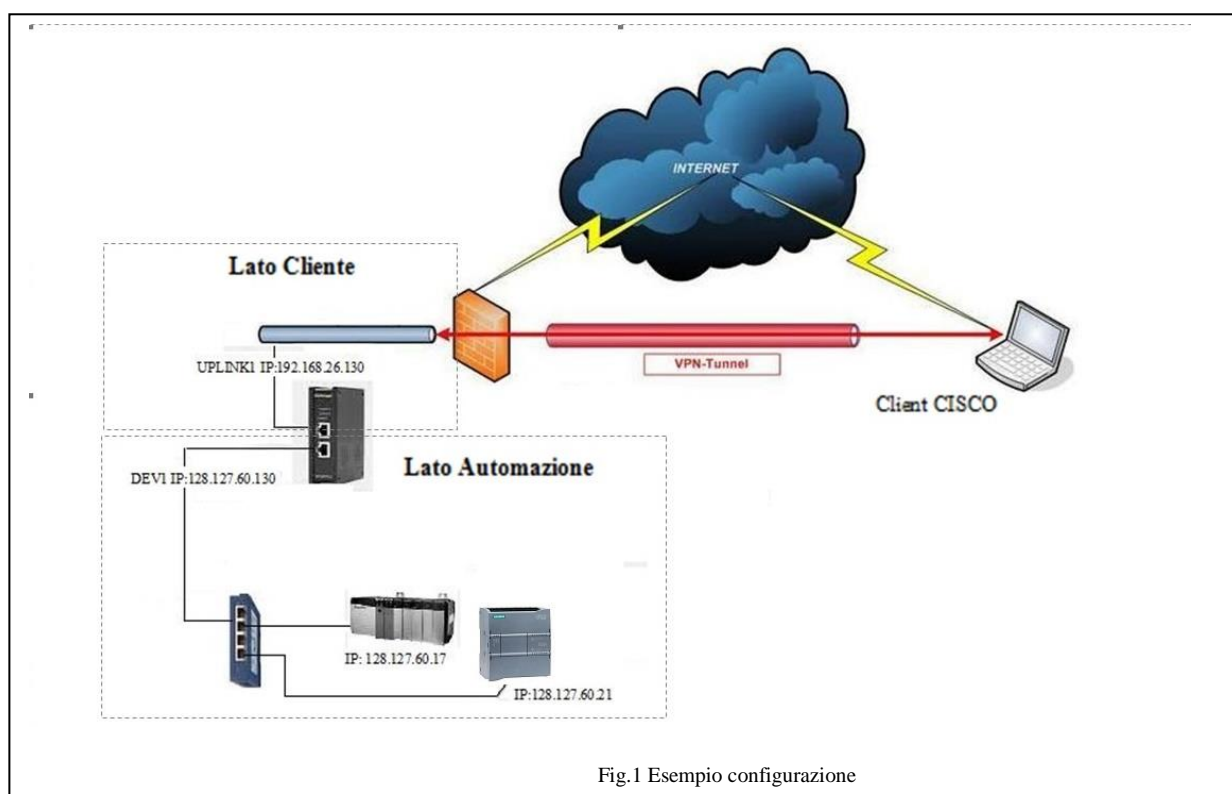




Come accedere dalla rete cliente a dispositivi sulla rete macchina con NAT 1:1

PREMESSA

Questa guida spiega come configurare il SiteManager per realizzare la funzione di **NAT 1:1**. Questa comoda funzione consente di accedere in modo trasparente a dei dispositivi della rete macchina (DEV), dal lato cliente (UPLINK). Si associa ad ogni dispositivo lato macchina che si vuole raggiungere un indirizzo corrispondente lato cliente, che si utilizzerà per l'accesso.



Indirizzi di configurazione

Supponiamo di avere uno scenario come in Fig.1, dove abbiamo la necessità di collegarci tramite la rete cliente dove è presente lo scada, a due dispositivi presenti nella rete macchina. Oltre all'indirizzo per la porta uplink/dev, per realizzare **la mappatura NAT 1:1** ci servono N indirizzi lato cliente, dove N sono i dispositivi che vogliamo raggiungere lato macchina. Tutti gli indirizzi **andranno forniti dal Cliente**. Nel caso in esempio serviranno quindi **tre indirizzi, uno per l'accesso ad internet e due per il NAT 1:1**.



GateManager

Supponiamo che il cliente ci fornisca i seguenti indirizzi IP: 192.168.26.130 / 131 / 132, con SUBNETMASK: 255.255.255.0 e un gateway: 192.168.26.5

Nota: l'indirizzo UPLINK serve per poter accedere alla pagina web del sitemanager per modificare la configurazione.

