SIEMENS

SIMATIC NET

Industrial Remote Communication - Remote Networks SINEMA Remote Connect - Server

Operating Instructions

01/2019

C79000-G8976-C383-07

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

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

C79000-G8976-C383-07
Ⓟ 01/2019 Subject to change

Preface

Purpose of this documentation

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

Validity of this documentation

This manual is valid for the following software version:

- SINEMA Remote Connect as of version V2.0

Licenses

The following licenses are available for the product:

Product name	Article number of licenses	Number of configurable participants (users and devices)
SINEMA Remote Connect	6GK1720-1AH01-0BV0	4
SINEMA Remote Connect 64	6GK1722-1JH01-0BV0	+64
SINEMA Remote Connect 256	6GK1722-1MH01-0BV0	+256
SINEMA Remote Connect 1024	6GK1722-1QH01-0BV0	+1024

The following products are available for activating the connection to the SINEMA Remote Connect Server:

Product name	Article number
SINEMA Remote Connect Client	6GK1721-1XG01-0AA0
KEY-PLUG SINEMA RC (SCALANCE M-800, SCALANCE S615)	6GK5908-0PB00

Supported products

In the "Connectable nodes (Page 25)" section, you can find information about the nodes supported.

Abbreviations/acronyms and terminology

- **SINEMA RC**

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

- **SCALANCE M-800**

  This abbreviation applies to the following devices if the content of the description applies equally to these devices in the relevant context:

  – SCALANCE M874-2

  – SCALANCE M874-3

  – SCALANCE M876-3

  – SCALANCE M876-4

  – SCALANCE M812

  – SCALANCE M816

New in this release

- Dedicated Device Access (DDA)

  User-specific access rights for dedicated nodes can be stored in the subnet via DDA.

- Optimization of the device configuration

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 - Remote Networks
- IP-based communication
- STEP 7 Basic / Professional
- SIMATIC S7

Further documentation

- Operating instructions "SINEMA Remote Connect Client"

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

- 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 remote networks 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 "Remote Networks" area:

  Link to the "Remote Networks" area (https://support.industry.siemens.com/cs/ww/en/ps/21778)

  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 entry ID:

  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

Application and properties 1

1.1 Application

Use of the SINEMA Remote Connect server

The SINEMA RC Server provides end-to-end connection management of distributed networks via the Internet. This also includes secure remote access to underlying networks for maintenance, control and diagnostics purposes. The communication between SINEMA RC Server and the remote participants is via a VPN tunnel taking into account the stored access rights. The connection is established encoded using IPsec or OpenVPN.

The SINEMA RC Server can be configured via the Web Based Management (WBM).

The connection to the WBM via the Internet/WAN takes place over the HTTPS protocol. To establish a connection to the WBM of the server, users must log in by entering a user name and password or with a smartcard.

Supported products

The following products are suitable for connecting to the SINEMA RC Server:

- SCALANCE M874, SCALANCE M876, SCALANCE M816, SCALANCE M826, SCALANCE M804PB
- SCALANCE S615
- SINEMA RC Client
- SCALANCE S602, SCALANCE S612, SCALANCE S623, SCALANCE S627-2M
- SCALANCE SC632-2C, SCALANCE SC636-2C, SCALANCE SC642-2C,SCALANCE SC646-2C
- CP 1200
- CP 1543-1, CP 1543-1SP
- RM 1224
- RTU3010C, RTU3030C, RTU3031C

In the section "Connectable nodes (Page 25)" you will find information about which product versions and SINEMA RC versions are compatible with each other.

Protection concept

To protect the SINEMA RC Server from unauthorized access, system access is protected in several ways:

- Authentication
  - Access is password protected by entering the user name and password, see section Create a new user (Page 86).
  - Access is achieved using a Smartcard with a PIN procedure (Personal Identification Number). To check the identity a certificate is used.
- User rights and roles

  The task-dependent access rights are specified using roles and user rights. For more detailed information, refer to the section Managing roles and rights (Page 83).

1.2 Overview of functions

Configuring the SINEMA Remote Connect server

The SINEMA RC Server can be configured via a Web Based Management (WBM).

Configuration of the SINEMA RC Server

In the WBM, you can use the following functions:

- Basic settings of the system
  - Settings of the system and address parameters
  - Language of the WBM
- Specifying users, groups and their rights
  - Creation of users and devices including password assignment
  - Creation and assignment of roles and rights
  - Assignment of participant groups
- Configuration of connections
  - Creation of communication relations between the participant groups

Commissioning/configuration of end devices

- You can create partial configurations globally for the end devices. This includes, for example, configuration of NAT etc.
- Via the server, configuration information can be loaded on the end device.

Management of the server

- Changing settings of the system or participants
- Activating / deactivating connections between participants

Connection management

- Display of all connections available online and offline
- Connection configuration with creation of certificates
- Establishment and termination of connections
- Sending a wake-up SMS message to a device, for example to establish a secure connection

1.3 User concept

SINEMA RC Server has an extensive system of access rights. This system allows the administrator to grant or deny user access to certain program objects individually and according to need. During configuration, you should take into account the following criteria in the role:

- Network security
- IT experience of the users
- The necessity for certain functions
- User friendliness

Note

The management of rights is one of the most important tasks of an administrator

This should therefore be planned and configured to meet the specific requirements while taking into account security-relevant aspects. We strongly advise you to familiarize yourself with the user and roles concept of SINEMA RC Server. New or modified settings should always be checked in terms of their intended effect.

Basics

The access rights in SINEMA RC are specified using the following objects:

- Users
- Roles
- Rights
- Participant groups

In principle, the following applies:

Every user can be assigned certain rights.

Every role can be assigned various rights that are transferred automatically to all its members (users, participant groups).

Each user can have several roles and be a member of several participant groups.

Users

So that a created user can create and manage other users, the user must have the user right "Manage users" assigned.

"admin" user

As default, after the installation the predefined user "admin" is available. With this user name, you can log in once after the installation. After this you will be prompted to create a new user. The "admin" role is assigned to this user automatically.

This administrator has the right to access all functions and can set up the system. This includes creating users and assigning roles and rights to them. For more detailed information, refer to the section "Managing roles and rights (Page 83)".

This administrator is listed with the user accounts and can neither be edited or deleted. The "admin" user is no longer available.

Logging on

The following options are available:

- Logon with user name and password
- Logon with the Smartcard
- Logon with PKI certificate

Roles

In SINEMA Server, there are two predefined roles available with corresponding access rights.

Standard role	Description
admin	The role has all access rights and does not belong to a participant group.
vpn_user	The role has no access rights and is assigned to the participant group automatically. The role may only establish VPN connections to the participants that belong to the participant group vpn_user_group.

Participant group

in SINEMA RC Server, there is a predefined participant group available.

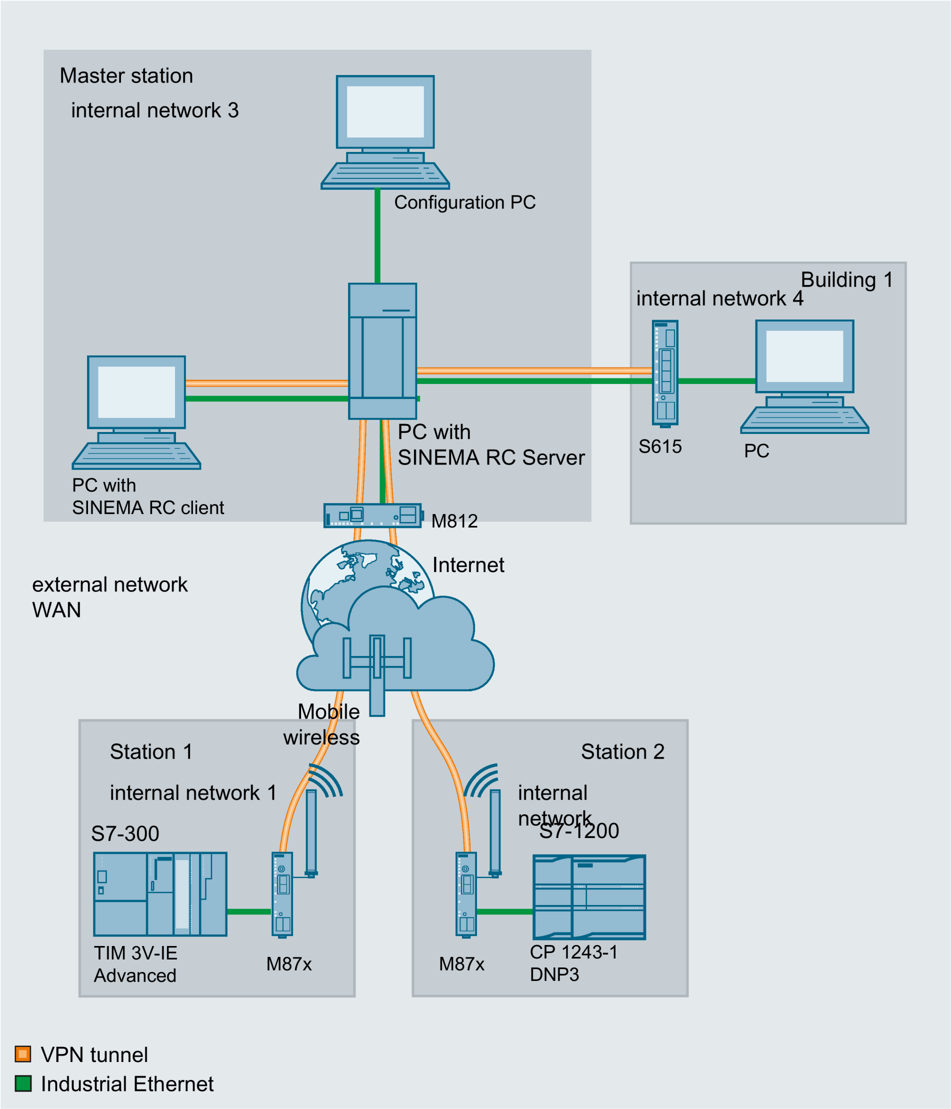
Standard participant group	Description
vpn_user_group	The communication between the nodes is not permitted.

1.4 Configuration example

1.4.1 TeleControl with SINEMA RC

In this configuration, the remote maintenance master station is a connected to the Internet/intranet via the SINEMA RC Server. The plants communicate via SCALANCE M or the SCALANCE S615 that establish a VPN tunnel to the SINEMA RC Server. In the master station, the SINEMA RC Client establishes a VPN tunnel to the SINEMA RC Server. To establish the VPN tunnel, OpenVPN is used.

The devices must log on to the SINEMA RC server. For this, a WBM is available. The VPN tunnel between the device and the SINEMA RC Server is established only after successful authentication. Depending on the configured communication relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.



Procedure

To be able to access a plant via a remote maintenance master station, follow the steps below:

1. Establish the Ethernet connection between the device and the connected configuration PC.
2. Establish a connection to the WAN.
3. Log the new device on to the SINEMA RC Server.
4. Set up the connection to the SINEMA RC Server on the device.
5. Put the new device into operation.

You will find instructions on the procedure in the Getting Started for SINEMA Remote Connect.

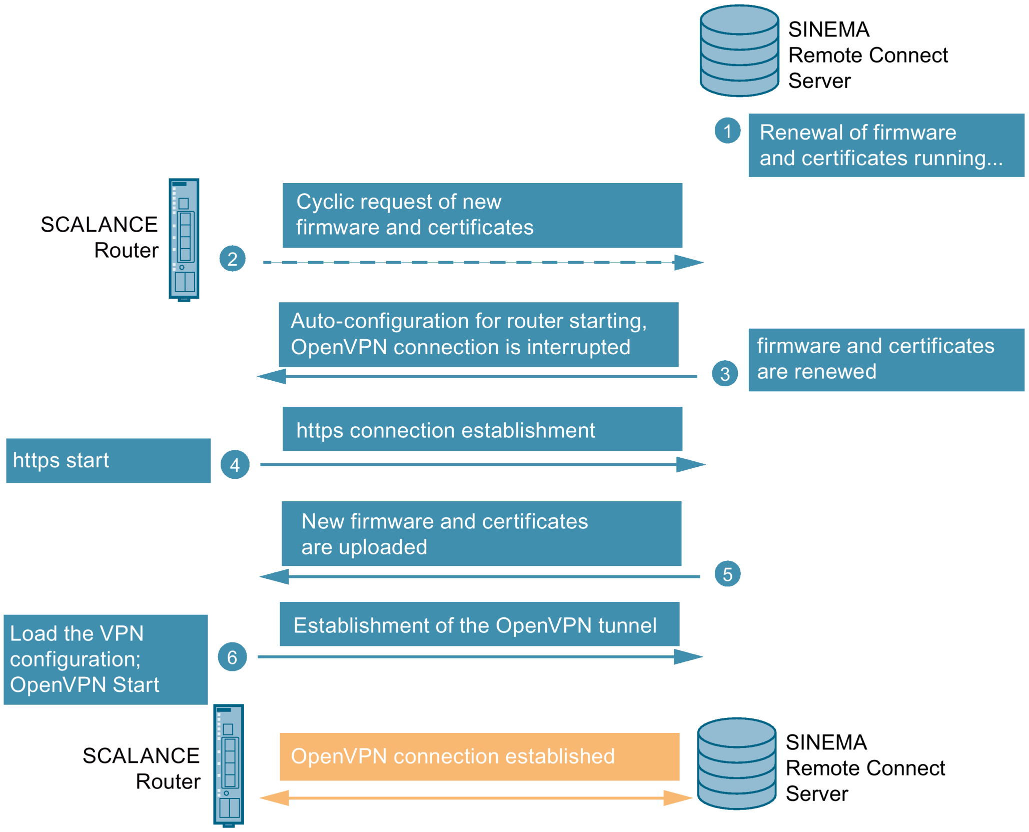
1.5 Automatic distribution of certificates and firmware

1.5.1 Automatic updating of certificates and firmware

If a connection is established between the SINEMA RC Server and the SCALANCE router, the router automatically requests firmware and certificate updates. This request is made cyclically at specified time intervals, which you can set as the "Autoenrollment Interval" parameter on the router. For the SCALANCE S615/M-800/SC-600, configure the parameter in the WBM under "System > SINEMA RC".

You can find additional information about this in the configuration manual of the respective device.

Procedure


SINEMA
Remote Connect
Server
1
Renewal of firmware and certificates running...
SCALANCE
Router
Cyclic request of new firmware and certificates
2
Auto-configuration for router starting, OpenVPN connection is interrupted
firmware and certificates are renewed
3
https connection establishment
https start
4
New firmware and certificates are uploaded
5
Load the VPN configuration; OpenVPN Start
6
Establishment of the OpenVPN tunnel
SCALANCE
Router
OpenVPN connection established
SINEMA
Remote Connect
Server

1. If firmware and certificate updates are available, the SINEMA RC Server renews them automatically or the user can renew them manually.
2. After a time configured in the router, the SCALANCE router cyclically asks the server whether a newer firmware file is available or whether a new certificate is available. The default polling interval is 60 minutes.
3. If the firmware or the certificate has been renewed on the server, the autoconfiguration starts: The OpenVPN connection is terminated briefly.
4. The SCALANCE router initiates the https connection to the SINEMA RC Server.

5. The SINEMA RC Server sends a configuration file to the SCALANCE router. The SCALANCE router receives the new firmware and certificates and stores them.
6. The SCALANCE router load the complete VPN configuration and establishes the OpenVPN tunnel to the server.

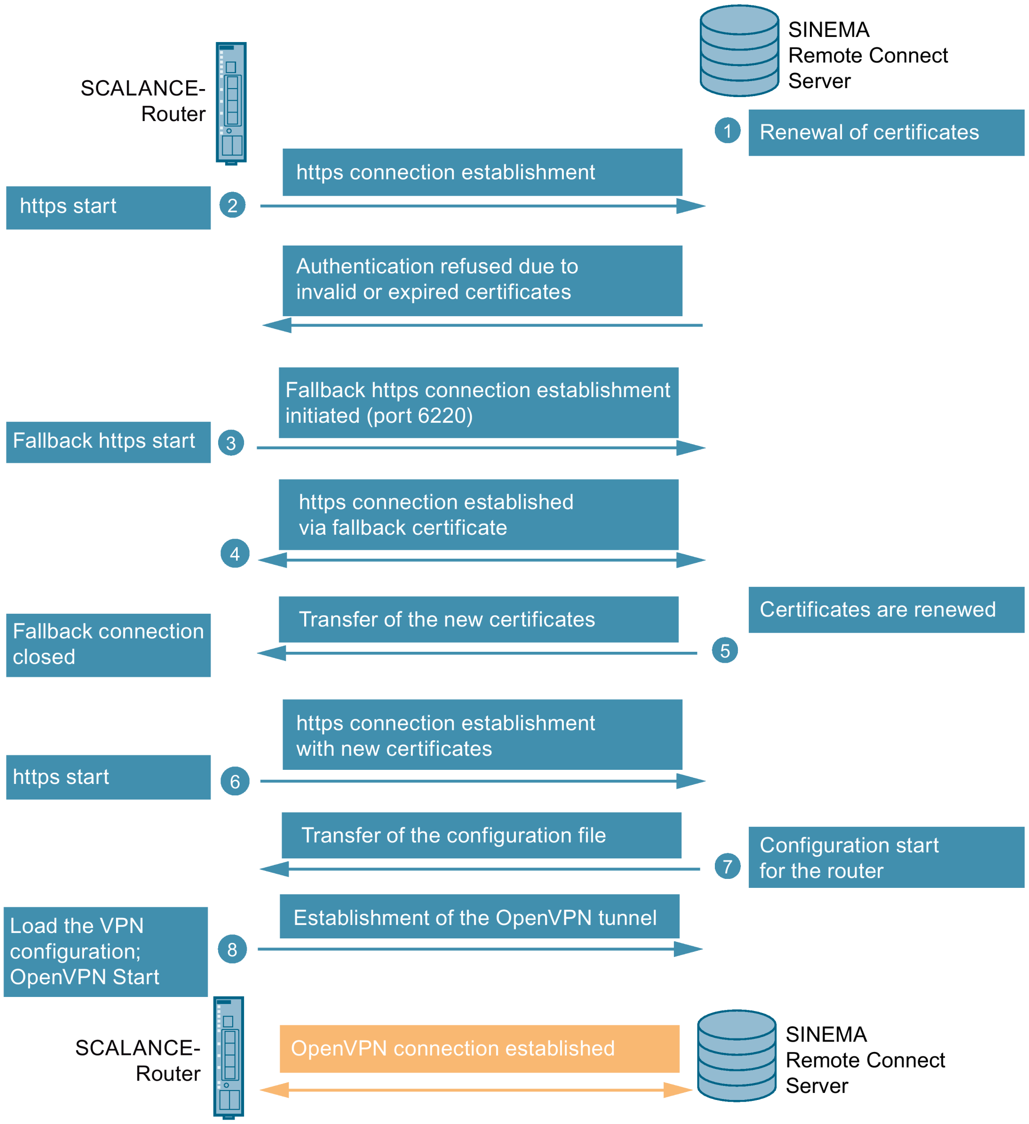
Result

The VPN connection between the SINEMA RC Server and the SCALANCE router is set up.

1.5.2 Updating certificates with fallback connection

Due to expired or invalid certificates, it is not possible to establish a connection via https. As a result, the SCALANCE router cannot automatically update the relevant certificates. To be able to establish the connection between the server and the router despite expired or invalid certificates, the fallback connection takes over during this time.

