SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks Configuring VPN tunnel

Getting Started

01/2019

C79000-G8976-C541-01

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Global Services Information Technology
80200 MÜNCHEN
GERMANY

Document order number: C79000-G8976-C541
℗ 01/2019 Subject to change

Preface

Purpose

Access via the user-specific firewall is configured based on an example.

IP settings for the examples

Note

The IP settings used in the examples were freely chosen.

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

General naming conventions

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

Further documentation

- Operating instructions

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

  – SCALANCE M874, M876

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

  – SCALANCE M812, M816

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

  – SCALANCE M804PB:

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

  – SCALANCE M826:

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

  – SCALANCE S615:

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

- "Web based Management" configuration manual

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

  – SCALANCE M-800:

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

  – SCALANCE S615:

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

- Configuration manual Command Line Interface

  This document contains the CLI commands supported by the devices.

  – SCALANCE M-800

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

  – SCALANCE S615

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

- Industrial Ethernet Security – Basics and Application

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

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

- SIMATIC NET Industrial Ethernet Network manual

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

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

SIMATIC NET manuals

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

- using the search function:

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

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

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

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

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

Training, Service & Support

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

SIMATIC NET glossary

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

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

50305045*** NO TRANSLATION IN THIS VERSION! ***
(https://support.industry.siemens.com/cs/ww/en/view/50305045)

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit
Link:*** NO TRANSLATION IN THIS VERSION! ***
(https://www.siemens.com/industrialsecurity)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link:*** NO TRANSLATION IN THIS VERSION! ***
(https://www.siemens.com/industrialsecurity)

Firmware

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

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Table of contents

VPN tunnel between SCALANCE M-800 and S612

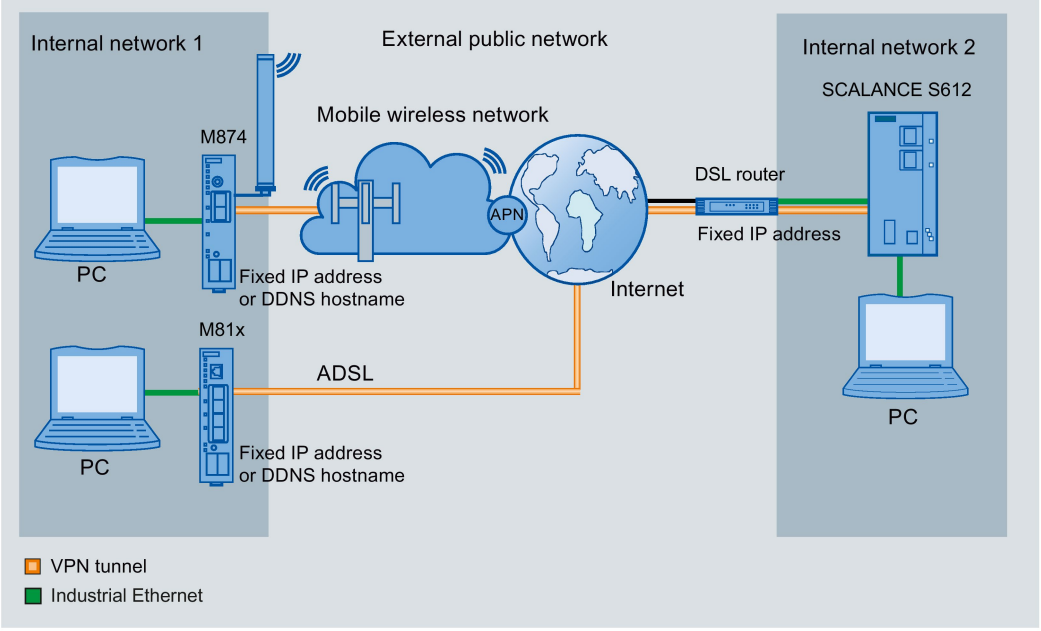
1

1.1 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".
- 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
2. Configuring a tunnel connection
3. Configuring the properties of the S612
4. Downloading the configuration to the S612 and saving the M-800 configuration

Configuring a VPN tunnel with the SCT V4.x

1. Creating the project and modules (Page 15)
2. Configuring a tunnel connection (Page 18)
3. Configuring the properties of the S612 (Page 19)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 20)

Configuring the SCALANCE M-800

1. Activating VPN (Page 21)
2. Configuring the VPN remote end (Page 22)
3. Configuring a VPN connection (Page 23)
4. Configuring VPN authentication (Page 24)
5. Configuring phase 1 and phase 2 (Page 24)
6. Establishing the VPN connection (Page 26)

Example 2: Secure VPN tunnel with certificates

Configuring a VPN tunnel with the SCT V3.x

1. Creating the project and modules
2. Configuring a tunnel connection
3. Configuring the properties of the S612
4. Downloading the configuration to the S612 and saving the M-800 configuration

Configuring a VPN tunnel with the SCT V4.x

1. Creating the project and modules (Page 28)
2. Configuring a tunnel connection (Page 31)
3. Configuring the properties of the S612 (Page 32)
4. Downloading the configuration to the S612 and saving the M-800 configuration (Page 33)

Configuring the SCALANCE M-800

1. Loading a certificate (Page 34)
2. Activating VPN (Page 40)
3. Configuring the VPN remote end (Page 36)
4. Configuring a VPN connection (Page 37)
5. Configuring VPN authentication (Page 38)
6. Configuring phase 1 and phase 2 (Page 39)
7. Establishing the VPN connection (Page 41)

1.2 Secure VPN tunnel with PSK

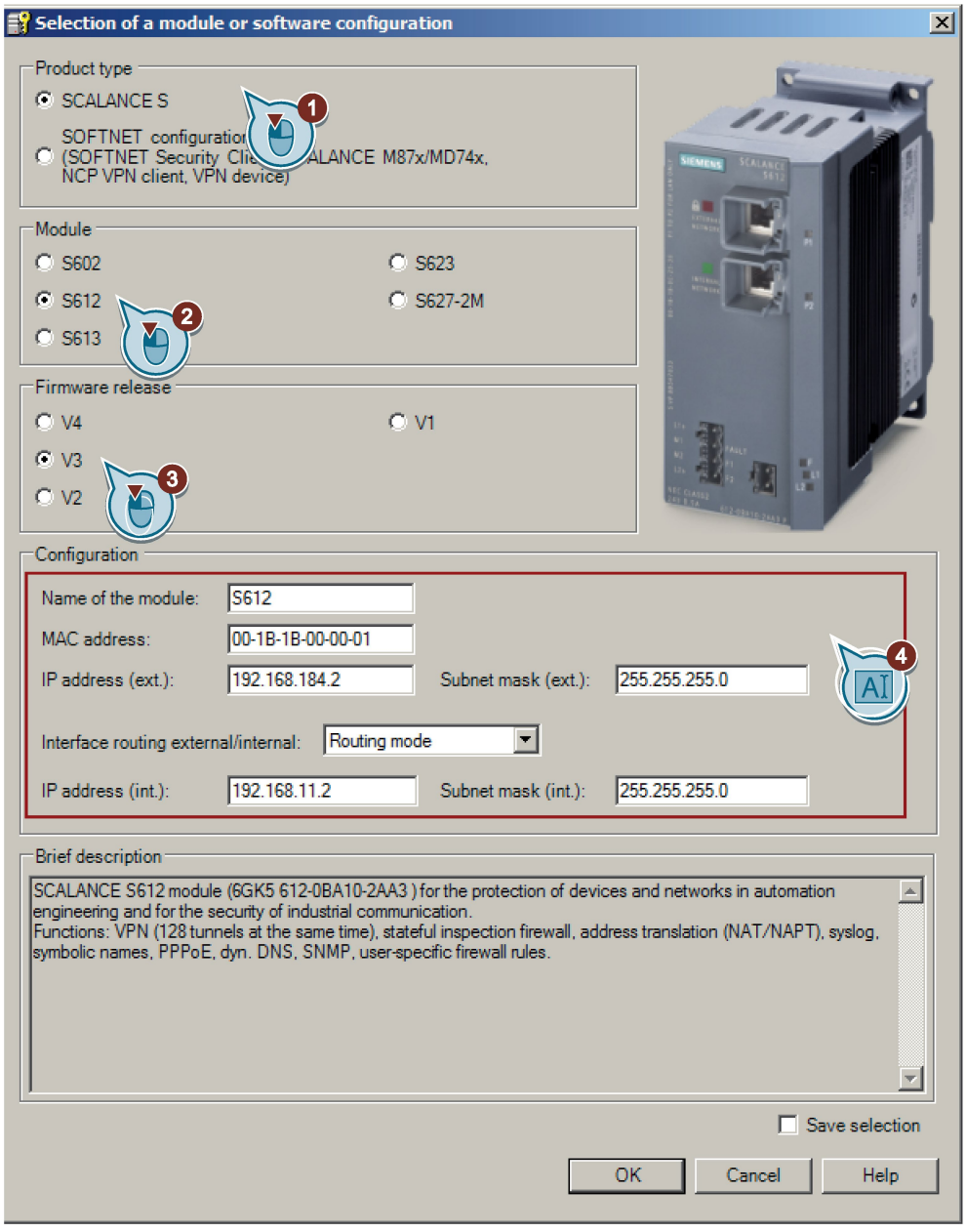
1.2.1 Configuring a VPN tunnel with the SCT V4.x

1.2.1.1 Creating the project and modules

Procedure

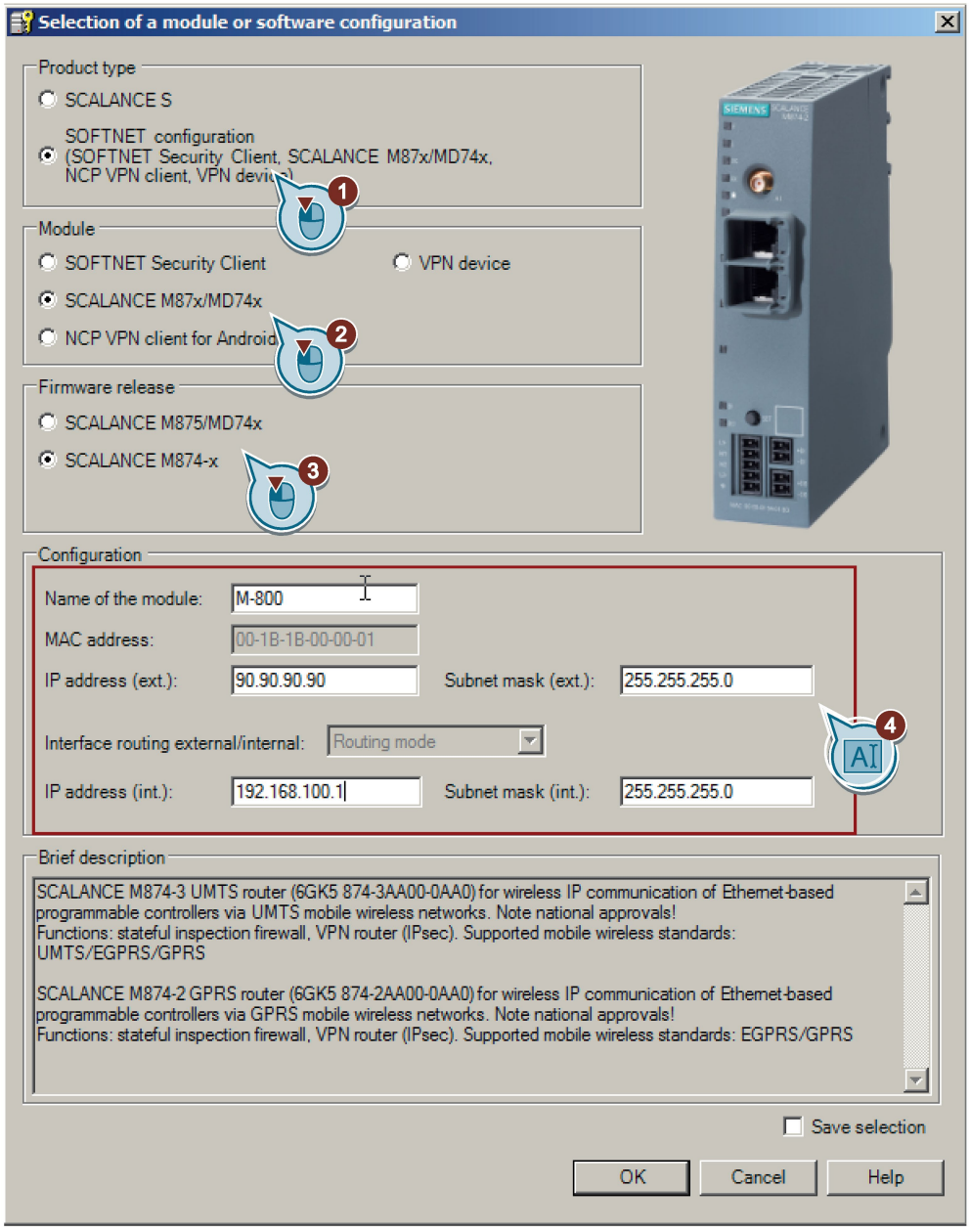
1. Start the Security Configuration Tool V4.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new 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 11)" 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 11)" table.



9. Close the dialog with "OK".

Result

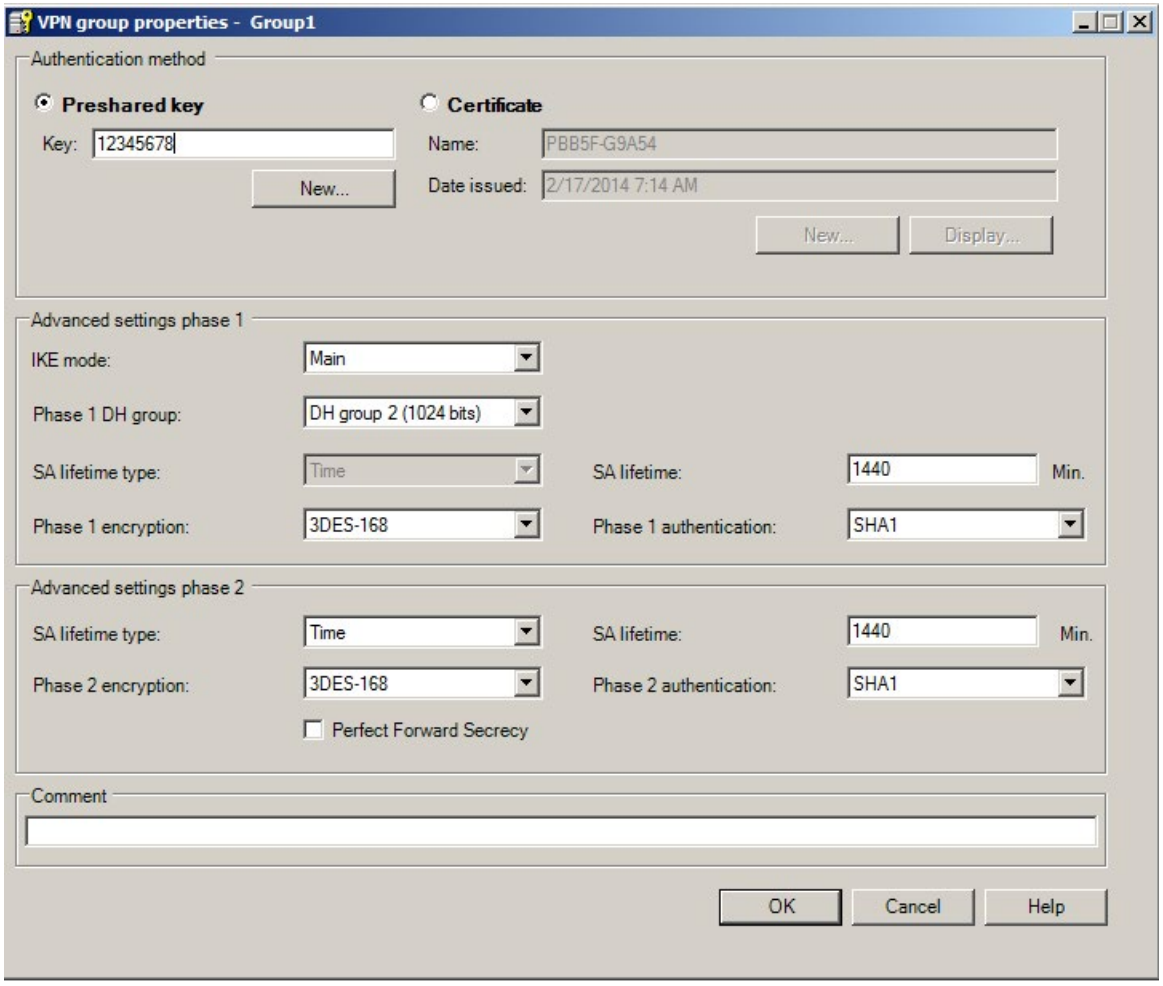
The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

1.2.1.2 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

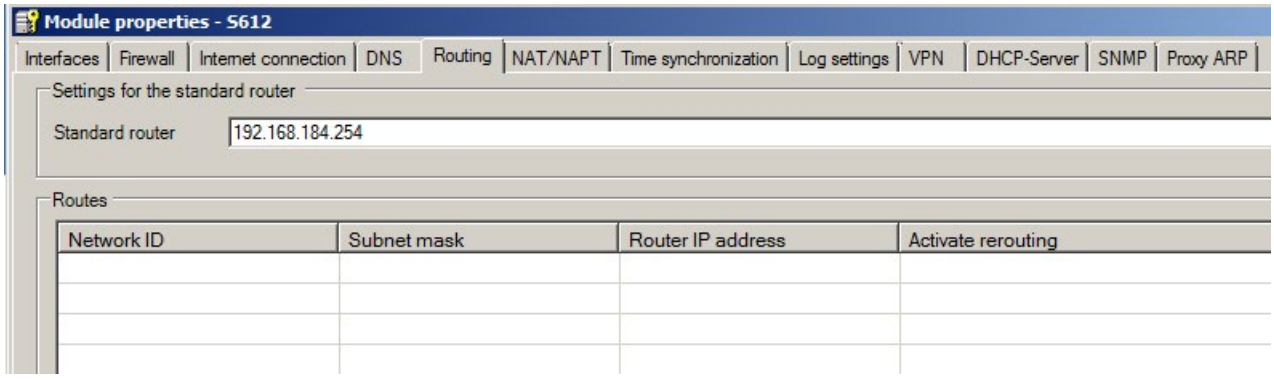
The configuration of the tunnel connection is complete.

1.2.1.3 Configuring the properties of the S612

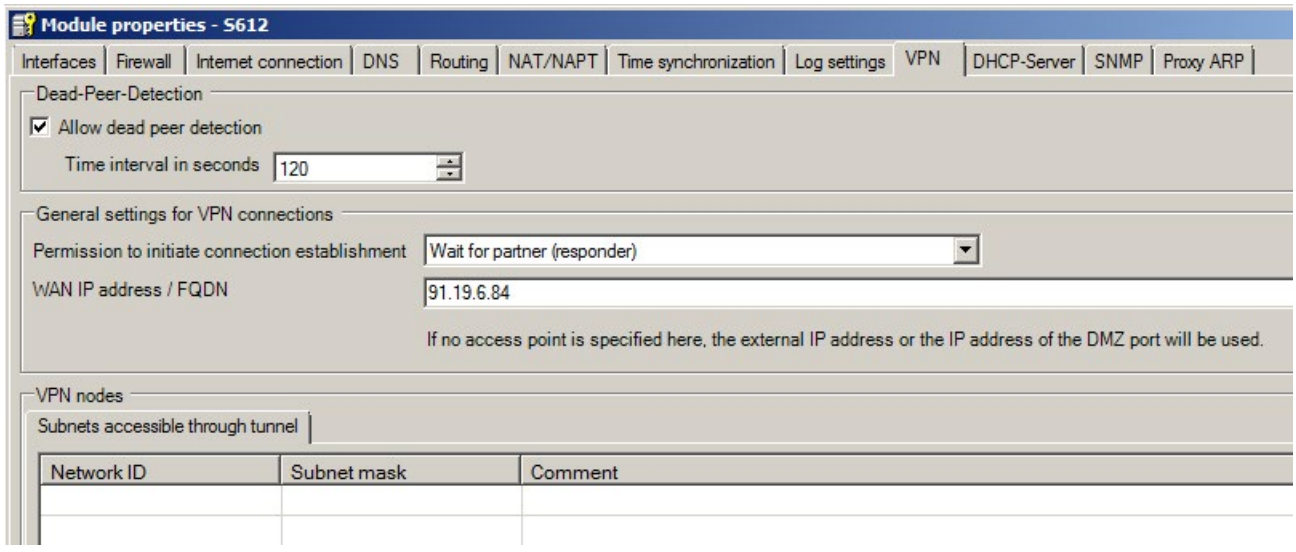
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

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

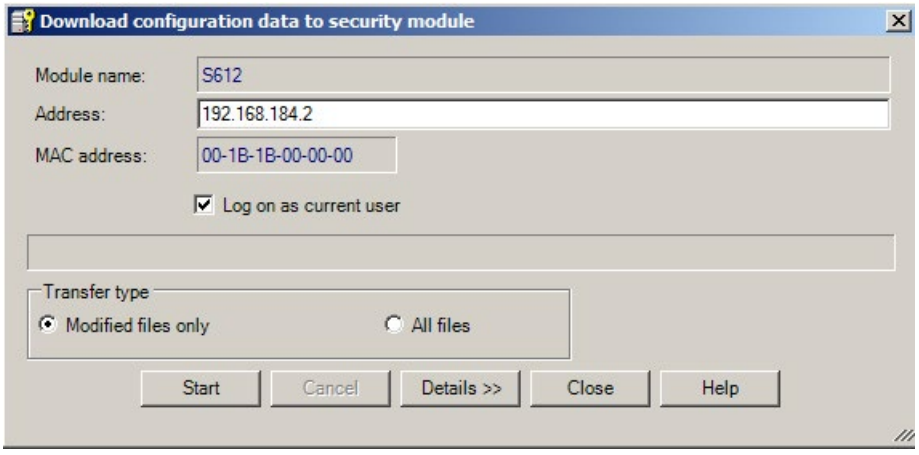
Result

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

1.2.1.4 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 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

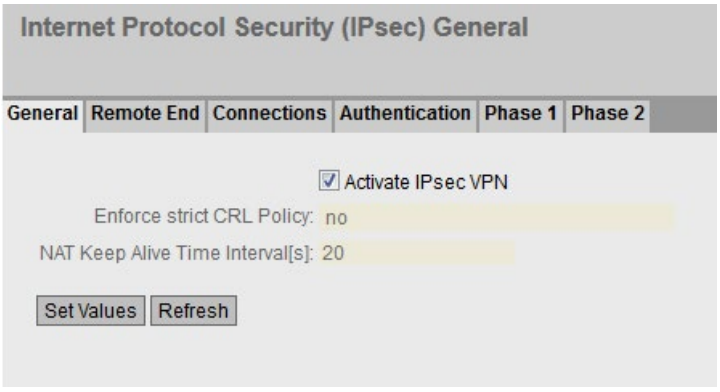
The configuration file contains the exported configuration information for the SCALANCE M-800. Follow the instructions in the configuration file.

1.2.2 Configuring SCALANCE M-800

1.2.2.1 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.



3. Click on "Set Values".

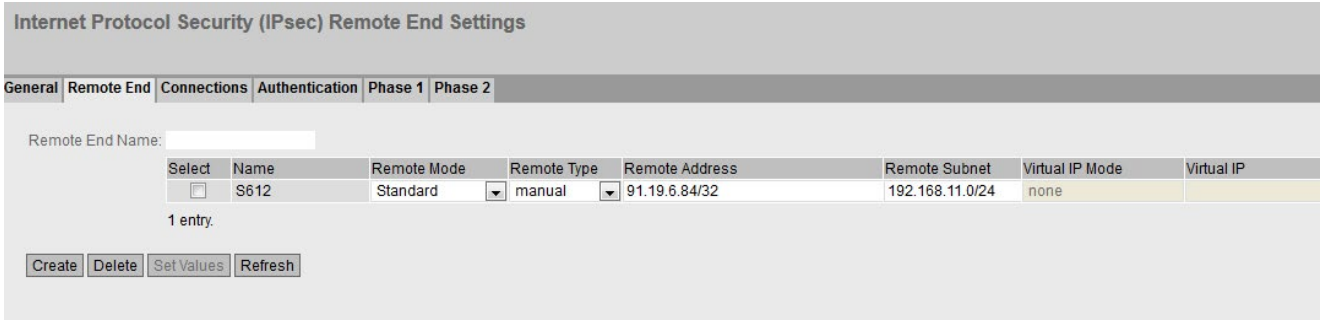
1.2.2.2 Configuring the VPN remote end

M81x in the master station: Configuring the VPN remote end

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 Type	Manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.11.0/24

5. Click on "Set Values".



1.2.2.3 Configuring a VPN connection

Requirement

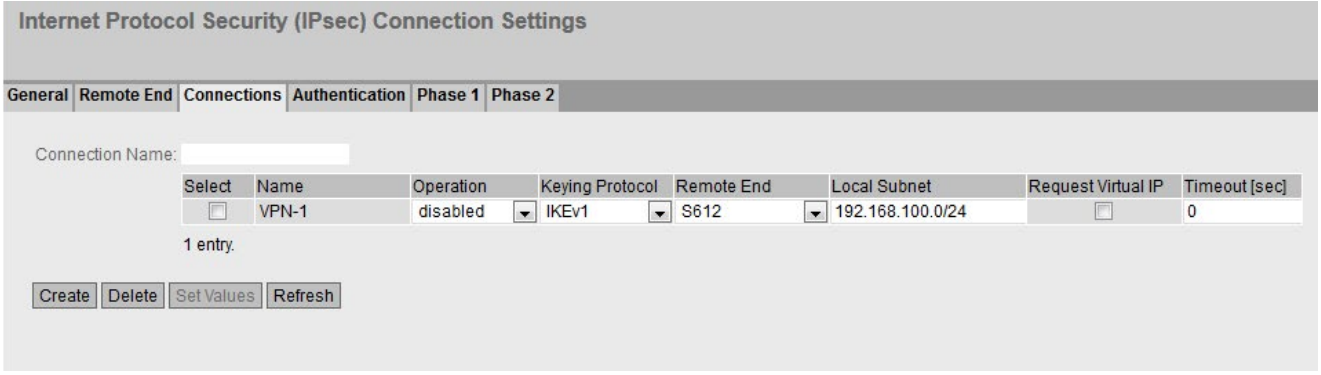
- The VPN remote end has been created.

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" 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 subnet 1 in CIDR notation.

5. Click on "Set Values".



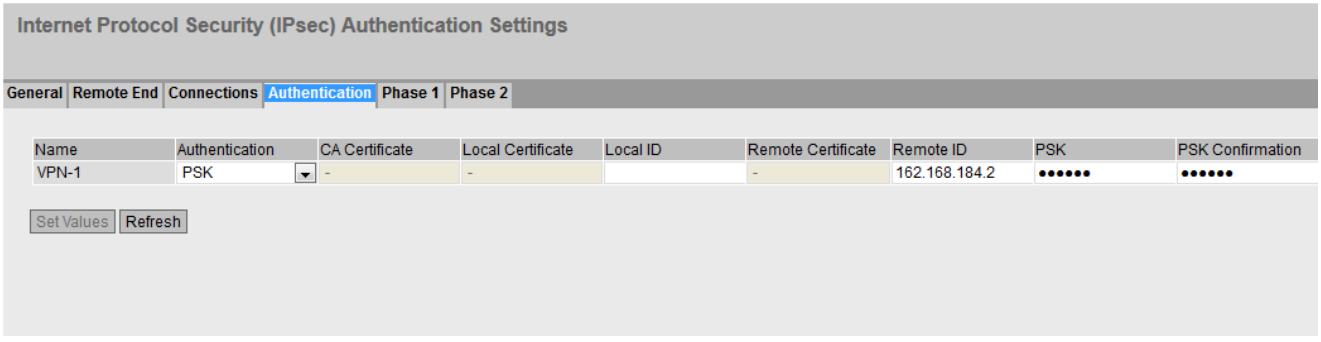
1.2.2.4 Configuring VPN authentication

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 on "Set Values".



