

SIEMENS

Ingegno per la vita



LOGO! CMR

Guida alla configurazione della VPN

siemens.it/logo

Contenuti

Introduzione.....	3
1. Primi passi per la configurazione	4
2. Impostazione tunnel VPN	6
2.1 Impostazione data e ora del CMR.....	6
2.2 Configurazione SIM.....	7
2.3 Connettere il CMR al LOGO! BM	8
2.4 Configurazione del DNS dinamico	9
2.5 Configurazione della comunicazione VPN	10
2.6 Configurazione del client OpenVPN	11
2.7 Collegamento in VPN al CMR.....	11
2.8 Collegamento in VPN a LOGO!.....	12
Link utili.....	13

Introduzione

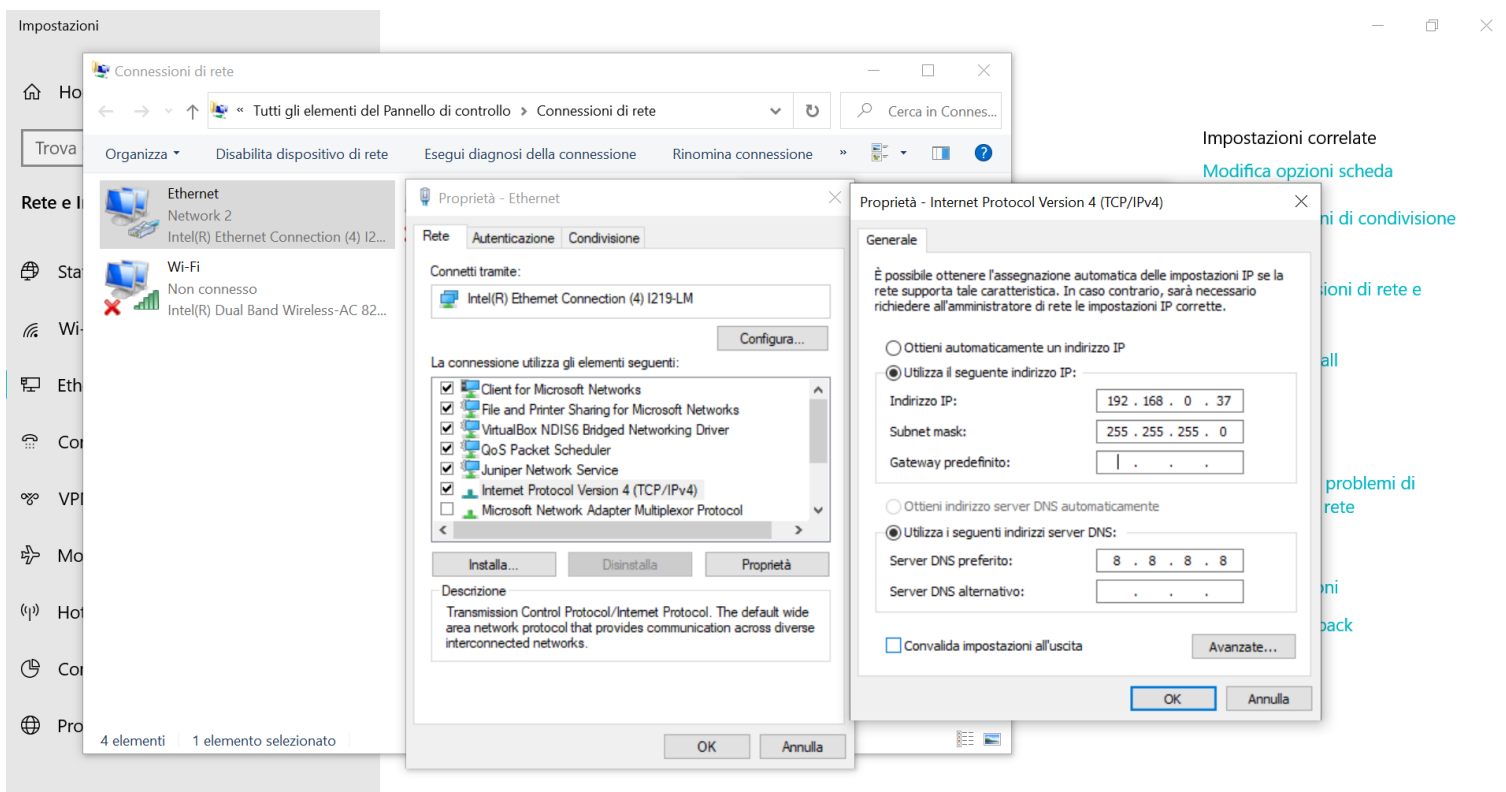
Lo scopo del presente documento è fornire agli utenti che si avvicinano per la prima volta al modulo LOGO! CMR 2020/2040 le nozioni di base per la configurazione e la parametrizzazione del dispositivo per la creazione del tunnel VPN (Virtual Private Network). Tramite l'instaurazione del tunnel VPN, è possibile il collegamento da remoto verso il modulo base LOGO!, previa definizione del CMR come gateway all'interno delle impostazioni di rete di LOGO!.

