dormakaba

Connector One G2

Instructions d'emploi

060947 45532/TECHDOC-716 - 02/2026

FR

Contenu

1 Informations relatives au présent document

1.1 Contenu et finalité

Ces instructions d'utilisation décrivent l'utilisation du Connector One G2.

1.2 Groupe cible

Ce document s'adresse aux professionnels techniquement qualifiés.
Un professionnel techniquement qualifié dispose d'une formation technique et d'une expérience adéquates dans l'utilisation de cette technologie. Il est de la responsabilité du spécialiste que les conditions énoncées par le fabricant, ainsi que les prescriptions et normes applicables pour la manipulation du produit décrit soient respectées.

1.3 Conservation des documents

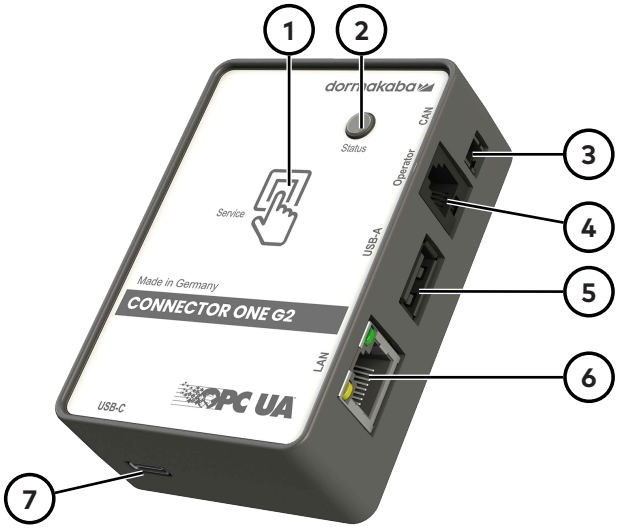
Ce document et les autres pièces y afférentes doivent être remis à l'exploitant. Les documents doivent être conservés pendant la durée de vie du produit et être rendus accessibles au personnel.

1.4 Utilisation conforme

- Extension des systèmes de portes dormakaba par une interface Ethernet.
- Utilisation à l'intérieur des bâtiments

2 Description du produit

Avec un Connector One G2, les portes et systèmes de portes automatiques de dormakaba peuvent être étendus à une interface réseau. Cela permet d'accéder à distance via le réseau local. L'échange de données indépendant de la plate-forme s'effectue en toute sécurité via la norme OPC UA. Grâce au Connector One G2, les systèmes de bâtiment intelligents prenant en charge OPC UA bénéficient d'un accès complet aux informations et aux possibilités de contrôle. En outre, le Connector One G2 prend en charge l'EntriWorX EcoSystem. Les appareils connectés peuvent être surveillés, contrôlés et gérés avec EntriWorX Insights.



1 Touche Service pour configurer le Connector One G2

2 LED de statut

3 Raccordement BUS CAN*

4 Interface RS 232 pour la connexion avec le contrôleur d'opérateur

5 Interface USB-A
AVIS! L'interface USB-A ne doit être utilisée que pour des appareils partagés***. Aucun autre appareil ne doit être branché, car cela peut provoquer des dysfonctionnements ou, dans des cas extrêmes, des dommages.

6 Interface LAN pour la connexion au réseau client ou à l'ordinateur

7 Interface USB-C pour l'alimentation électrique

2.1 Caractéristiques techniques

Tension**	24 V DC ± 20 % / 5 V DC
Température de service	de -15 °C à +55 °C
Humidité relative de l'air	5 à 95 %
Interfaces	RS232, LAN, USB-A, USB-C, CAN*
Radio	Bluetooth LE

* Prévu pour les applications futures

** L'alimentation est fournie directement via l'opérateur de porte ou via l'interface USB-C et une alimentation USB.

*** La liste des appareils partagés peut être téléchargée ici : https://dormakaba.com/connector-one

2.2 Batterie au lithium

L'appareil contient 1 batterie au lithium de type CR1220 comme pile de secours.

La batterie ne nécessite aucun service ni entretien. La durabilité de la batterie est prévue jusqu'à la fin de son cycle de vie.

Respecter les consignes de sécurité pour le transport des appareils équipés d'une batterie au lithium.

