dormakaba

Connector One G2

Istruzioni per l'uso

060948 45532/TECHDOC-716 - 02/2026

IT

Contenuto

1 Informazioni sul documento

1.1 Contenuto e scopo

Questo manuale descrive come utilizzare il Connector One G2.

1.2 Destinatari

Questo documento è destinato a specialisti tecnicamente qualificati.
Uno specialista tecnicamente qualificato ha un'adeguata formazione tecnica ed esperienza nel trattare con la tecnologia. È responsabilità dello specialista garantire che le condizioni specificate dal produttore, nonché le normative e gli standard applicabili siano rispettati durante l'utilizzo del prodotto descritto.

1.3 Conservazione dei documenti

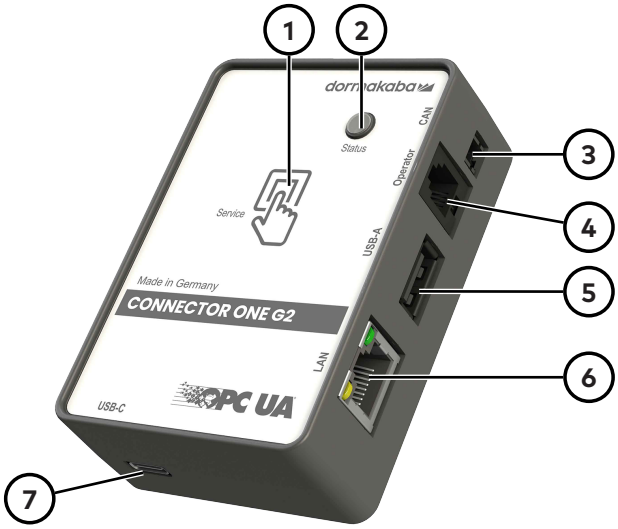
Questo documento e gli altri documenti di riferimento devono essere consegnati all'operatore. I documenti devono essere conservati per tutta la durata di vita del prodotto e resi accessibili al personale.

1.4 Uso previsto

- Estensione dei sistemi di porte dormakaba con un'interfaccia Ethernet.
- Utilizzo in ambienti interni

2 Descrizione del prodotto

Con un Connector One G2, le porte automatiche e i sistemi di porte dormakaba possono essere ampliati per includere un'interfaccia di rete. Ciò consente l'accesso remoto tramite la rete locale. Lo scambio di dati indipendente dalla piattaforma avviene in modo sicuro tramite lo standard OPC UA. Grazie al Connector One, i sistemi di edifici intelligenti che supportano lo standard OPC G2 hanno un ampio accesso alle informazioni e alle opzioni di controllo. Il Connector One G2 supporta anche l'EntriWorX EcoSystem. I dispositivi connessi possono essere monitorati, controllati e gestiti con EntriWorX Insights.



1 Pulsante di servizio per la configurazione del Connector One G2

2 LED di stato

3 Collegamento CAN-bus*

4 Interfaccia RS 232 per il collegamento al comando di azionamento

5 Interfaccia USB-A
AVVISO L'interfaccia USB-A può essere utilizzata solo per dispositivi approvati***. Non è consentito collegare altri dispositivi, poiché questo potrebbe causare malfunzionamenti o, in casi estremi, danni.

6 Interfaccia LAN per il collegamento al computer o alla rete del cliente

7 Interfaccia USB-C per l'alimentazione

2.1 Dati tecnici

Tensione**	24 V DC ± 20 % / 5 V DC
Temperatura di esercizio	-15 °C – +55 °C
Umidità relativa	5 % – 95 %
Interfacce	RS232, LAN, USB-A, USB-C, CAN*
Radio	Bluetooth LE

* Destinato ad applicazioni future

** L'alimentazione viene fornita direttamente tramite l'azionamento della porta o tramite l'interfaccia USB-C e un alimentatore USB.

*** L'elenco dei dispositivi approvati può essere scaricato qui:
https://www.dormakaba.com/connector-one

2.2 Batteria al litio

Il dispositivo contiene 1 batteria al litio CR1220 come batteria di riserva.

La batteria non richiede interventi di servizio o manutenzione. La batteria è prevista per durare fino alla fine del ciclo di vita.

Attenersi alle norme di sicurezza per il trasporto di dispositivi con batterie al litio.

2.3 Conformità

2.3.1 Dichiarazione di conformità UE

Questo capitolo è un estratto della dichiarazione di conformità completa.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Germania

dichiara con la presente che il prodotto descritto è pienamente conforme agli standard delle direttive CE elencate e che sono state adottate le norme e/o le specifiche tecniche di seguito riportate.

