



SIEMENS

Secure connection of an RTU with CP 1243-7 LTE to TeleControl Server Basic

TeleControl Server Basic/ SINEMA Remote Connect/
CP 1243-7 LTE

<https://support.industry.siemens.com/cs/ww/en/view/39863979>

Siemens
Industry
Online
Support



Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

Security information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: <https://www.siemens.com/cert>.

Table of contents

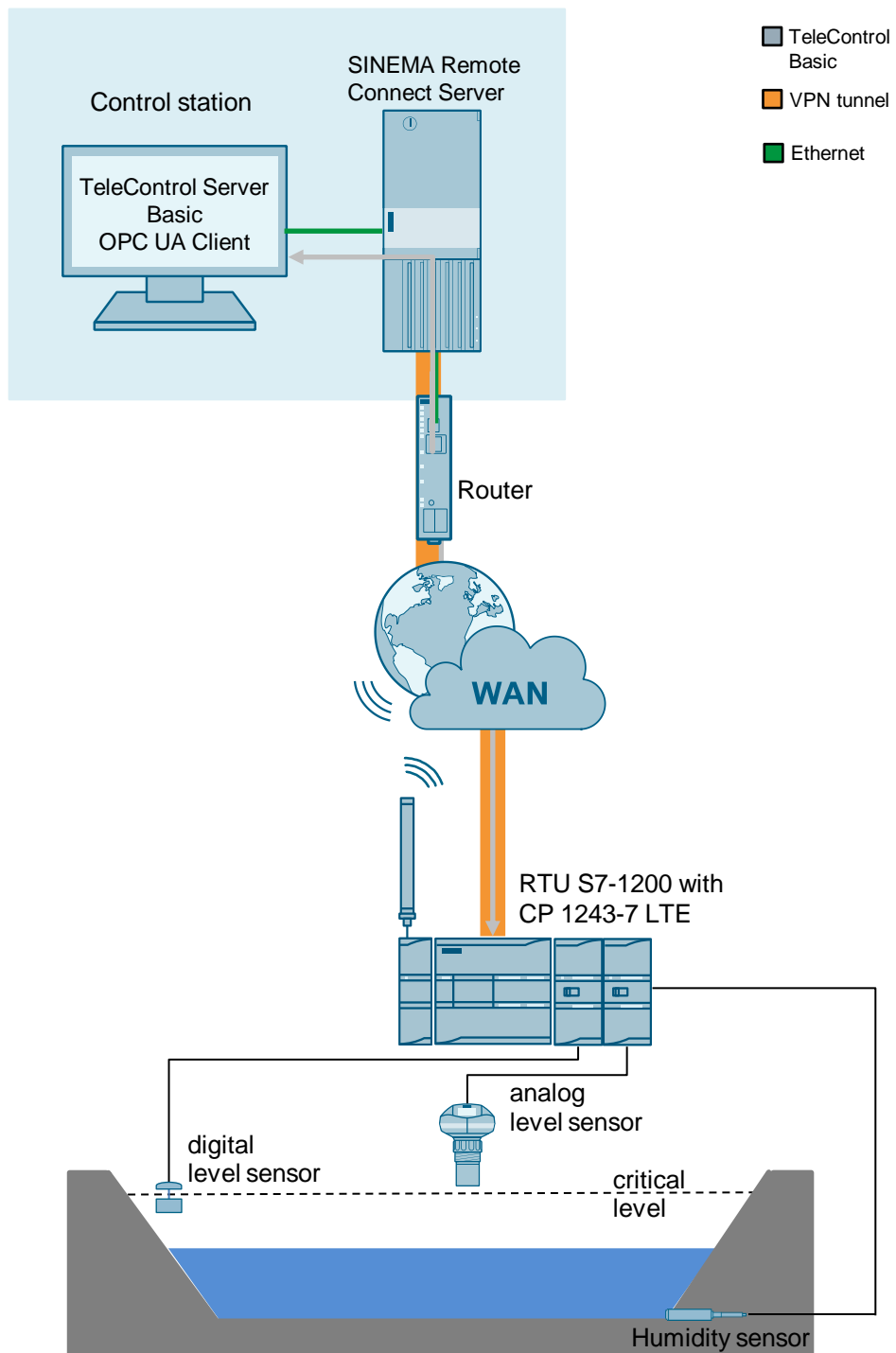
Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Components used	6
2 Engineering	7
2.1 Hardware configuration	7
2.2 Configuration and project engineering	9
2.2.1 Configuring SINEMA Remote Connect Server	9
Configure default settings	10
Creating participant groups	14
Create devices	15
2.2.2 Configure RTU with SIMATIC S7-1200.....	17
2.2.3 Configure TeleControl Server Basic.....	23
2.2.4 Download TIA project to the RTU with SIMATIC S7-1200.....	28
3 Useful information	30
3.1 SINEMA Remote Connect.....	30
3.2 TeleControl Basic	32
3.2.1 Transmission types of data points.....	32
3.2.2 Transmission mode of the data points	33
4 Appendix	34
4.1 Service and Support.....	34
4.2 Industry Mall	35
4.3 Links and literature	35
4.4 Change documentation	35

1 Introduction

1.1 Overview

The infrastructure of a water treatment plant contains an RTU (Remote Terminal Unit) with S7-1200 and CP 1243-7 LTE to securely transmit encrypted process data over the mobile radio network to the control station.

Figure 1-1



Use case

The RTU needs to monitor the level of a stormwater overflow basin with a fill level sensor. To do this, a digital level sensor (float) is installed which is activated when a critical level is exceeded. In this case, the RTU must send an alarm to the control station.

The RTU establishes an OpenVPN connection to SINEMA Remote Connect Server.

The RTU communicates with TeleControl Server Basic via this OpenVPN connection and transmits process data over the TeleControl Basic protocol.

Any OPC client, for example WinCC Professional RT, can be connected via the OPC interface of the TeleControl server.

Advantages

The solution presented in this document offers you the following advantages:

- TeleControl Server Basic enables economical data communication between remote stations and a control center.
- The OPC UA interfaces of TCSB provide the data from the connected stations to one or more connected OPC UA clients.
- To increase reliability, the CPs can cache event data of various classes in the event of connection loss, then send the data to the TeleControl server in bundled form.
- If a brief connection loss occurs between the OPC UA client and the TCSB OPC UA server, the data remain available in the data buffer. Once the connection is restored, all the data that were not transmitted are then sent to the OPC UA client.

1.2 Components used

This application example was created with the following hardware and software components:

Table 1-1

Component	Quantity	Item number	Note
CPU 1212C DC/DC/DC	1	6ES7 212-1AE40-0XB0	V.4.4 or higher
CP 1243-7 LTE	1	6GK7 243-7KX30-0XE0	V3.3 or higher
ANT794-4MR	1	6NH9860-1AA0	Omnidirectional antenna for 4G, 2G and 3G networks
SIM card	1		
SCALANCE M816-1	2	6GK5816-1AA00-2AA2	Or another DSL router
TeleControl Server Basic 8 V3.1.1.0	1	6NH9910-0AA31-0AA0	
UaExpert	1	Freeware	Download via https://www.unified-automation.com/downloads/opc-ua-clients.html
SINEMA Remote Connect Server V3.1	1	6GK1720-1AH01-0BV0	License for 4 VPN connections
SIMATIC IPC627D	1	6AG4131-2.....-.....	Serves as SINEMA Remote Connect Server. You can also use another PC.
M6 programming device	1-3	6ES7718-1.....-0...	Required for: <ul style="list-style-type: none"> SINEMA Remote Connect Client TeleControl Server Basic Engineering You can also use other PDs/PCs.
STEP 7 Professional V17		6ES7822-1AA07-0YA5	

This application example consists of the following components:

Table 1-2

File name	Note
39863979_TCSB_CP_SRC_DOC_V10_de.pdf	This document
39863979_TCSB_CP_SRC_PROJ_V10.zip	TIA V17 Project

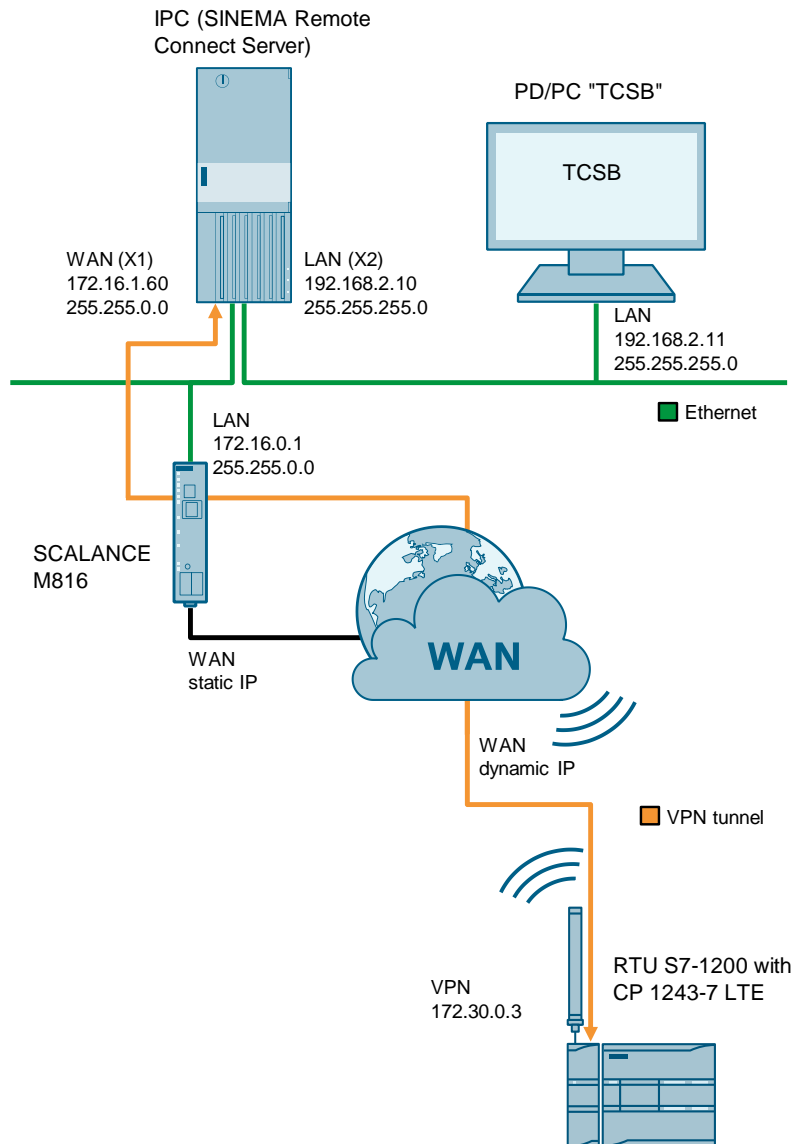
2 Engineering

2.1 Hardware configuration

The focus of this application example is on the communication between the RTU and the control station. Therefore, the implementation does not use any sensors, nor does it use an OPC client.

