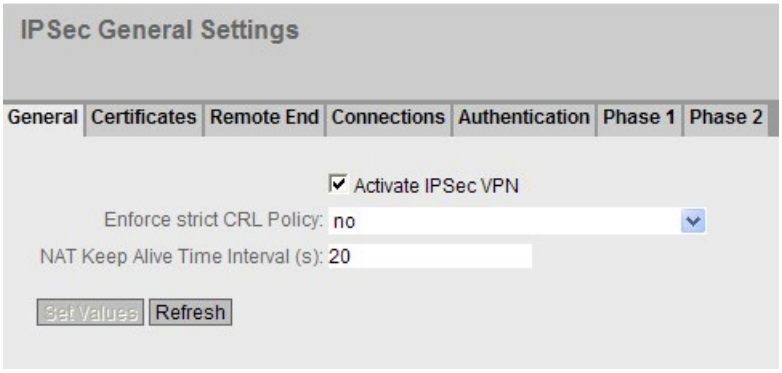
The configuration file contains the exported configuration information for the SCALANCE M-800. Follow the instructions in the configuration file.

3.2.3 Configuring SCALANCE M-800

3.2.3.1 Activating VPN

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select Activate IPSec VPN".



3. Click "Set Values"

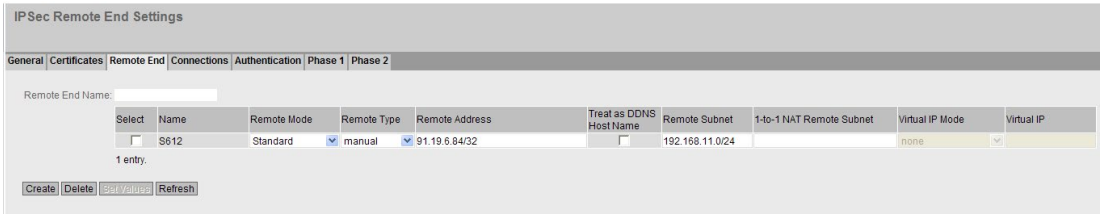
3.2.3.2 Configuring the VPN remote end

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Remote End" tab in the content area.
2. Enter the name of the VPN partner (tunnel endpoint) in "Remote End Name", e.g. S612.
3. Click "Create". A new row is created in the table.
4. Configure the VPN remote end with the following settings from the configuration file:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.11.0/24

5. Click "Set Values".



3.2.3.3 Configuring a VPN connection

Requirement

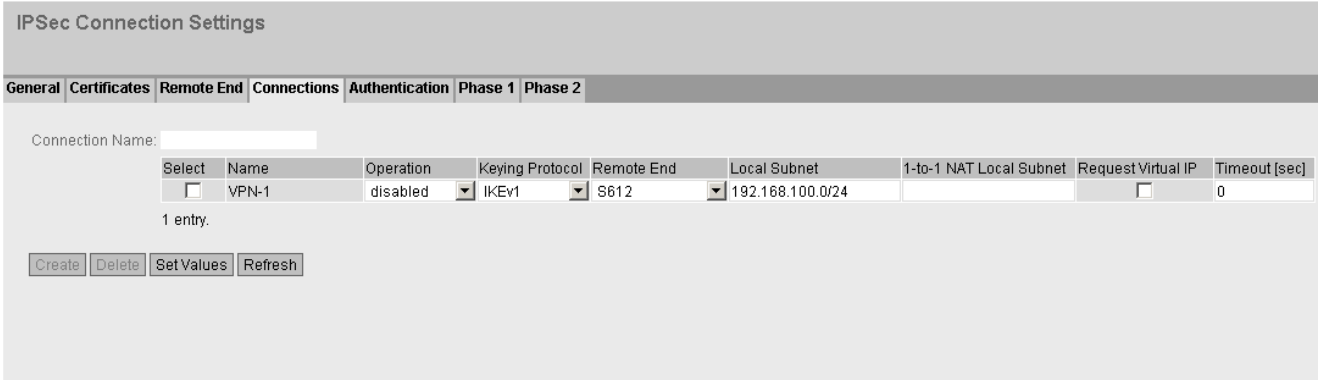
- The VPN remote end has been created.

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Click "Create". A new row is created in the table.
4. Configure the VPN connection with the following settings:

Operation	disabled
Keying Protocol	IKEv1
Remote End	S612 Name of the VPN remote station
Local Subnet	192.168.100.0/24 The local internal subnet 1 in CIDR notation.

5. Click "Set Values".



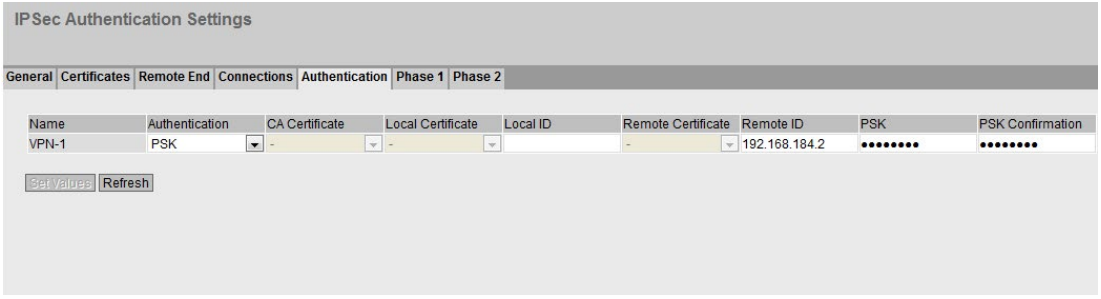
3.2.3.4 Configuring VPN authentication

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Authentication" tab in the content area.
2. Configure the VPN authentication with the following settings:

Authentication	PSK
Local ID	no entry necessary
Remote ID	External IP address of the S612, e.g. 162.168.184.2
PSK / PSK Confirmation	12345678 The key that you configured in the SCT.

3. Click "Set Values".



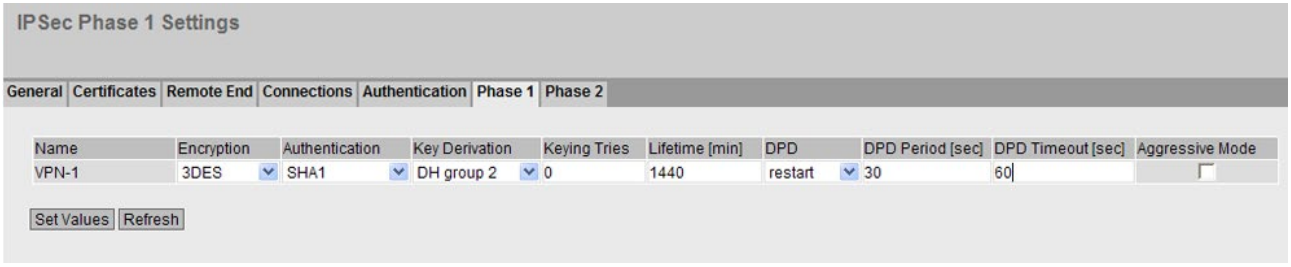
3.2.3.5 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Phase 1" tab in the content area.
2. For "DPD", select "restart".
3. Configure phase 1 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

4. Click "Set Values".

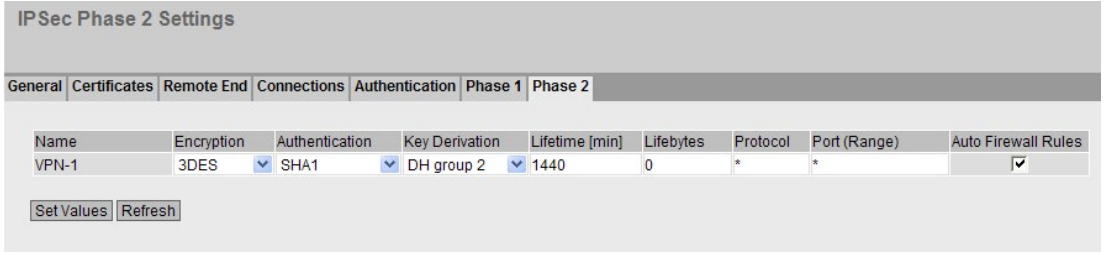


Configuring phase 2

1. Click the "Phase 2" tab.
2. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

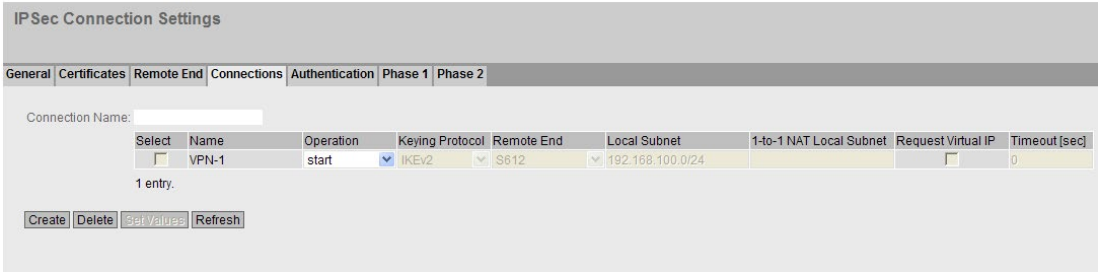
3. Click "Set Values".



3.2.3.6 Establishing the VPN connection

Procedure

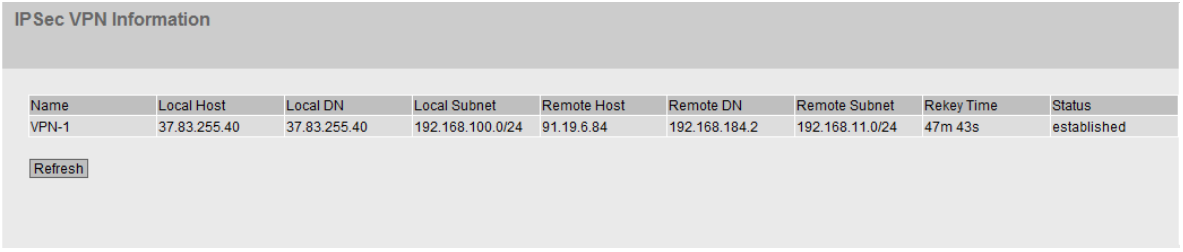
1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Connection" tab in the content area.
2. As "Operation", select "start" and click "Set Values".



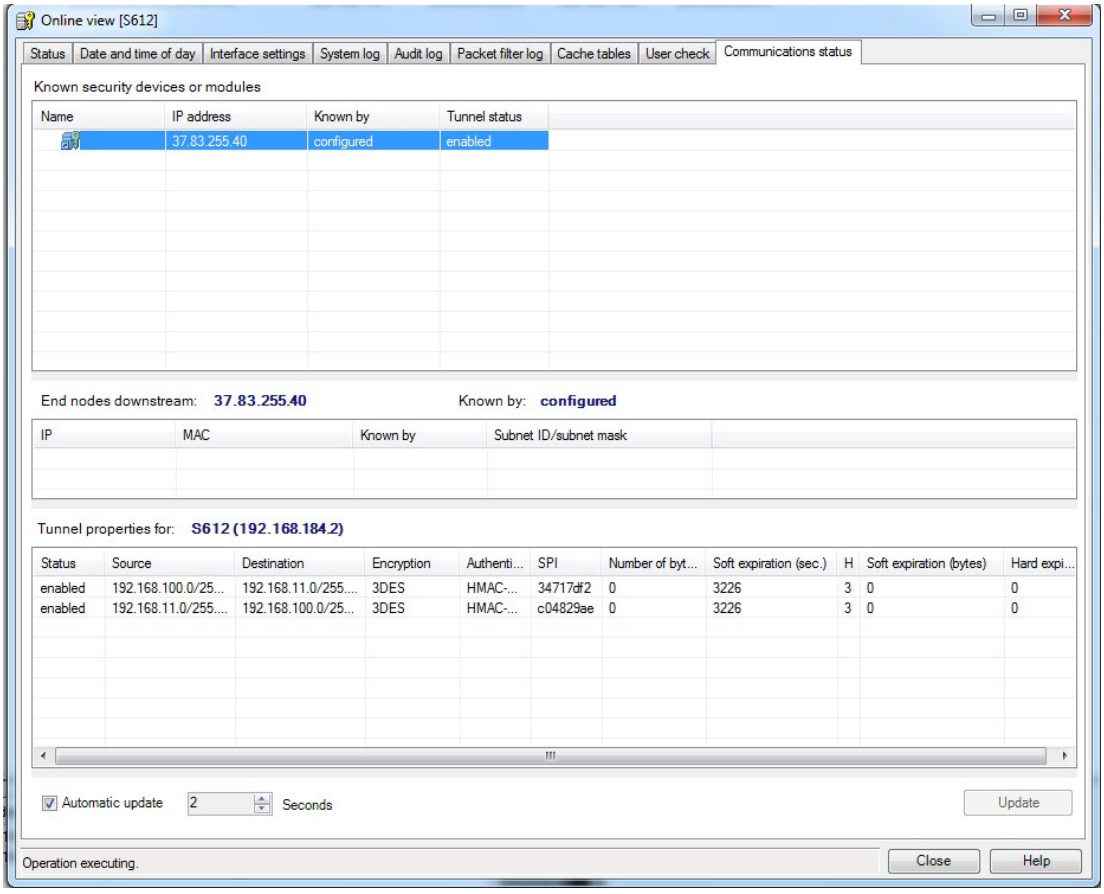
Result

The M-800 establishes the VPN tunnel to the S612. If the VPN tunnel is established, the LED is lit green on the device.

You will find more detailed information in "Information" > "IPSec VPN".



In the online view of the SCT, you can see the communications status on the S612.


Online view [S612]
Status
Date and time of day
Interface settings
System log
Audit log
Packet filter log
Cache tables
User check
Communications status
Known security devices or modules
Name
IP address
Known by
Tunnel status
37.83.255.40
configured
enabled
End nodes downstream: 37.83.255.40
Known by: configured
IP
MAC
Known by
Subnet ID/subnet mask
Tunnel properties for: S612 (192.168.184.2)
Status
Source
Destination
Encryption
Authenti...
SPI
Number of byt...
Soft expiration (sec.)
H
Soft expiration (bytes)
Hard expi...
enabled
192.168.100.0/25...
192.168.11.0/255....
3DES
HMAC-...
34717df2
0
3226
3
0
0
enabled
192.168.11.0/255....
192.168.100.0/25...
3DES
HMAC-...
c04829ae
0
3226
3
0
0
Automatic update
2
Seconds
Update
Operation executing.
Close
Help

3.3 Secure VPN tunnel with certificates

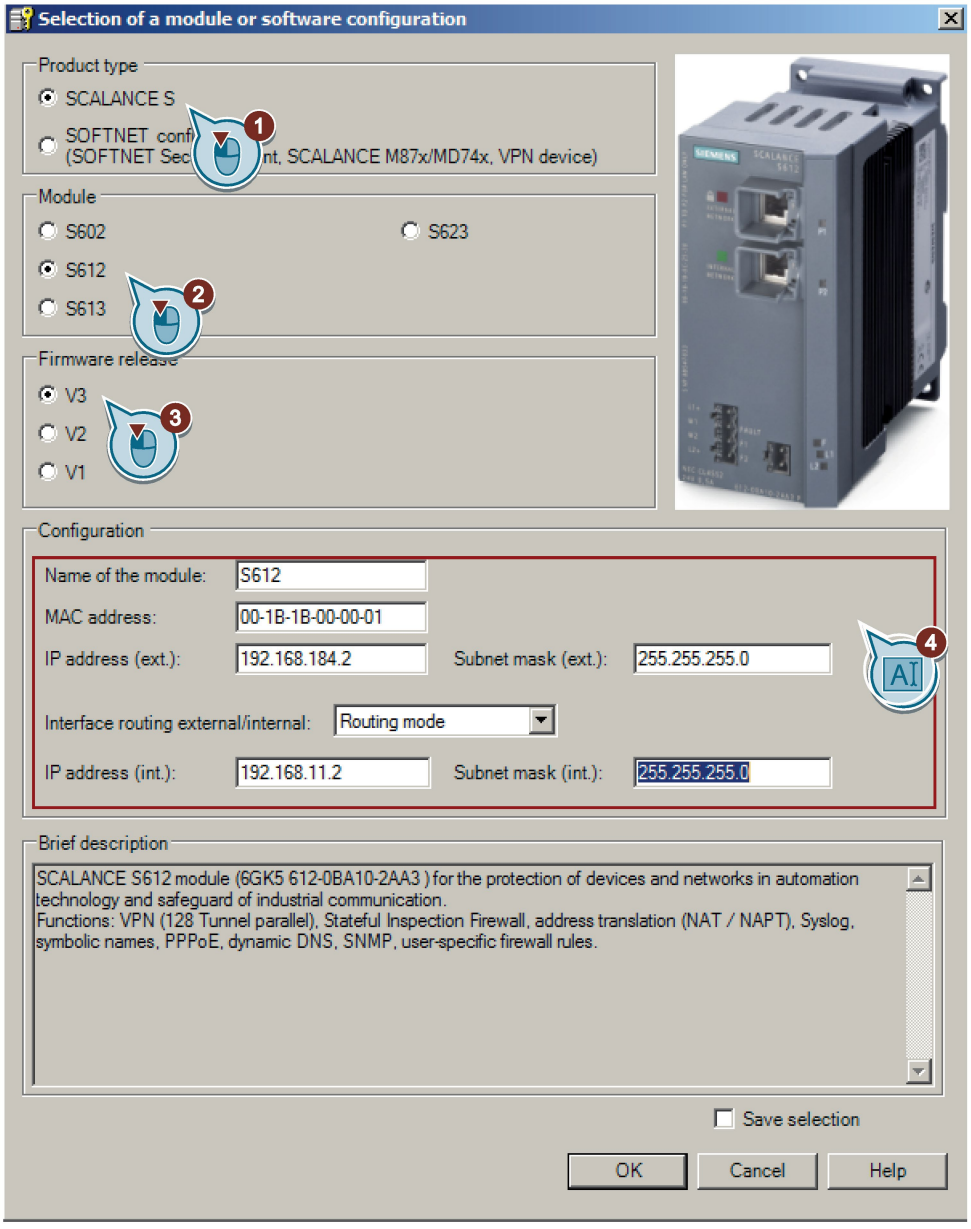
3.3.1 Configuring a VPN tunnel with the SCT V3.x

3.3.1.1 Creating the project and modules

Procedure

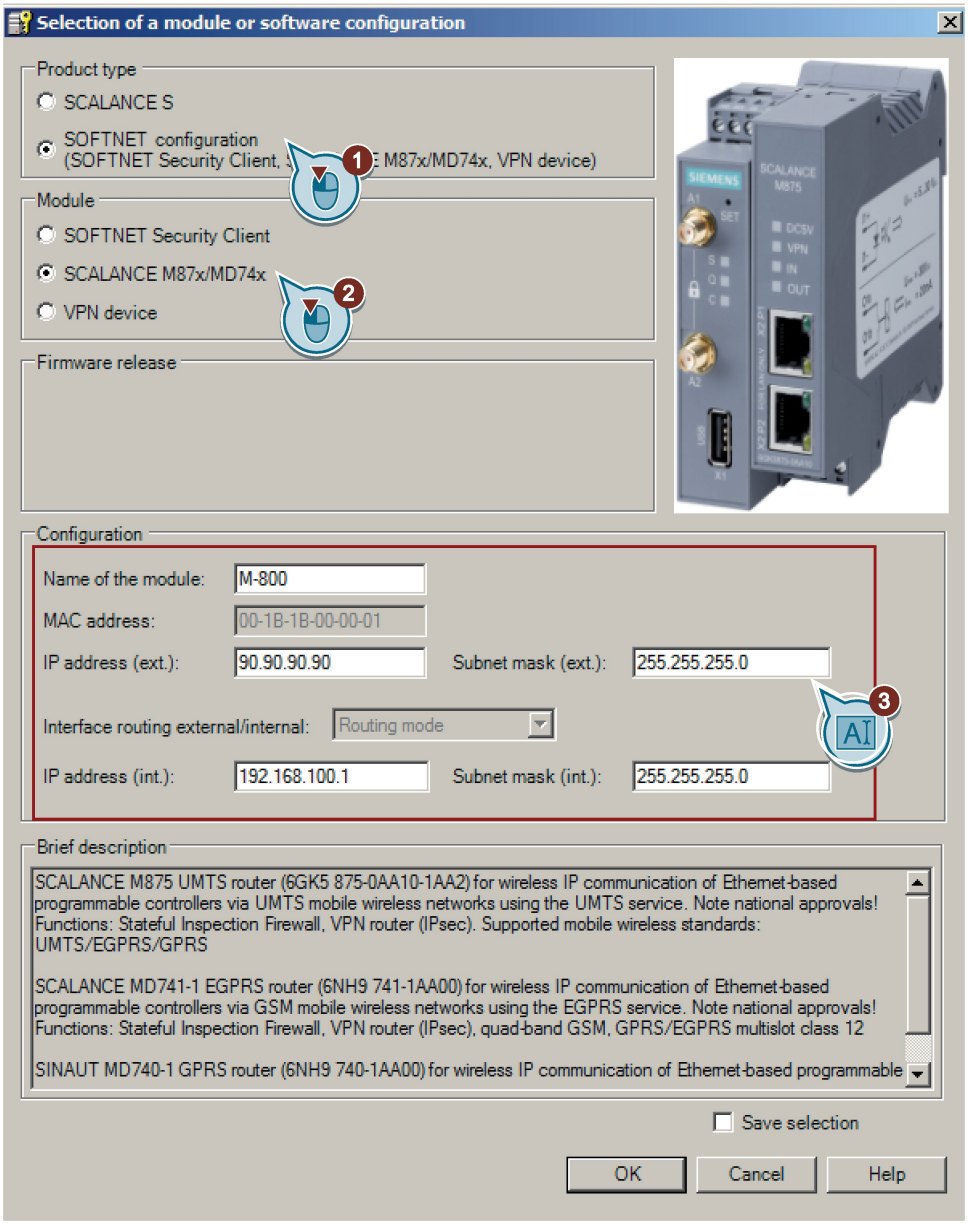
1. Start the Security Configuration Tool V3.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new project has been created and the "Selection of a module or software configuration" dialog is open.

5. Enter the values assigned to the S612 from the "Settings used (Page 91)" table. In addition to this, enter the MAC address printed on the front of the security module



6. Close the dialog with "OK".
7. Generate a second module with the "Insert" > "Module" menu command

8. Enter the values assigned to the M-800 from the "Settings used (Page 91)" table.



9. Close the dialog with "OK".

Result

The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

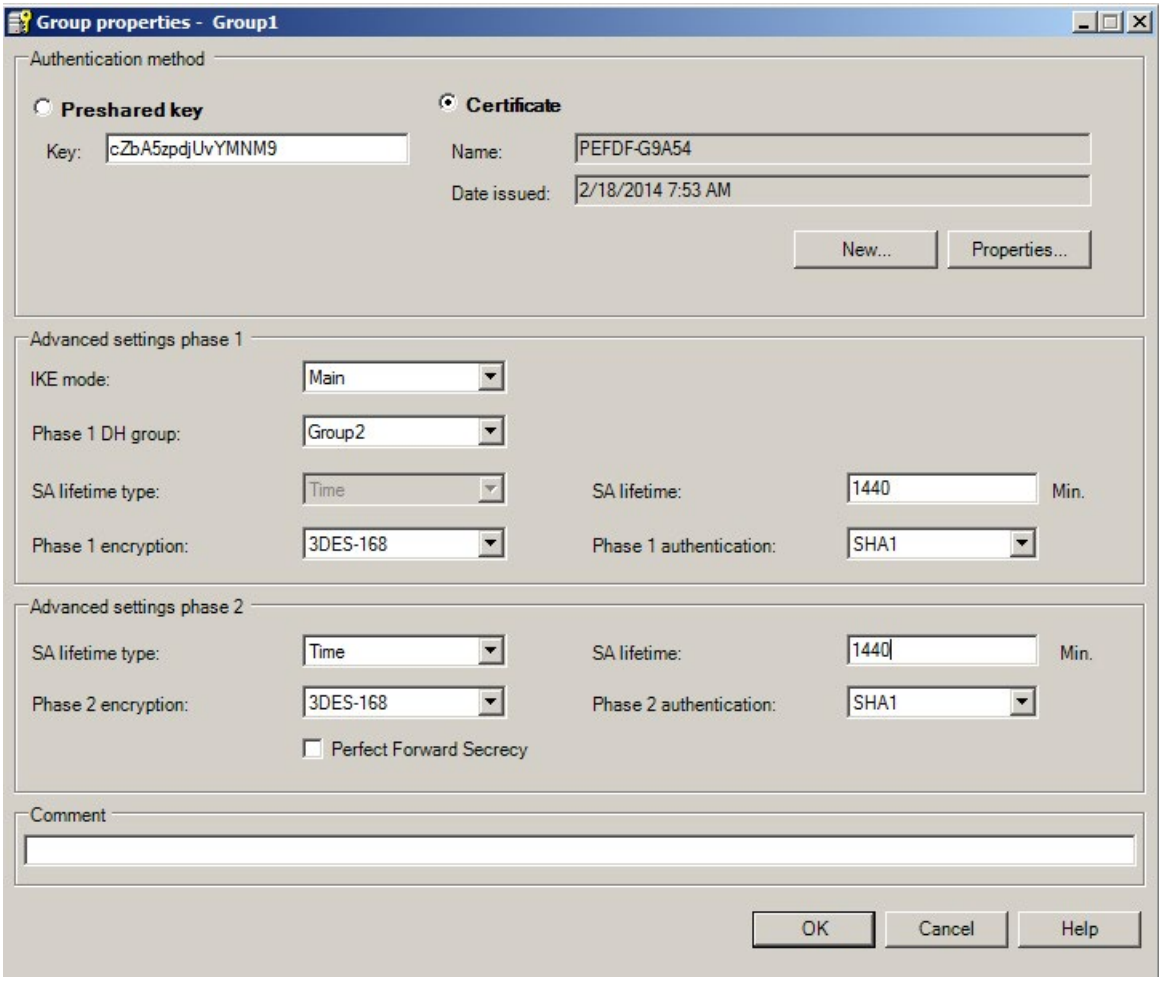
3.3.1.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the S612 are assigned to the same group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the SCALANCE M-800 and the S612 in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu.
6. For this configuration example, configure the group properties with the following settings.

   If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.