1.2.2.5 Configuring phase 1 and phase 2

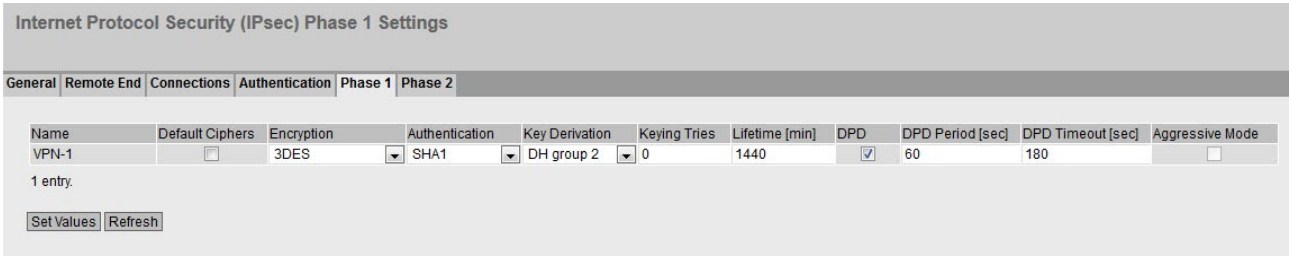
Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.

4. Configure phase 1 with the following settings from the configuration file:

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

5. Click on "Set Values".

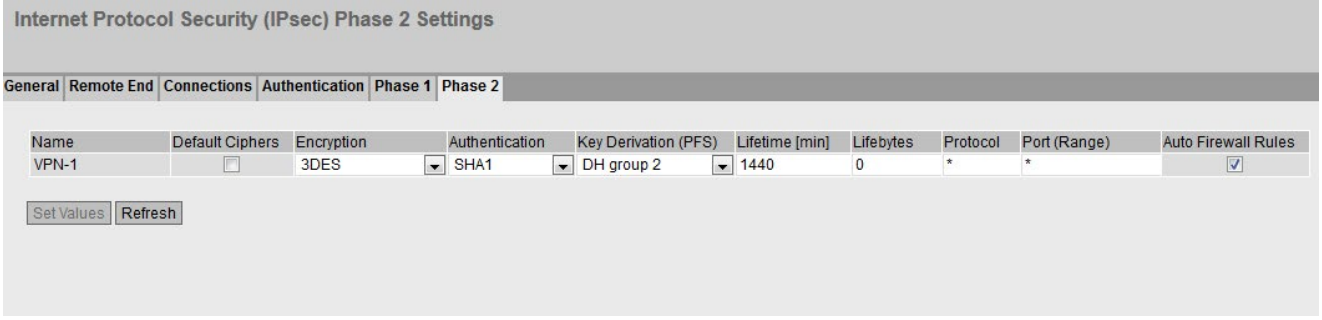


Configuring phase 2

1. Click the "Phase 2" tab.
2. Deselect the "Default Ciphers" check box.
3. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
Key Derivation (DFS)	DH group 2
Lifetime [min]:	1440

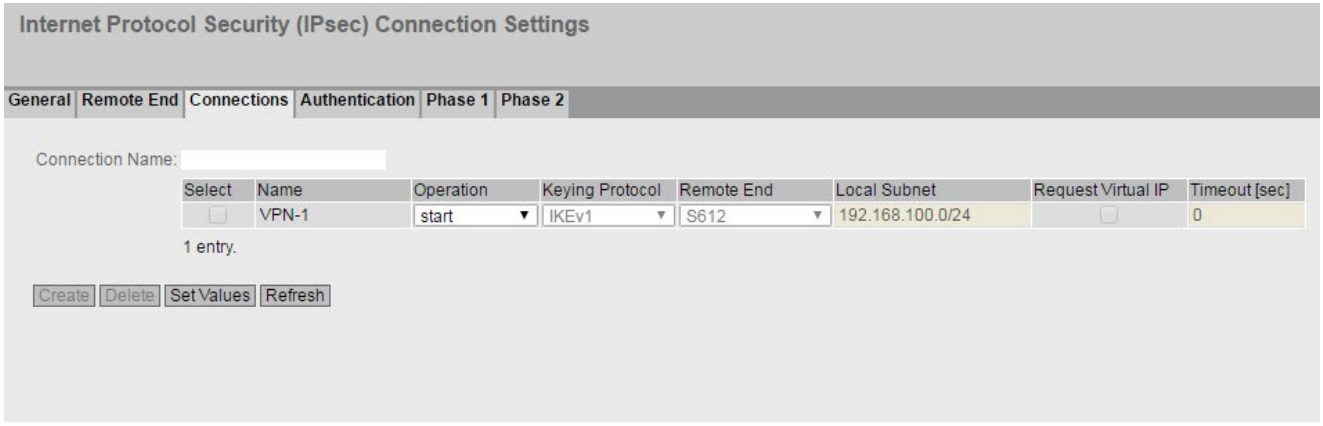
4. Click on "Set Values".



1.2.2.6 Establishing the VPN connection

Procedure

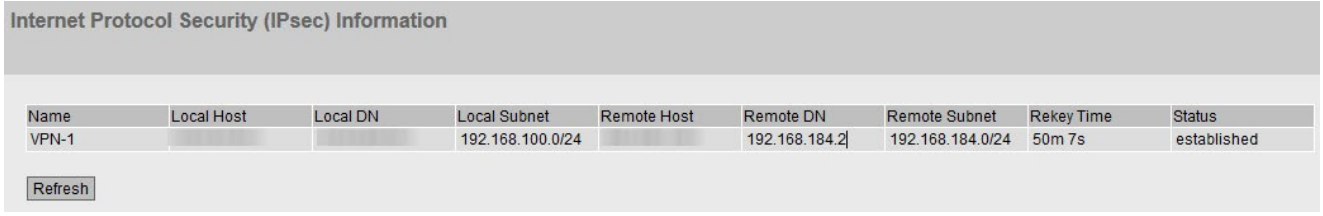
1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" tab in the content area.
2. As "Operation", select "Start" and click "Set Values".



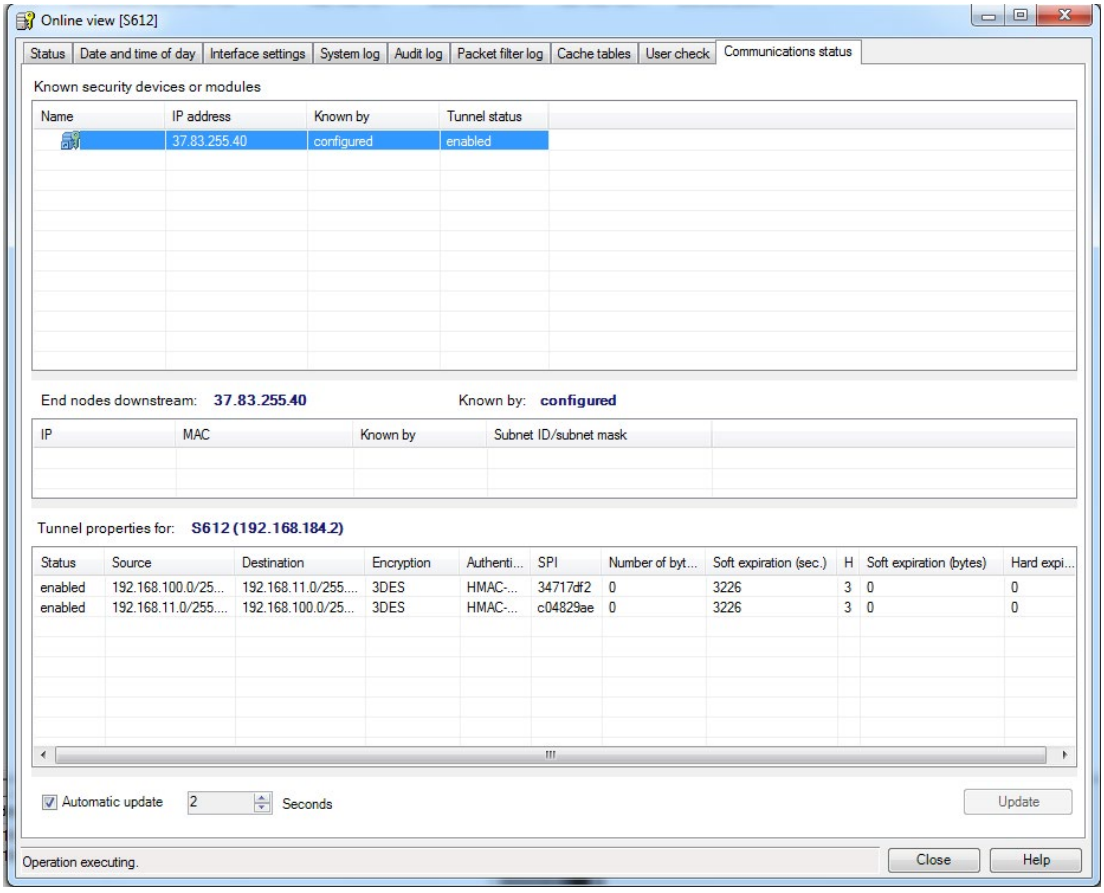
Result

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.



1.3 Secure VPN tunnel with certificates

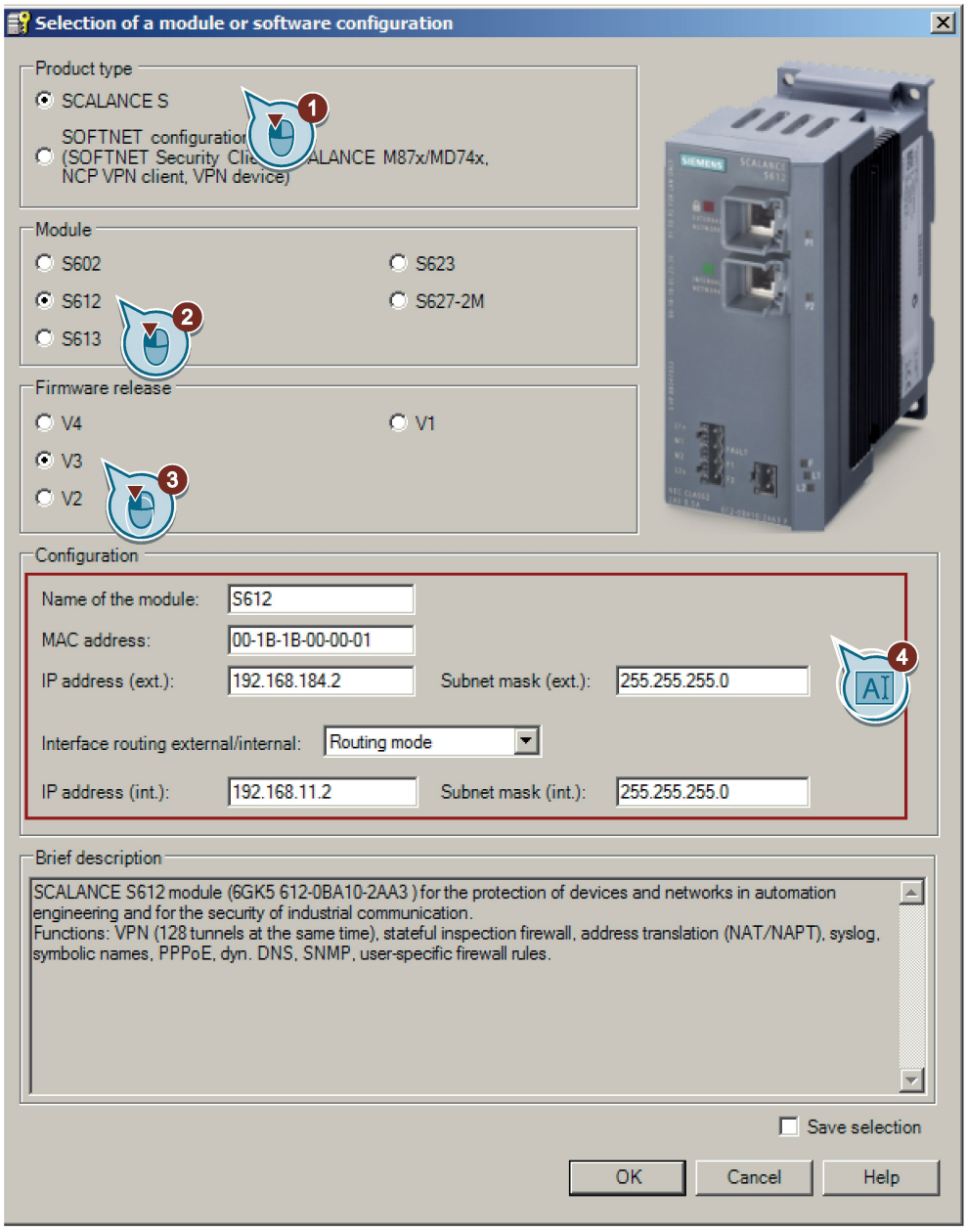
1.3.1 Configuring a VPN tunnel with the SCT V4.x

1.3.1.1 Creating the project and modules

Procedure

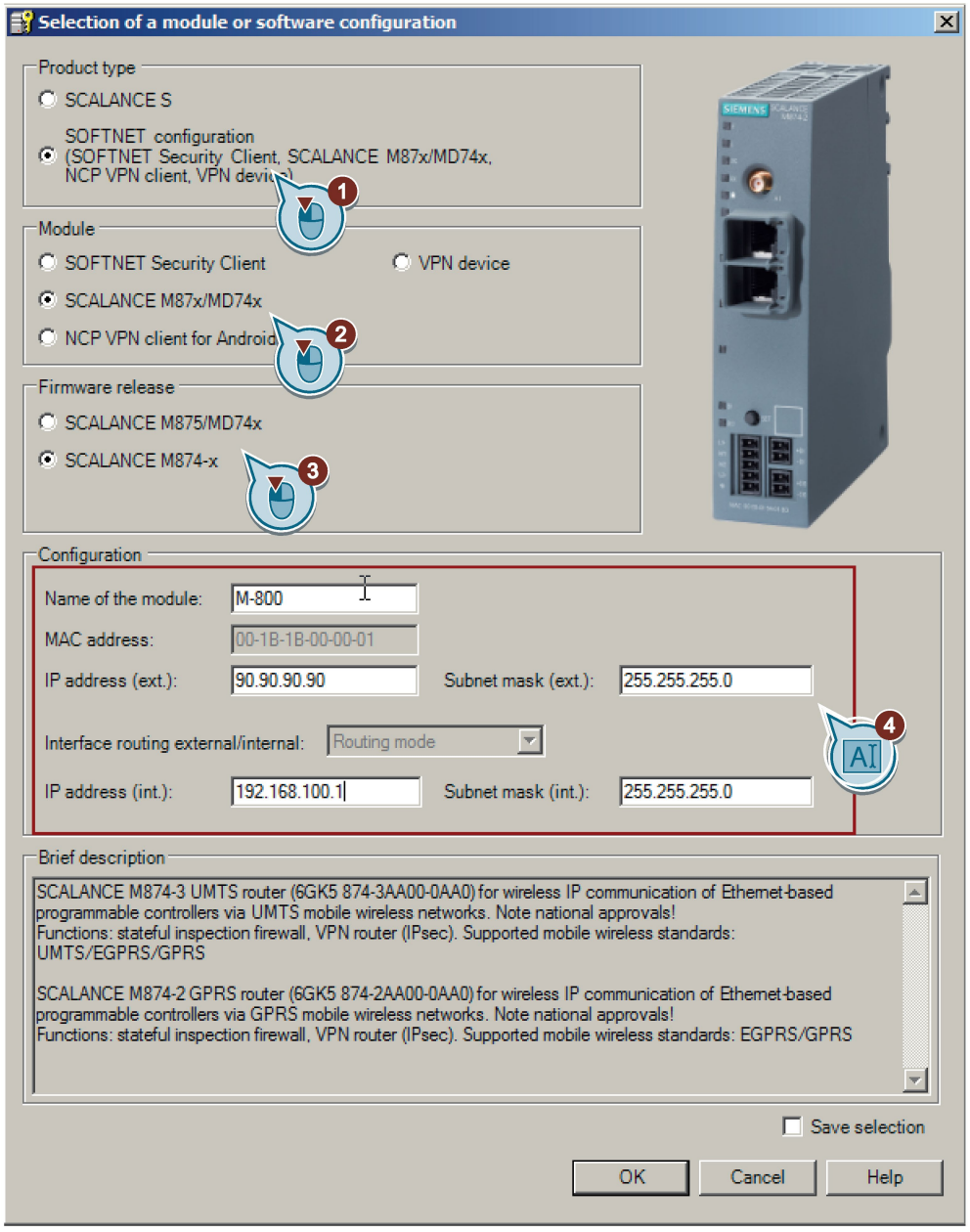
1. Start the Security Configuration Tool V4.x on the PC.
2. Select the menu command "Project" > "New".
3. In the dialog that follows, create a new user with a user name and the corresponding password. The "administrator" role is assigned to the user automatically.
4. Confirm the dialog with "OK". A new 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 11)" 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 11)" table.



9. Close the dialog with "OK".

Result

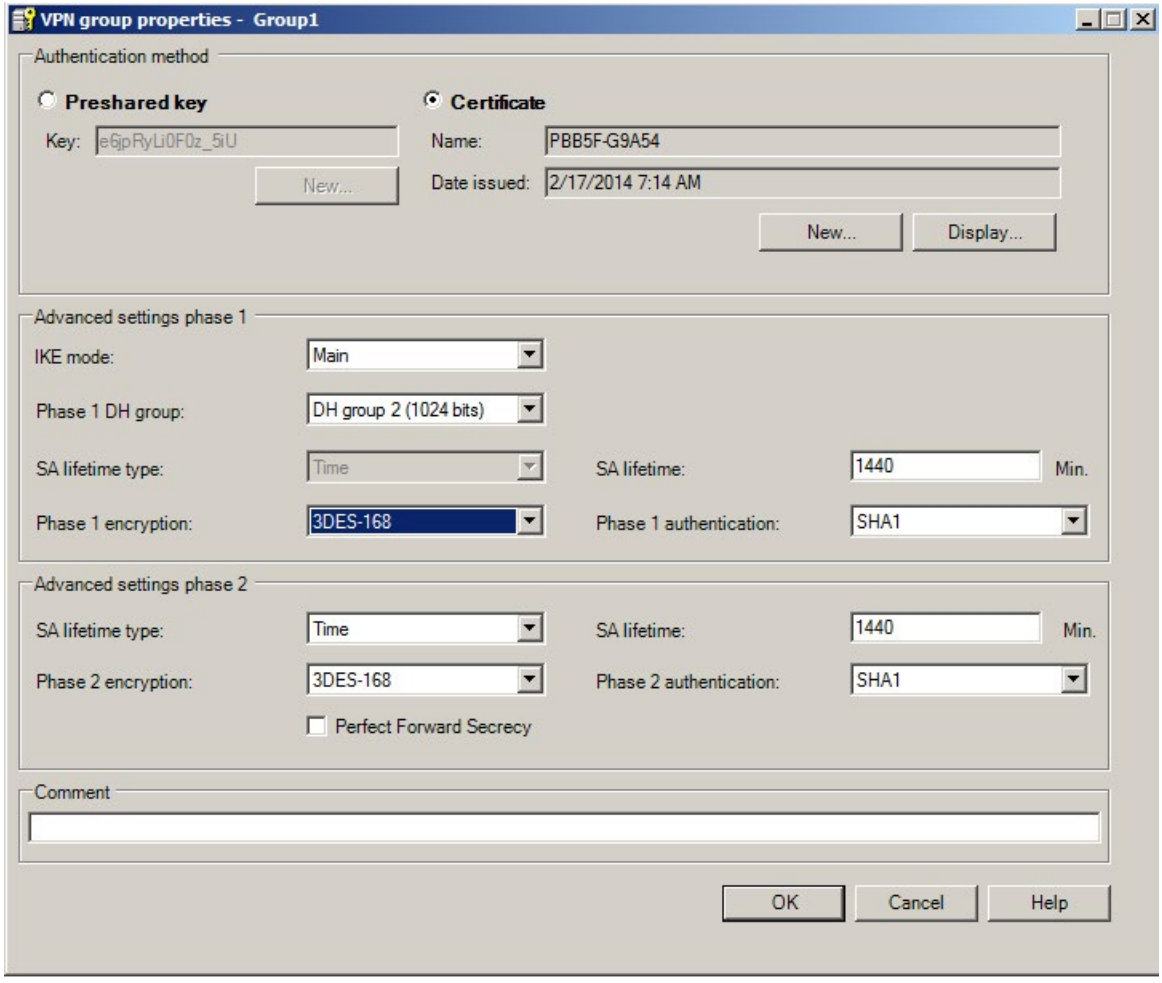
The security module S612 and the SCALANCE M-800 will then be displayed in the list of configured modules.

1.3.1.2 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

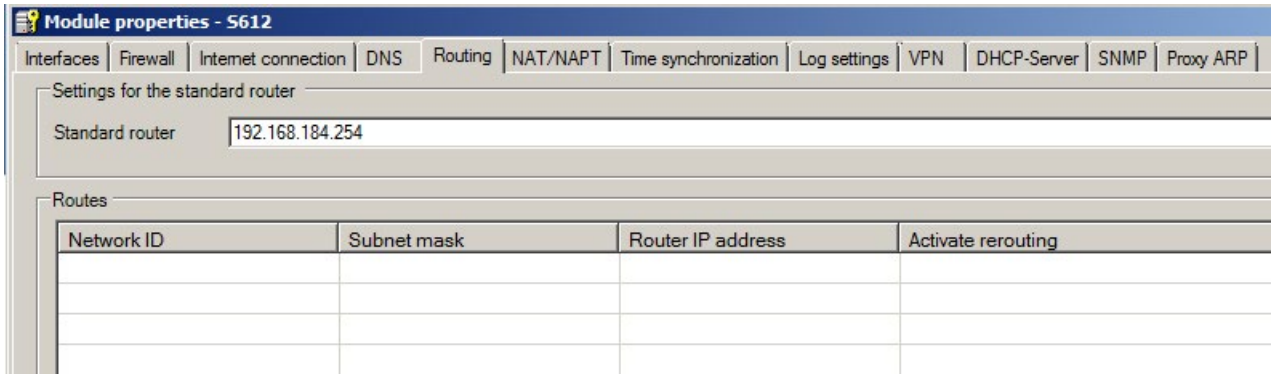
The configuration of the tunnel connection is complete.

1.3.1.3 Configuring the properties of the S612

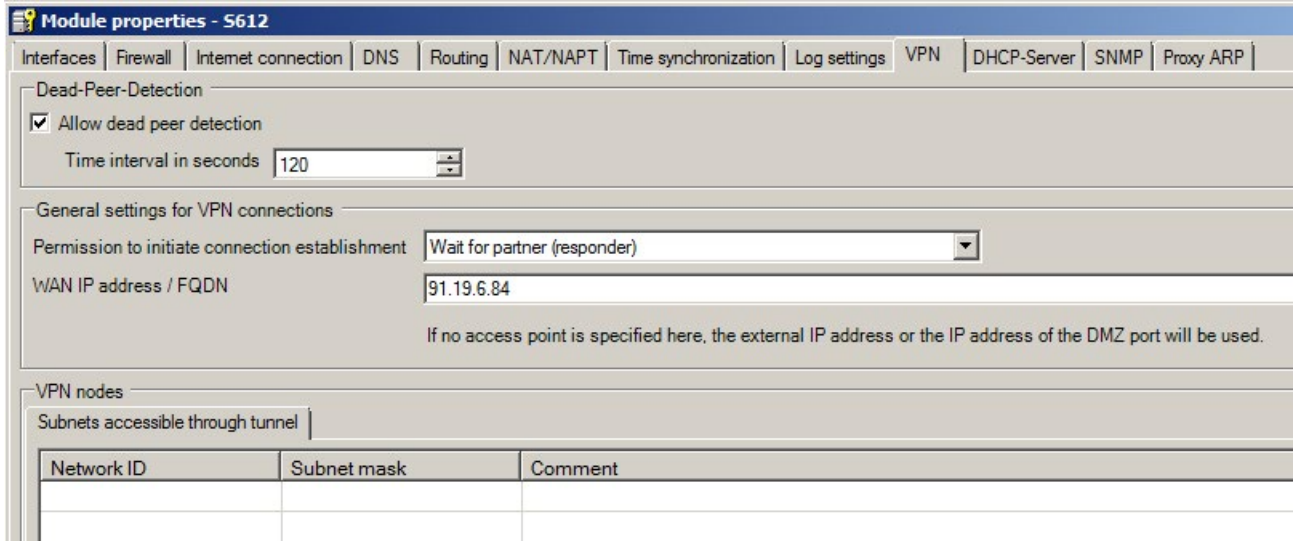
Since the S612 is connected to the Internet via a DSL router, the properties of the S612 must be configured accordingly.

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

Result

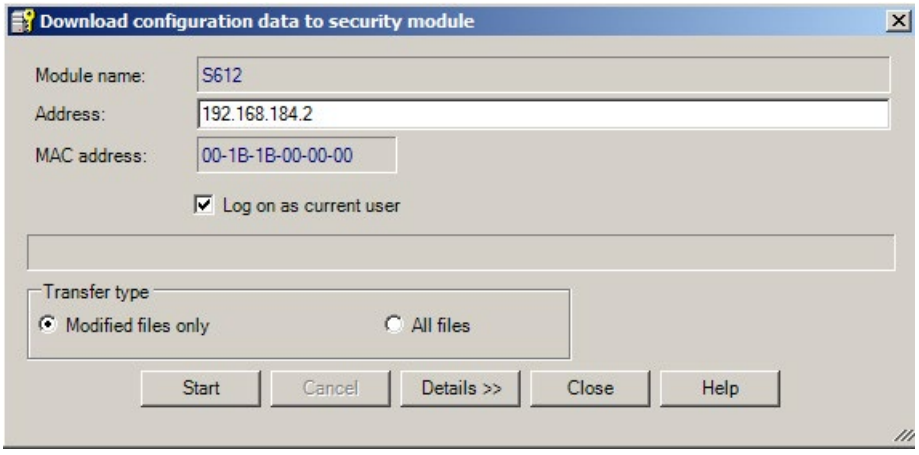
The security project is configured. The settings are saved in the configuration file.

1.3.1.4 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. Follow the instructions in the configuration file.

1.3.2 Configuring SCALANCE M-800 (*** NO TRANSLATION IN THIS VERSION! ***)

1.3.2.1 Loading a certificate

Requirement

- The correct time is set on the SCALANCE M-800, refer to the section AUTOHOTSPOT.
- Certificates are available.