The following graphic shows the hardware setup of the solution.

Figure 2-1



The following Table provides an overview of all IP addresses used in this example. Assignment of static IP addresses is assumed.

Table 2-1

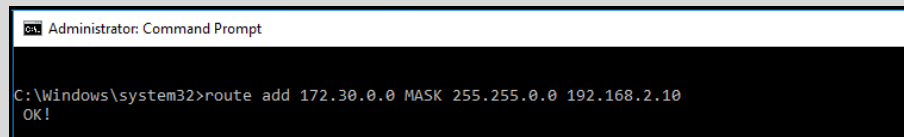
Component	IP address	Subnet mask	Description
Programming device or PC "TCSB"	192.168.2.11	255.255.255.0	TeleControl Server Basic
IPC (SINEMA Remote Connect Server)	WAN (X1) 172.16.1.50	255.255.0.0	
	LAN (X2) 192.168.2.10	255.255.255.0	
RTU with S7-1200 (CPU)	192.168.2.3	255.255.255.0	For downloading
SINEMA Remote Connect clients	172.30.0.1- 172.30.255.254	255.255.0.0	Virtual IP addresses (defined IP range)

Note

If you have configured multiple interface cards on your PC or server (e.g. PD/PC "TCSB"), and you cannot configure a default gateway for the TCSB, add a static route to the Windows routing table.

1. Start Command Prompt (Desktop app) as an administrator.
2. Enter the following command:
`route add 172.30.0.0 MASK 255.255.0.0 192.168.2.10`
3. Press the Enter key.

Result:



172.30.0.0: Target subnet (VPNs defined IP range)
192.168.2.10: SINEMA RC Server (LAN)

2.2 Configuration and project engineering

This chapter describes the most important steps of the configuration:

- Configure SINEMA Remote Connect Server (chapter [2.2.1](#))
- Configure RTU with SIMATIC S7-1200 (chapter [2.2.2](#)) or download the included project (chapter [2.2.4](#))
- Configure TeleControl Server Basic (chapter [2.2.3](#))

Note

To check the time validity of certificates, it is important that the current date and time is kept on all devices.

Check the time specification on all devices and adjust if necessary. Alternatively, you can have the system time automatically synchronized with an NTP Time Server. This ensures that the current time is obtained precisely.

2.2.1 Configuring SINEMA Remote Connect Server

This chapter shows you all the necessary steps to configure SINEMA Remote Connect Server for the application described here.

In order to put the application example into operation, SINEMA Remote Connect Server must be installed and the web server must be accessible via the WAN interface.

The process for installing SINEMA Remote Connect Server can be found in its instruction manual:

<https://support.industry.siemens.com/cs/ww/en/view/109482121>.

Note

The router through which SINEMA Remote Connect Server is connected to the internet must have a fixed public IP address or a DNS name.

Note

To enable a secure VPN connection, you must set up port sharing on the VPN client side and port forwarding on the VPN server side for each of the routers. The following FAQ shows you which ports (UDP port 1194 by default) are necessary for this:

<https://support.industry.siemens.com/cs/ww/en/view/109745584>

Configure default settings

This chapter explains how to configure the default settings of SINEMA Remote Connect Server.

1. Assign an IP address (in the address range of the server) to your "PD/PC" to configure SINEMA Remote Connect Server (e.g. 172.16.1.50).
2. Connect your "PD/PC" to the WAN port of SINEMA Remote Connect Server.
3. Open the SINEMA Remote Connect Server web server via the IP address that you assigned to the WAN port during the installation (e.g. 172.16.1.60).
4. Depending on your browser, you may need to trust a certificate or confirm a security exception.
5. Log into the web server with your user data.

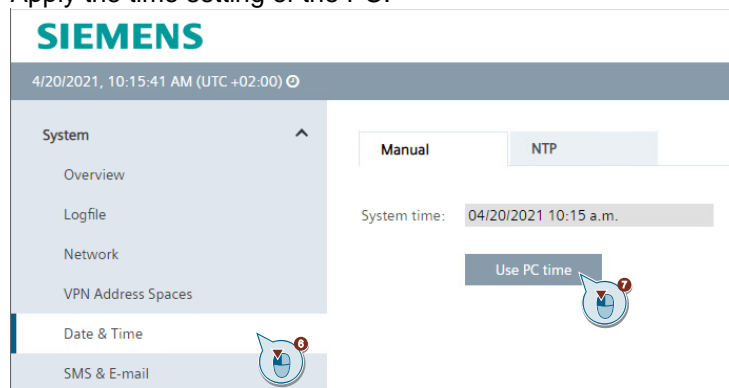
Note

When you log in for the first time, or after a reset to factory settings, the login details are set as follows:

- Name: admin
- Password: admin

Assign a username and a new password for the administrator.

6. Navigate to "System > Date & Time".
7. Apply the time setting of the PC.

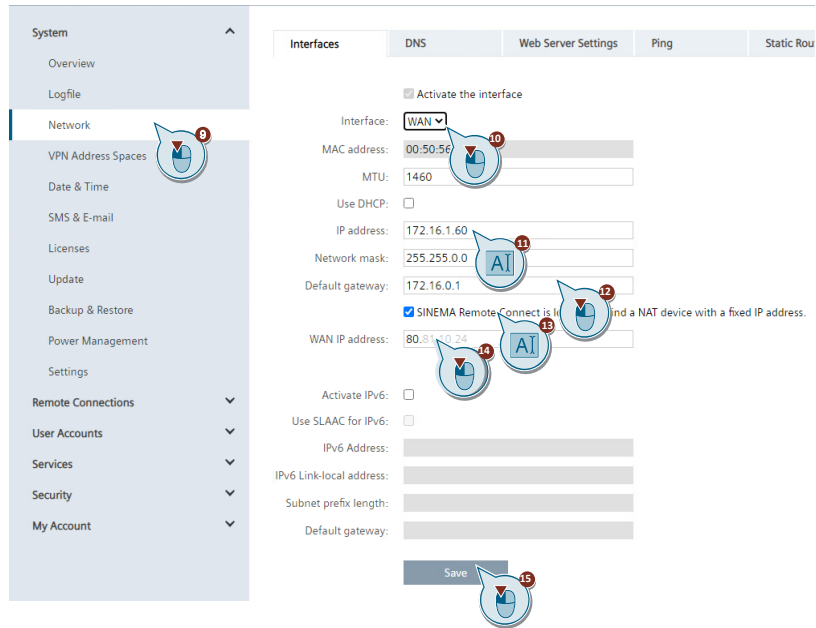


Note

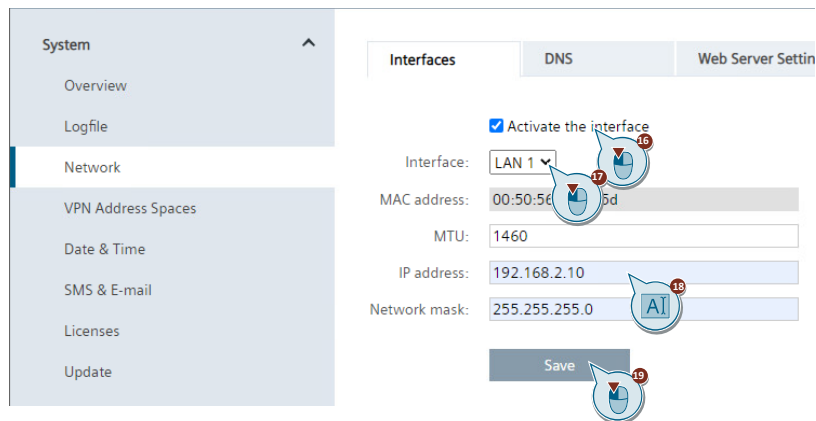
To establish secure communication, it is essential that the current time and date are set on the SINEMA Remote Connect Server. Otherwise the certificates used will be interpreted as invalid and secure VPN communication is not possible.

8. Optionally, you can also specify an NTP server in the "NTP" tab.

9. Navigate to the menu item "System > Network".
10. Select the WAN port from the drop-down list.
11. Set the IP address and subnet mask.
12. Enter the LAN IP address of your DSL router as the "default gateway".
13. Enable the option "SINEMA Remote Connect is located behind a NAT device".
14. Enter the WAN IP address of your DSL router.
15. Save the settings with "Save".



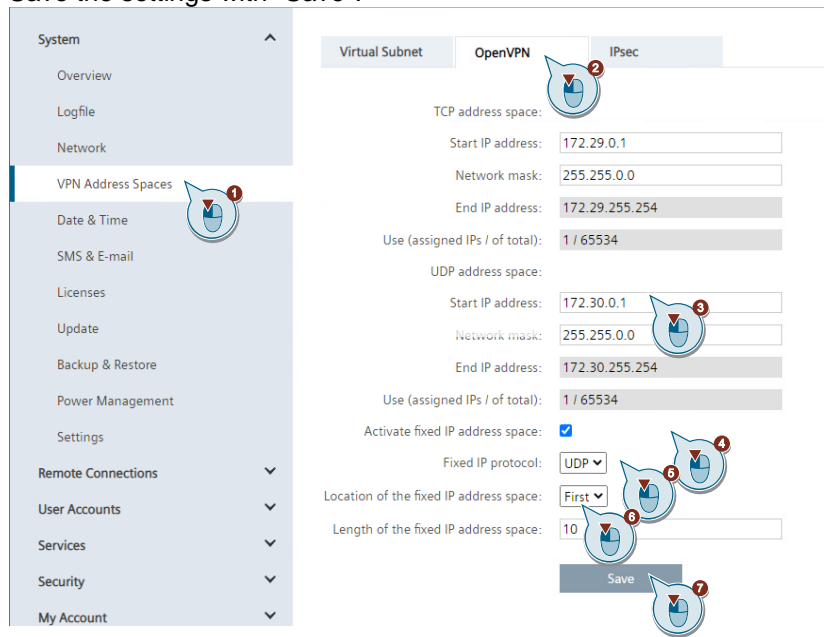
16. Enable the interface (via "Activate the interface").
17. Select the LAN port from the drop-down list.
18. Set the local IP address (192.168.2.10) and subnet mask.
19. Save the settings with "Save".



