Manuale installatore

01548
Router KNX IP

BUILDING AUTOMATION

WELL-CONTACT PLUS

Indice

1. **Descrizione del prodotto** . . . 4
   - 1.1 Vista frontale del dispositivo . . . 4
   - 1.2 Segnalazioni dei LED . . . 5
   - 1.3 LED funzioni speciali . . . 6
   - 1.4 Messa in servizio . . . 7
   - 1.5 Secure Commissioning . . . 8
   - 1.6 Note importanti . . . 8
   - 1.8 Conservazione del Certificato del dispositivo . . . 9
   - 1.9 Riepilogo delle funzioni . . . 9

2. **KNXnet/IP** . . . 10
   - 2.1 IP (Secure) Tunnelling . . . 10
   - 2.2 IP (Secure) Routing . . . 10
   - 2.3 Aggiornamento del firmware IP . . . 10

3. **KNX Secure** . . . 10

4. **Descrizione del funzionamento** . . . 11
   - 4.1 Applicazione del router IP Secure . . . 11
   - 4.2 Rete IP . . . 11
   - 4.3 Installazione della rete KNX . . . 12
   - 4.4 Aggiunta del Certificato del dispositivo . . . 13
   - 4.5 Programmazione . . . 14
     - 4.5.1 Programmazione dell'Indirizzo individuale (e applicazione) . . . 14
     - 4.5.2 Configurazione IP . . . 15
   - 4.6 Funzioni speciali . . . 16
     - 4.6.1 Funzione manuale . . . 16
     - 4.6.2 Reset di fabbrica . . . 17
     - 4.6.3 Richiesta di aggiornamento del firmware IP . . . 17

5. **Database ETS** . . . 18
   - 5.1 Generale . . . 18
   - 5.2 Linea principale (IP) . . . 19
   - 5.3 Linea secondaria (KNX TP) . . . 19
   - 5.4 Assegnazione dell'indirizzo per l'IP (Secure) Tunnelling . . . 21

6. **Front-end Web** . . . 22
   - 6.1 Protezione del front-end Web di 01548 . . . 22
   - 6.2 Accesso al front-end Web di 01548 . . . 22
     - 6.2.1 Con Esplora risorse di Windows . . . 22
     - 6.2.2 Con l'indirizzo IP . . . 23
     - 6.2.3 Con l'indirizzo MAC . . . 23
   - 6.3 Informazioni sul dispositivo . . . 24
   - 6.4 KNX . . . 24
   - 6.5 Aggiornamento del firmware IP . . . 25

7. **Glossario** . . . 27

8. **Informazioni tecniche** . . . 28
   - 8.1 Stato alla consegna . . . 28
   - 8.2 Scheda dati . . . 29

9. **FAQ** . . . 30

1. Descrizione del prodotto

La funzione di base del router 01548 è quella di far interagire tra loro dispositivi di sistemi KNX IP/Ethernet (linea principale) con quelli di sistemi KNX bus TP (linea secondaria). È alimentato dal bus TP e non necessita di alimentazione esterna. Il router è in grado di filtrare il traffico in base al tipo di installazione nella gerarchia del sistema bus e in base alle tabelle filtro incorporate per la comunicazione orientata ai gruppi. La configurazione dalla linea secondaria può essere disattivata. Utilizzato come interfaccia, il dispositivo effettua funzioni di configurazione, messa in servizio, visualizzazione, protocollo e diagnostica. Gli stati operativi e di filtro, i malfunzio¬namenti e gli errori di comunicazione sono indicati mediante LED. Il dispositivo supporta messaggi con APDU di lunghezza fino a 240 byte e presenta il tasto “Function” per disattivare temporaneamente il filtro durante la messa in servizio o la risoluzione dei problemi.

Il dispositivo è KNXnet/IP (Secure) Routing e Tunnelling ed è provvisto di un apposito QR code da utilizzare con ETS (versione 5.5 e successive) in fase di con¬figurazione. È possibile attivare il Secure Tunnelling (tunnelling protetto), il Secure Commissioning (messa in servizio protetta) e la protezione della dorsale IP.

Il router 01548 viene visualizzato in rete; via web si possono gestire le impostazioni del dispositivo, attivare le funzionalità e visualizzare la cronologia del traffico bus entro i 60 minuti. Inoltre, la funzione di “bootloader”, consente l’aggiornamento da remoto del firmware tramite IP/Ethernet.

1.1 Vista frontale del dispositivo

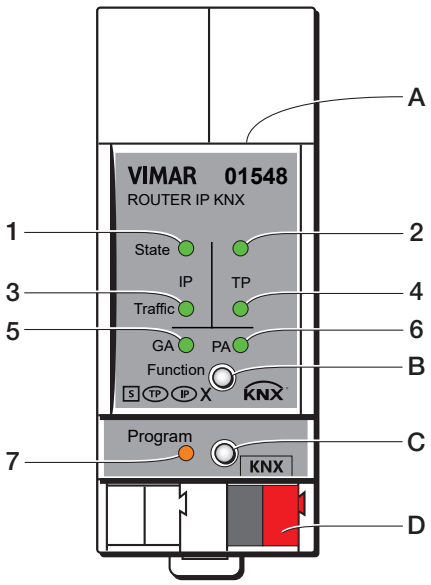


Figura 1: Vista frontale

Tabella 1: Elementi del dispositivo

LED	
1	Stato IP (linea principale)
2	Stato bus KNX TP (linea secondaria)
3	Traffico dati IP (linea principale)
4	Traffico dati KNX TP (linea secondaria)
5	Routing indirizzo di gruppo*
6	Routing indirizzo individuale (fisico)
7	LED programmazione

Tasti/Connettori	
A	Connettore Ethernet
B	Tasto funzione
C	Tasto programmazione
D	Connettore KNX TP

*solo telegrammi di gruppo con gruppi principali 0...13

Descrizione del prodotto

1.2 Segnalazioni dei LED

Nella tabella riassuntiva che segue sono descritte le segnalazioni dei LED visibili durante il funzionamento normale. Le segnalazioni dei LED per le Funzioni Speciali sono descritte nel capitolo successivo.

Tabella 2: LED nel funzionamento normale

Numero	Led	Colore	Spiegazione/Range
1	**Stato IP (linea principale)**	verde	Linea IP OK (connessione stabilita)
		arancio	Funzione manuale attiva
		< spento >	Connessione IP assente
2	**Stato bus KNX TP (linea secondaria)**	verde	Linea secondaria OK
		< spento >	Linea secondaria non collegata
3	**Traffico dati IP (linea principale)**	verde lampeggiante	La quantità di traffico dati è indicata dal lampeggio
		< spento >	Assenza di traffico dati
4	**Traffico dati KNX TP (linea secondaria)**	verde lampeggiante	La quantità di traffico dati è indicata dal lampeggio
		rosso lampeggiante	Errore di trasmissione (BUSY, NACK, IACK mancante)
		< spento >	Assenza di traffico dati
5	**Routing indirizzo di gruppo**	verde	Tabella filtro attiva
		arancio	Inoltra tutti
		rosso	Blocca tutti
		< spento >	Il routing dei messaggi di gruppo cambia a seconda della linea principale o secondaria
6	**Routing indirizzo individuale (fisico)***	verde	Filtro attivo
		arancio	Inoltra tutti
		rosso	Blocca tutti
		< spento >	Il routing dei messaggi fisici cambia a seconda della linea principale o secondaria
7	**LED programmazione**	rosso	Modalità programmazione attiva
		rosso lampeggiante	Connessione IP assente
		< spento >	Modalità programmazione non attiva

*Il comportamento non è definito per i router che hanno una configurazione non valida, tipo l'Indirizzo individuale

1.3 LED funzioni speciali

Quando è attiva una funzione speciale sono accesi solo i LED qui descritti. Gli altri LED sono spenti.

Tabella 3: Stato dei LED nella funzione manuale

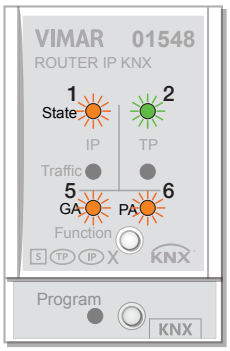
Numero	Led	Colore	Commento	
1	**Stato IP**	arancio	Diventa rosso se non è connesso	
2	**Stato bus KNX TP**	verde		
5	**Routing indirizzo di gruppo**	verde: filtro arancio: inoltra tutti rosso: blocca tutti		
6	**Routing indirizzo individuale**			

Tabella 4: Stato dei LED per il ripristino dei valori predefiniti di fabbrica dopo la prima pressione del tasto funzione

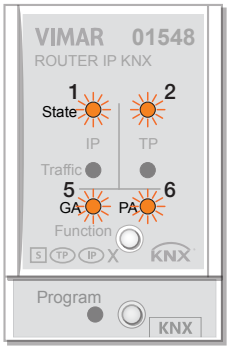
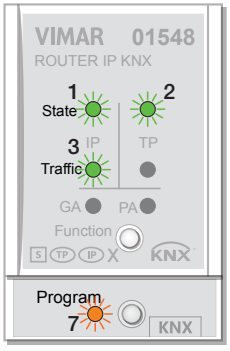
Numero	Led	Colore	Commento	
1	**Stato IP**	arancio	Diventa rosso se non è connesso	
2	**Stato bus KNX TP**	arancio		
5	**Routing indirizzo di gruppo**	verde: filtro arancio: inoltra tutti rosso: blocca tutti		
6	**Routing indirizzo individuale**			

Tabella 5: Stato dei LED per l'aggiornamento del firmware

Numero	LED	Colore	Commento	
1	**Stato IP**	verde	lampeggiante, in seguito acceso	
2	**Stato bus KNX TP**	verde lampeggiante		
3	**Traffico dati IP**	verde		
7	**Led di programmazione**	rosso		

1.4 Messa in servizio

Per la messa in servizio con le impostazioni predefinite tenere presente quanto segue:

- Tutti i messaggi sono bloccati perché la tabella filtri non è definita
- Il tempo di spegnimento temporizzato della funzione manuale è 120 min
- L'indirizzo individuale è 15.15.0
- Per l'attivazione della funzione di sicurezza e del Secure Commissioning è necessario il Certificato del dispositivo
- L'attivazione della funzione di sicurezza richiede uno specifico numero minimo di versione ETS

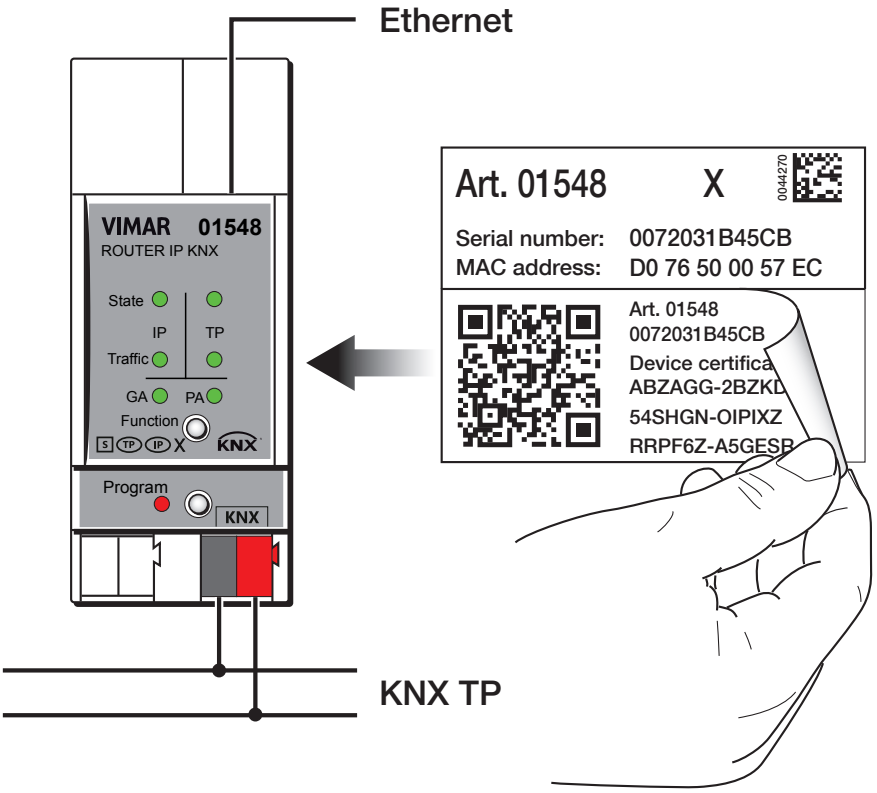


Figura 2: Schema di collegamento

✓ Per avviare un download della configurazione sicura, è necessario prima attivare il Secure Commissioning nel progetto ETS. Senza attivazione, il dispositivo 01548 si comporterà come il 01547.1 (senza supporto di KNX Secure).

