

REMOTE MONITORING OPTIONS FOR ABB DRIVES

# EGW-02 Connectivity Edge Gateway

## Cyber security guide





# EGW-02 Connectivity Edge Gateway

## Cyber security guide

[Table of contents](#)





# Table of contents

---

## 1 Introduction to the document

Applicability.....	7
Target audience.....	7
Personnel definitions.....	7
IEC 62443-4-1 security guidelines.....	8
Terms and abbreviations.....	8
Related documents.....	9

## 2 ABB approach to cyber security

Cyber security of the drive system.....	11
Device Security Assurance Center (DSAC).....	11
Suppliers.....	11

## 3 Cyber security in the EGW-02 gateway

Access credentials.....	13
EGW-02 gateway connectivity.....	14
Network connection example.....	14
Communication interfaces.....	15
Wired interfaces.....	15
Wireless interfaces.....	15
Communication protocols.....	15
Vulnerability handling.....	16
Cyber security disclaimer.....	16

## 4 Security guidelines

Product defense in depth (SG-1).....	17
Defense in depth measures expected in the environment (SG-2).....	18
Before the installation.....	18
Installation of the gateway.....	18
Physical security.....	19
After the installation.....	19
Installation checklist for the installer ( <b>Authorized Person</b> or <b>End User</b> with a JWT from an <b>Authorized Person</b> ):.....	19
Installation checklist for the <b>End User</b> :.....	19
Installation checklist for the <b>Authorized Person</b> :.....	20
Installation checklist for the <b>Asset Owner</b> :.....	20
Security hardening guidelines (SG-3).....	20
Security capabilities.....	20
Periodic security maintenance activities.....	20
Troubleshooting package and reporting security incidents to ABB.....	21
Secure disposal guidelines (SG-4) .....	22
Secure operation guidelines (SG-5).....	23
Account management (SG-6) .....	23
Documentation review (SG-7).....	23

---



**5 Additional features**

Network diagram.....	25
Modbus TCP.....	25
OPC UA server.....	26
OPC UA client.....	26
PC Tool mode.....	26

**Further information**



# 1

## Introduction to the document

---

This is the cyber security guide for the EGW-02 Connectivity Edge Gateway with information on the installation, use, service, and decommissioning of the product throughout its service life.

This document refers to the product as the EGW-02 gateway or gateway.

### Applicability

This manual applies to the EGW-02 Connectivity Edge Gateway with firmware version 1.3.\*.

### Target audience

This document is intended for persons responsible for the cyber security of the EGW-02 gateway.

#### ■ Personnel definitions

In this document, we use these entities.

Entity	Role/definition
<b>Asset Owner</b>	A person or organization that owns or is responsible for one or more products or systems.
<b>Authorized Person</b>	A person authorized to access and control the security policies and capabilities of the product or system.
<b>End User</b>	An end user of the product or system.

---

## IEC 62443-4-1 security guidelines

IEC 62443 is an international series of standards that address cyber security for operational technology in automation and control systems.

This document is based on the security guidelines of the IEC 62443-4-1 standard.

For more information, refer to

<https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.

## Terms and abbreviations

Term	Description
CIAM	Customer Identity and Access Management. Another name for DMS.
CMD	ABB Ability™ Condition Monitoring for drives. CMD is a cloud service to remotely store, monitor, and analyse drive data. It is also a part of the ABB Ability™ Digital Powertrain offering.
DDCS	Distributed Drive Communication System. Optical fiber-based industrial protocol.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks to automatically assign IP addresses to network devices in a client-server architecture.
DMS	Device Management System
eSIM	Digital SIM embedded in the gateway for mobile network data connection
HTTP(S)	Hypertext Transfer Protocol (secure variant)
JWT	JSON Web Token
LAN	Local Area Network
LTE	Long-Term Evolution. A standard for wireless broadband communication that is typically referred to as 4G.
Modbus	Industrial client/server communications protocol. Refer to <a href="https://modbus.org/">https://modbus.org/</a> .
OPC UA	OPC Unified Architecture. Refer to <a href="https://opcfoundation.org/about/opc-technologies/opc-ua/">https://opcfoundation.org/about/opc-technologies/opc-ua/</a> .
PGP	Pretty Good Privacy. A set of tools for secure communication.
PLC	Programmable Logic Controller
SG	Security Guideline (requirements according to IEC 62443-4-1)
TCP	Transmission Control Protocol. One of the primary Internet protocols.
TLS	Transport Layer Security, secure communications protocol
TPM 2	Trusted Platform Module. A hardware-backed secure information enclave.
USB	Universal Serial Bus. A communication standard to interconnect equipment such as computers, mobile devices, and peripheral devices.
WAN	Wide Area Network

