SIEMENS

SIMATIC NET

Network management SINEC INS V1.0 SP2

Operating Instructions

06/2022
C79000-G8976-C566-04

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C566
Ⓟ 06/2022 Subject to change

Table of contents

Preface

1

Purpose of this software

SINEC INS makes various network services available and enables central configuration of these services via a common Web interface.

Purpose of this documentation

This manual supports you when installing and operating SINEC INS.

Scope of validity

The information in this document applies to SINEC INS V1.0 SP2.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

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

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

To prevent unauthorized access, note the following security recommendations.

Security recommendations

General

- You should make regular checks to make sure that this product meets these recommendations and/or other internal security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- SINEC INS is only intended for connections with trusted networks and should not be connected directly with networks such as the Internet. Take this into consideration in a holistic security concept for your plant.
- Keep the software you are using up to date. Check regularly for security updates for the product. You will find information on this at:
  Link: (https://www.siemens.com/industrialsecurity)
- Only activate services that you require for your network.
- Whenever possible, always use the variants of services that provide greater security (e.g. Secure Syslog, DNSSEC extension, access control lists (ACL) for DNS, etc.).
- Connections over unsecured network areas must be secured by security mechanisms such as SSL VPN.
- Always click on the "Log out" button in the Web interface when you have finished working with SINEC INS.
- Restrict access to SINEC INS to qualified personnel.
- Use the user and role administration of SINEC INS to configure the rights of the users according to their authorizations, refer to section Authorization management (Page 65).

Users, roles and passwords

- Define rules for the use of the software and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Create users and roles that are tailored to the scope of authorization required by each user. Do not use only the default user "SuperAdmin" and the default role "Admin".
- Define unique passwords for each new user.
- Only use passwords with a high password strength. Avoid weak passwords, for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized persons.
- Do not use the same password for different users and systems.

License conditions

Note

Open source software

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

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

OSS_SINEC-INS_99.pdf

Note on firmware/software support

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

Decommissioning

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

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

For decommissioning, delete all data from the device.

Trademarks

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

SINEC, SIMATIC

SIMATIC NET glossary

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

You can find the SIMATIC NET glossary on the Internet on our Industry Online Support pages at the following address:

Entry ID 50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

Installation and logon

2

2.1 License types

Each SINEC INS license contains a specific number of license nodes. The number of license nodes determines how many devices can use the services. The license nodes are identified based on the IP addresses of the devices. Depending on the respective service, licensing has the following effects:

- Syslog: The Syslog server receives Syslog messages only from a limited number of Syslog clients.
- RADIUS: You can only configure a limited number of RADIUS clients on the page "Network services > RADIUS service > RADIUS configuration > RADIUS clients". The end devices and RADIUS users of the RADIUS clients do not count as license nodes.
- TFTP / SFTP: These servers can only be used by a limited number of their clients. Downloading, uploading and deleting data via the SINEC INS Web interface uses HTTPS and these operations are not limited.
- DNS: The DNS server responds to name resolution requests from a limited number of devices.

Each license node can use the specified services simultaneously. There are no restrictions for using the DHCP and NTP services.

By default, SINEC INS includes a free demo license with 10 license nodes. To increase the number of devices that may use the Syslog, RADIUS, TFTP, SFTP and DNS service, you need to purchase a license. The following license types are available:

- SINEC INS Basic 50
- SINEC INS Basic 100
- SINEC INS Basic 250
- SINEC INS Basic 500
- SINEC INS Basic 1000
- SINEC INS Basic 5000

The number in the license name specifies how many license nodes can be used for the SINEC INS network services. The licenses can be combined. You can find information on activating purchased licenses in section License (Page 60).

2.2 System requirements

Hardware requirements

Depending on the number of nodes used, the following hardware requirements apply:

Table 2-1 Hardware requirements

Component	Up to 500 nodes	Up to 5000 nodes	More than 5000 nodes
Processor	2 cores with 2.16 GHz x64	2 cores with 2.6 GHz x64	4 cores with 3.6 GHz x64
Work memory	2 GB	8 GB	16 GB
Hard disk space	128 GB HDD	256 GB SSD	512 GB SSD

Note

Check the hard disk usage regularly. When your hard disk is full, correct operation of SINEC INS can no longer be guaranteed.

Software requirements

The following requirements apply to the software to be used:

Table 2-2 Software requirements

Operating system	• Linux Ubuntu 18.04.2 LTS Desktop (64-bit) • Linux Ubuntu 18.04.2 LTS Server (64-bit) • Linux Ubuntu 20.04.4 LTS Desktop (64-bit) • Linux Ubuntu 20.04.4 LTS Server (64-bit) • RX1500 APE 1808 Debian 9.6.0 • SIMATIC OS 1.3 • SIMATIC Industrial OS 2.4
Supported operating system languages	• German • English
Web browser	• Google Chrome 67.0 or higher • Firefox 68.0 or higher • Microsoft Edge 96.0 or higher
Screen resolution	1920 x 1080 pixels (size can be changed)
Recommended virtualization platforms	• VMware ESXi 7.0 Update 2a / Workstation Pro 16.x / Workstation Player 16.x • Oracle VirtualBox 6.1.32 You can find more information in the following section.

Limitations in the use of virtualization platforms

The recommended virtualization platforms VMware Workstation and VirtualBox offer the ability to use snapshots to store the status and data of the virtual machine at a given time. Note that snapshots should not be created during the operation of SINEC INS.

Before taking a snapshot, ensure that you have disabled all network services.

When a snapshot is restored on the virtual machine, the IP address of the network interface must remain unchanged. Otherwise, you need to regenerate the certificate of SINEC INS. If the license was locked because of it, contact Customer Support to release (Page 60) the license.

2.3 Ports used

SINEC INS uses the following ports as default ports for communication. Keep in mind that two different programs cannot communicate at the same time via the same port. If, for example, other SIMATIC applications or devices use one of the ports, this port is not available for SINEC INS.

Table 2-3 Ports used

Service/Protocol	Protocol / Port number	Default port status	Configurable port status	Configurable port number	Authentication	Encryption
SFTP	TCP/22	Closed	Yes	Yes	Yes	Yes
DNS server	UDP/53	Closed	Yes	No	No	No
DNS client	UDP/53	Closed	Yes	No	Yes	No
DHCP	UDP/67	Closed	Yes	No	No	No
TFTP	UDP/69	Closed	Yes	Yes	No	No
HTTP [1]	TCP/80	Open	No	Yes	No	No
NTP Server	UDP/123	Closed	Yes	No	Yes	Yes
NTP Client	UDP/123	Closed	Yes	No	Yes	Yes
HTTPS	TCP/443	Open	No	Yes	Yes	Yes
Syslog server	UDP/514	Closed	Yes	Yes	No	No
Secure Syslog server	TCP/6514	Closed	Yes	Yes	Yes	Yes
Syslog server relay	UDP/dynamic	Open (internal)	Yes	Yes	Yes	Yes
RADIUS Server	UDP/1812	Closed	Yes	Yes	Yes	Yes
RADIUS server	UDP/1820	Open	Yes	Yes	Yes	No
RADIUS Server proxy	UDP/dynamic [2]	Open (internal)	Yes	Yes	Yes	Yes
Web Backend	TCP/5053	Open (internal)	No	Yes	Yes	Yes
CodeMeter Linux	TCP/22350	Open (internal)	No	No	Yes	Yes
Codemeter WebAdmin	TCP/22352	Open (internal)	No	No	Yes	Yes

1) The address is automatically redirected to HTTPS.

2) The port does not process any incoming RADIUS requests. It is used internally for the relay functionality.
The port number changes on each RADIUS restart.

2.4 Installation

Signature validation prior to installation

Before you install SINEC INS, check the integrity of the Debian packages by validating their signatures. To do this, follow the steps outlined below:

1. In the terminal of your operating system, navigate to the SINECINS_V1.0_SP2/deb directory containing the "key.gpg" file.
2. Execute the following command to import the public key: *gpg --import key.gpg*.
3. In the terminal of your operating system, navigate to the directory containing the "sinecins.deb" and "codemeter-lite_7.21.4611.501_amd64.deb" files.
4. Validate the signature of the Debian packages as follows:
   - For "sinecins.deb": *dpkg-sig --verify sinecins.deb*
   - For "codemeter-lite_7.21.4611.501_amd64.deb": *dpkg-sig --verify codemeter-lite*_7.21.4611.501_amd64.*deb*

If the signature validation was successful, install SINEC INS according to the instructions in the section below.

Installation

Note

Keyboard layout during installation

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

Follow these steps to install SINEC INS:

1. Check the Internet connection.
   If there is no active Internet connection for SIMATIC OS V1.3, SIMATIC Industrial OS V2.4 and RX1500 APE 1808 Debian 9.6.0, make sure that the following packets are installed:
   - systemd
   - libusb-1.0-0
   - libcap2-bin
   - libpcap-dev
   - libwrap0-dev
   - libglib2.0-0
   - libreadline7
   - libncursesw6
2. To install SINEC INS from the product DVD, copy the contents of the DVD into a local directory of your PC.
   To install the download version of SINEC INS, extract the contents of the file "SINECINS_V1.0_SP2.tar.gz".

3. In the terminal of your operating system, navigate to the SINECINS_V1.0_SP2 directory containing the "install.sh" file.
4. Execute the following command:
   - For Linux Ubuntu operating systems: *sudo ./install.sh*
   - For SIMATIC OS V1.3, SIMATIC Industrial OS V2.4 and RX1500 APE 1808 Debian 9.6.0 (active Internet connection required): *sudo ./installDebianPkgDeps.sh*

   SINEC INS will now be installed. During installation you must accept the licensing conditions and security recommendations.
   SINEC INS uses the following TCP ports as standard:
   - HTTPS Web server port TCP 443
   - HTTP Web server port TCP 80
   - HTTPS Backend port TCP 5053

   If any of these ports is already in use, installation is paused and you need to define a different port for SINEC INS. The entered value must be between 1 - 65535 and not yet occupied. However, we do not recommend using standardized ports between 1 - 1023 for HTTP(S). Note that entered ports cannot be identical.
   The installation is continued when you confirm the entry.

Once the installation is complete, you can log on to the Web interface; refer to section Logon (Page 14).

2.5 Migration

The existing installations of SINEC INS V1.0, SINEC INS V1.0 SP1 and SINEC INS V1.0 SP1 Upd1 can be migrated to SINEC INS V1.0 SP2. The respective basic license is still used after the migration.

Previously created user accounts and devices, as well as configurations for network services, are retained after the migration. All license nodes used, with the exception of RADIUS clients, are deleted during the migration. All functions remain available.

Note

No downgrade possible

In general, downgrading the SINEC INS software to a previous version is not possible. The installer prevents this. However, a downgrade is possible due to a bug in V1.0, but this causes SINEC INS to crash.

Procedure

Proceed as follows to migrate SINEC INS:

1. Extract the contents of the file "SINECINS_V1.0_SP2.tar.gz".
2. Follow the procedure described in the section on "Installation (Page 12)".
   Before the migration, confirm the message about the update process with "y" or "yes". You can end the migration process with "n" or "no".
   During the migration, you are prompted:
   - To accept the license conditions and security recommendations.
   - To specify new HTTP(S) ports if the standardized HTTP(S) ports are already being used by another application; refer to section "Installation (Page 12)".

   No network services are available during the migration. Services that you have enabled prior to migration will receive the status "Enabled".
3. Check the status of the network services after migration.

2.6 Uninstalling

Follow these steps to uninstall SINEC INS:

1. On the page "System Administration > License > Licenses", release the licenses to be able to reuse the used license keys to activate the licenses after the uninstallation; refer to section "Licenses (Page 61)".
2. In the terminal of your operating system, navigate to the directory containing the "uninstall.sh" file. You will find this file on the product DVD of SINEC INS and in the "SINECINS_V1.0_SP2.tar.gz" download folder.
3. Execute the following command:
   sudo ./uninstall.sh
   SINEC INS and all associated services will now be uninstalled.

After the uninstallation, you will be asked whether you want to delete the license container with activated licenses or retain it on the device on which SINEC INS is installed.

2.7 Logon

The Web interface of SINEC INS can be called via the IP address or URL of the PC/device on which SINEC INS is installed. Access to the Web interface of SINEC INS takes place via the HTTPS protocol.

You are recommended to empty the browser cache before you access the SINEC INS Web interface.

Note

Check the status of the network services after every SINEC INS restart.

You can select the desired language on the start page.

Initial logon

The first time you log into SINEC INS, use the following local user and the corresponding password:

Table 2-4 User data for initial logon

User name	SuperAdmin
Password	sinecins

After you have logged on to SINEC INS for the first time, you are forwarded to a page on which you must change the password. Use a secure password and make sure to note it. If the password is lost, it may be necessary to reinstall SINEC INS.

Login options

After the first login, login to SINEC INS can take place with a local user or with a user configured in UMC.

Login with UMC

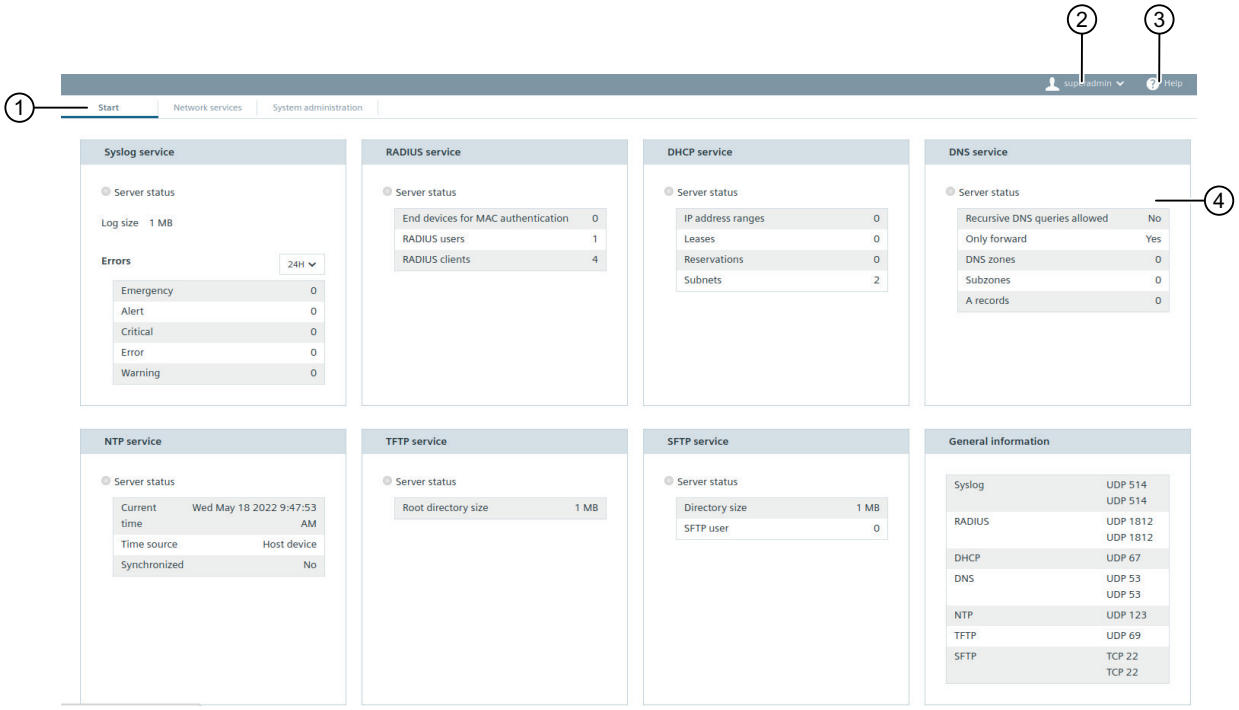
UMC stands for User Management Component, a database for the central administration of user data. If a user is created in UMC and is assigned to a UMC user group, this user can log into SINEC INS with his or her UMC user name and password. For this purpose, the UMC server must be activated in SINEC INS under "System Administration > General settings > UMC" and the connection to the UMC server configured. In addition, the UMC user group must be created in SINEC INS on the page "System Administration" > "Users" in the "UMC user groups" tab. The name of the UMC user group specified in SINEC INS must correspond to the name of the user group in UMC. If authentication via the UMC server is activated, SINEC INS attempts to perform login with a UMC user. If login with a UMC user fails, SINEC INS attempts to perform login with a local user.