2.3 Conformité

2.3.1 Déclaration de conformité UE

Ce chapitre est un extrait de la déclaration de conformité complète.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Allemagne

déclare par la présente que le produit décrit est conforme aux dispositions de la ou des directive(s) énumérées et que les normes et/ou spécifications techniques mentionnées ci-dessous ont été appliquées.

Directives communautaires :

2014/53/EU	Équipements radioélectriques
2011/65/EU	RoHS

La documentation technique est disponible auprès du Manager Productcompliance à l'adresse suivante : product-compliance.dach@dormakaba.com

Norme européenne normalisée, règlement national :

EN 301 489-1 V2.2.3:2019

EN 301 489-3 V2.1.1:2019

EN 62368-1:2014+AC:2015

EN IEC 63000:2018

EN 62479:2010

2.3.2 Déclaration de conformité UKCA

Ce chapitre n'est qu'un extrait de la déclaration de conformité complète.

dormakaba Deutschland GmbH
DORMA Platz 1
58256 Ennepetal
Allemagne

déclare par la présente que le produit décrit est conforme aux dispositions de la ou des directive(s) énumérées et que les normes et/ou spécifications techniques mentionnées ci-dessous ont été appliquées.

Directives communautaires :

Règlements d'équipement radio 2017

RoHS, La limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques de 2012

La documentation technique est disponible auprès du Manager Productcompliance à l'adresse suivante : product-compliance.dach@dormakaba.com

Norme européenne normalisée, règlement national :

EN 301 489-1 V2.2.3:2019

EN 301 489-3 V2.1.1:2019

EN 62368-1:2014+AC:2015

EN IEC 63000:2018

EN 62479:2010

2.3.3 FCC & IC

FCC Le produit répond aux exigences de :

- **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 Le produit répond aux exigences de :

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

2.4 Codes LED

État	Couleur	Mode
Démarrage du système	jaune	clignotement lent
configuration requise	jaune	mise en place permanente
prêt à l'emploi, une commande de porte a été détectée	vert	mise en place permanente
prêt à l'emploi, une commande de porte n'a pas été reconnue	vert	clignotement lent
Erreur	rouge	mise en place permanente
Mode de service ou connexion Bluetooth activé(e)	bleu	mise en place permanente
Mode de service activé ou identification de l'appareil activée	bleu	clignotement lent
transmission des données/mise à jour logicielle	cyan	clignotement rapide

2.5 Opérateurs de portes et systèmes de portes supportés

Produits avec protocole 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

Produits avec protocole Datalink issus de l'ETS22

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

Produits avec le protocole portatif issus du contrôleur ESA2

ESA 100
ESA 200
ESA 300
ESA 400
ESA 500

Produits avec le protocole EL

EL 301	AL 501
AL 401	AL 1001

Pour ces actionneurs de porte, un convertisseur RS485/RS232 (élément n° 29262009) est nécessaire pour permettre la connexion au Connecteur Un G2.

2.6 Points de données OPC UA & mises à jour logiciel

Le modèle d'information et le logiciel connecteur One G2 étant en constante évolution et en ajoutant d'autres appareils et fonctionnalités, les mises à jour du logiciel et les tableaux de points de données OPC UA peuvent être consultés sur les entraînements spécifiques en ligne sur le portail my.dormakaba.
Pour ce faire, une inscription gratuite unique est nécessaire à l'adresse :
https://portal.dormakaba.com/registration
Une fois connecté, les données du Connector One G2 sont accessibles à l'adresse suivante :
https://dormakaba.com/connector-one

3 Mise en service

3.1 Conditions de la mise en service

Appareils TMS
Configurer l'interface RS232 du contrôleur d'opérateur en mode TMS.

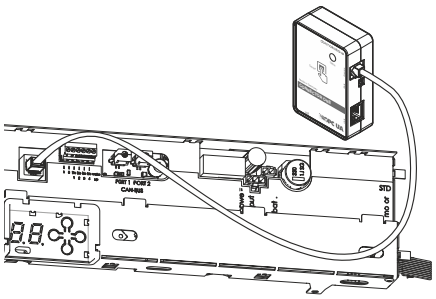
ETS22
Une interface RS232 est disponible.

Entraînements EL
Un convertisseur RS485/RS232 est disponible.

