Gateway IP BMS SpaceLogic KNX

LSS100300

Guida utente

LSS100300
Data di pubblicazione 07/2025

www.se.com

Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nel presente documento sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari.

Il presente documento e il relativo contenuto sono protetti dalle leggi vigenti sul copyright e vengono forniti esclusivamente a titolo informativo. Si fa divieto di riprodurre o trasmettere il presente documento o parte di esso, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione o altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

Schneider Electric non concede alcun diritto o licenza per uso commerciale del documento e del relativo contenuto, a eccezione di una licenza personale e non esclusiva per consultarli "così come sono".

Schneider Electric si riserva il diritto di apportare modifiche o aggiornamenti relativi al presente documento o ai suoi contenuti o al formato in qualsiasi momento senza preavviso.

Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per qualsiasi utilizzo non previsto o improprio delle informazioni ivi contenute.

Sommario

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avvertimento” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

⚠ PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un ***AVVISO*** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avvertimento” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

⚠ PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un ***AVVISO*** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Prima di iniziare

Non utilizzare questo prodotto su macchinari privi di sorveglianza attiva del punto di funzionamento. La mancanza di un sistema di sorveglianza attivo sul punto di funzionamento può presentare gravi rischi per l'incolumità dell'operatore macchina.

⚠AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

- Non utilizzare questo software e la relativa apparecchiatura di automazione su macchinari privi di protezione per le zone pericolose.
- Non avvicinarsi ai macchinari durante il funzionamento.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Questa apparecchiatura di automazione con il relativo software permette di controllare processi industriali di vario tipo. Il tipo o il modello di apparecchiatura di automazione adatto per ogni applicazione varia in funzione di una serie di fattori, quali la funzione di controllo richiesta, il grado di protezione necessario, i metodi di produzione, eventuali condizioni particolari, la regolamentazione in vigore, ecc. Per alcune applicazioni può essere necessario utilizzare più di un processore, ad esempio nel caso in cui occorra garantire la ridondanza dell'esecuzione del programma.

Solo l'utente, il costruttore della macchina o l'integratore del sistema sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina e possono quindi determinare l'apparecchiatura di automazione e i relativi interblocchi e sistemi di sicurezza appropriati. La scelta dell'apparecchiatura di controllo e di automazione e del relativo software per un'applicazione particolare deve essere effettuata dall'utente nel rispetto degli standard locali e nazionali e della regolamentazione vigente. Per informazioni in merito, vedere anche la guida National Safety Council's Accident Prevention Manual (che indica gli standard di riferimento per gli Stati Uniti d'America).

Per alcune applicazioni, ad esempio per le macchine confezionatrici, è necessario prevedere misure di protezione aggiuntive, come un sistema di sorveglianza attivo sul punto di funzionamento. Questa precauzione è necessaria quando le mani e altre parti del corpo dell'operatore possono raggiungere aree con ingranaggi in movimento o altre zone pericolose, con conseguente pericolo di infortuni gravi. I prodotti software da soli non possono proteggere l'operatore dagli infortuni. Per questo motivo, il software non può in alcun modo costituire un'alternativa al sistema di sorveglianza sul punto di funzionamento.

Accertarsi che siano stati installati i sistemi di sicurezza e gli asservimenti elettrici/meccanici opportuni per la protezione delle zone pericolose e verificare il loro corretto funzionamento prima di mettere in funzione l'apparecchiatura. Tutti i dispositivi di blocco e di sicurezza relativi alla sorveglianza del punto di funzionamento devono essere coordinati con l'apparecchiatura di automazione e la programmazione software.

NOTA: Il coordinamento dei dispositivi di sicurezza e degli asservimenti meccanici/elettrici per la protezione delle zone pericolose non rientra nelle funzioni della libreria dei blocchi funzione, del manuale utente o di altre implementazioni indicate in questa documentazione.

Avviamento e verifica

Prima di utilizzare regolarmente l'apparecchiatura elettrica di controllo e automazione dopo l'installazione, l'impianto deve essere sottoposto ad un test di avviamento da parte di personale qualificato per verificare il corretto funzionamento dell'apparecchiatura. È importante programmare e organizzare questo tipo di controllo, dedicando ad esso il tempo necessario per eseguire un test completo e soddisfacente.

⚠AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

- Verificare che tutte le procedure di installazione e di configurazione siano state completate.
- Prima di effettuare test sul funzionamento, rimuovere tutti i blocchi o altri mezzi di fissaggio dei dispositivi utilizzati per il trasporto.
- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Eseguire tutti i test di avviamento raccomandati sulla documentazione dell'apparecchiatura. Conservare con cura la documentazione dell'apparecchiatura per riferimenti futuri.

Il software deve essere testato sia in ambiente simulato che in ambiente di funzionamento reale..

Verificare che il sistema completamente montato e configurato sia esente da cortocircuiti e punti a massa, ad eccezione dei punti di messa a terra previsti dalle normative locali (ad esempio, in conformità al National Electrical Code per gli USA). Nel caso in cui sia necessario effettuare un test sull'alta tensione, seguire le raccomandazioni contenute nella documentazione dell'apparecchiatura al fine di evitare danni accidentali all'apparecchiatura stessa.

Prima di mettere sotto tensione l'apparecchiatura:

- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.
- Chiudere lo sportello del cabinet dell'apparecchiatura.
- Rimuovere tutte le messa a terra temporanee dalle linee di alimentazione in arrivo.
- Eseguire tutti i test di avviamento raccomandati dal costruttore.

Funzionamento e regolazioni

Le precauzioni seguenti sono contenute nelle norme NEMA Standards Publication ICS 7.1-1995:

(In caso di divergenza o contraddizione tra una traduzione e l'originale inglese, prevale il testo originale in lingua inglese).

- Indipendentemente dalla qualità e della precisione del progetto nonché della costruzione dell'apparecchiatura o del tipo e della qualità dei componenti scelti, possono sussistere dei rischi se l'apparecchiatura non viene utilizzata correttamente.
- Eventuali regolazioni involontarie possono provocare il funzionamento non soddisfacente o non sicuro dell'apparecchiatura. Per effettuare le regolazioni funzionali, attenersi sempre alle istruzioni contenute nel manuale fornito dal costruttore. Il personale incaricato di queste regolazioni deve avere esperienza con le istruzioni fornite dal costruttore delle apparecchiature e con i macchinari utilizzati con l'apparecchiatura elettrica.
- All'operatore devono essere accessibili solo le regolazioni funzionali richieste dall'operatore stesso. L'accesso agli altri organi di controllo deve essere riservato, al fine di impedire modifiche non autorizzate ai valori che definiscono le caratteristiche di funzionamento delle apparecchiature.

Informazioni sul manuale

Scopo del documento

Questo documento descrive il software applicativo, le funzionalità del dispositivo e l'interfaccia utente del **Gateway IP SpaceLogic KNX BMS** LSS100300.

Si rivolge a integratori di sistemi, ingegneri e utenti tecnici responsabili dell'impostazione della comunicazione tra i sistemi KNX e i sistemi di gestione degli edifici basati su IP (BMS).

Nota di validità

Questa guida utente è valida per il software **Gateway IP SpaceLogic KNX BMS** dalla versione specificata nel documento. Si applica alla configurazione e al funzionamento delle funzionalità software disponibili al momento della pubblicazione.