## Related documents

These documents are related to the product. For more documentation, go to [www.abb.com/drives/documents](http://www.abb.com/drives/documents).

Document	Code (English)
EGW-02 Connectivity Edge Gateway user's manual	<a href="#">3AXD50000929719</a>
EGW-02 Connectivity Edge Gateway quick installation guide	<a href="#">3AXD50001069537</a>
EGW-02 Connectivity Edge Gateway cyber security guide	<a href="#">3AXD50001061845</a>
EGW-02 Connectivity Edge Gateway recycling instructions and environmental information	<a href="#">3AXD50001069544</a>
Bluetooth antenna kit installation guide	<a href="#">3AXD50001141370</a>
GSM (LTE) antenna kit installation guide	<a href="#">3AXD50001141387</a>

---





## ABB approach to cyber security

---

This is information on the ABB approach to cyber security. For more information, go to <https://global.abb/group/en/technology/cyber-security>.

### Cyber security of the drive system

Refer to [Cyber Security for ABB Drives White Paper \(3AXD10000492137 \[English\]\)](#) for the cyber security of the drive system.

### Device Security Assurance Center (DSAC)

In 2009, ABB established the Device Security Assurance Center (DSAC) to improve product quality by testing.

The DSAC Cyber Security Test Process is [certified by exida](#) for IEC 62443 Part 4-1: 2018 Secure product development lifecycle requirements.

For information on DSAC, refer to [DSAC White Paper](#).

### Suppliers

Refer to [ABB Cyber Security Requirements for Suppliers](#).

---





## Cyber security in the EGW-02 gateway

---

Information on the EGW-02 gateway from a cyber security perspective.

### Access credentials

An **Authorized Person** can access the ABB Device Management System (DMS) to do actions such as examine the gateway status, update the gateway, and make an access token (JWT) for the local user interface of the EGW-02 gateway. Access to the DMS is controlled by ABB, and the credentials are available only from ABB.

An **Authorized Person** who has an access token from the DMS, or an **End User** who has a JWT from an **Authorized Person** can access the local user interface of the EGW-02 gateway. The local user interface permits the person with access to change the network configuration, see the status of connected drives, and secure drive connections with an x.509 certificate.

The local user interface is available only through the local network, and only with an access token (JWT) from the ABB DMS.

For information on the local user interface, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

An **End User** or **Asset Owner** can have access to the ABB Condition Monitoring for Drives cloud functionality. This is a part of the ABB Ability™ Digital Powertrain offering (CMD/Powertrain). This service permits the user to see telemetry data and historical telemetry data, and to set notifications and alerts, for example, for drive disconnects.

For information on Modbus and OPC UA connectivity and security, refer to [Additional features \(page 25\)](#).