Con riferimento alla figura di esempio (Fig.1), questa è la configurazione standard del sitemanager:

Porta UPLINK1 IP: 192.168.26.130 GW 192.168.26.5 Porta DEV1 IP: 128.127.60.130

Dispositivi da raggiungere su lato DEV

PLC Rokwell: IP 128.127.60.17,

PLC Siemens: IP 128.127.60.21

Ai due dispositivi sulla porta DEV1 andranno associati i due indirizzi lato uplink

Tabella mappatura NAT 1:1		
Descrizione	Indirizzo lato cliente (UPLINK) →	Indirizzo Lato Macchina (DEV)
PLC Rockwell:	192.168.26.131	128.127.60.17
PLC Siemens	192.168.26.132	128.127.60.21

Configurazione SiteManager

Come prima operazione entriamo nella pagina di Setup del Sitemanager attraverso la sua interfaccia WEB (<https://IP dev1>) (vedi Fig.2).

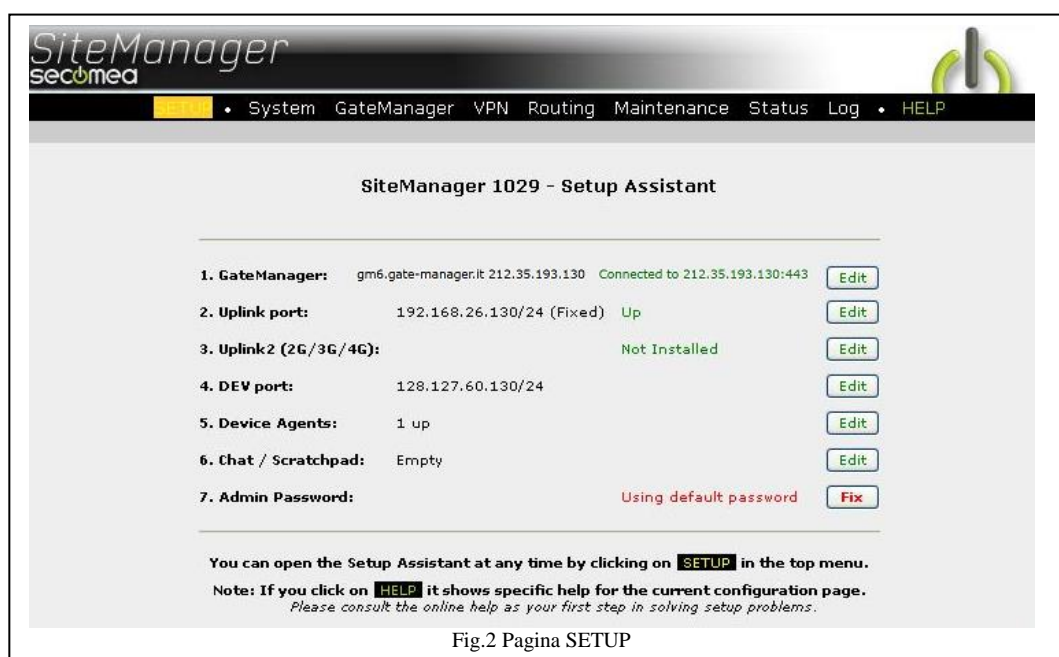


Fig.2 Pagina SETUP



Supporto tecnico:

tecnico@gate-manager.it



Inserimento Indirizzo porta UPLINK1

Nella sezione UPLINK1 (punto 2 del setup) andiamo a inserire l'indirizzo IP con relativa SUBNETMASK e GATEWAY forniti dal cliente **Nota:** L'indirizzo IP della porta Uplink1 deve essere un IP STATICO e non in DHCP

The screenshot shows the 'UPLINK - Setup Assistant' window. It contains instructions and configuration fields. A red box highlights the 'Mode' dropdown set to 'Static', and the 'IP Address', 'Subnet Mask', and 'Default Gateway' fields, which are pre-filled with '192.168.26.130', '255.255.255.0', and '192.168.26.5' respectively. Other fields include 'Ethernet Settings' (Autonegotiation), 'Priority' (First), 'Probe Type' (Any), 'Probe Hosts', 'Probe Port (TCP)' (80), 'Probe Interval A' (10 seconds), and 'Probe Interval B' (60 seconds). Buttons for 'Help' and 'Continue Setup >' are visible.

