



HOW TO

Configurazione per connessione a SINEMA RC senza Basic Wizard

SIEMENS

Contents

Configurazione per connessione a SINEMA RC senza Basic Wizard	3
Configurazione senza Basic Wizard	3
Configurazione DNS	8
Verifica connessione al Sinema RC	10
Considerazioni sulla connettività e sulle porte di comunicazione	11

Configurazione per connessione a SINEMA RC senza Basic Wizard

La seguente guida illustra come configurare uno Scalance S615 attraverso la sua pagina web (Web Based Management) per stabilire una connessione VPN al software Sinema Remote Connect Server.

La guida è valida fino al firmware 7.1 di Scalance S615 e server Sinema RC 3.1.

Prima di iniziare la configurazione è necessario avere a disposizione un software Sinema RC Server funzionante con almeno un dispositivo correttamente parametrizzato.

Per configurare il Sinema RC Server o per configurare gli altri parametri sullo Scalance si può fare riferimento alle guide apposite.

Configurazione senza Basic Wizard

Per la configurazione della connessione a SINEMA RC è opportuno assegnare correttamente gli indirizzi IP alle interfacce di rete. Accedere al menù **Layer 3** → **Subnets**

192.168.1.1/SCALANCE S615

Welcome admin
Logout

Connected Subnets Overview

Overview Configuration

Interface: VLAN1

Select	Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask
<input checked="" type="checkbox"/>	vlan1	yes	enabled	INT	20-87-56-7a-bb-68	192.168.1.1	255.255.255.0
<input type="checkbox"/>	vlan2	-	enabled	EXT	20-87-56-7a-bb-6c	192.168.2.2	255.255.255.0
<input type="checkbox"/>	ppp2	-	disabled	ppp2	00-00-00-00-00-00	0.0.0.0	0.0.0.0

3 entries.

Create Delete Refresh

La modifica dell'IP della singola rete può essere apportata cliccando sulla tab Configuration o direttamente sul nome dell'interfaccia. In particolare, è importante assegnare un indirizzo IP alla vlan2, di norma utilizzata per l'accesso internet che garantisce la connessione al SINEMA RC, oppure alla nuova VLAN programmata per questo scopo, se questa non lavora in DHCP.

Remuovere il flag da DHCP e impostare i parametri di "IP Address" e "Subnet Mask" desiderati. Cliccare su "Set Values".

SIEMENS 192.168.1.1/SCALANCE S615

Welcome admin [Logout](#)

Connected Subnets Configuration

Overview Configuration

Interface (Name): vlan2 (EXT) ▾
 Status: enabled ▾
 Interface Name: EXT
 MAC Address: 20-87-56-7a-bb-6c
 DHCP
 IP Address: 192.168.2.2
 Subnet Mask: 255.255.255.0
 Broadcast IP Address: 192.168.2.255
 Address Type: Primary
 TIA Interface
 MTU: 1500

[Set Values](#) [Refresh](#)

Se non lo si è già fatto, assegnare nello stesso modo gli indirizzi IP alle restanti VLAN configurate.

Qualora la rete del cliente lo richieda, l'inserimento del **default gateway** è possibile nella pagina **Layer 3** → **Static Routes**.

Qui va inserita una rotta statica con i seguenti parametri:

- Destination: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Gateway: x.y.z.m (cioè l'indirizzo IP del default gateway)

Cliccare su "Create"

SIEMENS 192.168.1.1/SCALANCE S615

Welcome admin [Logout](#)

Static Routes

Destination Network:
 Subnet Mask:
 Gateway:
 Interface: auto ▾
 Administrative Distance: -1

Select	Destination Network	Subnet Mask	Gateway	Interface
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.2.1	vlan2

1 entry.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Un altro parametro fondamentale, se non già configurato in precedenza, è la parametrizzazione di **data e ora**. Questa può avvenire in modo manuale o con server **NTP**.

Accedere al menù **System** → **System Time**.