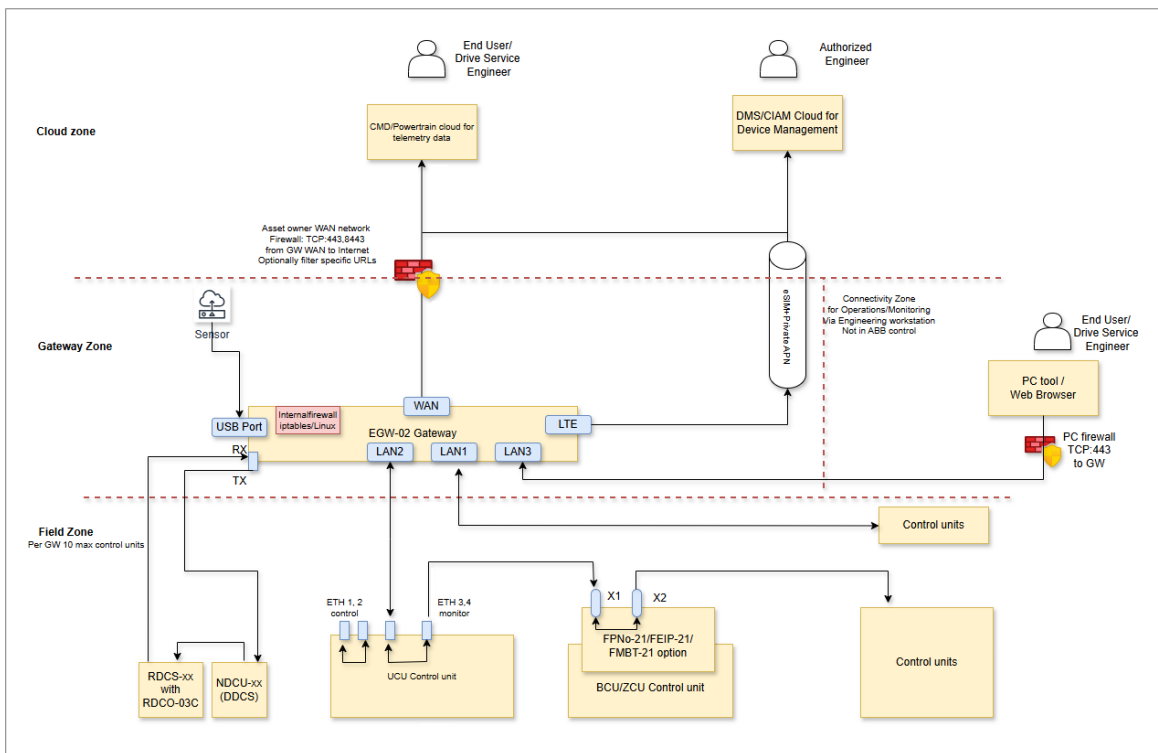
---

## EGW-02 gateway connectivity

The EGW-02 gateway can be connected to:

- ABB drives for monitoring
- ABB Device Management System
- ABB Condition Monitoring for drives (over the Internet)
- A PLC through the Modbus server for protocol translation to drives
- A PC with a suitable tool through the OPC UA server for protocol translation to drives
- A PC with Drive Composer or other software application
- USB-connected environmental sensors to monitor temperature, humidity, and air pressure

## Network connection example



## Communication interfaces

### ■ Wired interfaces

- Ethernet connectors:
  - RJ45 WAN connector for wired Internet connection (external network)
  - RJ45 LAN1...LAN3 connectors for wired local area connection (internal network for drives, service access, and internal tools)
- USB Type A connector for external USB-connected environmental sensors (Yocto-Meteo-V2)
- RS-485 connector for the panel bus (currently not in use)
- Fiber-optic connectors (DDCS) for an alternative drive network connection

### ■ Wireless interfaces

- LTE antennas for mobile Internet connection (requires activated eSIM). Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).
- Bluetooth antenna for Bluetooth connections (currently not in use)

## Communication protocols

If your firewall requires a full list of cloud endpoints, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

The EGW-02 gateway uses these protocols:

- External connections to the Internet (WAN, LTE)
    - The gateway connects to cloud servers on the Internet through TCP 443 and 8443 ports over a secure TLS connection.
    - No other external connections to the WAN port. No listening ports.
    - No configuration access to the local user interface over WAN or LTE.
  - Internal: LAN1...LAN3 Ethernet connections
    - TCP 443 port to access the local user interface (HTTPS server).
    - TCP 80/443 outbound port to monitor local Ethernet-connected drives.
    - UDP 24576 port to discover monitorable drive control units on the LAN.
    - TCP 502 listening port (disabled by default) for the Modbus TCP server.
    - TCP 4840 listening port for the OPC UA server (when it is enabled in the local user interface).
    - TCP 4840 outbound port to monitored drives through the OPC UA client.
  - Industrial (through LAN ports)
    - Ethernet connection to drive control units
    - Modbus TCP server
    - OPC UA server and client
  - Physical:
    - Fiber-optic connection (DDCS) to drive control units
    - USB connection to Yocto-Meteo-V2 sensors for environmental measurements
-