Fig.3 configurazione IP su UPLINK1

Associazione IP (Alias)

Dobbiamo inserire ora gli indirizzi IP aggiuntivi lato UPLINK, usando gli **IP aliases**. In questo modo verranno mappati 1:1 gli indirizzi rete cliente con gli indirizzi IP rete macchina.

The screenshot shows the 'IP Aliases' configuration page. The breadcrumb trail at the top is 'Routing Info > Static Routes > IP Aliases'. A red box highlights a table with two entries. Red numbers 1, 2, and 3 point to the 'Routing' menu item, the 'IP Aliases' sub-menu, and the table respectively.

Disable	IP Address	Interface	Comment
<input type="checkbox"/>	192.168.26.131	UPLINK	Alias_1
<input type="checkbox"/>	192.168.26.132	UPLINK	Alias_2

Buttons for 'Save', 'New', and 'Back' are at the bottom.

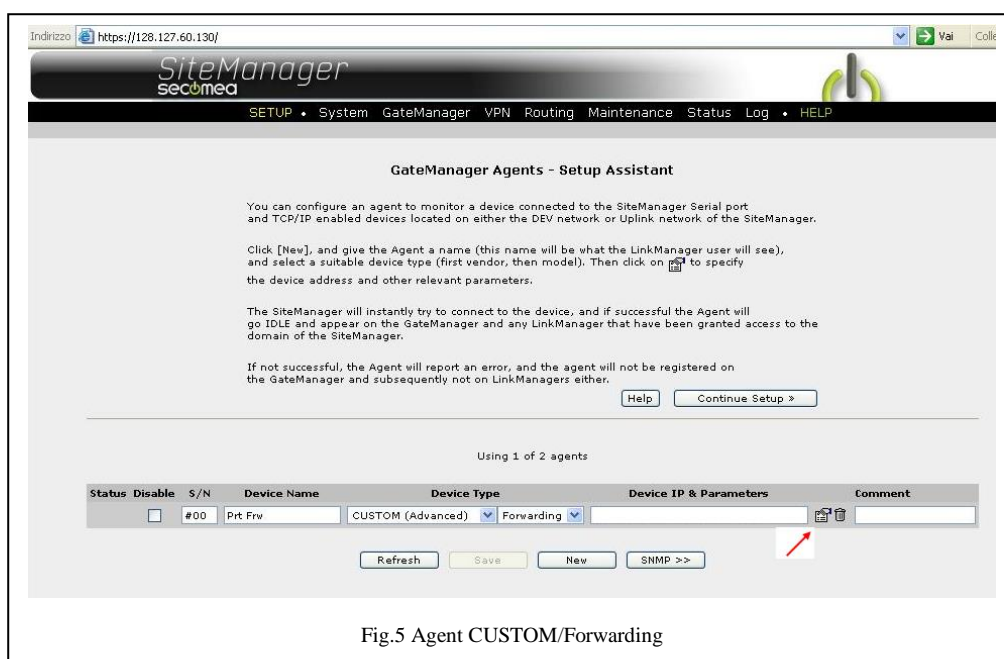
Fig.4 Creazione Alias



Per Creare gli Alias selezioniamo la voce **Routing → IP Aliases**, e creiamo un alias per ogni indirizzo IP esterno che ci ha fornito il cliente, selezionando “UPLINK” nel campo interface(Fig.4).

Creazione configurazione NAT 1:1 tramite Agent “CUSTOM Forwarding”

Per collegarsi ai dispositivi presenti sulla porta DEV1, occorre creare un Agent di tipo **CUSTOM Forwarding** che consente di implementare il NAT 1:1.



Una volta creato l’Agent **CUSTOM Forwarding** (Fig.5), clicchiamo sull’editor dell’Agent per inserire le regole di NAT relative ai dispositivi associati.

Creazione regole forwarding (NAT 1:1)

Dobbiamo creare **tante** regole di NAT 1:1 **quanti** sono i dispositivi che vogliamo raggiungere.

Regola Forwarding 1: => \$Indirizzo.2:ANY:1-65535>>Indirizzo Agent1:1-65535

Regola Forwarding 2: => \$Indirizzo.3:ANY:1-65535>>IndirizzoAgent2:1-65535

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



Nel nostro caso i dispositivi collegati alla porta DEV1 sono **due**, per cui andremo a creare **due** regole di NAT (Fig.6).

