

Industrial Remote Communication - Remote Networks SINEMA Remote Connect V3.1 - Client

Operating Instructions

Preface

Requirements for operation

1

Installation and
commissioning

2

Configuration

3

Appendix A

A

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 Version V3.1 or higher

Article number - licenses

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

Product name	Order ID
SINEMA Remote Connect Client (1 VPN client)	6GK1721-1XG03-0AA0
SINEMA Remote Connect Client (OSD)	6GK1721-1XG03-0AK0

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

- TOTP-based two-factor authentication
- RTU 303xC: Deadline-based sending of wake-up SMS message

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

(<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/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

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following documents on the supplied data medium:

- OSS_SINEMA-RC-Client_86.pdf

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> (<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 customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

<https://www.siemens.com/cert> (<https://www.siemens.com/cert>).

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Decommissioning

Note that personal data such as addresses or passwords can also be saved on the computer on which the software is installed.

Decommission the device properly to prevent unauthorized persons from accessing confidential data.

To this end, reset the SINEMA RC Client to factory settings.

Procedure

To reset the SINEMA RC Client to factory setting, follow the steps described below:

1. In the "Settings" tab, disable the option "Start SINEMA RC Client automatically after Windows login".
2. Confirm the setting with the "Save" button.
3. Exit the SINEMA RC Client.
4. Delete the folder "C:\ProgramData\Siemens\Automation\SINEMA_RC_Client".

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 Requirements for operation	9
2 Installation and commissioning	11
2.1 Planned operating environment.....	11
2.2 Security recommendations.....	11
2.3 Installation	13
2.4 Licensing	16
3 Configuration.....	17
3.1 Login.....	17
3.2 Account.....	21
3.3 Server Profiles.....	26
3.4 Settings	27
3.4.1 Making general settings.....	28
3.4.2 Notification settings.....	29
3.4.3 Settings for automatic functions	29
A Appendix A	31
A.1 Syslog messages.....	31
A.1.1 Tags in Syslog Messages	31
A.1.2 List of Syslog Messages	32
A.1.2.1 Identification and authentication of human users.....	32
A.1.2.2 Unsuccessful logon attempts	33
A.1.2.3 Access via untrusted networks	33
A.1.2.4 Software and information integrity	33
Index.....	35

Requirements for operation

Hardware requirements

Parameter	Minimum requirements
Processor (x86)	1 GHz
RAM	2 GB (64-bit)
Storage requirements hard disk	approx. 2.1 GB (with a 64-bit operating system)

Operating systems

- Microsoft Windows 11
- Microsoft Windows 10 Professional (64-bit)
- Microsoft Windows 10 Enterprise (64-bit)
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)

Required license

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

- SINEMA Remote Connect Client

The license must be enabled on the SINEMA Remote Connect Server.

Compatibility

The table shows which SINEMA RC Client versions and SINEMA RC versions are compatible with each other.

		SINEMA RC Client version								
		1.0	1.0 SP1	1.0 SP2	1.0 SP3 + SP4	2.0	2.1	3.0	3.0 SP1	3.1
SINEMA RC server version	1.0	✓	-	-	-	-	-	-	-	-
	1.1	-	✓	-	-	-	-	-	-	-
	1.2	-	-	✓	-	-	-	-	-	-
	1.3	-	-	-	✓	-	-	-	-	-
	2.0	-	-	-	-	✓	-	-	-	-
	2.1	-	-	-	-	-	✓	-	-	-
	3.0	-	-	-	-	-	-	✓	-	-
	3.0 SP1 + SP2	-	-	-	-	-	-	-	✓	-
	3.1	-	-	-	-	-	-	-	-	✓

Installation and commissioning

2.1 Planned operating environment

This section describes the recommended boundary conditions for using the SINEMA Remote Connect client.