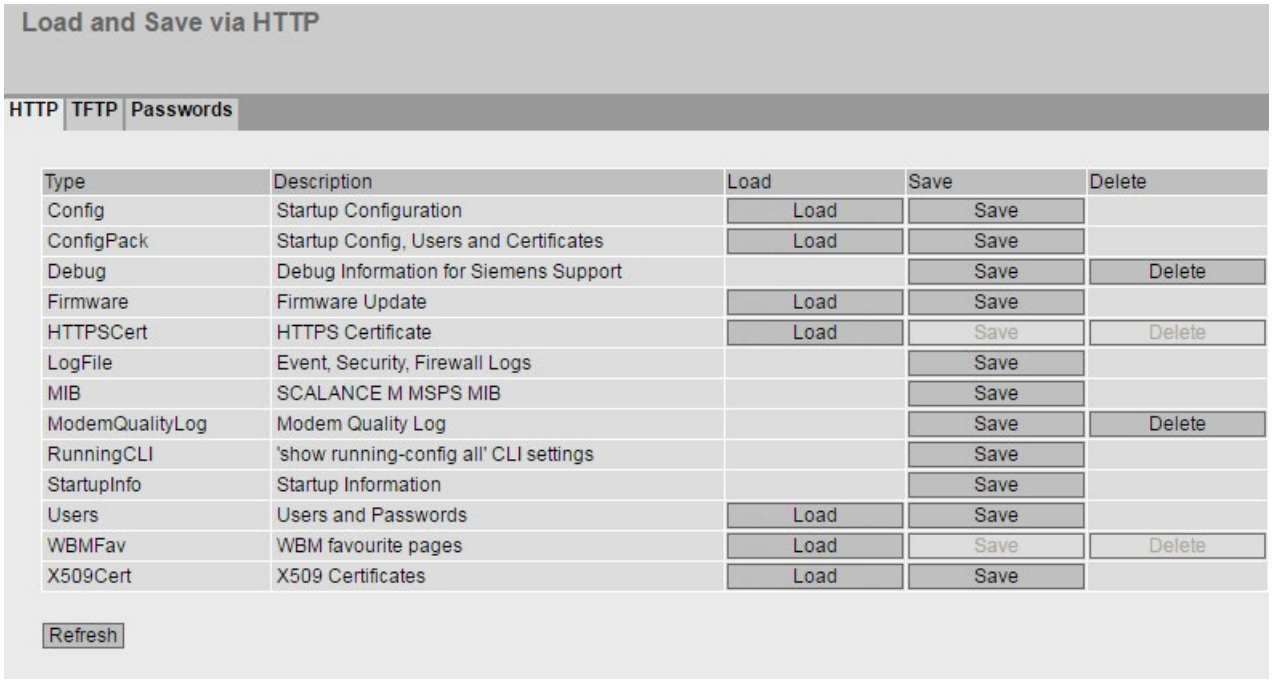
  You saved the required certificates on the PC in the last section and assigned a password for the private key.

  Transfer the certificates for the SCALANCE M-800 to the Admin PC.

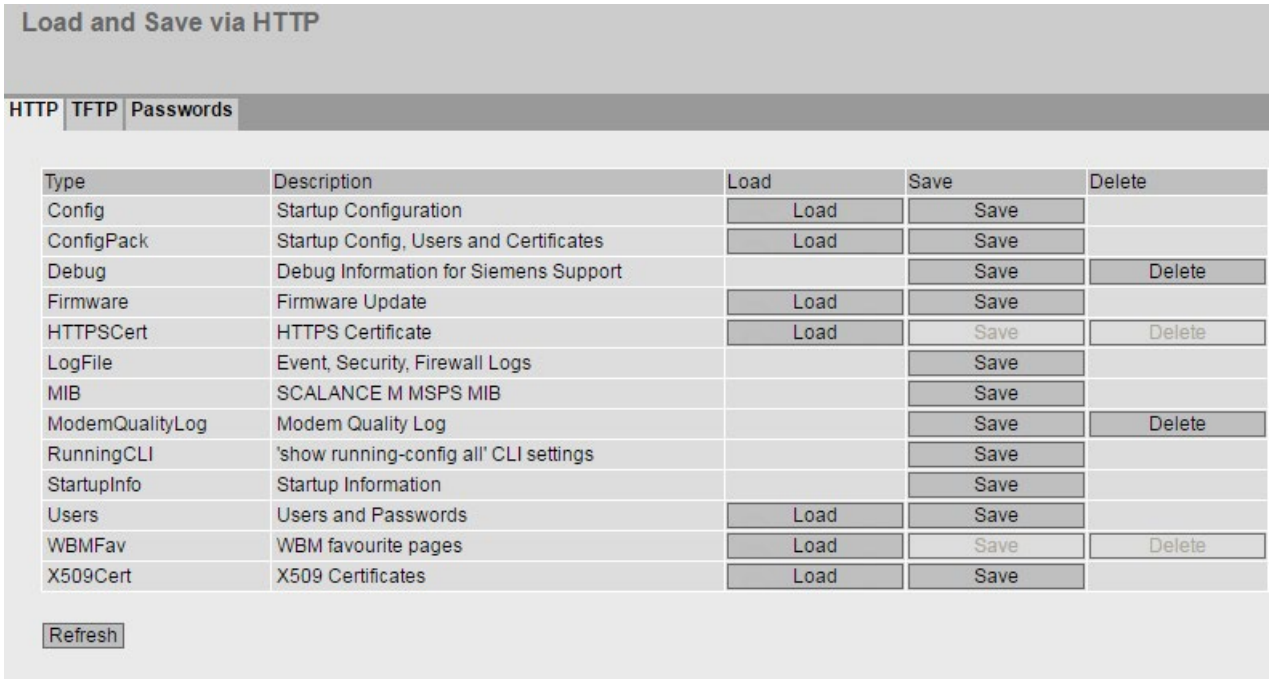
Procedure

1. Click on "System" > "Load&Save" in the navigation area and on the "Passwords"" tab in the content area.
2. In the line "X509Cert" enter the password that you specified for the PKCS12 file in "Password" and "Password confirmation".
3. Enable the password

4. Click on "Set Values".



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



6. For "X509Cert" click the "Loading" button. The dialog for loading a file is opened. Navigate to the remote certificate.

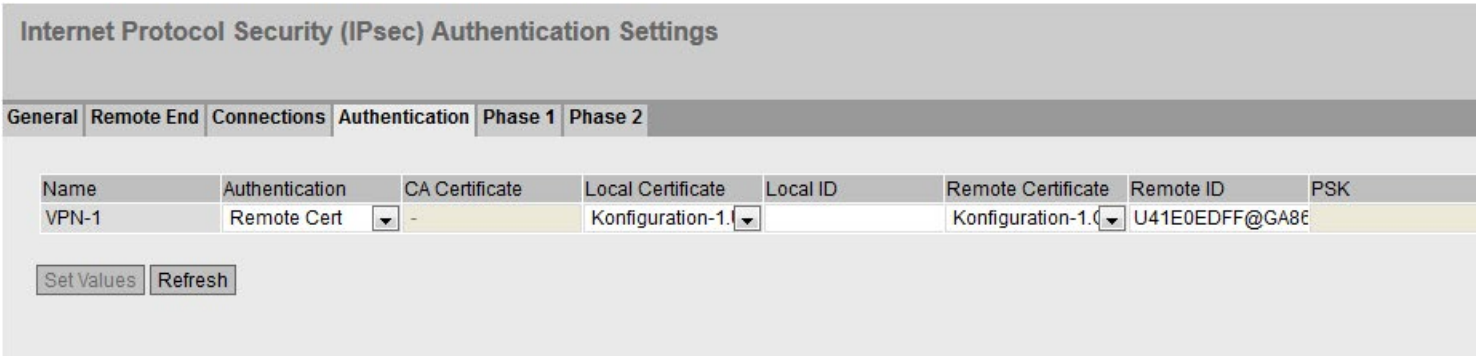
7. Click the "Open" button in the dialog.

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

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

Result

Certificates are loaded and are displayed in "Security" > "Certificates". The loaded certificates must have the status "Valid".



1.3.2.2 Configuring the VPN remote end

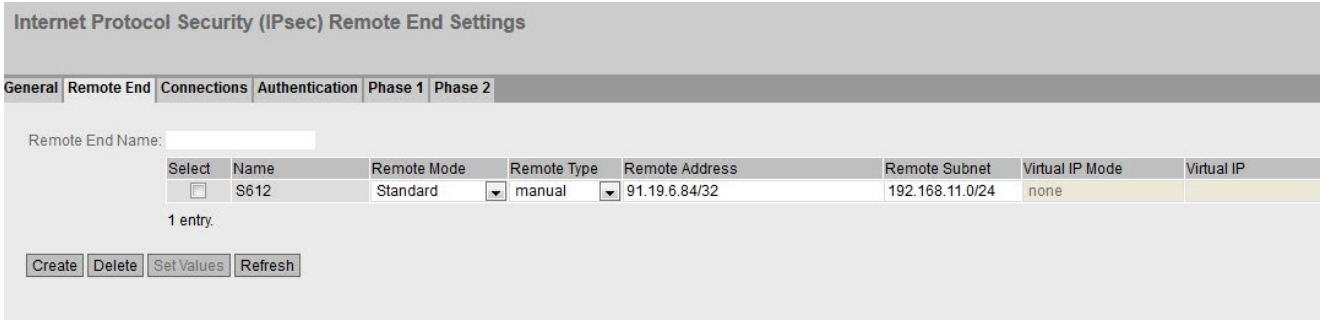
M81x in the master station: Configuring the VPN remote end

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 Type	Manual
Remote Address	91.19.6.84/32 WAN IP address of the DSL router
Remote Subnet	192.168.11.0/24

5. Click on "Set Values".



1.3.2.3 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

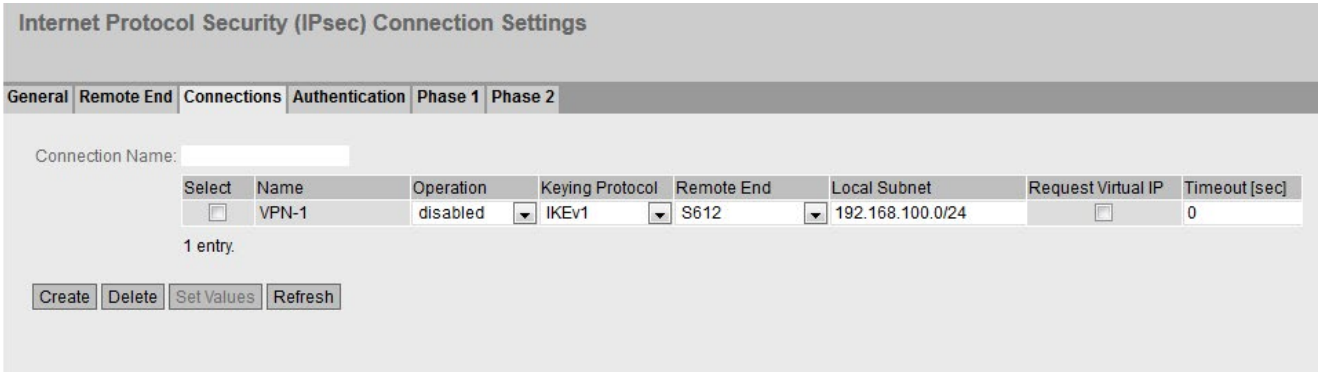
Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" 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 subnet 1 in CIDR notation.

5. Click on "Set Values".



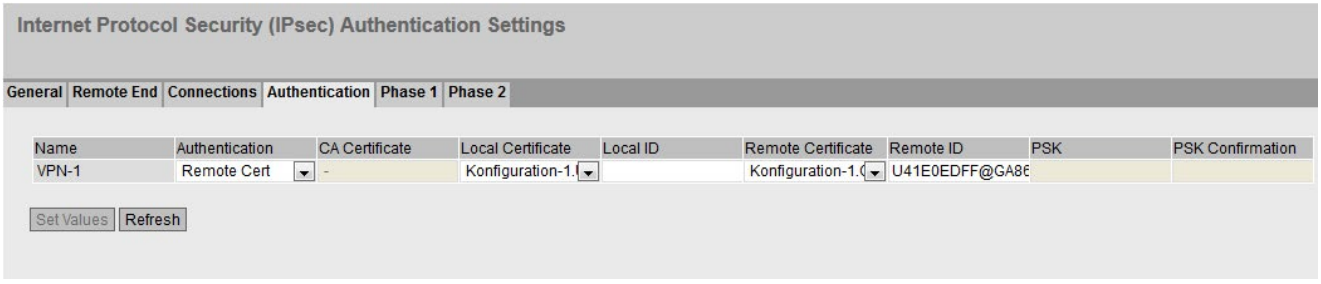
1.3.2.4 Configuring VPN authentication

M81x in the master station: Configuring VPN authentication

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 on "Set Values".



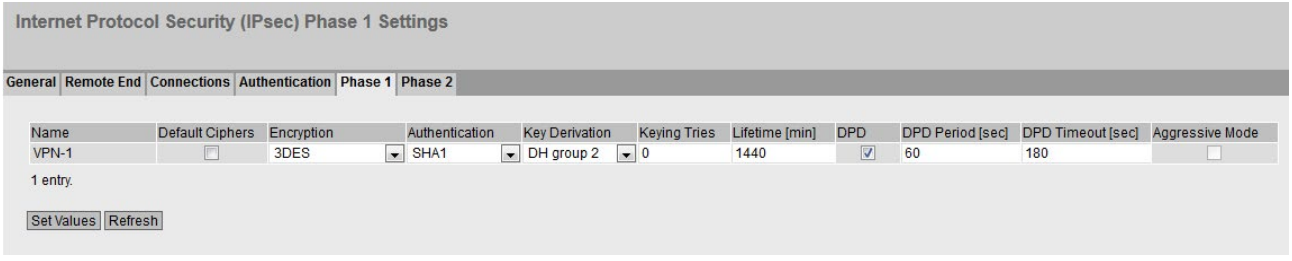
1.3.2.5 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.
4. Configure phase 1 with the following settings from the configuration file:

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

5. Click on "Set Values".



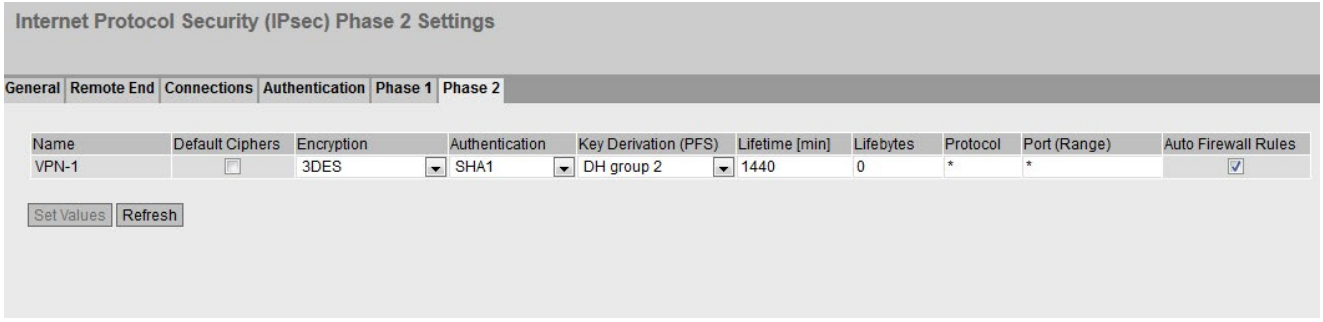
Configuring phase 2

1. Click the "Phase 2" tab.
2. Deselect the "Default Ciphers" check box.

3. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
Key Derivation (DFS)	DH group 2
Lifetime [min]:	1440

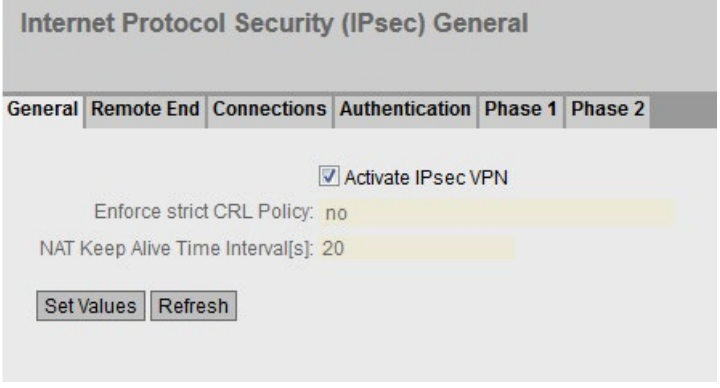
4. Click on "Set Values".



1.3.2.6 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.

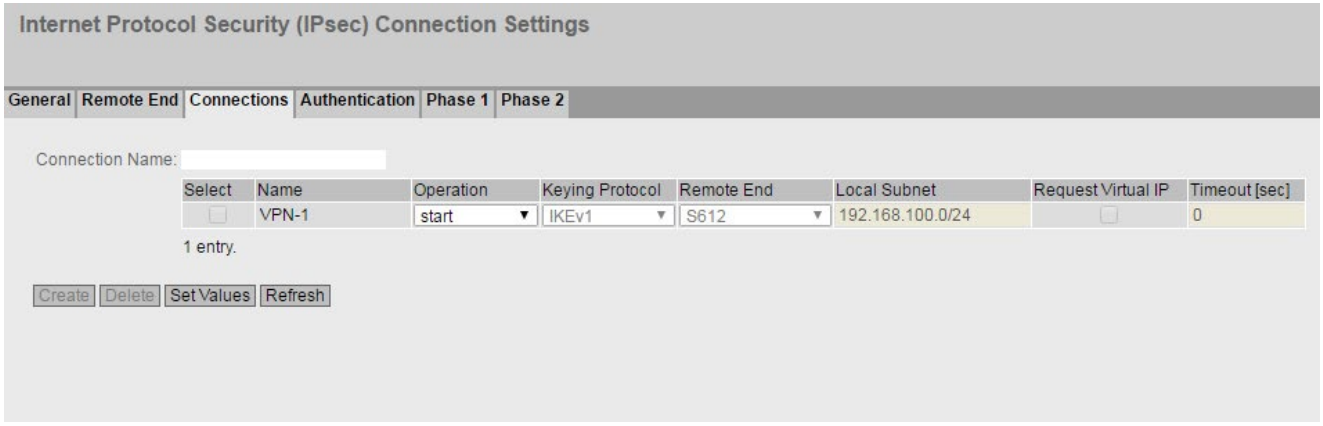


3. Click on "Set Values".

1.3.2.7 Establishing the VPN connection

Procedure

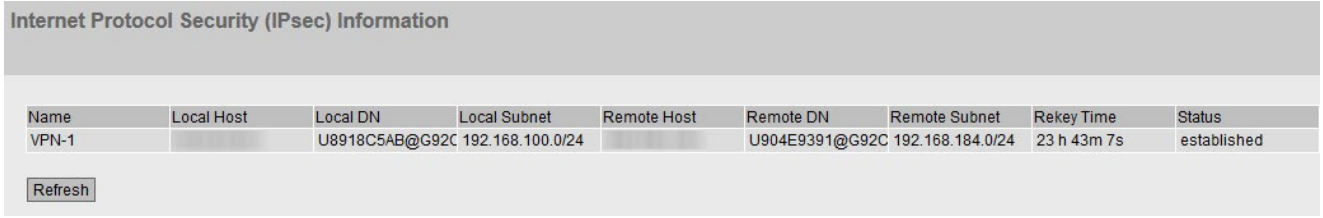
1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" tab in the content area.
2. As "Operation", select "Start" and click "Set Values".



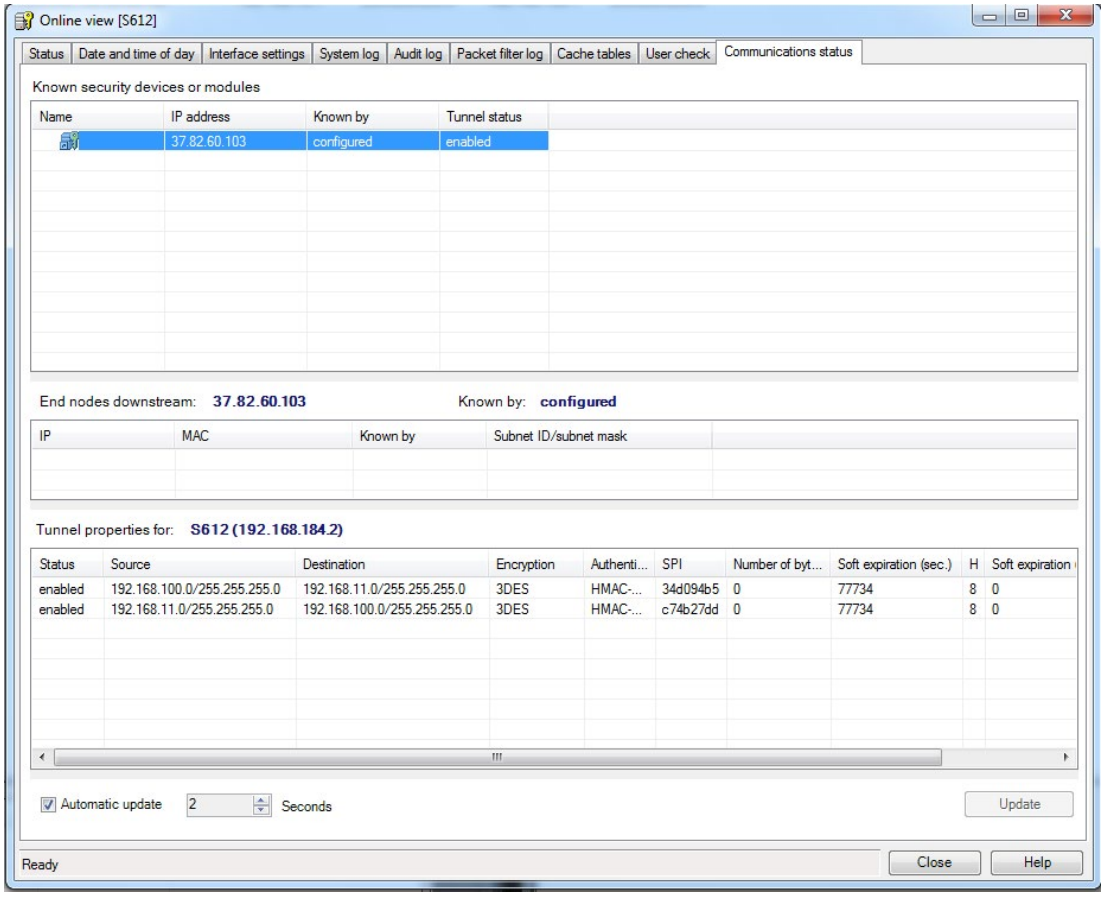
Result

The SCALANCE M-800 establishes the VPN tunnel to the 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.



1.4 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.

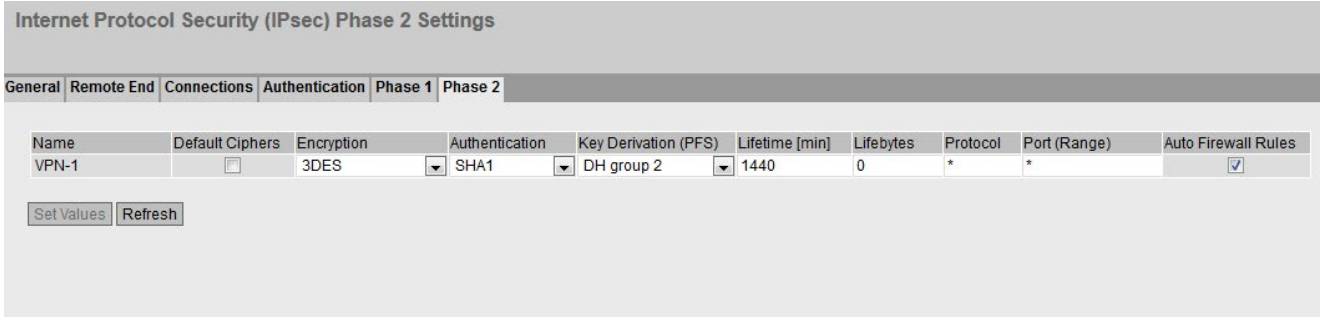
1.4.1 Creating firewall rules automatically

For the example, the VPN tunnel described in the section "Secure VPN tunnel with certificates (Page 62)" is used. The devices have the following IP address setting:

		Internal address
Local area network	SCALANCE M-800	192.168.100.1 255.255.255.0
Remote network	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 setting "Auto Firewall Rules" is enabled as default.



Result

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

Action	From / to	Permitted protocols	For	Source IP addresses	Dest. IP addresses
Allow	Internal network (VLAN1) / remote network (IPsec tunnel x)	All services	all ports or all ICMP packet types	192.168.100.0/24	192.168.11.0/24
Allow	Remote network (IPsec tunnel x) / internal network (VLAN1)	All services	all ports or all ICMP packet types	192.168.11.0/24	192.168.100.0/24

These firewall rules make data exchange between the internal network and the remote network possible, however it is not possible for remote clients to reach the modem although they also belong to the tunnel subnet.

Apart from ICMP Echo Request no access to the remote VPN partner.

See also

Creating firewall rules manually (Page 45)

1.4.2 Creating firewall rules manually

Requirement

The IP service HTTP has been created, see the section "AUTOHOTSPOT".

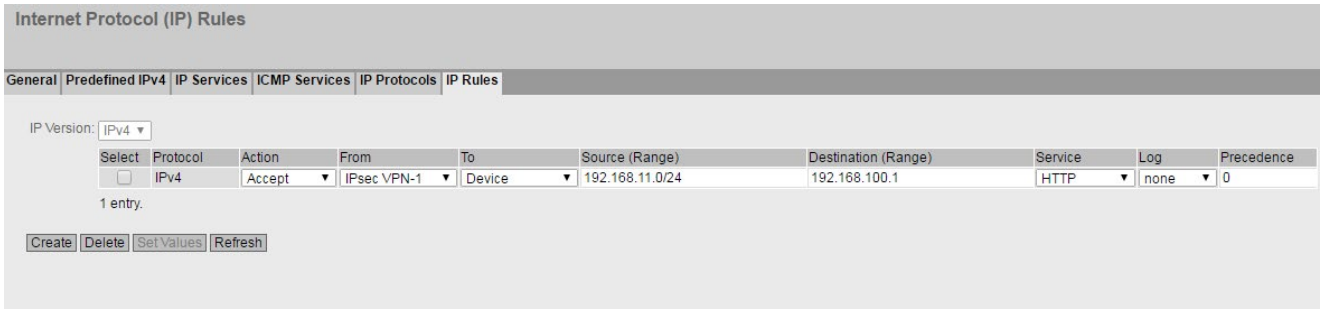
Allow all nodes from the remote subnet HTTP-based access to the SCALANCE M-800.

In the following example an additional firewall rules is specified, that applies in addition to the automatic firewall rules.

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 VPN-1
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 on "Set Values". The SCALANCE M can be reached through the VPN tunnel and can be configured with WBM.



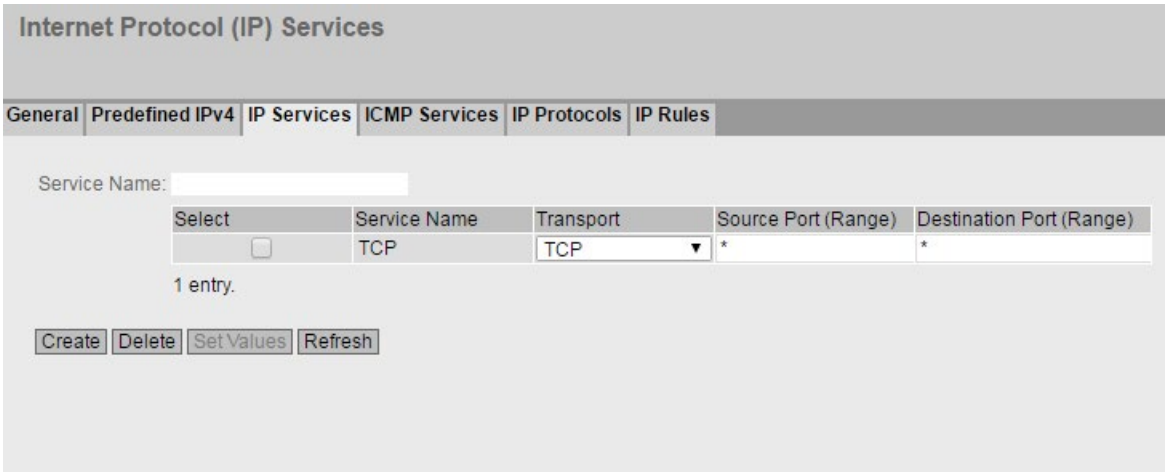
Allow HTTP-based access through the VPN tunnel for a specific device

In the following example, a firewall rule is specified manually, the automatic firewall rules are deactivated.

