SIEMENS

SIMATIC NET

Industrial Remote Communication - Remote Networks
SINEMA Remote Connect V3.2

Operating Instructions

04/2025
C79000-G8976-C383-18

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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. 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 Aktiengesellschaft. 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 Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C383
Ⓟ 10/2025 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 V3.2 SP4

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
SINEMA Remote Connect (OSD)	6GK1722-1VH01-0BK0	+ X (variable number depending on order)

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

Product name	Order ID
KEY-PLUG SINEMA RC (SCALANCE M-800, SCALANCE S615)	6GK5908-0PB00
SINEMA RC UMC license	6GK1724-2VH03-0BV0
SINEMA RC Client V3 (1 VPN client) license	6GK1721-1XG03-0AA0
SINEMA RC Client V3 (OSD) license	6GK1721-1XG03-0AK0
SINEMA RC API license	6GK1724-3VH03-0BV0
SINEMA RC Edge client (OSD) license	6GK1721-4XG01-0BK0
SINEMA RC Layer 2 (OSD) license	6GK1724-6XG01-0BK0
SINEMA RC device license	6GK1724-5XG01-0BK0
SINEMA RC IAM license	6GK1724-7XG01-0BK0

The following licenses are available for the connection to UMC:

Software/License	Order ID
TIA Portal User Management Component (UMC) Rental License for 100 user accounts and 365 days Certificate of License for download	6ES7823-1UE30-0YA0
TIA Portal User Management Component (UMC) Rental License for 4000 user accounts and 365 days Certificate of License for download	6ES7823-1UE10-0YA0

Supported products

In the "Connectable nodes (Page 24)" 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
  - SCALANCE MUM853
  - SCALANCE MUM856
- **UMC**
  This abbreviation is used for "User Management Component", a database for the central administration of user data.
- **API**
  This abbreviation stands for "Application Programming Interface", an HTTP-based AP interface via which you can configure the WBM of the SINEMA RC server.

New in this release

- Server information text: Display on the login page and in the header
- OAuth/OpenID policy: Defining the relationship between claims via logical operators
- Client settings: Display of the logo in the header

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.
- Getting Started "SINEMA Remote Connect API server"
  This manual supports you with the WBM configuration of the SINEMA RC server via the AP interface.
- Getting Started "SINEMA RC Cloud Installation"
  This manual supports you with the SINEMA RC installation in a cloud.
  You can find the manual on the Internet pages of Siemens Industry Online Support
- "UMC Web UI User Manual"
  This manual supports you when creating and managing user accounts in the UMC.

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

License conditions

Note

Open source software

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

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

- OSS_SINEMA-RC_86.pdf

Cybersecurity notes

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry (https://www.siemens.com/industrialsecurity).

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert (https://www.siemens.com/cert).

Note on firmware/software support

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

Decommissioning

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

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

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

To reset the SINEMA RC Server to factory settings, re-install the SINEMA RC Server.

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

1 Application and properties

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 smart card.

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 MUM856-1, SCALANCE MUM853-1
- 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 24)" 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 115)".
  - Access is achieved using a smart card with a PIN procedure (Personal Identification Number). To check the identity a certificate is used.
  - Access takes place via OAuth/OpenID.
- 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 108)".

1.2 Overview of functions

Configuring the SINEMA Remote Connect Server

The SINEMA RC Server can be configured via a Web Based Management (WBM). In addition, via the HTTP-based API interface, you can access the WBM of the SINEMA RC server and configure API requests with it. To do this, you need an API license with which you can enable the API server on the SINEMA RC server. You can find additional information in the section "API (Page 120)".

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 nodes

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

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 "administrator" role is assigned automatically to this newly created user.

The 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 rights and roles (Page 108)".

The administrator is listed with the user accounts and can neither be edited nor deleted. The "admin" user name is no longer available.

UMC users

SINEMA RC provides the possibility to use the user data stored centrally on a UMC server. In addition, the UMC server can connect to the Windows Active Directory and access its user data. Using the UMC user data means it is not necessary to create individual user accounts locally on the SINEMA RC. The administrator only needs to configure a connection to the UMC on the SINEMA RC server and enter the name of the UMC user group in the role settings for the affected role. The names of the UMC user groups in SINEMA RC must match exactly the names of the UMC user groups in UMC. When a UMC user logs on with UMC, SINEMA RC establishes a connection to the UMC server, accesses the user account via the UMC user group and creates a temporary user with the assigned role.

You can find information on creating and managing user accounts in UMC in the "UMC Web UI User Manual".

Licensing on SINEMA RC

You need a UMC license to be able to use the UMC server.

- Trial license
  With the trial license, you have unrestricted use of UMC for 14 days for test and evaluation purposes, but not for productive use. All liability claims are excluded. After the trial license has expired, you need to procure a rental license.
- Rental license
  With an activated rental license, you can use UMC without restrictions in SINEMA RC. The rental license is available directly as Certificate of License (CoL).

Logging on

The following options are available for logging on:

- Locally to the WBM
  - Logon with user name and password (Page 39)
  - Logon with the Smartcard (Page 43)
  - Logon with PKI certificate (Page 43)
  - Logon with TOTP-based two-factor authentication (Page 47)
  - Login with OAuth/OpenID (Page 48)
- Via a UMC server (Page 41)
  - Login with user name and password with two-factor authentication

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.

Rights are distinguished as follows:

- Group rights
  Rights are applied at the participant group level. With group rights, the user can see and manage only the devices, users, remote connections and LANs that are in the same participant group as the user.
- Global rights
  The user can manage all devices.

Participant group

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

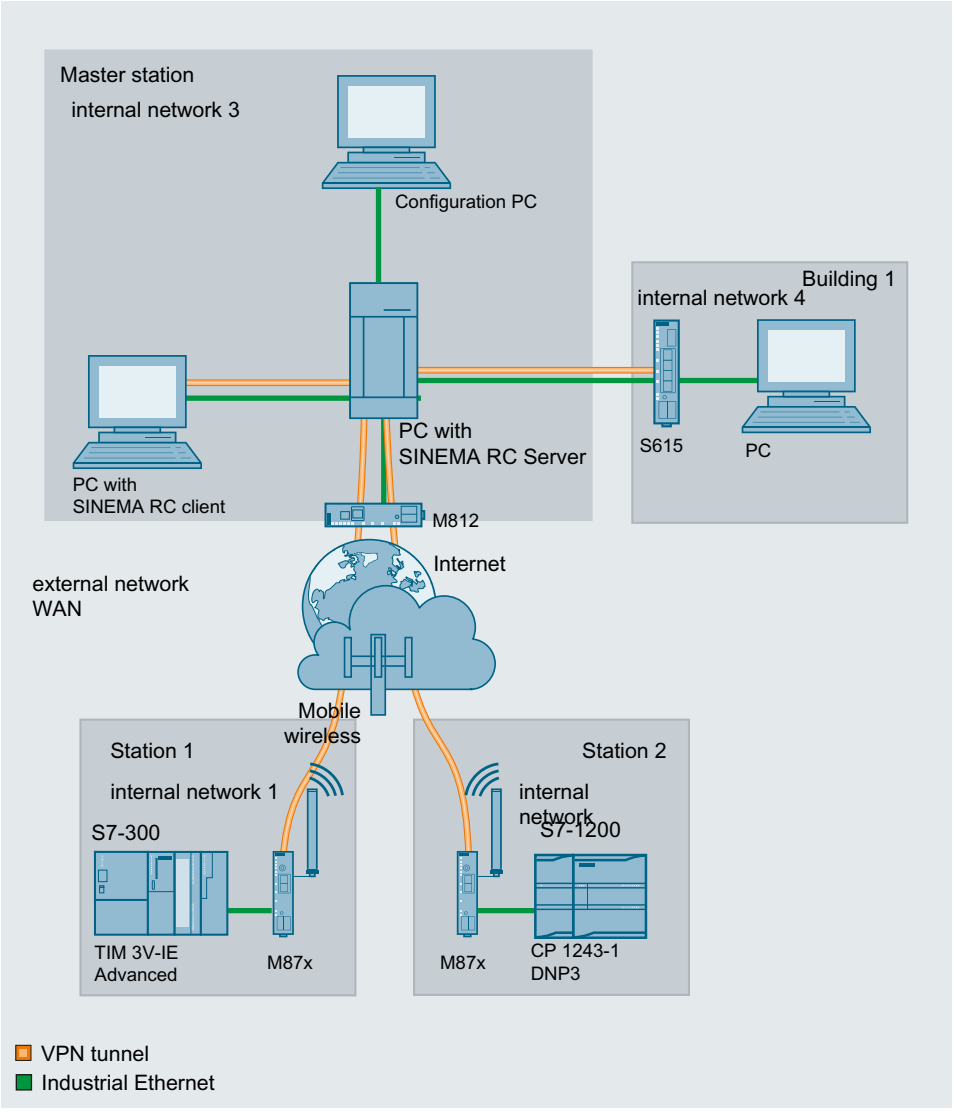
Standard participant group	Description
vpn_user_group	The communication between the nodes is not permitted.
vpn_device_group	

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.

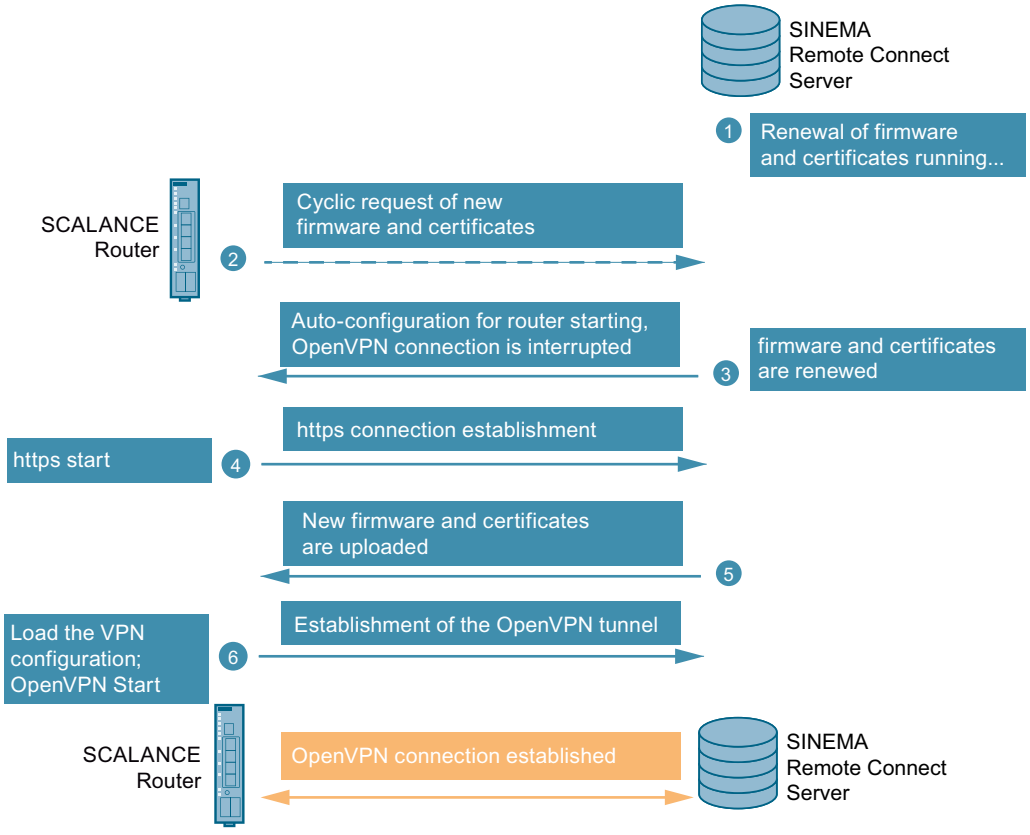
1.5 Automatic distribution of certificates and firmware

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



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.

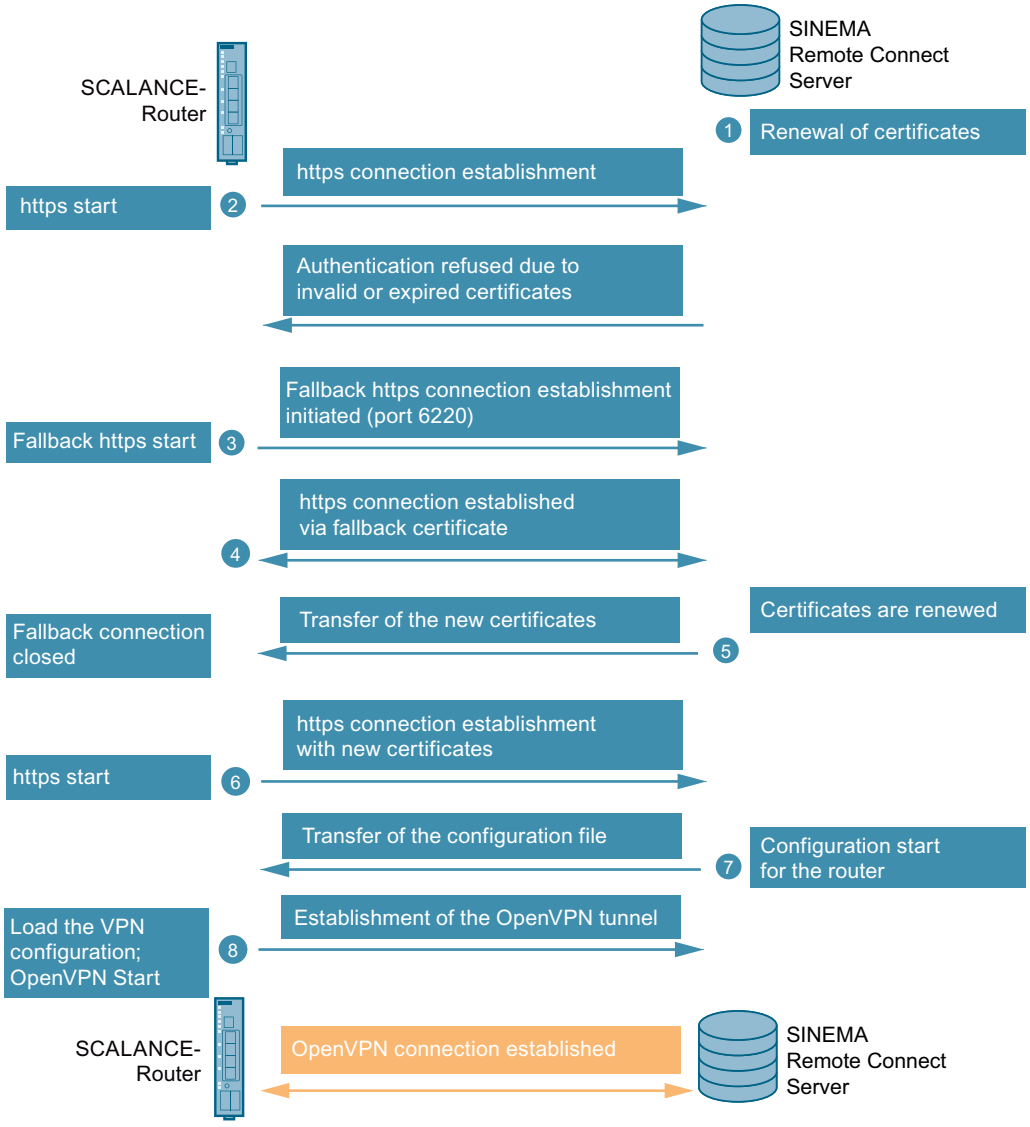
Result

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



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 (x86)	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	> 25 GB	> 60 GB	250 GB SSD

Virtualization platforms

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

- Proxmox version 8.2.2
- Hyper-V V10.0
- VMware vSphere
  - vMotion enables flexible and interruption-free migration of VMs.
  - RAID ensures redundancy and protection of data on the memory systems.
  - HA makes sure that VMs are restarted automatically when a host fails.

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.

Note

Snapshot and copies

For licensing reasons, loading a snapshot and copying a virtual machine is not supported. Use the Backing up & restoring (Page 78) function.

More information is available in the FAQ "How do you move a SINEMA Remote Connect Server via a backup copy if the network environment does not change?" with the entry ID: 109748144 (https://support.industry.siemens.com/cs/en/view/109748144).

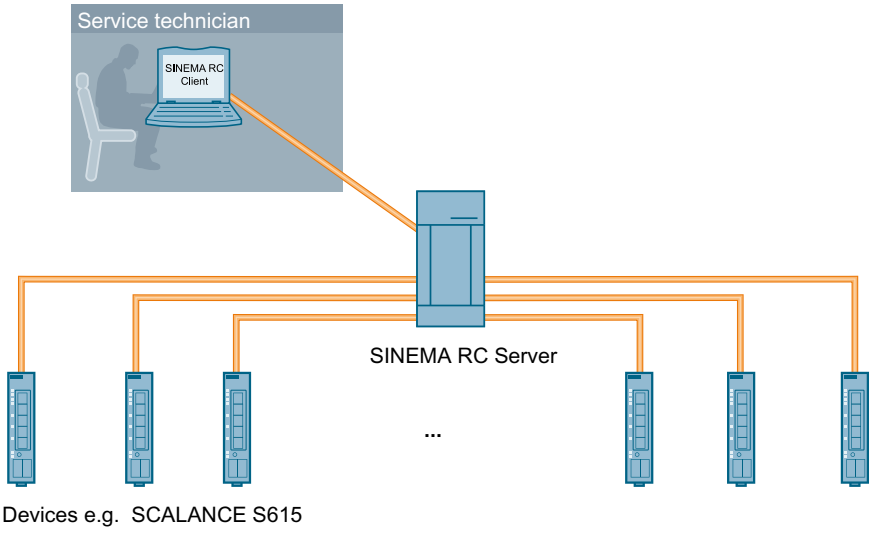
Maximum configuration limits

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.

SINEMA RC Client

The SINEMA RC Client should always have the same version as the SINEMA RC Server.

Connectable nodes

The following nodes are suitable for connection to SINEMA RC.

Device type	Node	Article number	Firmware version [5]	Connection establishment to the SINEMA RC Server					Subnets (vlan)
				Wake-up SMS	Digital input [6]	Permanent	IPsec	OpenVPN	
SCALANCE S615	S615	6GK5615-0AA00-2AA2	As of 4.0	-	✓	✓	✓	✓	16
SCALANCE SC-600	SC622-2C	6GK5622-2GS00-2AC2		-	✓	✓	-	✓ [1]	257
	SC626-2C	6GK5626-2GS00-2AC2		-	✓	✓	-	✓ [1]	257
	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
SCALANCE M804 PB	M804PB	6GK5804-0AP00-2AA2	As of 6.0	-	✓	✓	✓	✓	16
SCALANCE MUM800	MUM856-1	6GK5856-2EA00-3DA1 (EU) 6GK5856-2EA00-3AA1 (ROW)	As of 7.1	✓	✓	✓	✓	✓	16
	MUM853-1	6GK5853-2EA00-3DA1 (EU)	As of 7.1	✓	✓	✓	✓	✓	16

Device type	Node	Article number	Firmware version [5]	Connection establishment to the SINEMA RC Server					Subnets (vlan)
				Wake-up SMS	Digital input [6]	Permanent	IPsec	OpenVPN	
SIMATIC CP1200	CP 1243-1	6GK7243-1BX30-0XE0	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 IRC	6GK7542-6VX00-0XE0	As of 2.0	-	-	✓	✓	✓	
SIMATIC RTU 3010C	RTU3010C	6NH3112-0BA00-0XX0		-	- [4]	✓	-	✓	
SIMATIC RTU 303XC	RTU3031C	6NH3112-3BB00-0XX0		✓	- [4]	✓	-	✓	
	RTU3030C	6NH3112-3BA00-0XX0		✓	- [4]	✓	-	✓	
SIMATIC RTU 3040C	RTU3041C	6NH3112-4BB00-0XX0		✓	- [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 can 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.

5) The "SINEMA RC" function is available in the node from this firmware version.

6) Initiation of connection establishment through digital input on the device.

2.3 License information

Licenses

We distinguish between the following license types. The behavior of the software differs depending on the license type:

License types	Description
Demo	The following licenses are already included in the installation of the SINEMA RC server: • SINEMA Remote Connect 4: 4 participants • SINEMA Remote Connect Client 1 The Certificate of License determines the type of use. **Note** The SINEMA Remote Client 1 license cannot be converted to a Floating license.
Update	Usage is limited to the specified number of participants or clients With multiple licenses, the participants or clients under "Number" are added. The number of participants can be increased with the following connection 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 The number of SINEMA RC Clients can be increased with the following licenses: • SINEMA Remote Connect Client SW, +1 VPN
Floating	Use does not depend on the number of client installations but the number of clients that can be connected simultaneously to the SINEMA RC server. Three client standard licenses can be converted into one floating license. The floating license is only blocked during actual use. When it is no longer in use, the license is available again and can be temporarily assigned to any user.
Trial	This license restricts use of the function to a specific number of days from the time of first use. The software can only be used for test and validation purposes.
Single	The use of UMC (Page 41), API (Page 3) and Layer 2 is not time-limited.

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/clients, you require an update to a new license. To be able to make a license update, you need to obtain a new license and enter the ticket ID in the WBM.

The procedure for activating the license in the WBM is described in the section "Overview (Page 69)".

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

2.4 Permitted characters

Passwords

Observe the following rules when creating or changing the passwords:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z !#$%&()*+,-./:;<=>?@[~]_{|}^
Length of the password	8 ... 128 characters The password depends on the configured password rules, see section "Access (Page 129)".

Note

Passwords

Use passwords with a high password strength. The password should contain special characters, lowercase and uppercase letters as well as numbers.

Using password policies, you can tighten the restrictions listed above for passwords even further. How to define password policies is described in the section "Managing roles and rights (Page 108)".

