




**SIEMENS**



**Setting up  
a VPN connection  
between a mobile end  
device (iOS),  
SCALANCE SC  
and SINEMA  
Remote Connect  
Server**

SINEMA Remote Connect

<https://support.industry.siemens.com/cs/ww/en/view/109479578>

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/industrialsecurity>.

# Table of contents

<b>Legal information</b> .....	<b>2</b>
<b>1 Introduction</b> .....	<b>4</b>
1.1 Overview .....	4
1.2 Principle of operation .....	5
1.3 Components used.....	8
<b>2 Engineering</b> .....	<b>9</b>
2.1 Setting up the environment.....	9
2.1.1 IP address overview .....	9
2.1.2 Composition of the infrastructure.....	10
2.2 Preparing the devices .....	10
2.2.1 Router .....	10
2.2.2 SINEMA Remote Connect server.....	12
2.2.3 SCALANCE SC-600 security appliance .....	19
2.2.4 Tablet.....	29
2.3 Setting up remote access on the SINEMA Remote Connect server .....	30
2.3.1 Configure new group membership .....	31
2.3.2 Create a remote connection for the SCALANCE SC-600 security appliance .....	33
2.3.3 Create user account for the tablet .....	40
2.4 Setting up remote access on the SCALANCE device .....	46
2.4.1 Load CA certificate .....	47
2.4.2 Configure VPN connection .....	49
2.5 Setting up remote access on the tablet .....	54
<b>3 Operation</b> .....	<b>59</b>
3.1 Check VPN connection.....	59
3.2 Test VPN connection .....	60
<b>4 Appendix</b> .....	<b>61</b>
4.1 Service and support.....	61
4.2 Industry Mall .....	62
4.3 Links and literature .....	62
4.4 Change documentation .....	62

# 1 Introduction

## 1.1 Overview

### Industry 4.0

The Internet serves as an enormous accelerator of business processes and has revolutionized business operations around the world. The resulting change in the manufacturing industry is also referred to as Industry 4.0.

Industry 4.0 affects all aspects of the industrial value chain, with industrial communication and security being the important aspects we will consider here.

### Industrial security

In the face of digitization and the increasing networking of machinery and equipment, data security must always be taken into account. The use of industrial security solutions precisely tailored to the needs of industry is therefore of fundamental importance – and should be inseparably linked with industrial communication.

This includes the following points:

- Use of robust products with security features and security services
- Use of concepts such as "Defense in Depth" and a holistic security concept

### Measures

The measures for safe operation in a digital enterprise are:

- Encryption and monitoring of communication
- Access control for industrial components and networks
- Protection of transfer and saving of data
- Authentication of devices and users

### The virtual private network (VPN) as a solution

To ensure secure operation in a digital enterprise, data transmission can be encrypted using a VPN to protect against data espionage and tampering. The communication partners are securely authenticated.

SINEMA Remote Connect – the management platform for remote networks – provides support in this area. SINEMA Remote Connect is a server application that allows for easy management of VPN connections between the control center, service technicians and the installed machines or plants.

### Implementation in practice

This application example will show you how to set up secure remote access to SINEMA Remote Connect Server and underlying devices for a service employee so that he or she can perform maintenance, control and diagnostics tasks.

The service employee in this example will use a mobile end device running iOS.

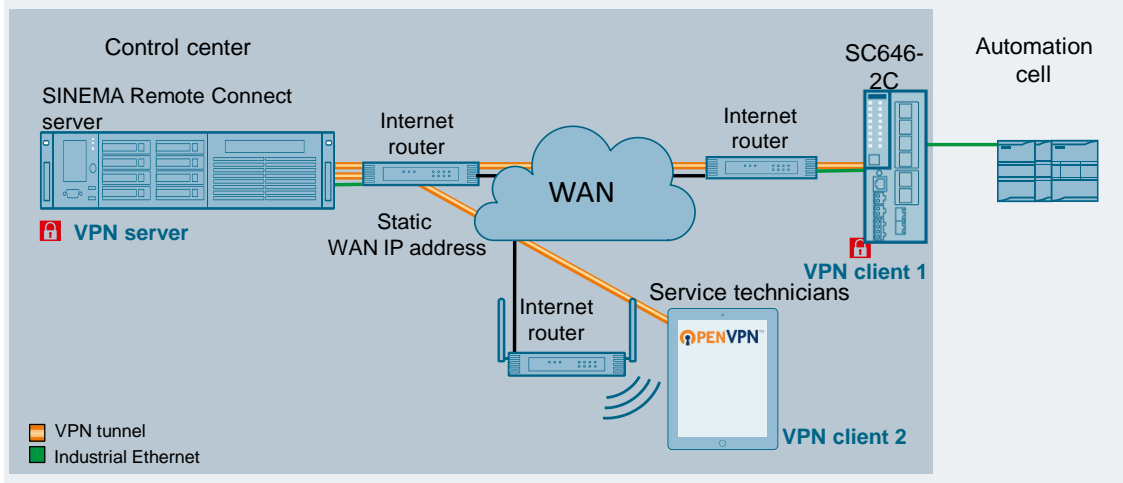
The automation network is protected by a SCALANCE SC-600 security appliance.

SINEMA Remote Connect is used for secure and central management of the tunnel connections.

## 1.2 Principle of operation

### Schematic representation

The Figure below shows a schematic view of the application example.



### Description

The internal network of a SCALANCE SC-600 security appliance is connected with an automation cell consisting of nodes such as SIMATIC Station, a panel, drives and PCs. The service technician uses a mobile end device.

The service technician and the automation cell communicate via the SINEMA Remote Connect server located in the control center. Remote access is secured with two VPN tunnels:

- VPN tunnel 1: Client access from the mobile end device (tablet/smartphone) to the SINEMA Remote Connect server is established via the "OpenVPN Connect" app, a VPN client software application.
- VPN tunnel 2: Automation cell client access runs via the SCALANCE SC-600 security appliance.

Depending on the configured communication relationships and the security settings, the SINEMA Remote Connect server will route between the separate VPN tunnels.

Access to the SINEMA Remote Connect server (VPN server) is defined with a static WAN IP address.

Access paths on the part of the two clients are flexible; the external IP addresses of the routers are not relevant.

The role distribution when establishing the VPN tunnel is defined as follows:

Component	VPN role
Mobile end device	Initiator (VPN client 2); starts the VPN connection
SCALANCE SC	Initiator (VPN client 1); starts the VPN connection
SINEMA Remote Connect server	Responder (VPN server); waits for the VPN connections

#### Note

In place of the SCALANCE SC-600 industrial security appliance, you can also use a SCALANCE S615 or a SCALANCE M industrial router.



### **SINEMA Remote Connect**

SINEMA Remote Connect is a server application and offers integrated connection management of distributed networks via the Internet. This also includes secure remote access to subordinate networks for maintenance, control and diagnostic purposes. SINEMA Remote Connect comprises the following components:

- SINEMA Remote Connect server
- Users (such as service employees) with the "SINEMA RC-client" software or an OpenVPN connection
- Devices that support a connection to the SINEMA Remote Connect server (e.g. SCALANCE SC-600)

The connection setup for secure remote access is very simple.

The service technician and the machine undergoing maintenance separately establish an OpenVPN connection to the SINEMA Remote Connect server. 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.

The connection to SINEMA Remote Connect can be established using cellular phone networks, DSL, or existing private network infrastructure.

The SINEMA Remote Connect server is configured using Web Based Management (WBM).

### **SCALANCE security appliance**

The industrial security appliances and industrial routers support the industrial security concept of "defense in depth". They secure automation networks and seamlessly connect to the security structures of the office and IT world.

The security components protect devices and networks in discrete manufacturing and the process industry and help to set up a flexible security zone concept.

The functions they provide include the following:

- High-quality stateful inspection firewall with filtering of IP-based data traffic
- Global and dynamic firewall rules
- Management of multiple IPsec VPN connections simultaneously
- NAT/NAPT for communication with serial machines with identical IP addresses
- Secure remote access via SINEMA Remote Connect with autoconfiguration interface
- Digital input for local activation of secure remote access
- Redundant power supply
- Simple device replacement with C-PLUG removable storage device for automatic backup of configuration data

### **Advantages of the solution**

This solution has the following advantages:

- User administration and connection management via a central server application
- Secure and easy access to facilities from anywhere in the world
- Simple configuration of the SCALANCE SC-600 security appliance thanks to an autoconfiguration interface
- Controlled and encrypted data exchange between users, far-flung facilities and machinery
- Verification of end devices using a CA certificate or fingerprint
- Low investment and operating costs for operator control and monitoring of remotely connected substations
- High security for machines and systems by implementing the cell security concept
- Easy integration into existing networks and protection of devices without their own security functions

## 1.3 Components used

### Software packages

This solution is based on a SINEMA Remote Connect appliance. It requires SINEMA Remote Connect Server for the software.

Install this software on a PC without an operating system. Note the installation requirements. You must enter the IP address of the server during the installation. Use the IP address from [Table 2-1](#) for this.

The tablet requires the "OpenVPN Connect" app. Download this free app from the Apple store and install it on your tablet.

<b>CAUTION</b>	<b>The SINEMA Remote Connect Server installation contains its own operating system. If you use a PC that already has an operating system installed, the hard disk will be formatted and all stored data will be lost.</b>
----------------	---

### Required devices/components:

Use the following components for the setup:

Table 1-1

Hardware component	Locus of use	Note
PC with the "SINEMA Remote Connect Server" software	VPN server	SINEMA Remote Connect Server <b>firmware &gt; V3.0</b> . In this example: Firmware V3.1
DSL access and a DSL router	VPN server	Static WAN IP address required
SCALANCE SC-600 security appliance with current firmware	VPN client 1	In this example: SCALANCE SC646-2C with firmware V2.3
DSL access and a DSL router	VPN client 1	Dynamic WAN IP address
24 V power supply with cable connector and terminal block plug	VPN client 1	For the SCALANCE SC
Tablet with the "iOS" operating system and the "OpenVPN Connect" app	VPN client 2	In this example: <ul style="list-style-type: none"> <li>• iOS version 15.5</li> <li>• "OpenVPN Connect" app version 3.2.3</li> </ul>
DSL access and a DSL router with WLAN functionality	VPN client 2	Dynamic WAN IP address
A configuration PC with a web browser	All	
Required network cables, TP cables (twisted pair) complying with the IE FC RJ45 standard for Industrial Ethernet	All	

**Note**

You can also use a different internet access method (e.g. UMTS) and, rather than a SCALANCE SC-600, a SCALANCE M-800 or a SCALANCE S615 (each including "SINEMA RC" KEY-Plug) with the latest firmware. The configuration described below refers explicitly to the components mentioned in the section "Required devices/components".



