MANUALE TECNICO


# ELMOGWAY - ELMOGWAY2

Gateway multiprotocollo fra centrali EL.MO. e sistemi di Home & Building Automation

090001051

EL.MO. SPA

# AVVERTENZE

## PER L'INSTALLATORE:

Attenersi scrupolosamente alle norme operanti sulla realizzazione di impianti elettrici e sistemi di sicurezza, oltre che alle prescrizioni del costruttore riportate nella manualistica a corredo dei prodotti.
Fornire all'utilizzatore tutte le indicazioni sull'uso e sulle limitazioni del sistema installato, specificando che esistono norme specifiche e diversi livelli di prestazioni di sicurezza che devono essere commisurati alle esigenze dell'utilizzatore.
Far prendere visione all'utilizzatore delle avvertenze riportate in questo documento.

## PER L'UTILIZZATORE:

Verificare periodicamente e scrupolosamente la funzionalità dell'impianto accertandosi della correttezza dell'esecuzione delle manovre di inserimento e disinserimento.
Curare la manutenzione periodica dell'impianto affidandola a personale specializzato in possesso dei requisiti prescritti dalle norme vigenti.
Provvedere a richiedere al proprio installatore la verifica dell'adeguatezza dell'impianto al mutare delle condizioni operative (es. variazioni delle aree da proteggere per estensione, cambiamento delle metodiche di accesso ecc...)

---

Questo dispositivo è stato progettato, costruito e collaudato con la massima cura, adottando procedure di controllo in conformità alle normative vigenti. La piena rispondenza delle caratteristiche funzionali è conseguita solo nel caso di un suo utilizzo esclusivamente limitato alla funzione per la quale è stato realizzato, e cioè:

**Gateway fra centrali EL.MO. e sistemi di Home & Building Automation.**

Qualunque utilizzo al di fuori di questo ambito non è previsto e quindi non è possibile garantire la sua corretta operatività e pertanto è fatto espresso divieto al detentore del presente manuale di utilizzarlo per ragioni diverse da quelle per le quali è stato redatto ovvero esplicative delle caratteristiche tecniche del prodotto e delle modalità di uso.
I processi produttivi sono sorvegliati attentamente per prevenire difettosità e malfunzionamenti; purtuttavia la componentistica adottata è soggetta a guasti in percentuali estremamente modeste, come d'altra parte avviene per ogni manufatto elettronico o meccanico. Vista la destinazione di questo articolo (protezione di beni e persone) invitiamo l'utilizzatore a commisurare il livello di protezione offerto dal sistema all'effettiva situazione di rischio (valutando la possibilità che detto sistema si trovi ad operare in modalità degradata a causa di situazioni di guasti od altro), ricordando che esistono norme precise per la progettazione e la realizzazione degli impianti destinati a questo tipo di applicazioni.

**Richiamiamo l'attenzione dell'utilizzatore (conduttore dell'impianto) sulla necessità di provvedere regolarmente ad una manutenzione periodica del sistema almeno secondo quanto previsto dalle norme in vigore oltre che ad effettuare, con frequenza adeguata alla condizione di rischio, verifiche sulla corretta funzionalità del sistema stesso segnatamente alla centrale, sensori, avvisatori acustici, combinatore/i telefonico/i ed ogni altro dispositivo collegato. Al termine del periodico controllo l'utilizzatore deve informare tempestivamente l'installatore sulla funzionalità riscontrata.**

La progettazione, l'installazione e la manutenzione di sistemi incorporanti questo prodotto sono riservate a personale in possesso dei requisiti e delle conoscenze necessarie ad operare in condizioni sicure ai fini della prevenzione infortunistica. È indispensabile che la loro installazione sia effettuata in ottemperanza alle norme vigenti. Le parti interne di alcune apparecchiature sono collegate alla rete elettrica e quindi sussiste il rischio di folgorazione nel caso in cui si effettuino operazioni di manutenzione al loro interno prima di aver disconnesso l'alimentazione primaria e di emergenza. Alcuni prodotti incorporano batterie ricaricabili o meno per l'alimentazione di emergenza. Errori nel loro collegamento possono causare danni al prodotto, danni a cose e pericolo per l'incolumità dell'operatore (scoppio ed incendio).

## DICHIARAZIONE DI CONFORMITÀ UE

Prodotti conformi alle vigenti direttive europee EMC ed LVD, il testo completo della Dichiarazione di Conformità è disponibile al seguente indirizzo internet elmospa.com previa semplice registrazione.

## AVVERTENZE PER LO SMALTIMENTO - INFORMAZIONI AGLI UTENTI

**IT08020000001624**

Ai sensi della Direttiva 2012/19/UE, relativa allo smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE), si precisa che il dispositivo AEE è immesso sul mercato dopo il 13 Agosto 2005 con divieto di conferimento all'ordinario servizio di raccolta dei rifiuti urbani.

## 1. GENERALITÀ

ELMOGWAY ed ELMOGWAY2 **consentono di interfacciare centrali EL.MO. a sistemi di automazione**, integrando la protezione fornita da EL.MO. in impianti home & building di ultima generazione.
ELMOGWAY ed ELMOGWAY2 **operano con il concetto universalmente noto come sistema MASTER-SLAVE**. Nei sistemi Master-Slave due dispositivi dialogano fra loro secondo una regola ben precisa: il Master è l'unità che desidera ricevere informazioni, lo slave è l'unità che può fornire informazioni.
Il dispositivo Master esegue dei processi di domanda (query) nei confronti di un dispositivo detto Slave, che "a domanda risponde" con il dato richiesto, se disponibile.
Un dispositivo Slave non eroga dati in modo autonomo, ma solo su richiesta esplicita. Questo permette di collegare molti Slave sul medesimo bus, e il Master indirizza la domanda allo Slave di interesse. Gli altri Slave ascoltano ma se la domanda non è diretta a loro, tacciono.
**ELMOGWAY ed ELMOGWAY2 sono contemporaneamente Master e Slave**:

- sono Master nei confronti della centrale EL.MO., eseguono query e sistemano i dati.
- sono Slave nei confronti di un'unità Master, ad esempio un PLC, un supervisore, o altro. A domanda, rispondono al Master.

È il criterio del bucket brigade: il gateway chiede alla centrale slave e trasferisce, su richiesta, al proprio master.
**I gateway sono compatibili con tutte le centrali antintrusione EL.MO presenti a catalogo e con le centrali antincendio EL.MO. della serie TACÓRA** (TA1002, TA1004, TA2000, TA4000).
ELMOGWAY ed ELMOGWAY2 sono in grado di dialogare con il sistema di automazione utilizzando **protocolli di comunicazione** differenti, **MODBUS, KNX e SCS**, garantendo grande flessibilità di utilizzo.
Supportano connessioni con centrali antintrusione e antincendio (della gamma TACÓRA) via LAN, USB o porta seriale a seconda dei modelli.
**Un'interfaccia web consente la programmazione e configurazione** veloce dei gateway e, tra le varie funzioni, la definizione di regole operative tra stati e comandi.

## 2. CARATTERISTICHE

| **Modello gateway** | ELMOGWAY | ELMOGWAY2 |
|---|---|---|
| **Grado di protezione EN 60335-1** | II | |
| **Alimentazione** | 10 - 16 VDC | |
| **Assorbimento** | 3 W - 300 mA max | |
| **LED di segnalazione** | 1 LED rosso: allarme/reset;<br>1 LED verde: power ON (normalmente ON se dispositivo alimentato). | |
| **Porte di comunicazione** | **KNX**: Connettore a innesto.<br>**RS-485:** Connettore a innesto.<br>**RS-232:** Connettore a innesto.<br>**LAN:** Connettore RJ45 (10/100 Mbps).<br>**USB 2.0:** 2 porte. | **KNX**: Connettore a innesto.<br>**RS-485:** Connettore a innesto.<br>-<br>**LAN:** Connettore RJ45 (10/100 Mbps).<br>**USB 2.0:** 1 porta. |
| **Pulsante di reset** | Sul lato superiore del case. | Accessibile rimuovendo il coperchio frontale. |
| **Slot espansione memoria** | MicroSD (fino a 32 GB per usi futuri). | - |
| **Temperatura operativa** | 0 °C — +50 °C | |
| **Temperatura di stoccaggio** | −10 °C — + 70°C | |
| **Dimensioni** | L90 × H98 × P62 mm<br>5 moduli DIN. | L90 × H36 × P62 mm<br>2 moduli DIN. |
| **Materiale involucro** | Materiale termoplastico autoestinguente. | |

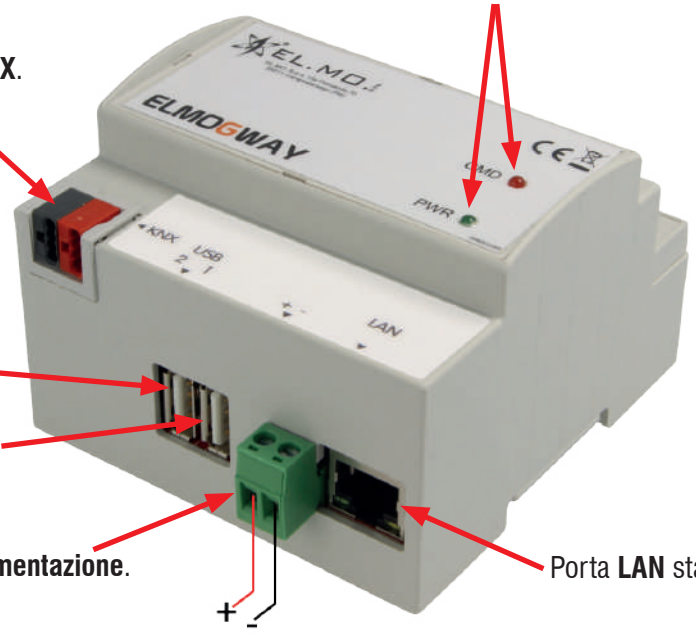
**AVVERTENZA:**
Nell'integrazione di un gateway in sistemi antintrusione, occorre mantenere intatto il livello di sicurezza ottenuto in fase di installazione.
Inserimento e disinserimento delle centrali devono avvenire sempre attraverso gli organi di comando delle centrali stesse.
Anche la disabilitazione e l'esclusione di sensori devono essere effettuate con estrema cautela.
Una centrale che non rispetta i dettami delle norme decade a livello zero di sicurezza.
Per eventuali approfondimenti, si rimanda alle norme CEI79-3:2012 e EN50131-1:2009.

## 3. STRUTTURA DI ELMOGWAY

**Vista del lato inferiore e del pannello frontale.**

Indicatori **LED**:
**Verde**: Alimentazione;
**Rosso**: Reset/Service.

Connettore standard rosso-nero per collegamento a bus **KNX**.




Porta **USB2**.

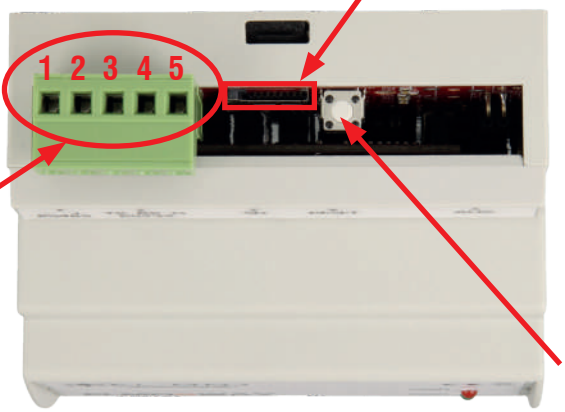
Porta **USB1**.

Connettore di **alimentazione**.

Porta **LAN** standard RJ45.

**Vista del lato superiore.**

Alloggiamento per MicroSD (usi futuri).



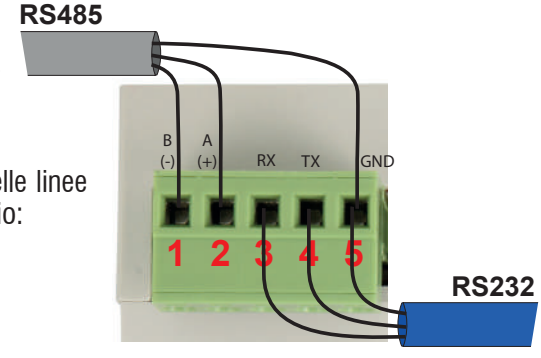

Morsettiera a innesto:

**RS-485**: Morsetto 1 TX/B/(-)
Morsetto 2 RX/A/(+)
Morsetto 5 GND

**RS-232**: Morsetto 3 RX
Morsetto 4 TX
Morsetto 5 GND

Pulsante di **RESET** (raggiungibile utilizzando un utensile isolato, in caso di necessità).

Collegamenti delle linee seriali in dettaglio:



## 4. STRUTTURA DI ELMOGWAY2

**Vista dall'alto.**

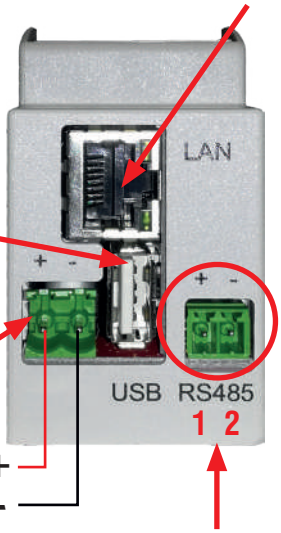
Indicatori **LED**:
**Verde (PWR)**: Alimentazione;
**Rosso (CMD)**: Reset/Service.


**Vista del lato superiore.**

Porta **LAN** standard RJ45.

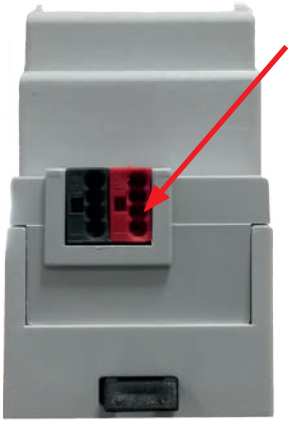
Porta **USB**.

Connettore di **alimentazione**.



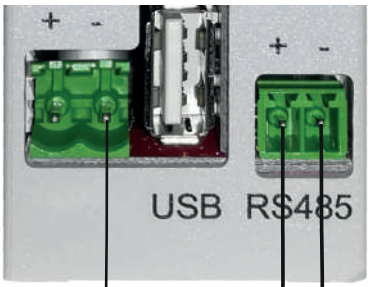

**Vista del lato inferiore.**

Connettore standard rosso-nero per collegamento a bus **KNX**.

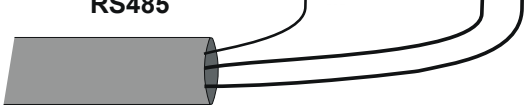


Morsettiera per linea seriale RS-485:

**RS-485**: Morsetto 1 RX/A/(+)
Morsetto 2 TX/B/(-)




Collegamenti della linea seriale in dettaglio:




Collegare il filo GND della linea seriale RS-485 al negativo di alimentazione.

# 5. INSTALLAZIONE E RIPRISTINO

## 5.1 Montaggio

Montare il dispositivo in area protetta contro l'apertura (tamper), non liberamente accessibile da utenti.
Il contenitore del gateway va fissato, ad esempio, su barra DIN standard da 35 mm.

## 5.2 Collegamenti elettrici

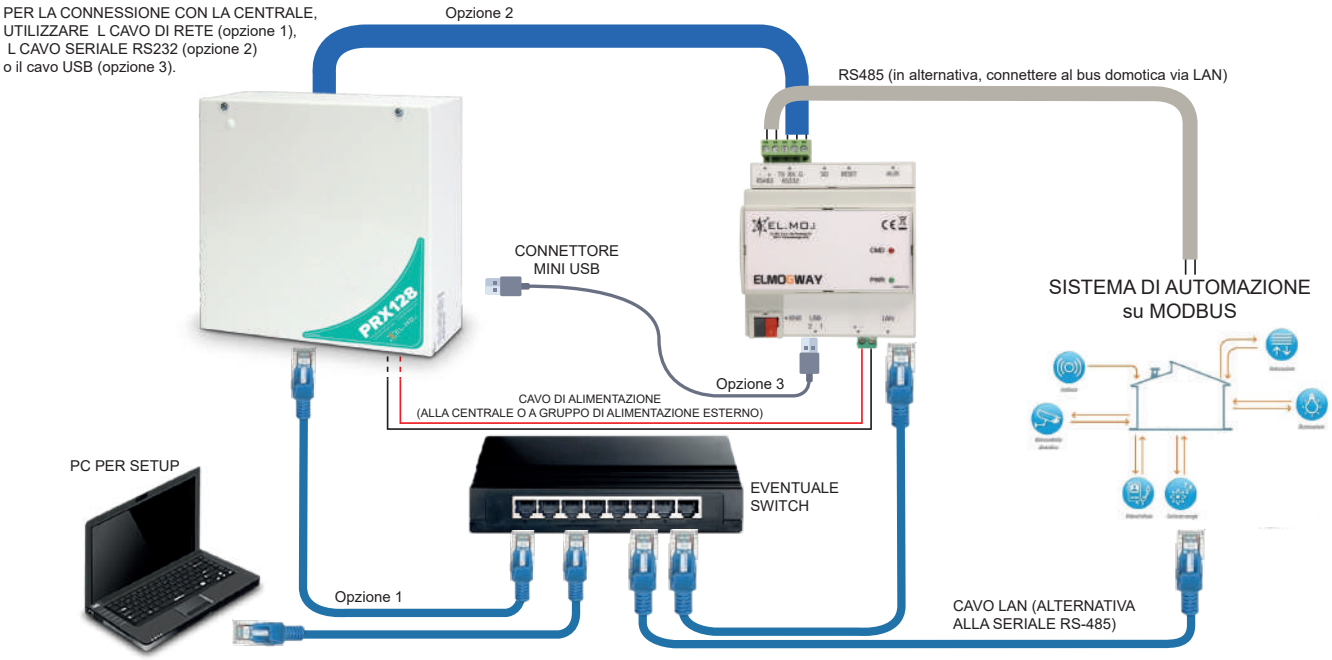
1. **Alimentazione**: fornire alimentazione tramite l'apposito connettore Sauro CGM verde. Il gateway potrà essere alimentato direttamente da centrale (nel qual caso si avrà la garanzia di continuità in caso di mancanza rete) oppure tramite gruppo di alimentazione esterno.
2. **Connessione alla centrale**: procedere connettendo il gateway alla centrale.
   Per ELMOGWAY sono possibili tre tipologie di connessione: RS-232, USB o LAN.
   Per ELMOGWAY2 sono possibili due tipologie di connessione: USB o LAN.
3. **Connessione al bus domotica**: collegare il gateway utilizzando un connettore diverso a seconda del protocollo in uso. Fare riferimento alla seguente tabella:

| Protocollo | Connettore |
|---|---|
| **MODBUS** | LAN oppure RS-485 |
| **KNX** | connettore KNX a bordo |
| **SCS** | LAN |

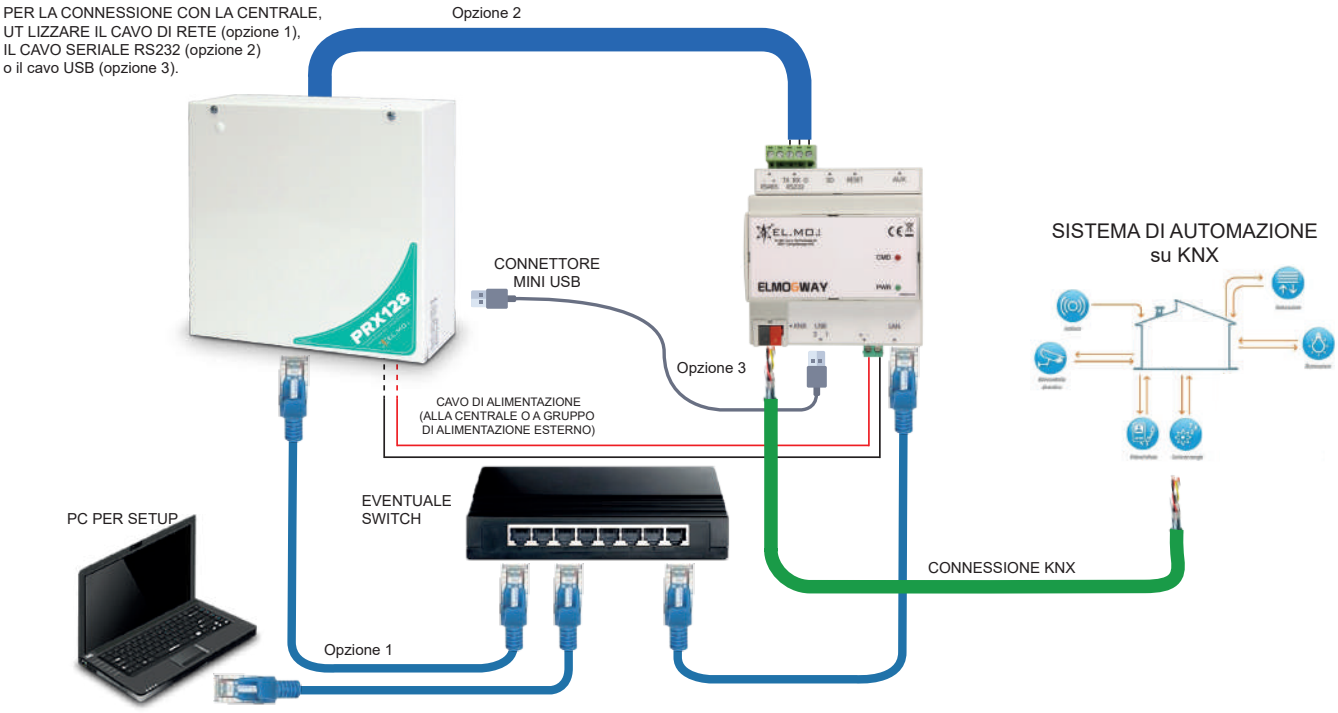
Una volta eseguito il cablaggio, procedere con la prima configurazione software come indicato nella sezione "6.1 Accesso al software di configurazione" a pagina 17.
**Nota**: qualora venga utilizzata una connessione via LAN, è d'obbligo assicurarsi che la connessione sia protetta e che la rete non sia aperta verso internet.
**Nota**: nel caso di connessione via RS-485, la linea seriale RS-485 del bus domotica **non deve mai** essere collegata alla linea seriale RS-485 del bus centrale.

## 5.3 Esempi di collegamento: ELMOGWAY

### Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo MODBUS.