✓ Leggere anche il capitolo “1.6 Note importanti” prima di mettere in funzione il dispositivo.

1.5 Secure Commissioning

Per avviare il download sicuro delle impostazioni di configurazione e/o dell'indirizzo individuale, è necessario aggiungere prima il Certificato individuale del dispositivo 01548 al progetto ETS. Per aggiungerlo, il progetto ETS deve essere protetto da password.

✓ Il download sicuro è possibile solo dopo l'attivazione del Secure Commissioning.

✓ Per l'attivazione del Secure Commissioning è necessario il Certificato individuale del dispositivo.

✓ I certificati dispositivo possono essere aggiunti solo a un progetto ETS protetto da password.

Se non è impostata una password per il progetto, il Secure Commissioning non può essere attivato. I progetti ETS con Secure Commissioning e/o la funzione Security impostati su attivo, richiedono sempre una password di progetto. Se all'attivazione della funzione Security non risulta impostata alcuna password di progetto, ETS chiede di inserirne una.

Figura 3: Impostazione della password di progetto

✓ Il Certificato individuale del dispositivo è sempre incluso con il prodotto KNX Secure. Affinché il prodotto possa essere configurato dall'utente, è importante accertarsi di non perdere il Certificato del dispositivo (vedere il capitolo 1.7 Conservazione del Certificato del dispositivo).

1.6 Note importanti

Si consiglia di partecipare ai corsi standardizzati di un centro di formazione certificato per KNX prima di installare, programmare ed eseguire la messa in servizio di un sistema KNX. Il partecipante potrà acquisire le conoscenze e le competenze necessarie, richieste anche per eseguire la ricerca guasti, tramite esercitazioni pratiche.

Leggere attentamente questo capitolo prima del primo utilizzo e dell'installazione:

1.6.1 Installazione e messa in servizio

- Se il dispositivo viene danneggiato durante lo stoccaggio o il trasporto, le riparazioni dovranno essere eseguite esclusivamente da personale autorizzato.
- Una volta connesso al sistema bus KNX, il dispositivo entra in funzione con le impostazioni predefinite.
- Avvertenza: non collegare a una sorgente a 230 V. Il dispositivo è alimentato dal bus KNX e non necessita di altra alimentazione esterna.
- Il dispositivo deve essere installato e messo in servizio esclusivamente da un elettricista qualificato o da una persona autorizzata.
- Per la progettazione e la realizzazione di impianti elettrici attenersi alle specifiche, alle linee guida e alle normative applicabili locali vigenti.
- Per la configurazione, utilizzare l'ETS (o ETS Inside)

1.6.2 Montaggio e sicurezza

- Per il montaggio, utilizzare attrezzatura adeguata, conformemente a IEC60715.
- Installazione su guida DIN da 35 mm (TH35)
- Collegare la linea del bus KNX come per i consueti collegamenti di bus KNX con un cavo per bus KNX, da spelare e inserire in un connettore KNX TP.
- Non danneggiare gli isolamenti elettrici durante le operazioni di collegamento.
- Installare esclusivamente in luoghi asciutti.

1.6.3 Manutenzione

- Assicurare l'accessibilità al dispositivo per l'azionamento e l'ispezione visiva.
- Non aprire l'involucro esterno.
- Proteggere il dispositivo da umidità, sporco e danneggiamenti.
- Il dispositivo non richiede manutenzione.
- Se necessario, può essere pulito con un panno asciutto.

1.7 Conservazione del Certificato del dispositivo

Il Certificato del dispositivo si trova sull'etichetta apposta sul lato dell'involucro. Per evitare l'accesso non autorizzato, il Certificato del dispositivo deve essere tolto dal dispositivo dopo la messa in servizio. A questo scopo l'etichetta si compone di due parti, una fissa, che rimane applicata all'involucro (per l'identificazione), e una rimovibile (da conservare).

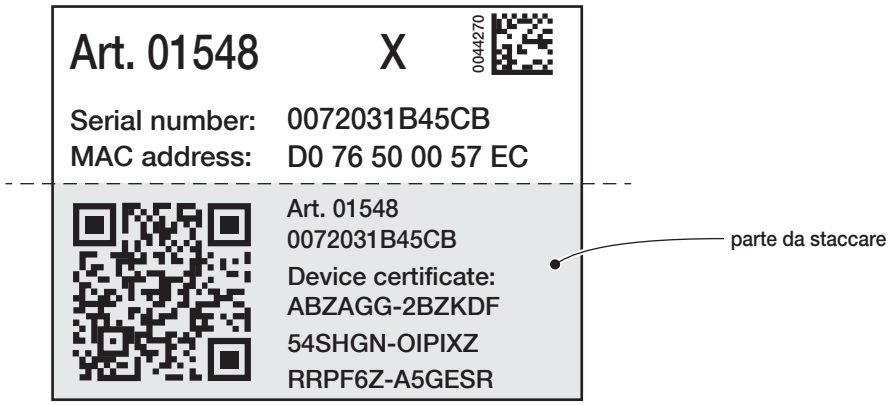


Figura 4: Etichetta con il Certificato del dispositivo

Dopo aver aggiunto il Certificato del dispositivo all'apposito elenco in ETS, conservare la parte rimossa dell'etichetta in un luogo sicuro. Nell'elenco dei Certificati dei dispositivi devono essere inclusi solo i certificati dei dispositivi KNX Secure utilizzati per i progetti ETS. ETS utilizzerà automaticamente i certificati corretti per la programmazione dei dispositivi.

Per identificare chiaramente il dispositivo dopo aver rimosso la parte staccabile, il numero di serie è stampato su entrambe le parti dell'etichetta, quella che è stata rimossa e quella che rimane sull'involucro.

✓ Se si perde la parte rimossa con il Certificato del dispositivo, questo sarà disponibile sono nel progetto ETS protetto da password.

✓ Attenzione! Se il Certificato del dispositivo viene perso e non può essere recuperato, cioè se la parte dell'etichetta rimossa non è più reperibile e si è persa anche la password del progetto, il dispositivo non potrà più essere utilizzato in modalità sicura (non sarà più possibile attivare la funzione Security). In tal caso, anche dopo aver eseguito un reset di fabbrica, il dispositivo potrà essere utilizzato solo in modalità non protetta, come dispositivo "normale".

1.8 Riepilogo delle funzioni

- Il Certificato del dispositivo garantisce che solo le persone autorizzate possano accedere al dispositivo 01548.
- Quando è attiva la funzione ETS “Secure Commissioning” i dati di configurazione vengono scaricati solo nel formato KNX Data Secure criptato.
- Attivazione di “IP Backbone Security” per la protezione del routing IP.
- Qualora si renda necessaria ulteriore protezione (ad esempio se la linea secondaria si trova all'esterno dell'edificio) è possibile disattivare completamente la configurazione di 01548 mediante la linea secondaria.
- 01548 supporta messaggi con APDU di lunghezza fino a 240 byte.
- 01548 sostituisce egregiamente un normale accoppiatore di linea/campo TP. Il grande vantaggio consiste nella possibilità di usare KNX IP come un supporto veloce per la dorsale KNX.
- 01548 funziona senza alimentazione esterna.
- Per il (Secure) Tunnelling IP è possibile effettuare quattro connessioni tunnelling in parallelo. Quando si attiva il Secure Tunnelling, diventa disponibile la protezione con password.
- Sono disponibili impostazioni che consentono di aumentare il flusso dei dati o diminuire il traffico elevato sul bus.
- L'invio di IACK sui messaggi inviati è configurabile.
- La ripetizione è configurabile per i messaggi fisici e per i messaggi di gruppo.
- È possibile sospendere temporaneamente il filtro dei dati semplicemente premendo il tasto funzione. Il filtro viene limitato per facilitare la messa in servizio, la ricerca guasti o per velocizzare la diagnostica in loco, inoltre l'accesso alle altre linee sarà possibile senza ulteriori download di ETS.
- Ritorno automatico al filtro dei messaggi di runtime alla fine del periodo di sospensione configurato (vedere la modalità Manuale). Questa funzionalità evita che si dimentichi di riattivare i filtri.
- UPnP Discovery consente l'individuazione del dispositivo 01548 nella rete IP.
- ETS riconosce il dispositivo 01548 come interfaccia di connessione al bus tramite una richiesta di ricerca di KNXnet/IP.
- Il firmware può essere facilmente aggiornato da un browser web.
- Il front-end Web disponibile fornisce impostazioni informative e consente di commutare il dispositivo in Modalità programmazione da remoto senza usare il tasto programmazione.
- Tramite il front-end Web è possibile visualizzare la cronologia del traffico bus entro i 60 minuti.
- Quando è attiva la funzione Security, il front-end Web può essere usato in modalità limitata o completamente disattivato.
- 01548 supporta KNXnet/IP, ARP, ICMP, IGMP, HTTP, UPnP discovery, UDP/IP, TCP/IP, DHCP e AutoIP.

2. KNXnet/IP

La presenza del protocollo Internet (IP) ha reso possibile la definizione del protocollo KNXnet/IP Come documentato nelle specifiche del protocollo KNXnet/IP, i dati KNX possono essere trasmessi incapsulati in pacchetti IP. È possibile utilizzare reti Ethernet per eseguire il routing e il tunnelling dei dati KNX.

I router KNX IP sono molto simili agli accoppiatori di linea TP. La sola differenza è che i primi utilizzano il mezzo trasmissivo IP invece del TP e il protocollo di comunicazione KNXnet/IP. Per questo motivo, le interfacce IP e i router IP rappresentano un'ottima alternativa alle interfacce dati USB e agli accoppiatori di linea/campo TP. Una dorsale TP può essere completamente sostituita da una linea dorsale IP veloce basata su Ethernet. I dispositivi terminali KNX possono essere integrati direttamente tramite IP. Queste caratteristiche rendono Ethernet un efficace mezzo trasmissivo KNX.

2.1 IP (Secure) Tunnelling

La tecnologia KNXnet/IP offre la possibilità di eseguire connessioni point-to-point per ETS (connessioni IP Tunnelling) oppure, ad esempio, tra il sistema di supervisione e l'impianto KNX. All'attivazione di “Secure Tunnelling” queste connessioni diventano connessioni IP Secure Tunnelling. Sono protette mediante crittografia e l'utilizzo di password supplementari.

2.2 IP (Secure) Routing

L'IP Routing è il protocollo KNXnet/IP per connettere tra loro le linee e le aree KNX mediante reti IP. In questo caso, il protocollo KNXnet/IP determina la comunicazione KNX IP. L'utilizzo dell'IP Secure Routing comporta che la comunicazione di runtime su KNX IP sia interamente criptata secondo il meccanismo KNX IP Secure.

2.3 Aggiornamento del firmware IP

Grazie alla funzione di bootloader IP è possibile eseguire gli aggiornamenti del firmware da remoto e la riscrittura del contenuto della memoria flash tramite una connessione IP. Non si tratta di un semplice download dell'applicazione. Vengono scaricati lo stack di comunicazione e il software applicativo.

La procedura di aggiornamento del firmware tramite IP può essere eseguita dal front-end Web di 01548, che è indipendente dall'ETS e che utilizza messaggi speciali per velocizzare il processo. Ai fini della protezione questo processo utilizza una crittografia speciale.

3. KNX Secure

La tecnologia KNX Secure aggiunge un ulteriore livello di sicurezza all'impianto KNX, sia durante la messa in servizio sia per gli impianti KNX in esecuzione. La differenza tra i dispositivi KNX normali e i dispositivi KNX Secure è che questi ultimi sono in grado di criptare e decriptare i dati.

