CONTROL YOUR LIVING SPACE

Manuale applicativo

KNX-IP Interfaccia secure
EK-IE1-SEC-TP

KNX-IP Router secure
EK-IF1-SEC-TP

Indice

Revisione	Modifiche	Data	Redatto da	Verificato da
1.0	Prima versione	07/10/2022	G. Schiochet	C. Baldini

1. Documento

Questo manuale applicativo si riferisce alla versione A1.0 dell'interfaccia secure KNX-IP ekinex® EK-IE1-SEC-TP e router secure KNX-IP ekinex® EK-IF1-SEC-TP.
Il manuale applicativo e il programma applicativo per ETS® sono disponibili per il download all'indirizzo www.ekinex.com.

Elemento	Nome file	Release dispositivo	Aggiornamento
Manuale applicativo	MAEKIE1IF1SECTP_IT.pdf	A1.0	10 / 2022
Applicativo ETS KNX-IP interface secure	APEKIE1SECTP01.knxproj		
Applicativo ETS KNX-IP router secure	APEKIF1SECTP01.knxproj		

Altre informazioni tecniche sui dispositivi sono disponibili nel documento STEKIE1IF1SECTP_IT.pdf.

2. Descrizione dei prodotti

L'interfaccia IP ekinex® KNX EK-IE1-SEC-TP secure è un'interfaccia bus compatta tra LAN/Ethernet e bus KNX. Con il suo design compatto ha una larghezza di solo 1 modulo (18 mm) ed è alimentato dal bus KNX. Il dispositivo è un'interfaccia tra IP e KNX e può essere utilizzato come interfaccia di programmazione per il software ETS®. Puoi accedere al Bus KNX da ogni punto della tua LAN. Inoltre, l'interfaccia IP KNX EK-IE1-SEC-TP secure consente di programmare il bus KNX su Internet.
Il dispositivo supporta KNX Security che può essere abilitato in ETS®. Con la sua funzionalità di interfaccia (tunneling) la sicurezza KNX impedisce l'accesso non autorizzato.
I pulsanti e i LED sul dispositivo consentono una diagnosi locale che include lo stato di funzionamento e gli errori di comunicazione.
Il Router IP ekinex® EK-IF1-SEC-TP secure consente l'inoltro di telegrammi tra linee diverse attraverso una LAN (IP) come backbone veloce. Inoltre questo dispositivo è adatto per collegare un PC alla rete KNX ad es. per la programmazione ETS®.
Il dispositivo supporta KNX Security che può essere abilitato in ETS®. In quanto router sicuro, il dispositivo consente l'accoppiamento di comunicazioni non protette su KNX TP a una dorsale IP protetta. Anche per la funzionalità di interfaccia (tunneling) la sicurezza KNX impedisce l'accesso non autorizzato.
L'indirizzo IP può essere ottenuto rispettivamente da un server DHCP o mediante configurazione manuale (ETS®). Questo dispositivo funziona secondo la specifica KNXnet/IP utilizzando il core, la gestione del dispositivo, il tunneling e la parte di routing.
Il router IP KNX EK-IF1-SEC-TP secure ha una tabella di filtri estesa per il gruppo principale 0 ... 31 ed è in grado di memorizzare fino a 150 telegrammi. L'alimentazione viene fornita tramite il bus KNX.

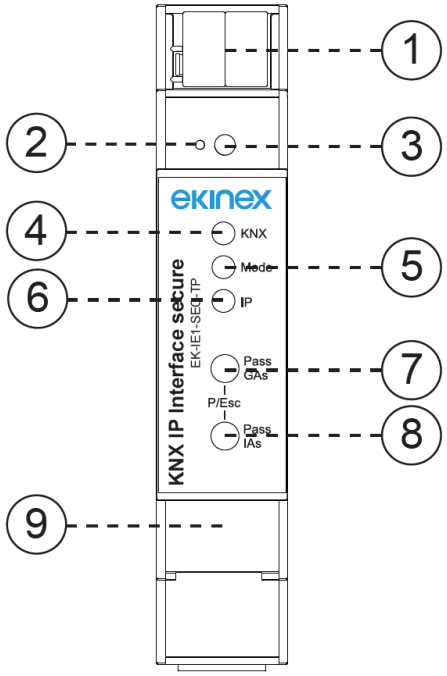
Di seguito le caratteristiche principali dei dispositivi:

- Pulsante di programmazione e LED sul frontale
- LED di segnalazione stato e traffico dati su linea bus e rete Ethernet
- Pulsanti per l'attivazione delle funzioni di connessione
- Collegamento linea bus tramite terminale KNX
- Collegamento a rete Ethernet tramite connettore RJ45
- Ethernet 100BaseT (100MBit/s)
- Protocolli Internet supportati ARP, ICMP, IGMP, UDP/IP, TCP/IP, DHCP e IP automatico

- Supporto per la tecnologia *secure* KNX, attivabile tramite ETS®
- Fino a 8 connessioni KNXnet/IP Tunneling contemporaneamente
- Lunghezza massima APDU: 55
- Sicurezza KNXnet/IP (AES-128)
- Funzionalità accoppiatore di linea/area KNX (solo EK-IF1-SEC-TP)
- Tabella filtri estesa per il gruppo principale 0 ... 31 (solo EK-IF1-SEC-TP)

3. Elementi di commutazione, visualizzazione e collegamento

I dispositivi sono dotati di un pulsante di programmazione e di un LED di programmazione, due pulsanti operativi, tre LED di indicazione dello stato, morsetti per il collegamento della linea bus KNX e della rete Ethernet/LAN.



1. Connettore bus KNX
2. LED per modalità di programmazione (rosso)
3. Pulsante per modalità di programmazione
4. LED KNX (multicolore)
5. LED Mode (multicolore)
6. LED IP (multicolore)
7. Pulsante Connection Up
8. Pulsante Connection Down
9. Connettore Ethernet/LAN

Figura 1 - Elementi EK-IE1-SEC-TP

3.1 Elementi di commutazione

- Pulsante ❸ per passare dalla modalità di funzionamento normale a quella di programmazione. Questa operazione può essere effettuata anche premendo contemporaneamente I pulsanti ❼ e ❽;
- Pulsanti ❼ and ❽ per le seguenti operazioni:
    - per EK-IE1-SEC-TP, consentono di scegliere ogni singola connessione. ***Conn Up*** conta i numeri di connessione verso l'alto e ***Conn Dn*** verso il basso. Il numero di connessione effettivamente selezionato è indicato dal lampeggio (1x…5x volte) del LED Mode ❺;
    - per EK-IF1-SEC-TP, con il pulsante ***Pass GAs*** si attiva l'inoltro di telegrammi indirizzati di gruppo (Group Addressed), mentre il pulsante ***Pass IAs*** attiva l'inoltro di telegrammi indirizzati individualmente (Individually Addressed).

3.2 Elementi di visualizzazione e collegamento

- LED rosso ❷ per visualizzare la modalità di funzionamento attiva del dispositivo (acceso = programmazione, spento = funzionamento normale).
- LED KNX multicolore ❹, che si illumina di verde se il dispositivo è alimentato correttamente dal bus KNX. Il LED segnala i telegrammi sul bus KNX con uno sfarfallio. Gli errori di comunicazione (ad es. ripetizioni di telegrammi o frammenti di telegrammi) sono indicati da un breve cambiamento del colore del LED in rosso.

  Sintesi delle indicazioni del LED KNX ❹:

Stato LED	Significato
LED acceso fisso verde	Tensione disponibile su bus KNX.
LED lampeggia verde	Presenza di telegrammi (traffico) su bus KNX
LED acceso brevemente di rosso	Problemi di comunicazione su bus KNX

- Mode LED multicolore ❺:
  A scopo di test (ad esempio durante la messa in servizio) le impostazioni di routing configurate (filtro o blocco) possono essere bypassate tramite il funzionamento manuale.