- For secure operation, observe the security recommendations (Page 11).
- Check that open ports comply with security standards. All firewall changes are displayed during installation.
- Check that the offered ciphers comply with security standards. You can find more information on ciphers used in the SINEMA RC Server operating instructions.
- Use the user and group settings in the SINEMA Remote Connect Server to grant the respective users access to only the necessary plant parts.
- Use Public Key Infrastructure (PKI) certificates or two-factor authentication for the users.
- Use hardware encryption on the PCs, e.g. BitLocker.
- Make sure that only authorized persons have access to the system.
- Install and run antivirus software on the PC.
- As user with operator rights, configure and maintain the platform securely, including the hardware, the operating system and the adjacent network with additional SINEMA RC clients.
- As user with administrator rights, protect your Windows operating system. Keep it up to date and apply updates to the operating system when they are available.
- As user with administrator rights, use different accounts - one for administration and one for operative use.

2.2 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 (<https://www.siemens.com/industrialsecurity>).
- Do not connect the device directly to the Internet. Operate the device within a protected network area.

Physical access / Remote access

- Restrict physical access to the device to qualified personnel. Use the security mechanisms of the operating system.
- Decommission the device properly to prevent unauthorized persons from accessing confidential data. For more information, refer to "Decommissioning".
- Terminate management connections (e.g. HTTPS, SSH) properly.

Software

- 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.
- Check regularly for new software versions or security updates and apply them.
- You can find the latest information on security patches for Siemens products on the Industrial Security (<https://www.siemens.com/industrialsecurity>) and ProductCERT Security Advisories (<https://www.siemens.com/cert>) web pages.
- For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- If a new version is available for the SINEMA RC Server, you can find the update on the Internet pages of Siemens Industry Online Support under the following ID: 21816 (<https://support.industry.siemens.com/cs/ww/en/ps/21816/dl>)
- You will find a SHA256 hash value in the update file. With this, you can check whether the file was downloaded unchanged. To check this, you calculate the hash value of the downloaded file and compare it with the value specified on the download page.

Keys and certificates

- Use certificates with a key length of 4096 bits.
- The product supports RSA 1024 - 8192 bits key length.
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.

Available protocols

The following list provides you with an overview of all used services of the product.

Keep this in mind when configuring a firewall.

The table includes the following columns:

- Protocol
- All protocols that the device supports

- Port number
Port number assigned to the protocol
- Port status
 - Open, authentication required
The port is always open and cannot be closed. To use it, authentication is necessary.
 - Open (when configured), authentication necessary
The port is open if it has been configured. To use it, authentication is necessary.

Protocol		Port number	Port status
OpenVPN	UDP	1194	Outgoing
	TCP	5443	Outgoing
Web client	TCP	443	Outgoing
Routing update	UDP	5243	Open, authentication required

2.3 Installation

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 only install the SINEMA Remote Connect as an OpenVPN client.

Note

Prior to installation

Before installing, read the "Readme" and follow the instructions for installation and updating.

Installing client software from the installation DVD

To install the 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 on the "Continue" button.
3. Click the "Open source license agreement" button to display the license agreement. Read the license agreement and select the option "I accept the conditions of the above license agreement as well as the conditions of the Open Source license agreement".
4. Click on the "Next" button.

A list with programs to be installed opens. Leave the preselection of the components as it stands. These include:

- SINEMA RC Client
- TAP-Windows Adapter V9.24.2
- Microsoft .NET Framework
- Microsoft VC++ Redistributable

You can find information about the programs to be installed in the respective readme file. To do this, select the component in the tree view and click the "Read Me" button.

5. Click the "Next" button. The "System settings" dialog box opens.
6. The overview lists the changes made to the system settings during installation.
If you want, you can either print the overview or save it as a text file.
7. Accept the changes to the system settings and click the "Next" button.

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

At the end of the installation process, a dialog window appears with the status message about the successful installation of the SINEMA RC Client.

Here, you can choose to either restart the computer immediately or later.
Select the desired option.

