



Usare il SiteManager per connessioni attraverso una VPN

PREMESSA

La seguente guida vuole dimostrare come configurare il SiteManager per il collegamento ad una connessione diretta tramite VPN fornita dal Cliente con le rispettive credenziali (Es.Cisco).

In questo scenario non è possibile utilizzare il programma LinkManager ma è comunque possibile utilizzare il SiteManager con una configurazione apposita. Per la connessione ai dispositivi si dovrà poi utilizzare il Software Client VPN fornito dal cliente.

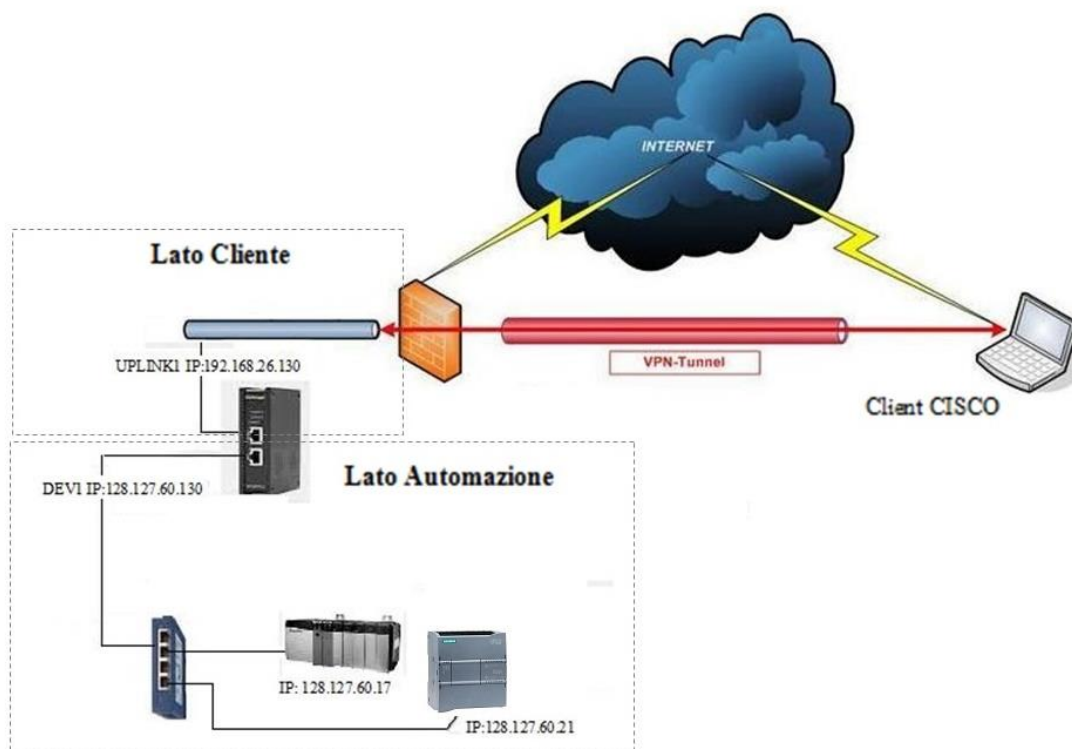


Fig.1 Esempio configurazione



Indirizzi di configurazione

Supponiamo di avere uno scenario come in Fig.1, dove abbiamo la necessità di collegarci tramite VPN a due dispositivi. Cio' che ci occorre sono: un indirizzo VPN per la porta di collegamento UPLINK1 e un indirizzo VPN per ogni dispositivo collegato alla porta DEV1 (lato Automazione). **Indirizzi che andranno forniti dal Cliente.** Nel caso in esempio serviranno quindi **tre indirizzi VPN**.

Supponiamo che il Cliente ci fornisca i seguenti indirizzi IP: 192.168.26.130 / 131 / 132, con SUBNETMASK: 255.255.255.0 e un indirizzo di Gateway: 192.168.26.5

Come nella figura di esempio (Fig.1), la configurazione di indirizzi IP sarà costituita nel seguente modo:

Porta di comunicazione UPLINK1 IP VPN: 192.168.26.130

Porta di comunicazione DEV1 IP: 128.127.60.130

PLC Rokwell: IP 128.127.60.17

PLC Siemens: IP 128.127.60.21

Ai due dispositivi sulla porta DEV1 andranno associati i seguenti indirizzi VPN:

PLC Rokwell: IP 128.127.60.17 ➔ 192.168.26.131

PLC Siemens: IP 128.127.60.21 ➔ 192.168.26.132

Nota: E' importante che tutti i dispositivi presenti nel lato macchina (PLC, HMI ecc.) abbiano come DEFAULT GATEWAY l'indirizzo IP della porta DEV1 (nel nostro esempio: 128.127.60.130).