UMC is included in the SINEC INS product scope and must be installed on a Windows PC. For information on configuring UMC user groups in SINEC INS, refer to section UMC user groups (Page 66).

2.8 Start Page

After successful login, the start page is displayed. You cannot configure anything on this page.

The start page is the dashboard of SINEC INS. It contains an overview of basic information about the available network services and is updated every 60 seconds. The display of the start page is individual and is adapted to the authorizations of the respective user. Therefore, the start page only displays those network services for which the logged in user is configured with the "View" or "Edit" right. Users with the "Edit" right, and for some network services also with the "View" right, can switch to a service by clicking on the service in the dashboard.



① Navigation
② User menu, see section below
③ Button for calling online help
④ Content area, see section below

Figure 2-1 Start page of SINEC INS

User menu

The user menu displays the name of the logged in user and contains the following functions:

- **Profile (only for local users)**
  Opens a window that displays the details of the logged in user. The password of the logged in user can be changed using the "Change password" button.
- **Language**
  Selecting the language for the user interface
- **Log out**
  Logs out the user of SINEC INS.
- **Version information**
  Shows the installed version of SINEC INS.

Content area

Available network services and general information is displayed in the content area of the start page.

You can find detailed information on the individual network services in section Network services (Page 21).

Syslog service

The following information is shown:

- **Server status**
  - Green symbol: The Syslog server is enabled.
  - Yellow symbol: The specified log directory or archive directory cannot be reached. The default directory "/opt/sinecins/bin/syslog-ng/logs" is used instead of the log directory. The default directory "/opt/sinecins/bin/syslog-ng/archive" is used instead of the archive directory.
  - Gray symbol: The Syslog server is disabled.
- **Log size**
  Size of the log file in MB for Syslog messages.
- **Fault**
  This table specifies the number of Syslog messages that have the following severities:
  - 0: Emergency
  - 1: Alert
  - 2: Critical
  - 3: Error
  - 4: Warning

  The time period from which the received Syslog messages originate can be selected from the drop-down list.

RADIUS service

The following information is shown:

- **Server status**
  - Green symbol: The RADIUS server is enabled.
  - Gray symbol: The RADIUS server is disabled.
- **End Devices for MAC Authentication**
  Specifies the number of configured end devices of RADIUS clients that are authenticated based on their MAC addresses.
- **RADIUS users**
  Specifies the number of configured RADIUS users that are required for user authentication.
- **RADIUS clients**
  Specifies the number of configured RADIUS clients. The RADIUS server accepts authentication requests from these RADIUS clients.

DHCP service

The following information is shown:

- **Server status**
  - Green symbol: The DHCP server is enabled.
  - Gray symbol: The DHCP server is disabled.
- **IP address ranges**
  Specifies the number of IP address ranges from which the DHCP server can assign IP addresses to DHCP clients.
- **Leases**
  Specifies the number of devices to which IP addresses are currently leased by the DHCP server.
- **Reservations**
  Specifies the number of devices for which IP addresses are currently reserved by the DHCP server.
- **Subnets**
  Specifies the number of subnets in which SINEC INS can perform IP address assignments.

NTP service

The following information is shown:

- **Server status**
  - Green symbol: The NTP server is enabled.
  - Gray symbol: The NTP server is disabled.
- **Current time**
  Specifies the time that is used as current time by the NTP server.
- **Time source**
  Specifies the SINEC INS time source that is used for the current time.
- **Synchronized**
  Specifies whether the time is synchronized between SINEC INS and the time source used.
- **Last synchronization (if the time is synchronized between SINEC INS and the time source)**
  Specifies in seconds when the last synchronization between SINEC INS and the time source took place.
- **Synchronization server**
  IP address of the time source

TFTP service

The following information is shown:

- **Server status**
  - Green symbol: The TFTP server is enabled.
  - Gray symbol: The TFTP server is disabled.
- **Root directory size**
  Specifies the size of the root directory.

SFTP service

The following information is shown:

- **Server status**
  - Green symbol: The SFTP server is enabled.
  - Gray symbol: The SFTP server is disabled.
- **Directory size**
  Specifies the size of the SFTP directory.
- **SFTP users**
  Specifies the number of SFTP users.

DNS service

The following information is shown:

- **Server status**
  - Green symbol: The DNS server is enabled.
  - Gray symbol: The DNS server is disabled.
- **Recursive DNS requests**
  - Yes / No
    Specifies whether further name servers are enabled for recursive resolutions of domain names.
- **Only forward**
  - Yes: SINEC INS does not attempt to contact other name servers to answer the name resolution request if SINEC INS itself or the configured name server cannot provide a response.
  - No: SINEC INS attempts to contact other name servers, including the root DNS server, to answer the name resolution request if SINEC INS itself or the configured name server cannot provide a response. This option is used for searching for domains on the Internet.
- **DNS zones**
  Specifies the number of configured DNS zones.

- **Sub-zones**
  Specifies the number of configured DNS sub-zones.
- **A records**
  Specifies the number of configured A records.

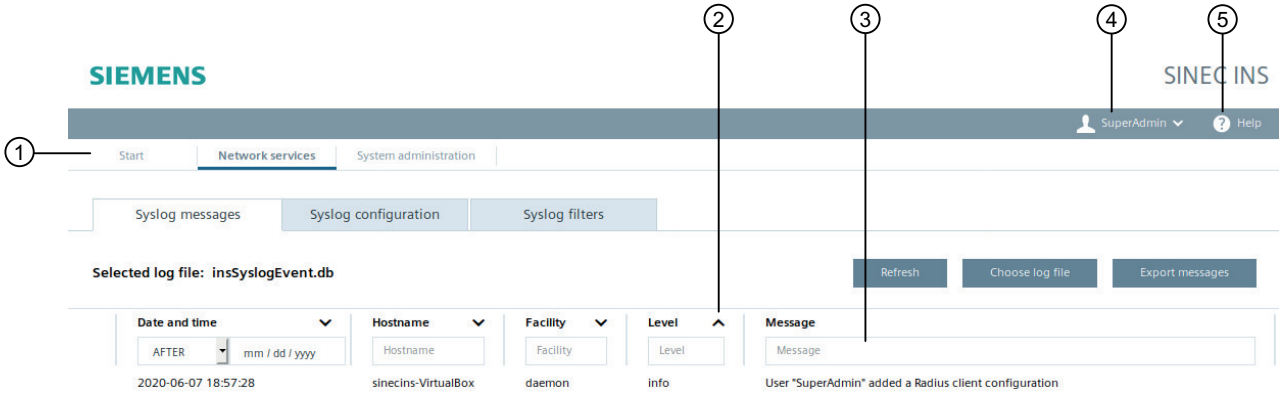
General information

The ports that are currently used for the individual network services are displayed in this area.

2.9 Structure of the user interface

SINEC INS can be configured via a user interface. The rights of a user's roles determine which network services and system functions are available for this user in the user interface.

The following figure shows essential elements of the user interface of SINEC INS using the page for received Syslog messages.



① Navigation
② Icons for ascending/descending sorting of column contents
③ Input box for textual filtering of column contents
④ User menu
⑤ Button for calling online help

Figure 2-2 User interface of SINEC INS

On all WBM pages with tables, you have the option displayed here to sort ② and filter ③ the table entries.

Network services 3

3.1 Syslog service

SINEC INS can be used as Syslog server and receive Syslog messages from devices or other Syslog clients in the network. SINEC INS can also work as Syslog relay and forward received Syslog messages to other Syslog servers or Siemens systems. Both communication paths can be secured with TLS. SINEC INS supports the Syslog server functionality in accordance with RFC 5424 and RFC 3164 and the Syslog client functionality in accordance with RFC 5424.

Note

When Syslog messages are transferred via TCP, SINEC INS supports the non-transparent framing method. The octet counting method according to RFC 6587 is not supported by SINEC INS.

3.1.1 Syslog messages

Syslog messages that SINEC INS received from devices or other Syslog servers are displayed on the page "Network services > Syslog service > Syslog messages". The Syslog messages are saved with the UTC system time of the Syslog server. The time is displayed according to the respective browser time zone on the PC. In addition to Syslog messages of network devices, internal messages generated by SINEC INS are also displayed. When you click on an entry on the "Syslog messages" page, the associated message is shown in its full length.

To receive Syslog messages, you need to enable the Syslog server and specify the interface and the port via which SINEC INS is to receive Syslog messages on the page "Network services > Syslog service > Syslog configuration".

Operator controls

The following operator controls are available above the table:

- **Refresh**
  Updates the table with Syslog messages
- **Choose log file**
  Opens a dialog in which you can select the log file whose Syslog messages are to be displayed. Received Syslog messages are always saved in the "insSyslogEvent.db" log file. This file is moved to an archive directory as soon as your configured maximum limit has been exceeded. All log files in the log file directory and in the archive directory are available for selection in the dialog. When there are several log files, you can search for the file name. You configure these two directories as well as the maximum size of the log file on the page "Network services > Syslog service > Syslog configuration".
- **Export messages**
  Exports the displayed Syslog messages to a CSV file.
  You can find an overview of exporting Syslog messages in the section "Overview of importing and exporting configurations (Page 77)".

Display of Facilities

The origin of the messages is shown in abbreviated form in the facility field. The following table assigns the facility names displayed in SINEC INS to the names specified in RFC 5424:

Table 3-1 Syslog Facilities

Numerical code	Facility name in SINEC INS	Facility name in RFC 5424
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	security/authorization	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock daemon	clock daemon
10	security/authorization	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	log audit	log audit
14	log alert	log alert
15	clock daemon (note 2)	clock daemon (note 2)
16-23	local0..local7	locally used facilities (local0-local7)

Display of Severities

The severity of the messages is displayed in the severity field. The following table assigns the severity names displayed in SINEC INS to the names specified in RFC 5424:

Table 3-2 Syslog-Severities

Numerical code	Severity name in SINEC INS	Severity name in RFC 5424
0	emergency	Emergency
1	alert	Alert
2	critical	Critical
3	error	Error
4	warning	Warning
5	notice	Notice
6	info	Informational
7	debug	Debug

3.1.2 Syslog configuration

Users that have the "Edit" right for the Syslog service can configure the Syslog server. The following parameters are available for configuring the Syslog server on the "Network services > Syslog service > Syslog configuration" page:

- **Enable Syslog server**
  Enables or disables the Syslog server.
  Disable the Syslog server before you configure it or make configuration changes. You enable the Syslog server again after the configuration.
- **Input interfaces**
  - Enable network adapter for Syslog service
    Selection of the network adapter via which the Syslog server should receive Syslog messages. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the Syslog service.
  - Protocol
    Selection of the transport protocol via which the Syslog server should receive Syslog messages.
  - Port
    Port via which the Syslog server should receive Syslog messages. Make sure that the specified port is not already used by another application.
  - Syslog filter
    Selection of the filter to be applied to the received Syslog messages. The Syslog filters that were configured on the page "Network services > Syslog service > Syslog filters" are available for selection; see section Syslog filters (Page 28).

- **Syslog relay**
  - Enable Syslog relay
    If you activate this option, the Syslog server forwards received Syslog messages to the specified Syslog servers. Syslog messages can be forwarded to up to five Syslog servers. Before forwarding to another Syslog server, a filter can be applied to the Syslog messages. The Syslog filters that were configured on the page "Network services > Syslog service > Syslog filters" are available for selection; see section Syslog filters (Page 28).
    When the Syslog messages are forwarded, SINEC INS uses the host name from the received Syslog message. If the received Syslog message does not contain a host name, SINEC INS uses the IP address from which the message was sent.
- **Logging**
  - Maximum size of log file
    Syslog messages received by the Syslog server are saved in the "insSyslogEvent.db" file. When this log file has reached the size given here, it is moved to the archive directory specified in the "Archive directory" text box. Afterwards, SINEC INS creates the "insSyslogEvent.db" file again in the directory specified in the "Log directory" text box so that further Syslog messages can be received.
  - Log directory
    Directory in which the "insSyslogEvent.db" log file is saved. Received Syslog messages are saved in this file. It is recommended that you save the log files locally and not on a network drive. On the "Network services > Syslog service > Syslog messages" page, you can select the log files located in the specified log directory and in the specified archive directory.
    If the specified log directory cannot be reached, the default directory "/opt/sinecins/bin/syslog-ng/logs" is used. This state is displayed on the start page with a yellow symbol for the Syslog server.
  - Archive directory
    Directory in which the "insSyslogEvent.db" log file is archived after it has reached the specified maximum size. In this directory, the file receives the current time stamp as a prefix in its name. It is recommended that you archive the log files locally and not on a network drive. On the "Network services > Syslog service > Syslog messages" page, you can select the log files located in the specified log directory and in the specified archive directory.
    If the specified archive directory cannot be reached, the default directory "/opt/sinecins/bin/syslog-ng/archive" is used. This state is displayed on the start page with a yellow symbol for the Syslog server.
  - Manage archive directory
    The following options are available:
    Maximum number of files: After the specified number of log files has been reached, a new log file replaces the oldest log file in each case.
    Maximum file age: After the file age specified in days has been reached, log files are deleted by SINEC INS.