## Vulnerability handling

ABB products have advanced security features to prevent cyber security threats. These include, but are not limited to:

- Secure communication protocols
- Encryption mechanisms
- Access control mechanisms to limit and monitor user access

ABB supplies firmware updates and security patches to address vulnerabilities and maintain a secure environment.

The **Asset Owner** prepares a policy to schedule the updates and agrees with ABB to receive information on the available updates.

An **Authorized Person** applies the updates manually through the ABB Device Management System.

For more information, refer to [ABB's approach to Software Vulnerability Handling \(9ADB005059 \[English\]\)](#).

To report a cyber security vulnerability, contact us at [cybersecurity@ch.abb.com](mailto:cybersecurity@ch.abb.com).

For secured reporting, use the PGP key in [ABB Product Security Incident Response Team - PGP Key \(9AKK107991A5089 \[English\]\)](#).

## Cyber security disclaimer

This product is designed to be connected to and to communicate information and data via a network interface. It is Customer's sole responsibility to provide and continuously ensure a secure connection between the product and Customer network or any other network (as the case may be). Customer shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

---



## Security guidelines

---

These are the security guidelines of the EGW-02 gateway.

### Product defense in depth (SG-1)

The cyber security capabilities of the EGW-02 gateway:

- Certificate-based authentication for communication
  - Modern encryption algorithms (TLS/mTLS) towards the Internet. The key lengths were chosen in conformance with IEC 62443.
  - Communication is two-way authenticated (client and server authenticate individually) using a public key infrastructure and idevID, IEEE 802.1AR.
  - Communication in the local (isolated) network is encrypted and authenticated when legacy communication is not required.
  - Installation and update archives are signed and verified using cryptography.
  - Over-the-air update capability. The gateway can be remotely updated through the ABB Device Management System (DMS)
  - Secure boot starts from a hardware-backed root of trust.
  - Hardware-backed trusted platform module (TPM2) for critical cryptographic material.
  - Physically separate Ethernet controllers for explicit communication with internal and external entities.
  - Device access is controlled by access layers.
  - Advanced logging capabilities to establish non-repudiation and assist in solving problems and edge cases.
  - Each security component is independent.
-

- Tamper-resistant casing (antitamper sticker on top case seam and type designation label on bottom case seam)
- Only limited devices and device types can connect through USB.
- For some industrial protocols, there is additional connection protection with IP filtering.

## Defense in depth measures expected in the environment (SG-2)

### ■ Before the installation

The **Asset Owner** prepares the items and information that follow:

- The external network connectivity information (for example, the required proxies and IP settings).
- The X.509 cryptographic certificates to secure drive connectivity. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#). The **Asset Owner** keeps the certificates secure and gives only the public keys of the applicable certificates to the person who installs the EGW-02 gateway.
- The physical installation location of the EGW-02 gateway and the correct wiring. The EGW-02 gateway is typically installed when the drives are not in use, so it may be necessary to schedule downtime and other resources for the installation.
- If USB-connected sensors for environmental measurements are used, the **Asset Owner** communicates this to the **Authorized Person** and **End User**. This is required because sensor installation can occur outside of the cabinet.
- Information on the correct LTE antenna type. For more information, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

The **Asset Owner** makes this information available to the person who installs the EGW-02 gateway:

- **Authorized Person**
- **End User** with a JWT from an **Authorized Person**

The **Asset Owner** prepares policies to make sure that the EGW-02 gateway is in a location with physical access control, such as a locked cabinet.

### ■ Installation of the gateway

---

**NOTICE** Make the communication connections according to the information in [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#). Incorrect connections can cause communication failures and compromise system security.

---

Connect the external network interface (WAN connector) of the EGW-02 gateway only to a trusted external network.

