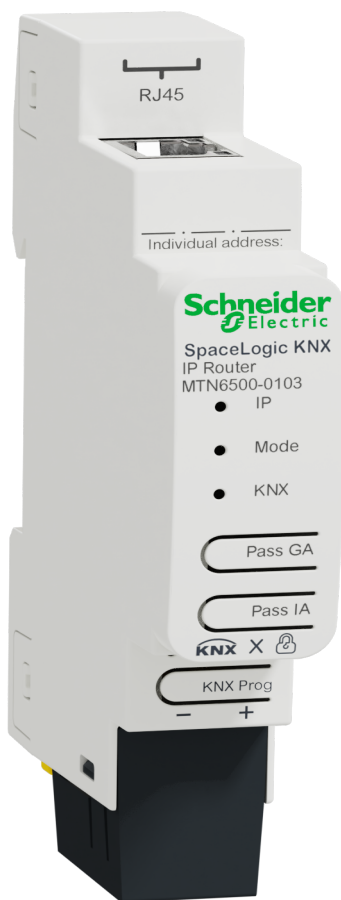


Router IP de Carril DIN SpaceLogic KNX

Información del producto y descripción de la aplicación

Este documento le brinda información sobre el Router IP de Carril DIN SpaceLogic KNX, MTN6500-0103, y describe la aplicación de ETS: Router IP de KNX seguro 7127/1.2.

MTN6500-0103
12/2019



Información legal

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en esta guía son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios. Esta guía y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este manual puede ser reproducida o transmitida de cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otro), para ningún propósito, sin el permiso previo por escrito de Schneider Electric.

Schneider Electric no concede ningún derecho o licencia para el uso comercial de la guía o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

La instalación, utilización, mantenimiento y reparación de los productos y equipos de Schneider Electric la debe realizar solo personal cualificado.

Debido a la evolución de las normativas, especificaciones y diseños con el tiempo, la información contenida en esta guía puede estar sujeta a cambios sin previo aviso.

En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este material o por las consecuencias derivadas o resultantes del uso de la información contenida en el presente documento.

Tabla de contenido

Información de seguridad	5
Por su seguridad	6
Información del producto	7
KNX Security.....	7
KNX IP Security para la función de router	7
KNX IP Security para la función de interfaz.....	7
KNX Data Security para el dispositivo	8
KNX Data Security para telegramas de grupo	8
Instalación y conexión.....	9
Instalación	9
Extracción.....	10
Conexión	10
Datos técnicos.....	11
Función de acoplador (enrutamiento KNXnet/IP y enrutamiento TP).....	12
Router IP KNX como acoplador de línea.....	12
El router IP KNX como acoplador de área.....	13
El Router IP KNX como acoplador de área y de línea	14
Función de acceso al bus (tunelización KNXnet/IP).....	15
Conexiones y elementos de mando.....	16
Modo de programación KNX.....	17
Indicador de estado	18
Modo de funcionamiento manual	19
Ajustes predeterminados de fábrica	20
Restablecimiento de los ajustes de fábrica (restablecimiento maestro).....	20
Ajustes de la interfaz mediante ETS	21
Aplicación ETS.....	22
Proyecto ETS	23
Parámetros adicionales.....	25
Dirección IP	27
Máscara de subred	27
Gateway predeterminada	27
Enrutamiento de la dirección de multidifusión	27
Ejemplo de asignación de direcciones IP.....	28
Acceso remoto	28
Acceso VPN	29
Diálogo de parámetros ETS	30
"Configuraciones generales.....	30
Funcionamiento manual en dispositivo	30
Enrutamiento (KNX → IP)	30
Telegramas de grupo (desde el grupo principal 0 al 13).....	30
Telegramas de grupo (grupos principales 14 a 31).....	30
Telegramas de dirección individual	31
Telegramas a todos los terminales	31

Confirmación (ACK) de telegramas de grupo	31
Confirmación (ACK) de telegramas con dirección física	31
Enrutamiento (IP → KNX)	31
Telegramas de grupo (desde el grupo principal 0 al 13).....	32
Telegramas de grupo (grupos principales 14 a 31).....	32
Telegramas de dirección individual	32
Telegramas a todos los terminales	32
Envío repetido de telegramas de grupo	32
Repetición de telegramas de dirección individual.....	32
Envío repetido de telegramas a todos los terminales	32
Programación	33
A través del bus KNX	33
A través de tunelización KNXnet/IP	33
A través del enrutamiento KNXnet/IP	33
A través de una conexión IP directa	33
Software de código abierto utilizado en el producto:.....	35
Garantía sobre el uso futuro del software de código abierto	35
Directiva RAEE.....	36

Información de seguridad

Información importante

Lea estas instrucciones con atención y observe el equipo para familiarizarse con el dispositivo antes de su instalación, puesta en marcha, reparación o mantenimiento. Es probable que los siguientes mensajes especiales aparezcan a lo largo del presente manual o en el equipo para advertirle sobre posibles peligros o llamar su atención con el propósito de proporcionarle información que aclare o simplifique un procedimiento.



Si se añade uno de estos símbolos a las etiquetas de seguridad «Peligro» o «Advertencia», se está indicando la existencia de un peligro eléctrico que podría provocar lesiones personales en caso de no seguir las instrucciones.



Este es el símbolo de alerta de seguridad y se utiliza para avisarle sobre posibles peligros de lesiones personales. Acate todos los mensajes de seguridad que acompañen este símbolo para evitar posibles lesiones o la muerte.

⚡⚠ PELIGRO
<p>PELIGRO indica una situación peligrosa que, si no se evita, causará la muerte o lesiones graves.</p> <p>Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.</p>
⚠ ADVERTENCIA
<p>ADVERTENCIA indica una situación peligrosa que, si no se evita, podría causar la muerte o lesiones graves.</p>
⚠ ATENCIÓN
<p>PRECAUCIÓN indica una situación peligrosa que, si no se evita, podría causar lesiones leves o moderadas.</p>
AVISO
<p>NOTA se utiliza para abordar prácticas no relacionadas con las lesiones físicas.</p>

Por su seguridad

PELIGRO

PELIGRO DE DESCARGA ELÉCTRICA, EXPLOSIÓN O ARCO ELÉCTRICO

Solo el personal cualificado debe llevar a cabo la instalación eléctrica de forma segura. El personal cualificado debe demostrar poseer amplios conocimientos en las siguientes áreas:

- Conexión a redes de instalación
- Conexión de varios dispositivos eléctricos
- Tendido de cables eléctricos
- Conexión y creación de redes KNX
- Conexión y creación de redes LAN
- Normas de seguridad, normativas y reglamentos sobre cableado

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

Información del producto

El router IP SpaceLogic KNX compacto (en lo sucesivo, **Router IP KNX**) permite el reenvío de telegramas entre diferentes líneas a través de una LAN (IP) que actúa como eje central rápido. El dispositivo también se puede usar como interfaz de programación entre un ordenador y el bus KNX (por ejemplo, para la programación de ETS).

El dispositivo es compatible con KNX Security. Dicha opción puede activarse en ETS. Como router seguro, el dispositivo permite el acoplamiento de comunicaciones no seguras en una línea TP KNX con un eje central IP seguro.

Además, KNX Security evita los accesos no autorizados a la función de interfaz (tunelización).

La dirección IP puede asignarse mediante DHCP o a través de la configuración de ETS. El dispositivo funciona conforme a la especificación KNXnet/IP utilizando los servicios básicos, la administración de dispositivos, la tunelización y el enrutamiento.

El router IP KNX incluye una tabla de filtros ampliada para los grupos principales (entre 0 y 31) y puede almacenar en búfer hasta 150 telegramas. La alimentación se suministra a través del bus KNX.

KNX Security

KNX Security ha ampliado el estándar KNX para proteger las instalaciones KNX ante accesos no autorizados. KNX Security impide el control de las comunicaciones y la manipulación del sistema de forma fiable.

Las especificaciones de KNX Security son diferentes entre KNX IP Security y KNX Data Security. KNX IP Security protege la comunicación en la IP, mientras que en el caso de TP KNX (par trenzado) la comunicación no se cifra. Por consiguiente, KNX IP Security también se puede utilizar en sistemas KNX existentes y con dispositivos TP KNX no seguros.

KNX Data Security entabla el cifrado a nivel de telegrama, lo que significa que los telegramas del bus KNX también están cifrados.

KNX IP Security para la función de router

El acoplamiento de líneas TP KNX individuales a través de la IP se denomina enrutamiento IP KNX. La comunicación entre todos los routers IP KNX conectados se realiza a través de una multidifusión UDP.

Con KNX IP Security, se cifra la comunicación de enrutamiento, de modo que solo los dispositivos IP que conocen la clave pueden descifrar la comunicación y enviar telegramas válidos. En caso de que exista una instalación previa con un router IP antiguo no compatible con IP Security, la instalación al completo podrá funcionar solo como instalación no segura. La marca de hora en el telegrama de enrutamiento garantiza que no se puedan reproducir telegramas previamente almacenados. De esta manera, se evita el llamado ataque de reproducción.

