Wachendorff Prozesstechnik GmbH & Co. KG
Industriestr. 7, D-65366 Geisenheim
Fon: 0 67 22 / 99 65 -20
Fax: 0 67 22 / 99 65 -78
E-Mail: wp@wachendorff.de
www.wachendorff-prozesstechnik.de

Technical Note

Ewon

TN 1102

Talk2M-Voraussetzungen

Talk2M Requirements

Version: 1.6

Inhaltsverzeichnis

Deutsch (for English please see next page)

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	Bemerkung
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

Hinweis: Die aktuelle Version des Dokuments finden Sie in der Fußzeile.

1. Einleitung

Diese Technical Note beschreibt die Voraussetzungen, die erfüllt sein müssen, damit der Verbindungsdienst Talk2M (Talk to Machine) für Ewon-Router genutzt werden kann. Grundlegende Informationen zum Fernwartungssystem Ewon finden Sie in der TN 1101 "Fernwartungssystem Ewon".
Talk2M arbeitet als s. g. Rendezvous-Server mit OpenVPN zur Verschlüsselung der Datenübertragung, d. h. 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 von Ewon ist!

2. Funktionsweise Talk2M

Die Ewon-Router sind nach der Einrichtung für Talk2M mit einem der weltweit verteilten Talk2M-Server verbunden. Diese Verbindung sollte eine permanente Verbindung (auch initiierte Verbindung möglich) über WAN (Netzwerk), GSM (Mobilfunk) oder WLAN sein.
Wenn der Anwender sich auf einen Ewon-Router verbinden möchte, stellt er mittels der "eCatcher"-Software eine Verbindung zu seinem Talk2M-Konto her und wählt dann das jeweilige Ewon-Gerät in seinem Konto aus (s. TN 1210 "eCatcher").
eCatcher stellt dann zunächst eine HTTPS-Verbindung zum s. g. Access-Server her. Der Access-Server weiß, auf welchem Talk2M-Server sich der Ewon-Router gerade befindet. Danach werden eine OpenVPN-Verbindung zu dem jeweiligen Talk2M-Server und die Verbindung auf den Ewon-Router hergestellt. Der Anwender ist dann mit dem Ewon-Router und damit mit dem lokalen Netzwerk, das an den Router angeschlossen ist, verbunden.

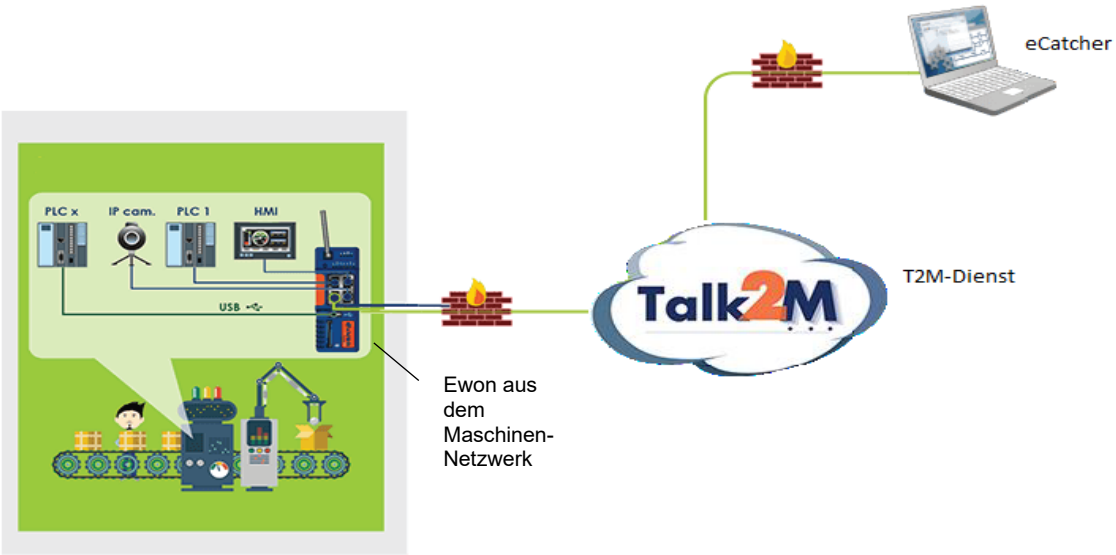


Abbildung 1: Talk2M Prinzip

3. 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:

- Erforderlich: *.talk2M.com:443 (TCP-Protokoll)
- Empfohlen: *.talk2M.com:443 (TCP-Protokoll) und *.talk2M.com:1194 (UDP-Protokoll)

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.
- 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.

