

Jump Host Application with SINEMA RC

SINEMA Remote Connect, SCALANCE S615

<https://support.industry.siemens.com/cs/ww/de/view/109746841>

Siemens
Industry
Online
Support



Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document. Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Table of Contents

Warranty and Liability	2
1 Task and Solution	4
1.1 Task	4
1.2 Possible solution	4
1.2.1 Complete overview	4
1.2.2 Participants' functions and tasks	5
1.2.3 Process	6
1.2.4 SINEMA Remote Connect	10
1.3 Features of the solution	12
2 Configuration and Project Engineering	13
2.1 Setting up the environment	13
2.1.1 Required components and IP address overview	13
2.1.2 Router on the service technician side	16
2.1.3 Service technician PC	16
2.1.4 Router on the DMZ side	17
2.1.5 JumpHost	17
2.1.6 SCALANCE S615	17
2.2 Setting up the SINEMA Remote Connect Server	18
2.2.1 Configuring basic parameters	18
2.2.2 Defining participant groups	21
2.2.3 Creating a new device	23
2.2.4 Creating new user accounts	28
2.3 Setting up the remote connection on the S615	35
2.4 Setting up the remote connection on the service technician side	41
2.5 Establishing the remote desktop connection	43
3 Testing the Tunnel Function	47
4 Appendix	48
4.1 Service and Support	48
4.2 Links and Literature	49
4.3 Change documentation	49

1 Task and Solution

1.1 Task

The task is to provide a service technician with secure remote access to a plant for maintenance, control and diagnostic purposes.

The company's security policies prohibit direct access to the plant network from an external public network.

According to the company's security policies, the service technician is only allowed to access the demilitarized zone (DMZ) implemented in the corporate network. The VPN tunnels protect the communication connections. The SINEMA Remote Connect Server will manage and provide the VPN tunnels.

The security policies have the following requirements for the task:

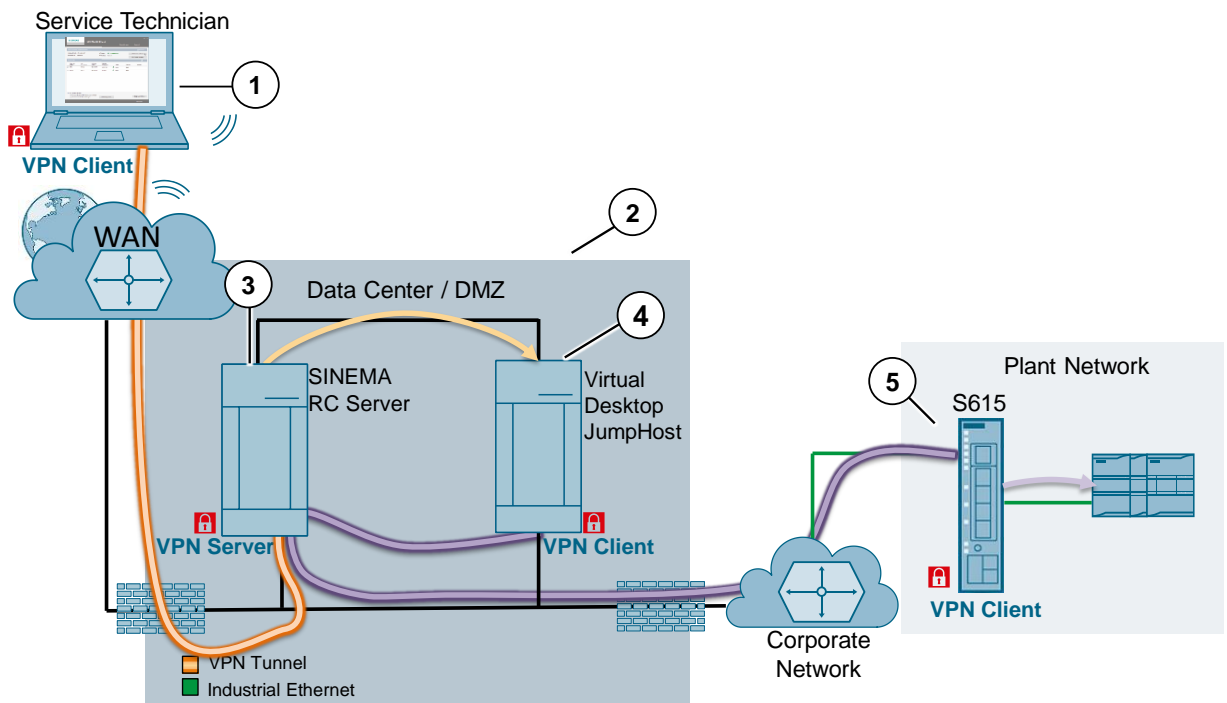
- Prevent unauthorized access to company data.
- Prevent direct access to the plant network by external users.
- Protect against data manipulation and spying.
- Protect the plant network against manipulation and unauthorized access.

1.2 Possible solution

1.2.1 Complete overview

The figure below shows one way of implementing the security requirements. The participants are explained in greater detail in [Table 1-1](#):

Figure 1-1



Brief description

Devices of the plant such as SIMATIC stations, panels, drives, PCs, etc. are connected to the SCALANCE S615.

The service technician uses a mobile device, for example a notebook computer.

The DMZ is a stand-alone subnet that separates the private local network from the external public network using firewall routers. This DMZ contains the company's servers and computer hosts.

Multiple VPN tunnels protect the communication between the nodes/areas.

1.2.2 Participants' functions and tasks

The following table shows the functions and tasks of the individual participants:

Table 1-1

No.	Participant	Task and function
1	Service technician	The service technician has SINEMA Remote Connect Client installed on his mobile device. With this software, the service technician establishes a VPN tunnel to the SINEMA Remote Connect Server.
2	DMZ	A DMZ is a neutral zone between a company's private network and the external public network. This DMZ contains the following corporate servers and computer hosts: <ul style="list-style-type: none"> • SINEMA Remote Connect Server • Virtual Desktop JumpHost Moving the devices to the DMZ prevents external users from directly accessing a server with company data.
3	SINEMA Remote Connect Server	The SINEMA Remote Connect Server is the endpoint of all VPN connections. Depending on the configured communication relationships and the security settings, the SINEMA Remote Connect Server routes between the individual VPN tunnels. Depending on the configured communication groups, the SINEMA Remote Connect Server enables its LAN interface for access to the internal network. Note: Hardware-wise, the SINEMA Remote Connect Server has two physically separate interfaces: <ul style="list-style-type: none"> • WAN interface for connecting the external network. This interface is used for the VPN tunnels. • LAN interface for connecting to the internal network in the DMZ.
4	JumpHost	A JumpHost is a special-purpose computer on a network. It is typically used to control or configure devices in a different security zone. To solve the task of this application example, the following software packages are installed on the JumpHost: <ul style="list-style-type: none"> • SINEMA Remote Connect Client • TIA Portal • Remote Desktop A remote desktop connection provides you with the following options: <ul style="list-style-type: none"> • Start SINEMA Remote Connect Client and establish a VPN tunnel to the SINEMA Remote Connect Server. • Start TIA Portal and configure the devices in the plant. Note: Hardware-wise, the JumpHost has two physically separate interfaces:

No.	Participant	Task and function
		<ul style="list-style-type: none"> LAN interface for connecting the external network. This interface is used for the VPN tunnel. WAN interface for connecting to the internal network in the DMZ.
5	SCALANCE S615	The SCALANCE S615 automatically establishes a VPN tunnel to the SINEMA Remote Connect Server. The S615 is connected upstream to the plant and protects it against unauthorized access.

1.2.3 Process

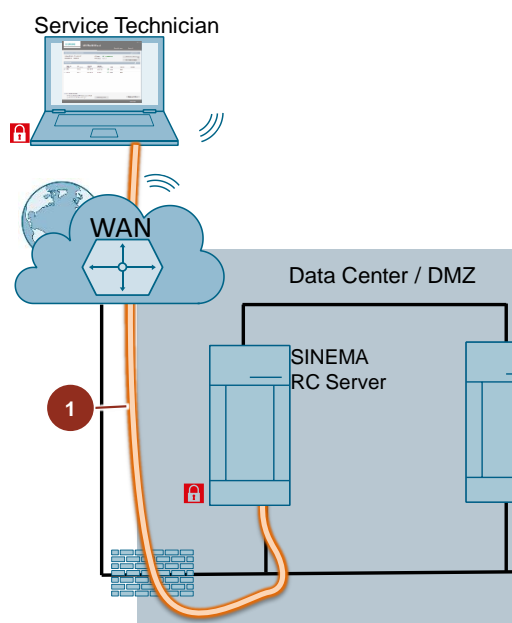
Description

As the corporate security policies prohibit direct access to the plant, the company has set up a DMZ with the required servers. In combination with VPN connections and a remote desktop connection, the service technician can remotely access the plant.

Individual steps of the process

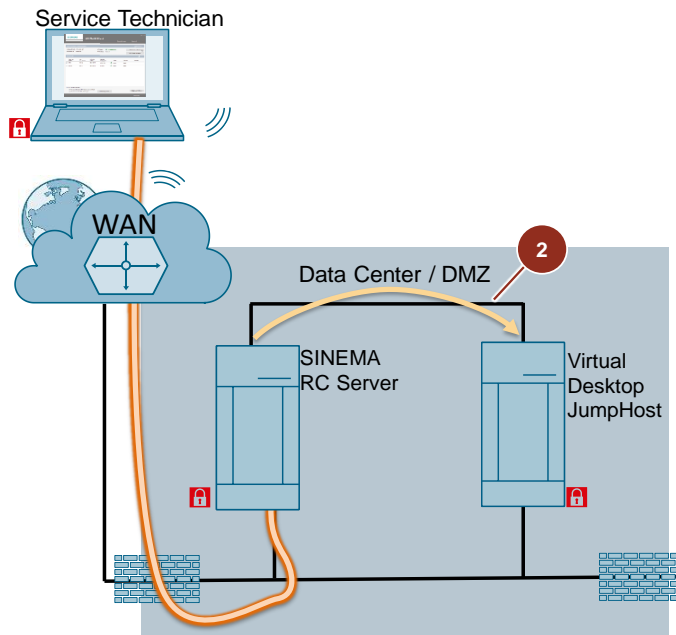
Secure remote maintenance using a JumpHost application consists of several steps:

1. On his PC, the service technician starts SINEMA Remote Connect Client and uses it to establish a VPN tunnel (VPN Tunnel1) to the SINEMA Remote Connect Server.

