



HOW TO

Troubleshooting connessione SINEMA RC

SIEMENS

Contents

| | |
|---|----------|
| Troubleshooting connessione SINEMA RC | 3 |
| Verifiche preliminari | 3 |
| Verifica della connessione a Sinema RC sul device | 5 |
| Verifica della log table | 7 |
| Connessione ai dispositivi a valle dello Scalance | 16 |
| Settaggi lato Sinema RC Client | 18 |

Troubleshooting connessione SINEMA RC

La seguente guida illustra come analizzare le problematiche che possono avvenire nella connessione di un dispositivo Siemens Scalance S o M alla piattaforma Siemens Sinema Remote Connect.

Per quanto riguarda la configurazione corretta dei device e di Sinema RC Server e Client si faccia riferimento alle guide apposite.

La guida è valida fino alle versioni firmware 7.1 di Scalance S615/M800, 2.3 per Scalance SC600 e 3.1 per Sinema RC.

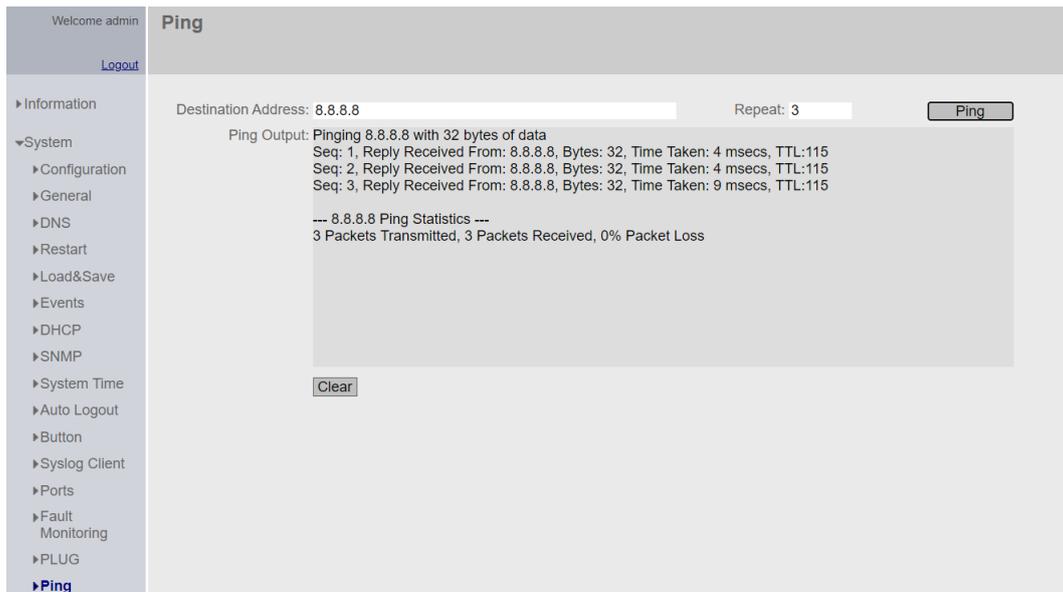
Verifiche preliminari

Se si sperimentano problematiche nella connessione a Sinema RC è bene verificare che prima di tutto si operi in un ambiente che sia funzionante. Occorre quindi verificare che:

- Il device sia **connesso a internet** o comunque alla rete in cui si trova il Sinema RC Server
- Il **Sinema RC Server sia online e funzionante**

Per verificare che il device sia connesso, a valle della configurazione del dispositivo, si può semplicemente eseguire un **test di ping** direttamente dalla pagina web del dispositivo dal menu **System** → **Ping**.

Si può quindi ad esempio pingare direttamente l'indirizzo del server (se pingabile) oppure, se il dispositivo è su Internet, un indirizzo pubblico sicuramente online (ad esempio il classico 8.8.8.8, DNS di Google)



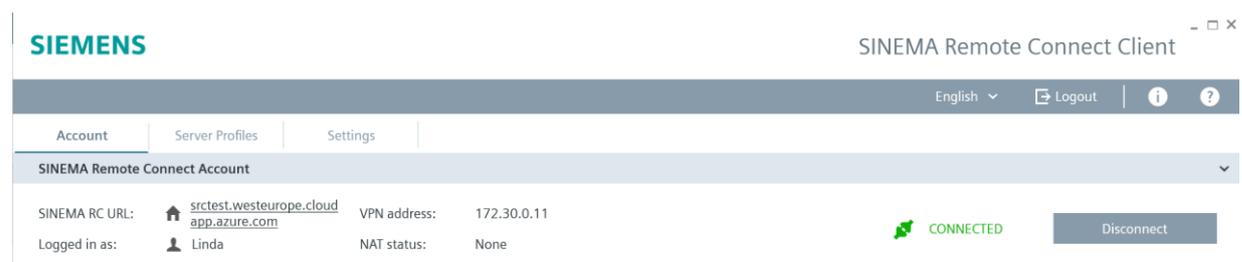
Se l'indirizzo prescelto è raggiungibile saranno ricevute delle risposte come in immagine, altrimenti **in caso di mancata connettività saranno mostrati dei messaggi di "Reply not Received"**

N.B.: alcuni firewall aziendali, seppur raramente, prevengono la possibilità di fare uscire dei messaggi di ping, in tal caso è possibile provare ad aprire delle pagine web qualsiasi dal PC di configurazione impostando come default gateway l'indirizzo dello Scalance S615, aprendo o disabilitando temporaneamente il firewall nella sezione Security → firewall e applicando il masquerading sulla VLAN esterna nella sezione layer 3 → NAT, tab Masquerading.

Per verificare che il Sinema RC server sia correttamente funzionante, se il server è online, si consiglia di testarlo da una rete diversa da quella utilizzata dal dispositivo onde escludere che ci sia un problema proprio su tale rete.

Si può innanzitutto provare ad aprire la pagina web del Sinema RC server ad <https://x.y.m.z> dove x.y.m.z è l'indirizzo IP o hostname del Sinema RC Server. Se il server è online, apparirà la pagina di login dopo aver accettato il certificato.

In seconda istanza **per verificare la funzionalità VPN si può usare direttamente il Sinema RC Client**, collegandosi al server con un utente creato e abilitando la funzionalità (si rimanda alle guide apposite per ulteriori informazioni).