## 2 Engineering

### 2.1 Setting up the environment

#### 2.1.1 IP address overview

The assignment of the IP addresses is defined as follows:

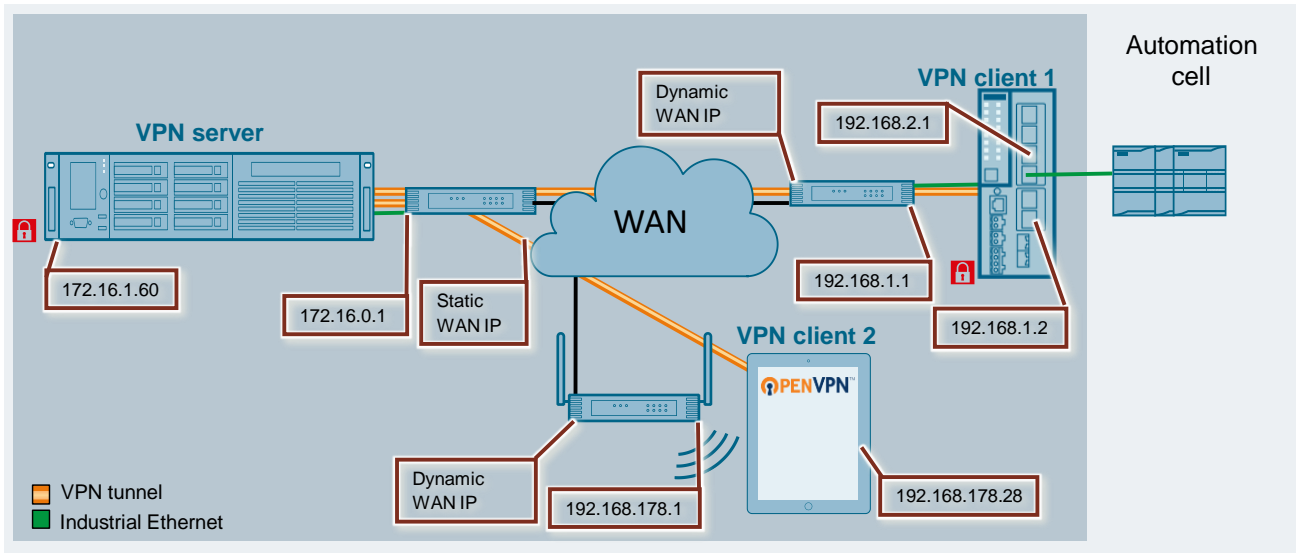


Table 2-1

Component	Port	IP address	Router	Subnet mask
SINEMA Remote Connect server (VPN server)	LAN port	172.16.1.60	172.16.0.1	255.255.0.0
Router on the SINEMA Remote Connect server	LAN port	172.16.0.1	-	255.255.0.0
	WAN port	Static IP address of the provider	-	Assigned by the provider
SCALANCE SC646-2C (VPN client 1)	Zone EXT; vlan2; LAN port: P5 or P6	192.168.1.2	192.168.1.1	255.255.255.0
	Zone INT; vlan1 LAN port: P1 to P4	192.168.2.1	-	255.255.255.0
Router on the SCALANCE SC	WAN port	Dynamic IP address of the provider	-	Assigned by the provider
	LAN port	192.168.1.1	-	255.255.255.0
Tablet (VPN client 2)	WLAN	192.168.178.26	192.168.178.1	255.255.255.0
WLAN router on the tablet	WAN port	Dynamic IP address of the provider	-	Assigned by the provider
	LAN port	192.168.178.1	-	255.255.255.0
Configuration PC (not included in the graphic)	LAN port	172.16.1.100	-	255.255.0.0
		192.168.2.100	-	255.255.255.0

**Note**

In every device that is located in the internal network of the SCALANCE device, you must enter the internal IP address of the SCALANCE device (Zone INT; LAN port: P1 to P4) as the default router.

## 2.1.2 Composition of the infrastructure

Connect all participating components of this solution.

Table 2-2

Component	Local port	Partners	Partner port
SINEMA Remote Connect server	LAN port	Router on the VPN server	LAN port
Tablet	WLAN interface	Router on the tablet	WLAN interface
SCALANCE SC646-2C	Zone EXT; vlan2 LAN port: P5 or P6	Router on the SCALANCE	LAN port
	Zone INT; vlan1 LAN port: P1 to P4	Automation cell	

## 2.2 Preparing the devices

### 2.2.1 Router

#### VPN

If VPN connections have been configured on your router and activated, terminate them.

#### LAN port

On the LAN port, use a static IP address in accordance with [Table 2-1](#).

#### WLAN router on the tablet

Set up the WLAN (Wi-Fi) on the WLAN router.

#### Static IP address on the SINEMA Remote Connect server's router

The SCALANCE device (VPN client 1) and the tablet (VPN client 2) gain WAN access to the SINEMA Remote Connect server (VPN server) via a fixed public IP address. You must apply for it with the provider and then enter it in the DSL router.

**Port forwarding on the SINEMA Remote Connect server's router**

In order for the tunnel packages to pass freely between the tablet, SCALANCE device and the SINEMA Remote Connect server, make sure that port forwarding for "OpenVPN" and "https" is enabled with TCP and UDP, and that the packets can be routed to the SINEMA Remote Connect server. Port forwarding pertains to the following port numbers:

Table 2-3

Protocol	Port number
TCP	443
UDP	1194
TCP	5443
TCP	6220

**Note**

You can modify the port numbers in SINEMA Remote Connect Server. The port numbers above are only correct if you leave the preset values.

OpenVPN uses exclusively either UDP or TCP.

UDP should be preferred (wherever possible ) since it is faster and exhibits better performance.

See also the FAQ "Settings of the ports for secure VPN connections with SINEMA Remote Connect" (see \3\ in [chapter 4.3](#)).

### 2.2.2 SINEMA Remote Connect server

The SINEMA Remote Connect server is configured using Web Based Management (WBM).

#### Preparation

The SINEMA Remote Connect server is set up via WBM on the configuration PC. To access the WBM, the following requirements must be met:

- You will need an Ethernet connection between the configuration PC and the SINEMA Remote Connect server.
- The configuration PC has an IP address in the network of the SINEMA Remote Connect server, for example 172.16.1.100/16.

#### Open the WBM

Proceed as follows to open the WBM:

1. Use the configuration PC to connect to the web interface of the SINEMA Remote Connect server. The IP address was set during installation.
2. Open the WBM, for example with the address "https://172.16.1.60".

#### Note

If you use a different port as the default HTTPS port 443, then enter the port number together with the IP address. You must enter the colon ":" separator between the IP address and the port number, for example: "https://172.16.1.60:6443".

The port for access to the web server can be set in the "System > Network > Web Server Settings" tab.

### Sign in to the WBM (without a prior fresh installation)

**Note**

To sign in to the SINEMA Remote Connect server after a fresh install, see the section "Sign in after a fresh installation".

Proceed as follows to log in to the WBM:

1. Enter your name and password in the corresponding input fields.

The screenshot shows a login interface with two tabs: 'Local' and 'UMC'. The 'UMC' tab is selected. Below the tabs are two input fields: 'User name:' containing the text 'User' and 'Password:' containing a series of dots. A blue callout bubble with a red '1' points to the 'User name' field, and another blue callout bubble with a red '2' points to the 'Password' field. Below the input fields is a dark blue 'Log on' button. At the bottom of the form is a 'PKI Login' button with a smart card icon.

This screenshot shows the same login interface as above, but with a blue callout bubble pointing to the 'Log on' button. The 'User name' field contains 'User' and the 'Password' field contains dots. The 'PKI Login' button is visible at the bottom.

2. Click "Log on".

**Result**

The start page appears.

### Sign in after a fresh installation

Proceed as follows to log in to the WBM after a fresh installation:

1. After the fresh installation, enter "admin" as the username and password, then click "Log on".

Welcome to SINEMA Remote Connect

Local UMC

User name: admin

Password: .....

Log on

PKI Login

The WBM "Change Password" page will open.

2. Set the user name and the password for the administrator. This newly created user will automatically be assigned the role of "Administrator". Click the "Save" button.

User name: User

\* Current password: .....

\* New password: .....

\* Confirm password: .....

Save

### Result

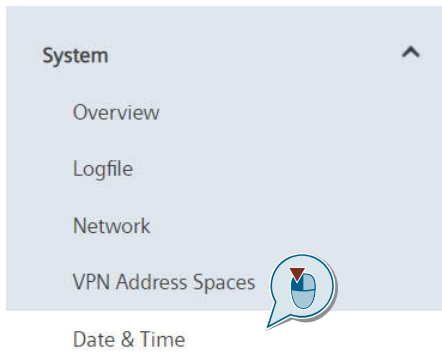
After saving, you will be automatically logged on with the newly created administrator. The "admin" user is no longer available. The start page appears. From now on, log on with the new username and password.

### Set the time

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

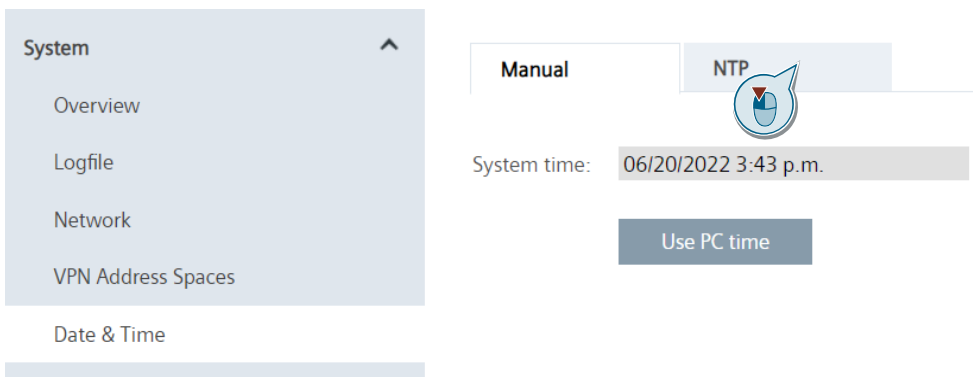
To synchronize the time automatically using the NTP protocol, proceed as follows:

1. In the navigation bar, navigate to "System > Date & Time".

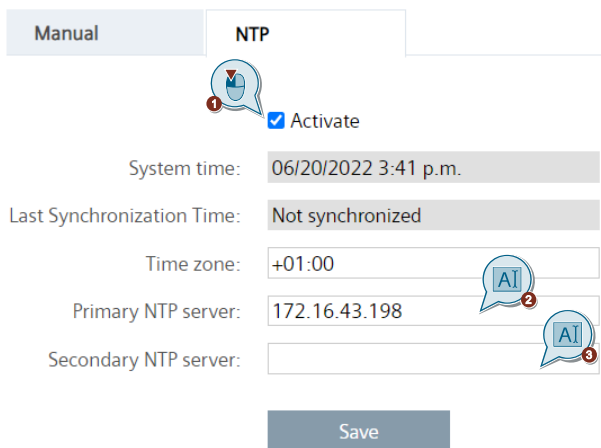


The time setting window will open and you will be in the "Manual" tab.

2. To automatically synchronize the system time with an NTP time server, switch to the "NTP" tab.



3. Tick the "Activate" box.  
Enter the IP address or the hostname of the primary NTP server.  
Optionally enter the IP address or the hostname of the secondary NTP server.





4. Click "Save" to save the settings.

Manual  NTP

Activate

System time: 06/20/2022 3:41 p.m.

Last Synchronization Time: Not synchronized

Time zone: +01:00

Primary NTP server: 172.16.43.198

Secondary NTP server:

**Result**

The time is now set. The date and time appear in the "System time" field.

### Configure the WAN interface

To access the SINEMA Remote Connect server from the internet, you will need a WAN address. This could be the WAN IPv4 address of a DSL router that the SINEMA RC server uses to connect to the internet.

**Note**

If the SINEMA Remote Connect server only needs to be reachable in the local network, then you do not need to configure the WAN interface.

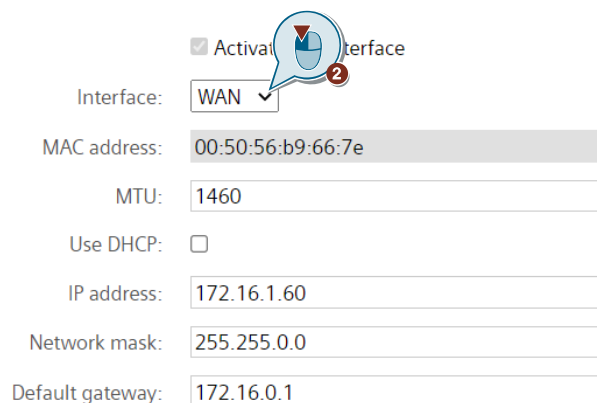
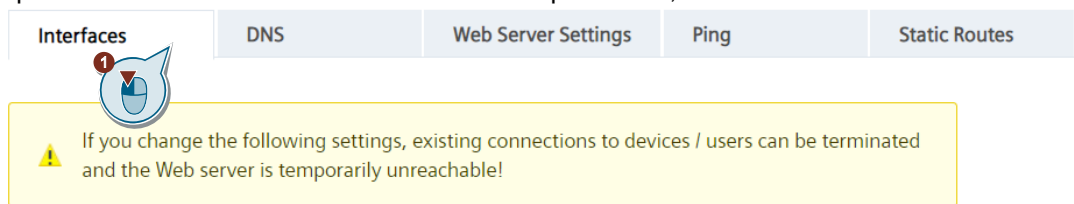
Proceed as follows to modify the WAN IPv4 address:

1. Click on "System > Network" in the navigation area.




A new window opens.

2. Open the "Interfaces" tab. In the "Interface" dropdown list, select "WAN".



- To enter the required external WAN IPv4 address for the router, tick the checkbox for "SINEMA RC is located behind a NAT device with a fixed IP address.". Enter the WAN IPv4 address of the router in the "WAN IP address" field.

Interfaces	DNS	Web Server Settings	Ping	Static Routes
------------	-----	---------------------	------	---------------

 If you change the following settings, existing connections to devices / users can be terminated and the Web server is temporarily unreachable!

Activate the interface

Interface:


MAC address:

MTU:


Use DHCP:

IP address:

Network mask:

Default gate :

SINEMA Remote Connect is located behind a NAT device with a fixed IP address.

