dormakaba

Connector One G2

Operating Manual

060869 45532/TECHDOC-716 - 02/2026

EN

Table of contents

1 Information about this document

1.1 Contents and purpose

This manual describes how to use Connector One G2.

1.2 Target group

This document is designed for technically qualified specialists, who have suitable technical training and experience in using the technology. It is the specialist's responsibility to ensure that the conditions set out by the manufacturer as well as applicable regulations and standards are complied with when handling the product in question.

1.3 Documents storage

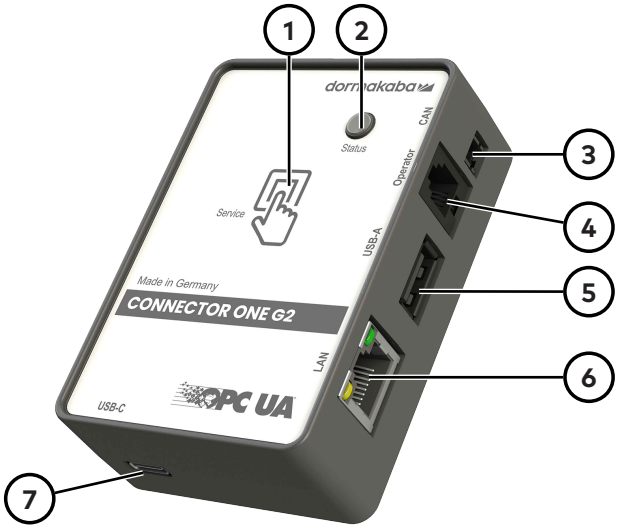
This document and the applicable documents must be handed over to the facility operator. The documents must be kept during the service life of the product and made accessible to staff.

1.4 Intended use

- Extension of dormakaba door systems with an Ethernet interface
- Use in the interior of buildings

2 Product description

A Connector One G2 enables automatic doors and door systems from dormakaba to be extended by an network interface. As a result, remote access is possible via the local network. The platform-independent data exchange is performed securely via the OPC UA standard. Smart building systems that support OPC UA gain extensive access to information and control options with Connector One G2. Furthermore, the Connector One G2 supports the EntriWorX Ecosystem. Connected devices can be monitored, controlled, and managed with EntriWorX Insights.



1 Service button for configuring Connector One G2

2 Status LED

3 CAN BUS connection*

4 RS 232 interface for connection to the operator control unit

5 USB-A interface
NOTICE! The USB-A interface may only be used for approved devices***. No other devices may be plugged in, as this may lead to malfunctions or, in extreme cases, damage.

6 LAN interface for connection to the customer network or computer

7 USB-C interface for power supply

2.1 Technical data

Voltage**	24 V DC ± 20% / 5 V DC
Operating temperature	-15°C to 55°C
Rel. humidity	5% to 95%
Interfaces	RS232, LAN, USB-A, USB-C, CAN*
Radio	Bluetooth LE

* Intended for future applications

** Power is supplied directly via the door operator or via the USB-C interface and a USB power supply.

*** The list of approved devices can be downloaded here: https://www.dormakaba.com/connector-one

2.2 Lithium battery

The device contains 1 CR1220 lithium battery as a backup battery.

The battery does not require any service or maintenance. The battery is designed to last until the end of its life cycle.

Comply with safety regulations for transporting devices with lithium batteries.

2.3 Conformity

2.3.1 EU Declaration of Conformity

This chapter is an extract from the full declaration of conformity.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Germany

hereby declares that the product described complies with the provisions of the listed directive(s) and that the standards and/or technical specifications referred to below have been applied.

Directives:

2014/53/EU	Radio equipment
2011/65/EU	RoHS

The technical documentation is available from the Product Compliance Manager at: product-compliance.dach@dormakaba.com

Harmonized European standard, national rule:

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 Declaration of Conformity

This chapter is only an extract from the full declaration of conformity.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Germany

hereby declares that the product described complies with the provisions of the listed Directive(s) and that the standards and/or technical specifications referred to below have been applied.