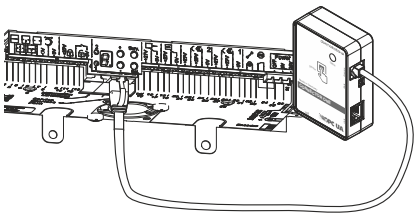
3.2 Raccorder le Connector One G2

Raccorder le Connector One G2 à l'unité de commande via l'interface RS 232.

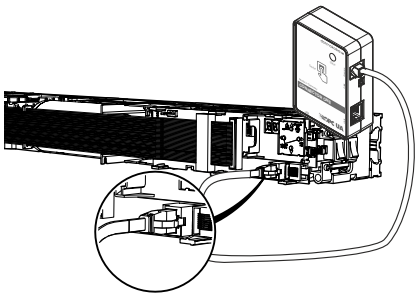
Connexion à l'ES PROLINE



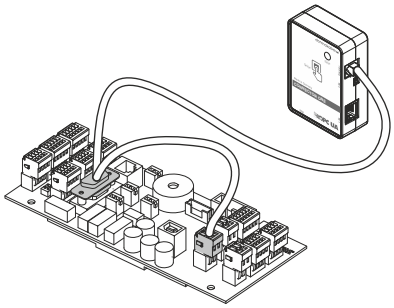
Raccordement à l'ES 200



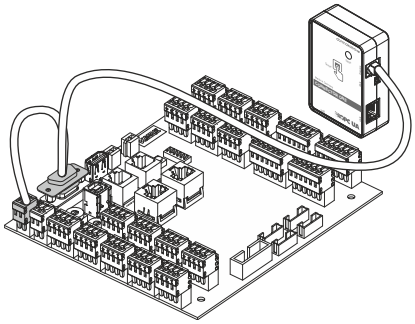
Connexion à l'ED 100, ED 250



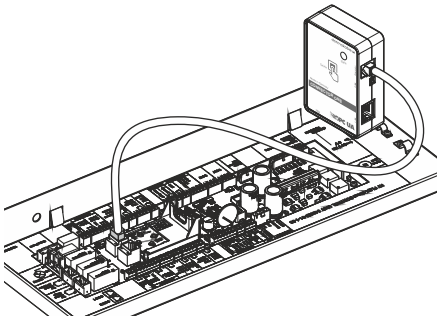
Raccordement à l'ETS22



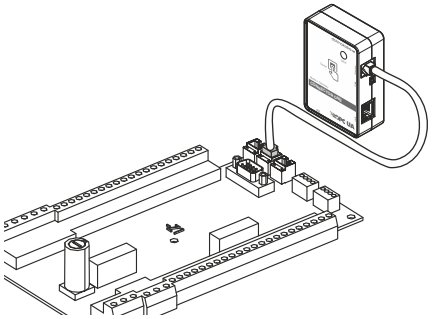
Connexion avec l'ETS22sc2



Raccordement à une KTV



Connexion à une KTC 2 III



3.3 Mettre en service le Connector One G2 avec un système de Smart Building

1. Connecter le Connector One G2 à un ordinateur à l'aide d'un câble LAN ou à un smartphone/tablette à l'aide d'un adaptateur Ethernet pour appareils intelligents.
   - ⇨ La LED d'état clignote en jaune. Le clignotement indique l'opération de démarrage.
   - ⇨ Une fois le processus de démarrage terminé, la LED change de couleur et, le cas échéant, son type de clignotement.
2. Appuyer sur la touche Service pour démarrer le mode Service.
   - ⇨ Après quelques secondes, le voyant d'état clignote en bleu.
   - ⇨ Si la LED s'allume en permanence bleue, le mode Service est activé.
   - ⇨ Si aucune connexion au Connector One G2 n'est effectuée, le mode Service s'arrête automatiquement après 1 minute.
   - ⇨ Si le paramètre réseau du PC est réglé sur « Obtenir l'adresse IP automatiquement » (par défaut), le Connector One G2 attribue automatiquement une adresse IP à l'ordinateur connecté ou à l'appareil intelligent. Si cela n'est pas souhaité, vous devez préconfigurer les paramètres réseau appropriés sur l'ordinateur ou sur le Smart-Device.
3. Veuillez vous rendre sur l'adresse http://192.168.10.4 dans le navigateur. Les navigateurs Web habituels comme Chrome, Firefox, Opera et Safari sont pris en charge.
4. Configurez un mot de passe à 12 chiffres.
   - ⇨ Le menu de connexion s'affiche.