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

Hinweis: 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!

Hinweis: 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(s) zu verbinden.

3.1. Deep-Packet-Inspection von TLS/SLL verschlüsseltem Datenverkehr

Einige Firewalls oder Antiviren-Software 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.

- In einem Ewon, während der Ausführung des T2M-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 / Anti-Virus-Software zu deaktivieren, zumindest für die folgend aufgelisteten URLs / IP-Adressen des Talk2M-Systems!

3.2. 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 das die Benutzer den Zertifikaten der Talk2M CA genauso vertrauen wie Zertifikaten von öffentlichen Zertifizierungsstellen.

Wenn das Ewon-Gerät versucht, über die URL device.api.talk2m.com (as.pro.talk2m.com) 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!

3.3. Liste der Talk2M VPN Server

Falls die für die Netzwerksicherheit zuständige Firewall keine Wildcard als Schutzregel erlaubt, finden Sie eine Liste aller Talk2M VPN-Server auf der Ewon Support-Website.

Diese Liste ist nach Gebieten in der Welt unterteilt. Sie enthält die IP-Adressen und die Domänennamen für jeden Talk2M VPN-Server.

Dank dieser Liste können Sie die Firewall mit der/den erforderlichen IP-Adresse(n) und / oder Domänennamen einstellen.

3.4. VPN Server Switch-Benachrichtigung

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, haben Sie die Möglichkeit, die Mailingliste HMS Customer and Distributor Information System CDIS zu abonnieren, die verwendet wird, um eine Benachrichtigung zu versenden, wenn Ewon einen Talk2M VPN-Serverwechsel durchführt, wodurch die IP-Adresse eines solchen Talk2M VPN-Servers geändert wird.

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.

4. Talk2M-Voraussetzungen für Ewon Router

Voraussetzungen und Einstellungen im Netzwerk und in der Firewall, in dem der Ewon-Router mit Talk2M betrieben werden soll.
Der Ewon-Router benötigt IP-Einstellungen (IP-Adresse, Subnet-Maske und DNS-Server), um über die WAN-Seite eine Internetverbindung herstellen zu können.

Folgende Protokolle und deren TCP-Ports müssen im Netzwerk und in der Firewall ausgehend frei sein. Ebenso die genannten URLs respektive 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:

4.1. Access Server

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

4.2. VPN Server

- Protokoll: **UDP**, TCP-Port: **1194** oder **TCP**, TCP-Port: **443**
- Adressen (URLs):
  - **device.vpnX.talk2m.com**, wobei X die Nummer des VPN-Servers ist. Die VPN-Servernummer kann zwischen 1 und 100 liegen.

Hinweis: Derzeit sind noch nicht alle Server aktiv. Die Platzhalter dienen als Puffer für hinzukommende Server. Dadurch können zurzeit noch nicht alle Adressen gepingt werden!

Hinweis: Wenn es nicht möglich ist alle Talk2M-Server mit ***.talk2M**.com auf die Whitelist zu setzen oder aus Sicherheitsgründen nicht gestattet ist, raten wir Ihnen alle oben aufgelisteten Server-URLs einzeln einzutragen!

Hinweis: 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. Bsp. Google DNS 8.8.8.8).

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

Wenn Ihr Ewon Firmware Ver. >= 6.4s6 sich über einen Proxy-Server verbindet, sollte dieser Proxy-Server auf der lokalen Site ausgehende Verbindungen auf Port **TCP 443** zum Hostnamen ***.talk2m.com** erlauben.

5. Talk2M-Voraussetzung für VPN-Client "eCatcher "

Voraussetzungen und Einstellungen im Netzwerk und in der Firewall, in dem der PC betrieben wird, auf dem "eCatcher" (OpenVPN-Client) läuft um die Talk2M-Verbindung herzustellen.