User names

Observe the following rules when creating or changing the user names:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z @, . _
User names not allowed	admin, conn
Length of the user name	1 to 30 characters

Role names

Observe the following rules when creating or changing the role names:

Allowed characters of a character set	0123456789 A...Z a...z _ - . +
Length of the role name	1 to 80 characters

Group names

Observe the following rules when creating or changing the group names:

Allowed characters of a character set	0123456789 A...Z a...z _ . @ + -
Length of the group name	1 to 50 characters

Device names

When creating or changing the device names, remember the following rules:

Allowed characters of a character set	0123456789 A...Z a...z _
Device names not allowed	conn
Length of the device name	1 to 30 characters

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 Planned operating environment

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

- For secure operation, observe the security recommendations (Page 31).
- Check that the offered ciphers (Page 191) comply with security standards.
- Use the device, user and group settings in the SINEMA Remote Connect Server to grant the respective devices and users access to only the necessary plant parts.
- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length on the SINEMA RC Server. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("Security > Certificate management > Web server (Page 135)").
- Use Public Key Infrastructure (PKI) certificates or two-factor authentication for the users.
- Use a second network adapter and allow access to the WBM only over LAN.
- Make sure that only authorized persons have access to the system.
- Only connect appropriate and trusted devices or USBs to the server in order to protect the server from unauthorized access to data.
- As user with administrator rights, keep the SINEMA RC Server up to date and apply updates when they are available.
- Use the SINEMA RC Server in secure networks.
- Connect a central Syslog server to the SINEMA Remote Connect Server.
- As user with administrator rights, use different accounts - one for administration and one for operative use.
- Set up at least two administrators. If only one administrator is set up, the loss of the administrator password means that no more administrator tasks can be performed.

3.2 Security recommendations

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

General

- You should make regular checks to make sure that this product meets these recommendations and/or other internal security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products (https://www.siemens.com/industrialsecurity).

- If possible, do not connect the SINEMA RC Server directly to the Internet. Operate the SINEMA RC Server within a secure network area.
- When the internal and external network are disconnected, an attacker cannot access internal data. If possible, operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (Page 139) (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.)
- Check the user documentation of other Siemens products that are used together with the product for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central Syslog server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.
- Use the "High (Page 129)" setting for the encryption (ciphers).
- Decommission the SINEMA RC Server properly to prevent unauthorized persons from accessing confidential data. For more information, refer to "Decommissioning (Page 3)".

Software

- Check regularly for new software versions or security updates and apply them.
- You can find the latest information on security patches for Siemens products on the Industrial Security (https://www.siemens.com/industrialsecurity) and ProductCERT Security Advisories (https://www.siemens.com/cert) web pages.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- If a new version is available for the SINEMA RC Server, you can find the update on the Internet pages of Siemens Industry Online Support under the following ID: 21816 (https://support.industry.siemens.com/cs/ww/en/ps/21816/dl)
  You will find a SHA256 hash value in the update file. With this, you can check whether the file was downloaded unchanged. To check this, you calculate the hash value of the downloaded file and compare it with the value specified on the download page.
- Logs and backup files can be downloaded from the SINEMA RC Server. Ensure that the files are adequately protected. The options for achieving this include storing the files in a secure location, or transmitting configuration files only through secure communication channels. Backup files are encrypted with a backup encryption key, see "Backup & Restore (Page 78)".

Physical/remote access

- Restrict 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.
- Protect the SINEMA RC Server from unauthorized access by installing it in racks / control cabinets / control rooms that can be locked.

- Lock unused physical ports on the device. Unused ports can be used to access the system without authorization.
- If possible, use the VPN functionality (Page 139) to encrypt and authenticate communication for communication via non-secure networks.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods (Page 129) and protocols are configured for the server.
- Terminate management connections (e.g. HTTPS, SSH) properly.
- Use Dedicated Device Access (DDA). User-specific access rights for dedicated nodes can be stored in the subnet with this, see "Devices (Page 86)".
- Use SNMPv3 only on the LAN interface.

Authentication

- Define rules for the use of devices and assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
- This recommendation also applies to symmetrical passwords/keys configured on the device.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- Do not use one password for different users and systems.
- Use the following password policies (Page 108):
  - When the current password expires.
  - The current password can be reused only after different passwords.
  - User must change password after first login.
  - Two-factor authentication is used.
    Keep the operating system on the mobile device and the authentication app up to date. The authentication app must be trusted. Keep your password safe on the device, see "Login with TOTP-based two-factor authentication (Page 47)".
- When authentication is performed via UMC, make sure that all communication takes place within the security environment or is protected by a secure channel. Specify when the temporary UMC user will be deleted, see UMC policy (Page 108). You can find more information in "Login via UMC (Page 41)".

- If authentication via smart card/PKI is performed, use the following PKI policy (Page 108).
  - Filter criteria according to which a check is made at the login, see "Login with the smart card/PKI certificate (Page 43)".
  - When the temporary user is deleted.

  There are two options to lock out users:
  - Certificate Revocation List (CRL), see "PKI certificate management (Page 144)".
  - PKI DN Blacklist, see "PKI certificate management (Page 144)".
- Use participant groups (Page 99) and roles (Page 108) that are tailored to the scope of authorization required by each user. Do not use only the default role "admin".

Keys and certificates

- The device contains a pre-installed X.509 certificate with key, see "Using certificates (Page 132)". Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed by a reliable external or internal certification authority, see "Import Web server certificate (Page 135)".
- Use a certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Use password-protected certificates in the format "PKCS #12".
- Change keys and certificates immediately if there is a suspicion of compromise.
- 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 change-able**	**Authentica-tion**
HTTPS	TCP	443	Open	✓	✓
HTTPS for certifi-cate auto enroll-ment	TCP	6220	Open	✓	✓
IPsec	ESP	n/a	Open	--	✓
IPsec encapsulated	UDP	500	Open	--	✓
IPsec encapsulated NAPT	UDP	4500	Open	--	✓
OpenVPN	UDP	1194	Open	✓	✓
	TCP	5443	Open	✓	✓
SFTP	TCP	22	Outgoing only	✓	✓
SMTP	TCP	25	Outgoing only	✓	--
	TCP	587	Outgoing only	✓	✓
SNMP	UDP	161	Outgoing only	✓	✓
SSH	TCP	22	Open (when configured)	✓	✓
Syslog	UDP TCP	514	Outgoing only	✓ ✓	-- ✓
UMC	TCP	442	Outgoing only	✓	✓
VXLAN (Layer2)	UDP	4789	Open (when configured)	✓	--

Table 3-2 Services used

Protocol		**Port num-ber**	**Port status**
NTP	UDP	123	Outgoing when configured
DNS	TCP	53	Outgoing when configured
E-mail client	TCP	25 or other	Outgoing

Protocol		Port number	Port status
HTTPS - CRL retrieval	TCP	according to URL	Outgoing
HTTPS - license activation	TCP	443	Outgoing with activation of the online license of the product
NTS	TCP	4460	Outgoing when configured

3.3 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. 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.

Before installing SINEMA Remote Connect from the DVD, compare the SHA256 hash value of the DVD with the SHA256 hash value specified on the download page.

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, specify the IP address, the network mask and the gateway for the WAN interface. Alternatively, select dynamic assignment of the IP address via DHCP.

Result

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

Note

SINEMA RC server with cloud connection

If you download the server into the cloud and want to set up multiple servers from one image, you need to log in with "admin" directly after the installation and do this. This is the only way to guarantee that each server has its own certificates.

Before you can configure further settings using WBM, you are prompted to create a new user and check the network configuration. Note that login with "admin" is no longer possible after this.

Upgrading the server version

The update must be performed in the correct order:
V1.0 > V1.1 > V1.2 > V1.3 > V2.0 > V2.1 > V3.0 > V3.1 > 3.2

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; see section "System update V1.2 > V1.3 (Page 161)".

Note

System Update V2.0 > V2.1

Before you update the software version, you need to release the licenses for "SINEMA RC (2.0)" and reactivate them in server version V2.1. The procedure is described in the section "System Update V2.0 > V2.1 (Page 166)".

Procedure

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

Result

The system is 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.

You can find more detailed information in the section "Update (Page 77)".

3.4 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 90)".
   - 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 102)".

   When the device is configured, the certificate is created automatically.
   For more detailed information, refer to the section "Overview of certificate management (Page 132)".
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".
   If you have forgotten the password, you can reset it; see "Reset password".
3. Click the "Log in" button.
   When the "Two-factor authentication" setting is enabled, generate a one-time token using the Authentication app. When you enable "Remember for this browser", the one-time token is saved and remains valid for 30 days. After this time, another one-time token is required.
   The start page of the WBM opens. A user agreement may be displayed, see section "User agreement (Page 118)". If you click the "Accept" button, the start page appears.

Changing the current password

As a logged-on user, you can change your current password; refer to the section "Changing the current password (Page 157)".

First login: After the new installation or after resetting to factory settings

1. 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 "administrator" role is assigned automatically to this newly created user.
   The 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 on 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 118)". If you click the "Accept" button, the start page appears.

Note

Password change after first login of a user

After the first login, a configured user is forwarded automatically to a page on which to change the password. Without this process, login to the SINEMA RC Client is not possible.

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.

To ensure that all sensitive data is being deleted, reinstall SINEMA Remote Connect. This step deletes all data on the hard disk.

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.

Reset password

Requirement:

- The "Enable password reset via e-mail" parameter is configured in the local password policies.
- The e-mail address is stored for the user account.
- E-mail client is configured and enabled.

Procedure

1. Click the "Forgot password?" link.
2. Enter the user name in the following dialog.
3. Click "Send reset link". The link to reset the password is sent to the stored e-mail address.
4. Click the link in the e-mail.
   - Link is valid
     Specify a new password.
   - Link is invalid
     Either the link has already been used or the link has expired. Go back to the login page and request a new reset link.

4.2.2 Logging on with UMC

UMC (User Management Component) is a database for the central administration of user data. UMC offers efficient user management that reduces the workload for maintaining user data in the plant. UMC can optionally be part of the AD domain so that the user data can be directly read out from a Microsoft Active Directory.

If a UMC server is configured on SINEMA RC, a user created on the UMC can log onto SINEMA RC with their UMC access data.

You will find additional information under the entry ID: 109780337

How it works

First, a UMC user is created on the UMC server and assigned to one or multiple UMC user groups. The name of the UMC user group is found later in SINEMA RC.

The administrator configures the connection to the UMC server on the SINEMA RC server and also creates a role for which the name of the UMC user group associated with the UMC user is entered in addition.

When a UMC user logs onto SINEMA RC using their UMC login, the SINEMA RC establishes a connection to the UMC server. SINEMA RC checks whether the user is assigned to a UMC user group entered on SINEMA RC and enabled for the connection.

Data exchange between the two servers is only possible when the names of the UMC user groups in SINEMA RC match exactly the names of the UMC user groups in UMC.

After successful login, the "Two-factor authentication" page opens.

On first login, scan the QR token with the authenticator app or enter the alphanumeric token in the app. This page is only shown on first login.
If the QR token is already enabled, enter the one-time token generated with the authentication app.

Note

Labeling of a UMC user with prefix

Every UMC user receives the prefix "Umcuser_". The backslash "\" in the user name of the user of a UMC server is converted to an underscore "_" in SINEMA RC.

Licensing on UMC server

- The UMC server is part of the SINEMA RC client program download/program DVD.
- With the installation of the software, you can manage up to 10 user accounts without a license. For more user accounts, you require a license.
- You can cumulate this license. If you have multiple licenses, the permissible configuration limit for user accounts is derived from the sum of the licenses.
- The license is required for the ring server of the User Management Component domain. The license is offered as Rental License for 365 days. The Certificate of License (CoL) can be downloaded directly.

Software/License	Article number
TIA Portal User Management Component (UMC) Rental License for 100 user accounts and 365 days Certificate of License for download	6ES7823-1UE30-0YA0
TIA Portal User Management Component (UMC) Rental License for 4000 user accounts and 365 days Certificate of License for download	6ES7823-1UE10-0YA0

Requirements on the SINEMA RC server

- A user is created on the UMC and assigned to a UMC user group.
- A valid SINEMA RC UMC license (MLFB 6GK1724-2VH03-0BV0) or trial license is activated on SINEMA RC.

- The connection to the UMC server is set up on the SINEMA RC, see section "UMC Settings (Page 120)".
- The UMC user group is linked to a role in SINEMA RC via the UMC guidelines, see section ”Managing roles and rights (Page 108)”.

Procedure

1. Select the "UMC" tab on the SINEMA RC login Web page.
2. Enter the user name.
3. Enter the corresponding password.
4. Click the "Log on with UMC" button.
   After successful login, the "Two-factor authentication" page opens. The prerequisite is that two-factor authentication is enabled for the UMC user group.
   On first login, scan the QR token with the authenticator app or enter the alphanumeric token in the app. This page is only displayed on first login to the UMC server.
   If the QR token is already enabled, enter the one-time token generated with the authentication app.

Note

Changing the data of a UMC user

UMC users logged onto SINEMA RC cannot edit their access data and their profile in SINEMA RC.

The administrator only has the rights to delete a UMC user from the user list or assign the name of a UMC user group to a role.

See also

109780337 (https://support.industry.siemens.com/cs/en/de/view/109780337)

4.2.3 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 called "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 (the certificate path) must exist on the SINEMA RC server to allow validation of 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 115)".
- 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".

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 144)".
- 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 corresponding login method has been set, see section "Create a new user (Page 115)".
- 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: The suitable PKCS11-DLL must be selected for the card reader and smartcard.

Procedure

1. Insert your smart card in the reader device.
2. Click the card symbol.
3. Enter your PIN and click on "Log on".
   A user agreement may be displayed, see section "User agreement (Page 118)". 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 144)".
- 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 corresponding login method has been set, see section "Create a new user (Page 115)".

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. A user agreement may be displayed, see section "User agreement (Page 118)". 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, the PKI card with this user name is logged on with the SINEMA RC Server, see section "Creating a new user (Page 115)".
- Temporary users
  If the PKI DN filter rule applies to a role, a temporary user "carduser_X" is created. The temporary user is listed in "User accounts > Users & Roles". The user receives the rights 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". 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.

4.2.4 Logon with TOTP-based two-factor authentication

With two-factor authentication, a second query is added after authentication with user name and password. To log on to the SINEMA RC server, you need a user name, a password and a onetime token; this token is also referred to as TOTP (Time-based One-Time Password) or token. The one-time token is generated by an authentication app and is valid for 30 seconds.

Two-factor authentication is enabled by default. The configuration is made for the user in the role settings. The administrator can enable two-factor authentication for the administrator user account. The administrator can also generate a list of tokens that serve as backup tokens in case the device and its one-time token is lost. Each backup token can only be used once.

Note

Security requirements

Keep the operating system on the mobile device and the authentication app up to date. The authentication app must be trusted. Keep your password safe on the device.

Requirement

- An authentication app is installed on the smartphone.

Procedure

1. Enter the user name and the associated password.
2. After successful logon, the "Two-factor authentication" page opens.
3. Generate a one-time token using the authentication app.
4. If the "Enable Remember Token" option is activated for the role, the one-time token is saved. A new one-time token is required after the validity expires.
5. In "Token", enter the one-time token. If administrators lose their device and its one-time token, they can enter a backup token.

User: First use of two-factor authentication

Enable Two-Factor Authentication

1. Create a role. For the local password policies, "Enable Two-Factor Authentication" is enabled by default, see section "Managing roles and rights (Page 108)".
2. Assign the corresponding role to the user.

Procedure

1. Enter the user name and the associated password.
2. After successful logon, the "Two-factor authentication" page opens.
3. Scan the QR token with the authentication app or enter the alphanumeric token in the app.
4. Generate a one-time token using the authentication app.
5. In "Token", enter the one-time token and click "Save".

Administrator: Enable two-factor authentication.

1. In the navigation, select "My Account > Manage authentication > Two-Factor".
2. Click "Enable".
3. Scan the QR token with the authenticator app or enter the alphanumeric token in the app.
4. Generate a one-time token using the authentication app.
5. In "Token", enter the one-time token and click "Save".
6. An additional "backup token" is shown on the page. To generate the backup tokens, click "Generate".
7. A page with 10 backup tokens opens. Store the backup tokens in a safe but accessible location.

4.2.5 Login with OAuth/OpenID

OAuth is an open standard protocol that allows secure authentication of users without sharing their credentials.

Users such as Microsoft Entra ID (formerly Azure AD) can log into the SINEMA RC Server with the OAuth/OpenID Connect protocol without creating the users in the SINEMA RC Server.

For more information, see the application example "Login to SINEMA RC via Microsoft Entra ID" (entry ID: 109974429 (https://support.industry.siemens.com/cs/en/view/109974429))

Requirement

- On SINEMA RC:
  - A valid SINEMA RC IAM license (MLFB 6GK1724-7XG01-0BK0) or trial license is activated.
  - The settings for the application registration server are configured; see section "OAuth/ OpenID settings (Page 121)".
  - OAuth/OpenID is configured; see section "Managing roles and rights (Page 108)".
- On the application registration server:
  - SINEMA RC Server is registered as application (app)
  - The corresponding app roles are present

Procedure

1. Select the "OAuth/OpenID" tab on the SINEMA RC login Web page.
2. Click the button. You configure the text of the button in "OAuth/OpenID settings (Page 121)". The SINEMA RC Server forwards you to the address of the application registration server, where you can log in.
   The application registration server forwards the user with a validity code to the SINEMA RC Server, which converts the validity code to an access token from the application registration server. After the access token is retrieved, the application registration server checks the user and compares it to the defined role policy OAuth/OpenID of the SINEMA RC Server.
   The SINEMA RC Server creates an OAuth/OpenID user, assigns the corresponding roles and then logs this user in.

4.3 Layout of the window

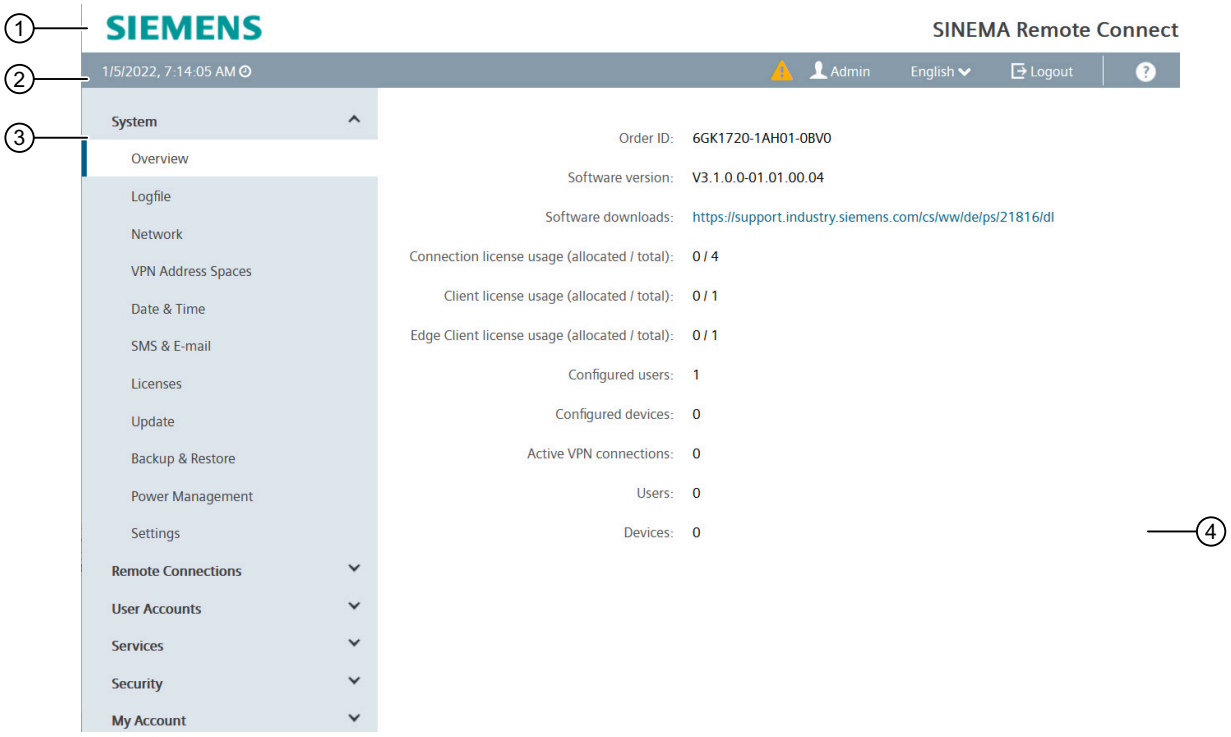
View of the Start page

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



Header area ①

The following is available in the header area:

- Logo of Siemens AG
- Product name

Display area ②

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

- System time and date
  You can change the content of this display with "System > System time".

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

- Display of a message. The message appears when you hover over it with the mouse.
- Display of the user name under which you are logged in.
- Drop-down list for language selection.
  The current language of the WBM is shown.
- **Logout**
  Button for logging out of the WBM. You can log out from any WBM page.
-
  Opens the online help in a new browser window.

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 15)".

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 108)".

  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.
- **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 "F5" function key.

4.5 System

4.5.1 Overview

After logging in to the WBM, the system overview appears. This page contains a configuration overview of the device.

Calling the Web page

In the navigation, select "System > Overview".

Displayed entries

The following entries are displayed:

Field	Meaning
Order ID	Displays the article number of the current software.
Software version	Displays the version number of the current software.
Software download	Shows the link to download the current software version. Clicking this link takes you to the Siemens Industry Online Support page with the current software version. Here you can check whether your software version is up-to-date or download the current version.
Disk Usage	Used memory/total memory
VMWare Tool Version	Displays the version number of the installed VMWare tool.
Configured Layer 2 Connections	Displays the number of Layer 2 connections created in the project.
Connection license usage (allocated / total)	Displays the number of currently active participants and how many participants can be configured in total.
Client standard license usage (allocated / total)	Displays the number of currently active SINEMA RC Client connections and how many client connections are possible in total. **Note** The SINEMA Remote Client 1 license present during the installation cannot be converted to a Floating license.
Client floating license usage (allocated / total)	
Edge client license usage (allocated / total)	Displays the number of currently active Edge client connections and how many client connections are possible in total.
Device license usage (allocated / total)	Displays the number of currently active device connections and how many device connections are possible in total.
Configured users	Displays the number of users created in the project.
Configured devices	Displays the number of devices created in the project.
Active VPN connections	Displays the number of active VPN connections.
Users	Displays the number of active VPN connections to the users created in the project.
Devices	Display the number of active VPN connections to the devices created in the project.

4.5.2 Log

4.5.2.1 Event log

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 "System > Logfile" navigation, select the "Event Log" tab.