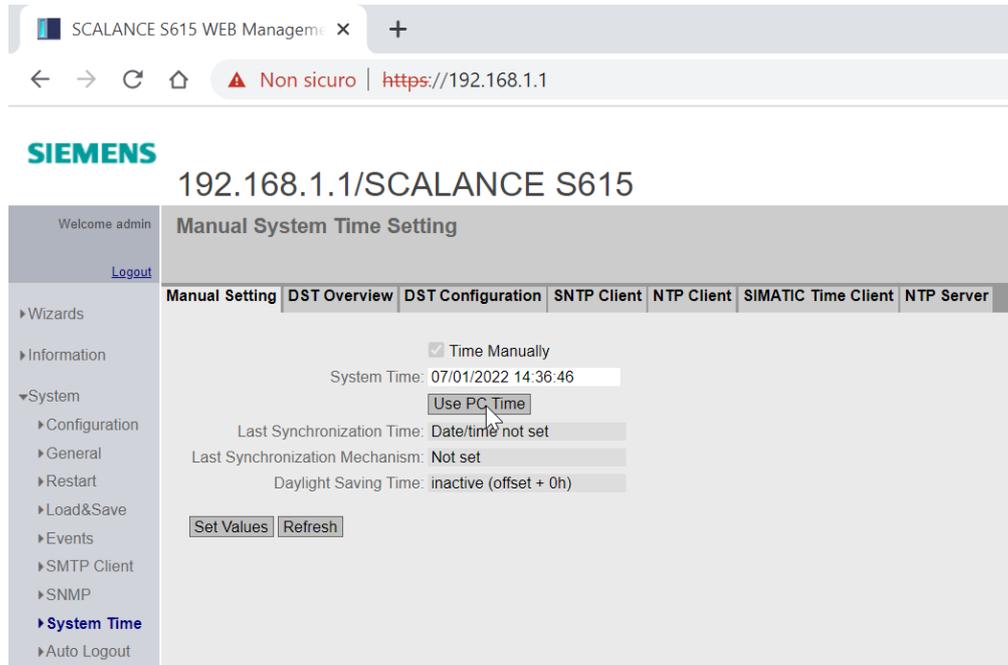
Sono disponibili due modalità di configurazione:

1. Impostazione manuale

L'impostazione manuale consente all'ora di scorrere fintanto che il PC è acceso ma in caso di spegnimento rimarrà congelata e ripartirà al riavvio del dispositivo. E' quindi una configurazione rapida ma poco robusta a eventuali spegnimenti.

Per impostare il tempo cliccare su System → System Time → Manual Setting.

Premere sul pulsante "Use PC Time" e cliccare su "Set Values".



2. Sincronizzazione con server NTP

Accedere a System → System Time → NTP Client.

Cliccare su "Create" ed inserire l'indirizzo IP del server NTP da utilizzare, che di norma sono in ascolto sulla porta 123 UDP, presente all'interno della rete d'impianto o raggiungibile con la connessione internet (ad es.: 193.204.114.232)

Se la porta è differente può essere specificata nell'apposito campo della tabella, dove è anche possibile impostare l'intervallo di polling sul server.

Indicare la relativa time zone e spuntare la modalità "NTP Client" o in alternativa la modalità sicura (NTPsec da non confondersi con SNTP) "Secure NTP Client Only". Cliccare "Set Values".

192.168.1.1/SCALANCE S615

Network Time Protocol (NTP) Client

Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client | NTP Server

NTP Client
 Secure NTP Client only

Current System Time: 01/01/2000 00:15:10
 Last Synchronization Time: Date/time not set
 Last Synchronization Mechanism: Not set
 Time Zone: +01:00
 Daylight Saving Time: inactive (offset + 0h)

NTP Server Index: 1

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key	Key Confirmation
<input type="checkbox"/>	1	193.204.114.232	123	64	1	DES		

1 entry

Create Delete Set Values Refresh

La parametrizzazione per la connessione a Sinema RC è disponibile in **System** → **Sinema RC**.

Per recuperare i valori da inserire all'interno di questa pagina, bisogna andare sul Sinema RC Server nella sezione Remote Connections → Devices. Selezionare il dispositivo cliccando sul simbolo di "i" (Informazione)

SINEMA Remote Connect

7/11/2022, 4:40:37 PM (UTC +02:00) Admin English Logout

System
Remote Connections
Devices
Device Update
Participant Groups
Communication Relations
User Accounts
Services
Security
My Account

All s615_demo Show all

Filter active Precise match

Create Delete Edit table

Device name	VPN address	Remote subnet	Virtual Subnet	Status	Last connection	Location	Connection type	VPN protocol	Actions
S615_De mo	-	192.168.1 15.0/24	172.24.1 15.0/24	Offline	Aug. 24, 2021, 10:15 a.m.		Permanent	OpenVPN	i

Da qui è possibile copiare tutti i valori utili per l'inserimento nella pagina di configurazione dello SCALANCE S615.

The screenshot shows the SIEMENS SINEMA Remote Connect web interface. The browser address bar displays the URL: <https://srctest.westeurope.cloudapp.azure.com/wbm/device/9/info/>. The page title is "SIEMENS SINEMA Remote Connect". The user is logged in as "Admin" and the language is set to "English". The date and time are "7/1/2022, 5:08:42 PM (UTC +02:00)".