Certificate-based authentication

Communication between Syslog clients and the Syslog server can be encrypted with TLS. The following figure shows an illustration of the certificate-based authentication procedure:

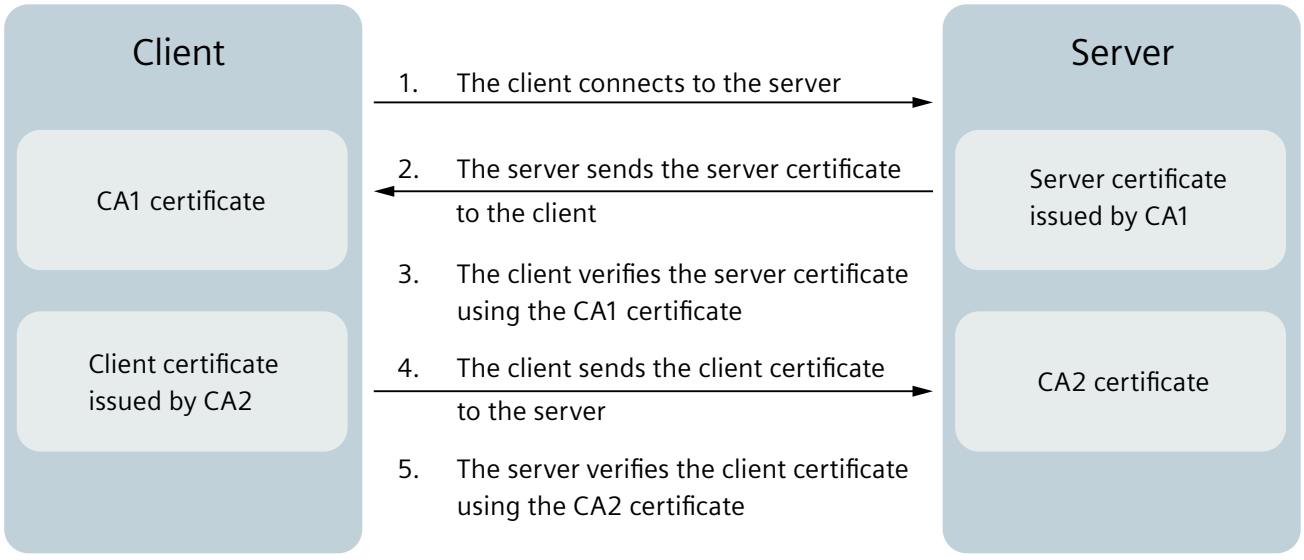


Figure 3-1 Certificate-based authentication

Note

Requirements on certificates

The "Common Name" or "subject_alt_name" property must contain the host name or the IP address of the Syslog server. Otherwise, the encrypted connection between Syslog client and Syslog server cannot be established.

Keys with password protection are not supported by SINEC INS.

Make sure that the certificates are renewed before their expiration date.

SINEC INS Syslog supports certificates signed with SHA-256, SHA-384 and SHA-512 algorithms. Use only these algorithms in your certificates.

Note

Access rights for certificate files

Observe the access rights for the SSL certificates that are used for Secure Syslog.

Example:

- rwx-r--r-- for all files except the sym link file
- rwx-rwx-rwx for the sym link-file

Note

Input interface for Secure Syslog

For Secure Syslog, the input interface must be switched to TCP port 6514.

- **Secure Syslog server**
  With the options in this dialog area, you can protect communication between Syslog clients and the Syslog server of SINEC INS. Certificates and keys are not provided by SINEC INS. You need to generate them according to your own requirements and make them available to SINEC INS and to the Syslog clients. Only certificates in *.pem and *.key format are permissible.
  In the "Input interface" area, make sure that the TCP protocol was selected for secure communication.
  The following settings are available:

  – Enable secure Syslog server
    Activates secure communication of Syslog clients with the Syslog server of SINEC INS. All input interfaces subsequently receive secure Syslog messages.

  – Secure Syslog server with TLS
    If you enable this option, TLS is used to log encrypted Syslog messages.
    Before communication begins, the Syslog clients authenticate the Syslog server based on its certificate. For this purpose, you need to specify the path to the certificate of the Syslog server in the "Certificate of Syslog server" text box. The self-signed certificate of the Syslog server or CA that created the certificate of the Syslog server must be known to the Syslog clients for authentication of the Syslog server. For the Syslog messages to be decrypted by the Syslog server, the path to the associated private key must be specified in the "Private key" text box.

  – Enable mutual authentication with TLS
    If you enable this option, TLS is used to log encrypted Syslog messages.
    Before communication begins, the Syslog clients authenticate the Syslog server based on its certificate. For this purpose, you need to specify the path to the certificate of the Syslog server in the "Certificate of Syslog server" text box. The self-signed certificate of the Syslog server or CA that created the certificate of the Syslog server must be known to the Syslog clients for authentication of the Syslog server. For the Syslog messages to be decrypted by the Syslog server, the path to the associated private key must be specified in the "Private key" text box.
    In addition, before communication starts, the Syslog server authenticates the Syslog clients based on their certificates. For this purpose, you need to specify in the "CA certificate directory of client" text box the directory containing the self-signed certificates of the Syslog clients or the CAs that created the certificates of the Syslog clients. You then need to generate a hash value for each of these certificates according to the instructions below and link the hash value with the relevant certificate.

  – Certificate of Syslog server
    Path to the certificate that the Syslog clients use to authenticate the Syslog server. The self-signed certificate of the Syslog server or the CA that created the certificate of the Syslog server must be known to the Syslog clients.

  – Private key
    Path to the private key that the Syslog server uses to decrypt received Syslog messages.

- CA certificate directory of client (only active when the "Enable mutual authentication with TLS" option is activated)
  Path to the directory containing the self-signed certificates of the Syslog clients or the certificates of the CAs that created the certificates of the Syslog clients. Follow these steps so that the Syslog server can authenticate the Syslog clients based on their certificates:
  1. Copy the self-signed certificates of the Syslog clients or the CA certificates to the specified directory.
  2. Perform the following command for every certificate to generate an alphanumeric hash value for the certificate:
  `openssl x509 -noout -hash -in cacert.pem`
  3. Perform the following command to establish a symbolic link between the certificate and the created hash value:
  `In -s cacert.pem <hash value>.0`

- **Secure Syslog client**
  When SINEC INS is used as Syslog relay, you can protect communication between SINEC INS as Syslog client and other Syslog servers with the options in this dialog area. Certificates and keys are not provided by SINEC INS. You need to generate them according to your own requirements and make them available to SINEC INS and to the Syslog servers. The following settings are available:

  - Enable secure Syslog client
    Activates secure communication between SINEC INS as Syslog client and other Syslog servers. Secure Syslog messages are then sent to all configured Syslog servers.

  - Encrypt Syslog messages with TLS
    If you activate this option, TLS is used to encrypt the communication between SINEC INS as Syslog client and other Syslog servers.
    Before communication begins, the Syslog client authenticates the Syslog servers based on their certificates. For this purpose, you need to specify in the "CA certificate directory of servers" text box the directory containing the self-signed certificates of the Syslog servers or the certificates of the CAs that created the certificates of the Syslog servers. You then need to generate a hash value for each of these certificates according to the instructions below and link the hash value with the relevant certificate.

  - Enable mutual authentication with TLS
    If you activate this option, TLS is used to encrypt the communication between SINEC INS as Syslog client and other Syslog servers.
    Before communication begins, the Syslog client authenticates the Syslog servers based on their certificates. For this purpose, you need to specify in the "CA certificate directory of servers" text box the directory containing the self-signed certificates of the Syslog servers or the certificates of the CAs that created the certificates of the Syslog servers. You then need to generate a hash value for each of these certificates according to the instructions below and link the hash value with the relevant certificate.
    In addition, before communication starts, the Syslog servers authenticate the Syslog client based on its certificate. For this purpose, you need to specify the path to the certificate of the Syslog client in the "Certificate of Syslog client" text box. The self-signed certificate of the Syslog client or CA that created the certificate of the Syslog client must be known to the Syslog servers for authentication of the Syslog client. For the TLS handshake data to be decrypted by the Syslog client, the path to the associated private key must be specified in the "Private key" text box.

- CA certificate directory of servers
  Path to the directory containing the self-signed certificates of the Syslog servers or the certificates of the CAs that created the certificates of the Syslog servers.
  Follow these steps so that the Syslog client can authenticate the Syslog servers based on their certificates:
  1. Copy the self-signed certificates of the Syslog servers or the CA certificates to the specified directory.
  2. Perform the following command for every certificate to generate an alphanumeric hash value for the certificate:
  `openssl x509 -noout -hash -in cacert.pem`
  3. Perform the following command to establish a symbolic link between the certificate and the created hash value:
  `In -s cacert.pem <hash value>.0`
- Certificate of Syslog client (only active when the "Enable mutual authentication with TLS" option is activated)
  Path to the certificate that the Syslog servers use to authenticate the Syslog client. The self-signed certificate of the Syslog client or CA that created the certificate of the Syslog client must be known to the Syslog servers.
- Private key (only active when the "Enable mutual authentication with TLS" option is activated)
  Path to the private key that the Syslog client uses to decrypt data exchanged in the context of the TLS handshake.

Note

To apply the settings after the completed configuration of Secure Syslog, you need to disable the Syslog server and enable it again.

3.1.3 Syslog filters

On the "Network services > Syslog service > Syslog filters" page, you can create the filters that can be applied to the Syslog messages received and forwarded by SINEC INS. A filter can contain multiple conditions that can be set for properties such as the Severity and Facility of Syslog messages. You can link these conditions with the OR or AND operators.

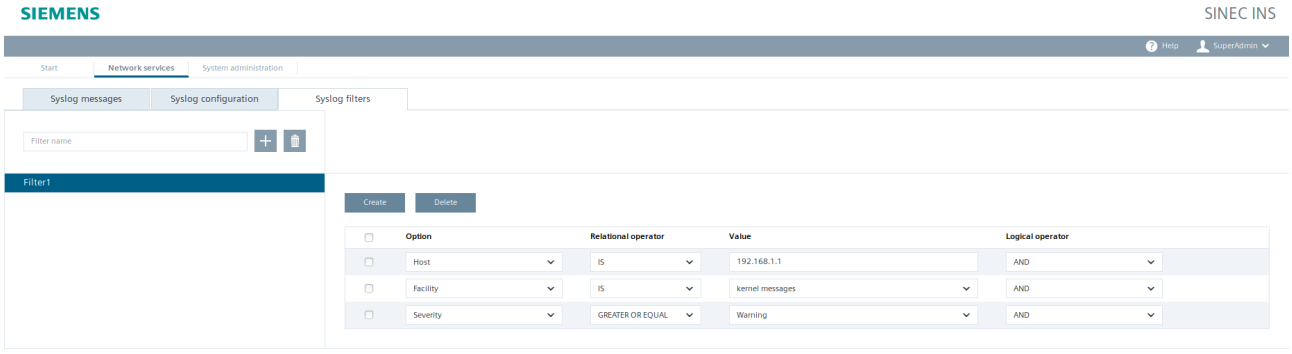


Figure 3-2 Syslog filter

On the "Network services > Syslog service > Syslog configuration" page, you can select created filters for the network adapters via which the Syslog server receives Syslog messages. Filters can also be applied to Syslog messages that are to be forwarded to other Syslog servers.

3.2 RADIUS service

SINEC INS can be used as RADIUS server. RADIUS is a protocol for the authentication, authorization and accounting of users and devices by servers on which user names, passwords and device information can be stored centrally. The use of a RADIUS server can increase the protection of this data. SINEC INS supports the authentication and authorization of users and devices and can forward RADIUS requests to other RADIUS servers.

The following applications are supported by SINEC INS:

- **User authentication**
  A user enters his/her user name and password on the WBM/SSH/Telnet login page of a device. The user data is sent by the device to the RADIUS server of SINEC INS. SINEC INS checks whether the user data is present on the RADIUS server. PAP (Password Authentication Protocol) is the only authentication protocol used by SINEC INS.
- **Port-based authentication**
  An end device is connected to the port of a RADIUS client device. The end device is authenticated for access to the RADIUS client device with the mode configured for the port. The following port authentication modes are supported by SINEC INS:
  - **MAC Address**
    An end device is authenticated by its MAC address.
    SINEC INS checks whether the MAC address of the end device is present in SINEC INS under "Network services > RADIUS service > RADIUS configuration > End Devices MAC Authentication".
  - **802.1X (EAP)**
    The Extensible Authentication Protocol (EAP) is based on the Challenge-Response authentication. The exchange of authentication information takes place between a wireless or wired RADIUS client (Supplicant) and the RADIUS server (Authentication server) via a wired switch or a wireless access point (Authenticator) that acts as proxy. End devices are authenticated either with certificates (EAP-TLS) or with user credentials (EAP-TTLS or EAP-PEAP). EAP supports both RSA-based and Elliptic-Curve-based (EC) certificates.

    Note

    To use EEC-based certificates in Windows, you need to enable their support in Windows. For more information, visit FAQ.

    The following EAP authentication types are available:
    EAP-TLS / EAP-TTLS / EAP-PEAP
    Supported by SINEC INS. With EAP-TLS authentication, the RADIUS client checks the certificate of the RADIUS server and, in the next step, the RADIUS server checks the certificate of the RADIUS client. Authentication takes place after successful verification. If EAP-TTLS / EAP-PEAP are used, only a server-side certificate is required. For EAP-TTLS and EAP-PEAP, the RADIUS user must be configured for successful authentication. When EAP-TTLS is used, authentication information is transferred via an encrypted tunnel. With PEAP, SINEC INS authenticates the client based on the user credentials. You configure the parameters under "Network services > RADIUS service > RADIUS configuration > End Devices EAP Authentication".
    EAP-MD5
    SINEC INS cannot process EAP-MD5 queries as RADIUS server, but it can forward the request to other RADIUS servers. For successful forwarding, a corresponding RADIUS user group must be configured in SINEC INS for the specified user name under "Network services > RADIUS service > Relay configuration".
- **User authentication with UMC server**
  The users on the UMC server can be used for the RADIUS authentication. When a user logs in to the RADIUS client, the authentication request is sent to the RADIUS server. When RADIUS authentication with the UMC server is enabled, the authentication request is sent to the UMC server. For successful authentication, settings on RADIUS clients must be configured accordingly; refer to section "RADIUS configuration (Page 31)".

3.2.1 RADIUS configuration

Users that have the "Edit" right for the RADIUS service can configure the RADIUS server and can export and import configurations. You can find an overview of exporting and importing configurations in the section "Overview of importing and exporting configurations (Page 77)".