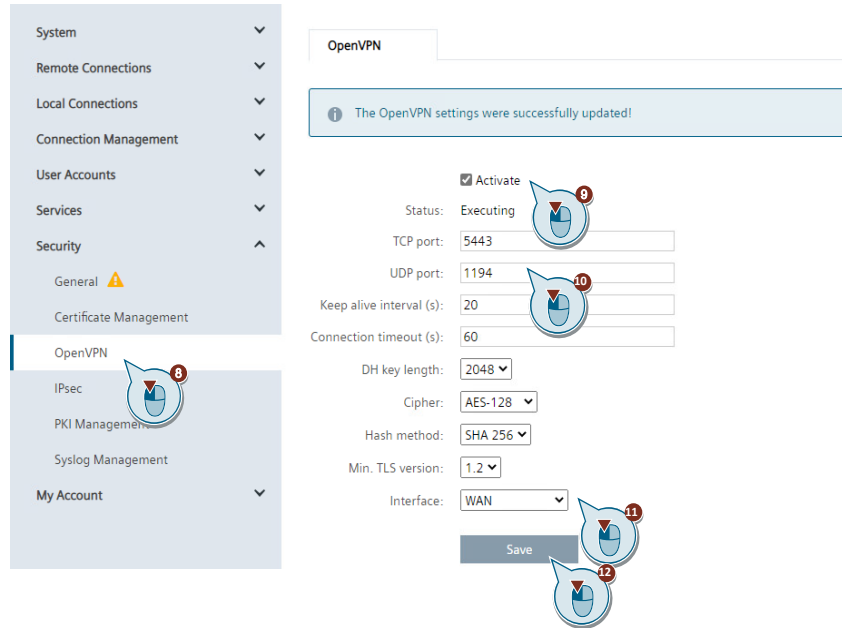
VPN settings

The address range for the VPN must be defined.

1. Navigate to "System > VPN Address Spaces".
2. Change to the "OpenVPN" tab.
3. Assign a virtual IP address to SINEMA Remote Connect clients by defining an IP range in the server.
4. Enable the fixed IP address range.
5. Select "UDP" as the fixed IP protocol.
6. Select "First" as the location of the fixed IP address space.
7. Save the settings with "Save".



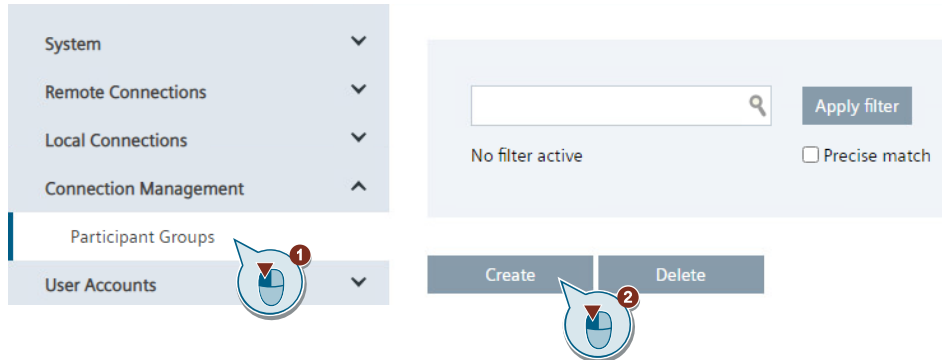
8. Navigate to the menu item "Security > OpenVPN " to enable the OpenVPN protocol in the VPN server.
9. Enable the OpenVPN protocol.
10. Set the ports for OpenVPN. The ports must match the ports that were opened in the DSL router.
11. Select "WAN" as the interface. The OpenVPN connection to the OpenVPN clients is established via this interface.
12. Save the settings with "Save".



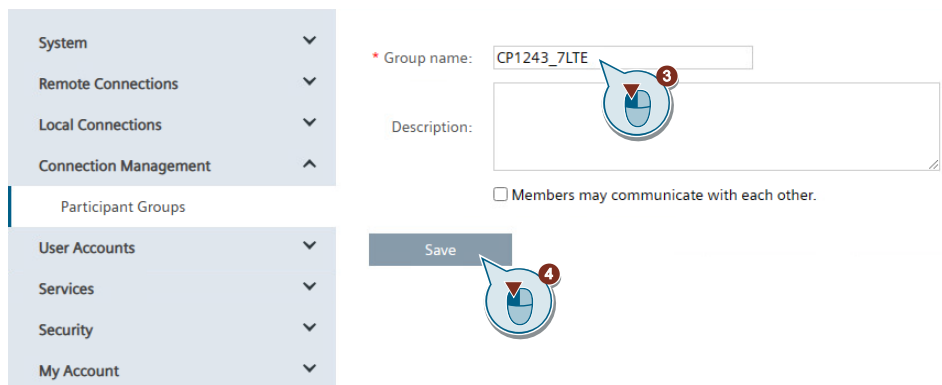
Creating participant groups

To manage users and devices in an orderly manner, you can create participant groups. Participant groups are also needed so that participants can communicate with each other.

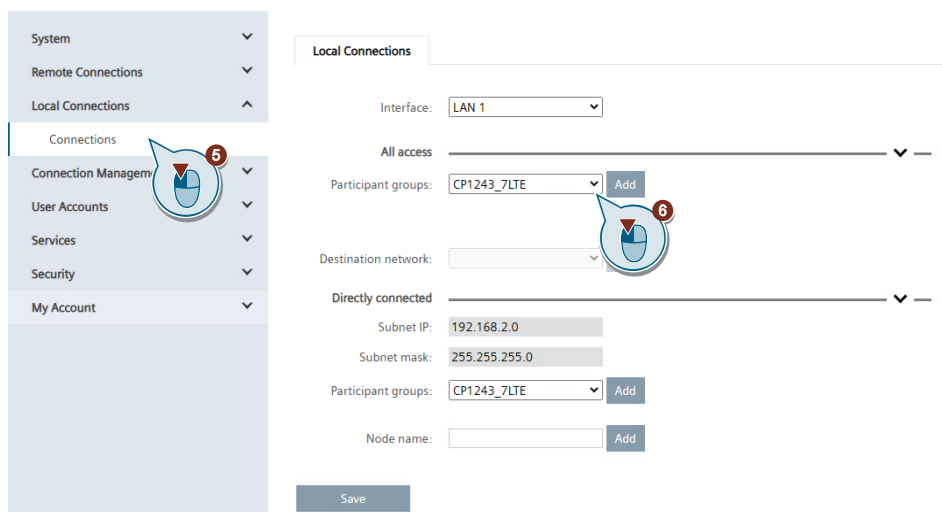
1. Navigate to the "Connection Management > Participant groups" menu.
2. Click "Create".



3. Assign a group name (e.g. "CP1243_7LTE").
4. Save the settings with "Save".



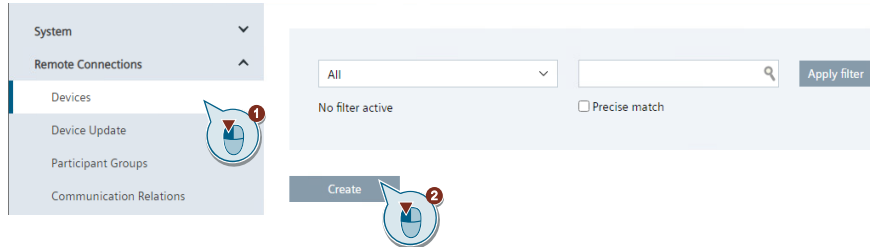
5. Change to the "Local connections > connections" menu.
6. Activate access for the participant group you created above to the LAN of SINEMA Remote Connect.



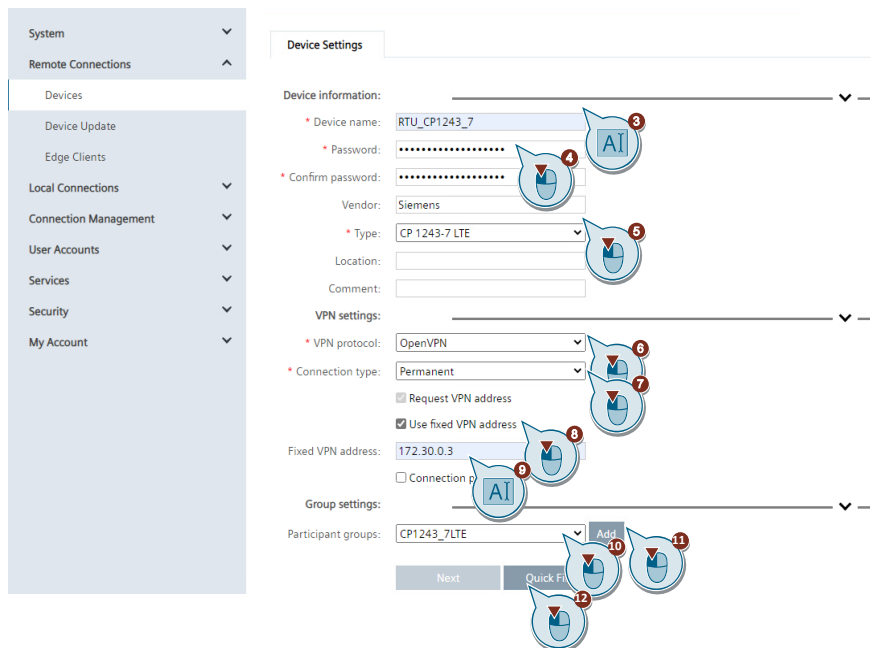
Create devices

The RTU is created as a device in SINEMA Remote Connect Server.