Directives:

Radio Equipment Regulations 2017

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

The technical documentation is available from the Product Compliance Manager at: product-compliance.dach@dormakaba.com

Harmonized European standard, national rule:

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 The product meets the requirements of:

- **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 The product meets the requirements of:

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

2.4 LED codes

Status	Color	Mode
System start	Yellow	Slow flashing
Configuration required	Yellow	Permanently on
Ready for operation, a door control was detected	Green	Permanently on
Ready for operation, a door control was not detected	Green	Slow flashing
Error	Red	Permanently on
Service mode or Bluetooth connection active	Blue	Permanently on
Service mode activated or device identification active	Blue	Slow flashing
Data transmission/software update	Cyan	Rapid flashing

2.5 Supported door operators and door systems

Products with TMS protocol

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

Products with Datalink protocol from ETS22 onwards

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

Products with handheld protocol from ESA2 controller

ESA 100
ESA 200
ESA 300
ESA 400
ESA 500

Products with EL protocol

EL 301	AL 501
AL 401	AL 1001

These door operators require an RS485/RS232 converter (article no. 29262009) to enable connection to Connector One G2.

2.6 OPC UA data points & software updates

As the information model and Connector One G2 software are constantly being developed and additional devices and functionalities are added as necessary, the software updates and OPC UA data point tables for the specific operators can be viewed online in the my.dormakaba Portal.
This requires a one-off, free registration at:
https://portal.dormakaba.com/registration
Following login, Connector One G2 data can be viewed at:
https://dormakaba.com/connector-one

3 Commissioning

3.1 Requirements for commissioning

TMS devices
The RS232 interface of the operator control is configured as TMS mode.

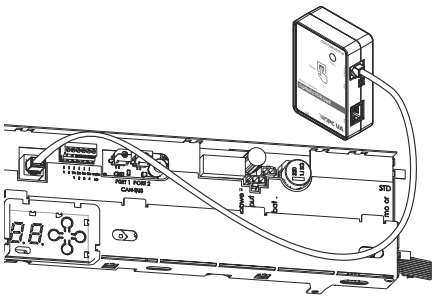
ET22
An RS232 interface is available.

EL operators
An RS485/RS232 converter is available.

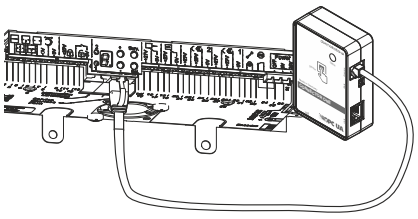
3.2 Connecting Connector One G2

Connect Connector One G2 to the control unit via the RS 232 interface.