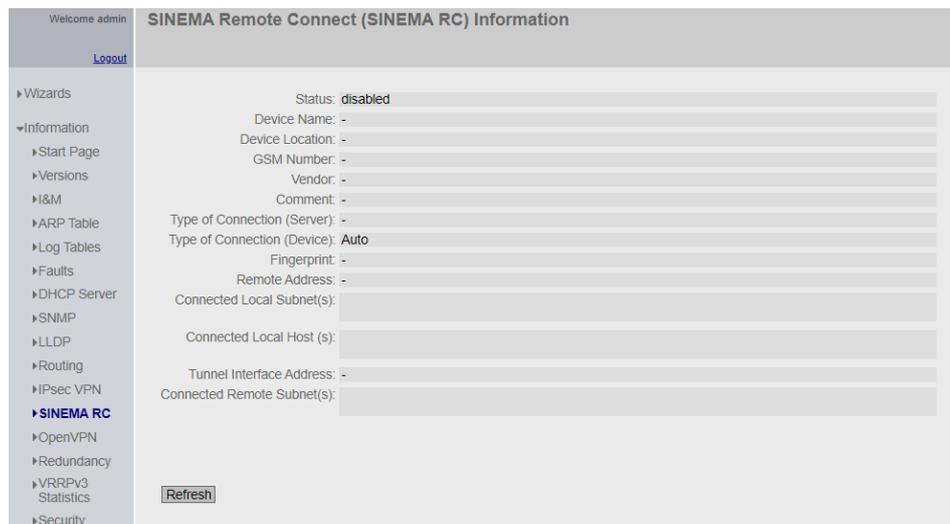
Se il Sinema RC Client è in grado di andare online questo significa che il server è in grado di stabilire connessioni VPN e che eventuali anomalie vanno ricercate più probabilmente dal lato del dispositivo.

Verifica della connessione a Sinema RC sul device

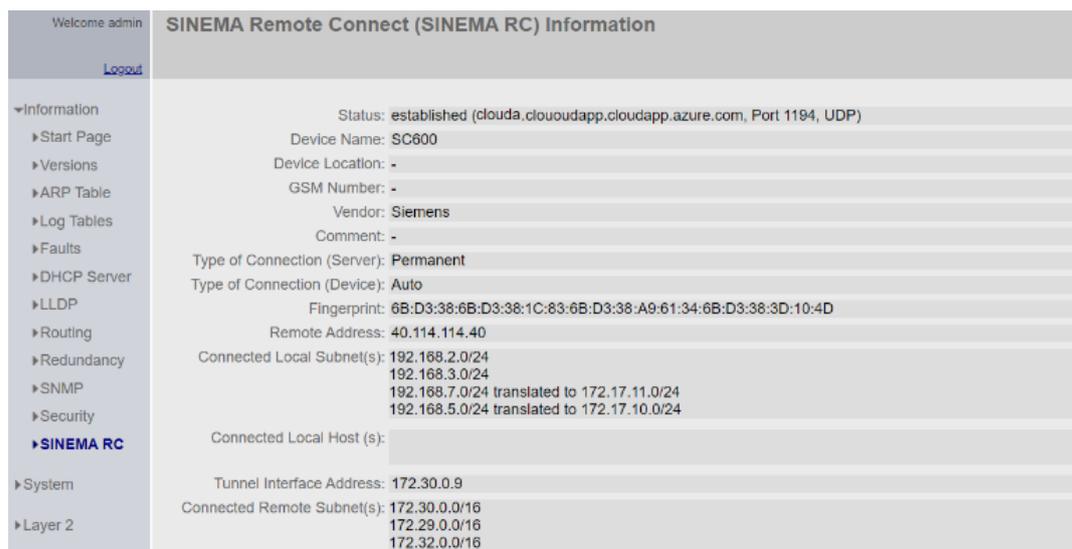
Una volta concluse le verifiche preliminari, occorre verificare lo stato del collegamento a Sinema RC. Questo può essere visionato nel menù del configuratore web alla voce **Information** → **Sinema RC**.

Ci sono 4 possibili stati in questa pagina:

- **Disabled:** la VPN non è configurata o abilitata (stato di default) → occorre tornare alla configurazione per abilitare o configurare la connessione a Sinema RC (menu System→Sinema RC)



- **Established:** la VPN è stabilita → nessun problema da analizzare lato connessione al server



N.B.: In questo caso dovrete vedere il dispositivo online sulla pagina web di Sinema RC server e sul Sinema RC Client, **se ci fossero comunque problemi di connettività consultare l'ultima sezione del documento.**

| | | | | | | | | | | |
|----------|------------|-------|-----------------|----------------|--------|------|--------|----|-----|-----|
| Macchina | 172.30.0.7 | Rete1 | 192.168.10.0/24 | 172.18.10.0/24 | ONLINE | Home | Mobile | NO | YES | NAT |
| | | Rete2 | 192.168.52.0/24 | 172.21.52.0/24 | | | | | | |

- **Waiting for Digital Input:** la VPN è configurata per stabilirsi con Digital Input → alzare il DI o cambiare questa configurazione per far partire la VPN

The screenshot shows the 'SINEMA Remote Connect (SINEMA RC) Information' page. The status is 'waiting for digital input'. The left sidebar contains a navigation menu with 'SINEMA RC' highlighted. The main content area lists various fields: Device Name, Device Location, GSM Number, Vendor, Comment, Type of Connection (Server), Type of Connection (Device) set to 'Digital Input', Fingerprint, Remote Address, Connected Local Subnet(s), Connected Local Host (s), Tunnel Interface Address, and Connected Remote Subnet(s). A 'Refresh' button is located at the bottom left of the main content area.

- **Pending:** la VPN è configurata e il device tenta di connettersi senza successo → occorre un'analisi più approfondita

The screenshot shows the 'SINEMA Remote Connect (SINEMA RC) Information' page. The status is 'pending'. The left sidebar contains a navigation menu with 'SINEMA RC' highlighted. The main content area lists various fields: Device Name, Device Location, GSM Number, Vendor, Comment, Type of Connection (Server), Type of Connection (Device) set to 'Auto', Fingerprint, Remote Address, Connected Local Subnet(s), Connected Local Host (s), Tunnel Interface Address, and Connected Remote Subnet(s). A 'Refresh' button is located at the bottom left of the main content area.

Verifica della log table

Qualora la VPN sia in "pending", occorre verificare il messaggio di errore ricevuto lato diagnostica dispositivo. Per fare ciò, occorre visualizzare i messaggi di log che trovate nella pagina web del dispositivo in **Information** → **Log Tables (tab Security Log)**

The screenshot shows the 'Security Log Table' interface. The left sidebar contains a navigation menu with 'Log Tables' highlighted. The main area shows 'Severity Filters' (Info, Warning, Critical) and a table with columns: System Up Time, Restart, System Time, Severity, and Log Message. The table is currently empty, displaying '0 entries.' and buttons for 'Clear' and 'Refresh'.

Nell'immagine sopra viene riportato il log al default (vuoto), mentre sotto viene riportato il log di una connessione che avviene correttamente.