Tutti i dispositivi KNX Secure supportano la modalità protetta. Il dispositivo KNX Secure è in grado di criptare/decriptare i dati soltanto quando questa modalità è attiva. Per l'attivazione sono necessari i certificati del dispositivo (vedere il capitolo 1.5 Secure Commissioning).

I messaggi KNX criptati dai dispositivi KNX Secure sono definiti messaggi KNX Secure. Per quanto riguarda entrambi i meccanismi di KNX Security, KNX IP Secure e KNX Data Secure, si possono distinguere due tipi di crittografia:

- KNX IP Secure può essere applicato solo al mezzo trasmissivo KNX IP. I messaggi KNX vengono inviati come frame IP criptati, detti anche dati interamente criptati (indipendentemente dall'utilizzo di KNX Data Secure).
- KNX Data Secure può essere applicato a qualsiasi mezzo trasmissivo KNX. La comunicazione end-to-end tra i dispositivi è criptata. Grazie a una chiave di sicurezza individuale, i dispositivi terminali criptano/decriptano parti dei loro dati. Quindi solo i dispositivi con indirizzi di gruppo identici possono criptare/decriptare i dati.

Per la programmazione di un dispositivo KNX Secure, ETS deve conoscere sia il relativo codice di fabbrica (FDSK) sia il relativo numero di serie. Tuttavia non è necessario inserire il codice di fabbrica né il numero di serie, in quanto ETS recupera automaticamente queste informazioni dal Certificato del dispositivo.

Il Certificato del dispositivo è un codice di 32 caratteri specifico del dispositivo e contiene il numero di serie e il codice FDSK (Factory Default Setup Key, codice di configurazione predefinito di fabbrica). Il numero di serie e il codice FDSK non possono essere modificati. ETS recupera il codice FDSK mediante il Certificato del dispositivo (vedere il capitolo 1.5 Secure Commissioning).

Dopo che un dispositivo KNX Secure è stato aggiunto a un progetto ETS e dopo che il relativo Certificato del dispositivo è stato aggiunto, ETS imposta autonomamente il Tool Key (Codice strumento) del progetto. Il Tool Key non è modificabile. Può essere ripristinato il relativo FDSK soltanto mediante un reset di fabbrica (vedere il capitolo 4.6.2 Reset di fabbrica).

✓ Non è possibile utilizzare una combinazione di comunicazione protetta e non protetta sullo stesso indirizzo di gruppo.

✓ Una combinazione di router KNX IP Secure in modalità protetta e router KNX IP Secure in modalità normale o semplicemente router KNX IP normali, non funziona.

4. Descrizione del funzionamento

Negli impianti di rete KNX, il router 01548 viene utilizzato come accoppiatore di linea/campo KNX IP per accoppiare KNX IP e KNX TP (vedere anche il capitolo 2.2 IP (Secure) Routing). Può essere utilizzato normalmente senza l'attivazione della funzione Security e nei progetti ETS in cui la funzione Security sia attiva. Dopo la connessione a KNX TP, il dispositivo 01548 funziona con le sue impostazioni predefinite. È necessario impostare un indirizzo individuale corretto. Sono consentiti solo indirizzi individuali x.y.0.

4.1 Applicazione del router IP Secure

Quando 01548 riceve messaggi (ad esempio durante la messa in servizio) che utilizzano gli indirizzi individuali come indirizzi di destinazione, confronta gli indirizzi individuali del destinatario con il proprio indirizzo individuale e decide se deve inoltrare i messaggi oppure no.

Quando 01548 riceve dati che utilizzano gli indirizzi di gruppo come indirizzi individuali, reagisce in base alle impostazioni dei parametri. Durante il funzionamento normale (con il routing dei dati di gruppo impostato per filtrarli), 01548 inoltra solo i messaggi i cui indirizzi di gruppo sono inseriti nella tabella del filtro dei gruppi.

Se i messaggi inoltrati da 01548 non ricevono conferma, ad esempio a causa di destinatario mancante o di un errore di trasmissione, i messaaggi saranno ripetuti fino a tre volte (a seconda dell'impostazione di ETS). Il parametro "Ripetizioni se errori..." consente di impostare separatamente questa funzione per ciascuna linea e per entrambi i tipi di messaggi. Si raccomanda di utilizzare l'impostazione predefinita del parametro.

Il router IP è destinato all'utilizzo nelle reti 10/100 BaseT conformi a IEEE802.3. La funzione AutoSensing imposta automaticamente il baud rate (10 Mbit o 100 Mbit). L'indirizzo IP può essere ricevuto da un server DHCP. A questo scopo, l'impostazione dell'assegnazione automatica dell'indirizzo IP può essere impostata mediante ETS (“Ottieni un indirizzo IP automaticamente”). Se è configurata questa impostazione ma non viene trovato alcun server DHCP, 01548 avvia una procedura AutoIP e si assegna autonomamente l'indirizzo IP. Se 01548 deve avere un indirizzo IP fisso (un indirizzo di sottorete e di gateway standard) è possibile impostarlo mediante ETS.

4.2 Rete IP

Il dispositivo 01548 invia messaggi da/verso la rete TP verso/da la rete IP conformemente alla specifica del protocollo KNXnet/IP. In base all'impostazione predefinita, i dati IP sono inviati come IP Multicast all'indirizzo IP 224.0.23.12 porta 3671. L'indirizzo IP Multicast 224.0.23.12 è l'indirizzo per KNXnet/IP stabilito dalla KNX Association insieme alla IANA. Si raccomanda di cambiare questo indirizzo esclusivamente se ne esiste la necessità a causa della rete esistente.

Note importanti

- Tutti i dispositivi KNX IP che devono comunicare tra loro mediante IP devono avere lo stesso indirizzo IP multicast.
- Potrebbe essere necessario cambiare l'indirizzo IP multicast 224.0.23.12 a seconda del tipo di rete e delle impostazioni dei componenti della rete.
- Per il routing IP e l'individuazione viene utilizzato il protocollo IGMP (Internet Group Management Protocol).
- In caso di problemi relativi all'assegnazione dell'indirizzo IP rivolgersi all'amministratore della rete.
- Secondo la topologia, gli indirizzi individuali utilizzati per i canali tunneling devono sempre essere assegnati nel range degli indirizzi della linea secondaria. Informazioni dettagliate sugli indirizzi individuali aggiunti per il (Secure) Tunnelling sono disponibili nel capitolo 5.4 Assegnazione dell'indirizzo per l'IP (Secure) Tunnelling.

4.3 Installazione della rete KNX

È possibile definire fino a 15 campi e 225 diversi indirizzi per gli accoppiatori di linea. Per la funzionalità di accoppiatore di linea in una rete KNX, 01548 deve utilizzare l'indirizzo individuale corretto di un accoppiatore di linea (x.y.0). Per la funzionalità di accoppiatore di dorsale in una rete KNX, 01548 deve utilizzare l'indirizzo individuale corretto di un accoppiatore di campo (x.0.0).

✓ Si raccomanda di accertarsi che l'indirizzo individuale predefinito di fabbrica 15.15.0 non venga utilizzato nella rete di installazione.

✓ La definizione di una topologia corretta è assolutamente indispensabile per garantire il corretto funzionamento di un'installazione.

In un sistema KNX con accoppiatori di dorsale 01548 e accoppiatori di linea 01504.2, è necessario assicurare che a 01548 sia assegnato un indirizzo da un campo di indirizzo libero. Nella figura seguente è illustrato un possibile scenario di topologia.

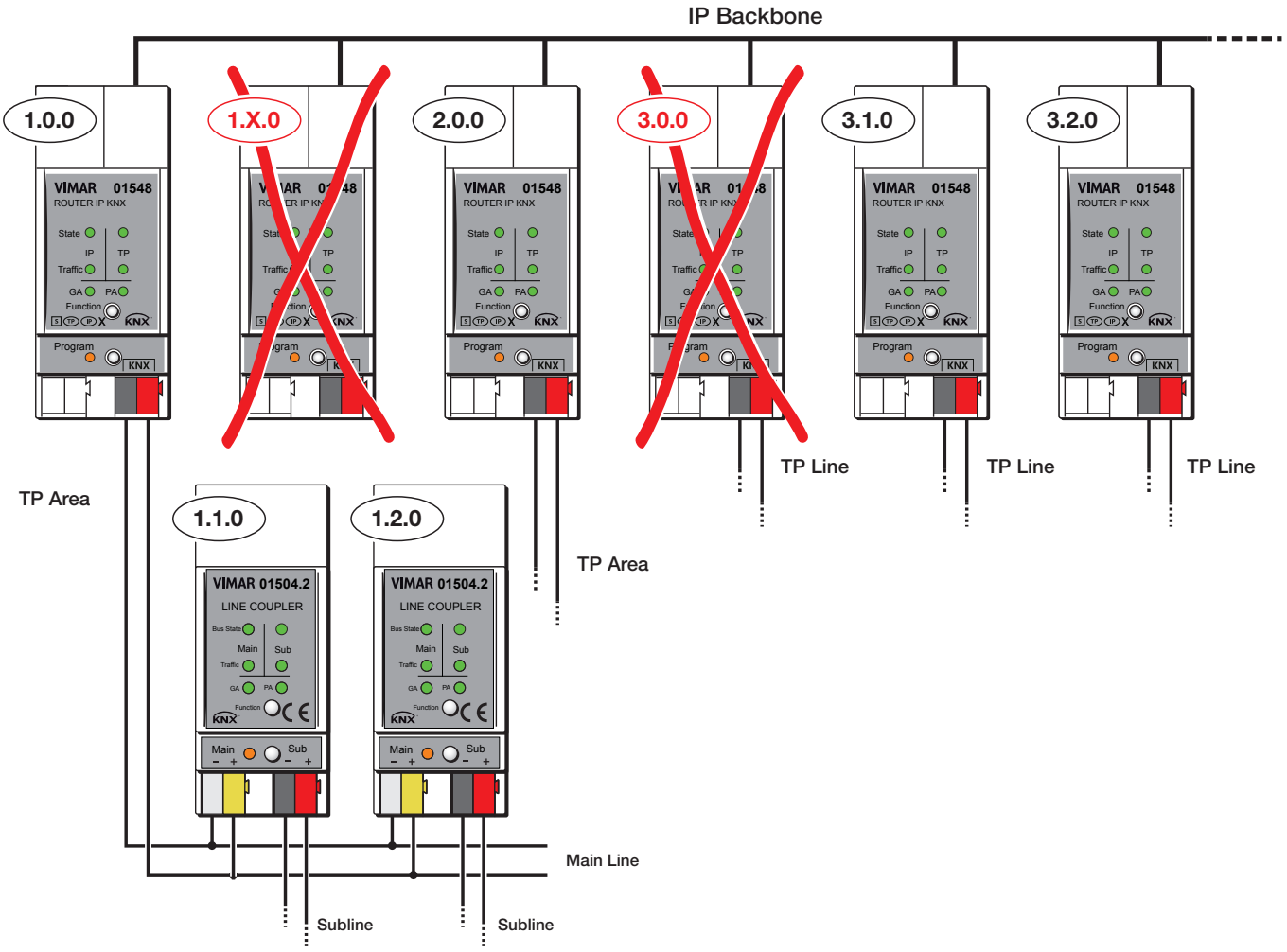


Figura 5: Topologia delle reti per 01548

Esempio:
se esiste già un router KNX IP con indirizzo 1.0.0 sulla dorsale non è possibile aggiungere alcun router KNX IP con indirizzo 1.x.0, anche se non esiste alcun accoppiatore di linea con l'indirizzo 1.1.0 sulla linea secondaria del router 1.0.0. Viceversa, se esistono già accoppiatori di linea con indirizzi 3.x.0 in un'installazione, non è possibile aggiungere un router IP con indirizzo 3.0.0.

4.4 Aggiunta del Certificato del dispositivo

Ciascun dispositivo KNX Secure utilizza il proprio Certificato. È indispensabile inserire il Certificato del dispositivo in ETS prima di attivare o utilizzare le funzioni di sicurezza KNX.

✓ Il Certificato del dispositivo è stampato su un'etichetta apposta sul lato dell'involucro.