The following parameters are available for configuring the RADIUS server on the "Network services > RADIUS service > RADIUS configuration" page:

- **Enable RADIUS server**
  Enables or disables the RADIUS server
  Disable the RADIUS server before you configure it or make configuration changes. You enable the RADIUS server again after the configuration.
- **"Export configurations" button**
  Button for exporting the configurations of RADIUS users, RADIUS clients and end devices. The created files are used to back up the configurations.
  After the export, you will receive a ZIP file "sinecinsRadiusConfiguration.zip" with three configurations in CSV format for users, clients and end devices.
  The exported CSV files of RADIUS users "sinecinsRadiusUsers.csv", of RADIUS clients "sinecinsRadiusClients.csv" and the VLAN assignments "sinecinsRadiusEapTlsVlans.csv" are encrypted by SINEC INS. The exported CSV file from RADIUS end devices "sinecinsRadiusEndDevices.csv" is unencrypted and can be edited by the user. After the export, the CSV is edited using the operating system. Note that the names of the three CSV files as well as the names and order of the columns contained cannot be changed after the export. Otherwise, it will not be possible to import the configurations later.
- **"Import configurations" button**
  Button for importing the configurations of RADIUS users, RADIUS clients and end devices. You can import previously exported configurations for users, clients and end devices from a ZIP file into SINEC INS.
  Follow these steps to import the RADIUS configuration:

1. Disable the RADIUS server before the import.
2. Click "Import configurations".
   The "Import configurations" dialog window is displayed.
3. In the browser, navigate to the directory containing the "sinecinsRadiusConfiguration.zip" configuration file to be loaded. Double-click on the relevant ZIP file to apply it. Note that none of the file names can be changed. Otherwise, the import will be aborted.

4. Select the "Override existing configurations" check box to overwrite the existing entries. Overwriting is based on the user name specified for RADIUS users, on the client name and client IP address specified for RADIUS clients, and on the MAC address specified for end devices.
   If you have changed the VLAN name or the VLAN ID for an end device in the unencrypted file "sinecinsRadiusEndDevices.csv", the old VLAN name or the old VLAN ID will be overwritten if the option "Override existing configurations" is selected.
5. Click "Import".
   All RADIUS configurations for users, clients and end devices are imported into SINEC INS. Note that all RADIUS users are imported with the "enabled" status, regardless of whether they had the "enabled" or "disabled" status before the export.
   During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. Each import process is logged by the Syslog service.
   Note that the number of RADIUS clients is limited by the available license. If the maximum number of RADIUS clients is exceeded, addition of further RADIUS clients is stopped. This information is logged.

- **Input interfaces**
  - Enable network adapter for RADIUS service
    Selection of the network adapter via which the RADIUS server should receive authentication requests. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the RADIUS service.
  - Port
    UDP ports through which the RADIUS server should receive authentication requests. Make sure that the specified port is not already used by another application.
- **RADIUS users**
  User data that is needed for user authentication can be managed in this dialog area. Using the "Create" button, you can create new RADIUS users. To do this, enter the user name and the password and confirm the password. Use passwords with a high password strength. To assign write permissions to the user on the device, enable the "Administrative user" option. When the RADIUS server receives an authentication request from a device, it checks whether the specified user data is present in this dialog area. If the user data is present, the user receives access to the device.
  An "enabled/disabled" status is shown for configured RADIUS users and they can be filtered by status.
- **"Enable" and "Disable" buttons**
  You can enable or disable previously selected RADIUS users with these buttons. A newly created user receives the "enabled" status by default. The buttons are available when at least one RADIUS user is selected in the list.
- **"Import RADIUS users" button**
  The button for importing RADIUS user data is located on the right in the "RADIUS users" area. You can import previously created RADIUS user data from a CSV file into SINEC INS.
  Follow these steps to import the RADIUS users:

1. First, create a CSV file with user data. To do this, enter the data of the RADIUS users in a table and then save the table as CSV file. The table must have **no header** and contain the data in the following order:
   - First column: User name
   - Second column: Corresponding password
   - Third column: User type, e.g. admin or operator (the entries are not case-sensitive)
     If no user type or a user type other than "admin" is entered, SINEC INS automatically converts it to the "Operator" user type. The "admin" user type receives write permissions for RADIUS clients and the "Operator" user type receives read permissions. The specified user names and passwords must be valid. Otherwise, no data is saved.
     Please note that the number of RADIUS users to be imported from a CSV file is limited to max. 10000.
     The column delimiter of the CSV file must be "," (comma).

     ```
     sinecins@sinecins-VirtualBox:~/test$ cat ImportSinecinsRadiusUsers.csv
     user1,pwd1,admin
     user2,pwd2,test
     user3,pwd3,operator
     user4,Pwd4,operator
     ```

     Figure 3-3 Example of a CSV file for importing the RADIUS users
2. Disable the RADIUS server before the import.
3. Click "Import RADIUS users".
   The "Import RADIUS users" dialog box appears.
4. Navigate in the browser to the directory in which the CSV file to be loaded is located. Double-click on the desired file to apply it.
5. Click "Import".
   RADIUS user data is imported into SINEC INS.
   During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. Each import process is logged by the Syslog service. The information on the users not added is logged.
   If the maximum number of entries is exceeded, addition of further RADIUS users is stopped and superfluous entries are not logged.

- **RADIUS clients**
  Every device that sends authentication requests to the RADIUS server must be known to the RADIUS server. With the "Create" button, you can make these devices known to the RADIUS server by creating them as RADIUS clients with names and IP addresses. For each RADIUS client, a Shared Secret that also needs to be configured on the RADIUS client needs to be specified. The specified client names do not need to match the device names.
  Select the "Message-Authenticator attribute supported" check box if the RADIUS client can send a Message-Authenticator attribute for access requirements. This switches on a RADIUS security mechanism. The RADIUS client then needs to calculate a key with HMAC MD5 from its own request package and add this to the Message-Authenticator attribute as signature. The RADIUS server validates the package. If the check is successful, the RADIUS client receives a response from the RADIUS server. If the check fails due to an incorrect or missing Message-Authenticator attribute, the RADIUS access request is discarded. All supported SCALANCE devices automatically generate a Message-Authenticator attribute and add it to the request package. Leave the "Message-Authenticator attribute supported" check box selected for SCALANCE devices. RUGGEDCOM devices, in contrast, do **not** have this option. For this reason, you need to uncheck this check box for RUGGEDCOM devices; otherwise, the RADIUS server cannot answer the RUGGEDCOM devices.
  Note that the number of configurable RADIUS clients is limited by the present license.
- **"Import RADIUS clients" button**
  The button for importing RADIUS client data is located on the right in the "RADIUS clients" area.
  You can import previously created data of RADIUS clients from a CSV file into SINEC INS. The procedure is identical to the import of RADIUS users; see the "Import radius users" button above. The table must have **no header** and contain the data in the following order:
  - First column: Name of the RADIUS client
  - Second column: IP address of the RADIUS client
  - Third column: Corresponding Shared Secret
  - Fourth column: "yes" or "no" (not case-sensitive)
    - "yes", if the Message-Authenticator attribute is enabled at the RADIUS client (e.g. for SCALANCE devices)
    - "no", if the Message-Authenticator attribute is disabled at the RADIUS client (e.g. for RUGGEDCOM devices).
    If the fourth column does not contain an entry or contains an entry other than "yes" or "no", SINEC INS automatically converts it to "yes".

  The specified user names and IP addresses must be valid. Otherwise, no data is saved.
  The column delimiter of the CSV file must be "," (comma). The max. number of RADIUS users to be imported from a CSV file is 10000.

```
sinecins@ubuntu13:~$ cat radiusClients.csv
client1,192.168.0.1,secret1,yes
client2,192.168.0.2,secret2,no
client3,192.168.0.3,secret3,no
client4,192.168.0.4,secret4,no
```

Figure 3-4 Example of a CSV file for importing the RADIUS client

- **Guest VLAN**
  The guest VLAN allows unknown end devices to access the RADIUS client by specifying the guest VLAN name or guest VLAN ID.
  Enable this option if you want the end device to be permitted in the guest VLAN if authentication fails. The device can only be assigned to the corresponding VLAN if the VLAN has been created on the device. Otherwise, authentication is rejected. Make sure that the "RADIUS VLAN assignment permissible" option is also enabled on the device itself so that the device can authenticate itself in the guest VLAN.

  – **Enable guest VLAN**
    Enables or disables the guest VLAN.

  – **VLAN ID or name**
    The VLAN ID or VLAN name for the guest VLAN.
    The VLAN ID or name can be handled differently depending on the client configuration. Check the client configuration to avoid unintentional authorization.

- **End Devices MAC Authentication**
  End devices that are connected to the port of a RADIUS client can be authenticated based on their MAC address. In the "Create End Devices" dialog area, you can specify the MAC addresses of these end devices. You can also assign the guest VLAN to an end device.
  If you also specify the VLAN ID or name for an end device, the response of SINEC INS to the request of a RADIUS client additionally contains the specified VLAN information. The RADIUS client can then check whether the specified VLAN corresponds to the VLAN of the end device that is connected to the respective port.

- **"Import RADIUS devices" button**
  The button for importing end devices is located on the right in the "End devices" area.
  You can import previously created data of end devices from a CSV file into SINEC INS. The procedure is identical to the import of RADIUS users; see the "Import radius users" button above. The table must have **no header** and contain the data in the following order**:**

  – First column: MAC address
    "-" or ":" can be used for MAC addresses.

  – Second column: VLAN name/VLAN ID

  The specified MAC addresses and VLAN names/VLAN IDs must be valid. Otherwise, no data is saved.
  The column delimiter of the CSV file must be "," (comma). The max. number of RADIUS users to be imported from a CSV file is 10000.

```
sinecins@sinecins-VirtualBox:~/test$ cat sinecinsRadiusEndDevices.csv
12:F4:8D:E3:47:03,VLAN1
10-F4-8D-E3-47-12,VLAN2
```

Figure 3-5 Example of a CSV file for importing the end devices

- **End Devices EAP Authentication**
  Authenticates end devices in wireless and wired networks.
  In this area, you can specify one or more certificates and configure the required parameters with which end devices connected to the port of a RADIUS client authenticate themselves to the RADIUS server.
  Three authentication procedures are available. Select one or more methods:

  – **EAP-TLS** (EAP Transport Layer Security)
    Mutual certificate authentication is performed with this protocol. This is based on the handshake of the certificates of the end device and the RADIUS server. SINEC INS checks the client certificate signed by the CA and the end device checks the RADIUS server certificate signed by the same CA.

  – **EAP-TTLS** (EAP Tunneled Transport Layer Security)
    This protocol is an extension of EAP-TLS: After the RADIUS server authenticates itself to the end device with its certificate, the end device proves its identity via PAP or MSCHAPv2. SINEC INS checks whether the entered combination of user name and password exists among the configured RADIUS users. The PAP authentication method is used when only the EAP TTLS is selected. When EAP TTLS and EAP PEAP are enabled at the same time, the MSCHAPv2 authentication method is used. The EAP TTLS in combination with the RADIUS authentication via UMC server, only uses the PAP authentication method.

  – **EAP-PEAP** (EAP Protected Extensible Authentication Protocol)
    Only the RADIUS server requires a certificate with this protocol. With this certificate, the endpoints create an encrypted TLS tunnel for the transmission of authentication data. MSCHAPv2 challenge-response is used to authenticate the endpoints with the PEAP. This authenticates both the server and the end device. SINEC INS checks whether the entered combination of user name and password exists among the configured RADIUS users. The EAP PEAP cannot be used in combination with the UMC server.
    After EAP-PEAP is activated, the stored RADIUS users are deleted. You are informed about this by a dialog box. After the warning is confirmed with Yes, all RADIUS users are deleted and must be entered again.

  Depending on the selected authentication procedure, the following entries are required for the certificate of the RADIUS server:

  – **Path to server certificate**
    Path to the certificate file of the RADIUS server. Possible certificate formats are .cer, . pem or .crt.

  – **Path to private key**
    Path to the private key file of the server certificate in .pem format.

  – **Password protected**
    Select the check box if the private key is password protected.

  – **Password of private key**
    Password of the private key file of the server certificate.
    Enter the password. By using the eye symbol next to the text box, you can hide or show the password.

- **Path to CA certificate**
  Path to the CA certificate file. This entry is required only for EAP-TLS. Possible certificate formats are .cer, . pem or .crt. The certificates for the client and the server should be issued and signed by the same certificate authority.
  You can create a combined PEM file for more than one CA certificate file. For this, use the command:
  -cat serverca.crt ca2.crt > combined.pem

Note

The specified path must be valid and contain the file extension of the certificate. Paths to certificates and private keys are checked for accessibility.

SINEC INS RADIUS Server supports certificates signed with SHA-256, SHA-384 and SHA-512 algorithms. Use only these algorithms in your certificates.

- **Area for VLAN assignments for clients**
  For clients authenticating with EAP-TLS, you can configure client certificate common names with assigned VLAN IDs or names. After a client successfully authenticates using EAP-TLS, the RADIUS server checks whether the common name of the client certificate matches its certificate. If so, the RADIUS server sends the VLAN ID or the name to the RADIUS client so that the RADIUS client can authenticate the end devices according to this information.
  The "Create" button allows you to create VLAN assignments by specifying the common certificate name of the client and the associated VLAN ID or VLAN name.

- **"Import VLAN Assignments" button**
  The button for importing VLAN assignments is located in the "End Devices EAP Authentication" area on the right.
  You can import previously created data of VLAN assignments from a CSV file into SINEC INS. The procedure is identical to the import of RADIUS users; see the "Import radius users" button above. The table must have **no header** and contain the data in the following order:

  – First column: General certificate name of the client

  – Second column: VLAN ID or name

  The VLAN assignments must be valid, otherwise no data will be saved.
  The column delimiter of the CSV file must be "," (comma). The maximum number of assignments to be imported from a CSV file is 10000.

```
sinecins@sinecins-VirtualBox:~/Desktop$ cat ImportsinecinsRadiusEapTlsVlans.csv
ClientcertCommonName4;VLAN1
ClientcertCommonName5;VLAN2
ClientcertCommonName6;VLAN3
```

Figure 3-6 Example of a CSV file for importing VLAN assignments

- **RADIUS authentication with UMC server**
  The login data of UMC users can be used for the RADIUS authentication to access the devices, provided that these devices are able to send the Message-Authenticator attribute in their RADIUS authentication requests. RADIUS authentication requests without a message authentication attribute are only processed with local RADIUS users.
  To be able to use RADIUS authentication with the UMC server, you need to make sure on the RADIUS client side that the RADIUS client supports authorization in vendor specific mode and that RADIUS authentication is configured based on the vendor specific mode for it. The names of the user groups in the RADIUS client must match exactly the names of the user groups on the UMC server.
  If the authentication request via the UMC server is successful, SINEC INS returns an Access-Acceptmessage with the UMC user group name of the UMC user to be authorized and tries to authenticate the RADIUS client.

  – **RADIUS authentication with UMC server**
    Enables or disables RADIUS authentication via the UMC server
    When enabled, all users are verified using the UMC user database. The local RADIUS user database is no longer verified.