Direttive:

2014/53/UE	Apparecchiature radio
2011/65/UE	RoHS

La documentazione tecnica è disponibile presso il product compliance manager all'indirizzo: product-compliance.dach@dormakaba.com

Norma europea armonizzata, normativa nazionale:

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 Dichiarazione di conformità UKCA

Questo capitolo è solo un estratto della dichiarazione di conformità completa.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Germany

dichiara con la presente che il prodotto descritto è pienamente conforme agli standard delle direttive CE elencate e che sono state adottate le norme e/o le specifiche tecniche di seguito riportate.

Direttive:

Radio Equipment Regulations 2017

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

La documentazione tecnica è disponibile presso il product compliance manager all'indirizzo: product-compliance.dach@dormakaba.com

Norma europea armonizzata, normativa nazionale:

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 Il prodotto soddisfa i requisiti di:

- **FCC Titolo 47 CFR Parte 15**
  ID 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 Il prodotto soddisfa i requisiti di:

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

2.4 Codici LED

Stato	Colore	Modalità
avvio del sistema	giallo	lampeggiamento lento
configurazione richiesta	giallo	luce fissa
pronto per il funzionamento, è stato rilevato un controllo porta	verde	luce fissa
pronto per il funzionamento, non è stato riconosciuto un controllo porta	verde	lampeggiamento lento
errore	rosso	luce fissa
Modalità di servizio o connessione Bluetooth attiva	blu	luce fissa
Modalità di servizio attivata o identificazione del dispositivo attiva	blu	lampeggiamento lento
trasferimento dati/aggiornamento software	ciano	lampeggiamento rapido

2.5 azionamenti porte e sistemi di porte supportati

Prodotti con protocollo 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

Prodotti con protocollo Datalink a partire da ETS22

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

Prodotti con protocollo palmare del controller ESA2

ESA 100
ESA 200
ESA 300
ESA 400
ESA 500

Prodotti con protocollo EL

EL 301	AL 501
AL 401	AL 1001

Per questi azionamenti per porte è necessario un convertitore RS485/RS232 (codice articolo 29262009) per consentire il collegamento al Connector One G2.

2.6 Punti dati OPC UA e aggiornamenti software

Poiché il modello informativo e il software Connector One G2 vengono costantemente sviluppati e possono essere aggiunti ulteriori dispositivi e funzionalità, gli aggiornamenti del software e le tabelle dei punti dati OPC UA per gli azionamenti specifici possono essere visualizzati online nel portale my.dormakaba.
Ciò richiede una registrazione gratuita una tantum all'indirizzo:
https://portal.dormakaba.com/registration
Dopo aver effettuato l'accesso, i dati relativi al Connector One G2 possono essere visualizzati seguendo questo percorso:
https://dormakaba.com/connector-one

3 Messa in servizio

3.1 Requisiti per la messa in funzione

Dispositivi TMS
L'interfaccia RS232 del comando azionamento è configurata come in modalità TMS.

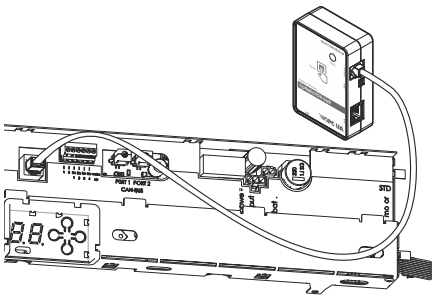
ETS22
È disponibile un'interfaccia RS232.

Azionamenti EL
È disponibile un convertitore RS485/RS232.

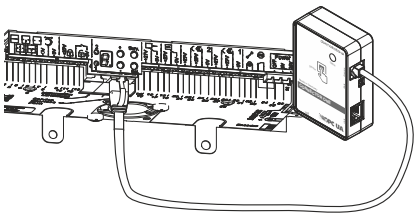
3.2 Connessione del Connector One G2

Connettere il Connector One G2 all'unità di comando tramite l'interfaccia RS 232.

