SIMATIC NET

Industrial Remote Communication - Remote Networks SINEMA Remote Connect

Getting Started

11/2017

C79000-G8976-C394-04

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C394-04
Ⓟ 10/2017 Subject to change

Preface

Purpose

Based on examples, the configuration of SINEMA Remote Connect is shown.

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 . . .	
SINEMA RC	SINEMA Remote Connect
SINEMA RC Server	SINEMA Remote Connect server
S615	SCALANCE S615
S623	SCALANCE S623

Further documentation

- Operating instructions "SINEMA Remote Connect Client"

  This manual supports you when installing, configuring and operating the application SINEMA RC Client.

- Operating instructions "SINEMA Remote Connect server"

  This manual supports you when installing, configuring and operating the application SINEMA RC Server.

- "Industrial Remote Communication Remote Networks - SCALANCE S615 Web Based Management" configuration manual

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

- Getting Started "Industrial Remote Communication Remote Networks - SCALANCE S615"

  Based on examples, this document explains the configuration of the SCALANCE S615.

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

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

Current manuals and further information

You will find the current manuals and further information on telecontrol products on the Internet pages of Siemens Industry Online Support:

- Using the search function:

  Link to Siemens Industry Online Support (http://support.automation.siemens.com/)

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

- via the navigation in the "Telecontrol" area:

  Link to the area "Telecontrol" (https://support.industry.siemens.com/cs/ww/en/ps/15915)

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

You will find the documentation for the products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

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.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For additional information on industrial security measures that may be implemented, please visit
Link: (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: (https://www.siemens.com/industrialsecurity)

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 here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

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

Trademarks

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

SINEMA, SCALANCE

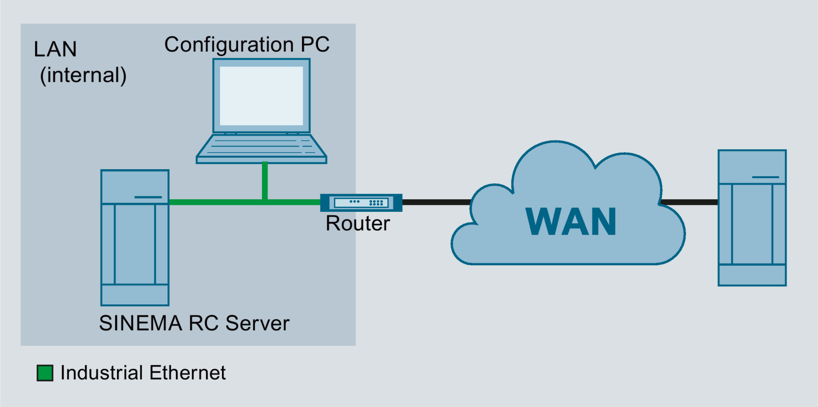
Table of contents

Connecting the SINEMA RC Server to the WAN 1

1.1 Procedure in principle

In this example, the SINEMA RC Server is configured using the Web Based Management (WBM). On the WAN/LAN access is via a router that is connected to the WAN port of the server.

Structure



Required devices/components

- 1 x PC without operating system
- 1 x router

  On the router PORT forwarding for the Web Based Management, OpenVPN and CA rollout with TCP and UDP (TCP/443,UDP/1194,TCP/5443, TCP/6220) must be released.
- 1 x PC for configuring the SINEMA RC Server
- 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:

	Name	Interface	IP address
LAN	SINEMA RC Server	WAN port (eth0)	192.168.20.250 255.255.255.0 Gateway: IP address of the router 192.168.20.2
	PC	Ethernet	192.168.20.20 255.255.255.0
	Router	LAN port	192.168.20.2 255.255.255.0
		WAN port	192.168.184.20 255.255.255.0

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.

Steps in configuration

1. Installing SINEMA RC Server (Page 11)
2. Launching Web Based Management (Page 12)
3. Check the interface (Page 15)
4. Setting the time (Page 16)

1.2 Installing SINEMA RC Server

NOTICE
Installation formats the hard disk The installation of the SINEMA RC Server includes its own operating system. If you use a PC on which an operating system already exists, the hard disk will be formatted. This means that existing data is lost. Make sure that all important data on the PC has been backed up.

Requirement

- PC without operating system. The hard disk should be at least 60 GB.
- In the boot order, CD/DVD is set as the first boot medium.

Procedure

1. Turn on the PC.
2. Insert the data medium in the drive. Installation starts automatically.
3. In the following dialog, the entry "Install/Update SINEMA Remote Connect Server" is selected. Press <Return> to confirm the selection.
4. In the following dialog, the entry "eth0" is selected. Press <Return> to confirm the selection.
5. Enter the WAN IP address of the SINEMA RC Server, refer to the table "Settings used (Page 9)". Press <Return> to confirm the entry.
6. For the network mask, leave the entry unchanged. Press <Return> to confirm the entry.
7. As the gateway enter the LAN IP address of the router, refer to the table "Settings used (Page 9)". Press <Return> to confirm the entry.

   The operating system and the SINEMA RC Server are installed. Follow the further instructions on the screen.

1.3 Launching Web Based Management

After installation, the SINEMA RC Server is reachable via the WAN interface at the following IP address 192.168.20.250

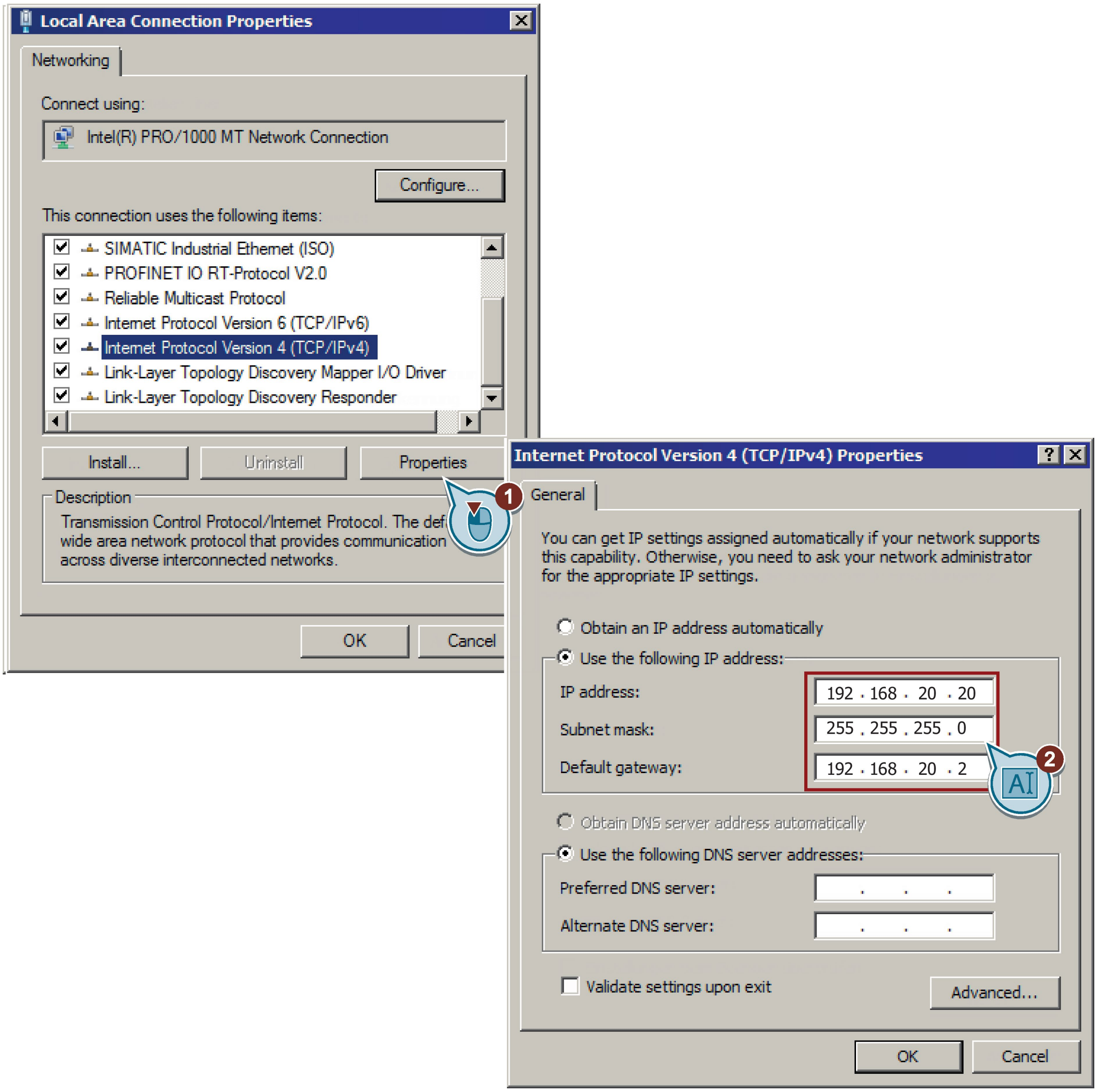
In this configuration example, the configuration PC has the following IP address setting to allow it to access the Web Based Management of the SINEMA RC Server.

IP address	Subnet mask	Gateway
192.168.20.20	255.255.255.0	192.168.20.2

Procedure

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

5. Enter the values in the table above.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

- ☑ SIMATIC Industrial Ethernet (ISO)
- ☑ PROFINET IO RT-Protocol V2.0
- ☑ Reliable Multicast Protocol
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The def wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 20 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 20 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

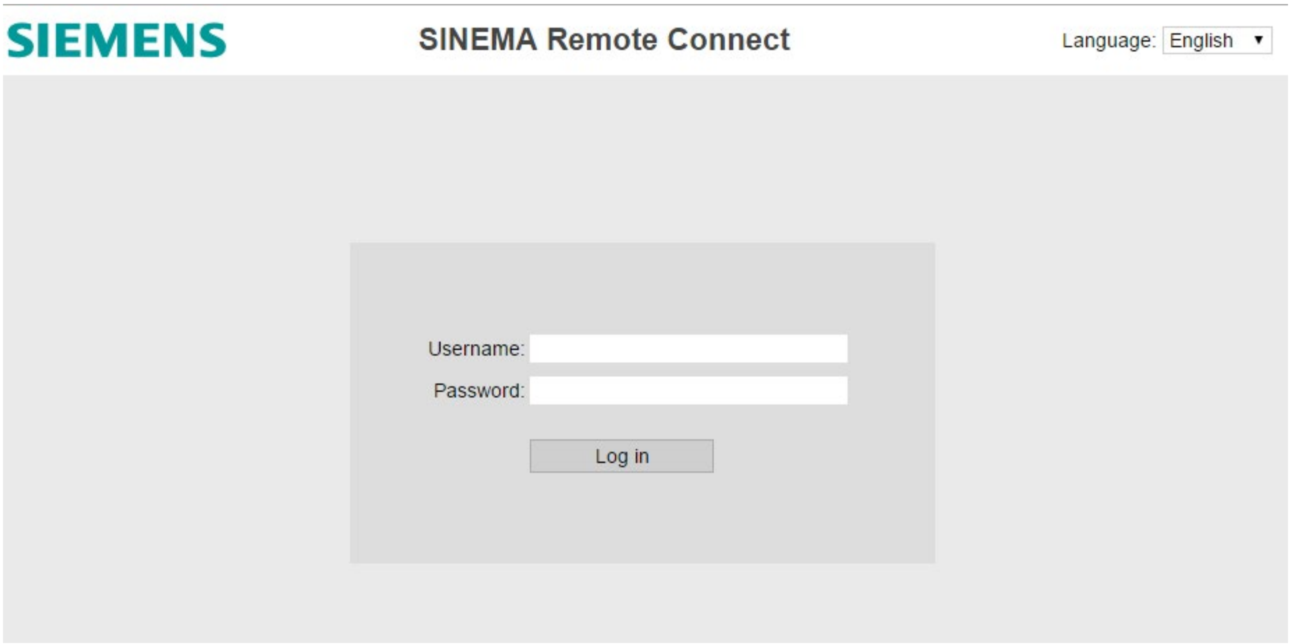
□ Validate settings upon exit

Advanced...

OK Cancel

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

7. In the address box of the Web browser enter "https://192.168.20.250". If there is a problem-free connection, the login page of Web Based Management (WBM) is displayed.



8. After installation, log in with the user name "admin" and the password "admin".
9. After logging in the WBM page "Change password" is opened. Specify the user name and the password for the administrator.

   The new password must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers, refer to the section "Permitted characters". As administrator, you can change the settings of the device (read and write access to the configuration data).
10. Click the "Save" button. After saving, you are automatically logged on with the newly created administrator.

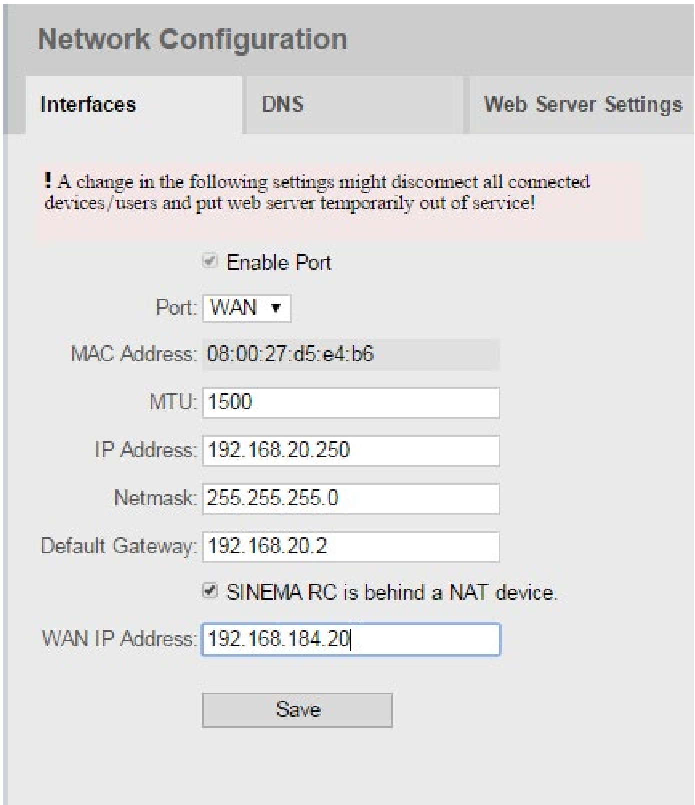
1.4 Check the interface

Procedure

1. Click on "System > Network configuration" in the navigation area and on the "Interfaces" tab in the content area.
2. For "Interface" select "WAN". The configuration of the port is displayed.
3. Check the settings of the WAN port.

IP address	WAN IP address of the SINEMA RC Server according to the table "Settings used (Page 9)".
Network mask	Network mask according to the table "Settings used (Page 9)"
Standard gateway	LAN IP address of the router according to the table "Settings used (Page 9)"

4. Enable "SINEMA Remote Connect is downstream from a NAT device" to enter the external WAN IP for the gateway.
5. For the WAN IP address, enter the WAN IP address of the router, see table "Settings used (Page 9)".



Network Configuration

! A change in the following settings might disconnect all connected devices/users and put web server temporarily out of service!

☑ Enable Port

Port: WAN ▾

MAC Address: 08:00:27:d5:e4:b6

MTU: 1500

IP Address: 192.168.20.250

Netmask: 255.255.255.0

Default Gateway: 192.168.20.2

☑ SINEMA RC is behind a NAT device.

WAN IP Address: 192.168.184.20

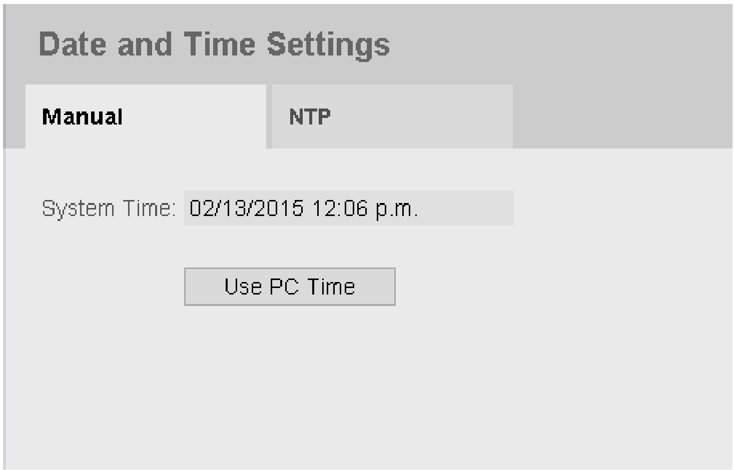
6. Click "Backup".

1.5 Setting the time

The date and time are kept on the SINEMA RC Server to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server.

Procedure

1. Click on "System" > "Date and time settings" in the navigation area and on the "Manual" tab in the content area.
2. Click "Use PC time".



System Time: 02/13/2015 12:06 p.m.

Result

System time using PC is set.

Creating devices using a csv file 2

2.1 Introduction

In this example three devices are created using a csv file. The csv file has a certain structure, see section "Structure of the csv file (Page 18)".

