dormakaba

Connector One G2

Betriebsanleitung

060868 45532/TECHDOC-716 - 02/2026

DE

Inhaltsverzeichnis

1 Informationen zu diesem Dokument

1.1 Inhalt und Zweck

Die vorliegende Anleitung beschreibt die Verwendung des Connector One G2.

1.2 Zielgruppe

Dieses Dokument richtet sich an technisch qualifiziertes Fachkräfte.
Eine technisch qualifizierte Fachkraft besitzt eine geeignete technische Ausbildung und Erfahrung im Umgang mit der Technik. Es liegt in der Verantwortung der Fachkraft, dass die vom Hersteller genannten Bedingungen sowie geltende Vorschriften und Normen bei der Handhabung des beschriebenen Produkts eingehalten werden.

1.3 Dokumentenaufbewahrung

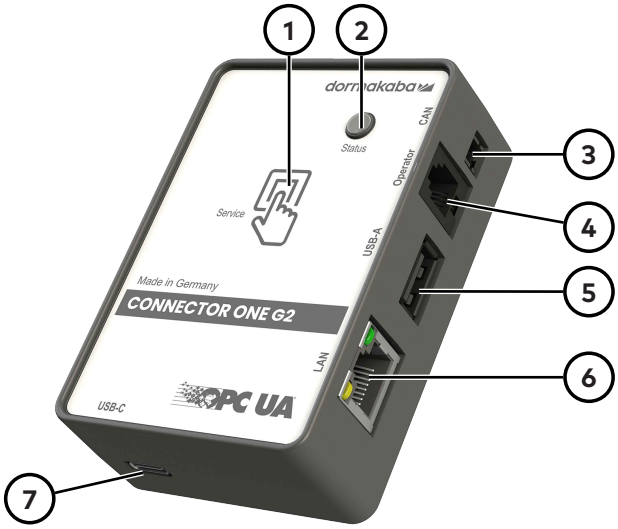
Dieses Dokument und die mitgeltenden Dokumente müssen an den Betreiber übergeben werden. Die Dokumente müssen während der Lebensdauer des Produkts aufbewahrt und dem Personal zugänglich gemacht werden.

1.4 Bestimmungsgemäße Verwendung

- Erweiterung von dormakaba Türsystemen um eine Ethernet-Schnittstelle.
- Einsatz im Innenbereich von Gebäuden

2 Produktbeschreibung

Mit einem Connector One G2 lassen sich automatische Türen und Türsysteme von dormakaba um eine Netzwerk-Schnittstelle erweitern. Dadurch wird ein Fernzugriff über das lokale Netzwerk ermöglicht. Der plattformunabhängige Datenaustausch erfolgt sicher über den OPC UA-Standard. Smart-Building-Systeme, die OPC UA unterstützen, erhalten mit dem Connector One G2 umfangreichen Zugriff auf Informationen und Steuerungsmöglichkeiten. Des Weiteren unterstützt der Connector One G2 das EntriWorX Ecosystem. Verbundene Geräte können mit EntriWorX Insights überwacht, gesteuert und verwaltet werden.



1 Service-Taste zur Konfiguration des Connector One G2

2 Status-LED

3 CAN BUS-Anschluss*

4 RS 232-Schnittstelle zur Verbindung mit der Antriebssteuerung

5 USB-A-Schnittstelle
ACHTUNG Die USB-A Schnittstelle darf nur für freigegebene Geräte*** genutzt werden. Es dürfen keine anderen Geräte eingesteckt werden, da dies zu Störungen oder im Extremfall zu Beschädigungen führen kann.

6 LAN-Schnittstelle zur Verbindung mit dem Kundennetzwerk oder Computer

7 USB-C-Schnittstelle zur Stromversorgung

2.1 Technische Daten

Spannung**	24 V DC ± 20 % / 5 V DC
Betriebstemperatur	-15 °C bis + 55 °C
Rel. Luftfeuchtigkeit	5 % bis 95 %
Schnittstellen	RS232, LAN, USB-A, USB-C, CAN*
Funk	Bluetooth LE

* Vorgesehen für zukünftige Anwendungen

** Die Stromversorgung erfolgt direkt über den Türantrieb oder über die USB-C-Schnittstelle und ein USB-Netzteil.

*** Die Liste mit den freigegebenen Geräten kann hier heruntergeladen werden: https://www.dormakaba.com/connector-one

2.2 Lithium-Batterie

Das Gerät enthält 1 Lithium-Batterie des Typs CR1220 als Stützbatterie.

Die Batterie benötigt keine Service- oder Wartungsarbeiten. Die Haltbarkeit der Batterie ist bis zum Ende des Lebenszyklus ausgelegt.

Die Sicherheitsvorschriften für den Transport von Geräten mit Lithium-Batterie einhalten.