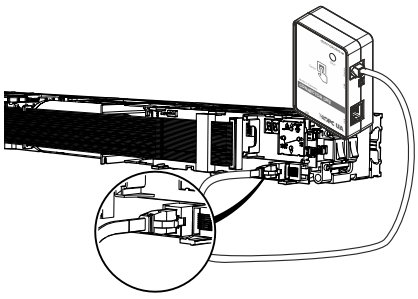
Connessione a ES PROLINE



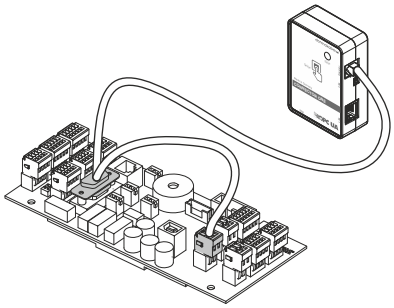
Connessione a ES 200



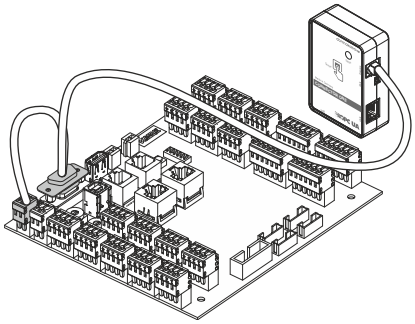
Connessione a ED 100, ED 250



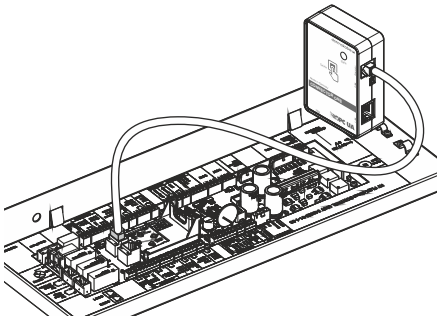
Collegamento all'ETS22



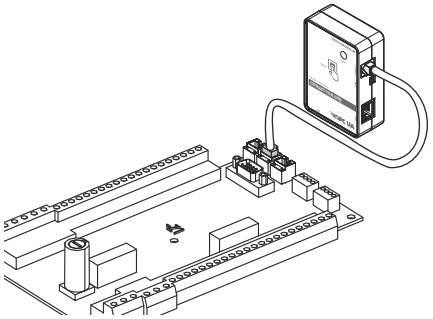
Collegamento all'ETS22sc2



Connessione a un KTV



Connessione a un KTC 2 III



3.3 Messa in funzione del Connector One G2 con un sistema di edifici intelligenti

1. Connettere il Connector One G2 a un computer tramite un cavo LAN oppure a uno smartphone o un tablet tramite un adattatore Ethernet per dispositivi smart.
   - ⇨ Il LED di stato lampeggia in giallo. Il lampeggiamento segnala il processo di avvio.
   - ⇨ Al termine del processo di avvio, il LED cambia colore e, se necessario, lampeggia.
2. Premere il pulsante di assistenza per avviare la modalità di assistenza.
   - ⇨ Dopo alcuni secondi, il LED di stato inizierà a lampeggiare in blu.
   - ⇨ Se il LED emette una luce blu fissa, la modalità di assistenza è attivata.
   - ⇨ Se non avviene alcun accesso al Connector One G2, la modalità di assistenza viene terminata automaticamente dopo 1 minuto.
   - ⇨ Se nelle impostazioni di rete sul PC è configurata l'opzione "Ottieni automaticamente un indirizzo IP" (impostazione predefinita), il Connector One G2 assegna automaticamente un indirizzo IP al computer o al dispositivo smart connesso. Se si desidera che ciò non avvenga, è necessario configurare in anticipo l'impostazione di rete appropriata sul computer o sul dispositivo smart.
3. Accedere all'indirizzo http://192.168.10.4 dal browser. Sono supportati i comuni browser come Chrome, Firefox, Opera e Safari.
4. Impostare una password di 12 caratteri.
   - ⇨ Viene visualizzato il menu di accesso.

5. Immettere la password precedentemente impostata.
6. Selezionare la lingua di visualizzazione.
7. Confermare cliccando sul pulsante di accesso.
   - ⇨ Dopo più di 5 minuti di inattività, l'utente viene disconnesso automaticamente e il sistema si riavvia.
8. Aggiornare data, ora e fuso orario nel menu di sistema.
9. Eliminare il certificato server nel menu "OPC UA".