ETS se encarga de asignar la clave para la comunicación de enrutamiento de cada instalación. Si se utiliza KNX IP Security durante el enrutamiento, todos los dispositivos IP KNX conectados deben ser compatibles con Security y estar configurados de forma adecuada.

KNX IP Security para la función de interfaz

Cuando se utiliza el dispositivo como interfaz del bus, cualquier dispositivo que tenga acceso a la red IP podrá acceder a la instalación sin necesidad de sortear

ninguna medida de seguridad. Con KNX Security, es necesario introducir una contraseña. A la hora de transmitir la contraseña, ya se ha establecido una conexión segura. Todas las comunicaciones a través de IP están cifradas y aseguradas.

En ambos modos, la interfaz reenvía telegramas KNX cifrados y no cifrados. El destinatario o herramienta correspondiente se encargará de comprobar las propiedades de seguridad.

KNX Data Security para el dispositivo

Router IP KNX también es compatible con KNX Data Security, que protege el dispositivo ante accesos no autorizados desde el bus KNX. En caso de que Router IP KNX se programe a través del bus KNX, se utilizan los telegramas cifrados.

NOTA: Los telegramas cifrados son más largos que aquellos que no se cifran. Por lo tanto, para realizar una programación a través del bus de forma segura, es necesario que tanto la interfaz utilizada (por ejemplo, USB) como cualquier acoplador de línea intermediario soporten los denominados marcos largos KNX.

La configuración segura de dispositivos también se incluye en KNX Data Security.

KNX Data Security para telegramas de grupo

Los telegramas del bus que no tienen en cuenta Router IP KNX como dispositivo se reenvían o bloquean de acuerdo con los ajustes de los filtros (parámetros y tabla de filtros), sin tener en cuenta si están descifrados o cifrados. El reenvío se basa únicamente en la dirección de destino. El destinatario correspondiente se encargará de comprobar las propiedades de seguridad.

KNX Data Security y KNX IP Security pueden utilizarse de forma paralela. Pongamos, por ejemplo, que un sensor KNX envía al bus un telegrama de grupo cifrado con KNX Data Security. En el momento de reenviarlo a través de IP KNX con KNX IP Security, el telegrama cifrado se volvería a cifrar de igual manera que si se tratase de un telegrama no cifrado. Todos los partícipes del nivel IP KNX compatibles con KNX IP Security pueden decodificar el cifrado IP, pero no la seguridad de los datos. Así, el telegrama de Router IP KNX se transmite de nuevo a las líneas de destino con KNX Data Security. Solo aquellos dispositivos que dispongan de la clave utilizada para la seguridad de datos podrán leer el telegrama.

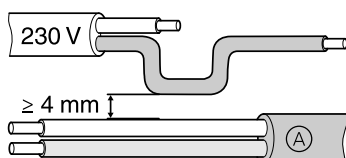
Instalación y conexión

El dispositivo está diseñado para su instalación en un carril DIN con un ancho de 1 unidad (18 mm).

⚡⚠ PELIGRO

PELIGRO DE DESCARGA ELÉCTRICA Y DAÑOS EN EL DISPOSITIVO

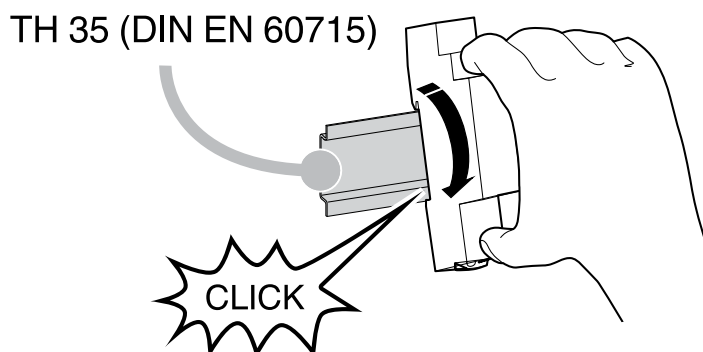
- Compruebe que existe un espacio de seguridad de, al menos, 4 mm entre los núcleos individuales del cable de alimentación de 230 V y la línea KNX ^(A), de acuerdo con la norma IEC 60664-1.



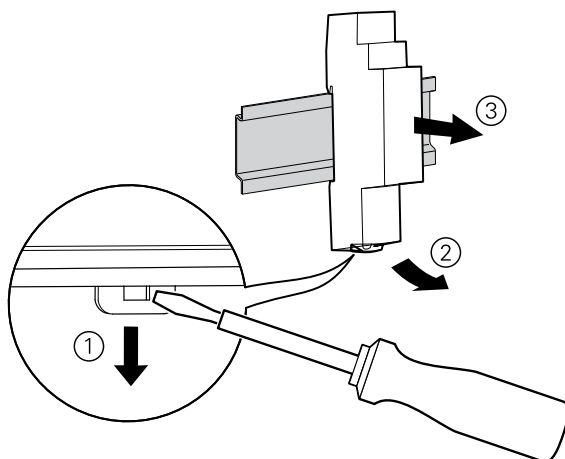
- Compruebe que exista un aislamiento básico mínimo al lado de los dispositivos instalados.

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

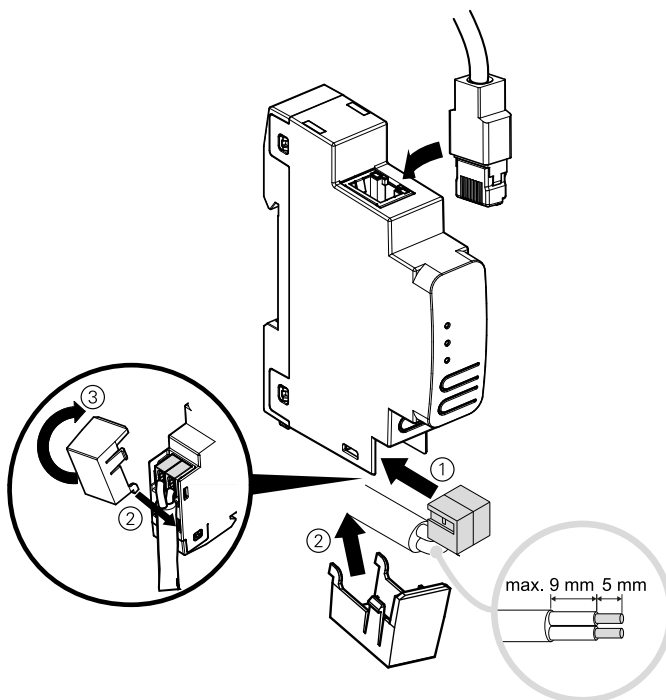
Instalación



Extracción



Conexión



AVISO

DAÑOS EN EL EQUIPO E INTERRUPCIÓN DE LA COMUNICACIÓN

La instalación del cableado de comunicación para la tecnología de la información debe garantizarse de acuerdo con la norma DIN EN 50174.

Si no se siguen estas instrucciones, pueden producirse daños en el equipo.

Datos técnicos

Fuente de alimentación	a través del bus KNX, <20 mA
Conexión	
LAN	Conector RJ45
KNX	Terminal de conexión del bus
Dimensión (LxAnxPr)	
	100x18x86 mm
Ancho del dispositivo	1 módulo = 18 mm

Función de acoplador (enrutamiento KNXnet/IP y enrutamiento TP)

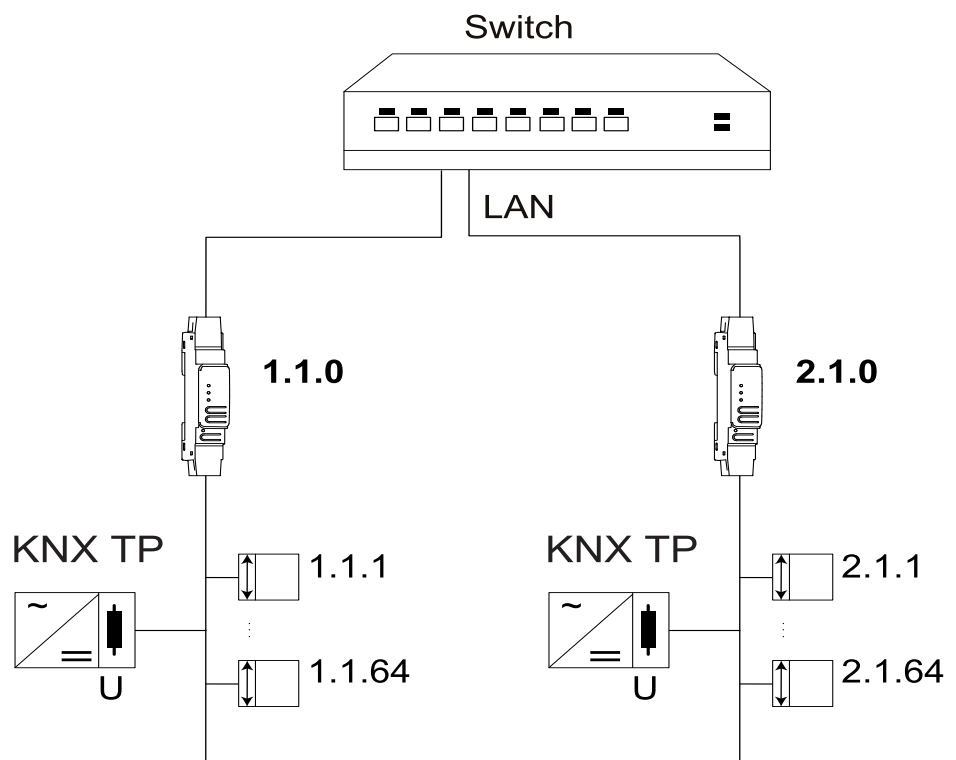
Router IP KNX funciona como acoplador de línea o de área. En ambos casos, se usa la LAN (IP) como eje central.