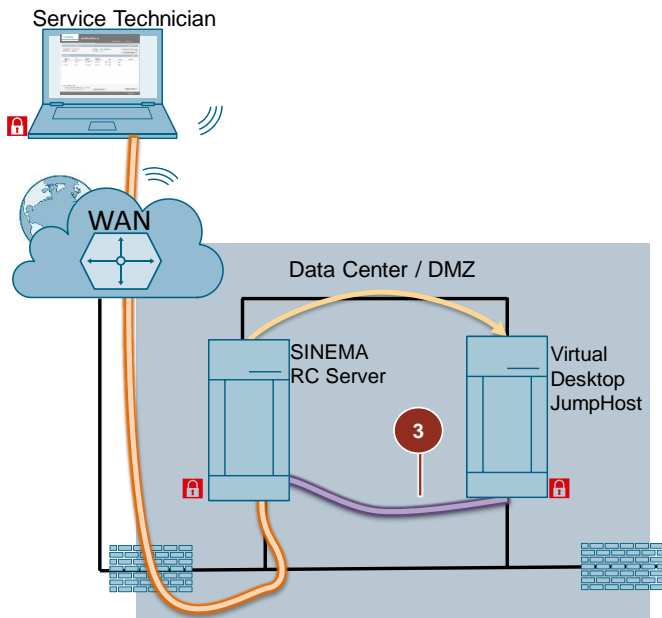


1 Task and Solution

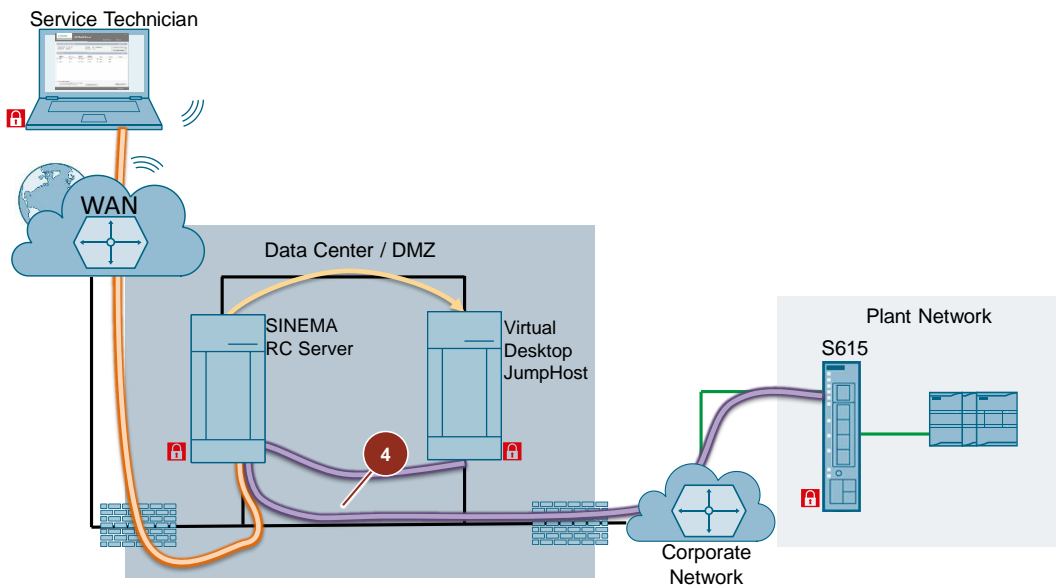
2. Due to the configuration setting in the SINEMA Remote Connect Server, the server enables its LAN interface for the service technician. Using a remote desktop connection, the service technician connects his PC to the JumpHost.



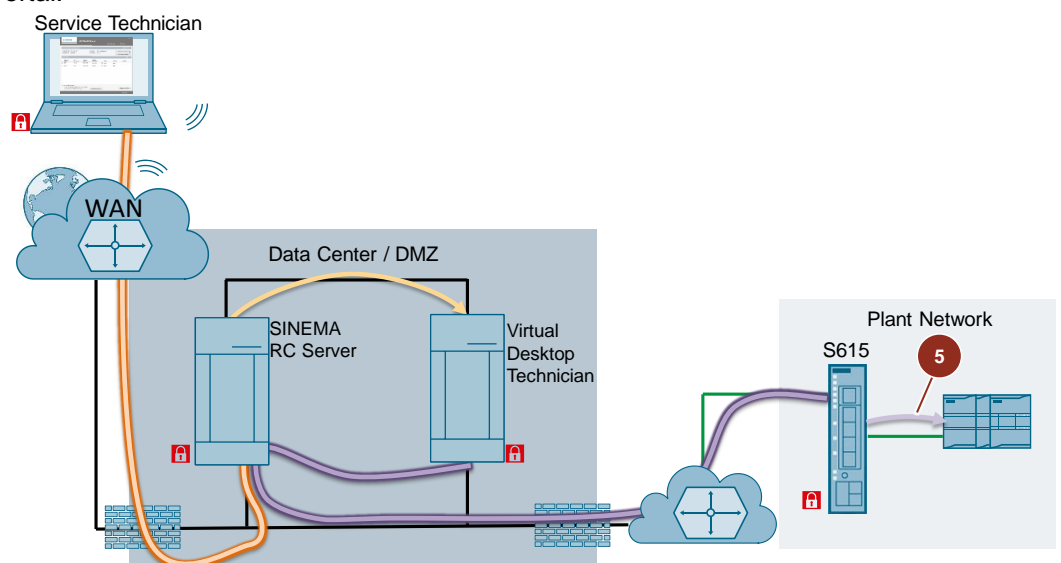
3. Using the remote desktop connection, the service technician starts SINEMA Remote Connect Client on the JumpHost. The SINEMA Remote Connect Client establishes a VPN tunnel to the SINEMA Remote Connect Server.



4. The SCALANCE S615 automatically establishes a VPN tunnel to the SINEMA Remote Connect Server. Due to the configuration setting in the SINEMA Remote Connect Server, the JumpHost and the SCALANCE S615 belong to the same communication group.



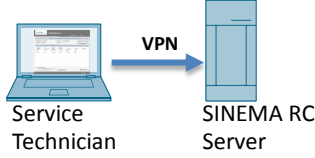
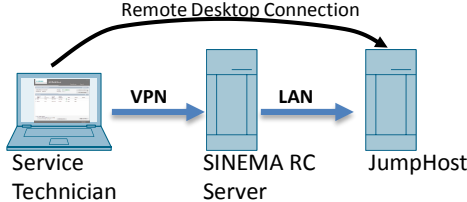
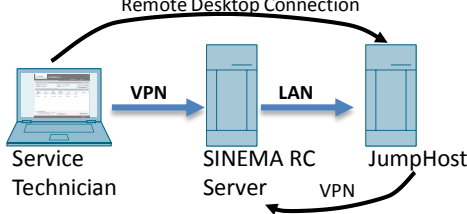
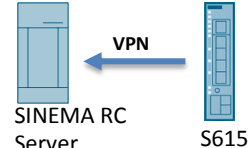
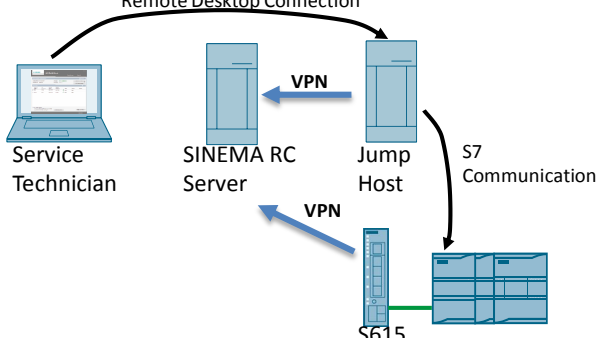
5. Using the remote desktop connection, the service technician starts software on the JumpHost that he needs for remote access to the plant, for example TIA Portal.



Summary

Implementing the task of the application example requires several steps. The following table lists the individual steps and the chapters that explain the associated configuration.

Table 1-2

Step	Brief description	Chapter
1.	<p>The service technician establishes a VPN tunnel to the SINEMA Remote Connect Server. A user account for the service technician is defined in the SINEMA Remote Connect Server.</p> 	Chapter 2.2.4 Chapter 2.4
2.	<p>Using a remote desktop connection, the service technician connects his PC to the JumpHost in the DMZ. The SINEMA Remote Connect Server enables its LAN interface for the service technician.</p> 	Chapter 2.2.2 Chapter 2.5
3.	<p>Using the remote desktop connection, the service technician starts the SINEMA Remote Connect Client on the JumpHost. The SINEMA Remote Connect Client establishes a VPN tunnel to the SINEMA Remote Connect Server.</p> 	Chapter 2.2.4 Chapter 2.5
4.	<p>The SCALANCE S615 automatically establishes a VPN tunnel to the SINEMA Remote Connect Server.</p> 	Chapter 2.2.3 Chapter 2.3
5.	<p>Using the remote desktop connection, the service technician starts software on the JumpHost that he needs for remote access to the plant, for example TIA Portal.</p> 	Chapter 2.5

1.2.4 SINEMA Remote Connect

SINEMA Remote Connect is a management platform for remote networks that centrally manages secure tunnel connections. It allows convenient and secure maintenance of widely distributed plants or machines via remote access. Remote access is possible even if the machines are integrated in third-party networks, for example, in the plants of end customers.

The solution with SINEMA Remote Connect consists of the following parts:

- SINEMA Remote Connect as the VPN server
- Terminal units (VPN client):
 - SCALANCE S615 (with KEY-PLUG)
 - SCALANCE S612, S623, S627
 - SCALANCE M-800 (with KEY-PLUG)
 - SINEMA Remote Connect Client
 - SOFTNET Security Client
 - OpenVPN client

SINEMA Remote Connect Server

SINEMA Remote Connect Server is a server application that provides integrated connection management of distributed networks via the Internet.

The server application coordinates secure connection establishment between users, widely distributed plants and machines.

The SINEMA Remote Connect Server performs the following functions:

- Management and establishment of encrypted connections using OpenVPN and IPSec
- Verification via CA certificate or fingerprint
- User management with rights configuration
- Support of routing and NAT to connect subnets behind the SCALANCE S615
- Provision of secure remote access to lower-level networks for maintenance, control and diagnostic purposes
- Web Based Management (WBM) to configure the server

SCALANCE S615

The SCALANCE S615 is a security module for the protection of devices, automation cells or network segments in Ethernet networks against internal and external threats.

The SCALANCE S615 has the same functions and features as the available SCALANCE M variants. It additionally provides a number of specific LAN functions that allow optimum connection to SINEMA Remote Connect.

Among other things, the SCALANCE S615 is characterized by the following functions:

- Support of VPN for secure authentication of network users, data encryption and data integrity check
 - IPSec VPN tunnel (server and client functionality)
 - OpenVPN for connection to SINEMA Remote Connect (Client function)
- Stateful inspection firewall with filtering of IP-based data traffic and communications protocols
- Support of NAT and NAPT, even in conjunction with IPSec and OpenVPN
- Support of VLAN
- Flexible, reaction-free and protocol-independent protection
- Support of multiple VPN tunnels at a time
- Easiest connection to SINEMA Remote Connect using the auto-configuration interface (can be activated with the KEY-PLUG SINEMA REMOTE CONNECT)
- Establishment of permanent or event-based connections (established by a wake-up SMS text message or a signal at the digital input)

SINEMA Remote Connect Client

SINEMA Remote Connect Client is an OpenVPN client software product for optimum connection to SINEMA Remote Connect.