Result

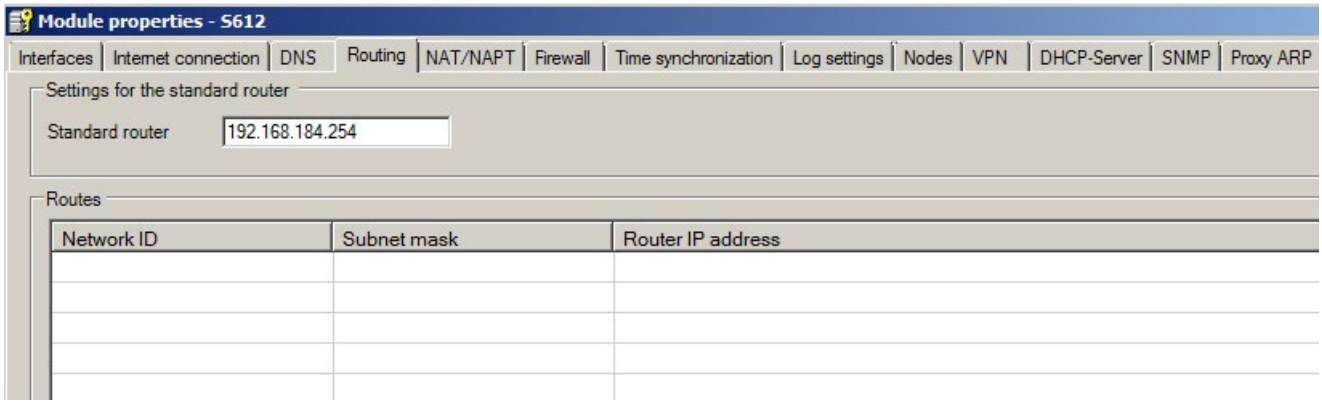
The configuration of the tunnel connection is complete.

3.3.1.3 Configuring the properties of the S612

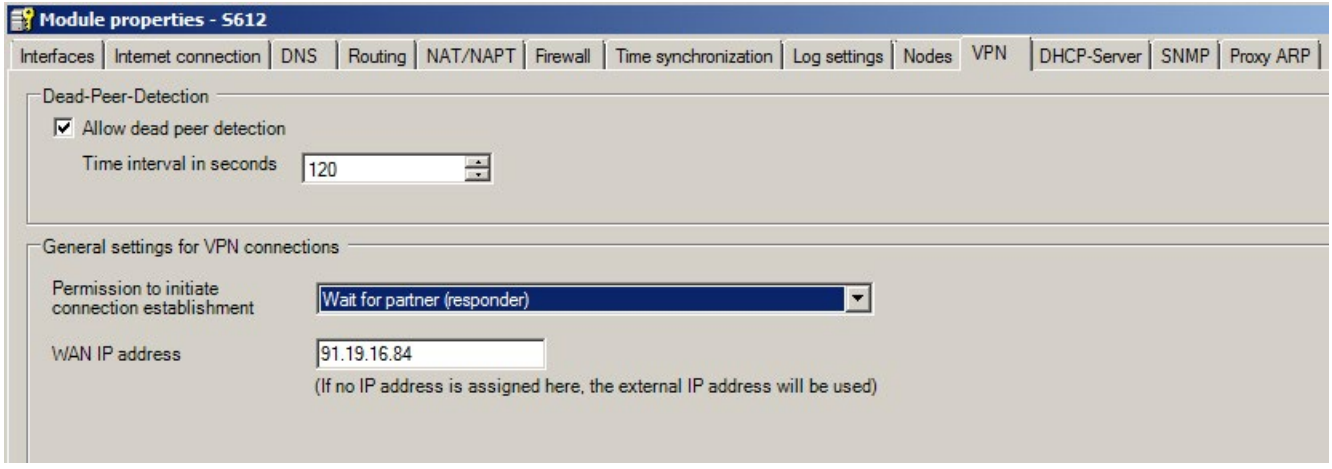
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

Procedure

1. Select the "S612" in the content area.
2. Select the menu command "Edit" > "Properties". Click the "Routing" tab.
3. For "Default router", enter the internal IP address of the default router "192.168.184.254". Click "Apply"



4. Click the "VPN" tab.
5. For "Permission to initiate connection establishment", select the "Wait for partner (responder)" entry.
6. Enter the WAN IP address of the DSL router, e.g. 91.19.6.84



7. Click "Apply" and close the dialog with "OK".
8. Select the "Project" > "Save" menu command. Save the security project under the required name.

Result

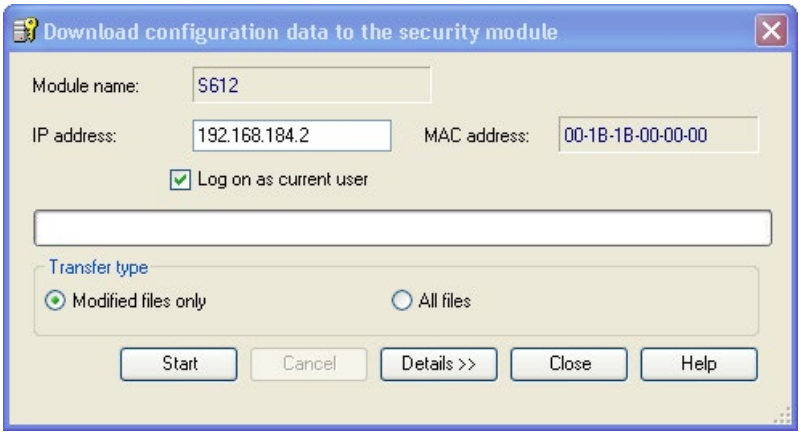
The security project is configured. The settings are saved in the configuration file:

3.3.1.4 Downloading the configuration to the S612 and saving the M-800 configuration

Downloading the configuration to the S612

1. In the content area, select the "S612" security module and select the menu command "Transfer" > "To module(s) …".

   The following dialog opens.



2. Click the "Start" button to start the download.

   If the download was completed free of errors, the security module is restarted automatically and the new configuration activated.

Saving the SCALANCE M-800 configuration

1. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project folder and assign a password for the private key of the certificate, e.g. Di1S+Xo?.

Result

The following files will be saved in the project directory:

- Configuration file: projectname.M-800.txt
- PKCS12 file: projectname.string.M-800.p12
- Remote certificate: Projectname.group1.S612.cer

The configuration file contains the exported configuration information for the SCALANCE M-800 including information on the additionally generated certificates.

Configuration file	Settings in WBM
IPsec VPN > Certificates Upload Remote Site Certificate: Configuration-1.group1.S612.cer Upload PKCS12 File (.p12): Configuration-1.U800CB3FF@G471C.M-800.p12	System > Load&Save > HTTP > IPSecCert : Load
IPsec VPN > Connections > VPN Standard Mode - Edit Settings	Security > IPSec VPN > Remote End > Remote Mode: Standard
Address of the remote site's VPN gateway: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentication method: X.509 remote certificate	Security > IPSec VPN > Authentication > Authentication: Remote Cert
Remote Certificate: Configuration-1.group1.S612.cer	Security > IPSec VPN > Authentication > Remote Certificate: Configuration-1.Gruppe1.CP.cer
Remote ID: U5A634732@GC4D8	Security > IPSec VPN > Authentication > Remote ID: U5A634732@GC4D8
Remote net address: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Remote subnet mask: 255.255.255.0	
Local net address: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Local subnet mask: 255.255.255.0	
IPsec VPN > Connections > Edit IKE	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA encryption: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA mode: Main mode	--
ISAKMP-SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPsec SA encryption: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPsec SA hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPsec SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): No	--
DH/PFS group: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: On	--
DPD delay (seconds): 150	--

Configuration file	Settings in WBM
DPD timeout (seconds): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD maximum failures: 5	--

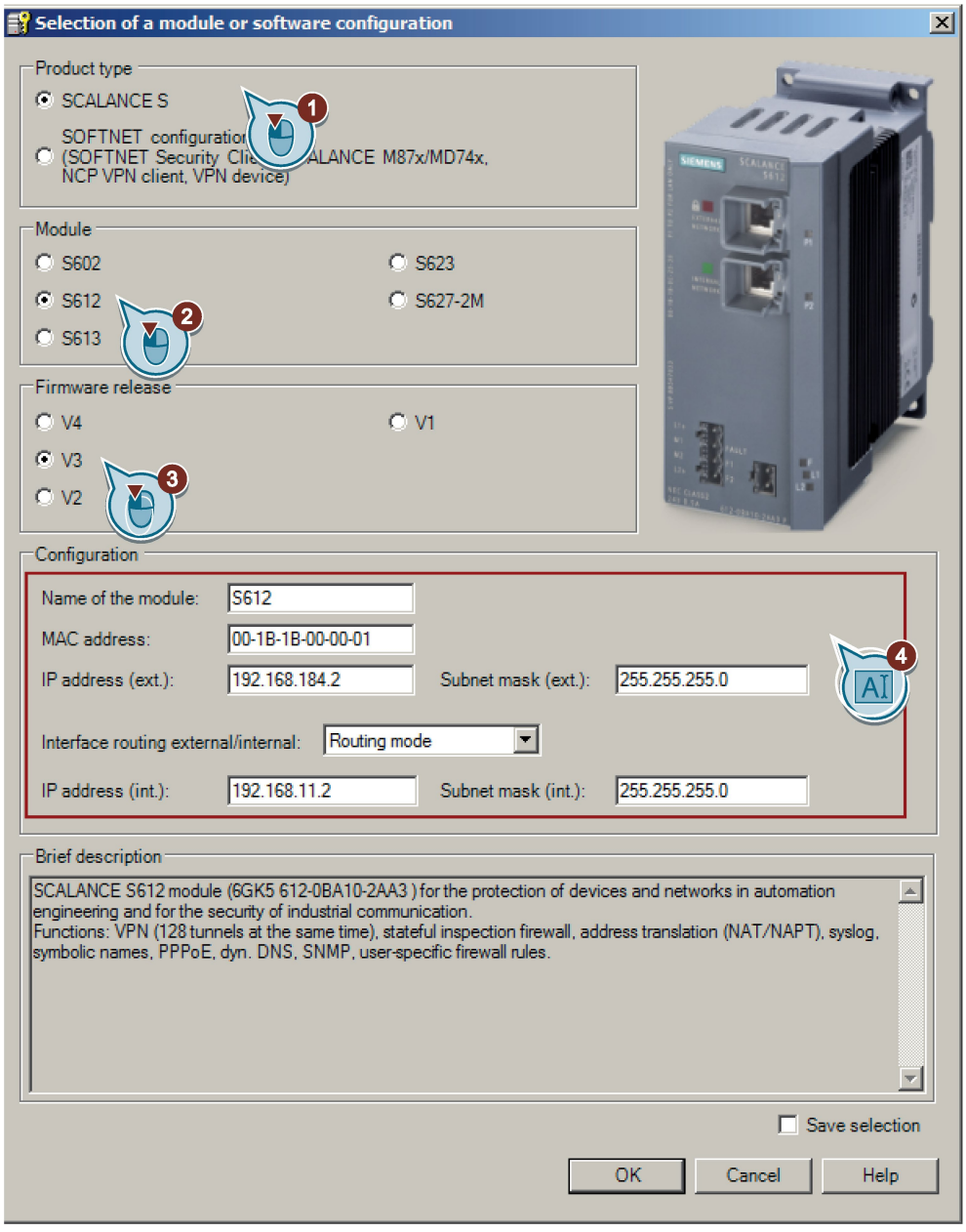
3.3.2 Configuring a VPN tunnel with the SCT V4.x

3.3.2.1 Creating the project and modules

Procedure

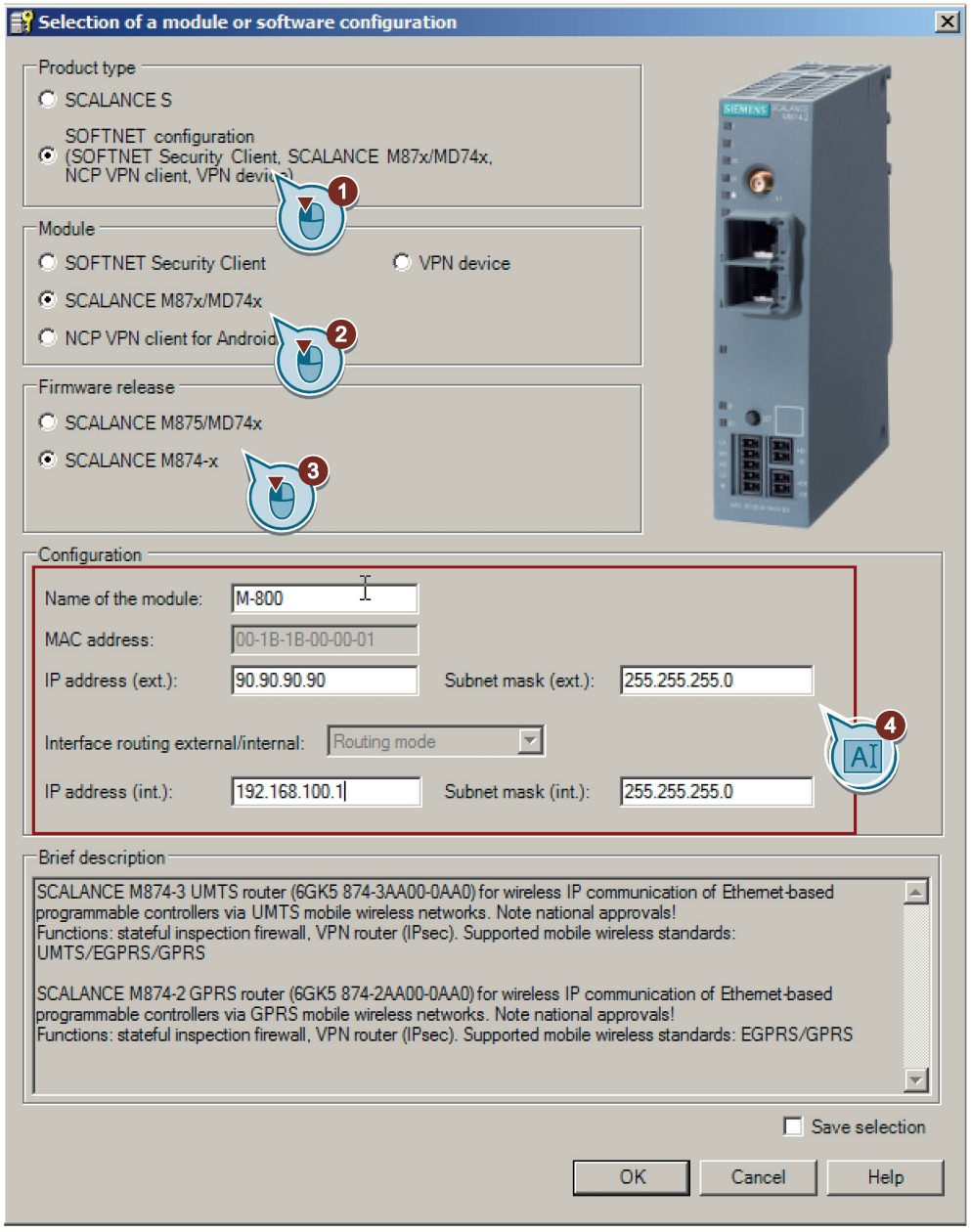
1. Start the Security Configuration Tool V4.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new project has been created and the "Selection of a module or software configuration" dialog is open.

5. Enter the values assigned to the S612 from the "Settings used (Page 91)" table. In addition to this, enter the MAC address printed on the front of the security module



6. Close the dialog with "OK".
7. Generate a second module with the "Insert" > "Module" menu command

8. Enter the values assigned to the M-800 from the "Settings used (Page 91)" table.



9. Close the dialog with "OK".

Result

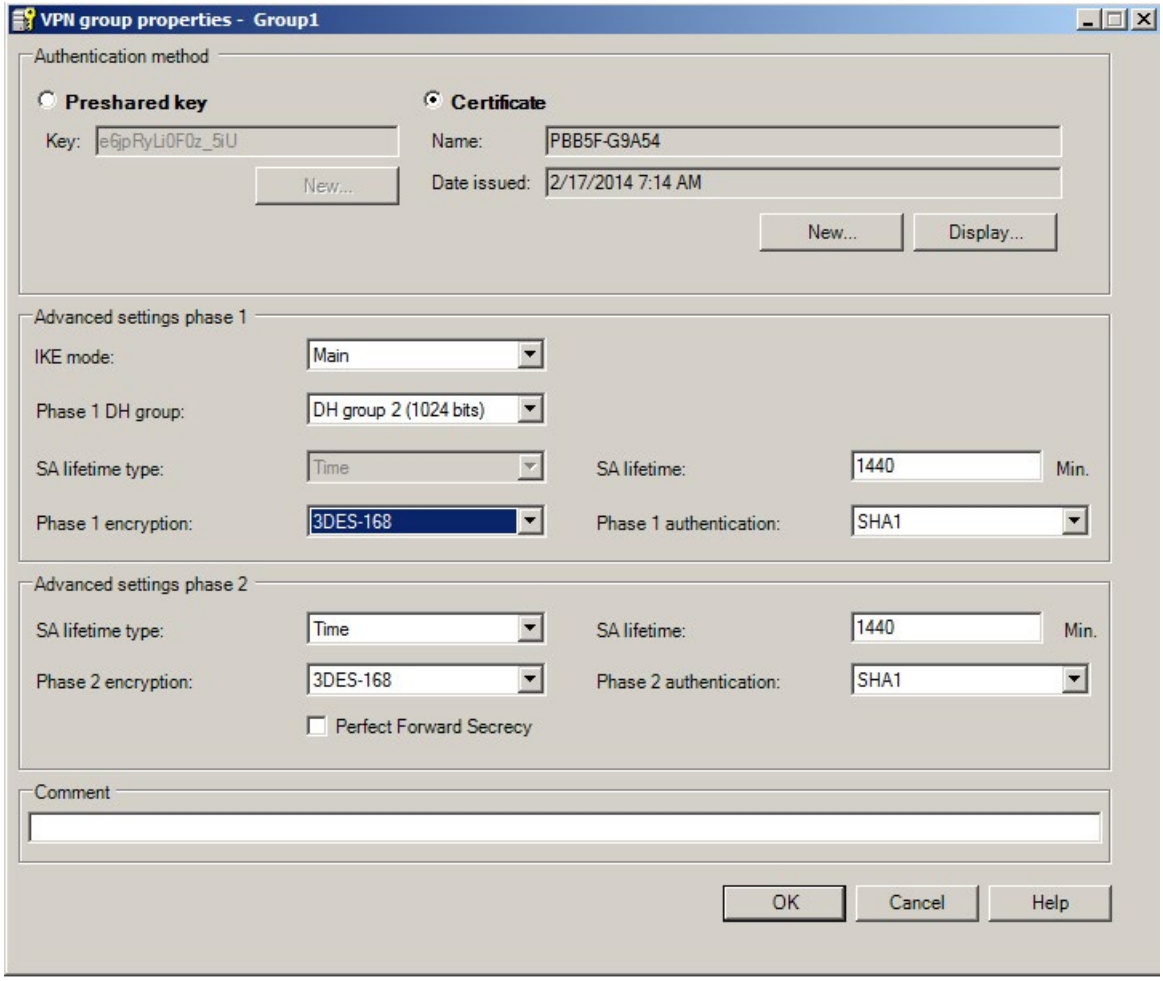
The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

3.3.2.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M and the S612 are assigned to the same group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the SCALANCE M and the S612 in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu.
6. For this configuration example, configure the group properties with the following settings.



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

Result

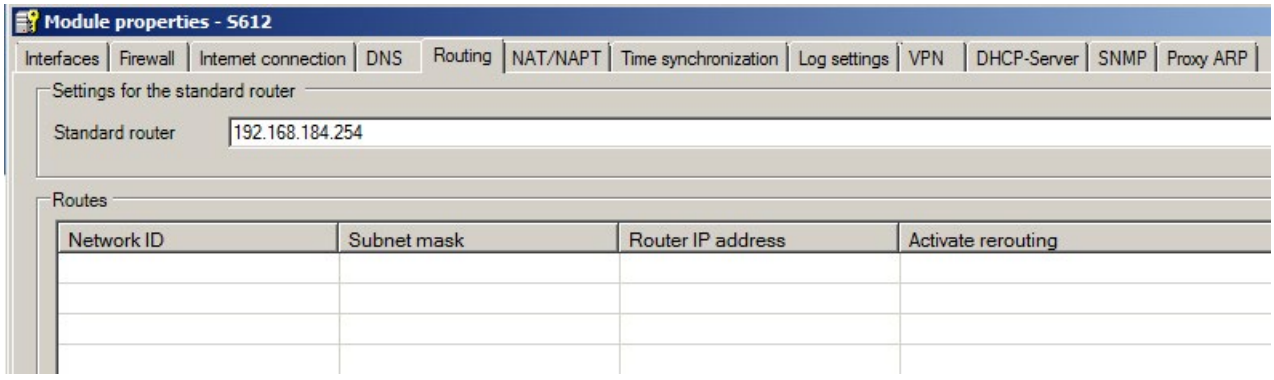
The configuration of the tunnel connection is complete.

3.3.2.3 Configuring the properties of the S612

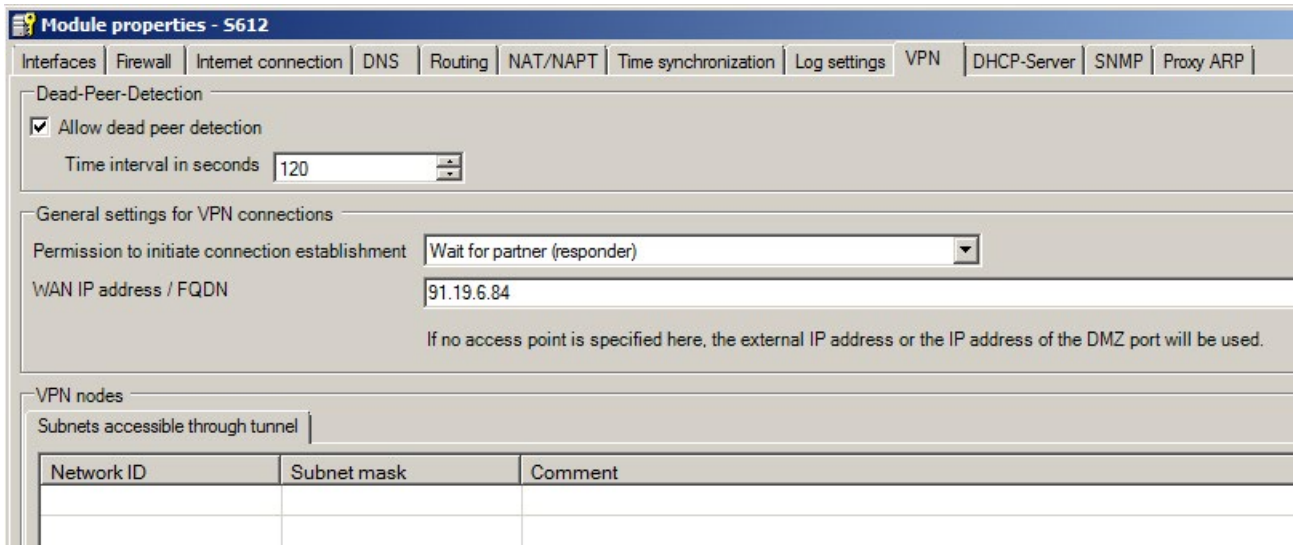
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

Procedure

1. Select the "S612" in the content area.
2. Select the menu command "Edit" > "Properties". Click the "Routing" tab.
3. For "Default router", enter the internal IP address of the default router "192.168.184.254". Click "Apply"



4. Click the "VPN" tab.
5. For "Permission to initiate connection establishment", select the "Wait for partner (responder)" entry.
6. Enter the WAN IP address of the DSL router, e.g. 91.19.6.84



7. Click "Apply" and close the dialog with "OK".
8. Select the menu command "Project" > "Save". Save the security project under the required name.

Result

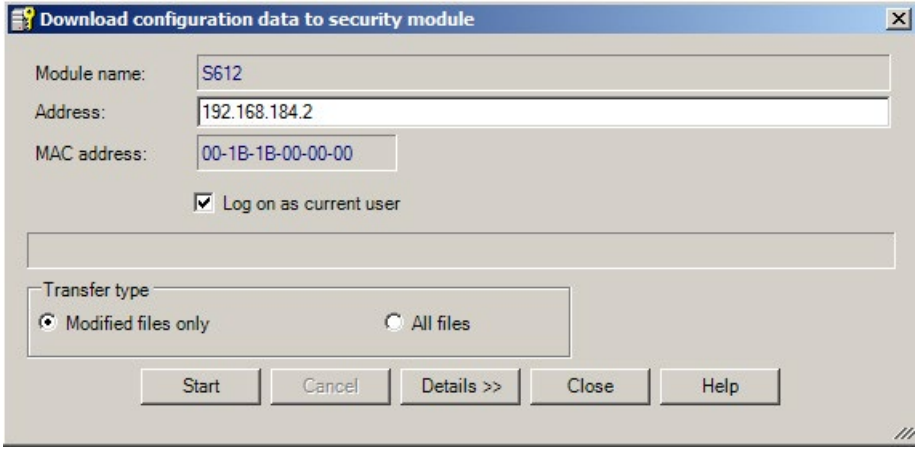
The security project is configured. The settings are saved in the configuration file.

3.3.2.4 Downloading the configuration to the S612 and saving the M-800 configuration

Downloading the configuration to the S612

1. In the content area, select the "S612" security module and select the menu command "Transfer" > "To module(s) …".

   The following dialog opens.



2. Click the "Start" button to start the download.

   If the download was completed free of errors, the security module is restarted automatically and the new configuration activated.

Saving the SCALANCE M-800 configuration

1. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project folder and assign a password for the private key of the certificate, e.g. Di1S+Xo?.

Result

The following files will be saved in the project directory:

- Configuration file: projectname.M-800.txt
- PKCS12 file: projectname.string.M-800.p12
- Remote certificate: Projectname.group1.S612.cer

The configuration file contains the exported configuration information for the SCALANCE M-800 including information on the additionally generated certificates. Follow the instructions in the configuration file.

3.3.3 Configuring SCALANCE M-800

3.3.3.1 Loading a certificate

Requirement

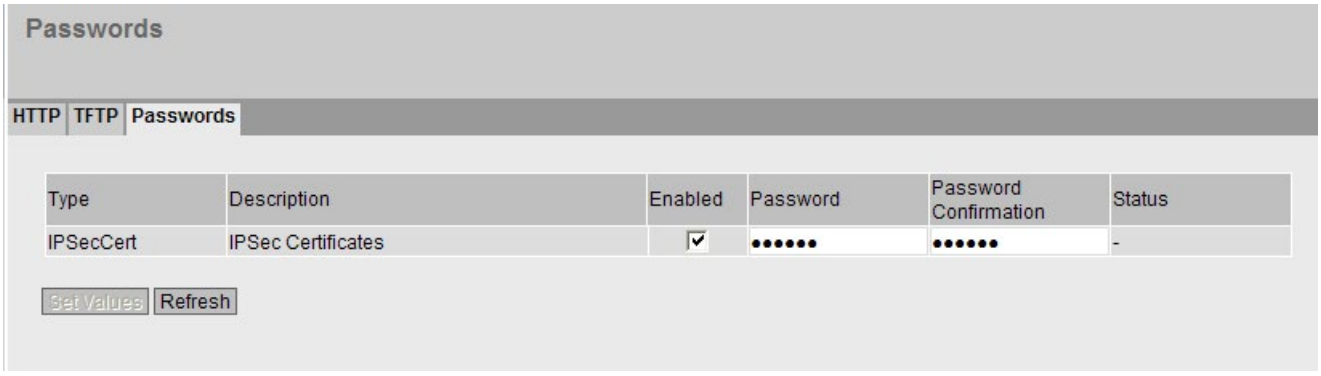
- The correct time is set on the SCALANCE M, refer to the section Setting the time (Page 23).
- Certificates are available.