8. Click on the "Finish" button to end the installation.

Loading and installing client software from the SINEMA RC server

Configured users that have the "Download client software" right can download and install the client software from the SINEMA RC server.

1. Log in to the SINEMA RC server with your user account.
2. In the navigation, select "My Account > Client Software".
3. Check the software version and the displayed SHA fingerprint to see whether it corresponds to the fingerprint on the Siemens Online Support website.
4. Download the self-extracting ZIP file with the client software to your PC.
5. Double-click on the file to unzip it. You can also run it by right-clicking it.
The file is unzipped.
6. Follow the instructions and start the setup.
7. Perform steps 2 - 8 as described in the section on installing from a DVD.

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 Licensing

To be able to connect the SINEMA RC Client with the SINEMA RC server, you need a client license. You can find the MLFB numbers of the licenses in the preface (Page 3). Each obtained license contains a specific number of license nodes. The number of license nodes determines how many clients you can enable. You can enable clients as needed, or release unused license nodes again and enable them later.

You can manage the client licenses on the SINEMA RC server on the tab "System > Licenses". You can enable client licenses either online or offline there. With online activation, you specify how many license nodes you want to activate. With offline activation, all licenses are always activated. Specification of the number of license nodes to be activated is not possible offline.

Three client licenses can be converted into one floating license. The floating license is only blocked during actual use. When it is no longer in use, the license is available again and can be temporarily assigned to any user.

Configuration

3

3.1 Login

First login to SINEMA RC server after installation of the client software

After the SINEMA RC client is started, the login dialog is displayed. Because no SINEMA RC server profile has been configured yet, the input boxes in the login dialog are empty. However, you can enter the IP address of the server in the "SINEMA RC Server URL" entry field, select a login method and log in to the SINEMA RC server.

Creating a server profile simplifies login. You can then select the desired server in the login dialog. The data of the server and the user are applied to the login dialog. You can find additional information in the section "Server Profiles (Page 26)".

Logging on to SINEMA RC Server

1. Double-click on the "SINEMA RC Client" icon on your desktop.
As an alternative, start the SINEMA RC Client with "Start > All Programs > Siemens Automation > SIMATIC > SINEMA RC Client".
The SINEMA RC Client login dialog is displayed.
2. Select the relevant SINEMA RC server name from the drop-down list.
The IP address of the SINEMA RC server and the configured login method are displayed.

3.1 Login

3. If necessary, select a different login method from the drop-down list.

You have the following options for this:

Login via ...	Procedure
User name / Password	<p>Requirement</p> <ul style="list-style-type: none"> • The user name and password are stored on the SINEMA RC Server • TOTP-based two-factor authentication is enabled (default setting). Two-factor authentication is configured for the user in the role settings. <p>Procedure</p> <ol style="list-style-type: none"> 1. Enter the user name and password. Note: You cannot log in to the SINEMA RC Client with the user name of the system administrator or "admin" (after a new installation). 2. Click the "Log in" button. 3. If two-factor authentication is enabled in the role setting, you generate a one-time token with the authentication app. Enter the token in the following dialog. 4. Click the "OK" button.
Smart card	<p>Requirement</p> <ul style="list-style-type: none"> • The relevant PKI CA certificates are installed on the SINEMA RC server. • A card reader is available on the PC or notebook • The card reader is connected according to the manufacturer's specifications and the corresponding driver is installed • The card has a valid end-entity certificate. • The path to the library file pks11-dll is set, see section "General settings (Page 28)" <p>Procedure</p> <ol style="list-style-type: none"> 1. Insert the card into the card reader. 2. Select "Smartcard" as the login method. 3. Click the "Smartcard PKI Login" icon. 4. Enter your PIN. 5. Click the "Log in" button.
Local certificate	<p>Requirement</p> <ul style="list-style-type: none"> • The relevant PKI CA certificates are installed on the SINEMA RC server. • The certificate file (*.p12 *.pfx) is available on the PC or notebook. • The user is configured as PKI user on the server. <p>Procedure</p> <ol style="list-style-type: none"> 1. Navigate to the storage directory of the certificate file. 2. Select the certificate file and click the "Open" button. 3. If the file is password-protected, enter the password. 4. Click the "Log in" button.