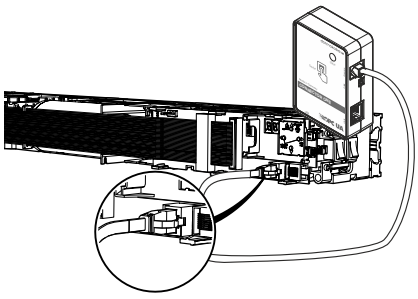
Connection to ES PROLINE



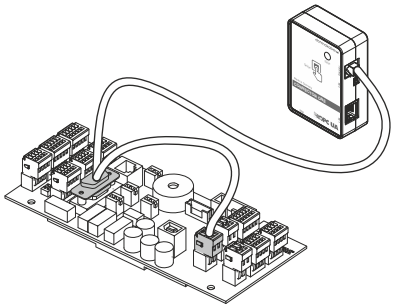
Connection to ES 200



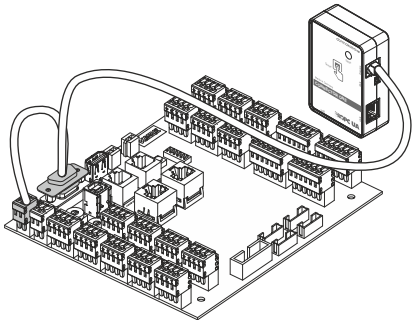
Connection to ED 100, ED 250



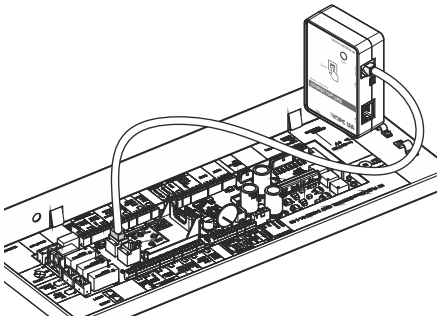
Connection to the ETS22



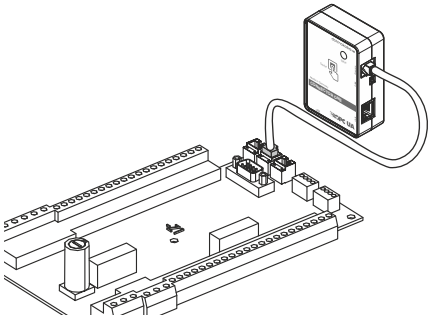
Connection to the ETS22sc2



Connection to KTV

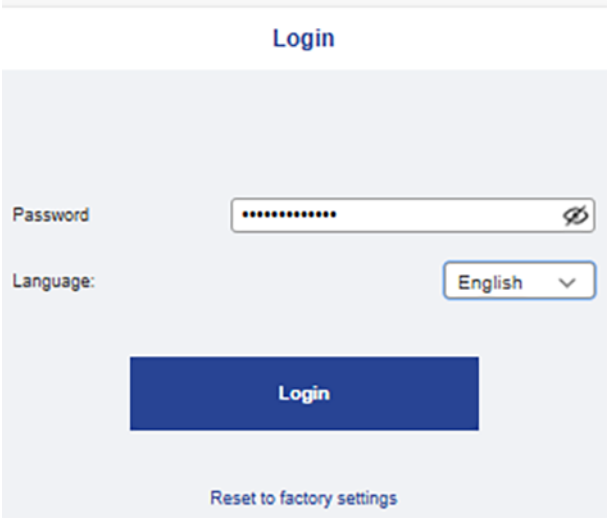


Connection to KTC 2 III



3.3 Commissioning the Connector One G2 with a smart building system

1. Connect Connector One G2 to a computer with a LAN cable or an Ethernet adapter for smart devices to a smartphone/tablet.
   - ⇨ The status LED flashes yellow. Flashing indicates the start-up process.
   - ⇨ At the end of the startup process, the LED changes its color and, if necessary, the flashing behavior.
2. Press the Service button to start Service mode.
   - ⇨ After a few seconds, the status LED will start flashing blue.
   - ⇨ If the LED lights up blue permanently, Service mode is being activated.
   - ⇨ If you do not log in to Connector One G2, Service mode ends after 1 minute.
   - ⇨ If the network setting on the PC is set to "Obtain IP address automatically" (default), Connector One G2 automatically assigns an IP address to the connected computer or smart device. If this is not desired, the appropriate network setting on the computer or smart device must be configured in advance.
3. Call up the address http://192.168.10.4 in the browser. The usual web browsers such as Chrome, Firefox, Opera and Safari are supported.
4. Set up a 12-digit password.
   - ⇨ The login menu appears.



5. Enter the previously defined password.
6. Select the display language.
7. Confirm by clicking on Login.
   - ⇨ If inactive for more than 5 minutes, the user is automatically logged out and the system is restarted.
8. In the "System" menu, update the date, time and time zone.
9. Delete the server certificate in the "OPC UA" menu.

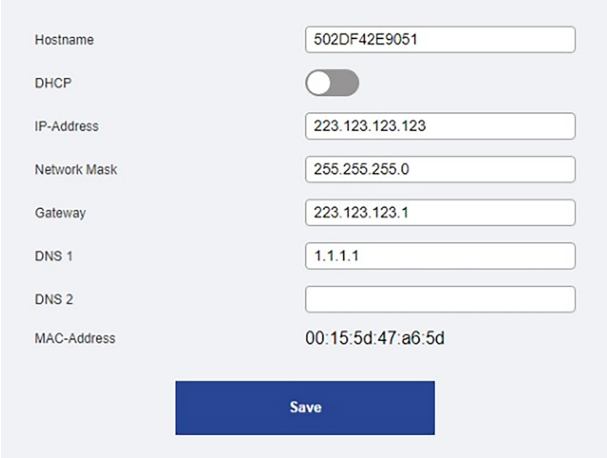
If the password is lost, Connector One G2 can be reset to factory settings in the login menu. This deletes all customer-specific settings. Connector One G2 is then in the delivery state, whereby the last firmware status is retained.