GateManager

Configurazione SiteManager

Inserimento Indirizzo VPN su porta UPLINK1

The screenshot shows the 'UPLINK - Setup Assistant' page in the SiteManager web interface. The browser address bar shows 'https://10.0.0.1'. The page has a navigation bar with links: SETUP, System, GateManager, VPN, Routing, Maintenance, Status, Log, and HELP. The main content area contains instructions and configuration fields. A red box highlights the IP configuration section:

Mode:	Static
IP Address:	192.168.26.130
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.26.5

Below this, other settings are visible: Ethernet Settings (Autonegotiation), Priority (First), Probe Type (Any), Probe Hosts (empty), Probe Port (TCP) (80), Probe Interval A (10 seconds), and Probe Interval B (60 seconds). Buttons for 'Help' and 'Continue Setup >' are at the top right of the configuration area.

Fig.2 configurazione IP su UPLINK1

Come prima operazione entriamo nella pagina di Setup del Sitemanger attraverso la sua interfaccia WEB (<https://IP dev1>) e nella sezione UPLINK1 andiamo a inserire l'indirizzo IP VPN con relativa SUBNETMASK e GATEWAY forniti dal cliente (Fig.2).

The screenshot shows the 'SiteManager 1029 - Setup Assistant' page. It lists the current configuration status for various components:

Component	Value	Status	Action
1. GateManager:		Not configured	Fix
2. Uplink port:	192.168.26.130/24 (Fixed)	Up	Edit
3. Uplink2 (2G/3G/4G):		Not Installed	Edit
4. DEV port:	128.127.60.130/24		Edit
5. Device Agents:	1 up		Edit
6. Chat / Scratchpad:	Empty		Edit
7. Admin Password:		Using default password	Fix

Below the table, there is a note: 'You can open the Setup Assistant at any time by clicking on **SETUP** in the top menu. Note: If you click on **HELP** it shows specific help for the current configuration page. Please consult the online help as your first step in solving setup problems.'

Fig.3 Pagina SETUP a configurazione IP VPN uplink ultimata



Supporto tecnico:

tecnico@gate-manager.it



GateManager

Una volta salvato i parametri relativi alla porta UPLINK1 e DEV1 la pagina di SETUP si presenterà come in Fig.3.

Nota: Essendo la connessione VPN diretta verso il cliente e non verso il server Secomea, la sezione **1.GateManager** non va configurata.

Creazione Agent “CUSTOM Forwarding”

Per collegarsi ai dispositivi presenti sulla porta DEV1, occorre creare un Agent di tipo **CUSTOM Forwarding**.

Indirizzo <https://128.127.60.130/>

SiteManager
secomea

SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

GateManager Agents - Setup Assistant

You can configure an agent to monitor a device connected to the SiteManager Serial port and TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager.

Click [New], and give the Agent a name (this name will be what the LinkManager user will see), and select a suitable device type (first vendor, then model). Then click on to specify the device address and other relevant parameters.

The SiteManager will instantly try to connect to the device, and if successful the Agent will go IDLE and appear on the GateManager and any LinkManager that have been granted access to the domain of the SiteManager.

If not successful, the Agent will report an error, and the agent will not be registered on the GateManager and subsequently not on LinkManagers either.

[Help](#) [Continue Setup »](#)

Using 1 of 2 agents

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Comment
<input type="checkbox"/>		#00	Prt Frw	CUSTOM (Advanced) Forwarding		

[Refresh](#) [Save](#) [New](#) [SNMP >>](#)

Fig.4 Agent CUSTOM/Forwarding

Una volta creato l'Agent **CUSTOM Forwarding** (Fig.4), clicchiamo sull'editor dell'Agent per inserire le regole di Forwarding relative ai dispositivi associati.



