GB

Software manual
(Addition)

Cyber security

moneo|edgeGateway

AE2100
AE2400

11621108 / 00 09 / 2024

Contents

1 Preliminary note

1.1 Purpose of the document

This document provides an overview of the cyber security mechanisms for the moneo|edgeGateway from ifm.

This document provides information for system integrators and machine builders so that the moneo|edgeGateway can be integrated into a comprehensive security concept and contribute to a robust security architecture.

1.2 Symbols used

✓	Requirement
▶	Instructions
▷	Reaction, result
[...]	Designation of keys, buttons or indications
→	Cross-reference
!	Important note Non-compliance may result in malfunction or interference.
i	Information Supplementary note

1.3 Applicable documents

- Data sheet
- Quick reference guide
- Operating instructions
- moneo|Appliance Management System (AMS) software manual
- ifm moneo online help

2 Security instructions

2.1 Cyber security

Installation

The device is suitable for operation in a secure environment according to IEC 62443-1-1.

The device was designed for operation behind a firewall.

- ▶ Carry out a risk assessment of the system according to IEC 62443-1-1.
- ▶ Take measures to ensure physical security.

User and rights management

- ▶ Only assign the user rights required according to the risk assessment.
- ▶ When setting up user accounts, observe the specifications of your company's security policy.
- ▶ Change default passwords immediately during installation / initial set-up.

Operation

- ▶ Only use communication protocols with sufficiently secure encryption technologies.
- ▶ Observe the security functions described in the product documentation and the recommendations for their use.

Maintenance

- ▶ Regularly check whether software updates are available for the device.
- ▶ Back up system configuration and system data in accordance with your company's change management processes.

Decommissioning

- ▶ Always reset the system settings to the factory settings before decommissioning the device.
- ▶ Ensure that no sensitive information can fall into unauthorised hands.

3 System overview

The moneo|edgeGateway is an embedded device for control cabinet installation or field applications.

The moneo|edgeGateway serves as an end point for the provision of data from the production environment for further processing in the moneo|Cloud or in other customer-specific data platforms.

