Talk2m-Voraussetzungen

Seitentyp	Ersteller	Datum
Technische Anleitung	FK	10.01.2025

Haftungsausschluss

Diese Technical Note dient als Beispiel einer funktionierenden Anwendung. Eine Haftung ist für Sach- und Rechtsmängel dieser Dokumentation, insbesondere für deren Richtigkeit, Fehlerfreiheit, Freiheit von Schutz- und Urheberrechten Dritter, Vollständigkeit und/oder Verwendbarkeit – außer bei Vorsatz oder Arglist – ausgeschlossen.

Sicherheitshinweise

Zur Gewährleistung eines sicheren Betriebes darf das Gerät nur nach den Angaben in der Betriebsanleitung betrieben werden. Bei der Verwendung sind zusätzlich die für den jeweiligen Anwendungsfall erforderlichen Rechts- und Sicherheitsvorschriften zu beachten. Sinngemäß gilt dies auch bei Verwendung von Zubehör.

Dokument Version

Version	Autor	Datum	Änderung
1.0	GI	23.04.19	Dokument erstellt
1.1	GI	28.07.19	Talk2m VPN-Server erweitert
1.2	GI	19.10.19	Access Server Router
1.3	MH	23.09.20	Kap. 3, Firewall Konfiguration

			Überarbeitung der anderen Kapitel
1.4	MH	07.07.21	Kap. 4.2, mögliche VPN-Server = bis 100
1.5	MH	17.11.21	Kap. 4.1, AS für Cosy+
1.6	MGI	16.01.23	Kap. 4.1 englisch, aktualisiert
1.7	FK	10.01.25	Links aktualisiert
1.8	CLI	28.04.25	Alle Kap. überarbeitet Kap. 9 und 10 ergänzt

Für englischsprachige Kunden gibt es die folgenden Informationen vom Hersteller direkt unter diesem Link: Talk2m Onsite Firewall Requirements

Einleitung

Diese Technical Note beschreibt die Voraussetzungen, die erfüllt sein müssen, damit der Verbindungsdienst Talk2m (Talk to machine) für Ewon-Router genutzt werden kann.

Talk2m arbeitet als sog. Rendezvous-Server mit OpenVPN zur Verschlüsselung der Datenübertragung. Feldseitig verbinden sich die Router mit dem Dienst und anwenderseitig gibt es die kosten- und lizenzfreie Software "eCatcher" (OpenVPN-Client), mit der die Verbindung zu dem Dienst und zu den Routern hergestellt wird. Die Verbindung vom Anwender und Router erfolgt im Dienst, somit wird beidseitig nur mit ausgehenden Verbindungen gearbeitet. Dadurch ist es nicht erforderlich, in den Netzwerken Ports eingehend zu öffnen, was ein wesentliches Sicherheitskriterium für die Fernwartungslösung Ewon ist.

Funktionsweise Talk2m

Die Ewon-Router verbinden sich nach der Einrichtung über das OpenVPN-Protokoll mit einem der weltweit verteilten Talk2m-Server. Diese Verbindung sollte eine permanente Verbindung (auch initiierte Verbindung möglich) über Ethernet (kabelgebunden), GSM (Mobilfunk) oder WLAN (WiFi) sein.

Wenn der Anwender eine Verbindung auf die LAN-seitig angeschlossenen Geräte herstellen möchte, stellt er zunächst mittels der Software „eCatcher“ eine Verbindung zu seinem Talk2m-Konto her.

Er wählt dann das jeweilige Ewon-Gerät in seinem Konto aus, und betätigt den Button [Verbinden]. Damit wird eine Verbindung zwischen dem PC, auf dem der eCatcher ausgeführt wird und dem LAN-Netzwerk vor Ort hergestellt. Diese Verbindung ist eine vollwertige IP-Verbindung. Es können alle Dienste und Applikationen verwendet werden, die auch mit einer lokalen Verbindung genutzt werden können. Der Zugriff auf serielle Geräte und USB ist ebenfalls über diese Verbindung möglich.