Displayed entries

The following entries are displayed:

Field	Meaning
Date	Shows the date and time.
Message level	The following message levels are possible: 1. Emergency 2. Alert 3. Critical 4. Error e.g. when exporting the server certificate fails 5. Warning, e.g. when a CA is deleted 6. Notice, e.g. when a CA is created 7. Info, e.g. when a user has logged on 8. Debug The selected entries and all higher-level entries are displayed. If you select the "Warning" message level, for example, the messages of the levels "Error", "Critical", "Alert" and "Emergency" are also displayed in addition to the messages of the "Warning" level.
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.

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.

To export the log entries, click on the Export button. Navigate to the storage directory and save the current log file in *.csv format. All the entries are exported even if you have filtered the entries.

You can, for example, send the data with a support request.

Note

Protecting exported log files from unauthorized access

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

"Restart" log message

When SINEMA RC Server performs a restart, the same message is always output: `User {user name} rebooting system`.

- System > Power Management > Reboot System
- System > Power Management > Shutdown System
- Configuration changes that force a restart, e.g. Security > General > Global cipher settings

4.5.2.2 User log

On this page, you specify whether the user activities are tracked. To activate tracking, click "Connection tracking active".

Calling the Web page

In the "System > Logfile" navigation, select the "User log" tab.

Displayed entries

The following entries are displayed:

Field	Meaning
User name	Shows the user who accesses the endpoint.
Node	Possible values for the endpoint are as follows: • Device name • Subnet name • Node name with or without IP address • Interface • IP address: When the IP address does not belong to a device or node, the IP address is displayed. Appearance: • Device name.subnet name.node name (IP address) • IP address
Destination port	Shows the port via which the device is accessed.
Protocol	Shows the protocol that was used
Start time	Shows the connection times: • When was the connection started. • When was the connection terminated. • How long did the connection last.
End time	
Duration	
Package counter	Shows the number of packages and the number of bytes that were sent.

Filtering log entries

1. Enter the desired period in the fields "From" / "To".
2. In the drop-down list, select a filter for user or device name.
3. 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.

To export the log entries, click on the Export button. Navigate to the storage directory and save the current log file in *.csv format. All the entries are exported even if you have filtered the entries.

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.

4.5.2.3 Firewall Log

On this page, you can enable the events to be entered in a log file for the firewall. This information may be helpful to you when troubleshooting connection problems through a firewall.

Calling the Web page

In the navigation, select "System > Logfile" and the "Firewall Log" tab.

Displayed entries

Make the following settings. Then click the "Save" button:

Field	Meaning
File name	Shows the file name of the firewall log. The "firewall.log" file name is stored in the system and cannot be changed here. You can rename the file during the export.
Dropped packages	When enabled, information about discarded packets is output.
Allowed connections	When enabled, information about successful connections is output.
Rejected packages	When enabled, information about rejected packages is output.

Exporting Firewall Logs

With the "Export" button, you can download the log file to your PC, for example in order to send it with a support request.

1. Click the "Export" button.
   A dialog to save the current log file opens.
2. Navigate to the directory where you want to save the file and confirm with "Save".

4.5.2.4 Log archives

The log is saved in the log archive

- When the log contains more than one million messages, it is archived. The number is checked every hour.
- When log messages are more than four weeks old.

Calling the Web page

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

Displayed entries

The following entries are displayed:

Field	Meaning
Date (UTC)	Shows the date and time.
Type	The following log types are available: • Event log • User log
Size	Displays the size of the log archive.
Start date (UTC)	Shows when creation of the archive was started.
End date (UTC)	Shows when creation of the archive was ended.
Actions	You can manage log archive entries using the following button: •  Export and save the selected log archive as a file.

Deleting the log archive

1. Select the check box in front of the log archive to be deleted.
2. Click the "Delete" button.

4.5.3 Network

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 61).
  - for HTTPS TCP port 443 (preset, can be changed)
- For the establishment of the OpenVPN tunnel, see OpenVPN settings (Page 140)
  - 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" and the "Interfaces" tab.

Configuring an 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. 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. The maximum size is 1500 bytes. Enter a value ≤ 1 500.
Use DHCP	Enables the assignment of an IP address of the interface via the DHCP server.
IP address	Enter the IPv4 address of the interface. The IP address must be unique. Input is possible when the "Use DHCP" option is disabled.
Network mask	Enter the subnet mask of the subnet you are creating. Input is possible when the "Use DHCP" option is disabled.
Enabling Masquerading	Enables masquerading for a LAN interface.

Additional settings for the WAN interface

Field	Meaning
Setting for IPv4	
Default gateway	When operating a VPN over the Internet, additional IPv4 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 with a fixed IP address	If you select the check box, you can enter the external WAN IPv4 address of the Internet gateway.
WAN IP address	The WAN IPv4 address via which SINEMA RC can be reached. This can, for example, be the WAN IPv4 address of a DSL router via which SINEMA RC is connected to the Internet. Note that the use of NAT IP addresses with "0" in the 4th octet, e.g. 35.157.191.0, is not permitted in SINEMA RC Server. In this case, request a different public/status IP address from your Internet provider.
Settings for IPv6	
Activate IPv6	Also activates IPv6 at the WAN interface.
Use SLAAC for IPv6	Uses Stateless Address Autoconfiguration (SLAAC) for IPv6.
IPv6 address	Enter an IPv6 address of the interface.
Link-local IPv6 address	If "Use SLAAC for IPv6" is activated on the interface, a link local IPv6 address is formed automatically
Subnet prefix length	The IPv6 prefix represents the subnet identifier. Enter the number of left-hand bits belonging to the prefix. Prefixes and IPv6 addresses are specified in the same way as with the CIDR notation (Classless Inter-Domain Routing) for IPv4. Example: 2001:0db8:1234::1111/48
Default gateway	Enter the IPv6 address of the gateway via which this network address is reachable.

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, select "System > Network" 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.
DNS over HTTPS	If enabled, DNS resolution is performed using the HTTPS protocol.
DNS Resolver	A DNS resolver is a program that acts as an interface between DNS clients and DNS servers. It resolves a client request by collecting the requested information from DNS servers and forwarding it to the client.
DNS stamp	The DNS stamp encodes all parameters required to connect to a secure DNS server.

4.5.3.3 Web server

Calling the Web page

In the navigation, select "System > Network" and the "Web Server" 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
HTTPS forwarding port	Specify the port to which the HTTPS request is forwarded.
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
Block Webserver access from WAN interface	When enabled, remote access to the WBM is denied.

Set protocol

Specify the TLS version to be used.

- TLS V1.2
- TLS V1.3
  - Automatic: SINEMA RC checks whether the user equipment uses TLS1.3 or TLS1.2.
  - Disabled: Only TLS1.2 is used.
  - Enabled: Only TLS1.3 is used.

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

4.5.3.4 Ping

On this page, you check with a ping whether a specific device can be reached in the network.

Calling the Web page

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

Set ping

Make the following settings:

Field	Meaning
IP address	Enter the IP address of the device.
Repeat	Enter the number of ping retries.
Timeout	Enter the waiting time within which the ping checks the device.
Ping Output	Shows whether the device can be reached via the specified address.

Click the "Ping" button to start the ping.

Result

Ping sends ping requests to the IP address to be checked and receives responses from the target device, if it can be reached. After the timeout has elapsed, you receive a status message.

4.5.3.5 Static routes

On this page, you define static routes for communication between subnets.

Requirement

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

Calling the Web page

In the navigation, select "System > Network" and the "Static Routes" tab.

Creating static routes

Make the following settings and then click "Save":

Field	Meaning
Destination Network	Enter the network address of the destination that can be reached via this route.
Network mask	Enter the network mask of the destination.
Gateway	Enter the IP address of the gateway via which this network address is reachable.
Interface	Specify the interface via which the network address of the destination is reached.
Description	Filled automatically when the static route is created and can be adapted at any time.

Result

The static route for communication is configured. The route is entered in the following table.

Note

Only the static routes with the LAN interface are forwarded to the devices, unlike those with the WAN interface.

Displayed entries

The following entries are displayed:

Field	Meaning
Destination Network	Shows the destination address of the route.
Network mask	Shows the network mask of the route.
Gateway	Shows the gateway for the route.

Field	Meaning
Interface	Shows the interface of the route.
Description	Shows the description of the route.

4.5.4 Address spaces

4.5.4.1 Virtual Subnet

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 "System > Address Pools > 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.

4.5.4.2 VPN address spaces

You define the VPN 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.
- The maximum possible address space comprises 65535 addresses. The start address of the address space must be selected in such a way that at least two addresses from the address space are used.
- The configured virtual subnets are suggested for the NAT in the devices.

Calling the Web page

In the navigation, select "System > Address Pools".

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 end address is calculated from the network mask and the start address and cannot be configured.
Use (assigned IPs / of total)	The following values are displayed: • Number of assigned IP addresses • Number of available IP addresses
Activate fixed IP 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

4.5.5 Date & Time

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".

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". 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

For time-of-day synchronization via NTP, you 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". The display depends on the language that is set.
Last Synchronization Time	Shows the last synchronization time. • Time in "DD.MM.YYYY HH:MM" format Or • Not synchronized
Network Time Security (NTS)	When enabled, time synchronization is cryptographically secured via NTP.
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 secondary NTP server.

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

4.5.6 SMS messages and e-mails

4.5.6.1 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 sectionMonitoring and time response of wake-up SMS messages (Page 174).

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 173)" 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.

4.5.6.2 E-mail 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

Select the "Enable E-mail client" check box and make the following settings. 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 "Via relay server" method of delivery, the e-mail address of the user account of the respective SMTP relay server is specified.

Additional settings for the "Via relay server" method of delivery

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 server 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.
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 method of delivery. • Binding: The transmission of the e-mail is encrypted via TLS. If the receiving mail server does not support encrypted transfer, the e-mail is not forwarded.
The 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.

4.5.7 Licenses

4.5.7.1 Overview

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

You can also manage the entries with the "Manage licenses (Page 71)" button.

Calling the Web page

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

Displayed entries

Order data

Lists the available licenses and their article numbers.

Active licenses

A list of the existing licenses is displayed:

Field	Meaning
Number	Number of licenses that are currently available and can be used. In this field, you can reduce the number of activated licenses if required. The released licenses are booked back onto the ticket ID.
License type	Name of the license package
Ticket ID	Ticket number used when the license was activated. Switch for showing or hiding the ticket number
Activation date	Date on which the license was activated.
License value	Number of currently active participants / number of activated licenses. The number of activated licenses determines how many participants can be active at the same time.
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	You obtain an overview of the license information. This is also displayed for users with the right "read only".

Releasing the online license

You can release unused licenses or partial licenses in order to activate them on another system, for example.

Note

Before changing systems, you need to release online licenses because they are not included in a backup.

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 or partial license is not used.

Procedure

1. Click on the "Overview" tab.
2. Select the check box for the relevant online license and enter the number of activated licenses, if applicable.
3. Click the "Release license" button.
   The client licenses are released as follows: The number of licenses that are released is the difference between the last value and the current value. The released licenses are booked back onto the ticket ID. The license value is updated.

Result

The licenses are free again and can be activated again on this system or another system.

Reset / Activate

Reset container

If you have a defective license, the license container can be reset with the button. There are no more licenses on the system after the reset. These must be activated again. Only use this button after consultation with the hotline.

Reactivate pending licenses

With this button, you can activate pending licenses.

4.5.7.2 Managing licenses

Calling the Web page

In the navigation, select "System > Licenses > Overview" and click the "Manage licenses" button.

Displayed entries

A list of the existing licenses is displayed on the following tabs:

- Manage Connection Licenses
- Manage Client Licenses
- Manage Edge Client
- Manage Device Licenses

Field	Description	
License type	Name of the license package	
Ticket ID	Total number of available licenses.	
Activation date	Ticket ID used when the license was activated.	
License value	Number of currently active participants / number of activated licenses. The number of activated licenses determines how many participants can be active at the same time.	
Actions		You obtain an overview of the license information. This is also displayed for users with the right "read only".

Releasing blocked licenses

Example

The following licenses are available on the SINEMA RC Server:

- SINEMA Remote Connect 64
  The license is used by 64 participants.
- SINEMA Remote Connect 256
  No license is used.

The SINEMA Remote Connect 64 license should be used on a different server. As long as the participants are active, the license is blocked and cannot be released.

Procedure

1. Click on the "Overview" tab.
2. Click the "Manage licenses" button.
3. You can transfer the license value of one blocked license to another on the "Manage Connection Licenses" page.
4. Select both licenses in the table.
   Number of the first license that can be transferred to the second license or vice versa.

First License		Second License
64/64		0/256

5. Click "Save".

Result

First License		Second License
0/64		64/256

Choose the SINEMA Remote Connect 64 license on the "Overview" tab and click the "Loose License" button.

Converting client standard licenses into floating license

You can convert three client standard licenses that are not in use into one floating license.

Requirements

- The licenses are not in use.

Procedure

1. Click on the "Overview" tab.
2. Click the "Manage licenses" button.

3. On the "Manage Floating Licenses" page, you specify whether client standard licenses are converted into floating licenses.

Field	Description	
License type	The following license types are available: • Standard: Client standard licenses • Floating: Floating license	
Total	Total number of available licenses.	
Available	Number of licenses currently not in use.	
To be converted	Number of client standard licenses that can be converted into floating licenses and vice versa.	
		Converts client standard licenses into floating licenses.
		Converts floating licenses into client standard licenses.

4. Click "Save".

Result

The licenses are converted.

Note

Backing up & restoring floating licenses

The setting of the floating licenses is stored in the backup copies. If the licenses are activated again after importing the backup copy, the floating licenses must be restored. To do so, click the "Restore" button.

If there are not enough client standard licenses or only test licenses available on the system, no floating license can be restored. A logbook entry is made in these cases.

On the "Client Licenses" page, you receive an overview of client logins. You can also manage these entries.

For connections from two SINEMA RC Clients, you need the SINEMA RC Client license (MLFB 6GK1721-1XG03-0AA0 or 6GK1721-1XG03-0AK0 for OSD).

Calling the Web page

In the "System > Licenses" navigation, select the "Client licenses" tab.

Client standard licenses

With "Client standard license usage (allocated / total)", the number of currently active SINEMA RC Client connections and the number of client connections that are possible in total is displayed.

Field	Meaning
Client system ID	Shows the client system ID on the server.
Client device name	Shows the PC name from which the client logged into the server.

Field	Meaning
Last login	Shows the time stamp of the client login with the date and time.
Last logged in user	Shows the name of the user who was logged in last.

To delete a table entry, select the check box in front of the entry to be deleted and click the "Delete" button. A license can be released in this way.

Floating licenses

With "Client floating license usage (allocated / total)", the number of currently active connections is displayed and how many connections are possible in total.

Note

SINEMA Remote Connect 4

The SINEMA Remote Client 1 license present during the installation cannot be converted to a Floating license.

Field	Meaning
Client system ID	Shows the client system ID on the server.
Client device name	Shows the PC name from which the client logged into the server.
Status	Displays the status. • - : Status unknown • Connected: A connection is established. • Not connected: There is no connection.
Last logged in user	Shows the name of the user who was logged in last.
Show History	Opens the "Client Floating License History"

4.5.7.3 Device license

In the "Device License" tab, you can see an overview of device logins.

For connections, you need the license (6GK1724-5XG01-0BK0).

Calling the Web page

In the "System > Licenses" navigation, select the "Device Licenses" tab.

Displayed entries

Field	Meaning
Device system ID	Shows the system ID of the device on the server.
Last login	Shows the time stamp of the client login with the date and time.
Last connected device	Shows the name of the device that last established the connection to the server.

4.5.7.4 Edge Client

In the "Edge Client" tab, you can see an overview of client logins.

For connections, you need the SINEMA RC Edge Client OSD (6GK1721-4XG01-0BK0) license.

Calling the Web page

In the "System > Licenses" navigation, select the "Edge client" tab.

Displayed entries

The Edge client logins overview is displayed:

Field	Meaning
Edge client system ID	Shows the system ID of the Edge client on the server.
Edge client device name	Shows the name from which the Edge Client has logged in to the server.
Last login	Shows the time stamp of the client login with the date and time.
Last connected device	Shows the name of the user that last established the connection from the Edge Client to the server.

4.5.7.5 Online Licenses

On this page, you can activate online license packages.

Calling the Web page

In the navigation, select "System > Licenses" and the "Online License" tab.

Online license activation

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. Enter the ticket ID belonging to the online license.
2. Click the "Check License" button.
   The system checks whether the ticket ID is valid and which license package it activates. After a successful check, the license type and the license value are displayed. The license value shows the number of available licenses.
3. In addition with client licenses: Enter the number of licenses to be activated in the "Number" field.
4. Click the "Activate license" button to confirm the activation of the online license.
   The license value in the overview table is updated to the number of licenses activated in this step.

Result

The license is activated and is displayed on the "Overview" tab.

To deactivate online licenses, change the number of activated licenses on the "Overview (Page 69)" tab.

4.5.7.6 Offline Licenses

On this page, you can activate new offline license packages and deactivate existing licenses.

Calling the Web page

In the navigation, select "System > Licenses" and the "Offline License" tab.

Activate offline license

To enable an offline license, do the following:

1. Click on the "Export License Container" button.
2. Navigate to the storage directory where the file "sinemarc.WibuCmRaC" is stored.
3. Contact Customer Support via:
   Support Request (https://support.industry.siemens.com/cs/my?lc=en-US)
   - Create a new support request.
     Enter "SINEMA License" in the search bar and select the "Licensing/Authorization" check box.
   - Click "Search". Under "Authorization", select the "SINEMA License" check box and click "Next".
   - Fill in the "Problem description" form.
   - Provide the ticket ID of the license package and attach the file "sinemarc.WibuCmRaC".
   - Click "Next".
   - Enter your contact data and click "Send".
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 "Choose file" button.
6. Navigate to the storage directory and select the "sinemarc.WibuCmRaU" 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.

Note

With offline activation, all licenses are always activated. Specification of the number to be activated is not possible.

Releasing the offline license

To release an offline license, do the following:

1. Contact Customer Support by e-mail (support.automation@siemens.com).
   Enter the "SINEMA License" keyword in the subject line. Include the ticket ID of the license package to be activated in the e-mail.
   You can also contact Customer Support using a Support Request or by telephone; see the procedure for "Offline license activation".
2. Select the required offline license.
3. Click the "Release license" button.

Result

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

4.5.8 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

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.

You will find a SHA256 hash value in the update file. With this, you can check whether the file was downloaded unchanged. To check this, you calculate the hash value of the downloaded file and compare it with the value specified on the download page.

The update must be performed in the correct order:
V1.0 > V1.1 > V1.2 > V1.3 > V2.0 > V2.1 > V3.0 > V3.1 > 3.2

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.

Note

System Update V2.0 > V2.1

Before you update the software version, you need to release the licenses for "SINEMA RC (2.0)" and reactivate them in server version V2.1. The procedure is described in the section "System Update V2.0 > V2.1 (Page 166)".

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 has been downloaded. The update file has the format *.tar.gz.
- The user has access to the storage directory.

System update

Procedure

1. Click the "Choose 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 is 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.

Note

Functions after system update

We recommend that you restore the connection to all clients after the SINEMA RC server system update. This ensures that the functions are working as intended.

4.5.9 Backing up & restoring

4.5.9.1 Backup copies

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 159)".
- On the Internet under the following entry ID: 109748144 (https://support.industry.siemens.com/cs/cn/en/view/109748144)

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	
ID	Consecutive number	
Date (UTC)	Date on 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.	
Version	The backup copy was created with this SINEMA RC version.	
Actions		For this action, you require the user right "Restore the system". SINEMA RC Server takes specific settings from the selected backup copy and continues working with these, see section "Restoring settings".
		Exporting and saving the selected backup copy as a file (*.backup).

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:

- Log messages
- Backup copy
- Boot partition settings
- Client software
- Firmware files for updating the devices

Importing the backup

Note

Make sure that you only load backups from trusted sources.

Store the coding key carefully and protect it from unauthorized access.

Requirement

- The user has been assigned the "Restore System" right.

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 "Select file" button.
4. Select the required file in the format *.backup and confirm your selection with the "Open" button.
5. Click the "Finish" button.
6. For "Password", enter the coding key of the selected backup copy.
7. 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.

After the import, the password is applied as new coding key by SINEMA RC.

All settings made up to this point that have not been saved in a backup copy are lost.

Note

Partial restore from backups

During the partial restore of a backup, the settings for the LAN interfaces are not restored, as this would be a system change.

After a partial restore, check the group settings of the LAN devices.

Restoring settings

Requirement

- The user has been assigned the "Restore System" right.

This action applies specific system settings from the selected backup copy.

1. Click on the  icon.
   A new page opens.
2. Specify which settings of the selected backup copy are applied.

Setting	Description
All	Applies all settings and continues working with them. All settings made up to this point that have not been saved in a backup copy are lost.
Devices & Users	For backup files V3.1 and higher Applies the settings for devices and users.
Devices, Users & Groups	For backup files V3.1 and higher Applies the settings for devices, users and groups.
Restore fallback certificate	Available with "Devices & Users" and "Devices, Users & Groups" Also accepts the fallback certificate

3. Click the "Restore" button.

Delete backup copy

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

1. Select the check box in front of the entry to be deleted.
2. Click the "Delete backup copy" button.

Result

The selected backup copy has been deleted.

Licenses in the backup file

If the backup contains licenses, the DNS settings are also restored. The system attempts to activate each individual license (ticket number) in the database.

- Activation successful:
  The users, devices and client license information are restored.
- Activation not successful:
  The system settings are restored, but instead of the license a "14-day test license" is created in the quantity of the missing licenses. To reactivate this, you need to activate valid licenses in the quantity of the test license.
  - Activation after 14 days:
    After 14 days, the test licenses are deleted and all users and devices are disabled. After the activation of valid licenses, you need to enable the uses and devices manually.
  - Activation within 14 days:
    All users and devices remain enabled. The test licenses are deleted.

  Example 1:
  The backup contains the following licenses that cannot be activated:
  - 1 x SINEMA Remote Connect 64 license
  - 25 x SINEMA RC Client V3 licenses

  After the restore, the license overview contains a 14-day test license for 64 connections and one test license for 25 client connections. Activate valid licenses within 14 days.
  Example 2:
  The backup contains the following:
  - 2 x SINEMA Remote Connect 64 licenses: One license can be activated, the other cannot.
  - 70 configured connections

  After the restore, the license overview contains an activated license for 64 connections and one 14-day test license for 64 connections. For 64 configured
  connections, the activated license is sufficient. The 14-day license is valid for six configured connections. Activate a valid SINEMA Remote Connect 64 license before the 14 days elapse.

