SIEMENS

# SIMATIC NET

# Industrial Remote Communication SINEMA Remote Connect - Server

Operating Instructions




04/2016

C79000-G8976-C383-03

# Legal information

## Warning notice system

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

**⚠ DANGER**

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

**⚠ WARNING**

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

**⚠ CAUTION**

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

**NOTICE**

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

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

## Qualified Personnel

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

## Proper use of Siemens products

Note the following:

**⚠ WARNING**

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

## Trademarks

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

## Disclaimer of Liability

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

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

C79000-G8976-C383-02
℗ 06/2016 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 V1.0

## Article numbers - licenses

The following licenses are available for the product:

| Product name | Article number | 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 |

Also available for enabling connection to the SINEMA Remote Connect server:

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

## Supported devices

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

- SCALANCE M-800 as of firmware version V4.1
- SCALANCE S615 as of firmware version V4.0
- SINEMA RC Client
- SCALANCE S612, SCALANCE S623, SCALANCE S627-2M

## Abbreviations/acronyms and terminology

- **SINEMA RC**

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

- **SCALANCE M-800**

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

  – SCALANCE M874-2
  – SCALANCE M874-3
  – SCALANCE M876-3
  – SCALANCE M876-4
  – SCALANCE M812
  – SCALANCE M816

## New in this release

- Support of IPsec
- Power management
- Server upload

## Replaced documentation

None

## Required experience

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

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

## Further documentation

- Operating instructions "SINEMA Remote Connect Client"

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

- Getting Started "SINEMA Remote Connect"

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

## Current manuals and further information

You will find the current manuals and further information on telecontrol products on the Internet pages of Siemens Industry Online Support:

- Using the search function:

  Link to Siemens Industry Online Support (http://support.automation.siemens.com/WW/view/en)

  Enter the entry ID of the relevant manual as the search item.

- via the navigation in the "Telecontrol" area:

  Link to the area "Telecontrol" (https://support.industry.siemens.com/cs/ww/en/ps/15915)

  Go to the required product group and make the following settings:
  "Entry list" tab, Entry type "Manuals"

You will find the documentation for the products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

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

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

## Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

## SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following address:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

## Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SINEMA, SCALANCE

# Table of contents

# Application and properties

# 1

## 1.1 Application

### Use of the SINEMA Remote Connect server

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

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

The connection via the Internet/WAN to the WBM uses the HTTPS protocol. To establish a connection to the WBM of the server, users must authenticate themselves by entering a user name and password.

### Connectable end devices

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

- SCALANCE M
- SCALANCE S615
- SINEMA RC client

### Protection concept

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

- Users and passwords

  The users are assigned various roles. Access is password protected, see section Create a new user (Page 63).

- User rights

  Different permissions and rights are assigned to the various user types. For more detailed information, refer to the section Managing roles and rights (Page 61).

# 1.2 Overview of functions

## Configuring the SINEMA Remote Connect server

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

### Configuration of the SINEMA RC Server

In the WBM, you can use the following functions:

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

### Commissioning/configuration of end devices

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

### Management of the server

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

### Connection management

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

## 1.3 User concept

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

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

**Note**

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

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

### Administrator

After installation specify the user name and the password for the administrator. This administrator has the right to access all functions. The administrator has technical responsibility for the system. Only the administrator can set up the system. This includes creating users and assigning roles and rights to them. For more detailed information, refer to the section "Managing roles and rights (Page 61)".

The administrator cannot be deleted.

### Users

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

## Basics

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

- Users
- Roles
- Rights

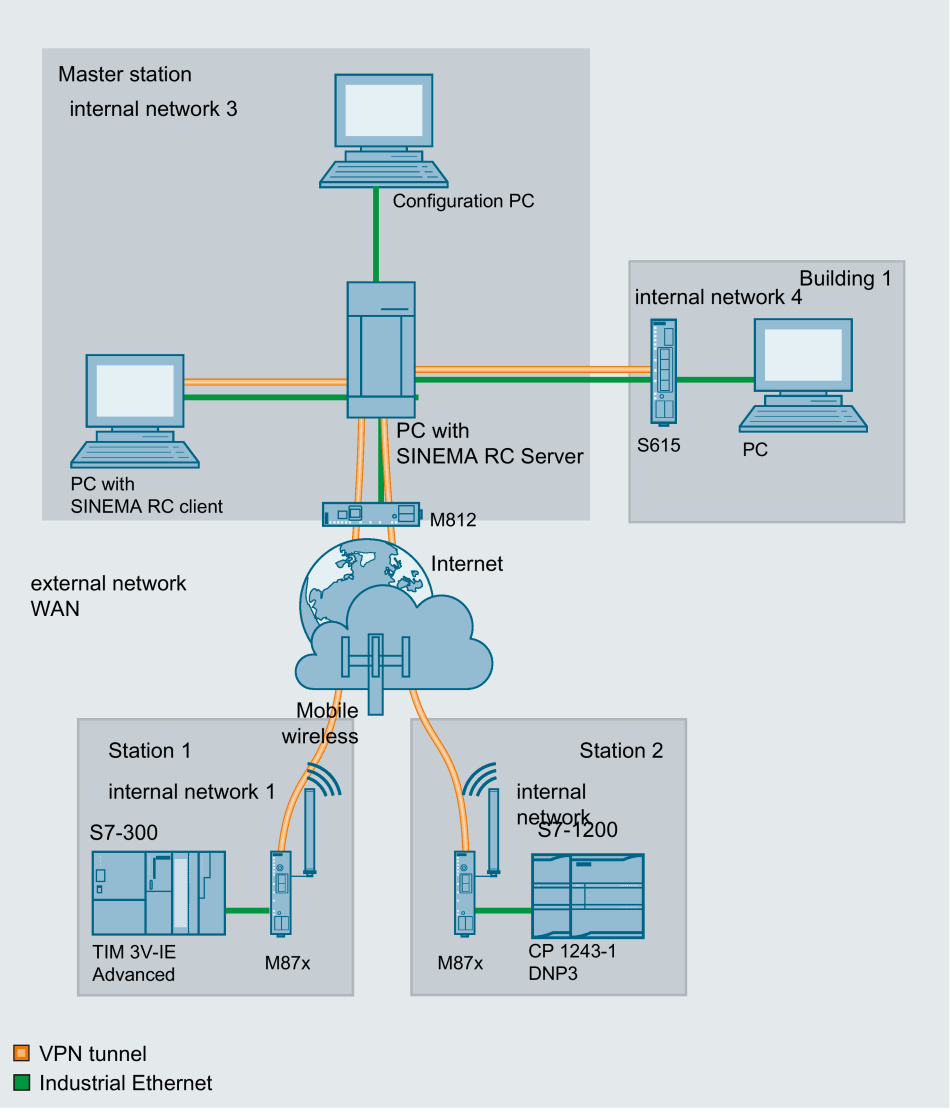
In principle, the following applies: Every user can be assigned certain rights. Every role can be assigned various rights that are transferred automatically to all its members (users).