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:

Transportation	TCP

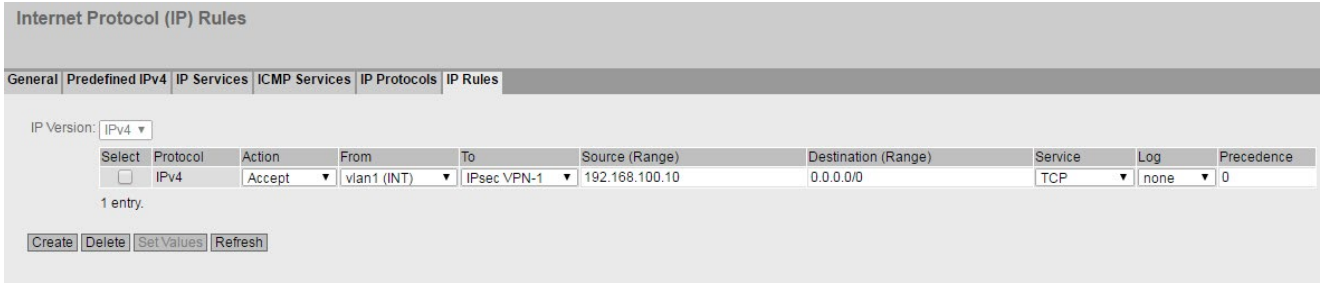
4. Click on "Set Values".



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	vlan1 (INT)
To	IPsec VPN-1
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

8. Click "Create". A new entry is created in the table.
9. Click on "Set Values".



VPN tunnel between SCALANCE M-800 and security CPs

2

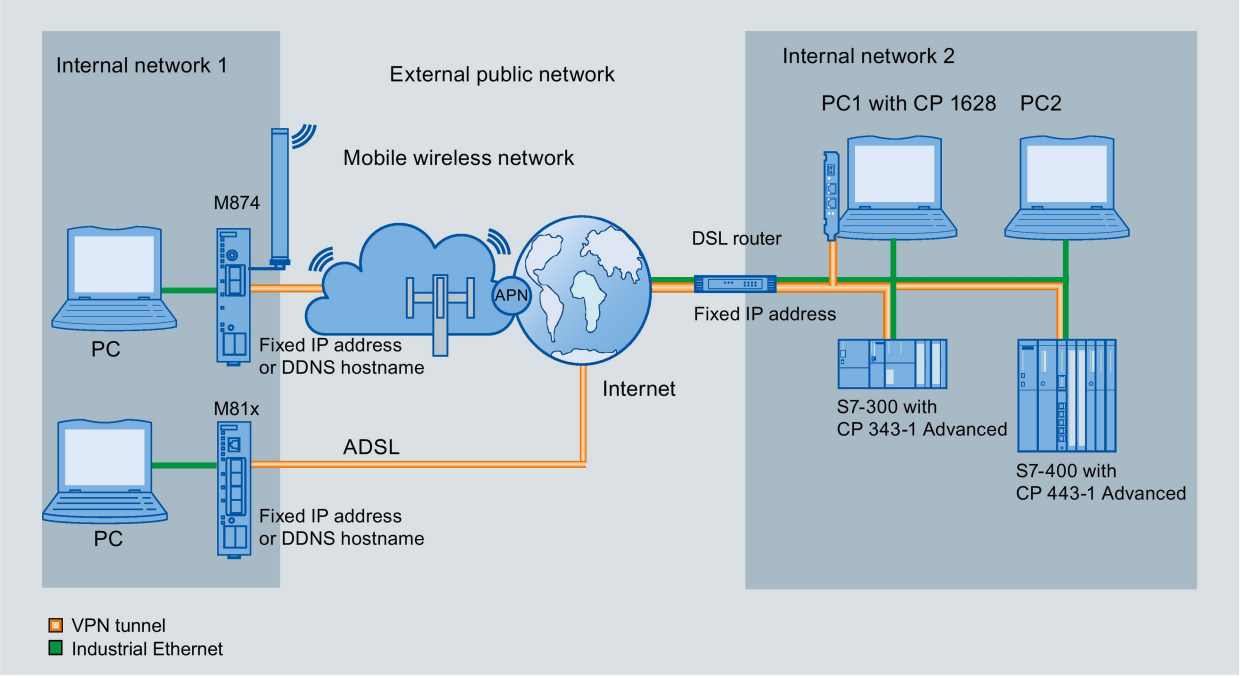
2.1 Procedure in principle

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 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".
- 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
2. Configuring a tunnel connection
3. Downloading the configuration to the CP and saving the M-800 configuration

Configuring a VPN tunnel with the SCT V4.x

1. Creating project and modules with SCT (Page 51)
2. Configuring a tunnel connection (Page 53)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 55)

Configuring SCALANCE M-800

1. Activating VPN (Page 60)
2. Configuring the VPN remote end (Page 55)
3. Configuring a VPN connection (Page 56)
4. Configuring VPN authentication (Page 58)
5. Configuring phase 1 and phase 2 (Page 58)
6. Establishing the VPN connection (Page 60)

Example 2: Secure VPN tunnel with certificates

Configuring a VPN tunnel with the SCT V3.x

1. Creating project and modules with SCT
2. Configuring a tunnel connection
3. Downloading the configuration to the CP and saving the M-800 configuration

Configuring a VPN tunnel with the SCT V3.x

1. Creating project and modules with SCT (Page 62)
2. Configuring a tunnel connection (Page 64)
3. Downloading the configuration to the CP and saving the M-800 configuration (Page 66)

Configuring SCALANCE M-800

1. Loading a certificate (Page 67)
2. Activating VPN (Page 72)
3. Configuring the VPN remote end (Page 69)
4. Configuring a VPN connection (Page 69)
5. Configuring VPN authentication (Page 70)
6. Configuring phase 1 and phase 2 (Page 71)
7. Establishing the VPN connection (Page 73)

2.2 Secure VPN tunnel with PSK

2.2.1 Configuring a VPN tunnel with the SCT V4.x

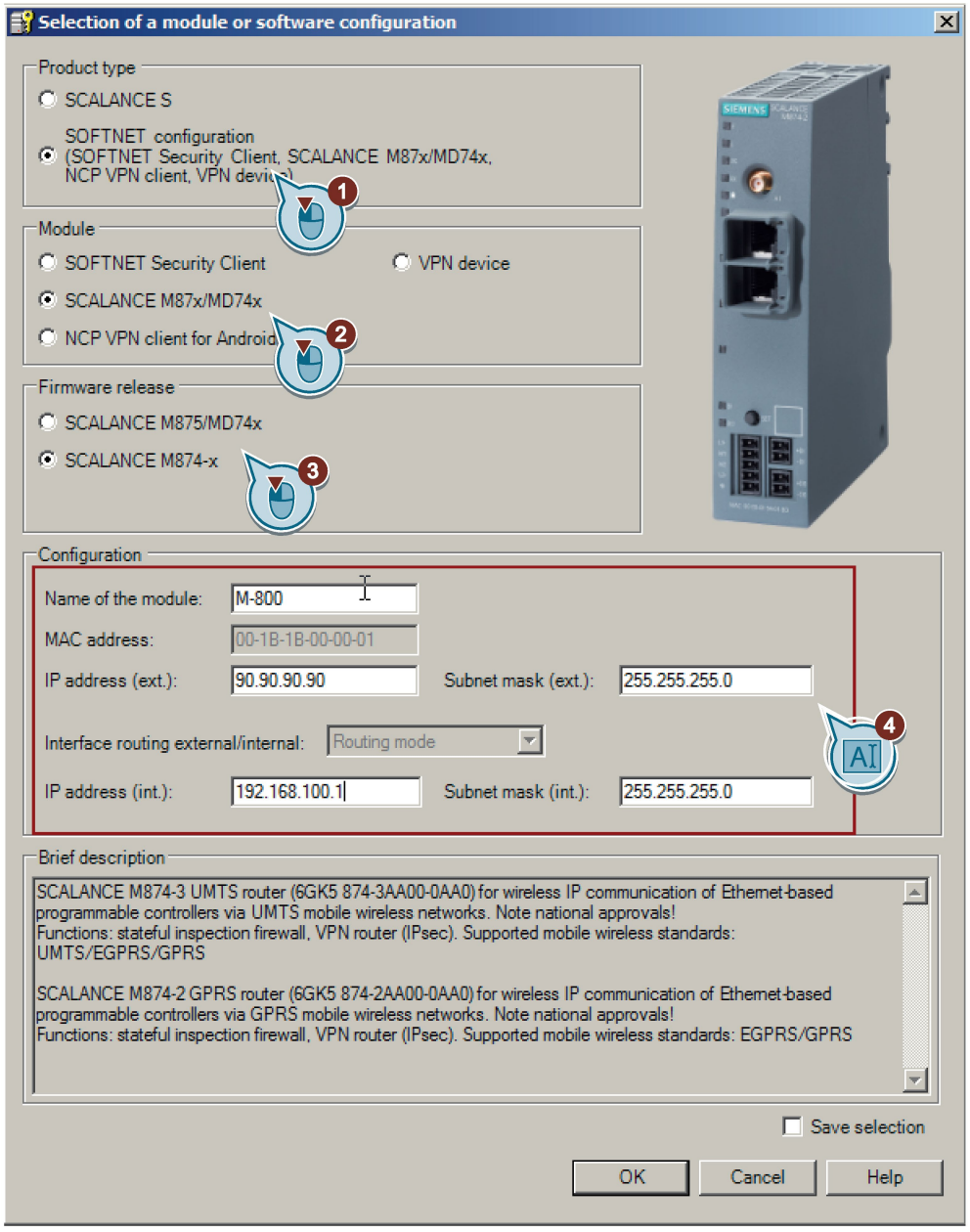
2.2.1.1 Creating project and modules with SCT

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 47)" 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.

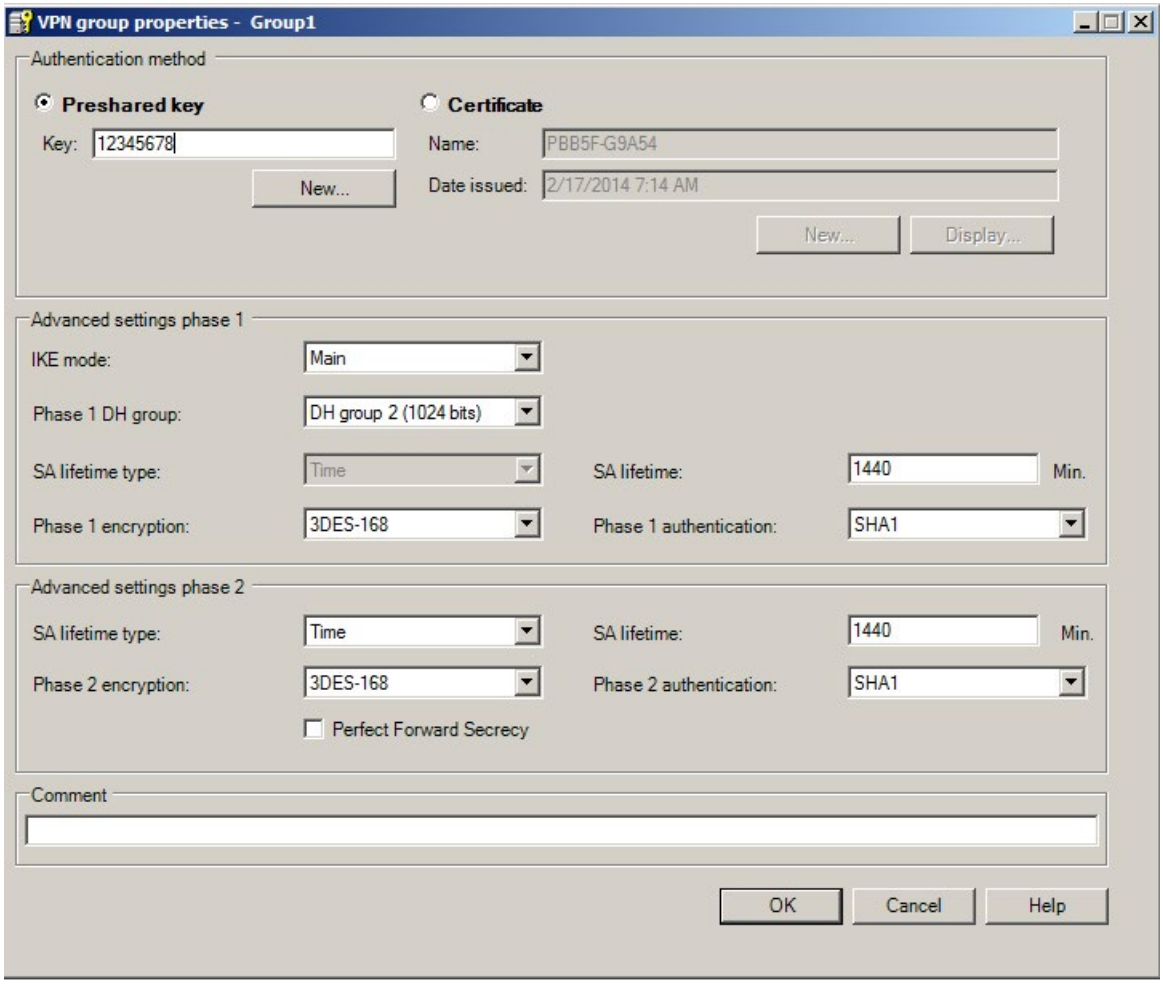
2.2.1.2 Configuring a tunnel connection

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 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.

2.2.1.3 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. Follow the instructions in the configuration file.

2.2.2 Configuring SCALANCE M-800

2.2.2.1 Configuring the VPN remote end

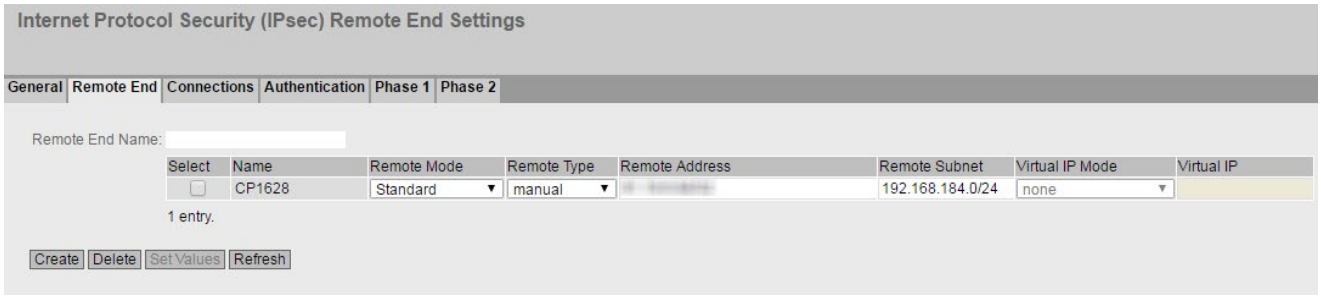
Procedure

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

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

5. Click on "Set Values".



2.2.2.2 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

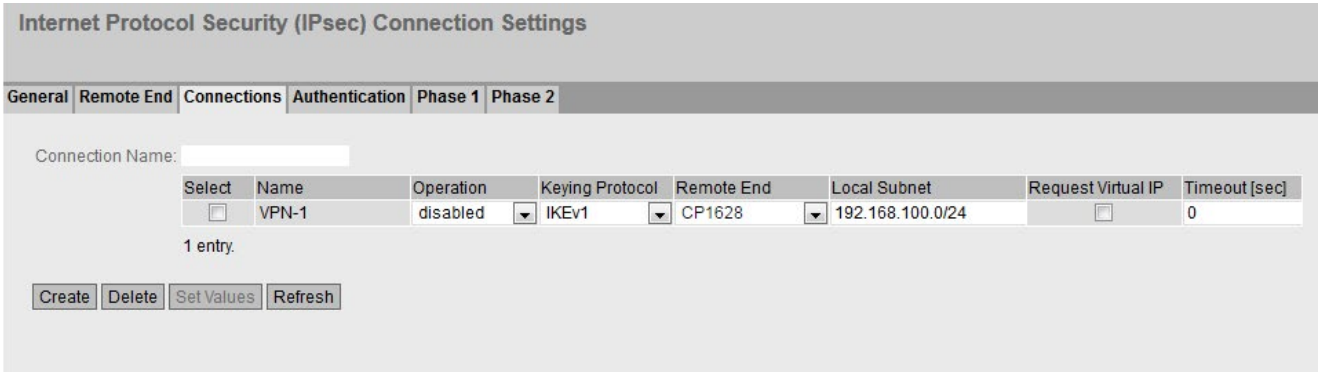
Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" 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 subnet 1 in CIDR notation.

5. Click on "Set Values".



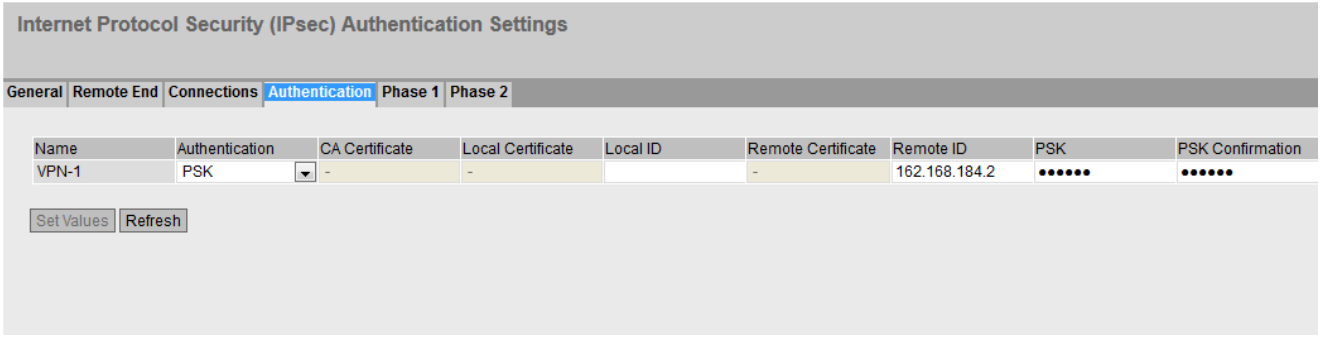
2.2.2.3 Configuring VPN authentication

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 on "Set Values".



2.2.2.4 Configuring phase 1 and phase 2

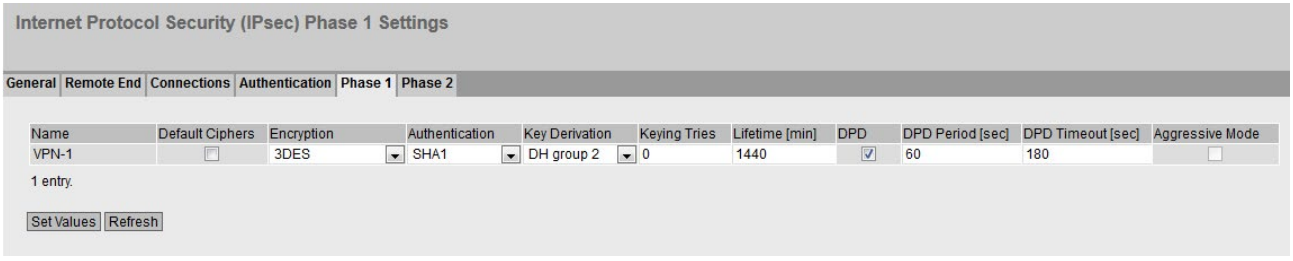
Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.

4. Configure phase 1 with the following settings from the configuration file:

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

5. Click on "Set Values".

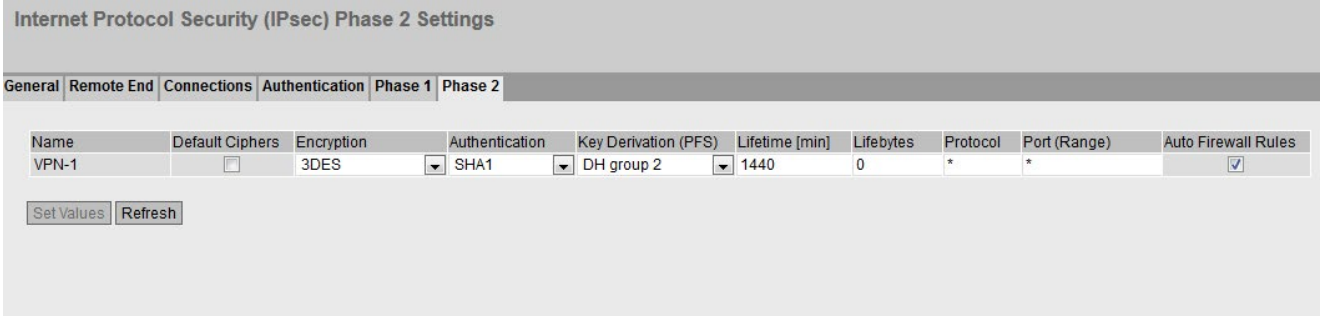


Configuring phase 2

1. Click the "Phase 2" tab.
2. Deselect the "Default Ciphers" check box.
3. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
Key Derivation (DFS)	DH group 2
Lifetime [min]:	1440

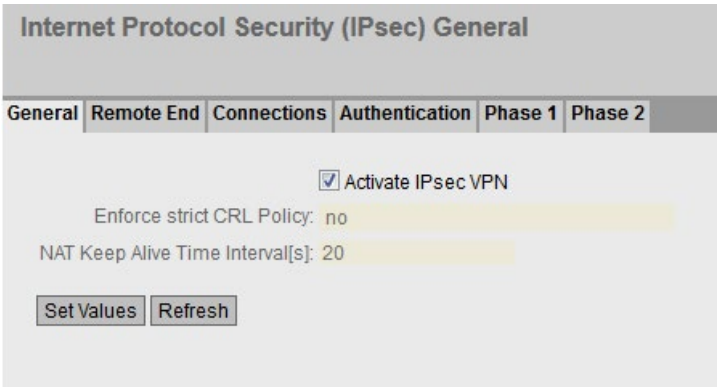
4. Click on "Set Values".



2.2.2.5 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.

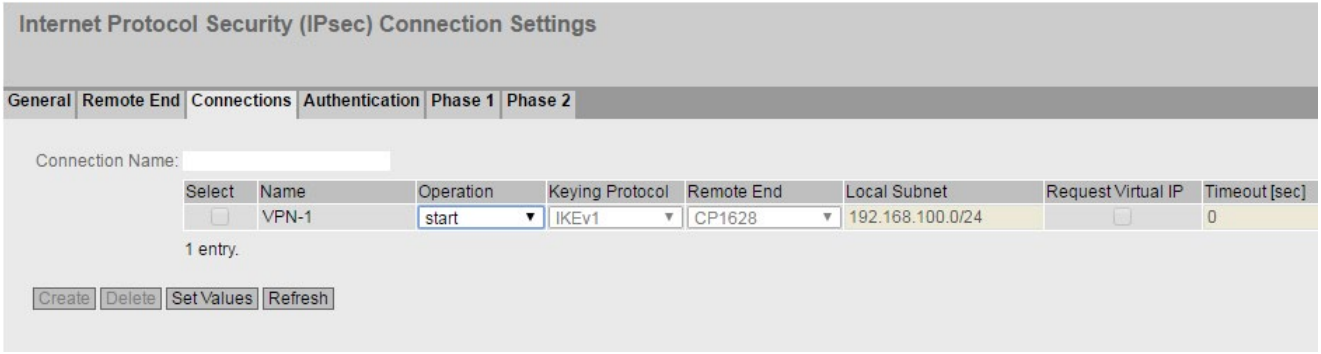


3. Click on "Set Values".

2.2.2.6 Establishing the VPN connection

Procedure

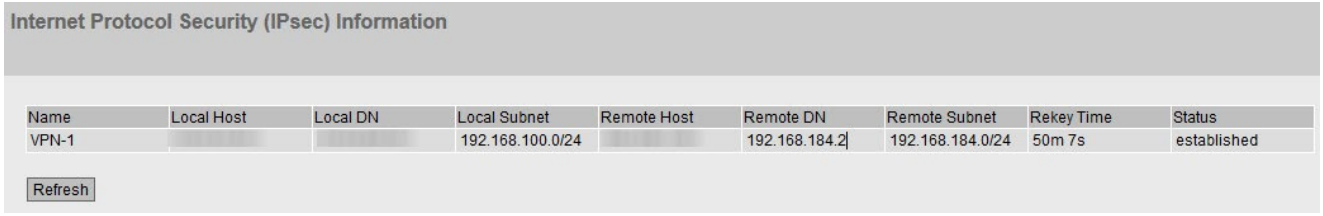
1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" tab in the content area.
2. As "Operation", select "Start" and click "Set Values".



Result

The M-800 establishes the VPN tunnel to the CP 128. If the VPN tunnel is established, the LED is lit green on the device.

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



2.3 Secure VPN tunnel with certificates

2.3.1 Configuring a VPN tunnel with the SCT V4.x

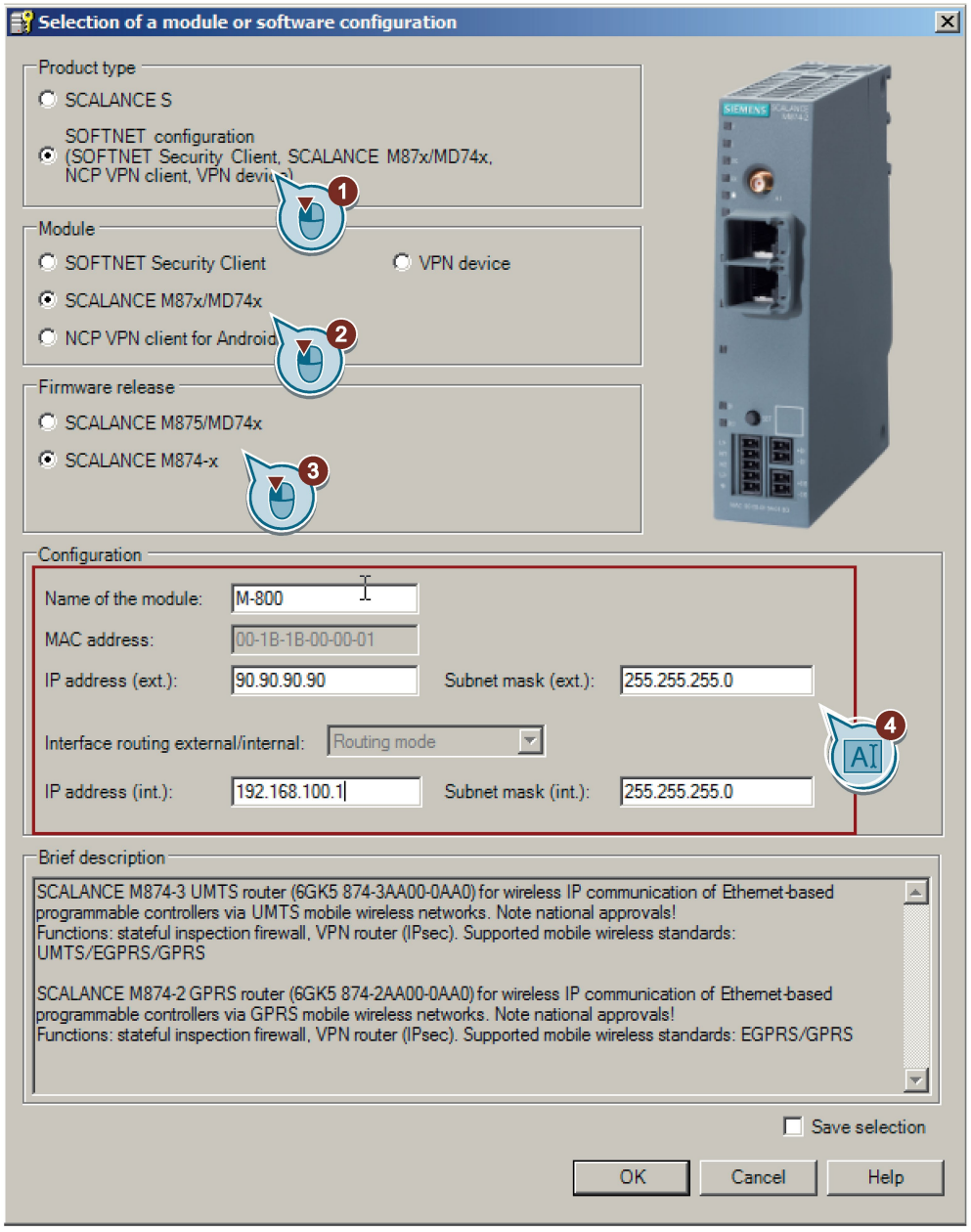
2.3.1.1 Creating project and modules with SCT

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 47)" 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.

