SpaceLogic KNX

Gateway IP BMS

LSS100300

Guida utente

10/22 – SpaceLogic KNX Gateway IP BMS

www.se.com

Schneider Electric

Informazioni legali

Marchi

Avvertenze

Leggere attentamente le seguenti istruzioni e familiarizzare con il modulo ibrido prima dell'installazione, della messa in funzione e della manutenzione. Le avvertenze elencate di seguito sono presenti nella documentazione e indicano rischi e pericoli potenziali, o informazioni specifiche che chiariscono o semplificano una procedura.

L'aggiunta di un simbolo alle istruzioni di sicurezza in caso di "Pericolo" o di "Avvertenza" indica un pericolo elettrico che potrebbe causare lesioni gravi in caso di mancato rispetto delle istruzioni.

Questo simbolo rappresenta un avviso di sicurezza. Indica il rischio potenziale di lesioni personali. Seguire tutte le istruzioni di sicurezza contrassegnate con questo simbolo per evitare lesioni gravi o mortali.

PERICOLO

PERICOLO indica una situazione di pericolo imminente che inevitabilmente provocherà lesioni gravi o fatali, se le istruzioni non vengono rispettate**.**

AVVERTENZA

AVVERTENZA indica un possibile pericolo che potrebbe causare lesioni gravi o mortali se non viene evitato.

ATTENZIONE

ATTENZIONE indica un possibile pericolo che potrebbe causare lesioni di lieve entità se non viene evitato.

NOTA

NOTA fornisce informazioni su procedure che non presentano alcun rischio di lesioni fisiche.

Simboli

Informazioni aggiuntive

È necessario rispettare le informazioni fornite, altrimenti si potrebbero verificare errori del programma o dei dati.

Indice

1 Per la sicurezza del personale

AVVERTENZA

RISCHIO DI FOLGORAZIONE O ARCO ELETTRICO

L'installazione elettrica sicura deve essere eseguita solo da professionisti qualificati. I professionisti qualificati devono dimostrare di possedere conoscenze approfondite nei seguenti settori:

- Collegamento di impianti elettrici in rete
- Collegamento di molteplici dispositivi elettrici
- Posa di cavi elettrici
- Collegamento e realizzazione di reti KNX
- Norme di sicurezza, prescrizioni e regolamenti locali per il cablaggio.

La mancata osservanza di queste istruzioni può causare lesioni gravi o la morte..

AVVERTENZA

PERICOLO DI INFORMAZIONI ERRATE

- Non configurare il software in modo scorretto in quanto ciò può causare errori nei report e/o nei risultati dei dati.
- Non basare le azioni di manutenzione o assistenza esclusivamente sulle informazioni e sui messaggi visualizzati dal software.
- Non affidarsi esclusivamente ai report e ai messaggi software per determinare se il sistema funziona correttamente o soddisfa tutti gli standard e i requisiti applicabili.
- Considerare le conseguenze di ritardi di trasmissione imprevisti o di guasti ai collegamenti di comunicazione.

La mancata osservanza di tali istruzioni può causare lesioni personali gravi, anche letali, o danni all'apparecchiatura.

Personale qualificato

Questo documento è destinato al personale responsabile di configurazione, installazione, messa in servizio e dell'utilizzo del dispositivo e del sistema in cui è installato.

Una competenza approfondita, acquisita tramite corsi di formazione sul sistema KNX, è un prerequisito.

2 Introduzione

SpaceLogic KNX Gateway IP BMS (di seguito denominato **gateway**) è un dispositivo multifunzionale che consente di integrare l'installazione di KNX con i dispositivi di automazione degli edifici.

L'interfaccia di comunicazione principale è KNX TP e IP, che supportano il protocollo BACnet.

Esistono tre componenti combinati in un unico dispositivo:

- router KNX IP (max 500 oggetti)
- Interfaccia KNX IP
- Bobina DPSU

Il gateway consente agli installatori professionisti di distribuire installazioni KNX in modo più efficace in termini di costi e di tempo grazie alla combinazione di funzioni.

L'architettura è più semplice perché non è più necessario utilizzare router KNX e alimentatori KNX in relazione a determinati parametri.

Il gateway è progettato per installazioni commerciali.

Questo documento descrive il software applicativo del gateway, le funzionalità del dispositivo e l'interfaccia utente.

2.1 Raccomandazioni sulla sicurezza

- La sicurezza di rete deve essere impostata al livello appropriato. Il gateway deve far parte di una rete sicura con accesso limitato. In caso di connessione Internet, si consiglia vivamente l'utilizzo del canale VPN o HTTPS.
- Utilizzare l'accesso protetto al protocollo HTTPS://IP:Port.
- Il metodo di sicurezza è determinato dalla capacità di altri elementi di rete (firewall, protezione da virus e minacce malware).
- Si consiglia vivamente di conservare i file contenenti i backup in un luogo sicuro e inaccessibile a persone non autorizzate.
- Assicurarsi che il gateway non abbia un indirizzo IP accessibile pubblicamente.
- Non utilizzare il port forwarding per accedere al gateway dalla rete Internet pubblica.
- Il gateway deve essere collocato sul proprio segmento di rete.
- Se il router supporta una rete guest o VLAN, è preferibile collocarvi il gateway.

In caso di vulnerabilità o problemi di sicurezza informatica, contattateci attraverso questa pagina:
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp.
Di seguito sono riportate ulteriori informazioni sull'indurimento del sistema:
https://www.se.com/ww/en/download/document/AN002_107/.

NOTA

DANNI MATERIALI TRAMITE ACCESSO NON AUTORIZZATO ALL'INSTALLAZIONE KNX

Non appena si accede all'installazione KNX tramite Internet, il traffico di dati può essere letto da terzi.

- Utilizzare un accesso VPN solo per questa connessione con crittografia sicura per tutti i pacchetti dati.
- L'hardware richiesto (router VPN) e le funzionalità offerte dai provider di servizi mobili differiscono sensibilmente per quanto riguarda le impostazioni e le possibilità tecniche, a seconda del Paese o dell'area geografica.
- Disporre sempre dell'accesso VPN configurato e commissionato da un provider di servizi VPN specializzato. Il provider di servizi VPN seleziona un provider di servizi mobili appropriato e un hardware adatto per l'accesso VPN e assicura che la VPN sia configurata da uno specialista qualificato.

Schneider Electric non può essere ritenuta responsabile di problemi di prestazioni e incompatibilità causati da applicazioni, servizi o dispositivi di fornitori terzi. Schneider Electric non offre assistenza tecnica durante la configurazione di un accesso VPN.

La mancata osservanza di queste istruzioni può comportare danni all'apparecchio.

L'accesso VPN (VPN = Virtual Private Network) autorizza il dispositivo portatile ad accedere alla rete locale, e quindi anche all'installazione KNX tramite Internet.