  - per l'interfaccia EK-IE1-SEC-TP, il Mode LED ❺ visualizza lo stato di ogni connessione di tunneling KNXnet/IP. Con i pulsanti ***Conn Up/Dn*** ❼ ❽ si può scegliere ciascuna singola connessione. ***Conn Up*** ❼ conta il numero di connessioni Up, mentre ***Conn Dn*** ❽ quelle Down. Il numero di connessioni effettivamente selezionato è indicato dal lampeggio (1x…5x) del LED Mode ❺. Una connessione di tunneling KNXnet/IP disponibile è indicata dal LED in colore verde, mentre una connessione di tunneling utilizzata è indicata da LED di colore arancione. Tramite la funzione Escape (Esc) è possibile terminare questa indicazione premendo contemporaneamente i pulsanti ***Conn Up/Dn*** ❼ ❽.
    Se non sono attive né la modalità di programmazione né il funzionamento manuale, il Mode LED ❺ può visualizzare errori di configurazione.

    Sintesi delle indicazioni del Mode LED ❺ per l'interfaccia EK-IE1-TP-SEC-TP:

Stato LED	Significato
LED acceso verde	Il dispositivo funziona in modalità standard.
LED acceso rosso	La modalità di programmazione è attiva.
LED lampeggia verde 1x..5x volte	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Il tunnel selezionato (1-5) non è utilizzato e libero.
LED lampeggia arancione 1x..5x volte	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Il tunnel selezionato (1-5) è utilizzato.
LED lampeggia rosso	La modalità di programmazione non è attiva. Il funzionamento manuale non è attivo. Il dispositivo non è caricato correttamente, ad es. dopo un download interrotto.

  - per il router EK-IF1-SEC-TP, il Mode LED ❺ mostra l'inoltro di telegrammi indirizzati individualmente (IAs) e/o di gruppo (GAs).

Con il pulsante **Pass GAs** ❼ è possibile attivare l'inoltro di telegrammi indirizzati di gruppo. Con il pulsante **Pass IAs** ❽ the forwarding of individually addressed telegrams can be activated.
Questo viene visualizzato con un lampeggio singolo del LED Mode ❺ (arancione). Se entrambe le modalità sono attivate, il LED Mode ❺ lampeggia due volte.
Premendo nuovamente il pulsante **Pass GAs** ❼ o il pulsante **Pass IAs** ❽ queste impostazioni possono essere selezionate e deselezionate su richiesta. Tramite la funzione Escape (Esc) è possibile interrompere il funzionamento manuale premendo contemporaneamente i pulsanti **Pass GAs** ❼ e **Pass IAs** ❽.
Se né la modalità di programmazione né la modalità manuale sono attive, il LED ❺ può visualizzare errori di configurazione.

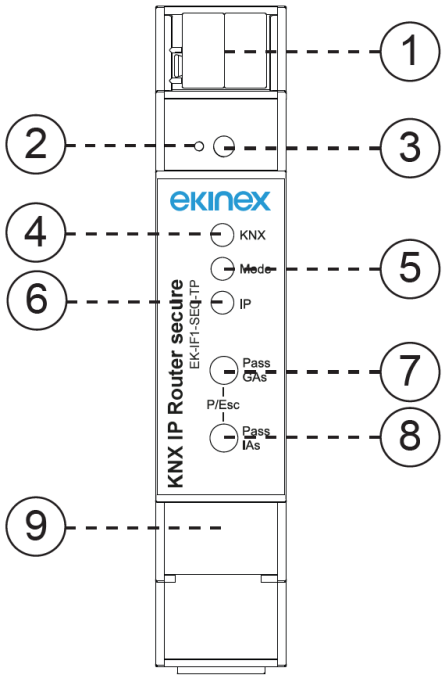
Sintesi delle possibili indicazioni del Mode LED ❺:

Stato LED	**Significato**
LED acceso verde	Il dispositivo funziona in modalità standard.
LED acceso rosso	La modalità di programmazione è attiva.
LED lampegga 1x volta arancione	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Inoltro IA **o** GA.
LED lampeggia 2x volte arancione	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Inoltro IA **e** GA.
LED lampeggia rosso	La modalità di programmazione non è attiva. Il funzionamento manuale non è attivo. Il dispositivo non è caricato correttamente, ad es. dopo un download interrotto.

- LED IP multicolore ❻ che si accende quando è attivo un collegamento Ethernet. Questo LED è verde se il dispositivo ha impostazioni IP valide (indirizzo IP, rete secondaria e gateway). Con impostazioni IP non valide o inesistenti il LED è rosso. Questo è anche il caso se ad esempio il dispositivo non ha ancora ricevuto le impostazioni IP da un server DHCP. Il LED indica il traffico dei telegrammi IP con uno sfarfallio.

  Panoramica delle diverse indicazioni del LED IP ❻:

Stato LED	**Significato**
LED acceso verde	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP valide.
LED acceso rosso	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP non valide, oppure non ha ancora ricevuto le impostazioni IP da un server DHCP.
LED lampeggia verde	Traffico di telegrammi IP.



1. Connettore bus KNX
2. LED per modalità di programmazione (rosso)
3. Pulsante per modalità di programmazione
4. LED KNX (multicolore)
5. LED Mode (multicolore)
6. LED IP (multicolore)
7. Pulsante Pass GAs (Group Addresses)
8. Pulsante Pass IAs (Individual Addresses)
9. Connettore Ethernet/LAN

Figura 2 - Elementi EK-IF1-SEC-TP

3.3 Impostazioni di fabbrica

Configurazione di default di fabbrica:

- Indirizzo del singolo dispositivo:
  - EK-IE1-SEC-TP: 15.15.255
  - EK-IF1-SEC-TP: 15.15.0
- Numero di connessioni di tunneling KNXnet/IP configurate: 1
- Indirizzo individuale delle connessioni tunneling: 15.15.240
- Assegnazione indirizzo IP: DHCP
- Chiave iniziale (FDSK): attiva
- Modo Sicurezza: non attivo

3.4 Reset alle impostazioni di fabbrica (Master-Reset)

È possibile ripristinare il dispositivo alle impostazioni di fabbrica nel modo seguente:

- scollegare il connettore Bus KNX ❶ dal dispositivo;
- premere il pulsante di programmazione KNX ❸ e tenerlo premuto;
- ricollegare il connettore Bus KNX ❶ del dispositivo;
- tenere premuto il pulsante di programmazione KNX ❸ per almeno altri 6 secondi;
- un breve lampeggio di tutti i LED (❷ ❹ ❺ ❻) segnala il corretto ripristino del dispositivo alle impostazioni di fabbrica.

4. Sicurezza KNX

Lo standard KNX è stato esteso da KNX Security per proteggere le installazioni KNX da accessi non autorizzati. KNX Security impedisce in modo affidabile il monitoraggio della comunicazione e la manipolazione del sistema.
La specifica per KNX Security distingue tra KNX IP Security e KNX Data Security. KNX IP Security protegge la comunicazione su IP mentre su KNX TP la comunicazione rimane non crittografata. Pertanto, KNX IP Security può essere utilizzato anche in sistemi KNX esistenti e con dispositivi KNX TP non sicuri.
KNX Data Security descrive la crittografia a livello di telegramma. Ciò significa che anche i telegrammi sul bus twisted pair sono crittografati.

4.1 Sicurezza KNX IP per la funzione interfaccia

Quando si utilizza un'interfaccia IP KNX collegata al bus, l'accesso all'installazione è possibile senza sicurezza per tutti i dispositivi che hanno accesso alla rete IP. Con KNX Security è necessaria una password. È già stata stabilita una connessione sicura per il trasferimento della password. Tutte le comunicazioni tramite IP sono crittografate e protette.
In entrambe le modalità, l'interfaccia inoltra telegrammi KNX crittografati e non crittografati. Le proprietà di sicurezza vengono verificate dal rispettivo ricevitore o strumento.

4.2 Sicurezza KNX IP per la funzione router

L'accoppiamento di singole linee TP KNX tramite IP viene denominato “routing IP KNX”. La comunicazione tra tutti i router IP KNX collegati avviene tramite multicast UDP.

