Softwarehandbuch

Cybersecurity

ifm moneo|remoteConnect

DE

11653713 / 00 02 / 2025

Inhaltsverzeichnis

1 Vorbemerkung

1.1 Verwendete Symbole

✓	Voraussetzung
▶	Handlungsanweisung
▷	Reaktion, Ergebnis
[...]	Bezeichnung von Tasten, Schaltflächen oder Anzeigen
→	Querverweis
	Wichtiger Hinweis Fehlfunktionen oder Störungen sind bei Nichtbeachtung möglich
	Information Ergänzender Hinweis

1.2 Rechtliche Hinweise

1.3 Mitgeltende Dokumente

▶ Mitgeltende Dokumente beachten:

- Installationsanleitung ifm moneo remoteConnect-Client
- Datenblatt
- Release Notes
- ifm moneo Online-Hilfe
- Anwenderdokumentation zu den in der jeweiligen Applikation verwendeten Geräten und Softwareprodukten, zum Beispiel Betriebsanleitungen, Softwarehandbücher, etc.

1.4 Zweck des Dokuments

Dieses Dokument gibt einen Überblick über die Cybersecurity-Mechanismen für die Software moneo|remoteConnect von ifm.

Dieses Dokument stellt Informationen für Systemintegratoren und Maschinenbauer zur Verfügung, damit die Software moneo|remoteConnect in ein umfassendes Sicherheitskonzept integriert werden und zu einer robusten Sicherheitsarchitektur beitragen kann.

2 Bestimmungsgemäße Verwendung

remoteConnect ermöglicht den Fernzugriff auf Geräte und Anlagen-Komponenten, z.B. edgeGateways, IO-Link-Master, ifm VSE, IO-Link-Sensoren, Steuerungen etc., über die vorhandene Software, Hardware und Netzwerkinfrastruktur. Für den Fernzugriff wird eine gesicherte Punkt-zu-Punkt-Verbindung verwendet.

Der ifm moneo remoteConnect-Client läuft im Hintergrund unter Windows und ermöglicht den Aufbau einer gesicherten Punkt-zu-Punkt-Verbindung für den Zugriff auf Geräte, welche mit einer moneo|Cloud-Instanz verbunden sind, mittels moneo|remoteConnect.

3 Cybersecurity

moneo|remoteConnect wurde mit dem Ziel, höchstmögliche Cybersecurity zu bieten, entwickelt. Dazu gehören eine hohe technische Sicherheit und eine gute Bedienbarkeit, um Fehler bei der Anwendung zu vermeiden.

remoteConnect ermöglicht Fernwartungen anhand der Empfehlungen und des Maßnahmenkatalogs „Absicherung von Fernwartung“ (M 5.33) des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Dies beinhaltet unter anderem folgende Aspekte:

- Fernwartungszugriffe können nur vom lokalen IT-System des Kunden initiiert werden und können technisch nicht von außen gestartet werden.
- Durchführung der Fernwartung protokollieren.
- Einhaltung des 4-Augen-Prinzips, d. h. Fernwartung durch Freigabe des Kunden.
- Authentisierung und abgestufte Rechteverwaltung des Servicepersonals.
- Verschlüsselung der übertragenen Daten.

4 Funktionsweise und Komponenten

remoteConnect besteht aus 3 Hauptkomponenten, deren Zusammenspiel die Fernwartungsverbindung ermöglicht.