3.3.1 Configuring Connector One G2

When commissioning with EntriWorX, the Connector One G2 configuration must not be changed.

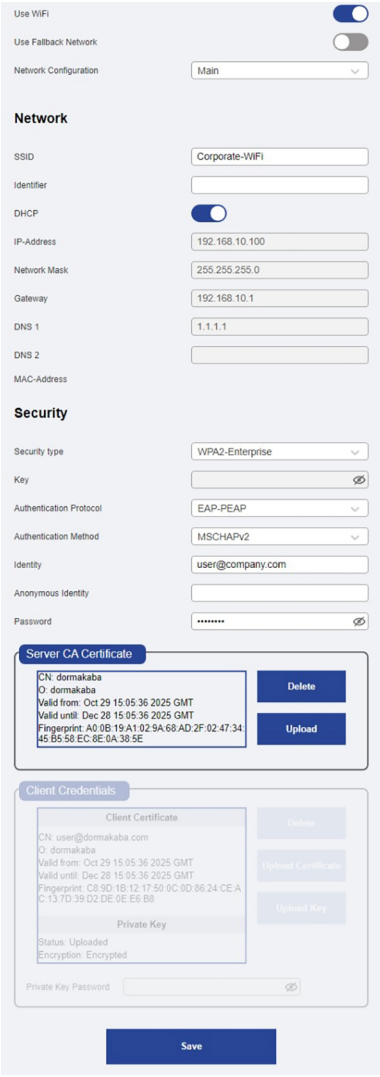
3.3.1.1 Configuring LAN

Make the required settings under “LAN” and save them by clicking “Save”.



3.3.1.2 Configuring Wi-Fi

Make the required settings under “Wi-Fi” and save them by clicking “Save”.



WiFi settings	
Using WiFi	This parameter must be enabled when using WiFi.
Using fallback network	Enables the use of a fallback network that automatically takes over if the main network fails or is unavailable. It serves as an backup connection to maintain communication or data transmission.

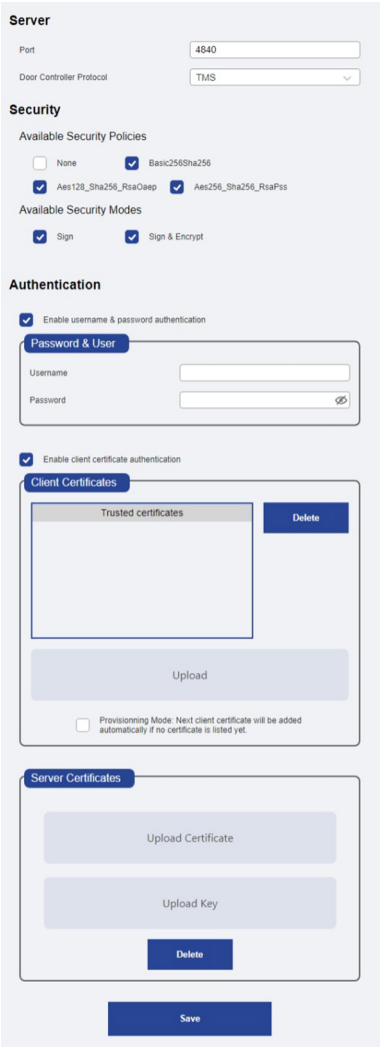
It is not possible to configure and save the networks simultaneously. After configuring a network (primary or fallback network), the settings must be saved. Otherwise, your entries will be lost when switching networks.

Network	
Identifier	This allows you to assign your own name to the Wi-Fi network.