La siguiente tabla muestra las posibilidades de uso del acoplador SpaceLogic KNX, en comparación con la tipología según la IP:

	Topología clásica (sin IP)	Acoplamiento IP de áreas (acoplador de área IP)	Acoplamiento IP de líneas (acoplador de línea IP)
Área (eje central)	TP	IP	IP
Acoplamiento	Acoplador de línea KNX (máx. 15)	Router IP KNX (máx. 15)	Directamente a través del conmutador LAN
Línea principal	TP	TP	IP
Acoplamiento	Acoplador de línea KNX (máx. 15x15)	Acoplador de línea KNX (máx. 15x15)	Router IP KNX (máx. 225)
Línea	TP	TP	TP

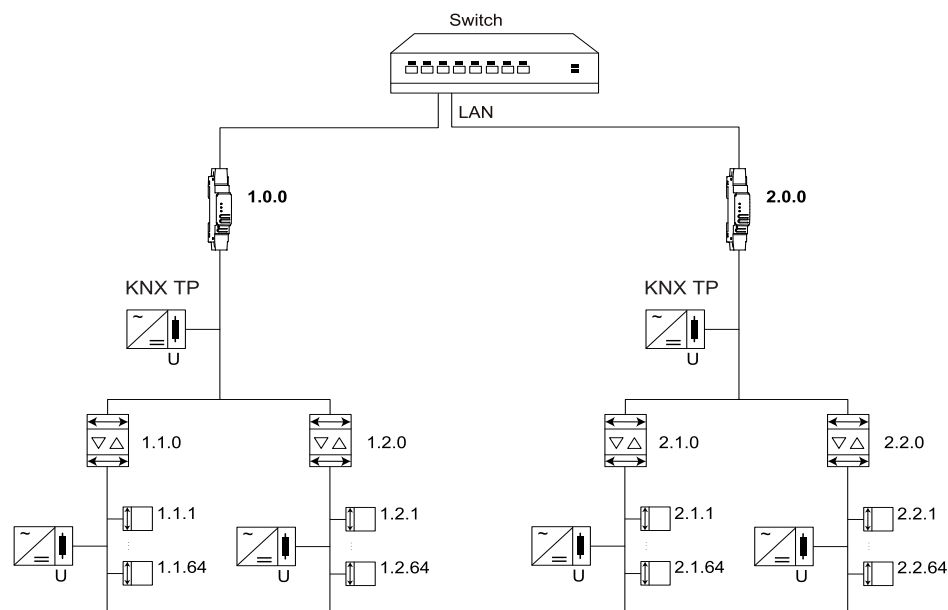
Router IP KNX como acoplador de línea

La dirección individual asignada al acoplador Router IP KNX determina si el dispositivo funciona como acoplador de línea o de área.



Si la dirección individual presenta el formato x.y.0 (x, y: 1-15), ello implica que el router funciona como acoplador de línea. Por su parte, el formato x.0.0 (x: 1-15), implica que el del router actúa como acoplador de área.

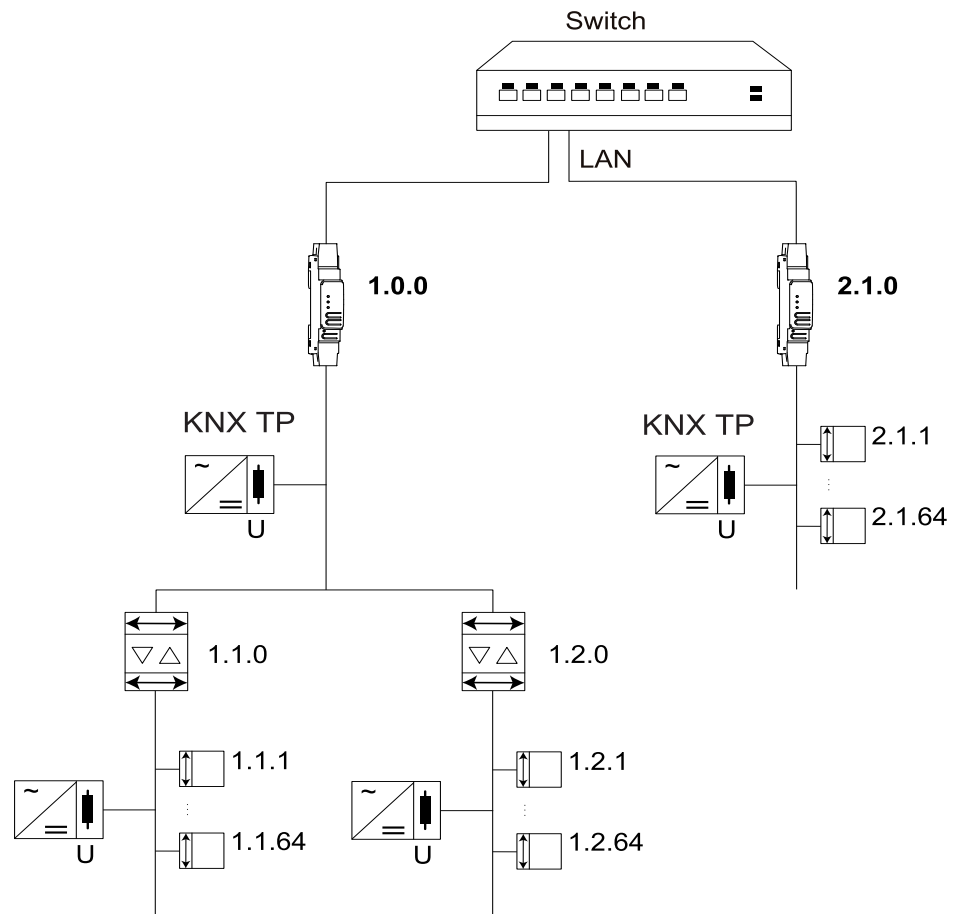
El router IP KNX como acoplador de área



Si el router IP KNX se utiliza como acoplador de área (x.0.0), no debe haber un router IP KNX por debajo de él en la topología. Por ejemplo, si el router IP KNX tiene la dirección individual 1.0.0, no debe haber ningún router IP KNX con la dirección 1.1.0.

Si el router IP KNX se utiliza como acoplador de línea (x.y.0), no debe haber un router IP KNX por encima de él en la topología. Por ejemplo, si el router IP KNX tiene la dirección individual 1.1.0, no debe haber ningún router IP KNX con la dirección 1.0.0.

El Router IP KNX como acoplador de área y de línea



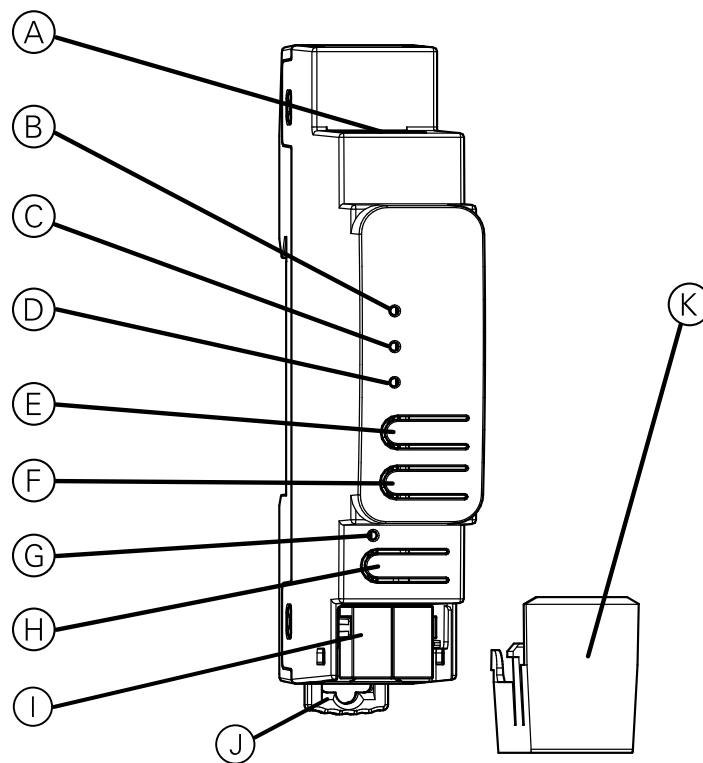
El Router IP KNX incluye una tabla de filtros, por lo que contribuye a reducir la carga del bus. La tabla de filtros (8 kB), generada de manera automática por ETS, puede ampliarse con direcciones de grupo (grupos principales de 0 a 31).