The screenshot shows the 'Security Log Table' interface with a list of log entries. The entry 'OpenVPN connection established.' is highlighted with a red box. The table columns are: System Up Time, Restart, System Time, Severity, and Log Message.

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:43:20 | 1 | 11/13/2020 11:45:00 | 6 - Info | SINEMA RC - OpenVPN connection established. |
| 00:43:20 | 1 | 11/13/2020 11:45:00 | 6 - Info | SINEMA RC - Received initial routes from server. Routing tables and automatic firewall rules configured. |
| 00:43:15 | 1 | 11/13/2020 11:44:55 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:43:15 | 1 | 11/13/2020 11:44:55 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:43:15 | 1 | 11/13/2020 11:44:54 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:43:15 | 1 | 11/13/2020 11:44:54 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:1194 using UDP |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:43:10 | 1 | 11/13/2020 11:44:49 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:43:08 | 1 | 11/13/2020 11:44:47 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:43:00 | 1 | 11/13/2020 11:44:40 | 4 - Warning | SINEMA RC has been activated. |

Se la connessione a Sinema RC non si è stabilita le ragioni possono essere facilmente individuate dai messaggi di log.

Le ragioni possono essere:

- **Couldn't resolve hostname server** → il dispositivo non risolve il nome DNS del Sinema RC Server
- **Timeout was reached** → Il Sinema RC Server è irraggiungibile
- **Fingerprint verification failed** → il controllo del fingerprint non è corretto
- **Configuration is empty** → le credenziali del device (ID e password) non sono corrette

- **Certificate not yet valid** → il system time non combacia con il certificato
- **OpenVPN terminated** → la connessione VPN è andata in time-out
- **Download failed because of mismatch in fallback info** → il device ha cercato di connettersi sulla porta di fallback senza successo (caso speciale a valle di un check fingerprint failed)

Vediamo ora nel dettaglio i singoli messaggi con i possibili errori o problemi che li possono causare.

Couldn't resolve hostname server (Mancata risoluzione hostname).

The screenshot shows the 'Event Log' tab in a network device's management interface. The log table contains the following entries:

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:28:30 | 1 | 11/13/2020 11:37:12 | 6 - Info | SINEMA RC - Configuration download retry in 10 seconds |
| 00:28:30 | 1 | 11/13/2020 11:37:12 | 4 - Warning | SINEMA RC - Precheck fingerprint: curl easy perform failed: Couldn't resolve host name [6] server sinema.server.it:443 |
| 00:28:30 | 1 | 11/13/2020 11:37:12 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:28:28 | 1 | 11/13/2020 11:37:10 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:28:21 | 1 | 11/13/2020 11:37:02 | 4 - Warning | SINEMA RC has been activated. |

Below the table, there are 5 entries, a 'Clear' button, and a 'Refresh' button.

Questo problema si verifica quando il Sinema RC server a cui il dispositivo deve connettersi viene indirizzato tramite un hostname (es: server.sinema.it) e non attraverso un IP statico (es: 1.1.1.1).

Per risolvere il nome (ovvero capire a quale indirizzo IP è associato tale nome,) il device deve prima chiamare un server DNS che è sua volta indicato con un indirizzo IP.

Se il dispositivo non riesce a risolvere l'hostname le possibilità sono 2:

1. Il server **DNS non è configurato** o non è configurato correttamente
2. Il server **DNS non è raggiungibile** o non risponde, in questo caso è possibile che:
 - a. il **dispositivo non** sia effettivamente **connesso alla rete** (vedere verifiche preliminari sopra)
 - b. il firewall aziendale sui cui è connesso blocchi la **porta 53 UDP** utilizzata dal servizio DNS (consultare l'amministratore di rete a tale proposito e consentire la comunicazione su questa porta).

Per verificare la configurazione DNS andare nel menù System → DNS

SCALANCE 5615 WEB Management x +

Non sicuro | https://192.168.115.254

SIEMENS LuogoProva/DeviceProva

Welcome admin [Logout](#)

Wizards

Information

System

- Configuration
- General
- Restart
- Load&Save
- Events
- SMTTP Client
- SNMP
- System Time
- Auto Logout
- Button
- Syslog Client
- Fault Monitoring
- PLUG
- Ping
- DCP Discovery
- DNS**

Domain Name System (DNS) Client

DNS Client | DNS Proxy | DDNS Client

DNS Client

Used DNS Servers: all

DNS Server Address: 8.8.4.4

| DNS Server Address | Origin |
|--------------------|---------|
| 8.8.8.8 | learned |

1 entry.

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

Ci deve essere almeno un indirizzo che sia “learned” (fornito da DHCP) o “manual”, qualora non ci sia, aggiungerlo manualmente digitando l’indirizzo e cliccando su “Create” (utilizzare 8.8.8.8 o 8.8.4.4 di Google se non si sa cosa usare).

N.B.: talvolta può capitare che i DNS pubblici come quelli di Google siano bloccati da firewall aziendali o regionali, nel caso consultare l’amministratore di rete per ulteriori informazioni.

Timeout was reached (Sinema RC Server è irraggiungibile).

Wizards

Information

- Start Page
- Versions
- I&M
- ARP Table
- Log Tables**
- Faults
- DHCP Server
- SNMP
- LLDP
- Routing
- IPsec VPN
- SINEMA RC
- OpenVPN
- Redundancy
- VRRPv3 Statistics
- Security

Event Log | Security Log | Firewall Log

Severity Filters

Info

Warning

Critical

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|---|
| 00:20:28 | 1 | 11/13/2020 11:29:09 | 6 - Info | SINEMA RC - Configuration download retry in 10 seconds |
| 00:20:28 | 1 | 11/13/2020 11:29:09 | 4 - Warning | SINEMA RC - Precheck fingerprint: curt easy perform failed: Timeout was reached [28] server |
| 00:20:20 | 1 | 11/13/2020 11:29:01 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:20:18 | 1 | 11/13/2020 11:28:59 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:20:09 | 1 | 11/13/2020 11:28:51 | 4 - Warning | SINEMA RC has been activated. |

5 entries.

[Clear](#)

[Refresh](#)

Questo problema si verifica quando il dispositivo non riesce a raggiungere il server sulla porta HTTPS (default 443 TCP). In questo caso bisogna verificare che:

1. Le verifiche preliminari (vedere sopra) di connettività e funzionamento del server diano esito positivo.
2. La porta 443 o comunque la porta configurata per il web server non sia bloccata dal firewall aziendale.

Per verificare che la porta 443 sia libera è sufficiente provare a navigare con un PC con l'indirizzo dello Scalance (o col PC configurato per la navigazione sotto lo Scalance) per vedere se la pagina web del Sinema RC server sia in grado di aprirsi sul web browser.

Fingerprint verification failed (Fallito controllo fingerprint).