  – **"Configure UMC server" button**
    With this button, you can switch to the UMC configuration page to configure the UMC server or enable the login to SINEC INS there via the UMC server; refer to section "UMC (Page 59)".
    For RADIUS authentication via the UMC server, it is only necessary to specify the UMC server address. If you do not want to use RADIUS authentication via the UMC server, you need to disable this function after configuring the UMC server using the slider "Enable Radius authentication with UMC server". The slider on the UMC configuration page under "System Administration > General settings > UMC" is used to enable login to SINEC INS via UMC. For this purpose, you need the "Edit" right for the "General settings".

3.2.2 Relay configuration

Users that have the "Edit" right for the RADIUS service can configure the forwarding of RADIUS requests to other RADIUS servers on the "Network services > RADIUS service > Relay configuration" page.

The following control elements are available:

- **RADIUS user groups**
  SINEC INS forwards a RADIUS request to other RADIUS servers if the user name of the RADIUS request belongs to one of the specified RADIUS user groups and is specified as follows:
  - User@RADIUS user group
    The RADIUS user group must contain the character ".", for example mycompany.com
  - RADIUS-Benutzergruppe/Benutzer

  Example: In SINEC INS, the "siemens.com" RADIUS user group is configured. If a RADIUS request contains the user name "testuser@siemens.com", this RADIUS request is forwarded.
- **Relay RADIUS server groups**
  In this area, you configure the RADIUS servers to which RADIUS requests should be forwarded. You combine these RADIUS servers into relay RADIUS server groups.
- **Relay assignment**
  In this area, you define which RADIUS user groups should be assigned to which relay RADIUS server groups. A RADIUS request with a user name that belongs to a RADIUS user group is forwarded to all RADIUS servers of the associated relay RADIUS server groups.

3.3 DHCP Service

SINEC INS can be used as DHCP server and assign IP addresses to devices in the network. The IP addresses can be assigned to devices from configurable IP address ranges or they can be reserved for the MAC addresses of devices.

3.3.1 DHCP configuration

Users that have the "Edit" right for the DHCP service can configure the DHCP server on the "Network services > DHCP service > DHCP configuration" page.

The following control elements are available:

- **Enable DHCP Server**
  Enables / disables the DHCP server.
  Disable the DHCP server before you configure it or make configuration changes. You enable the DHCP server again after the configuration.
- **Subnets**
  In this dialog area you configure the subnets in which SINEC INS is to make the IP address assignments. Based on the specified subnets, you can define in the "IP address ranges" the IP address ranges of these subnets from which the IP addresses are to be assigned.
  The network addresses of the available network adapters are predefined by SINEC INS in the "Subnets" dialog area. Depending on the network adapter via which SINEC INS receives an IP address request from a DHCP client, SINEC INS offers the DHCP client an IP address from the associated IP address range.
  In addition to the predefined network addresses, you can manually specify subnets which can be reached via a router. When a DHCP Relay Agent is set up on the router, SINEC INS uses the Relay Agent IP address in the DHCPDISCOVER message to recognize the subnet in which the IP address assignment must take place.
  You configure a new subnet with the "Create" button. You can modify parameters in configured subnets with the "Edit" button.
  Enter the following parameters in the dialog for configuring a new or existing subnet:
  - **IP Address**
    First IP address of the subnet in which SINEC INS is to make the IP address assignments. The network address of the subnet depends on the subnet mask used.
  - **Subnet Mask**
    Mask to determine the network part and host part of the specified IP address. The first IP address of a subnet can be determined using the subnet mask.

  You can define additional parameters under "Options":

  - **DNS server**
    IP addresses of DNS servers that are sent to the DHCP client as part of the IP address leasement.
  - **Router**
    IP addresses of routers that are sent to the DHCP client as part of the IP address leasement.
  - **NTP server**
    IP addresses of NTP servers that are sent to the DHCP client as part of the IP address leasement.
  - **TFTP server**
    IP address of the TFTP server that is sent to the DHCP client as part of the IP address leasement.
  - **Broadcast address**
    IP address that is used as broadcast IP address of the subnet. Only one IP address is permissible. If you do not want to assign a specific broadcast address, the last IP address of the subnet is used automatically by the device.
  - **Default lease time (seconds)**
    Time period for which an IP address is leased to a DHCP client when the DHCP client does not request a specific lease time from SINEC INS.

  - **Maximum lease time (seconds)**
    The maximum time period that a DHCP client can request for leasing an IP address from SINEC INS.

- **IP address ranges**
  In this dialog area you enter, based on the configured subnets, the IP address ranges from which SINEC INS is to assign IP addresses to DHCP clients. You can specify a maximum of one IP address range per subnet.

- **IP address reservations**
  In this dialog area you can reserve IP addresses for DHCP clients. DHCP clients are identified according to the specified criterion: either by their MAC address or by client identifier/device name. An IP address that is reserved for a DHCP client is not assigned to any other DHCP client by SINEC INS.

  Note

  Do not use IP addresses from dynamic IP ranges for IP address reservations.

  You use the arrow button in the header to update the list of IP address reservations. You configure a new address reservation with the "Create" button. You can modify parameters in configured address reservations with the "Edit" button.
  The following parameters can be specified:

  - **Name**
    Name of the IP address reservation. This name is only used for display in SINEC INS and does not impact the configuration of the DHCP client.
  - **Reservation criterion**
    The DHCP server reserves IP addresses according to the selected criterion. The following criteria are available for selection:
    - MAC address
    - Client identifier/ Device name
  - **Subnets**
    Selection of the subnet in which the IP address is to be reserved. You configure the subnets that are available for selection in the dialog area "Subnets", see section above.
  - **IP Address**
    IP address that is to be reserved for the DHCP client.
  - **MAC Address**
    MAC address of the DHCP client for which the IP address is reserved. Input required if selected as a reservation criterion.
  - **Hostname**
    Hostname that is assigned to the DHCP client.
  - **Client identifier/Device name**
    Client identifier or name of the device assigned to the DHCP client. Input required if selected as a reservation criterion.
  - **DNS server**
    IP addresses of DNS servers that are sent to the DHCP client as part of the IP address leasement. The parameters configured here overwrite the parameters that are configured for the associated subnet.
  - **Router**
    IP addresses of routers that are sent to the DHCP client as part of the IP address leasement. The parameters configured here overwrite the parameters that are configured for the associated subnet.
  - **NTP server**
    IP addresses of NTP servers that are sent to the DHCP client as part of the IP address leasement. The parameters configured here overwrite the parameters that are configured for the associated subnet.

  - **TFTP server**
    IP address of the TFTP server that is sent to the DHCP client as part of the IP address leasement. The parameter configured here overwrites the parameter that is configured for the associated subnet.
  - **Broadcast address**
    IP address that is used as broadcast IP address of the subnet. Only one IP address is permissible. The parameter configured here overwrites the parameter that is configured for the associated subnet. If you do not want to assign a specific broadcast address, the last IP address of the subnet is used automatically by the device.
  - **Domain name**
    Domain name that is sent to the DHCP client as part of the IP address leasement.
  - **Boot file name**
    Path to the file that is to be executed by the DHCP client.
  - **Default lease time (seconds)**
    Time period for which an IP address is leased to the DHCP client when the DHCP client does not request a specific lease time from SINEC INS. The parameter configured here overwrites the parameter that is configured for the associated subnet.
  - **Maximum lease time (seconds)**
    The maximum time period that the DHCP client can request for leasing an IP address from SINEC INS. The parameter configured here overwrites the parameter that is configured for the associated subnet.

- **"Export configurations" button**
  Button for exporting the IP address reservations for DHCP clients. The created file is used to back up the configuration.
  After the export, you will receive a ZIP file "sinecinsDhcpClients.zip" with all DHCP client configurations in CSV format. The selected reservation criterion is also saved.
  The exported CSV file "sinecinsDhcpClients.csv" is unencrypted and can be edited by the user. After the export, the CSV is edited using the operating system. Note that the name of the CSV file as well as the names and the order of the columns contained cannot be changed after the export. Otherwise, it will not be possible to import the configurations later.

- **"Import configurations" button**
  Button for importing the IP address reservations for DHCP clients
  Users with the "Edit" right can import previously exported IP address reservations for DHCP clients from a ZIP file into SINEC INS.
  Follow these steps to import the IP address reservations:

1. Deactivate the DHCP server before the import.
2. Click "Import configurations".
   The "Import configurations" dialog window is displayed.
3. In the browser, navigate to the directory containing the "sinecinsDhcpClients.zip" configuration file to be loaded. Double-click on the relevant ZIP file to apply it.

4. Select the "Override existing configurations" check box to overwrite the existing entries. For IP address reservations, overwriting is based on the name.
5. Click "Import".
   All IP address reservations are imported into SINEC INS.
   During the import, the results of the import process are logged in a log file. The log file is automatically saved on the PC of the user. Each import process is logged by the Syslog service.

You can find an overview of exporting and importing configurations in the section "Overview of importing and exporting configurations (Page 77)".

3.3.2 DHCP assignments

The IP address assignments to devices are displayed on the page "Network services > DHCP service > DHCP assignments". The information in the "Type" column specifies whether the IP address is leased to a device from a configured IP address range or was "reserved" for the MAC address of a device. You can configure IP address ranges for the dynamic assignment on the page "Network services > DHCP service > DHCP configuration" in the area "IP address ranges" and for static IP address reservations in the area "IP address reservations".

Users with the "Edit" right for the DHCP service can refresh the page using the "Refresh" button and convert a leased into a reserved IP address assignment with the "Reserve IP address" button.

A reserved IP address cannot be reserved again using the "Reserve IP address" button.

3.4 NTP service

SINEC INS can be used as NTP server and provide the current time to devices in the network. As a source for the current time, SINEC INS can either use the time of the host PC or the time of another NTP server. To ensure that NTP clients obtain the time from a trusted NTP server, the NTP data packets can be protected with hash algorithms.

NOTICE
Time source NTP server ("Insane time" detection) When SINEC INS uses a different NTP server as time source and detects a time difference of more than 1000 seconds between the NTP server and the PC on which SINEC INS is installed, SINEC INS classifies the NTP server as an untrustworthy time source and cancels the NTP service. Make sure that the time difference between the NTP servers and the SINEC INS PC is less than 1000 seconds.

Users that have the "Edit" right for the NTP service can configure the NTP server on the page "Network services > NTP service".

The following parameters are available for configuring the NTP server:

- **Enable NTP server**
  Enables or disables the NTP server.
  Disable the NTP server before you configure it or make configuration changes. You enable the NTP server again after the configuration.
- **Input interfaces**
  Selection of the network adapter via which the NTP server is to receive NTP requests. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the NTP service.
- **Time source**
  In this dialog area, you specify which time SINEC INS uses as the current time and provides to NTP clients on request.
  - Host device
    SINEC INS uses the time of the device on which SINEC INS is installed as the current time.
  - NTP server
    SINEC INS uses the time of a configured NTP server as the current time. The first NTP server in the list that can be reached by SINEC INS is used as time source. If SINEC INS cannot reach any of the configured NTP servers, SINEC INS uses the host device as time source. If SINEC INS is to authenticate an NTP server before using the time, enter the key ID of an NTP key that you configured in the "NTP keys" dialog area. For successful authentication through SINEC INS, the same NTP key must be installed on this NTP server.
- **NTP keys**
  In this dialog area you can configure NTP keys. These NTP keys can be used for authentication of NTP servers through SINEC INS or for the authentication of SINEC INS through NTP clients. Make sure that the NTP keys are configured on the NTP server and on the NTP clients.
  Note that, if the entered NTP key is longer than 20 characters, SINEC INS considers this value to be hexadecimal. In this case, you need to select the hexadecimal NTP key configuration on your device.
- **Endless NTP Request**
  Allows sending multiple requests from the NTP client to the NTP server at the same time. This function is recommended for SIMATIC devices, for example, SIMATIC S7 PLCs or SIMATIC WinCC Panels.
  In this dialog area, you can manage subnets that are allowed for endless NTP requests. You can configure new subnets with the "Create" button. To do this, enter the following subnet data:
  - IP Address
    First IP address of the subnet. The network address of the subnet depends on the subnet mask used.
  - Subnet Mask
    Mask of the IP subnet
- **"Import subnets" button**
  The button for importing subnets is located in the "Endless NTP Request" area on the right. You can import previously created data of subnets from a CSV file into SINEC INS.

1. First create a CSV file with subnet data. To do this, enter the data in a table and then save the table as CSV file. The table must have **no header** and contain the data in the following order**:**
   - First column: IP Address
   - Second column: Subnet Mask
2. Disable the NTP server before the import.
3. Click "Import subnets".
   The "Import subnets" dialog box appears.
4. Navigate in the browser to the directory in which the CSV file to be loaded is located. Double-click on the desired file to apply it.
5. Click "Import".
   Subnet data is imported into SINEC INS. During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. Each import process is logged by the Syslog service. The information about the subnets that have not been added is logged. If the maximum number of entries is exceeded, addition of further subnets is stopped and superfluous entries are not logged.
   The specified IP addresses and subnet masks must be valid, otherwise no data will be saved. The column delimiter of the CSV file must be "," (comma). The maximum number of subnets to be imported from a CSV file is 10000.

```
sinecins@sinecins-VirtualBox:~/Desktop$ cat sinecinsNTPEndlessRequest.csv
192.168.1.0;255.255.255.0
192.168.2.0;255.255.255.0
192.168.3.0;255.255.255.0
```

Figure 3-7 Example of a CSV file for importing subnets

- **"Export subnets" button**
  Button for exporting the subnet data. The created files are used for data backup.
  After exporting, you obtain a ZIP file "sinecinsNTPEndlessRequest.csv" in CSV format.
  The exported CSV file is unencrypted and can be edited by the user. This ZIP file is downloaded to your device via the browser.

3.5 TFTP service

SINEC INS can be used as TFTP server for file exchange between TFTP clients within a local network area.

3.5.1 TFTP configuration

Users that have the "Edit" right for the TFTP service can configure the TFTP server. The following parameters are available for configuring the TFTP server on the "Network services > TFTP service > TFTP configuration" page:

- **Enable TFTP server**
  Enables or disables the TFTP server.
  Disable the TFTP server before you configure it or make configuration changes. You enable the TFTP server again after the configuration.
- **Input interfaces**
  - Enable network adapter for TFTP service
    Selection of the network adapter via which the TFTP server is to receive TFTP requests. When you select the entry "All / 0.0.0.0", the TFTP server receives TFTP requests from all network adapters. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the TFTP service.
  - Port
    Specification of the port via which the TFTP server is to receive TFTP requests.
- **TFTP root directory**
  Shows the TFTP server root directory of SINEC INS.
  The default path "/opt/sinecins/bin/tftp/var/tftpboot" is set by SINEC INS and cannot be changed.