Broadcasts (z.B. verfügbare LAN-Geräte in einer Software automatisch anzeigen) werden über diese geroutete Verbindung standardmäßig nicht unterstützt.

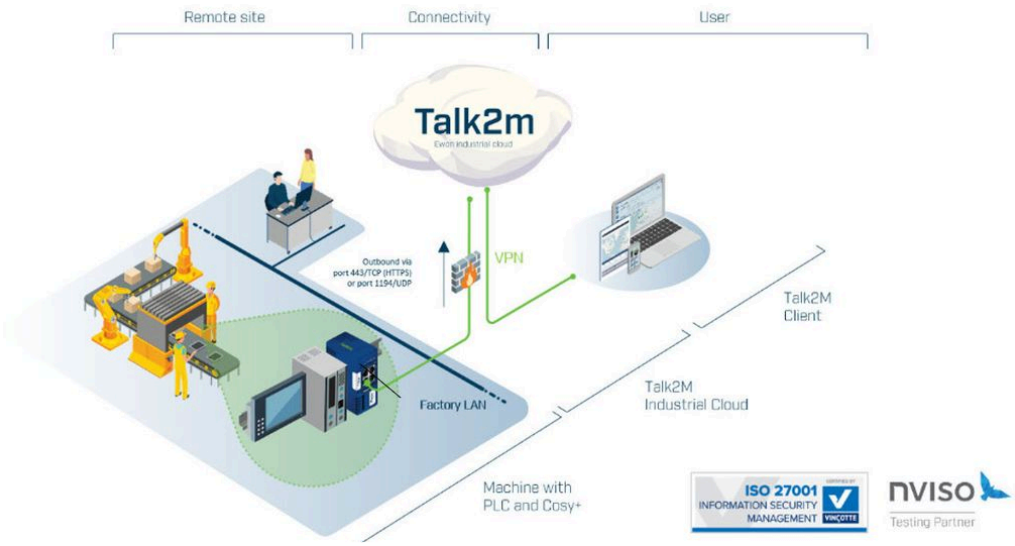

Bild 1: Talk2m Prinzip

Firewall-Konfiguration

Talk2m ist ein hoch verfügbares System. Um die Verfügbarkeit möglichst immer und unter allen Umständen zu garantieren ist es in manchen Situationen oder unter bestimmten Umständen erforderlich, ein Talk2m-Konto oder einen Ewon-Router auf einen anderen VPN-Server „umzuziehen“. In diesem Fall muss sich dann auch der eCatcher auf einen anderen VPN-Server verbinden. Daher sollte die Firewall-Regel wie folgt aussehen:

- Mindestens erforderlich: *.talk2m.com:443 (TCP-Protokoll)
- **Empfohlen: *.talk2m.com:443 (TCP-Protokoll) und *.talk2m.com:1194 (UDP-Protokoll)**

Das Verzichten auf die Freigabe des UDP-Protokolls hat eine langsamere Verbindung zur Folge.

Wenn alle Talk2m-Server mit *.talk2m.com auf der Whitelist stehen, führt die Verschiebung eines Kontos oder eines Routers nicht zu Verbindungsproblemen.

Wenn Sie *.talk2m.com (oder alle erforderlichen Server) nicht auf die Whitelist setzen, können folgende Probleme auftreten:

- Ein Fernzugriff ist nicht mehr möglich, das Gerät wird im eCatcher als „offline“ angezeigt.
- Wenn Ihr Ewon VPN-Router Talk2m als E-Mail Server oder SMS-Relay verwendet, funktioniert die Alarmierung und die Benachrichtigung nicht mehr.
- Wenn Ihr Ewon VPN-Router die DataMailbox verwendet, werden historische Daten nicht mehr an die DataMailbox gesendet.