Eventuali aggiornamenti, ottimizzazioni o modifiche futuri al software potrebbero non essere riflessi in questa guida. Gli utenti sono invitati a consultare la documentazione più recente o a contattare il supporto tecnico per informazioni relative alle versioni più recenti o alle funzionalità aggiuntive.

Informazioni generali sulla sicurezza informatica

Negli ultimi anni, il numero crescente di macchine e impianti di produzione collegati in rete ha visto un corrispondente aumento del potenziale di minacce informatiche, come accessi non autorizzati, violazioni dei dati e interruzioni operative. È pertanto necessario prendere in considerazione tutte le possibili misure di sicurezza informatica per proteggere risorse e sistemi da tali minacce.

Per consentire di mantenere i prodotti Schneider Electric sicuri e protetti, è nell'interesse dell'utente implementare le pratiche migliori di sicurezza informatica come indicato nel documento Cybersecurity Best Practices:

Schneider Electric fornisce ulteriori informazioni e assistenza:

- Iscriversi alla newsletter sulla sicurezza Schneider Electric.
- Visitare la pagina Web Cybersecurity Support Portal per:
  - Trovare notifiche di sicurezza.
  - Segnalare vulnerabilità e incidenti.
- Visitare la pagina Web Schneider Electric Cybersecurity and Data Protection Posture per:
  - Accedere alla postura di sicurezza informatica.
  - Ulteriori informazioni sulla sicurezza informatica nell'accademia di sicurezza informatica.
  - Esplorare i servizi di sicurezza informatica di Schneider Electric.

Informazioni relative alla sicurezza informatica del prodotto

- La sicurezza di rete deve essere configurata correttamente. Il Gateway deve funzionare all'interno di una rete sicura ad accesso limitato. Se connesso a Internet, è fortemente consigliato utilizzare una **VPN** o un canale crittografato **HTTPS**.
- Accedere sempre al Gateway utilizzando un protocollo sicuro, ad esempio `https://<IP>:<Port>`.
- Il livello di sicurezza globale dipende dalle capacità di altri componenti di rete, quali i firewall e la protezione da virus e malware.
- I file di backup devono essere conservati in un luogo sicuro, inaccessibile a persone non autorizzate.
- Assicurarsi che il Gateway non abbia un indirizzo IP accessibile al pubblico.
- Evita di utilizzare il port forwarding per accedere al Gateway da Internet pubblico.
- Il Gateway deve essere posizionato su un segmento di rete dedicato per isolarlo da altri dispositivi.
- Se il router supporta reti guest o VLAN, si consiglia di collocare il Gateway all'interno di tale segmento per un ulteriore isolamento.

Per ulteriori informazioni sull'hardening del sistema, fare clic qui: https://www.se.com/ww/en/download/document/AN002_107/.

Lingue disponibili per il documento

Il documento è disponibile nelle seguenti lingue:

- **Inglese** (LSS100300_SW_EN)
- Cinese (LSS100300_SW_ZH)
- Francese (LSS100300_SW_FR)
- Tedesco (LSS100300_SW_DE)
- Italiano (LSS100300_SW_IT)
- Spagnolo (LSS100300_SW_ES)

Documenti correlati

Titolo della documentazione	Codice prodotto
Gateway IP BMS KNX SpaceLogic, LSS100300, Installazione e collegamento	LSS100300_HW
Wiser per KNX, SpaceLYnk - Linea guida per il rafforzamento del sistema	AN002_107

Come trovare documenti online:

1. Vai a www.se.com/ww/en/download/.
2. Nell'angolo in alto a sinistra, selezionare il proprio **Paese** dal menu a discesa.
3. Nella barra di ricerca, immettere il **nome documento** o **numero di riferimento**.
4. Fare clic sull'icona della lente di ingrandimento per avviare la ricerca.
5. Dai risultati della ricerca, selezionare la scheda **Documenti**.
6. **Aprire il documento** necessario dalla lista.

Informazioni sulla terminologia non inclusiva o non sensibile

In qualità di azienda responsabile e inclusiva, Schneider Electric aggiorna costantemente le sue comunicazioni e i suoi prodotti che contengono una terminologia non inclusiva o indelicata. Tuttavia, nonostante questi sforzi, i nostri contenuti possono ancora contenere termini ritenuti inappropriati da alcuni clienti.

Marchi

QR Code è un marchio registrato di DENSO WAVE INCORPORATED in Giappone e in altri paesi.

Introduzione

Gateway IP SpaceLogic KNX BMS (di seguito "Gateway") è un dispositivo multifunzionale progettato per integrare le installazioni KNX con i sistemi di automazione degli edifici.

Le sue interfacce di comunicazione primarie sono KNX TP e IP, con supporto per il protocollo **BACnet**.

Il Gateway combina tre componenti chiave in un unico dispositivo:

- router KNX IP (fino a 500 oggetti)
- interfaccia KNX IP
- bobina DPSU

Questa integrazione consente agli installatori professionisti di implementare i sistemi KNX in modo più efficiente in termini di costo e tempo, grazie alla combinazione di funzionalità in un'unica unità.

L'architettura del sistema è semplificata, poiché non è più necessario utilizzare router KNX e alimentatori KNX separati, a condizione che l'installazione rispetti i parametri specificati.

Il Gateway è destinato all'uso in impianti commerciali.

Accesso remoto sicuro tramite VPN

Quando si accede a un'installazione KNX tramite Internet, il traffico dati può essere esposto a terze parti. Per garantire una comunicazione sicura, adottare le seguenti precauzioni:

- Utilizzare sempre una connessione VPN (Virtual Private Network) con crittografia avanzata per proteggere tutti i pacchetti di dati.
- L’hardware richiesto (ad esempio un router VPN) e le capacità dei fornitori di servizi mobili possono variare significativamente a seconda del Paese o della regione.
- L’accesso VPN deve essere sempre configurato e messo in servizio da un provider di servizi VPN qualificato. Il provider selezionerà l’hardware appropriato e un provider di servizi mobili adeguato e garantirà che la VPN sia configurata da uno specialista certificato.

Schneider Electric non è responsabile di problemi di prestazioni o incompatibilità causati da applicazioni, servizi o dispositivi di terze parti. Inoltre, Schneider Electric non fornisce supporto tecnico per la configurazione VPN.

Il mancato rispetto di queste linee guida può provocare danni all'apparecchiatura.

Una VPN consente a un dispositivo remoto di accedere in modo sicuro alla rete locale – e quindi all'installazione KNX – tramite Internet.

Vantaggi dell'uso di una VPN

- Solo gli utenti autorizzati possono accedere alla rete locale.
- Tutti i dati vengono crittografati durante la trasmissione.
- I dati rimangono intatti e protetti da intercettazioni, manipolazioni o reindirizzamenti, comunemente definiti tunnel VPN.

Requisiti per la configurazione di una connessione VPN

- Una connessione Internet attiva.

- Un dispositivo portatile e un router che supportano le connessioni VPN (con un client VPN installato).
- Il Gateway deve essere posizionato su un segmento di rete dedicato.
- Se il router supporta reti guest o VLAN, si consiglia di inserire il Gateway in tale segmento.