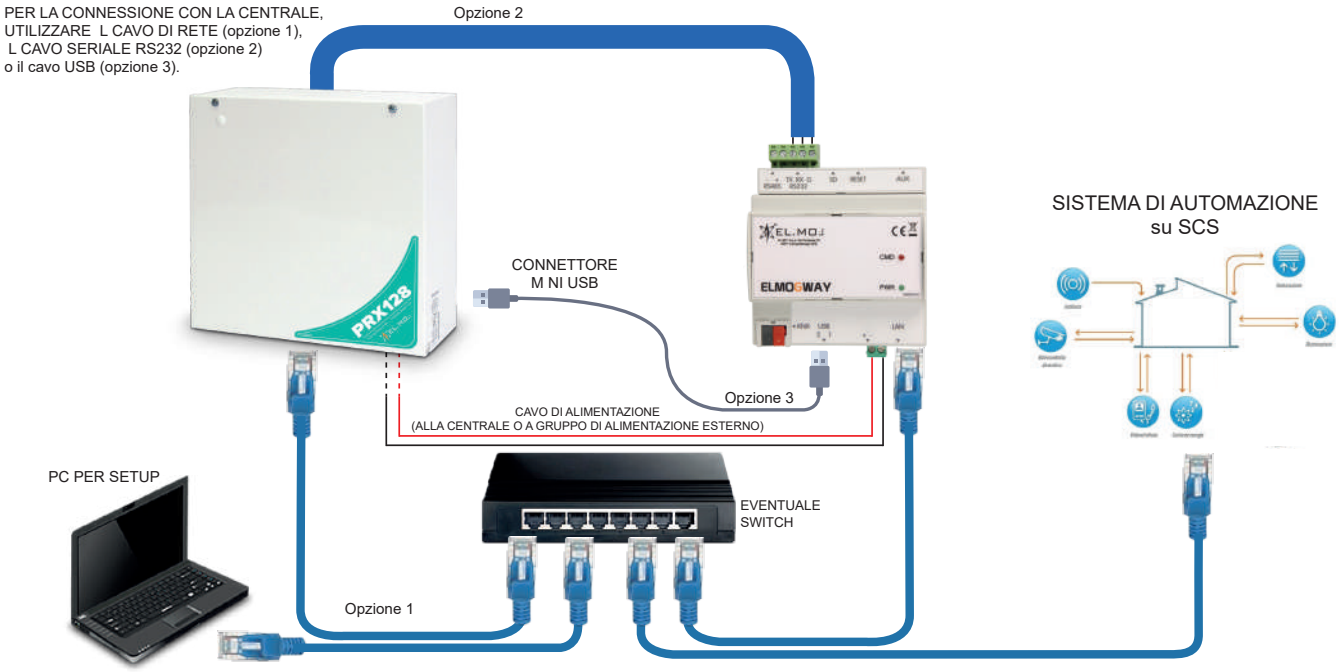

### Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo KNX.



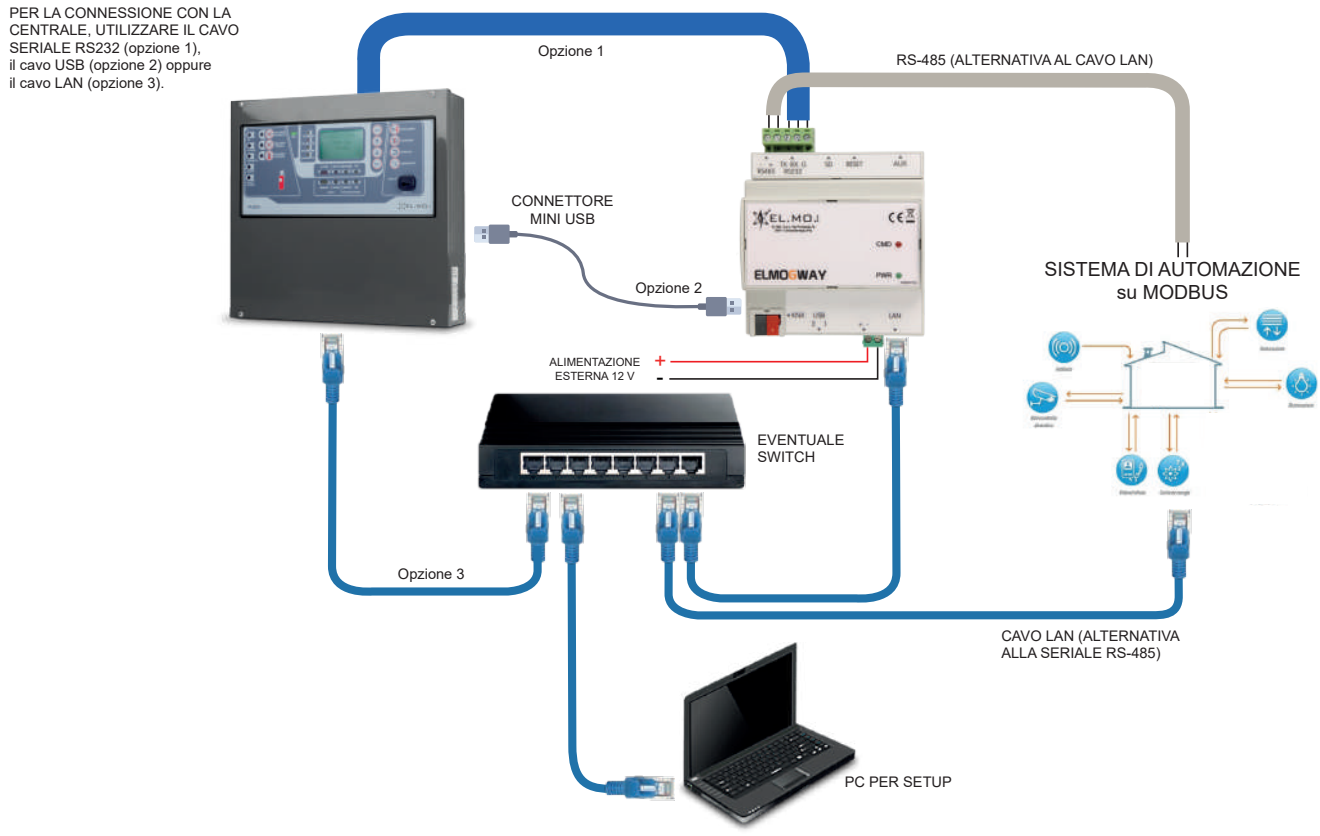



info@elmospa.com
elmospa.com

## Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo SCS.




## Esempi di connessione di una centrale antincendio TACÓRA ad un sistema di automazione attraverso il protocollo MODBUS.




**Nota:** Per realizzare la connessione via LAN, la centrale TACÓRA deve essere dotata di uno dei seguenti moduli:

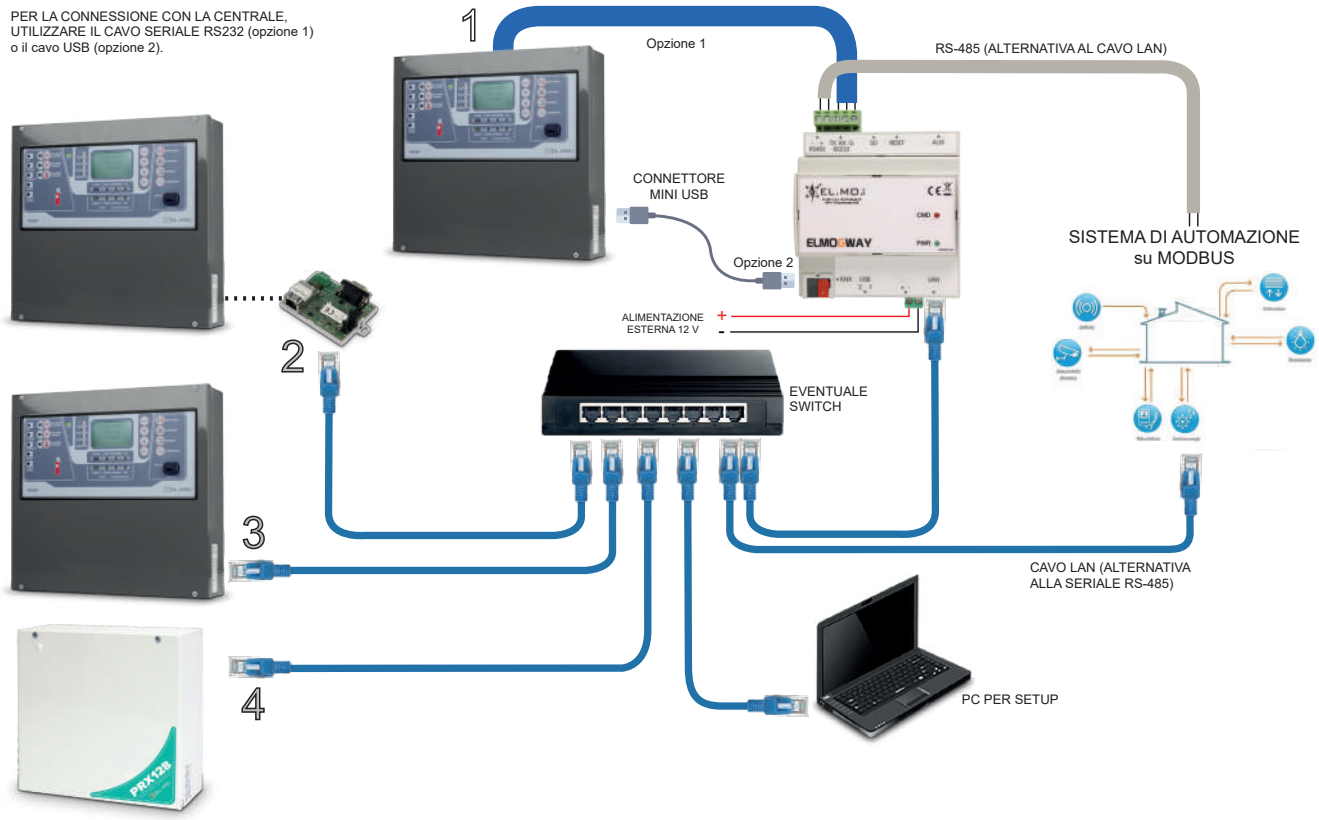
- scheda FXLAN2 (per qualsiasi versione firmware di TACÓRA)
- scheda MDLAN (per TACÓRA aventi versione firmware 5.2.2 o superiore)

**Esempio di connessione di una centrale antintrusione e più centrali antincendio TACÓRA contemporaneamente ad un sistema di automazione attraverso il protocollo MODBUS.**

È possibile connettere a ELMOGWAY una o più centrali TACÓRA e una centrale antintrusione contemporaneamente, purché nella sezione **Bridge Modbus** (vedere relative impostazioni di comunicazione alle pagine 30 e 35) venga impostata una porta IP diversa per ciascuna centrale.

Per realizzare la connessione centrale-gateway, è possibile scegliere una delle seguenti alternative:

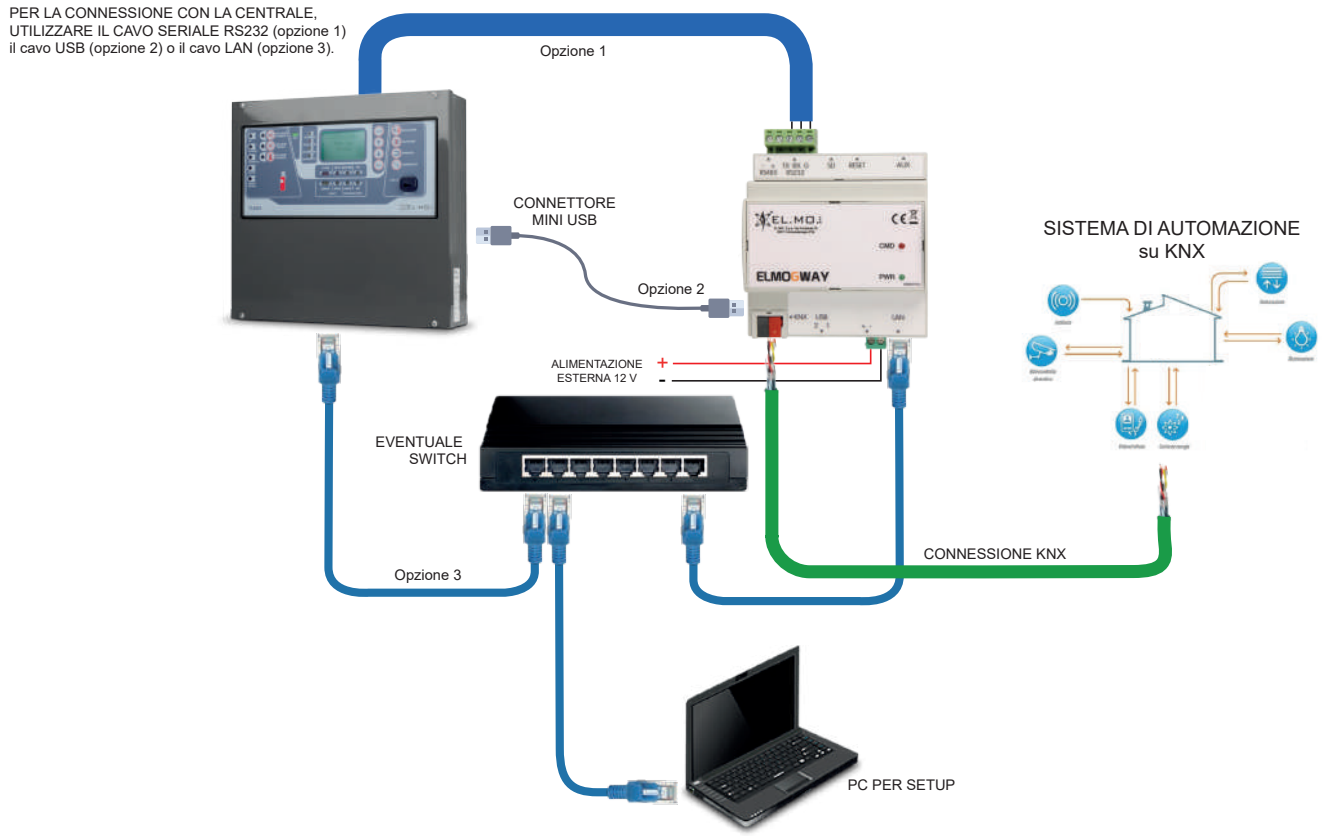
- collegare una centrale tramite cavo seriale RS-232 o USB e tutte le altre centrali tramite cavo LAN
- collegare tutte le centrali tramite cavo LAN




Nell'esempio, si suppone che siano connesse a ELMOGWAY:

1) una centrale TACÓRA via RS-232 o USB
2) una centrale TACÓRA avente firmware inferiore alla versione 5.2.2 connessa via LAN tramite FXLAN2
3) una centrale TACÓRA avente firmware di versione 5.2.2 connessa via LAN tramite MDLAN
4) una centrale antintrusione connessa via LAN

## Esempi di connessione di una centrale antincendio TACÓRA ad un sistema di automazione attraverso il protocollo KNX.



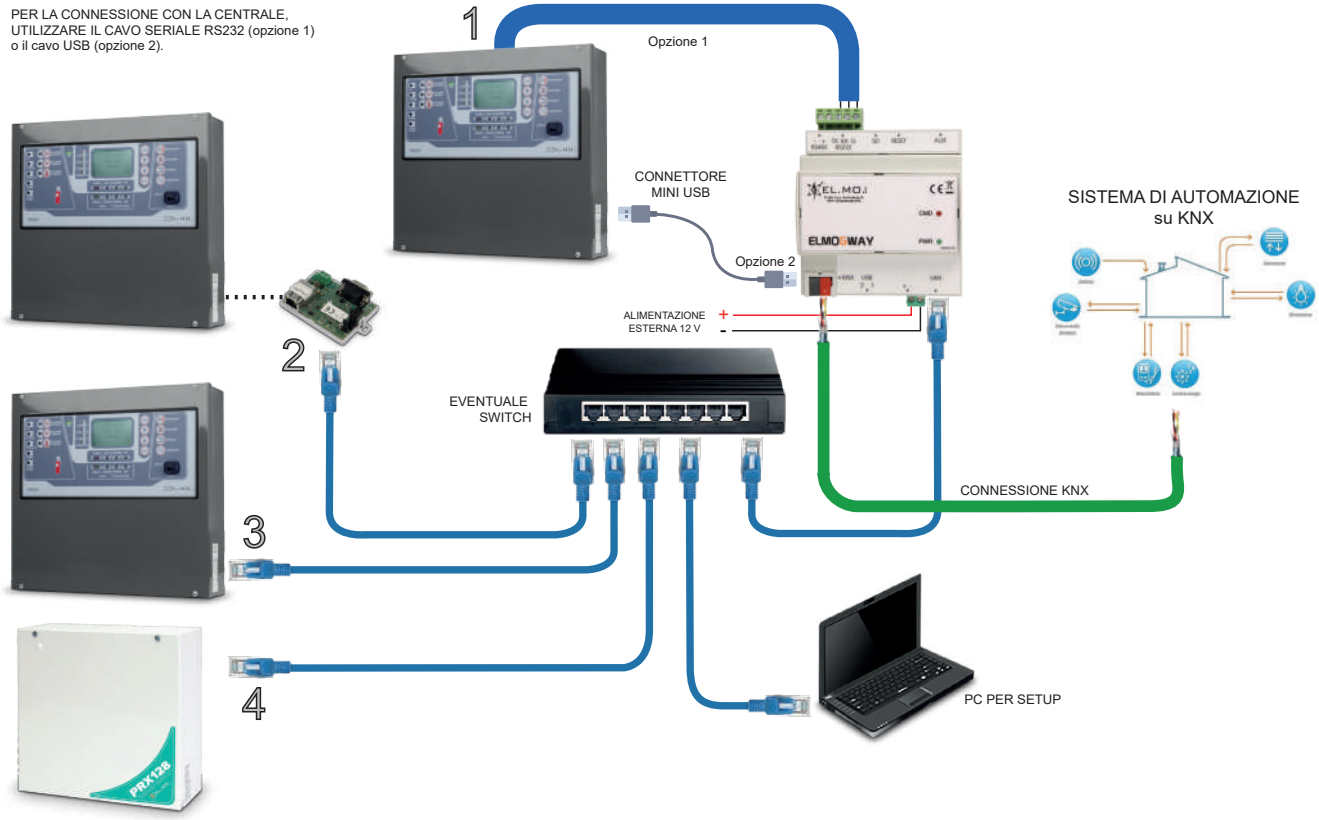

**Nota:** Per realizzare la connessione via LAN, la centrale TACÓRA deve essere dotata di uno dei seguenti moduli:

- scheda FXLAN2 (per qualsiasi versione firmware di TACÓRA)
- scheda MDLAN (per TACÓRA aventi versione firmware 5.2.2 o superiore)

**Esempio di connessione di una centrale antintrusione e più centrali antincendio TACÓRA contemporaneamente ad un sistema di automazione attraverso il protocollo KNX.**

Per realizzare la connessione centrale-gateway, è possibile scegliere una delle seguenti alternative:

- collegare una centrale tramite cavo seriale RS-232 o USB e tutte le altre centrali tramite cavo LAN
- collegare tutte le centrali tramite cavo LAN

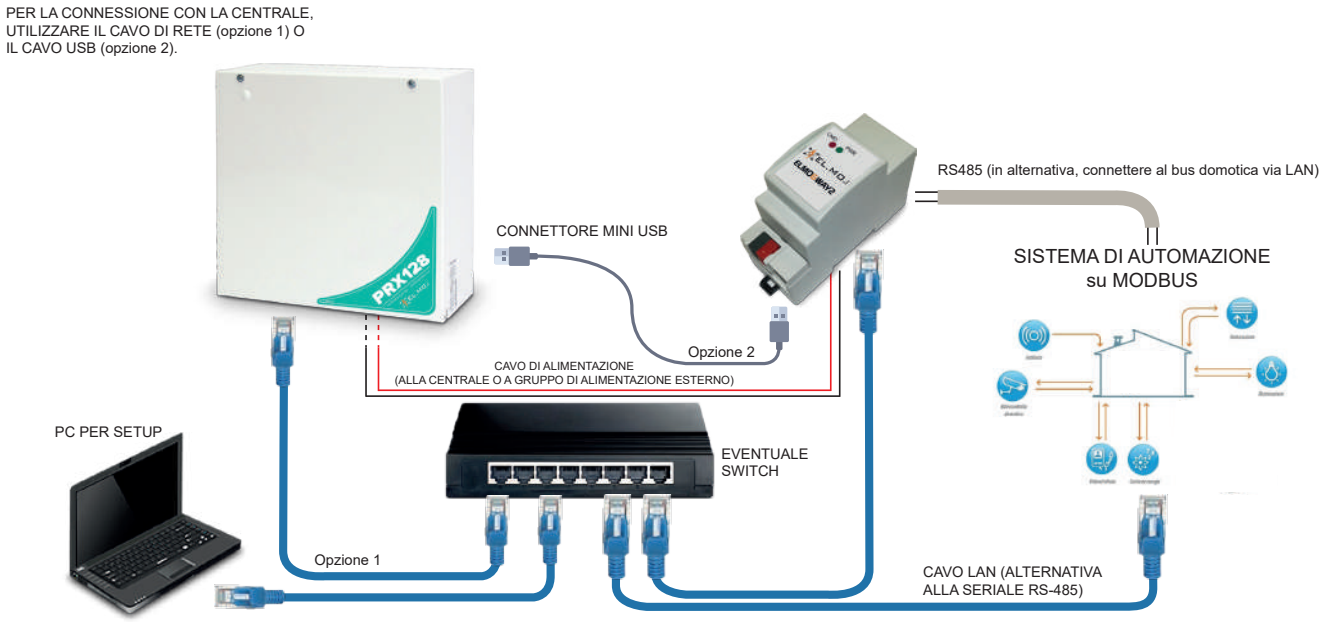



Nell'esempio, si suppone che siano connesse a ELMOGWAY:

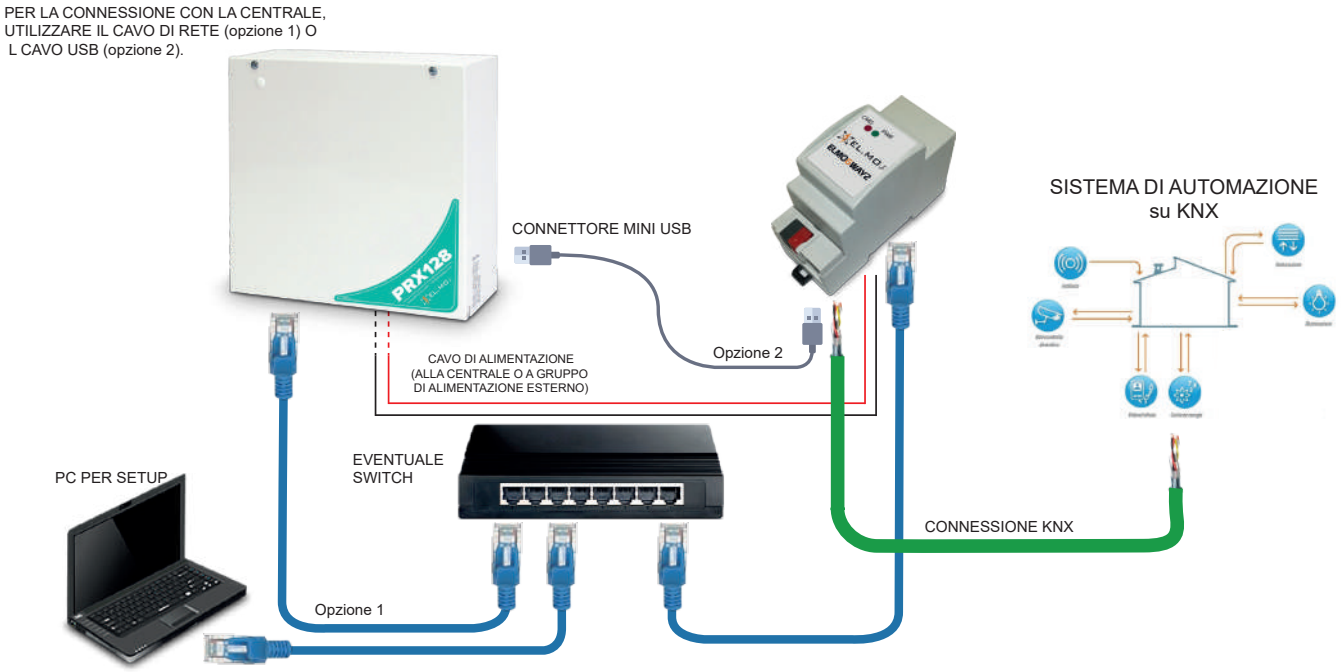
1) una centrale TACÓRA via RS-232 o USB
2) una centrale TACÓRA avente firmware inferiore alla versione 5.2.2 connessa via LAN tramite FXLAN2
3) una centrale TACÓRA avente firmware di versione 5.2.2 connessa via LAN tramite MDLAN
4) una centrale antintrusione connessa via LAN