1. Navigate to the menu item "Remote Connections > Devices".
2. Click "Create".



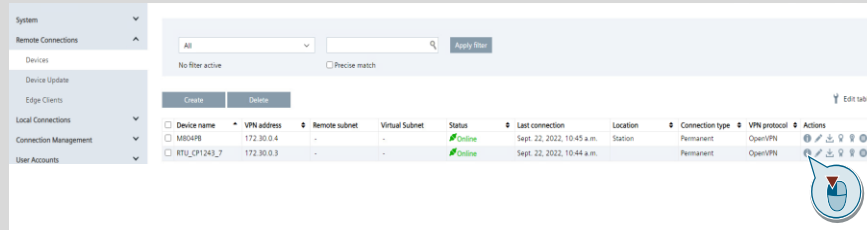
3. Assign a unique device name for the RTU, e.g. "RTU_CP1243_7".
4. Assign a password.
5. Under "Type", select "CP 1243-7 LTE" in the dropdown list.
6. Select "OpenVPN" as the VPN protocol.
7. Select "Permanent" as the connection type.
8. Enable the use of a fixed IP address.
9. Assign an IP address within the previously defined IP address range (e.g. 172.30.0.3).
10. Select the previously created group "CP1243_7LTE".
11. Click "Add".
12. Check the data entered and then click "Quick Finish".



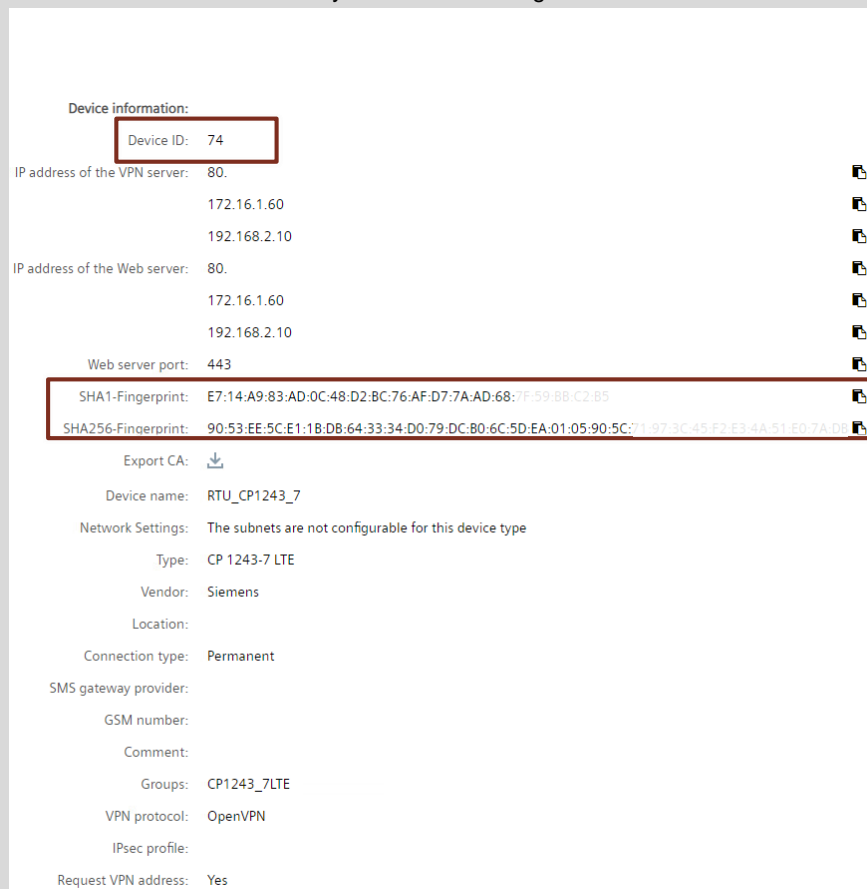
Note

The "Device ID" and the SHAx fingerprint are required during RTU configuration to establish the VPN connection. This information can be found in the Device overview of the created RTU:

1. Open the Device overview of the newly-created RTU via "Remote Connections > Devices > RTU_CP1243_7> i".



2. Take the information necessary for the RTU configuration:



If you want to operate multiple RTUs, you must create another device for each RTU in SINEMA Remote Connect Server.

2.2.2 Configure RTU with SIMATIC S7-1200

This chapter shows you all necessary steps to configure the RTU for the application described here.

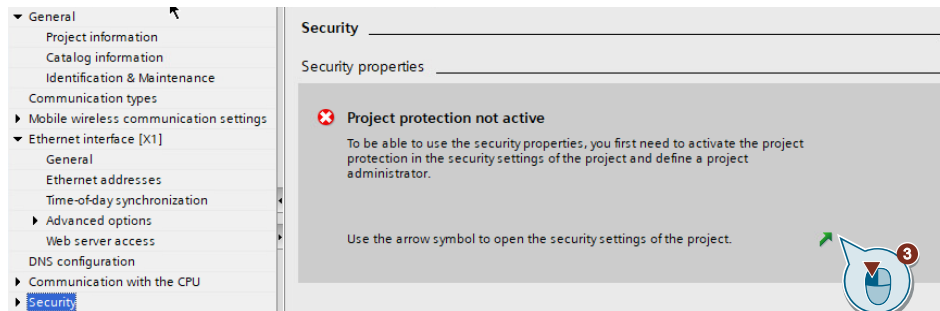
Note

The included project "39863979_TCSB_CP_SRC_PROJ_V10.zip" contains the finished configuration which you can download to your RTU and adapt to suit your application in just a few steps (see chapter [2.2.4](#)).

This chapter is for information only.

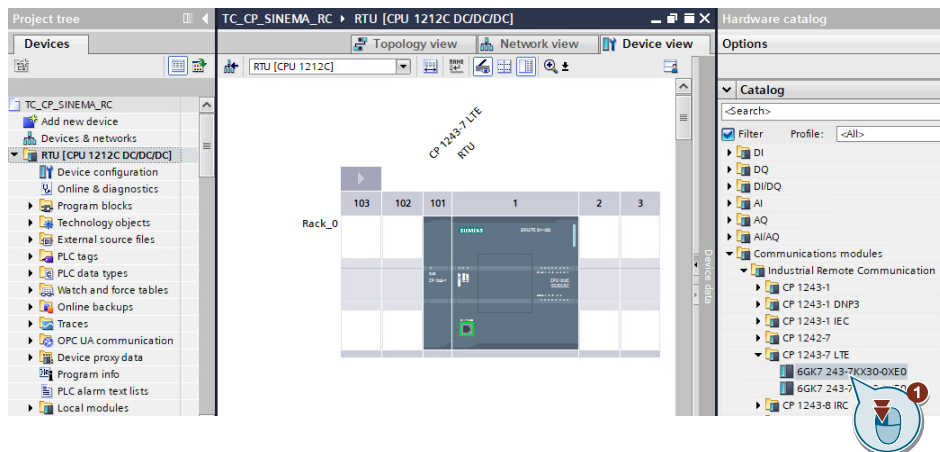
Basic settings

1. Create a TIA project and add a new device of type "S7-1200 CPU".
2. Adjust the IP address of the CPU (per [Table 2-1](#)).
3. Open the "Security Settings" and create a user with administrator rights in order to protect your project.

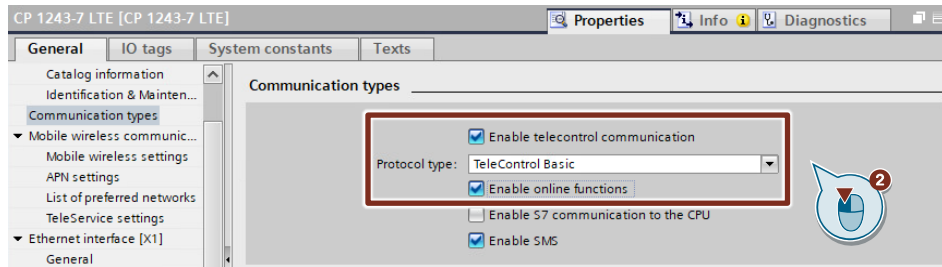


Configure telecontrol connection

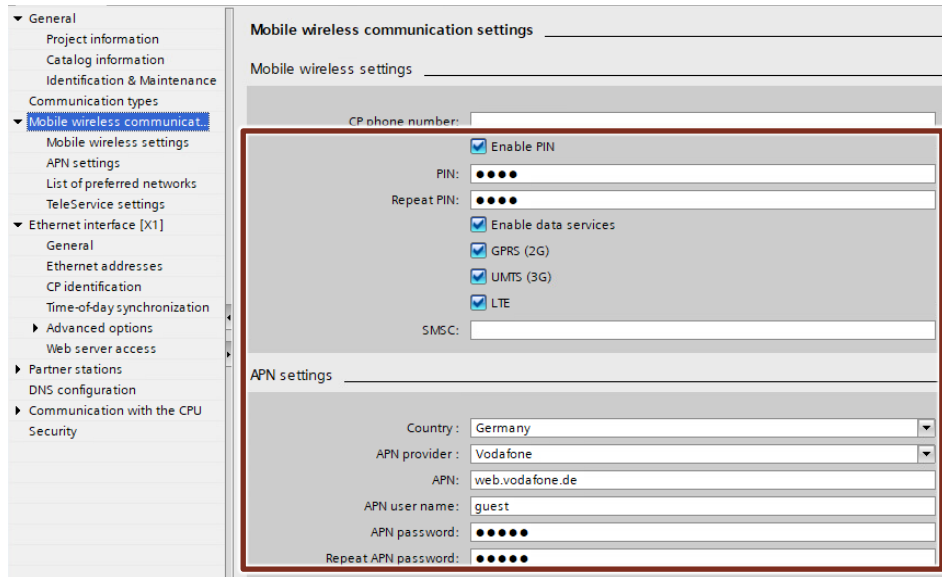
1. Select the CP 1243-7 LTE in the "Device configuration".