The gateway has an internal firewall. The **Asset Owner** makes sure that there is an external firewall between the EGW-02 gateway and the Internet. The EGW-02 gateway uses only client ports 443 and 8443 towards cloud endpoints, and the EGW-02 gateway does not need to be reached from the Internet. For a list of cloud endpoints, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

---

Connect the drives to the internal network to connectors LAN1...LAN3 of the EGW-02 gateway. These LAN connectors are used for authenticated and authorized service access. The security of the internal network is the responsibility of the **Asset Owner**. Do not connect the internal network to the Internet.

An **Authorized Person** or **End User** with a JWT from an **Authorized Person** uses the local user interface to set:

- External network settings of the EGW-02 gateway (proxy configuration)
- Drive network settings of the EGW-02 gateway

If no proxy is used, minimal configuration is required. If the EGW-02 gateway can reach ports 443 and 8443 over the Internet directly without a proxy through the WAN connection, no configuration is necessary. For the internal network, it may be necessary to decide and configure whether the EGW-02 gateway functions as a DHCP server for the network.

Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

### Physical security

For connections between the EGW-02 gateway and drive control units, such as DDCS optical fiber, and Ethernet to embedded fieldbus and embedded tool Ethernet ports, the **Asset Owner** makes sure that proper physical security is applied. This includes, but is not limited to, physical access control to the drives and cables, locked cabinets, and secure cable conduits.

If the customer does not require specific connections, such as DDCS optical fiber or USB, the connections can be blocked on the EGW-02 gateway with port blockers. The **Asset Owner** makes sure that the use of these port blockers is documented for periodic checking.

### ■ After the installation

#### Installation checklist for the installer (Authorized Person or End User with a JWT from an Authorized Person):

- In the local user interface, all drives are visible.
- In the local user interface, all connections to drives that can and should be secured have the correct secured icon. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).
- In the local user interface, make sure that the settings for Modbus and OPC UA are correct for the environment. Refer to [Additional features \(page 25\)](#).

#### Installation checklist for the End User:

- All of the wiring of the EGW-02 gateway is secure, and the correct networks are connected.
  - If the cloud server connection LED is visible, it is green. The LED is not visible when the EGW-02 gateway is installed in a cabinet that must be closed during operation.
  - If CMD/Powertrain is in use, all of the drives are visible in the portal, and they have secured connections (if applicable).
  - If CMD/Powertrain is in use, SMS/e-mail alerts are defined in the portal so that the **End User** receives a message if a drive is disconnected.
-

If USB environmental monitoring is in use and USB-connected sensors are correctly connected, the blue light indicator on the sensor flashes.

**Installation checklist for the Authorized Person:**

The EGW-02 gateway is visible and online in the ABB Device Management System (DMS).

**Installation checklist for the Asset Owner:**

All of the previous checks are done by the applicable personnel.

## Security hardening guidelines (SG-3)

### ■ Security capabilities

As standard, the system operates in a secure state. For example, cloud communication is possible only after a successful secure boot of the EGW-02 gateway. The secure boot starts from a hardware-backed root of trust. The relevant cryptographic certificates are in a secure enclave.

In the local user interface of the EGW-02 gateway, an **Authorized Person** or **End User** with a JWT from an **Authorized Person** can:

- Enable, disable, and examine the encrypted channels between the EGW-02 gateway and the drives.
- Set a cryptographic certificate to enable the encrypted channels through the local user interface with a local network connection.
- Set the communication settings for the drive network.
- Set the external network settings of the EGW-02 gateway.
- Enable and change the settings of the Modbus interface.
- Enable and change the settings of the OPC UA interface.

For more information, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

**Note:** A change in the network settings can have an effect on the security of the EGW-02 gateway. Other configuration changes do not have an effect on security.

### ■ Periodic security maintenance activities

Do these maintenance tasks periodically, for example, every 6 months. Obey the local service periods and processes.