✓ I Certificati dei dispositivi possono essere inseriti manualmente o inquadrando il codice QR con la webcam.

Dopo l'apertura del progetto, è possibile modificare l'elenco dei Certificati dei dispositivi nella scheda Sicurezza in Project Overview.

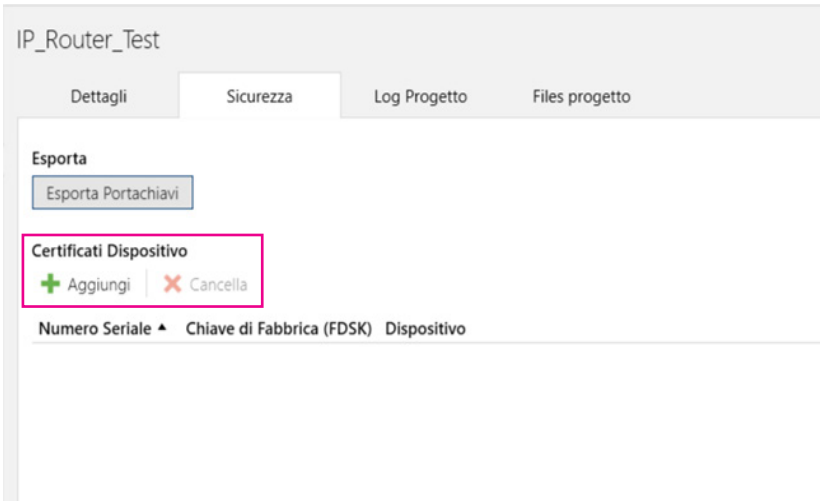


Figura 6: Elenco dei Certificati dei dispositivi

Se il Certificato del dispositivo non è ancora stato aggiunto all'elenco, quando si avvia un download protetto, viene visualizzata la finestra seguente.

Figura 7: Aggiunta del Certificato del dispositivo

4.5 Programmazione

4.5.1 Programmazione dell'Indirizzo individuale (e applicazione)

Per scaricare l'Indirizzo individuale in un dispositivo, è necessario che sia attiva la modalità Programmazione. Per attivare o disattivare la modalità di programmazione premere il tasto programmazione. Il LED 7 acceso rosso indica che la modalità di programmazione è attiva. Quando si attiva il download da ETS e si preme il tasto programmazione, il dispositivo archivia il nuovo Indirizzo individuale nella memoria. Le impostazioni di sicurezza sono aggiornate tramite il download dell'indirizzo individuale e dell'applicazione.

✓ Quando 01548 è l'interfaccia corrente, è necessario un download dell'applicazione per aggiornare le impostazioni IP di 01548.

✓ Per il download è richiesta la connessione dell'interfaccia al sistema bus KNX.

✓ Per programmare i dispositivi di una linea diversa da quella per cui il dispositivo viene utilizzato come interfaccia ETS corrente, è necessaria una topologia corretta.

L'indirizzo individuale può essere assegnato al dispositivo impostando l'indirizzo desiderato nella finestra delle proprietà di ETS. Al termine del download da ETS, il dispositivo si riavvia.

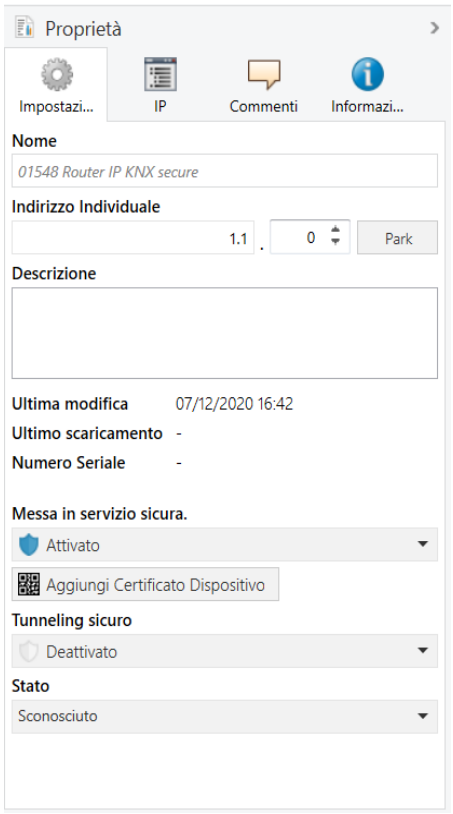


Figura 8: Finestra delle proprietà ETS

✓ Il dispositivo è fornito con l'indirizzo individuale 15.15.0 (impostazione predefinita di fabbrica). Si consiglia di non utilizzare questo indirizzo per il normale funzionamento di un impianto e di assegnare un indirizzo diverso al momento della messa in servizio.

✓ Se il LED di programmazione lampeggia rosso significa che il cavo Ethernet non è correttamente collegato o che non è disponibile una connessione a una rete IP.

✓ Il database ETS è disponibile sul sito web dell'azienda e nel catalogo online ETS.

4.5.2 Configurazione IP

La configurazione IP di 01548 può essere specificata nella finestra delle proprietà di ETS. Per attivare DHCP/AutoIP, impostare l'opzione “Ottieni automaticamente un indirizzo IP”. Per maggiori dettagli e informazioni sulla configurazione delle reti IP, rivolgersi al proprio amministratore di rete locale.

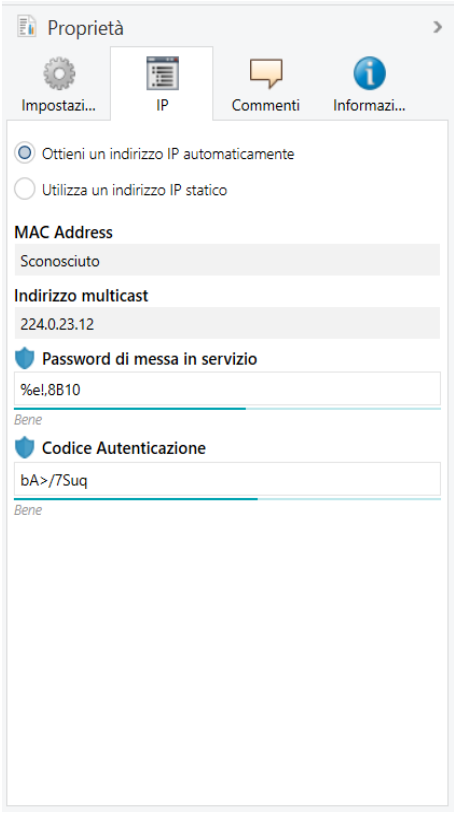


Figura 9: Assegnazione automatica dell'indirizzo IP

Se si seleziona l'opzione “Usa un indirizzo IP statico”, è possibile impostare manualmente l'indirizzo IP, l'indirizzo di sottorete e di gateway predefinito.

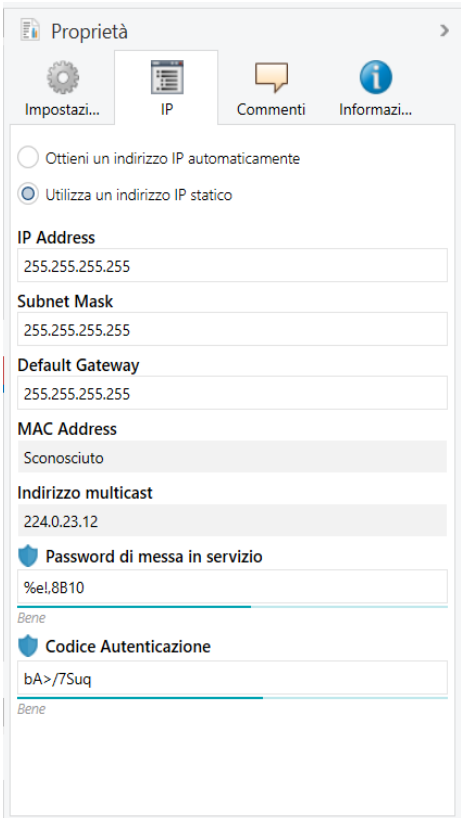


Figura 10: Assegnazione manuale dell'indirizzo IP

- ✓ I dispositivi KNX IP destinati a comunicare tra loro tramite il protocollo di routing IP (Secure) devono utilizzare lo stesso indirizzo multicast.
- ✓ La modifica dell'indirizzo multicast può avvenire esclusivamente nella scheda di configurazione IP della finestra delle proprietà della dorsale. Per visualizzarla fare clic sulla barra azzurra " "Backbone topologia".
- ✓ Quando 01548 viene utilizzato come interfaccia corrente dell'ETS e il relativo indirizzo IP viene modificato da un download di configurazione, ETS tenta di mantenere la connessione all'interfaccia corrente che ha l'indirizzo IP precedente. È necessario selezionare di nuovo il dispositivo 01548 (che ora contiene l'indirizzo IP aggiornato) come interfaccia corrente dall'elenco delle interfacce individuate. Fino a quel momento l'indirizzo IP precedente resterà visibile nella finestra del tunnelling IP e ETS informerà che non è possibile raggiungere l'interfaccia corrente.

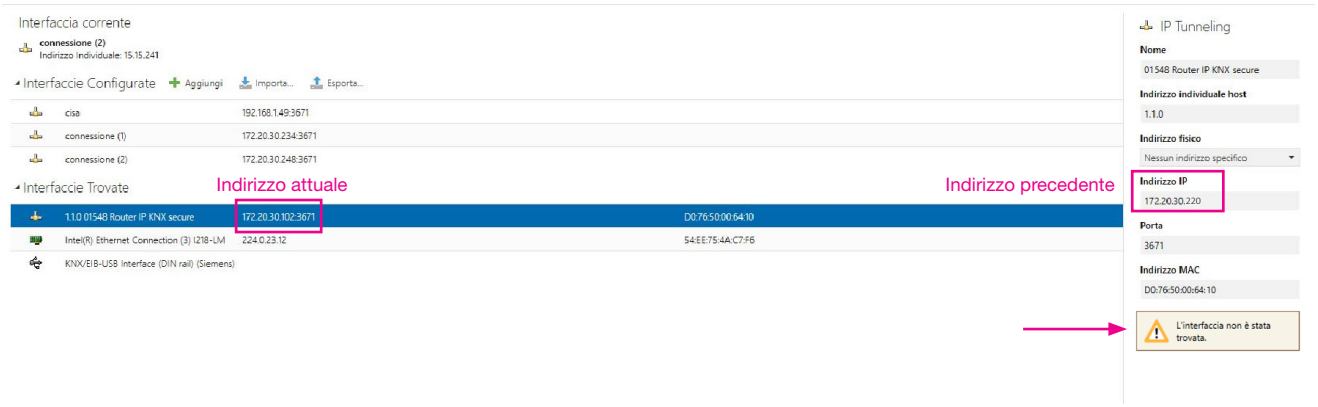


Figura 11: Indirizzo IP dell'interfaccia corrente prima e dopo l'aggiornamento

4.6 Funzioni speciali

Il tasto funzione attiva le funzioni speciali di 01548. È possibile attivare la funzione manuale e il reset di fabbrica. Le impostazioni dispositivo di 01548 possono essere ripristinate ai valori predefiniti del produttore con la funzione reset di fabbrica. A questo scopo occorre premere il tasto funzione durante la procedura di aggiornamento del firmware. Lo stato di funzione speciale attiva è indicata dallo stato dei LED (vedere il capitolo “1.3 LED funzioni speciali”).

4.6.1 Funzione manuale

Nel corso del normale funzionamento, un breve pressione (circa 3 sec) attiva o disattiva la funzione Manuale. Il LED 5 e il LED 6 mostrano lo stato corrente di filtro.

Quando è attiva la funzione manuale, tutti i messaggi fisici o tutti i messagi di gruppo o entrambi possono attraversare il dispositivo 01548 senza essere filtrati. Al termine del tempo di funzionamento manuale, il dispositivo 01548 torna automaticamente al funzionamento normale. Per configurare la funzione manuale e la durata della stessa, modificare i parametri generali come descritto nel capitolo 5.1 Impostazioni generali. Dopo la commutazione dalla modalità manuale al funzionamento normale, le impostazioni dei parametri/voci della tabella filtri scaricate più di recente sono di nuovo attive.