Vantaggi della VPN:

- Solo gli utenti autorizzati hanno accesso alla rete locale.
- Tutti i dati sono crittografati.
- I dati non vengono modificati, registrati o deviati durante il trasferimento. Questo viene spesso definito tunnel VPN.

Requisiti per la configurazione di una connessione VPN:

- connessione Internet.
- Il dispositivo portatile e il router sono abilitati per una connessione VPN (client VPN installato).
- Il gateway deve essere collocato sul proprio segmento di rete.
- Se il router supporta una rete guest o VLAN, è preferibile collocarvi il gateway.

2.2 Creare una password complessa

- La password può essere costituita da qualsiasi combinazione di caratteri maiuscoli e minuscoli, numeri e caratteri speciali.
- Utilizzare un minimo di 8 caratteri.
- Rendere la password difficile da indovinare o trovare nei dizionari relativi alla criminalità informatica.
- Prediligere frasi.
- Modificare la password frequentemente, almeno una volta all'anno.
- Modificare la password predefinita "Admin" subito dopo averla ottenuta e dopo un ripristino delle impostazioni di fabbrica.
- Non riutilizzare mai le password.

3 Specifiche dispositivo

Specifiche	Descrizione	Nota
Terminali, interfaccia	1 x RJ45 – ethernet 10BaseT/100BaseTx 1 x KNX TP 1 x Pulsante di ripristino	
Connettività	Connessione IP LAN 10/100 Mbit Bus KNX / EIB TP	
Indicatori LED	2 LED, CPU (Funzionamento + Ripristino)	
Inoltro KNX IP	500 oggetti (disabilitati automaticamente quando supera questo limite)	È possibile utilizzare fino a 4000 punti BACnet. Vedi Prestazioni → 10.
Tunneling KNX IP	Per la messa in servizio dei dispositivi KNX tramite ETS	
Limitazione KNX TP	Il limite della larghezza di banda del mezzo KNX TP è limitato a 9,6 kbits/s. Su ciascuna linea KNX TP è possibile trasferire da 20 a 40 telegrammi al secondo.	
Sistema operativo (firmware)	Flashsys	
Applicazioni	Applicazione di configurazione integrata con webserver.	
Impostazione interfaccia IP	Per impostazione predefinita – IP statico 192.168.0.10/255.255.255.0	
Revisione protocollo BACnet	22	
Profilo dispositivo BACnet	B – ASC, B – GW	

4 Compatibilità

Il Gateway è compatibile con i seguenti standard:

- KNX/EIB TP
- KNXnet/IP
- BACnet IP

5 Prestazioni

Parametro	Nota	
Numero di oggetti BACnet	4000	Numero massimo di punti definibili nel dispositivo virtuale BACnet all'interno del gateway. Gli oggetti che superano il limite vengono scartati in modo silenzioso.
Numero di richieste di sottoscrizioni BACnet (COV)	4000 (1500*)	Numero massimo di richieste di sottoscrizioni BACnet (COV) accettate dal gateway.
Oggetti gruppo KNX	4000	Numero massimo di indirizzi di gruppo KNX diversi importabili/definibili.

*Il supporto BACnet COV offre una comunicazione dati veloce riducendo, al contempo, il traffico di rete BACnet.

*1500 per SXWAUTSVR10001 – Server di automazione di Schneider Electric.

6 Per iniziare

Avant de commencer, assurez-vous que la passerelle est correctement connectée, conformément aux instructions d'installation.

Vous avez besoin d'un navigateur web standard pour travailler avec l'application et configurer la passerelle. Les navigateurs web Google Chrome ou Mozilla Firefox sont recommandés.

Lors de l'accès initial :

Adresse IP par défaut

1. Tapez l'adresse IP par défaut 192.168.0.10 dans la barre d'adresse de votre navigateur web et cliquez sur *Entrée*.

La passerelle utilise un certificat autosigné, et le message suivant s'affiche :

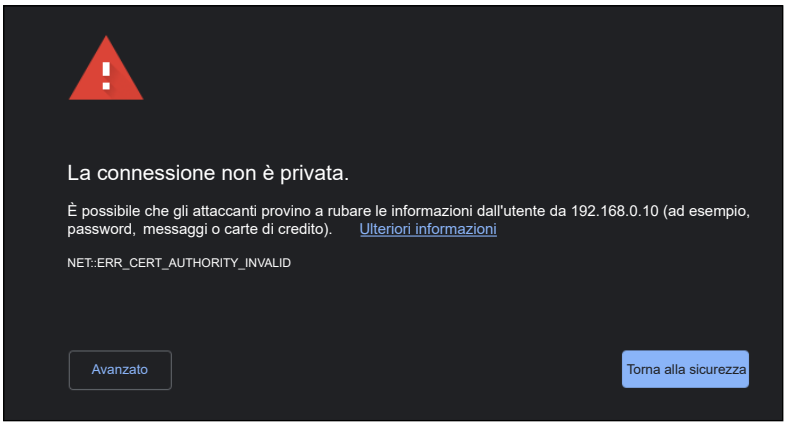

Fig. 1 Avertissement : Votre connexion n'est pas privée

Par défaut, la passerelle utilise un mode de communication HTTPS. En raison du certificat autosigné utilisé, vous devez confirmer l'exception pour continuer. HTTPS fournit une communication cryptée entre la passerelle et le client.

2. Cliquez sur *Réglages avancés* > *Passer à 192.168.0.10*.

Fig. 2 Avertissement : Passer à 192.168.0.10

Nom d'utilisateur et mot de passe

3. Saisissez les identifiants de connexion par défaut et cliquez sur *Entrée*.

nom d'utilisateur : **admin**

mot de passe : **admin**

Invitation à modifier le mot de passe

4. Vous serez invité(e) à modifier votre mot de passe. Saisissez le mot de passe et cliquez sur *Sauvegarder*.

Votre nouveau mot de passe doit contenir au moins 8 caractères, comme suit :

- une lettre majuscule
- une lettre minuscule
- un chiffre

Page de démarrage

5. L'étape suivante vous conduit à la page de démarrage.

Fig. 3 Page de démarrage

Vous y trouverez :

- les paramètres de langue
- les paramètres de la passerelle ( )
- un outil pour filtrer et travailler avec les objets
- le bouton *Importer le projet KNX*

Paramètres de langue

Tout d'abord, sélectionnez votre langue préférée pour l'application dans le menu déroulant.

Fig. 4 Sélectionnez votre langue

Dans les étapes suivantes, vous importerez votre projet KNX et définirez les paramètres de l'appareil.

.

7 Importa progetto KNX

Il pulsante *Importa progetto KNX* in alto a destra consente di importare il file *.knxproj direttamente nel gateway. Questo conserva la struttura del progetto e i DPT degli indirizzi di gruppo, incluse le unità e i suffissi automatici.

Gli oggetti con lo stesso nome sono considerati duplicati e potrebbero non essere importati e contrassegnati come scartati.