The **Asset Owner** makes policies to make sure that:

- The **End User** handles SMS or e-mail alerts from the DMS or CMD services.
  - The **End User** can see all of the drives in the CMD cloud service and that they send data, and that the connection to the Powertrain is active in the EGW-02 local user interface.
  - The **End User** makes sure that all of the applicable drives have a secure connection to the CMD cloud service in the local user interface of the EGW-02 gateway.
  - The **End User** makes sure that there are no communication fault indications in the CMD cloud service. If there are communication faults, make sure that the drives do not have faults and that the connection settings are correct.
-

- If it is possible to see the status LEDs, the **End User** makes sure that they show normal operation. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).
- If it is possible to do it safely, the **End User** makes sure that the external network cable and the drive network cable are connected to the correct connectors on the EGW-02 gateway.
- An **Authorized Person** or **End User** with a JWT from an **Authorized Person** examines the status of the connected drives in the local user interface of the EGW-02 gateway.
- The **Asset Owner** has a subscription to cyber security alerts and notifications at <https://global.abb/group/en/technology/cyber-security/alerts-and-notifications>.
- The **Asset Owner** or **End User** examines the storage security of the drive certificates. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).
- The **Authorized Person** makes sure that there are no reports of EGW-02 gateway connectivity-related faults in the ABB Device Management System.
- If USB-connected environmental sensors are in use, the **End User** can make sure from the CMD cloud service that sensor data is transmitted correctly. If it is possible to safely see the USB-connected environmental sensor, the **End User** can also make sure that the blue LED on the sensor flashes.
- If port blockers are used in unused connections, the **End User** makes sure that they are correctly installed.
- For OPC UA and Modbus use, the **Asset Owner** makes sure that the **Authorized Person** knows whether the services should be active on the EGW-02 gateway and makes sure that the settings are correct. Refer to [Additional features \(page 25\)](#).
- If Modbus, OPC UA or PC Tool mode have been in use, and the **Authorized Person** wants to turn telemetry monitoring back on, the **Authorized Person** uses the local user interface and the CMD/Powertrain service to make sure that telemetry monitoring is active and that the CMD/Powertrain service receives data.
- If the LTE connection is in use, the **Authorized Person** examines the LTE connection status and signal strength. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

#### ■ Troubleshooting package and reporting security incidents to ABB

If there are problems, an **Authorized Person** can remotely collect a troubleshooting package.

As the **Asset Owner**:

- Contact ABB for more information.
- Subscribe to cyber security alerts and notifications at <https://global.abb/group/en/technology/cyber-security/alerts-and-notifications>.
- Send an e-mail to [cybersecurity@ch.abb.com](mailto:cybersecurity@ch.abb.com) to report a vulnerability in the ABB offering. Use the **PGP (Pretty Good Privacy) key** for secure reporting.

For more information, refer to [ABB's approach to Software Vulnerability Handling \(9ADB005059 \[English\]\)](#).

---

## Secure disposal guidelines (SG-4)

This section gives instructions for EGW-02 gateway decommissioning. To decommission the drive, refer to the applicable drive documentation.

The **Asset Owner** prepares policies to make sure that the correct person does these tasks to decommission the EGW-02 gateway.

1. Software:

- An **Authorized Person** de-registers the EGW-02 gateway in the ABB Device Management System (DMS). This prevents further telemetry data, logs, and auditable events from being sent, as well as connections from the EGW-02 gateway (if it is not commissioned again).
- The **End User** or an **Authorized Person** does the factory reset of the gateway. This deletes the local telemetry data of the EGW-02 gateway. Refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).  
To make sure that the EGW-02 gateway is on, but is removed from the ABB DMS: Make sure that the EGW-02 gateway is connected to the Internet, the power LED is on, and the green LED is off (no cloud connection). For a full check or if the LEDs are not visible due to security or otherwise, connect to the local user interface.

**Note:** If you do a factory reset before the EGW-02 gateway is de-registered in the DMS, the gateway automatically enables itself again. This is normal.

2. Telemetry data from drives on the EGW-02 gateway:

- No actions are needed. The factory reset deletes the drive telemetry data.

3. Telemetry data from drives in the ABB DMS:

- Decommissioning the EGW-02 gateway does not affect data from the drives in the cloud.
- Discuss data disposal and data retention policies with an **Authorized Person** to be aware of the status of your data after disposal.