5. Saisir le mot de passe défini précédemment.
6. Sélectionner la langue d'affichage.
7. En cliquant sur Confirmer l'inscription.
   - ⇨ Si l'inactivité est supérieure à 5 minutes, l'utilisateur se déconnecte automatiquement et redémarre le système.
8. Mettre à jour la date, l'heure et le fuseau horaire dans le menu Système.
9. Effacer le certificat du serveur dans le menu « OPC UA ».

En cas de perte du mot de passe, le Connector One G2 peut être réinitialisé aux paramètres d'usine dans le menu de connexion. Tous les paramètres personnalisés sont alors supprimés. Le Connector One G2 se trouve à l'état de livraison, le dernier firmware étant conservé.

3.3.1 Configurer le Connector One G2

Lors d'une mise en service avec EntriWorX, la configuration du Connector One G2 ne doit pas être modifiée.

3.3.1.1 Configurer le LAN

Dans « Réseau », régler les paramètres requis et les appliquer à l'aide de la fonction « Sauvegarder ».

3.3.1.2 Configurer le WLAN

Dans « WLAN », régler les paramètres requis et les appliquer à l'aide de la fonction « Sauvegarder ».

Paramètres WiFi	
Utilisation du WiFi	Ce paramètre doit être activé lors de l'utilisation du WiFi.
Utiliser le réseau de secours	Cela permet d'utiliser un réseau de secours qui s'active automatiquement si le réseau principal est hors service ou indisponible. Il sert de connexion de secours pour maintenir la communication ou la transmission de données.

Il n'est pas possible de configurer et stocker les réseaux en même temps. Après configuration, un réseau (principal ou réseau de secours) doit être sauvegardé. Sinon, les entrées seront perdues lors du changement de réseau.

network (réseau)	
Identifiant	Vous pouvez ainsi attribuer un nom distinct au réseau WLAN.

Sécurité	
Type de sécurité	Ici, vous pouvez choisir entre WPA2 Personal et WPA2 Enterprise. WPA2 Personal utilise un mot de passe Wi-Fi commun pour tous les appareils du réseau. Avec WPA2-Enterprise, la connexion basée sur l'utilisateur se fait via un serveur pour authentifier individuellement les utilisateurs ou les appareils.
Clés	C'est là que le mot de passe commun utilisé dans le réseau pour se connecter au Wi-Fi est saisi.
Protocole d'authentification	EAP-TLS EAP-TLS offre le plus haut niveau de sécurité car le client et le serveur utilisent tous deux des certificats pour l'authentification mutuelle. Cette méthode est particulièrement adaptée aux environnements disposant d'une infrastructure de certificats existante. EAP-PEAP (avec MSCHAPv2) EAP-PEAP établit d'abord un tunnel TLS chiffré vers le serveur. Dans ce tunnel, la connexion se fait par nom d'utilisateur et mot de passe. Cette méthode allie une bonne sécurité à une aisance de gestion. EAP-MD5 EAP-MD5 est une procédure simple basée sur un mot de passe qui ne vérifie que le nom d'utilisateur et un mot de passe haché. C'est facile à configurer, mais il offre un faible niveau de sécurité, donc il n'est recommandé que pour les applications non critiques.
Méthode d'authentification	MSCHAPv2 est une méthode d'authentification électronique souvent utilisée en combinaison avec EAP-PEAP dans les réseaux d'entreprise WPA2. L'utilisateur se connecte avec son nom d'utilisateur et son mot de passe personnels. La vérification effective du mot de passe est effectuée via une méthode de défi-réponse au sein d'un tunnel PEAP chiffré, qui protège les données d'accès.
Identité	Ici est saisie l'identité d'un utilisateur, par exemple un e-mail.
Identité anonyme	L'identité anonyme est un nom d'utilisateur optionnel qui est envoyé au serveur lors de l'établissement du tunnel PEAP. Elle sert à protéger l'identifiant utilisateur réel. Si aucune identité anonyme n'est définie, l'identité utilisateur normale est automatiquement utilisée.
Mot de passe	Le mot de passe de l'utilisateur correspondant est saisi ici.
Certificat d'AC serveur	Un certificat de CA serveur est un certificat délivré par une autorité de certification de confiance qui confirme l'identité du serveur. Il est nécessaire pour que les clients puissent vérifier en toute sécurité la connexion au serveur et établir une communication chiffrée.
Certificats de serveur / « Télécharger le certificat »	Transmission manuelle des certificats du serveur.