Creazione Regole Forwarding

The screenshot shows the 'Device "Prt Frw" (Forwarding Agent) Details - Setup Assistant' window. It includes a navigation bar with 'SETUP', 'System', 'GateManager', 'VPN', 'Routing', 'Maintenance', 'Status', 'Log', and 'HELP'. The main content area contains instructions: 'When you configure an agent to monitor a TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager, you must specify the device IP address below.' and 'Click [Save] and then [Back] to make the SiteManager instantly try to connect to the device.' Below this, it states: 'If not successful, the Agent will report an error, and the agent will not be registered on the GateManager and subsequently not on LinkManagers either.' There are 'Help' and 'Continue Setup >' buttons. A table lists 10 forwarding rules. Rule 1 is selected and shows the configuration: '\$192.168.26.131:ANY:1-65535>>128'. Rule 2 shows '\$192.168.26.132:ANY:1-65535>>128'. Rules 3 through 10 are empty.

Forwarding Rule	Configuration
Forwarding Rule 1:	* \$192.168.26.131:ANY:1-65535>>128
Forwarding Rule 2:	\$192.168.26.132:ANY:1-65535>>128
Forwarding Rule 3:	
Forwarding Rule 4:	
Forwarding Rule 5:	
Forwarding Rule 6:	
Forwarding Rule 7:	
Forwarding Rule 8:	
Forwarding Rule 9:	
Forwarding Rule 10:	

Fig.5 Creazione regole forwarding

Nel nostro caso i dispositivi collegati alla porta DEV1 sono due, per cui andremo a creare due regole (Fig.5).

Regola Forwarding 1: => \$IndirizzVPN2:ANY:1-65535>>Indirizzo Agent1:1-65535

Regola Forwarding 2: => \$IndirizzoVPN3:ANY:1-65535>>IndirizzoAgent2:1-65535

Regola Forwarding n: => \$IndirizzoVPNn:ANY:1-65535>>IndirizzoAgentn:1-65535

Nel nostro caso la regola di Forwarding per i due agent sarà:

Regola Forwarding 1: => \$192.168.26.131:ANY:1-65535>>128.127.60.17:1-65535

Regola Forwarding 2: => \$192.168.26.132:ANY:1-65535>>128.127.60.21:1-65535

Nota: Confermare sempre premendo il pulsante SAVE per memorizzare le modifiche effettuate.



Creazione Associazione IP VPN (Alias)

Una volta creato l'agent con le regole di Forwarding occorre creare una associazione tra gli indirizzi IP dei dispositivi, lato DEV1, con gli indirizzi VPN (Alias). In questo modo verranno mappati ad uno ad uno gli indirizzi VPN con gli indirizzi Ip lato macchina.

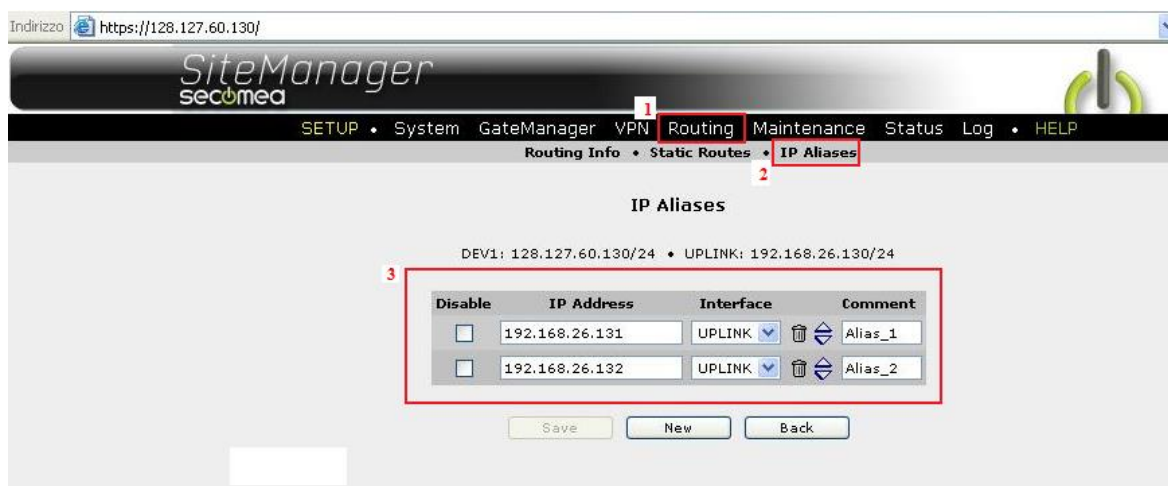


Fig.6 Creazione Alias

Per Creare gli Alias selezioniamo la voce **Routing, IP Aliases**, e creiamo un alias per ogni dispositivo associando ad ognuno il rispettivo indirizzo IP VPN (Fig.6).