Settings used

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

Name of the device	Setting	
S615_001	Type of connection	1 = permanent
	Participant group	Station1
	Network gateway	Yes
	Local LAN IP address 1	192.168.10.1 255.255.255.0
	Local LAN IP address 2	192.168.20.1 255.255.255.0
	NAT for local subnet Virtual local LAN IP address	10.90.80.1 255.255.255.0 Assigned to local LAN IP address 2
S615_002	Type of connection	1 = permanent
	Participant group	Station2
	Network gateway	No
	Local LAN IP address	192.168.30.1 255.255.255.0
	NAT for local subnet Virtual local LAN IP address	10.90.90.1 255.255.255.0

	NAT for local hosts
	Virtual local LAN IP address
	Local host
		
		10.90.90.x
		192.168.30.y
		x = 2 - 20
		y = 1 - 19

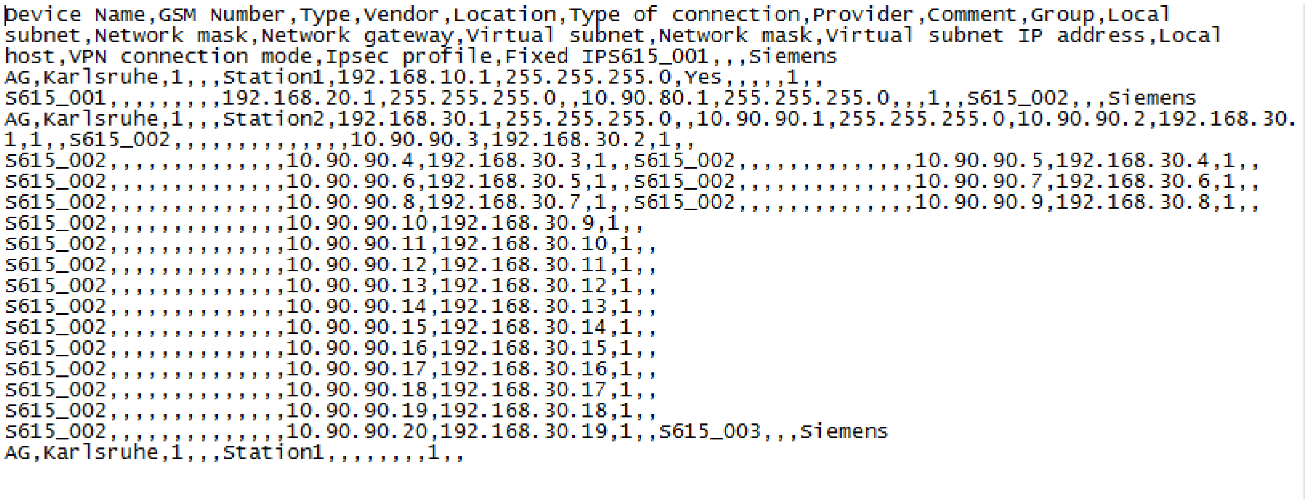
S615_003	Type of connection	1 = permanent
	Participant group	Station1

Steps in configuration

1. Creating a csv file (Page 20)
2. Importing a csv file (Page 22)

2.2 Structure of the csv file

On the data medium, you will find a template of the csv file. The entries are separated by semicolons.



```
Device Name,GSM Number,Type,Vendor,Location,Type of connection,Provider,Comment,Group,Local
subnet,Network mask,Network gateway,Virtual subnet,Network mask,Virtual subnet IP address,Local
host,VPN connection mode,Ipsec profile,Fixed IPS615_001,,,Siemens
AG,Karlsruhe,1,,,Station1,192.168.10.1,255.255.255.0,Yes,,,,,1,,
S615_001,,,,,,,,,192.168.20.1,255.255.255.0,,10.90.80.1,255.255.255.0,,,1,,S615_002,,,Siemens
AG,Karlsruhe,1,,,Station2,192.168.30.1,255.255.255.0,,10.90.90.1,255.255.255.0,10.90.90.2,192.168.30.
1,1,,S615_002,,,,,,,,,,,,,,10.90.90.3,192.168.30.2,1,,
S615_002,,,,,,,,,,,,,,10.90.90.4,192.168.30.3,1,,S615_002,,,,,,,,,,,,,,10.90.90.5,192.168.30.4,1,,
S615_002,,,,,,,,,,,,,,10.90.90.6,192.168.30.5,1,,S615_002,,,,,,,,,,,,,,10.90.90.7,192.168.30.6,1,,
S615_002,,,,,,,,,,,,,,10.90.90.8,192.168.30.7,1,,S615_002,,,,,,,,,,,,,,10.90.90.9,192.168.30.8,1,,
S615_002,,,,,,,,,,,,,,10.90.90.10,192.168.30.9,1,,
S615_002,,,,,,,,,,,,,,10.90.90.11,192.168.30.10,1,,
S615_002,,,,,,,,,,,,,,10.90.90.12,192.168.30.11,1,,
S615_002,,,,,,,,,,,,,,10.90.90.13,192.168.30.12,1,,
S615_002,,,,,,,,,,,,,,10.90.90.14,192.168.30.13,1,,
S615_002,,,,,,,,,,,,,,10.90.90.15,192.168.30.14,1,,
S615_002,,,,,,,,,,,,,,10.90.90.16,192.168.30.15,1,,
S615_002,,,,,,,,,,,,,,10.90.90.17,192.168.30.16,1,,
S615_002,,,,,,,,,,,,,,10.90.90.18,192.168.30.17,1,,
S615_002,,,,,,,,,,,,,,10.90.90.19,192.168.30.18,1,,
S615_002,,,,,,,,,,,,,,10.90.90.20,192.168.30.19,1,,S615_003,,,Siemens
AG,Karlsruhe,1,,,Station1,,,,,,,,1,,
```

Values to be set

The table contains the entries that you can enter in the csv file. For more detailed information on these entries, refer to the section "Creating a new device" and device information..

The entry ...	stands for ...
Device Name	Name of the device
GSM Number	GSM number
Type	Device type
Vendor	Manufacturer
Location	Location
Type of connection	Type of connection Enter the number for the relevant type of connection. 1 = permanent: 2 = digital input 3 = wake-up SMS 4 = digital input & wake-up SMS
Provider	Name of the SMS gateway provider
Comment	Comment
Group	Participant group The requirement is that the participant group has already been created.
Local subnet	Local LAN IP address
Network mask	Network mask of the local LAN IP address
Network gateway	Device is a network gateway If the device is a network gateway, enter "Yes".
Virtual subnet	Virtual subnet IP address

The entry ...	stands for ...
Network mask	Network mask of the virtual subnet IP address
Virtual subnet IP address	Virtual subnet address
Local host	Local host
VPN donnection mode	VPN connection mode 1 = OpenVPN: The connection will be established via OpenVPN. 2 = IPsec: The connection will be established via IPsec.
Ipsec profile	Name of the IPsec profile The requirement is that the IPsec profile has already been created.
Fixed IP	Fixed IP address for OpenVPN or IPsec connections

2.3 Creating a csv file

Procedure

1. Open the csv template with MS Excel or a text editor.
2. Specify the first device.

   ```
   S615_001;;;Siemens
   AG;Karlsruhe;1;;;Station1;192.168.10.1;255.255.255.0;Yes;;;;;1;;
   ```

   ```
   S615_001;;;;;;;;;192.168.20.1;255.255.255.0;;10.90.80.1;255.255.255.0;;;1;;
   ```

   Specify the number for the relevant type of connection: 1 for permanent

   If the device is a network gateway, specify "Yes". Otherwise no entry is necessary.
3. Specify the second device:

   ```
   S615_002;;;Siemens
   AG;Karlsruhe;1;;;Station2;192.168.30.1;255.255.255.0;;10.90.90.1;255.255.255.0;10.
   90.90.2;192.168.30.1;1;;
   ```

   ```
   S615_002;;;;;;;;;;;;;;10.90.90.3;192.168.30.2;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.4;192.168.30.3;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.5;192.168.30.4;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.6;192.168.30.5;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.7;192.168.30.6;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.8;192.168.30.7;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.9;192.168.30.8;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.10;192.168.30.9;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.11;192.168.30.10;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.12;192.168.30.11;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.13;192.168.30.12;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.14;192.168.30.13;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.15;192.168.30.14;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.16;192.168.30.15;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.17;192.168.30.16;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.18;192.168.30.17;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.19;192.168.30.18;1;;

   S615_002;;;;;;;;;;;;;;10.90.90.20;192.168.30.19;1;;
   ```

   For "NAT for local subnet", a row is necessary for every assignment.

4. Specify the third device.

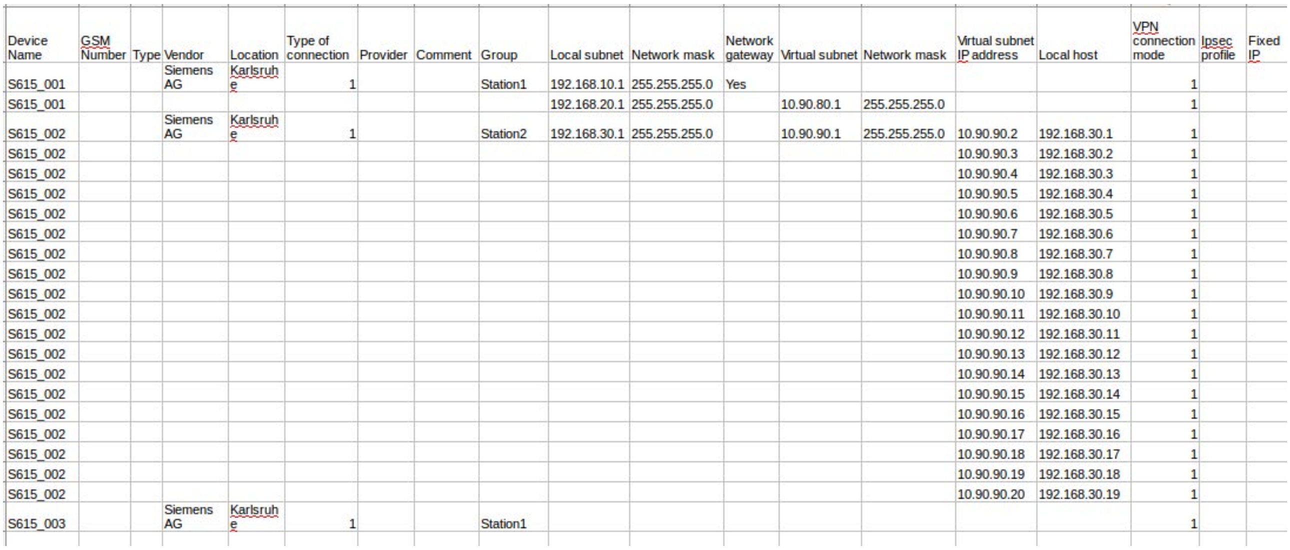
   ```
   S615_003;;;Siemens AG;Karlsruhe;1;;;Station1;;;;;;;;;;
   ```

   In this case, only the name, the location and the group of the device are created. The rest is entered later in the WBM of the SINEMA RC server.

5. Save the csv file.

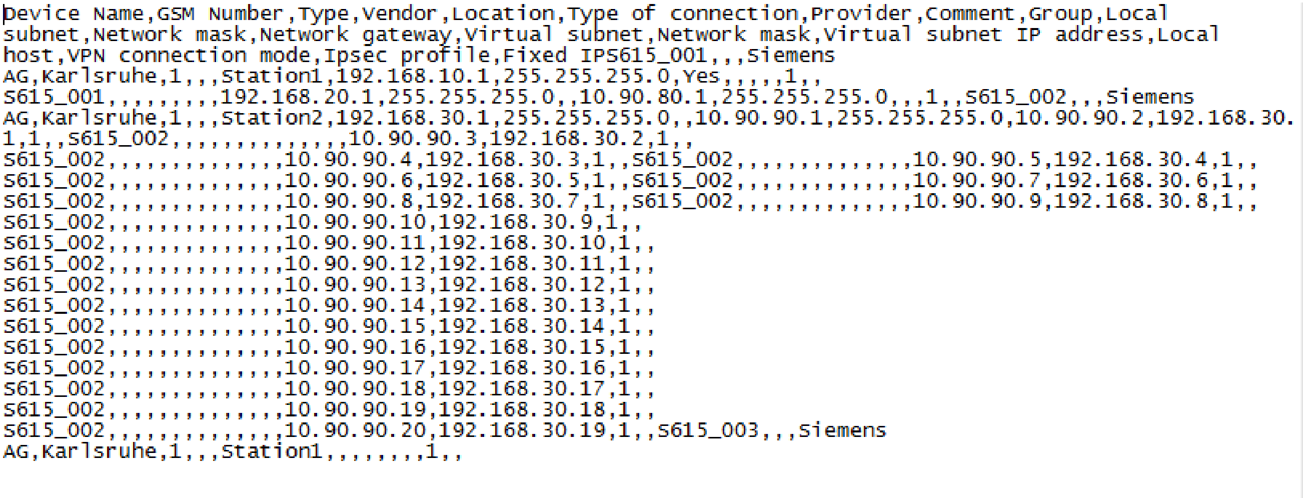
Result

The csv file has been created with the three devices.



Device Name	GSM Number	Type	Vendor	Location	Type of connection	Provider	Comment	Group	Local subnet	Network mask	Network gateway	Virtual subnet	Network mask	Virtual subnet IP address	Local host	VPN connection mode	Ipsec profile	Fixed IP
S615_001			Siemens AG	Karlsruhe	1			Station1	192.168.10.1	255.255.255.0	Yes					1		
S615_001									192.168.20.1	255.255.255.0		10.90.80.1	255.255.255.0			1		
S615_002			Siemens AG	Karlsruhe	1			Station2	192.168.30.1	255.255.255.0		10.90.90.1	255.255.255.0	10.90.90.2	192.168.30.1	1		
S615_002														10.90.90.3	192.168.30.2	1		
S615_002														10.90.90.4	192.168.30.3	1		
S615_002														10.90.90.5	192.168.30.4	1		
S615_002														10.90.90.6	192.168.30.5	1		
S615_002														10.90.90.7	192.168.30.6	1		
S615_002														10.90.90.8	192.168.30.7	1		
S615_002														10.90.90.9	192.168.30.8	1		
S615_002														10.90.90.10	192.168.30.9	1		
S615_002														10.90.90.11	192.168.30.10	1		
S615_002														10.90.90.12	192.168.30.11	1		
S615_002														10.90.90.13	192.168.30.12	1		
S615_002														10.90.90.14	192.168.30.13	1		
S615_002														10.90.90.15	192.168.30.14	1		
S615_002														10.90.90.16	192.168.30.15	1		
S615_002														10.90.90.17	192.168.30.16	1		
S615_002														10.90.90.18	192.168.30.17	1		
S615_002														10.90.90.19	192.168.30.18	1		
S615_002														10.90.90.20	192.168.30.19	1		
S615_003			Siemens AG	Karlsruhe	1			Station1								1		

Figure 2-1 csv file: Table editor



```
Device Name,GSM Number,Type,Vendor,Location,Type of connection,Provider,Comment,Group,Local
subnet,Network mask,Network gateway,Virtual subnet,Network mask,Virtual subnet IP address,Local
host,VPN connection mode,Ipsec profile,Fixed IPS615_001,,,Siemens
AG,Karlsruhe,1,,,Station1,192.168.10.1,255.255.255.0,Yes,,,,,1,,
S615_001,,,,,,,,,192.168.20.1,255.255.255.0,,10.90.80.1,255.255.255.0,,,1,,S615_002,,,Siemens
AG,Karlsruhe,1,,,Station2,192.168.30.1,255.255.255.0,,10.90.90.1,255.255.255.0,10.90.90.2,192.168.30.
1,1,,S615_002,,,,,,,,,,,,,,10.90.90.3,192.168.30.2,1,,
S615_002,,,,,,,,,,,,,,10.90.90.4,192.168.30.3,1,,S615_002,,,,,,,,,,,,,,10.90.90.5,192.168.30.4,1,,
S615_002,,,,,,,,,,,,,,10.90.90.6,192.168.30.5,1,,S615_002,,,,,,,,,,,,,,10.90.90.7,192.168.30.6,1,,
S615_002,,,,,,,,,,,,,,10.90.90.8,192.168.30.7,1,,S615_002,,,,,,,,,,,,,,10.90.90.9,192.168.30.8,1,,
S615_002,,,,,,,,,,,,,,10.90.90.10,192.168.30.9,1,,
S615_002,,,,,,,,,,,,,,10.90.90.11,192.168.30.10,1,,
S615_002,,,,,,,,,,,,,,10.90.90.12,192.168.30.11,1,,
S615_002,,,,,,,,,,,,,,10.90.90.13,192.168.30.12,1,,
S615_002,,,,,,,,,,,,,,10.90.90.14,192.168.30.13,1,,
S615_002,,,,,,,,,,,,,,10.90.90.15,192.168.30.14,1,,
S615_002,,,,,,,,,,,,,,10.90.90.16,192.168.30.15,1,,
S615_002,,,,,,,,,,,,,,10.90.90.17,192.168.30.16,1,,
S615_002,,,,,,,,,,,,,,10.90.90.18,192.168.30.17,1,,
S615_002,,,,,,,,,,,,,,10.90.90.19,192.168.30.18,1,,
S615_002,,,,,,,,,,,,,,10.90.90.20,192.168.30.19,1,,S615_003,,,Siemens
AG,Karlsruhe,1,,,Station1,,,,,,,,1,,
```

Figure 2-2 csv file: Text editor

2.4 Importing a csv file

Requirement

- The csv file exists and is filled correctly.
- The activated license is adequate.
- The participant groups "Station1" and "Station2" have been created.
- The names of the devices have not yet been created.
- The logged on user has the right "Manage devices"

Procedure

1. Click the "Import" button on the page with the device list.
2. Click the "Browse" button and select the csv file.
3. Click "Import".

