

SIEMENS

SIMATIC NET

Industrial Remote Communication - Remote Networks SINEMA Remote Connect

Getting Started

Preface

Connecting the SINEMA RC
Server to the WAN

1

VPN tunnel with SCALANCE
S615 and M876

2

01/2019

C79000-G8976-C394-05

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.

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.

You can find this document on the Internet under the following entry ID: 109482124 (<https://support.industry.siemens.com/cs/ww/en/view/109482124>)

- Operating instructions "SINEMA Remote Connect server"

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

You can find this document on the Internet under the following entry ID: 109482121 (<https://support.industry.siemens.com/cs/ww/en/view/109482121>)

- Configuration manual "Industrial Ethernet Security SCALANCE S615 Web Based Management"

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

You can find this document on the Internet under the following entry ID: 109751632 (<https://support.industry.siemens.com/cs/ww/en/view/109751632>)

- Getting Started "Industrial Ethernet Security SCALANCE S615"

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

You can find this document on the Internet under the following entry ID: 109475913 (<https://support.industry.siemens.com/cs/ww/en/view/109475913>)

- Application example "Setting up a Secure VPN Connection between SINEMA Remote Connect Client, SCALANCE S615 and SINEMA Remote Connect Server"

This application example shows how SINEMA Remote Connect can be used to establish a secure VPN connection between a service technician with a mobile node and an automation cell via the Internet.

You can find this document on the Internet under the following entry ID: 109479599 (<https://support.industry.siemens.com/cs/ww/en/view/109479599>)

- 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 can find this document on the Internet under the following entry ID: 27069465 (<https://support.industry.siemens.com/cs/ww/en/view/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

(<https://support.industry.siemens.com/cs/ww/en/ps/21816>)

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.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

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

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

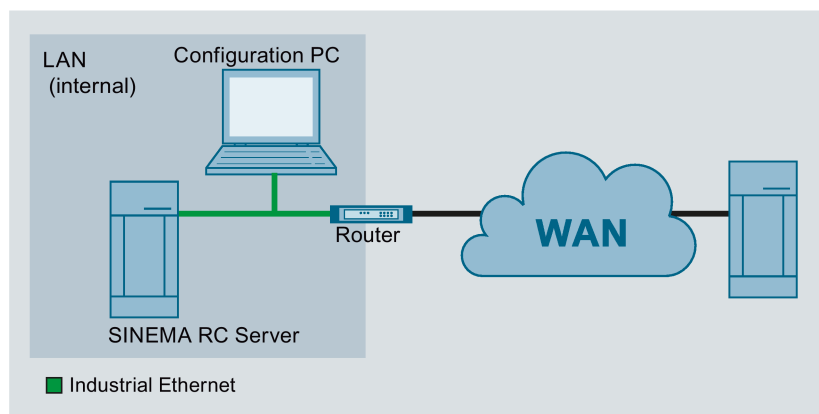
| | | |
|----------|---|-----------|
| | Preface | 3 |
| 1 | Connecting the SINEMA RC Server to the WAN | 9 |
| 1.1 | Procedure in principle | 9 |
| 1.2 | Installing SINEMA RC Server | 11 |
| 1.3 | Launching Web Based Management..... | 11 |
| 1.4 | Check the interface | 14 |
| 1.5 | Setting the time | 15 |
| 2 | VPN tunnel with SCALANCE S615 and M876 | 17 |
| 2.1 | Procedure in principle | 17 |
| 2.2 | Configuring a remote connection on the SINEMA RC Server | 22 |
| 2.2.1 | Creating node groups | 22 |
| 2.2.2 | Create devices | 24 |
| 2.2.3 | Creating a user account for service technician..... | 25 |
| 2.2.4 | Configure communications relations..... | 26 |
| 2.2.5 | Exporting a certificate | 28 |
| 2.3 | Configuring a remote connection on the device | 28 |
| 2.3.1 | Loading a certificate..... | 28 |
| 2.3.2 | Configuring a route on the SCALANCE S615 | 29 |
| 2.3.3 | Configuring a VPN connection to the SINEMA RC Server..... | 30 |
| 2.4 | Establishing a remote connection with the SINEMA RC Client..... | 33 |
| 2.4.1 | Installing SINEMA RC Client | 33 |
| 2.4.2 | Logging on to SINEMA RC Server with SINEMA RC Client..... | 35 |
| | Index..... | 37 |

Connecting the SINEMA RC Server to the WAN

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

PORT forwarding must be enabled in the router for Web Based Management, OpenVPN and CA rollout with TCP and UDP (TCP/443, UDP/1194, TCP/5443, TCP/6220).