4.5.9.2 Settings

Use this page to set the settings for the backup copies.

Calling the Web page

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

Displayed entries

In the "Settings" tab, you configure data for the backup copy:

Field	Meaning
Maximum number of local backup copies	Maximum number of local backup copies allowed An entry between 10 and 30 is permitted. When the maximum number is reached, the oldest backup copy is overwritten.
Automatic backup interval	Enables automatic backup if the system is to be backed up at regular intervals. The following entries are possible: • Disabled • Daily • Every Sunday • Every Saturday • Every first day of the month
Automatic backup time (UTC)	Time information for automatic saving
Coding key	Coding key for encrypting a backup copy The coding key must be have at least 8 characters and include special characters, uppercase and lowercase characters as well as numbers; refer to the section "Permitted characters (Page 28)". **Note:** Store the coding key carefully and protect it from unauthorized access.
Confirm coding key	The coding key must be entered twice.

Configuring settings for backup copies

Requirement

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

Procedure

1. Enter the number of permitted backup copies.
2. Select the suitable entry in the "Automatic backup interval" drop-down list to create backup copies automatically.
3. Enter the time for the automatic backup.
4. Enter a "Coding key" with which the backup copy is encrypted.
5. Confirm the "Coding key".
6. Click the "Save" button.

4.5.10 Power Management

4.5.10.1 Power Management

The system can be restarted or shut down on this page. You can also define a boot partition for the restart.

Calling the Web page

In the navigation, select "System > Power Management".

Power management

The system can be restarted or shut down using the following buttons:

- Restart system
- System shutdown

4.5.10.2 Boot Partition

This page is available as of version 3.0 and shows the currently installed SINEMA RC server version. As of version 3.0, the two most recently installed SINEMA RC server versions are always available: the current version and the previous version. The previous version serves as a backup copy.

Calling the Web page

In the navigation, select "System > Power Management > Boot Partition".

Defining the Boot Partition

1. Click on the check box for the version with which the operating system should start.
2. Save your selection with "Save".

Result

The selected partition is started after the next system restart.

4.5.11 Settings

4.5.11.1 Server Information

On this page, you can create your own information text which is displayed on the SINEMA RC server login screen.

Calling the Web page

Select "System > Settings > Server Information" in the navigation.

Requirement

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

Creating a server information text

1. Select the check box "Show server information text on login screen".
2. Enter the text and confirm your entry with "Save". The text can be up to a maximum of 250 characters long.
   The text is displayed above the login screen of the SINEMA RC server. This text is displayed in the server info box on the SINEMA RC Client.

When you select the "Show server information text on server header" check box, this text is shown in the header of the server.

4.5.11.2 Auto Logout

You can define the session time on this page.

Calling the Web page

Select "System > Settings > Auto Logout" in the navigation.

Requirement

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

Setting the time interval

1. Enter the time in minutes. The entered value must be between 1 and 60.
2. Confirm the entry with "Save".
   After the time expires, the server ends the session when there is no activity.

4.5.11.3 Restore factory defaults

The page allows you to restore the factory settings of the SINEMA RC server which it had when first installed.

Note

Releasing licenses

When resetting, the licenses are also deleted. Release the licenses before resetting the system.

Calling the Web page

Select "System > Setting > Restore Factory Defaults" in the navigation.

Reset SINEMA RC

1. Enter the password of the system administrator.
2. If you enable the "Delete inactive boot partitions" setting, these will be deleted.
3. Click the "Reset system" button.
4. If you really want to reset the system, click the "Yes, reset system" button.
   All data will be removed from the system (except for the WAN IP address). The reset may take some time.
   After that, you will be redirected to the login page.
5. After the new installation log on as user name and password "admin".

4.6 Remote Connections

4.6.1 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 above the table 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 99)").

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 has been assigned the right "Manage devices".

Calling the Web page

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

Displayed entries

Field	Meaning	
Device name	Shows the device name.	
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.	
Subnet name	Shows the subnet name.	
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 89)". If several IP addresses are created, they are displayed one under the other.	
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 89)". If several IP addresses are created, they are displayed one under the other.	
Node address	The IP address of the node	
Node virtual address	The virtual IP address of the node.	
Status	Online	The device is connected to SINEMA RC server via VPN.
	Offline	The device is not connected to SINEMA RC server via VPN.
	Disabled	The device is disabled.
Last login	Indicates when the device was last logged in.	
Date of the last autoconfiguration	Shows when the autoconfiguration file is from.	
Fallback certificate fingerprint	Shows the fingerprint used by the fallback certificate.	
Fallback port	When reachable, the used fallback port is shown.	
Fallback status	⇌	The device has not yet sent a request for configuration or has a different configuration.
	⇌	A response to automatic configuration was sent to the device but the device has not yet confirmed it.
	⇌	The device confirms that the fallback information was updated and the fallback port can be reached.
Location	Location of the device. This can, for example, be the installation location of the device.	
Type of connection	Shows how the VPN connection will be established.	
Device type	Shows the type designation of the device.	
Vendor	Displays the manufacturer of the device.	
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.	
Phone number	Only for M800 Mobile, RTU 303xC, RM1224 Shows the call number of the end device to which the wake-up SMS is sent.	

Field	Meaning	
Layer 2 configuration	Shows whether the Layer 2 function is configured and whether the configuration is correct. You configure Layer 2 under "Layer 2".	
		Layer 2 is disabled on the SINEMA RC server and the device.
		Layer 2 is only enabled on the SINEMA RC server.
		Layer 2 is enabled only on the device.
		Layer 2 is enabled on the SINEMA RC server and the device.
		VPN tunnel is online
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 node.
		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 node. When the password is queried, enter the password you specified when you created the device (refer to the section "Creating a new device (Page 89)").
		The certificate and the key are stored as Base64-coded ASCII text.
		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. • Only with RTU 303xC: For RTUs, you can also add a wake-up SMS message with a specified deadline. At exactly the time you send with the SMS message, the RTU establishes a connection to its communication partner. When you click on the action, the "Choose Wake-up time" dialog opens. – Wake-up at Selected Time: The RTU sends the SMS message at the selected time. – Wake up now: The RTU sends the SMS message immediately.

Creating a device

Click the "Create" button and configure the required settings, see Creating a new device (Page 89).

Filtering entries

1. Select an entry in "Search filter".
2. Enter a search term or part of the search term in the search box.
3. To limit the search further, select the "Precise match" check box.
   When this is selected, case is taken into account and the entire search word is searched for. The search results will match the entered search term exactly.
4. 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

Dedicated access

You can explicitly configure access to subnets or nodes of a device (e.g. SCALANCE SC-600). In addition, you can allow access only over specific ports, e.g. SSH via TCP port 21.

For this purpose, users, devices, nodes, subnets and port groups are combined in participant groups (Page 99).

Access level	
All access	All users that are also members of this participant group have access to the subnets and nodes accessible via the device. Device > All access
Device access	All users that are also members of this participant group can only access the device itself. Access to the subnets or node connected to the device is not possible. Device settings > Device

Access level	
Subnet-specific access	One or more subnets that can be reached via the device are assigned to a participant group. All users that are also members of this participant group only have access to the nodes that are in this internal subnet of the device. • Network setting > Subnet: Participant group One or more ports are assigned to a participant group. All users that are also members of this participant group only have access via these ports to the nodes that are in this internal subnet of the device. • Network setting > Subnet: Participant group > Port group: Participant group
Device-specific access	Specific nodes are assigned to a participant group within the subnet. All users that are also members of this participant group only have access to these nodes. • Network setting > Subnet: Participant group > Node: Participant group One or more ports are assigned to a participant group. All users that are also members of this participant group only have access to these nodes via these ports. • Network setting > Subnet: Participant group > Node: Participant group > Port group: Participant group

You can find additional information on dedicated access on the Internet with the following entry ID: 109765714 (https://support.industry.siemens.com/cs/ww/en/view/109765714)

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 > Devices".

Procedure

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

Field	Meaning
Device name	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 your device type is not shown 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".
Phone 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 the 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.
Type of connection	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 30XXC) 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.
Layer-2 network	If the option is enabled, a Layer 2 connection can be established to the end device. Only the Layer-2 networks configured under "Layer 2 > Connection" can be selected. If the device already has a local Layer 2 configuration, this is retained and the setting is ignored by SINEMA RC.
Request VPN address	When this option is 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: System > VPN address spaces > OpenVPN • IPsec: System > VPN 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 profile	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 device (including its subnets and the nodes contained) is now a member of this participant group. The users that are also members of this participant group have access to the subnets and nodes accessible via the device.
   You can assign one or more participant groups. Select the desired user group and click on the "Add" button. To delete, click on ⊖.
6. Configure **device access** (device-specific access).
   The members of this participant group can only access the device itself. Access to subnets or nodes that are connected to the device is not possible.
   You can assign one or more participant groups.
   Select the desired user group and click on the "Add" button. To delete, click on ⊖.
7. If you do not need any further network settings,
   – (Without Layer 2 support) click the "Quick Finish" button.
   – (With Layer 2 support) click the "Quick Finish Layer2" button.

   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 24)".

On this page, you define the subnets and nodes that can be reached via the device and who can access them. This function is also known as "Dedicated Device Access" (DDA for short).

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. Only the configured nodes are reachable.

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 "Port group name" and click "Add".
The "Port group [name]" area is created in the "Subnet" area. To delete, click on ⊖.

Field	Meaning
Port group name	Displays the name you assigned.
Allow ICMP	ICMP is blocked by default. Allows ICMP, e.g. ping
Filtering port	Specify which protocols can access the configured subnet via which ports.
Participant groups	Select the participant group that has access to the port group and click the "Add" button. You can assign one or more participant groups. To delete, click on ⊖.

7. Enter a unique name for "Node name" and click "Add".
The "Node [node name]" area is created. To delete, click on ⊖.
8. 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	Virtual IP address of the node. The IP address must be in the configured virtual subnet.
Participant groups	Select the participant group that has access to the node and click "Add". You can assign one or more participant groups. To delete, click on ⊖.

9. Enter a unique name for "Port group name" and click "Add".
The "Port group [name]" area is created in the "Node" area. To delete, click on ⊖.

10. Configure the port group:

Field	Meaning
Port group name	Displays the name you assigned.
Allow ICMP	ICMP is blocked by default. Allows ICMP, e.g. ping
Filtering port	Specify which protocols can access the configured node via which ports.
Participant groups	Select the participant group that has access to the port group and click the "Add" button. You can assign one or more participant groups. To delete, click on .

11. 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 overwritten 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

4.6.2 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	
Device name	Shows the device name.	
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.
		Offline: The device is not connected to SINEMA RC Server via VPN.
	Disabled	The device is disabled.
Location		Information on the device location
Comment		Enter a brief description as comment.
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 "Choose file" button.

3. Navigate to the storage directory and select the update file (*.swf). Confirm your selection with the "Open" button.
   You can upload a firmware for each of the SCALANCE devices M800/S600/MUM85x and SC600. If a firmware has already been imported and another firmware is being uploaded, the existing file is overwritten.
4. Click the "Import" button.
5. Click on the "Devices" tab.
6. Select the devices to be updated.
7. Click the "Save" button.

Result:

- Create a configuration backup before saving on the device.
- After saving, the SINEMA RC Server sends the request to the device to load the new firmware.
  The request to the device to load firmware depends on the "Automatic Registration Interval" parameter on the remote device. The device downloads the firmware and restarts. The device is not reachable during this time.

  Note

  Firmware downgrade

  If a firmware version that is older than the installed version is loaded (downgrade), this may result in the factory settings being restored. The device then can no longer connect to the SINEMA RC.

- The current firmware version is entered in the table under "Last known firmware version".
- Each device update is documented in the "Logfile messages" under "System > Logfile".
- It is not logged whether the device successfully requested the firmware. You can check whether the firmware was updated in "Last Known Firmware Version" on the page "Remote Connect > Device Update > Devices".

4.7 Local connections

On this page, you define the local networks and nodes that can be reached via the LAN interface and who can access them. This function is also known as "DDA for static routes".

Note

Routing between LAN interfaces

Routing between the LAN interfaces of the SINEMA Remote Connect servers is possible with the "DDA for static routes" function but not recommended for security reasons.

Note: The function does not represent an adequate replacement for a separate router in the network.

Procedure

1. Select the LAN interface.
2. Configure the group settings:

Field	Meaning
Participant groups	Select the participant group that has access to the destination network and click the "Add" button. You can assign one or more participant groups. To delete, click on ⊖.
Destination Network	Enter the destination network.

3. Configure the subnet that can be reached directly via the interface.

Field	Meaning
Subnet IP	Enter the IPv4 address of the subnet that is accessible via the local interface.
Subnet mask	Specify the network mask of the subnet.
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 ⊖.

4. Enter a unique name for "Node name" and click "Add".
5. 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.
Participant groups	Select the participant group that has access to the node and click "Add". You can assign one or more participant groups. To delete, click on ⊖.

6. Click the "Save" button.

4.8 Connection Management

4.8.1 Participant groups

Users, devices, nodes 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 (Page 101) between the groups.

Requirement for creating participant groups

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

Calling the Web page

In the navigation, select "Connection Management > 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	
Users	Number of users assigned to the participant group. When you click on the number, the Users (Page 107) overview page opens.	
Devices (All access)	Number of devices assigned to the participant group. The users that are also members of this participant group have access to the subnets and nodes accessible via the device. When you click on the number, the Devices (Page 86) overview page opens.	
Devices (Device access)	Number of devices assigned to the participant group. The users that are also members of this participant group only have access to these nodes. When you click on the number, the Devices (Page 86) overview page opens.	
Remote subnets	Number of subnets assigned to the group. When you click on the number, the Devices (Page 86) overview page opens.	
Remote nodes	Number of nodes assigned to the group. When you click on the number, the Devices (Page 86) overview page opens.	
Local connections	Participant group whose members can access the local subnet. When you click on the number, the local connections (Page 98) overview page opens.	
Local subnets	Number of configured subnets that are accessible via the local interface. When you click on the number, the local connections (Page 98) overview page opens.	
Local nodes	Number of nodes in the local subnet. When you click on the number, the local connections (Page 98) overview page opens.	
Roles	Number of roles assigned to the group. When you click on the number, the Roles (Page 108) overview page opens.	
Destination group	Names of the destination groups whose members are allowed to communicate with the members of this participant group.	
Actions		Open member list. In the list, all the devices and users belonging to the participant group and their status (online or offline) are displayed.
		Click on the icon to change the settings for the participant groups.
		Click the icon to manage the communication relationships (Page 101) of the participants.

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.

4.8.2 Specifying communications relations between node groups

On the "Connection Management > Participant Groups" page, you can manage the communication relationships between the participant groups with ⇄.

Requirement

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

Creating communication relations between the participant groups

1. Click on the ⇄ icon in the overview of participant groups.
   The participant groups that have already been created are displayed.
2. Select the source group.

3. Define the destination groups to which connections are allowed from the source group.
4. 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. Click on the icon. Change the corresponding communication relationships.
2. Then click the "Save" button.

Result

The communication between the participant groups is updated.

Filtering entries

1. Enter a name or part of the name in the search box.
2. 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.

4.8.3 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.

4.9 Layer 2

4.9.1 Connections

4.9.1.1 Networks

On this page, you specify the Layer 2 network. Communication between the Layer 2 networks is not possible.

Requirement for changing the Layer 2 network

- The user has the "Manage Layer 2" or "Manage Own Layer 2" right.
  With these rights, all Layer 2 networks and the number of assigned devices are displayed. This user can create Layer 2 networks and also delete them.
- To be able to use this function, you need the SINEMA RC Layer 2 Connection License (MLFB 6GK1724-6XG01-0BK0).
  You can test the function for free for a period of 14 days. For this purpose, you need to activate the trial license.

Calling the Web page

Select "Layer 2 > Connections > Network" in the navigation.

Creating a Layer 2 network

1. Enter a network name.
2. Specify the endpoint type.
   - SRC server disabled: Layer 2 communication takes place on the SCALANCE device.
   - SRC server enabled: Layer 2 communication takes place via the SINEMA RC server.
3. Click "Add".
   The Layer 2 network is included in the list.

Deleting a Layer 2 network

1. Select the required Layer 2 network.
2. Click "Delete".
   Layer 2 networks can only be deleted if no device is assigned to them; otherwise, the check box is grayed out

Displayed entries

Field	Meaning	
Network name	Name of the Layer 2 network Permitted characters: **0-9, a-z**, **A-Z**,+ **_** Names not allowed: **conn**	
Assigned devices	Number of devices assigned to the Layer 2 network. When you click on the number, the Devices (Page 104) overview page opens.	
Assigned users	Number of users assigned to Layer 2 network. When you click on the number, the Users overview page opens.	
Endpoint type	• SRC server: Layer 2 communication via the SRC server • Device: Layer 2 communication takes place on the SCALANCE devices	
Actions		Open the Layer 2 member list. Users and devices that are assigned to the Layer 2 network are shown in the member list.
		Only available for the "Device" endpoint type Edit settings of the Layer-2 member list

4.9.1.2 Devices

Requirement

- The user has the "Manage Layer 2" or "Manage Own Layer 2" right.
  With these rights, all Layer 2 networks and the number of assigned devices are displayed. This user can create Layer 2 networks and also delete them.
- To be able to use this function, you need the SINEMA RC Layer 2 Connection License (MLFB 6GK1724-6XG01-0BK0).
  You can test the function for free for a period of 14 days. For this purpose, you need to activate the trial license.

Calling the Web page

Select "Layer 2 > Connection > Devices" in the navigation.

Displayed values

Field	Description	
Device	Device assigned to a Layer-2 network. The settings are divided by devices, which are collapsible > and expandable ⌄ for clarity.	
Layer 2 configuration	Indicates the status of the Layer 2 configuration	
	⇌	Layer 2 is disabled on the SINEMA RC server and the device.
	⇌	Layer 2 is only enabled on the SINEMA RC server.
	⇌	Layer 2 is enabled only on the device.
	⇌	Layer 2 is enabled on the SINEMA RC server and the device.
	⇌	VPN tunnel is online
Actions	DCP Discovery	Searches for the end devices that can be reached via the device. The end devices are listed under "Discovered nodes". If the user has only group rights, the user can see only the devices that are in the same group as the user. The button is only displayed when the VPN tunnel is online.
	Update	Only available when the "DCP Auto Scan" entry is present under "Discovered nodes".

Allow access to the discovered end devices

1. The end devices are listed that can be reached via the device.

Field	Description
Node name	End device name
IP Address	End device IP address
MAC address	End device MAC address
PROFINET device name	If available, the configured PROFINET device name is displayed.
PROFINET device type	PROFINET device type of the end device

2. Select the desired end device.
3. Under "Group", specify the participant group. Via the groups, access within the network can be set.
4. If necessary, enter a comment.
5. Click "Allow".

Result

The end device is listed under "Allowed communication".

The members of this participant group can access this end device.

In "Scan result", all nodes found are listed automatically under "Allowed communication". The last scan time is shown in the comment.

The MAC address appears in the found nodes when you hover with the mouse over "*" in the "MAC" column.

4.9.1.3 Settings

On this page, you enable Layer 2 support on the SINEMA RC server.

Requirement

- The user has the "Manage Layer 2" or "Manage Own Layer 2" right.
  With these rights, all Layer 2 networks and the number of assigned devices are displayed. This user can create Layer 2 networks and also delete them.
- To be able to use this function, you need the SINEMA RC Layer 2 Connection License (MLFB 6GK1724-6XG01-0BK0).
  You can test the function for free for a period of 14 days. For this purpose, you need to activate the trial license.

Calling the Web page

Select "Layer 2 > Connections > Settings" in the navigation.

Activate Layer 2

1. Select the "Enable Layer 2" check box.
2. Make the following setting for the "Network ID (VNI)":

Field	Meaning
VNI start ID	The identifier that is automatically assigned to the Layer 2 network. You configure the Layer 2 network under "Layer 2 > Connections > Network". Default setting: 1000000
VNI port	The port that is used for the Layer 2 connection.

3. The MAC address that is used for the Layer 2 interface is shown under "User client MAC address".
4. Click "Save" to save the settings.

4.10 User Accounts

4.10.1 Users & Roles

4.10.1.1 Overview of the user accounts

Requirement for creating and changing users

The user has been 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.

Field	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 "Create a new user (Page 115)".	
User ID	The user ID is created automatically when the user is created.	
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	
Last name	Last name of the user	
Account created	Date and time at which this user account was created	
Last login	Date and time of the last login	
Roles	Shows which roles are assigned to the user.	
Local Password Policy	Displays the password policy used. You set the password policy when you create a role, see "Manage roles and rights".	
2FA	Shows whether 2-factor authentication is enabled. You make the setting when you create a role; see "Managing roles and rights".	
Status	Online	The user is logged on to SINEMA RC.
	Offline	The user is not logged on to SINEMA RC.
	Disabled	The user is disabled.
VPN protocol	Shows which protocol is being used for the VPN connection.	
Email	Email address of the user	

Field	Meaning	
Layer 2 Configuration	Shows whether the Layer 2 function is configured and whether the configuration is correct. You configure Layer 2 under "Layer 2".	
Session policy	Shows whether the session policy is enabled. You make the setting when you create a role; see "Managing roles and rights".	
Actions		Layer 2 is disabled on the SINEMA RC server and the user.
		Layer 2 is only enabled on the SINEMA RC server.
		Layer 2 is only enabled for the user.
		Layer 2 is enabled on the SINEMA RC server and the user.
		VPN tunnel is online

Filtering entries

1. Select an entry in the "Search filter" pop-up menu.
2. Enter a search term or part of the search term in the search box.
3. To limit the search further, select the "Precise match" check box.
   When this is selected, case is taken into account and the entire search word is searched for. The search results will match the entered search term exactly.
4. 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

Managing roles and rights (Page 108)

4.10.1.2 Managing roles and rights

Requirement for creating roles

The user has been assigned the right "Manage users and roles".

Displayed entries

A list of the created roles is displayed.