WAN IP address:  

- Save the settings with "Save".

SINEMA Remote Connect is located behind a NAT device with a fixed IP address.

WAN IP address:

Activate IPv6:


Use SLAAC for IPv6:

IPv6 Address:

Link-local IPv6 address:

Subnet prefix length:

Default gateway:



**Note**

To access the SINEMA Remote Connect server from the internet, you also have the following options besides a WAN IPv4 address:

- IPv6 address
- Hostname

### 2.2.3 SCALANCE SC-600 security appliance

#### Factory setting

To ensure that there are no old configurations or certificates stored in the SCALANCE device, reset the appliance to its factory settings.

You will find instructions in the module manual (see [chapter 4.3](#)).

#### Preparation

The SCALANCE device is set up using the configuration PC and the WBM. To access the WBM, the following requirements must be met:

- You will need an Ethernet connection between the configuration PC and the SCALANCE device (Zone INT; LAN port: P1 to P4).
- The configuration PC has an IP address in the network of the SCALANCE device, for example 192.168.2.100/24.

#### Assign the IP address

To open the WBM or to download the configuration to the module via TIA Portal, the SCALANCE device needs an IP address. The initial assignment of an IP address for the device cannot be done with the WBM because this configuration tool itself requires an IP address. You have the following options for assigning the associated IP address to the unconfigured device (see [Table 2-1](#)):

- SINEC PNI  
To assign the device an IP address with SINEC PNI, the device must be available over Ethernet. You can download SINEC PNI for free from the Siemens Industry Online Support pages (see [chapter 4.3](#)).
- Command Line Interface (CLI)
- TIA Portal and the "Accessible Devices..." function

Assign the SCALANCE device the associated IP address for the internal network.

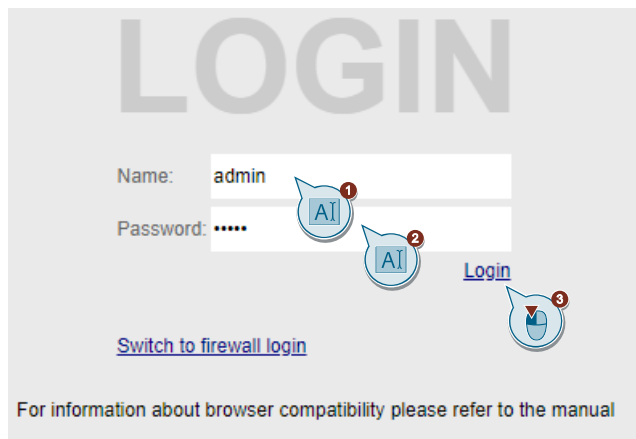
## Open the WBM

Proceed as follows to open the WBM of the SCALANCE device:

1. In the address bar of the internet browser, enter the internal IP address of the SCALANCE device (see [Table 2-1](#)) ("https://192.168.2.1").  
A message about the security certificate will appear.
2. Acknowledge this message and continue loading the page.  
The WBM login page appears.
3. If you are signing in for the first time or after a "Restore Factory Defaults and Restart", the login credentials are set as follows:
  - "Name" field: "admin"
  - "Password" field: "admin"

Enter the name and the password in the corresponding fields.

Click the "Login" button or confirm with the Enter key.



4. If you are signing in for the first time or after a "Restore Factory Defaults and Restart", you will be prompted to change the password.  
Enter the current password in the "Current User Password" field.  
The new password must meet the following password requirements:
  - Password length: a minimum of 8 characters, a maximum of 128 characters
  - At least 1 uppercase letter
  - At least 1 special character (special characters § and ß are not allowed)
  - At least 1 numberSet the new password in the "New Password" field. Repeat your password to confirm. Both passwords must match.  
Click the "Set Values" button to finish the process.

### **Result**

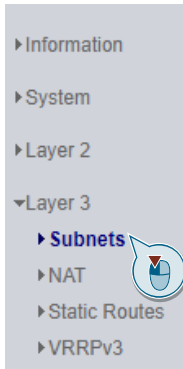
The homepage of the WBM appears.

### Set the IP address

At the start of the chapter, you already assigned the SCALANCE device an internal IP address (Zone: INT; vlan1).

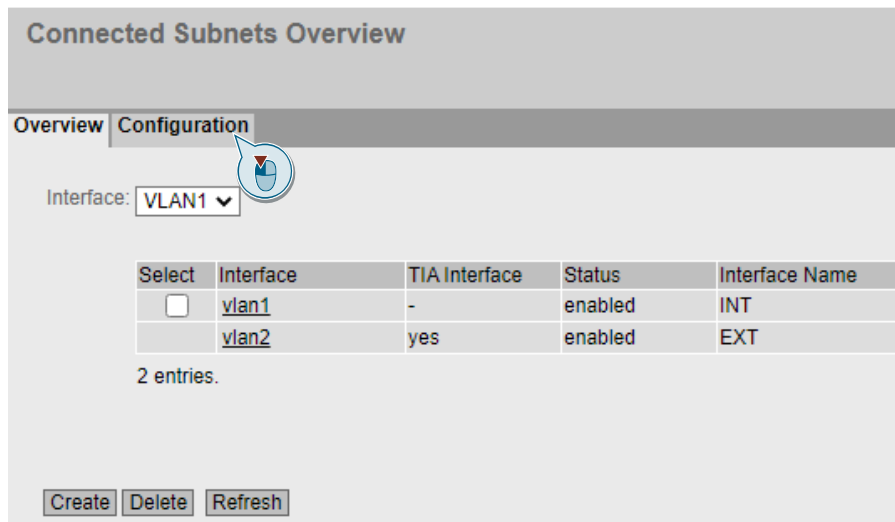
To set up the external IP address (Zone: EXT; vlan2) in the SCALANCE device, proceed as follows:

1. Open the menu "Layer 3 > Subnets".



The "Connected Subnets Overview" window will open and you will be in the "Overview" tab. This page shows you the subnets for the selected interface.

2. Switch to the "Configuration" tab.



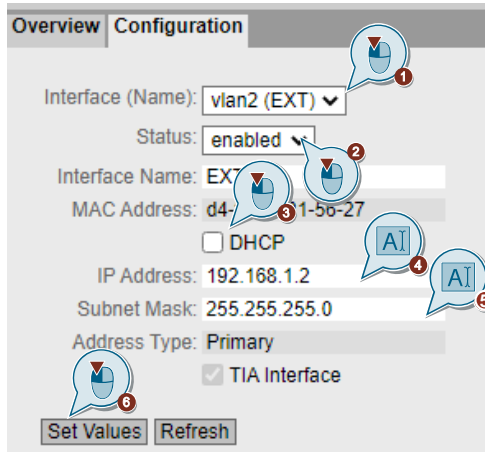
The "Configuration" tab opens. Configure the subnet for the interface on this page.



3. Make the following settings:

- Set the interface to "vlan2 (EXT)".
- Check whether the status is "enabled".
- Disable DHCP.
- For "vlan2 (EXT)", enter the IP address and subnet mask for the external network (Zone: EXT; vlan2; P5 or P6) (see [Table 2-1](#)).

To confirm your changes, click on the "Set Values" button.



**Result**

The SCALANCE device has an IP address for all VLANs.

You will be automatically taken back to the "Overview" tab. Here you will see an overview of the IP addresses.

Overview | Configuration

Interface: VLAN1

Select	Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status
<input type="checkbox"/>	vlan1	-	enabled	INT	d4-15-27-21-56-27	192.168.2.1	255.255.255.0	Primary	Static	Idle
<input type="checkbox"/>	vlan2	yes	enabled	EXT	d4-15-27-21-56-27	192.168.1.2	255.255.0.0	Primary	Static	Active

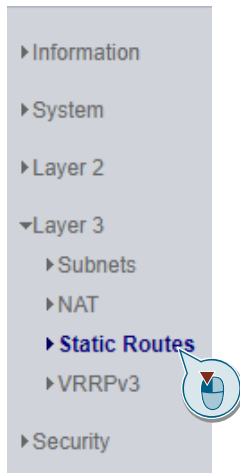
2 entries.

### Define default router

A static route lets you specify the routes through which data can be exchanged between the various subnets.

To store a static route in the SCALANCE device, proceed as follows:

1. Open the menu "Layer 3 > Static Routes".

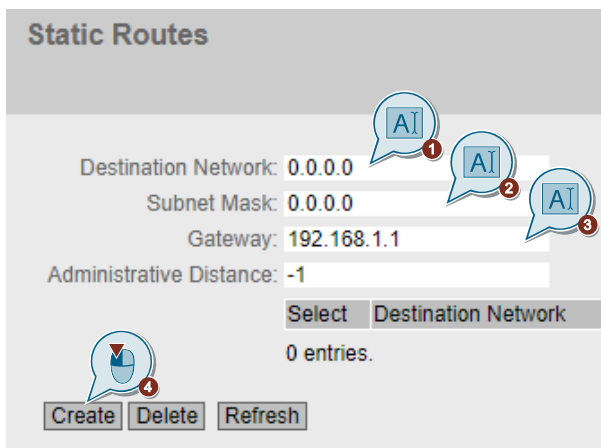


The "Static Routes" page opens.

Here you can specify the routes through which data can be exchanged between the various subnets.

2. To reach all subnets, enter the following values:
  - In the field "Destination network" and in the field "Subnet mask", enter: the network address "0.0.0.0"
  - In the "Gateway" field, enter: the corresponding router (see [Table 2-1](#))

Click the "Create" button.



## Result

The static route for the module has been set up. A new entry is created in the table.

Destination Network:   
 Subnet Mask:   
 Gateway:   
 Administrative Distance: -1

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.1.1	vlan1	not used	active

1 entry.

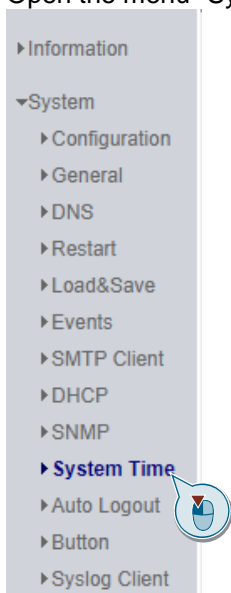
## Define time synchronization

In this application example, the VPN connection is secured by the CA certificate of the SINEMA Remote Connect server. If you work with certificates, it is essential that the correct time be entered in the VPN partners. If the time in the device is incorrect, then the certificates will be considered invalid and discarded.

Use a time synchronization protocol such as NTP to set the system time of the device.

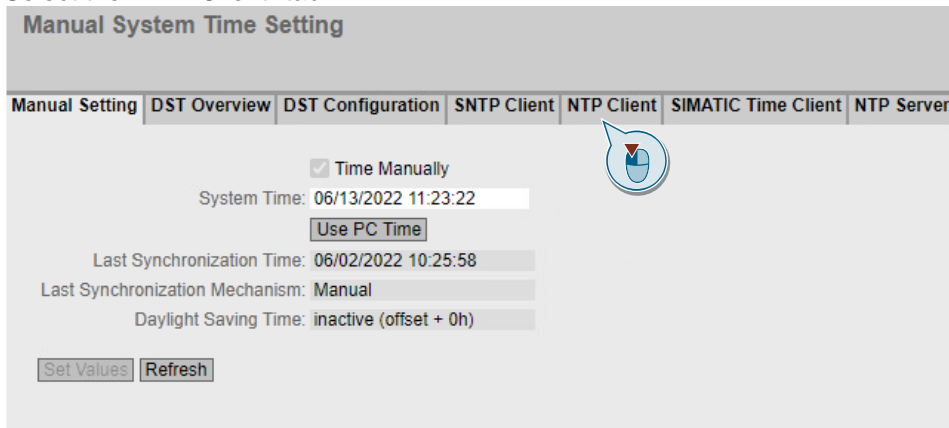
To set up time synchronization with NTP, proceed as follows:

1. Open the menu "System > System time".



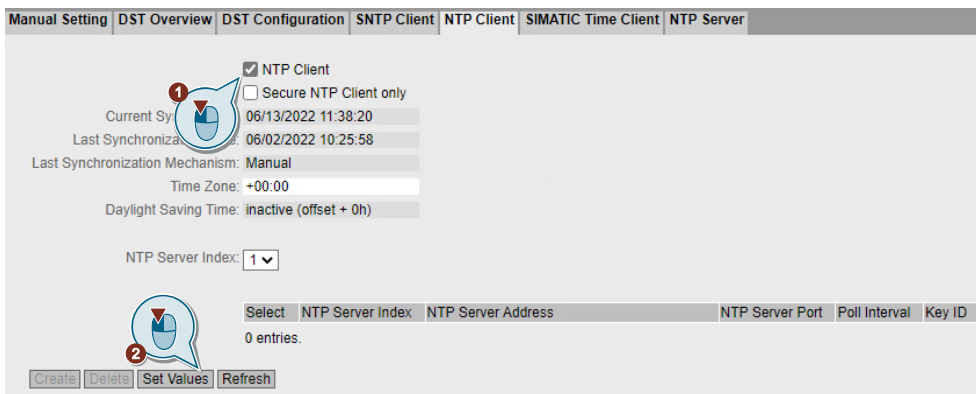
The "Manual System Time Setting" window will open and you will be in the "Manual Setting" tab.

