SIEMENS

SIMATIC NET

Industrial Remote Communication
SINEMA Remote Connect

Operating Instructions

04/2016
C79000-G8976-C395-03

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

Purpose of this documentation

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

Validity of this documentation

This manual is valid for the following software version:

- SINEMA Remote Connect as of version V1.0

Article number - licenses

To enable the connection functionality on the SINEMA RC Server, the following license is available:

Product name	Article number
SINEMA Remote Connect Client	6GK1721-1XG01-0AA0

Abbreviations/acronyms and terminology

- **SINEMA RC**

  In the remainder of the manual, the "SINEMA Remote Connect" software is abbreviated to "SINEMA RC".

New in this release

- Automatic login settings
- Automatic tunnel establishment
- When ending force comment

Required experience

To be able to configure and operate the system described in this document, you require experience of the following products, systems and technologies:

- SIMATIC NET - Telecontrol
- IP-based communication
- STEP 7 Basic / Professional
- SIMATIC S7

Further documentation

- Operating instructions "SINEMA Remote Connect server"

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

- Getting Started "SINEMA Remote Connect"

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

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/WW/view/en)

  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/de/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, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

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

Requirements for operation

<div style="text-align: right">1</div>

Hardware requirements

Parameter	Minimum requirements
Processor	1 GHz
RAM	1 GB (32-bit) or 2 GB (64-bit)
Storage requirements hard disk	• approx. 900 MB (with a 32-bit operating system) • approx. 2.1 GB (with a 64-bit operating system)

Required operating systems

- 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
- Windows Server 2008 R2 x64 (requirement: NET 3.5 or higher is installed)

Required license

For SINEMA RC Client, the following license type is available:

- SINEMA Remote Connect Client

Installation and commissioning

<div style="text-align: right; font-size: 3em;">2</div>

2.1 Security recommendations

Keep to the following security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Operate the device within a protected network area.

Physical access

Restrict physical access to the device to qualified personnel. Use the security mechanisms of the operating system.

Security functions of the software

- Keep the software up to date. Check regularly for security updates for the product. You will find information on this at:
  http://www.siemens.com/industrialsecurity
- Keep the operating system up to date. Check regularly for security updates of the operating system and use them.

  Use the options of the Windows firewall and the configuration options of the product.

Automation License Manager (ALM)

Turn off remote access to the ALM service. This option can be found in the "Connections" tab in the ALM settings.

2.2 Installing SINEMA RC Client

Overview

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

---

Sequence

To install SINEMA RC Client on your computer, follow the steps below:

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.

2.3   Licensing

Automation License Manager

To manage your license, you use the Automation License Manager (ALM) program. This program is used to manage the license keys. Software products that require license keys automatically indicate this requirement to the Automation License Manager. If the ALM finds a valid license key for the software, this can be used according to the end user license agreement.

After installing the SINEMA RC Client, you can call up the documentation for the Automation License Manager. To do this, select "Start > All Programs > Siemens Automation > Documentation in the Windows menu.

Storage location for license keys

You can store license keys on storage devices such as USB dongles, on exchangeable drives or on USB memory sticks, however not on CD, CD RW. For productive operation of the SINEMA RC client, the license key must be saved locally on your computer or must be located on a USB dongle.

Note

Prior to installing/uninstalling a license key, check that your PC is free of viruses. It is possible that viruses are exchanged between the hard disks and storage data media.

To transfer the license keys, write protection of the storage data medium must be disabled.

Non-existent license key

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.

Configuration

<div align="right">

3

</div>

3.1 Logging in

Connecting to the SINEMA RC Server

To establish an OpenVPN connection from the SINEMA RC Client to the server, follow the steps below:

1. Double-click on the "SINEMA RC Client" icon on your desktop.

   Or in the menu "Start > All Programs > Siemens Automation > SIMATIC > SINEMA RC Client" select the "SINEMA RC Client" entry.

2. Enter the IP address of the SINEMA RC Server:

   If the SINEMA RC Server uses a port other than 443 as the HTTPS standard port, enter the port number along with the IP address. A colon ":" must be entered between the IP address and the port number as a delimiter e.g.: https://192.168.234.1:6443.

3. Enter the user name and the password.

   Assuming that the user name and the password have been created on the SINEMA RC Server. You cannot log on to SINEMA RC Client with the "admin" user.

4. Click the "Log on" button

   The SINEMA RC Client establishes an HTTPS connection to the SINEMA RC Server and the start page is displayed, refer to the section "Start page (Page 17)".

5. Click the "Open VPN tunnel" button.

Result:

- The OpenVPN configuration file is downloaded from the SINEMA RC server

- The SINEMA RC client automatically creates a configuration file with the most important settings. These include among other things the IP addresses and NAT settings.

- The SINEMA RC Client establishes the VPN tunnel.

Connecting to the SINEMA RC Server automatically

To establish an OpenVPN connection from the SINEMA RC Client to the server automatically, follow the steps below:

1. Start the SINEMA RC Client.

2. Enter the user name and the password. Click the "Login" button.

3. In the area SINEMA Remote Connect user account, click the symbol

4. Enable the option "Start SINEMA RC Client automatically after Windows login"

5. Enter the user name and the password.

   Assuming that the user name and the password have been created on the SINEMA RCSINEMA RC Server. You cannot log on to the SINEMA RC Client with the "adminadmin" user.

