



HOW TO

Prima configurazione Sinema Remote Connect

SIEMENS

Contents

Prima configurazione Sinema Remote Connect	3
Prima Connessione da pagina Web	3
Configurazioni opzionali	9

Prima configurazione Sinema Remote Connect

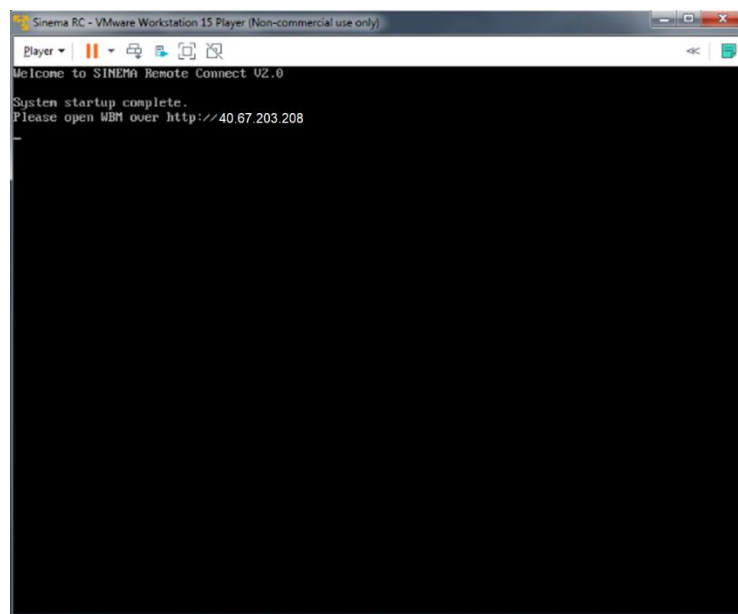
La seguente guida illustra come configurare il software Sinema RC Server nella fase immediatamente successiva all'installazione.

Per l'installazione di Sinema RC Server su macchina fisica o virtuale si può fare riferimento alle apposite guide. Questa guida è redatta con la versione di Sinema RC Server 3.1

Per la parametrizzazione dei servizi e la pubblicazione del server online si osservi la sezione finale "Considerazioni sul Port Forwarding" al termine del documento.