## 5.4 Esempi di collegamento: ELMOGWAY2

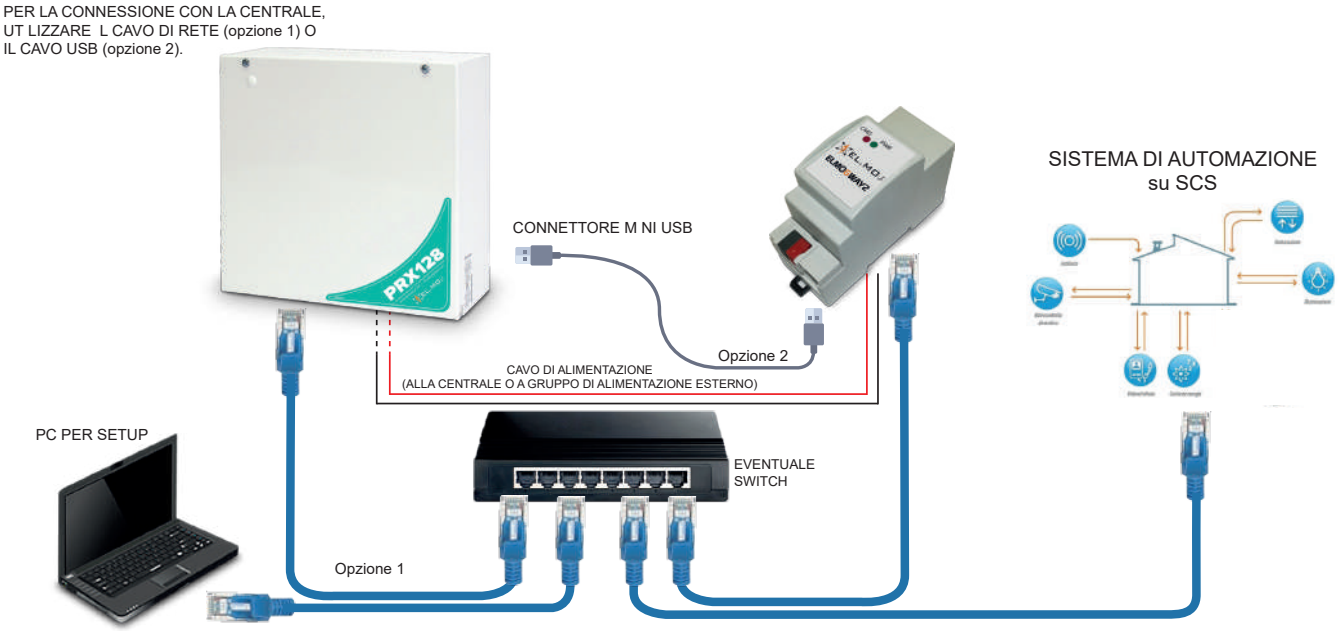
### Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo MODBUS.




### Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo KNX.



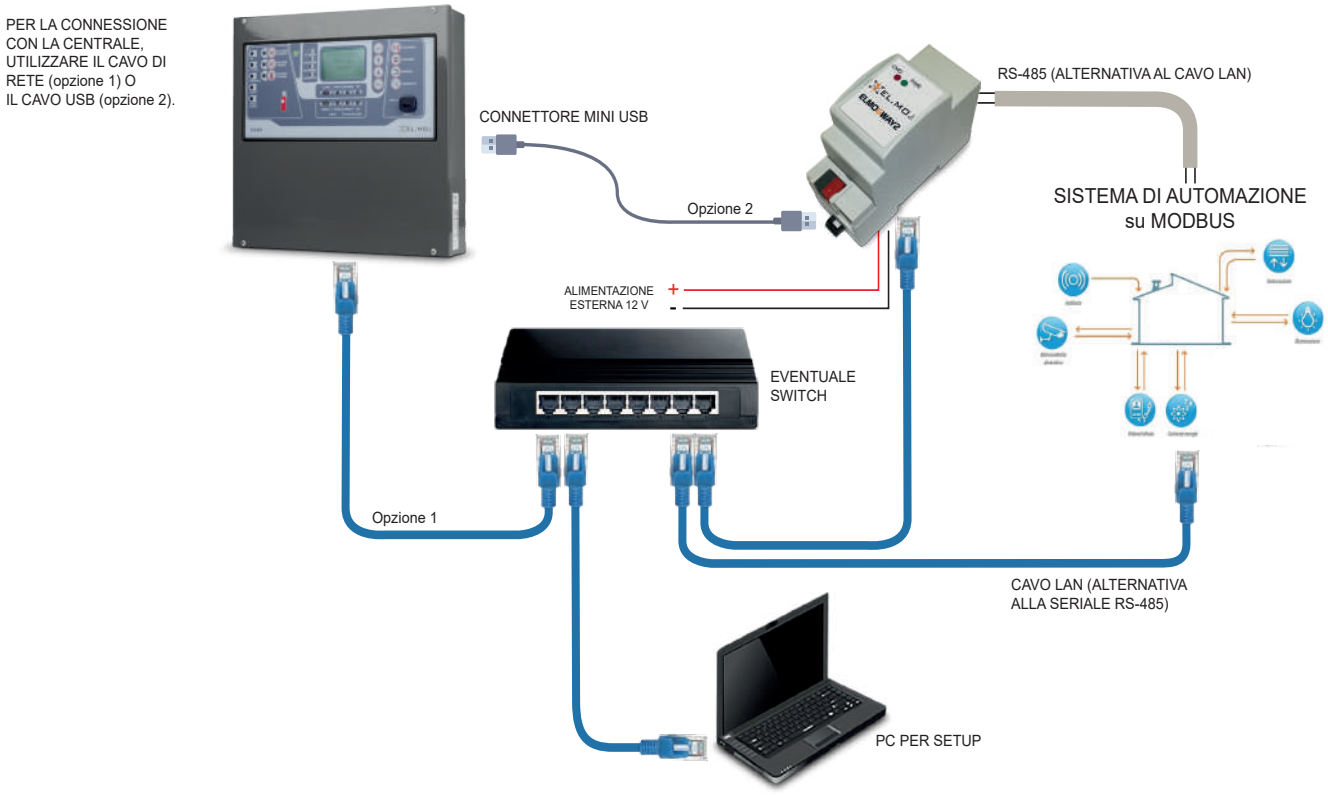
## Esempio di connessione di una centrale antintrusione ad un sistema di automazione attraverso il protocollo SCS.




## Esempio di connessione di una centrale antincendio TACÓRA ad un sistema di automazione attraverso il protocollo MODBUS.

Per realizzare la connessione via LAN, la centrale TACÓRA deve essere dotata di uno dei seguenti moduli:

- scheda FXLAN2 (per qualsiasi versione firmware di TACÓRA)
- scheda MDLAN (per TACÓRA aventi versione firmware 5.2.2 o superiore)



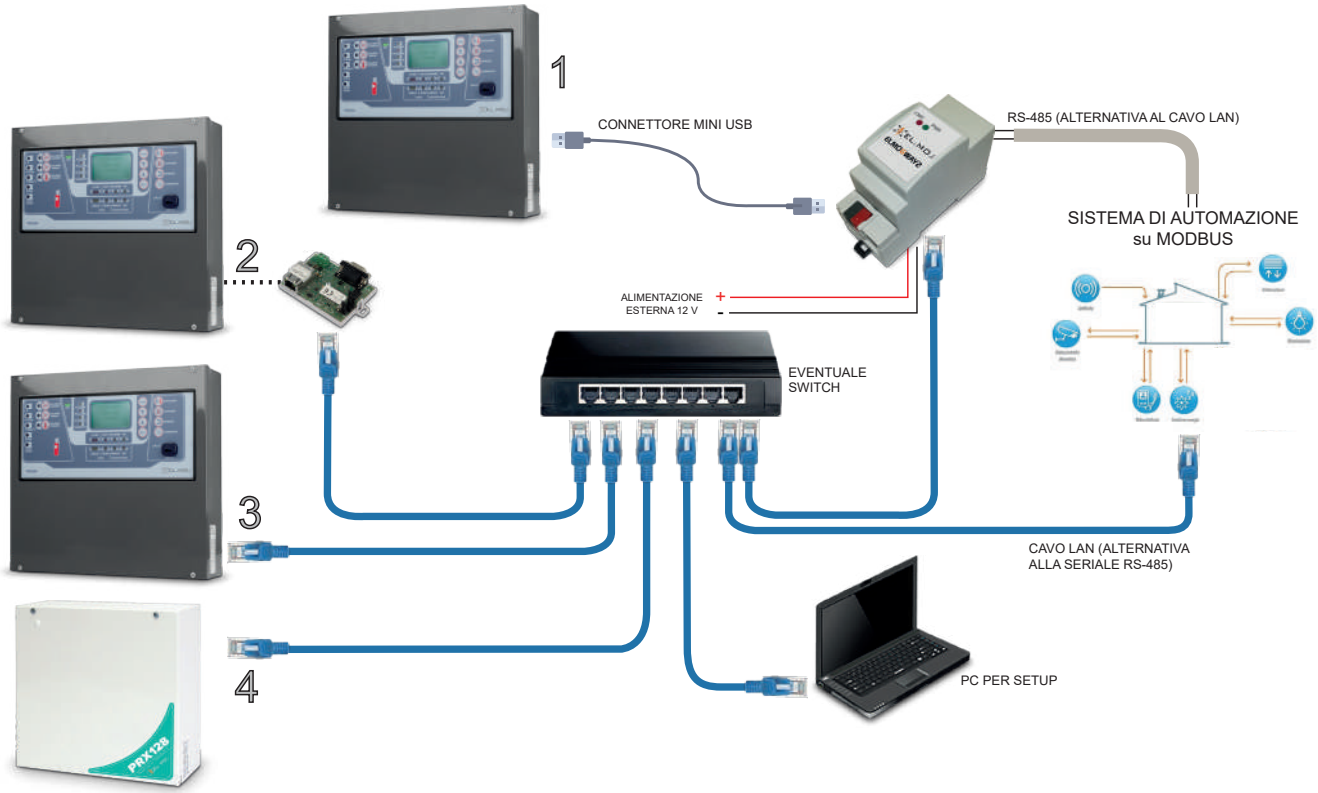

In alternativa, è possibile connettere la centrale antincendio al gateway via USB.

**Esempio di connessione di una centrale antintrusione e più centrali antincendio TACÓRA contemporaneamente ad un sistema di automazione attraverso il protocollo MODBUS.**

È possibile connettere a ELMOGWAY2 una o più centrali TACÓRA e una centrale antintrusione contemporaneamente, purché nella sezione **Bridge Modbus** (vedere relative impostazioni di comunicazione alle pagine 30 e 35) venga impostata una porta IP diversa per ciascuna centrale.

Per realizzare la connessione centrale-gateway, è possibile scegliere una delle seguenti alternative:

- collegare una centrale tramite cavo USB e tutte le altre centrali tramite cavo LAN
- collegare tutte le centrali tramite cavo LAN

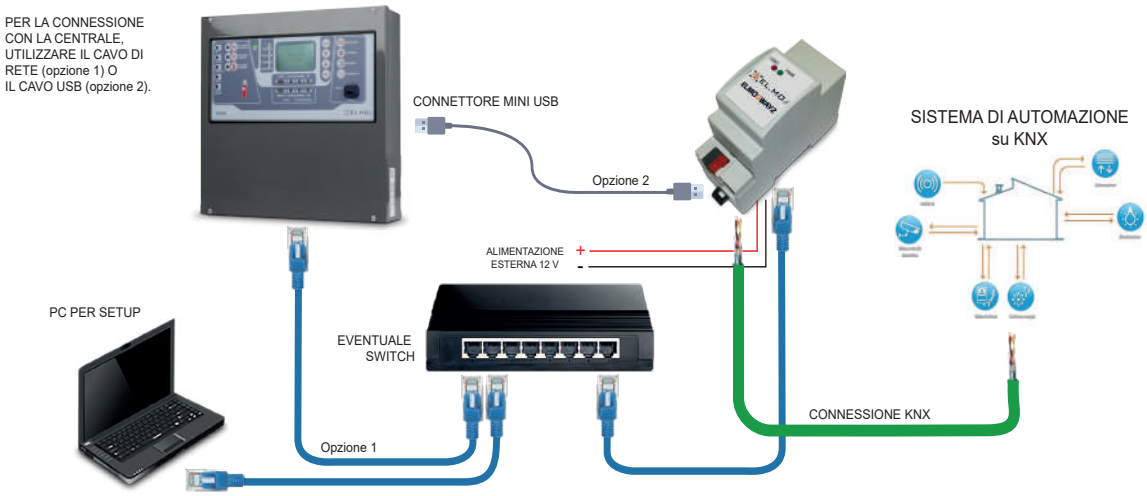



Nell'esempio, si suppone che siano connesse a ELMOGWAY2:

1) una centrale TACÓRA via USB
2) una centrale TACÓRA avente firmware inferiore alla versione 5.2.2 connessa via LAN tramite FXLAN2
3) una centrale TACÓRA avente firmware di versione 5.2.2 o superiore connessa via LAN tramite MDLAN
4) una centrale antintrusione connessa via LAN

**Esempio di connessione di una centrale antincendio TACÓRA ad un sistema di automazione attraverso il protocollo KNX.**
Per realizzare la connessione via LAN, la centrale TACÓRA deve essere dotata di uno dei seguenti moduli:

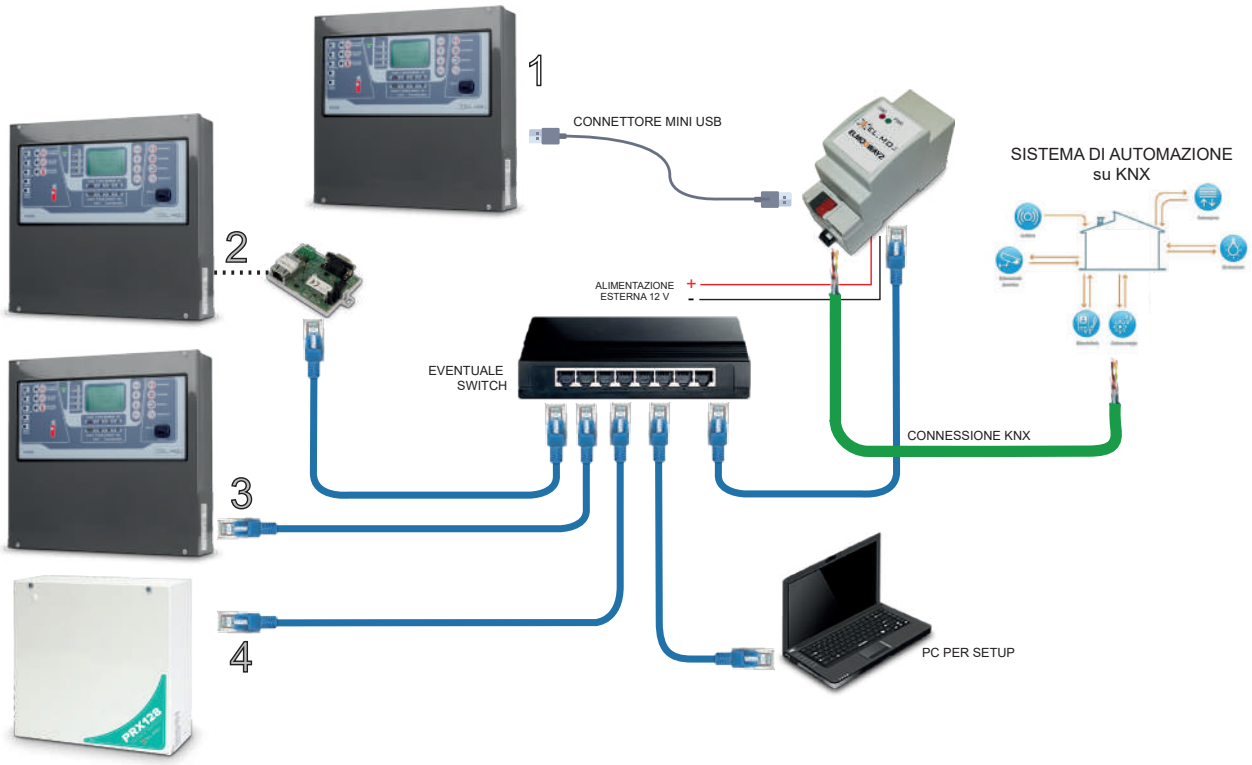
- scheda FXLAN2 (per qualsiasi versione firmware di TACÓRA)
- scheda MDLAN (per TACÓRA aventi versione firmware 5.2.2 o superiore)




In alternativa, è possibile connettere la centrale antincendio al gateway via USB.

**Esempio di connessione di una centrale antintrusione e più centrali antincendio TACÓRA contemporaneamente ad un sistema di automazione attraverso il protocollo KNX.**
Per realizzare la connessione centrale-gateway, è possibile scegliere una delle seguenti alternative:

- collegare una centrale tramite cavo USB e tutte le altre centrali tramite cavo LAN
- collegare tutte le centrali tramite cavo LAN

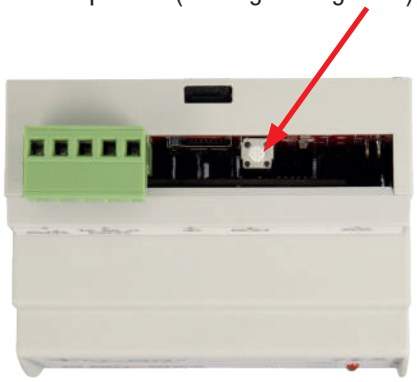



Nell'esempio, si suppone che siano connesse a ELMOGWAY2:

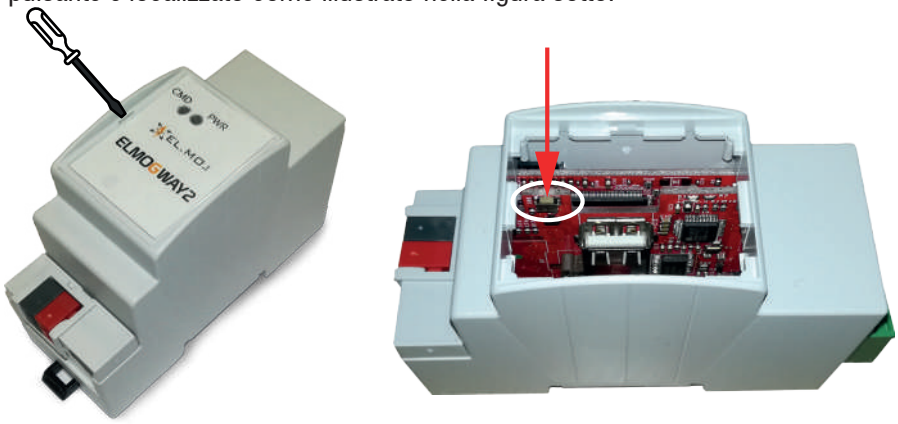
1) una centrale TACÓRA via USB
1) una centrale TACÓRA avente firmware inferiore alla versione 5.2.2 connessa via LAN tramite FXLAN2
2) una centrale TACÓRA avente firmware di versione 5.2.2 o superiore connessa via LAN tramite MDLAN
3) una centrale antintrusione connessa via LAN

### 5.5 Procedure di ripristino

È possibile effettuare due livelli di ripristino, quello del solo indirizzo IP di fabbrica e quello della configurazione di fabbrica (reset totale), a seconda della pressione esercitata sul pulsante RESET.
Su ELMOGWAY il pulsante è localizzato sul lato superiore (vedi figura seguente), liberamente accessibile.



Su ELMOGWAY2, per accedere al pulsante rimuovere il coperchio frontale facendo leva con un cacciavite in una delle due scanalature laterali. Il pulsante è localizzato come illustrato nella figura sotto.




Procurarsi un attrezzo isolato delle dimensioni sufficienti a raggiungere il pulsante.

#### 5.5.1 Ripristino indirizzo IP di fabbrica

Utilizzare la seguente procedura in caso sia necessario ripristinare il solo indirizzo IP di fabbrica:

1. Premere e tenere premuto il pulsante RESET per almeno 10 secondi, fino a che il LED rosso sul frontale del dispositivo non inizia a lampeggiare, quindi rilasciare il pulsante;
2. Entro i successivi 5 secondi, premere e tenere premuto per 1 secondo il pulsante, e in seguito rilasciarlo. Entro un paio di secondi, il LED frontale si accenderà fisso per circa 2 secondi;
3. Una volta che il LED si sarà spento, il gateway sarà raggiungibile all'indirizzo IP di fabbrica (192.168.0.110).

Se il LED si spegne dopo la pressione lunga (10 secondi) prima di aver effettuato la pressione breve, ripetere l'intera procedura.

#### 5.5.2 Ripristino configurazione di fabbrica

Utilizzare la procedura esposta di seguito in caso si debba effettuare un reset totale di ELMOGWAY, necessario qualora la configurazione effettuata renda impossibile l'accesso ad ELMOGWAY o il suo corretto utilizzo.
Durante il reset, il dispositivo verrà riconfigurato con i parametri di fabbrica, incluso il suo indirizzo IP.

1. Premere e tenere premuto il pulsante RESET per almeno 10 secondi, fino a che il LED rosso sul frontale del dispositivo non inizia a lampeggiare, quindi rilasciare il pulsante;
2. Entro i successivi 5 secondi, premere e tenere premuto il pulsante per almeno 10 secondi;
3. Quando il LED si accende fisso, rilasciare il pulsante ed attendere che il LED si spenga;
4. Allo spegnimento del LED, togliere e poi ripristinare l'alimentazione;
5. Attendere circa un minuto e infine accedere ad ELMOGWAY con l'indirizzo IP di fabbrica (192.168.0.110).

