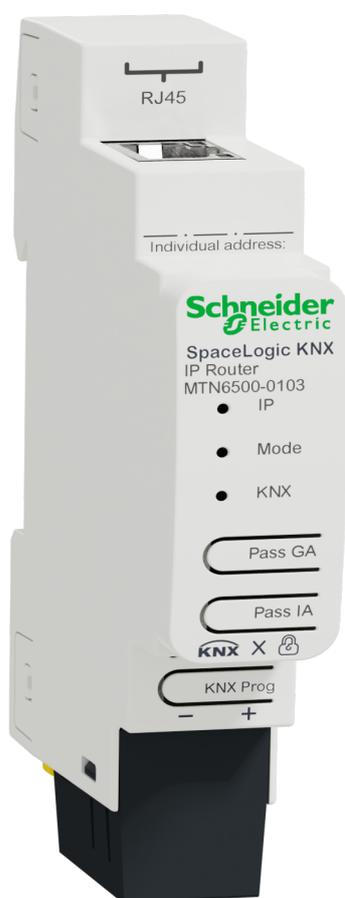


Router IP SpaceLogic KNX guida DIN

Informazioni sul prodotto e descrizione dell'applicazione

Questo documento fornisce informazioni sul prodotto Router IP SpaceLogic KNX guida DIN MTN6500-0103 e descrive il router IP KNX secure 7127 /1.2 per l'applicazione ETS.

MTN6500-0103
12/2019



Informazioni di carattere legale

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nella presente guida sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari. La presente guida 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 la presente guida o parte di essa, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione, o in altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

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

I prodotti e le apparecchiature di Schneider Electric devono essere installati, utilizzati, posti in assistenza e in manutenzione esclusivamente da personale qualificato.

Considerato che le normative, le specifiche e i progetti possono variare di volta in volta, le informazioni contenute nella presente guida possono essere soggette a modifica senza alcun 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 le conseguenze risultanti dall'uso delle informazioni ivi contenute.

Sommario

Informazioni sulla sicurezza	5
Per la vostra sicurezza	6
Informazioni sul prodotto	7
KNX Security.....	7
KNX IP Security per la funzione router.....	7
KNX IP Security per la funzione di interfaccia.....	7
KNX Data Security per il dispositivo	8
KNX Data Security per telegrammi di gruppo	8
Installazione e collegamento.....	9
Installazione.....	9
Rimozione.....	10
Collegamento.....	10
Dati tecnici.....	11
Funzione di accoppiamento (KNXnet/inoltro IP e inoltro TP).....	12
Router IP KNXcome accoppiatore di linea	12
Router IP KNX come accoppiatore di area	13
Router IP KNX come accoppiatore di area e linea	14
Funzione di accesso bus (KNXnet/IP Tunneling)	15
Collegamenti ed elementi di comando	16
Modalità di programmazione KNX.....	17
Display stato	18
Funzionamento manuale	19
Impostazioni predefinite di fabbrica	20
Ripristino delle impostazioni di fabbrica del dispositivo (reset del master).....	20
Impostazioni interfaccia con ETS	21
Applicazione ETS	22
Progetto ETS	23
Parametri aggiuntivi	25
Indirizzo IP	27
Subnet mask	27
Gateway predefinito.....	27
Indirizzo multicast di inoltro.....	27
Esempio di assegnazione di indirizzi IP	28
Accesso remoto	28
Accesso VPN	29
Finestra di dialogo dei parametri ETS	30
Impostazioni generali	30
Funzionamento manuale sul dispositivo	30
Inoltro (KNX → IP).....	30
Telegrammi di gruppo (gruppo principale da 0 a 13).....	30
Telegrammi di gruppo (gruppi principali da 14 a 31)	30
Telegrammi indirizzati singolarmente	31
Telegrammi broadcast.....	31
Conferma (ACK) di telegrammi di gruppo.....	31

Conferma (ACK) di telegrammi inviati singolarmente	31
Inoltro (IP → KNX)	31
Telegrammi di gruppo (gruppo principale da 0 a 13)	32
Telegrammi di gruppo (gruppi principali da 14 a 31)	32
Telegrammi indirizzati singolarmente	32
Telegrammi broadcast	32
Ripetizione di telegrammi di gruppo	32
Ripetizione di telegrammi indirizzati singolarmente	32
Ripetizione di telegrammi di broadcast	32
Programmazione	33
Tramite bus KNX	33
Tramite KNXnet/IP Tunneling	33
Via KNXnet/Inoltro IP	33
Tramite connessione IP diretta	33
Software open source utilizzato nel prodotto	35
Garanzia sull'ulteriore utilizzo del software open source	35
Direttiva RAEE	36

Informazioni sulla sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per acquisire familiarità con il dispositivo prima di procedere all'installazione, all'uso, alla manutenzione o alla manutenzione. I seguenti messaggi speciali possono essere visualizzati in tutto il manuale o sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.



L'aggiunta di uno dei due simboli a un'etichetta di sicurezza di "Pericolo" o di "Avvertenza" indica la presenza di un pericolo elettrico che potrebbe causare lesioni personali in caso di mancato rispetto delle istruzioni.



Questo è il simbolo dell'avviso di sicurezza. Viene utilizzato per avvisare l'utente di potenziali rischi di lesioni personali. Attenersi a tutti i messaggi di sicurezza che accompagnano questo simbolo per evitare possibili lesioni o morte.

PERICOLO

PERICOLO indica una situazione di pericolo che, se non evitata, **provocherà** lesioni gravi o letali.

Il mancato rispetto delle presenti istruzioni comporta pericolo di morte e di lesioni gravi.

AVVERTENZA

AVVERTENZA indica una situazione di pericolo che, se non evitata, **potrebbe avere come conseguenza** lesioni gravi o letali.

Il mancato rispetto delle presenti istruzioni può comportare pericolo di morte, lesioni gravi o danni all'attrezzatura.

ATTENZIONE

ATTENZIONE indica una situazione di pericolo che, se non evitata, **potrebbe avere come conseguenza** lesioni di lieve o moderata entità.

Il mancato rispetto delle presenti istruzioni può comportare pericolo di lesioni o danni all'attrezzatura.

AVVISO

AVVISO serve a segnalare procedure non correlate a lesioni fisiche.

Per la vostra sicurezza

PERICOLO

PERICOLO DI FOLGORAZIONE, ESPLOSIONE O ARCO ELETTRICO

L'installazione elettrica sicura deve essere eseguita solo da personale elettrico qualificato. Il personale elettrico qualificato deve dimostrare di possedere conoscenze approfondite nei seguenti settori:

- Collegamento di impianti elettrici in rete
- Collegamento di molteplici dispositivi elettrici
- Posa di cavi elettrici
- Collegamento e realizzazione di reti KNX
- Connessione e realizzazione di reti LAN
- Norme di sicurezza, regole e regolamenti per il cablaggio locale

Il mancato rispetto delle presenti istruzioni comporta pericolo di morte e di lesioni gravi.

Informazioni sul prodotto

Il router IP SpaceLogic KNX compatto (di seguito chiamato **router IP KNX**) consente l'inoltro di telegrammi tra linee diverse tramite una LAN (IP) come dorsale veloce. Il dispositivo funge anche da interfaccia di programmazione tra un PC e il bus KNX (ad esempio per la programmazione ETS).

Il dispositivo supporta KNX Security. L'opzione può essere attivata nel ETS. Come router sicuro, il dispositivo consente l'accoppiamento di comunicazioni non protette su una linea TP KNX con una dorsale IP sicura.

KNX Security impedisce inoltre l'accesso non autorizzato alla funzione di interfaccia (tunneling).

L'indirizzo IP può essere assegnato tramite DHCP o tramite la configurazione ETS. Il dispositivo funziona in base alle specifiche KNXnet/IP tramite core, gestione dispositivi, tunneling e inoltro.

Il router IP KNX dispone di una tabella dei filtri estesa per i gruppi principali da 0 a 31 e può memorizzare fino a 150 telegrammi. L'alimentazione viene fornita attraverso il bus KNX.

KNX Security

Lo standard KNX è stato esteso da KNX Security per proteggere gli impianti 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 la comunicazione su TP KNX (doppino intrecciato) rimane non crittografata. Pertanto, KNX IP Security può essere utilizzato anche nei sistemi KNX esistenti e con dispositivi TP KNX non sicuri.

KNX Data Security descrive la crittografia a livello di telegramma. Ciò significa che anche i telegrammi sul bus KNX sono codificati.

KNX IP Security per la funzione router

L'accoppiamento delle singole linee TP KNX tramite IP è denominato inoltro IP KNX. La comunicazione tra tutti i router IP KNX collegati avviene tramite multicast UDP.