Attraverso la sezione **Status / Extended** è possibile verificare le corrette impostazioni delle regole di Forwarding appena create (Fig.7).

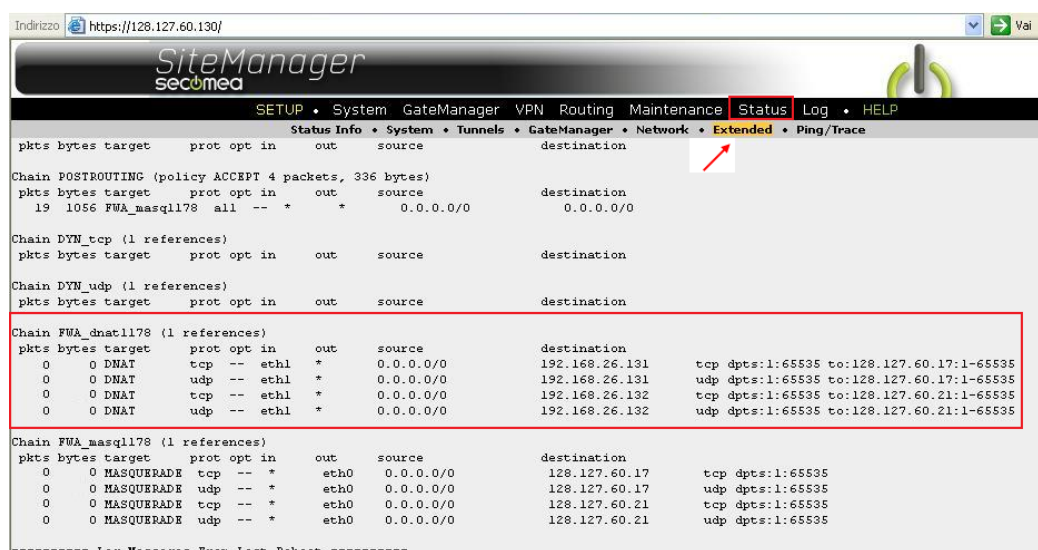


Fig.7 Verifica regole di Forwarding



Test collegamento dispositivi

La configurazione del Sitemanager per la connessione tramite accesso VPN è terminata, dato che i dispositivi usati nel nostro esempio, hanno entrambi a bordo una WebPage, come test, è possibile via Browser accedervi attraverso il loro indirizzo VPN, che corrisponderà all'indirizzo UPLINK: **192.168.26.131** e **192.168.26.132**. Indirizzi che dovremo usare anche per collegarci con il Software di automazione dei rispettivi dispositivi.

Test accesso alla WebPage del PLC Rockwell con IP VPN: 192.168.26.131



Fig.8 Test accesso WebPage PLC Rockwell



Test accesso al PLC Siemens attraverso Tia Portal

Una volta avviato Tia Portal, apriamo il progetto e nella sezione Hardware effettuiamo un doppio click sul connettore di rete del PLC (Fig.9)