# 6. CONFIGURAZIONE VIA SOFTWARE

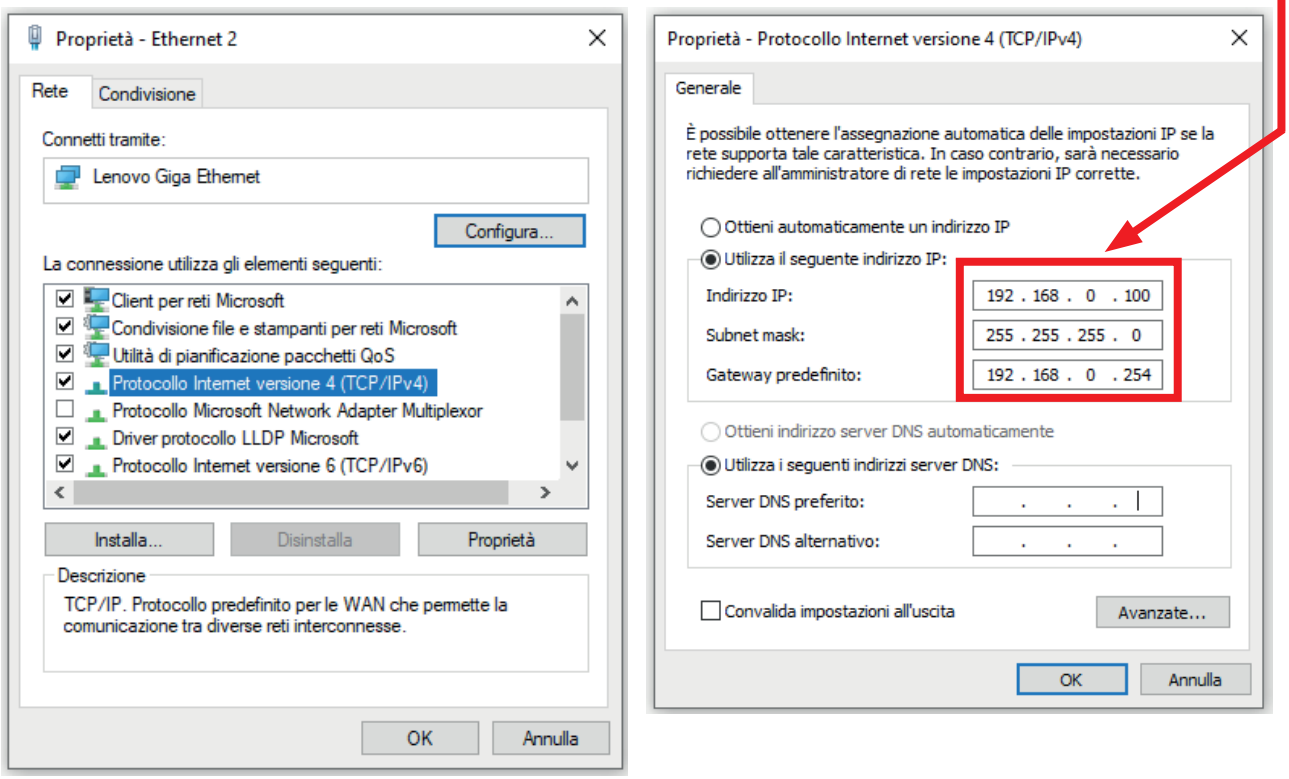
## 6.1 Accesso al software di configurazione

Procedere come segue per configurare il gateway tramite software dedicato, in caso di prima installazione o comunque ogni volta che vi sia necessità di manutenzione.

1. Connettere direttamente il gateway ad un PC tramite un cavo di rete, utilizzando la porta LAN presente sul lato inferiore.
2. Accedere alle proprietà LAN e TCP/IP del proprio PC e impostare temporaneamente l'indirizzo IP del PC come segue:

| | |
|---|---|
| ***Indirizzo IP*** | 192.168.0.100 |
| ***Maschera di rete*** | 255.255.255.0 |
| ***Gateway predefinito*** | 192.168.0.254 |

L'indirizzo del gateway potrà essere in seguito cambiato con quello della rete nella quale il dispositivo sarà inserito. A titolo esemplificativo, si riportano le finestre in cui impostare gli indirizzi se il PC utilizza il sistema operativo Windows 10:



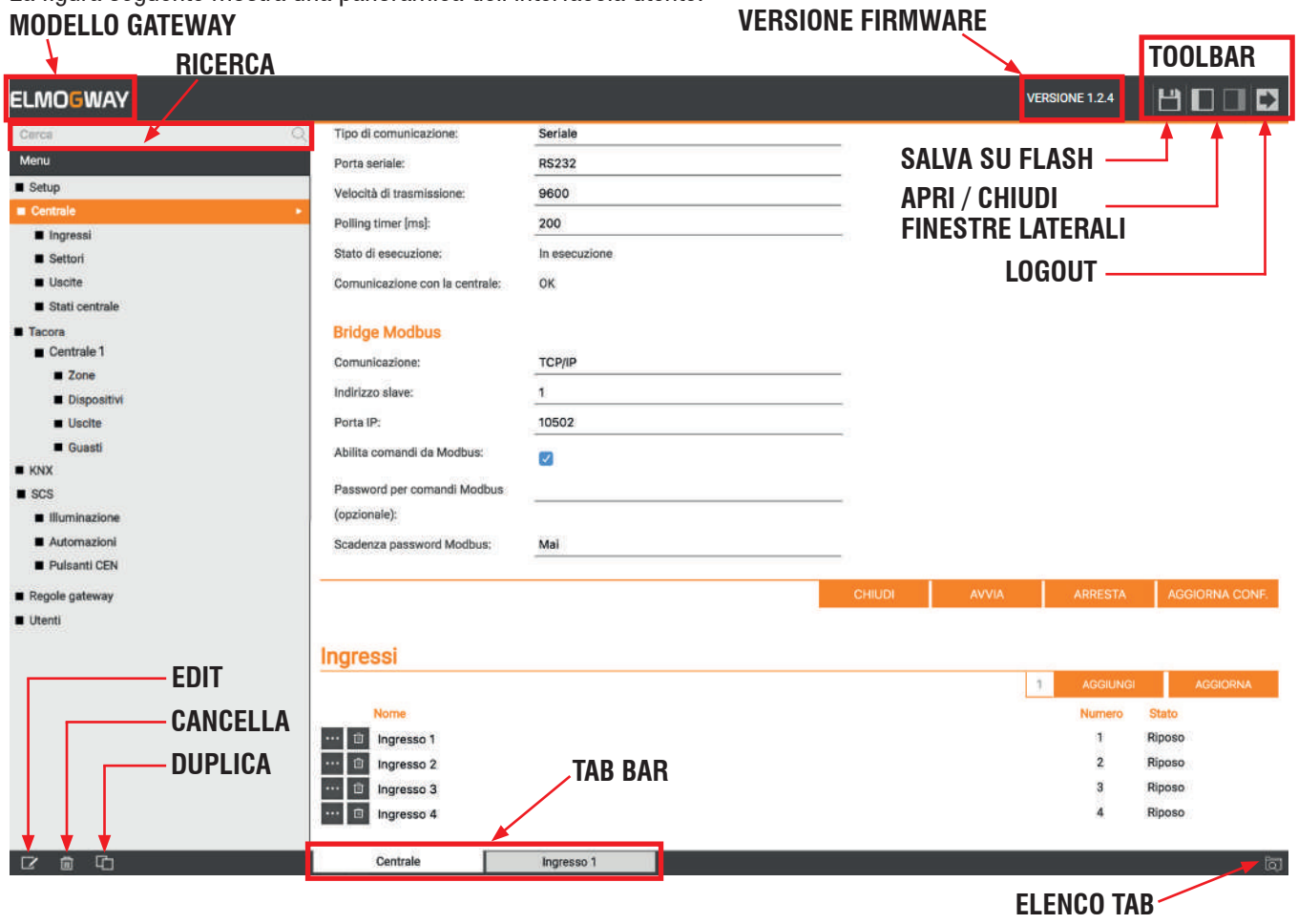

3. Aprire un browser (preferibilmente Google Chrome) al seguente indirizzo: **http://192.168.0.110**.
4. Una volta connessi al dispositivo, inserire quando richiesto le seguenti credenziali:

| | |
|---|---|
| ***Username*** | admin |
| ***Password*** | admin |

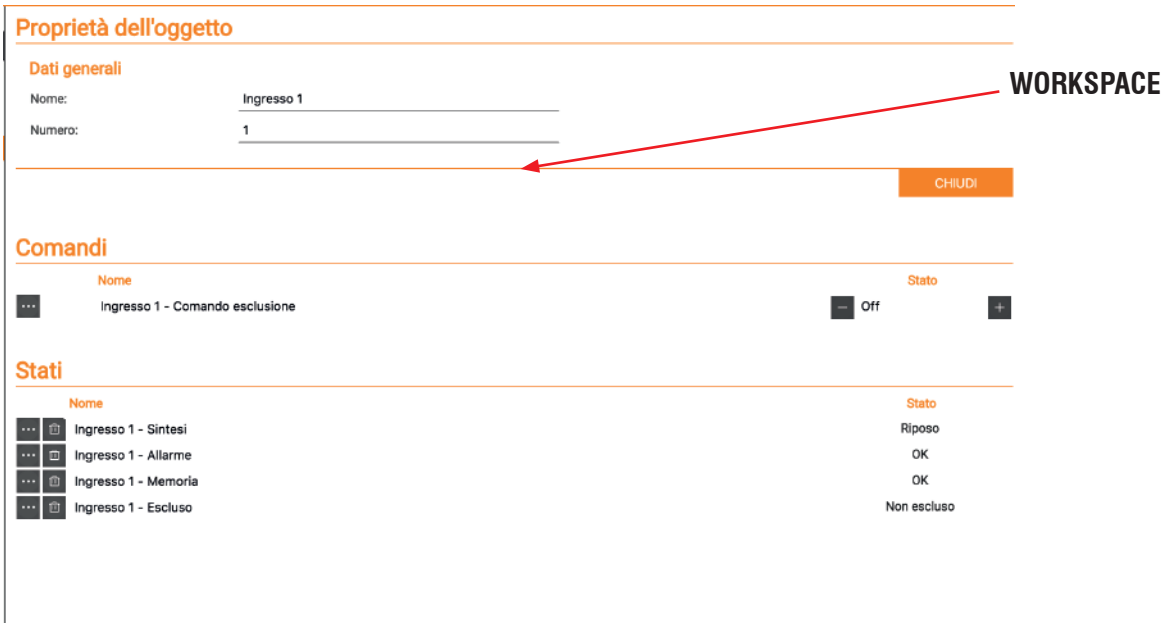
Una volta eseguito l'accesso, sarà possibile effettuare diverse operazioni.
Nei capitoli seguenti verranno fornite informazioni specifiche di configurazione per ciascuna sezione.

## 6.2 Panoramica generale dell'interfaccia utente

La figura seguente mostra una panoramica dell'interfaccia utente.




Lo spazio di lavoro principale viene chiamato **WORKSPACE**. Esso permette di operare su più pagine, passando da una all'altra tramite la **TAB BAR** presente in basso.
Se il numero di tab eccede lo spazio disponibile, la lista completa di tutte le pagine può essere consultata tramite l'apposito pulsante **ELENCO TAB** in basso a destra.



## MENU


Il menu nella parte sinistra della pagina del software fornisce accesso a tutte le funzioni del gateway
Aprendo una sezione, questa viene evidenziata ed eventualmente espansa per mostrare sotto-voci, se previste.
Alcune voci prevedono la visualizzazione, nella parte inferiore del menu, di uno o più dei seguenti pulsanti:

- NUOVO: crea un nuovo elemento all'interno della sezione evidenziata del menu.
- EDIT: modifica l'elemento selezionato.
- CANCELLA: rimuove definitivamente l'elemento selezionato.
- DUPLICA: duplica l'elemento selezionato.

Se un elemento è selezionato e può essere modificato, oltre al pulsante "EDIT" nella toolbar in basso, è disponibile anche una "scorciatoia" a fianco di esso sotto forma di tre puntini. 

In entrambi i casi, la pressione provoca l'apertura di un nuovo tab all'interno del workspace.
Se un elemento è già aperto, è visibile in corrispondenza una freccia. 

## TOOLBAR

La toolbar (in alto a destra) contiene i seguenti pulsanti:

- SALVA SU FLASH: Forza il salvataggio su memoria persistente.
  Il salvataggio avviene in automatico durante la configurazione; se è necessario togliere alimentazione al gateway mentre questo pulsante è rosso, premerlo per forzare il salvataggio.
- APRI / CHIUDI FINESTRE LATERALI: apre e chiude i pannelli laterali dell'interfaccia utente.
- LOGOUT: Termina la sessione di lavoro.

## RICERCA

Inserire qui una o più parole chiave, per ricercare uno o più elementi nel progetto che siano stati precedentemente creati.
È possibile selezionare più elementi dalla ricerca tenendo premuto il pulsante CTRL.
È possibile interagire con i risultati della ricerca tramite i pulsanti disponibili nella toolbar (i pulsanti hanno lo stesso significato della toolbar del menu).

## 6.3 Menu SETUP

La pagina "**Setup**" permette di effettuare la configurazione dei parametri generali del gateway e svolgere le principali operazioni di manutenzione.


### 6.3.1 Lingua

Questa sezione permette di selezionare la lingua del gateway (italiano o inglese).

### 6.3.2 Rete

In questa sezione è possibile impostare i seguenti parametri per la configurazione in rete LAN del gateway:

| | |
|---|---|
| ***INDIRIZZO IP*** | Indirizzo del gateway nella rete LAN |
| ***MASCHERA DI RETE*** | Default: 255.255.255.0 |
| ***GATEWAY*** | Gateway predefinito<br>Default: indirizzo IP del router |
| ***DNS PRIMARIO***<br>***DNS SECONDARIO*** | Indirizzi DNS per accesso a Internet |

### 6.3.3 Backup/Restore

In questa sezione è possibile:

- effettuare una copia di backup del proprio progetto
- importare un backup effettuato in precedenza
- riportare il gateway alle impostazioni di fabbrica scegliendo l'apposita voce (l'indirizzo di rete non viene modificato)

Scelta l'operazione che si desidera effettuare (e selezionato il file di backup nel caso di importazione), premere il pulsante "ESEGUI" ed attendere la fine delle operazioni, segnalata da un apposito messaggio a video.
Non interrompere la procedura effettuando altre operazioni nel browser o chiudendolo, pena possibili malfunzionamenti.

### 6.3.4 Data/Ora

In questa sezione è possibile impostare una serie di opzioni relative all'orologio di sistema.
Le informazioni richieste sono le seguenti:

| | |
|---|---|
| ***ORA***<br>***DATA*** | Data e ora correnti. |
| ***AREA***<br>***CITTÀ*** | Area geografica e capitale di riferimento per impostare il corretto fuso orario. |
| ***SERVER NTP***<br>***OGNI*** | Eventuale server per l'aggiornamento automatico dell'ora, e periodicità (in minuti) della sincronizzazione dell'orologio di sistema. |

**Nota**: Salvo esigenze specifiche, si consiglia di mantenere le impostazioni predefinite.

### 6.3.5 Aggiornamento software

In questa sezione è possibile aggiornare il software del gateway.
**Utilizzare solo pacchetti di installazione ufficiali, pena possibili malfunzionamenti.**
Aggiornare il software del gateway procedendo come segue:

1. Salvare il pacchetto di aggiornamento (scaricato dal sito oppure ricevuto via email) sul proprio PC, senza scompattarlo;
2. Aprire la pagina di aggiornamento;
3. Selezionare il pacchetto di aggiornamento mediante il pulsante "SFOGLIA" (o similare, in base al proprio browser).

**Nota per gli utenti MAC**: se si scarica il pacchetto utilizzando il browser SAFARI oppure il client di posta elettronica MAIL, il pacchetto viene automaticamente scompattato: questo comporta il mancato funzionamento dell'aggiornamento. Si consiglia di scaricare il pacchetto utilizzando un browser e/o client di posta elettronica differente.

**Nota**: per effettuare l'aggiornamento, utilizzare esclusivamente i browser Google Chrome (in ambiente Windows) o Apple Safari (in ambiente Mac OSX): altri browser potrebbero indurre problemi e rendere inutilizzabile il webserver.

4. Accertarsi di non disporre già della medesima versione software (riportata all'inizio della pagina);
5. Fare click sul pulsante "AGGIORNA".

La procedura di aggiornamento avviene automaticamente; attendere il suo completamento **senza effettuare alcuna altra operazione sul browser e senza chiuderlo (pena il possibile malfunzionamento del webserver)**.
La procedura può richiedere anche diversi minuti, in base alla propria versione del software e configurazione.
Al termine viene proposto un riepilogo sintetico dell'operazione, con la nuova versione software: per completare la procedura, premere sul pulsante "RIAVVIA" che provvede a riavviare il sistema operativo del gateway.

Qualora la procedura di aggiornamento dovesse interrompersi per cause accidentali (ad esempio: interruzione dell'alimentazione o della connessione di rete con il proprio PC), si consiglia di provare ad effettuare le seguenti operazioni:

1. Spegnere ed accendere nuovamente il gateway:
2. Attendere un minuto, quindi aprire il browser all'indirizzo IP del gateway;
3. Attendere che la procedura di ripristino automatico venga completata, ed il gateway venga nuovamente riavviato.

**Nota**: la procedura di ripristino automatico viene avviata anche eseguendo un ripristino completo da pulsante di reset. Se il ripristino automatico non si sblocca (attendere almeno 15 minuti per sicurezza), contattare la nostra assistenza tecnica.

### 6.3.6 Manutenzione

In questa sezione è possibile:

- accedere ai parametri hardware del dispositivo (**dati macchina**: codice seriale, codice hardware, chipset);
- consultare lo stato del sistema (tempo dall'ultimo avvio e informazioni RAM, con possibilità di scaricare il file di storico dati);
- effettuare il riavvio dei servizi di comunicazione e del sistema.

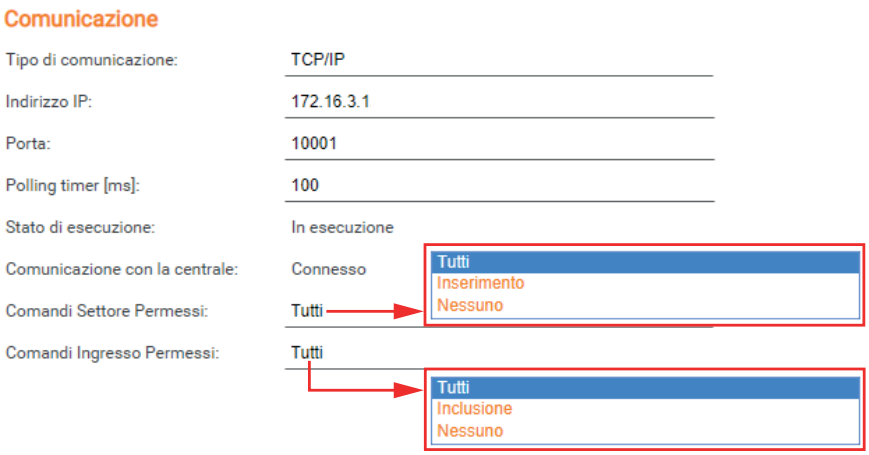
## 6.4 Menu CENTRALE - centrale antintrusione

La pagina "**Centrale**" consente di mappare la comunicazione con la centrale antintrusione e gestire ingressi, uscite, settori e stati della centrale.


**ATTENZIONE:**
Nell'integrazione del gateway in sistemi antintrusione, occorre mantenere intatto il livello di sicurezza ottenuto in fase di installazione rispettando i dettami delle norme.
In particolare, inserimento e disinserimento delle centrali devono avvenire sempre attraverso gli organi di comando delle centrali stesse. Anche la disabilitazione e l'esclusione di sensori devono essere effettuate con estrema cautela.

**Nota**: le pagine web sono uno strumento di verifica. Esse non sono indicative dei tempi di risposta reali del sistema.

### 6.4.1 Impostazioni generali




In questa sezione preliminare del menu "**Centrale**" vengono impostati i parametri di connessione con la centrale antintrusione:

| DATI GENERALI | |
|---|---|
| ***NOME*** | Etichetta identificativa della centrale. |
| ***UTENTE*** | Codice utente che il gateway utilizza per dialogare con la centrale.<br>Deve essere un codice numerico valido in centrale. |
| ***CODICE*** | Codice numerico (password) di autenticazione dell'utente in centrale. |

| COMUNICAZIONE | |
|---|---|
| ***TIPO DI COMUNICAZIONE*** | Scelta della modalità di comunicazione del gateway: RS-232 (comunicazione seriale), IP (comunicazione tramite protocollo TCP/IP), USB (comunicazione tramite porta USB) |
| ***PORTA SERIALE*** | Porta di comunicazione da utilizzare, in caso di comunicazione seriale (default: RS-232). ***(opzione disponibile solo in comunicazione seriale)*** |
| ***VELOCITÀ DI TRASMISSIONE*** | Baud rate di comunicazione ***(opzione disponibile solo in comunicazione seriale e USB. Per la USB, impostare 9600)*** |
| ***INDIRIZZO IP*** | Indirizzo e porta della centrale in rete LAN<br>(default: 10001). |
| ***PORTA*** | |

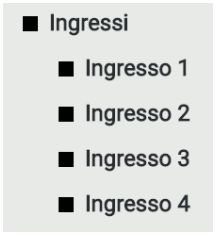
| COMUNICAZIONE | |
|---|---|
| ***POLLING TIMER*** | Tempo di interrogazione della centrale (in ms).<br>Regolare il tempo di interrogazione per accelerare o ridurre la frequenza con cui il gateway richiede lo stato alla centrale. |
| ***STATO DI ESECUZIONE*** | Stato di funzionamento del driver di comunicazione con la centrale.<br>In condizioni normali deve essere "IN ESECUZIONE". |
| ***COMUNICAZIONE CON LA CENTRALE*** | **Connesso**: connessione presente.<br>**Non connesso**: comunicazione assente.<br>**Password error**: password o codice utente errato. |
| ***COMANDI SETTORE PERMESSI (*)*** | Selezionare uno dei seguenti valori:<br>**Tutti**: sono ammessi sia il comando di inserimento che il comando di disinserimento.<br>**Inserimento**: è ammesso solo il comando di inserimento.<br>**Nessuno**: non è ammesso alcun comando. |
| ***COMANDI INGRESSO PERMESSI (*)*** | Selezionare uno dei seguenti valori:<br>**Tutti**: sono ammessi sia il comando di inclusione che il comando di esclusione.<br>**Inclusione**: è ammesso solo il comando di inclusione.<br>**Nessuno**: non è ammesso alcun comando. |

***(*) Nota:*** i Comandi Settore e Ingresso Permessi definiti sopra agiscono sui comandi da KNX, SCS, Modbus e da pannello.