The screenshot shows the 'Event Log' tab in a network device's management interface. The log table contains several entries, with one entry highlighted in red: 'SINEMA RC - Fingerprint verification failed!'. The interface also includes a sidebar with navigation options like 'Wizards', 'Information', 'Start Page', 'Versions', 'I&M', 'ARP Table', 'Log Tables', 'Faults', 'DHCP Server', 'SNMP', 'LLDP', 'Routing', 'IPsec VPN', 'SINEMA RC', 'OpenVPN', 'Redundancy', 'VRRPv3', 'Statistics', 'Security', 'System', and 'Interfaces'. There are also 'Severity Filters' (Info, Warning, Critical) and 'Clear' and 'Refresh' buttons.

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:23:59 | 1 | 11/13/2020 11:32:41 | 2 - Critical | SINEMA RC - Download failed because of mismatch in fallback info! Start reading fallback info saved on plug. It can take up to 2 minutes |
| 00:23:59 | 1 | 11/13/2020 11:32:40 | 4 - Warning | SINEMA RC - No fallback information found on device |
| 00:23:59 | 1 | 11/13/2020 11:32:40 | 6 - Info | SINEMA RC - CA update download thread started |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Server fingerprint: <DF:94:AB:12:80:DA:31:CA:A4:30:42:E2:64:72:8D:96:26:F0:51:98> |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Configured fingerprint: <DD:94:AB:12:80:DA:31:CA:A4:30:42:E2:64:72:8D:96:26:F0:51:98> |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 4 - Warning | SINEMA RC - Fingerprint verification failed! |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Precheck fingerprint: curl easy perform done (server 192.168.3.3:443) |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:23:56 | 1 | 11/13/2020 11:32:37 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:23:50 | 1 | 11/13/2020 11:32:31 | 4 - Warning | SINEMA RC has been activated. |

Questo problema si verifica quando il dispositivo riceve una risposta alla connessione HTTPS ma verificando il fingerprint del server remoto ritrova un valore diverso. In questo caso occorre verificare che:

1. Il fingerprint sia stato **inserito correttamente** nella configurazione del dispositivo.
2. Il fingerprint sia **aggiornato con quello del server** (se il device non si è mai connesso al server e il certificato del server è cambiato successivamente alla configurazione il fingerprint sarà cambiato).
3. Il **server sia raggiungibile e l'indirizzo inserito sia corretto**: talvolta collegandosi a un altro indirizzo si può ricevere una risposta che viene interpretata come un fingerprint errato.
4. La **porta del web server sia corretta**: se si è spostata la porta su un altro numero diverso da 443 è infatti probabile che sia presente un Web Server sulla 443 originale che risponderà col proprio fingerprint alla richiesta del dispositivo e verrà considerato ovviamente errato.
5. Il **firewall aziendali non blocchi le connessioni HTTPS con certificato self-signed**. In tal caso la risposta che si riceve viene deformata da una richiesta di accettazione e il pacchetto non viene riconosciuto dal dispositivo.

Welcome admin **SINEMA Remote Connect (SINEMA RC)**

[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

DHCP

cRSP / SRS

Proxy Server

SINEMA RC

Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168.4.4

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint: 77:7D:BB:DA:52:0A:13:13:6

CA Certificate: -

Device Credentials

Device ID: 12

Device Password:

Device Password Confirmation:

Optional Settings

Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

Timeout[min]: 0

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

Configuration is empty (le credenziali del device (ID e password) non sono corrette).

Wizards

Information

Start Page

Versions

I&M

ARP Table

Log Tables

Faults

DHCP Server

SNMP

LLDP

Routing

IPsec VPN

SINEMA RC

OpenVPN

Redundancy

VRRPv3 Statistics

Security

Event Log | Security Log | Firewall Log

Severity Filters

Info

Warning

Critical

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 4 - Warning | SINEMA RC - Configuration downloaded from server is empty. Please verify that Device ID and Device Password are correct. |
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 2 - Critical | SINEMA RC - Configuration download failed: file size is zero! |
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 6 - Info | SINEMA RC - Configuration download: curl easy perform done (server 192.168.3.443) |
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:31:48 | 1 | 11/13/2020 11:40:30 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:31:47 | 1 | 11/13/2020 11:40:29 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:31:38 | 1 | 11/13/2020 11:40:19 | 4 - Warning | SINEMA RC has been activated. |
| 00:30:18 | 1 | 11/13/2020 11:38:59 | 2 - Critical | SINEMA RC has been deactivated. |

9 entries.

[Clear](#)

[Refresh](#)

Se il device controlla con successo il fingerprint, il device sfrutterà la connessione HTTPS per effettuare l'auto-enrollment e scaricare il proprio file di configurazione dal server autenticandosi con le proprie credenziali. Se questa procedura fallisce occorre verificare che:

1. Il **device ID** del dispositivo esista sul server e sia corretto

2. La **password** del dispositivo sia corretta (si consiglia di sovrascriverla nel server se non si è sicuri)

Welcome admin **SINEMA Remote Connect (SINEMA RC)**

[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
 - DHCP
 - cRSP / SRS
 - Proxy Server
 - SINEMA RC**

Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168.4.4

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint: 77:7D:BB:DA:52:0A:13:13:6

CA Certificate: -

Device Credentials

Device ID: 12

Device Password: *****

Device Password Confirmation: *****

Optional Settings

Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

Timeout[min]: 0

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

In caso di errore correggere l'impostazione in System → Sinema RC.

Certificate not yet valid (System Time errato).

Event Log Security Log Firewall Log

Severity Filters

Info

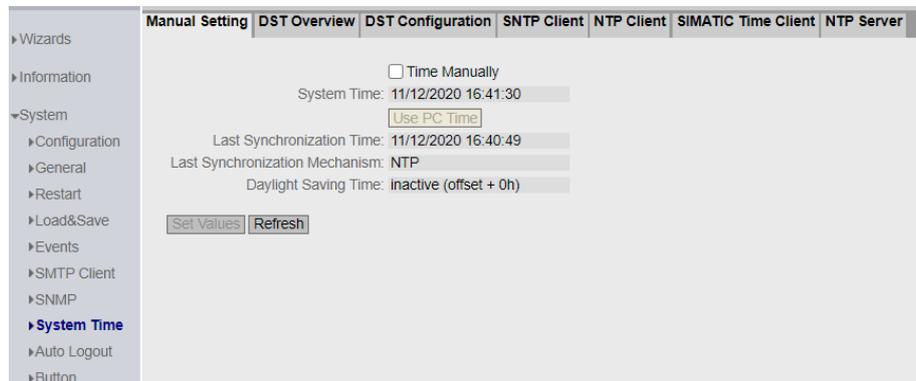
Warning

Critical

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:36:49 | 1 | 11/13/2010 11:45:22 | 4 - Warning | SINEMA RC - OpenVPN terminated. |
| 00:36:44 | 1 | 11/13/2010 11:45:17 | 4 - Warning | SINEMA RC - OpenVPN Certificate not yet valid. Please set the correct system time. |
| 00:36:44 | 1 | 11/13/2010 11:45:17 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:36:44 | 1 | 11/13/2010 11:45:17 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:1194 using UDP |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 4 - Warning | SINEMA RC - OpenVPN terminated. |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:36:42 | 1 | 11/13/2010 11:45:15 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 4 - Warning | SINEMA RC - OpenVPN Certificate not yet valid. Please set the correct system time. |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:1194 using UDP |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:36:37 | 1 | 11/13/2010 11:45:09 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:36:35 | 1 | 11/13/2010 11:45:07 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |

Una volta che la configurazione è stata scaricata correttamente dal server, il device riceverà anche il suo certificato. A questo punto confronterà il proprio System Time per stabilire la validità temporale di tale certificato. La maggior parte dei device in configurazione iniziale non ha un orario aggiornato (in genere parte all'1/1/2000), se l'ora non viene almeno impostata manualmente il device non ha la possibilità di connettersi in VPN.

In caso di questo messaggio di errore verificare l'ora nel cursore in alto a destra e/o su System → Time e aggiornarla in caso di errore.



N.B.: Se l'ora fosse corretta e il messaggio di errore persiste verificare l'ora del Sinema RC Server.

N.B.: ad ogni spegnimento il dispositivo congelerà l'ora, questo può essere un problema per il rinnovo dei certificati per cui **si raccomanda l'uso di un NTP server per sincronizzare l'ora alla riaccensione** (vedere guida di configurazione per maggiori dettagli).

OpenVPN terminated (Connessione terminata).

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:39:29 | 1 | 11/13/2035 11:47:46 | 4 - Warning | SINEMA RC - OpenVPN terminated. |
| 00:39:21 | 1 | 11/13/2035 11:47:38 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:39:21 | 1 | 11/13/2035 11:47:38 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:5443 using TCP |
| 00:39:21 | 1 | 11/13/2035 11:47:38 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:39:19 | 1 | 11/13/2035 11:47:36 | 4 - Warning | SINEMA RC - OpenVPN terminated. |
| 00:39:13 | 1 | 11/13/2035 11:47:30 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:39:13 | 1 | 11/13/2035 11:47:30 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:39:13 | 1 | 11/13/2035 11:47:30 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:39:13 | 1 | 11/13/2035 11:47:30 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:39:13 | 1 | 11/13/2035 11:47:30 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:39:12 | 1 | 11/13/2035 11:47:29 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:1194 using UDP |
| 00:39:12 | 1 | 11/13/2035 11:47:28 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:39:12 | 1 | 11/13/2035 11:47:28 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:39:12 | 1 | 11/13/2035 11:47:28 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:39:12 | 1 | 11/13/2035 11:47:28 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:39:11 | 1 | 11/13/2035 11:47:28 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:39:10 | 1 | 11/13/2035 11:47:27 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:39:04 | 1 | 11/13/2035 11:47:20 | 4 - Warning | SINEMA RC has been activated. |

Se il device ha raggiunto correttamente il server in HTTPS, ha scaricato e validato configurazione e i certificati, ora non deve fare altro che connettersi in VPN. Sul log pubblicherà il messaggio "OpenVPN Started". Se dopo un certo periodo non viene ricevuta risposta dal server, il timeout di connessione scade e si entrerà nello stato di "OpenVPN terminated". In questo caso occorre verificare che:

1. La funzionalità VPN del Sinema RC server sia attiva (vedere **verifiche preliminari**)
2. Non ci sia un **firewall** sulla rete che blocchi le porte **1194 UDP e/o 5443 TCP**

N.B.: di default il device tenta la connessione prima sulla porta UDP e poi sulla porta TCP

Download failed because of mismatch in fallback (Connessione fallita su procedura di Fallback).

Se il dispositivo si è già connesso al server, può capitare che a causa del cambio di certificato debba usare la **procedura di fallback per aggiornare il fingerprint e caricare il nuovo certificato**.

Se la procedura non va in porto correttamente, il device non può collegarsi e sul log verrà riportato il relativo messaggio di errore.

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:52:34 | 1 | 11/13/2020 11:54:13 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:52:32 | 1 | 11/13/2020 11:54:12 | 6 - Info | SINEMA RC - OpenVPN connection established. |
| 00:52:32 | 1 | 11/13/2020 11:54:11 | 6 - Info | SINEMA RC - Received initial routes from server. Routing tables and automatic firewall rules configured. |
| 00:52:28 | 1 | 11/13/2020 11:54:07 | 6 - Info | SINEMA RC - OpenVPN started. |
| 00:52:28 | 1 | 11/13/2020 11:54:07 | 6 - Info | SINEMA RC - Trying to connect to 192.168.3.3:1194 using UDP |
| 00:52:27 | 1 | 11/13/2020 11:54:06 | 6 - Info | SINEMA RC - Starting new OpenVPN connection. |
| 00:52:27 | 1 | 11/13/2020 11:54:06 | 6 - Info | SINEMA RC - Configuration download successful. |
| 00:52:27 | 1 | 11/13/2020 11:54:06 | 6 - Info | SINEMA RC - Fingerprint already checked before config download |
| 00:52:27 | 1 | 11/13/2020 11:54:06 | 6 - Info | SINEMA RC - Check fingerprint before connecting to server successful |
| 00:52:27 | 1 | 11/13/2020 11:54:06 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:52:23 | 1 | 11/13/2020 11:54:03 | 2 - Critical | SINEMA RC: Device configuration has been changed. |
| 00:52:21 | 1 | 11/13/2020 11:54:00 | 6 - Info | SINEMA RC - New CA information ready for installation. |
| 00:52:18 | 1 | 11/13/2020 11:53:58 | 6 - Info | SINEMA RC - CA update download thread started |
| 00:52:17 | 1 | 11/13/2020 11:53:57 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. |
| 00:52:17 | 1 | 11/13/2020 11:53:57 | 6 - Info | SINEMA RC - Server fingerprint: <E9:2C:B2:39:6F:F6:26:0F:F5:05:A9:C4:C9:E4:63:3A:B2:E F:DA:8E:9E:9C:25:F1:F1:D5:36:58:8B:C0:DA:13> |
| 00:52:17 | 1 | 11/13/2020 11:53:57 | 6 - Info | SINEMA RC - Configured fingerprint: <9F:5D:30:88:AD:F4:C2:13:59:D7:59:41:7E:E2:33:C4:1 3:8C:35:56:C1:81:4B:B8:D0:6D:AF:9A:87:CF:C5:96> |
| 00:52:17 | 1 | 11/13/2020 11:53:57 | 4 - Warning | SINEMA RC - Fingerprint verification failed! |