6. Enable the option "Automatic tunnel establishment after SINEMA RC Client login".

7. Confirm the settings with the "OK" button.

Result:

The SINEMA RC Client logs in with the SINEMA RC Server automatically after Windows login and establishes the VPN tunnel.

3.2 Start page

Selection area ①

The following is available in the selection area:

- Settings: Click the button to make settings for local ports and the proxy, refer to the section "Making general settings (Page 20)".

- Language settings: Select a user interface language.

- ? : Select the required information.

SINEMA Remote Connect user account ②

You obtain an overview of the user account. These include the IP address of the SINEMA RC Server and the user name. Click the "Log out" button.

To start VPN connection establishment to the SINEMA RC server, click the "Open VPN tunnel" button.

You terminate the VPN connection with the "Close VPN tunnel" button. If the user account is assigned the right "Force comment", the user will be prompted to enter a comment. Only then is the VPN connection terminated. The comment is entered in the log of the SINEMA RC Server.

The "VPN Status" shows whether or not the VPN connection is established (online / offline). If a VPN connection exists, the VPN address of the client is displayed

This area contains the following symbols:

* Opens the WBM on the SINEMA RC Server.

* Opens the autostart settings, see section "Logging in (Page 15)".

Device list ③

In the device list, you obtain the following information:

Box	Description
Name of the device	Name of the available device. The name is adopted from the settings of the SINEMA RC Server. If a check box is displayed in front of the device name, the NAT function is enabled, refer to the section "Making NAT settings (Page 21)".
VPN address	VPN address of the device that the device receives from the SINEMA RC Server.
Remote sub-net	The IP address of the remote subnet.
Virtual local LAN	The virtual LAN IP address. Assuming that this is configured on the SINEMA RC Server.
Status	• online: The device is connected • offline: The device is not connected
Location	Location of the device
Actions	Shows the actions enabled for this device.

Actions	🏠	Opens the WBM on the device
	📱	Only available with the type of connection "Wake-up SMS" or "Digital input & Wake-up SMS". • If the device is not connected, the SINEMA RC Server sends the wake-up SMS message to the device.

Buttons ④

Activate NAT	A NAT IP address is assigned to the device in the remote subnet.
	When you enable or disable the option, existing VPN tunnels are closed. Click the "Open VPN tunnel" button to re-establish the VPN tunnel.
	To update the display in the device list, click the "Update" button.
NAT configuration	See section "Making NAT settings (Page 21)".
Show log files	You receive the following log information. The path on which the log file is stored is shown in brackets. • SINEMA RC Client (C:\ProgramData\Siemens\Automation\SINEMA_RC_Client\logs\SRCClient.log) • SINEMA RC Service (C:\ProgramData\Siemens\Automation\SINEMA_RC_Client\logs\srccService.log) • Open VPN Client (C:\ProgramData\Siemens\Automation\SINEMA_RC_Client\logs\openvpn.log)
Exit	The SINEMA RC Client application is closed.

3.3 Making general settings

Local port settings

The local port settings are used for internal communication of the SINEMA RC client. Adaptations are only necessary if there is a port conflict in the system.

1. Select the port via which the OpenVPN service is addressed.

2. Select the port via which the SINEMA RC Client service can be reached.

If you change the default port, existing connections are terminated. In this case, click the "Open VPN tunnel" button again.

VPN proxy settings

A proxy is a communications interface in a network and serves as an intermediary between the Internet and the network to be protected. The proxy receives queries from the client and forward these to the relevant server via its own address. The address of the client is not made known to the server.

In contrast to simple address translation using NAT, a proxy server can run communication itself instead of passing on packets unseen to the recipient.

If you use a proxy server, for example to reach a Web server via this in the remote subnet, make the following settings:

User proxy settings	Enable the check box to make the proxy settings (disabled as default).
Proxy type	Type of the proxy server • HTTP: Proxy server only for access using HTTP. • SOCKS: Universal proxy server
Server	Enter the address of the proxy server.
Port	Specify via which port via which the proxy server can be reached.
Authentication	Select an authentication method: • None: No authentication • Basic: Standard authentication. User name and password are sent unencrypted. • NTML: Authentication according to the NTML standard (Windows user logon)
User name	If you have selected an authentication method other than "none", enter a user name for access to the proxy server.
Password	Enter a corresponding password.
Confirm password	Confirm the password.

3.4 Making NAT settings

Activate NAT

1. Enable the "Activate NAT on Client" option.

2. Select a device in the list.

Result

NAT is activated. As default the NAT settings of the device are used. If you require different settings, adapt the NAT setting.

If changes are made to NAT, existing VPN tunnels are closed. Click the "Open VPN tunnel" button to re-establish the VPN tunnel.

Configuring destination NAT

1. If you require certain settings, enable the option "Using manual NAT settings" and click the "NAT configuration" button.

2. Click the "NAT configuration" button.

3. Configure the "Destination subnet".

	Description
Network	Network address of the destination subnet
Subnet mask	The subnet mask matching the destination network.

4. Configure the "Translated subnet".

	Description
Network	Network address of the translated subnet into which the destination IP address will be converted or translated.
Subnet mask	The subnet mask matching the network.

5. Click the "OK" button to apply the changed settings.

Result

Destination NAT is configured. For the data packets to be sent to an IP address within the destination subnet, the destination IP address is replaced by the suitable IP address from the translated subnet.

Existing VPN tunnels are closed. Click the "Open VPN tunnel" button to re-establish the VPN tunnel.

Index