2.3 Konformität

2.3.1 EU-Konformitätserklärung

Dieses Kapitel ist ein Auszug aus der vollständigen Konformitätserklärung.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Deutschland

erklärt hiermit, dass das beschriebene Produkt in Übereinstimmung mit den Bestimmungen der aufgeführten Richtlinie(n) ist und dass die Normen und/oder technischen Spezifikationen zur Anwendung gelangt sind, auf die im Folgenden Bezug genommen werden.

Richtlinien:

2014/53/EU	Funkanlagen
2011/65/EU	RoHS

Die technischen Unterlagen sind erhältlich beim Manager Productcompliance unter: product-compliance.dach@dormakaba.com

Harmonisierte europäische Norm, nationale Regel:

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 UKCA-Konformitätserklärung

Dieses Kapitel ist nur ein Auszug aus der vollständigen Konformitätserklärung.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Germany

erklärt hiermit, dass das beschriebene Produkt in Übereinstimmung mit den Bestimmungen der aufgeführten Richtlinie(n) ist und dass die Normen und/oder technischen Spezifikationen zur Anwendung gelangt sind, die im Folgenden in Bezug genommen werden.

Richtlinien:

Radio Equipment Regulations 2017

RoHS, The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Regulation 2012

Die technischen Unterlagen sind erhältlich beim Manager Productcompliance unter: product-compliance.dach@dormakaba.com

Harmonisierte europäische Norm, nationale Regel:

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 & IC

FCC Das Produkt erfüllt die Anforderungen von:

- **FCC Title 47 CFR Part 15**
  FCC ID: 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 Das Produkt erfüllt die Anforderungen von:

- **ISED Canada RSS-247 and ISED Canada RSS-Gen**
  IC: 11038A-CON1G2

2.4 LED-Codes

Status	Farbe	Modus
Systemstart	gelb	langsames Blinken
Konfiguration erforderlich	gelb	dauerhaft an
Betriebsbereit, eine Türsteuerung wurde erkannt	grün	dauerhaft an
Betriebsbereit, eine Türsteuerung wurde nicht erkannt	grün	langsames Blinken
Fehler	rot	dauerhaft an
Service-Modus oder Bluetooth-Verbindung aktiv	blau	dauerhaft an
Service-Modus aktiviert oder Geräteidentifikation aktiv	blau	langsames Blinken
Datenübertragung/Softwareupdate	cyan	schnelles Blinken

2.5 Unterstützte Türantriebe und Türsysteme

Produkte mit TMS-Protokoll

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

Produkte mit Datalink-Protokoll ab ETS22

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

Produkte mit Handheld-Protokoll von ESA2-Controller

ESA 100
ESA 200
ESA 300
ESA 400
ESA 500

Produkte mit EL-Protokoll

EL 301	AL 501
AL 401	AL 1001

Bei diesen Türantrieben wird ein RS485/RS232 Konverter (Artikel-Nr. 29262009) benötigt, um die Verbindung zum Connector One G2 zu ermöglichen.

2.6 OPC UA-Datenpunkte & Software Updates

Da das Informationsmodell und die Connector One G2 Software ständig weiterentwickelt wird und ggf. weitere Geräte und Funktionalitäten hinzugefügt werden, können die Software Updates und OPC UA-Datenpunkttabellen zu den spezifischen Antrieben online im my.dormakaba Portal eingesehen werden.
Dazu ist eine einmalige kostenlose Registrierung erforderlich unter:
https://portal.dormakaba.com/registration
Nach der Anmeldung sind die Daten des Connector One G2 einsehbar unter:
https://dormakaba.com/connector-one

3 Inbetriebnahme

3.1 Voraussetzungen für die Inbetriebnahme

TMS-Geräte
Die RS232-Schnittstelle der Antriebssteuerung ist als TMS-Modus konfiguriert.

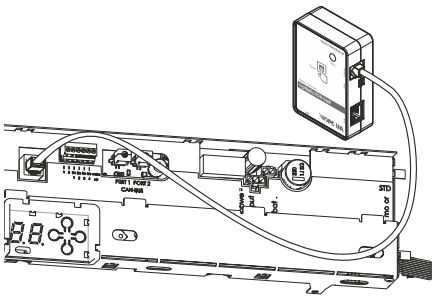
ETS22
Eine RS232-Schnittstelle ist verfügbar.

EL-Antriebe
Ein RS485/RS232-Konverter ist vorhanden.

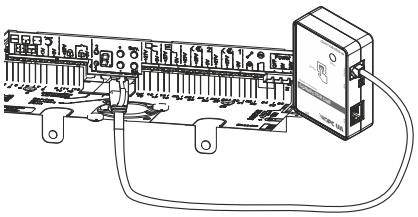
3.2 Den Connector One G2 anschließen

Den Connector One G2 über die RS 232-Schnittstelle an die Steuerung anschließen.