Field	Meaning	Calling the Web page
Role name	Name of the role	-

Field		Meaning	Calling the Web page
Global rights	Manage address spaces	Edit parameters of the address spaces	Remote connections > Address spaces
	Create backup copies	Create, delete and export a backup copy	System > Backup & Restore
	Restore System	Restore the system based on the saved system file	System > Backup & Restore
	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 firmware updates	Load the update file with the new firmware onto the device and start the update process	System > Devices-Update
	Manage devices	Create new devices; edit and delete devices already created; create, delete and edit participant groups; assign devices; create and download configuration file with VPN settings for the device.	Remote connections > Devices
	Manage remote connections	Define communication relations: Communication between participants within a participant group and participant groups with one another	Remote connections > Participant groups Remote connections > Communication relations
	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	
	Certificate management	Create new CA certificates and server certificates; edit and delete existing certificates	Security > Certificates
	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
	Download client software	Download SINEMA RC Client software	User accounts > Client Software
	Password policy	Guideline for the assignment of passwords	User accounts > Users and roles Create new roles: Password policy
	Session policy	Policy for session duration	User accounts > Users and roles Create new roles: Session policy
	2FA	Shows whether TOTP-based two-factor authentication is enabled.	User accounts > Users and roles

Field		Meaning	Calling the Web page
			Create new roles: Password Policy > Enable Two-Factor Authentication
	PKI policy	Guideline for the PKI certificate	User accounts > Users and roles Create new roles: PKI policy
	UMC policy	Shows whether access to the UMC is activated or not	User accounts > Users and roles Create new roles: UMC policy
	OAuth/OpenID policy	Shows whether access to the authorization server is activated or not.	User accounts > Users and roles Create new roles: OAuth/ OpenID policy
	View log file message	Log messages can be viewed and exported.	System > Log file
	Full access read only	Can access the entire system read-only.	
	Manage Layer 2	Can configure Layer 2 connections.	Layer 2 > Connections
Group rights (Bound to the participant group)	Manage own devices	With group rights, the user can see and manage only the devices, users, remote connections and LANs that are in the same participant group as the user. For devices, the user must have "All access" to the device.	
	Manage own remote connections		
	Manage own users		
	Manage own Layer 2		
Action		 Edit settings of the role	

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. Activate the relevant group memberships. Click the "Next" button.

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 users (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. If this role is to be activated for UMC logins, select the "Activated" check box and define the following settings:

Field	Description
UMC user group	Enter the name of the UMC user group. The entered name should match the name on the UMC server. If the name contains the < > & " symbols, they are shown in SINEMA RC as < > & ". Login with these symbols is possible.
Delete temporary users (in hours)	• 1 - 9999 hours: When the time expires, the temporary user is deleted.

8. If this role is to be activated for OAuth/OpenID logins, select the "Activated" check box and define the following settings:

Field	Description
Key in claim	Claims are key-value pairs contained in tokens that transmit role information. With Microsoft Entra ID, this is the key "roles". With other application registration servers, the key is user-defined. The entry must match the entry on the application registration server.
Value in claim	The role name created on the application registration server. You can assign one or more key-value pairs.
	You obtain an overview of the available claims, provided the claims available on the application registration server were retrieved. You retrieve the available claims under "Services > OAuth/OpenID > Claims > Get claims".
Relationship between claims	Defines the relationship between claims. • AND: The specified claims must be fulfilled. • OR: At least one of the specified clients must be fulfilled.
Delete temporary users (in days)	• 1 - 9999 days: When the time expires, the temporary user is deleted.

9. Define policies for the session. The session policy defines how long a user must be connected to the SINEMA RC Client
before needing to log in again.

Field	Description
Access token timeout (min)	Specifies the validity of the new access token in minutes. After this has expired, a new access token is requested from the authorization server via the update token.
Session never expires	If enabled, the session never expires.
Update token timeout (hour)	Specifies whether the update token expires after a certain period. If the update token expires, the session between the server and the client is ended. The client is forced to log out and log in again with the credentials in order to receive a new access and update token pair.

10. Specify the local password policy:

Area	Field	Description
Lifetime	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.
	Renew password after expiration	When this is enabled, users can log in after password expiry and are forwarded to the "Change Password" page.
	Password expiration tolerance (in days)	Defines how long the password can be used after expiry.
Notification	Enable password reset via e-mail	When this is enabled, the "Reset password" link is shown on the login page. Requirement: • An e-mail address is configured for the user. • The SMTP client is configured
	Password reset link validity (hours)	Specifies how long the link to reset the password is valid.
Handling	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.
	User must change password after first login	Specifies whether a user needs to change their password after the first login.
	Enable Two-Factor Authentication	Specifies whether the user will be asked for the TOTP (one-time password) after logging in with user name and password.
	Enable Remember Token	When enabled, the one-time token is saved. You specify the duration of validity under "Remember Token Time (in days)". A new one-time token is required after this time.

11. Click the "Finish" button.

4.10.1.3 Create a new user

Create a new user

1. Open the "Local user" 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 names are not allowed: admin, conn

   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
Login method	• Password Login with user name and password • PKI Login only 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. Assign rights and roles
   - Assignment of rights via role assignment:
     Click + and select the required role in the drop down list. Click "Add".
     Global user rights
     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.
     Group rights
     The user is given the rights assigned to the participant group.
     To cancel the role assignment, click the check box for the role again.
   - 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. Create Group memberships
   - Select one or more participant groups to which the user will be assigned. You will find information on creating participant groups (Page 99)".
   - Click the "Next" button.
6. Configure the VPN connection mode
   - Set the OpenVPN connection mode:

Field	Meaning
Request virtual IP address	When enabled, a virtual IP address is requested during connection establishment.
Fixed VPN 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

   - Forward via the firewall
     The following parameters are required if the WAN IP address of the SINEMA RC server is implemented with NAT.

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

     Click "Add". Once added, the entries are listed in a table. To delete, click on ⊖ in the actions.

7. Set the Layer 2 connection parameters.
   - Enable Layer 2. The MAC address (Page 106) that is used for the Layer 2 interface is shown for "MAC address".
   - Select the desired Layer-2 network and click the "Add" button.
   - Enter a free IP address from the Layer-2 network for "IP address".
   - Select the required participant group.
   - Click "Add". Once added, the entries are listed in a table. To delete, click on in the actions.
8. Click "Next".
9. Specifying the password
   Enter a password and confirm it. The password depends on the configured password rules, see section "Access (Page 129)".
   The assigned password can be changed later by the relevant user, refer to the section "Changing the current password (Page 157)".
10. Reset 2FA
    A new QR code and a new alphanumerical code are generated.
11. Click the "Finish" button.

Changing user settings

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

Note

Changing the login method

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

4.10.2 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 into the 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.

4.10.3 Client Software

4.10.3.1 Client Software

On this page, you can upload the installation software of the SINEMA RC Client to the SINEMA RC server.

Requirement

- The user has access to the storage directory.

Calling the Web page

In the navigation, select "User Accounts > Client Software".

Importing client software

Procedure

1. Click "Choose file" on the "Client Software" tab.
2. Navigate to the storage directory and select the file to be loaded (*.exe). Confirm your selection with the "Open" button.
3. Click the "Import" button.

Result

The SINEMA RC Client software is uploaded to the SINEMA RC server. The file name and the fingerprint with SHA256 are displayed. Check the displayed fields.

4.10.3.2 Client Settings

On the "Client Settings" tab, you can load your own logo image in PNG, JPEG or BMP format. This image is shown in the client interface instead of the SIEMENS logo. To avoid image distortions or cropping, use images with an aspect ratio of 2 : 1 (height x width), e.g. 200 x 100px or 600 x 300px.

Requirement

- The user has access to the storage directory.

Calling the Web page

In the navigation, select "User Accounts > Client Software" and the "Client Settings" tab.

Client settings

1. Click "Choose file" on the "Client Settings" tab.
2. Navigate to the storage directory and select the image file to be loaded. Confirm your selection with the "Open" button.
3. Click the "Import" button.
   Result
   The image is uploaded to the SINEMA RC server. The file name and the miniature view are displayed. The logo is applied next time the client starts. You can switch back to the standard image with the "Reset to default logo" button.
4. To show the logo as banner image in the server header, activate the "Show as banner" setting.

4.11 Services

4.11.1 API

On this page, you set up the SINEMA RC API server, which answers the API requests of the API client.

Requirement

To be able to use this function, you need the SINEMA RC API license (MLFB 6GK1724-3VH03-0BV0).

You can test the function for free for a period of 14 days. For this purpose, you need to activate the trial license. You can find additional information in section "Overview (Page 69)" and in the "SINEMA Remote Connect API server" Getting Started manual.

Calling the Web page

In the navigation, select "Services > API".

Setting up the API server

Select the "API server" check box and make the following setting:

Field	Meaning
API Token expire time (days)	Enter the expiry time of the authentication token.
Time-Based System Token expire time (mins)	Enter the expiry time of the system token.

Click "Save" to save the settings.

Result

The API server is set up. Via the API, you can access the WBM of the SINEMA RC server to configure it.

You can find more information on configuring the WBM of the SINEMA RC server with API in the "SINEMA RC API server" Getting Started.

4.11.2 UMC

On this page, you set up the connection to the UMC server.

Requirement

To be able to use this function, you need the SINEMA RC UMC license (order no. 6GK1724-2VH03-0BV0).

You can test the function for free for a period of 14 days. For this purpose, you need to activate the trial license. For more information, refer to the section "Logging on with UMC (Page 41)".

Calling the Web page

In the navigation, select "Services > UMC".

Setting up the connection to the UMC server

Select the "UMC server" check box and make the following settings:

Field	Meaning
UMC server IP address	Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the UMC server.
UMC server port	Enter the port number of the UMC server.

Click the "Save & Verify Certificate" button.

The result of verification is output in "Certificate Status".

4.11.3 OAuth/OpenID

On this page, you configure access to the application registration server.

Requirement

- To be able to use this function, you need the license SINEMA RC IAM (MLFB 6GK1724-7XG01-0BK0).
- You can test the function for free for a period of 14 days.
- On the application registration server:
  - SINEMA RC Server is registered as application (app)
  - The corresponding app roles are present

Calling the Web page

In the navigation, select "Services > OAuth/OpenID".

Configuring OAuth/OpenID

1. Select the "OAuth/OpenID" check box and make the following settings:

Field	Meaning
Client ID	The client ID or application ID is assigned by the application registration server.
Client secret	The client secret is assigned by the application registration server. Used by the token for authentication.
Metadata URL	Path to the OpenID configuration document on the application registration server
Redirect URL	The request to the application registration server is forwarded by the SINEMA RC Server to this URL. This URL must be entered in the settings of the application registration server as callback URL or redirect URL. • 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 58)". • The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 60)"). • The local IP address from the "System > Network > Interfaces" (Page 58) page is used.
Redirect URL client	The request to the application registration server is sent by the SINEMA RC client to the application registration server.
Provider description	Enter a description text that is shown on the login page as button on the "OAuth/OpenID" tab.

2. Click "Save" to save the settings.
   On saving, a check is performed to determine whether the OpenID configuration document can be retrieved.

Retrieving available claims

1. In the navigation, select "Services > OAuth/OpenID" and click "Claims".
2. Click the "Get claims" button.
   The claims available on the application registration server are shown.

4.11.4 Server upload

This page provides you with the option of uploading configuration files or logfile messages to an SFTP server. SFTP stands for Secure File Transfer Protocol, but this is often confused with Simple File Transfer Protocol. The SFTP server uses a separate protocol which enables the transfer of files via a secure SSH connection.

Calling the Web page

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

Displayed entries

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

Field	Meaning
Automatic file upload	When activated, the newly generated files are uploaded to the SFTP server.
Files for upload	Specify which file types are to be uploaded: • Backup file • Log archives • Backup file and Logfile archives
SFTP server name	IP address or FQDN 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 ":" is entered as separator between the IP address and the port number, 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. Check with the "Check fingerprint" button whether the new fingerprint matches that of the SFTP server.
Upload directory	The user is assigned a storage directory, the so-called home directory. This field cannot be empty. If you enter "\", the file will be uploaded directly to the home directory. To upload the file to a subdirectory, specify the subdirectory. 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
Upload old files	Button for uploading all currently present files to the SFTP server

After the configuration is saved, newly generated files are automatically transferred to the SFTP server.

To upload currently present files to the SFTP server, click the "Upload old files" button.

4.11.5 Syslog client

On this page, you set up the Syslog client on the SINEMA RC server to establish the connection to the Syslog server and check its connection status.

Calling the Web page

In the navigation, select "Services > Syslog Client".

Establishing a connection to the Syslog server

Make the following settings and then click "Save & check connection":

Field	Meaning
Client Identifier (Hostname)	Enter the IP address of the SINEMA RC server. With this IP address, SINEMA RC identifies itself as Syslog client on the Syslog server.
Syslog server IP address	Enter the IP address of the Syslog server.
Syslog server port	Enter the port number of the Syslog server.
Protocol	Select the desired IP protocol (TCP (TLS) or UDP) from the list.
Syslog server requests client authentication	When enabled, the Syslog server requires client authentication. A connection certificate should be specified in the field below for this purpose. This setting is used for mutual authentication between the Syslog client and the Syslog server (server and client authentication) and is only relevant for the selected protocol TCP (TLS). This check box cannot be activated for the selected UDP protocol.
Connection certificate	Only available when "Syslog server requests client authentication" is enabled. Select the certificate that our SRC server used to authenticate itself as Syslog client on the Syslog server. You can import certificates via the Web page "Security > Syslog CA certificate"; see section "Syslog CA Certificates (Page 147)".

Note

No suitable certificate for connection

If the Syslog client wants to establish a connection with the Syslog server and no suitable certificate is found in the Syslog management, the Syslog server certificate is displayed.

In this case, you have the option to add this to SINEMA RC with "Accept" and to authorize the Syslog connection with "Save & check connection".

Before you apply the Syslog certificate in the certificate store, compare the displayed fingerprint with the fingerprint of the Syslog server.

With "Refuse", you deny the use of the respective certificate.

Result

The connection to the newly created Syslog server is established. The connection parameters and the status are displayed in a table.

Displayed entries

The following entries are displayed:

Field	Meaning
IP address of the connection	Shows the IP address of the Syslog server.
Connection port	Shows the number of the connection port.

Field	Meaning	
IP protocol	Shows the IP protocol used.	
Status	Shows the connection status to the Syslog server. The following statuses are possible: • Connections over UDP: – "-" Connection monitoring via UDP is not possible. • Connections over TCP (TLS): – Online Establishing a connection to the Syslog server. – Offline An established connection to the Syslog server is interrupted, e.g. if the Syslog server is no longer available. – Rejected If it transpires during a connection check, e.g. using the button, that a certificate is invalid or has expired or the Syslog server is not responding. – Disabled The connection to the Syslog server is disabled. – Certificate deleted A Syslog certificate based on which the connection was established has been deleted.	
Actions		Check connection to the Syslog server (only with connections over TCP (TLS)).
		Download Syslog client certificate from SINEMA RC.
		Click this button to disable the Syslog server.
		The Syslog server is disabled and no messages are sent to it. Click this button to enable the Syslog server.
		Remove the Syslog server from the list. The Syslog server configuration is deleted immediately.

4.11.6 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 "Services > Debug Login".

Setting up the debug login

1. Select the "Enable debug login" check box and 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.
Remaining time (minutes)	Remaining time for external access to the SINEMA RC server

2. Click "Save" to save the settings.
   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 password is deleted. The settings for Timeout and Port remain unchanged.

4.11.7 Tools

Requirement for installing tools

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

Calling the Web page

In the navigation, select "Services > Tools".

Installing VMWare tools

With "Status of the VMWare installation", you can see whether the VMWare tool is installed on the system.

To install the VMWare tool, click the "Install" button.

4.11.8 SNMP

Requirement for SNMP

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

Calling the Web page

In the navigation, select "Services > SNMP".

Configuring SNMP

1. Specify which SNMP version should be used:
   - SNMPv3 and
   - also "SNMPv1 & SNMPv2c support"
2. Specify the interface for SNMP access.

3. Specify the port at which the SNMP agent waits for the SNMP queries. Standard port 161 is the default.
4. Configure the following parameters:

Field	Meaning
SNMP user name	User name for SNMP access Range: 1... 32 characters
Read community string	String for read access via SNMP For security reasons, do not use the default values "public". The recommended minimum length for community strings is 6 characters. For security reasons, only write access is possible. Range: 1... 255 characters
Security level	Security level (authentication, encryption) for access authorization • **No Auth/no Priv** No authentication enabled/no encryption enabled. The authentication and encryption fields are not editable. • **Auth/no Priv** Authentication enabled/no encryption enabled. • **Auth/Priv** Authentication enabled/encryption enabled.
Authentication algorithm	Set the authentication algorithm for which an SNMP authentication password is stored. The following settings are available: • MD5 • SHA
Encryption algorithm	Set the encryption algorithm for which an SNMP encryption password is stored. The following settings are available: • DES • AES-128
SNMP authentication password SNMP Authentication Password Confirmation	Enter a password and confirm this password. See also the guidelines in the section "Permitted characters".
SNMP encryption password SNMP Privacy Password Confirmation	Enter a password and confirm this password. See also the guidelines in the section "Permitted characters".

Note

Length of SNMP authentication password / SNMP encryption password

As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters and numbers.

4.12 Security

4.12.1 General

4.12.1.1 General

Calling the Web page

In the navigation, select "Security > General".

Global encryption settings

On this page, you specify whether the "High" or "Low" setting is valid for the encryption (ciphers).

The SINEMA RC server restarts if you change the encryption. The CA certificate and the certificates derived form the CA certificate are re-generated.

- **High**
  - Min. 4096 bits
  - Min. SHA256
  - DH = 4096
  - Min. AES256
  - Min. TLS1.2
- **Low**
  - 2048 bits
  - SHA256
  - AES256

See also

Appendix D (Page 191)

4.12.1.2 Access

This page enables you to make the settings for the password and for Brute Force protection.

Calling the Web page

Select "Security > General > Access" in the navigation.

Configure password rules

Field	Meaning	
Policy	Sets password rule • Standard: Pre-configured settings – Password length: at least 12 characters, maximum 128 characters – At least 1 number – At least 0 special characters – At least 1 lowercase letter – At least 1 uppercase letter • Custom The desired requirements for passwords are configured. 8 ... 128 characters	
Custom requirements	Minimum Password Length	Length that the password must be at least.
	Minimum Number of Numeric Characters	Number of digits a password must contain at least.
	Minimum Number of Special Characters	Number of special characters a password must contain at least.
	Minimum Number of Lowercase Letters	Number of lowercase letters a password must contain at least.
	Minimum Number of Uppercase Letters	Number of uppercase letters that a password must contain at least.

Configure protection against Brute Force

Brute Force Prevention (BFP) refers to the protection from unauthorized access by trying a sufficiently large number of passwords. For this purpose, the login attempts are blocked within a specific period.

Field	Meaning	
Policy	Sets rule for protection against Brute Force • Standard: Pre-configured settings – Permitted number of invalid login attempts: 3 – Permitted number of invalid token requests: 5 – Blocking duration of the IP address: 1 minute • Custom Configures the desired settings.	
Custom settings	Permitted number of invalid login attempts	The maximum number of invalid login attempts that will be accepted. Further login attempts will be blocked for a specified time.
	Permitted number of invalid token requests	The maximum number of invalid token requests that will be accepted. Further requests will be blocked for a specified time.
	Maximum number of password reset requests	The maximum number of password reset requests that will be accepted. Further requests will be blocked for a specified time.
	Blocking duration of the IP address (min.)	Time for which login is blocked because the maximum number was exceeded.
	Disable instead of block	If enabled, login will not be blocked, but the user or device will be disabled.

4.12.2 Managing certificates

4.12.2.1 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 133)
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 134)
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 86)
User certificate	SINEMA RC Server creates a personal certificate for each created user. You obtain an overview of the user certificate on the page "My Account > User Certificate".	*.p12 *.pem	User certificate (Page 155)
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 144)
Syslog server CA certificate	For authentication on the Syslog server.	*.crt	Syslog CA Certificates (Page 147)

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.

4.12.2.2 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.

Field	Meaning	
Actions		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.

Deleting a CA certificate

CA certificates with the "Out of service" status can be deleted. For this purpose, select the relevant certificate in the overview and click the "Delete" button.

4.12.2.3 Server certificate

Calling the Web page

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

Displayed entries

In the "Web server certificate", "Fallback 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 60)"). • The IP address of the WAN or LAN interface, see section "Interfaces (Page 58)".
Issuer	Display of the certificate authority that issued the certificate.
Valid from	Date from which the certificate is valid.
Valid until	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

Field	Meaning
SHA256 fingerprint	Fingerprint with SHA256 (SH2) as hash algorithm
Alternative names	• IP: The IP address of the WAN interface, see section "Interfaces (Page 58)". • 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 58)". • DNS: The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 60)").

Renew web server certificate, fallback 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.

4.12.2.4 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 the certificate, click the "Choose file" button in "Select the certificate file".
2. Select the certificate file and confirm your selection with the "Open" button.
3. Click the "Choose file" button in "Select the key file".
4. Select the corresponding key file and confirm your selection with the "Open" button.
5. To import the certificate of a higher ranking certification authority, click the “Choose file" button in "Select the CA chain file".
6. Select the CA certificate file and confirm your selection with the "Open" button.
7. For password-protected files, enter the password specified for the file and repeat the entry.

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.

Field	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 applicant
Issuer	Display of the certificate authority that issued the certificate.
Valid from	Date from which the certificate is valid.
Valid until	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.

4.12.2.5 Device certificate

Calling the Web page

In the navigation, select "Security > Certificate Management" and the "Device certificate" tab.

Displayed entries

On the "Device Certificate" tab, you can see an overview of the imported certificates:

Field	Meaning
Type	Type of the loaded file. For more information, refer to the section "Overview of certificate management (Page 132)".
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 (Common Name CN).
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.
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 into 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.

Field	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 applicant
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 (bits)	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.

4.12.2.6 Making settings for certificates

Calling the Web page

In the navigation, 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. You can generate a new server certificate on the following tabs with the "Renew" button:

- Web server certificate
- Fallback certificate
- VPN Server Certificate

Field	Meaning
CA lifetime (years)	Enter the validity of the CA certificate after it is issued.
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

Field	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 CA 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.