Se la procedura di fallback non è avvenuta correttamente verificare che:

1. Il dispositivo si sia **connesso almeno una volta** a quello specifico server

| System Up Time | Restart | System Time | Severity | Log Message |
|----------------|---------|---------------------|--------------|--|
| 00:23:59 | 1 | 11/13/2020 11:32:41 | 2 - Critical | SINEMA RC - Download failed because of mismatch in fallback info! Start reading fallback info caused on plug. It can take up to 2 minutes. |
| 00:23:59 | 1 | 11/13/2020 11:32:40 | 4 - Warning | SINEMA RC - No fallback information found on device. |
| 00:23:59 | 1 | 11/13/2020 11:32:40 | 6 - Info | SINEMA RC - CA update download thread started |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Server fingerprint: <DF:94:AB:12:80:DA:31:CA:A4:30:42:E2:64:72:8D:96:26:F0:51:96> |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Configured fingerprint: <DD:94:AB:12:80:DA:31:CA:A4:30:42:E2:64:72:8D:96:26:F0:51:96> |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 4 - Warning | SINEMA RC - Fingerprint verification failed! |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Precheck fingerprint: curl easy perform done (server 192.168.3.3:443) |
| 00:23:58 | 1 | 11/13/2020 11:32:39 | 6 - Info | SINEMA RC - Checking server fingerprint |
| 00:23:56 | 1 | 11/13/2020 11:32:37 | 2 - Critical | SINEMA-RC: Device configuration has been changed. |
| 00:23:50 | 1 | 11/13/2020 11:32:31 | 4 - Warning | SINEMA RC has been activated. |

Se il device non si è connesso infatti non ha le informazioni per effettuare la procedura di fallback e scaricare il nuovo certificato VPN.

2. Il System time sia **sincronizzato** con quello del server

| Event Log Security Log Firewall Log | | | | | |
|-------------------------------------|---------|---------------------|--------------|---|--|
| Severity Filters | | | | | |
| <input type="checkbox"/> Info | | | | | |
| <input type="checkbox"/> Warning | | | | | |
| <input type="checkbox"/> Critical | | | | | |
| System Up Time | Restart | System Time | Severity | Log Message | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 2 - Critical | SINEMA RC - Download failed because of mismatch in fallback info! Start reading fallback info saved on plug. It can take up to 2 minutes | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 2 - Critical | SINEMA RC - CA update configuration download failed: SSL peer certificate or SSH remote key was not OK [60] server 192.168.3.3:6220) | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - CA update download thread started | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - Server fingerprint: <EF:CE:63:F4:B5:70:1E:EF:BC:D2:A9:C8:C3:F4:F7:25:F3:17:02:D5:38:D6:95:A2:BB:E1:F6:51:87:FE:9D:0A> | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - Configured fingerprint: <E9:2C:B2:39:6F:F6:26:0F:F5:05:A9:C4:C9:E4:63:3A:B2:EF:DA:8E:9E:9C:25:F1:F1:D5:36:58:8B:C0:DA:13> | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - Fingerprint verification failed! | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - Precheck fingerprint: curl easy perform done (server 192.168.3.3:443) | |
| 01:06:44 | 1 | 11/13/2019 12:08:01 | 6 - Info | SINEMA RC - Checking server fingerprint | |
| 01:06:43 | 1 | 11/13/2019 12:08:00 | 4 - Warning | SINEMA RC has been activated. | |
| 01:06:36 | 1 | 11/13/2019 12:07:53 | 2 - Critical | SINEMA RC has been deactivated. | |

Se il device non ha il system time corretto, il nuovo certificato VPN scaricato tramite la procedura di fallback non può essere validato.

- Non ci sia un firewall sulla rete che blocchi la **porta 6220 TCP** e questa sia correttamente inoltrata lato server

| Event Log Security Log Firewall Log | | | | | |
|-------------------------------------|---------|---------------------|--------------|--|--|
| Severity Filters | | | | | |
| <input type="checkbox"/> Info | | | | | |
| <input type="checkbox"/> Warning | | | | | |
| <input type="checkbox"/> Critical | | | | | |
| System Up Time | Restart | System Time | Severity | Log Message | |
| 01:00:47 | 1 | 11/13/2020 12:02:27 | 2 - Critical | SINEMA RC - Download failed because of mismatch in fallback info! Start reading fallback info saved on plug. It can take up to 2 minutes | |
| 01:00:47 | 1 | 11/13/2020 12:02:27 | 2 - Critical | SINEMA RC - CA update configuration download failed: Timeout was reached [28] server 192.168.3.3:6220) | |
| 01:00:42 | 1 | 11/13/2020 12:02:22 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. | |
| 01:00:42 | 1 | 11/13/2020 12:02:21 | 6 - Info | SINEMA RC - Server fingerprint: <EF:CE:63:F4:B5:70:1E:EF:BC:D2:A9:C8:C3:F4:F7:25:F3:17:02:D5:38:D6:95:A2:BB:E1:F6:51:87:FE:9D:0A> | |
| 01:00:42 | 1 | 11/13/2020 12:02:21 | 6 - Info | SINEMA RC - Configured fingerprint: <E9:2C:B2:39:6F:F6:26:0F:F5:05:A9:C4:C9:E4:63:3A:B2:EF:DA:8E:9E:9C:25:F1:F1:D5:36:58:8B:C0:DA:13> | |
| 01:00:42 | 1 | 11/13/2020 12:02:21 | 4 - Warning | SINEMA RC - Fingerprint verification failed! | |
| 01:00:42 | 1 | 11/13/2020 12:02:21 | 6 - Info | SINEMA RC - Precheck fingerprint: curl easy perform done (server 192.168.3.3:443) | |
| 01:00:42 | 1 | 11/13/2020 12:02:21 | 6 - Info | SINEMA RC - Checking server fingerprint | |
| 01:00:38 | 1 | 11/13/2020 12:02:17 | 6 - Info | SINEMA RC - CA update download thread started | |
| 01:00:37 | 1 | 11/13/2020 12:02:16 | 4 - Warning | SINEMA RC - Download failed because of mismatch in fingerprint or server certificate! Trying fallback port. | |
| 01:00:37 | 1 | 11/13/2020 12:02:16 | 6 - Info | SINEMA RC - Server fingerprint: <EF:CE:63:F4:B5:70:1E:EF:BC:D2:A9:C8:C3:F4:F7:25:F3:17:02:D5:38:D6:95:A2:BB:E1:F6:51:87:FE:9D:0A> | |
| 01:00:37 | 1 | 11/13/2020 12:02:16 | 6 - Info | SINEMA RC - Configured fingerprint: <E9:2C:B2:39:6F:F6:26:0F:F5:05:A9:C4:C9:E4:63:3A:B2:EF:DA:8E:9E:9C:25:F1:F1:D5:36:58:8B:C0:DA:13> | |
| 01:00:36 | 1 | 11/13/2020 12:02:16 | 4 - Warning | SINEMA RC - Fingerprint verification failed! | |
| 01:00:36 | 1 | 11/13/2020 12:02:16 | 6 - Info | SINEMA RC - Precheck fingerprint: curl easy perform done (server 192.168.3.3:443) | |
| 01:00:36 | 1 | 11/13/2020 12:02:16 | 6 - Info | SINEMA RC - Checking server fingerprint | |

Se la connessione sulla porta di fallback è bloccata o non instradata correttamente, il collegamento al server andrà in timeout e non sarà possibile scaricare il nuovo certificato.