È possibile aggiungere oggetti senza tipi di dati definiti e anche nomi dei livelli di struttura agli oggetti.

I file *.knxproj protetti da password richiedono l'impostazione della password in ETS. Non è possibile importare il progetto senza conoscere la password corretta.

Importare progetto KNX

Per importare il progetto, procedere come segue:

1. fare clic sul pulsante *Importa progetto KNX* e scegliere il file.
2. Digitare la password corretta, se applicabile.
3. Selezionare *Aggiungi nomi di livello agli oggetti* se si desidera importare anche nomi degli oggetti e la relativa designazione di posizione della struttura.
4. È possibile selezionare *Sovrascrivi oggetti esistenti* se si desidera sovrascrivere gli oggetti esistenti.
5. Fare clic su *Avanti*.

Le tabelle di filtraggio vengono compilate automaticamente in base al progetto KNX importato e possono essere modificate ulteriormente.

Anche la chiave dorsale viene importata automaticamente dal progetto KNX.

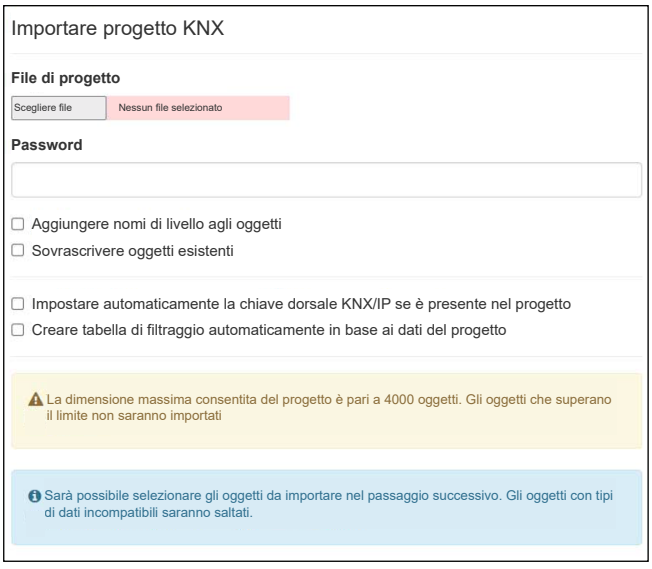

Fig. 5 Importare il progetto KNX.

Impossibile abilitare l'inoltro KNX per progetti di dimensioni superiori a 500 oggetti.

Selezionare gli oggetti da importare

Nel passaggio successivo, si scelgono gli oggetti del progetto KNX che si desidera esportare in BACnet. Solo gli oggetti selezionati vengono importati nel database del gateway.

È possibile filtrare gli oggetti in base a nome, indirizzo di gruppo o tipo di dati per semplificare la ricerca dell'oggetto. Scopri di più in Filtraggio e modifica delle proprietà degli oggetti → 16.

Scegliere gli oggetti e fare clic su *Avanti*.

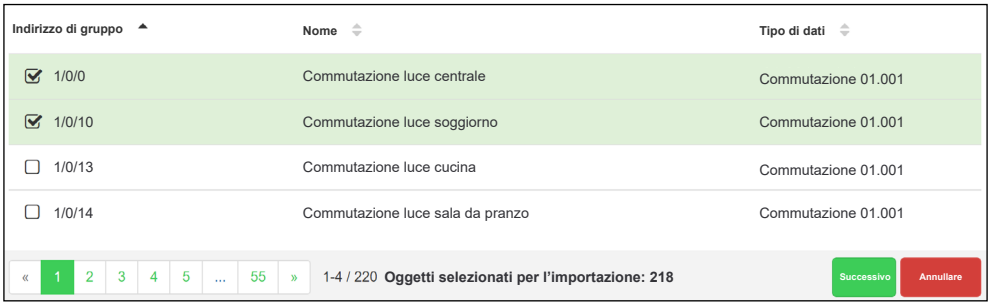

Fig. 6 Scegliere gli oggetti da importare.

Concludere l'importazione degli oggetti

Compare una finestra pop-up che informa sul numero di oggetti importati.

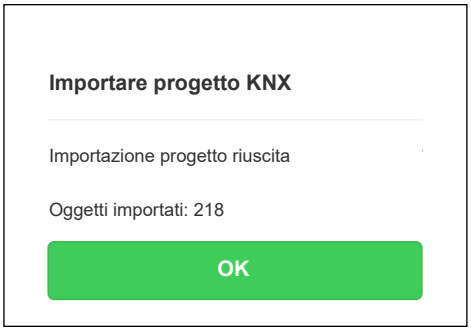

Fig. 7 Finestra di dialogo finale Importa progetto KNX.

Fare clic su *OK* per completare il processo di importazione.

7.1 Aggiungi oggetto

La funzione *Aggiungi oggetto* è utile quando è necessario aggiungere un unico oggetto in un secondo momento e non si desidera importare nuovamente l'intero file *.knxproj.

Aggiungere oggetti

Per aggiungere un nuovo oggetto, procedere come segue:

1. fare clic su *Aggiungi oggetto*.
2. Compilare i dati dell'oggetto.
3. Fare clic su *Salva*.

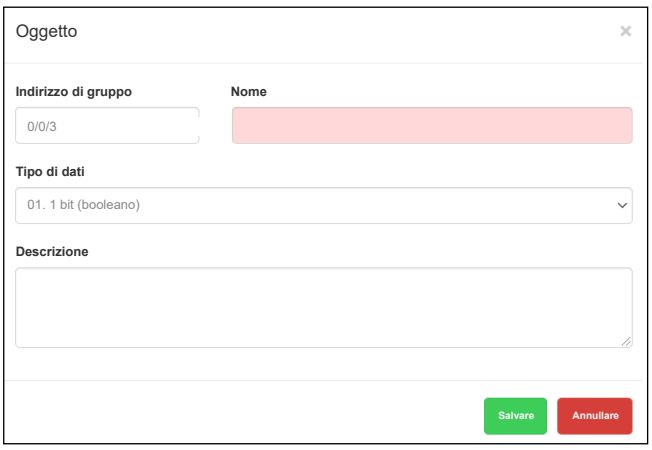

Fig. 8 Aggiunta di oggetti.

7.2 Azioni

Eliminazione di massa

La funzione *Eliminazione di massa* consente di eliminare oggetti in blocco.

Vi sono due opzioni:

- *Elimina tutti gli oggetti*
- *Elimina oggetti dal filtro corrente*

Nel passaggio successivo, gli oggetti vengono eliminati nel modo selezionato.

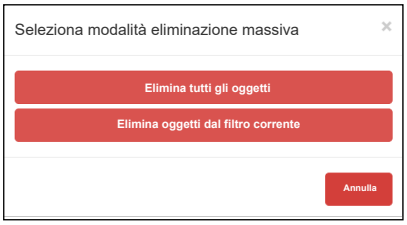

Fig. 9 Eliminazione di oggetti in blocco

Modifica di massa

È possibile modificare unità e incrementi COV degli oggetti in blocco.