Among other features, it provides the following functions:

- Support of VPN (OpenVPN) for secure authentication of network users, data encryption and data integrity check
- Easy connection to SINEMA Remote Connect using the auto-configuration interface
- Phone book with all the devices assigned to the user
- Proxy server for communication with networks behind a proxy server infrastructure
- Support of HTTPS and SOCKS proxy servers

1.3 Features of the solution

- User management and connection management via a central server application.
- No direct access to the plant possible due to the implementation of a DMZ.
- Secure, worldwide access to the plant
- Controlled, encrypted data traffic between users, widely distributed plants and machines through a VPN tunnel.
- Verification of the SINEMA Remote Connect Server through the CA certificate.
- Low investment and operating costs for monitoring and controlling remotely connected substations.
- High degree of security for machines and plants through the implementation of the cell protection concept.
- Protocol-independent, IP-based communication
- Easy connection of terminal units (SCALANCE S615) and SINEMA Remote Connect Client using the auto-configuration interface.

2 Configuration and Project Engineering

2.1 Setting up the environment

2.1.1 Required components and IP address overview

Software packages

This application example is based on SINEMA Remote Connect Appliance and requires the SINEMA Remote Connect Server as software. Install this software on a PC without an operating system. Please consider the requirements necessary for the installation. During the installation, you have to enter the server's IP address. Use the IP address from [Table 2-1](#).

The service technician's PC requires the SINEMA Remote Connect Client software. Install this software on your PC.

The JumpHost in the DMZ requires the SINEMA Remote Connect Client software and other software packages for the engineering and remote maintenance of the plant, for example TIA Portal and a web browser. Install the software packages on the JumpHost.

NOTICE

The installation of the SINEMA Remote Connect Server includes its own operating system. If you are using a PC on which an operating system already exists, the hard disk will be formatted and stored data will be lost.

Required devices and components:

To set up the environment, use the following components:

- A PC in the DMZ with "SINEMA Remote Connect Server V1.2" installed on it.
- A PC ("JumpHost") in the DMZ with "SINEMA Remote Connect Client V1.0 SP2" and other engineering tools installed on it, for example TIA Portal and a web browser.
- A service technician PC with "SINEMA Remote Connect Client V1.0 SP2" installed on it.
- A SCALANCE S615.
- A KEY-PLUG SINEMA REMOTE CONNECT.
- DSL access with a dynamic WAN IP address and a DSL router.
- DSL access with a static WAN IP address and a DSL router.
- Two switches.
- A configuration PC with a web browser installed on it.
- The necessary network cables, TP cables (twisted pair) according to the IE FC RJ45 standard for Industrial Ethernet.

Note

You can also use a different Internet access method (e.g., UTMS). The configuration described below explicitly refers only to the components listed in "Required devices and components".

IP addresses

For this application example, the IP addresses are assigned as follows:

Figure 2-1

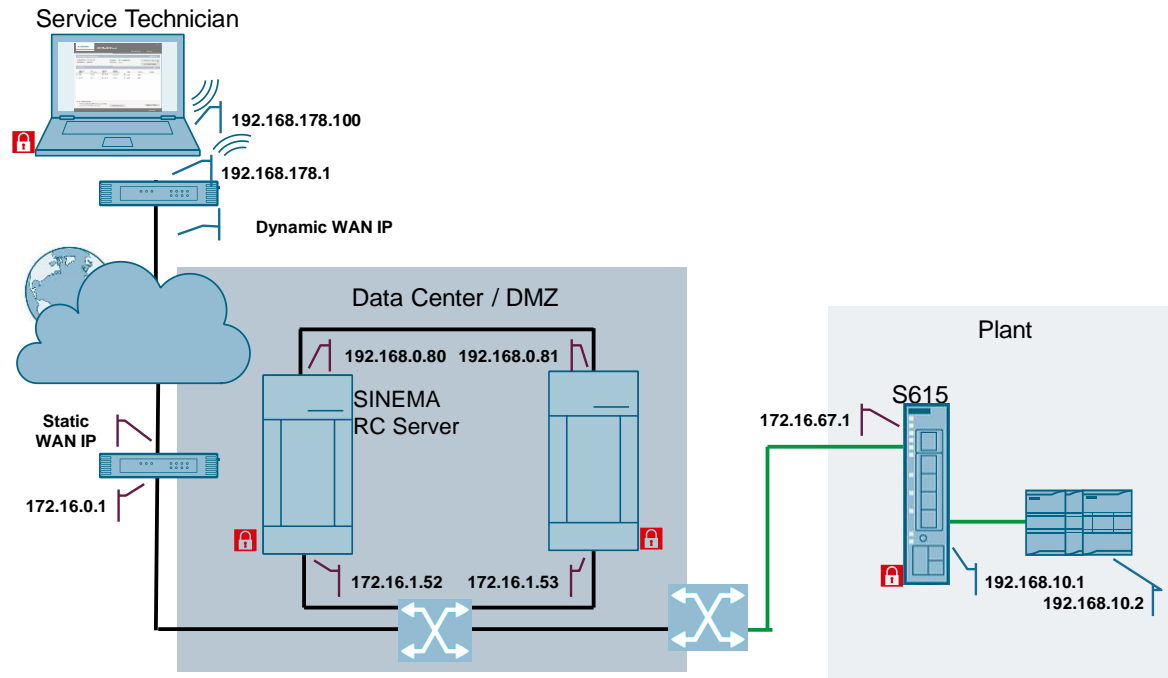


Table 2-1

Component	Port	IP address	Default gateway	Subnet mask
SINEMA Remote Connect Server	LAN port	192.168.0.80	-	255.255.255.0
JumpHost	LAN port	192.168.0.81	192.168.0.80	255.255.255.0
SINEMA Remote Connect Server	WAN port	172.16.1.52	-	255.255.0.0
JumpHost	WAN port	172.16.1.53	-	255.255.0.0
Configuration PC (not shown in the figure)	LAN port	172.16.67.10 192.168.10.10 192.168.1.1	-	255.255.0.0 255.255.255.0 255.255.255.0
Router on the DMZ side	LAN port	172.16.0.1	-	255.255.0.0
Router on the DMZ side	WAN port	Static IP address from the provider	-	Assigned by the provider
Router on the service technician side	WAN port	Dynamic IP address from the provider	-	Assigned by the provider
Router on the service technician side	WLAN	192.168.178.1	-	255.255.255.0
Service technician PC	WLAN	192.168.178.100	192.168.178.1	255.255.255.0
SCALANCE S615	WAN port "vlan2" (P5)	172.16.67.1	172.16.0.1	255.255.0.0
SCALANCE S615	LAN port "vlan1" (P1 to P4)	192.168.10.1	-	255.255.255.0
Programmable controller, for example a PN CPU	LAN port	192.168.10.2	192.168.10.1	255.255.255.0

Note

With the PC, you configure the SINEMA Remote Connect Server and the SCALANCE S615 using Web Based Management. This requires that you assign multiple IP addresses to the PC network adapter. In the advanced TCP/IP settings of the network adapter configuration, you can add more IP addresses.

Setting up the infrastructure

Connect all the components involved in this application example.

Figure 2-2

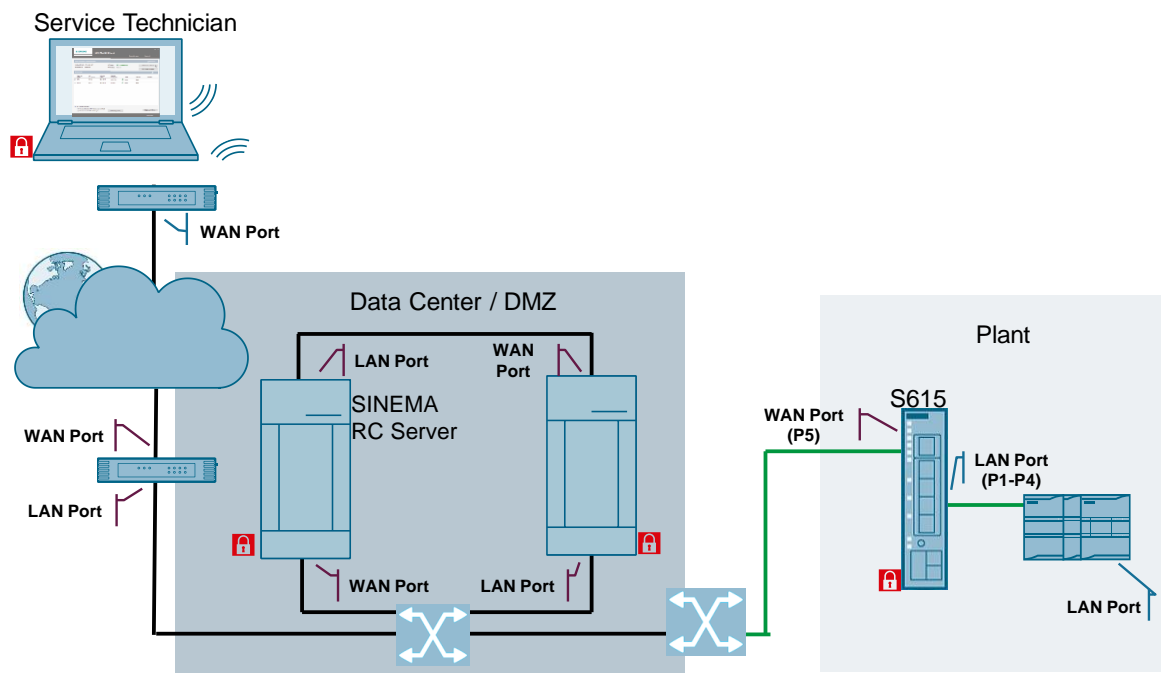


Table 2-2

Component	Local port	Partner	Partner port
SINEMA Remote Connect Server	WAN port	Router in front of the DMZ	LAN port (via switch)
JumpHost	LAN port	Router in front of the DMZ	LAN port (via switch)
SINEMA Remote Connect Server	LAN port	JumpHost	WAN port
Router on the service technician side	WLAN interface	Service technician PC	WLAN interface
SCALANCE S615	WAN port P5	Router in front of the DMZ	LAN port (via switch)
SCALANCE S615	LAN port P1 to P4	Programmable controller	Port of the programmable controller

2.1.2 Router on the service technician side

VPN

If VPN connections are configured and enabled on your router, close them.

WLAN

Using the WLAN router, the service technician's PC (SINEMA Remote Connect Client) is connected to the LAN via the WLAN. Set up the WLAN on the WLAN router.

LAN IP addresses

On the LAN ports, use an IP address as shown in [Table 2-1](#).

2.1.3 Service technician PC

Time

To correctly analyze the SINEMA Remote Connect Client log files in terms of time, for example if the VPN connection cannot be established, it is important that the PC always maintains the current date and time.