Certificats de serveur / « Supprimer »	Les certificats existants peuvent être supprimés manuellement.
« Sauvegarder »	Ceci permet d'appliquer tous les paramètres.

3.3.1.3 Configuration de l'OPC UA

Dans « OPC UA », définissez les paramètres qui régissent l'accès au serveur OPC UA.

- Port IP du serveur OPC UA
- Protocole RS232 de la commande de porte connectée (voir annexe)
- Méthode d'authentification
- Verrouillage des données

Paramètres du serveur	
Port serveur	Vous pouvez définir ici le port TCP/IP par lequel le Connector One G2 doit être accessible. Le port par défaut pour OPC UA est 4840.
Protocole de pilote de porte	Selon le contrôle de la porte, il faut choisir entre différents protocoles. Les informations relatives au protocole figurent dans la documentation correspondante.

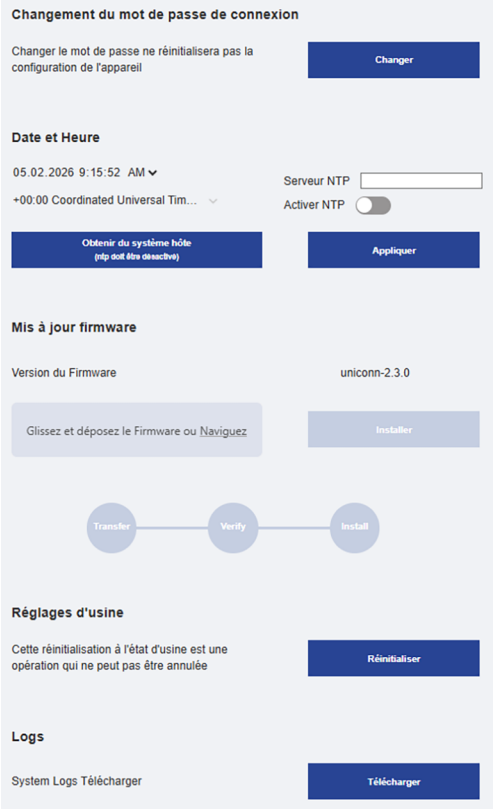
Authentification	
Mot de passe d'authentification et utilisateur	L'utilisation d'un nom d'utilisateur et d'un mot de passe est une caractéristique de sécurité OPC UA. Le nom d'utilisateur et le mot de passe permettent au client OPC UA de se connecter au Connector One G2 (serveur OPC UA). Les données saisies ici doivent être utilisées dans le client OPC UA pour accéder au Connector One G2.
Certificats client d'authentification	Les certificats client sont une caractéristique de sécurité OPC UA. Avec un certificat client, un système s'authentifiera sur le Connector One G2. Plusieurs certificats peuvent être déposés à la

	fois. Les certificats peuvent être transférés à l'avance au Connector One G2. Il est possible que le Connector One G2 accepte automatiquement le premier certificat qui lui est fourni.
Certificats client <Supprimer>	Supprime les certificats clients existants.
Certificats client <chargement>	Transmission manuelle de certificats clients.
Certificats client / mode Provisioning	Ce n'est pas encore un certificat. Lorsqu'un client ouvre une session avec son certificat, celui-ci est accepté par le Connector One G2. D'autres certificats ne peuvent pas être acceptés automatiquement.

Règles de sécurité	
Directives de sécurité disponibles	Une stratégie de sécurité détermine les mécanismes à utiliser pour le canal sécurisé entre le client et le serveur. La stratégie de sécurité définit les algorithmes de signature et de chiffrement, l'algorithme de dérivation de clé et les longueurs de clé utilisées dans les algorithmes. L'une des règles suivantes doit être sélectionnée. Plusieurs règles sont possibles à la fois. • None • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Pour plus d'informations sur les règles de sécurité, voir: https://profiles.opcfoundation.org/profilefolder/474
Modes de sécurité disponibles	Le mode Sécurité détermine les niveaux de sécurité généraux offerts par le Connector One G2 à un client qui peut s'appliquer aux messages. Cela dépend également des capacités du client. • None Tous les messages ne sont ni signés ni cryptés. • Sign Tous les messages sont signés, mais ils ne sont pas cryptés. • Sign & encrypt Tous les messages sont signés et cryptés.
Certificats de serveur	Avec un certificat serveur, le Connector One G2 (serveur OPC UA) s'authentifiera auprès d'un client. Il peut être créé automatiquement ou utiliser un certificat existant. Lors du premier démarrage, un certificat serveur OPC UA est automatiquement généré. Ce certificat de serveur doit être supprimé manuellement après avoir modifié le nom d'hôte ou la date, afin de créer un nouveau certificat au prochain démarrage.
Certificats de serveur / « Télécharger le certificat »	Transmission manuelle des certificats du serveur.
Certificats de serveur / « Télécharger la clé »	Transmission manuelle de la clé correspondant au certificat du serveur.
Certificats de serveur / « Supprimer »	Les certificats existants peuvent être supprimés manuellement.
« Sauvegarder »	Ceci permet d'appliquer tous les paramètres.

