dormakaba

Connector One G2

Instrucciones de operación

060949 45532/TECHDOC-716 - 02/2026

ES

Contenido

1 Información sobre este documento

1.1 Contenido y finalidad

Estas instrucciones describen la utilización del Connector One G2.

1.2 Grupo objetivo

Este documento está dirigido a técnicos cualificados.
Un técnico cualificado cuenta con la formación técnica adecuada y experiencia en el uso de la tecnología. Es responsabilidad del técnico asegurarse de que al manipular el producto descrito se respeten las condiciones especificadas por el fabricante, así como los reglamentos y normas aplicables.

1.3 Conservación de los documentos

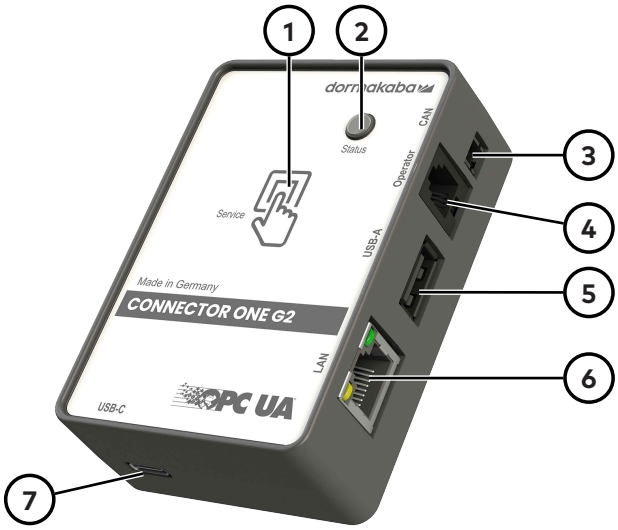
Este documento y los demás documentos aplicables deben entregarse al operador. Los documentos deben conservarse durante toda la vida útil del producto y ponerse a disposición del personal.

1.4 Uso previsto

- Ampliación de los sistemas de puerta dormakaba mediante la incorporación de una interfaz Ethernet.
- Uso en el interior de edificios

2 Descripción del producto

Con un Connector One G2, las puertas y los sistemas de puertas automáticos de dormakaba pueden ampliarse para incluir una interfaz de red. Esto posibilita el acceso remoto a través de la red local. El intercambio de datos independiente de la plataforma tiene lugar de forma segura mediante el estándar OPC UA. Connector One G2 proporciona un amplio acceso a la información y a las opciones de control a los sistemas de edificios inteligentes compatibles con OPC UA. Además, el Connector One G2 es compatible con el EntriWorX EcoSystem. Los dispositivos conectados se pueden monitorizar, controlar y administrar mediante EntriWorX Insights.



1 Botón de servicio para configurar el Connector One G2

2 LED de estado

3 Conexión CAN BUS*

4 Interfaz RS 232 para la conexión al control del accionamiento

5 Interfaz USB-A
AVISO La interfaz USB-A solo debe utilizarse para dispositivos autorizados***. No se deben conectar otros dispositivos, ya que esto puede provocar interferencias o — en casos extremos— daños.

6 Interfaz LAN para la conexión a la red del cliente o al ordenador

7 Interfaz USB-C para alimentación eléctrica

2.1 Datos técnicos

Tensión**	24 V CC ± 20 % / 5 V CC
Temperatura de funcionamiento	-15 °C a +55 °C
Hum. relativa del aire	5 % a 95 %
Interfaces	RS232, LAN, USB-A, USB-C, CAN*
Radio	Bluetooth LE

* Destinado a futuras aplicaciones

** La alimentación eléctrica tiene lugar directamente a través del accionamiento de la puerta o mediante la interfaz USB-C y una fuente de alimentación USB.

*** La lista con los dispositivos aprobados se puede descargar aquí: https://www.dormakaba.com/connector-one

2.2 Pila de litio

El dispositivo incorpora una pila de litio del tipo CR1220 como pila de respaldo.

La pila no requiere servicio ni mantenimiento. La pila está dimensionada para durar hasta el final del ciclo de vida.

Tenga en cuenta las normas de seguridad para el transporte de dispositivos con pilas de litio.

2.3 Conformidad

2.3.1 Declaración UE de conformidad

Este capítulo es un extracto de la declaración de conformidad completa.

dormakaba Alemania GmbH
DORMA Place 1
58256 Ennepetal
Alemania

declara por la presente que el producto descrito cumple los requisitos de la(s) Directiva(s) enumerada(s), y que se han aplicado las normas y/o especificaciones técnicas a las que se hace referencia a continuación.