- 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 11)
3. Checking the interface (Page 14)
4. Setting the time (Page 15)

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 the ENTER key to confirm the selection.
4. In the following dialog, the entry "eth0" is selected. Press the ENTER key to confirm the selection.
5. Enter the WAN IP address of the SINEMA RC Server, refer to the table "Settings used (Page 9)". Press the ENTER key to confirm the input.
6. For the network mask, leave the entry unchanged. Press the ENTER key to confirm the input.
7. As the gateway enter the LAN IP address of the router, refer to the table "Settings used (Page 9)". Press the ENTER key to confirm the input.

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

1.3 Launching Web Based Management

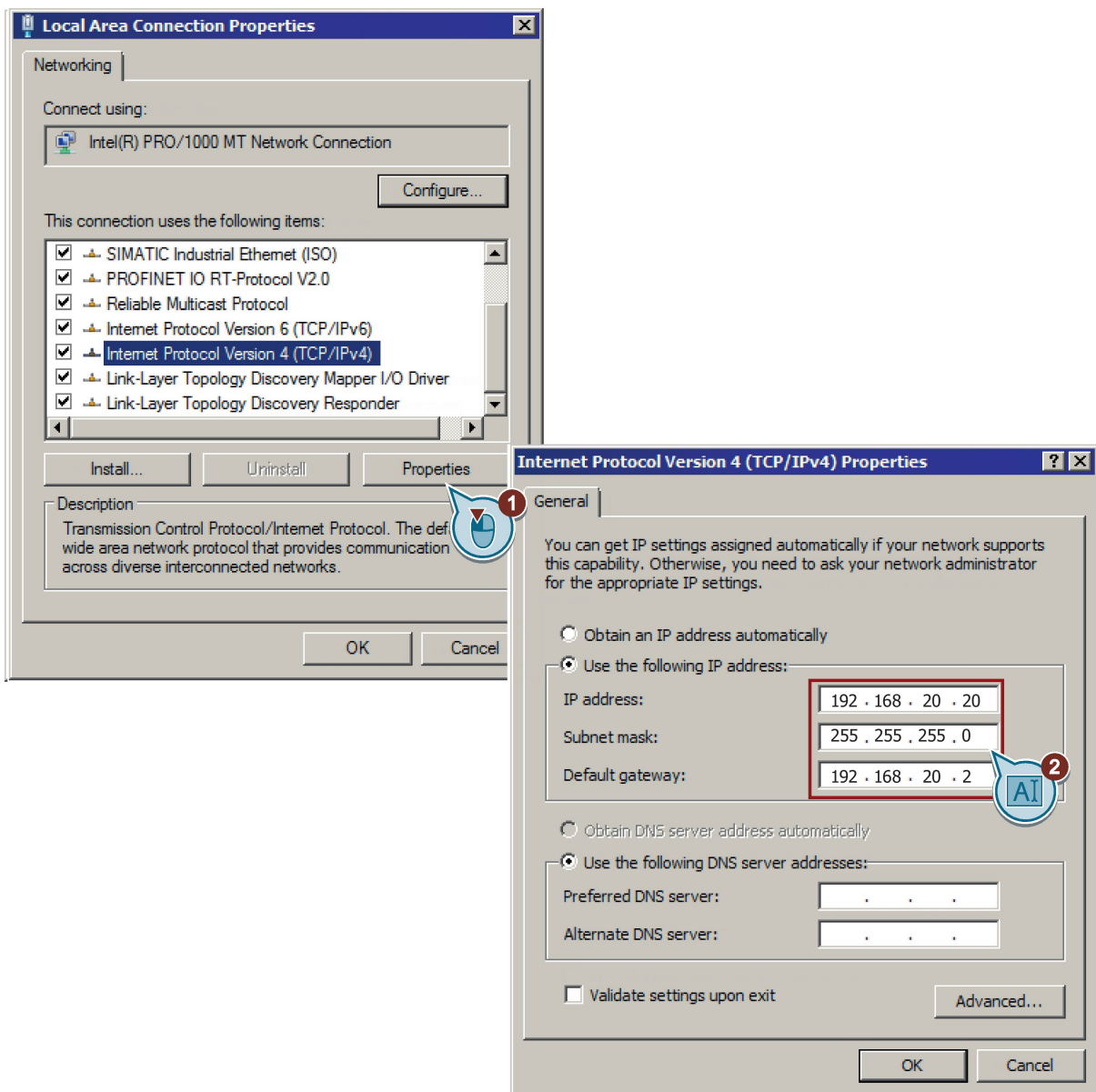
After installation, the SINEMA RC Server is reachable via the WAN interface at the following IP address 192.168.20.250