Procedure


SCALANCE-Router
SINEMA Remote Connect Server
1 Renewal of certificates
https connection establishment
https start
2
Authentication refused due to invalid or expired certificates
Fallback https connection establishment initiated (port 6220)
Fallback https start
3
https connection established via fallback certificate
4
Transfer of the new certificates
Certificates are renewed
Fallback connection closed
5
https connection establishment with new certificates
https start
6
Transfer of the configuration file
7 Configuration start for the router
Establishment of the OpenVPN tunnel
Load the VPN configuration; OpenVPN Start
8
SCALANCE-Router
OpenVPN connection established
SINEMA Remote Connect Server

1. Before the certificates expire, the SINEMA RC Server renews them automatically or the user renews them manually.
2. The SCALANCE router tries to establish an https connection so that automatic configuration is possible. However, the connection is rejected because the certificate of the SCALANCE router is invalid or has expired.
3. The SCALANCE router then starts a fallback connection.
   The fallback connection is an https connection through a separate https port (port 6220), via which the server sends a fallback certificate to the router for verification. The router can now authenticate the server with the fallback certificate.
4. An https connection to the server is established.
5. The SCALANCE router can receive the new certificates and stores them under Certificates. The invalid certificates are automatically deleted. The fallback connection is now complete.

6. The connection to the SINEMA RC Server is now established as usual, but with the new certificates. The SCALANCE router establishes an https connection to the SINEMA RC Server for this purpose. The server identifies itself with its Web server certificate. The router authenticates itself on the server using a fingerprint or CA certificate.
7. The server now starts the automatic configuration for the router. The router receives a configuration file with the required parameters and certificates for setting up the VPN tunnel, including the device certificate and the fallback certificate.
8. The SCALANCE router load the complete VPN configuration and establishes the OpenVPN tunnel to the server.

Result

The VPN connection between the SINEMA RC Server and the SCALANCE router is set up.

Requirements for operation 2

2.1 Requirements

Hardware requirements

Component	Minimum requirements	Recommended requirements	Recommended requirements for the maximum configuration limits (see below)
Processor	Dual Core CPU 2.4 GHz	Quad Core CPU 2.66 GHz	Quad Core CPU 3.6 GHz 4 threads and hyperthreading disabled
RAM	2 GB	4 GB	8 GB
Network adapter	1x	1x **Note:** SINEMA RC Server supports up to four network adapters.	1x Gbps Ethernet **Note:** SINEMA RC Server supports up to four network adapters.
Hard disk	> 60 GB	> 60 GB	250 GB SSD

Virtualization platforms

The SINEMA RC Server application can also be installed in a virtual machine (VM).

- VMware vSphere Hypervisor (ESXi) 6.5
- VMWare Workstation 14

If you want to install the SINEMA RC Server application on a virtual machine, create a partition for a 64-bit Ubuntu system. SINEMA RC itself is an application that already brings the 64-bit Ubuntu system with it as the operating system and installs it like an operating system.

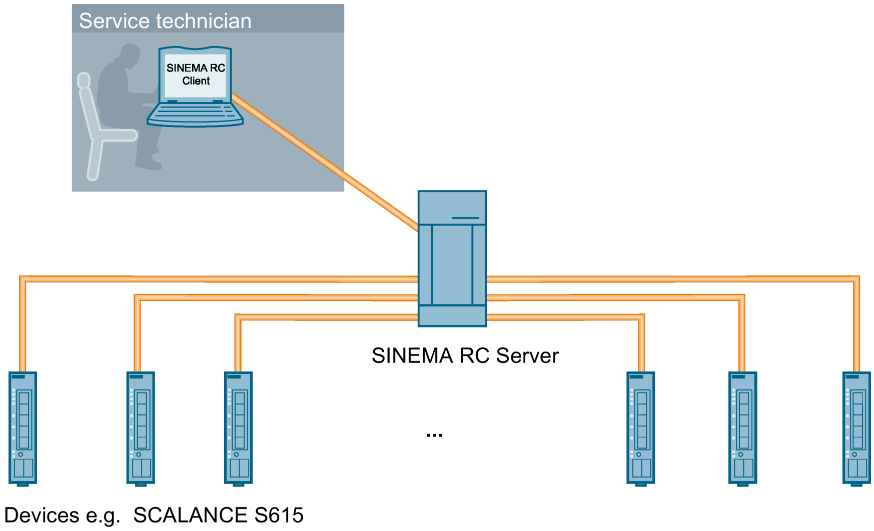
Maximum configuration limits

Maximum overall data transfer for all devices: 800 Mbps

Maximum number of devices and users connected simultaneously for one subnet per device: **1024**

User/device combinations can be freely selected up to the maximum overall quantity structure.

As the number of subnets is also dependent on the communication relationships permitted among one another, for example, these must be checked/questioned and restricted, where necessary. If devices do not need to communicate with each other, you should suppress communication in order to ensure optimal behavior of the devices.



2.2 Connectable nodes

The connection to SINEMA RC can be established via various media such as mobile wireless, DSL or existing private network infrastructures.

The following SCALANCE products have been tested for connection to SINEMA RC:

SINEMA RC client

		SINEMA RC Client Version				
		1.0	1.0 SP1	1.0 SP2	1.0 SP3 + SP4	2.0
SINEMA RC Server Version	1.0	✓	-	-	-	-
	1.1		✓	-	-	-
	1.2	-	-	✓	-	-
	1.3	-	-	-	✓	-
	2.0	-	-	-	-	✓

Connectable nodes

Device type	Node	MLFB number	Firmware version	Connection establishment to the SINEMA RC Server					Sub-nets (vlan)
				Wake-up SMS	Digital input	Per-manent	IPsec	Open VPN	
SCALANCE S615	S615	6GK5615-0AA00-2AA2	As of 4.0	-	✓	✓	✓	✓	16
SCALANCE SC-600	SC632-2C	6GK5632-2GS00-2AC2	as of 1.0	-	✓	✓	-	✓ [1]	257
	SC636-2C	6GK5636-2GS00-2AC2	as of 1.0	-	✓	✓	-	✓ [1]	257
	SC642-2C	6GK5642-2GS00-2AC2	as of 1.0	-	✓	✓	✓	✓ [1]	257
	SC646-2C	6GK5646-2GS00-2AC2	as of 1.0	-	✓	✓	✓	✓ [1]	257
SCALANCE S600 [2]	S612	6GK5612-0BA10-2AA3	As of 4.0.1.1	-	-	✓	✓	-	
	S623	6GK5623-0BA10-2AA3	As of 4.0.1.1	-	-	✓	✓	-	
	S627-M	6GK5627-2BA10-2AA3	As of 4.0.1.1	-	-	✓	✓	-	
SCALANCE M800 Mobile	M874-2	6GK5874-2AA00-2AA2	As of 4.1	✓	✓	✓	✓	✓	16
	M874-3	6GK5874-3AA00-2AA2	As of 4.1	✓	✓	✓	✓	✓	16
	M876-3	6GK5876-3AA02-2BA2	As of 4.1	✓	✓	✓	✓	✓	16
	M876-4	6GK5876-4AA00-2BA2 (EU) 6GK5876-4AA00-2DA2 (NAM) [3]	As of 4.1	✓	✓	✓	✓	✓	16
SCALANCE M816 Modems	M816-1	6GK5816-1AA00-2AA2 (EU) 6GK5816-1BA00-2AA2 (NAM) [3]	As of 4.2	-	✓	✓	✓	✓	16

Device type	Node	MLFB number	Firmware version	Connection establishment to the SINEMA RC Server					Sub-nets (vlan)
				Wake-up SMS	Digital input	Per-ma-nent	IPsec	Open VPN	
SCALANCE M804 PB	M804PB	6GK5804-0AP00-2AA2	As of 6.0	-	✓	✓	✓	✓	16
SIMATIC CP1200	CP 1243-1	6GK7243-1BX30-0XE0	As of 3.1	-	-	✓	-	✓	
	CP 1242-7 GPRS	6GK7242-7KX31-0XE0	As of 3.1	-	-	✓	-	✓	
	CP 1243-7 LTE	6GK7243-7KX30-0XE0 (EU) 6GK7243-7SX30-0XE0 (NAM) [3]	As of 3.1	-	-	✓	-	✓	
	CP 1243-8 IRC	6GK7243-8RX30-0XE0	As of 3.1	-	-	✓	-	✓	
SIMATIC CP 1543-1	CP 1543-1	6GK7543-1AX00-0XE0		-	-	✓	✓	-	1
SIMATIC ET 200SP CPs	CP 1543SP-1	6GK7543-6WX00-0XE0	As of 2.0	-	-	✓	-	✓	
	CP 1542SP-1 IR C	6GK7542-6VX00-0XE0	As of 2.0	-	-	✓	✓	✓	
SIMATIC RTU 303XC	RTU3031C	6NH3112-3BB00-0XX0		✓	- [4]	✓	-	✓	
	RTU3030C	6NH3112-3BA00-0XX0		✓	- [4]	✓	-	✓	
SIMATIC RTU 3010C	RTU3010C	6NH3112-0BA00-0XX0		-	- [4]	✓	-	✓	
RUGGEDCOM RM1224	RM1224 LTE(4G)	6GK6108-4AM00-2BA2 (EU) 6GK6108-4AM00-2DA2 (NAM) [3]	As of 4.1	✓	✓	✓	✓	✓	16

1) The OpenVPN connection can only be established to the SINEMA RC Server.

2) The configuration must only be performed via SCT (IPsec) with the export/import functions. Autoconfiguration with OpenVPN is not possible.

3) North America

4) The digital input on the device is not used to establish a connection to the SINEMA RC Server.

2.3 License information

To run the SINEMA RC Server application, you require a license for the product SINEMA RC.

Licenses

The license SINEMA Remote Connect is already included in the installation of the SINEMA RC Server. With this license, you can configure up to 4 participants. The number of participants can be increased with the following licenses:

- SINEMA Remote Connect 64: This license supports up to +64 participants.
- SINEMA Remote Connect 256: This license supports up to +256 participants.
- SINEMA Remote Connect 1024: This license supports up to +1024 participants.

You can find the article numbers of the licenses in the section "Preface (Page 3)".

License update

To expand the license to a higher number of participants, you require an update to a new license. To be able to make a license update, you need to obtain a new license key and enter the corresponding license number in the WBM.

The procedure for activating the license in the WBM is described in the section "Managing licenses (Page 58)".

License types 64/256/1024 can be combined. The license type is expanded according to the addition.

How many connections can actually be established simultaneously depends on the performance of the server platform.

2.4 Permitted characters

User names, passwords

When creating or changing, remember the following rules:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z !#$%&()*+,-./:;<=>?@[\]_{|}~^
Characters not allowed	" ' `
Length of the device, user or group name	1 to 30 characters
Length of the role name	1 to 80 characters
Length of the password	at least 8 characters and maximum 128 characters

Note

User names and passwords

To improve security, make sure that user names and passwords are as long as possible.

Passwords must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers.

Hostname

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z -.

2.5 Performance data

Maximum number of participant groups	Not limited
Maximum number of participants per participant group	Not limited
Maximum number of local backup copies	30
Maximum number of log archives	100

Installation and commissioning 3

3.1 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 (https://www.industry.siemens.com/topics/global/en/industrial-security/network-security/Pages/Default.aspx).
- Do not connect the device directly to the Internet. Operate the device within a protected network area.

Access to the server

- Restrict physical access to the SINEMA RC Server to qualified personnel.

  The SINEMA RC Server has an extensive system of access rights. This system allows you to grant or deny access to certain program objects individually and according to need.

Physical access

- Restrict physical access to the device to qualified personnel. Use the security mechanisms of SINEMA RC.
- Protect the SINEMA RC Server from unauthorized access by installing it in racks / control cabinets / in control rooms that can be locked.

Security functions of the software

- Keep the software up to date.
  - Check regularly for security updates for the product. You can find information on this at (https://support.industry.siemens.com/cs/ww/en/ps/21713/dl):

    The update file is signed. This ensures that only an update file created by Siemens can be downloaded.
  - Inform yourself regularly about security recommendations by published by Siemens ProductCERT (https://www.siemens.com/global/en/home/produkte/services/cert.html).
- The SINEMA RC Server includes an automatic logging function. Check this information regularly for unauthorized access.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use one password for different users and systems.

Keys and certificates

This section deals with the security keys and certificates you require to establish a connection.

- We recommend that you use certificates with a key length of 4096 bits.
- The product supports RSA 1024 - 8192 bits key length.

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

    The port is always open and cannot be closed. To use it, authentication is necessary.
  - Open (when configured)

    The port is open if it has been configured. To use it, authentication is necessary.

Table 3- 1 Services available

Protocol		Port number	Port status	Port changeable	Authentication
HTTPS	TCP	443	Open	✓	✓
HTTPS for certificate auto enrollment	TCP	6220	Open	✓	✓
OpenVPN	UDP	1194	Open	✓	✓
	TCP	5443	Open	✓	✓
IPsec	ESP	n/a	Open	--	✓
IPsec encapsulated	UDP	500	Open	--	✓
IPsec encapsulated NAPT	UDP	4500	Open	--	✓
SSH	TCP	22	Open (when configured)	✓	✓
Licensing	TCP	22350	Open	--	✓
	UDP				

Table 3- 2 Services used

Protocol		Port number	Port status
NTP	UDP	123	Outgoing when configured
DNS	TCP	53	Outgoing when configured
E-mail client	TCP	25 or other	Outgoing
HTTPS - CRL retrieval	TCP	according to URL	Outgoing
HTTPS - license activation	TCP	443	Activating the product

3.2 Installing SINEMA RC Server

Note

Keyboard layout during installation

During installation the keyboard layout "English (USA, International)" is set.

Requirement

- In the startup order, the CD/DVD is set as the first boot medium.
- The hardware requirements are met.

New installation

NOTICE

Re-installation formats the hard disk

The new installation of the SINEMA RC Server includes its own operating system, based on Ubuntu 16.04 LTS. 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.

1. Insert the data medium in the drive.
2. Switch on the PC or restart the server.
   Installation starts automatically.
3. In the following dialog, select the entry "Install/Update SINEMA Remote Connect Server". Confirm the selection with the ENTER key.

   If a version is already installed, select "Install - Fresh installation" in the following dialog. The previous configurations of the SINEMA RC Server are not adopted.
4. Follow the further instructions on the screen.

   During the installation, make the following settings for the WAN interface:

   – IP address

   – Network mask

   – Gateway

Result

The SINEMA RC Server is installed. Login with the predefined user "admin".

Before you can configure further settings using WBM, you are prompted to create a new user and check the network configuration.

Upgrading the server version

The update must be performed in the correct order: V1.0 > V1.1 > V1.2 > V1.3 > V2.0

Note

System update V1.2 > V1.3

Due to changes in the basic installation an update from V1.2 to V 1.3 is only possible using the installation CD.

1. In the navigation, select "System > Update > System update".
2. Click the "Select file" button.
3. Navigate to the storage directory and select File *.tar.gz.
4. Confirm your selection with the "Open" button.
5. Click the "Import" button.

Result

The system has been updated. Depending on the type of update, individual functions, or the entire system is restarted. To check the version following the restart, in the navigation click "System > Overview" and check the displayed software version.

See also

Update (Page 61)

Connectable nodes (Page 25)

System update V1.2 > V1.3 (Page 112)

3.3 Initial commissioning of end devices using the WBM

Commissioning the node via the WBM

Procedure

1. Configure the new device on the SINEMA RC Server.
   For more detailed information, refer to the section "Device settings (Page 70)".
   - Specify the required device information. e.g. device name, manufacturer, location etc.
   - Configure the VPN connection mode
   - Enter the password to identify the end device during the logon.
   - Assign the device to a participant group.
     For more detailed information, refer to the section "Assigning a node to a group (Page 81)".

   When the device is configured, the certificate is created automatically.
   For more detailed information, refer to the section "Overview of certificate management (Page 90)".
2. Transfer the configuration settings of the SINEMA RC Server to the device.
   - To identify the device to the SINEMA RC Server, transfer the certificate to the device and enter the password.
   - Enter the IP address of the SINEMA RC Server.
3. Put the device into operation.

Result

The device connects to the SINEMA RC Server. When the connection has been successfully established, a virtual IP address for example is transferred.

If necessary, perform further configuration steps:

1. At the device end, for example, configure firewall rules, NAT, etc.
   You can find precise step-by-step instructions in the Getting Started for SINEMA Remote Connect and in the Getting Started of the relevant device.

Configuring with Web Based Management 4

4.1 Opening Web Based Management

Calling the start page of the WBM

1. Open the Web browser.
2. In the address line of the browser, enter **https**://<IP address> of the SINEMA RC Server. You specified the IP address during the installation.

   If you use 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.

   Note

   You set the port for access to the Web server in the "System > Network configuration > Web server settings" tab.

Result

The start page of the WBM opens.

4.2 Starting the WBM

4.2.1 Logon with user name and password

Procedure

1. Enter a configured user name.

   You can find information on the first login in the following section "Logging on after the new installation".

2. Enter the corresponding password.

   You can find information on the first login in the following section "Logging on after the new installation".

3. Click the "Log in" button.
   The start page of the WBM opens. A user agreement may be displayed, see section "User agreement (Page 89)". If you click the "Accept" button, the start page appears.

Changing the current password

As a logged-in user, you can change your current password; refer to the section "Changing the current password (Page 107)".

Logging on after installing new

1. After a new installation, enter "admin" as the user name and password.

2. Click the "Log in" button.
   The WBM page "Change password" opens.

3. 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 (Page 28)". The "admin" user name is not permitted. The "admin" role is assigned to this user automatically.

   This administrator has the right to access all functions and can set up the system. This includes creating users and assigning roles and rights to them.

4. Click the "Save" button.
   After saving, you are automatically logged in with the newly created administrator. The "admin" user is no longer available.

Once you have logged on successfully, the start page appears. A user agreement may be displayed, see section "User agreement (Page 89)". If you click the "Accept" button, the start page appears.

Entering the wrong user name or password

If you enter a user name that is not configured, an error message is displayed regardless of the password entered. A user name or a variety of incorrect user names can be entered any number of times without the system being locked.

Note

Loss of the administrator password

Note down a newly assigned or modified administrator password and keep this in a safe place.

If only one administrator is set up, the loss of the administrator password means that no more administrator tasks can be performed.

There is no possibility of resetting the assigned administrator password.

Note

Incorrect entry of the password

If you enter an incorrect password with the user name an error message is displayed.

If you enter an incorrect password, a lock out time begins that is extended with each attempt to logon with an incorrect password.

4.2.2 Logon with the Smartcard / user certificates

Logging on with the smart card corresponds to a two-level security system.

The 1st level is possession of the card and the 2nd level is the personal identification number (PIN) for unlocking the smart card. On the smart card there must be the PKI certificate and the private key belonging to it.

As an alternative the PKI certificate can also be on the hard disk of the SINEMA RC client. The private key is then, however, not protected by the Smartcard, but must be protected by a different suitable measure, e.g. encryption of the private key, integrated measures in the Web browser.

Chain of certificates to the root certificate

The certificates of a PKI are often organized hierarchically:

At the tip of the hierarchy are the root certificates. These are certificates that are not certified by a higher-level certification authority. Certificate owner and certificate issuer of root certificates are identical. Root certificates are fully trusted, they are the "anchor" of trust and must therefore be known by the recipient as trustworthy certificates. They are stored in an area intended for trustworthy certificates.

Depending on the PKI, the function of root certificates can be, for example, to sign certificates of lower-level certification authorities, so called intermediate certificates. This transfer the trust from the root certificate to the intermediate certificate. An intermediate certificate can sign a certificate just like a root certificate, therefore both are "CA certificates". CA is the acronym for "Certification Authority".