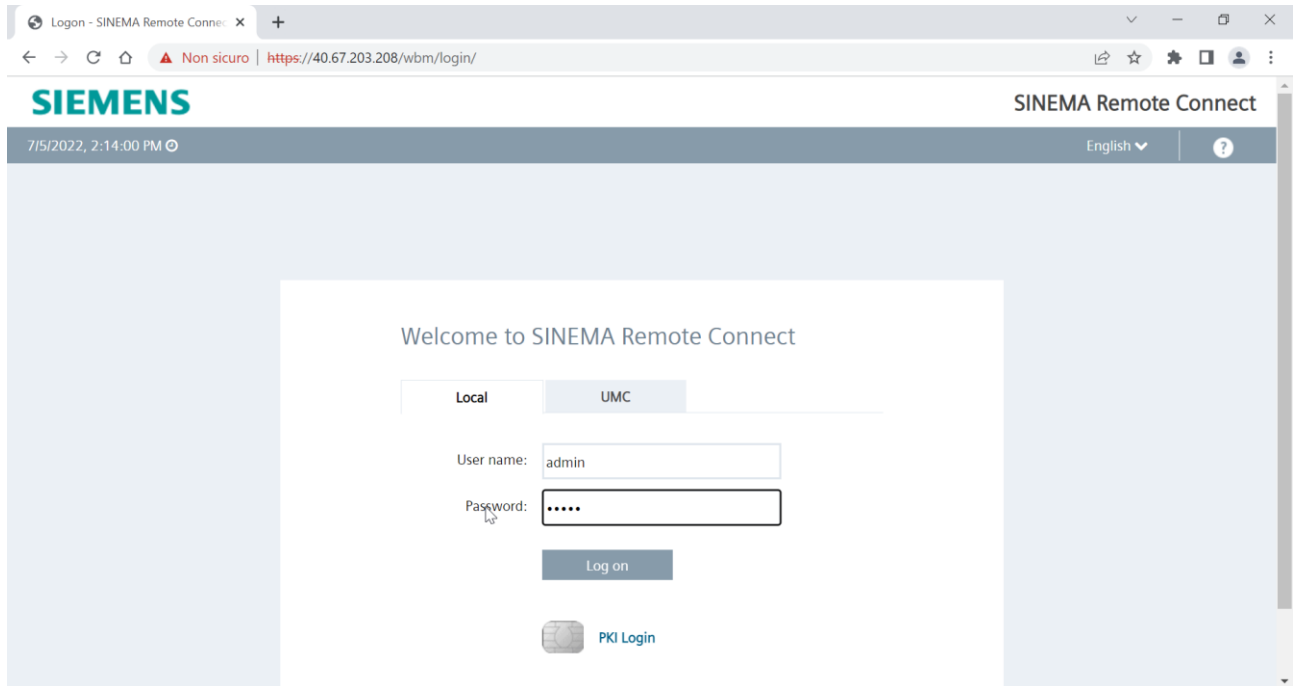
Prima Connessione da pagina Web

Una volta installato il Sinema RC è possibile connettersi al server stesso mediante l'indirizzo IP configurato nella fase di installazione come indicato sulla console.

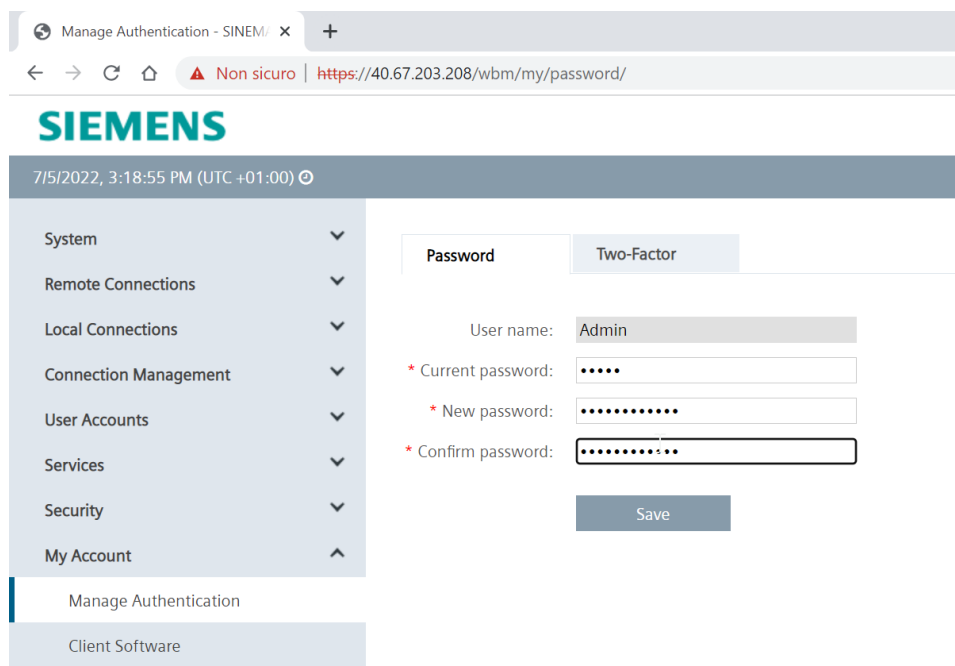


La connessione è possibile solo in HTTPS (<https://x.y.z.m> dove x.y.z.m è il suddetto IP configurato) su porta 443 (successivamente è possibile cambiare la porta) essendo il certificato di tipo "self-signed" verrà richiesto di accettare la connessione untrusted (nell'esempio di Chrome occorre cliccare su "Continue..." ma per ogni browser è diverso).