La comunicazione con la centrale può essere avviata o arrestata utilizzando rispettivamente i pulsanti "AVVIA" e "ARRESTA". Il pulsante "AGGIORNA CONF." effettua un arresto e successivo avvio della comunicazione.

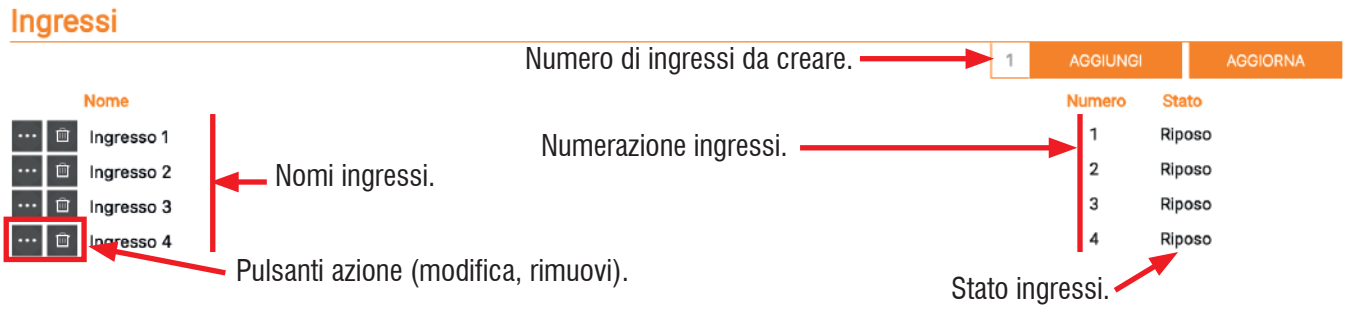

Tra i parametri configurabili in questa sezione, rientrano anche quelli relativi alla connessione tramite protocollo MODBUS ("**Bridge Modbus**"). Si rimanda alla sezione specifica di questo manuale ("7. PROTOCOLLO MODBUS - CENTRALI ANTINTRUSIONE" a pagina 30) per informazioni sulla configurazione con questo protocollo.

### 6.4.2 Ingressi




In questa sezione è possibile aggiungere e configurare i sensori della centrale antintrusione all'interno del gateway. Per inserire gli ingressi, procedere nel modo seguente:

1. Specificare il numero di ingressi che si desidera aggiungere nell'apposito campo a fianco del pulsante "AGGIUNGI" (default: 1);
2. Premere il pulsante "AGGIUNGI" ed attendere la fine dell'operazione. Gli ingressi appena creati verranno automaticamente accodati a quelli esistenti.




Una volta creati, è possibile modificare il nome degli ingressi e la loro numerazione (si consiglia comunque di mantenere la numerazione proposta in automatico), e consultarne lo stato.
I pulsanti azione a lato di ogni nome ingresso permettono di accedere alla scheda di dettaglio del singolo ingresso e rimuovere definitivamente un ingresso dal progetto.


L'immagine precedente mostra la scheda di un singolo ingresso nel dettaglio.
Tramite la sezione "**Comandi**" è possibile inviare il comando di esclusione all'ingresso: impostando ON attraverso l'apposito selettore, verrà escluso l'ingresso in questione.
La sezione "**Stati**" visualizza le diverse informazioni di stato aggiornate in tempo reale. Ciascun ingresso è caratterizzato dai seguenti stati:

- **Sintesi**: Etichetta che identifica lo stato di riepilogo dell'ingresso;
- **Allarme**: ON/OFF in base allo stato di allarme del sensore;
- **Memoria**: ON/OFF in base alla memoria di allarme del sensore;
- **Escluso**: ON/OFF in base allo stato di esclusione del sensore.

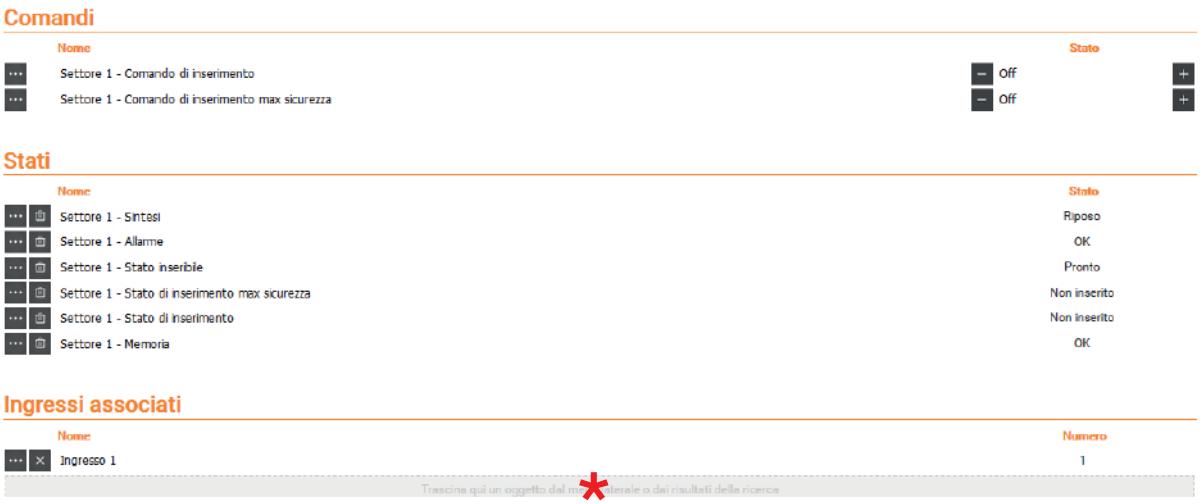
Normalmente il gateway non si interfaccia con tutti gli ingressi disponibili, ma solo con un numero ridotto.
Per facilitare il setup, è possibile generare solamente il numero di ingressi necessari, assegnando poi ad ogni elemento creato il reale indirizzo fisico ed etichetta:


In tal modo, se ad esempio le linee da interfacciare effettivamente necessarie sono solo 16, se ne possono generare 16 utilizzando la procedura esposta in precedenza e poi, ad esempio, si può attribuire l'ultima linea all'ingresso 233 senza necessità di generare 233 ingressi. È possibile procedere in modo analogo anche per le uscite e i settori.

**Nota:** se un ingresso di centrale è stato impostato via BrowserOne come ingresso di tipo "Controllo remoto", per il corretto funzionamento con il gateway è necessario che sia abilitata la proprietà "Piccola manutenzione" per l'utente associato alla domotica.

### 6.4.3 Settori


In questa sezione è possibile configurare i settori della centrale, associandovi i vari ingressi.
In modo analogo a quanto visto nella sezione precedente per gli ingressi, è possibile specificare quanti settori creare e confermarne la creazione premendo il pulsante "AGGIUNGI"; una volta creati gli elementi, è possibile modificarne alcuni attributi, consultarne lo stato, oppure accedere alla scheda di dettaglio di ciascun settore come illustrato nell'immagine seguente:




Sono configurabili i seguenti "**Comandi**" tramite gli appositi selettori:

- **Comando di inserimento**: inserisce il settore in modalità "normale";
- **Comando di inserimento massima sicurezza**: inserisce il settore in modalità "alta sicurezza" o prioritaria.

La sezione "**Stati**" visualizza le diverse informazioni di stato aggiornate in tempo reale.
Ciascun settore è caratterizzato dai seguenti stati:

- **Sintesi**: stato del settore;
- **Allarme**: stato di allarme del settore;
- **Stato inseribile**: identifica se il settore è pronto per essere inserito o meno;
- **Stato di inserimento**: ON se il settore è inserito;
- **Stato di inserimento massima sicurezza**: ON se il settore è inserito in modalità massima sicurezza;
- **Memoria**: stato di memoria allarme del settore.

**Nota**: nella sezione "**Ingressi associati**" è possibile associare gli ingressi desiderati a ciascun settore: è sufficiente cercare gli ingressi (identificandoli nel menu laterale oppure cercandoli con lo strumento di ricerca) e trascinarli nel campo grigio indicato da * . Sono possibili selezioni multiple.

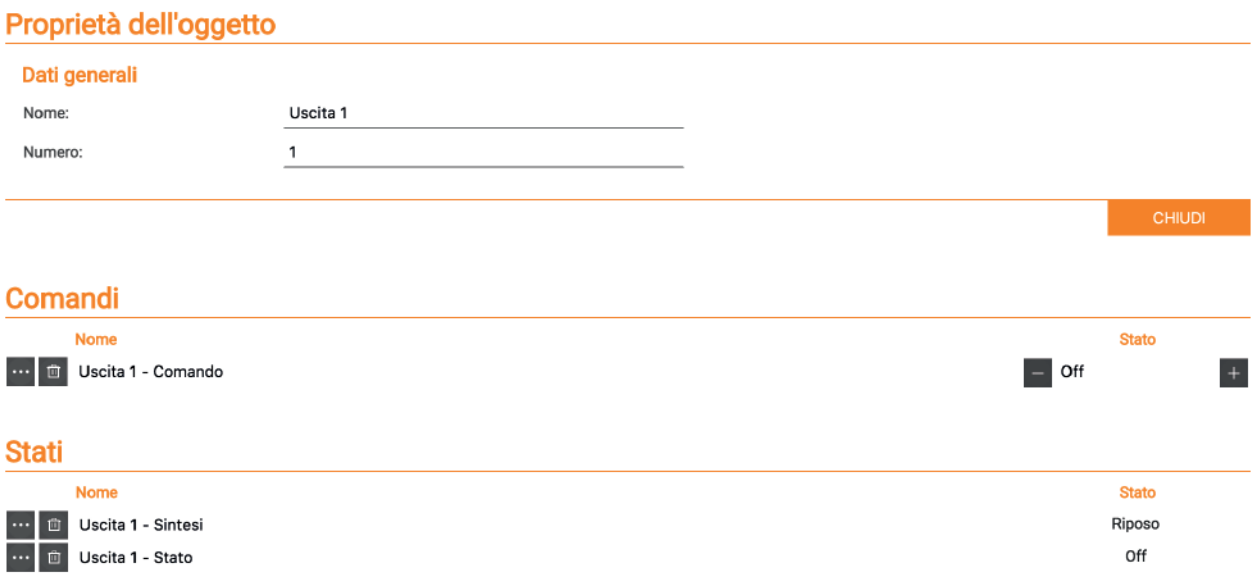
Associando gli ingressi al settore, diventano disponibili la lettura dei registri modbus "stato allarme settore 1...x" e "stato memoria settore 1...x" e le uscite dell'elemento settore nelle regole.
Un ingresso non associato non rende disponibili tali registri o uscite.

**Numerazione dei settori**
I settori sono sempre numerati in modo sequenziale. Ad esempio, una centrale con 8 aree di 4 settori ciascuna ha in totale 32 settori numerati da 1 a 32: di conseguenza, il settore 2 dell'area 2 è il numero 6 dell'elenco.

### 6.4.4 Uscite

In questa sezione è possibile configurare le uscite della centrale.


In modo analogo a quanto visto nelle sezioni precedenti, è possibile specificare quante uscite creare e confermarne la creazione premendo il pulsante "AGGIUNGI"; una volta creati gli elementi, è possibile modificarne alcuni attributi, consultarne lo stato, oppure accedere alla scheda di dettaglio di ciascuna uscita come illustrato nell'immagine seguente:

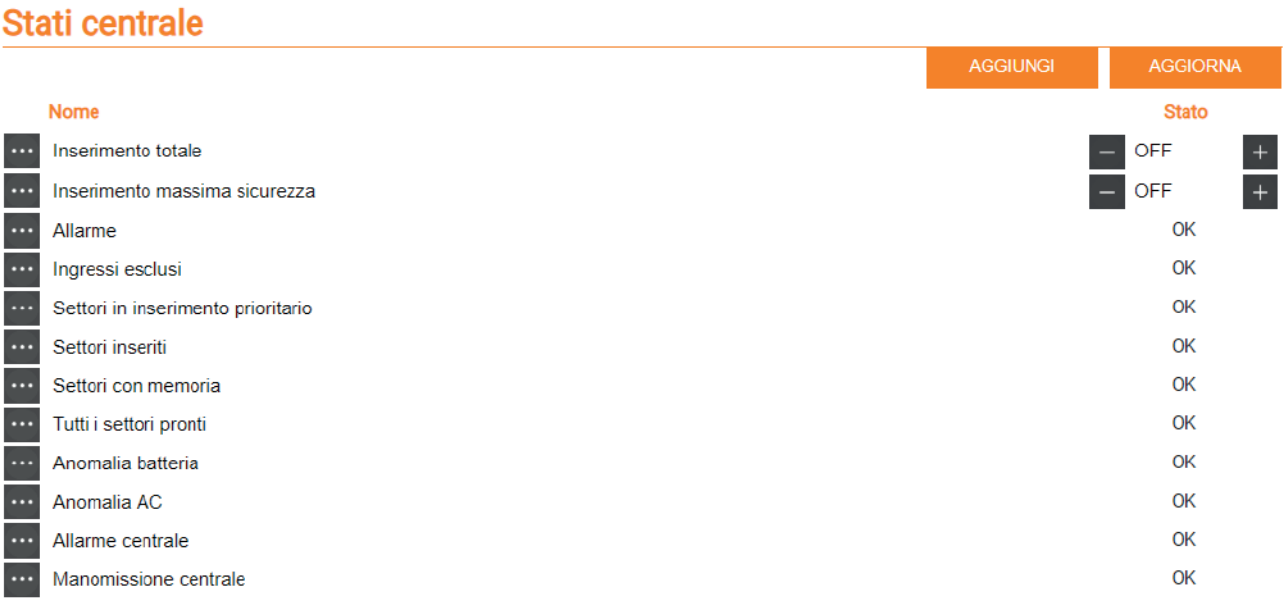



Nella sezione "**Comandi**" è possibile forzare l'uscita ad ON o OFF.
Nella sezione "**Stati**" vengono riportati lo stato di sintesi e lo stato di accensione dell'uscita.

### 6.4.5 Stati centrale

In questa sezione è possibile gestire le segnalazioni generali della centrale. Premere il pulsante "AGGIUNGI" nell'apposita sezione: vengono creati tutti gli oggetti che successivamente è possibile gestire a livello gateway.
Tra gli stati disponibili, possono essere comandati:

- **Inserimento totale**: Inserimento di tutti i settori;
- **Inserimento massima sicurezza totale**: Inserimento di tutti i settori in modalità massima sicurezza.



## 6.5 Menu CENTRALE - centrale antincendio

**A partire dalla versione software 1.0.10**, il gateway supporta la connessione con centrali antincendio TACÓRA.
Per aggiungere una centrale, posizionarsi sul menu **Tacora** e cliccare su ⊞: comparirà il sotto-menu "Centrale 1".

La pagina "**Centrale**" consente di mappare la comunicazione con la centrale TACÓRA, gestirne le zone e consultare gli stati delle sue uscite e dei guasti.


### 6.5.1 Impostazioni generali

In questa sezione preliminare del menu "**Centrale**" vengono impostati i parametri di connessione con la centrale antincendio:

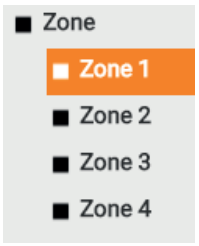
| DATI GENERALI | |
|---|---|
| ***NOME*** | Etichetta identificativa della centrale. |
| ***UTENTE*** | Codice utente che il gateway utilizza per dialogare con la centrale.<br>Deve essere un codice numerico valido in centrale. |
| ***CODICE*** | Codice numerico (password) di autenticazione dell'utente in centrale. |

| | |
|---|---|
| ***TIPO DI COMUNICAZIONE*** | Scelta della modalità di comunicazione del gateway: TCP/IP oppure Seriale/USB |
| ***PORTA*** | Porta di comunicazione da utilizzare (opzione disponibile solo in comunicazione TCP/IP). |
| ***INDIRIZZO IP*** | Indirizzo e porta della centrale su rete LAN. |
| ***PORTA*** | |
| ***VELOCITÀ DI TRASMISSIONE*** | Baud rate di comunicazione (opzione disponibile solo in comunicazione seriale). |
| ***POLLING TIMER*** | Tempo di interrogazione della centrale (in ms).<br>Regolare il tempo di interrogazione per accelerare o ridurre la frequenza con cui il gateway richiede lo stato alla centrale. |
| ***STATO DI ESECUZIONE*** | Stato di funzionamento del driver di comunicazione con la centrale.<br>In condizioni normali deve essere "IN ESECUZIONE". |
| ***COMUNICAZIONE CON LA CENTRALE*** | **Connesso**: connessione presente.<br>**Non connesso**: comunicazione assente. |

La comunicazione con la centrale può essere avviata o arrestata utilizzando rispettivamente i pulsanti "AVVIA" e "ARRESTA". Il pulsante "AGGIORNA CONF." effettua un arresto e successivo avvio della comunicazione.

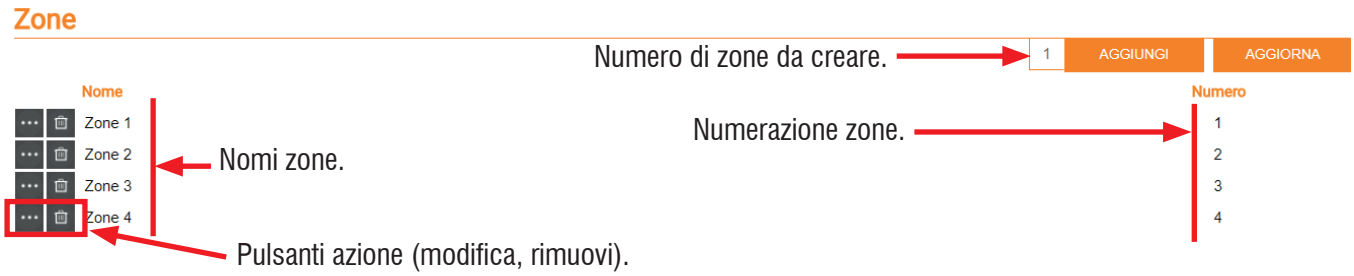

Tra i parametri configurabili in questa sezione, rientrano anche quelli relativi alla connessione tramite protocollo MODBUS ("**Bridge Modbus**"). Si rimanda alla sezione specifica di questo manuale ("8. PROTOCOLLO MODBUS - CENTRALI ANTINCENDIO TACÓRA" a pagina 35) per informazioni sulla configurazione con questo protocollo.

### 6.5.2 Zone



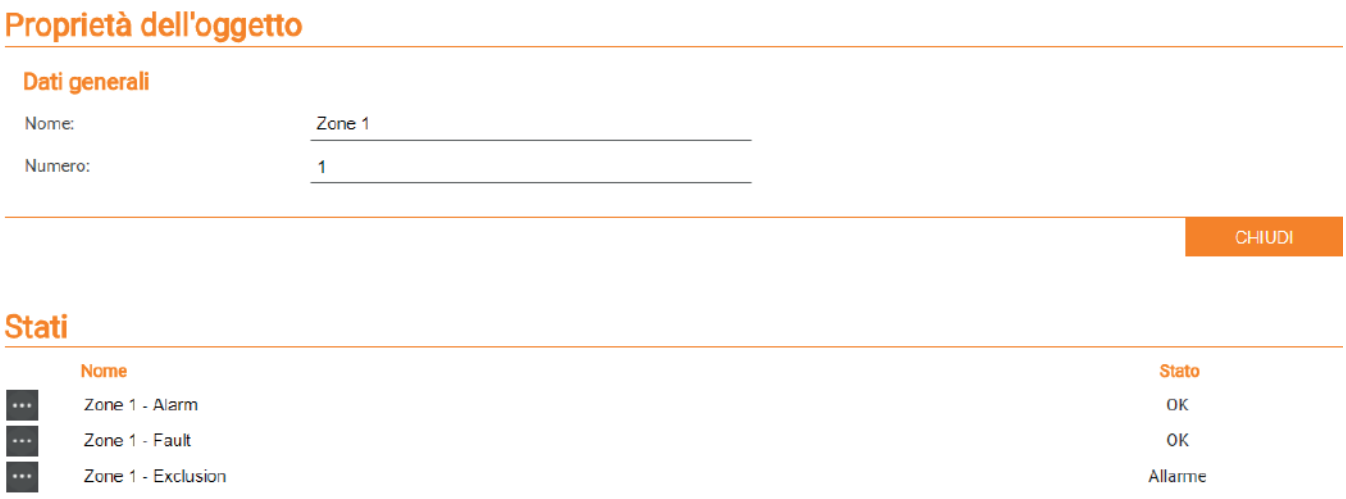

In questa sezione è possibile aggiungere e configurare zone della centrale all'interno del gateway.
Per inserire le zone, procedere come segue:

1. Specificare il numero di zone che si desidera aggiungere nell'apposito campo a fianco del pulsante "AGGIUNGI" (default: 1);
2. Premere il pulsante "AGGIUNGI" ed attendere la fine dell'operazione. Le zone appena create verranno automaticamente accodate a quelle esistenti.




Una volta create, è possibile modificare il nome delle zone e la loro numerazione (si consiglia comunque di mantenere la numerazione proposta in automatico), e consultarne lo stato.
La zona 0 di bordo, riservata ai pulsanti, non si crea automaticamente. Se si desidera crearla, rinominare una zona (ad esempio l'ultima) come zona 0 e numero 0.
I pulsanti azione a lato di ogni nome zona permettono di accedere alla scheda di dettaglio della singola zona e rimuovere definitivamente una zona dal progetto.

Scheda di una singola zona nel dettaglio:




La sezione "**Stati**" visualizza le diverse informazioni di stato aggiornate in tempo reale. Ciascuna zona è caratterizzata dai seguenti stati:

- **Alarm**: stato di allarme della zona;
- **Fault**: stato di guasto della zona;
- **Exclusion**: stato di esclusione della zona.

### 6.5.3 Dispositivi

Questa sezione permette di associare dispositivi alle zone. Funzione attualmente non supportata.

### 6.5.4 Uscite

Questa sezione mostra gli stati delle uscite di centrale. Gli stati sono accessibili in sola lettura, pertanto non comandabili ma solo visualizzabili in tempo reale.
Lo stato dell'uscita **Allarme** riveste primaria importanza, in quanto segnala in tempo reale lo stato di allarme della centrale.

**Uscite**

| Nome | Stato |
|---|---|
| Allarme | OK |
| Preallarme | OK |
| Guasto | Allarme |
| Buzzer | OK |
| OpenCollector 1 | OK |
| OpenCollector 2 | OK |
| OpenCollector 3 | OK |
| OpenCollector 4 | OK |
| Alimentazione sensori | OK |
| Uscita alimentazione sensori | OK |
| Esclusione campana | OK |
| Esclusione repeater 1 | OK |
| Esclusione repeater 2 | OK |
| Stato relay Zona 1 | OK |
| Stato relay Zona 2 | OK |
| Stato relay Zona 3 | OK |
| Stato relay Zona 4 | OK |
| Esclusione relay Zona 1 | OK |
| Esclusione relay Zona 2 | OK |
| Esclusione relay Zona 3 | OK |
| Esclusione relay Zona 4 | OK |
| Stato relay Aux 1 | OK |
| Stato relay Aux 2 | OK |
| Esclusione relay Aux 1 | OK |
| Esclusione relay Aux 2 | OK |

### 6.5.5 Guasti

Questa sezione permette di consultare gli eventuali stati di guasto della centrale.
Tra tutti gli stati ha rilevanza massima lo stato **Guasto generale**, in quanto riassuntivo di tutti i guasti.