Check the time on your PC. If the time displayed is not the current time, change it.

VPN

If other VPN connections are configured and enabled on your PC, close them.

WLAN

On the PC, set up the WLAN according to your router configuration. Use an IP address as shown in [Table 2-1](#).

2.1.4 Router on the DMZ side

Static IP address for the DSL router

The service technician connects his PC to the Internet. For VPN access, he uses the SINEMA Remote Connect Client (VPN client). WAN access of the VPN client to the SINEMA Remote Connect Server (VPN server) is implemented using a static public IP address. Request this IP address from the provider and then store it in the DSL router.

Port forwarding on the DSL router

To allow smooth exchange of the tunnel packets, make sure that PORT forwarding for OpenVPN and https with TCP and UDP (TCP/443, UDP/1194 and TCP/5443) is enabled and that the tunnel packets are forwarded to the SINEMA Remote Connect Server.

Note

These ports can be changed in the SINEMA Remote Connect Server. This means the port numbers are only correct if you keep the default settings. Either only UDP or TCP is used for OpenVPN. Where possible, always prefer UDP as it is faster/performs better than TCP.

2.1.5 JumpHost

For the remote desktop connection, you need a user account on the JumpHost. Set up a new user account and assign the remote desktop connection permission to the user.

2.1.6 SCALANCE S615

Factory default

To make sure that no existing configurations and certificates are stored in the SCALANCE S615, reset the modules to factory default.

KEY-PLUG

The "KEY-PLUG SINEMA REMOTE CONNECT" is required for the SCALANCE S615. The KEY-PLUG enables the connection between the SCALANCE S615 and SINEMA Remote Connect.

Make sure that a valid KEY-PLUG is inserted in the SCALANCE S615.

2.2 Setting up the SINEMA Remote Connect Server

To allow the service technician's PC to access the plant using a remote desktop connection, all terminal units (SINEMA Remote Connect Clients and SCALANCE S615) must log on to the server. The respective VPN tunnel between the terminal unit and the SINEMA Remote Connect Server is established only after successful authentication.

Depending on the configured communication relationships and the security settings, the SINEMA Remote Connect Server interconnects the individual VPN tunnels and thus enables the service technician to access the plant.

To enable access, the following configuration steps are required:

- Make basic settings such as the IP address and the time.
- Define participant groups.
- Implement the SCALANCE S615 as a device.
- Create a user account for the service technician and the JumpHost.

2.2.1 Configuring basic parameters

Opening Web Based Management

Connect the configuration PC to the local network of the SINEMA Remote Connect Server, for example, using the local ports on the switch and connect to the SINEMA Remote Connect Server web user interface. The IP address was defined during the installation.

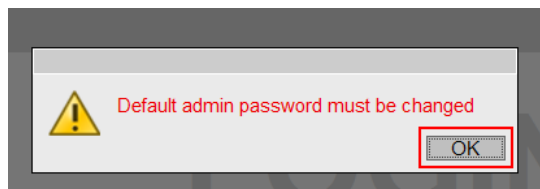
Use the following address to open Web Based Management: "https://172.16.1.52"

Web Based Management login

When you log in for the first time or after setting to factory default, the login data is defined as follows:

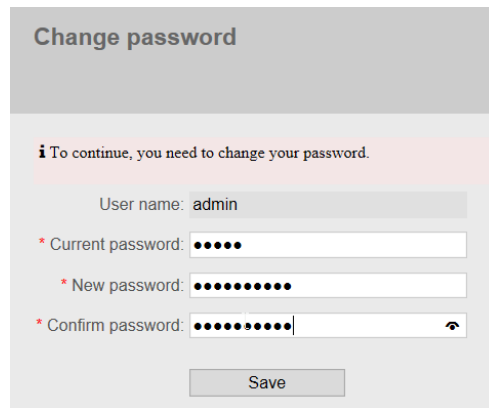
- Name: "admin"
- Password: "admin"

1. Enter the name and password in the appropriate text boxes.
Click the "Login" button.
2. When you log in for the first time or after setting to factory default, you are prompted to change the password.



3. Enter the old and new password. The new password must meet at least the following requirements:
 - Eight characters long
 - One special character
 - Upper/lower case letters

- One number.



4. Click the “Save” button to complete the operation and activate the new password.
5. When you have logged in, the start page appears.

Result

The password for the “admin” user has been changed. In the future, log in with the changed password.

Note

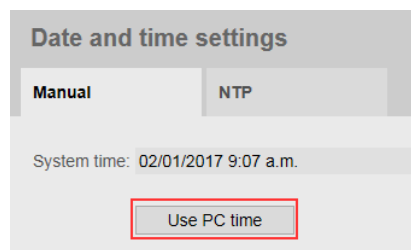
Only the “admin” user type has write access to the configuration in the SINEMA Remote Connect Server.

Setting the time

It is important that the SINEMA Remote Connect Server always maintains the current date and time. The current time is required to correctly perform the following functions:

- Check the time validity of certificates
- Correctly enter the time stamps in the log files

1. In the navigation bar, navigate to “System > Date & time settings”.
2. To apply the PC’s time setting, click the “Use PC time” button.



Result

The SINEMA Remote Connect Server applies the date and time and displays the current values in the "System time" field.

Note

Alternatively, you can have the system time automatically synchronized with an NTP time server to retrieve the exact current time.

Defining the interface parameters

SINEMA Remote Connect has two physically separate network interfaces:

- WAN interface to connect the external network
- LAN interface to connect the internal network

You can configure the network interfaces as follows:

1. In the navigation pane, click "Security > Network" and in the content pane, click the "Interfaces" tab.
2. Select the "WAN" interface. The configuration is displayed.
Check the WAN interface settings.
Check "SINEMA RC is located behind a NAT device" to enter the required external WAN IP address for the router. In "WAN IP address", enter the WAN IP address of the router.
Click "Save" to save the settings.

Logged on as "Admin"

Log off

▼ System

- Overview
- Logfile
- Network configuration
- Date & time settings
- SMS & E-mail
- Licenses
- Update
- Upload Server
- Backup & restore
- Remote connections
- User accounts
- Security
- My account

Network configuration

Interfaces DNS Web server settings

! 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: WAN

MAC address: 00:0e:8c:c5:56:5b

MTU: 1460

IP address: 172.16.1.52

Network mask: 255.255.0.0

Default gateway: 172.16.0.1

☒ SINEMA Remote Connect is located behind a NAT device.

WAN IP address:

Save

Note

Keep the default settings if you want the SINEMA Remote Connect Server to be accessible only from a local network.

3. Select the “LAN” interface. The configuration is displayed.
Check the “Activate the interface” check box to enable the LAN interface. Keep the other default settings.
Click “Save” to save the settings.

2.2.2 Defining participant groups

You can combine users and devices into participant groups. All members of a group belong to a shared VPN tunnel.

The following groups are created for this application example.

- “Station”: SCALANCE S615 and the user account for the JumpHost.
- “ServicePC”: User account for the service technician.

To define the participant groups, proceed as follows:

4. In the navigation pane, click “Remote connections > Participant groups”.
Click “Create”.

- The “New participant group” page opens.
In “Group name”, enter the text “Station” and (optionally) a description. Check the “Members may communicate with each other” check box.
Click “Save”.

New participant group

* Group name:

Description:

☒ Members may communicate with each other.

Network interfaces reachable through the VPN tunnel:

☐ LAN 1

- The “Station” participant group has been created and appears in the content pane.
Click “Create” again.

Logged on as "Admin"
Log off

Participant groups

no filter active

Group name	Members may communicate	Reachable Ethernet interfaces	Number of users	Number of devices	Actions
Station	Yes	No	0	0	

- In “Group name”, enter the text “Service” and (optionally) a description. Enable the “LAN 1” network interface. This enable allows the members of this group to communicate via the internal interface of the SINEMA Remote Connect Server.
Click “Save”

New participant group

Group name:

Description:

☐ Members may communicate with each other.

Network interfaces reachable through the VPN tunnel:

☒ LAN 1

Result

You have created the two participant groups. The two participant groups are displayed in the content pane.

<input type="checkbox"/>	Group name	Members may communicate	Reachable Ethernet interfaces	Number of users	Number of devices	Actions
<input type="checkbox"/>	Service	No	LAN1	0	0	
<input type="checkbox"/>	Station	Yes	No	0	0	

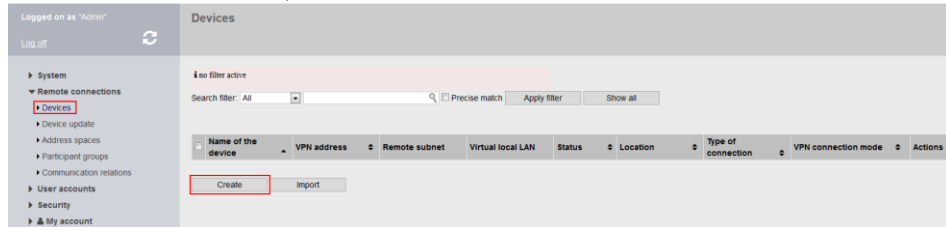
2.2.3 Creating a new device

Create the SCALANCE S615 as a new device in the SINEMA Remote Connect Server.

Integrating the SCALANCE S615

To integrate the SCALANCE, perform the following steps:

1. In the navigation pane, click “Remote connections > Devices”.
To create a new device, click “Create”.



2. The “New device” page opens.
Specify a unique device name for the device, for example “S615_Cell1”.
Click “Next”.

- The “VPN connection mode” tab opens. Apply the default setting, “OpenVPN”, and click “Next”.

The screenshot shows the 'New device' configuration page with the 'VPN connection mode' tab selected. The 'Connection parameters' section has a dropdown for 'VPN connection mode' set to 'OpenVPN'. Below it, 'Request virtual IP address' is checked. The 'OpenVPN connection parameters' section has fields for 'IP address', 'Port', and 'Protocol' (set to 'tcp'). At the bottom, there is a table with columns 'IP address of the connection', 'Connection port', 'IP protocol', and 'Actions'. The 'Next' button is highlighted.

- The “Network settings” tab opens. Check the “Connect local subnets” check box and configure the parameters. Enter the network ID 192.168.10.0 along with the subnet mask 255.255.255.0. If “Device is a network gateway” is not checked, check this check box. Select “Add” to add the network. Click “Next”.

The screenshot shows the 'New device' configuration page with the 'Network settings' tab selected. The 'Connection parameters' section has a checkbox for 'Connected local subnets' checked. Below it, 'Local LAN IP address' is set to '192.168.10.0' and 'Network mask' is set to '255.255.255.0'. The 'Device is a network gateway' checkbox is also checked. An 'Add' button is highlighted. Below this is a table with columns 'Local subnet', 'Network gateway', and 'Actions'. The table contains one entry: '192.168.10.0/24' for the local subnet, 'Yes' for the network gateway, and a delete icon in the actions column. The 'Next' button is highlighted.