La comunicazione di inoltro è crittografata con KNX IP Security. Ciò significa che solo i dispositivi IP che conoscono la chiave possono decifrare la comunicazione e inviare telegrammi validi. Se esiste un'installazione con un vecchio router IP che non supporta IP Security, l'intera installazione può funzionare solo come non sicura. Una marca temporale nel telegramma di inoltro garantisce che non sia possibile riprodurre telegrammi registrati in precedenza. Questo previene il cosiddetto attacco di ripetizione.

La chiave per la comunicazione di inoltro viene riassegnata da ETS per ogni installazione. Se si utilizza KNX IP Security per l'invio, tutti i dispositivi IP KNX collegati devono supportare la sicurezza e devono essere configurati di conseguenza.

KNX IP Security per la funzione di interfaccia

Quando si utilizza il dispositivo come interfaccia con il 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 la trasmissione della password. Tutte le comunicazioni via IP sono crittografate e protette.

In entrambe le modalità, l'interfaccia inoltra telegrammi KNX crittografati e non. Le proprietà di sicurezza sono controllate dal rispettivo ricevitore o strumento.

KNX Data Security per il dispositivo

Il Router IP KNX supporta anche KNX Data Security per proteggere il dispositivo dall'accesso non autorizzato dal bus KNX. Se il Router IP KNX è programmato tramite il bus KNX, questo avviene con telegrammi crittografati.

NOTA: I telegrammi crittografati sono più lunghi di quelli non crittografati utilizzati in precedenza. Per una programmazione sicura tramite il bus, è quindi necessario che l'interfaccia utilizzata (ad esempio, USB) e gli eventuali accoppiatori di linea intermedi supportino i cosiddetti long frames KNX.

La configurazione del dispositivo protetto è contenuta anche in KNX Data Security.

KNX Data Security per telegrammi di gruppo

I telegrammi provenienti dal bus che non indirizzano il Router IP KNX come dispositivo sono inoltrati o bloccati in base alle impostazioni del filtro (parametri e tabella dei filtri). Non importa se i telegrammi non sono criptati o se lo sono. L'inoltro avviene esclusivamente in base all'indirizzo di destinazione. Le proprietà di sicurezza vengono controllate dal destinatario corrispondente.

KNX Data Security e KNX IP Security possono essere utilizzati in parallelo. In questo caso, ad esempio, un sensore KNX invia un telegramma di gruppo crittografato con KNX Data Security al bus. Quando si esegue l'inoltro tramite IP KNX con KNX IP Security, il telegramma crittografato viene crittografato di nuovo come quello non crittografato. Tutti i partecipanti al livello IP KNX che supportano KNX IP Security possono decodificare la crittografia IP, ma non la sicurezza dei dati. Pertanto, il telegramma proveniente dall'altro Router IP KNX viene di nuovo trasmesso alle linee target con KNX Data Security. Solo i dispositivi che conoscono la chiave utilizzata per la sicurezza dei dati possono interpretare il telegramma.

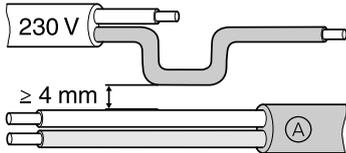
Installazione e collegamento

Il dispositivo è progettato per essere installato su una guida DIN di larghezza pari a 1 unità (18 mm).

⚡ ⚠ PERICOLO

PERICOLO DI FOLGORAZIONE E DI DANNI AL DISPOSITIVO

- Ⓐ Accertarsi che tra i singoli conduttori del cavo di alimentazione da 230 V e la linea KNX vi sia uno spazio di sicurezza minimo di 4 mm , in conformità con lo standard IEC 60664-1.

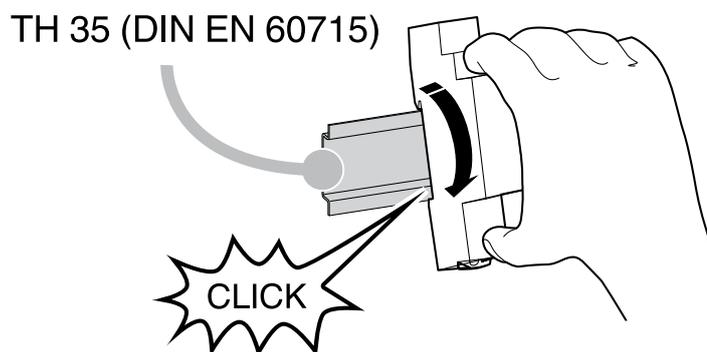


The diagram shows a 230V cable with two conductors on the left and a KNX line with two conductors on the right. A vertical double-headed arrow between the two cables is labeled '≥ 4 mm', indicating the required safety gap. A circled 'A' symbol is placed near the KNX line.

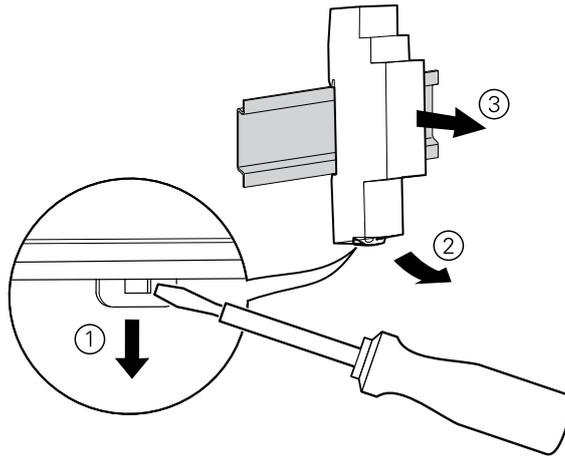
- Accertarsi che i dispositivi installati abbiano un isolamento di base minimo accanto al dispositivo.

Il mancato rispetto delle presenti istruzioni comporta pericolo di morte e di lesioni gravi.

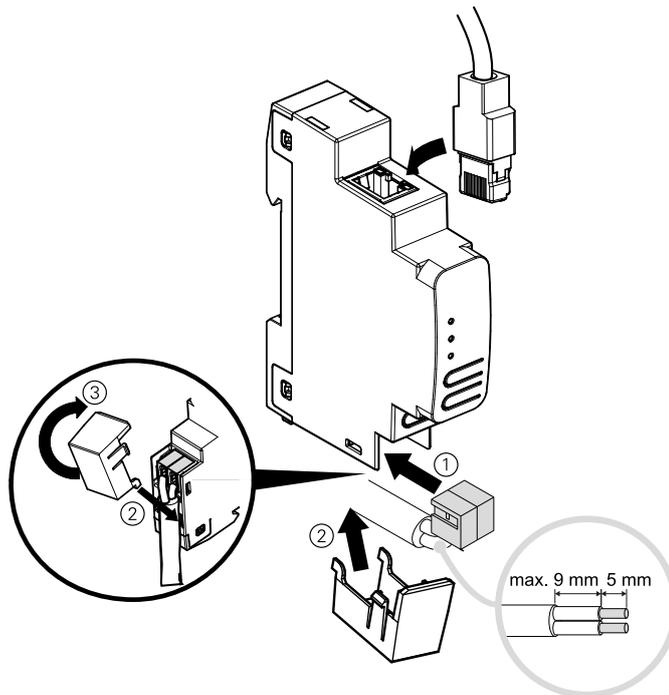
Installazione



Rimozione



Collegamento



AVVISO

DANNI ALLE APPARECCHIATURE E PERDITA DI COMUNICAZIONE

L'installazione del cavo di comunicazione per le tecnologie informatiche deve essere garantita in conformità con DIN EN 50174.

Il mancato rispetto delle presenti istruzioni può comportare pericolo di danni all'attrezzatura.

Dati tecnici

Alimentazione	tramite bus KNX, < 20mA
Collegamento	
LAN	Connettore RJ45
KNX	morsetto di collegamento al bus
Dimensioni (LxWxD)	
Dimensioni (LxWxD)	100x18x86 mm
Larghezza del dispositivo	1 modulo = 18 mm

Funzione di accoppiamento (KNXnet/inoltro IP e inoltro TP)