# 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.

# Requirements for operation

# 2

## 2.1 Requirements

### Hardware requirements

| Component | Minimum requirements | Recommended requirements |
|---|---|---|
| Processor | Intel Dual Core CPU 2.4 GHz | Intel Quad Core CPU 2.66 GHz |
| RAM | 2 GB | 4 GB |
| Network adapter | 1 | 1<br>**Note:** SINEMA RC Server supports up to four network adapters. |
| Hard disk | 30 GB | > 50 GB |

### Used hardware of the vSphere Server (ESXi 5.5)

| Component | PC 847D (6AG4114-2KV83-0XX6) |
|---|---|
| Processor | Xeon E3-1268L v3 (4C/8T, 2.3 (3.3) GHz, 8 MB cache, VT-d, AMT) |
| RAM | 32 GB DDR3 SDRAM (4X 8GB) |
| Network adapter | 2x Gbit Ethernet (IE/PN) |
| Hard disk | RAID5, 2 TB(3x 1 TB HDD SAS, Stripping with Parity), in the removable drive bay, hot swap; and 1 TB HDD SAS as hot spare in the removable drive bay |

### See also

Using a "virtual machine" (Page 84)

## 2.2 License information

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

### Licenses

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

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

### License update

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

The procedure for activating the license in the WBM is described in the section "Managing licenses (Page 40)".

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

How many connections can actually be established simultaneously depends on the hardware of the PC.

# 2.3 Permitted characters

## User names, passwords

When creating or changing, remember the following rules:

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

**Note**

**User names and passwords**

As an important measure to increase security, make sure that user names and passwords are as long as possible.

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

## Hostname

| | |
|---|---|
| Permitted characters | The following characters from the ANSI X 3.4-1986 character set are permitted:<br>0123456789<br>A...Z a...z<br>-. |
| Characters not allowed | " ' `!#$%&()*+,/:;<=>?@[\]_{\|}~^ |

## 2.4 Performance data

| | |
|---|---|
| Maximum number of participant groups | Unlimited |
| Maximum number of participants per participant group | Unlimited |
| Maximum number of local backup copies | 30 |
| Maximum number of log archives | 100 |

**Note**

**Communication relations**

SINEMA RC supports a maximum of 100 communication relations to a device or user (SINEMA RC Client).

The number of communication relations is made up as follows:

- The participants of your own group. Assuming that the participants can communicate with each other.
- The number of participants in the destination group to which your own group has a communication relation.

Everything going beyond 100 communication relations is discarded by the device or SINEMA RC Client.

# Installation and commissioning 3

## 3.1 Security recommendations

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

### General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.

### Access to the server

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

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

### Physical access

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

### Security functions of the software

- Keep the software up to date.
  - Check regularly for security updates for the product. You will find information on this at:
    http://www.siemens.com/industrialsecurity
  - Check regularly for updates for the product. You will find information on this at:
- The SINEMA RC Server includes an automatic logging function. Check this information regularly for unauthorized access.

### Passwords

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

### Keys and certificates

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

- We recommend that you use certificates with a key length of 4096 bits.

## 3.2 Installing SINEMA RC Server

| NOTICE |
| --- |
| **Installation formats the hard disk**<br>The installation of the SINEMA RC Server includes its own operating system. If you use a PC on which an operating system already exists, the hard disk will be formatted. This means that existing data is lost. Make sure that all important data on the PC has been backed up. |

### Requirement

- In the startup order, the CD/DVD is set as the first boot medium.

### Sequence

1. Turn on the PC.
2. Insert the data medium in the drive. Installation starts automatically.
3. Follow the further instructions on the screen.

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

   – IP address
   – Network mask
   – Gateway

### Result

The SINEMA RC Server is installed. You can configure the other settings using the WBM.

## 3.3 Initial commissioning of end devices using the WBM

### Commissioning and devices via the WBM:

Follow these steps:

1. Configure the new device on the SINEMA RC Server. For more detailed information, refer to the section I Create new device (Page 49).
   - 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 58).

   When the device is configured, the certificate is created automatically. For more detailed information, refer to the section Overview of certificate management (Page 65).
2. Configure 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: e.g. creation of firewall rules, NAT

You will 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 bar of the browser enter **https**://<IP address>. You specify the IP address during 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 Start of the WBM - changing the password

### Logging on

After calling the Web user interface, the logon window appears:

1. Enter a configured user name.

   You will find information on the first logon in the next section.

2. Enter the corresponding password.

   You will find information on the first logon in the next section.

3. Click the "Log on" button.

   The start page of the WBM opens.

### Initial logon: User name and password

1. After installation, log in with the user name "admin" and the password "admin".
2. After logging on, 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 17)".

   As administrator, you can change the settings of the device (read and write access to the configuration data).

4. Click the "Save" button.

   After saving, you are automatically logged on with the newly created administrator.

#### Changing the current password

As a logged-on user, you can change your current password, refer to the section "Changing the current password (Page 80)".

## 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. One or a variety of incorrect user names can be entered any number of times without the system being locked.

**Note**

**Loss of the administrator password**

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

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

**There is no possibility of resetting the assigned administrator password.**

**Note**

**Incorrect entry of the password**

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

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

# 4.3 Layout of the window

## View of the Start page

When you enter the IP address, the start page is displayed after a successful login. You cannot configure anything on this page.

## General layout of the WBM page

The following areas are available on every WBM page:

## Header area ①

The following is available in the header area:

- Logo of Siemens AG
- Product name
- Drop-down list for language selection
- Button Help

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

## Logon area ②

The following is available in the logon area:

- **Logged on as**

  Display of the user name under which you are logged on.

- **Logout**

  You can log out from any WBM page by clicking the "Log off" link.

- **"Update" button**

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

  **Note**

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

## Navigation area ③

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

**Note**

Depending on the rights you have been assigned, not all submenus are available to you. For more detailed information on the user concept, refer to the section "User concept (Page 11)".

### Exiting the submenu with "Exit dialog"

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

## Content area ④

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

**Buttons you require often**

The WBM pages contain the following standard buttons:

- **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 61)".

  **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.

- **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.

## 4.4 Start page of the Web user interface

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

### Update of the displayed values

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

### Calling the Web page

In the navigation, select "System > Overview".

### Displayed entries

The following entries are displayed:

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

# 4.5 Language selection

## Changing the language setting

1. Open the drop-down list for the language setting at the top right of the start page.
2. Select the required language.

**Result**

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

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

# 4.6 System

## 4.6.1 Log

### 4.6.1.1 Log messages

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

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

#### Calling the Web page

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

#### Displayed entries

The following entries are displayed:

| Box | Meaning |
|---|---|
| Date | Time stamp with the date and time |
| Message level | The message levels are possible:<br>• Emergency<br>• Alert<br>• Critical<br>• Error, e.g. when the export of the server certificate fails<br>• Warning, e.g. when a CA is deleted<br>• Notice, e.g. when a CA is created<br>• Info, e.g. when a user has logged on<br>• Debug |
| Function | Coded operating status |
| Category | Category of the log message |
| Message | Displays a description of the event that has occurred. |

## Filtering log entries

1. Select the required level from the "Message level" drop-down list.
2. Select the required category in the "Category" drop-down list.
3. Click the "Apply filter" button.