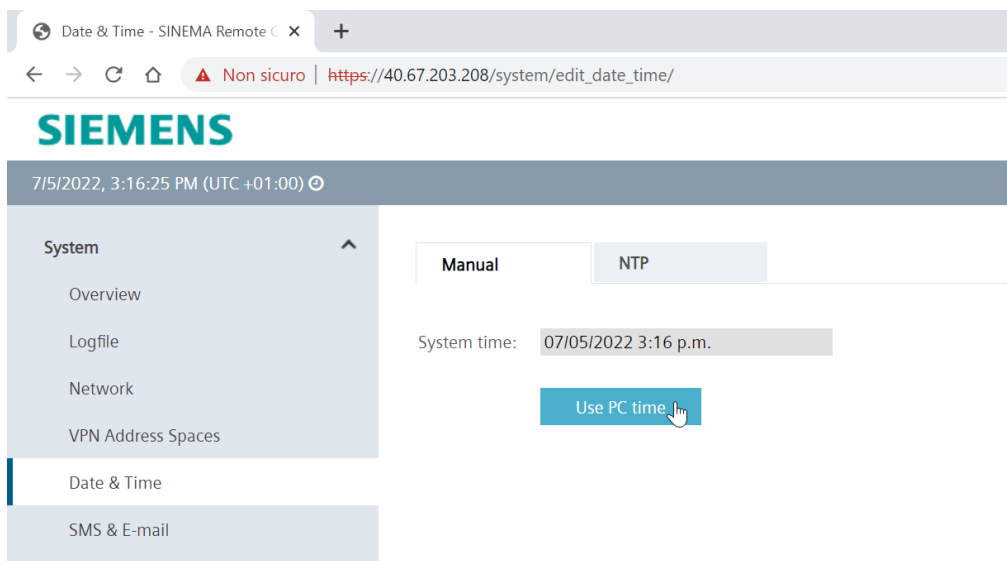
Accettata la connessione la pagina web si presenta per il login (default user: admin, Password: admin)



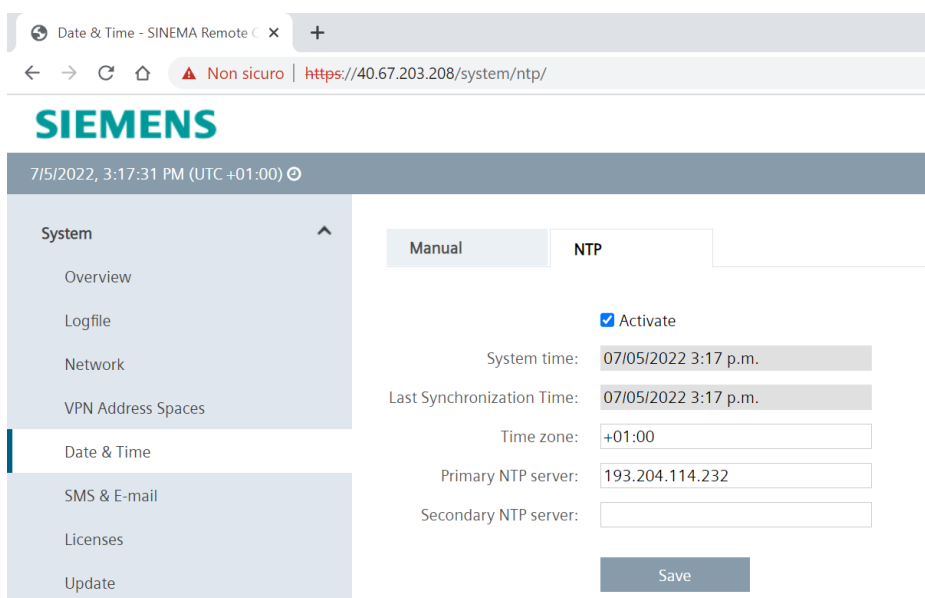
Come si entra viene forzato il cambio di User e Password.



La schermata successiva richiede l'impostazione dell'ora (fondamentale per l'instaurazione delle connessioni VPN), quantomeno va impostata manualmente da "System" → "Date & Time" da tab "Manual" cliccare su "Use PC Time".