   After importing the file, the devices are listed on the "Device selection" tab
4. Select the check box for "S615_001", "S615_002" and "S615_003".
5. Click "Finish".

Result

After creating (importing) the devices are displayed in the device list. Click on ℹ to check the settings.

OpenVPN tunnel between SCALANCE S615 and SINEMA RC Server 3

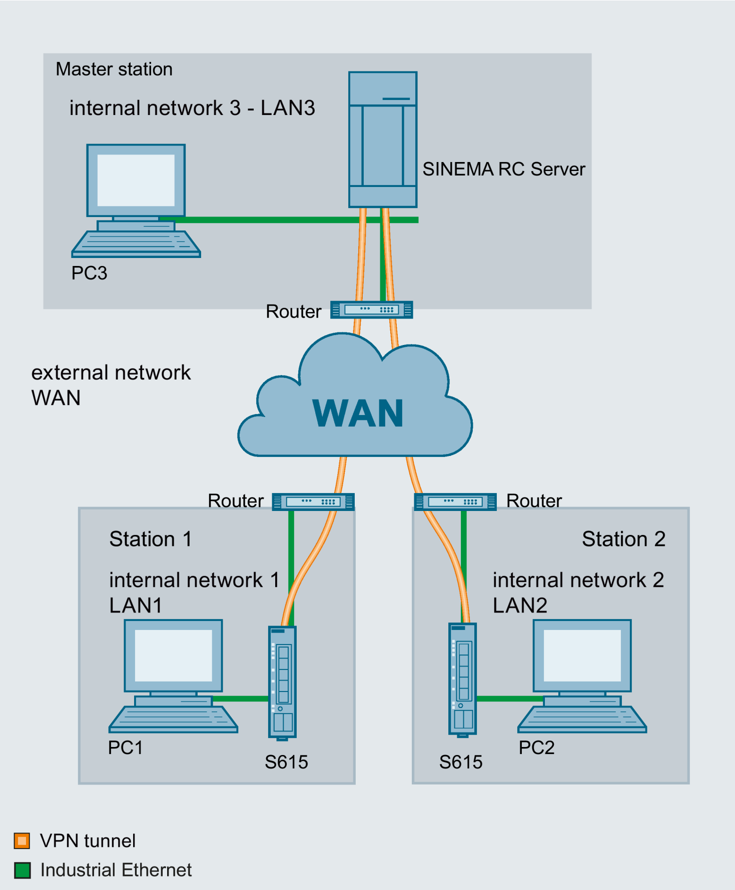
3.1 Procedure in principle

In this sample configuration two distributed stations are connected using a SCALANCE S615. The devices communicate via the SINEMA RC Server located in the master station.

A KEY-PLUG SINEMA Remote Connect is required for each SCALANCE S615 device. The KEY-PLUG enables the connection from SCALANCE S615 to SINEMA RC.

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

Structure



Master station - connection to SINEMA RC Server

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

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

Station 1 / 2 - Connection to SCALANCE S615

- In the test setup in the internal network, a network node is implemented by a PC connected to the Ethernet interface P1 of the S615.
  - PC: represents a participant in internal network 1/2
  - S615: SCALANCE S module for protection of the internal network 1/2
- Connection to the external network via a router

  Access to the external network is via a router connected to the Ethernet interface P5 of the S615.

Required devices/components

Use the following components for setup:

- 2 x S615 (additional option: a suitably installed standard rail with fittings)
- 2 x KEY-PLUG SINEMA RC
- 2 x 24 V power supply with cable connector and terminal block plug
- 2 x PC each connected to a SCALANCE S615.
- 1 x PC on which the SINEMA RC Server is installed.
- 1 x PC that is connected to the SINEMA RC Server.
- 3 x 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:

	Name	Interface	IP address
Station1 LAN1	S615_1	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
	PC1	LAN port	192.168.100.20 255.255.255.0
	Router1	LAN port	192.168.50.2 255.255.255.0
Station2 LAN2	S615_2	LAN port P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN port P5 (vlan2)	192.168.40.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.40.2
	PC2	Ethernet (LAN 2)	192.168.10.20 255.255.255.0
	Router 2	LAN port	192.168.40.2 255.255.255.0
Master station LAN3	SINEMA RC Server	WAN port	192.168.20.250 255.255.255.0 The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example. 192.168.184.20 Default gateway is the LAN IP address of the router 192.168.20.2
	PC3	Ethernet (LAN3)	192.168.20.20 255.255.255.0
	Router 3	LAN port	192.168.20.2 255.255.255.0
		WAN port	192.168.184.20

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, see "Connecting the SINEMA RC Server to the WAN (Page 9)".

SCALANCE S615

- The SCALANCE S is connected to the WAN. You will find the configuration steps in the 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 45)".
- The SCALANCE S can be reached via PC1/2 and you are logged on to the WBM as "admin".
- A valid KEY-PLUG SINEMA Remote Connect is inserted in the SCALANCE S.

Steps in configuration

Configuring access to the SINEMA RC Server on the S615

To allow a VPN connection to the SINEMA RC Server, a route must be created on the S615:

1. Configuring a route (Page 27)

For the PC to be able to access the WBM of the SINEMA RC Server via S615, the following steps are necessary on the S615:

1. Activate Basic NAT (Page 28)
2. Allow access (Page 28)

Configure a remote connection on the SINEMA RC Server

1. Creating participant groups (Page 30)
2. Create devices (Page 31)
3. Configure communication relations (Page 34)

Configure the remote connection on the S615

- Secure OpenVPN connection with fingerprint (Page 36)
- Secure OpenVPN connection with CA certificate
  - Loading a certificate (Page 39)
  - Configure an OpenVPN connection to the SINEMA RC Server (Page 40)

3.2 Configuring access to the SINEMA RC Server on the S615

3.2.1 Configuring a route

The stations and master station are in different IP subnets. So that the stations can communicate with the master station, the appropriate default route is created on the S615.

Procedure

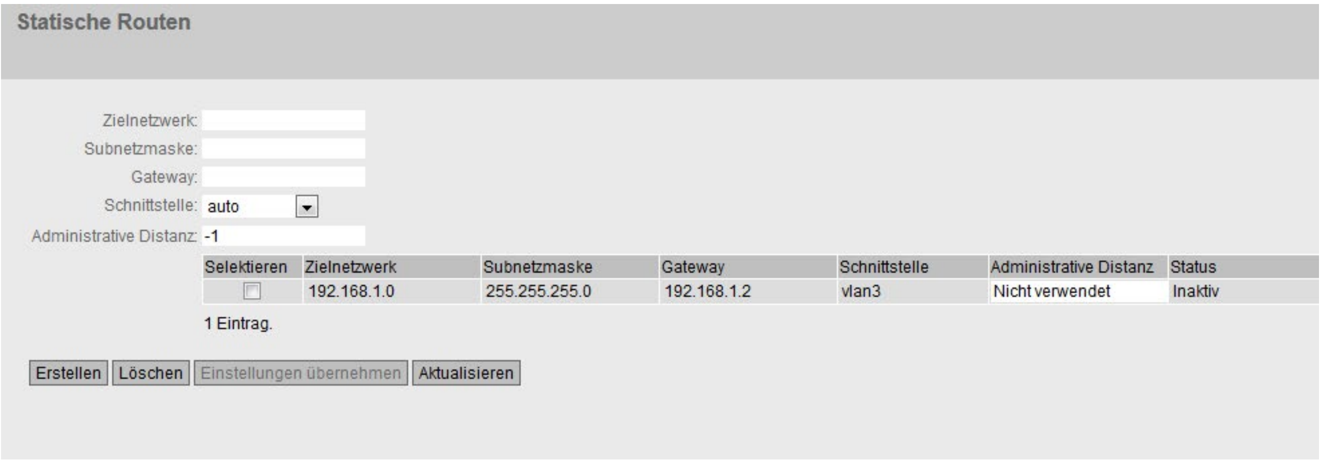
1. In the address box of the Web browser, enter the LAN IP address of the S615, see table "Settings used (Page 45)".
2. Log in as the "admin" user and the corresponding password.
3. Click "Layer 3 > Static Routes" in the navigation area.
4. Configure the route to the router with the following settings:

Destination Network	0.0.0.0 (all IP addresses)
Subnet Mask	0.0.0.0
Gateway	LAN IP address of the router according to the table "Settings used"
Administrative Distance	-1

5. When you have entered the values, click "Create".
6. To update the display, click "Refresh".

Result

The route is created.



Statische Routen

Zielnetzwerk:
Subnetzmaske:
Gateway:
Schnittstelle: auto
Administrative Distanz: -1

Selektieren	Zielnetzwerk	Subnetzmaske	Gateway	Schnittstelle	Administrative Distanz	Status
□	192.168.1.0	255.255.255.0	192.168.1.2	vlan3	Nicht verwendet	Inaktiv

1 Eintrag.

3.2.2 Activating IP masquerading

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

Procedure

1. Click on "Layer 3 > NAT" in the navigation area and on the "Masquerading" tab in the content area.
2. Activate "Enable Masquerading" for vlan2.
3. Click on "Set Values".

Result

Masquerading is activated on the WAN port vlan2. When a packet is sent via this interface, the source address is translated to the IP address assigned to vlan2.

3.2.3 Allow access

So that the PC can access the SINEMA RC Server, access from vlan1 to vlan2 is enabled on the device.

Procedure

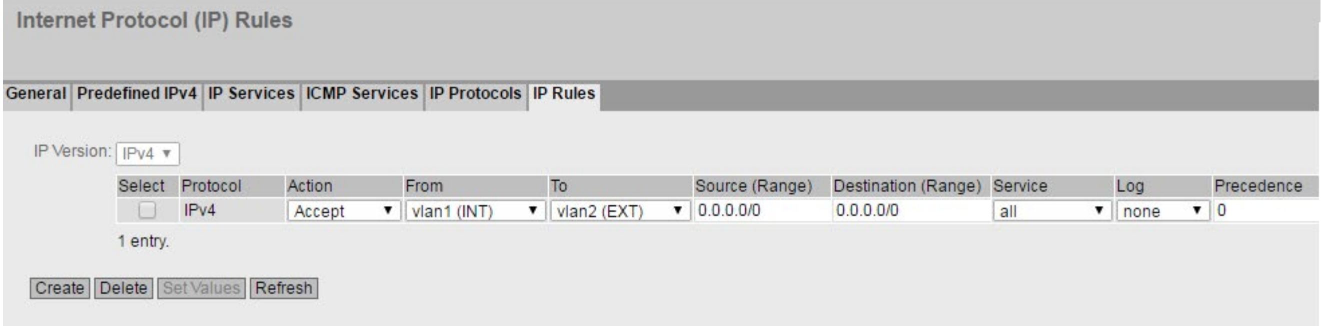
1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule with the following settings:

Action	Accept
From	vlan1 (internal)
To	vlan2 (external)
Source (Range)	0.0.0.0 (all IP addresses)
Destination (Range)	0.0.0.0 (all IP addresses)
Service	all As default, the service is always available

4. Click on "Set Values".

Result

Due to this firewall rule, all services between vlan1 and vlan2 are possible without restrictions, e.g. HTTPS



IP Version: IPv4

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence
□	IPv4	Accept	vlan1 (INT)	vlan2 (EXT)	0.0.0.0/0	0.0.0.0/0	all	none	0

1 entry.

3.3 Configure a remote connection on the SINEMA RC Server

3.3.1 Creating node groups

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

For this sample configuration, the following groups are created.

- Station1
- Station2
- Service

  The Service group is required for the sample configuration "OpenVPN tunnel between SINEMA RC Client and SINEMA RC Server (Page 45)".

Requirement

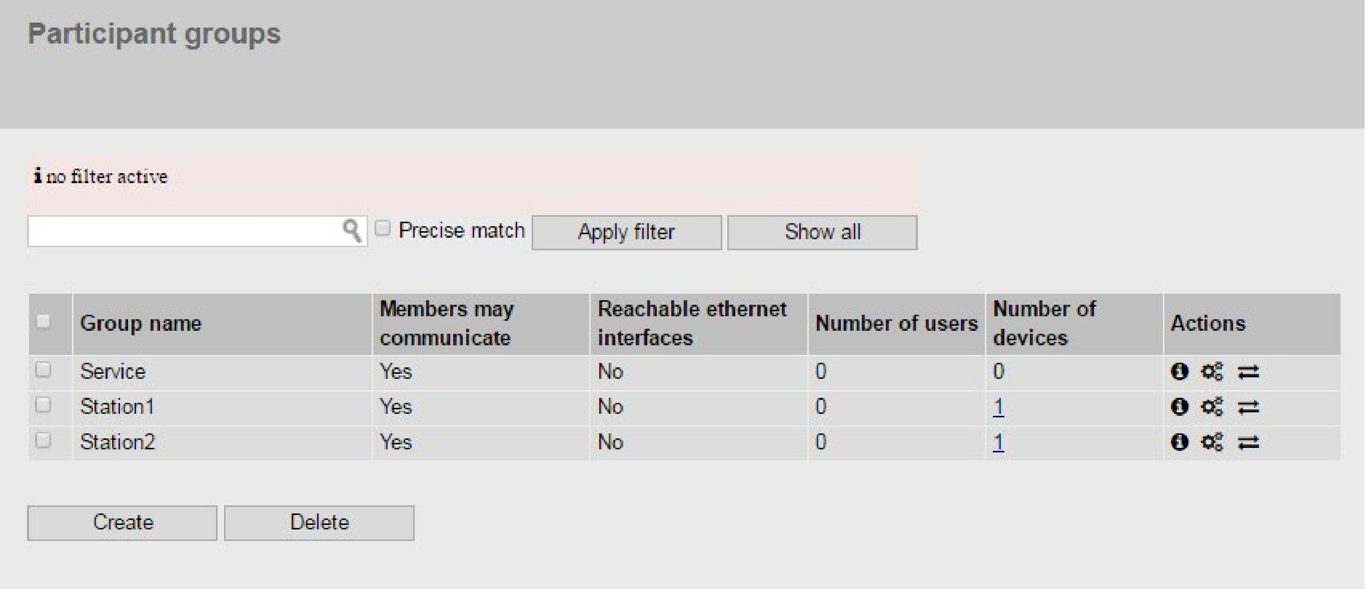
- The SINEMA RC Server is connected to the WAN.

Procedure

1. In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server "https://<WAN IP address>", see table "Settings used (Page 45)".
2. Log on with the user data of the administrator, see section "Starting Web Based Management".
3. In the navigation area, click "Remote connections" > "Participant groups". The participant groups that have already been created are listed in the content area.
4. Click "Create". The page "New participant group" is opened.
5. For group name enter "Station1". Enable the setting "Members may communicate" and click "Save".
6. Repeat steps 1 - 3 for the groups "Station2" and "Service"

Result

The participant groups have been created.



Participant groups

i no filter active

□	Group name	Members may communicate	Reachable ethernet interfaces	Number of users	Number of devices	Actions
□	Service	Yes	No	0	0	ℹ ⚙ ⇄
□	Station1	Yes	No	0	1	ℹ ⚙ ⇄
□	Station2	Yes	No	0	1	ℹ ⚙ ⇄

3.3.2 Create devices

Procedure

1. In the navigation area, click "Remote connections" > "Devices". The devices that have already been created are listed in the content area.
2. Click "Create" button to create a new device.
3. Enter the device name for the device e.g. "S623" for station 1 and "S615_2" for station 2.
4. Click "Continue".
5. For "VPN connection mode", select "OpenVPN". Click "Continue".
6. Enable the parameter "Connected local subnets".
7. Enable the parameter "Device is a network gateway".
8. Configure the devices with the following settings and click "Add":

Local LAN IP address	IP address for vlan1 according to the table "Settings used (Page 45)".
Network mask	255.255.255.0

9. Click "Continue". The "Group memberships" tab is displayed.

10. Enable the appropriate group.

    For the device "S615_1" the group "Station1"

    For the device "S615_2" the group "Station2"

11. Click "Continue". The "Password" tab is displayed.
12. Specify the password for the access e.g. An:t_010 for S615_1 and An:t_020 for S615_2.