Le comunicazioni di routing sono crittografate con KNX IP Security. Ciò significa che solo i dispositivi IP che conoscono la chiave possono decrittare la comunicazione e inviare telegrammi validi. Un timestamp nel telegramma di routing garantisce che nessun telegramma precedentemente registrato possa essere riprodotto. Ciò impedisce il cosiddetto attacco di replay.

La chiave per la comunicazione di instradamento viene riassegnata da ETS per ogni installazione. Se la Security IP KNX viene utilizzata per il routing, tutti i dispositivi IP KNX collegati devono supportare la sicurezza ed essere configurati di conseguenza.

4.3 Sicurezza KNX IP dei dati per i dispositivi

Sia l’interfaccia secure EK-IE1-SEC-TP che il router secure EK-IF1-SEC-TP supportano anche KNX Data Security per proteggere il dispositivo da accessi non autorizzati dal bus KNX. Se il dispositivo IP KNX è programmato tramite il bus KNX, ciò avviene con telegrammi crittografati.

Nota: *i telegrammi crittografati sono più lunghi di quelli non crittografati utilizzati in precedenza. Per una programmazione sicura tramite bus è quindi necessario che l'interfaccia utilizzata (es. USB) ed eventuali accoppiatori di linea intermedi supportino i cosiddetti long frame KNX.*

4.4 Sicurezza KNX dei dati per telegrammi di gruppo (solo EK-IF1-SEC-TP)

I telegrammi dal bus che non indirizzano il router IP KNX come dispositivo vengono inoltrati o bloccati in base alle impostazioni del filtro (parametri e tabella dei filtri). Non importa se i telegrammi sono crittografati

oppure no: l'inoltro avviene esclusivamente sulla base dell'indirizzo di destinazione. Le proprietà di sicurezza vengono verificate dal rispettivo destinatario.

La sicurezza KNX dei dati e la sicurezza KNX IP possono essere utilizzate in parallelo. In questo caso, ad esempio, un sensore KNX invierebbe sul bus un telegramma di gruppo crittografato con sicurezza KNX dei dati. Durante l'inoltro tramite KNX IP con sicurezza KNX IP, il telegramma crittografato verrebbe nuovamente crittografato proprio come quelli non crittografati. Tutti i partecipanti al livello IP KNX che supportano la sicurezza KNX IP possono decodificare la crittografia IP, ma non la sicurezza dei dati. In questo modo il telegramma degli altri router IP KNX viene nuovamente trasmesso alla linea o alle linee di destinazione con Sicurezza KNX dei dati. Solo i dispositivi che conoscono la chiave utilizzata per la sicurezza dei dati possono interpretare il telegramma.

5. Funzione accoppiatore (solo EK-IF1-SEC-TP)

Il router secure KNX IP EK-IF1-SEC-TP funziona come un accoppiatore di linea o accoppiatore backbone. In entrambi i casi, la LAN (IP) viene utilizzata come backbone.

La tabella seguente mostra le possibilità applicative del Router IP KNX rispetto alla topologia classica:

	Topologia classica (senza IP)	**Accoppiamento IP delle aree (IP area coupling)**	**Accoppiamento IP delle linee (IP line coupler)**
Area (Backbone)	TP	IP	IP
Accoppiamento	Accoppiatore di linea KNX (max. 15 Pcs.)	Router KNX IP (max. 15 Pcs.)	Diretto via LAN Switch
Linea principale	TP	TP	IP
Accoppiamento	Accoppiatore di linea KNX (max. 15x15 Pcs.)	Accoppiatore di linea KNX (max. 15x15 Pcs.)	Router KNX IP (max. 225 Pcs..)
Linea	TP	TP	TP

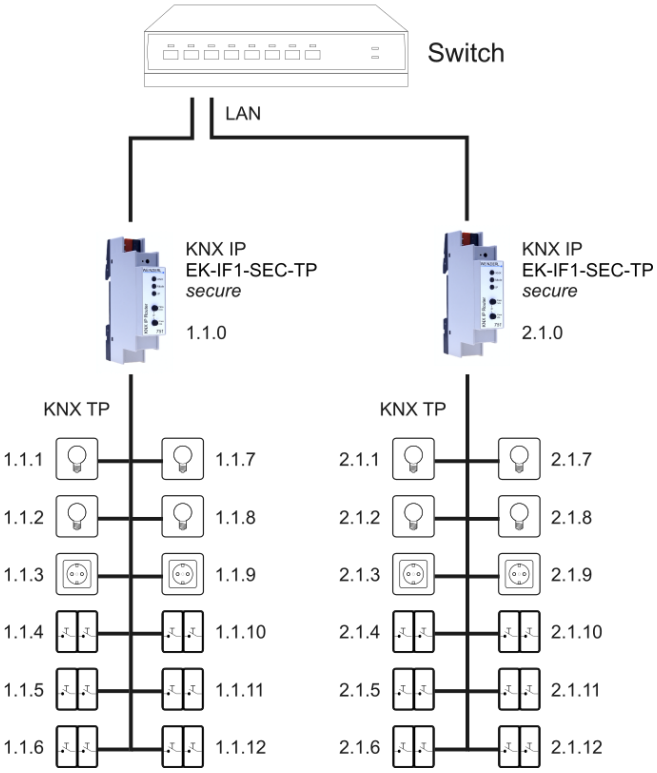


Figura 3 - Router KNX IP come accoppiatore di linea

Nota: *se il router IP KNX secure viene utilizzato come accoppiatore di linea (x.y.0), non deve essere presente un router IP KNX nella topologia al di sopra di esso. Ad esempio, se un router IP KNX ha l'indirizzo individuale 1.1.0, non deve esserci alcun router IP KNX con l'indirizzo 1.0.0.*

L'indirizzo individuale assegnato al router KNX IP secure determina se il dispositivo funziona come accoppiatore di linea o di area. Se l'indirizzo individuale ha la struttura x.y.0 (x, y: 1..15), il router funziona come accoppiatore di linea. Se invece la struttura è del tipo x.0.0 (x: 1..15), il router funge da accoppiatore backbone.

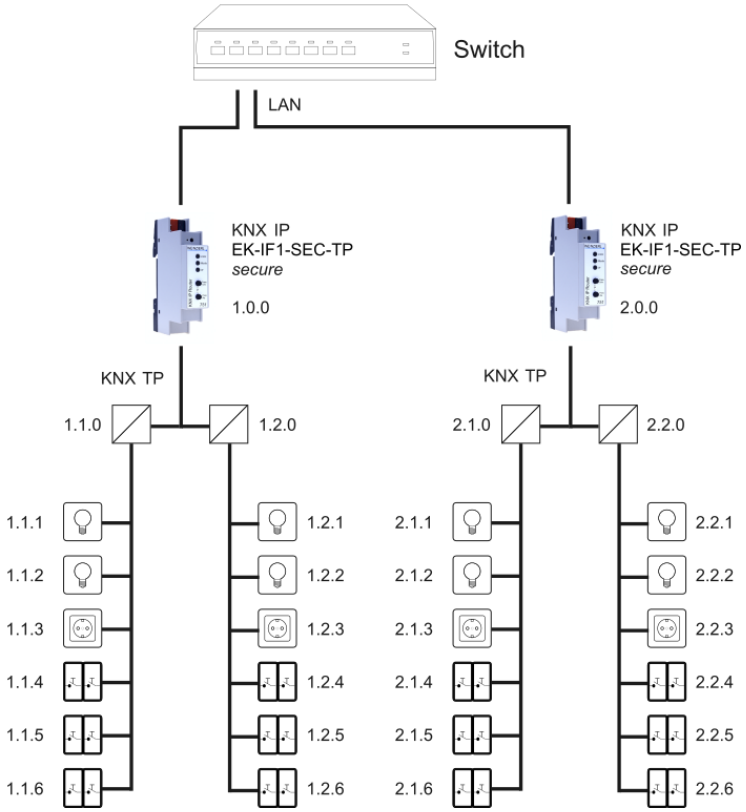


Figura 4 - Router KNX IP come accoppiatore di area

Nota: *se il router IP KNX secure viene utilizzato come accoppiatore di linea (x.y.0), non deve essere presente un router IP KNX nella topologia al di sopra di esso. Ad esempio, se un router IP KNX ha l'indirizzo individuale 1.1.0, non deve esserci alcun router IP KNX con l'indirizzo 1.0.0.*