4.12.3 VPN connections

4.12.3.1 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 132)".

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 86)".

For users, the file is called in the personal user account (see section "User certificate (Page 155)").

4.12.3.2 OpenVPN

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 > OpenVPN".

Configuring OpenVPN

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

Field	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)

Field	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

4.12.3.3 IPsec

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 "Security & IPsec", select the "IPsec profile" tab.

Configuring the IPsec basic settings

On the "IPsec" tab, configure the following settings that are valid for all IPsec VPN profiles after you have saved:

Field	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 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

IPsec profiles

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

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

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 142)"	
Key exchange	Key exchange method	
IKE	Settings of Phase 1 - IKE (KE/Key exchange)	
ESP	Settings of Phase 2 - ESP (authentication)	
Actions		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 Phase 2.

Using the "Create" button, you can create new IPsec profiles, see "Creating IPsec profiles (Page 142)".

With the "Copy" button, you create a copy of the selected profile in which you adapt parameters and which you can save as new IPsec profile. You delete created IPsec profiles with "Delete".

Creating IPsec profiles

Requirement for changing the IPsec VPN 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. Make the settings of Phase 1 - IKE (SA/Key exchange):

Field	Meaning
Encryption algorithm	The selection depends on the phase und the key exchange method (IKE)
Hash algorithm	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 (m)	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):

Field	Meaning
Protocol	Selection of the protocol AH: The IP Authentication Header (AH) handles the authentication and identification of the source. If the AH protocol is selected, the data traffic is not encrypted. Use this protocol with the security setting “High”. ESP: The Encapsulation Security Payload (ESP) encrypts the data.
Encryption algorithm	The selection depends on the phase und the key exchange method (IKE)
Hash algorithm	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 (m)	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 "Create".

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

4.12.4 PKI Certificate Management

4.12.4.1 PKI CA certificate

Calling the Web page

In the navigation, select "Security > PKI Certificate Management".

Displayed entries

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

Field	Meaning
Common name	Name of the applicant, e.g. the user name
Status	Shows whether the certificate is valid or has already expired.
Certificate type	Type of imported certificate
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 until	Date on which the certificate expires.
Fingerprint	Checksum of the certificate to ensure integrity

To delete a PKI CA certificate, select the check box in front of the certificate to be deleted and click the "Delete" button.

Importing PKI CA certificates

1. To import PKI CA certificates click the "Import" button.
2. Select the certificate file (*.crt) 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".

4.12.4.2 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, select "Security > PKI Certificate Management" and the "Certificate Revocation" tab.

Certificate revocation list

The output certificates that are no longer valid are listed in a certificate revocation list. If, for example, employees leave the company, their certificates are called back and included in the list. Logging in 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.
Revoked serial numbers	Shows the revoked serial numbers.
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 or deleting the certificate revocation list

Import

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

Delete

1. Select the check box in front of the certificate revocation list to be deleted.
2. Click the "Delete" button.

Obtaining the certificate revocation list automatically

In a certificate according to the X.509v3 standard, you can specify a certificate revocation list distribution point. To do this, specify a URL in the attribute "CRL Distribution Point" 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
Activate CRL checking	When enabled, the validity of the user certificate is checked based on the certificate revocation list.
CRL update interval (min)	Specify the intervals at which the certificate revocation list is checked for changes. If there are changes, the certificate revocation list is downloaded from 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.

PKI DN blacklist

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

1. Click on the "PKI DN blacklist" tab.
2. Enter the corresponding filter rule in "PKI DN". 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 blocked.

To delete a PKI DN filter rule, select the check box in front of the entry to be deleted and click the "Delete" button.

4.12.5 Syslog Certificate Management

4.12.5.1 Syslog CA Certificates

You can import the CA certificate required for the Syslog server authentication on this page.

Note

Importing the CA certificates

Import Syslog server CA certificates first. If you load Syslog certificates later, it will not be possible to run some functions, such as chain inspection or certificate revocation list. Connection without imported Syslog server CA certificates is possible, however.

Types of Syslog authentication

During a **Syslog server authentication**, the Syslog client checks the identity of the Syslog server using the CA Syslog server certificate**.**

As an option, mutual authentication between the client and the server can take place (**server and client authentication**). In this case, the Syslog server requests the certificate of the Syslog client after Syslog server authentication in order to check the identity of the Syslog client. The certificate check takes place according to RFC 5280. For server and client authentication, the Syslog client certificate must be imported; see "Importing Syslog certificates". These certificates can be selected as connection certificates for the Syslog client, see "Syslog client (Page 123)".

Requirement

- The user has been assigned the right "Certificate management".

Calling the Web page

In the navigation, select "Security > Syslog Certificate Management".

Displayed entries

On the "Syslog CA Certificates" tab, you can see an overview of the imported CA certificates:

Field	Meaning
Common name	Name of the applicant, e.g. the user name
Status	Shows whether the certificate is valid or has already expired
Certificate type	Type of imported certificate
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 until	Date on which the certificate expires

Field	Meaning	
Fingerprint	Checksum of the certificate to ensure integrity	
Actions		Export certificate

Importing Syslog certificates

1. To import Syslog certificates, click the "Import" button.
   The dialog page for importing certificates is displayed. You can load the following files:
   - Syslog server CA certificate (required)
   - Syslog client certificate (optional)
   - Syslog client private key (optional)
2. Click the "Choose file" button for the certificate type to be imported.
   Navigate to the storage directory and select the relevant file. Confirm your selection with the "Open" button.
3. To load the files onto the SINEMA RC server, click the "Save" button.

Result

The certificate file is imported onto the SINEMA RC server. The Syslog certificate is shown in the table.

Note

Incorrect parameters of the server certificate

The encrypted connection between the server and the client fails if the "commonName" or the parameter of the server certificate "subject_alt_name" does not contain either the host name or the IP address of the server (e.g. CN = 192.168.10.10).

Note

Renewing certificates

SINEMA RC does not renew the certificates automatically. To avoid certificate problems, update the expired certificate files manually on the Syslog server and the SINEMA RC server.

4.12.5.2 Syslog Certificates

On this page, you can import the Syslog client certificates and manage the imported certificates. For authentication, the Syslog server requests the certificate of the Syslog client in order to check the identity of the Syslog client.

Requirement

- The user has been assigned the right "Certificate management".

Calling the Web page

In the navigation, select "Security > Syslog Certificate Management".

Displayed entries

On the "Syslog Certificates" tab, you can see an overview of the imported Syslog certificates:

Field	Meaning	
Common name	Name of the applicant, e.g. the user name	
Status	Valid: The certificate is used. Invalid: The certificate is not used. A newer certificate was generated or the certificate has expired.	
Certificate type	Type of imported certificate	
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 until	Date on which the certificate expires.	
Fingerprint	Checksum of the certificate to ensure integrity	
Actions		Export certificate
		Renew certificate

Importing Syslog certificates

1. To import Syslog certificates, click the "Import" button.
   The dialog page for importing certificates is displayed. You can load the following files:
   - Syslog server CA certificate (required)
   - Syslog client certificate (optional)
   - Syslog client private key (optional)
2. Click the "Choose file" button for the certificate type to be imported.
   Navigate to the storage directory and select the relevant file. Confirm your selection with the "Open" button.
3. To load the files onto the SINEMA RC server, click the "Save" button.

Result

The certificate file is imported onto the SINEMA RC server. The Syslog certificate is shown in the table.

Note

Incorrect parameters of the server certificate

The encrypted connection between the server and the client fails if the "commonName" or the parameter of the server certificate "subject_alt_name" does not contain either the host name or the IP address of the server (e.g. CN = 192.168.10.10).

Note

Renewing certificates

SINEMA RC does not renew the certificates automatically. To avoid certificate problems, update the expired certificate files manually on the Syslog server and the SINEMA RC server.

Deleting Syslog certificates

You can delete expired certificates using the "Delete" button.

1. Select the check box of the certificate to be deleted.
2. Click the "Delete" button.

4.12.5.3 Revoking Syslog Certificates

You can revoke users by means of the Syslog Certificate Revocation List (CRL).

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

Calling the Web page

In the navigation, select "Security > Syslog Certificate Management".

Certificate revocation list

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

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

Field	Meaning
Issuer	Display of the certification authority that issued the certificate revocation list.
Revoked serial numbers	Shows the revoked serial numbers.
Last update	Date on which the certificate revocation list was last updated.

Field	Meaning
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 or deleting the certificate revocation list

Import

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

Delete

1. Select the check box in front of the certificate revocation list to be deleted.
2. Click the "Delete" button.

Obtaining the certificate revocation list automatically

In a certificate according to the X.509v3 standard, you can specify a certificate revocation list distribution point. To do this, specify a URL in the attribute "CRL Distribution Point" at which the current CRL of this certification authority is stored. To use this function, the attribute must exist in the Syslog 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
Activate CRL checking	When enabled, the validity of the user certificate is checked based on the certificate revocation list.
CRL update interval (min)	Specify the intervals at which the certificate revocation list is checked for changes. If there are changes, the certificate revocation list is downloaded from the distribution point.
Allow missing CRL	• Disabled Each Syslog certificate requires a valid certificate revocation list. If this is missing, the user certificates derived from the Syslog 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 Syslog certificate are permitted.

4.12.6 UMC certificate management

4.12.6.1 UMC CA certificates

You can import the CA certificate required for the UMC server authentication on this page.

Note

Importing the CA certificates

Import UMC server CA certificates first. If you load UMC certificates later, it will not be possible to run some functions, such as chain inspection or certificate revocation list. Connection without imported UMC server CA certificates is possible, however.

Requirement

- The user has been assigned the right "Certificate management".

Calling the Web page

In the navigation panel, select "Security > UMC Certificate Management".

Displayed entries

On the "UMC CA certificate management" tab, you can see an overview of the imported CA certificates:

Field	Meaning	
Common name	Name of the applicant, e.g. the user name	
Status	Shows whether the certificate is valid or has already expired	
Certificate type	Type of imported certificate	
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 until	Date on which the certificate expires	
Fingerprint	Checksum of the certificate to ensure integrity	
Actions		Exporting a CA certificate By clicking on the icon, the CA certificate (*.crt) is exported.

Importing a UMC CA certificate

1. To import a UMC CA certificate, click the "Import" button.
2. Select, for example, the PKCS12 file (*.p12) and confirm your selection with the "Open" button.
3. The files are password-protected. To load the files into 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.

Field	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 applicant
Issued by	Display of the certificate authority that issued the certificate.
Valid from	Date from which the certificate is valid.
Valid until	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 onto the SINEMA RC Server, click the "Import" button.

Result:

The PKCS12 file is imported onto the SINEMA RC Server.

4.12.6.2 UMC certificates

On this page, you can import the UMC certificates and manage the imported certificates. For authentication, the UMC server requests the certificate of the UMC client in order to check the identity of the UMC client.

Requirement

- The user has been assigned the right "Certificate management".

Calling the Web page

In the navigation panel, select "Security > UMC Certificate Management".

Displayed entries

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

Field	Meaning
Common name	Name of the applicant, e.g. the user name
Status	Valid: The certificate is used. Invalid: The certificate is not used. A newer certificate was generated or the certificate has expired.
Certificate type	Type of imported certificate
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.

Field	Meaning
Valid until	Date on which the certificate expires.
Fingerprint	Checksum of the certificate to ensure integrity

Importing UMC certificates

1. To import UMC certificates, click the "Import" button.
   The dialog page for importing certificates is displayed. You can load the following files:
   - UMC client certificate
   - UMC client private key (optional)
2. Click the "Choose file" button for the certificate type to be imported.
   Navigate to the storage directory and select the relevant file. Confirm your selection with the "Open" button.
3. To load the files onto the SINEMA RC server, click the "Save" button.

Result

The certificate file is imported onto the SINEMA RC server. The UMC certificate is shown in the table.

4.12.7 OID certificate management

4.12.7.1 OAuth/OpenID CA certifiate

You can import the CA certificate required for the OAtuh/OpenID authentication on this page.

Note

Importing the CA certificates

Import CA certificates first. If you load certificates later, it will not be possible to run some functions, such as chain inspection or certificate revocation list. Connection without imported CA certificates is possible, however.

Requirement

- The user has been assigned the right "Certificate management".

Calling the Web page

In the navigation, select "Security > OID Certificate Management".

Displayed entries

On the "OAuth/OpenID CA certificate" tab, you can see an overview of the imported CA certificates:

Field	Meaning	
Common name	Name of the applicant, e.g. the user name	
Status	Shows whether the certificate is valid or has already expired	
Certificate type	Type of imported certificate	
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 until	Date on which the certificate expires	
Fingerprint	Checksum of the certificate to ensure integrity	
Actions		Export certificate

Importing OAuth/OpenID certofocates

1. To import OAuth/OpenID-CA certificates, click the "Import" button.
2. Select the certificate file (*.crt) 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 certificate is displayed on the following tab "OAuth/OpenID CA certificate".

4.13 My Account

4.13.1 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.

Field	Meaning
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 > Certificate management", "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 > Certificate management", "Settings" tab under "Preferred hash method".

Personal Certificate: Request Renewal

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.

4.13.2 Manage authentication

4.13.2.1 Change password

Changing the current password

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

1. In the navigation, select "My Account > Manage Authentication > Password".
2. Enter the old password.
3. Enter the new password and confirm it.
   The password depends on the configured password rules, see section "Access (Page 129)". See also "Permitted characters (Page 28)".

4.13.2.2 TOTP-based two-factor authentication

TOTP-based two-factor authentication with a one-time token (Time-based One-time Password) is disabled by default. The configuration is made for the user in the role settings. The administrator can enable two-factor authentication for the administrator user account. The administrator can also generate a list of tokens that serve as backup tokens in case the device and its one-time token is lost. Each backup token can only be used once.

Note

Security requirements

Keep the operating system on the mobile device and the authentication app up to date. The authentication app must be trustworthy. Keep your password safe on the device.

Requirement

- An authentication app that supports TOTP is installed on the smartphone.

Enable Two-Factor Authentication

1. In the navigation, select "My Account > Manage authentication > Two-Factor".
2. Click the "Activate" button.
3. Scan the QR code with the authentication app or enter the alphanumeric code in the app.
4. Generate a one-time token using the authentication app.
5. In "Token", enter the one-time token and click "Save".
6. An additional "backup token" is shown on the page.
7. To generate backup tokens, click "Generate".
   A page with 10 backup tokens opens. Store the backup tokens in a safe but accessible location.

4.13.3 Download client software

On this page, you can download the SINEMA RC Client software from the SINEMA RC server to your PC.

Requirement

- The user has been assigned the right "Download client software".
- A client software package was loaded to the server.

Calling the Web page

In the navigation, select "My Account > Client Software".

Download client software

Procedure

1. Check the displayed software version of the SINEMA RC Client and the fingerprint.
2. Click the "Download software" button.
   A dialog for opening and saving files opens. Follow the instructions in the dialog to save the client software on the user PC.

Result

The SINEMA RC Client is downloaded onto your PC.

Depending on the setting, the file can also be loaded to the download folder.

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:

- Log messages
- Backup copy
- Boot partition settings
- Client software
- Firmware files for updating the devices

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/en/view/109748144)

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)".
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.

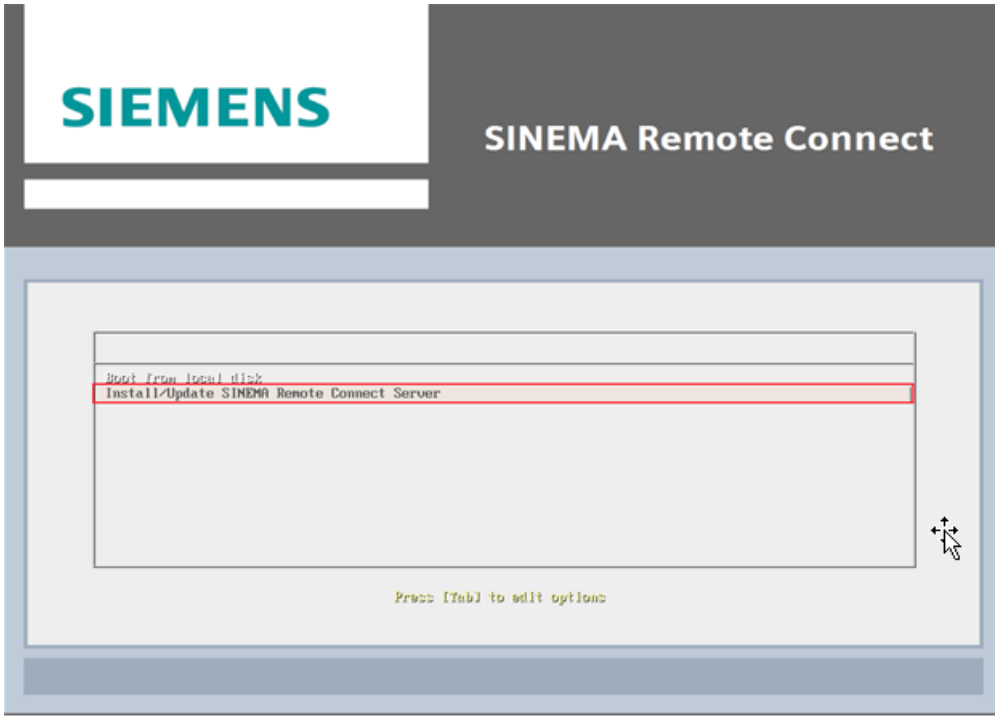
Result

- 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.

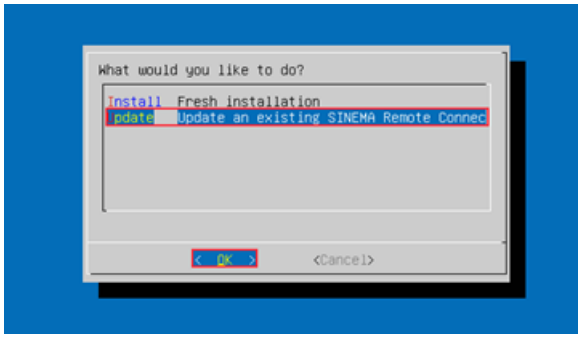
5.2 System update V1.2 > V1.3

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" and "Upload Server (Page 122)".
2. Insert the V1.3 data medium into the drive.
3. Navigate to the WBM menu "System > Update (Page 77)".
   Restart via the "Energy management (Page 77)".
   Installation starts automatically.
4. Select the "Install/Update SINEMA Remote Connect Server" entry in the following dialog.
   Confirm the selection with the ENTER key.

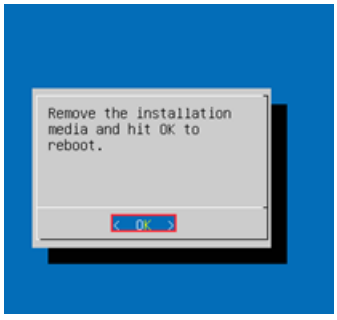


5. In the next dialog, select the entry "Update - Update an existing SINEMA Remote Connect" and click on the < OK > button.



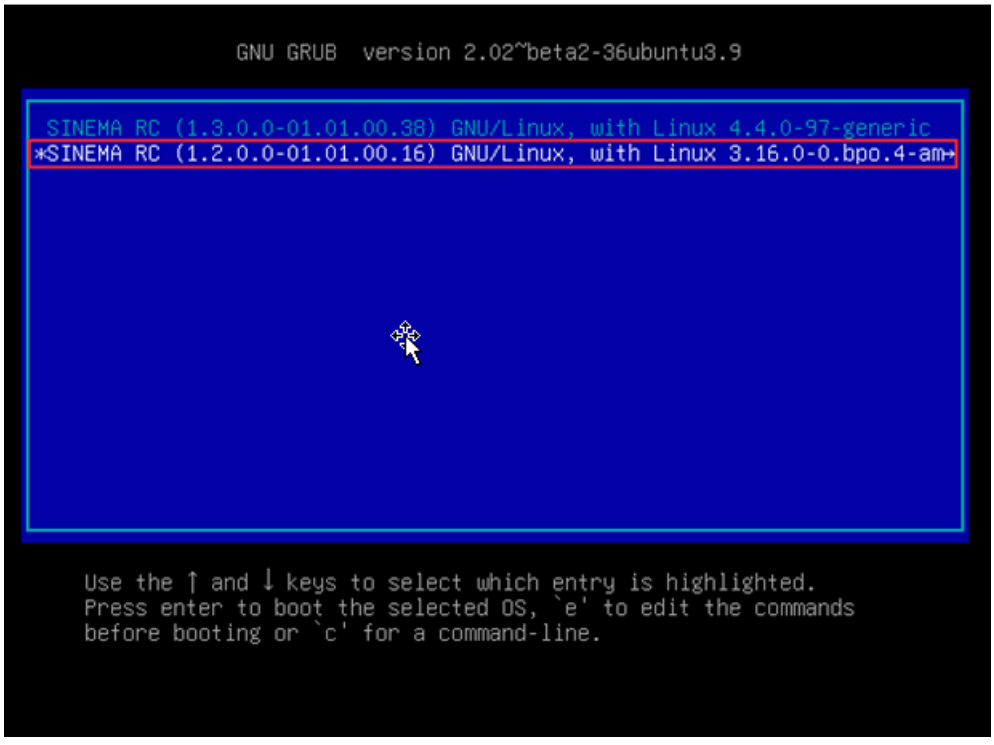
The SINEMA RC server was updated to version V1.3. After this update installation, two boot partitions are available. One partition still contains your operational server version V1.2. Another partition now contains an operational server version V1.3 with the identical server configuration including devices, 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.