Migliori pratiche per la sicurezza delle password

- La password deve includere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.
- Utilizzare un minimo di 8 caratteri.
- Scegliere password difficili da indovinare o trovare nei dizionari utilizzati dai cybercriminali.
- Preferire passphrase anziché parole singole.
- Modificare la password regolarmente, almeno una volta all'anno.
- Cambiare sempre la password amministratore predefinita immediatamente dopo averla ricevuta o dopo aver eseguito un ripristino alle impostazioni di fabbrica.
- Non riutilizzare mai password tra account o sistemi diversi.

Specifiche dispositivo

Specifiche	Descrizione	Note
Terminali, interfaccia	1 × RJ45 – ethernet 10BaseT/100BaseTx 1 × KNX TP 1 × Pulsante di reset	
Connettività	Connessione LAN IP 10/100 Mbit Bus TP KNX/EIB	
Indicatori LED	2 × LED, CPU, (Funzionamento + Ripristino)	
Routing IP KNX	500 oggetti (disabilitati automaticamente quando supera questo limite)	È possibile utilizzare fino a 4000 punti BACnet. Vedere Prestazioni, pagina 16.
Tunneling IP KNX	Per la messa in servizio dei dispositivi KNX tramite ETS	
Limitazione KNX TP	Il mezzo KNX TP ha una larghezza di banda limitata 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	
BACnet Revisione protocollo	22	
BACnet Profilo dispositivo	B – ASC, B – GW	

Compatibilità

Il Gateway è compatibile con i seguenti standard:

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

Prestazioni

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

*BACnet Il supporto COV garantisce una comunicazione dati rapida riducendo il BACnet traffico di rete.

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

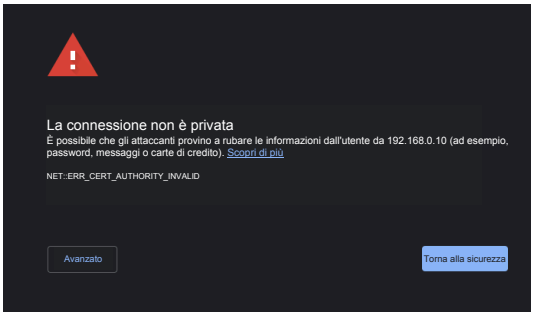
Guida rapida

Prima di iniziare, verificare che il Gateway sia collegato correttamente in base alle istruzioni di installazione.

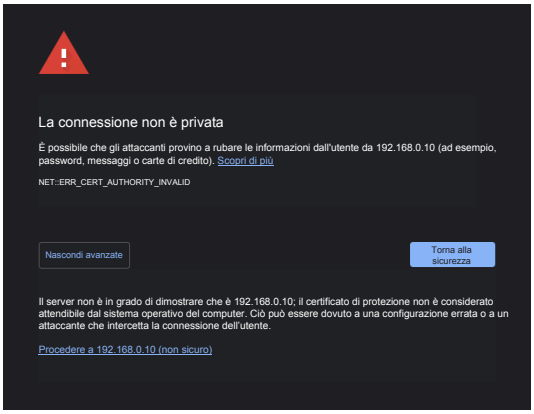
Per configurare il Gateway, è necessario un browser web standard. Si consiglia di utilizzare Google Chrome o Mozilla Firefox per la migliore esperienza di utilizzo.

Primo accesso:

1. Aprire il browser e immettere l'indirizzo IP predefinito: 192.168.0.10. Premere **Invio**.
2. Poiché il Gateway utilizza un certificato autofirmato, è probabile che il browser visualizzi un avviso che segnala che la connessione non è privata.



3. Procedere comunque facendo clic su **Avanzate**, quindi procedere a 192.168.0.10. Il Gateway utilizza HTTPS per garantire la comunicazione crittografata tra il browser e il dispositivo.



4. Accedere utilizzando le credenziali predefinite e fare clic su **Invio**.

   login: `admin`

   password: `admin`

5. Verrà chiesto di modificare la password (Migliori pratiche per la sicurezza delle password, pagina 13). Immettere una nuova password e fare clic su **Salva**.

   La nuova password deve includere almeno:

   - 8 caratteri
   - Una lettera maiuscola
   - Una lettera minuscola
   - Una cifra

6. Dopo l'accesso, verrà visualizzata la pagina iniziale:

Qui è possibile:

- Selezionare la lingua preferita (angolo in alto a destra)
- Accedere alle impostazioni del Gateway tramite
- Utilizzare strumenti e filtri oggetto
- Fare clic sul pulsante **Importa progetto KNX**

Nei passi successivi, si importa il progetto di KNX e si configurano i parametri del dispositivo.

Importazione di un progetto KNX

Il pulsante **Importa progetto KNX** nell'angolo in alto a sinistra dell'interfaccia, consente di caricare un `.knxproj` file direttamente sul Gateway. Il processo di importazione preserva:

- La struttura del progetto
- DPT (Data Point Types) degli indirizzi di gruppo
- Unità e suffissi

NOTA: Gli oggetti con nomi identici vengono trattati come duplicati e possono essere eliminati durante l'importazione.

È inoltre possibile importare oggetti senza tipi di dati predefiniti e assegnare loro nomi a livello di struttura, se necessario.

Se il file `.knxproj` è protetto da password, è necessario immettere la password impostata in ETS. Il progetto non può essere importato senza di essa.

Gestione dei dispositivi KNX Secure

Durante l'importazione, il Gateway preserva l'**identificazione dei dispositivi KNX Secure** inclusi nel progetto. Questo influisce sul modo in cui il Gateway elabora i telegrammi.

- I **telegrammi protetti** provenienti da dispositivi protetti vengono accettati solo su indirizzi di gruppo protetti.
- **Telegrammi non protetti** inviati a **indirizzi di gruppo protetti** sono **rifiutati** dal Gateway per motivi di sicurezza.
- Su **indirizzi di gruppo non protetti**, il Gateway accetta telegrammi provenienti da **qualsiasi sorgente non protetta**.

Ciò garantisce che la comunicazione sicura rimanga protetta consentendo al contempo la comunicazione aperta su canali non sicuri.

Come importare un progetto KNX

1. Fare clic sul pulsante **Importa progetto KNX** e selezionare il `.knxproj` file.
2. Se richiesto, immettere la password corretta.
3. (Opzionale) Spuntare l'opzione **Aggiungi nomi di livello agli oggetti** se si desidera includere i nomi degli oggetti e le rispettive posizioni nella struttura.
4. (Opzionale) Spuntare **Sovrascrivi oggetti esistenti** per sostituire eventuali oggetti esistenti nel Gateway.
5. Per abilitare la comunicazione sicura con i dispositivi KNX Secure, si consiglia di selezionare l'opzione **Importa chiavi di sicurezza**. Questo passaggio è fondamentale, in quanto consente al Gateway di importare le chiavi di crittografia necessarie direttamente dal progetto ETS. Questi tasti sono collegati a indirizzi di gruppo specifici, consentendo al gateway di interpretare e integrare correttamente i telegrammi di KNX con le informazioni di sicurezza necessarie per il corretto funzionamento.
6. (Opzionale) Selezionare **Crea automaticamente una tabella di filtro in base ai dati del progetto** per consentire al Gateway di generare una tabella di filtro utilizzando gli indirizzi di gruppo importati. Ciò consente di ottimizzare le prestazioni e la sicurezza consentendo l'elaborazione solo degli indirizzi di gruppo pertinenti.