Tabella 6: Attivazione delle funzioni manuali

Passaggio	Funzione manuale
1	Tenere premuto il tasto funzione per 3 secondi
2	Il LED 1 diventa arancione per indicare che la funzione manuale è attiva
3	Dopo lo spegnimento, il funzionamento normale è indicato dal LED 1 acceso con luce verde

4.6.2 Reset di fabbrica

Per eseguire il reset di fabbrica premere a lungo (circa 15 sec) il tasto funzione e immediatamente dopo premerlo di nuovo brevemente (circa 3 sec). Dopo la prima pressione il LED si illumina come descritto nella Tabella 4: Stato dei LED per il reset di fabbrica dopo la prima pressione del tasto funzione. Dopo la seconda pressione tutti i parametri (incluso l'indirizzo individuale) vengono reimpostati sui valori predefiniti di fabbrica. Quando è attiva la funzione Security, anche il Tool Key viene ripristinato sul relativo FDSK. Successivamente i LED tornano allo stato di funzionamento normale.

Tabella 7: Attivazione del reset di fabbrica

Passaggio	Reset di fabbrica
1	Tenere premuto il tasto funzione per 15 secondi
2	I LED 1 e 2 sono accesi con luce arancione
3	Tenere premuto il tasto funzione per 3 secondi
4	Il dispositivo si riavvia

4.6.3 Richiesta di aggiornamento del firmware IP

Nel corso del normale funzionamento, una breve pressione (circa 3 sec) attiva o disattiva la funzione Manuale. Il LED 5 e il LED 6 mostrano lo stato corrente di filtro.

Dopo aver premuto il tasto “request update” nel web front-end, lo 01548 entra in boot-mode indicato da “Status: update authorized”.

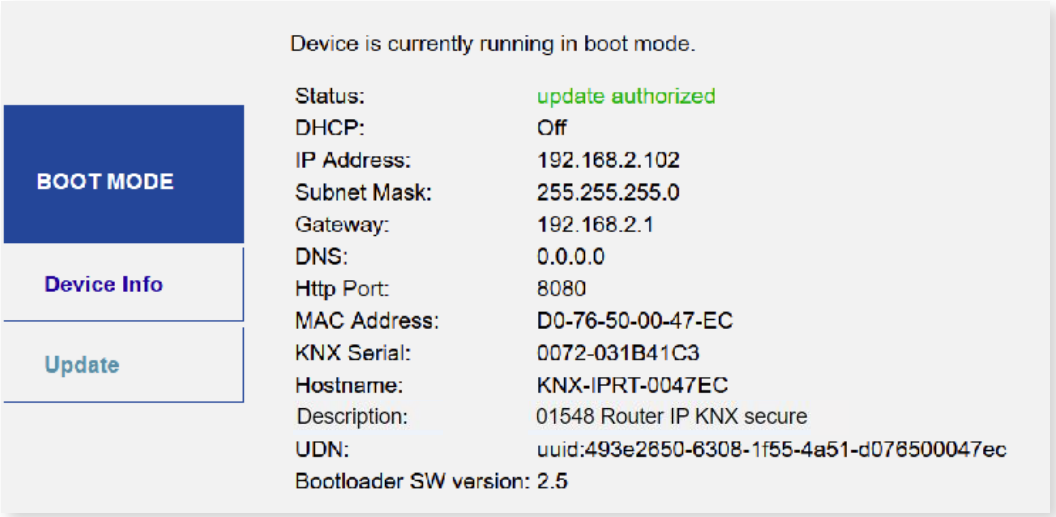


Figura 12: Richiesta di aggiornamento autorizzata

Tabella 8: Attivazione dell'aggiornamento del firmware

Passaggio	Aggiornamento Firmware
1	Pressione breve del tasto programmazione
2	Pressione breve del tasto funzione
3	Fare clic su “request update” nel front-end Web
4	Il LED 2 è verde lampeggiante
5	È possibile selezionare il file del firmware
6	Il dispositivo si riavvia

5. Database ETS

5.1 Generale

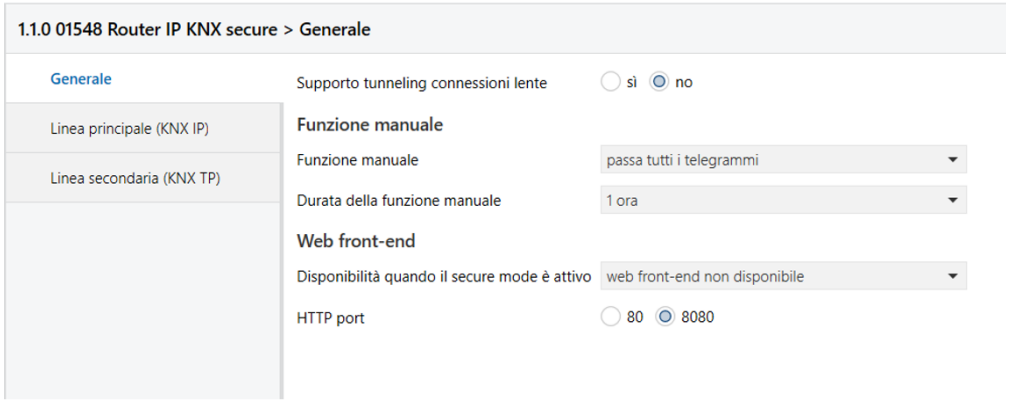


Figura 13: Parametri della sezione Generale

Tabella 9: Impostazioni dei parametri nella sezione Generale

Parametro ETS	Impostazioni [Parametro predefinito]	Commento
Supporto tunneling connessioni lente	sì no **[no]**	Attiva o disattiva il supporto delle connessioni di tunnelling lente.
Funzione manuale		
Funzione manuale	disabilitata passa tutti i telegrammi passa i telegrammi fisici passa i telegrammi di gruppo **[passa tutti i telegrammi]**	Impostazione di configurazione per l'inoltro dei messaggi quando è attiva la funzione manuale.
Durata della funzione manuale	10 min, 1 ora, 4 ore 8 ore **[1 ora]**	Dopo questo intervallo di tempo la funzione manuale si disattiva automaticamente.
Web front-end		
Disponibilità quando il secure mode è attivo	disponibile con tutte le funzioni solo visualizzazione dello stato web front-end non disponibile **[web front-end non disponibile]**	Quando è attiva la modalità sicurezza, il front-end Web può essere completamente disponibile (lettura/scrittura), essere disponibile per un uso limitato (solo lettura) o essere disattivato.
HTTP port	80 8080 **[8080]**	Selezione della porta HTTP.

5.2 Linea principale (IP)

✓ L'impostazione “trasmetti tutto” è destinata esclusivamente all'uso di prova. Non utilizzarla per il funzionamento nornale.

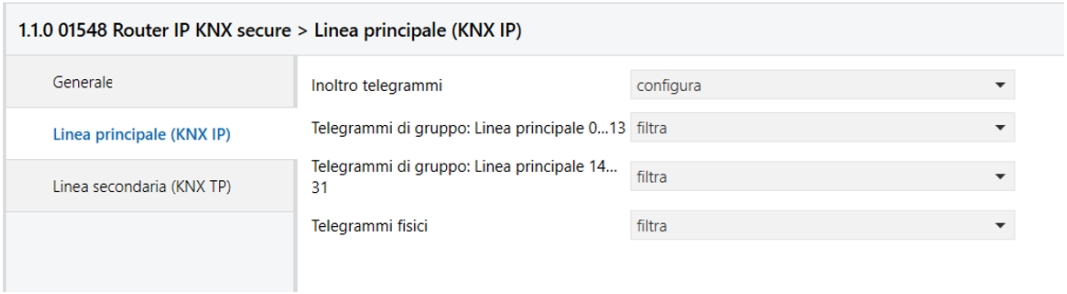


Figura 14: Parametri per Main Line (IP)

Tabella 10: Impostazioni dei parametri per la linea Principale (IP)

Parametro ETS	Impostazioni [Parametro predefinito]	Commento
Inoltro telegrammi (Linea principale -> linea secondaria)	gruppi: filtra, fisici: blocca gruppi, fisici: filtra gruppi: inoltra, fisici: filtra gruppi e fisici: inoltra configura **[gruppi fisici: filtra]**	L'inoltro dei messaggi fisici e dei messaggi di gruppo può essere impostato su "blocca" (nessun inoltro), "filtra" (i messaggi sono inoltrati in base al filtro) e "inoltra" (tutti i messaggi vengono trasmessi). Per impostare parametri diversi da quelli disponibili qui, utilizzare "configura".
Telegrammi di gruppo: Linea principale 0...13	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi di gruppo (con gruppi principali 0 ... 13) può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi inseriti nella tabella filtri.
Telegrammi di gruppo: Linea principale 14...31	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi di gruppo (con gruppi principali 14 ... 31) può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi inseriti nella tabella filtri.
Telegrammi fisici	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi fisici può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi in base ai loro indirizzi individuali.

5.3 Linea secondaria (KNX TP)

L'impostazione “trasmetti tutto” è destinata esclusivamente all'uso di prova. Non utilizzarla per il funzionamento nornale.

✓ Se il parametro "Invia conferma su telegrammi propri" è impostato su "si", 01548 invierà sistematicamente un ACK su ogni messaggio proprio inoltrato. Ad esempio, poiché i ripetitori non utilizzano tabelle filtro, è utile avere un ACK inviato insieme ai messaggi inoltrati.

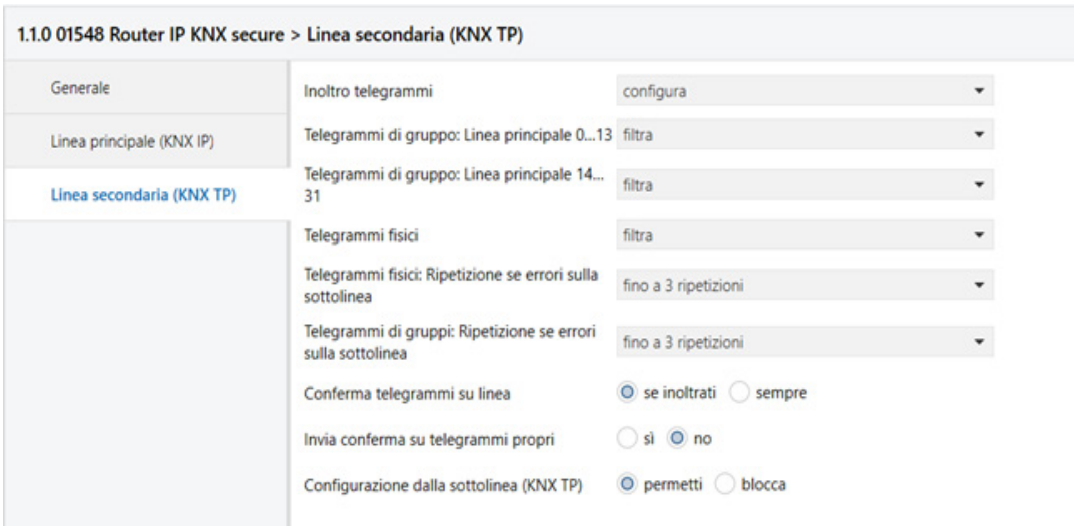


Figura 15: Parametri per la Linea secondaria (KNX TP)

Tabella 11: Impostazioni dei parametri per la Linea secondaria (KNX TP)

Parametro ETS	Impostazioni [Parametro predefinito]	Commento
Inoltro telegrammi (Linea secondaria > Linea principale)	gruppi: filtra, fisici, blocca gruppi, fisici: filtra gruppi: inoltra, fisici: filtra gruppi e fisici: inoltra configura **[gruppi, fisici: filtra]**	L'inoltro dei messaggi fisici e dei messaggi di gruppo può essere impostato su "blocca" (nessun inoltro), "filtra" (i messaggi sono inoltrati in base al filtro) e "inoltra" (tutti i messaggi vengono trasmessi). Per impostare parametri diversi da quelli disponibili qui, utilizzare "configura".
Telegrammi di gruppo: Linea principale 0...13	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi di gruppo (con gruppi principali 0 ... 13) può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi inseriti nella tabella filtri.
Telegrammi di gruppo: Linea principale 14...31	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi di gruppo (con gruppi principali 14 ... 31) può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi inseriti nella tabella filtri.
Telegrammi fisici	trasmetti tutto (solo per test) blocca filtra **[filtra]**	Il filtro dei messaggi fisici può essere configurato in modo che inoltri tutti i messaggi, nessun messaggio o solo i messaggi in base ai loro indirizzi individuali.
Telegrammi fisici: Ripetizione se errori sulla sottolinea	no fino a 3 ripetizioni solo una ripetizione **[fino a 3 ripetizioni]**	Dopo un errore di trasmissione della linea secondaria (ad es. per un destinatario mancante) i messaggi fisici possono non essere ripetuti, ripetuti per una volta o ripetuti per tre volte al massimo.
Telegrammi di gruppo: Ripetizione se errori sulla sottolinea	no fino a 3 ripetizioni solo una ripetizione **[fino a 3 ripetizioni]**	Dopo un errore di trasmissione della linea secondaria (ad es. per un destinatario mancante) i messaggi di gruppo possono non essere ripetuti, ripetuti per una volta o ripetuti per tre volte al massimo.
Conferma telegrammi su linea	se inoltrati sempre **[se inoltrati]**	Solo i messaggi inoltrati alla linea principale IP sono confermati sulla linea secondaria KNX oppure sono confermati tutti i messaggi.
Invia conferma su telegrammi propri	sì no **[no]**	I messaggi inviati alla linea secondaria possono essere confermati da un ACK aggiunto.
Configurazione dalla sottolinea (KNX TP)	permetti blocca [**permetti]**	Se è selezionata l'opzione blocca, il dispositivo 01548 può essere configurato solo dalla linea principale.