Connessione ai dispositivi a valle dello Scalance

Può capitare che, nonostante la connessione VPN sia stata stabilita correttamente, permangano dei problemi di connessione ai dispositivi che si trovano in campo, a valle dello Scalance.

Se tali problemi risultano dall'uso di programmi o protocolli applicativi, conviene innanzitutto tentare di raggiungere con un *ping* tali dispositivi per escludere un problema applicativo. Se il dispositivo risponde al *ping*, la connessione VPN al device e l'indiradamento al device sono sicuramente attivi.

Se il dispositivo non risponde al *ping*, conviene utilizzare la funzionalità di DCP Discovery per scansionare la rete. Tale funzionalità (in System → DCP Discovery) permette di visionare tutti i device di automazione che sono effettivamente connessi allo Scalance in VLAN1 con i relativi indirizzi.

Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)

Timeout[s]: 5

Blink Own LEDs

Interface: vlan1

Discover

| Port | MAC Address | Device Type | Device Name | IP Address | Mask Address | Gateway Address | Name Status | IP Status |
|------|-------------------|-----------------|-----------------|----------------|---------------|-----------------|-------------|---------------|
| P1 | 00-1b-1b-13-3c-a1 | S7-1500 | plcxb1d0ed | 192.168.1.7 | 255.255.255.0 | 192.168.1.7 | Discovered | Discovered/IP |
| P1 | 00-1b-1b-e7-c6-66 | SCALANCE XB-200 | plppo | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | Discovered | Discovered/IP |
| P1 | 00-1b-1b-f5-4c-1f | SIMATIC-PC | nico-pc | 172.16.100.104 | 255.255.255.0 | 0.0.0.0 | Discovered | Discovered/IP |
| P1 | 02-1b-1b-91-00-01 | SIMATIC-PC | desktop-rrfc5g2 | 169.254.142.27 | 255.255.0.0 | 0.0.0.0 | Discovered | Discovered/IP |
| P1 | 08-00-27-35-0a-59 | SIMATIC-PC | desktop-rrfc5g2 | 192.168.1.145 | 255.255.255.0 | 0.0.0.0 | Discovered | Discovered/IP |
| P1 | 20-87-56-1d-0d-4a | SCALANCE XC-200 | | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | None | Discovered/IP |
| P1 | 28-63-36-0a-6b-37 | SIMATIC-HMI | hmixbdemo5661 | 192.168.1.216 | 255.255.255.0 | 0.0.0.0 | Discovered | Discovered/IP |
| P1 | d4-f5-27-34-87-c8 | SCALANCE W-700 | | 192.168.1.8 | 255.255.255.0 | 192.168.1.1 | None | Discovered/IP |

8 entries.

Set Values Refresh

N.B. dalla versione 6.3 di Scalance S615/M800 è possibile realizzare la scansione anche con la combinazione di TIA Cloud Connector e la funzionalità "nodi accessibili" Step 7 (vedere l'apposita guida per ulteriori informazioni).

Se è un device non risponde al DCP è anche possibile provare a pingarlo localmente con la funzionalità di ping che si trova in System → Ping.

Se il device non è presente nella lista della scansione è probabile che sia fisicamente scollegato, se invece è presente è possibile verificare che i parametri di rete siano corretti. E' possibile che lo si stia cercando con un indirizzo sbagliato o duplicato oppure non abbia il default gateway corretto.

Nel caso tramite la pagina DCP Discovery si possono apportare modifiche necessarie dei parametri: **Device Name, IP Address, Mask Address e Gateway Address.**

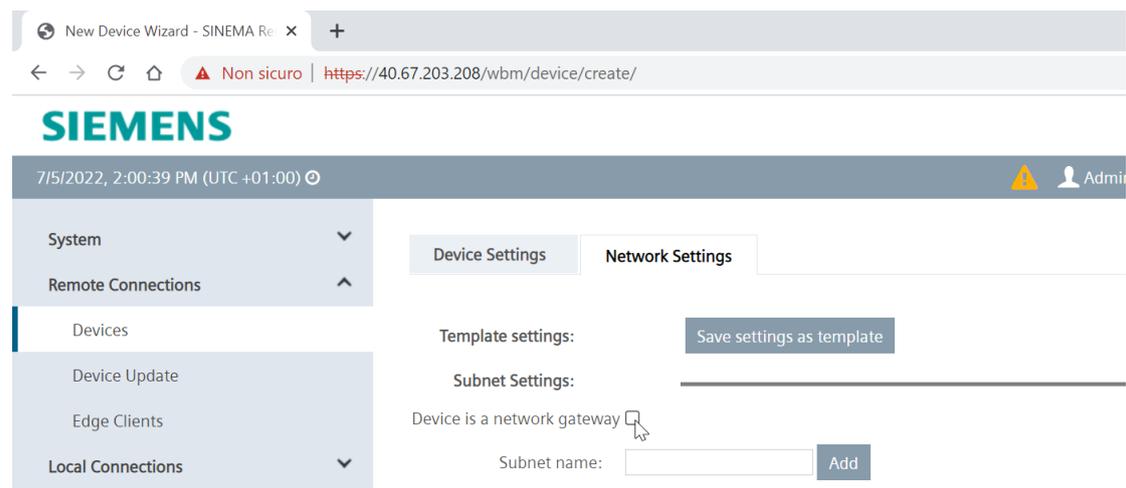
Molto spesso capita che il device in campo non abbia il **default gateway che punta correttamente al dispositivo Scalance** connesso in VPN. In questo caso tutte le richieste che arrivano dalla VPN come quelle tramite il Sinema RC Client si presentano con indirizzi IP sconosciuti al device in campo che, senza il corretto gateway, non potrà quindi rispondere a queste richieste che andranno di conseguenza in time-out.