Per tutte le altre informazioni si rimanda al sito <http://www.siemens.it/logo>

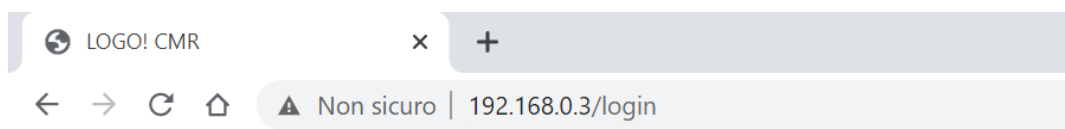
1. Primi passi per la configurazione

Il modulo LOGO! CMR2020/2040 (da qui in avanti solo CMR) è dotato di interfaccia web integrata da cui si effettua la configurazione e si ottengono informazioni di diagnostica circa il suo funzionamento. Non servono quindi software per la sua parametrizzazione ma basta dotarsi di un normale web browser.

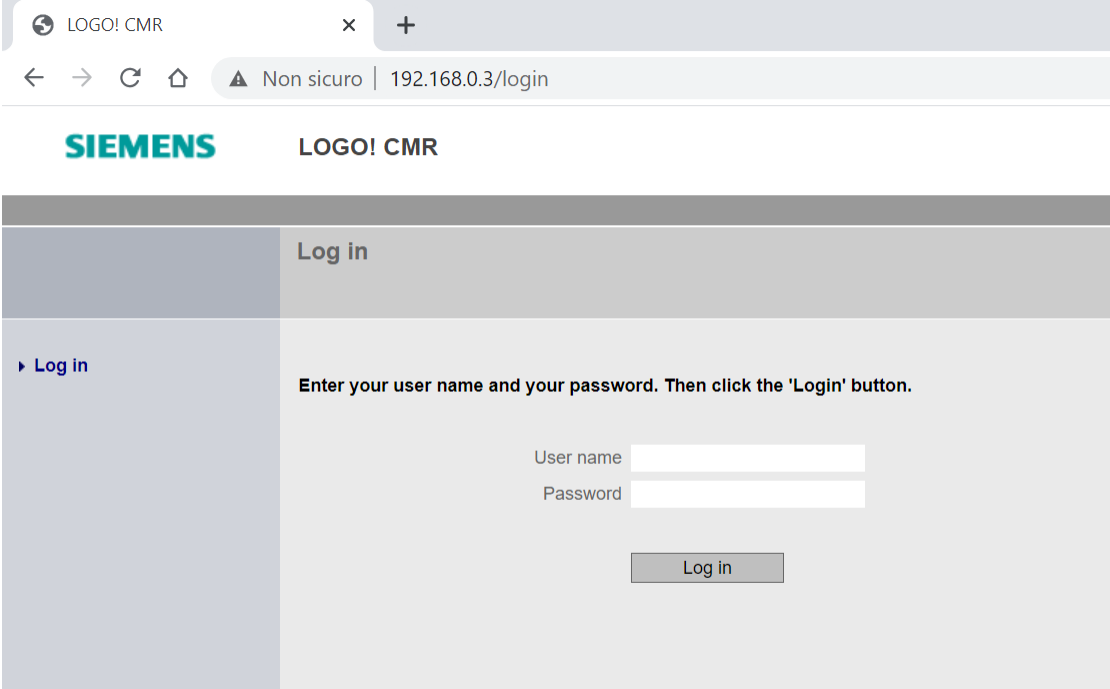
Prima di connettersi al CMR, assicurarsi che la scheda di rete presente sul PC abbia un indirizzo IP compatibile per la connessione al CMR. Per farlo occorre andare nelle *impostazioni* del PC, cliccare su *Ethernet* e quindi *Modifica opzioni scheda*, selezionare la scheda di rete e cliccare su *Proprietà*. Scorrere fino a raggiungere la proprietà *Protocollo internet versione 4*. Facendo doppio click si apre una pagina dove impostare l'indirizzo IP della vostra scheda di rete. Immettere un indirizzo IP compatibile (ad esempio IP CMR di default: 192.168.0.3 e IP scheda di rete: 192.168.0.37).