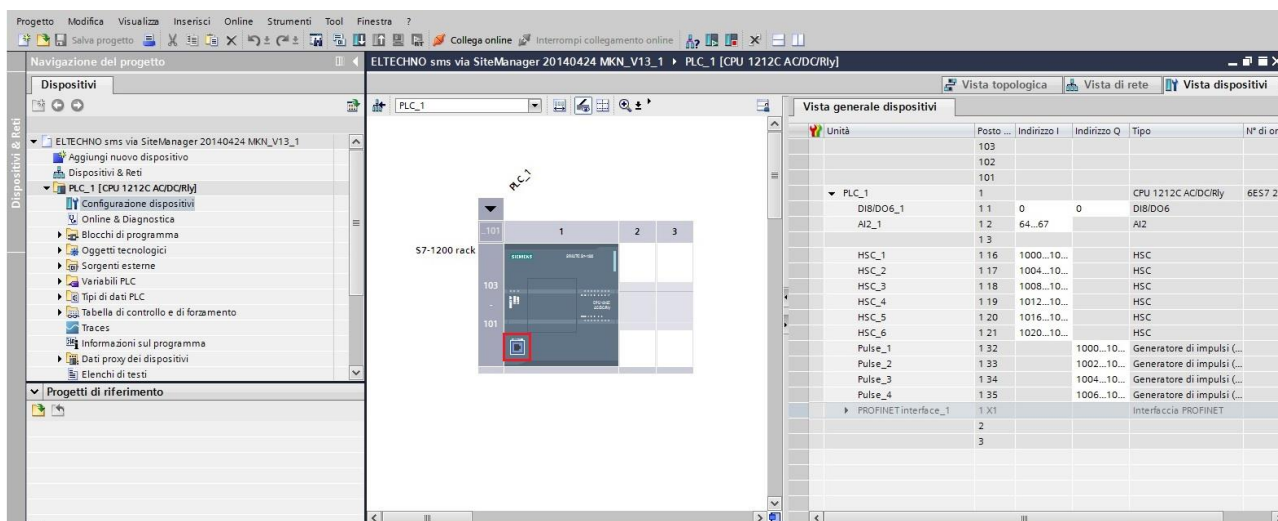


Fig.9 Configurazione Hardware PLC

Abilitare Flag “Consenti la modifica dell’Indirizzo IP direttamente nel dispositivo” per assegnare l’indirizzo VPN associato al PLC (Fig.10)

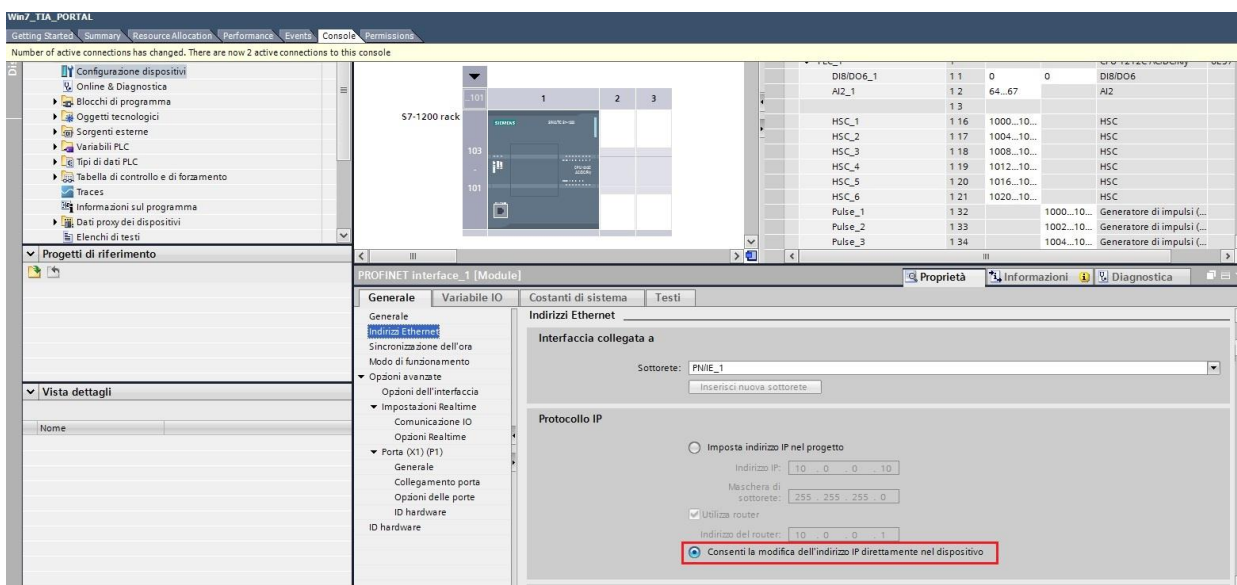


Fig.10 associazione indirizzo IP di VPN



Selezionare l'icona "Collega online" (Fig.11)