Directivas:

2014/53/EU	Equipos radioeléctricos
2011/65/UE	RoHS

Para obtener los documentos técnicos dirigirse al responsable de conformidad del producto enviando un mensaje a product-compliance.dach@dormakaba.com

Normativa europea armonizada, normativas nacionales:

EN 301 489-1 V 2.2.3:2019

EN 301 489-3 V 2.1.1:2019

EN 62368-1:2014+AC:2015

EN IEC 63000:2018

EN 62479:2010

2.3.2 Declaración de conformidad de UKCA

Este capítulo es solo un extracto de la declaración de conformidad completa.

dormakaba Alemania GmbH
DORMA Place 1
58256 Ennepetal
Alemania

declara por la presente que el producto descrito cumple los requisitos de la(s) Directiva(s) enumerada(s), y que se han aplicado las normas y/o especificaciones técnicas a las que se hace referencia a continuación.

Directivas:

Reglamento de equipos radioeléctricos 2017

RoHS, Restricción de ciertas Sustancias Peligrosas en aparatos eléctricos y electrónicos 2012

Para obtener los documentos técnicos dirigirse al responsable de conformidad del producto enviando un mensaje a product-compliance.dach@dormakaba.com

Normativa europea armonizada, normativas nacionales:

EN 301 489-1 V 2.2.3:2019

EN 301 489-3 V 2.1.1:2019

EN 62368-1:2014+AC:2015

EN IEC 63000:2018

EN 62479:2010

2.3.3 FCC e IC

FCC El producto cumple los requisitos de:

- **Título 47 CFR Parte 15 de la FCC**
  ID de la FCC: NVI-CON1G2

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

§ 15.105 Class B This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

§ 15.21 [Any] changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IC El producto cumple los requisitos de:

- **ISED Canadá RSS-247 e ISED Canadá RSS-Gen**
  IC: 11038A-CON1G2

2.4 Códigos LED

Estado	Color	Modo
Inicio del sistema	amarillo	intermitencia lenta
Se requiere configuración	amarillo	encendido permanentemente
Listo para funcionar, se ha detectado un control de puerta	verde	encendido permanentemente
Listo para funcionar, no se ha detectado un control de puerta	verde	intermitencia lenta
Error	rojo	encendido permanentemente
Modo de servicio o conexión Bluetooth activa	azul	encendido permanentemente
Modo de servicio activado o identificación de dispositivo activa	azul	intermitencia lenta
Transmisión de datos/actualización del software	cian	intermitencia rápida

2.5 Accionamientos y sistemas de puertas compatibles

Productos con protocolo TMS

ED 100
ED 250
ED 250 PA
ED 900
ES PROLINE Easy
ES PROLINE Standard
ES PROLINE FST
ES PROLINE FST FIA
ES 200
ES 200-2D
ES 200 SWR
ES 200 FIA
FFT
FFT-2D
KTV
KTC 2

Productos con protocolo Datalink a partir de ETS22

Kerberos TPB
Kentaur FTS
Kentaur FGE-Mxx
Charon HTS
Charon HSD
Argus 40/60/80
Argus V60
Argus HSB
Orthos PIL-M02
Geryon

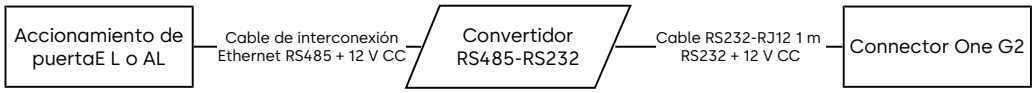
Productos con protocolo de terminal de mano del controlador ESA2:

ESA 100
ESA 200
ESA 300
ESA 400
ESA 500

Productos con protocolo EL

EL 301	AL 501
AL 401	AL 1001

Para estos accionamientos de puerta se necesita un convertidor RS485/RS232 (n.º de artículo 29262009) para posibilitar la conexión al Connector One G2.