**Result**

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

## Saving log entries

**Note**
**Saving log entries**

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

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

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

**Note**
**Protecting exported log files from unauthorized access**

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

#### 4.6.1.2 Log archives

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

### Calling the Web page

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

### Displayed entries

The following entries are displayed:

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

## 4.6.2 Network configuration

### 4.6.2.1 Interfaces

**Note**

**IPv4 addresses and netmask according to RFC 1918**

The factory-set IPv4 addresses and netmasks can be changed as required, but must keep to the specification RFC 1918.

### Calling the Web page

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

## Configuring the interface

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

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

## Additional settings for the WAN interface

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

### 4.6.2.2 DNS

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

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

The setting is also required for licensing.

#### Calling the Web page

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

#### Creating a new DNS server

Make the following settings and then click the "Save" button:

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

### 4.6.2.3 Web server settings

#### Calling the Web page

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

#### Changing the port for HTTPS remote access

Specify via which port HTTPS remote access to the WBM will take place. Then click the "Save" button.

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

If you use a port other than 443 as the HTTPS standard port, the port number along with the IP address needs to 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

## 4.6.3 Setting the date and 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 settings".

### Setting the time manually

You set the date and time of the system in the "Manual" tab:

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

### Automatic time-of-day setting with NTP

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

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

## 4.6.4 SMS messages and e-mails

### 4.6.4.1 SMS gateway provider

To wake a station, the SINEMA RC Server sends an e-mail. The e-mail is sent to an SMS gateway via an SMTP server. 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.

**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 86).

#### 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

| Box | Meaning |
|---|---|
| Name | Name of the SMS gateway provider |
| Address | Email address of the recipient of the SMS message<br>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 85)"<br>Check with your network provider whether or not it is necessary to send an activation SMS message.<br>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<br>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.<br>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. For address, enter the e-mail address of the recipient. For the phone number, use the placeholder "$SMS-NO".
4. As the "Subject" or "Text" enter the placeholder "$MSG". This depends on your network provider.
5. Click the "Create" button.

## 4.6.4.2 SMTP client

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.

SINEMA RC provides the option of automatically sending an e-mail if an alarm event occurs for example to the network administrator.

**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".

### Making settings for the SMTP client

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

| Box | Meaning |
|---|---|
| Method of delivery | Direct: The e-mail is forwarded directly to the SMTP server.<br>Via relay host: 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.<br>With the transmission method relay host, the e-mail address of the user account of the SMTP relay server is specified. |

### Additional settings for the transmission method "Via relay host"

Enter the following additional access data of the SMTP server:

| Box | Meaning |
|---|---|
| SMTP relay server | Enter the name or the IP address of the SMTP relay server that is intended to forward the received e-mails. |
| SMTP relay port | Specify the port on which the SMTP relay server accepts connections. As default port 587 is set so that mail is received only from authenticated users. |
| Transport Layer Security (TLS) | Specify whether the e-mails are transferred unencrypted via TSL:<br>• Opportunistic: The e-mail can be transferred encrypted via TSL. If the receiving mail server does not support encrypted transfer, the e-mail is forwarded via an unencrypted connection.<br>This setting is used automatically if you have selected "Direct" as the Transmission method.<br>• Binding: The e-mail is transferred encrypted via TSL. If the receiving mail server does not support encrypted transfer, the e-mail is not forwarded. |
| Server requires authentication | Some SMTP relay servers require a login. Enter the user name and the password. Some providers use the e-mail address as the user name. You will obtain more detailed information from your provider. |

### 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.

## 4.6.5 Managing licenses

On this page you obtain an overview of the existing licenses. You can also activate new license packages and deactivate existing licenses. You will find an overview of the available licenses in the section "License information (Page 16)".

### Calling the Web page

In the navigation, select "System > Licenses".

### Displayed entries

A list of the existing licenses is displayed:

| Box | Meaning | |
|---|---|---|
| License type | Name of the license package | |
| Ticket number | Ticket number used when the license was activated. | |
| Activation Date | Date on which the license was activated. | |
| License value | Number of currently activated participants and how many participants can be configured in total. | |
| Status | • Active: The license is activated and is being used.<br>• 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". |

### Activating a license

#### Requirements

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

#### Procedure

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

#### Result

The system of checks whether the ticket number is valid and which license package is activated with it.

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

### Enabling the license

For if you change the system, you can return undamaged licenses.

**Requirements**

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

**Procedure**

1. Select the required license.
2. Click the "Enable license" button.

**Result**

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

## 4.6.6 System update

If a new version is available for the SINEMA RC Server, you will find the update on the Internet pages of Siemens Industry Online Support:
http://support.automation.siemens.com/WW/view/en/2173

Under "Entry type", select "Download".

The update must be performed in the correct order:

- From V1.0 to V1.1
- From V1.1 to V1.2

### Requirement

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

### Calling the Web page

In the navigation, select "System > Update".

### Updating the system

With this function, you update your existing system.

1. Click the "System update " tab.
2. Click the "Select file" button.
3. Navigate to the storage directory and select the file *.tar.gz.

4. Confirm your selection with the "Open" button.
5. Click the "Import" button.

**Result**

The system has been updated. Depending on the type of update, individual functions, or the entire system is restarted.

To check the version following the restart, in the navigation click "System > Overview" and check the displayed software version.

### Shutting down the system

On the "Power management" tab you have the following options for shutting down the system:

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

## 4.6.7 Server upload

This page provides you with the option of loading the configuration file and log files from the PC to the SINEMA RC using SFTP. SFTP stands for Secure File Transfer Protocol.

### Calling the Web page

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

### Displayed entries

| Field | Meaning |
|---|---|
| Automatic file upload | When enabled the files are uploaded to the SINEMA RC using SFTP. |
| Files for upload | Specify which files are to be uploaded:<br>• Configuration file<br>• Log file<br>• Configuration file and log fle |
| SFTP server name | IP address of the SFTP server |
| Fingerprint SFTP server | Before establishing the connection the SFTP server transfers its fingerprint. The fingerprint is generated from its private key. This ensures that the data is exchanged with the correct SFTP server. |
| Upload directory: | Storage directory of the file |
| User name | User name for access to the SFTP server |
| Password | Password for access to the SFTP server |

## 4.6.8 Backup copy & restoring the system

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 can be saved as a file in the format *.backup and imported into another system.

**Note**

**System settings that are not taken**

When you create backup copies, the log messages are not included.

### 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 panel, select "System > > Backup & restore".

### Displayed entries

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

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

## Configuring settings for backup copies

Requirement:

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

**Procedure**

1. In the navigation panel, select "System > Backup & restore" and the "Settings" tab.
2. Enter the number of permitted backup copies.
3. An entry between 10 and 30 is permitted. When the maximum number is reached, the oldest backup copy is overwritten.
4. If the system should be backed up at regular intervals, specify the interval and the time for the backup.
5. Enter a "coding 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 17)".
6. Confirm the coding key.
7. Click the "Save" button.