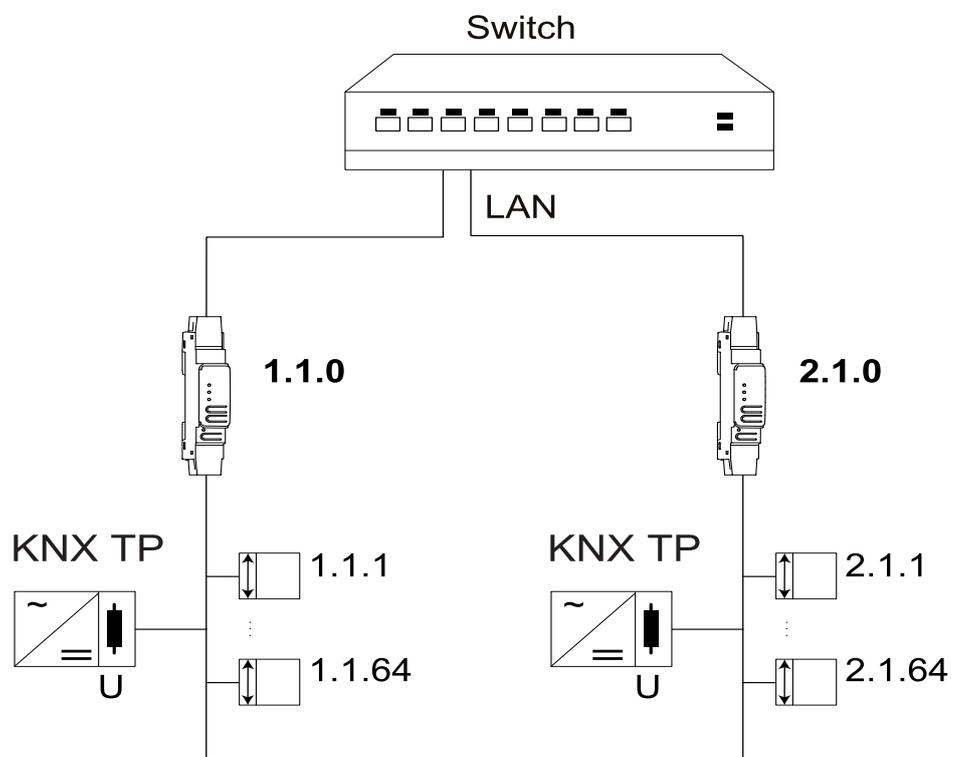
Il Router IP KNX funziona come accoppiatore di linea o dorsale. In entrambi i casi la LAN (IP) è usata come una dorsale.

La tabella seguente mostra le possibilità di applicazione dell'accoppiatore Spacelogic KNX rispetto alla topologia basata su IP:

	Topologia classica (senza IP)	Accoppiamento IP delle zone (accoppiatore di area IP)	Accoppiamento IP di linee (accoppiatore di linea IP)
Area (dorsale)	TP	IP	IP
Accoppiamento	Accoppiatore di linea KNX (max 15)	Router IP KNX (max. 15)	Direttamente tramite switch LAN
Linea principale	TP	TP	IP
Accoppiamento	Accoppiatore di linea KNX (max 15x15)	Accoppiatore di linea KNX (max 15x15)	Router IP KNX (max. 225)
Linea	TP	TP	TP

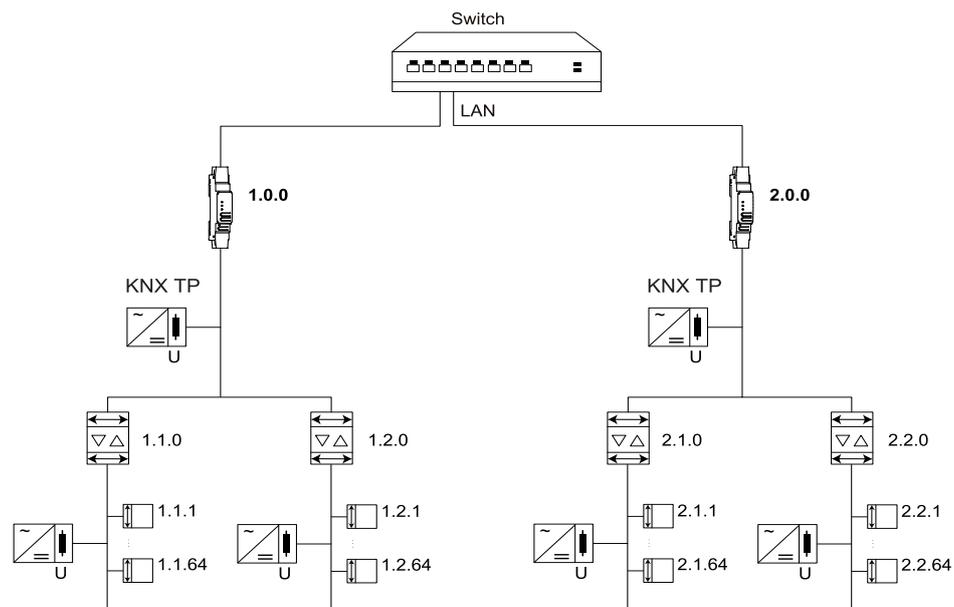
Router IP KNX come accoppiatore di linea

L'indirizzo individuale assegnato all'accoppiatore Router IP KNX determina se il dispositivo funziona come accoppiatore di linea o di area.



Se il singolo indirizzo è in formato x.y.0 (x, y: 1...15), il router funziona come accoppiatore di linea. Se è in formato x.0.0 (x: 1...15), l'accoppiatore funge da accoppiatore dorsale.

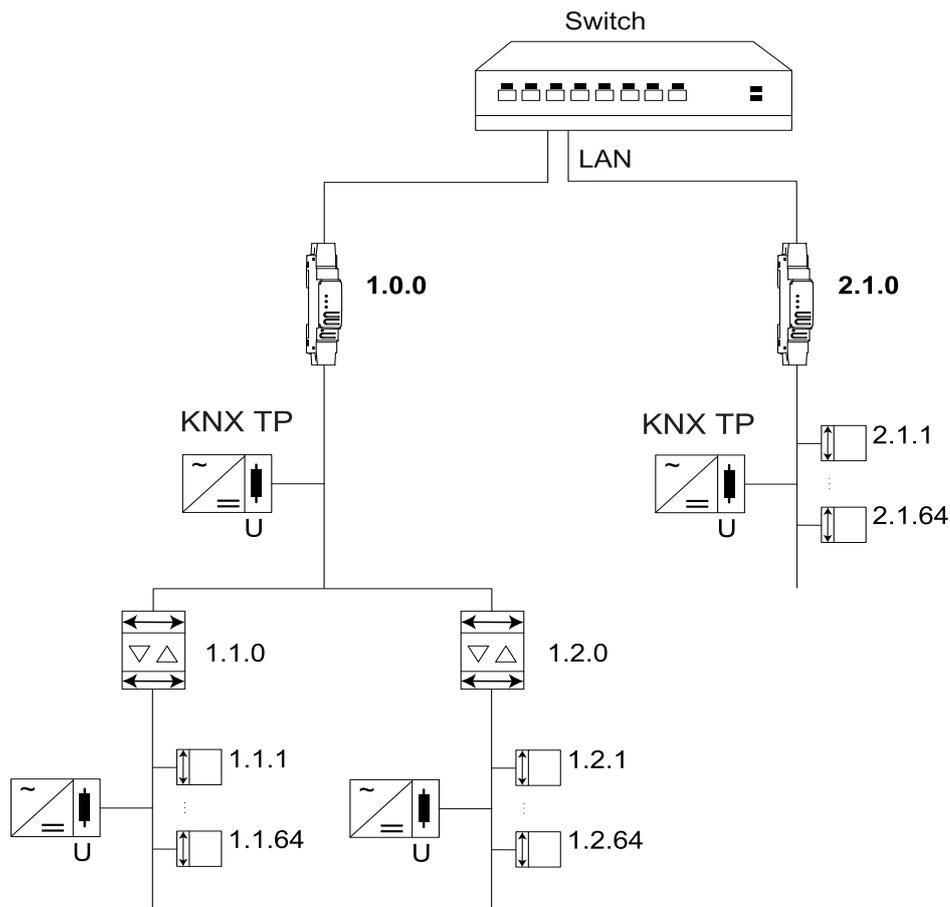
Router IP KNX come accoppiatore di area



Se il router IP KNX viene utilizzato come accoppiatore di area (x.0.0), non deve essere presente un router IP KNX nella topologia sottostante. Ad esempio, se un router IP KNX ha l'indirizzo singolo 1.0.0, non deve essere presente alcun router IP KNX con l'indirizzo 1.1.0.

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

Router IP KNX come accoppiatore di area e linea



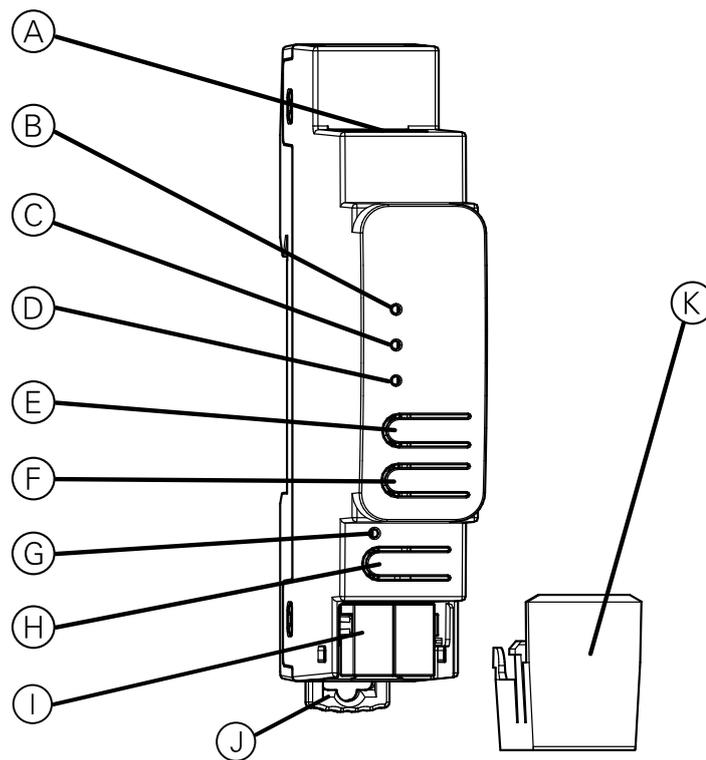
Il Router IP KNX dispone di una tabella dei filtri che contribuisce a ridurre il carico del bus. La tabella dei filtri (8 kB) supporta l'intervallo esteso di indirizzi del gruppo (gruppi principali 0 ... 31) e viene generata automaticamente da ETS.