2. Select the "NTP Client" tab.

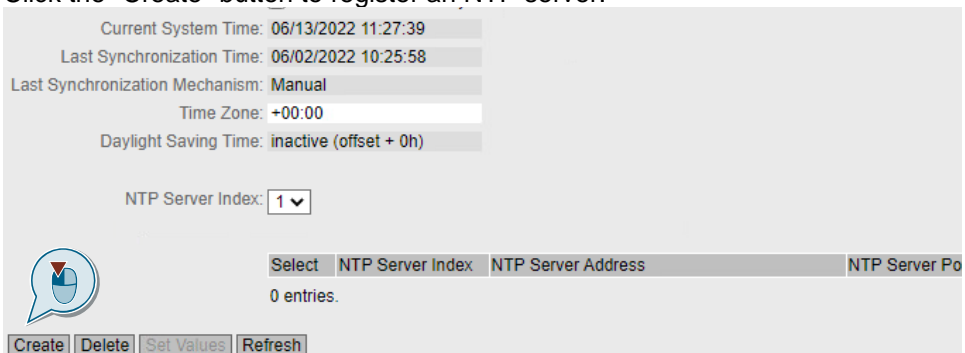


The "NTP Client" tab opens.

3. Tick the "NTP Client" box and click the "Set Values" button.



4. Click the "Create" button to register an NTP server.

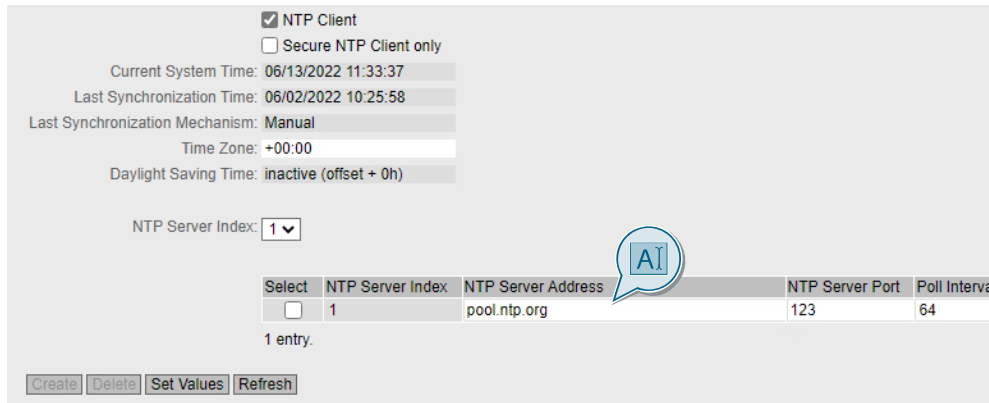


A new table row is added.

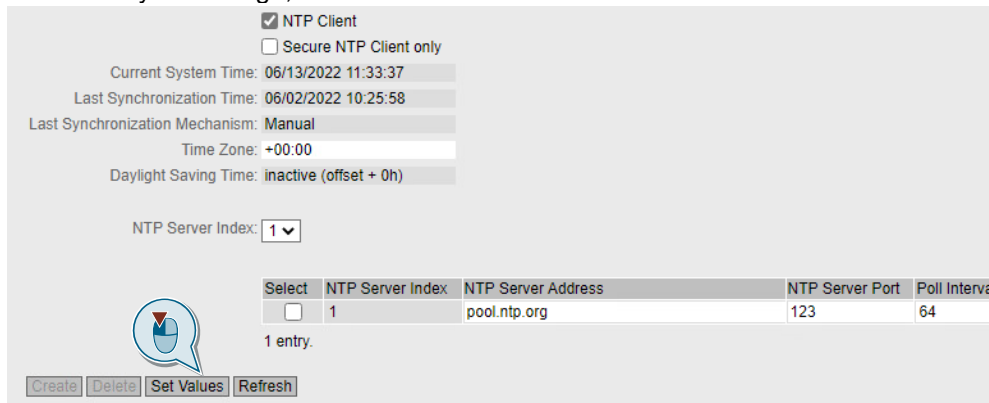
- In the "NTP Server Address" column, enter the address of the NTP server, for example "pool.ntp.org".

**Note**

The "pool.ntp.org" project is a network of time servers that provide simple, reliable time synchronization over NTP.



- To confirm your change, click on the "Set Values" button.



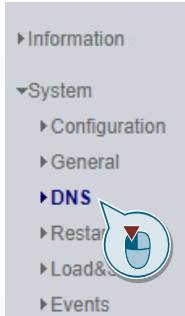
**Result**

The time synchronization protocol has been set up.

### Enter DNS

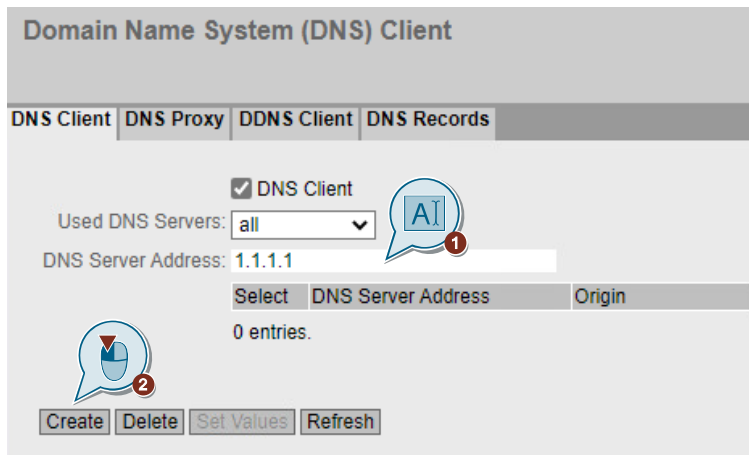
The SCALANCE device requires a DNS server address to resolve the name of the NTP server. Follow these steps:

1. Open the menu "System > DNS".



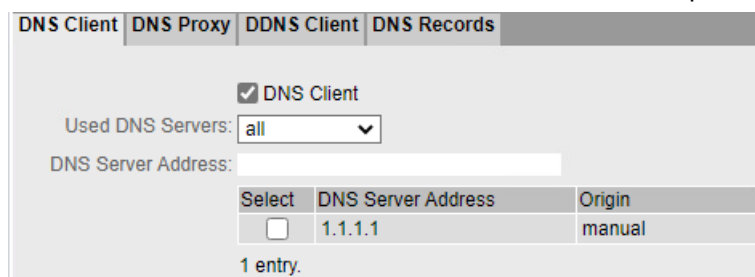
The "Domain Name System (DNS) Client" window opens and you will be in the "DNS Client" tab.

2. Enter the IP address "1.1.1.1" in the "DNS Server Address" column. Click the "Create" button.



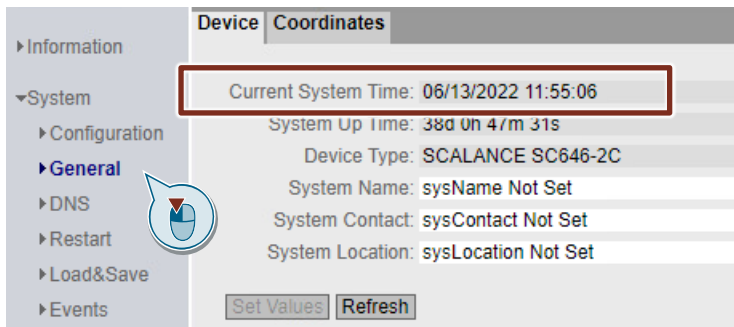
### Result

The DNS server in the SCALANCE device has been set up.



### Check the clock time

You can check the current system time in the SCALANCE device in the menu "System > General" in the "Device" tab.



## 2.2.4 Tablet

### Time

To check the time validity of certificates, it is important that the tablet always has the current date and time.

Check the time on your tablet and adjust it if necessary.

### VPN

If other VPN connections have been configured on your tablet and activated, terminate them.

### WLAN

Set up Wi-Fi on your tablet in accordance with your router configuration. Use a static IP address in accordance with [Table 2-1](#).



## 2.3 Setting up remote access on the SINEMA Remote Connect server

### Overview

In order for the service employee to access the automation cell on his tablet through the SINEMA Remote Connect server, the end devices (the tablet and the SCALANCE device) must sign in to the server. The respective VPN tunnel between the end device and the SINEMA Remote Connect server is only established after successful authentication.

Depending on the configured communication relationships and the security settings, the SINEMA Remote Connect server interconnects the individual VPN tunnels, thus granting access.

The following configuration steps are necessary for this:

- Define participant groups
- Set up remote connection for the SCALANCE device
  - Implement SCALANCE as device
  - Ascertain device ID and export CA certificate
- Set up remote connection for the service employee
  - Create user account
  - Export user configuration

### Preparation

In order to access the WBM, check the following requirements:

- You will need an Ethernet connection between the configuration PC and the SINEMA Remote Connect server.
- The configuration PC has an IP address in the network of the SINEMA Remote Connect server, for example 172.16.1.100/16.

### Open the WBM

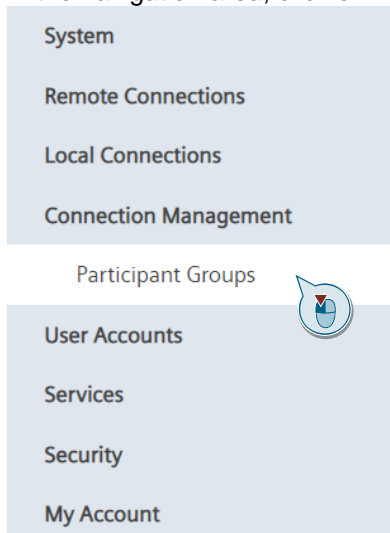
On the configuration PC, open the WBM of the SINEMA Remote Connect server ("https://172.16.1.60") and log on as an administrator.

### 2.3.1 Configure new group membership

Users, devices, end devices and subnets can be grouped together in participant groups. You will define whether communication between the participants in an individual group is allowed or forbidden.

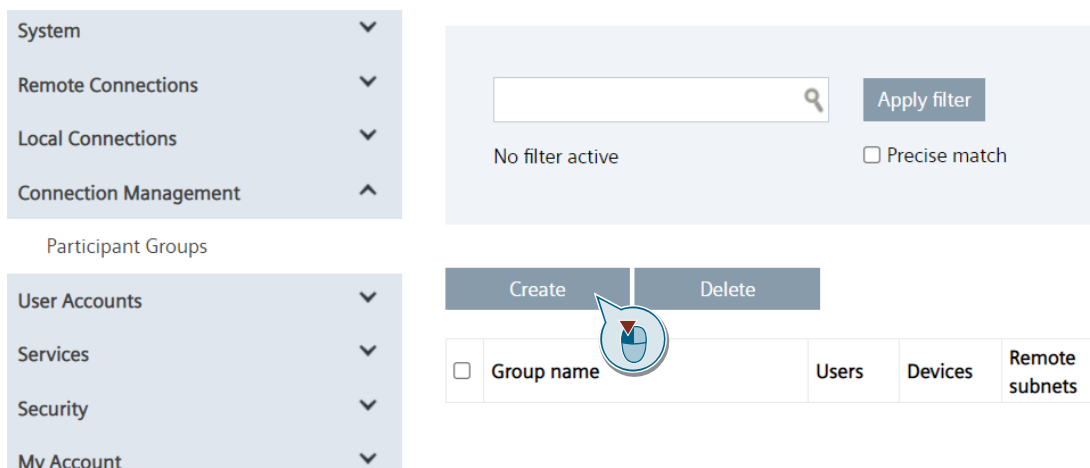
To create a new participant group, proceed as follows:

1. In the navigation area, click on "Connection Management > Participant Groups".



A new window opens. A list of already existing participant groups will appear.