2.6 Puntos de datos OPC UA y actualizaciones de software

Dado que el modelo de información y el software Connector One G2 se desarrollan constantemente y se añaden dispositivos y funciones adicionales según sea necesario, las actualizaciones de software y las tablas de puntos de datos OPC UA para los accionamientos específicos pueden consultarse en línea en el portal my.dormakaba.
Para ello es necesario registrarse gratuitamente una sola vez en:
https://portal.dormakaba.com/registration
Tras iniciar sesión, los datos del Connector One G2 pueden consultarse en:
https://dormakaba.com/connector-one

3 Puesta en funcionamiento

3.1 Requisitos previos para la puesta en marcha

Dispositivos TMS
La interfaz RS232 del control del accionamiento está configurada como modo TMS.

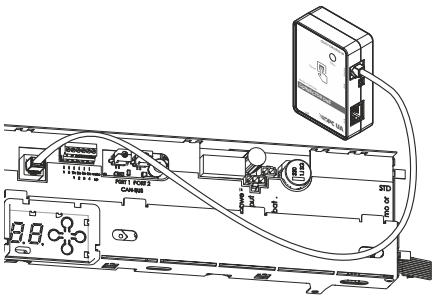
ETS22
Hay disponible una interfaz RS232.

Accionamientos EL
Hay disponible un convertidor RS485/RS232.

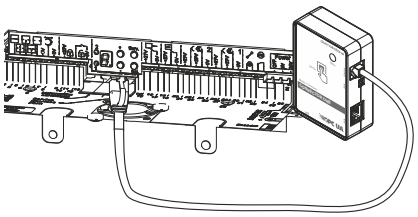
3.2 Conexión del Connector One G2

Conecte el Connector One G2 a la unidad de control a través de la interfaz RS 232.