Debido a la diferencia de velocidad entre Ethernet (10/100 Mb/s) y TP KNX (9,6 Kb/s), es posible transmitir un número de telegramas mucho mayor en IP. Si se transmiten varios telegramas por la misma línea de manera consecutiva, estos deben almacenarse en el búfer del router para evitar que se pierdan. El router IP KNX permite almacenar hasta 150 telegramas (de IP a KNX).

Función de acceso al bus (tunelización KNXnet/IP)

El router IP KNX puede utilizarse como interfaz hacia KNX. Es posible acceder al bus KNX desde cualquier punto de la LAN. Para ello, debe asignarse una dirección individual adicional. Podrá encontrar más información al respecto en las secciones siguientes.

Conexiones y elementos de mando




(A)	Conector Ethernet/LAN
(B)	Led IP (multicolor)
(C)	Led de modo (multicolor)
(D)	Led KNX (multicolor)
(E)	Botón: Permitir GA (envío de telegramas de dirección de grupo)
(F)	Botón: Permitir IA (envío de telegramas de dirección individual)
(G)	Led de programación (rojo)
(H)	Botón para el modo de programación
(I)	Conector de bus KNX
(J)	Palanca de liberación para desmontaje
(K)	Cubierta del cable

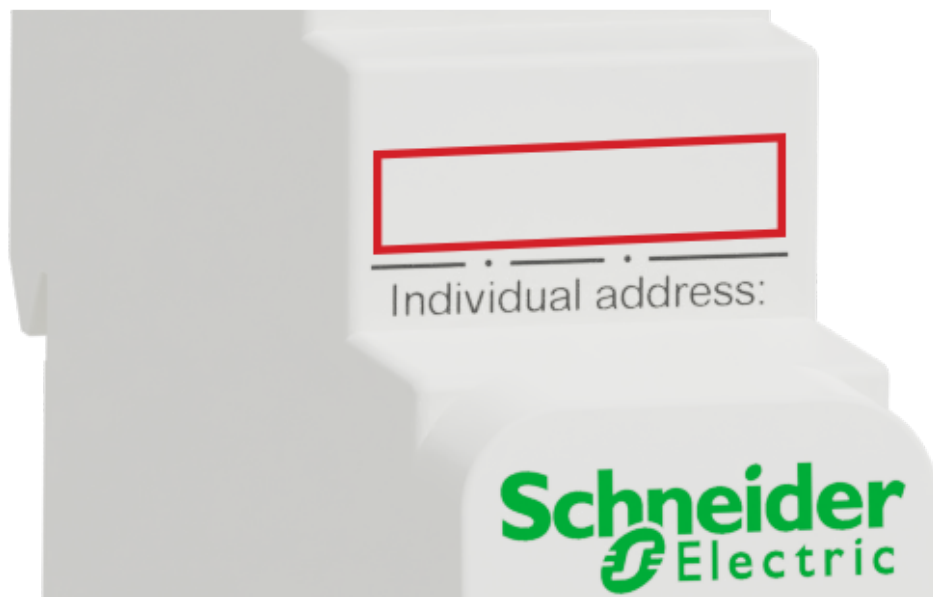
Router IP KNX recibe la alimentación del bus KNX, por lo que no se necesita una fuente de alimentación externa.

NOTA: El dispositivo no funcionará sin la alimentación del bus.

Modo de programación KNX

El modo de programación KNX se activa/desactiva al pulsar el botón de programación KNX .

Es posible escribir la dirección individual programada en el campo destinado a tal uso en el etiquetado con un lápiz o rotulador no permanente. De esta forma, podrá cambiarla en caso necesario.



Indicador de estado

Descripción general de las diferentes indicaciones del led IP

Led IP [ⓑ] Estado	Significado
Led iluminado en color verde	El dispositivo presenta una conexión Ethernet activa y unos ajustes de IP válidos (dirección IP, subred y gateway).
Led iluminado en color rojo	El dispositivo presenta una conexión Ethernet activa y unos ajustes de IP no válidos o aún no ha recibido los ajustes de IP enviados por un servidor DHCP.
Led con parpadeo en color verde	Tráfico de telegramas IP.

Descripción general de las diferentes indicaciones del led de modo


Led de modo [ⓒ] Estado	Significado
Led iluminado en color verde	El dispositivo funciona en el modo de funcionamiento estándar.
Led con 1 parpadeo en color naranja por segundo	El funcionamiento manual se encuentra activo. Reenvío de la dirección individual (IA) o la dirección de grupo (GA).
Led con 2 parpadeos en color naranja por segundo	El funcionamiento manual se encuentra activo. Reenvío de la dirección individual (IA) y la dirección de grupo (GA).
Led con parpadeo en color rojo	El funcionamiento manual no se encuentra activo. El dispositivo no se ha cargado de forma correcta. Por ejemplo, tras una descarga interrumpida.


Descripción general de las diferentes indicaciones del Led KNX



Led KNX [ⓓ] Estado	Significado
Led iluminado en color verde	El bus KNX alimenta de forma correcta el dispositivo
Led con parpadeo en color verde	Tráfico de telegramas en el bus KNX.
Led iluminado brevemente en color rojo	Fallos de comunicación en el bus KNX. Por ejemplo, la repetición de telegramas o de fragmentos de telegramas se indica mediante un breve cambio en el color del led al color rojo.


Modo de funcionamiento manual


Con el objetivo de realizar pruebas (por ejemplo, durante la puesta en marcha), el modo de funcionamiento manual permite ignorar los ajustes de enrutamiento establecidos (filtro o bloqueo).

El botón Permitir GA  permite activar el reenvío de todos los telegramas de dirección de grupo.

El botón Permitir IA  permite activar el reenvío de todos los telegramas de dirección individual.

Esto se indica mediante el parpadeo del led de modo  (1 vez por segundo, en color naranja). Si ambos modos están activados, el led de modo  parpadeará 2 veces por segundo.

Al pulsar de nuevo el botón Permitir GA  o el botón Permitir IA , es posible activar y desactivar estos ajustes según sea necesario.

Si ni el modo de programación ni el modo de funcionamiento manual se encuentran activos, el led  indicará que hay errores en la configuración.





Ajustes predeterminados de fábrica




Se establece la siguiente configuración de fábrica de manera predeterminada:

Dirección individual del dispositivo	15.15.0
Número de configuraciones de tunelización KNXnet/IP realizadas	8
Dirección individual de la configuración de tunelización	15.15.240
Asignación de direcciones IP	DHCP
Clave inicial (FDSK)	activa
Modo de seguridad	no activo

Restablecimiento de los ajustes de fábrica (restablecimiento maestro)

Es posible restablecer los ajustes de fábrica del dispositivo:

1. Desconecte el conector del bus KNX  del dispositivo.
2. Pulse el botón de programación KNX  y manténgalo pulsado.
3. Vuelva a conectar el conector del bus KNX  del dispositivo.
4. Mantenga pulsado el botón de programación KNX  durante al menos 6 segundos.

Un breve parpadeo de todos los ledes (, , ) le indicará que el restablecimiento de los ajustes predeterminados de fábrica se ha realizado correctamente en el dispositivo.

Ajustes de la interfaz mediante ETS

ETS permite seleccionar y configurar interfaces KNX a través del menú **Interfaces del bus (Bus Interfaces)**.

ETS puede acceder a Router IP KNX que se haya configurado, incluso sin una entrada de la base de datos. Si la configuración de Router IP KNX no cumple con las condiciones de la instalación KNX, esta deberá realizarse a través de un proyecto ETS. Para obtener más información, consulte *Proyecto ETS, página 23*.

Si Router IP KNX tiene el modo de seguridad activado, será necesario introducir una contraseña para establecer la conexión.

Como ajuste predeterminado de fábrica, la asignación de la dirección IP se establecerá como **Automática a través del DHCP (Automatically via DHCP)** y, por lo tanto, no será necesario realizar ningún otro ajuste. Para usar esta función, debe disponerse de un servidor DHCP en la LAN (por ejemplo, muchos routers DSL tienen un servidor DHCP integrado).

Una vez Router IP KNX se haya conectado a la LAN y disponga de una dirección IP válida, su denominación aparecerá de manera automática en ETS, dentro del menú **Bus—Interfaces encontradas (Discovered Interfaces)**.

Al hacer clic en **Interfaz encontrada (Discovered Interface)**, esta se seleccionará como la interfaz actual. En el lado derecho de la ventana de ETS, podrá consultar la información relativa, así como las opciones disponibles para dicha conexión.

A continuación, dentro del proyecto ETS, podrá cambiar el nombre del dispositivo indicado y la **dirección individual del host (Host Individual Address)** (dirección individual del dispositivo).

Al igual que todos los dispositivos KNX programables, Router IP KNX dispone de una dirección individual que se puede utilizar para acceder al dispositivo, por ejemplo, cuando se realiza una descarga a Router IP KNX a través del bus.