Ein Serverwechsel von einem Server auf einen anderen kann während einer VPN-Serverwartung oder aufgrund eines VPN-Serverproblems erforderlich sein.

Wenn Ihre Firewall auf IP-Basis arbeitet, achten Sie bitte darauf, dass die IP-Adressen der o.g. URLs vom Ewon-Router erreicht werden können.

Wenn Ihre Firewall über eine Option "OpenVPN-Verbindung blockieren" (oder eine ähnliche Option) verfügt, deaktivieren Sie diese, da Talk2m die OpenVPN-Technologie verwendet, um Benutzer mit ihren Ewon-Geräten zu verbinden.

Deep-Packet-Inspection von TLS/SSL verschlüsseltem Datenverkehr

Einige Firewalls oder Antivirensoftwares enthalten eine s.g. Deep Packet Inspection (DPI). Dabei werden die Daten des verschlüsselten Datenverkehrs, die von einer Anwendung gesendet und empfangen werden, überwacht.

Bei diesem Mechanismus ersetzt die Firewall oder die Antivirensoftware das Talk2m HTTPS-Zertifikat durch ihr eigenes Zertifikat. Das kann als "Man in the Middle"-Angriff angesehen werden.

Diese Methode des Ersetzens von Zertifikaten wird von eCatcher und den Ewon VPN-Routern aus Sicherheitsgründen abgelehnt.

Wenn Sie mit diesem Problem konfrontiert sind, erscheint folgende Fehlermeldung:

- eCatcher meldet während einem Verbindungsaufbau zu einem VPN-Router folgendes:

> ***Server communication error: peer not authenticated***

- Im Webbrowser des Ewon-Routers, während der Ausführung des Talk2m-Assistenten:

> ***HTTPS dialog failed (Server certificate verification failed: certificate issue for a different hostname, issue is not trusted)***

Die einzige Lösung für dieses Problem besteht darin, diese Funktion Ihrer Firewall bzw. Antivirensoftware zu deaktivieren, zumindest für die folgend aufgelisteten URLs / IP-Adressen des Talk2m-Systems.

Selbstsignierte Zertifikate (Self-Signed Certificates)

HMS Ewon ist selbst Zertifizierungsstelle (Certificate Authority CA) der VPN-Zertifikate die für Talk2m verwendet werden (Talk2m CA). Das hat Vorteile für die Sicherheit von Talk2m, setzt aber voraus, dass die Benutzer den Zertifikaten der Talk2m CA genauso vertrauen, wie Zertifikaten von öffentlichen Zertifizierungsstellen.

Wenn das Ewon-Gerät versucht, eine sichere Verbindung zu einem Talk2m VPN-Server herzustellen, verwendet es ein Zertifikat der Talk2m CA, ein s.g. selbstsigniertes Zertifikat. Die Talk2m CA kann von einigen Firewalls blockiert oder nicht erkannt werden.

Wenn Ihre Firewall die CA-Ursprünge verifiziert, muss sie die Talk2m CA akzeptieren, damit sich der Ewon-Router mit Talk2m verbinden kann.

Talk2m-Statusbenachrichtigung

Wenn Sie sich entscheiden, eine Regel für jede spezifische URL zu erstellen - aufgrund von Firewall-Einschränkungen oder aufgrund des Designs - anstatt die Wildcard-Domain zu verwenden, sollten Sie den Talk2m Status abonnieren (ganz unten). Sie erhalten dann eine Information per Email, wenn es Änderungen bzgl. der VPN-Server gibt (z.B. bei einer Wartung).

Durch diese Benachrichtigung wissen Sie, ob und wann Ihre Regeln innerhalb Ihrer Firewall aktualisiert werden müssen, um eine Unterbrechung der Verbindung zu Talk2m zu verhindern.

Generell empfiehlt sich das Abonnieren des Talk2m Status auch, um jederzeit über ggf. auftretende Störungen informiert zu sein.