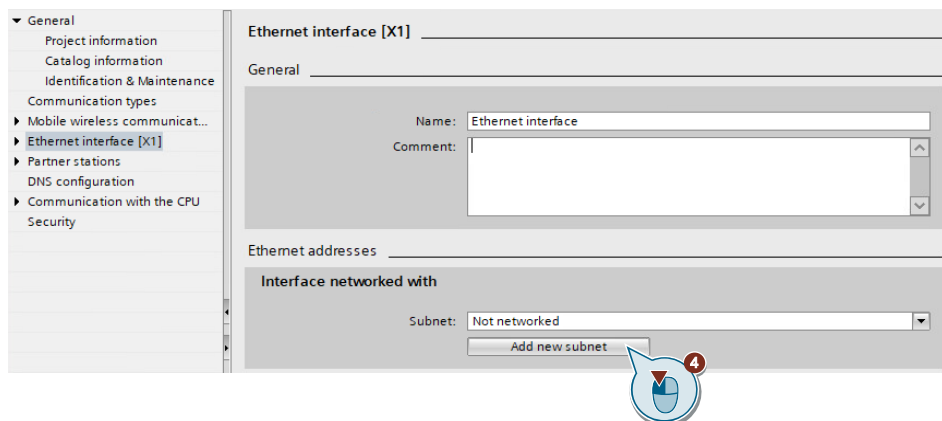
- In the "Properties" of the CP, enable the telecontrol communication via TeleControl Basic and the offline functions.



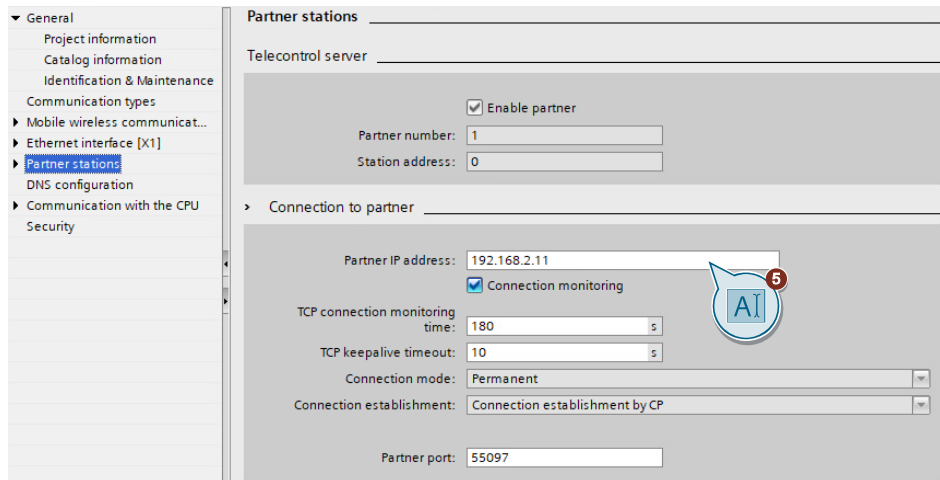
- Enter the PIN of the internal SIM card and the APN of the mobile network operator.



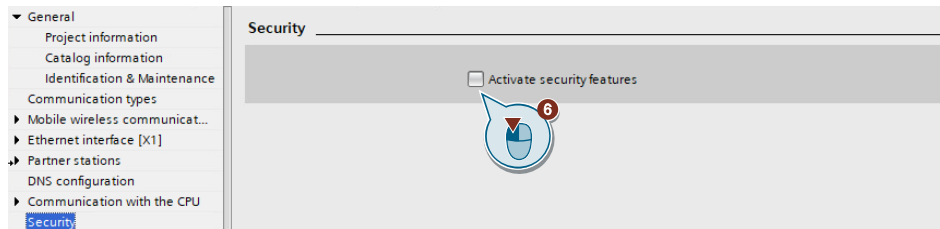
- Add a new subnet for the CP.



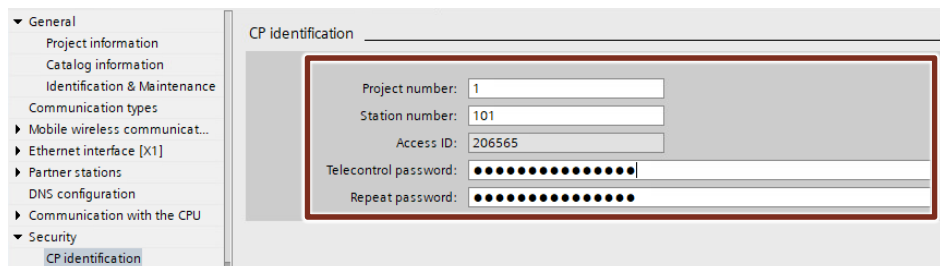
5. Enter the IP address that connects the TeleControl server to the LAN of SINEMA Remote Connect Server (per [Table 2-1](#)).



6. Activate the security functions.



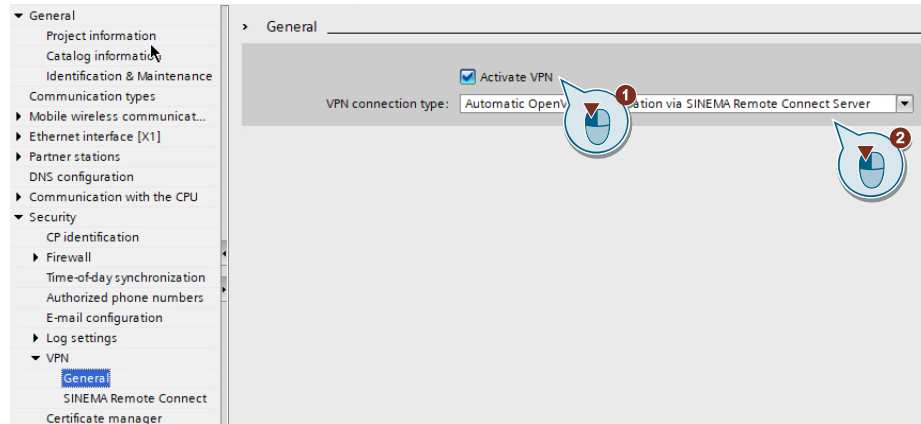
7. Enter
 - a unique project number,
 - a unique station number and
 - a TeleControl password.



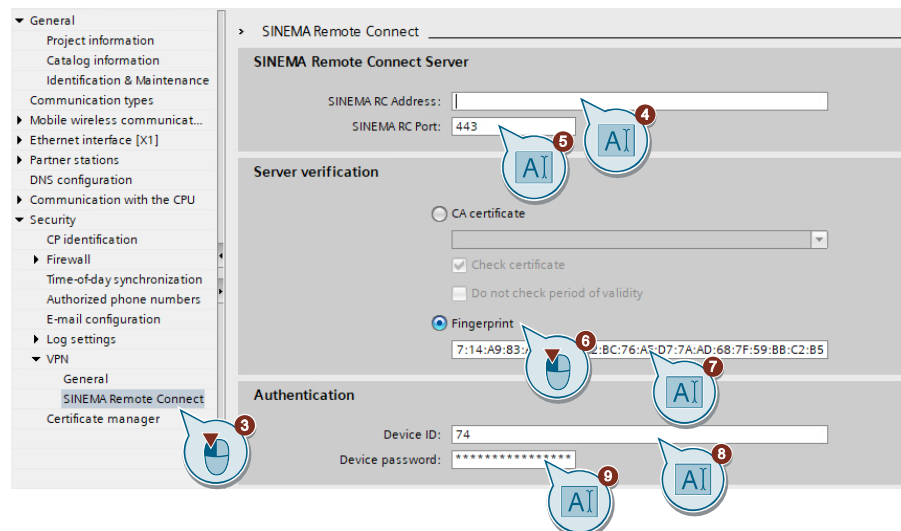
Note The parameters entered here must match the parameters in the "TeleControl Server Basic" software.

Configure VPN Connection

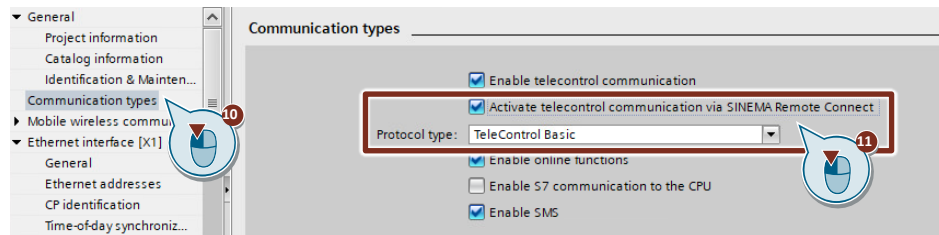
1. Enable VPN to configure the VPN connection parameters.
2. Then, in the "VPN connection type" field, select the option "Automatic OpenVPN configuration via SINEMA Remote Connect Server".



3. Navigate to the "SINEMA Remote Connect" menu.
4. Then enter the static IP address of your DSL router in the "SINEMA RC Address" field.
5. Set the SINEMA RC port. This setting must match the setting in SINEMA RC.
6. Select the "Fingerprint" option for server verification.
7. Enter the SHA 256 fingerprint from SINEMA Remote Connect Server (see note at the end of chapter [2.2.1](#)).
8. Enter the "Device ID" for the RTU, displayed in the device information of SINEMA Remote Connect Server.
9. Enter the password for this device (in this example, device RTU_CP1243_7). The password was configured in SINEMA Remote Connect Server.



10. Switch to the "Communication types" tab.
11. Enable telecontrol communication via SINEMA Remote Connect with the protocol type "TeleControl Basic". This option is visible once VPN is activated.