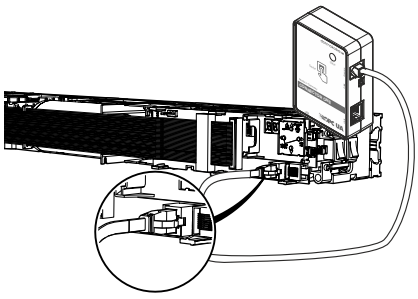
Conexión al ES PROLINE



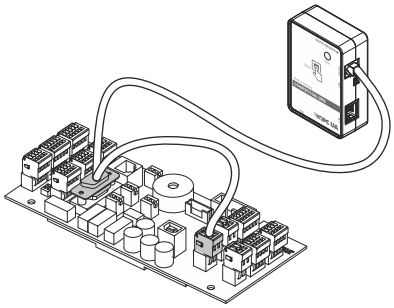
Conexión al ES 200



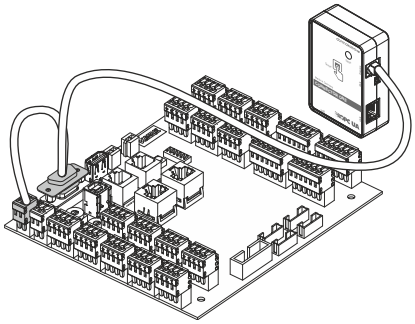
Conexión al ED 100, ED 250



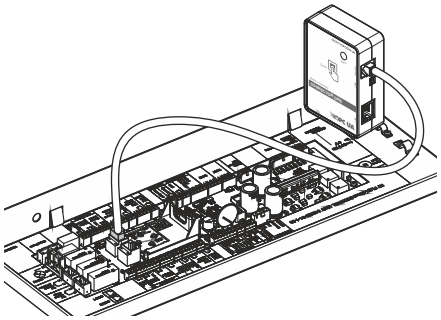
Conexión a la ETS22



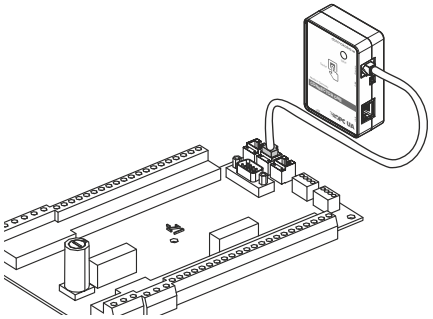
Conexión a la ETS22sc2



Conexión a una KTV

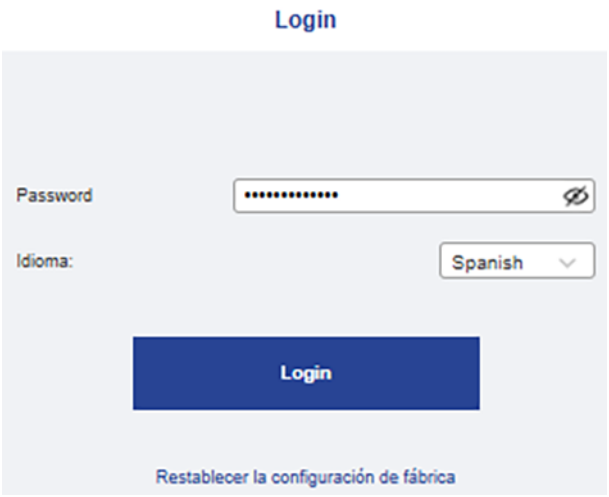


Conexión a un KTC 2 III



3.3 Puesta en servicio del Connector One G2 con un sistema de edificio inteligente

1. Conecte el Connector One G2 a un ordenador mediante un cable LAN o a un smartphone/tableta mediante un adaptador Ethernet para dispositivos inteligentes.
   - ⇨ El LED de estado parpadea en amarillo. El parpadeo señaliza el proceso de puesta en marcha.
   - ⇨ Una vez finalizado el proceso de puesta en marcha, el LED cambia de color y, dado el caso, de comportamiento de parpadeo.
2. Pulse el botón de servicio para iniciar el modo de servicio.
   - ⇨ Transcurridos unos segundos, el LED de estado empieza a parpadear en azul.
   - ⇨ Si el LED permanece iluminado en azul, el modo de servicio está activado.
   - ⇨ Si no tiene lugar un inicio de sesión en el Connector One G2, el modo de servicio finaliza automáticamente al cabo de 1 minuto.
   - ⇨ Si la configuración de red del PC está establecida en «Obtener automáticamente dirección IP» (predeterminado), el Connector One G2 asigna automáticamente una dirección IP al ordenador o dispositivo inteligente conectado. Si no se desea dicha asignación, debe configurarse previamente el ajuste de red adecuado en el ordenador o dispositivo inteligente.
3. Acceda a la dirección http://192.168.10.4 en el navegador. Es compatible con los navegadores habituales, como Chrome, Firefox, Opera y Safari.
4. Establezca una contraseña de 12 caracteres.
   - ⇨ Aparecerá el menú de inicio de sesión.



5. Introduzca la contraseña previamente establecida.
6. Seleccione el idioma de visualización.
7. Confirme haciendo clic en Iniciar sesión.
   - ⇨ Si no hay actividad durante más de 5 minutos, se cierra automáticamente la sesión del usuario y se reinicia el sistema.
8. Actualice la fecha, la hora y la zona horaria en el menú «Sistema».
9. Borre el certificado del servidor en el menú «OPC UA».

Si se pierde la contraseña, se puede restablecer la configuración de fábrica del Connector One G2 en el menú de inicio de sesión. En el proceso se borran todos los ajustes específicos del cliente. Tras el restablecimiento, el Connector One G2 se encuentra en el estado de entrega, si bien se conserva la última versión de firmware.

3.3.1 Configuración del Connector One G2

Durante la puesta en servicio con EntriWorX no está permitido modificar la configuración del Connector One 2.

3.3.1.1 Configuración de LAN

Realice los ajustes necesarios en «LAN» y aplíquelos mediante «Guardar».

3.3.1.2 Configuración de WLAN

Realice los ajustes necesarios en «WLAN» y aplíquelos mediante «Guardar».

Ajustes de wifi	
Utilizar wifi	Es necesario activar este parámetro cuando se utiliza wifi.
Utilizar red de respaldo	Posibilita el uso de una red de respaldo que se activa automáticamente cuando la red principal falla o no está disponible. Sirve como conexión alternativa para mantener la comunicación o la transmisión de datos.

No es posible configurar y guardar las redes al mismo tiempo. Después de configurar una red (red principal o alternativa) es necesario guardar los cambios. De lo contrario, los datos introducidos se perderán al cambiar de red.

Red	
Identificador	Permite asignar una denominación propia a la red WLAN.