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

Funzione di accesso bus (KNXnet/IP Tunneling)

Il router IP KNX può essere utilizzato come interfaccia con KNX. È possibile accedere al bus KNX da qualsiasi punto della LAN. A questo scopo, è necessario assegnare un indirizzo individuale aggiuntivo. Questa procedura è descritta nelle sezioni seguenti.

Collegamenti ed elementi di comando



(A)	Connettore Ethernet/LAN
(B)	LED IP (multicolore)
(C)	LED modalità (multicolore)
(D)	LED KNX (multicolore)
(E)	Pulsante: Pass GA (inoltrato di telegrammi indirizzati al gruppo)
(F)	Pulsante: Pass IA (inoltrato di telegrammi indirizzati singolarmente)
(G)	LED di programmazione (rosso)
(H)	Pulsante per la modalità di programmazione
(I)	Connettore bus KNX
(J)	Leva di rilascio per smontaggio
(K)	Copertura cavo

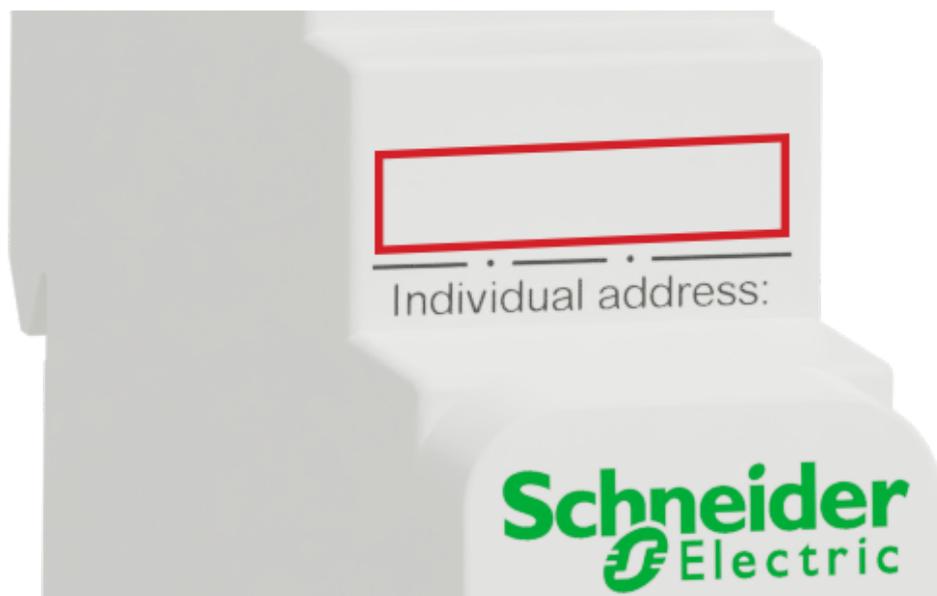
Il Router IP KNX è alimentato dal bus KNX. Non è necessario un alimentatore esterno.

NOTA: Il dispositivo non funziona senza alimentazione del bus.

Modalità di programmazione KNX

La modalità di programmazione KNX viene attivata/disattivata premendo il pulsante di programmazione KNX [®].

È possibile scrivere l'indirizzo individuale programmato sul campo di etichettatura con un marcatore o una matita non permanente in modo tale da poter cambiarlo, se necessario.



Display stato

Panoramica delle diverse indicazioni del LED IP

LED IP [ⓑ] Stato	Significato
LED verde acceso	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP valide (indirizzo IP, subnet e gateway).
LED rosso acceso	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP non valide o non ha ancora ricevuto le impostazioni IP da un server DHCP.
LED sfarfallante verde	Traffico di telegrammi IP.

Panoramica delle diverse indicazioni del LED di modalità

LED di modalità [ⓒ] Stato	Significato
LED verde acceso	Il dispositivo funziona in modalità di funzionamento standard.
LED arancione lampeggiante 1x/s	Il funzionamento manuale è attivo. Inoltre IA o GA.
LED arancione lampeggiante 2x/s	Il funzionamento manuale è attivo. Inoltre IA e GA.
Il LED lampeggia in rosso	Il funzionamento manuale non è attivo. Il dispositivo non è stato caricato correttamente. Ad esempio, dopo un download interrotto.

Panoramica delle diverse indicazioni del LED KNX

LED KNX [ⓓ] Stato	Significato
LED verde acceso	Il dispositivo è alimentato correttamente dal bus KNX.
LED sfarfallante verde	Traffico di telegrammi sul bus KNX.
LED brevemente rosso	Errori di comunicazione sul bus KNX. Ad esempio, le ripetizioni di telegrammi o frammenti di telegrammi sono indicate da una breve modifica del colore del LED a rosso.

Funzionamento manuale

A scopo di test (ad esempio, durante la messa in servizio), le impostazioni di inoltro configurate (filtro o blocco) possono essere bypassate tramite il funzionamento manuale.

Con il pulsante Pass GA [Ⓔ] è possibile attivare l'inoltro di tutti i telegrammi indirizzati del gruppo.

Con il pulsante Pass IA [Ⓕ] è possibile attivare l'inoltro di tutti i telegrammi indirizzati singolarmente.

Questo viene visualizzato mediante il lampeggiamento del LED di modalità [Ⓒ] 1x/s (arancione). Se entrambe le modalità sono attivate, il LED di modalità [Ⓒ] lampeggia 2x/s.

Premendo nuovamente il pulsante Pass GA [Ⓔ] o Pass IA [Ⓕ], queste impostazioni possono essere selezionate e deselezionate su richiesta.

Se non sono attivi né la modalità di programmazione né quella manuale, il LED [Ⓒ] può visualizzare gli errori di configurazione.

Impostazioni predefinite di fabbrica

Di default è impostata la seguente configurazione:

Indirizzo singolo dispositivo	15.15.0
Numero di configurazioni di KNXnet/IP tunneling configurate	8
Indirizzo individuale della configurazione di tunneling	15.15.240
Assegnazione indirizzo IP	DHCP
Chiave iniziale (FDSK)	attivo
Modalità di sicurezza	non attivo

Ripristino delle impostazioni di fabbrica del dispositivo (reset del master)

È possibile ripristinare le impostazioni di fabbrica del dispositivo:

1. Scollegare il connettore del bus KNX  dal dispositivo.
2. Premere il pulsante di programmazione KNX  e tenerlo premuto.
3. Ricollegare il connettore del bus KNX  del dispositivo.
4. Tenere premuto il pulsante di programmazione KNX  per almeno altri 6 secondi.

Un breve lampeggiamento di tutti i LED (, , , ) visualizza il ripristino corretto del dispositivo alle impostazioni predefinite di fabbrica.

Impostazioni interfaccia con ETS

Nel ETS, le interfacce KNX possono essere selezionate e configurate attraverso il menu ETS **Interfacce bus**.

Il sistema ETS può accedere alla configurazione Router IP KNX anche senza una voce di database. Se la configurazione del Router IP KNX non è conforme alle condizioni dell'installazione KNX, è necessario configurarlo mediante un progetto ETS. Per ulteriori informazioni, vedere la sezione *Progetto ETS, pagina 23*.

Se è attivata la modalità di sicurezza nel Router IP KNX, è necessaria una password per stabilire una connessione.

Come impostazione predefinita, l'assegnazione dell'indirizzo IP è impostata su **Automaticamente tramite DHCP** e quindi non sono necessarie ulteriori impostazioni. Per utilizzare questa funzionalità, è necessario che esista un server DHCP nella LAN. (Ad esempio, molti router DSL dispongono di un server DHCP integrato).

Se il Router IP KNX è stato collegato alla LAN e ha un indirizzo IP valido, dovrebbe apparire automaticamente in ETS nel menu **Bus in Interfacce scoperte**.