3.3.1.4 Configuration du système

Dans <System>, les informations et les paramètres sont affichés et peuvent être modifiés.



Authentification	
Modifier le mot de passe	Vous pouvez modifier le mot de passe ici.
Modifier la date et l'heure	Pour utiliser le Connector One G2, vous devez disposer d'une heure correcte. Il est donc recommandé d'utiliser un serveur NTP. Si cela n'est pas possible, l'heure peut aussi être réglée manuellement. • L'horloge du Connector One G2 est rechargeable. Après une coupure d'électricité, le temps ne doit pas être réajusté. • La date définie manuellement est enregistrée dans un fichier sur l'appareil et récupérée au prochain démarrage. Si l'appareil n'est pas utilisé pendant une longue période après avoir réglé l'heure, la date ou l'utilisation d'un serveur NTP doivent être mises à jour.
Activer NTP	Si NTP est activé, le Connector One G2 synchronise son temps avec un serveur NTP. Le serveur NTP est entré dans le paramètre réseau. Si la fonction est activée, la configuration manuelle du temps n'est pas possible.
Réglage manuel de l'heure	En cliquant sur l'heure et le fuseau horaire, vous pouvez saisir manuellement l'heure actuelle.
Récupérer l'heure du système hôte	Pour faciliter la configuration manuelle du temps, vous pouvez charger l'heure actuelle et le fuseau horaire du système hôte.
Modifier la date et l'heure	L'heure et le fuseau horaire affichés sont pris en charge par le Connector One G2.
Mettre à jour le firmware	Cette fonctionnalité permet d'installer un nouveau firmware. La dernière version s'affiche.
Ajouter ou rechercher un nouveau firmware par glisser-déposer	Il s'agit d'un nouveau fichier de firmware envoyé au Connector One G2.
Installation	Après avoir transféré un firmware, l'installation peut être effectuée.
Réinitialisation aux paramètres d'usine	Un Connector One G2 peut être réinitialisé à ses paramètres d'usine. L'appareil se trouve alors en état de livraison, la dernière version du micrologiciel est conservée.

3.4 Mettre en service le Connector One G2 avec EntriWorX

1. La LED d'état clignote en jaune. Le clignotement indique le processus de démarrage.
   ⇨ À la fin du processus de démarrage, la LED change de couleur et éventuellement de comportement de clignotement, voir Codes LED [▶ 2.4].

3.4.1 Conditions préalables

- Un projet client a été créé dans EntriWorX Planner.
- Un lot de travaux contenant la porte à installer a été attribué à un installateur.
- L'invitation par e-mail pour le technicien a été acceptée.

3.4.2 EntriWorX Planner

1. Placer une porte sur le plan.
2. Sélectionner un modèle avec le protocole souhaité (TMS, Datalink, Handheld) et le placer.
3. Attribuer un Connector One G2 à la porte.
4. Définir les paramètres du réseau et du Wifi.
5. Définir les paramètres OPC UA.
6. Créer un nouveau lot de travaux (commissioning) et ajouter la porte.
7. Attribuer le lot de travaux au technicien.

⇨ Avec l'attribution du lot de travaux, le technicien reçoit une invitation par e-mail.

⇨ Le technicien doit accepter l'invitation afin d'obtenir les droits de mise en service dans l'application EntriWorX Setup App.