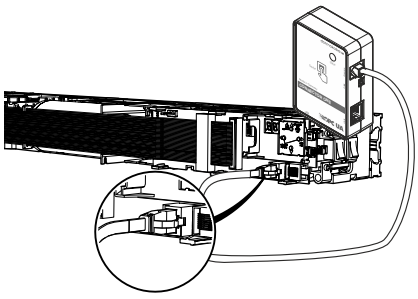
Anschluss an den ES PROLINE



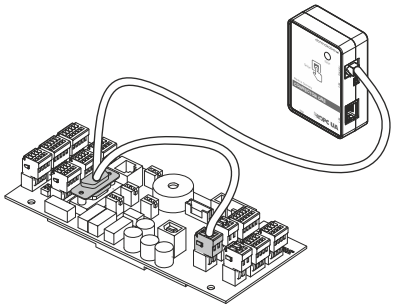
Anschluss an den ES 200



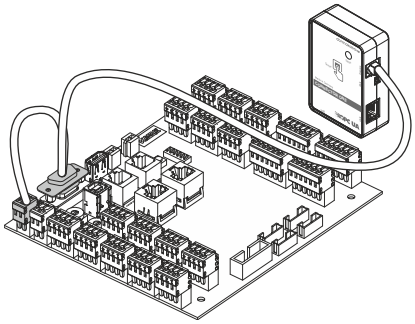
Anschluss an den ED 100, ED 250



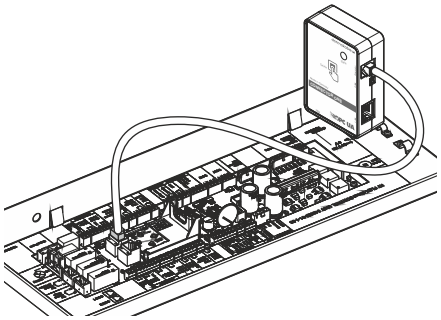
Anschluss an die ETS22



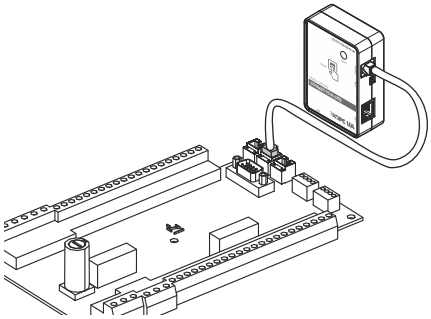
Anschluss an die ETS22sc2



Anschluss an eine KTV



Anschluss an eine KTC 2 III



3.3 Den Connector One G2 mit einem Smart-Building-System in Betrieb nehmen

1. Den Connector One G2 mit einem LAN-Kabel an einen Computer oder mit einem Ethernet-Adapter für Smart-Devices an ein Smartphone/Tablet anschließen.
   - ⇨ Die Status-LED blinkt gelb. Das Blinken signalisiert den Startvorgang.
   - ⇨ Nach Abschluss des Startvorgangs wechselt die LED ihre Farbe und ggf. das Blinkverhalten.
2. Die Service-Taste drücken, um den Service-Modus zu starten.
   - ⇨ Nach wenigen Sekunden beginnt die Status-LED blau zu blinken.
   - ⇨ Leuchtet die LED dauerhaft blau, ist der Service-Modus aktiviert.
   - ⇨ Wenn keine Anmeldung am Connector One G2 erfolgt, wird der Service-Modus nach 1 Minute automatisch beendet.
   - ⇨ Wenn die Netzwerkeinstellung am PC auf "IP-Adresse automatisch beziehen" eingestellt ist (Standard), weist der Connector One G2 dem angeschlossenen Computer oder Smart-Device automatisch eine IP-Adresse zu. Ist das nicht gewünscht, muss die passende Netzwerkeinstellung am Computer oder Smart-Device vorab konfiguriert werden.
3. Die Adresse http://192.168.10.4 im Browser aufrufen. Unterstützt werden die üblichen Webbrowser wie Chrome, Firefox, Opera und Safari.
4. Ein 12-stelliges Passwort einrichten.
   - ⇨ Das Anmeldemenü erscheint.

5. Das zuvor festgelegte Passwort eingeben.
6. Die Anzeigensprache auswählen.
7. Mit einem Klick auf Anmelden bestätigen.
   - ⇨ Bei einer Inaktivität von mehr als 5 Minuten wird der Benutzer automatisch abgemeldet und das System neu gestartet.
8. Im Menü "System" Datum, Uhrzeit und Zeitzone aktualisieren.
9. Im Menü "OPC UA" das Server-Zertifikat löschen.