Se possibile aggiungere un eventuale indirizzo di server NTP dalla tab "NTP" (nell'esempio sono stati utilizzati gli indirizzi dell'INRIM. Istituto Nazionale di Ricerca Metrologica) con relativa time zone e cliccare sul flag "Activate".



La schermata successiva riguarda la configurazione di rete. Su System → Network è possibile cambiare l'indirizzo IP o il gateway della rete locale nonché aggiungere l'indirizzo IP pubblico dopo aver spuntato su "SINEMA Remote Connect is located behind a NAT device".

Network - SINEMA Remote Conn x +

Non sicuro | <https://40.67.203.208/system/network/interfaces/>

7/5/2022, 3:21:05 PM (UTC +01:00) Admin English

System

- Overview
- Logfile
- Network**
 - VPN Address Spaces
 - Date & Time
 - SMS & E-mail
 - Licenses
 - Update
 - Backup & Restore
 - Power Management
 - Settings
 - Remote Connections
 - Local Connections

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

Warning: 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: 60:45:bd:87:d4:42

MTU: 1460

Use DHCP:

IP address: 10.0.0.53

Network mask: 255.255.255.0

Default gateway: 10.0.0.1

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

WAN IP address:

Dopodichè è sufficiente cliccare su "Save".

Network - SINEMA Remote Conn x +

Non sicuro | <https://40.67.203.208/system/network/interfaces/>

SMS & E-mail

Licenses

Update

Backup & Restore

Power Management

Settings

Remote Connections

Local Connections

Connection Management

User Accounts

Services

Security

My Account

Interface: **WAN**

MAC address: 60:45:bd:87:d4:42

MTU: 1460

Use DHCP:

IP address: 10.0.0.53

Network mask: 255.255.255.0

Default gateway: 10.0.0.1

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

WAN IP address: 19.18.17.16

Activate IPv6:

Use SLAAC for IPv6:

IPv6 Address:

Link-local IPv6 address:

Subnet prefix length:

Default gateway:

Save

Successivamente nella pagina System → Network nel tab DNS è possibile fare due cose:

- a. Inserire i DNS (Nell'esempio sono stati utilizzati gli indirizzi di Google: 8.8.8.8 e 8.8.4.4). Questi sono assolutamente necessari per poter inserire le licenze del Sinema RC o sincronizzarsi con un NTP server indicato attraverso un hostname.

Network - SINEMA Remote Conn x +

Non sicuro | <https://40.67.203.208/system/network/dns/>

SIEMENS SINEMA

7/5/2022, 3:23:10 PM (UTC +01:00) Admin English

System

- Overview
- Logfile
- Network
- VPN Address Spaces
- Date & Time
- SMS & E-mail
- Licenses
- Update
- Backup & Restore
- Power Management

Interfaces DNS Web Server Settings Ping Static Routes

! If you change the host name, existing connections to devices / users will be terminated and the Web server will be temporarily unreachable!

* Host name:

Externally resolvable host name.

Primary DNS server:

Secondary DNS server:

Save

- b. **Opzionale**, se disponibile (**si raccomanda comunque di farlo onde facilitare il passaggio a un diverso indirizzo pubblico**) inserire un Hostname DNS per il server (es.: sinemarc.example.com). Tale nome deve essere risolto esternamente (ovvero dal router dietro a cui è posizionato il Sinema RC Server) previo il clic sulla spunta "Externally resolvable host name" e cliccare su Save.

Network - SINEMA Remote Conn x +

Non sicuro | <https://40.67.203.208/system/network/dns/>

SIEMENS SINEMA

7/5/2022, 3:24:19 PM (UTC +01:00) Admin English

System

- Overview
- Logfile
- Network
- VPN Address Spaces
- Date & Time
- SMS & E-mail
- Licenses
- Update
- Backup & Restore
- Power Management

Interfaces DNS Web Server Settings Ping Static Routes

! If you change the host name, existing connections to devices / users will be terminated and the Web server will be temporarily unreachable!

* Host name:

Externally resolvable host name.