Nel nostro caso la regola di Forwarding/NAT, in base alla tabella vista prima,

Tabella mappatura NAT 1:1		
Descrizione	Indirizzo lato cliente (UPLINK) →	Indirizzo Lato Macchina (DEV)
PLC Rockwell:	192.168.26.131	128.127.60.17
PLC Siemens	192.168.26.132	128.127.60.21

Le regole di NAT 1:1 saranno quindi

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

SiteManager
secu@mea

SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

Device "Prt Frw" (Forwarding Agent) Details - Setup Assistant

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.

Click [Save] and then [Back] to make the SiteManager instantly try to connect to the device.

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 >](#)

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.6 Creazione regole forwarding



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

Indirizzo <https://128.127.60.130/> Vai

SiteManager
secmedia

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)								
pkts	bytes	target	prot	opt	in	out	source	destination
0	0	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
0	0	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)								
pkts	bytes	target	prot	opt	in	out	source	destination
0	0	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
0	0	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.7 Verifica regole di Forwarding

Test collegamento dispositivi

La configurazione del Sitemanager per la connessione 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 “esterno” 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 Rokwell con IP: 192.168.26.131



GateManager

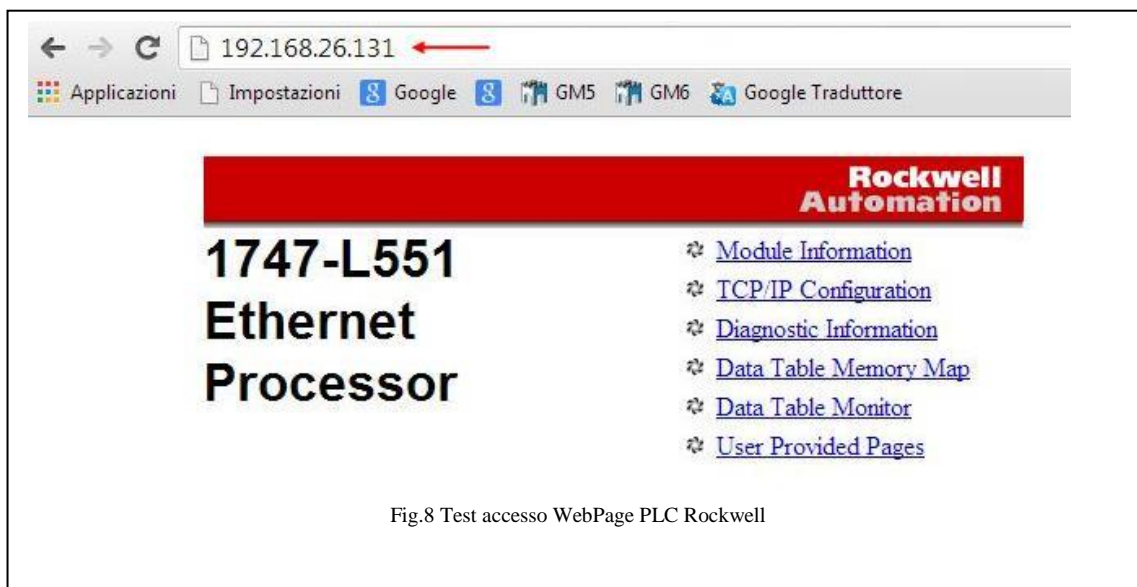


Fig.8 Test accesso WebPage PLC Rockwell

Come conferma del corretto funzionamento delle regole di Forwarding, attraverso la sezione **Status / Extended** è possibile verificare l'incremento dei pacchetti che transitano nel SiteManager ad ogni connessione dei dispositivi sul lato macchina (Fig.10).