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

5.1. Access Server

- Protokoll: **HTTPS**, TCP-Port: **443**
- Adressen (URLs):
  - **as.pro.talk2m.com** (für eCatcher Ver. < 6.35)
  - **client.api.talk2m.com** (für eCatcher Ver. >= 6.3.5)

5.2. VPN Server

- Protokoll: **UDP**, TCP-Port: **1194** oder **TCP**, TCP-Port: **443**
- Adressen (URLs):
  - **client.vpnX.talk2m.com**, wobei X die Nummer des VPN-Servers ist. Die VPN-Servernummer kann zwischen 1 und 50 liegen.
  - NAP Server in China:
    - Primär: **sclient.vpn30.talk2m.com**
    - Backup: **sclient.vpn31.talk2m.com**

Hinweis: Derzeit sind noch nicht alle 50 Server aktiv. Die Platzhalter dienen als Puffer für hinzukommende Server. Dadurch können zurzeit noch nicht alle 50 Adressen gepingt werden!

Hinweis: Wenn es nicht möglich ist alle Talk2M-Server mit ***.talk2M**.com auf die Whitelist zu setzen oder aus Sicherheitsgründen nicht gestattet ist, raten wir Ihnen alle oben aufgelisteten Server-URLs einzeln einzutragen!

Hinweis: Sie müssen den NAP-Server verwenden, wenn sich der Ewon VPN-Router in China befindet. Wenn sich der Ewon VPN-Router außerhalb Chinas befindet, der Benutzer aber in China ist, sind möglicherweise zusätzliche URLs erforderlich.

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

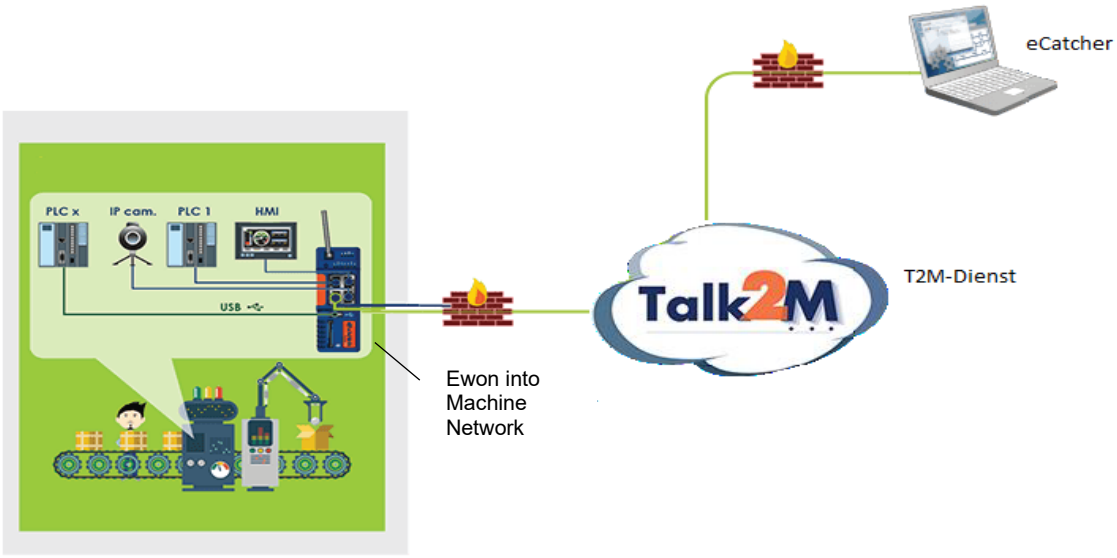
Wenn Ihr Ewon Firmware Ver. >= 6.4s6 sich über einen Proxy-Server verbindet, sollte dieser Proxy-Server auf der lokalen Site ausgehende Verbindungen auf Port **TCP 443** zum Hostnamen ***.talk2m.com** erlauben.

1. Introduction

This Technical Note describes the requirements that must be met in order to use the Talk2M (Talk to Machine) connection service for Ewon routers.
Talk2M works as a so-called rendezvous server with OpenVPN to encrypt the data transfer, i.e. the routers connect to the service on the field side and on the user side there is the cost- and license-free software "eCatcher" (quasi an OpenVPN client) with which the connection to the service and to the routers is established. The connection between the user and the router is made in the service, so that only outgoing connections are used on both sides. Thus it is not necessary to open ports in the networks in detail, which is an essential security criterion for the remote maintenance solution of Ewon!