Seguridad	
Tipo de seguridad	Aquí se puede elegir entre WPA2-Personal y WPA2-Enterprise. En el caso de WPA2-Personal se utiliza una contraseña WLAN común para todos los dispositivos de la red. En el caso de WPA2-Enterprise tiene lugar un inicio de sesión basado en el usuario a través de un servidor para autenticar individualmente a los usuarios o dispositivos.
Clave	Aquí se introduce la contraseña común que se utiliza en la red para conectarse a WLAN.
Protocolo de autenticación	EAP-TLS EAP-TLS ofrece la máxima seguridad, ya que tanto el cliente como el servidor utilizan certificados para la autenticación mutua. Este método es especialmente adecuado para entornos con una infraestructura de certificados existente. EAP-PEAP (con MSCHAPv2) EAP-PEAP establece primero un túnel TLS cifrado con el servidor. Dentro de este túnel tiene lugar el inicio de sesión mediante nombre de usuario y contraseña. Este método combina una buena seguridad con una gestión sencilla. EAP-MD5 EAP-MD5 es un sencillo procedimiento basado en contraseña que solo comprueba el nombre de usuario y una contraseña con hash. Es fácil de configurar, pero ofrece un nivel de seguridad bajo, por lo que solo se recomienda para aplicaciones no críticas.
Método de autenticación	MSCHAPv2 es un método de autenticación electrónica que se utiliza con frecuencia en redes WPA2 Enterprise en combinación con EAP-PEAP. El usuario inicia sesión con su nombre de usuario y contraseña personales. La comprobación real de la contraseña tiene lugar mediante un método de desafío-respuesta dentro de un túnel PEAP cifrado, lo que protege los datos de acceso.
Identidad	Aquí se introduce la identidad de un usuario, por ejemplo, su dirección de correo electrónico.
Identidad anónima	La identidad anónima es un nombre de usuario opcional que se envía al servidor al establecer el túnel PEAP. Sirve para proteger el identificador real del usuario. Si no se define ninguna identidad anónima, se utilizará automáticamente la identidad de usuario normal.
Contraseña	Aquí se introduce la contraseña del usuario correspondiente.
Certificado CA del servidor	Un certificado CA de servidor es un certificado emitido por un organismo de certificación de confianza que confirma la identidad del servidor. Es necesario para que los clientes puedan verificar de forma segura la conexión con el servidor y establecer una comunicación cifrada.

Certificado de servidor / «cargar certificado»	Transmisión manual de certificados de servidor.
Certificados de servidor / «borrar»	Los certificados existentes pueden borrarse manualmente.
«Guardar»	Esto aplica todos los ajustes de la configuración.

3.3.1.3 Configuración de OPC UA

En «OPC UA», configure los parámetros que controlan el acceso al servidor OPC UA.

- Puerto IP del servidor OPC UA
- Protocolo RS232 del control de puerta conectado (véase el anexo)
- Método de autenticación
- Cifrado de datos

Configuración del servidor	
Puerto del servidor	Aquí se establece el puerto TCP/IP a través del cual se accederá al Connector One G2. El puerto estándar para OPC UA es 4840.
Protocolo del controlador de la puerta	Dependiendo del control de la puerta, se debe elegir entre diferentes protocolos. Encontrará información sobre el protocolo en la documentación correspondiente.

Autenticación	
Contraseña de autenticación y usuario	El uso de un nombre de usuario y una contraseña es una característica de seguridad de OPC UA. El nombre de usuario y la contraseña son utilizados por el cliente OPC UA para iniciar sesión en Connector One G2 (servidor OPC UA). Los datos aquí introducidos deben utilizarse en el cliente OPC UA para acceder al Connector One G2.

Certificados de cliente de autenticación	Los certificados de cliente son una característica de seguridad de OPC UA. Un sistema se autentica en Connector One G2 mediante un certificado de cliente. Se pueden guardar varios certificados al mismo tiempo. Los certificados pueden transferirse previamente al Connector One G2. Es posible que el Connector One G2 acepte automáticamente el primer certificado que se le proporcione.
<borrar> certificados de cliente	Borra los certificados de cliente existentes.
<cargar> certificados de cliente	Transferencia manual de certificados de cliente.
Certificados de cliente / Modo de aprovisionamiento	Todavía no hay ningún certificado en la memoria. En cuanto un cliente se conecta con su certificado, este es aceptado por el Connector One G2. No se pueden aceptar automáticamente más certificados.