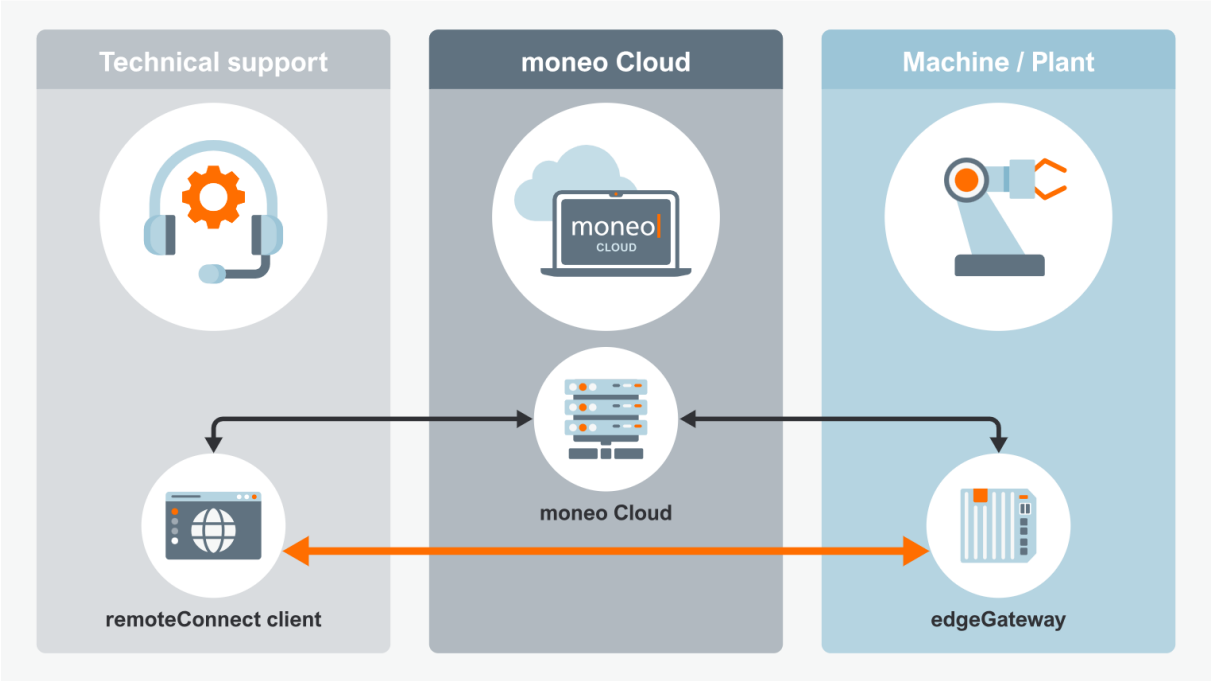

Abb. 1: Die 3 Hauptkomponenten von remoteConnect

Die zentrale Komponente ist die moneo|Cloud, von der aus alle Fernwartungsverbindungen verwaltet und gestartet werden können.

In der moneo|Cloud findet die Verwaltung und Freigabe von Benutzern, Stammdaten, Geräten und Fernwartungsverbindungen statt.

Die Endpunkte (Clients), zwischen denen die Verbindung verschlüsselt aufgebaut wird, sind auf der einen Seite ein ifm edgeGateway, das vor Ort in der Produktion oder an einer Maschine angebracht ist, und auf der anderen Seite der remoteConnect-Windows-Client, der auf dem Computer des Service-Mitarbeiters installiert ist.

4.1 Cloud

4.1.1 Übersicht

Die Applikation remoteConnect ist Bestandteil der ifm moneo|Cloud.

Über die moneo|Cloud erfolgt die zentrale Steuerung der Fernwartungsverbindungen auf die entsprechenden Anlagen und Maschinen.

Es gibt somit nur ein Ort, von dem aus remoteConnect-Sitzungen verwaltet werden können.

Eine Erstellung oder Nutzung einer Sitzung kann nicht von einem Gateway oder einem Windows-Client aus gestartet werden.

Für spätere Überprüfungen oder externe Audits gibt es eine historische Darstellung der Sitzungen und ein umfangreiches Logging in der Cloud.

4.1.2 Benutzer- und Rechte-Verwaltung

Um remoteConnect zu nutzen, benötigt der Anwender einen Nutzer in der moneo|Cloud-Instanz, mit der auch das edgeGateway verbunden ist.

Es existieren in moneo 3 Benutzerrollen mit verschiedenen Rechten, die mit remoteConnect interagieren dürfen:

1. Administrator
2. remoteConnect Administrator
3. remoteConnect User

Der Administrator und der remoteConnect Administrator können neue Sitzungen erstellen und Geräte dafür freigeben, sowie Sitzungen selbst nutzen.

Der remoteConnect User kann nur vorbereitete und für ihn freigegebene Sitzungen nutzen. Er hat nicht die Möglichkeit eigene Sitzungen zu erstellen.

Damit kann der Zugriff auf einzelne Geräte gesteuert werden und nur dem gewünschten Kreis freigegeben werden. Ein Verbindungsaufbau ist nur für autorisierte Personen möglich.

Durch die Trennung der Rollen Administrator und User kann beispielsweise der Fernzugriff durch externe Service-Mitarbeiter gesteuert werden.