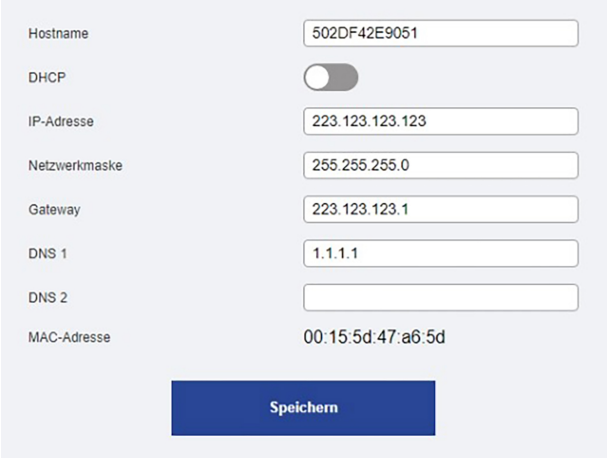
Sollte das Passwort verloren gehen, kann der Connector One G2 im Anmeldemenü auf Werkseinstellungen zurückgesetzt werden. Dabei werden alle kundenspezifischen Einstellungen gelöscht. Der Connector One G2 befindet sich danach im Auslieferungszustand, wobei der letzte Firmware-Stand erhalten bleibt.

3.3.1 Den Connector One G2 konfigurieren

Bei einer Inbetriebnahme mit EntriWorX darf die Konfiguration des Connectors One G2 nicht geändert werden.

3.3.1.1 LAN konfigurieren

Unter "LAN" die erforderlichen Einstellungen vornehmen und mit "Speichern" übernehmen.



3.3.1.2 WLAN konfigurieren

Unter "WLAN" die erforderlichen Einstellungen vornehmen und mit "Speichern" übernehmen.

WiFi-Einstellungen	
WiFi verwenden	Dieser Parameter muss aktiviert werden, wenn WiFi verwendet wird.
Fallback-Netzwerk verwenden	Ermöglicht die Verwendung eines Fallback-Netzwerks, das automatisch einspringt, wenn das Hauptnetzwerk ausfällt oder nicht verfügbar ist. Es dient als Ausweichverbindung, um die Kommunikation oder Datenübertragung aufrechtzuerhalten.

Eine gleichzeitige Konfiguration und Speicherung der Netzwerke ist nicht möglich. Nach der Konfiguration eines Netzwerks (Haupt- oder Fallback-Netzwerk) muss gespeichert werden. Andernfalls gehen die Eingaben beim Wechseln des Netzwerkes verloren.

Netzwerk	
Kennung	Hiermit kann eine eigene Bezeichnung für das WLAN-Netzwerk vergeben werden.

Sicherheit	
Sicherheitstyp	Hier kann zwischen WPA2-Personal und WPA2-Enterprise gewählt werden. Bei WPA2-Personal wird ein gemeinsames WLAN-Passwort für alle Geräte im Netzwerk genutzt. Bei WPA2-Enterprise erfolgt eine benutzerbasierte Anmeldung über einen Server, um Benutzer oder Geräte individuell zu authentifizieren.
Schlüssel	Hier wird das gemeinsame Passwort eingetragen, das im Netzwerk verwendet wird, um sich mit dem WLAN zu verbinden.
Authentifizierungsprotokoll	EAP-TLS EAP-TLS bietet die höchste Sicherheit, da sowohl Client als auch Server Zertifikate für die gegenseitige Authentifizierung verwenden. Diese Methode eignet sich besonders für Umgebungen mit einer bestehenden Zertifikatsinfrastruktur. EAP-PEAP (mit MSCHAPv2) EAP-PEAP baut zunächst einen verschlüsselten TLS-Tunnel zum Server auf. Innerhalb dieses Tunnels erfolgt die Anmeldung per Benutzername und Passwort. Diese Methode kombiniert gute Sicherheit mit einfacher Verwaltung. EAP-MD5 EAP-MD5 ist ein einfaches passwortbasiertes Verfahren, das nur den Benutzernamen und ein gehashtes Passwort prüft. Es ist leicht einzurichten, bietet jedoch nur ein geringes Sicherheitsniveau und wird daher nur für unkritische Anwendungen empfohlen.
Authentifizierungsmethode	MSCHAPv2 ist ein eAuthentifizierungsmethode, die in WPA2-Enterprise-Netzwerken häufig in Kombination mit EAP-PEAP verwendet wird. Der Benutzer meldet sich mit seinem persönlichen Benutzernamen und Passwort an. Die eigentliche Passwortprüfung erfolgt über eine Challenge-Response-Methode innerhalb eines verschlüsselten PEAP-Tunnels, wodurch die Zugangsdaten geschützt werden.
Identität	Hier wird die Identität eines User eingetragen, z.B. E-Mail.
Anonyme Identität	Die anonyme Identität ist ein optionaler Benutzername, der beim Aufbau des PEAP-Tunnels an den Server gesendet wird. Sie dient dem Schutz der eigentlichen Benutzerkennung. Falls keine anonyme Identität definiert wird, wird automatisch die normale Benutzeridentität verwendet.
Passwort	Hier wird das Passwort des entsprechenden Users eingetragen.
Server CA-Zertifikat	Ein Server-CA-Zertifikat ist ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat, das die Identität des Servers bestätigt. Es wird benötigt, damit Clients die Verbindung zum Server sicher prüfen und eine verschlüsselte Kommunikation aufbauen können.