Normas de seguridad	
Directrices de seguridad disponibles	Una directriz de seguridad establece qué mecanismos deben utilizarse para el canal seguro entre el cliente y el servidor. La directriz de seguridad define los algoritmos de firma y cifrado, el algoritmo de derivación de claves y las longitudes de clave utilizadas en los algoritmos. Debe seleccionarse una de las siguientes reglas. Son posibles varias reglas al mismo tiempo. • None • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Encontrará más información sobre las reglas de seguridad en: https://profiles.opcfoundation.org/profilefolder/474
Modos de seguridad disponibles	El modo de seguridad establece los niveles generales de seguridad que el Connector One G2 ofrece a un cliente y que se pueden aplicar a los mensajes. Esto también depende de las capacidades del cliente. • None No se firma ni se cifra ningún mensaje. • Sign Se firman todos los mensajes, pero no se cifran. • Sign & encrypt Se firman y se cifran todos los mensajes.
Certificados de servidor	El Connector One G2 (servidor OPC UA) se autentica ante un cliente mediante un certificado de servidor. Puede generarse automáticamente el certificado o puede utilizarse un certificado existente. En el primer inicio se genera automáticamente un certificado de servidor OPC UA. Este certificado de servidor debería borrarse manualmente después de cambiar el nombre de host o la fecha, para que se genere un nuevo certificado en el siguiente inicio.
Certificados de servidor / «cargar certificado»	Transmisión manual de certificados de servidor.
Certificados de servidor / «cargar clave»	Transmisión manual de la clave correspondiente al certificado de servidor.
Certificados de servidor / «borrar»	Los certificados existentes pueden borrarse manualmente.
«Guardar»	Esto aplica todos los ajustes de la configuración.

3.3.1.4 Configuración del sistema

En «Sistema» se muestran información y ajustes que pueden modificarse.

Autenticación	
Modificación de la contraseña de inicio de sesión	Aquí puede modificarse la contraseña de inicio de sesión.
Modificación de la fecha y la hora	La indicación correcta de la hora es imprescindible para el uso del Connector One G2. Por lo tanto, se recomienda utilizar un servidor NTP. Si esto no es posible, también puede ajustarse manualmente la hora. • El reloj del Connector One G2 cuenta con respaldo de batería. Tras una interrupción del suministro eléctrico, no es necesario volver a ajustar la hora. • La fecha ajustada manualmente se guarda en un archivo del dispositivo y se recupera en el siguiente inicio. Si no se utiliza el dispositivo durante un largo periodo de tiempo después de ajustar la hora, es necesario actualizar la fecha o utilizar un servidor NTP.
Activación de NTP	Si NTP está activado, el Connector One G2 sincroniza su hora con un servidor NTP. Debe introducirse el servidor NTP en la configuración de red. Cuando esta función está activada, no es posible la configuración manual de la hora.
Ajuste manual de la hora	Haciendo clic en la indicación de la hora y la zona horaria, se puede introducir manualmente la hora actual.
Obtención de la hora del sistema anfitrión	Para facilitar la configuración manual de la hora, es posible cargar la hora actual y la zona horaria se pueden cargar desde el sistema anfitrión.
Modificación de la fecha y la hora	El Connector One G2 adopta la hora y la zona horaria mostradas.
Actualización del firmware	Esta función permite instalar un nuevo firmware. Se muestra la versión actual.
Añadir nuevo firmware mediante arrastrar y soltar o examinar	Esto transfiere un nuevo archivo de firmware al Connector One G2.
Instalación	Después de transferir un firmware, se puede proceder a la instalación.
Restablecimiento de los ajustes de fábrica	Permite restablecer un Connector One G2 a los ajustes de fábrica. Tras el restablecimiento, el dispositivo se encuentra en el estado de entrega, si bien se conserva la última versión de firmware.

3.4 Puesta en funcionamiento del Connector One G2 con EntriWorX

1. El LED de estado parpadea en amarillo. El parpadeo indica el proceso de puesta en funcionamiento.
   ⇨ Al finalizar el proceso de puesta en funcionamiento, el LED cambia de color y, dado el caso, de comportamiento de parpadeo, véase Códigos LED [▸ 2.4].

3.4.1 Requisitos

- Se ha creado un proyecto de cliente en EntriWorX Planner.
- Se ha asignado a un instalador un paquete de trabajo con la puerta que se debe instalar.
- Se ha aceptado la invitación por correo electrónico para el técnico.

3.4.2 Planificador EntriWorX

1. Incorpore una puerta en el plano de planta.
2. Seleccione y coloque una plantilla con el protocolo deseado (TMS, Datalink, Handheld o protocolo EL).
3. Asigne un conector One G2 a la puerta.
4. Establezca la configuración de red y de wifi.
5. Establezca la configuración de OPC UA.
6. Cree un nuevo paquete de trabajo (puesta en servicio) y agregue la puerta.
7. Asigne el paquete de trabajo al técnico.

⇨ Junto con la asignación del paquete de trabajo, el técnico recibe una invitación por correo electrónico.