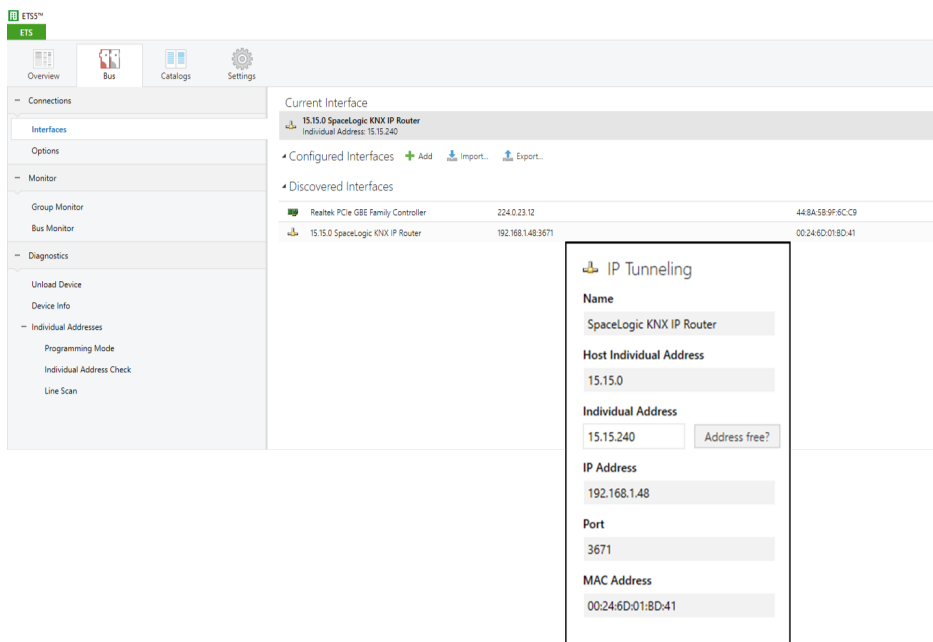
El dispositivo dispone de direcciones individuales adicionales para la función de interfaz que se pueden configurar en ETS. Cuando un cliente (por ejemplo, ETS) envía telegramas al bus a través de Router IP KNX, dichos telegramas incluyen la dirección remitente como una de las direcciones adicionales. Cada una de las direcciones está asociada a una conexión, por lo que los telegramas de respuesta pueden transmitirse sin error al cliente correspondiente.

Las direcciones individuales adicionales se seleccionarán del conjunto de direcciones de la línea de bus en la que está instalada la interfaz y ningún otro dispositivo podrá utilizarlas.

Ejemplo:

Dirección del dispositivo	1.1.0	(dirección dentro de la topología de ETS)
Conexión 1	1.1.240	(Dirección adicional 1)
Conexión 2	1.1.241	(Dirección adicional 2)
Conexión 3	1.1.242	(Dirección adicional 3)
Conexión 4	1.1.243	(Dirección adicional 4)
Conexión 5	1.1.244	(Dirección adicional 5)
Conexión 6	1.1.245	(Dirección adicional 6)
Conexión 7	1.1.246	(Dirección adicional 7)
Conexión 8	1.1.247	(Dirección adicional 8)

La sección **Dirección individual (Individual Address)** le permitirá seleccionar la dirección KNX individual de la conexión de tunelización KNXnet/IP que se encuentre en uso.



La dirección KNX individual del dispositivo y las direcciones KNX individuales para conexiones de tunelización adicionales pueden cambiarse dentro del proyecto ETS, una vez se haya añadido el dispositivo al proyecto.

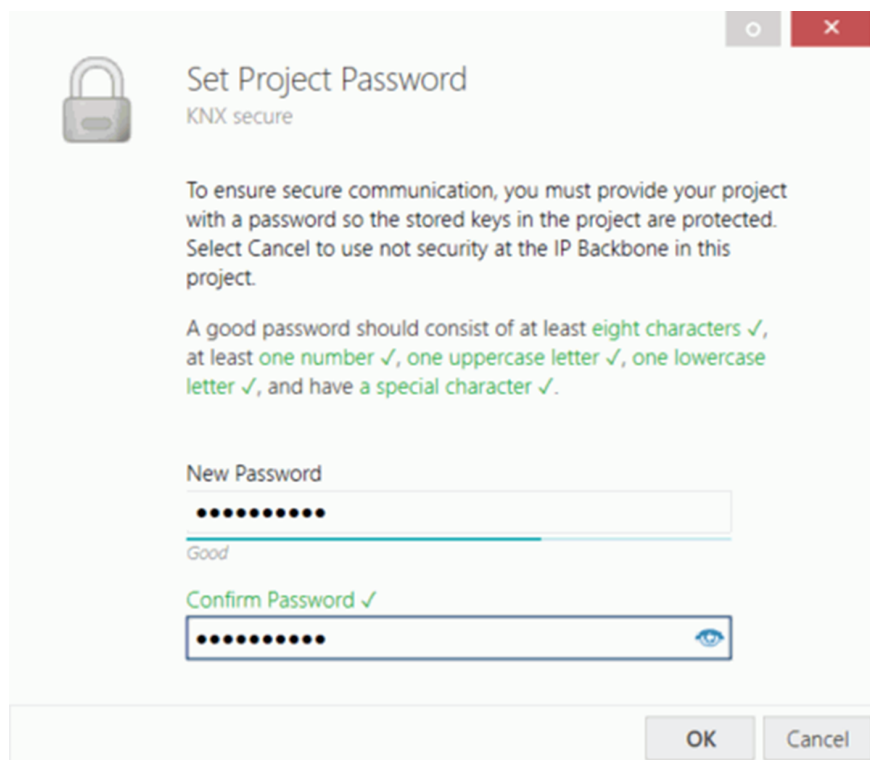
Aplicación ETS

La base de datos de ETS (ETS 5.7.3 o superior) puede descargarse desde el sitio web de producto del Router IP KNX (www.schneider-electric.com) o a través del catálogo en línea KNX.

Familia de productos	1.3 Interfaces/Gateways
Tipo de producto	1.3.14 Dispositivos IP
Fabricante	Schneider Electric Industries SAS
Nombre	Router IP de Carril DIN SpaceLogic KNX
Número de pedido	MTN6500-0103

Proyecto ETS

En el momento en el que se añade el primer producto en un proyecto con KNX Security, ETS le solicitará que introduzca una contraseña para el proyecto.



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** ✓.