Server-Zertifikat / "Zertifikat hochladen"	Manuelle Übertragung von Server-Zertifikaten.
Server-Zertifikate / "löschen"	Vorhandene Zertifikate können manuell gelöscht werden.
"Speichern"	Hiermit werden alle Einstellungen übernommen.

3.3.1.3 OPC UA konfigurieren

Unter "OPC UA" die Parameter einstellen, die den Zugriff auf den OPC UA-Server regeln.

- IP-Port des OPC UA-Servers
- RS232-Protokoll der angeschlossenen Türsteuerung (siehe Anhang)
- Authentifizierungsmethode
- Datenverschlüsselung

Server-Einstellungen	
Server-Port	Hier wird der TCP/IP-Port festgelegt, über den der Connector One G2 erreichbar sein soll. Der Standard-Port für OPC UA ist 4840.
Türtreiberprotokoll	Je nach Türsteuerung muss zwischen verschiedenen Protokollen gewählt werden. Angaben zum Protokoll sind in der entsprechenden Dokumentation zu finden.

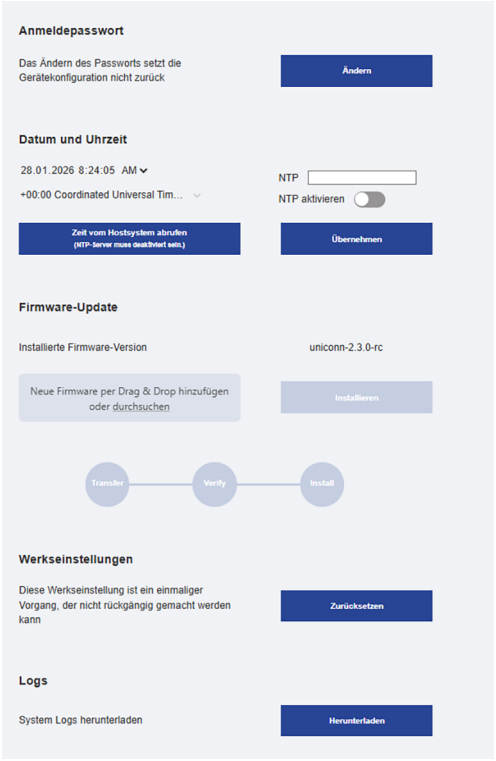
Authentifizierung	
Authentifizierungs-passwort und Benutzer	Die Verwendung eines Benutzernamens und eines Passworts ist ein OPC UA-Sicherheitsmerkmal. Der Benutzername und das Passwort dienen dem OPC UA-Client zur Anmeldung am Connector One G2 (OPC UA-Server). Die hier eingegebenen Daten müssen im OPC UA-Client verwendet werden, um Zugriff auf den Connector One G2 zu erhalten.

Authentifizierungs-Client-Zertifikate	Die Client-Zertifikate sind ein OPC UA-Sicherheitsmerkmal. Mit einem Client Zertifikat authentifiziert sich ein System beim Connector One G2. Es können mehrere Zertifikate gleichzeitig hinterlegt werden. Zertifikate können dem Connector One G2 vorab übertragen werden. Es ist möglich, dass der Connector One G2 das erste ihm bereitgestellte Zertifikat automatisch akzeptiert.
Client-Zertifikate <löschen>	Löscht vorhandene Client-Zertifikate.
Client-Zertifikate <hochladen>	Manuelle Übertragung von Client-Zertifikaten.
Client-Zertifikate / Provisioning-Mode	Es ist noch kein Zertifikat im Speicher. Sobald sich ein Client mit seinem Zertifikat anmeldet, wird dieses vom Connector One G2 akzeptiert. Weitere Zertifikate können nicht automatisch akzeptiert werden.