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.



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.

The screenshot shows the login interface for SINEMA Remote Connect. At the top left is the SIEMENS logo. In the center is the text 'SINEMA Remote Connect'. On the top right, there is a 'Language:' dropdown menu currently showing 'English'. The central part of the page is a light gray box containing a white login form. The form has two text input fields: the first is labeled 'Username:' and the second is labeled 'Password:'. Below these fields is a rectangular button labeled 'Log in'.

8. After installation, log in with the user name "admin" and the password "admin".
9. After logging in, the WBM page "Change password" opens. 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)".

The screenshot shows the 'Network Configuration' page with the 'Interfaces' tab selected. A warning message states: '! A change in the following settings might disconnect all connected devices/users and put web server temporarily out of service!'. The 'Enable Port' checkbox is checked, and the 'Port' is set to 'WAN'. The MAC Address is 08:00:27:d5:e4:b6, MTU is 1500, IP Address is 192.168.20.250, Netmask is 255.255.255.0, and Default Gateway is 192.168.20.2. The 'SINEMA RC is behind a NAT device' checkbox is also checked, and the WAN IP Address is set to 192.168.184.20. A 'Save' button is visible at the bottom.

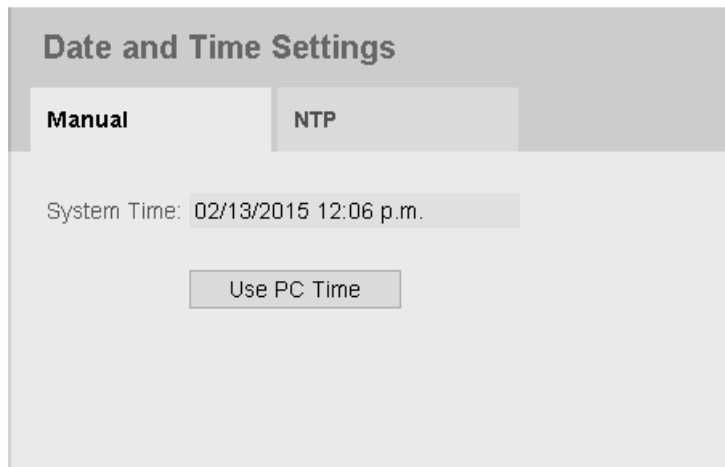
6. Click "Backup".

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".



Result

System time using PC is set.

VPN tunnel with SCALANCE S615 and M876

2.1 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.