  You saved the required certificates on the PC in the last section and assigned a password for the private key.

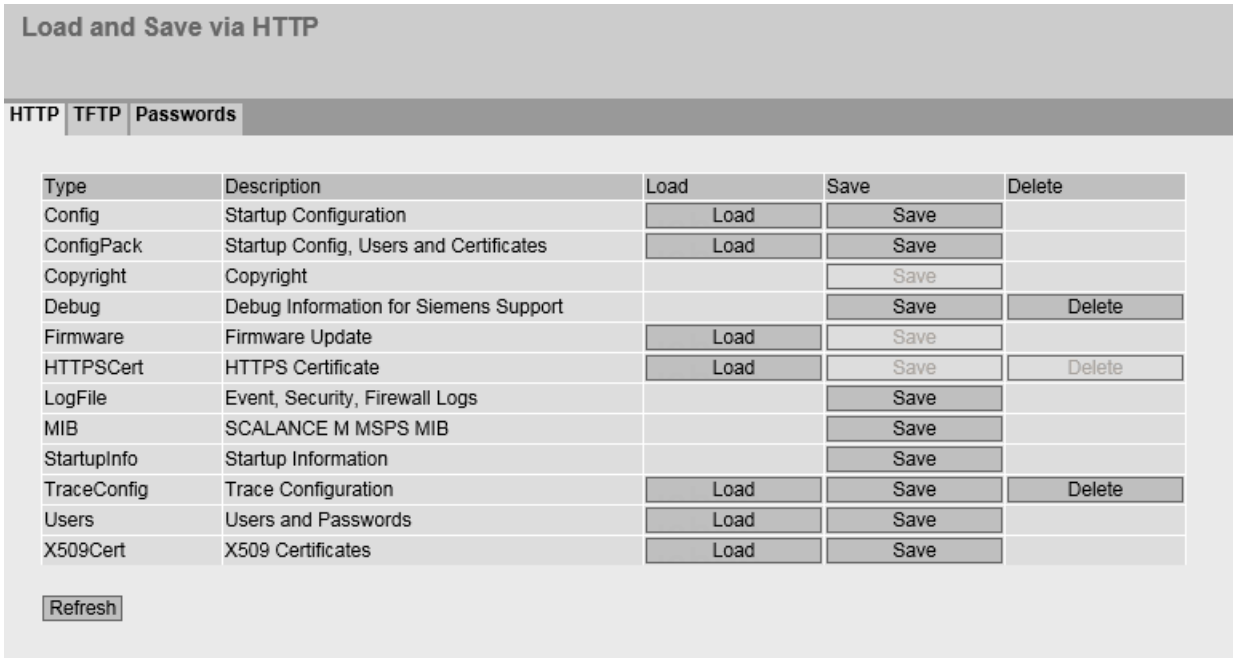
  Transfer the certificates for the SCALANCE M to the Admin PC.

Procedure

1. Click on "System" > "Load & Save" in the navigation area and on the "Password" tab in the content area.
2. For "Password" and "Password Confirmation", enter the password Di1S+Xo?, that you specified for the PKCS12 file.
3. Select "Enabled" and click "Set Values".



4. Click on the "HTTP" tab in the content area.



5. Click on the "Load" button beside "IPSecCert" or "X509cert". The dialog for loading a file is opened.

   Navigate to the remote certificate.

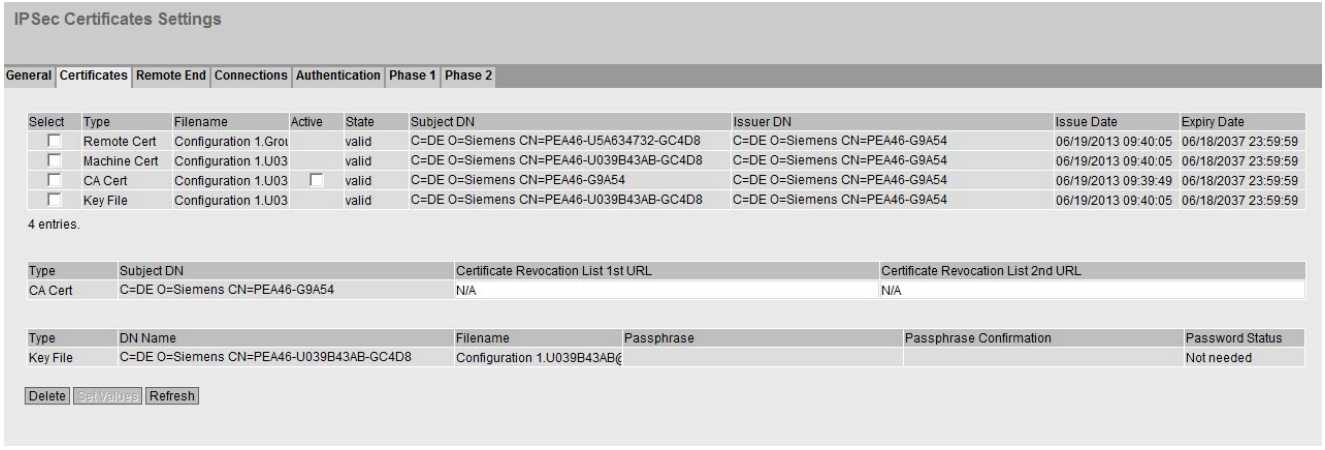
6. Click the "Open" button in the dialog.

   The file is now loaded on the device. After loading successfully, confirm the next dialog with "OK".

7. Repeat steps 5 and 6 for the PKCS12 file.

Result

The certificates are loaded. With "Security" > "IPSec VPN" > "Certificates", you can display the certificates. The loaded certificates must have the status "valid".

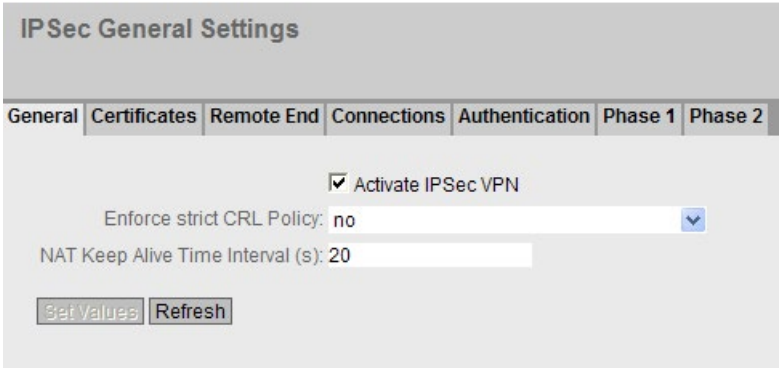


As of firmware version 4.0 certificates are displayed in "Security" > "Certificates".

3.3.3.2 Activating VPN

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select Activate IPSec VPN".



3. Click "Set Values"

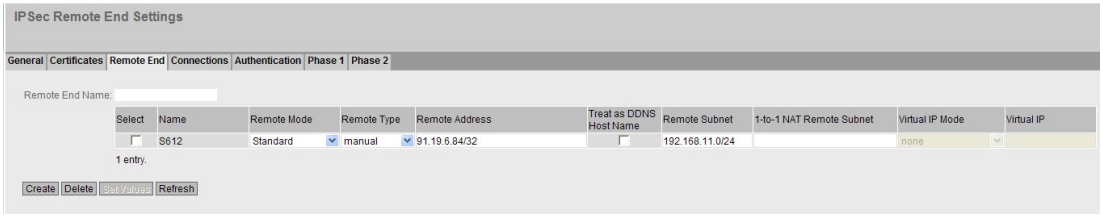
3.3.3.3 Configuring the VPN remote end

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Remote End" tab in the content area.
2. Enter the name of the VPN partner (tunnel endpoint) in "Remote End Name", e.g. S612.
3. Click "Create". A new row is created in the table.
4. Configure the VPN remote end with the following settings from the configuration file:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.11.0/24

5. Click "Set Values".



3.3.3.4 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

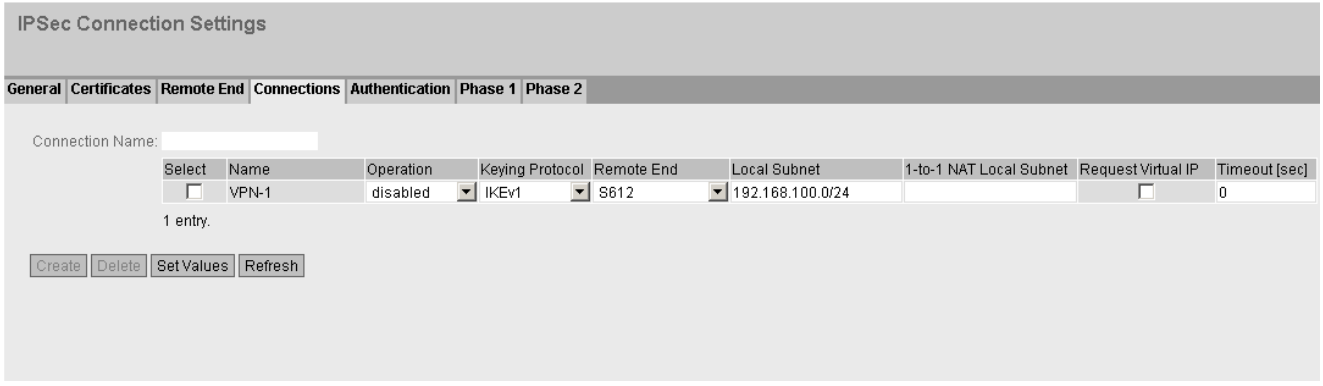
Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Click "Create". A new row is created in the table.

4. Configure the VPN connection with the following settings:

Operation	disabled
Keying Protocol	IKEv1
Remote End	S612 Name of the VPN remote station
Local Subnet	192.168.100.0/24 The local internal subnet 1 in CIDR notation.

5. Click "Set Values".



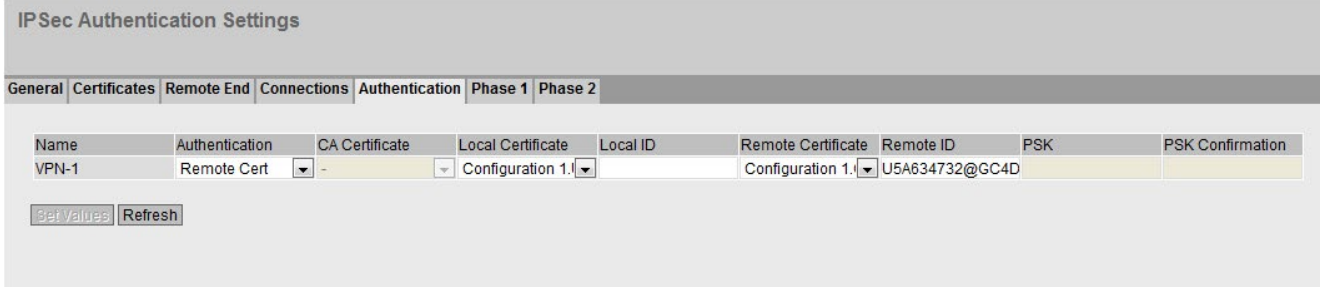
3.3.3.5 Configuring VPN authentication

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Authentication" tab in the content area.
2. Configure the VPN authentication with the following settings from the configuration file:

Authentication	Remote Cert
Local Certificate	projectname.string.M-800.p12
Remote Certificate	Projectname.group1.S612.cer
Remote ID	Remote ID from the configuration file

3. Click "Set Values".



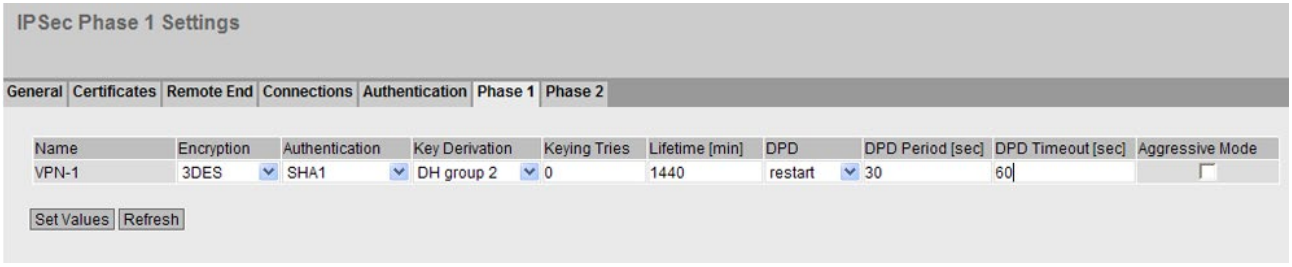
3.3.3.6 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Phase 1" tab in the content area.
2. For "DPD", select "restart".
3. Configure phase 1 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

4. Click "Set Values".

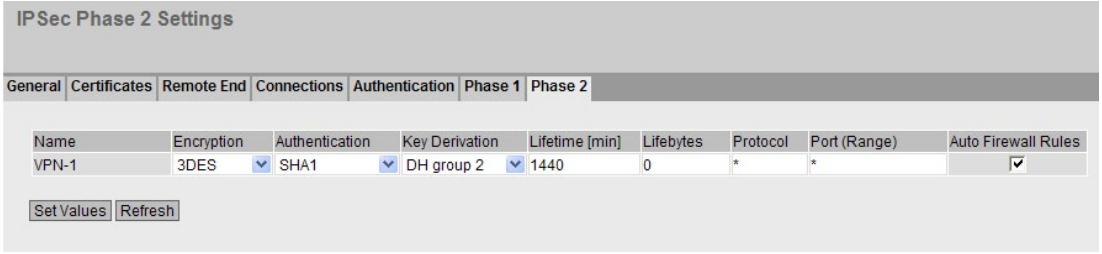


Configuring phase 2

1. Click the "Phase 2" tab.
2. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

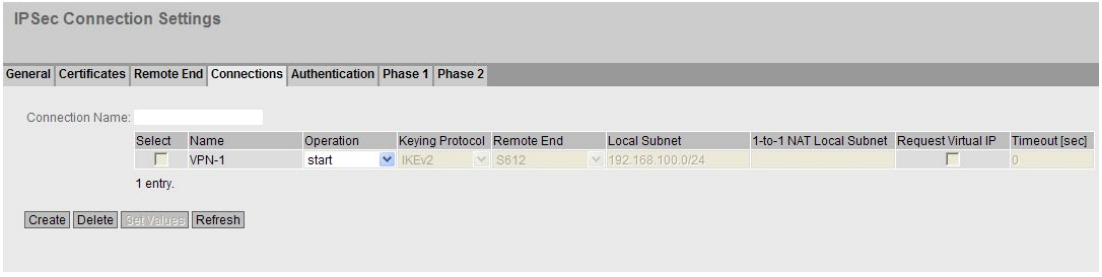
3. Click "Set Values".



3.3.3.7 Establishing the VPN connection

Procedure

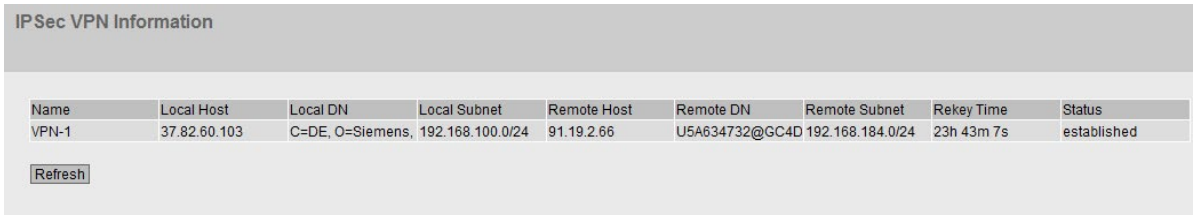
1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. As "Operation", select "start" and click "Set Values".



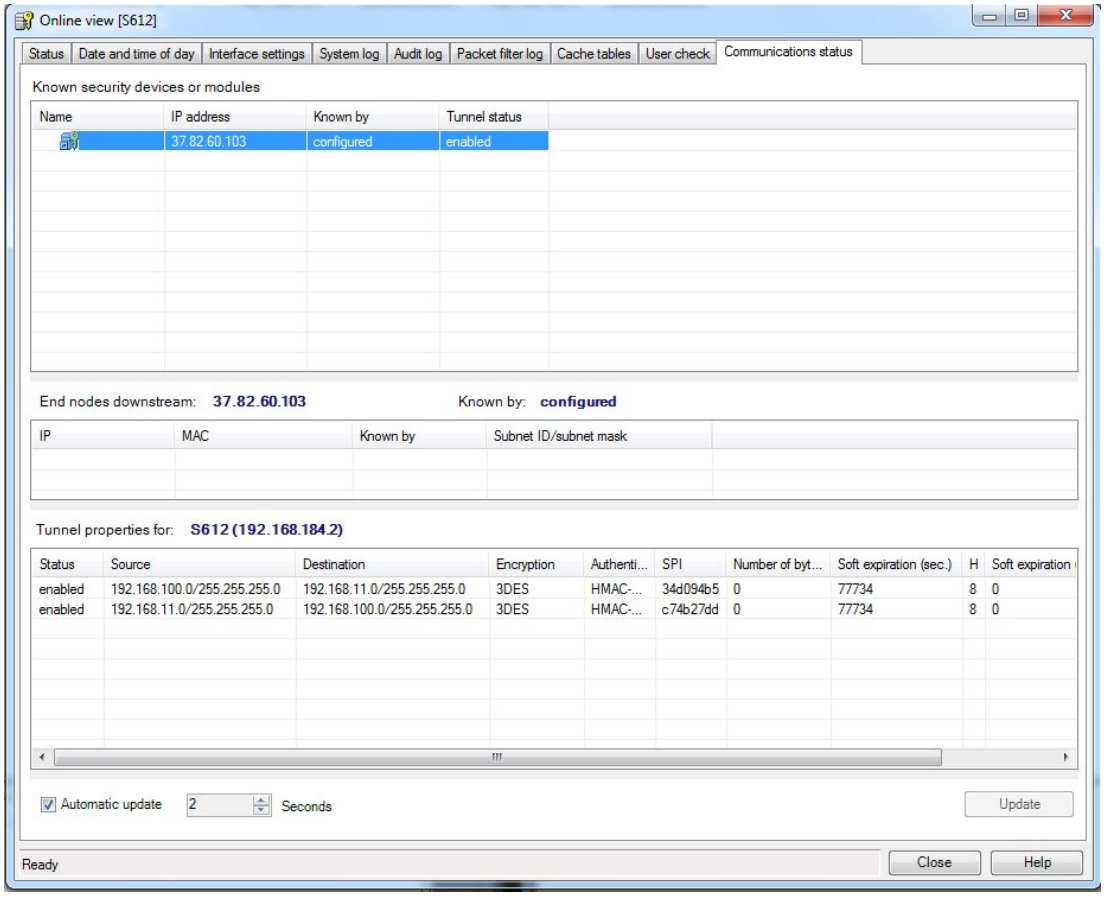
Result

The SCALANCE M establishes the VPN tunnel to the S612. If the VPN tunnel is established, the 🔒 LED is lit green on the device.

You will find more detailed information in "Information" > "IPSec VPN".



You can also see the status of the tunnel connection in the online view of the SCT.



3.4 Firewall with a VPN connection

You can create firewall rules for IPsec in the following ways:

- Automatic

  Here, the firewall rules are created automatically for the specified VPN connection.
- Manual

  Here, you define your own firewall rules for the specified VPN connection.

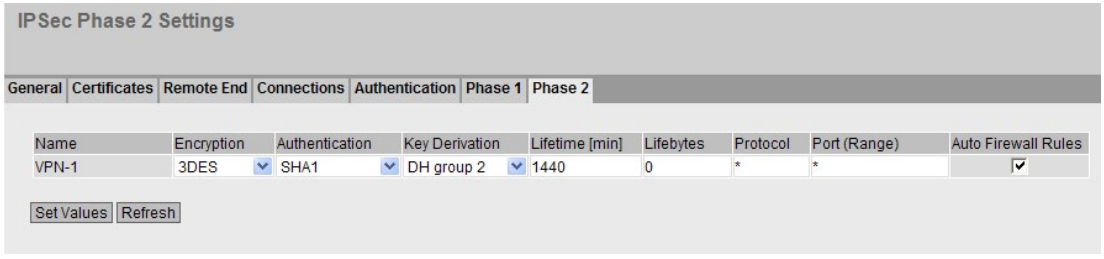
3.4.1 Creating firewall rules automatically

For the example, the VPN tunnel described in the section "Secure VPN tunnel with certificates (Page 162)" is used. The devices have the following IP address setting:

		Internal address
Internal network 1	SCALANCE M-800	192.168.100.1 255.255.255.0
Internal network 2	S612	internal port 192.168.11.2 255.255.255.0

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Phase 2" tab in the content area. The "Auto Firewall Rules" setting is activated as default.



Result

If "Auto Firewall Rule" is enabled, the following firewall rules are active.

Action	From / to	Permitted protocols	For	Source IP addresses	Dest. IP addresses
Allow	VPN tunnel / internal network 1	TCP / UDP / ICMP	all ports or all ICMP packet types	192.168.100.0/24	192.168.11.0/24
Allow	VPN tunnel / internal network 2	TCP / UDP / ICMP	all ports or all ICMP packet types	192.168.11.0/24	192.168.100.0/24
Allow	internal network 2 / VPN tunnel	TCP / UDP / ICMP	all ports or all ICMP packet types	192.168.11.0/24	192.168.100.0/24
Allow	internal network 1 / VPN tunnel	TCP / UDP / ICMP	all ports or all ICMP packet types	192.168.100.0/24	192.168.11.0/24

With these firewall rules, data traffic between internal network 1 and internal network 2 is possible without any restrictions.

HTTP-based access to the remote VPN partner is not allowed. The appropriate firewall rule is created in the section "Creating firewall rules manually (Page 139)".

3.4.2 Creating firewall rules manually

Requirement

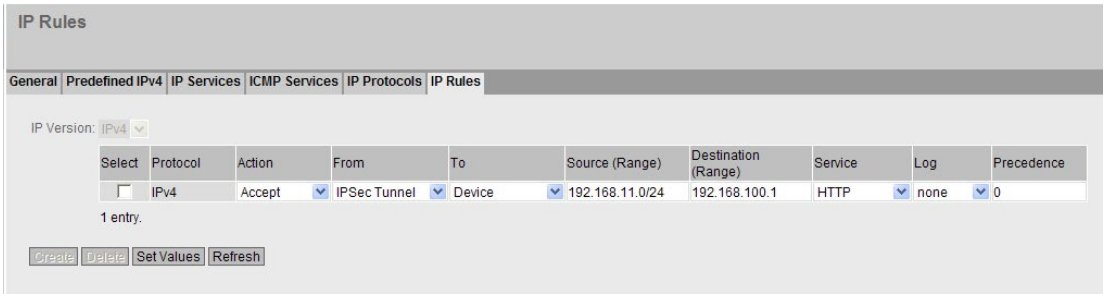
The IP service HTTP has been created, see the section "Auto-Hotspot".

Allow HTTP-based access through the VPN tunnel

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Configure the firewall rule for HTTP with the following settings:

Action	Accept
From	IPsec tunnel
To	Device
Source (Range)	192.168.11.0/24 (all devices of the remote internal network 2)
Destination (Range)	192.168.100.1 (to the required device)
Service	HTTP

3. Click "Set Values". The SCALANCE M can be reached through the VPN tunnel and can be configured with WBM.

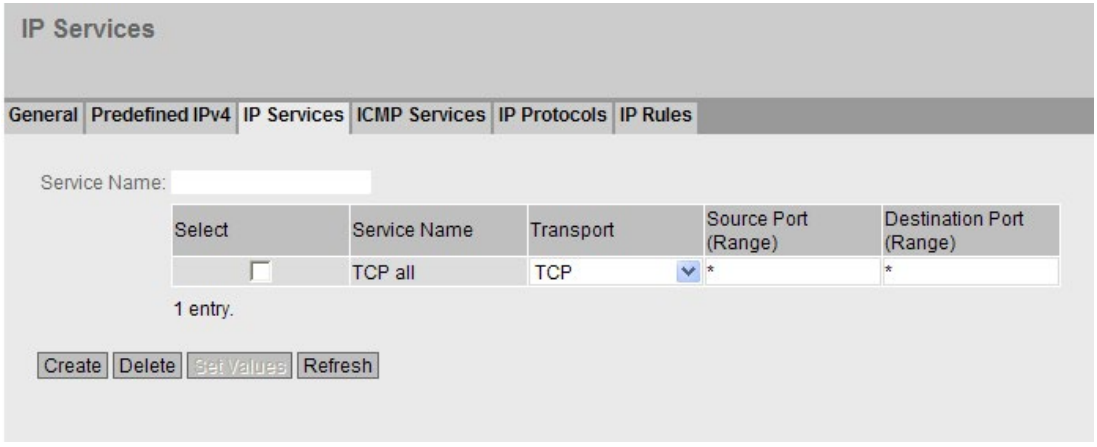


Allow HTTP-based access through the VPN tunnel for a specific device

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. As "Service Name", enter "TCP all" and click "Create". A new entry is created in the table.
3. Configure the service with the following setting:

Transport	TCP

4. Click "Set Values".



5. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
6. Click "Create". A new entry is created in the table.
7. Configure the firewall rule with the following settings:

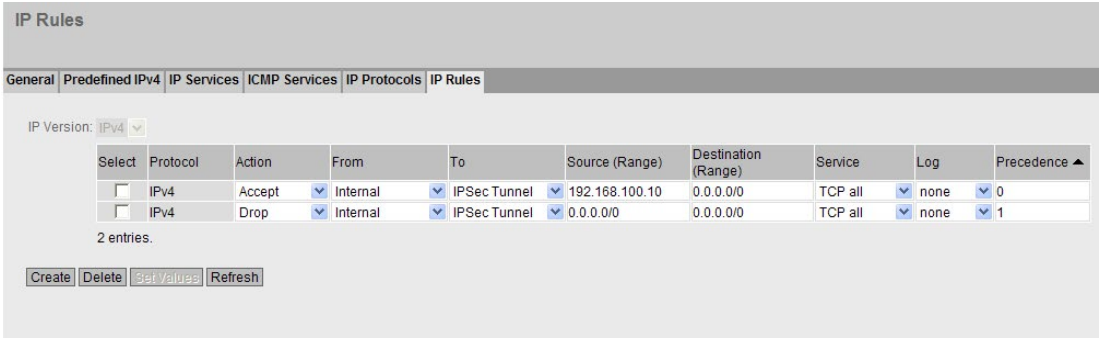
Action	Accept
From	Internal
To	IPsec tunnel
Source (Range)	192.168.100.10 (only this device is allowed to communicate from internal network 1 through the VPN tunnel with TCP)
Destination (Range)	0.0.0.0/0 (to all addresses)
Service	TCP all

8. Click "Create". A new entry is created in the table.

9. Configure the second firewall rule with the following settings:

Action	Drop
From	Internal
To	IPsec tunnel
Source (Range)	0.0.0.0/0 (Prevents TCP data traffic between the internal network and the remote network connected via the VPN tunnel.)
Destination (Range)	
Service	TCP all

10. Click "Set Values".



VPN tunnel between SCALANCE M-800 and security CPs

4

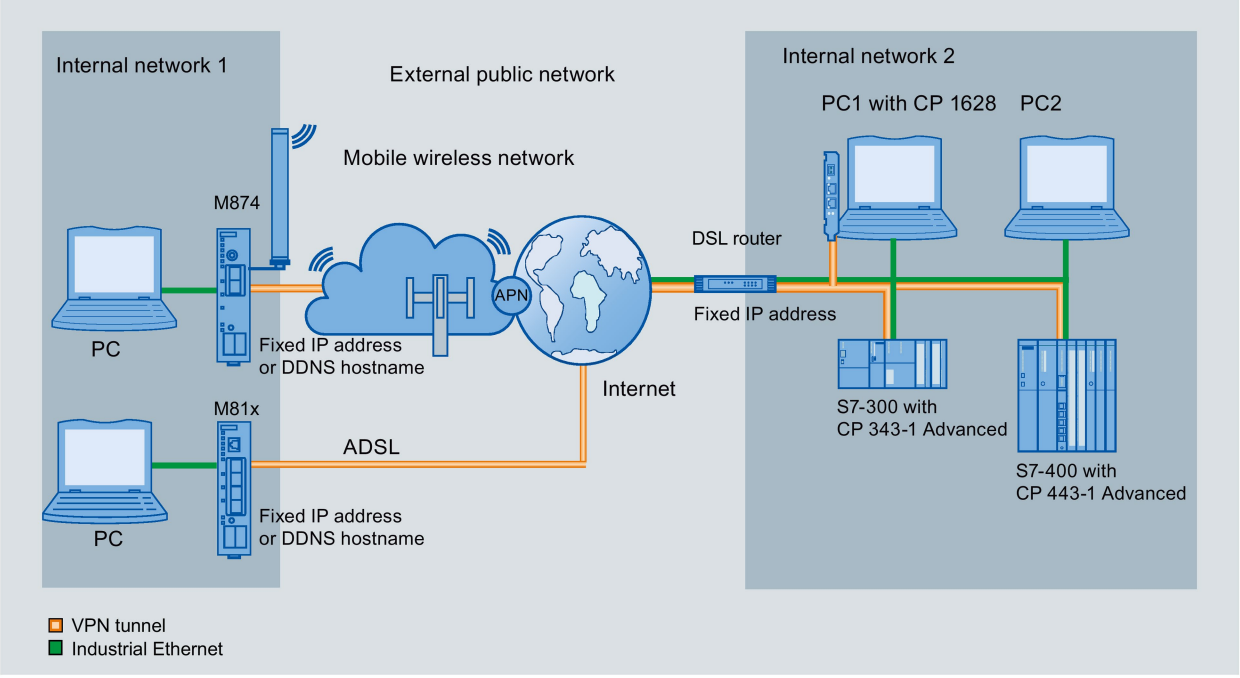
4.1 Procedure in principle

In these examples, a secure VPN tunnel is configured between a SCALANCE M-800 and the CP 1628.