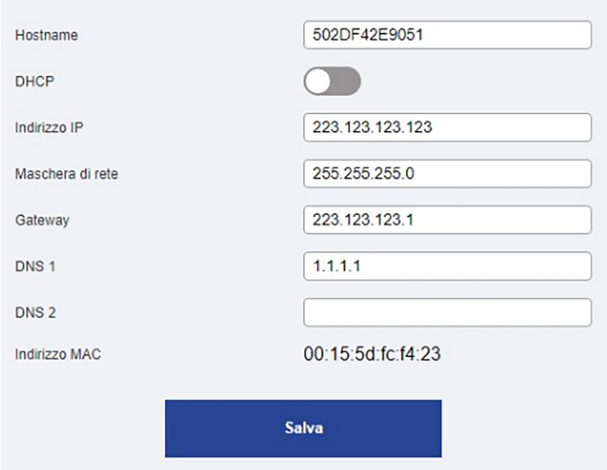
Se la password viene persa, il Connector One G2 può essere ripristinato alle impostazioni di fabbrica nel menu di accesso. Tutte le impostazioni specifiche del cliente vengono cancellate durante il processo. Il Connector One G2 si trova quindi allo stato di fabbrica, per cui viene mantenuta l'ultima versione del firmware.

3.3.1 Configurazione del Connector One G2

Durante la messa in funzione con EntriWorX, la configurazione del Connector One G2 non deve essere modificata.

3.3.1.1 Configurare la LAN

Selezionare le impostazioni necessarie in "LAN" e salvare con il comando "Salva".



3.3.1.2 Configurare la WLAN

Selezionare le impostazioni necessarie in "WLAN" e salvare con il comando "Salva".

Impostazioni WiFi	
Utilizzare il WiFi	Questo parametro deve essere attivato quando si utilizza il WiFi.
utilizzare la rete di riserva	Consente l'utilizzo di una rete di riserva che subentra automaticamente quando la rete principale non funziona o non è disponibile. Funge da collegamento alternativo per mantenere la comunicazione o la trasmissione dei dati.

Non è possibile configurare e salvare contemporaneamente le reti. Dopo aver configurato una rete (rete principale o di riserva), è necessario salvare le impostazioni. In caso contrario, i dati inseriti andranno persi al momento del cambio di rete.

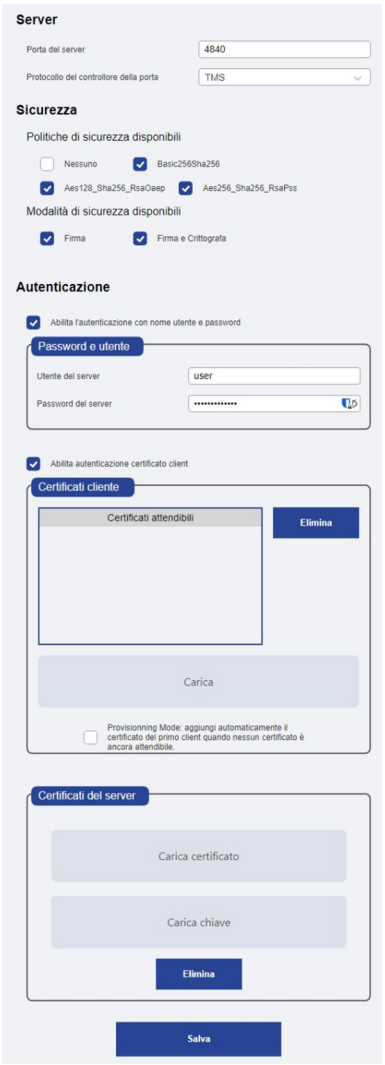
Rete	
identificativo	In questo modo è possibile assegnare un nome personalizzato alla rete WLAN.

Sicurezza	
Tipo di sicurezza	Qui è possibile scegliere tra WPA2-Personal e WPA2-Enterprise. Con WPA2-Personal viene utilizzata una password WLAN comune per tutti i dispositivi della rete. Con WPA2-Enterprise, l'accesso basato sull'utente avviene tramite un server per autenticare individualmente utenti o dispositivi.
Chiave	Qui deve essere inserita la password comune utilizzata nella rete per connettersi alla WLAN.
Protocollo di autenticazione	EAP-TLS EAP-TLS offre la massima sicurezza, poiché sia il client sia il server utilizzano certificati per l'autenticazione reciproca. Questo metodo è particolarmente indicato per ambienti con un'infrastruttura di certificati già esistente. EAP-PEAP (con MSCHAPv2) EAP-PEAP stabilisce innanzitutto un tunnel TLS crittografato verso il server. All'interno di questo tunnel, l'accesso avviene tramite nome utente e password. Questo metodo combina una buona sicurezza con una facile gestione. EAP-MD5EAP-MD5 è un semplice metodo basato su password che verifica solo il nome utente e una password cifrata tramite funzione di hash. È facile da configurare, ma offre solo un basso livello di sicurezza ed è pertanto consigliato solo per applicazioni non critiche.
Metodo di autenticazione	MSCHAPv2 è un metodo di autenticazione elettronica comunemente utilizzato nelle reti WPA2 Enterprise in combinazione con EAP-PEAP. L'utente accede con il proprio nome utente personale e la propria password. L'autenticazione della password viene eseguita mediante un meccanismo di challenge-response all'interno di un tunnel PEAP crittografato, che protegge i dati di accesso.
Identità	Qui viene inserita l'identità di un utente, ad esempio l'indirizzo e-mail.
Identità anonima	L'identità anonima è un nome utente facoltativo che viene inviato al server durante la creazione del tunnel PEAP. Serve a proteggere l'identificativo utente effettivo. Se non viene definita alcuna identità anonima, viene utilizzata automaticamente l'identità utente normale.
Password	Qui deve essere inserita la password dell'utente corrispondente.
Certificato di CA del server	Un certificato CA del server è un certificato rilasciato da un'autorità di certificazione affidabile che conferma l'identità del server. È necessario affinché i client possano verificare in modo sicuro la connessione al server e stabilire una comunicazione crittografata.
Certificati server / "Carica certificato"	Trasferimento manuale dei certificati server.
Certificati server / "Elimina"	I certificati esistenti possono essere eliminati manualmente.