Per la configurazione di LOGO! CMR basta aprire un qualsiasi browser per la navigazione Internet (es. Internet Explorer, Google Chrome, ecc...) e digitare nella barra degli indirizzi l'IP del dispositivo. Da impostazioni di fabbrica, l'indirizzo IP di un LOGO! CMR è 192.168.0.3



A questo punto apparirà la seguente schermata.



The screenshot shows a web browser window with the address bar displaying "192.168.0.3/login". The page header includes the Siemens logo and "LOGO! CMR". The main content area is titled "Log in" and contains the instruction: "Enter your user name and your password. Then click the 'Login' button." Below this instruction are two input fields labeled "User name" and "Password", and a "Log in" button.

Inserire *User name* e *Password*.

N.B. da impostazioni di fabbrica: *User name* = admin, *password* = admin.

Al primo accesso reimpostare la password come richiesto.

2. Impostazione tunnel VPN

In questa sezione saranno descritti i parametri da inserire nel browser del CMR per la creazione del tunnel VPN.

2.1 Impostazione data e ora del CMR

Operazione preliminare a qualsiasi altra che coinvolga il CMR è l'impostazione della data e dell'ora corretta. Per farlo, accedere alla pagina *System*, nella sezione *System time*. Scegliere la modalità di sincronizzazione dell'ora cliccando sul pulsante *Adopt PC time*.

SIEMENS LOGO! CMR

User: admin [Log out](#)

System

General | Device info | SD card | **System time**

▶ Start page

▶ **System**

▶ Diagnostics

▶ Maintenance

▶ LAN

▶ WAN

▶ Security

▶ Users / groups

▶ Monitoring

Local time zone

(UTC+01:00) Berlin ▼

+ 01 h 00 min

Automatic daylight saving time switch

Beginning of daylight saving time Last Sunday March 02 h 00 min

End of daylight saving time Last Sunday October 03 h 00 min

Enable time-of-day synchronization

Time-of-day synchronization method NTP ▼

Last time-of-day synchronization (dd:hh:mm:ss) ago - [Synchronize immediately](#)

Accept time-of-day from non-synchronized NTP servers

IP address or DNS name of the NTP server

Update interval 1 hour ▼

NOTE:
If you want to use time-of-day synchronization through the mobile wireless network, check whether this service is supported by your mobile wireless provider.

Forward time of day to LOGO! BM

NOTE:
If you have selected to forward the time of day to LOGO! BM, make sure that you have deactivated the automatic changeover to daylight saving time in LOGO! BM. This avoids different settings and resulting time deviations in LOGO! BM and LOGO! CMR.

[Apply](#)

Set system time manually:

New system time Year-month-day hour:minute:second

[Adopt new system time](#)

[Adopt PC time](#)

2.2 Configurazione SIM

Prima operazione è configurare i parametri della scheda SIM inserita all'interno del CMR. Per fare questo cliccare sulla pagina WAN.