The left sidebar contains a navigation menu with the following items: System, Remote Connections, Devices, Device Update, Participant Groups, Communication Relations, User Accounts, Services, Security, and My Account. The "Devices" section is expanded, showing "Device overview".

The "Device overview" section displays the following information:

- Device information:
- Device ID: 9
- IP address of the VPN server: 10.0.0.20
- IP address of the Web server: 10.0.0.20
- Web server port: 443
- SHA1-Fingerprint: 68:D3:38:B6:B9:73:1C:83:F3:F9:CB:A9:61:34:FF:4E:B7:3D:10:4D
- SHA256-Fingerprint: 84:25:59:C4:AD:53:0A:A4:69:2A:BE:96:90:85:5B:34:0C:7E:83:12:44:09:F7:71:5E:C4:32:CE:FE:A8:C3:27
- Export CA: [Download icon]
- Device name: S615_Demo
- Network Settings: [Edit icon]
- Type: SCALANCE S615 / M804PB / M826 / M816
- Vendor: Siemens
- Location:

Inserire quindi i seguenti parametri:

- Device ID
- IP address of the VPN server (IP oppure hostname)
- Web Server Port (443 se non è stata modificata in fase di configurazione del server).
- Fingerprint (scegliere quale utilizzare in base al livello di crittografia desiderato: SHA1 oppure SHA256).
- Password (non è riportata, è stata inserita in fase di creazione del device sul server, se è stata dimenticata è possibile comunque farla modificare dall'amministratore del server senza conoscere quella precedente)

The screenshot shows the "SINEMA Remote Connect (SINEMA RC)" configuration page. The page title is "SINEMA Remote Connect (SINEMA RC)". The user is logged in as "admin" and the language is set to "English". The date and time are "7/1/2022, 5:08:42 PM (UTC +02:00)".

The left sidebar contains a navigation menu with the following items: Welcome admin, Logout, Wizards, Information, System, Configuration, General, Restart, Load&Save, Events, SMTP Client, SNMP, System Time, Auto Logout, Button, Syslog Client, Fault Monitoring, PLUG, Ping, DCP Discovery, DNS, DHCPV4, cRSP / SRS, Proxy Server, SINEMA RC, and Cloud. The "SINEMA RC" section is expanded.

The "SINEMA RC" section displays the following configuration options:

- Enable SINEMA RC
- Server Settings:
 - SINEMA RC Address: srctest.westeurope.cloudapp.azure.com
 - SINEMA RC Port: 443
- Server Verification:
 - Verification Type: Fingerprint
 - Fingerprint: 68:D3:38:B6:B9:73:1C:83:F3:F9:CB:A9:61:34:FF:4E:B7:3D:10:4D
 - CA Certificate: -
- Device Credentials:
 - Device ID: 9
 - Device Password: [Masked]
 - Device Password Confirmation: [Masked]
- Optional Settings:
 - Auto Firewall/NAT Rules
 - Type of connection: Auto
 - Use Proxy: none
 - Autoenrollment Interval [min]: 60
 - Timeout[min]: 0

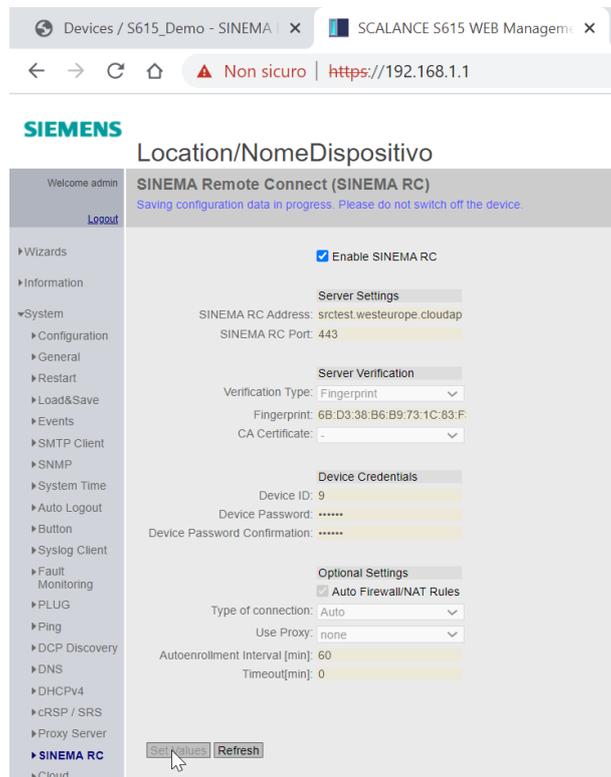
Buttons: [Set Values] [Refresh]

Cliccare su "Set Values".