## Creating a new backup copy

Requirement:

- The settings for the backup copies are configured.

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

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

**Result**

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

## Importing a file with a backup copy

**Note**

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

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

1. Click the "Import backup copy" button.
2. In the dialog that follows, if required enter a comment on the backup copy.
3. Click the "Browse" button.
4. Select the required file in the format *.backup and confirm your selection with the "Open" button.
5. Click the "Finish" button.

**Result**

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

# 4.7 Remote connections

## 4.7.1 Managing devices

### 4.7.1.1 Overview of device management

In this tab, you can create devices. After creating the device, you can assign it to individual participant groups. Prior to creating the devices it therefore makes sense to create the individual groups first (refer to the section ""Creating participant groups (Page 56)").

**Note**

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

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

### Requirement

- The user is assigned the right "Manage devices"

### Calling the Web page

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

## Displaying entries

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

| Box | Meaning | |
|---|---|---|
| Name of the device | Name of the device | |
| VPN address | The IP address of the device used during communication via VPN. The address is automatically assigned by SINEMA RC. If communication via VPN is not active, " none is displayed. | |
| Remote subnet | The IP address of the remote subnet. If the option "Connected local subnets" is not enabled, "none" is displayed, refer to the section "Creating a new device (Page 49)".<br>If several IP addresses are created, ⊞ is displayed. If you hover over ⊞ with the mouse pointer, this information is displayed. | |
| Virtual local LAN | 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 49)".<br>If several IP addresses are created, ⊞ is displayed. If you hover over ⊞ with the mouse pointer, this information is displayed. | |
| Status |  | The device is connected to SINEMA RC server via VPN. |
| |  | The device is not connected to SINEMA RC server via VPN. |
| Location | Location of the device. This can, for example, be the installation location of the device. | |
| Type of connection | Shows when the connection will be established.<br>1. Permanent: The VPN connection exists permanently:<br>2. Digital input: The VPN connection is established as soon as a signal is applied to the "digital input".<br>3. Wake-up SMS: An alarm SMS message is sent to the device.<br>4. Digital input & Wake-up SMS | |
| VPN connection mode | Shows which protocol is being used for the VPN connection.<br>1. OpenVPN: The connection will be established via OpenVPN.<br>2. IPsec: The connection will be established via IPsec. | |
| Actions |  | You obtain an overview of the device information.<br>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. |
| |  | Changing device settings |
| |  | The configuration file with the OpenVPN settings for this device is created and can be saved. The file can be exported to the end device. |
| |  | A password protected PKCS#12 file is created and can be saved. The certificate is derived from the last valid CA. The file contains the private key of the device with the corresponding certificate. The file can be exported to the end device. When the password is queried, enter the password you specified when you created the device (refer to the section "Creating a new device (Page 49)"). |
| |  | The certificate and the key are stored as Base64-coded ASCII text. |
| |  | Displays the participant group to which the selected device is assigned. |

| Box | Meaning | |
|---|---|---|
| | | Deactivate device.<br>• If the device is connected, the existing connection is also deactivated.<br>• 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".<br>• If the device is not connected, the SINEMA RC Server sends the wake-up SMS message to the device. |

## Creating a device

To create devices, the options are as follows:

- Creating directly in the WBM

  Click the "Create" button and configure the required settings, see .Creating a new device (Page 49).

- Creating using a CSV file

  The required settings are stored in a csv file. With the "Import" button, the file is loaded on the SINEMA RC Server and the devices are created according to the settings, refer to Creating several devices (Page 53).

## Filtering entries

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

**Result**

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

### 4.7.1.2 Create new device

## Procedure

1. Click the "Create" button on the page of the device list.
2. **Configure device setting**
   - Specify the following for the device.

| Box | Meaning |
|---|---|
| Name of the device | Enter a unique name. |
| Type of connection | 1. Permanent: The VPN connection exists permanently:<br>2. Digital input: The VPN connection is established as soon as a signal is applied to the "digital input".<br>3. Wake-up SMS: An alarm SMS message is sent to the device.<br>4. Digital input & Wake-up SMS |
| SMS gateway provider | Can only be selected with the type of connection "Wake-up SMS" or "Digital input & Wake-up SMS".<br>Select the SMS gateway provider. You configure the gateway provider in "System > SMS & e-mail" |
| GSM number | For SCALANCE M-800 with SIM card:<br>Call number of the end device to which the wake-up SMS is sent. |

   - If required, enter additional device information and click the "Continue" button..

3. **Configuring the VPN connection mode**
   – Set the following parameters:

| Field | Meaning |
|---|---|
| VPN connection mode | Specify which protocol will be used for the VPN connection.<br>1. OpenVPN: The connection will be established via OpenVPN. You configure the settings in "Security > VPN basic settings > OpenVPN".<br>2. IPsec: The connection will be established via IPsec. |
| IPsec profiles | Can only be selected in the "IPsec" connection mode. You configure the IPsec profiles in "Security > VPN basic settings > IPsec profile". |
| Request virtual IP address | When enabled, a virtual IP address is requested during connection establishment.<br>• OpenVPN: The setting is always enabled and cannot be modified.<br>• IPsec: Enable or disable the setting. |
| Fixed IP address | The IP address that is always assigned to the device. Via the VPN connection, the device can always be reached at this address.<br>This is only possible when the parameter "Activate fixed IP address space" is enabled.<br>The parameter depends on the VPN connection mode.<br>• OpenVPN: Remote connections > Address spaces > OpenVPN<br>• IPsec: Remote connections > Address spaces > IPsec |
| OpenVPN connection parameters | Can only be configured in the "OpenVPN" connection mode.<br>Only necessary when the WAN IP address of the SINEMA RC Server is translated with NAT.<br>• IP address of the connection<br>Enter the IP address via which the SINEMA RC Server can be reached.<br>• Port of the connection<br>Enter the port at which the SINEMA RC Server receives the OpenVPN connection.<br>• IP protocol<br>Specify whether the OpenVPN connection goes via TCP or UDP.<br>• Actions<br>To delete, click on ✖ in the actions. |

| Field | Meaning |
|---|---|
| IPsec connection parameters | Can only be configured in the "IPsec" connection mode.<br>• Authentication:<br>– CA Cert: CA certificate<br>The certificate of the certification authority is used for authentication. You specify the certificate in "Certificate".<br>• Certificate<br>Select the CA certificate for the IPsec connection. Only imported certificates can be selected<br>• Local ID<br>Enter the local ID. Necessary when the VPN tunnel partner evaluates the entry.<br>• ID of the partner<br>Specify the ID of the partner. Necessary when the VPN tunnel partner evaluates the entry. |

– Click the "Continue" button.

4. **Using the local subnet**

– If the subnet downstream from the device also needs to be exported, enable the check box "Connected local subnets".