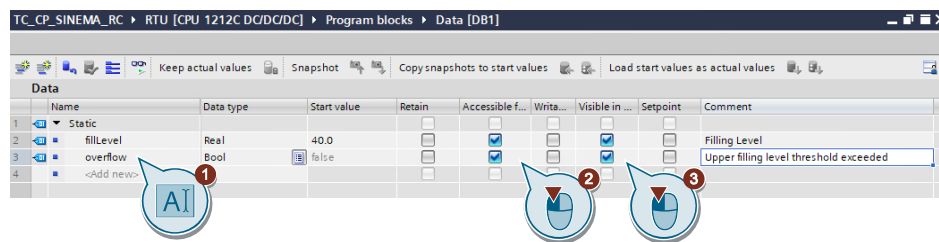


Configure data points

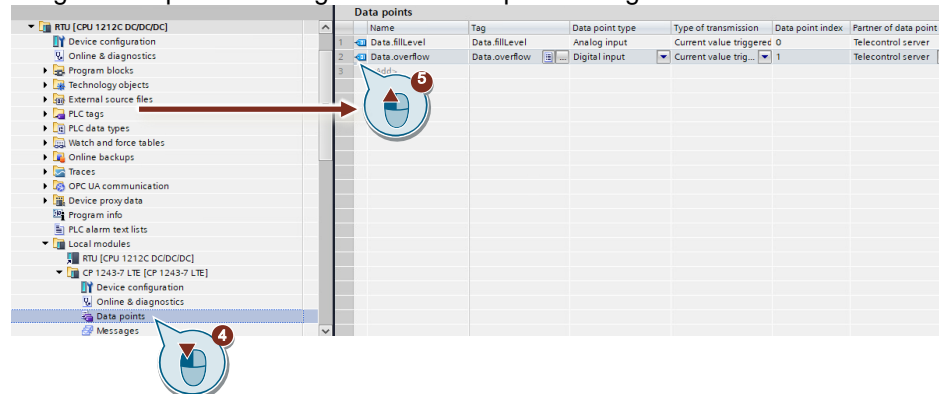
No programming of program blocks is necessary to transmit payload data between the RTU and the control station. The data ranges in the CPU memory provided for communication with the control station are configured by data points in the CP 1243-7 LTE. Here, each data point is linked with a PLC tag in the CPU.

Follow the steps below to configure the data points:

1. In a data block of the CPU, create the tags that you wish to send to the control station.
2. Select the option "Accessible from HMI / OPC UA / Web API".
3. Select the option "Visible in HMI engineering".



4. Open the editor for data point configuration.
5. Drag and drop the PLC tags into the data point configuration editor.



6. Configure the transmission type and trigger for the data points. You can find more information on this in chapter [3.2](#).
7. To download the CPU, assign your "PD/PC" an IP address in the address range of the CPU (e.g. 192.168.0.11).
8. Download the RTU configuration to the CPU.
9. Apply the PC time to the CP so that the VPN connection can be established.
10. Modify the IP address of your "PD/PC" (per [Table 2-1](#)).

2.2.3 Configure TeleControl Server Basic

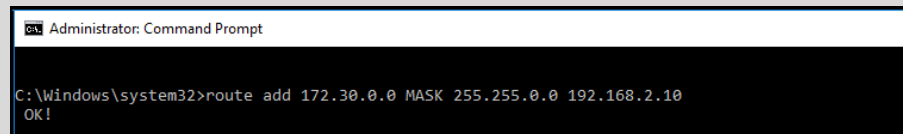
Note

To make TeleControl Server Basic accessible via the LAN interface of SINEMA Remote Connect Server, store the local IP address of SINEMA Remote Connect Server in your PD/PC "TCSB" as the default gateway (192.168.2.10).

If you have configured multiple interface cards on your PC or server (e.g. PD/PC "TCSB"), and you cannot configure a default gateway for the TCSB, add a static route to the Windows routing table.

3. Start Command Prompt (Desktop app) as an administrator.
4. Enter the following command:
`route add 172.30.0.0 MASK 255.255.0.0 192.168.2.10`
5. Press the Enter key.

Result:



```
Administrator: Command Prompt

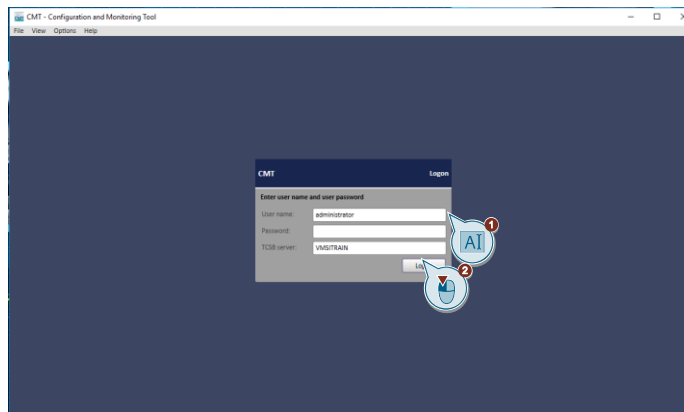
C:\Windows\system32>route add 172.30.0.0 MASK 255.255.0.0 192.168.2.10
OK!
```

172.30.0.0: Target subnet (VPNs defined IP range)
192.168.2.10: SINEMA RC Server (LAN)

Create project

To configure TeleControl Server Basic, proceed as follows:

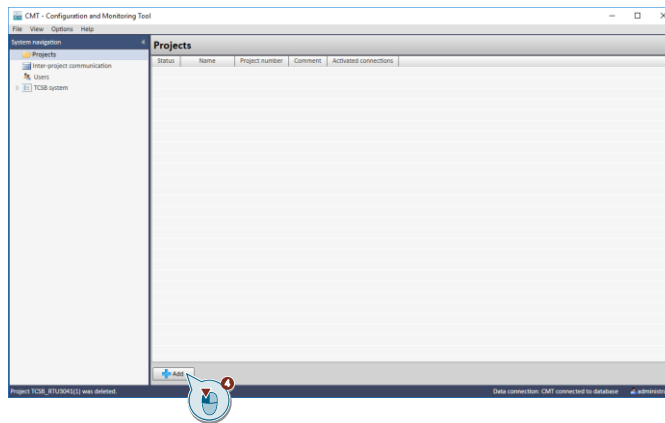
1. Open the program "CMT – Configuration and Monitoring Tool" on your PD/PC "TCSB". TeleControl Server Basic must be installed on the PD/PC.
2. Log in with your user data.



The following user data is preset at the factory:

- User: administrator
 - Password: 0000
3. When you log in for the first time, assign your own password.

- 4. Create a new project by clicking "Add".



- 5. Assign a project name and a project number.

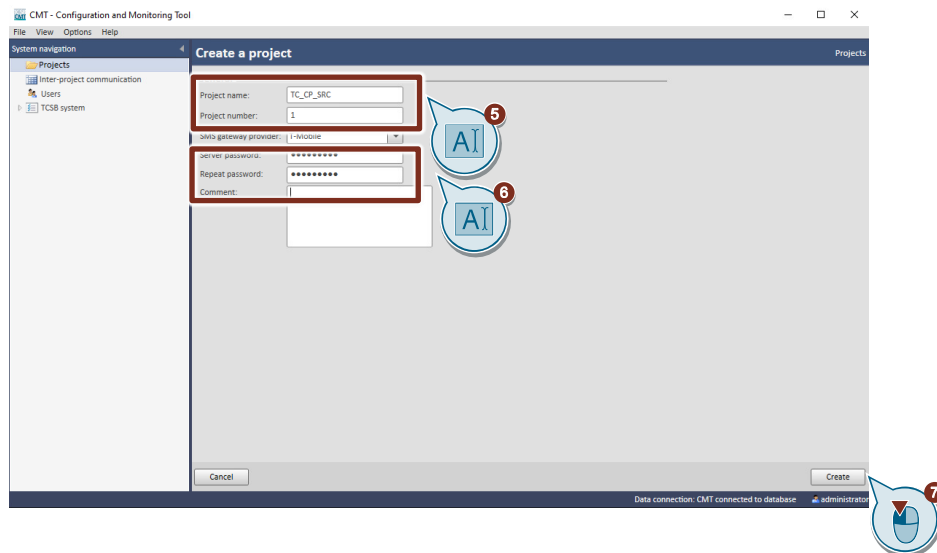
Note The parameter "Project number" must match the parameter in chapter [2.2.2](#) in the configuration of the connection to the TeleControl server ([7](#)).

- 6. Assign a server password.

Note The "Server password" parameter is needed for Teleservice. It is not relevant for this application example, but it must be assigned.

The SMS gateway operator is not relevant for this application example.

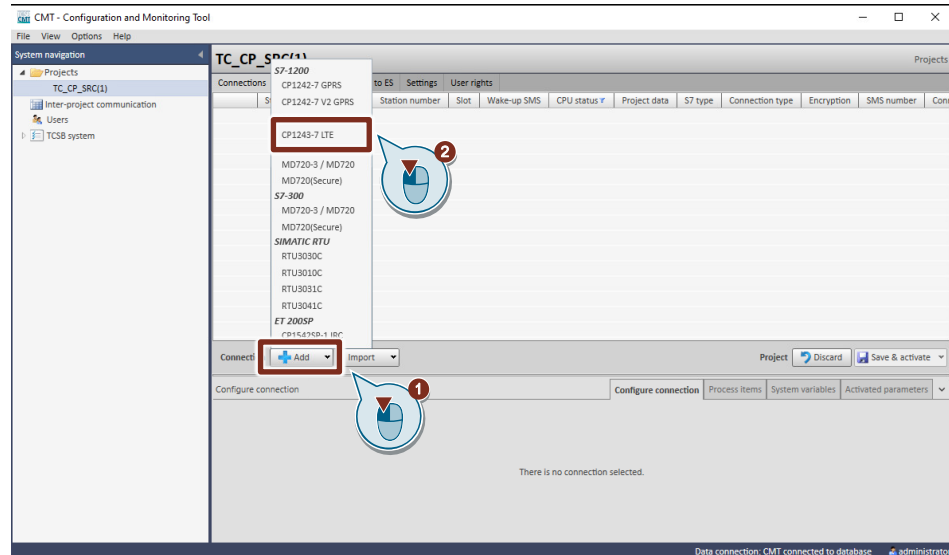
- 7. Then click "Create".



Configure the station

1. Click "Add".
2. Select "CP 1243-7 LTE".

Figure 2-2

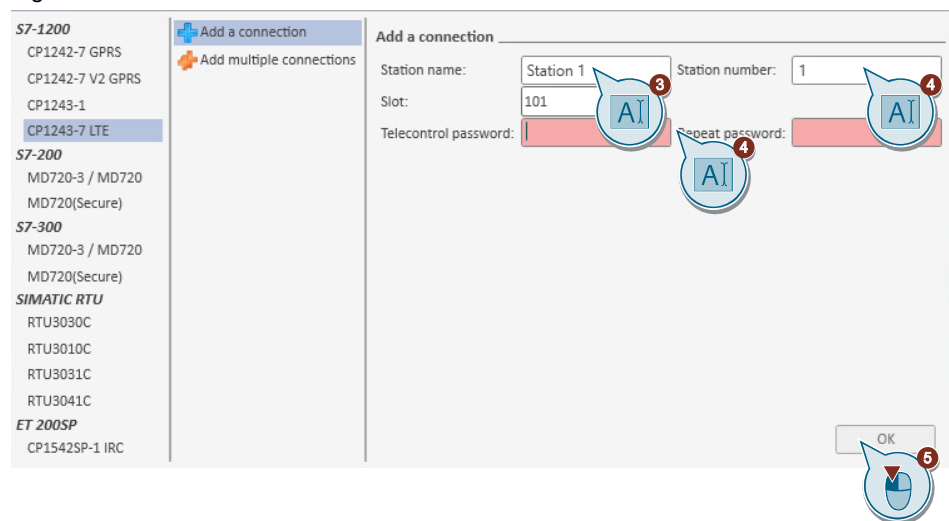


3. Assign a station name for the RTU.
4. Assign values for the parameters "Station number" and "Telecontrol password".

Note The parameters "Station number" and "Telecontrol password" must match the parameters in chapter 2.2.2 in the configuration of the connection to the TeleControl server (7).