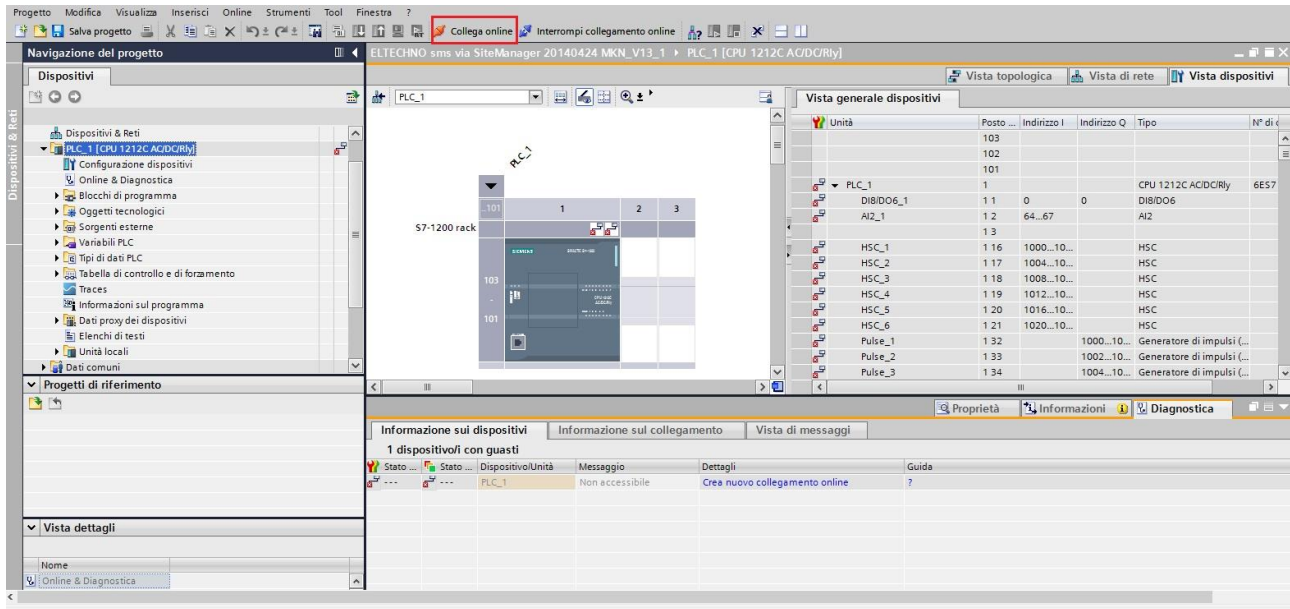


Fig.11 Selezione Icona Online

Impostare l'indirizzo IP di VPN associato al PLC e selezionare il pulsante "Avvio Ricerca" (Fig.12)

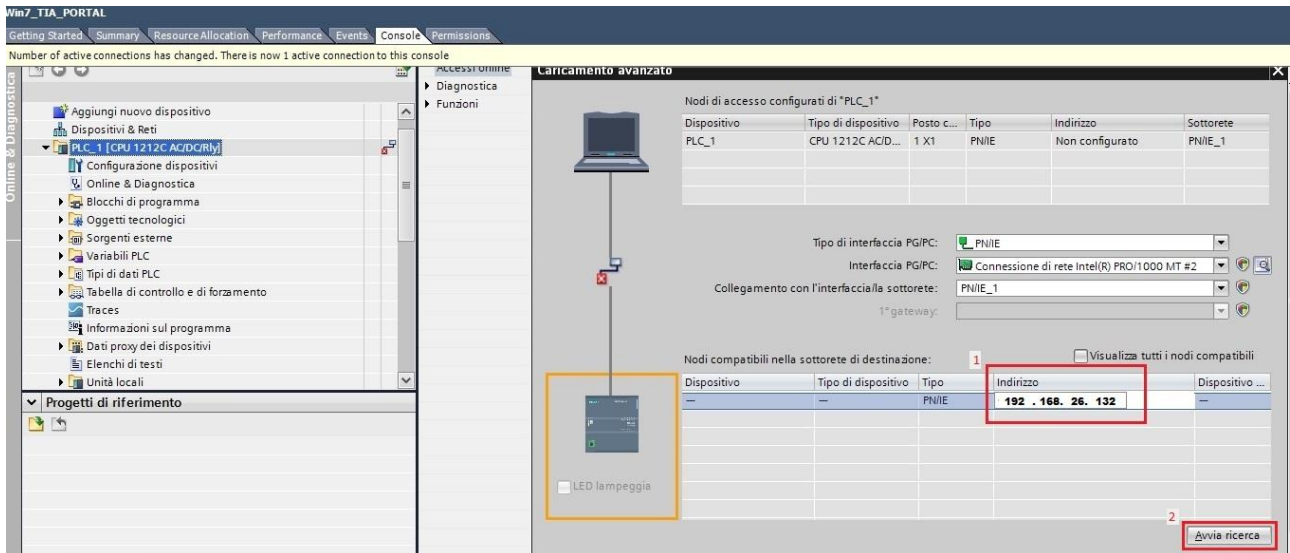


Fig.12 Inserimento IP VPN e avvio ricerca dispositivo



GateManager

Una volta visualizzato trovato il PLC, selezionare il pulsante “Carica” per andare online (Fig.13)