1. Filtrare gli oggetti che si desidera modificare.
2. Fare clic su *Azioni* > *Modifica di massa*.
3. Selezionare i parametri – unità e/o valore di incremento COV e fare clic su *Salva*.

Esporta CSV

È possibile esportare oggetti in un file .csv.

Fare clic su *Azioni* > *Esporta in CSV*.

Il file .csv con tutti gli oggetti viene scaricato automaticamente nella cartella *Download* locale, da dove è possibile aprirlo in MS Excel.

7.3 Filtraggio e modifica delle proprietà degli oggetti

Filtraggio oggetti

È possibile filtrare gli oggetti in base al nome, all'indirizzo di gruppo o al tipo di dati. È possibile selezionare dal menù a tendina o digitare ciò che si sta cercando.

Fig. 10 Filtraggio oggetti

Modifica delle proprietà dell'oggetto

È possibile modificare le proprietà degli oggetti e i relativi valori in un secondo momento, se necessario. Oppure è possibile eliminarli singolarmente.

Modificare le proprietà dell'oggetto osservando i seguenti passaggi:

Editing delle proprietà dell'oggetto

1. Fare clic su .
2. Modificare proprietà dell'oggetto.
3. Fare clic su *Salva*.

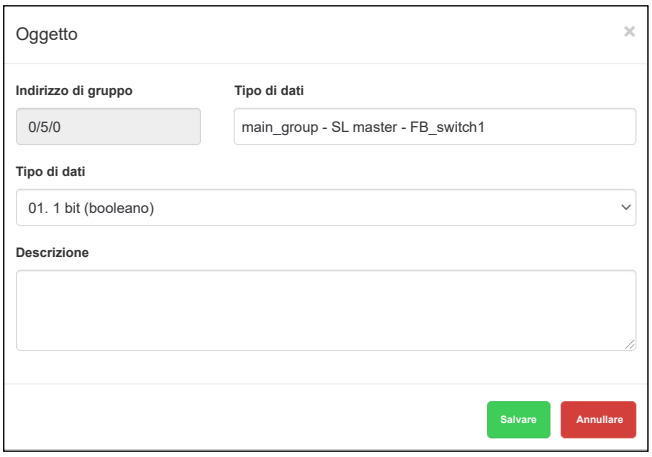

Fig. 11 Modifica delle proprietà dell'oggetto

Impostazione del valore dell'oggetto

È possibile impostare il valore dell'oggetto.

1. Fare clic su .
2. Selezionare nell'elenco a discesa *Valore*.
3. Fare clic su *Imposta*.

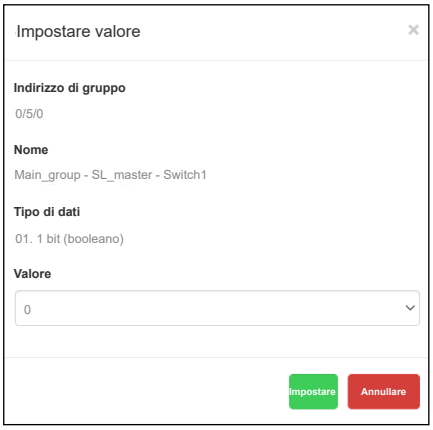

Fig. 12 Impostazione del valore dell'oggetto

Eliminazione dell'oggetto

Se si desidera eliminare un oggetto, fare clic su . Fare clic su *Sì* per confermare.

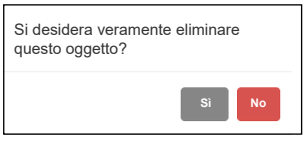

Fig. 13 Eliminazione dell'oggetto

8 Impostazioni dell'applicazione

Dopo aver configurato l'interfaccia utente dell'applicazione e dopo aver importato il progetto ETS, è possibile impostare i singoli parametri del gateway.

Nel menù principale sono disponibili le seguenti opzioni:

- Backup
- Ripristina
- Modifica password
- Nome host
- Configurazione BACnet
- Configurazione KNX
- Configurazione di rete
- Configurazione server HTTP
- Certificato SSL HTTP
- Configurazione client NTP
- Data e ora
- Registro di sistema
- Ping
- Attiva/disattiva identificazione dispositivo
- Aggiorna firmware
- Ripristino delle impostazioni di fabbrica
- Riavvia
- Arresta

8.1 Backup

La finalità del backup è creare una copia dei dati ripristinabile in caso di guasto dei dati primari.

Per creare un file di backup, andare su  e selezionare l'opzione *Backup* dal menù a discesa.

Il file di backup viene scaricato immediatamente nella cartella *Download* del browser. Il nome del file di backup è costituito dai seguenti dati:

Hostname-backup-yyyy.mm.dd-hh.mm.bckp

La data e l'ora effettive del gateway vengono utilizzate quando viene generato il backup. Successivamente è possibile rinominare il file e salvarlo in un'altra cartella.

8.2 Ripristina

Viene eseguito un ripristino per ripristinare i dati persi, rubati o danneggiati alle condizioni originali o per spostarli in una nuova posizione. Utilizzare i file di backup per ripristinare i dati del gateway a un punto precedente.

Per ripristinare i dati, procedere come segue:

Ripristino dati

1. andare su ☰.
2. Fare clic su *Ripristina*.
3. Fare clic su *Scegli file* e trovare il file di backup.

Se si desidera ripristinare anche i file di configurazione, selezionare l'opzione *Ripristina file di configurazione*.

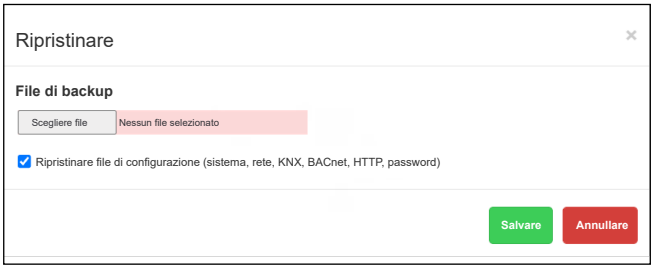

Fig. 14 Ripristino della configurazione dell'applicazione

Dopo aver fatto clic su *Salva*, compare una finestra pop-up che chiede se si desidera riavviare il sistema. Selezionare *Sì* o *No*. Se si seleziona *No*, non verrà importato nulla.

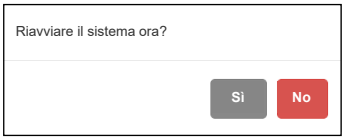

Fig. 15 Riavvio del sistema

8.3 Modifica password

Per modificare la password, procedere come segue:

1. Andare su ☰.
2. Fare clic su *Modifica password*.
3. Inserire la password attuale e quella nuova.
4. Fare clic su *Salva*.