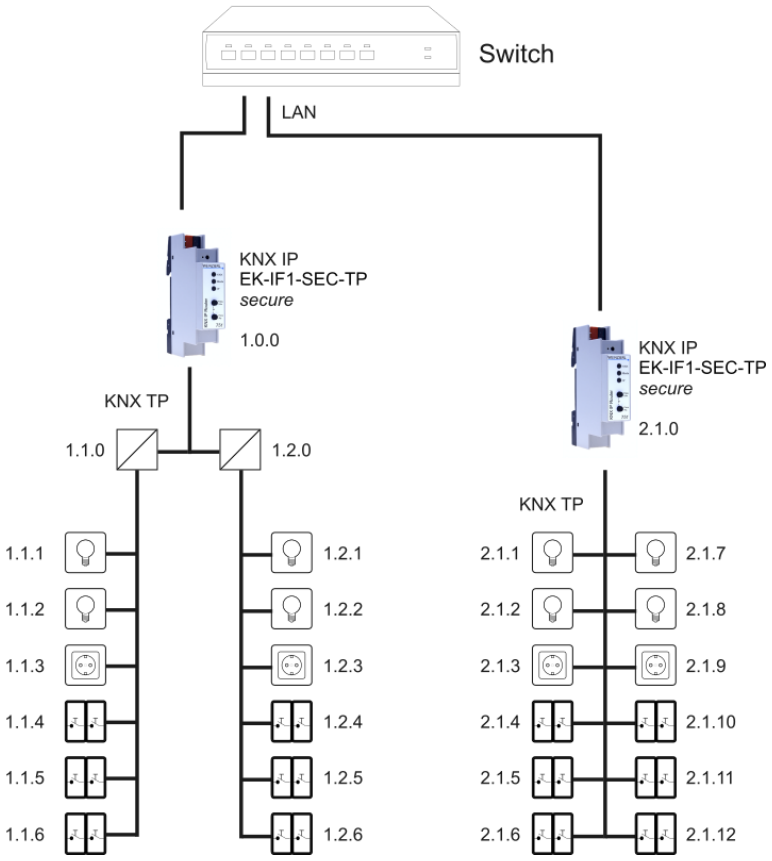


Figura 5 - Router KNX IP come accoppiatore di area e di linea

Il router KNX IP ha una tabella di filtri e contribuisce quindi a ridurre il carico del bus. La tabella di filtri (8kB) supporta l'intervallo di indirizzi di gruppo esteso (gruppi principali 0 … 31) e viene generata automaticamente da ETS.

A causa della differenza di velocità tra Ethernet (10/100 MBit/s) e KNX TP (9,6 kBit/s), è possibile trasmettere un numero molto maggiore di telegrammi su IP. Se vengono trasmessi più telegrammi consecutivi per la stessa linea, è necessario memorizzarli nel router per evitare la perdita di telegrammi. Il router KNX IP secure ha una memoria per 150 telegrammi (da IP a KNX).

5.1 Funzione di accesso al bus (KNXnet/IP Tunneling)

Il router KNX IP secure può essere utilizzato come interfaccia per KNX. È possibile accedere al bus KNX da qualsiasi punto della LAN. A tale scopo deve essere assegnato un ulteriore indirizzo individuale. Ciò è descritto nel capitolo 6.

6. Parametri ETS KNX-IP

Il software ETS (ETS 5.7 o superiore) può essere scaricato dal sito Web del prodotto www.ekinex.com o tramite il catalogo online KNX.

Se il primo prodotto viene inserito in un progetto con KNX Security, ETS richiede di inserire una password di progetto.

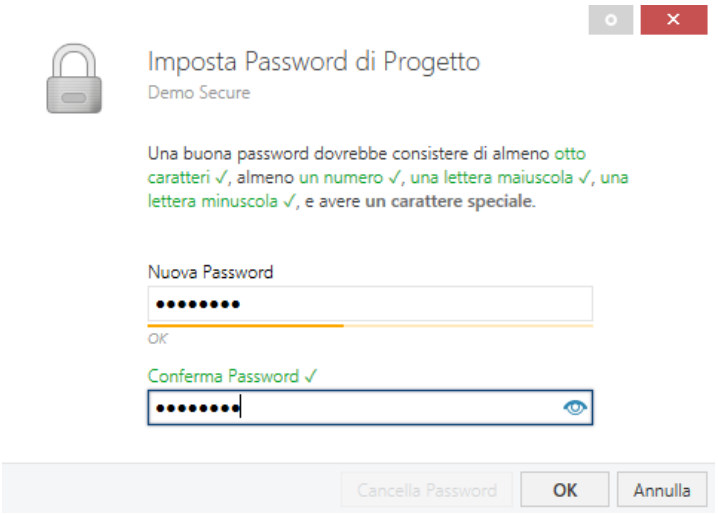


Figura 6 - impostazione password di progetto

Questa password protegge il progetto ETS da accessi non autorizzati. Questa password non è una chiave utilizzata per la comunicazione KNX. L'inserimento della password può essere bypassato con "Annulla", ma questo non è consigliato per motivi di sicurezza.

ETS richiede un certificato del dispositivo per ogni dispositivo con KNX Security creato in ETS. Questo certificato contiene il numero di serie del dispositivo e una chiave immateriale (FDSK = Factory Default Setup Key).

Figura 7 - aggiunta certificato del dispositivo

Il certificato viene stampato come testo sul dispositivo. Può anche essere comodamente scansionato dal codice QR stampato tramite una webcam.

L'elenco di tutti i certificati dei dispositivi può essere gestito nella finestra Vista Principale - Progetti - Sicurezza.

Questa chiave iniziale è necessaria per mettere in funzione in sicurezza un dispositivo dall'inizio. Anche se il download ETS viene registrato da una terza parte, questa non ha accesso ai dispositivi protetti in seguito. Durante il primo download sicuro, la chiave iniziale viene sostituita da ETS con una nuova chiave che viene generata individualmente per ogni dispositivo. Ciò impedisce a persone o dispositivi che potrebbero conoscere la chiave iniziale di accedere al dispositivo. La chiave iniziale viene riattivata solo dopo un reset principale.

Il numero di serie nel certificato consente a ETS di assegnare la chiave corretta a un dispositivo durante un download.

In ETS, oltre alla finestra di dialogo dei parametri, vengono visualizzate alcune impostazioni nella finestra di dialogo delle proprietà (a bordo schermo). Le impostazioni IP possono essere effettuate qui. Gli indirizzi aggiuntivi per i collegamenti dell'interfaccia vengono visualizzati nella vista della topologia.

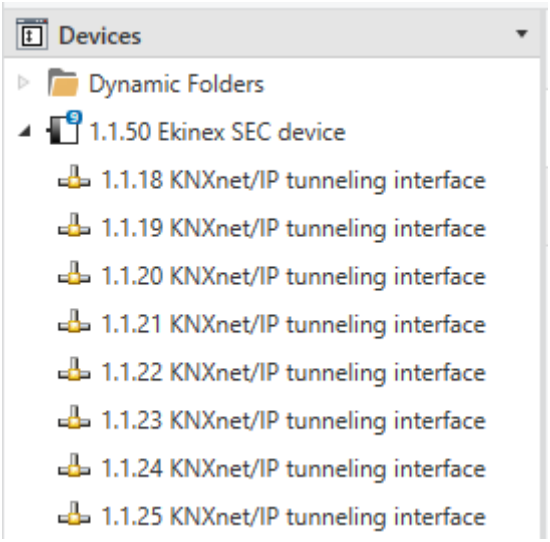


Figura 8 - indirizzi aggiuntivi

Ogni singolo indirizzo KNX può essere modificato cliccando sulla voce dell'elenco e digitando l'indirizzo desiderato nel campo di testo “Indirizzo individuale”. Se la cornice del campo di testo diventa rossa dopo aver inserito l'indirizzo, l'indirizzo è già stato preso all'interno del progetto ETS.