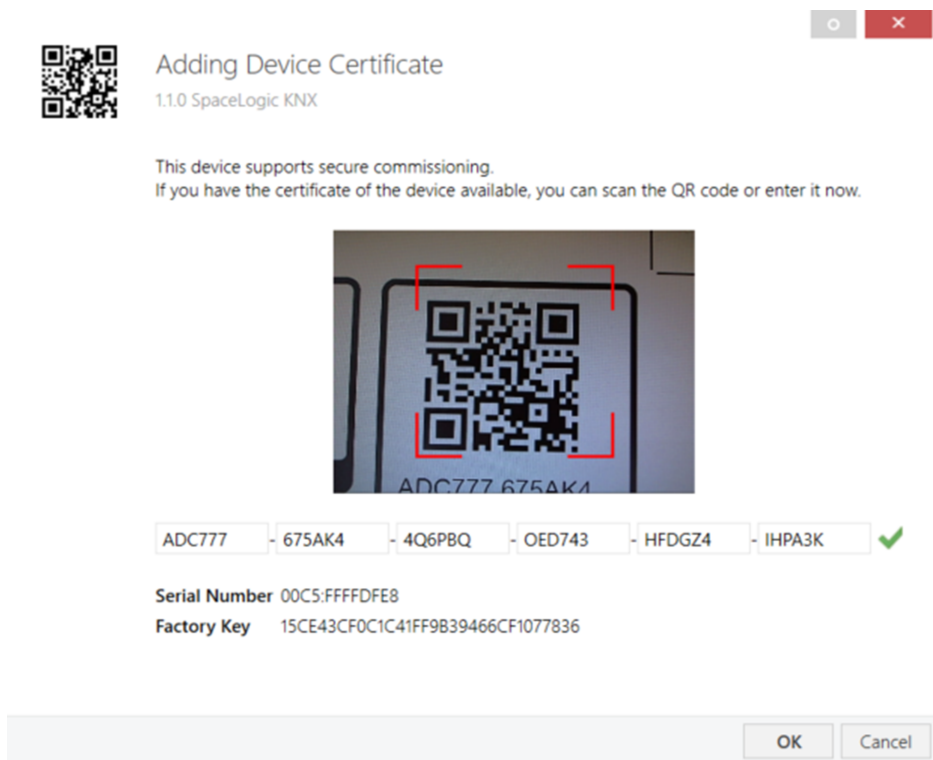
New Password
●●●●●●●●
Good

Confirm Password ✓
●●●●●●●●

OK Cancel

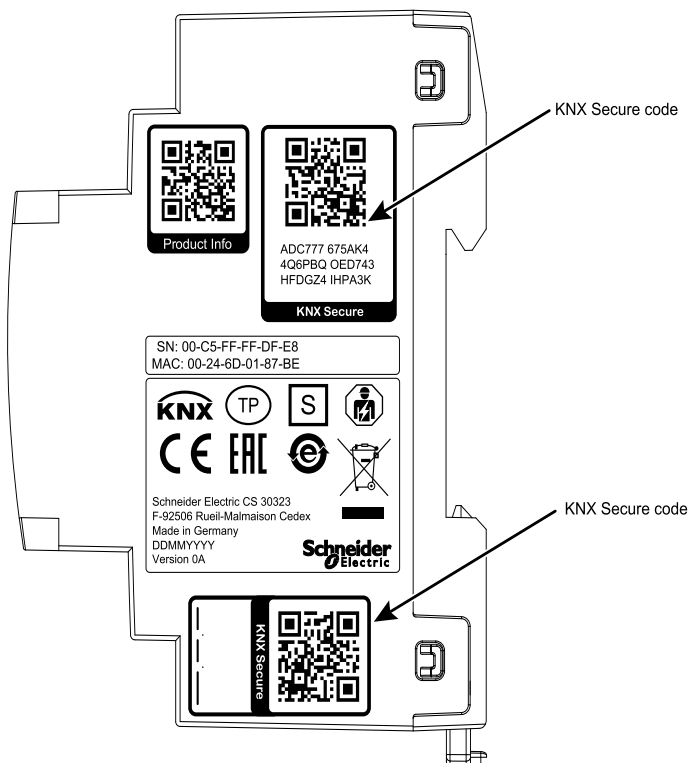
Esta contraseña protege el proyecto ETS ante accesos no autorizados y no constituye una clave utilizada para la comunicación KNX. Es posible omitir la introducción de la contraseña al hacer clic en **Cancelar (Cancel)**, pero, por razones de seguridad, dicha acción no se recomienda.

ETS requiere un certificado de dispositivo para cada uno de los dispositivos con KNX Security que se añaden a ETS. Dicho certificado contiene el número de serie del dispositivo y una clave sólida (FDSK = Factory Default Setup Key).



El certificado se imprime como texto sobre el dispositivo. También se puede obtener de forma sencilla al escanear el código QR impreso con una cámara conectada al ordenador que ejecuta ETS.

El código de KNX Security podrá encontrarse en el lado derecho del dispositivo. Es posible quitar la pequeña pegatina de KNX Security que muestra el código y un espacio de etiquetado y se encuentra situada en la parte inferior del dispositivo para fines de documentación.



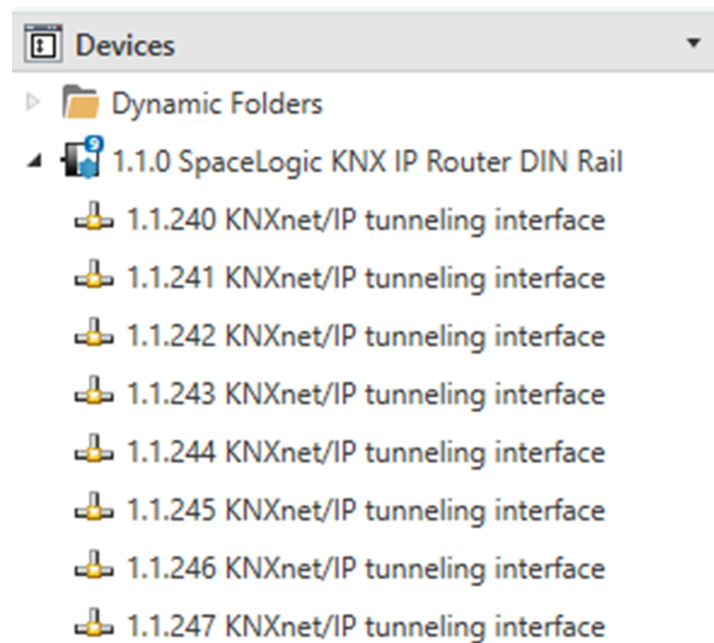
Podrá administrar la lista de certificados de todos los dispositivos en la ventana **Descripción general (Overview) > Proyectos (Projects) > Seguridad (Security)** de ETS.

Esta clave inicial es necesaria para poner un dispositivo en funcionamiento de manera segura desde el inicio. Incluso cuando la descarga de ETS se realiza a través de un tercero, este no tendrá acceso a los dispositivos asegurados. Durante la primera descarga segura, ETS sustituye la clave inicial por una clave nueva que se genera de manera individual para cada dispositivo, lo que impide que personas o dispositivos que puedan conocer la clave inicial accedan al dispositivo. La clave inicial solo se vuelve a activar si se realiza un restablecimiento maestro.

El número de serie del certificado permite que ETS asigne la clave correcta a un dispositivo durante una descarga.

Parámetros adicionales

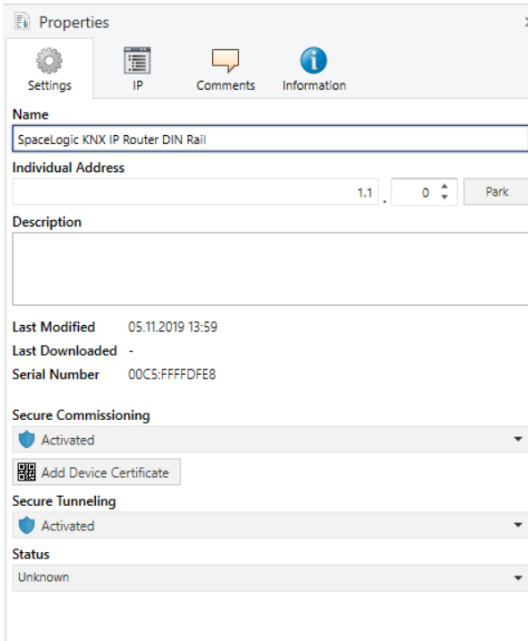
En ETS, existen algunos ajustes adicionales, además de los incluidos en el diálogo de parámetros del diálogo de propiedades (situado en el borde de la pantalla). Aquí, podrá realizar los ajustes relacionados con la IP. Las direcciones adicionales para las conexiones de la interfaz se muestran en la vista de topología.



Es posible cambiar las direcciones KNX individuales haciendo clic en la entrada correspondiente de la lista e introduciendo la dirección deseada en el campo de texto **Dirección individual (Individual Address)**. Si, una vez introducida la dirección, el color del marco del campo de texto cambia a rojo, se está indicando que la dirección ya existe en ese proyecto ETS.

NOTA: Compruebe que ninguna de las direcciones anteriores exista en su instalación KNX.

Al hacer clic en la entrada del dispositivo Router IP KNX desde la vista de topología de proyectos ETS, aparecerá la columna de información **Propiedades (Properties)** en el lado derecho de la ventana de ETS. En la descripción general de **Ajustes (Settings)**, podrá cambiar el nombre del dispositivo.



Properties

Settings IP Comments Information

Name
SpaceLogic KNX IP Router DIN Rail

Individual Address
1.1 . 0 Park

Description

Last Modified 05.11.2019 13:59
Last Downloaded -
Serial Number 00CS:FFFFDFE8

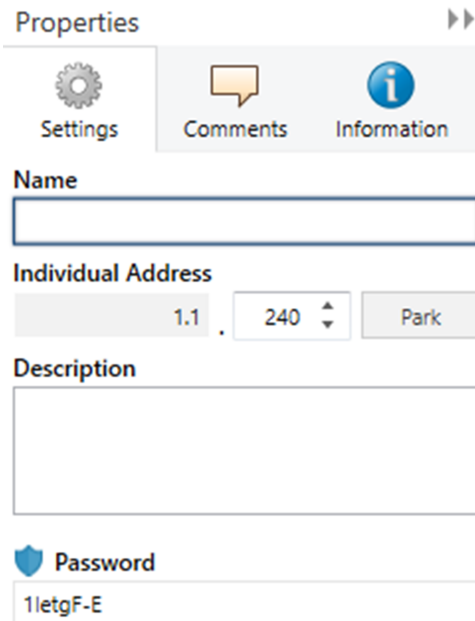
Secure Commissioning
Activated

Add Device Certificate

Secure Tunneling
Activated

Status
Unknown

Si se activa la tunelización segura, se creará una contraseña única para cada túnel de forma automática. Dicha contraseña puede consultarse en la descripción general de **Ajustes (Settings)** al seleccionar un túnel.