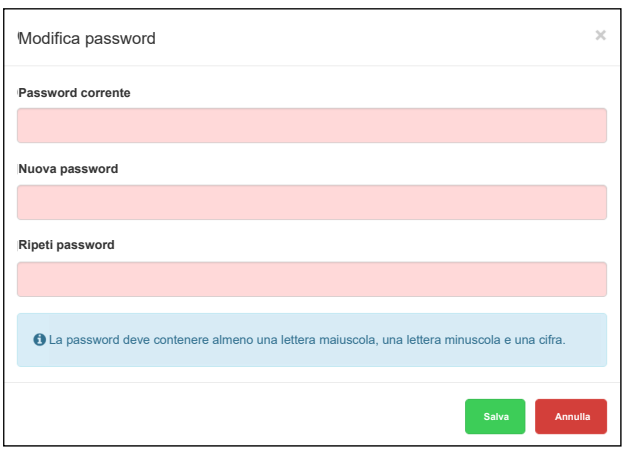

Fig. 16 Modifica della password

8.4 Nome host

È possibile modificare il nome host del gateway per facilitare l'identificazione. Questo viene visualizzato nel nome del file di backup.

Per modificare il nome host, procedere come segue:

Modifica del nome host

1. andare su .
2. Selezionare *Nome host*.
3. Digitare il nome host.
4. Fare clic su *Salva*.

8.5 Configurazione BACnet

Server BACnet

Il gateway funge da server BACnet. Serve dati leggibili per i dispositivi client BACnet, che possono scrivere dati sul server.

Il protocollo BACnet consente lo scambio di informazioni per i dispositivi di automazione degli edifici, indipendentemente dal particolare servizio che essi eseguono.
I dispositivi sono collegati tramite il livello fisico Ethernet.

La connessione alla rete BACnet proviene dagli oggetti del gruppo KNX, che vengono esportati in BACnet.

Gli oggetti binari vengono visualizzati come valori binari, mentre i valori numerici verranno visualizzati come valori analogici. Gli altri tipi di dati non sono supportati.

Configurazione BACnet

1. Andare su .
2. Selezionare *Configurazione BACnet*.

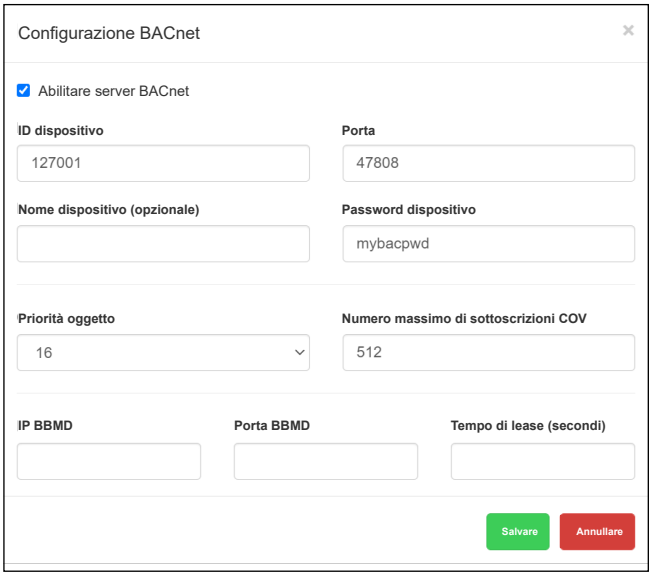

Fig. 17 Configurazione BACnet

3. Configurare i seguenti parametri BACnet e fare clic su *Salva*.

Parametro	Nota
Abilitare server BACnet	Disabilitato per impostazione predefinita
ID dispositivo	Scegliere ID di rete univoco
Porta	Porta BACnet, 47808 per impostazione predefinita
Nome dispositivo (opzionale)	hostname_Device ID del controller per impostazione predefinitaSe si inserisce qui il nome del dispositivo, allora nome BACnet = nome dispositivo.
Password dispositivo	Password BACnet La password verrà utilizzata per i servizi BACnet (per es., "DeviceCommunicationControl" e "ReInitializeDevice" – reinizializzazione del dispositivo). Se la password non è definita, non viene inviata al dispositivo BACnet.
Priorità oggetto	Posizione predefinita dell'array di priorità
Numero massimo di sottoscrizioni COV	4000 (vedi Prestazioni → 10).
IP BBMD	IP router BACnet
Porta BBMD	Porta router BACnet
Tempo di lease (secondi)	Intervallo di reinvio della registrazione BBMD

8.6 Configurazione KNX

Nel menù *Configurazione KNX*, è possibile configurare le impostazioni dei dati di KNX quando il gateway viene utilizzato come interfaccia KNX IP o router.

Configurazione KNX

1. Andare su .
2. Fare clic su *Configurazione KNX*.

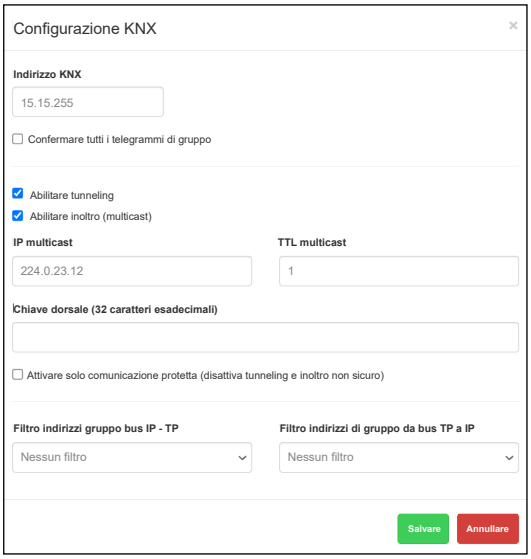

Fig. 18 Configurazione KNX

3. Configurare i seguenti parametri BACnet e fare clic su *Salva*.

Parametro	Nota
Indirizzo KNX	Indirizzo individuale KNX del dispositivo. 15.15.255 da impostazione predefinita.
Confermare tutti i telegrammi di gruppo	Se il gateway comunica direttamente con un altro dispositivo KNX, deve riconoscere i telegrammi ricevuti. Deselezionare l'opzione se il gateway funziona esclusivamente come sniffer di indirizzi di gruppo.
Abilitare il tunneling	Consente a più dispositivi di collegarsi alla rete pubblica utilizzando lo stesso indirizzo IPv4 pubblico. Modifica le informazioni dell'indirizzo IP nelle intestazioni IPv4 in transito su un dispositivo di routing del traffico. La connessione IP è 1000 volte più rapida di TP-UART. Il gateway come server. Unicast, scambio dati riconosciuto, indirizzo individuale aggiuntivo per connessione tunneling.
Abilitare inoltro (multicast)	Trasferimento dati Multicast non riconosciuto. Gateway come accoppiatore di linea o dorsale.
IP multicast	Indirizzo IP multicast, 224.0.23.12 per impostazione predefinita.
TTL multicast	Il valore predefinito è 1; consente la comunicazione tra sottoreti diverse.
Chiave dorsale (32 caratteri esadecimali)	Chiave dorsale per la crittografia e la decrittografia dei telegrammi protetti per l'inoltro IP.
Abilitare solo comunicazioni sicure -	Il tunneling e il routing non sicuro sono disabilitati.
Filtro indirizzi gruppo bus IP - TP	Nessun filtro Accettare indirizzi di gruppo selezionati Eliminare indirizzi di gruppo selezionati Esempi di immissione filtro: - Indirizzo singolo (1/1/1) - Intervallo (1/1/1-1/1/100) - Wildcard (1/1/* or 1/*/*)
Filtro indirizzi di gruppo da bus TP a IP	