Nota: *assicurarsi che nessuno degli indirizzi sopra indicati sia già in uso all'interno dell'installazione KNX.*

Cliccando su uno specifico dispositivo interfaccia o router KNX IP secure nella vista della topologia dei progetti ETS, sul lato destro della finestra ETS viene visualizzata la colonna di informazioni "Proprietà". All'interno di questa, nel Tab "Impostazioni", è possibile modificare il nome del dispositivo.

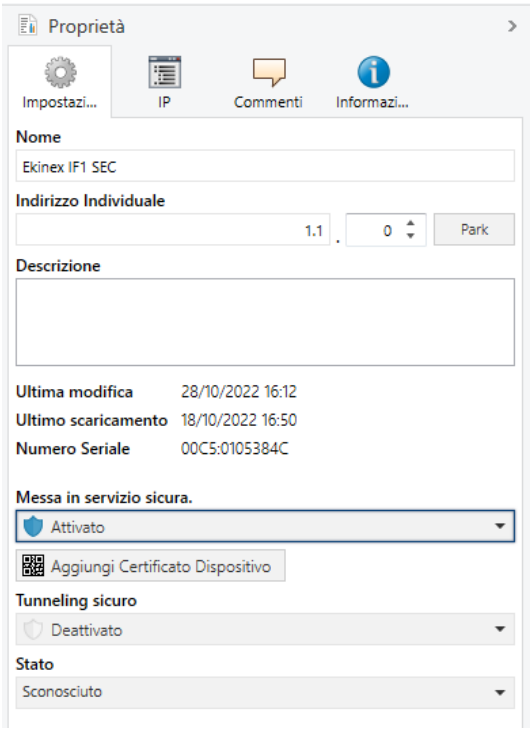


Figura 9 - Proprietà del dispositivo - impostazioni

Se il tunneling sicuro è attivato, verrà creata automaticamente una password univoca per ogni connessione tunnel. Queste password possono essere visualizzate nella panoramica "Impostazioni", quando viene selezionato un tunnel.

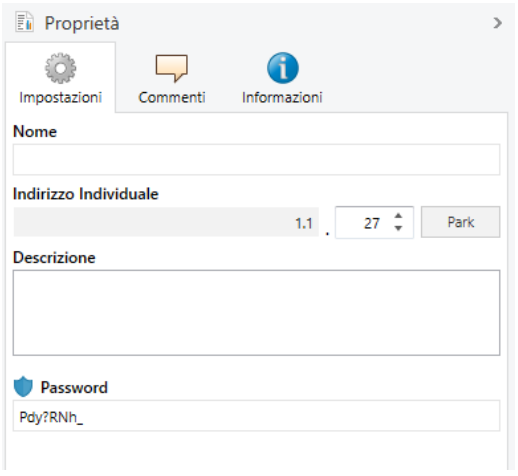


Figura 10 - password per tunneling sicuro

All'interno della Tab "IP", è possibile modificare le opzioni specifiche della rete IP dell'interfaccia IP KNX o del router sicuro.

Passando da "Ottieni un indirizzo IP automaticamente (tramite DHCP)" a "Utilizza un indirizzo IP statico", l'indirizzo IP, la maschera di sottorete e il gateway predefinito possono essere impostati liberamente.

Nota: *Tutte le modifiche nel menu delle proprietà diventano effettive solo dopo un download dell'applicazione concluso correttamente.*

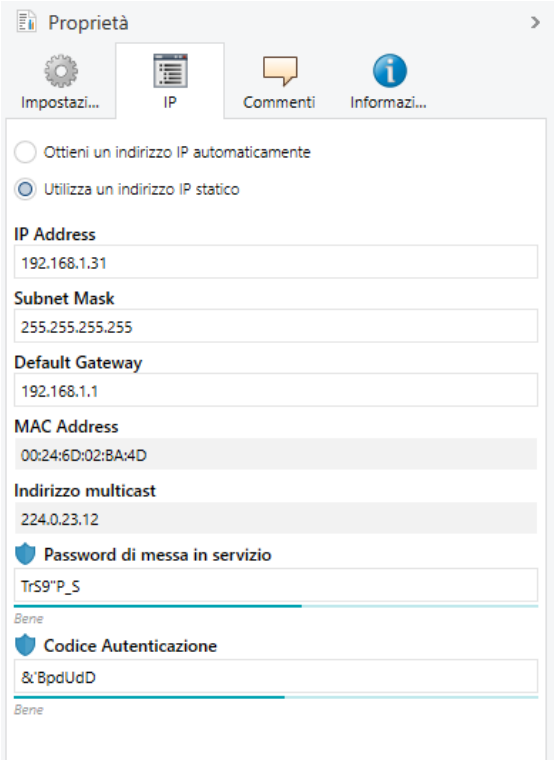


Figura 11 - impostazione indirizzo IP statico

6.1 Indirizzo IP

Qui è possibile inserire l'indirizzo IP dell'interfaccia o del router KNX IP secure. Viene utilizzato per indirizzare il dispositivo tramite la rete IP (LAN). L'indirizzamento IP deve essere coordinato con l'amministratore della rete.

6.2 Subnet Mask

Immettere qui la maschera di sottorete. Il dispositivo utilizza i valori immessi in questa maschera per determinare se nella rete locale è presente un partner di comunicazione. Se non c'è un partner nella rete locale, il dispositivo non invierà i telegrammi direttamente al partner ma al gateway che instrada il telegramma.

6.3 Default Gateway

Immettere qui l'indirizzo IP del gateway, ad es. il router DSL dell'installazione.

6.4 Esempio di assegnazione indirizzo IP

Utilizzare un PC per accedere all'interfaccia o al router KNX IP secure:

- Indirizzo IP del PC: **192.168.1.30**
- Sottorete del PC: **255.255.255.0**

L'Interfaccia o il router IP KNX secure si trova nella stessa LAN locale del PC, ovvero utilizza la stessa sottorete. La sottorete vincola gli indirizzi IP che possono essere assegnati. In questo esempio, l'indirizzo IP dell'interfaccia IP o del router deve essere 192.168.1.xx, dove xx può essere un numero compreso tra 1 e 254 (ad eccezione di 30, che è già in uso). È necessario assicurarsi che nessun numero venga assegnato due volte.

- Indirizzo IP dell'interfaccia/router IP secure: 192.168.1.31
- Sottorete dell'interfaccia/router IP secure: 255.255.255.0

6.5 Accesso remoto

L'interfaccia o il router IP KNX secure consentono l'accesso remoto tramite Internet.

7. Impostazione dei parametri ETS

I seguenti parametri possono essere impostati utilizzando ETS

7.1 Impostazioni generali

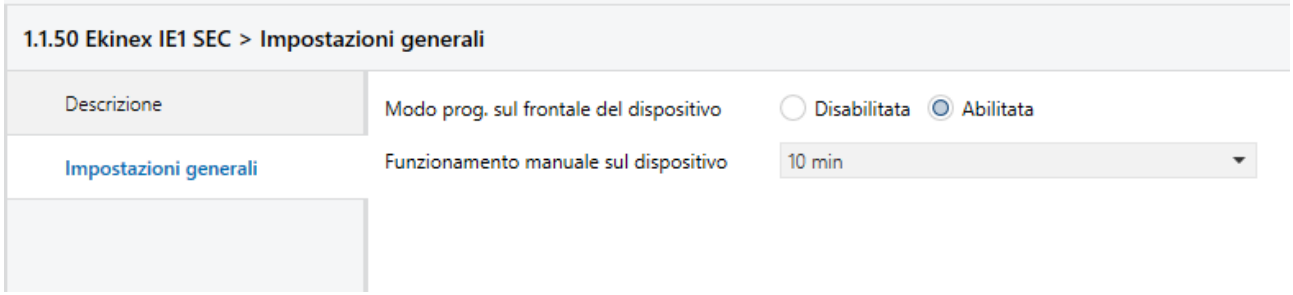


Figura 12 - impostazioni generali

Modo programmazione sul frontale del dispositivo

Oltre al normale pulsante di programmazione ❸, il dispositivo permette di attivare la modalità di programmazione dal frontale del dispositivo senza aprire il coperchio del centralino. La modalità di programmazione può essere attivata e disattivata premendo contemporaneamente entrambi i pulsanti ❼ e ❽.