Cliccando su **Interfaccia scoperta**, viene selezionato come interfaccia corrente. Sul lato destro della finestra ETS, vengono visualizzate tutte le informazioni e le opzioni specifiche della connessione.

Il nome del dispositivo indicato e l'**Indirizzo singolo dell'host** (indirizzo singolo del dispositivo) possono essere modificati all'interno del progetto ETS.

Come tutti i dispositivi KNX programmabili, il Router IP KNX ha un indirizzo individuale che può essere utilizzato per accedere al dispositivo. Questo valore viene utilizzato, ad esempio, per il download nel ETS Router IP KNX tramite il bus.

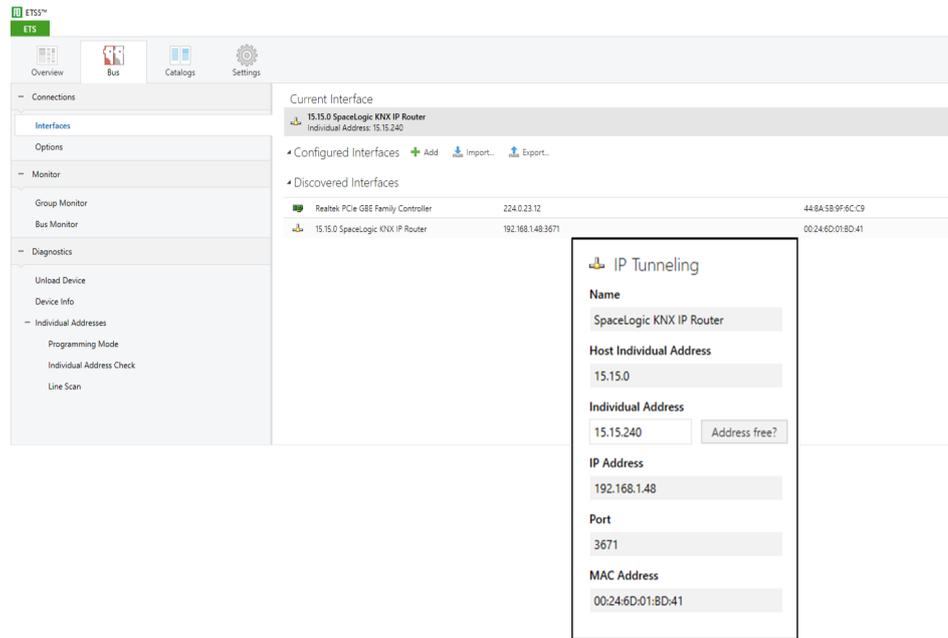
Per la funzione di interfaccia, il dispositivo contiene indirizzi individuali aggiuntivi che possono essere impostati nel ETS. Quando un client (ad esempio, ETS) invia tramite Router IP KNX telegrammi al bus, esso contiene un indirizzo del mittente come un indirizzo aggiuntivo. Ogni indirizzo è associato a una connessione. In questo modo, i telegrammi di risposta possono essere trasmessi chiaramente al rispettivo client.

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

Esempio:

Indirizzo dispositivo	1.1.0	(indirizzo nella 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)

La sezione **Indirizzo individuale** consente di selezionare il singolo indirizzo KNX del collegamento KNXnet/IP Tunneling attualmente utilizzato.



Il singolo indirizzo del dispositivo KNX e i singoli indirizzi KNX per i collegamenti di tunneling aggiuntivi possono essere modificati nel progetto ETS dopo che il dispositivo è stato aggiunto al progetto.

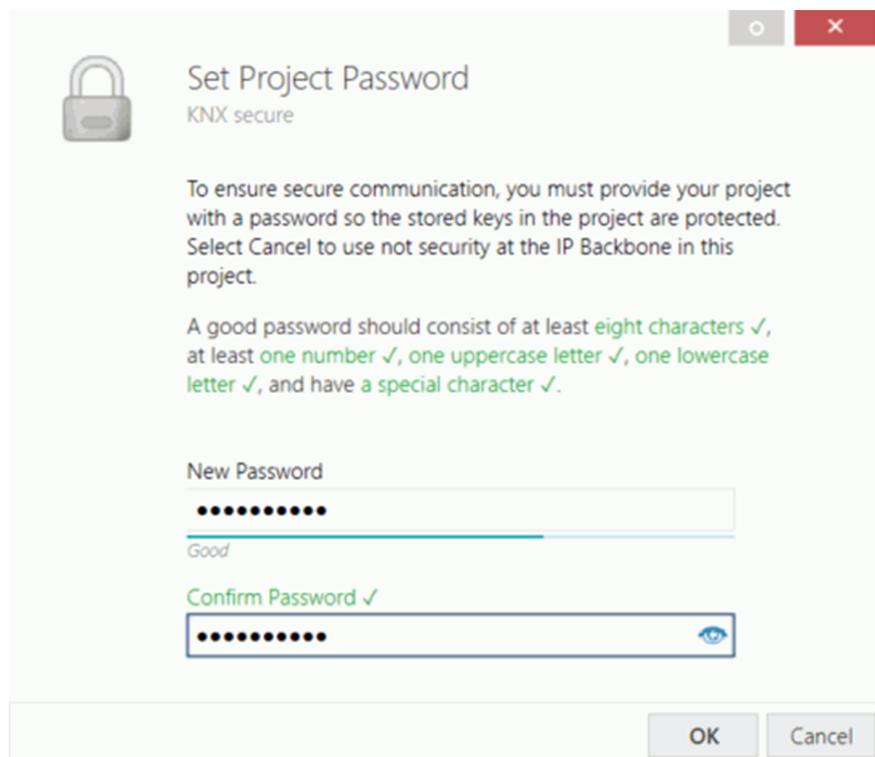
Applicazione ETS

Il database ETS (ETS 5.7.3 o superiore) può essere scaricato dal sito web del prodotto del Router IP KNX(www.schneider-electric.com) o tramite il catalogo online KNX.

Famiglia di prodotti	1.3 Interfacce/Gateway
Tipo di prodotto	1.3.14 Dispositivi IP
Produttore	Schneider Electric Industries SAS
Nome	Router IP SpaceLogic KNX guida DIN
Numero ordine	MTN6500-0103

Progetto ETS

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



Set Project Password
KNX secure

To ensure secure communication, you must provide your project with a password so the stored keys in the project are protected. Select Cancel to use not security at the IP Backbone in this project.

A good password should consist of at least **eight characters** ✓, at least **one number** ✓, **one uppercase letter** ✓, **one lowercase letter** ✓, and have a **special character** ✓.