3.5.2 TFTP file transfer from the SINEC INS Web user interface to the TFTP directory

Users that have the "View" right for the TFTP service can view the files and folders on the TFTP server on the "Network services > TFTP service > File transfer" page. You can manage the files using the "Select an action" drop-down list. The HTTPS protocol is used to execute these actions in SINEC INS. New directories can only be created via the operating system. For created directories, you can navigate to lower-level directories by double-clicking on a directory. To go back to a higher-level directory, double click on ".." in the first line of the directory. The navigation path to the current directory is displayed above the file list to facilitate orientation.

The following actions are available in the "Select an action" drop-down list:

- **Refresh**
  Updates the Web interface
- **Upload / Download / Delete**
  With these actions, you can upload, download or delete one or more selected files.

Note

SINEC INS must have read access rights for the files to be loaded. Otherwise, the file transfer will fail.

To upload a file, proceed as follows:

1. Select the "Upload" action in the drop-down list.
   The "Upload" dialog box appears.
2. Navigate in the browser to the directory in which the file to be uploaded is located. Double-click on the desired file to apply it.
   You can select multiple files.
3. Click "Upload" to upload the file to the TFTP server.
   The file is saved in the current TFTP directory.
   Each upload process is registered by the Syslog service.

To download a file, proceed as follows:

1. Select the required file from the file list. Click on the relevant check box.
   You can select multiple files.
2. Select "Download" in the drop-down list.
3. Navigate to the directory where you want to save the file and confirm the save.
   Each download process is registered by the Syslog service.

3.6 SFTP service

SINEC INS can be used as SFTP server for encrypted file exchange between SFTP clients.

This type of data transfer is protected against unauthorized access by the use of a private key.

The SFTP service can be used, for example, for firmware updates on network devices or for backing up and restoring configuration files for network devices.

The default port for the SFTP server is TCP 22. The port number is configurable.

3.6.1 SFTP configuration

Users that have the "Edit" right for the SFTP service can configure the SFTP server and can export and import configurations. You can find an overview of exporting and importing configurations in the section "Overview of importing and exporting configurations (Page 77)".

The following parameters are available for configuring the SFTP server on the "Network services > SFTP service > SFTP configuration" page:

- **Enable SFTP server**
  Enables or disables the SFTP server.
  Disable the SFTP server before you configure it or make configuration changes. You enable the SFTP server again after the configuration.
- **"Export configuration" button**
  Button for exporting the SFTP configuration. The created file is used to back up the user details.
  After the export, you receive a ZIP file "sinecinsSftpUserBackup.zip" with user configurations. This ZIP file is downloaded to your device via the browser.
  Exported CSV files with SFTP users are encrypted by SINEC INS.
- **"Import configuration" button**
  Button for importing the SFTP configuration
  You can import a previously exported SFTP configuration from a ZIP file into SINEC INS. Follow these steps to import the SFTP configuration:

1. Disable the SFTP server before the import.
2. Click on "Import configuration".
   The "Import configuration" dialog window is displayed.
3. Click "Choose file" and navigate in the browser to the directory containing the "sinecinsSftpUserBackup.zip" configuration file to be loaded. Double-click on the relevant ZIP file to apply it.
4. Click "Import".
   All SFTP configurations for users are imported into SINEC INS. After a successful import, the ZIP file of SINEC INS is extracted and decrypted.
   If a configuration to be imported is already present in the database, it will not be imported. Note that a maximum of 10000 SFTP users can be imported at the same time. If the maximum number of SFTP users is exceeded, addition of further SFTP users is stopped. During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. Each import process is registered by the Syslog service. All information on the users not added is logged.

- **Input interfaces**
  If a host device has multiple network interfaces, you can enable desired network interfaces for the SFTP server. By default, all available network interfaces are enabled. SINEC INS uses TCP port 22 for the SFTP server. This port can be configured. Note that the TCP port 22 may already be used for the SSH connections.
  - Enable network adapter for SFTP service
    Selection of the available network adapters via which the SFTP server is to receive SFTP requests. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the SFTP service.
  - Port
    TCP port via which the SFTP server is to receive SFTP requests. Make sure that the specified port is not already used by another application.
- **SFTP configurations**
  - SFTP server root directory
    Shows the SFTP server root directory of SINEC INS.
    The default path "/opt/sinecins/bin/proftpd/var/sftpboot" is set by SINEC INS and cannot be changed.
  - Enable outgoing/incoming speed limitation
    Enables the text boxes for the maximum data transmission speed
    You can set the upload and download speed of the SFTP server to suit your requirements. The value should be between 10 - 1000000 KBps for the download and upload. If the speed limit is not activated, files are transferred with default speed of 10240 KBps.
  - Max server incoming speed (KBps)
    Specification of the maximum download speed
    The maximum value is 1000000 KBps = 1 GBps.
  - Max server outgoing speed (KBps)
    Specification of the maximum upload speed
    The maximum value is 1000000 KBps = 1 GBps.
  - "Save" button
    Saves changes to the speed limitation entries.
- **SFTP users**
  User data that is needed for user authentication on the SFTP server can be managed in this dialog area. When the SFTP server receives an authentication request from an SFTP user, it checks whether the specified user and the associated password are configured in this dialog area. If the relevant user data is present, the user receives access to the SFTP server and can upload files to the server and download the files stored on the server.
  When creating an SFTP user, note that, to avoid possible SFTP connections from the Linux host, the user name cannot be identical to the Linux host name.
- **"Import SFTP users" button**
  The button for importing SFTP user data is located on the right in the "SFTP users" area. You can import previously created SFTP user details from a CSV file into SINEC INS.
  Follow these steps to import the SFTP users:

1. First, create a CSV file with the SFTP users to be imported. To do this, enter the data of the SFTP users in a table and then save the table as CSV file.
   The table must have **no header** and contain the data in the following order:
   - First column: User name
   - Second column: Corresponding password

   The specified user names and passwords must be valid. Otherwise, no data is saved.
   Please note that the number of SFTP users to be imported from a CSV file is limited to max. 10000.
   The column delimiter of the CSV file must be "," (comma).
2. Disable the SFTP server before the import.
3. Click "Import SFTP users".
   The "Import SFTP users" dialog box appears.
4. Navigate in the browser to the directory in which the CSV file to be loaded is located. Double-click on the desired file to apply it.
5. Click "Import".
   SFTP user data is imported into SINEC INS.
   During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. If a user to be imported is already present in the database, it will not be imported.
   Each import process is logged by the Syslog service. The information on the users not added is logged.
   If the maximum number of entries is exceeded, addition of further SFTP users is stopped and superfluous entries are not logged.

- **SFTP SSH keys**
  The client can use a host key to check the host identity in order to make sure that the connection was established to the correct host (the SFTP server). SINEC INS generates SSH key pairs with the RSA and DSA algorithms. The length of an RSA key is at least 2048 bits and the length of a DSA key is 1024 bits.
  In this area, you can view public keys or regenerate an SSH key pair.
  - RSA public keys
    Display box with the current public RSA host key
  - DSA public keys
    Display box with the current public DSA host key
  - "Copy" button
    Button for copying the relevant public host key to the clipboard
  - "Regenerate SSH key pairs" button
    Button for regenerating the key pairs
    After the operation is confirmed, the public and private host keys are renewed on the user interface with RSA and DSA algorithms.

3.6.2 SFTP file transfer from the SINEC INS Web user interface to the SFTP directory

Users that have the "View" right for the SFTP service can manage SFTP directories and upload and download files on the SFTP server. The HTTPS protocol is used to execute these actions in SINEC INS.

The files and SFTP folders on the SFTP server are displayed on the "Network services > SFTP service > File transfer" page. The "Select an action" drop-down list contains available actions with which you can manage the directories and files. By double-clicking on a directory, you navigate step-by-step to lower-level directories. To go back to a higher-level directory, double click on ".." in the first line of the directory. The navigation path to the current directory is displayed above the file list to facilitate orientation.

The following actions are available in the "Select an action" drop-down list:

- **Refresh**
  Updates the Web interface
- **Upload / Download**
  With these actions, you can upload one or more selected files to the current SFTP directory and download them from the directory to your PC.

  Note

  SINEC INS must have read access rights for the files to be loaded. Otherwise, the file transfer will fail.

- **Move**
  You can move one or more files into a created SFTP directory.
- **Create directory**
  You can create a new directory in the current SFTP directory.
  In the dialog area, enter the name of the directory and save it.
- **Delete**
  You can delete one or more selected files in the current SFTP directory.

To upload a file, proceed as follows:

1. Navigate to the SFTP directory to which you want to upload the desired file.
2. Select the "Upload" action in the drop-down list.
   The "Upload" dialog box appears.
3. In the browser of your operating system, navigate to the directory in which the file to be uploaded is located. Double-click on the desired file to apply it.
   You can select multiple files. The max. size of the files to be uploaded is 1024 MB.
4. Click "Upload" to upload the file to the SFTP server. The file is saved in the current SFTP directory.
   Each upload process is registered by the Syslog service.

To download a file, proceed as follows:

1. Navigate to the SFTP directory in which the file to be downloaded is located.
2. Select the file. Click on the relevant check box.
   You can select multiple files. Directories cannot be downloaded.

3. Select the "Download" action in the drop-down list.
4. In the browser of your operating system, navigate to the directory in which you want to save the file and confirm saving.
   Each download process is registered by the Syslog service.

To move a file, proceed as follows:

1. Navigate to the SFTP directory in which the file to be moved is located.
2. Select the file.
   You can select multiple files.
3. Select the "Move" action in the drop-down list.
   The "Move" dialog box appears.
4. Select the target directory from the list or navigate with a double-click to the target directory to which you want to move the file. If you want to move the file to the root directory, do not select any of the entries in the list. With the "Back" button, you can return to the higher-level directory step by step.
5. Click "Move".
   Each move process is registered by the Syslog service.

3.7 DNS service

SINEC INS can be used as DNS server and respond to name resolution requests from devices or users in the network.

The default port for the DNS server, via which it is to receive requests, is UDP 53. The port number is not configurable. To be able to enable the DNS service, make sure that the UDP port 53 is not already used by another application.

3.7.1 DNS configuration

Users that have the "Edit" right for the DNS service can configure the DNS server.

The following parameters are available for configuring the DNS server on the "Network services > DNS service > DNS configuration" page:

- **Enable DNS server**
  Enables or disables the DNS server
  If the DNS server is enabled, at least one zone and corresponding A records need to be defined. Otherwise, the DNS server cannot resolve any domain name.
  Disable the DNS server before you configure it or make configuration changes. You enable the DNS server again after the configuration.
- **Input interfaces**
  SINEC INS uses UDP port 53 for the DNS server. This port cannot be configured. If a host device has multiple network interfaces, you can enable them for the DNS server. By default, all available network adapters are enabled.
  - Enable network adapter for DNS service
    Selection of the network adapters via which the DNS server is to receive DNS requests. Changes to the network adapter configuration in the operating system are only applied by SINEC INS after a restart of the DNS service.
- **Access Control List (ACL)**
  With access control lists (ACL), access to the DNS server can be restricted and the security of the DNS service can be increased. In ACLs, the devices that can request domain names and make recursive requests are defined by their IP addresses.
  You configure your access control lists in this dialog area.
  You create a new ACL with the "Create" button. You can modify parameters in a configured ACL with the "Edit" button. ACLs that are used by recursive DNS requests or zones cannot be removed. To be able to delete an ACL, you must remove its usage first.
  Enter the following parameters in the dialog for configuring a new or existing ACL:
  - **ACL name**
    Name of the ACL
  - **Subnets / IP addresses**
    Valid subnet address or IPv4 address of the device
  - **"Add" button**
    You can enter up to ten additional IP and subnet addresses with the "Add new" button.

- **Recursive DNS requests**
  If SINEC INS cannot answer a name resolution request itself, SINEC INS can forward this DNS request to other name servers.
  In this dialog area, you configure the following parameters for recursive DNS requests:
  - **Allow recursive DNS requests from**
    Enables or disables recursive DNS requests to the name servers configured in this section
  - **"Create", "Edit" and "Delete" buttons**
    You configure a new recursive name server with the "Create" button. You can create a total of five name servers. You can modify parameters in a configured name server with the "Edit" button.
    Enter the following parameters in the dialog for configuring a new or existing name server:
    • Name server
    • IP address
    Valid IPv4 address of the name server
  - **Allow query from**
    • Any IP address
    Selected by default. All users and devices can make recursive DNS requests.
    • Access Control List
    If at least one ACL is defined, this option can be enabled and the desired ACL entry can be selected from the drop-down list. Only the devices entered in the ACL are authorized to make recursive requests in this case.
  - **Only forward**
    Enabled by default. SINEC INS first checks the saved DNS records and responds to the DNS request itself when it has found the corresponding A record. If the search fails, SINEC INS forwards the request to configured name servers. If one of the addressed name servers has the requested information, the DNS request is resolved and the user can reach the device with the domain name entered in the browser.
    • "Only forward" activated: If neither SINEC INS nor the configured name servers can answer the DNS request, SINEC INS does not make any further attempts to contact other name servers.
    • "Only forward" deactivated: If neither SINEC INS nor the configured name servers can answer the DNS request, SINEC INS attempts to contact other name servers, including the root DNS server, to find information. When the SINEC INS host computer is connected to the Internet, SINEC INS can also forward DNS requests to the upstream DNS server of your provider. For example, when a DNS request is being forwarded to the Google Public DNS, devices will receive replies when they request a domain name, such as www.google.com.
- **DNSSEC-Enable extension**
  Enables the security extension of the DNS protocol for signing the DNS data.
  If enabled, security is guaranteed when resolving domain names. If the addressed name server has resolved the domain name, it secures the data to be sent with its digital signature. SINEC INS validates the signature. If authentication is successful, SINEC INS trusts the data contained in the response and forwards it to the user. The user can then reach the device with the domain name entered in the browser. If authentication fails, the data received from the name server is discarded. If multiple name servers are configured, the DNS request is forwarded sequentially to the next name server until it is resolved or not resolved.
  If the addressed name server does not support a DNSSEC-extension but this is enabled on SINEC INS, the response of the name server is rejected.

3.7.2 DNS zones

To be able to resolve a domain name, the DNS server requires the zone assigned to the domain being searched for. Users that have the "Edit" right for the DNS service can configure DNS zones. Users with the "View" right can view "DNS zones".