"Salva"	Questa opzione conferma tutte le impostazioni.

3.3.1.3 Configurare OPC UA

Alla voce "OPC UA" impostare i parametri che controllano l'accesso al server OPC UA.



- Porta IP del server OPC UA
- Protocollo RS232 del controllo porta collegato (vedi appendice)
- Metodo di autenticazione
- Codifica dei dati

Impostazioni del server	
Porta del server	Qui viene specificata la porta TCP/IP attraverso la quale deve essere accessibile il Connector One G2. La porta predefinita per OPC UA è 4840.
Protocollo del controllore della porta	In base al sistema di controllo delle porte, è necessario scegliere tra diversi protocolli. È possibile ottenere maggiori informazioni sul protocollo nella relativa documentazione.

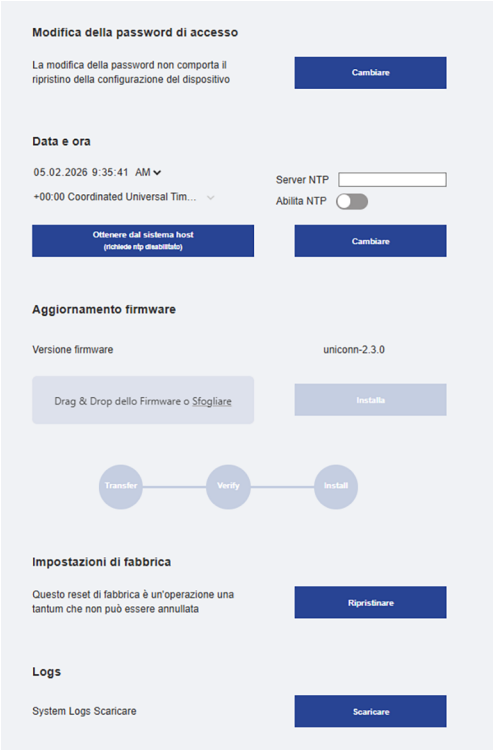
Autenticazione	
Password e utente di autenticazione	L'utilizzo di un nome utente e di una password è una funzionalità di sicurezza di OPC UA. Il nome utente e la password vengono utilizzati dal client OPC UA per accedere al Connector One G2 (server OPC UA). I dati qui inseriti devono essere utilizzati nel client OPC UA per poter accedere al Connector One G2.

Certificati client di autenticazione	I certificati client sono una funzionalità di sicurezza OPC UA. Con un certificato client un sistema si autentica nel Connector One G2. È possibile registrare più certificati contemporaneamente. I certificati possono essere trasferiti al Connector One G2 in anticipo. È possibile che il Connector One G2 accetti automaticamente il primo certificato fornitogli.
Certificati Cliente <elimina>	Eliminazione dei certificati client esistenti.
Certificati Cliente <carica>	Trasferimento manuale dei certificati client.
Certificati Cliente / Provisioning-Mode	Non è ancora presente alcun certificato in memoria. Non appena un client si registra con il proprio certificato, questo viene accettato dal Connector One G2. Altri certificati non possono essere accettati automaticamente.