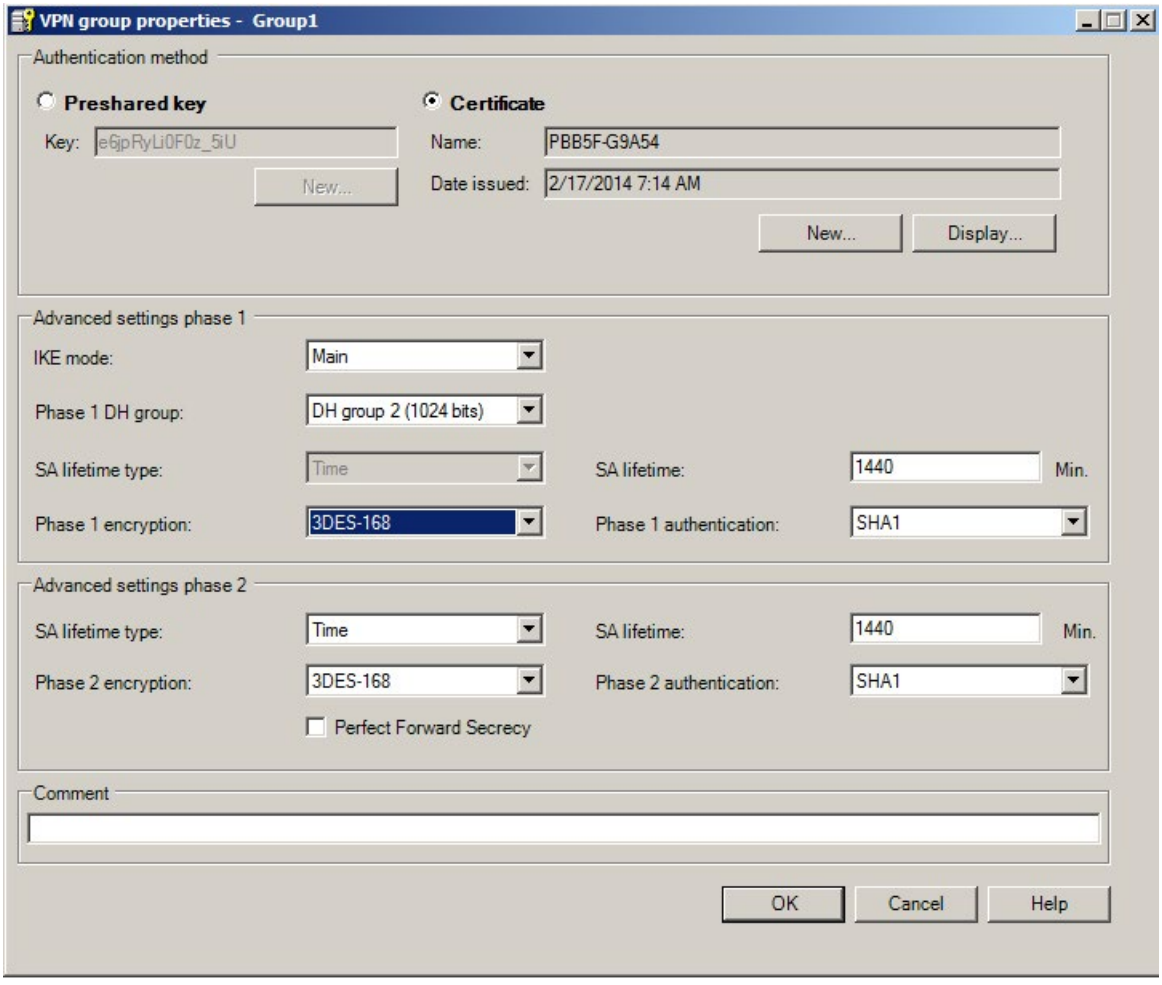
2.3.1.2 Configuring a tunnel connection

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.

2.3.1.3 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-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.

2.3.2 Configuring SCALANCE M-800 (*** NO TRANSLATION IN THIS VERSION! ***)

2.3.2.1 Loading a certificate

Requirement

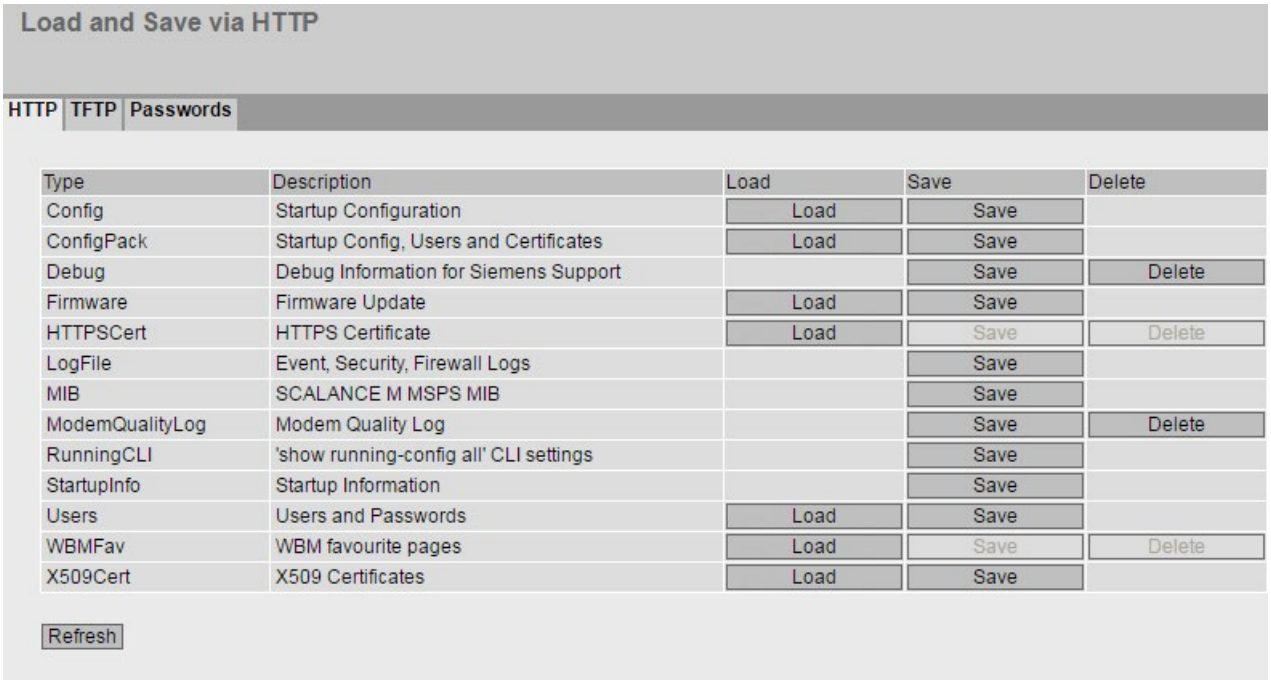
- The correct time is set on the SCALANCE M-800, refer to the section AUTOHOTSPOT.
- Certificates are available.

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

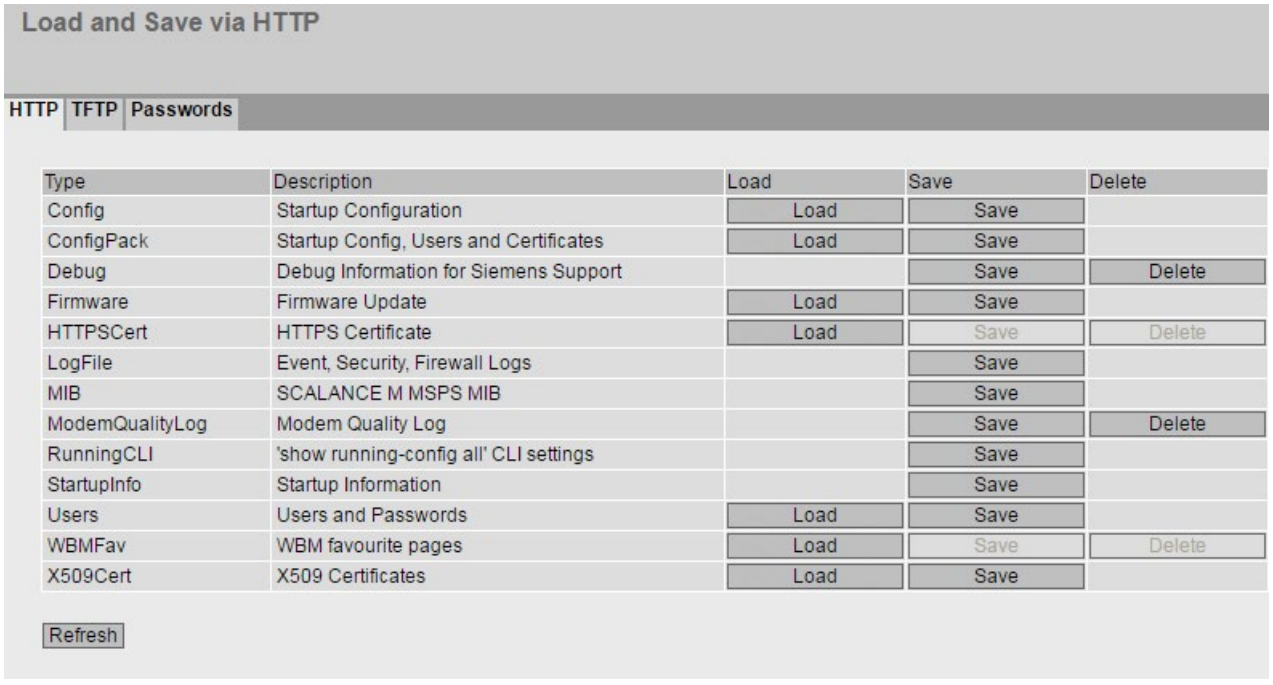
  Transfer the certificates for the SCALANCE M-800 to the Admin PC.

Procedure

1. Click on "System" > "Load&Save" in the navigation area and on the "Passwords"" tab in the content area.
2. In the line "X509Cert" enter the password that you specified for the PKCS12 file in "Password" and "Password confirmation".
3. Enable the password
4. Click on "Set Values".



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



6. For "X509Cert" click the "Loading" button. The dialog for loading a file is opened.

   Navigate to the remote certificate.

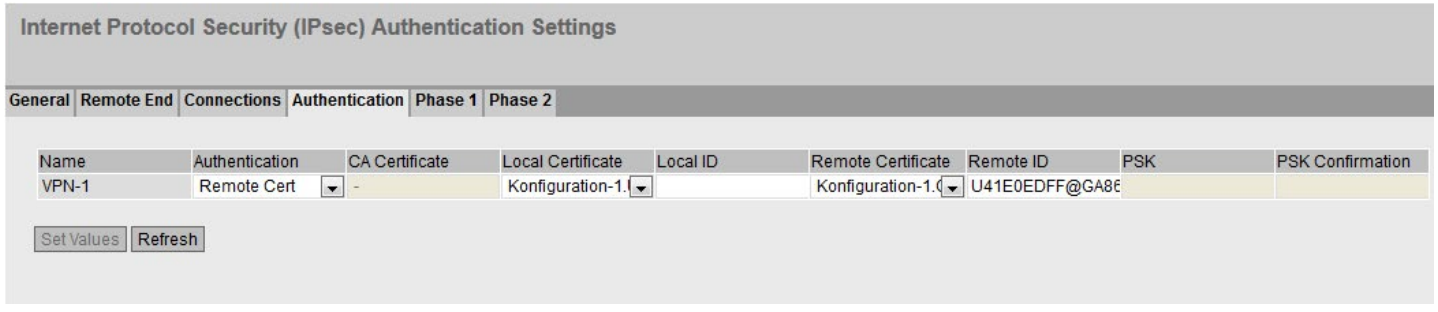
7. Click the "Open" button in the dialog.

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

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

Result

Certificates are loaded and are displayed in "Security" > "Certificates". The loaded certificates must have the status "Valid".



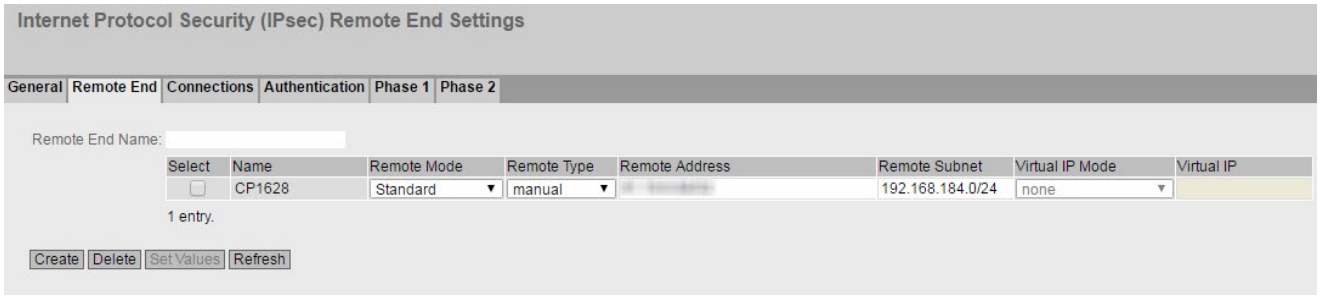
2.3.2.2 Configuring the VPN remote end

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

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

5. Click on "Set Values".



2.3.2.3 Configuring a VPN connection

Requirement

- The VPN remote end has been created.

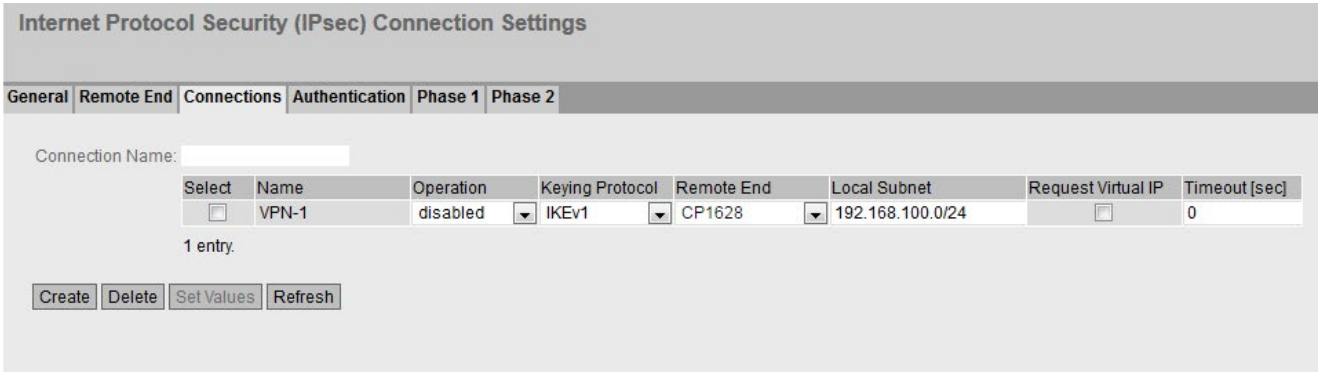
Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" 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 subnet 1 in CIDR notation.

5. Click on "Set Values".



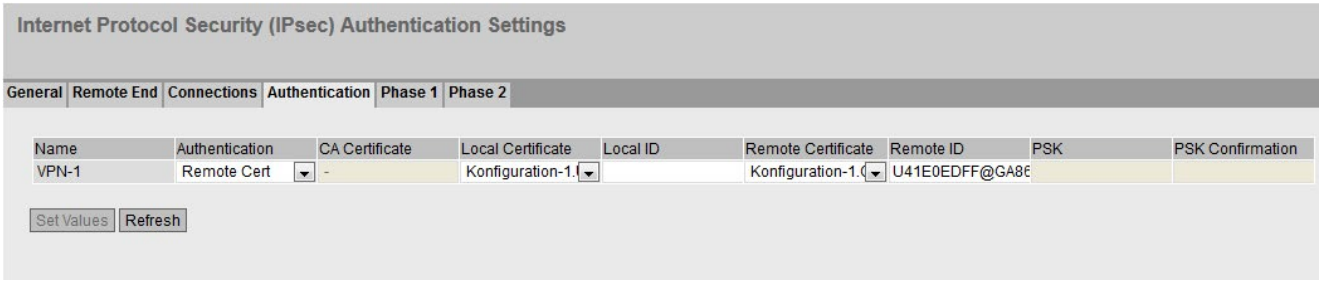
2.3.2.4 Configuring VPN authentication

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Authentication" tab in the content area.
2. 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 on "Set Values".



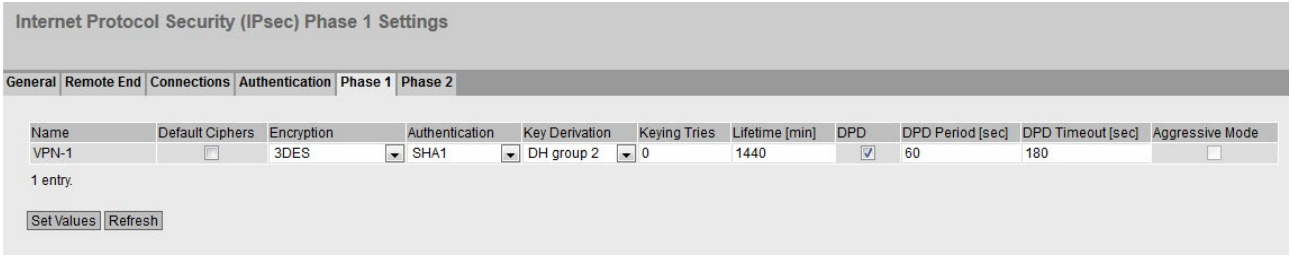
2.3.2.5 Configuring phase 1 and phase 2

Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.
4. Configure phase 1 with the following settings from the configuration file:

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

5. Click on "Set Values".

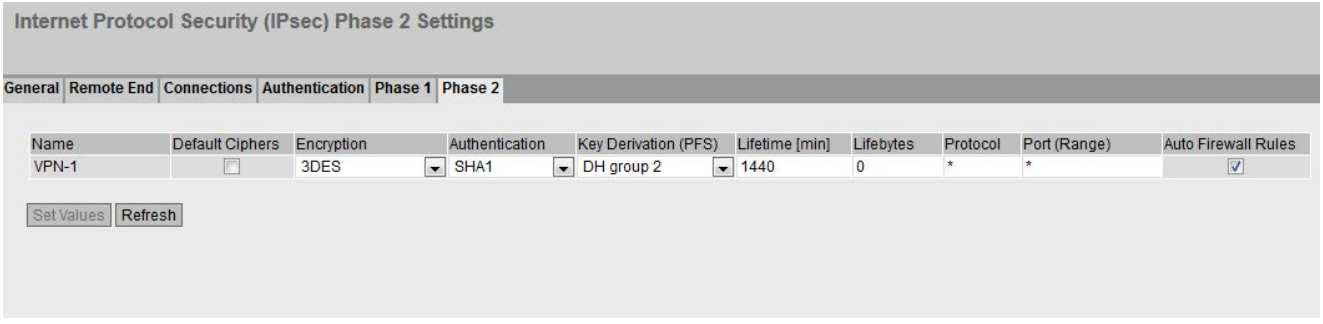


Configuring phase 2

1. Click the "Phase 2" tab.
2. Deselect the "Default Ciphers" check box.
3. Configure phase 2 with the following settings from the configuration file:

Encryption	3DES
Authentication	SHA1
Key Derivation (DFS)	DH group 2
Lifetime [min]:	1440

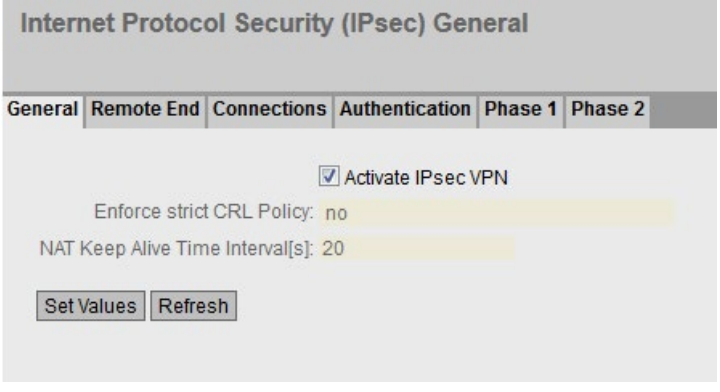
4. Click on "Set Values".



2.3.2.6 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.

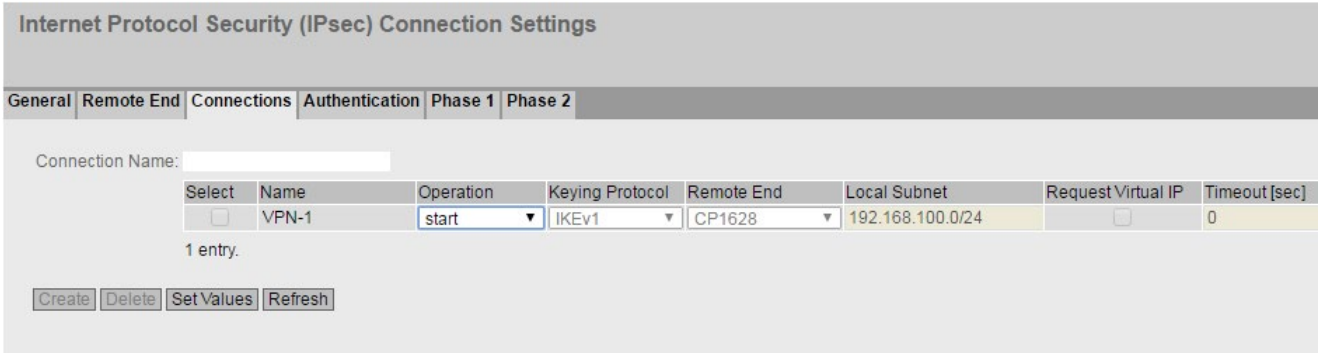


3. Click on "Set Values".

2.3.2.7 Establishing the VPN connection

Procedure

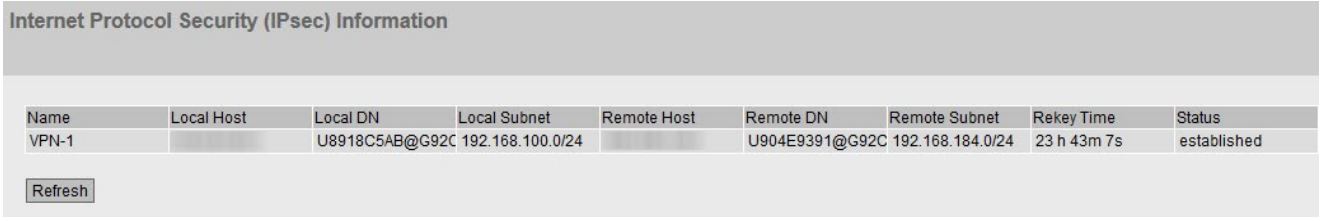
1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" tab in the content area.
2. As "Operation", select "Start" and click "Set Values".



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 two M-800s

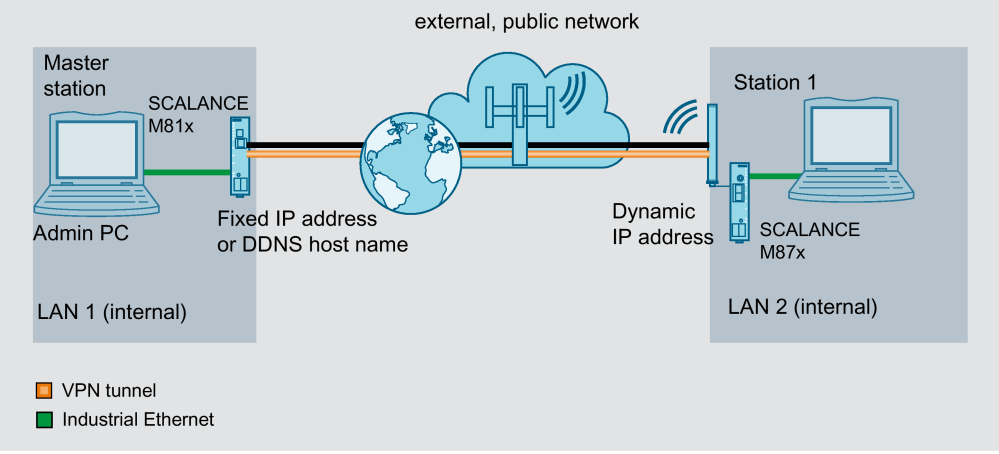
3

3.1 Procedure in principle

In this example a secure VPN connection with certificates is established between two SCALANCE M-800 devices.

In this example of a configuration the SCALANCE M81x in the master station is the VPN server and this can be reached from the WAN via its fixed IP address. The SCALANCE M87x in the station is the VPN client that establishes the connection to the VPN server when necessary.

Layout



Internal network 1 / 2 - connection to SCALANCE M

- In the test setup in the internal network, a network node is implemented by an Admin PC or SIMATIC station connected to an Ethernet interface of the SCALANCE M-800.
  - Admin PC: Represents a node in the internal network
  - M87x\M81x: 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.
  - Wired via the RJ-45 jack of the M81x to ADSL.

Required devices/components

Use the following components to set up the network:

- 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 which the SCALANCE M is connected.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Settings used

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

		Interface		IP address
Master station	M81x	ADSL (external)	Vlan 2	Fixed IP address, e.g. 90.90.90.90 (VPN server) Provider dependent As an alternative, the DDNS hostname can also be used.
		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	M87x	Mobile wireless (external)	Vlan 2	Dynamic IP address (VPN client)
		Ethernet (internal)	Vlan 1	192.168.11.2 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.11.40 255.255.255.0

Note

For the devices located in the internal network, the IP address of the internal port must be entered as the standard gateway.