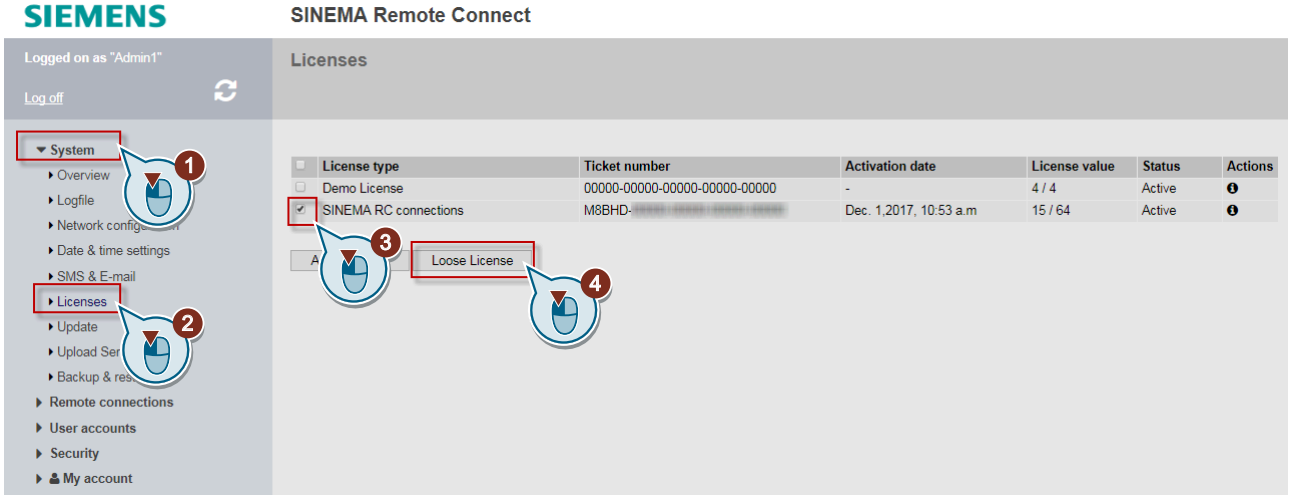


Restart the server. In the boot menu, you can see the partitions of both server versions V1.2 and V1.3.

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



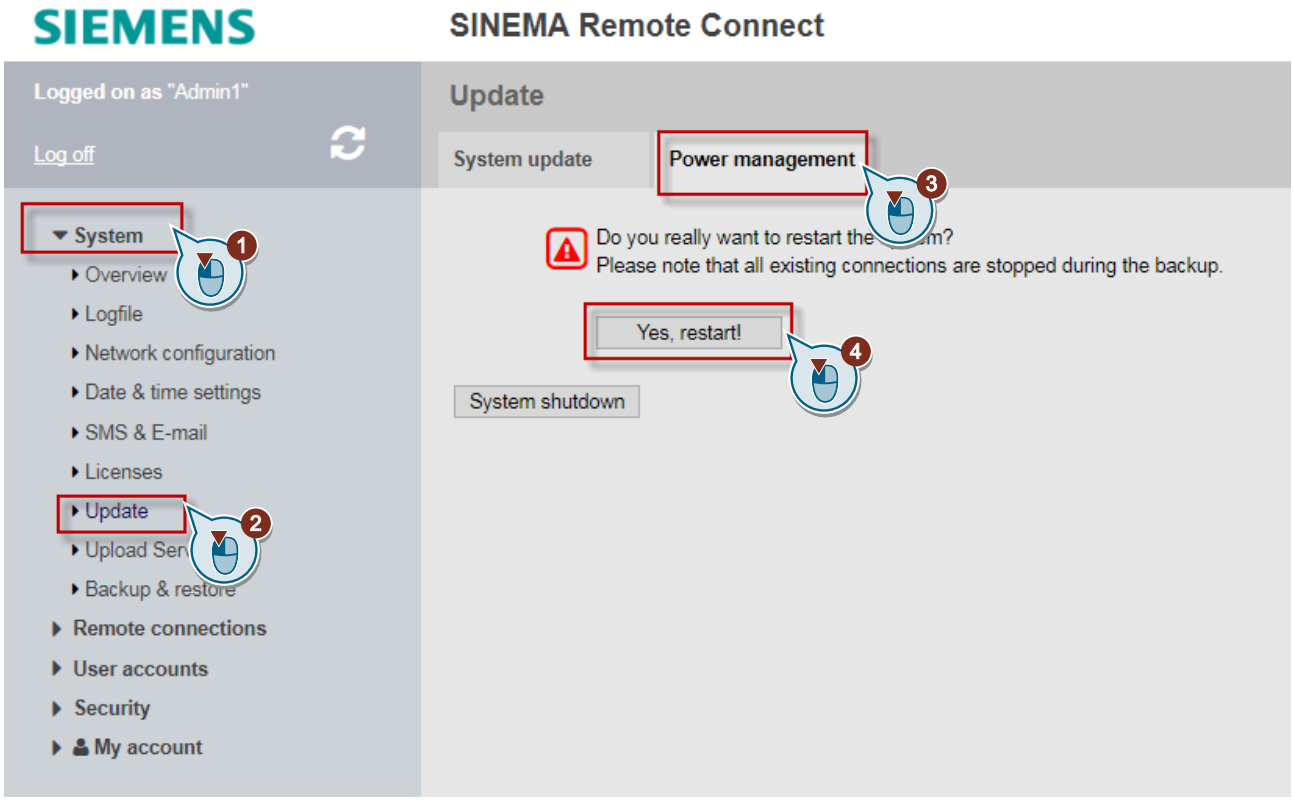
8. Log in with your user credentials and navigate to the menu "System > Licenses (Page 69)". Release the licenses to reactivate them in server version V1.3.



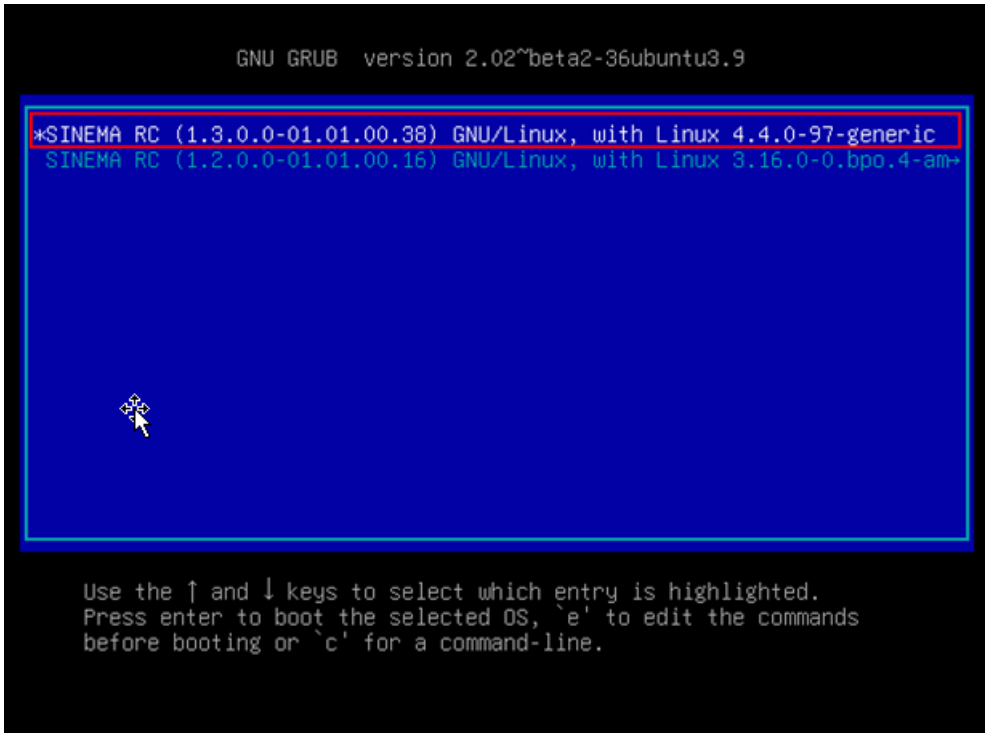
Note

If it is not possible to deactivate the license in WBM (e.g. no connection to the license server), contact Customer Support via a Support Request (https://support.industry.siemens.com/cs/us/en/my). All further steps are then coordinated with Customer Support to reactivate the license.

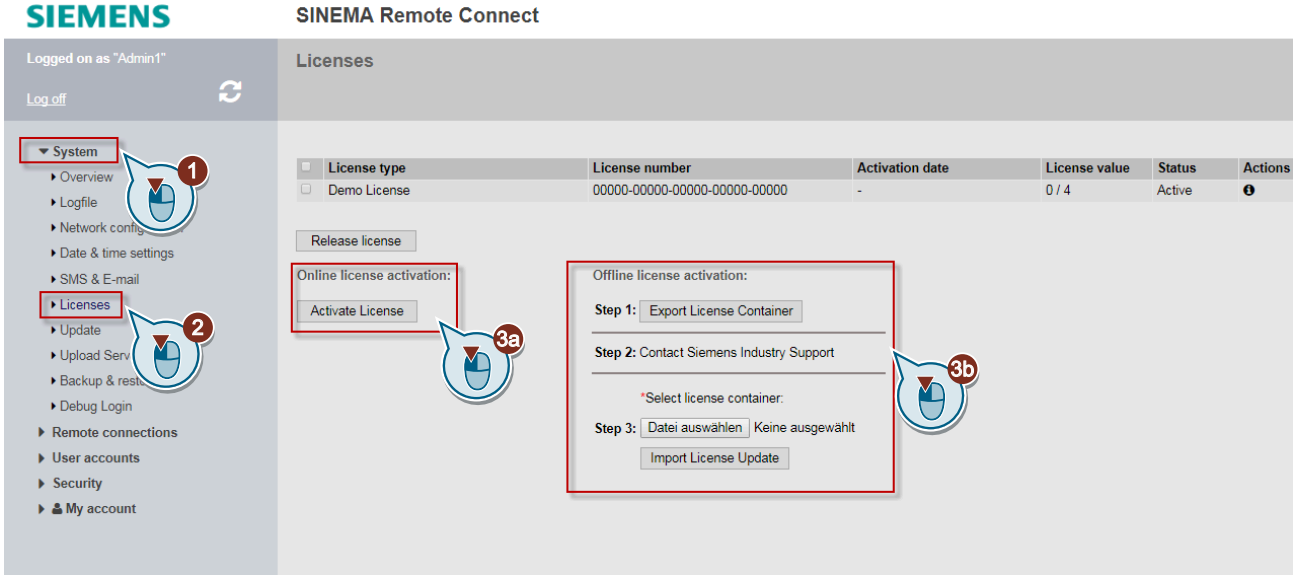
9. Navigate to the WBM menu "System > Update (Page 77)".
   Perform a restart via the "Energy Management (Page 77)".



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



11. Log in with your user credentials and navigate again to the menu "System > Licenses (Page 69)".
Activate the licenses.
You can select between offline or online activation. You can find additional information on this in the section "Managing licenses (Page 69)" .



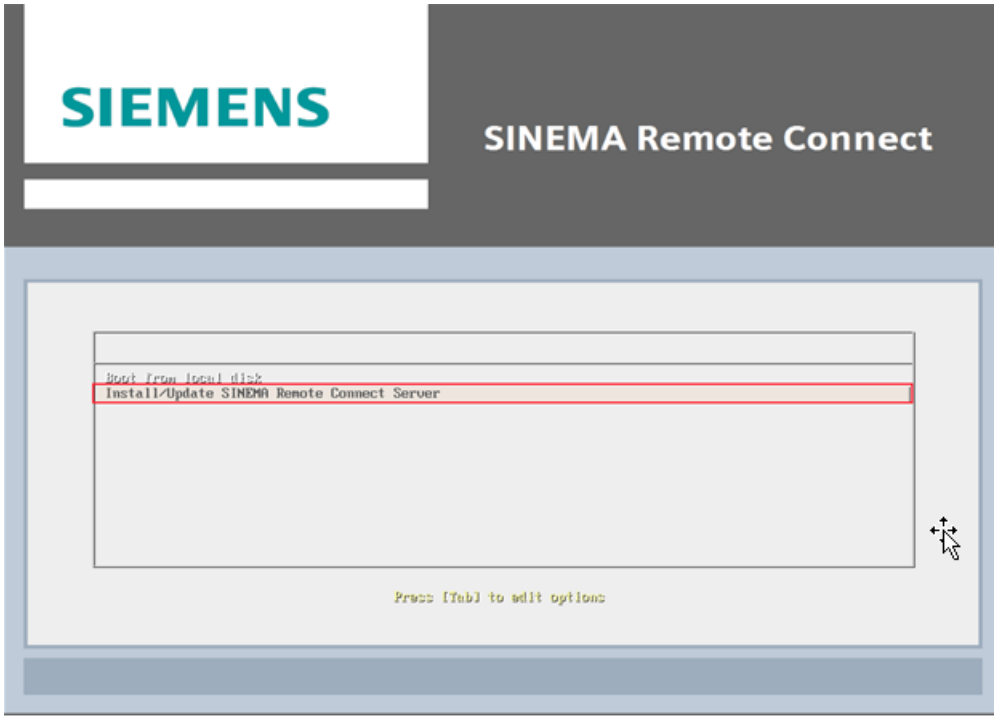
Result

The SINEMA RC server and its license have been updated to version V1.3. 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.

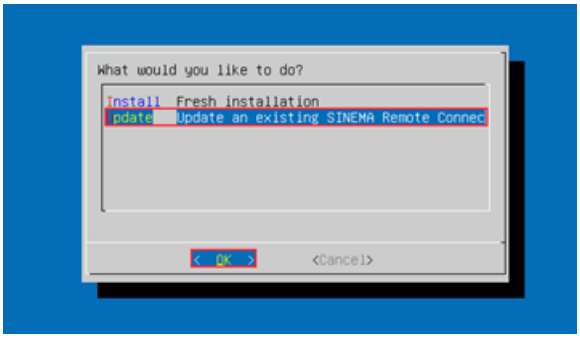
5.3 System Update V2.0 > V2.1

Procedure

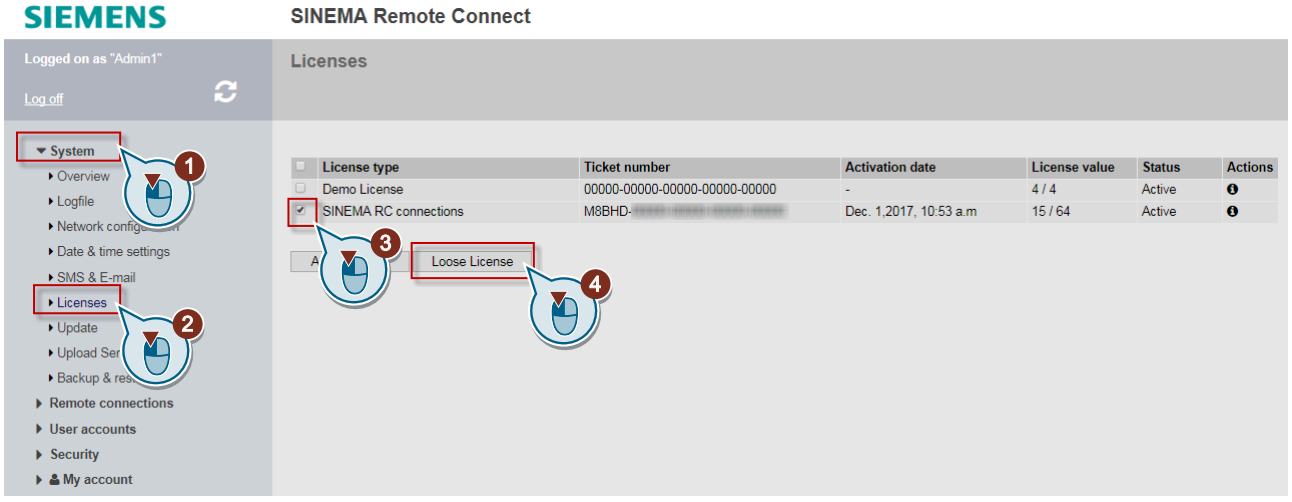
1. Back up your configuration using SINEMA RC server V2.0 WBM and export this backup file to your PC or SFTP server.
   You can find more detailed information on this in the sections "Backup & Restore" and "Upload Server (Page 122)".
2. Navigate to the WBM menu "System > Update (Page 77)".
   Restart via the "Energy management (Page 84)".
   Installation starts automatically.
3. Select the "Install/Update SINEMA Remote Connect Server" entry in the following dialog.
   Confirm the selection with the ENTER key.



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



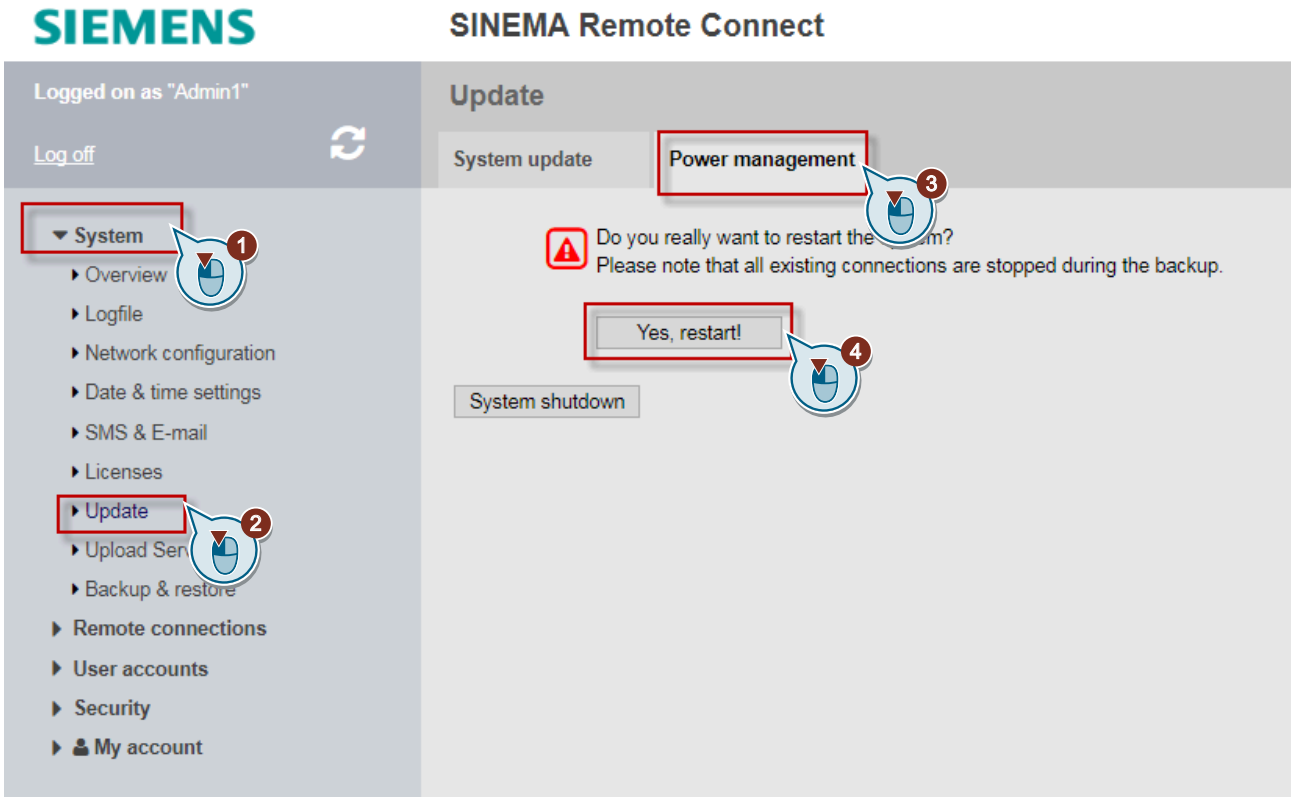
5. Select "SINEMA RC (2.0)" from the boot menu and confirm your selection with the ENTER key.
6. Log in with your user credentials and navigate to the menu "System > Licenses (Page 69)". Release the licenses for "SINEMA RC (2.0)" to reactivate them afterwards in server version V2.1.



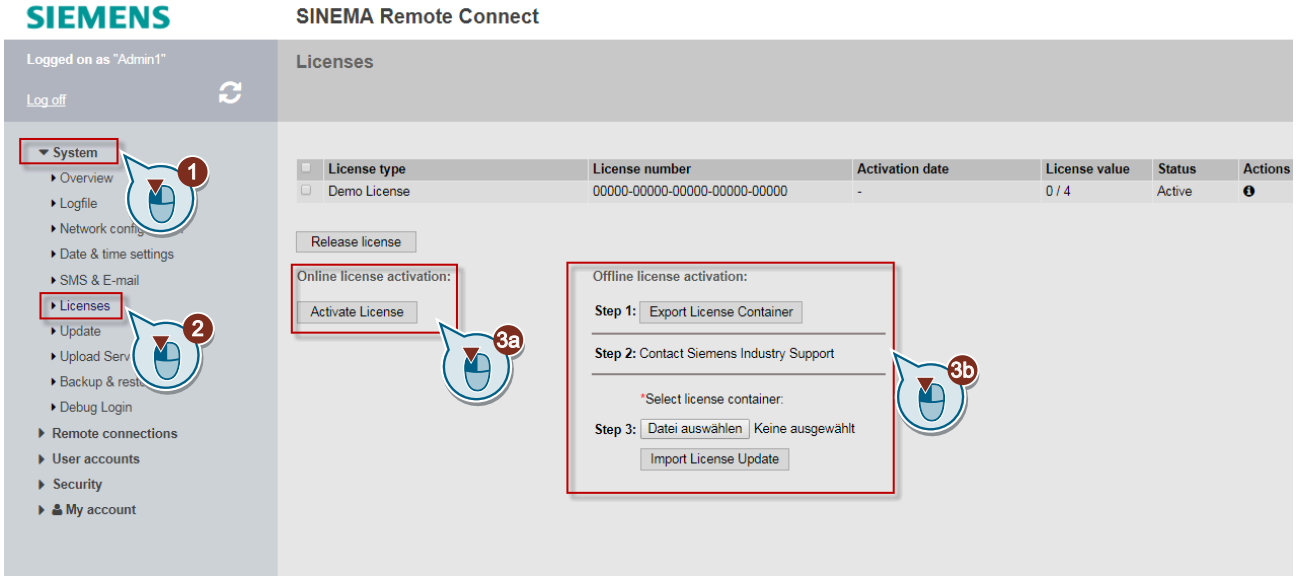
Note

If it is not possible to deactivate the license in WBM (e.g. no connection to the license server), contact Customer Support via a Support Request (https://support.industry.siemens.com/cs/us/en/my). All further steps are then coordinated with Customer Support to reactivate the license.

7. Navigate to the WBM menu "System > Update (Page 77)".
   Perform a restart via the "Energy Management (Page 84)".



8. Select "SINEMA RC (2.1)" from the boot menu and confirm your selection with the ENTER key.
9. Log in with your user credentials and navigate again to the menu "System > Licenses (Page 69)".
   Activate the licenses.
   You can select between offline or online activation. You can find additional information on this in the section "Managing licenses (Page 69)" .