2. Click the "Create" button.




The dialog for creating a new participant group appears.


3. Create a new participant group.
  - Enter a group name and an optional description.
  - Tick the "Members may communicate with each others" checkbox to allow the group members to communicate with each other.
  - Click the "Save" button.


**Note**

The "Members may communicate with each others" setting not only allows all devices, but also all users to communicate with each other. If you do not want this, you must create multiple participant groups and define the communication relationships.

\* Group name:   1




Description:

 2  Members may communicate with each other.

 3

**Result**

The participant group has been created. You will be automatically taken back to the overview page. The participant group appears as a new entry in the list.

Group name	Users	Devices	Remote subnets	Remote nodes	Local connections	Local subnets	Local nodes	Roles	Destination group	Actions
<input type="checkbox"/> MobileUser	0	0	0	0	No	0	0	0	MobileUser	  

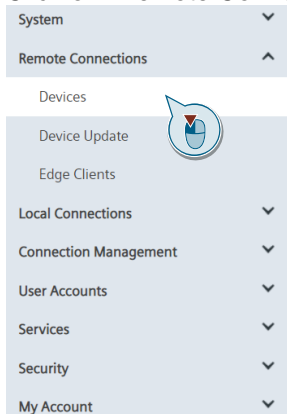
## 2.3.2 Create a remote connection for the SCALANCE SC-600 security appliance

### Create a device

In order for the SCALANCE device to initiate a VPN connection to the SINEMA Remote Connect server, it is declared as a device to the SINEMA Remote Connect server.

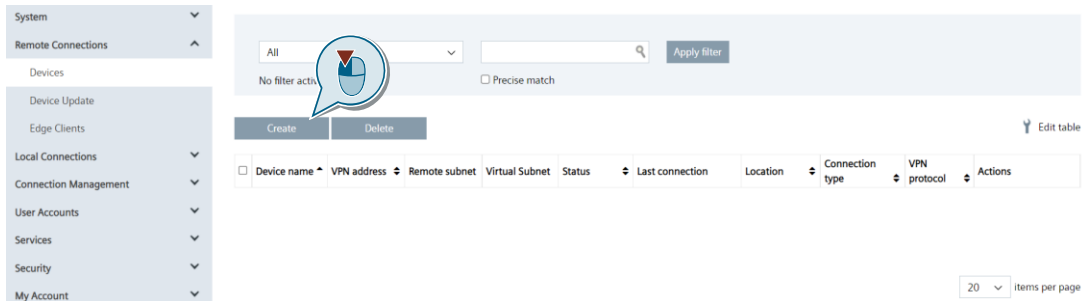
Proceed as follows to manage the devices:

1. Click on "Remote Connections > Devices" in the navigation area.



The device overview opens. This page shows a table listing the existing device records. The most important information for each device appears in various columns.

2. Click the "Create" button to create a new device.



A new window will open and you will be in the "Device Settings" tab. The device settings comprise three sections.

3. In the first section, "Device information", configure the general device information:
  - Give the device a name.
  - Assign a password and confirm it.
  - Select the end device type from the list (here: "SCALANCE SC-600")

Device Settings | Network Settings

Device information: ▼

\* Device name: SCALANCE\_SC

\* Password: .....

\* Confirm password: .....

Vendor: Siemens

\* Type: SCALANCE SC-600

Location:

Comment:

4. Leave the settings in the second section, "VPN settings", at the default values.

VPN settings: ▼

\* VPN protocol: OpenVPN

\* Connection type: Permanent

Request VPN address

Use fixed VPN address

Connection parameters

5. In the third section, "All access", configure the participant group. Select the participant group "MobileUser" (created in [chapter 2.3.1](#)). The subnets and end devices reachable via this device automatically become members in this participant group.

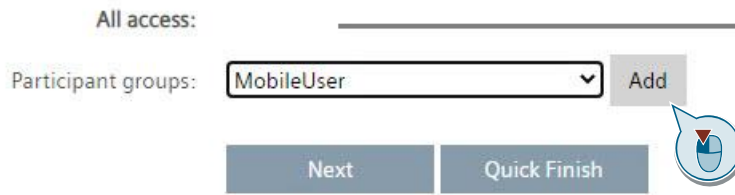
Group settings: ▼

Participant groups: MobileUser Add

MobileUser

Next Quick Finish

- 6. Click the "Add" button.



The participant group will be added.  
This completes the device settings.

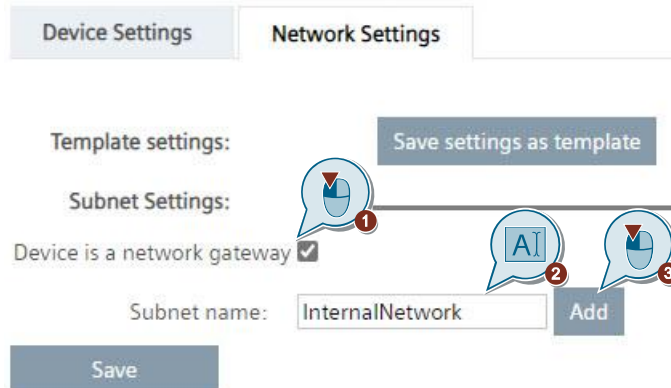
- 7. Click on "Next".



The "Network Settings" tab opens.

- 8. Since the SCALANCE device is a gateway, tick the checkbox for "Device is a network gateway".

In the "Subnet name" field, enter a unique name for the subnet behind the SCALANCE device, then click "Add".



The area "Subnet <InternalNetwork>" will be created.

9. You will configure the subnet in the steps below. Select the participant group you created in [chapter 2.3.1](#). This participant group is allowed to access the subnet. Click the "Add" button.

The screenshot shows a configuration page with two tabs: "Device Settings" and "Network Settings". Under "Network Settings", there is a "Template settings:" section with a "Save settings as template" button. Below that is a "Subnet Settings:" section. A checkbox "Device is a network gateway" is checked. There is a "Subnet name:" input field with an "Add" button. Below this, a list of subnets is shown, with one entry "Subnet InternalNetwork" highlighted by a red box. Below the list, there are fields for "Subnet name:" (containing "InternalNetwork"), "Participant groups:" (containing "MobileUser" and an "Add" button), "Subnet IP:", "Subnet mask:", and "NAT Mode:" (set to "None"). There are also two speech bubble icons with numbers 1 and 2 pointing to the "Add" buttons.

The participant group will be added.



10. Specify the IPv4 address of the internal subnet and the associated subnet mask reachable via the device (see [Table 2-1](#)). Save the settings with "Finish".

Device Settings

Network Settings

Template settings: Save settings as template

Subnet Settings:

Device is a network gateway

Subnet name:  Add

Subnet

InternalNetwork

Subnet name:

Participant groups:  Add

MobileUser X AI

Subnet IP:  AI

Subnet mask:

NAT Mode:

Node name:  Add

Back
Finish

**Result**

The device configuration is complete and the window will close. You will be taken back to the "Devices" tab in the "Remote Connections > Devices" menu. The "SCALANCE\_SC" device is created and appears as a new device in the list.

Create		Delete		Edit table						
Device name	VPN address	Remote subnet	Virtual Subnet	Status	Last connection	Location	Connection type	VPN protocol	Actions	
<input type="checkbox"/>	SCALANCE_SC	-	192.168.2.0/24	-	Offline	-	Permanent	OpenVPN	<span>ⓘ</span> <span>✎</span> <span>⬇</span> <span>🔒</span> <span>⏸</span>	

### Ascertain device ID and load CA certificate

For each device in the device overview, the SINEMA Remote Connect server generates a unique device ID and a unique fingerprint. The device ID and the fingerprint can be found in the device information for the device.


The device ID and fingerprint or CA certificate are information that the SCALANCE device uses to authenticate itself when connecting to the SINEMA Remote Connect Server. You will enter this information in the SCALANCE device when configuring the VPN connection.

**Note**

In place of the fingerprint, the device can also authenticate itself with the CA certificate of the SINEMA Remote Connect server. This is the method that this example uses.

Proceed as follows to open the device information:

1. Click the "i" icon in the "Actions" column.

Create		Delete										Edit table
Device name	VPN address	Remote subnet	Virtual Subnet	Status	Last connection	Location	Connection type	VPN protocol	Actions			
SCALANCE_SC	-	192.168.2.0/24	-	Offline	-		Permanent	OpenVPN	    			

The "Device information" is displayed.

2. Make a note of the entry for "Device ID" or copy the entry and save the value in a text file in your local directory.

**Note**

Your device ID can have a different value than the one shown here.

**Device overview**

---

**Device information:**

**Device ID:** 58


IP address of the VPN server: 192.168.2.1

IP address of the Web server: 192.168.2.1


Web server port: 443

SHA1-Fingerprint: 51:EA:3C:95:AB:C4:BB:7D:AD:3C:E7:E4:EB:F9:C7:AB:93:90:44:0F

SHA256-Fingerprint: 3E:B8:48:5A:91:73:49:CD:9A:94:27:F1:7B:CC:EE:77:67:2A:A1:B4:77:30:E5:37:B7:A7:2D:98:6E:2B:4D:E7

Export CA: 

Device name: SCALANCE\_SC

Network Settings: 

Type: SCALANCE SC-600

Vendor: Siemens

Location:

Connection type: Permanent

3. Click on the download icon in the "Export CA" row and place the CA certificate of the SINEMA Remote Connect server in a local directory of the configuration PC.

Device overview

Device information:

Device ID: 58

IP address of the VPN server: 192.168.1.60  
192.168.1.60  
192.168.1.60

IP address of the Web server: 192.168.1.60  
192.168.1.60  
192.168.1.60

Web server port: 443

SHA1-Fingerprint: 51:EA:3C:95:AB:C4:BB:7D:AD:3C:E7:E4:EB:F9:C7:AB:93:90:44:0F

SHA256-Fingerprint: 3E:B8:48:5A:91:73:49:CD:9A:94:27:F1:7B:CC:EE:77:67:2A:A1:B4:77:30:E5:37:B7:A7:2D:98:6E:2B:4D:E7

Export CA:  

Device name: SCA 

Network Settings: 

Type: SCALANCE SC-600


Vendor: Siemens

Location:

Connection type: Permanent

### Result

You have found the device ID of the SCALANCE device and loaded the CA certificate. You will need the device ID and the CA certificate when configuring the VPN connection in the SCALANCE device (see [chapter 2.4](#)).

 CA\_851622\_SINEMA\_RC.crt

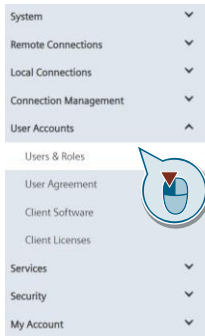
### 2.3.3 Create user account for the tablet

#### Define new user

In order to grant the service employee access to the SINEMA Remote Connect server with a tablet, set up a user account with a username and password.

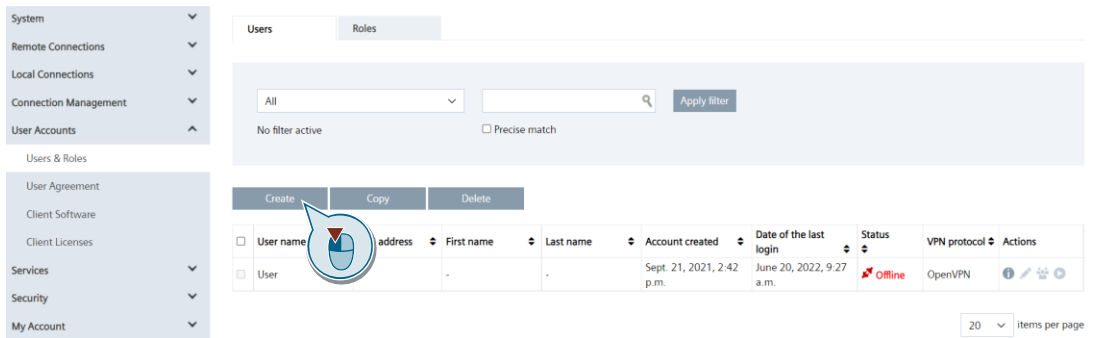
Follow these steps:

1. In the navigation area, click on "User Accounts > Users & Roles".



A new window opens and you will be in the "Users" tab. You will see a list of existing users and their status.

2. Click "Create".



A new window opens and you will be in the "Contact Data" tab.