- Example 1: Secure VPN tunnel with pre-shared keys (PSK)
- Example 2: Secure VPN tunnel with certificates

Instead of the CP 1628, a CP 343-1 Advanced or CP 434-1 Advanced can be used.

Structure



Internal network 1 - connection to SCALANCE M-800

- In the test setup, in the internal network, a network node is implemented by an Admin PC connected to an Ethernet interface of the SCALANCE M.
  - Admin PC: Represents a node in the internal network
  - M-800: SCALANCE M module for protection of the internal network
- Connection to the external, public network.
  - Wireless via the antenna of the M874 to the mobile wireless network.
  - Wired via the RJ-45 jack of the M81x to ADSL.

Internal network 2 - attachment to a port of the CP 1628

- In the test setup, in the internal network, each network node is implemented by one PC connected to the internal port of the security module.
  - PC1 with security module 1: PC with CP 1628 for protection of the internal network
  - PC2: PC with the Security Configuration Tool and STEP 7

    The PC represents a node in the internal network.
- Connection to the external, public network via DSL router

  Access to the Internet is via a DSL modem or a DSL router connected to one of the ports of the security module.

Required devices/components

Use the following components for setup:

- Connection to the mobile wireless network
  - 1 x M874 (additional option: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - 1 x suitable antenna
  - 1 x SIM card of your mobile wireless provider. Suitable services are enabled, e.g. Internet.
- Connecting to ADSL
  - 1 x M812 or 1 x M816 (optionally also: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - ADSL access is enabled
- 1 x PC with CP 1628
- 1 x PC with the Security Configuration Tool and STEP 7.
- 1 x DSL modem or DSL router
- 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

		Internal address	External address
Internal network 1	M-800	192.168.100.1 255.255.255.0	Fixed IP address, e.g. 90.90.90.90 Provider dependent As an alternative, the DDNS hostname can also be used.
	Admin PC	192.168.100.20 255.255.255.0	

		Internal address	External address
Internal network 2	DSL router	192.168.184.254 255.255.255.0	Fixed IP address (WAN IP address), e.g. 91.19.6.84
	PC1 with CP 1628	For CP 1628: The IP address of the NDIS interface, e.g. 192.168.184.10. (is configured on PC1) For CP 343-1 Advanced or CP 434-1 Advanced: The IP address of the PROFINET interface.	For CP 1628: The IP address of the Industrial Ethernet interface, e.g. 192.168.184.2. For CP 343-1 Advanced or CP 434-1 Advanced: The IP address of the Gbit interface.
	PC2	192.168.184.20 255.255.255.0	

Requirement

- The CP 1628 is connected to the Internet via the DSL router.
- In the properties of the CP, the internal IP address of the DSL router is configured as a default gateway.
- the SCALANCE M-800 is connected to the WAN , refer to "Connecting SCALANCE M-800 to the WAN (Page 11)".
- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

Example 1: Secure VPN tunnel with PSK

Configuring a VPN tunnel with the SCT V3.x

1. Creating project and modules with SCT (Page 147)
2. Configuring a tunnel connection (Page 148)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 150)

Configuring a VPN tunnel with the SCT V4.x

1. Creating project and modules with SCT (Page 152)
2. Configuring a tunnel connection (Page 154)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 156)

Configuring SCALANCE M-800

1. Activating VPN (Page 157)
2. Configuring the VPN remote end (Page 157)
3. Configuring a VPN connection (Page 158)
4. Configuring VPN authentication (Page 159)

5. Configuring phase 1 and phase 2 (Page 160)
6. Establishing the VPN connection (Page 161)

Example 2: Secure VPN tunnel with certificates

Configuring a VPN tunnel with the SCT V3.x

1. Creating project and modules with SCT (Page 162)
2. Configuring a tunnel connection (Page 164)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 166)

Configuring a VPN tunnel with the SCT V3.x

1. Creating project and modules with SCT (Page 168)
2. Configuring a tunnel connection (Page 170)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 172)

Configuring SCALANCE M-800

1. Loading a certificate (Page 173)
2. Activating VPN (Page 175)
3. Configuring the VPN remote end (Page 176)
4. Configuring a VPN connection (Page 176)
5. Configuring VPN authentication (Page 177)
6. Configuring phase 1 and phase 2 (Page 178)
7. Establishing the VPN connection (Page 179)

4.2 Secure VPN tunnel with PSK

4.2.1 Configuring a VPN tunnel with the SCT V3.x

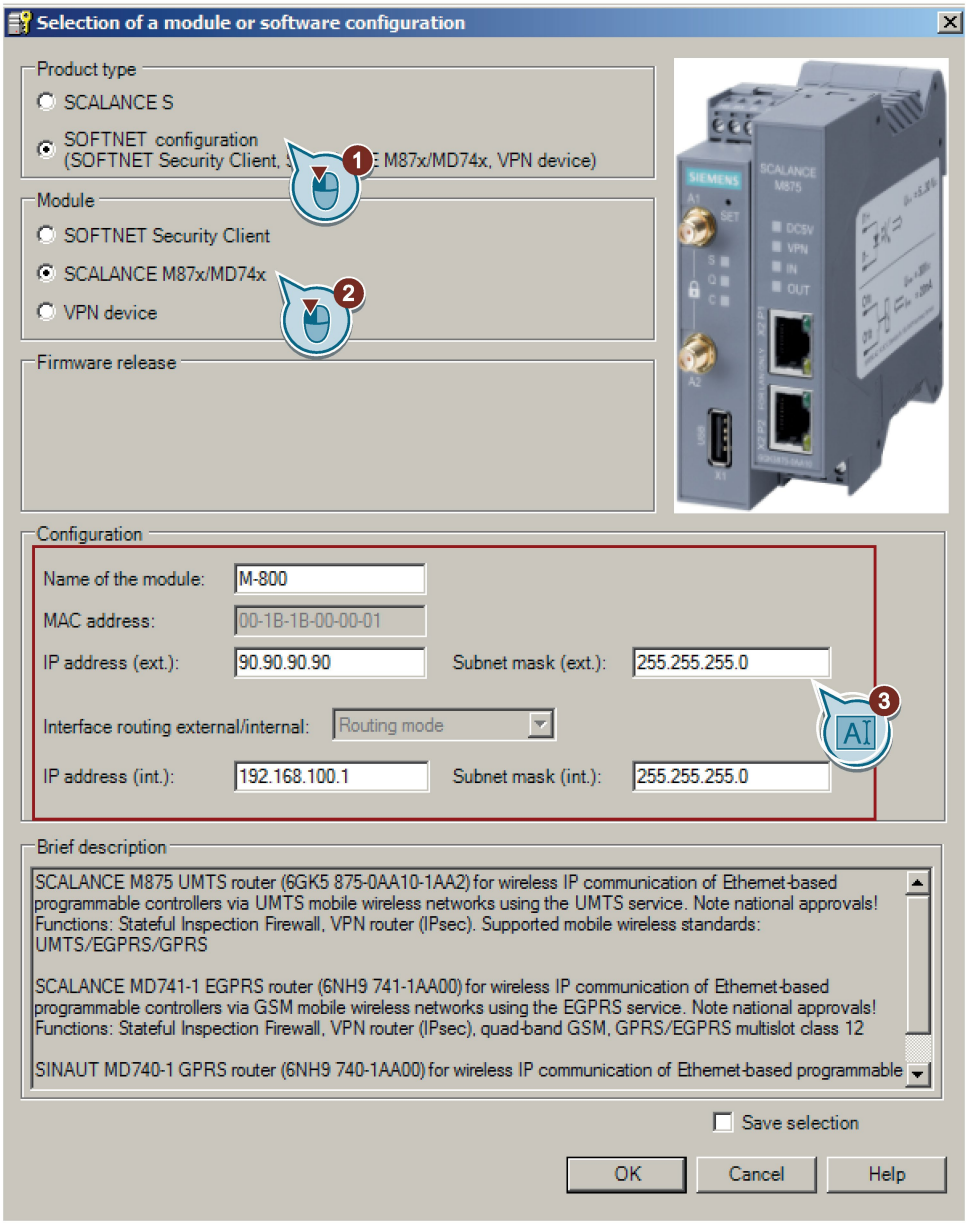
4.2.1.1 Creating project and modules with SCT

Procedure

1. On the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password.

   The "administrator" role is assigned to the user automatically.
3. Confirm the dialog with "OK". A new project is created.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
   The created CP is displayed in the list of configured modules.
5. Generate a second module with the "Insert" > "Module" menu command.

6. Enter the values assigned to the SCALANCE M-800 from the "Settings used (Page 143)" table.



7. Confirm the dialog with "OK".

Result

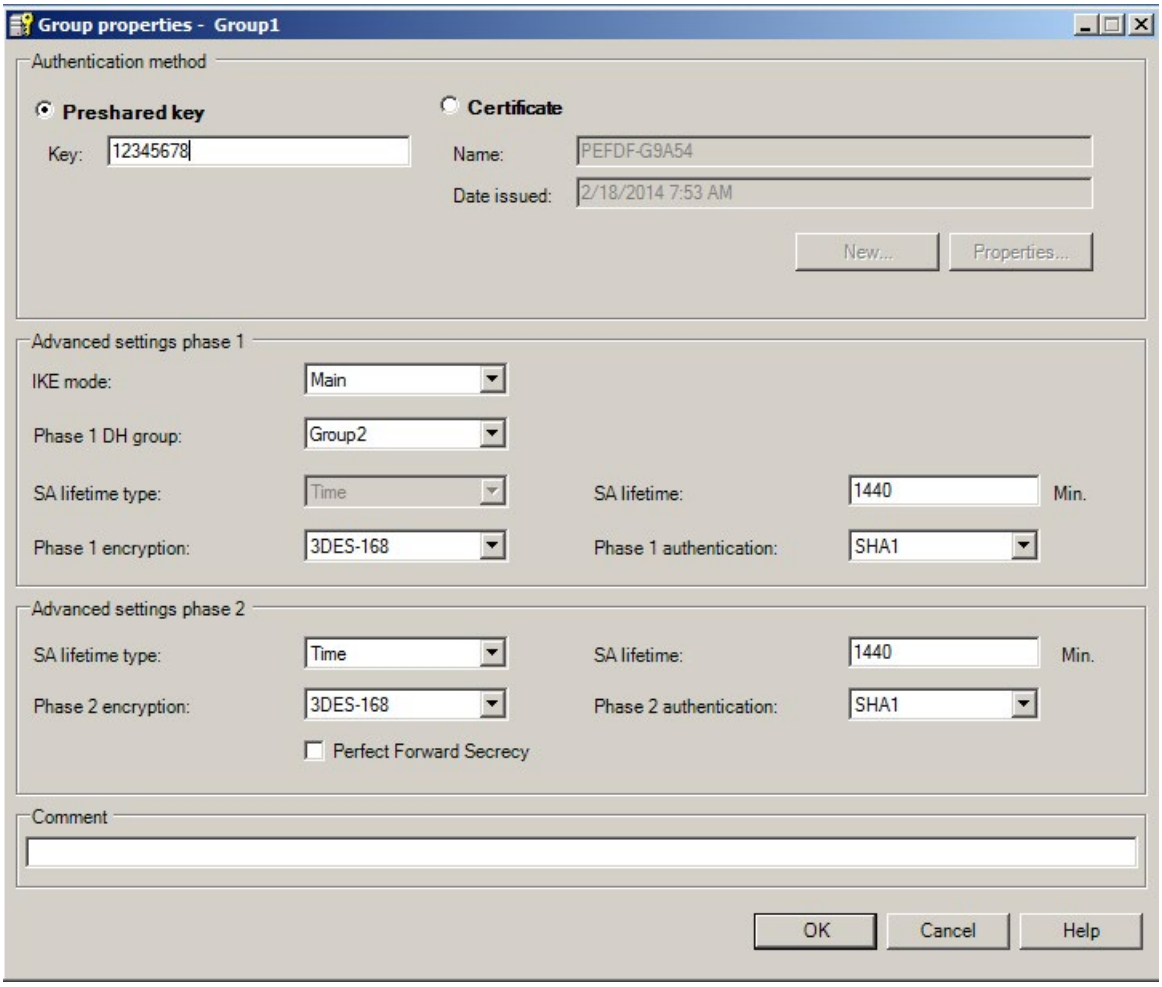
The CP and the SCALANCE M-800 will then be displayed in the list of configured modules.

4.2.1.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the CP are assigned to the same VPN group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the SCALANCE M-800 and the CP in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu
6. For this configuration example, configure the group properties with the following settings.



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

7. Save the project with the "Project" > "Save" menu command.

Result

The configuration of the tunnel connection is complete. The settings are saved in the configuration file.

4.2.1.3 Downloading the configuration to the CP and saving the M-800 configuration

Downloading the configuration to the CP

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module …" menu.
   - For CP 1628: If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.
   - For CP 343-1 Advanced or CP 434-1 Advanced: Restart the S7 CPU following the download, to activate the new configuration

Saving the SCALANCE M-800 configuration

1. In STEP 7, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
2. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
3. Save the configuration file "Projectname.M-800.txt" in your project directory.

Result

The following file will be saved in the project directory:

- Configuration file: projectname.M-800.txt

The configuration file contains the exported configuration information for the SCALANCE M-800.

Configuration file	Settings in WBM
IPsec VPN > Connections > VPN Standard Mode - Edit Settings	Security > IPSec VPN > Remote End > Remote Mode: Standard
Address of the remote site's VPN gateway: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentication method: Pre Shared Key	Security > IPSec VPN > Authentication > Authentication: PSK
Pre Shared Key: 12345678	Security > IPSec VPN > Authentication > PSK und PSK Confirmation: 12345678
Remote ID: U28098881@GEA32	Security > IPSec VPN > Authentication > Remote ID not required. In WBM, the IP address of the Industrial Ethernet interface is entered. In this example, this is 192.168.184.2

Configuration file	Settings in WBM
Local ID: U269159D5@GEA32	Security > IPSec VPN > Authentication > Local ID not required. The entry remains empty in the WBM.
Remote net address: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Remote subnet mask: 255.255.255.0	
Local net address: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Local subnet mask: 255.255.255.0	
IPsec VPN > Connections > Edit IKE	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA encryption: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA mode: Main mode	--
ISAKMP-SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPsec SA encryption: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPsec SA hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPsec SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 2 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--
DH/PFS group: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: On	--
DPD delay (seconds): 150	--
DPD timeout (seconds): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD maximum failures: 5	--

4.2.2 Configuring a VPN tunnel with the SCT V4.x

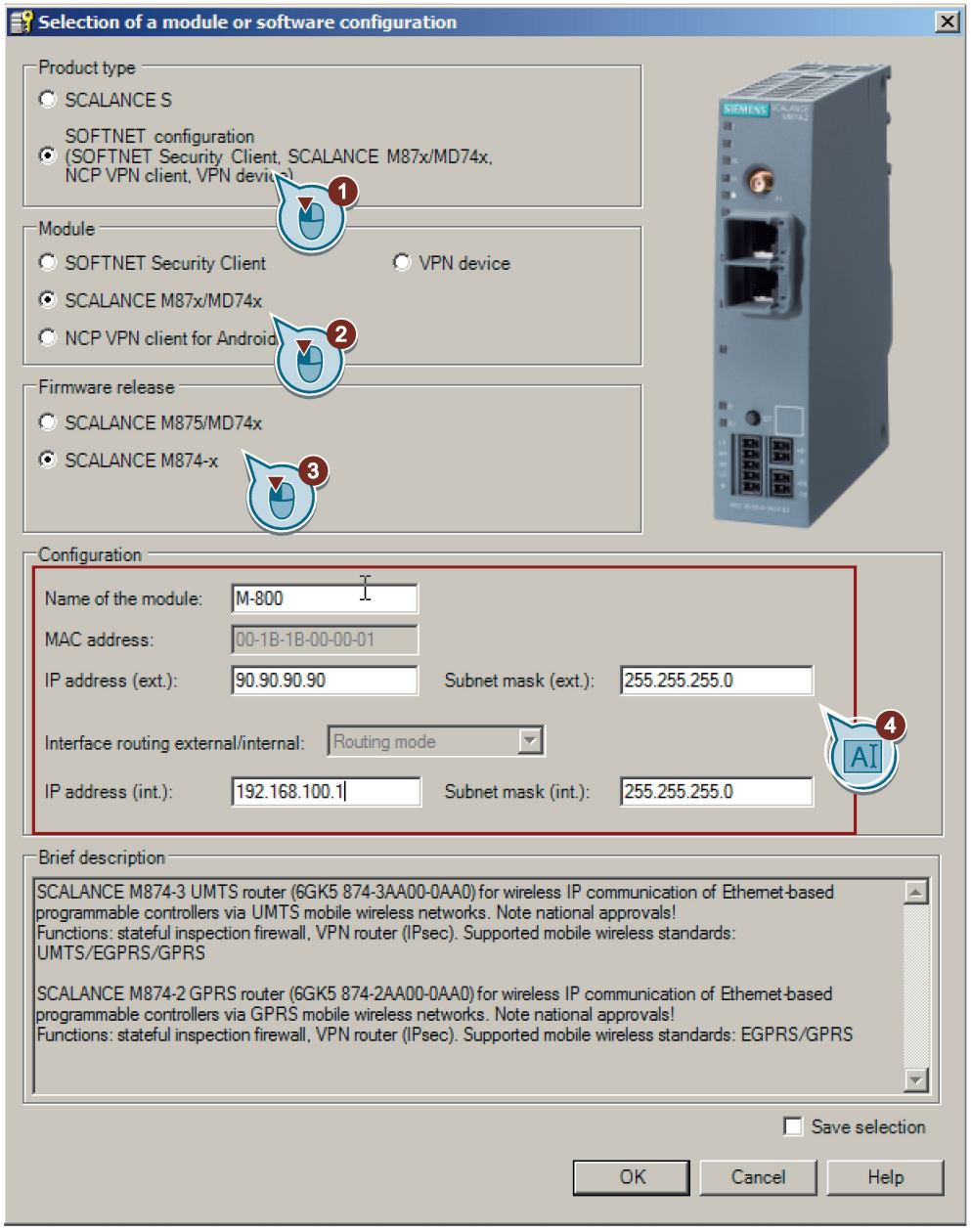
4.2.2.1 Creating project and modules with SCT

Procedure

1. On the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password.

   The "administrator" role is assigned to the user automatically.
3. Confirm the dialog with "OK". A new project is created.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
   The created CP is displayed in the list of configured modules.

5. Generate a second module with the "Insert" > "Module" menu command.



6. Enter the values assigned to the SCALANCE M-800 from the "Settings used (Page 143)" table.
7. Confirm the dialog with "OK".

Result

The CP and the SCALANCE M-800 will then be displayed in the list of configured modules.

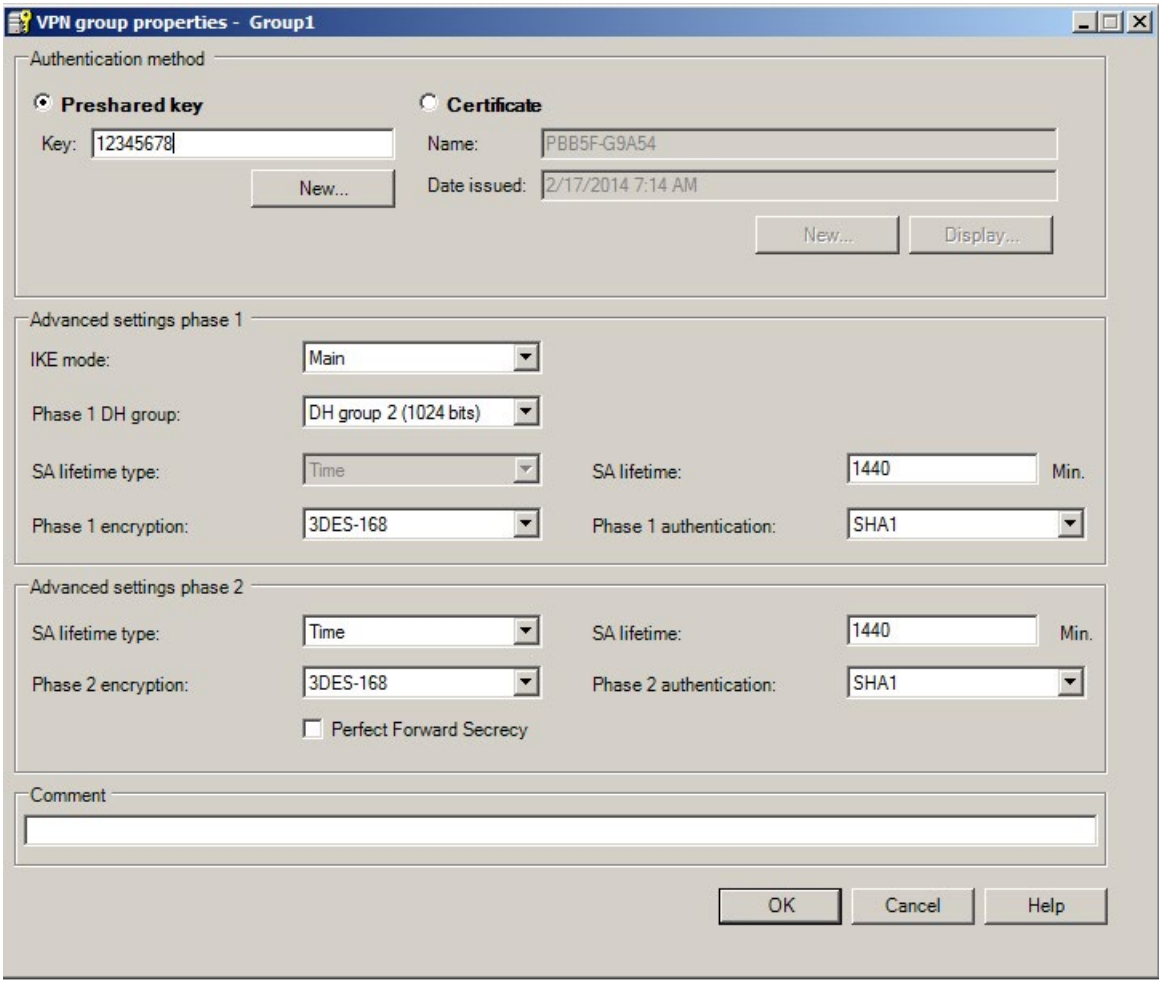
4.2.2.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the CP are assigned to the same VPN group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation panel.
3. Select the SCALANCE M-800 and the CP in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu

6. For this configuration example, configure the group properties with the following settings.



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

7. Save the project with the "Project" > "Save" menu command.

Result

The configuration of the tunnel connection is complete. The settings are saved in the configuration file.

4.2.2.3 Downloading the configuration to the CP and saving the M-800 configuration

Downloading the configuration to the CP

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module …" menu.
   - For CP 1628: If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.
   - For CP 343-1 Advanced or CP 434-1 Advanced: Restart the S7 CPU following the download, to activate the new configuration

Saving the SCALANCE M-800 configuration

1. In STEP 7, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
2. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
3. Save the configuration file "Projectname.M-800.txt" in your project directory.

Result

The following file will be saved in the project directory:

- Configuration file: projectname.M-800.txt

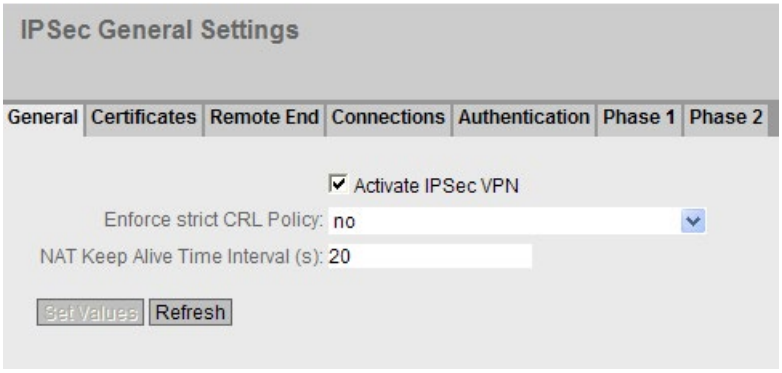
The configuration file contains the exported configuration information for the SCALANCE M-800. Follow the instructions in the configuration file.

4.2.3 Configuring SCALANCE M-800

4.2.3.1 Activating VPN

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select Activate IPSec VPN".



