GB

Software manual

Cybersecurity

ifm moneo|remoteConnect

11653713 / 00 02 / 2025

Contents

1 Preliminary note

1.1 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

1.2 Legal and copyright information

© All rights reserved by ifm electronic gmbh. No part of these instructions may be reproduced and used without the consent of ifm electronic gmbh.

All product names, pictures, companies or other brands used are the property of the respective rights owners.

1.3 Applicable documents

▶ Observe other applicable documents:

- ifm moneo remoteConnect client installation instructions
- Data sheet
- Release notes
- ifm moneo online help
- User documentation for the devices and software products used in the respective application, e.g. operating instructions, software manuals, etc.

1.4 Purpose of the document

This document provides an overview of the cybersecurity mechanisms for the moneo|remoteConnect software from ifm.

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

2 Intended use

remoteConnect enables you to remotely access devices and system components such as edgeGateways, IO-Link masters, ifm VSEs, IO-Link sensors or controllers via the existing software, hardware and network infrastructure. A secure point-to-point connection is used for remote access.

ℹ The ifm moneo remoteConnect client runs in the background under Windows and enables the establishment of a secure point-to-point connection for accessing devices that are connected to a moneo|cloud instance using moneo|remoteConnect.

3 Cybersecurity

moneo|remoteConnect was developed with the aim of offering the highest possible cybersecurity. This includes a high level of technical safety and ease of use in order to avoid errors during use.

remoteConnect enables remote maintenance based on the recommendations and the catalogue of measures "Securing remote maintenance" (M 5.33) of the German Federal Office for Information Security (BSI).

This includes the following aspects:

- Remote maintenance access can only be initiated from the customer’s local IT system and cannot technically be started from outside.
- Log the remote maintenance procedure.
- Compliance with the dual-control principle, i.e. remote maintenance by approval of the customer.
- Authentication and graduated rights management for service staff.
- Encryption of the transmitted data.

4 Functionality and components

remoteConnect consists of 3 main components whose interaction enables the remote maintenance connection.