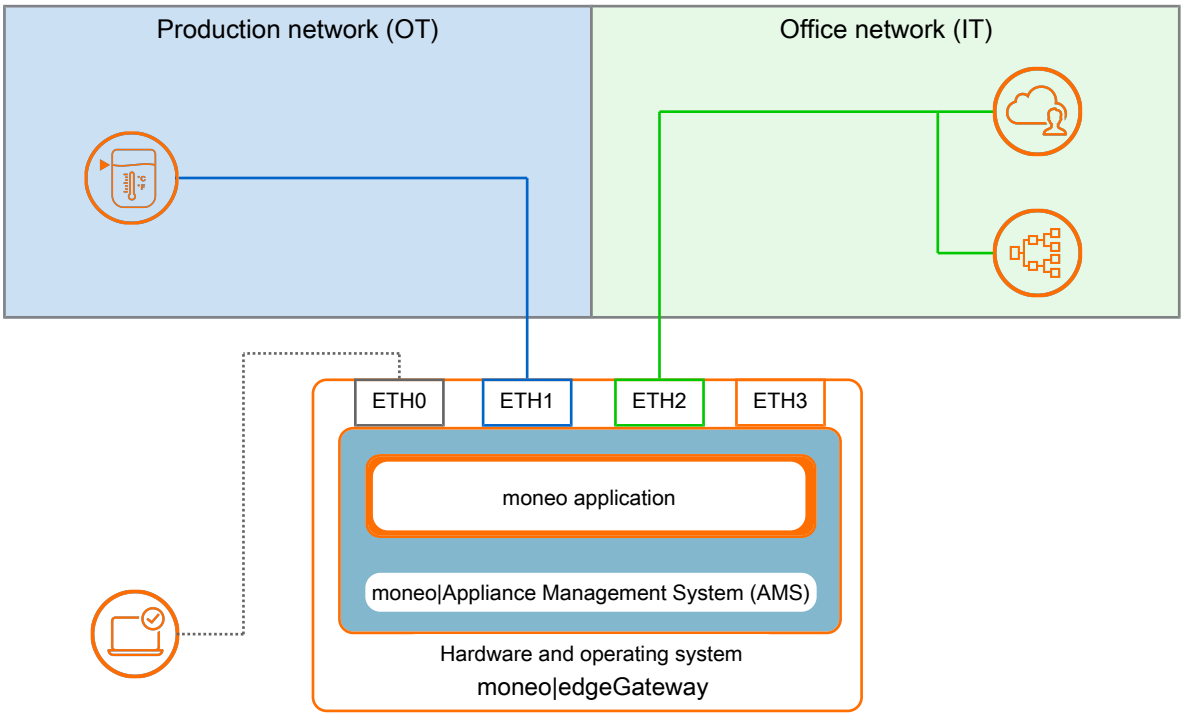

Fig. 1: moneo|edgeGateway system overview

The following table describes the individual components of the moneo|edgeGateway and their function:

Component	Function
Hardware and operating system	Fanless embedded hardware for running the hardened Debian Linux operating system.
Appliance Management System (AMS)	Web-based management platform for managing the moneo|edgeGateway. The AMS provides all the necessary management interfaces for administrators.
moneo application	The moneo application with the individual modules and software interfaces such as MQTT, OPC UA.
Ethernet port ETH0	Service interface Exclusively for setting up the device.
Ethernet port ETH1	OT interface For connecting the device to the OT network structure. The connection is used for communication with devices with ifm IoT Core (e.g. IO-Link master) and the connected sensors.
Ethernet port ETH2	IT interface For connecting the device to the IT network structure. The connection is used for communication with cloud systems.
Ethernet port ETH3	Deactivated and without function

4 Network communication

4.1 Segmentation of the network interfaces

The moneo|edgeGateway enables simultaneous operation in the office network (IT) and the production network (OT).

The IT network and the OT network are separated. It is ensured that no communication between the networks can take place via the network interfaces of the moneo|edgeGateway.

This does not affect IT security concepts.

5 Requirements for the network infrastructure

The moneo|edgeGateway is intended for operation within a secure zone in accordance with IEC 62443-1-1.

No functions are provided that ensure or regulate a secure transition between zones.

Requirements for the network environment are described below.

5.1 Standard network communication

Depending on the application and use of the moneo|edgeGateway, the following accesses to remote systems that must be accessible from the network are required.

Not every authorisation is required in every case.

- ▶ Check which authorisations are required for use.
- ▶ Provide the required authorisations in the firewall.

Use	Direction	Source	Target address (URL)	Ports	Protocol	Description
OPC UA	Incoming	Client	moneo OPC UA server	4840	TCP	Communication between OPC UA client and moneo OPC UA server.
Web UI	Incoming	Client	moneo	80, 443	TCP	Required for accessing the moneo website via the internet browser on a Linux system.
Web UI	Incoming	Client	moneo	5000	TCP	Required for accessing the moneo website via the internet browser on a Windows system.
SFI/SAP	Incoming	Client	moneo SfiHub (GraphQL Server)	5050	TCP	Required for an SFI/SAP connection to provide API information about Topology, ProcessData and moneo tickets.
Name resolution	Outgoing	System	DNS server	53	UDP/TCP	Translates domain names into IP addresses. Required if moneo is to be accessed using host names instead of IP addresses.
Time synchronisation	Outgoing	System	NTP server	123	UDP/TCP	Required to synchronise time across systems in a network to ensure accurate and consistent timestamps for logs, transactions and scheduled tasks (AMS Setup Wizard refers to {0... 3}.pool.ntp.org)
edgeConnect	Outgoing	moneo	Azure IoT Hub	5671, 5672	TCP (AMQP)	Required for using an Azure IoT hub to receive process data from moneo.
edgeConnect	Outgoing	moneo	MQTT (default)	1883, 8883	TCP	For using an MQTT broker to receive process data from moneo.
edgeConnect	Outgoing	moneo	AWS IoT Core	8883	TCP	For using an AWS IoT Core to receive process data from moneo.
remoteConnect	Outgoing	remoteConnect client	global.azure-devices-provisioning.net	443	TCP	Device onboarding and configuration
remoteConnect	Outgoing	remoteConnect client	rc-c-us-prod-iothub.azure-devices.net	8883	TCP	Device onboarding and configuration