3. Click "Set Values"

4.2.3.2 Configuring the VPN remote end

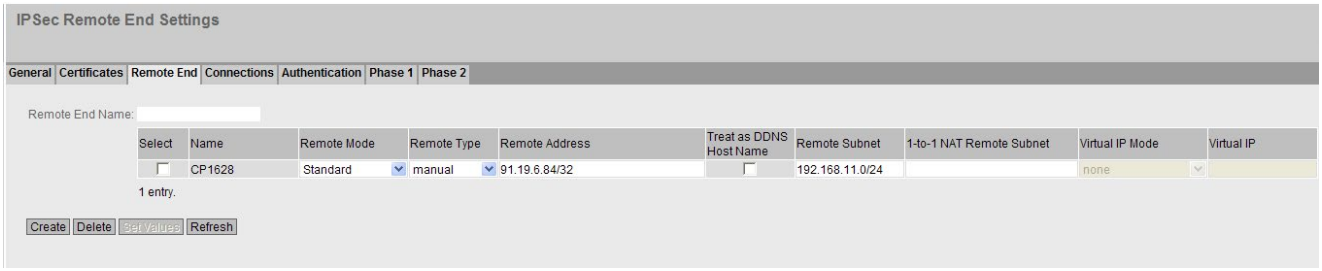
Procedure

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Remote End" tab in the content area.
2. Enter the name of the VPN partner (tunnel endpoint) in "Remote End Name", e.g. CP1628.
3. Click "Create". A new row is created in the table.

4. For the configuration example, configure the VPN remote end with the following settings:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.184.0/24

5. Click "Set Values".



4.2.3.3 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

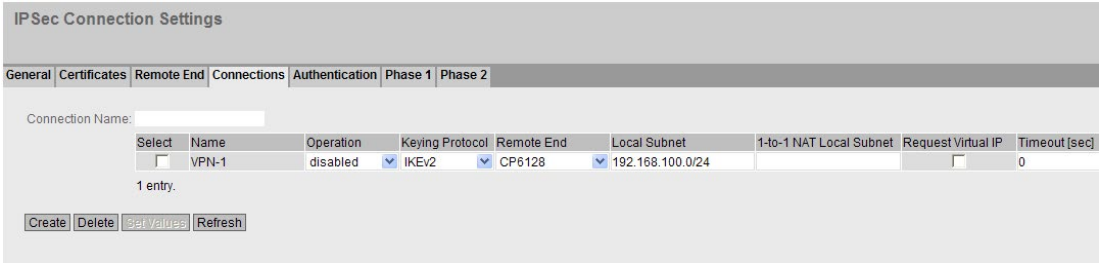
Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Click "Create". A new row is created in the table.

4. For the configuration example, configure the VPN connection with the following settings:

Operation	disabled
Keying Protocol	IKEv1
Remote End	CP1628 Name of the VPN remote station
Local Subnet	192.168.100.0/24 The local internal subnet 1 in CIDR notation.

5. Click "Set Values".



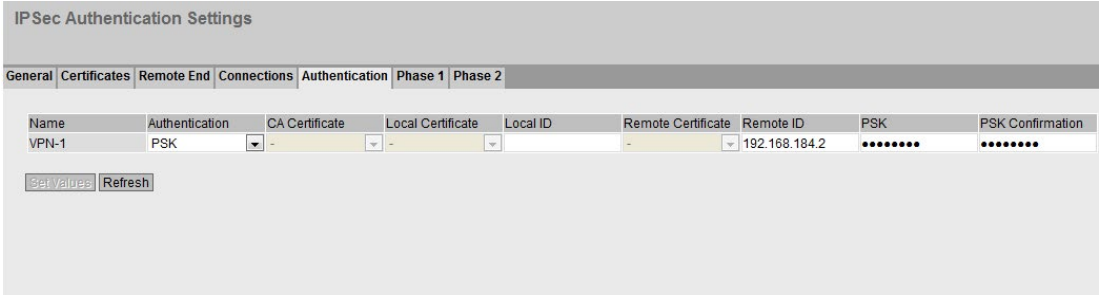
4.2.3.4 Configuring VPN authentication

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Authentication" tab in the content area.
2. Configure the VPN authentication with the following settings:

Authentication	PSK
Local ID	no entry necessary
Remote ID	192.168.184.2 The IP address of the VPN remote station.
PSK / PSK Confirmation	12345678 The key that you configured in the SCT.

3. Click "Set Values".



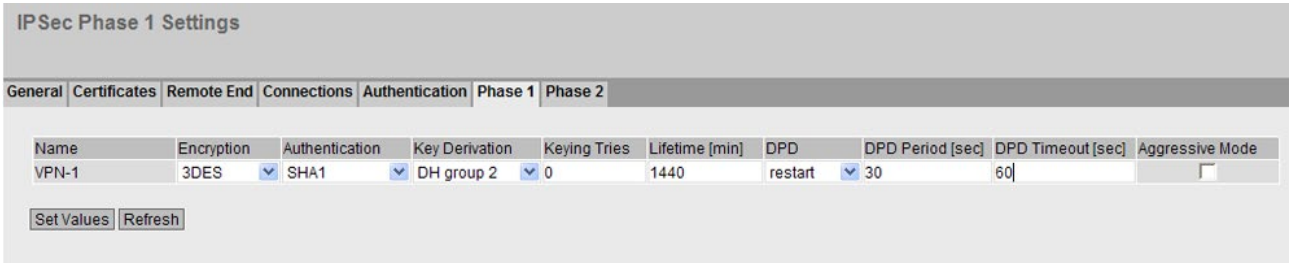
4.2.3.5 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Phase 1" tab in the content area.
2. For "DPD", select "restart".
3. Configure phase 1 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

4. Click "Set Values".

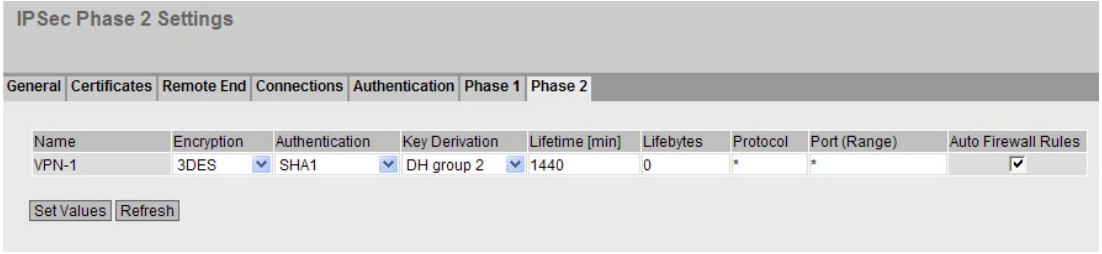


Configuring phase 2

1. Click the "Phase 2" tab.
2. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

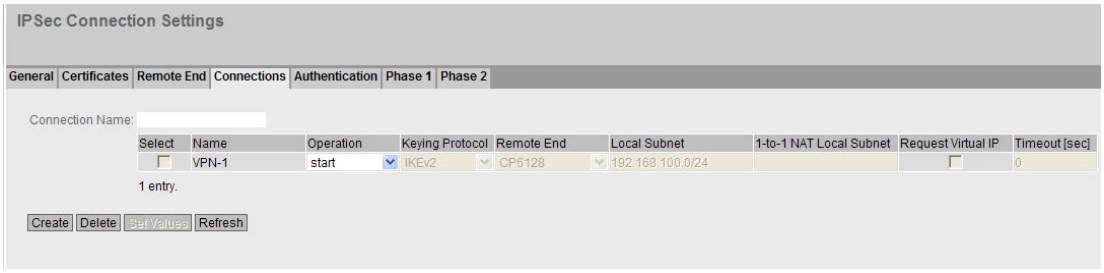
3. Click "Set Values".



4.2.3.6 Establishing the VPN connection

Procedure

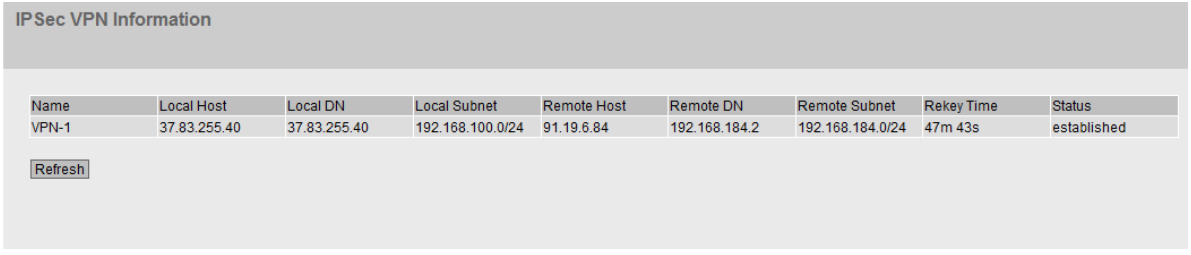
1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. As "Operation", select "start" and click "Set Values".



Result

The SCALANCE M-800 establishes the VPN tunnel to the CP 1628. If the VPN tunnel is established, the 🔒 LED is lit green on the device.

You will find more detailed information in "Information" > "IPSec VPN".



4.3 Secure VPN tunnel with certificates

4.3.1 Configuring a VPN tunnel with the SCT V3.x

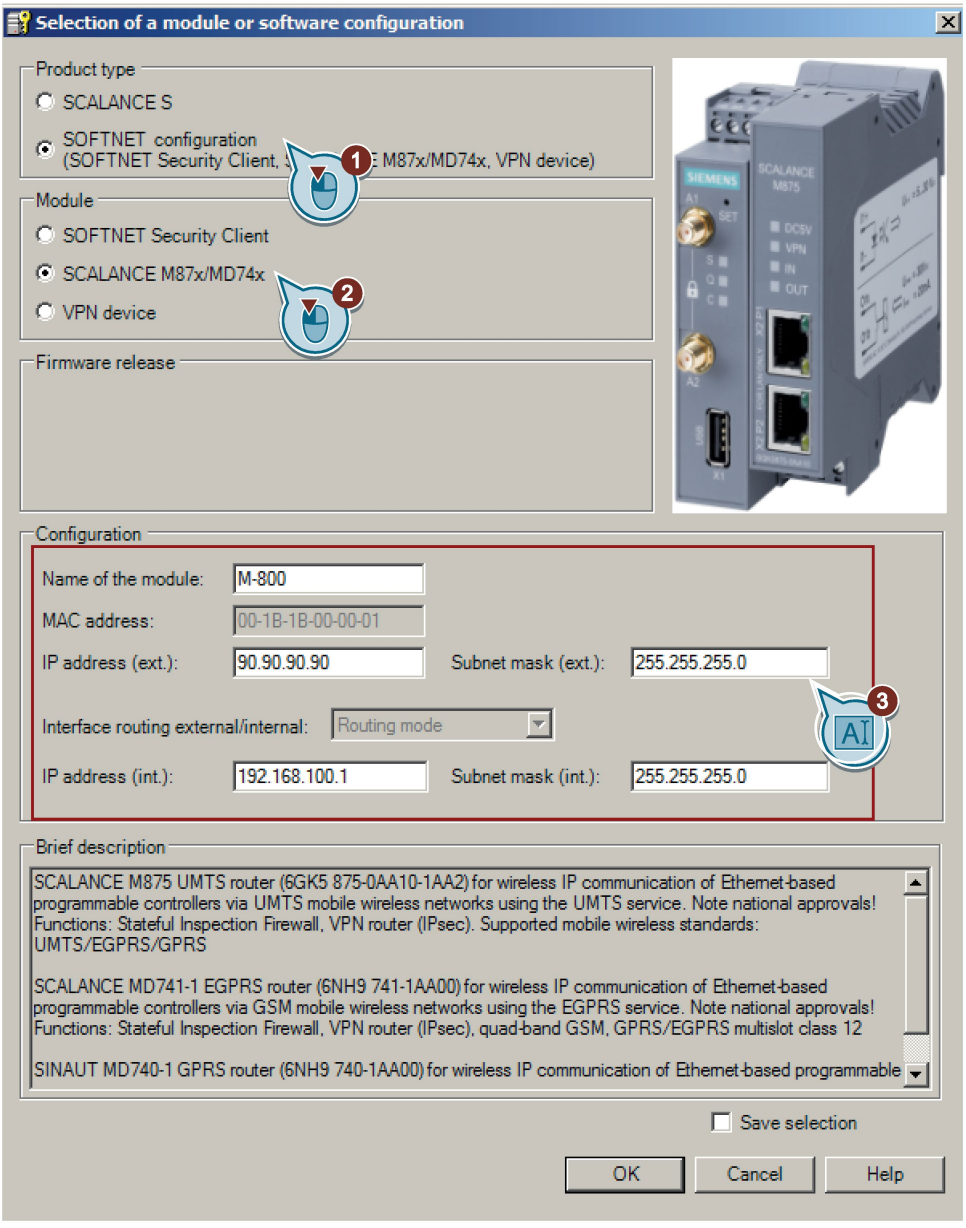
4.3.1.1 Creating project and modules with SCT

Procedure

1. On the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password.

   The "administrator" role is assigned to the user automatically.
3. Confirm the dialog with "OK". A new project is created.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
   The created CP is displayed in the list of configured modules.
5. Generate a second module with the "Insert" > "Module" menu command.

6. Enter the values assigned to the SCALANCE M-800 from the "Settings used (Page 143)" table.



7. Confirm the dialog with "OK".

Result

The CP and the SCALANCE M-800 will then be displayed in the list of configured modules.

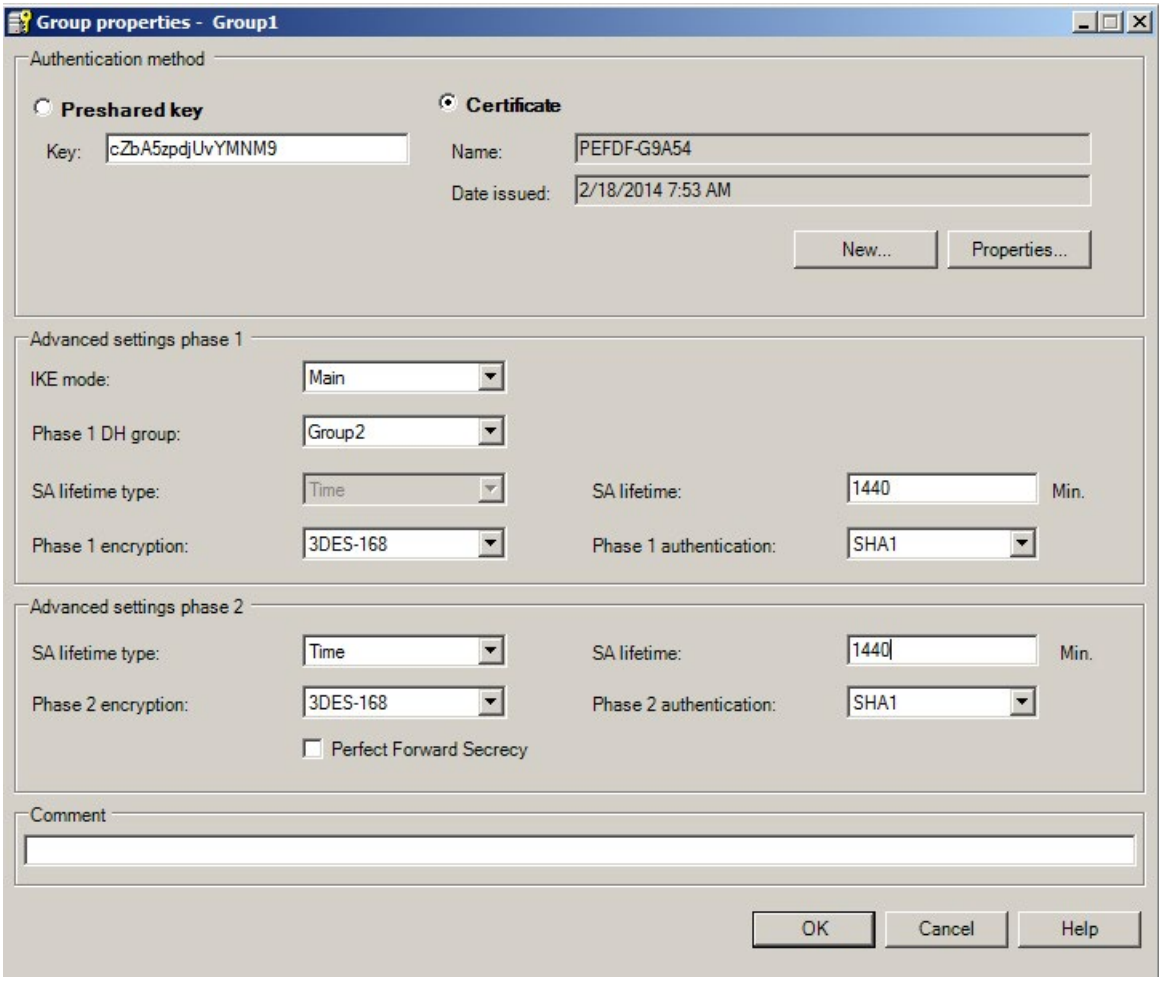
4.3.1.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the CP are assigned to the same group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the SCALANCE M-800 and the CP in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu

6. For this configuration example, configure the group properties with the following settings:



   If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

7. Select the menu command "Project" > "Save". Save the security project under the required name.

Result

The configuration of the tunnel connection is complete. The settings are saved in the configuration file.

4.3.1.3 Downloading the configuration to the CP and saving the M-800 configuration

Downloading the configuration to the CP

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module …" menu.
   - For CP 1628: If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.
   - For CP 343-1 Advanced or CP 434-1 Advanced: Restart the S7 CPU following the download, to activate the new configuration.

Saving the SCALANCE M configuration

1. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project folder and assign a password for the private key of the certificate, e.g. Di1S+Xo?.

Result

The following files will be saved in the project directory:

- Configuration file: projectname.M-800.txt
- PKCS12 file: projectname.string.M-800.p12
- Remote certificate: Projectname.group1.CP.cer

The configuration file contains the exported configuration information for the SCALANCE M-800 including information on the additionally generated certificates.

Configuration file	Settings in WBM
IPsec VPN > Certificates Upload Remote Site Certificate: Configuration-1.group1.CP.cer Upload PKCS12 File (.p12): Configuration-1.U800CB3FF@G471C.M-800.p12	System > Load&Save > HTTP > IPSecCert : Load
IPsec VPN > Connections > VPN Standard Mode - Edit Settings	Security > IPSec VPN > Remote End > Remote Mode: Standard
Address of the remote site's VPN gateway: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentication method: X.509 remote certificate	Security > IPSec VPN > Authentication > Authentication: Remote Cert
Remote Certificate: Configuration-1.group1.CP.cer	Security > IPSec VPN > Authentication > Remote Certificate: Configuration-1.Gruppe1.CP.cer

Configuration file	Settings in WBM
Remote ID: U5A634732@GC4D8	Security > IPSec VPN > Authentication > Remote ID: U5A634732@GC4D8
Remote net address: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Remote subnet mask: 255.255.255.0	
Local net address: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Local subnet mask: 255.255.255.0	
IPsec VPN > Connections > Edit IKE	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA encryption: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA mode: Main mode	--
ISAKMP-SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPsec SA encryption: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPsec SA hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPsec SA lifetime (seconds): 86400 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): No	--
DH/PFS group: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: On	--
DPD delay (seconds): 150	--
DPD timeout (seconds): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD maximum failures: 5	--

4.3.2 Configuring a VPN tunnel with the SCT V4.x

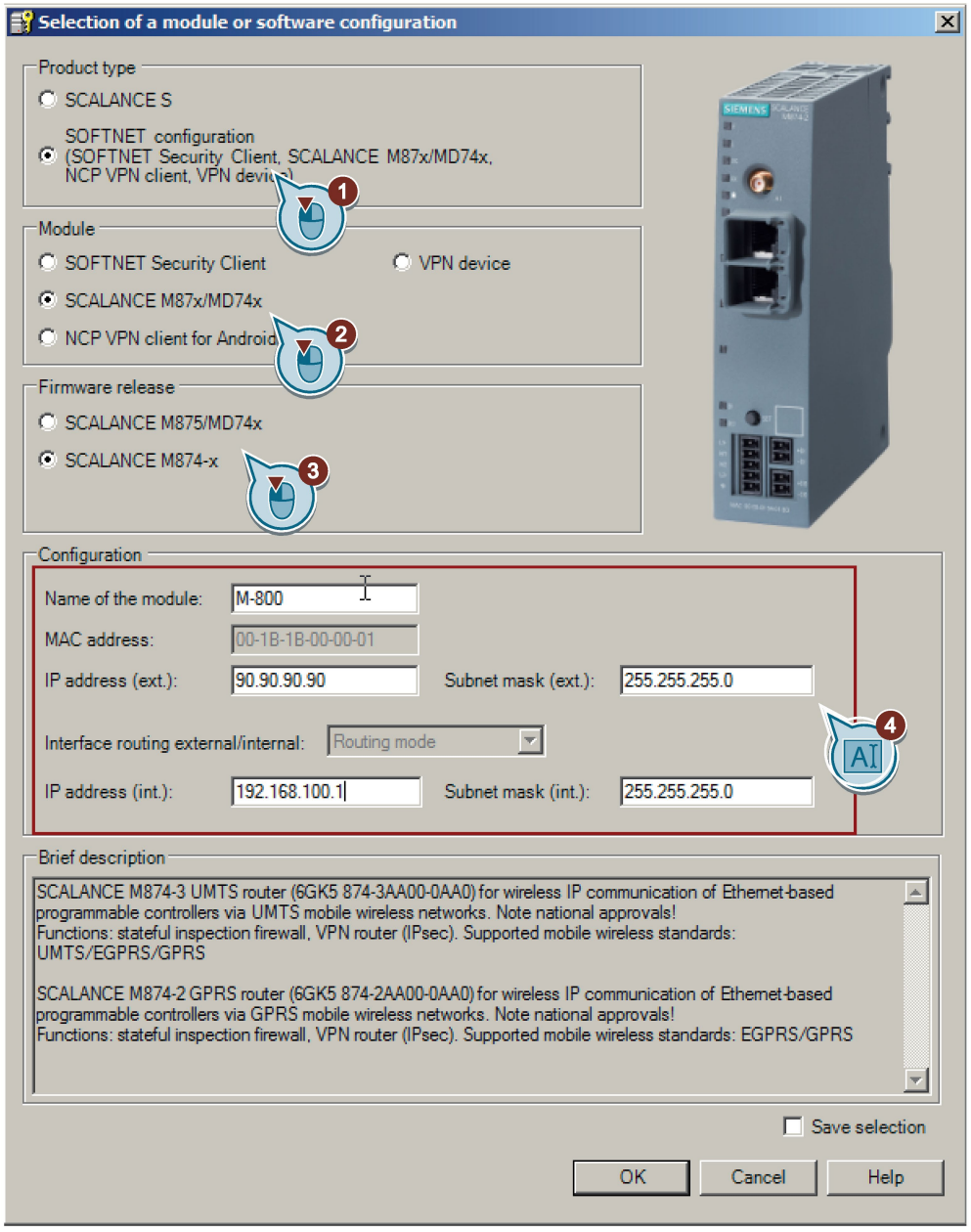
4.3.2.1 Creating project and modules with SCT

Procedure

1. On the "Security" tab of the object properties of the CP 1628, select the "Enable security" check box.
2. In the dialog that follows, create a new user with a user name and the corresponding password.

   The "administrator" role is assigned to the user automatically.
3. Confirm the dialog with "OK". A new project is created.
4. In HW Config, open the Security Configuration Tool with the "Edit" > "Security Configuration Tool" menu command.
   The created CP is displayed in the list of configured modules.

5. Generate a second module with the "Insert" > "Module" menu command.



6. Enter the values assigned to the SCALANCE M-800 from the "Settings used (Page 143)" table.
7. Confirm the dialog with "OK".

Result

The CP and the SCALANCE M-800 will then be displayed in the list of configured modules.

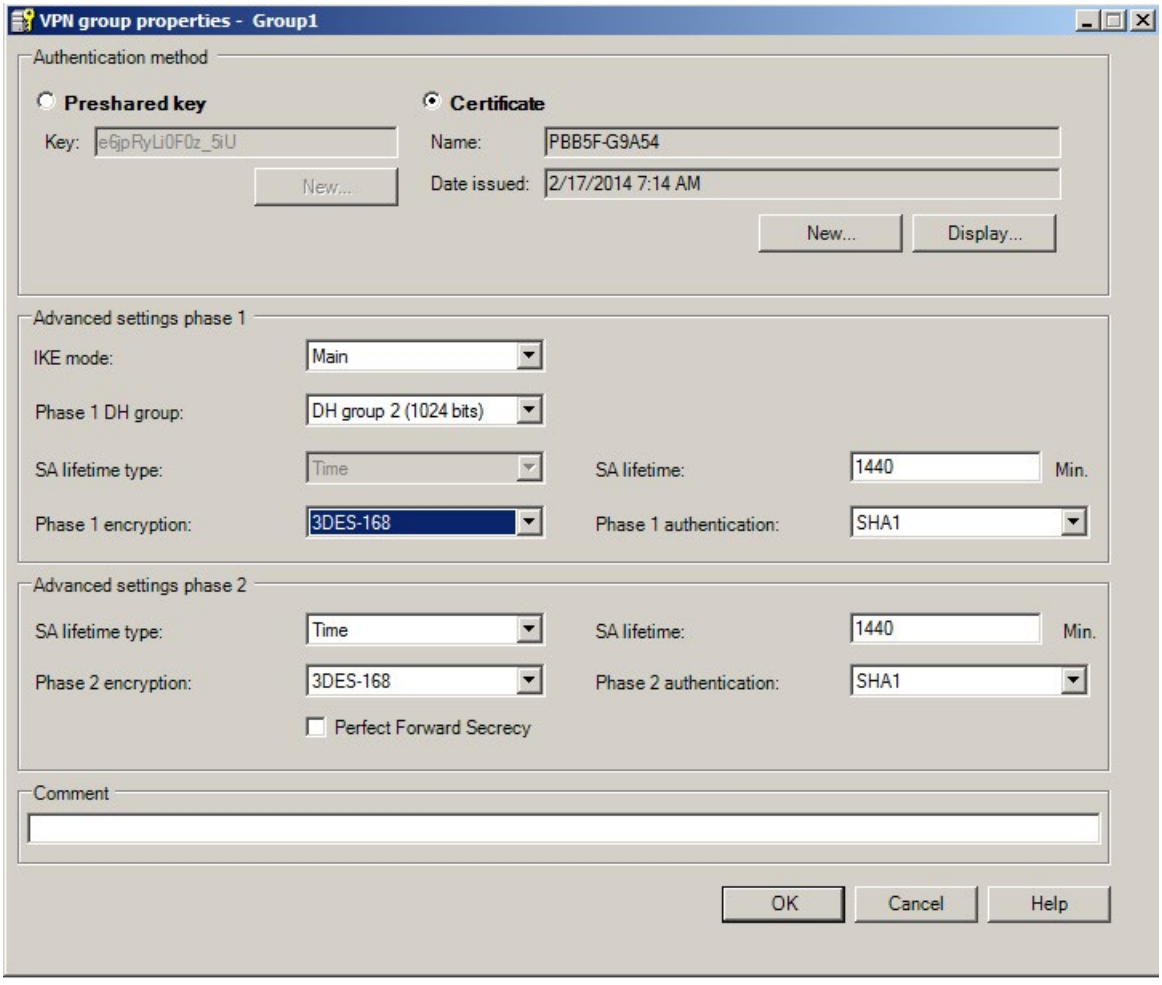
4.3.2.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M-800 and the CP are assigned to the same group.