In seguito spuntare il campo "Enable Sinema RC". Tutti i parametri appariranno in giallo e non saranno

più modificabili.

Cliccare di nuovo su “Set Values”.



N.B.: se si è scelto di utilizzare un hostname per il Sinema RC Server e non si ha la configurazione DHCP occorre anche configurare dei server DNS per risolvere il nome del server. Seguire quindi la sezione successiva.

Configurazione DNS

Per configurare il DNS occorre scorrere il menù della pagina web dello Scalance alla voce System → DNS

Se non si ha un DNS locale o raccomandato dal proprio provider è sempre possibile utilizzare i classici DNS di Google (8.8.8.8 e 8.8.4.4) laddove sia permesso il loro raggiungimento.

Digitare l'indirizzo in corrispondenza della voce “DNS Server Address” e cliccare su “Create”.

È possibile inserire anche più di un indirizzo.

N.B.: la connessione a un server DNS pubblico implica la comunicazione su porta 53 UDP che quindi non deve essere bloccata da eventuali firewall.

Qualora si abbia un DHCP che fornisce DNS sarà presente una linea "learned" in corrispondenza della colonna "Origin".

Verifica connessione al Sinema RC

Per verificare l'avvenuta connessione è sufficiente verificare l'accensione del led a "lucchetto" sullo Scalance oppure accedere alla pagina web Information → Sinema RC.

The screenshot shows the Siemens Scalance S615 WEB Management interface. The browser address bar indicates the URL is https://192.168.115.254. The page title is "LuogoProva/DeviceProva". The main content area displays "SINEMA Remote Connect (SINEMA RC) Information" with the following details:

- Status: established (srctest.westeurope.cloudapp.azure.com, Port 1194, UDP)
- Device Name: S815_Demo
- Device Location: -
- GSM Number: -
- Vendor: Siemens
- Comment: -
- Type of Connection (Server): Permanent
- Type of Connection (Device): Auto
- Fingerprint: 3E:D0:AA:13:2F:A6:95:FD:2E:4A:4C:29:B1:4E:D5:3E:7C:AE:45:FF
- Remote Address: 40.113.114.46
- Connected Local Subnet(s): 192.168.1.0/24
- Connected Local Host (s):
- Tunnel Interface Address: 172.30.0.7
- Connected Remote Subnet(s): 172.30.0.0/16, 172.29.0.0/16, 172.32.0.0/16

A "Refresh" button is located at the bottom of the information section.

Per essere stabilita la connessione deve essere "Established", se non è stata abilitata lo status è invece in "Disabled" o "Waiting for Digital Input". Se invece la configurazione rimane in "Pending" c'è un problema di connessione e va esaminato facendo del troubleshooting (seguire apposita guida).

Considerazioni sulla connettività e sulle porte di comunicazione

Lo Scalance S può essere su rete WAN con firewall e quindi può necessitare di permessi di comunicazione. In quanto client lo Scalance non necessita di abilitazioni in ingresso e/o port forwarding ma deve poter semplicemente uscire sulle seguenti porte (non devono essere bloccate dal firewall) per raggiungere il server Sinema RC:

443 TCP → porta di destinazione del web server (**HTTPS**) fondamentale per negoziare i certificati

1194 UDP → porta di comunicazione del protocollo **OpenVPN** per l'instaurazione del tunnel

Non sono fondamentali ma sono anche utilizzabili le seguenti porte:

5443 TCP → porta per connessione TCP **OpenVPN**. Qualora la connessione UDP sia instabile, il protocollo tenta la connessione in TCP su questa porta, che garantisce una maggior stabilità (è comunque impossibile imporre l'utilizzo di TCP o UDP nella configurazione del server).

6220 TCP → qualora il dispositivo sia rimasto spento o disconnesso durante la fase di rinnovo dei certificati e alla successiva connessione il certificato sia cambiato è possibile effettuare il rinnovo forzato (procedura di **fallback**) del certificato (cambio fingerprint) attraverso questa porta.

N.B: Tutte queste porte derivano direttamente dalla configurazione OpenVPN e sono parametrizzate direttamente nel Sinema RC Server. L'amministratore del server Sinema RC può quindi modificarle ma tale modifica coinvolge tutti i device. Fa eccezione la porta 443 che può invece essere modificata per singolo dispositivo nella pagina di parametrizzazione per Sinema RC. Il server rimane comunque in ascolto sulla 443 se non modificato.

Inoltre, se sono stati utilizzati NTP e/o DNS pubblici e anche necessario che non siano bloccate le porte:

53 UDP → porta di comunicazione DNS

123 UDP → porta di comunicazione NTP

Con riserva di modifiche e salvo errori.

Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.

Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.