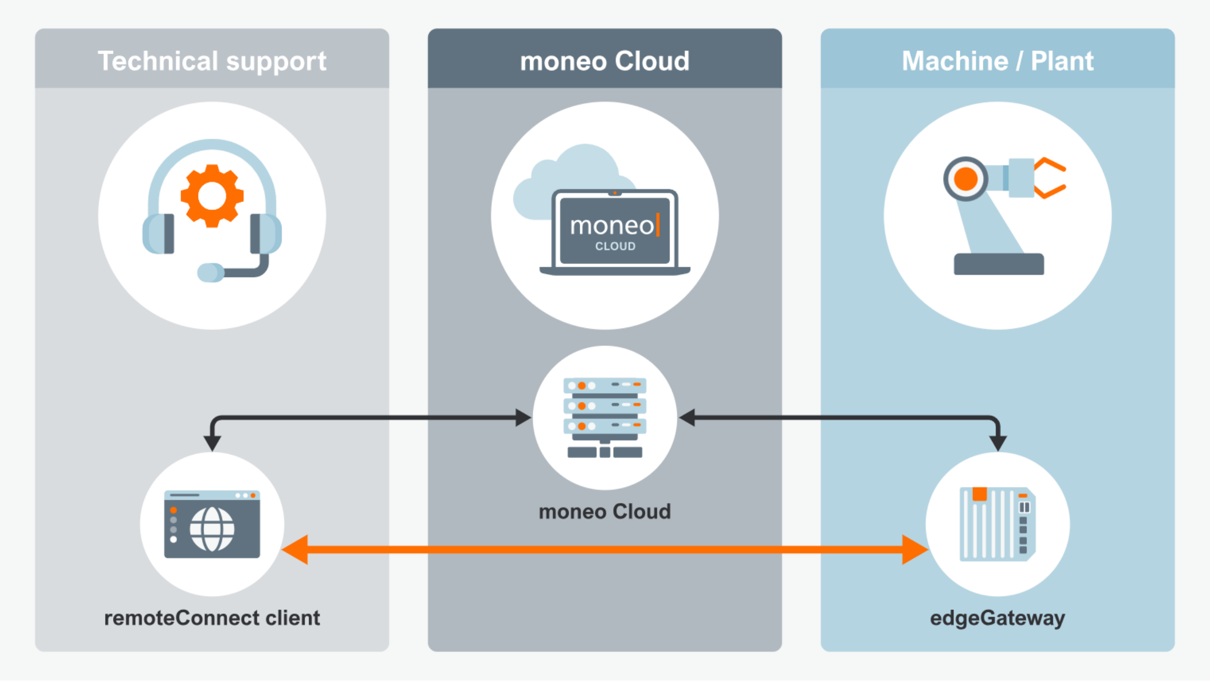

Fig. 1: The 3 main components of remoteConnect

The central component is the moneo|Cloud, from which all remote maintenance connections can be managed and started.

Users, master data, devices and remote maintenance connections are managed and released in the moneo|Cloud.

The endpoints (clients) between which the connection is established in encrypted form are, on the one hand, an ifm edgeGateway installed on site in production or on a machine and, on the other hand, the remoteConnect Windows client installed on the service employee’s computer.

4.1 Cloud

4.1.1 Overview

The remoteConnect application is part of the ifm moneo|Cloud.

The moneo|Cloud is used to centrally control the remote maintenance connections to the corresponding plants and machines.

There is therefore only one location from which remoteConnect sessions can be managed.

A session cannot be created or used from a gateway or a Windows client.

For later checks or external audits, there is a historical display of the sessions and extensive logging in the cloud.

4.1.2 User and rights management

To use remoteConnect, the user requires a user in the moneo|Cloud instance to which the edgeGateway is also connected.

There are 3 user roles in moneo with different rights that are authorised to interact with remoteConnect:

1. Administrator
2. remoteConnect Administrator*
3. remoteConnect User

The administrator and the remoteConnect administrator can create new sessions and authorise devices for them as well as use sessions themselves.

The remoteConnect user can only use sessions that have been prepared and authorised for them. They do not have the option of creating their own sessions.

This means that access to individual devices can be controlled and only authorised for the required group. A connection can only be established for authorised persons.

By separating the roles of administrator and user, remote access by external service employees can be controlled, for example.

	Administrator	remoteConnect Administrator	remoteConnect User
Add new devices to the cloud	Yes (the administrator can add new devices in Device Management and thus make them usable for remoteConnect)	No	No
Add new users and assign rights	Yes	No	No
Create new sessions and select devices	Yes	Yes	No
Add devices to existing sessions	Yes	Yes	No
Start and use prepared sessions	Yes	Yes	Yes
End sessions	Yes (all sessions can be ended at any time)	Yes (all sessions can be ended at any time)	Own sessions only
Overview of all active and historical sessions	Yes	Yes	Own sessions only

Tab. 1: Rights overview of the moneo roles for remoteConnect

ℹ ▶ For a detailed overview of the user roles and rights in moneo, see the information in the moneo online help under "User management".

4.1.3 remoteConnect sessions and logging

remoteConnect is session-based.

To access devices, a session is first created in which the corresponding devices are released.

Every remote maintenance connection is stored centrally in the moneo|Cloud and can be traced retrospectively.

Comprehensive logging records which action was carried out in remoteConnect at what time and which users were involved in a session.

This enables easy traceability, for example during external audits.

4.1.4 Establishing and using a connection in the cloud

General procedure for setting up and using a remoteConnect connection:

On the edgeGateway

▶ Activate remoteConnect on the edgeGateway in the AMS. Activation can be permanent or switched on and off as required.

In the moneo|Cloud

▶ Log in to the moneo|Cloud as a moneo user with the role "Administrator" or "remoteConnect Administrator".