Procedure

1. Select "VPN groups" in the navigation area and create a new group with the menu command "Insert" > "Group". The group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation area.
3. Select the SCALANCE M-800 and the CP in the content area. Drag the modules to "Group1". Both modules are now assigned to "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".
5. Open the group properties of Group1 by selecting the "Properties ..." shortcut menu

6. For this configuration example, configure the group properties with the following settings:



If you use different parameter settings, it is possible that the two tunnel partners will not be able to set up a VPN connection between them.

7. Select the menu command "Project" > "Save". Save the security project under the required name.

Result

The configuration of the tunnel connection is complete. The settings are saved in the configuration file.

4.3.2.3 Downloading the configuration to the CP and saving the M-800 configuration

Downloading the configuration to the CP

1. Close the Security Configuration Tool.
2. In HW Config, select the "Station" > "Save and Compile" menu.
3. Download the new configuration to the security module using the "PLC" > "Download to Module …" menu.
   - For CP 1628: If the download was completed free of errors, the security module restarts automatically and the new configuration is activated.
   - For CP 343-1 Advanced or CP 434-1 Advanced: Restart the S7 CPU following the download, to activate the new configuration.

Saving the SCALANCE M-800 configuration

1. In the content area, select the "M-800" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M-800.txt" in your project folder and assign a password for the private key of the certificate, e.g. Di1S+Xo?.

Result

The following files will be saved in the project directory:

- Configuration file: projectname.M-800.txt
- PKCS12 file: projectname.string.M-800.p12
- Remote certificate: Projectname.group1.CP.cer

The configuration file contains the exported configuration information for the SCALANCE M-800 including information on the additionally generated certificates. Follow the instructions in the configuration file.

4.3.3 Configuring SCALANCE M-800

4.3.3.1 Loading a certificate

Requirement

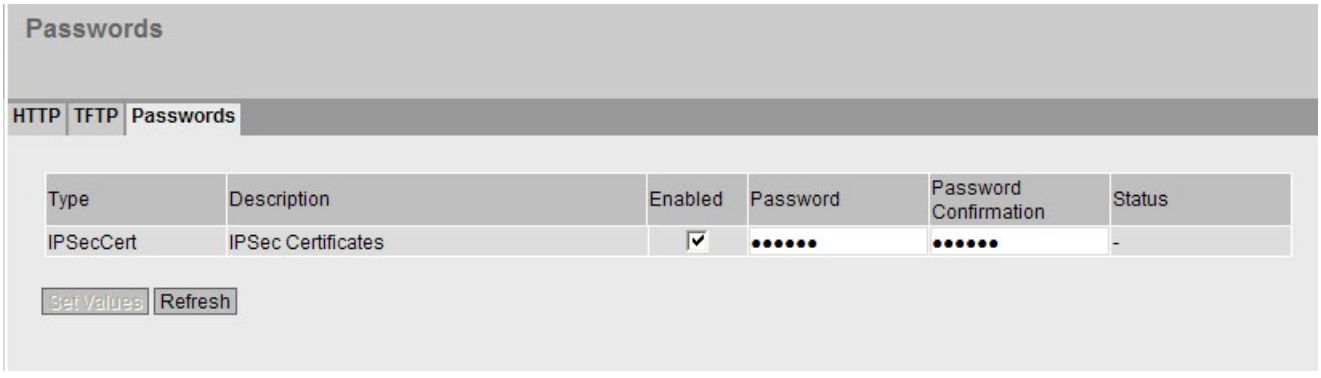
- The correct time is set on the SCALANCE M, refer to the section Setting the time (Page 23).
- Certificates are available.

  You saved the required certificates on the PC in the last section and assigned a password for the private key.

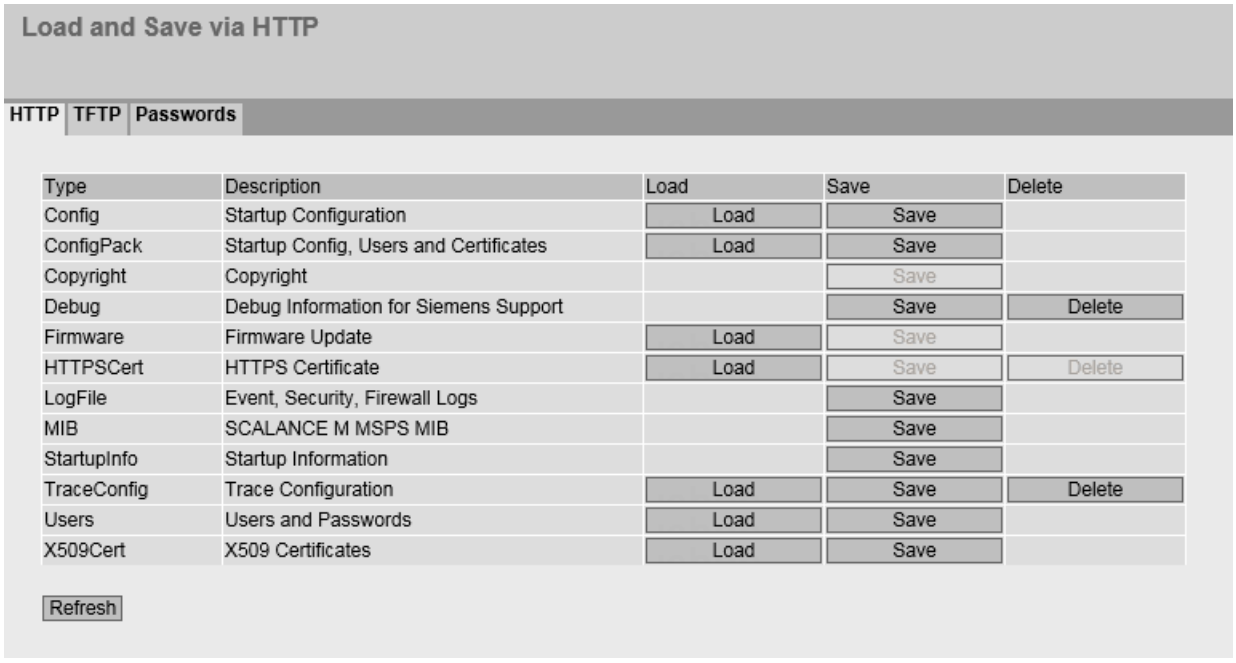
  Transfer the certificates for the SCALANCE M to the Admin PC.

Procedure

1. Click on "System" > "Load & Save" in the navigation area and on the "Password" tab in the content area.
2. For "Password" and "Password Confirmation", enter the password Di1S+Xo?, that you specified for the PKCS12 file.
3. Select "Enabled" and click "Set Values".



4. Click on the "HTTP" tab in the content area.



5. Click on the "Load" button beside "IPSecCert" or "X509cert". The dialog for loading a file is opened.

   Navigate to the remote certificate.

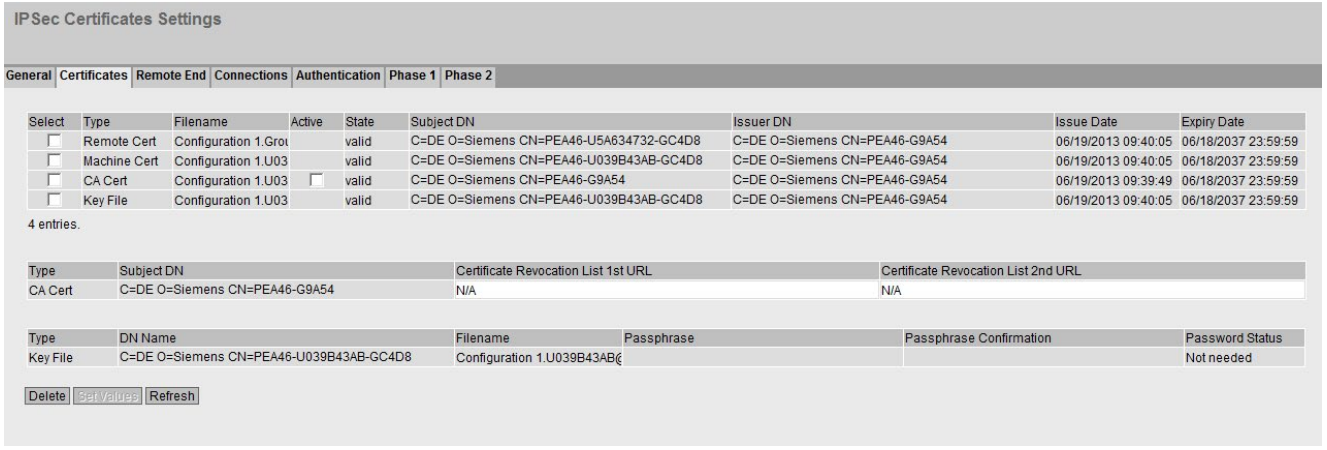
6. Click the "Open" button in the dialog.

   The file is now loaded on the device. After loading successfully, confirm the next dialog with "OK".

7. Repeat steps 5 and 6 for the PKCS12 file.

Result

The certificates are loaded. With "Security" > "IPSec VPN" > "Certificates", you can display the certificates. The loaded certificates must have the status "valid".



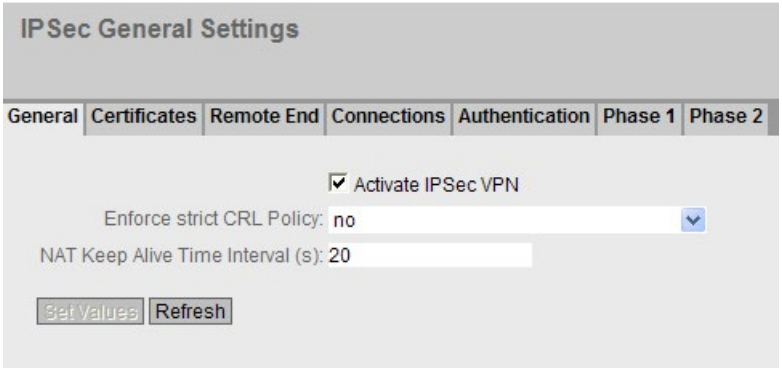
As of firmware version 4.0 certificates are displayed in "Security" > "Certificates".

Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Usec
☐	Remote Cert	startssl_spacewaffles_Cert.pem	expired	N/A	N/A	00/00/0 00:00:00	00/00/0 00:00:00	-
☐	Machine Cert	honkCert.pem	expired	N/A	N/A	00/00/0 00:00:00	00/00/0 00:00:00	-
☐	CA Cert	SiemensTestCAcert.pem	expired	N/A	N/A	00/00/0 00:00:00	00/00/0 00:00:00	-
☐	Key File	honkKeyUnc.pem	expired	N/A	N/A	00/00/0 00:00:00	00/00/0 00:00:00	-
☐	CA Cert	CA_000008_SINEMA_RC.crt	valid	CN=CA 000008 SINEMA RC	CN=CA 000008 SINEMA RC	10/17/2014 07:42:32	10/14/2024 07:42:32	-
☐	Machine Cert	S615_Ursel_Cert.pem	valid	CN=S615@1.8	CN=CA 000008 SINEMA RC	10/17/2014 09:10:34	10/17/2015 09:10:34	-
☐	CA Cert	S615_Ursel_CACert.pem	valid	CN=CA 000001 SINEMA RC	CN=CA 000001 SINEMA RC	09/16/2014 05:30:42	09/13/2024 05:30:42	-
☐	Key File	S615_Ursel_Key.pem	valid	CN=S615@1.8	CN=CA 000008 SINEMA RC	10/17/2014 09:10:34	10/17/2015 09:10:34	-
☐	Machine Cert	M800-2_Cert.pem	expired	CN=M800-2@D.1	CN=CA 000001 SINEMA RC	11/10/2014 14:47:30	11/10/2015 14:47:30	-
☐	CA Cert	M800-2_CACert.pem	expired	CN=CA 000001 SINEMA RC	CN=CA 000001 SINEMA RC	11/04/2014 12:27:09	11/01/2024 12:27:09	-
☐	Key File	M800-2_Key.pem	valid	CN=M800-2@D.1	CN=CA 000001 SINEMA RC	11/10/2014 14:47:30	11/10/2015 14:47:30	-
☐	Machine Cert	M800-1_Cert.pem	expired	CN=M-800@C.1	CN=CA 000001 SINEMA RC	11/10/2014 14:20:29	11/10/2015 14:20:29	-
☐	Key File	M800-1_Key.pem	valid	CN=M-800@C.1	CN=CA 000001 SINEMA RC	11/10/2014 14:20:29	11/10/2015 14:20:29	-

4.3.3.2 Activating VPN

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select Activate IPSec VPN".



3. Click "Set Values"

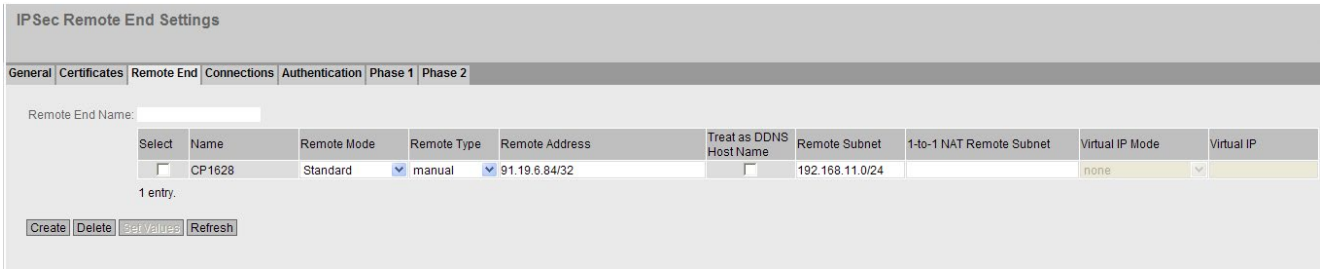
4.3.3.3 Configuring the VPN remote end

Procedure

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Remote End" tab in the content area.
2. Enter the name of the VPN partner (tunnel endpoint) in "Remote End Name", e.g. CP1628.
3. Click "Create". A new row is created in the table.
4. For the configuration example, configure the VPN remote end with the following settings:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.184.0/24

5. Click "Set Values".



4.3.3.4 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

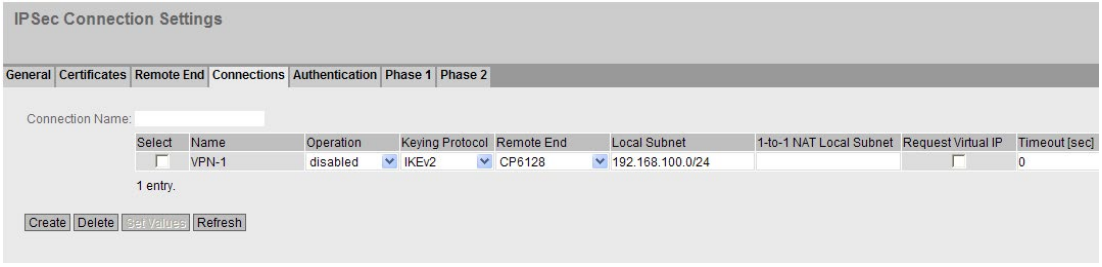
Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Click "Create". A new row is created in the table.

4. For the configuration example, configure the VPN connection with the following settings:

Operation	disabled
Keying Protocol	IKEv1
Remote End	CP1628 Name of the VPN remote station
Local Subnet	192.168.100.0/24 The local internal subnet 1 in CIDR notation.

5. Click "Set Values".



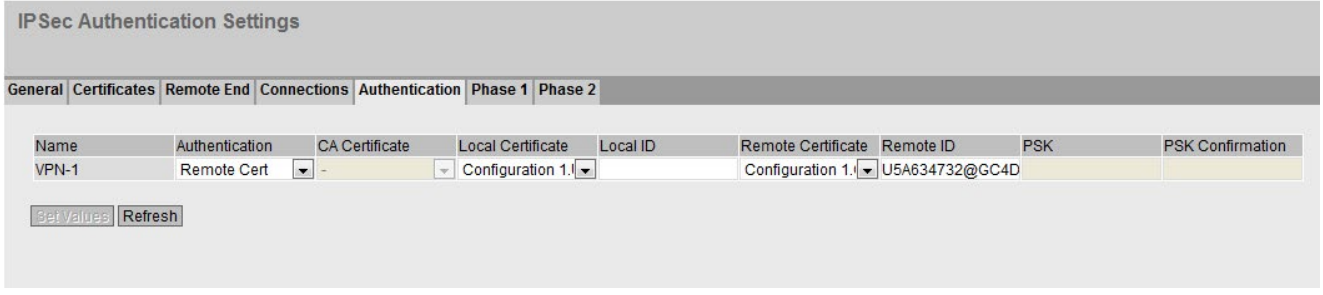
4.3.3.5 Configuring VPN authentication

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Authentication" tab in the content area.
2. For the configuration example, configure the VPN authentication with the following settings:

Authentication	Remote Cert
Local Certificate	projectname.string.M-800.p12
Remote Certificate	Projectname.group1.CP.cer
Remote ID	Remote ID from the configuration file

3. Click "Set Values".



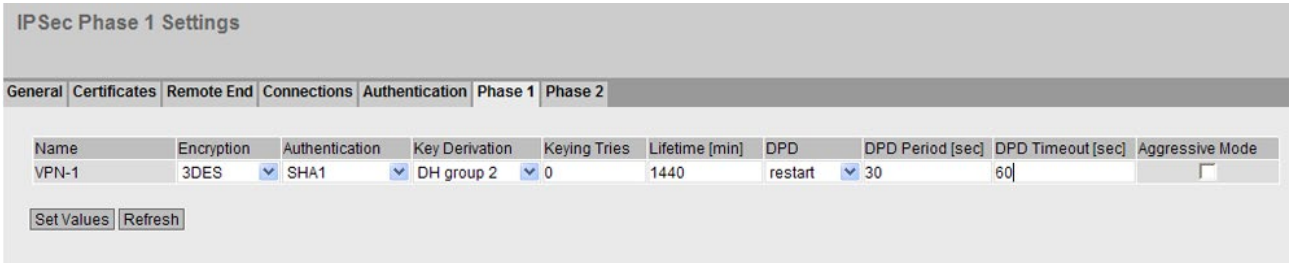
4.3.3.6 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPSecVPN" in the navigation area and on the "Phase 1" tab in the content area.
2. For "DPD", select "restart".
3. Configure phase 1 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

4. Click "Set Values".

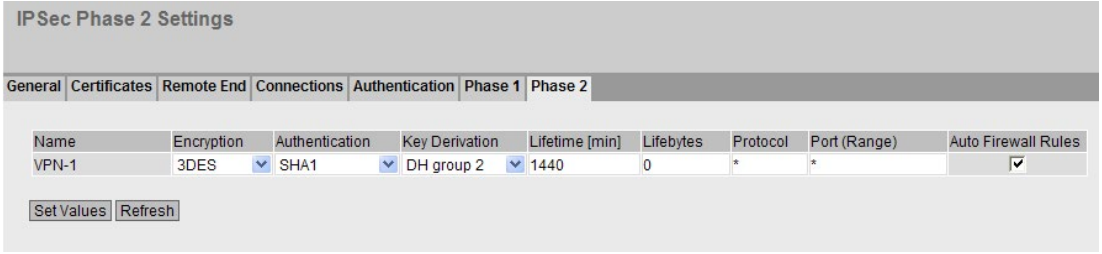


Configuring phase 2

1. Click the "Phase 2" tab.
2. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

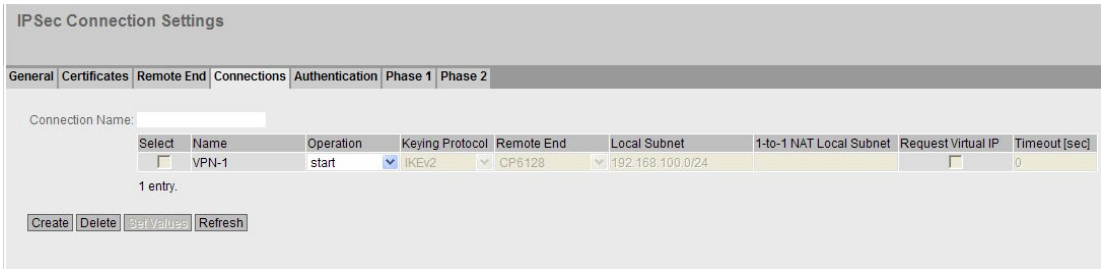
3. Click "Set Values".



4.3.3.7 Establishing the VPN connection

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "Connection" tab in the content area.

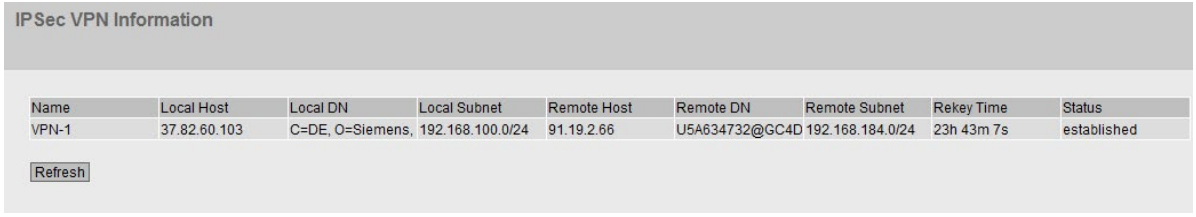


2. As "Operation", select "start" and click "Set Values".

Result

The SCALANCE M-800 establishes the VPN tunnel to the CP 1628. If the VPN tunnel is established, the 🔒 LED is lit green on the device.

You will find more detailed information in "Information" > "IPSec VPN".



VPN tunnel between SCALANCE M87x and SINEMA RC Server

5

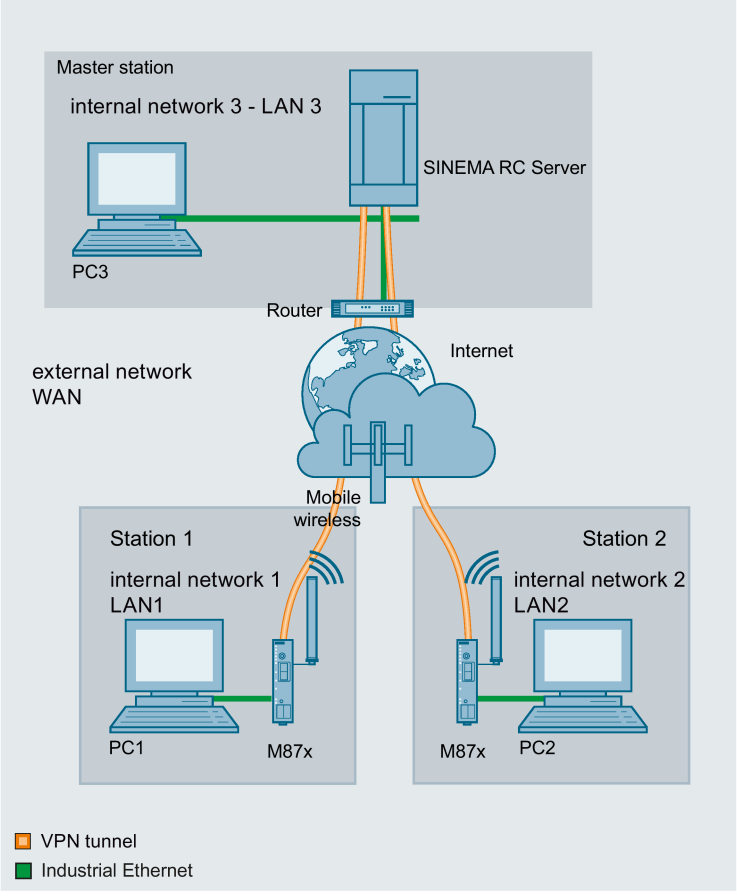
5.1 Procedure in principle

In this sample configuration, two distributed stations are connected using the SCALANCE M87x. The devices communicate via the SINEMA RC Server located in the master station. The SINEMA RC is addressed using a WAN IP address obtained from a provider. As an alternative, you can also address the SINEMA RC Server using a defined name (FQDN).

A KEY-PLUG SINEMA Remote Connect is required for each SCALANCE M87x device. The KEY-PLUG enables the connection from SCALANCE M87x to SINEMA RC.

To do this, the devices need to logon to the SINEMA RC Server. The VPN tunnel between the device and the SINEMA RC Server is established only after successful authentication. Depending on the configured communication relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

Structure



Master station - connection to SINEMA RC Server

- In the test setup in the internal network, a network node is implemented by a PC connected to the LAN interface of the SINEMA RC Server.
  - PC: represents a participant in internal network 3
  - SINEMA RC Server
- Connection to the external network via a router

  Access to the external network is via a router connected to the WAN interface of the SINEMA RC Server.

Station 1 / 2 - connection to SCALANCE M87x

- In the test setup in the internal network, a network node is implemented by a PC connected to the Ethernet interface P1 of the M-800.
  - PC: represents a participant in internal network 1/2
  - M-87x: SCALANCE M module for protection of the internal network 1/2
- Connection to the external, public network
  - Wireless via the antenna of the M87x on the mobile wireless network (as of firmware 4.0)

Required devices/components

Use the following components for setup:

- 2 x M874 (additional option: a suitably installed standard rail with fittings)
- 2 x KEY-PLUG SINEMA RC
- 2 x 24 V power supply with cable connector and terminal block plug
- 2 x PC each connected to a SCALANCE M874.
- 2 x suitable antennas
- 2 x SIM card of your mobile wireless provider. Suitable services are enabled, e.g. Internet.
- 1 x PC on which the SINEMA RC Server is installed.
- 1 x PC that is connected to the SINEMA RC Server.
- 1 x router
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Note

You can also use a SCALANCE M876. The configuration described below relates specifically to the components mentioned in the section "Required devices/components".

Settings used

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

	Name	Interface	IP address
Station -1 LAN1	M874-1	LAN interface P1 (vlan1)	192.168.100.1 255.255.255.0
		WAN interface (ppp0)	Dynamic IP address from provider
	PC1	LAN interface	192.168.100.20 255.255.255.0
Station-2 LAN2	M874-2	LAN interface P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN interface (ppp0)	Dynamic IP address from provider
	PC2	Ethernet (LAN 2)	192.168.10.20 255.255.255.0
Master station LAN3	SINEMA RC Server	WAN interface	192.168.20.250 255.255.255.0 The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example. 90.90.90.90 The default gateway is the LAN IP address of the router 192.168.20.1 As an alternative, the SINEMA RC Server can also be addressed using a defined host name (FQDN).
	PC3	Ethernet (LAN3)	192.168.20.20 255.255.255.0
	Router 3	LAN interface	192.168.20.1 255.255.255.0
		WAN interface	Static IP address from the provider e.g. 90.90.90.90

Note

The IP settings used in the configuration example were freely chosen.

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

Requirement

SINEMA RC Server

- The SINEMA RC Server is connected to the WAN. You will find the configuration steps in the Getting Started "SINEMA Remote Connect".