Requirement

- The SCALANCE M87x/SCALANCE M81x is connected to the WAN, refer to "Connecting SCALANCE M to the WAN".
- The SCALANCE M87x/SCALANCE M81x can be reached via the Admin PC and you are logged in to the WBM as "admin".
- The "Security Configuration Tool V4.x" is installed

Steps in configuration

1. Configuring a VPN tunnel with the SCT
   - Creating the project and modules (Page 78)
   - Configuring a tunnel connection (Page 81)
   - Configuring VPN parameters (Page 83)
   - Saving the M-800 configuration (Page 84)
2. Configuring the SCALANCE M81x (VPN server)
   - Loading a certificate (Page 85)
   - Configuring the VPN remote end (Page 87)
   - Configuring a VPN connection (Page 88)
   - Configuring VPN authentication (Page 89)
   - Configuring phase 1 and phase 2 (Page 90)
   - Activating VPN (Page 91)
   - Establishing the VPN connection (Page 92)
3. Configuring the SCALANCE M87x (VPN client)
   - Loading a certificate (Page 93)
   - Configuring the VPN remote end (Page 95)
   - Configuring a VPN connection (Page 96)
   - Configuring VPN authentication (Page 97)
   - Configuring phase 1 and phase 2 (Page 98)
   - Activating VPN (Page 100)
   - Establishing the VPN connection (Page 100)
4. Displaying the status of the VPN connection (Page 101)

3.2 Configuring a VPN tunnel with the SCT

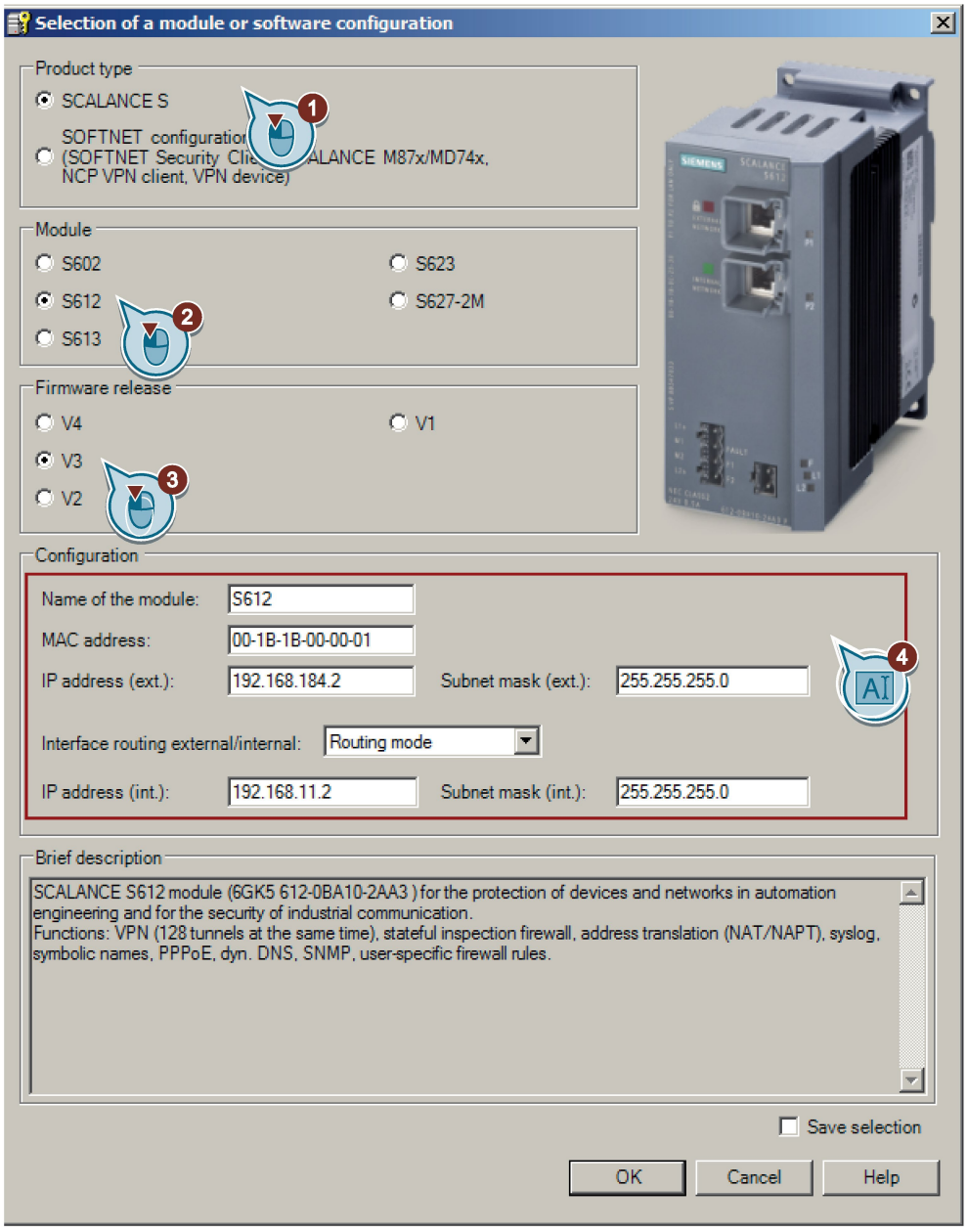
3.2.1 Creating the project and modules

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.

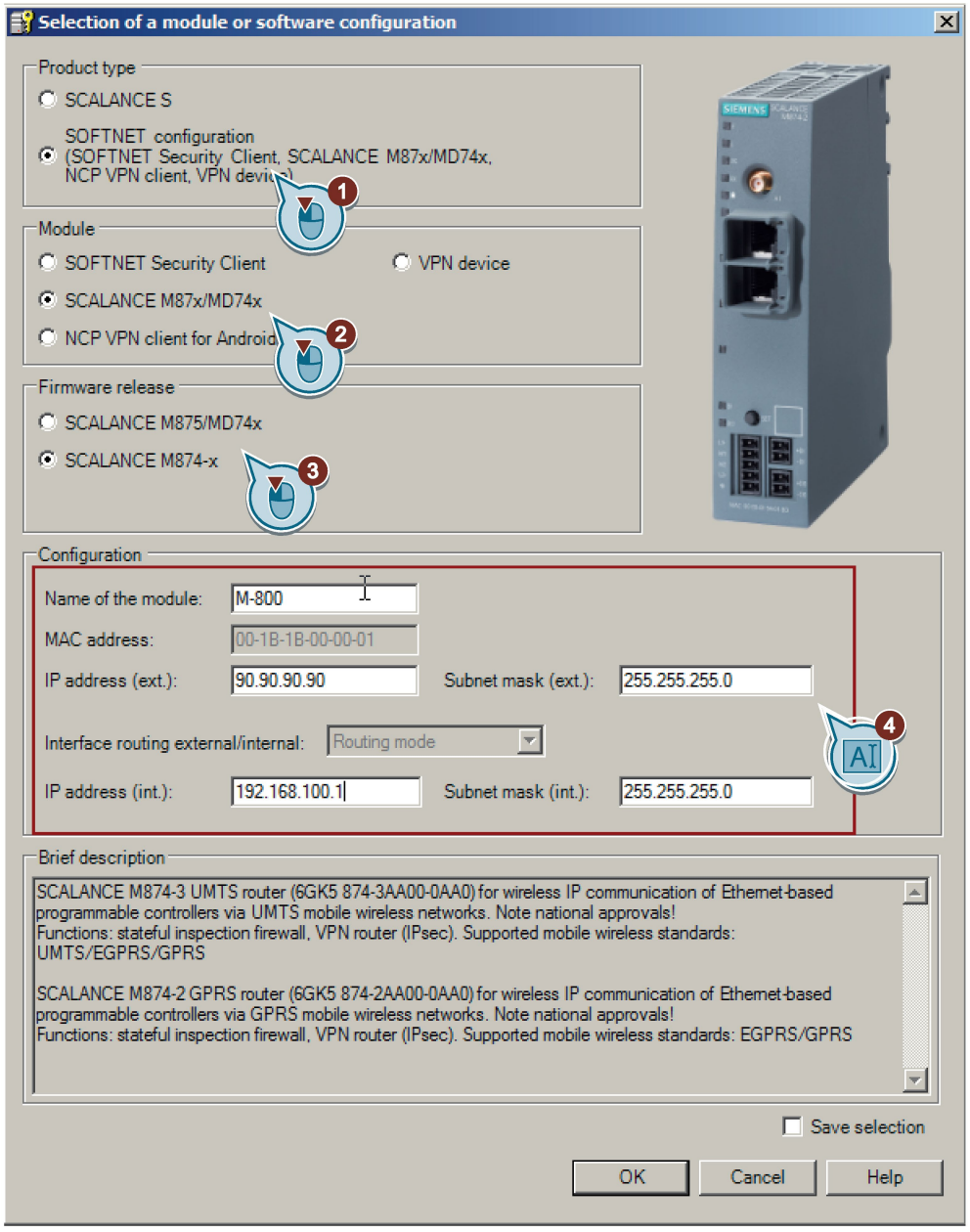
5. Enter the values assigned to the M87x from the "Settings used (Page 75)" table.

   With the M87x, the external IP address is not relevant. For the IP address (ext) use the default settings.



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

8. Enter the values assigned to the M81x from the "Settings used (Page 75)" table.



9. Close the dialog with "OK".

Result

The devices will then be displayed in the list of configured modules.

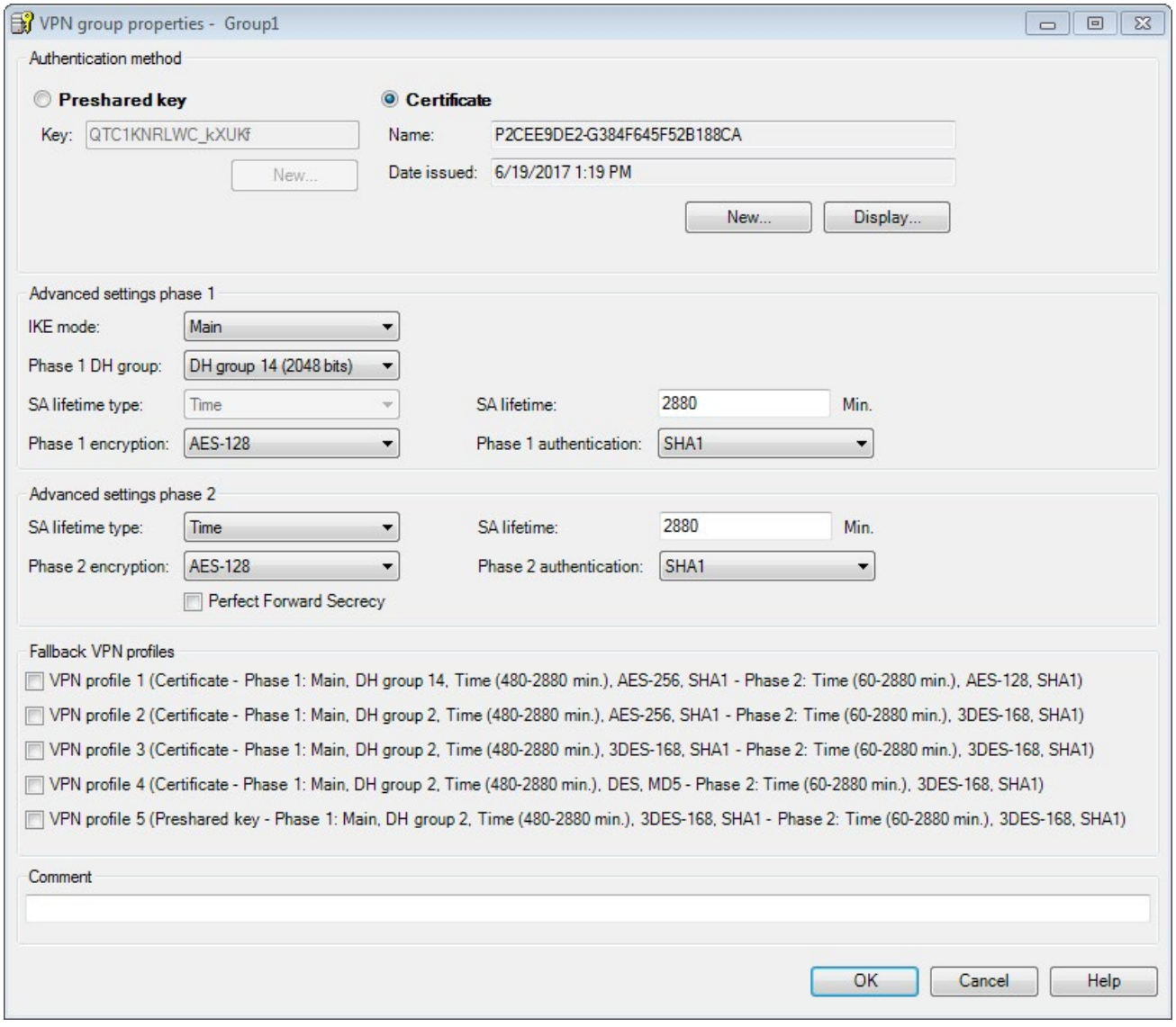
3.2.2 Configuring a tunnel connection

A VPN tunnel for secure communication can only be established if the SCALANCE M81x and the SCALANCE M87x 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 two entries 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.



7. Close the dialog with "OK".

Result

The configuration of the tunnel connection is complete.

3.2.3 Configuring VPN parameters

In this configuration example, the M81x (VPN server) is "passive". The M81x waits for the partner M87x to initiate the connection establishment.

Procedure

Configuring VPN parameters for M81x (VPN server)

1. Select the "M81xServer" in the content area.
2. Select the menu command "Edit" > "Properties". Click the "VPN" tab.
3. Click on the "VPN" tab.
4. For "Permission to initiate connection establishment", select the "Wait for partner (responder)" entry.
5. Enter the WAN IP address e.g. 90.90.90.90
6. Click "Apply" and close the dialog with "OK".

Configuring VPN parameters for M87x (VPN client)

1. Select the "M81xServer" in the content area.
2. Select the menu command "Edit" > "Properties". Click on the "VPN" tab.
3. Click on the "VPN" tab.
4. For "Permission to initiate connection establishment", select the "Start connection to partner (initiator/responder)" entry.
5. Click "Apply" and close the dialog with "OK".
6. 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.

3.2.4 Saving the configuration

Procedure

1. In the content area, select the "M81xServer" and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.M81xServer.txt" in your project folder and assign a password for the private key of the certificate, e.g. Di1S+Xo?.
3. In the content area, select the "M87xClient" and select the menu command "Transfer" > "To module(s) …".
4. Save the configuration file "Projectname.M87xClient.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: Project name of the module.txt
- PKCS12 file: Project name.string.name of the module.p12
- Remote certificate: Projectname.group1module name.cer

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

3.3 Configuring the SCALANCE M81x (VPN server)

3.3.1 Loading a certificate

The certificates are necessary to authenticate the VPN node and therefore for the establishment of a secure VPN connection.

You obtain the information which certificate is to be loaded on which device from the configuration file.

Requirement

- The correct time is set on the SCALANCE M-800, refer to the section AUTOHOTSPOT.
- Certificates are available.

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

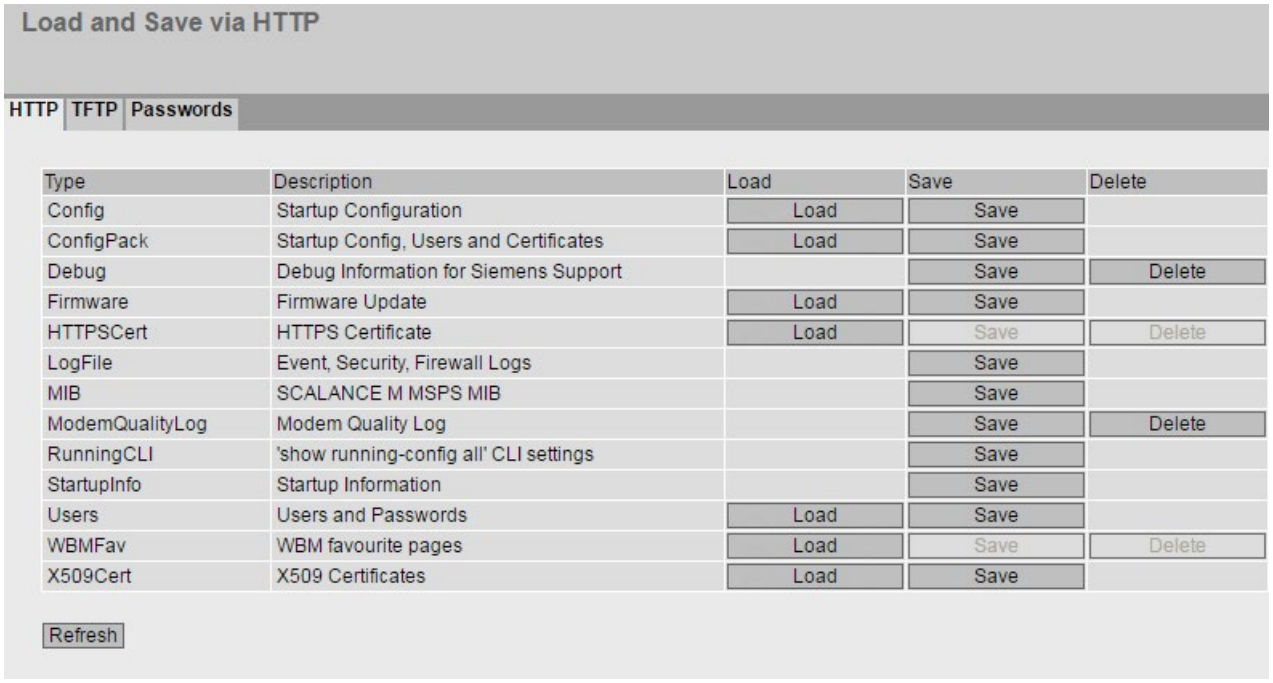
  Transfer the certificates for the SCALANCE M-800 to the Admin PC.

Procedure

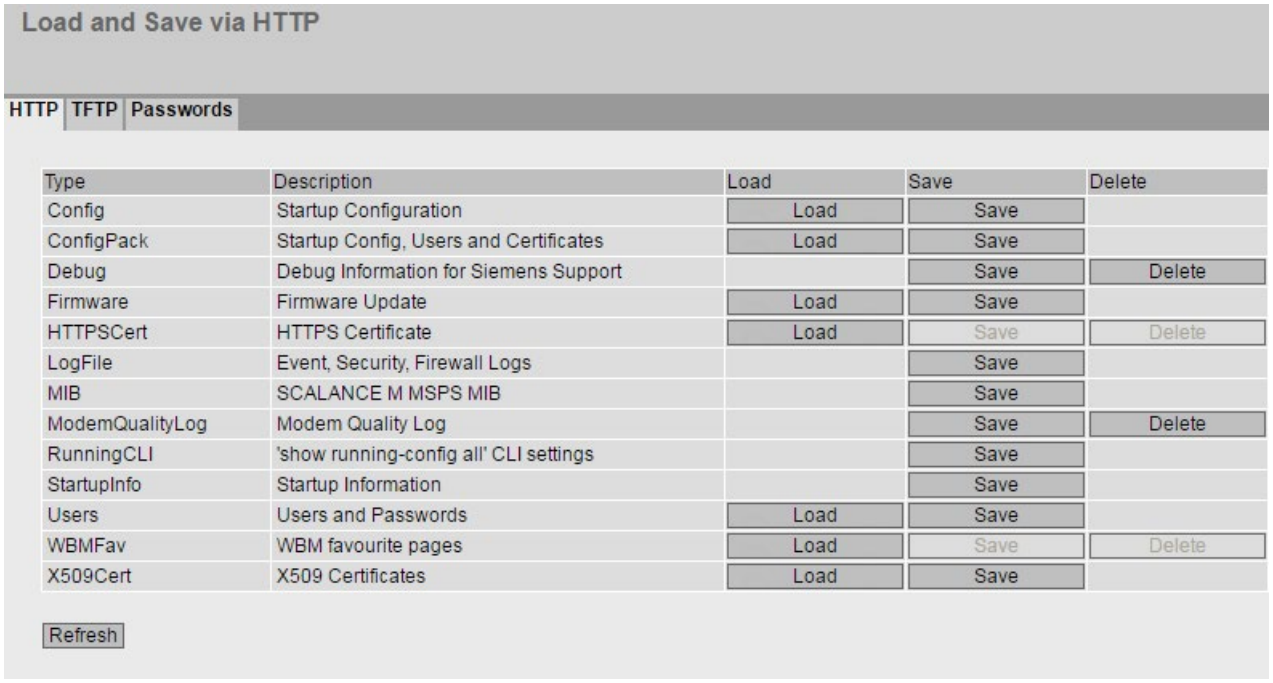
1. Click on "System" > "Load&Save" in the navigation area and on the "Passwords"" tab in the content area.
2. To load the file successfully on the SCALANCE M enter the password specified for the file in the line "X509Cert" in "Password" and "Password confirmation"

   When you saved the configuration files of the SCALANCE M from the Security Configuration Tool, you were requested to assign a password for the private key of the certificate or to use the project name for this.
3. Enable the password

4. Click on "Set Values".



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



6. For "X509Cert" click the "Loading" button. The dialog for loading a file is opened.

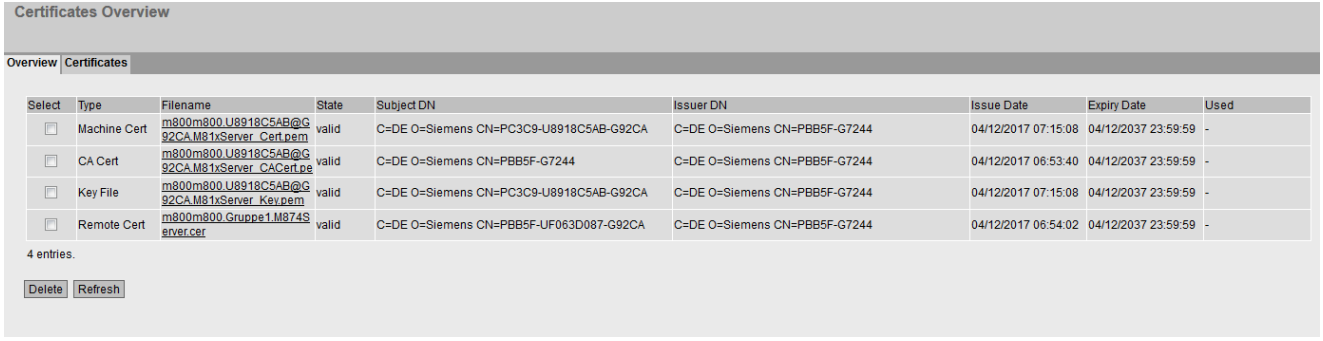
7. Click the "Open" button in the dialog.

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

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

Result

Certificates are loaded and are displayed in "Security" > "Certificates". The loaded certificates must have the status "Valid".



3.3.2 Configuring the VPN remote end

In this example of a configuration the M81x in the master station is the VPN server that accepts the connection of VPN partners with any IP address.

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. VPN_Client_M87x.
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 Type	Any Accepts the connection from VPN partners with any IP address address from the remote subnet.
Remote Subnet	192.168.11.0/24 The subnet that can be reached through the VPN tunnel

5. Click on "Set Values".

3.3.3 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 "Connections" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Configure the VPN connection with the following settings:

Operation	Disabled
Keying Protocol	IKEv2
Remote End	VPN_Client_M87x Name of the VPN remote station
Local Subnet	192.168.100.0/24 The local subnet 1 in CIDR notation.

4. Click on "Set Values".

3.3.4 Configuring VPN authentication

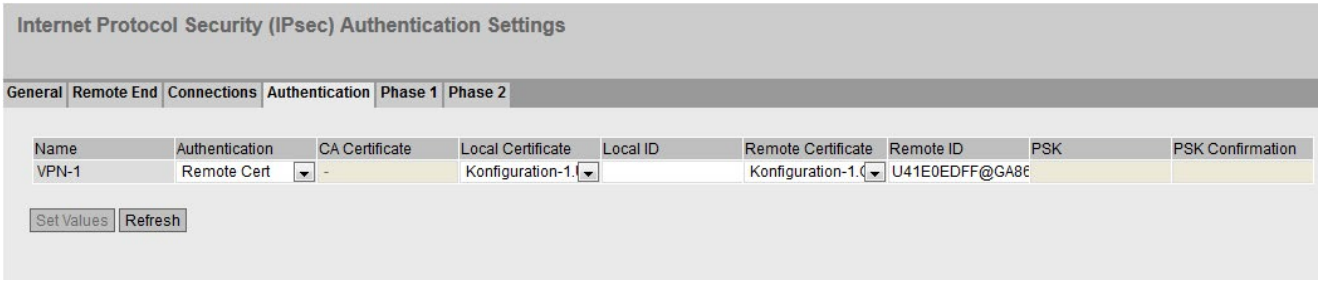
For secure communication via VPN, all VPN partners need to authenticate themselves with each other. In this configuration example, the certificate of the VPN remote station.

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	Remote Cert
Local certificate	The precise names of the certificates and the remote ID can be found in the relevant configuration file.
Remote Certificate	
Remote ID	

3. Click on "Set Values".



3.3.5 Configuring phase 1 and phase 2

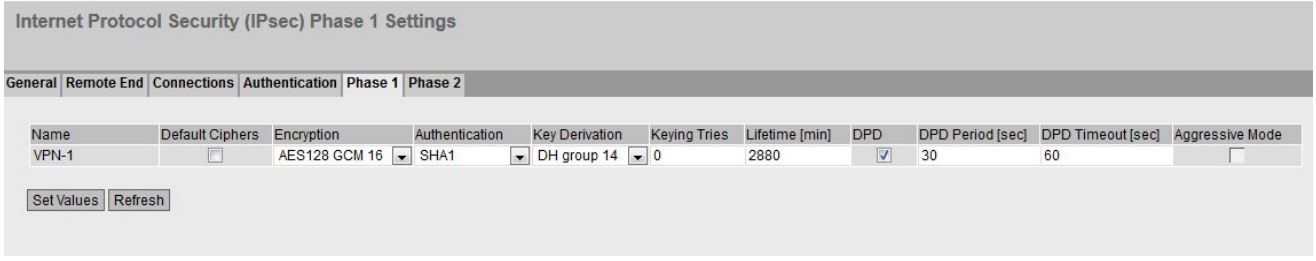
The settings must match on both devices.

Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.
4. Configure phase 1 with the following settings from the configuration file:

Encryption	AES 128
Authentication	SHA1
Key Derivation	DH group 14
Lifetime [min]:	2880
DPD Period [sec]	60
Aggressive Mode	no

5. Click on "Set Values".



Configuring phase 2

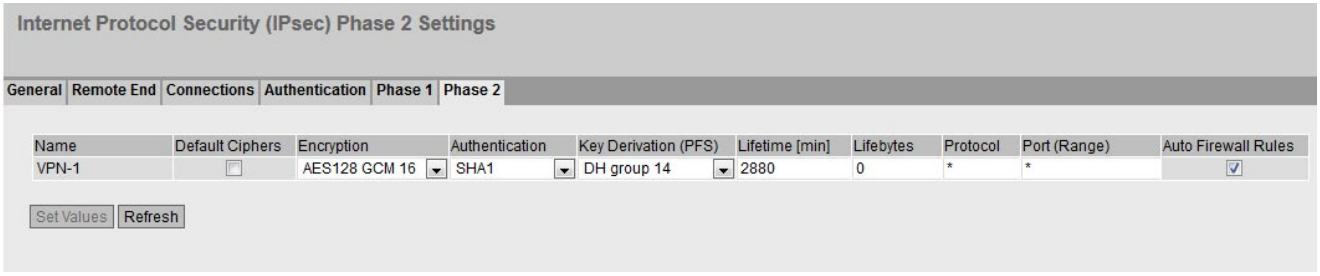
1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 2" tab in the content area.
2. Leave the "Default Ciphers" check box enabled.

   When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. The selection depends on the key exchange method.
3. Select the "DPD" check box.