N.B.: Si ricorda che per la configurazione del tunnel VPN è necessario utilizzare una scheda SIM abilitata all'uso dei dati internet. Questa SIM deve inoltre NON essere nattata con la rete pubblica di tipo mobile. Una scheda SIM con queste caratteristiche viene definita machine-to-machine (M2M) o denat e deve essere specificatamente richiesta al provider della scheda SIM.

Nella sezione *Mobile wireless settings* spuntare il flag *Enable mobile wireless interface*, inserire il PIN della SIM (se presente) e attivare il roaming spuntando il flag *Allow roaming*. Abilitare la connessione dati spuntando il flag *Enable data service in the mobile wireless network*. Inserire l'APN indicato dal provider della SIM e selezionare il metodo di autenticazione al servizio internet in *Authentication Method*. Se il metodo lo prevede, indicare un nome e una password. Cliccare su *Apply*.

N.B.: Per il corretto funzionamento della connessione dati è opportuno indicare l'APN corretto. Questo parametro dipende dal provider della SIM e dalla tipologia di SIM acquistata. Fare sempre riferimento alle indicazioni fornite dal provider della SIM, che deve essere di tipologia machine-to-machine.

The screenshot shows the LOGO! CMR web interface for WAN configuration. The browser address bar shows '192.168.0.3/wan_2'. The page title is 'WAN' and the user is 'admin'. The 'Mobile wireless settings' tab is active, showing the following configuration:

- Enable mobile wireless interface
- PIN of the SIM card: [REDACTED]
- The PIN was accepted by the SIM card.
- Allow roaming
- Enable data service in the mobile wireless network
- APN: m2mbis.vodafone.it
- Authentication method: CHAP
- Name: Guest
- Password: [REDACTED]

An 'Apply' button is visible at the bottom of the configuration area. The Windows taskbar at the bottom shows the date and time as 15:50 on 28/05/2021.

2.3 Connettere il CMR al LOGO! BM

Per connettere il CMR al modulo base LOGO!8.3 è necessario che il firmware del CMR sia V2.1.8.

A partire dalla versione 8.3 LOGO! supporta solo connessioni sicure con il CMR. Il CMR comunica con LOGO! tramite l'accesso a LSC/LWE. È pertanto necessario abilitare questo accesso in LOGO! Soft Comfort (*Impostazioni comando accesso*) ed inserire una password.

Se il modulo CMR non viene utilizzato in modalità stand alone, ma in accoppiata con LOGO!, questa connessione va impostata nel CMR nella pagina *Monitoring* nella sezione *LOGO! BM*. Per attivare la comunicazione con LOGO! spuntare la proprietà *Active*, inserire l'indirizzo IP del LOGO! a cui è connesso il CMR, scegliere l'intervallo di aggiornamento dell'immagine di processo e la versione di LOGO! che si sta utilizzando (nel caso di esempio LOGO!8.3).

Spuntare *Password protection* ed inserire la password che è stata inserita in LOGO! Soft Comfort quando è stato abilitato l'accesso a LSC/LWE.

Confermare il tutto con *Apply*.

SIEMENS LOGO! CMR

User: admin [Log out](#)

Monitoring

Overview | **LOGO! BM** | Constants | Message texts | Signals | Events | Actions | Assignments

- Start page
- System
- Diagnostics
- Maintenance
- LAN
- WAN
- Security
- Users / groups
- Monitoring**

Active

IP address of LOGO! BM

Update interval for process image ▾

Communication profile ▾

Password protection

Password

CA certificate

Fingerprint SHA-1 actually used

Fingerprint SHA-1 used after Apply

Load new file

2.4 Configurazione del DNS dinamico

Nella pagina *WAN*, all'interno della sezione *DynDNS* si configura l'assegnazione di un indirizzo DNS dinamico all'interfaccia della rete mobile.

N.B.: Prima di procedere con la configurazione è necessario dotarsi di un servizio di assegnazione dinamica del DNS. LOGO! supporta due diversi servizi: No-IP e DynDNS. Prima di procedere con la configurazione nel CMR è quindi necessario seguire le procedure di ottenimento dell'indirizzo DNS dinamico indicate sui siti web dei fornitori del servizio.