- The “Group memberships” tab is displayed. Check the “Station” participant group. Click “Next”.

Group members /

Device	VPN connection mode	Network settings	Group memberships	Password	Device overview
<input type="checkbox"/> Service <input checked="" type="checkbox"/> Station					
<div>Back</div> <div>Next</div>					

- The “Password” tab is displayed. Define the password for access. The password must be a combination of upper and lower case letters, digits and special characters. You will need this password later when configuring the SCALANCE S615 (see [Chapter 2.3](#)). Click “Next”.

New device

Device	VPN connection mode	Network settings	Group memberships	Password	Device overview
Name of the device: S615					
<div> * New password: </div> <div> * Confirm password: </div>					
<div>Back</div> <div>Next</div>					

- The “Device overview” tab is displayed. This tab summarizes all the information about the SCALANCE S615. At the end of the summary, click “Finish”.

Devices / S615

Device	VPN connection mode	Network settings	Group memberships	Password	Device overview								
Device information:													
IP address of the VPN server: 172.16.1.52, 192.168.0.80													
IP address of the Web server: 172.16.1.52, 192.168.0.80													
Web server port: 443													
Fingerprint: 9C:BD:B7:41:20:4D:6C:73:A4:36:25:03:28:80:6B:C9:15:0C:8A:AE													
Name of the device: S615													
<table border="1"> <thead> <tr> <th>Local LAN IP address:</th> <th>Local subnet</th> <th>Network gateway</th> </tr> </thead> <tbody> <tr> <td>192.168.10.0/24</td> <td></td> <td>Yes</td> </tr> </tbody> </table>						Local LAN IP address:	Local subnet	Network gateway	192.168.10.0/24		Yes		
Local LAN IP address:	Local subnet	Network gateway											
192.168.10.0/24		Yes											
<table border="1"> <thead> <tr> <th>Virtual local LAN IP address:</th> <th>Virtual local LAN</th> <th>Local subnet</th> <th>Network gateway</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>						Virtual local LAN IP address:	Virtual local LAN	Local subnet	Network gateway				
Virtual local LAN IP address:	Virtual local LAN	Local subnet	Network gateway										

Result

The SCALANCE S615 is stored in the SINEMA Remote Connect Server as a new device.

<input type="checkbox"/>	Name of the device	VPN address	Remote subnet	Virtual local LAN	Status	Location	Type of connection	VPN connection mode	Actions
<input type="checkbox"/>	S615	None	192.168.10.0/24	None	offline	Cell 1	Permanent	OpenVPN	    

Determining the device ID

The device ID and the fingerprint are pieces of information the SCALANCE S615 uses for authentication on the SINEMA Remote Connect Server during connection establishment. You need these two parameters for the SINEMA Remote Connect configuration in the SCALANCE S615 (see [Chapter 2.3](#)).

To view the device ID and the fingerprint, proceed as follows:

1. In the navigation pane, click “Remote connections > Devices”. The SCALANCE S615 is displayed. In the “Actions” column, click the first icon to open the device information for this SCALANCE.

<input type="checkbox"/>	Name of the device	VPN address	Remote subnet	Virtual local LAN	Status	Location	Type of connection	VPN connection mode	Actions
<input type="checkbox"/>	S615	None	192.168.10.0/24	None	offline	Cell 1	Permanent	OpenVPN	    

2. The “Device information” is displayed. Note down the values displayed in “Device ID” and “Fingerprint”.

Device information:


Device ID: 8

IP address of the VPN server: 80.81.10.24
172.16.1.52
192.168.0.80

IP address of the Web server: 80.81.10.24
172.16.1.52
192.168.0.80

Web server port: 443

Fingerprint: 9C:BD:B7:41:20:4D:6C:73:A4:36:25:03:28:80:6B:C9:15:0C:8A:AE

Export CA 

Name of the device: S615

Local LAN IP address:	Local subnet	Network gateway
	192.168.10.0/24	Yes

3. To avoid mistakes when noting down the fingerprint, you can copy the fingerprint and save it to a text file. To do this, click the icon next to the field. This selects the value in "Fingerprint". Copy the selected value to a text file and save the file to your local directory. Select "Exit dialog" to close the dialog.

Device information:

Device ID: 8

IP address of the VPN server

80.81.10.24

172.16.1.52

192.168.0.80

IP address of the Web server

80.81.10.24

172.16.1.52

192.168.0.80


Web server port

443

Fingerprint:

9C:BD:B7:41:20:4D:6C:73:A4:36:25:03:28:80:6B:C9:15:0C:8A:AE

Export CA



Name of the device:

S615

Local LAN IP address:

Local subnet	Network gateway
192.168.10.0/24	Yes

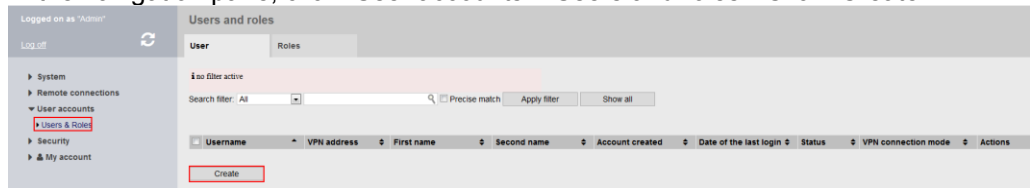
2.2.4 Creating new user accounts

Make the service technician and the JumpHost known to the SINEMA Remote Connect Server as new users. To do this, both user accounts need a user name and password.

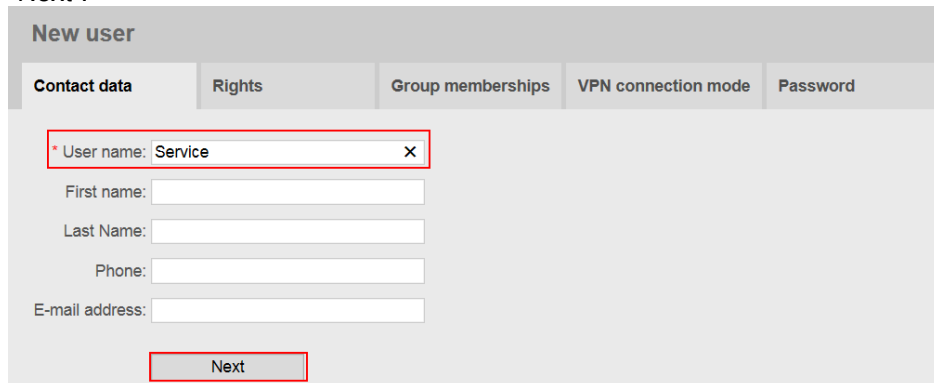
Integrating the service technician as a user

To create the service technician as a new user, proceed as follows:

1. In the navigation pane, click “User accounts > Users and roles”. Click “Create”.



2. The “New user” page opens. Enter the “User name”, e.g., Service and click “Next”.



3. The “Rights” tab is displayed.
You have the following option to assign rights to the user:
 - Rights assignment through role assignment
Select an existing role. The associated rights are automatically assigned to the user. For additional rights, check the check boxes.
 - Rights assignment without role assignment
If you have not selected a role, check the check boxes to assign the appropriate rights to the user.

At this point, select your desired rights.
Click “Next”.

The screenshot shows the 'New user' configuration window with the 'Rights' tab selected. The 'Role assignment' section has a 'Select role:' dropdown menu. The 'Additional rights' section contains a list of checkboxes for various permissions: Manage address spaces, Create backup copies, Restore the system, Force comment, Manage firmware updates, Manage devices, Manage remote connections, Edit system parameters, Certificate management, and Manage users and roles. At the bottom, there are 'Back' and 'Next' buttons, with the 'Next' button highlighted by a red rectangle. A footnote at the bottom states: '*The marked rights are preset by the selected role.'

4. The “Group memberships” tab is displayed. Assign the new user to the “Service” participant group.
Click “Next”.

The screenshot shows the 'Group members /' configuration window with the 'Group memberships' tab selected. The 'Service' checkbox is checked and highlighted by a red rectangle. The 'Station' checkbox is unchecked. At the bottom, there are 'Back' and 'Next' buttons, with the 'Next' button highlighted by a red rectangle.

5. The “VPN connection mode” tab opens.
Apply the default setting, “OpenVPN”, and click “Next”.

The screenshot shows the 'New user' configuration interface with the 'VPN connection mode' tab selected. The 'Contact data' tab is also visible. The 'VPN connection mode' dropdown is set to 'OpenVPN'. Below it, the 'Request virtual IP address' checkbox is checked, and the 'Use fixed IP address' checkbox is unchecked. The 'Fixed IP address' field is empty. The 'OpenVPN connection parameters' section includes fields for 'IP address', 'Port', and 'Protocol' (set to 'tcp'), with an 'Add' button. Below this is a table with columns: 'IP address of the connection', 'Connection port', 'IP protocol', and 'Actions'. At the bottom, there are 'Back' and 'Next' buttons.

6. The “Password” tab is displayed. In this tab, define the password for the new user. The password must meet at least the following requirements:
- Eight characters long
 - One special character
 - Upper/lower case letters
 - One number

You will need this password later when configuring the SINEMA Remote Connect Client (see [Chapter 2.4](#)).
Select “Finish” to complete the user creation process.

Note:




The new user can change the assigned password later.

The screenshot shows the 'New user' configuration interface with the 'Password' tab selected. The 'User name' field is set to 'Service'. The 'New password' and 'Confirm password' fields are both filled with dots. At the bottom, there are 'Back' and 'Finish' buttons.

Integrating the JumpHost as a user

To create the JumpHost as a new user, proceed as follows:

1. In the navigation pane, click “User accounts > Users and roles”. Click “Create”.

<input type="checkbox"/>	Username	VPN address	First name	Second name	Account created	Date of the last login	Status	VPN connection mode	Actions
<input type="checkbox"/>	Service	None			March 29, 2017, 10:43 a.m.	March 29, 2017, 10:43 a.m.	offline	OpenVPN	  
<div>CreateCopyDelete</div>									

2. The “New user” page opens. Enter the “User name”, e.g., JumpHost and click “Next”.

New user

Contact dataRightsGroup membershipsVPN connection modePassword

* User name: JumpHost

First name:

Last Name:

Phone:

E-mail address:

Next

3. The “Rights” tab is displayed.
You have the following option to assign rights to the user:
 - Rights assignment through role assignment
Select an existing role. The associated rights are automatically assigned to the user. For additional rights, check the check boxes.
 - Rights assignment without role assignment
If you have not selected a role, check the check boxes to assign the appropriate rights to the user.

At this point, select your desired rights.
Click “Next”.