– Enter the following connection parameters as well:

| Box | Meaning |
|---|---|
| Local IP address | IP address at which the device in the remote subnet can be reached. |
| Network mask | The network mask of the remote subnet. |
| Device is a network gateway | The device in the remote subnet is a network gateway.<br>When enabled, "Yes" is displayed for network gateway in the tables. |

– Click the "Add" button. The IP address of the remote subnet is displayed in the table.

– To change an entry, you must first delete this entry and then create a new one. To delete, click on ✖ in the actions.

5. **Using NAT for the local subnet**
   - Enable the option "NAT for local subnet" if the device in the remote subnet is to be assigned a NAT IP address.
   - Enter the following parameters as well.

| Box | Meaning |
|---|---|
| Virtual local LAN IP address | NAT IP address at which the device in the remote subnet can be reached. |
| Network mask | The network mask of the virtual local subnet. |
| Local subnet | The IP address of the remote subnet to which the NAT IP address is assigned. |

   - Click the "Add" button. The table shows the NAT IP address at which the IP address of the device can be reached.
   - To change an entry, you must first delete this entry and then create a new one. To delete, click on ✖ in the actions.
6. **Using NAT for local hosts**
   - Enable the option "NAT for local hosts" if a specific destination IP address in the remote subnet needs to be reached via the NAT IP address of the device.
   - Enter the following parameters as well:

| Box | Meaning |
|---|---|
| Virtual local LAN IP address | Select the subnet matching the NAT IP address of the device. |
| Local host | The destination IP address to be reached in the remote subnet. |

   - Click the "Add" button. The table shows the NAT IP address at which the destination IP address can be reached in the remote network.
   - To change an entry, you must first delete this entry and then create a new one. To delete, click on ✖ in the actions.
7. Click the "Continue" button.
8. Select one or more groups to which the device will be assigned. You will find information on creating groups in the section "Creating participant groups (Page 56)".
9. Click the "Continue" button.
10. Enter a password and confirm it. See also the guidelines in the section "Permitted characters (Page 17)".
11. Click the "Continue" button. Check your settings and click the "Finish" button.

### 4.7.1.3 Creating several new devices

#### Requirement

- The csv file exists and is filled correctly, see Structure of the csv file (Page 87).
- The activated license is adequate, see Managing licenses (Page 40).

#### Importing a csv file

1. Click the "Import" button on the page with the device list.
2. Click the "Browse" button and select the csv file.
3. Click "Import".

**Result**

Before it is imported, the csv file is checked to make sure it is correct. After importing the file, the devices are listed on the "Device selection" tab. The devices have not yet, however, been created on the SINEMA Server.

#### Creating a device

1. Check the status of the devices. The devices can have the following status.

| Symbol | Status | Description |
|---|---|---|
|  | Valid | All settings are OK. The device can be created without problems. |
|  | Warning | A device with this name already exists.<br>The settings of this device will be overwritten by the settings from the csv file. |
|  | Invalid | The device cannot be imported. Either there is a conflict in the network settings or the participant group does not exist.<br>If you hover over the symbol with the mouse pointer somewhat longer, the name of the device with which the conflict exists will be displayed. |

2. Select the required devices.
3. Enter a password and confirm it. See also the guidelines in the section "Permitted characters (Page 17)".
4. Click "Finish".

**Result**

The devices will be created on the SINEMA RC Server. Depending on how many devices you have selected, creating them may take some time.

### 4.7.1.4 Updating devices

On these pages you can load the update file with the new firmware (*.swf) on the device and start the update process.

## Calling the Web page

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

## Displayed entries

A list of the devices that support this function is displayed.

| Box | Meaning | |
|---|---|---|
| Name of the device | Name of the device | |
| Last known firmware version | The firmware version that the device transferred to the SINEMA RC Server. | |
| Last known request of the firmware | Provides information when the device last requested the firmware. | |
| Status |  | The device is connected to SINEMA RC Server via VPN. |
| |  | The device is not connected to SINEMA RC Server via VPN. |
| Actions |  | Deactivate device.<br>• If the device is connected, the existing connection is also deactivated.<br>• If the device attempts to establish a VPN connection, the device is ignored by the SINEMA RC Server. |

## Updating firmware

1. Click on the "Firmware file" tab.
2. Click the "Select file" button.
3. Navigate to the storage directory and select the update file (*.swf).
4. Confirm your selection with the "Open" button and click the ".Import" button.
5. Click on the "Devices" tab.
6. Select the devices to be updated.
7. Save your selection.

Result:

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

## 4.7.2 Address spaces

### 4.7.2.1 Network address space

On this page you define the address space for the virtual local LAN.

**Note**

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

#### Calling the Web page

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

#### Manage address spaces

| Box | 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<br>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) | Virtual local LAN:<br>Number of available networks determined from the start address and the end address. |

So that the address space is used for the virtual local LAN, enable the setting "Activate the network address space" on the "Virtual local LAN" tab.

### 4.7.2.2 VPN address spaces

On this page you define the address spaces for TCP, UDP and IPsec. When a VPN client logs on to SINEMA RC Server, this receives an IP address from the address space for the time of the connection.

**Note**

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

#### Calling the Web page

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

### Manage address spaces

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

| Box | 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<br>The address space is limited by the start address and the network mask. The end address must be within this range. |
| Use (assigned IPs / of total) | The following is displayed:<br>• Number of available IP addresses and<br>• how many of these IP addresses are assigned. |
| Activate the network address space | When enabled the device can be assigned a fixed IP address from the address space. |
| Fixed IP protocol | Only with OpenVPN:<br>• TCP: Applies to OpenVPN connections via TCP<br>• UDP: Applies to OpenVPN connections via UDP |
| Location of the fixed IP address space: | • First: The fixed IP addresses are from the starting area of the address space. The first IP address is reserved for the SINEMA RC Server.<br>The first fixed IP address is always the second IP address after the start IP address.<br>• 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 |

## 4.7.3 Creating node groups

Users and devices can be put together in participant groups. A user or a device can be assigned to more than one participant group. You also specify whether the communication between the participants of an individual group is permitted or forbidden.

Once the participant groups have been created, you can define communication relations between the groups (see section "Communication relations between participant groups (Page 58)").

### Requirement for creating participant groups

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

### Calling the Web page

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

## Displayed entries

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

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

## Creating individual participant groups

1. Click the "Create" button.
2. In the following dialog, enter a group name and optionally a description.
3. Specify whether or not the group members can 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 is created. You have specified whether communication between the members of this group is permitted or forbidden.

## Changing settings of the participant groups

1. Change the corresponding settings of the participant groups.
2. Then click the "Save" button.

## 4.7.4 Specifying communications relations between node groups

### Creation of communication relations between the participant groups

Once the participant groups have been created, you define the communication relations between the groups.