5.4 Assegnazione dell'indirizzo per l'IP (Secure) Tunnelling

Il dispositivo 01548 fornisce 4 canali per connessioni attraverso il tunneling su IP (secure). Per stabilire tale connessione tunneling deve essere assegnato un indirizzo individuale libero al canale di tunneling. A tal fine utilizzare la finestra di impostazioni presente per ogni canale di tunneling.

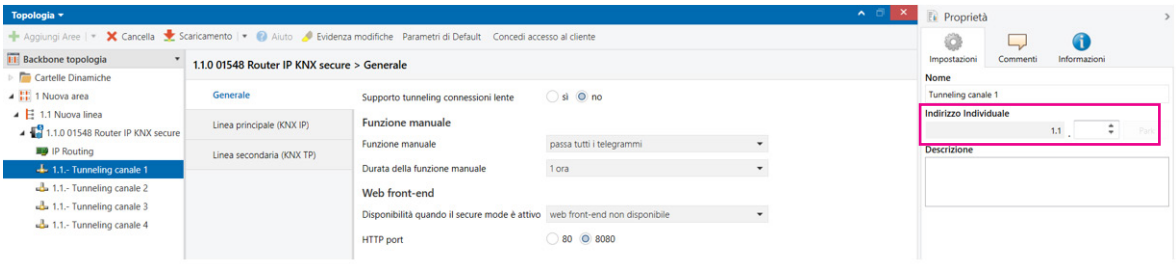


Figura 16: Configurazione dei canali di tunnelling IP (Secure)

Per utilizzare il tunnelling IP protetto, è necessario attivare la messa in servizio protetta e il tunnelling protetto nella finestra delle proprietà di 01548. Sarà quindi disponibile anche l'opzione di protezione con password dei singoli canali di tunnelling.

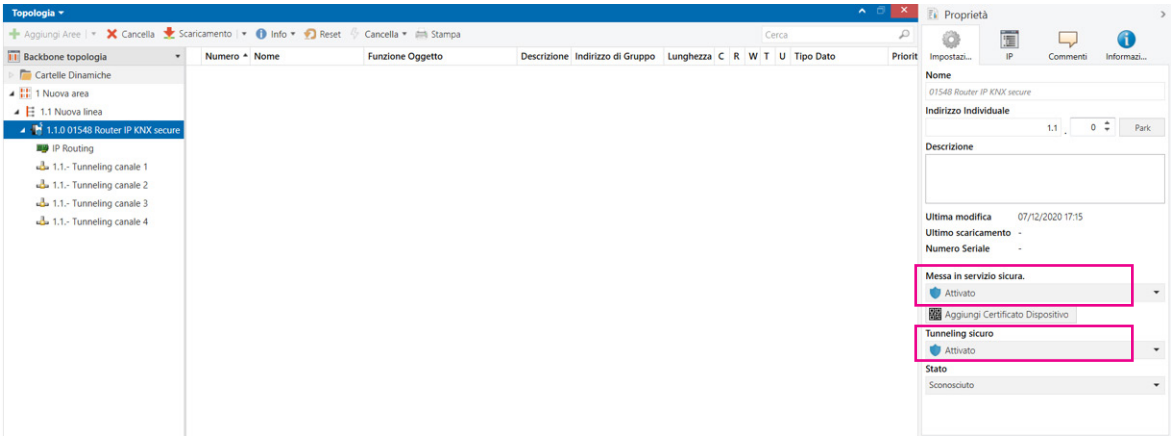


Figura 17: Attivazione del Secure Tunnelling

6. Front-end Web

È possibile utilizzare il front-end Web per leggere i parametri effettivi del dispositivo 01548 (porta HTTP, indirizzo IP, indirizzo MAC ecc.) per aggiornarne il firmware e impostare gli indirizzi individuali per il tunnelling. Per identificare un determinato dispositivo 01548 in una rete KNX, è possibile accendere e spegnere il LED di programmazione/la modalità di programmazione da remoto, senza premere il tasto di programmazione sul dispositivo.

✓ Per tornare dalla modalità di avvio al funzionamento normale è necessario eseguire la procedura di aggiornamento del firmware, quindi annullarla o attendere 10 minuti fino al timeout automatico.

6.1 Protezione del front-end Web dello 01548

Il front-end Web può essere utilizzato per l'esecuzione da remoto degli aggiornamenti del firmware, per le funzioni di controllo e per la lettura delle impostazioni del dispositivo. Per garantire la protezione totale di un'installazione il front-end Web deve essere impostato su "non disponibile" durante il funzionamento di runtime.

Per utilizzare le funzioni remote del front-end Web quando è attiva la sicurezza, questo deve essere impostato su “disponibile con tutte le funzioni”.

Figura 18: Parametro ETS per la disponibilità del front-end Web

Se il front-end Web è impostato su “solo visualizzazione dello stato”, le funzioni di controllo remote (attivazione della modalità programmazione, impostazione del tunnelling) e la funzione di aggiornamento sono disattivate. È disponibile solo la lettura delle informazioni.

✓ Per assicurare la protezione completa di un'installazione protetta, la disponibilità del front-end Web deve essere impostata su “web front-end non disponibile” che è il valore predefinito.

✓ Per una protezione efficace si sconsiglia fortemente di utilizzare l'opzione “disponibile con tutte le funzioni” come impostazione permanente.

6.2 Accesso al front-end Web dello 01548

È possibile accedere al front-end Web dello 01548 in tre modi. Vi si può accedere direttamente da Esplora risorse in Windows o da un browser web. Per accedere via browser web è necessario conoscere l'indirizzo IP o l'indirizzo MAC e la porta HTTP. Di seguito è descritto come utilizzare l'indirizzo IP e l'indirizzo MAC nella barra degli indirizzi del browser.

✓ Per accedere da un browser web si deve utilizzare la porta HTTP corretta.

✓ Il valore predefinito di fabbrica della porta HTTP è 8080.

6.2.1 Con Esplora risorse di Windows

Il dispositivo 01548 è visualizzato nella rete locale di Windows grazie alla ricerca UPnP. Fare doppio clic sul dispositivo 01548 per aprire il front-end Web nel browser predefinito.

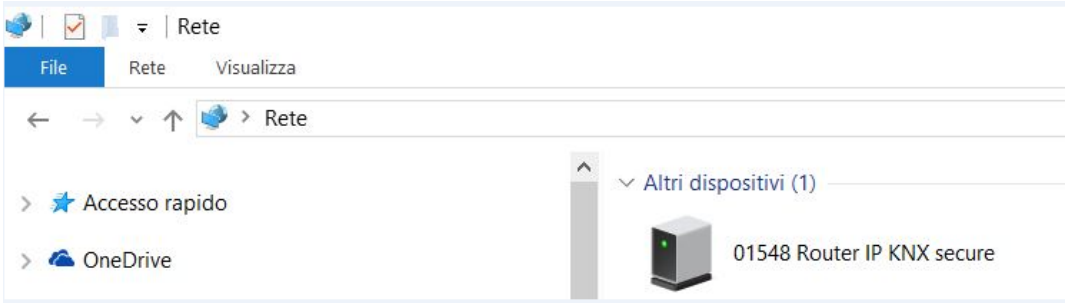


Figura 19: 01548 in Esplora risorse di Windows.

6.2.2 Con l'indirizzo IP

Se si conoscono l'indirizzo IP e la porta HTTP si hanno le informazioni sufficienti per accedere al front-end Web dello 01548 da un browser web. Poiché il dispositivo 01548 può fungere anche da interfaccia corrente dell'ETS, il relativo indirizzo IP è visualizzato sotto "Interfacce trovate" in ETS. Per lo 01548, è possibile impostare la porta HTTP su 80 o 8080.

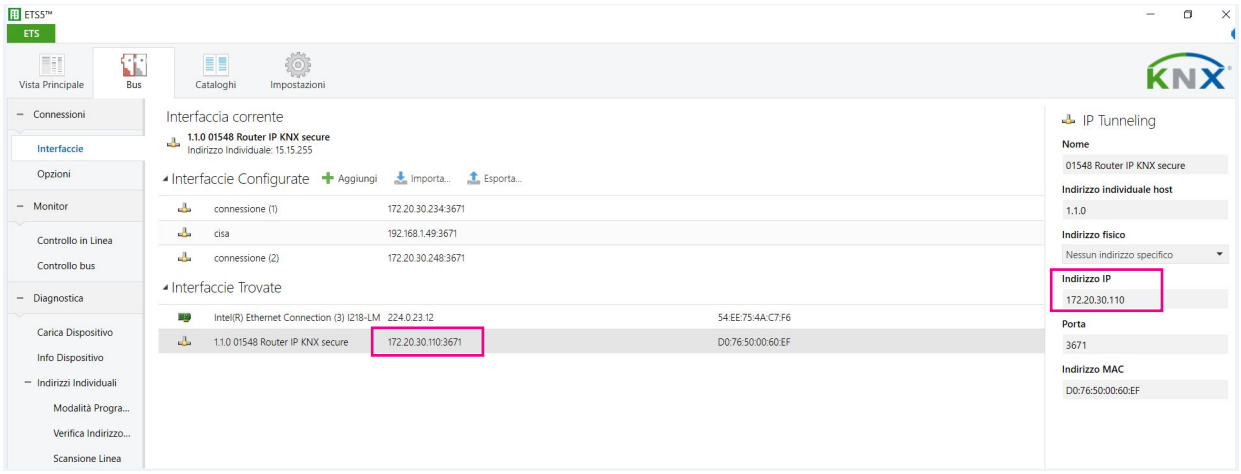


Figura 20: Identificazione dell'indirizzo IP dello 01548 mediante ETS

In base alla configurazione preimpostata dello 01548 (rispettivamente porta HTTP, indirizzo IP e DHCP) inserire quanto segue nella barra degli indirizzi, senza le parentesi:

http://[IP address]:[HTTP port]/

Esempio 1:
DHCP non è utilizzato. Con l'ultimo download ETS l'indirizzo IP era stato impostato su 192.168.1.32 e la porta HTTP su 80. Inserire “http://192.168.1.32:80/” nella barra degli indirizzi del browser.

Esempio 2:
01548 è usato con la sua impostazione predefinita di fabbrica. Questo significa che la porta HTTP è 8080 e DHCP è attivo. Il server DHCP ha assegnato l'indirizzo IP 192.168.1.201. Inserire “http://192.168.1.201:8080/” nella barra degli indirizzi del browser.