▶ Create a remoteConnect session in the moneo|Cloud. To do this, assign a name for the remoteConnect connection and select at least one device.

▶ Optional: Make further additions.

▶ Optional: Select a remoteConnect user if the session is to be released for this user.

▷ Once the individual steps have been completed, the session is prepared, but not yet active.

❗ ▶ For detailed information on setting up and managing a remoteConnect session, refer to the "remoteConnect" section in the moneo online help.

▶ Start the session. By starting the session, the connection is established and data can flow. This can be done either by the administrator or remoteConnect administrator themselves or by the authorised remoteConnect user.

Prerequisite for starting a remoteConnect connection

- An active edgeGateway
- An installed remoteConnect client on the service employee’s computer
- A RemoteConnect connection set up in the moneo|Cloud instance

4.2 edgeGateway

ifm offers various edgeGateways that establish the connection between OT and IT. These devices can be accessed via remoteConnect.

An Appliance Management System (AMS) is installed on the edgeGateway. The AMS is protected locally with a password.

Before remoteConnect can be used to access an edgeGateway, remoteConnect must be activated on the edgeGateway in the AMS. On delivery, remoteConnect is switched off by default to prevent unwanted remote maintenance connections.

The remoteConnect service can be enabled and disabled in the AMS

Customers can control remote maintenance connections by switching the remoteConnect service on and off in the AMS, even if they do not have access to the moneo|Cloud themselves. A remote maintenance connection can be switched off by the customer at any time.

❗ For detailed information, refer to the user documentation and in particular the cybersecurity documents for the corresponding edge gateway: see ifm.com

4.3 remoteConnect client (on the computer)

The remoteConnect client on the computer is software available for Windows that serves as a counterpart to the edgeGateway. The remoteConnect client can be downloaded free of charge at ifm.com

Administrator rights under Windows are required once to install the client (→ remoteConnect installation instructions). No special rights are required to use the client.

A minimal GUI is included to display status information. The client is not controlled via the local GUI, but via the moneo|Cloud web interface to provide a standardised and simple interface. After starting a session in the moneo|Cloud, you are prompted to start the remoteConnect client. The client then communicates with the moneo|Cloud to obtain its configuration and enables the encrypted connection to the remote end.

5 Technologies and services used

remoteConnect is part of the moneo|Cloud that is operated in Microsoft Azure data centres and uses components of Microsoft Azure services.

As the central technology for establishing and encrypting the connections, remoteConnect uses the WireGuard open source protocol.

5.1 Microsoft Azure

Microsoft Azure is the central cloud solution from Microsoft. Microsoft operates its own solutions on Azure.

ifm uses Azure as a secure and globally available cloud platform for moneo.

Azure’s technological capabilities ensure high availability and, in partnership with Microsoft, a high level of security.

5.2 WireGuard

remoteConnect uses the WireGuard protocol to set up encrypted VPN data tunnels. All data streams are routed through the data tunnel of the remoteConnect connection and thus protected against unauthorised access.

remoteConnect connections are preferably established directly between the edgeGateway and the remoteConnect client on the Windows PC. The cloud only provides the connection configuration for the clients. The advantages of the direct connection are lower latency and higher connection speed, especially over long distances.

If a direct connection is not possible, all data streams run via the cloud as a central server. The cloud serves as a bridge and does not have access to the end-to-end encrypted connection itself.

remoteConnect supports roaming and automatic restoration of an interrupted connection.

remoteConnect only allows access to shared IP addresses. When creating a session, devices or IP addresses that are to be reached via the tunnelled connection can be selected (whitelisting).

If a client attempts to access IP addresses or devices that have not previously been released for the session, these packets are routed via the local network of the Windows client and are therefore not accessible via the tunnelled connection.

This enables the simultaneous use of local network resources with an active remoteConnect connection (split tunnelling).