Es gibt noch eine weitere Statusseite, diese finden Sie hier. Beide Seiten werden regelmäßig synchronisiert, Updates sollten daher auf beiden Seiten erscheinen.

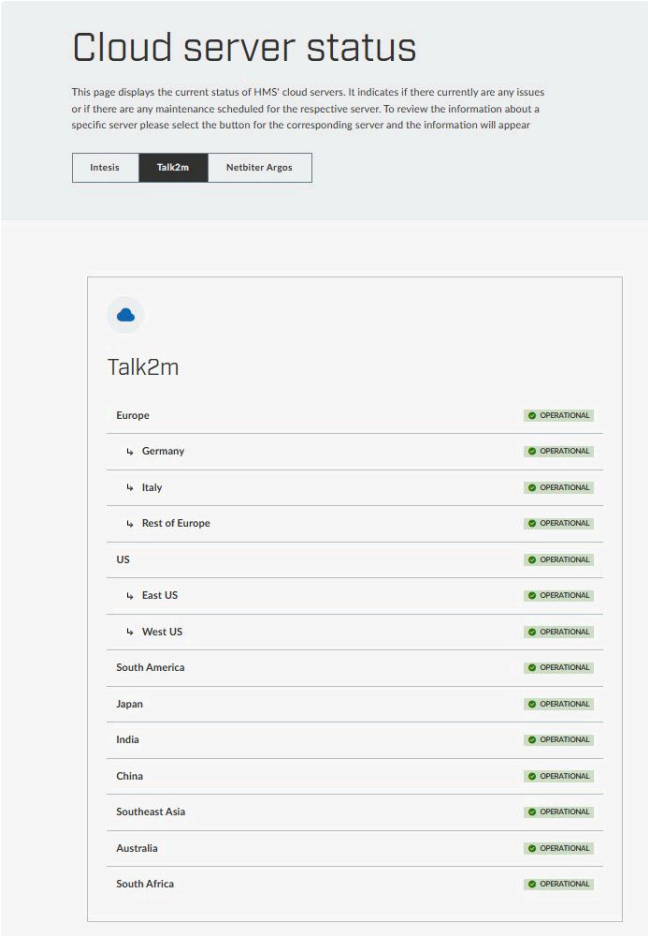

Bild 2: Server Status Seite HMS

Talk2m-Voraussetzungen für Ewon-Router

Im Folgenden werden die Voraussetzungen und Einstellungen im Netzwerk (bzw. in der Firewall) beschrieben, in dem der Ewon-Router mit Talk2m betrieben werden soll. Der Ewon-Router benötigt grundsätzlich IP-Einstellungen (IP-Adresse, Subnet-Maske und DNS-Server), um über seine WAN-Seite eine Internetverbindung herstellen zu können. Diese Einstellungen kann der Router auch per DHCP erhalten.

Die angegebenen Protokolle und deren TCP-Ports müssen im Netzwerk und in der Firewall ausgehend frei sein. Ebenso die genannten URLs und die zugehörigen IP-Adressen der Server dürfen für den Ewon-Router nicht geblockt sein. Der Ewon-Router muss sich mit den folgenden Servern verbinden können:

Access Server

- Protokoll: **HTTPS**, TCP-Port: **443**
- Adressen (URLs):
  - **as.pro.talk2m.com** (Ewon Firmware < 12.2, z.B. Ewon CD, Cosy141)
  - **device.api.talk2m.com** (Ewon Firmware >= 12.2, z.B. Cosy131, Flexy)
  - **device.talk2m.com** (Ewon Cosy+, Firmware >= 20.0)
  - **deviceupdate.talk2m.com** (Ewon Cosy+, wenn die Funktion „Firmware-Update“ im Ewon Web-Interface benutzt wird)

VPN Server

- Protokoll: **UDP**, TCP-Port: **1194** und **TCP**, TCP-Port: **443**
- Adressen (URLs):
  - **device.vpnX.talk2m.com**, wobei X der Nummer des VPN-Servers entspricht.