	Adminstrator	**remoteConnect Administrator**	**remoteConnect User**
Neue Geräte in die Cloud hinzufügen	Ja (Der Administrator kann im Device-Management neue Geräte hinzufügen und somit nutzbar für remoteConnect machen)	Nein	Nein
Neue Nutzer hinzufügen und Rechte vergeben	Ja	Nein	Nein
Neue Sitzungen erstellen und Geräte auswählen	Ja	Ja	Nein
Geräte zu existierenden Sitzungen hinzufügen	Ja	Ja	Nein
Vorbereitete Sitzungen starten und nutzen	Ja	Ja	Ja
Sitzungen beenden	Ja (alle Sitzungen können jederzeit beendet werden)	Ja (alle Sitzungen können jederzeit beendet werden)	Nur eigene Sitzungen
Übersicht über alle aktiven und historischen Sitzungen	Ja	Ja	Nur eigene Sitzungen

Tab. 1: Rechteübersicht der moneo-Rollen für remoteConnect

▶ Für eine detaillierte Übersicht über die Benutzerrollen und Rechte in moneo die Angaben in der moneo-Online Hilfe unter „Benutzerverwaltung“ beachten.

4.1.3 remoteConnect Sitzungen und Logging

remoteConnect ist sitzungsbasiert aufgebaut.

Um auf Geräte zuzugreifen, wird zuerst eine Sitzung erstellt, in der entsprechende Geräte freigegeben werden.

Jede Fernwartungsverbindung, wird zentral in der moneo|Cloud gespeichert und kann im Nachhinein nachvollzogen werden.

Ein umfangreiches Logging hält fest, welche Aktion in remoteConnect zu welcher Zeit durchgeführt wurde und welche Benutzer an einer Sitzung beteiligt waren.

Dies ermöglicht eine leichte Nachvollziehbarkeit, zum Beispiel bei externen Audits.

4.1.4 Aufbauen und Nutzen einer Verbindung in der Cloud

Generelle Vorgehensweise zum Aufbauen und Nutzen einer remoteConnect-Verbindung:

Auf dem edgeGateway

▶ remoteConnect auf dem edgeGateway im AMS aktivieren. Die Aktivierung kann permanent erfolgen oder bei Bedarf eingeschaltet und ausgeschaltet werden.

In der moneo|Cloud

▶ Als moneo-Benutzer mit der Rolle „Administrator“ oder „remoteConnect Administrator“ in die moneo|Cloud einloggen.

▶ Eine remoteConnect-Sitzung in der moneo|Cloud erstellen. Dazu einen Namen für die remoteConnect-Verbindung vergeben und mindestens ein Gerät auswählen.

▶ Optional: Weitere Ergänzungen vornehmen.

▶ Optional: Einen remoteConnect-User auswählen, wenn die Sitzung für diesen freigegeben werden soll.

▷ Nach dem Fertigstellen der einzelnen Schritte ist die Sitzung vorbereitet, allerdings noch nicht aktiv.

▶ Für detaillierte Informationen zum Einrichten und Verwalten einer remoteConnect-Sitzung die Angaben in der moneo-Online Hilfe im Abschnitt „remoteConnect“ beachten.

▶ Die Sitzung starten. Durch das Starten der Sitzung wird die Verbindung aufgebaut und Daten können fließen. Dies kann entweder durch den Administrator oder remoteConnect Administrator selbst passieren oder durch den freigegeben remoteConnect User.

Voraussetzung für das Starten einer remoteConnect-Verbindung

- Ein aktives edgeGateway
- Ein installierter remoteConnect-Client auf dem Computer des Service-Mitarbeiters
- Eine eingerichtete RemoteConnect-Verbindung in der moneo|Cloud-Instanz

4.2 edgeGateway

ifm bietet unterschiedliche edgeGateways an, die die Verbindung zwischen der OT und der IT herstellen. Auf diese Geräte kann per remoteConnect zugegriffen werden.

Auf dem edgeGateway ist ein Appliance Management System installiert (AMS). Das AMS ist lokal mit einem Passwort geschützt.

Bevor der Zugriff über remoteConnect auf ein edgeGateway erfolgen kann, muss remoteConnect auf dem edgeGateway im AMS aktiviert werden. Bei Auslieferung ist remoteConnect standardmäßig ausgeschaltet, um unerwünschte Fernwartungsverbindungen zu verhindern.

Der remoteConnect-Dienst kann im AMS aktiviert und deaktiviert werden

Kunden haben die Möglichkeit, über Einschalten und Ausschalten des remoteConnect-Dienstes im AMS, Fernwartungsverbindungen zu steuern, auch wenn sie selbst nicht über Zugriff auf die moneo|Cloud verfügen. Eine Fernwartungsverbindung kann jederzeit kundenseitig ausgeschaltet werden.