Properties

Settings Comments Information

Name

Individual Address
1.1 . 240 Park

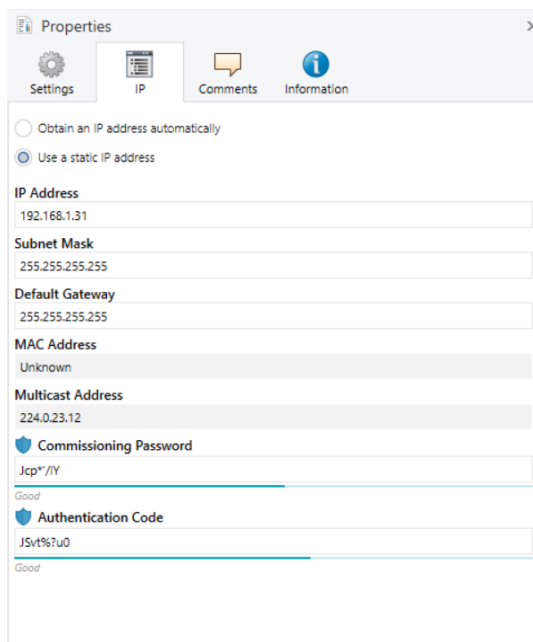
Description

Password
1letgF-E

Es posible modificar las opciones específicas de la red IP de Router IP KNX en la descripción general de **IP**.

Al cambiar la opción **Obtener dirección IP de forma automática (a través del DHCP (Obtain an IP address automatically [via DHCP]))** por **Usar una dirección IP estática (Use a static IP address)** (dirección IP estática), podrá configurar libremente la dirección IP, la máscara de subred y la gateway establecida de forma predeterminada.

NOTA: Los cambios realizados en el menú **Propiedades (Properties)** solo se aplicarán una vez se haya descargado la aplicación de forma correcta.



Dirección IP

Aquí podrá introducir la dirección IP de Router IP KNX, que se utilizará para dirigir el dispositivo a través de la red IP (LAN). El direccionamiento IP debe coordinarse con el administrador de la red.

Máscara de subred

Aquí podrá definir la máscara de subred. El dispositivo utiliza los valores introducidos en esta máscara para determinar si existe un interlocutor en la red local. En caso de no haberlo, el dispositivo no enviará los telegramas directamente al interlocutor, sino a la gateway, quien encaminará el telegrama.

Gateway predeterminada

Introduzca la dirección IP de la gateway aquí. Por ejemplo, el router DSL de la instalación.

Enrutamiento de la dirección de multidifusión

Esta dirección se utiliza para transmitir telegramas en IP. Se ha reservado la dirección IP de multidifusión **224.0.23.12** (KNXnet/IP) en la IANA (Autoridad de asignación de números de Internet) para dicho uso. En caso de necesitar una dirección IP de multidifusión diferente, esta debe encontrarse dentro del rango comprendido entre **239.0.0.0** y **239.255.255.255**.

Ejemplo de asignación de direcciones IP

Es posible acceder a Router IP KNX mediante un ordenador.

Dirección IP del ordenador	192.168.1.30
Subred del ordenador	255.255.255.0

Router IP KNX se ubica en la misma LAN, es decir, utiliza la misma subred. La subred limita el número de direcciones IP que se pueden asignar. En este ejemplo, la dirección IP de Router IP KNX será **192.168.1.xx**, donde xx constituye un número comprendido entre el 1 y el 254 (a excepción del 30, que ya utiliza el ordenador cliente). Es importante verificar que las direcciones IP no se asignen dos veces.

Router IP KNX: dirección IP	192.168.1.31
Router IP KNX: subred	255.255.255.0

Acceso remoto

Router IP KNX permite acceder a internet de forma remota.

AVISO
<p>DAÑOS MATERIALES DERIVADOS DE UN ACCESO NO AUTORIZADO A LA INSTALACIÓN KNX</p> <p>Una vez acceda a la instalación KNX a través de internet, el tráfico de datos quedará expuesto ante terceros.</p> <ul style="list-style-type: none"> • Para llevar a cabo esta conexión, utilice solo un acceso VPN que incluya un cifrado seguro para todos los paquetes de datos. • El hardware requerido (router VPN) y las funcionalidades ofrecidas por los proveedores de servicios móviles difieren significativamente según el país o región, en lo que respecta a los ajustes y las posibilidades técnicas. • Asegúrese de que un proveedor de servicios VPN especializado configure el acceso VPN y lo mantenga siempre preparado para su uso. El proveedor de servicios VPN se encargará de seleccionar el proveedor de servicios móviles y hardware adecuados para disponer de un acceso VPN, lo que garantiza que el VPN cuente con la garantía de un especialista cualificado. <p>Schneider Electric no se responsabiliza de problemas en el funcionamiento o de incompatibilidades originadas por aplicaciones, servicios o dispositivos de un tercer proveedor. Schneider Electric no ofrece soporte técnico a la hora de configurar un acceso VPN.</p> <p>Si no se siguen estas instrucciones, pueden producirse daños en el equipo.</p>

Acceso VPN

El acceso VPN (Red privada virtual) permite que un dispositivo portátil acceda a la red local a través de Internet y, por lo tanto, también a la instalación KNX.

Ventajas del acceso VPN:

- Solo los usuarios autorizados tienen acceso a la red local.
- Todos los datos están cifrados.
- Durante la transferencia, los datos no se modifican, guardan ni desvían. A menudo, a esto se le denomina túnel VPN.

Requisitos para configurar una conexión VPN:

- Conexión a Internet.
- Dispositivo portátil y router habilitados para una conexión VPN (cliente VPN instalado).

Diálogo de parámetros ETS

A través de ETS, pueden ajustarse los siguientes parámetros.

"Configuraciones generales

Funcionamiento manual en dispositivo

Este parámetro establece la duración del modo manual. Al finalizar, se restablece el modo de funcionamiento normal.

Enrutamiento (KNX → IP)

Telegramas de grupo (desde el grupo principal 0 al 13)

Bloqueados	Ningún telegrama de grupo incluido en estos grupos principales se encamina a IP.
Encaminados	Todos los telegramas de grupo incluidos en estos grupos principales se encaminan a IP, sin tener en cuenta la tabla de filtros. Este ajuste se utiliza únicamente para realizar pruebas.
Filtro	Se utiliza la tabla de filtros para verificar si el telegrama de grupo recibido debe encaminarse o no a IP.

Telegramas de grupo (grupos principales 14 a 31)

Bloqueados	Ningún telegrama de grupo incluido en estos grupos principales se encamina a IP.
Encaminados	Todos los telegramas de grupo incluidos en estos grupos principales se encaminan a IP, sin tener en cuenta la tabla de filtros. Este ajuste se utiliza únicamente para realizar pruebas.
Filtro	Se utiliza la tabla de filtros para verificar si el telegrama de grupo recibido debe encaminarse o no a IP.

Telegramas de dirección individual

<i>Bloqueados</i>	Los telegramas de dirección individual no se transmiten a IP.
<i>Encaminados</i>	La totalidad de los telegramas de dirección individual recibidos se transmiten a IP.
<i>Filtro</i>	Se utiliza la dirección individual para verificar si el telegrama de dirección individual recibido debe encaminarse a IP.

Telegramas a todos los terminales

<i>Bloqueados</i>	Los telegramas a todos los terminales recibidos no se transmiten a IP.
<i>Encaminados</i>	La totalidad de los telegramas a todos los terminales recibidos se transmiten a IP.

Confirmación (ACK) de telegramas de grupo

<i>Siempre</i>	Se genera una confirmación por cada telegrama de grupo recibido (de KNX).
<i>Solo ante transmisión</i>	Solo se genera confirmación para aquellos telegramas de grupo recibidos (de KNX) que se encaminan a IP.

Confirmación (ACK) de telegramas con dirección física

<i>Siempre</i>	Se genera una confirmación por cada telegrama de dirección individual recibido (de KNX).
<i>Solo ante transmisión</i>	Solo se genera confirmación para aquellos telegramas de dirección individual recibidos (de KNX) que se encaminan a IP.
<i>Respuesta con NACK</i>	Se responde con NACK (Sin confirmar) a todos los telegramas con dirección individual recibidos (de KNX). Esto significa que no es posible establecer la comunicación con telegramas de dirección individual en la línea KNX en cuestión. La comunicación de grupo (telegramas de grupo) no se ve afectada. Puede utilizarse este ajuste para bloquear intentos de manipulación.

NOTA: Cuando se utiliza **Respuesta con NACK (Answer with NACK)**, ya no es posible acceder al dispositivo a través del TP KNX. La configuración deberá realizarse a través del IP. Es posible utilizar esta opción para dotar a la instalación de una mayor seguridad.

Enrutamiento (IP → KNX)

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

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	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Repetition of group telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of individual addressed telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of broadcast telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Telegramas de grupo (desde el grupo principal 0 al 13)

<i>Bloqueados</i>	Ningún telegrama de grupo incluido en estos grupos principales se encamina a KNX.
<i>Encaminados</i>	Todos los telegramas de grupo incluidos en estos grupos principales se encaminan a KNX, sin tener en cuenta la tabla de filtros. Este ajuste se utiliza únicamente para realizar pruebas.
Filtro	Se utiliza la tabla de filtros para verificar si el telegrama de grupo recibido debe encaminarse a KNX.