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

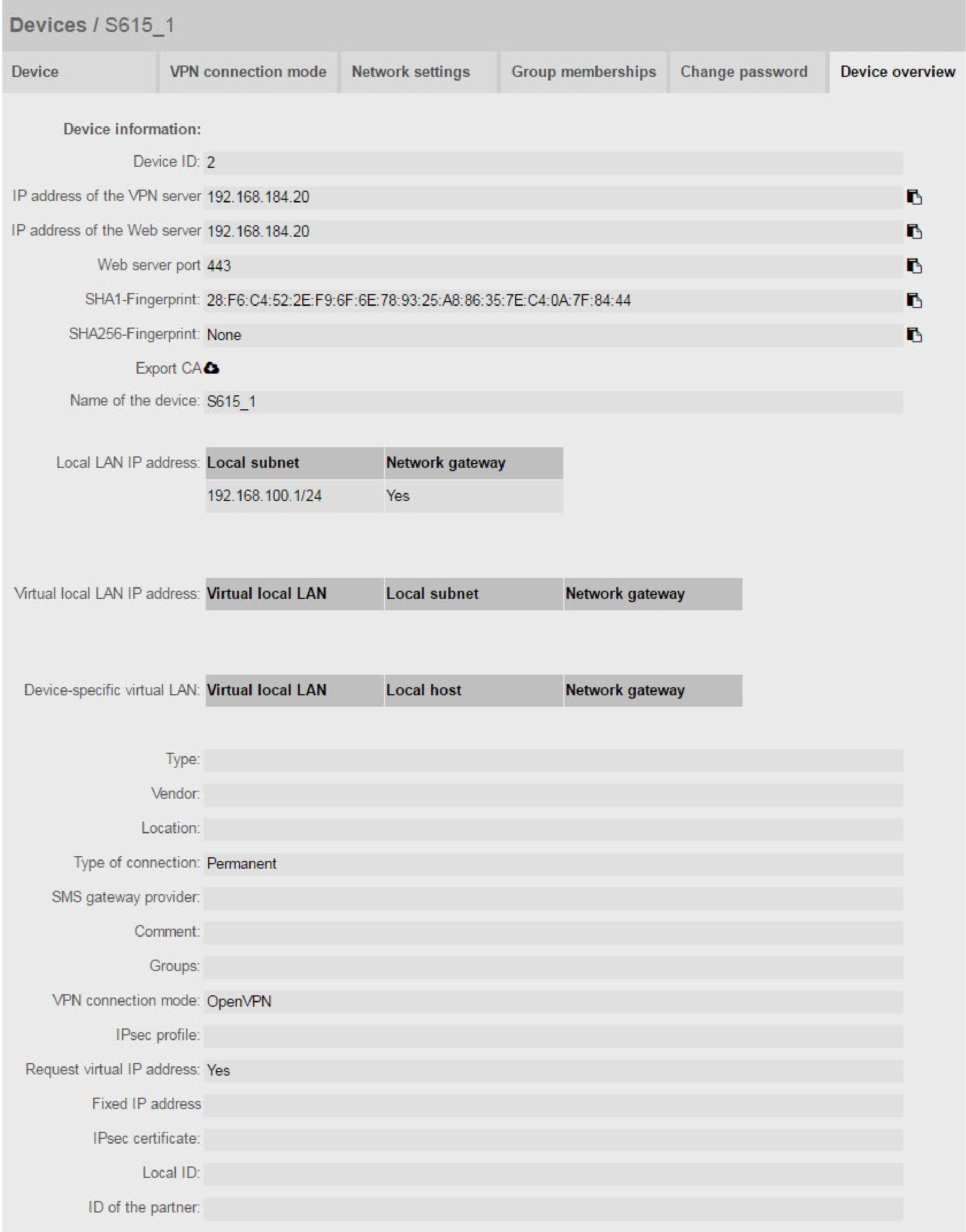
13. Click "Complete".

Result

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

- Device password
- Device ID
- Fingerprint

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



Devices / S615_1

Device information:

Device ID: 2

IP address of the VPN server 192.168.184.20

IP address of the Web server 192.168.184.20

Web server port 443

SHA1-Fingerprint: 28:F6:C4:52:2E:F9:6F:6E:78:93:25:A8:86:35:7E:C4:0A:7F:84:44

SHA256-Fingerprint: None

Export CA

Name of the device: S615_1

Local LAN IP address:

Local subnet	Network gateway
192.168.100.1/24	Yes

Virtual local LAN IP address:

Virtual local LAN	Local subnet	Network gateway

Device-specific virtual LAN:

Virtual local LAN	Local host	Network gateway

Type:

Vendor:

Location:

Type of connection: Permanent

SMS gateway provider:

Comment:

Groups:

VPN connection mode: OpenVPN

IPsec profile:

Request virtual IP address: Yes

Fixed IP address

IPsec certificate:

Local ID:

ID of the partner:

3.3.3 Configure communications relations

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

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

from group	to the destination group
Service	Station1
	Station2
Station1	Station2

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

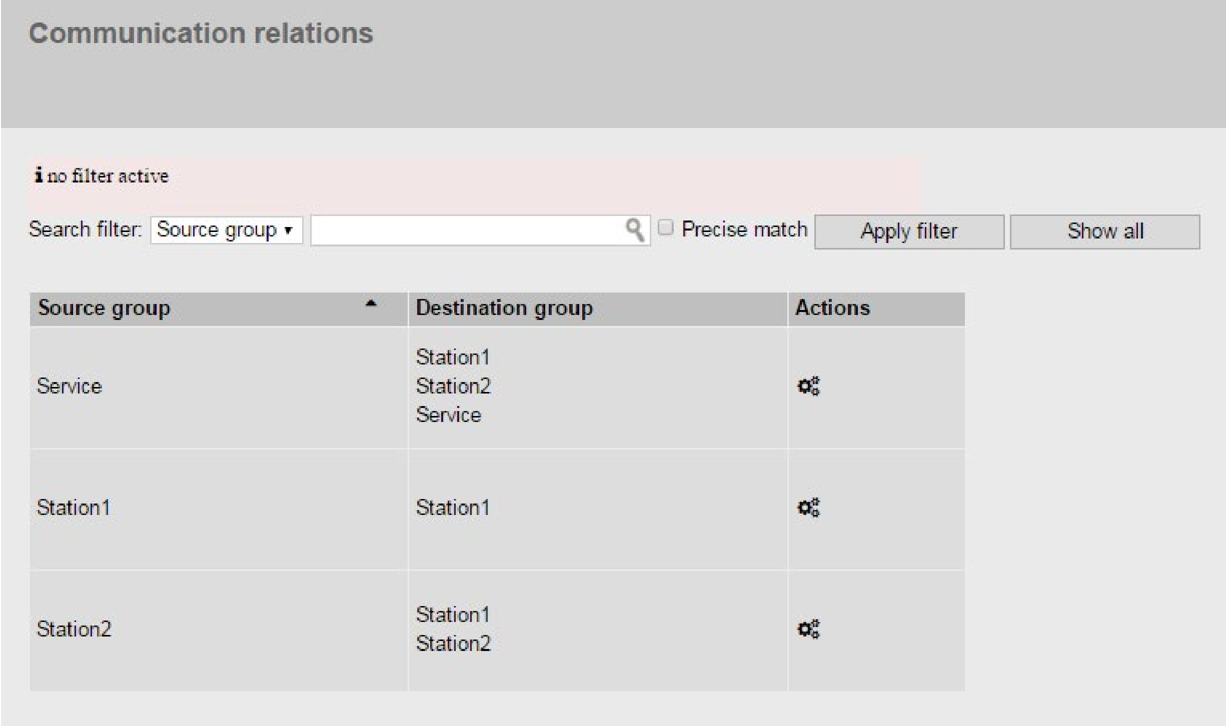
Procedure

1. In the navigation area, click "Remote connections" > "Participant groups". The participant groups that have already been created are listed in the content area.
2. For "Station1" in the "Actions" column click on the icon ⇄. The page "Destination group" is opened.
3. Enable "Station2" and click on "Save".
4. Click "Exit dialog".
5. For "Service", click the symbol ⇄ in the "Actions" column. The page "Destination group" is opened.
6. Enable "Station1" and "Station2". Click "Save".
7. Click "Exit dialog".

Result

The communication relations have been created.

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



Communication relations

i no filter active

Search filter: Source group ▾ □ Precise match Apply filter Show all

Source group ▲	Destination group	Actions
Service	Station1 Station2 Service	⚙
Station1	Station1	⚙
Station2	Station1 Station2	⚙

3.4 Configure the remote connection on the S615

3.4.1 Secure OpenVPN connection with fingerprint

Requirement

- On PC1/2 there are two Web browser windows open.
- Web browser 1 for access to Web Based Management of the SCALANCE S615.
- Web browser 2 for access to SINEMA RC.
- A valid KEY-PLUG is inserted in the S615.

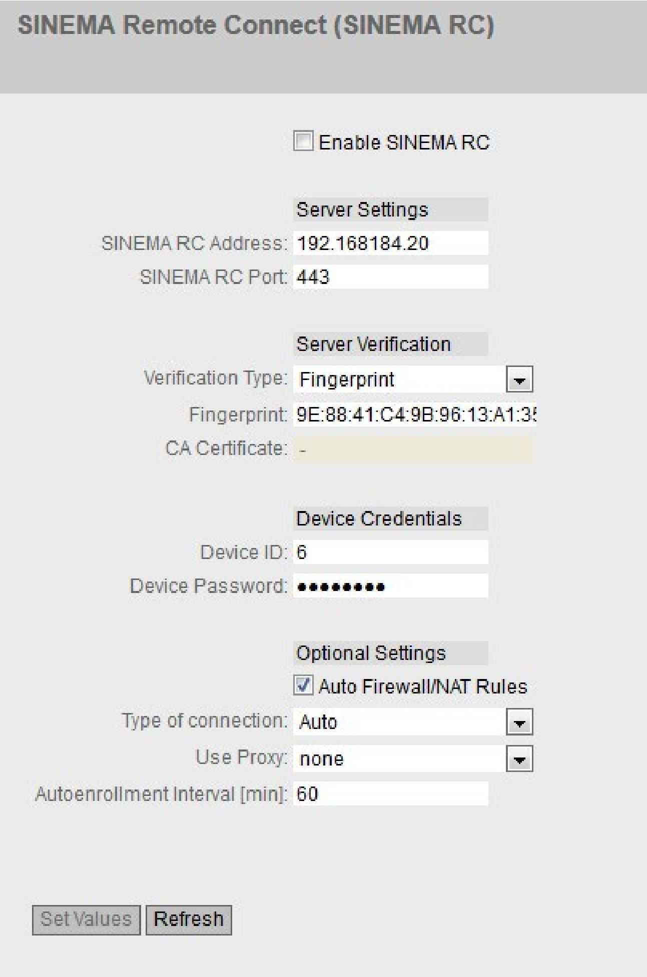
Procedure

1. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - In the address box of the Web browser, enter the LAN IP address of the S615, see table "Settings used (Page 45)".
   - Log in as the "admin" user and with the corresponding password.
   - Click "System" > "SINEMA RC" in the navigation area.
   - For "Sinema RC Address", enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 45)".
2. Change to the Web browser for access to SINEMA RC.
   - In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 45)".
   - Log in as the "admin" user and the corresponding password.
   - In the navigation area, click "Remote connections" > "Devices".
   - Click on the symbol ℹ in "Actions" to open the device information.
   - Holding down the left mouse button, select the entry for device ID.
   - Right-click on the selection and in the shortcut menu, select the copy command.
3. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - Right click in the input box of "Device ID".
   - In the shortcut menu, select the menu command for inserting.
   - For "Device Password" enter the password that you configured for access, An:t_010 for S615_1 and An:t_020 for S615_2
   - Enable "Auto Firewall/NAT Rules"

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

     For "Verification Type", select "Fingerprint".

4. Change to the Web browser for access to SINEMA RC.
   - For "Fingerprint" click on the icon 📋.
5. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - Right click in the input box of "Fingerprint".
   - In the shortcut menu, select the menu command for inserting.
   - Activate "Enable SINEMA RC" and click on "Set Values".



SINEMA Remote Connect (SINEMA RC)

☐ Enable SINEMA RC

Server Settings
SINEMA RC Address: 192.168184.20
SINEMA RC Port: 443

Server Verification
Verification Type: Fingerprint
Fingerprint: 9E:88:41:C4:9B:96:13:A1:3
CA Certificate: -

Device Credentials
Device ID: 6
Device Password: ●●●●●●●●

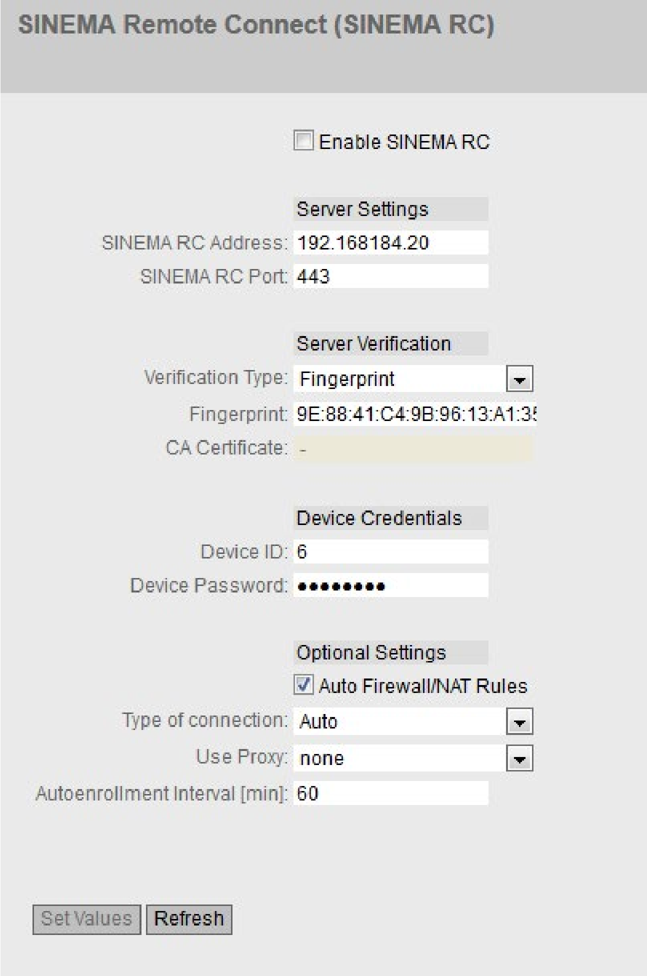
Optional Settings
☑ Auto Firewall/NAT Rules
Type of connection: Auto
Use Proxy: none
Autoenrollment Interval [min]: 60

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.

In the Web browser for access to Web Based Management of SCALANCE S615: In the navigation area, click "Information" > "SINEMA RC".



SINEMA Remote Connect (SINEMA RC)

☐ Enable SINEMA RC

Server Settings

SINEMA RC Address:	192.168184.20
SINEMA RC Port:	443

Server Verification

Verification Type:	Fingerprint
Fingerprint:	9E:88:41:C4:9B:96:13:A1:3!
CA Certificate:	-

Device Credentials

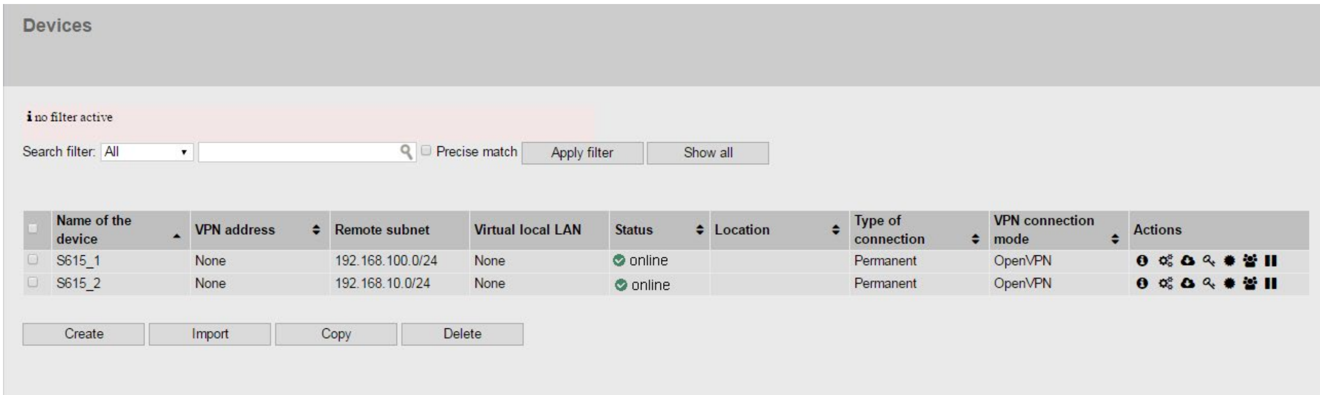
Device ID:	6
Device Password:	●●●●●●●●

Optional Settings

☑ Auto Firewall/NAT Rules

Type of connection:	Auto
Use Proxy:	none
Autoenrollment Interval [min]:	60

Web browser for access to SINEMA RC: Click "Remote connections" > "Devices" in the navigation area.



Devices

i no filter active

Search filter: All ☐ Precise match

☐	Name of the device	VPN address	Remote subnet	Virtual local LAN	Status	Location	Type of connection	VPN connection mode	Actions
☐	S615_1	None	192.168.100.0/24	None	✓ online		Permanent	OpenVPN	
☐	S615_2	None	192.168.10.0/24	None	✓ online		Permanent	OpenVPN	

3.4.2 Secure OpenVPN connection with CA certificate

3.4.2.1 Loading a certificate

Requirement

- The correct time is set on the S615 and the SINEMA RC Server.
- On PC1/2 there are two Web browser windows open.