Login via ...	Procedure
A UMC server with user name / password	<p>Requirement</p> <ul style="list-style-type: none"> • A user is created on the UMC and assigned to a UMC user group. • A valid SINEMA RC UMC license (MLFB 6GK1724-2VH03-0BV0) or trial license is activated on the SINEMA RC server. • The connection to the UMC server is set up on SINEMA RC server; see SINEMA Remote Connect - Server, "UMC Settings" section. • A role is created on the SINEMA RC server and uses the same name for the UMC user group to which the relevant user is assigned on the UMC; see SINEMA Remote Connect - Server, section "Managing roles and rights". <p>Procedure</p> <ol style="list-style-type: none"> 1. Enter the user name and the password. 2. Click the "Log in" button.

4. Log in to the SINEMA RC Client.
5. Check the validity of the certificates.
 - If the CA certificate of the server has not been stored in the certificate store of the PC before logging in, you are prompted to check the Web server certificate and confirm it if required.
Click on the "Allow" button when you are sure that the correct Web server certificate is displayed.
 - Possibly a user agreement will be displayed. If you click the "Allow" button, the start page appears, see section "Account (Page 21)".
6. To establish a VPN tunnel to the SINEMA RC server, click the  button on the start page on the right.

A VPN tunnel is established after successful authentication and authorization. The status  **OFFLINE** to the left of the button changes to  **CONNECTED**.

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

With this function, the SINEMA RC Client logs in to the SINEMA RC Server automatically and establishes the VPN tunnel.

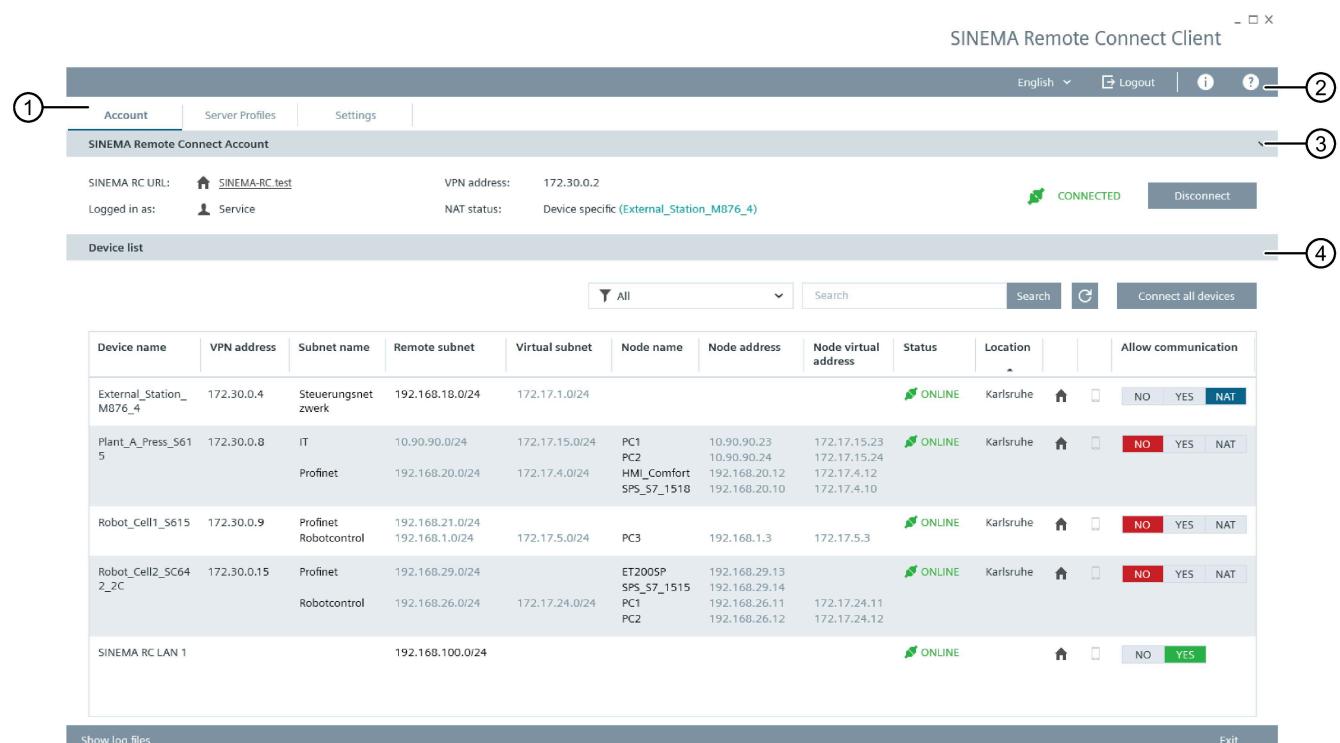
The automatic establishment is only possible with a valid SINEMA RC user account. You can find additional information in the section "Settings for automatic functions (Page 29)".