2. Talk2M Functionality

The Ewon routers are connected to one of the worldwide distributed Talk2M servers after the setup for Talk2M. This connection should be a permanent connection (initiated connection possible) via WAN (network), GSM (mobile radio) or WLAN.
If the user wants to connect to an Ewon router, he connects to his Talk2M account using the "eCatcher" software and then select the Ewon device in his account.
eCatcher then first establishes an HTTPS connection to the so-called access server. The access server knows on which Talk2M server the Ewon router is currently located. An OpenVPN connection to the respective Talk2M server and the connection to the Ewon router are then established. The user is then connected to the Ewon router and thus to the local network connected to the router.



Picture 1: Talk2M Principle

3. Firewall Configuration

Talk2M is a highly available system! In order to guarantee availability at all times and under all circumstances it is necessary in some situations or under certain circumstances to "move" a Talk2M account or an Ewon router to another VPN server. In this case the eCatcher must then also connect to another VPN server. Therefore the firewall rule should look like this:

- Required: *.talk2M.com:443 (TCP protocol)
- Recommended: *.talk2M.com:443 (TCP protocol) and *.talk2M.com:1194 (UDP protocol)

If all Talk2M servers with *.talk2M.com are on the whitelist, moving an account or router will not cause connection problems.

- Remote access is no longer possible.
- If your Ewon VPN router uses Talk2M as e-mail server or SMS relay, the alerting and notification no longer works.
- If your Ewon VPN router uses the DataMailbox, historical data is no longer sent to the DataMailbox.

Note: A server change from one server to another may be necessary during VPN server maintenance or due to a major VPN server problem.

Note: If your firewall is IP-based, please make sure that the IP addresses of the above URLs can be reached by the Ewon router!

Note: If your firewall has an option "Block OpenVPN connection" (or a similar option), disable it because Talk2M uses OpenVPN technology to connect users to their Ewon(s).

3.1. Deep-Packet-Inspection of TLS/SSL Encrypted Traffic

Some firewalls or anti-virus software contain a so-called deep packet inspection DPI. This monitors the encrypted data traffic sent and received by an application.
In this mechanism, the firewall or antivirus software replaces the Talk2M HTTPS certificate with its own certificate. This can be considered a "Man in the Middle" attack.
This method of replacing certificates is rejected by eCatcher and the Ewon VPN routers for security reasons!

If you encounter this problem, the following error message appears:

- In eCatcher, while connecting to the Ewon VPN-router:
  Server communication error: peer not authenticated.
- In the Ewon VPN-router, while running the Talk2M wizard: HTTPS dialog failed
  (Server certificate verification failed: certificate issue for a different hostname, issue is not trusted

The only solution is to disable the Deep Packet Inspection feature in the firewall / anti-virus software, at least for our URLs/IP adresses.

3.2. Self-Signed Certificates

HMS Ewon itself is the Certificate Authority CA of the VPN certificates used for Talk2M (Talk2M CA). This has advantages for the security of Talk2M, but requires that the users trust the certificates of the Talk2M CA just as much as certificates from public certification authorities.

When the Ewon device tries to establish a secure connection to a Talk2M VPN server via the URL device.api.talk2m.com (as.pro.talk2m.com), it uses a certificate from the Talk2M CA, a self-signed certificate. The Talk2M CA can be blocked or not recognised by some firewalls.

If your firewall verifies the CA origins, it must accept the Talk2M CA so that the Ewon router can connect to Talk2M!

3.3. List of Talk2M VPN Server

If the firewall responsible for network security does not allow a wildcard as a protection rule, you will find a list of all Talk2M VPN servers on the Ewon support website.

This list is divided by areas in the world. It contains the IP addresses and domain names for each Talk2M VPN server.

This list allows you to set the firewall with the required IP address(es) and/or domain name(s).

3.4. VPN Server Switch Notification

If you decide to create a rule for each specific URL - due to firewall restrictions or due to design - instead of using the wildcard domain, you have the option to subscribe to the HMS Customer and Distributor Information System CDIS mailing list, which is used to send a notification when Ewon performs a Talk2M VPN server switch, thereby changing the IP address of such Talk2M VPN server.

This notification tells you if and when your rules need to be updated within your firewall to prevent an interruption of the connection to Talk2M ...