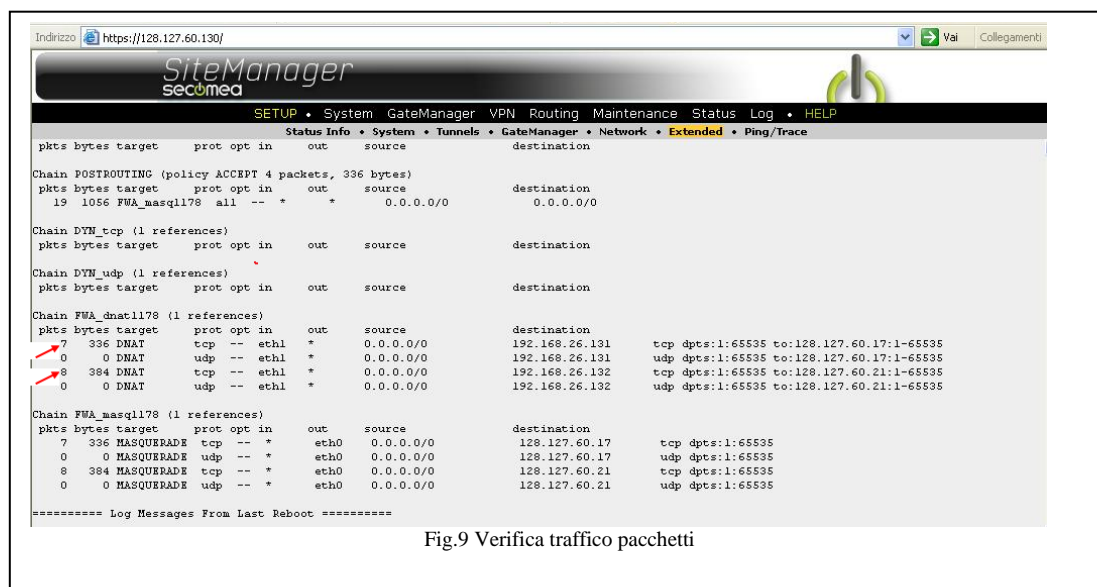


Fig.9 Verifica traffico pacchetti

Test accesso al PLC Siemens attraverso Tia Portal



Supporto tecnico:

tecnico@gate-manager.it



GateManager

Una volta avviato Tia Portal, apriamo il progetto e nella sezione Hardware effettuiamo un doppio click sul connettore di rete del PLC (Fig.10)

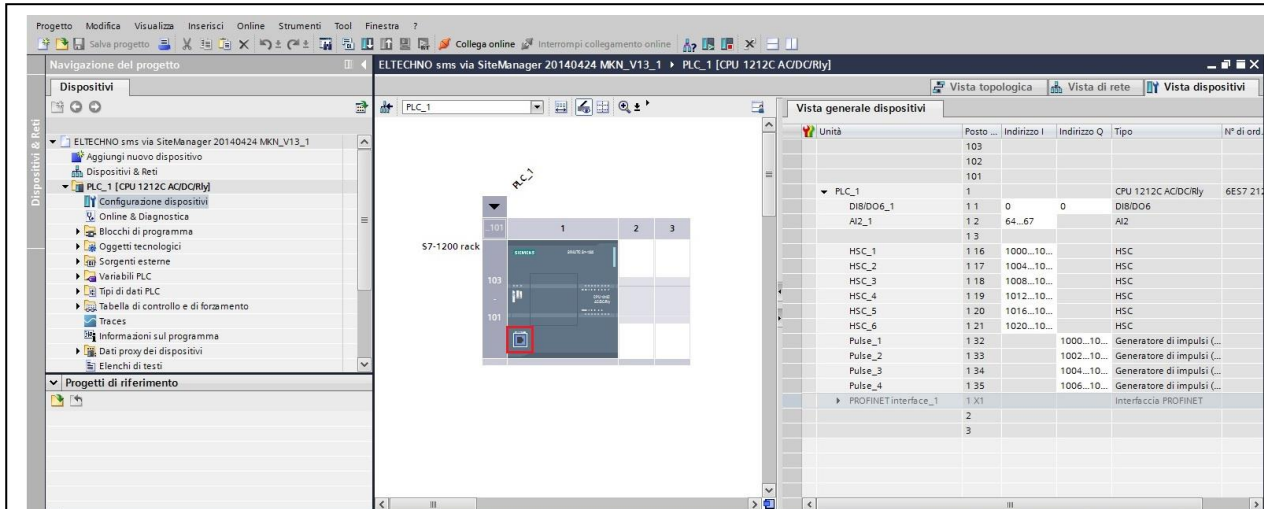


Fig.10 Configurazione Hardware PLC

Abilitare Flag “Consenti la modifica dell’Indirizzo IP direttamente nel dispositivo” per assegnare l’indirizzo VPN associato al PLC (Fig.11)