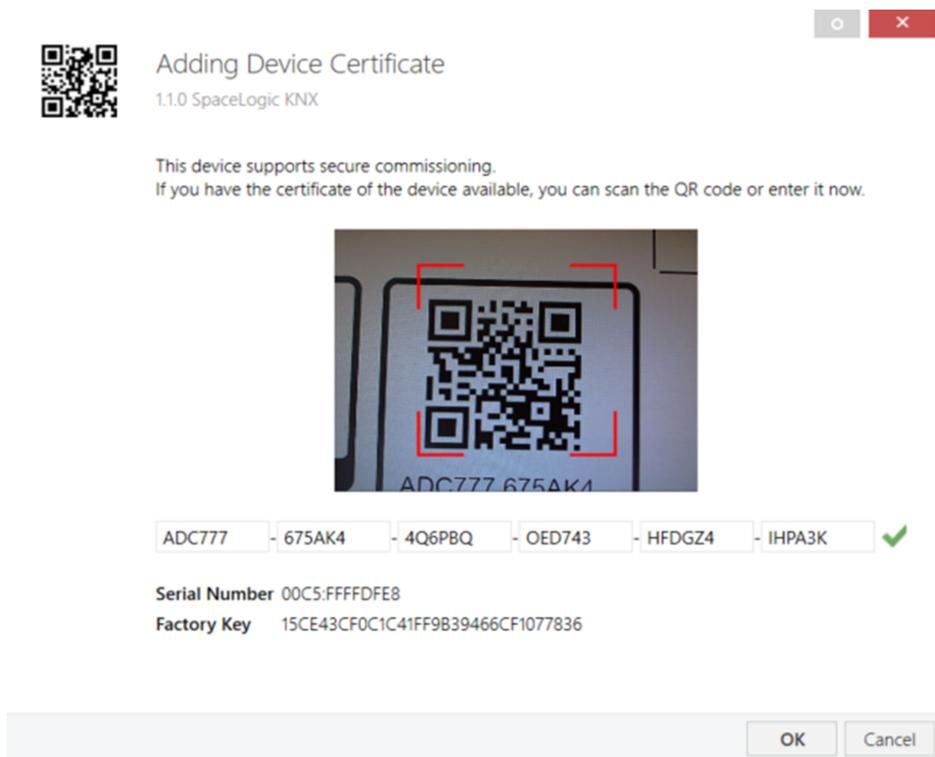
New Password
●●●●●●●●
Good

Confirm Password ✓
●●●●●●●●

OK Cancel

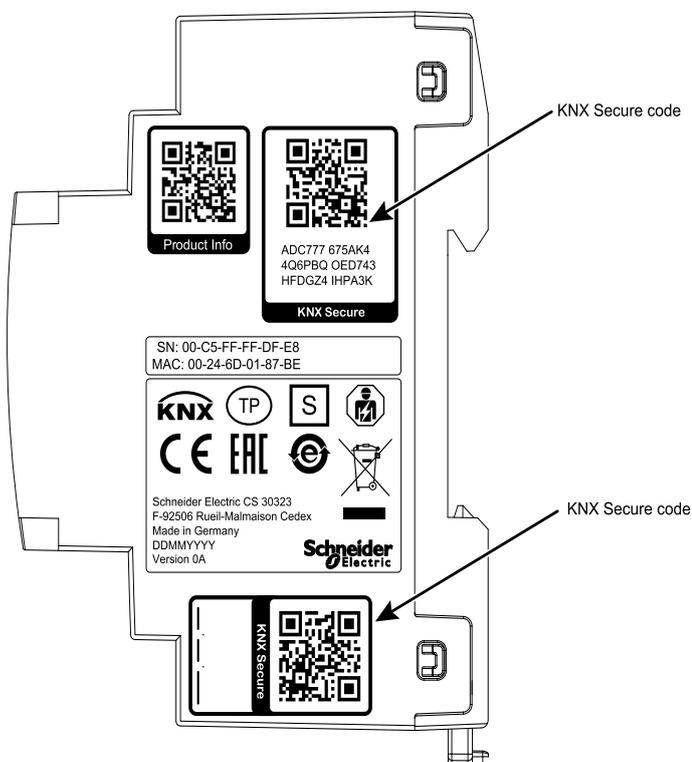
Questa password protegge il progetto ETS dall'accesso non autorizzato. Questa password non è una chiave utilizzata per la comunicazione KNX. È possibile ignorare l'immissione della password con **Annulla**, ma ciò non è consigliato per motivi di sicurezza.

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



Il certificato viene stampato come testo sul dispositivo. Può inoltre essere analizzato comodamente dal codice QR stampato tramite una telecamera collegata al PC che esegue ETS.

Il codice KNX Secure si trova sul lato destro del dispositivo. Il piccolo adesivo con codice KNX Secure con campo di etichettatura nella parte inferiore del dispositivo può essere rimosso a scopo di documentazione.



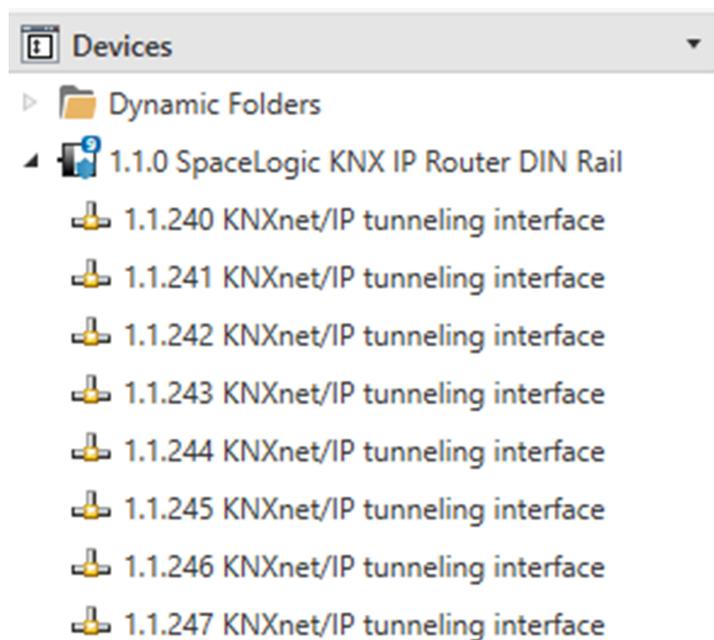
L'elenco di tutti i certificati dei dispositivi può essere gestito nella finestra ETS **PanoramicaProgetti > Sicurezza**.

Questa chiave iniziale è necessaria per mettere in sicurezza un dispositivo dall'inizio. Anche se il download ETS viene registrato da terzi, il terzo non ha accesso ai dispositivi protetti in seguito. Durante il primo download sicuro, la chiave iniziale viene sostituita dal ETS con una nuova, generata singolarmente per ogni dispositivo. Ciò impedisce a persone o dispositivi che conoscono la chiave iniziale di accedere al dispositivo. La chiave iniziale viene riattivata solo dopo un reset del master.

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

Parametri aggiuntivi

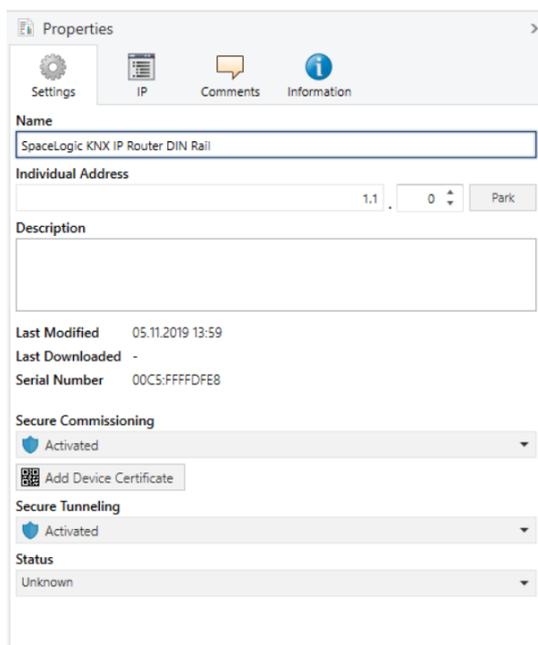
Nel ETS, oltre alla finestra di dialogo dei parametri, vengono visualizzate alcune impostazioni nella finestra di dialogo delle proprietà (ai bordi della schermata). Le impostazioni IP possono essere effettuate qui. Gli indirizzi aggiuntivi per le connessioni dell'interfaccia sono visualizzati nella vista della topologia.



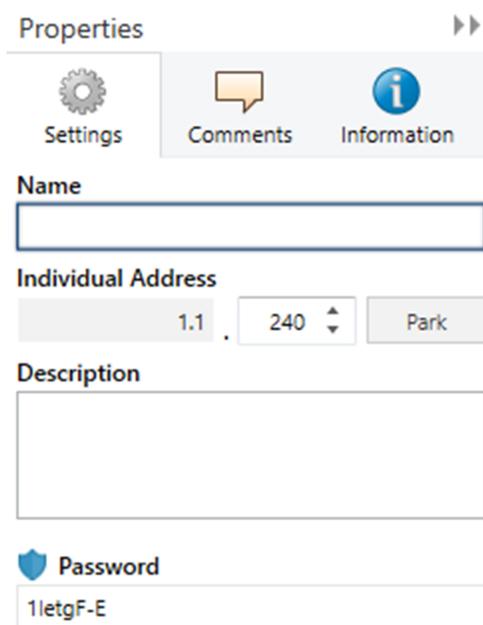
Ogni singolo indirizzo KNX può essere modificato facendo clic sulla voce dell'elenco e digitando l'indirizzo desiderato nel campo di testo **Indirizzo individuale**. Se il riquadro del campo di testo diventa rosso dopo aver immesso l'indirizzo, l'indirizzo è già stato acquisito nel progetto ETS.

NOTA: Accertarsi che nessuno degli indirizzi precedenti sia già presente nell'installazione KNX.

Facendo clic sulla voce del dispositivo Router IP KNX nella vista della topologia dei progetti ETS, sul lato destro della finestra ETS viene visualizzata una colonna informativa **Proprietà**. Nella panoramica **Impostazioni**, è possibile modificare il nome del dispositivo.



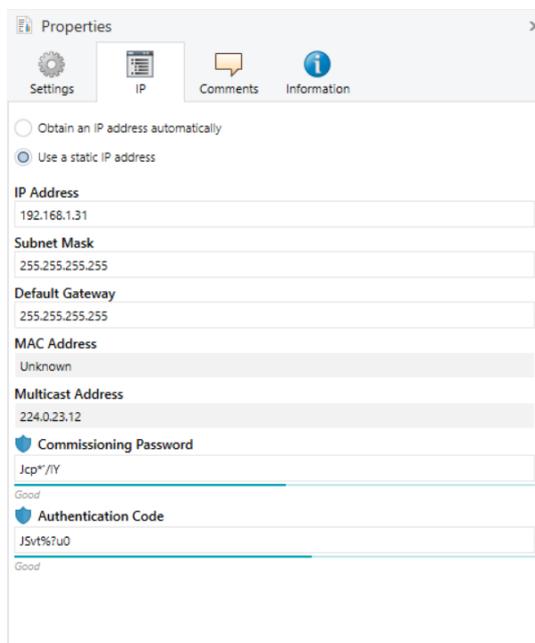
Se è attivato il tunneling sicuro, viene creata automaticamente una password univoca per ogni tunnel. Queste password possono essere visualizzate sotto la panoramica **Impostazioni**, quando viene selezionato un tunnel.