4. Hardware:

- Correctly recycle and dispose of the hardware of the EGW-02 gateway. Refer to [EGW-02 Connectivity Edge Gateway recycling instructions and environmental information \(3AXD50001069544 \[English\]\)](#).

5. Network environment:

- If the EGW-02 gateway is disposed of permanently, no additional checks are required in the customer network.

6. Commissioning again:

- If you replace the EGW-02 gateway with a new one, obey the security instructions in this document.
  - If you move the old EGW-02 gateway to another location in the same legal jurisdiction, contact an **Authorized Person** for the correct steps to commission the EGW-02 gateway again.
  - If you move the old EGW-02 gateway to another location in a different legal jurisdiction, make sure that the old EGW-02 gateway and the transfer of the EGW-02 gateway obey all local laws (for example, radio approval) in both jurisdictions.
  - USB-connected environmental sensors:
-

- If the EGW-02 gateway is replaced, you can connect the existing environmental sensor to the new EGW-02 gateway.
- If the environmental sensor is replaced, you can connect the new sensor to the existing EGW-02 gateway.

## Secure operation guidelines (SG-5)

Do not try to open the enclosure of the EGW-02 gateway or remove its seals.

If CMD/Powertrain is in use, the **End User** does these tasks:

- If you change the external network, make sure that the EGW-02 gateway still transfers data to the CMD cloud service.
- Activate the automatic alarm messages in the CMD cloud service, and define the alarm method (SMS/e-mail) and the persons to be reached.
- If there is a drive-related change in the system, make sure that the CMD cloud service still receives data correctly.
- For information on Modbus and OPC UA security and secure operation, refer to [Additional features \(page 25\)](#).

## Account management (SG-6)

The EGW-02 gateway does not have default user accounts or passwords.

Only ABB (or a trusted ABB partner) can make **Authorized Person** accounts for an EGW-02 gateway. Only **Authorized Persons** can access the configuration settings of an EGW-02 gateway.

## Documentation review (SG-7)

ABB has a user documentation review process and a process to get feedback on user documentation, including cyber security issues.

If you find a cyber security-related or other issue in the user documentation, send an e-mail to the ABB cyber security mailbox: [cybersecurity@ch.abb.com](mailto:cybersecurity@ch.abb.com) or contact an ABB representative. Give information on the document number and the revision.

---





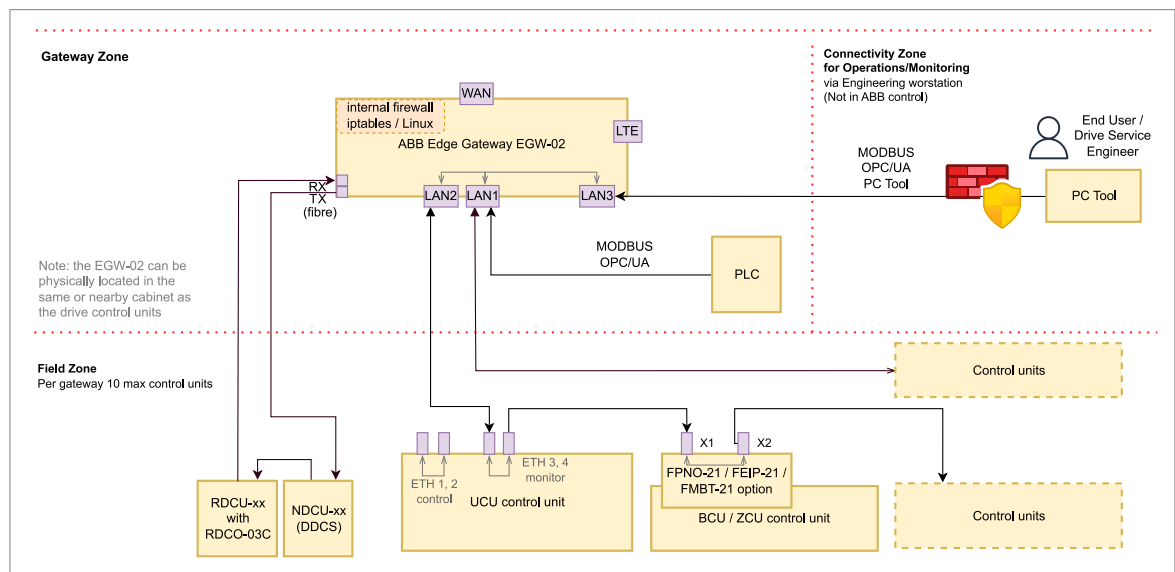
## Additional features

This section has security guidelines and information for the additional features of the gateway.