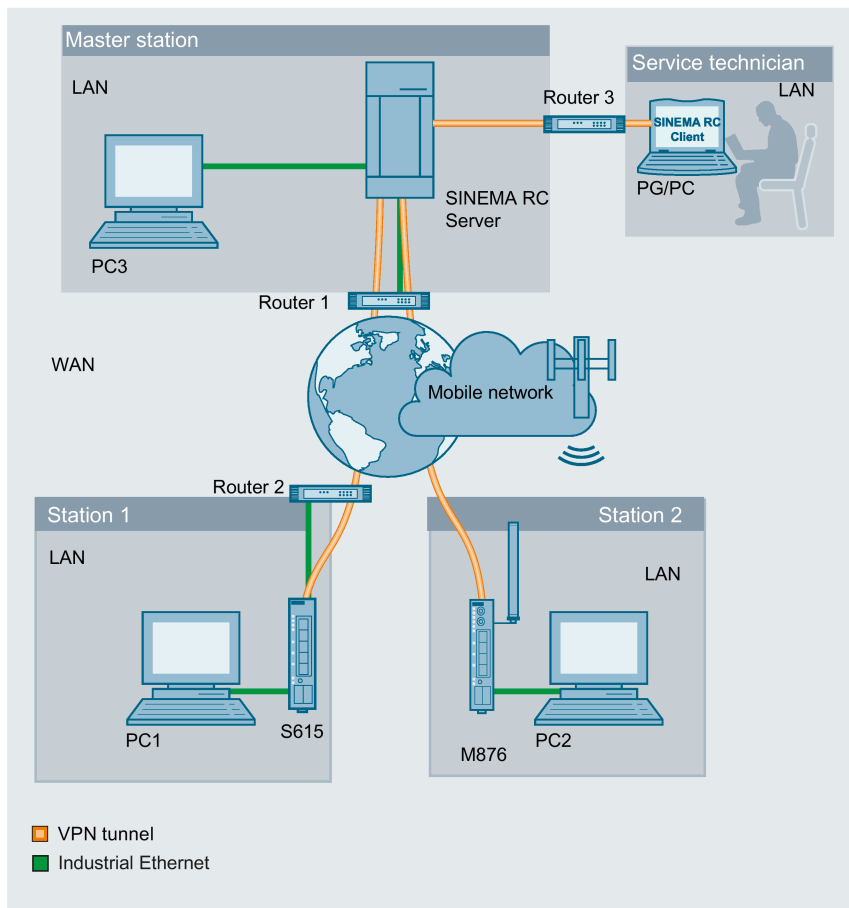
Station 2 is directly connected to the WAN via SCALANCE M876, the others via a router.

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.

2.1 Procedure in principle



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".

2.1 Procedure in principle

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 |
| 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".

- 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
2. Creating a device
3. Creating a user account for service technician
4. Configuring communication relations
5. Exporting a certificate

2.2 Configuring a remote connection on the SINEMA RC Server

Configuring a remote connection on the device

1. Loading a certificate
2. Configuring a route on the SCALANCE S615
3. Configuring the VPN connection to the SINEMA RC

Establishing a remote connection with the SINEMA RC Client

1. Installing SINEMA RC Client
2. Logging in to SINEMA RC Server with SINEMA RC Client

2.2 Configuring a remote connection on the SINEMA RC Server

2.2.1 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".
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.

Participant groups

i No filter active

 Precise match

| <input type="checkbox"/> | Group name | Members may communicate | Reachable Ethernet interfaces | Number of users | Number of devices | Number of subnets | Number of nodes | Number of roles | Actions |
|--------------------------|------------|-------------------------|-------------------------------|-----------------|-------------------|-------------------|-----------------|-----------------|---------|
| <input type="checkbox"/> | Service | No | No | 0 | <u>2</u> | 0 | 0 | 0 | |
| <input type="checkbox"/> | Station1 | No | No | 0 | <u>1</u> | 0 | 0 | 0 | |
| <input type="checkbox"/> | Station2 | No | No | 0 | <u>1</u> | 0 | 0 | 0 | |

2.2.2 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".

2.2.3 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.

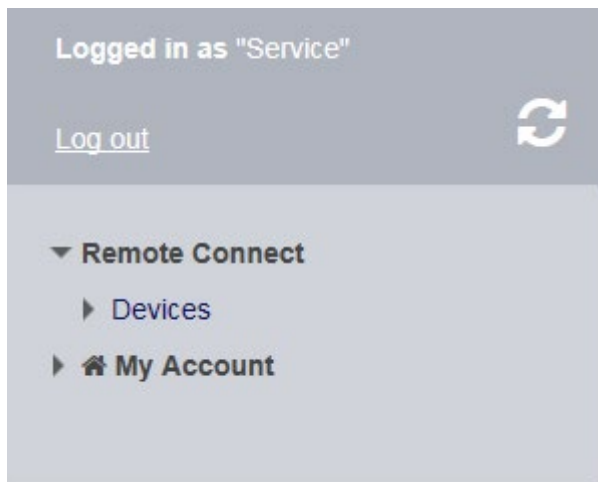
Create users

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.