Security	
Security type	Here you can choose between WPA2-Personal and WPA2-Enterprise. WPA2-Personal uses a single Wi-Fi password for all devices on the network. WPA2-Enterprise uses user-based authentication via a server to individually authenticate users or devices.
Key	This is where you enter the shared password used on the network to connect to the Wi-Fi.
Authentication protocol	EAP-TLS EAP-TLS offers the highest level of security because both client and server certificates for mutual authentication. This method is particularly suitable for environments with an existing certificate infrastructure. EAP-PEAP (with MSCHAPv2) EAP-PEAP first establishes an encrypted TLS tunnel to the server. The user logs in with their username and password within this tunnel. This method combines good security with easy administration. EAP-MD5 EAP-MD5 is a simple password-based method that only checks the username and a hashed password. It is easy to set up, but offers only a low level of security and is therefore only recommended for non-critical applications.
Authentication method	MSCHAPv2 is an eAuthentication method that is frequently used in WPA2-Enterprise networks in combination with EAP-PEAP. The user logs in with their personal username and password. The actual password verification is carried out via a challenge-response method within an encrypted PEAP tunnel, thus protecting the access data.
Identity	This is where a user's identity is entered, e.g., email address.
Anonymous identity	The anonymous identity is an optional username that is sent to the server when the PEAP tunnel is established. It serves to protect the actual user ID. If no anonymous identity is defined, the normal user ID will be used automatically.
Password	Enter the corresponding user's password here.
Server CA certificate	A server CA certificate is a certificate issued by a trusted certificate authority that confirms the server's identity. It is required so that clients can securely verify the server connection and establish encrypted communication.
Server certificate / "Upload certificate"	Manual transfer of server certificates.
Server certificates / "Delete"	Existing certificates can be manually deleted.
"Save"	All settings are hereby applied.

3.3.1.3 Configuring OPC UA

Under "OPC UA", set the parameters that control access to the OPC UA server.



- IP port of OPC UA server
- RS232 protocol for the connected door control unit (see Appendix)
- Authentication method
- Data encryption

Server settings	
Server port	The TCP/IP port via which the Connector One G2 should be accessible is defined here. The standard port for OPC UA is 4840.
Door Controller Protocol	Different protocols must be selected depending on the door control system. Information on the protocol can be found in the corresponding documentation.

Authentication	
Authentication password and users	The use of a username and password is an OPC UA security feature. The username and password are used for the OPC UA client to log in to Connector One G2 (OPC UA server). The details entered here must be used in the OPC UA client to gain access to the Connector One G2.
Authentication client certificates	The client certificates are an OPC UA security feature. A system authenticates itself to the Connector One G2 with a client certificate. Multiple certificates can be stored at the same time.

	Certificates can be transferred to Connector One G2 in advance. Connector One G2 may automatically accept the first certificate provided to it.
<Delete> client certificates	Deletes existing client certificates.
<Upload> client certificates	Manual transfer of client certificates.
Client certificates / Provisioning mode	There are not yet any certificates stored. Once a client logs in with their certificate, it will be accepted by Connector One G2. No further certificates can be automatically accepted.

Security rules	
Available security policies	A security policy defines which mechanisms should be used for the secure channel between the client and the server. The security policy defines the algorithms for signing and encrypting, the algorithm for key derivation and the key lengths used in the algorithms. One of the following rules must be selected. Several rules are possible at the same time. • None • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss More information about the security rules can be found at: https://profiles.opcfoundation.org/profilefolder/474
Available security modes	The security mode specifies which general security levels of Connector One G2 are offered to a client that can be applied to messages. It also depends on the client's capabilities. • None All messages are not signed or encrypted. • Sign All messages are signed, but not encrypted. • Sign & encrypt All messages are signed and encrypted.
Server certificates	The Connector One G2 (OPC UA server) uses a server certificate to authenticate itself to a client. It can be created automatically or an existing certificate can be used. An OPC UA server certificate is automatically generated during the first startup. After changing the host name or date, this server certificate should be manually deleted so that a new certificate is generated during the next startup.
Server certificates / "Upload certificate"	Manual transfer of server certificates.
Server certificates / "Upload key"	Manual transfer of the key according to the server certificate.
Server certificates / "Delete"	Existing certificates can be manually deleted.
"Save"	All settings are hereby applied.

3.3.1.4 Configuring the system

Information and settings are displayed under “System” and can be changed.