7. (Opzionale) Selezionare **Imposta criteri di filtro su Accetta indirizzi di gruppo selezionati** per garantire che solo gli indirizzi di gruppo definiti nel progetto vengano accettati dal Gateway.
8. Fai clic su **Avanti** per procedere.

Una volta importate, le tabelle di filtro vengono compilate automaticamente in base al progetto KNX e possono essere adattate secondo necessità. Anche la chiave dorsale viene importata automaticamente.

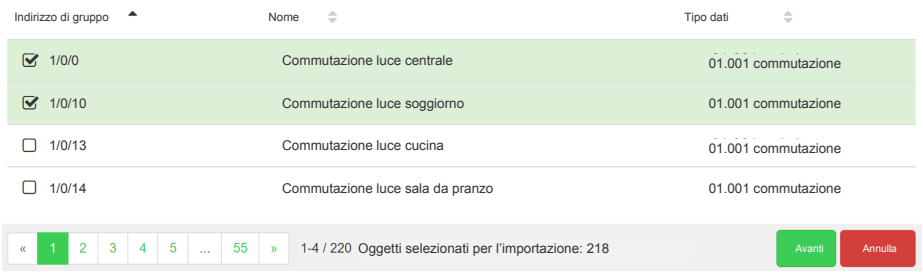
NOTA: Il routing KNX non è supportato per progetti contenenti più di 500 oggetti.

Selezione degli oggetti per l’esportazione BACnet

Nel passo successivo, sceglierai quali oggetti di KNX importare nel Gateway. Solo gli oggetti selezionati verranno aggiunti al database del Gateway.

È possibile filtrare gli oggetti per nome, indirizzo di gruppo o tipo di dati per semplificare la selezione. Per maggiori dettagli, vedere Filtraggio e modifica delle proprietà dell'oggetto, pagina 23.

1. Selezionare gli oggetti da esportare e fare clic su **Avanti**.



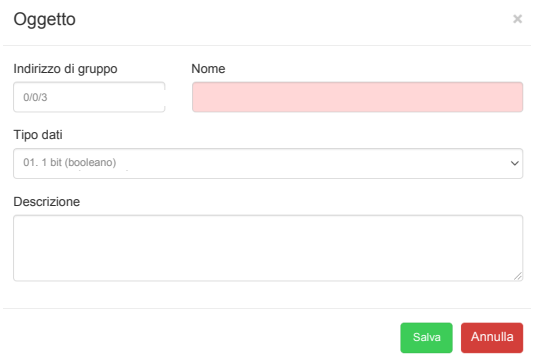
2. Una finestra popup conferma il numero di oggetti importati.
3. Fare clic su **OK** per completare il processo di importazione.

Aggiungere un oggetto

La funzione **Aggiungi oggetto** è utile quando si desidera aggiungere manualmente un singolo oggetto senza reimportare l'intero `.knxproj` file.

Per aggiungere un nuovo oggetto:

1. Fare clic sul pulsante **Aggiungi oggetto**.



2. Specificare i dettagli dell'oggetto richiesti, ad esempio nome, indirizzo di gruppo, tipo di dati ed eventuali parametri aggiuntivi.
3. Fare clic su **Salva** per confermare e aggiungere l'oggetto all'elenco.

Azioni

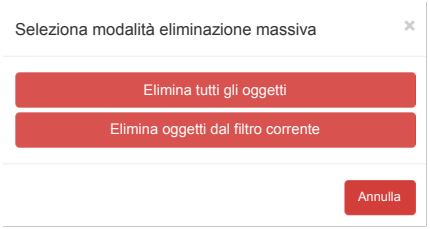
Eliminazione di massa di oggetti

La funzione **Eliminazione di massa** consente di rimuovere rapidamente più oggetti dal database del Gateway con un'unica azione.

È possibile scegliere tra due opzioni:

- **Elimina tutti gli oggetti** – rimuove ogni oggetto dal database.
- **Elimina oggetti dal filtro corrente** – rimuove solo gli oggetti correntemente visualizzati in base alle impostazioni del filtro.

Dopo aver selezionato l'opzione desiderata, il sistema procederà a eliminare gli oggetti di conseguenza.



SUGGERIMENTO: Utilizzare i filtri per restringere la selezione prima di utilizzare l'eliminazione di massa, in particolare se si desidera rimuovere solo gruppi specifici di oggetti.

Modifica di massa di oggetti

La funzione **Modifica di massa** consente di aggiornare rapidamente le unità e l'incremento COV (Change of Value) per più oggetti contemporaneamente.

Per modificare gli oggetti in blocco:

1. Usare il filtro per visualizzare gli oggetti da modificare.
2. Fare clic su **Azioni** > selezionare **Modifica di massa** dal menu a discesa.
3. Scegliere i parametri da aggiornare:
   - **Unità**
   - **Valore di incremento COV**
4. Fare clic su **Salva** per applicare le modifiche a tutti gli oggetti selezionati.

Esportazione di oggetti in CSV

È possibile esportare facilmente tutti gli oggetti in un file `.csv` per ulteriore analisi o conservazione dei documenti.

Per esportare:

1. Fare clic su **Azioni**.
2. Selezionare **Esporta in CSV** dal menu a discesa.

Il file `.csv` verrà scaricato automaticamente nella cartella **Download** sul computer. È possibile aprirlo utilizzando Microsoft Excel o qualsiasi altra applicazione per fogli di calcolo per visualizzare e utilizzare i dati.

SUGGERIMENTO: Utilizzare i filtri prima dell'esportazione se si desidera includere solo oggetti specifici nel file.

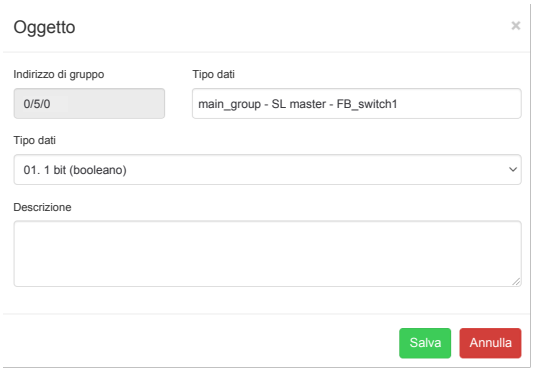
Filtraggio e modifica delle proprietà dell'oggetto

È possibile filtrare e gestire facilmente gli oggetti utilizzando vari criteri, ad esempio **nome**, **indirizzo gruppo**, oppure **tipo di dati**. È sufficiente digitare il termine da cercare o selezionare dal menu a discesa per restringere l'elenco.

Una volta filtrato, è possibile modificare le proprietà dell'oggetto, aggiornare i valori o eliminare gli oggetti singolarmente in base alle esigenze.

Per modificare le proprietà dell'oggetto:

1. Fare clic su .
2. Modificare le proprietà desiderate nella finestra popup.
3. Fare clic su **Salva** per applicare le modifiche.



Per impostare il valore di un oggetto:

1. Fare clic su .
2. Scegliere un valore dall'elenco a discesa **Valore**.
3. Fare clic su **Conferma** per confermare.

Per eliminare un oggetto:

1. Fare clic su .
2. Confermare l'eliminazione facendo clic su **Sì** nella finestra di conferma.

Panoramica delle impostazioni dell'applicazione

Dopo aver configurato l'interfaccia utente e importato il progetto ETS, è possibile configurare i parametri del Gateway in base alle esigenze di installazione.