8.7 Configurazione di rete

La configurazione di rete è il processo di impostazione dei controlli, del flusso e del funzionamento di una rete per supportare la comunicazione di rete. Dopo aver impostato i parametri di rete, è necessario riavviare il sistema per rendere effettive le modifiche.

Configurazione di rete

1. Andare su .
2. Fare clic su *Configurazione di rete*.

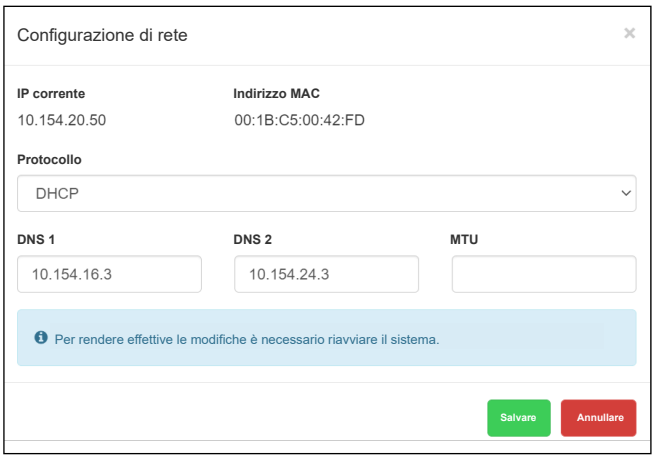

Fig. 19 Configurazione di rete

3. Configurare i seguenti parametri di rete e fare clic su *Salva*.

Parametro	Nota
IP corrente	L'indirizzo IP fornito dal server DHCP o l'indirizzo IP statico. Questo campo compare solo se viene fornito l'indirizzo IP, altrimenti è nascosto.
Indirizzo MAC	Ciascun dispositivo ha il proprio indirizzo MAC univoco.
Protocollo	Protocollo specifico utilizzato per l'indirizzamento: IP statico DHCP
Indirizzo IP	192.168.0.10 per impostazione predefinita
Maschera di rete	255.255.255.0 per impostazione predefinita
IP gateway	Nessuno per impostazione predefinita
DNS 1	Indirizzo IP del server DNS primario.
DNS 2	Indirizzo IP del server DNS secondario.
MTU	Unità di trasmissione massima, la dimensione massima del pacchetto che può essere passata nel protocollo di comunicazione. (Valore predefinito 1500).

Nella finestra pop-up, fare clic su *Sì* e confermare il riavvio del sistema per rendere effettive le modifiche.

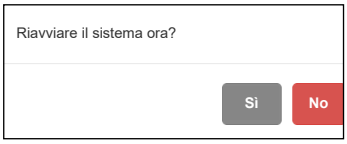

Fig. 20 Riavvio del sistema

8.8 Configurazione server HTTP

In questa sezione viene impostato il livello di sicurezza della comunicazione del gateway con il server web e le porte HTTP/S aggiuntive.

Configurazione server HTTP

1. Andare su .
2. Selezionare *Configurazione server HTTPS*.

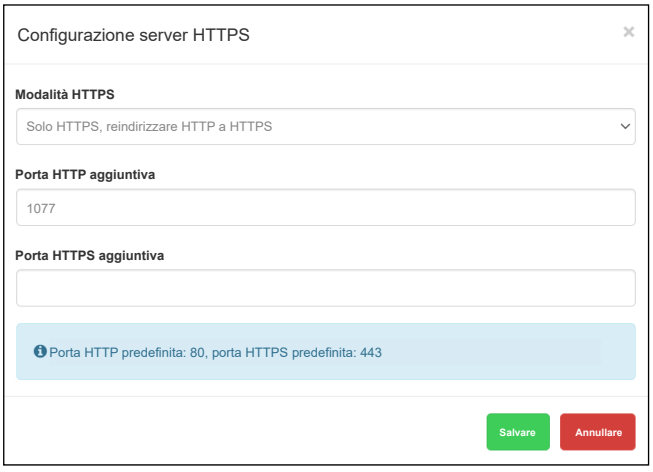

Fig. 21 Configurazione del server HTTP

3. Configurare i seguenti parametri del server HTTPS e fare clic su *Salva*.
4. Riavviare per rendere effettive le modifiche.

Parametro	Nota
Modalità HTTPS	HTTP e HTTPS abilitati Solo HTTPS, reindirizzamento ad HTTPS Solo HTTPS, porta HTTP disabilitata
Porta HTTP aggiuntiva	Selezionare il numero. (Porta HTTP predefinita: 80.)
Porta HTTPS aggiuntiva	Selezionare il numero. Porta HTTPS predefinita: 443.

Modalità HTTPS:

- **HTTP e HTTPS abilitati** – comunicazione HTTP e HTTPS consentite
- **Solo HTTPS, reindirizzamento da HTTP ad HTTPS** – tutte le comunicazioni sulle porte HTTP verranno reindirizzate ad HTTPS
- **Solo HTTPS, la porta HTTP è disabilitata** – è abilitata solo la comunicazione protetta

Per motivi di sicurezza, si consiglia la modalità di comunicazione HTTPS.

8.9 Certificato SSL HTTP

I certificati SSL sono file di dati che legano digitalmente una chiave crittografica ai dati di un dispositivo. Quando viene installato su un server web, attiva il lucchetto e il protocollo HTTPS e consente connessioni protette da un server web a un browser.

Impostazioni certificato HTTP SSL

1. Andare su .
2. Fare clic su *Certificato SSL HTTP*.
3. Scegliere la *Modalità*:
   - *Carica nuova/o chiave/certificato privata/o*: caricare la chiave RSA/il certificato SSL esistente
   - *Genera nuova/o chiave/certificato privata/o*: Genera una chiave RSA/un certificato SSL da un(a) già installata/o
4. Fare clic su *Salva* e riavviare per rendere effettive le modifiche.