Authentication	
Change login password	The login password can be changed here.
Change date and time	A correct time is essential for using Connector One G2. It is therefore recommended to use an NTP server. If this is not possible, the time can also be set manually. • The Connector One G2's clock is battery-backed. The time does not need to be reset following a power failure. • The manually set date is saved to a file on the device and retrieved during the next startup. If the device is not in use for a longer period of time after setting the time, the date must be updated or an NTP server used.
Activate NTP	If NTP is activated, Connector One G2 synchronizes its time with an NTP server. Enter the NTP server in the network setting. Manual time configuration is not possible if the function is activated.
Manual time setting	By clicking on the time and time zone, the current time can be manually entered.
Obtain time from the host system	To simplify the manual time configuration, the current time and time zone can be loaded from the host system.
Change date and time	The time and time zone displayed is adopted by Connector One G2.
Firmware update	New firmware can be installed using this function. The current version is displayed.
Add or browse for new firmware via drag & drop	This transfers a new firmware file to the Connector One G2.
Install	After transferring firmware, the installation can be run.
Reset to factory settings	This resets Connector One G2 to factory settings. The device is then in the delivery state, while the last firmware status is retained.

3.4 Commissioning Connector One G2 with EntriWorX

1. The status LED flashes yellow. Flashing indicates the start-up process.
   ⇨ At the end of the start-up process, the LED changes its color and, if necessary, its flashing behavior, see LED codes [▶ 2.4].

3.4.1 Prerequisites

- A customer project has been created in the EntriWorX Planner.
- A work package with the door to be installed was assigned to an installer.
- The e-mail invitation for the technician was accepted.

3.4.2 EntriWorX Planner

1. Place a door on the floor plan.
2. Select and place a template with the desired protocol (TMS, Datalink, Handheld or EL protocol).
3. Assign a Connector One G2 to the door.
4. Set the settings for network and Wi-Fi.
5. Set the OPC UA settings.
6. Create a new work package (commissioning) and add the door.
7. Assign the work package to the technician.

⇨ When the work package is assigned, the technician receives an e-mail invitation.

⇨ The technician must accept the invitation to receive the rights in the EntriWorX Setup App for commissioning.

Information on network and WiFi settings

- To use WPA2-Enterprise for accessing the corporate WiFi, the connection must first be set up in Connector One G2's web UI with certificate and access data. The connection can then be selected in the setup app.
- The LTE modem is automatically detected by Connector One G2 and displayed in the setup app.

3.4.3 EntriWorX Setup App

1. Log in to the app by entering the email and password and select the market.
2. Select the building and the door.
   ⇨ The LED on the Connector changes to blue and indicates a Bluetooth connection to the EntriWorX Setup app.
3. Start the commissioning with network settings.
   ⇨ The LTE modem is automatically detected by Connector One G2 and displayed in the EntriWorX Setup App.
4. Transfer the configuration from the EntriWorX Planner to the Connector One G2.
   ⇨ The Bluetooth connection is interrupted and the door is in operation.
5. Transfer the OPC UA settings.

Information on network and WiFi settings

- In the EntriWorX Planner, LAN and Wi-Fi (WPA2-Personal) can be predefined in the Planner and transferred to the EntriWorx Setup App.
- In the EntriWorx Setup app, the predefined corporate WiFi can be selected via the "WiFi local Setup" option.
- The LTE modem is automatically detected by Connector One G2 and displayed in the EntriWorx Setup app.

Server settings	
TCP port	Specifies the TCP/IP port from which Connector One G2 can be accessed. The standard port for OPC UA is 4840.

Security policy	
Available security policies	A security policy defines which mechanisms should be used for the secure channel between the client and the server. The security policy defines the algorithms for the signature and encryption, the algorithm for key derivation and the key lengths used in the algorithms. The following guidelines are available (multiple selection possible): • None • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss For more information on the security rules, see: https://profiles.opcfoundation.org/profilefolder/474
Security mode	
Available security modes	The security mode specifies which general security levels can be applied to messages. The Connector One G2 offers the following security modes: (Multiple selection possible): • None No messages are signed or encrypted. • Sign All messages are signed, but not encrypted. • Sign and encrypt All messages are signed and encrypted. The security mode also depends on the OPC UA client's capabilities.

Authentication	
Authentication, password and users	The use of a username and password is an OPC UA security feature. The user name and password are used to allow the OPC UA client to log in to Connector One G2 (OPC UA server). The details entered here must be used in the OPC UA client to gain access to Connector One G2.

1. To complete the process, click “Save”.

3.5 Connecting and configuring OPC UA Client

Prerequisites

- Connector One G2 is ready for operation.