3. Edit the contact data:

- Enter the necessary information. The "User name" field is required. The other contact information is optional and can be entered or modified by the user himself.
- For "Login method", select "Password".
- Click on "Next".

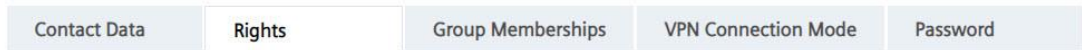
Contact Data	Rights	Group Memberships	VPN Connection Mode	Password
* User name:	Mobile_iOS			
First name:	Service_1			
Last name:				
Phone:				
E-mail address:				
* Login method:	Password			
PKI DN filter rule:				
<input type="button" value="Next"/>				

You are in the "Rights" tab.

- 4. You are able to give the user rights:
  - Assign rights by assigning a role:  
Click "+" and select the desired role from the dropdown menu. The user receives the rights that are assigned to the role. Tick the boxes to assign additional rights.
  - Assign rights without assigning a role:  
If you have not selected a role, activate the pertinent role by clicking on the checkbox.

The user is not assigned any additional rights in this example.

Click on "Next".



### Roles



### Rights

- Manage address spaces
- Create backup copies
- Restore the system
- Force comment
- Manage firmware updates
- Manage devices
- Manage remote connections
- Edit system parameters
- Certificate management
- Manage users and roles
- Download client software



The "Group Memberships" tab appears.

- 5. If you already created participant groups, you can assign the new user to one of them.  
Select the participant group "MobileUser" (see [chapter 2.3.1](#)).  
Click on "Next".



Participant group Mobile\_iOS

- MobileUser



The "VPN Connection Mode" tab appears.

6. Do not make any changes in this tab.

Click on "Next".

The "Password" tab appears.

7. Enter a password and confirm it. The assigned password can be changed later by the respective user himself.

Click "Finish".

**Result**

The window closes and you will be back in the "Users" tab in the menu "User Accounts > Users & Roles".

The user "Mobile\_iOS" has been created and appears in the list as a new user.

<input type="checkbox"/>	User name	VPN address	First name	Last name	Account created	Date of the last login	Status	VPN protocol	Actions
<input type="checkbox"/>	Mobile_iOS	-	Service_1	-	June 20, 2022, 10:34 a.m.	None	<span style="color: red;">Offline</span>	OpenVPN	
<input type="checkbox"/>	User	-	-	-	Sept. 21, 2021, 2:42 p.m.	June 20, 2022, 10:31 a.m.	<span style="color: red;">Offline</span>	OpenVPN	

## Load user configuration

The following data are automatically generated when the user is created:

- The configuration file "<Username>.ovpn" containing various parameters necessary for a connection with the server
- A file "<Username>.pem" with the certificate and the key as ASCII code
- A certificate container "<Username>.pkcs12" in PFX format

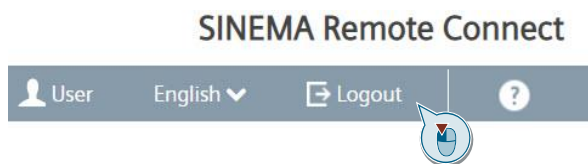
These files are downloaded to the participant in the remote network who establishes a VPN connection to the SINEMA Remote Connect server.

For the tablet, you only need the configuration file.

To download the file to the service worker's tablet, first export it from the SINEMA Remote Connect server.

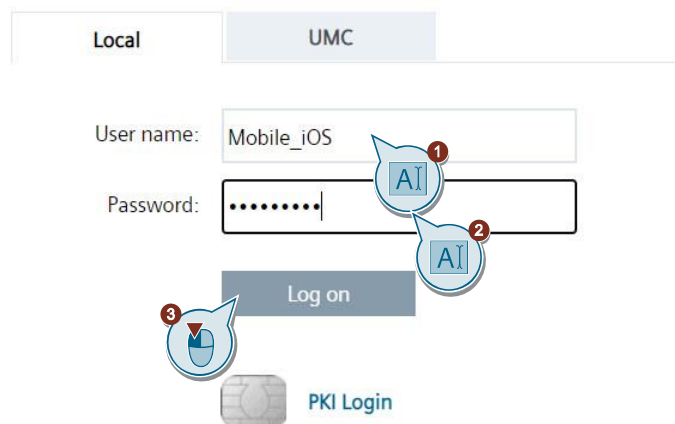
Proceed as follows to export the file:

1. Log off as an administrator from the WBM. The "Logout" button is located in the display area of the window.



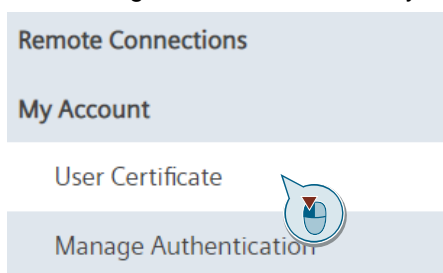
2. Log back in with the new user you just created.

### Welcome to SINEMA Remote Connect



The user's homepage will open.

3. In the navigation area, click on "My Account > User Certificate".





- You will be in the "Details" tab. Here you will see an overview of the user certificate, which is derived from the CA certificate. Click on the "Exports" tab.

The "Exports" tab opens.

- All exportable files will appear here. Click on the format descriptions to download the OpenVPN configuration for the user to a local directory on your configuration PC.

Format	Description
<a href="#">PKCS #12</a>	Container in the Personal Information Exchange format (PFX)
<a href="#">PEM</a>	Certificates and key as Base64 encoded ASCII text
<a href="#">OVPN</a>	Export OpenVPN configuration

### Result

The configurations file was saved in the local directory.

 Mobile\_iOS.ovpn

## 2.4 Setting up remote access on the SCALANCE device

### Overview

The following configuration steps are required in order to successfully establish a VPN tunnel between the SCALANCE device and the SINEMA Remote Connect server:

- Download certificate to device
- Configure VPN connection

### Preparation

To access the WBM, the following requirements must be met:

- You will need an Ethernet connection between the configuration PC and the SCALANCE device (Zone INT; LAN port: P1 to P4).
- The configuration PC has an IP address in the network of the SCALANCE device, for example 192.168.2.100/24.

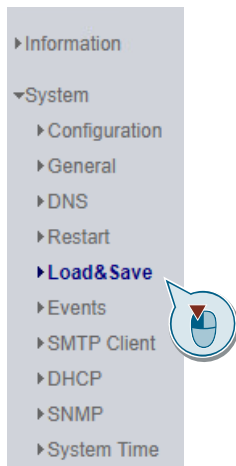
### Open the WBM

Open the WBM of the SCALANCE device with the address "https://192.168.2.1". Log on as an administrator.

### 2.4.1 Load CA certificate

When the OpenVPN connection is established, the SCALANCE device authenticates itself with the SINEMA Remote Connect server using its CA certificate. This certificate is exported from the SINEMA Remote Connect server (see chapter [2.3.2](#)) and downloaded to the SCALANCE device as follows:

1. In the navigation pane, click "System > Load & Save".



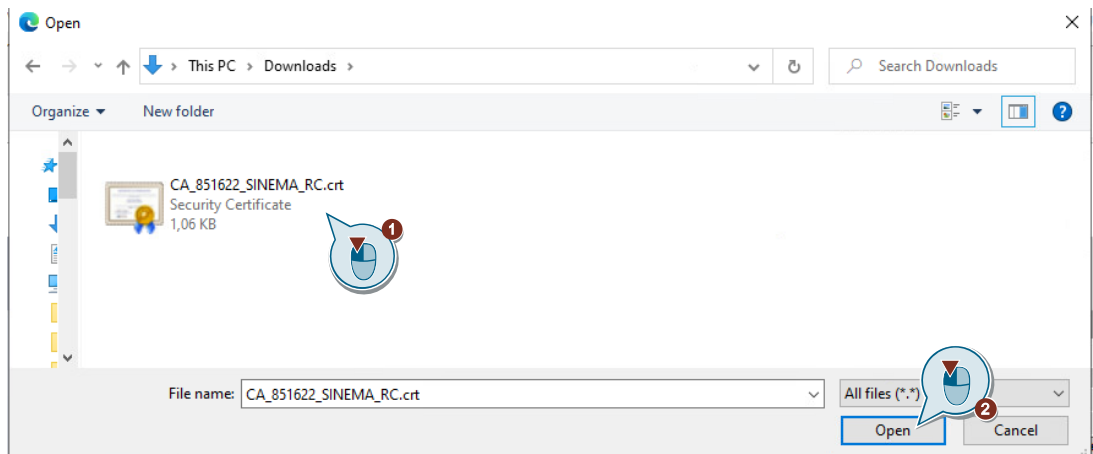
A new window opens.

2. You will be in the "HTTP" tab. Here you can load the certificates required in order to establish a secure VPN connection. By the type "X509Cert", click the "Load" button.

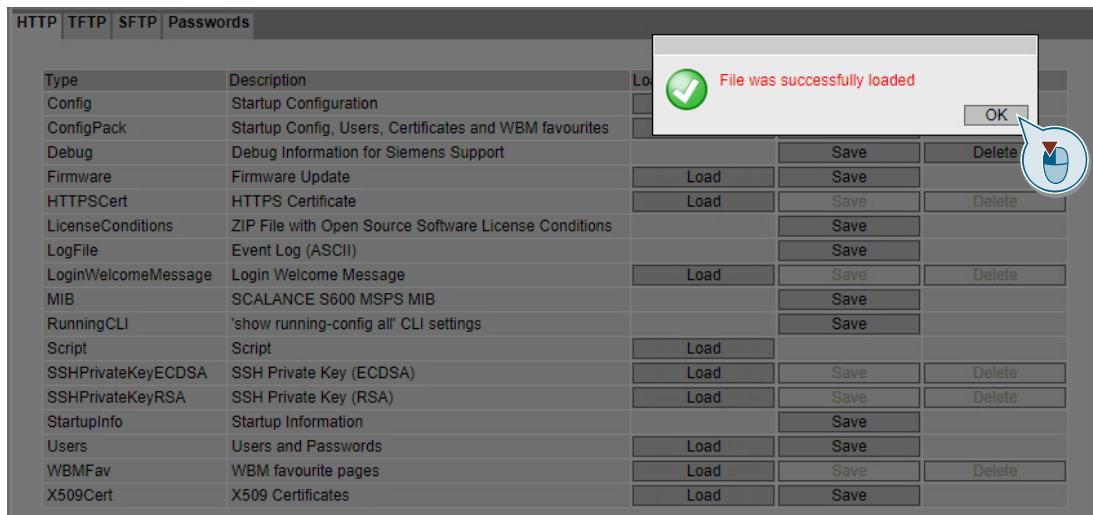
Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LicenseConditions	ZIP File with Open Source Software License Conditions		Save	
LogFile	Event Log (ASCII)		Save	
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
MIB	SCALANCE S600 MSPS MIB		Save	
RunningCLI	'show running-config all' CLI settings		Save	
Script	Script	Load		
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	Load	Save	Delete
SSHPrivateKeyRSA	SSH Private Key (RSA)	Load	Save	Delete
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBM Fav	WBM favourite pages	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	

The file upload dialog will open.

3. Navigate to the CA certificate exported from the SINEMA Remote Connect server. Click on the "Open" button in the dialog.



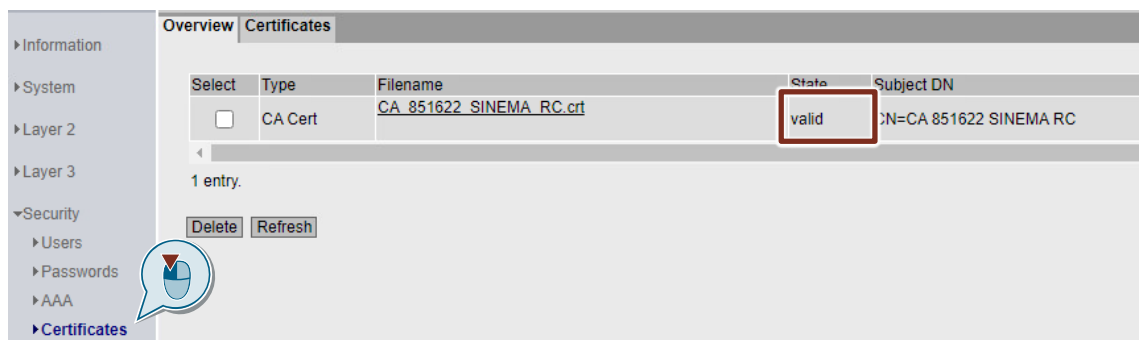
4. The file will now be loaded to the device. Once the file is loaded, confirm the message with "OK".