Per lo sviluppo della seguente guida è stato scelto No-IP.

Spuntare *Active*, nel campo *DynDNS provider* scegliere il fornitore del servizio. Nel campo *Host* indicare l'hostname selezionato sul sito del fornitore. Nei campi *Name* e *Password* indicare il nome e la password dell'account registrato sul sito del fornitore del servizio.

Cliccare su *Apply*.

The screenshot displays the LOGO! CMR web interface for the 'WAN' section, specifically the 'DynDNS' configuration page. The interface includes a navigation menu on the left with options like 'Start page', 'System', 'Diagnostics', 'Maintenance', 'LAN', 'WAN', 'Security', 'Users / groups', and 'Monitoring'. The main configuration area shows the following settings:

- Active:**
- DynDNS provider:** No-IP
- Host:** testlogo.ddns.net
- Name:** testlogo_2021@libero.it
- Password:** [masked]
- CA certificate:**
 - Currently used file: No file loaded (Delete button)
 - File used after applying: -
 - Load new file: No file selected (Search button)
 - Load on device button
- Apply** button

The top right corner of the interface shows the date '2010-01-01', time '00:10:08', and language 'English'. The bottom of the screenshot shows a Windows taskbar with the search bar and various application icons.

2.5 Configurazione della comunicazione VPN

Nella pagina *Security*, nella sezione *OpenVPN-PSK* spuntare la casella *Active*. Indicare in *Port Number* il numero della porta che il tunnel VPN utilizzerà per la comunicazione, di default 1194.

Nella sezione *Pre-shared key* è possibile generare una nuova chiave oppure caricare una chiave generata dal client, che sarà utilizzata da entrambi i partner della VPN (CMR e PC) per stabilire la comunicazione.

Per generare una nuova chiave, cliccare sul pulsante *Generate new key* e successivamente *Apply*.

La configurazione del server OpenVPN (il CMR) e la chiave dovranno essere condivise con il client OpenVPN. Per questo motivo cliccare su *Save standard server configuration for client*. Viene scaricato sul PC un file *vpnpeer.conf*

La configurazione all'interno di CMR è terminata.

Per consentire l'instaurazione della comunicazione il file *vpnpeer.conf* dovrà essere caricato sul client OpenVPN.