Result

The SINEMA RC server and its license have been updated to version 2.1. The previous configurations of the server are retained.

5.4 System update as of V2.1

On the "System > Update" page, you can update the SINEMA RC server as of V2.1 to the next version. After the update, the server restarts. The previous configurations of the server are retained. You can find additional information in the section "Update (Page 77)".

Appendix A

A

A.1 OpenVPN connection to an iOS device

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 tap on the "Exports" tab.
3. Tap the OVPN configuration file to be loaded and confirm the dialog with "Load".
   The OVPN file is downloaded and saved in the "Downloads" folder.
4. Open the "Downloads" folder and perform a long tap on the OVPN file until a popup window appears. In the popup window, tap "Share".
5. Now select the "OpenVPN Connect" icon.
   The new profile is displayed in the "OpenVPN Connect" app.
6. With "ADD", import the profile and give the profile a name.
   Optionally, you can enter a password.
7. Tap "ADD" to set up the profile for the VPN connection on the iOS device.
   To complete the process, confirm the dialog "OpenVPN wants to add VPN configurations" with "Allow" and authenticate yourself on the iOS device.
   The profile is displayed with the specified name.
8. Tap on the profile and use the slider to establish a VPN connection.
   If a password has been configured, you need to enter it for the connection establishment.

Result:

The OpenVPN profile is enabled in the iOS device. The connection between the iOS device and the SINEMA Remote Connect Server is established using the OpenVPN Connect app.

To terminate the VPN connection again, slide the slider to the left and confirm termination with OK.

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 67)

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 > 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.

Appendix C

C

C.1 Syslog messages

Event Viewer

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

1. Enter "Event Viewer" in the search line of the start menu.
2. Click the "Event Viewer" entry to start the Event Viewer.
3. Click the "Siemens Automation" entry for "Application and Services Logs".
   The log entries are listed in tabular form. When you click on an entry, the detail view opens in the bottom window area.

C.1.1 Tags in Syslog Messages

The Syslog messages can contain variables that are filled dynamically with the data of the respective event. These variables are displayed within curly brackets {variable} in the "Message text" field in section "List of Syslog Messages (Page 176)".

The following variables occur in Syslog messages:

Parameter	Description	Format	Possible values or example
User name	String that identifies the authenticated user based on his/her name without spaces	%s	Peter_Maier
IP address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2	192.168.10.128
Destination user name	String for the name of the destination user. This is not the authenticated user.	%s	Peter_Maier
Device name	String for the name of the device	%s	S615_1
Temp user name	String for the name of the temporary user	%s	Peter_Maier
Cert parameters	String for the certificate parameters	%s	
Role	String for the name of the group role	%s	Technical_Consulting
Group	String for the name of the group	%s	IT_Service
CN Name	String for the parameter host name of the server "commonName"	%s	Server1 192.168.10.10
Config detail	String for the configuration with spaces	%s	the DNS settings the backup settings etc.

Parameter	Description	Format	Possible values or example
File name	String for the file name	%s	2019_04_03_09_53_23.backup
File version	String for the file version	%s	2019_06_13_23_00_01.backup
Software version	String for the installed software version	%s	V3.0.0.0-01.01.00.04
Target software version	String for the loaded software version	%s	V3.0.0-01.01.00.01
Source software version	String for the installed software version	%s	V2.0.1.0-01.01.00.04
Version number	String for the version of the user agreement	%d	1

C.1.2 List of Syslog Messages

C.1.2.1 Identification and authentication of human users

Message text	User {Username} has logged in to {WEB interface}
Example	User "Peter_Maier" has logged in to {web interface}
Explanation	A user has successfully logged into the server via the Web interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	Failed login attempt with {username} from source IP {ip}
Example	Failed login attempt with "Service" from source IP "192.168.16.0"
Explanation	Failed login attempt of the user from the following source IP address
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

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

C.1.2.2 User account management

Message text	User {User name} has deactivated the user {Destination user name}
Example	User "Admin" has deactivated the user "Peter_Maier"

Explanation	A user has disabled a user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} has deactivated the device {Device name}
Example	User "Admin" has deactivated the device "S615_1"
Explanation	A user has disabled a device account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User name} has created the user {Destination user name}
Example	"Admin" has created the user "Peter_Maier"
Explanation	A user has created a user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Temp user name} has been created with {Cert parameters}
Example	"temp_user" has been created with DN= "xxxx"
Explanation	A temporary user account was created.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} has created the device {Device name}
Example	User "Admin" has created the device "S615_1"
Explanation	A user created a device account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {Username} has edited the user {Destination user name}.
Example	User "Admin" has edited the user "Peter_Maier"
Explanation	A user has changed an existing user account or assigned a different role to this account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} has edited the device: {Device name}
Example	User "Admin" has edited the device: "S_615"
Explanation	A user has changed an existing device account.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User name} has deleted the user: {Destination user name}
Example	"Admin" has deleted the user: "Peter_Maier"
Explanation	A user has deleted another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User name} has deleted the device: {Device name}
Example	"Admin" has deleted the device "S615_1"
Explanation	A user has deleted the device.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	Temporary user {User name} is deleted
Example	Temporary user "Temp_User" is deleted
Explanation	An existing temporary user account was deleted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	Temporary user {User name} associated with role {Role} deleted by {User name}
Example	Temporary user "Tempuser" associated with role "vpn" deleted by "Systemadministrator"
Explanation	A user has deleted an existing user account.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} changed the password of device: {Device name}
Example	User "Admin" changed the password of the device: "S615_1"
Explanation	A user has changed the password of a device.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	Debug user password changed
Example	Debug user password changed
Explanation	An authenticated user changed the password for the debug account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} has activated the user {Destination user name}
Example	User "Admin" has activated the user "Peter_Maier"
Explanation	A user has activated the account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User {User name} has activated the device {Device name}
Example	User "Admin" has activated the device "S615_1"
Explanation	A user has enabled a device account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

C.1.2.3 Management of the identifiers

Message text	User {User name} has created the role {Role}
Example	User "Admin" has created the role "IT_Service"
Explanation	The user has created a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {User name} has deleted the role {Role}
Example	User "Admin" has deleted the role "Technical_Consulting"
Explanation	The user has deleted an existing role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {User name} has edited the role {Role}
Example	User "Admin" has edited the role "Technical_Consulting"
Explanation	The user has changed the role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {User name} has deleted the group: {Group}
Example	User "Admin" has deleted the group "IT_Service"
Explanation	The user has deleted the user group.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {user name} has edited the group {Group}
Example	User "Admin" has edited the group "IT_Service"
Explanation	The user has changed the user group.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {User name} has created the role {Role}
Example	User "Admin" has created the role "Technical_Consulting"
Explanation	The user created a new role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	User {user name} has edited the communication destinations of the group {Group}
Example	User "Admin" has edited the communication destinations of the group "IT_Service"
Explanation	The user changed the communication targets of the user group.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

C.1.2.4 Unsuccessful logon attempts

Message text	{IP address} is locked for {Time second} seconds after {Failed login count} unsuccessful login attempts.
Example	192.168.1.105 is locked for 5 seconds after 3 unsuccessful login attempts.
Explanation	If there were too many failed logins, the corresponding IP address was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	Brute force blocking is activated for {user type} {User name}
Example	Brute force blocking is activated for user "Peter_Maier"
Explanation	After multiple failed login attempts, the corresponding user account is locked for a specific time. The default setting for the number of failed login attempts after which the user account is locked is 10.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	Brute force blocking is deactivated for {user type} {User name}
Example	Brute force blocking is deactivated for User "Peter_Maier"
Explanation	The user account is unlocked.

Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

C.1.2.5 Access via untrusted networks

Message text	{User name} rejected due to unsupported client version
Example	"Peter_Maier" rejected due to unsupported client version
Explanation	The client user login was rejected due to a version conflict.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	{Name} connected via OpenVPN
Example	Peter_Maier@8.1 connected via OpenVPN
Explanation	The OpenVPN connection to a device or user is established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	{Name} disconnected via OpenVPN
Example	Peter_Maier@8.1 disconnected via OpenVPN
Explanation	The OpenVPN connection to a device or user is closed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	{Device name} connected via IPsec
Example	"S615_1" connected via IPsec
Explanation	The IPsec connection to a device is established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	{Device name} disconnected via IPsec
Example	"S615_1" disconnected via IPsec
Explanation	The IPsec connection to a device is closed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

C.1.2.6 Identification and authentication of devices

Message text	No valid client with CN {CN Name}
Example	No valid client with CN Device1
Explanation	Device authentication failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	Participiant with CN {CN name} is not allowed to establish OpenVPN connection
Example	Participiant with CN Device1 is not allowed to establish OpenVPN connection
Explanation	Device authentication failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

C.1.2.7 Nonrepudiation

Message text	User {User name} has changed {Config detail}
Examples	"Admin" has changed the system time to 04/03/2019, 11:44:46 "Admin" has changed the settings of the network interface "Admin" has changed the DNS settings "Admin" has changed the settings of the Upload Server "Admin" has changed the backup settings
Explanation	The user changed certain configuration data. Any settings can be specified in the server as configuration details.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	User {User name} rebooting system
Examples	User "Admin" rebooting system
Explanation	The user restarts the system.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	User {User name} has exported the {log type} messages
Examples	User "Admin" has exported the "user log" messages
Explanation	The user exported log messages.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	Connection check to syslog server {IP address} successful
Examples	Connection check to syslog server "172.168.16.10" successful
Explanation	The check of the connection to the Syslog server was completed successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	Connection check to syslog server {IP address} failed
Examples	Connection check to syslog server "172.168.16.10" failed
Explanation	The check of the connection to the Syslog server failed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

C.1.2.8 Data backup in automation system (backup)

Message text	User {User name} has created a new backup : {File name} (Id: {Id}, Comment: {Comment})
Example	User "Admin" has created a new backup: "2019_04_03_09_53_23.backup""ID:4",Comment:"To secure the configuration"
Explanation	The user has created a backup copy on the server.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	Automatic backup copy has been created: {File name}
Example	Automatic backup copy has been created: "2019_04_03_09_53_23.backup"
Explanation	An automatic backup copy was created on the server.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	{User name} has uploaded the backup: {File name}
Example	"Admin" has uploaded the backup: "2019_04_03_09_53_23.backup"
Explanation	The user has uploaded a backup copy.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	User {User name} has deleted the backup: {File name}
Example	User "Admin" has deleted the backup copy: "2019_04_03_09_53_23.backup"
Explanation	The user has deleted a backup copy on the server.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

C.1.2.9 Restoration of the automation system

Message text	User "{username}" has uploaded the backup: "{filename}"
Example	User "Admin" has uploaded the backup: "2019_06_13_23_00_01.backup".
Explanation	The user has imported a backup copy. If the action was successful, no further messages will appear.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	Restore backup failed
Example	Restore backup failed
Explanation	The system could not use the backup file for the restore.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Invalid backup loaded, rejecting...
Example	Invalid backup loaded, rejecting...
Explanation	The restore failed. The loaded backup file is not compatible with the system.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	License resource count is not enough to restore
Example	License resource count is not enough to restore
Explanation	The restore failed due to missing licenses.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	User {User name} has started the restoration from: {File name}
Example	"Admin" has started the restoration from: "2023_04_03_09_53_23.backup"
Explanation	The user has successfully applied the backup file for the restore.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{User name} has started the restoration of the backup copy: {File name}
Example	"Admin" has started the restoration of the backup copy: "2019_06_13_23_00_01.backup"
Explanation	The user started the restore of a backup copy.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	Restored backup version: {File version}
Example	Restored backup version: "2019_06_13_23_00_01.backup"
Explanation	Shows the version information of the loaded backup file.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Upload to the Upload Server was successful.
Example	WBM: Upload to the Upload Server was successful.
Explanation	The backup files were successfully uploaded to the upload server.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	{Protocol}: Upload failed! Upload Server is not reachable. Failed to upload file(s) {File name} to folder at {Destination address}.
Example	Automatic / manual upload: Upload failed! Server is not reachable. Failed to upload file(s) "file1, file2 ..." to folder at 192.168.10.10.
Explanation	The backup file could not be uploaded to the upload server.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	Import of firmware successful: {File name}
Example	Import of firmware successful: "SCALANCE_M800_S615_V06.02.00_30.01_estc.sfw"
Explanation	The device firmware was successfully imported by the user.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{Device name} requests the firmware
Example	"S615_1" requests the firmware
Explanation	The device requested the firmware.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{Device name} has started downloading the firmware
Example	"S615_1" has started downloading the firmware
Explanation	The device is downloading the firmware.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	The file "{File name}" extension is not valid.
Example	The file "SINEMARC_*.iso" extension is not valid.
Explanation	File could not be imported. File extension is not valid.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Import of firmware failed: Integrity check failed!
Example	Import of firmware failed: Integrity check failed!
Explanation	The firmware import failed during the integrity check.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	No imported firmware file in store
Example	No imported firmware file in store
Explanation	Cannot start updating the device because no firmware file has been imported.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	User {User name} is trying to upload the file {filename}. he update file {filename} successfully uploaded
Example	User "admin" is trying to upload the file "SINEMARC_V3.2.0.1-01.01.00.04.tar.gz". The update file "SINEMARC_V3.2.0.1-01.01.00.04.tar.gz" successfully uploaded.
Explanation	The user has uploaded a server update.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Upgrading SINEMA RC to version: {Software version}
Example	Upgrading SINEMA RC to version: 2.0.1.0-01.01.00.04
Explanation	The server is being updated to the specified version.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Sinema RC updated to version {Software Version} successfully.
Example	Sinema RC updated to version 2.0.1.0-01.01.00.04 successfully.
Explanation	The server was updated successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	The update package is not applicable to the current installed version:{Source software version} Installation is possible only on version: {Target software version}
Example	The update package is not applicable to the current version " V3.1.0.0-01.01.00.38" Installation is possible only on version " V3.2.0.0-01.01.00.38".
Explanation	The software activation failed. The loaded software update is not compatible with the installed version.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Failed to apply system update!
Example	Failed to apply system update!
Explanation	The server update failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

C.1.2.10 Network and IT security settings

Message text	Device information sent to {User name}
Example	Device nformation sent to "Peter_Maier"
Explanation	Device information is sent to the client user via the automatic configuration mechanism.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	The OpenVPN configuration was sent to {User name}
Example	The OpenVPN configuration was sent to "Peter_Maier"
Explanation	Die OpenVPN-Konfiguration wird über den automatischen Konfigurationsmechanismus an den Client-Benutzer gesendet.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	Failed login attempt with an anonymous username {User name} from source IP {IP address}
Example	Failed login attempt with an anonymous username "Unknown" from source IP "192.168.16.2"
Explanation	Failed login attempt with an anonymous user name from source IP address.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

25.1_SE_Unable_to_login

Message text	Failed login attempt with username {User name} from source IP {IP address} .
Example	Failed login attempt with username "Service" from source IP "192.168.16.2"
Explanation	Failed login attempt with a user name from source IP address.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Upload to Upload Server

Message text	Upload to Upload Server successful.
Example	Upload to Upload Server successful.
Explanation	Successfully uploaded to the upload server.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	Sending {message_type} to {device_common_name}({address}) via {protocol}
Example	Sending {message_type} to {device_common_name}({address}) via {protocol}
Explanation	The route update was sent to a device or a user due to configuration changes.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	Successfully uploaded file {File names} to folder at {IP address}
Example	Successfully uploaded file "2019_04_03_09_53_23.backup" to folder at "192.168.1.110"
Explanation	The files were successfully uploaded to the upload server (SFTP server).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	{Protocol}: Upload failed! Upload Server is not reachable
Example	Upload failed! Server is not reachable
Explanation	The file could not be uploaded to the upload server (SFTP server).
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

Message text	Failed to upload file {File name} to folder at {IP address}
Example	Failed to upload file "2019_04_03_09_53_23.backup" to folder at "192.168.10.10"
Explanation	The file could not be uploaded to the upload server (SFTP server).
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Message text	{User name} has accepted the user agreement {Version number}
Example	"Peter_Maier" has accepted the user agreement 1
Explanation	The user accepted the user agreement.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3: SR 7.6

Message text	{User name} has refused the user agreement {Version number}.
Example	"Peter_Maier" has refused the user agreement 1
Explanation	The user rejected the user agreement.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6

C.1.2.11 System status

Message text	Syslog server {IP Address} connection status "Online"
Example	Syslog server 192.168.50.10 connection status "Online"
Explanation	The status of a Syslog server was changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3

Message text	Syslog server {IP Address} connection status "Online"
Example	Syslog server 192.168.50.10 connection status "Online"
Explanation	The status of a Syslog server was changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3

Appendix D

D

D.1 Ciphers Used

SINEMA RC Server

Table D-1 HTTPS WBM server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHA-CHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xc060	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xc061	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-2 HTTPS WBM client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_ARIA_128_GCM_SHA256	0xc05c	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	0xc05d	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xc060	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xc061	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-3 OAuth/OpenID via HTTPS WBM Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	0xc05c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	0xc05d	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xc060	✓
Encryption suite	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xc061	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-4 OAuth/OpenID via Entra ID

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	0xc05c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	0xc05d	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-5 UMC client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1.2	-	✓

Table D-6 SMTP client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-7 Syslog client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	✓
Protocol version	TLSv1	.	✓
Protocol version	TLSv1.1	.	✓
Protocol version	TLSv1.2	.	✓

Table D-8 OpenVPN server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓

Category	IANA name	Hexadecimal value	Enabled by default
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

Table D-9 SSH server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	n/a	✓
Host key (key)	ssh-ed25519	n/a	✓
Key exchange (kex)	curve25519-sha256	n/a	✓
Key exchange (kex)	ecdh-sha2-nistp256	n/a	✓
Key exchange (kex)	ecdh-sha2-nistp384	n/a	✓
Key exchange (kex)	ecdh-sha2-nistp521	n/a	✓
MAC	hmac-sha2-256-etm@openssh.com	n/a	✓
Protocol version	SSHv2.0	n/a	✓

Table D-10 SFTP server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption method (enc)	chacha20-poly1305@openssh.com	n/a	✓
Encryption method (enc)	aes128-ctr	n/a	✓
Encryption method (enc)	aes192-ctr	n/a	✓
Encryption method (enc)	aes256-ctr	n/a	✓
Encryption method (enc)	aes128-gcm@openssh.com (AEAD_AES_128_GCM)	n/a	✓
Encryption method (enc)	aes256-gcm@openssh.com (AEAD_AES_256_GCM)	n/a	✓
Host key (key)	ssh-ed25519-cert-v01@openssh.com	n/a	✓
Host key (key)	ecdsa-sha2-nistp256-cert-v01@openssh.com	n/a	✓
Host key (key)	ecdsa-sha2-nistp384-cert-v01@openssh.com	n/a	✓
Host key (key)	ecdsa-sha2-nistp521-cert-v01@openssh.com	n/a	✓
Key exchange (kex)	curve25519-sha256	n/a	✓
Key exchange (kex)	curve25519-sha256@libssh.org	n/a	✓

Category	IANA name	Hexadecimal value	Enabled by default
Key exchange (kex)	ecdh-sha2-nistp256	n/a	✓
Key exchange (kex)	ecdh-sha2-nistp384	n/a	✓
Key exchange (kex)	ecdh-sha2-nistp521	n/a	✓
Key exchange (kex)	diffie-hellman-group-exchange-sha256	n/a	✓
Key exchange (kex)	diffie-hellman-group16-sha512	n/a	✓
MAC	hmac-sha2-256-etm@openssh.com	n/a	✓
MAC	hmac-sha2-512-etm@openssh.com	n/a	✓
MAC	hmac-sha2-512-96	n/a	✓
Protocol version	SSHv2.0	n/a	✓

Table D-11 SMTP client

Category	IANA name	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	n/a	--
Authentication	HMAC-SHA-96	n/a	--
Encryption	des-cbc	n/a	--
Encryption	aes128-cbc	n/a	--

Table D-12 IPSec (IKEv2) server

Category	IANA name	Hexadecimal value	Enabled by default
IKE authentication	hmac-SHA256	n/a	--
IKE authentication	hmac-SHA384	n/a	--
IKE authentication	hmac-SHA512	n/a	--
IKE DH groups	Group 1 (modp768)	n/a	--
IKE DH groups	Group 2 (modp1024)	n/a	--
IKE DH groups	Group 5 (mod1536)	n/a	--
IKE DH groups	Group 14 (modp2048)	n/a	--
IKE DH groups	Group 15 (modp3072)	n/a	--
IKE DH groups	Group 16 (modp4096)	n/a	--
IKE DH groups	Group 18 (modp8192)	n/a	--
IKE encryption	aes128-GCM	n/a	--
IKE encryption	aes192-GCM	n/a	--
IKE encryption	aes256-GCM	n/a	--
IKE encryption	aes128-CCM	n/a	--
IKE encryption	aes192-CCM	n/a	--
IKE encryption	aes256-CCM	n/a	--

Table D-13 IPSec (ESP) server

Category	IANA name	Hexadecimal value	Enabled by default
ESP/AH authentication	SHA256	n/a	--
ESP/AH authentication	SHA384	n/a	--
ESP/AH authentication	SHA512	n/a	--
ESP encryption	aes128-GCM	n/a	--
ESP encryption	aes192-GCM	n/a	--
ESP encryption	aes256-GCM	n/a	--
ESP encryption	aes128-CCM	n/a	--
ESP encryption	aes192-CCM	n/a	--
ESP encryption	aes256-CCM	n/a	--
ESP encryption	aes128-ctr	n/a	--
ESP encryption	aes192-ctr	n/a	--
ESP encryption	aes256-ctr	n/a	--
ESP encryption	aes128-cbc	n/a	--
ESP encryption	aes192-cbc	n/a	--
ESP encryption	aes256-cbc	n/a	--

SINEMA RC Client

Table D-14 HTTPS client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006b	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xc023	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xc0ac	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xc024	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xc0ad	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Table D-15 OpenVPN client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006b	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA256	0xc023	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA384	0xc024	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Protocol version	TLSv1.2	.	✓
Protocol version	TLSv1.3	.	✓

Index

M

N

O

P

R

S

T

U

V

W