Notes sur les réglages réseau et WiFi

- Pour utiliser WPA2-Enterprise afin d'accéder au WiFi d'entreprise, la connexion doit d'abord être configurée dans l'interface web du Connector On G2 avec les données de certificat et d'accès. La connexion peut alors être sélectionnée dans l'application de configuration.
- Le modem LTE est automatiquement détecté par le Connector One G2 et affiché dans l'application de configuration.

3.4.3 EntriWorX Setup App

1. Se connecter à l'application avec un e-mail et un mot de passe et sélectionner le marché.
2. Choisir le bâtiment et la porte.
   ⇨ La LED du connecteur passe au bleu et indique une connexion Bluetooth à l'application EntriWorX Setup App.
3. Démarrer la mise en service avec les paramètres réseau.
   ⇨ Le modem LTE est automatiquement détecté par le Connector One G2 et affiché dans l'application EntriWorX Setup.
4. Transférer la configuration du EntriWorX Planner vers le Connector One G2.
   ⇨ La connexion Bluetooth est interrompue et la porte est en marche.
5. Transmettre les paramètres OPC UA.

Notes sur les réglages réseau et WiFi

- Le LAN et le WiFi (personnel WPA2) peuvent être prédéfinis dans le Planner et transférés vers l'application de configuration EntriWorx.
- Dans l'application EntriWorx Setup, le WiFi d'entreprise prédéfini peut être sélectionné via l'option « WiFi local setup ».
- Le modem LTE est automatiquement détecté par le Connector One G2 et affiché dans l'application EntriWorx Setup.

Paramètres du serveur	
Port TCP	Indique le port TCP/IP par lequel il est possible d'accéder à Connector One G2. Le port par défaut pour OPC UA est 4840.

Stratégie de sécurité	
Directives de sécurité disponibles	Une stratégie de sécurité détermine les mécanismes à utiliser pour le canal sécurisé entre client et serveur. La stratégie de sécurité définit les algorithmes pour la signature et le chiffrement, l'algorithme de dérivation de clé et les longueurs de clé utilisées dans les algorithmes. Les directives suivantes sont disponibles (plusieurs choix possibles) : • Aucun • Basic256Sha256 • Aes128_Sha256_RsaOaep • Aes256-Sha256-RsaPss Pour plus d'informations sur les règles de sécurité, voir : https://profiles.opcfoundation.org/profilefolder/474
Mode de sécurité	
Modes de sécurité disponibles	Le mode de sécurité indique les niveaux de sécurité généraux qui peuvent être appliqués aux messages. Le Connector One G2 propose les modes de sécurité suivants : (plusieurs choix possibles) : • Aucun Tous les messages ne sont pas signés ni cryptés. • Signer Tous les messages sont signés, mais ils ne sont pas cryptés. • Signer et crypter Tous les messages sont signés et cryptés. Le mode de sécurité dépend également des capacités du client OPC UA.

Authentification	
Authentification, mot de passe et utilisateur	L'utilisation d'un nom d'utilisateur et d'un mot de passe est une fonction de sécurité OPC UA. Le nom d'utilisateur et le mot de passe sont utilisés pour permettre au client OPC UA de se connecter à Connector One G2 (serveur OPC UA). Les données saisies ici doivent être utilisées dans le client OPC UA pour accéder au Connector One G2.

1. Pour terminer le processus, cliquer sur « Enregistrer ».

3.5 Connexion et configuration du client OPC UA

Conditions préalables

- Le Connector One G2 est prêt à l'emploi.

  => La LED de statut s'allume ou clignote en vert.
- Le Connector One G2 est correctement connecté au réseau.

Établir la connexion

1. Entrez l'URL endpoint ci-dessous dans le navigateur.
   opcp://[adresse IP Connector One G2] :[port du serveur]
   Exemple : opc.tcp://192.168.1.20:4840

Configurer le client OPC UA

1. Définir les règles de sécurité en conformité avec les règles du Connector One G2.
2. Sélectionner la méthode d'authentification correspondant au réglage dans le Connector One G2.

Si des certificats sont utilisés, ceux-ci doivent être remplacés à l'avance si nécessaire.

3. Établir la connexion.

4 Montage

AVIS

Dommages matériels dus à une collision

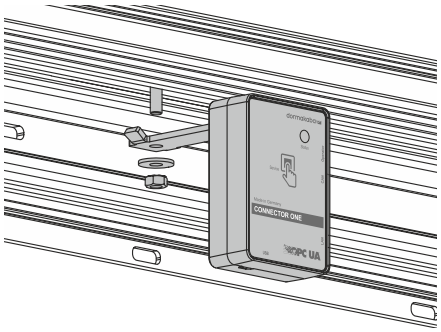
En cas de collision avec des pièces mobiles, le Connector One G2 et/ou les câbles peuvent s'endommager.