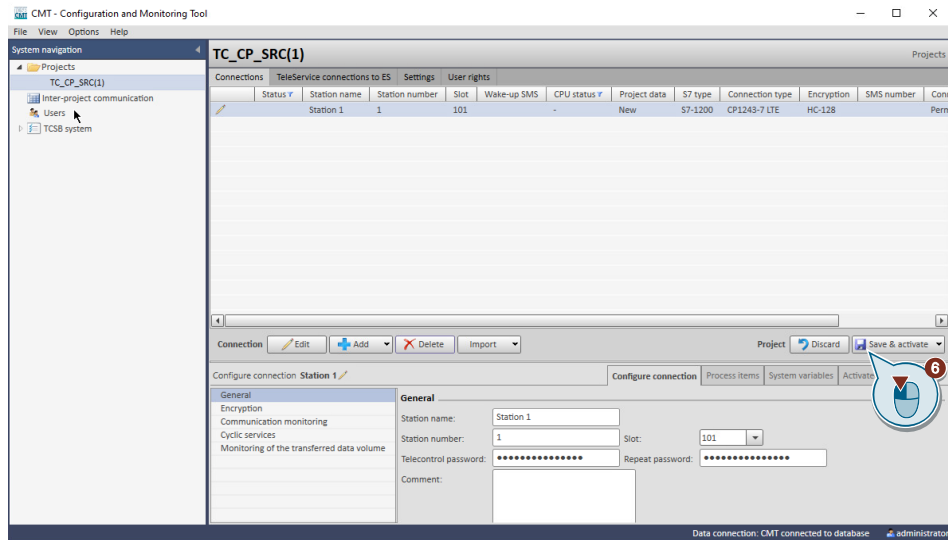
5. Click "OK".

Figure 2-3

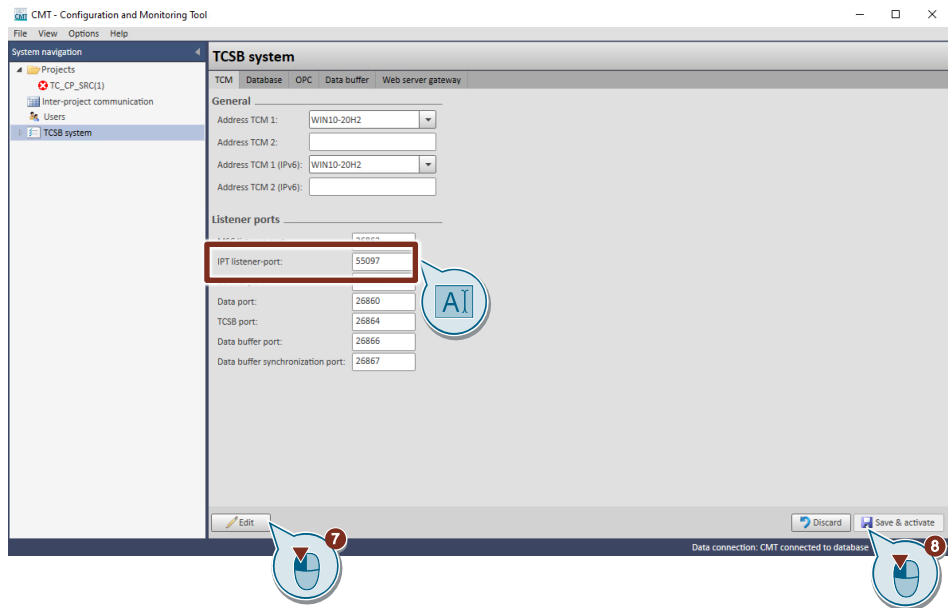


Note If you use more than one RTU, you can configure all RTUs in this step. To do this, select "Add multiple connections" and assign the station data. Click "OK".

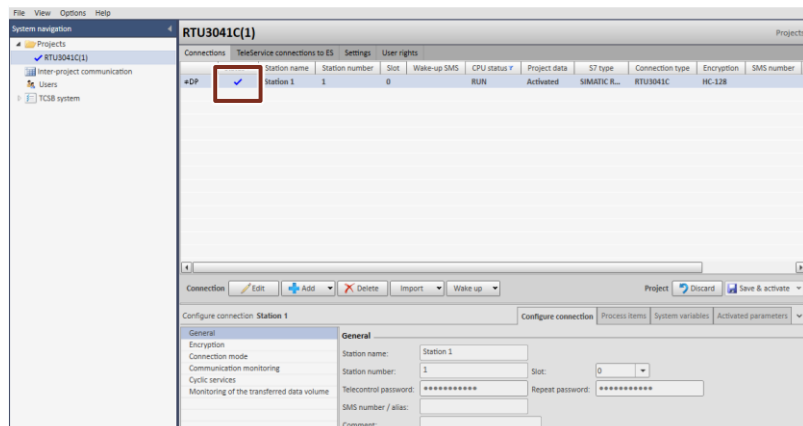
- Click "Save & activate" and confirm the action in the drop-down list.



- Configure the IPT listener port (55097) of the TeleControl server: "TCSB system > TCM > Listener ports > IPT listener port".
- Click on "Save & activate".



The configuration of the TeleControl server is now completed.



Note

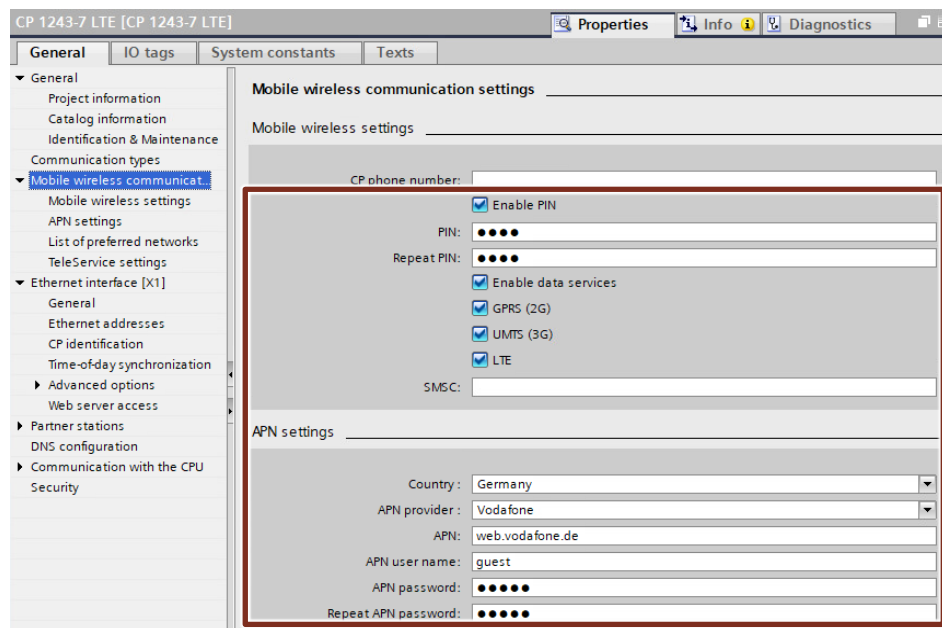
The "Connected" status only appears if the TeleControl server has established a connection to the RTU, the same RTU whose configuration data were sent to the runtime system (in chapter [2.2.2](#) or chapter [2.2.4](#)).

2.2.4 Download TIA project to the RTU with SIMATIC S7-1200

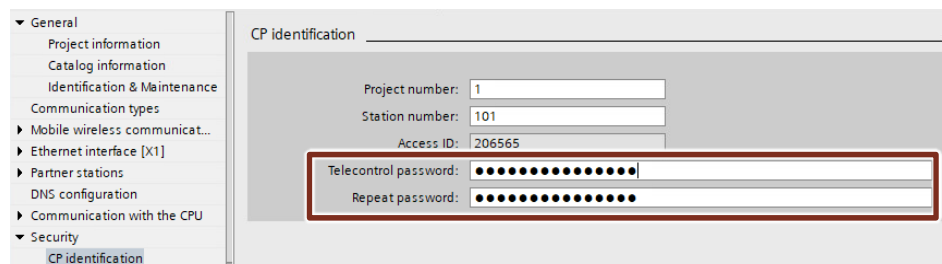
The included archive "39863979_TCSB_CP_SRC_PROJ_V10.zip" contains the ready-to-use configuration file that you can download to your RTU and adapt to your application in just a few steps.

To load the supplied configuration to your RTU, proceed as follows:

1. To download the CPU, assign your "PD/PC" an IP address in the address range of the CPU (e.g. 192.168.0.11).
2. Unzip the project and open it with TIA Portal V17 or later (Username: "admin", password:"Telecontrol_SRC123!").
3. In the "Device configuration", open the "Properties" of the CP 1243-7 LTE.
4. Enter the PIN of the internal SIM card and the APN of the mobile network operator.