Dal menu principale si accede ai seguenti strumenti e impostazioni:

- **Backup**: Salvare la configurazione corrente per un ripristino futuro.
- **Ripristina**: Caricare una configurazione salvata in precedenza.
- **Cambia password**: Aggiornare le credenziali di accesso per una maggiore sicurezza.
- **Nome host**: Impostare un nome personalizzato per il Gateway nella rete.
- **Configurazione BACnet**: Regolare le impostazioni specifiche del BACnet.
- **Configurazione KNX**: Gestire i parametri correlati a KNX.
- **Configurazione di rete**: Impostare indirizzo IP, subnet, gateway e DNS.
- **Configurazione server HTTP**: Personalizzare le impostazioni del server web.
- **Certificato SSL HTTP**: Caricare o gestire il certificato HTTPS.
- **Configurazione client NTP**: Sincronizzare l'ora utilizzando un server dell'ora di rete.
- **Data e ora**: Impostare o regolare manualmente l'orologio di sistema.
- **Registro di sistema**: Visualizzare i registri di attività e diagnostica del sistema.
- **Ping**: Verificare la connettività di rete ad altri dispositivi.
- **Attiva/disattiva identificazione dispositivo**: Attivare l'identificazione visiva (ad es., LED)
- **Aggiorna firmware**: Installare la versione firmware più recente.
- **Ripristino delle impostazioni di fabbrica**: Ripristinare il Gateway alle impostazioni predefinite.
- **Reboot**. Riavviare il dispositivo.
- **Arresto**: Spegnere il Gateway in sicurezza.

Creazione di un backup

La creazione di un backup consente di salvare una copia della configurazione del Gateway, che può essere ripristinata in un secondo momento in caso di perdita di dati o guasto del sistema.

Come creare un backup:

1. Aprire il menu principale facendo clic su  .
2. Selezionare l'opzione **Backup** dall'elenco a discesa.

Il file di backup verrà scaricato automaticamente nella cartella **Download** del browser.

Formato nome file di backup:

```
[Hostname]-backup-[YYYY.MM.DD]-[HH.MM].bckp
```

Il nome file include il nome host del Gateway e la data e l'ora esatte in cui è stato creato il backup. È possibile rinominare il file e spostarlo in un'altra cartella per conservarlo.

SUGGERIMENTO: Archiviare i file di backup in un percorso sicuro ed evitare di condividerli con utenti non autorizzati.

Ripristino di un backup

La funzione **Ripristina** consente di ripristinare i dati del Gateway da un backup salvato in precedenza. Ciò è utile se i dati sono andati persi, sono danneggiati o se occorre trasferire le impostazioni a un nuovo dispositivo.

Per ripristinare i dati:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Ripristina** dall'elenco a discesa.
3. Fare clic su**Scegli file** e individuare il file di backup sul computer.
4. (Opzionale) Se si desidera ripristinare anche i file di configurazione, selezionare l'opzione **Ripristina file di configurazione**.

5. Fare clic su **Salva** per avviare il processo di ripristino.

Dopo aver fatto clic su **Salva**, viene visualizzata una finestra popup che chiede se si desidera riavviare il sistema:

- Fare clic su **Sì** per riavviare e completare il ripristino.
- Fare clic su **No** per annullare l'operazione. Se si sceglie **No**, non verranno importati dati.

  SUGGERIMENTO: Verificare sempre che si stia ripristinando il file di backup corretto per evitare di sovrascrivere dati importanti.

Modifica della password

Per garantire la sicurezza del Gateway, è importante aggiornare regolarmente la password.

Procedere come segue per modificarla:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Cambia password** dal menu.
3. Immettere la password corrente, quindi digitare la nuova password.
4. Fare clic su **Salva** per confermare la modifica.

Modifica del nome host del Gateway

Il nome host è il nome univoco assegnato al Gateway nella rete. Aiuta a identificare facilmente il dispositivo, in particolare quando si gestiscono più installazioni. Il nome host è utilizzato anche nel nome file dei file di backup, facilitando il tracciamento e l'organizzazione dei file.

Perché cambiare il nome host?

- Per identificare chiaramente il Gateway nella rete.
- Per personalizzare il nome del dispositivo per facilitarne la gestione.
- Per rendere i file di backup più riconoscibili (ad esempio,`Office1-backup-2025.05.23-14.30.bckp`).

Come modificare il nome host:

1. Aprire il menu principale facendo clic su  .
2. Selezionare **Nome host** dal menu.
3. Inserire il nome host desiderato.
   - Utilizzare solo lettere, numeri e trattini.
   - Evitare spazi o caratteri speciali.
   - Sceglierlo breve e descrittivo (ad es. `Lobby-Gateway`,`KNX-BMS-01`).
4. Fare clic su **Salva** per applicare le modifiche.

   NOTA: La modifica del nome host non influisce sull'indirizzo IP o sulla configurazione di rete. Tuttavia, potrebbe essere necessario un riavvio per visualizzare il nuovo nome in alcuni tool di rete o log.

Configurazione BACnet

Il Gateway funziona come server BACnet, consentendo la comunicazione tra gli oggetti di gruppo KNX e i dispositivi client BACnet. Ciò consente l'integrazione perfetta dei sistemi di automazione degli edifici in diverse piattaforme.

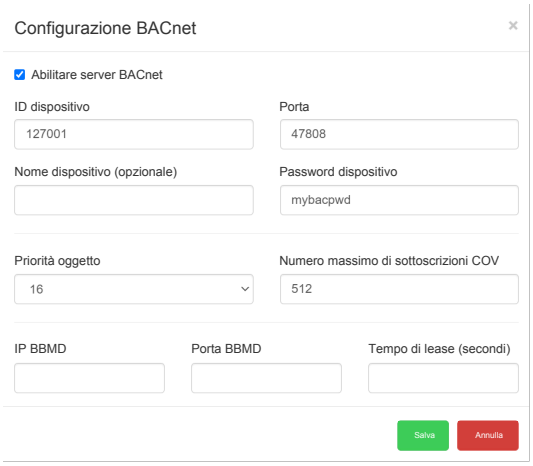
BACnet (Building Automation and Control Network) è un protocollo standardizzato utilizzato per lo scambio di dati tra dispositivi nei sistemi di automazione degli edifici, indipendentemente dalla loro funzione specifica (ad es. illuminazione, HVAC, sicurezza). Il Gateway si collega alla rete BACnet tramite l'interfaccia Ethernet e fornisce dati provenienti dagli oggetti di gruppo KNX esportati su BACnet.

- Gli oggetti KNX binari sono mappati come valori binari in BACnet.
- Gli oggetti numerici KNX sono mappati come valori analogici.
- Gli altri tipi di dati non sono supportati.