Wenn die für die Netzwerksicherheit zuständige Firewall keine Wildcard als Schutzregel erlaubt, gibt es eine Liste aller Talk2m VPN-Server für Ewon-Router, die für eine funktionierende VPN-Verbindung notwendig sind. Diese Liste ist nach Gebieten in der Welt unterteilt. Sie enthält die IP-Adressen und die Domänennamen für jeden Talk2m VPN-Server. Mit dieser Liste können Sie die Firewall mit der/den erforderlichen IP-Adresse(n) und Domänennamen für den Ewon-Router einstellen.

Um die URLs aufzulösen, benötigt der Ewon-Router einen entsprechenden DNS-Server in den IP-Einstellungen. Bitte kontrollieren Sie die IP-Einstellungen des Ewon-Routers, ob ein entsprechender DNS-Server eingetragen ist (z.B. Google DNS 8.8.8.8).

Wenn die Internetverbindung über einen Proxy-Server hergestellt wird, dann verwendet Ihr Ewon-Router das TCP-Protokoll.

Der Proxy-Server muss ausgehende Verbindungen auf Port **TCP 443** zum Hostnamen ***.talk2m.com** erlauben.

Talk2m-Voraussetzungen für VPN-Client "eCatcher"

Im Folgenden werden die Voraussetzungen und Einstellungen im Netzwerk (bzw. in der Firewall) beschrieben, in dem der PC betrieben wird und auf dem die Software "eCatcher" (OpenVPN-Client) installiert ist, um die Talk2m-Verbindung herzustellen.

Die angegebenen Protokolle und deren TCP-Ports müssen im Netzwerk und in der Firewall ausgehend frei sein. Ebenso die genannten URLs und die zugehörigen IP-Adressen der Server dürfen für den eCatcher nicht geblockt sein. Der eCatcher muss sich mit den folgenden Servern verbinden können:

Access Server

- Protokoll: **HTTPS**, TCP-Port: **443**
- Adressen (URLs):
  - as.pro.talk2m.com (für eCatcher Ver. < 6.3.5)
  - **client.api.talk2m.com** (für aktuelle eCatcher Ver. >= 6.3.5)

VPN Server

- Protokoll: **UDP**, TCP-Port: **1194** und **TCP**, TCP-Port: **443**
- Adressen (URLs):
  - **client.vpnX.talk2m.com** oder **sclient.vpnX.talk2m.com** wobei X der Nummer des VPN-Servers entspricht.

Wenn die für die Netzwerksicherheit zuständige Firewall keine Wildcard als Schutzregel erlaubt, gibt es eine Liste aller Talk2m VPN-Server für den eCatcher, die für eine funktionierende VPN-Verbindung notwendig sind. Diese Liste ist nach Gebieten in der Welt unterteilt. Sie enthält die IP-Adressen und die Domänennamen für jeden Talk2m VPN-Server. Mit dieser Liste können Sie die Firewall mit der/den erforderlichen IP-Adresse(n) und Domänennamen einstellen.

Wenn es nicht möglich ist alle Talk2m-Server mit *.talk2m.com auf die Whitelist zu setzen, weil dies z.B. aus Sicherheitsgründen nicht gestattet ist, oder die Freigabe per Whitelist nicht funktioniert, ist es ggf. notwendig, die Server-URLs einzeln einzutragen.

Wenn ein Ewon-Router in China in Betrieb genommen wird, wird er automatisch auf einen speziellen NAP-Server verbunden und ist dann von überall aus erreichbar. Eine Verbindung mit dem eCatcher heraus aus China ist nur möglich, wenn sich der entsprechende Ewon-Router auf einem solchen NAP-Server befindet.

Den aktuellen Server eines Ewon-Routers sehen Sie in den eCatcher online/offline Gerätelogs, in eckigen Klammern.