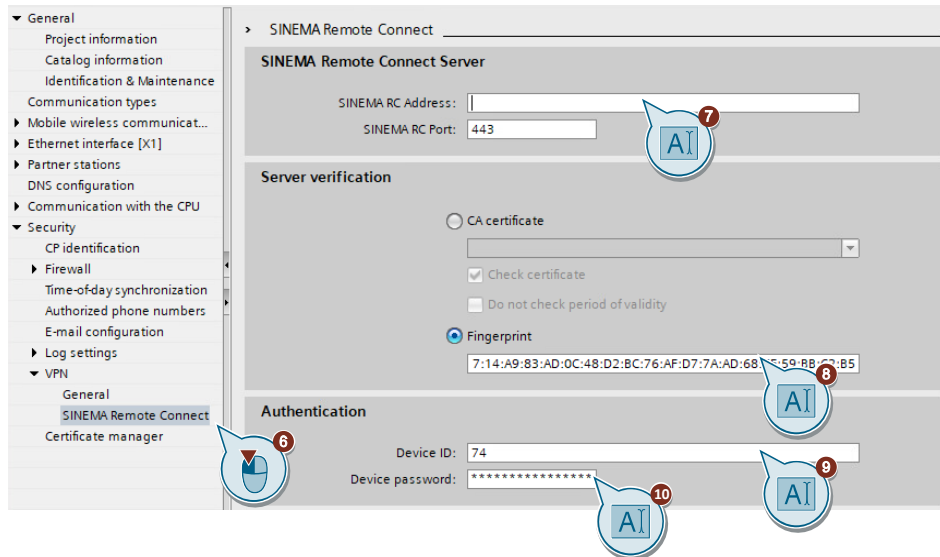
5. Navigate to the "CP identification" menu and set a TeleControl password.



Note

The parameters entered here must match the parameters in the "TeleControl Server Basic" software.

6. Navigate to the "SINEMA Remote Connect" menu.
7. Then enter the static IP address of your DSL router in the "SINEMA RC Address" field.
8. Enter the SHA 256 fingerprint from SINEMA Remote Connect Server (see note at the end of chapter [2.2.1](#)).
9. Enter the "Device ID" for the RTU, displayed in the device information of SINEMA Remote Connect Server.
10. Enter the password for this device (in this example, device RTU_CP1243_7). The password was configured in SINEMA Remote Connect Server.



11. Download the RTU configuration to the CPU.
12. Adjust the IP address of your "PD/PC" (in accordance with [Table 2-1](#)) again.

3 Useful information

3.1 SINEMA Remote Connect

Industrial facilities are often spread over a large area. SINEMA Remote Connect (SINEMA RC) is a management platform for remote networks that centrally manage secure tunnel connections. In this way, widely distributed systems or machines can be conveniently and securely maintained, controlled, and diagnosed via remote access. Even if the machines are integrated within foreign networks. For example, in the facilities of machine manufacturers' end customers.

The core of SINEMA RC is a scalable server application that provides end-to-end connection management of distributed networks via the internet. It coordinates the secure connection setup between the individual participants:

- control center
- service technicians/mechanical engineers
- machines or their VPN tunnel endpoints (e.g. SCALANCE S615, SCALANCE SC-600 or SCALANCE M).

Communication between SINEMA RC Server and the remote participants takes place via Layer 3 VPN tunnels, observing the stored access permissions.

The VPN tunnel endpoints are used for both network separation via firewall and for secure remote access via VPN.

To enable a secure VPN connection, you must set up port sharing on the VPN client side and port forwarding on the VPN server side for each of the routers. The following FAQ shows which ports are necessary for this:

<https://support.industry.siemens.com/cs/ww/en/view/109745584>

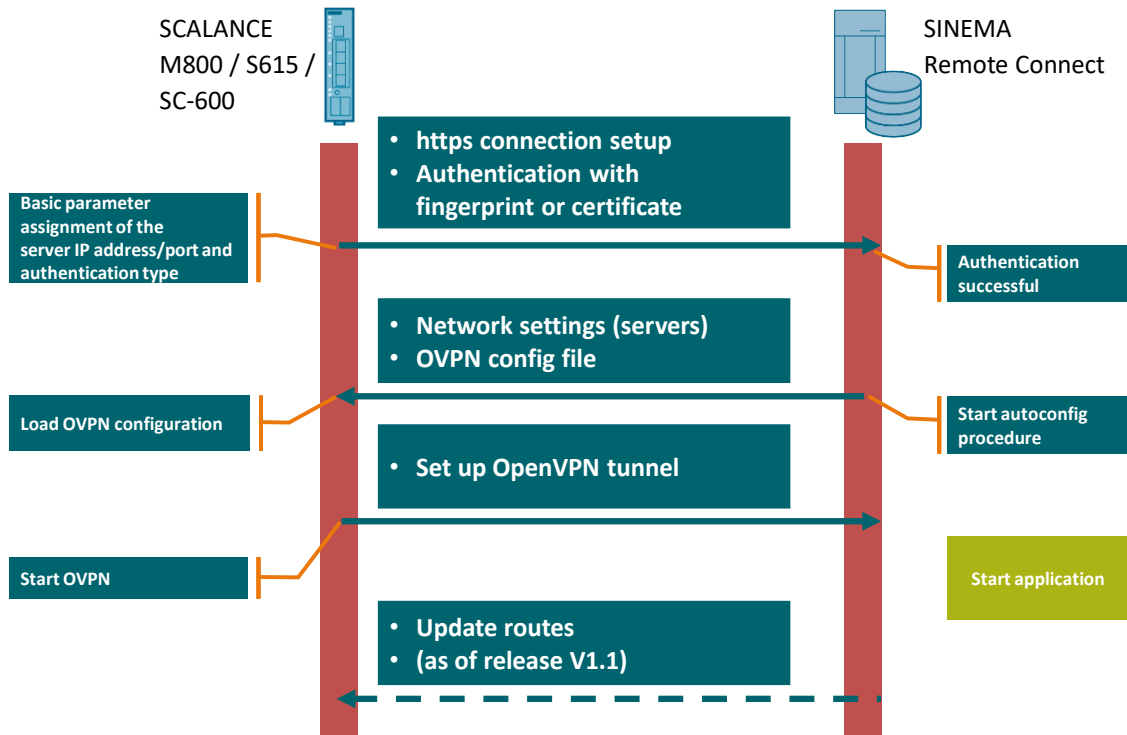
Sequence of connection establishment

The connection setup for secure remote access is very easy. The service technician and the machine to be serviced each establish a connection to a SINEMA RC server separately.

There, the identity of the participants is determined by certificate exchange. Only then is the remote access to the machine available.

The administration of all licenses and the software for the connected clients is done centrally. Recurring tasks can be automated thanks to a REST API, making it easy to manage even very large installations.

Figure 3-1



3.2 TeleControl Basic

3.2.1 Transmission types of data points

The RTU has different transmission modes to transfer data points. You can parameterize the transmission type for each data point individually.

The following transmission types are defined in the TIA Portal data configuration.

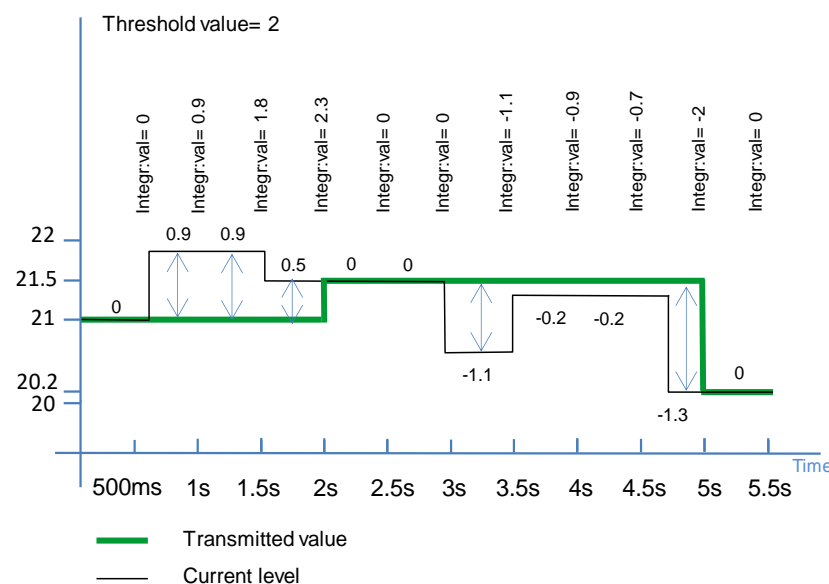
Threshold-triggered

The current value is transmitted to the control center when it has risen by a given threshold value compared to the last transmitted value.

The threshold value calculation does not analyze the absolute value of the deviation in the current value, but rather the absolute value of the integrated deviation.

The deviations in the current value are added up in each calculation cycle (500 ms). Only when the sum reaches the configured value for the threshold trigger (here: 2) is the trigger activated and the current outflow rate is sent.

Figure 3-2



Time-triggered

The current value is transmitted cyclically to the control center.

Event-triggered

The value is transmitted to the control center when the trigger signal is activated. The trigger signal is set by the user program if the current inflow is greater than the limit value. Transmission of the alarm bit resets the trigger signal.

Transmit after call

The current value of the data point is stored in the RTU. New values of a data point overwrite the last stored value.

Event (current value)

If the transmission type "Event" is selected, a threshold (absolute or percentage) can be specified for each data point. Only if the value of the data point has changed beyond this threshold is this is evaluated as an event and the new value stored. New values of a data point overwrite the last stored value.

In communication mode, the last stored value is transmitted.

Event (any value)

All values that differ from the last stored value are stored in chronological order and transmitted to the communication partner during the communication mode.

3.2.2 Transmission mode of the data points

If you parameterize "Event (current value)" or "Event (any value)" as the transmission type, you can additionally select a transmission mode for each data point.

Buffered transmission

The stored value of the data point is transmitted in the next communication mode.

Unsolicited transmission

A value change of the datapoint (event) starts an additional communication mode. The data point is transmitted immediately.

4 Appendix

4.1 Service and Support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Industry Mall



The Siemens Industry Mall is the platform on which the entire Siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:

mall.industry.siemens.com

4.3 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/39863979
\3\	SIMATIC NET: TeleControl Configuration - TeleControl Basic https://support.industry.siemens.com/cs/ww/en/view/109777045
\4\	SIMATIC NET: S7-1200 - TeleControl CP 1243-7 LTE https://support.industry.siemens.com/cs/ww/en/view/109476704
\5\	SIMATIC NET: Industrial Remote Communication - Remote Networks SINEMA Remote Connect V3.1- Server https://support.industry.siemens.com/cs/ww/en/view/109482121

4.4 Change documentation

Table 4-2

Version	Date	Change
V1.0	05/2023	First edition