**Result**

The certificate has been loaded. You can view the certificate under "Security > Certificates".

5. Check whether the certificate has the status "valid".



**Note**

If the certificate appears with the status "expired", then check whether the time on the SCALANCE device is correct.

## 2.4.2 Configure VPN connection

The link to the SINEMA Remote Connect server has already been allowed in the SCALANCE SC-600. Thanks to the autoconfiguration interface, the connection to the SINEMA Remote Connect server is simple to configure.

**Note**

To allow the connection to the SINEMA Remote Connect server with a SCALANCE S615 or SCALANCE M-800 industrial router, you will need the "SINEMA RC" KEY-Plug.

Proceed as follows to set up the VPN connection:

1. Click "System > SINEMA RC" in the navigation area.



The "SINEMA Remote Connect (SINEMA RC)" window opens. Here you will configure access to the SINEMA Remote Connect server in multiple sections.

2. Configure the "Server settings" section.  
In the "SINEMA RC Address" field, enter the WAN IPv4 address. In the "SINEMA RC Port" field, enter the HTTPS port of the SINEMA Remote Connect server.

**Note**

If you entered a hostname in the SINEMA Remote Connect server, then enter the FQDN (fully qualified domain name) here.

If you use a different port than the default HTTPS port 443, then enter your modified port number.

Enable SINEMA RC

**Server Settings**

SINEMA RC Address: WAN-IPv4-Address

SINEMA RC Port: 443

**Server Verification**

Verification Type: Fingerprint

Fingerprint:

CA Certificate: -

**Device Credentials**

Device ID: 0

Device Password:

Device Password Confirmation:

**Optional Settings**

Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

Set Values Refresh

3. Change to the "Server Verification" section.  
In the "Verification Type" dropdown list, select "CA Certificate". In the "CA Certificate" dropdown list, select the server certificate that you loaded previously (see [chapter 2.4.1](#)).

**Server Verification**

Verification Type: CA Certificate

Fingerprint:

CA Certificate: CA\_851622\_SINEMA\_I

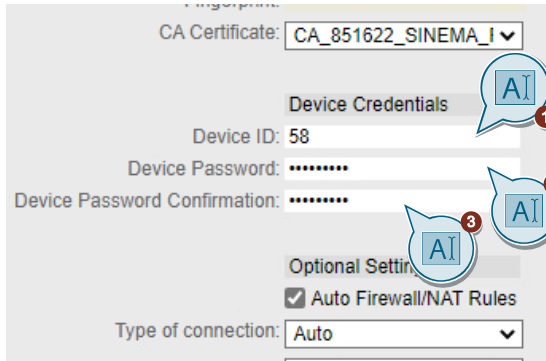
**Device Credentials**

Device ID: 0

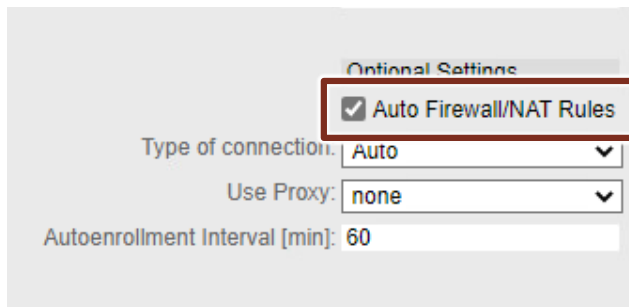
4. Change to the "Device Credentials" section.

In the "Device ID" field, you will enter the value for the "device ID" that the SCALANCE device received from the SINEMA Remote Connect server (see [chapter 2.3.2](#)).

In the "Device Password" field, enter the access password that you configured earlier (see [chapter 2.3.2](#)).



5. By default, the "Auto Firewall/NAT Rules" checkbox in the "Optional Settings" section is ticked so that the appropriate NAT and firewall rules will be created automatically. Leave the default setting or tick the box if it is not ticked.



6. Click the "Set Values" button.

Enable SINEMA RC

**Server Settings**

SINEMA RC Address:

SINEMA RC Port:

**Server Verification**

Verification Type:

Fingerprint:

CA Certificate:

**Device Credentials**

Device ID:

Device Password:

Device Password Confirmation:


**Optional Settings**

Auto Firewall/NAT Rules

Type of connection:

Use Proxy:

Autoenrollment Interval [min]:





- To activate the SINEMA Remote Connect server, tick the "Activate SINEMA RC" checkbox. Click the "Set Values" button.

### Result

The SCALANCE device will automatically establish the OpenVPN tunnel to the SINEMA Remote Connect server.

You can check whether the connection is successful in the WBM under "Information > SINEMA RC".

## 2.5 Setting up remote access on the tablet

Remote access between the tablet and the SINEMA Remote Connect server is secured with an OpenVPN connection.

The party that initiates the connection is the "OpenVPN Connect" app installed on the tablet.

### Transfer configuration file

Transfer the configuration file to the tablet.

You have the following options:

- Synchronize data via iTunes
- Transfer via email. In this case, make sure the transfer is secure, for example with appropriate encryption.

1. Import the file "Mobile\_iOS.ovpn" (for example via iTunes) and save the file locally on your tablet.



Mobile\_iOS.ovpn  
Heute, 08:34  
9 KB

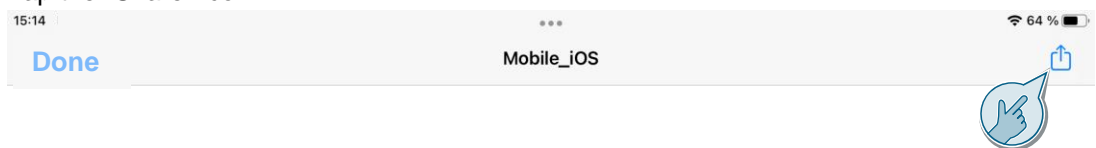
2. Tap the file to open it.



Mobile\_iOS.ovpn  
Heute, 08:34  
9 KB

The file opens.

3. Tap the "Share" icon.

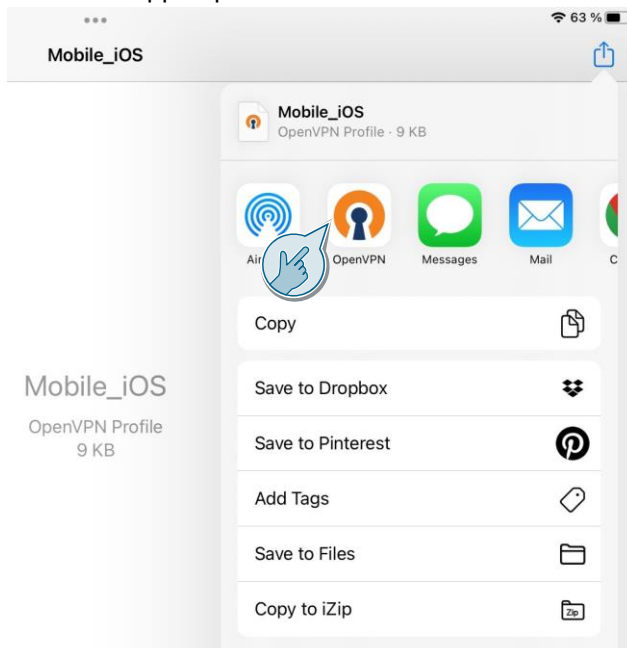


Mobile\_iOS

OpenVPN Profile  
9 KB

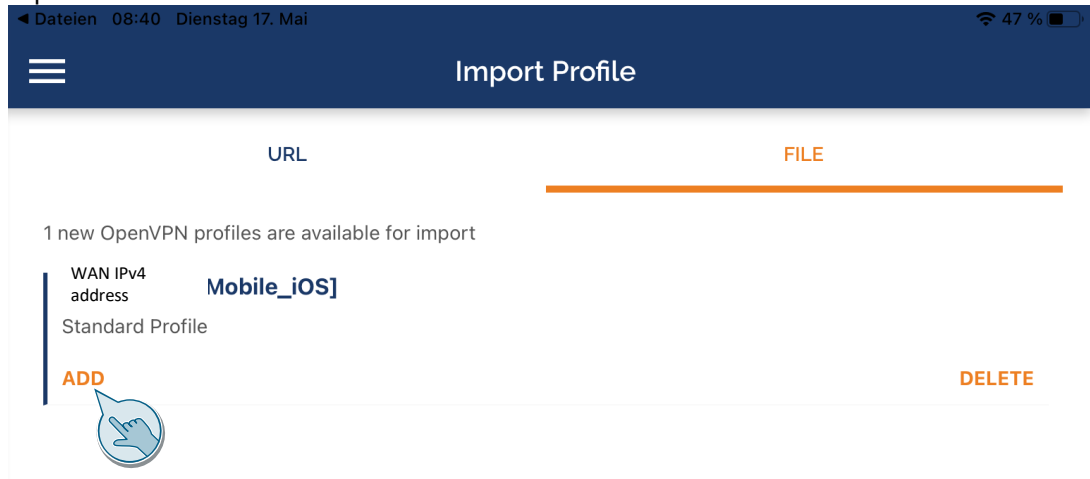
The context menu opens.

4. Select the app "OpenVPN Connect".



Once in the "OpenVPN Connect" app, you will be prompted to apply the new configuration.

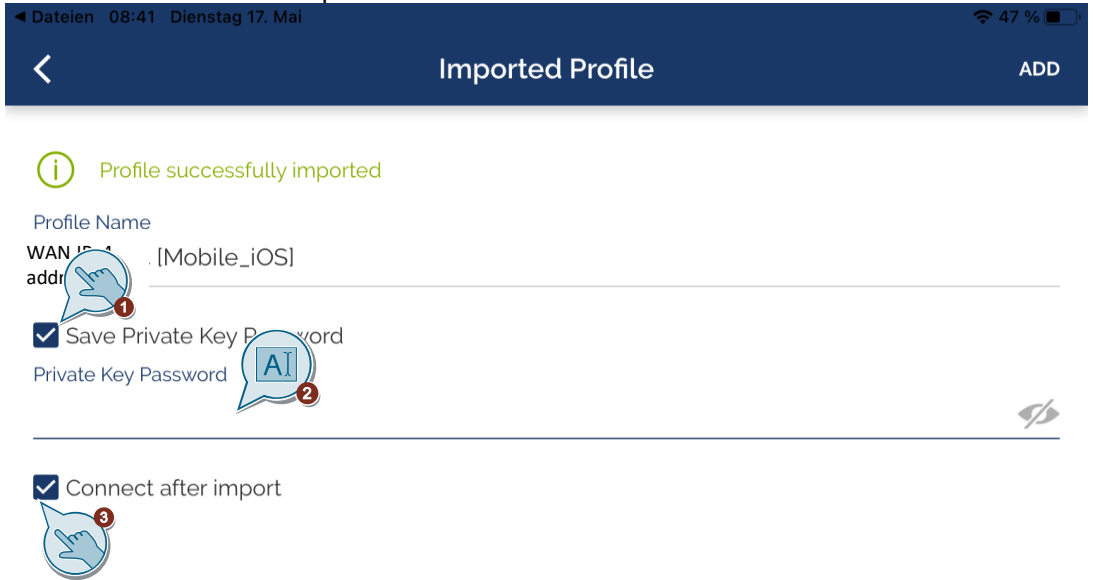
5. Tap "ADD".



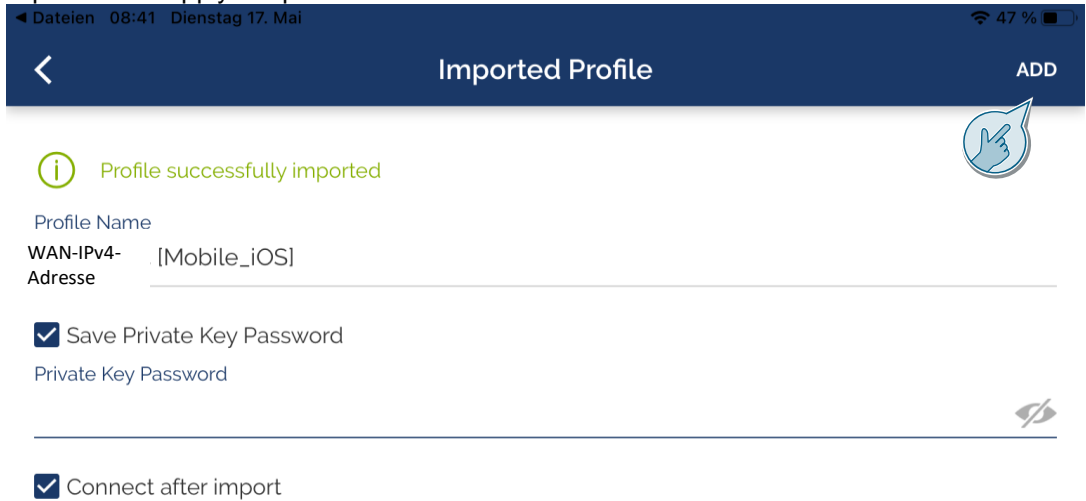
The profile opens.