3.2 Account

After successful login, the start page of the SINEMA RC Client is displayed on the "Account" tab.

The following areas are available:

- Navigation ①
- Selection area ②
- SINEMA Remote Connect user account ③
- Content area with the device list ④



Navigation ①

You can switch to the desired page via the navigation. The following tabs are available:

- **Account**

You manage your devices on this tab.

- **Server Profiles**

On this tab, you configure connections to your SINEMA RC servers.

- **Settings**

On this tab, you make settings for the SINEMA RC Client.

Selection area ②

The following is available in the selection area:

- Drop-down list for language selection

Select the required language.

-  **Logout**

Closes the application but does not stop communication between the SINEMA RC Client and the server.

-  **Info**

Opens information on the product.

-  **Help**

Opens the online help in a new browser window.

SINEMA Remote Connect account ③

In the left section, you get an overview of the user account with the IP address of the SINEMA RC server as well as the name of the user currently logged in. The  button or clicking the IP address of the SINEMA RC server opens the WBM on the SINEMA RC Server.

Information on the client is shown in the middle part. If a VPN connection exists, the VPN address of the client is displayed. "NAT Status" indicates whether the manual or device-specific NAT settings are used.

The status of the VPN connection is displayed on the right:

-  **CONNECTED** - VPN connection is established
-  **OFFLINE** - No VPN connection established

Buttons:

-  **Connect**

Start the VPN connection establishment to the SINEMA RC server

-  **Disconnect**

Terminates the VPN connection

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.

Device list ④

The following buttons are located above the device list:

-  **Search parameter**

Selection list with search criteria

-  **Search filter**

Input box for the search function

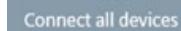
Enter a term in the input box, e.g. a device name for which you need more information, and start the search with the ENTER key or by clicking on the magnifying glass symbol. Choose the desired filter criterion with the magnifying glass symbol to restrict the search results.

-  **Refresh**

To update the display in the device list, click the "Refresh" button.

-  **Disconnect all devices**

To terminate the connections to the server for all devices from the device list, click the button "Disconnect all devices".

-  **Connect all devices**

To connect all devices in the device list to the server, click on the "Connect all devices" button. The route to each individual device is transferred to the routing table of the client PC. All devices can be reached by the client.

The device list contains information about the connected devices.