Questa funzionalità può essere abilitata e disabilitata tramite il parametro ETS "Modo programmazione sul frontale del dispositivo". Il pulsante di programmazione incassato ❸ (accanto al LED di programmazione ❷) è sempre abilitato e non influenzato da questo parametro.

Funzionamento manuale del dispositivo

Il Tab "funzionamento manuale del dispositivo" consente di impostare la durata della modalità manuale. Al termine viene ripristinata la normale modalità di visualizzazione.

7.2 Routing (KNX -> IP) per Router EK-IF1-SEC-TP

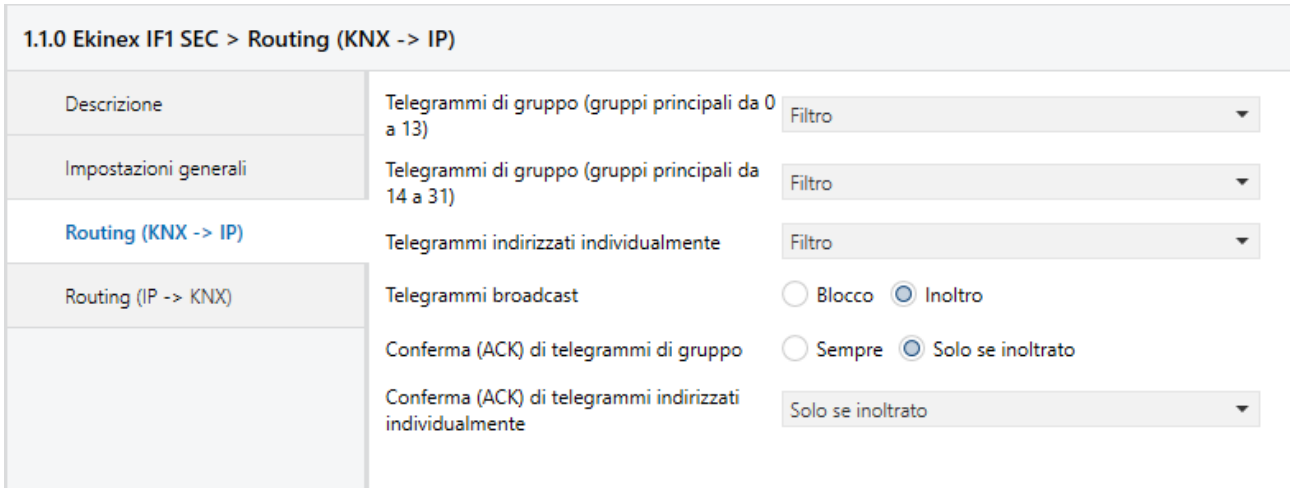


Figura 13 - Routing KNX -> IP Tab

Telegrammi di gruppo (gruppi principali da 0 a 13)

- Blocco: Nessun telegramma di gruppo dei gruppi principali da 0 a 13 viene instradato su IP.
- Inoltro: Tutti i telegrammi di gruppo dei gruppi principali da 0 a 13 vengono instradati su IP, indipendentemente dalla tabella dei filtri. Questa impostazione è solo a scopo di test.
- Filtro: La tabella dei filtri consente di verificare se il telegramma di gruppo ricevuto deve essere instradato o meno su IP.

Telegrammi di gruppo (gruppi principali da 14 a 31)

- Blocco: Nessun telegramma di gruppo dei gruppi principali da 14 a 31 viene instradato su IP.
- Inoltro: Tutti i telegrammi di gruppo dei gruppi principali da 14 a 31 vengono instradati su IP.
- Filtro: La tabella dei filtri consente di verificare se il telegramma di gruppo ricevuto deve essere instradato o meno su IP.

Telegrammi indirizzati individualmente

- Blocco: Nessun telegramma indirizzato individualmente viene instradato su IP.
- Inoltro: Tutti i telegrammi indirizzati individualmente vengono instradati su IP.
- Filtro: l'indirizzo individuale viene usato per verificare se il telegramma ricevuto con indirizzo individuale deve essere inoltrato su IP.

Telegrammi broadcast

- Blocco: Nessun telegramma broadcast ricevuto viene instradato su IP.
- Inoltro: Tutti i telegrammi broadcast ricevuti vengono instradati su IP.

Conferma (ACK) di telegrammi di gruppo

- Sempre: viene generata una conferma per ogni telegramma di gruppo ricevuto (da KNX).

- Solo se inoltrato: una conferma viene generata per i telegrammi di gruppo ricevuti (da KNX) solo se sono instradati su IP.

Conferma (ACK) di telegrammi indirizzati individualmente

- Solo se inoltrato: una conferma viene generata per i telegrammi indirizzati individualmente ricevuti (da KNX) solo se sono instradati su IP.
- Sempre: una conferma viene generata per ogni singolo telegramma indirizzato individualmente ricevuto (da KNX).
- Risposta con NACK: ad ogni telegramma ricevuto indirizzato individualmente (da KNX) si risponde con NACK (non riconoscimento). Ciò significa che la comunicazione con telegrammi indirizzati individualmente sulla linea KNX corrispondente non è possibile. La comunicazione di gruppo (telegrammi di gruppo) non viene influenzata. Questa impostazione può essere utilizzata per bloccare i tentativi di manipolazione.

Nota: *quando si utilizza "Risposta con NACK" non è più possibile l'accesso al dispositivo tramite KNX TP. La configurazione deve essere eseguita tramite IP.*

7.3 Routing (IP -> KNX) per Router EK-IF1-SEC-TP

Figura 14 - Routing IP -> KNX Tab

Telegrammi di gruppo (gruppi principali da 0 a 13)

- Blocco: Nessun telegramma di gruppo dei gruppi principali da 0 a 13 viene instradato su IP.
- Inoltro: Tutti i telegrammi di gruppo dei gruppi principali da 0 a 13 vengono instradati su IP, indipendentemente dalla tabella dei filtri. Questa impostazione è solo a scopo di test.
- Filtro: La tabella dei filtri consente di verificare se il telegramma di gruppo ricevuto deve essere instradato o meno su IP.

Telegrammi di gruppo (gruppi principali da 14 a 31)

- Blocco: Nessun telegramma di gruppo dei gruppi principali da 14 a 31 viene instradato su IP.
- Inoltro: Tutti i telegrammi di gruppo dei gruppi principali da 14 a 31 vengono instradati su IP.
- Filtro: La tabella dei filtri consente di verificare se il telegramma di gruppo ricevuto deve essere instradato o meno su IP.

Telegrammi indirizzati individualmente

- Blocco: Nessun telegramma indirizzato individualmente viene instradato su IP.
- Inoltro: Tutti i telegrammi indirizzati individualmente vengono instradati su IP.
- Filtro: l'indirizzo individuale viene usato per verificare se il telegramma ricevuto con indirizzo individuale deve essere inoltrato su IP.

Telegrammi broadcast

- Blocco: Nessun telegramma broadcast ricevuto viene instradato su IP.
- Inoltro: Tutti i telegrammi broadcast ricevuti vengono instradati su IP.

Ripetizione di telegrammi di gruppo

- Disabilitato: Il telegramma di gruppo ricevuto non viene re-inviato su KNX in caso di guasto.
- Abilitato: Il telegramma di gruppo ricevuto viene re-inviato fino a 3 volte su KNX in caso di guasto.

Ripetizione di telegrammi indirizzati individualmente

- Disabilitato: Il telegramma indirizzato individualmente ricevuto non viene re-inviato su KNX in caso di guasto.
- Abilitato: Il telegramma indirizzato individualmente ricevuto viene re-inviato fino a 3 volte su KNX in caso di guasto.

Ripetizione di telegrammi broadcast

- Disabilitato: Il telegramma broadcast ricevuto non viene re-inviato su KNX in caso di guasto.
- Abilitato: Il telegramma broadcast ricevuto viene re-inviato fino a 3 volte su KNX in caso di guasto.