This hierarchy can continue over several intermediate certificates as far as the end entity certificate. The end entity certificate is the certificate of the user to be identified. In the remaining description the end entity certificate will be known as PKI certificate

During validation the hierarchy is run through in the opposite direction. As described above the certificate issuer is identified, the signature checked with the public key, then the certificate of the higher-level certificate issuer is identified until the trust chain has been run through as far as the root certificate.

Summary: The chain of intermediate certificates as far as the root certificate must exist on the SINEMA RC Server that should validate the PKI certificate of the user.

How it works

After the chain of certificates has been installed on the SINEMA RC Server, the user can log on with his or her PKI certificate. After successfully logging on, a check is made to establish whether the contained PKI certificate of the user is valid.

Then a check is made as to whether the attributes of the PKI DN filter rules are included in the PKI certificate.

There are the following types of logon:

- User identification

  if the PKI DN filter rule applies to a user, this user is logged on with the SINEMA RC Server with the user name, see section "Creating new users (Page 86)".

- Temporary users

  If the PKI filter rule applies to a role, a temporary user is created. pkiuser _X is used as the user name. The temporary user receives the right and the access to the participant groups assigned to the role. This user is listed in "User accounts > Users & Roles".

  In the role you also specify when the temporary user will be deleted, see section "Managing role and rights (Page 83)".

Logging on with Smartcard

Requirement

- A card reader on the PC or notebook
- The card reader is connected according to the manufacturer's instructions and the driver belonging to it is installed.
- The PKI CA certificate chain is installed on the SINEMA RC Server, see section "PKI CA certificate (Page 98)".
- A smart card with a valid PKI certificate derived from one of the PKI CA certificates imported into SINEMA RC.
- PKI DN filter rules have been created.
- For the user, the logon method has been set, see section "Creating new users (Page 86)"
- The client software (Web browser or SINEMA RC client) is capable of communicating with the card reader.
  - Internet Explorer, Microsoft Edge and Google Chrome: Use Windows Crypto API which automatically recognizes an attached card reader.
  - Firefox and SINEMA RC client: For the card reader and Smartcard, the suitable PKCS11-DLL must be selected.

Procedure

1. Insert your smart card in the reader device.
2. Click the card symbol.
3. Enter your PIN and click on Log on. Possibly a user agreement will be displayed, see section "User agreement (Page 89)". If you click the "Accept" button, the start page appears.

Logon with a user certificate

Requirement

- The PKI CA certificate chain is installed on the SINEMA RC Server, see section "PKI CA certificate (Page 98)".
- The valid user certificate derived from one of the PKI CA certificates imported into SINEMA RC exists on the PC.
- PKI DN filter rules have been created.
- For the user, the logon method has been set, see section "Creating new users (Page 86)"

Procedure

1. Navigate to the storage directory of the PKI certificate.
2. Select the certificate file and click the "Open" button.

   If the file is password protected, enter the password.
3. Click the "Log on" button. Possibly a user agreement will be displayed, see section "User agreement (Page 89)". If you click the "Accept" button, the start page appears.

Result

During the logon, a check is made to establish whether the PKI certificate is valid. Then a check is made as to whether the attributes of the PKI DN filter rules are included in the PKI certificate.

- User identification

  If the PKI DN filter rule applies precisely to a user, this user is logged on with the SINEMA RC Server with the user name, see section "Creating new users (Page 86)".
- Temporary users

  If the PKI filter rule applies to a role, a temporary user "pkiuser_X" is created. The temporary user is listed in "User accounts > Users & Roles". The user receives the right and the access to the participant groups assigned to the role.

  In the role you also specify when the temporary user will be deleted, see section "Managing role and rights (Page 83)". You can also delete the temporary user in "User accounts > Users & Roles".

Locking out Smartcard / user certificate

To lock out users, you have the following options:

- Revocation list
- PKI DN blacklist
- Expired user certificate
- Automatic blocking of the Smartcard after entering the wrong PIN several times. Only the issuer of the Smartcard can release this again.

You will find more information on the certificate revocation list and PKI DN blacklist in the section "Locking out Smartcard / user certificate".

PKI DN filter rules

The attributes of the names (Distinguished Name acc. to the X.509 standard) are used as filter criteria for the filter rules.

You specify the PKI DN filter rules for the user and the role.

The following table shows several examples:

PKI DN filter rule	Description
For the user "JohnDoe" the following filter rule is defined: CN = max johndoe, OU = PD, O = Siemens, C = DE	The attribute values exist in the user certificate. The system signals the smart card user as user "JohnDoe" who is assigned the "admin" role. The role has all access rights.
For the role "Service" the following filter rule is defined: CN = *, OU = Service_Group_Plant_1, O = Siemens, C = DE	Only PKI card users obtain access for whom the relevant attribute values exist for OU, O and C. This restricts access to a certain service group. The system creates a temporary user who receives the rights assigned to the "Service" role. This user is listed in "User accounts > Users & Roles".
For the role "Service" the following filter rule is defined: CN = *, OU = *, O = *, C = DE	In this case, there is only the restriction to C = DE. As placeholder the "*" character is used.

4.3 Layout of the window

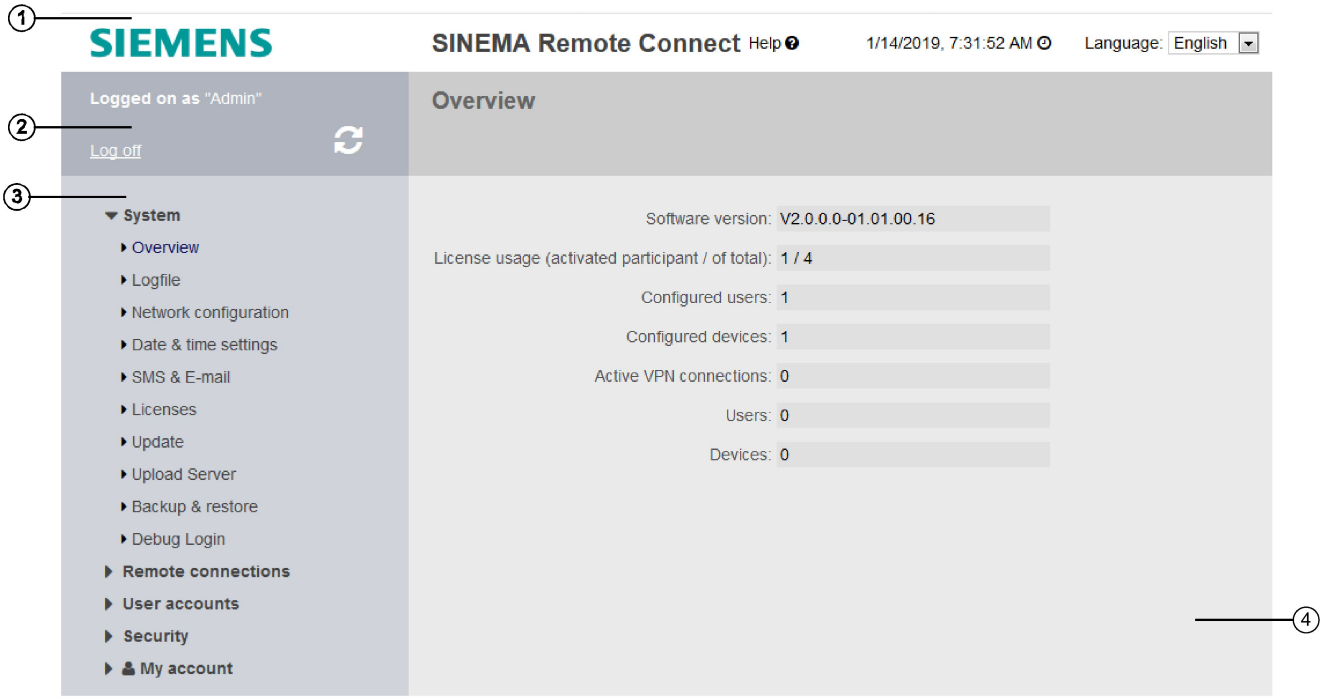
View of the Start page

If you enter the IP address of the SINEMA Remote Connect, the start page is displayed after successful login. You cannot configure anything on this page.

General layout of the WBM page

The following areas are generally available on every WBM page:

- Header area (1): Top area
- Display area (2): Top area
- Navigation area (3): Left-hand area
- Content area (4): Middle area



Software version: V2.0.0.0-01.01.00.16
License usage (activated participant / of total): 1 / 4
Configured users: 1
Configured devices: 1
Active VPN connections: 0
Users: 0
Devices: 0

Header area ①

The following is available in the header area:

- Logo of Siemens AG
- Product name
- Button Help

  If you click on this button, the help page of the currently selected menu item is opened in a new browser window.

- System time and date

  You can change the content of this display with "System > System time".
- Drop-down list for language selection

Display area ②

The full title of the currently selected menu item is displayed in the middle of the display area.

The left part of the display area contains the following fields and buttons:

- **Logged on as**

  Display of the user name under which you are logged on.
- **Log off**

  You can log out from any WBM page by clicking the "Log off" link.
- 🔄 **"Refresh" button**

  Click this button to request up-to-date information for the current page.

  Note

  If you click "Update", before the configuration changes have been saved with the "Save" button, your changes will be deleted.

Navigation area ③

In the navigation area, you have various menus available. Click the individual menus to display the submenus. The submenus contain pages on which information is available to you or with which you can create configurations. These pages are always displayed in the content area.

Note

Not all submenus may be available since this depends on the rights assigned to you. For more detailed information on the user concept, refer to the section "User concept (Page 14)".

Content area ④

The content area includes pages with input or display fields that are displayed depending on the menus clicked in the navigation area.

- In the navigation area, click a menu to display the pages of the WBM in the content area.

Buttons you require often

The pages of the WBM contain the following standard buttons:

- **Exiting the submenu with ⊗ "Exit dialog"**

  To exit a submenu again and to return to the main menu, use the "Exit dialog" button.

- **Changing settings with "Save"**

  WBM pages on which you can make settings have the "Save" button. Click the button to save data you have entered.

  Note

  To change settings, you require suitable user rights that are described in the section "Managing roles and rights (Page 83)".

  Note

  The changes take immediate effect. It can, however, take some time before changes are saved in the configuration.

- **Creating entries with "Create"**

  WBM pages on which you can create new entries have the "Create" button. Click this button to create a new entry.

- **Creating entries with "Copy"**

  WBM pages on which you can copy entries have the "Copy" button. Click on this button to copy the desired entry.

- **Deleting entries with "Delete"**

  WBM pages on which you can delete entries have the "Delete" button. Click this button to delete the previously selected entries. Deleting also results in an update of the page in the WBM.

- **Searching within a list**

  In the overview lists of the devices, users, roles and participant groups, you can search for certain entries. To do this, enter the name or part of the name in the search box 🔍. Then press the ENTER key on your keyboard.

- **Refresh the display with "Refresh"**
  Web Based Management pages that display current parameters have a "Refresh" button at the bottom edge of the page. Click this button to request up-to-date information from the device for the current page.

  Note

  If you click the "Refresh" button, before you have transferred your configuration changes to the device using the "Set Values" button, your changes will be deleted and the previous configuration will be loaded from the device and displayed here.

- **Page down with "Next"**
  The number of data records that can be displayed on a page is limited. Click the "Next" button to page forward through the data records.

- **Page back with "Prev"**
  The number of data records that can be displayed on a page is limited. Click the "Prev" button to page back through the data records.
- **"Show all" button**
  You can show all entries in pages with a large number of data records. Click "Show all" to display all entries on the page. Note that displaying all messages can take some time.
- **Drop-down list for selecting the number of displayed entries**

  You can set the number of displayed entries for pages with a large number of data records. Select the desired number of entries from the drop-down list to display them.

4.4 Language selection

Set language

1. In the header area on the right, open the drop-down list for the language setting.
2. Select the required language.

Result

The user interface of the SINEMA RC Server is displayed in the selected language regardless of the Web browser being used.

If the language is not changed immediately, use the "Update" button or the "F5" function key.

4.5 System

4.5.1 Overview

After logging on to the WBM, the system overview appears.

Update of the displayed values

You can update the displayed values with the "Update" button or the "F5" function key.

Calling the Web page

In the navigation, select "System > Overview".

Displayed entries

The following entries are displayed:

Box	Meaning
Software version	Version number of the current software.
License usage (activated participant / of total)	Number of currently activated participants and how many participants can be configured in total.
Configured users	Number of users created in the project.
Configured devices	Number of devices created in the project.
Active VPN connections	Number of active VPN connections
Users	Number of active VPN connections to the users created in the project.
Devices	Number of active VPN connections to the devices created in the project.

4.5.2 Log

4.5.2.1 Log messages

System events that have occurred are saved in the log messages. These include:

- Logons to the system
- Changes to the configuration
- Connection establishment
- Interruption of connections
- Operational messages

Calling the Web page

In the navigation area, select "System > Log" and the "Log messages" tab.

Displayed entries

The following entries are displayed:

Field	Meaning
Date	Shows the date and time.
Message level	The following message levels are possible: • Emergency • Alert • Critical • Error e.g. when exporting the server certificate fails • Warning, e.g. when a CA is deleted • Notice, e.g. when a CA is created • Info, e.g. when a user has logged on • Debug
Function	Displays the coded operating status.
Category	Displays the category of the log message.
Message	Displays information about the event that occurred.

Filtering log entries

1. Enter the desired period in the fields "From" / "To".
2. Select the required level from the "Message level" drop-down list.
3. Select the required category in the "Category" drop-down list.
4. Click on the "Apply filter" button.

Result

The display is updated according to the selected filter settings. Only the selected entries are displayed.

Saving log entries

Note

Saving log entries

The log is saved in the log archive after reaching 1,000,000 entries. In addition to this a week log is saved and archived on a weekly basis.

When you click the "Export" button, a dialog opens for opening or saving the current log file in *.csv format. All the entries are exported even if you have filtered the entries.

You can save the data locally and, for example, send it in if requested by support.

Note

Protecting exported log files from unauthorized access

Exported log files can contain information relevant for security. You should therefore make sure that these files are protected from unauthorized access. Remember this particularly when passing on the files.

4.5.2.2 Log archives

The log is saved in the log archive after reaching 1,000,000 log messages. A maximum of 100 log archives are possible.

Calling the Web page

In the navigation panel, select "System" > "Logfile" and the "Logfile archive" tab.

Displayed entries

The following entries are displayed:

Box	Meaning	
Date	Time stamp with the date and time	
Size	Size of the log archives	
Actions	☁	Export and save the selected log archive as a file.
	⊗	Remove the selected log archive from the list.

4.5.3 Network configuration

4.5.3.1 Interfaces

Note

IPv4 addresses and subnet mask according to RFC 1918

The factory IPv4 addresses and subnet masks can be changed as required, but must comply with the specification RFC 1918.

Note

So that the SINEMA RC can be reached via the Internet router, on the router, port forwarding needs to be set up for the following ports:

- For the WBM, see Web server settings (Page 53).
  - for HTTPS TCP port 443 (preset, can be changed)
- For the establishment of the OpenVPN tunnel, see OpenVPN settings (Page 102)
  - the UDP port 1194 (preset, can be changed)
  - the TCP port 5443 (preset, can be changed)
- For the certificate update the TCP port 6220 (fallback port preset, can be changed)
- For the establishment of the IPsec VPN tunnel
  - UDP port 500 (cannot be changed) and UDP port 4500 (cannot be changed)
  - IP protocol ESP (layer 3 protocol)

Calling the Web page

In the navigation, select "System > Network configuration" and the "Interfaces" tab.

Configuring the interface

Make the following settings and then click "Save":

Field	Meaning
Activate the interface	The WAN interface cannot be deactivated. The LAN interfaces are optional and can be disabled.
Interface	Select the interface to be configured. If you select the WAN interface, additional entries are required, see table "Additional settings of the WAN interface".
MAC address	Displays the MAC address of the selected interface. Is entered automatically by the system.
MTU	MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU they are fragmented. Maximum size 1500 bytes. Enter a value ≤ 1 500.
IP address	Enter the IP address of the interface. The IP address must be unique.
Network mask	Enter the subnet mask of the subnet you are creating.

Additional settings for the WAN interface

Field	Meaning
Default gateway	When operating a VPN over the Internet, additional IP addresses are generally required for the Internet gateways such as DSL routers. In the VPN, the individual modules must know the public IP addresses of the partner modules to be reached via the Internet. Enter the IP address for the gateway.
SINEMA Remote Connect is located behind a NAT device.	If you select the check box, you can enter the external WAN IP address of the Internet gateway.
WAN IP address	The WAN IP address via which SINEMA RC can be reached. This can, for example, be the WAN IP address of a DSL router via which SINEMA RC is connected to the Internet.

4.5.3.2 DNS

VPN clients can also reach the SINEMA RC Server using a host name. To do this, specify a host name, e.g. sinemarc.example.org

For the name resolution, specify the DNS server. This setting is adopted in the VPN configuration of the clients.

The setting is also required for licensing.

Calling the Web page

In the navigation panel, select "System > Network configuration" and the "DNS" tab.

Creating a new DNS server

Make the following settings and then click "Save":

Field	Meaning
Hostname	Enter the host name under which SINEMA RC can be reached, e.g. sinemarc.example.org
Externally resolvable host name	When activated, the host name is included in the VPN configuration and in the configuration of the VPN clients.
Primary DNS server	Enter the IPv4 address of the primary DNS server.
Secondary DNS server	Enter the IPv4 address of the secondary DNS server that is then used if the primary DNS server is not reachable.

4.5.3.3 Web server settings

Calling the Web page

In the navigation panel, select "System > Network configuration" and the "Web server settings" tab.

Configuring the Web server

Make the following settings and then click "Save":

Field	Meaning
HTTPS port	Specify via which port HTTPS remote access to the WBM will take place. HTTPS default port 443
Fallback port	Specify the fallback port. This port is used by OpenVPN devices that update the configurations using the auto enrollment mechanism (update interval). If these devices cannot be accessed via the HTTPS port, the update takes place via the fallback port. Fallback default port 6220

Changing port numbers

If you change port numbers, use ports from the number range 1024 ... 65535.

Select a free port that is not otherwise being used e.g.by the TCP port in OpenVPN.

Ports 0 ... 1023 are standardized (well known ports). From the registered ports as of 1024, for example no. 1024 is reserved.

If you use another port as the default port 443, the port number along with the IP address must be entered. A colon ":" must be entered between the IP address and the port number as a delimiter.

Example:

If SINEMA RC can be reached via the Internet at the IP address 192.144.112.5, and when in addition to this port number 6443 was specified for remote access, the following information must be specified for the remote station in the Web browser:

- https://192.144.112.5:6443

4.5.4 Date and time settings

To check the validity of certificates and for the time stamps of log entries, the current date and time are kept. You can set the system time yourself manually or have it synchronized automatically with an NTP server. Only one method can be active at any one time.

Calling the Web page

In the navigation, select "System > Date & time settings".

Setting the time manually

Make the following settings in the "Manual" tab:

Field	Meaning
System time	Shows the current system time in the format "DD.MM.YYYY HH:MM:SS". The display depends on the language that is set.
Use PC time	Click the button to use the time setting of the PC.

Automatic time-of-day setting with NTP

If the time-of-day synchronization is performed via NTP, you can make the following settings in the "NTP" tab:

Field	Meaning
Activate	If enabled, automatic time synchronization is performed via NTP.
System time	Shows the current system time in the format "DD.MM.YYYY HH:MM:SS". The display depends on the language that is set.
Last Synchronization Time	Shows how the last time synchronization was performed. The following methods are possible: • not synchronized • synchronized
Time zone	Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
Primary NTP server	Enter the IP address or host name of the primary NTP server.
Secondary NTP server	Enter the IP address or host name of the primary secondary NTP server.