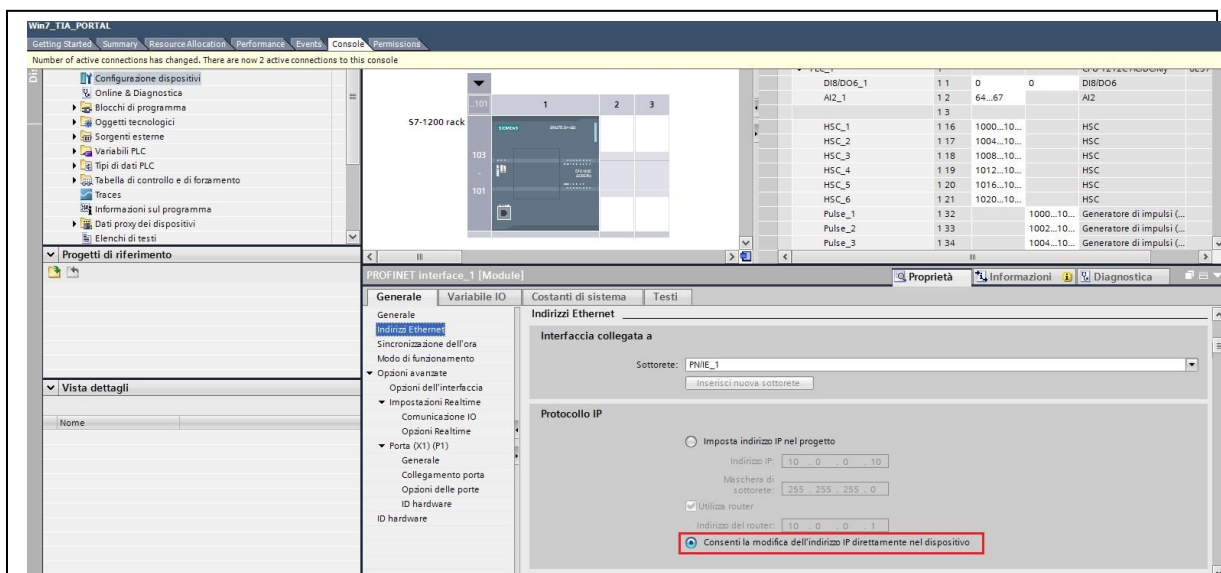


Fig.11 associazione indirizzo IP di VPN



GateManager

Selezionare l'icona "Collega online" (Fig.12)

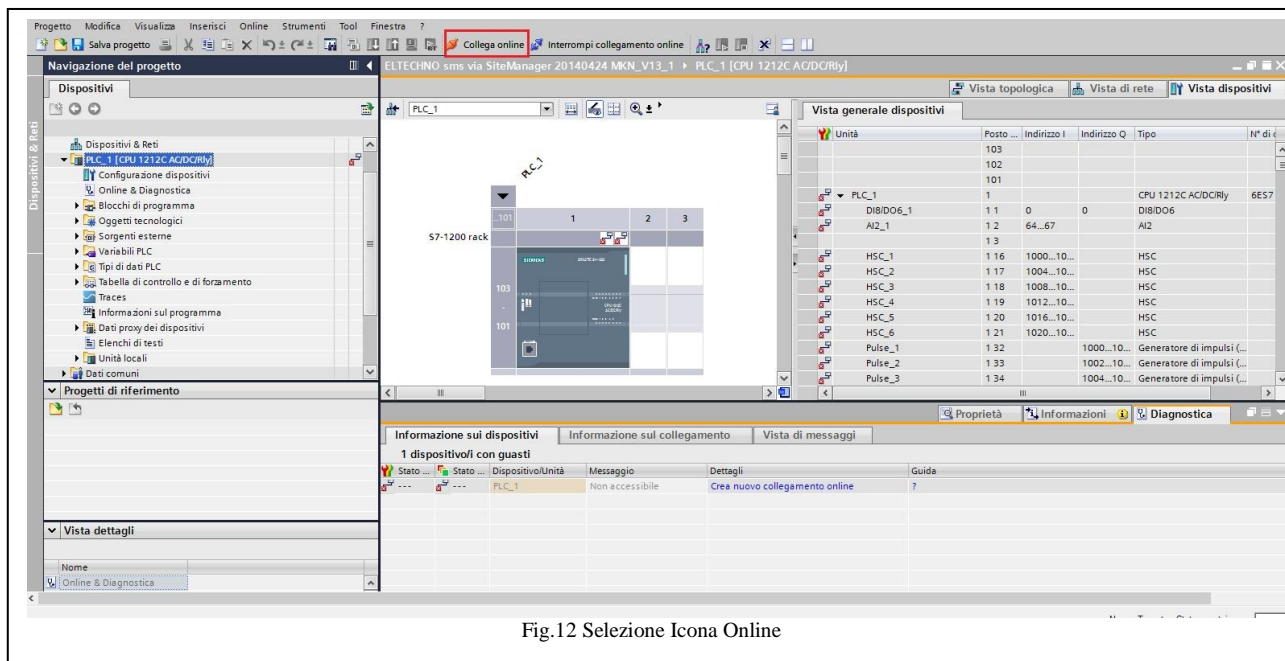


Fig.12 Selezione Icona Online

Impostare l'indirizzo IP di VPN associato al PLC e selezionare il pulsante "Avvio Ricerca" (Fig.13)