1. In the navigation, select "Remote connections > Participant groups".
2. Specify the source group. For this group click on the icon ⇄.
3. On the following page you specify the destination groups. This means groups to which connections from the source group are permitted.
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. In the navigation, select "Remote connections > Communication relations".
2. Click on the icon ⚙. Change the relevant communication relations and then click the "Save" button.

## 4.7.5 Assigning a node to a group

### Assigning participants (users or devices) to one or more groups

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

   **Result**

   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.

# 4.8 User accounts

## 4.8.1 Overview of the user accounts

**Note**

**Order when creating users**

If a newly created user needs to be assigned to a role or a participant group, this must already have been created.

For information on the procedure, refer to the section "Managing roles and rights" (Page 61)" or "Creating participant groups (Page 56)".

### Requirement for creating and changing users

The user is assigned the right "Manage users".

### Calling the Web page

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

### Displayed entries

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

| Box | Meaning |
|---|---|
| User name | The name assigned to the user. The user name must be unique throughout the system and cannot be changed. Refer to the note in the section ""Creating a new user". |
| 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. |

| Box | Meaning | |
|---|---|---|
| First name | First name of the user | |
| Second name | Second name of the user | |
| Account created | Date and time at which this user account was created | |
| Date of the last login | Date and time of the last login | |
| Status |  | The user is logged on to SINEMA RC. |
| |  | The user is not logged on to SINEMA RC. |
| |  | The user is disabled. |
| VPN connection mode | Shows which protocol is being used for the VPN connection. | |
| Actions |  | Overview of the user settings. This is also displayed for users with the right "read only". |
| |  | Change user settings. This includes changing the contact data, assigning new roles and rights and changing the password. |
| |  | Display of which participant group the selected user is assigned to. The user can be assigned to one or more groups. |
| |  | Deactivate user.<br>• If the user is online, the existing VPN connection is also deactivated.<br>• When the user attempts to log on, the message "Account is deactivated" is displayed. |
| |  | Activate the user again. The user can log on to the SINEMA RC server again. |

## Filtering entries

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

**Result**

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

## See also

Create a new user (Page 63)

## 4.8.2 Managing roles and rights

### Requirement for creating roles

The user is assigned the right "Manage users".

### Displayed entries

A list of the created roles is displayed.

| Box | Meaning | |
|---|---|---|
| Role name | Name of the role | - |
| Manage address spaces | Edit parameters of the address spaces | Remote connections > Address spaces |
| Create backup copies | Create, delete, export and import a backup copy. | System > Backup copy and restoring the system |
| Restore the system | Restoring the system based on the saved system file. | System > Backup copy and restoring the system |
| 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 Servers. | SINEMA RC client |
| Manage firmware updates | Load the update file with the new firmware on the device and start the update process. | System > Update |
| Manage devices | Create new devices; edit and delete devices already created; create participant groups and assign devices to them; create and download configuration file with VPN settings for the device; | Remote connections > Devices |
| Manage remote connections | Specify communication relations; this includes how the participants within a participant group may communicate and which participant group may communicate with which other participant group | Remote connections > Participant groups<br>Remote connections > Communication relations |
| Edit system parameters | Read, create and delete system parameters. The system parameters include:<br>• Overview<br>• Event log<br>• Web server<br>• Licenses<br>• Network<br>• Date and time of day<br>• VPN<br>• Maximum number and coding key for backup copies | |

| Box | Meaning | |
|---|---|---|
| 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 |

## Creating a new role

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

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

6. Click the "Finish" button.

## 4.8.3 Create a new user

### Create a new user

1. Open the "Users" tab.
2. Click the "Create" button.
3. Configuring 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 name cannot be changed**

     After creating a user, the user name can no longer be modified because the user name is used for encryption of the password.

     If a user name needs to be changed, the user must be deleted and a new user created.

   – Click the "Next" button.
4. Assignment of rights and roles
   – Assignment of rights via role assignment:

     In the "Rights" tab select a role that has already been created.

     Result:

     All rights marked with * are assigned to the user even if the check box in front is not enabled. To assign additional rights to the user apart from those marked with *, click on the check box in front of the particular right.

   – Assignment of rights without role assignment:

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

   – Click the "Next" button.

5. Configuring the VPN connection mode

   Set the following parameters:

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

6. Creating participant groups
   - Select one or more participant groups to which the device will be assigned. You will find information on creating participant groups in the section " Creating participant groups (Page 56)".
   - Click the "Next" button.
7. Specifying the password

   Enter a password and confirm it. The assigned password can be changed later by the relevant user, refer to the section "Changing the current password (Page 80)".
8. Click the "Finish" button.

## Changing user settings

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

# 4.9 Security

## 4.9.1 Managing certificates

### 4.9.1.1 Overview of certificate management

#### Certificate types

SINEMA RC uses different certificates to authenticate the various participants 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 a Certificate Authority from which the server, device and user certificates are derived. To allow a certificate to be derived, the CA certificate has a private key signed by the certificate authority.<br>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 69) |
| 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. The server certificate is derived from the oldest valid CA, even if this is "out of service". The crucial thing is the validity date of the CA. | *.p12 | Server certificate (Page 69) |
| Device certificate | Device certificates and corresponding keys can only be created when the user has the appropriate rights.<br>For each created device, a device certificate is derived. | *.p12 | Overview of device management (Page 46) |
| User certificate | For each created user, a personal certificate is derived. | *.p12<br>*.pem | User certificate (Page 79) |

#### File types

| File type | Description |
|---|---|
| *.crt | File that contains the certificate. |
| *.p12 | In the PKCS12 certificate file, the private key is stored with the corresponding certificate and is password protected.<br>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 key as Base64-coded ASCII text. |

## 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.

### 4.9.1.2 Certificate overview

## Calling the Web page

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

## Displayed entries

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

| Box | Meaning |
|---|---|
| Serial number | Number to identify the certificate. The serial number is assigned automatically when the certificate is created. |
| Common name | The name used is generated automatically by the system. |
| Issued by | Display of the certificate authority that issued the certificate. The system uses the last valid CA certificate. |
| 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.<br>The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred key length". |
| Signature method | Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate.<br>The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred hash method". |

## Renewing a user certificate

**Note**

**Only renew valid certificates**

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

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

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

## Exporting a user certificate

In the "Exports" tab, you can download personal certificates. These include:

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

### 4.9.1.3 CA certificate

#### Calling the Web page

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

#### Displayed entries

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

| Box | 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.<br>Out of service: A newer CA certificate was generated or the CA certificate has expired. | |
| Actions |  | Calling up CA information<br>You obtain information on the selected CA. This is also displayed for users with the right "read only". |
| |  | Exporting a CA certificate<br>By clicking on the icon, the password-protected CA certificate (*.crt) is exported. The file can, for example, the exported to the end device or to the destination server. |

#### Renewing a CA certificate

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

### 4.9.1.4 Server certificate

#### Calling the Web page

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

## Displayed entries

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

| Box | 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 adopted from the network configuration:<br>• The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 35)").<br>• The IP address of the WAN or LAN interface, see section "Interfaces (Page 33)". |
| Issuer | Display of the certificate authority that issued the certificate. |
| Valid from | Date from which the certificate is valid. |
| Valid to | Date on which the certificate expires. |
| Key length (bits) | Specifies the key length being used.<br>The value can be set in the "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.<br>The value can be set in the "Settings" tab under "Preferred hash method". |
| Alternative names | • IP: The IP address of the WAN interface, see section "Interfaces (Page 33)".<br>• 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 33)").<br>• DNS: The DNS name when you have activated the option "Externally resolvable host name" and have entered a value (see section "DNS (Page 35)"). |

## Renewing the Web server certificate and VPN server certificate

**Note**

**Only renew valid certificates**

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

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

### 4.9.1.5 Importing the Web server certificate

The following can be imported:

- Self signed certificate issued by the certification authority of the company.
- Certificate of a higher ranking certification authority.