8. Programmazione ETS

L'interfaccia e il router IP KNX secure possono essere programmati in diversi modi tramite l'ETS.

8.1 Programmazione via bus KNX

Il dispositivo deve solo essere collegato al bus KNX. Il software ETS richiede un'interfaccia aggiuntiva (ad esempio USB) per accedere al bus. In questo modo è possibile programmare sia il singolo indirizzo che l'intera applicazione inclusa la configurazione IP. La programmazione tramite bus è consigliata se non è possibile stabilire una connessione IP.

8.2 Programmazione via Tunneling KNXnet/IP

Non è richiesta alcuna interfaccia aggiuntiva. La programmazione tramite Tunneling KNXnet/IP è possibile se il dispositivo dispone già di una configurazione IP valida (ad es. tramite DHCP). In questo caso il dispositivo viene visualizzato nella configurazione dell'interfaccia dell'ETS e deve essere selezionato. Il download viene eseguito tramite il progetto ETS come con molti altri dispositivi.

8.3 Programmazione via connessione IP diretta

Sebbene il tunneling KNXnet/IP sia limitato dalla velocità di KNX TP, l'applicativo ETS può essere scaricato ad alta velocità tramite una connessione IP diretta. La connessione IP diretta è possibile se il dispositivo dispone già di una configurazione IP valida e di un indirizzo fisico. A tale scopo, selezionare "Usa connessione diretta IP se possibile" dal software ETS in "Bus - Connessioni - Opzioni". Il download avviene in questo caso direttamente nel dispositivo e non è visibile nel monitor di gruppo ETS.

8.4 Programmazione via KNXnet/IP Routing (solo EK-IF1-SEC-TP)

La programmazione tramite KNXnet/IP Routing è possibile se il dispositivo dispone già di una configurazione IP valida (ad es. tramite DHCP o Auto IP). In ETS, l'interfaccia di routing viene visualizzata se è disponibile almeno un dispositivo sulla rete che supporta il routing. Il nome dell'interfaccia di rete appare nel PC come descrizione. Se si seleziona il routing come interfaccia, la programmazione eseguita dal progetto ETS avviene come per altri dispositivi. In questo caso la LAN viene utilizzata come mezzo KNX analogamente a TP. Non è richiesto alcun dispositivo di interfaccia aggiuntivo.

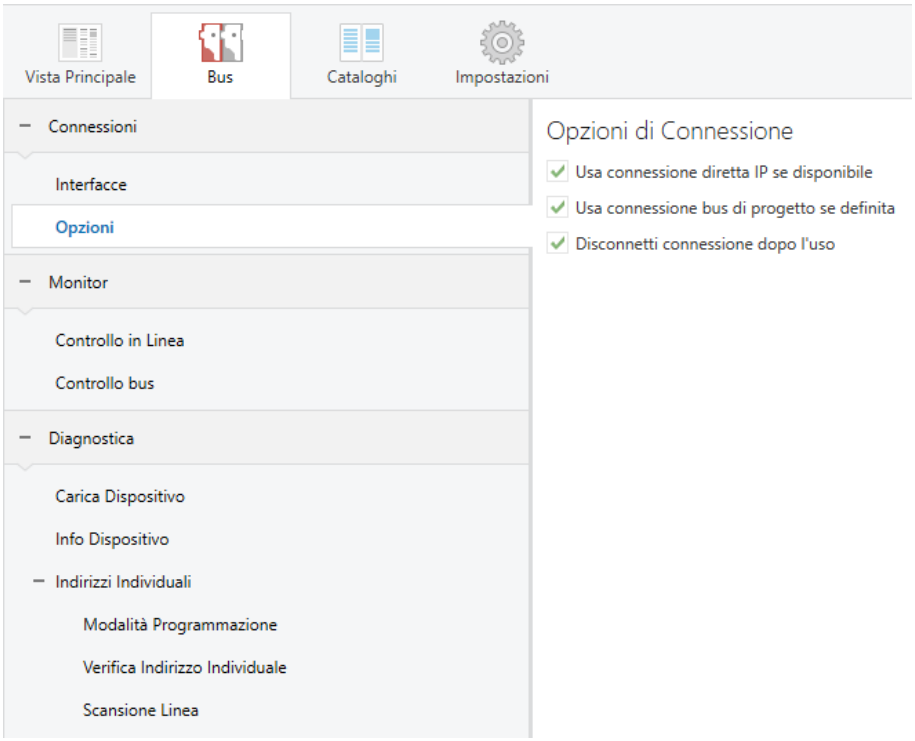


Figura 15 - opzioni di connessione da ETS

Nota: *a causa dei tempi di trasmissione notevolmente ridotti, si consiglia di eseguire i download tramite IP.*

9. Impostazioni dell'interfaccia con ETS

I dispositivi di sicurezza KNX-IP fungono da interfaccia di programmazione. ETS può utilizzare questa funzione per stabilire una connessione tramite IP alla rispettiva linea TP.

All'interno dell'ETS, le interfacce o i router KNX-IP secure possono essere selezionati e configurati tramite il menu ETS "Bus – connessioni - interfacce".

ETS può accedere all'interfaccia o al router KNX-IP secure configurati anche senza una voce nel database. Se la configurazione del dispositivo non soddisfa le condizioni dell'installazione KNX, è necessario configurarla tramite un progetto ETS. Per ulteriori informazioni, consultare la sezione Programmazione ETS.

Se la modalità di sicurezza è attivata nell'interfaccia o nel router KNX-IP secure, è necessaria una password per stabilire una connessione.

Per impostazione predefinita, l'assegnazione dell'indirizzo IP è impostata su "Ottieni un indirizzo IP automaticamente" (tramite DHCP) e quindi non sono necessarie ulteriori impostazioni. Per utilizzare questa funzione deve esistere un server DHCP sulla LAN (ad es. molti router DSL hanno un server DHCP integrato).

Se l'interfaccia e/o il router KNX-IP secure è stato collegato alla LAN e dispone di un indirizzo IP valido, dovrebbe apparire automaticamente nella voce di menu "Bus – connessioni – interfacce" sotto "Interfacce trovate".

Cliccando sul dispositivo rilevato, questo viene selezionato come interfaccia corrente. Sul lato destro della finestra ETS vengono visualizzate tutte le informazioni e le opzioni specifiche della connessione (si veda Figura 16).

Il nome del dispositivo indicato e l'"Indirizzo individuale host" (indirizzo individuale del dispositivo) possono essere modificati solo all'interno del progetto ETS.

Come tutti i dispositivi KNX programmabili, l'interfaccia e il router KNX-IP secure hanno un indirizzo individuale che può essere utilizzato per accedere al dispositivo. Viene utilizzato, ad esempio, durante il download dell'applicazione ETS sul dispositivo tramite il bus KNX.

Per la funzione di interfaccia il dispositivo contiene indirizzi individuali aggiuntivi che possono essere impostati da ETS. Quando un client (ad es. ETS) invia telegrammi al bus tramite i dispositivi KNX-IP secure, questi contengono un indirizzo mittente come uno degli indirizzi aggiuntivi. Ogni indirizzo è associato a una connessione. In questo modo i telegrammi di risposta possono essere trasmessi in chiaro al rispettivo client.

I singoli indirizzi aggiuntivi devono essere selezionati all'interno del range di indirizzi della linea bus in cui è installata l'interfaccia e non possono essere utilizzati da un altro dispositivo.

Esempio:

Indirizzo del dispositivo	1.1.10	(indirizzo all'interno della topologia ETS)
Connessione 1	1.1.240	(1. indirizzo aggiuntivo)
Connessione 2	1.1.241	(2. indirizzo aggiuntivo)
Connessione 3	1.1.242	(3. indirizzo aggiuntivo)
Connessione 4	1.1.243	(4. indirizzo aggiuntivo)
Connessione 5	1.1.244	(5. indirizzo aggiuntivo)
Connessione 6	1.1.245	(6. indirizzo aggiuntivo)
Connessione 7	1.1.246	(7. indirizzo aggiuntivo)
Connessione 8	1.1.247	(8. indirizzo aggiuntivo)

Il menu a tendina "Indirizzo fisico" consente di selezionare l'indirizzo KNX individuale della connessione KNXnet/IP Tunneling attualmente utilizzata.