The screenshot shows the 'New user' configuration window with the 'Rights' tab selected. The 'Role assignment' section has a 'Select role:' dropdown menu. The 'Additional rights' section lists ten checkboxes: 'Manage address spaces', 'Create backup copies', 'Restore the system', 'Force comment', 'Manage firmware updates', 'Manage devices', 'Manage remote connections', 'Edit system parameters', 'Certificate management', and 'Manage users and roles'. The 'Next' button is highlighted with a red rectangle. A footer note states: '*The marked rights are preset by the selected role.'

4. The “Group memberships” tab is displayed. Assign the new user to the “Station” participant group.
Click “Next”.

The screenshot shows the 'Group members /' configuration window with the 'Group memberships' tab selected. The 'Service' checkbox is unchecked, and the 'Station' checkbox is checked and highlighted with a red rectangle. The 'Next' button is also highlighted with a red rectangle.

5. The “VPN connection mode” tab opens.
Apply the default setting, “OpenVPN”, and click “Next”.

The screenshot shows the 'New user' configuration interface with the 'VPN connection mode' tab selected. The 'Contact data' tab is also visible. The 'VPN connection mode' dropdown is set to 'OpenVPN'. Below it, the 'Request virtual IP address' checkbox is checked, and the 'Use fixed IP address' checkbox is unchecked. The 'Fixed IP address' field is empty. The 'OpenVPN connection parameters' section includes fields for 'IP address', 'Port', and 'Protocol' (set to 'tcp'), with an 'Add' button. Below this is a table with columns: 'IP address of the connection', 'Connection port', 'IP protocol', and 'Actions'. At the bottom, there are 'Back' and 'Next' buttons.

IP address of the connection	Connection port	IP protocol	Actions
------------------------------	-----------------	-------------	---------

6. The “Change password” tab is displayed. In this tab, define the password for the new user. The password must meet at least the following requirements:
- Eight characters long
 - One special character
 - Upper/lower case letters
 - One number.

You will need this password later when configuring the SINEMA Remote Connect Client (see [Chapter 2.5](#)).
Select “Finish” to complete the user creation process.









Note:

The new user can change the assigned password later.

The screenshot shows the 'New user' configuration interface with the 'Password' tab selected. The 'User name' field is filled with 'JumpHost'. The 'New password' and 'Confirm password' fields are both filled with eight dots. At the bottom, there are 'Back' and 'Finish' buttons.

Result

You have created the service technician and the JumpHost in SINEMA Remote Connect Server with their own user accounts.

<input type="checkbox"/>	Username	VPN address	First name	Second name	Account created	Date of the last login	Status	VPN connection mode	Actions
<input type="checkbox"/>	JumpHost	None			March 29, 2017, 10:46 a.m.	March 29, 2017, 10:46 a.m.	offline	OpenVPN	   
<input type="checkbox"/>	Service	None			March 29, 2017, 10:43 a.m.	March 29, 2017, 10:43 a.m.	offline	OpenVPN	   

2.3 Setting up the remote connection on the S615

To establish a VPN tunnel between the SCALANCE S615 and the SINEMA Remote Connect Server, perform the following steps:

- First commissioning of the SCALANCE to set the basic parameters, for example IP address and time.
- Configure the VPN connection.

Opening Web Based Management

Connect the configuration PC to a LAN port of the SCALANCE S615 (port 1 to port 4).

By factory default, the IP address of the device is 192.168.1.1/24.

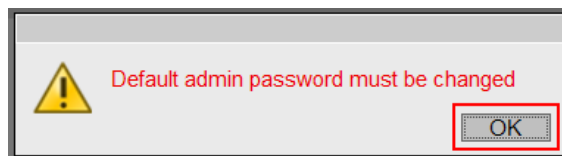
Use the following address to open Web Based Management: "http://192.168.1.1"

Web Based Management login

When you log in for the first time or after setting to factory default, the login data is defined as follows:

- Name: "admin"
- Password: "admin"

1. Enter the name and password in the appropriate text boxes.
Click the "Login" button.
2. When you log in for the first time or after setting to factory default, you are prompted to change the password.



3. Enter the old and new password. In "Password Confirmation", repeat the password to confirm it. Both entries must match.

 A screenshot of the "Local Passwords" configuration page. The page has a grey header with the title "Local Passwords". Below the header, there are several input fields: "Current Admin Password" (masked with dots), "Username" (with a dropdown menu showing "admin"), "Password Policy" (set to "high"), "New Password" (masked with dots), and "Password Confirmation" (masked with dots). At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

4. Click the "Set Values" button to complete the operation and activate the new password.
5. When you have logged in, the start page appears.

Result

The password for the “admin” user has been changed. In the future, log in with the changed password.

WAN Basic Wizard

To set basic WAN parameters such as the IP address and the time, firmware version 4.2 or higher provides a wizard. The wizard starts automatically when you first log in.

1. The first step prompts you to set the IP addresses.
The SCALANCE S615 features five ports that have the following factory default settings:

- Port 1 to port 4: vlan 1
For access from the local network (LAN) to the device.
- Port 5: vlan 2
For access from the external network (WAN) to the device.

Enter the IP address for “Internal vlan1” as shown in [Table 2-1](#). Uncheck “DHCP” and enter the IP address for “External (vlan2)” as shown in [Table 2-1](#). Click “Next”.

WAN Basic Wizard: IP Settings

IP	Device	Time	DDNS	SINEMA RC	Summary
----	--------	------	------	-----------	---------

Enter the IP address and the subnet mask via which the management is accessible. If the device is intended for communication with devices (diagnostics stations, e-mail servers etc.) in another subnet, also enter the IP address of the default gateway.

Internal (vlan1)

IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0

External (vlan2)

☐ DHCP
IP Address: 172.16.67.1
Subnet Mask: 255.255.0.0
Gateway: 172.16.0.1

Abort Next

2. In order to identify the device, it is recommended to define the following SNMP parameters:

- Name
- Location
- Contact

If necessary, enter a name in “System Name”, a location in “System Location” and a contact in “System Contact”.
Click “Next”.

WAN Basic Wizard: Device Settings

IP | Device | Time | DDNS | SINEMA RC | Summary

To allow better identification of the device, you can specify general device information. Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application. You also can enter the contact person responsible for the device and the identifier for the location at which the device is installed, for example the room number.

System Name: SCALANCE S615
System Location: Cell 1
System Contact: SIEMENS

Previous Abort Next

3. It is important that the SCALANCE always maintains the current date and time.
The current time is required to perform the following functions:

- Check the time validity of certificates
- Correctly enter the time stamps in the log files

To set the current time, you have the following options:

- Set the time manually
- Apply the PC time
- Synchronize the time automatically using an NTP time server

In the following screenshot, the PC date and time are applied.
Click “Next”.

WAN Basic Wizard: Time Settings

IP | Device | Time | DDNS | SINEMA RC | Summary

Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. The WAN Basic Wizard is using NTP for the time server. If you want to use another method, configure these method after completing the WAN Basic Wizard.

☒ Time Manually
System Time: 03/29/2017 10:10:21
Use PC Time

☐ NTP Client
Time Zone: +00:00

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval
<input type="checkbox"/>	1	0.0.0.0	123	64

Previous Abort Next

4. The next step allows you to configure the DynDNS service. If you are not using DynDNS, click “Next” to skip this step.

WAN Basic Wizard: DDNS Settings

IP	Device	Time	DDNS	SINEMA RC	Summary
<p>DDNS stands for 'dynamic domain name system'. If you log the device on to a DDNS service, the device can be reached from the external network under a hostname, e.g. 'example.no-ip.com'. Here you enter the hostname that you have agreed with your DDNS provider for the device and the login data (User name, Password) for the DDNS server. To use the required Service, select the check box 'Enabled'.</p>					
Service	Enabled	Host	User name	Password	Password confirmation
No-IP	<input type="checkbox"/>				
DynDNS	<input type="checkbox"/>				

Previous Abort **Next**

5. The use of a valid KEY-PLUG activates the auto-configuration interface and enables easy connection configuration to the SINEMA Remote Connect Server.

The next step is to configure the parameters for the connection to the SINEMA Remote Connect Server:

- In “SINEMA RC Address”, enter the IP address of the SINEMA Remote Connect Server.
- In “Fingerprint”, enter the fingerprint assigned to the SCALANCE S615 by the SINEMA Remote Connect Server during the configuration. To avoid mistakes when entering, use the text file and copy the string directly from the text file to the input box.
- In “Device ID”, enter the “device ID” value assigned to the SCALANCE S615 in the SINEMA Remote Connect Server (see [Chapter 2.1.1](#)).
- In “Device Password”, enter the password you have configured for access (see [Chapter 2.1.1](#)).

WAN Basic Wizard: SINEMA Remote Connect

IP	Device	Time	DDNS	SINEMA RC	Summary
----	--------	------	------	-----------	---------

Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

☐ Enable SINEMA RC

Server Settings

SINEMA RC Address: 172.16.1.52
SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint
Fingerprint: 3:28:80:6B:C9:15:0C:8A:AE
CA Certificate: -

Device Credentials

Device ID: 8
Device Password:

Optional Settings

☒ Auto Firewall/NAT Rules

Type of connection: Auto
Use Proxy: -
Autoenrollment Interval [min]: 60

6. Check the "Enable SINEMA RC" check box.
Click "Next".

WAN Basic Wizard: SINEMA Remote Connect

IP	Device	Time	DDNS	SINEMA RC	Summary
----	--------	------	------	-----------	---------

Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

☒ Enable SINEMA RC

Server Settings

SINEMA RC Address: 172.16.1.52
SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint
Fingerprint: 3:28:80:6B:C9:15:0C:8A:AE
CA Certificate: -

Device Credentials

Device ID: 8
Device Password:

Optional Settings

☒ Auto Firewall/NAT Rules

Type of connection: Auto
Use Proxy: -
Autoenrollment Interval [min]: 60

Previous Abort Next

- At the end, the wizard provides you with a summary of the settings made. Select "Set Values" to complete the wizard.

WAN Basic Wizard: Summary

IP	Device	Time	DDNS	SINEMA RC	Summary												
<p>Internal (vlan1)</p> <p>IP Address: 192.168.10.1</p> <p>Subnet Mask: 255.255.255.0</p>																	
<p>External (vlan2)</p> <p>IP Address: 172.16.67.1</p> <p>Subnet Mask: 255.255.0.0</p> <p>DHCP: disabled</p> <p>Gateway: 172.16.0.1</p>																	
<p>System Name: S615</p> <p>System Location: Cell 1</p> <p>System Contact: SIEMENS</p>																	
<p>Time Manually: enabled</p> <p>System Time: 03/29/2017 11:00:11</p> <p>NTP Client: disabled</p> <p>Time Zone: +00:00</p>																	
<table border="1"> <thead> <tr> <th>NTP Server Index</th> <th>NTP Server Address</th> <th>NTP Server Port</th> <th>Poll Interval</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0.0.0.0</td> <td>123</td> <td>64</td> </tr> </tbody> </table>						NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	1	0.0.0.0	123	64				
NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval														
1	0.0.0.0	123	64														
<table border="1"> <thead> <tr> <th>Service</th> <th>Enabled</th> <th>Host</th> <th>User name</th> </tr> </thead> <tbody> <tr> <td>No-IP</td> <td>disabled</td> <td></td> <td></td> </tr> <tr> <td>DynDNS</td> <td>disabled</td> <td></td> <td></td> </tr> </tbody> </table>						Service	Enabled	Host	User name	No-IP	disabled			DynDNS	disabled		
Service	Enabled	Host	User name														
No-IP	disabled																
DynDNS	disabled																
<p>SINEMA RC: enabled</p>																	
<p>Click the 'Set Values' button to apply the changes!</p>																	
<p>Previous Abort Set Values</p>																	

Result

The device establishes an OpenVPN tunnel to the SINEMA Remote Connect Server. In WBM, "Information > SINEMA RC" allows you to check whether the connection has been established.