To apply the selected settings, click on the "Save" button:

4.5.5 SMS messages and e-mails

4.5.5.1 SMS gateway provider

To wake a station, the SINEMA RC Server sends an e-mail. The e-mail is sent to an SMS gateway. The SMS gateway converts the e-mail into an SMS message and transfers this to the device, e.g. an M87x . When the SMS message is accepted, the device establishes the connection to the SINEMA RC Server.

The requirement is that the SIM card in the device is prepared to receive the SMS message. You will find further information on this in the configuration manual of the device.

Note

The time at which the wake-up SMS message will be sent to the station cannot be predicted precisely and depends on the current network load. Due to special events, an SMS message can take a long time to arrive. Take this into account when you send the wake-up SMS message, see section Monitoring and time response of wake-up SMS messages (Page 124).

Calling the Web page

In the navigation, select "System > SMS & E-mail > SMS gateway provider".

Displayed entries

A list of the already existing SMS gateway providers is displayed. As default the data of four network providers is already set

Field	Meaning
Name	Name of the SMS gateway provider
Address	Email address of the recipient of the SMS message The e-mail address is generally made up of the call number of the SIM card and the SMS gateway name. The requirement is that the e-mail address is activated, "Activating the e-mail address (Page 123)" Check with your network provider whether or not it is necessary to send an activation SMS message. With the placeholder $SMS-NO the phone number the device is used automatically.
Sender number	Identification that is transferred in the e-mail.
Subject	Subject of the e-mail
CC	E-mail address of another recipient The recipient receives only an e-mail. This could, for example, be a service technician who always wants to be informed when a certain device is woken.
Text	$MSG - The message text of the wake-up SMS message is entered automatically. Depending on the network provider either the text from the subject or the text box is sent as the SMS message. You can obtain more detailed information on this from your network provider.
Actions	⚙ Open the overview for changing the SMS gateway provider.

Creating an SMS gateway provider

1. Click the "Create" button.
2. In the following dialog, enter a name.
3. Under "Address", enter the recipient's e-mail address. For the phone number, use the placeholder "$SMS-NO".

4. For "Subject" or "Text", enter a "$MSG" placeholder. This depends on your network provider.
5. Click the "Create" button.

4.5.5.2 Settings

On this page, you specify whether an e-mail is forwarded directly to the recipient or via an SMTP relay server. You can also specify that the transfer of the e-mail takes place via an encrypted connection.

Note

Sending via an SMTP relay server

To send the e-mail it is recommended that you use an SMTP relay server. If you use the "Direct" transmission method, it is possible that the e-mail will be classified as not being secure. The e-mail is then blocked and does not arrive.

Calling the Web page

In the navigation, select "System > SMS & E-mail > Settings".

Configuring the SMTP client

Make the following settings in the "Settings" tab. Then click the "Save" button:

Field	Meaning
Method of delivery	Direct: The e-mail is forwarded directly to the SMTP server. Via relay server: The e-mail is forwarded via an SMTP relay server to the recipient. Make the additional settings listed in the following table.
Maximum life in the queue(s)	Maximum time in seconds that the sender waits for a reply from the mail server. When the time elapses, the transfer of the e-mail is aborted.
Sender	The E-mail address specified as the sender when transferring to the mail server. With the transmission method relay host, the e-mail address of the user account of the SMTP relay server is specified.

Additional settings for the transmission method "Via relay server"

Enter the following additional access data of the SMTP server:

Field	Meaning
SMTP relay server	Enter the name or the IP address of the SMTP relay server that is intended to forward the received e-mails.
SMTP relay port	Specify the port on which the SMTP relay server accepts connections. As default port 587 is set so that mail is received only from authenticated users.

Field	Meaning
Transport Layer Security (TLS)	Specify whether the e-mails are to be transmitted encrypted via TLS: • Opportunistic: The transmission of the e-mail can be encrypted via TLS. If the receiving mail server does not support encrypted transfer, the e-mail is forwarded via an unencrypted connection. This setting is used automatically if you have selected "Direct" as the Transmission method. • Binding: The transmission of the e-mail is encrypted via TLS. If the receiving mail server does not support encrypted transmission, the e-mail is not forwarded.
Server requires authentication	Some SMTP relay servers require a login. Enter the user name and the password. Some providers use the e-mail address as the user name. You will obtain more detailed information from your provider.
User name	User name for access to the SMTP relay server
Password	Password for access to the SMTP relay server

Sending a test e-mail

After configuration, you can send a test e-mail in the "Test e-mail" tab. To do this, enter the Recipient, the Subject and a text. Then click the "Send" button.

4.5.6 Managing licenses

On this page you obtain an overview of the existing licenses. You can also activate new license packages and deactivate existing licenses. You will find an overview of the available licenses in the section "License information (Page 27)".

Calling the Web page

In the navigation area, select "System > Licenses".

Displayed entries

A list of the existing licenses is displayed:

Field	Meaning
License type	Name of the license package
License number	License number used when the license was activated.
Activation date	Date on which the license was activated.
License value	Number of currently activated participants and how many participants can be configured in total.
Status	• Active: The license is activated and is being used. • Locked: The license is invalid or damaged, e.g. if you have changed the hardware equipment.
Actions	ℹ You obtain an overview of the license information. This is also displayed for users with the right "read only".

Online license

Activating the online license

Requirements

- There is a connection to the Internet.
- A valid DNS server is configured. You configure the DNS server in "System > Network > DNS".

Procedure

1. Click the "Activate license" button.
2. In the following dialog, enter the license number belonging to the online license.
3. Click the "Activate" button to confirm the online license.

Result

The system checks whether the license number is valid and which license package is activated.

The license is activated and is displayed in the overview of the existing licenses.

Deactivating the online license

Before changing systems, you need to return online licenses.

Requirements

- There is a connection to the Internet.
- A valid DNS server is configured. You configure the DNS server in "System > Network > DNS".
- The license is not used.

Procedure

1. Select the required online license.
2. Click the "Loose license" button.

Result

The license is free again and can be activated again on a different system.

Offline license

Activate offline license

1. Click on the "Export License Container" button.
2. Navigate to the storage directory where the file "sinemarc.WibuCmRaC" is stored.
3. Send an e-mail to your Siemens contact with the following:
   – File "sinemarc.WibuCmRaC"
   – License number of the license package
4. If the license package is activated, you will receive the offline license "sinemarc.WibuCmRaU" by e-mail.

   Save the file in your storage directory.
5. Click the "Select file" button.
6. Navigate to the storage directory and select the file.
7. Confirm your selection with the "Open" button and click the "Import license update" button.

Result

The license is imported and it is displayed in the overview of existing licenses.

Deactivate offline license

1. Send an e-mail to your Siemens contact with the license number of the license package you want to release.
2. Select the required offline license.
3. Click the "Loose license" button.

Result

Offline license is deactivated. To activate the offline license on a new system, take the steps in "Activate offline license".

4.5.7 Update

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)

Update files

The update files are signed and encrypted. This ensures that only update files created by Siemens can be downloaded to the device. Automatic update is not possible, the update files are only provided via SIOS.

The update must be performed in the correct order: V1.0 > V1.1 > V1.2 > V1.3 > V2.0

Note

System update V1.2 > V1.3

Due to changes in the basic installation an update from V1.2 to V 1.3 is only possible using the installation CD.

Calling the Web page

In the navigation, select "System > Update > System update".

Requirement

- The user has been assigned the right "Edit system parameters".
- The latest version of SINEMA RC is downloaded. The update file has the format *.tar.gz.
- The user has access to the storage directory.

System update

Procedure

1. Click the "Select file" button.
2. Navigate to the storage directory and select the file *.tar.gz.
3. Confirm your selection with the "Open" button.
4. Click the "Import" button.

Result

The system has been updated. Depending on the type of update, individual functions, or the entire system is restarted. To check the version following the restart, in the navigation click "System > Overview" and check the displayed software version.

Power management

In the navigation, select "System > Update" and click on the "Power management" tab. You have the following options for ending the system:

- Restart: To run a restart click the "Restart system" button
- Shut down: To shut the system down click the "System shutdown" button.

4.5.8 Server upload

This page provides you with the option of uploading files to an SFTP server. SFTP stands for Secure File Transfer Protocol.

Calling the Web page

In the navigation, select "System > Upload Server".

Displayed entries

Make the following settings in the "Settings Server upload" tab. Then click the "Save" button.

Field	Meaning
Automatic file upload	When activated, the files are uploaded to the SFTP server.
Files for upload	Specify which files are to be uploaded: • Configuration • Log files • Configuration and log files
SFTP server name	IP address of the SFTP server If you use a port other than the standard port 22, 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.: 192.168.234.1:622.
Fingerprint SFTP server	Display of the current fingerprint (last working connection) If the fingerprint changes e.g. after renewing the fingerprint, the function is disabled and a warning message to this effect is entered in the log. To be able to upload files to the SFTP server again, you need to enable the automatic file upload and check whether the new fingerprint matches that of the SFTP server.
Upload directory:	The user is assigned a storage director, the so-called home directory. If you do not enter anything, the file is uploaded directly to the home directory. To upload the file to a subdirectory, specify the subdirectory here. Provided that the subdirectory is created in the home directory.
User name	User name for access to the SFTP server
Password	Password for access to the SFTP server

4.5.9 Backing up & restoring

You can make up to 30 backup copies of the system settings of the SINEMA RC Server and reload these when necessary. The individual backup copies are saved in the format *.backup and can be imported into another system with the same SINEMA RC version.

You can find additional information

- In the section "Maintenance and service (Page 109)".
- On the Internet under the following entry ID: 109748144 (https://support.industry.siemens.com/cs/ww/de/view/109748144/en)

Requirement for creating backup copies

- The user has been assigned the right "Create backup copies".
- The settings for the backup copy are configured.

Calling the Web page

In the navigation, select "System > Backup & Restore > Backup copies".

Displayed entries

In the "Backup copies" tab, a list of the existing backup copies is displayed:

Field	Meaning	
Date	Date at which the backup copy was created.	
Name of the creator	Name of the user who created the backup copy.	
Size	File size of the backup copy.	
Comment	Comment on the backup copy. The text can be entered when creating or importing a backup copy.	
Status	• Done The backup copy has been created. • Restore: The system settings from the selected backup copy are restored.	
Actions	⤓	For this action, you require the user right "Restore the system". SINEMA RC Server takes the system settings from the selected backup copy and continues working with these. All settings made up to this point that have not been saved in a backup copy are lost.
	☁	Exporting and saving the selected backup copy as a file (*.backup).
	⊗	Removing the selected backup copy from the list.

Configuring settings for backup copies

Requirement

- The user has been assigned the right "Edit system parameters".

Procedure

1. In the navigation panel, select "System > Backup & restore" and the "Settings" tab.
2. Enter the number of permitted backup copies.
3. An entry between 10 and 30 is permitted. When the maximum number is reached, the oldest backup copy is overwritten.
4. If the system should be backed up at regular intervals, specify the interval and the time for the backup.
5. Enter a "encryption key".

   The coding key 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 (Page 28)".
6. Confirm the coding key.
7. Click the "Save" button.

Creating a new backup copy

Requirement

- The settings for the backup copies are configured.

With this function, you create a new backup copy with the current settings of the system.

1. Click the "Create new backup copy" button.
2. In the dialog that follows, if required enter a comment on the backup copy.
3. Click the "Finish" button.

Result

The backup copy is created and displayed in the list of backup copies.

Note

Settings that are not taken

The following settings are not backed up:

- Network settings (exception: HTTPS port)
- Log messages

Importing the backup

Note

The coding key must be identical on both systems. A backup copy coded with the key (x) cannot be imported on a system with the key (y).

With this function, a previously created backup copy that was saved as a file is loaded.

1. Click the "Import backup copy" button.
2. In the dialog that follows, if required enter a comment on the backup copy.
3. Click the "Browse" button.
4. Select the required file in the format *.backup and confirm your selection with the "Open" button.
5. Click the "Finish" button.
6. In "Actions" click on the "Restore" button to adopt the system configuration of the selected backup copy.

Result

SINEMA RC Server takes the system settings from the selected backup copy and continues working with these settings. All settings made up to this point that have not been saved in a backup copy are lost.

4.5.10 Debug login

You can grant your Siemens contact access to the SINEMA RC Server for a certain period of time via the debug logon.

The contact at Siemens can only access the data if you provide information on the port and password and enable the function.

Calling the Web page

In the navigation, select "System > Debug-Login".

Activating Debug login

1. Make the following settings:

Field	Meaning
Debug login timeout (minutes)	Specify the duration of the access. When this time elapses user is automatically logged off.
Debug login port	Specify the TCP port via which the system of the SINEMA RC Server is accessed. You may need to set up PORT forwarding to SINEMA RC on the Internet router.
Debug login password	Enter the password. 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 (Page 28)".
Confirm debug login password	Confirm this password.

2. Activate "Enable debug login" and click on "Save".

   When the settings are saved, the remaining time is displayed in the "Remaining time (minutes)" box.

Deactivating Debug-Login

1. Disable "Enable Debug login".
2. Click the "Save" button.

   The settings are returned to the default values and the password is deleted.

4.6 Remote connections

4.6.1 Managing devices

4.6.1.1 Overview of device management

The existing device entries are listed in tabular form on this page. The most important information for each device is displayed in different columns. Use the ⚙ button to show or hide the columns and change their order.

When you create the device, you can use participant groups to restrict access to specific nodes. Prior to creating the devices, it therefore makes sense to create the individual groups first (refer to the section "Creating participant groups (Page 78)").

Note

Note that a device should be assigned to at least one participant group.

If the device is not assigned to any participant group, this can only be edited by users with the "Manage devices" right.

Requirement

- The user is assigned the right "Manage devices"

Calling the Web page

In the navigation, select "Remote connections > Device".

Displayed entries

Field	Meaning
Name of the device	Name of the device
Device ID	The device ID is created automatically when the device is created. Required to log in to the SINEMA RC Server.
VPN address	The IP address of the device used during communication via VPN. The address is automatically assigned by SINEMA RC. If communication via VPN is not active, " none is displayed.
Remote subnet	The IP address of the remote subnet. If the option "Connected local subnets" is not enabled, "none" is displayed, refer to the section "Creating a new device (Page 70)". If several IP addresses are created, ⊞ is displayed. If you hover over ⊞ with the mouse pointer, this information is displayed.
Virtual subnet	The subnet matching the NAT IP address of the device. If the option "NAT for local subnet" is not enabled, "none" is displayed, refer to the section "Creating a new device (Page 70)". If several IP addresses are created, ⊞ is displayed. If you hover over ⊞ with the mouse pointer, this information is displayed.
Status	✓ The device is connected to SINEMA RC server via VPN. ⊖ The device is disabled. ⊗ The device is not connected to SINEMA RC server via VPN.
Date of the last login	Indicates when the device was last logged in.
Location	Location of the device. This can, for example, be the installation location of the device.
Type of connection	Shows when the connection will be established. • Permanent: The VPN connection exists permanently. • Digital input: The VPN connection is established as soon as a signal is present at the "digital input" of the device. • Wake-up SMS (M-800) or Wake-up SMS (RTU 3030) Sends an SMS to the device. The connection is established as soon as the device receives the SMS. • Wake-up SMS \ Digital input (M-800) The connection is established either via the digital input or via a command SMS.
Device type	Shows the type designation of the device.
Vendor	Displays the manufacturer of the device.
VPN protocol	Shows which protocol is being used for the VPN connection. 1. OpenVPN: The connection will be established via OpenVPN. 2. IPsec: The connection will be established via IPsec.
SMS gateway provider	Only for M800 Mobile, RTU 303xC, RM1224 Displays the SMS gateway provider. You can configure the SMS gateway provider under "System > E-mail & SMS".
Comment	Displays the comment.

Field	Meaning	
Actions	ⓘ	You obtain an overview of the device information. The device information contains the device ID and the fingerprint. These two pieces of information need to be entered on the device. During connection establishment, the device authenticates itself with the SINEMA RC Server using this information.
	⚙	Edit device settings
	☁	The configuration file with the OpenVPN settings for this device is created and can be saved. The file can be exported to the end device.
	🔑	A password protected PKCS#12 file is created and can be saved. The certificate is derived from the last valid CA. The file contains the private key of the device with the corresponding certificate. The file can be exported to the end device. When the password is queried, enter the password you specified when you created the device (refer to the section "Creating a new device (Page 70)").
	✹	The certificate and the key are stored as Base64-coded ASCII text.
	👥	Displays the participant group to which the selected device is assigned.
	⏸	Deactivate device • If the device is connected, the existing connection is also deactivated. • If the device attempts to establish a VPN connection, the device is ignored by the SINEMA RC Server.
	▶	Activate device. The device can establish a VPN connection to the SINEMA RC Server.
	📱	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.

Creating a device

Click the "Create" button and configure the required settings, see Creating a new device (Page 70).

Filtering entries

1. Select an entry in "Search filter".
2. Enter a name or part of the name in the search box.
3. Click on the "Apply filter" button.

Result

The list is updated based on the settings made. To show all entries again, click the "Show all" button.

4.6.1.2 Creating a new device

Device settings

You set the settings for the desired device on this page. The settings are divided into areas that can be collapsed ❯ and expanded ⌄ for clarity.

Calling the Web page

In the navigation, select "Remote connections > Device".

Procedure

1. Click the "Create" button.
2. Configure the **General device information:**

Field	Meaning
Name of the device	Enter a name. The name must meet the following conditions: • It must be unique • it must start with a letter. • The following characters are permitted: a-z, A-Z, 0-9 and _ • "conn" cannot be used as a name.
Password	Enter a password and confirm this password. See also the guidelines in the section "Permitted characters (Page 28)".
Confirm password	
Vendor	You can enter the manufacturer of the device.
Type	Select the type of node from the list. If the your device type does not exist or you do not know it, select "Other". All functions are now enabled.
SMS gateway provider	Only for M800 Mobile, RTU 303xC, RM1224 Select the SMS gateway provider. You can configure the SMS gateway provider under "System > E-mail & SMS".
GSM number	Only for M800 Mobile, RTU 303xC, RM1224 Enter the phone number of the node to which the wake-up SMS is sent.
Sender ID	Only with RTU 303xC This ID identifies SINEMA RC Server to the RTU. The ID must also be configured in the RTU.
Location	You can enter the installation location of the device.
Comment	You can enter a comment.

3. Configure the **VPN settings:**

Field	**Meaning**
VPN protocol	Specify which protocol will be used for the VPN connection. The selection depends on the selected device type. • OpenVPN: The connection will be established via OpenVPN. You configure the settings in "Security > VPN basic settings > OpenVPN". • IPsec: The connection will be established via IPsec.
VPN connection type	Specify when the VPN connection is to be established. The selection depends on the selected device type. • Permanent The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is maintained permanently. • Digital input Establishing the connection is controlled via the digital input (DI) of the device. • Wake-up SMS (SCALANCE M-800) / Wake-up SMS (RTU) When the device receives a wake-up SMS, it establishes a connection to the SINEMA RC Server. • Digital input / wake-up SMS (SCALANCE M-800) Establishing the connection is controlled either via the digital input or via a wake-up SMS.
Request VPN address	When enabled, a VPN address is requested during connection establishment. • OpenVPN: The setting is always selected and cannot be changed. • IPsec: Enable or disable the option.
Use fixed VPN address	If this option is selected, you can assign a fixed VPN address to the device. Via the VPN connection, the device can always be reached at this VPN address. This is only possible when the parameter "Activate fixed IP address space" is enabled. The parameter depends on the VPN connection mode. • OpenVPN: Remote connections > Address spaces > OpenVPN • IPsec: Remote connections > Address spaces > IPsec
Fixed VPN address	Enter the desired VPN address.