Regole di sicurezza	
Criteri di sicurezza disponibili	Un criterio di sicurezza definisce quali meccanismi devono essere utilizzati per il canale sicuro tra il client e il server. Il criterio di sicurezza definisce gli algoritmi di firma e crittografia, l'algoritmo di derivazione della chiave e le lunghezze delle chiavi utilizzate negli algoritmi. Deve essere selezionata una delle seguenti regole. È possibile selezionare più regole contemporaneamente. • Nessuna • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Maggiori informazioni sulle regole di sicurezza sono disponibili al sito: https://profiles.opcfoundation.org/profilefolder/474
Modalità di sicurezza disponibili	La modalità di sicurezza determina i livelli di sicurezza generale offerti dal Connector One G2 a un client per i messaggi. Questo dipende anche dalle caratteristiche del client. • Nessuna Tutti i messaggi non sono né firmati né crittografati. • Firma Tutti i messaggi sono firmati ma non crittografati. • Firma e crittografa Tutti i messaggi sono firmati e crittografati.
Certificati server	Con un certificato server, il Connector One G2 (server OPC UA) si autentica presso un client. È possibile generarlo automaticamente o utilizzare un certificato esistente. Al primo avvio viene generato automaticamente un certificato server OPC UA. Questo certificato server deve essere eliminato manualmente dopo aver modificato il nome host o la data, in modo che venga generato un nuovo certificato al successivo avvio del server.
Certificati server / "Carica certificati"	Trasferimento manuale dei certificati server.
Certificati server / "Carica chiave"	Trasferimento manuale della chiave corrispondente al certificato server.
Certificati server / "Elimina"	I certificati esistenti possono essere eliminati manualmente.
"Salva"	Questa opzione conferma tutte le impostazioni.

3.3.1.4 Configurare il sistema

Le informazioni e le impostazioni possono essere visualizzate e modificate nella sezione "Sistema".



Autenticazione	
Modifica password di accesso	La password di accesso può essere modificata qui.
Modifica data e ora	Impostare correttamente data e ora è essenziale per l'utilizzo del Connector One G2. Si consiglia pertanto di utilizzare un server NTP. Qualora questo non fosse possibile, l'ora può essere impostata anche manualmente. • L'orologio del Connector One G2 è alimentato a batteria. Dopo un'interruzione dell'alimentazione, data e ora devono essere reimpostate. • La data impostata manualmente viene memorizzata in un file sul dispositivo e recuperata al successivo avvio. Se il dispositivo non viene utilizzato per molto tempo dopo aver impostato l'ora, è necessario aggiornare la data o utilizzare un server NTP.
Abilita NTP	Se l'opzione NTP è attiva, il Connector One G2 sincronizza le indicazioni di data e ora con un server NTP. Il server NTP deve essere inserito nelle impostazioni di rete. La configurazione manuale di data e ora non è possibile quando la funzione è attivata.
Impostazione manuale dell'ora	L'ora corrente può essere inserita manualmente facendo clic sulle indicazioni relative all'ora e al fuso orario.
Ottenere l'ora dal sistema host	Per facilitare la configurazione manuale di data e ora, l'ora e il fuso orario correnti possono essere caricati dal sistema host.
Modifica data e ora	L'ora e il fuso orario visualizzati vengono confermati dal Connector One G2.
Aggiorna il firmware	Questa funzione può essere utilizzata per installare un nuovo firmware. Viene visualizzata la versione corrente.
Drag & Drop dello Firmware o Sfogliare	Questa opzione consente di trasferire un nuovo file firmware al Connector One G2.
Installazione	Dopo aver trasferito un firmware, è possibile eseguire l'installazione.
Ripristino delle impostazioni di fabbrica	Questa opzione consente di ripristinare un Connector One G2 alle impostazioni di fabbrica. Il dispositivo si trova quindi allo stato di fabbrica, per cui viene mantenuta l'ultima versione del firmware.

3.4 Messa in funzione del Connector One G2 con EntriWorX

1. Il LED di stato lampeggia in giallo. Il lampeggiamento indica l'avvio del processo.
   ⇨ Al termine del processo di avvio, il LED cambia colore e, se necessario, il comportamento di lampeggiamento, vedi Codici LED [▶ 2.4].

3.4.1 Prerequisiti

- È stato creato un progetto del cliente in EntriWorX Planner.
- Un pacchetto di lavoro con la porta da installare è stato assegnato a un installatore.
- L'invito tramite e-mail per il tecnico è stato accettato.

3.4.2 EntriWorX Planner

1. Posizionare una porta sulla pianta.
2. Selezionare e posizionare un modello con il protocollo desiderato (TMS, Datalink, Palmare o Protocollo EL).
3. Assegnare un Connector One G2 alla porta.
4. Impostare le impostazioni di rete e WiFi.
5. Impostare le impostazioni OPC UA.
6. Creare un nuovo pacchetto di lavoro (Commissioning) e aggiungere la porta.
7. Assegnare il pacchetto di lavoro al tecnico.