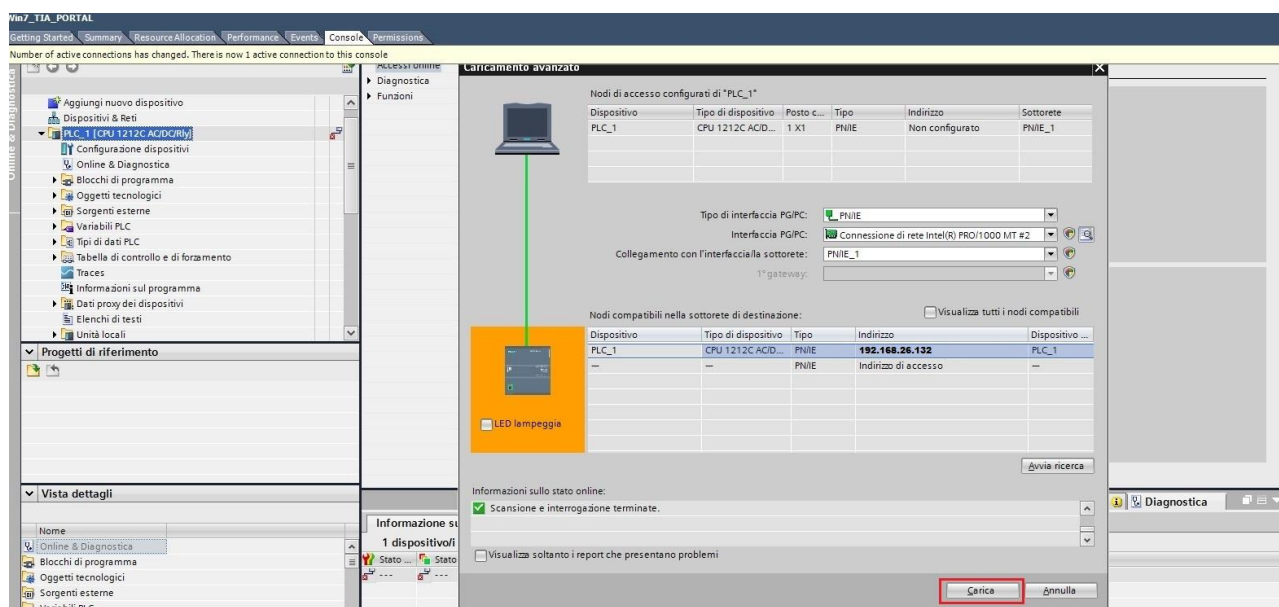


Fig.13 collegamento PLC a Tia Portal

Una volta terminata la procedura in Tia Portal, il PLC sarà collegato correttamente (Fig.14)