Field	Description	
Device name	Displays the name of the available device. The name is adopted from the settings of the SINEMA RC Server.	
VPN address	Shows the VPN address of the device that the device receives from the SINEMA RC Server.	
Subnet name	Shows the name of the subnet accessible from the device.	
Remote subnet	<p>Shows the IP address of the subnet. This requires the logged-on user to be a member of the user group that is permitted to access the subnet.</p> <p>If this is not the case, only the subnet name and the nodes that they are permitted to access are shown.</p> <p>If several IP addresses are created, they are displayed one under the other.</p>	
Virtual subnet	<p>Shows the IP address of the virtual subnet if NAT mode is configured on SINEMA RC Server.</p> <p>If several IP addresses are created, they are displayed one under the other.</p>	
Node name	Shows the name of the node.	
Node address	Shows the IP address of the node.	
Node virtual address	Shows the virtual IP address of the node if NAT mode is configured on the SINEMA RC Server.	
Status	Indicates whether the connection to the device is established:	
	 ONLINE	The device is connected
	 OFFLINE	The device is not connected
	Disabled	The device is disabled.
Location	Displays the location of the device.	

Field	Description
Actions	<p>Shows the actions enabled for this device:</p> <ul style="list-style-type: none"> Opens the WBM on the device. If the device is not connected, the SINEMA RC Server sends the wake-up SMS message to the device. <p>This action is only available for the connection type "Wake-up SMS" or "Wake-up SMS & digital input".</p> <p>Only with RTU 303xC:</p> <p>For RTUs, you can also add a wake-up SMS message with a specified deadline. At exactly the time you send with the SMS message, the RTU establishes a connection to its communication partner.</p> <p>When you click on the action, the "Select wake-up time" dialog opens.</p> <ul style="list-style-type: none"> Wake up at selected time: The RTU sends the SMS message at the selected time. Wake up now: The RTU sends the SMS message immediately.
Allow communication	<p>Use the following buttons to manage routes and NAT settings to the remote subnets of individual devices.</p> <ul style="list-style-type: none"> NO The route to the device is removed from the routing table of the client PC. The device can no longer be reached by the SINEMA RC Client. YES The route to the device is entered in the routing table of the client PC. The device can be reached by the SINEMA RC Client. NAT Only for devices with virtual subnets In addition to the route entry, the destination NAT settings of the device are configured in the SINEMA RC Client and on the client PC. <p>Note: If you activate NAT, existing VPN tunnels are automatically terminated. Then click on the "Connect" button to re-establish the connection to the SINEMA RC server.</p>

To show and hide columns in the device list, right-click the device list and make the desired adjustments. You can change the sorting order of the columns by left-clicking the headers of the individual columns and moving them to the desired position of the header with the mouse button held down.

The following buttons are located below the device list:

- Show log files

Click on "Show log files" to obtain log information.

On three tabs, you can view saved log files with time stamp and edition.

To open log files on your PC, click the "Open log folder" button, which is located below the list on the left. You can find saved log files under the following paths:

- 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)

- OpenVPN

(C:\ProgramData\Siemens\Automation\SINEMA_RC_Client\logs\openvpn.log)

To close the "Show log files" window, click "Close" on the bottom right.

- Exit

Closes the SINEMA RC Client application and closes the connection to the SINEMA RC Server.

3.3 Server Profiles

You configure the access data in the server profiles in the "Server Profiles" tab. You manage the created server profiles on this page.

Adding a server profile

For a clearer overview, you can collapse  and expand  this area.

1. Configure the SINEMA RC server:

Field	Meaning
SINEMA RC server name	Enter a name.
SINEMA RC server URL	Enter the IP address of the SINEMA RC server. If the SINEMA RC server uses a port other than the HTTPS standard port 443, enter the port number along with the server address (IP address or FQDN). Separate the entries of the server address and the port number with a colon ":", e.g. 192.168.234.1:6443
SINEMA RC username	Enter the name of the user. The user should be created on the SINEMA RC server.
Login method	From the list, select the method with which the user should log in to the SINEMA RC server: <ul style="list-style-type: none">• User name and password• Smart card• Local certificate• User name and password (UMC user) For more information, see section "Login (Page 17)".
Comment	You can enter a comment.