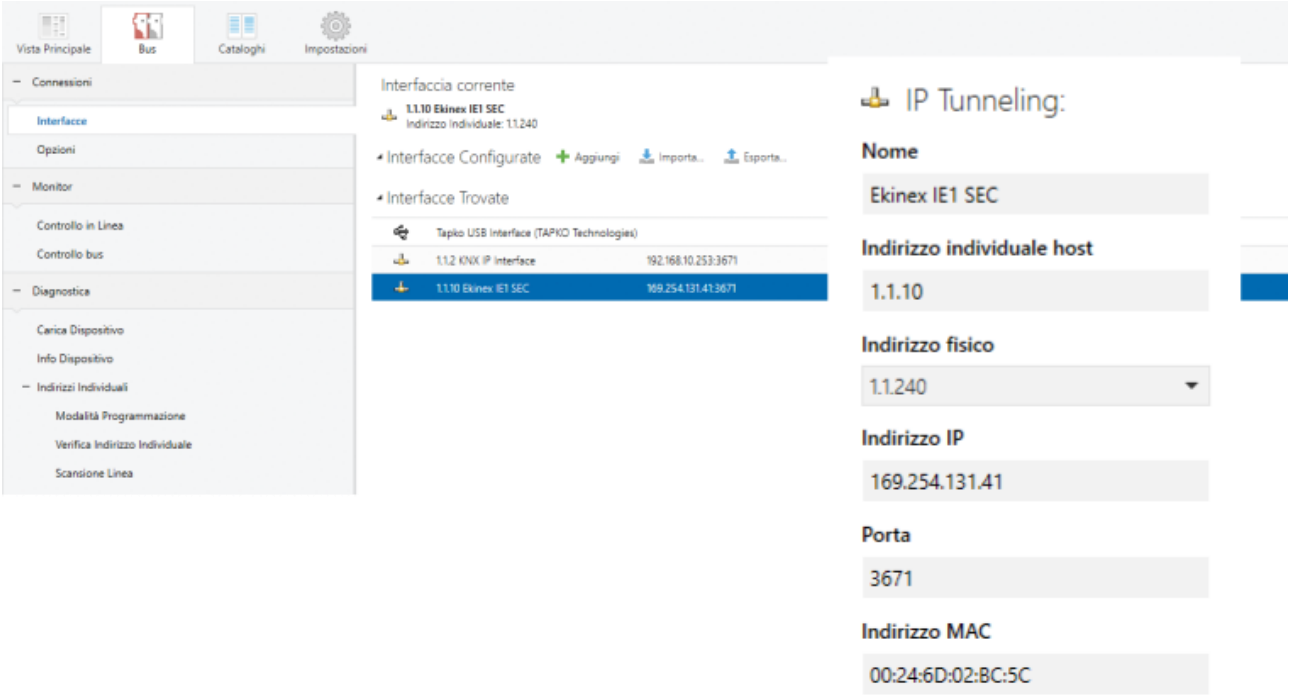


Figura 16 - connessione tunneling per l'interfaccia trovata

L'indirizzo del singolo dispositivo KNX e i singoli indirizzi per ulteriori connessioni di tunneling possono essere modificati all'interno del progetto ETS dopo che il dispositivo è stato aggiunto al progetto.

10. Licenze Open Source

Questi prodotti contengono una licenza software open source:

curve25519-donna: Curve25519 elliptic curve, public key function

Fonte: http://code.google.com/p/curve25519-donna/

La ridistribuzione e l'uso in forma sorgente e binaria, con o senza modifiche, sono consentiti a condizione che siano soddisfatte le seguenti condizioni:

- Le ridistribuzioni del codice sorgente devono conservare l'avviso di copyright di cui sopra, questo elenco di condizioni e il seguente disclaimer.
- Le ridistribuzioni in forma binaria devono riprodurre l'avviso di copyright di cui sopra, questo elenco di condizioni e il seguente disclaimer nella documentazione e/o altro materiale fornito con la distribuzione.
- Né il nome di Google Inc. né i nomi dei suoi collaboratori possono essere utilizzati per avallare o promuovere prodotti derivati da questo software senza una specifica autorizzazione scritta.

QUESTO SOFTWARE È FORNITO DAI TITOLARI DEL COPYRIGHT E DAI CONTRIBUTORI "COSÌ COM'È" E QUALSIASI GARANZIA ESPRESSA O IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO PARTICOLARE VIENE ESCLUSA. IN NESSUN CASO IL PROPRIETARIO DEL COPYRIGHT O I CONTRIBUTORI SARANNO RESPONSABILI PER EVENTUALI DANNI DIRETTI, INDIRETTI, ACCIDENTALI, SPECIALI, ESEMPLARI O CONSEQUENZIALI (INCLUSI, A TITOLO ESEMPLIFICATIVO, APPROVVIGIONAMENTO DI BENI O SERVIZI SOSTITUTIVI; PERDITA DI UTILIZZO, DATI O PROFITTI; O INTERRUZIONE DI ATTIVITÀ) COMUNQUE CAUSATE E DA QUALSIASI TEORIA DI RESPONSABILITÀ, SIA CONTRATTUALE, OGNI RESPONSABILITÀ O ILLECITO (COMPRESO NEGLIGENZA O ALTRO) DERIVANTI IN QUALSIASI MODO DALL'UTILIZZO DI QUESTO SOFTWARE, ANCHE SE AVVISATO DELLA POSSIBILITÀ DI TALE DANNO.

11. Appendice

ATTENZIONE:

- ***L'installazione, il collegamento elettrico, la configurazione e la messa in servizio del dispositivo possono essere eseguiti solo da personale qualificato.***
- ***Devono essere rispettate le norme di sicurezza vigenti.***
- ***Il dispositivo non deve essere aperto. L'apertura dell'involucro del dispositivo fa decadere immediatamente il periodo di garanzia.***
- ***Per la progettazione e la costruzione di impianti elettrici, devono essere prese in considerazione le linee guida, i regolamenti e gli standard pertinenti del rispettivo paese.***

11.1 Restituzione dei prodotti difettosi

I dispositivi ekinex® KNX difettosi possono essere restituiti per la riparazione/sostituzione seguendo la procedura descritta di seguito.

11.2 Dispositivi acquistati direttamente da ekinex®

E' necessario richiedere un numero RMA (Rientro Merce Autorizzato) inviando una e-mail all'indirizzo support@ekinex.com con le seguenti informazioni obbligatorie:

- Modello del dispositivo
- Numero di serie del dispositivo (si trova sull'etichetta del prodotto)
- Data di acquisto/Riferimento ordine
- Descrizione dettagliata del guasto o del problema

Il team di assistenza tecnica contatterà l'utente il prima possibile per approfondire il problema, suggerire possibili soluzioni o autorizzare la restituzione del dispositivo per la sostituzione o la riparazione.

Se il dispositivo deve essere restituito, questo va spedito al seguente indirizzo:

EKINEX S.p.A. - Via Novara, 37 / SP229 - I-28010 Vaprio d'Agogna (NO) - Italy.

Ulteriori accordi verranno presi con il team di supporto tecnico, a seconda del tipo di problema e del dispositivo.

11.3 Dispositivi acquistati presso rivenditori ekinex®

Se il dispositivo è stato acquistato tramite un rivenditore, fare riferimento al contatto dell'assistenza tecnica del rivenditore. A seconda del problema e di altri fattori, su decisione di ekinex® e previo accordo con il rivenditore, al cliente potrebbe essere richiesto di contattare direttamente ekinex® secondo la procedura di cui sopra.

11.4 Altre informazioni

Questo manuale applicativo è rivolto a installatori, integratori di sistemi e progettisti.

Per ulteriori informazioni sul prodotto, contattare il supporto tecnico ekinex® all'indirizzo e-mail support@ekinex.com o visitare il sito http://www.ekinex.com.

KNX® e ETS® sono marchi registrati da KNX Association cvba, Bruxelles.