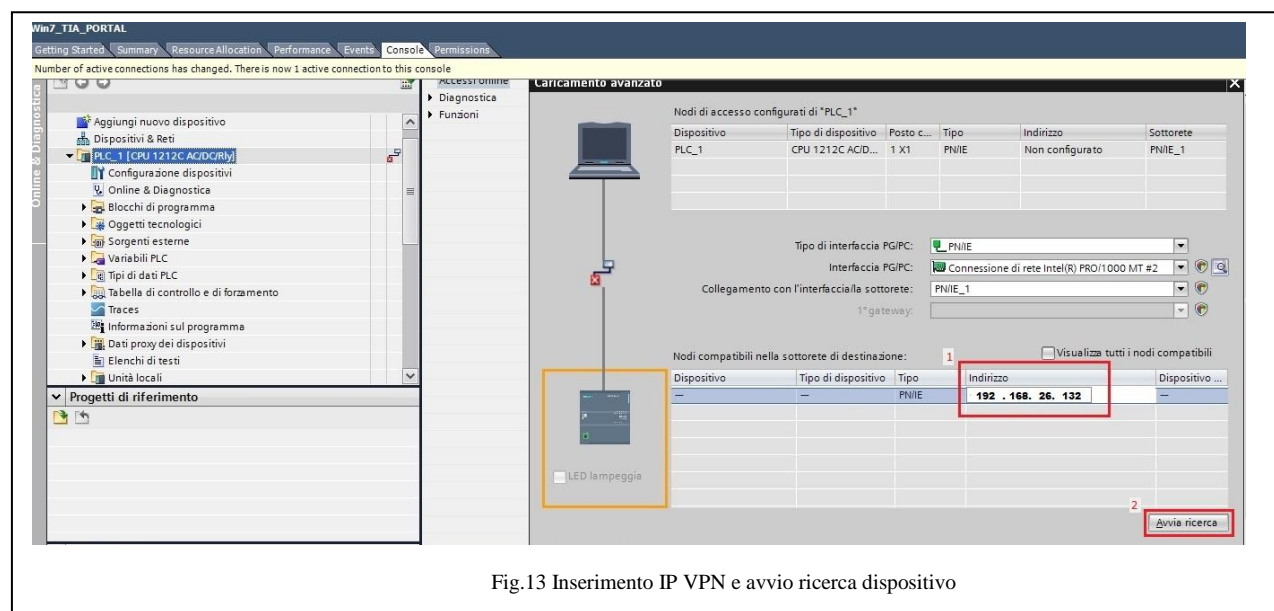


Fig.13 Inserimento IP VPN e avvio ricerca dispositivo



GateManager

Una volta visualizzato trovato il PLC, selezionare il pulsante “Carica” per andare online (Fig.14)