All'interno della panoramica **IP**, è possibile modificare le opzioni specifiche della rete IP del Router IP KNX.

Modificando **Ottenere un indirizzo IP automaticamente (tramite DHCP)** in **Usare un indirizzo IP statico** (indirizzo IP statico), l'indirizzo IP, la subnet mask e il gateway predefinito possono essere impostati liberamente.

NOTA: Tutte le modifiche nel menu **Proprietà** diventano effettive solo dopo il download riuscito dell'applicazione.



Indirizzo IP

Qui è possibile inserire l'indirizzo IP del Router IP KNX. Utilizzato per indirizzare il dispositivo tramite la rete IP (LAN). L'indirizzamento IP deve essere coordinato con l'amministratore della rete.

Subnet mask

Immettere qui la subnet mask. Il dispositivo utilizza i valori immessi in questa maschera per determinare se vi è un partner di comunicazione nella rete locale. Se nella rete locale non vi è alcun partner, il dispositivo non invierà i telegrammi direttamente al partner, ma al gateway che inoltra il telegramma.

Gateway predefinito

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

Indirizzo multicast di inoltro

Questo indirizzo è utilizzato per l'inoltro di telegrammi su IP. A tal fine, l'indirizzo IP multicast **224.0.23.12** è stato riservato (KNXnet/IP) all'IANA (Internet Assigned Numbers Authority). Se è necessario un indirizzo IP multicast diverso, deve essere compreso nell'intervallo compreso tra **239.0.0.0** e **239.255.255.255**.

Esempio di assegnazione di indirizzi IP

Per accedere al Router IP KNX è necessario utilizzare un PC.

Indirizzo IP del PC	192.168.1.30
Subnet del PC	255.255.255.0

Il Router IP KNX si trova nella stessa LAN, ovvero utilizza la stessa subnet. La subnet vincola gli indirizzi IP che possono essere assegnati. In questo esempio, l'indirizzo IP del Router IP KNX deve essere **192.168.1.xx**, dove xx può essere un numero compreso tra 1 e 254 (ad eccezione di 30, già utilizzato dal PC client). È necessario assicurarsi che nessun indirizzo IP venga assegnato due volte.

Indirizzo IP del Router IP KNX	192.168.1.31
Subnet del Router IP KNX	255.255.255.0

Accesso remoto

È possibile l'accesso remoto via Internet con il Router IP KNX.

AVVISO

DANNI MATERIALI DOVUTI ALL'ACCESSO NON AUTORIZZATO ALL'IMPIANTO KNX

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

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

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

Il mancato rispetto delle presenti istruzioni può comportare pericolo di danni all'attrezzatura.

Accesso VPN

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

Vantaggi della VPN:

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

Requisiti per la configurazione di una connessione VPN:

- Connessione Internet.
- Il dispositivo portatile e il router sono abilitati per una connessione VPN (client VPN installato).

Finestra di dialogo dei parametri ETS

Con ETS è possibile impostare i seguenti parametri:

Impostazioni generali

1.1.0 SpaceLogic KNX IP Router DIN Rail > General settings

Description Note: For device name and IP settings see dialog "Properties"

General settings Manual operation on device Enabled with time limit 1 min

Routing (KNX -> IP)

Routing (IP -> KNX)

Funzionamento manuale sul dispositivo

Questo parametro imposta la durata della modalità manuale. Al termine, viene ripristinata la modalità di funzionamento normale.

Inoltro (KNX → IP)

1.1.0 SpaceLogic KNX IP Router DIN Rail > Routing (KNX -> IP)

Description Group telegrams (main groups 0 to 13) Filter

General settings Group telegrams (main groups 14 to 31) Filter

Routing (KNX -> IP) Individual addressed telegrams Filter

Routing (IP -> KNX) Broadcast telegrams Block Route

Acknowledge (ACK) of group telegrams Always Only if routed

Acknowledge (ACK) of individual addressed telegrams Only if routed

Telegrammi di gruppo (gruppo principale da 0 a 13)

Disabilita	Nessun telegramma di gruppo di questi gruppi principali è inoltrato a IP.
Inoltra	Tutti i telegrammi di gruppo di questi gruppi principali vengono inoltrati a IP a prescindere dalla tabella dei filtri. Questa impostazione è solo a scopo di prova.
Filtra	La tabella dei filtri serve a verificare se il telegramma di gruppo ricevuto deve essere inoltrato o meno a IP.

Telegrammi di gruppo (gruppi principali da 14 a 31)

Disabilita	Nessun telegramma di gruppo di questi gruppi principali è inoltrato a IP.
Inoltra	Tutti i telegrammi di gruppo di questi gruppi principali vengono inoltrati a IP a prescindere dalla tabella dei filtri. Questa impostazione è solo a scopo di prova.
Filtra	La tabella dei filtri serve a verificare se il telegramma di gruppo ricevuto deve essere inoltrato o meno a IP.

Telegrammi indirizzati singolarmente

<i>Disabilita</i>	Nessun telegramma indirizzato singolarmente viene inoltrato a IP.
<i>Inoltra</i>	Tutti i telegrammi indirizzati individualmente vengono inoltrati a IP.
<i>Filtra</i>	Il singolo indirizzo permette di verificare se il telegramma indirizzato singolarmente e ricevuto deve essere inoltrato a IP.

Telegrammi broadcast

<i>Disabilita</i>	Nessun telegramma broadcast ricevuto è inoltrato a IP.
<i>Inoltra</i>	Tutti i telegrammi broadcast ricevuti vengono inoltrati a IP.

Conferma (ACK) di telegrammi di gruppo

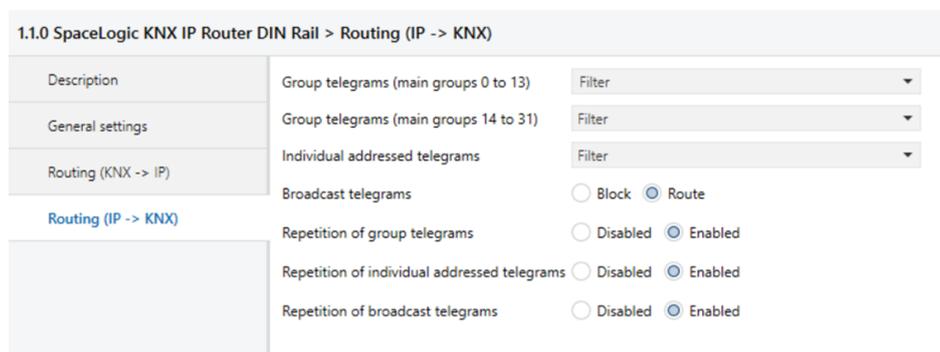
<i>Sempre</i>	Viene generata una conferma per ogni indirizzo di gruppo ricevuto (da KNX).
<i>Solo se inoltrato</i>	Una conferma viene generata solo per gli indirizzi di gruppo ricevuti (da KNX) se inoltrati a IP.

Conferma (ACK) di telegrammi inviati singolarmente

<i>Sempre</i>	Viene generata una conferma per ogni telegramma inviato singolarmente e ricevuto (da KNX).
<i>Solo se inoltrato</i>	Una conferma viene generata solo per gli indirizzi di gruppo inviati singolarmente e ricevuti (da KNX) se inoltrati a IP.
<i>Risposta con NACK</i>	A ogni telegramma inviato singolarmente e ricevuto (da KNX) viene risposto con NACK (non confermare). Ciò significa che non è possibile comunicare con telegrammi inviati singolarmente sulla linea KNX corrispondente. La comunicazione di gruppo (telegrammi di gruppo) non è interessata. Questa impostazione può essere utilizzata per bloccare i tentativi di manipolazione.

NOTA: Quando si usa **Risposta con NACK**, non è più possibile accedere al dispositivo via TP KNX. La configurazione deve essere eseguita tramite IP. Ciò può essere utilizzato per rendere più sicura un'installazione.

Inoltro (IP → KNX)



Telegrammi di gruppo (gruppo principale da 0 a 13)

<i>Disabilita</i>	Nessun telegramma di gruppo di questi gruppi principali viene inoltrato a KNX.
<i>Inoltra</i>	Tutti i telegrammi di gruppo di questi gruppi principali vengono inoltrati a KNX indipendentemente dalla tabella dei filtri. Questa impostazione viene utilizzata solo a scopo di prova.
<i>Filtra</i>	La tabella dei filtri serve a verificare se il telegramma di gruppo ricevuto deve essere inoltrato a KNX.