- Monter le Connector One G2 de manière à ce qu'il ne puisse pas entrer en collision avec des pièces mobiles.
- Insérer/ranger tous les câbles situés à l'intérieur de l'opérateur dans les chemins de câbles existants ou les fixer avec un support de câble,

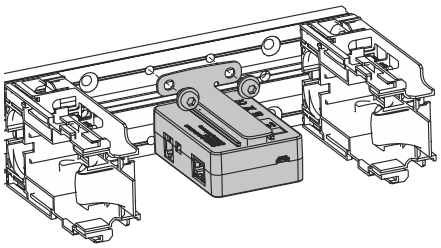
---

Une fois la configuration complète terminée, le Connector One G2 est monté dans l'opérateur de porte.
Différents matériaux de montage sont disponibles en fonction de l'opérateur de porte.

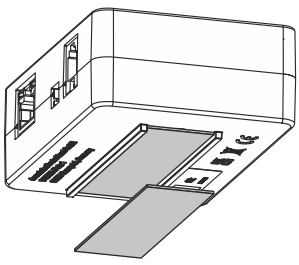
Monter dans l'ES PROLINE
Dans l'ES PROLINE, le Connector One G2 est monté à l'aide de l'équerre de fixation fournie dans l'opérateur.



Monter l'ED 250 dans l'ED 100
Dans l'ED 100, l'ED 250 est monté au Connector One G2 à l'aide de l'équerre de montage fournie et de l'insert ED dans l'opérateur.



Monter dans d'autres opérateurs
Pour un montage sans équerre de fixation, le Connector One G2 est fixé à un emplacement approprié à l'aide de la bande Velcro.



5 Élimination des pannes

Erreur	Solution
Le certificat serveur OPC UA a expiré.	Mode Service : Vérifier la date/l'heure dans le menu <System> et, le cas échéant, la corriger. Puis, dans le <menu> OPC UA, supprimer le certificat serveur. Ensuite, redémarrez le Connector One G2. Après le redémarrage, un nouveau certificat est automatiquement généré. Ce certificat est valable 4 ans à partir de sa création.
Impossible d'accéder au site Web des services.	Vérifiez que l'URL du navigateur est correcte. http://192.168.10.4 Le cas échéant, effacer le cache du navigateur et recharger la page.
L'erreur «BadUserIdentity » s'affiche dans le client OPC UA.	Vérifier l'authentification en mode Service et, le cas échéant, ajuster.
Pour les appareils TMS, le commutateur de programme ne peut pas être modifié via OPC UA.	Si nécessaire, à l'aide des instructions d'opérateur, assurez-vous que le commutateur de programme peut être modifié de l'extérieur (configuration de l'opérateur). Pour les commandes des issues de secours, un micrologiciel d'opérateur spécial (par exemple ES 200 2D ou FFT) est nécessaire car la loi interdit la manipulation à distance du commutateur de programme. Pour ce faire, contactez les services dormakaba.
Aucune connexion n'est établie sur le dispositif TMS.	Assurez-vous que l'interface RS 232 est configurée en mode TMS (voir instructions d'utilisation de l'opérateur correspondant).
Aucune connexion n'est établie lors de l'entraînement avec le protocole portable.	Assurez-vous que l'interface RS 232 est configurée en mode portable (voir instructions d'utilisation de l'opérateur correspondant).
Après une mise à jour du micrologiciel, il n'est plus possible d'accéder au Connector One G2.	Réinitialiser le Connector One G2 aux paramètres d'usine, voir Mettre en service le Connector One G2 avec un système de Smart Building [▶ 3.3].

6 Démontage et mise au rebut

Le démontage s'effectue dans l'ordre inverse du montage et doit être réalisé par du personnel qualifié.

Le produit ne doit pas être mis au rebut avec les ordures ménagères. Éliminez le produit de façon respectueuse de l'environnement, dans les centres de réception et de collecte prévus à cet effet. Respecter les réglementations nationales en vigueur applicables dans votre cas.

Notes

www.dormakaba.com

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

www.dormakaba.com