## Procedure

1. To import the signed certificate of the certification authority, click the "Select file" button in "Select CA certificate file".
2. Select the CA certificate *.crt and confirm your selection with the "Open" button.
3. Click the "Select file" button in "Select the key file".
4. Select the corresponding key file *.pem and confirm your selection with the "Open" button.
5. The files are password protected. To load the files on the device, enter the password and repeat the input.
6. To import the certificate of a higher ranking certification authority, click the "Select file" button in "Select the CA chain file".
7. Select the CA certificate *.crt and confirm your selection with the "Open" button.
8. Click the "Next" button. Details of the signed certificate are displayed on the "Activate certificate" tab. You can, for example, check whether the certificate is still valid.

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

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

### 4.9.1.6 Making settings for certificates

#### Calling the Web page

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

#### Changing settings

The changes made in the "Settings" tab are used when creating or renewing a certificate:

| Box | Meaning |
|---|---|
| Preferred key length (bits) | Select the number of bits of the various possible keys for the procedure. |
| Preferred hash method | Select the hash method for the certificate: SHA256 or SHA512 |
| CA certificate renewal (days) | Specify how many days before it expires the certificate will be automatically renewed.<br>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.<br>The previous CA certificate is then "Out of service" but is valid for another 365 days. The clients that use this CAA certificate can continue to log on with it for another 365 days. After this time, the CA certificate counts as being "Expired" and the clients need to use the new CA certificate. |
| Validity of client certificates (days) | Specify for how many days the certificate will be valid. A certificate whose CA has already expired can no longer be used. |

### 4.9.1.7 Own certificate

#### Calling the Web page

In the navigation panel, select "Security > Certificate management" and the "Own certificates" tab.

#### Displayed entries

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

| Box | Meaning |
|---|---|
| Type | Type of the loaded file. For more information, refer to the section Overview of certificate management (Page 65).<br>• CA certificate<br>• Participant certificate<br>• Key file<br>• Remote station certificate<br>• Machine certificate |
| File name | File name of the certificate |
| Status | Display of whether the certificate is valid or has already expired. |

| Box | Meaning |
|---|---|
| Applicant | Display of the applicant obtained from the common name. |
| Issuer | Display of the certification authority that issued the certificate. |
| Valid from: | Date from which the certificate is valid. |
| Valid to: | Date on which the certificate expires. |
| Use | The function that uses the certificate. |

### Importing your own certificates

1. To import your own certificates, click the "Import" button.
2. Select the PKCS12 file (*.p12) and confirm your selection with the "Open" button.
3. The files are password protected. To load the files on the device, enter the password and repeat the input.
4. Click the "Next" button. Details of the CA certificate are displayed on the "Activate certificate" tab. You can, for example, check whether the certificate is still valid.

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

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.

## 4.9.2 VPN connections

### 4.9.2.1 Making VPN basic settings

### VPN basic settings

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

### OpenVPN file

When creating a device or a user, 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 65)".

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 46)".

For users, the file is called in the personal user account (see section "User certificate (Page 79)").

## 4.9.2.2 Making OpenVPN settings

### Requirement for changing the OpenVPN settings

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

### Calling the Web page

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

### Configuring OpenVPN

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

| Box | Meaning |
|---|---|
| Activate | When enabled, OpenVPN is used. |
| Status | Shows whether OpenVPN is enabled or disabled. |
| TCP port | Specify the port on which the SINEMA RC Server server accepts TCP connections. Assuming that TCP frames can be sent to this port. In a preconnected DSL router, for example, port forwarding must be entered. |
| UDP port | Specify the port on which the SINEMA RC Server server accepts UDP connections. Assuming that UDP frames can be sent to this port. In a preconnected DSL router, for example, port forwarding must be entered. |
| Keepalive monitoring time (s) | Enter the interval in seconds at which connected clients send keepalive packets.<br>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. As a response, for example, the connection from the server or the protocol can be closed with an error message. |

| Box | Meaning |
|---|---|
| Connection timeout (sec) | Specify the maximum time in seconds that the client waits for a response from the server before the connection is 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:<br>• AES-128, 192, 256: Advanced Encryption Standard (128, 192 or 256 bit key length, mode CBC)<br>• DES-EDE, DES-EDE3: Data Encryption Standard (128 or 192 bit key length, mode CBC) |
| Hash method | Selection of the authentication algorithm:<br>SHA-1, 256, 512: Secure Hash Algorithm 1, 256 or 512 |
| 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.<br>• WAN: Connection only via the WAN interface<br>• LAN 1-n: Connection via available LAN interfaces:<br>• WAN + LAN 1-n: Connection via all interfaces |

#### 4.9.2.3 Making the IPsec settings

### Requirement for changing the IPsecVPN settings

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

### Calling the Web page

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

### Configuring the basic setting

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

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

### 4.9.2.4 IPsec profiles

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

#### Calling the Web pages

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

#### Displayed values

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

| Field | Meaning | |
|---|---|---|
| Profile name | The name assigned to the IPsec profile. The name must be unique throughout the system and cannot be changed, refer to the section "Creating IPsec profiles (Page 76)". | |
| Key exchange | Key exchange method | |
| ESP | Settings of phase 1 - ESP (authentication) | |
| IKE | Settings of phase 2 - IKE (KE/key exchange) | |
| Actions |  | Overview of the IPsec profile. This is also displayed for users with the right "read only". |
| |  | Change IPsec profile. This also includes changing the settings for phase 1 and 2. |

### 4.9.2.5 Creating IPsec profiles

#### Requirement for changing the IPsecVPN settings

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

#### Creating a new IPsec profile

1. Open the "IPsec profile" tab.
2. Click the "Create" button.
3. Enter a name for the IPsec profile.
4. In Key exchange method specify whether IKEv2 or IKEv1 will be used.