Important features of WireGuard:

- Uses modern cryptography methods
- Secure, trustworthy architecture
- Lower complexity than comparable technologies such as OpenVPN or IPsec, as a result:
  - Better maintainability and less attack surface ⇒ higher security
  - Higher performance
- Decentralised peer-to-peer VPN protocol
- Requires little bandwidth
- Supports roaming (automatic uninterrupted switching of networks, for example from WLAN to mobile phone network).
- Is licensed as open source software under the GPLv2 licence

5.3 Technical connection setup

Various services are required to establish the connection.

In the moneo|Cloud, this includes the STUN server and the relay server in particular.

STUN server

The STUN server implements the STUN protocol for UDP endpoint detection through NAT firewalls and helps edge devices and clients to discover their UDP endpoints for direct communication.

Relay server

The relay server acts as an intermediary if direct communication between the Edge device and Windows client via UDP is not possible. It provides a web socket endpoint to which edge devices and clients can connect. Received WireGuard packets are then forwarded to the corresponding peer.

Various services that are required for a remoteConnect connection run on the edgeGateway. The actual remote maintenance connection is created via the remoteConnect service. This service is responsible for maintaining remote connections with WireGuard. It communicates with clients and relay servers and forwards packets to the actual IP devices that are addressed. To receive its configuration and send audit events to the cloud, it interacts directly with the cloud.

The actual connection setup with WireGuard works in a similar way to Secure Shell (SSH): The endpoints (clients) generate public keys with WireGuard and exchange them with each other. The clients use the keys to authenticate each other and encrypt the data packets for the corresponding other party.

In addition to generating the cryptographic keys, various network settings must be made on each client. For data exchange, permitted IP address ranges on the clients are linked to the cryptographic key. Packets that do not originate from the permitted address ranges are discarded. Data is sent with WireGuard via the User Datagram Protocol (UDP).

For the initial connection and if direct communication between the clients is prevented by firewall rules, the peers exchange packets via a relay server. Communication with the relay server then takes place via WebSocket. Preferably, remoteConnect always establishes a direct connection between the edgeGateway and the service PC. In this variant, the client and the edge gateway are connected directly via the WireGuard-based overlay network.

6 Network communication

To be able to use remoteConnect, the following authorisations are required in the network:

For detailed information, refer to the user documentation and in particular the cybersecurity documents for the corresponding edge gateway: see ifm.com

Use	Direction	Source	Target address (URL)	Ports	Protocol	Description
remoteConnect	Outgoing	edgeGateway	global.azure-devices-provisioning.net	443	TCP	Device onboarding and configuration
remoteConnect	Outgoing	edgeGateway	rc-c-us-prod-iothub.azure-devices.net	8883	TCP	Device onboarding and configuration
remoteConnect	Outgoing	edgeGateway remoteConnect Windows client	relay0.remoteconnect-c-us-prod.moneo.ifm	443	TCP	Remote access rendezvous server in c-us
			relay1.remoteconnect-c-us-prod.moneo.ifm			
remoteConnect	Outgoing	edgeGateway remoteConnect Windows client	stun0.remoteconnect-c-us-prod.moneo.ifm	3478	UDP	Remote access rendezvous server for a direct P2P connection in c-us
			stun1.remoteconnect-c-us-prod.moneo.ifm			
remoteConnect	Outgoing	edgeGateway remoteConnect Windows client	relay0.remoteconnect-w-eu-prod.moneo.ifm	443	TCP	Remote access rendezvous server in w-eu
			relay1.remoteconnect-w-eu-prod.moneo.ifm			
remoteConnect	Outgoing	edgeGateway remoteConnect Windows client	stun0.remoteconnect-w-eu-prod.moneo.ifm	3478	UDP	Remote access rendezvous server for a direct P2P connection in w-eu
			stun1.remoteconnect-w-eu-prod.moneo.ifm			

7 Reporting cybersecurity vulnerabilities / questions

▶ If you have any questions about cybersecurity for ifm products or to report cybersecurity vulnerabilities in ifm products, please contact the „Product Security Incident Response Team“ (PSIRT) of the ifm group: psirt@ifm.com