The following parameters are available for configuring the DNS zones on the "Network services > DNS service > DNS zones" page:

- DNS zones
  In this dialog area, you configure DNS zones to define a domain in the domain tree.
  You configure a new zone with the "Create" button. You can modify parameters in a configured zone with the "Edit" button.
  Enter the following parameters in the dialog for configuring a new or existing zone:
  - Zone name
  - Allow query from
    • Any IP address
    Selected by default
    • Access Control List
    If at least one ACL is defined, this option can be enabled and the desired ACL entry can be selected from the drop-down list.
- Sub-zones
  You configure DNS sub-zones in this dialog area. Sub-zones are usually defined for sub-domains.
  Example: A domain is divided into DNS zones according to geographical location (Europe, Asia, North America etc.). Sub-zones can then represent different areas within each DNS zone, e.g. production, marketing, sales etc.
  You configure a new sub-zone with the "Create" button. You can modify parameters in a configured sub-zone with the "Edit" button.
  Enter the following parameters in the dialog for configuring a new or existing sub-zone:
  - Sub-zone name
  - Select parent zone
    Selection of a parent zone from the drop-down list

Note

Deleting a zone

When a zone or sub-zone is deleted, please note that all associated configurations, such as sub-zones and DNS records, are also deleted.

3.7.3 DNS records

DNS records are entries in the database of a DNS server in which a domain name is assigned to every IP address known to the server. The server searches its DNS records to answer a request for name resolution.

Users that have the "Edit" right for the DNS service can configure DNS records on the page "Network services > DNS service > DNS records".

To be able to create DNS records, you first need to configure DNS zones on the page "Network services > DNS service > DNS records", to which the DNS records created here are assigned. Users with the "View" right can view DNS records.

The following parameters are available on this page for configuring the DNS records:

- **A records**
  In this dialog area, you configure A records to assign an IP address to a domain.
  - Select zone
    Selection of a zone or a sub-zone from the drop-down list
  - You configure a new A record with the "Create" button. You can modify parameters in a configured A record with the "Edit" button.
    Enter the following parameters in the dialog for configuring a new or existing A record:
    • Domain name
    Name of the domain. The following characters are permitted: "a-z", "." and "-". A domain name cannot begin or end with "-" and ".".
    • IP address
    IPv4 address for the relevant domain
    • Comment
    Optional text

  After you have created an A record for an IP address, you can reach the device via its FQDN (Fully Qualified Domain Name).
  If an ACL is created for a zone, only the device whose IP addresses are specified in the ACL can receive responses to their DNS requests.

- **"Export A records" button**
  Button for exporting the A records of selected zones. Users with the "Edit" right can export A records.
  Follow these steps to export the A records:

1. In the drop-down list, select the zone for which you want to export the A records.
2. Click "Export A records".
   After the export, you receive a CSV file containing A records for the selected zone with pairs of domain name (domain) and IP address (ip). The CSV file is downloaded to your device via the browser. The file name corresponds to the name of the selected zone.
   The exported CSV file is not encrypted by SINEC INS.

- **"Import A records" button**
  Button for importing the A records for the selected zone. Users with the "Edit" right can import A records.
  Follow these steps to import the A records:

1. If no previously exported CSV file with A records is available to you, create it in the following way:
   Enter the A records consisting of domain name and their IPv4 address in a table and then save the table as CSV file.
   The table must have two columns and contain a header with the "domain, ip" titles. The column delimiter of the CSV file must be "," (comma).
2. Disable the DNS server before the import.
3. In the drop-down list, select the zone or sub-zone for which you want to import the CSV file with A records.

4. Click "Import A records".
   The "Import A records" dialog box appears.
5. Click "Choose file" and navigate in the browser to the directory containing the CSV file to be loaded. Double-click on the relevant CSV file to apply it.
6. Click "Import".
   New A records are imported for the affected zone in SINEC INS.
   If an A record to be imported is already present in the database, it will not be imported, but will be recorded in the log file.
   During the import, the results of the import process are logged in a log file. The log file is automatically saved in the browser on the user's PC. Each import process is registered by the Syslog service.
   Note that a maximum of 10000 A records can be imported at the same time. If the maximum number of A records is exceeded, addition of further A records is stopped. This information is logged.
   You can find an overview of exporting and importing A records in the section "Overview of importing and exporting configurations (Page 77)".

- **CNAME records**
  In this dialog area, you configure CNAME records to assign a further domain or subdomain to a domain. A CNAME record therefore references an existing domain and serves to forward multiple names to the same IP address, as shown by the example in the table:

Domain/Subdomain	Record type	Destination
mydomain.com	A record	111.222.333.444
mail.mydomain.com	CNAME	mydomain.com
addressbook.mydomain.com	CNAME	mydomain.com
support.mydomain.com	CNAME	mydomain.com

  – Select zone
    Selection of a zone or a sub-zone from the drop-down list
  – You configure a new CNAME record with the "Create" button. You can modify parameters in a configured CNAME record with the "Edit" button.
    Enter the following parameters in the dialog for configuring a new or existing CNAME record:
    • CNAME
    The alias name of the domain. The following characters are permitted: "a-z", "." and "-".
    • Domain name
    The actual name of the domain or subdomain to which the CNAME record forwards requests.
    • Comment
    Optional text

System administration

4

4.1 General settings

4.1.1 UMC

On the page "System administration > General settings > UMC", you can specify whether SINEC INS should be connected to UMC. Connection to UMC enables authentication via a centralized user management system. UMC users are integrated in SINEC INS using their UMC user groups and assigned to the desired roles there. For information on integrating UMC user groups into SINEC INS, refer to section UMC user groups (Page 66).

The UMC server V2.9.2 is part of the program download/program DVD SINEC INS. Unpack the ZIP file and install the UMC server. You can find the UMC user manual in the directory under "Delivery > BUNDLE > UMC > Documents > Readme > English > UMC_InstallationManual".

Note

You need Windows operating system to install the UMC server.

Configuring UMC

Users that have the "Edit" right for the "General settings" can configure the UMC server on the page "System Administration > General settings > UMC".

The following parameters are available here for configuring the UMC server:

- **Enable login SINEC INS with UMC server**
  Enables or disables the login to SINEC INS with the UMC server
- **UMC server configuration**
  IP address and port of the UMC server via which SINEC INS can reach the UMC server.
- **"Save" button**
  Saves the configuration data

4.1.2 Security configuration

On this page, you can enable the "Legacy ciphers" encryption methods that are no longer recommended and regenerate the SSH key required for them.

By default, legacy ciphers are disabled due to the security restrictions. You can enable legacy ciphers if you agree to the security risks of using them. After you have enabled or disabled legacy ciphers for the SFTP configuration, you need to regenerate SSH keys on the page "SFTP Service > SFTP Configuration". Otherwise, SINEC INS may not be accessible via SFTP clients that use legacy ciphers.

In the event of communication problems via the Secure Syslog server or SFTP server, check the Syslog messages. If the problem is caused by legacy ciphers, one of the following Syslog messages is displayed:

- The SINEC INS SFTP server has detected deviating encryption. Enable the "Legacy ciphers" option under "System administration > General settings > Security configuration".
- The SINEC INS Syslog server has detected deviating encryption. Enable the "Legacy ciphers" option under "System Administration > General Settings > Security Configuration".

Note

Communication with RUGGEDCOM ROX FW V2.15.0

Communication with these devices as SFTP client is only possible with enabled legacy ciphers.

The following operator control is available:

- **Enable legacy ciphers**
  Enables or disables the encryption methods that are no longer recommended.

  Note

  After enabling the legacy ciphers, the Syslog service restarts automatically. If Secure Syslog is enabled, restarting the Syslog service may result in a delay of up to 1 minute when reconnecting Syslog clients.

If the communication problems continue even though legacy ciphers are enabled, this may be caused by the following:

- The SINEC INS SFTP server has detected a different encryption where the legacy ciphers also do not match. The SFTP client is not compatible for a secure connection to the SINEC INS SFTP server.
- The SINEC INS Syslog server has detected a encryption that differs because the legacy ciphers also do not match. The Syslog client is not compatible for a secure connection with the SINEC INS Syslog server.

4.1.3 License

You can activate purchased licenses for SINEC INS on the page "System administration > General settings > License > Licenses". The page "System administration > General settings > License > Used license nodes" provides information on the number of license nodes currently being used by the activated SINEC INS licenses and which services are currently being used by the license nodes.

You can find general information on licensing SINEC INS in section License types (Page 9).

Buffer time for license renewal

If a license has been removed or damaged, SINEC INS triggers a 4-week buffer time for renewal of the license. During the buffer time, all SINEC INS functions remain available. The user is reminded three times a day via Syslog to renew the license and informed about the remaining time.

Once the buffer time expires, SINEC INS switches to demo mode.

4.1.3.1 Activating licenses

On the page "System administration > License > Licenses", you can add licenses for SINEC INS through online or offline activation and view the active SINEC INS licenses on the PC/device.

Active licenses

This dialog area displays the licenses that were activated on the PC/device through online activation. The SINEC INS demo license is not displayed in this dialog area. The SINEC INS licenses that were activated through online activation can be disabled with the "Release" button. An active Internet connection is required for this action. After deactivating licenses, they can be used on a different PC/device with the same license key.

Online activation

In this dialog area you can activate your SINEC INS license using the code that you received when purchasing the license. This type of activation requires an Internet connection on the PC/device on which SINEC INS is installed.

Follow these steps to activate the license:

1. Enter the code in the "License code" text box.
2. Click the "Check" button.
   If the entered code is valid, the associated license type is displayed and the "Activate" button will become active.
3. Click the "Activate" button to activate the SINEC INS license.

Offline activation

In this dialog area you can activate your SINEC INS license using a license container that you export from SINEC INS.

Follow these steps to activate the license:

1. Click on the "Export license container" button.
2. Navigate to the storage directory where the file "SINEC_INS_LICENSE_CONTAINER.WibuCmRaC" is stored.
3. Send the license container to the Siemens Industry Online Support:
   - Log in on the Support Request (https://support.industry.siemens.com/cs/my?lc=en-US) Internet page.
   - Create a new support request. Enter "SINEC INS" in the search bar and click "Find". Select "SINEC INS Basic" under Products and click "Next".
   - Fill in the "Problem description" form. Enter the "SINEC INS License" keyword for "Topic". Provide the ticket ID of the license package and attach the file "SINEC_INS_LICENSE_CONTAINER.WibuCmRaC". Click "Next".
   - Enter your contact data and click "Send".

4. The Siemens Industry Online Support verifies your request and will then return the license container that you can use to activate your SINEC INS license. Save the file in your storage directory.
   Contact Customer Support via:
5. Click the "Choose file" button.
6. Navigate to the storage directory and select the license container "SINEC_INS_LICENSE_CONTAINER.WibuCmRaU".
7. Confirm your selection with the "Open" button and click the "Import license" button.

Result

The offline license is imported.

Deactivating the offline license

Contact Customer Support via Support request, see the procedure "Offline activation". Provide the license number of the license package to be released.

Result

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

4.1.3.2 Used license nodes

The page "System administration > General settings > License > Used license nodes" provides information on the number of license nodes currently being used by the activated SINEC INS licenses and which services are currently being used by the license nodes. You can use the "Remove nodes" button to remove IP addresses from the license and thus release the license for other IP addresses. This makes sense after IP address changes of Syslog and TFTP clients. SINEC INS automatically considers changed and deleted IP addresses of RADIUS clients in the license nodes used. A SINEC INS restart automatically removes use of the Syslog, TFTP, SFTP and DNS services through license nodes.

4.1.4 Certificates

By default, SINEC INS contains a self-signed server certificate for HTTPS connections that you can generate again on the page "System administration > General settings > Certificates". Generate the server certificate again when the network adapter configuration of the PC on which SINEC INS is installed has changed. You will have to log in to SINEC INS again afterward. Also check the status of the network services after each login.

Certificates must be stored in a directory under /opt/sinecins . The owner and directory group must be sinecins. The path should be provided via the corresponding configuration of the SINEC INS user interface.
We urgently recommend saving the certificates securely on the SINEC INS host PC.

Using your own certificate

If you want to use your own certificate for SINEC INS instead of the default server certificate, proceed as follows:

1. Specify the parameters of this certificate.
2. Copy the files of your certificate into the specified directories and then click the "Import" button.
   The certificate to be imported should fulfill the following requirements:
   - The certificate must have one of the supported formats; see below.
   - The Subject and Issuer of the certificate must have a CN (Common Name) entry.
   - An End entity must be declared as End entity and a Certificate authority as Certificate authority in the Basic constraints.

   The following signature algorithms are supported:
   - sha1-with-RSA
   - sha224-with-RSA
   - sha256-with-RSA
   - sha384-with-RSA
   - sha512-with-RSA

   The following public keys are supported:
   - RSA 2048 Bit
   - RSA 4096 Bit
   - The Key usage box cannot be empty.

   After the certificate has been imported, the connection to SINEC INS is set up again.
3. Refresh your browser about 30 seconds after importing the certificate.
4. Depending on the certificate type, enter the following parameters for the certificate you are importing:
   - Certificate type
     You can select from types crt/cer and p12. Certificates in crt/cer format should be encoded with Base64.

For crt/cer certificates:

- Path to certificate
  Path to the certificate file.
- Path to private key
  Path to the private key of the certificate in pem format.
- Password protected
  Select this check box if the private key is protected by a password.
- Password of private key
  By using the eye symbol next to the text box, you can hide or show the password.

- Signed by CA
  Select this check box when the certificate was signed by a Certificate Authority (CA).
- Path to CA certificate
  Path to the CA certificate file. If there is a CA certificate chain, this certificate chain must be imported.

For p12 certificates:

- Path to container (for p12 certificates)
  Path to the container file of the certificate.
- Password protected
  Select this check box if the container is protected by a password.
- Container password (for p12 certificates)
  By using the eye symbol next to the text box, you can hide or show the password.
- Signed by CA
  Select this check box when the certificate was signed by a Certificate Authority (CA).
- Path to CA certificate
  Path to the CA certificate file. If there is a CA certificate chain, this certificate chain must be imported.

4.1.5 HTTP(S) port configuration

SINEC INS uses the following TCP ports by default:

- TCP port 5053 for HTTPS backend connection
- TCP port 443 for HTTPS Web server connection
- TCP port 80 for HTTP Web server connection

Users that have the "Edit" right for system settings can define HTTP(S) ports on the page "System Administration > General settings > HTTP(S) port configuration". The entered value must be between 1 and 65535 and not yet occupied.

Enter the desired port number in the relevant input box and confirm the change with the "Save" button. Make sure that the specified port is not already used by another application. However, we do not recommend using standardized ports between 1 and 1023 for HTTP(S). Note that entered ports cannot be identical.

After a port is updated, the user session is ended because the backend and/or frontend services are restarted. You need to log in again.