5. Make the settings of phase 1 - ESP (authentication)

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

6. Specify the settings of phase 2 - IKE (KE/key exchange):

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

7. Click "Finish".

## Changing an IPsec profile

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

## Encryption algorithm

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

x: is supported

-: is not supported

# 4.10 My account

## 4.10.1 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:

| Box | Meaning |
|---|---|
| Serial number | Number to identify the certificate. The serial number is assigned automatically when the certificate is created. |
| Common name | The name used is generated automatically by the system. |
| Issued by | Display of the certificate authority that issued the certificate. The system uses the last valid CA certificate. |
| 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.<br>The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred key length". |
| Signature method | Specifies which digital signature method with the corresponding signature key ("hash value") was used for the certificate.<br>The value can be set in the menu "Security > Certificates" , "Settings" tab under "Preferred hash method". |

### Renewing a user certificate

**Note**

**Only renew valid certificates**

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

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

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

### Exporting a user certificate

In the "Exports" tab, you can download personal certificates. These include:

| Box | 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. |

## 4.10.2 Changing the current password

### Changing the current password

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

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

   The new must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers. See also the section "Permitted characters (Page 17)".

# Appendix A

A

## A.1 OpenVPN connection to an iOS device

The procedure was tested with iOS 7.1.2.

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

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

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

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

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

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

   - As of SINEMA RC V 1.1

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

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

<ca>-----BEGIN CERTIFICATE-----
MIIDHDCCAgSgAwIBAgIJAOBS47hEYgV/MA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME0NBIDAwMDAwMSBTSU5FTUEgUkMwHhcNMTUwNzIwMTEwMjIwWhcNMjUwNzE5
.....
AMx0VPyj9aPanl//whbpvOsFmiRNrXbynLZ/hsCEAkcjZLcVsDYEIVpp6E3ja93U
dffKYKqL9KGGO3tnkSSfdjxkRrJ4ory16wO378p/+P70YZq7aksiumxjLhDhEask
bNSBRyLgaU0AWVwAy7JIMm/DVU49z7NuOqlUhAGxkcw=
-----END</ca>
```

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

8. Insert the following in the configuration file:

   With SINEMA RC V1.0

   – Insert <ca> </ca>.

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

   As of SINEMA RC V 1.1

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

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

<connection>
remote 192.168.1.1 1194 udp
</connection>

<connection>
remote 192.168.1.1 1194 udp
</connection>

<connection>
remote 192.168.1.1 5443 tcp
</connection>

<connection>
remote 192.168.1.1 5443 tcp
</connection>
```

```
<ca>
-----BEGIN CERTIFICATE-----
MIIDHDCCAgSgAwIBAgIJALQz+EqerQolMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME0NBIDAwMDAwMSBTSU5FTUEgUkMwHhcNMTUwNTEzMTEyMDM0WhcNMjUwNTEy
MTEyMDM0WjAeMRwwGgYDVQQDDBNDQSAwMDAwMDEgU0lORU1BIFJDMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApau4G+6dV5mslG/V/K3Ujk5QvfhSJ76F
......
MTEyMDM0WjAeMRwwGgYDVQQDDBNDQSAwMDAwMDEgU0lORU1BIFJDMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApau4G+6dV5mslG/V/K3Ujk5QvfhSJ76F
-----END CERTIFICATE-----
</ca>
```

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

## A.2 Using a "virtual machine"

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

When assigning parameters to the virtual machines base the assignment on the hardware requirements for SINEMA Remote Connect.

### See also

Requirements (Page 15)

# 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 that is made up of the phone number and the SMS gateway name of your network provider, for example: 0123412345678@providersms.com

**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**<br>Send SMS with text to short number | Text: START<br>Short number: 7676245 | Text: OPEN<br>Short number: 6245 | Text: OPEN<br>Short number: 8000 | Text: OPEN<br>Short number: 3400 |
| **Deactivating**<br>Send SMS with text to short number | Text: STOP<br>Short number: 7676245 | Text: STOP<br>Short number: 6245 | Text: CLOSE<br>Short number: 8000 | Text: CLOSE<br>Short number: 3400 |

### See also

SMS gateway provider (Page 37)

# 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, in "Remote connections > Manage devices", click

  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 forged 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 recognized by 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.

## B.3 Structure of the csv file

On the data medium, you will find a template of the csv file. The entries are separated by semicolons.

```
Device Name;GSM Number;Type;Vendor;Location;Type of connection;Provider
;Comment;Group;Local LAN IP;Network mask;Network gateway;Virtual local LAN
IP;Network mask;Virtual local LAN address;Local Single host;VPN connection
mode;Ipsec profile;Fixed IP
S615_001;;;Siemens
AG;Karlsruhe;1;;;Station1;192.168.10.1;255.255.255.0;Yes;;;;;1;;
S615_001;;;;;;;;;192.168.20.1;255.255.255.0;;10.90.80.1;255.255.255.0;;;1;;
S615_002;;;Siemens
AG;Karlsruhe;1;;;Station2;192.168.30.1;255.255.255.0;;10.90.90.1;255.255.255
.0;10.90.90.2;192.168.30.1;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.3;192.168.30.2;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.4;192.168.30.3;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.5;192.168.30.4;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.6;192.168.30.5;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.7;192.168.30.6;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.8;192.168.30.7;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.9;192.168.30.8;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.10;192.168.30.9;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.11;192.168.30.10;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.12;192.168.30.11;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.13;192.168.30.12;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.14;192.168.30.13;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.15;192.168.30.14;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.16;192.168.30.15;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.17;192.168.30.16;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.18;192.168.30.17;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.19;192.168.30.18;1;;
S615_002;;;;;;;;;;;;;;;10.90.90.20;192.168.30.19;1;;
S615_003;;;Siemens AG;Karlsruhe;1;;;Station1;;;;;;;;;
```

### Values to be set

The table contains the entries that you can enter in the csv file. For more detailed information on these entries, refer to the section "Creating a new device (Page 49)" and device information..

| The entry ... | stands for ... |
|---|---|
| Device Name | Name of the device |
| GSM Number | GSM number |
| Type | Device type |
| Vendor | Manufacturer |
| Location | Location |

| The entry ... | stands for ... |
|---|---|
| Type of connection | Type of connection<br>Enter the number for the relevant type of connection.<br>1 = permanent:<br>2 = digital input<br>3 = wake-up SMS<br>4 = digital input & wake-up SMS |
| Provider | Name of the SMS gateway provider |
| Comment | Comment |
| Group | Participant group<br>The requirement is that the participant group has already been created. |
| Local LAN IP | Local LAN IP address |
| Network mask | Network mask of the local LAN IP address |
| Network gateway | Device is a network gateway<br>If the device is a network gateway, enter "Yes". |
| Virtual local LAN IP | Virtual local LAN IP address |
| Network mask | Network mask of the virtual local LAN IP address |
| Virtual local LAN address | Virtual local LAN address |
| Local Single host | Local host |
| VPN Connection | VPN connection mode<br>1 = OpenVPN: The connection will be established via OpenVPN.<br>2 = IPsec: The connection will be established via IPsec. |
| Ipsec Profile | Name of the IPsec profile<br>The requirement is that the IPsec profile has already been created. |
| Fixed IP | Fixed IP address for OpenVPN or IPsec connections |

# Index

## M



## N



## O



## P



## R



## S



## T



## U



## V

## W