⇨ Quando il pacchetto di lavoro viene assegnato, il tecnico riceve un invito via e-mail.

⇨ Per acquisire i diritti per la messa in funzione nella EntriWorX Setup App il tecnico deve accettare l'invito.

Note sulle impostazioni di rete e WiFi

- Per utilizzare WPA2 Enterprise per l'accesso al WiFi aziendale, è necessario prima configurare la connessione nell'interfaccia utente web del Connector On G2 con certificato e dati di accesso. Quindi è possibile selezionare la connessione nell'app di configurazione.
- Il modem LTE viene rilevato automaticamente dal Connector One G2 e visualizzato nell'app di configurazione.

3.4.3 EntriWorX Setup App

1. Accedere all'app con il proprio indirizzo e-mail e la password e selezionare il mercato.
2. Selezionare l'edificio e la porta.
   ⇨ Il LED sul Connector diventa blu e visualizza una connessione Bluetooth alla EntriWorX Setup App.
3. Avviare la messa in funzione con le impostazioni di rete.
   ⇨ Il modem LTE viene riconosciuto automaticamente dal Connector One G2 e visualizzato nella EntriWorX Setup App.
4. Trasferire la configurazione da EntriWorX Planner a Connector One G2.
   ⇨ La connessione Bluetooth viene interrotta e la porta è in funzione.
5. Trasferire le impostazioni OPC UA.

Note sulle impostazioni di rete e WiFi

- In EntriWorX Planner è possibile predefinire LAN e WiFi (WPA2-Personal) e trasferirli nella EntriWorx Setup App.
- Nella EntriWorx Setup App è possibile selezionare il WiFi aziendale predefinito tramite l'opzione "WiFi local Setup".
- l modem LTE viene rilevato automaticamente dal Connector One G2 e visualizzato nella EntriWorx Setup App.

Impostazioni del server	
Porta TCP	Specifica la porta TCP/IP attraverso la quale è possibile accedere a Connector One G2. La porta predefinita per OPC UA è 4840.

Politica di sicurezza	
Criteri di sicurezza disponibili	Un criterio di sicurezza definisce quali meccanismi devono essere utilizzati per il canale sicuro tra il client e il server. Il criterio di sicurezza definisce gli algoritmi di firma e crittografia, l'algoritmo di derivazione della chiave e le lunghezze delle chiavi utilizzate negli algoritmi. Sono disponibili le seguenti linee guida (è possibile una selezione multipla): • Nessuna • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Per ulteriori informazioni sulle norme di sicurezza, vedere: https://profiles.opcfoundation.org/profilefolder/474
Modalità di sicurezza	
Modalità di sicurezza disponibili	La modalità di sicurezza specifica quali livelli di sicurezza generali possono essere applicati ai messaggi. Il Connector One G2 offre le seguenti modalità di sicurezza: (è possibile una selezione multipla): • Nessuno Tutti i messaggi non sono firmati o crittografati. • Firma Tutti i messaggi sono firmati ma non crittografati. • Firma e crittografia Tutti i messaggi sono firmati e crittografati. La modalità di sicurezza dipende anche dalle capacità del client OPC UA.

Autenticazione	
Autenticazione, password e utente	L'utilizzo di un nome utente e di una password è una funzionalità di sicurezza di OPC UA. Il nome utente e la password sono utilizzati per consentire al client OPC UA di accedere a Connector One G2 (server OPC UA). I dati inseriti qui devono essere utilizzati nel client OPC UA per ottenere l'accesso al Connector One G2.

1. Per concludere il processo, fare clic su "Salva".

3.5 Connettere e configurare il client OPC UA

Prerequisiti

- Il Connector One G2 è pronto per il funzionamento.

  => Il LED di stato si accende o lampeggia in verde.
- Il Connector One G2 è connesso correttamente alla rete.

Realizzazione della connessione

1. Immettere il seguente URL dell'endpoint nel browser.
   opc.tcp://[indirizzo IP del Connector One G2]:[porta del server]
   Esempio: opc.tcp://192.168.1.20:4840

Configurazione del client OPC UA

1. Impostare le regole di sicurezza in modo che corrispondano a quelle del Connector One G2.
2. Selezionare il metodo di autenticazione corrispondente a quello del Connector One G2.

Se si utilizzano i certificati, potrebbe essere necessario cambiarli in anticipo.