Für Detailinformationen die Anwenderdokumentation und insbesondere die Cybersecurity-Dokumente des entsprechenden edgeGateways beachten: siehe ifm.com

4.3 remoteConnect-Client (auf dem Computer)

Der remoteConnect-Client auf dem Computer ist für Windows verfügbare Software, welche als Gegenstück zum edgeGateway dient. Der remoteConnect-Client kann kostenlos heruntergeladen werden unter: ifm.com

Zur Installation des Clients sind einmalig Administrator-Rechte unter Windows notwendig (→ Installationsanleitung remoteConnect). Zur Nutzung des Clients sind keine gesonderten Rechte notwendig.

Eine minimale GUI ist enthalten, um Statusinformationen anzuzeigen. Der Client wird nicht über die lokale GUI gesteuert, sondern über die moneo|Cloud-Weboberfläche, um eine einheitliche und einfache Schnittstelle bereitzustellen. Nach Starten einer Sitzung in der moneo|Cloud erfolgt die Aufforderung den remoteConnect-Client zu starten. Der Client kommuniziert dann mit der moneo|Cloud, um seine Konfiguration zu erhalten und ermöglicht die verschlüsselte Verbindung zur Gegenseite.

5 Eingesetzte Technologien und Dienste

remoteConnect ist Teil der moneo|Cloud, die in Microsoft Azure-Rechenzentren betrieben wird und Komponenten der Microsoft Azure-Dienste nutzt.

Als zentrale Technologie zum Aufbau und zur Verschlüsselung der Verbindungen nutzt remoteConnect als Open-Source-Protokoll WireGuard.

5.1 Microsoft Azure

Microsoft Azure ist die zentrale Cloud-Lösung von Microsoft. Microsoft betreibt eigene Lösungen auf Azure.

ifm nutzt Azure als sichere und global verfügbare Cloud-Plattform für moneo.

Mit den technologischen Möglichkeiten von Azure kann eine hohe Verfügbarkeit und in Partnerschaft mit Microsoft ein hohes Sicherheitslevel gewährt werden.

5.2 WireGuard

remoteConnect nutzt das Protokoll WireGuard für den Aufbau von verschlüsselten VPN-Datentunneln. Alle Datenströme werden durch den Datentunnel der remoteConnect-Verbindung geleitet und somit vor unbefugtem Zugriff geschützt.

remoteConnect-Verbindungen werden bevorzugt direkt zwischen dem edgeGateway und dem remoteConnect-Client auf dem Windows-PC hergestellt. Die Cloud stellt nur die Verbindungskonfiguration für die Clients zur Verfügung. Vorteile der Direktverbindung sind eine geringere Latenz und höhere Geschwindigkeit der Verbindung, insbesondere bei großen Distanzen.

Sollte eine Direktverbindung nicht möglich sein, laufen alle Datenströme über die Cloud als zentraler Server. Die Cloud dient als Brücke und bekommt selbst keinen Zugriff auf die Ende-zu-Ende-verschlüsselte Verbindung.

remoteConnect unterstützt Roaming und automatisches Wiederherstellen einer unterbrochenen Verbindung.

remoteConnect ermöglicht nur Zugriff auf freigegebene IP-Adressen. Beim Erstellen einer Sitzung können Geräte bzw. IP-Adressen ausgewählt werden, die über die getunnelte Verbindung erreicht werden sollen (Whitelisting).

Sollte ein Client versuchen auf IP-Adressen bzw. Geräte zuzugreifen, die nicht vorher für die Sitzung freigegeben wurden, werden diese Pakete über das lokale Netzwerk des Windows-Client ausgeleitet und sind somit nicht über die getunnelte Verbindung erreichbar.

Somit ist die gleichzeitige Nutzung von lokalen Netzwerkressourcen bei aktiver remoteConnect Verbindung möglich (Split Tunneling).

Wichtige Eigenschaften von WireGuard:

- Verwendet moderne Kryptografieverfahren
- Sichere vertrauenswürdige Architektur
- Geringere Komplexität als vergleichbare Technologien wie OpenVPN oder IPsec, dadurch:
  - Bessere Wartbarkeit und weniger Angriffsfläche ⇒ Höhere Sicherheit
  - Höhere Performance
- Dezentrales Peer-to-Peer-VPN-Protokoll
- Benötigt wenig Bandbreite
- Unterstützt Roaming (Automatischer unterbrechungsfreier Wechsel von Netzwerken, zum Beispiel von WLAN zum Handynetz.)
- Ist unter der GPLv2-Lizenz als Open Source Software lizensiert

5.3 Technischer Verbindungsaufbau

Für den Verbindungsaufbau sind verschiedene Dienste notwendig.