4. Configure phase 1 with the following settings from the configuration file:

Encryption	AES128
Authentication	SHA1
Key Derivation	DH group 14
Lifetime [min]:	2880

5. Enable "Auto Firewall Rules" The firewall rule is created automatically for the VPN connection.

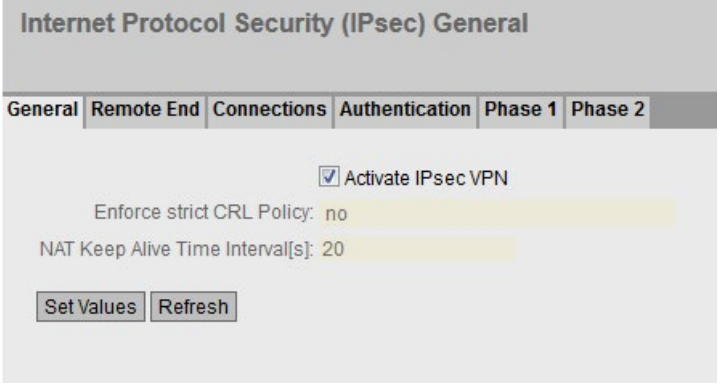


6. Click on "Set Values".

3.3.6 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.



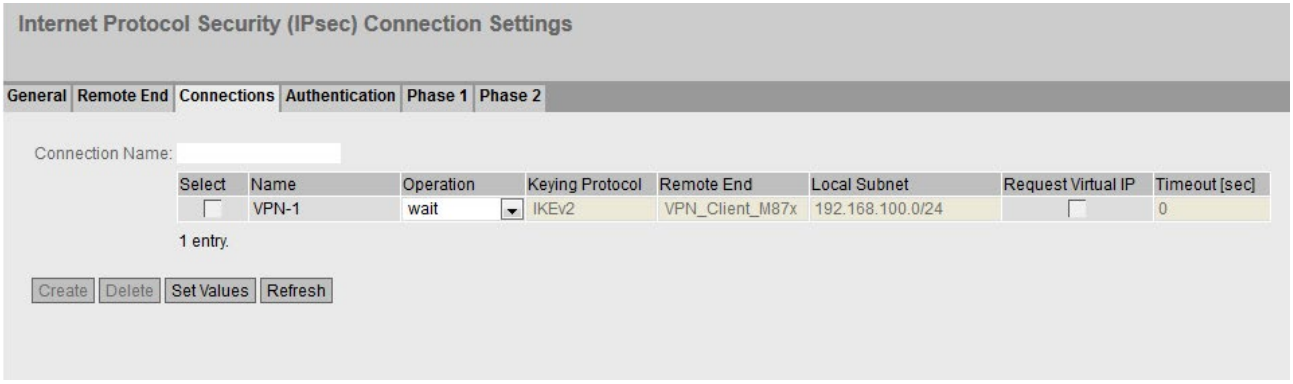
3. Click on "Set Values".

3.3.7 Establishing the VPN connection

The M81x (VPN server) is configured as the reponder.

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Connections" tab in the content area.
2. As "Operation", select "wait" and click "Set Values".



3.4 Configuring the SCALANCE M87x (VPN client)

3.4.1 Loading a certificate

The certificates are necessary to authenticate the VPN node and therefore for the establishment of a secure VPN connection.

You obtain the information which certificate is to be loaded on which device from the configuration file.

Requirement

- The correct time is set on the SCALANCE M-800, refer to the section AUTOHOTSPOT.
- Certificates are available.

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

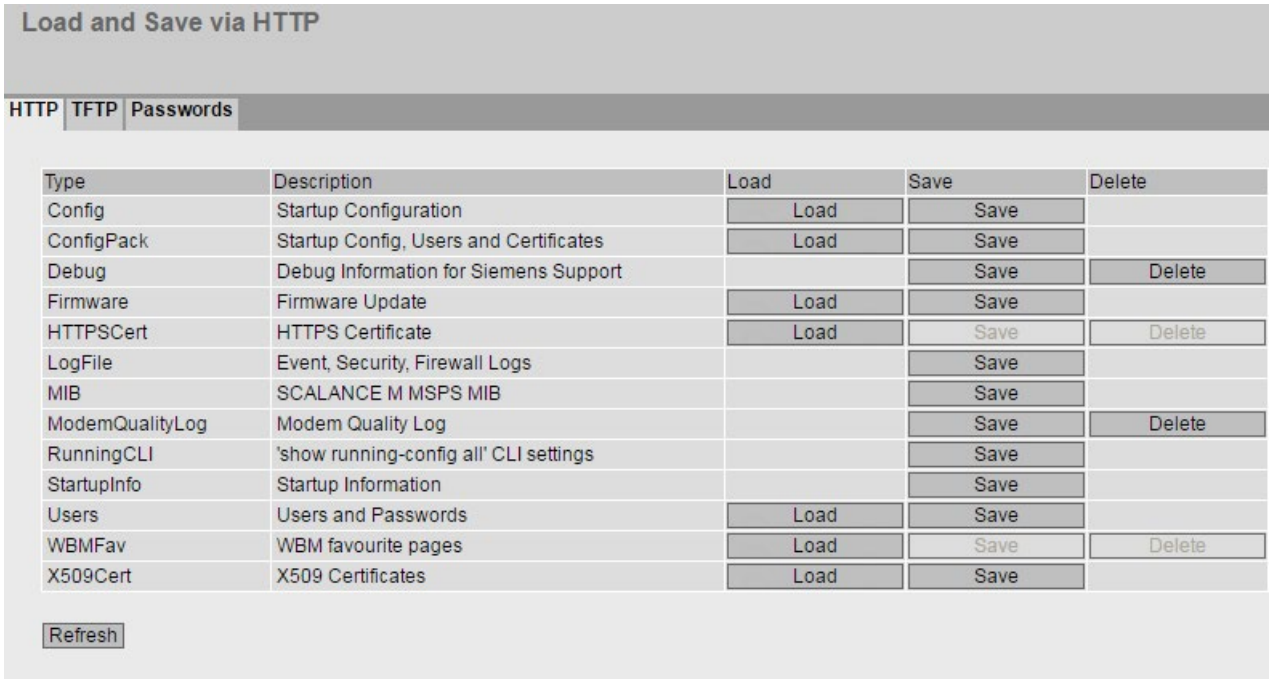
  Transfer the certificates for the SCALANCE M-800 to the Admin PC.

Procedure

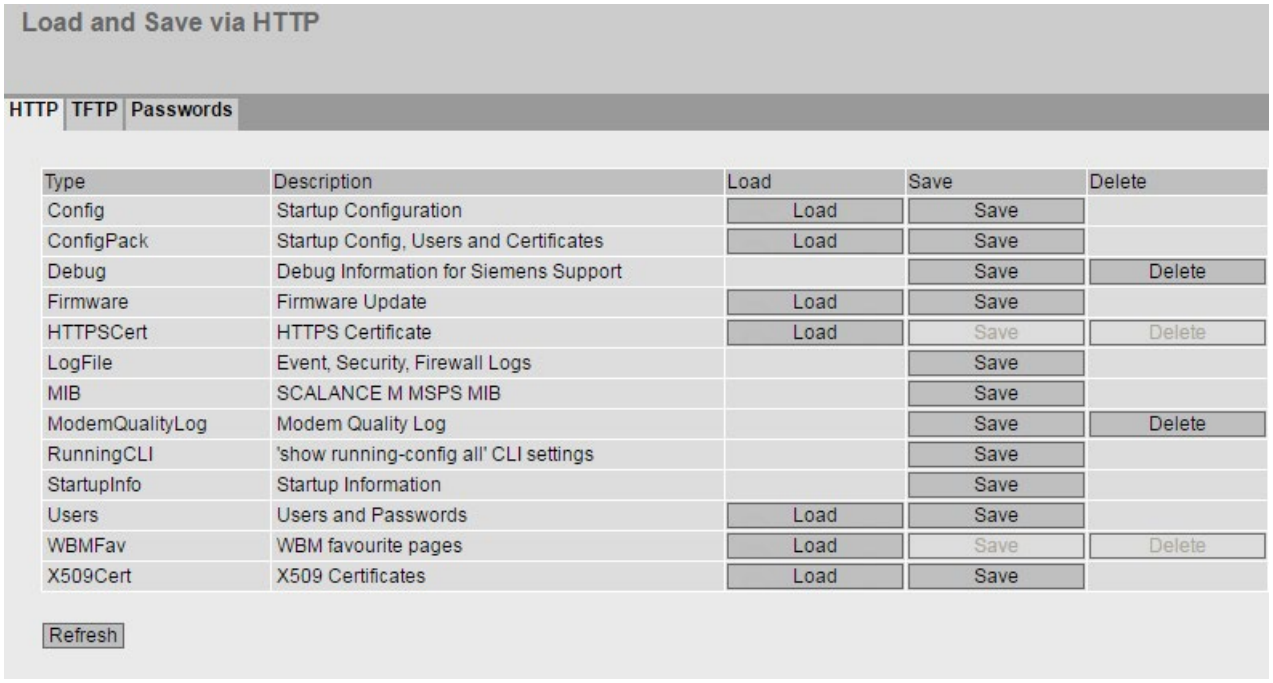
1. Click on "System" > "Load&Save" in the navigation area and on the "Passwords"" tab in the content area.
2. To load the file successfully on the SCALANCE M enter the password specified for the file in the line "X509Cert" in "Password" and "Password confirmation"

   When you saved the configuration files of the SCALANCE M from the Security Configuration Tool, you were requested to assign a password for the private key of the certificate or to use the project name for this.
3. Enable the password

4. Click on "Set Values".



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



6. For "X509Cert" click the "Loading" button. The dialog for loading a file is opened.

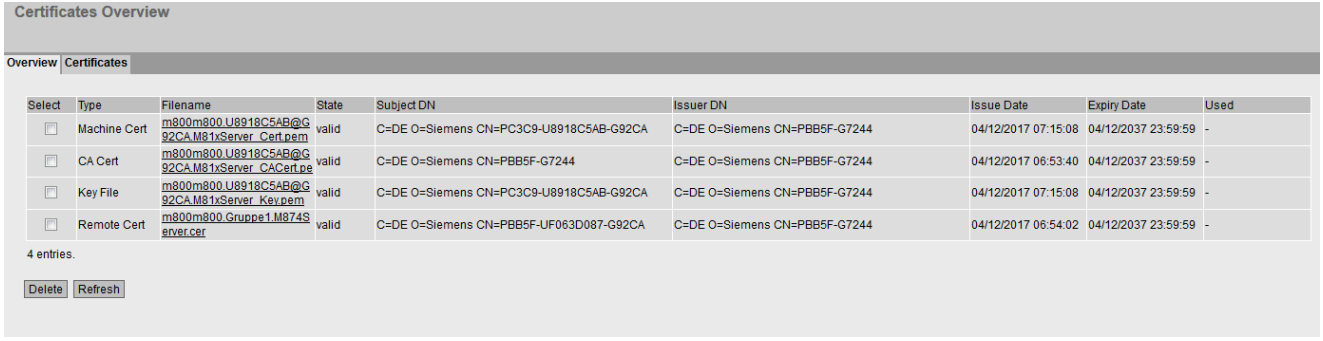
7. Click the "Open" button in the dialog.

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

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

Result

Certificates are loaded and are displayed in "Security" > "Certificates". The loaded certificates must have the status "Valid".



3.4.2 Configuring the VPN remote end

In the configuration example, the M87x in the station is the VPN client that establishes the connection to the VPN server with a fixed IP address.

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. VPN_Server_M81x.
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 Type	Manual
Remote Address	Fixed external IP address of the M81x e.g. 90.90.90.90
Remote Subnet	192.168.100.0/24 The subnet that can be reached through the VPN tunnel

5. Click on "Set Values".

3.4.3 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 "Connections" tab in the content area.
2. In "Connection Name" enter a name for the VPN connection.
3. Configure the VPN connection with the following settings:

Operation	Disabled
Keying Protocol	IKEv2
Remote End	VPN_Server_M81x Name of the VPN remote station
Local Subnet	192.168.11.0/24 The local subnet 1 in CIDR notation.

4. Click on "Set Values".

3.4.4 Configuring VPN authentication

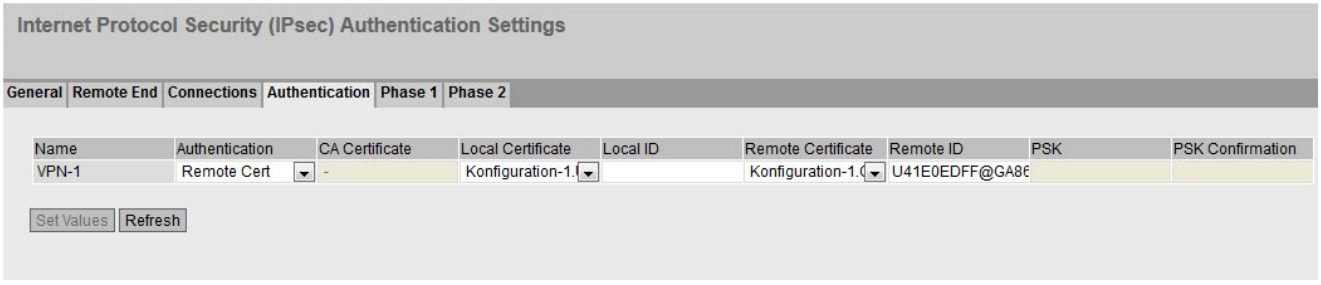
For secure communication via VPN, all VPN partners need to authenticate themselves with each other. In this configuration example, the certificate of the VPN remote station.

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	Remote Cert
Local certificate	The precise names of the certificates and the remote ID can be found in the relevant configuration file.
Remote Certificate	
Remote ID	

3. Click on "Set Values".



3.4.5 Configuring phase 1 and phase 2

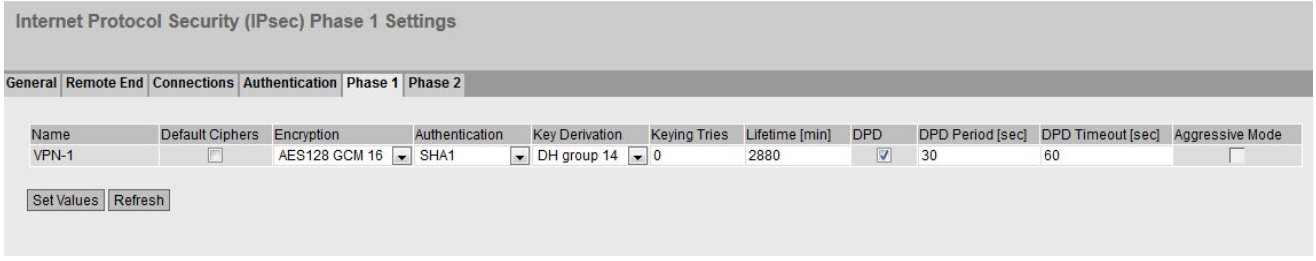
The settings must match on both devices.

Configuring phase 1

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 1" tab in the content area.
2. Deselect the "Default Ciphers" check box.
3. Select the "DPD" check box.
4. Configure phase 1 with the following settings from the configuration file:

Encryption	AES 128
Authentication	SHA1
Key Derivation	DH group 14
Lifetime [min]:	2880
DPD Period [sec]	60
Aggressive Mode	no

5. Click on "Set Values".



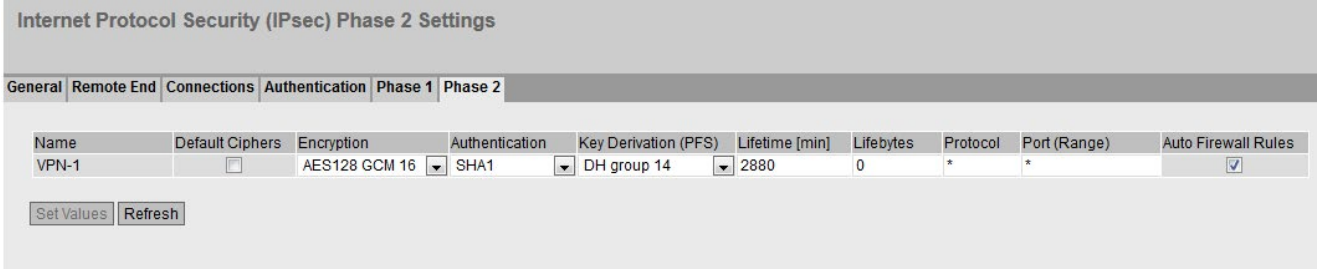
Configuring phase 2

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "Phase 2" tab in the content area.
2. Leave the "Default Ciphers" check box enabled.

   When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. The selection depends on the key exchange method.
3. Select the "DPD" check box.
4. Configure phase 1 with the following settings from the configuration file:

Encryption	AES128
Authentication	SHA1
Key Derivation	DH group 14
Lifetime [min]:	2880

5. Enable "Auto Firewall Rules" The firewall rule is created automatically for the VPN connection.

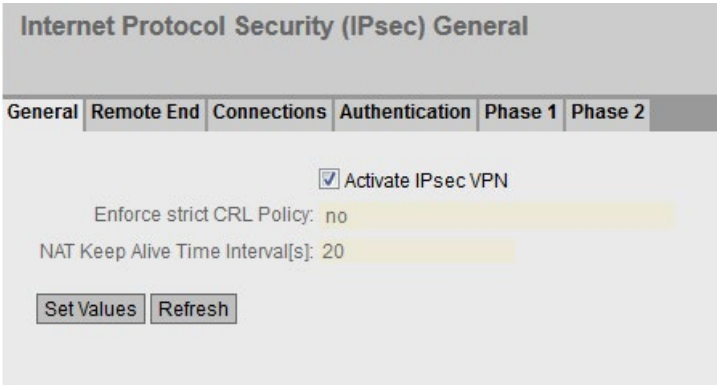


6. Click on "Set Values".

3.4.6 Activating VPN

Procedure

1. Click on "Security" > "IPsec VPN" in the navigation area and on the "General" tab in the content area.
2. Enable the "IPsec VPN" setting.



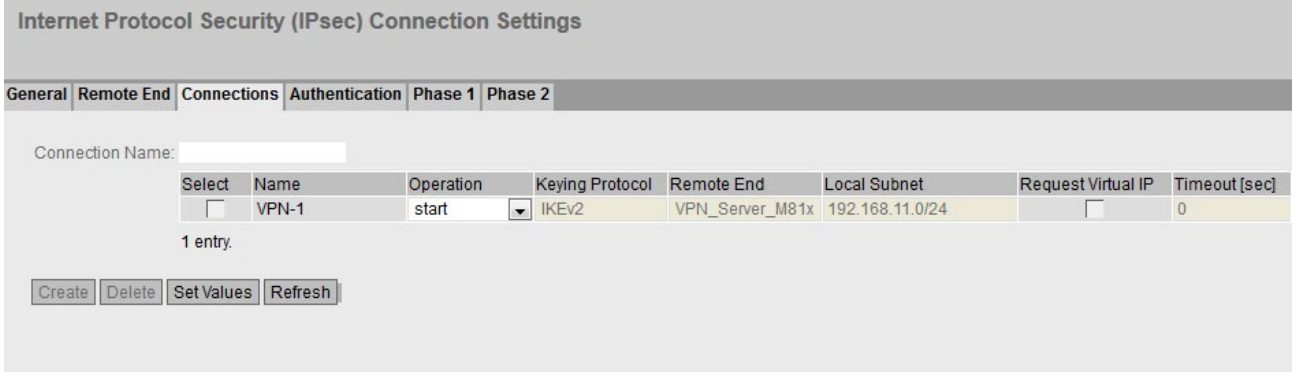
3. Click on "Set Values".

3.4.7 Establishing the VPN connection

The M87x (VPN client) is configured as the initiator of the VPN tunnel and establishes the VPN connection to the SCALANCE M87x (VPN server)

Procedure

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



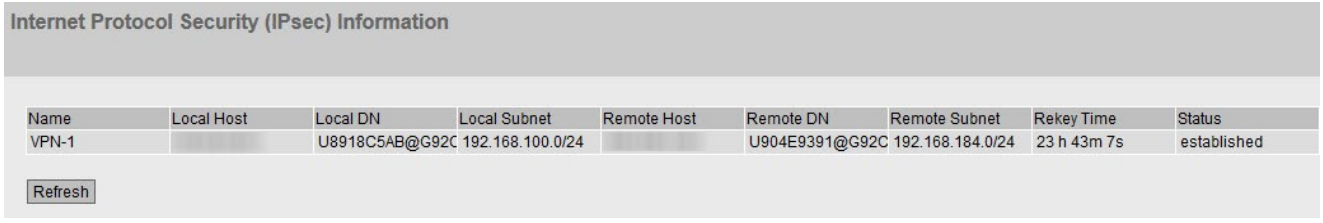
3.5 Displaying the status of the VPN connection

The devices are configured and connected to the Internet. The M87x (VPN client) starts connection establishment to the M81x (VPN server). To display the status of the VPN connection, you have the following options:

- Status display in the WBM
- LED display

Status display in the WBM

In the navigation area, click "Information" > "IPsec VPN". "Status" displays the status of the configured VPN connection.



LED display

If the VPN connection is established, the 🔒 LED is lit green on the device.

VPN tunnel between SCALANCE S615 and SINEMA RC Server

4

4.1 Procedure in principle

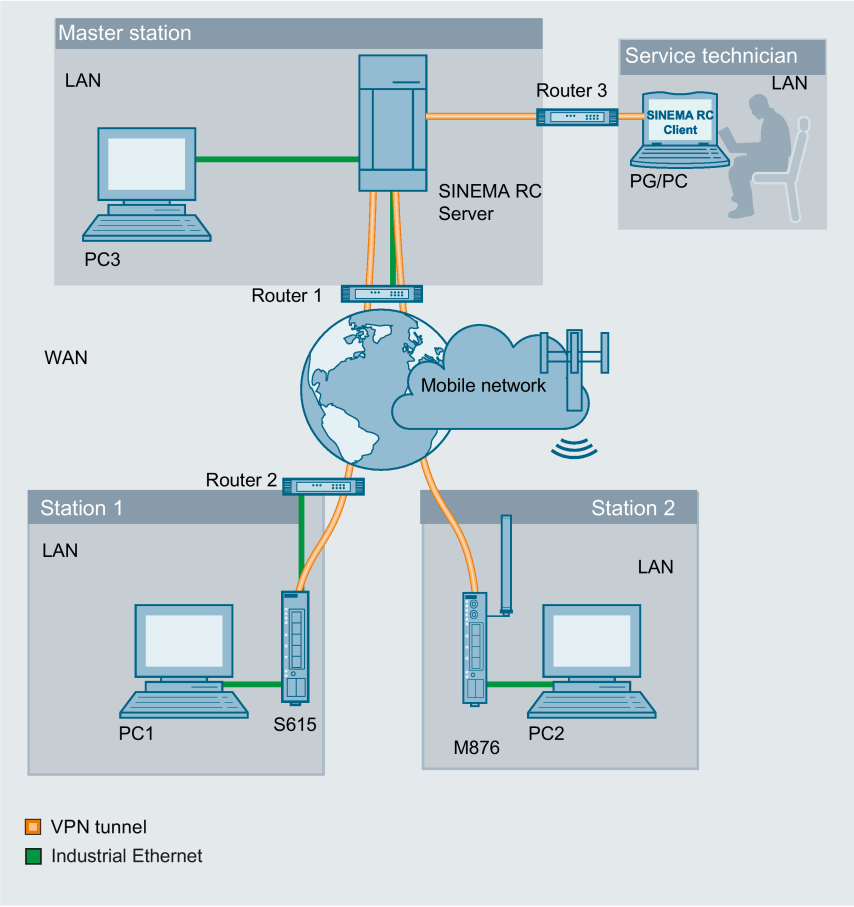
In this example configuration, a service technician is to access two distributed stations for maintenance purposes. Station 1 is connected via a SCALANCE S615 and Station 2 via a SCALANCE M876. The service technician uses a PG/PC. Communication takes place via a SINEMA RC Server located in the master station.

Station 2 is directly connected to the WAN via SCALANCE M876, the others via a router.

The service technician and the devices establish the OpenVPN connection to the SINEMA RC Server, which can be reached via a static IP address. The service technician uses the SINEMA RC Client, OpenVPN client software, to establish the VPN connection.

When establishing a connection, the devices authenticate themselves to the SINEMA RC Server with the CA certificate.

After the connection has been established, the devices and the service technician must log in to the SINEMA RC Server. The VPN tunnel between the devices, the service technician and the SINEMA RC Server is only established after successful login. Depending on the configured communication relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.



Required devices/components

Use the following components for setup:

Master station

- 1 x PC on which the SINEMA RC Server is installed.
- 1 x PC for configuring the SINEMA RC Server
- 1 x VPN-capable DSL router

Station 1

- 1 x S615 (additional option: a suitably installed standard rail with fittings)
- 1 x KEY-PLUG SINEMA RC
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuration
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ45 standard for Industrial Ethernet.
- 1 x VPN-capable DSL router

Station 2

- 1 x M876 (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 are enabled, e.g. the Internet.
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuration
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ45 standard for Industrial Ethernet.

Service technician

- 1 x PG/PC on which the "SINEMA RC Client" is installed.
- 1 x DSL router with dynamic WAN IP address

Note

You can also use another SCALANCE M-800 or SC-600 device. 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
Master station LAN	SINEMA RC Server (VPN server)	LAN port	192.168.20.250
		WAN port	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. 192.168.184.20 Default gateway is the LAN IP address of the router 192.168.1.2
	PC1	LAN port	192.168.20.20 255.255.255.0
	Router 1	LAN port	192.168.20.2 255.255.255.0
		WAN port	Static IP address assigned by the provider, e.g. 192.168.184.20

	Name	Interface	IP address
Station1 LAN	S615 (VPN client)	LAN port P1 (vlan1)	192.168.100.1 255.255.255.0
		WAN port P5 (vlan2)	192.168.50.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.50.2
	PC2	LAN port	192.168.100.20 255.255.255.0
	Router 2	LAN port	192.168.50.2 255.255.255.0
		WAN port	Dynamic IP address from provider
Station2 LAN	M874 (VPN client)	LAN port P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN port (ppp0)	Dynamic IP address from provider
	PC3	LAN port	192.168.10.20 255.255.255.0
Service technician	PG /PC	LAN port	192.168.1.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.1.2
	Router 3	LAN port	192.168.1.2 255.255.255.0
		WAN port	Dynamic IP address from provider

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 via the DSL router. You will find the configuration steps in the Getting Started "SINEMA Remote Connect".

  The DSL router has a permanently assigned public IP address. This must be requested from the provider and then stored in the DSL router.

SCALANCE S615/M876

- The devices are connected to the WAN, see Getting Started "SCALANCE M-800" and Getting Started "SCALANCE S615".

  The steps in configuration are the same for all devices, the only difference being the settings, see table "Settings used (Page 103)".
- The devices can be accessed via the configuration PC and you are logged in to the WBM as a user with administrator rights.
- A valid KEY-PLUG SINEMA Remote Connect is plugged into the devices.
- SCALANCE S615 is connected to the WAN via the DSL router.

Note

Port forwarding on the DSL data router

To ensure that the packets can be exchanged unhindered between PG/PC (SINEMA Remote Connect Client), SCALANCE S615 and SINEMA Remote Connect Server, ensure that PORT forwarding for OpenVPN and https with TCP and UDP (TCP/443, UDP/1194, TCP/5443, TCP/6220) is enabled and forwarded to the SINEMA Remote Connect Server.