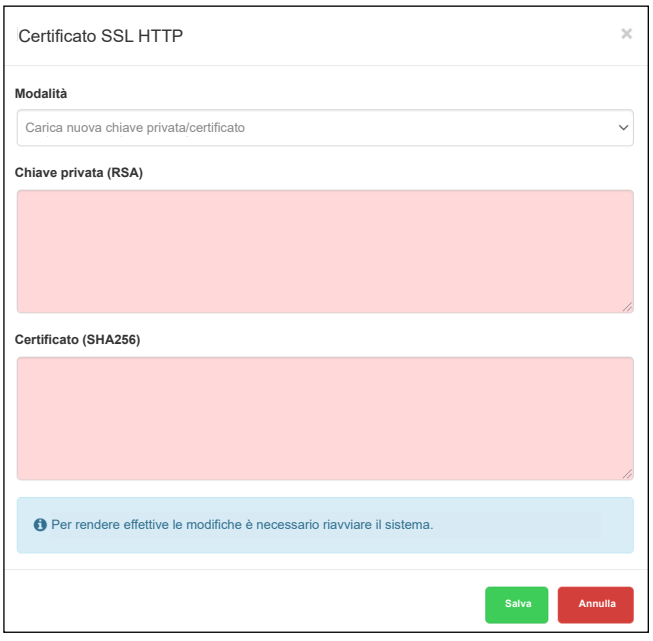

Fig. 22 Certificato SSL HTTP

8.10 Configurazione client NTP

L'NTP (Network Time Protocol) è pensato per sincronizzare tutti i dispositivi partecipanti entro pochi millisecondi dal tempo coordinato universale (UTC - Coordinated Universal Time). È progettato per mitigare gli effetti della latenza di rete variabile.

Se il client NTP è abilitato, il gateway può acquisire dati da un massimo di 4 server selezionati (priorità da 1 a 4 in una riga).

Definire il server da cui vengono ottenute la data e l'ora.

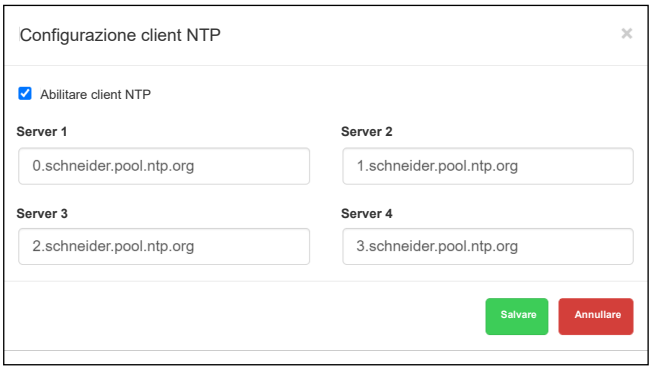

Fig. 23 Configurazione client NTP

È necessario riavviare dopo la configurazione del client NTP.

Verificare la disponibilità del server NTP con lo strumento ping, se necessario.

8.11 Data e ora

Il Network Time Protocol (NTP) è implementato. Insieme alla connessione Internet, il gateway aggiorna automaticamente l'ora da un server NTP.

Impostazione data e ora

1. Andare su .
2. Fare clic su *Data e ora*.
3. Se non vi è alcuna connessione Internet, fare clic su *Recupera dal sistema* per adottare l'ora dal PC.
4. Selezionare il fuso orario e fare clic su *Salva*.

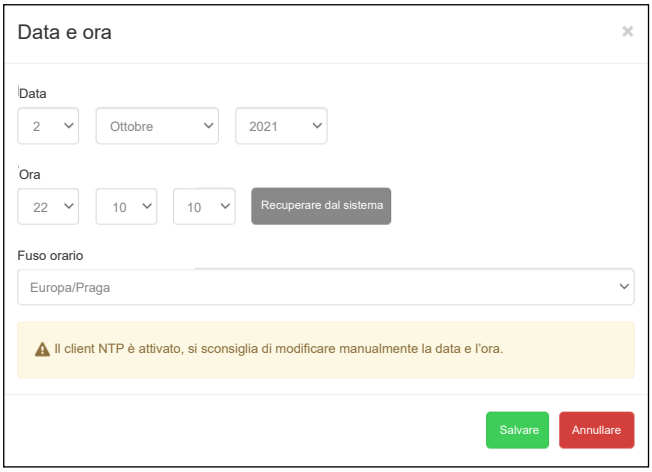

Fig. 24 Impostazione data e ora

8.12 Registro di sistema

Il gateway registra ogni avvio del sistema e disconnessione TP / KNX. Le transazioni vengono registrate cronologicamente in un semplice file di registro. Il file di registro viene creato e gestito automaticamente dal gateway.

Il registro di sistema compare quando si accede a e si fa clic su *Registro di sistema*.

Nella parte inferiore sono riportate le informazioni sul carico della CPU.

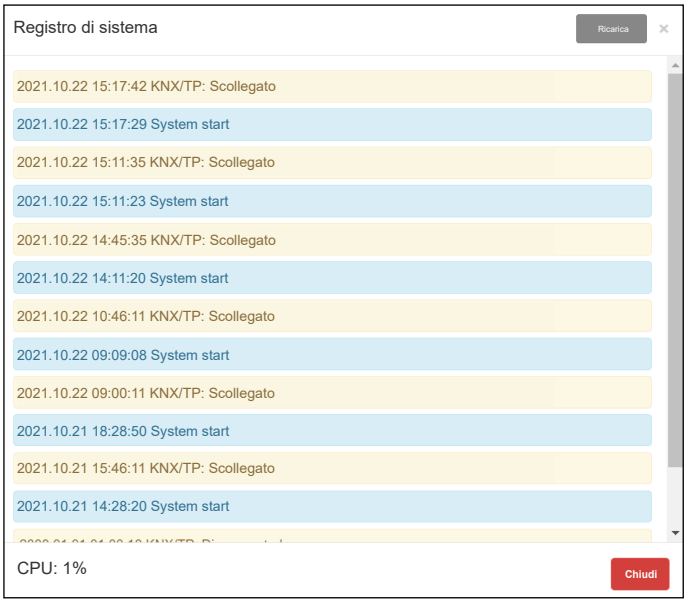

Fig. 25 File di registro

8.13 Ping

Il ping è uno strumento utile per testare la raggiungibilità di un host su una rete con protocollo Internet (IP). Il ping misura il Round Trip Time (percorso) per i pacchetti inviati dall’host di origine a una destinazione che vengono ritrasmessi all’origine.