Come configurare le impostazioni BACnet:

1. Aprire il menu principale facendo clic su  .

2. Selezionare **Configurazione BACnet** dal menu.



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

Parametro	**Note**
Abilitare server BACnet	Attiva o disattiva la funzionalità BACnet. Disattivato per impostazione predefinita.
ID dispositivo	Identificatore univoco del Gateway sulla rete BACnet. Non deve essere in conflitto con altri dispositivi.
Porta	Porta di comunicazione per BACnet. Il valore predefinito è 47808.
Nome dispositivo (opzionale)	Nome personalizzato del dispositivo. Se lasciato vuoto, il valore predefinito è `hostname_DeviceID`.
Password dispositivo	Password opzionale per i servizi BACnet come `DeviceCommunicationControl` e `ReInitializeDevice`. Se non è impostata, non viene utilizzata alcuna password.
Priorità oggetto	Imposta la posizione predefinita nell'array delle priorità per gli oggetti BACnet.
Numero massimo di sottoscrizioni COV	Numero massimo di sottoscrizioni COV (Change of Value). Il valore predefinito è 4000. Vedere Prestazioni, pagina 16 per ulteriori informazioni.
IP BBMD	Indirizzo IP del dispositivo di gestione delle trasmissioni BACnet (BBMD), se utilizzato.
Porta BBMD	Porta utilizzata dal BBMD.
Tempo di lease (secondi)	Intervallo per rinnovo registrazione BBMD.

SUGGERIMENTO: Accertarsi che l'ID dispositivo sia univoco nella rete BACnet per evitare conflitti di comunicazione.

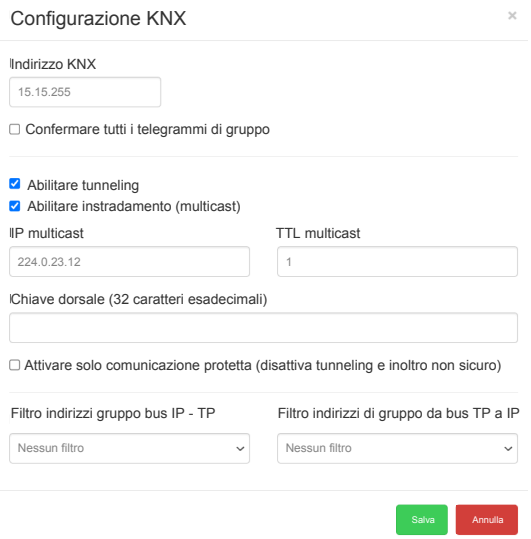
Configurazione KNX

Il menu **Configurazione KNX** consente di configurare il Gateway quando viene utilizzato come **Interfaccia KNX IP** o **router**.

Per accedere e configurare le impostazioni, procedere come segue:

1. Aprire il menu principale facendo clic su .

2. Selezionare la **Configurazione KNX** dal menu.



3. Regolare i seguenti parametri in base alle esigenze, quindi fare clic su **Salva** per applicare le modifiche.

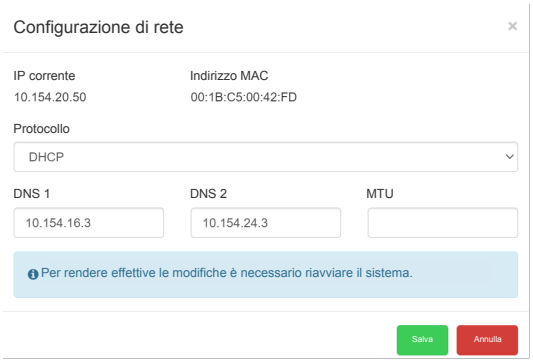
Parametro	**Note**
Indirizzo KNX	L'indirizzo KNX individuale del dispositivo. Predefinito: 15.15.255.
Confermare tutti i telegrammi di gruppo	Attivare questa opzione se il Gateway comunica direttamente con altri dispositivi KNX e deve riconoscere i telegrammi ricevuti. Disattivare se il Gateway controlla solo indirizzi di gruppo (modalità sniffer).
Abilitare il tunneling	Consente a più dispositivi di condividere un indirizzo IPv4 pubblico modificando le intestazioni IP durante la trasmissione. Questo consente una comunicazione IP più rapida (fino a 1000 volte più veloce rispetto a TP-UART). Il Gateway funge da server utilizzando unicast e lo scambio di dati riconosciuti. Ogni connessione di tunneling richiede un indirizzo individuale univoco.
Abilitare instradamento (multicast)	Abilita il trasferimento dati basato su multicast, senza conferma. Il Gateway funziona come accoppiatore di linea o dorsale.
IP multicast	L'indirizzo IP multicast utilizzato per l'instradamento. Predefinito: 224.0.23.12.
TTL multicast	Valore time-to-live per pacchetti multicast. Predefinito: 1. Ciò consente la comunicazione tra sottoreti.
Chiave dorsale (32 caratteri esadecimali)	Chiave esadecimale a 32 caratteri utilizzata per criptare e decriptare i telegrammi sicuri nell'instradamento IP.
Abilitare solo comunicazioni sicure	Se attivato, è consentita solo la comunicazione sicura. Il tunneling e l'instradamento non sicuro sono disabilitati.
Filtro indirizzi gruppo bus IP - TP	Nessun filtro
Filtro indirizzi di gruppo da bus TP a IP	Accetta gli indirizzi di gruppo selezionati Elimina gli indirizzi di gruppo selezionati Esempi di immissione filtro: • Indirizzo singolo (1/1/1) • Intervallo (1/1/1-1/1/100) • Wildcard (1/1/* o 1/*/*)

Configurazione della rete

La configurazione di rete prevede la configurazione di controlli e parametri che gestiscono la modalità di comunicazione del dispositivo su una rete. Dopo l'aggiornamento delle impostazioni di rete, è necessario riavviare il sistema per rendere effettive le modifiche.

Accesso alla configurazione di rete:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Configurazione di rete**.



3. Regolare i seguenti parametri di rete in base alle esigenze, quindi fare clic su **Salva** per applicare le modifiche:

Parametro	Note
IP corrente	La configurazione di rete prevede la configurazione di controlli e parametri che gestiscono la modalità di comunicazione del dispositivo su una rete. Dopo l'aggiornamento delle impostazioni di rete, è necessario riavviare il sistema per rendere effettive le modifiche.
Indirizzo MAC	Un identificativo hardware univoco assegnato al dispositivo.
Protocollo	Protocollo specifico utilizzato per l'indirizzamento: IP statico: Assegnare manualmente un indirizzo IP. DHCP: Ottenere automaticamente un indirizzo IP dalla rete.
Indirizzo IP	Indirizzo IP del dispositivo. Predefinito: 192.168.0.10.
Maschera di rete	Definisce la sottorete. Predefinito: 255.255.255.0.
IP gateway	L'indirizzo IP del gateway di rete. Predefinito: Nessuno.
DNS 1	Indirizzo IP del server DNS primario.
DNS 2	Indirizzo IP del server DNS secondario.
MTU	Maximum Transmission Unit (Unità di trasmissione massima): la massima dimensione di pacchetto che può essere inviato. Predefinito: 1500.

Dopo aver salvato la configurazione, viene visualizzata una finestra di conferma. Fare clic su **Sì** per riavviare il sistema e applicare le nuove impostazioni.

Configurazione server HTTP

In questa sezione è possibile configurare il livello di sicurezza della comunicazione del Gateway con il server web e impostare porte HTTP/HTTPS aggiuntive.

Procedura di configurazione del server HTTP

1. Aprire il menu principale facendo clic su .

2. Selezionare **Configurazione server HTTPS**.

3. Regolare i parametri elencati di seguito e fare clic su **Salva**.
4. Riavviare il sistema per rendere effettive le modifiche.