Use	Direction	Source	Target address (URL)	Ports	Proto-col	Description
remoteConnect	Outgoing	remoteCon-nect client	relay0.remoteconnect-c-us-prod.moneo.ifm relay1.remoteconnect-c-us-prod.moneo.ifm	443	TCP	Remote access rendezvous server in c-us
remoteConnect	Outgoing	remoteCon-nect client	stun0.remoteconnect-c-us-prod.moneo.ifm stun1.remoteconnect-c-us-prod.moneo.ifm	3478	UDP	Remote access rendezvous server for a direct P2P con-nection in c-us
remoteConnect	Outgoing	remoteCon-nect client	relay0.remoteconnect-w-eu-prod.moneo.ifm relay1.remoteconnect-w-eu-prod.moneo.ifm	443	TCP	Remote access rendezvous server in w-eu
remoteConnect	Outgoing	remoteCon-nect client	stun0.remoteconnect-w-eu-prod.moneo.ifm stun1.remoteconnect-w-eu-prod.moneo.ifm	3478	UDP	Remote access rendezvous server for a direct P2P con-nection in w-eu
Remote access	Outgoing	ifm remote support	gm01-emea.ifm.com	443	TCP	Required when ifm accesses the system remotely to pro-vide customer support.
moneo Cloud	Outgoing	moneo	mqtt.w-eu.moneo.cloud mqtt.e-us.moneo.cloud	8883	TCP	Required for an active con-nection from an edge client to the corresponding cloud clus-ter for process data transfer.
moneo Cloud	Outgoing	AMS	mqtt.moon-w-eu.moneo.cloud	8883	TCP	Required for the cloud on-boarding of an edge client in the corresponding cloud clus-ter.
moneo Cloud	Outgoing	AMS	ifm-mobileiot-services-prod.azurewebsites.net	443	TCP	Required for the cloud on-boarding of an edge client in the corresponding cloud clus-ter.
IODD descrip-tions	Outgoing	moneo	https://ioddfinder.io-link.com	443	TCP	Required to load IODD files if necessary. IODD files (IO De-vice Description files) are re-quired to configure and inte-grate IO-Link devices.
moneo notifica-tion	Outgoing	moneo	MS Teams	Depend-ing on the configura-tion	HTTP	Required to receive notifica-tions from moneo that are sent to this communication channel.
moneo notifica-tion	Outgoing	moneo	SMS Gateway	Depend-ing on the configura-tion	SMS Gate-way	Required to receive notifica-tions from moneo that are sent to this communication channel.
moneo notifica-tion	Outgoing	moneo	Discord	Depend-ing on the configura-tion	HTTP	Required to receive notifica-tions from moneo that are sent to this communication channel.
moneo notifica-tion	Outgoing	moneo	Slack	Depend-ing on the configura-tion	HTTP	Required to receive notifica-tions from moneo that are sent to this communication channel.
Online update	Outgoing	AMS	system.update.ifm	443	HTTP	Required to receive online up-dates for edgeGateways or (v)Appliances.
Sensor data	Outgoing	moneo	VSE	3321	TCP	Required to request data from a VSE device.
Sensor data	Outgoing	moneo	IoTCore	Depend-ing on the device	TCP	Required to request data from an IoT Core device.

Use	Direction	Source	Target address (URL)	Ports	Proto-col	Description
Sensor data	Outgoing	moneo	LRAgent	Depend-ing on the configura-tion	TCP	Required to request data from an LRAgent.

6 Security functions

6.1 Encryption and integrity security

▶ Use communication protocols with encryption technologies.

When accessing via the browser, all communication between the client and the moneo|edgeGateway is TLS-encrypted (4096-bit RSA or 256-bit AES). By default, the moneo|edgeGateway provides a self-signed certificate.

Encrypted communication between client and moneo is ensured.

Due to the inherent behaviour of self-signed certificates, authenticity cannot be verified, which leads to warning messages in some browsers.