Note

Port forwarding at the router

By using a router as a gateway you must enable the following ports on the router and forward the data packets to the SINEMA RC Server:

- TCP 443
- TCP 5443
- UDP 1194

Router with VPN capability

If your router itself has VPN capability, make sure that the ports do not overlap or this function is disabled.

You will find further information on this in the documentation of the router.

SCALANCE M874

- The M874 is connected to the WAN, refer to "Connecting SCALANCE M874 to the WAN (Page 11)".

  The steps in configuration are the same for all devices, the only difference being the settings, see table "Settings used (Page 181)".
- The M874 can be reached via PC1 or PC2 and you are logged in to the WBM as "admin".
- A valid KEY-PLUG SINEMA Remote Connect is inserted in the SCALANCE M.

Steps in configuration

Configuring access to the SINEMA RC Server

For the PC to be able to access the WBM of the SINEMA RC Server via the M874, the following steps are necessary on the M874:

1. Activate IP masquerading (Page 186)
2. Allow access (Page 186)

Configure a remote connection on the SINEMA RC Server

1. Creating participant groups (Page 188)
2. Create devices (Page 190)
3. Configure communication relations (Page 192)

Configure a remote connection on the M874

- Secure VPN connection with fingerprint (Page 194)
- Secure VPN connection with CA certificate
  - Loading a certificate (Page 197)
  - Configuring a VPN connection to the SINEMA RC Server (Page 199)

5.2 Configuring access to the SINEMA RC Server

5.2.1 Activating IP masquerading

IP masquerading is used so that the internal IP addresses are not forwarded to external. In addition to this, no further routing settings are necessary on the router.

Procedure

1. Click on "Layer 3" > "NAT" in the navigation area and on the "Masquerading" tab in the content area.
2. Activate "Enable Masquerading" on the WAN interface.
   - M874, M876-3: ppp0
   - M876-4: usb0
3. Click "Set Values"

Result

Masquerading is enabled on the WAN interface. When a packet is sent via this interface, the source address is rewritten to the IP address assigned to the WAN interface.

5.2.2 Allow access

So that the PC can access the SINEMA RC Server, on the device access from vlan1 to the WAN interface is enabled.

Procedure

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.

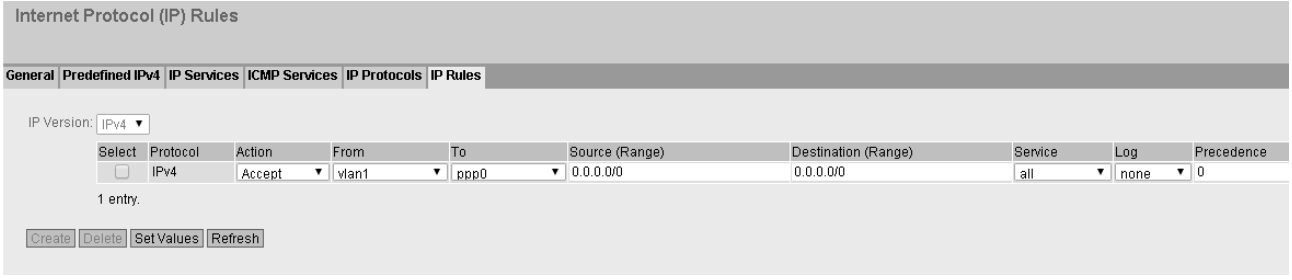
3. Configure the firewall rule with the following settings:

Action	Accept
From	vlan1 (internal)
To	external M874, M876-3: ppp0 M876-4: usb0
Source (Range)	0.0.0.0 (all IP addresses)
Destination (Range)	0.0.0.0 (all IP addresses)
Service	all As default, the service is always available

4. Click "Set Values".

Result

Due to this firewall rule, all services between vlan1 and ppp0 or usb0 are possible without restrictions, e.g. HTTPS



5.3 Configure a remote connection on the SINEMA RC Server

5.3.1 Creating node groups

Users and devices can be put together in participant groups. You can also specify whether the communication between the participants of an individual group is permitted or forbidden.

For this sample configuration, the following groups are created.

- Station -1
- Station-2
- Service

Requirement

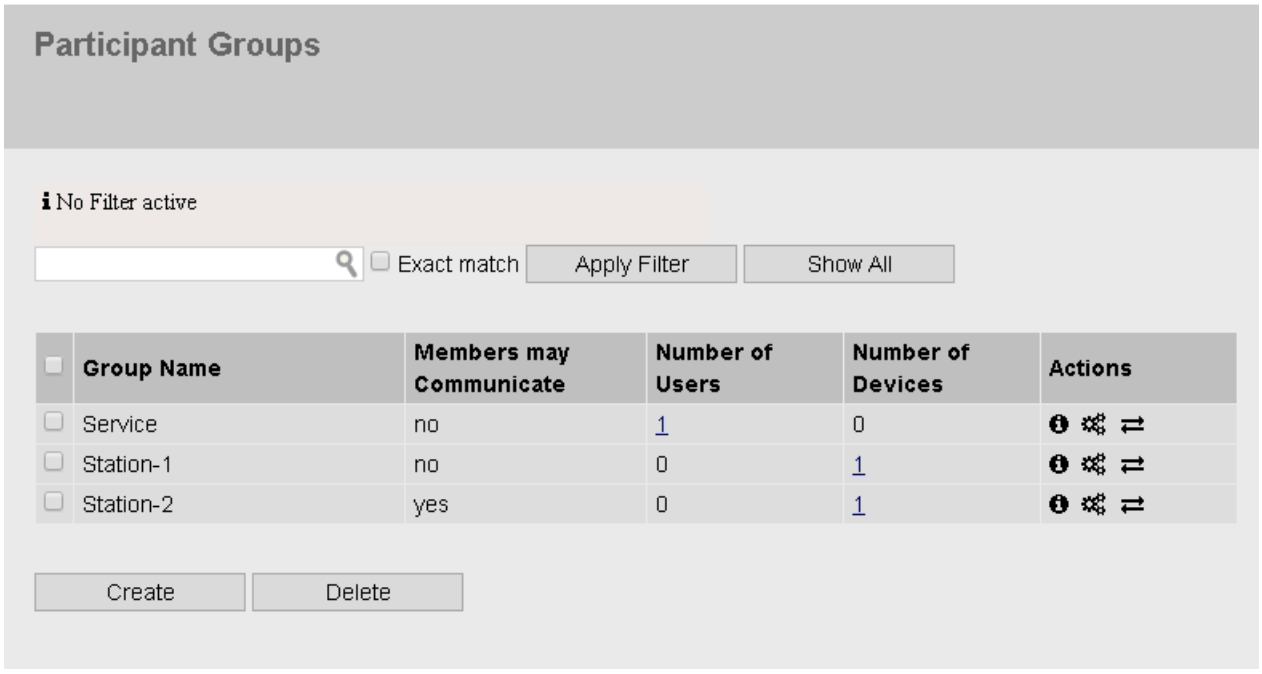
- The SINEMA RC Server is connected to the WAN.

Procedure

1. In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server "https://<WAN IP address>", see table "Settings used (Page 181)".
2. Log in as the "admin" user and with the corresponding password.
3. In the navigation area, click "Remote connections" > "Participant groups". The participant groups that have already been created are listed in the content area.
4. Click "Create". The page "New participant group" is opened.
5. Enter "Station 1" for group name and click "Exit".
6. Repeat steps 1 - 3 for the groups "Station-2" and "Service"

Result

The participant groups have been created.



5.3.2 Create devices

Procedure

1. In the navigation area, click "Remote connections" > "Devices". The devices that have already been created are listed in the content area.
2. Click "Create" button to create a new device.
3. Enter the device name for the device e.g. "M874-1" for station 1 and "M874-2" for station 2.
4. Click "Continue".
5. Enable the option "Connected local subnets".
6. Configure the devices with the following settings:

Local LAN IP address	IP address for vlan1 according to the table "Settings used (Page 181)".
Network mask	255.255.255.0

7. Click "Continue". The "Group memberships" tab is displayed.
8. Enable the appropriate group.

   On the device "M874-1" the group "Station-1"

   On the device "M874-2" the group "Station-2"
9. Click "Continue". The "Password" tab is displayed.
10. Specify the password for the access e.g. An:t_010 for M874-1 and An:t_020 for M874-2.

    The password must be made up of uppercase and lowercase letters, numbers and special characters.
11. Click "Exit".

Result

The devices are listed with the devices that have already been created.

- Device password
- Device ID
- Fingerprint

You will find the device ID and the fingerprint in the device information. Click on the symbol to open the device information.


Devices / M874-1
Device
Network settings
Group memberships
Change password
Device overview
Device information:
Device ID: 3
Fingerprint: D5:5A:DD:63:A9:36:3E:72:BB:29:99:1A:7A:9D:2D:D4:66:F8:8B:1A
Device name: M874-1
Local LAN IP address:
Local subnet
Network of the gateway
192.168.100.1/24
Yes
Virtual local LAN IP address:
Virtual local LAN
Local subnet
Network of the gateway
Virtual local LAN device specific:
Virtual local LAN
Local Single Host
Network of the gateway
Type:
Vendor:
Location: Station 1
Type of connection: Permanent
Comment:
Groups: Station-1

5.3.3 Configure communications relations

So that participant groups can communicate with each other, communication relations are necessary. A communication relation can be created for every direction.

For this sample configuration, the following communication relations are created:

from group	to the destination group
Service	Station -1
	Station-2
Station -1	Station-2

In this configuration example, communication is only from the group "Station 1" to the group "Station 2". In the opposite direction, no communication is possible. For the communication from the group "Station 2" to the group "Station 1" another communication relation is necessary.

The group "Service" can also communicate with the groups "Station 1" and "Station 2" but not the other way round.

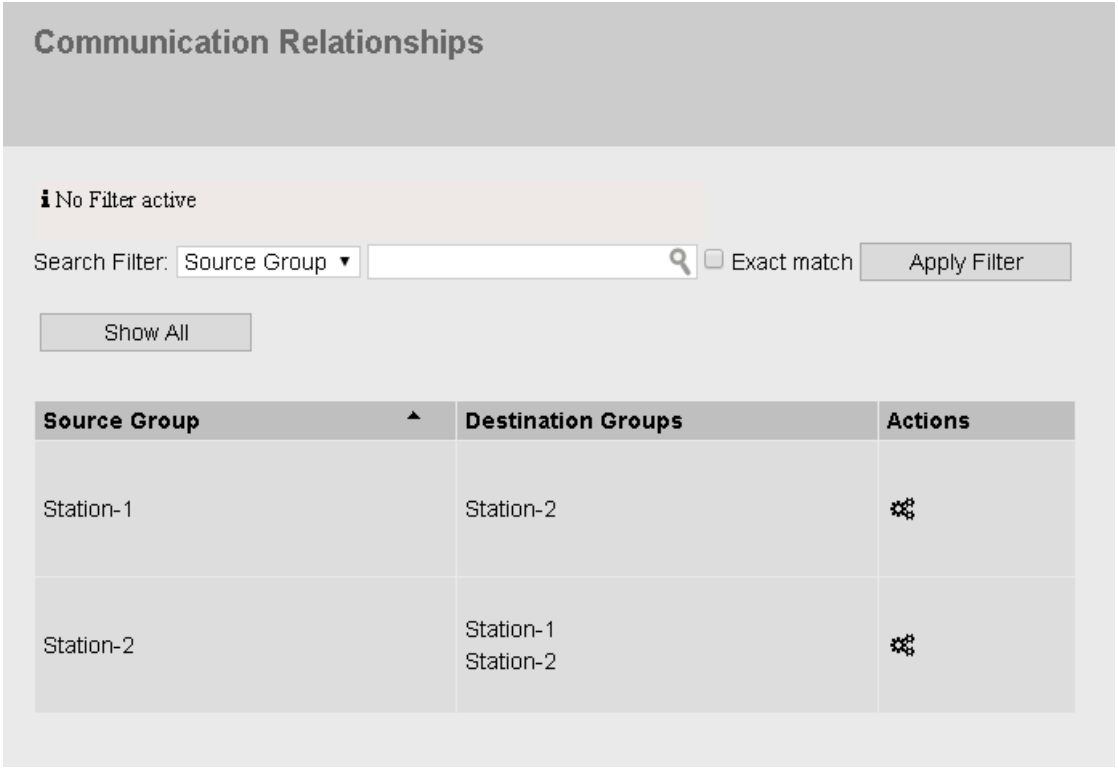
Procedure

1. In the navigation area, click "Remote connections" > "Participant groups". The participant groups that have already been created are listed in the content area.
2. For "Station 1", click the symbol ⇄ in the "Actions" column. The page "Destination group" is opened.
3. Enable "Station 2" and click on "Save".
4. Click "Exit dialog".
5. For "Service", click the symbol ⇄ in the "Actions" column. The page "Destination group" is opened.
6. Enable "Station 1" and "Station 2". Click "Save".
7. Click "Exit dialog".

Result

The communication relations have been created.

Click "Remote connections" > "Communication relations" in the navigation area. The created relations are listed in the content area.



5.4 Configuring a remote connection on the M87x

5.4.1 Secure VPN connection with fingerprint

Requirement

- On PC1/2 there are two Web browser windows open.
- Web browser 1:

  You are logged in as the "admin" user to the WBM of the M874.
- Web browser 2:

  You are logged on to the WBM of the SINEMA RC Server as user "service" or "admin".
- A valid KEY-PLUG is inserted in the M87x.

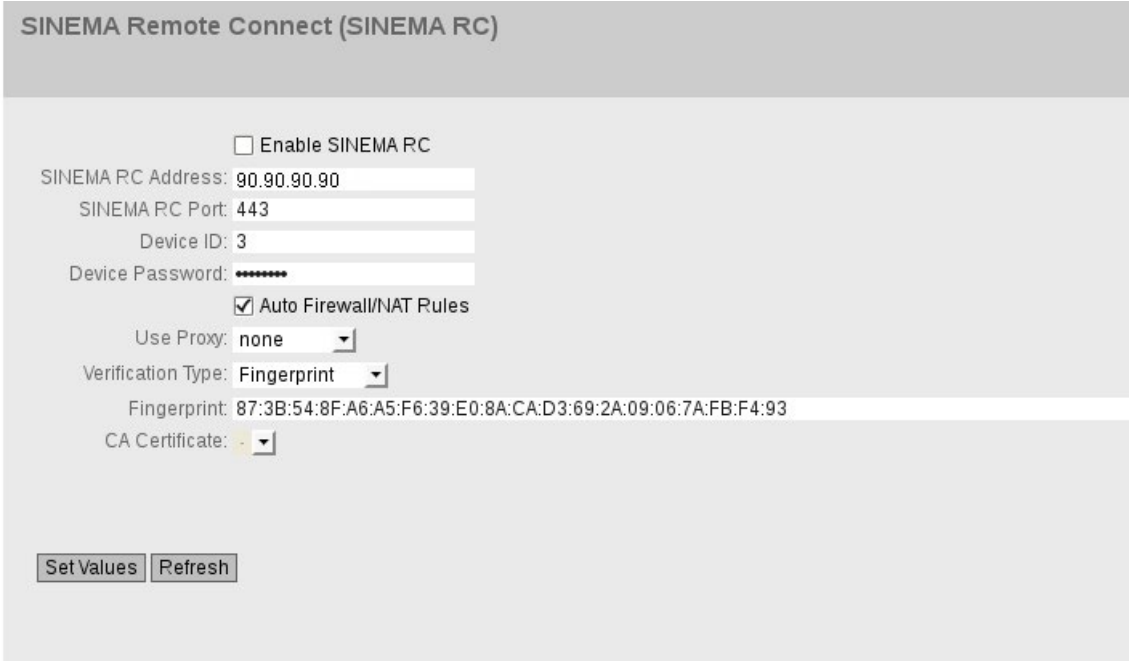
Procedure

1. Change to Web browser 1.
   - In the address box of the Web browser, enter the LAN IP address of the M874, see table "Settings used (Page 181)".
   - Log in as the "admin" user and with the corresponding password.
   - Click "System" > "SINEMA RC" in the navigation area.
   - For "Sinema RC Address", enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 181)".
2. Change to Web browser 2.
   - In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 181)".
   - Log in as the "admin" user and the corresponding password.
   - In the navigation area, click "Remote connections" > "Devices".
   - Click on the symbol in "Actions" to open the device information.
   - Holding down the left mouse button, select the entry for device ID.
   - Right-click on the selection and in the shortcut menu, select the copy command.

3. Change to Web browser 1.
   - Right click in the input box of "Device ID".
   - In the shortcut menu, select the menu command for inserting.
   - For "Device Password" enter the password that you configured for access, An:t_010 for M874-1 and An:t_020 for M874-2.
   - Enable "Auto Firewall / NAT Rules".

     When enabled, the suitable NAT and firewall rules are created automatically.

     For "Verification Type" select "Fingerprint".
4. Change to Web browser 2.
   - Holding down the left mouse button, select the entry for fingerprint.
   - Right-click on the selection and in the shortcut menu, select the copy command.
5. Change to Web browser 1.
   - Right click in the input box of "Fingerprint".
   - In the shortcut menu, select the menu command for inserting.
   - Select "Enable SINEMA RC" and click on "Set Values".



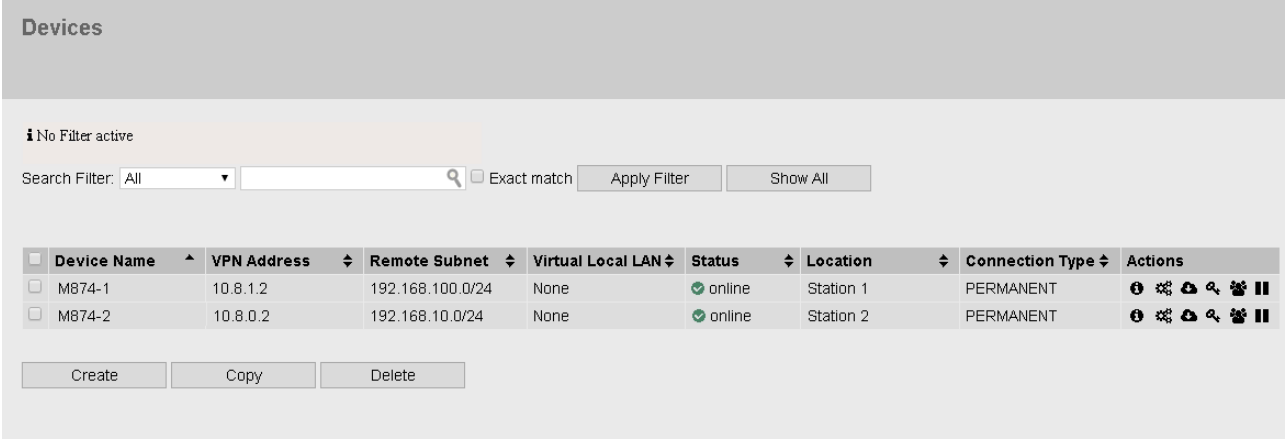
Result

The device establishes a VPN tunnel to the SINEMA RC Server.

You can check in the WBM to see whether the connection was successful.

Web browser 1: In the navigation area, click "Information" > "SINEMA RC".

Web browser 2: Click "Remote connections" > "Devices" in the navigation area.



5.4.2 Secure VPN connection with CA certificate

5.4.2.1 Loading a certificate

Requirement

- The correct time is set on the M874 and the SINEMA RC Server.
- On PC1/2 there are two Web browser windows open.
- Web browser 1:

  You are logged in as the "admin" user to the WBM of the M874.
- Web browser 2:

  You are logged on to the WBM of the SINEMA RC Server as the user "admin".

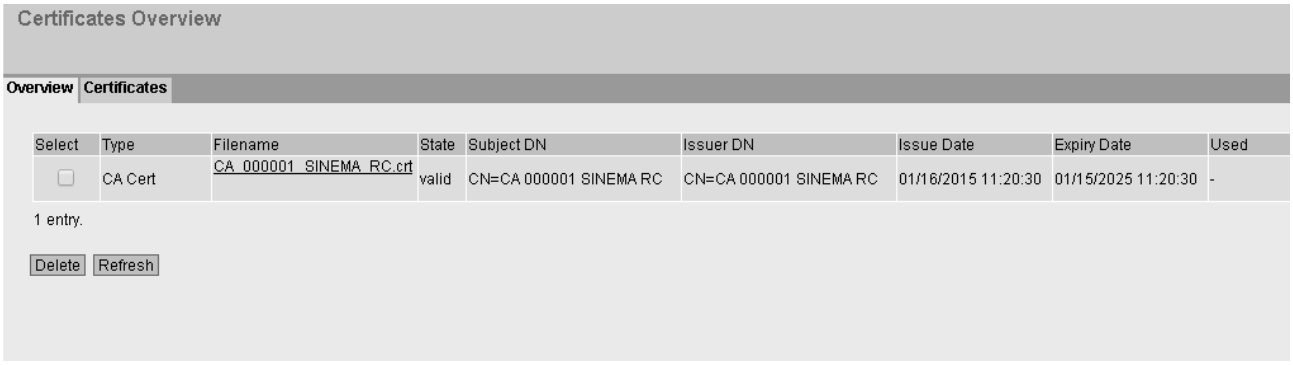
Procedure

1. Change to Web browser 2.
   - In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 181)".
   - Log in as the "admin" user and the corresponding password.
   - Click "Security" > "Certificates" in the navigation area.
   - Click on the symbol in "Actions" to export the certificate.
2. Change to Web browser 1.
   - In the address box of the Web browser, enter the LAN IP address of the M874, see table "Settings used (Page 181)".
   - Log in as the "admin" user and with the corresponding password.
   - Click on "System" > "Load & Save" in the navigation area and on the "HTTP" tab in the content area.
   - Click the "Load" button next to "X509Cert". The dialog for loading a file is opened.
   - Navigate to the exported server certificate. Click the "Open" button in the dialog.

     The file is now loaded on the device. After loading successfully, confirm the next dialog with "OK".

Result

The certificates are loaded. With "Security" > "Certificates", you can display the certificates. The loaded certificates must have the status "valid".



5.4.2.2 Configuring a VPN connection to the SINEMA RC Server

Requirement

- A valid KEY-PLUG is inserted in the M87x.

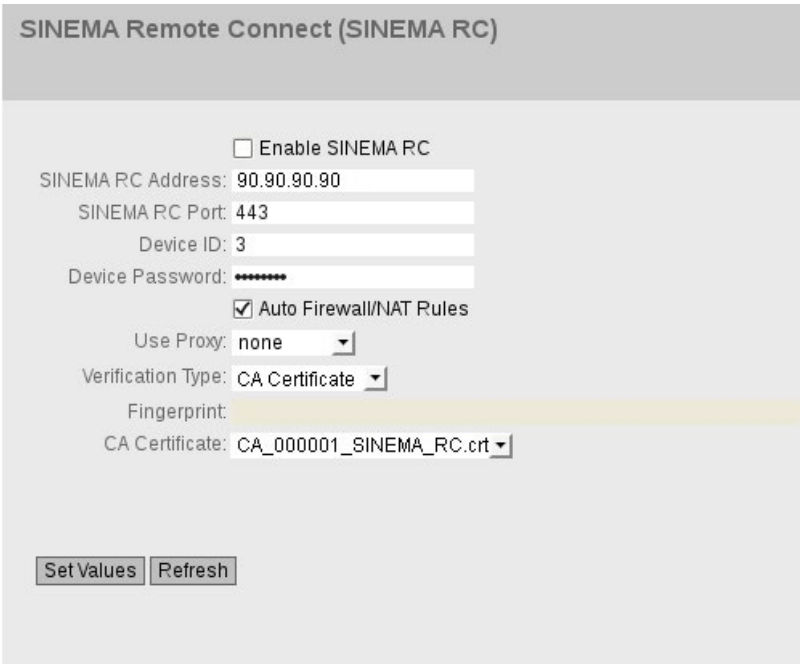
Procedure

1. Change to Web browser 1.
   - Click "System" > "SINEMA RC" in the navigation area.
   - For "Sinema RC Address", enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 181)".
2. Change to Web browser 2.
   - In the navigation area, click "Remote connections" > "Devices".
   - Click on the symbol in "Actions" to open the device information.
   - Holding down the left mouse button, select the entry for device ID.
   - Right-click on the selection and in the shortcut menu, select the copy command.
3. Change to Web browser 1.
   - Right click in the input box of "Device ID".
   - In the shortcut menu, select the menu command for inserting.
   - For "Device Password" enter the password that you configured for access, An:t_010 for M874-1 and An:t_020 for M874-2.
   - Enable "Auto Firewall / NAT Rules".

     When enabled, the suitable NAT and firewall rules are created automatically.

     In "Verification Type", select "CA Certificate".

– In "CA Certificate" select the server certificate. Only loaded certificates can be selected.



– Select "Enable SINEMA RC" and click on "Set Values".

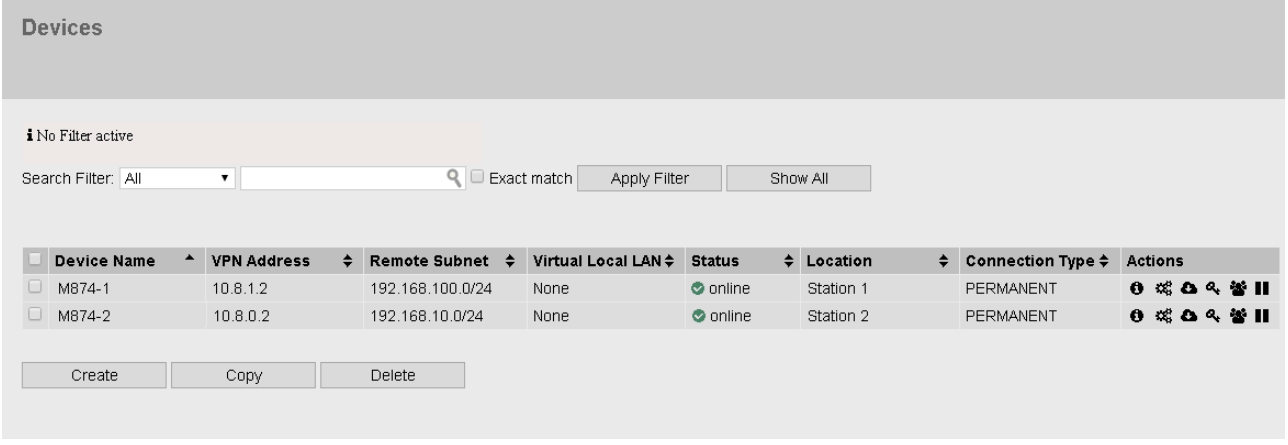
Result

The device establishes a VPN tunnel to the SINEMA RC Server.

You can check in the WBM to see whether the connection was successful.

Web browser 1: In the navigation area, click "Information" > "SINEMA RC".

Web browser 2: Click "Remote connections" > "Devices" in the navigation area.