⇨ El técnico debe aceptar la invitación para obtener los derechos para la puesta en servicio en la EntriWorX Setup App.

Notas sobre la configuración de red y de wifi

- Para utilizar WPA2-Enterprise para acceder a la red WiFi corporativa, primero debe configurarse la conexión en la interfaz de usuario web del Connector On G2 con el certificado y los datos de acceso. A continuación, se puede seleccionar la conexión en la aplicación de configuración.
- El módem LTE es detectado automáticamente por el Connector One G2 y se muestra en la aplicación de configuración.

3.4.3 EntriWorX Setup App

1. Inicie sesión en la aplicación con su correo electrónico y contraseña y seleccione el mercado.
2. Seleccione el edificio y la puerta.
   ⇨ El LED en el Connector cambia a azul e indica una conexión Bluetooth a la EntriWorX Setup App.
3. Comience la puesta en servicio con la configuración de red.
   ⇨ El módem LTE es detectado automáticamente por el Connector One G2 y se muestra en la aplicación de configuración EntriWorX Setup App.
4. Transfiera la configuración del EntriWorX Planner al Connector One G2.
   ⇨ La conexión Bluetooth se interrumpe y la puerta está en funcionamiento.
5. Transfiera la configuración de OPC UA.

Notas sobre la configuración de red y de wifi

- En EntriWorX Planner pueden predefinirse en el Planner el LAN y el wifi (WPA2-Personal) y adoptarse en la aplicación EntriWorX Setup App.
- En la aplicación EntriWorX Setup App se puede seleccionar el wifi corporativo predefinido mediante la opción «WiFi local Setup».
- El módem LTE es detectado automáticamente por el Connector One G2 y se muestra en la aplicación de configuración EntriWorX Setup App.

Configuración del servidor	
Puerto TCP	Especifica el puerto TCP/IP a través del cual se puede acceder al Connector One G2. El puerto estándar para OPC UA es 4840.

Directriz de seguridad	
Directrices de seguridad disponibles	Una directriz de seguridad establece qué mecanismos deben utilizarse para el canal seguro entre el cliente y el servidor. La directriz de seguridad define los algoritmos para la firma y el cifrado, el algoritmo para la derivación de claves y las longitudes de clave utilizadas en los algoritmos. Están disponibles las siguientes directrices (posibilidad de selección múltiple): • Ninguna • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Encontrará más información sobre las reglas de seguridad en: https://profiles.opcfoundation.org/profilefolder/474
Modo de seguridad	
Modos de seguridad disponibles	El modo de seguridad especifica qué niveles de seguridad generales se pueden aplicar a los mensajes. El Connector One G2 ofrece los siguientes modos de seguridad: (Posibilidad de selección múltiple): • Ninguno No se firma ni se cifra ningún mensaje. • Firmar Se firman todos los mensajes, pero no se cifran. • Firmar y cifrar Se firman y se cifran todos los mensajes. El modo de seguridad también depende de las capacidades del cliente OPC UA.

Autenticación	
Autenticación, contraseña y usuario	El uso de un nombre de usuario y una contraseña es una función de seguridad de OPC UA. El nombre de usuario y la contraseña se utilizan para permitir que el cliente OPC UA inicie sesión en Connector One G2 (servidor OPC UA). Los datos aquí introducidos deben utilizarse en el cliente OPC UA para acceder al Connector One G2.

1. Para completar el proceso, haga clic en «Guardar».

3.5 Conexión y configuración del cliente OPC UA

Requisitos

- El Connector One G2 está listo para funcionar.

  => El LED de estado está encendido o parpadea en verde.
- El Connector One G2 está correctamente conectado a la red.

Establecimiento de la conexión

1. Introduzca la siguiente URL de punto final en el navegador.
   opc.tcp://[Dirección IP del Connector One G2]:[Puerto del servidor]
   Ejemplo: opc.tcp://192.168.1.20:4840

Configuración del cliente OPC UA

1. Configure las reglas de seguridad que se correspondan con las reglas en el Connector One G2.
2. Seleccione el método de autenticación que se corresponda con la configuración del Connector One G2.

Si se van a utilizar certificados, es posible que haya que sustituirlos previamente.