Welcome admin [Logout](#)

SINEMA Remote Connect (SINEMA RC) Information

Status: established

Remote Address: 172.16.1.52

Tunnel Interface Address: 10.8.1.12

Connected Local Subnet(s): 192.168.10.0/24

Connected Remote Subnet(s): 10.8.1.0/24
10.8.0.0/24
172.32.0.0/16

Fingerprint: 9C:BD:B7:41:20:4D:6C:73:A4:36:25:03:28:80:6B:C9:15:0C:8A:AE

[Refresh](#)

SINEMA RC

2.4 Setting up the remote connection on the service technician side

Due to the auto-configuration interface, it is not required to explicitly configure the remote connection in the SINEMA Remote Connect Client.

You only have to transfer the user logon data and the server's WAN IP address to the software.

When the user has logged on, the SINEMA Remote Connect Client downloads the OpenVPN file from the SINEMA Remote Connect Server.

This file contains the parameters that are required for the VPN connection to the SINEMA Remote Connect Server.

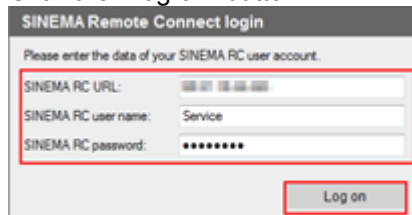
Then the SINEMA Remote Connect Client uses these parameters to establish the VPN connection.

To establish the remote connection, proceed as follows:

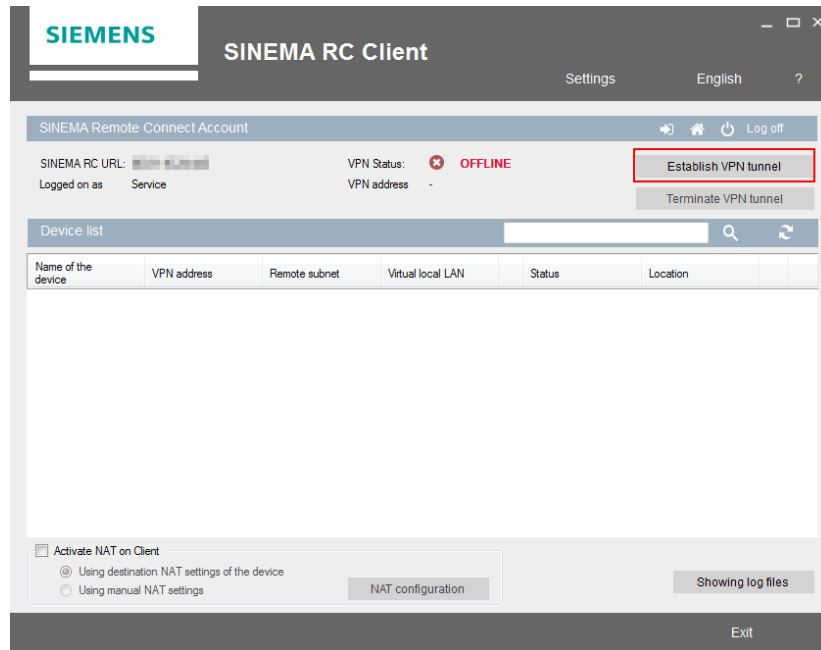
1. On the PC, double-click the desktop icon to open the "SINEMA Remote Connect Client". The client starts.
2. In "SINEMA RC URL", enter the WAN IP address of the SINEMA Remote Connect Server.
In "SINEMA RC user name", enter the text "Service".
In "SINEMA RC Password", enter the password defined for this user.

This logon data is the data defined when creating the user account for the service technician in the SINEMA Remote Connect Server (see [Chapter 2.2.4](#)).

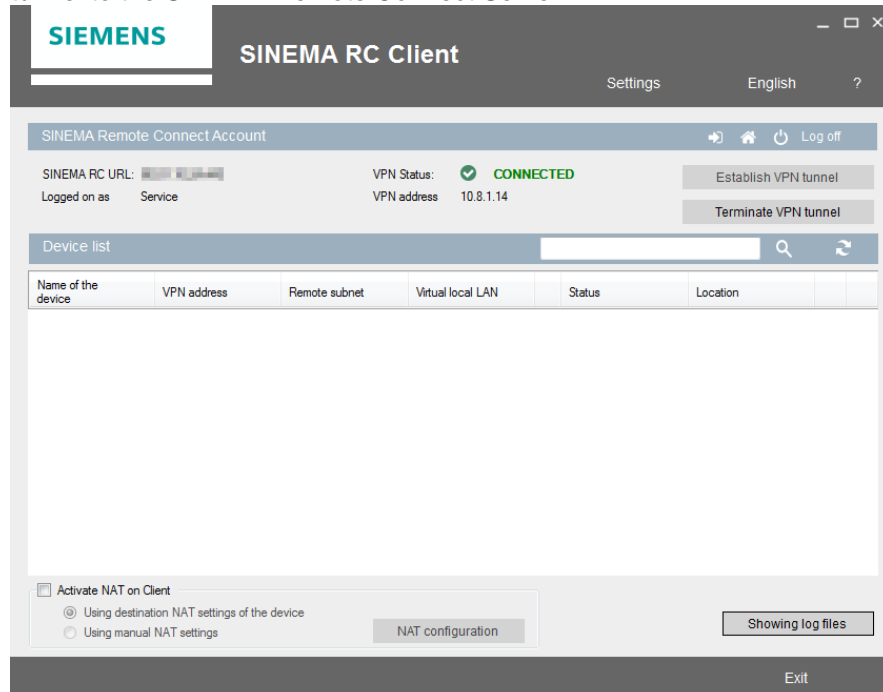
Click the "Log on" button.



3. After logon, the start page is displayed.
The SINEMA Remote Connect Client has automatically loaded the configuration profile of the logged in user from the SINEMA Remote Connect Server.
The “Device list” displays all devices with which the user has a communication relationship.
Click the “Establish VPN tunnel” button to initialize an OpenVPN tunnel to the SINEMA Remote Connect Server.



4. The “SINEMA Remote Connect Client” software establishes an OpenVPN tunnel to the SINEMA Remote Connect Server.



2.5 Establishing the remote desktop connection

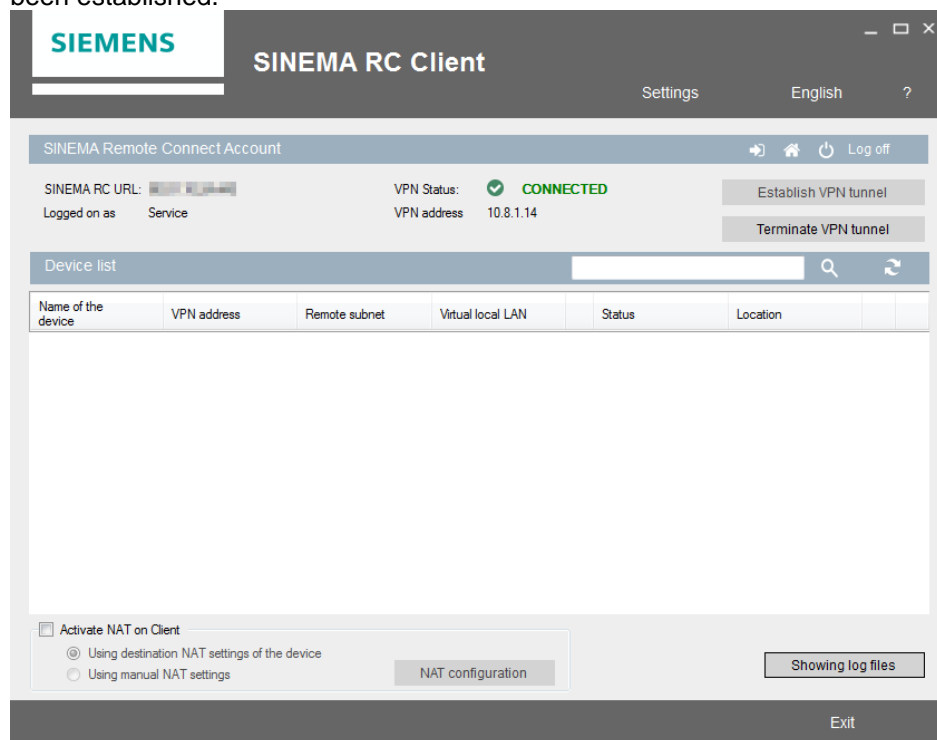
In the configuration of the “Service” participant group, you have enabled the LAN interface of the SINEMA Remote Connect Server (see [Chapter 2.2.2](#)). With this setting, the service technician as a member of this group can communicate with the internal network of the SINEMA Remote Connect Server. The enable of the internal interface is important for the remote desktop connection to the JumpHost.

Using the remote desktop connection, the service technician can perform the following functions on the JumpHost:

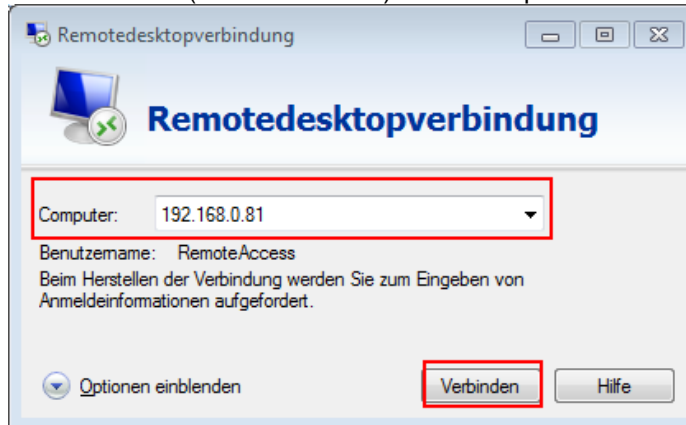
- Start SINEMA Remote Connect Client. Then the SINEMA Remote Connect Client establishes a VPN tunnel to the SINEMA Remote Connect Server.
- Start TIA Portal and configure the devices in the plant.