2. Save the settings with "Save".

Result

The server profile has been created and the new entry will be added in the table under the most recently configured server.

Editing the server profile

If you want to edit or copy a server profile, click on  for the respective server profile. The current settings are applied to the configuration fields. Adapt the settings and save the profile.

To delete, click on .

3.4 Settings

You can make the following settings on the "Settings" tab:

- General Settings
 - Connection settings
 - Local port settings
 - Proxy settings
 - Smartcard settings
- Notification settings
- Settings for automatic functions
 - Settings for automatic login
 - Settings for automatic operations
 - Automatic update of the device list

The settings are divided into areas that can be collapsed  and expanded  for clarity.

3.4.1 Making general settings

Connection settings

You define the protocol under the connection settings.

- UDP: Connection over UDP
- TCP: Connection over TCP
- All: Connection over UDP and TCP

Local port settings

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

To change the local ports, make the following settings:

OpenVPN management port	Enter the OpenVPN management port via which the OpenVPN service is addressed.
SINEMA RC Client service port	Enter the SINEMA RC client service port via which the SINEMA RC client service can be reached.
SINEMA RC Client service status	Shows the status of the SINEMA RC client services. The following statuses are possible: <ul style="list-style-type: none">• Certificate valid• Certificate invalid• Certificate error, unable to connect

If you change the default port, existing connections are terminated. In this case, click the "Connect" button on the "Account" tab again to re-establish the connection to the SINEMA RC server.

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 requests from the client and forwards them to the responsible 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. You can find out whether your proxy server supports OpenVPN from your network administrator.

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

Proxy settings	Select the check box to make the proxy settings. The proxy server is disabled by default.
Proxy type	Select the type of proxy server: <ul style="list-style-type: none">• HTTP: Proxy server only for access using HTTP• SOCKS: Universal proxy server

Server	Enter the IP address of the proxy server.
Port	Enter the port through which the proxy server can be reached.
OpenVPN auth. method	<p>Select the authentication method:</p> <ul style="list-style-type: none"> None: No authentication Basic: Standard authentication. User name and password are sent unencrypted. NTLM: Authentication according to NTLM standard (Windows user login). <p>Note: When the "Using proxy" option is selected, authentication according to the NTLM standard is not available.</p>
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.

Smart card setting

1. Make sure that the selected driver is compatible with the OpenSSL version 1.1.1.
2. To log in with the smartcard, specify the path to the PKCS#11 library.

3.4.2 Notification settings

In the "Notification settings" area, you can enable the "Show client-server incompatibility notification" option. If there are existing problems, you receive a note on them. You can disable this option to no longer receive incompatibility notifications.

3.4.3 Settings for automatic functions

Connecting to the SINEMA RC server automatically

The automatic establishment is only possible with a valid SINEMA RC user account.

Logging in to SINEMA RC server automatically:

1. Enable the option "Start SINEMA RC Client automatically after Windows login" under "Settings for automatic login".
2. Enter the user name, the password and the password confirmation.
3. Click the "Save" button.

The SINEMA RC client logs into the SINEMA RC server automatically after Windows login. If two-factor authentication is enabled in the role setting, you generate a one-time token with the authentication app and enter this token.

Automatic establishment of the VPN tunnel

1. If the VPN tunnel should be established automatically after login, enable the option "Automatic tunnel establishment after SINEMA RC Client login" under "Settings for automatic operations".
2. Confirm the settings with the "Save" button.

Updating the device list automatically

You can configure an interval for automatic update of the device list under "Settings for automatic operations".

The range of values for the interval is: 1 ... 999 minutes.

Appendix A

A

A.1 Syslog messages

Event Viewer

The Syslog messages are saved locally in the Microsoft Windows Event Viewer and not sent to a Syslog server.