Parametri del server HTTPS

Parametro	Nota
Modalità HTTPS	Scegliere la modalità di sicurezza desiderata: **HTTP e HTTPS abilitati**: Sono consentite comunicazioni sicure e non sicure. **solo HTTPS, reindirizzare a HTTPS**: Tutto il traffico HTTP viene reindirizzato automaticamente a HTTPS per una comunicazione sicura. **Solo HTTPS, porta HTTP disabilitata**: È consentita solo la comunicazione HTTPS sicura. HTTP è completamente disattivato.
Porta HTTP aggiuntiva	Opzionale: Specificare una porta HTTP aggiuntiva. Il valore predefinito è 80.
Porta HTTPS aggiuntiva	Opzionale: Specificare una porta HTTPS aggiuntiva. Il valore predefinito è 443.

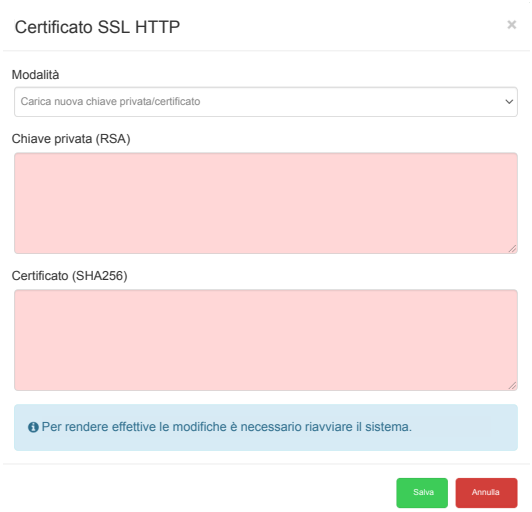
Certificato SSL HTTP

I certificati SSL sono file digitali che collegano in modo sicuro una chiave di crittografia all'identità di un dispositivo. Se installati su un server web, abilitano le connessioni HTTPS sicure e attivano l'icona a forma di lucchetto nel browser.

Come configurare un certificato SSL:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Certificato SSL HTTP** dal menu.
3. Selezionare la **Modalità** desiderata:
   - **Carica nuova chiave privata/certificato**: Utilizzare questa opzione per caricare una chiave privata RSA esistente e un certificato SSL.
   - **Genera nuova chiave privata/certificato**: Utilizzare questa opzione per generare una nuova chiave RSA e un certificato SSL in base a quello attualmente installato.

4. Fare clic su **Salva** per applicare le modifiche.



5. Riavviare il sistema per rendere effettive le nuove impostazioni del certificato.

Configurazione client NTP

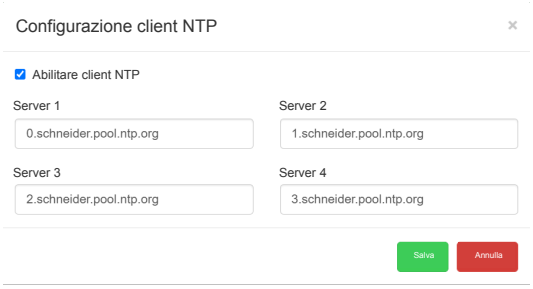
Il client NTP (Network Time Protocol) garantisce che il Gateway rimanga sincronizzato con l'ora UTC (Coordinated Universal Time), mantenendo un'ora precisa su tutti i dispositivi collegati. Compensa i ritardi di rete per garantire una sincronizzazione temporale precisa.

Funzioni chiave:

- Sincronizza l'orologio interno del Gateway con fino a **4 server NTP**, con priorità da 1 a 4.
- Contribuisce a garantire timestamp accurati per registri, eventi e comunicazione dati.

Come configurare il client NTP:

1. Aprire il menu principale facendo clic su .
2. Navigare in **Configurazione client NTP**.
3. Immettere gli indirizzi IP o i nomi di dominio di un massimo di quattro server NTP, in ordine di priorità.
4. Fare clic su **Salva** per applicare le impostazioni.



5. Riavviare il sistema per attivare la nuova configurazione.

   SUGGERIMENTO:

   - Se non si è sicuri della raggiungibilità di un server NTP, utilizzare il **ping tool** per verificarne la disponibilità.
   - Per ottenere risultati ottimali, utilizzare server NTP affidabili e geograficamente vicini.

Data e ora

Il Gateway utilizza il protocollo NTP (Network Time Protocol) per sincronizzare automaticamente il proprio orologio interno con un server dell'ora basato su Internet. Ciò assicura un'accurata gestione del tempo senza l'immissione manuale.

Come impostare la data e l'ora:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Data e ora** dal menu.
3. Se il Gateway non è connesso a Internet, fare clic su **Ottieni dal sistema** per sincronizzare l'ora con il PC.
4. Scegliere il fuso orario dall'elenco.
5. Fare clic su **Salva** per applicare le impostazioni.

Registro di sistema

Il **Registro di sistema** fornisce una registrazione cronologica di eventi chiave nel Gateway, quali:

- Avvii del sistema
- Disconnessione TP/KNX

Questi eventi vengono registrati automaticamente dal Gateway in un formato semplice e di facile lettura.

Come visualizzare il registro di sistema:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Registro di sistema** dal menu.

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

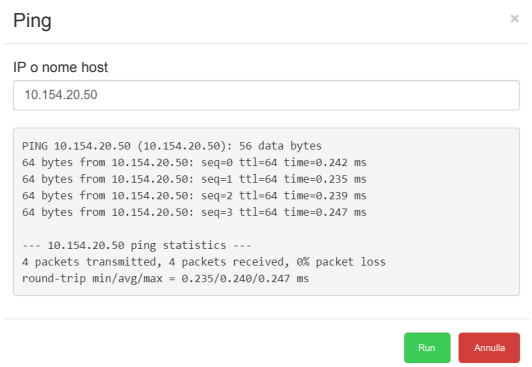
Nella parte inferiore della schermata di registro è inoltre possibile visualizzare **Carico CPU**, che fornisce informazioni sull'attività di elaborazione corrente del Gateway.

Ping

Il tool **Ping** consente di verificare se un dispositivo o un server specifico è raggiungibile su una rete IP. Misura il **tempo di andata e ritorno** per i pacchetti dati inviati dal Gateway all'host di destinazione e viceversa.

Come usare il tool **Ping**:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Ping** dal menu.
3. Immettere l'indirizzo IP o il nome host del dispositivo da testare.
4. Fare clic su **Run** per avviare il test ping.



I risultati mostreranno il tempo di risposta, aiutando a determinare se la destinazione è raggiungibile e la sua rapidità di risposta.

Attiva/disattiva identificazione dispositivo

La funzione **Attiva/disattiva identificazione dispositivo** permette di localizzare un dispositivo Gateway specifico sulla rete attivando un segnale visivo.

Come funziona:

Quando l'identificazione è attivata, **LED 2** sul dispositivo selezionato lampeggia in **rosso e verde**, il che facilita l'individuazione del dispositivo.

Come usarlo:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Attiva/disattiva identificazione dispositivo** dal menu.
3. Osservare il dispositivo: il LED 2 deve iniziare a lampeggiare per indicare la sua posizione.

Questa funzione è particolarmente utile quando si gestiscono più dispositivi in un ambiente di rete.