6.2.3 Con l'indirizzo MAC

Quando è installato NetBIOS (per impostazione predefinita nei sistemi Windows), è possibile utilizzare l'indirizzo MAC, stampato sull'etichetta applicata sul lato dell'involucro del dispositivo 01548 (che è anche elencato nelle interfacce individuate da ETS). A causa della risoluzione del nome è indispensabile stabilire la comunicazione in base al nome Host. Per questo è necessaria l'attivazione del NetBIOS.

Utilizzare l'indirizzo MAC nella forma AA-BB-CC-XX-YY-ZZ e la porta HTTP preimpostata da inserire nella barra degli indirizzi del browser come indicato sotto, senza le parentesi:

http://knx-iprt-[XXYYZZ]:[HTTP port]/

Esempio:
sull'etichetta a lato dell'involucro del dispositivo 01548 è riportato l'indirizzo MAC D0-76-50-11-22-33 e la porta HTTP preimpostata è 8080. Inserire “http://knx-iprt-112233:8080/” nella barra degli indirizzi del browser.

6.3 Informazioni sul dispositivo

Dopo aver eseguito l'accesso al front-end Web viene visualizzata la scheda Device Info, in cui sono riportare informazioni generali sui parametri del dispositivo corrente (indirizzi, nome, versioni software).

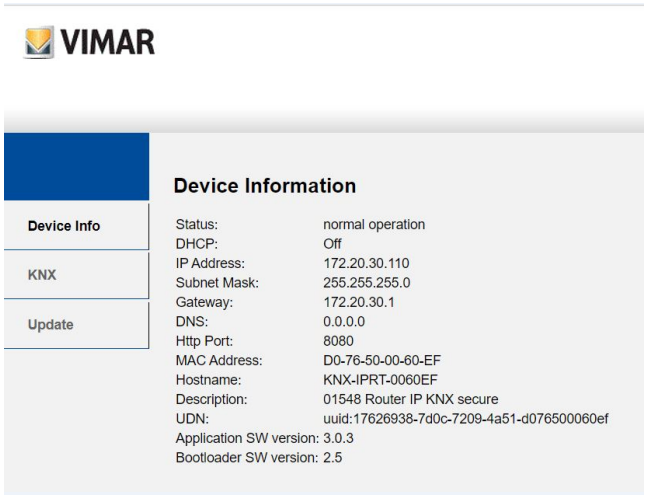


Figura 21: Schermata Informazioni dispositivo

6.4 KNX

Gli indirizzi specifici KNX sono indicati su questa schermata. Controllare le impostazioni è semplice. Fare clic su "ON" per attivare la modalità programmazione (equivale a premere il tasto programmazione). Insieme alla schermata delle informazioni dispositivo, questa funzione è utile per distinguere il dispositivo interessato (in quanto ha un determinato indirizzo IP, indirizzo MAC e numero di serie) da altri dispositivi simili nella rete.

Sono visualizzati l'indirizzo individuale, i quattro indirizzi individuali per il tunnelling (indirizzi individuali aggiuntivi), l'indirizzo di routing multicast, il serial number del dispositivo 01548 e uno schema con la cronologia del carico del bus negli ultimi 60 minuti (il browser deve supportare la grafica SVG). La curva rossa indica il carico massimo del bus su TP mentre quella verde indica il carico medio del bus su TP.

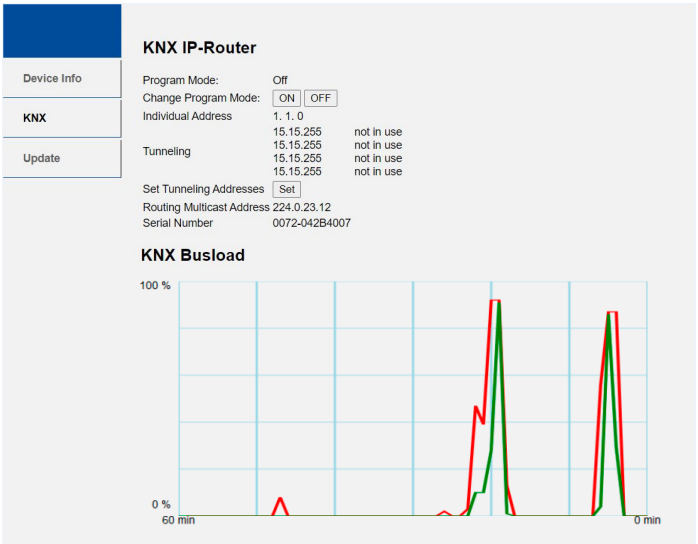


Figura 22: Schermata KNX

✓ Per visualizzare il diagramma del carico del bus, il browser web deve supportare la grafica SVG.

Per il tunnelling IP è possibile impostare quattro indirizzi individuali. L'impostazione di un indirizzo individuale diverso per ogni canale di tunnelling attraverso il front-end Web è rilevante per le versioni di ETS precedenti alla 5.7. In questo caso il primo indirizzo di tunnelling deve essere impostato nel campo "Indirizzo individuale" della finestra Connections della scheda Bus di ETS. Facendo clic su "Set" gli altri indirizzi seguono il primo in sequenza. Questo perché i canali di tunnelling che usano lo stesso indirizzo individuale possono causare una riduzione della connessioni utilizzabili. Con il pulsante Set è possibile riassegnarli in modo che abbiano indirizzi individuali diversi.

✓ Prima della riassegnazione con il pulsante Set, accertarsi che tali indirizzi non esistano già nel progetto o nell'impianto e che i client non perdano la connettività a causa della riassegnazione.

✓ Quando è attiva la sicurezza, si raccomanda fortemente di assegnare gli indirizzi individuali esclusivamente tramite progetti ETS e download di configurazione (vedere il capitolo “5.4 Assegnazione dell'indirizzo per l'IP (Secure) Tunnelling”).

6.5 Aggiornamento del firmware IP

Nella schermata Update del dispositivo 01548 è possibile aggiornare il firmware via IP, ovvero la rete Ethernet. Nei passaggi seguenti è descritta la procedura completa di aggiornamento remoto. Durante il processo, il dispositivo 01548 entra in boot mode. Quindi i LED 1, 2, 3 e 7 si illuminano come descritto nella Tabella 5: Stato dei LED per l'aggiornamento del firmware

✓ Se è già attivo il boot mode, seguire solo le istruzioni del front-end Web dal passaggio 3 al 5 (update, request update).

Per uscire dalla modalità di avvio, è necessario accedere alla schermata Update del front-end Web. Quindi è possibile completare l'aggiornamento del firmware, come descritto nei passaggi da 1 a 5, oppure interrompere l'aggiornamento del firmware facendo clic sul pulsante "Abort" (vedere passaggio 5, Figura 27). Dopodiché il dispositivo 01548 si riavvia e riprende il funzionamento normale.

Passaggio 1: Aprire la schermata Update del front-end Web.

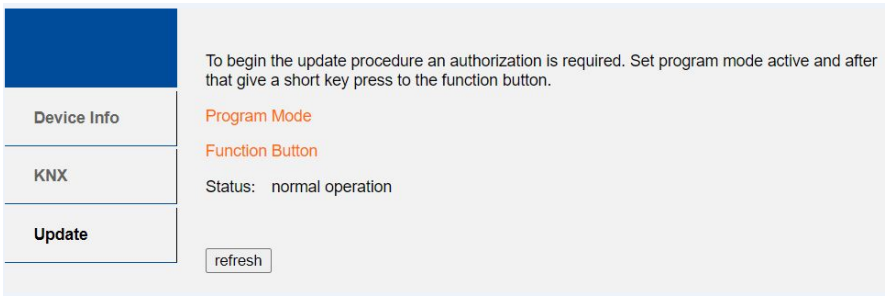


Figura 23: Schermata Update

Passaggio 2: Attivare la modalità programmazione (scheda KNX o tasto programmazione).

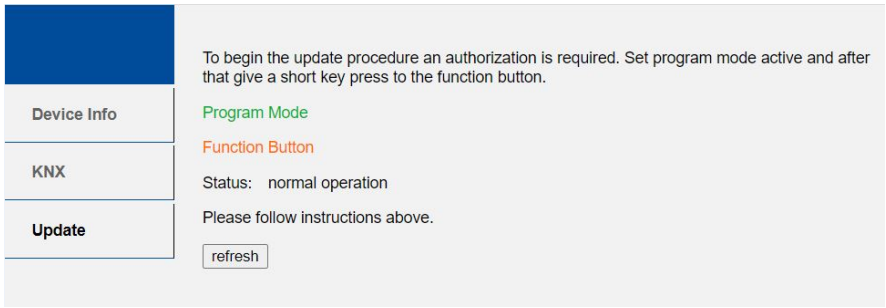


Figura 24: Schermata Update e modalità programmazione attivata

Passaggio 3: Dopo aver attivato la modalità programmazione, premere brevemente il tasto funzione. Quindi premere il pulsante “refresh”.

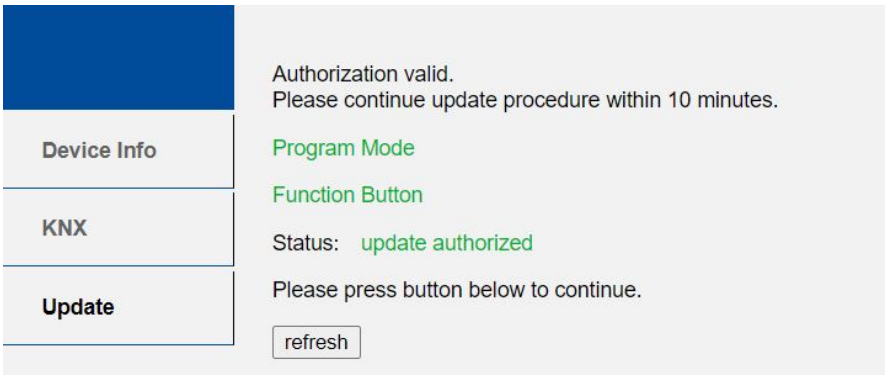


Figura 25: Aggiornamento autorizzato

Passaggio 4: Quando viene visualizzato il pulsante “request update”, premerlo per selezionare il file di aggiornamento e accedere al boot mode.

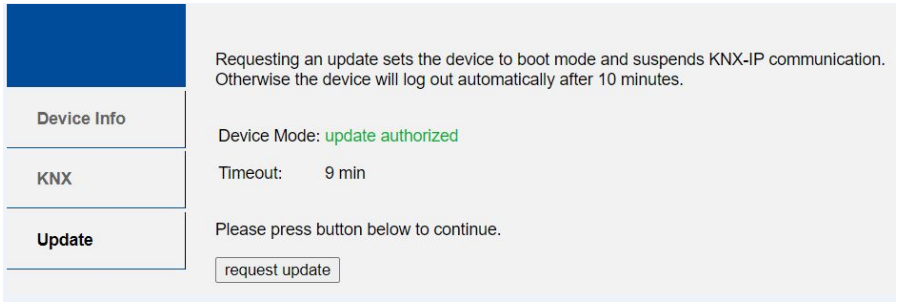


Figura 26: Richiedi aggiornamento

Passaggio 5: È possibile selezionare il file di aggiornamento e caricarlo. Al termine, il dispositivo esce dal boot mode e si riavvia. Se si fa clic sul pulsante “Abort” la procedura di aggiornamento del firmware viene annullata e il dispositivo esce del boot mode.