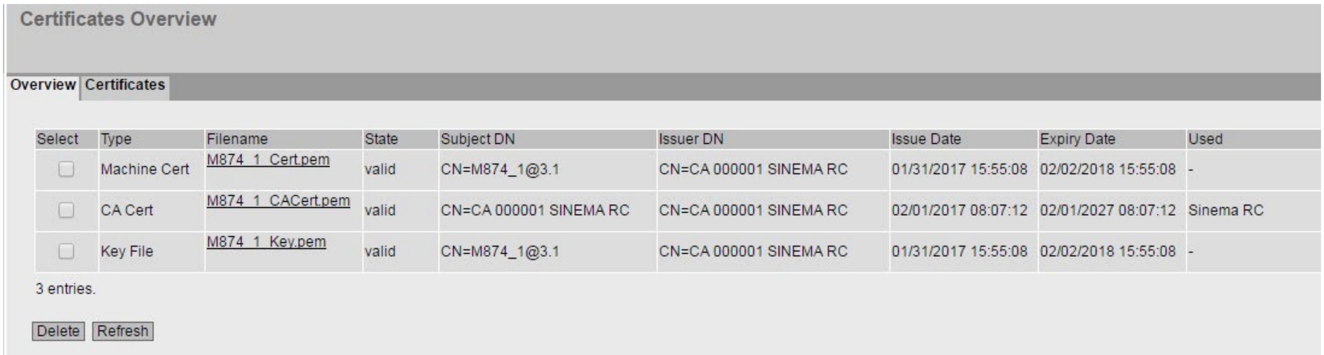
Procedure

1. Change to the Web browser for access to SINEMA RC.
   - In the address box of the Web browser, enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 45)".
   - Log in as the "admin" user and the corresponding password.
   - Click "Security" > "Certificates" in the navigation area.
   - Click on the ☁ symbol in "Actions" to export the certificate.
2. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - In the address box of the Web browser, enter the LAN IP address of the S615, see table "Settings used (Page 45)".
   - Log in as the "admin" user and with the corresponding password.
   - Click on "System" > "Load&Save" in the navigation area and on the "Passwords"" tab in the content area.
   - Enter the device password in "X509Cert". Enable the entry and click on "Set Values".
   - Click on the "HTTP" tab in the content area.
   - Click the "Load" button next to "X509Cert". The dialog for loading a file is opened.
   - Navigate to the exported server certificate. Click the "Open" button in the dialog.

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

Result

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



Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
□	Machine Cert	M874_1_Cert.pem	valid	CN=M874_1@3.1	CN=CA 000001 SINEMA RC	01/31/2017 15:55:08	02/02/2018 15:55:08	-
□	CA Cert	M874_1_CACert.pem	valid	CN=CA 000001 SINEMA RC	CN=CA 000001 SINEMA RC	02/01/2017 08:07:12	02/01/2027 08:07:12	Sinema RC
□	Key File	M874_1_Key.pem	valid	CN=M874_1@3.1	CN=CA 000001 SINEMA RC	01/31/2017 15:55:08	02/02/2018 15:55:08	-

3 entries.

3.4.2.2 Configure an OpenVPN connection to the SINEMA RC Server

Requirement

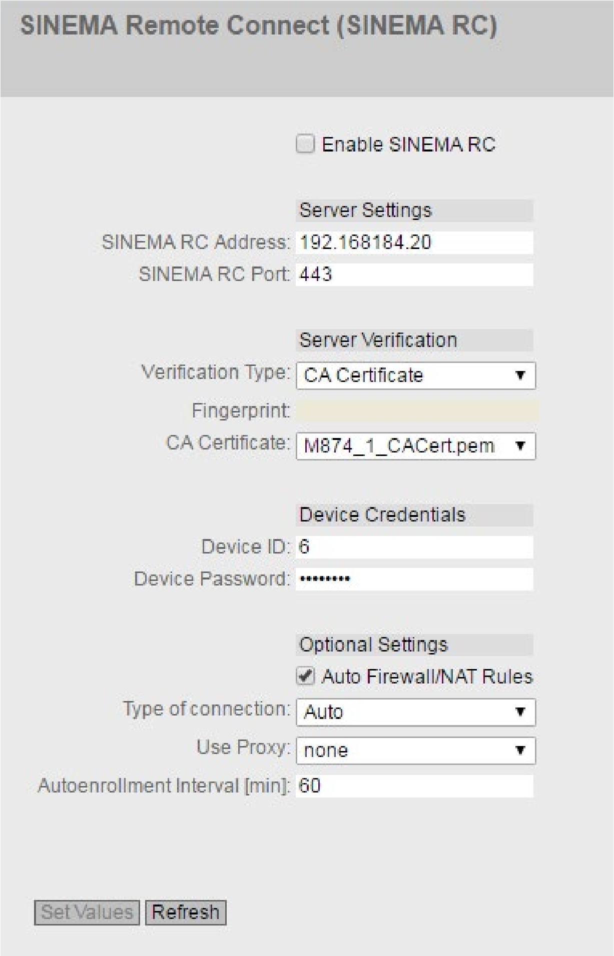
- A valid KEY-PLUG is inserted in the S615.

Procedure

1. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - Click "System > SINEMA RC" in the navigation area.
   - For "Sinema RC Address", enter the WAN IP address of the SINEMA RC Server, see table "Settings used (Page 45)".
2. Change to the Web browser for access to SINEMA RC.
   - In the navigation area, click "Remote connections" > "Devices".
   - Click on the symbol ℹ in "Actions" to open the device information.
   - Holding down the left mouse button, select the entry for device ID.
   - Right-click on the selection and in the shortcut menu, select the copy command.
3. Change to the Web browser for access to Web Based Management of the SCALANCE S615.
   - Right click in the input box of "Device ID".
   - In the shortcut menu, select the menu command for inserting.
   - For "Device Password" enter the password that you configured for access, An:t_010 for S615-1 and An:t_020 for S615-2.
   - Enable "Auto Firewall / NAT Rules".

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

     For "Verification Type" select "CA Certificate".
   - In "CA Certificate" select the server certificate. Only loaded certificates can be selected.



SINEMA Remote Connect (SINEMA RC)

□ Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168184.20
SINEMA RC Port: 443

Server Verification

Verification Type: CA Certificate
Fingerprint:
CA Certificate: M874_1_CACert.pem

Device Credentials

Device ID: 6
Device Password: ••••••••

Optional Settings

☑ Auto Firewall/NAT Rules
Type of connection: Auto
Use Proxy: none
Autoenrollment Interval [min]: 60

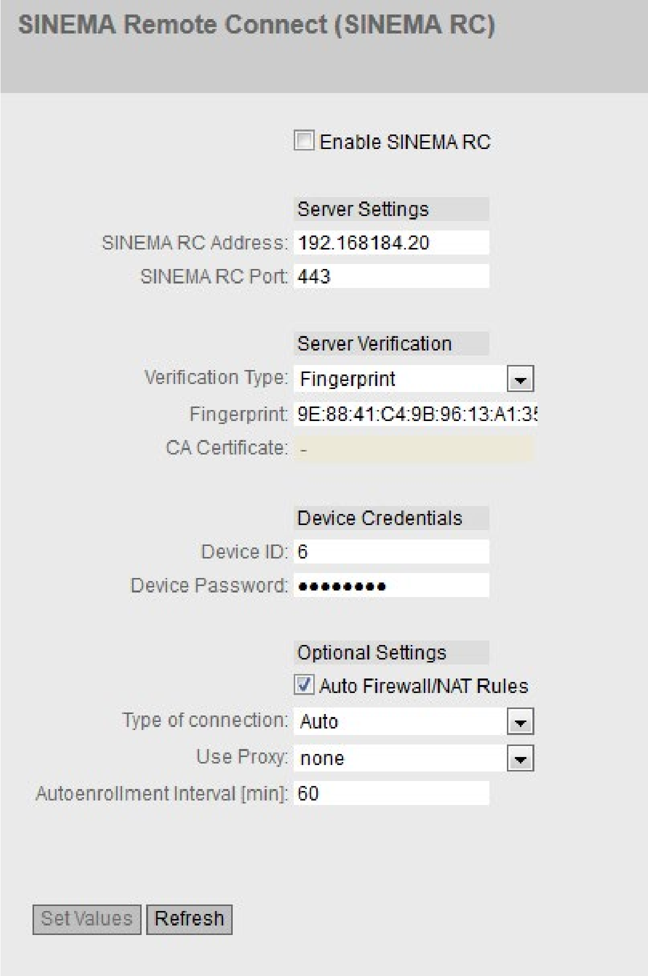
– Activate "Enable SINEMA RC" and click on "Set Values".

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, click "Information" > "SINEMA RC".



SINEMA Remote Connect (SINEMA RC)

☐ Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168184.20

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint: 9E:88:41:C4:9B:96:13:A1:3

CA Certificate: -

Device Credentials

Device ID: 6

Device Password: ●●●●●●●●●

Optional Settings

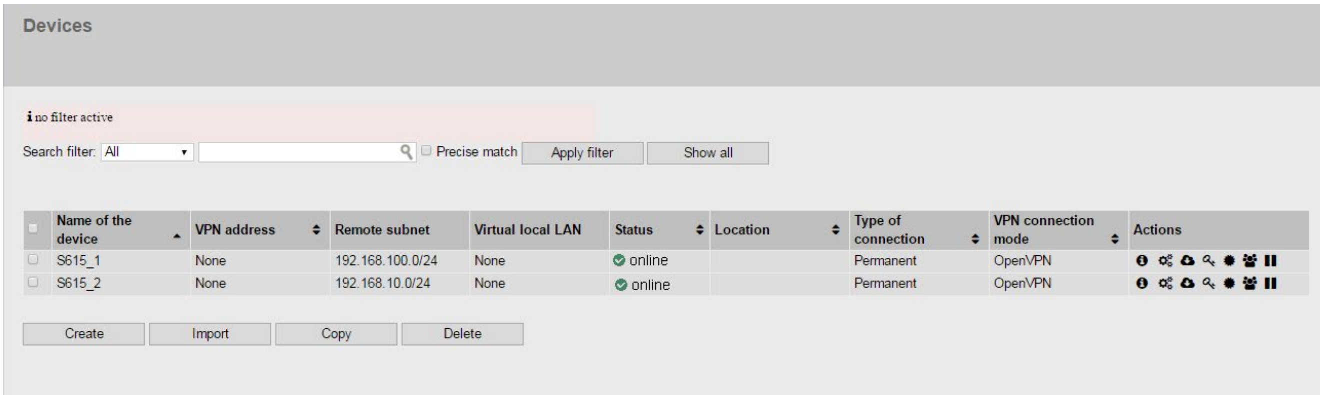
☑ Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

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



Devices

no filter active

Search filter: All ☐ Precise match

☐	Name of the device	VPN address	Remote subnet	Virtual local LAN	Status	Location	Type of connection	VPN connection mode	Actions
☐	S615_1	None	192.168.100.0/24	None	✓ online		Permanent	OpenVPN	
☐	S615_2	None	192.168.10.0/24	None	✓ online		Permanent	OpenVPN	

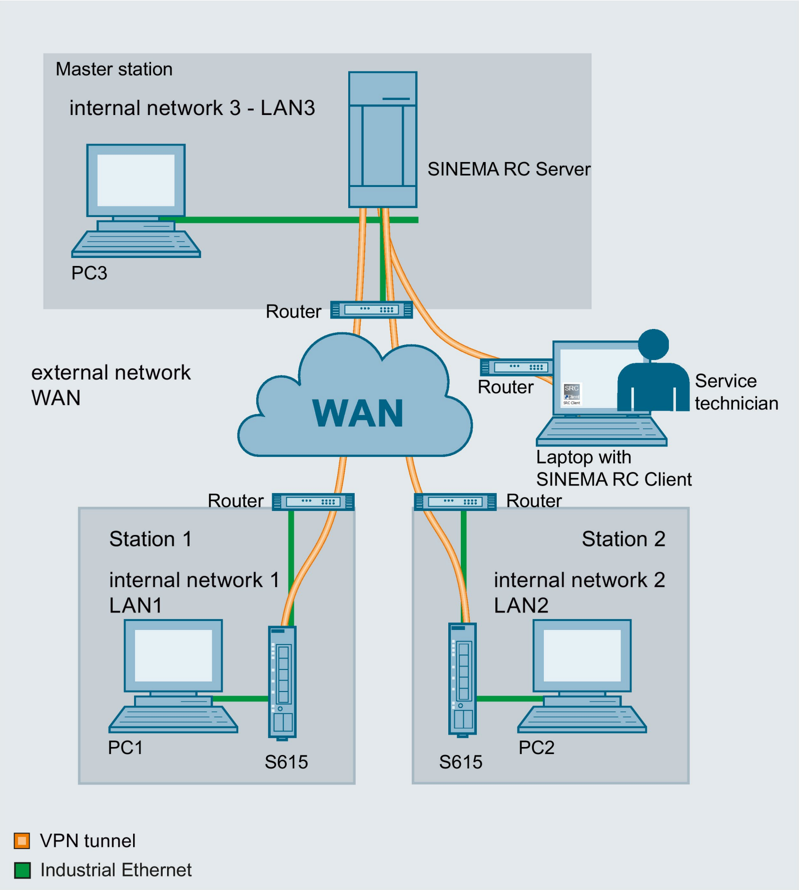
OpenVPN tunnel between SINEMA RC Client and SINEMA RC Server 4

4.1 Procedure in principle

This example expands the configuration example "OpenVPN tunnel between SCALANCE S615 and SINEMA RC Server (Page 23)".

A service technician starts the SINEMA RC Client on a laptop and logs on to the SINEMA RC Server with his or her user data. The VPN tunnel between the SINEMA RC Client and the SINEMA RC Server is established after successful authentication.

Structure



Master station - connection to SINEMA RC Server

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

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

Station 1 / 2 - Connection to SCALANCE S615

- In the test setup in the internal network, a network node is implemented by a PC connected to the Ethernet interface P1 of the S615.
  - PC: represents a participant in internal network 1/2
  - S615: SCALANCE S module for protection of the internal network 1/2
- Connection to the external network via a router

  Access to the external network is via a router connected to the Ethernet interface P5 of the S615.

Service technician - connection to SINEMA RC Client

- Connection to the external network via a router

  Access to the external network is via a router connected to the Ethernet interface of the laptop.

Required devices/components

Use the following components for setup:

- 2 x S615 (additional option: a suitably installed standard rail with fittings)
- 2 x 24 V power supply with cable connector and terminal block plug
- 2 x PC each connected to a SCALANCE S615.
- 1 x PC on which the SINEMA RC Server is installed.
- 1 x PC that is connected to the SINEMA RC Server.
- 1 x laptop
- 4 x 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:

	Name	Interface	IP address
Station -1 LAN1	S615-1	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
	PC1	LAN port	192.168.100.20 255.255.255.0
	Router1	LAN port	192.168.50.2 255.255.255.0
Station-2 LAN2	S615-2	LAN port P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN port P5 (vlan2)	192.168.40.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.40.2
	PC2	Ethernet (LAN 2)	192.168.10.20 255.255.255.0
	Router 2	LAN port	192.168.40.2 255.255.255.0
Master station LAN3	SINEMA RC Server	WAN port	192.168.20.250 255.255.255.0 The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example. 192.168.184.20 Default gateway is the LAN IP address of the router 192.168.20.2
	PC3	Ethernet (LAN3)	192.168.20.20 255.255.255.0
	Router 3	LAN port	192.168.20.2 255.255.255.0
		WAN port	192.168.184.20
Service technician	Laptop	Ethernet	192.168.1.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.1.2
	Router 4	LAN port	192.168.1.2 255.255.255.0
		WAN port	WAN IP address is assigned by the 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, see "Connecting the SINEMA RC Server to the WAN (Page 9)".
- The SINEMA RC Server can be reached via PC3.

SINEMA RC client

- The laptop is connected to the WAN.

Steps in configuration

1. Create a user on the SINEMA RC Server (Page 49)

On the laptop of the service technician

1. Installing SINEMA RC Client (Page 51)
2. Logging SINEMA RC Client on to SINEMA RC Server (Page 53)

4.2 Create a user on the SINEMA RC Server

In this configuration example, access via the SINEMA RC Client is handled by a service technician. To log on, the service technician requires a user name and a password.

The administrator creates the user data on the master station.