4.2 Authorization management

4.2.1 Components

The following components are important for configuring user authorizations:

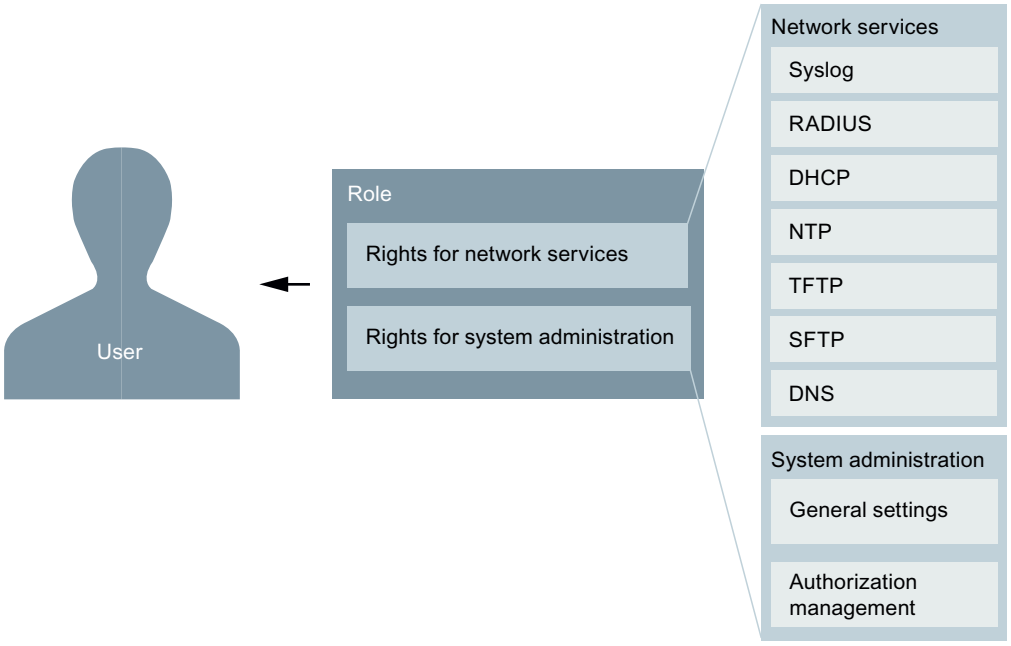


Figure 4-1 Authorization management components

One or more roles are assigned to each user. Each role includes rights for configuration of the network services as well as for system administration.

Users

Users can be centrally managed in User Management Component (UMC) and then used in SINEC INS or configured locally in SINEC INS, refer to section Users (Page 66).

The "SuperAdmin" user with the "admin" role is available by default after the installation of SINEC INS. This role contains all rights for network services and for system administration. The user and the role can only be edited or deleted by the user "SuperAdmin". You can find information on the initial credentials of the "SuperAdmin" user in section Logon (Page 14).

Roles

A role uses included rights to determine which functions are available to the user, see section Roles (Page 66).

Rights

There are rights for network services and rights for system administration. The rights for network services grant permission to configure services such as RADIUS and NTP. The rights for system administration grant permission for general settings and for authorization management. While the authorization management includes the configuration of users, roles and role assignments, the general settings include UMC and license settings as well as the configuration of the server certificate.

Rights are assigned to roles on the "System Administration > Role assignments" page.

4.2.2 Users

4.2.2.1 UMC user groups

UMC (User Management Component) is a database for the central administration of user data. In SINEC INS, the UMC users can be used after the UMC user groups have been included by specifying the UMC user group names. The editor under "System administration > Users > UMC user groups" can be used to integrate the UMC user groups. The specified name of the UMC user group in SINEC INS must be identical to the name of the UMC user group on the UMC server. The UMC group names are case-sensitive.

The name of the UMC user group can contain max. 60 characters. The following characters are permitted: a-z, A-Z, 0-9 and _ . / \

The user of a UMC user group can be used to log in when UMC was set up and the UMC address data were specified in SINEC INS under "System administration > General settings > UMC".

4.2.2.2 Local users

As an alternative to employing users from UMC, users can be configured under "System administration > Users > Local users". Users that are to be used must be enabled. The system-defined user "SuperAdmin" can only be edited by itself and it cannot be deleted.

4.2.3 Roles

You can create, edit and delete roles on the "System administration > Roles" page. The system-defined role "admin" can only be edited by the user "SuperAdmin" and it cannot be deleted.

4.2.4 Role assignments

On the page "System administration > Role assignments", UMC user groups and local users as well as rights can be assigned to the roles that were created in the role administration. For a user to be able to log in to SINEC INS, a user must be assigned to a role.

In the "Assigned UMC user groups/Local users" tab, the desired UMC user groups and users are assigned to a role via the "Assign UMC user groups" or "Assign local users" buttons.

The authorizations for the configuration of network services as well as rights for system administration are assigned to a role in the "Rights" tab.

Syslog messages

5

5.1 Structure of the Syslog Messages

SINEC INS supports both RFC 5424 and RFC 3164 for receiving events. By default SINEC INS stores events in its own Syslog server. Using the relay functionality SINEC INS can forward events to other Syslog servers. The events are transferred to this Syslog server in accordance with RFC 5424.

A Syslog message is composed of the following parameters:

Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification
TIMESTAMP	Time stamp in the format "2010-01-01T02:03:15.0003+02:00" as the local time including the time zone and correction for daylight saving / standard time if needed.
HOSTNAME	References the source computer with its FQDN, hostname or IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time. Example: [timeQuality tzKnown="0" isSynced="0"] The "tzKnown" parameter indicates whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter indicates whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
MSG	
MESSAGE	Message as ASCII string (English)

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in RFC 5424 under: (https://tools.ietf.org/html/rfc5424)

5.2 Tags in Syslog Messages

The "MESSAGE" parameter contains tags that are filled dynamically with the data of the respective event. These tags are displayed within curly brackets {variable} in the "Message text" field in section "List of security-related Syslog messages (Page 70)".

The following tags occur in the "MESSAGE" parameter of the Syslog messages:

Tag	Description	Format	Possible values or example
{User type}	String that categorizes users according to the existing authentication procedure	%s	Local UMC
{User name}	String that identifies the authenticated user based on their name	%s	SuperAdmin
{Destination user name}	String that identifies the target user based on his/her name	%s	Testuser
{Role name}	String that identifies a role based on its name.	%s	Administrator
{Operation Type}	String for the designation of an operation	%s	added changed updated deleted edited imported exported etc.
{Service Type}	String for the designation of a SINEC INS network service	%s	RADIUS, TFTP, Syslog etc.
{Service Feature}	String for the designation of a function of the network service	%s	Syslog Relay, RADIUS Clients, DHCP Assignments etc.
{License Activation Method}	String to indicate the current license type	%s	Offline Online
{Request Owner Name}	String for the user name of WBM authentication or MAC address of the device for port authentication	%s	Station1
{Client Name}	String for the name of the RADIUS clients	%s	SCALANCE_M876

5.3 List of security-related Syslog messages

This section describes the security-relevant Syslog messages. The structure of the messages is based on IEC 62443-3-3.

Identification and authentication of human users

Message text	{User type} User {User name} logged in
Example	Local User "SuperAdmin" logged in
Explanation	A user has successfully logged in.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{User type} User {User name} failed to log in
Example	Local User "SuperAdmin" failed to log in
Explanation	The login of a user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{User type} User {User name} logged out
Example	Local User "SuperAdmin" logged out
Explanation	A user has logged out successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

User account management

Message text	{User type} User {User name} changed {User Type} user {Destination user name}'s password
Example	Local User "SuperAdmin" changed Local user "Tester"'s password
Explanation	A user has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} disabled {User Type} user {Destination user name}
Example	Local User "SuperAdmin" disabled Local user "Tester"
Explanation	A user has disabled the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} created {User Type} user {Destination user name}
Example	Local User "SuperAdmin" created Local user "Tester"
Explanation	A user has created a user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} changed {User Type} user {Destination user name}
Example	Local User "SuperAdmin" changed Local user "Tester"
Explanation	A user has changed an existing user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} changed {User type} user {Destination user name} to {Destination user name}
Example	Local User "SuperAdmin" changed Local user "Tester1" to "Tester2"
Explanation	A user has changed the name of an existing user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} deleted {User Type} User {Destination user name}
Example	Local User "SuperAdmin" deleted Local user "Tester"
Explanation	A user has deleted an existing user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{User type} User {User name} enabled {User Type} User {Destination user name}
Example	Local User "SuperAdmin" enabled Local user "Tester"
Explanation	A user has enabled the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Management of the identifiers

Message text	{User type} User {User name} added a user-role matching
Example	Local User "SuperAdmin" added a user-role matching
Explanation	A user has assigned the UMC user groups or local users to a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 1.4

Message text	{User type} User {User name} deleted a user-role matching
Example	Local User "SuperAdmin" deleted a user-role matching
Explanation	A user has deleted the assignment of a role to the UMC user groups or local users.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: SR 1.4

Message text	{User type} User {User name} created role {Role name}
Example	Local User "SuperAdmin" created role "Service"
Explanation	A user has created a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: Reference SR 1.4

Message text	{User type} User {User name} deleted role {Role name}
Example	Local User "SuperAdmin" deleted role "Service"
Explanation	A user has deleted a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3: Reference SR 1.4

Message text	{User type} User {User name} updated role {Role name}
Example	Local User "SuperAdmin" updated role "Service"
Explanation	A user has changed the configuration of an existing role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	{User type} User {User name} updated role {Role name} to {Role name}
Example	Local User "SuperAdmin" updated role "Service01" to "Service02"
Explanation	A user has changed the name of an existing role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	{User type} User {User name} changed role {Role name}s rights
Example	Local User "SuperAdmin" changed role "SyslogAdmin"s rights
Explanation	A user has changed the rights of an existing role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Failed login attempts

Message text	The session of {User type} user {User name} was ended after 10 minutes of inactivity
Example	The session of Local user "SuperAdmin" was ended after 10 minutes of inactivity
Explanation	The session of a user was terminated due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Identification and authentication of devices

Message text	Authentication request of {Request Owner Name} for radius client {Client Name} is accepted
Example	Authentication request of "Station1" for radius client "SCALANCE_M876_1" is accepted
Explanation	Device access is granted due to successful 802.1X authentication.
Severity	Info
Facility	Security/authorization
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	Authentication request of {Request Owner Name} for radius client: {Client Name} is rejected
Example	Authentication request of "Station1" for radius client "SCALANCE_M876_1" is rejected
Explanation	Device access is denied due to unsuccessful 802.1X authentication.
Severity	Warning
Facility	Security/authorization
Standard	IEC 62443-3-3 Reference: SR 1.2

Limiting the number of simultaneous sessions

Message text	The max number of 10 concurrent login sessions exceeded
Example	The max number of 10 concurrent login sessions exceeded
Explanation	The maximum number of simultaneous Web sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Non-deniability

Message text	{User type} User {User Name} {Operation type} {Service type} {Service feature} configuration
Examples	Local User "SuperAdmin" changed Syslog network interfaces configuration UMC User "Tester" updated a DHCP IP ranges configuration Local User "SuperAdmin" added a DHCP Host Specific IP configuration Local User "SuperAdmin" deleted a RADIUS relay user group configuration
Explanation	A user has changed a configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{User type} User {User Name} activated an {License Activation Method} license
Example	Local User "SuperAdmin" activated an Online license
Explanation	A user has enabled a license.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{User type} User {User Name} released a license
Example	Local User "SuperAdmin" released a license
Explanation	A user has released a license.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Software and information integrity

Message text	Integrity check failed for {service type} service
Example	Integrity check failed for Syslog service

Explanation	Integrity check failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Appendix A

A

A.1 Overview of importing and exporting configurations

Importing own configurations

For some network services, users that have the "Edit" right for the relevant network service can import their own CSV files with configuration data. The following table provides an overview of the necessary data and requirements for importing the configurations. The order of the data is specified in the "Column number and input data" column and cannot be changed. The specified names, passwords, IP addresses and MAC addresses must be valid. Otherwise, no data is saved. The column delimiter in the CSV file must be "," (comma). The number of configurations to be imported from a CSV file can be no more than 10000 entries. Before the import, you need to disable the relevant network service.

Service	Button for import	Header in the CSV file	Column number and input data	Comment
RADIUS service > RADIUS configuration	Import radius users	No	1. User name 2. Password 3. admin/operator	The user names and passwords are case-sensitive. The "admin" user type receives write permissions for RADIUS clients and the "operator" user type receives read permissions.
	Import radius clients	No	1. Name of the RADIUS client 2. IP address 3. Shared secret 4. yes/no	The names and shared secrets are case-sensitive. The "yes" parameter enables the Message-Authenticator attribute on the RADIUS client (e.g. for SCALANCE devices). The "no" parameter disables the Message-Authenticator attribute on the RADIUS client (e.g. for RUGGEDCOM devices).
	Import radius devices	No	1. MAC address 2. VLAN ID or name	"-" or ":" can be used for MAC addresses. The MAC addresses are case-sensitive.
	Import VLAN assignments	No	1. General certificate name of the client 2. VLAN ID or name	The names are case sensitive.
SFTP service > SFTP configuration	Import SFTP users	No	1. User name 2. Password	The user names and passwords are case-sensitive
DNS service > DNS records	Import A records	Yes: domain,ip	1. Domain name 2. IP address of the domain	The domain names are case-sensitive

Exporting and importing SINEC INS configurations

Users that have the "Edit" right for the relevant network service can export network service configurations to back up the configuration data. The "Export configurations" button is available for the relevant network service for this purpose. You can import the configuration to SINEC INS with the "Import configurations" button of the respective network service. Before the import, you need to disable the relevant network service. Some CSV files are unencrypted and can be edited by users. After the export, the CSV files are edited using the operating system. Note that the names of the ZIP and CSV files as well as the names and order of the columns contained cannot be changed.

The following table provides you with an overview of the network services for which you can export the configurations with the "Export configurations" button:

Service	ZIP file name and contents of the file	Comment
RADIUS service > RADIUS configuration	sinecinsRadiusConfiguration.zip • sinecinsRadiusUsers.csv • sinecinsRadiusClients.csv • sinecinsRadiusEapTlsVlans.csv • sinecinsRadiusEndDevices.csv	The "sinecinsRadiusUsers.csv", "sinecinsRadiusClients.csv" and "sinecinsRadiusEapTlsVlans.csv" files are encrypted and cannot be edited. The "sinecinsRadiusEndDevices.csv" file is unencrypted and can be edited by the user.
DHCP service > DHCP configuration > IP address reservations	sinecinsDhcpClients.zip • sinecinsDhcpClients.csv	The CSV file is unencrypted and can be edited by the user
SFTP service > SFTP configuration	sinecinsSftpUserBackup.zip • sinecinsSftpUserBackup.csv	The CSV file is encrypted and cannot be edited

You can also export the files as CSV files with the following network services:

Service	Button for export	Comment
Syslog service > Syslog messages	Export messages	The file is unencrypted.
DNS service > DNS records > A records	Export A records	The file is unencrypted and can be edited by the user. You can import the file with "Import A records". The file name can be freely selected.
NTP service > NTP configuration	Export subnets	The "sinecinsNTPEndlessRequest.csv" file is unencrypted and can be edited by the user. You can import the file with "Import subnets".

Index

T

U