Dazu gehören in der moneo|Cloud insbesondere der STUN-Server und der Relay-Server.

STUN-Server

Der STUN-Server implementiert das STUN-Protokoll zur UDP-Endpunkterkennung durch NAT-Firewalls und hilft Edge-Geräten und Clients, ihre UDP-Endpunkte für die direkte Kommunikation zu entdecken.

Relay-Server

Der Relay-Server fungiert als Vermittler, wenn keine direkte Kommunikation zwischen Edge-Gerät und Windows-Client via UDP möglich ist. Er bietet einen Websocket-Endpunkt, mit dem sich Edge-Geräte und Clients verbinden können. Empfangene WireGuard-Pakete werden dann an den entsprechenden Peer weitergeleitet.

Auf dem edgeGateway laufen verschiedene Services, die für eine remoteConnect-Verbindung notwendig sind. Die eigentliche Fernwartungsverbindung wird über den remoteConnect-Dienst erzeugt. Dieser Dienst ist für die Aufrechterhaltung der Remoteverbindungen mit WireGuard verantwortlich. Er kommuniziert mit Clients und Relay-Servern und leitet Pakete an die tatsächlichen IP-Geräte weiter, die angesprochen werden. Um seine Konfiguration zu empfangen und Audit-Ereignisse an die Cloud zu senden, interagiert er direkt mit der Cloud.

Der eigentliche Verbindungsaufbau mit WireGuard funktioniert ähnlich wie bei Secure Shell (SSH): Die Endpunkte (Clients) erzeugen mit WireGuard öffentliche Schlüssel und tauschen diese untereinander aus. Mithilfe der Schlüssel authentifizieren sich die Clients gegenseitig und verschlüsseln die Datenpakete für das jeweilige Gegenüber.

Neben der Erzeugung der kryptografischen Schlüssel müssen auf jedem Client verschiedene Netzwerkeinstellungen vorgenommen werden. Zum Datenaustausch werden auf den Clients erlaubte IP-Adressbereiche mit dem kryptografischen Schlüssel verknüpft. Nicht den erlaubten Adressbereichen entstammende Pakete werden verworfen. Der Datenversand mit WireGuard läuft über das User Datagram Protocol (UDP).

Für die anfängliche Verbindung und falls die direkte Kommunikation zwischen den Clients durch Firewall Regeln verhindert wird, tauschen die Peers Pakete über einen Relay-Server aus. Die Kommunikation mit dem Relay-Server erfolgt dann über WebSocket. Präferiert stellt remoteConnect immer eine Direktverbindung zwischen dem edgeGateway und dem Service-PC her. In dieser Variante sind der Client und das edgeGateway direkt über das auf WireGuard basierende Overlay-Netzwerk miteinander verbunden.

6 Netzwerkkommunikation

Um remoteConnect nutzen zu können bedarf es folgender Freigaben im Netzwerk:

Für Detailinformationen die Anwenderdokumentation und insbesondere die Cybersecurity-Dokumente des entsprechenden edgeGateways beachten: siehe ifm.com

Verwendung	Richtung	Quelle	Ziel-Adresse (URL)	Ports	Proto-koll	Beschreibung
remoteConnect	Ausgehend	edgeGateway	global.azure-devices-pro-visioning.net	443	TCP	Device Onboarding und Konfi-guration
remoteConnect	Ausgehend	edgeGateway	rc-c-us-prod-iothub.azu-re-devices.net	8883	TCP	Device Onboarding und Konfi-guration
remoteConnect	Ausgehend	edgeGateway remoteConnect-Windows-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	Ausgehend	edgeGateway remoteConnect-Windows-Client	stun0.remoteconnect-c-us-prod.moneo.ifm stun1.remoteconnect-c-us-prod.moneo.ifm	3478	UDP	Remote Access Rendezvous Server für eine direkte P2P-Verbindung in c-us
remoteConnect	Ausgehend	edgeGateway remoteConnect-Windows-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	Ausgehend	edgeGateway remoteConnect-Windows-Client	stun0.remoteconnect-w-eu-prod.moneo.ifm stun1.remoteconnect-w-eu-prod.moneo.ifm	3478	UDP	Remote Access Rendezvous Server für eine direkte P2P-Verbindung in w-eu

7 Cybersecurity-Schwachstellen melden / Fragen

▶ Bei Fragen zum Thema Cybersecurity bei ifm-Produkten und zum Melden von Cybersecurity-Schwachstellen in ifm-Produkten bitte an das „Product Security Incident Response Team“ (PSIRT) der ifm-Unternehmensgruppe wenden: psirt@ifm.com