Sicherheitsregeln	
Verfügbare Sicherheitsrichtlinien	Eine Sicherheitsrichtlinie legt fest, welche Mechanismen für den sicheren Kanal zwischen dem Client und dem Server verwendet werden sollen. Die Sicherheitsrichtlinie definiert die Algorithmen zum Signieren und Verschlüsseln, den Algorithmus zur Schlüsselableitung und die in den Algorithmen verwendeten Schlüssellängen. Eine der folgenden Regeln muss ausgewählt werden. Mehrere Regeln gleichzeitig sind möglich. • None • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Weitere Informationen zu den Sicherheitsregeln sind verfügbar unter: https://profiles.opcfoundation.org/profilefolder/474
Verfügbare Sicherheitsmodi	Der Sicherheitsmodus legt fest, welche generelle Sicherheitsstufen der Connector One G2 einem Client anbietet, die auf Nachrichten angewendet werden können. Dies ist auch abhängig von den Fähigkeiten des Clients. • None Alle Nachrichten werden weder signiert noch verschlüsselt. • Sign Alle Nachrichten werden signiert, aber nicht verschlüsselt. • Sign & encrypt Alle Nachrichten werden signiert und verschlüsselt.
Server-Zertifikate	Mit einem Server-Zertifikat authentifiziert sich der Connector One G2 (OPC UA-Server) gegenüber einem Client. Es kann automatisch erzeugt oder ein bereits vorhandenes Zertifikat verwendet werden. Beim ersten Start wird automatisch ein OPC UA-Server-Zertifikat erzeugt. Dieses Server-Zertifikat sollte nach Änderung des Hostnamens oder des Datums manuell gelöscht werden, damit beim nächsten Start ein neues Zertifikat erzeugt wird.
Server-Zertifikate / "Zertifikat hochladen"	Manuelle Übertragung von Server-Zertifikaten.
Server-Zertifikate / "Schlüssel hochladen"	Manuelle Übertragung des Schlüssels passend zum Server-Zertifikat.
Server-Zertifikate / "löschen"	Vorhandene Zertifikate können manuell gelöscht werden.
"Speichern"	Hiermit werden alle Einstellungen übernommen.

3.3.1.4 System konfigurieren

Unter "System" werden Informationen und Einstellungen angezeigt und können geändert werden.



Authentifizierung	
Login-Passwort ändern	Hier kann das Login-Passwort geändert werden.
Datum und Uhrzeit ändern	Eine korrekte Zeitangabe ist für die Nutzung des Connector One G2 unerlässlich. Es empfiehlt sich daher die Verwendung eines NTP-Servers. Ist das nicht möglich, kann die Zeit auch manuell eingestellt werden. • Die Uhr des Connector One G2 ist batteriegepuffert. Nach einer Unterbrechung der Stromversorgung muss die Zeit nicht neu eingestellt werden. • Das manuell eingestellte Datum wird in einer Datei auf dem Gerät gespeichert und beim nächsten Start abgerufen. Sollte das Gerät nach Einstellung der Uhrzeit längere Zeit nicht in Benutzung sein, muss das Datum aktualisiert oder ein NTP-Server verwendet werden.
NTP aktivieren	Wird NTP aktiviert, synchronisiert der Connector One G2 seine Zeit mit einem NTP-Server. Der NTP-Server ist in der Netzwerk-Einstellung einzugeben. Bei aktivierter Funktion ist eine manuelle Zeitkonfiguration nicht möglich.
Manuelle Einstellung der Uhrzeit	Durch Klicken auf die Zeitangabe und Zeitzone kann die aktuelle Uhrzeit manuell eingegeben werden.
Uhrzeit vom Host-System holen	Zur Erleichterung der manuellen Zeitkonfiguration können die aktuelle Zeit und Zeitzone vom Host-System geladen werden.
Datum und Uhrzeit ändern	Die angezeigte Zeit und Zeitzone wird vom Connector One G2 übernommen.
Firmware aktualisieren	Über diese Funktion lässt sich eine neue Firmware installieren. Die aktuelle Version wird angezeigt.
Neue Firmware per Drag & Drop hinzufügen oder durchsuchen	Hierüber wird eine neue Firmware-Datei an den Connector One G2 übertragen.
Installieren	Nach der Übertragung einer Firmware kann die Installation ausgeführt werden.
Zurücksetzen auf Werkseinstellungen	Hierüber kann ein Connector One G2 auf Werkseinstellungen zurückgesetzt werden. Das Gerät befindet sich danach im Auslieferungszustand, wobei der letzte Firmware-Stand erhalten bleibt.

3.4 Den Connector One G2 mit EntriWorX in Betrieb nehmen

1. Die Status-LED blinkt gelb. Das Blinken zeigt den Startvorgang an.
   ⇨ Am Ende des Startvorgangs ändert die LED ihre Farbe und ggf. das Blinkverhalten, siehe LED-Codes [▸ 2.4].

3.4.1 Voraussetzungen

- Ein Kundenprojekt wurde im EntriWorX Planner angelegt.
- Ein Arbeitspaket mit der zu installierenden Tür wurde einem Installateur zugewiesen.
- Die E-Mail-Einladung für den Techniker wurde angenommen.

3.4.2 EntriWorX Planner

1. Eine Tür auf dem Grundriss platzieren.
2. Eine Vorlage mit dem gewünschten Protokoll (TMS, Datalink, Handheld oder EL-Protokoll) auswählen und platzieren.
3. Der Tür einen Connector One G2 zuweisen.
4. Die Einstellungen für Netzwerk und WiFi setzen.
5. Die OPC UA Einstellungen setzen.
6. Ein neues Arbeitspaket (Commissioning) anlegen und die Tür hinzufügen.
7. Das Arbeitspaket dem Techniker zuweisen.

⇨ Mit der Zuweisung des Arbeitspakets, bekommt der Techniker eine E-Mail-Einladung.