  => The status LED lights up or flashes green.
- Connector One G2 is correctly connected to the network.

Establish connection

1. Enter the following endpoint URL in the browser.
   opc.tcp://[Connector One G2 IP address]:[Server Port]
   Example: opc.tcp://192.168.1.20:4840

Configure OPC UA client

1. Set the security rules to match the rules in Connector One G2.
2. Select the authentication method that matches the setting in Connector One G2.

If certificates are to be used, they may have to be exchanged in advance.

3. Establish the connection.

4 Mounting

NOTICE

Property damages due to collision

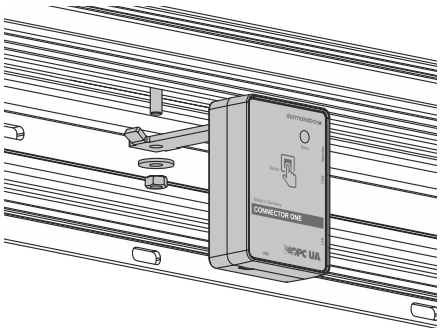
Connector One G2 and/or cables may be damaged due to collision with moving parts.

- Mount Connector One G2 in such a way that it cannot collide with moving parts.
- Guide/stow all cables inside the operator in existing cable ducts or secure them with a cable holder.

After finishing the complete configuration, Connector One G2 is mounted in the door operator.
Different mounting materials are available, depending on the door operator.

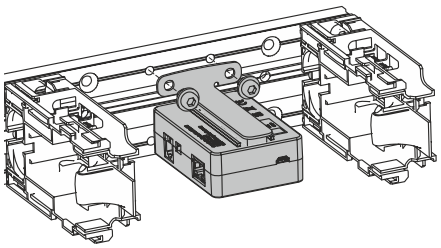
Mounting in ES PROLINE

In ES PROLINE, Connector One G2 is mounted with the enclosed mounting bracket in the operator.



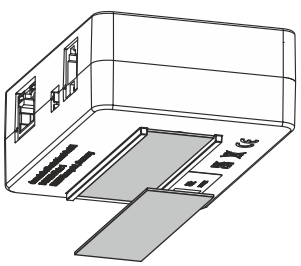
Mounting in ED 100, ED 250

In ED 100, ED 250, Connector One G2 is mounted in the operator with the enclosed mounting bracket and ED installation kit.



Mounting in other operators

For mounting without a mounting bracket, Connector One G2 is attached to a suitable point with the Velcro strip.



5 Troubleshooting

Error	Solution
The OPC UA server certificate has expired.	Service mode: Check the <System> date/time menu and correct it if necessary. Then delete the server certificate in the OPC UA <menu>. Then restart Connector One G2. Following the reboot, a new certificate is automatically generated. The certificate is valid for 4 years from the date of creation.
The service website cannot be accessed.	Check that the URL in the browser is correctly entered. http://192.168.10.4 If necessary, delete the browser cache and reload the page.
The "BadUserIdentity" error is displayed in the OPC UA client.	Check the authentication in service mode and adjust if necessary.
For TMS devices, the program switch cannot be changed via OPC UA.	If necessary, use the operator manual to ensure that the program switch can be changed from outside (operator configuration). For escape route controls, special drive firmware may be required (e.g. ES 200 2D or FFT), as it is legally prohibited to remotely manipulate the program switch. Contact dormakaba Service for this purpose.
No connection is established with the TMS device.	Ensure that the RS-232 interface is configured to TMS mode (see the corresponding operator manual).
No connection is established with the operator using the Handheld protocol.	Ensure that the RS 232 interface is configured to Handheld mode (see the corresponding operator manual).
After a firmware update, the Connector One G2 can no longer be used.	Reset the Connector One G2 to factory settings, see Commissioning the Connector One G2 with a smart building system [▶ 3.3].

6 Disassembly and disposal

Disassembly is carried out in the reverse order of mounting and must be carried out by qualified personnel.

The product must not be disposed of in domestic waste. Dispose of the product in an environmentally friendly manner at the collection points set up for this purpose. Refer to the statutory regulations for your country.

www.dormakaba.com

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

www.dormakaba.com