Telegrammi di gruppo (gruppi principali da 14 a 31)

<i>Disabilita</i>	Nessun telegramma di gruppo di questi gruppi principali viene inoltrato a KNX.
<i>Inoltra</i>	Tutti i telegrammi di gruppo di questi gruppi principali vengono inoltrati a KNX indipendentemente dalla tabella dei filtri. Questa impostazione viene utilizzata solo a scopo di prova.
<i>Filtra</i>	La tabella dei filtri serve a verificare se il telegramma di gruppo ricevuto deve essere inoltrato a KNX.

Telegrammi indirizzati singolarmente

<i>Disabilita</i>	Nessun telegramma indirizzato singolarmente viene inoltrato a KNX.
<i>Inoltra</i>	Tutti i telegrammi indirizzati individualmente vengono inoltrati a KNX.
<i>Filtra</i>	Il singolo indirizzo permette di verificare se il telegramma indirizzato singolarmente e ricevuto deve essere inoltrato a KNX.

Telegrammi broadcast

<i>Disabilita</i>	Nessun telegramma broadcast ricevuto è inoltrato a KNX.
<i>Inoltra</i>	Tutti i telegrammi broadcast ricevuti vengono inoltrati a KNX.

Ripetizione di telegrammi di gruppo

<i>Disabilitato</i>	Il telegramma di gruppo ricevuto non viene rinviato a KNX in caso di guasto.
<i>Abilitato</i>	In caso di guasto, il telegramma di gruppo ricevuto viene rinviato fino a tre volte.

Ripetizione di telegrammi indirizzati singolarmente

<i>Disabilitato</i>	In caso di guasto, il telegramma indirizzato singolarmente e ricevuto non viene rinviato a KNX.
<i>Abilitato</i>	In caso di guasto, il telegramma indirizzato singolarmente e ricevuto viene rinviato fino a tre volte.

Ripetizione di telegrammi di broadcast

<i>Disabilitato</i>	In caso di guasto, il telegramma di broadcast ricevuto non viene rinviato a KNX.
<i>Abilitato</i>	In caso di guasto, il telegramma di broadcast ricevuto viene rinviato fino a tre volte.

Programmazione

Il Router IP KNX può essere programmato in diversi modi dal ETS:

Tramite bus KNX

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

Tramite KNXnet/IP Tunneling

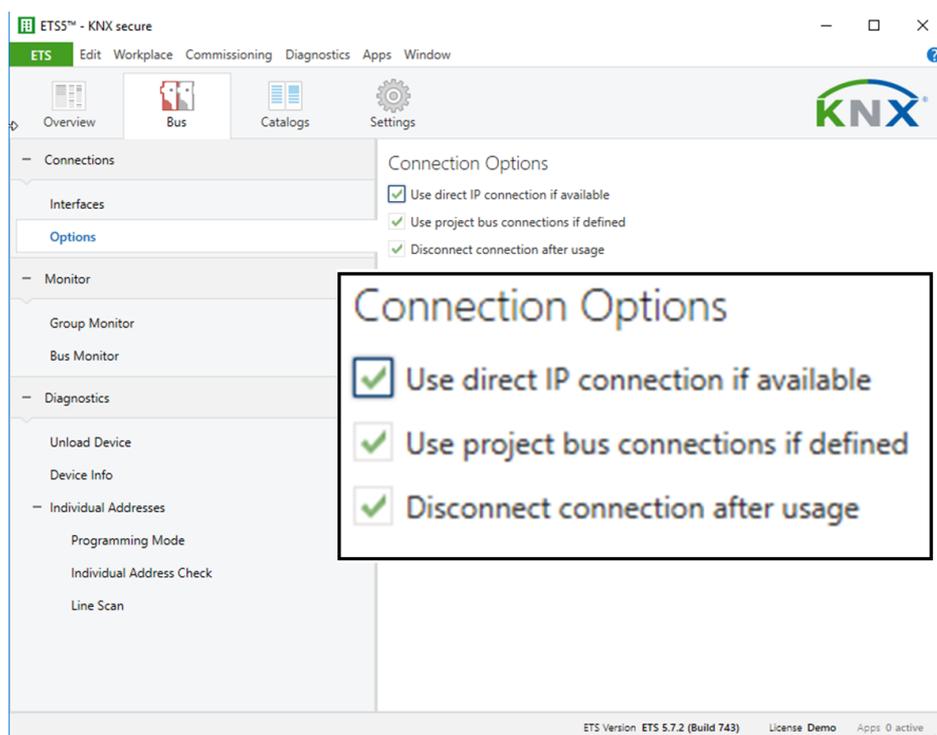
Non è richiesta alcuna interfaccia aggiuntiva. La programmazione tramite KNXnet/IP Tunneling è possibile se il dispositivo ha già una configurazione IP valida (ad esempio tramite DHCP). In questo caso, il dispositivo viene visualizzato nella configurazione dell'interfaccia del ETS e deve essere selezionato.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

Via KNXnet/Inoltro IP

La programmazione tramite KNXnet/inoltro IP è possibile se il dispositivo ha già una configurazione IP valida (ad esempio, tramite DHCP o IP automatico). Nel ETS, l'interfaccia di inoltro viene visualizzata se è disponibile almeno un dispositivo sulla rete che supporta l'inoltro. Il nome dell'interfaccia di rete viene visualizzato nel PC come descrizione. Se l'inoltro è selezionato come interfaccia, la programmazione effettuata dal progetto ETS avviene come con altri dispositivi. In questo caso, LAN viene utilizzato come supporto KNX come TP. Non è necessario alcun dispositivo di interfaccia aggiuntivo.

Tramite connessione IP diretta

Mentre KNXnet/IP Tunneling e KNXnet/inoltro IP è limitato alla velocità di KNX TP, il dispositivo può essere caricato tramite una connessione IP diretta ad alta velocità. La connessione IP diretta è possibile se il dispositivo dispone già di una configurazione IP valida e di un indirizzo singolo (questo può anche essere l'indirizzo individuale predefinito). Per farlo, selezionare **Usare connessione IP diretta, se disponibile** nel menu ETS **BusConnessioni Opzioni**. Il download viene eseguito direttamente nel dispositivo e non è visibile nel monitor del gruppo ETS.



NOTA: A causa dei tempi di trasmissione notevolmente più brevi, si consiglia di eseguire download via IP.

Software open source utilizzato nel prodotto

Il prodotto contiene, tra le altre cose, file software open source, come specificato di seguito, sviluppati da terzi e concessi in licenza con una licenza software open source. Questi file software open source sono protetti da copyright. Il diritto d'uso del software open source è disciplinato dalle condizioni di licenza applicabili del software open source.

La conformità alle condizioni di licenza consentirà all'utente di utilizzare il software open source come previsto nella licenza. In caso di conflitti tra altre condizioni di licenza di Schneider Electric applicabili al prodotto e le condizioni di licenza del software open source, prevalgono queste ultime. Il software open source è royalty-free (ovvero non sono previsti oneri per l'esercizio dei diritti concessi in licenza). Di seguito è riportato l'elenco dei file software open source inclusi nel prodotto e dei rispettivi termini e condizioni applicabili:

Elenco dei file software open source	Licenze applicabili
curve25519-donna	Vedere https://github.com/agl/curve25519-donna

Se il software open source contenuto in questo prodotto è concesso in licenza in base a GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) o a qualsiasi altra licenza software open source che richiede la disponibilità del codice sorgente, è possibile scaricare il codice sorgente corrispondente del software open source dal seguente link:

Elenco dei file software open source	Accesso ai file software open source
curve25519-donna	Vedere https://github.com/agl/curve25519-donna

Garanzia sull'ulteriore utilizzo del software open source

Schneider Electric SE e tutte le sue filiali ("Schneider Electric Group") non forniscono alcuna garanzia per il software open source contenuto in questo prodotto, se utilizzato in modo diverso da quello previsto dal gruppo Schneider Electric. Le licenze sopra elencate definiscono la garanzia, se esistente, degli autori o dei licenziatari del software open source. Il gruppo Schneider Electric disconosce espressamente qualsiasi garanzia per difetti causati dalla modifica di software open source o della configurazione del prodotto. Sono escluse eventuali rivendicazioni di garanzia nei confronti del gruppo Schneider Electric nel caso in cui il software open source contenuto in questo prodotto violi i diritti di proprietà intellettuale di terzi.

Verrà fornita assistenza tecnica, eventualmente, solo per software non modificato.

Direttiva RAEE



Non smaltire l'apparecchio con i rifiuti domestici, ma conferirlo a un centro di raccolta ufficiale.

Il riciclaggio professionale protegge le persone e l'ambiente da eventuali effetti nocivi.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

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

www.schneider-electric.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.

© 2019 – Schneider Electric. Tutti i diritti sono riservati.

MTN6500-0103_SW_EN