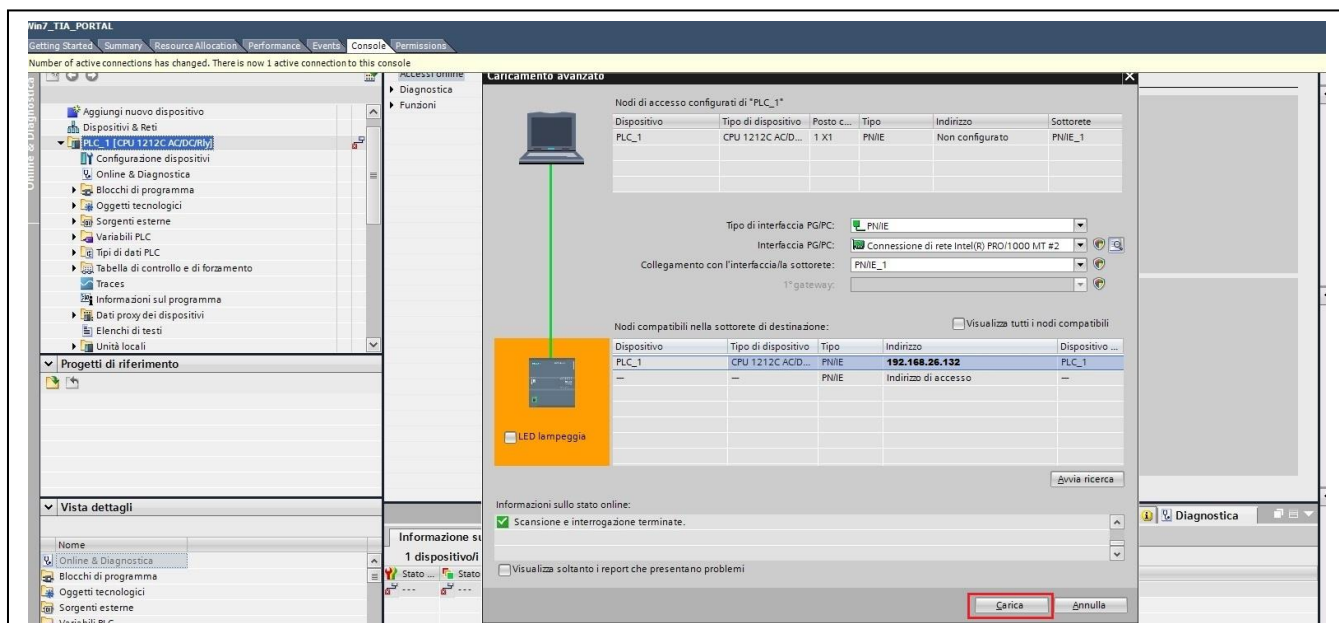


Fig.14 collegamento PLC a Tia Portal

Una volta terminata la procedura in Tia Portal, il PLC sarà collegato correttamente (Fig.15)

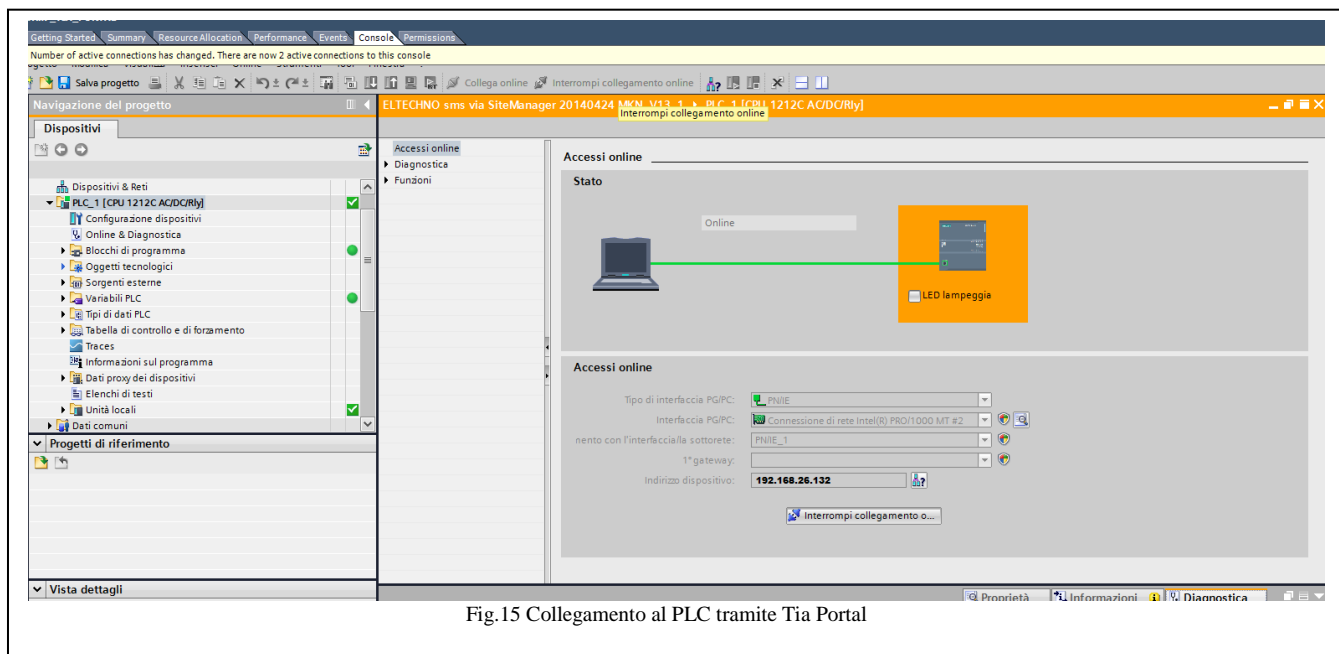


Fig.15 Collegamento al PLC tramite Tia Portal



GateManager

Troubleshooting

Nota:

- Con questa configurazione il protocollo FTP non è supportato.
- Con l'agent Forwarding il Ping Test non è supportato. Ovvero il ping agli indirizzi esterni non riflette lo stato dei dispositivi interni lato macchina.



Supporto tecnico:

tecnico@gate-manager.it