To start the remote desktop connection from the service technician’s PC to the JumpHost, proceed as follows:

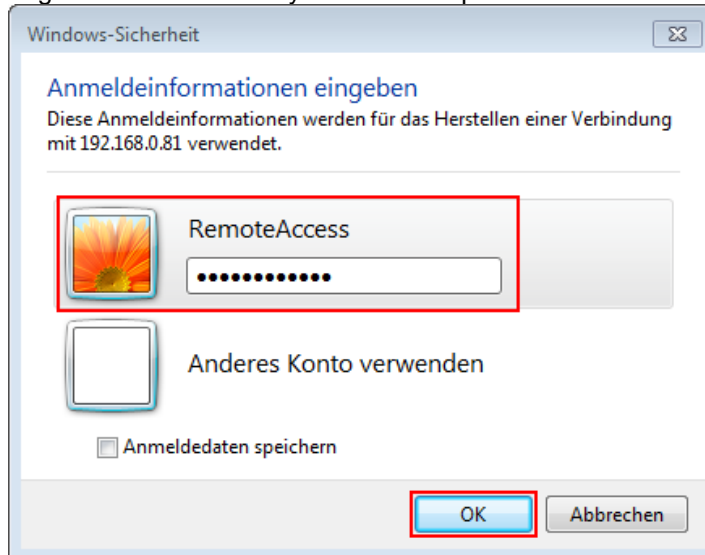
1. On the service technician’s PC, open the SINEMA Remote Connect Client to check whether the VPN tunnel to the SINEMA Remote Connect Server has been established.



2. On the service technician's PC, open the remote desktop connection and enter the IP address (LAN IP address) of the JumpHost. Click "Connect".



3. Log in with the account you have set up for the remote desktop connection.



Result:

The JumpHost's desktop is displayed.

4. Double-click the desktop icon to open the "SINEMA Remote Connect Client" using the remote desktop connection on the JumpHost. The client starts.

5. In “SINEMA RC URL”, enter the LAN IP address of the SINEMA Remote Connect Server.

Note:

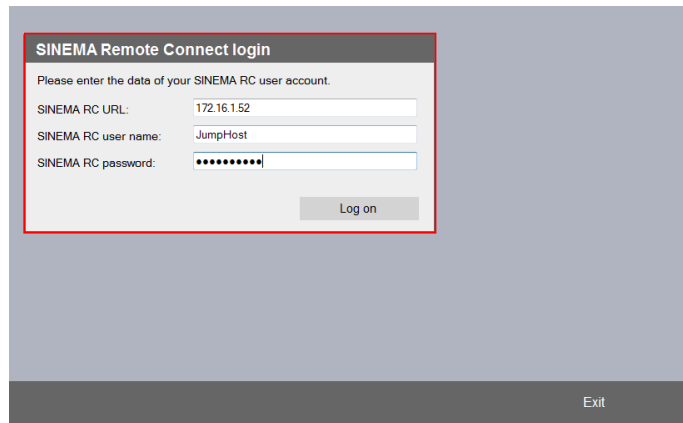
Alternatively, you can enter the DNS name or URL of the SINEMA Remote Connect Server.

In “SINEMA RC user name”, enter the text “JumpHost”.

In “SINEMA RC Password”, enter the password defined for this user.

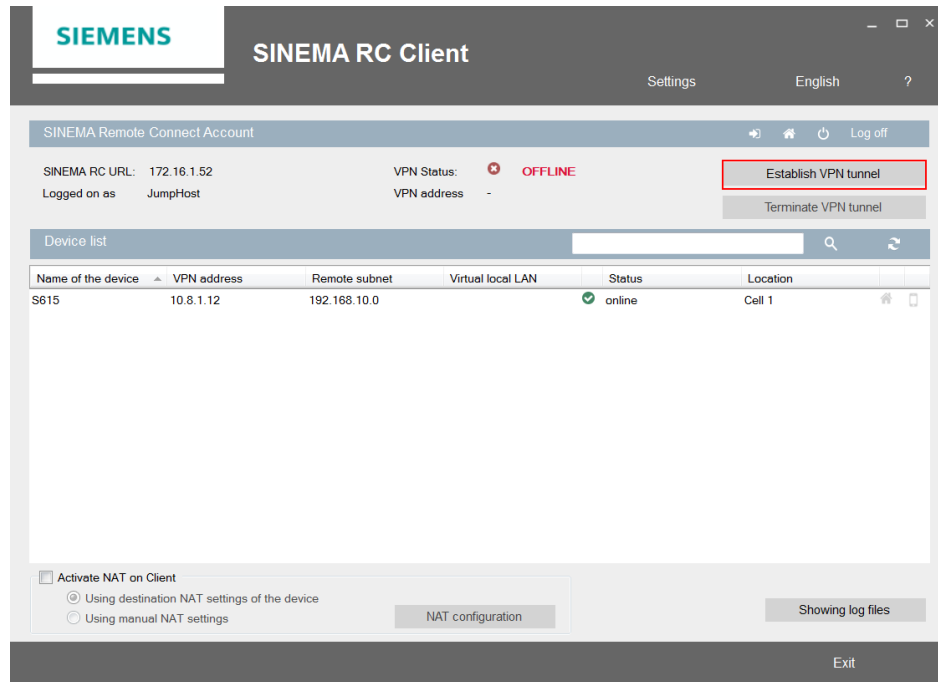
This logon data is the data defined when creating the user account for the JumpHost in the SINEMA Remote Connect Server (see [Chapter 2.2.4](#)).

Click the “Log on” button.

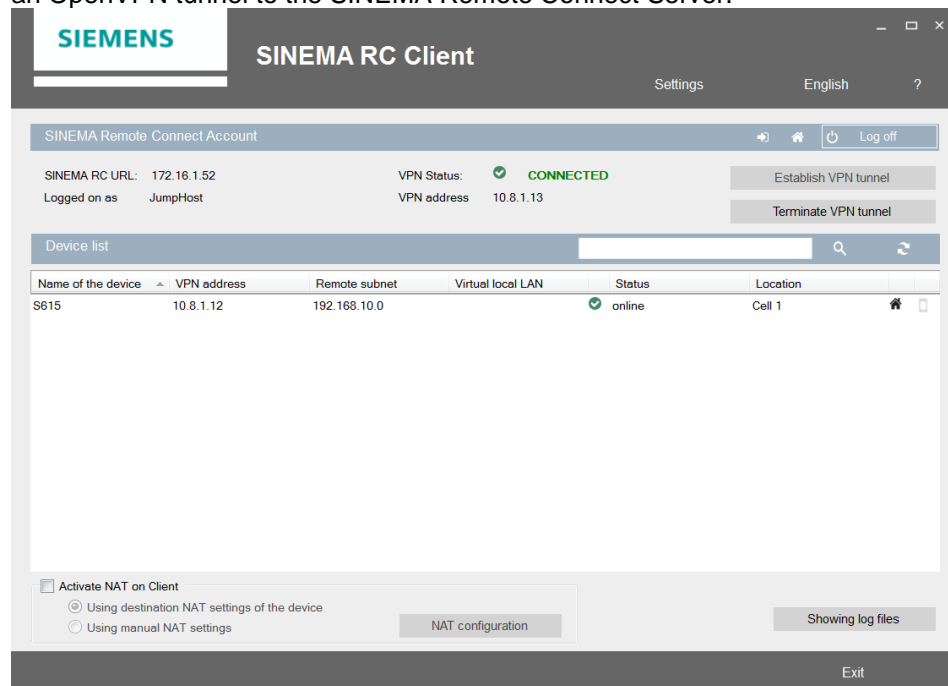


The screenshot shows a login window titled "SINEMA Remote Connect login". Inside the window, there is a prompt: "Please enter the data of your SINEMA RC user account." Below this prompt are three input fields: "SINEMA RC URL:" with the value "172.16.1.52", "SINEMA RC user name:" with the value "JumpHost", and "SINEMA RC password:" with a masked password represented by dots. To the right of the password field is a "Log on" button. The window has a red border and is set against a light blue background. At the bottom right of the window, there is an "Exit" button.

6. After logon, the start page is displayed.
The SINEMA Remote Connect Client has automatically loaded the configuration profile of the logged in user from the SINEMA Remote Connect Server.
The “Device list” displays all devices with which the user has a communication relationship.
Click the “Establish VPN tunnel” button to initialize an OpenVPN tunnel to the SINEMA Remote Connect Server.



7. The “SINEMA Remote Connect Client” software on the JumpHost establishes an OpenVPN tunnel to the SINEMA Remote Connect Server.



3 Testing the Tunnel Function

Chapter 2 completes the commissioning of the configuration.

The following VPN tunnels for secure communication with the SINEMA Remote Connect Server have been established:

- VPN tunnel with the “service technician” participant
- VPN tunnel with the SCALANCE S615 and SINEMA Remote Connect Client participants on the JumpHost.

Communication groups

The service technician is a member of the “Service” group. When configuring the communication groups for the “Service” group, you have enabled the internal interface of the SINEMA Remote Connect Server. With this setting, the service technician can now access the internal network of the SINEMA Remote Connect Server and control the JumpHost using a remote desktop connection.

The SCALANCE S615 and the JumpHost are members of the “Station” group. When configuring the communication groups for the “Station” group, you have allowed communication between the members of the “Station” group. The JumpHost and the devices behind the SCALANCE S615 can communicate with each other.

This allows the service technician to operate and monitor the plant indirectly via the JumpHost.

Testing access

To test the service technician’s indirect access to the plant, proceed as follows:

1. On the service technician’s PC, start a remote desktop connection to the JumpHost.
2. On the JumpHost, open, for example, a web browser to open the internal web page of a PROFINET CPU in the LAN of the SCALANCE S615.
3. In the address bar, enter the IP address of the PROFINET CPU. The programmable controller in the plant can be accessed using the IP address “192.168.10.2”.

4 Appendix

4.1 Service and Support

Industry Online Support

Do you have any questions or do you need support?

With Industry Online Support, our complete service and support know-how and services are available to you 24/7.

Industry Online Support is the place to go to for information about our products, solutions and services.

Product Information, Manuals, Downloads, FAQs and Application Examples – all the information can be accessed with just a few clicks:

<https://support.industry.siemens.com/> .

Technical Support

Siemens Industry's Technical Support offers you fast and competent support for any technical queries you may have, including numerous tailor-made offerings ranging from basic support to custom support contracts.

You can use the web form below to send queries to Technical Support:

www.siemens.com/industry/supportrequest.

Service offer

Our service offer includes the following services:

- Product Training
- Plant Data Services
- Spare Part Services
- Repair Services
- Field & Maintenance Services
- Retrofit & Modernization Services
- Service Programs & Agreements

For detailed information about our service offer, please refer to the Service Catalog:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support app

The "Siemens Industry Online Support" app provides you with optimum support while on the go. The app is available for Apple iOS, Android and Windows Phone.

<https://support.industry.siemens.com/cs/en/en/sc/2067>

4.2 Links and Literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/de/view/109746841
\3\	

4.3 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	05/2017	First version