Steps in configuration

Configuring a remote connection on the SINEMA RC Server

1. Creating participant groups (Page 108)
2. Creating a device (Page 109)
3. Creating a user account for service technician (Page 111)
4. Configuring communication relations (Page 112)
5. Exporting a certificate (Page 114)

Configuring a remote connection on the device

1. Loading a certificate (Page 115)
2. Configuring a route on the SCALANCE S615 (Page 116)
3. Configuring the VPN connection to the SINEMA RC (Page 117)

Establishing a remote connection with the SINEMA RC Client

1. Installing SINEMA RC Client (Page 120)
2. Logging in to SINEMA RC Server with SINEMA RC Client (Page 122)

4.2 Configure a remote connection on the SINEMA RC Server

4.2.1 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.

- Station1: SCALANCE S615
- Station2: SCALANCE M876
- Service: For the service technician

Requirement

- The SINEMA RC Server is connected to the WAN.

Open page

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 103)".
2. Log in as the "admin" user and with the corresponding password.
3. Select "Remote connections > Participant groups" in the navigation area.
4. Click "Create".
   The "New participant group" page opens.

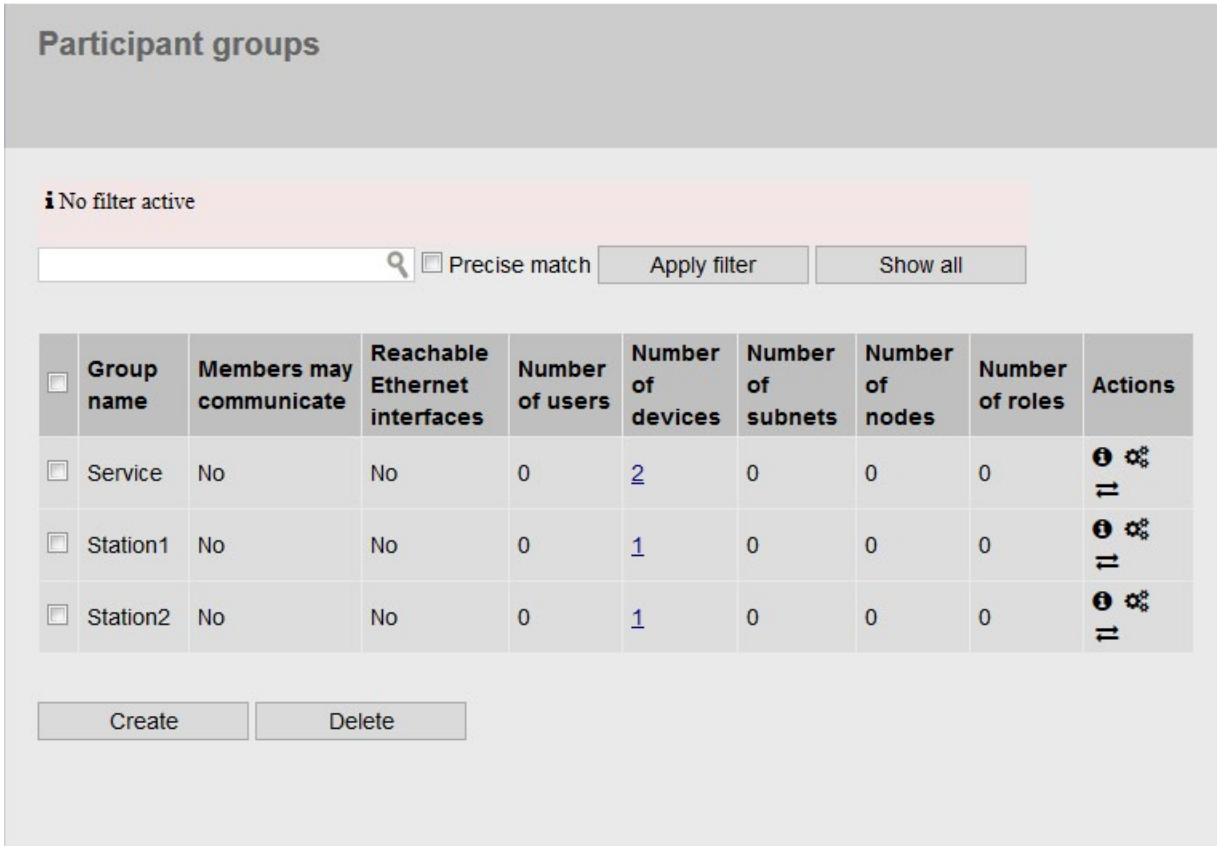
Create participant group

1. Enter the name "Station1" for "Group name".
2. You can optionally enter a description.
3. Enable the "Members may communicate with each other" option.
4. Enable the network interface which is accessible through the VPN tunnel and click "Save".

Result

The "Station1" participant group has been created.

Now create the participant groups "Station2" and "Service". To do this, click "Create" and repeat the steps described above.



4.2.2 Create devices

Open page

1. In the navigation area, select "Remote connections > Devices".
2. Click "Create" button to create a new device.

Enter device information

1. Enter a device name, e.g. S615.
   The following characters are allowed: a-z, A-Z, 0-9 and _. The space character is not allowed. "conn" cannot be used as a name.
2. Enter a password and confirm this password.
   The password must be made up of uppercase and lowercase letters, numbers and special characters.
3. Optionally, you can enter the manufacturer of the device.
4. Select the type of device from the list.
5. Make the following settings for the devices M800 Mobile, RTU 303xC, RM1224:
   - Select the SMS gateway provider.
     You can configure the SMS gateway provider under "System > E-mail & SMS".
   - Specify the GSM number of the node to which a wake-up SMS is to be sent.
6. Specify the installation location of the device if needed.
7. Enter a comment if needed.

Establish OpenVPN connection

1. Select "OpenVPN" for VPN protocol.
2. Select the "Permanent" connection type from the list.

Configure all access

1. Select the entry "Station1" for "Participant groups" and click "Add".
2. Click on "Next".
   The "Network settings" page opens.

Set Values

1. Enable the "Device is a network gateway" option.
2. Click on "Finish" to complete the configuration.

Result

Device S615 is connected.
Now create the device M876. To do this, click "Create" and repeat the steps described above. You assign the device M876 to the participant group "Station2".

See also

Procedure in principle (Page 103)

4.2.3 Creating a user account for service technician

To log in, the service technician requires a user name and a password.

Requirement

- The "Service" participant group has been created, refer to the section "Creating participant groups".

Open page

1. In the navigation area, select "User accounts > Users and roles".
   The users that have already been created are listed in the content area.
2. Click "Create".
   The "New user" page opens.

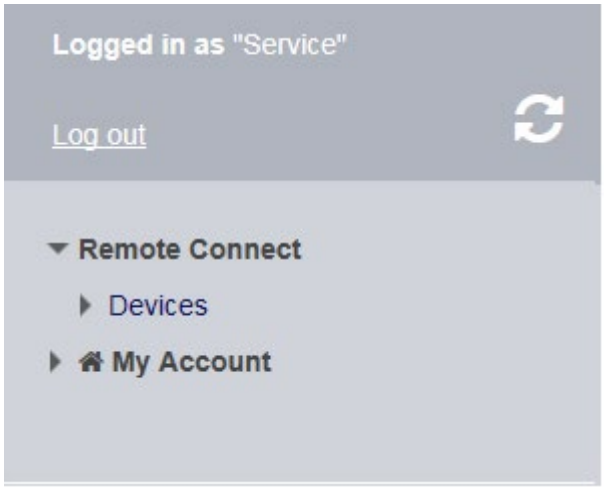
Create users

1. Enter the user name e.g. Service.
2. Optionally, enter the name and contact information of the user.
3. Select "Password" for "Login procedure" and click "Next".
   The "Rights" tab is displayed.
4. Specify the rights for the service technician and click on "Next".
   The "Group memberships" tab is displayed.
5. Enable the "Service" participant group and click "Next".
   The "VPN connection mode" tab is displayed.
6. Enable the "OpenVPN" VPN connection mode and click "Next".
   The "Password" tab is displayed.
7. Specify and confirm the password for the user. Click "Complete".

Result

The "Service" user has been created. In the "Status" column you can see whether or not the user is currently online.

If the user is logged on, he or she can only access the entries in the navigation area for which he or she has rights.



4.2.4 Configure communications relations

Communication relations are required to enable participant groups to communicate with each other. 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	Station1
	Station2
Station1	Station2

In this configuration example, the communication only goes from group "Station1" to group "Station2". In the opposite direction, no communication is possible. For the communication from the group "Station2" to the group "Station1" another communication relation is necessary.

The group "Service" can also communicate with the groups "Station1" and "Station2" but they cannot communicate with "Service".

Requirement

- The participant groups Service, Station1, and Station2 have been created.

Open page

1. Select "Remote connections > Participant groups" in the navigation area.
   The participant groups that have already been created are listed in the content area.

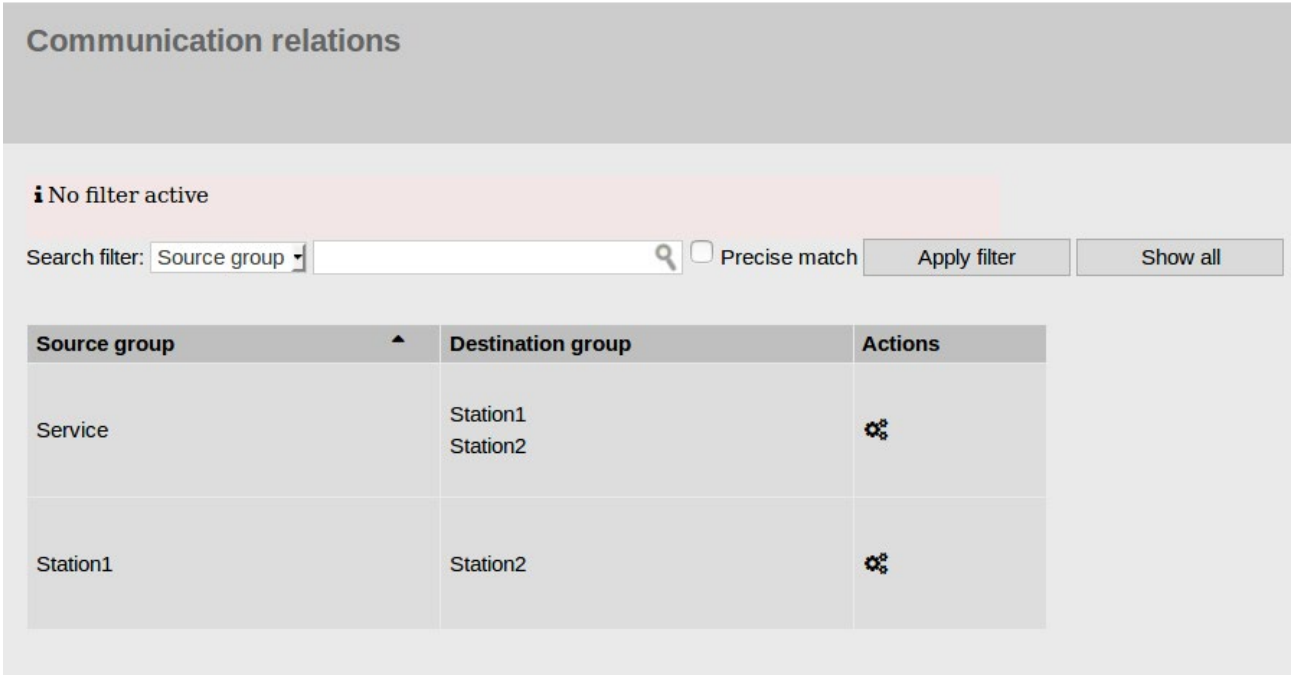
Configuring communication relations

1. For "Service", click on the ⇄ icon in the "Actions" column.
   The "Destination group / Station1" page opens.
2. Enable "Station2" and click on "Save".
3. Click "Exit dialog✖".
4. For "Service", click on the ⇄ icon in the "Actions" column.
   The "Destination group" page opens.
5. Enable "Station1" and "Station2" and click on "Save".
6. 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.



4.2.5 Exporting a certificate

In this configuration example, the CA certificate is used for authentication. The CA certificate must be exported from the SINEMA Remote Connect Server since it is required for configuring the devices.

Open page

1. In the navigation area, select "Security > Certificate management" .
   The "Certificate Management" page opens.

Exporting a certificate

1. Click on the icon for "Actions" to export the certificate.
2. Save the certificates in a local directory.

4.3 Configure a remote connection on the device

4.3.1 Loading a certificate

In this configuration example, the device authenticates itself to the SINEMA RC Server with the CA certificate. You have already exported the CA certificate from SINEMA RC Server, see section "Exporting a certificate (Page 114)". Now you have to load the CA certificate into the device.

Requirement

- The correct time is set on the devices.

Open page

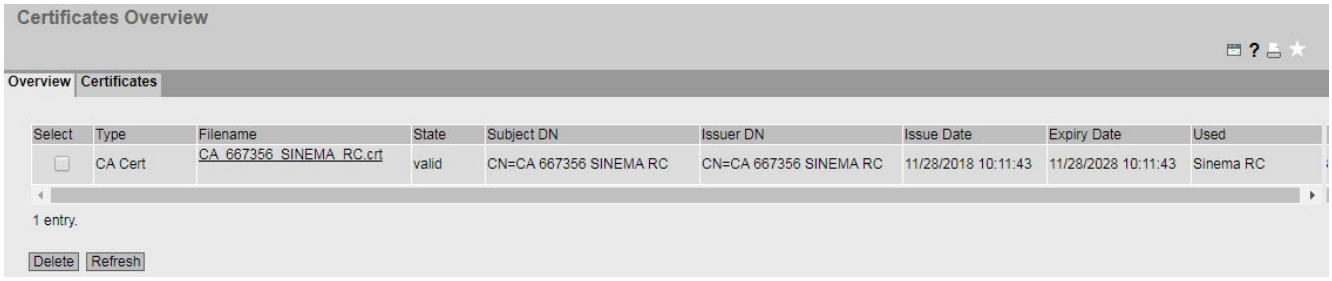
1. In the address field of the Web browser, enter the LAN IP address of the S615 "https://<IP address>", see table "Settings used (Page 103)".
2. Log in as the "admin" user and with the corresponding password.
3. In the navigation area, select "System > Load & Save" and the "Passwords" tab in the content area.

Loading a certificate

1. Enter the device password in "X509Cert". Enable the entry and click on "Set Values".
2. Click on the "HTTP" tab in the content area.
3. Click the "Load" button next to "X509Cert".
   The dialog for loading a file opens.
4. Navigate to the exported server certificate. Click the "Open" button in the dialog.
   The file is now loaded onto the device.
5. After loading successfully, confirm the next dialog with "OK".

Result

The certificate is loaded. Certificates are displayed in "Security" > "Certificates". The loaded certificates must have the status "Valid".



4.3.2 Configuring a route on the SCALANCE S615

The DSL router in Station1 is used as a gateway to access the SINEMA RC Server from the SCALANCE S615. Therefore, the SCALANCE S615 configures a route to the SINEMA RC Server with the DSL router as gateway.

Open page

1. In the address field of the Web browser, enter the LAN IP address of the S615 "https://<IP address>", see table "Settings used".
2. Log in as the "admin" user and with the corresponding password.
3. In the navigation area, select "Layer 3 > Static Routes".

Configuring a route

1. Configure the route to the router with the following settings:

Destination Network	Static IP address of the SINEMA RC Server
Subnet mask	255.255.255.255
Gateway	LAN IP address of the router according to the table "Settings used"
Administrative Distance	-1

2. When you have entered the values, click "Create".
3. Click "Refresh" to update the display.

Result

The route is created.

4.3.3 Configuring a VPN connection to the SINEMA RC Server

Requirement

- A valid KEY-PLUG is plugged into the device.

  The KEY-PLUG unlocks the SINEMA RC function. Now you can configure the connection to SINEMA Remote Connect.

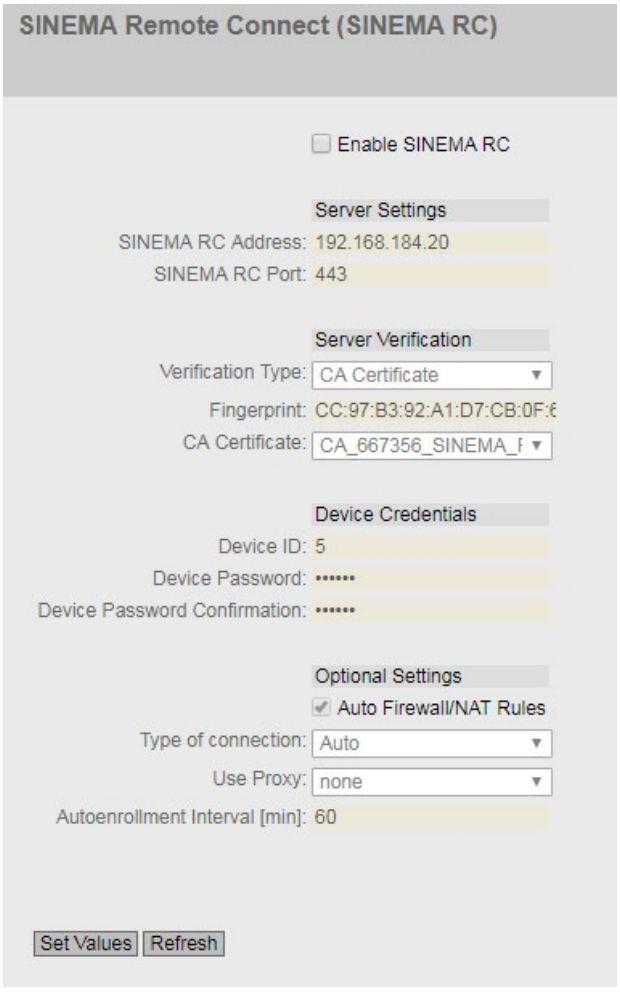
Open page

1. In the navigation area, select "System > SINEMA RC".

Configuring the VPN connection to the server

1. Clear the "SINEMA RC Server" check box.
2. For "SINEMA RC address", enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 103)".
3. For "CA certificate", select the valid certificate for the device.
4. Enter the appropriate ID for "Device ID".
   You can find the Device ID on the SINEMA RC Server in the "Device overview" tab under "Remote connections > Devices". Click on the icon in the "Actions" column for the relevant device.
5. For "Device password", enter the password that you configured for access. Confirm the password.

6. Enable "Auto Firewall/NAT Rules" to automatically create the required NAT and firewall rules.



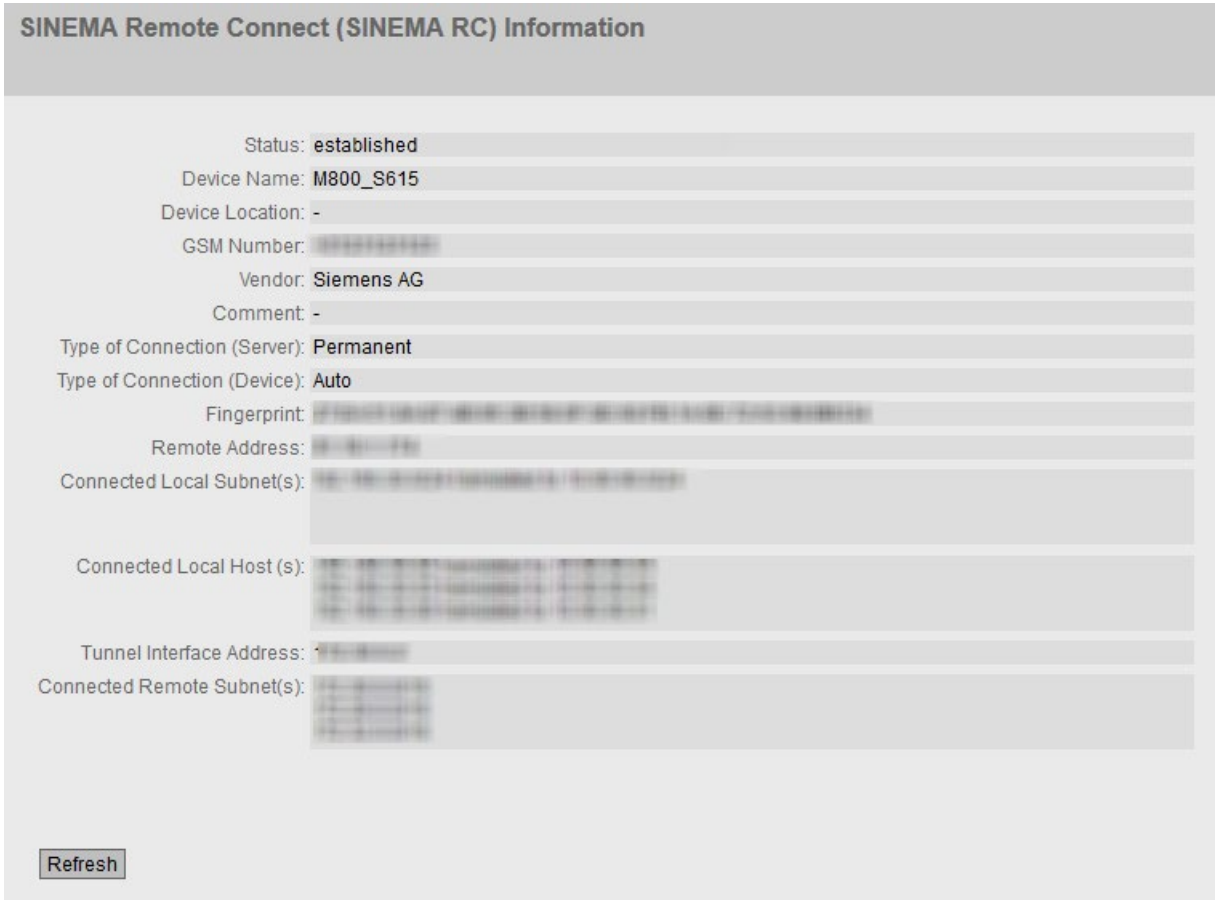
7. Select the "Enable SINEMA RC" check box and click on "Set Values".

Result

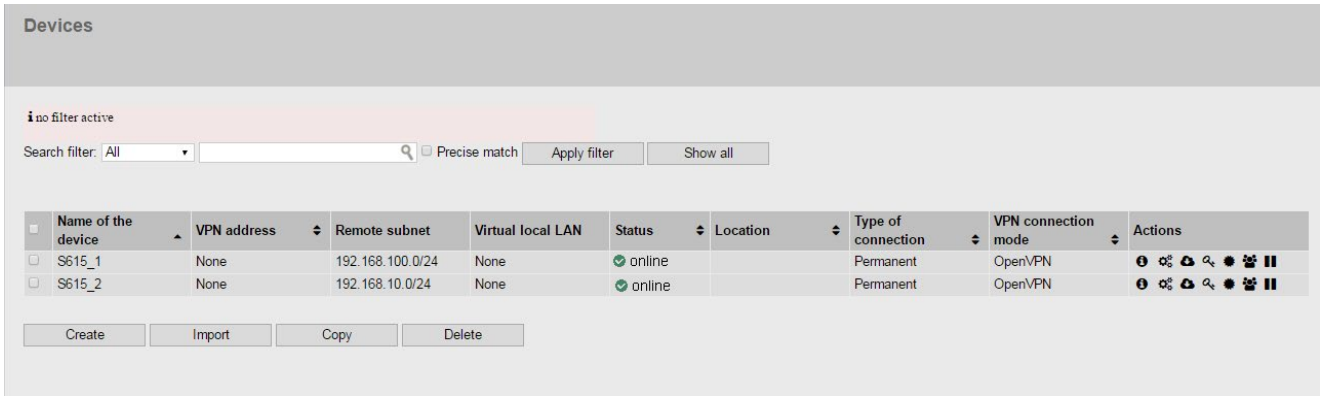
The device establishes an OpenVPN tunnel to the SINEMA RC Server.

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

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



Web browser 2: In the navigation area, select "Remote connections > Devices".



Establishing a remote connection with the SINEMA RC Client

4.3.4 Installing SINEMA RC Client

Most of the installation is handled automatically. The SETUP routine itself recognizes whether other program components apart from SINEMA RC Client itself need to be installed. The installation routine takes the required actions as necessary.

Note

You can only install one SINEMA RC Client per PC.

Note

Multiple OpenVPN clients

If the SINEMA Remote Connect client is installed parallel to other OpenVPN clients, perfect functioning cannot be guaranteed.

It is recommended to install only the SINEMA Remote Connect as OpenVPN client

Requirement

The SINEMA RC Client can be installed on the following operating system:

- Microsoft Windows 7 Professional 32/64-bit + Service Pack 1
- Microsoft Windows 7 Enterprise 32/64-bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64-bit + Service Pack 1
- Microsoft Windows 8.1 Professional 64-bit
- Microsoft Windows Server 2008 R2 x64 (requirement: NET 3.5 or higher is installed)
- Microsoft Windows Server 2016 Standard (Desktop representation)
- Microsoft Windows 10 Professional 64-bit
- Microsoft Windows Server 2012 64-bit

Procedure

1. Log in to the Windows operating system as administrator. Open the Windows Explorer and double-click on the "Setup.exe" file in the root directory of the installation DVD. As an alternative, start the program from the Windows menu "Start > Run".

   If the Auto Run function is enabled for your DVD drive, the installation will start automatically.
2. Select the language for the Setup wizard of SINEMA RC Client and click "Continue".
3. Click the "Open source license agreement" button to display the license agreement. After reading the license agreement, select the option "I accept the conditions of the above

license agreement as well as the conditions of the Open Source license agreement" and then click "Continue".

4. A dialog box opens containing the list of programs to be installed. Leave the preselection of the components as it stands. These include:
   - .NET Framework
   - Open VPN
   - Automation License Manager (ALM)
5. If you require further information about the ALM, click the "Readme" button on the right of the dialog box.
6. Select the "Save as" button to display the current storage space of the computer.
7. Click the "Browse" button if you want to change the standard target directory and install the application somewhere else.
8. Select the required storage location and click the "Continue" button.

   Note

   Memory requirements

   If the drive does not have enough free storage space, click the "Browse" button to select a different location for the installation.

   The "System settings" dialog box opens.
9. Accept the changes to the system settings.

   Follow the further instructions that guide you through the entire installation. This process can take several minutes.

   When it is finished, a final window is displayed for the setup. This contains a status message about the successful installation of the SINEMA RC Client.

   In the setup window, you can either restart the computer immediately or later. Select the required option and click the "Finish" button to complete the installation.

Result

After restarting you will find a new link "SINEMA RC Client" on your desktop and a new entry in the Start menu "All Programs > Siemens Automation > SIMATIC > SINEMA RC Client".

In addition, the network interface "TAP Windows Adapter V9" is installed. Via this interface, the SINEMA RC Client establishes a VPN connection to the SINEMA RC Server.

4.3.5 Logging on to SINEMA RC Server with SINEMA RC Client

Requirement

- The laptop and the SINEMA RC Server are connected to the WAN.
- The "Service" user has been created, see "AUTOHOTSPOT".

Procedure

1. Double-click on the "SINEMA RC Client" icon on your desktop.
   The SINEMA RC Client starts.
2. For "SINEMA RC URL", enter the WAN IP address of the SINEMA Remote Connect Server, see table "Settings used".
3. Enter "Service" as the user name.
4. Enter the valid password and click the "Log in" button.

   After successful login, the start page appears.
5. Click the "Open VPN tunnel" button.

Result

The SINEMA RC Client downloads the OpenVPN file from the SINEMA RC Server. The file contains the parameters required for the VPN connection to the SINEMA RC Server. After the download, the SINEMA RC Client establishes the VPN connection with these parameters.

The SINEMA RC Client checks at regular intervals whether a valid license key exists. If it does not, for example if you remove the USB dongle during operation, you will receive a system message.

The "Service" user is a member of the "Service" participant group. All devices that are assigned to this group are displayed.