To ensure end point integrity, the customer has the option of importing their own trusted certificates for the web front end.

The security of the connection between the moneo|edgeGateway and the cloud platform is also secured via TLS. In addition, each moneo|edgeGateway has a multi-level certificate-based authentication method for secure and unique access to the moneo Cloud instance.

6.2 Remote access via moneo|Cloud

The moneo|edgeGateway includes the moneo|remoteConnect service from ifm for remote access.

The moneo|remoteConnect service must be explicitly authorised via the AMS.

The service is not active when the device is set up.

6.3 Data backup and restore

▶ Save the system configuration and system data in accordance with your company's change management processes.

The moneo|edgeGateway has a backup and restore option for backing up the moneo configuration.

Local USB devices or network storage can be used as storage destinations. The backup can be done manually if required or automatically according to a schedule.

By using a network storage location, the data backups created can be included in the customer's existing data backup concept.

The data backups are encrypted.

▶ Recommendation: To ensure disaster recovery options, data backup should be physically separated from the operation of the moneo|edgeGateway.

6.4 Execution protection at operating system level

Since the moneo|edgeGateway does not allow direct access to the operating system level, no malicious code can be transferred to the system.

6.5 Secured update procedure via dedicated and signed update packages

▶ Regularly check whether software updates are available for the product.

An online update for the moneo|edgeGateway can be carried out via the AMS.

Alternatively, the update package can be downloaded from www.ifm.com and installed via the AMS. If the moneo|edgeGateway is used in conjunction with the moneo|Cloud, it is also possible to initiate an update directly from the cloud. The update will then be carried out immediately.

As the moneo|edgeGateway is updated exclusively via ifm servers, it cannot be compromised by updates. The update packages are encrypted and signed by ifm development.

All updates provided include:

- moneo operating system platform
- Appliance Management System
- Security updates

The updates can be installed by the customer in accordance with the change management process.

7 User access and user roles

moneo and the Appliance Management System (AMS) are applications that can be accessed via a web browser.

Access to the AMS or to moneo is secured via separate user authentication mechanisms. The separation of applications makes it possible to divide access to different user groups.

Different user accounts are provided for the moneo application and the AMS. This enables a separation of responsibilities.

Access to the command line (CLI) via SSH must be explicitly authorised for use. The command line can be used for the initial set-up and for ifm support if required.

The standard users and standard user groups with their authorisations are listed below.

7.1 Standard users

System	Name	Authorisation	Description
AMS & AMS Console	Administrator	Full access	Central administrator for the basic configuration of the Appliance
OS	Maintenance	Full access	ifm maintenance user. The user "Maintenance" is only available after successful activation and only for access via SSH CLI.
moneo	Administrator	Full access	The user is created automatically. When the system is first set up, a common password is defined for the moneo administrator account and the AMS administrator account. A subsequent password change in moneo or AMS means that the password is no longer the same. The program for which the password has been changed will now use the new password, and the other application will not.
moneo	Created during the initial set-up.	Full access	At least one administrator is required. The administrator has the option of creating additional users in different authorisation groups.

7.2 Standard user groups

- ▶ Assign the necessary user rights according to the risk assessment.
- ▶ Use passwords according to the company security policy.

System	Group	Authorisation	Description
moneo	Administrator	Full access	User group for basic set-up of moneo. In addition, users of this group have access to the user account administration
moneo	User	Default user group	Users of this group can edit and use elements within the modules (→ user rights in the moneo help). Users of this group can edit tickets.
moneo	Visitor	Read access	Users of this group can view information in the moneo modules. Users of this group can edit tickets.

8 Decommissioning

- ▶ Ensure that no sensitive information can fall into unauthorised hands during decommissioning.
- ▶ Always reset the system settings to the factory settings before decommissioning the device.

9 Reporting cyber security vulnerabilities / Questions

▶ If you have any questions about cyber security in ifm products or if you want to report cyber security vulnerabilities in ifm products, please contact the "Product Security Incident Response Team" (PSIRT) of the ifm group of companies: psirt@ifm.com