3. Establezca la conexión.

4 Montaje

AVISO

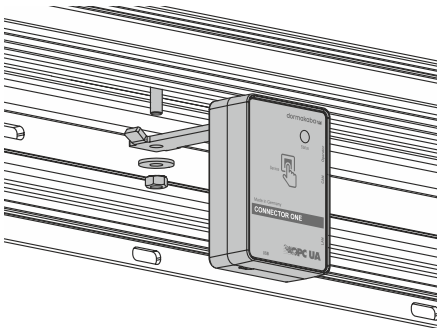
Daños materiales por colisión

La colisión con piezas móviles puede dañar el Connector One G2 y/o los cables.

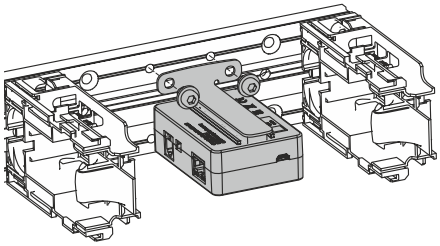
- Monte el Connector One G2 de forma que no pueda colisionar con piezas móviles.
- Tienda/almacene todos los cables en el interior del accionamiento en los conductos de cables existentes o fíjelos mediante un soporte para cables.

Una vez finalizada la configuración completa, se monta el Connector One G2 en el accionamiento de la puerta.
En función del accionamiento de la puerta, están disponibles diferentes materiales para el montaje.

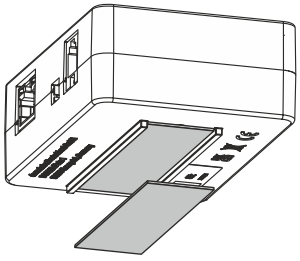
Montaje en el ES PROLINE
En el ES PROLINE, el Connector One G2 se monta en el accionamiento con la escuadra de montaje suministrada.



Montaje en el ED 100, ED 250
En los modelos ED 100, ED 250, el Connector One G2 se monta en el accionamiento mediante la escuadra de montaje suministrada y el kit de instalación ED.



Montaje en otros accionamientos
Para el montaje sin escuadra de montaje, el Connector One G2 se fija en un lugar adecuado mediante la cinta de velcro.



5 Resolución de problemas

Error	Solución
El certificado del servidor OPC UA ha caducado.	Modo de servicio: En el menú <Sistema>, compruebe la fecha/hora y corríjala si es necesario. A continuación, elimine el certificado del servidor en el <menú> OPC UA. A continuación, reinicie el Connector One G2. Tras el reinicio, se genera automáticamente un nuevo certificado. Este certificado es válido durante 4 años a partir de la fecha de generación.
No se puede acceder al sitio web del servicio.	Compruebe que ha introducido correctamente la URL en el navegador. http://192.168.10.4 Si es necesario, borre la caché del navegador y vuelva a cargar la página.
Se muestra el error «BadUserIdentity» en el cliente OPC UA.	Compruebe la autenticación en el modo de servicio y ajústela si es necesario.
En dispositivos TMS, no puede modificarse el conmutador de programa a través de OPC UA.	En caso necesario, utilice las instrucciones del accionamiento para asegurarse de que está permitido modificar el conmutador de programa desde el exterior (configuración del accionamiento). Para los controles de las vías de evacuación, puede ser necesario un firmware de accionamiento especial (p. ej., ES 200 2D o FFT), ya que está prohibido por ley manipular a distancia el conmutador de programa. A este respecto, póngase en contacto con el Servicio de dormakaba.
No se establece ninguna conexión en el dispositivo TMS.	Asegúrese de que la interfaz RS 232 esté configurada en el modo TMS (véanse las instrucciones del accionamiento correspondiente).
En caso de accionamiento con el protocolo de terminal de mano, no se establece ninguna conexión.	Asegúrese de que la interfaz RS 232 esté configurada en el modo de terminal de mano Handheld (véanse las instrucciones del accionamiento correspondiente).
Después de una actualización de firmware, ya no se puede utilizar el Connector One G2.	Restablezca el Connector One G2 a la configuración de fábrica, véase Puesta en servicio del Connector One G2 con un sistema de edificio inteligente [▸ 3.3].

6 Desmontaje y eliminación

El desmontaje se realiza en el orden inverso al montaje y únicamente por personal capacitado.

El producto no debe desecharse junto con los residuos domésticos. Deshágase del producto de forma respetuosa con el medio ambiente en los puntos de aceptación y recogida establecidos para este fin. Deben respetarse las directrices legales nacionales aplicables.

Notas

www.dormakaba.com

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Alemania
+49 2333 793-0

www.dormakaba.com