4. Configure additional parameters for the VPN connection.
   The configuration mask depends on the selected VPN protocol.

   – OpenVPN connection

     To configure the parameters, enable "Connection parameters".

Field	**Meaning**
IP address	IP address of the connection Enter the IP address via which the SINEMA RC Server can be reached.
Port	Enter the port at which the SINEMA RC Server receives the OpenVPN connection.
Protocol	Specify whether the OpenVPN connection goes via TCP or UDP.

   – IPsec connection

Field	**Meaning**
IPsec profiles	Can only be selected in the "IPsec" connection mode. You configure the IPsec profiles in "Security > VPN basic settings > IPsec profile".
Certificate	• Default certificate The CA certificate of the SINEMA Remote Connect Server is used for authentication. You must export the certificate, since it is required for the configuration of the devices. You export the certificate via "Security > Certificate management > CA certificate". • Imported certificates Only imported certificates can be selected with IPsec VPN. You can import certificates via "Security > Certificate management > Device certificate".
Local ID	The local ID and the remote ID are used by IPsec to uniquely identify the partners (VPN end point) during establishment of a VPN connection. Only required if the VPN tunnel partner evaluates the entry.
Remote ID	

5. Configure **All access.**

   The subnets and nodes accessible via the device are members of this participant group. You can assign one or more participant groups.

   Select the desired user group and click on the "Add" button. To delete, click on ✖.

6. If you do not need any further network settings, click "Quick Finish".

   If you need further network settings, click "Next". The prerequisite is that the device supports subnets.

Network settings

This page is only available for device types that support the subnets. You can find information about your device in the section "Connectable nodes (Page 25)".

On this page, you define the subnets and nodes that can be reached via the device and who can access them.

Requirement

- The device supports subnets.

Procedure

1. If the device is a gateway, activate "Device is a network gateway". If the device does not function as a network gateway, a source NAT is forced on the device with this setting.
2. In the "Subnet name" input box, enter a valid name and click "Add".

   The "Subnet name [Subnet name]" area is created. To delete, click on ✖.
3. Configure the subnet:

Field	Meaning
Participant groups	Select the participant group that has access to the subnet and click the "Add" button. You can assign one or more participant groups. To delete, click on ✖.
Subnet IP	Enter the IPv4 address of the subnet accessible from the device.
Subnet mask	Specify the network mask of the subnet.

4. Specify the NAT mechanism for "NAT mode":
   – Without
   For transparent IP communication through the OpenVPN tunnel without NAT. The devices communicating with each other always use the explicit IP address of the communication partner.
   – 1:1 NAT
   The network IP address of the remote subnet is represented by a virtual network IP address. The network IP addresses are converted in the remote device. The host IP address remains unchanged. The virtual IP address must be used to address a node in the remote subnet.
   – NAT for local hosts
   The IP address of the device in the remote subnet is hidden behind a dedicated IP address. The device IP addresses are converted in the remote device. You can specify the dedicated virtual IP address to address a node in the remote subnet.
5. If you have enabled NAT mode, configure the virtual subnet:

Field	Meaning
Virtual subnet IP	Specify the IP address for the virtual subnet. If the network address space is enabled, the start address is entered automatically. You can customize this address.
Virtual subnet mask	Only available with "NAT for local hosts": Enter the network mask of the virtual subnet.

6. Enter a unique name for "Node name" and click "Add".

   The "Node [node name]" area is created. To delete, click on ✖.

7. Configure the node:

Field	Meaning
Node name	Displays the name you assigned to the node.
Node IP	Specify the IP address of the node. The IP address must be in the configured subnet.
Virtual Node IP	• 1:1 NAT The virtual IP address is entered automatically. • NAT for local hosts Specify the translated NAT IPv4 addresses.
Participant group	Select the remote participant group that has access to the device and click "Add". You can assign one or more participant groups. To delete, click on ✖.

8. Click the "Save" button.

Setting up a template with network settings

To transfer the same network settings to other devices, you can create a template in "Template settings" and use it.

Button	Meaning
Save settings as template	To save network settings to a template, click the "Save settings as template" button. **Note**: When a new template is saved, the existing template is over-written with new values.
Load settings from template	To copy network settings from the template, click on the "Load settings from template" button. **Note**: When the template is loaded, all new settings are overwritten with the template values without warning. Newly created subnets are deleted if the template does not contain them.

When creating the template, note that only the last saved template is available.
The following values are entered in the template:

- Setting for "Device is a network gateway".
- Subnet name and assignment of participant groups
- Subnet IP address and subnet mask
  If NAT mode is set to "without", this information must be unique. Adapt the information before saving the network settings.
- Selected NAT mode
- Virtual subnet IP and virtual subnet mask
  If the virtual subnet is activated, these values are not taken from the template, but

automatically filled with the next free address. If NAT is not enabled, enter the values before saving the network settings.

- Node name
- Node IP
- Virtual node IP
  Calculation continues automatically with the next free IP address.
- Assignment of the participant groups

4.6.1.3 Updating devices

You can find information about the status of the loaded firmware on this page.

Calling the Web page

In the navigation, select "Remote connections > Device update > Devices".

Displayed entries

A list of information about the installed firmware version is displayed.

Field	Meaning	
Name of the device	Name of the device	
Last known firmware version	The firmware version that the device transferred to the SINEMA RC Server.	
Last known request of the firmware	Information on when the device last requested the firmware.	
Status	✓	Online: The device is connected to SINEMA RC Server via VPN.
	⊖	The device is disabled.
	⊗	Offline: The device is not connected to SINEMA RC Server via VPN.
Actions	❚❚	Deactivate device. • If the device is connected, the existing connection is also deactivated. • If the device attempts to establish a VPN connection, the device is ignored by the SINEMA RC Server.
	▶	Activate the device again.

Updating firmware

1. Click on the "Firmware file" tab.
2. Click the "Select file" button.
3. Navigate to the storage directory and select the update file (*.swf).

4. Confirm your selection with the "Open" button. Click the "Import" button.
5. Click on the "Devices" tab.
6. Select the devices to be updated.
7. Save your selection.

Result:

After saving, the SINEMA RC Server sends the request to the device to load the new firmware. The device downloads the firmware and restarts.

4.6.2 Address spaces

4.6.2.1 Network address space

You define the address space for the virtual local LAN on this page.

Note

The first IP address of the address space is always assigned to the SINEMA RC Server.

Calling the Web page

In the navigation, select "Remote connections > Address spaces > Virtual subnet".

Manage address space

1. Click on "Activate network address space" to set the virtual subnet settings.
2. Configure the address space for the virtual subnet **:**

Field	Meaning
Start address	Start address of the address space.
Network mask	The network mask belonging to the address space.
End address	End address of the address space The address space is limited by the start address and the network mask. The end address must be within this range.
Available networks (in total)	Displays the number of available networks determined from the start address and the end address.

3. Click the "Save" button.

4.6.2.2 VPN address spaces

You define the address spaces for TCP, UDP and IPsec on this page. When a VPN client logs into SINEMA RC Server, it receives an IP address from the address space for the duration of the connection.

Note

The first IP address of the address space is always assigned to the SINEMA RC Server.

Calling the Web page

In the navigation, select "Remote connections > Address spaces".

Manage address space

In the "OpenVPN" and "IPsec" tabs, you can make the following settings for the address spaces:

Field	Meaning
Start IP address	Start address of the address space.
Network mask	The network mask belonging to the address space.
End IP address	End address of the address space The address space is limited by the start address and the network mask. The end address must be within this range.
Use (assigned IPs / of total)	The following values are displayed: • Number of assigned IP addresses • Number of available IP addresses
Activate the network address space	When enabled the device can be assigned a fixed IP address from the address space.
Fixed IP protocol	Only with OpenVPN: • TCP: Applies to OpenVPN connections via TCP • UDP: Applies to OpenVPN connections via UDP
Location of the fixed IP address space:	• First: The fixed IP addresses are from the start area of the address space. The first IP address is reserved for the SINEMA RC Server. The first fixed IP address is always the second IP address after the start IP address. • Last: The fixed IP addresses are from the end area of the address space. The last fixed IP address is always the end IP address.
Length of the fixed IP address space:	Number of fixed IP addresses

4.6.3 Participant groups

Users, devices, end devices and subnets can be grouped together into participant groups. The nodes can also be assigned to several participant groups. You also specify whether the communication between the participants of an individual group is permitted or forbidden.

Once the participant groups have been created, you can define communication relations between the groups (see section "Communication relations between participant groups (Page 79)").

Requirement for creating participant groups

- The user has been assigned the right "Manage remote connections".

Calling the Web page

In the navigation, select "Remote connections > Participant groups".

Displayed entries

A list of the participant groups that have already been created is displayed:

Field	Meaning	
Group Name	Name of the group	
Members may communicate	Indicates that members of this group may communicate with each other.	
Reachable Ethernet interfaces	Shows the LAN interface via which the VPN tunnel can be reached.	
Number of users	Number of users assigned to the group.	
Number of devices	Number of devices assigned to the group.	
Number of subnets	Number of subnets assigned to the group.	
Number of nodes	Number of nodes assigned to the group.	
Number of roles	Number of roles assigned to the group.	
Actions	ℹ	In the participant list, all the devices and users belonging to the participant group and their status (online or offline) are displayed.
	⚙	Open the overview for changing the settings for the participant groups.
	⇄	Open the overview for changing the communication relations.

Create new participant group

1. Click the "Create" button.
2. Enter a group name and optionally a description in the following dialog.
3. Specify whether the group members are allowed to communicate with each other.
4. Specify which LAN interface can be reached via the VPN tunnel.
5. Click the "Save" button.

Result

The participant group has been created. You have specified whether communication between the members of this group is permitted or forbidden.

Changing the settings of the participant groups

1. Change the relevant participant group settings.
2. Then click the "Save" button.

Filtering entries

1. Select an entry in "Search filter".
2. Enter a name or part of the name in the search box.
3. Click on the "Apply filter" button.

Result

The list is updated based on the settings made. To show all entries again, click the "Show all" button.

4.6.4 Communication relations

You define the communication relationships between the groups on this page.

Requirement

- The user has been assigned the right "Manage remote connections".
- Participant groups have been created.

Calling the Web page

In the navigation, select "Remote connections > Communication relations".

Displayed entries

A list of the communication relations already created is displayed:

Field	Meaning	
Source group	Name of the source group	
Destination group	Names of the destination groups whose members are allowed to communicate with the members of the source group.	
Actions	⚙	Open the overview for changing the settings for the participant groups.

Creating communication relations between the participant groups

1. Specify the source group. For this group click on the icon ⇄.
2. On the following page, you define the destination groups to which connections are allowed from the source group.
3. Click the "Save" button.

Result

The communication between the participant groups is specified. You have specified whether communication between the members of this group is permitted or forbidden.

Changing communication relations between the participant groups

1. In the navigation, select "Remote connections > Communication relations".
2. Click on the ⚙ icon. Change the relevant communication relations and then click the "Save" button.

Filtering entries

1. Select an entry in "Search filter".
2. Enter a name or part of the name in the search box.
3. Click on the "Apply filter" button.

Result

The list is updated based on the settings made. To show all entries again, click the "Show all" button.

4.6.5 Assigning a node to a group

Assign users to one or more groups

1. Click on the 👥 icon in the user overview.

   The participant groups that have already been created are displayed.
2. Select the group/groups to which the participant will be assigned.
3. Click the "Save" button.

Assign devices, subnets, or nodes to one or more groups.

1. Click on the ⚙ icon in the device overview.

   The general device settings open.
2. Under "All access", select the desired user group and click the "Add" button.
3. Click the "Save" button.
4. If the device supports subnets, you can assign the subnets and nodes accessible via the device to participant groups in the network settings.

   Select the participant group that has access to the subnet or node and click the "Add" button.
5. Click the "Save" button.

4.7 User accounts

4.7.1 Overview of the user accounts

Requirement for creating and changing users

The user is assigned the right "Manage users".

Calling the Web page

In the navigation, select "User accounts > Users & Roles".

Displayed entries

A list of the users that have already been created along with their status is displayed: In addition, the temporary users are shown that are created when logging on with Smartcard or the PKI certificate.

Box	Meaning
User name	The name assigned to the user. The user name must be unique throughout the system and can be changed. Refer to the note in the section ""Creating a new user (Page 86)".
VPN address	The IP address of the device used during communication via VPN. The address is automatically assigned by SINEMA RC. If communication via VPN is not active, "none" is displayed.
First name	First name of the user
Second name	Second name of the user
Account created	Date and time at which this user account was created
Date of the last login	Date and time of the last login

Box	Meaning	
Status	✅	The user is logged on to SINEMA RC.
	⊗	The user is not logged on to SINEMA RC.
	⛔	The user is disabled.
VPN connection mode	Shows which protocol is being used for the VPN connection.	
Actions	ℹ	Overview of the user settings. This is also displayed for users with the right "read only".
	⚙	Change user settings. This includes changing the contact data, assigning new roles and rights and changing the password.
	👥	Display of which participant group the selected user is assigned to. The user can be assigned to one or more groups.
	⏸	Deactivate user. • If the user is online, the existing VPN connection is also deactivated. • When the user attempts to log on, the message "Account is deactivated" is displayed.
	▶	Activate the user again. The user can log on to the SINEMA RC server again.

Filtering entries

1. Select an entry in the "Search filter" pop-up menu.
2. Enter a name or part of the name in the search box.
3. Click the "Apply filter" button.

Result

The list is updated based on the settings made. To show all entries again, click the "Show all" button.

See also

Participant groups (Page 78)

Managing roles and rights (Page 83)

4.7.2 Managing roles and rights

Requirement for creating roles

The user is assigned the right "Manage users".

Displayed entries

A list of the created roles is displayed.

Field	**Meaning**	
Role name	Name of the role	-
Force comment	When the VPN tunnel between SINEMA RC client and server is ended, the user is requested to enter a comment. Only then can the current session be closed. The comment is entered in the log of the SINEMA RC Server.	SINEMA RC client
Manage remote connections	Specify communication relations; this includes how the participants within a participant group may communicate and which participant group may communicate with which other participant group	Remote connections > Participant groups Remote connections > Communication relations
Certificate management	Create new CA certificates and server certificates, edit and delete existing certificates;	Security > Certificates
Manage firmware updates	Load the update file with the new firmware on the device and start the update process.	System > Devices-Update
Create backup copies	Create, delete, export and import a backup copy.	System > Backup & restore
Manage address spaces	Edit parameters of the address spaces	Remote connections > Address spaces
Edit system parameters	Read, create and delete system parameters. The system parameters include: • Overview • Event log • Web server • Licenses • Network • System update • Date and time of day • VPN • Maximum number and coding key for backup copies	
Manage devices	Create new devices; edit and delete devices already created; create participant groups and assign devices to them; create and download configuration file with VPN settings for the device;	Remote connections > Devices
Manage users and roles	Create new users and roles, edit and delete existing users and roles; assign rights and change your own assigned rights.	User accounts > Users and roles
Restore the system	Restoring the system based on the saved system file.	System > Backup Copy and System Restore
Password policy	Guideline for the assignment of passwords	
PKI policy	Guideline for the PKI certificate	

Creating a new role

1. Open the "Roles" tab.
2. Click the "Create" button.
3. Enter a role name.
4. Assign rights to the role according to the next table. Click the "Next" button.
5. Specify the password policy:

Field	Description
Password expires in (days)	Specifies that the password expires after a certain period. • Never (set as default) • 30 days • 90 days • 360 days 14 days before expiry the user receives an e-mail. Requirement: • An e-mail address is configured for the user. • The SMTP client is configured.
Reusing the same password	• 0: The setting is disabled • 1 - 5: If, for example, you enter 3, the current password can be reused only after 3 different passwords. As default, 3 is set.

6. Specify the settings for the logon with the PKI certificate.

Field	Description
PKI DN filter rule	Filter criteria according to which a check is made at the logon. The attributes of the names (Distinguished Name acc. to the X.509 standard) are used as filter criteria. This requires that the attributes are included in the PKI certificate of the user. For more detailed information, refer to the section "Logon with the Smartcard / PKI certificates".
Delete temporary user (in hours)	• 0: The setting is disabled. The temporary user must be deleted manually. • 1 - 72 hours: When the time expires, the temporary user is deleted.

7. Click the "Finish" button.

4.7.3 Create a new user

Create a new user

1. Open the "Users" tab.
2. Click the "Create" button.
3. Configure the contact data
   - Enter the necessary information in the "Contact data" tab. A mandatory box is the "User name".
   - The remaining contact information is optional and can be entered and modified by the users themselves.

Note

User names

The user name must meet the following conditions:

- It must be unique
- it must start with a letter.
- The following characters are permitted: a-z, A-Z, 0-9 and _
- The following user name is not allowed: admin

User names: admin

As default, after the installation the predefined user "admin" is available.

- admin: You can log in once after the installation using this user name and the password "admin". After this you will be prompted to create a new user. The "admin" role is assigned to this user automatically. This administrator has the right to access all functions and can set up the system. This includes creating users and assigning roles and rights to them. The "admin" user is no longer available.

Changing a user name

You can change the user name later. If you change the user name, you must either change the password or the user must log in to generate a new certificate and a new PKCS#12 file.

– Specify how the user can log in to the SINEMA RC Server:

Field	Meaning
Logon procedure	• Password Login with user name and password • PKI Login only with PKI certificate • Password + PKI Login with user name and password or with PKI certificate
PKI DN filter rule	Only required when logging in with PKI certificate. Filter criteria according to which a check is made at the logon. The attributes of the names (Distinguished Name acc. to the X.509 standard) are used as filter criteria. This requires that the attributes are included in the end entity certificate of the user. As placeholder use the "*" character.

– Click the "Next" button.

4. Assignment of rights and roles

   – Assignment of rights via role assignment:

   In the drop down list, select the required role and click "Add".

   The user receives the rights assigned to the role. To assign additional rights to the user, click on the check box in front of the respective right.

   To cancel the role assignment, click the "-" button beside the role.

   – Assignment of rights without role assignment:

   If you have not selected a role, enable the corresponding rights by clicking on the check box.

   – Click the "Next" button.

5. Configuring the VPN connection mode

   Set the following parameters:

Field	Meaning
Request virtual IP address	When enabled, a virtual IP address is requested during connection establishment.
Fixed IP address	The IP address that is always assigned to the user. This is only possible when the parameter "Activate fixed IP address space" is enabled. • OpenVPN: Remote connections > Address spaces > OpenVPN
OpenVPN connection parameters	Only necessary when the WAN IP address of the SINEMA RC Server is translated with NAT. • IP address of the connection Enter the IP address via which the SINEMA RC Server can be reached. • Port of the connection Enter the port at which the SINEMA RC Server receives the OpenVPN connection. • IP protocol Specify whether the OpenVPN connection runs via TCP or UDP. • Actions To delete, click on ✖ for actions

6. Creating participant groups

   – Select one or more participant groups to which the device will be assigned. You will find information on creating participant groups in the section "Creating participant groups (Page 78)".

   – Click the "Next" button.

7. Specifying the password

   Enter a password and confirm it. The assigned password can be changed later by the relevant user, refer to the section "Changing the current password (Page 107)".

8. Click the "Finish" button.

Changing user settings

Change the corresponding user settings. Then click the "Save" button.

Note

Changing the logon method

If you change the method from password to PKI, the configured password is deleted.

4.7.4 User agreement

On this page you can enter a user agreement.

Field	Meaning
Display option	• Never The user agreement is not displayed. • First login When the user logs in for the first time, the user agreement is displayed. After accepting the user agreement, the user can access the WBM of the SINEMA RC Server. • Every login Each time the user logs in, the user agreement is displayed. After accepting the user agreement, the user can access the WBM of the SINEMA RC Server.
Message	In the editor, enter the text for the user agreement. In the toolbar there are tools available for formatting the text. The symbols provide brief information in the form of a tooltip. After making your entry, click the "Save" button.
Export	Exports the selected version of the user agreement.