⇨ Die Einladung muss der Techniker annehmen, damit er die Rechte in der EntriWorX Setup App zur Inbetriebnahme erhält.

Hinweise zu Netzwerk- und WiFi-Einstellungen

- Um WPA2-Enterprise für den Zugriff auf das Corporate-WiFi zu nutzen, muss die Verbindung zuerst im Web-UI des Connector On G2 mit Zertifikat und Zugangsdaten eingerichtet werden. Anschließend kann die Verbindung in der Setup-App ausgewählt werden.
- Das LTE-Modem wird vom Connector One G2 automatisch erkannt und in der Setup-App angezeigt.

3.4.3 EntriWorX Setup App

1. In der App mit E-Mail und Passwort anmelden und den Markt auswählen.
2. Das Gebäude und die Tür auswählen.
   ⇨ Die LED am Connector wechselt auf blau und zeigt eine Bluetooth Verbindung zur EntriWorX Setup App an.
3. Die Inbetriebnahme mit Netzwerkeinstellungen starten.
   ⇨ Das LTE-Modem wird vom Connector One G2 automatisch erkannt und in der EntriWorX Setup App angezeigt.
4. Die Konfiguration vom EntriWorX Planner auf den Connector One G2 übertragen.
   ⇨ Die Bluetooth-Verbindung wird unterbrochen und die Tür ist in Betrieb.
5. Die OPC UA Einstellungen übertragen.

Hinweise zu Netzwerk- und WiFi-Einstellungen

- Im EntriWorX Planner können LAN und WiFi (WPA2-Personal) kann im Planner vordefiniert und in der EntriWorx Setup App übernommen werden.
- In EntriWorx Setup-App kann das vordefinierte Corporate WiFi über die Option „WiFi local Setup“ ausgewählt werden.
- Das LTE-Modem wird vom Connector One G2 automatisch erkannt und in der EntriWorx Setup-App angezeigt.

Servereinstellungen	
TCP-Port	Gibt den TCP/IP-Port an, über den auf Connector One G2 zugegriffen werden kann. Der Standardport für OPC UA ist 4840.

Sicherheitsrichtlinie	
Verfügbare Sicherheitsrichtlinien	Eine Sicherheitsrichtlinie legt fest, welche Mechanismen für den sicheren Kanal zwischen Client und Server verwendet werden sollen. Die Sicherheitsrichtlinie definiert die Algorithmen für die Signatur und Verschlüsselung, den Algorithmus für die Schlüsselableitung und die in den Algorithmen verwendeten Schlüssellängen. Folgende Richtlinien stehen zur Verfügung (Mehrfachauswahl möglich): • Keine • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Weitere Informationen zu den Sicherheitsregeln siehe unter: https://profiles.opcfoundation.org/profilefolder/474
Sicherheitsmodus	
Verfügbare Sicherheitsmodi	Der Sicherheitsmodus gibt an, welche allgemeinen Sicherheitsstufen auf Nachrichten angewendet werden können. Der Connector One G2 bietet folgende Sicherheitsmodi an: (Mehrfachauswahl möglich): • Keine Alle Nachrichten werden nicht signiert oder verschlüsselt. • Signieren Alle Nachrichten werden signiert, aber nicht verschlüsselt. • Signieren und verschlüsseln Alle Nachrichten werden signiert und verschlüsselt. Der Sicherheitsmodus hängt auch von den Fähigkeiten des OPC UA Clients ab.

Authentifizierung	
Authentifizierung, Passwort und Benutzer	Die Verwendung eines Benutzernamens und eines Passworts ist eine OPC UA-Sicherheitsfunktion. Der Benutzername und das Passwort werden verwendet, damit sich der OPC UA-Client bei Connector One G2 (OPC UA-Server) anmelden kann. Die hier eingegebenen Daten müssen im OPC UA-Client verwendet werden, um Zugriff auf den Connector One G2 zu erhalten.

1. Um den Prozess abzuschließen, auf "Speichern" klicken.

3.5 OPC UA Client verbinden und konfigurieren

Voraussetzungen

- Der Connector One G2 ist betriebsbereit.

  => Die Status-LED leuchtet oder blinkt grün.
- Der Connector One G2 ist korrekt mit dem Netzwerk verbunden.

Verbindung herstellen

1. Die folgende Endpoint-URL in den Browser eingeben.
   opc.tcp://[IP-Adresse Connector One G2]:[Server-Port]
   Beispiel: opc.tcp://192.168.1.20:4840

OPC UA-Client konfigurieren

1. Die Sicherheitsregeln passend zu den Regeln im Connector One G2 einstellen.
2. Die Authentifizierungsmethode passend zur Einstellung im Connector One G2 wählen.

Sollen Zertifikate zum Einsatz kommen, müssen diese ggf. vorab ausgetauscht werden.