2.2.4 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.

Communication relations

i No filter active

Search filter: Source group Precise match Apply filter Show all

| Source group | Destination group | Actions |
|--------------|----------------------|---|
| Service | Station1 Station2 |  |
| Station1 | Station2 |  |

2.3 Configuring a remote connection on the device


2.2.5 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.

2.3 Configuring a remote connection on the device

2.3.1 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 28)". 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".
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".

| Select | Type | Filename | State | Subject DN | Issuer DN | Issue Date | Expiry Date | Used |
|--------------------------|---------|-------------------------|-------|------------------------|------------------------|---------------------|---------------------|-----------|
| <input type="checkbox"/> | CA Cert | CA_667356_SINEMA_RC.crt | valid | CN=CA 667356 SINEMA RC | CN=CA 667356 SINEMA RC | 11/29/2018 10:11:43 | 11/29/2028 10:11:43 | Sinema RC |

1 entry.

Delete Refresh

2.3.2 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 (Page 17)".
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 (Page 17)" |
| Administrative Distance | -1 |

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

Result

The route is created.

Static Routes

Destination Network:
Subnet Mask:
Gateway:
Interface: auto
Administrative Distance: -1

| Select | Destination Network | Subnet Mask | Gateway | Interface | Administrative Distance | Status |
|--------------------------|---------------------|-----------------|--------------|-----------|-------------------------|----------|
| <input type="checkbox"/> | 192.168.184.20 | 255.255.255.255 | 192.168.50.2 | | not used | inactive |

1 entry.

2.3.3 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".
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.

SINEMA Remote Connect (SINEMA RC)

Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168.184.20

SINEMA RC Port: 443

Server Verification

Verification Type: CA Certificate

Fingerprint: CC:97:B3:92:A1:D7:CB:0F:6

CA Certificate: CA_667356_SINEMA_f

Device Credentials

Device ID: 5

Device Password: *****

Device Password Confirmation: *****

Optional Settings

Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

[Set Values](#) [Refresh](#)

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".

2.3 Configuring a remote connection on the device

SINEMA Remote Connect (SINEMA RC) Information

Status: **established**

Device Name: **M800_S615**

Device Location: -

GSM Number: [REDACTED]

Vendor: **Siemens AG**

Comment: -

Type of Connection (Server): **Permanent**

Type of Connection (Device): **Auto**

Fingerprint: [REDACTED]

Remote Address: [REDACTED]

Connected Local Subnet(s): [REDACTED]

Connected Local Host (s): [REDACTED]

Tunnel Interface Address: [REDACTED]

Connected Remote Subnet(s): [REDACTED]

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

Devices

i no filter active

Search filter: All Precise match

| <input type="checkbox"/> | Name of the device | VPN address | Remote subnet | Virtual local LAN | Status | Location | Type of connection | VPN connection mode | Actions |
|--------------------------|--------------------|-------------|------------------|-------------------|--------|----------|--------------------|---------------------|---------|
| <input type="checkbox"/> | S615_1 | None | 192.168.100.0/24 | None | online | | Permanent | OpenVPN | |
| <input type="checkbox"/> | S615_2 | None | 192.168.10.0/24 | None | online | | Permanent | OpenVPN | |

2.4 Establishing a remote connection with the SINEMA RC Client

2.4.1 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 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".

2.4 Establishing a remote connection with the SINEMA RC Client

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.

2.4.2 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 "Creating a user account for service technician (Page 25)".

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.

Index

G

Glossary, 5

S

Service & Support, 5

SIMATIC NET glossary, 5

SIMATIC NET manual, 4

SINEMA RC client

 Installing, 33

SINEMA RC Server

 Installing, 11

T

Training, 5

W

WBM

 Logging in, 35

 Starting, 11