4. Talk2M Requirements for Ewon Router

Requirements and settings in the network and in the firewall in which the Ewon router is to be operated with Talk2M.
The Ewon router requires IP settings (IP address, subnet mask, and DNS server) to establish an Internet connection from the WAN side.

The following protocols and their TCP ports must be free from the network and firewall. Likewise, the named URLs and the corresponding IP addresses of the servers must not be blocked for the Ewon router. The Ewon router must be able to connect to the following servers:

4.1. Access Server

- Protocol: **HTTPS**, TCP port: **443**
- Adresses (URLs):
  - **as.pro.talk2m.com** (Ewon Firmware < 12.2)
  - **device.api.talk2m.com** (Ewon Firmware >= 12.2)
  - **device.talk2m.com** (Ewon Cosy+, Firmware >= 20.0)
  - **deviceupdate.talk2m.com** (If the „Firmware-Update“ function is used in the Ewon Web-Interface)

4.2. VPN Server

- Protocol: **UDP**, TCP port: **1194** or **TCP**, TCP port: **443**
- Adresses (URLs):
  - **device.vpnX.talk2m.com**, where X is the number of the VPN server. The VPN server number can be between 1 and 100.

Note: Currently not all servers are active. The placeholders serve as buffers for additional servers. This means that not all addresses can be pinged at the moment!

Note: If it is not possible to whitelist all Talk2M servers with ***.talk2M**.com or if it is not allowed for security reasons, we advise you to enter all server URLs listed above individually!

Note: To resolve the URLs, the Ewon router needs an appropriate DNS server in the IP settings. Please check the IP settings of the Ewon router, if a corresponding DNS server is registered (e.g. Google DNS 8.8.8.8)?

Note: If the Internet connection is established via a proxy server, your Ewon VPN router uses the TCP protocol.

If your Ewon firmware version >= 6.4s6 connects via a proxy server, this proxy server on the local site should allow outgoing connections on port **TCP 443** to hostname ***.talk2m.com**.

5. Talk2M Requirements for VPN client "eCatcher "

Requirements and settings in the network and in the firewall in which the PC is used to run "eCatcher" to establish the Talk2M connection.

The following protocols and their TCP ports must be free from the network and firewall. Also the mentioned URLs respectively the corresponding IP addresses of the servers must not be blocked for eCatcher. eCatcher must be able to connect to the following servers:

5.1. Access Server

- Protocol: **HTTPS**, TCP port: **443**
- Adresses (URLs):
  - **as.pro.talk2m.com** (for eCatcher Ver. < 6.35)
  - **client.api.talk2m.com** (for eCatcher Ver. >= 6.3.5)

5.2. VPN Server

- Protocol: **UDP**, TCP port: **1194** or **TCP**, TCP port: **443**
- Adresses (URLs):
  - **client.vpnX.talk2m.com**, where X is the number of the VPN server. The VPN server number can be between 1 and 50.
  - NAP server in China:
    - Primary: **sclient.vpn30.talk2m.com**
    - Backup: **sclient.vpn31.talk2m.com**

Note: Currently not all 50 servers are active. The placeholders serve as a buffer for added servers. Therefore not all 50 addresses can be pinged at the moment!

Note: If it is not possible to whitelist all Talk2M servers with ***.talk2M**.com or if it is not allowed for security reasons, we advise you to enter all server URLs listed above individually!

Note: You must use the NAP server if the Ewon VPN router is located in China. If the Ewon VPN router is located outside China, but the user is in China, additional URLs may be required.

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

Anwendungsberatung, Produktauswahl
(Zur Geräteauswahl vor einer Kaufentscheidung.)
wenden Sie sich bitte an:

T: +49 6722 9965-544
M: Beratung@wachendorff.de

Technische Unterstützung
(Bei der Inbetriebnahme oder im laufenden Betrieb.)
wenden Sie sich bitte an:

T: +49 6722 9965-966
M: Support@wachendorff.de

WACHENDORFF
Prozesstechnik GmbH & Co. KG

Wachendorff Prozesstechnik GmbH & Co. KG
Industriestrasse 7 . D-65366 Geisenheim

Tel.: +49 (0) 6722 / 9965 - 20
Fax: +49 (0) 6722 / 9965 - 78
E-Mail: wp@wachendorff.de
www.wachendorff-prozesstechnik.de