3. Die Verbindung herstellen.

4 Montage

ACHTUNG

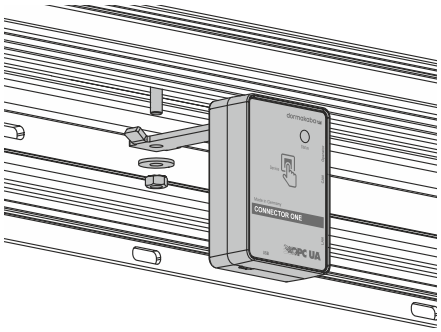
Sachschäden durch Kollision

Durch Kollision mit beweglichen Teilen können der Connector One G2 und/oder die Leitungen beschädigt werden.

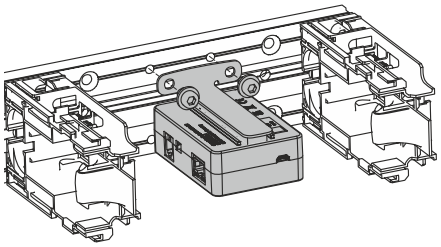
- Den Connector One G2 so montieren, dass er nicht mit beweglichen Teilen kollidieren kann.
- Alle Leitungen innerhalb des Antriebs in vorhandenen Kabelkanälen führen/verstauen oder mit einem Kabelhalter befestigen.

Nach Abschluss der vollständigen Konfiguration wird der Connector One G2 im Türantrieb montiert.
Je nach Türantrieb stehen unterschiedliche Montagematerialen zur Verfügung.

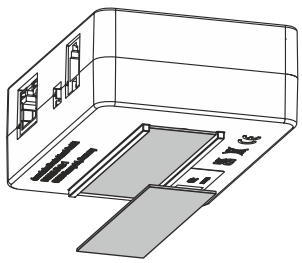
Im ES PROLINE montieren
Im ES PROLINE wird der Connector One G2 mit dem beiliegenden Montagewinkel Im Antrieb montiert.



Im ED 100, ED 250 montieren
Im ED 100, ED 250 wird der Connector One G2 mit dem beiliegenden Montagewinkel und dem ED-Einbausatz im Antrieb montiert.



In anderen Antrieben montieren
Für die Montage ohne Montagewinkel wird der Connector One G2 an einer geeigneten Stelle mit dem Klettband befestigt.



5 Störungsbehebung

Fehler	Lösung
Das OPC UA-Server-Zertifikat ist abgelaufen.	Service-Modus: Im Menü <System> Datum/Uhrzeit überprüfen und ggf. korrigieren. Danach im <Menü> OPC UA das Server-Zertifikat löschen. Anschließend den Connector One G2 neustarten. Nach dem Reboot wird automatisch ein neues Zertifikat generiert. Dieses Zertifikat ist ab Erstellung 4 Jahre gültig.
Die Service-Webseite lässt sich nicht aufrufen.	Die URL im Browser auf korrekte Eingabe überprüfen. http://192.168.10.4 Ggf. den Browser Cache löschen und die Seite neu laden.
Der Fehler „BadUserIdentity“ wird im OPC UA-Client angezeigt.	Die Authentifizierung im Service-Modus prüfen und ggf. anpassen.
Bei TMS-Geräten lässt sich der Programmschalter nicht über OPC UA ändern.	Ggf. mit Hilfe der Antriebsanleitung sicherstellen, dass der Programmschalter von außen verändert werden darf (Konfiguration des Antriebs). Bei Fluchtwegsteuerungen ist ggf. eine spezielle Antriebsfirmware erforderlich (z. B. ES 200 2D oder FFT), da es gesetzlich untersagt ist, aus der Ferne den Programmschalter zu manipulieren. Hierzu den dormakaba Service kontaktieren.
Beim TMS-Gerät kommt keine Verbindung zustande.	Sicherstellen, dass die RS 232-Schnittstelle auf den TMS-Modus konfiguriert ist (siehe Anleitung des entsprechenden Antriebs).
Beim Antrieb mit dem Handheld-Protokoll kommt keine Verbindung zustande.	Sicherstellen, dass die RS 232-Schnittstelle auf den Handheld-Modus konfiguriert ist (siehe Anleitung des entsprechenden Antriebs).
Nach einem Firmwareupdate kann nicht mehr auf den Connector One G2 zurückgegriffen werden.	Den Connector One G2 auf Werkseinstellungen zurücksetzen, siehe Den Connector One G2 mit einem Smart-Building-System in Betrieb nehmen [▶ 3.3].

6 Demontage und Entsorgung

Die Demontage erfolgt in umgekehrter Reihenfolge der Montage und muss durch sachkundiges Personal erfolgen.

Das Produkt darf nicht zusammen mit dem Hausmüll entsorgt werden. Das Produkt umweltgerecht in den dafür eingerichteten Annahme- und Sammelstellen entsorgen. Die geltenden nationalen gesetzlichen Vorschriften beachten.

Notizen

www.dormakaba.com

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

www.dormakaba.com