Requirement

- The SINEMA RC Server can be reached via PC3.
- The "Service" participant group has been created, refer to the section "Creating participant groups (Page 30)"

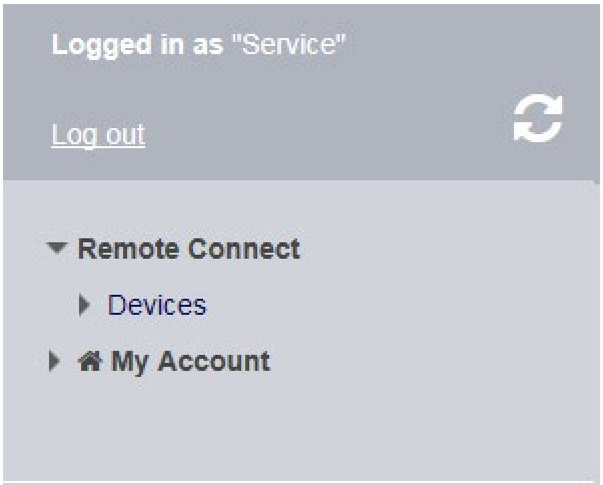
Create users

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 45)".
2. Log on with the user data of the administrator, see section "Starting Web Based Management".
3. In the navigation area, click "User accounts" > "Users and roles". The users that have already been created are listed in the content area.
4. Click "Create". The "New User" page is opened.
5. Enter the user name e.g. Service.
6. As "Login method", select "Password" and click "Next".
7. The "Rights" tab is displayed. Specify the rights for the service technician and click on "Next"
8. The "Group memberships" tab is displayed. Enable the "Service" participant group.
9. Click "Continue". The "VPN connection mode" tab is displayed.
10. Activate the VPN connection mode "Open VPN".
11. Click "Continue". The "Password" tab is displayed.
12. Specify the password for the user e.g. Di1S+Xo? and click "Finish".

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.


Logged in as "Service"
Log out
Remote Connect
Devices
My Account

4.3 On the laptop of the service technician

4.3.1 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 64-bit + Service Pack 1 (requirement: NET 3.5 or higher is installed)
- Microsoft Windows 10 Professional 64-bit
  Please note for SINEMA RC Client V1.0 SP3, secure boot is not supported. The parameter “nointegritychecks on" must be set.
- 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.

4.3.2 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 "Create a user on the SINEMA RC Server (Page 49)".

Procedure

1. Double-click on the "SINEMA RC Client" icon on your desktop. The SINEMA RC Client starts.
2. Enter the WAN IP address of the SINEMA RC Server as the IP address, refer to the table "Settings used (Page 45)".
3. Enter "Service" as the user name and as the password e.g. Di1S+Xo? Click the "Log on" button.

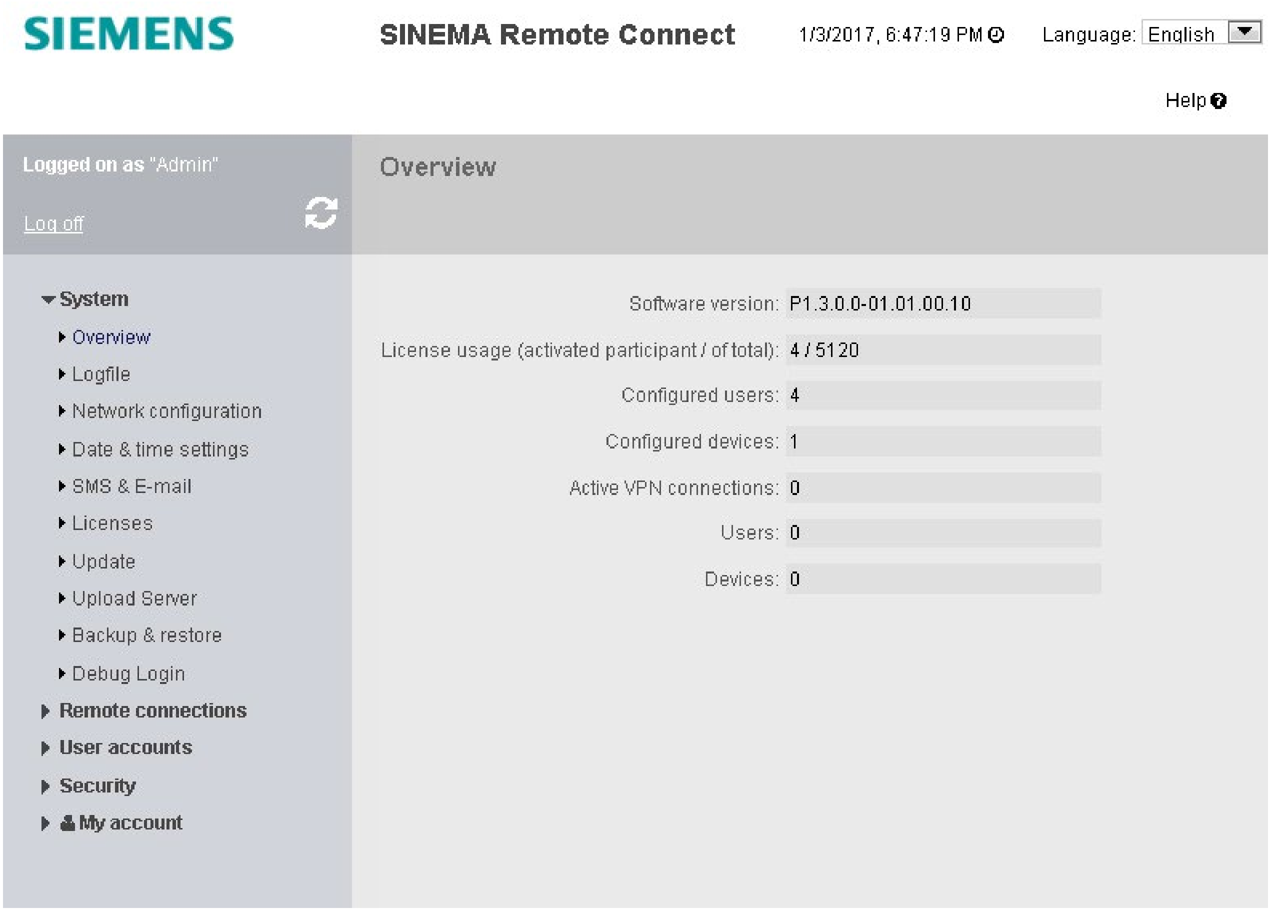
   After logging on successfully, the start page is displayed.
4. Click the "Open VPN tunnel" button.

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.



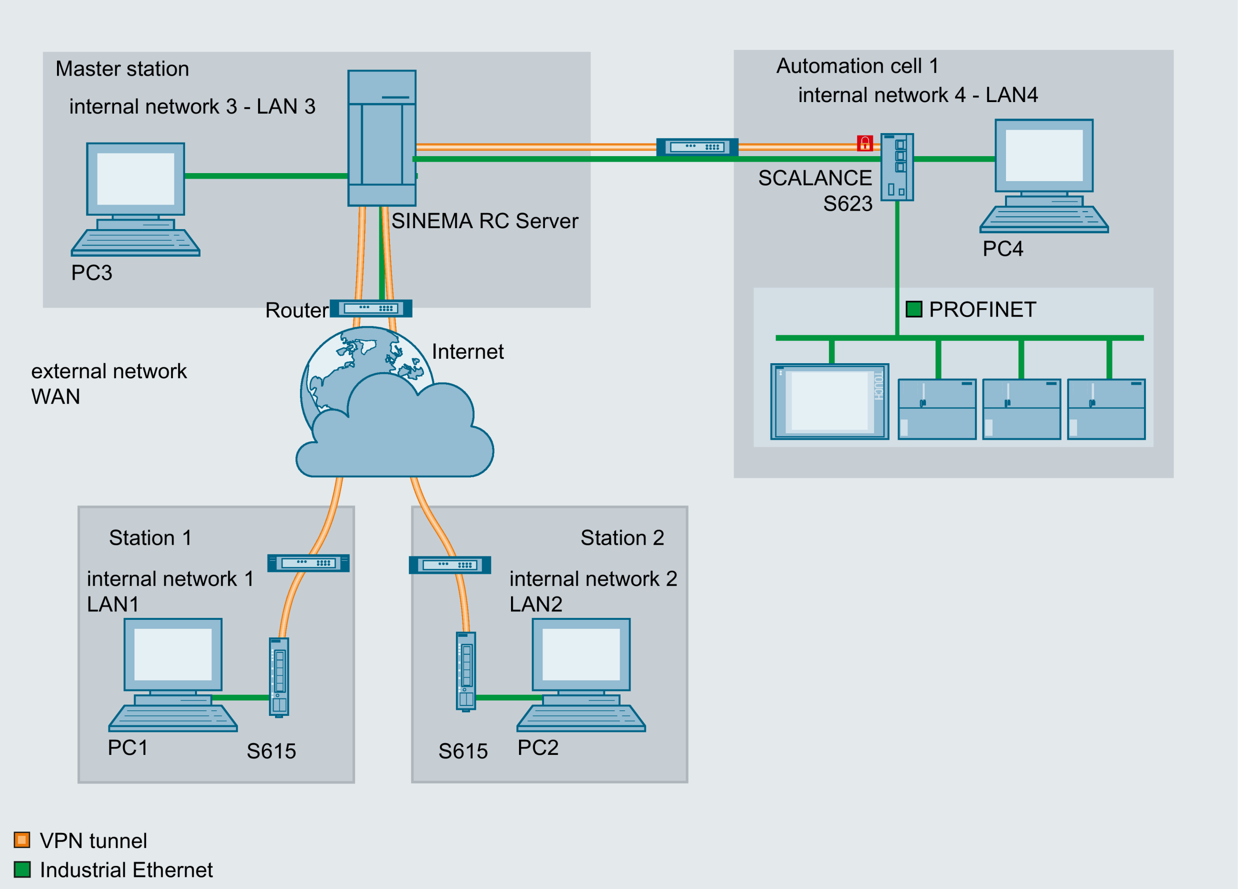
Software version: P1.3.0.0-01.01.00.10
License usage (activated participant / of total): 4 / 5120
Configured users: 4
Configured devices: 1
Active VPN connections: 0
Users: 0
Devices: 0

IPsecVPN tunnel between SINEMA RC Server and S623 5

5.1 Procedure in principle

In this example the configuration from "OpenVPN tunnel between SCALANCE S615 and SINEMA RC Server" is expanded. The security module SCALANCE S623 and the SINEMA RC Server form the two endpoints of a VPN tunnel. In this case, the VPN tunnel is set up between the DMZ interface of the SCALANCE S623 module and the WAN interface of the SINEMA RC Server. On the SINEMA RC Server the security modules are participants in the same group, so that the SCALANCE S623 can exchange data with the SCALANCE S615.

Structure



Master station - connection to SINEMA RC Server

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

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

Station 1 - connection to SCALANCE M87x

- 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 internal network 1
  - M-800: SCALANCE M module for protection of the internal network 1
- Connection to the external, public network:
  - Wireless via the antenna of the M874 to the mobile wireless network.

Station 2 - connection to SCALANCE S615

- In the test setup in the internal network, a network node is implemented by a PC connected to the Ethernet interface P1 of the S615.
  - PC: represents a participant in internal network 2
  - S615: SCALANCE S module for protection of the internal network 2
- Connection to the external network via a router

  Access to the external network is via a router connected to the Ethernet interface P5 of the S615.

Automation cell 1 - connection to SCALANCE S623

- Internal network - attachment to the internal interface of the security module

  Both internal networks include a PC connected to the internal interface of the security module.
  - PC4: Represents a node in internal network 4
- External network - attachment to the external interface of the security module

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

Settings used

	Name	Interface	IP address
Station1 LAN1	S615_1	LAN port P1 (vlan1)	192.168.100.1 255.255.255.0
		LAN 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
	PC1	LAN port	192.168.100.20 255.255.255.0
	Router1	LAN port	192.168.50.2 255.255.255.0
Station2 LAN2	S615_2	LAN port P1 (vlan1)	192.168.10.1 255.255.255.0
		LAN port P5 (vlan2)	192.168.40.1 255.255.255.0 Default gateway is the LAN IP address of the router 192.168.40.2
	PC2	Ethernet (LAN 2)	192.168.10.20 255.255.255.0
	Router 2	LAN port	192.168.40.2 255.255.255.0
Master station LAN3	SINEMA RC Server	LAN port	192.168.20.250 255.255.255.0 The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example. 192.168.184.20 Default gateway is the LAN IP address of the router 192.168.20.2
	PC3	Ethernet (LAN3)	192.168.20.20 255.255.255.0
	Router 3	LAN port	192.168.20.2 255.255.255.0
		LAN port	192.168.184.20
Automation cell LAN4	S623	External port P1	192.168.8.1 255.255.255.0
		Internal port (LAN4) P2	192.168.5.100 255.255.255.0
	PC4	Ethernet (LAN4)	192.168.5.20 255.255.255.0

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, see "Connecting the SINEMA RC Server to the WAN (Page 9)".
- You are logged on to the SINEMA RC Server.

SCALANCE S615

- The SCALANCE S is connected to the WAN. You will find the configuration steps in the 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 55)".
- The SCALANCE S can be reached via PC1/2 and you are logged on to the WBM as "admin".
- A valid KEY-PLUG SINEMA Remote Connect is inserted in the SCALANCE S.

SCALANCE S623

- The SCALANCE S623 is connected to the WAN. You will find the configuration in the Getting Started "Setting up security".

  The steps in configuration are the same for all devices, the only difference being the settings, see table "Settings used (Page 55)".
- The SCALANCE S623 can be reached via PC 4
- On the PC4, the Security Configuration Tool V4.x is installed.

Steps in configuration

Configuring a VPN tunnel with SCT

1. Create project and module with the SCT (Page 60)
2. Configure VPN group (Page 63)
3. Configure the properties of the SCALANCE S623 (Page 64)
4. Configure the properties of the SINEMA RC Server (Page 65)
5. Configure VPN connection (Page 66)
6. Download the configuration to the SCALANCE S623 and save the SINEMA RC configuration (Page 68)

Configure a remote connection on the SINEMA RC Server

1. Create IPsec profile (Page 69)
2. Load certificate (Page 70)
3. Create device (Page 72)

5.2 Configuring a VPN tunnel with SCT

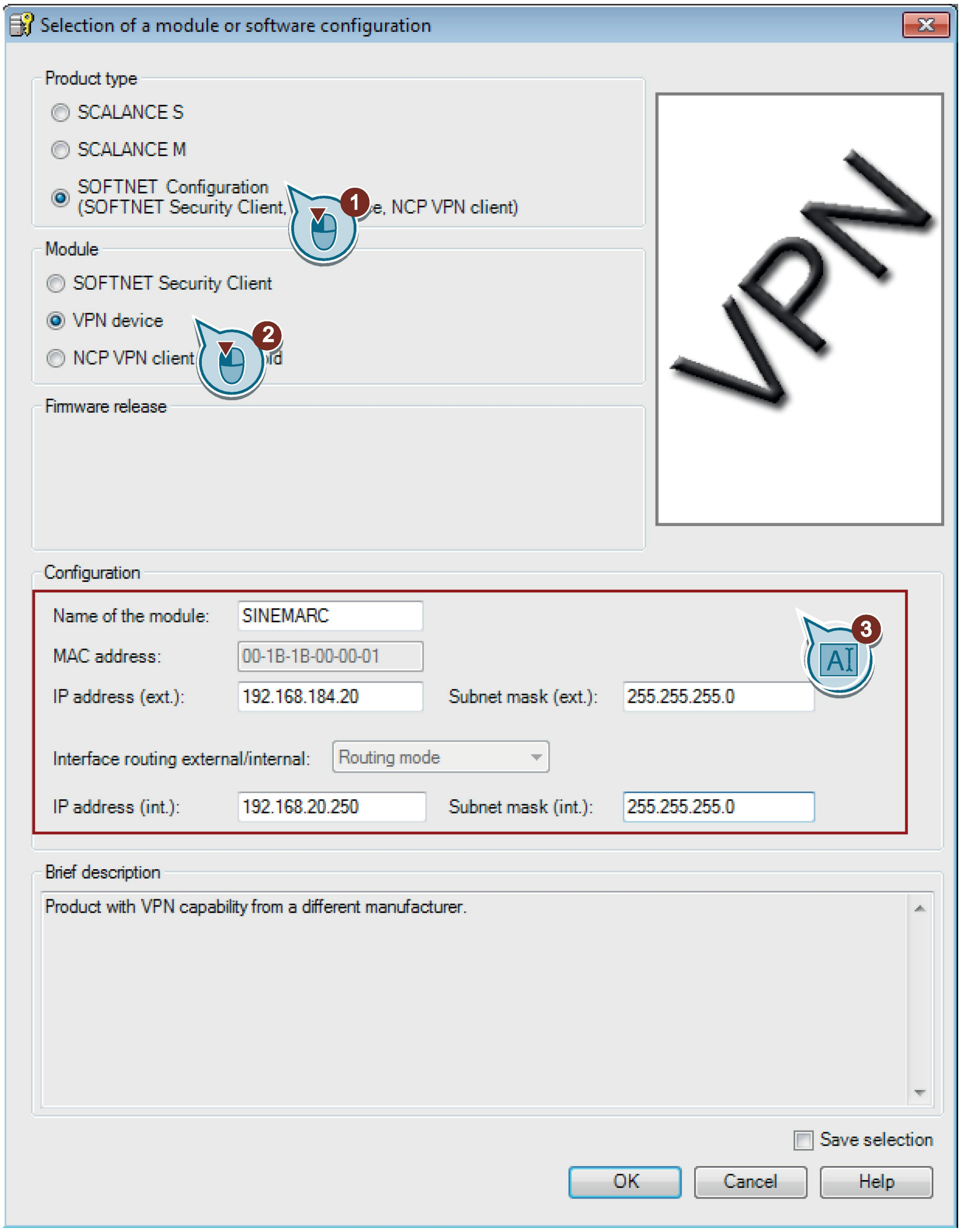
5.2.1 Create project and modules with the SCT

Procedure

1. Start the Security Configuration Tool V4.x on the PC.
2. Select the "Project" > "New..." menu command.
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 SINEMA RC from the "Settings used (Page 55)" table.