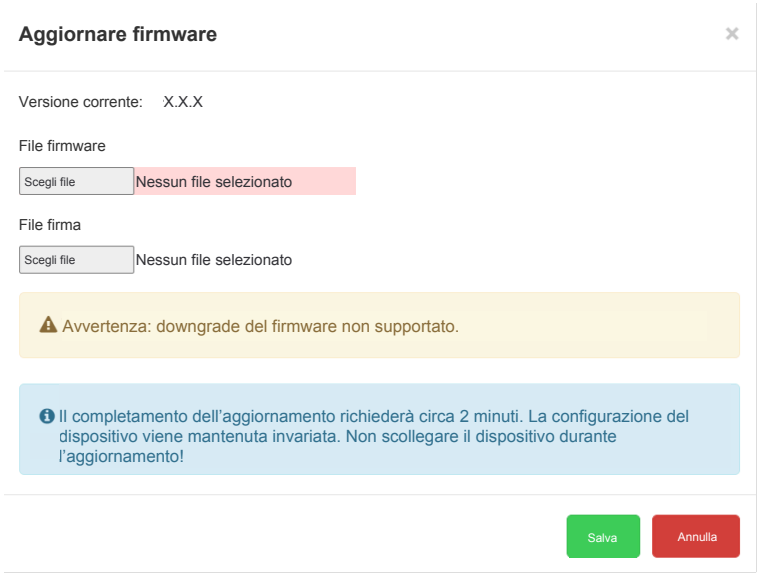
Aggiornamento firmware

L'aggiornamento del firmware aggiorna il Gateway con le funzioni e i miglioramenti più recenti, senza modificare la configurazione esistente o richiedere modifiche hardware.

IMPORTANTE: Non scollegare il Gateway durante la procedura di aggiornamento. Il dispositivo verrà riavviato più volte e **il LED 1 lampeggerà in rosso e verde** per indicare che l'aggiornamento è in corso.

Come aggiornare il firmware

1. Aprire il menu principale facendo clic su .
2. Selezionare **Aggiornamento firmware** dal menu.
3. Scegliere il file del firmware da installare.
4. Selezionare il file di firma corrispondente (necessario per la convalida).
5. Fare clic su **Salva** per iniziare l'aggiornamento.



Dopo l'aggiornamento

- Il Gateway si riavvia automaticamente.
- È **fortemente raccomandato** di **cancellare la cache del browser** dopo l'aggiornamento per evitare problemi di visualizzazione.
- I downgrade del firmware non sono supportati.

  NOTA: Un **file di firma** valido è richiesto per ogni aggiornamento del firmware. I pacchetti firmware sono sempre distribuiti con i file di firma corrispondenti.

Ripristino delle impostazioni di fabbrica

Un ripristino delle impostazioni di fabbrica cancella tutti i dati e le impostazioni del Gateway e ripristina il suo stato originale. Questa azione è irreversibile, quindi utilizzarla con cautela.

È possibile eseguire un ripristino alle impostazioni di fabbrica in due modi:

- **Tramite l'applicazione**: Usare l'interfaccia software per avviare un ripristino dal menu Impostazioni.
- **Utilizzando il pulsante di ripristino hardware**: Premere e tenere premuto il pulsante di ripristino fisico sul dispositivo per attivare un ripristino manualmente.

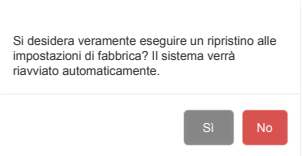
Ripristino delle impostazioni di fabbrica dell'applicazione

È possibile ripristinare il Gateway alle impostazioni di fabbrica direttamente tramite l'applicazione. Questo processo cancella tutte le configurazioni utente e ripristina il dispositivo allo stato originale.

NOTA: Con un ripristino delle impostazioni di fabbrica si cancellano tutte le impostazioni e le configurazioni personalizzate. Utilizzare questa opzione solo quando necessario.

Come eseguire un ripristino delle impostazioni di fabbrica tramite l'applicazione:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Ripristino delle impostazioni di fabbrica** dal menu.
3. Confermare il ripristino quando richiesto. Il sistema si riavvia automaticamente.



Parametri dispositivo dopo il ripristino:

Parametro	Risultato
Nome dispositivo	LSS100300
Indirizzo IP	Preservato (rimane invariato)
Nessun oggetto	Cancellato (la configurazione BACnet/KNX viene rimossa)

Ripristino delle impostazioni di fabbrica dell'hardware

Il ripristino delle impostazioni di fabbrica dell'hardware è utile quando il Gateway diventa inaccessibile a causa di impostazioni non corrette o problemi di configurazione della rete.

Quando utilizzarlo:

- Il Gateway non risponde.
- Non è possibile accedere all'interfaccia web.
- Le impostazioni di rete impediscono la connessione.

Come eseguire un ripristino dell'hardware:

1. Individuare il tasto **RESET** rosso sul dispositivo.

2. Seguire una delle seguenti procedure di ripristino:

Azione	Risultato
Tenere premuto il pulsante per **meno di 10 secondi**	Riavvia il dispositivo (nessuna impostazione viene modificata).
Tenere premuto il pulsante per **più di 10 secondi**	Ripristina solo le **impostazioni di rete**. L'indirizzo IP viene ripristinato ai valori predefiniti di fabbrica: 192.168.0.10.
Premere e tenere premuto per **più di 10 secondi**, rilasciare, quindi premere e tenere premuto di nuovo per **più di 10 secondi**	Esegue un **ripristino delle impostazioni di fabbrica completo**, ripristinando tutte le impostazioni ai valori predefiniti.

NOTA: Un ripristino completo cancellerà tutte le configurazioni, comprese le impostazioni BACnet e KNX.

Reboot

Se il Gateway non risponde come previsto, è possibile eseguire un **reboot** per riavviare il sistema.

Il riavvio arresta il dispositivo e lo riaccende, senza influire sulla configurazione o sui dati.

Come riavviare il Gateway:

1. Aprire il menu principale facendo clic su .
2. Selezionare **Reboot** dal menu.
3. Quando richiesto, fare clic su **Sì** per confermare.

Il Gateway si riavvierà automaticamente. Questo processo richiede in genere alcuni minuti.

Arresto e riavvio del Gateway

L'attivazione della modalità di sospensione del Gateway garantisce il completamento sicuro di tutte le operazioni sui dati, mantenendo la stabilità del sistema e prevenendo perdite o danneggiamenti dei dati.

IMPORTANTE: Non scollegare l'alimentazione finché il LED 2 non si spegne.

Passaggio alla modalità di sospensione

Per arrestare il Gateway in sicurezza:

1. Aprire il menu principale facendo clic sull'icona del menu .
2. Selezionare **Shutdown** (Arresto).
3. Confermare facendo clic su **Sì**.

Cosa accade durante la modalità di sospensione

Il Gateway entra in una **Modalità sospensione di 3 minuti**. Durante questo periodo:

- Il LED 1 (verde) si **spegne**.
- Il LED 2 (verde) si **spegne**.

- Il Gateway **non risponde alla comunicazione di rete**.

Se il dispositivo **non è scollegato** dall'alimentazione durante questo periodo, **si riavvia automaticamente**.

Riavvio manuale del Gateway

Per riavviare manualmente il Gateway:

- scollegare e ricollegare l'alimentazione dopo che il **LED 2** si spegne.
- Il Gateway **non** dispone di un pulsante di alimentazione dedicato.

Printed in:
Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison - Francia
+ 33 (0) 1 41 29 70 00

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

© Schneider Electric. Tutti i diritti sono riservati.

2507_LSS100300_SW