Telegramas de grupo (grupos principales 14 a 31)

<i>Bloqueados</i>	Ningún telegrama de grupo incluido en estos grupos principales se encamina a KNX.
<i>Encaminados</i>	Todos los telegramas de grupo incluidos en estos grupos principales se encaminan a KNX, sin tener en cuenta la tabla de filtros. Este ajuste se utiliza únicamente para realizar pruebas.
Filtro	Se utiliza la tabla de filtros para verificar si el telegrama de grupo recibido debe encaminarse a KNX.

Telegramas de dirección individual

<i>Bloqueados</i>	Los telegramas de dirección individual no se transmiten a KNX.
<i>Encaminados</i>	La totalidad de los telegramas de dirección individual recibidos se transmiten a KNX.
Filtro	Se utiliza la dirección individual para verificar si el telegrama de dirección individual recibido debe encaminarse a KNX.

Telegramas a todos los terminales

<i>Bloqueados</i>	Los telegramas a todos los terminales recibidos no se transmiten a KNX.
<i>Encaminados</i>	La totalidad de los telegramas a todos los terminales recibidos se transmiten a KNX.

Envío repetido de telegramas de grupo

<i>Bloqueado</i>	El telegrama de grupo recibido no se enviará a KNX en caso de fallo.
Permitido	El telegrama de grupo recibido se enviará hasta tres veces en caso de fallo.

Repetición de telegramas de dirección individual

<i>Bloqueado</i>	El telegrama de dirección individual recibido no se enviará a KNX en caso de fallo.
Permitido	El telegrama de dirección individual recibido se enviará hasta tres veces en caso de fallo.

Envío repetido de telegramas a todos los terminales

<i>Bloqueado</i>	El telegrama a todos los terminales recibido no se enviará a KNX en caso de fallo.
Permitido	El telegrama a todos los terminales recibido se enviará hasta tres veces en caso de fallo.

Programación

Router IP KNX se puede programar de diferentes maneras a través de ETS:

A través del bus KNX

El dispositivo solo debe conectarse al bus KNX. ETS requiere una interfaz adicional (por ejemplo, USB) para tener acceso al bus. De este modo, se pueden programar tanto la dirección individual como toda la aplicación, incluida la configuración IP. Se recomienda realizar la programación a través del bus si no se puede establecer una conexión IP.

A través de tunelización KNXnet/IP

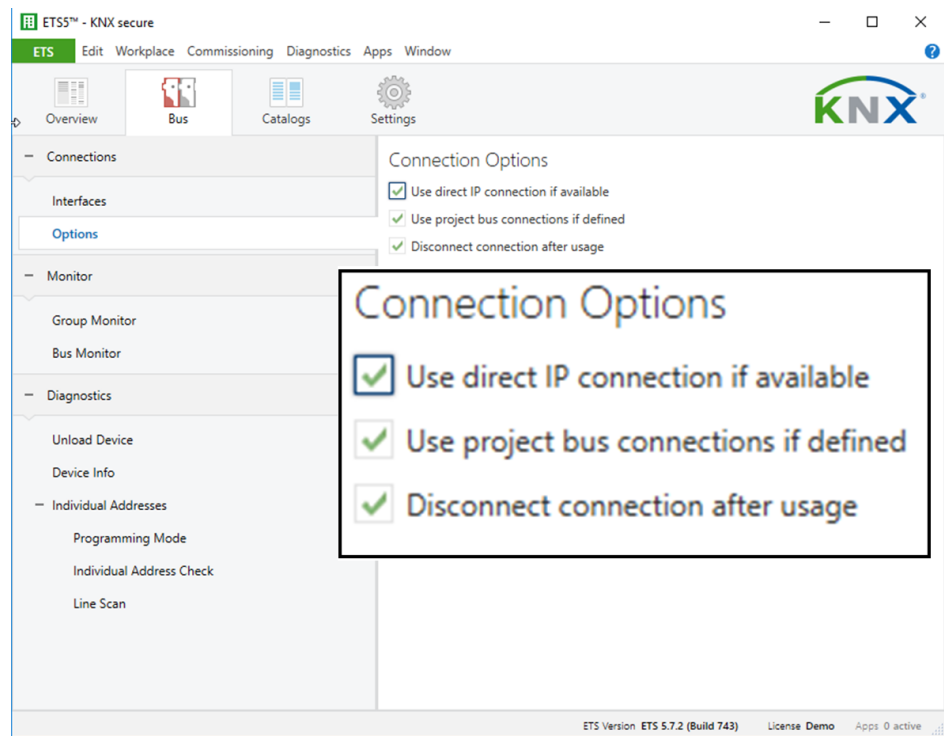
No se necesita ninguna interfaz adicional. La programación a través de la tunelización KNXnet/IP es posible si el dispositivo dispone de una configuración IP válida (por ejemplo, mediante DHCP). En dicho caso, el dispositivo se mostrará en la configuración de la interfaz de ETS y deberá seleccionarse. La descarga se realizará a través del proyecto ETS, tal como ocurre en el caso de otros dispositivos.

A través del enrutamiento KNXnet/IP

La programación a través del enrutamiento KNXnet/IP es posible si el dispositivo ya presenta una configuración IP válida (por ejemplo, mediante DHCP o IP automática). En ETS, la interfaz de enrutamiento aparecerá si hay, al menos, un dispositivo disponible en la red que en la que se va a realizar el enrutamiento. El nombre de la interfaz de red se mostrará como descripción en el ordenador. Si se selecciona el enrutamiento como interfaz, la programación se realizará desde el proyecto ETS, tal como se sucede con otros dispositivos. En dicho caso, se utiliza la LAN como un medio KNX, al igual que TP. No se requiere ningún dispositivo de interfaz adicional.

A través de una conexión IP directa

Si bien la tunelización KNXnet/IP y el enrutamiento KNXnet/IP están limitados a la velocidad de TP KNX, es posible cargar el dispositivo a alta velocidad, a través de una conexión IP directa. Podrá realizarse una conexión IP directa si el dispositivo ya cuenta con una configuración IP válida y una dirección individual (esta también puede ser la dirección individual predeterminada). Para llevar a cabo la conexión, seleccione la opción **Usar conexión IP directa cuando esté disponible (Use direct IP connection if available)** en el menú **Opciones > de conexiones de bus > (Bus Connections Options)** de ETS. De esta manera, la descarga se realizará directamente en el dispositivo y no se podrá ver en el monitor de grupos de ETS.



NOTA: Se recomienda realizar las descargas a través de la IP, debido a sus tiempos de transmisión considerablemente más cortos.

Software de código abierto utilizado en el producto:

El producto contiene, entre otras cosas, archivos de software de código abierto, como se especifica a continuación, desarrollados por terceros y con licencia bajo una licencia de software de código abierto. Los archivos de dicho software de código abierto están protegidos por derechos de autor. Su derecho a usar el software de código abierto se rige por las condiciones de licencia de software de código abierto aplicables.

El cumplimiento de dichas condiciones de licencia le permitirá utilizar el software de código abierto según lo previsto en la licencia en cuestión. En caso de conflictos entre otras condiciones de licencia de Schneider Electric aplicables al producto y las condiciones de licencia del software de código abierto, prevalecerán las condiciones del software de código abierto. El software de código abierto se proporciona sin regalías (es decir, no se cobran tarifas por ejercer los derechos de licencia). La lista de software de código abierto contenido en este producto y los respectivos términos y condiciones aplicables se enumeran a continuación:

Lista de archivos de software de código abierto	Licencias aplicables
curve25519-donna	Consulte https://github.com/agl/curve25519-donna

Si el software de código abierto contenido en este producto tiene licencia bajo Licencia pública general GNU (GPL), Licencia pública general menor GNU (LGPL), Licencia pública de Mozilla (MPL) o cualquier otra licencia de software de código abierto que requiera que el código fuente esté disponible, puede descargar el código fuente correspondiente del software de código abierto desde el siguiente enlace:

Lista de archivos de software de código abierto	Acceso a los archivos de software de código abierto
curve25519-donna	Consulte https://github.com/agl/curve25519-donna

Garantía sobre el uso futuro del software de código abierto

Schneider Electric SE y todas sus subsidiarias («Schneider Electric Group») no proporcionan garantía para el software de código abierto contenido en este producto, si dicho software de código abierto se usa de formas distintas de la prevista por Schneider Electric Group. Las licencias enumeradas con anterioridad definen la garantía, si existe, de los autores o licenciadores del software de código abierto. Schneider Electric Group específicamente renuncia a toda garantía por defectos producidos al alterar cualquier software de código abierto o la configuración del producto. Se excluyen las reclamaciones de garantía contra Schneider Electric Group en caso de que el software de código abierto contenido en este producto infrinja los derechos de propiedad intelectual de un tercero.

El soporte técnico, de haberlo, solo se proporcionará para software no modificado.

Directiva RAEE



Deseche el dispositivo separado de la basura doméstica en los puntos de recogida oficiales.

Realizar un buen reciclado protege a las personas y al medio ambiente de posibles efectos negativos.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

Para consultas técnicas, póngase en contacto con el servicio de atención al cliente de su país.
www.schneider-electric.com/contact

www.schneider-electric.com

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.

© 2019 – Schneider Electric. Reservados todos los derechos

MTN6500-0103_SW_ES