1. Enter "Event Viewer" in the search line of the start menu.
2. Click the "Event Viewer" entry to start the Event Viewer.
3. Click the "Siemens Automation" entry for "Application and Services Logs".

The log entries are listed in tabular form. When you click on an entry, the detail view opens in the bottom window area.

A.1.1 Tags in Syslog Messages

The Syslog messages can contain variables that are filled dynamically with the data of the respective event. These variables are displayed within curly brackets {variable} in the "Message text" field in section "List of Syslog Messages (Page 32)".

The following variables occur in Syslog messages:

Parameter	Description	Format	Possible values or example
User name	String that identifies the authenticated user based on his/her name without spaces	%s	Peter_Maier
IP address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2	192.168.10.128
Client version	String for the version of the installed client software	%s	V3.0
Server version	String for the version of the installed server software	%s	V3.0
Time seconds	Number of seconds	%d	600
Reason	String for the cause of the event	%s	e.g. unsuccessful authentication

Appendix A

A.1 Syslog messages

A.1.2 List of Syslog Messages

A.1.2.1 Identification and authentication of human users

Message text	User {User name} has logged in via HTTPS to server {IP address}
Example	User Peter_Maier has logged in via HTTPS to server 192.168.10.128
Explanation	The user has successfully logged in to the device with the user name/password or PKI via a local interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	User {User name} failed to log in via HTTPS to server {IP address}
Example	User Peter_Maier failed to log in via HTTPS to server 192.168.10.128
Explanation	Login to the device via a local interface failed. Incorrect user name or password entered during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	Client version {Client version} is fully compatible with server version {Server version}.
Example	Client version V2.1 is fully compatible with server version V2.1.
Explanation	The client and server versions are compatible with one another.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	Client version {Client version} is not fully compatible with server version {Server version}
Example	Client version V2.1 is not fully compatible with server version V2.1
Explanation	The client version is not fully compatible with the server version.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	User {User name} has logged out
Example	User Peter_Maier has logged out
Explanation	A user logged out, either manually or automatically via the Web interface due to a timeout. User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

A.1.2.2 Unsuccessful logon attempts

Message text	User {User name} account is locked for {Time seconds} seconds after {Failed login count} unsuccessful login attempts
Example	User Peter_Maier account is locked for 600 seconds after 10 unsuccessful login attempts
Explanation	If there were too many failed logins, the corresponding user account has been locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

A.1.2.3 Access via untrusted networks

Message text	VPN connection to server {IP Address} successfully established via OpenVPN
Example	VPN connection to server 192.168.1.105 successfully established via OpenVPN
Explanation	The VPN connection is established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	VPN tunnel to server {IP address} closed
Example	VPN tunnel to server 192.168.1.105 is closed
Explanation	The VPN connection is closed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	VPN connection to server {IP address} failed. Fatal error: {Reason}
Example	VPN connection to server 192.168.10.128 failed. Fatal error: unsuccessful authentication
Explanation	The VPN connection could not be established due to invalid authentication.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

A.1.2.4 Software and information integrity

Message text	Integrity violations in configuration data detected
Example	Integrity violations in configuration data detected
Explanation	An integrity fault was detected while the configuration integrity was being checked.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Index

A

Abbreviations/acronyms, 3

D

Definition of terms, 3

G

Glossary, 6

I

Installation

Procedure, 14

L

License, 3, 9

Local port settings, 28

M

Minimum requirements, 9

O

Order ID, 3

P

Processor, 9

R

RAM, 9

S

Service & Support, 6

Set

Local port, 28

VPN proxy, 28

SIMATIC NET glossary, 6

SIMATIC NET manual, 4

Start page

Device list, 23

Navigation, 21

Selection area, 22

User account, 22

VPN proxy settings, 28

Syslog messages

Variables, 31

T

Training, 6