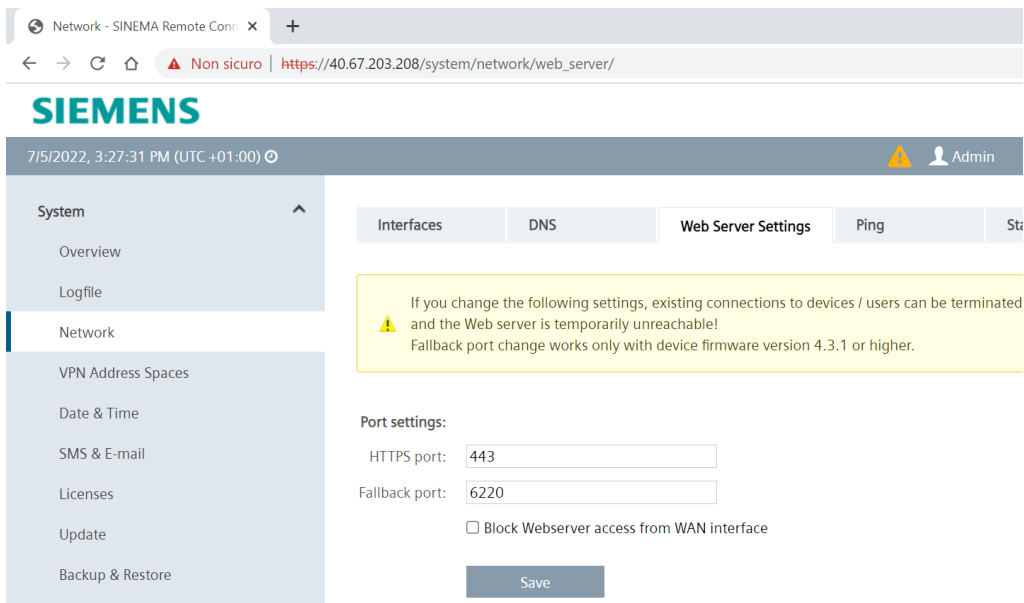
Primary DNS server:

Secondary DNS server:

Save

Nota Bene: se si imposta un hostname pubblico è anche possibile non impostare alcun IP pubblico statico (è sufficiente solo uno dei due per rendere il certificato valido e il server raggiungibile dall'esterno).

Infine nel tab "Web Server Settings" è possibile cambiare le porte del Web Server (ad esempio se sono già occupate da altre applicazioni che convivono sull'indirizzo IP pubblico) i default sono 443 TCP per HTTPS e 6220 TCP per la procedura di fallback (rinnovo automatico dei certificati in caso di connessione successiva alla scadenza).



The screenshot shows the Siemens web management interface. The browser address bar indicates a non-secure connection to https://40.67.203.208/system/network/web_server/. The page header includes the Siemens logo, the date and time (7/5/2022, 3:27:31 PM UTC +01:00), and the user name (Admin). The left sidebar contains a menu with options: System, Overview, Logfile, Network, VPN Address Spaces, Date & Time, SMS & E-mail, Licenses, Update, and Backup & Restore. The main content area has tabs for Interfaces, DNS, Web Server Settings, Ping, and Sta. The "Web Server Settings" tab is active, displaying a warning message: "If you change the following settings, existing connections to devices / users can be terminated and the Web server is temporarily unreachable! Fallback port change works only with device firmware version 4.3.1 or higher." Below the warning, the "Port settings" section includes input fields for "HTTPS port" (443) and "Fallback port" (6220), and a checkbox for "Block Webserver access from WAN interface" which is currently unchecked. A "Save" button is located at the bottom of the settings section.

Da questo momento in poi è terminato il Wizard ed è possibile muoversi liberamente sul menù e la configurazione può dirsi eseguita.