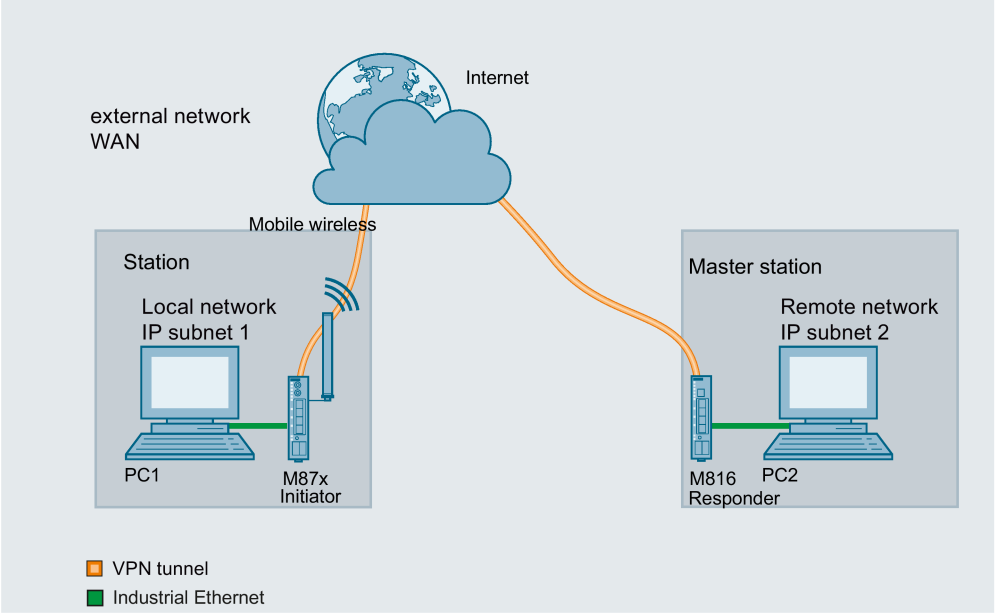


NETMAP with SCALANCE M-800

6

In these examples, two different IP subnets are connected together via a SCALANCE M-800. Between the two SCALANCE M devices a VPN tunnel is established. The VPN connection is initiated by the M876. Via the established tunnel, the addresses are translated with NETMAP. In this translation, the subnet part of the IP address is changed and the host part remains.

NETMAP can translate both the source IP address and the destination IP address.



Local area network - connection to SCALANCE M-800

- In the test setup, in the local network, a network node is implemented by a PC connected to an Ethernet interface of the SCALANCE M-800.
  - PC: represents a node in the local network
  - M-800: SCALANCE M module for protection of the internal network
- Connection to the external, public network:
  - Wireless via the antenna of the M87x to the mobile wireless network.

Remote network - connection to M-800

- In the test setup, in the remote network, the network node is implemented by a PC in each case connected to an Ethernet interface of the SCALANCE M-800.
  - PC: represents a node in the remote network
  - M-800: SCALANCE M module for protection of the external network
- Connection to the external, public network

  Wired via the RJ-45 jack of the M816 to ADSL.

Required devices/components

Use the following components to set up the network:

- Connection to the mobile wireless network
  - 1 x M876 (additional option: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - 1 x suitable antenna
  - 1 x SIM card of your mobile wireless provider. Suitable services are enabled, e.g. Internet.
- Connecting to ADSL
  - 1 x M816 (additional option: a suitably installed standard rail with fittings)
  - 1 x 24 V power supply with cable connector and terminal block plug
  - ADSL access is enabled
- 2 x PCs connected to the SCALANCE M-800.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

---

Note

You can also use other SCALANCE M-800 devices. The configuration described below relates explicitly to the components mentioned in the Section "Required devices/components".

Settings used

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

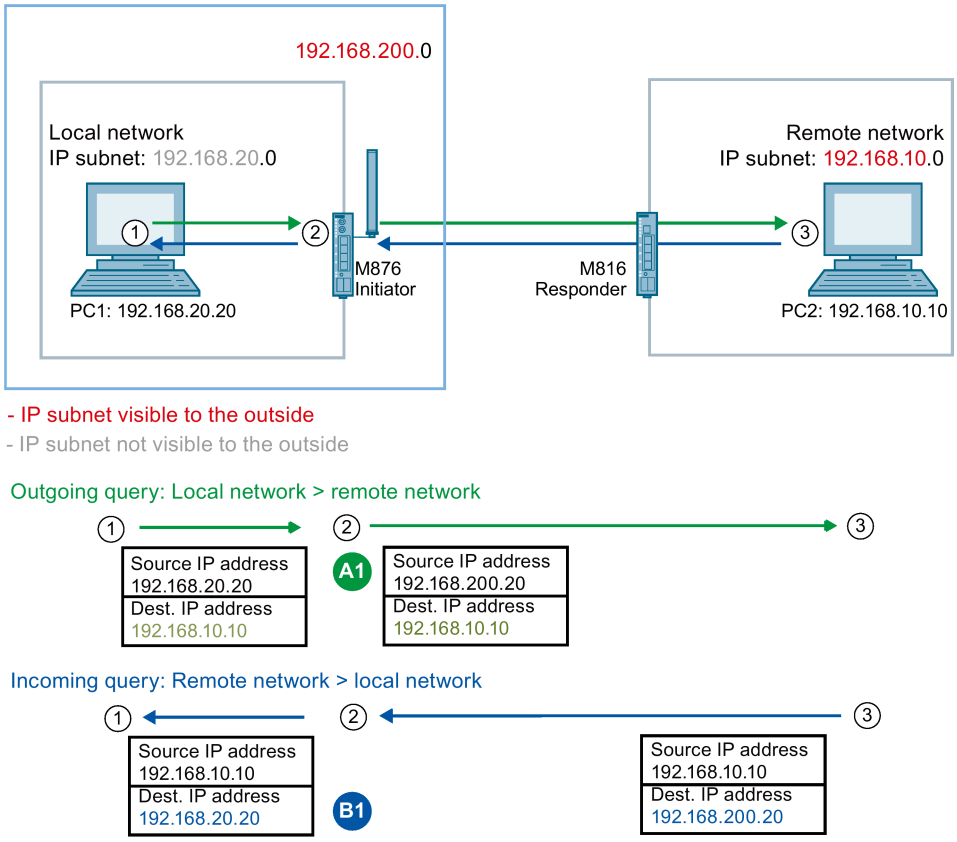
	Name	Interface	IP address
Station IP subnet 1	M876	LAN interface P1 (vlan1)	192.168.20.1 255.255.255.0
		WAN interface (ppp0)	Dynamic IP address from the provider The device is, however, reachable via a dynamic DNS service, e.g. example.no-ip.com
	PC1	LAN interface	192.168.20.20 255.255.255.0
Master station IP subnet 2	M816	LAN interface P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN interface (ppp0)	Fixed IP address (WAN IP address), e.g. 91.19.6.84
	PC2	Ethernet (LAN 2)	192.168.10.10 255.255.255.0

Examples

There are the following examples of NETMAP

1. NETMAP for the local network (Page 206)
2. NETMAP for the remote network (Page 211)
3. NETMAP for the local and remote network (Page 216)

6.1 NETMAP for the local network



With NETMAP of the local network, the source address ① e.g. 192.168.20.20 is translated. In this translation, the subnet part of the IP address is changed and the host part remains. In the example, the subnet part is 192.168.20.0. This subnet part is replaced by 192.168.200.0. The source IP address is translated by the M876 ② and forwarded to the destination ③.

With incoming queries ③, the destination IP address 192.168.200.0 is replaced by 192.168.20.0. The destination IP address is translated by the M876 ② and forwarded to the destination ①. Only the NETMAP rules for the direction of the query are necessary. The NETMAP rules for the replies are added implicitly. When PC1 sends a query to PC2, the reply is translated based on it. This, however, does not apply to queries from PC2 to PC1.

For this, the following NETMAP rules are created on the M876 (initiator):

A1 Local network > remote network:
The source IP subnet 192.168.20.0/24 is replaced by 192.168.200.0/24.

B1 Remote network > local network:
The destination IP subnet 192.168.200.0/24 is replaced by 192.168.20.0/24

The two devices also communicate via a VPN tunnel.

Requirement

- The SCALANCE M-800 is connected to the WAN , refer to "Connecting SCALANCE M-800 to the WAN (Page 81)".
- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

The following steps are necessary to create NETMAP rules:

1. Creating a VPN connection (Page 207)
2. Creating NETMAP rules (Page 209)

6.1.1 Creating a VPN connection

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select "Activate IPSec VPN" and click "Set Values".
3. Click on the "Remote End" tab in the content area and create the VPN partner with the following settings:

	On the M816	On the M876
Remote End Name	M876	M816
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Reachable via a dynamic DNS service, e.g. example.no-ip.com	Fixed IP address (WAN IP address) of the M816, e.g. 91.19.6.84
Remote Subnet	192.168.200.0/24	192.168.10.0/24

4. Click on the "Connections" tab in the content area and create the VPN connection with the following settings:

	On the M816	On the M876
Connection Name	M816_to_M876	M876_to_M816
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M876	M816
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Click on the "Authentication" tab in the content area and configure the VPN authentication with the following settings:

	On the M816	On the M876
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	e. g. 12345678	e. g. 12345678

6. Click on the "Phase 1" tab in the content area and configure the following settings:

	M816 / M876
DPD	enabled
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

7. Click on the "Phase 2" tab in the content area and configure the following settings:

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M816)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Result

The VPN connection on the devices is configured. To establish the VPN connection, click on the "Connection" tab in the content area.

For "Operation" select the following and click "Set Values"

	On the M816	On the M876
Operation	wait (Responder)	start (Initiator)

The M876 establishes the VPN tunnel to the M816. If the VPN tunnel is established, the LED is lit green on the devices.

6.1.2 Creating NETMAP rules

Requirement

- The VPN connection M876_to_M816 is configured, see Creating a VPN connection (Page 207).

Procedure

1. Click on "Layer 3" > "NAT" in the navigation area and on the "NETMAP" tab in the content area.
2. Specify the NETMAP rule A1 for the outgoing queries with the following settings:

Type	Source
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816
Source IP Subnet	192.168.20.0/24
Translated Source IP Subnet	192.168.200.0/24
Destination IP Subnet	192.168.10.0/24

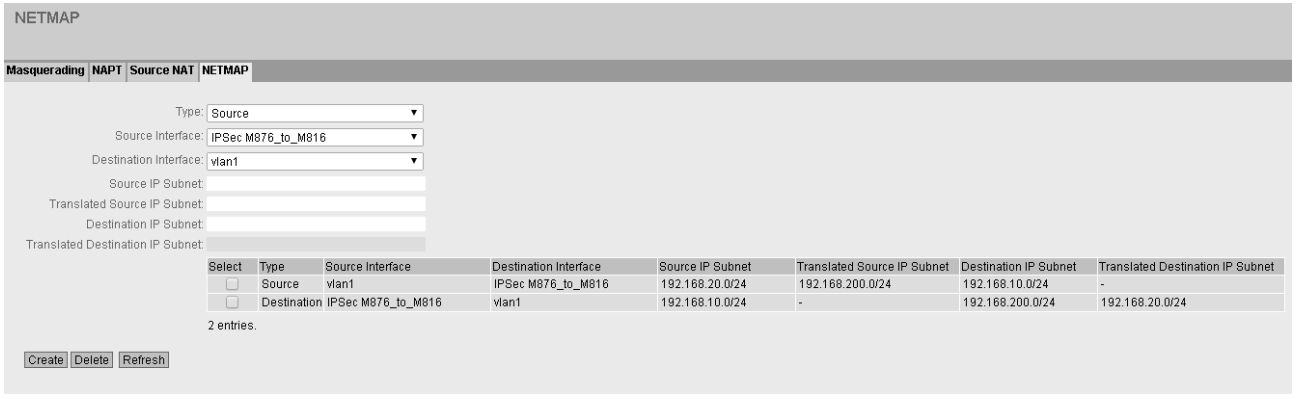
3. Click "Create". A new row is created in the table with the settings.
4. Specify the NETMAP rule B1 for the incoming queries with the following settings:

Type	Destination
Source Interface	IPSec M876_to_M816
Destination Interface	vlan1
Source IP Subnet	192.168.10.0/24
Destination IP Subnet	192.168.200.0/24
Translated Destination IP Subnet	192.168.20.0/24

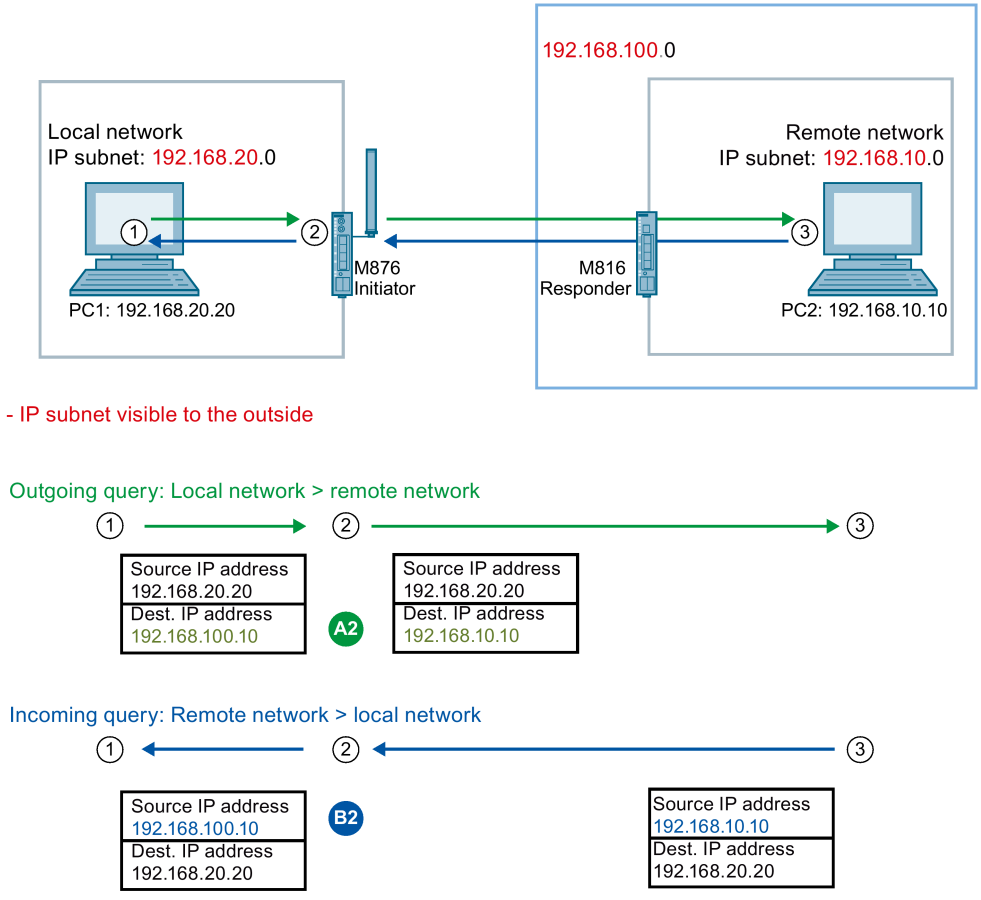
5. Click "Create". A new row is created in the table with the settings.
6. Click "Set Values".

Result

The rules for the outgoing and incoming queries have been created.



6.2 NETMAP for the remote network



With NETMAP of the remote network, the destination ① e.g. 192.168.100.10 is translated. In the example, the subnet part is 192.168.100.0 and this is replaced by 192.168.10.0. This means that the remote network can also be reached in addition to 192.168.10.0 also via 192.168.100.0. The destination IP address is translated by the M876 ② and forwarded to the destination ③.

With incoming queries ③, the source IP address 192.168.10.0 is replaced by 192.168.100.0. The source IP address is translated by the M876 ② and forwarded to the destination ①.

Only the NETMAP rules for the direction of the query are necessary. The NETMAP rules for the replies are added implicitly. When PC1 sends a query to PC2, the reply is translated based on it. This, however, does not apply to queries from PC2 to PC1.

For this, the following NETMAP rules are created on the M876 (initiator):

- A2 Local network > remote network:
  The destination IP subnet 192.168.100.0/24 is replaced by 192.168.10.0/24.
- B2 Remote network > local network:
  The source IP subnet 192.168.10.0/24 is replaced by 192.168.100.0/24

The two devices should also communicate with each other via a VPN tunnel.

Requirement

- The SCALANCE M-800 is connected to the WAN , refer to "Connecting SCALANCE M-800 to the WAN (Page 11)".
- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

The following steps are necessary

1. Creating a VPN connection (Page 212)
2. Creating NETMAP rules (Page 214)

6.2.1 Creating a VPN connection

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select "Activate IPSec VPN" and click "Set Values".
3. Click on the "Remote End" tab in the content area and create the VPN partner with the following settings:

	On the M816	On the M876
Remote End Name	M816	M876
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Reachable via a dynamic DNS service, e.g. example.no-ip.com	Fixed IP address (WAN IP address) of the M816, e.g. 91.19.6.84
Remote Subnet	192.168.20.0/24	192.168.10.0/24

4. Click on the "Connections" tab in the content area and create the VPN connection with the following settings:

	On the M816	On the M876
Connection Name	M816_to_M876_2	M876_to_M816_2
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M816	M876
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Click on the "Authentication" tab in the content area and configure the VPN authentication with the following settings:

	On the M816	On the M876
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	e. g. 12345678	e. g. 12345678

6. Click on the "Phase 1" tab in the content area and configure the following settings:

	M816 / M876
DPD	enabled
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

7. Click on the "Phase 2" tab in the content area and configure the following settings:

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Result

The VPN connection on the devices is configured. To establish the VPN connection, click on the "Connection" tab in the content area.

For "Operation" select the following and click "Set Values"

	On the M816	On the M876
Operation	wait (Responder)	start (Initiator)

The M876 establishes the VPN tunnel to the M816. If the VPN tunnel is established, the 🔒 LED is lit green on the devices.

6.2.2 Creating NETMAP rules

Requirement

- The VPN connection M876_to_M816_2 is configured, see Creating a VPN connection (Page 212).

Procedure

1. Click on "Layer 3" > "NAT" in the navigation area and on the "NETMAP" tab in the content area.
2. Specify the NETMAP rule A2 for the outgoing queries with the following settings:

Type	Destination
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816_2
Source IP Subnet	192.168.20.0/24
Destination IP Subnet	192.168.100.0/24
Translated Destination IP Subnet	192.168.10.0/24

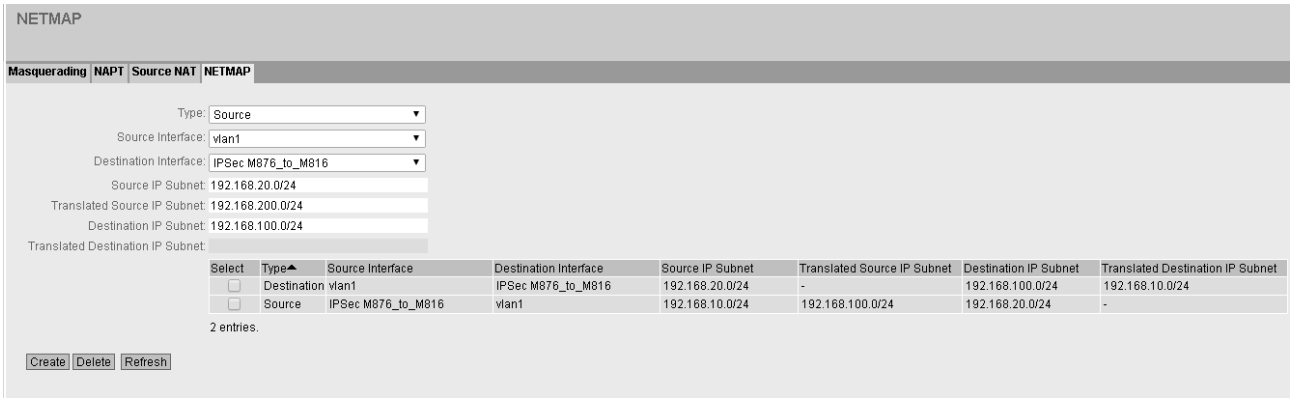
3. Click "Create". A new row is created in the table with the settings.
4. Specify the NETMAP rule B2 for the incoming queries with the following settings:

Type	Source
Source Interface	IPSec M876_to_M816_2
Destination Interface	vlan1
Source IP Subnet	192.168.10.0/24
Translated Source IP Subnet	192.168.100.0/24
Destination IP Subnet	192.168.20.0/24

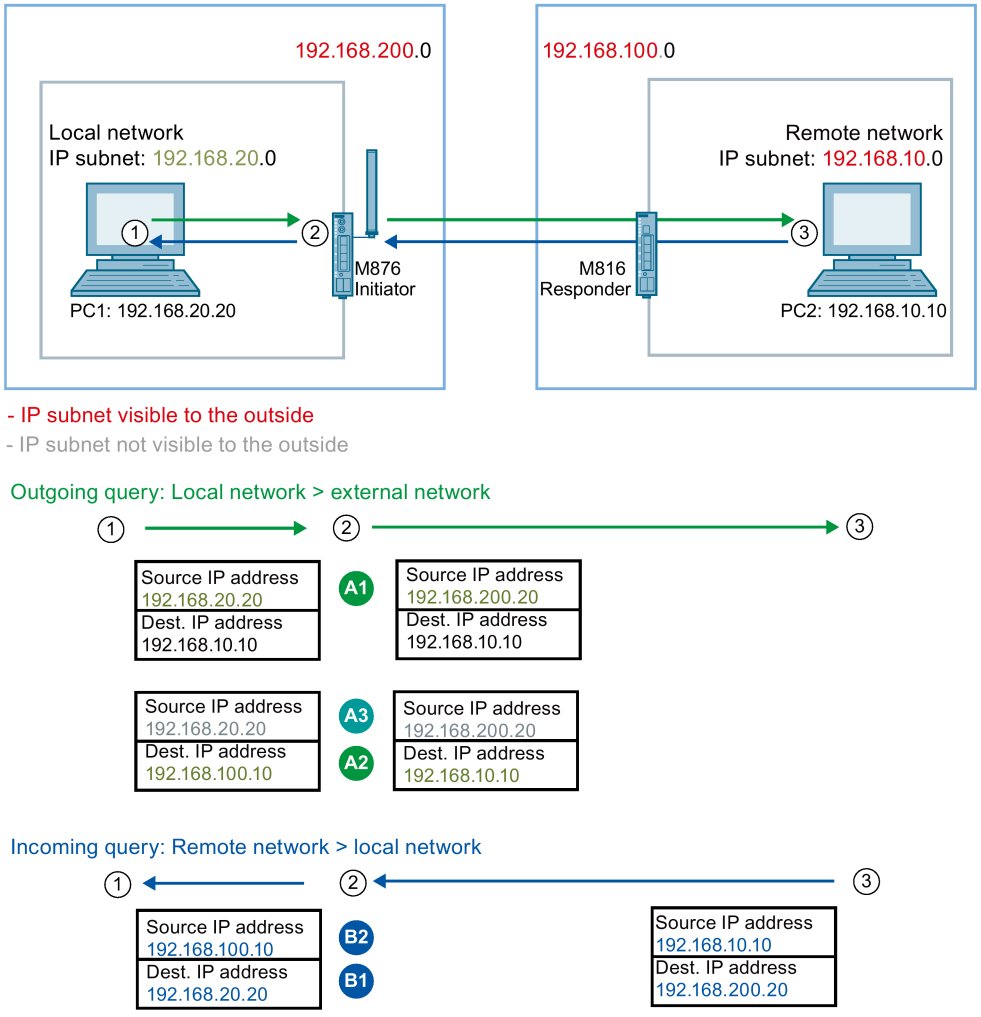
5. Click "Create". A new row is created in the table with the settings.
6. Click "Set Values".

Result

The rules for the outgoing and incoming queries have been created.



6.3 NETMAP for the local and remote network



In this example, the NETMAP rules from NETMAP for the local network (Page 206)and from NETMAP for the remote network (Page 211) are combined. There is, however, a special feature with the outgoing queries. With outgoing queries, whose source IP address is translated from 192.168.20.0 to 192.168.200.0, they can have both the IP address 192.168.10.10 as well as 192.168.100.10 as the destination IP address. The rule for translating the destination IP address requires a further NETMAP rule. The addresses are translated by the M876 ② and forwarded to the destination ③.

With the incoming query both IP addresses are exchanged.

A1 Local network > remote network:
The source IP subnet 192.168.20.0/24 is replaced by 192.168.200.0/24.

A2 The destination IP subnet 192.168.100.0/24 is replaced by 192.168.10.0/24.

A3 With queries with the destination IP subnet 192.168.100.0/24 the source IP subnet 192.168.20.0/24 is replaced by 192.168.200.0/24.

B1 Remote network > local network:
The destination IP subnet 192.168.200.0/24 is replaced by 192.168.20.0/24

B2 The source IP subnet 192.168.10.0/24 is replaced by 192.168.100.0/24

The two devices should also communicate with each other via a VPN tunnel.

Requirement

- The SCALANCE M-800 is connected to the WAN , refer to "Connecting SCALANCE M-800 to the WAN (Page 11)".
- The SCALANCE M-800 can be reached via the Admin PC and you are logged in to the WBM as "admin".

Steps in configuration

The following steps are necessary

1. Creating a VPN connection (Page 217)
2. Creating NETMAP rules (Page 219)

6.3.1 Creating a VPN connection

Procedure

1. Click on "Security" > "IPSec VPN" in the navigation area and on the "General" tab in the content area.
2. Select "Activate IPSec VPN" and click "Set Values".
3. Click on the "Remote End" tab in the content area and create the VPN partner with the following settings:

	On the M816	On the M876
Remote End Name	M876	M816
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Reachable via a dynamic DNS service, e.g. example.no-ip.com	Fixed IP address (WAN IP address) of the M816, e.g. 91.19.6.84
Remote Subnet	192.168.200.0/24	192.168.10.0/24

4. Click on the "Connections" tab in the content area and create the VPN connection with the following settings:

	On the M816	On the M876
Connection Name	M816_to_M876	M876_to_M816
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M876	M816
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Click on the "Authentication" tab in the content area and configure the VPN authentication with the following settings:

	On the M816	On the M876
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	e. g. 12345678	e. g. 12345678

6. Click on the "Phase 1" tab in the content area and configure the following settings:

	M816 / M876
DPD	enabled
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	no

7. Click on the "Phase 2" tab in the content area and configure the following settings:

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M816)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Result

The VPN connection on the devices is configured. To establish the VPN connection, click on the "Connection" tab in the content area.

For "Operation" select the following and click "Set Values"

	On the M816	On the M876
Operation	wait (Responder)	start (Initiator)

The M876 establishes the VPN tunnel to the M816. If the VPN tunnel is established, the LED is lit green on the devices.

6.3.2 Creating NETMAP rules

Requirement

- The VPN connection M876_to_M816_2 is configured, see Creating a VPN connection (Page 217).
- The NETMAP rules for the local network (Page 214)have been created.
- The NETMAP rules for the remote network (Page 209)have been created.

Procedure

1. Click on "Layer 3" > "NAT" in the navigation area and on the "NETMAP" tab in the content area.
2. Specify the NETMAP rule A3 for the outgoing queries with the following settings:

Type	Source
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816_2
Source IP Subnet	192.168.20.0/24
Destination IP Subnet	192.168.100.0/16
Translated Source IP Subnet	192.168.200.0/24

3. Click "Create". A new row is created in the table with the settings.
4. Click "Set Values".

Result

The rules for the outgoing and incoming queries have been created.