6. Fill out the password entry view.

- Tick the checkbox for "Save Private Key Password" to save the password.
- The password is required for the certificate. In the "Private Key Password" field, enter the password that you defined in SINEMA Remote Connect Server for the new user (see [chapter 2.3.3](#)).
- Tick the "Connect after import" box to make the app connect with the SINEMA Remote Connect server after the import.



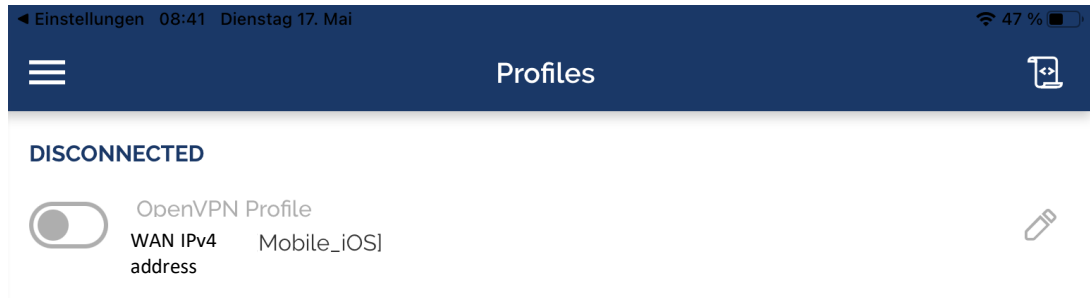
7. Tap "ADD" to apply the profile.



8. You will be prompted to enter your iPad's code to give the "OpenVPN Connect" app permission to set up VPN connections. Confirm this.

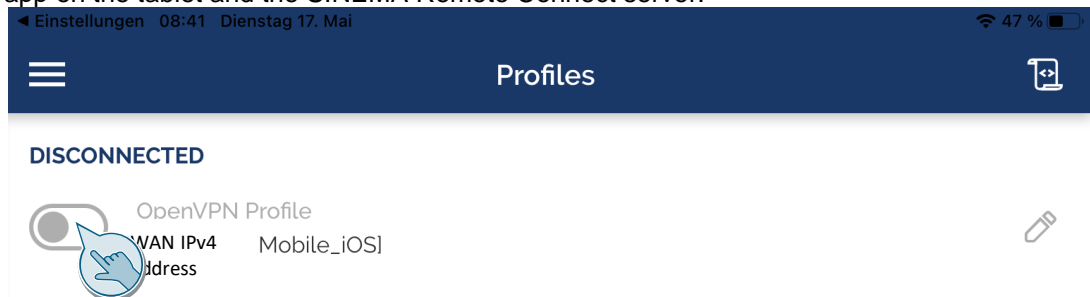
### Result

The profile has been imported. The VPN connection is inactive and appears as "DISCONNECTED".



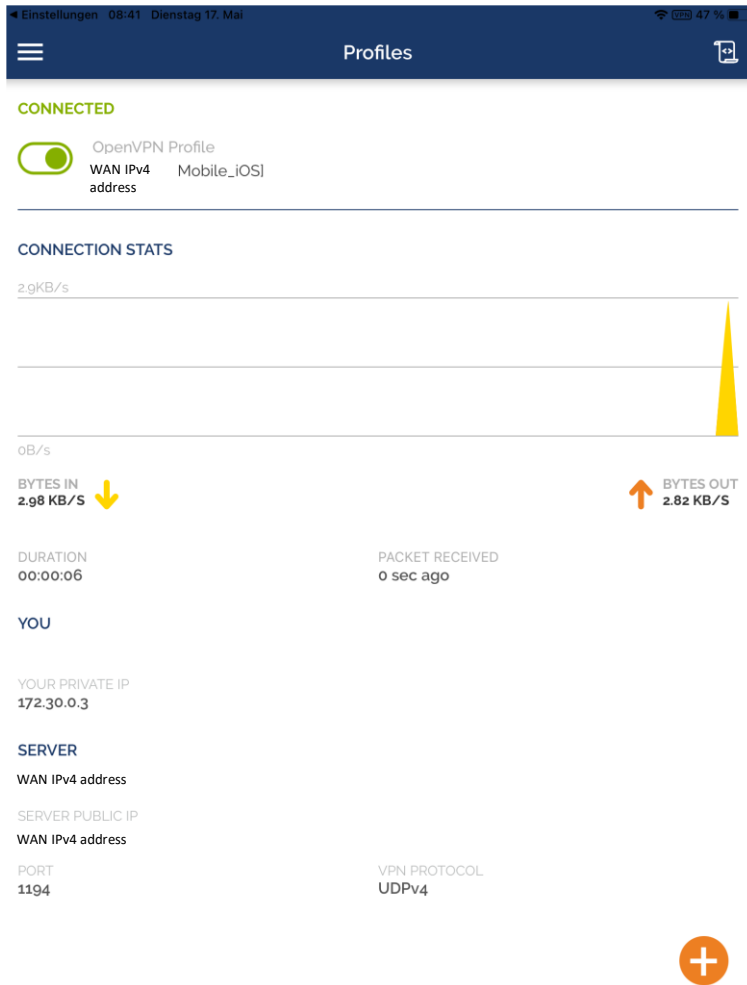
### Initialize VPN

Slide the switch to the right to initialize the OpenVPN tunnel between the "OpenVPN Connect" app on the tablet and the SINEMA Remote Connect server.



### Result

Once the connection has been established, the status in the "OpenVPN Connect" app will appear as "CONNECTED".



## 3 Operation

### 3.1 Check VPN connection

After [chapter 2](#), the configurations on the SCALANCE device and the tablet are complete. The partners establish a VPN tunnel to the SINEMA Remote Connect server.

You can check the status in the devices themselves or centrally in the SINEMA Remote Connect server.

#### Preparation

To access the WBM of the SINEMA Remote Connect server, check the following points:

- You will need an Ethernet connection between the configuration PC and the SINEMA Remote Connect server.
- The configuration PC has an IP address in the network of the SINEMA Remote Connect server, for example 172.16.1.100/16.

#### Open the WBM

On the configuration PC, open the WBM of the SINEMA Remote Connect server ("https://172.16.1.60") and log on as an administrator.

#### Check the connection

Proceed as follows to check the status in the SINEMA Remote Connect server:

1. In the navigation area, click on "User Accounts > Users & Roles". You can see the user "Mobile\_iOS" online.

User name	VPN address	First name	Last name	Account created	Date of the last login	Status	VPN protocol	Actions
Mobile_iOS	172.30.0.4	Service_1	-	May 17, 2022, 7:59 a.m.	May 17, 2022, 9:20 a.m.	Online	OpenVPN	

2. Click on "Remote Connections > Devices" in the navigation area. You can see the SCALANCE device online.

Device name	VPN address	Remote subnet	Virtual Subnet	Status	Last connection	Location	Connection type	VPN protocol	Actions
SCALANCE_SC	172.30.0.6	192.168.2.0/24	-	Online	June 1, 2022, 10:19 a.m.		Permanent	OpenVPN	

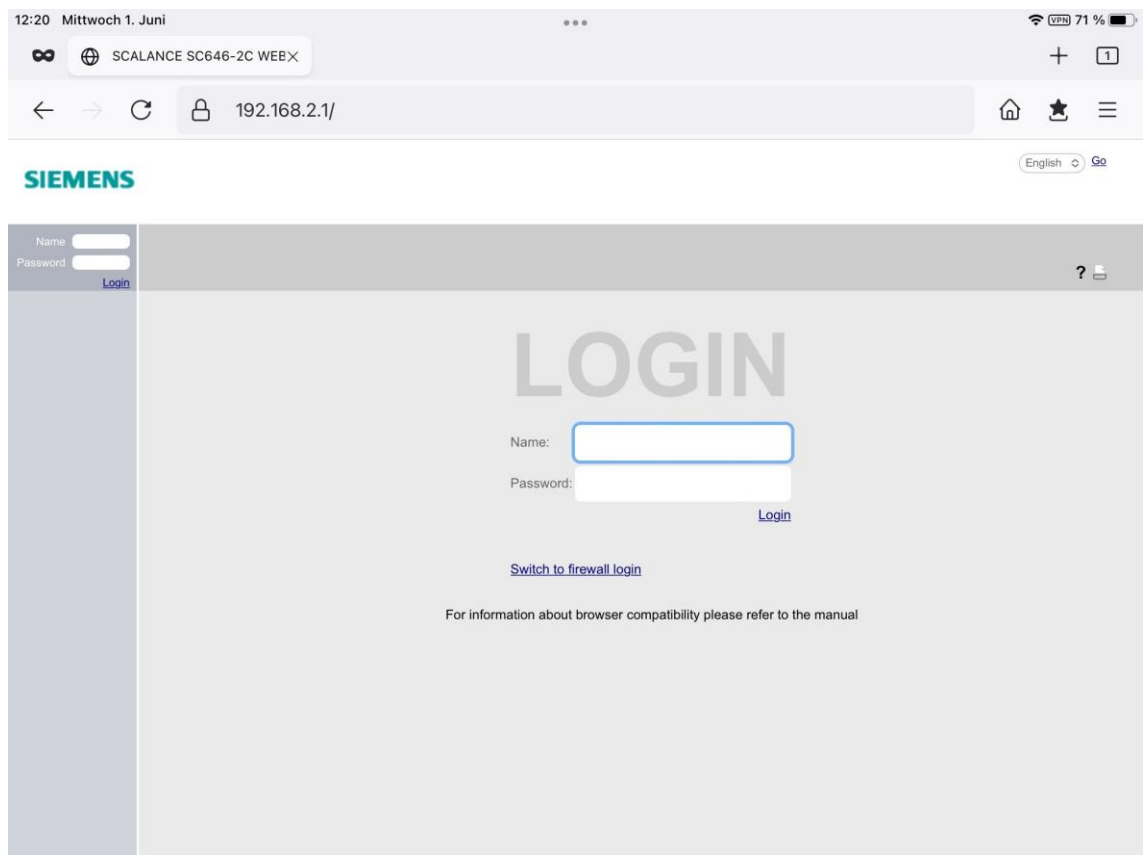
### 3.2 Test VPN connection

If the tablet and the SCALANCE device have initiated their OpenVPN tunnel to the SINEMA Remote Connect server, then the tablet can access the internal network of the SCALANCE device (subnet 192.168.2.0).

**Note**

In every device that is located in the internal network of the SCALANCE device, the internal IP address of the SCALANCE device (Zone INT; LAN port: P1 to P4) must be entered as the default router.

You can test this by opening the WBM of the SCALANCE device via its internal IP address ("https://192.168.2.1"). The start page appears.





## 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](https://support.industry.siemens.com)

#### Technical Support

The Technical Support of Siemens Industry provides you with 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](https://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 training and courses, as well as their locations and dates, refer to our web page:

[siemens.com/sitrain](https://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 on the service catalog web page:

[support.industry.siemens.com/cs/sc](https://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](https://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](http://mall.industry.siemens.com)

## 4.3 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Link to the article page of the application example <a href="https://support.industry.siemens.com/cs/ww/en/view/109479578">https://support.industry.siemens.com/cs/ww/en/view/109479578</a>
\3\	FAQ: Settings of the ports for secure VPN connections with SINEMA Remote Connect <a href="https://support.industry.siemens.com/cs/de/en/view/109745584">https://support.industry.siemens.com/cs/de/en/view/109745584</a>
\4\	Overview document: Secure remote access with VPN <a href="https://support.industry.siemens.com/cs/de/en/view/26662448">https://support.industry.siemens.com/cs/de/en/view/26662448</a>

## 4.4 Change documentation

Table 4-2

Version	Date	Change
V1.0	09/2015	First version
V1.1	06/2018	Revision of chapter 2.2.2
V1.2	09/2020	Revision of chapter 2.2.2
V2.0	06/2022	Complete revision