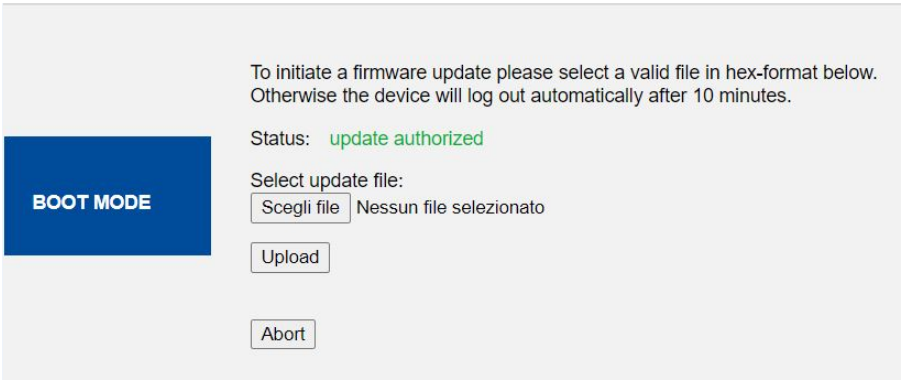


Figura 27: Selezionare Aggiorna file

7. Glossario

Passaggio	Funzione manuale
ACK	Un ACK è un frame IACK positivo. Se il mittente rileva un ACK (acknowledgment, conferma), significa che i dati del mittente sono stati ricevuti correttamente, ovvero sono stati trasmessi con esito positivo al destinatario.
Frame di acknowledgement	La conferma sul Link layer KNX è definita anche Immediate ACK (IACK) nel gergo KNX, per differenziarla dagli altri metodi di conferma dei livelli superiori. Nella pratica i frame IACK sono utilizzati per confermare a un mittente se i dati trasmessi sono stati ricevuti correttamente dal destinatario (ACK) oppure no (BUSY/NACK). Inoltre, un destinatario non può rispondere inviando uno IACK al mittente se un frame è danneggiato o indirizzato in modo errato (IACK mancante).
BUSY	Un frame BUSY (Occupato) indica un frame IACK negativo. Se il mittente rileva un frame BUSY, significa che il destinatario non ha potuto elaborare il frame ricevuto. Di conseguenza, il mittente aspetta qualche istante e invia di nuovo il frame (fino a tre volte).
Oggetto di comunicazione	Vedere Oggetto di gruppo
Formato frame estesi	Un frame esteso ha un lunghezza APDU massima di 254 ottetti e una lunghezza massima di 263 ottetti (incluso il checksum).
Filtro	Il filtro dei messaggi può essere realizzato in base alla topologia tramite gli indirizzi individuali (messaggi fisici) e in base alle tabelle dei filtri per le comunicazioni di gruppo (messaggi di gruppo) tramite gli indirizzi di gruppo.
Oggetto di gruppo	Un datapoint in KNX è definito "Oggetto di gruppo" o semplicemente "Oggetto".
Messaggi di gruppo	I dati orientati a un gruppo sono denominati messaggi di gruppo. Il filtro dei messaggi di gruppo viene effettuato in base alle tabelle dei filtri incorporate per la comunicazione di gruppo.
IACK	Vedere Frame di acknowledgement
Indirizzo individuale	L'indirizzo individuale di un dispositivo specifica la posizione del dispositivo all'interno della topologia.
Long Data	I Long data o frame lunghi sono dati con una lunghezza APDU che supera i 15 ottetti. I Long data utilizzano il formato frame esteso.
NACK	Un NACK (not acknowledged, non confermato) indica un frame IACK negativo. Se il mittente rileva un NACK, significa che i dati del mittente non sono stati ricevuti correttamente, ovvero non sono stati trasmessi con esito positivo al destinatario. Di conseguenza, il mittente invia di nuovo il frame (fino a tre volte).
Indirizzo fisico	Vedere Indirizzo individuale
Messaggi fisici	I messaggi indirizzati individualmente sono denominati messaggi fisici.
Ripetizione dei messaggi	Se sulla linea TP non viene ricevuto alcuno IACK positivo (ovvero si riceve NACK, BUSY, IACK mancante), gli accoppiatori in genere ripetono i messaggi fino a tre volte. Il numero di ripetizioni è configurabile.
Funzioni di sicurezza	L'utilizzo delle funzioni di sicurezza di ETS dipende dal numero di versione di ETS. Le funzioni di sicurezza sono disponibili a partire dal numero di versione ETS 5.7.2 (ETS Inside 1.4.0).
Short Data	Gli Short data o frame brevi sono dati la cui lunghezza APDU non supera i 15 ottetti. Gli Short data utilizzano il formato frame standard.
Formato frame standard	Un frame standard ha un lunghezza APDU massima di 15 ottetti e una lunghezza massima di 23 ottetti (incluso il checksum).

8. Informazioni tecniche

8.1 Stato alla consegna

Tabella 12: Impostazioni di fabbrica

Generale	
Indirizzo individuale	15.15.0
Indirizzi individuali per il (Secure) Tunnelling	• 15.15.241 • 15.15.242 • 15.15.243 • 15.15.244

Configurazione IP	
Assegnazione dell'indirizzo IP	DHCP/AutoIP
Indirizzo multicast di routing IP	224.0.23.12

IP (da linea principale IP a linea secondaria KNX TP)	
Messaggi di gruppo (gruppo principale 0...13)	DHCP/AutoIP
Messaggi di gruppo (gruppo principale 14...31)	224.0.23.12
Messaggi fisici	filtra

KNX TP (da linea secondaria KNX TP a linea principale IP)	
Messaggi di gruppo (gruppo principale 0...13)	filtra (la tabella filtri è vuota)
Messaggi di gruppo (gruppo principale 14...31)	inoltra tutti
Messaggi fisici	filtra
Fisico: Ripetizione se errori su linea secondaria (KNX TP)	fino a 3 ripetizioni
Gruppo: Ripetizione se errori su linea secondaria (KNX TP)	fino a 3 ripetizioni
Conferma dati su linea secondaria (KNX TP)	se inoltrati
Invia conferma su dati propri	no
Configurazione dalla linea secondaria (KNX TP)	consenti

8.2 Caratteristiche tecniche

Tabella 13

Marcatura/Design	01548	
Corrente assorbita	< 20 mA	
Collegamenti	IP (linea):	presa RJ45 da 100 Mbit e 10 Mbit BaseT, reti IEEE 802.3
	Linea KNX TP:	Connettore KNX TP (rosso/nero), senza viti, per cavo unipolare Ø 0,6…0,8 mm
Elementi LED	Stato (IP e TP) Traffico (IP e TP) Routing (GA e PA) LED programmazione	
Elementi di comando	Tasto funzione Tasto programmazione	
Montaggio	Guida DIN da 35 mm (TH35) conforme a IEC60715	
Tipo di protezione	IP20 conforme a IEC60529	
Grado di inquinamento	2 conforme a IEC60664-1	
Grado di protezione	III conforme a IEC61140	
Categoria di sovratensione	II conforme a IEC60664-1	
Approvazione	Certificato KNX conforme a ISO/IEC14543-3 ed EN ISO 22510	
Marchio CE	Conforme alle direttive 2014/35/EU (LVD), 2014/30/EU (EMC), 2011/65/EU (RoHS)	
Norme	EN50491-5-1, EN50491-5-2, EN50491-5-3, EN50581, EN60950-1, EN61000-6-2, EN61000-6-3, IEC60950-1	
Alimentazione	KNX: 21…30 V DC (SELV)	
Colore involucro	Involucro in plastica PA66, grigio	
Dimensioni involucro	H = 90 mm, Largh = 36 mm (2 moduli), Profondità = 71 mm	
Profondità di montaggio	64 mm	
Peso	68 g	
Temperatura di funzionamento	-5…45 °C	
Temperatura di stoccaggio	-20…60 °C	
Umidità ambientale	5…93 %, senza condensazione	

9. FAQ

- **Ho smarrito il Certificato del dispositivo. Come posso fare?**

  Aprire un progetto ETS in cui è contenuto il certificato, quindi aprire il report dei certificati di progetto.

- **Ho aperto un nuovo progetto in ETS e ho aggiunto il Certificato del dispositivo, ma il download su 01548 protetto non funziona.**

  Utilizzare la password di messa in servizio e il codice di autenticazione del progetto precedente oppure eseguire un reset di fabbrica per riportare il Tool Key di 01548 al codice FDSK originale.

- **Ho smarrito il Certificato del dispositivo e la password del progetto che lo conteneva. Come posso fare?**

  Eseguire un reset di fabbrica. Sarà quindi possibile utilizzare il dispositivo solo in modalità non protetta.

- **L'aggiornamento del firmware è andato a buon fine ma il dispositivo non funziona.**

  Per riavviarlo, spegnere e riaccendere l'alimentazione (disconnessione/riconnessione della linea KNX TP).

- **Va bene se scollego e ricollego rapidamente il cavo Ethernet?**

  No! Non ricollegare subito il cavo. Attendere alcuni secondi prima della riconnessione.

- **Qual è lo stato del LED programmazione quando il cavo Ethernet non è collegato?**

  Il LED programmazione lampeggia con luce rossa, come quando non è disponibile una rete IP.

- **Quale tipo di errore di trasmissione può essersi verificato quando il LED 2 di stato del bus KNX TP è acceso rosso?**

  Per ogni messaggio che viene inviato su KNX TP, 01548 attende una conferma sulla linea TP. Se il destinatario è occupato (BUSY) o se ha ricevuto dati non corretti (NACK) o se 01548 non ha ricevuto una risposta (IACK mancante), il LED 2 è acceso con luce rossa per indicare che è presente un errore di trasmissione sulla linea.

- **Il LED 2 Stato bus KNX TP lampeggia continuamente con luce verde. Perché?**

  Indica che 01548 è in attesa del download del file del firmware. Per maggiori informazioni e per sapere come tornare al funzionamento normale, vedere il capitolo 6.5.

- **Ho disattivato DHCP e assegnato una configurazione IP corretta, ma non riesco ad accedere al front-end Web.**

  Eseguire un reset del dispositivo 01548 e riprovare. Maggiori informazioni sulla modifica della configurazione della rete IP sono disponibili nel capitolo 4.5.2.

- **Quando cerco di accedere al front-end Web non ci riesco. Come posso fare?**

  Verificare che il front-end Web non sia disattivato e che l'URL nella barra degli indirizzi corrisponda all'indirizzo IP corretto e che la porta HTTP utilizzata sia corretta, oppure utilizzare l'indirizzo MAC esattamente come spiegato (capitolo 6.2.3). Quindi aggiornare il browser e riprovare. Oppure controllare la configurazione IP via TP mediante ETS.

- **È possibile accedere al front-end Web quando il dispositivo è in boot mode?**

  Sì. Il front-end Web è accessibile (capitolo 6.5). Quando è attiva la modalità di avvio, il front-end Web appare come nella Figura 12. Per uscire dalla modalità di avvio è necessario usare la schermata Update del front-end Web, oppure attendere 10 minuti, quando verrà disattivata automaticamente.

- **È possibile eseguire un reset di fabbrica quando il dispositivo è in modalità di avvio?**

  No. Il LED 2 stato bus KNX TP si accende con luce rossa quando si tiene premuto il tasto funzione.

- **Dove posso trovare l'indirizzo IP corrente del mio 01548?**

  Nel front-end Web, nella schermata Device Info (Info dispositivo) è visualizzato l'indirizzo IP corrente.

  Quando ETS può connettersi a 01548 via IP, l'indirizzo IP è contenuto nell'elenco delle Interfacce trovate.

  In Windows, fare clic con il pulsante destro del mouse sul dispositivo di rete per aprire la finestra delle proprietà. Qui sono visualizzati l'indirizzo MAC, l'indirizzo IP, la porta HTTP, il numero di serie e la versione del firmware (versione del software dell'applicazione).

- **Come faccio per accedere al front-end Web se non conosco l'indirizzo IP e l'indirizzo MAC?**

  Quando non è possibile accedere a 01548 tramite l'elenco dispositivi nelle risorse di rete di Windows (dopo aver aggiornato la finestra) è necessario trovare prima l'indirizzo IP. Utilizzare quindi Windows o ETS come descritto nella precedente domanda.

- **Quando può essere necessario inviare IACK sui messaggi inviati?**

  Ad esempio, quando un display fa parte dell'impianto ma non è configurabile mediante ETS.

- **Ho collegato il mio router IP a un router DSL. Posso aprire una porta sul lato WAN per collegare la mia installazione da Internet?**

  Non aprire una porta sul lato WAN. KNXnet/IP, persino KNX IP Secure, non sono progettati per questo scopo. Si raccomanda vivamente di utilizzare una connessione VPN o di utilizzare una soluzione IoT web o KNX disponibile.

CE

01548 IT 01 2011

VIMAR
Viale Vicenza, 14
36063 Marostica VI - Italia
www.vimar.com