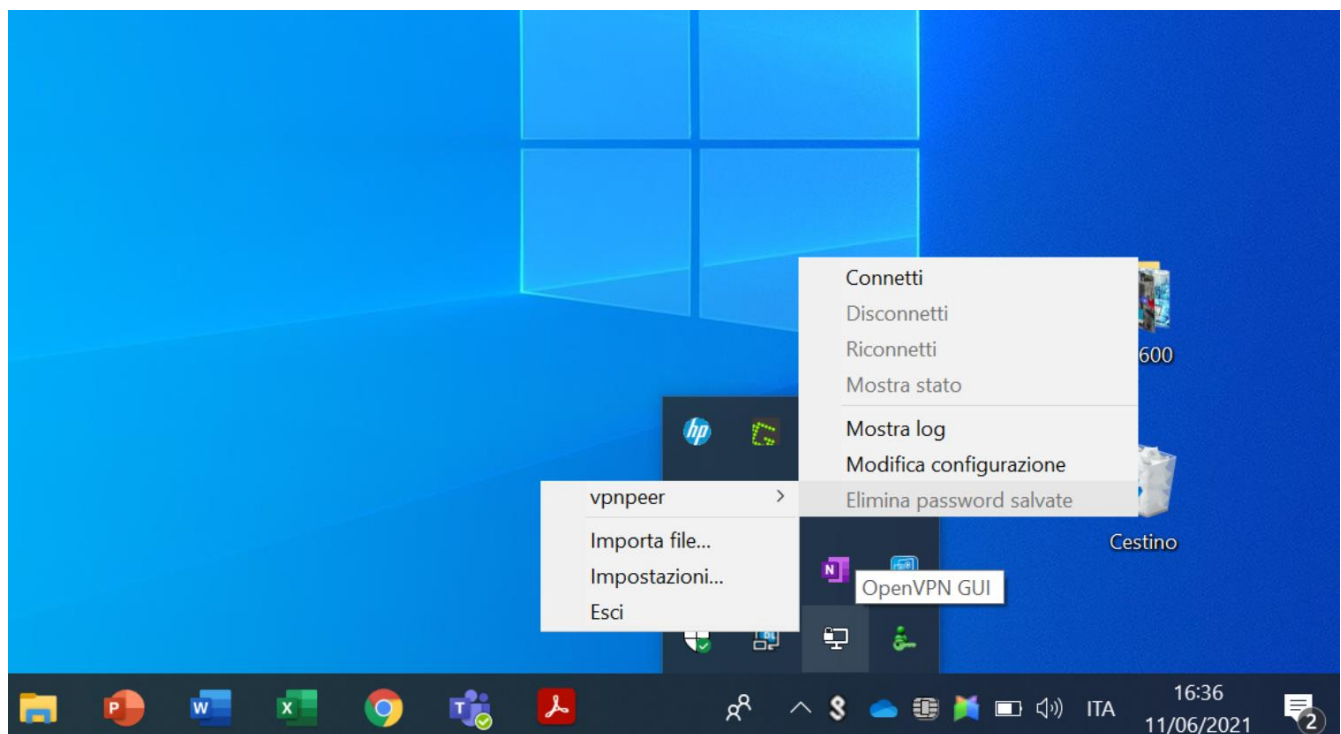
The screenshot shows the LOGO! CMR web interface. The browser address bar displays '192.168.0.3/sec_2'. The page title is 'Security' and the user is logged in as 'admin'. The 'OpenVPN-PSK' tab is selected in the navigation menu. A green checkmark indicates 'The new key was correctly generated'. The 'OpenVPN-PSK' section has the 'Active' checkbox checked. The 'Port number' is set to 1194 and the 'Keep-alive monitoring time (s)' is 120. In the 'Pre-shared key' section, the 'Generate new key' button is visible. Below it, the 'Currently used file' is 'No file loaded', the 'File used after applying' is 'static_g.key', and the 'Load new file' section shows 'No file selected' with a 'Search' button. At the bottom of the configuration area, there is a button labeled 'Apply' and a link 'Save standard server configuration for client'. The Windows taskbar at the bottom shows the time as 15:56 on 28/05/2021.

2.6 Configurazione del client OpenVPN

Per instaurare la comunicazione VPN è necessario avere il software client *OpenVPN GUI* che permette di stabilire il tunnel VPN con il server OpenVPN (CMR). L'OpenVPN client deve supportare la funzione OpenVPN V2.3.11 o superiore.

Nel client OpenVPN è necessario importare il file *vpnpeer.conf* scaricato precedentemente cliccando con il tasto destro del mouse sull'icona di *OpenVPN GUI – Importa file*.

Una volta importato il file, per instaurare il tunnel VPN cliccare con il tasto destro del mouse sull'icona *OpenVPN GUI*, selezionare il nome del file appena importato e selezionare *Connetti*.



2.7 Collegamento in VPN al CMR

Una volta stabilito il tunnel VPN, per collegarsi da remoto verso il CMR, inserire in un browser Internet l'indirizzo IP del CMR. Se il collegamento funziona, appariranno le schermate del web server di programmazione del CMR.