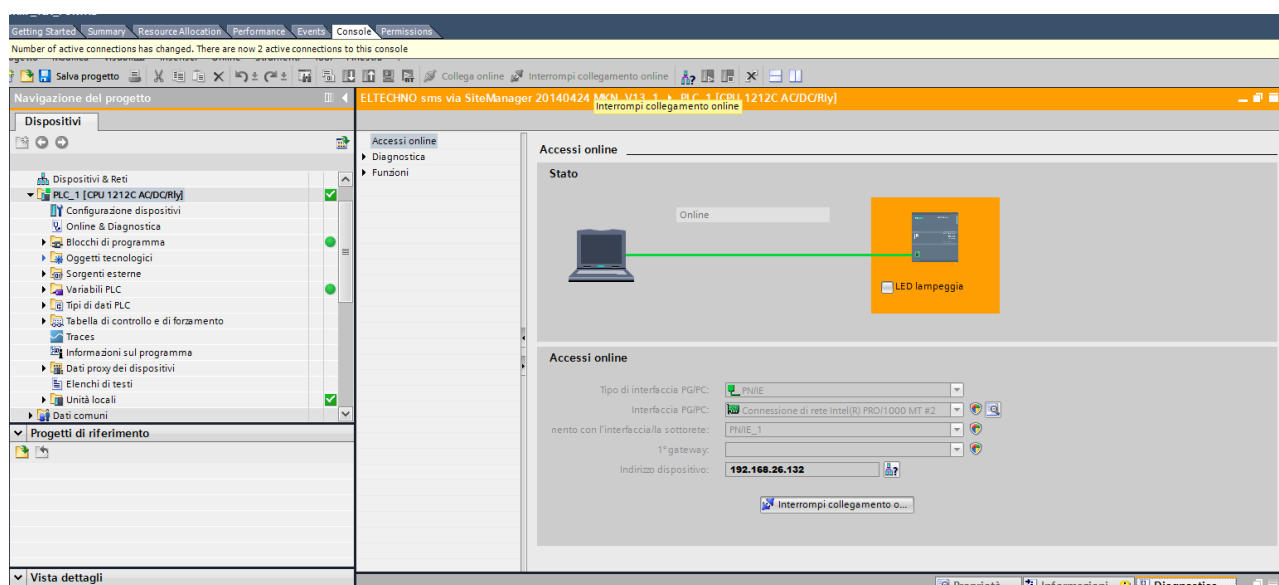


Fig.14 Collegamento al PLC tramite Tia Portal



Supporto tecnico:

tecnico@gate-manager.it




Verifica traffico Pacchetti

Nella Sezione Status/Extended del SiteManager è possibile verificare i pacchetti trasmessi (Fig.15)

Indirizzo <https://128.127.60.130/>

SiteManager
secured



SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

STATUS INFO • System • Tunnels • GateManager • Network • Extended • Ping/Trace

pkts	bytes	target	prot	opt	in	out	source	destination	
Chain POSTROUTING (policy ACCEPT 4 packets, 336 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
19	1056	FWA_masq1178	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
Chain DYN_tcp (1 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
Chain DYN_udp (1 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
Chain FWA_dnat1178 (1 references)									
7	336	DNAT	tcp	--	eth1	*	0.0.0.0/0	192.168.26.131	tcp dpts:1:65535 to:128.127.60.17:1-65535
0	0	DNAT	udp	--	eth1	*	0.0.0.0/0	192.168.26.131	udp dpts:1:65535 to:128.127.60.17:1-65535
8	384	DNAT	tcp	--	eth1	*	0.0.0.0/0	192.168.26.132	tcp dpts:1:65535 to:128.127.60.21:1-65535
0	0	DNAT	udp	--	eth1	*	0.0.0.0/0	192.168.26.132	udp dpts:1:65535 to:128.127.60.21:1-65535
Chain FWA_masq1178 (1 references)									
7	336	MASQUERADE	tcp	--	*	eth0	0.0.0.0/0	128.127.60.17	tcp dpts:1:65535
0	0	MASQUERADE	udp	--	*	eth0	0.0.0.0/0	128.127.60.17	udp dpts:1:65535
8	384	MASQUERADE	tcp	--	*	eth0	0.0.0.0/0	128.127.60.21	tcp dpts:1:65535
0	0	MASQUERADE	udp	--	*	eth0	0.0.0.0/0	128.127.60.21	udp dpts:1:65535

***** Log Messages From Last Reboot *****

Fig.15 Verifica traffico pacchetti

Troubleshooting

Come Troubleshooting e' possibile provare la configurazione in locale connettendo un PC alla porta UPLINK1, assegnando ad esso un indirizzo IP compatibile, ad esempio 192.168.26.100 e mettendo come GATEWAY l'indirizzo IP della porta UPLINK1 (Fig.16)

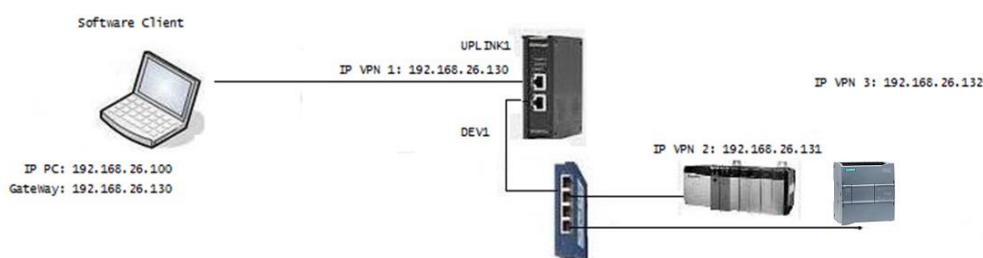


Fig.16 Test in configurazione Locale

A questo punto è possibile provare a collegarsi ai dispositivi mediante un IP Alias: 192.168.26.131 per il PLC Rockwell e 192.168.26.132 per il PLC Siemens.

IMPORTANTE:

- Con questa configurazione il protocollo FTP non è supportato.
- Con l'agent Forwarding il Ping Test non è supportato