Eseguire il ping dell’host

Per eseguire il ping dell’host, procedere come segue:

1. Andare su .
2. Selezionare *Ping*.
3. Digitare l’IP o il nome host.
4. Fare clic su *Esegui*.

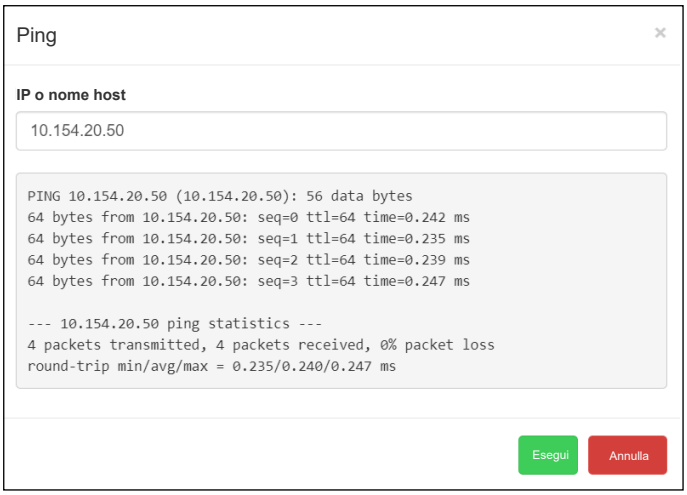

Fig. 26 Statistiche del ping.

8.14 Attiva/disattiva identificazione dispositivo

Attiva/disattiva identificazione dispositivo è una funzione che consente di cercare i singoli dispositivi gateway in una rete. Attivando l’identificazione, il LED 2 lampeggia (rosso/verde) sul dispositivo specifico.

Attiva/disattiva identificazione dispositivo

Andare su , fare clic su *Attiva/disattiva l’identificazione del dispositivo*. Controllare la segnalazione del dispositivo.

8.15 Aggiorna firmware

Un aggiornamento del firmware aggiorna il gateway con istruzioni operative avanzate senza bisogno di aggiornamenti nell'hardware. L'aggiornamento non modifica la configurazione del gateway.

Durante l'aggiornamento del firmware, il dispositivo non risponde e si riavvia più volte.

Il LED1 lampeggia in rosso/verde durante l'aggiornamento. Non scollegare il gateway mentre il LED1 lampeggia.

Aggiornamento del firmware

1. Andare su .
2. Fare clic su *Aggiorna firmware*,
3. Scegliere il file firmware.
4. Scegliere il file firma.
5. Fare clic su *Salva*.

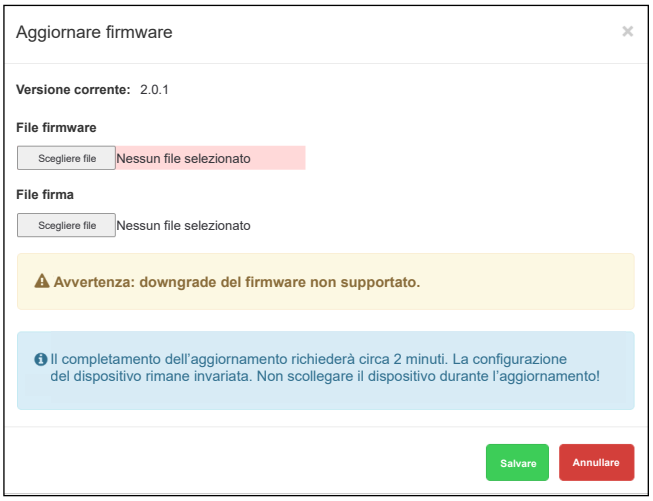

Fig. 27 Aggiornamento del firmware.

Dopo ogni aggiornamento, si consiglia vivamente di pulire la cache del browser.

Il downgrade del gateway con il firmware non è supportato.

Impossibile eseguire l'aggiornamento senza un file firma. Il firmware è sempre distribuito con il file firma appropriato.

8.16 Ripristino delle impostazioni di fabbrica

Un ripristino delle impostazioni di fabbrica cancella tutte le informazioni sul gateway e ripristina il software allo stato originale.

Il gateway può essere ripristinato allo stato originale in due modi:

- nell'applicazione
- con il pulsante di ripristino hardware

Ripristino delle impostazioni di fabbrica dell’applicazione

Per ripristinare il dispositivo tramite l’applicazione, andare su , fare clic su *Ripristino delle impostazioni di fabbrica* e confermare. Il sistema si riavvia automaticamente.

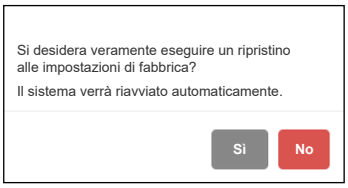

Fig. 28 Ripristino delle impostazioni di fabbrica dell’applicazione.

Parametri del dispositivo dopo il ripristino delle impostazioni di fabbrica:

Parametro	Risultato
Nome dispositivo	LSS100300
Indirizzo IP	L’IP viene mantenuto dopo il ripristino delle impostazioni di fabbrica
Nessun oggetto	Configurazione come BACnet, KNX

Ripristino delle impostazioni di fabbrica dell’hardware

Il ripristino delle impostazioni di fabbrica dell’hardware è adatto per le situazioni in cui il gateway non è disponibile a causa di impostazioni errate.

Premere a lungo (10 s) sul pulsante rosso RIPRISTINO sul lato anteriore. Rilasciare e premere nuovamente per 10 secondi.

L’indirizzo IP dopo il ripristino delle impostazioni di fabbrica dell’HW con il pulsante hardware è sempre 192.168.0.10.

3 tipi di pressione del pulsante HW

Tenere premuto per <10 secondi - riavviare il dispositivo

Tenere premuto per >10 secondi - ripristinare la rete con IP ai valori predefiniti di fabbrica

Tenere premuto per >10 secondi e tenere nuovamente premuto per >10 secondi – ripristino completo della configurazione alle impostazioni predefinite di fabbrica

8.17 Riavviare

Se il dispositivo non funziona come previsto, è possibile riavviare il gateway. Un riavvio è un unico passaggio che prevede sia l’arresto che l’accensione.

Riavvio del gateway

Per riavviare il dispositivo, andare su , selezionare *Riavvia* e fare clic su *Sì*.

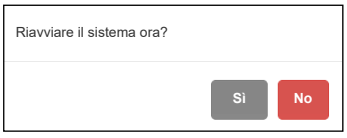

Fig. 29 Riavvio del gateway.

8.18 Arresta

L’*arresto* prevede lo spegnimento del gateway in modo da garantire che non si perdano dati e che il sistema non sia danneggiato. Tutte le impostazioni verranno salvate.

Arresto

Per arrestare correttamente il dispositivo, andare su  , selezionare *Arresto*, fare clic su *Sì* per confermare.

Non scollegare l’alimentazione finché il LED 1 (verde) non smette di lampeggiare! In caso contrario, il database potrebbe non essere salvato in modo sicuro.

L’unico modo per riattivare il gateway è scollegando e ricollegando l’alimentazione.

Schneider Electric SA
35 rue Joseph Monier
92500 Rueil Malmaison - Francia
Telefono: +33 (0) 1 41 29 70 00
Fax: +33 (0) 1 41 29 71 00

Per domande di natura tecnica, contattare il Centro di assistenza clienti del proprio Paese.
schneider-electric.com/contact

LSS100300_SW_IT 10/22