Configurazioni opzionali

Oltre alle configurazioni di base è possibile portare una serie di modifiche al Sinema RC server per il suo funzionamento:

- Ad esempio, è possibile cambiare le porte di comunicazione per OpenVPN (default 1194 UDP e 5443 TCP) su "Security" → "OpenVPN"

The screenshot shows the 'OpenVPN basic settings' page in the SINEM web interface. The browser address bar shows the URL <https://40.67.203.208/vpn/openvpn/>. The left sidebar contains a navigation menu with categories like System, Remote Connections, Local Connections, Connection Management, User Accounts, Services, Security, and My Account. The 'Security' category is expanded, showing 'General' (with a warning icon), 'Certificate Management', 'OpenVPN', 'IPsec', 'PKI Management', and 'Syslog Management'. The 'OpenVPN' section is selected, displaying the following settings:

- Activate
- Status: Executing
- TCP port: 5443
- UDP port: 1194
- Keep alive interval (s): 20
- Connection timeout (s): 60
- DH key length: 2048
- Cipher: AES-128
- Hash method: SHA 256
- Min. TLS version: 1.2
- Interface: WAN

A yellow warning box at the top of the settings area states: "If you change the following settings, any connections to devices / users may be terminated!". A 'Save' button is located at the bottom right of the settings area.

Nota bene: per le impostazioni sulle porte si raccomanda di seguire la guida apposita

- Oppure è possibile allungare la scadenza dei certificati portandoli fino a 3650 giorni accedendo a "Security" → "Certificate Management"

Certificate Management - SINEMA x +

Non sicuro | <https://40.67.203.208/pki/settings/>

SIEMENS SINEMA Rem

7/5/2022, 3:50:17 PM (UTC +01:00) Admin English Log

System Remote Connections Local Connections Connection Management User Accounts Services Security

General Certificate Management OpenVPN IPsec

CA Certificate Web Server Certificate VPN Server Certificate Device Certificate Settings

If you change the following settings, existing certificates are not affected. You can renew certificates manually to force immediate usage of these settings.

* CA Lifetime (years): 10

* Preferred key length (bits): 2048

* Preferred hash method: SHA256

* CA certificate renewal (days before expiry): 365

* Validity of client certificates (days): 3650

Save

Per rendere effettiva la modifica occorre però rinnovare i certificati del Web Server e della VPN.

Certificate Management - SINEMA x +

Non sicuro | <https://40.67.203.208/pki/vpnsvrcert/>

System Remote Connections Local Connections Connection Management User Accounts Services Security

General Certificate Management OpenVPN IPsec PKI Management Syslog Management My Account

CA Certificate Web Server Certificate VPN Server Certificate Device Certificate Settings

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

Serial number: 15

Common name: 10.0.0.53

Issuer: CA 834972 SINEMA RC

Valid from: 09/08/2021 7:26 a.m.

Valid to: 09/10/2022 7:26 a.m.

Key length (bits): 2048

Signature method: SHA256 with RSA encryption

SHA1-Fingerprint: 3B:0D:9B:2B:5C:80:81:43:11:00:CC:F4:28:B0:E8:10:CA:A3:0A:85

SHA256-Fingerprint: 32:80:57:B1:10:C1:CD:B1:63:85:15:97:13:97:4F:1C:59:55:68:73:4E:3B:4E:72:3C:F1:F3:42:63:19:DC:BF

Alternative names:

IP: 10.0.0.53

Renew

Per ulteriori dettagli si raccomanda di seguire la guida apposita sulla gestione dei certificati

Un altro esempio è la possibilità di cambiare gli indirizzi delle subnet VPN qualora queste si sovrappongono con indirizzi già usati dai device

VPN Address Spaces - SINEMA R. x +

Non sicuro | https://40.67.203.208/system/openvpn/address_pools/

System ^

- Overview
- Logfile
- Network
- VPN Address Spaces**
- Date & Time
- SMS & E-mail
- Licenses
- Update
- Backup & Restore
- Power Management
- Settings
- Remote Connections** v
- Local Connections** v
- Connection Management** v
- User Accounts** v

Virtual Subnet
OpenVPN
IPsec

TCP address space:

Start IP address:

Network mask:

End IP address:

Use (assigned IPs / of total):

UDP address space:

Start IP address:

Network mask:

End IP address:

Use (assigned IPs / of total):

Activate fixed IP address space:

Fixed IP protocol:

Location of the fixed IP address space:

Length of the fixed IP address space:

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.