3. Realizzare la connessione.

4 Montaggio

AVVISO

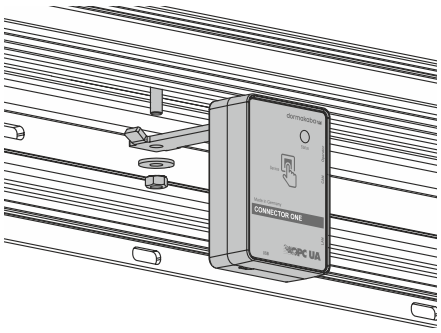
Danni materiali da collisione

La collisione con parti in movimento può danneggiare il Connector One G2 e/o i cavi.

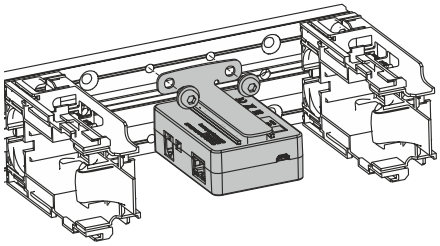
- Montare il Connector One G2 in modo che non possa entrare in collisione con parti in movimento.
- Posizionare/stoccare tutti i cavi all'interno dell'azionamento nei canali passacavo esistenti o fissarli con un reggicavi.

Al termine della configurazione completa, il Connector One G2 viene installato nell'azionamento della porta.
Sono disponibili diversi materiali di montaggio a seconda dell'azionamento della porta.

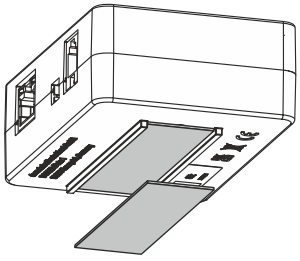
Montaggio con ES PROLINE
Con ES PROLINE, il Connector One G2 viene montato nell'azionamento utilizzando la staffa angolare fornita.



Montaggio con ED 100, ED 250
Con ED 100, ED 250, il Connector One G2 viene montato nell'azionamento utilizzando la staffa angolare fornita e il kit di installazione ED.



Montaggio con altre unità
Per il montaggio senza staffa angolare, il Connector One G2 viene fissato a un punto adatto con la striscia in velcro.



5 Eliminazione delle anomalie

Errore	Soluzione
Il certificato del server OPC UA è scaduto.	Modalità assistenza: Controllare data e ora nel menu di sistema e correggere se necessario. Dopodiché eliminare il certificato del server nel menu OPC UA. Quindi riavviare il Connector One G2. Dopo il riavvio, viene generato automaticamente un nuovo certificato. Questo certificato ha una validità di 4 anni dalla data di emissione.
Non è possibile accedere al sito web del servizio.	Controllare che l'URL sia stato immesso correttamente nel browser. http://192.168.10.4 Se necessario, cancellare la cache del browser e ricaricare la pagina.
Nel client OPC UA viene visualizzato l'errore "BadUserIdentity".	Controllare l'autenticazione in modalità di assistenza e modificare se necessario.
Con i dispositivi TMS, il commutatore a programma non può essere modificato tramite OPC UA.	Se necessario, utilizzare le istruzioni per l'operatore per assicurarsi che il commutatore a programma possa essere modificato dall'esterno (configurazione dell'operatore). Per il controllo delle uscite di emergenza può essere necessario un firmware di azionamento apposito (ad es. ES 200 2D o FFT), poiché controllare da remoto il commutatore a programma è vietato dalla legge. A tal proposito, contattare l'assistenza dormakaba.
Non viene stabilita alcuna connessione con il dispositivo TMS.	Assicurarsi che l'interfaccia RS 232 sia configurata in modalità TMS (vedere il manuale del drive in questione).
Non viene stabilita alcuna connessione con l'unità tramite il protocollo palmare.	Assicurarsi che l'interfaccia RS 232 sia configurata in modalità palmare (vedere il manuale del drive in questione).
Dopo un aggiornamento del firmware, non è più possibile accedere al Connector One G2.	Ripristinare le impostazioni di fabbrica del Connector One G2, vedere Messa in funzione del Connector One G2 con un sistema di edifici intelligenti [▶ 3.3].

6 Smontaggio e smaltimento

Per lo smontaggio seguire la procedura di montaggio in ordine inverso. L'operazione dev'essere eseguita da tecnici esperti.

Il prodotto non deve essere smaltito insieme ai rifiuti domestici. Si prega di smaltire il prodotto nel rispetto dell'ambiente presso gli appositi centri di raccolta. Osservare le normative nazionali vigenti.

Note

www.dormakaba.com

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

www.dormakaba.com