Come detto precedentemente, è possibile utilizzare direttamente la funzionalità di DCP Discovery o TIA Cloud Connector per impostare correttamente il gateway.

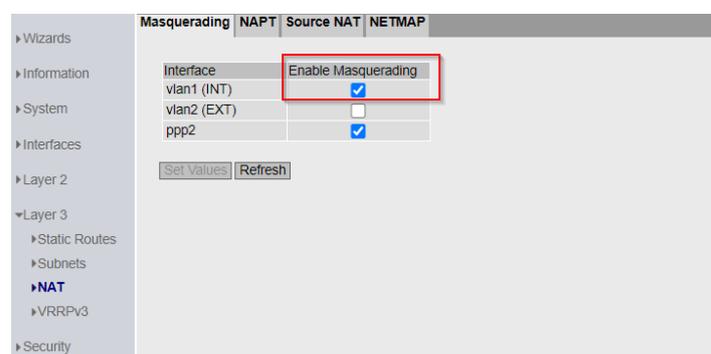
Talvolta però non è possibile andare a modificare il gateway sui devices, perché o il sistema è già in campo e non può essere riprogrammato oppure perché per altre applicazioni il gateway deve per forza puntare verso un indirizzo che non è la VLAN1 dello scalance S615.

In questo caso esistono due vie alternative che consentono la teleassistenza anche verso questi dispositivi.

La prima è quella di mascherare le connessioni in ingresso dalla VPN con l'indirizzo dello Scalance. Questo può essere fatto semplicemente **eliminando la spunta "Device is a network gateway"** nella configurazione del device in **Sinema RC Server**



In alternativa è possibile **abilitare il masquerading sulla VLAN1** direttamente sul device Scalance (vedere guida apposita per ulteriori informazioni)



Settaggi lato Sinema RC Client

Ricordiamoci che quando viene programmato un nuovo device sul Sinema RC server, nei parametri di rete, il sistema consente di inserire una sottorete interna uguale o sovrapponibile ad uno Scalance già presente solo se si prevede anche una sottorete nattata 1:1 (anche quest'ultima non può risultare sovrapponibile con sottoreti già presenti nei parametri di rete dei device programmati).

Solo se si inserisce un nuovo device con una sottorete non ancora presente e prevista per un altro scalance si può "evitare" il settaggio della rete nattata.

Questa funzionalità di NAT è presente poichè dal Client si ha anche la possibilità di potersi connettere a più Scalance contemporaneamente. Questo non sarebbe possibile se anche solo due dispositivi avessero degli indirizzi sovrapposti.

Quando dal Client si crea la connessione cliccando **ALLOW COMMUNICATION "Yes"**, si raggiungeranno tutti i devices (è possibile selezionarne più di uno) **con gli indirizzi virtuali che sono stati assegnati in fase di creazione del device in Sinema RC**

The screenshot shows the SINEMA Remote Connect Client interface. At the top, there's a navigation bar with 'SIEMENS' logo, 'SINEMA Remote Connect Client', and options for 'English', 'Logout', and help icons. Below this is a menu with 'Account', 'Server Profiles', and 'Settings'. The 'Account' section is active, displaying 'SINEMA Remote Connect Account' details: 'SINFMA RC URL: srcctest.westeurope.cloud app.azure.com', 'VPN address: 172.30.0.11', and 'Logged in as: Linda'. The 'NAT status' is 'None'. A 'CONNECTED' status is shown with a green icon and a 'Disconnect' button. Below this is the 'Device list' section, which includes a search bar and a 'Connect all devices' button. The table below lists devices with columns for Device name, VPN address, Location, Subnet name, Remote subnet, Virtual subnet, Node name, Node address, Node virtual address, Status, and Allow communication. The 'Allow communication' column has 'NO', 'YES', and 'NAT' options. The 'YES' option is selected for the device 'MACCHINA'.

| Device name | VPN address | Location | Subnet name | Remote subnet | Virtual subnet | Node name | Node address | Node virtual address | Status | Allow communication |
|-------------|-------------|----------|-------------|-----------------|----------------|-----------|--------------|----------------------|--------|---------------------|
| MACCHINA | 172.30.0.7 | | Rete1 | 192.168.10.0/24 | 172.18.10.0/24 | | | | ONLINE | NO YES NAT |
| | | | Rete2 | 192.168.52.0/24 | 172.21.52.0/24 | | | | | |

Solitamente nel caso di teleassistenza si vuole raggiungere un solo device alla volta.

Questo è possibile con la configurazione **ALLOW COMMUNICATION "NAT"**, dove si utilizzano sempre **gli indirizzi IP reali** per raggiungere i device. La spunta NAT sul CLIENT è possibile su un solo device.

SIEMENS SINEMA Remote Connect Client

English | Logout | ?

Account | Server Profiles | Settings

SINEMA Remote Connect Account

SINEMA RC URL: [srcctest.westeurope.cloud](#) app.azure.com | VPN address: 172.30.0.11 | **CONNECTED** | Disconnect

Logged in as: Linda | NAT status: Device specific (DEXpneumax)

Device list

All | Search | Search | Refresh | Connect all devices

| Device name | VPN address | Location | Subnet name | Remote subnet | Virtual subnet | Node name | Node address | Node virtual address | Status | Allow communication |
|-------------|-------------|----------|-------------|-----------------|----------------|-----------|--------------|----------------------|--------|---------------------|
| Macchina | 172.30.0.7 | | Rete1 | 192.168.10.0/24 | 172.18.10.0/24 | | | | ONLINE | NO YES NAT |
| | | | Rete2 | 192.168.52.0/24 | 172.21.52.0/24 | | | | | |

È possibile talvolta dimenticarsi la configurazione corretta e cercare di raggiungere i device con gli indirizzi non corretti. **Verificare sempre di aver impostato la modalità NAT se necessaria.**

Infine, si ricorda sempre che se si deve selezionare l'interfaccia di rete (ad esempio su Step 7) è importante **selezionare la scheda di rete corretta**. Le connessioni di Sinema RC Client escono infatti dalla scheda di rete virtuale denominata come **"TAP-Windows Adapter V9"**.

Connessioni di rete

Pannello di controllo > Rete e Internet > Connessioni di rete >

Organizza ▾

- Bluetooth Network Connection**
Disabilitata
Bluetooth Device (Personal Area ...
- Ethernet**
Cavo di rete scollegato
Intel(R) Ethernet Connection (6) I2...
- Ethernet 3** (highlighted)
Unidentified network
TAP-Windows Adapter V9
- vEthernet (Default Switch)**
ad001.siemens.net
Hyper-V Virtual Ethernet Adapter
- Wi-Fi**
ad001.siemens.net
Intel(R) Wireless-AC 9560 160MHz

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.