Note

Changed user agreement

If you change the user agreement while users are logged on with SINEMA RC client, this change does not take immediate effect for these users. These users remain logged on after the change is made to the user agreement.

The changed user agreement is displayed only when these users log in again. After accepting the user agreement, these users can access the WBM of the SINEMA RC Server.

4.8 Security

4.8.1 Managing certificates

4.8.1.1 Overview of certificate management

Certificate types

SINEMA RC uses different certificates to authenticate the various nodes when establishing a VPN connection. These include:

Certificate	Is used for ...	File type	Description in section ...
CA certificate	The CA certificate is a certificate issued by the "Certificate Authority" from which certificates are derived. So that a certificate is derived, a private key belongs to every CA certificate. The derived certificates are signed with the private key. The signature of the derived certificate is checked with the public key of the CA certificate. When SINEMA RC Server is installed a CA certificate is generated. When necessary the CA certificate can be renewed. The server, device and user certificates are derived from the currently valid CA certificate. The key exchange between the device and the VPN gateway of the partner takes place automatically when establishing the OpenVPN connection. No manual exchange of key files is necessary.	*.crt	CA certificate (Page 93)
Server certificate	Server certificates are required to establish secure communication (e.g. HTTPS, VPN...) between the device and another network participant. The server certificate is an encrypted SSL certificate.	*.p12	Server certificate (Page 93)
Device certificate	Device certificates and corresponding keys are only created when the user has the appropriate rights. For each created device, SINEMA RC Server creates a device certificate.	*.p12	Overview of device management (Page 67)
User certificate	SINEMA RC Server creates a personal certificate for each created user.	*.p12 *.pem	User certificate (Page 106)
PKI CA certificate	For the logon with the PKI certificate. The PKI CA certificate is created by an external certification authority.	*.pem	PKI CA certificate (Page 98)

File types

File type	Description
*.crt	File that contains the certificate.
*.p12 *.pfx	The formats *.p12 and *.pfx are used to save the certificate along with the private key. The private key with the corresponding certificate is stored password protected. The CA creates a certificate file (PKCS12) for both ends of a VPN connection with the file extension ".p12". This certificate file contains the public and private key of the local station, the signed certificate of the CA and the public key of the CA.
*.pem	Certificate and/or key as Base64-coded ASCII text.
*.key	Unprotected Base64-coded private key

Additional functions

In addition, in conjunction with certificates the following functions are also available:

- Exporting used certificates.
- Importing certificates.
- Renewal of expired certificates.
- Replacing existing certificate authorities.

Note

Current date and current time of day on the devices

When using secure communication (for example HTTPS, VPN...), make sure that the devices involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as invalid and the secure communication will not work.

4.8.1.2 Certificate overview

Calling the Web page

In the navigation, select "My account > User certificate".

Displayed entries

In the "Details" tab, you will see an overview of the user certificate derived from the CA certificate:

Field	Meaning
Serial number	Number to identify the certificate. The serial number is assigned automatically when the certificate is created.
Common name	The name used is generated automatically by the system.
Issued by	Display of the certificate authority that issued the certificate. The system uses the last valid CA certificate.

Field	Meaning
Valid from	Date from which the certificate is valid.
Valid to	Date on which the certificate expires.
Key length (bits)	Specifies the key length being used. The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred key length".
Signature method	Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate. The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred hash method".

Renewing a user certificate

Note

Only renew valid certificates

You cannot renew a certificate that has already expired. If you attempt to renew an expired certificate, the certificate authority will reject the request. When a certificate has already expired, instead of renewing the existing certificate, you need to request a new certificate.

With the "Renew" button, you can when necessary, e.g. with compromised certificates, generate a new certificate.

To do this, enter the corresponding password. The serial number is automatically incremented by one.

Exporting a user certificate

You can download the personal certificate in the "Export" tab. These include:

Field	Meaning
PKCS#12	Download a container in the Personal Information Exchange format (PFX).
PEM	Download certificate and key as Base64-coded ASCII text.
OVPN	Download OpenVPN configuration for user.

4.8.1.3 CA certificate

Calling the Web page

In the navigation panel, select "Security > Certificate management".

Displayed entries

In the "CA certificates" tab, you can see an overview of the CA certificates:

Field	Meaning	
CA certificate name	The name of the CA is generated automatically by the system.	
Expiry time	Shows how long the CA certificate is valid. You can specify the validity date in the "Settings" tab. There, you can also set how many days before expiry of the CA certificate it is automatically renewed.	
Status	Active: The CA certificate is valid. Out of service: A newer CA certificate was generated or the CA certificate has expired.	
Actions	ℹ	Calling up CA information You obtain information on the selected CA. This is also displayed for users with the right "read only".
	⬇	Exporting a CA certificate By clicking on the icon, the CA certificate (*.crt) is exported. The file is, for example, exported to the end device or to the destination server.

Renewing a CA certificate

With the "New CA certificate" button, you can when necessary, e.g. with compromised certificates, generate a new certificate.

4.8.1.4 Server certificate

Calling the Web page

In the navigation panel, select "Security > Certificate management".

Displayed entries

In the "Web server certificate" and "VPN server certificate" tabs, you can see an overview of the certificates:

Field	Meaning
Serial number	Number to identify the certificate. The serial number is automatically incremented by one when the certificate is created.
Common name	The name is taken from the network configuration: • The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 53)"). • The IP address of the WAN or LAN interface, see section "Interfaces (Page 51)".
Issuer	Display of the certificate authority that issued the certificate.
Valid from	Date from which the certificate is valid.
Valid to	Date on which the certificate expires.
Key length (bits)	Key length that was set in "Settings" when this certificate was generated.
Signature method	Signature method with corresponding signature key ("hash value") that was set in "Settings" when this certificate was generated.
SHA1 fingerprint:	Fingerprint with SHA1 as hash algorithm
SHA256 fingerprint	Fingerprint with SHA256 (SH2) as hash algorithm
Alternative names	• IP: The IP address of the WAN interface, see section "Interfaces (Page 51)". • IP: The WAN IP address when you have activated the function "SINEMA Remote Connect is located behind a NAT device" and have entered an IP address, refer to the section "Interfaces (Page 51)". • DNS: The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 53)").

Renewing the Web server certificate and VPN server certificate

With the "Renew" button, you can when necessary, e.g. with compromised certificates, generate a new certificate. The certificates are derived from the currently valid CA certificate. The serial number is automatically incremented by one.

Importing the Web server certificate

With the "Import" button, you can import CA certificates for the encryption of the data traffic.

4.8.1.5 Importing the Web server certificate

If you do not want to use the Web server certificate issued by SINEMA RC, here you can import a Web server certificate from an external certification authority. The Web server certificate can, for example, be issued by a company internal certification authority or by a public certification authority.

Note

Supported encryption

SINEMA RC supports Web server certificates encrypted according to RSA (Rivest, Shamir und Adleman).

To import the Web server certificate, you require the following files:

- Certificate file

  Examples of the content of a certificate file (.crt, .pem)

  -----BEGIN CERTIFICATE----- .... -----END CERTIFICATE-----

  -----BEGIN X509 CERTIFICATE----- .... -----END X509 CERTIFICATE-----

- Key file

  The RSA key file that belongs to the certificate file.

  Examples of the content of a certificate file of a key file (.pem, .key)

  Encrypted:

  -----BEGIN ENCRYPTED PRIVATE KEY----- ... -----END ENCRYPTED PRIVATE KEY---
  --

  Unencrypted:

  -----BEGIN PRIVATE KEY----- ... -----END RSA PRIVATE KEY-----

  -----BEGIN RSA PRIVATE KEY----- ... -----END RSA PRIVATE KEY-----

- CA chain file

  This file contains the certificates of all certification authorities involved. Base on the certificate chain the validity of the Web server certificate is checked.

  Examples of the content of a CA chain file (.crt, .pem):

  Several certificate blocks one after the other:

  -----BEGIN CERTIFICATE----- ... -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE----- ... -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE----- ... -----END CERTIFICATE-----

Procedure

1. To import this click the "Select file" button in "Select the certificate file".
2. Select the certificate file and confirm your selection with the "Open" button.
3. Click the "Select file" button in "Select the key file".

4. Select the corresponding key file and confirm your selection with the "Open" button.
5. There are files to which access is password protected. To load the file successfully in SINEMA RC, enter the password specified for the file and repeat the entry.
6. To import the certificate of a higher ranking certification authority, click the "Select file" button in "Select the CA chain file".
7. Select the CA certificate file and confirm your selection with the "Open" button.
8. Click the "Next" button. Details of the signed certificate are displayed on the "Activate certificate" tab. You can, for example, check whether the certificate is still valid.

Box	Meaning
Serial number	Number to identify the certificate. The serial number is automatically incremented by one when the certificate is created.
Common name	Name of the issuer
Issuer	Display of the certificate authority that issued the certificate.
Valid from:	Date from which the certificate is valid.
Valid to:	Date on which the certificate expires.
Key length	Specifies the key length being used.
Signature method	Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate.

9. To finally import the files, click the "Import" button.

4.8.1.6 Making settings for certificates

Calling the Web page

In the navigation panel, select "Security > Certificate management".

Changing settings

The changes made in the "Settings" tab are used only used when renewing the server certificate: The changes do not apply to existing certificates. On the tabs "Web server certificate" and "VPN server certificate" you can use the "Renew" button to generate a new server certificate.

Box	Meaning
Preferred key length (bits)	Select the number of bits of the various possible keys for the procedure.
Preferred hash method	Select the hash method for the certificate: SHA256 or SHA512

Box	Meaning
CA certificate renewal (days before expiry)	Specify how many days before it expires the certificate will be automatically renewed. As default, the CA certificate of the server is valid for 10 years. If, for example, you specify 365 days, a new CA certificate will be generated after 9 years. The previous CA certificate is then "Out of service" but is valid for another 365 days. The clients that use this CAA certificate can continue to log on with it for another 365 days. After this time, the CA certificate counts as being "Expired" and the clients need to use the new CA certificate.
Validity of client certificates (days)	Specify for how many days the certificate will be valid. A certificate whose CA has already expired can no longer be used.

4.8.1.7 Device certificate

Calling the Web page

In the navigation panel, "Security > Certificate management" select the "Device certificate" tab.

Displayed entries

In the "Device certificate" tab, you can see an overview of the imported certificates:

Box	Meaning
Type	Type of the loaded file. For more information, refer to the section Overview of certificate management (Page 90).
Common name	Name of the applicant
Status	Display of whether the certificate is valid or has already expired.
Subject	Display of the owner obtained from the common name (CN).
Issuer	Display of the certification authority that issued the certificate.
Valid from:	Date from which the certificate is valid.
Valid to:	Date on which the certificate expires.
Use	The function that uses the certificate.

Importing device certificates

1. To import device certificates click the "Import" button.
2. Select the PKCS12 file (*.p12) and confirm your selection with the "Open" button.
3. The files are password protected. To load the files on the device, enter the password and repeat the input.

4. Click the "Next" button. Details of the CA certificate are displayed on the "Activate certificate" tab. You can, for example, check whether the certificate is still valid.

Box	Meaning
Serial number	Number to identify the certificate. The serial number is automatically incremented by one when the certificate is created.
Common name	Name of the issuer
Issued by	Display of the certificate authority that issued the certificate.
Valid from:	Date from which the certificate is valid.
Valid to:	Date on which the certificate expires.
Key length	Specifies the key length being used.
Signature method	Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate.

5. To load the files on the SINEMA RC Server, click the "Import" button.

Result:

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

4.8.1.8 PKI CA certificate

Calling the Web page

In the navigation panel, select "Security > PKI CA certificate management".

Displayed entries

On the "PKI Ca certificates " tab, you can see an overview of the imported certificates:

Box	Meaning
Common name	Name of the applicant e.g the user name
Status	Shows whether the certificate is valid or has already expired.
Subject	Owner of the private key assigned in the certificate.
Issuer	Display of the certificate authority that issued the certificate.
Valid from	Date from which the certificate is valid.
Valid to	Date on which the certificate expires.
Fingerprint	Checksum of the certificate ensure the integrity.
Delete	Deletes the PKI CA certificate

Importing PKI CA certificates

1. To import PKI CA certificates click the "Import" button.
2. Select the CA certificate file (*.crl) and confirm your selection with the "Open" button.
3. To load the file on the SINEMA RC Server, click the "Save" button.

Result:

The certificate file is imported onto the SINEMA RC Server. The PKI CA certificate is displayed on the following tab "PKI CA certificate".

4.8.1.9 Locking out Smartcard / user certificate

To lock out users, you have two options:

- Certificate Revocation List (CRL)
- PKI DN blacklist

Calling the Web page

In the navigation panel, select "Security > PKI CA certificate management".

PKI DN blacklist

The user is blocked if a suitable PKI DN filter rule exists in the PKI DN blacklist.

1. Click on the "PKI DN Blacklist" tab.
2. Enter the corresponding rule in "PKI DN filter rule". The attributes of the names (Distinguished Name acc. to the X.509 standard) are used as filter criteria. This requires that the attributes are included in the PKI certificate of the user. For more detailed information, refer to the section "Logon with the Smartcard / PKI certificates".
3. Click "Add".

Result:

The created entries are listed on the page:

Field	Meaning
DN filter	Shows the PKI DN filter rule.
Deactivated user	Displays the users to whom the rule applies and who are therefore locked.
Delete	Deletes the entry

Certificate revocation list

The output certificates that are no longer valid are listed in the certificate revocation list. If, for example, employees leave the company, their certificates are called back and included in the list. Logging on with this certificate is then no longer possible.

So that the revocation list is used, activate the CRL check on the "Settings" tab.

On the "Revocation list" tab, you can see an overview of the available revocation lists:

Field	Meaning
Issuer	Display of the certification authority that issued the certificate revocation list.
Status	Shows whether the certificate revocation list is valid or has already expired.
Revoked Serial numbers	Shows the revoked serial numbers.
Valid from	Date from which the certificate revocation list is valid.
Valid to	Date up to which the certificate revocation list is valid.
Last update	Date on which the certificate revocation list was last updated.
Next update	Date on which the certificate revocation list will next be updated.
Origin	Shows where the certificate revocation list originates from: File: The certificate revocation list was imported URL: The certificate revocation list is stored at the distribution point.

Importing the certificate revocation list as a file

1. In the "Revocation list" tab, click the "Import from file" button.
2. Click the "Select file" button and select the certificate revocation list. Generally the file has the extension *.crl.
3. Confirm your selection with the "Open" button. To import the certificate revocation list click the "Save" button.

Obtaining the certificate revocation list automatically

According to the X.509v3 standard n the certificate you can specify a certificate revocation list distribution point. To do this in the attribute "CRL Distribution Point" specify a URL at which the current CRL of this certification authority is stored. To use this function, the attribute must exist in the PKI CA certificate.

At certain intervals SINEMA RC downloads the file and uses it. You specify the interval on the "Settings" tab.

Settings of the certificate revocation list

Field	Meaning
Enable CRL checking	When enabled, the validity of the user certificate is checked based on the certificate revocation list.
CRL update interval	Specify the intervals at which the certificate revocation list is checked for changes. If this is the case, the certificate revocation list is downloaded to the distribution point.
Allow missing CRL	• Disabled Every PKI CA certificate requires a valid certificate revocation list. If this is missing, the user certificates derived from the PKI CA certificate are invalid. • Enabled: When enabled, the absence of the certificate revocation list is allowed. Please note that if the certificate revocation list is missing, all the user certificates derived from the PKI CA certificate are permitted.

4.8.2 VPN connections

4.8.2.1 Making VPN basic settings

VPN basic settings

OpenVPN is a program for establishing an encrypted TLS connection. OpenSSL is used for the encryption.

OpenVPN file

When a device or user is created, a configuration file with the extension *.ovpn is generated automatically. The file contains various parameters required for a connection to the server. These include e.g. the certificates; refer to the section "Overview of certificate management (Page 90)".

The file must be loaded on the participant in the remote network to which the SINEMA RC Server establishes a VPN connection.

The SINEMA RC Client always fetches this data automatically. The S615 either fetches the data automatically or the file must be loaded. This depends on the configuration.

Downloading an OpenVPN file

For devices, the file is called in the device list; refer to the section "Overview of device management (Page 67)".

For users, the file is called in the personal user account (see section "User certificate (Page 106)").

4.8.2.2 Making OpenVPN settings

Requirement for changing the OpenVPN settings

The user has been assigned the right "Edit system parameters".

Calling the Web page

In the navigation, select "Security > VPN basic settings" and the OpenVPN tab.

Configuring OpenVPN

Configure the following settings that are valid for all OpenVPN connections after you have saved:

Box	Meaning
Activate	When enabled, OpenVPN is used.
Status	Shows whether OpenVPN is enabled or disabled.
TCP port	Specify the port on which the SINEMA RC Server server accepts TCP connections. Assuming that TCP frames can be sent to this port. In a preconnected DSL router, for example, port forwarding must be entered.
UDP port	Specify the port on which the SINEMA RC Server server accepts UDP connections. Assuming that UDP frames can be sent to this port. In a preconnected DSL router, for example, port forwarding must be entered.
Keep alive interval (s)	Enter the interval in seconds at which connection partners send keep alive packets. This setting is automatically transferred to the client when the connection is established. The keep alive packets are sent only when there was no communication during the last interval. If there is no response to the packet, the communications partner assumes an interruption on the connection or that the communications partner is not functioning. Measures are taken according to the "Connection timeout" setting.
Connection timeout (s)	Specify the maximum time in seconds that the communications partner waits for a response from the server before the connection is considered to be interrupted. This setting is automatically transferred to the client when the connection is established. Detection of a connection interruption is achieved with keep alive packets (see setting "Keep alive interval"). If the client detects a connection interruption, it reacts by re-establishing the connection when the connection timeout has elapsed. On the server the set connection timeout is doubled. After the doubled connection timeout has elapsed, the server considers the connection to the client as being interrupted.
DH key length	Select the Diffie-Hellman key exchange protocol to be used between the communications partners.
Cipher	Selection of the algorithm for encryption of the transferred data. The following are available: • AES-128, 192, 256: Advanced Encryption Standard (128, 192 or 256 bit key length, mode CBC) • DES-EDE, DES-EDE3: Data Encryption Standard (128 or 192 bit key length, mode CBC)

Box	Meaning
Hash method	Selection of the authentication algorithm: SHA-1, 256, 512: Secure Hash Algorithm 1, 256 or 512
Min. TLS version	Specify the TLS version.
Interface	The interface that forms the local VPN endpoint. Via this interface the OpenVPN connection to the OpenVPN partner (SINEMA RC client, device) is established. • WAN: Connection only via the WAN interface • LAN 1-n: Connection via available LAN interfaces: • WAN + LAN 1-n: Connection via all interfaces

4.8.2.3 Making the IPsec settings

Requirement for changing the IPsec VPN settings

The user has been assigned the right "Edit system parameters".

Calling the Web page

In the navigation, select "Security > VPN basic settings" and the IPsec tab.

Configuring the basic setting

Configure the following settings that are valid for all IPsec VPN profiles after you have saved:

Box	Meaning
Activate	When activated, IPSec is used.
Status	Shows whether IPsec is enabled or disabled.
Interval after DPD query (s)	Period after which DPD queries are sent. These queries test whether or not the remote station is still reachable.
Timeout after after DPD query (s)	If there is no response to the DPD query, the VPN connection to the remote station is declared to be invalid after this time interval has elapsed.
Interface	The interface is the local endpoint of the VPN connection. Via this interface the VPN connection to the VPN partner (SINEMA RC client, device) is established. • WAN: Connection only via the WAN interface • LAN 1-n: Connection via available LAN interfaces: • WAN + LAN 1-n: Connection via all interfaces

4.8.2.4 IPsec profiles

The devices and users are assigned IPsec profiles The profiles contain the settings of phase 1 and phase 2.