**Guasti**

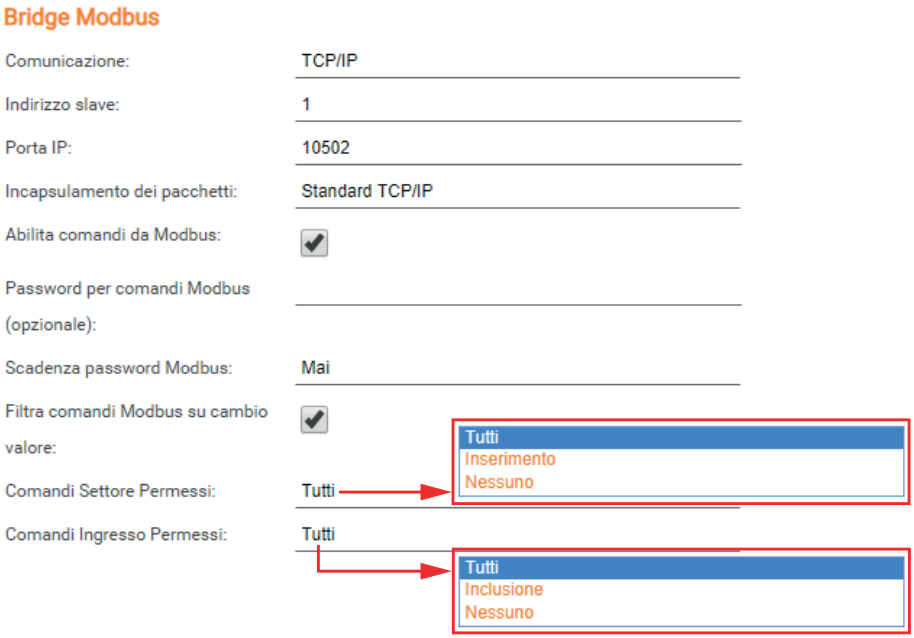
| Nome | Stato |
|---|---|
| Guasto generale | OK |
| Guasto campana | OK |
| Guasto batteria | OK |
| Guasto alimentatore | OK |
| Guasto 24V | OK |
| Guasto 24V resettabile | OK |
| Guasto alimentazione vs terra | OK |
| Guasto massa vs terra | OK |
| Guasto GSM | OK |
| Guasto CPU | OK |
| Guasto EEPROM | OK |
| Guasto comunicazione card | OK |
| Guasto registrazione card | OK |
| Guasto loop | OK |

# 7. PROTOCOLLO MODBUS - CENTRALI ANTINTRUSIONE

Il gateway può essere configurato per monitorare e gestire le funzioni delle centrali antintrusione tramite il protocollo MODBUS. Questo protocollo è basato su una comunicazione di tipo master-slave, in cui un dispositivo Modbus master (ad esempio un PLC o uno SCADA) interroga vari dispositivi slave (ad esempio ELMOGWAY o ELMOGWAY2).
Come dispositivo di tipo slave, il gateway fornisce informazioni circa il suo stato tramite *registri* aggiornati in tempo reale.

## 7.1 Impostazioni comunicazione per centrali antintrusione

È possibile configurare i parametri della connessione con protocollo Modbus nella sezione "**Bridge Modbus**", accessibile scorrendo fino in fondo la pagina "**Centrale**".




I parametri da fornire sono i seguenti:

| | |
|---|---|
| ***COMUNICAZIONE*** | Tipologia di connessione.<br>Sono disponibili tre tipi di connessione Modbus:<br>• RTU, tramite seriale RS-485 (vedere guida v.1.02 alla pagina web www.modbus.org);<br>• TCP/IP, tramite LAN (vedere guida v.1.0b alla pagina web www.modbus.org);<br>• RTU incapsulato (RTU over IP, vedere sotto).<br>Il gateway può anche mettere a disposizione entrambe le connessioni contemporaneamente (RTU + TCP/IP).<br>Nel caso di connessione via seriale, verranno abilitati i campi ***PORTA SERIALE*** e ***VELOCITÀ DI TRASMISSIONE***: inserire i rispettivi valori. |
| ***INDIRIZZO SLAVE*** | Numero di identificazione del gateway come dispositivo slave.<br>Utile nel caso di connessione tramite linea seriale.<br>(Default: 1. Si suggerisce di non cambiarlo.) |
| ***PORTA IP*** | Numero di porta IP su cui avviene la comunicazione Modbus, nel caso di comunicazione TCP/IP. Specificare un numero di porta superiore a 1024.<br>**Attenzione: la porta IP deve essere diversa da quella utilizzata da una eventuale centrale antincendio presente.** |
| ***INCAPSULAMENTO PACCHETTI*** | Tipologia di incapsulamento dei pacchetti in caso di comunicazione TCP/IP. Opzioni possibili:<br>• Standard TCP/IP<br>• RTU over IP |
| ***ABILITA COMANDI*** | Spuntare la casella per permettere di inviare comandi alla centrale tramite Modbus. |

| | |
|---|---|
| ***FILTRA COMANDI*** | Spuntare la casella per eliminare gli invii multipli di comandi uguali.<br>**Nota:** spuntare la casella Filtra Comandi solo se il server PLC invia ripetutamente lo stesso comando. |
| ***COMANDI SETTORE PERMESSI (*)*** | Selezionare uno dei seguenti valori:<br>**Tutti**: sono ammessi sia il comando di inserimento che il comando di disinserimento.<br>**Inserimento**: è ammesso solo il comando di inserimento.<br>**Nessuno**: non è ammesso alcun comando. |
| ***COMANDI INGRESSO PERMESSI (*)*** | Selezionare uno dei seguenti valori:<br>**Tutti**: sono ammessi sia il comando di inclusione che il comando di esclusione.<br>**Inclusione**: è ammesso solo il comando di inclusione.<br>**Nessuno**: non è ammesso alcun comando. |

***(*) Nota:*** i Comandi Settore e Ingresso Permessi definiti sopra agiscono solo sui comandi provenienti da Modbus (non SCS o KNX).

### 7.2 Registri per centrali antintrusione

Se la comunicazione Modbus è abilitata, sono disponibili i registri elencati nelle tabelle seguenti. Tali registri contengono informazioni aggiornate in tempo reale sullo stato del gateway.
La mappatura stati-indirizzi viene preconfigurata in fase di sviluppo, pertanto il protocollo Modbus non prevede la necessità di definire regole gateway. Gli indirizzi sono espressi sia in formato esadecimale che decimale; per ottenere la codifica decimale utilizzare una normale conversione HEX → DEC, ad esempio:

**0x3001 → 12289**

**ATTENZIONE: Alcuni poller considerano i registri a partire dallo 0, altri da 1.**

**LETTURA STATI:**

| INDIRIZZO / RANGE | | FUNZIONE | CODIFICA | DESCRIZIONE |
|---|---|---|---|---|
| 0x0000 | 0 | FC3 | Unsigned integer | Stato comunicazione con la centrale<br>0: errore<br>1: ok<br>2: password errata |
| 0x0001 | 1 | FC2 | INPUT (0/1) | Stato comunicazione con la centrale<br>0: errore<br>1: ok |
| 0x0100 | 256 | FC2 | INPUT (0/1) | Stato anomalia alimentazione centrale |
| 0x0101 | 257 | FC2 | INPUT (0/1) | Stato anomalia batteria centrale |
| 0x0200 (*) | 512 | FC2 | INPUT (0/1) | Allarme centrale |
| 0x0201 (*) | 513 | FC2 | INPUT (0/1) | Manomissione centrale |
| 0x0401 (*) | 1025 | FC2 | INPUT (0/1) | Tutti i settori pronti |
| 0x0402 (*) | 1026 | FC2 | INPUT (0/1) | Settori inseriti |
| 0x0403 (*) | 1027 | FC2 | INPUT (0/1) | Settori in inserimento massima sicurezza |
| 0x0404 (*) | 1028 | FC2 | INPUT (0/1) | Allarme |
| 0x0405 (*) | 1029 | FC2 | INPUT (0/1) | Settori con memoria |
| 0x0406 (*) | 1030 | FC2 | INPUT (0/1) | Ingressi esclusi |
| 0x1001<br>…<br>0x1400 | 4097<br>…<br>5120 | FC2 | INPUT (0/1) | Stato allarme ingresso 1 … X |
| 0x1401<br>…<br>0x1440 | 5121<br>…<br>5184 | FC2 | INPUT (0/1) | Stato allarme settore 1 … X (**) |
| 0x1501<br>…<br>0x1900 | 5377<br>…<br>6400 | FC2 | INPUT (0/1) | Stato memoria ingresso 1 … X |
| 0x1901<br>…<br>0x1940 | 6401<br>…<br>6464 | FC2 | INPUT (0/1) | Stato memoria settore 1 … X (**) |
| 0x2001<br>…<br>0x2400 | 8193<br>…<br>9216 | FC2 | INPUT (0/1) | Stato inclusione ingresso 1 … X |
| 0x3001<br>…<br>0x3040 | 12289<br>…<br>12352 | FC2 | INPUT (0/1) | Stato di inserimento settore 1 … X |
| 0x3101<br>…<br>0x3140 | 12545<br>…<br>12608 | FC2 | INPUT (0/1) | Stato massima sicurezza settore 1 … X |
| 0x3201<br>…<br>0x3240 | 12801<br>…<br>12864 | FC2 | INPUT (0/1) | Settore inseribile 1 … X |
| 0x5001<br>…<br>0x5400 | 20481<br>…<br>21504 | FC2 | INPUT (0/1) | Stato uscita 1 … X |

*(*) stati disponibili a partire dalla versione software 1.0.5*
*(**) vedere Nota a pag. 25*

Se sono stati abilitati i comandi modbus, sarà possibile inviare comandi alla centrale. La mappatura comandi-indirizzi avviene come illustrato nella tabella seguente.

**COMANDI**:

| INDIRIZZO / RANGE | | FUNZIONE | CODIFICA | DESCRIZIONE |
|---|---|---|---|---|
| 0x0100 | 256 | FC5 | COIL (0/1) | Comando di inserimento generale |
| 0x0101 | 257 | FC5 | COIL (0/1) | Comando di inserimento generale prioritario |
| 0x2001<br>…<br>0x2400 | 8193<br>…<br>9216 | FC5 | COIL (0/1) | Comando di esclusione ingresso 1 … X |
| 0x3001<br>…<br>0x3040 | 12289<br>…<br>12352 | FC5 | COIL (0/1) | Comando di inserimento settore 1 … X |
| 0x3101<br>…<br>0x3140 | 12545<br>…<br>12608 | FC5 | COIL (0/1) | Comando di massima sicurezza settore 1 … X |
| 0x4401<br>…<br>0X4800 | 17409<br>…<br>18432 | FC6 | 0/1/2 | Comando ingresso remoto<br>0 = riposo; 1 = allarme; 2 = manomissione<br>(solo per Villeggio v.8.6.10, Pregio v.3.0.7, Proxima v.1.0.7<br>o versioni firmware superiori) |
| 0x5001<br>…<br>0x5400 | 20481<br>…<br>21504 | FC5 | COIL (0/1) | Comando uscita 1 … X |

**NOTA**: interrogando un registro non configurato nel gateway, viene restituito un errore di tipo “ILLEGAL ADDRESS” (risposta hex81).

### 7.3 Protezione dei comandi

È possibile proteggere l’invio di comandi tramite Modbus attraverso una password. Tale password deve essere preventivamente specificata nell’interfaccia di configurazione della centrale, attraverso i seguenti parametri (disponibili se l’opzione “ABILITA COMANDI” è attiva):

| | |
|---|---|
| ***PASSWORD PER COMANDI MODBUS*** | Password che sarà necessario specificare via Modbus (16 caratteri massimo). |
| ***SCADENZA PASSWORD MODBUS*** | Stabilisce la durata di validità della password quando specificata valida:<br>• Mai (non scade finché non viene resettata)<br>• da 30 secondi a 30 minuti<br>• Ad ogni comando |

Per inviare la password via Modbus è necessario utilizzare i seguenti registri, in sola scrittura:

| INDIRIZZO / RANGE | | FUNZIONE | CODIFICA | DESCRIZIONE |
|---|---|---|---|---|
| 0xFF01<br>0xFF10 | 65281<br>65296 | FC6<br>FC16 | ASCII | Caratteri (da 1 a 16) della password |
| 0xFF11 | 65297 | FC6<br>FC16 | 0/1 | Se impostato ad 1, determina la verifica della password<br>Se impostato a 0, determina il reset della password |

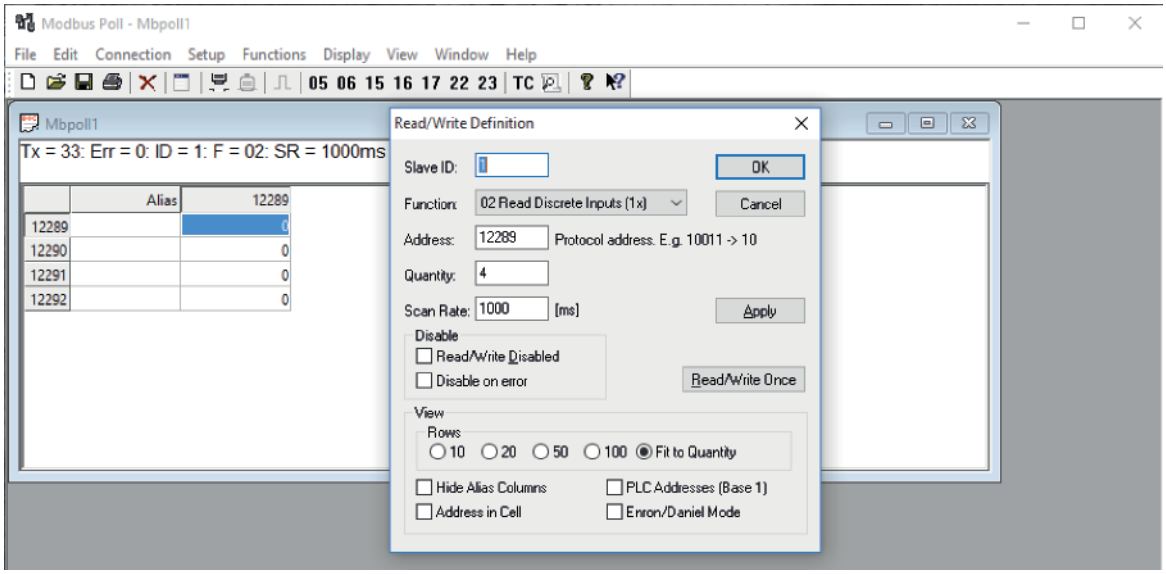
I caratteri della password (e registro di conferma finale) possono essere passati via Modbus uno alla volta (nel qual caso, solo quando si imposta ad 1 il registro 0xFF11 viene processata) oppure con un unico comando di scrittura multipla.
È possibile conoscere lo stato di utilizzo della password leggendo il seguente registro:

| INDIRIZZO / RANGE | | FUNZIONE | CODIFICA | DESCRIZIONE |
|---|---|---|---|---|
| 0xFF00 | 65280 | FC3 | Unsigned Integer | 0 = non abilitata / non usata<br>1 = Password non valida<br>2 = Password valida |

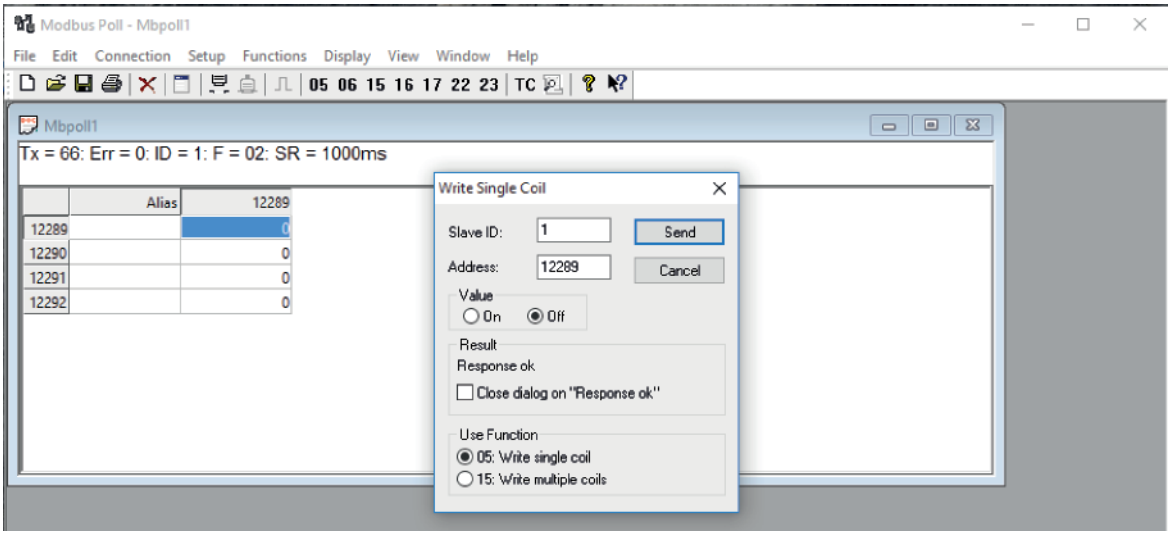
**Esempio**

Le seguenti schermate mostrano un esempio di lettura e di comando del gateway tramite software di test Modbus:

- lettura dello stato di inserimento di 4 settori:




- comando del primo settore:



# 8. PROTOCOLLO MODBUS - CENTRALI ANTINCENDIO TACÓRA

Le centrali antincendio TACÓRA possono dialogare con il sistema di domotica tramite il gateway (dotato di versione firmware 1.0.10 o superiore) attraverso il protocollo MODBUS. Questo protocollo è basato su una comunicazione di tipo master-slave, in cui un dispositivo Modbus master (ad esempio un PLC o uno SCADA) interroga vari dispositivi slave. Come dispositivo di tipo slave, il gateway fornisce informazioni circa il suo stato tramite *registri* aggiornati in tempo reale.

## 8.1 Impostazioni comunicazione per centrali antincendio

È possibile configurare i parametri della connessione con protocollo Modbus nella sezione "**Bridge Modbus**", accessibile scorrendo fino in fondo la pagina "**Centrale**".


A differenza di quanto avviene per le centrali antintrusione, le normative antincendio prevedono che non possano transitare comandi verso la centrale. Pertanto, la casella ***Abilita comandi da Modbus*** non è presente.

I parametri da fornire sono i seguenti:

| | |
|---|---|
| ***COMUNICAZIONE*** | Tipologia di connessione.<br>Sono disponibili due tipi di connessione Modbus:<br>• RTU, tramite seriale RS-485 (vedere guida v.1.02 alla pagina web www.modbus.org);<br>• TCP/IP, tramite LAN (vedere guida v.1.0b alla pagina web www.modbus.org).<br>Il gateway può anche mettere a disposizione entrambe le connessioni contemporaneamente (RTU + TCP/IP).<br>Nel caso di connessione via seriale, verranno abilitati i campi ***PORTA SERIALE*** e ***VELOCITÀ DI TRASMISSIONE***: inserire i rispettivi valori. |
| ***INDIRIZZO SLAVE*** | Numero di identificazione del gateway come dispositivo slave.<br>Utile nel caso di connessione tramite linea seriale.<br>(Default: 1. Si suggerisce di non cambiarlo.) |
| ***PORTA IP*** | Numero di porta IP su cui avviene la comunicazione Modbus, nel caso di comunicazione TCP/IP. Specificare un numero di porta superiore a 1024.<br>**Attenzione: la porta IP deve essere diversa da quella utilizzata da una eventuale centrale antintrusione presente.** |
| ***INCAPSULAMENTO PACCHETTI*** | Tipologia di incapsulamento dei pacchetti in caso di comunicazione TCP/IP. Opzioni possibili:<br>• Standard TCP/IP<br>• RTU over IP |

## 8.2 Registri per centrali antincendio

Per la connessione della centrale TACÓRA al sistema di domotica, sono disponibili i registri elencati nella tabella seguente. Tali registri contengono informazioni aggiornate in tempo reale sullo stato del gateway.
Gli indirizzi sono espressi sia in formato esadecimale che decimale; per ottenere la codifica decimale utilizzare una normale conversione HEX → DEC, ad esempio:

**0x006C → 108**

**ATTENZIONE: Alcuni poller considerano i registri a partire dallo 0, altri da 1.**

**LETTURA STATI:**

| INDIRIZZO | | FUNZ. | CODIFICA | DESCRIZIONE |
|---|---|---|---|---|
| 0x0065 | 101 | FC2 | INPUT (0/1) | Uscita zona 1 |
| 0x0066 | 102 | FC2 | INPUT (0/1) | Uscita zona 2 |
| 0x0067 | 103 | FC2 | INPUT (0/1) | Uscita zona 3 |
| 0x0068 | 104 | FC2 | INPUT (0/1) | Uscita zona 4 |
| 0x0069 | 105 | FC2 | INPUT (0/1) | Aux 1 |
| 0x006A | 106 | FC2 | INPUT (0/1) | Aux 2 |
| 0x006B | 107 | FC2 | INPUT (0/1) | Uscita open-collector 1 |
| 0x006C | 108 | FC2 | INPUT (0/1) | Uscita open-collector 2 |
| 0x006D | 109 | FC2 | INPUT (0/1) | Uscita open-collector 3 |
| 0x006E | 110 | FC2 | INPUT (0/1) | Uscita open-collector 4 |
| 0x006F | 111 | FC2 | INPUT (0/1) | Buzzer |
| 0x0070 | 112 | FC2 | INPUT (0/1) | Preallarme |
| 0x0071 | 113 | FC2 | INPUT (0/1) | Allarme |
| 0x0072 | 114 | FC2 | INPUT (0/1) | Guasto |
| 0x0073 | 115 | FC2 | INPUT (0/1) | Alimentazione sensori |
| 0x0074 | 116 | FC2 | INPUT (0/1) | Uscita alimentatore resettabile |
| 0x0075 | 117 | FC2 | INPUT (0/1) | Esclusione uscita zona 1 |
| 0x0076 | 118 | FC2 | INPUT (0/1) | Esclusione uscita zona 2 |
| 0x0077 | 119 | FC2 | INPUT (0/1) | Esclusione uscita zona 3 |
| 0x0078 | 120 | FC2 | INPUT (0/1) | Esclusione uscita zona 4 |
| 0x0079 | 121 | FC2 | INPUT (0/1) | Esclusione aux 1 |
| 0x007A | 122 | FC2 | INPUT (0/1) | Esclusione aux 2 |
| 0x007B | 123 | FC2 | INPUT (0/1) | Esclusione uscita campana |
| 0x007C | 124 | | | |
| 0x007D | 125 | | | |
| 0x007E | 126 | | | |
| 0x007F | 127 | | | |
| 0x0080 | 128 | | | |
| 0x00C9 | 201 | FC2 | INPUT (0/1) | Guasto generale |
| 0x00CA | 202 | FC2 | INPUT (0/1) | Guasto uscita campana |
| 0x00CB | 203 | FC2 | INPUT (0/1) | Guasto batteria |
| 0x00CC | 204 | FC2 | INPUT (0/1) | Guasto alimentatore |
| 0x00CD | 205 | FC2 | INPUT (0/1) | Guasto out 24V |
| 0x00CE | 206 | FC2 | INPUT (0/1) | Guasto out 24V RST |
| 0x00CF | 207 | FC2 | INPUT (0/1) | Guasto corto terra alimentazione |
| 0x00D0 | 208 | FC2 | INPUT (0/1) | Guasto corto terra massa |
| 0x00D1 | 209 | FC2 | INPUT (0/1) | Guasto GSM |
| 0x00D2 | 210 | FC2 | INPUT (0/1) | Guasto CPU |
| 0x00D3 | 211 | FC2 | INPUT (0/1) | Guasto EEPROM |
| 0x012D | 301 | FC2 | INPUT (0/1) | Mancata comunicazione |
| 0x012E | 302 | FC2 | INPUT (0/1) | Non registrato |
| 0x012F | 303 | FC2 | INPUT (0/1) | Loop guasto |
| 0x0135 | 309 | FC2 | INPUT (0/1) | Esclusione repeater 1 |
| 0x0136 | 310 | FC2 | INPUT (0/1) | Esclusione repeater 2 |
| 0x1000 ... 0x102F | 4096 ... 4143 | FC2 | INPUT (0/1) | Zone in allarme **(*)** |
| 0x1100 ... 0x112F | 4352 ... 4399 | FC2 | INPUT (0/1) | Zone in guasto **(*)** |
| 0x1200 ... 0x122F | 4608 ... 4655 | FC2 | INPUT (0/1) | Zone escluse **(*)** |
| 0x2001 ... 0x2FFF | 8193 ... 12287 | FC2 | INPUT (0/1) | Dispositivi loop esclusi |
| 0x3001 ... 0x3FFF | 12289 ... 16383 | FC2 | INPUT (0/1) | Stato uscite dispositivi del loop |
| 0x4001 ... 0x4FFF | 16385 ... 20479 | FC2 | INPUT (0/1) | Dispositivi loop in richiesta di ripristino |
| 0x5001 ... 0x5FFF | 20481 ... 24575 | FC2 | INPUT (0/1) | - Non attivo - |
| 0xF001 | 61441 | FC2 | INPUT (0/1) | Stato comunicazione con la centrale 0: errore 1: ok |

**(*)** Il conteggio delle zone parte da 0 comprendendo così la zona 0 di bordo dedicata ai soli pulsanti.

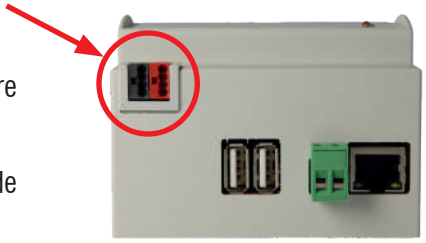
# 9. PROTOCOLLO KNX

Il protocollo KNX si basa su un sistema distribuito con un bus condiviso al quale sono connessi tutti i dispositivi.
Esso prevede due tipi di indirizzi:

- un indirizzo fisico, diverso per ogni dispositivo connesso al bus KNX, avente la sintassi X.Y.Z;
- un indirizzo logico di gruppo, relativo alla funzione, avente la sintassi X/Y/Z.

Il gateway può essere collegato ad un impianto KNX ed interagire con le funzioni domotiche in modo bidirezionale, inviando segnalazioni di stato della centrale e ricevendo comandi su altrettanti indirizzi di gruppo.


## 9.1 Collegamento al bus KNX



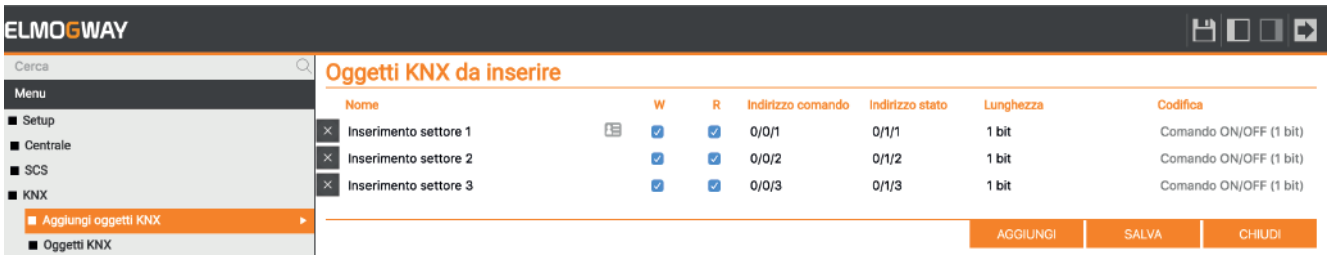
È possibile collegare i gateway al bus KNX attraverso l'apposito connettore standard rosso-nero, disponibile sul dispositivo.
Non è necessaria alcuna interfaccia aggiuntiva.
La procedura di interfacciamento tra la centrale ed un impianto KNX prevede i seguenti passaggi:

1. Creazione degli indirizzi di gruppo;
2. Associazione tra indirizzi di gruppo KNX e funzioni della centrale attraverso una o più *regole gateway* (vedere "11. REGOLE GATEWAY" a pagina 44).

**Nota per le creazione di regole con elementi KNX**: per la corretta reazione e propagazione del segnale, è necessario che sia presente almeno l'alimentazione sul bus KNX.

## 9.2 Creazione indirizzi di gruppo

Per predisporre il gateway alla comunicazione su uno o più indirizzi di gruppo KNX, è necessario innanzitutto aggiungerli al progetto, attraverso la voce "**Aggiungi oggetti KNX**" nella sezione "**KNX**" del menu laterale.




Premendo il pulsante AGGIUNGI, viene inserita nella lista (inizialmente vuota) una nuova riga, nella quale è possibile specificare i seguenti parametri:

| | |
|---|---|
| ***NOME*** | Etichetta di testo che identifica il nuovo indirizzo nel progetto. |
| ***W / R*** | Flag di abilitazione rispettivamente in scrittura e lettura.<br>Specificano se i nuovi indirizzi debbano essere comandabili dal gateway e/o leggibili. |
| ***INDIRIZZO COMANDO*** | Se il flag W è attivo, inserire l'indirizzo di gruppo per il comando (verso il bus KNX) nel formato a 3 livelli (X/Y/Z). |
| ***INDIRIZZO STATO*** | Se il flag R è attivo, inserire l'indirizzo di gruppo per la lettura dal bus KNX nel formato a 3 livelli (X/Y/Z).<br>**Nota**: questo campo è facoltativo se è attivo anche il flag di W ed è stato inserito un indirizzo di comando. In questo caso, verrà letto lo stato dallo stesso indirizzo di gruppo di comando. |
| ***LUNGHEZZA*** | Selezionare, tra quelle disponibili, la lunghezza del *payload* dei telegrammi inviati/ricevuti sul bus KNX sugli indirizzi specificati. Questa scelta deve essere coerente con quanto specificato nel progetto ETS. |
| ***CODIFICA*** | In base alla lunghezza prescelta, selezionare la codifica più idonea per rappresentare i dati inviati o ricevuti sugli indirizzi di gruppo da creare. |

Una volta compilata la lista di tutti gli indirizzi di gruppo da aggiungere, premere il pulsante "SALVA" per avviare la procedura di creazione, ed attendere il suo completamento. Una volta ricevuto il messaggio di conferma, è possibile aggiungere nuovi indirizzi, oppure procedere con i passaggi successivi.

### 9.3 Lista oggetti KNX

L'elenco degli oggetti KNX creati con la procedura vista in precedenza è disponibile nella sezione "**OGGETTI KNX**" del menu laterale. Selezionando una di queste voci, è possibile accedere alla sua scheda di dettaglio, procedendo in due modi alternativi:

- Premendo i "tre puntini" a lato del suo nome;
- Premendo il pulsante "MODIFICA" della toolbar al fondo del menu.

In entrambi i casi, si accede ad una pagina simile a quella della figura seguente:


All'interno di questa scheda è possibile modificare il nome precedentemente assegnato.
L'indirizzo di gruppo, viceversa, non può essere modificato; se necessario, a tale scopo, occorrerà rimuovere l'oggetto cliccando sul pulsante "ELIMINA" della toolbar, e crearne uno nuovo con l'indirizzo desiderato.
Una volta creati tutti gli oggetti KNX desiderati, essi dovranno essere associati alle funzioni della centrale attraverso apposite regole gateway, come illustrato nel capitolo "11. REGOLE GATEWAY".

### 9.4 Configurazione comunicazione

Questa pagina permette di impostare l'*indirizzo fisico* utilizzato dal gateway per inviare comandi sul bus KNX.
Inserire nell'apposito campo un valore nel formato X.Y.Z coerente con l'indirizzamento di linea e settore nel quale il gateway è fisicamente collegato.
In caso di dubbi, lasciare il valore predefinito **0.0.255** che, tipicamente, permette la corretta comunicazione con tutti i dispositivi dell'impianto.

## 9.5 Importazione da ETS (opzionale)

ETS (Engineering Tool Software) è un software sviluppato per progettare e configurare un impianto KNX.
Il gateway può importare un progetto realizzato in ETS per velocizzare la creazione degli oggetti KNX, rispetto alla procedura manuale descritta in precedenza.
È possibile importare il progetto da ETS nei seguenti formati supportati:

- **ESF + PHD:** esportazione per OPC
- **CSV:** esportazione indirizzi di gruppo (contiene solo l'elenco degli indirizzi di gruppo: eventuali informazioni sul tipo di dato vanno inserite a mano)

### 9.5.1 Formato ESF + PHD

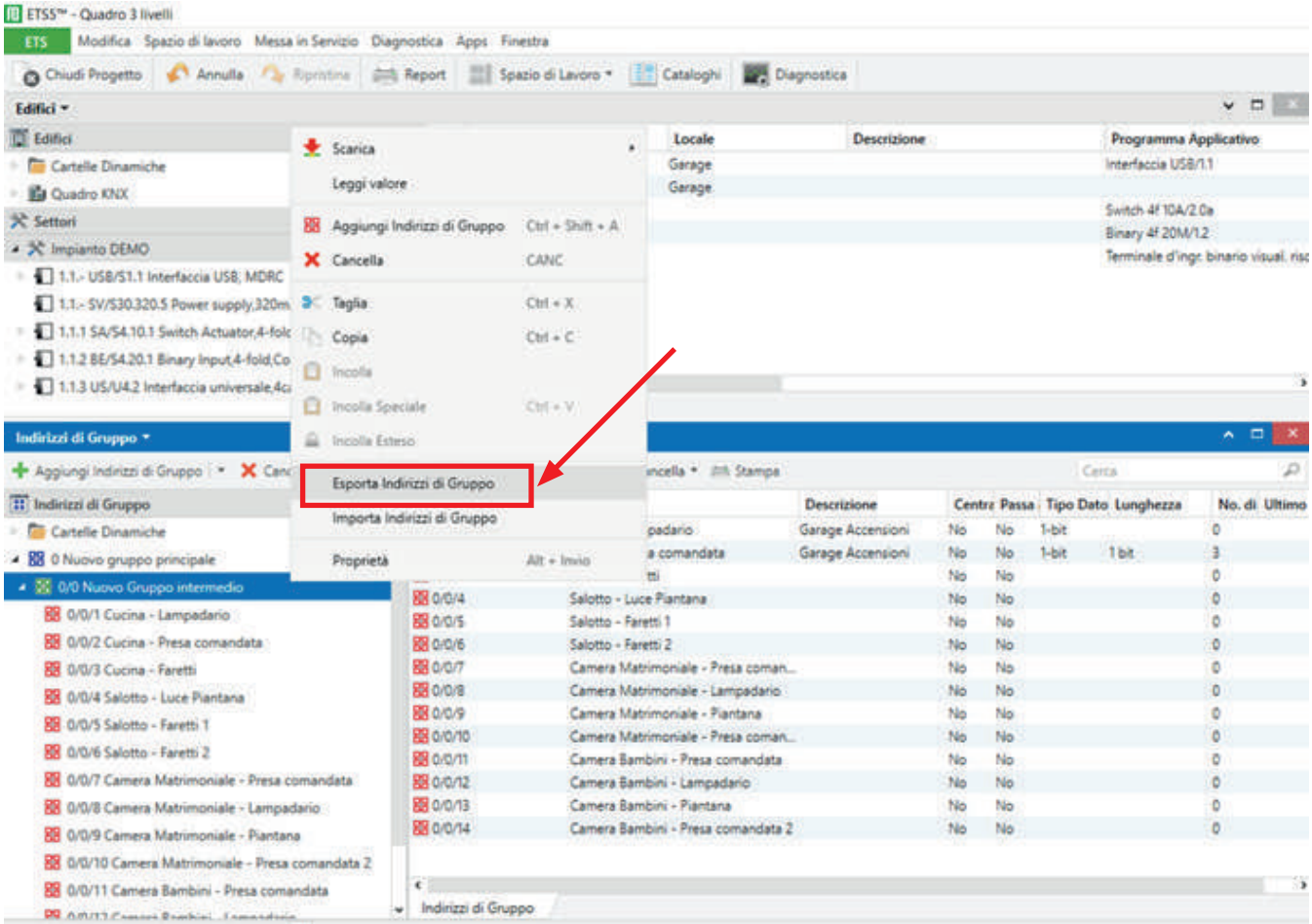
Selezionare la voce "**Esporta per OPC server**" all'interno di ETS. Vengono così generati due file:
- ESF: contiene gli indirizzi di gruppo, le relative etichette e relazioni con altri indirizzi di gruppo
- PHD: contiene gli indirizzi fisici dei dispositivi presenti nel progetto

### 9.5.2 Formato CSV

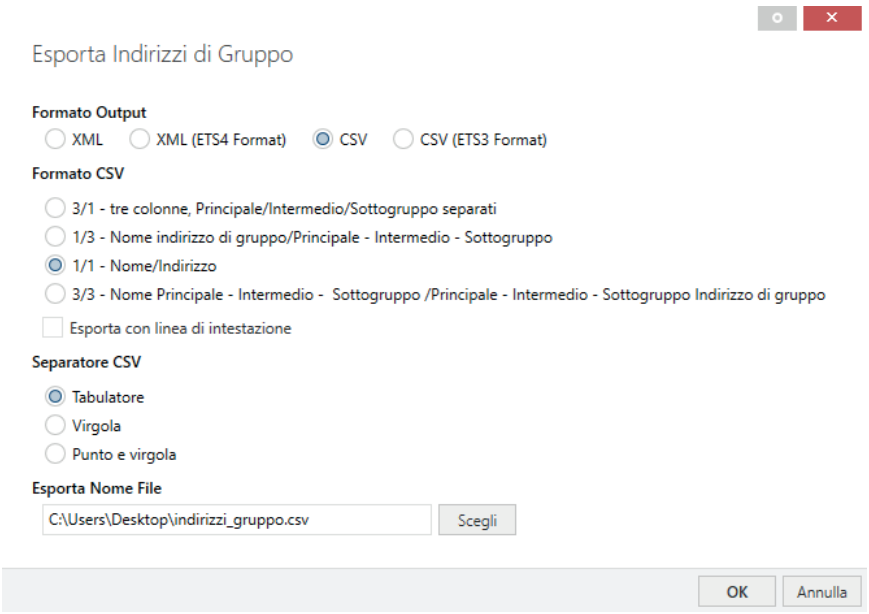
Il gateway è in grado di importare indirizzi KNX anche da un file CSV così costituito:
- Tabulazione come separatore delle colonne
- Etichetta degli indirizzi di gruppo nella prima colonna
- Indirizzo di gruppo nella seconda colonna
- Lunghezza in bit (facoltativa) nella terza colonna

Questo tipo di file può essere generato manualmente (utilizzando, ad esempio, Microsoft Excel) oppure in automatico dal software ETS. In quest'ultimo caso, è necessario:

1. Selezionare il ramo degli indirizzi di gruppo che si desidera esportare
2. Selezionare "ESPORTA INDIRIZZI DI GRUPPO" dal menu contestuale



3. Specificare le seguenti opzioni:
   - Dati organizzati in 2 colonne (etichetta + indirizzo)
   - Tabulazione come separazione tra le colonne




**Nota**: L'importazione da CSV può risultare comoda anche per creare velocemente nuovi oggetti KNX all'interno del gateway senza passare necessariamente attraverso ETS: è sufficiente infatti compilare le informazioni relative ad etichetta ed indirizzo di gruppo all'interno di un nuovo file, ed avviare la procedura di importazione.

# 10. PROTOCOLLO SCS

Il gateway può essere collegato ad un impianto SCS/MyHOME ed interagire con le funzioni domotiche in modo bidirezionale, inviando segnalazione di stato della centrale e ricevendo comandi su altrettanti indirizzi di comunicazione.
Il protocollo SCS prevede l'interfacciamento via IP con un dispositivo Bticino che funge da gateway.

## 10.1 Collegamento a SCS

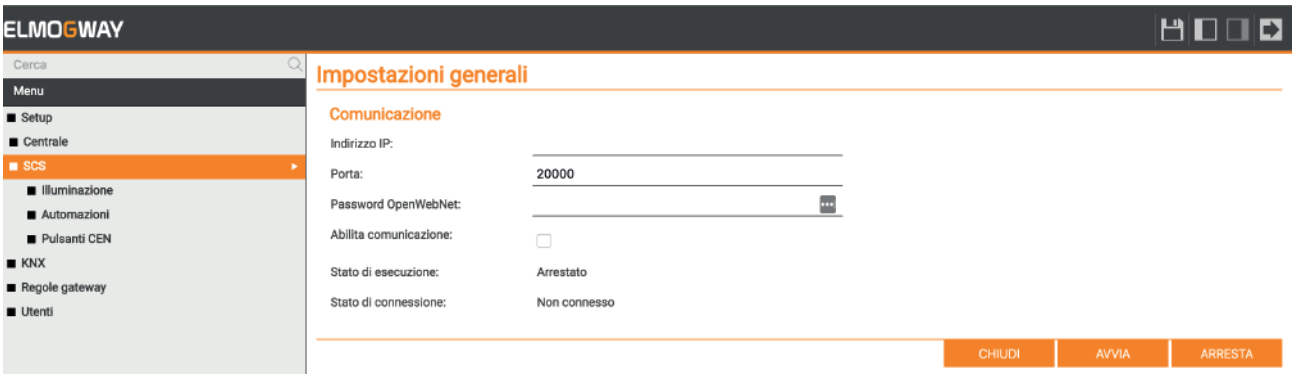
Sui modelli abilitati, è possibile collegare il gateway al bus SCS attraverso la rete utilizzando un *gateway OpenWebNet* opportunamente configurato (tramite il software *MyHome Suite* di Bticino).
**Il gateway compatibile è F454, unico marcato OpenWebNet.**
Il funzionamento con F459, MH202, MH200N è stato testato, ma con limitazioni funzionali e quindi va considerato non consigliato. Il funzionamento con altri modelli di gateway non è testato né garantito.

La procedura di interfacciamento tra la centrale ed un impianto SCS / MyHOME prevede i seguenti passaggi:

- Creazione degli oggetti con il relativo indirizzamento;
- Associazione tra oggetti SCS e funzioni della centrale attraverso una o più *regole gateway* (vedere "11. REGOLE GATEWAY" a pagina 44).

## 10.2 Configurazione della comunicazione

Per configurare la comunicazione con il gateway OpenWebNet presente nell'impianto MyHOME, è necessario innanzitutto accedere alla scheda di dettaglio della voce "**SCS**" del menu laterale, attraverso i "tre puntini" a fianco del nome (una volta selezionato) oppure cliccando sul pulsante "MODIFICA" della toolbar in basso.




Nella sezione iniziale della pagina è possibile configurare la comunicazione, inserendo i seguenti parametri:

| | |
|---|---|
| ***INDIRIZZO IP*** | Indirizzo IP assegnato al gateway OpenWebNet. |
| ***PORTA*** | Specificare la porta di comunicazione con il gateway OpenWebNet.<br>Lasciare il valore predefinito 20.000 salvo diverse esigenze. |
| ***PASSWORD OPENWEBNET*** | Specificare la password per l'accesso al protocollo Open, se diversa da quella predefinita (12345). |
| ***ABILITA COMUNICAZIONE*** | Selezionare questa voce per attivare la comunicazione con il gateway OpenWebNet.<br>In caso contrario, la configurazione effettuata rimarrà inerte. |
| ***STATO DI ESECUZIONE STATO DI CONNESSIONE*** | Indicano rispettivamente lo stato di esecuzione del driver di comunicazione (che deve essere attivato con il pulsante AVVIA, una volta configurato) e di comunicazione effettiva con il gateway OpenWebNet. |

Una volta terminata la configurazione, avviare la comunicazione con il pulsante AVVIA e verificare che lo "Stato di connessione" risulti *connesso*.
I dispositivi SCS che si possono aggiungere al gateway si possono suddividere in tre categorie: **luci**, **automazioni** e **pulsanti CEN**.

### 10.3 Aggiunta di Luci

È possibile inserire una o più luci SCS all'interno del gateway per poterle poi comandare (o reagire alla loro accensione). Dalla pagina di configurazione "**SCS**", accedere alla sezione "**Illuminazione**" e procedere come segue:

1. Inserire il numero di luci che si desidera creare nell'apposito campo accanto al pulsante "AGGIUNGI" (default: 1);
2. Cliccare sul pulsante "AGGIUNGI".

Al termine della procedura, i nuovi comandi luce sono elencati come nella figura seguente:


Per ogni voce è possibile specificare quanto segue:

| | |
|---|---|
| ***NOME*** | Etichetta identificativa del comando luci all'interno del progetto. |
| ***INDIRIZZAMENTO*** | Stabilire se il comando debba essere:<br>• **Punto-punto** (ovvero il comando "diretto" di un singolo punto luce);<br>• **Ambiente** (comando di tutti i dispositivi di una determinata area);<br>• **Gruppo** (comando di tutti i dispositivi facenti parte di un gruppo);<br>• **Generale** (comando di tutto l'impianto). |
| ***A***<br>***PL***<br>***GR*** | In base al tipo di indirizzamento, specificare l'indirizzo da comandare, inserendo:<br>• **A:** numero di ambiente;<br>• **PL:** numero di punto luce;<br>• **GR**: numero di gruppo; |
| ***TIPOLOGIA*** | Specificare se il comando debba essere di tipo ON/OFF o dimmer. |
| ***STATO*** | Permette di vedere lo stato aggiornato in tempo reale oppure di comandare la luce (dopo aver premuto il pulsante "AGGIORNA"). |

Una volta configurati i comandi luce desiderati, premere il pulsante "AGGIORNA" per riavviare la comunicazione.