2.8 Collegamento in VPN a LOGO!

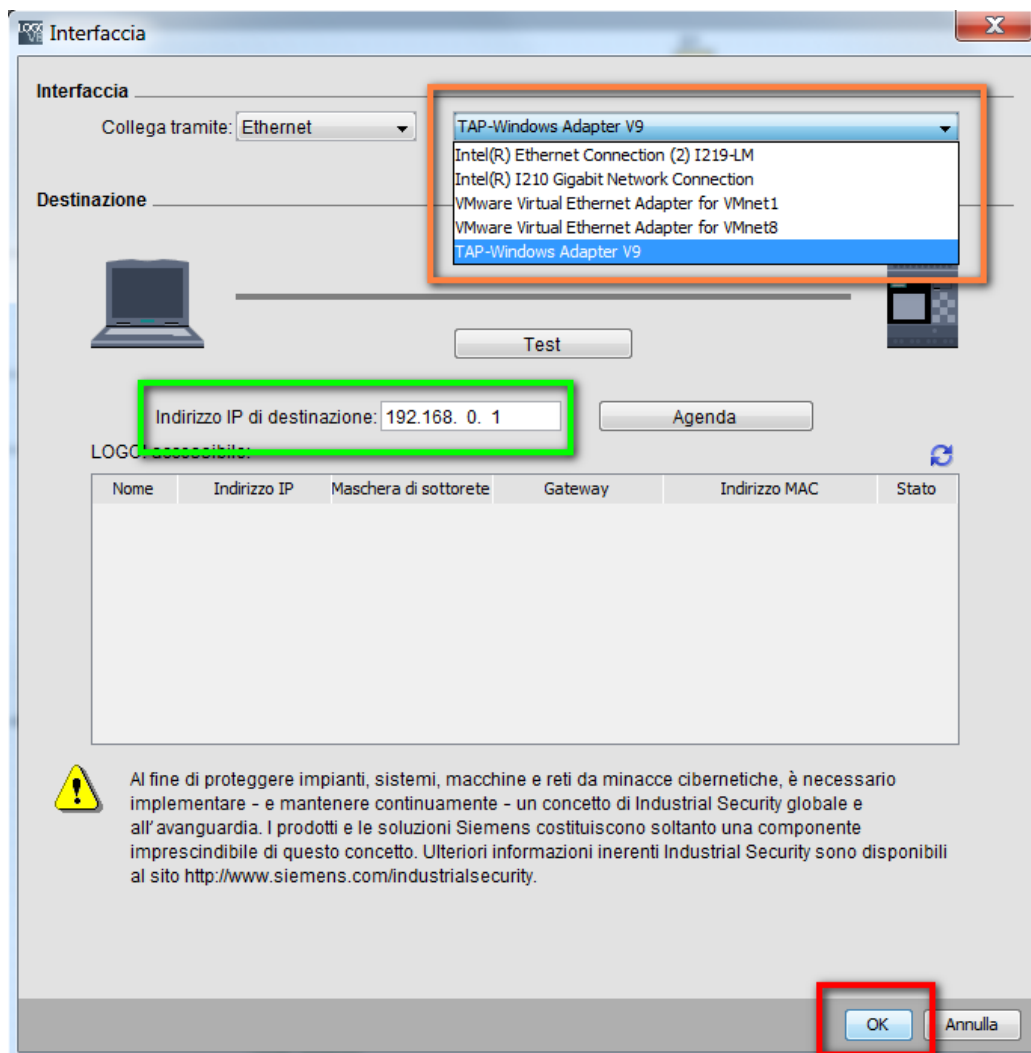
Quando il tunnel VPN è stabilito, tramite il CMR è possibile anche collegarsi da remoto a LOGO!.

È possibile sia accedere al web server di LOGO!, inserendo l'indirizzo IP di LOGO! nel browser, sia effettuare il download/upload tramite LOGO! Soft Comfort, selezionando la scheda di rete corretta in LSC.

Per rendere possibile questo collegamento bisogna impostare il CMR come gateway di LOGO!.

Per collegarsi a LOGO!, aprire l'interfaccia di collegamento. Scegliere *TAP-Windows Adapter V9* e come *Indirizzo IP di destinazione* inserire l'indirizzo IP di LOGO! configurato sul dispositivo. Cliccare OK.

A questo punto, il software si conetterà a LOGO! attraverso la VPN creata con il CMR.



Link Utili

- (1) **Manuale di riferimento – LOGO!**
- (2) **Manuale di riferimento – CMR**
- (3) **Aggiornamento firmware CMR – versione V2.1.8**
- (4) **Aggiornamento software di programmazione di LOGO!**
- (5) **Sito web LOGO!**

Siemens S.p.A.
Via Vipiteno 4
20128 Milano
Tel. 02 243 1
Mail: infodesk.it@siemens.com

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.