For information on how to set and control the additional features in this section, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

### Network diagram

The network diagram shows the connection of the additional features.



### Modbus TCP

The EGW-02 can operate as a gateway between a PLC and drives. The PLC connects to the gateway with a Modbus client, and EGW-02 translates the queries to ABB protocols or other protocols, depending on the drive.

An **Authorized Person** can enable the Modbus server in the local user interface. When the Modbus server is active, telemetry monitoring and telemetry data transfer to the cloud are disabled. If telemetry monitoring and telemetry data transfer is required, the **Authorized Person** should make sure that all additional services, such as the Modbus server, OPC UA server, and PC Tool mode, are disabled.

When the Modbus server is active, the **Authorized Person** can enable additional security features such as IP filtering in the local user interface. For more information, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

This connection only supports read-type operations, so it is not possible to control or configure the drive through this connection.

Note that Modbus communication is unencrypted, so the **Asset Owner** must make sure that environmental protections are applied as described in [Defense in depth measures expected in the environment \(SG-2\) \(page 18\)](#).

## OPC UA server

The EGW-02 gateway can operate as a gateway between an OPC UA client and connected drives. The EGW-02 gateway translates the OPC UA queries to ABB protocols and other protocols, depending on the drive.

An **Authorized Person** can enable the OPC UA server and manage the required certificates in the EGW-02 local user interface. When the OPC UA server is active, telemetry monitoring and telemetry data transfer to the cloud are disabled. If telemetry monitoring and telemetry data transfer is required, the **Authorized Person** should make sure that all additional services, such as the Modbus server, OPC UA server, and PC Tool mode, are disabled.

When the OPC UA server is active, the **Authorized Person** can add certificates for an encrypted connection in the local user interface. Note that the OPC UA server cannot be reached if a certificate containing a private key has not been added. For more information, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).

This connection only supports read-type operations, so it is not possible to control or configure the drive through this connection.

## OPC UA client

The EGW-02 can connect to drives through an OPC UA connection.

An **Authorized Person** can enable the connection and manage the required certificates in the EGW-02 local user interface.

## PC Tool mode

The EGW-02 can operate as a protocol translator for PC software applications. PC Tool mode requires that the drives are connected to the gateway.

An **Authorized Person** can enable PC Tool mode in the local user interface of the EGW-02 gateway. When PC Tool mode is active, telemetry monitoring and telemetry data transfer to the cloud are disabled. If telemetry monitoring and telemetry data transfer are required, the **Authorized Person** makes sure that all additional services, such as the Modbus server, OPC UA server, and PC Tool mode, are disabled.

---

For more information, refer to [EGW-02 Connectivity Edge Gateway user's manual \(3AXD50000929719 \[English\]\)](#).





# Further information

## Product and service inquiries

Address any inquiries about the product to your local ABB representative, quoting the type designation and serial number of the unit in question. A listing of ABB sales, support and service contacts can be found by navigating to [new.abb.com/contact-centers](http://new.abb.com/contact-centers).

## Product training

For information on ABB product training, navigate to [new.abb.com/service/training](http://new.abb.com/service/training).

## Providing feedback on ABB manuals

Your comments on our manuals are welcome. Navigate to [forms.abb.com/form-26567](http://forms.abb.com/form-26567).

## Document library on the Internet

You can find manuals and other product documents in PDF format on the Internet at [www.abb.com/drives/documents](http://www.abb.com/drives/documents).



[www.abb.com/drives](http://www.abb.com/drives)



3AXD50001061845C