### 10.4 Aggiunta di Automazioni

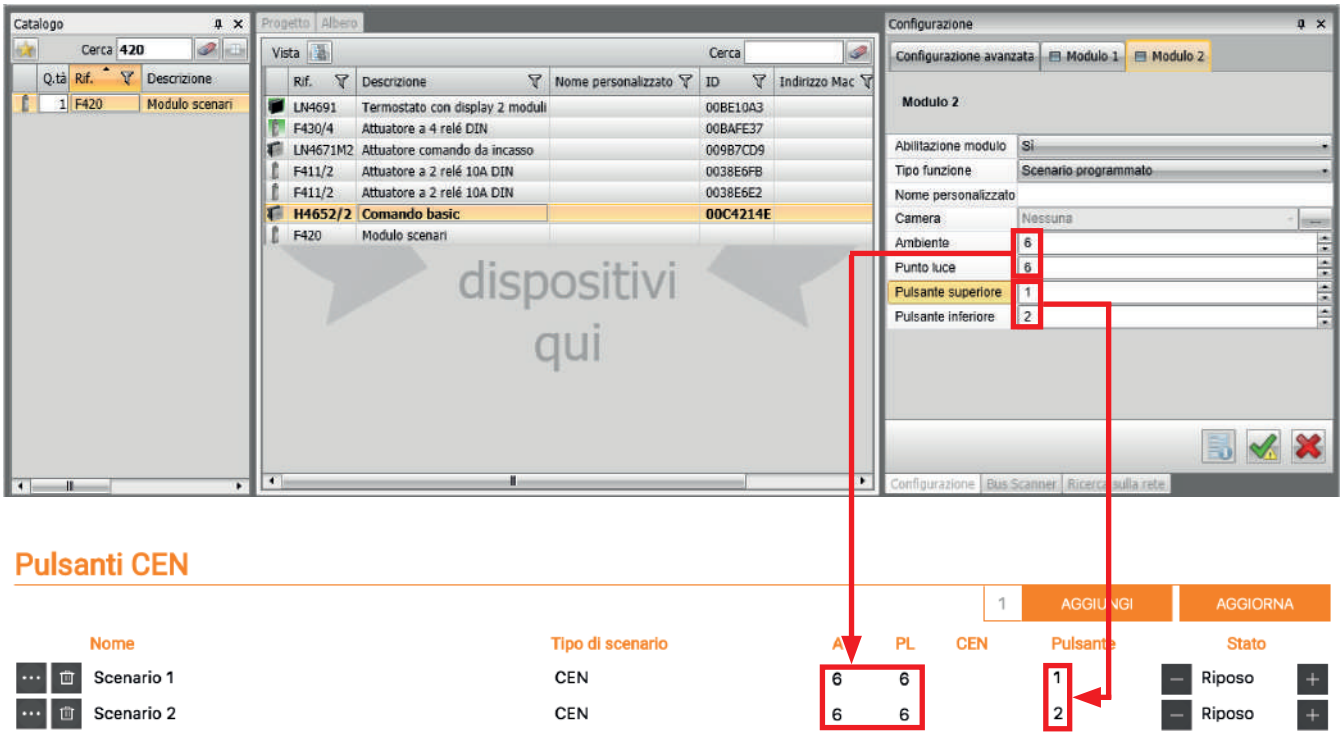
In modo del tutto analogo a quanto visto per le luci, è possibile inserire una o più automazioni, per le quali – a differenza di quanto visto per le luci – è possibile specificare:

| | |
|---|---|
| ***TIPOLOGIA*** | Specificare se il comando debba essere di tipo tapparella (SU/GIU) oppure ON/OFF. |


### 10.5 Aggiunta di Pulsanti CEN

Questa sezione permette di configurare all'interno del gateway uno o più pulsanti MyHOME per associare alla loro pressione un comando da inviare alla centrale. A tale scopo, i pulsanti devono essere preliminarmente configurati (tramite *jumper* o tramite il software *MyHome Suite*) per il comando di scenari CEN oppure CEN PLUS.

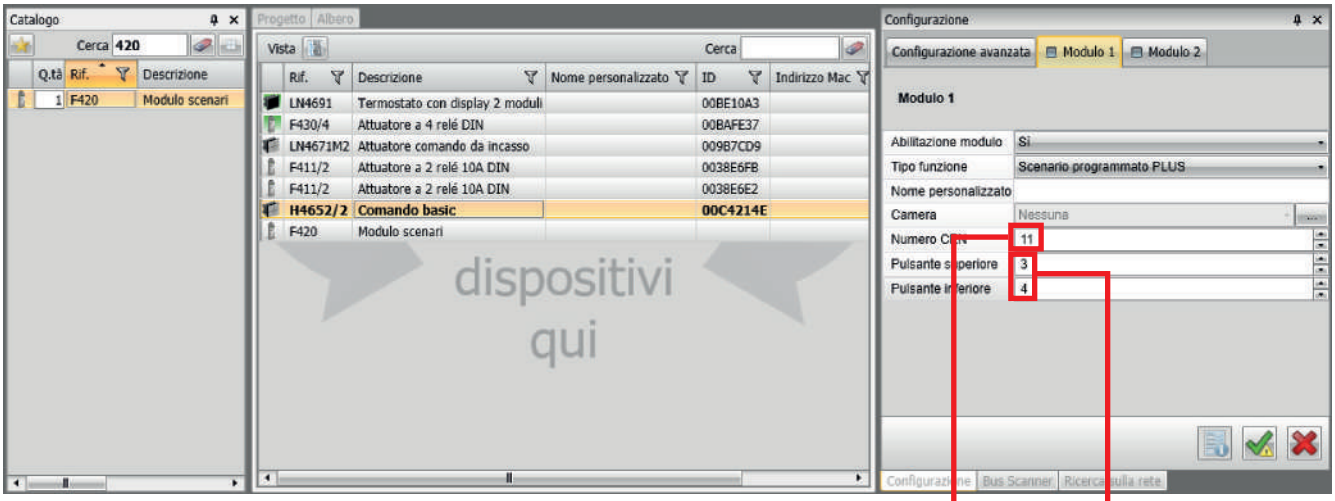
Nel caso di pulsanti CEN, è necessario inserire il loro indirizzo (A e PL) ed il numero di pulsante:







Nel caso di pulsanti per il richiamo di scenari programmati CEN PLUS, viceversa, va specificato il numero CEN ed il numero di pulsante:







info@elmospa.com
elmospa.com

# 11. REGOLE GATEWAY

Una volta creati oggetti di tipo KNX o SCS, come visto nei precedenti capitoli, è possibile impiegarli nella definizione di particolari regole.
Le *regole gateway* sono associazioni grafiche tra comandi e stati delle centrali (per TACÓRA solo stati), e oggetti di tipo KNX o SCS. Esse specificano quali stati e comandi debbano essere scambiati, e in quali condizioni; ogni regola può contenere un numero a piacere di oggetti e di connessioni; tuttavia, per ragioni di leggibilità, si consiglia di creare regole separate per le diverse funzioni gateway.

**Nota**: Le regole gateway non sono necessarie per l'interfacciamento Modbus, essendo questo preconfigurato sull'apposita mappatura di registri.

**Nota per le creazione di regole con elementi KNX**: per la corretta reazione e propagazione del segnale, è necessario che sia presente almeno l'alimentazione sul bus KNX.

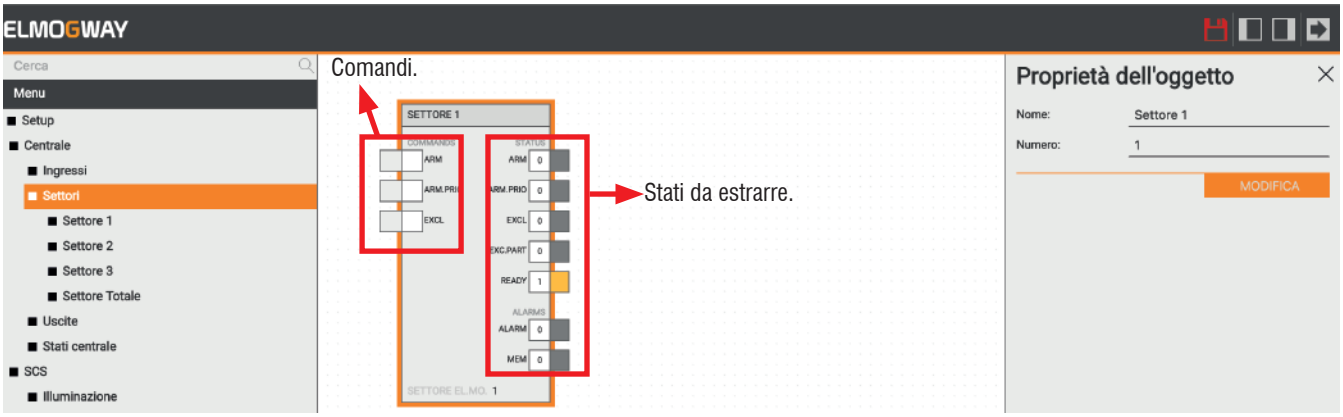
## 11.1 Creazione di una regola


Per aggiungere una nuova regola gateway, procedere come segue:

1. Identificare la sezione "**Regole gateway**" del menu (figura a lato);
2. Cliccare sul pulsante "AGGIUNGI" nella toolbar;
3. Selezionare la nuova regola;
4. Premere i "tre puntini" a lato o il pulsante "MODIFICA" nella toolbar. Accedendo alla regola, viene mostrata una pagina inizialmente vuota, nella quale andranno trascinati gli oggetti che si desidera interconnettere. Premendo il tasto destro in qualunque punto, si apre il pannello di dettaglio (sul lato destro della schermata), con cui è possibile assegnare un nome alla regola.
5. Identificare nel menu laterale gli oggetti "ingresso", "settore", "uscita", nonché gli indirizzi di gruppo KNX o gli oggetti SCS che si desidera aggiungere, e trascinarli nello spazio libero.
   In alternativa, è possibile cercare gli oggetti che si desidera inserire tramite la barra di ricerca, e trascinarli (uno alla volta) dai risultati della ricerca.
   Gli oggetti sono rappresentati come **blocchi** caratterizzati da uno o più **nodi** sul lato sinistro (ingressi) e destro (uscite). I nodi di ingresso possono essere connessi con altri oggetti per comandare l'oggetto in questione, mentre i nodi di uscita possono a loro volta comandare altri oggetti. I comandi tra oggetti all'interno delle regole gateway avvengono comunque sempre solo su variazione di valore.

### Esempio con centrale antintrusione

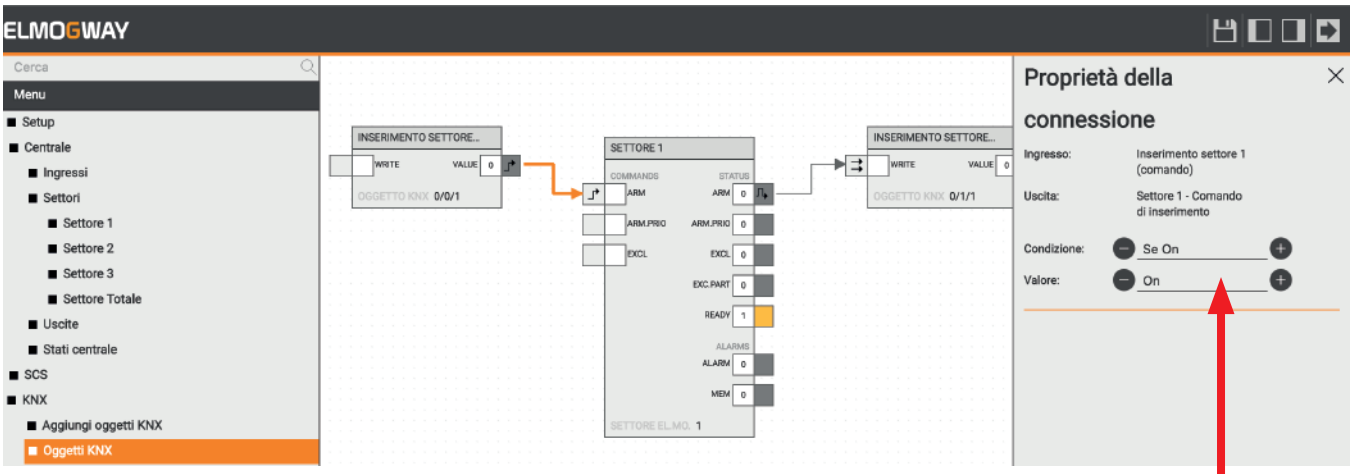
Volendo interagire con il settore 1 della centrale, è sufficiente identificarlo nella sezione "**Centrale → Settori**" e trascinarlo come illustrato nell'immagine seguente:




Se si desidera comandare il settore 1 della centrale dall'apposito indirizzo di comando KNX e, al variare del suo stato di inserimento, notificarne lo stato sull'indirizzo di stato (entrambi creati in precedenza come illustrato nel capitolo "9. PROTOCOLLO KNX"), procedere effettuando le seguenti operazioni:

1. Trascinare il settore 1 dalla sezione "**Centrale → Settori**";
2. Trascinare l'indirizzo "**Settore 1 – Inserimento (comando)**" a sinistra del settore 1;

3. Trascinare l'indirizzo "**Settore 1 – Inserimento (stato)**" a destra del settore 1;
4. Premere il pulsante sinistro del mouse in corrispondenza del nodo di comando del primo oggetto KNX e, sempre tenendo premuto, connetterlo al nodo "ARM" del settore (in questo modo, viene comandato il settore al cambio di stato dell'indirizzo KNX);
5. Analogamente, connettere il nodo di uscita "ARM" all'oggetto KNX di stato. In questo modo:
   - Quando si riceve un valore 1 sull'indirizzo di gruppo 0/0/1, viene inserito il settore e, viceversa, esso viene disinserito alla ricezione del valore 0;
   - Quando varia lo stato di inserimento del settore (non solo ad opera del gateway, ma anche in virtù di un comando in campo), lo stato di inserimento (1 o 0) viene inviato sul bus all'indirizzo di gruppo 0/1/1.




È possibile modificare il comportamento predefinito di una connessione premendo il pulsante destro sopra di essa; viene aperto il pannello laterale (visibile nella figura accanto), nel quale è possibile specificare:


- **Condizione**: Il valore dell'oggetto di origine che determina il comando sull'oggetto di destinazione. Può essere "SEMPRE" (quindi non viene applicato alcun filtro) oppure uno dei possibili valori per l'oggetto selezionato;
- **Valore**: Valore da inviare all'oggetto di destinazione. Può essere:
  - VALORE CORRENTE: viene passato il valore dell'oggetto di origine a quello di destinazione;
  - VALORE NEGATO: il valore dell'oggetto sorgente viene invertito prima di essere passato alla destinazione;
  - Un valore specifico tra quelli disponibili per l'oggetto di destinazione.

Riprendendo l'esempio precedente, se si vuole inserire solo il settore 1 alla ricezione di un valore 1 sull'indirizzo di gruppo 0/0/1 ma non disinserirlo alla ricezione di uno 0 occorre:

- Indicare "Se ON" come condizione;
- Specificare "ON" come valore.

Gli indicatori grafici sui nodi interessati dalla connessione si modificano di conseguenza, per evidenziare graficamente il comportamento della connessione stessa.
È possibile anche simulare il funzionamento delle regole gateway in tempo reale, interagendo con i nodi di comando (lato destro) degli oggetti KNX e SCS; a tale scopo:

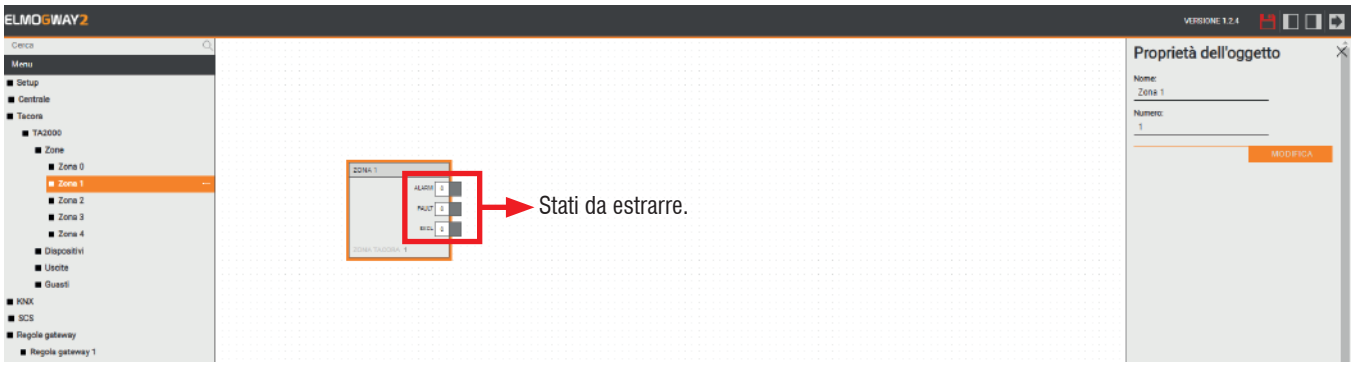
- Fare doppio click sul valore numerico del nodo (quadrato bianco);
- In caso di nodi ON/OFF, viene immediatamente inviato un valore;
- In caso di nodi numerici, viceversa, viene presentata la possibilità di inserire un valore (digitandolo e premendo INVIO).

### Esempio con centrali antincendio TACÓRA

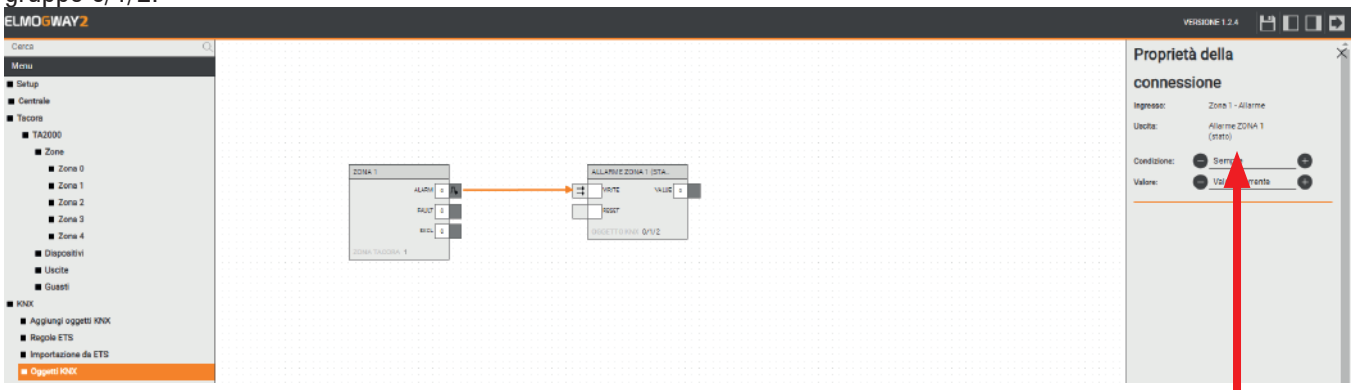
A partire dalla versione firmware 1.2.4, nelle regole gateway inerenti le centrali antincendio Tacóra è possibile trascinare blocchi relativi a:

- zone (allarme, guasto, esclusione)
- dispositivi (esclusione, richiesta ripristino, stato uscita a bordo)
- uscite (gestite dalla centrale)
- guasti (gestiti dalla centrale)

con la possibilità di gestirne gli stati (indicati tra parentesi).
Non è possibile effettuare operazioni di comando sugli elementi precedentemente descritti.




Nell'esempio seguente, quando varia lo stato di allarme della zona 1, lo stato di allarme (1 o 0) viene inviato all'indirizzo di gruppo 0/1/2.




È possibile modificare il comportamento predefinito di una connessione premendo il pulsante destro sopra di essa; viene aperto il pannello laterale (visibile nella figura accanto), nel quale è possibile specificare:

- **Condizione**: Il valore dell'oggetto di origine che determina il comando sull'oggetto di destinazione. Può essere "SEMPRE" (quindi non viene applicato alcun filtro) oppure uno dei possibili valori per l'oggetto selezionato;
- **Valore**: Valore da inviare all'oggetto di destinazione. Può essere:
  - VALORE CORRENTE: viene passato il valore dell'oggetto di origine a quello di destinazione;
  - VALORE NEGATO: il valore dell'oggetto sorgente viene invertito prima di essere passato alla destinazione;
  - Un valore specifico tra quelli disponibili per l'oggetto di destinazione.

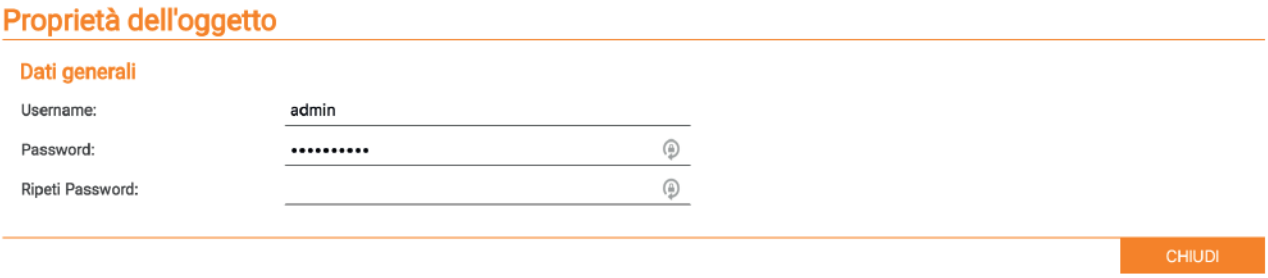

**Nota**: se nella barra in alto appare il messaggio "**Oggetto non supportato all'interno delle regole gateway**", verificare che non si stia tentando di aggiungere un oggetto non previsto per le regole, oppure un oggetto previsto ma incompleto in qualche parametro (ad esempio gli indirizzi di gruppo, ecc.).

# 12. UTENTI


## 12.1 Cambio credenziali

È possibile cambiare le credenziali di accesso dell'utente admin nel seguente modo:

1. Selezionare la voce "admin" nella sezione "**Utenti**" del menu;
2. Accedere alla sua scheda cliccando sui "tre puntini" o sul pulsante "MODIFICA" presente nella toolbar;
3. Modificare a piacimento lo username: non deve contenere spazi o caratteri speciali;
4. Modificare la password, avendo cura di inserirla due volte.





info@elmospa.com
elmospa.com

## 13. INDICE




ELMOGWAY, ELMOGWAY2 - Gateway fra centrali EL.MO. e sistemi di Home & Building Automation
MANUALE TECNICO - Edizione maggio 2022 090001051





**EL.MO. Spa** Via Pontarola, 70 - 35011 Campodarsego (PD) - Italy
Tel. +390499203333 - Fax +390499200306 - Technical Ass. +390499200426 - www.elmospa.com - info@elmospa.com