Wenn sich der eCatcher über einen Proxy-Server verbindet, muss dieser Proxy-Server ausgehende Verbindungen auf Port **TCP 443** zum Hostnamen ***.talk2m.com** erlauben.

Weitere Verbindungen

- Während des **Talk2m-Registrierungsassistenten** führt das Ewon-Gerät einen **UDP-Verbindungstest auf Port 1194 zur Talk2m Access Server IP-Adresse** durch, um zu prüfen, ob seine VPN-Verbindung über eine UDP Verbindung aufgebaut werden kann. Wenn dieser Verbindungstest fehlschlägt, wird das Ewon-Gerät auf eine TCP-Verbindung über Port 443 zurückgreifen.
- Während des **Internet-Konfigurationsassistenten** führt das Ewon-Gerät einen **TCP-Verbindungstest auf Port 80 (HTTP) zur IP-Adresse des Talk2m Access Servers** durch, um den Zugang zum Internet zu überprüfen.
  Falls keine Freigabe für Port 80 im Netzwerk vorhanden ist, kann der Verbindungstest im Assistenten deaktiviert werden um diesen trotzdem erfolgreich abzuschließen und die Einstellungen zu übernehmen.
- Ewon-Geräte führen mit den empfohlenen Einstellungen nach jedem Neustart und zusätzlich in der eingestellten zeitlichen Frequenz eine **NTP-Synchronisierung mit der IP „162.159.200.123“ (time.cloudflare.com)** über **Port 123** durch.

Talk2m Connection Checker

Mit dieser Software können die Firewallfreigaben für ein Ewon-Gerät bzw. einen eCatcher-PC getestet werden. Fehlende Freigaben werden hierbei gemeldet.

Den Connection Checker finden Sie **hier** zum Download.

Wenn die Verbindung für ein Ewon-Gerät getestet wird, muss dabei die gleiche Internetverbindung genutzt werden wie die des Ewon, mit identischen IP-Einstellungen am PC. Achten Sie darauf, dass z.B. WLAN oder sonstige weitere Internetschnittstellen am PC deaktiviert sind.

Es muss zwingend die aktuellste Version des Checkers verwendet werden.

Es besteht die Möglichkeit, dass der Test erfolgreich ist, die Verbindung jedoch aufgrund fehlender Freigaben trotzdem nicht funktioniert. Der Checker kann nicht alle Einschränkungen erkennen und ist nur als zusätzliches Werkzeug zu betrachten.

Es besteht z.B. auch die Möglichkeit, dass in der Firewall die MAC-Adresse des Ewons freigegeben werden muss, oder dass z.B. VPN-Verbindungen von der Firewall erst nach einiger Zeit getrennt werden. Diese Einschränkungen kann der Checker nicht erkennen.

Copyright

Erweiterter Haftungsausschluss

Alle technischen Inhalte innerhalb dieses Dokuments können ohne vorherige Benachrichtigung modifiziert werden. Der Inhalt des Dokuments ist Inhalt einer wiederkehrenden Revision. Bei Verlusten durch Feuer, Erdbeben, Eingriffe durch Dritte oder anderen Unfällen, oder bei absichtlichem oder versehentlichem Missbrauch oder falscher Verwendung, oder Verwendung unter unnormalen Bedingungen werden Reparaturen dem Benutzer in Rechnung gestellt. Wachendorff Prozesstechnik ist nicht haftbar für versehentlichen Verlust durch Verwendung oder Nichtverwendung dieses Produkts, wie etwa Verlust von Geschäftserträgen. Wachendorff Prozesstechnik haftet nicht für Folgen einer sachwidrigen Verwendung.

Ansprechpartner

Wachendorff Prozesstechnik GmbH & Co. KG

: support@wachendorff.de

: +49-6722/9965-966

AGB´s Wachendorff Prozesstechnik GmbH & Co. KG

Datenschutz Wachendorff Prozesstechnik GmbH & Co. KG

Impressum Wachendorff Prozesstechnik GmbH & Co. KG