Calling the Web pages

In the navigation, select "Security > VPN basic settings" and the "IPsec profile" tab.

Displayed values

A list of the IPsec profiles that have already been created along with their status is displayed:

Field	Meaning	
Profile name	The name assigned to the IPsec profile. The name must be unique throughout the system and cannot be changed, refer to the section "Creating IPsec profiles (Page 104)".	
Key exchange	Key exchange method	
IKE	Settings of phase 1 - IKE (KE/key exchange)	
ESP	Settings of phase 2 - ESP (authentication)	
Actions	ℹ	Overview of the IPsec profile. This is also displayed for users with the right "read only".
	⚙	Changing an IPsec profile. This also includes changing the settings for phase 1 and 2.

4.8.2.5 Creating IPsec profiles

Requirement for changing the IPsecVPN settings

The user has been assigned the right "Edit system parameters".

Creating a new IPsec profile

1. Open the "IPsec profile" tab.
2. Click the "Create" button.
3. Enter a name for the IPsec profile.
4. In Key exchange method specify whether IKEv2 or IKEv1 will be used.
5. Specify the settings of phase 1 - IKE (KE/key exchange):

Box	Meaning
Encryption algorithm:	The selection depends on the phase und the key exchange method (IKE)
Hash method	Selection of the authentication algorithm: SHA 1, 256, 384, 512
Key derivation	Select the required Diffie-Hellmann group (DH) from which a key will be generated.
Lifetime	The lifetime of the authentication. When the time has elapsed, the VPN endpoints involved must authenticate themselves with each other again and generate a new key

6. Make the settings of phase 2 - ESP (authentication):

Box	Meaning
Protocol	Selection of the protocol AH: The IP Authentication Header (AH) handles the authentication and identification of the source. ESP: The Encapsulation Security Payload (ESP) encrypts the data.
Encryption algorithm:	The selection depends on the phase und the key exchange method (IKE)
Hash method	Selection of the authentication algorithm: SHA 1, 256, 384, 512
Key derivation	Select the required Diffie-Hellmann group (DH) from which a key will be generated.
Lifetime	The lifetime of the authentication. When the time has elapsed, the VPN endpoints involved must authenticate themselves with each other again and generate a new key

7. Click "Finish".

Changing an IPsec profile

Change the corresponding user settings. Then click the "Save" button.

Encryption algorithm

	Phase 1		Phase 2	
	IKEv1	IKEv2	IKEv1	IKEv2
3DES	x	x	x	x
AES128 CBC	x	x	x	x
AES192 CBC	x	x	x	x
AES256 CBC	x	x	x	x
AES128 CTR	-	x	x	x
AES192 CTR	-	x	x	x
AES256 CTR	-	x	x	x
AES128 CCM 16	-	x	x	x
AES192 CCM 16	-	x	x	x
AES256 CCM 16	-	x	x	x
AES128 GCM 16	-	x	x	x
AES192 GCM 16	-	x	x	x
AES256 GCM 16	-	x	x	x

x: is supported

-: is not supported

4.9 My account

4.9.1 User certificate

Calling the Web page

In the navigation, select "My account > User certificate".

Displayed entries

In the "Details" tab, you will see an overview of the user certificate derived from the CA certificate:

Field	Meaning
Serial number	Number to identify the certificate. The serial number is assigned automatically when the certificate is created.
Common name	The name used is generated automatically by the system.
Issuer	Display of the certificate authority that issued the certificate. The system uses the last valid CA certificate.
Valid from	Date from which the certificate is valid.
Valid to	Date on which the certificate expires.
Key length (bits)	Specifies the key length being used. The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred key length".
Signature method	Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate. The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred hash method".

Renewing a user certificate

Note

Only renew valid certificates

You cannot renew a certificate that has already expired. If you attempt to renew an expired certificate, the certificate authority will reject the request. When a certificate has already expired, instead of renewing the existing certificate, you need to request a new certificate.

With the "Renew" button, you can when necessary, e.g. with compromised certificates, generate a new certificate.

To do this enter the relevant user password. The serial number is automatically incremented by one.

Exporting a user certificate

You can download the personal certificate in the "Export" tab. These include:

Field	Meaning
PKCS#12	Download a container in the Personal Information Exchange format (PFX).
PEM	Download certificate and key as Base64-coded ASCII text.
OVPN	Download OpenVPN configuration for user.

4.9.2 Changing the current password

Changing the current password

As a logged-on user, you can change your current password:

1. In the navigation, select "My account > Change password".
2. Enter the old password.
3. Enter the new password and confirm it.

   The new must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers. See also the section "Permitted characters (Page 28)".

Upkeep and maintenance 5

5.1 Backing up and restoring the system configuration

In the backup copy, the current system settings of the SINEMA RC Server are backed up, e.g. configured devices, users.

Note

Settings that are not taken

The following settings are not backed up:

- Network settings
- Log messages

With the backup copy, you can restore the system settings of the server within a SINEMA RC version or transfer them to another server. A backup copy created on a SINEMA RC version e.g. 1.2 cannot be read into a system with SINEMA RC version V1.3.

You can find additional information on the Internet with the following entry ID: 109748144 (https://support.industry.siemens.com/cs/ww/de/view/109748144/en)

Configuring settings

Requirement:

- The user has been assigned the right "Edit system parameters".

Procedure

1. In the navigation panel "System > Backup & restore" select the "Settings" tab.

   Enter the number of permitted backup copies.

   An entry between 10 and 30 is permitted. When the maximum number is reached, the oldest backup copy is overwritten.

2. If the system should be backed up at regular intervals, specify the interval and the time for the backup.

3. Enter a "encryption key".

   The coding key 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 (Page 28)".

   To the backup copy successfuly

4. Confirm the coding key.

5. Click the "Save" button.

Backing up configurations

Requirement

- The user has been assigned the right "Create backup copies".
- The settings for the backup copy are configured.

Procedure

1. In the navigation panel, select "System > > Backup & restore".
2. Click the "Create new backup copy" button.
3. In the dialog that follows, enter a comment on the backup copy.
4. Click the "Finish" button.

Result

A backup copy (*.backup) with the system settings of the SINEMA RC Server has been created.

Restoring the configuration

Requirement

- On the system, the SINEMA RC version is installed with which the backup copy was created.

Importing the backup

1. In the navigation panel "System > Backup & restore" select the "Settings" tab.
2. Enter the same coding key with which the backup was created and save the settings.
3. Click the "Import backup copy" button.
4. Click the "Browse" button.
5. Select the required file in the format *.backup and confirm your selection with the "Open" button.
6. Click the "Finish" button. The backup is displayed in the overview.
7. Click on the "Restore" button to adopt the system configuration of the selected backup copy.

   Click the "Restore" button in the next dialog.

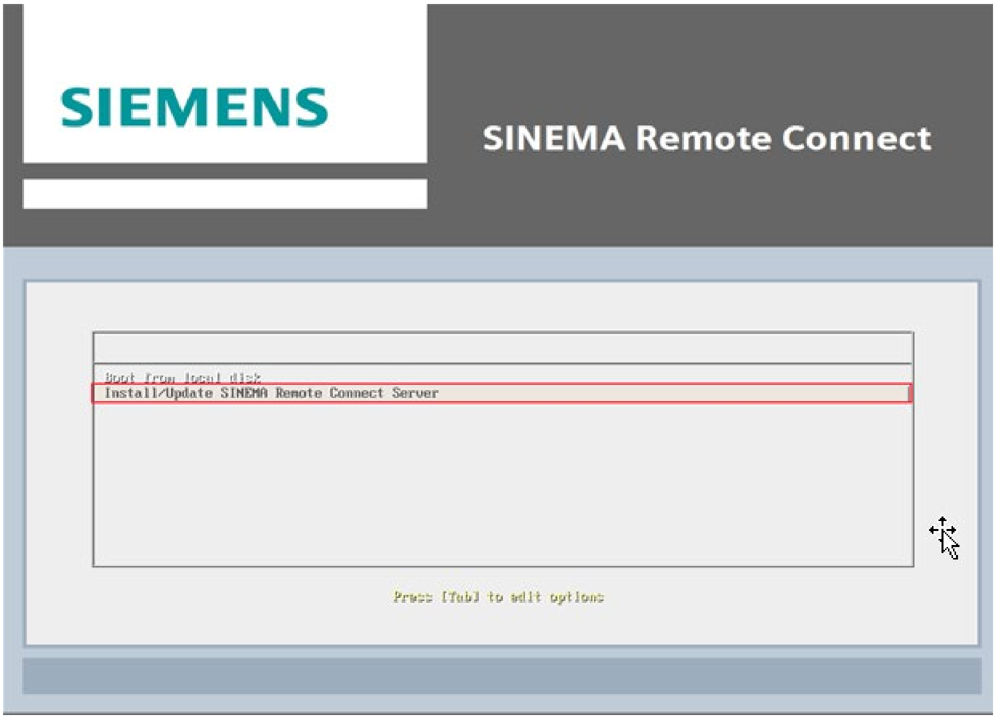
Result

- Backup copy was imported into the same server / hardware with existing installation
  SINEMA RC Server takes the system settings from the selected backup copy and continues working with them. All settings made up to this point that have not been saved in a backup copy are lost.
- Backup copy was imported into another server / hardware with new installation and same network settings
  After successful transfer, the system is restarted and the login page of the SINEMA RC Server opens. The backed up certificates are imported.
- Backup was imported into a different server / hardware and a new installation with different network settings.
  After the restart, the login page of the SINEMA RC Server opens. The certificates are not imported but created new.

5.2 System update V1.2 > V1.3

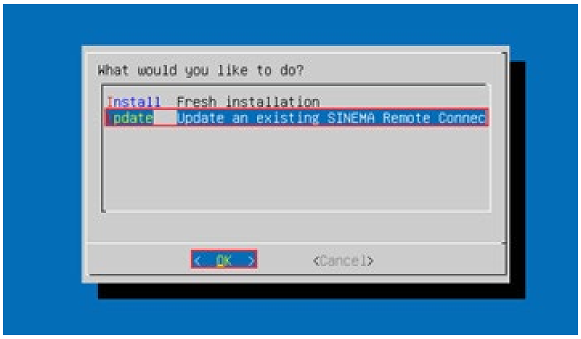
Procedure

1. Back up your configuration using SINEMA RC Server V1.2 WBM and export this backup file to your PC or SFTP server.
   You can find more detailed information on this in the sections "Backup & Restore (Page 63)" and "Server upload (Page 62)".
2. Insert the V1.3 data medium into the drive.
3. Navigate to the WBM menu "System > Update (Page 61)".
   Restart via the "Energy management (Page 61)".
   Installation starts automatically.
4. Select the "Install/Update SINEMA Remote Connect Server" entry in the following dialog.
   Confirm the selection with the ENTER key.



Press [Tab] to edit options

5. In the next dialog, select the entry "Update - Update an existing SINEMA Remote Connect" and click on the < OK > button.



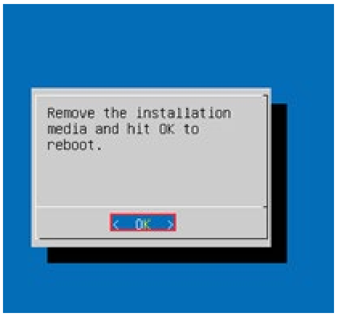
```
What would you like to do?

Install   Fresh installation
 pdate    Update an existing SINEMA Remote Connec

          <  OK  >        <Cancel>
```

The SINEMA RC Server was updated to version 1.3. After this update installation, two boot partitions are available. A partition also contains your operational server version 1.3. Another partition now contains an operational server version 1.3 with the identical server configuration including devices, users and certificates. However, your SINEMA RC Server license was not automatically transferred to V1.3. To enable it on your new V1.3 server, you first need to release the license in version V1.2.

6. Remove the V1.3 disk from the drive and click the < OK > button.

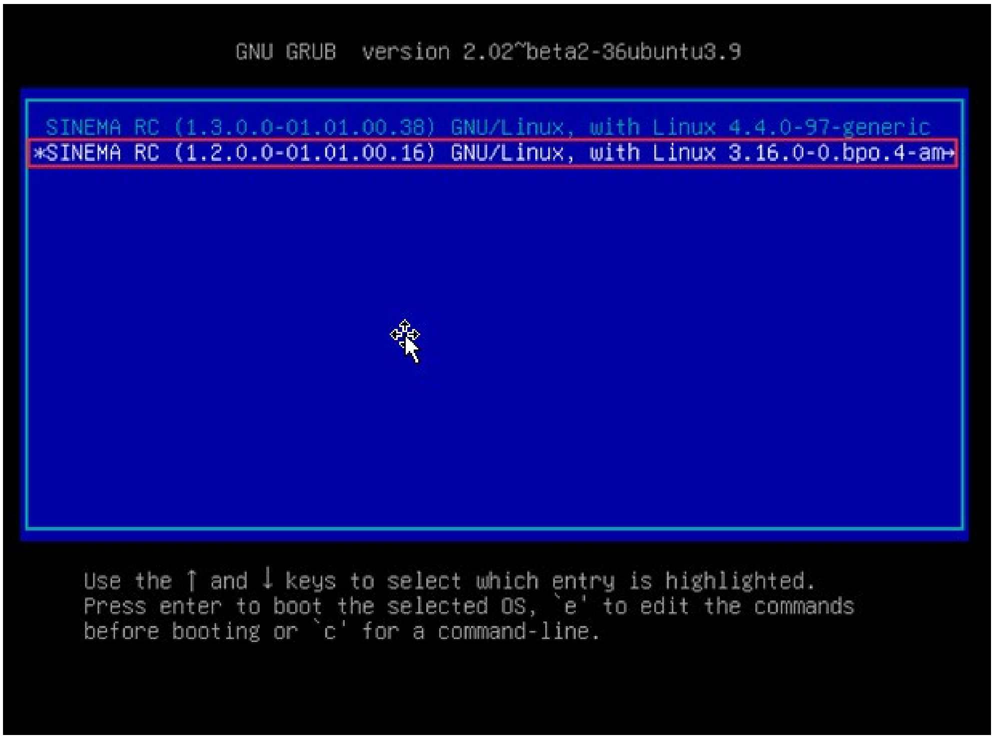


```
Remove the installation
media and hit OK to
reboot.

      <  OK  >
```

Restart the server. In the boot menu, you can see the partitions of both server versions V1.2 and V1.3.