   The VPN device is a substitute for the SINEMA RC Server.



Selection of a module or software configuration

Product type
○ SCALANCE S
○ SCALANCE M
● SOFTNET Configuration (SOFTNET Security Client, ...e, NCP VPN client)

Module
○ SOFTNET Security Client
● VPN device
○ NCP VPN client ...id

Firmware release

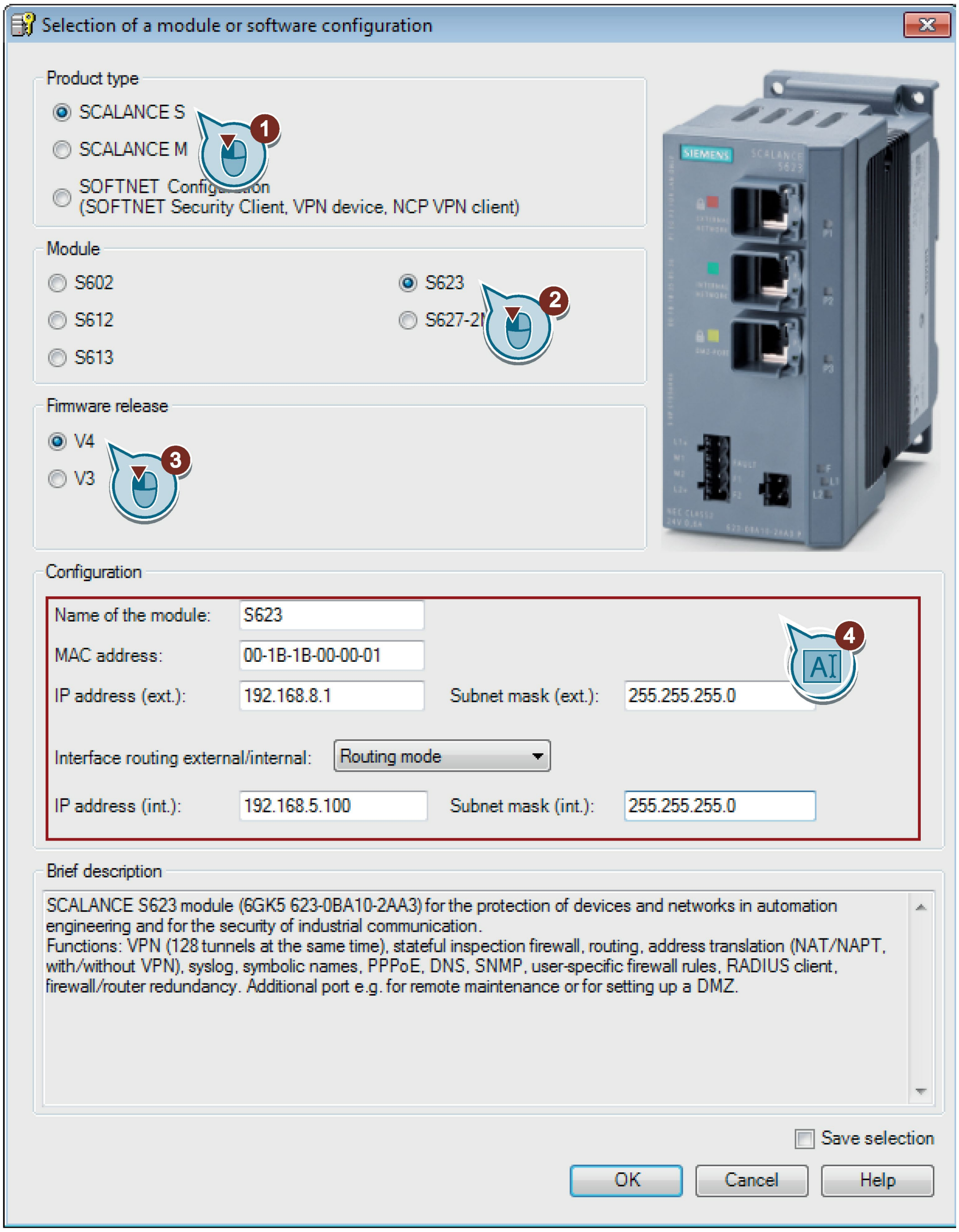
Configuration
Name of the module: SINEMARC
MAC address: 00-1B-1B-00-00-01
IP address (ext.): 192.168.184.20 Subnet mask (ext.): 255.255.255.0
Interface routing external/internal: Routing mode
IP address (int.): 192.168.20.250 Subnet mask (int.): 255.255.255.0

Brief description
Product with VPN capability from a different manufacturer.

□ Save selection

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

8. Enter the values assigned to the SCALANCE S623 from the "Settings used (Page 55)" table. In addition to this, enter the MAC address printed on the front of the security module



Selection of a module or software configuration

Product type

- ● SCALANCE S
- ○ SCALANCE M
- ○ SOFTNET Configuration (SOFTNET Security Client, VPN device, NCP VPN client)

Module

- ○ S602
- ○ S612
- ○ S613
- ● S623
- ○ S627-2M

Firmware release

- ● V4
- ○ V3

Configuration

Name of the module:	S623		
MAC address:	00-1B-1B-00-00-01		
IP address (ext.):	192.168.8.1	Subnet mask (ext.):	255.255.255.0
Interface routing external/internal:	Routing mode		
IP address (int.):	192.168.5.100	Subnet mask (int.):	255.255.255.0

Brief description

SCALANCE S623 module (6GK5 623-0BA10-2AA3) for the protection of devices and networks in automation engineering and for the security of industrial communication.
Functions: VPN (128 tunnels at the same time), stateful inspection firewall, routing, address translation (NAT/NAPT, with/without VPN), syslog, symbolic names, PPPoE, DNS, SNMP, user-specific firewall rules, RADIUS client, firewall/router redundancy. Additional port e.g. for remote maintenance or for setting up a DMZ.

□ Save selection

9. Close the dialog with "OK".

Result

The VPN device and the security module SCALANCE S623 will then be displayed in the list of configured modules.

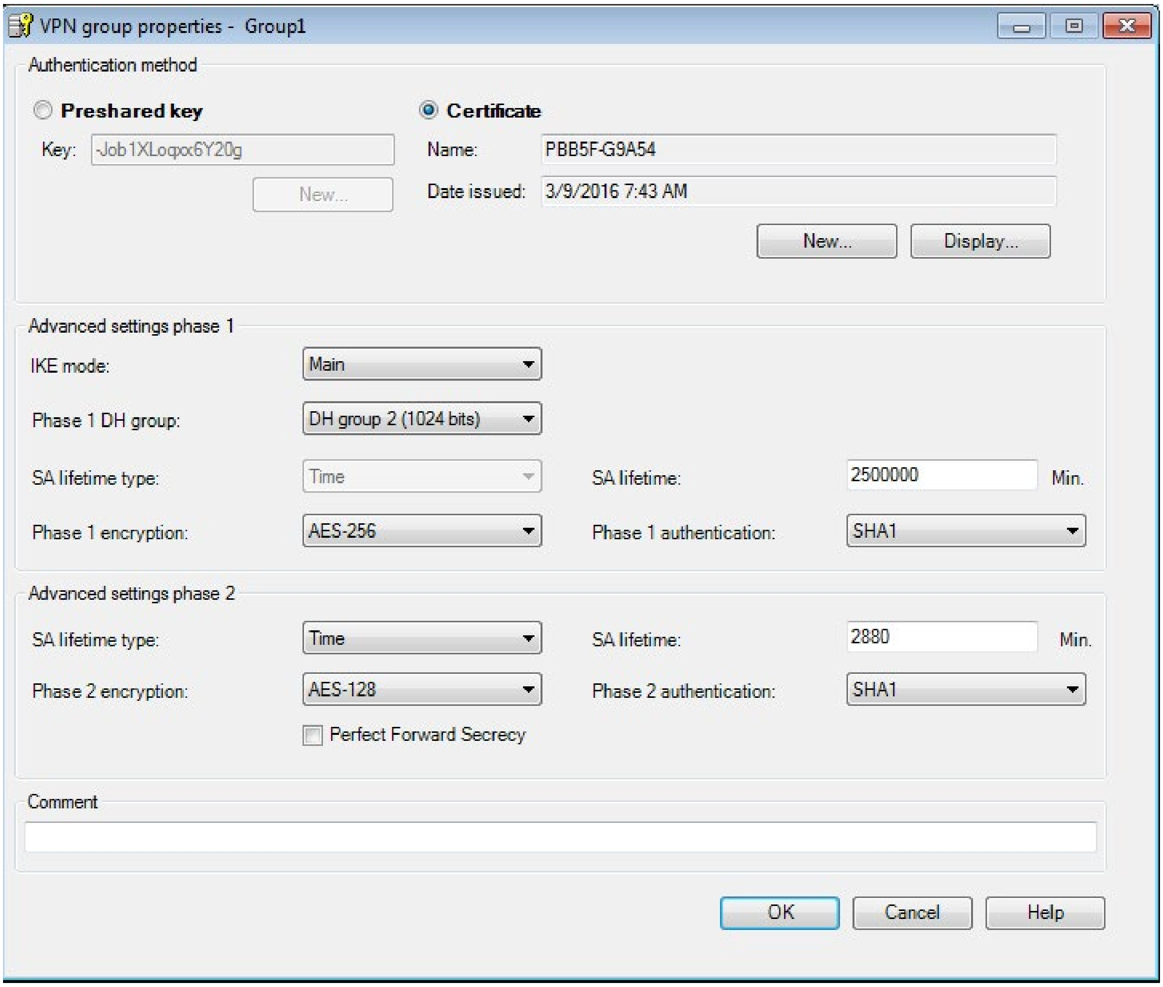
5.2.2 Configuring a VPN group

Only when the SINEMA RC Server and the security module S623 are assigned to the same VPN group can a VPN connection be established for secure communication.

Procedure

1. Select the "VPN groups" folder in the navigation panel and create a new VPN group with the menu command "Insert" > "Group". The VPN group is automatically given the name "Group1".
2. Select the "All modules" entry in the navigation panel.
3. Select the VPN device "SINEMARC" and the security module S623 in the content area. Drag the modules to "Group1". Both modules are now assigned to the VPN group "Group1".
4. Change to advanced mode with the menu command "View" > "Advanced mode".

5. Open the VPN group properties of the VPN group "Group 1" by selecting the "Properties ..." command in the shortcut menu.
6. For this configuration example, configure the group properties with the following settings.



VPN group properties - Group1

Authentication method

○ **Preshared key**

Key: -Job1XLoqxx6Y20g

● **Certificate**

Name: PBB5F-G9A54

Date issued: 3/9/2016 7:43 AM

Advanced settings phase 1

IKE mode: Main

Phase 1 DH group: DH group 2 (1024 bits)

SA lifetime type: Time

SA lifetime: 2500000 Min.

Phase 1 encryption: AES-256

Phase 1 authentication: SHA1

Advanced settings phase 2

SA lifetime type: Time

SA lifetime: 2880 Min.

Phase 2 encryption: AES-128

Phase 2 authentication: SHA1

□ Perfect Forward Secrecy

Comment

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 VPN connection is complete.

5.2.3 Configuring the properties of the S623

The security module S623 establishes the VPN connection to the SINEMA RC Server via the DMZ interface. To do this the properties of the S623 must be configured accordingly.

Procedure

1. Select the security module S623 in the content area and select the "Edit" > "Properties..." menu command.
2. Click the "Interfaces" tab.
3. In the area "DMZ port (X3)", enable the check box "Activate the interface".
4. In the "IP assignment" drop down list, select the entry "PPPoE" and click "Apply".
5. On the "Internet connection" tab, enter the data with which you authenticate yourself with your Internet Service Provider (ISP).
6. Click "Apply".
7. Click the "VPN" tab.
8. From the "Permission to initiate connection establishment" drop-down list, select the "Start connection to partner (initiator/responder)" entry.
9. In the "WAN IP address / FQDN" input box enter the IP address of the SINEMA RC Server see table "Settings used (Page 55)".
10. Click "Apply" and close the dialog with "OK".
11. Select the menu command "Project" > "Save". Save the security project under the required name.

Result

The security module S623 is completely configured. The settings are stored in the security project.

5.2.4 Configuring the properties of the SINEMA RC Server

The devices SCALANCE S615 are intended to communicate with the SCALANCE S623 via the SINEMA RC Server. With the Security Configuration Tool, configure the VPN connection between a SCALANCE S623 and the SINEMA RC Server.

To allow communication via this VPN tunnel with the other devices, these must be released for VPN tunnel communication. You configure the release of the devices in the properties of the VPN device "SINEMARC".

Procedure

1. Select the VPN device "SINEMARC" in the content area and select the "Edit" > "Properties..." menu command.
2. Click on the "VPN" tab and click the "Add" button.
3. In "Subnets to be reached through tunnel", enter the participants to be included in tunnel communication.

4. Click the "Add" button and configure the devices with the following settings:

Network ID	IP address (vlan 1) of the S615 devices, see table "Settings used (Page 55)".
Network mask	255.255.255.0
Comment	S615_1 or S615_2

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

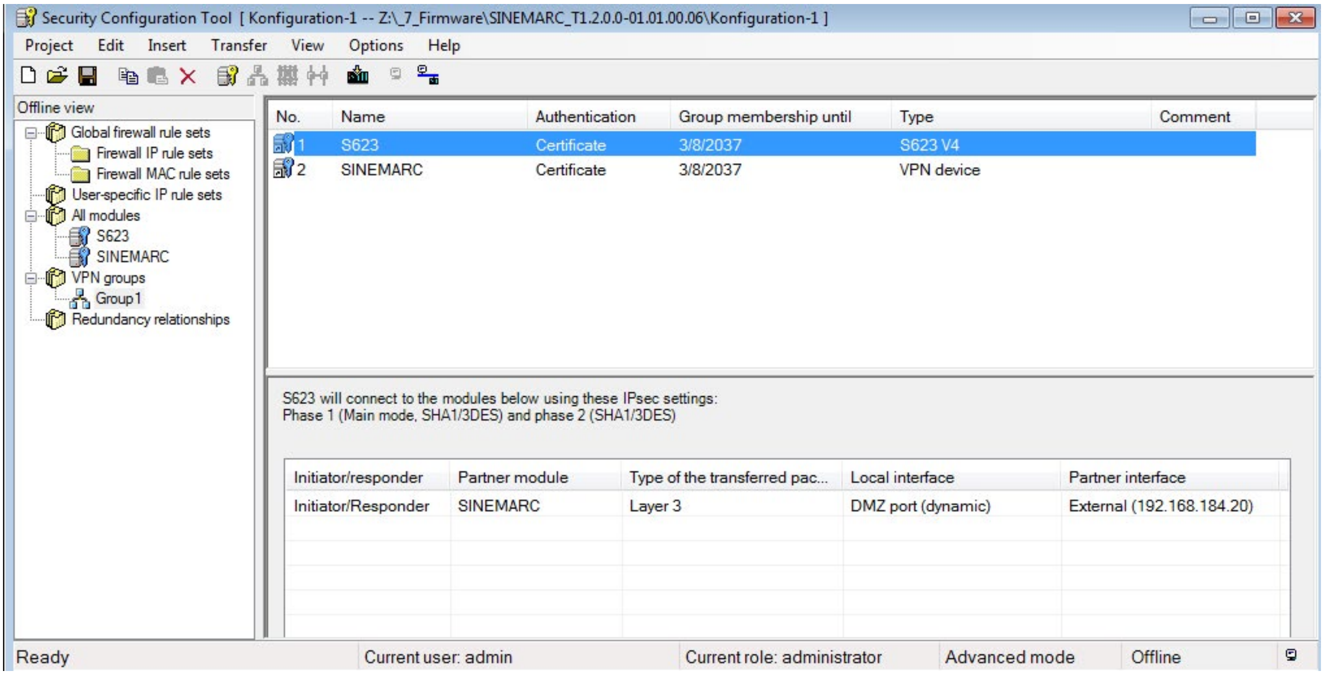
Result

The VPN device "SINEMARC" is completely configured. The settings are stored in the security project.

5.2.5 Configuring a VPN connection

Procedure

1. Click on "Group1" under "VPN groups" in the navigation panel.
2. Select the security module S623 in the content area. In the Details window, details of the VPN partners are displayed.
3. Select the "DMZ port (dynamic)" as the "Local interface".

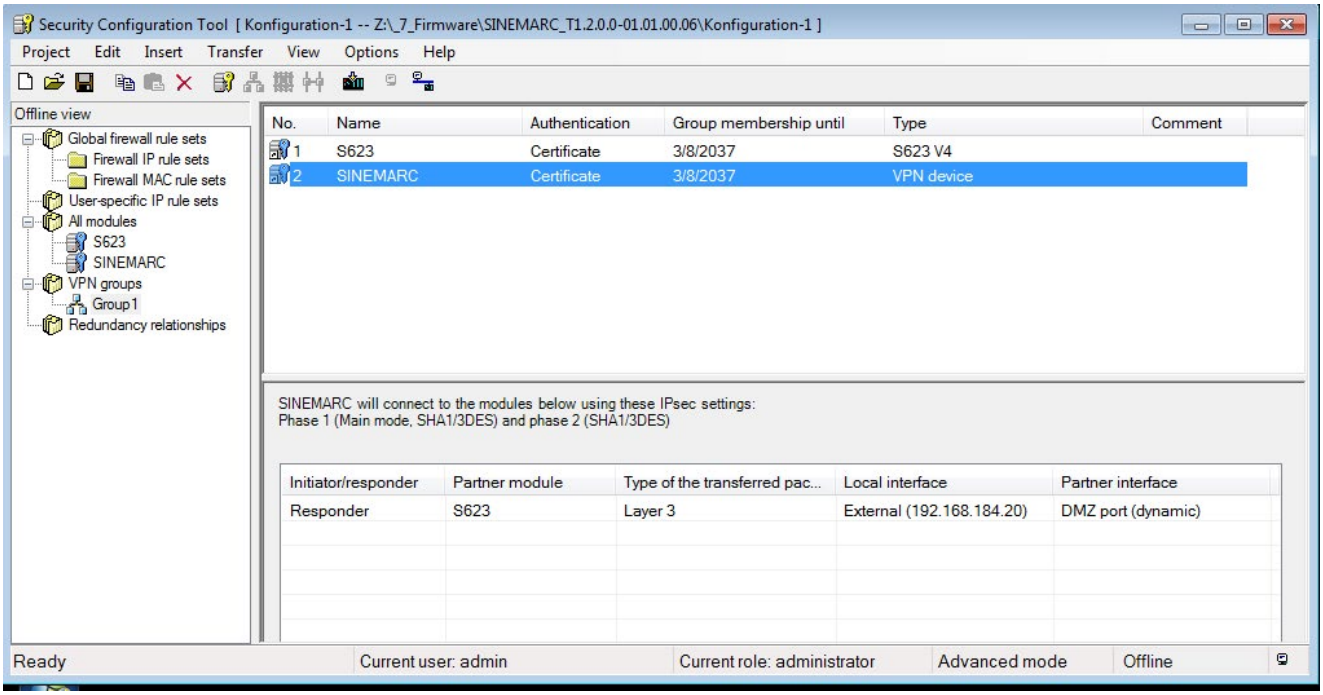

Security Configuration Tool [Konfiguration-1 -- Z:_7_Firmware\SINEMARC_T1.2.0.0-01.01.00.06\Konfiguration-1]
Project
Edit
Insert
Transfer
View
Options
Help
Offline view
Global firewall rule sets
Firewall IP rule sets
Firewall MAC rule sets
User-specific IP rule sets
All modules
S623
SINEMARC
VPN groups
Group1
Redundancy relationships

No.	Name	Authentication	Group membership until	Type	Comment
1	S623	Certificate	3/8/2037	S623 V4	
2	SINEMARC	Certificate	3/8/2037	VPN device	

S623 will connect to the modules below using these IPsec settings:
Phase 1 (Main mode, SHA1/3DES) and phase 2 (SHA1/3DES)

Initiator/responder	Partner module	Type of the transferred pac...	Local interface	Partner interface
Initiator/Responder	SINEMARC	Layer 3	DMZ port (dynamic)	External (192.168.184.20)

4. If you select the VPN device "SINEMARC" in the content area, the "DMZ port (dynamic)" will automatically be displayed as the "Partner interface".



No.	Name	Authentication	Group membership until	Type	Comment
1	S623	Certificate	3/8/2037	S623 V4	
2	SINEMARC	Certificate	3/8/2037	VPN device	

SINEMARC will connect to the modules below using these IPsec settings:
Phase 1 (Main mode, SHA1/3DES) and phase 2 (SHA1/3DES)

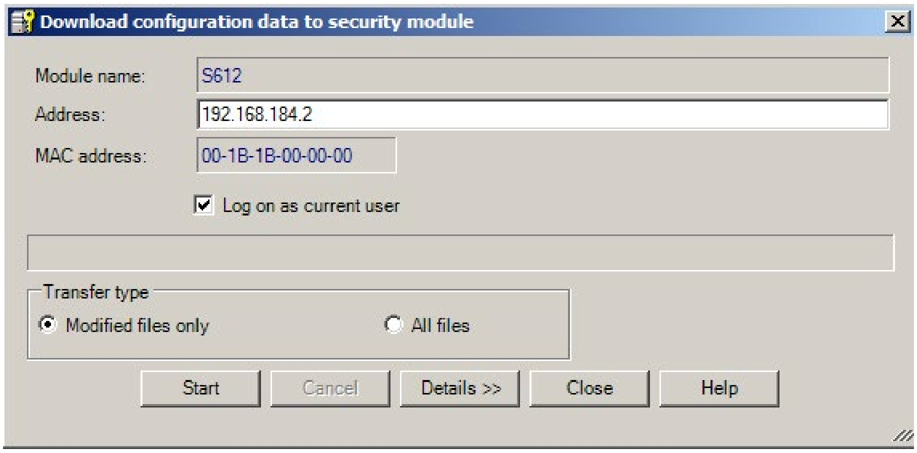
Initiator/responder	Partner module	Type of the transferred pac...	Local interface	Partner interface
Responder	S623	Layer 3	External (192.168.184.20)	DMZ port (dynamic)

5. For "Initiator/responder" select the entry "Responder". The connection is established from the security module S623 to the SINEMA RC Server.

5.2.6 Downloading the configuration to the S623 and saving the SINEMA RC configuration

Downloading the configuration to the S623

1. In the content area, select the "S623" security module and select the menu command "Transfer" > "To module(s) …". The following dialog opens.



Download configuration data to security module

Module name: S612

Address: 192.168.184.2

MAC address: 00-1B-1B-00-00-00

☑ Log on as current user

Transfer type

● Modified files only ○ All files

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 SINEMA RC configuration

1. In the content area, select the SINEMA RC Server and select the menu command "Transfer" > "To module(s) …".
2. Save the configuration file "Projectname.SINEMARC.txt" in your project folder and assign a password for the private key of the certificate.

Result

The following files will be saved in the project directory:

- Configuration file: Projectname.SINEMARC.txt
- PKCS12 file: Projectname.character string.SINEMARC.p12
- Remote certificate: Projectname.Group1.SINEMARC.cer

The configuration file contains the exported configuration information for the SINEMA RC Server including information on the additionally generated certificates. Follow the instructions in the configuration file.

5.3 Configure a remote connection on the SINEMA RC Server

5.3.1 Creating an IPsec profile

In the IPsec profile S623 configure the settings for phase 1 and phase 2.

Requirement

- You are logged on to the Web Based Management of the SINEMA Server.
- Die configuration file: Projectname.SINEMARC.txt is open.

Procedure

1. Click on "Security" > "VPN basic settings" in the navigation area and on the "IPsec profiles" tab in the content area.
2. Click the "Create" button.
3. In "Profile name" enter a name for the IPsec profile.
4. For "Key exchange method", select "IKEv1".
5. Configure phase 1 with the following settings:

Configuration file	Settings in WBM
Encryption: AES-256	Encryption algorithm: AES-256 CBC
Hash: SHA-1	Hash algorithm: SHA-1
DG group Group2	Key derivation: DH group 2 (1024 bits)
Lifetime: 150000000 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Lifetime (min): 2500000

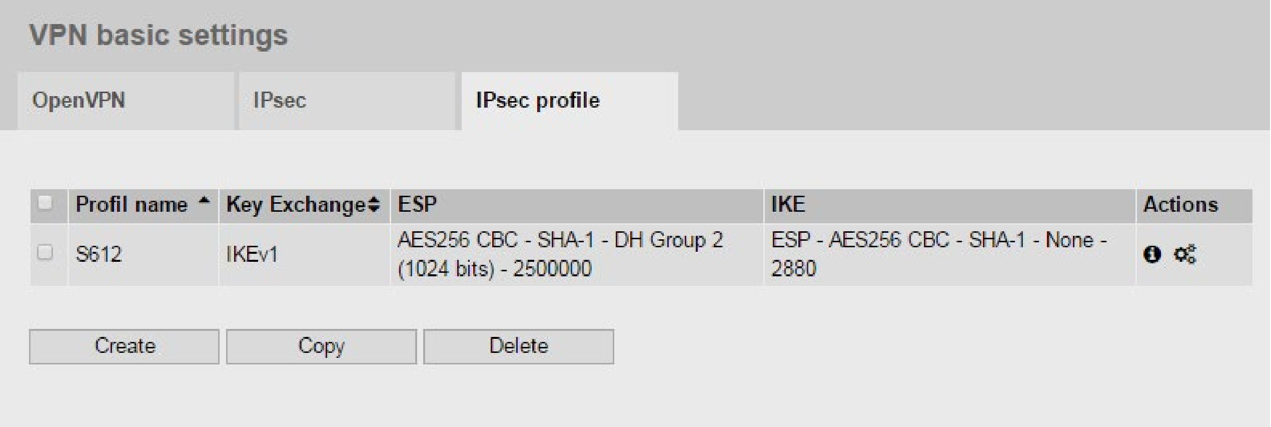
6. For protocol select "ESP".
7. Configure phase 2 with the following settings:

Configuration file	Settings in WBM
Encryption: AES-128	Encryption algorithm: AES-128 CBC
Hash: SHA-1	Hash algorithm: SHA-1
--	Key derivation: None
SA Life: 172800 The value is specified in seconds in the text file. In the WBM, the value must be entered in minutes.	Lifetime (min): 2880

8. Click "Create".

Result

The IPsec profile is listed on the "IPsec profiles" tab.



□	Profil name	Key Exchange	ESP	IKE	Actions
□	S612	IKEv1	AES256 CBC - SHA-1 - DH Group 2 (1024 bits) - 2500000	ESP - AES256 CBC - SHA-1 - None - 2880	ℹ ⚙

5.3.2 Loading a certificate

Requirement

- Certificates are available.

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

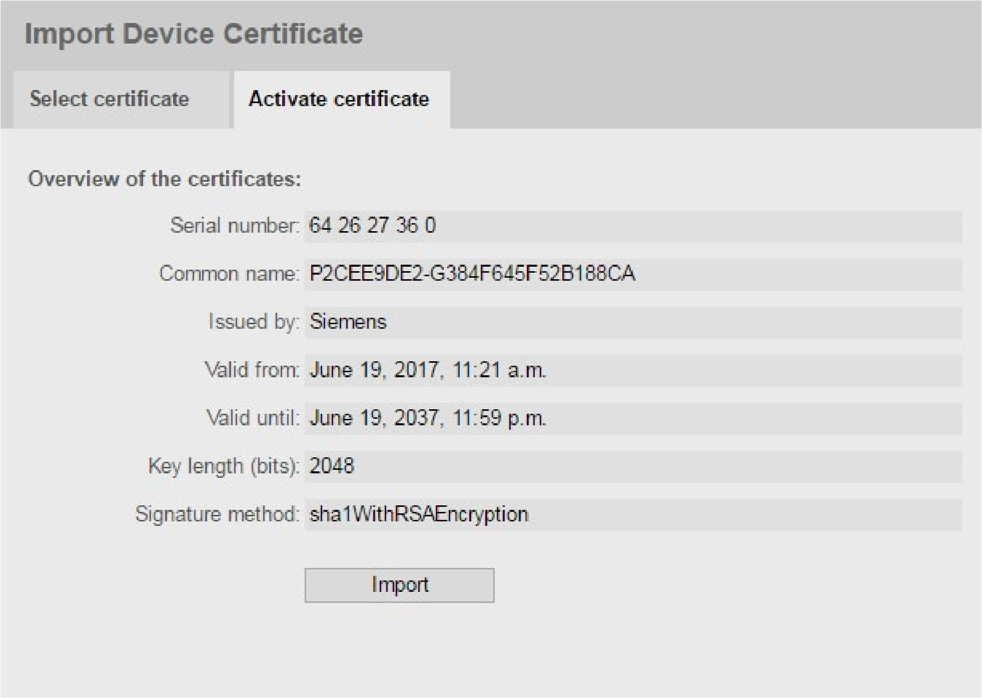
  Transfer the certificates for the SINEMA RC Server to PC 4.

Procedure

1. Click on "Security" > "Certificate management" in the navigation area and on the "Device certificates" tab in the content area.

   The certificates already loaded are listed in the content area.
2. Click the "Import" button.
3. Click the "Select file" button and select the PKCS12 file Projectname.character string.SINEMARC.p12.
4. For "password" and "Confirm password", enter the password that you specified for the PKCS12 file.

5. Click the "Continue" button. Details of the certificate are displayed on the "Activate certificate" tab.



Overview of the certificates:

Serial number: 64 26 27 36 0

Common name: P2CEE9DE2-G384F645F52B188CA

Issued by: Siemens

Valid from: June 19, 2017, 11:21 a.m.

Valid until: June 19, 2037, 11:59 p.m.

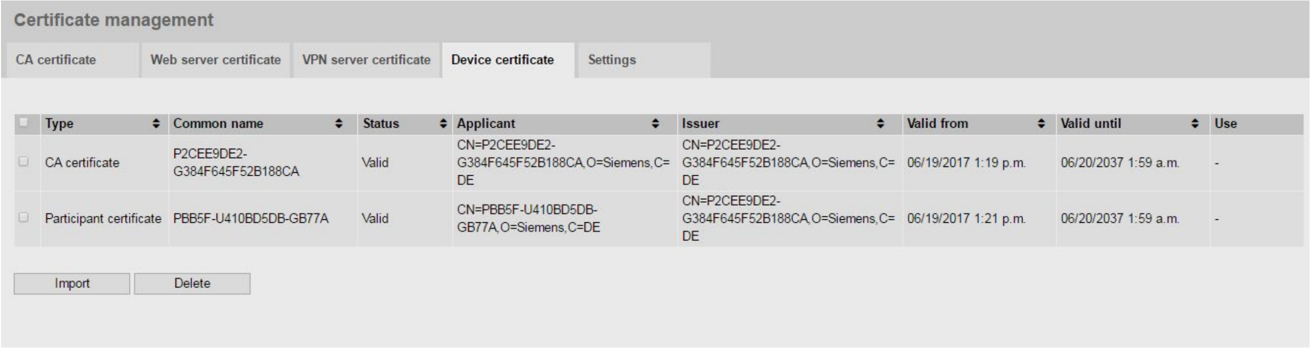
Key length (bits): 2048

Signature method: sha1WithRSAEncryption

6. To finally import the certificate, click the "Import" button.

Result

The PKCS12 file is imported onto the SINEMA RC Server. This certificate file contains the participant certificate and the signed certificate of the certification authority.



□	Type	Common name	Status	Applicant	Issuer	Valid from	Valid until	Use
□	CA certificate	P2CEE9DE2-G384F645F52B188CA	Valid	CN=P2CEE9DE2-G384F645F52B188CA,O=Siemens,C=DE	CN=P2CEE9DE2-G384F645F52B188CA,O=Siemens,C=DE	06/19/2017 1:19 p.m.	06/20/2037 1:59 a.m.	-
□	Participant certificate	PBB5F-U410BD5DB-GB77A	Valid	CN=PBB5F-U410BD5DB-GB77A,O=Siemens,C=DE	CN=P2CEE9DE2-G384F645F52B188CA,O=Siemens,C=DE	06/19/2017 1:21 p.m.	06/20/2037 1:59 a.m.	-

5.3.3 Create device

Requirement

- A partcipant group "S600" has been created, see Creating participant groups (Page 30)
- The devices S615_1 and S615_2 participants in this group.
- Die configuration file: Projectname.SINEMARC.txt is open.

Procedure

1. In the navigation area, click "Remote connections" > "Devices". The devices that have already been created are listed in the content area.
2. Click "Create" button to create a new device.
3. Enter the device name for the device e.g. "" for the security module
4. Click "Continue".
5. For "VPN connection mode", select "IPsec". For IPsec profile select the previously configured IPsec profile.
6. For "Authentication", select "CA cert".
7. For "Certificate" select the certificate loaded earlier.
8. Configure the local ID and the ID of the partner with the following settings:

Configuration file	**Settings in WBM**
Local ID: <Local ID>	Local ID: Entry from the configuration file
Remote ID: <Remote ID>	ID of the partner: Entry from the configuration file

9. Click "Continue".
10. Enable the parameter "Connected local subnets".
11. Enable the parameter "Device is a network gateway".
12. Configure the devices with the following settings and click "Add":

Local LAN IP address	IP address of the internal port P2 according to the table "Settings used (Page 55)"
Network mask	255.255.255.0

13. Click "Continue". The "Group memberships" tab is displayed.
14. Activate the group "S600"
15. Click "Continue". The "Password" tab is displayed.
16. Specify the password for the access e.g. An:t_030.

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

Result

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

Index