7. Select "SINEMA RC (1.2.0)" from the boot menu and confirm your selection with the ENTER key.

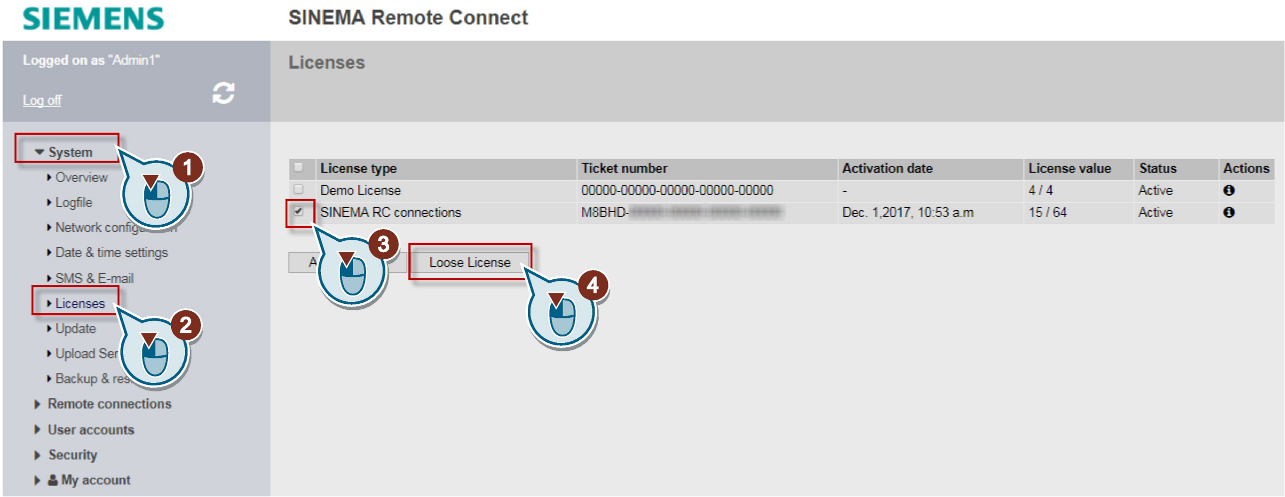


```
                 GNU GRUB  version 2.02~beta2-36ubuntu3.9

   SINEMA RC (1.3.0.0-01.01.00.38) GNU/Linux, with Linux 4.4.0-97-generic
  *SINEMA RC (1.2.0.0-01.01.00.16) GNU/Linux, with Linux 3.16.0-0.bpo.4-am→

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

8. Log in with your user credentials and navigate to the menu "System > Licenses". Release the licenses to reactivate them in server version V1.3.



SINEMA Remote Connect

Logged on as "Admin1"

Log off

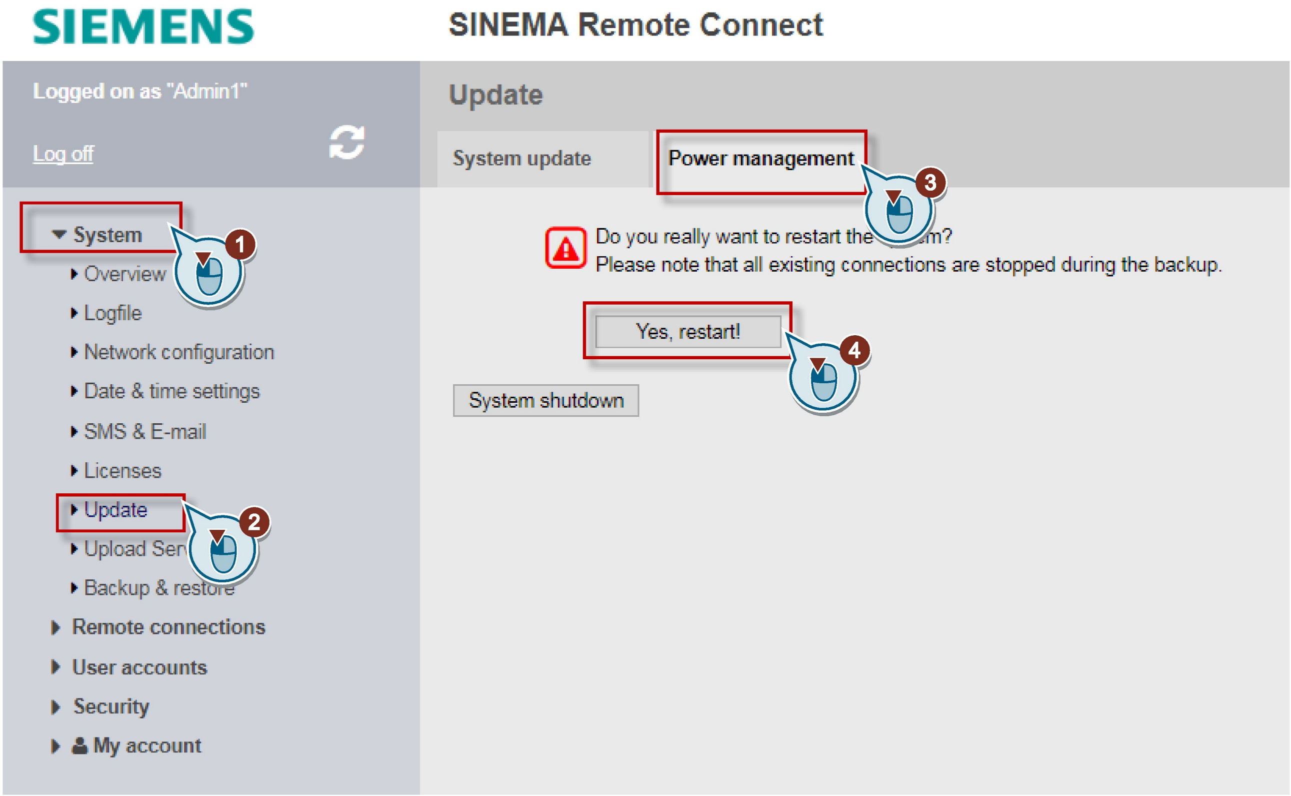
Licenses

□	License type	Ticket number	Activation date	License value	Status	Actions
□	Demo License	00000-00000-00000-00000-00000	-	4 / 4	Active	❶
☑	SINEMA RC connections	M8BHD-[redacted]	Dec. 1,2017, 10:53 a.m	15 / 64	Active	❶

Note

If it is not possible to deactivate the license in WBM (e.g. no connection to the license server), contact our hotline. All further steps are then coordinated with the hotline to reactivate the license.

9. Navigate to the WBM menu "System > Update".
   Perform a restart via the "Energy Management".



SIEMENS SINEMA Remote Connect

Logged on as "Admin1"

Log off

Update

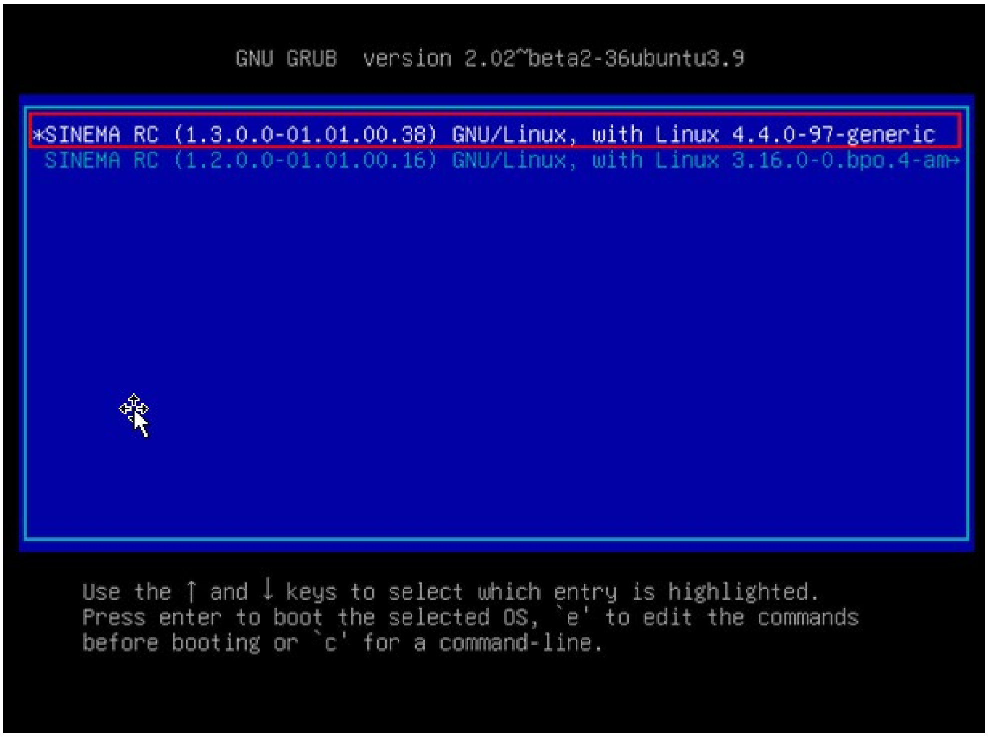
System update | Power management

Do you really want to restart the system?
Please note that all existing connections are stopped during the backup.

Yes, restart!

System shutdown

10. Select "SINEMA RC (1.3.0)" from the boot menu and confirm your selection with the ENTER key.

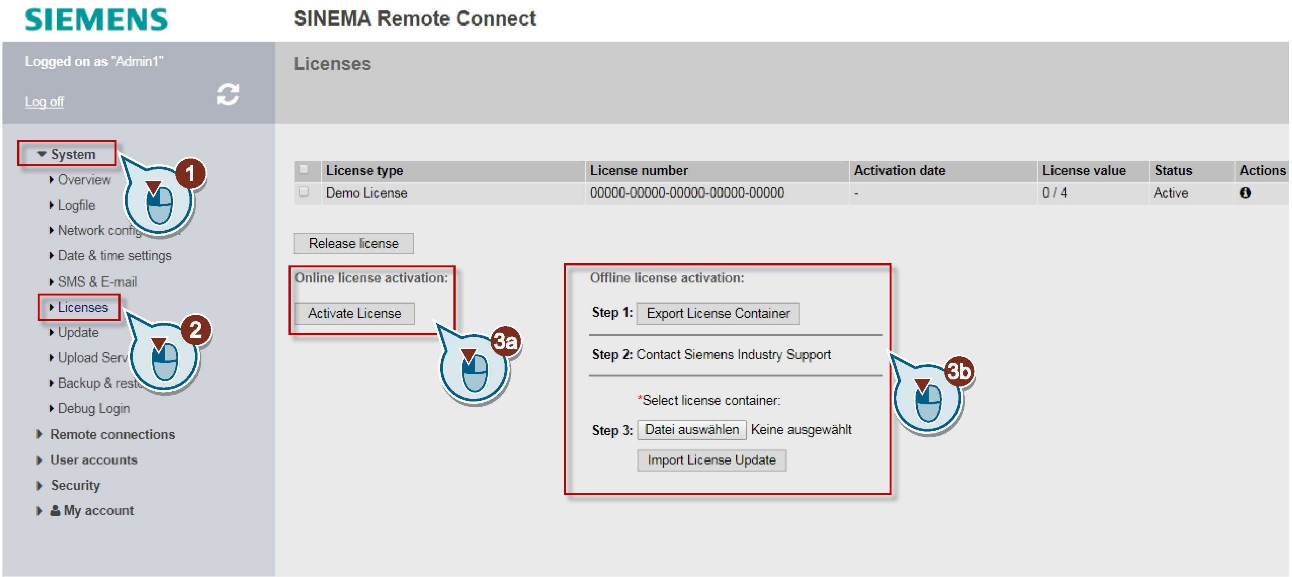


```
                 GNU GRUB  version 2.02~beta2-36ubuntu3.9

*SINEMA RC (1.3.0.0-01.01.00.38) GNU/Linux, with Linux 4.4.0-97-generic
 SINEMA RC (1.2.0.0-01.01.00.16) GNU/Linux, with Linux 3.16.0-0.bpo.4-am→

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

11. Log in with your user credentials and navigate again to the menu "System > Licenses". Activate the licenses.
    You can select between offline or online activation. You can find additional information on this in the section "Managing licenses" .



Licenses

□	License type	License number	Activation date	License value	Status	Actions
□	Demo License	00000-00000-00000-00000-00000	-	0 / 4	Active	ℹ

Online license activation:

Offline license activation:

Step 1: Export License Container

Step 2: Contact Siemens Industry Support

*Select license container:

Step 3: Datei auswählen Keine ausgewählt

Import License Update

Result

The SINEMA RC Server and its license have been updated to version 1.3. The previous configurations of the server are retained. In addition to this updated server version, there is another partition on the PC with the original server version V1.2 as backup. Server version V1.2 can still be started from the boot menu of the PC if the update needs to be undone. No further devices or users can be created in server version V1.2. When you restart the server, the last partition that was started is always used.

Appendix A

A

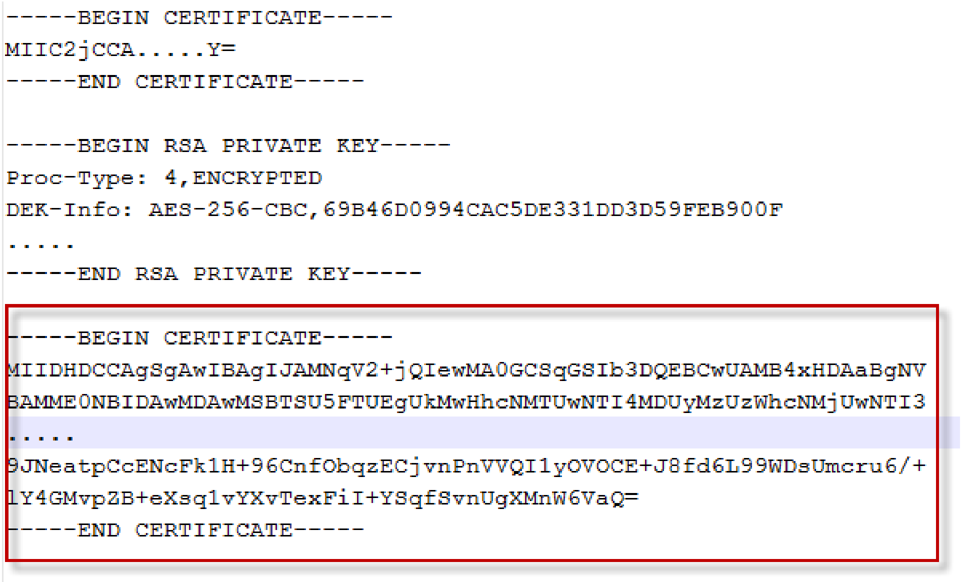
A.1 OpenVPN connection to an iOS device

The procedure was tested with iOS 7.1.2.

To establish an OpenVPN connection to an iOS device, follow the steps below:

1. Log on to the SINEMA RC Server with your user data.
2. In the navigation, select "My account > User certificate" and click on the "Exports" tab.
3. Click on PKCS#12 to load the user certificate on the iOS device in the format PKCS#12. Install the user certificate.
4. Click on PEM to load the CA certificate on the iOS device.

5. Open the pem file with an editor and copy the certificate area to the clipboard.
   - With SINEMA RC V1.0 this is the 3rd section

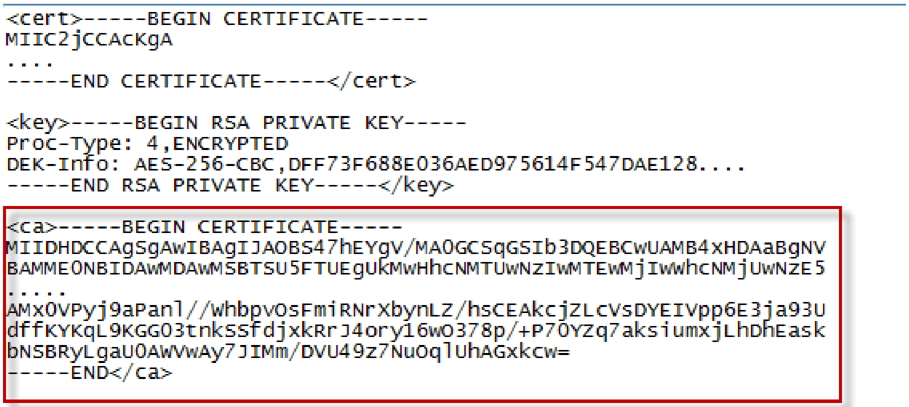


```
-----BEGIN CERTIFICATE-----
MIIC2jCCA.....Y=
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,69B46D0994CAC5DE331DD3D59FEB900F
.....
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDHDCCAgSgAwIBAgIJAMNqV2+jQIewMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME0NBIDAwMDAwMSBTSU5FTUEgUkMwHhcNMTUwNTI4MDUyMzUzWhcNMjUwNTI3
.....
9JNeatpCcENcFk1H+96CnfObqzECjvnPnVVQI1yOVOCE+J8fd6L99WDsUmcru6/+
lY4GMvpZB+eXsq1vYXvTexFiI+YSqfSvnUgXMnW6VaQ=
-----END CERTIFICATE-----
```

   - As of SINEMA RC V 1.1



```
<cert>-----BEGIN CERTIFICATE-----
MIIC2jCCAcKgA
....
-----END CERTIFICATE-----</cert>

<key>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,DFF73F688E036AED975614F547DAE128....
-----END RSA PRIVATE KEY-----</key>

<ca>-----BEGIN CERTIFICATE-----
MIIDHDCCAgSgAwIBAgIJAOBS47hEYgV/MA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME0NBIDAwMDAwMSBTSU5FTUEgUkMwHhcNMTUwNzIwMTEwMjIwWhcNMjUwNzE5
.....
AMx0VPyj9aPanl//whbpvOsFmiRNrXbynLZ/hsCEAkcjZLcVsDYEIVpp6E3ja93U
dffKYKqL9KGG03tnkSSfdjxkRrJ4ory16wO378p/+P70YZq7aksiumxjLhDhEask
bNSBRyLgaU0AWVwAy7JIMm/DVU49z7NuOqlUhAGxkcw=
-----END</ca>
```

6. Click on OVPN to download the OpenVPN configuration file "username.ovpn".
7. Open the file and delete the user certificate from the configuration file. Remove everything from <pkcs12>-----BEGIN CERTIFICATE----- ..... to-----END CERTIFICATE-----</pkcs12>.

8. Insert the following in the configuration file:

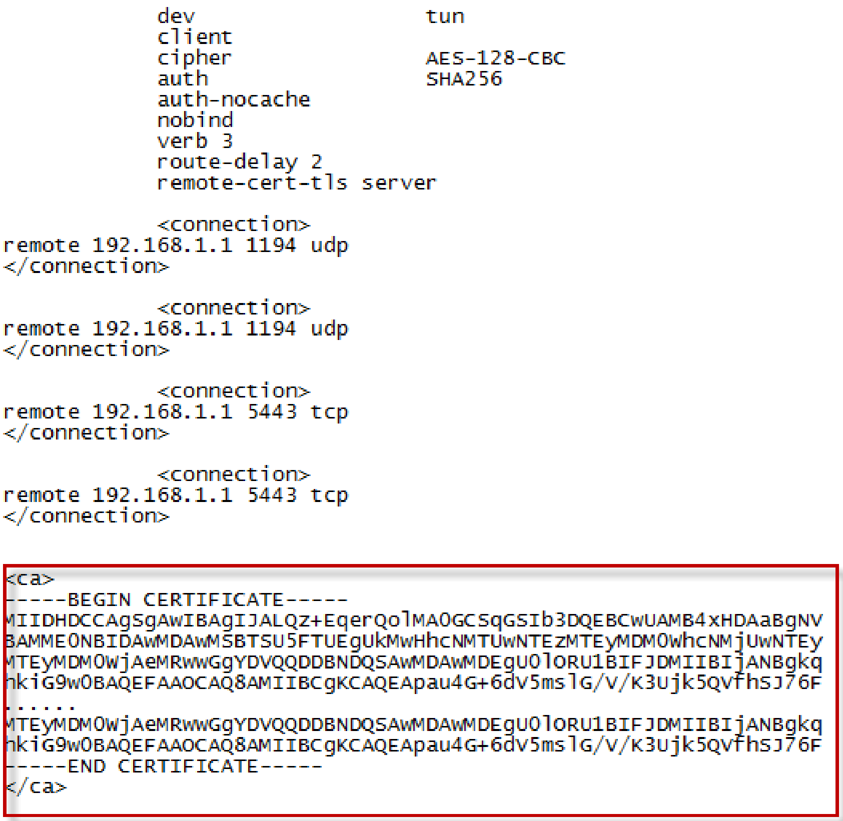
   With SINEMA RC V1.0

   – Insert <ca> </ca>.

   – Insert the content of the clipboard between <ca> and </ca>.

   As of SINEMA RC V 1.1

   – Insert everything from <ca>-----BEGIN CERTIFICATE----- ..... to-----END CERTIFICATE-----</ca>.



```
            dev                   tun
            client
            cipher                AES-128-CBC
            auth                  SHA256
            auth-nocache
            nobind
            verb 3
            route-delay 2
            remote-cert-tls server

            <connection>
remote 192.168.1.1 1194 udp
</connection>

            <connection>
remote 192.168.1.1 1194 udp
</connection>

            <connection>
remote 192.168.1.1 5443 tcp
</connection>

            <connection>
remote 192.168.1.1 5443 tcp
</connection>

<ca>
-----BEGIN CERTIFICATE-----
MIIDHDCCAgSgAwIBAgIJALQz+EqerQolMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME0NBIDAwMDAwMSBTSU5FTUEgUkMwHhcNMTUwNTEzMTEyMDM0WhcNMjUwNTEy
MTEyMDM0WjAeMRwwGgYDVQQDDBNDQSAwMDAwMDEgU0lORU1BIFJDMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApau4G+6dV5mslG/V/K3Ujk5QvfhsJ76F
......
MTEyMDM0WjAeMRwwGgYDVQQDDBNDQSAwMDAwMDEgU0lORU1BIFJDMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApau4G+6dV5mslG/V/K3Ujk5QvfhsJ76F
-----END CERTIFICATE-----
</ca>
```

9. Save the configuration file.

10. Load the OpenVPN configuration file on the iOS device. You can also send yourself the file in an e-mail.

11. Start the OpenVPN app.

Appendix B

B

B.1 Enabling the e-mail address

To receive the e-mail, with some network providers the e-mail address for the recipient of the SMS message first needs to be enabled.

To enable the e-mail address, you normally send a special activation text to an abbreviated number of your network provider. You will find several examples in the following table "Activation and deactivation SMS".

You will receive a reply SMS with the e-mail address containing the phone number and the SMS gateway name of your network operator:

12345@<Domain of the SMS provider>.<Top-level domain>

Note

Check with your network provider whether or not it is necessary to send activation and deactivation SMS messages. Your network provider will inform you of the texts and short number.

Table B- 1 Activation and deactivation SMS (examples)

	E-Plus	**O_2 Germany**	**T-Mobile**	**Vodafone**
SMS gateway name	smsmail.eplus.de	o2online.de	t-mobile-sms.de	vodafone-sms.de
Enabling Send SMS with text to short number	Text: START Short number: 7676245	Text: OPEN Short number: 6245	Text: OPEN Short number: 8000	Text: OPEN Short number: 3400
Deactivating Send SMS with text to short number	Text: STOP Short number: 7676245	Text: STOP Short number: 6245	Text: CLOSE Short number: 8000	Text: CLOSE Short number: 3400

See also

SMS gateway provider (Page 55)

B.2 Monitoring and time response of wake-up SMS messages

Possible causes for unsuccessful wake-up attempts

If a station cannot be woken up, there are different possible reasons for this.

- **Time blocks of SMS gateway providers**

  To trigger a wake-up SMS message, click 📱 in "Remote connections > Manage devices".

  As a defense against spam, some network providers filter out SMS messages with the same content sent to the same subscriber within a limited time, for example 1 minute.

  If you repeatedly try to wake up a device because it does not establish a connection within a short time, wait a suitable time between repetitions. Check the log entries. Messages such as Mail appeared to be SPAM or forget indicate that this is the case.

  If necessary, check with your network provider.

- **Not executed**

  The wake-up job was transferred to SINEMA RC but not executed. Check the connections of SINEMA RC Server, including the connection to the Internet.

- **Negative reply**

  The SMS gateway has not received the message.

  The success of sending a wake-up e-mail to the SMS gateway can be detected via a log message. If the acknowledgement is not received and this status is displayed, there is a disruption on the path between the SINEMA RC Server and the SMS gateway.

Index